

Dr. Mehmet Bedii KAYA
Furkan Güven TAŞTAN

KİŞİSEL VERİ KORUMA HUKUKU

Mevzuat · İçtihat · Bibliyografya



GÜNCELLENMİŞ

2023

ÇEVİRİMİÇİ
TAM SÜRÜM

KİŞİSEL VERİ KORUMA HUKUKU

Mevzuat - İctihat - Bibliyografya

Doç. Dr. Mehmet Bedii KAYA

Furkan Güven TAŞTAN

İstanbul Bilgi Üniversitesi

Ankara Yıldırım Beyazıt Üniversitesi

Hukuk Fakültesi

Hukuk Fakültesi

Bilişim ve Teknoloji Hukuku Ana Bilim Dalı

Medeni Hukuk Ana Bilim Dalı

Öğretim Üyesi

Araştırma Görevlisi

KİŞİSEL VERİ KORUMA HUKUKU

Mevzuat - İçtihat - Bibliyografya

Kişisel Verilerin Korunması Kanunu

Yönetmelikler

Tebliğler

Düzenleyici Kurul Kararları

Diğer Kurul Kararları

Taahhütnameler

Veri İhlali Bildirimleri

Kurul Duyuruları (Türkçe ve İngilizce)

İlgili Diğer Mevzuat

Avrupa Birliği Düzenlemeleri

Uluslararası Düzenlemeler

Ulusal ve Uluslararası İçtihatlar

Bibliyografya

Nisan 2023 itibariyle güncel düzenlemeleri içerir.

Çevrimiçi Sürüm 2.6

ÖNSÖZ

Devletlerden, şirketlere, işverenlerden aile üyelerine kadar hemen herkesteki başkası hakkında bilgi sahibi olma arzusunun varlığı, modern toplumun en temel sorunlarından biri haline getirmiştir. Temel bir hak olarak kişisel verilerin korunmasını talep etme hakkı bu sorunun önlenmesindeki en önemli hukuk enstrümanlarından biridir.

Kişisel verilerin korunmasıyla ilgili hem normatif düzenlemelerin hem de içtihatların sayısı sürekli olarak çoğalmaktadır. Bu hakkın uygulanmasına ilişkin olarak Avrupa Konseyi, Avrupa Birliği ve bunun ötesinde dünyanın birçok ülkesinde kişisel verilerle ilgili müstakil düzenlemeler yapıldığına ve bu alanla ilgili bağımsız kurumlar kurulmaktadır. Kişisel verilerin korunmasını talep etme hakkının dünyadaki hemen her meridyene dokunmaya başlaması, aynı zamanda kişisel veriler açısından yeni bir farkındalık dönemine girildiğini de göstermektedir.

Her ne kadar Türkiye’de başlangıç noktası olarak 2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu (“KVKK”) esas alınsa da bu dönemden önce de Türk hukukunda kod kanun olmaksızın dağınık şekilde yer alan düzenlemelerle sürdürülen bir uygulama bulunuyordu. Ancak KVKK, bu alanda kurumsal çerçeveyi çizmiş ve Kişisel Verileri Koruma Kurumu’nu bu çerçevenin temel aktörü haline getirmiştir.

Bilişim ve teknoloji hukuku alanında çalışan akademisyenler olarak hem dünyada hem Türkiye’de bu dinamik hukuk alanındaki gelişmeleri yakından takip etmek amacıyla ekranınızda yer alan bu çalışmayı hazırladık. Amacımız, kişisel veri koruma hukuku alanındaki mevzuat, içtihat ve Türkçe akademik çalışmalara pratik erişim imkânı sağlamaktır. Bir cümlede özetlemek mümkün olmamakla birlikte bu çalışmada, Kişisel Verileri Koruma Kurulu’nun karar ve duyurularından ilişkili kanun ve ikincil düzenlemelere, dünyadaki önemli regülasyonlardan içtihatlarla kadar çok geniş olarak değerlendirilebilecek bir yelpazede metinleri derlemeye çalıştık. Bunu yaparken amacımız, bu alanda çalışan akademisyen ve uygulamacılar için temel kaynaklara erişebilecekleri tek bir nokta ihdas etmektir.

Bu çalıřmaya bugüne kadar katkı yapan tüm akademisyen ve uygulamacılara teřekkür ediyoruz. Bu kapsamda, bu versiyon için desteklerini esirgemeyen meslektařlarımız Sena Kontođlu ve Ayře Sidal Yařar'a katkıları için özel olarak teřekkür etmek isteriz. Kontrollere rađmen bu çalıřmada řüphesiz eksiklikler ve hatalar çıkacaktır. Çalıřmanın daha iyi bir hale gelmesi için deđerli katkılarınızı, yorumlarınızı ve eleřtirilerinizi mehmet@mbkaya.com veya furkanguventastan@gmail.com adresleri üzerinden bizimle paylařabilirsiniz.

Açık eriřimin akademiye olan faydasının bilincinde olan akademisyenleriz. Bu çalıřmanın tamamına veya bir kısmına belirli bir formatta veya eriřilebilirlik aracıyla kullanmak isterseniz bizimle iletiřime geçmeniz yeterlidir. Bu konuda makul olan her türlü desteđi vermekten memnuniyet duyarız. Keza özel bir engellilik durumu sebebiyle dosyanın belirli bir formatta oluřturulmasını talep ederseniz size bu konuda da yardımcı olmaktan memnuniyet duyarız.

Ekranınızdaki bu çalıřma, yedi bin+ sayfadan oluřan bir dijital dosyasıdır. Konforlu bir çalıřma deneyimi için çalıřmayı teřkil eden bu PDF dosyası oluřturulurken her bir bařlık için yer imi atanmıřtır. Yer imleri panelinin otomatik olarak açılmaması halinde, PDF okuyucunuzun Göster menüsünden yer imleri panelini açabilirsiniz.

Çalıřmanın akademi ve uygulamaya faydalı olmasını temenni ederiz!

Yeni bir sürümde buluřmak dileđiyle...

Mehmet Bedii Kaya - Furkan Güven Tařtan

Nisan 2022

Çalışmanın güncel sürümünü ücretsiz olarak aşağıdaki linklerden veya QR kod kullanarak indirebilirsiniz:



<https://mbkaya.com/hukuk/veri-koruma-hukuku.pdf>

<https://sinerjik.org/hukuk/veri-koruma-hukuku.pdf>

GÜNCELLEME GEÇMİŞİ

Çevrim İçi Sürüm 2.6 (Tam Sürüm) / Nisan 2023

- Kurul tarafından yayınlanan yeni karar özetleri eklendi.
- Güncel veri ihlal bildirimleri eklendi.
- Yurtdışına aktarım taahhütnamesi listesi güncellendi.
- Bibliyografya güncellendi.
- Yeni Kurul duyuruları eklendi: 27.03.2023 - Vekaleten Yapılacak Şikayetlerin Elektronik Ortamda Kurula İletilmesine İlişkin Kamuoyu Duyurusu, 23.03.2023 - Seçim Faaliyetleri Kapsamında Siyasi Partiler ve Bağımsız Adaylar Tarafından İşlenen Kişisel Veriler Hakkında Kamuoyu Duyurusu
- 1211 sayılı Türkiye Cumhuriyet Merkez Bankası Kanunu eklendi.
- Anayasa Mahkemesi - 7246 sayılı Kanun - Rekabet Kanunu Kararı (E. 2020/67) kararı eklendi.

Çevrim İçi Sürüm 2.5 (Tam Sürüm) / Ocak 2023

- Güncel veri ihlal bildirimleri eklendi.
- Bibliyografya güncellendi.
- KVKK Depremden Etkilenen İlgili Kişilere ve Veri Sorumlularına Yönelik Kamuoyu Duyurusu eklendi.

Çevrim İçi Sürüm 2.5 (Tam Sürüm) / Ocak 2023

- Güncel veri ihlal bildirimleri eklendi.
- Bibliyografya güncellendi.
- İdari para cezası tutarları 2023 oranına göre güncellendi.
- KVKK - 17.12.2021 - Mağazalarda SMS Doğrulama Duyurusu eklendi.
- Anayasa Mahkemesi - 715 sayılı Kanun - MİT Kanunu Kararı (E. 2018/137) eklendi.
- Anayasa Mahkemesi - Ümit Eyüpoğlu Kararı (2018/6161) eklendi.
- Anayasa Mahkemesi - Alper Erarslan Kararı (2018/16857) eklendi.
- Anayasa Mahkemesi - Fırat Gerçek Kararı (2019/25604) eklendi.
- Yargıtay Kararı - 12. Ceza Dairesi (E. 2020/974) eklendi.
- Yargıtay Kararı - 6. Ceza Dairesi (E. 2021/10682) eklendi.

- Avrupa Birliđi - European Declaration on Digital Rights and Principles for the Digital Decade eklendi.
- ABAD - Österreichische Post (C-154/21) eklendi.
- ABAD - Autoriteit Persoonsgegevens (C-245/20) eklendi.
- ABAD - Meta Platforms Ireland (Case C-319/20) eklendi.
- ABAD - PNR Directive (C-817/19) eklendi.
- OECD Declaration on Government Access to Personal Data Held by Private Sector Entities eklendi.
- Sađlık Bilgi Sistemleri Hakkında Yönetmelik eklendi.
- BTK - 27.12.2016 tarihli Posta Gönderilerine İlişkin Güvenlik Tedbirlerine Yönelik Usul ve Esaslar eklendi.
- AİHM kararları kısmı güncellendi.

Çevrimiçi Sürüm 2.4 (Tam Sürüm) / Eylül 2022

- Güncel veri ihlal bildirimleri eklendi.
- Bibliyografya güncellendi.
- BDDK - Sır Niteliğindeki Bilgilerin Paylaşılması Genelgesi (2022/1) eklendi.

Çevrimiçi Sürüm 2.3 (Tam Sürüm) / Ağustos 2022

- Kurul tarafından yayınlanan yeni karar özetleri eklendi.
- Güncel veri ihlal bildirimleri eklendi.
- İngilizce duyurular kısmına “Binding Corporate Rules Application Form” eklendi.
- Anayasa Mahkemesi - 5188 sayılı Özel Güvenlik Hizmetlerine Dair Kanun Kararı (E. 2021/42) eklendi.
- Yargıtay 14. Hukuk Dairesi (E. 2016/2792) eklendi.
- Yargıtay 12. Ceza Dairesi (E. 2019/4369) eklendi.
- ABAD’ın önemli kararları tam metin olarak eklendi.
- ABD - Virginia Consumer Data Protection Act (CDPA) eklendi.
- ABD - Colorado Privacy Act (CPA) eklendi.

Çevrimiçi Sürüm 2.2 (Tam Sürüm) / Temmuz 2022

- Kurul tarafından yayınlanan yeni karar özetleri eklendi.
- Güncel veri ihlal bildirimleri eklendi.
- AİHM kararları güncellendi.
- Kimlik Bildirme Kanununun Uygulanması ile İlgili Yönetmelik güncellendi.
- Tapu ve Kadastro Verilerinin Paylaşımı Hakkında Yönetmelik kaldırıldı, yerine Tapu ve Kadastro Verilerinin İşlenmesi ve Elektronik Ortamda Yapılacak İşlemler Hakkında Yönetmelik eklendi.
- Tıbbi Cihaz Klinik Araştırmaları Yönetmeliği eklendi.

Çevrimiçi Sürüm 2.1 (Tam Sürüm) / Haziran 2022

- Kurul tarafından yayınlanan yeni karar özetleri eklendi.
- Güncel veri ihlal bildirimleri eklendi.
- Anayasa Mahkemesi: 1 numaralı CBK Kararı (MASAK) (E. 2019/96), Ümit Karaduman Kararı (2020/20874), Ramazan Şahin Kararı (2018/11988), Bülent Kaya Kararı (2013/2941), Ali Çığır Kararı (2015/19298), B.K. Kararı (2014/14189) kararları eklendi.
- Yargıtay: 22. Hukuk Dairesi (E. 2017/21857), 20.Hukuk Dairesi (E. 2017/2277), 12. Ceza Dairesi (E. 2017/2960) kararları eklendi.
- Bursa BAM - 6. Hukuk Dairesi (E. 2019/2251) kararı eklendi.
- Kuzey Kıbrıs Türk Cumhuriyeti - 89/2007 Kişisel Verilerin Korunması Yasası eklendi.
- Güvenlik Soruşturması ve Arşiv Araştırması Yapılmasına Dair Yönetmelik eklendi.
- Vergi Usul Kanunu Genel Tebliği (Sıra No: 538) eklendi.

Çevrimiçi Sürüm 2.0 (Tam Sürüm) / Nisan 2022

- Çalışmanın tüm sistematığı yenilenmiştir. Mevzuat güncellenmiş; ilgili tüm KVK Kurulu kararları eklenmiş; KVK Kurulu'nun önemli sayılacak duyuruları dahil edilmiş; literatür taraması yapılarak ilgili tüm akademik çalışmalar eklenmiştir.

Çevrimiçi Sürüm 1.3 / 2. Baskı / 2019 Eylül

- Çalışmanın sistematığı yenilenmiş ve yeni mevzuat ve içtihat metinleri eklenmiş; çalışmaya bibliyografya kısmı dâhil edilmiştir.

Çevrimiçi Sürüm 1.2 / 1. Baskı / 2018 Ocak

- Türk hukukuna ilişkin yeni mevzuat metinleri ve içtihatları eklenmiştir.

Çevrimiçi Sürüm 1.1 / 2017 Şubat

- Kullanım kolaylığı sağlamak adına tasarım yenilenerek güncellenen mevzuat metinleri yeniden sıralanmıştır.

Çevrimiçi Sürüm 1.0 / 2016 Ekim

- Kişisel verilerin korunmasına dair ulusal ve uluslararası temel kaynaklar eklenmiştir.

İÇİNDEKİLER - ANA BAŞLIKLAR

ÖNSÖZ	iii
GÜNCELLEME GEÇMİŞİ	vi
İÇİNDEKİLER - ANA BAŞLIKLAR	x
İÇİNDEKİLER - TÜM İNDEKS.....	xii
ANAYASA	1
KİŞİSEL VERİLERİN KORUMASI KANUNU.....	2
GEREKÇE.....	25
TEMEL YÖNETMELİKLER.....	51
TEBLİĞLER VE GENELGELER.....	148
USUL/ESASLAR VE DİĞER GENEL KONULAR	199
İDARİ PARA CEZASI TUTARLARI	241
İNGİLİZCE MEVZUAT.....	242
KİŞİSEL VERİLERİ KORUMA KURULU İLKE KARARLARI.....	291
KİŞİSEL VERİLERİ KORUMA KURULU KARARLARI	337
YURTDIŞINA KİŞİSEL VERİ AKTARMA TAAHHÜTNAMELERİ	1633
KİŞİSEL VERİ İHLAL BİLDİRİMİ FORMU.....	1651
VERİ İHLALİ BİLDİRİMLERİ.....	1660
DİĞER KURUL KARARLARI VE DUYURULARI.....	1876
İNGİLİZCE DUYURULAR	1974
TÜRK HUKUKUNDAKİ DİĞER DÜZENLEMELER	2053
KANUNLAR.....	2054
TÜZÜKLER.....	2410
YÖNETMELİKLER.....	2414
TEBLİĞLER.....	2931
CUMHURBAŞKANLIĞI KARARNAMELERİ	2962

MUHTELİF DÜZENLEMELER.....	2969
ANAYASA MAHKEMESİ NORM DENETİMİ KARARLARI.....	2975
ANAYASA MAHKEMESİ BİREYSEL BAŞVURU KARARLARI.....	4309
YARGITAY KARARLARI	4934
DANIŞTAY KARARLARI	5131
BÖLGE İDARE MAHKEMESİ KARARLARI.....	5575
UYUŞMAZLIK MAHKEMESİ KARARLARI	5644
BÖLGE ADLİYE MAHKEMESİ KARARLARI.....	5654
ADLİ YARGI İLK DERECE MAHKEMELERİ KARARLARI.....	5762
KAMU İHALE KURULU KARARLARI.....	5773
ULUSLARARASI DÜZENLEMELER	5837
AVRUPA KONSEYİ.....	5838
AVRUPA BİRLİĞİ.....	5885
ULUSLARARASI DİĞER DÜZENLEMELER.....	6258
AVRUPA BİRLİĞİ ADALET DİVANI KARARLARI (GENEL ÇERÇEVE)	6271
AVRUPA BİRLİĞİ ADALET DİVANI KARARLARI (TAM METİN).....	6326
AVRUPA İNSAN HAKLARI MAHKEMESİ (AİHM) KARARLARI.....	6610
MUHTELİF ÜLKE DÜZENLEMELERİ	6656
BİBLİYOGRAFYA	7327

İÇİNDEKİLER - TÜM İNDEKS

ÖNSÖZ	iii
GÜNCELLEME GEÇMİŞİ	vi
İÇİNDEKİLER - ANA BAŞLIKLAR	x
İÇİNDEKİLER - TÜM İNDEKS.....	xii
ANAYASA	1
KİŞİSEL VERİLERİN KORUMASI KANUNU.....	2
GEREKÇE.....	25
KVKK Genel Gerekçe.....	26
KVKK Madde Gerekçeleri	31
Anayasa Madde 20(3) Gerekçesi.....	50
TEMEL YÖNETMELİKLER.....	51
Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği	52
Kişisel Verileri Koruma Kurumu Disiplin Amirleri Yönetmeliği	64
Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik	67
Kişisel Verileri Koruma Uzmanlığı Yönetmeliği.....	75
Kişisel Verileri Koruma Kurumu Personeli Görevde Yükselme ve Ünvan Değişikliği Yönetmeliği	88
Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik	98
Veri Sorumluları Sicili Hakkında Yönetmelik	104
Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik.....	115
Kişisel Sağlık Verileri Hakkında Yönetmelik.....	123
Sosyal Güvenlik Kurumu Nezdindeki Verilerin Korunmasına ve İşlenmesine İlişkin Yönetmelik.....	132
TEBLİĞLER VE GENELGELER.....	148
Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğ	149
Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ.....	156
Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ	160
2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi	164

BDDK - Sır Niteliğindeki Bilgilerin Paylaşılması Genelgesi (2022/1).....	168
USUL/ESASLAR VE DİĞER GENEL KONULAR	199
Kullanıcı Güvenliğine İlişkin Veri Sorumluları Tarafından Alınması Tavsiye Edilen Teknik ve İdari Tedbirler.....	200
Katılım Belgesinin Verilmesine Dair Usul ve Esaslar	203
Bağlayıcı Şirket Kuralları.....	208
Veri Sorumluları İçin Bağlayıcı Şirket Kuralları Başvuru Formu	210
Veri Sorumluları İçin Bağlayıcı Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin Yardımcı Doküman	224
İDARİ PARA CEZASI TUTARLARI	241
İNGİLİZCE MEVZUAT.....	242
Law on the Protection of Personal Data	243
By-Law On Data Controllers Registry	266
By-Law on Erasure, Destruction or Anonymization of Personal Data	277
Comminuque on the Principles and Procedures for the Request to Data Controller	283
Communique on Principles and Procedures to be Followed in Fullfillment of the Obligation to Inform....	287
KİŞİSEL VERİLERİ KORUMA KURULU İLKE KARARLARI.....	291
2022/388 sayılı KVKK Kararı - Belediyelerin Ödeme Ve Borç Sorgulama Hizmetlerine İlişkin Karar	292
2021/1304 sayılı KVKK Kararı - Araç Kiralama Sektöründe Kara Liste Uygulamalarına İlişkin Karar	295
2020/966 sayılı KVKK Kararı - İletişim Bilgilerinin Doğrulanmasına İlişkin Karar	300
2020/481 sayılı KVKK Kararı - Unutulma Hakkı Kararı	302
2020/71 sayılı KVKK Kararı - Veri Sorumlusu ve Veri İşleyen Tespitinde Göz Önünde Bulundurulması Gereken Hususlar	314
2019/308 sayılı KVKK Kararı - Hukuka Aykırı Verilere Dayalı Sorgulamalara İlişkin Karar	319
2019/271 sayılı KVKK Kararı - Veri İhlal Bildirimi Asgari Unsurlarına İlişkin Karar.....	321
2019/125 sayılı KVKK Kararı - Yeterli Korumaya Sahip Ülkelerin Belirlenmesinde Esas Alınacak Kriterler	323
2019/10 sayılı KVKK Kararı - Kişisel Veri İhlal Bildirimine İlişkin Karar.....	326
2018/119 sayılı KVKK Kararı - Ticari İletilere İlişkin Karar	328
2018/63 sayılı KVKK Kararı - Personelin Yetki Aşımına İlişkin Karar	330
2018/10 sayılı KVKK Kararı - Özel Nitelikli Kişisel Verilere İlişkin Yeterli Önlemlere İlişkin Karar	331
2017/62 sayılı KVKK Kararı - Banko, Gişe, Masa gibi Hizmet Alanlarına İlişkin Karar	334
2017/61 sayılı KVKK Kararı - Rehberlik Hizmetleri Veren İnternet Sitelerine İlişkin Karar.....	335

KİŞİSEL VERİLERİ KORUMA KURULU KARARLARI	337
2023/426 sayılı KVKK Kararı.....	384
2023/437 sayılı KVKK Kararı.....	390
2023/224 sayılı KVKK Kararı.....	396
2023/134 sayılı KVKK Kararı.....	401
2023/86 sayılı KVKK Kararı.....	404
2023/78 sayılı KVKK Kararı.....	415
2023/67 sayılı KVKK Kararı.....	421
2023/4 sayılı KVKK Kararı.....	427
2022/1358 sayılı KVKK Kararı.....	433
2022/1357 sayılı KVKK Kararı.....	437
2022/1281 sayılı KVKK Kararı.....	442
2022/1249 sayılı KVKK Kararı.....	447
2022/1201 sayılı KVKK Kararı.....	457
2022/1147 sayılı KVKK Kararı.....	464
2022/1072 sayılı KVKK Kararı.....	469
2022/925 sayılı KVKK Kararı.....	473
2022/923 sayılı KVKK Kararı.....	476
2022/902 sayılı KVKK Kararı.....	482
2022/896 sayılı KVKK Kararı.....	485
2022/863 sayılı KVKK Kararı.....	492
2022/861 sayılı KVKK Kararı.....	500
2022/853 sayılı KVKK Kararı.....	505
2022/798 sayılı KVKK Kararı.....	520
2022/790 sayılı KVKK Kararı.....	526
2022/787 sayılı KVKK Kararı.....	532
2022/776 sayılı KVKK Kararı.....	538
2022/774 sayılı KVKK Kararı.....	544
2022/768 sayılı KVKK Kararı.....	551
2022/655 sayılı KVKK Kararı.....	557
2022/653 sayılı KVKK Kararı.....	564
2022/630 sayılı KVKK Kararı.....	572
2022/594 sayılı KVKK Kararı.....	577
2022/545 sayılı KVKK Kararı.....	583
2022/491 sayılı KVKK Kararı.....	590
2022/489 sayılı KVKK Kararı.....	594

2022/386 sayılı KVKK Kararı.....	600
2022/328 sayılı KVKK Kararı.....	604
2022/325 sayılı KVKK Kararı.....	608
2022/277 sayılı KVKK Kararı.....	614
2022/249 sayılı KVKK Kararı.....	624
2022/662 sayılı KVKK Kararı.....	629
2022/243 sayılı KVKK Kararı.....	638
2022/229 sayılı KVKK Kararı.....	644
2022/224 sayılı KVKK Kararı.....	655
2022/184 sayılı KVKK Kararı.....	660
2022/172 sayılı KVKK Kararı.....	666
2022/137 sayılı KVKK Kararı.....	672
2022/107 sayılı KVKK Kararı.....	680
2022/103 sayılı KVKK Kararı.....	685
2022/31 sayılı KVKK Kararı.....	689
2022/13 sayılı KVKK Kararı.....	694
2022/6 sayılı KVKK Kararı.....	698
2021/1324 sayılı KVKK Kararı.....	705
2021/1303 sayılı KVKK Kararı.....	708
2021/1262 sayılı KVKK Kararı.....	723
2021/1258 sayılı KVKK Kararı.....	729
2021/1243 sayılı KVKK Kararı.....	736
2021/1239 sayılı KVKK Kararı.....	740
2021/1218 sayılı KVKK Kararı.....	746
2021/1217 sayılı KVKK Kararı.....	758
2021/1214 sayılı KVKK Kararı.....	772
2021/1210 sayılı KVKK Kararı.....	780
2021/1187 sayılı KVKK Kararı.....	787
2021/1153 sayılı KVKK Kararı.....	800
2021/1127 sayılı KVKK Kararı.....	805
2021/1111 sayılı KVKK Kararı.....	812
2021/1110 sayılı KVKK Kararı.....	820
2021/1107 sayılı KVKK Kararı.....	824
2021/1104 sayılı KVKK Kararı.....	832
2021/1069 sayılı KVKK Kararı.....	839
2021/1051 sayılı KVKK Kararı.....	844

2021/909 sayılı KVKK Kararı.....	851
2021/925 sayılı KVKK Kararı.....	855
2021/989 sayılı KVKK Kararı.....	860
2021/993 sayılı KVKK Kararı.....	866
2021/889 sayılı KVKK Kararı.....	871
2021/859 sayılı KVKK Kararı.....	875
2021/850 sayılı KVKK Kararı.....	881
2021/847 sayılı KVKK Kararı.....	888
2021/799 sayılı KVKK Kararı.....	892
2021/761 sayılı KVKK Kararı.....	902
2021/670 sayılı KVKK Kararı.....	911
2021/666 sayılı KVKK Kararı.....	918
2021/664 sayılı KVKK Kararı.....	923
2021/603 sayılı KVKK Kararı.....	927
2021/584 sayılı KVKK Kararı.....	932
2021/572 sayılı KVKK Kararı.....	941
2021/548 sayılı KVKK Kararı.....	945
2021/545 sayılı KVKK Kararı.....	949
2021/511-512-513 sayılı KVKK Kararı	952
2021/424 sayılı KVKK Kararı.....	957
2021/422 sayılı KVKK Kararı.....	965
2021/470 sayılı KVKK Kararı.....	969
2021/464 sayılı KVKK Kararı.....	973
2021/427 sayılı KVKK Kararı.....	976
2021/426 sayılı KVKK Kararı.....	980
2021/407 sayılı KVKK Kararı.....	984
2021/389 sayılı KVKK Kararı.....	988
2021/361 sayılı KVKK Kararı.....	995
2021/359 sayılı KVKK Kararı.....	999
2021/358 sayılı KVKK Kararı.....	1004
2021/333 sayılı KVKK Kararı.....	1010
2021/311 sayılı KVKK Kararı.....	1015
2021/242 sayılı KVKK Kararı.....	1018
2021/241 sayılı KVKK Kararı.....	1023
2021/238 sayılı KVKK Kararı.....	1028
2021/230 sayılı KVKK Kararı.....	1029

2021/228 sayılı KVKK Kararı.....	1033
2021/227 sayılı KVKK Kararı.....	1038
2020/216 sayılı KVKK Kararı.....	1042
2021/205 sayılı KVKK Kararı.....	1046
2021/190 sayılı KVKK Kararı.....	1051
2021/187 sayılı KVKK Kararı.....	1054
2021/154 sayılı KVKK Kararı.....	1057
2021/140 sayılı KVKK Kararı.....	1060
2021/115 sayılı KVKK Kararı.....	1062
2021/111 sayılı KVKK Kararı.....	1068
2021/85 sayılı KVKK Kararı.....	1076
2021/84 sayılı KVKK Kararı.....	1081
2021/79 sayılı KVKK Kararı.....	1084
2021/78 sayılı KVKK Kararı.....	1089
2021/32 sayılı KVKK Kararı.....	1094
2020/957 sayılı KVKK Kararı.....	1099
2020/935 sayılı KVKK Kararı.....	1101
2020/934 sayılı KVKK Kararı.....	1103
2020/927 sayılı KVKK Kararı.....	1106
2020/915 sayılı KVKK Kararı.....	1110
2020/905 sayılı KVKK Kararı.....	1116
2020/816 sayılı KVKK Kararı.....	1119
2020/787 sayılı KVKK Kararı.....	1121
2020/769 sayılı KVKK Kararı.....	1126
2020/766 sayılı KVKK Kararı.....	1131
2020/765 sayılı KVKK Kararı.....	1135
2020/763 sayılı KVKK Kararı.....	1139
2020/755 sayılı KVKK Kararı.....	1141
2020/746 sayılı KVKK Kararı.....	1144
2020/744 sayılı KVKK Kararı.....	1149
2020/715 sayılı KVKK Kararı.....	1152
2020/710 sayılı KVKK Kararı.....	1155
2020/691 sayılı KVKK Kararı.....	1159
2020/667 sayılı KVKK Kararı.....	1163
2020/649 sayılı KVKK Kararı.....	1165
2020/622 sayılı KVKK Kararı.....	1168

2020/608 sayılı KVKK Kararı.....	1172
2020/567 sayılı KVKK Kararı.....	1175
2020/560 sayılı KVKK Kararı.....	1177
2020/559 sayılı KVKK Kararı.....	1181
2020/542 sayılı KVKK Kararı.....	1195
2020/532 sayılı KVKK Kararı.....	1198
2020/530 sayılı KVKK Kararı.....	1201
2020/511 sayılı KVKK Kararı.....	1203
2020/508 sayılı KVKK Kararı.....	1206
2020/507 sayılı KVKK Kararı.....	1210
2020/504 sayılı KVKK Kararı.....	1214
2020/494 sayılı KVKK Kararı.....	1218
2020/482 sayılı KVKK Kararı.....	1223
2020/471 sayılı KVKK Kararı.....	1225
2020/466 sayılı KVKK Kararı.....	1228
2020/465 sayılı KVKK Kararı.....	1232
2020/463 sayılı KVKK Kararı.....	1235
2020/435 sayılı KVKK Kararı.....	1238
2020/429 sayılı KVKK Kararı.....	1245
2020/421 sayılı KVKK Kararı.....	1260
2020/414 sayılı KVKK Kararı.....	1262
2020/407 sayılı KVKK Kararı.....	1268
2020/404 sayılı KVKK Kararı.....	1272
2020/396 sayılı KVKK Kararı.....	1279
2020/379 sayılı KVKK Kararı.....	1286
2020/359 sayılı KVKK Kararı.....	1290
2020/357 sayılı KVKK Kararı.....	1294
2020/355 sayılı KVKK Kararı.....	1297
2020/345 sayılı KVKK Kararı.....	1300
2020/344 sayılı KVKK Kararı.....	1303
2020/335 sayılı KVKK Kararı.....	1305
2020/336 sayılı KVKK Kararı.....	1311
2020/325 sayılı KVKK Kararı.....	1315
2020/315 sayılı KVKK Kararı.....	1318
2020/307 sayılı KVKK Kararı.....	1321
2020/286 sayılı KVKK Kararı.....	1326

2020/255 sayılı KVKK Kararı.....	1328
2020/226 sayılı KVKK Kararı.....	1337
2020/213 sayılı KVKK Kararı.....	1340
2020/212 sayılı KVKK Kararı.....	1342
2020/201 sayılı KVKK Kararı.....	1347
2020/196 sayılı KVKK Kararı.....	1350
2020/191, 2020/192, 2020/193, 2020/194 sayılı KVKK Kararları.....	1354
2020/187 sayılı KVKK Kararı.....	1361
2020/173 sayılı KVKK Kararı.....	1363
2020/172 sayılı KVKK Kararı.....	1375
2020/167 sayılı KVKK Kararı.....	1382
2020/166 sayılı KVKK Kararı.....	1385
2020/145 sayılı KVKK Kararı.....	1391
2020/138 sayılı KVKK Kararı.....	1396
2020/124 sayılı KVKK Kararı.....	1400
2020/120 sayılı KVKK Kararı.....	1406
2020/118 sayılı KVKK Kararı.....	1413
2020/113 sayılı KVKK Kararı.....	1417
2020/108 sayılı KVKK Kararı.....	1419
2020/103 sayılı KVKK Kararı.....	1426
2020/93 sayılı KVKK Kararı.....	1428
2020/86 sayılı KVKK Kararı.....	1434
2020/78 sayılı KVKK Kararı.....	1437
2020/67 sayılı KVKK Kararı.....	1442
2020/66 sayılı KVKK Kararı.....	1445
2020/65 sayılı KVKK Kararı.....	1450
2020/63 sayılı KVKK Kararı.....	1454
2020/59 sayılı KVKK Kararı.....	1457
2020/58 sayılı KVKK Kararı.....	1461
2020/50 sayılı KVKK Kararı.....	1464
2020/43 sayılı KVKK Kararı.....	1466
2020/41 sayılı KVKK Kararı.....	1471
2020/34 sayılı KVKK Kararı.....	1473
2020/32 sayılı KVKK Kararı.....	1477
2020/26 sayılı KVKK Kararı.....	1479
2020/20 sayılı KVKK Kararı.....	1483

2020/13 sayılı KVKK Kararı.....	1484
2019/393 sayılı KVKK Kararı.....	1486
2019/389 sayılı KVKK Kararı.....	1491
2019/387 sayılı KVKK Kararı.....	1493
2019/276 sayılı KVKK Kararı.....	1500
2019/372 sayılı KVKK Kararı.....	1502
2019/269 sayılı KVKK Kararı.....	1504
2019/353 sayılı KVKK Kararı.....	1509
2019/352 sayılı KVKK Kararı.....	1511
2019/333 sayılı KVKK Kararı.....	1513
2019/332 sayılı KVKK Kararı.....	1518
2019/331 sayılı KVKK Kararı.....	1520
2019/316 sayılı KVKK Kararı.....	1521
2019/297 sayılı KVKK Kararı.....	1524
2019/296 sayılı KVKK Kararı.....	1526
2019/294 sayılı KVKK Kararı.....	1528
2019/273 sayılı KVKK Kararı.....	1532
2019/265 sayılı KVKK Kararı.....	1534
2019/255 sayılı KVKK Kararı.....	1535
2019/254 sayılı KVKK Kararı.....	1538
2019/227 sayılı KVKK Kararı.....	1540
2019/225 sayılı KVKK Kararı.....	1542
2019/222 sayılı KVKK Kararı.....	1547
2019/206 sayılı KVKK Kararı.....	1550
2019/204 sayılı KVKK Kararı.....	1554
2019/198 sayılı KVKK Kararı.....	1556
2019/188 sayılı KVKK Kararı.....	1559
2019/170 sayılı KVKK Kararı.....	1561
2019/166 sayılı KVKK Kararı.....	1563
2019/162 sayılı KVKK Kararı.....	1564
2019/159 sayılı KVKK Kararı.....	1566
2019/157 sayılı KVKK Kararı.....	1568
2019/144 sayılı KVKK Kararı.....	1569
2019/143 sayılı KVKK Kararı.....	1572
2019/141 sayılı KVKK Kararı.....	1575
2019/138 sayılı KVKK Kararı.....	1578

2019/122 sayılı KVKK Kararı.....	1580
2019/104 sayılı KVKK Kararı.....	1582
2019/82 sayılı KVKK Kararı.....	1586
2019/81, 2019/165 sayılı KVKK Kararı.....	1590
2019/78 sayılı KVKK Kararı.....	1596
2019/52 sayılı KVKK Kararı.....	1599
2019/47 sayılı KVKK Kararı.....	1601
2019/23 sayılı KVKK Kararı.....	1603
2019/9 sayılı KVKK Kararı.....	1605
2018/156 sayılı KVKK Kararı.....	1607
2018/143 sayılı KVKK Kararı.....	1609
2018/142 sayılı KVKK Kararı.....	1611
2018/131 sayılı KVKK Kararı.....	1613
2018/118 sayılı KVKK Kararı.....	1615
2018/106 sayılı KVKK Kararı.....	1617
2018/91 sayılı KVKK Kararı.....	1619
2018/90 sayılı KVKK Kararı.....	1621
2018/88 sayılı KVKK Kararı.....	1623
2018/87 sayılı KVKK Kararı.....	1625
2018/75 sayılı KVKK Kararı.....	1626
2018/69 sayılı KVKK Kararı.....	1627
2018/68 sayılı KVKK Kararı.....	1630
2018/32 sayılı KVKK Kararı.....	1631

YURTDIŐINA KİŐİSEL VERİ AKTARMA TAAHHÜTNAMELERİ.....1633

Veri Sorumlusundan Veri Sorumlusuna Aktarım	1634
Veri Sorumlusundan Veri İŐleyene Aktarım.....	1640
Otokoç Otomotiv Ticaret ve Sanayi A.Ő. Taahhütname Başvurusu	1646
Türkiye Futbol Federasyonu Taahhütname Başvurusu.....	1647
Decathlon Türkiye Taahhütname Başvurusu	1648
TEB Arval Taahhütname Başvurusu.....	1649
Amazon Taahhütname Başvurusu.....	1650

KİŐİSEL VERİ İHLAL BİLDİRİMİ FORMU.....1651

VERİ İHLALİ BİLDİRİMLERİ.....	1660
2023/638 - Beytıp Sağlık Hizmetleri Ltd. Şti.....	1666
2023/504 - Sahibinden Bilgi Teknolojileri Paz. ve Tic. A.Ş.....	1667
2023/503 - Destek Bilgisayar ve İletişim Hizmetleri Tic. A.Ş.	1669
2023/496 - Getir Perakende Lojistik Anonim Şirketi – Bitaksi Mobil Teknoloji Anonim Şirketi.....	1670
2023/463 - Akbank T.A.Ş.	1672
2023/375 - Marifet Saatçilik Kuym. Teks. Tur. Gıda İnş. Taah. San. ve Tic. Ltd. Şti.	1673
2023/56 - Yalova Uzmanlar Sağlık Hizmetleri San.Paz.Tic.A.Ş.....	1674
2023/55 - Reon Sağlık Hizmetleri İnş. Tur. San ve Tic. A.Ş.(Özel Aktif Hastanesi)	1675
2023/54 - Okko Sağlık Turizm İnşaat San. ve Tic. A.Ş.	1676
2022/1332 - Sital Çizgi İnşaat Turizm ve Tekstil Anonim Şirketi.....	1677
2022/1271 - Pamukkale Belediyesi.....	1678
2022/1264 - Shangai Moonton Technology Co Ltd.....	1679
2022/1197 - Aktif İnş. Taşımacılık Paz. San. ve Tic. AŞ.....	1680
2022/1196 - Aliza Otelcilik Turizm ve Tic. AŞ.....	1681
2022/1195 - AES Otelcilik Turizm ve Tic. AŞ	1682
2022/1194 - Baykar Motorlu Araçlar A.Ş.	1683
2022/1138 - Denizli Özel Egekent Hastanesi	1684
2022/1096 - Quick Sigorta Anonim Şirketi.....	1685
2022/1032 - Flo Mağazacılık ve Pazarlama A.Ş.....	1687
2022/1018 - Özel Keystone Eğitim ve Eğitim Dan. A.Ş.....	1688
2022/990 - Marmara Üniversitesi.....	1689
2022/987 - Fuudy Elektronik İletişim Perakende Gıda Lojistik Anonim Şirketi	1690
2022/882 - Biblos Alaçatı Turizm Yatırımları A.Ş.....	1691
2022/891 - Posta ve Telgraf Teşkilatı Biriktirme ve Yardım Sandığı.....	1692
2022/850 - Güreli Yeminli Mali Müşavirlik ve Bağımsız Denetim Hizmetleri Anonim Şirketi	1693
2022/831 - AstraZeneca İlaç San. ve Tic. Ltd. Şti.....	1694
2022/757 - NeoPets Inc.....	1696
2022/722 - Surtaş Otomotiv ve Servis Hizmetleri Sanayi Ticaret Limited Şirketi	1697
2022/687 - Knauf İnşaat ve Yapı Elemanları San. ve Tic. A.Ş ile Knauf Insulation Izolation San. ve Tic. A.Ş	1698
2022/686 - Türkiye Elektrik Dağıtım A.Ş.	1700
2022/685 - Meklas Otomotiv San. ve Tic. A.Ş.....	1701
2022/649 - Tofisa Tekstil Sanayi ve Ticaret Limited Şirketi.....	1702
2022/646-647-648 - ARG Denizcilik İnşaat Otomotiv Sanayi ve Ticaret Ltd. Şti, İstek Gemi İnşaa Bakım İnşaat Hırdavat Sanayi ve Ticaret Ltd. Şti, Safter Ulubay	1703

2022/? - Barçın Spor Malzemeleri Ticaret ve Sanayi Anonim Şirketi.....	1704
2022/569 - Pegasus Hava Taşımacılığı Anonim Şirketi.....	1705
2022/554 - MBtech Mühendislik ve Danışmanlık Ltd. Şti.	1706
2022/536 - Baydöner Restoranları A.Ş.	1707
2022/535 - ZkSoftware The Advanced Biometric Solution Elektronik San. ve Tic. Ltd. Şti.	1708
2022/478 - Yıldız Teknoloji Geliştirme Bölgesi Teknopark AŞ	1709
2022/446 - Keyubu İnternet ve Bilişim Hizmetleri	1710
2022/441 - Paketman E-Ticaret Sanayi Ticaret AŞ	1711
2022/440 - Magna Ventures Yazılım ve Teknoloji Girişimleri Ticaret Anonim Şirketi	1712
2022/404 - Villacım Emlak Turizm İnşaat Sanayi ve Ticaret Limited Şirketi.....	1713
2022/334, 335,336 ve 337 - Yıldızlar Yatırım Holding AŞ, Yıldız Demir Çelik Sanayi AŞ, Yıldız Entegre Ağaç Sanayi AŞ, İstanbul Gübre Sanayi AŞ (İGSAŞ).....	1714
2022/304 - Yonca Sağlık Hizmetleri Ltd. Şti.	1715
2022/209 - Martı İleri Teknoloji A.Ş.	1717
2022/157 - Arı İnovasyon ve Bilim Eğitim Hizmetleri Anonim Şirketi (İTÜ ETA Vakfı Doğa Koleji).....	1718
2022/156 - Kentyol Kent Hizmetleri AŞ	1719
2022/155 - Şişli Belediye Başkanlığı.....	1720
2022/154 - T.C. Acıbadem Mehmet Ali Aydınlar Üniversitesi	1721
2022/124 - Kent Konut İnşaat Sanayi ve Ticaret Anonim Şirketi.....	1722
2022/94 - Pizza Restaurantları AŞ (Dominos Pizza).....	1723
2022/93 - Moncler İstanbul Giyim ve Tekstil Ticaret Ltd. Şti.....	1724
2022/92 - Industries S.p.A.	1725
2022/16 - Logo Yazılım Sanayi ve Ticaret AŞ.....	1726
2021/1327 - Eureko Sigorta AŞ	1727
2021/1326 - GoDaddy.com, LLC (“GoDaddy”)	1728
2021/1231 - T.C. İstanbul Kültür Üniversitesi	1729
2021/1175 - Media Markt Turkey Ticaret Limited Şirketi.....	1730
2021/1168-1174 - May Şirketler Grubu	1731
2021/1146 - Tasfiye Halinde Hedefevim Gayrimenkul ve Otomotiv Tic. AŞ.....	1732
2021/1099 - İzmir Bakırçay Üniversitesi.....	1733
2021/1027 - Panasonic Business Support Europe GmbH	1735
2021/983 - Elginkan Topluluğu Şirketleri	1736
2021/977 - Art Sistem Bilgisayar ve Güvenlik Teknolojileri Ltd. Şti	1738
2021/951 - Arvato Lojistik Dış Ticaret ve E-Ticaret Hizmetleri AŞ	1739
2021/895 - AK Gıda Sanayi ve Ticaret AŞ.....	1740
2021/875 - MNG Kargo Yurtiçi ve Yurtdışı Taşımacılık AŞ.....	1741

2021/874 - Sinoz Kozmetik Sanayi Ticaret AŞ.....	1742
2021/844 - Subway International B.V.	1743
2021/843 - Pied Piper Fansub (piedpiperfb.com).....	1744
2021/787 - Oriflame Kozmetik Ürünleri Ticaret Limited Şirketi	1745
2021/758 - Motor Trend Group LLC.....	1746
2021/752 - Timurlar Sigorta Aracılık Hizmetleri Ltd. Şti.....	1747
2021/729 - Özel Dentapoint Diş Sağlığı Polikliniği	1749
2021/725 - Webhosting Bilişim Teknolojileri AŞ.....	1750
2021/677 - T. Garanti Bankası AŞ.....	1752
2021/675 - Cosmolog Kozmetik Sanayi ve Ticaret AŞ.....	1753
2021/633 - INTERGEN Genetik ve Nadir Hastalıklar Tanı Araştırma & Uygulama Merkezi	1754
2021/593 - Prof. Dr. Birol CİVELEK.....	1755
2021/728 - Düzen Biyolojik Bilimler Araştırma Geliştirme ve Üretim A.Ş.	1756
2021/517 - Pakten Sağlık Ürünleri Sanayi ve Ticaret AŞ (onlemmarket.com)	1757
2021/537 - Rahmet Ragıp Kuğu (Serbest Muhasebeci Mali Müşavir).....	1758
2021/502 - Eliptik Yazılım ve Ticaret AŞ (BtcTurk)	1759
2021/498 - E-Data Teknoloji Pazarlama Anonim Şirketi.....	1761
2021/517 - Pakten Sağlık Ürünleri Sanayi ve Ticaret AŞ (onlemmarket.com)	1762
2021/272 - Acer Bilişim Teknolojileri Limited Şirketi.....	1763
2021/271 - Acer Sales International SA.....	1764
2021/222 - Adım Adım Oluşumu.....	1765
2021/329 - Air India Limited.....	1767
2021/414 - Akademisyen Yayınevi Kitabevi Dağıtım Bilgisayar Tercümanlık İth. İhr. Tic. AŞ (www.nobelkitabevi.com.tr)	1769
2020/486 - Avivasa Emeklilik ve Hayat A.Ş.	1770
2020/487 - Avon Kozmetik Ürünleri Sanayi ve Ticaret A.Ş.	1771
2020/631 - Barilla Gıda A.Ş.	1772
2021/463 - Bulut Elektromarket Bilgi Teknolojileri ve Dış Tic. AŞ.....	1773
2020/863 - Çizgi Telekomünikasyon A.Ş.	1774
2021/462 - ClearVoiceResearch.com, LLC	1775
2020/635 - Dap Rotana Dalga ve Vazo Rezidans Toplu Yapı Yöneticiliği	1776
2020/737 - PSL Elektronik San. ve Tic. A.Ş.	1777
2020/636 - Rezzan Günday (Şimşek Eczanesi)	1778
2020/485 - Sezgi Dental Ağız ve Diş Sağlığı Polikliniği.....	1780
2021/382 - Sine İriyat Par. Tem. Ür. Gıd. İnş. Mim. Müh. İth. İhr. ve Tic. AŞ	1782
2021/132 - So CHIC Mağazacılık San. ve Tic. AŞ.....	1783

2021/18 - T.C. Özyeğin Üniversitesi	1784
2020/207 - Türk Ekonomi Bankası A.Ş.	1785
2020/290 - Turkon Holding A.Ş. ve Grup Şirketleri	1786
2020/984 - UiPath SRL	1787
2020/848 - UPI Trans Dış Ticaret AŞ.....	1789
2020/789 - Vatan Bilgisayar Sanayi ve Ticaret AŞ.....	1790
2021/326 - West Gate Toplu Yapı Sitesi Yöneticiliği.....	1791
2020/675 - Yalova Belediyesi	1792
2021/376 - Yapı ve Kredi Bankası AŞ	1793
2021/321 - Yemek Sepeti Elektronik İletişim Perakende Gıda Lojistik AŞ.....	1794
2020/830 - Hanon Automotive Climate Sys. Manufacturing Industrial and Commercial Co.....	1796
2021/351 - Pierre Fabre Dermokozmetik Ltd. Şti.....	1797
2021/350 - Pierre Fabre İlaç AŞ.....	1798
2019/286 - Gardrops Elektronik Hizmetler ve Ticaret Anonim Şirketi.....	1799
2021/444 - DLSY Adi Ortaklığı.....	1800
2020/206 - Doğa Sigorta A.Ş.....	1802
2020/540 - Doktor Atadan Egemen KOYUNCU.....	1803
2020/443 - EasyJet Plc	1804
2020/46 - Exeltis İlaç Sanayi ve Ticaret A.Ş.....	1806
2021/194 - Fibabanka AŞ	1807
2020/1011 - Ficosa International Otomotiv San. ve Tic. AŞ.....	1808
2020/987 - Ficosa Otomotiv San. ve Tic. AŞ.....	1809
2020/555 - Fluke Corporation ve Fluke Electronics Corporation	1810
2021/323 - Generali Sigorta AŞ.....	1811
2020/211 - Gratis İç ve Dış Tic. A.Ş.	1812
2020/600-601-602-603-604 - Penti Giyim Sanayi ve Ticaret Anonim Şirketi ve İştirakleri	1813
2020/554 - Mert Grup Sigorta Aracılık Hizmetleri Ltd. Şti.....	1814
2021/192 - Oto Rapor Araç Muayene ve Ekspertiz Hizmetleri San. ve Tic. AŞ.....	1815
2020/82 - Microsoft Corporation	1816
2020/468 - Halk Sigorta A.Ş.	1817
2020/986 - Otokur Otomotiv İnşaat Turizm Sanayi ve Ticaret A.Ş.	1819
2020/857-858-859-860-861-862 - Kale Holding A.Ş. ve Grup Şirketleri	1820
2019/406-407-408-409-410 - CM Holding A.Ş. ve Grup Şirketleri.....	1821
2021/386 - Karacabay Turizm San. ve Dış Tic. Ltd. Şti.....	1822
2020/634 - Kariyer.net Elektronik Yayıncılık ve İletişim Hiz. A.Ş.....	1823
2019/384 - Küçükçekmece Belediyesi	1824

2019/381 - T. Garanti Bankası A.Ş.....	1825
2019/401 - Dođuş Planet Elektronik Ticaret ve Biliřim Hizmetleri A.Ş. (n11.com).....	1826
2019/360 - Edenred Kurumsal Çözümler A.Ş.	1827
2019/313 - EDS Enjeksiyon Dök. San. Tic. A.Ş.	1828
2019/311 - Premierdc Veri Merkezi A.Ş.	1829
2019/286 - Gardrops Elektronik Hizmetler ve Ticaret Anonim Őirketi.....	1830
2019/285 - Zynga Game Ireland Limited	1831
2019/281 - Furtrans Denizcilik Ticaret ve San. A.Ş.	1832
2019/268 - Türkiye İř Bankası A.Ş.....	1833
2019/267 - FER Gayrimenkul Geliřtirme ve İnř. A.Ş.....	1834
2019/230 - DenizBank A.Ş.	1835
2019/219 - Türk Ekonomi Bankası A.Ş.	1836
2019/190 - Pizza Restaurantları A.Ş. (Domino’s Pizza).....	1838
2019/181 - Metro Grosmarket Bakırköy Alıřveriř Hiz.Tic.Ltd.Őti.	1839
2019/178 - Vodafone Telekomünikasyon A.Ş.....	1840
2019/169 - Bartu Turizm Yatırımları A.Ş.....	1841
2019/130 - Microsoft Corporation	1842
2019/74 - Hunko Motorlu Araçlar San. Ve Tic. Ltd. Őti.	1844
2019/73 - ASF Otomotiv A.Ş.	1845
2019/72 - Kaya Seyehat Turizm San. Ve Dıř. Tic. Ltd. Őti.....	1846
2019/67 - Turmobil Turizm Rent a Car Tařımacılık ve Nakliyat San. Tic. Ltd. Őti.....	1847
2019/56 - Adnan Özen İnřaat Taah. En. Turz. Tiç. ve San. A.Ş.....	1848
2019/43 - ING Bank A.Ş.....	1849
2019/35 - Borlease Otomotiv A.Ş.....	1852
2019/32 - Garanti Filo Yönetim Hizmetleri A.Ş.....	1853
2019/30 - Derindere Turizm Otomotiv San. ve Tic. A.Ş.....	1855
2019/29 - Clickbus Seyahat Hizmetleri A.Ş. (Nereden Nereye).....	1856
2019/28 - Enterprise (“Yes Oto”).....	1858
2019/27 - Arkas Otomotiv Servis ve Ticaret A.Ş. (“Arkas Otomotiv”)	1859
2019/20 - Holiday Inn İstanbul - Őiřli	1860
2019/17 - Hedef Araç Kiralama ve Servis A.Ş. (HedefFilo)	1861
2019/16 - Optimum Otomotiv Satıř Sonrası Çözümleri Tic. A.Ş. (OPTİMUM).....	1862
2019/15 - TEB Arval Araç Filo Kiralama A.Ş.(TEB ARVAL).....	1863
2019/14 - ALD Automotive Turizm Ticaret A.Ş. (ALD AUTOMOTIVE).....	1865
2019/13 - ANIMOTO Inc. (Animoto).....	1867
2018/147 - Marriott International Inc.....	1868

2018/124 - Cathay Pacific Airways Limited.....	1870
2018/72 - Ticketmaster UK (Ticketmaster İngiltere) adına Biletix Bilet Dağıtım Basım ve Tic. A.Ş.	1872
2018/45 - Careem Networks Teknoloji A.Ş.....	1874

DİĞER KURUL KARARLARI VE DUYURULARI.....1876

27.03.2023 - Vekaleten Yapılacak Şikayetlerin Elektronik Ortamda Kurula İletilmesine İlişkin Kamuoyu Duyurusu.....	1878
23.03.2023 - Seçim Faaliyetleri Kapsamında Siyasi Partiler ve Bağımsız Adaylar Tarafından İşlenen Kişisel Veriler Hakkında Kamuoyu Duyurusu.....	1879
09.02.2023 - Depremden Etkilenen İlgili Kişilere Ve Veri Sorumlularına Yönelik Kamuoyu Duyurusu	1889
17.12.2021 - Mağazalarda SMS Doğrulama Duyurusu.....	1890
21.04.2022 - VERBİS Ceza Duyurusu	1893
04.01.2022 - Verbis Duyurusu	1895
17.12.2021 - Mağazalarda SMS Doğrulaması Duyurusu	1897
10.12.2021 - Veri Koruma Görevlisi Hakkında Kamuoyu Duyurusu.....	1900
07.12.2021 - Sertifikasyon Duyurusu.....	1901
05.11.2021 - Belediyeler Duyurusu	1912
28.09.2021 - Covid-19 PCR Test Sonucu ve Aşı Bilgisi Uygulamaları	1915
03.09.2021 - WhatsApp (3)	1918
09.08.2021 - Yurt Dışında Yaşayan Türkiye Cumhuriyeti Vatandaşlarının Kişisel Verilerinin Yurt Dışına Aktarılmamasına İlişkin Talepleri.....	1921
25.06.2021 - Ortaklıkların VERBİS'e Kayıt Yükümlülüğü.....	1924
25.06.2021 - Dernek, Vakıf ve Sendikalara Ait İktisadi İşletmelerin VERBİS'e Kayıt Yükümlülüğü.....	1925
30.03.2021 - Kurumumuza Yapılan Şikayetlerin Usul Şartları	1927
11.03.2021 - VERBİS'e Kayıt Sürelerinin Uzatılması	1931
12.01.2021 - WhatsApp (2)	1932
12.01.2021 - WhatsApp (1)	1936
26.10.2020 - Yurtdışına Veri Aktarımı.....	1937
01.10.2020 - Sicile Kayıt Yükümlülüğü	1948
17.07.2020 - Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına Yönelik Talepler	1949
23.06.2020 - VERBİS'e Kayıt Sürelerinin Uzatılması	1951
07.05.2020 - Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhünamelelerde Dikkat Edilmesi Gereken Hususlar	1952
18.03.2020 - COVID-19 Tedbirleri.....	1961
06.01.2020 - Kişisel Veri İhlali Bildirimlerinin Elektronik Ortamda Kurula İletilmesi.....	1962

08.11.2019 - Veri Sorumlularının GDPR Atıfları.....	1963
06.11.2019 - Kişisel Verilerin Korunması Kanunu Uyum Süreci.....	1965
05.09.2019 - VERBİS'e Kayıt Süresinin Uzatılması.....	1967
12.10.2018 - VERBİS'e Yapılan Kayıt Başvuruları.....	1968
16.05.2018 - Yurtdışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurlar.....	1969
06.04.2018 - Kanuna Uyum Süreci (Geçici 1. madde)	1971
28.03.2018 - Rehberlik Hizmeti Veren İnternet Siteleri ve Uygulamalar.....	1973

İNGİLİZCE DUYURULAR.....1974

Board Resolution on Protecting Personal Data at Service Areas such as the Counters, Box Offices and Desks	1976
Binding Corporate Rules Application Form	1977
The Transfer of Personal Data Abroad on the Basis of Convention No. 108.....	1990
Search Engine Delist Criteria	2004
Board Decision about Cathay Pasific Airway.....	2011
Board Decision about Clickbus Travel Services	2012
Board Decision on Minimum Elements that Should be Included in the Communication of the breach by the Data Controller to the Data Subject.....	2017
Board Decisions on Providing Derogations from The Obligation of Registration with the Data Controllers' Registry	2019
Board Resolution on Preventing Data Controllers and Data Processors From Forwarding Advertising Messages/Calls to Email Addresses of Data Subjects or to Their Phones By Sms or Phone Calls	2020
Protection of Personal Data During the Fight Against COVID-19.....	2022
Public Announcement - Microsoft Corporation.....	2029
Public Announcement on Application for Commitment.....	2030
Public Announcement on Covid-19	2031
Public Announcement on Distance Learning Platforms	2032
Public Announcement on the Commitment Application	2033
Public Announcement on the Extension of the Registration Periods to Verbis (Data Controllers Registry)	2034
Public Announcement on Whatsapp Application	2035
Regarding Processing of Location Data and Tracking Mobility of Individuals to Combat Covid-19	2039
The Board Decision No. 2019/10 of 24.01.2019 about Procedures and Principles of Personal Data Breach Notification.....	2041

The Board Decision No. 2019/125 of 02/05/2019 about the form prepared to be used in the determination of the countries having adequate level of protection	2043
The Decision of Personal Data Protection Board No. 2018/88 of 19/07/2018 on “The Starting Dates of Obligation to Register with the Data Controller’s Registry”	2047
Fulfilment of Obligation to Inform.....	2050

TÜRK HUKUKUNDAKİ DİĞER DÜZENLEMELER2053

KANUNLAR.....2054

7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu	2056
7252 sayılı Dijital Mecralar Komisyonu Kurulması ile Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun	2062
7223 sayılı Ürün Güvenliği ve Teknik Düzenlemeler Kanunu.....	2065
7091 sayılı Olağanüstü Hal Kapsamında Alınması Gereken Tedbirler Hakkında Kanun Hükmünde Kararnamenin Kabul Edilmesine Dair Kanun.....	2067
7075 sayılı Olağanüstü Hal İşlemleri İnceleme Komisyonu Kurulması Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun.....	2069
7068 sayılı Genel Kolluk Disiplin Hükümleri Hakkında Kanun Hükmünde Kararnamenin Kabul Edilmesine Dair Kanun.....	2072
6713 sayılı Kolluk Gözetim Komisyonu Kurulması Hakkında Kanun	2083
6706 sayılı Cezai Konularda Uluslararası Adli İşbirliği Kanunu	2092
6701 sayılı Türkiye İnsan Hakları ve Eşitlik Kurumu Kanunu	2112
6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunu.....	2135
6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun	2141
6475 sayılı Posta Hizmetleri Kanunu	2143
6458 sayılı Yabancılar ve Uluslararası Koruma Kanunu.....	2146
6362 sayılı Sermaye Piyasası Kanunu	2150
6328 sayılı Kamu Denetçiliği Kurumu Kanunu.....	2154
6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun	2156
6114 sayılı Ölçme, Seçme ve Yerleştirme Merkezi Başkanlığının Teşkilat ve Görevleri Hakkında Kanun	2160
6102 sayılı Türk Ticaret Kanunu.....	2168
6100 sayılı Hukuk Muhakemeleri Kanunu	2175
6098 sayılı Türk Borçlar Kanunu	2184
5809 sayılı Elektronik Haberleşme Kanunu	2185
5718 sayılı Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun.....	2199

5684 sayılı Sigortacılık Kanunu.....	2201
5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.....	2229
5624 sayılı Kan ve Kan Ürünleri Kanunu.....	2249
5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun.....	2255
5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu.....	2258
5502 sayılı Sosyal Güvenlik Kurumu Kanunu.....	2260
5490 sayılı Nüfus Hizmetleri Kanunu.....	2262
5464 sayılı Banka Kartları ve Kredi Kartları Kanunu	2296
5429 sayılı Türkiye İstatistik Kanunu.....	2299
5411 sayılı Bankacılık Kanunu	2303
5352 sayılı Adli Sicil Kanunu	2313
5271 sayılı Ceza Muhakemesi Kanunu	2321
5258 sayılı Aile Hekimliği Kanunu	2338
5237 sayılı Türk Ceza Kanunu	2340
5070 sayılı Elektronik İmza Kanunu	2346
4982 sayılı Bilgi Edinme Hakkı Kanunu.....	2348
4904 sayılı Türkiye İş Kurumu ile İlgili Bazı Düzenlemeler Hakkında Kanun.....	2357
4857 sayılı İş Kanunu	2359
4721 sayılı Türk Medeni Kanunu	2361
4632 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanunu.....	2366
3359 sayılı Sağlık Hizmetleri Temel Kanunu	2370
2937 sayılı Devlet İstihbarat Hizmetleri Ve Milli İstihbarat Teşkilatı Kanunu	2373
2920 sayılı Türk Sivil Havacılık Kanunu	2392
2559 sayılı Polis Vazife ve Selâhiyet Kanunu.....	2394
1774 sayılı Kimlik Bildirme Kanunu	2398
1512 sayılı Noterlik Kanunu.....	2404
1136 sayılı Avukatlık Kanunu.....	2406
1211 sayılı Türkiye Cumhuriyet Merkez Bankası Kanunu	2407
211 sayılı Türk Silahlı Kuvvetleri İç Hizmet Kanunu	2409

TÜZÜKLER.....2410

Tıbbi Deontoloji Nizamnamesi	2411
Özel Hastaneler Tüzüğü.....	2412

YÖNETMELİKLER.....	2414
Türkiye Cumhuriyeti Kimlik Kartı Yönetmeliği.....	2416
Türkiye Cumhuriyeti Kimlik Kartı Elektronik Kimlik Doğrulama Sistemi Yönetmeliği.....	2429
Kimlik Paylaşımı Sistemi Yönetmeliği.....	2445
Veri Paylaşımı Kurulu Yönetmeliği.....	2454
Kimlik Bildirme Kanununun Uygulanması ile İlgili Yönetmelik.....	2463
E-Devlet Hizmetlerinin Yürütülmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik.....	2475
Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik.....	2485
Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik.....	2492
Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında Yönetmelik.....	2544
Hasta Hakları Yönetmeliği.....	2552
Özel Hastaneler Yönetmeliği.....	2555
Kan ve Kan Ürünleri Yönetmeliği.....	2560
Bulaşıcı Hastalıklar Sürveyans ve Kontrol Esasları Yönetmeliği.....	2565
Uluslararası Sağlık Turizmi ve Turistin Sağlığı Hakkında Yönetmelik.....	2575
Tıbbi Cihaz Yönetmeliği.....	2584
Tıbbi Cihaz Klinik Araştırmaları Yönetmeliği.....	2614
Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmelik.....	2628
6713 Sayılı Kolluk Gözetim Komisyonu Kurulması Hakkında Kanunun Uygulanmasına Dair Yönetmelik.....	2637
Hukuk Muhakemelerinde Ses ve Görüntü Nakledilmesi Yoluyla Duruşma İcrası Hakkında Yönetmelik.....	2684
Yolcu Gemilerinin Emniyetine ve Gemilerdeki Yolcuların Kayıt Altına Alınmasına İlişkin Yönetmelik.....	2691
Eczacılar ve Eczaneler Hakkında Yönetmelik.....	2696
Genel Sağlık Sigortası Kapsamında Gelir Tespiti, Tescil ve İzleme Sürecine İlişkin Usul ve Esaslar Hakkında Yönetmelik.....	2698
Bireysel Emeklilik Sistemi Hakkında Yönetmelik.....	2701
112 Acil Çağrı Merkezleri Kuruluş, Görev ve Çalışma Yönetmeliği.....	2702
Afet ve Acil Durum Müdahale Hizmetleri Yönetmeliği.....	2705
Bilgi Teknolojileri ve İletişim Kurumu İdari Yaptırımlar Yönetmeliği.....	2707
Bilgi Teknolojileri ve İletişim Kurumu Posta Sektöründe İdari Yaptırımlar Yönetmeliği.....	2730
Bilgi Teknolojileri ve İletişim Kurumu Teşkilât Yönetmeliği.....	2734
Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik.....	2736
Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği.....	2744
İnternet Alan Adları Yönetmeliği.....	2750

Sosyal Yardım Verilerinin Kaydedilmesine ve Paylaşılmasına İlişkin Yönetmelik	2752
Mesafeli Sözleşmeler Yönetmeliği.....	2765
Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik	2767
Elektronik Ticarete Hizmet Sağlayıcı ve Aracı Hizmet Sağlayıcılar Hakkında Yönetmelik.....	2770
Özel İstihdam Büroları Yönetmeliği	2773
Ticaret Sicili Yönetmeliği	2776
Veri Depolama Kuruluşunun Faaliyet, Çalışma ve Denetim Esasları Hakkında Yönetmelik.....	2778
Yenilenmiş Ürünlerin Satışı Hakkında Yönetmelik.....	2788
Elektrikli Skuter Yönetmeliği.....	2798
Yabancı Plakalı Araçlara Verilen Trafik İdari Para Cezalarının Tahsiline İlişkin Yönetmelik	2814
Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanunun Uygulanmasına İlişkin Yönetmelik.....	2817
Nüfus Hizmetleri Uygulama Yönetmeliği	2821
Genel Ürün Güvenliği Yönetmeliği	2848
Tapu ve Kadastro Verilerinin İşlenmesi ve Elektronik Ortamda Yapılacak İşlemler Hakkında Yönetmelik	2850
Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik.....	2870
Vakıflar Yönetmeliği	2879
Türkiyede Oturan Yabancıların Nüfus Kayıtlarının Tutulması Hakkında Yönetmelik	2885
Güvenlik Soruşturması ve Arşiv Araştırması Yapılmasına Dair Yönetmelik.....	2893
Sigortacılık Verilerinin Toplanması, Saklanması ve Paylaşılmasına Dair Yönetmelik.....	2903
Sağlık Bilgi Sistemleri Hakkında Yönetmelik.....	2914
TEBLİĞLER.....	2931
Vergi Usul Kanunu Genel Tebliği (Sıra No: 538)	2932
İnternet Alan Adları Tebliği.....	2938
Elektronik Ticarete Güven Damgası Hakkında Tebliğ	2943
Kamu İç Kontrol Standartları Tebliği.....	2946
Bilgi Sistemleri Yönetimi Tebliği	2958
Yapı Kooperatiflerine Ait Bilgilerin Elektronik Ortamda Kaydına Dair Tebliğ	2960
CUMHURBAŞKANLIĞI KARARNAMELERİ	2962
1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi.....	2963
49 sayılı Coğrafi Bilgi Sistemleri Hakkında Cumhurbaşkanlığı Kararnamesi.....	2967

MUHTELİF DÜZENLEMELER.....	2969
BTK - 27.12.2016 tarihli Posta Gönderilerine İlişkin Güvenlik Tedbirlerine Yönelik Usul ve Esaslar	2970
ANAYASA MAHKEMESİ NORM DENETİMİ KARARLARI.....	2975
Anayasa Mahkemesi - 6698 sayılı Kişisel Verilerin Korunması Kanunu Kararı (E. 2016/125)	2977
Anayasa Mahkemesi - 7246 sayılı Kanun - Rekabet Kanunu Kararı (E. 2020/67).....	3047
Anayasa Mahkemesi - 715 sayılı Kanun - MİT Kanunu Kararı (E. 2018/137)	3085
Anayasa Mahkemesi - 5188 sayılı Özel Güvenlik Hizmetlerine Dair Kanun Kararı (E. 2021/42)	3115
Anayasa Mahkemesi - 1 numaralı CBK Kararı (MASAK) (E. 2019/96)	3122
Anayasa Mahkemesi - 7068 sayılı Genel Kolluk Disiplin Hükümleri Hakkında Kanun Hükmünde Karamamenin Kabul Edilmesine Dair Kanun Kararı (E. 2020/77)	3168
Anayasa Mahkemesi - 77 numaralı CBK Kararı (E. 2021/88).....	3179
Anayasa Mahkemesi - 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu Kararı (E. 2021/43)	3186
Anayasa Mahkemesi - 6791 sayılı Kanun Kararı (E. 2020/41).....	3200
Anayasa Mahkemesi - 4045 sayılı Kanun Kararı (E. 2020/24).....	3208
Anayasa Mahkemesi - 4045 sayılı Kanun Kararı (E. 2018/163).....	3222
Anayasa Mahkemesi - 14 numaralı CBK Kararı (E. 2018/134).....	3229
Anayasa Mahkemesi - 13 numaralı CBK Kararı (E. 2018/133).....	3281
Anayasa Mahkemesi - 2559 sayılı Polis Vazife ve Salahiyet Kanunu Kararı (E. 2018/91)	3301
Anayasa Mahkemesi - 657 sayılı Kanun Kararı (E. 2018/73).....	3346
Anayasa Mahkemesi - 5490 sayılı Nüfus Hizmetleri Kanunu Kararı (2017/180).....	3420
Anayasa Mahkemesi - 5809 sayılı Elektronik Haberleşme Kanunu Kararı (Madde 60) (E. 2017/16).....	3440
Anayasa Mahkemesi - 4632 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanunu Kararı (E. 2016/179).....	3472
Anayasa Mahkemesi - 5809 sayılı Elektronik Haberleşme Kanunu Kararı (Revize-Madde 51) (E. 2015/61)	3487
Anayasa Mahkemesi - 5237 sayılı Türk Ceza Kanunu Kararı (E. 2015/32).....	3556
Anayasa Mahkemesi - 6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun Kararı (E. 2014/196).....	3562
Anayasa Mahkemesi - 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu Kararı (E. 2014/180)	3591
Anayasa Mahkemesi - 5651 sayılı Kanun (Trafik Bilgisi) Kararı (E. 2014/149)	3604
Anayasa Mahkemesi - 6532 sayılı Kanun - MİT Kanunu Kararı (E. 2014/122)	3643
Anayasa Mahkemesi - 5651 sayılı Kanun (TİB Yetkileri) Kararı (E. 2014/87).....	3723

Anayasa Mahkemesi - 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu (Madde 78) Kararı (E. 2014/74).....	3831
Anayasa Mahkemesi - 663 Sayılı KHK Kararı (E. 2013/114).....	3842
Anayasa Mahkemesi - 5809 sayılı Elektronik Haberleşme Kanunu (Madde 51) Kararı (E. 2013/122).....	3923
Anayasa Mahkemesi - 6475 sayılı Posta Hizmetleri Kanunu (E. 2013/84).....	3927
Anayasa Mahkemesi - 2004 sayılı İcra ve İflas Kanunu Kararı (E. 2012/100).....	3969
Anayasa Mahkemesi - 663 sayılı Kanun Kararı (E. 2011/150).....	4072
Anayasa Mahkemesi - 5952 sayılı Kanun Kararı (E. 2010/40).....	4236
Anayasa Mahkemesi - 5429 sayılı Türkiye İstatistik Kanunu (2010/12).....	4294
Anayasa Mahkemesi - 5237 sayılı Türk Ceza Kanun (245. Madde) Kararı (E. 2006/123)	4305

ANAYASA MAHKEMESİ BİREYSEL BAŞVURU KARARLARI.....4309

Anayasa Mahkemesi - Ümit Eyüpoğlu Kararı (2018/6161).....	4311
Anayasa Mahkemesi - Alper Erarslan Kararı (2018/16857)	4328
Anayasa Mahkemesi - Fırat Gerçek Kararı (2019/25604).....	4341
Anayasa Mahkemesi - Ümit Karaduman Kararı (2020/20874)	4351
Anayasa Mahkemesi - H.Ö. Kararı (2019/20473).....	4373
Anayasa Mahkemesi - Samet Ayyıldız Kararı (2018/34548)	4389
Anayasa Mahkemesi - Sebiha Kaya Kararı (2018/34124).....	4404
Anayasa Mahkemesi - Celal Oraj Altunörgü Kararı (2018/31036)	4446
Anayasa Mahkemesi - Bestami Eroğlu Kararı (2018/23077)	4459
Anayasa Mahkemesi - Ertan Erçikti (3) Kararı (2018/14040)	4513
Anayasa Mahkemesi - Ramazan Şahin Kararı (2018/11988).....	4531
Anayasa Mahkemesi - Kemal Karanfil Kararı (2017/24776)	4553
Anayasa Mahkemesi - A.A.Y. Kararı (2016/13011)	4574
Anayasa Mahkemesi - E.Ü. Kararı (2016/13010).....	4592
Anayasa Mahkemesi - Arif Ali Cangı Kararı (2016/4060)	4621
Anayasa Mahkemesi - Ali Çığır Kararı (2015/19298).....	4652
Anayasa Mahkemesi - C.K. (Unutulma Hakkı) Kararı (2014/19685).....	4662
Anayasa Mahkemesi - Asli Alp ve Şükrü Alp (Unutulma Hakkı) Kararı (2014/18260).....	4680
Anayasa Mahkemesi - Fahri Göncü (Unutulma Hakkı) Kararı (2014/17943).....	4687
Anayasa Mahkemesi - N.B.B. (2) (Unutulma Hakkı) Kararı (2014/17143).....	4695
Anayasa Mahkemesi - G.Y. (Unutulma Hakkı) Kararı (2014/16026).....	4700
Anayasa Mahkemesi - Turgut Duman Kararı (2014/15365).....	4708
Anayasa Mahkemesi - B.K. Kararı (2014/14189).....	4737
Anayasa Mahkemesi - Nurcan Belin Kararı (2014/14187).....	4756

Anayasa Mahkemesi - Fatih Saraman Kararı (2014/7256).....	4770
Anayasa Mahkemesi - Güzide Defne Samyeli Kararı (2014/4399).....	4797
Anayasa Mahkemesi - Asım Bayar ve Veysel Bayar (Unutulma Hakkı) Kararı (2014/4141).....	4824
Anayasa Mahkemesi - G.D. (2) (Unutulma Hakkı) Kararı (2014/1808).....	4831
Anayasa Mahkemesi - E.Ç.A. Kararı (2014/5671).....	4839
Anayasa Mahkemesi - N.B.B. (Unutulma Hakkı) Kararı (2013/5653).....	4858
Anayasa Mahkemesi - Ömür Kara ve Onursal Özbek Kararı (2013/4825).....	4879
Anayasa Mahkemesi - Bülent Kaya Kararı (2013/2941).....	4899

YARGITAY KARARLARI4934

Yargıtay Kararı - Ceza Genel Kurulu (E. 2015/708).....	4936
Yargıtay Kararı - Ceza Genel Kurulu (E. 2012/1510).....	4950
Yargıtay Kararı - Hukuk Genel Kurulu (E. 2017/1340).....	4976
Yargıtay Kararı - Hukuk Genel Kurulu (E. 2014/56).....	4993
Yargıtay Kararı - 19. Ceza Dairesi (E. 2017/3325).....	5003
Yargıtay Kararı - 19. Ceza Dairesi (E. 2017/6127).....	5007
Yargıtay Kararı - 19. Ceza Dairesi (E. 2017/6532).....	5010
Yargıtay Kararı - 19. Ceza Dairesi (E. 2018/3318).....	5013
Yargıtay Kararı - 19. Ceza Dairesi (E. 2019/28161).....	5028
Yargıtay Kararı - 19. Ceza Dairesi (E. 2020/4751).....	5038
Yargıtay Kararı - 17. Ceza Dairesi (E. 2016/10020).....	5058
Yargıtay Kararı - 17. Ceza Dairesi (E. 2016/9901).....	5063
Yargıtay Kararı - 17. Ceza Dairesi (E. 2015/22839).....	5067
Yargıtay Kararı - 17. Ceza Dairesi (E. 2015/18421).....	5071
Yargıtay Kararı - 12. Ceza Dairesi (E. 2020/974).....	5076
Yargıtay Kararı - 12. Ceza Dairesi (E. 2019/4369).....	5078
Yargıtay Kararı - 12. Ceza Dairesi (E. 2017/2960).....	5084
Yargıtay Kararı - 12. Ceza Dairesi (E. 2015/13758).....	5087
Yargıtay Kararı - 12. Ceza Dairesi (E. 2015/13582).....	5089
Yargıtay Kararı - 12. Ceza Dairesi (E. 2013/9043).....	5093
Yargıtay Kararı - 12. Ceza Dairesi (E. 2014/607).....	5096
Yargıtay Kararı - 7. Ceza Dairesi (E. 2021/21566).....	5102
Yargıtay Kararı - 6. Ceza Dairesi (E. 2021/10682).....	5105
Yargıtay Kararı - Hukuk Genel Kurulu (E. 2014/56).....	5108
Yargıtay Kararı - 22. Hukuk Dairesi (E. 2017/21857).....	5117
Yargıtay Kararı - 20.Hukuk Dairesi (E. 2017/2277).....	5121

Yargıtay Kararı - 14. Hukuk Dairesi (E. 2016/2792)	5125
Yargıtay Kararı - 9. Hukuk Dairesi (E. 2014/37215)	5127

DANIŞTAY KARARLARI5131

Danıştay Kararı - İDDK. (E. 2020/1455)	5133
Danıştay Kararı - İDDK. (E. 2020/1454)	5138
Danıştay Kararı - İDDK. (E. 2020/1038)	5143
Danıştay Kararı - İDDK. (E. 2020/937)	5149
Danıştay Kararı - İDDK. (E. 2019/3003)	5168
Danıştay Kararı - İDDK. (E. 2019/2983)	5171
Danıştay Kararı - İDDK.(E. 2019/2549)	5178
Danıştay Kararı - İDDK. (E. 2019/2425)	5187
Danıştay Kararı - İDDK. (E. 2019/2273)	5197
Danıştay Kararı - İDDK. (E. 2019/2365)	5204
Danıştay Kararı - İDDK. (E. 2019/2278)	5210
Danıştay Kararı - İDDK. (E. 2018/4437)	5216
Danıştay Kararı - İDDK (E. 2014/2242)	5228
Danıştay Kararı - 10. Daire (E. 2020/4379)	5232
Danıştay Kararı - 2. Daire (E. 2020/847)	5236
Danıştay Kararı - 10. Daire (E. 2019/10118)	5245
Danıştay Kararı - 12. Daire (E. 2019/7364)	5257
Danıştay Kararı - 12. Daire (E. 2019/7283)	5262
Danıştay Kararı - 10. Daire (E. 2019/7114)	5267
Danıştay Kararı - 10. Daire (E. 2019/7092)	5287
Danıştay Kararı - 10. Daire (E. 2019/7049)	5293
Danıştay Kararı - 12. Daire (E. 2019/5658)	5310
Danıştay Kararı - 15. Daire (E. 2018/1490)	5318
Danıştay Kararı - 12. Daire (E. 2019/1428)	5326
Danıştay Kararı - 10. Daire (E. 2018/3449)	5332
Danıştay Kararı - 13. Daire (E. 2018/2910)	5350
Danıştay Kararı - 15. Daire (E. 2018/844)	5375
Danıştay Kararı - 15. Daire (E. 2018/530)	5390
Danıştay Kararı - 15. Daire (E. 2018/251)	5401
Danıştay Kararı - 8. Daire (E. 2017/7307)	5409
Danıştay Kararı - 10. Daire (E. 2017/4211)	5414
Danıştay Kararı - 8. Daire (E. 2017/1388)	5439

Danıştay Kararı - 10. Daire (E. 2017/1141)	5444
Danıştay Kararı - 11. Daire (E. 2017/816)	5453
Danıştay Kararı - 15. Daire (E. 2016/10500)	5456
Danıştay Kararı - 15. Daire (E. 2016/10488)	5467
Danıştay Kararı - 8. Daire (E. 2016/3355)	5474
Danıştay Kararı - 8. Daire (E. 2016/3316)	5481
Danıştay Kararı - 8. Daire (E. 2016/2727)	5487
Danıştay Kararı - 15. Daire (E. 2015/6279)	5492
Danıştay Kararı - 10. Daire (E. 2015/5219)	5521
Danıştay Kararı - 10. Daire (E. 2015/3902)	5530
Danıştay Kararı - 15. Daire (E. 2015/3035)	5539
Danıştay Kararı - 10. Daire (E. 2015/2995)	5548
Danıştay Kararı - 10. Daire (E. 2015/2787)	5557
Danıştay Kararı - 10. Daire (E. 2015/2696)	5566
BÖLGE İDARE MAHKEMESİ KARARLARI.....	5575
Ankara BİM - 1. İdari Dava Dairesi (E. 2020/557).....	5576
Ankara BİM - 1. İdari Dava Dairesi (E. 2020/324).....	5591
İstanbul BİM - 7. İdari Dava Dairesi (E. 2020/412)	5605
İstanbul BİM - 7. İdari Dava Dairesi (E. 2020/288)	5612
İstanbul BİM - 7. İdari Dava Dairesi (E. 2020/284)	5619
İstanbul BİM - 3. İdari Dava Dairesi (E. 2017/1689)	5626
İzmir BİM - 6. İdari Dava Dairesi (E. 2017/1238)	5635
Konya BİM - 4. İdari Dava Dairesi (E. 2020/731)	5638
UYUŞMAZLIK MAHKEMESİ KARARLARI	5644
Uyuşmazlık Mahkemesi Kararı - HB. (E. 2021/313).....	5645
BÖLGE ADLİYE MAHKEMESİ KARARLARI.....	5654
Ankara BAM - 19. Hukuk Dairesi (E. 2019/3312)	5655
Ankara BAM - 3. Hukuk Dairesi (E. 2017/388)	5659
Bursa BAM - 6. Hukuk Dairesi (E. 2019/2251)	5663
Bursa BAM - 9. Hukuk Dairesi (E. 2018/2576)	5667
İstanbul BAM - 41. Hukuk Dairesi (E. 2020/1833).....	5672
İstanbul BAM - 43. Hukuk Dairesi (E. 2020/448).....	5682
İstanbul BAM - 21. Hukuk Dairesi (E. 2018/3160).....	5689

İstanbul BAM - 4. Hukuk Dairesi (E. 2017/1495).....	5693
İstanbul BAM - 23. Hukuk Dairesi (E. 2017/596).....	5698
İzmir BAM - 12. Hukuk Dairesi (E. 2019/2210).....	5700
İzmir BAM - 12. Hukuk Dairesi (E. 2019/2033).....	5706
İzmir BAM - 12. Hukuk Dairesi (E. 2019/1873).....	5711
İzmir BAM - 9. Hukuk Dairesi (E. 2018/2398).....	5716
İzmir BAM - 8. Hukuk Dairesi (E. 2018/2146).....	5723
İzmir BAM - 8. Hukuk Dairesi (E. 2018/1633).....	5726
İzmir BAM - 12. Hukuk Dairesi (E. 2017/499).....	5729
İzmir BAM - 12. Hukuk Dairesi (E. 2017/498).....	5735
İzmir BAM - 12. Hukuk Dairesi (E. 2016/59).....	5740
Samsun BAM - 4. Hukuk Dairesi (E. 2018/3525)	5746
Samsun BAM - 4. Hukuk Dairesi (E. 2018/3158)	5751
Samsun BAM - 4. Hukuk Dairesi (E. 2018/1643)	5755
ADLİ YARGI İLK DERECE MAHKEMELERİ KARARLARI.....	5762
İstanbul 10. Asliye Ticaret Mahkemesi (E. 2020/616).....	5763
İstanbul 4. Asliye Ticaret Mahkemesi (E. 2019/279).....	5769
KAMU İHALE KURULU KARARLARI.....	5773
Kamu İhale Kurulu Kararı - KİK (K. 2021/UH.II-111)	5774
Kamu İhale Kurulu Kararı - KİK (K. 2020/UY.I-470)	5782
Kamu İhale Kurulu Kararı - KİK (K. 2018/UH.II-1130)	5797
Kamu İhale Kurulu Kararı - KİK (K. 2016/UH.II-1732)	5830
ULUSLARARASI DÜZENLEMELER	5837
AVRUPA KONSEYİ.....	5838
İnsan Hakları Avrupa Sözleşmesi	5839
Avrupa Konseyi - 108 nolu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi	5840
Avrupa Konseyi - 108 nolu Sözleşme (İngilizce).....	5853
Avrupa Konseyi - 108 nolu Sözleşmeye Ek Protokol.....	5863
Avrupa Konseyi - 108 nolu Sözleşmeye Ek Protokol (İngilizce).....	5866
Avrupa Konseyi - 108+ Sözleşmesi (108 Plus)	5869

AVRUPA BİRLİĞİ.....	5885
Avrupa Birliği'nin İşleyişi Hakkında Anlaşma	5886
Avrupa Birliği Temel Haklar Şartı	5887
Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR).....	5888
GDPR Recitals	5981
Avrupa Birliği - 95/46 sayılı Direktif (Türkçe)	6040
Avrupa Birliği - 95/46 sayılı Direktif (İngilizce)	6072
Avrupa Birliği - E-Mahremiyet Direktifi (E-Privacy Directive)	6107
Avrupa Birliği - Polis ve Yargı Kişisel Veriler Direktifi (LED Directive).....	6134
Avrupa Birliği - Açık Veri Direktifi (Open Data Directive).....	6208
Avrupa Birliği - European Declaration on Digital Rights and Principles for the Digital Decade	6247
ULUSLARARASI DİĞER DÜZENLEMELER.....	6258
İnsan Hakları Evrensel Beyanamesi.....	6259
Medeni ve Siyasal Haklar Sözleşmesi.....	6260
OECD - Özel Yaşamın Korunması ve Kişisel Verilerin Sınırlanması Akışına İlişkin Rehber İlkeler	6261
Birleşmiş Milletler - Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler	6268
AVRUPA BİRLİĞİ ADALET DİVANİ KARARLARI (GENEL ÇERÇEVE)	6271
The right to the protection of personal data recognised by the Charter of Fundamental Rights of the European Union.....	6272
<i>Compatibility of secondary EU law with the right to the protection of personal data</i>	<i>6272</i>
<i>Respect for the right to the protection of personal data in the implementation of EU law.....</i>	<i>6277</i>
The processing of personal data within the meaning of Directive 95/46/EC.....	6278
<i>Personal data-processing operations excluded from the scope of Directive 95/46/EC</i>	<i>6278</i>
<i>Concept of 'personal data'</i>	<i>6281</i>
<i>Concept of 'processing of personal data'</i>	<i>6284</i>
<i>Concept of a 'personal data filing system'</i>	<i>6287</i>
<i>Concept of a 'controller of the processing of personal data'</i>	<i>6287</i>
<i>Conditions for lawful processing of personal data in the light of Article 7 of Directive 95/46/EC.....</i>	<i>6290</i>
The processing of personal data within the meaning of Directive 2002/58/EC.....	6295
Transfer of personal data to third countries.....	6297
Protection of personal data on the internet	6305
<i>Right to object to the processing of personal data ('right to be forgotten').....</i>	<i>6305</i>
<i>Processing of personal data and intellectual property rights</i>	<i>6306</i>
<i>De-referencing of personal data.....</i>	<i>6310</i>

<i>Consent by a website user to the storage of or access to information in the form of cookies</i>	6313
National supervisory authorities.....	6315
<i>Scope of the requirement of independence</i>	6315
<i>Determination of the applicable law and of the competent supervisory authority</i>	6318
<i>Powers of the national supervisory authorities</i>	6320
Territorial application of EU legislation	6321
Right of public access to documents of the institutions of the European Union and protection of personal data	6322
AVRUPA BİRLİĞİ ADALET DİVANİ KARARLARI (TAM METİN).....	6326
ABAD - Österreichische Post (C-154/21)	6327
ABAD - Autoriteit Persoonsgegevens (C-245/20).....	6344
ABAD - Meta Platforms Ireland (Case C-319/20).....	6355
ABAD - PNR Directive (C-817/19).....	6379
ABAD - Schrems II - Data Protection Commissioner v. Facebook Ireland Ltd. (C-311/18).....	6475
ABAD - Prokuratuur Case (C-746/18).....	6545
ABAD - G.D. v The Commissioner of the Garda Síochána Case (C-140/20)	6570
AVRUPA İNSAN HAKLARI MAHKEMESİ (AİHM) KARARLARI.....	6610
Electronic data.....	6610
E-mail	6624
GPS (Global Positioning System).....	6627
Internet	6628
Mobile telephone	6644
Copyright of books and musical work	6645
Online harassment.....	6646
Radio communications	6647
Satellite dish.....	6647
Telecommunications	6648
Use of hidden cameras	6650
Video surveillance	6651
MUHTELİF ÜLKE DÜZENLEMELERİ	6656
ABD Federe Devlet Anayasalarında Özel Hayat ve Mahremiyet.....	6657
ABD - California Consumer Privacy Act of 2018 (CCPA).....	6660
ABD - Virginia Consumer Data Protection Act (CDPA).....	6750

ABD - Colorado Privacy Act (CPA)	6767
Almanya - Federal Data Protection Act (BDSG).....	6790
İrlanda - Data Protection Act 2018.....	6854
Estonya - Personal Data Protection Act.....	7059
Çin - Personal Information Protection Law of the People's Republic of China	7094
Çin - Data Security Law of the People's Republic of China.....	7115
Güney Kore - Personal Information Protection Act.....	7128
Güney Kore - Personal Information Safeguard and Security Standard	7200
Japonya - Act on the Protection of Personal Information	7208
Katar - Personal Data Privacy Protection	7261
Kuzey Kıbrıs Türk Cumhuriyeti - 89/2007 Kişisel Verilerin Korunması Yasası	7272
Asya-Pasifik Ekonomik İş Birliği Forumu (APEC) - APEC Privacy Framework.....	7294
OECD Declaration on Government Access to Personal Data Held by Private Sector Entities	7319
BİBLİYOGRAFYA	7327
Kitap	7327
Kitap Bölümleri.....	7334
Editörlü Kitaplar	7335
Makaleler	7336
Raporlar.....	7355
Mevzuat Derlemeleri.....	7356

ANAYASA

IV. Özel hayatın gizliliği ve korunması

A. Özel hayatın gizliliği

Madde 20 - Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. (Mülga üçüncü cümle: 3/10/2001-4709/5 md.) (...)

(Değişik fıkra: 3/10/2001-4709/5 md.) Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.

(Ek fıkra: 7/5/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.

C. Haberleşme hürriyeti

MADDE 22- (Değişik: 3/10/2001-4709/7 md.)

Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.

İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir.

KİŞİSEL VERİLERİN KORUMASI KANUNU

Kanun Numarası : 6698

Kabul Tarihi : 24.03.2016

Resmî Gazete Tarihi : 07.04.2016

Resmî Gazete Sayısı : 29677

KİŞİSEL VERİLERİN KORUMASI KANUNU

Amaç

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

MADDE 1 - (1) Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.

Kapsam

MADDE 2 - (1) Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır.

Tanımlar

MADDE 3 - (1) Bu Kanunun uygulanmasında;

- a) Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,
- b) Anonim hâle getirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini,
- c) Başkan: Kişisel Verileri Koruma Kurumu Başkanı,
- ç) İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,
- d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

f) Kurul: Kişisel Verileri Koruma Kurulunu,

g) Kurum: Kişisel Verileri Koruma Kurumunu,

ğ) Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,

h) Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,

ı) Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,

ifade eder.

Genel ilkeler

İKİNCİ BÖLÜM

Kişisel Verilerin İşlenmesi

MADDE 4 - (1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.

(2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

a) Hukuka ve dürüstlük kurallarına uygun olma.

b) Doğru ve gerektiğinde güncel olma.

c) Belirli, açık ve meşru amaçlar için işlenme.

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

Kişisel verilerin işlenme şartları

MADDE 5 - (1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın

kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Özel nitelikli kişisel verilerin işlenme şartları

MADDE 6 - (1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.

Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi

MADDE 7 - (1) Bu Kanun ve ilgili dięer kanun hkmlerine uygun olarak iřlenmiř olmasına raęmen, iřlenmesini gerektiren sebeplerin ortadan kalkması hlinde kiřisel veriler resen veya ilgili kiřinin talebi zerine veri sorumlusu tarafından silinir, yok edilir veya anonim hle getirilir.

(2) Kiřisel verilerin silinmesi, yok edilmesi veya anonim hle getirilmesine iliřkin dięer kanunlarda yer alan hkmler saklıdır.

(3) Kiřisel verilerin silinmesine, yok edilmesine veya anonim hle getirilmesine iliřkin usul ve esaslar ynetmelikle dzenlenir.

Kiřisel verilerin aktarılması

MADDE 8 - (1) Kiřisel veriler, ilgili kiřinin aık rızası olmaksızın aktarılamaz.

(2) Kiřisel veriler;

a) 5 inci maddenin ikinci fıkrasında,

b) Yeterli nlemler alınmak kaydıyla, 6 ncı maddenin cnc fıkrasında,

belirtilen řartlardan birinin bulunması hlinde, ilgili kiřinin aık rızası aranmaksızın aktarılabilir.

(3) Kiřisel verilerin aktarılmasına iliřkin dięer kanunlarda yer alan hkmler saklıdır.

Kiřisel verilerin yurt dıřına aktarılması

MADDE 9 - (1) Kiřisel veriler, ilgili kiřinin aık rızası olmaksızın yurt dıřına aktarılamaz.

(2) Kiřisel veriler, 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin cnc fıkrasında belirtilen řartlardan birinin varlıęı ve kiřisel verinin aktarılacaęı yabancı lkede;

a) Yeterli korumanın bulunması,

b) Yeterli korumanın bulunmaması durumunda Trkiye'deki ve ilgili yabancı lkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahht etmeleri ve Kurulun izninin bulunması, kaydıyla ilgili kiřinin aık rızası aranmaksızın yurt dıřına aktarılabilir.

(3) Yeterli korumanın bulunduęu lkeler Kurulca belirlenerek ilan edilir.

(4) Kurul yabancı lkede yeterli koruma bulunup bulunmadıęına ve ikinci fıkranın (b) bendi uyarınca izin verilip verilmeyeceęine;

a) Trkiye'nin taraf olduęu uluslararası szleřmeleri,

b) Kiřisel veri talep eden lke ile Trkiye arasında veri aktarımına iliřkin karřılıklılık durumunu,

- c) Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işleme amaç ve süresini,
- ç) Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını,
- d) Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri, değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir.
- (5) Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir.
- (6) Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.

ÜÇÜNCÜ BÖLÜM

Haklar ve Yükümlülükler Veri sorumlusunun aydınlatma yükümlülüğü

MADDE 10 - (1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere;

- a) Veri sorumlusunun ve varsa temsilcisinin kimliği,
- b) Kişisel verilerin hangi amaçla işleneceği,
- c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabilceği,
- ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,
- d) 11 inci maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür.

İlgili kişinin hakları

MADDE 11 - (1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

- a) Kişisel veri işlenip işlenmediğini öğrenme,
- b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- c) Kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,

- e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
- f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme,
- haklarına sahiptir.

Veri güvenliğine ilişkin yükümlülükler

MADDE 12 - (1) Veri sorumlusu;

- a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
- c) Kişisel verilerin muhafazasını sağlamak,
- amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.
- (2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.
- (3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.
- (4) Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.
- (5) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.

DÖRDÜNCÜ BÖLÜM

Başvuru, Şikâyet ve Veri Sorumluları Sicili Veri sorumlusuna başvuru

MADDE 13 - (1) İlgili kişi, bu Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir.

(2) Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak, işlemin ayrıca bir maliyeti gerektirmesi hâlinde, Kurulca belirlenen tarifedeki ücret alınabilir.

(3) Veri sorumlusu talebi kabul eder veya gerekçesini açıklayarak reddeder ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. Başvuruda yer alan talebin kabul edilmesi hâlinde veri sorumlusunca gereği yerine getirilir. Başvurunun veri sorumlusunun hatasından kaynaklanması hâlinde alınan ücret ilgiliye iade edilir.

Kurula şikâyet

MADDE 14 - (1) Başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyette bulunabilir.

(2) 13 üncü madde uyarınca başvuru yolu tüketilmeden şikâyet yoluna başvurulamaz.

(3) Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır.

Şikâyet üzerine veya resen incelemenin usul ve esasları

MADDE 15 - (1) Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapar.

(2) 1/11/1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesinde belirtilen şartları taşımayan ihbar veya şikâyetler incelemeye alınmaz.

(3) Devlet sırrı niteliğindeki bilgi ve belgeler hariç; veri sorumlusu, Kurulun, inceleme konusuyla ilgili istemiş olduğu bilgi ve belgeleri on beş gün içinde göndermek ve gerektiğinde yerinde inceleme yapılmasına imkân sağlamak zorundadır.

(4) Şikâyet üzerine Kurul, talebi inceleyerek ilgililere bir cevap verir. Şikâyet tarihinden itibaren altmış gün içinde cevap verilmezse talep reddedilmiş sayılır.

(5) Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması hâlinde Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ eder. Bu karar, tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilir.

(6) Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin yaygın olduğunun tespit edilmesi hâlinde Kurul, bu konuda ilke kararı alır ve bu kararı yayımlar. Kurul, ilke kararı almadan önce ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşlerini de alabilir.

(7) Kurul, telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması hâlinde, veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulmasına karar verebilir.

Veri Sorumluları Sicili

MADDE 16 - (1) Kurulun gözetiminde, Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili tutulur.

(2) Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir.

(3) Veri Sorumluları Siciline kayıt başvurusu aşağıdaki hususları içeren bir bildirimle yapılır:

- a) Veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri.
- b) Kişisel verilerin hangi amaçla işleneceği.
- c) Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar.
- ç) Kişisel verilerin aktarılabilmesi için alıcı veya alıcı grupları.
- d) Yabancı ülkelere aktarımı öngörülen kişisel veriler.
- e) Kişisel veri güvenliğine ilişkin alınan tedbirler.
- f) Kişisel verilerin işlendikleri amaç için gerekli olan azami süre.

(4) Üçüncü fıkra uyarınca verilen bilgilerde meydana gelen değişiklikler derhâl Başkanlığa bildirilir.

(5) Veri Sorumluları Siciline ilişkin diğer usul ve esaslar yönetmelikle düzenlenir.

Suçlar

BEŞİNCİ BÖLÜM

Suçlar ve Kabahatler

MADDE 17 - (1) Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümleri uygulanır.

(2) Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır.

Kabahatler

MADDE 18 - (1) Bu Kanunun;

a) 10 uncu maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar,

b) 12 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar,

c) 15 inci maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar,

ç) 16 ncı maddesinde öngörülen Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar,

idari para cezası verilir.

(2) Bu maddede öngörülen idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır.

(3) Birinci fıkrada sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu Kurula bildirilir.

ALTINCI BÖLÜM

Kişisel Verileri Koruma Kurumu ve Teşkilat Kişisel Verileri Koruma Kurumu

MADDE 19 - (1) Bu Kanunla verilen görevleri yerine getirmek üzere, idari ve mali özerkliğe sahip ve kamu tüzel kişiliğini haiz Kişisel Verileri Koruma Kurumu kurulmuştur.

(2) Kurum Cumhurbaşkanının görevlendireceği bakan ile ilişkilidir.¹

(3) Kurumun merkezi Ankara'dadır.

¹ 2/7/2018 tarihli ve 703 sayılı KHK'nin 163 üncü maddesiyle, bu fıkrada yer alan "Başbakanlıkla" ibaresi "Cumhurbaşkanının görevlendireceği bakan ile" şeklinde değiştirilmiştir.

(4) Kurum, Kurul ve Başkanlıktan oluşur. Kurumun karar organı Kuruldur.

Kurumun görevleri

MADDE 20 - (1) Kurumun görevleri şunlardır:

- a) Görev alanı itibarıyla, uygulamaları ve mevzuattaki gelişmeleri takip etmek, değerlendirme ve önerilerde bulunmak, araştırma ve incelemeler yapmak veya yaptırmak.
- b) İhtiyaç duyulması hâlinde, görev alanına giren konularda kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri veya üniversitelerle iş birliği yapmak.
- c) Kişisel verilerle ilgili uluslararası gelişmeleri izlemek ve değerlendirmek, görev alanına giren konularda uluslararası kuruluşlarla iş birliği yapmak, toplantılara katılmak.
- ç) Yıllık faaliyet raporunu Cumhurbaşkanlığına, Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonuna (...)² sunmak.³
- d) Kanunlarla verilen diğer görevleri yerine getirmek.

Kişisel Verileri Koruma Kurulu

MADDE 21- (1) Kurul, bu Kanunla ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getirir ve kullanır. Görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişi, Kurula emir ve talimat veremez, tavsiye veya telkinde bulunamaz.

(2) Kurul, dokuz üyeden oluşur. Kurulun beş üyesi Türkiye Büyük Millet Meclisi, dört üyesi Cumhurbaşkanı tarafından seçilir.⁴

(3) Kurula üye olabilmek için aşağıdaki şartlar aranır:

- a) Kurumun görev alanındaki konularda bilgi ve deneyim sahibi olmak.
- b) 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanununun 48 inci maddesinin birinci fıkrasının (A) bendinin (1), (4), (5), (6) ve (7) numaralı alt bentlerinde belirtilen nitelikleri taşımak.
- c) Herhangi bir siyasi parti üyesi olmamak.

² 2/7/2018 tarihli ve 703 sayılı KHK'nin 163 üncü maddesiyle, bu bentte yer alan " ve Başbakanlığa" ibaresi yürürlükten kaldırılmıştır.

³ 2/7/2018 tarihli ve 703 sayılı KHK'nin 163 üncü maddesiyle, bu bentte yer alan " ve Başbakanlığa" ibaresi yürürlükten kaldırılmıştır.

⁴ 2/7/2018 tarihli ve 703 sayılı KHK'nin 163 üncü maddesiyle, bu maddenin ikinci fıkrasında yer alan "iki üyesi Cumhurbaşkanı, iki üyesi Bakanlar Kurulu" ibaresi "dört üyesi Cumhurbaşkanı" şeklinde değiştirilmiştir.

ç) En az dört yıllık lisans düzeyinde yükseköğrenim görmüş olmak.

d) (Mülga: 2/7/2018-KHK-703/163 md.)

(4) (Mülga: 2/7/2018-KHK-703/163 md.)

(5) Türkiye Büyük Millet Meclisi, Kurula üye seçimini aşağıdaki usulle yapar:

a) Seçim için, siyasi parti gruplarının üye sayısı oranında belirlenecek üye sayısının ikişer katı aday gösterilir ve Kurul üyeleri bu adaylar arasından her siyasi parti grubuna düşen üye sayısı esas alınmak suretiyle Türkiye Büyük Millet Meclisi Genel Kurulunca seçilir. Ancak, siyasi parti gruplarında, Türkiye Büyük Millet Meclisinde yapılacak seçimlerde kime oy kullanılacağına dair görüşme yapılamaz ve karar alınmaz.

b) Kurul üyelerinin seçimi, adayların belirlenerek ilanından sonra on gün içinde yapılır. Siyasi parti grupları tarafından gösterilen adaylar için ayrı ayrı listeler hâlinde birleşik oy pusulası düzenlenir. Adayların adlarının karşısındaki özel yer işaretlenmek suretiyle oy kullanılır. Siyasi parti gruplarının ikinci fıkraya göre belirlenen kontenjanlarından Kurula seçilecek üyelerin sayısından fazla verilen oylar geçersiz sayılır.

c) Karar yeter sayısı olmak şartıyla seçimde en çok oyu alan boş üyelik sayısı kadar aday seçilmiş olur.

ç) Üyelerin görev sürelerinin bitiminden iki ay önce; üyeliklerde herhangi bir sebeple boşalma olması hâlinde, boşalma tarihinden veya boşalma tarihinde Türkiye Büyük Millet Meclisi tatilde ise tatilin bitiminden itibaren bir ay içinde aynı usulle seçim yapılır. Bu seçimlerde, boşalan üyeliklerin siyasi parti gruplarına dağılımı, ilk seçimde siyasi parti grupları kontenjanından seçilen üye sayısı ve siyasi parti gruplarının hâlihazırdaki oranı dikkate alınmak suretiyle yapılır.

(6) Cumhurbaşkanı (...) ⁵ tarafından seçilen üyelerden birinin görev süresinin bitiminden kırk beş gün önce veya herhangi bir sebeple görevin sona ermesi hâlinde durum, on beş gün içinde Kurum tarafından, Cumhurbaşkanlığına (...) ⁶ bildirilir. Üyelerin görev süresinin dolmasına bir ay kala yeni üye seçimi yapılır. Bu üyeliklerde, görev süresi dolmadan herhangi bir sebeple boşalma olması hâlinde ise bildirimden itibaren on beş gün içinde seçim yapılır.

⁵ 2/7/2018 tarihli ve 703 sayılı KHK'nin 163 üncü maddesiyle, bu fıkrada yer alan "veya Bakanlar Kurulu" ve "veya Bakanlar Kuruluna sunulmak üzere Başbakanlığa" ibareleri madde metninden çıkarılmıştır.

⁶ 2/7/2018 tarihli ve 703 sayılı KHK'nin 163 üncü maddesiyle, bu fıkrada yer alan "veya Bakanlar Kurulu" ve "veya Bakanlar Kuruluna sunulmak üzere Başbakanlığa" ibareleri madde metninden çıkarılmıştır.

(7) Kurul, üyeleri arasından Başkan ve İkinci Başkanı seçer. Kurulun Başkanı, Kurumun da başkanıdır.

(8) Kurul üyelerinin görev süresi dört yıldır. Süresi biten üye yeniden seçilebilir. Görev süresi dolmadan herhangi bir sebeple görevi sona eren üyenin yerine seçilen kişi, yerine seçildiği üyenin kalan süresini tamamlar.

(9) Seçilen üyeler Yargıtay Birinci Başkanlık Kurulu huzurunda "Görevimi Anayasaya ve kanunlara uygun olarak, tam bir tarafsızlık, dürüstlük, hakkaniyet ve adalet anlayışı içinde yerine getireceğime, namusum ve şerefim üzerine yemin ederim." şeklinde yemin ederler. Yargıtaya yemin için yapılan başvuru acele işlerden sayılır.

(10) Kurul üyeleri özel bir kanuna dayanmadıkça, Kuruldaki resmî görevlerinin yürütülmesi dışında resmî veya özel hiçbir görev alamaz, dernek, vakıf, kooperatif ve benzeri yerlerde yöneticilik yapamaz, ticaretle uğraşamaz, serbest meslek faaliyetinde bulunamaz, hakemlik ve bilirkişilik yapamazlar. Ancak, Kurul üyeleri, asli görevlerini aksatmayacak şekilde bilimsel amaçlı yayın yapabilir, ders ve konferans verebilir ve bunlardan doğacak telif hakları ile ders ve konferans ücretlerini alabilirler.

(11) Üyelerin görevleri sebebiyle işledikleri iddia edilen suçlara ilişkin soruşturmalar 2/12/1999 tarihli ve 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanuna göre yapılır ve bunlar hakkında soruşturma izni Cumhurbaşkanı tarafından verilir.⁷

(12) Kurul üyeleri hakkında yapılacak disiplin soruşturması ve kovuşturmasında 657 sayılı Kanun hükümleri uygulanır.

(13) Kurul üyelerinin süreleri dolmadan herhangi bir nedenle görevlerine son verilemez. Kurul üyelerinin;

a) Seçilmek için gereken şartları taşımadıklarının sonradan anlaşılması,

b) Görevleriyle ilgili olarak işledikleri suçlardan dolayı haklarında verilen mahkûmiyet kararının kesinleşmesi,

c) Görevlerini yerine getiremeyeceklerinin sağlık kurulu raporuyla kesin olarak tespit edilmesi,

ç) Görevlerine izinsiz, mazeretsiz ve kesintisiz olarak on beş gün ya da bir yılda toplam otuz gün süreyle devam etmediklerinin tespit edilmesi,

⁷ 2/7/2018 tarihli ve 703 sayılı KHK'nin 163 üncü maddesiyle, bu fıkrada yer alan "Başbakan" ibaresi "Cumhurbaşkanı" şeklinde değiştirilmiştir.

d) Bir ay içinde izinsiz ve mazeretsiz olarak toplam üç, bir yıl içinde toplam on Kurul toplantısına katılmadıklarının tespit edilmesi,

hâllerinde Kurul kararıyla üyelikleri sona erer.

(14) Kurul üyeliğine seçilenlerin Kurulda görev yaptıkları sürece önceki görevleri ile olan ilişkileri kesilir. Kamu görevlisi iken üyeliğe seçilenler, memuriyete giriş şartlarını kaybetmemeleri kaydıyla, görev sürelerinin sona ermesi veya görevden ayrılma isteğinde bulunmaları ve otuz gün içinde eski kurumlarına başvurmaları durumunda atamaya yetkili makam tarafından bir ay içinde mükteseplerine uygun bir kadroya atanır. Atama gerçekleşinceye kadar, bunların almakta oldukları her türlü ödemelerin Kurum tarafından ödenmesine devam olunur. Bir kamu kurumunda çalışmayanlardan üyeliğe seçilip yukarıda belirtilen şekilde görevi sona erenlere herhangi bir görev veya işe başlayıncaya kadar, almakta oldukları her türlü ödemeler Kurum tarafından ödenmeye devam edilir ve bu şekilde üyeliği sona erenlere Kurum tarafından yapılacak ödeme üç ayı geçemez. Bunların Kurumda geçirdiği süreler, özlük ve diğer hakları açısından önceki kurum veya kuruluşlarında geçirilmiş sayılır.

Kurulun görev ve yetkileri

MADDE 22 - (1) Kurulun görev ve yetkileri şunlardır:

- a) Kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak.
- b) Kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikâyetlerini karara bağlamak.
- c) Şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde bu konuda geçici önlemler almak.
- ç) Özel nitelikli kişisel verilerin işlenmesi için aranan yeterli önlemleri belirlemek.
- d) Veri Sorumluları Sicilinin tutulmasını sağlamak.
- e) Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmak.
- f) Veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak.
- g) Veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmak.
- ğ) Bu Kanunda öngörülen idari yaptırımlara karar vermek.

h) Diđer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek.

ı) Kurumun; stratejik planını karara bağlamak, amaç ve hedeflerini, hizmet kalite standartlarını ve performans kriterlerini belirlemek.

i) Kurumun stratejik planı ile amaç ve hedeflerine uygun olarak hazırlanan bütçe teklifini görüşmek ve karara bağlamak.

j) Kurumun performansı, mali durumu, yıllık faaliyetleri ve ihtiyaç duyulan konular hakkında hazırlanan rapor taslaklarını onaylamak ve yayımlamak.

k) Taşınmaz alımı, satımı ve kiralanması konularındaki önerileri görüşüp karara bağlamak.

l) Kanunlarla verilen diđer görevleri yerine getirmek.

Kurulun çalışma esasları

MADDE 23 - (1) Kurulun toplantı günlerini ve gündemini Başkan belirler. Başkan gereken hâllerde Kurulu olağanüstü toplantıya çağırabilir.

(2) Kurul, başkan dâhil en az altı üye ile toplanır ve üye tam sayısının salt çoğunluğuyla karar alır. Kurul üyeleri çekimser oy kullanamaz.

(3) Kurul üyeleri; kendilerini, üçüncü dereceye kadar kan ve ikinci dereceye kadar kayın hısımlarını, evlatlıklarını ve aralarındaki evlilik bağı kalkmış olsa bile eşlerini ilgilendiren konularla ilgili toplantı ve oylamaya katılamaz.

(4) Kurul üyeleri çalışmaları sırasında ilgililere ve üçüncü kişilere ait öğrendikleri sırları bu konuda kanunen yetkili kılınan mercilerden başkasına açıklayamazlar ve kendi yararlarına kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

(5) Kurulda görüşülen işler tutanağa bağlanır. Kararlar ve varsa karşı oy gerekçeleri karar tarihinden itibaren en geç on beş gün içinde yazılır. Kurul, gerekli gördüğü kararları kamuoyuna duyurur.

(6) Aksi kararlaştırılmadıkça, Kurul toplantılarındaki görüşmeler gizlidir.

(7) Kurulun çalışma usul ve esasları ile kararların yazımı ve diđer hususlar yönetmelikle düzenlenir.

Başkan

MADDE 24 - (1) Başkan, Kurul ve Kurumun başkanı sıfatıyla Kurumun en üst amiri olup Kurum hizmetlerini mevzuata, Kurumun amaç ve politikalarına, stratejik planına, performans ölçütlerine ve

hizmet kalite standartlarına uygun olarak düzenler, yürütür ve hizmet birimleri arasında koordinasyonu sağlar.

(2) Başkan, Kurumun genel yönetim ve temsilinden sorumludur. Bu sorumluluk, Kurum çalışmalarının düzenlenmesi, yürütülmesi, denetlenmesi, değerlendirilmesi ve gerektiğinde kamuoyuna duyurulması görev ve yetkilerini kapsar.

(3) Başkanın görevleri şunlardır:

a) Kurul toplantılarını idare etmek.

b) Kurul kararlarının tebliğini ve Kurulca gerekli görülenlerin kamuoyuna duyurulmasını sağlamak ve uygulanmalarını izlemek.

c) Başkan Yardımcısını, daire başkanlarını ve Kurum personelini atamak.

ç) Hizmet birimlerinden gelen önerilere son şeklini vererek Kurula sunmak.

d) Stratejik planın uygulanmasını sağlamak, hizmet kalite standartları doğrultusunda insan kaynakları ve çalışma politikalarını oluşturmak.

e) Belirlenen stratejilere, yıllık amaç ve hedeflere uygun olarak Kurumun yıllık bütçesi ile mali tablolarını hazırlamak.

f) Kurul ve hizmet birimlerinin uyumlu, verimli, disiplinli ve düzenli bir biçimde çalışması amacıyla koordinasyonu sağlamak.

g) Kurumun diğer kuruluşlarla ilişkilerini yürütmek.

ğ) Kurum Başkanı adına imzaya yetkili personelin görev ve yetki alanını belirlemek.

h) Kurumun yönetim ve işleyişine ilişkin diğer görevleri yerine getirmek.

(4) Kurum Başkanının yokluğunda İkinci Başkan, Başkana vekalet eder.

Başkanlığın oluşumu ve görevleri

MADDE 25 - (1) Başkanlık; Başkan Yardımcısı ve hizmet birimlerinden oluşur. Başkanlık, dördüncü fıkrada sayılan görevleri daire başkanlıkları şeklinde teşkilatlanan hizmet birimleri aracılığıyla yerine getirir. Daire başkanlıklarının sayısı yediyi geçemez.

(2) Başkan tarafından, Kuruma ilişkin görevlerinde yardımcı olmak üzere bir Başkan Yardımcısı atanır.

(3) Başkan Yardımcısı ve daire başkanları; en az dört yıllık yükseköğretim kurumu mezunu, on yıl süreyle kamu hizmetinde bulunan kişiler arasından Başkan tarafından atanır.

(4) Başkanlığın görevleri şunlardır:

a) Veri Sorumluları Sicilini tutmak.

b) Kurumun ve Kurulun büro ve sekreteryaya işlemlerini yürütmek.

c) Kurumun taraf olduğu davalar ile icra takiplerinde avukatlar vasıtasıyla Kurumu temsil etmek, davaları takip etmek veya ettirmek, hukuk hizmetlerini yürütmek.

ç) Kurul üyeleri ile Kurumda görev yapanların özlük işlemlerini yürütmek.

d) Kanunlarla mali hizmet ve strateji geliştirme birimlerine verilen görevleri yapmak.

e) Kurumun iş ve işlemlerinin yürütülmesi amacıyla bilişim sisteminin kurulmasını ve kullanılmasını sağlamak.

f) Kurulun yıllık faaliyetleri hakkında veya ihtiyaç duyulan konularda rapor taslaklarını hazırlamak ve Kurula sunmak.

g) Kurumun stratejik plan taslağını hazırlamak.

ğ) Kurumun personel politikasını belirlemek, personelin kariyer ve eğitim planlarını hazırlamak ve uygulamak.

h) Personelin atama, nakil, disiplin, performans, terfi, emeklilik ve benzeri işlemlerini yürütmek.

ı) Personelin uyacağı etik kuralları belirlemek ve gerekli eğitimi vermek.

i) 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanunu çerçevesinde Kurumun ihtiyacı olan her türlü satın alma, kiralama, bakım, onarım, yapım, arşiv, sağlık, sosyal ve benzeri hizmetleri yürütmek.

j) Kuruma ait taşınır ve taşınmazların kayıtlarını tutmak.

k) Kurul veya Başkan tarafından verilen diğer görevleri yapmak.

(5) Hizmet birimleri ile bu birimlerin çalışma usul ve esasları, bu Kanunda belirtilen faaliyet alanı, görev ve yetkilere uygun olarak Kurumun teklifi üzerine Cumhurbaşkanınca yürürlüğe konulan yönetmelikle belirlenir.⁸

⁸ 2/7/2018 tarihli ve 703 sayılı KHK'nin 163 üncü maddesiyle, bu fıkrada yer alan "Bakanlar Kurulu kararıyla" ibaresi "Cumhurbaşkanınca" şeklinde değiştirilmiştir.

Kişisel Verileri Koruma Uzmanı ve uzman yardımcıları

MADDE 26 - (1) Kurumda, Kişisel Verileri Koruma Uzmanı ve Kişisel Verileri Koruma Uzman Yardımcısı istihdam edilebilir. Bunlardan 657 sayılı Kanunun ek 41 inci maddesi çerçevesinde Kişisel Verileri Koruma Uzmanı kadrosuna atananlara bir defaya mahsus olmak üzere bir derece yükseltilmesi uygulanır.

Personele ve özlük haklarına ilişkin hükümler

MADDE 27 - (1) Kurum personeli, bu Kanunla düzenlenen hususlar dışında 657 sayılı Kanuna tabidir.

(2) Kurul Başkan ve üyeleri ile Kurum personeline 27/6/1989 tarihli ve 375 sayılı Kanun Hükmünde Kararnamenin ek 11 inci maddesi uyarınca belirlenmiş emsali personele mali ve sosyal haklar kapsamında yapılan ödemeler aynı usul ve esaslar çerçevesinde ödenir. Emsali personele yapılan ödemelerden vergi ve diğer yasal kesintilere tabi olmayanlar bu Kanuna göre de vergi ve diğer kesintilere tabi olmaz.

(3) Kurul Başkan ve üyeleri ile Kurum personeli 31/5/2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 4 üncü maddesinin birinci fıkrasının (c) bendi hükümlerine tabidir. Kurul Başkan ve üyeleri ile Kurum personeli emeklilik hakları bakımından da emsali olarak belirlenen personel ile denk kabul edilir. 5510 sayılı Kanunun 4 üncü maddesinin birinci fıkrasının (c) bendi kapsamında sigortalı iken Kurul Başkanı ve üyeliklerine atananlardan bu görevleri sona erenler veya bu görevlerinden ayrılma isteğinde bulunanların bu görevlerde geçen hizmet süreleri kazanılmış hak aylık, derece ve kademelerinin tespitinde dikkate alınır. Bunlardan bu görevleri sırasında 5510 sayılı Kanunun geçici 4 üncü maddesi kapsamına girenlerin bu görevlerde geçen süreleri makam tazminatı ile temsil tazminatı ödenmesi gereken süre olarak değerlendirilir. Kamu kurum ve kuruluşlarında 5510 sayılı Kanunun 4 üncü maddesinin birinci fıkrasının (a) bendi kapsamında sigortalı iken Kurul Başkanı ve üyeliklerine atananların, önceki kurum ve kuruluşları ile ilişkilerinin kesilmesi kendilerine kıdem tazminatı veya iş sonu tazminatı ödenmesini gerektirmez. Bu durumda olanların kıdem tazminatı veya iş sonu tazminatı ödenmesi gereken hizmet süreleri, Kurul Başkanı ile Kurul üyeliği olarak geçen hizmet süreleri ile birleştirilir ve emeklilik ikramiyesi ödenecek süre olarak değerlendirilir.

(4) Merkezi yönetim kapsamındaki kamu idarelerinde, sosyal güvenlik kurumlarında, mahallî idarelerde, mahallî idarelere bağlı idarelerde, mahallî idare birliklerinde, döner sermayeli kuruluşlarda, kanunlarla kurulan fonlarda, kamu tüzel kişiliğini haiz kuruluşlarda, sermayesinin

yüzde ellisinden fazlası kamuya ait kuruluşlarda, iktisadi devlet teşekkülleri ve kamu iktisadi kuruluşları ile bunlara bağlı ortaklıklar ve müesseselerde görevli memurlar ile diğer kamu görevlileri kurumlarının muvafakati, hâkimler ve savcılar ise kendilerinin muvafakati ile aylık, ödenek, her türlü zam ve tazminatlar ile diğer mali ve sosyal hak ve yardımları kurumlarınca ödenmek kaydıyla geçici olarak Kurumda görevlendirilebilir. Kurumun bu konudaki talepleri, ilgili kurum ve kuruluşlarca öncelikle sonuçlandırılır. Bu şekilde görevlendirilen personel, kurumlarından aylıklı izinli sayılır. Bu personelin izinli oldukları sürece memuriyetleri ile ilgileri ve özlük hakları devam ettiği gibi, bu süreler yükselme ve emekliliklerinde de hesaba katılır ve yükselmeleri başkaca bir işleme gerek duyulmadan süresinde yapılır. Bu madde kapsamında görevlendirilenlerin, Kurumda geçirdikleri süreler, kendi kurumlarında geçirilmiş sayılır. Bu şekilde görevlendirilenlerin sayısı Kişisel Verileri Koruma Uzmanı ve Kişisel Verileri Koruma Uzman Yardımcısı toplam kadro sayısının yüzde onunu aşamaz ve görevlendirme süresi iki yılı geçemez. Ancak ihtiyaç hâlinde bu süre bir yıllık dönemler hâlinde uzatılabilir.⁹

(5) Kurumda istihdam edilecek personele ilişkin kadro unvan ve sayıları ekli (I) sayılı cetvelde gösterilmiştir. Toplam kadro sayısını geçmemek üzere 13/12/1983 tarihli ve 190 sayılı Genel Kadro ve Usulü Hakkında Kanun Hükmünde Kararnamenin eki cetvellerde yer alan kadro unvanlarıyla sınırlı olmak kaydıyla unvan ve derece değişikliği yapma, yeni unvan ekleme ve boş kadroların iptali Kurul kararıyla yapılır.

İstisnalar

YEDİNCİ BÖLÜM

Çeşitli Hükümler

MADDE 28 - (1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:

- a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi.
- b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.

⁹ 28/11/2017 tarihli ve 7061 sayılı Kanununun 119 uncu maddesiyle bu fıkrada yer alan “diğer kamu görevlileri kurumlarının muvafakati” ibaresinden sonra gelmek üzere “, hâkimler ve savcılar ise kendilerinin muvafakati” ibaresi eklenmiştir.

c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.

ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

(2) Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri aşağıdaki hâllerde uygulanmaz:

a) Kişisel veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.

b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.

c) Kişisel veri işleminin kanunun verdiği yetkiye dayanarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.

ç) Kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

Kurumun bütçesi ve gelirleri

MADDE 29- (1) Kurumun bütçesi, 5018 sayılı Kanunda belirlenen usul ve esaslara göre hazırlanır ve kabul edilir.

(2) Kurumun gelirleri şunlardır:

a) Genel bütçeden yapılacak hazine yardımları.

b) Kuruma ait taşınır ve taşınmazlardan elde edilen gelirler.

c) Alınan bağış ve yardımlar.

ç) Gelirlerinin değerlendirilmesinden elde edilen gelirler.

d) Diğer gelirler.

Değiştirilen ve eklenen hükümler

MADDE 30 - (1) (10/12/2003 tarihli ve 5018 sayılı Kanun ile ilgili olup yerine işlenmiştir.)

(2) ila (5) - (26/9/2004 tarihli ve 5237 sayılı Kanun ile ilgili olup yerine işlenmiştir.)

(6) (7/5/1987 tarihli ve 3359 sayılı Sağlık Hizmetleri Temel Kanunu ile ilgili olup yerine işlenmiştir.)

(7) (11/10/2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile ilgili olup yerine işlenmiştir.)

Yönetmelik

MADDE 31 - (1) Bu Kanunun uygulanmasına ilişkin yönetmelikler Kurum tarafından yürürlüğe konulur.

Geçiş hükümleri

GEÇİCİ MADDE 1 - (1) Bu Kanunun yayımı tarihinden itibaren altı ay içinde 21 inci maddede öngörülen usule göre Kurul üyeleri seçilir ve Başkanlık teşkilatı oluşturulur.

(2) Veri sorumluları, Kurul tarafından belirlenen ve ilan edilen süre içinde Veri Sorumluları Siciline kayıt yaptırmak zorundadır.

(3) Bu Kanunun yayımı tarihinden önce işlenmiş olan kişisel veriler, yayımı tarihinden itibaren iki yıl içinde bu Kanun hükümlerine uygun hâle getirilir. Bu Kanun hükümlerine aykırı olduğu tespit edilen kişisel veriler derhâl silinir, yok edilir veya anonim hâle getirilir. Ancak bu Kanunun yayımı tarihinden önce hukuka uygun olarak alınmış rızalar, bir yıl içinde aksine bir irade beyanında bulunulmaması hâlinde, bu Kanuna uygun kabul edilir.

(4) Bu Kanunda öngörülen yönetmelikler bu Kanunun yayımı tarihinden itibaren bir yıl içinde yürürlüğe konulur.

(5) Bu Kanunun yayımı tarihinden itibaren bir yıl içinde, kamu kurum ve kuruluşlarında bu Kanunun uygulanmasıyla ilgili koordinasyonu sağlamak üzere üst düzey bir yönetici belirlenerek Başkanlığa bildirilir.

(6) İlk seçilen Başkan, İkinci Başkan ve kura ile belirlenen iki üye altı yıl; diğer beş üye ise dört yıl görev yapar.

(7) Kuruma bütçe tahsis edilene kadar;

a) Kurumun giderleri Başbakanlık bütçesinden karşılanır.

b) Kurumun hizmetlerini yerine getirmesi amacıyla bina, araç, gereç, mefruşat ve donanım gibi gerekli tüm destek hizmetleri Başbakanlıkça sağlanır.

(8) Kurumun hizmet birimleri faaliyete geçinceye kadar sekretarya hizmetleri Başbakanlık tarafından yerine getirilir.

GEÇİCİ MADDE 2 - (Ek:28/11/2017-7061/120 md.)

(1) En az dört yıllık lisans öğrenimi veren siyasal bilgiler, iktisadi ve idari bilimler, iktisat, hukuk ve işletme fakültelerinden, mühendislik fakültelerinin elektronik, elektrik-elektronik, elektronik ve haberleşme, bilgisayar, bilişim sistemleri mühendisliği bölümlerinden ya da bunlara denkliği Yükseköğretim Kurulu tarafından kabul edilen yurt içi ve yurt dışındaki yükseköğretim kurumlarından mezun olanlardan; mesleğe özel yarışma sınavı ile girilen ve belirli süreli meslek içi eğitimden ve özel bir yeterlik sınavından sonra 657 sayılı Kanununun 36 ncı maddesinin “Ortak Hükümler” başlıklı bölümünün (A) fıkrasının (11) numaralı bendinde belirtilen unvanlara ilişkin kurumların merkez teşkilatlarına ait kadrolara atanmış ve bu kadrolarda aylıksız izin süreleri hariç en az iki yıl bulunmuş olanlar ile öğretim üyesi kadrolarında bulunanlar, Yabancı Dil Bilgisi Seviye Tespit Sınavından en az yetmiş puan almış olmak ve atama tarihi itibarıyla kırk yaşından gün almamış olmak kaydıyla, bu maddenin yürürlüğe girdiği tarihten itibaren bir yıl içinde Kişisel Verileri Koruma Uzmanı olarak atanabilirler. Bu şekilde atanacakların sayısı on beşi geçemez.

Yürürlük

MADDE 32 - (1) Bu Kanunun;

- a) 8 inci, 9 uncu, 11 inci, 13 üncü, 14 üncü, 15 inci, 16 ncı, 17 nci ve 18 inci maddeleri yayımı tarihinden altı ay sonra,
- b) Diğer maddeleri ise yayımı tarihinde, yürürlüğe girer.

Yürütme

MADDE 33 - (1) Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

(I) SAYILI CETVEL

KİŞİSEL VERİLERİ KORUMA KURUMU KADRO LİSTESİ

SINIF	UNVAN	DERECE	TOPLAM
GIH	Başkan Yardımcısı	1	1
GIH	Daire Başkanı	1	7
GIH	Hukuk Müşaviri	1	1
GIH	Hukuk Müşaviri	3	3
AH	Avukat	6	4
GIH	Kişisel Verileri Koruma Uzmanı	5	10
GIH	Kişisel Verileri Koruma Uzmanı	7	20
GIH	Kişisel Verileri Koruma Uzman Yardımcısı	9	60
GIH	Mali Hizmetler Uzmanı	6	2
GIH	Mali Hizmetler Uzman Yardımcısı	9	2
GIH	Memur	5	5
GIH	Memur	7	5
GIH	Memur	9	5
GIH	Memur	11	5
GIH	Memur	13	5
GIH	Bilgisayar İşletmeni	7	5
GIH	Veri Hazırlama ve Kontrol İşletmeni	6	5
GIH	Veri Hazırlama ve Kontrol İşletmeni	7	5
GIH	Veri Hazırlama ve Kontrol İşletmeni	8	5
GIH	Veri Hazırlama ve Kontrol İşletmeni	9	5
GIH	Veri Hazırlama ve Kontrol İşletmeni	10	5
GIH	Sekreter	5	3
GIH	Sekreter	8	7
GIH	Santral Memuru	9	1
GIH	Şoför	11	4
TH	Teknisyen	6	3
YH	Teknisyen Yardımcısı	9	2
YH	Hizmetli	11	10
	TOPLAM		195

6698 SAYILI KANUNA EK VE DEĞİŞİKLİK GETİREN MEVZUATIN VEYA ANAYASA MAHKEMESİ TARAFINDAN İPTAL EDİLEN HÜKÜMLERİN YÜRÜRLÜĞE GİRİŞ TARİHİNİ GÖSTERİR LİSTE

Değiştiren Kanunun/KHK'nin/ İptal Eden Anayasa Mahkemesi Kararının Numarası	6698 sayılı Kanunun değişen veya iptal edilen maddeleri	Yürürlüğe Giriş Tarihi
7061	27, GEÇİCİ MADDE 2	5/12/2017
KHK/703	19, 20, 21, 25	24/6/2018 tarihinde birlikte yapılan Türkiye Büyük Millet Meclisi ve Cumhurbaşkanlığı seçimleri sonucunda Cumhurbaşkanının andiçerek göreve başladığı tarihte (9/7/2018)

GEREKÇE

Bölüm İçeriği

- KVKK Genel Gerekçe
- KVKK Madde Gerekçeleri
- Anayasa Madde 20(3) Gerekçesi

KVKK Genel Gerekçe

TÜRKİYE BÜYÜK MİLLET MECLİSİ

YASAMA DÖNEMİ: 26

YASAMA YILI: 1

SIRA SAYISI: 117

Kişisel Verilerin Korunması Kanunu Tasarısı

(1/541) ve Adalet Komisyonu Raporu

T.C. Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü

18/1/2016 Sayı: 31853594-101-580-249

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

Adalet Bakanlığınca hazırlanan ve Başkanlığınıza arzı Bakanlar Kurulunca 4/1/2016 tarihinde kararlaştırılan “Kişisel Verilerin Korunması Kanunu Tasarısı” ile gerekçesi ilişikte gönderilmiştir.

Gereğini arz ederim.

Ahmet Davutoğlu

Başbakan

HAVALE EDİLDİĞİ KOMİSYONLAR (1/541)	
ESAS	Adalet Komisyonu
TALİ	Anayasa Komisyonu Avrupa Birliği Uyum Komisyonu İnsan Haklarını İnceleme Komisyonu Plan ve Bütçe Komisyonu

Kişisel veri, bireylerin kimliklerini belirli hale getirmeye elverişli her türlü bilgi olarak tanımlanabilir. Bu bağlamda kişinin kimlik, iletişim, sağlık ve mali bilgileri ile özel hayatına, dini inancına ve siyasi görüşüne ilişkin bilgiler, kişisel veri olarak nitelendirilmektedir.

Günümüzde bu veriler, gerek özel sektör ve gerekse kamu sektörü tarafından bilişim sistemleri üzerinden otomatik yollarla sıkça kullanılmaktadır. Bu bilgilerin kullanılması bireyler ile mal ve hizmet sunanlar bakımından bazı kolaylıklar veya avantajlar sağlasa da, bu durum söz konusu bilgilerin istismar edilme riskini de beraberinde getirmektedir. Bu verilerin yetkisiz kişiler tarafından elde edilmesi, kullanılması ve ifşa edilmesi gerek taraf olduğumuz sözleşmeler ve gerekse Anayasamızda koruma altına alınan temel hakların ihlali olarak karşımıza çıkmaktadır. Bu iki menfaat arasında makul bir dengenin oluşturulması gerekmektedir.

Kişisel verilerin işlenebilmesi hususunda özel bir kanun ve etkin bir denetim mekanizmasının bulunmaması toplumumuzda olumsuz bir algının oluşmasına sebebiyet vermektedir. Oluşan bu algının ortadan kaldırılması için kişisel verilerin belli şartlar dahilinde işlenmesine, muhafaza edilmesine ve kontrolüne ilişkin esasların belirlenmesi gerekmektedir.

Çağımızda insan haklarının korunması bilincinin gelişmesine paralel olarak, kişisel verilerin korunmasının da önemi her geçen gün artmaktadır. Bu nedenle günümüzde gelişmiş ülkelerde kişisel verilerin korunması alanında detaylı kanuni düzenlemelerin uygulanmakta olduğu görülmektedir.

Buna karşın ülkemizde, kişisel verilerin korunmasına ilişkin alanı bütüncül olarak düzenleyen bir kanun bulunmamakta, bu konuya ilişkin hükümler farklı kanunlarda yer almaktadır. Ayrıca ülkemizde kişisel verilerin işlenmesi sürecini kontrol edecek ve denetleyecek bir kurum da bulunmamaktadır.

Bunun bir sonucu olarak, halen kişisel veriler yeterli düzenleme ve denetime tabi olmaksızın, birçok kişi veya kurum tarafından kullanılabilen ve bu durum bazı hak ihlallerinin yaşanmasına sebep olabilmektedir.

Ülkemizde kişisel verilerin korunmasını sağlayacak bir kanunun yürürlüğe girmesini gerektiren değişik sebepler bulunmaktadır. Öncelikle, 5237 sayılı Türk Ceza Kanununun 135 ve devamı maddelerinde, kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa edilmesi fiilleri suç olarak düzenlenmiş ve yaptırıma bağlanmıştır. Bununla birlikte, kişisel verilerin işlenmesine yönelik özel bir kanunun bulunmaması sebebiyle, bu fiillerin ne zaman hukuka aykırı, ne zaman hukuka uygun olduğunun belirlenmesinde tereddütlerin yaşandığı görülmektedir.

Öte yandan 12 Eylül 2010 tarihinde yapılan halkoylaması sonucu kabul edilen 5982 sayılı Kanunla Anayasanın 20 nci maddesinde yapılan düzenlemeyle, kişisel verilerin korunması temel bir insan hakkı olarak güvence altına alınmış ve detayların kanunla düzenlenmesi öngörülmüştür.

Yine ülkemizle ilgili olarak devam etmekte olan Avrupa Birliği tam üyelik sürecinde, müzakere fasıllarından dördü, doğrudan kişisel verilerle ilgilidir. Bu fasıllarla ilgili sürecin ilerleyebilmesi için ülkemizde kişisel verilerin korunmasına ilişkin temel bir kanunun yürürlüğe girmesi gerekmektedir.

Avrupa Birliğinin Türkiye ile ilgili olarak hazırladığı ilerleme raporlarında Türkiye’de veri koruma alanındaki kanuni boşluğa işaret edilmektedir.

Ülkemizde kişisel verilerin korunmasına ilişkin kanuni bir düzenleme olmaması sebebiyle, polis birimleri arasında etkin bir işbirliğini hayata geçiren EUROPOL ile ülkemiz güvenlik birimleri arasında operasyonel işbirliği anlaşması yapılamamakta ve elektronik bilgi değişimi gerçekleştirilememektedir.

Benzer şekilde, sınır aşan suçlarla ilgili değişik ülkelerin yargı mercilerinin ortak operasyonlar yapabilmesi amacıyla oluşturulan EURO JUST ile çok sayıda sınır aşan suçun işlendiği geçiş güzergahında bulunan ülkemiz arasında bu suçlarla mücadeleye yönelik işbirliği yapılamamaktadır.

Sağlık kuruluşlarında hastalara ilişkin çok sayıda özel nitelikli veri tutulmakta olup, bu verilerin tutulmasına ilişkin kanuni dayanağın olmayışı, verilerin güvenliğinin sağlanmasına yönelik yeterli önlemlerin alınmaması ve yetkisiz kişilerce bu nitelikteki bilgilerin ifşa edilmesi, Avrupa İnsan Hakları Mahkemesince özel hayatın gizliliğine müdahale olarak nitelendirilmekte ve ihlal kararları verilebilmektedir.

Aynı şekilde, ülkemizde yaşayan yabancılar ile yurtdışında yaşayan Türk vatandaşları bakımından Dışişleri Bakanlığı askerlik, vatandaşlık, kimlik ve malvarlığı gibi konularda veri paylaşımında sorunlar yaşamaktadır.

Ayrıca, kişisel verilerin korunması konusunda kanun hazırlanması, ülkemizin Katılım Ortaklığı Belgesine cevap olarak hazırladığı 2003 Ulusal Programında taahhüt ettiği yükümlülüklerdendir.

Diğer taraftan, 64. Hükümet 2016 yılı Eylem Planında üç ay içerisinde gerçekleştirilecek reformlar arasında kişisel verilerin korunmasına ilişkin kanuni düzenlemelerin hayata geçirileceği yer almaktadır. Kişisel verilerin korunması konusu ekonomik alanla da yakından ilgilidir. Zira yabancı sermayenin ülkemizde yatırım yapması ve başka ülkelerdeki yatırımları ile ülkemizdeki yatırımlarını etkin bir şekilde yönetebilmesi için ihtiyaç duyduğu veri aktarımı, ülkemizde kanuni düzenleme olmaması sebebiyle gerçekleştirilememekte ve bu durum yabancı sermayenin ülkemizde yatırım

yapması bakımından caydırıcı bir etken olarak değerlendirilmektedir. Yine işadamlarımızın yabancı ülkelerdeki yatırımları ve ortaklıklarıyla ilgili ihtiyaç duydukları veri aktarımında sorunlar yaşanmaktadır.

Tüm bu açıklamalar, ülkemizde kişisel verilerin korunmasına ilişkin kanunun bir an önce yürürlüğe girmesini gerekli kılmaktadır.

Kişisel verilerin korunması konusu 1980'li yıllardan itibaren uluslararası belgelerde yer almaya başlamıştır. İlk olarak, ülkemizin de üyesi bulunduğu, İktisadi İşbirliği ve Kalkınma Teşkilatı (OECD) tarafından 23/9/1980 tarihinde "Kişisel Alanın ve Sınır Aşan Kişisel Bilgi Trafikinin Korunmasına İlişkin Rehber İlkeler" kabul edilmiştir.

Avrupa Konseyi tarafından, tüm üye ülkelerde kişisel verilerin aynı standartlarda korunması ve sınır ötesi veri akışı ilkelerinin belirlenmesi amacıyla hazırlanan 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi", 28 Ocak 1981 tarihinde imzaya açılmış ve ülkemiz tarafından da imzalanmıştır.

Avrupa Konseyi ayrıca, kişisel verilerin korunmasına yönelik, tıbbi veri bankaları, bilimsel araştırma ve istatistik, doğrudan pazarlama, sosyal güvenlik, sigorta, polis kayıtları, istihdam, elektronik ödeme, telekomünikasyon ve internet gibi çeşitli sektörlerde uygulanacak ilkeleri belirleyen tavsiye kararları da kabul etmiştir. Tasarının hazırlanması sırasında, söz konusu tavsiye kararları gözönüne alınmakla beraber, Tasarının "çerçeve tasarı" niteliği korunmuştur. Tüm sektörlerle ilgili düzenlemelere yer verilmesi halinde, Tasarının hacminin çok genişleyeceği düşünülerek, söz konusu tavsiye kararları Tasarıya alınmamıştır. Bu tavsiye kararlarında yer alan ilkelere, ilerleyen süreçte, değişik sektörlerle ilgili yapılacak düzenlemelerde yer verilebileceği değerlendirilmiştir.

Öte yandan, Avrupa Birliği, üye ülkelerin kişisel verilerin korunmasına ilişkin mevzuatı arasında uyum sağlamak üzere, 24/10/1995 tarihinde "Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafik Direktifi"ni (95/46/EC) yürürlüğe koymuştur. Bu Direktifle, üye ülkelerdeki bireylerin kişisel verilerinin üst düzeyde korunması ve kişisel verilerin Avrupa Birliği içerisinde özgür dolaşımını sağlayacak açık ve kalıcı bir düzenleme yapılması amaçlanmıştır.

Kişisel verilerin korunmasına yönelik uluslararası belgeler gözönüne alındığında; bu konuya ilişkin hazırlanacak kanunda, kişisel verilerin işleme şartlarının, bireylerin aydınlatılmasının, bu alanı denetleyecek ve düzenleyecek bir otoritenin oluşturulmasının, veri güvenliğine ilişkin gerekli tedbirlerin alınmasının temel ilkeler olarak kabul edildiği görülmektedir.

Uluslararası belgeler, mukayeseli hukuk uygulamaları ve ülkemiz ihtiyaçları gözönüne alınmak suretiyle hazırlanan Tasarıyla, kişisel verilerin çağdaş standartlarda işlenmesi ve koruma altına alınması amaçlanmaktadır.

KVKK Madde Gereklere

Madde 1

Maddeyle, Kanunun amacı belirlenmektedir. Amaç, kişisel verilerin işlenmesinin disiplin altına alınması ve Anayasada öngörülen başta özel hayatın gizliliği olmak üzere temel hak ve özgürlüklerin korunmasıdır. Son yıllarda önem kazanan kişinin mahremiyet hakkı ile bilgi güvenliği hakkının korunması da bu kapsamda değerlendirilmektedir. Ayrıca, kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların da düzenlenmesi Kanunun amaçları arasında yer almaktadır.

Madde 2

Maddeyle, Kanunun kapsamı belirlenmektedir. Buna göre Kanun, kişisel verileri işlenen gerçek kişiler ile bu verileri işleyen gerçek ve tüzel kişiler hakkında uygulanacaktır. Özel sektör ile kamu sektörü bakımından bir ayırım yapılmamış olup, öngörülen usul ve esasların her iki sektörde de uygulanması benimsenmektedir. Kişisel verilerin otomatik olan veya herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenmesi bakımından da herhangi bir fark öngörülmemektedir. Veri kayıt sistemi, Kanunun 3 üncü maddesinde tanımlandığı üzere kişisel verilere ulaşımı kolaylaştıracak şekilde, belirli bir kritere göre yapılandırılmış kayıt sistemini ifade etmektedir. Bir dosyalama sistemi olarak nitelenebilecek veri kayıt sistemi sadece dijital yahut elektronik ortamda oluşturulması gereken bir sistem değildir. Bu kapsamda, otomatik olmayan yollarla işlenen kişisel veriler bir veri kayıt sisteminin parçası değilse Kanun kapsamında değerlendirilmeyecektir. Ancak, bu hüküm anılan verilerin kişisel veri niteliğini etkilemeyeceğinden, bu tür verilere ilişkin hukuka aykırı eylemler 5237 sayılı Türk Ceza Kanunu uyarınca suç teşkil etmeye devam edecektir.

Madde 3

Maddeyle, Kanunda kullanılan bazı terimlerin tanımları yapılmıştır. Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Bu bağlamda sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgiler de kişisel veridir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin

belirlenmesini sađlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilme özellikleri nedeniyle kişisel verilerdir.

Kişisel verilerin işlenmesi kavramı geniş bir alanı kapsamaktadır. Buna göre kişisel verilerin işlenmesi, verilerin ilk defa elde edilmesinden başlayarak veriler üzerinde gerçekleştirilen tüm işlem türlerini ifade etmektedir.

Açık rıza, 95/46 EC sayılı Direktif dikkate alınarak tanımlanmaktadır. Buna göre, açık rıza ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı şeklinde anlaşılmalıdır.

Kişisel verilerin anonim hale getirilmesi, verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini ifade etmektedir. Bu kapsamda, elde kalan veri üzerinden bir izleme yapılarak başka verilerle eşleştirme ve destekleme sonrasında verinin kime ait olduğu anlaşılabilirse, bu verinin anonim hale getirildiği kabul edilemez.

Veri kayıt sistemi, kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade etmektedir. Bu sistemler elektronik yahut fiziki ortamda oluşturulabilir. Buna göre, veri kayıt sisteminde kişisel veriler, ad, soyad veya kimlik numarası üzerinden sınıflandırılabilir gibi, kredi borcunu ödemeyenlere ilişkin oluşturulacak sınıflandırma da bu kapsamda değerlendirilecektir.

Veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olanlardır. Bu kişiler, gerçek kişiler olabileceği gibi, kamu kurumları, şirketler, dernekler veya vakıflar gibi tüzel kişiler de olabilecektir.

Veri işleyen, veri sorumlusu adına verileri işleyen gerçek ve tüzel kişilerdir. Bu kişiler, kişisel verileri kendisine verilen talimatlar çerçevesinde işleyen çalışanlar olabileceği gibi, veri sorumlusunun hizmet satın almak suretiyle belirlediği ayrı bir gerçek veya tüzel kişi de olabilir. Herhangi bir gerçek veya tüzel kişi aynı zamanda hem veri sorumlusu, hem de veri işleyen olabilir. Örneğin, bir muhasebe şirketi kendi personeliyle ilgili tuttuğu verilere ilişkin olarak veri sorumlusu sayılırken, müşterisi olan şirketlere ilişkin tuttuğu veriler bakımından ise veri işleyen olarak kabul edilecektir.

Madde 4

Maddeyle, kişisel verilerin işlenmesine ilişkin genel ilkeler düzenlenmektedir. Buna göre kişisel veriler ancak Kanunda ve diğer Kanunlarda öngörülen usul ve esaslar çerçevesinde işlenebilecektir.

Maddenin ikinci fıkrasında kişisel verilerin işlenmesine ilişkin ilkeler sayılmaktadır. Bu ilkeler; hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmektir.

Belirli, açık ve meşru amaçlar için işlenme ilkesi, veri sorumlusunun, veri işleme amacını açık ve kesin olarak belirlemesini ve bu amacın meşru olmasını zorunlu kılmaktadır. Veri sorumluları, belirttikleri bu amaçlar dışında, başka amaçlarla veri işlemleri halinde, bu fiillerinden dolayı sorumlu olacaklardır. Amacın meşru olması, veri sorumlusunun işlediği verilerin, yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması anlamına gelmektedir. Örneğin, bir hazır giyim mağazasının, müşterilerinin kimlik ve iletişim bilgilerini işlemesi meşru amaç kapsamındayken, kan gruplarını işlemesi meşru amaç kapsamında değerlendirilemeyecektir.

Kişisel verilerin, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ilkesi, işlenen verilerin, belirlenen amaçların gerçekleştirilebilmesine elverişli olmasını, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirmektedir. Yine, sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik veri işlenebilmesi için, işlemeye ilk kez başlıyor gibi, 5 inci maddede düzenlenmiş olan kişisel verilerin işlenme şartlarından birinin gerçekleşmesi gerekecektir. Ayrıca işlenen veri, sadece amacın gerçekleştirilmesi için gerekli olanla sınırlı tutulacaktır.

Kişisel verilerin, ancak ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi zorunludur. Buna göre, veri sorumluları, ilgili mevzuatta verilerin saklanması için öngörülen bir süre varsa bu süreye uyacak; yoksa verileri, ancak işlendikleri amaç için gerekli olan süre kadar muhafaza edebilecektir. Bir verinin daha fazla saklanması için geçerli bir sebep olmaması durumunda, o veri silinecek veya anonim hale getirilecektir. Gelecekte kullanma ihtimalinin varlığına dayanarak veri saklanamayacaktır. Veri sorumlusu, Kanunun 16 ncı maddesi uyarınca Sicile kayıt için başvuru yaparken kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi bildirmek zorundadır.

Madde 5

Maddeyle, kişisel verilerin işlenme koşulları düzenlenmektedir.

Kural olarak kişisel verilerin ilgili kişinin açık rızası veya maddede sayılan istisnalar dışında işlenmesi yasaktır, 95/46 EC sayılı Avrupa Birliği Direktifine göre rıza, ilgili kişinin kendisiyle ilgili veri

işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanıdır.

Maddenin ikinci fıkrasıyla ilgili kişinin açık rızası olmasa dahi bazı hallerde kişisel verilerin işlenebilmesi öngörülmektedir.

Fıkranın (a) bendine göre ilgili kişinin açık rızası olmasa dahi kanunlarda açıkça öngörülen hallerde kişisel veri işlenebilecektir. Örneğin, kolluk tarafından bir suç soruşturması sebebiyle, 2559 sayılı Polis Vazife ve Salahiyet Kanununun 5 inci maddesi uyarınca şüphelilerin parmak izlerinin alınması; 5352 sayılı Adli Sicil Kanunu uyarınca Adalet Bakanlığının kişilerin ceza mahkûmiyetlerine ilişkin verilerini işlemesi gibi.

Fıkranın (b) bendine göre, rızanın açıklanamadığı ya da geçerli olmadığı hallerde, kişilerin hayat veya beden bütünlüğünün korunması için kişisel verilerin işlenmesi öngörülmektedir. Örneğin kişinin şuurunun yerinde olmadığı veya akıl hastası olması sebebiyle rızasının geçerli olmadığı bir durumda, hayat veya beden bütünlüğünün korunması amacıyla, tıbbi müdahale yapılması sırasında, kişisel verileri işlenebilecektir. Bu bağlamda kan grubu, geçirilen hastalıklar ve ameliyatlar, kullanılan ilaçlar gibi veriler, ilgili sağlık sistemi üzerinden işlenebilecektir. Yine hürriyeti tahdit edilen bir kişinin kurtarılması amacıyla, kendisinin veya şüphelinin taşımakta olduğu telefon, bilgisayar, kredi kartı, banka kartı veya diğer teknik bir araç üzerinden yerinin belirlenmesi için bu veriler işlenebilecektir.

Fıkranın (c) bendine göre, bir sözleşmenin kurulması veya ifasıyla ilgili olarak kişisel veri işlenebilecektir. Örneğin, yapılan bir sözleşme gereği paranın ödenmesi için alacaklı tarafın hesap numarası alınabilecektir. Yine bir bankayla kredi sözleşmesi yapılması sırasında bankanın, o kişiye ait maaş bordrosunu, tapu kayıtlarını, icra borcu olmadığına dair belgeyi edinmesi bu kapsamda değerlendirilecektir.

Fıkranın (ç) bendine göre, veri sorumlusu, hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olan verileri, ilgili kişinin rızası olmasa dahi işleyebilecektir. Örneğin bir şirketin çalışanına maaş ödeyebilmesi için, banka hesap numarası, evli olup olmadığına bakmakla yükümlü olduğu kişiler, eşinin çalışıp çalışmadığı, sosyal sigorta numarası gibi verileri işlemesi bu bendin verdiği yetkiye istinaden olacaktır.

Fıkranın (d) bendine göre, ilgili kişinin kendisi tarafından alenileştirilen bir başka ifadeyle herhangi bir şekilde kamuoyuna açıklanmış olan kişisel verileri işlenebilecektir. Çünkü ilgili kişi tarafından alenileştirilen ve böylelikle herkes tarafından bilinebilecek hale gelen bu tür verilerin işlenmesinde, korunması gereken hukuki yararın ortadan kalktığı kabul edilmektedir.

Fıkranın (e) bendine göre, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması durumunda kişisel veriler işlenebilecektir. Bu bağlamda, bir şirketin kendi çalışanı tarafından açılan bir davada ispat için bazı verileri kullanması veya kısıtlı bir kişinin haklarının korunması amacıyla vasinin veya kayyımın, kısıtlının mali bilgilerini tutması hukuka uygun sayılacaktır.

Fıkranın (f) bendine göre, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması durumunda da açık rıza şartı aranmaksızın kişisel veriler işlenebilecektir. Buna göre, örneğin bir şirket sahibi, çalışanlarının temel hak ve özgürlüklerine zarar vermemek kaydıyla, onların terfileri, maaş zamları yahut sosyal haklarının düzenlenmesinde ya da işletmenin yeniden yapılandırılması sürecinde görev ve rol dağıtımında esas alınmak üzere çalışanların kişisel verilerini işleyebilecektir. Burada, işletmenin yeniden yapılandırılması ya da ehliyetli ve liyakatli çalışanların terfi almaları, veri sorumlusu statüsündeki şirket sahibinin meşru menfaati cümlesindedir. Kişisel verilerin korunmasına ilişkin temel ilkelere uyulması ve veri sorumlusu ile ilgili kişinin menfaat dengesinin gözetilmesi gerekmektedir.

Madde 6

Maddeyle, kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, biyometrik verisi veya haklarında verilen ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verilerinin, özel nitelikli kişisel veri olduğu belirtilmektedir. Bu verilerin, başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden olabilecek nitelikte veriler olmaları dikkate alınmakta, bu sebeple bu tür veriler özel nitelikli (hassas) veri olarak kabul edilmektedir.

Kurul tarafından belirlenen yeterli önlem alınmaksızın özel nitelikli verilerin işlenememesi öngörülmekte, ayrıca kural olarak bu tür verilerin ilgili kişinin açık rızası olmaksızın da işlenememesi hükme bağlanmaktadır.

Maddenin dördüncü fıkrasında tahdidi olarak sayılan şartların varlığı halinde, yeterli önlem alınması şartı baki kalmak kaydıyla ilgili kişinin açık rızası aranmaksızın özel nitelikli kişisel verilerin işlenmesine imkân tanınmaktadır.

Dördüncü fıkranın (a) bendine göre, ilgili kişinin rızası olmasa bile, kanunlarda açıkça öngörülen hallerde özel nitelikli kişisel veriler işlenebilecektir. Örneğin, askerlik yapacak kişilerin bazı özel

sağlık bilgilerinin ilgili kanun hükümleri uyarınca işlenmesi, yine hastanelerin, eczanelerin ya da Sosyal Güvenlik Kurumunun hastalarla ilgili veri işleme bu kapsamda değerlendirilecektir.

Fıkranın (b) bendinde, siyasi parti, vakıf, dernek veya sendika gibi kâr amacı gütmeyen kuruluş ya da oluşumlar tarafından, özel nitelikli kişisel verilerden bazılarının işlenebilmesi düzenlenmektedir. Buna göre, bu kuruluş ve oluşumlar, kendi üye ve mensuplarının özel nitelikli verilerini, kuruluş amaçlarına ve tabi oldukları mevzuata uygun, faaliyet alanlarıyla sınırlı ve üçüncü kişilere açıklanmamak kaydıyla işleyebileceklerdir. Örneğin, bir siyasi partinin veya sendikanın üyelerine ilişkin kimlik ve iletişim bilgilerini, fıkrada belirtilen şartlarla tutması, bu bent kapsamında değerlendirilecektir. Bu kuruluşlar, sadece kendi faaliyet alanlarıyla sınırlı olarak özel nitelikli veri işleyebileceklerdir. Örneğin, bir sendika, kendi faaliyet alanına ve amacına ilişkin olarak sadece sendika üyeliğiyle ilgili verileri işleyebilecektir. Buna karşın üyelerin sağlık veya din ya da mezhebine yönelik kişisel verileri, faaliyet alanıyla ve amacıyla ilgisi olmaması sebebiyle işleyemeyecektir.

Fıkranın (c) bendine göre, ilgili kişinin kendisi tarafından kamuoyuna açıklanmış olan özel nitelikli kişisel verileri işlenebilecektir. Zira ilgili kişi tarafından alenileştirilen ve böylelikle herkes tarafından bilinen bu tür verilerin işlenmesinde, korunması gereken hukuki yararın ortadan kalktığı kabul edilmektedir.

Fıkranın (ç) bendinde, özel niteliği olan kişisel verilerin, bir hakkın tesisi, kullanılması veya korunması için işlenmesinin zorunlu olması hali düzenlenmektedir. Örneğin, bir işverenin, engelli çalıştırma zorunluluğu kapsamında, işyerinde, bu statüde çalıştırdığı kişilere ilişkin rapor ve belgeleri işleme bu kapsamda değerlendirilecektir. Yine engelli bir kişinin özel tüketim vergisinden muaf özel donanımlı araç almak hakkından yararlanabilmesi için, engelliliğine ilişkin sağlık raporlarının vergi dairesi tarafından edinilmesi ve işlenmesi de bu bent kapsamında değerlendirilecektir.

Fıkranın (d) bendiyle, özel nitelikli verilerin; kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmesi düzenlenmektedir. Bu bağlamda, Sağlık Bakanlığı ile her türlü sağlık kuruluşunun ve Sosyal Güvenlik Kurumunun bu bentte yazılı amaçlarla tuttukları veriler ve kayıtlar bu kapsamda değerlendirilecektir.

Madde 7

Maddeyle, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi düzenlenmektedir. Buna göre, hukuka uygun olarak işlenmiş olup da işlenmesini gerektiren sebepler ortadan kalkmışsa,

söz konusu veriler resen veya ilgili kişinin talebi üzerine silinecek, yok edilecek veya anonim hale getirilecektir. Kişisel verilerin silinmesiyle, bu verilerin tekrar hiçbir şekilde kullanılmayacak ve geri getirilemeyecek şekilde imhası amaçlanmaktadır. Buna göre veriler, kayıtlı oldukları evrak, dosya, CD, disket, hard disk gibi araçlardan geri dönüştürülemez şekilde silinecektir. Verilerin yok edilmesi ise, bilgilerin tekrar geri getirilemeyecek ve kullanılmayacak şekilde, verilerin kaydedildiği evrak, dosya, CD, disket, hard disk gibi veri saklamaya elverişli materyallerin imha edilmesini ifade etmektedir. Verilerin anonim hale getirilmesiyle, kişisel verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi kastedilmektedir.

Maddenin ikinci fıkrasıyla, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin diğer kanunlarda yer alan hükümlerin saklı tutulması öngörülmektedir. Bu kapsamda, örneğin Adli Sicil Kanununda verilerin silinmesini veya yok edilmesini düzenleyen hükümler Kanuna göre öncelikli olarak uygulanacaktır. Maddenin son fıkrasında, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasların yönetmelikte düzenlenmesi hüküm altına alınmaktadır.

Madde 8

Maddeyle kişisel verilerin, üçüncü kişilere aktarılması düzenlenmektedir. Kanunun hem 5 inci maddesinde düzenlenen kişisel veriler hem de 6 ncı maddesinde düzenlenen özel nitelikli (hassas) kişisel veriler madde kapsamındadır. Kanunun 9 uncu maddesinde kişisel verilerin yurtdışına aktarılması düzenlendiğinden bu maddede belirtilen üçüncü kişiler yurtiçindeki kişilerdir.

Maddenin birinci fıkrasında, kişisel verilerin ilgilinin açık rızası olmaksızın üçüncü kişilere aktarılamayacağına ilişkin ilke hükme bağlanmaktadır. Kanunun 3 üncü maddesinin birinci fıkrasının (d) bendi uyarınca verilerin aktarılması veya devralınması kişisel verilerin işlenmesi olarak tanımlandığından; verileri alanların, kişisel verilerin işlenmesi için Kanunun 5 inci ve 6 ncı maddelerinde öngörülen şartları yerine getirmeleri ve bu kapsamda özel nitelikte veriler yönünden yeterli önlem almaları da gerekmektedir.

Maddenin ikinci fıkrasında verilerin, ilgilinin açık rızası olmaksızın üçüncü kişilere aktarılmasına ilişkin düzenleme yapılmaktadır. Bu düzenleme yapılırken 5 inci maddenin ikinci fıkrası uyarınca ilgili kişinin açık rızası olmaksızın işlenmesine izin veren şartlar aranmakta ve bu şartların birinin varlığı halinde, kişisel verilerin üçüncü kişilere aktarılabilmesine imkân tanınmaktadır.

Özel nitelikli kişisel veriler yönünden ise yeterli önlemler alınmak kaydıyla, 6 ncı maddenin (b) bendi hariç olmak üzere dördüncü fıkrasında belirtilen verilerin ilgili kişinin açık rızası olmaksızın işlenmesine izin veren şartlar esas alınmaktadır. Bir başka ifadeyle, 6 ncı maddenin dördüncü fıkrasının (b) bendi hariç olmak üzere ilgili kişinin açık rızası aranmaksızın işlenebilen kişisel verilerin, 6 ncı maddenin ikinci fıkrasında öngörülen yeterli önlemler alınmak kaydıyla ilgili kişinin rızası aranmaksızın üçüncü kişilere aktarılmasına izin verilmektedir.

Maddenin üçüncü fıkrasında, kişisel verilerin üçüncü kişilere aktarılmasına ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu hüküm altına alınmaktadır.

Madde 9

Maddeyle kişisel verilerin, yurtdışına aktarılması düzenlenmektedir. Kanunun hem 5 inci maddesinde düzenlenen kişisel veriler hem de 6 ncı maddesinde düzenlenen özel nitelikli (hassas) kişisel veriler madde kapsamındadır.

Maddenin birinci fıkrasında, kişisel verilerin ilgilinin açık rızası olmaksızın yurtdışına aktarılamayacağına ilişkin ilke hükme bağlanmaktadır.

Maddenin ikinci fıkrasında kişisel verilerin, ilgilinin açık rızası olmaksızın yurtdışına aktarılmasına ilişkin düzenleme yapılmaktadır. Bu düzenleme yapılırken 5 inci maddenin ikinci fıkrası kapsamındaki kişisel veriler ile 6 ncı maddenin dördüncü fıkrasının (a), (c), (ç) ve (d) bentlerinde belirtilen özel nitelikli kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenmesine izin veren şartlar esas alınmakta ve bu şartlardan birinin varlığı halinde, kişisel verinin aktarılacağı yabancı ülkede, yeterli korumanın bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurtdışına aktarılmasına imkân tanınmaktadır. Şayet ilgili yabancı ülkede yeterli koruma bulunmuyorsa, Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın kişisel verilerin yurtdışına aktarılmasına imkân verilmektedir.

Maddenin üçüncü fıkrasına göre yabancı ülkelerde yeterli koruma bulunup bulunmadığı Kurulca belirlenerek ilan edilecektir.

Maddenin dördüncü fıkrasıyla, Kurulun, yabancı ülkede yeterli koruma bulunup bulunmadığına karar ve verilerin yurtdışına aktarılmasına izin verirken hangi kriterleri dikkate alacağı düzenlenmektedir. Buna göre Kurul, maddede sayılan hususları değerlendirecek, ihtiyaç duyması halinde ilgili kurum ve kuruluşların da görüşünü almak suretiyle bir karar verecektir.

Maddenin beşinci fıkrasında, kişisel verilerin yurtdışına aktarılmasına ilişkin ilgili kanunlarda yer alan hükümlerin saklı olduğu hüküm altına alınmaktadır. Buna göre, örneğin 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanunun, uluslararası bilgi değişimi konusunda Malî Suçları Araştırma Kurulu Başkanına yetki veren 12 nci ve 19 uncu maddeleri öncelikli olarak uygulanacaktır.

Madde 10

Maddeyle, 95/46/EC sayılı Direktife uygun olarak, veri sorumlusunun aydınlatma yükümlülüğü düzenlenmektedir. Veri sorumlusu veya yetkilendirdiği kişi, aydınlatma yükümlülüğü kapsamında; veri sorumlusunun ve varsa temsilcisinin kimliği, veri işleme amacı, verilerin kimlere ve hangi amaçla aktarılacağı, veri toplamanın yöntemi ve hukuki sebebi ile 11 inci maddede sayılan diğer hakları konusunda, ilgili kişiyi bilgilendirecektir.

Madde 11

Maddeyle, kişisel verileri işlenen kişinin hakları düzenlenmektedir. Buna göre, kişi kendisiyle ilgili kişisel veri işlenip işlenmediğini öğrenme, işlenmişse buna ilişkin bilgileri talep etme, verilerin işleme amacı ile bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurtiçinde veya yurtdışında verilerin aktarıldığı üçüncü kişileri bilme, 7 nci maddede öngörülen koşullar çerçevesinde kişisel verilerin silinmesini, yok edilmesini veya verinin muhtevasının eksik ya da gerçeğe aykırı olması hallerinde bunların düzeltilmesini isteme hakkına sahiptir.

Yine ilgili kişi, talebi doğrultusunda yapılan düzeltme, silme ve yok etme işlemlerinin, verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, verilerinin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde, zararın giderilmesini talep etme hakkına da sahiptir.

Maddenin birinci fıkrasının (g) bendinde, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle aleyhe bir sonucun ortaya çıkmasına itiraz hakkı düzenlenmektedir. Örneğin, bir çalışanın performansının, onun tarafından yapılan işlerin, otomatik bir sisteme işlenip analiz edilerek, analiz sonucuna göre değerlendirilmesine, çalışanın itiraz edebilmesi bu kapsamda değerlendirilecektir.

Madde 12

Maddeyle, veri sorumlusunun, veri güvenliğinin sağlanmasına ilişkin yükümlülükleri düzenlenmektedir. Buna göre, veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini ve verilere hukuka aykırı olarak erişilmesini önlemek, ayrıca verilerin muhafazasını sağlamak için

uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almakla yükümlü tutulmaktadır.

İkinci fıkrada, veri sorumlusunun, verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi durumunda, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumlu olacağı düzenlenmektedir. Buna göre, veri sorumlusu, örneğin şirketine ilişkin kayıtları bir muhasebe şirketine tutturuyorsa, verilerin işlenmesine ilişkin birinci fıkrada belirtilen tedbirlerin alınması hususunda muhasebe şirketiyle birlikte müştereken sorumlu olacaktır.

Üçüncü fıkrada, veri sorumlusunun, kendi kurum veya kuruluşunda, Kanun hükümlerinin uygulanmasını sağlama ve kişisel verilerin Kanunda öngörülen usul ve esaslara uygun olarak işlenmesi amacıyla gerekli denetimleri yapma veya yaptırma yükümlülüğü düzenlenmektedir.

Dördüncü fıkrada, veri sorumluları ile veri işleyenlerin sır saklama yükümlülüğü düzenlenmektedir. Buna göre, veri sorumluları ile veri işleyenler, öğrendikleri kişisel verileri, Kanuna aykırı olarak başkalarına açıklayamayacak veya şahsi çıkarları için kullanamayacaklardır. Bu yükümlülük görevden ayrılmalarından sonra da devam edecektir.

Beşinci fıkrada, işlenen verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri sorumlusunun bu durumu en kısa sürede ilgisine ve Kurula bildireceği düzenlenmektedir. Kurul, gerekmesi halinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yolla ilan edebilecektir.

Madde 13

Maddeyle, veri sorumlusuna başvuru yolu düzenlenmektedir. Buna göre, ilgili kişilerin, Kanunun uygulanmasıyla ilgili taleplerini, öncelikle veri sorumlusuna iletmeleri zorunludur. İlgili kişilerin, taleplerini veri sorumlusuna yazılı olarak ya da uygulamada oluşacak ihtiyaca göre Kurulun belirleyeceği diğer yöntemlerle iletebilmelerine imkân sağlanmaktadır.

Bu talebi alan veri sorumlusunun, ücretsiz olarak veya işlemin ayrıca bir maliyeti gerektirmesi halinde, Kurul tarafından belirlenen tarifeye göre alacağı ücret mukabilinde en kısa sürede ve en geç otuz gün içinde talebi incelemesi; kabul veya gerekçesini açıklayarak reddetmesi, ayrıca cevabını ilgili kişiye bildirmesi öngörülmektedir. Veri sorumlusunun gerçek kişi veya özel hukuk tüzel kişisi olabileceği ve bunların 7201 sayılı Tebligat Kanununa tabi olmamaları dikkate alınarak, veri sorumlusunun cevabını ilgili kişiye "bildirmesi" hükme bağlanmaktadır. Bu bildirim, bir ispat sorunu olup gerektiğinde yargı mercilerince ele alınacaktır. 7201 sayılı Kanuna tabi kurum ve kuruluşların bu bildirimleri anılan Kanun hükümleri uyarınca resmi tebligat yoluyla yapacakları da açıktır.

Veri sorumlusunun talebi kabul etmesi halinde, gereğini yerine getirmesi; şayet ilgili kişinin, Kanunun uygulanmasıyla ilgili talebine konu hususta veri sorumlusu hatalıysa, alınan ücretin ilgiliye iade edilmesi hükme bağlanmaktadır.

Madde 14

Maddeyle, şikâyet yolu düzenlenmektedir. Buna göre, 13 üncü madde uyarınca yapmış olduğu başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hallerinde; ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her halde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyette bulunabilir.

İkinci fıkrada, 13 üncü maddede öngörülen başvuru müessesesinin, zorunlu bir başvuru yolu olduğu ve bu yol tüketilmeden şikâyet yoluna gidilemeyeceği hükme bağlanmaktadır. Böylece uyuşmazlıkların belirli bir kısmının veri sorumluları tarafından giderilmesi ve bu suretle Kurulun yoğun bir iş yüküyle karşı karşıya kalmasının önlenmesi amaçlanmaktadır. Başvuru yoluna gitmenin zorunlu, şikâyet yoluna gitmenin ise ihtiyari olması sebebiyle, başvurusu zımnen veya açıkça reddedilen ilgili kişinin bir yandan Kurula şikâyette bulunabilmesi, diğer yandan doğrudan adli veya idari yargı yoluna gidebilmesi mümkün olacaktır. Ancak, ilgililerin masrafsız ve daha hızlı sonuç alınması mümkün olan şikâyet yolunu tercih edecekleri değerlendirilmektedir.

Üçüncü fıkrada, kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklı tutulmaktadır. Veri sorumlusunun hukuki statüsüne göre ilgililer adli ya da idari yargıda dava açabileceklerdir.

Madde 15

Maddeyle, Kurul tarafından yapılacak incelemenin usul ve esasları düzenlenmektedir. Buna göre, Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi halinde resen, görev alanına giren konularda gerekli incelemeyi yapabilecektir. Bu inceleme şikâyete ya da resen öğrenilen şikâyet konusuna münhasır olacaktır. Kurulun resen genel inceleme yetki ve görevi bulunmamaktadır. Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesinde belirtilen şartları taşımayan ihbar ve şikâyetler incelemeye alınmayacaktır. Veri sorumluları, Devlet sırrı niteliğindeki bilgi ve belgeler hariç, talep edilen bilgi ve belgeleri, Kurula onbeş gün içinde göndermek veya gerektiğinde yerinde inceleme yapılmasına imkân sağlamak zorundadır.

Kurulun, şikâyet üzerine yapacağı inceleme sonunda cevap vermesi öngörülmekte, şikâyet tarihinden itibaren altmış gün içinde cevap verilmezse talebin reddedilmiş sayılacağı hükme

bağlanmaktadır. Buna göre, şikâyet tarihinden itibaren altmış günlük sürenin geçmesiyle idari yargıda dava açma süresi başlayacaktır.

Kurulun, şikâyet üzerine yapacağı inceleme için altmış günlük süre öngörülmüş ise de resen yapacağı incelemeler yönünden herhangi bir süre öngörülmemektedir.

Kurul, şikâyet üzerine veya resen yapılacak inceleme sonucunda, Kanun hükümlerinin ihlal edildiği kanaatine varırsa, tespit ettiği hukuka aykırılıkların ilgili veri sorumlusu tarafından giderilmesine karar verir ve kararı ilgililere tebliğ eder. Bu karar, tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilecektir.

Yine şikâyet üzerine veya resen yapılan inceleme sonucunda, kanuna aykırı uygulamanın yaygın olduğunun Kurul tarafından tespit edilmesi üzerine ilgili kurum ve kuruluşların görüşü de alınmak suretiyle bu konuda ilke kararı alınır ve bu karar yayımlanır.

Ayrıca Kurula, telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık şartlarının birlikte gerçekleşmesi halinde, nihai karardan önce veri işlenmesinin veya verinin yurtdışına aktarılmasının durdurulmasına karar verme yetkisi verilmektedir.

İlgililerin, Kurulca verilen kararlara karşı idare mahkemelerinde dava açabilmeleri mümkündür.

Madde 16

Maddeyle, veri sorumlularının kaydedileceği Veri Sorumluları Sicili düzenlenmektedir. Buna göre Veri Sorumluları Sicili, Kişisel Verileri Koruma Kurulunun gözetiminde Başkanlık tarafından kamuya açık olarak tutulacaktır. Veri sorumluları veri işlemeye başlamadan önce bu Sicile kaydolacaklardır. Ancak işlenen verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler gözönüne alınmak suretiyle, Kurul tarafından, Sicile kayıt zorunluluğuna istisna getirilebilecektir.

Maddenin üçüncü fıkrasında Sicile kayıt başvurusunda bildirilmesi gereken hususlar düzenlenmektedir. Bu kapsamda, örneğin veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri, kişisel verilerin hangi amaçla işleneceği, kişisel verilerin aktarılabilmesi için alıcı veya alıcı grupları, veri güvenliğine ilişkin alınan tedbirler, kişisel verilerin işlendikleri amaç için gerekli olan azami süre gibi hususlar Sicile kayıt başvurusunda bildirilmelidir. Ayrıca, üçüncü fıkra uyarınca bildirilmesi gerekli bilgilerde meydana gelen değişiklikler de derhal Başkanlığa bildirilecektir. Veri Sorumluları Siciline ilişkin diğer usul ve esaslar yönetmelikle düzenlenecektir.

Madde 17

Maddeyle, kişisel verilere ilişkin suçlar ve cezai yaptırımlar 5237 sayılı Türk Ceza Kanununun ilgili hükümlerine atıf yapılmak suretiyle düzenlenmektedir. Kişisel verileri silmeyen veya anonim hale getirmeyenlerin ise Türk Ceza Kanununun 138 inci maddesi hükmü uyarınca cezalandırılmaları öngörülmektedir.

Madde 18

Maddeyle, Kanunda öngörülen yükümlülüklerle aykırı davranılması halinde uygulanacak idari yaptırımlar düzenlenmektedir. Bu kapsamda aydınlatma ve veri güvenliğini sağlama, Kurul kararlarını yerine getirme ve Sicile kayıt ve bildirim yükümlülüklerine aykırı davranılması kabahat olarak öngörülmekte ve idari para cezası yaptırımına bağlanmaktadır. İdari yaptırımlara Kurul tarafından karar verilecektir. Verilen yaptırım kararlarına karşı idari yargı yolu açıktır.

Maddede kabahatler karşılığında öngörülen idari para cezalarının alt ve üst sınırları arasındaki makas bilinçli olarak geniş tutulmuştur. Kurul karar verirken kabahatler hususunda genel kanun niteliğinde olan 30/3/2005 tarihli ve 5326 sayılı Kabahatler Kanununun 17 nci maddesinin ikinci fıkrasında belirtildiği üzere kabahatin haksızlık içeriği ile failin kusuru ve ekonomik durumunu dikkate alacaktır. Bu şekilde düzenleme yapılmak suretiyle, söz konusu kabahatlerin çok farklı ekonomik güce sahip gerçek veya tüzel kişiler hakkında uygulanacak olması nedeniyle yaptırım uygulanmasında hakkaniyeti sağlamak amaçlanmıştır. Buna göre örneğin, küçük bir şehirde faaliyet gösteren bir aile şirketiyle ülke çapında faaliyet gösteren bir holdingin Kanun hükümlerini ihlal etmesi durumunda belirlenecek idari para cezalarının miktarı söz konusu şirketlerin ekonomik durumlarına göre farklı olacaktır.

İdari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanacaktır. Maddede kabahat olarak düzenlenen eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi halinde. Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılacaktır.

Kanunda kabahatlerle ilgili hüküm bulunmayan hallerde genel kanun niteliğindeki 5326 sayılı Kabahatler Kanunu hükümlerinin uygulanacağı açıktır.

Madde 19

Maddeyle, Kanunla verilen görevleri yerine getirmek üzere, idari ve mali özerkliğe sahip ve kamu tüzel kişiliğini haiz Kişisel Verileri Koruma Kurumunun kuruluşu düzenlenmektedir. Avrupa

Konseyinin 108 sayılı Sözleşmesi ve Avrupa Birliğinin 95/46/EC sayılı Direktifi, kişisel verilerin işlenmesine ilişkin ilkelerin uygulanmasını izlemek ve yönlendirmek üzere fonksiyonel olarak bağımsız bir şekilde görev yapacak otoritelerin oluşturulmasını öngörmektedir. Avrupa Birliği üyesi tüm ülkelerde veri koruma kurulları görevlerinde bağımsız otoriteler şeklinde yapılandırılmıştır. Sayılan uluslararası belgeler ve mukayeseli hukuk uygulamaları gözönüne alınmak suretiyle, Kişisel Verileri Koruma Kurumu kurulmuştur. Kurumun Başbakanlıkla ilişkili olduğu hüküm altına alınmaktadır.

Madde 20

Maddeyle, Kurumun görevleri belirlenmektedir. Buna göre Kuruma, görev alanı itibarıyla, başlıca ulusal ve uluslararası düzlemde uygulama ve mevzuattaki gelişmeleri takip ederek araştırma ve inceleme faaliyetlerinde bulunma ve ulusal ve uluslararası; kurum ve kuruluşlarla işbirliği yapma ve ihtiyaç duyulan hususlarda önerilerde bulunma görevleri verilmektedir.

Ayrıca, Kurum faaliyetleri hakkında hazırlanan yıllık faaliyet raporlarının Cumhurbaşkanlığına, Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonuna ve Başbakanlığa sunulması, Kurumun şeffaflığının ve hesap verebilirliğinin sağlanmasına yardımcı olacaktır. Kurumun etkin ve verimli bir şekilde çalışabilmesi için hizmet alımı yapabilmesi de hüküm altına alınmaktadır.

Madde 21

Maddeyle, Kişisel Verileri Koruma Kurulu düzenlenmekte ve Kurulun, Kurumun karar organı olduğu belirtilmektedir. Avrupa Konseyinin 108 sayılı Sözleşmesi ve Avrupa Birliğinin 95/46/EC sayılı Direktifine uygun şekilde Kurul bağımsız olarak kurgulanmaktadır. Kurulun, Kanunla ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getireceği ve kullanacağı, görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişinin Kurula emir ve talimat veremeyeceği hüküm altına alınmaktadır. Bu hüküm, Kurumun görevini, bağımsız bir şekilde yerine getirebilmesi bakımından önem arz etmektedir.

Ayrıca, Kurulun yedi üyeden oluşması öngörülmekte ve üyelerin nitelikleri, seçimi ve görev süreleri düzenlenmektedir. Üyelerin Cumhurbaşkanınca ve Bakanlar Kurulunca seçilmesi Kurulun demokratik meşruiyetini güçlendirmektedir. Öte yandan, üyelerin seçiminde, özel sektör ile kamu sektöründe on yıl çalışmış olma, dört yıllık lisans mezunu olma ve Devlet memuru olmaya ilişkin genel şartları taşıma dışında özel başka bir şart aranmayarak üyelerin çok geniş bir alandan seçilmesi imkânı getirilmektedir. Maddede ayrıca, Kurul üyelerinin ilk toplantının başında yemin etmeleri

düzenlenmekte ve Kurul Başkanı ile İkinci Başkanın, üyeler arasından Bakanlar Kurulunca seçilmesi hükme bağlanmaktadır.

Madde ile ayrıca, üyelerin görevleri sebebiyle işledikleri suçlar bakımından soruşturma usulü düzenlenmektedir. Buna göre üyeler hakkında görevleri sebebiyle işledikleri suçlar bakımından soruşturma yapılabilmesi Başbakanın iznine bağlanmakta ve Kurul üyelerinin görev süreleri dolmadan herhangi bir şekilde görevlerine son verilemeyeceği öngörülmek suretiyle üyelerin, dolayısıyla Kurulun bağımsızlığı teminat altına alınmaktadır.

Madde 22

Maddeyle Kurulun görev ve yetkileri düzenlenmektedir. Buna göre, kişisel verilerin temel hak ve özgürlükleri koruyacak şekilde işlenmesi, kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikâyetlerinin karara bağlanması, Veri Sorumluları Sicilinin tutulmasının sağlanması, kişisel verilerin işlenmesi konusunda gerekli düzenleyici işlemlerin yapılması, kişisel verilerin Kanuna uygun olarak işlenip işlenmediğinin incelenmesi, idari yaptırımların uygulanması, stratejik planın ve bütçenin kabul edilmesi gibi görevler Kurulun görevleri arasında sayılmaktadır. Kurul, özel nitelikli kişisel verilerin yeterli önlem alınmaksızın işlenemeyeceğine ilişkin Kanunun 6 ncı maddesinde düzenlenen hüküm uyarınca yeterli önlemin ne olduğunu verinin niteliği ve sektörün özelliğine göre belirleyecektir.

Ayrıca, Başkanlık tarafından hazırlanan Kurumun performansı, mali durumu, yıllık faaliyetleri ve diğer özel rapor taslakları Kurul tarafından onaylanacak, Kurumun ihtiyaç duyduğu taşınmazların alım ve satımı ile kiralanması konularındaki önerileri karara bağlayacaktır.

Madde 23

Maddeyle Kurulun çalışma esasları düzenlenmektedir. Bu kapsamda, Kurulun toplantı ve karar yeter sayısı, Kurul üyelerinin kendilerini ve yakınlarını ilgilendiren konularda yasaklılıkları ve sır saklama yükümlülükleri düzenlenmektedir. Kurulun çalışma usul ve esasları ile kararların yazımı ve diğer hususlar yönetmelikle düzenlenecektir.

Madde 24

Maddeyle Kurum Başkanının görevleri düzenlenmektedir. Kurumun üst yöneticisi ve Kurulun da Başkanı olan Kurum Başkanının, Kurumu yönetmek ve temsil etmek, stratejik planın uygulanmasını sağlamak, Kurumun ve hizmet birimlerinin uyumlu, verimli, disiplinli ve düzenli bir biçimde çalışmasını temin etmek yanında, Kurul toplantılarının gündemini belirleyerek toplantılara başkanlık etmek, Kurul kararlarının gereğinin yerine getirilmesini takip etmek ve Kurumun mali tabloları ile

bütçesini hazırlamak başlıca görevleri arasındadır. Ayrıca, Kurum Başkanının yokluğunda Başkana, İkinci Başkanın vekalet edeceği öngörülmektedir.

Madde 25

Maddeyle Kişisel Verileri Koruma Kurumu Başkanlığının oluşumu ve görevleri düzenlenmektedir. Başkanlık, Kurumun ve Kurulun idari ve mali işleri ile sekreteryaya hizmetlerini yerine getirecektir. Başkanlık; Başkan Yardımcısı ve daire başkanlıkları şeklinde teşkilatlanan hizmet birimlerinden oluşmaktadır. Maddeyle, Başkan Yardımcısı ve Daire Başkanlarının nitelikleri ve atanma usulü ile Başkanlığın görevleri ayrıntıları olarak düzenlenmektedir. Hizmet birimleri ile bu birimlerin çalışma usul ve esasları Bakanlar Kurulu kararı ile yürürlüğe konulan yönetmelikle düzenlenecektir.

Madde 26

Kurum görevlerinin daha etkin bir şekilde yerine getirilebilmesi için, bu görevlerin, konusunda uzmanlaşmış kişiler tarafından yürütülmesi şarttır. Bu kapsamda Kurumda Kişisel Verileri Koruma Uzmanı ve Kişisel Verileri Koruma Uzman Yardımcısı çalıştırılacaktır. Maddeyle, Kişisel Verileri Koruma Uzman Yardımcısı kadrolarına atanmak için gereken şartlar bakımından 657 sayılı Kanunun ek 41 inci maddesine atıf yapılmaktadır.

Madde 27

Maddeyle, Kurul Başkan ve üyeleri ile Kurum personelinin mali ve sosyal hakları düzenlenmektedir. Bununla birlikte başka kurum ve kuruluşlarda çalışanlardan uzmanlığına ihtiyaç duyulanların Kurumda görevlendirilmesine ilişkin düzenleme hüküm altına alınmaktadır.

Maddeyle ayrıca, Kurumda istihdam edilecek personele ilişkin kadro unvan ve sayıları da belirlenmektedir.

Madde 28

Maddeyle, Kanunun kapsamı dışında tutulan hususlar düzenlenmektedir.

Birinci fıkrada, tamamen Kanun kapsamı dışında tutulan hususlar düzenlenmektedir. Buna göre kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklerle uyulmak kaydıyla, gerçek kişilerin kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetleri kapsamında; anonim hale getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla; milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği veya kişilik haklarını ihlal etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla veya ifade özgürlüğü kapsamında işlenmesi Kanunun tamamen kapsamı dışında tutulmaktadır.

Bunun gibi kişisel verilerin, milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi istisna olarak düzenlenmektedir. Buna göre Milli İstihbarat Teşkilatı ile diğer istihbarat birimlerinin milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik faaliyetler kapsamında işlediği veriler Kanun kapsamı dışında tutulmaktadır. Aynı şekilde belirtilen amaçlarla, suç gelirlerinin aklanması, terörizmin finansmanının önlenmesi ve mali suçların araştırılması konusunda; yetkili birim tarafından yürütülen faaliyetler kapsamında işlenen veriler de bu istisna kapsamındadır. Bu konulardaki yetkili birimin; milli savunmayı, milli güvenliği kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik olmak üzere mali araştırma yapmak, mali istihbarat elde etmek ve üretmek, veri toplamak, şüpheli işlem bildirimleri ve diğer bildirimleri almak, analiz etmek, değerlendirmek, inceleme yapmak ve ilgili kurumlarla paylaşmak suretiyle işlediği veriler de kapsam dışında tutulmaktadır. Ayrıca, kişisel verilerin; soruşturma, kovuşturma, yargılama ve infaz mercileri ile disiplin soruşturma ve kovuşturma makamları tarafından ilgili kanun hükümleri uyarınca işlenmesi de kapsam dışında tutulmuştur.

Maddenin ikinci fıkrasında, kısmen Kanun kapsamı dışında kalan hususlar düzenlenmektedir. Buna göre, kural olarak bu fıkrada sayılan haller kanun hükümlerine tabi olmakla birlikte, sadece fıkrada belirtilen kanun maddelerinde düzenlenen hükümler bakımından istisna tutulmaktadır. Bu bağlamda ikinci fıkrada, Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla; veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Sicile kayıt yükümlülüğünü düzenleyen 16 ncı maddelerinin uygulanmayacağı haller düzenlenmektedir. Bu haller; veri işleminin suç işlenmesinin önlenmesi için gerekli olması; ilgili kişinin kendisi tarafından alenileştirilmiş verilerin işlenmesi; veri işleminin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi için gerekli olması şeklinde tespit edilmektedir.

Madde 29

Maddeyle Kurumun bütçesi ve gelirleri düzenlenmektedir.

Madde 30

Maddeyle, Kanun sebebiyle diğer kanunlarda yapılacak değişiklikler ile eklemeler düzenlenmektedir. Bu kapsamda Kişisel Verileri Koruma Kurumu, 5018 sayılı Kanuna ekli (III) sayılı cetvele eklenmektedir.

İkinci fıkrayla, 5237 sayılı Türk Ceza Kanununun 135 inci maddesinin ikinci fıkrasında deęişiklik yapılmak suretiyle, birinci fıkrada işlenen suçun konusunun özel nitelikli (hassas) veriler olması halinde verilecek cezanın yarı oranında artırılması öngörülmektedir.

Ayrıca, elektronik haberleşme ve veri kayıt sistemlerinde meydana gelen gelişmeler doğrultusunda 3359 sayılı Sağlık Hizmetleri Temel Kanununun 3 üncü maddesinin birinci fıkrasının (f) bendinde deęişiklik yapılarak kayıt ve bildirim sisteminin elektronik ortamda da yapılabilmesine imkan sağlanmaktadır.

Dördüncü fıkrayla, 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 47 maddesi deęiştirilmektedir. Yapılan deęişiklikle, sağlık hizmeti almak üzere, kamu veya özel sağlık kuruluşları ile sağlık mesleęi mensuplarına müracaat eden kişilerin verilerinin işlenebilmesi hükme bağlanmakta, işlenen bu verilerin; sağlık hizmetinin verilmesi, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve finansmanı amacıyla Sağlık Bakanlığınca toplanarak işlenebileceęi düzenlenmektedir. Sağlık Bakanlığınca toplanan bu verilere, ilgili kişilerin kendileri veya yetki verdikleri üçüncü kişilerin erişimlerini sağlayacak bir sistem kurmaları da ayrıca hüküm altına alınmaktadır.

Öte yandan, kişisel sağlık verisi kayıtlarının tutulduęu bu sistemlerin güvenlięi ve güvenilirlięi ile ilgili standartlar Sağlık Bakanlığınca belirlenecek, elde edilen kişisel sağlık verilerinin güvenlięinin sağlanması için gerekli olan tedbirler Bakanlıkça alınacak ve bu amaçla, sistemde kayıtlı bilgilerin hangi görevli tarafından ne amaçla kullanıldığının denetlenmesine imkân tanıyan bir güvenlik sistemi yine adı geçen Bakanlıkça kurulacaktır. Ayrıca, veri güvenlięini sağlamak amacıyla sağlık personeli istihdam eden kamu kurum ve kuruluşları ile özel hukuk tüzel kişileri ve gerçek kişiler, istihdam ettikleri personeli ve personel hareketlerini Bakanlığa bildirmekle yükümlü olacaktır.

Son fıkrada ise kişisel sağlık verilerinin işlenmesi, güvenlięi ve bu maddenin uygulanması ile ilgili dięer hususların Bakanlıkça çıkarılan yönetmelikle düzenleneceęi öngörülmektedir.

Madde 31

Maddeyle, Kanunun uygulanmasına ilişkin yönetmeliklerin, Kurum tarafından yürürlüğe konulması öngörülmektedir,

GEÇİCİ MADDE 1

Maddenin birinci fıkrasıyla, Kanunun yayımı tarihinden itibaren altı ay içinde Kurul üyelerinin seçilmesi ve Başkanlığın kurulması ve teşkilatlanmasının tamamlanması düzenlenmektedir.

Maddenin ikinci fıkrasında, veri sorumlularının Kurul tarafından belirlenecek ve ilan edilecek süre içinde Sicile kayıt olmaları öngörülmektedir. Bu düzenlemeyle Kurumun, Sicile yönelik gerekli fiziki ve teknik altyapıyı tamamlaması amaçlanmaktadır.

Üçüncü fıkrayla, Kanunun yürürlüğe girdiği tarihten önce işlenmiş olan kişisel verilerin iki yıl içinde Kanunda öngörülen usul ve esaslara uygun hale getirilmesi öngörülmektedir. Kanunda öngörülen usul ve esaslara aykırı olduğu anlaşılan kişisel verilerin ise derhal silinmesi, yok edilmesi veya anonim hale getirilmesi düzenlenmektedir.

Dördüncü fıkrayla, Kanunda öngörülen yönetmeliklerin bir yıl içinde yürürlüğe konulması hükme bağlanmaktadır.

Beşinci fıkrayla, kamu kurum ve kuruluşlarında Kanunun uygulanmasıyla ilgili koordinasyonu sağlamak üzere üst düzey bir yönetici belirlenerek Başkanlığa bildirilmesi hususu düzenlenmektedir.

İlk seçilen Başkan, İkinci Başkan ve kura ile belirlenen bir üyenin altı yıl, diğer dört üyenin ise dört yıl görev yapması öngörülmekte ve böylelikle, Kurum hafızasının devamı için Kurul üyelerinin dönüşümlü olarak görev yapmaları amaçlanmaktadır.

Öte yandan, Kişisel Verileri Koruma Kurumuna bütçe tahsis edilene kadar Kurumun giderlerinin Başbakanlık bütçesinden karşılanacağı, hizmetin yerine getirilmesi için gerekli desteğin Başbakanlıkça sağlanacağı ve hizmet birimleri faaliyete geçinceye kadar sekretarya hizmetlerinin Başbakanlık tarafından yürütüleceği hükme bağlanmaktadır.

Madde 32

Yürürlük maddesidir.

Madde 33

Yürütme maddesidir.

Anayasa Madde 20(3) Gerekçesi

5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun

Anayasa'nın 20. Maddesinin Üçüncü Fıkrasının Gerekçesi

Madde 2- Anayasada kişisel verilerin korunmasına yönelik dolaylı hükümler bulunmakla, birlikte yeterli değildir. Mukayeseli hukukta ve tarafı olduğumuz uluslararası belgelerde de kişisel, verilerin korunması önemle vurgulanmaktadır., Maddeyle, herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı, anayasal bir, hak olarak teminat altına alınmaktadır. Bu bağlamda, bireylerin kendilerini ilgilendiren kişisel veriler, üzerinde hangi hak ve yetkilere sahip olduğu ve kişisel verilerin hangi hallerde işlenebileceği hükme, bağlanırken, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği, öngörülmektedir.

TEMEL YÖNETMELİKLER

Bölüm İçeriği

- Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği
- Kişisel Verileri Koruma Kurumu Disiplin Amirleri Yönetmeliği
- Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik
- Kişisel Verileri Koruma Uzmanlığı Yönetmeliği
- Kişisel Verileri Koruma Kurumu Personeli Görevde Yükselme ve Ünvan Değişikliği Yönetmeliği
- Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik
- Veri Sorumluları Sicili Hakkında Yönetmelik
- Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik
- Kişisel Sağlık Verileri Hakkında Yönetmelik
- Sosyal Güvenlik Kurumu Nezdindeki Verilerin Korunmasına ve İşlenmesine İlişkin Yönetmelik

Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği

Resmi Gazete Tarihi : 26.04.2018

Resmi Gazete Sayısı : 30403

Bakanlar Kurulu Kararının Tarihi ve No : 17.01.2018 - 2018/11296

KİŞİSEL VERİLERİ KORUMA KURUMU TEŞKİLAT YÖNETMELİĞİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç ve kapsam

MADDE 1- (1) Bu Yönetmeliğin amacı; Kişisel Verileri Koruma Kurumunun teşkilat yapısı, hizmet birimlerinin görev, yetki ve sorumlulukları ile çalışma usul ve esaslarını belirlemektir.

Dayanak

MADDE 2- (1) Bu Yönetmelik 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununun 25 inci maddesinin beşinci fıkrasına dayanılarak hazırlanmıştır.

Tanımlar

MADDE 3- (1) Bu Yönetmeliğin uygulanmasında;

- a) Başkan: Kişisel Verileri Koruma Kurumu Başkanı,
 - b) Kanun: 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununu,
 - c) Kurul: Kişisel Verileri Koruma Kurulunu,
 - ç) Kurum: Kişisel Verileri Koruma Kurumunu,
 - d) Üye: Kişisel Verileri Koruma Kurulu üyesini,
- ifade eder.

İKİNCİ BÖLÜM

Kişisel Verileri Koruma Kurumu

Kurum

MADDE 4- (1) Kurum, Kurul ile Başkanlık teşkilatından oluşur.

(2) Kurum hizmet birimleri daire başkanlıkları şeklinde teşkilatlanır.

(3) Kurum, Başbakanlık ile ilişkilidir. Kurumun merkezi Ankara'dadır.

(4) Kurum, ilgili mevzuatta kendisine tahsis edilen mali kaynaklarını, görev ve yetkilerinin gerektirdiği ölçüde, kendi bütçesinde belirlenen usul ve esaslar dahilinde serbestçe kullanır.

Kurumun görevleri

MADDE 5- (1) Kurumun görev ve yetkileri şunlardır:

a) Görev alanı itibarıyla, uygulamaları ve mevzuattaki gelişmeleri takip etmek, değerlendirme ve önerilerde bulunmak, araştırma ve incelemeler yapmak veya yaptırmak.

b) İhtiyaç duyulması hâlinde, görev alanına giren konularda kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri veya üniversitelerle işbirliği yapmak.

c) Kişisel verilerle ilgili uluslararası gelişmeleri izlemek ve değerlendirmek, görev alanına giren konularda uluslararası kuruluşlarla işbirliği yapmak, toplantılara katılmak.

ç) Yıllık faaliyet raporunu Cumhurbaşkanlığına, Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonuna ve Başbakanlığa sunmak.

d) Kanunlarla verilen diğer görevleri yerine getirmek.

ÜÇÜNCÜ BÖLÜM

Kişisel Verileri Koruma Kurulu

Kurul

MADDE 6- (1) Kurul, Kurumun karar organıdır. Kurul; biri Başkan, biri İkinci Başkan olmak üzere dokuz üyeden oluşur. Kurul, üyeleri arasından Başkan ve İkinci Başkanı seçer.

Kurulun görev ve yetkileri

MADDE 7- (1) Kurulun görev ve yetkileri şunlardır:

a) Kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak.

b) Kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikâyetlerini karara bağlamak.

- c) Şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde bu konuda geçici önlemler almak.
- ç) Veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak.
- d) Özel nitelikli kişisel verilerin işlenmesi için alınması gereken yeterli önlemleri belirlemek.
- e) Veri Sorumluları Sicilinin tutulmasını sağlamak.
- f) Kişisel verilerin silinmesine, yok edilmesine veya anonim hale getirilmesine ilişkin usul ve esasları belirlemek.
- g) Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmak.
- ğ) Veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmak.
- h) Yurtdışına veri aktarılabilmesi için yeterli korumaya sahip olan ve olmayan ülkeleri belirleyip ilan etmek.
- ı) Kişisel verilerin korunması, işlenmesi ve güvenliği ile ilgili sektörel uygulama esaslarını belirlemek ve akreditasyon, sertifikasyon, eğitim ile rehberlik konularında usul ve esasları belirlemek.
- i) Kişisel verilerin korunması konusunda kurum ve kuruluşları bilgilendirmek ve kamuoyuna yönelik farkındalık faaliyetleri gerçekleştirmek.
- j) Üniversiteler ve ilgili diğer yurtiçi ve yurtdışı kurum ve kuruluşlarla işbirliği ve koordinasyon çalışmalarını yürütmek.
- k) Kanunda öngörülen idari yaptırımlara karar vermek.
- l) Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek.
- m) Kurumun; stratejik planını karara bağlamak, amaç ve hedeflerini, hizmet kalite standartlarını ve performans kriterlerini belirlemek.
- n) Kurumun stratejik planı ile amaç ve hedeflerine uygun olarak hazırlanan bütçe teklifini görüşmek ve karara bağlamak.
- o) Kurumun performansı, mali durumu, yıllık faaliyetleri ve ihtiyaç duyulan konular hakkında hazırlanan rapor taslaklarını onaylamak ve yayımlamak.
- ö) Taşınmaz alımı, satımı ve kiralınması konularındaki önerileri görüşüp karara bağlamak.

p) Kanunlarla verilen diğer görevleri yerine getirmek.

DÖRDÜNCÜ BÖLÜM

Başkanlık Teşkilatı

Başkanlık

MADDE 8- (1) Başkanlık; Başkana bağlı Başkan Yardımcısı ve hizmet birimlerinden oluşur.

Başkan

MADDE 9- (1) Başkan, Kurul üyeleri arasından Kurul tarafından seçilir.

(2) Başkan, Kurul ve Kurumun başkanı sıfatıyla Kurumun en üst amiri olup Kurum hizmetlerini mevzuata, Kurumun amaç ve politikalarına, stratejik planına, performans ölçütlerine ve hizmet kalite standartlarına uygun olarak düzenler, yürütür ve hizmet birimleri arasında koordinasyonu sağlar.

(3) Başkan, Kurumun genel yönetim ve temsilinden sorumludur. Bu sorumluluk, Kurum çalışmalarının düzenlenmesi, yürütülmesi, denetlenmesi, değerlendirilmesi ve gerektiğinde kamuoyuna duyurulması görev ve yetkilerini kapsar.

(4) Başkanın görev ve yetkileri şunlardır:

a) Kurul toplantılarını idare etmek.

b) Kurul kararlarının tebliğini ve Kurulca gerekli görülenlerin kamuoyuna duyurulmasını sağlamak ve uygulanmalarını izlemek.

c) Başkan Yardımcısını, daire başkanlarını ve Kurum personelini atamak.

ç) Hizmet birimlerinden gelen önerilere son şeklini vererek Kurula sunmak.

d) Stratejik planın uygulanmasını sağlamak, hizmet kalite standartları doğrultusunda insan kaynakları ve çalışma politikalarını oluşturmak.

e) Belirlenen stratejilere, yıllık amaç ve hedeflere uygun olarak Kurumun yıllık bütçesi ile mali tablolarını hazırlamak.

f) Kurul ve hizmet birimlerinin uyumlu, verimli, disiplinli ve düzenli bir biçimde çalışması amacıyla koordinasyonu sağlamak.

g) Kurumun diğer kuruluşlarla ilişkilerini yürütmek.

ğ) Kurum Başkanı adına imzaya yetkili personelin görev ve yetki alanını belirlemek.

h) Kurumun yönetim ve işleyişine ilişkin diğer görevleri yerine getirmek.

Başkana vekâlet

MADDE 10- (1) Kurul, üyelerden birini İkinci Başkan olarak seçer. Başkanın yokluğunda İkinci Başkan, onun da bulunmadığı hallerde Başkan tarafından belirlenen bir üye Başkana vekâlet eder.

Başkan Yardımcısı

MADDE 11- (1) Başkan Yardımcısı, Başkanlığa ilişkin görevlerinde Başkana yardımcı olmak, ilgili mevzuat ve Kurul kararlarıyla verilen görevlerin yerine getirilmesini sağlamak, hizmet birimleri arasında uyum ve işbirliğini temin etmek ve Başkan tarafından verilen diğer görevleri yerine getirmekle yükümlüdür.

(2) Başkan Yardımcısının; en az dört yıllık yükseköğretim kurumu mezunu ve on yıl süreyle kamu hizmetinde bulunmuş olması gerekir.

Hizmet birimleri yöneticileri

MADDE 12- (1) Hizmet birimleri yöneticileri, Başkan tarafından atanır.

(2) Daire başkanlarının; en az dört yıllık yükseköğretim kurumu mezunu ve on yıl süreyle kamu hizmetinde bulunmuş olması gerekir.

(3) Hizmet birimleri yöneticileri; kanun, yönetmelik, ilgili diğer mevzuat ve Kurul kararlarıyla birime verilen görevleri yerine getirmek, personeli arasında uyum, işbirliği ve işbölümünü temin etmek ve Başkan tarafından verilen diğer görevleri yapmakla yükümlüdürler.

BEŞİNCİ BÖLÜM

Hizmet Birimleri ve Görevleri

Hizmet birimleri

MADDE 13- (1) Kurumun hizmet birimleri şunlardır:

- a) Veri Yönetimi Dairesi Başkanlığı.
- b) İnceleme Dairesi Başkanlığı.
- c) Hukuk İşleri Dairesi Başkanlığı.
- ç) Veri Güvenliği ve Bilgi Sistemleri Dairesi Başkanlığı.
- d) Rehberlik, Araştırma ve Kurumsal İletişim Dairesi Başkanlığı.
- e) İnsan Kaynakları ve Destek Hizmetleri Dairesi Başkanlığı.
- f) Strateji Geliştirme Dairesi Başkanlığı.

Veri Yönetimi Dairesi Başkanlığı

MADDE 14- (1) Veri Yönetimi Dairesi Başkanlığının görevleri şunlardır:

- a) Kişisel verilerin işlenmesine ilişkin usul ve esasların belirlenmesi ile ilgili çalışmalarını yürütmek.
- b) Veri sorumlusunun, temsilcisinin ve irtibat kişisinin görev, yetki ve sorumluluklarına ilişkin iş ve işlemleri yürütmek.
- c) Veri Sorumluları Sicili ile ilgili iş ve işlemleri yürütmek.
- ç) Veri sorumluları ile ilgili her türlü bilgilendirici çalışmalarını yürütmek.
- d) Veri sorumlusu siciline kayıt zorunluluğu istisnalarıyla ilgili işleri yürütmek.
- e) Veri sorumluları siciline kayıt ve bildirim yükümlülüklerini yerine getirmeyen, gerçek ve tüzel kişilerle ilgili iş ve işlemleri yürütmek.
- f) Aydınlatma yükümlülüğünü yerine getirmeyenler hakkındaki iş ve işlemleri yürütmek.
- g) Veri sorumluları sicil kayıt modülü ile ilgili iş ve işlemleri Veri Güvenliği ve Bilgi Sistemleri Dairesi Başkanlığı ile birlikte yürütmek.
- ğ) Veri silme, yok etme ve anonimleştirme usulleri ile ilgili çalışmalarını yürütmek.
- h) Başkan tarafından verilen diğer görevleri yapmak.

İnceleme Dairesi Başkanlığı

MADDE 15- (1) İnceleme Dairesi Başkanlığının görevleri şunlardır:

- a) Veri sorumlusuna başvuru ve Kurula yapılan şikâyete ilişkin iş ve işlemleri yürütmek.
- b) Kurula yapılan şikâyetlerle ilgili ön inceleme ve esas incelemeleri yapmak.
- c) Şikâyet üzerine veya resen incelemeye ilişkin iş ve işlemleri yürütmek.
- ç) Şikâyet başvuru ve takip sistemiyle ilgili iş ve işlemleri Veri Güvenliği ve Bilgi Sistemleri Dairesi Başkanlığıyla birlikte yürütmek.
- d) Kurul tarafından verilen kararları yerine getirmeyenler hakkındaki iş ve işlemleri yürütmek.
- e) Başkan tarafından gündeme alınması uygun görülen konuları içeren Kurul toplantı gündemini hazırlamak, gündemi ve gündemdeki konulara ilişkin takrirleri Kurul üyelerine dağıtmak.
- f) Talep edilmesi halinde Kurul toplantılarının kaydını tutmak ve muhafaza etmek.

- g) Kurul tarafından alınan kararları imzaya açmak, imzaların tamamlanmasını müteakip kararları ilgili birimlere göndermek.
- ğ) Kurul tarafından talep edilen kişilerin toplantıya katılımlarını temin etmek.
- h) Kurul toplantılarında alınan kararları tutanağa geçirmek, tutanak ve varsa eklerinin her sayfasını toplantıya katılan üyelere imzalatmak.
- ı) Kurula ait yazışmaları yapmak, karar ve yazışmalara ilişkin arşiv oluşturmak ve bunları muhafaza etmek.
- i) Kurumun internet sitesinde yayımlanması istenen Kurul kararlarının yayımlanmasını sağlamak.
- j) Başkan tarafından verilen diğer görevleri yapmak.

Hukuk İşleri Dairesi Başkanlığı

MADDE 16- (1) Hukuk İşleri Dairesi Başkanlığının görevleri şunlardır:

- a) Kurumun taraf olduğu dava ve icra takiplerinde, Kurumu temsil etmek, bunları takip etmek, sonuçlandırılmasını sağlamak, gerektiğinde serbest çalışan avukatlar ve/veya avukatlık ortaklıklarıyla avukatlık sözleşmeleri akdedilmesine ilişkin işlemleri yürütmek.
- b) Kurumun görevlerine ilişkin hukuki konularda; adlî ve idari yargı mercileri, hakemler, icra daireleri, komisyonlar ve ilgili kamu kurum ve kuruluşları ile milletlerarası tahkim mahkemeleri nezdinde Kurumu temsil etmek.
- c) Dava veya icra takibinden veya kanun yoluna müracaattan vazgeçilmesine ilişkin işlemler ile dava veya icraya intikal etmiş uyuşmazlıkların sulh yoluyla çözümlenmesine veya davanın kabulüne ilişkin işlemleri yürütmek.
- ç) Başkan veya Kurul tarafından intikal ettirilen konularda hukuki görüş bildirmek ve hukuki yollara başvurulmasına ilişkin değerlendirme yapmak.
- d) Kurumun birimleri tarafından tereddüt edilen hukuki konularda görüş talebinde bulunulması halinde, sorulan hususlarla ilgili mevzuat ve genel hukuk kuralları çerçevesinde konu ile ilgili hukuki görüşü ilgili birime bildirmek.
- e) Kurumun görev alanı ile ilgili olarak diğer kamu kurum ve kuruluşları veya Kurumun hizmet birimleri tarafından hazırlanan mevzuat taslakları hakkında hukuki görüş bildirmek.
- f) Konusuna münhasıran özel ihtisas gerektiren istisnai durumlarda, uzman kişi ve kuruluşlardan hukuki görüş alınmasına ilişkin işlemleri yürütmek.

g) Kişisel verilerin yurtdışına aktarılmasında yeterli korumanın bulunduğu ülkelerin belirlenmesine ilişkin işlemleri yürütmek.

ğ) Başkan tarafından verilen diğer görevleri yapmak.

Veri Güvenliği ve Bilgi Sistemleri Dairesi Başkanlığı

MADDE 17- (1) Veri Güvenliği ve Bilgi Sistemleri Dairesi Başkanlığının görevleri şunlardır:

a) Veri güvenliği ile ilgili iş ve işlemleri yürütmek.

b) Kişisel verilerin korunmasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü tedbirin alınması hususundaki işlemleri yürütmek.

c) Kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi durumlarına ilişkin alınması gereken tedbirlerle ilgili işlemleri yürütmek.

ç) Özel nitelikli kişisel verilerin işlenmesi için alınması gereken önlemleri belirlemekle ilgili çalışmaları yürütmek.

d) Veri güvenliğine ilişkin yükümlülüklerini yerine getirmeyenlerle ilgili iş ve işlemleri yürütmek.

e) Veri aktarımına ilişkin alınması gereken güvenlik önlemlerini belirlemek.

f) Kurum birimlerinin bilgi işlem ve otomasyon ihtiyacını karşılamak ve işletimini sağlamak, Kurumun bilgi işlem hizmetlerini yürütmek.

g) Kurum projelerinin Kurumun bilişim altyapısına uygun olarak ilgili daire başkanlıklarıyla birlikte tasarlanmasını ve uygulanmasını sağlamak, teknolojik gelişmeleri takip etmek, bilgi ve veri güvenliği konusunun gerektirdiği önlemleri almak, politikaları ve ilkeleri belirlemek, kamu bilişim standartlarına uygun çözümler üretmek.

ğ) Kurumun mevcut bilişim altyapısının kurulumu, bakımı, ikmali, geliştirilmesi ve güncellenmesi ile ilgili işleri yürütmek, haberleşme güvenliğini sağlamak ve bu konularda görev üstlenen personelin bilgi teknolojilerindeki gelişmelere paralel olarak düzenli şekilde hizmet içi eğitim almalarını sağlamak.

h) Kurumun internet sayfaları, elektronik imza ve elektronik belge gibi uygulamalar ile ilgili teknik çalışmalar yapmak.

ı) Kurumun siber güvenliğinin sağlanmasına yönelik çalışmalar yapmak.

i) Kurum hizmetleriyle ilgili bilgileri toplamak ve ilgili birimlerle işbirliği içinde veri tabanları oluşturmak.

j) Başkan tarafından verilen diğer görevleri yapmak.

Rehberlik, Araştırma ve Kurumsal İletişim Dairesi Başkanlığı

MADDE 18- (1) Rehberlik, Araştırma ve Kurumsal İletişim Dairesi Başkanlığının görevleri şunlardır:

a) Kişisel verilerin korunması ile ilgili standartların belirlenmesi, yetkilendirme ve sertifika işlemlerini yürütmek.

b) Kurumun görev alanına giren konularda faaliyet gösteren kamu kurum ve kuruluşları, gerçek ve tüzel kişiler ile gönüllü kuruluşlara faaliyetlerinde yol gösterecek plan ve programlar oluşturmak ve rehberlik etmek.

c) Kurumun, görev alanı ile ilgili ihtiyaç duyacağı konularda araştırma ve proje yapmak, yaptırmak, gerektiğinde ihtisas komisyonları oluşturulmasını önererek komisyon çalışmalarından elde edilecek sonuçları Kurula sunmak.

ç) Görev alanına giren konularda ulusal ve uluslararası kurum ve kuruluşlar, üniversiteler ve sivil toplum kuruluşları ile işbirliği yapmak; bunlarla ortak çalışma, araştırma, eğitim programları düzenlemek.

d) Kurumun eğitim faaliyetleri ile ilgili dokümantasyon, yayın ve arşiv hizmetleri ile Kurumun kütüphanecilik hizmetlerini yürütmek.

e) Kamu kurumları ve özel kuruluşlarla ilişkileri sağlamak, geliştirmek ve yürütmek.

f) Kurumun ulusal ve uluslararası düzeyde işbirliği geliştirmesi ve Kurumun tanıtılmasına ilişkin işleri yürütmek.

g) Kurumun yurtiçi ve yurtdışı görev ve faaliyetlerini raporlamak ve arşivlemek.

ğ) Kurumsal amaçlar ve politikalar doğrultusunda Kurumun iletişim stratejisinin oluşturulması ve yürütülmesini sağlamak, bu amaç ve politikalar doğrultusunda Kurumun basın ve yayın kuruluşlarıyla ilişkilerini yürütmek.

h) Kurum faaliyetleri konusunda kamuoyunun bilgilendirilmesi amacıyla basın açıklaması, bülten, haber ve duyurular hazırlamak.

ı) Kurumun görev alanına giren konular hakkında basında ve sosyal medyada yer alan haber, yazı ve programları takip ederek bunların arşivini oluşturmak, ilgili birimleri bilgilendirmek, gerektiğinde medya analiz raporları hazırlamak veya hazırlatmak, Kurumu ilgilendiren haberlerin ilgili birimlere ve tüm personele duyurulmasını sağlamak.

- i) 9/10/2003 tarihli ve 4982 sayılı Bilgi Edinme Hakkı Kanunu kapsamında yapılacak başvurular ile bu nitelikteki diğer başvuruların sonuçlandırılmasına ilişkin işlemlerin koordinasyonunu sağlamak.
- j) Başkan tarafından verilen diğer görevleri yapmak.

İnsan Kaynakları ve Destek Hizmetleri Dairesi Başkanlığı

MADDE 19- (1) İnsan Kaynakları ve Destek Hizmetleri Dairesi Başkanlığının görevleri şunlardır:

- a) Kurumun insan kaynakları politikasını belirlemek, personelin kariyer ve eğitim planlarını hazırlamak ve uygulamak.
- b) Personel ihtiyaçlarını tespit etmek, insan kaynaklarının etkin ve verimli şekilde kullanılmasını sağlamak, Kuruma ait kadroların dağıtım ve tahsis işlemlerini yapmak.
- c) Kurum personelinin nitelikleri ve yeterliklerinin belirlenmesi ve geliştirilmesine yönelik politikaları oluşturmak, bu amaçla ilgili birim, kurum ve kuruluşlarla işbirliği yapmak.
- ç) Kurumun hizmet içi eğitim planını hazırlamak ve eğitim programları düzenlemek.
- d) Genel evrak işlemlerini yürütmek.
- e) Başkan, üyelerin ve Kurum personelinin mali ve sosyal haklarının tahakkuk ettirilerek ödenmesini sağlamak; atama, nakil, performans, terfi, özlük, emeklilik, mal bildirim ve benzeri işlemlerini yürütmek.
- f) Uzman yardımcılarının uzman olabilmeleri için hazırlanması gereken tezler ve gireceği sınavlar ile ilgili iş ve işlemleri yürütmek.
- g) 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanunu çerçevesinde Kurumun ihtiyacı olan her türlü satın alma, kiralama, bakım, onarım, yapım, arşiv, sağlık, sosyal ve benzeri hizmetleri yürütmek.
- ğ) Kuruma ait taşınır ve taşınmazların kayıtlarını tutmak.
- h) Başkan tarafından verilen diğer görevleri yapmak.

Strateji Geliştirme Dairesi Başkanlığı

MADDE 20- (1) Strateji Geliştirme Dairesi Başkanlığının görevleri şunlardır:

- a) 5018 sayılı Kanun, 22/12/2005 tarihli ve 5436 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanunun 15 inci maddesi ve diğer mevzuatla strateji geliştirme ve mali hizmetler birimlerine verilen görevleri yapmak.

- b) Kurumun; stratejik planını hazırlamak, amaç ve hedeflerini, hizmet kalite standartlarını ve performans kriterlerini belirlemek.
- c) Kurumun stratejik planı ile amaç ve hedeflerine uygun olarak bütçe teklifini hazırlamak.
- ç) Kurumun performansı, mali durumu, yıllık faaliyetleri ve ihtiyaç duyulan konular hakkında rapor hazırlamak.
- d) Kurumun mali raporlarını ve kesin hesabını hazırlamak.
- e) Kurumun bütçesine, yıllık iş planına, gelir-gider kesin hesaplarına, yıllık raporuna ve sair raporlarına ilişkin işlemleri yapmak, gerekli hallerde bütçe kalemleri arasında aktarma yapılmasına ilişkin çalışmaları yürütmek.
- f) Bir önceki malî yıla ait, konsolide edilmiş gelir tablolarını, bilançoları ve yıllık faaliyetleri esas alan kapsamlı malî tabloları içeren yıllık raporu hazırlamak ve en geç bir sonraki yılın nisan ayının sonuna kadar bilgi için ilgili yerlere gönderilmesine ilişkin çalışmaları ve bütçenin ibrası ile ilgili işlemleri yapmak.
- g) Kurum gelirlerinin tahsili ve takibine ilişkin işlemleri yürütmek, Kurumun nakit varlığını yönetmek ve muhafaza etmek.
- ğ) Kurum harcamalarının, onaylı bütçe çerçevesinde ve harcama usul ve esaslarına uygun olarak gerçekleştirilmesini sağlamak.
- h) Kurumun hesap planları ve muhasebe kayıtlarıyla ilgili işlemleri yürütmek.
- ı) Kurumun görev kapsamına giren işlerle ilgili istatistiki bilgileri tutmak, yayınlamak.
- i) Mali konularla ilgili mevzuatın uygulanmasını sağlamak.
- j) Başkan tarafından verilen diğer görevleri yapmak.

ALTINCI BÖLÜM

Kurum Personeli

Unvan ve sayıları

MADDE 21- (1) Toplam kadro sayısını geçmemek üzere 13/12/1983 tarihli ve 190 sayılı Genel Kadro ve Usulü Hakkında Kanun Hükmünde Kararnamenin eki cetvellerde yer alan kadro unvanlarıyla sınırlı olmak kaydıyla unvan ve derece değişikliği yapma, yeni unvan ekleme ve boş kadroların iptali Kurul kararıyla yapılır.

(2) Personelin, hizmet birimleri itibarıyla dağılımını yapmaya Başkan yetkilidir.

Personel istihdamı

MADDE 22- (1) Kurum personeli Başkan tarafından atanır.

(2) Başkana danışmanlık hizmeti vermek ve Başkan tarafından verilen diğer görevleri yapmak amacıyla ihtiyaca göre sayıları toplam onu geçmemek üzere başkanlık müşaviri atanabilir. Başkanlık müşaviri kadrolarına Kurumdan atanacakların en az daire başkanı veya Kurul üyesi olarak görev yapmış olmaları; Kurum dışından atanacakların kamuda en az on yıllık mesleki tecrübeye veya doktora derecesinde akademik unvana sahip olmaları gerekir.

(3) Başkanın programını düzenlemek ve yürütmek, resmi ve özel yazışmalarını yapmak, Başkan ve üyelerin toplantı ve organizasyonlarda temsilini sağlamak üzere Başkan tarafından bir Özel Kalem Müdürü atanır.

YEDİNCİ BÖLÜM

Çeşitli ve Son Hükümler

Kurum içi denetim

MADDE 23- (1) Kurum içi denetim, inceleme ve soruşturma işlemleri, Başkan tarafından görevlendirilecek yetkililer tarafından yerine getirilir. Bu işlem ve sonuçlardan Kurulun görev ve yetki alanına giren hususların Kurulun bilgisine sunulması zorunludur.

Düzenleme yetkisi

MADDE 24- (1) Bu Yönetmelikte yer almayan ya da açıklık bulunmayan konularda ilgili mevzuat hükümleri çerçevesinde karar vermeye, uygulamayı düzenlemeye ve yönlendirmeye Kurul yetkilidir.

Yürürlük

MADDE 25- (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 26- (1) Bu Yönetmelik hükümlerini Başkan yürütür.

Kişisel Verileri Koruma Kurumu Disiplin Amirleri Yönetmeliği

Resmi Gazete Tarihi : 15.03.2022

Resmi Gazete Sayısı : 31779

KİŞİSEL VERİLERİ KORUMA KURUMU DİSİPLİN AMİRLERİ YÖNETMELİĞİ

Amaç

MADDE 1- (1) Bu Yönetmeliğin amacı; Kişisel Verileri Koruma Kurumunda görev yapan Devlet memurlarının disiplin amirlerini belirlemektir.

Kapsam

MADDE 2- (1) Bu Yönetmelik, Kişisel Verileri Koruma Kurumunda 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanununa göre görev yapan Devlet memurları hakkında uygulanır.

Dayanak

MADDE 3- (1) Bu Yönetmelik, 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanununun 124 üncü maddesi ile 29/4/2021 tarihli ve 3935 sayılı Cumhurbaşkanlığı Kararı ile yürürlüğe konulan Devlet Memurları Disiplin Yönetmeliğinin 5 inci maddesine dayanılarak hazırlanmıştır.

Disiplin amirleri

MADDE 4- (1) Bu Yönetmelik kapsamında görev yapan Devlet memurlarının disiplin amirleri Ek-1 sayılı Cetvelde gösterilmiştir.

Disipline ilişkin usul ve esaslar bakımından uygulanacak mevzuat

MADDE 5- (1) Disipline ilişkin usul ve esaslar bakımından 657 sayılı Kanun ile Devlet Memurları Disiplin Yönetmeliği hükümleri uygulanır.

Yürürlükten kaldırılan yönetmelik

MADDE 6- (1) 17/5/2019 tarihli ve 30777 sayılı Resmî Gazete’de yayımlanan Kişisel Verileri Koruma Kurumu Disiplin Amirleri Yönetmeliği yürürlükten kaldırılmıştır.

Yürürlük

MADDE 7- (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 8- (1) Bu Yönetmelik hükümlerini Kişisel Verileri Koruma Kurumu Başkanı yürütür.

KİŞİSEL VERİLERİ KORUMA KURUMU DİSİPLİN AMİRLERİ CETVELİ

UNVAN	DİSİPLİN AMİRİ
Başkan Yardımcısı	Kurum Başkanı
Başkanlık Müşaviri	Kurum Başkanı
Özel Kalem Müdürü	Kurum Başkanı
Daire Başkanı	Kurum Başkanı
Daire Başkan Yardımcısı, Kişisel Verileri Koruma Uzmanı, Kişisel Verileri Koruma Uzman Yardımcısı, Diğer Personel	Daire Başkanı

Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik

Resmî Gazete Tarihi : 16.11.2017

Resmî Gazete Sayısı : 30242

KİŞİSEL VERİLERİ KORUMA KURULU ÇALIŞMA USUL VE ESASLARINA DAİR YÖNETMELİK

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç ve kapsam

MADDE 1 - (1) Bu Yönetmelik Kişisel Verileri Koruma Kurulunun çalışma usul ve esaslarını, görevlerini, yetkilerini ve sorumluluklarını belirlemek için hazırlanmıştır.

Dayanak

MADDE 2 - (1) Bu Yönetmelik, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununun 22 nci ve 23 üncü maddesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 3 - (1) Bu Yönetmelikte geçen;

- a) Başkan: Kişisel Verileri Koruma Kurumu Başkanı,
 - b) Kanun: 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununu,
 - c) Kurul: Kişisel Verileri Koruma Kurulunu,
 - ç) Kurum: Kişisel Verileri Koruma Kurumunu,
 - d) Üye: Kişisel Verileri Koruma Kurulu üyesini,
- ifade eder.

İKİNCİ BÖLÜM

Kişisel Verileri Koruma Kurulu

Kurul

MADDE 4 - (1) Kurul, Kurumun karar organıdır. Kurul; biri Başkan, biri İkinci Başkan olmak üzere toplam dokuz üyeden oluşur.

(2) (Değişik:RG-17/5/2019-30777) Kurulun beş üyesi Türkiye Büyük Millet Meclisi, dört üyesi Cumhurbaşkanlığı tarafından seçilir.

(3) Kurul, Kanunla ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getirir ve kullanır. Görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişi, Kurula emir ve talimat veremez, tavsiye veya telkinde bulunamaz.

Başkan

MADDE 5 - (1) Kurumun en üst yöneticisi olan Başkan, Kurumun genel yönetim ve temsili ile Kurul tarafından alınan kararların yürütülmesinden sorumludur.

(2) Başkan ve İkinci Başkan Kurul tarafından ayrı ayrı seçilir. Seçimde aday gösterilmez. Seçimin gizli veya açık oylamayla yapılacağı Kurulca kararlaştırılır. Sonuç bir tutanakla belirtilir ve toplantıya katılan Kurul üyelerince imzalanır.

(3) Başkanın izin, hastalık, yurt dışı görev ve diğer nedenlerle yokluğunda İkinci Başkan, Başkana vekalet eder. (Ek cümle:RG-17/5/2019-30777) İkinci Başkanın da bulunmadığı hallerde, Başkan tarafından belirlenen bir üye Başkana vekalet eder.

Üyeler

MADDE 6 - (1) Kurul üyelerinin görev süresi dört yıldır. Süresi biten üye yeniden seçilebilir. Görev süresi dolmadan herhangi bir sebeple görevi sona eren üyenin yerine seçilen kişi, yerine seçildiği üyenin kalan süresini tamamlar.

(2) Kurul üyelerinin süreleri dolmadan herhangi bir nedenle görevlerine son verilemez. Kurul üyelerinin;

a) Seçilmek için gereken şartları taşımadıklarının sonradan anlaşılması,

b) Görevleriyle ilgili olarak işledikleri suçlardan dolayı haklarında verilen mahkûmiyet kararının kesinleşmesi,

c) Görevlerini yerine getiremeyeceklerinin sağlık kurulu raporuyla kesin olarak tespit edilmesi,

ç) Görevlerine izinsiz, mazeretsiz ve kesintisiz olarak on beş gün ya da bir yılda toplam otuz gün süreyle devam etmediklerinin tespit edilmesi,

d) Bir ay içinde izinsiz ve mazeretsiz olarak toplam üç, bir yıl içinde toplam on Kurul toplantısına katılmadıklarının tespit edilmesi,
hâllerinde Kurul kararıyla üyelikleri sona erer.

Kurulun görev ve yetkileri

MADDE 7 - (1) Kurulun görev ve yetkileri şunlardır:

- a) Kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak.
- b) Kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikâyetlerini karara bağlamak.
- c) Şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde bu konuda geçici önlemler almak.
- ç) Veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak.
- d) Özel nitelikli kişisel verilerin işlenmesi için alınması gereken yeterli önlemleri belirlemek.
- e) Veri Sorumluları Sicilinin tutulmasını sağlamak.
- f) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esasları belirlemek.
- g) Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmak.
- ğ) Veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmak.
- h) Yurt dışına veri aktarılabilmesi için yeterli korumaya sahip olan ve olmayan ülkeleri belirleyip ilan etmek.
- ı) Kişisel verilerin korunması, işlenmesi ve güvenliği ile ilgili sektörel uygulama esaslarını belirlemek ve akreditasyon, sertifikasyon, eğitim ile rehberlik konularında usul ve esasları belirlemek.
- i) Kişisel verilerin korunması ile ilgili yurt içi ve yurt dışı projeler yapmak ve yaptırmak.
- j) Kişisel verilerin korunması konusunda kurum ve kuruluşları bilgilendirmek, kamuoyuna yönelik farkındalık faaliyetleri gerçekleştirmek.
- k) Ücret tarifeleri ile ilgili çalışmalar yapmak.
- l) Üniversiteler ve ilgili diğer yurt içi ve yurt dışı kurum ve kuruluşlarla işbirliği ve koordinasyon çalışmaları yürütmek.

- m) Kanunda öngörülen idari yaptırımlara karar vermek.
- n) Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek.
- o) Kurumun; stratejik planını karara bağlamak, amaç ve hedeflerini, hizmet kalite standartlarını ve performans kriterlerini belirlemek.
- ö) Kurumun stratejik planı ile amaç ve hedeflerine uygun olarak hazırlanan bütçe teklifini görüşmek ve karara bağlamak.
- p) Kurumun performansı, mali durumu, yıllık faaliyetleri ve ihtiyaç duyulan konular hakkında hazırlanan rapor taslaklarını onaylamak ve yayımlamak.
- r) Taşınmaz alımı, satımı ve kiralanması konularındaki önerileri görüşüp karara bağlamak.

ÜÇÜNCÜ BÖLÜM

Kurulun Çalışma Usul ve Esasları

Kurulun gündemi

MADDE 8 - (1) Kurul toplantı gündemleri; Başkan tarafından belirlenir.

(2) Gündem ve gündemdeki konulara ilişkin karar taslakları, karar için gerekli dokümanlar ile Kurumun görüş ve önerileri, toplantı tarihinden en az 3 gün önce İnceleme Dairesi Başkanlığı tarafından üyelere dağıtılır.

(3) Bir toplantıda, gündem maddelerinin görüşülmesi süre nedeniyle bitirilemezse; görüşülemeyen maddeler herhangi bir işleme gerek kalmaksızın bir sonraki toplantı gündemine dahil edilir.

Toplantı ve karar yeter sayısı

MADDE 9 - (1) Kurul, Başkan dâhil en az altı üye ile toplanır.

(2) Kurul, Başkanın belirleyeceği tarihte toplanır. Başkan gereken hâllerde Kurulu olağanüstü toplantıya çağırabilir.

(3) Üyelerin bütün toplantılarda bulunmaları esastır.

(4) Toplantıya katılamayacak olan üyeler, geçerli mazeretlerini yazılı olarak Başkanlığa bildirirler.

(5) Kurul, üye tam sayısının salt çoğunluğuyla karar alır. Kurul üyeleri çekimser oy kullanamaz.

(6) Toplantılar esas itibarıyla Kurum merkezinde yapılır. İhtiyaç duyulması halinde Kurulca, Kurum merkezi dışındaki yerlerde de toplantı yapılabilmesine karar verilebilir.

(7) Toplantıların fiziki olarak yapılması esas olmakla birlikte ihtiyaç duyulması ve Başkanın uygun görmesi halinde gerekli güvenlik önlemleri alınarak elektronik ortamda toplantı yapılabilir ya da elektronik yollarla toplantıya katılım sağlanabilir.

Görüşmelerde usul ve oylama

MADDE 10 - (1) Kararlar, müzakere yapılarak alınır. Konular gündemdeki sıralarına göre görüşülür.

(2) Başkan, gündem maddelerinin görüşülmesinde sıra dâhilinde Kurul üyelerine söz verir. Konu üzerinde görüşmeler tamamlandıktan sonra gündem maddesi oya sunulur.

(3) Kararlar, kabul veya ret için el kaldırmak suretiyle işaretle oylanır.

(4) Kurul kararları toplantı bitiminde tutanak altına alınır.

(5) Kurul üyeleri; kendilerini, üçüncü dereceye kadar kan ve ikinci dereceye kadar kayın hısımlarını, evlatlıklarını ve aralarındaki evlilik bağı kalkmış olsa bile eşlerini ilgilendiren konularla ilgili toplantı ve oylamaya katılamaz. Bu durum karar metninde ayrıca belirtilir.

Görüşmelerin gizliliği ve toplantılara katılabilecek olanlar

MADDE 11 - (1) Aksi kararlaştırılmadıkça, Kurul toplantılarındaki görüşmeler gizlidir. Kurul toplantılarına, Başkan ve üyeler ile görüşme tutanaklarını düzenlemekle görevli personel dışında hiç kimse katılamaz. Ancak, Başkan tarafından, ihtiyaç duyulması halinde taraflar, kişiler veya temsilciler Kurul toplantısına davet edilebilir. Ancak Kurul kararları toplantıya dışarıdan katılanların yanında alınmaz.

Karar

MADDE 12 - (1) Toplantıda görüşülen gündem maddelerine ilişkin alınan kararlar tutanakla tespit edilir.

(2) Karar tutanağı toplantı esnasında toplantıya katılan tüm üyeler tarafından imzalanır.

(3) Kanunda belirtilen süreler saklı kalmak üzere, Kurul kararı, alındığı toplantı tarihinden itibaren en geç on beş gün içinde gerekçeleri, varsa karşı oy gerekçeleri ile birlikte yazılır.

(4) Toplantıya katıldığı halde Kurul kararlarını süresi içinde mazeretsiz olarak imzalamayan Kurul üyeleri, ilgili toplantı tutanağındaki beyanları doğrultusunda oy kullanmış sayılır.

(5) Kurul toplantısında alınan her bir kararın yazıldığı son sayfa, toplantıya katılan üyelerin isimleri yazılmak suretiyle üyelerce imzalanır, önceki sayfalar ise imzalanır veya paraflanır.

(6) Toplantı ve karar numaraları, her yıl birden başlar ve o yılın sonuna kadar sıra numarasını takip eder.

Kararlarda bulunması gereken hususlar

MADDE 13 - (1) Şikâyet üzerine veya ihlal iddiasının öğrenilmesi durumunda resen yapılan inceleme sonucu verilen kararlar aşağıdaki hususları ihtiva eder:

- a) Karar veren Kurul üyelerinin ad ve soyadları.
- b) İnceleme ve araştırmayı yapanların ad ve soyadları.
- c) Tarafların adı, soyadı ve unvanları ile adresleri ve sıfatları.
- ç) Tarafların iddia ve beyanlarının özeti.
- d) İddia ve beyanların değerlendirilmesi.
- e) Kararın hukuki dayanağı.
- f) Sonuç.
- g) Varsa karşı oy gerekçeleri.

(2) Diğer kararlar aşağıdaki hususları ihtiva eder:

- a) Karar veren Kurul üyelerinin ad ve soyadları.
- b) Kararın konusu ve hukuki dayanağı.
- c) Sonuç.
- ç) Varsa karşı oy gerekçeleri.

Kararların saklanması

MADDE 14 - (1) Kararlar İnceleme Dairesi Başkanlığı tarafından dosyalanır. Kararların onaylı örnekleri ilgili birimlere gönderilir.

(2) Birimlere gönderilecek onaylı karar örneklerinde karşı oy gerekçeleri bulunmaz.

(3) Karar örneklerinin aslına uygunluğu İnceleme Dairesi Başkanlığı tarafından onaylanır.

Kararların açıklanması ve yayımlanması

MADDE 15 - (1) Kurul, gerekli gördüğü kararları kamuya duyurur.

(2) Kurul kararları, yazımın tamamlanmasının ardından ilgili taraflara bildirilir.

(3) Toplantılarda görüŖülen konular ve alınan kararlar hakkında basın ve yayın organlarına ancak BaŖkan tarafından açıklama yapılabilir.

Komisyon alıŖmaları

MADDE 16 - (1) Kurulda görüŖülüp, kararlaŖtırılması gereken konuların ön incelemesini yapıp, daha ayrıntılı bir kapsam ve derinlikte Kurula sunmak üzere, üyelerden oluŖan ihtisas komisyonu veya alıŖma grupları Kurul kararıyla kurulabilir. Söz konusu komisyon veya alıŖma gruplarında Kurul kararıyla Kurum personeli görevlendirilebilir.

Sır saklama

MADDE 17 - (1) Kurul üyeleriyle, BaŖkan tarafından ihtiyaç duyulması halinde Kurul toplantısına ya da hazırlık alıŖmalarına katılanlar, alıŖmaları sırasında ilgililere ve üçüncü kiŖilere ait öğrendikleri sırları bu konuda kanunen yetkili kılınan mercilerden başkasına açıklayamazlar ve kendi yararlarına kullanamazlar. Bu yükümlölük görevden ayrılmalarından sonra da devam eder.

DÖRDÜNCÜ BÖLÜM

eŖitli ve Son Hükümler

Düzenleme yetkisi

MADDE 18 - (1) Bu Yönetmelikte yer almayan ya da açıklık bulunmayan konularda ilgili mevzuat hükümleri çerçevesinde karar vermeye, uygulamayı düzenlemeye ve yönlendirmeye Kurul yetkilidir.

Yürürlük

MADDE 19 - (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 20 - (1) Bu Yönetmelik hükümlerini BaŖkan yürütür.

Yönetmeliğin Yayınlandığı Resmî Gazete'nin		
1.	Tarihi	Sayısı
	16/11/2017	30242
	Yönetmelikte Değişiklik Yapan Yönetmeliklerin Yayınlandığı Resmî Gazetelerin	
	Tarihi	Sayısı
	17/5/2019	30777
2.		

Kişisel Verileri Koruma Uzmanlığı Yönetmeliği

Resmî Gazete Tarihi : 09.02.2018

Resmî Gazete Sayısı : 30327

KİŞİSEL VERİLERİ KORUMA UZMANLIĞI YÖNETMELİĞİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç ve kapsam

MADDE 1 - (1) Bu Yönetmelik; Kişisel Verileri Koruma Uzman Yardımcılarının mesleğe alınmalarını, yetiştirilmelerini, Kişisel Verileri Koruma Uzmanlığına atanmalarına ilişkin usul ve esaslar ile Kişisel Verileri Koruma Uzman ve Uzman Yardımcılarının görev, yetki ve sorumluluklarını düzenler.

Dayanak

MADDE 2 - (1) Bu Yönetmelik, 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanununun ek 41 inci maddesi ile 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununun 26 ncı maddesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 3 - (1) Bu Yönetmelikte geçen;

- a) Başkan: Kişisel Verileri Koruma Kurumu Başkanını,
- b) Birim Yöneticisi: Daire başkanı ve üstü yöneticiyi,
- c) Daire Başkanlığı: İnsan Kaynakları ve Destek Hizmetleri Dairesi Başkanlığını,
- ç) Giriş sınavı: Kişisel verileri koruma uzman yardımcılığı kadrolarına atanacakların seçimi için yapılacak yazılı ve sözlü veya yalnızca sözlü sınavı,
- d) KPSS: Kamu Personel Seçme Sınavını,
- e) Kurul: Kişisel Verileri Koruma Kurulunu,
- f) Kurum: Kişisel Verileri Koruma Kurumunu,
- g) ÖSYM: Ölçme, Seçme ve Yerleştirme Merkezini,

- ğ) Uzman: Kişisel Verileri Koruma Uzmanını,
h) Uzman Yardımcısı: Kişisel Verileri Koruma Uzman Yardımcısını,
ı) Tez: Bu Yönetmelik çerçevesinde hazırlanacak uzmanlık tezlerini,
i) Yeterlik sınavı: Kişisel verileri koruma uzmanlığı yeterlik sınavını,
j) YDS: Yabancı Dil Bilgisi Seviye Tespit Sınavını,
ifade eder.

İKİNCİ BÖLÜM

Uzman Yardımcılığına Giriş Sınavı, Atanma,

Eğitim ve Yetiştirilme

Giriş sınavı

MADDE 4 - (1) Uzman yardımcılığı giriş sınavı, yazılı ve sözlü olarak iki aşamalı veya sözlü olarak tek aşamalı yapılabilir.

(2) Özel yarışma sınavının yazılı ve sözlü sınav veya yalnızca sözlü sınav şeklinde yapılmasına Kurul tarafından karar verilir. Giriş sınavının sadece sözlü sınavdan oluşmasına karar verilmesi halinde bu Yönetmeliğin yazılı sınava ilişkin hükümleri uygulanmaz.

(3) Yazılı sınava, atama yapılacak kadro sayısının en çok yirmi katı kadar adayın başvurusu kabul edilir.

(4) Sözlü sınava, yetmiş puandan az olmamak kaydıyla en yüksek puandan başlanarak ilân edilen her KPSS puan türünde başvuran adaylardan veya yazılı sınavda başarılı olanlardan, atama yapılacak kadro sayısının en fazla dört katı kadar aday çağrılır. Sınavlarda son sıradaki aday ile eşit puan alan diğer adayların da başvuruları kabul edilir.

(5) Yazılı sınav, test usulü veya klasik usulde yapılabilir. Yazılı sınav, Milli Eğitim Bakanlığına, TODAİE'ye, üniversitelere veya ÖSYM'ye yaptırılır.

(6) Yazılı sınava başvuruda istenecek bilgi ve belgeler, başvuru sırasında adaylardan alınacak sınav bedeli, sınav yerleri, soruların konulara göre dağılımı, sınavın yürütülmesinde gözetilecek hususlar, sınavın tarihi ve süresi, kazananların belirlenmesi ve yerleştirmeye ilişkin hususlar, sınav ve yerleştirme sonuçlarının Kuruma, adaylara bildirilmesi, açıklanması ve itiraz ile diğer hususlar Kurum ile Milli Eğitim Bakanlığı, TODAİE, üniversiteler veya ÖSYM arasında yapılacak protokolle belirlenir.

Giriş sınavı duyurusu

MADDE 5 - (1) Giriş sınavının başvuru şartları, tarihleri ve yeri, başvuruda istenen belgeler, atama yapılacak kadro sayısı, gerek görülmesi halinde öğrenim alanları itibarıyla aranacak KPSS puan türleri, taban puanları ve sınava çağrılacak aday sayısı ile sınav şekli ve sınava ilişkin diğer hususlar ilk başvuru tarihinden en az otuz gün önce Resmî Gazete’de, Kurumun internet sitesinde ve Devlet Personel Başkanlığı internet adresinde yayımlanmak suretiyle duyurulur.

Başvuru şartları

MADDE 6 - (1) Uzman yardımcıları mesleğe özel yarışma sınavı ile alınır.

(2) Yarışma sınavına katılacaklarda aşağıdaki şartlar aranır:

- a) 657 sayılı Kanununun 48 inci maddesinin birinci fıkrasının (A) bendinde yer alan genel şartları taşımak.
- b) Son başvuru tarihi itibarıyla geçerlik süresi dolmamış KPSS’den, yarışma sınavı duyurusunda belirtilen puan türlerine göre asgarî puanı almış olmak.
- c) Kurumun kadro ve ihtiyaç durumuna göre;
 - 1) En az dört yıllık lisans öğrenimi veren sosyal bilimler alanında siyaset bilimleri, iktisadi ve idari bilimler, iktisat, hukuk ve işletme fakültelerinden ya da sayılan fakültelerde yer alan denkliği Yükseköğretim Kurulunca kabul edilmiş yurt dışındaki yüksek öğretim kurumlarından mezun olmak.
 - 2) En az dört yıllık lisans öğrenimi veren fakültelerin; mühendislik alanında elektronik, elektrik-elektronik, elektronik ve haberleşme, endüstri, bilgisayar, bilişim sistemleri mühendisliği bölümleri ve fakültelerin istatistik bölümlerinden ya da sayılan bölümlerin denkliği Yükseköğretim Kurulunca kabul edilmiş yurt dışındaki yükseköğretim kurumlarından mezun olmak.
- ç) Kurum tarafından gerekli görüldüğü takdirde, başvuru tarihi itibarıyla son beş yıl içinde YDS’den veya dil yeterliği bakımından bunlara denkliği ÖSYM tarafından kabul edilen ve uluslararası geçerliliği bulunan başka bir belgeye sahip olmak.
- d) Giriş sınavının yapıldığı yılın Ocak ayının birinci günü itibarıyla otuz beş yaşını doldurmamış olmak.

Başvuruda istenecek belgeler ve başvuru şekli

MADDE 7 - (1) Yarışma sınavına katılabilmek için ilânda belirtilen süre içinde elektronik ortamda doldurulacak Kişisel Verileri Koruma Uzman Yardımcılığı Yarışma Sınavı Başvuru Formu ile birlikte aşağıda yer alan belgelerin sınav ilanında belirtilen tarihe kadar Kuruma şahsen veya posta yoluyla teslim edilmesi gerekir:

- a) KPSS sonuç belgesinin aslı veya fotokopisi ya da bilgisayar çıktısı.
- b) Yabancı dil puanını beyan edecekler için sonuç belgesinin aslı veya bilgisayar çıktısı.
- c) Yükseköğrenim diplomasının veya geçici mezuniyet belgesinin aslı veya Kurumca onaylanmış örneği.
- ç) Üç adet vesikalık fotoğraf.

(2) Yurt dışındaki öğrenim kurumlarından mezun olan adayların diploma denkliğinin Yükseköğretim Kurulunca kabul edildiğini gösterir belgenin aslını veya Kurumca onaylı örneğini de başvuru belgelerine eklemeleri gerekir.

Giriş sınavına katılacakların tespit edilmesi

MADDE 8 - (1) Giriş sınavına süresi içinde başvuran adayların başvuruları incelenerek adaylarda aranılan şartların mevcut olup olmadığı Daire Başkanlığı tarafından tespit edilir. Daire Başkanlığınca, aranılan şartları taşıyan adaylar 4 üncü maddede belirtilen usule sıralamaya tabi tutulur. Giriş sınavına katılmaya hak kazanan adaylar, Kurumun internet sitesinde ilan edilir.

Sınav Komisyonu

MADDE 9 - (1) Giriş sınavlarının yapılması, sınav sonuçlarının değerlendirilmesi ve sözlü sınava itirazların incelenerek karara bağlanması ile ilgili çalışmalar, Sınav Komisyonu tarafından yapılır.

(2) Kurul tarafından belirlenecek Sınav Komisyonu, biri başkan olmak üzere beş üyeden oluşur. Asıl üyelerin herhangi bir nedenle Sınav Komisyonuna katılamamaları hâlinde, tespit sırasına göre çalışmalara katılmak üzere ayrıca iki yedek üye belirlenir. Gerek görüldüğünde, en çok iki üye, yükseköğretim kurumları öğretim elemanları arasından seçilebilir.

(3) Komisyon üye tam sayısı ile toplanır ve oy çokluğu ile karar alır.

(4) Giriş Sınav Komisyonu üyeleri kendilerinin, boşanmış olsalar dahi eşlerinin, üçüncü dereceye kadar (bu derece dâhil) kan ve kayın hısımları ile evlatlıklarının katıldıkları sınavlarda görev alamazlar. Bu durumda olanların yerine yedek üyelerden görevlendirme yapılır.

(5) Komisyonun sekretarya hizmetleri Daire Başkanlığınca yürütülür.

Yazılı sınav

MADDE 10 - (1) Yazılı sınav Milli Eğitim Bakanlığı, TODAİE, üniversiteler veya ÖSYM tarafından yapılır. Yazılı sınav, genel kültür ve genel yetenek ile ihtiyaç duyulan uzmanlık alan bilgisi konularından oluşur. Yazılı sınav, test ve/veya klasik usulde yapılır.

(2) Sınav sorularının yüzde 30'unu genel kültür ve genel yetenek, yüzde 70'ini alan bilgisi oluşturur.

(3) Yazılı sınav konuları, uzmanlık alanları dikkate alınmak suretiyle aşağıda sayılan konular arasından ve/veya adayların öğrenim dalına ilişkin bilgi düzeyinin tespitine yönelik konulardan Sınav Komisyonu tarafından seçilerek belirlenir:

- a) Genel kültür ve genel yetenek.
- b) Kişisel verilerin korunması ile ilgili mevzuat: Kişisel Verilerin Korunması Kanunu ve diğer düzenlemeler, kişisel verilerin korunması ile ilgili uluslararası mevzuat ve uygulamalar.
- c) Ayrıca 6 ncı maddenin ikinci fıkrasının (c) bendinin (1) numaralı alt bendinde belirtilen bölümlerden mezun olanlar için yazılı sınav aşağıdaki konuları da kapsayacak şekilde yapılır:
 - 1) Mikro ve makro iktisat.
 - 2) İktisat politikası.
 - 3) Türkiye ekonomisi.
 - 4) Uluslararası iktisat.
 - 5) Kamu maliyesi.
 - 6) Türk vergi sisteminin genel esasları.
 - 7) Maliye politikası.
 - 8) Anayasa hukuku.
 - 9) İdare hukuku ve idari yargılama hukuku.
 - 10) Ceza hukuku.
 - 11) Medeni hukuk.
 - 12) Ticaret hukuku.
 - 13) Borçlar hukuku.
 - 14) Personel yönetimi.

15) Uluslararası İlişkiler ve Siyasi Tarih Grubu: Uluslararası ilişkiler, uluslararası kuruluşlar, Türk dış politikası, siyasi tarih.

ç) Ayrıca 6 ncı maddenin ikinci fıkrasının (c) bendinin (2) numaralı alt bendinde belirtilen bölümlerden mezun olanlar için yazılı sınav aşağıdaki konuları da kapsayacak şekilde yapılır:

1) Temel bilgisayar programlama ve algoritma geliştirme.

2) Bilişim teknolojilerinde temel kavramlar (bilgisayar teknolojileri kavramları, temel bilgisayar ağları ve internet, temel bilgi güvenliği, temel veri tabanı).

3) Yöneylem araştırması, proje yönetimi, simülasyon, rassal modeller.

4) Olasılık, İstatistik.

5) Finansal matematik, maliyet muhasebesi; üstel ve logaritmik fonksiyonlar, diziler, seriler, türev, integral, lineer cebir, diferansiyel denklemler ve bu konuların iktisadi uygulamaları.

6) Yönetim bilişim sistemleri, yönetim ve organizasyon.

7) Yazılım mühendisliği, veri tabanı yönetim sistemleri, veri yapıları ve algoritmalar, bilgisayar ağları ve internet, bilgi güvenliği, işletim sistemleri.

8) Elektronik devreler, sayısal mantık tasarımı, mikro işlemciler, haberleşme, sinyaller ve sistemler.

(4) Yazılı sınavda soruların konu grupları bakımından hangi ağırlıkta değerlendirmeye tabi tutulacağına sınav duyurusunda yer verilir.

(5) Yazılı sınav sonucunda 70 puandan az olmamak üzere en yüksek puandan başlanarak giriş sınavı duyurusunda belirtilen kadronun dört katına kadar aday sözlü sınava girme hakkını kazanır. Yapılan sıralama sonucunda son sıradaki aday ile eşit puana sahip diğer adaylar da sözlü sınava çağrılır.

(6) Yazılı sınav sonuçları Kurumun ve protokol imzalanmış kurumların internet sitesinde sınavın yapıldığı tarihten itibaren en geç 45 gün içerisinde ilân edilir.

Sözlü sınav

MADDE 11 - (1) Sözlü sınav Kurum tarafından yapılır. Sözlü sınavın yeri, günü ve saati ile sınava katılacakların listesi Kurumun internet sitesinde ilân edilir. Adaylara ayrıca bir tebligat yapılmaz.

(2) Sözlü sınavda adaylar, Kişisel Verileri Koruma Uzman Yardımcılığı Yarışma Sınavı Değerlendirme Formu üzerinden;

a) Sınav konularına ilişkin bilgi düzeyi,

- b) Bir konuyu kavrayıp özetleme, ifade yeteneđi ve muhakeme gücü,
 - c) Liyakati, temsil kabiliyeti, davranış ve tepkilerinin mesleđe uygunluđu,
 - ç) Özgüveni, ikna kabiliyeti ve inandırıcılığı,
 - d) Genel yetenek ve genel kültürü,
 - e) Bilimsel ve teknolojik gelişmelere açıklığı,
- yönlerinden değerlendirilerek ayrı ayrı puan verilmek suretiyle gerçekleştirilir.

(3) Adaylar, Sınav Komisyonu tarafından birinci fıkranın (a) bendi için 50, diđer bentlerin her biri için 10 puan üzerinden değerlendirilir. Sözlü sınavda başarılı sayılmak için alınan puanların aritmetik ortalamasının en az 70 olması şarttır.

(4) Sözlü sınav ile ilgili herhangi bir kayıt sistemi kullanılmaz.

(5) Sözlü sınavda başarılı olanlar, başarı puanı en yüksek olan adaydan başlanmak suretiyle Kurumun internet sitesinde ilân edilir.

Giriş sınavı sonuçlarının değerlendirilmesi

MADDE 12 - (1) Yarışma sınavları sonucu puanı en yüksek adaydan başlanarak her bir alan için atama yapılacak kadro sayısı kadar asıl, asıl aday sayısının yarısı kadar da yedek aday belirlenir. Yedek listede yer alan adayların hakları, ilân tarihini takip eden 6 ay için geçerlidir ve daha sonraki sınavlar için müktesep hak veya herhangi bir öncelik teşkil etmez.

(2) Sözlü sınav puanlarının eşitliği halinde sırasıyla yazılı sınav yapılmışsa yazılı sınav puanı, yabancı dil puanı, KPSS puanı, diploma notu yüksek olan aday sıralamada üstte yer alır.

Yarışma sınavı sonuçlarına itiraz

MADDE 13 - (1) Adaylar, sınav sonuçlarına yazılı olarak itiraz edebilirler.

(2) Yazılı sınav sonucuna itirazlar sınav sonuçlarının açıklanmasından itibaren en geç 10 iş günü içinde yazılı sınavı yapan Kuruma yapılır.

(3) Sözlü sınav sonucuna ilişkin itirazlar ise sınav sonuçlarının açıklanmasından itibaren en geç 5 iş günü içinde Kuruma yapılır. Sözlü sınav sonuçlarına itirazlar, sınav komisyonu tarafından en geç 5 iş günü içinde değerlendirilir ve sonucu yazılı olarak ilgiliye bildirilir.

Ataması yapılacaklardan istenilecek belgeler

MADDE 14 - (1) Sınavda başarılı olan adaylar;

- a) Görevini devamlı yapmaya engel olabilecek herhangi bir sağlık sorunu olmadığına dair yazılı beyanını,
 - b) Adli sicil kaydı yazılı beyanını,
 - c) Erkek adaylar için askerlikle ilişkisi olmadığına dair yazılı beyanını,
 - ç) Son üç ay içinde çekilmiş 3 adet vesikalık fotoğrafını,
- sınav sonucunun ilan edildiği tarihi takip eden on gün içerisinde Kuruma teslim ederler.

(2) Gerçeğe aykırı beyanda bulunduğu tespit edilenlerin sınavları geçersiz sayılarak atamaları yapılmaz. Atamaları yapılmış olsa dahi iptal edilir. Bunlar hiçbir hak talep edemezler ve haklarında 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun ilgili hükümleri uygulanmak üzere Cumhuriyet Başsavcılığına suç duyurusunda bulunulur.

Uzman yardımcılığına atanma

MADDE 15 - (1) Giriş sınavını kazananların atama işlemleri, ilgisine göre güvenlik soruşturması ve/veya arşiv araştırması olumlu olması kaydıyla 657 sayılı Kanun hükümlerine göre yapılır. Süresi içinde belgelerini teslim etmeyenlerin atamaları yapılmaz.

(2) Geçerli bir mazereti olmadığı halde atama işlemlerinin yapılması için müracaat etmeyenlerin atama işlemleri yapılmaz.

(3) Yarışma sınavında başarılı olanlardan yasal süresi içinde göreve başlamayanlar, ataması yapıp da herhangi bir sebeple görevden ayrılanlar ile atama şartlarını taşımadığı anlaşılanların yerlerine sınav sonucunun ilanından itibaren (Mülga ibare:RG-2/4/2019-30733) (...) yedek adayların ataması puan üstünlüğüne göre yapılır.

Uzman yardımcılarının eğitimi ve yetiştirilmeleri

MADDE 16 - (1) Uzman yardımcılığı süresi en az üç yıldır. Bu süre içinde aylıksız izin ve toplamı üç ayı aşan hastalık ve refakat izni kullananların yardımcılık süreleri, ayrı kaldıkları süre kadar uzatılır.

(2) Uzman yardımcısı olarak atananlar, bu kadroda buldukları sürece, uzmanlığın gerektirdiği bilgi, beceri ve etik değerleri kazanmaları maksadıyla verilecek görevlerin yanı sıra;

- a) Kurumun teşkilât yapısı, görevleri ve çalışma usûl ve esasları hakkında bilgi ve tecrübe kazanmaya,
- b) Kurumun hizmet sahasına giren konulara ilişkin mevzuata ve bu mevzuatın uygulanmasına ilişkin bilgi ve becerileri kazanmaya,

- c) Yazışma, rapor yazma, inceleme ve araştırma teknikleri konularında gerekli bilgi ve yeteneği kazanmaya,
 - ç) Meslekî konularda ilmî ve teknik çalışma ve araştırma alışkanlığını kazanmaya,
 - d) Meslekî yabancı dil bilgisini geliştirmeye,
 - e) Kurumun hizmet sahası ile ilgili olarak, ulusal ve uluslararası konferans, seminer ve eğitim programlarına iştirake ve temsil kabiliyetini geliştirmeye,
- yönelik çalışmalarda bulunurlar.

(3) Uzman yardımcılarının eğitimi ve yetiştirilmelerinde 657 sayılı Kanun ile 21/2/1983 tarihli ve 83/6061 sayılı Bakanlar Kurulu Kararıyla yürürlüğe konulan Aday Memurların Yetiştirilmelerine İlişkin Genel Yönetmelik hükümleri saklıdır.

ÜÇÜNCÜ BÖLÜM

Uzmanlığa Atanma

Uzmanlığa atanabilmek için aranan şartlar

MADDE 17 - (1) Uzman yardımcıları;

- a) Uzman yardımcısı olarak aylıksız izin ile toplamı üç ayı aşan hastalık ve refakat izinleri hariç en az üç yıl çalışmış olması,
- b) Hazırlayacakları uzmanlık tezinin kabul edilmesi,
- c) Yeterlik sınavında başarılı olması,
- ç) Yeterlik sınavı tarihinde geçerli olan veya yeterlik sınavından itibaren en geç iki yıl içerisinde alınmış bulunan YDS'den asgari (C) düzeyinde puanın veya dil yeterliği bakımından bunlara denkliği kabul edilen ve uluslararası geçerliliği bulunan başka bir belgenin ibraz edilmesi şartıyla uzman olarak atanmaya hak kazanırlar.

(2) Uzmanlık tezi ve yeterlik sınavına ilişkin hizmetler Daire Başkanlığınca yürütülür.

Tez jürisi ve görevleri

MADDE 18 - (1) Tez Jürisi, tez savunmasını gerçekleştirmek üzere, bir Kurul üyesinin başkanlığında, uzman yardımcısının tez danışmanı ile birim yöneticileri, uzmanları ve öğretim üyeleri arasından Kurul tarafından belirlenen beş asıl üyeden oluşur. En çok iki üye yüksek öğretim kurumları öğretim

üyeleri arasından seçilebilir. Asıl üyelerin herhangi bir nedenle savunma komisyonuna katılmamaları hâlinde, tespit sırasına göre çalışmalara katılmak üzere ayrıca iki yedek üye belirlenir.

(2) Tez jürisi, tezi değerlendirmek üzere üye tam sayısı ile toplanır ve oy çokluğu ile karar alır.

Tez konusunun belirlenmesi ve tez hazırlama

MADDE 19 - (1) Daire Başkanlığı tarafından diğer birimlerin görüşleri de alınmak kaydıyla Kurumun ihtiyaçlarına göre tez konuları listesi oluşturulur ve Kurulun onayına sunulur.

(2) Başkan, tez konuları listesinden uzman yardımcısının tercih ettiği üç konudan birini en geç ikinci yılın sonunda belirler.

(3) Tez; öğretim üyesi, birim yöneticisi veya uzmanlar arasından Başkan tarafından seçilecek tez danışmanının gözetiminde bilimsel esaslara uygun olarak hazırlanır.

(4) Belirlenen tez konusu ilk bir ay içinde, uzman yardımcısının talebi ve birim amirinin uygun görmesi hâlinde bir defaya mahsus olmak üzere değiştirilebilir. Tez konusunun değiştirilmesi tezin teslim süresini uzatmaz.

(5) Hazırlanacak tezin uzman yardımcısının görüş, değerlendirme ve önerilerini içeren bilimsel çalışma etiğine uygun özgün bir eser olması gerekir. Tezin daha önce yüksek lisans, doktora tezi veya başka bir amaçla benzer tarzda hazırlanmamış, incelenip savunulmamış ve kullanılmamış olması gerekir. Aksi durumun tespiti halinde tez geçersiz sayılır ve ilgililer hakkında disiplin hükümleri ve cezaî işlemler uygulanır.

(6) Tez; aylıksız izin, toplamda üç ayı aşan hastalık ve refakat izni hariç olmak üzere adaylıkta geçen süre dâhil üç yıl içerisinde hazırlanır.

(7) Tez çalışması, yapılacak bir protokol çerçevesinde bir yükseköğretim kurumunda da yaptırılabilir.

Tezin teslimi

MADDE 20 - (1) Uzman yardımcısı tez konusunun kesinleşmesini takip eden en geç bir yılın sonunda hazırladığı tez ve tez danışmanının değerlendirme raporunu, on iş günü içinde tez jürisindeki üye sayısı kadar çoğaltarak bağlı olduğu birim amirine teslim eder. Birim amirleri tezleri beş iş günü içinde Daire Başkanlığına gönderir ve Başkanlık en kısa sürede jüri üyelerine teslim eder.

(2) Süresi içinde tezlerini sunamayan uzman yardımcılarının altı ayı aşmamak üzere ilave süre verilir.

Tezin değerlendirilmesi ve kabulü

MADDE 21 - (1) Tez jürisi, teslim aldığı tezleri en geç iki ay içinde inceler. Tezi uygun görülen uzman yardımcısı tezini savunmak üzere bir ay içerisinde çağrılır.

(2) Uzman yardımcısı tez jürisi önünde tezini sözlü olarak savunur ve tez konusu ile ilgili soruları cevaplandırır.

(3) Uzman yardımcısının sözlü savunmasından sonra tez jürisi üyeleri oylarını başarılı veya başarısız şeklinde kullanır ve karar oy çokluğu ile alınır.

(4) Tezini teslim ettiği halde geçerli bir mazereti nedeniyle tez savunmasına girememiş olan uzman yardımcısı için ayrı bir savunma tarihi belirlenir. Geçerli bir mazereti olmaksızın savunma toplantısına girmeyen uzman yardımcısı başarısız tez vermiş sayılır.

Tezin kabul edilmemesi

MADDE 22 - (1) Tez jürisi tarafından tezi başarısız kabul edilen uzman yardımcılarının tezlerini sunmaları veya yeni bir tez hazırlamaları için altı ayı aşmamak üzere ilave süre verilir. Bu süre sonunda tezini teslim etmeyen, savunmayan veya ikinci defa tezi başarısız kabul edilenler hakkında 26 ncı madde hükmü uygulanır.

Yeterlik Sınavı Komisyonu

MADDE 23 - (1) Yeterlik Sınavı Komisyonu, bir Kurul üyesinin başkanlığında, birim yöneticileri ve uzmanları ile öğretim üyeleri arasından Kurul tarafından belirlenen beş asıl üyeden oluşur. Aynı usulle başkan ve üyelerin yedekleri de seçilir.

(2) Yeterlik Sınavı Komisyonu üye tam sayısı ile toplanır. Kurulun sekretarya hizmetleri Daire Başkanlığınca yürütülür.

Yeterlik sınavına giriş şartı ve yeterlik sınavı

MADDE 24 - (1) Aylıksız izin ile toplamda üç ayı aşan hastalık ve refakat izni hariç olmak üzere uzman yardımcılığında fiilen en az üç yıl görev yapan ve uzmanlık tezi başarılı kabul edilenler yeterlik sınavına girmeye hak kazanır.

(2) Yeterlik sınavı, Kurum tarafından uygun görülen yer ve tarihte yazılı olarak yapılır.

(3) Yeterlik sınavı, Komisyonca belirlenen Kurumun görev alanına giren ve sınavdan en az iki ay önce ilan edilen konulardan yapılır. Sınavda 100 tam puan üzerinden en az 70 puan alanlar başarılı sayılır.

(4) Yeterlik sınavında başarılı olamayanlar veya sınava girmeye hak kazandığı hâlde geçerli mazereti olmaksızın sınav hakkını kullanmayanlara, bir yıl içinde ikinci kez sınav hakkı verilir.

Uzmanlığa atama

MADDE 25 - (1) Uzman yardımcılarında yeterlik sınavında başarılı olan ve yeterlik sınavı tarihinde geçerli olan veya yeterlik sınavından itibaren en geç iki yıl içerisinde alınmış bulunan YDS'den asgari (C) düzeyinde puanın veya dil yeterliği bakımından bunlara denkliği kabul edilen ve uluslararası geçerliliği bulunan başka bir belgeyi ibraz edenler uzmanlığa atanır.

Uzman yardımcısı unvanının sona ermesi

MADDE 26 - (1) Uzman yardımcılardan;

a) Verilen ilave süre içinde tezlerini sunmayan veya ikinci defa hazırladıkları tezleri de kabul edilmeyenler,

b) İkinci yeterlik sınavında da başarı gösteremeyen veya sınav hakkını kullanmayanlar,

c) Süresi içinde yabancı dil yeterliği şartını yerine getirmeyenler,

Kurumda durumlarına uygun memur unvanlı kadrolara atanırlar.

DÖRDÜNCÜ BÖLÜM

Çeşitli ve Son Hükümler

Görev ve sorumluluk

MADDE 27 - (1) Uzman ve uzman yardımcılarının görev ve sorumlulukları şunlardır:

a) Görevlendirildikleri birimin iş ve işlemlerini yürütmek.

b) Kurumun görev alanına ilişkin olarak politika, strateji ve hedeflerin tespiti maksadıyla araştırma ve incelemeler yapmak.

c) İlgili mevzuatın Kuruma verdiği görevlerin ifası amacıyla yürürlüğe konulan ikincil düzenlemeler ile alınan Kurul kararlarının uygulamalarını izlemek, değerlendirmek ve sonucunda tesis edilecek işlemler ve uygulamalarla ilgili öneriler geliştirmek, yapılacak işler ve alınacak tedbirlerle ilgili tekliflerde bulunmak.

ç) Uluslararası kurum ve kuruluşlar nezdinde yapılacak ve Kurumca uygun görülecek toplantı ve çalışmalara katılmak.

d) Kişisel verilerin korunması uygulamaları konusunda çalışmalarda bulunmak, yeni stratejiler geliştirmek.

- e) Kurumun hizmet kapasite ve kalitelerinin artırılmasına yönelik çalışmalar yapmak, hazırlanmakta olan çalışmalara katılmak.
- f) Kişisel verilerin korunması konusunda ulusal ve uluslararası çalışmaları takip etmek ve Türkiye’de uygulanabilir metotlar üzerinde çalışmalarda bulunmak.
- g) Verilen görevleri mevzuat hükümleri çerçevesinde yerine getirmek.
- h) (Ek:RG-2/4/2019-30733) Yerinde inceleme faaliyetlerine katılmak.

(2) Uzman ve uzman yardımcıları, görevlerini ilgili birim yöneticisine bağlı olarak yürütürler.

Yurt dışında eğitim

MADDE 28 - (1) Uzmanlar, 657 sayılı Kanun ve 21/1/1974 tarihli ve 7/7756 sayılı Bakanlar Kurulu Kararıyla yürürlüğe konulan Yetiştirilmek Amacıyla Yurt Dışına Gönderilecek Devlet Memurları Hakkında Yönetmelik hükümleri çerçevesinde, staj veya araştırma yapmak, meslekî bilgi ve görgülerini artırmak veya yurt dışındaki üniversitelerden kabul belgesi almaları şartıyla akademik çalışma yapmak üzere yurt dışına gönderilebilir.

Yeniden atanma

MADDE 29 - (1) Bu Yönetmelik hükümlerine göre uzman unvanını kazandıktan sonra Kurumdaki görevlerinden çeşitli sebeplerle ayrılıp yeniden atanmak isteyenler, boş kadro olması şartıyla uzman kadrosuna yeniden atanabilirler.

Hüküm bulunmayan haller

MADDE 30 - (1) Bu Yönetmelikte hüküm bulunmayan hallerde, 657 sayılı Kanun, 6698 sayılı Kanun, 18/3/2002 tarihli ve 2002/3975 sayılı Bakanlar Kurulu Kararıyla yürürlüğe konulan Kamu Görevlerine İlk Defa Atanacaklar İçin Yapılacak Sınavlar Hakkında Genel Yönetmelik ile diğer ilgili mevzuat hükümleri uygulanır.

Yürürlük

MADDE 31 - (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 32 - (1) Bu Yönetmelik hükümlerini Başkan yürütür.

Kişisel Verileri Koruma Kurumu Personeli Görevde Yükselme ve Ünvan Değişikliği
Yönetmeliği

Resmi Gazete Tarihi : 05.05.2018

Resmi Gazete Sayısı : 30412

KİŞİSEL VERİLERİ KORUMA KURUMU PERSONELİ GÖREVDE YÜKSELME VE UNVAN
DEĞİŞİKLİĞİ YÖNETMELİĞİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı, liyakat ve kariyer ilkeleri çerçevesinde, hizmet gerekleri ve personel planlaması esas alınarak, Kişisel Verileri Koruma Kurumunda görev yapan personelin görevde yükselme ve unvan değişikliğine ilişkin usul ve esasları belirlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, Kişisel Verileri Koruma Kurumunda 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanununa tabi olarak görev yapan ve bu Yönetmeliğin 5 inci maddesinde sayılan kadrolara görevde yükselme ve unvan değişikliği suretiyle atanacakları kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 657 sayılı Devlet Memurları Kanunu ile 15/3/1999 tarihli ve 99/12647 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan Kamu Kurum ve Kuruluşlarında Görevde Yükselme ve Unvan Değişikliği Esaslarına Dair Genel Yönetmelik hükümlerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Yönetmelikte geçen;

a) Alt görev: 27/9/1984 tarihli ve 3046 sayılı Kanunda belirtilen hiyerarşik kademeler çerçevesinde daha alt hiyerarşi içindeki görevleri,

- b) Aynı düzey görev: Hiyerarşi, görev, yetki ve sorumluluk açısından aynı grupta ya da grup içinde alt gruplar olması halinde aynı alt grupta gösterilen görevleri,
- c) Başkan: Kişisel Verileri Koruma Kurumu Başkanını,
- ç) Daire Başkanlığı: Kurumun insan kaynaklarından sorumlu daire başkanlığını,
- d) Görev grupları: Aynı düzey görevler ile benzer görevlerin yer aldığı grupları,
- e) Görevde yükselme: Bu Yönetmelikte belirlenen görevlere aynı veya başka görev gruplarından yapılacak atamaları,
- f) Görevde yükselme sınavı: 5 inci maddenin birinci fıkrasındaki unvanlara atanacaklar için yapılan yazılı ve sözlü sınavı,
- g) Hizmet süresi: 657 sayılı Kanununun 68 inci maddesinin (B) bendinde sayılan süreleri,
- ğ) İş günü: Ulusal bayram ile genel ve hafta sonu tatili hariç diğer günleri,
- h) Kurum: Kişisel Verileri Koruma Kurumunu,
- ı) Personel: Kurum kadrolarında 657 sayılı Devlet Memurları Kanununa tabi olarak görev yapan Devlet memurlarını,
- i) Unvan değişikliği: En az ortaöğretim düzeyinde mesleki veya teknik eğitim sonucu ihraz edilen unvanlara ilişkin görevlere yapılan atamaları,
- j) Unvan değişikliği sınavı: En az ortaöğretim düzeyinde mesleki veya teknik eğitim sonucu ihraz edilen unvanlara ilişkin görevlere atanabilmek için yapılan yazılı ve sözlü sınavı,
- k) Üst görev: 3046 sayılı Kanunda belirtilen hiyerarşik kademeler çerçevesinde daha üst hiyerarşi içindeki görevleri,
- ifade eder.

İKİNCİ BÖLÜM

Görevde Yükselme ve Unvan Değişikliğine İlişkin Esaslar

Görev grupları

MADDE 5 - (1) Bu Yönetmelik kapsamında görevde yükselmeye tabi kadrolar aşağıda belirtilmiştir.

a) Yönetim hizmetleri grubu:

1) Şube Müdürü.

2) Şef.

b) İdari hizmetler grubu:

1) Veri hazırlama ve kontrol işletmeni, memur.

c) Destek hizmetleri grubu:

1) Hizmetli.

(2) Unvan değişikliğine tabi kadrolar aşağıda belirtilmiştir:

a) Avukat, mühendis, istatistikçi, tekniker, teknisyen, mütercim (tercüman).

Görevde yükselme suretiyle atanacaklarda aranacak genel şartlar

MADDE 6 - (1) Bu Yönetmeliğe tabi kadrolara yapılacak atamalarda aşağıdaki genel şartlar aranır:

a) 657 sayılı Devlet Memurları Kanununun 68 inci maddesinin (B) bendinde belirtilen hizmet süresine sahip olmak.

b) Yapılacak görevde yükselme sınavında başarılı olmak.

c) İlan edilen kadro için aranan şartları sağlayan personel bulunmaması durumu hariç, Kurumda en az 6 ay çalışmış olmak.

Görevde yükselme suretiyle atanacaklarda aranacak özel şartlar

MADDE 7 - (1) Bu Yönetmeliğe tabi kadrolara yapılacak atamalarda aşağıdaki özel şartlar aranır:

a) Şube Müdürü kadrosuna atanabilmek için;

1) En az dört yıllık yükseköğretim kurumlarından mezun olmak,

2) Şef, avukat, mühendis ve istatistikçi kadrolarında en az iki yıl, tekniker, teknisyen, veri hazırlama ve kontrol işletmeni ile memur kadrolarında ise en az beş yıl çalışmış bulunmak,

b) Şef kadrosuna atanabilmek için;

1) En az iki yıllık yüksekokul mezunu olmak,

2) Dört yıl ve üzeri süreli yükseköğrenim mezunu olanların en az dört yıl, dört yıldan daha az süreli yükseköğrenim mezunu olanların ise en az altı yıl hizmeti bulunmak,

3) Veri hazırlama ve kontrol işletmeni veya memur kadrolarının birinde çalışmış bulunmak,

c) Veri hazırlama ve kontrol işletmeni kadrosuna atanabilmek için;

1) En az lise veya dengi okul mezunu olmak,

2) Milli Eğitim Bakanlıđından, yetkili özel eğitim kurumlarından veya yükseköğrenim kurumlarından birinin vermiş olduđu programcılık, işletmenlik, bilgisayar kullanım sertifikasına veya bitirdiđi okul itibarıyla verilen ders müfredatında bilgisayar işletmenliđi ile ilgili ders aldıđına dair belgeye sahip olmak ya da kamu kurum ve kuruluşlarınca düzenlenen aynı mahiyetteki kursta başarılı olmak,

3) Hizmetli kadrosunda en az 2 yıl çalışmış olmak,

ç) Memur kadrosuna atanabilmek için;

1) En az lise veya dengi okul mezunu olmak,

2) Hizmetli kadrosunda en az 2 yıl çalışmış bulunmak,

gerekir.

Unvan deđişikliđi suretiyle atanacaklarda aranacak genel şartlar

MADDE 8 - (1) Unvan deđişikliđi suretiyle atanacakların atanacađı unvanı öğrenim durumu itibarıyla kazanmış olmaları ve yapılacak unvan deđişikliđi sınavında başarılı olmaları şarttır.

Unvan deđişikliđi suretiyle atanacaklarda aranacak özel şartlar

MADDE 9 - (1) Unvan deđişikliđi sınavı sonucu atanacaklarda genel şartların yanında aşağıdaki özel şartlar aranır:

a) Avukat kadrosuna atanabilmek için;

1) Hukuk Fakültesi mezunu olmak,

2) Avukatlık ruhsatına sahip olmak.

b) Mühendis veya istatistikçi kadrolarına atanabilmek için fakülte veya dört yıllık yüksekokulların ilgili bölümlerinden mezun olmak,

c) Mütercim kadrosuna atanabilmek için aşağıdaki şartlar aranır;

1) Fakülte veya dört yıllık yüksekokulların filoloji, mütercimlik (tercümanlık) bölümlerinden veya ilgili diđer bölümlerden mezun olmak,

2) Son başvuru tarihinden önceki 3 yıl içinde, Yabancı Dil Bilgisi Seviye Tespit Sınavında (YDS) en az (B) düzeyinde veya uluslararası geçerliliđi bulunan ve Ölçme, Seçme ve Yerleřtirme Merkezi Başkanlıđınca (ÖSYM) eşdeğerliđi kabul edilen sınavlardan buna denk düzeyde başarılı olduđunu belgelemek.

ç) Tekniker kadrosuna atanabilmek için; en az iki yıl süreli mesleki veya teknik yükseköğretim bölümlerinden mezun olmak.

d) Teknisyen kadrosuna atanabilmek için; lise dengi mesleki veya teknik eğitim öğretim veren okullardan mezun olmak.

ÜÇÜNCÜ BÖLÜM

Görevde Yükselme ve Unvan Değişikliği Sınav Esasları

Duyuru ve başvuru

MADDE 10 - (1) Görevde yükselme veya unvan değişikliği için açılacak sınavlarla ilgili duyuru, Kurumun kadro durumu ile ihtiyaçları göz önüne alınarak, sınavlardan en az otuz gün önce yapılır.

(2) Görevde yükselme veya unvan değişikliği sınavı Kurum intranet veya internet sayfasından personele duyurulur. Duyuruda atama yapılacak boş kadroların sınıfı, unvanı, derecesi ve sayısı, aranacak şartlar, son başvuru tarihi ve diğer hususlar belirtilir ve başvuru süresi beş iş gününden daha az olarak belirlenemez. Bu duyuru üzerine, Kurum personelinin son başvuru tarihi itibarıyla sınav duyurusunda belirtilen şartları taşıyanlar, duyuruda belirtilen kadrolardan yalnızca birine ilişkin sınava katılmak amacıyla ilgili daire başkanlığına müracaat ederler. Aylıksız izinde bulunanlar da dâhil olmak üzere ilgili mevzuatı uyarınca verilmesi zorunlu olan izinleri kullanmakta olan personelin görevde yükselme sınavı ile unvan değişikliği sınavına katılmaları mümkündür.

(3) Görevde yükselme sınavına katılacak adayların duyuruda belirtilen şartları taşımaları gerekir.

(4) İlgili daire başkanlığınca, görevde yükselme sınavına veya unvan değişikliği sınavına katılma talebinde bulunan personelin durumu değerlendirilerek söz konusu sınavlara katılma şartlarını taşıyan ve taşımayan personele ait liste ile diğer hususlar uygun araçlarla, ayrıca Kurum intranet veya internet sayfasında duyurulur. Ayrıca, görevde yükselme sınavı veya unvan değişikliği sınavına katılma şartlarını taşıyan personele yazılı bildirimde bulunulur.

(5) Aday memurların, başvuruları kabul edilmez.

Yazılı sınav

MADDE 11 - (1) Yazılı sınav, bu sınava ilişkin konu başlıklarına duyuruda yer verilmek suretiyle bu Yönetmeliğin 17 nci maddesi uyarınca teşkil edilen sınav kurulu tarafından belirlenecek konularda yapılır. Yazılı sınav Kurumca yapılabileceği gibi, ÖSYM'ye, Milli Eğitim Bakanlığına, Türkiye ve Orta Doğu Amme İdaresi Enstitüsüne veya yükseköğretim kurumlarından birine yaptırılabilir.

(2) Görevde yükselmeye ilişkin yazılı sınav, yüz tam puan üzerinden değerlendirilir. Yazılı sınavda en az altmış puan alanlar başarılı sayılır.

(3) Sınavlara her ne sebeple olursa olsun girmeyenler haklarını kaybetmiş sayılır. Sınavda kopya çekenler, kopya verenler veya bunlara teşebbüs edenler, sınav kâğıtlarına belirtici işaret koyanlar sınav salonundan çıkarılır ve düzenlenecek bir tutanakla sınav kâğıtları geçersiz sayılır. Ayrıca, sınava girecek aday yerine başka bir kişinin sınava girdiğinin anlaşılması halinde, ilgililerin sınavı bir tutanakla belirlenerek geçersiz sayılır. Bu kişiler hakkında disiplin hükümlerine ve genel hükümlere göre işlem yapılır.

Sözlü sınav

MADDE 12 - (1) Yazılı sınavda başarılı olanlardan en yüksek puan alan adaydan başlamak üzere ilan edilen kadro sayısının beş katına kadar aday sözlü sınava alınır. Son adayla aynı puana sahip olan personelin tamamı sözlü sınava alınır.

(2) İlgili personel, Sınav Kurulunun her bir üyesi tarafından;

- a) Sınav konularına ilişkin bilgi düzeyi,
- b) Bir konuyu kavrayıp özetleme, ifade yeteneği ve muhakeme gücü,
- c) Liyakati, temsil kabiliyeti, tutum ve davranışlarının göreve uygunluğu,
- ç) Özgüveni, ikna kabiliyeti ve inandırıcılığı,
- d) Genel kültürü ve genel yeteneği,
- e) Bilimsel ve teknolojik gelişmelere açıklığı,

esas alınarak yüz tam puan üzerinden değerlendirilir. Her bir Sınav Kurulu üyesinin vermiş olduğu puanların aritmetik ortalaması alınarak personelin sözlü sınav puanı tespit edilir. Sözlü sınavda yüz üzerinden en az yetmiş puan alanlar başarılı sayılır.

Başarı sıralaması

MADDE 13 - (1) Görevde yükselme suretiyle ilan edilen boş kadro sayısı kadar atama yapılmasında başarı puanı esas alınır. Başarı puanı, yazılı ve sözlü sınav puanlarının aritmetik ortalaması esas alınmak suretiyle tespit edilir ve Kurumun intranet veya internet sayfasında ilan edilir. Başarı puanlarının eşit olması halinde sırasıyla; hizmet süresi fazla olanlara, daha üst öğrenimi bitirmiş olanlara, üst öğrenim mezuniyet notu yüksek olanlara öncelik verilmek suretiyle, en yüksek puandan başlamak üzere başarı sıralaması belirlenir.

(2) Görevde yükselme sınavında başarılı olmalarına rağmen, ilan edilen kadro sayısı nedeniyle ataması yapılamayacak personelden en fazla asıl aday sayısı kadar personel, Kurumca ihtiyaç duyulması halinde ve sınav duyurusunda da belirtilmek şartıyla başarı sıralaması listesinde yedek olarak belirlenebilir.

Sınav sonuçlarına itiraz

MADDE 14 - (1) İlgililer, sınav sonuçlarının ilanından itibaren beş iş günü içerisinde Sınav Kuruluna itiraz edebilirler. İtirazlar, itiraz süresinin bitiminden itibaren Sınav Kurulunca en geç on beş iş günü içinde değerlendirilir ve sonuç ilgiliye yazılı olarak bildirilir.

(2) Yapılan sınavlarda hatalı sorulara tekabül eden puanlar eşit şekilde diğer sorulara dağıtılır. Ancak, soruların yüzde onundan fazlasının hatalı olduğunun birinci fıkrada belirtilen süre içinde yapılan itirazlar üzerine veya herhangi bir şekilde tespit edilmesi halinde, sınav iptal edilir ve en kısa sürede yeni sınav yapılır.

(3) Kesin başarı listesi, sınav sonuçlarının ilk ilanından sonra beş iş günü içerisinde itiraz olmaması halinde takip eden iş günü, itiraz olması halinde söz konusu itirazın Sınav Kurulunca değerlendirilmesini müteakip ilan edilir.

Sınavı kazananların atanması

MADDE 15 - (1) Atanmaya hak kazanan personel, başarı sıralaması listesinin kesinleşmesini müteakip en yüksek puandan başlamak üzere belirlenen başarı sıralamasındaki başarı puanlarına göre atanır.

(2) Duyurulan kadrolardan;

a) Atanma şartlarını taşımadıkları için sınavlarının geçersiz sayılması veya bu sebeple atamalarının iptal edilmesi, atanılan göreve geçerli bir mazeret olmaksızın süresi içinde başlanmaması ya da atanma hakkından vazgeçilmesi,

b) Emeklilik, ölüm, memurluktan çekilme veya çıkarılma, başka unvanlı kadrolara ya da başka bir kuruma naklen atanma,

sebepleriyle boş kalan veya boşalan kadrolara, başarı sıralamasının kesinleştiği tarihten itibaren altı aylık süreyi aşmamak üzere aynı unvanlı kadrolar için yapılacak müteakip sınava ilişkin duyuruya kadar, 13 üncü maddeye göre belirlenmiş olması halinde yedekler arasından başarı sıralamasına göre atamaları yapılabilir.

(3) Sınavda başarılı olanlardan, atanma şartlarını taşımadıkları sonradan anlaşılanların sınavları geçersiz sayılarak atamaları yapılmaz. Atamaları yapılanların ise atamaları iptal edilir. Görevden uzaklaştırılanların, göreve iade edilinceye kadar atamaları yapılmaz.

(4) Görevde yükselme sınavına herhangi bir sebeple katılmayanlar ile başarısız olan veya yedeklerden altı ay içindeki müteakip sınava ilişkin duyuruya kadar atanmamış olanlar ya da atanma haklarından herhangi bir sebeple feragat edenler, aynı unvanlı kadroya yapılacak atamalar için bu Yönetmelikte öngörülen bütün usul ve esaslara tabidir.

Unvan değişikliği sınavı

MADDE 16 - (1) 5 inci maddenin ikinci fıkrasında belirtilen unvan değişikliğine tabi kadrolara, bu unvanları en az ortaöğretim düzeyinde mesleki veya teknik eğitim sonucu ihraz etmiş bulunan personelin atanması, bu Yönetmelikte belirtilen usul ve esaslar çerçevesinde yapılacak unvan değişikliği sınavı sonucundaki başarısına göre gerçekleştirilir.

(2) Unvan değişikliği sınavları, Başkanca belirlenecek görev alanları ve atama yapılacak görevin niteliğine ilişkin konularda yaptırılır ve bu sınavlara katılacaklarda, Kurumda veya öğrenim durumları ile ilgisi bulunmayan görevlerde belirli süre hizmet yapmış olma şartı aranmaz. Unvan değişikliği sınavı kapsamındaki görevlere, sadece Kurum personeli başvurabilir.

(3) Unvan değişikliği yazılı sınavında yüz puan üzerinden en az altmış, sözlü sınavında ise en az yetmiş puan alanlar başarılı sayılır.

(4) Bu Yönetmelik kapsamındaki personelden doktora öğrenimini bitirmiş olanlar, unvan değişikliği sınavına katılmaksızın öğrenimle ihraz edilen görevlere atanabilirler.

Sınav kurulu ve görevleri

MADDE 17 - (1) Görevde yükselme veya unvan değişikliği sınavlarını yürütmek üzere sınav kurulu teşkil edilir. Sınav kurulu, Başkan veya görevlendireceği başkan yardımcısının başkanlığında, aralarında Kurumun ilgili daire başkanının da bulunduğu toplam beş asıl ve üç yedek üyeden oluşur. Sınav kurulunu teşkil eden üyeler sınavlara alınacak personelden öğrenim ve ihraz ettikleri unvanlar itibarıyla daha düşük seviyede olamazlar. Sınavlara, sınav kurulunun başkan ve üyeleri, üçüncü dereceye kadar kan ve ikinci dereceye kadar kayın hısımlarının, evlatlıklarının ve aralarındaki evlilik bağı kalkmış olsa bile eşlerinin sınava katıldığı tespit edilmesi halinde, sınav kurulu üyesi olarak görev yapamazlar. Bu hallerde yerlerine yedek üye veya üyeler görevlendirilir.

(2) Sınav kurulu; sınavların yapılması, sınav sonuçlarının ilanı, itirazların sonuçlandırılması ve sınavlara ilişkin diğer işleri yürütür.

(3) Sınav kurulu üye tam sayısı ile toplanır ve kararlar oy çokluğu ile alınır. Oylamada çekimser oy kullanılamaz. Asil üyelerin bulunmadığı toplantılara yedek üyeler katılır.

(4) Sınav kurulunun sekreteryaya hizmetleri Daire Başkanlığınca yürütülür.

DÖRDÜNCÜ BÖLÜM

Çeşitli ve Son Hükümler

Gruplar arası geçişler

MADDE 18 - (1) 5 inci maddede belirtilen görev grupları ve görevler arasındaki geçişler aşağıdaki esaslar çerçevesinde yapılır:

a) Gruplar arası görevde yükselme niteliğindeki geçişler ve alt görevden üst göreve geçişler görevde yükselme sınavına tabidir.

b) Aynı ana hizmet grubunun alt hizmet grubunda yer alanlar, aynı alt grubun kendi içinde kalmak ve atanılacak kadronun gerektirdiği şartları taşımak kaydıyla, görevde yükselme sınavına tabi tutulmadan aynı hiyerarşik düzeydeki diğer görevlere atanabilirler.

c) Kurumda veya diğer kamu kurum ve kuruluşlarında daha önce bulunulan görevler ile bu görevlerle aynı düzey görevlere veya daha alt görevlere, personelin talep etmesi ve bu Yönetmelikte aranan öğrenim ile hizmetin yerine getirilmesi için gerekli sertifika, ehliyet ve benzeri belgelere sahip olma şartlarını taşıması kaydıyla görevde yükselme sınavına tabi tutulmadan atama yapılabilir.

ç) Unvan değişikliğine tabi kadrolar ile bu kadrolar arasındaki geçişler, ilgili kadro için düzenlenen unvan değişikliği sınavı sonucuna göre yapılır.

d) Bu Yönetmelik kapsamında bulunan ve doktora öğrenimini bitiren personelden, atanılacak görev için aranan ve 6 ncı maddeye göre hesaplanan toplam hizmet süresine sahip olmaları ve mevzuatla aranan öğrenim şartını taşımaları kaydıyla uzman veya aynı düzeydeki görevler ile daha alt görevlere atanmalarında bu Yönetmelik hükümleri uygulanmaz.

e) Avukat kadrosundan hukuk müşaviri kadrosuna yapılacak atamalarda bu Yönetmelik hükümleri uygulanmaz.

Naklen atamalar

MADDE 19 - (1) Dięer kamu kurum ve kuruluřlarının personelinden bu Yönetmelikte sayılan unvanları ihraz etmiş olanlar, Kurumdaki aynı unvana veya bu unvanın bulunduęu aynı alt gruptaki dięer unvanlara veya daha alt unvanlara; atanacakları unvan için bu Yönetmelikte öngörölen sınavda başarılı olma dıřındaki dięer řartları taşımaları kaydıyla genel hükümlere göre naklen atanabilirler.

Sınav belgelerinin saklanması

MADDE 20 - (1) Sınavlarda başarılı olan personelin sınavla ilgili belgeleri özlük dosyalarında; başarı gösteremeyenlerin belgeleri ise en az bir yıl veya müteakip sınava ve dava konusu olan sınav belgeleri ise yargı kararı kesinleşinceye kadar genel hükümlere göre ilgili daire başkanlığınca saklanır.

Kazanılmış haklar

MADDE 21 - (1) Bu Yönetmelik kapsamına giren unvanları, ilgili mevzuatı uyarınca kazananların hakları saklıdır.

Hüküm bulunmayan haller

MADDE 22 - (1) Bu Yönetmelikte hüküm bulunmayan hallerde; 657 sayılı Devlet Memurları Kanunu ile Kamu Kurum ve Kuruluşlarında Görevde Yükselme ve Unvan Deęişikliği Esaslarına Dair Genel Yönetmelik hükümleri uygulanır.

Yürürlük

MADDE 23 - (1) Bu Yönetmelik yayımı tarihinde yürürlüęe girer.

Yürütme

MADDE 24 - (1) Bu Yönetmelik hükümlerini Başkan yürütür.

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

Resmî Gazete Tarihi : 28.10.2017

Resmî Gazete Sayısı : 30224

KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VEYA ANONİM HALE GETİRİLMESİ HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasları belirlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik hükümleri; 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununun 7 nci maddesi uyarınca veri sorumluları hakkında uygulanır.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 6698 sayılı Kanunun 7 nci maddesinin üçüncü fıkrası ile 22 nci maddesinin birinci fıkrasının (e) bendine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Yönetmeliğin uygulanmasında;

- a) Alıcı grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini,
- b) İlgili kullanıcı: Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişileri,
- c) İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,
- ç) Kanun: 24/3/2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanununu,

d) Kayıt ortamı: Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı,

e) (Değişik:RG-28/4/2019-30758) Kişisel veri işleme envanteri: Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri,¹⁰

f) Kişisel veri saklama ve imha politikası: Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikayı,

g) Kurul: Kişisel Verileri Koruma Kurulunu,

ğ) Periyodik imha: Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemini,

h) Sicil: Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicilini,

ı) Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,

i) Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,

ifade eder.

(2) Bu Yönetmelikte yer almayan tanımlar için Kanundaki tanımlar geçerlidir.

İKİNCİ BÖLÜM

Kişisel Veri Saklama ve İmha Politikası

Kişisel veri saklama ve imha politikasına ilişkin esaslar

¹⁰ Değişiklik öncesi: “Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri,”

MADDE 5 - (1) Kanununun 16 ncı maddesi gereğince Veri Sorumluları Siciline kayıt olmakla yükümlü olan veri sorumluları, kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası hazırlamakla yükümlüdür.

(2) Kişisel veri saklama ve imha politikası hazırlanmış olması; kişisel verilerin Kanuna ve Yönetmeliğe uygun biçimde saklandığı, silindiği, yok edildiği veya anonim hale getirildiği anlamına gelmez.

(3) Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü altında bulunmayan veri sorumlularının, Kanun ve bu Yönetmelik uyarınca kişisel verileri saklama, silme, yok etme veya anonim hale getirme yükümlülükleri devam eder.

Kişisel veri saklama ve imha politikasının kapsamı

MADDE 6 - (1) Kişisel veri saklama ve imha politikası asgari olarak;

- a) Kişisel veri saklama ve imha politikasının hazırlanma amacına,
- b) Kişisel veri saklama ve imha politikası ile düzenlenen kayıt ortamlarına,
- c) Kişisel veri saklama ve imha politikasında yer verilen hukuki ve teknik terimlerin tanımlarına,
- ç) Kişisel verilerin saklanması ve imhasını gerektiren hukuki, teknik ya da diğer sebeplere ilişkin açıklamaya,
- d) Kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için alınmış teknik ve idari tedbirlere,
- e) Kişisel verilerin hukuka uygun olarak imha edilmesi için alınmış teknik ve idari tedbirlere,
- f) Kişisel verileri saklama ve imha süreçlerinde yer alanların unvanlarına, birimlerine ve görev tanımlarına,
- g) Saklama ve imha sürelerini gösteren tabloya,
- ğ) Periyodik imha sürelerine,
- h) Mevcut kişisel veri saklama ve imha politikasında güncelleme yapılmış ise söz konusu değişikliğe, ilişkin bilgileri kapsar.

ÜÇÜNCÜ BÖLÜM

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi

İlkeler

MADDE 7 - (1) Kanunun 5 inci ve 6 ncı maddelerinde yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin veri sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekir.

(2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Kanunun 4 üncü maddesindeki genel ilkeler ile 12 nci maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve kişisel veri saklama ve imha politikasına uygun hareket edilmesi zorunludur.

(3) Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

(4) (Değişik:RG-28/4/2019-30758) Veri sorumlusu, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemiyle ilgili uyguladığı yöntemleri ilgili politika ve prosedürlerinde açıklamakla yükümlüdür.¹¹

(5) Veri sorumlusu, Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçer. İlgili kişinin talebi halinde uygun yöntemi gerekçesini açıklayarak seçer.

Kişisel verilerin silinmesi

MADDE 8 - (1)Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

(2) Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Kişisel verilerin yok edilmesi

MADDE 9 - (1) Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

(2) Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Kişisel verilerin anonim hale getirilmesi

¹¹ Değişiklik öncesi: “Veri sorumlusu, kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesi işlemiyle ilgili uyguladığı yöntemleri ilgili politika ve prosedürlerinde açıklamakla yükümlüdür.”

MADDE 10 - (1) Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

(2) Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

(3) Veri sorumlusu, kişisel verilerin anonim hale getirilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Kişisel verileri resen silme, yok etme veya anonim hale getirme süreleri

MADDE 11 - (1) Kişisel veri saklama ve imha politikası hazırlamış olan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.

(2) Periyodik imhanın gerçekleştirileceği zaman aralığı, veri sorumlusu tarafından kişisel veri saklama ve imha politikasında belirlenir. Bu süre her halde altı ayı geçemez.

(3) Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden üç ay içinde, kişisel verileri siler, yok eder veya anonim hale getirir.

(4) Kurul, telafisi güç veya imkansız zararların doğması ve açıkça hukuka aykırılık olması halinde, bu maddede belirlenen süreleri kısaltabilir.

Kişisel verileri ilgili kişinin talep etmesi durumunda silme ve yok etme süreleri

MADDE 12 - (1) İlgili kişi, Kanunun (Değişik ibare:RG-28/4/2019-30758) 11 inci ve 13 üncü maddelerine istinaden veri sorumlusuna başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;¹²

a) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Veri sorumlusu, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir.

¹² Değişiklik öncesi: "13 üncü".

b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa veri sorumlusu bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde bu Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.

c) Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep veri sorumlusunca Kanununun 13 üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

DÖRDÜNCÜ BÖLÜM

Çeşitli ve Son Hükümler

Tereddütlerin giderilmesi

MADDE 13 - (1) Bu Yönetmeliğin uygulanması sırasında doğacak tereddütleri ve uygulamaya ilişkin aksaklıkları gidermeye ve uygulamayı yönlendirmeye, ilke ve standartları belirlemeye ve uygulama birliğini sağlayacak gerekli düzenlemeleri yapmaya, bu hususta gerekli her türlü bilgi ve belgeyi istemeye, bu Yönetmelikte yer almayan konularda ilgili mevzuat hükümleri çerçevesinde karar vermeye Kurul yetkilidir.

Yürürlük

MADDE 14 - (1) Bu Yönetmelik 1/1/2018 tarihinde yürürlüğe girer.

Yürütme

MADDE 15 - (1) Bu Yönetmelik hükümlerini Başkan yürütür.

Yönetmeliğin Yayınlandığı Resmî Gazete'nin		
1.	Tarihi	Sayısı
	28/10/2017	30224
	Yönetmelikte Değişiklik Yapan Yönetmeliklerin Yayınlandığı Resmî Gazetelerin	
	Tarihi	Sayısı
	28/4/2019	30758
2.		

Veri Sorumluları Sicili Hakkında Yönetmelik

Resmî Gazete Tarihi : 30.12.2017

Resmî Gazete Sayısı : 30286

VERİ SORUMLULARI SİCİLİ HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca Kurulun gözetiminde, Başkanlık tarafından kamuya açık olarak tutulacak olan Veri Sorumluları Sicilinin oluşturulması, idaresi ile Veri Sorumluları Siciline yapılması öngörülen kayıtlara ilişkin usul ve esasları belirlemek ve uygulanmasını sağlamaktır.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişileri kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 6698 sayılı Kanununun 16 ncı maddesinin beşinci fıkrası ile 22 nci maddesinin birinci fıkrasının (d) ve (e) bentlerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Yönetmelikte geçen;

- a) Alıcı grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini,
- b) Başkan: Kişisel Verileri Koruma Kurumu Başkanını,
- c) Başkanlık: Kişisel Verileri Koruma Kurumu Başkanlığını,
- ç) **(Değişik:RG-28/4/2019-30758)** İrtibat kişisi: Türkiye’de yerleşik olan gerçek ve tüzel kişiler için veri sorumlusu tarafından, Türkiye’de yerleşik olmayan gerçek ve tüzel kişiler için de veri sorumlusu temsilcisi tarafından, Kanun ve bu Kanuna dayalı olarak çıkarılacak ikincil düzenlemeler

kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile iletişimi sağlamak amacıyla Sicile kayıt esnasında bildirilen gerçek kişiyi,¹³

d) Kanun: 6698 sayılı Kişisel Verilerin Korunması Kanununu,

e) Kayıt: Kayıt yükümlülüğü altında bulunan veri sorumlularının Yönetmelik ile belirlenen usul ve esaslara uygun olarak yaptığı bildirimini,

f) Kayıt yükümlülüğü: Yönetmelik uyarınca gerçekleştirilmesi gereken kayıt ile ilgili yükümlülüğü,

g) Kayıtlı elektronik posta (KEP) adresi: Elektronik iletilerin, gönderimi ve teslimatı da dâhil olmak üzere kullanımına ilişkin olarak hukuki delil sağlayan, elektronik postanın nitelikli şeklini,

ğ) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

h) (Değişik:RG-28/4/2019-30758) Kişisel veri işleme envanteri: Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri,¹⁴

ı) Kişisel veri saklama ve imha politikası: Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikayı,

i) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

j) Kurul: Kişisel Verileri Koruma Kurulunu,

k) Kurum: Kurul ve Başkanlıktan oluşan Kişisel Verileri Koruma Kurumunu,

¹³ Değişiklik öncesi: "Türkiye'de yerleşik olan tüzel kişiler ile Türkiye'de yerleşik olmayan tüzel kişi veri sorumlusu temsilcisinin Kanun ve bu Kanuna dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile kurulacak iletişim için veri sorumlusu tarafından Sicile kayıt esnasında bildirilen gerçek kişiyi,"

¹⁴ Değişiklik öncesi "Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri,"

- l) Sicil: Başkanlık tarafından tutulan Veri Sorumluları Sicilini,
- m) Veri kategorisi: Kişisel verilerin ortak özelliklerine göre gruplandırıldığı veri konusu kişi grubu veya gruplarına ait kişisel veri sınıfını,
- n) Veri konusu kişi grubu: Veri sorumlularının kişisel verilerini işledikleri ilgili kişi kategorisini,
- o) Veri sorumluları sicil bilgi sistemi (VERBİS): Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemini,
- ö) Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,
- p) **(Değişik:RG-28/4/2019-30758)** Veri sorumlusu temsilcisi: Türkiye’de yerleşik olmayan veri sorumlularını bu Yönetmeliğin 11 inci maddesinin üçüncü fıkrasında belirtilen konularda asgari temsile yetkili Türkiye’de yerleşik tüzel kişi ya da Türkiye Cumhuriyeti vatandaşı gerçek kişiyi,¹⁵ ifade eder.

(2) Bu Yönetmelikte yer almayan tanımlar için Kanundaki tanımlar uygulanır.

İKİNCİ BÖLÜM

Sicilin Oluşturulması, İdaresi, Gözetimi ve Sicile Erişim

İlke, usul ve esaslar

MADDE 5 - (1) Sicilin oluşturulması, idaresi ve gözetimi hususunda aşağıdaki ilke, usul ve esaslara uyulur:

- a) Veri sorumluları, kişisel veri işlemeye başlamadan önce Sicile kaydolmak zorundadır.
- b) Türkiye’de yerleşik olmayan veri sorumluları, veri işlemeye başlamadan önce veri sorumlusu temsilcisi marifetiyle Sicile kaydolmak zorundadır.
- c) Sicil kamuya açık biçimde tutulur. Kurul, kamuya açıklık ilkesinin sağlanması şartıyla, bu ilkenin kapsamı ve istisnalarını belirleme yetkisini haizdir.

¹⁵ Değişiklik öncesi “Türkiye’de yerleşik olmayan veri sorumlularını bu Yönetmeliğin 11 inci maddesinin ikinci fıkrasında belirtilen konularda asgari temsile yetkili Türkiye’de yerleşik tüzel kişi ya da Türkiye Cumhuriyeti vatandaşı gerçek kişiyi,”

ç) (Değişik:RG-28/4/2019-30758) Sicile kayıtla yükümlü olan veri sorumluları, Kişisel Veri İşleme Envanteri hazırlamakla yükümlüdür. Sicil başvurularında Sicile açıklanacak bilgiler Kişisel Veri İşleme Envanterine dayalı olarak hazırlanır.¹⁶

d) Kanunun 10 uncu maddesinde veri sorumluları için belirtilen aydınlatma yükümlülüğünde, Kanunun 13 üncü maddesinde belirtilen ilgili kişi başvurularının yanıtlanmasında ve ilgili kişiler tarafından açıklanacak açık rızanın kapsamının belirlenmesinde kişisel veri işleme envanterine dayalı olarak Sicile sunulan ve Sicilde yayınlanan bilgiler esas alınır.

e) Veri sorumluları, Sicile sunulan ve Sicilde yayınlanan bilgilerin eksiksiz, doğru, güncel ve hukuka uygun olmasından sorumludur. Veri sorumlularının Sicile kaydolması Kanun kapsamındaki diğer yükümlülüklerini ortadan kaldırmaz.

f) Kanunun 28 inci maddesinde belirtilen durumlar saklı kalmak kaydıyla Yönetmeliğin 16 ncı maddesinde belirtilen objektif kriterlere dayalı olarak belirli şartları taşıyan veri sorumlularının Kurul tarafından Sicile kayıtla yükümlü tutulmaması; bu veri sorumlularının Kanun kapsamındaki yükümlülüklerini ortadan kaldırmaz.

g) Sicile ilişkin işlemler, veri sorumluları tarafından VERBİS üzerinden gerçekleştirilir.

ğ) (Değişik:RG-28/4/2019-30758) Veri sorumluları tarafından Sicile sunulan ve Sicilde yayınlanan kişisel verilerin işlendikleri amaç için gerekli olan azami muhafaza edilme süresi; Kanunun 7 nci maddesinde belirtilen veri sorumlularının silme, yok etme veya anonim hale getirme yükümlülüklerinin yerine getirilmesinde esas alınır.¹⁷

Sicilin oluşturulması, idaresi ve gözetimi

MADDE 6 - (1) Sicil, Başkanlık tarafından oluşturulur. Başkanlık, Sicilin oluşturulması, idaresi, güncel biçimde tutulması ve muhafaza edilmesi amacıyla; VERBİS'in kurulması ve işletilmesi için gerekli teknik ve idari tedbirleri alır.

(2) Sicilin oluşturulmasından ve idaresinden sorumlu hizmet birimi, Veri Yönetimi Dairesi Başkanlığıdır.

¹⁶ Değişiklik öncesi: "Sicil başvurularında Sicile açıklanacak bilgiler Kişisel Veri İşleme Envanterine dayalı olarak hazırlanır."

¹⁷ Değişiklik öncesi "Veri sorumluları tarafından Sicile sunulan ve Sicilde yayınlanan kişisel verilerin işlendikleri amaç için gerekli olan azami süre; Kanunun 7 nci maddesinde belirtilen veri sorumlularının silme, yok etme veya anonim hale getirme yükümlülüklerinin yerine getirilmesinde esas alınır."

(3) Sicilin gözetimi Kurul tarafından gerçekleştirilir. Veri Yönetimi Dairesi Başkanlığı tarafından üç aylık dönemler halinde hazırlanan ve kapsamı Kurul tarafından belirlenecek olan faaliyet raporu Kurula sunulur.

Sicile erişim

MADDE 7 - (1) Başkanlık, Sicilde yer alan güncel bilgileri Kurul kararları uyarınca belirlenecek uygun yöntemlerle kamuya açıklar.

(2) Veri sorumluları sicilinde yer alan bilgilerden aşağıdakiler kamuya açıklanır:

- a) (**Değişik:RG-28/4/2019-30758**) Veri sorumlusu, varsa veri sorumlusu temsilcisi, adresi ve alınmış olması halinde KEP adresi,¹⁸
- b) Kişisel verilerin hangi amaçlarla işlenebileceği,
- c) Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri,
- ç) Kişisel verilerin aktarılabilmesi için alıcı ve alıcı grupları,
- d) Yabancı ülkelere aktarımı öngörülen kişisel veriler,
- e) Sicile kayıt tarihi ile kaydın sona erdiği tarih,
- f) Kişisel veri güvenliğine ilişkin alınan tedbirler,
- g) Kişisel verilerin işlendikleri amaç için gerekli olan azami süre.

ÜÇÜNCÜ BÖLÜM

Kayıt Yükümlülüğünün Başlangıcı, VERBİS'e Girilecek Bilgiler, Kayıt Başvurusu,

Kaydın Yenilenmesi ve Silinmesi

Kayıt yükümlülüğünün başlangıcı

MADDE 8 - (1) Veri sorumluları, kişisel veri işlemeye başlamadan önce Sicile kayıt yükümlülüklerini yerine getirmek zorundadır.

(2) Kayıt yükümlülüğü altında bulunmayan, sonradan kayıt yükümlüsü haline gelen veri sorumluları, yükümlülük altına girmelerini müteakip otuz gün içerisinde Sicile kaydolurlar.

(3) Kayıt yükümlülüğü altında bulunan veri sorumluları, herhangi bir fiili, teknik ya da hukuki imkânsızlık nedeniyle kayıt yükümlülüklerinin yerine getirilememesi halinde, bu imkânsızlığın

¹⁸ Değişiklik öncesi "a) Veri sorumlusu, varsa veri sorumlusu temsilcisi ve irtibat kişinin adı, adresi ve alınmış olması halinde KEP adresi,".

ortaya çıktığı tarihten itibaren en geç 7 iş günü içerisinde Kuruma yazılı olarak başvurmak ve gerekçesini belirtmek şartıyla, kayıt yükümlülüklerini yerine getirmek için Kurumdan ek süre talep edebilirler. Kurum, bir defaya mahsus olmak ve her halde otuz günü geçmemek üzere ek süre verebilir.

Kayıt yükümlülüğü kapsamında iletilecek bilgiler

MADDE 9 - (1) Sicile yapılan kayıt başvurusu aşağıdaki bilgileri içerir:

- a) Veri sorumlusu, varsa veri sorumlusu temsilcisi ve irtibat kişisine ait kimlik ve adres bilgilerine ilişkin Kurul tarafından belirlenecek başvuru formunda yer alan bilgiler,
- b) Kişisel verilerin hangi amaçla işleneceği,
- c) Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar,
- ç) Kişisel verilerin aktarılabilmesi için alıcı veya alıcı grupları,
- d) Yabancı ülkelere aktarımı öngörülen kişisel veriler,
- e) Kanunun 12 nci maddesinde öngörülen ve Kurul tarafından belirlenen kriterlere göre alınan tedbirler,
- f) Kişisel verilerin mevzuatta öngörülen veya işlendikleri amaç için gerekli olan azami muhafaza edilme süresi.

(2) Veri sorumluları tarafından birinci fıkranın (b), (c), (ç) ve (d) bentleri uyarınca Sicile açıklanacak bilgiler; Kişisel Veri İşleme Envanterine dayalı olarak VERBİS'te belirtilen başlıklar kullanılarak VERBİS üzerinden Sicile iletilir.

(3) Veri sorumluları tarafından birinci fıkranın (e) bendi uyarınca Sicile açıklanacak bilgiler; Kanunun 12 nci maddesinde belirtilen hususları kapsayacak şekilde VERBİS'te belirtilen başlıklar kullanılarak VERBİS üzerinden Sicile iletilir.

(4) Veri sorumluları tarafından birinci fıkranın (f) bendi uyarınca Sicile açıklanacak kişisel verilerin mevzuatta öngörülen veya işlendikleri amaç için gerekli olan azami muhafaza edilme süresine ilişkin bilgiler veri kategorileri ile eşleştirilerek Sicile bildirilir. Veri sorumlusu tarafından Sicile bildirilen veri kategorilerinin işleme amaçları ve bu amaçlara dayalı olarak işlenmeleri için gerekli olan azami muhafaza edilme süreleri ile mevzuatta öngörülen süreler farklı olabilir. Bu durumda mevzuatta azami muhafaza edilme süresi öngörülmemişse öngörülen bu süre yoksa bunlardan en uzun süre esas alınarak bu veri kategorisi için Sicile bildirim yapılır. Kişisel verilerin işlendikleri amaç için gerekli olan azami muhafaza edilme süresi belirlenirken;

- a) İlgili veri kategorisinin işlenme amacı kapsamında veri sorumlusunun faaliyet gösterdiği sektörde genel teamül gereği kabul edilen süre,
- b) İlgili veri kategorisinde yer alan kişisel verinin işlenmesini gerekli kılan ve ilgili kişiyle tesis edilen hukuki ilişkinin devam edeceği süre,
- c) İlgili veri kategorisinin işlenme amacına bağlı olarak veri sorumlusunun elde edeceği meşru menfaatin hukuka ve dürüstlük kurallarına uygun olarak geçerli olacağı süre,
- ç) İlgili veri kategorisinin işlenme amacına bağlı olarak saklanması yaratacağı risk, maliyet ve sorumlulukların hukuken devam edeceği süre,
- d) Belirlenecek azami sürenin ilgili veri kategorisinin doğru ve gerektiğinde güncel tutulmasına elverişli olup olmadığı,
- e) Veri sorumlusunun hukuki yükümlülüğü gereği ilgili veri kategorisinde yer alan kişisel verileri saklamak zorunda olduğu süre,
- f) Veri sorumlusu tarafından, ilgili veri kategorisinde yer alan kişisel veriye bağlı bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi,

dikkate alınır.

(5) Veri sorumluları, kişisel verilerin işlendikleri amaç için gerekli olan azami sürenin belirlenmesi, bu sürelerin kişisel veri işleme envanterinde belirtilen bilgilerle uyumu ve azami sürenin aşıp aşılmadığının takibi için kişisel veri saklama ve imha politikası hazırlayarak, bu politikanın uygulanmasını temin ederler.

(6) VERBİS içerisinde belirtilen başlıkların ve içeriklerinin, veri sorumlusunun gerçekleştirdiği faaliyetleri ve Sicile iletmesi gereken bilgileri tam olarak kapsamaması durumunda; veri sorumlusu bu bilgileri ayrıca VERBİS içerisinde bu amaca ilişkin ayrılan "Diğer" başlıklı bölümlere girerek Sicile bildirimini tamamlar.

Kayıt başvurusu

MADDE 10 - (1) Veri sorumluları, 9 uncu maddede belirtilen bilgileri VERBİS'e yüklemek suretiyle kayıt yükümlülüğünü yerine getirmiş sayılır.

(2) Kurum tarafından 8 inci maddenin üçüncü fıkrasında belirtildiği üzere kendilerine ek süre verilmiş olan veri sorumluları, bu süre tamamlanmadan kayıt başvurusunu tamamlamak zorundadır.

Veri sorumlusu, veri sorumlusu temsilcisi ve irtibat kişininin yükümlülükleri

MADDE 11 - (1) Tüzel kişilerde veri sorumlusu tüzel kişiliğin kendisidir. Türkiye’de yerleşik olan tüzel kişilerin Kanun kapsamındaki veri sorumlusu yükümlülükleri, ilgili mevzuat hükümlerine göre tüzel kişiliği temsil ve ilzama yetkili organ veya ilgili mevzuatta belirtilen kişi veya kişiler marifetiyle yerine getirilir. Tüzel kişiliği temsile yetkili organ, Kanunun uygulanması bakımından yerine getirilecek yükümlülükler ile ilgili olarak bir veya birden fazla kişiyi görevlendirebilir. Bu görevlendirme Kanun hükümleri uyarınca tüzel kişiliğin sorumluluğunu ortadan kaldırmaz.

(2) Türkiye’de yerleşik olmayan veri sorumlusunun, veri sorumlusu temsilcisi atanmasına ilişkin yetkili organı veya kişisi tarafından alınacak kararın tasdikli örneği, kayıt başvurusu sırasında veri sorumlusu temsilcisi tarafından Kuruma sunulur.

(3) Veri sorumlusu temsilcisi atama kararı, asgari olarak aşağıda belirtilen hususları kapsayacak şekilde düzenlenir:

a) Kurum tarafından yapılan tebligat veya yazışmaları veri sorumlusu adına tebellüğ veya kabul etme,

b) Kurum tarafından veri sorumlusuna yöneltilen talepleri veri sorumlusuna iletme, veri sorumlusundan gelecek cevabı Kuruma iletme,

c) Kurul tarafından başkaca bir esasın belirlenmemiş olması halinde; ilgili kişilerin Kanunun 13 üncü maddesinin birinci fıkrası uyarınca veri sorumlusuna yönelteceği başvuruları veri sorumlusu adına alma ve veri sorumlusuna iletme,

ç) Kurul tarafından başkaca bir esasın belirlenmemiş olması halinde; ilgili kişilere Kanunun 13 üncü maddesinin üçüncü fıkrası uyarınca veri sorumlusunun cevabını iletme,

d) Veri sorumlusu adına Sicile ilişkin iş ve işlemleri yapma.

(4) **(Değişik:RG-28/4/2019-30758)** Türkiye’de yerleşik olan veri sorumluları ile Türkiye’de yerleşik olmayan veri sorumluları adına veri sorumlusu temsilcileri, Sicile kayıt sırasında irtibat kişisi bilgilerini Sicile işlerler. İrtibat kişisi veri sorumlusunu Kanun ve Yönetmelik hükümlerine göre temsile yetkili değildir.¹⁹

¹⁹ Değişiklik öncesi “Türkiye’de yerleşik olan tüzel kişiler Sicile kayıt sırasında irtibat kişisi bilgilerini Sicile işlerler. İrtibat kişisi veri sorumlusunu Kanun ve Yönetmelik hükümlerine göre temsile yetkili değildir. İrtibat kişisi, ilgili kişilerin veri sorumlusuna yönelteceği taleplerin cevaplandırılması konusunda iletişimi sağlar.”.

(5) (**Değişik:RG-28/4/2019-30758**) Kamu kurum ve kuruluşlarında irtibat kişisi, koordinasyonu sağlayacak üst düzey yönetici tarafından Kurum ile iletişimi sağlamak amacıyla belirlenerek Sicile kaydı yapılan daire başkanı veya üstü yöneticidir.²⁰

İletişimin sağlanması

MADDE 12 - (1) Kanunun uygulanmasıyla ilgili olarak Kurum tarafından veri sorumlusuyla kurulacak her türlü iletişim;

- a) Türkiye’de yerleşik tüzel kişiler için, Sicile bildirilen kimlik, adres veya KEP adresi bilgileri üzerinden ilgili tüzel kişi,
- b) Türkiye’de yerleşik gerçek kişiler için, Sicile bildirilen kimlik, adres veya KEP adresi bilgileri üzerinden ilgili gerçek kişi,
- c) Türkiye’de yerleşik olmayan veri sorumluları için, Sicile bildirilen veri sorumlusu temsilcisi, vasıtasıyla gerçekleştirilir.

Kayıt bilgilerinde değişiklikler

MADDE 13 - (Değişik:RG-28/4/2019-30758)

(1) Veri sorumluları, Sicilde kayıtlı bilgilerde değişiklik olması halinde meydana gelen değişiklikleri, değişikliğin meydana geldiği tarihten itibaren yedi gün içerisinde VERBİS üzerinden Kuruma bildirir.

Sicil kaydının silinmesi

MADDE 14 - (1) Veri sorumlusu, sicil kaydının silinmesine ilişkin olarak VERBİS üzerinden Kuruma başvurur.

(2) Kayıt yükümlüğünü gerektiren faaliyet sona erer ya da ortadan kalkarsa, sicil kaydı silinir. Bu kayıtlar, istendiğinde erişilebilir olmakla birlikte üzerinde herhangi bir değişiklik yapılamayacak şekilde tutulur.

(3) Sicil kaydının silinmesi veri sorumlusunun Sicile kayıtlı olduğu dönemdeki yükümlülüklerini ortadan kaldırmaz.

DÖRDÜNCÜ BÖLÜM

Kayıt Yükümlülüğünün İstisnaları

²⁰ Değişiklik öncesi “Kamu kurum ve kuruluşlarında irtibat kişisi, üst düzey yönetici tarafından Kurum ile iletişimi sağlamak amacıyla belirlenerek Sicile kaydı yapılan daire başkanı veya üstü yöneticidir.”.

İstisna uygulanacak haller

MADDE 15 - (1) Aşağıda belirtilen kişisel veri işleme faaliyetleri bakımından veri sorumlusunun bu faaliyetleri Sicile kayıt etmesi ve bildirmesi yükümlülüğü yoktur:

- a) Kişisel veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.
- b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.
- c) Kişisel veri işleminin kanunun verdiği yetkiye dayanarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.
- ç) Kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

İstisna kriterleri

MADDE 16 - (1) Kurul, aşağıdaki kriterleri göz önünde bulundurarak kayıt yükümlülüğüne istisna getirebilir:

- a) Kişisel verinin niteliği.
- b) Kişisel verinin sayısı.
- c) Kişisel verinin işleme amacı.
- ç) Kişisel verinin işlendiği faaliyet alanı.
- d) Kişisel verinin üçüncü kişilere aktarılma durumu.
- e) Kişisel veri işleme faaliyetinin kanunlardan kaynaklanması.
- f) Kişisel verilerin muhafaza edilmesi süresi.
- g) Veri konusu kişi grubu veya veri kategorileri.
- ğ) (Ek:RG-28/4/2019-30758) Veri sorumlusunun yıllık çalışan sayısı veya yıllık mali bilanço toplamı bilgisi.

(2) Kurul, birinci fıkrada sayılan kriterler çerçevesinde belirlenen istisnaların kapsamı ile uygulama usul ve esaslarını belirlemek amacıyla karar alma yetkisini haizdir. Kurul bu kararlarını uygun yöntemlerle yayımlayarak kamuya duyurur.

BEŞİNCİ BÖLÜM

Çeşitli ve Son Hükümler

İdari yaptırım

MADDE 17 - (1) Veri sorumluları siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında Kanunun 18 inci maddesinin birinci fıkrasının (ç) bendinde yer alan idari para cezası uygulanır.

(2) Veri sorumluları siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edilmesi eyleminin, kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu Kurula bildirilir.

Tereddütlerin giderilmesi

MADDE 18 - (1) Bu Yönetmeliğin uygulanması sırasında doğacak tereddütleri ve uygulamaya ilişkin aksaklıkları gidermeye ve uygulamayı yönlendirmeye, ilke ve standartları belirlemeye ve uygulama birliğini sağlayacak gerekli düzenlemeleri yapmaya, bu hususta gerekli her türlü bilgi ve belgeyi istemeye, bu Yönetmelikte yer almayan konularda ilgili mevzuat hükümleri çerçevesinde karar vermeye Kurul yetkilidir.

Yürürlük

MADDE 19 - (1) Bu Yönetmelik 1/1/2018 tarihinde yürürlüğe girer.

Yürütme

MADDE 20 - (1) Bu Yönetmelik hükümlerini Başkan yürütür.

**Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması
Hakkında Yönetmelik**

Resmî Gazete Tarihi : 04.12.2020

Resmî Gazete Sayısı : 31324

**ELEKTRONİK HABERLEŞME SEKTÖRÜNDE KİŞİSEL VERİLERİN İŞLENMESİ VE
GİZLİLİĞİN KORUNMASINA İLİŞKİN YÖNETMELİK**

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğın amacı, özel hayatın gizliliğı ile kiři temel hak ve özgürlüklerinin korunmasını teminen elektronik haberleşme sektöründe kişisel verilerin işlenmesi ve gizliliğın korunmasına yönelik usul ve esasları belirlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin tüzel kiři abonelikleri dâhil elektronik haberleşme hizmeti sunulması kapsamında elde ettikleri veriler bakımından uyacakları usul ve esasları kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun 4, 6, 12, 49, 51 ve 60 ıncı maddelerine dayanılarak hazırlanmıştır.

Tanımlar ve kısaltmalar

MADDE 4 - (1) Bu Yönetmelikte geçen;

- a) Abone: Bir işletmeci ile elektronik haberleşme hizmetinin sunumuna yönelik olarak yapılan bir sözleşmeye taraf olan gerçek ya da tüzel kişiyi,
- b) Acil yardım çağrıları: Ulusal ve uluslararası düzenlemelerde kabul görmüş yangın, sağlık, doğal afetler ve güvenlik gibi acil durumlarla ilgili olarak itfaiye, polis, jandarma, sağlık ve benzeri kuruluşlara yardım talebiyle yapılan çağrıları,

- c) Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,
- ç) İşlem kaydı: Kişisel verilere ve ilişkili diğer sistemlere erişen kişiler tarafından yapılan işlemin, işlemin gerçekleştiği tarihten sonra tanımlanabilmesini teminen tutulan ve asgari olarak işlem, işlemin detayı, işlemi yapan kişi, işlemin yapıldığı tarih ve zaman ile işlemi yapan kişinin bağlandığı nokta bilgilerini içeren elektronik kayıtları,
- d) İşletmeci: Yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirketi,
- e) Kanun: 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununu,
- f) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
- g) Kişisel veri ihlali: Yasa dışı, yetki dışı ya da istem dışı olarak; kişisel verilerin tahrip edilmesine, silinmesine, kaybolmasına, iletilmesine, değiştirilmesine, depolanmasına veya başka bir ortama kaydedilmesine, işlenmesine, ifşa edilmesine ve söz konusu verilere erişilmesine neden olan güvenlik ihlali,
- ğ) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,
- h) Konum verisi: Kamuya açık elektronik haberleşme hizmeti kullanıcısına ait bir cihazın coğrafi konumunu belirleyen ve elektronik haberleşme şebekesinde veya elektronik haberleşme hizmeti aracılığıyla işlenen belirli veriyi,
- ı) Kullanıcı: Aboneliği olup olmamasına bakılmaksızın elektronik haberleşme hizmetlerinden yararlanan gerçek veya tüzel kişiyi,
- i) Kurul: Bilgi Teknolojileri ve İletişim Kurulunu,
- j) Kurum: Bilgi Teknolojileri ve İletişim Kurumunu,
- k) Trafik verisi: Bir elektronik haberleşme şebekesinde haberleşmenin iletimi veya bu haberleşmenin faturalandırılması amacıyla işlenen her türlü veriyi,
- l) Veri: Kişisel veri, trafik verisi veya konum verisini,
- ifade eder.

(2) Bu Yönetmelikte geçen ancak birinci fıkrada tanımlanmayan kavramlar ve kısaltmalar için ilgili mevzuatta yer alan tanımlar geçerlidir.

İKİNCİ BÖLÜM

İlkeler ve Uygulama Esasları

İlkeler

MADDE 5 - (1) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

- a) Hukuka ve dürüstlük kurallarına uygun olarak işlenmesi.
- b) Doğru ve gerektiğinde güncel olması.
- c) Belirli, açık ve meşru amaçlar için işlenmesi.
- ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması.
- d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi.

(2) Milli güvenlik gerekçesiyle trafik ve konum verilerinin yurt dışına çıkarılmaması esastır.

Güvenlik

MADDE 6 - (1) İşletmeciler abonelerine/kullanıcılarına ait kişisel verilerin ve sundukları hizmetlerin güvenliğini sağlamak amacıyla Kanuna, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununa, ulusal ve uluslararası standartlara uygun olarak gerekli her türlü teknik ve idari tedbirleri alır. Bu güvenlik tedbirleri, teknolojik imkânlar göz önünde bulundurularak muhtemel riske uygun düzeyde alınır.

(2) Birinci fıkrada belirtilen tedbirler asgari olarak;

- a) 5 inci maddede yer alan ilkeler çerçevesinde kişisel verilerin işlenmesine ilişkin güvenlik politikalarını belirlemeyi,
- b) İstem dışı, yetki dışı ya da mevzuata aykırı olarak; kişisel verilerin tahrip edilmesi, kaybolması, değiştirilmesi, depolanması veya başka bir ortama kaydedilmesi, işlenmesi, ifşa edilmesi ve söz konusu verilere erişilmesi gibi ihlallere karşı kişisel verilerin korunmasını,
- c) Kişisel verilere sadece yetkili kişiler tarafından erişilebilmesini ve kişisel verilerin saklandığı sistemler ile kişisel verilere erişim sağlamak için kullanılan uygulamaların güvenliğinin sağlanmasını, içerir.

(3) Kurum, gerekli gördüğü hâllerde alınan güvenlik tedbirlerine ilişkin işletmecilerden, bilgi ve belge isteyebilir, ayrıca idari yaptırım uygulama hakkı saklı kalmak kaydıyla söz konusu güvenlik tedbirlerinde değişiklik talep edebilir.

(4) İşletmeciler, kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtlarını iki yıl saklamakla yükümlüdür.

(5) İşletmeciler, yetkilendirdikleri taraflarca bu Yönetmelik hükümlerinin ihlal edilmesi de dâhil olmak üzere, sundukları hizmetler kapsamında elde ettikleri verilerin gizliliğinin, güvenliğinin, bütünlüğünün, erişilebilirliğinin ve amacı doğrultusunda kullanılmasının temininden sorumludur.

Riskin ve kişisel veri ihlalinin bildirilmesi

MADDE 7 - (1) İşletmeciler, şebekelerinin ve sundukları hizmetlerin güvenliğini tehdit eden belirli bir risk olması durumunda;

a) Bu risk hakkında,

b) Bu riskin işletmeci tarafından alınan tedbirlerin dışında kalması hâlinde, söz konusu riskin kapsamı ve giderilme yöntemleri hakkında,

ilgili aboneleri/kullanıcıları en kısa sürede bilgilendirir.

(2) İşletmeciler, kişisel veri ihlali olması durumunda 6698 sayılı Kanun ve ilgili mevzuata uygun yöntemlerle Kuruma, Kişisel Verileri Koruma Kurumuna ve ilgili abonelere/kullanıcılara en kısa sürede bildirimde bulunur.

Açık rıza alma şartları

MADDE 8 - (1) İşletmeciler, aboneden/kullanıcıdan açık rıza alınmasını gerektiren durumlarda aşağıdaki şartları yerine getirir:

a) Açık rıza beyanı belirli bir konuya ilişkin olarak ilgili işlem öncesinde alınır. Belirli bir konu ile sınırlandırılmayan ve ilgili işlemle sınırlı olmayan genel nitelikteki rızalar geçersiz kabul edilir.

b) Açık rıza beyanı özgür iradeyle açıklanmış olmalıdır. Abonelik tesis edilmesi ve temel elektronik haberleşme hizmetleri veya cihazların sunulması, abonenin/kullanıcının verilerinin işlenmesine yönelik açık rıza verme ön şartına bağlanamaz. Hediye dakika, SMS ve veri gibi ek fayda sağlanması karşılığında aboneden/kullanıcıdan açık rıza talep edilebilir.

c) Abone/kullanıcı, açık rıza beyanının alınması öncesinde; işlenecek kişisel veri türü ile trafik ve konum verisi türleri, kapsamı, işleme amacı ve süresi hakkında işletmeciler tarafından açık ve

anlaşılır bir şekilde bilgilendirilir. Bu bilgilendirmenin yazılı yapılması halinde yazılar en az on iki punto ile hazırlanır.

ç) İşletmecinin gerekli bilgilendirmeyi yapması sonrasında abonenin/kullanıcının “evet/onay/kabul” şeklindeki irade beyanı yazılı veya elektronik ortamda alınır. Söz konusu irade beyanı rıza alınan duruma özgü olmalıdır. Bu irade beyanı, bir sözleşmenin veya hizmetin kabulü ya da pazarlama amaçlı haberleşmelere onay verilmesi ve benzeri hukuki işlemlere yönelik irade beyanları ile birleştirilemez.

d) İşletmeciler, abonelerin/kullanıcıların açık rızalarını gösteren kayıtları, ilgili mevzuat hükümlerinde yer alan süreler saklı kalmak kaydıyla, asgari abonelik süresince saklamakla yükümlüdür.

e) Trafik ve konum verilerinin üçüncü taraflara aktarımının söz konusu olduğu durumlar için;

1) Aktarılabacak verinin kapsamı,

2) Aktarılabacak tarafın adı ve açık adresi,

3) Aktarma amacı ve süresi,

4) Üçüncü tarafın yurt dışında olması halinde verinin aktarılabacağı ülkenin adı,

şeklindeki bilgiler verilerek ayrıca açık rıza alınır. Bu bilgilerde değişiklik olması halinde tekrar açık rıza alınır.

f) İşletmeciler, trafik ve konum verilerinin açık rıza alınarak üçüncü taraflara aktarımının söz konusu olduğu durumlarda, bu verilerin sadece açık rıza bilgilendirmesinde belirtilen üçüncü taraflarca ve belirtilen amaçla işlenmesini temin etmekle yükümlüdür.

Trafik ve konum verilerine ilişkin aydınlatma yükümlülüğü

MADDE 9 - (1) 6698 sayılı Kanununun 10 uncu maddesi hükümleri saklı kalmak üzere, trafik ve konum verilerinin işlenebildiği hallerde işletmeciler, işlenebilecek trafik veya konum verisi türleri, işleme amacı ve süresi hakkında abonelere/kullanıcılara bilgi vermekle yükümlüdür.

ÜÇÜNCÜ BÖLÜM

Sağlanan İmkânlar

Numaranın gizlenmesi

MADDE 10 - (1) İşletmeci, arayan numaranın görünmesine imkân sağladığı durumlarda;

a) Arayan kullanıcıya basit bir yöntemle ve ücretsiz olarak numarasını gizleme imkânı sağlamakla,

b) Aranan aboneye basit bir yöntemle ve ücretsiz olarak, gelen aramalarda arayan numaranın gösterilmesini engelleme imkânı sağlamakla,

c) Arayan kişinin numarasını gizlemesi hâlinde, ancak aranan abonenin/kullanıcının gizli arama alma yönündeki iradesini daha önceden işletmeciye beyan etmiş olması durumunda çağrıyı sonlandırmakla,

yükümlüdür.

(2) İşletmeci, yönlendirilmiş aramalar gibi bağlanılan numaranın görünmesine imkân sağladığı durumlarda, bağlanılan aboneye basit bir yöntemle ve ücretsiz olarak, bağlanılan numaranın arayan kullanıcıya gösterilmesini engelleme imkânı sağlamakla yükümlüdür.

(3) İşletmeci, birinci ve ikinci fıkralarda belirtilen imkânlar hakkında abonelerini/kullanıcılarını kısa mesaj, internet veya benzeri araçlarla bilgilendirmekle yükümlüdür.

(4) Arayan numaranın gizlenmesi imkânı, acil yardım çağrıları için geçerli değildir.

Otomatik çağrı yönlendirme

MADDE 11 - (1) İşletmeci, aboneye/kullanıcıya kendisine üçüncü kişilerden gelen otomatik yönlendirmeleri ücretsiz ve basit yöntemlerle durdurma imkânı tanır.

(2) İşletmeciler tarafından başka bir numaraya veya otomatik mesaj sistemine yapılan yönlendirmelerin ücretli olması hâlinde, abonenin/kullanıcının onayı alınır.

Ayrıntılı faturalarda gizlilik

MADDE 12 - (1) İşletmeciler, abonelerin talep etmeleri hâlinde kullanım detayında veya ayrıntılı faturada yer alan telefon numaralarının bazı rakamlarının gizlenmesini sağlar.

Abonenin/kullanıcının diğer hakları

MADDE 13 - (1) İşletmeciler, abonelerin/kullanıcıların verilerinin işlenmesine yönelik olarak, kısa mesaj, çağrı merkezi, internet ve benzeri yöntemlerle vermiş oldukları açık rızayı aynı yöntem ya da daha basit bir yöntem ile her zaman ücretsiz olarak geri almalarına imkân sağlar. Bu imkâna ilişkin bilgilendirme de açık rıza alınması sırasında yapılır.

(2) İşletmeciler tarafından her yılın üçüncü çeyreği içinde, mobil numara bilgisi bulunan abonelere/kullanıcılara asgari kısa mesajla, diğerlerine e-posta veya arama yöntemlerinden biri ile olmak üzere, daha önce alınan açık rızaları kapsamında verilerinin işlendiğine dair bilgilendirme

yapılır. Aksi durumda daha önce verilen açık rızalar kapsamındaki veri işleme faaliyeti bilgilendirme yapıncaya kadar durdurulur.

(3) İşletmeciler tarafından bu Yönetmelik kapsamında engelli tarifelerinden yararlanan abonelere/kullanıcılara yapılacak bilgilendirmeler, işitsel ve/veya görsel yöntemler kullanılarak Kurum düzenlemelerine uygun şekilde gerçekleştirilir.

(4) Aboneliğin sonlanması halinde, sona erme tarihi itibarıyla, abonenin aksi talebi olmaması halinde daha önce verilen tüm açık rızalar geri alınmış sayılır.

(5) Bu Yönetmelik kapsamındaki abonelere/kullanıcılara yapılacak tüm bilgilendirmeler, ücretsiz olarak gerçekleştirilir.

(6) Bu Yönetmelik kapsamındaki bilgilendirmeler, açık rıza, abone/kullanıcı talebi ve onayına ilişkin ispat sorumluluğu işletmeciye aittir.

(7) Açık rızanın geri alınması durumunda işletmeci açık rızaya dayalı olarak yapılan veri işleme faaliyetlerini derhal durdurur.

DÖRDÜNCÜ BÖLÜM

Çeşitli ve Son Hükümler

İdari para cezaları ve diğer yaptırımlar

MADDE 14 - (1) İşletmecilerin bu Yönetmelik ile belirlenen yükümlülükleri yerine getirmemeleri hâlinde 15/2/2014 tarihli ve 28914 sayılı Resmî Gazete’de yayımlanan Bilgi Teknolojileri ve İletişim Kurumu İdari Yaptırımlar Yönetmeliği hükümleri uygulanır.

Kurumun yetkisi

MADDE 15 - (1) Bu Yönetmeliğin uygulanması sırasında doğacak tereddütleri ve uygulamaya ilişkin aksaklıkları gidermeye ve uygulamayı yönlendirmeye, ilke ve standartları belirlemeye ve uygulama birliğini sağlamaya Kurum yetkilidir.

Yürürlükten kaldırılan yönetmelik

MADDE 16 - (1) 24/7/2012 tarihli ve 28363 sayılı Resmî Gazete’de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik yürürlükten kaldırılmıştır.

Atıflar

MADDE 17 - (1) Mevzuatta 24/7/2012 tarihli ve 28363 sayılı Resmî Gazete’de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmeliğe yapılan atıflar bu Yönetmeliğe yapılmış sayılır.

Mevcut rızaların durumu

GEÇİCİ MADDE 1 - (1) Bu Yönetmeliğin yürürlüğe girdiği tarihten önce hukuka uygun olarak alınmış rızalar geçerli sayılır.

(2) Bu Yönetmeliğin yürürlüğe girdiği tarihten önce rızaları alınarak verileri işlenen tarafların abonelikleri sona ermesine rağmen açık rızaları olmaksızın verilerinin işlenmeye devam etmesi durumunda bu işlem, ilgili mevzuatta yer alan yükümlülükler saklı kalmak kaydıyla, bu Yönetmeliğin yürürlüğe girdiği tarihi takip eden bir ay içinde durdurulur.

Yürürlük

MADDE 18 - (1) Bu Yönetmelik yayımı tarihinden altı ay sonra yürürlüğe girer.

Yürütme

MADDE 19 - (1) Bu Yönetmelik hükümlerini Bilgi Teknolojileri ve İletişim Kurulu Başkanı yürütür.

Kişisel Sağlık Verileri Hakkında Yönetmelik

Resmî Gazete Tarihi : 21.06.2019

Resmî Gazete Sayısı : 30808

Sağlık Bakanlığından:

KİŞİSEL SAĞLIK VERİLERİ HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı; 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu hükümleri kapsamında, Sağlık Bakanlığının merkez ve taşra teşkilatı birimleri ile bunlara bağlı olarak faaliyet göstermekte olan sağlık hizmeti sunucuları ile bağlı ve ilgili kuruluşları tarafından yürütülen süreç ve uygulamalarda uyulacak usul ve esasları düzenlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, kişisel sağlık verisi işleyen özel hukuk gerçek ve tüzel kişileri ile kamu hukuku tüzel kişilerinin, Sağlık Bakanlığı tarafından yürütülmekte olan süreç ve uygulamalara ilişkin faaliyetlerini kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 7/5/1987 tarihli ve 3359 sayılı Sağlık Hizmetleri Temel Kanunu ile 10/7/2018 tarihli ve 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinin 378 inci maddesinin altıncı fıkrası ve 508 inci maddesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Yönetmelikte geçen;

a) Açık veri: Ücretsiz olarak veya hazırlanma maliyetini geçmeyecek şekilde internet üzerinden herkesin erişimine sunulan, üzerinde herhangi bir fikri mülkiyet hakkı bulunmayan ve herhangi bir amaçla serbestçe kullanılabilen, makineler tarafından okunabilen ve böylelikle diğer veriler ve sistemlerle birlikte çalışabilen, anonim hale getirilmiş veriyi,

- b) Açık sağlık verisi: Açık veri haline getirilen sağlık verisini,
- c) Anonim hale getirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini,
- ç) Bakanlık: Sağlık Bakanlığını,
- d) e-Nabız: İlgili kişilerin sağlık verilerine kendilerinin, hekimlerin veya yetki verdikleri üçüncü kişilerin erişimini sağlayan, e-Devlet uygulamalarına uygun olarak Bakanlıkça kurulan sistemi,
- e) Genel Müdürlük: Sağlık Bilgi Sistemleri Genel Müdürlüğünü,
- f) İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,
- g) İlgili kullanıcı: Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişileri,
- ğ) KamuNET: Kamu kurum ve kuruluşları arasındaki veri iletişiminin sağlanması, bu veri iletişiminin internete kapalı, fiziksel ve siber saldırılara karşı daha güvenli sanal bir ağ üzerinden yapılması, siber güvenlik risklerinin minimize edilmesi, mevcut ve kurulacak olan güvenli kapalı devre çözümlere standart sağlanması, ortak uygulamalar için uygun alt yapının tesis edilmesi amaçlarıyla Ulaştırma ve Altyapı Bakanlığı tarafından geliştirilen projeyi,
- h) Kanun: 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununu,
- ı) Kimliksizleştirme: Kişisel verilerin; kimliği belirli veya belirlenebilir gerçek kişiyle ilişkilendirilememesi için teknik ve idari tedbirlerin alınması şartıyla ve farklı bir ortamda muhafaza edilen diğer verilerle bir araya getirilmeksizin ilgili kişiyle ilişkilendirilemeyecek şekilde işlenmesini,
- i) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
- j) Kişisel sağlık verisi: Kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgileri,
- k) Kişisel verilerin imha edilmesi: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,
- l) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması,

devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi sağlık verileri üzerinde gerçekleştirilen her türlü işlemi,

m) Kişisel verilerin silinmesi: Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hâle getirilmesi işlemi,

n) Kişisel verilerin yok edilmesi: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hâle getirilmesi işlemi,

o) Kurul: Kişisel Verileri Koruma Kurulunu,

ö) Kurum: Kişisel Verileri Koruma Kurumunu,

p) Maskeleye: Kişisel verilerin belirli alanlarının, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin çizilmesi, boyanması ve yıldızlanması gibi işlemleri,

r) Merkezi sağlık veri sistemi: Bakanlık tarafından oluşturulan kişisel sağlık verilerinin toplandığı veri sistemini,

s) Sağlık hizmeti sunucusu: Sağlık hizmetini sunan veya üreten gerçek kişiler ile kamu hukuku ve özel hukuk tüzel kişilerini,

ş) Veri sorumlusu: Kişisel sağlık verilerinin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,

ifade eder.

(2) Bu Yönetmelikte yer almayan tanımlar için Kanundaki tanımlar ile Kurum tarafından yapılan ikincil düzenlemelerde yer verilen tanımlar geçerlidir.

İKİNCİ BÖLÜM

Genel İlke ve Esaslar

Genel ilke ve esaslar

MADDE 5 - (1) Kişisel verilerin işlenmesinde Kanunun 4 üncü maddesinde yer alan genel ilkeler başta olmak üzere, Kanunda yer alan bütün esaslara riayet edilir.

(2) Herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi amacıyla, Bakanlık ile bağlı ve ilgili kuruluşlarınca gerekli kayıt ve bildirim sistemi kurulur. Bu sistem, e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabilir. Bu

amaçla Bakanlık tarafından, bağlı ve ilgili kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemleri kurulabilir.

(3) Hiç kimse, sağlık hizmeti sunumu için gerekli olan durumlar haricinde geçmiş sağlık verilerinin dökümünü sunmaya veya göstermeye zorlanamaz.

(4) Sağlık hizmeti sunucuları tarafından; banko, gişe ve masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda yakın konumda hizmet alanların birbirlerine ait kişisel verileri duymalarını, görmelerini, öğrenmelerini veya ele geçirmelerini engelleyecek nitelikte gerekli fiziki, teknik ve idari tedbirler alınır.

(5) Sağlık hizmeti sunucuları, tahlil ve tetkik sonuçları gibi hastaya ait kişisel sağlık verilerini içeren basılı materyal üzerinde gerekli kısmî kimliksizleştirme veya maskeleyen tedbirlerini uygular ve söz konusu materyalin yetkisiz kişilerin eline geçmesi hâlinde kime ait olduğunun tespit edilmesini zorlaştıracak diğer tedbirleri alır.

(6) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili olarak Kanunun 11 inci maddesinde yer alan hakları kullanabilir.

(7) Veri sorumlusuna başvuruda, Kanunun 13 üncü maddesi ile Kurum tarafından hazırlanarak 10/3/2018 tarihli ve 30356 sayılı Resmî Gazete’de yayımlanan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ hükümlerine riayet edilir.

(8) Aydınlatma yükümlülüğünün yerine getirilmesinde, Kanunun 10 uncu maddesi ile Kurum tarafından hazırlanarak 10/3/2018 tarihli ve 30356 sayılı Resmî Gazete’de yayımlanan Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerine riayet edilir.

ÜÇÜNCÜ BÖLÜM

Kişisel Sağlık Verilerine Erişim

Sağlık personelinin verilere erişimi

MADDE 6 - (1) Sağlık hizmeti sunumunda görevli kişiler; ilgili kişinin sağlık verilerine ancak, verilecek olan sağlık hizmetinin gereği ile sınırlı olmak kaydıyla erişebilir.

(2) e-Nabız hesabı bulunan kişilerin sağlık verilerine, kendi gizlilik tercihleri çerçevesinde erişim sağlanır. İlgili kişiler, gizlilik tercihleri ve sonuçları konusunda ayrıntılı şekilde bilgilendirilir. Gizlilik tercihi ve geçmiş sağlık verilerinin görüntülenememesi nedeniyle sağlık hizmeti sunumunda meydana gelebilecek aksaklık ve zararlardan Bakanlık sorumlu olmaz.

(3) e-Nabız hesabı bulunmayan kişilerin sağlık verilerine ise Kanununun 6 ncı maddesinin üçüncü fıkrasında yer alan istisnai amaçlarla sınırlı olmak üzere ancak;

a) Kişinin kayıtlı olduğu aile hekimi tarafından herhangi bir süre sınırı olmaksızın,

b) Kişinin sağlık hizmeti almak üzere randevu aldığı hekim tarafından, randevunun alındığı gün ile sınırlı olmak kaydıyla ve alınan sağlık hizmeti ile doğrudan bağlantılı işlemler sonlanana kadar,

c) Kişinin sağlık hizmeti almak üzere giriş yaptığı sağlık hizmeti sunucusunda görev yapan hekimler tarafından, yirmi dört saat süre ile sınırlı olmak kaydıyla,

ç) Hastanın yatışının yapıldığı sağlık hizmeti sunucusunda görev yapan hekimler tarafından, hasta sağlık hizmeti sunucusundan taburcu olana kadar,

erişilebilir.

(4) Üçüncü fıkrada yer alan erişim kuralları, Bakanlığın sağlık hizmeti sunumu ihtiyaçlarına göre ve Kanununun 6 ncı maddesinin üçüncü fıkrası kapsamında Genel Müdürlük tarafından yeniden değerlendirilebilir. Böyle bir durumda aydınlatma yükümlülüğü kapsamında gereklilikler sağlanır.

(5) Geçmiş sağlık verilerinin herhangi bir kimse tarafından erişilmesini istemeyen kişilere ilgili gizlilik tercihi e-Nabız üzerinden sunulur. Bu gizlilik tercihinin kullanan kişilerin geçmiş sağlık verilerine ancak kişinin kendisi tarafından beyan edilen telefon numarasına gönderilecek olan kodun hekim ile paylaşılması ve hekim tarafından sisteme girilmesi halinde erişilebilir.

(6) Mahremiyet düzeyi daha yüksek olan, başkaları tarafından görülmesi ve bilinmesi halinde kişilerin sosyal hayatını ve ruh sağlığını olumsuz etkileme riski taşıyan kişisel sağlık verileri Bakanlıkça belirlenir ve sağlık personelinin bu verilere erişimine ölçülü kısıtlar getirilebilir.

Bakanlık birimlerinin verilere erişimi

MADDE 7 - (1) Sağlık hizmeti sunucuları tarafından merkezi sağlık veri sistemine kimliksizleştirilerek gönderilen sağlık verilerini, ilişkisel veri tabanı aracılığı ile ait oldukları kişilerle eşleştirmeye yetkili kişileri Bakanlığın birim amirleri ayrı ayrı belirler ve Genel Müdürlükten bu kişilerin yetkilendirilmesini talep eder. Her birimin amiri, kendi biriminden en fazla üç kişinin yetkilendirilmesini talep edebilir.

(2) Birim amirinin talebi üzerine Genel Müdürlükçe yetkilendirilen kullanıcılar bu yetkiyi, yalnızca sağlık hizmetleri ile finansmanının planlanması ve yönetimi ile denetleme ve düzenleme görevleri kapsamında, kişisel veri koruma mevzuatı ilkelerine uygun olarak kullanabilirler.

(3) Sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacının sınırları, yasal ve idari düzenlemelerde ilgili birime verilen görevler üzerinden belirlenir.

Çocukların sağlık verilerine erişim

MADDE 8 - (1) Ebeveynler, çocuklarına ilişkin sağlık kayıtlarına herhangi bir onaya ihtiyaç duyulmaksızın e-Nabız üzerinden erişebilir. Ayırt etme gücüne sahip çocuklar, sağlık geçmişlerine ebeveynlerinin erişimini e-Nabız üzerinden izne tabi tutabilir.

(2) Anne ve babanın boşanması hâlinde velâyet hakkı üzerinde bırakılmayan taraf, çocuk ile velinin faydası gözetilmek suretiyle kişisel verilerin korunması mevzuatına uygun şekilde ve Genel Müdürlükçe belirlenen sınırlar çerçevesinde çocuğa ilişkin sağlık verilerine erişebilir.

Sağlık verilerine hasta yakınlarının erişimi

MADDE 9 - (1) Kişisel sağlık verilerinin hasta yakınları ile paylaşımında, Kanun ilkelerine aykırılık teşkil etmeyecek şekilde, 1/8/1998 tarihli ve 23420 sayılı Resmî Gazete’de yayımlanan Hasta Hakları Yönetmeliğinin 18 inci maddesinin üçüncü fıkrasına uygun hareket edilir.

Sağlık verilerine avukatların erişimi

MADDE 10 - (1) Avukatlar, müvekkilinin sağlık verilerini genel vekâletname ile talep edemezler. Müvekkiline ait sağlık verilerinin avukata aktarılması için düzenlenmiş olan vekâletnamede, ilgili kişinin özel nitelikli kişisel verilerinin işlenmesi ve aktarılmasına ilişkin açık rızasını gösteren özel bir hüküm bulunması gerekir.

Ölünün sağlık verilerine erişim

MADDE 11 - (1) Ölmüş bir kimsenin sağlık verilerini almaya, veraset ilamını ibraz etmek suretiyle murisin yasal mirasçıları münferit olarak yetkilidir.

(2) Ölmüş bir kimsenin sağlık verileri, en az 20 yıl süre ile saklanır.

DÖRDÜNCÜ BÖLÜM

Kişisel Sağlık Verilerinin Gizlenmesi, Düzeltilmesi,

İmha Edilmesi ve Aktarılması

Kişisel sağlık verilerinin gizlenmesi

MADDE 12 - (1) Hakkında gizlilik kararı verilen kişilere ait verilerin gizlenmesi için yargı makamları tarafından gönderilen müzekkerenin gereği il sağlık müdürlüğü tarafından yerine getirilir. İl sağlık müdürlüğü tarafından tesis edilen işlem doğrudan Kimlik Paylaşım Sistemine de yansır. Gizlilik

kararlarının sadece görevi gereği bilmesi gereken kişiler tarafından bilinmesini sağlamak üzere gerekli her türlü teknik ve idari tedbirler alınır.

Kişisel sağlık verilerinin düzeltilmesi

MADDE 13 - (1) İlgili kişi, kendisi hakkında sehven oluşturulan sağlık verilerinin düzeltilmesi hususunda sağlık verisinin oluşturulduğu sağlık hizmeti sunucusunun bağlı bulunduğu il sağlık müdürlüğüne başvurur. İl sağlık müdürlüğü, ilgili sağlık hizmeti sunucusunda yapacağı araştırma neticesinde sağlık verisinin sehven oluşturulduğu bilgisine ulaşırsa resmi yazı ile Genel Müdürlüğe başvurur ve sehven oluşturulan sağlık verisinin düzeltilmesini ister.

(2) Genel Müdürlük tarafından tesis edilecek işlem, sağlık hizmeti sunucusunun kendi veri tabanında da gerçekleştirilir.

(3) Genel Müdürlük, sağlık hizmeti sunucuları tarafından oluşturulan sağlık verilerinin kendileri tarafından düzeltilebileceği tarihi belirler ve bu tarihi ihtiyaca göre günceller. Genel Müdürlükçe belirlenen bu tarihten sonra oluşturulan sağlık verileri ilgili sağlık hizmeti sunucusu tarafından; bu tarihten önce oluşturulan sağlık verileri ise ilgili il sağlık müdürlüğünün talebi üzerine Genel Müdürlükçe düzeltilir.

Kişisel sağlık verilerinin imha edilmesi

MADDE 14 - (1) Kişisel verilerin imha edilmesinde, Kanunun 7 nci maddesi ile Kurum tarafından hazırlanarak 28/10/2017 tarihli ve 30224 sayılı Resmî Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik hükümlerine riayet edilir.

Kişisel sağlık verilerinin aktarılması

MADDE 15 - (1) Kişisel sağlık verilerinin yurtiçinde aktarımında Kanunun 8 inci maddesine, yurtdışına aktarımında ise Kanunun 9 uncu maddesine riayet edilir.

(2) Kişisel sağlık verilerinin, Kanunun 8 inci maddesinin ikinci fıkrasının (b) bendi ile üçüncü fıkrası ve 28 inci maddesi kapsamında kamu kurum ve kuruluşlarına aktarılması için protokol düzenlenir. Düzenlenen protokolda, kişisel veri koruma mevzuatının genel ilkeleri ile veri güvenliğine ilişkin hükümlere ve protokol kapsamında hangi verilerin aktarılacağına yer verilir. Verilerin aktarımı, teknik altyapının uygun olması hâlinde KamuNET üzerinden gerçekleştirilir.

(3) Kişisel sağlık verilerinin aktarımı talepleri, talep edilen sağlık verilerinin ilgili olduğu Bakanlık birimi tarafından Kanun ve ilgili diğer mevzuat açısından değerlendirilir, değerlendirme sonucuna göre Genel Müdürlükçe işlem tesis edilir.

BEŞİNCİ BÖLÜM

Bilimsel Amaçlarla İşleme ve Açık Sağlık Verisi

Bilimsel amaçlarla işleme

MADDE 16 - (1) Kanunun 28 inci maddesinin birinci fıkrasının (b) bendi kapsamında veri sorumlusu tarafından anonim hâle getirilen kişisel sağlık verileri ile bilimsel çalışma yapılabilir.

(2) Kanunun 28 inci maddesinin birinci fıkrasının (c) bendi kapsamında kişisel sağlık verileri, ilgili kişilerin özel hayatın gizliliğini veya kişilik haklarını ihlâl etmemek ya da suç teşkil etmemek kaydıyla alınacak teknik ve idari tedbirler çerçevesinde, bilimsel amaçlarla işlenebilir.

Açık sağlık verisi

MADDE 17 - (1) Genel Müdürlük tarafından, Bakanlığın merkez ve taşra teşkilatı ile bağlı ve ilgili kuruluşlarında kullanılan sistemlerde yer alan verilerin, veri mahremiyeti ile veri güvenliğine ilişkin düzenlemeler göz önünde bulundurularak, sağlık sisteminde şeffaflığı ve hesap verilebilirliği temin etmek, sağlık hizmeti sunumuna ilişkin politika ve stratejilere yön vermek, sağlık alanında yapılacak bilimsel araştırmalara destek olmak ve sağlığa ilişkin ürün ve hizmetlerin geliştirilmesini sağlamak amaçlarıyla, bu konuya özel olarak tahsis edilen bir internet sitesi üzerinden herkesin erişimine açılmasına ilişkin usûl ve esaslar Bakanlıkça belirlenir.

ALTINCI BÖLÜM

Veri Güvenliği

Veri güvenliğine ilişkin yükümlülükler

MADDE 18 - (1) Kanunun 12 nci maddesinde yer alan veri güvenliğine ilişkin yükümlülüklere riayet edilir. Teknik ve idari tedbirlerin alınmasında, Kurum tarafından hazırlanan Kişisel Veri Güvenliği Rehberi esas alınır.

(2) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde veri sorumlusu tarafından Kurula yapılacak bildirimde Kanun hükümleri ile Kurulun bu hususa ilişkin düzenleyici işlemleri esas alınır.

Bilgi güvenliği

MADDE 19 - (1) Bakanlık merkez birimleri ve taşra teşkilatı ile bağlı ve ilgili kuruluşlarda yürütülen bilgi güvenliği süreçleri, Genel Müdürlük tarafından hazırlanan Bilgi Güvenliği Politikaları Yönergesi ile belirlenir.

Yeterli önlemler

MADDE 20 - (1) Özel nitelikli kişisel verilerin işlenmesinde ayrıca, Kanununun 6 ncı maddesinin dördüncü fıkrası ile 22 nci maddesinin birinci fıkrasının (ç) bendi uyarınca Kişisel Verileri Koruma Kurulu tarafından yapılan ikincil düzenlemelerde yer alan yeterli önlemlere riayet edilir.

YEDİNCİ BÖLÜM

Çeşitli ve Son Hükümler

Yaptırım

MADDE 21 - (1) Bu Yönetmelikle korunan kişisel verilere ilişkin suçlar ve kabahatler bakımından Kanununun 17 nci ve 18 inci maddelerine göre işlem yapılır.

(2) Bu Yönetmelik gereklerini yerine getirmeyen kamu görevlileri için bağlı oldukları disiplin amirliğine bildirim yapılır ve varsa yetkileri iptal edilir. Gerçek kişiler ve özel hukuk tüzel kişileri hakkında ilgili mevzuata göre işlem yapılır.

(3) Merkezi sağlık veri sistemine Bakanlıkça belirlenen usul ve esaslara uygun bir şekilde veri gönderimi yapmayan sağlık hizmeti sunucularına, 3359 sayılı Sağlık Hizmetleri Temel Kanununun Ek 11 inci maddesinin üçüncü fıkrasına göre işlem tesis edilir.

Hüküm bulunmayan hâller

MADDE 22 - (1) Kişisel sağlık verilerinin işlenmesi ile ilgili olarak bu Yönetmelikte hüküm bulunmayan hâllerde; Kanun ve ilgili ikincil düzenlemeler uygulanır.

Yürürlükten kaldırılan yönetmelik

MADDE 23 - (1) 20/10/2016 tarihli ve 29863 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik yürürlükten kaldırılmıştır.

Yürürlük

MADDE 24 - (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 25 - (1) Bu Yönetmelik hükümlerini Sağlık Bakanı yürütür.

Sosyal Güvenlik Kurumu Nezdindeki Verilerin Korunmasına ve İşlenmesine İlişkin Yönetmelik

Resmî Gazete Tarihi : 19 Şubat 2022

Resmî Gazete Sayısı : 31755

Sosyal Güvenlik Kurumu Başkanlığından:

SOSYAL GÜVENLİK KURUMU NEZDİNDEKİ VERİLERİN KORUNMASINA VE İŞLENMESİNE İLİŞKİN YÖNETMELİK

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı; Kurumun 16/5/2006 tarihli ve 5502 sayılı Sosyal Güvenlik Kurumuna İlişkin Bazı Düzenlemeler Hakkında Kanun, 31/5/2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu ve 15/7/2018 tarihli ve 30479 sayılı Resmî Gazete’de yayımlanan 4 sayılı Bakanlıklara Bağlı, İlgili, İlişkili Kurum ve Kuruluşlar ile Diğer Kurum ve Kuruluşların Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinde belirtilen görev ve yetkileri kapsamında, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde ettiği verilerin işlenmesinde uyulacak usul ve esasları belirlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, Kurumun görev ve yetkileri kapsamında tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde ettiği verilerin işlenmesinde uyulacak usul ve esaslar doğrultusunda;

- a) Kurum personelini,
- b) Kişisel verileri işlenen gerçek kişileri,
- c) Kişisel verilerin işlenmesine ait bilgi işlem sistemleri yazılım ve donanımı ile dosyalama sistemi gibi hizmetleri sunan gerçek ve tüzel kişileri,
- ç) Kurumun faaliyetleri kapsamında mevzuat çerçevesinde kişisel verileri işleyen kamu kurum ve kuruluşları ile özel hukuk gerçek ve tüzel kişileri,

- d) Kurum adına kişisel verileri işleyen gerçek veya tüzel kişileri,
- e) Veri aktarımının yapıldığı kamu kurum ve kuruluşları ile özel hukuk gerçek ve tüzel kişilerini,
- kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 16/5/2006 tarihli ve 5502 sayılı Sosyal Güvenlik Kurumuna İlişkin Bazı Düzenlemeler Hakkında Kanununun 35 inci maddesi ile 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununa dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Yönetmelikte geçen;

- a) AFYDB: Kurum Aktüerya ve Fon Yönetimi Daire Başkanlığını,
- b) Anonim hâle getirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini,
- c) Anonim veri: Anonim hale getirilen ve kimliği belirli veya belirlenebilir gerçek kişiyle ilişkilendirilemeyen veriyi,
- ç) Başkan: Sosyal Güvenlik Kurumu Başkanı,
- d) Birim: 4 sayılı Cumhurbaşkanlığı Kararnamesinin 413 üncü maddesinde belirtilen hizmet birimlerini,
- e) Birim amiri: 4 sayılı Cumhurbaşkanlığı Kararnamesinin 413 üncü maddesinde belirtilen hizmet birimlerinin en üst amirini, taşra teşkilatında ise sosyal güvenlik il müdürlerini,
- f) Genel sağlık sigortalısı: 5510 sayılı Kanununun 60 ncı maddesinde sayılan kişileri,
- g) Genel sağlık sigortası: Kişilerin öncelikle sağlıklarının korunmasını, sağlık riskleri ile karşılaşmaları halinde ise oluşan harcamaların finansmanını sağlayan sigortayı,
- ğ) HSGM: Kurum Hizmet Sunumu Genel Müdürlüğünü,
- h) İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,
- ı) İlgili kullanıcı: Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişileri,

- i) Kişisel sağlık verisi: Kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgileri,
- j) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
- k) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,
- l) Kişisel verilerin silinmesi: Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesini,
- m) Kişisel verilerin yok edilmesi: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemini,
- n) Kurul: Kişisel Verileri Koruma Kurulunu,
- o) Kurum: Sosyal Güvenlik Kurumunu,
- ö) MEDULA: Sağlık hizmeti kullanım verisi toplamak ve bu verilere dayanarak faturalama işlemini gerçekleştirmek amacıyla Kurum tarafından uygulanan ve işletilen elektronik bilgi sistemini,
- p) Mevzuat birimi: Emeklilik Hizmetleri Genel Müdürlüğü, Sigorta Primleri Genel Müdürlüğü, Genel Sağlık Sigortası Genel Müdürlüğü, Rehberlik ve Teftiş Başkanlığı, Aktüerya ve Fon Yönetimi Daire Başkanlığı ile Strateji Geliştirme Başkanlığını,
- r) Sağlık hizmeti: Genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişilere 5510 sayılı Kanunun 63 üncü maddesi gereği finansmanı sağlanacak tıbbi ürün ve hizmetleri,
- s) Sağlık hizmeti sunucusu: Sağlık hizmetini sunan ve/veya üreten; gerçek kişiler, kamu kurum ve kuruluşları ile özel hukuk tüzel kişilerini ve bunların tüzel kişiliği olmayan şubelerini,
- ş) Sigortalı: Kısa ve/veya uzun vadeli sigorta kolları bakımından adına prim ödenmesi gereken veya kendi adına prim ödemesi gereken kişiyi,
- t) Sosyal sigortalar: 5510 sayılı Kanunda tanımlanan kısa ve uzun vadeli sigorta kollarını,
- u) Taşra birimi: Sosyal güvenlik il müdürlükleri ile sosyal güvenlik il müdürlüklerine bağlı sosyal güvenlik merkezlerini,

ü) Ticari sır niteliğindeki veri: Bir ticari işletme veya şirketin kendisine veya muvafakati çerçevesinde gerçek veya tüzel kişilere verilme durumları hariç olmak üzere; herkes tarafından bilinmeyen ve elde edilemeyen, başta rakipleri olmak üzere üçüncü kişilere ve kamuya açıklanması halinde ilgili ticari işletme veya şirketin zarar görme ihtimali bulunan ve ticari işletme veya şirketin ekonomik hayattaki başarı ve verimliliği için ticari önem atfettikleri veriyi,

v) Veri: Kurum nezdinde üretilen, işlenen veya arşivlenen her türlü bilgi ve belgeyi,

y) Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,

z) Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği Kurum veri kayıt sistemlerini,

aa) Veri paylaşım metodu: Talep edilen verilerin Kurum tarafından uygun bulunan Elektronik Belge Yönetimi Sistemi (EBYS) ortamında CD, DVD, sabit disk, taşınabilir bellek gibi elektronik-manyetik kayıt ortamlarında veya web servis, SFTP veya Kurumda kullanılan diğer yazılımlar gibi elektronik ortamlar üzerinden şifrelenerek paylaşım metotlarını,

bb) Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,

ifade eder.

İKİNCİ BÖLÜM

Kişisel Veriler, Kişisel Sağlık Verileri ile Ticari Sır Niteliğindeki Veriler

Kişisel veriler, kişisel sağlık verileri ile ticari sır niteliğindeki verilerin işlenmesi

MADDE 5 - (1) Kurum; 5502 sayılı Kanun, 5510 sayılı Kanun ve 4 sayılı Cumhurbaşkanlığı Kararnamesi ile kendisine verilen görevleri yerine getirmek amacıyla kişisel verilerin, kişisel sağlık verilerinin ve ticari sır niteliğindeki verilerin işlenmesinde aşağıdaki ilkelere uymak zorundadır:

a) Hukuka ve dürüstlük kurallarına uygun olma.

b) Doğru ve gerektiğinde güncel olma.

c) Belirli, açık ve meşru amaçlar için işlenme.

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

(2) Kurumla sözleşmeli sağlık hizmeti sunucuları, Kurum adına işledikleri kişisel sağlık verilerini Kurum veri kayıt sistemine aktarmakla yükümlüdür.

(3) Sağlık hizmeti sunucuları, sözleşme kapsamında Kurum adına işledikleri kişisel sağlık verilerini, Kurum veri kayıt sistemi dışında hiçbir yere kopyalayamaz veya aktaramaz.

(4) Kurum adına kişisel verileri, kişisel sağlık verilerini ve ticari sır niteliğindeki verileri işleyen veya görevi gereği bu verilere erişen herkes, sır saklama yükümlülüğü altında olup veri gizliliğinin sağlanması amacıyla Kurum ve Kurul tarafından belirlenen önlemlere uymakla yükümlüdür.

(5) Kişisel verilerin, kişisel sağlık verilerinin ve ticari sır niteliğindeki verilerin işlenmesinde ayrıca Kurul tarafından yapılan düzenlemelere uyulması zorunludur. Ancak veri aktarımında 5502 sayılı Kanunun 35 inci maddesi hükmü saklıdır.

(6) Kişisel verilerin, kişisel sağlık verilerinin ve ticari sır niteliğindeki verilerin bulunduğu Kurum veri kayıt sistemine erişim izni verilebilmesi için, yetkilendirme dahilinde kullanıcı tanımlanması gerekir. Kullanıcı tanımlama ve yetkilendirmeye ilişkin her türlü işlem kayıt altına alınır ve bu kayıtlar muhafaza edilir. Yetkilendirme, kayıt altına alma ve verilerin muhafazasına ilişkin hususlar veri sorumlusu tarafından belirlenir.

Veri sorumlusunun görev ve yükümlülükleri

MADDE 6 - (1) Veri sorumlusu, bu Yönetmelik kapsamındaki verilerin hukuka aykırı olarak işlenmesini ve bu verilere, hukuka aykırı bir şekilde erişilmesini önlemek, bu verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

(2) Veri sorumlusu, tedbirlerin alınması hususunda veri işleyenler ile birlikte müştereken sorumludur.

(3) Veri sorumlusu Kurul tarafından belirlenen düzenlemelerin uygulanmasını sağlamak amacıyla Kurumda gerekli denetimleri yapmak veya yaptırmak zorundadır.

(4) Kişisel verileri, kişisel sağlık verileri ile ticari sır niteliğindeki verileri işleyen kişiler, bu verilere erişen kişiler ve veri sorumluları; öğrendikleri kişisel verileri, kişisel sağlık verilerini ve ticari sır niteliğindeki verileri 6698 sayılı Kanun ve 5502 sayılı Kanun ile bu Yönetmelik hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

(5) Bu Yönetmelik kapsamında işlenen verilerin kanuni olmayan yollarla başkaları tarafından elde edildiğinin tespiti hâlinde veri sorumlusu, bu durumu gecikmeksizin ve en geç 72 saat içinde Kurula, söz konusu veri ihlalden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde bildirir.

(6) Bu Yönetmelik kapsamında kişisel veri işleyen veri sorumluları Kurul tarafından çıkarılacak düzenlemelere uymakla yükümlüdür.

Kişisel veriler, kişisel sağlık verileri ile ticari sır niteliğindeki verilere erişimler

MADDE 7 - (1) Kuruma verilen görevlerin yerine getirilebilmesi için kullanıcı tanımlaması ve yetkilendirmesi yapılan Kurum personelinin kişisel verilere, kişisel sağlık verilerine ve ticari sır niteliğindeki verilere erişimleri; üçüncü kişilere verilmemek, açıklanmamak ve veri güvenliğine ilişkin Kurum ve Kurul tarafından belirlenen yükümlülüklerle uyulmak kaydıyla veri aktarımı olarak değerlendirilmez.

(2) Bu Yönetmelik kapsamındaki kişisel verilere;

- a) Sağlık hizmetlerine ilişkin fatura bedellerinin incelenmesi ve ödenmesi,
 - b) Kurumun alacaklarının takip ve tahsili,
 - c) Denetim, teftiş ve kontrol,
 - ç) Verilerin işlenmesi,
 - d) Kurum mevzuatında yer alan sağlık ve sosyal sigorta hizmetlerine ilişkin kontrol parametrelerinin Kurum veri kayıt sistemine aktarılması ve takibi,
 - e) Sağlık ve sosyal sigorta hizmetlerinin izlenmesi, değerlendirilmesi, istatistik üretilmesi ve risk analizi yapılması,
 - f) Sağlık ve sosyal sigorta politikalarının belirlenmesi,
 - g) HSGM’de yazılım geliştirilmesi, sistem işletimi ve verilerin hazırlanması,
- amacıyla bu işlemlerde görevlendirilen ve 5 inci maddenin altıncı fıkrası kapsamında kullanıcı tanımlaması ve yetkilendirmesi yapılan Kurum personeli tarafından erişilebilir.

(3) Kullanıcı tanımlaması ve yetkilendirmesi yapılan Kurum personeli, kişisel verilere, kişisel sağlık verilerine ve ticari sır niteliğindeki verilere;

- a) Kurum veri kayıt sisteminde yer alan verilere şifre ile doğrudan erişim yetkisi verilmesi,

b) Kurumsal Raporlama ve İstatistik Sistemi, MEDULA gibi kişisel veriler, ticari sır niteliğindeki veriler ile kişisel sağlık verilerine ulaşılan uygulamalara şifre ile erişim yetkisinin verilmesi, yoluyla erişebilir.

(4) Kullanıcı tanımlaması ve yetkilendirmesi yapılmaksızın Kurum personelinin görevi kapsamında talep ettiği kişisel verilere, kişisel sağlık verilerine ve ticari sır niteliğindeki verilere;

a) İlgili mevzuat biriminin onayı sonrasında HSGM tarafından uygun veri paylaşım metodu ile personelin bağlı olduğu ilgili birime iletilmesi,

b) Kurum personelinin görevi kapsamında talep ettiği kişisel veriler, kişisel sağlık verileri ve ticari sır niteliğindeki verilere birimi içerisinde hazırlanması ve iletilmesi,

yöntemiyle erişebilir.

(5) İkinci fıkranın (c) bendi kapsamında yapılan veri talepleri doğrudan HSGM'ye yapılır ve HSGM tarafından karşılanır. Üçüncü fıkranın (a) bendi kapsamında verilere erişim yetkileri, personelin görev yaptığı birim tarafından Başkanlık Makamından alınan onaya istinaden HSGM tarafından verilir. Üçüncü fıkranın (b) bendi kapsamında verilere erişim yetkileri, personelin görev yaptığı birimin talebine istinaden Kurumun yetkilendirme işlemleri çerçevesinde HSGM tarafından verilir. Dördüncü fıkranın (a) bendi kapsamında yapılacak veri talepleri ilgili birim tarafından doğrudan mevzuat birimine yapılır ve bu talepler hakkında 20 nci maddenin bir ila yedinci fıkrası hükümleri uygulanır.

(6) Verilere erişim yetkileri, personelin görev süresi ve kapsamı ile sınırlı olup, erişim yetkisinin sona ermesini gerektirecek bir durumun meydana gelmesi halinde yetkinin kaldırılması ile ilgili gerekli işlemler personelin görev yaptığı birim tarafından derhal yapılır.

(7) Personelin verilere erişim yetki düzeyleri, personelin görev süresi ve kapsamı ile yapılacak çalışmanın niteliğinin gerektirdiği erişim ihtiyacı dikkate alınarak talebi yapan ilgili birimce belirlenir ve bu talep ilgili mevzuat biriminden alınacak onay ile HSGM'ye iletilir.

Kurumun iş ve işlemlerinin yürütülmesine ilişkin hususlar

MADDE 8 - (1) Veri işleyenler tarafından hizmetin gereği olarak veri kayıt sistemlerinden yapılan sorgular, veri aktarımı olarak değerlendirilmez.

Genel sağlık sigortası ile sosyal sigortalara yönelik iş ve işlemlerin paydaşlar ile yürütülmesi

MADDE 9 - (1) Kuruma verilen görevlerin yerine getirilebilmesine yönelik iş ve işlemlerin diğer kamu kurum ve kuruluşları ile üniversite, enstitü, oda, dernek gibi paydaşlar ile birlikte gerçekleştirilmesi amacıyla;

- a) Kurumca imzalanan işbirliği protokolü, hizmet alım sözleşmesi/protokolü kapsamındaki çalışmalarda,
- b) Genel sağlık sigortası ile sosyal sigortalar uygulamalarına ilişkin iş ve işlemlerin yürütülmesine yönelik olarak oluşturulan komisyonlarda,

Kurum dışından görev alan kişilerin kişisel verilere, kişisel sağlık verilerine ve ticari sır niteliğindeki verilere erişimlerine izin verilmez. Bu kişilerin anonim verilere erişimleri, veri aktarımı olarak değerlendirilmez.

(2) Kurum, bu madde kapsamında görevlendirilen kişiler ile ilgili olarak, bu Yönetmelik ve 6698 sayılı Kanununun 12 nci maddesi kapsamında veri güvenliğine ilişkin teknik ve idari tedbirleri almak, ilgili mevzuat hükümlerine uygun hareket edilmesini sağlamak zorundadır.

Kişinin kendisine ait kişisel veriler ile kişisel sağlık verilerine ilişkin talepleri

MADDE 10 - (1) Herkes, Kuruma başvurarak kendisiyle ilgili kişisel verileri ile kişisel sağlık verilerinin;

- a) İşlenip işlenmediğini öğrenme,
 - b) İşlenmişse buna ilişkin bilgi talep etme,
 - c) Silinmesini, yok edilmesini isteme,
 - ç) İşlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
 - d) Yurt içinde veya yurt dışında aktarıldığı üçüncü kişileri bilme,
 - e) Eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
 - f) İşlenenlerinin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
 - g) Mevzuata aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme,
 - ğ) (c) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- haklarına sahiptir.

(2) Kişilerin kişisel verileri ile kişisel sağlık verilerinin silinmesi veya yok edilmesi taleplerinde, kişisel verilerin işleme şartlarının tamamının ortadan kalkıp kalkmadığı yönünde ilgili mevzuat birimince değerlendirme yapılarak silme, yok etme veya anonim hâle getirme işlemlerinden hangisinin uygulanacağına karar verilir. Uygulanan yöntem ve gerekçesi en geç 30 gün içinde ilgili mevzuat birimi tarafından ilgili kişiye yazılı olarak veya elektronik tebligat adresine bildirilir.

(3) Kurum, kişinin kişisel verileri ile kişisel sağlık verilerini;

a) Kişinin kendisine veya noter onaylı muvafakatiyle veya e-Devlet uygulaması üzerinden kimlik teyidi ile verilen izin ile diğer gerçek veya tüzel kişilere,

b) Mahkeme kararı ile kişinin sağlık verilerine erişim izninde yetkilendirilmiş kişilere,

c) Müvekkili tarafından verilen özel vekâletnamede avukatın kişisel veriler ile kişisel sağlık verilerini talep edebileceğine yer verilmiş olması şartıyla ilgili avukatna,

aktarabilir veya gerekçesini açıklayarak veri taleplerini reddedebilir.

(4) Kuruma yapılan talepler, talebin niteliğine göre en kısa sürede ve en geç 30 gün içinde ücretsiz olarak sonuçlandırılır. Ancak, işlemin ayrıca bir maliyeti gerektirmesi halinde, Kurulca bu konuda belirlenen tarifedeki ücret alınabilir.

(5) Bu madde kapsamındaki veri talepleri taşra birimine yapılır. Taşra birimi, yetkileri dahilinde Kurum veri kayıt sisteminden temin edemediği verileri 20 nci maddenin iki ila beşinci fıkrası hükümlerine göre temin edebilir.

Kurum veya kuruluşların kişisel veri ile ticari sır niteliğindeki veri talepleri

MADDE 11 - (1) Kurum, işlediği kişisel veri ile ticari sır niteliğinde olan verileri, ilgili kişinin noter onaylı muvafakati veya e-Devlet uygulaması üzerinden kimlik teyidi ile verilen izni ile ve kişiler adına vekâlet ile yetkilendirilenler tarafından, kişisel veri veya ticari sır niteliğindeki veriler hususunda yetkiyi içeren özel vekâletnamenin veya vasi atamaya ilişkin mahkeme kararının Kuruma ibraz edilmesi koşuluyla gerçek veya tüzel kişilere, ilgili mevzuat birim amirinin onayı ile aktarılabilir.

(2) Ancak, 5502 sayılı Kanununun 35 inci maddesi uyarınca 10/12/2003 tarihli ve 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanununun ekinde yer alan (I), (II), (III) ve (IV) sayılı cetvellerde yer alan kamu idareleri ile Türkiye Cumhuriyet Merkez Bankasının ilgili mevzuatında belirtilen görevleri yapabilmeleri için ihtiyaç duydukları kişisel sağlık verisi dışındaki kişisel veriler ile ticari sır niteliğinde olan veriler aktarılabilir.

(3) Kamu kurum veya kuruluşları tarafından yazılı veya elektronik ortamda talep edilen tek seferlik kişisel veriler ile ticari sır niteliğindeki veriler, ikinci fıkradaki şartları taşıdığıının belirlenmesi halinde talep eden kamu kurum veya kuruluşlarının bulunduğu il müdürlüğüne karşılanır. İl müdürlüğü, yetkileri dahilinde Kurum veri kayıt sisteminden temin edemedikleri verileri, 20 nci maddenin bir ila dokuzuncu fıkrası hükümlerine göre temin ederek ilgili merciye teslim eder.

(4) Kamu kurum veya kuruluşları tarafından talep edilen sürekli nitelikteki kişisel veriler ile ticari sır niteliğindeki verilerin aktarılabilmesi için veri talebinde bulunanlar ile Kurum arasında ilgili mevzuat biriminin koordinasyonunda aktarımın usulünü ve diğer gerekli hususları belirleyen protokolün imzalanması zorunludur.

Sağlık Bakanlığının kişisel sağlık verisi talepleri

MADDE 12 - (1) Kurum, kişisel sağlık verilerini; kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, verilen sağlık hizmetlerinin uygunluğunun ve yerindeliliğinin takibi ve finansmanının planlanması amacıyla talebi hâlinde Sağlık Bakanlığı ile paylaşır.

(2) Sağlık Bakanlığı tarafından yapılan veri taleplerinde, 20 nci maddenin bir ila dokuzuncu fıkrası hükümleri uygulanır.

Sözleşmeli sağlık hizmeti sunucularının sundukları hizmetlere ilişkin veri talepleri

MADDE 13 - (1) Sağlık hizmetlerinin sağlanmasına yönelik olarak Kurumla sözleşme yapmış sağlık hizmeti sunucularınca, Kurum adına işledikleri kişisel sağlık verilerinden mücbir sebep dolayısıyla Kuruma faturalandırılmayan hizmetlere ilişkin verilerin talep edilmesi durumunda bu talepler hakkında 20 nci maddenin bir ila dokuzuncu fıkrası hükümleri uygulanır.

Yargı makamları ve infaz mercilerinin veri talepleri

MADDE 14 - (1) Yargı makamları ve infaz mercileri tarafından talep edilen kişisel veri ile kişisel sağlık verisi talepleri taşra birimine yapılır. Taşra birimi, yetkileri dahilinde Kurum veri kayıt sisteminden temin edemedikleri verileri, HSGM'den temin ederek ilgili merciye teslim eder.

ÜÇÜNCÜ BÖLÜM

Anonim Veriler

Anonim verilerin aktarılması

MADDE 15 - (1) İlgili mevzuat birimleri tarafından belirlenen kişisel verilerin, kişisel sağlık verilerinin ve ticari sır niteliğindeki verilerin anonim hale getirilmesinde, ulusal ve uluslararası kabul

görmüş istatistiki yöntemler uygulanır. Bu konuda Kurul tarafından yapılan düzenlemelerde yer alan hükümler uygulanır.

(2) Anonim veriler, bu Yönetmelik hükümlerine uygun olarak ve Kurum tarafından değerlendirilerek uygun görülmesi koşuluyla;

- a) Sağlık ile sosyal sigorta alanında stratejilerin ve hedeflerin gerçekleştirilmesi,
- b) Genel sağlık sigortası ile sosyal sigorta politika ve uygulamalarının geliştirilmesi,
- c) Sağlık ve sosyal sigorta hizmetlerinin finansmanı, yönetimi ve planlanması,
- ç) Kişi ve toplum sağlığının korunması ile koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetleri stratejilerinin oluşturulması,
- d) Kurumsal önceliklerin gerçekleştirilmesi,
- e) Sağlık ve sosyal sigorta istatistiklerinin hazırlanması,
- f) Bilimsel ve akademik araştırma ve çalışmaların gerçekleştirilmesi,
- g) Kamu alacaklarının takip ve tahsili,
- ğ) Kamu kurum ve kuruluşlarının mevzuatla verilen görevlerinin yerine getirilmesinin sağlanması ile denetim görevlerinin gerçekleştirilebilmesi,
- h) Kamu kurum ve kuruluşlarının faaliyetlerinde bürokrasinin azaltılması ve işlemlerin sadeleştirilmesi,

amacıyla aktarılabilir.

(3) Anonim veri talepleri;

- a) Verilerin ayrı veya özel bir çalışma, araştırma, inceleme ya da analiz neticesinde oluşturulabilecek nitelikte olup olmadığı,
- b) Verilerin anonim hale getirilme işlemlerinin karmaşıklığı,
- c) Verilerin ticari sır niteliğinde olup olmadığı,

gibi ölçütlere göre aktarılabilir.

(4) Anonim veri aktarımı yapılan gerçek ve tüzel kişiler aktarılan verileri aktarım amacı ve Kurum bilgisi dışında kullanamazlar.

Araştırma, planlama ve istatistik amaçlı anonim veri talepleri

MADDE 16 - (1) Kamu idarelerinin, 11 inci maddenin ikinci fıkrası kapsamına girmeyen araştırma, planlama ve istatistik amaçlı anonim veri talepleri veya bilimsel araştırma yapan kamu personelinin, bilimsel derneklerin, kamu kurumu niteliğindeki meslek kuruluşlarının veya üniversitelerin araştırma, planlama ve istatistik amaçlı ihtiyaç duydukları anonim veriler aktarılabilir.

(2) İlgili mevzuat birimleri ile AFYDB’de görevli personel hariç, Kurum personelinin görevi kapsamında yapılacak çalışmalarda kullanılmak üzere, anonim veri talepleri, talep eden personelin bağlı bulunduğu birim amiri tarafından ilgisine göre ilgili mevzuat birim amirine yapılır.

(3) Kurum içi birimler tarafından Kurumsal Raporlama ve İstatistik Sisteminde bulunan istatistik amaçlı veriler talep edilemez.

(4) Bu madde kapsamındaki veri taleplerinde, 20 nci madde hükümleri uygulanır.

(5) Bu madde kapsamında sürekli veya elektronik ortamda yapılacak anonim veri aktarımı, ilgili mevzuat biriminin koordinasyonunda aktarımın usulü ve diğer gerekli hususları belirleyen bir protokol aracılığıyla yapılır.

Tüzel kişilere ait olan anonim verilerin tüzel kişinin kendisine veya diğer kişilere aktarımı

MADDE 17 - (1) Tüzel kişilerin, 5510 sayılı Kanununun 63 üncü maddesinin birinci fıkrasının (f) bendinde belirtilen sağlık hizmetlerinden ruhsat veya satış iznine sahip olduğu ürünlere ait veriler; Kurum tarafından uygun görülmesi halinde tüzel kişiyi temsile yetkili olanların noter onaylı muvafakatlerinin alınması kaydıyla 20 nci maddenin bir ila yedinci fıkrası hükümlerine göre gerçek veya tüzel kişilere aktarılabilir.

(2) Bu madde kapsamında aktarılacak veriler, sağlık hizmeti sunucularının doğrudan ya da dolaylı tanınmasına yol açamaz.

(3) Bu madde kapsamında veri aktarılabilmesi için veri talebinde bulunanlar ile Kurum arasında ilgili mevzuat biriminin koordinasyonu ile aktarımın usulü ve diğer gerekli hususları belirleyen sözleşme/protokol imzalanması zorunludur.

Anonim istatistik yayınları

MADDE 18 - (1) Anonim veriler ile ticari sır niteliğindeki verileri içeren Kurum istatistik bültenlerinin, istatistik yıllıklarının ve faaliyet raporlarının yayımlanması veri aktarımı olarak değerlendirilmez.

(2) Kurum tarafından kamuya açıklanmış istatistik bültenleri, istatistik yıllıkları, faaliyet raporları ve benzeri yayımlarında yer alan anonim verilerin Kurum dışına verilmesi veri aktarımı olarak değerlendirilmez.

Kurum personelinin tezleri

MADDE 19 - (1) Kurum personeli, Kurum mevzuatı gereği hazırlayacakları tezleri için anonim veri talebinde bulunabilir.

(2) Bu madde kapsamında yapılacak anonim veri taleplerinde, 20 nci maddenin birinci, üçüncü ve beşinci fıkraları uygulanır.

DÖRDÜNCÜ BÖLÜM

Genel Hükümler

Verilerin aktarım taleplerine ilişkin genel hükümler

MADDE 20 - (1) Veri aktarım talepleri, ilgili mevzuat birimine yazılı olarak yapılır. İlgili mevzuat birimi gerekli gördüğü durumlarda istenilen veriye ilişkin detaylı veri deseninin hazırlanmasını talep edebilir.

(2) 11 inci maddenin ikinci fıkrasında sayılan kamu kurum ve kuruluşlarının talep ettikleri kişisel sağlık verisi dışındaki kişisel veriler, anonim veriler ile ticari sır niteliğindeki verilerin aktarılabilmesi için talebe ilişkin hukuki dayanağın Kuruma yapılacak yazılı talepte belirtilmesi zorunludur.

(3) Veri taleplerinin değerlendirilmesi sürecinde ihtiyaç duyulması halinde ilgili mevzuat birimince ayrıca bilgi ve belge istenebilir.

(4) Veri taleplerinin kabul edilmesi halinde, veri erişimi ve gizliliğine ilişkin gerekli şartları içeren Protokol ilgili mevzuat biriminin koordinasyonunda veri talebinde bulunanlarca imzalanır.

(5) Veri talepleri, ilgili mevzuat birimi tarafından incelenerek veri formatı ve başlıkları belirlenmiş şekilde verilerin hazırlanması için HSGM'ye iletilir. İlgili mevzuat birimi tarafından veri paylaşımının uygun görülmediği durumlarda veri talebinde bulunanlara ilgili mevzuat birimince bilgi verilir.

(6) Aktarılmak üzere hazırlanan veriler, HSGM tarafından Kurumca belirlenecek format ile uygun veri paylaşım metodu kullanılarak paylaşılır. Paylaşılacak veri, talebi yapan gerçek veya tüzel kişiye yazılı olarak taahhütlü veya iadeli taahhütlü posta ile veya elden teslim edilebilir.

(7) Anonim verilerin kamu kurum ve kuruluşlarına teslimi, talepleri halinde şifrelenmiş dosya ile "gov.tr" uzantılı e-posta adreslerine yapılabilir.

(8) Telefonla veri iletilemez.

(9) Veri talebinde bulunanlar, işledikleri verilerin sonuçlarını Kurum tarafından kontrol edilebilir bir dosya formatında hazırlar ve oluşturulan sonuçlarda bu Yönetmelik hükümlerine aykırı olarak işlenen verilere yer verilemez.

(10) Veri talebinde bulunanların işledikleri verilerin veri işleme süreçlerindeki tüm sonuçlarının bu Yönetmeliğe aykırı biçimde aktarılması sonucunu doğuracak veri içerip içermediği ilgili birim tarafından kontrol edilir. Bu Yönetmelik hükümlerine aykırı olarak işlenen verileri içeren bölümlerin tespit edilmesi halinde sonuçların kullanılmasına izin verilmez.

(11) Veri talebinde bulunanların hatalı hesaplama sonucu elde ettiği bulgular sadece veri talebinde bulunanları bağlar.

(12) Veri talebinde bulunanlar, çalışmalarında elde ettikleri sonuçları yayımlarken kullandıkları Kurum verilerini kaynak göstermek zorundadır.

(13) Veri talebinde bulunanlar yayımladıkları rapor, makale ve benzeri çalışmalarının bir kopyasını, yayımlarından sonraki 30 gün içerisinde veriyi talep ettiği Kurumun ilgili birimine göndermekle yükümlüdür.

(14) Veri talebinde bulunanlar, aldıkları verileri taleplerinde ifade ettikleri amaç dışında farklı bir amaçla kullanamaz, çoğaltamaz, üçüncü kişilere veremez, satamaz veya devredemez.

Verilerin aktarıldığı kişi, kurum/kuruluşların sorumlulukları

MADDE 21 - (1) Verilere erişen Kurum personeli ile verilere erişen veya veri aktarımı yapılan kamu kurum ve kuruluşlarının personeli de dahil olmak üzere gerçek ve tüzel kişiler, sağlık hizmeti sunucularına ait bilgi işlem sistemlerinin yazılımını ve donanımını sağlayan gerçek ve tüzel kişiler;

a) Veri talebine uygun olarak yaptıkları çalışmaların, kişisel verilerin açıklanmasına imkân vermeyecek şekilde yürütülmesini sağlar; verilerin istenilen amaç dışında kullanılmaması ve paylaşılmaması için süre ile sınırlandırılmaksızın her türlü önlemi alırlar.

b) Kurum tarafından görüntülenmesi sağlanan ve aktarım yapılan veriler, kişisel verilerin gizliliği ilkesine bağlı kalmak şartıyla ilgili mevzuat, uluslararası anlaşmalar ve kamu hizmetinin gerektirdiği yükümlülüklerle göre kullanılır. Aktarılan verilerin; yetkisi olmayan kişi, kurum ve kuruluşların eline geçmemesi için gerekli tüm tedbirler alınır.

(2) Bu Yönetmelik hükümlerine göre verilere erişen Kurum personeli dâhil olmak üzere veri aktarımı yapılan gerçek ve tüzel kişiler, sağlık hizmeti sunucularına ait bilgi işlem sistemlerinin yazılımını ve donanımını sağlayan gerçek ve tüzel kişiler;

a) Elde ettikleri verilerin gizliliğini korumak ve güvenliğini sağlamak, verileri yetkisiz kişilerin görmesini, öğrenmesini, eline geçirmesini ve amacı dışında kullanmasını önlemek amacıyla gerekli tedbirleri almak,

b) Verilerin aktarımı ve korunması hususunda mevzuatta yer alan hükümlere uymak, zorundadır.

(3) Kişisel verilerin güvenliğinin sağlanmasına yönelik Kurul tarafından çıkarılan düzenlemelere uyulur.

Uygulanacak müeyyideler

MADDE 22 - (1) Kişisel verilerin korunması hususu ile ilgili hükümlere aykırı hareket edenler hakkında kabahatler bakımından, 6698 sayılı Kanunun 18 inci maddesi hükümlerinin uygulanmasını teminen durum Kurula bildirilir.

(2) Kurum tarafından kendilerine erişim yetkisi verilen kişilerden, kişisel verileri değiştiren veya bütünlüğünü bozanlar hakkında 5237 sayılı Kanunun ilgili maddeleri uyarınca suç duyurusunda bulunulur.

Verilerin korunmasına ilişkin Kurumca yürütülecek işlemler

MADDE 23 - (1) Kurum, Kurum veri kayıt sisteminde tuttuğu verilerin her türlü tehlikeye karşı güvenliğinin sağlanması amacıyla güvenlik önlemlerinin hazırlanmasını, uygulamaya konulmasını, güncellenmesini ve denetlenmesini sağlamakla yükümlüdür.

(2) Veri aktarım talebinde bulunan gerçek ve tüzel kişilerin Kurum veri kayıt sistemine doğrudan erişimine izin verilmez. Talep edilen verinin aktarımı sağlanır.

(3) HSGM, veri taleplerini karşılarken gerekli güvenlik önlemlerini alır. Kurum veri kayıt sistemine şifre ile erişimler, gerçek kişi (ad-soyad veya domain kullanıcı adı) kullanıcı şifreleri kullanılarak Kurumun belirlediği güvenlik önlem ve uygulamaları çerçevesinde yapılır. Erişimler, HSGM tarafından güvenlik önlemleri çerçevesinde kayıt altına alınır.

(4) Kurum veri kayıt sisteminde sadece test edilmiş ve onaylanmış Kurum uygulamaları aracılığı ile toplanan veriler esas alınır. Hatalar sonucu veya farklı nedenlerle verilerde değiştirilme, silinme,

eklenme ihtiyacı oluřursa bu durum ilgili birim ile HSGM'deki yetkilendirilmiř kiřiler ile tutanak altına alınmak suretiyle gerekli iřlemler yapılır.

(5) Kurumca veriye eriřim yetkisi verilmiř personelin Kurumdan ayrılması veya grev yeri deęiřiklięi halinde yetkisiz kullanımın nlenebilmesi amacıyla eriřim yetkileri ilgili birim tarafından resmi yazı ile HSGM'ye bildirilir. HSGM tarafından yetkilendirme sona erdirilmeden ayrılıř iřlemleri yapılamaz. Birim amirleri gerekli bildirim ve iptal etme iřlemlerinin yerine getirilmesinden sorumludur. Personelin zerinde alıřtıęı veri ile ilgili sorumluluęu Kurumdan ayrıldıktan sonra da devam eder.

BEŐİNCİ BLM

Kurum Yazılımları ile Kurum DıŐı Yazılımların Entegrasyonu, Entegrasyon Usul

Kurum yazılımları ile kurum dıŐı yazılımların entegrasyonu

MADDE 24 - (1) Kurum ve Kurul tarafından belirlenen gvenlik tedbirlerine uyulmak kaydıyla dıŐ paydařların, Kuruma olan ykmllklerini yerine getirebilmek iin yazılımlarının Kurum yazılımları ile entegrasyon taleplerini karara baęlamaya Kurum yetkilidir.

Entegrasyon usul

MADDE 25 - (1) Yazılım entegrasyon ihtiyacı sz konusu olduęunda, Kurum dıŐı yazılım sahibi gerek ya da tzel kiřiler HSGM'ye yazılı baŐvuruda bulunur.

ALTINCI BLM

Son Hkmler

Yrrlk

MADDE 26 - (1) Bu Ynetmelik yayımı tarihinde yrrlęe girer.

Yrtme

MADDE 27 - (1) Bu Ynetmelik hkmlerini Sosyal Gvenlik Kurumu BaŐkanı yrtr.

TEBLİĞLER VE GENELGELER

Bölüm İçeriği

- Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğ
- Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ
- Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ
- 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi
- BDDK - Sır Niteliğindeki Bilgilerin Paylaşılması Genelgesi (2022/1)

Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğ

Resmi Gazete Tarihi : 06.12.2021

Resmi Gazete Sayısı : 31681

PERSONEL SERTİFİKASYON MEKANİZMASINA İLİŞKİN USUL VE ESASLAR HAKKINDA TEBLİĞ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Tebliğin amacı, (TS) EN ISO/IEC 17024 nolu standarda uygun olarak Veri Koruma Görevlisi Programı dâhilinde kişilerin sertifikasyonuna ilişkin usul ve esasları belirlemektir.

Kapsam

MADDE 2 - (1) Bu Tebliğ, (TS) EN ISO/IEC 17024 standardına uygun olarak akredite olan ve Kurum tarafından yetkilendirilen personel belgelendirme kuruluşları tarafından yürütülecek sertifikasyon faaliyetleri ile veri koruma görevlilerini ve adaylarını kapsar.

Dayanak

MADDE 3 - (1) Bu Tebliğ, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununun 22 nci maddesinin birinci fıkrasının (e) bendi ve 17/1/2018 tarihli ve 2018/11296 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliğinin 7 nci maddesinin birinci fıkrasının (g) ve (ı) bentleri ile 18 inci maddesinin birinci fıkrasının (a) bendine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Tebliğin uygulanmasında;

a) Akreditasyon: Türk Akreditasyon Kurumu tarafından; belgelendirme, doğrulama, yeterlik testi sağlama ile diğer uygunluk değerlendirme kuruluşlarının ulusal ve uluslararası kabul görmüş teknik kriterlere göre değerlendirilmesini, yeterliğinin onaylanmasını ve düzenli aralıklarla denetlenmesini,

- b) Başkan: Kişisel Verileri Koruma Kurumu Başkanını,
- c) Kanun: 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununu,
- ç) Katılım belgesi: Kurul tarafından usul ve esasları belirlenen eğitim programını tamamlayanlara Kurum tarafından verilen belgeyi,
- d) Kurul: Kişisel Verileri Koruma Kurulunu,
- e) Kurum: Kişisel Verileri Koruma Kurumunu,
- f) Personel: Sertifika almak isteyen gerçek kişiyi,
- g) Personel belgelendirme kuruluşu: Türk Akreditasyon Kurumu tarafından (TS) EN ISO/IEC 17024 standardı kapsamında akredite edilen, sertifikasyona ilişkin ilgili sınavlarda başarılı olanları belgelendirmeye yetkili kuruluşu,
- ğ) Program: Kurul tarafından ana hatları belirlenerek yayımlanan veri koruma görevlisinin sertifikasyon faaliyetlerine ilişkin şartların belirlendiği dokümanı,
- h) Program kullanma onayı: Kurul tarafından yayımlanacak kişisel verilerin korunması alanındaki sertifikasyona konu programların, personel belgelendirme kuruluşu tarafından kullanılabilmesini sağlayan Kurum ön iznini,
- ı) SERTABİS: Kurum tarafından, sertifikasyon faaliyetinin tarafsız, şeffaf ve etkin sürdürülmesini sağlamak amacıyla oluşturulan, personel belgelendirme kuruluşunun ve sertifika sahibi kişilerin bilgilerinin yanı sıra sertifikaların kapsamlarının, tarihlerinin, numaralarının, geçerlilik sürelerinin ve personel belgelendirme kuruluşunun bilgilerinin sorgulanabildiği, Sertifika Takip ve Doğrulama Bilgi Sistemini,
- i) Sertifikasyon: Kanun ve ilgili mevzuat çerçevesinde, sertifika almak için gereken şartları taşıyan ve sınavda başarılı olanların belgelendirilmesi işlemini,
- j) Sınav: Adayların bilgi, beceri ve yetkinliklerinin değerlendirilmesi amacıyla personel belgelendirme kuruluşları tarafından programa ve akreditasyon kurallarına göre gerçekleştirilen değerlendirme sürecini,
- k) Sözleşme: Personel belgelendirme kuruluşunun yetkilendirme kapsamında Program kullanma onayı için Kurum ile yapacağı sözleşmeyi,

l) Standart: Uluslararası Standardizasyon Teşkilatı tarafından kabul edilen "(TS) EN ISO/IEC 17024 Uygunluk Değerlendirmesi Personel Belgelendirmesi Yapan Kuruluşlar İçin Genel Şartlar" standardını,

m) TÜRKAK: Türk Akreditasyon Kurumunu,

n) Veri koruma görevlisi: Sınavda başarılı olarak veri koruma görevlisi unvanını kullanmaya hak kazanan gerçek kişiyi,

o) Yetkilendirme: TÜRKAK tarafından akredite edilmiş personel belgelendirme kuruluşuna Kurum tarafından bu Tebliğ kapsamında faaliyete başlamak için verilen izni,

ifade eder.

(2) Bu Tebliğde yer almayan tanımlar için Kanunda ve Standartta yer alan tanımlar geçerli olacaktır.

İKİNCİ BÖLÜM

Genel Esaslar

Genel esaslar

MADDE 5 - (1) Sertifikasyon işlemleri bu Tebliğde ve Standartta belirtilen usul ve esaslara uygun olarak yürütülür.

(2) Sertifikasyon için aşağıdaki esaslar uygulanır:

a) Personel belgelendirme kuruluşu tarafından, sertifikasyon faaliyetlerinin tüm süreçlerinde tarafsızlığın ve şeffaflığın sağlanması gerekmektedir.

b) Sertifikasyon faaliyetleri esnasında herhangi bir eksiklik ve aksaklık yaşanmaması adına personel belgelendirme kuruluşunun gerekli ve yeterli personele, kaynağa, fiziki, teknik ve idari altyapıya sahip olması gerekmektedir.

c) Veri sorumlusunun ve/veya veri işleyeninin bünyesinde veri koruma görevlisi istihdam etmesi, veri sorumlusunun ve veri işleyeninin Kanuna ve ilgili mevzuata uyma sorumluluğunu ortadan kaldırmaz.

ç) Katılım belgesi, veri koruma görevlisi unvanını kullanma ve veri koruma görevlisi olarak faaliyet gösterme imkânı sağlamaz.

(3) Katılım belgesine ilişkin usul ve esaslar Kurul tarafından belirlenerek ilan edilir.

ÜÇÜNCÜ BÖLÜM

Veri Koruma Görevlisi

Veri koruma görevlisi

MADDE 6 - (1) Katılım belgesini alan kişilerden sınavda başarılı olanlar veri koruma görevlisi unvanını kullanmaya hak kazanırlar.

(2) Veri koruma görevlisinin sertifikalandırıldıkları program kapsamında kişisel verilerin korunması mevzuatı açısından yeterli bilgiye sahip olduğu kabul edilir.

(3) Veri koruma görevlisi, sadece sertifikalarının geçerlilik süresi boyunca bu unvanı kullanabilir.

DÖRDÜNCÜ BÖLÜM

Program, Başvuru, Ölçme ve Değerlendirme, Geçerlilik ve Ücretler

Program kullanma onayı ve sözleşme

MADDE 7 - (1) Kurumun yayımladığı programın, personel belgelendirme kuruluşu tarafından akreditasyon sürecinde başvuru aşamasında kullanılabilmesi ancak Kurulun program kullanma onayını müteakiben sözleşmenin imzalanmasıyla mümkündür.

(2) Personel belgelendirme kuruluşu, programı Kurum tarafından yayımlanan güncel haliyle, herhangi bir değişiklik yapmaksızın kullanmak zorundadır.

(3) Personel belgelendirme kuruluşu, sözleşmenin imzalanmasını müteakiben 6 ay içinde sözleşme ile birlikte TÜRKAK'a akreditasyon başvurusunda bulunmalıdır. Bu süre içerisinde başvuruda bulunulmaması halinde sözleşme hükümsüz hale gelir.

Yetkilendirme

MADDE 8 - (1) TÜRKAK tarafından akredite edilen personel belgelendirme kuruluşu, belge vermeye başlamak için Kuruma yetkilendirme başvurusunda bulunmak zorundadır. Yetkilendirilmeyen personel belgelendirme kuruluşu bu Tebliğ kapsamında faaliyet gösteremez.

Yetkilendirmenin durdurulması

MADDE 9 - (1) TÜRKAK tarafından akreditasyonu tamamen veya kısmen askıya alınan ya da kapsamı daraltılan personel belgelendirme kuruluşunun, bu durumu 7 gün içinde Kuruma bildirmesi zorunludur.

(2) TÜRKAK tarafından akreditasyonun tamamen veya kısmen askıya alınması ya da kapsamının daraltılması hâllerinde, TÜRKAK tarafından belirlenen askıya alma veya kapsam daraltma süresi boyunca, personel belgelendirme kuruluşunun yetkilendirmesi Kurum tarafından durdurulur.

(3) Yetkilendirmesi durdurulan personel belgelendirme kuruluşu, durdurma süresi boyunca sertifikasyon faaliyetlerine devam edemez.

Yetkilendirmenin iptal edilmesi

MADDE 10 - (1) TÜRKAK tarafından akreditasyonu geri çekilen personel belgelendirme kuruluşunun, bu durumu 3 gün içinde Kuruma bildirmesi zorunludur.

(2) Personel belgelendirme kuruluşunun akreditasyonunun geri çekilmesi hâlinde veya sertifikasyon faaliyetine yönelik niteliği ve yeterliği ile ilgili olarak Kuruma sunulan bilgi ve belgelerin gerçeğe aykırı olduğunun tespiti ya da programın kapsamının dışında sertifikasyon faaliyetlerinin yürütüldüğünün anlaşılması hâllerinde, personel belgelendirme kuruluşunun yetkilendirilmesi Kurum tarafından iptal edilir.

(3) Personel belgelendirme kuruluşunun yetkilendirmesinin iptal edildiği bilgisi, Kurumun resmi internet sitesinde ilan edilir.

(4) Akreditasyonu geri çekilen personel belgelendirme kuruluşunun, bu durumu süresi içinde Kuruma bildirmemesi hâlinde, yetkilendirmesi iptal edildikten sonra yeniden program kullanma onayı alabilmesi için yetkilendirmenin iptali kararının üzerinden 6 ay geçmesi gerekmektedir.

Veri koruma görevlisi sertifikası sınavlarına başvuru

MADDE 11 - (1) Sınav tarihinden önceki son 4 yıl içinde katılım belgesi almış olanlar veya geçerli bir veri koruma görevlisi sertifikasına sahip olanlar arasından programda belirlenen şartları haiz olanlar veri koruma görevlisi sertifikası sınavına başvurmaya hak kazanırlar.

(2) Personel belgelendirme kuruluşu, bu madde kapsamında gelen başvuruların bu Tebliğde belirtilen ve programda belirlenen şartlara uygun olup olmadığının kontrolü ile sınav başvurusuna ilişkin iş ve işlemleri yürütme hususunda gerekli dikkat ve özeni göstermekle yükümlüdür.

Sınav ve değerlendirme

MADDE 12 - (1) Personel belgelendirme kuruluşunca yapılacak olan sınavlar, en geç sınavdan 15 gün önce personel belgelendirme kuruluşu tarafından ilan edilmelidir.

(2) Personel belgelendirme kuruluşunca yapılan sınavda başarılı olan adaylar, veri koruma görevlisi sertifikasını almaya hak kazanırlar.

Ücretler

MADDE 13 - (1) Personel belgelendirme kuruluđu tarafından program kapsamında alınacak ücretlerin belirlenmesinde ve güncellenmesinde Kurul yetkilidir. Belirlenen ücret her takvim yılı başında Kurum tarafından ilan edilir.

Geçerlilik süreleri

MADDE 14 - (1) Bu Tebliğ kapsamında verilen sertifikaların geçerlilik süreleri sınav sonuçlarının ilanından itibaren 4 yıldır.

(2) Geçerlilik süresi dolmadan sertifikasını yenilemek isteyen veri koruma görevlisi, programda belirlenen şartlar dâhilinde yeniden personel belgelendirme kuruluşuna başvurmalıdır.

BEŞİNCİ BÖLÜM

Yükümlülükler

Sertifika Takip ve Doğrulama Bilgi Sistemi (SERTABİS)

MADDE 15 - (1) Kurum, sertifikasyon faaliyetinin tarafsız, şeffaf ve etkin sürdürülmesini sağlamak amacıyla kamuya açık bir biçimde sorgulama imkânı tanıyan Sertifika Takip ve Doğrulama Bilgi Sisteminin kurulmasından ve yönetilmesinden sorumludur.

(2) SERTABİS'te; katılım belgesinde yer alan bilgiler, personel belgelendirme kuruluşunun bilgileri ve statülerinde gerçekleşen değişiklikler ile sertifika sahibi kişilerin bilgileri, program kapsamında yapılan sınavların tarihlerinin yanı sıra sınavda başarılı olan kişilerin; sertifika tarihleri, sertifika numaraları, sertifika geçerlilik süreleri ve sertifika statülerine dair bilgiler yer alır.

Kuruma bilgi ve belge gönderme

MADDE 16 - (1) Sertifikasyon sürecinin takibinin gerçekleştirilmesi, aksaklıkların giderilmesi ve sürece ilişkin uygulama birliğinin sağlanması konusunda gerekli düzenlemelerin yapılmasını teminen Kurum, ilgili taraflardan program kapsamında tüm bilgi ve belgeleri isteyebilir. Taraflar, istenen bilgi ve belgeleri 15 gün içinde Kuruma göndermek zorundadır. Kuruma gönderilmiş olan bilgi ve belgelerde herhangi bir değişiklik olması hâlinde, söz konusu değişiklik öğrenilmesinden itibaren 15 gün içinde Kuruma bildirilir.

(2) Personel belgelendirme kuruluşu, sertifika verdiği kişilerin kimlik ve iletişim bilgilerini, sertifika tarihini, numarasını ve statüsünü sertifikasyon tarihinden itibaren 15 gün içinde SERTABİS'e yükler. Bu bilgilerde herhangi bir değişiklik olması hâlinde, söz konusu değişiklik öğrenilmesinden itibaren 15 gün içinde SERTABİS'e yüklenir.

ALTINCI BÖLÜM

Şikâyet ve İtirazlar

Şikâyet, itiraz ve Kuruma başvuru

MADDE 17 - (1) Program kapsamında şikâyet veya itiraz başvuruları personel belgelendirme kuruluşuna yapılır. Başvuruların hangi yöntemlerle alınacağı ve sonuçlandırılacağı personel belgelendirme kuruluşu tarafından belirlenir.

(2) Personel belgelendirme kuruluşu tarafından şikâyet veya itiraz başvurusunun reddedilmesi ya da başvurudan itibaren 30 gün içinde cevap verilmemesi hâllerinde, şikâyet veya itiraz sahibi, personel belgelendirme kuruluşunun cevabını öğrendiği tarihten itibaren 30 ve her hâlde başvuru tarihinden itibaren 60 gün içinde Kuruma başvurabilir.

(3) Personel belgelendirme kuruluşuna şikâyet veya itiraz başvuru yolu tüketilmeden Kuruma başvuruda bulunulamaz.

(4) Kurum, bu başvuruları değerlendirirken ilgili taraflardan her türlü bilgi ve belgeyi isteyebilir. İlgili taraflar, istenen bilgi ve belgeleri 15 gün içinde Kuruma göndermek zorundadır.

YEDİNCİ BÖLÜM

Çeşitli ve Son Hükümler

Yaptırımlar

MADDE 18 - (1) Bu Tebliğde belirtilen yükümlülöklere aykırı davranan personel belgelendirme kuruluşunun yetkilendirmesini durdurmaya veya iptal etmeye Kurul yetkilidir.

Düzenleme yetkisi

MADDE 19 - (1) Bu Tebliğde yer almayan ya da açıklık bulunmayan konularda ilgili mevzuat hükümleri çerçevesinde karar vermeye ve düzenleme yapmaya Kurul yetkilidir.

Yürürlük

MADDE 20 - (1) Bu Tebliğ yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 21 - (1) Bu Tebliğ hükümlerini Kişisel Verileri Koruma Kurumu Başkanı yürütür.

Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ

Resmi Gazete Tarihi : 10.03.2018

Resmi Gazete Sayısı : 30356

VERİ SORUMLUSUNA BAŞVURU USUL VE ESASLARI HAKKINDA TEBLİĞ

Amaç ve kapsam

MADDE 1 - (1) Bu Tebliğ, veri sorumlusuna başvuru ve işlemin ayrıca bir maliyet gerektirmesi hâlinde alınacak ücret ile ilgili usul ve esasları belirlemek üzere hazırlanmıştır.

Dayanak

MADDE 2 - (1) Bu Tebliğ, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununun 13 üncü maddesi ve 22 nci maddesinin birinci fıkrasının (e) ve (g) bentlerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 3 - (1) Bu Tebliğde geçen;

- a) Başvuru: Kanunun 13 üncü maddesi kapsamında yapılan başvuruyu,
- b) Güvenli Elektronik İmza: Münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, imzalanmış elektronik veride sonradan herhangi bir değişiklik yapıp yapılmadığının tespitini sağlayan elektronik imzayı,
- c) İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,
- ç) Kanun: 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununu,
- d) Kayıt ortamı: Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı,
- e) Kayıtlı elektronik posta (KEP) adresi: Elektronik iletilerin, gönderimi ve teslimatı da dâhil olmak üzere kullanımına ilişkin olarak hukuki delil sağlayan, elektronik postanın nitelikli şeklini,
- f) Kurul: Kişisel Verileri Koruma Kurulunu,
- g) Kurum: Kişisel Verileri Koruma Kurumunu,

ğ) Mobil imza: Mobil bir cihaz kullanılarak oluşturulan elektronik imzayı ifade eder.

(2) Bu Tebliğde yer almayan tanımlar için Kanundaki tanımlar geçerli olacaktır.

Başvuru hakkı

MADDE 4 - (1) Kişisel verisi işlenen gerçek kişiler, veri sorumlusuna başvuru hakkına sahiptir.

(2) İlgili kişiler, başvurularını Türkçe olarak yapmak kaydıyla bu haktan yararlanabilir.

Başvuru usulü

MADDE 5 - (1) İlgili kişi, Kanununun 11 inci maddesinde belirtilen hakları kapsamında taleplerini, yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletir.

(2) Başvuruda;

a) Ad, soyad ve başvuru yazılı ise imza,

b) Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarası,

c) Tebligata esas yerleşim yeri veya iş yeri adresi,

ç) Varsa bildirim esas elektronik posta adresi, telefon ve faks numarası,

d) Talep konusu,

bulunması zorunludur.

(3) Konuya ilişkin bilgi ve belgeler başvuruya eklenir.

(4) Yazılı başvurularda, veri sorumlusuna veya temsilcisine evrakın tebliğ edildiği tarih, başvuru tarihidir.

(5) Diğer yöntemlerle yapılan başvurularda; başvurunun veri sorumlusuna ulaştığı tarih, başvuru tarihidir.

Başvuruya cevap

MADDE 6 - (1) Veri sorumlusu bu Tebliğ kapsamında ilgili kişi tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlüdür.

(2) Veri sorumlusu, başvuruyu kabul eder veya gerekçesini açıklayarak reddeder.

(3) Veri sorumlusu, cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir.

(4) Cevap yazısının;

a) Veri sorumlusu veya temsilcisine ait bilgileri,

b) Başvuru sahibinin; adı ve soyadını, Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarasını, yabancılar için uyruğunu, pasaport numarasını veya varsa kimlik numarasını, tebligata esas yerleşim yeri veya iş yeri adresini, varsa bildirim esas elektronik posta adresini, telefon ve faks numarasını,

c) Talep konusunu,

ç) Veri sorumlusunun başvuruya ilişkin açıklamalarını,

içermesi zorunludur.

(5) Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak, işlemin ayrıca bir maliyet gerektirmesi hâlinde, 7 nci maddede belirtilen ücret alınabilir. Başvurunun, veri sorumlusunun hatasından kaynaklanması hâlinde alınan ücret ilgiliye iade edilir.

(6) İlgili kişinin talebinin kabul edilmesi hâlinde, veri sorumlusunca talebin gereği en kısa sürede yerine getirilir ve ilgili kişiye bilgi verilir.

Ücret

MADDE 7 - (1) İlgili kişinin başvurusuna yazılı olarak cevap verilecekse, on sayfaya kadar ücret alınmaz. On sayfanın üzerindeki her sayfa için 1 Türk Lirası işlem ücreti alınabilir.

(2) Başvuruya cevabın CD, flash bellek gibi bir kayıt ortamında verilmesi halinde veri sorumlusu tarafından talep edilebilecek ücret kayıt ortamının maliyetini geçemez.

Yürürlük

MADDE 8 - (1) Bu Tebliğ yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 9 - (1) Bu Tebliğ hükümlerini Kişisel Verileri Koruma Kurumu Başkanı yürütür.

Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ

Resmi Gazete Tarihi : 10.03.2018

Resmi Gazete Sayısı : 30356

AYDINLATMA YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMESİNDE UYULACAK USUL VE ESASLAR HAKKINDA TEBLİĞ

Amaç ve kapsam

MADDE 1 - (1) Bu Tebliğin amacı, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununun 10 uncu maddesi uyarınca veri sorumluları veya yetkilendirdiği kişilerce yerine getirilmesi gereken aydınlatma yükümlülüğü kapsamında uyulacak usul ve esasları belirlemektir.

Dayanak

MADDE 2 - (1) Bu Tebliğ, 6698 sayılı Kişisel Verilerin Korunması Kanununun 22 nci maddesinin birinci fıkrasının (e) ve (g) bentlerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 3 - (1) Bu Tebliğde geçen;

- a) Alıcı grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini,
- b) İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,
- c) Kanun: 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununu,
- ç) Kurul: Kişisel Verileri Koruma Kurulunu,
- d) Kurum: Kişisel Verileri Koruma Kurumunu,
- e) Sicil: Başkanlık tarafından tutulan Veri Sorumluları Sicilini,
- f) **(Değişik:RG-28/4/2019-30758)** Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,²¹

²¹ Değişiklik öncesi “Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı,”

g) Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,

ğ) **(Değişik:RG-28/4/2019-30758)** Veri sorumlusu temsilcisi: Türkiye’de yerleşik olmayan veri sorumlularını 30/12/2017 tarihli ve 30286 sayılı Resmî Gazete’de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmeliğin 11 inci maddesinin üçüncü fıkrasında belirtilen konularda asgari temsile yetkili Türkiye’de yerleşik tüzel kişi ya da Türkiye Cumhuriyeti vatandaşı gerçek kişiyi,²² ifade eder.

(2) Bu Tebliğde yer almayan tanımlar için Kanundaki tanımlar geçerli olacaktır.

Aydınlatma yükümlülüğünün kapsamı

MADDE 4 - (1) Kanunun 10 uncu maddesine göre; kişisel verilerin elde edilmesi sırasında veri sorumluları veya yetkilendirdiği kişilerce, ilgili kişilerin bilgilendirilmesi gerekmektedir. Bu yükümlülük yerine getirilirken veri sorumluları veya yetkilendirdiği kişilerce yapılacak bilgilendirmenin asgari olarak aşağıdaki konuları içermesi gerekmektedir:

- a) Veri sorumlusunun ve varsa temsilcisinin kimliği,
- b) Kişisel verilerin hangi amaçla işleneceği,
- c) Kişisel verilerin kimlere ve hangi amaçla aktarılabilceği,
- ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,
- d) İlgili kişinin Kanunun 11 inci maddesinde sayılan diğer hakları.

Usul ve esaslar

MADDE 5 - (1) Veri sorumlusu ya da yetkilendirdiği kişi tarafından sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanılmak suretiyle aydınlatma yükümlülüğünün yerine getirilmesi esnasında aşağıda sayılan usul ve esaslara uyulması gerekmektedir:

- a) İlgili kişinin açık rızasına veya Kanundaki diğer işleme şartlarına bağlı olarak kişisel veri işlendiği her durumda aydınlatma yükümlülüğü yerine getirilmelidir.
- b) Kişisel veri işleme amacı değiştiğinde, veri işleme faaliyetinden önce bu amaç için aydınlatma yükümlülüğü ayrıca yerine getirilmelidir.

²² Değişiklik öncesi “Türkiye’de yerleşik olmayan veri sorumlularını 30/12/2017 tarihli ve 30286 sayılı Resmî Gazete’de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmeliğin 11 inci maddesinin ikinci fıkrasında belirtilen konularda asgari temsile yetkili Türkiye’de yerleşik tüzel kişi ya da Türkiye Cumhuriyeti vatandaşı gerçek kişiyi”

c) (Mülga:RG-28/4/2019-30758)²³

ç) Sicile kayıt yükümlülüğünün bulunması durumunda, aydınlatma yükümlülüğü çerçevesinde ilgili kişiye verilecek bilgiler, Sicile açıklanan bilgilerle uyumlu olmalıdır.

d) Aydınlatma yükümlülüğünün yerine getirilmesi, ilgili kişinin talebine bağlı değildir.

e) Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı veri sorumlusuna aittir.

f) Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir.

g) Aydınlatma yükümlülüğü kapsamında açıklanacak kişisel veri işleme amacının belirli, açık ve meşru olması gerekir. Aydınlatma yükümlülüğü yerine getirilirken, genel nitelikte ve muğlak ifadelerle yer verilmemelidir. Gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandıran ifadeler kullanılmamalıdır.

ğ) Aydınlatma yükümlülüğü kapsamında ilgili kişiye yapılacak bildirim anlaşılır, açık ve sade bir dil kullanılarak gerçekleştirilmesi gerekmektedir.

h) Kanununun 10 uncu maddesinin birinci fıkrasının (ç) bendinde yer alan “hukuki sebep” ten kasıt, aydınlatma yükümlülüğü kapsamında kişisel verilerin Kanununun 5 ve 6 ncı maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiğidir. Aydınlatma yükümlülüğünün yerine getirilmesi esnasında hukuki sebebin açıkça belirtilmesi gerekmektedir.

ı) Aydınlatma yükümlülüğü kapsamında, kişisel verilerin aktarılma amacı ve aktarılabilecek alıcı grupları belirtilmelidir.

i) Aydınlatma yükümlülüğü kapsamında kişisel verilerin, tamamen veya kısmen otomatik yollarla ya da veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yöntemlerden hangisiyle elde edildiği açık bir şekilde belirtilmelidir.

j) Aydınlatma yükümlülüğü yerine getirilirken eksik, ilgili kişileri yanıltıcı ve yanlış bilgilere yer verilmemelidir.

Kişisel verilerin ilgili kişiden elde edilmemesi halinde aydınlatma yükümlülüğü

MADDE 6 - (1) Kişisel verilerin ilgili kişiden elde edilmemesi halinde;

a) Kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde,

²³ Mülga edilen kısım “Veri sorumlusunun farklı birimlerinde kişisel veriler farklı amaçlarla işleniyorsa, aydınlatma yükümlülüğü her bir birim nezdinde ayrıca yerine getirilmelidir.”

b) Kişisel verilerin ilgili kişi ile iletişim amacıyla kullanılacak olması durumunda, ilk iletişim kurulması esnasında,

c) Kişisel verilerin aktarılacak olması halinde, en geç kişisel verilerin ilk kez aktarımının yapılacağı esnada

ilgili kişiyi aydınlatma yükümlülüğünün yerine getirilmesi gerekir.

Yürürlük

MADDE 7 - (1) Bu Tebliğ yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 8 - (1) Bu Tebliğ hükümlerini Kişisel Verileri Koruma Kurumu Başkanı yürütür.

2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi

Cumhurbaşkanlığından:

Konu: Bilgi ve İletişim Güvenliği Tedbirleri

GENELGE

2019/12

Bilginin dijital ortamlara taşınması, bilgiye erişimin kolaylaşması, altyapıların dijital hale gelmesi ve bilgi yönetim sistemlerinin yaygın olarak kullanılması, ciddi güvenlik risklerini beraberinde getirmektedir. Karşılaşılan güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla aşağıdaki tedbirlerin alınması uygun görülmüştür.

1. Nüfus, sağlık ve iletişim kayıt bilgileri ile genetik ve biyometrik veriler gibi kritik bilgi ve veriler yurtiçinde güvenli bir şekilde depolanacaktır.
2. Kamu kurum ve kuruluşlarında yer alan kritik veriler, internete kapalı ve fiziksel güvenliği sağlanmış bir ortamda bulunan güvenli bir ağda tutulacak, bu ağda kullanılacak cihazlara erişim kontrollü olarak sağlanacak ve log kayıtları değiştirilmeye karşı önlem alınarak saklanacaktır.
3. Kamu kurum ve kuruluşlarına ait veriler, kurumların kendi özel sistemleri veya kurum kontrolündeki yerli hizmet sağlayıcılar hariç bulut depolama hizmetlerinde saklanmayacaktır.
4. Mevzuatta kodlu veya kriptolu haberleşmeye yetkilendirilmiş kurumlar tarafından geliştirilen yerli mobil uygulamalar hariç olmak üzere, mobil uygulamalar üzerinden, gizlilik dereceli veri paylaşımı ve haberleşme yapılmayacaktır.
5. Sosyal medya üzerinden gizlilik dereceli veri paylaşımı ve haberleşme yapılmayacaktır.
6. Sosyal medya ve haberleşme uygulamalarına ait yerli uygulamaların kullanımı tercih edilecektir.
7. Kamu kurum ve kuruluşlarınca gizlilik dereceli bilgilerin işlendiği yerlerde yayma güvenliği (TEMPEST) veya benzeri güvenlik önlemleri alınacaktır.
8. Kritik veri, doküman ve belgelerin bulunduğu ve/veya görüşmelerin gerçekleştirildiği çalışma odalarında/ortamlarında mobil cihazlar ve veri transferi özelliğine sahip cihazlar bulundurulmayacaktır.

9. Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgeler kurumsal olarak yetkilendirilmemiş veya kişisel olarak kullanılan cihazlarda (dizüstü bilgisayar, mobil cihaz, harici bellek vb.) bulundurulmayacaktır.
10. Kişisel olarak kullanılanlar da dâhil olmak üzere kaynağından emin olunmayan taşınabilir cihazlar (dizüstü bilgisayar mobil cihazlar, harici bellek/disk, CD/DVD vb.) kurum sistemlerine bağlanmayacaktır. Gizlilik dereceli verilerin saklandığı cihazlar, ancak içerisinde yer alan veriler donanımsal ve/veya yazılımsal olarak kriptolanmak suretiyle kurum dışına çıkarılabilecek; bu amaçla kullanılan cihazlar kayıt altına alınacaktır.
11. Yerli ve milli kripto sistemlerinin geliştirilmesi teşvik edilerek, kurumlara ait gizlilik dereceli haberleşmenin bu sistemler üzerinden gerçekleştirilmesi sağlanacaktır.
12. Kamu kurum ve kuruluşlarınca temin edilecek yazılım veya donanımların kullanım amacına uygun olmayan bir özellik ve arka kapı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) açıklığı içermediğine dair üretici ve/veya tedarikçilerden imkânlar ölçüsünde taahhütname alınacaktır.
13. Yazılımların güvenli olarak geliştirilmesi ile ilgili tedbirler alınacaktır. Temin edilen veya geliştirilen yazılımlar kullanılmadan önce güvenlik testlerinden geçirilerek kullanılacaktır.
14. Kurum ve kuruluşlar, siber tehdit bildirimleri ile ilgili gerekli tedbirleri alacaktır.
15. Üst düzey yöneticiler de dahil olmak üzere, personelin sistemlere erişim yetkilendirmelerinin, fiilen yürütülen işler ve ihtiyaçlar nazara alınarak yapılması sağlanacaktır.
16. Endüstriyel kontrol sistemlerinin internete kapalı konumda tutulması sağlanacak, söz konusu sistemlerin internete açık olmasının zorunlu olduğu durumlarda ise gerekli güvenlik önlemleri (güvenlik duvarı, uçtan uca tünelleme yöntemleri, yetkilendirme ve kimliklendirme mekanizmaları vb.) alınacaktır.
17. Milli güvenliği doğrudan etkileyen stratejik önemi haiz kurum ve kuruluşların üst yöneticileri ile kritik altyapı, tesis ve projelerde görev alacak kritik önemi haiz personel hakkında ilgili mevzuat çerçevesinde güvenlik soruşturması veya arşiv araştırması yaptırılacaktır.
18. Kamu e-posta sistemlerinin ayarları güvenli olacak biçimde yapılandırılacak, e-posta sunucuları, ülkemizde ve kurumun kontrolünde bulundurulacak ve sunucular arasındaki iletişimin şifreli olarak yapılması sağlanacaktır.

19. Kurumsal olmayan şahsi e-posta adreslerinden kurumsal iletişim yapılmayacak, kurumsal e-postalar şahsi amaçlarla (özel iletişim, kişisel sosyal medya hesapları vb.) kullanılmayacaktır.

20. Haberleşme hizmeti sağlamak üzere yetkilendirilmiş işletmeciler Türkiye’de internet değişim noktası kurmakla yükümlüdür. Yurtiçinde değiştirilmesi gereken yurtiçi iletişim trafiğinin yurtdışına çıkarılmamasına yönelik tedbirler alınacaktır.

21. İşletmeciler tarafından, kritik kurumların bulunduğu bölgelerdeki veriler, radyolink ve benzeri yöntemlerle taşınmayacak, fiber optik kablolar üzerinden taşınacaktır. Kritik veri iletişimde, radyolink haberleşmesi kullanılmayacak; ancak kullanımın zorunlu olduğu durumlarda veriler milli kript sistemlerine sahip cihazlar kullanılarak kriptolanacaktır.

Güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla ulusal ve uluslararası standartlar ve bilgi güvenliği kriterleri çerçevesinde, kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerde uygulanmak üzere farklı güvenlik seviyeleri içeren “Bilgi ve İletişim Güvenliği Rehberi” Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı koordinasyonunda, ilgili kamu kurum ve kuruluşları tarafından gereken katkı sağlanarak hazırlanacak ve www.cbddo.gov.tr adresinde yayımlanacaktır. Rehber ihtiyaçlar, gelişen teknoloji, değişen şartlar ile Ulusal Siber Güvenlik Stratejisi ve eylem planlarında yapılacak değişiklikler göz önünde bulundurularak güncellenecektir.

Tüm kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerde yeni kurulacak bilgi sistemlerinde, Rehberde yer verilen usul ve esaslara uyulması zorunludur. Mevcut bilgi teknolojisi altyapıları, güvenlik seviyesi öncelikleri dikkate alınarak yayımlanmasını müteakip Rehberde yer alacak plan çerçevesinde kademeli olarak bu esaslara uyumlu hale getirilecektir. Uyum çalışmalarında ve yeni kurulacak bilgi sistemlerinde, belirtilen adreste yayımlanan güncel sürüm dikkate alınacaktır.

Milli güvenliğin sağlanması ve gizliliğin korunması kapsamında yürütülen görev ve faaliyetler hariç olmak üzere kurum ve kuruluşlar, Rehberin uygulanmasına ilişkin denetim mekanizmalarını oluşturacak ve yılda en az bir defa uygulamayı denetleyecektir. Denetim sonuçları ile yapılan düzeltici ve önleyici faaliyetler, Rehberde belirtilen usul ve esaslara göre bir rapor halinde Dijital Dönüşüm Ofisine iletilecektir.

Bilgilerini ve gereğini rica ederim.

5 Temmuz 2019

Recep Tayyip ERDOĞAN

CUMHURBAŞKANI

BDDK - Sır Niteliğindeki Bilgilerin Paylaşılması Genelgesi (2022/1)

T.C.

BANKACILIK DÜZENLEME VE DENETLEME KURUMU

Sayı: 24049440-010.06.02

Konu: Sır Niteliğindeki Bilgilerin Paylaşılması Hk.

GENELGE

(2022/1)

Bilindiği üzere, Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik (Yönetmelik) 04/06/2021 tarihli ve 31501 sayılı Resmî Gazete’de yayımlanmış olup, 24/12/2021 tarihli ve 31699 sayılı Resmî Gazete’de yayımlanan değişiklik çerçevesinde 01/07/2022 tarihi itibarıyla yürürlüğe girmiştir.

Söz konusu Yönetmeliğe ilişkin olarak uygulamada yaşanabilecek tereddütleri gidermek amacıyla, Yönetmeliğin uygulanmasında, 5411 sayılı Bankacılık Kanununun 73 üncü maddesinin beşinci fıkrası ile 93 üncü maddesi çerçevesinde alınan 11/08/2022 tarihli ve 10295 sayılı Kurul Kararı ile onaylanan ekte yer alan açıklamaların dikkate alınması gerekmektedir.

Tebliğ olunur.

Mehmet Ali AKBEN

Başkan

Ek: Açıklamalar

SIR NİTELİĞİNDEKİ BİLGİLERİN PAYLAŞILMASI HAKKINDA YÖNETMELİĞİN UYGULANMASI HAKKINDA EK AÇIKLAMALAR

1. Sır Saklama Yükümlülüğüne İlişkin Açıklamalar (Madde 4)

1.1. Banka çalışanlarına ait verilerin banka sırrı niteliğindeki bilgi olarak değerlendirilip değerlendirilmeyeceği:

5411 sayılı Bankacılık Kanununun (**Kanun**) 73 üncü maddesinin üçüncü fıkrası uyarınca, bankacılık faaliyetlerine özgü olarak bankayla müşteri ilişkisi kurulduktan sonra oluşan veriler müşteri sırrı niteliğini haiz olmaktadır. 04/06/2021 tarihli ve 31501 sayılı Resmî Gazete’de yayımlanan Sır Niteliğindeki Bilgilerin Paylaşılmasına İlişkin Yönetmeliğin (**Yönetmelik**) 4 üncü maddesinin üçüncü ve dördüncü fıkralarında da bankacılık faaliyetlerine özgü olarak bankalarla müşteri ilişkisi kurulduktan sonra oluşan gerçek ve tüzel kişilere ait verilerin müşteri sırrı hâline geleceği, bir gerçek veya tüzel kişi müşterinin, bankanın müşterisi olduğunu gösterir her türlü bilginin de müşteri sırrı kapsamında olduğu, kişisel veriler de dâhil olmak üzere, bankalar ile müşteri ilişkisi kurulmadan önce de var olan ve başka bir bankanın müşteri sırrı niteliğinde olmayan gerçek ve tüzel kişilere ilişkin verilerin, tek başına sır kapsamında bulunmadığı ancak ilgili kişinin banka müşterisi olduğunu gösterecek şekilde, tek başına ya da üçüncü fıkrada belirtilen müşteri ilişkisinin kurulmasından sonra oluşan verilerle birlikte işlendiğinde müşteri sırrı haline geleceği düzenlenmiştir.

Bu kapsamda, banka ile müşteri ilişkisi bulunmayan veya müşteri ilişkisi bulunsa dahi işveren-çalışan ilişkisinden kaynaklı olarak elde edilen banka çalışanına ait kişisel bilgilerin (T.C. kimlik numarası, adres, telefon, insan kaynakları verileri gibi), banka sırrı niteliğindeki bir bilgi ya da veriyle birlikte işlenmemiş olması kaydıyla, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında kişisel veri olarak ele alınması gerekmektedir.

Bununla birlikte, insan kaynakları verileri gibi, banka çalışanlarına ait kimi veriler bir bankanın mali durumu hakkında ya da kredi verme ve mevduat toplama gibi temel faaliyetlerine ilişkin banka yönetim esasları ve bankanın uyguladığı teknik yöntemler ile banka potansiyeli hakkında bilgiler barındırabileceğinden, bankaca korunmasında ve gizli tutulmasında yarar görülmesi halinde bu nitelikteki verilerin de “banka sırrı” kapsamında ele alınması mümkündür.

Diğer taraftan, yukarıda da belirtildiği üzere, banka ile çalışanı arasında müşteri ilişkisi bulunduğu durumlarda, söz konusu çalışana ilişkin kişisel bilgilerin bu kişinin banka müşterisi olduğunu gösterecek şekilde, tek başına ya da müşteri ilişkisinin kurulmasından sonra oluşan verilerle birlikte işlendiğinde müşteri sırrı haline geleceği de tabiidir.

2. Sır Saklama Yükümlülüğünden İstisna Tutulan Hallere İlişkin Açıklamalar (Madde 5)

2.1. Yönetmeliğin 5 inci maddesinin dördüncü fıkrası (“...Uyum riski amacıyla yapılacak paylaşımların, paylaşımı yapan ya da paylaşımın yapıldığı karşı tarafın tabi olduğu ulusal ya da uluslararası bir mevzuattan kaynaklanması şarttır.”) kapsamında, uyum riski yönetimi için talep edilen bilginin geçerli bir mevzuat maddesinden kaynaklandığı veya ilgili düzenleyicinin mevzuatın kendisine verdiği hak ile ana ortaktan uygulamasını talep ettiği bir kontrol çerçevesinde olduğu somut şekilde ortaya konulabiliyorsa ya da uyum riski kapsamında talep edilen bilgi ana ortaklığın/hâkim ortağın yasal yükümlülükleri çerçevesinde oluşturduğu dâhili politikalara/iş süreçlerine dayanıyorsa Yönetmeliğin 6 ncı maddesinin birinci fıkrasının (ç) bendine bağlı kalınmaksızın “ortak müşteri” niteliğinde olmayan müşteri bilgilerinin paylaşılıp paylaşılamayacağı:

Yönetmeliğin 5 inci maddesinin dördüncü fıkrasında; 5 inci maddenin ikinci fıkrasının (b) bendi ve üçüncü fıkrası kapsamında risk yönetimi amacıyla yapılabilecek paylaşımların, 11/7/2014 tarihli ve 29057 sayılı Resmî Gazete’de yayımlanan Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmeliğinde (İSEDES Yönetmeliği) yer verilen risk yönetim sistemi içinde yer alan uyum, kredi, itibar riskleri de dâhil olmak üzere tüm risk kategorilerine ilişkin risk yönetim faaliyetlerini kapsadığına hükmedilmiştir.

Yönetmeliğin 5 inci maddesinin ikinci fıkrasının (b) bendi uyarınca da; gizlilik sözleşmesi yapılması ve sadece belirtilen amaçlar ile sınırlı kılınması koşuluyla konsolide finansal tablo hazırlama çalışmaları, risk yönetimi ve iç denetim uygulamaları kapsamında bankaların sermayelerinin yüzde on veya daha fazlasına sahip olan yurt içinde veya yurt dışında yerleşik kredi kuruluşu ile finansal kuruluşlar da dâhil ana ortaklıklarına bilgi ve belge verilmesi sır saklama yükümlülüğünden istisna tutulmuştur.

Bu kapsamda, Yönetmelik hükümleri uyarınca risk yönetimi ve konsolidasyon amacı ile müşteri bilgisi paylaşılması mümkün olmakla birlikte **söz konusu paylaşımların “ölçülü” olması beklenmektedir.** Yapılacak paylaşımların ölçülü olabilmesi için sağlaması gereken asgari unsurlara da Yönetmeliğin 6 ncı maddesinin birinci fıkrasında yer verilmiş olup, bunların başında da “yapılacak paylaşımların yalnızca paylaşım amacının gerektirdiği kadar veriyi içermesi ve paylaşımına konu edilen tüm veri setinin belirtilen paylaşım amaçlarının gerçekleştirilmesi için gerekli olduğunun gösterilebilir olması” gerekmektedir.

Bunun yanında, Yönetmeliğin 6 ncı maddesinin birinci fıkrasına göre bilgisi paylaşılacak müşteri aynı zamanda ana ortaklığın/hakim ortağın da ortak müşterisi değilse paylaşılacak söz konusu

gerçek/tüzel kişi müşteriye ilişkin sır niteliğindeki bilgilerin, anılan müşterinin kimliğini belirli veya belirlenebilir kılacak nitelikte olmaması, diğer bir deyişle açık bir şekilde paylaşılmaması gerekmektedir. Ayrıca, Yönetmeliğin 6 ncı maddesinin sekizinci fıkrası uyarınca, **sır niteliğindeki müşteri bilgilerinin açık bir şekilde paylaşılabilmesi için zorunlu tutulan ortak müşteri olma şartı, Yönetmeliğin 5 inci maddesinin ikinci fıkrasının (b) bendi ile üçüncü fıkrası kapsamında yapılacak paylaşımlar için olmak üzere ve yalnızca aşağıdaki durumlarda aranmamaktadır:**

1. Kurumun paylaşım öncesinde uygun görüşünün alınmış olması kaydıyla, kredi karşılık hesaplamaları ile içsel sermaye yeterliliği hesaplamaları gibi çok sayıda müşteriye ilişkin kapsamlı veri paylaşımını gerektiren paylaşımlar,

2. Kurumun paylaşım öncesinde uygun görüşünün alınmış olması kaydıyla, karşı tarafın uyum riski amacıyla yapılacak paylaşımlar,

3. Kurumun paylaşım öncesinde uygun görüşünün alınmış olmasına gerek olmaksızın, banka ana sermayesinin yüzde onu veya daha fazlası oranında kredi kullanılmış bir gerçek ya da tüzel kişiye veya bir risk grubuna ait verileri içeren konsolide risk yönetimi amacıyla yapılacak paylaşımlar.

Bu çerçevede, bankanın ana ortaklığının/hakim ortağının kendi uyum riskini yönetebilmesi amacıyla, banka tarafından ana ortaklık/hakim ortak ile müşteri sırrı niteliğindeki bilgilerin açık bir şekilde paylaşılması mümkün olmakla birlikte, bankanın bu kapsamda Yönetmeliğin 6 ncı maddesinin sekizinci fıkrası uyarınca Kuruma yapacağı başvuruda, uyum riski çerçevesinde ana ortaklık/hakim ortak ile yapılması planlanan paylaşım kapsamında hangi verilerin paylaşılacağı, paylaşılacak verilerin paylaşım amacının yerine getirilmesi için gerekli olup olmadığı ve uyum riski yönetimi için talep edilen bilgilerin geçerli bir mevzuat hükmünden kaynaklanıp kaynaklanmadığının somut bir şekilde ortaya konulması gerekmekte ve uyum riskine konu yabancı mevzuat hükümlerinin orijinal metinleri ile birlikte Türkçe tercümelerinin de başvuru kapsamında Kuruma iletilmesi ve bu kapsamda bankanın Yönetmeliğin 7 nci maddesi uyarınca tesis edeceği Bilgi Paylaşım Komitesinin ölçülülük değerlendirmesinin ve paylaşım talebi hakkındaki uygunluk görüşünün de Kuruma iletilmesi gerekmektedir.

Benzer şekilde, paylaşım konu bilgiler yurt dışındaki ilgili düzenleyici otoritenin mevzuatın kendisine verdiği bir hak ile ana ortaklıktan/hakim ortaktan uygulamasını talep ettiği bir kontrol çerçevesinde bulunuyorsa ve ana ortaklığın/hakim ortağın bu talebi karşılamaması halinde ilgili düzenleyici otoritenin yaptırımına tabi tutulması riski bulunuyorsa, söz konusu talepler de uyum riski çerçevesinde değerlendirilir ve bankanın Kuruma yapacağı başvuruda yukarıda belirtilen

şartları aynı şekilde yerine getirmesi ve bu durumu somut bir şekilde ortaya koyması gerekmektedir.

Diğer taraftan, yabancı ülke kanunlarına göre denetime yetkili ve Kurum muadili yurt dışındaki ilgili düzenleyici otoritenin ana ortaklıktan/hakim ortaktan talep ettiği sır niteliğindeki bilgilerin, söz konusu ana ortaklık/hakim ortağın dünya genelindeki tüm iştiraklerine yönelik genel bir talep niteliğinde olmayıp Türkiye'deki iştiraklere yönelik özel bir talep niteliğinde olması halinde ya da söz konusu talebin ilgili otoritenin yaptırımına tabi tutulma riski bulunmayan bir talep niteliğinde olması (uyum riski kapsamında bulunmayan bir talep niteliğinde olması) halinde, bu bilgi taleplerinin Yönetmeliğin 6 ncı maddesinin dokuzuncu fıkrası kapsamında ele alınması gerekmektedir. Bu çerçevede, Yönetmeliğin 6 ncı maddesinin sekizinci fıkrası kapsamında karşı tarafın uyum riski amacıyla Kurumun uygun görüşünün alınması gereken paylaşım talepleri ile Yönetmeliğin 6 ncı maddesinin dokuzuncu fıkrası kapsamında ele alınması gereken taleplerin, yalnızca banka sırrı içerir bilgilere yönelik olsa dahi, Yönetmeliğin 5 inci maddesinin beşinci fıkrası kapsamında yerine getirilmesi mümkün bulunmamaktadır.

Ayrıca, uyum riski kapsamında talep edilen bilgi ana ortaklığın/hâkim ortağın yasal yükümlülükleri çerçevesinde oluşturduğu dâhili politikalara/iş süreçlerine dayanıyorsa söz konusu dâhili politikalara/iş süreçler kapsamında yapılacak paylaşımların uyum riski kapsamında değerlendirilebilmesi için, bu paylaşımların yapılmaması halinde ana ortaklığın/hâkim ortağın ilgili düzenleyici otoritenin yaptırımına tabi tutulma riskinin bulunması ve bankanın Kuruma yapacağı başvuruda yukarıda belirtilen şartları aynı şekilde yerine getirmenin yanında bu durumu da somut bir şekilde ortaya koyması gerekmektedir.

Bunun yanında, Yönetmeliğin 5 inci maddesinin ikinci fıkrasının (a) bendinde de belirtildiği üzere, gizlilik sözleşmesi yapılması ve sadece belirtilen amaçlar ile sınırlı kılınması koşuluyla, bankaların ve finansal kuruluşların, kendi aralarında doğrudan doğruya ya da Risk Merkezi veya en az beş banka ya da finansal kuruluş tarafından kurulacak şirketler vasıtasıyla yapılacak her türlü bilgi ve belge alışverişi sır saklama yükümlülüğünden istisna tutulmuş olup, bankaların iştiraki konumunda olan ve aynı zamanda ana ortaklığın/hakim ortağın da dolaylı kontrolünde bulunan **Türkiye'de yerleşik bir banka ile** yapılacak bilgi/belge paylaşımları da söz konusu istisnanın kapsamında değerlendirilebilecektir. Dolayısıyla, ana ortaklığın/hakim ortağın yurt içinde yerleşik bir banka olması ve bu ana ortaklığın/hakim ortağın yurt içindeki ortaklığı statüsünde olan diğer bir bankadan ülkemiz mevzuatından kaynaklı bir uyum riskinin yönetilmesi amacıyla Yönetmeliğin 5 inci maddesinin ikinci fıkrasının (b) bendi ile üçüncü fıkrası kapsamında veri talep etmesi halinde, ana

ortaklıkça talep edilen bu verilere ilişkin yapılacak paylaşımların Yönetmeliğin 5 inci maddesinin ikinci fıkrasının (a) bendine uygun yapılması kaydıyla, paylaşım öncesinde Kurumun uygun görüşünün alınmış olmasına ve Yönetmeliğin 6 ncı maddesinin birinci fıkrasının (ç) bendine uyumun sağlanmasına gerek bulunmamaktadır.

2.2. Suç gelirlerinin aklanmasının önlenmesi ve terörün finansmanı ile mücadele kapsamında ana ortaklığın aynı zamanda muhabir banka olarak aracılık ettiği SWIFT işlemleri ile ilgili gerçekleştirdiği “işlem sonrası” kontrolleri için talep etmesi halinde; işlem detaylarının (mahiyeti, tarafları, işleme ilişkin ek bilgi ve belgeler vb.), işlemde banka müşterisi olan veya olmayan taraflara ilişkin müşteri bilgilerinin (müşteri ismi, kimlik bilgileri, ortaklık yapısı, nihai faydalanıcı ismi, üst düzey yönetici isimleri, adres bilgileri, faaliyet alanları, meslek bilgisi vb.), müşteri hesap hareketlerinin ve müşterinin diğer finansal olan/olmayan bilgilerinin/belgelerinin, “ortak müşteri” olmasa dahi ana ortaklık ile paylaşımının, işlemin doğası kapsamında mümkün olup olmadığı:

Yönetmeliğin 5 inci maddesinin dördüncü fıkrasında “... 11/10/2006 tarihli ve 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun ile 7/2/2013 tarihli ve 6415 sayılı Terörizmin Finansmanının Önlenmesi Hakkında Kanunda tanımlanan suçların işlenmesine ilişkin mali suç riski de uyum riski kapsamında ele alınır. Uyum riski amacıyla yapılacak paylaşımların, paylaşımı yapan ya da paylaşımın yapıldığı karşı tarafın tabi olduğu ulusal ya da uluslararası bir mevzuattan kaynaklanması şarttır.” hükmüne yer verilmektedir.

Bu kapsamda, ana ortaklığın muhabir banka olarak aracılık ettiği fon transferi işlemleri için bu fıkrada belirtilen mali suç riskinin bertaraf edilmesine yönelik ana ortaklıkça gerçekleştirilecek kontroller kapsamında bankadan talep edilecek sır niteliğindeki bilgilerin de uyum riski çerçevesinde ele alınması mümkündür. Ancak yukarıda da belirtildiği üzere, bu gibi durumlarda Yönetmelik hükümleri uyarınca risk yönetimi amacı ile müşteri bilgilerinin paylaşılması mümkün olmakla birlikte, söz konusu paylaşımların “ölçülü” olması beklenmekte ve bankanın bu kapsamda Yönetmeliğin 6 ncı maddesinin sekizinci fıkrası uyarınca Kuruma yapacağı başvuruda, uyum riski çerçevesinde ana ortaklık ile yapılması planlanan paylaşım kapsamında hangi verilerin paylaşılacağı, paylaşılacak verilerin paylaşım amacının yerine getirilmesi için gerekli olup olmadığı ve uyum riski yönetimi için talep edilen bilgilerin geçerli bir mevzuat hükmünden kaynaklanıp kaynaklanmadığının somut bir şekilde ortaya konulması gerekmekte ve uyum riskine konu yabancı mevzuat hükümlerinin orijinal metinleri ile birlikte Türkçe tercümelerinin de başvuru kapsamında Kuruma iletilmesi ve bu kapsamda bankanın Yönetmeliğin 7 nci maddesi

uyarınca tesis edeceği Bilgi Paylaşım Komitesinin ölçülülük değerlendirmesinin ve paylaşım talebi hakkındaki uygunluk görüşünün de Kuruma iletilmesi gerekmektedir.

Diğer taraftan, Yönetmeliğin 6 ncı maddesinin altıncı fıkrasında "*İşlemin doğası gereği yurt içinde ya da yurt dışında kurulu banka, ödeme hizmeti sağlayıcısı, ödeme, menkul kıymet mutabakat veya mesajlaşma sistemleri ile etkileşimin gerekli olduğu ve işlemin tamamlanabilmesi için yurt içindeki ya da yurt dışındaki taraflarla müşteri sırrı niteliğindeki bilgilerin paylaşılmasının işlemin zorunlu unsuru olduğu, yurt içi/yurt dışı fon transferi, yurt dışı akreditif, teminat mektubu, referans mektubu gibi işlemler için, işlemin müşteri tarafından başlatılması ya da elektronik bankacılık hizmetlerine yönelik dağıtım kanalları üzerinden müşteri tarafından emir girilmesi, söz konusu paylaşımlar bakımından üçüncü fıkra da belirtilen müşteri talep ya da talimatı yerine geçer.*" hükmüne yer verilmektedir. **Ancak bu hüküm dayanak gösterilerek müşteri tarafından başlatılan işlemler ya da girilen emirler kapsamında yurt içindeki ya da yurt dışındaki taraflarla müşteri sırrı niteliğindeki bilgilerin paylaşılabilmesi için, banka tarafından müşteriye kullanılan sistem kuralları gereği söz konusu bilgi paylaşımının işlemin tamamlanabilmesi için zorunlu unsur olması gerekmektedir. Dolayısıyla müşteriye kullanılan sistem kurallarının zorunlu kılmadığı ancak ana ortaklığın kendi risk yönetim kontrolleri çerçevesinde paylaşımı zorunlu tutulan müşteri bilgilerine ilişkin paylaşımın bu fıkra kapsamında değil, yukarıda belirtildiği şekilde risk yönetimi ve uyum riski kapsamında yapılacak paylaşımlara ilişkin Yönetmelikte yer verilen hükümlere göre yapılması gerekmektedir.**

Bunun yanında, müşterinin talimatına konu **SWIFT gibi para transferi işlemlerinin gerçekleştirilmesi sonrasında**, muhabir bankalardan müşterinin talimatına konu işleme ve işlemin taraflarına ilişkin olarak gelebilecek bilgi taleplerinin karşılanmasını sistem kurallarının zorunlu kılması veya işlem sonrasında ilişkin olsa da işlem öncesinde banka tarafından bu taleplerin karşılanması taahhüdünün verilmemesi durumunda işlemin tamamlanabilmesinin mümkün olmaması halinde, işlem sonrasında yapılacak bu gibi paylaşımlar da Yönetmeliğin 6 ncı maddesinin altıncı fıkrasında belirtilen "*işlemin tamamlanabilmesi için yurt içindeki ya da yurt dışındaki taraflarla müşteri sırrı niteliğindeki bilgilerin paylaşılmasının işlemin zorunlu unsuru olduğu*" olduğu paylaşımlar olarak ele alınır. Ancak bu gibi durumlarda müşteri tarafından başlatılan işlemler ve girilen emirler müşterinin talep ya da talimatının yerine geçeceği için müşterinin işlem öncesinde, söz konusu sistem kuralları hakkında ve işlem sonrasında talimata konu işleme ve işlemin taraflarına ilişkin muhabir bankalar ile ne gibi bilgilerinin paylaşılacağı konusunda banka tarafından bilgilendirilmesi gerekmektedir.

2.3. Yönetmeliğin 5 inci maddesinin beşinci fıkrasındaki yönetim kurulunun onayı ile bilgi paylaşımı yapılabilecek üçüncü taraflardan kastedilenin kimler olduğu, Yönetmeliğin 5 inci maddesinin birinci ve ikinci fıkralarında belirtilen taraflara banka sırrı niteliğindeki bilgiler aktarılmadan önce de yönetim kurulu onayı gerekip gerekmediği, bağımsız denetim raporları ile kamuoyuna açıklanan alenileştirilmiş bilgilerin üçüncü taraflara aktarılması halinde de yönetim kurulu onayı gerekip gerekmediği:

Yönetmeliğin 5 inci maddesinin birinci fıkrasında banka sırrı ya da müşteri sırrı niteliğindeki bilgilerin bu konuda kanunen açıkça yetkili kılınan merciler ile paylaşılmasının sır saklama yükümlülüğünden istisna tutulduğu belirtilmiş olup, aynı maddenin ikinci fıkrasında ise gizlilik sözleşmesi yapılması ve sadece belirtilen amaçlar ile sınırlı kılınması koşuluyla yapılacak banka sırrı ya da müşteri sırrı niteliğindeki bilgilere ilişkin paylaşımların sır saklama yükümlülüğünden istisna tutulduğu haller sıralanmıştır. Aynı maddenin devamındaki fıkralarda ise banka sırrı niteliğindeki bilgiler de dahil olmak üzere, sır niteliğindeki bilgilerin paylaşılacağı hangi durumların sır saklama yükümlülüğünden istisna tutulduğu belirtilmiştir.

Yönetmeliğin 5 inci maddesinin beşinci fıkrasında ise *“Müşteri sırrı niteliğinde olmayıp yalnızca bankaya ait bilgileri içeren banka sırrı niteliğindeki bilgilerin, banka yönetim kurulu kararı ile banka sorumluluğunda üçüncü taraflar ile paylaşılması sır saklama yükümlülüğüne aykırılık teşkil etmez. Banka Yönetim Kurulu bu yetkisini usul ve esasları belirlemek suretiyle Genel Müdürlüğe devredebilir.”* hükmüne yer verilmiş olup, söz konusu hükümde yer verilen *“üçüncü taraflar”*, Yönetmeliğin 5 inci maddesinin beşinci fıkrası dışındaki, aynı maddede belirtilen sır saklama yükümlülüğünden istisna tutulan haller dışında paylaşım yapılacak tarafları ifade etmektedir.

Dolayısıyla Yönetmeliğin 5 inci maddesinin beşinci fıkrasında aranan yönetim kurulu kararı, aynı maddede belirtilen sır saklama yükümlülüğünden istisna tutulan hâller haricinde banka sırrı niteliğindeki bilgilerin üçüncü taraflar ile paylaşılması durumunda aranmaktadır.

Diğer taraftan, Yönetmeliğin 5 inci maddesinin birinci ya da beşinci fıkrası kapsamında bulunmadığı müddetçe, bağımsız denetim raporları ile banka sırrı niteliğindeki bir verinin kamuoyu ile paylaşılıp alenileştirilmesi mümkün olmadığından, bu tür alenileştirilmiş verilerin üçüncü taraflar ile paylaşılması için ilave bir yönetim kurulu kararı alınmasına gerek bulunmamaktadır.

2.4. Yönetmeliğin 5 inci maddesinin altıncı fıkrasına göre bankaların müşterileri ile olan ilişkilerinde hangi işlem türleri için müşteriden talep ya da talimat alınması gerektiği:

Yönetmeliğin 5 inci maddesinin altıncı fıkrası “Bankalar, Risk Merkezi veya en az beş banka ya da finansal kuruluş tarafından kurulmuş şirketlerce, müşterilerin kamu kurum ve kuruluşlarına kendi talepleri ile verdikleri müşteri sırrı niteliğindeki bilgilerin teyit edilmesi konusunda müşteri talep ya da talimatının alınmış olması şartıyla, söz konusu kamu kurum ve kuruluşlarına bu bilgilerin sadece doğru olup olmadığı şeklinde cevap verilmesi sır saklama yükümlülüğüne aykırılık teşkil etmez.” hükmünü amirdir.

Bu kapsamda, bir kamu kurumuna veya kuruluşuna herhangi bir işlemin gerçekleştirilebilmesi için müşteri tarafından verilen müşteri sırrı niteliğindeki bilginin, söz konusu kamu kurumu veya kuruluşu tarafından teyit edilebilmesini teminen, bankalar, Risk Merkezi veya mezkûr maddede belirtilen şirketler tarafından, bu bilginin doğru olup olmadığına ilişkin ilgili kamu kurumuna veya kuruluşuna bilgi verilebilmesi için müşterinin bu konuda talep ya da talimatının alınmış olması gerekmektedir.

2.5. Yönetmeliğin 5 inci maddesinin dokuzuncu fıkrasına göre altı aylık dönemler halinde yapılacak raporlamanın ilk olarak hangi tarihten itibaren başlayacağı, hangi biçim/yöntemlere göre yapılacağı, yapılan paylaşımların banka nezdinde ne şekilde denetime hazır bulundurulacağı ve bu kayıtların ne kadar süre ile saklanacağı:

Yönetmelik 01/07/2022 tarihinde yürürlüğe girmiş olup, Yönetmeliğin 5 inci maddesinin dokuzuncu fıkrasının “...Kurumca uygun görülen biçim ve yöntemlere göre, altı aylık dönemler halinde ve kritik bir değişiklik olması durumunda söz konusu değişiklik özelinde derhal Kuruma raporlanır...” hükmü uyarınca, altı aylık dönemler halinde yapılacak raporlamaların, Temmuz-Aralık raporlama dönemi için **31 Ocak**, Ocak-Haziran raporlama dönemi için **31 Temmuz** tarihine kadar **Kurumca uygun görülen format ve içerikte ve Kurumun bu konuda vereceği yönergeler doğrultusunda** Kuruma yapılması gerekmektedir. Kurumca uygun görülen format ve içerik ayrıca duyurulacak olup, gerekli görülmesi halinde bu format ve içeriğin Kurum tarafından değiştirilmesi ve güncellenmesi de mümkün bulunmaktadır.

Müşterinin kimliğini belirli veya belirlenebilir kılacak şekilde yapılan paylaşımlarla sınırlı olmak üzere, Yönetmeliğin 5 inci maddesi kapsamında yapılan tüm paylaşımların da banka nezdinde elektronik ortamda Kanununun 42 nci maddesi uyarınca on yıl süreyle denetime hazır bir şekilde saklanması ve Kurum tarafından talep edildiğinde makul bir süre içinde incelemeye elverişli bir formata dönüştürülmek suretiyle Kurum yetkililerine tevdi edilmesi gerekmektedir.

2.6. Yönetmeliğin 5 inci maddesinin dokuzuncu fıkrasına göre müşterinin kimliğini belirli veya belirlenebilir kılacak şekilde yapılan tüm paylaşımların banka nezdinde denetime hazır şekilde bulundurulması zorunluluğu ile kastedilenin paylaşılan bilgilerin bizatihi kendisinin saklanması

olup olmadığı, Yönetmeliğin 5 inci maddesi kapsamında kanuni zorunluluk gereği dahi olsa kamu kurum ve kuruluşları ile müşteri kimliğini belirli kılacak şekilde yapılacak paylaşımlar için de bu zorunluluğun geçerli olup olmadığı ve Yönetmeliğin 5 inci maddesinin dokuzuncu fıkrası uyarınca banka sırrı ve müşteri sırrı niteliğindeki bilgilerin aktarıldığı tüm üçüncü tarafların unvanı ve bulunduğu ülke bilgileri raporlanırken kanuni zorunluluk gereğince paylaşım yapılan kamu kurum ve kuruluşlarının belirtilmesinin gerekli olup olmadığı:

Yönetmeliğin 5 inci maddesinin dokuzuncu fıkrası uyarınca,

- Yönetmeliğin 5 inci maddesinin ikinci fıkrasının (b) bendi ile üçüncü fıkrası kapsamında yapılacak paylaşımlara ilişkin;

- Gizlilik sözleşmesinin bir örneğinin,
- Gerçekleştirilen paylaşımın amaçlarının,
- Sır kapsamındaki bilgilerin gizliliği ve güvenliğinin sağlanmasına yönelik hâkim ortak/ana ortaklık tarafından veya hâkim ortağın/ana ortaklığın bu kapsamda hizmet aldığı taraflarca alınan teknik ve idari tedbirlerin ve

- **Yönetmeliğin 5 inci maddesi kapsamında** banka sırrı ve müşteri sırrı niteliğindeki bilgilerin aktarıldığı tüm üçüncü tarafların (yurt içi yerleşikler dâhil) unvanı ve bulunduğu ülke bilgilerinin, Kurumca uygun görülen biçim ve yöntemlere göre, altı aylık dönemler halinde ve kritik bir değişiklik olması durumunda söz konusu değişiklik özelinde derhal Kuruma raporlanması gerektiği, ayrıca **müşterinin kimliğini belirli veya belirlenebilir kılacak şekilde bu madde (5 inci madde) kapsamında yapılan tüm paylaşımların banka nezdinde denetime hazır şekilde bulundurulacağı ve söz konusu bilgilerin Kurumca uygun görülen biçim ve yöntemlere göre talebi halinde Kuruma gönderileceği düzenlenmektedir.**

Bu kapsamda, müşterinin kimliğini belirli veya belirlenebilir kılacak şekilde Yönetmeliğin 5 inci maddesi çerçevesinde paylaşılan **sır niteliğindeki tüm bilgilerin bizatihi kendisinin** (yukarıda yer verilen dokuzuncu fıkra hükmünün giriş bölümünde belirtilen bilgileri de içerecek şekilde) denetime hazır bir şekilde bulundurulması gerekmektedir. **Ancak Yönetmeliğin 5 inci maddesinin ikinci fıkrasının (ç) bendi uyarınca, bankanın birincil sistemleri kapsamında süreklilik arz edecek şekilde destek hizmeti/hizmet aldığı kuruluşlar ile paylaştığı sır kapsamındaki bilgiler için ayrı bir kopya oluşturacak şekilde veri saklanması gerek bulunmamakta olup, bu tür paylaşımlar için 5 inci maddenin dokuzuncu fıkrası çerçevesinde ve Kurumun bu konuda vereceği yönergeler**

doğrultusunda paylaşımın kapsamını ve taraflarını gösterecek şekilde ve Kurumca uygun görülen format ve içerikte Kuruma raporlama yapılması yeterli olacaktır.

Diğer taraftan, müşterinin kimliğini belirli veya belirlenebilir kılacak şekilde bahse konu madde kapsamında, kamu kurumları da dâhil olmak üzere, kanunen açıkça yetkili kılınan merciler ile yapılan tüm paylaşımların da yukarıda belirtilen bilgileri kapsayacak şekilde banka nezdinde denetime hazır şekilde bulundurulması gerekmektedir.

2.7. Yönetmeliğin muhtelif maddelerinde belirtilen “hâkim ortak/ana ortaklık tarafından veya hâkim ortağın/ana ortaklığın hizmet aldığı taraflarca teknik ve idari tedbirlerin alınması” yükümlülüğü kapsamında bankalarca alınması gereken tedbirlerin asgari unsurlarının ne olduğu:

Yönetmeliğin;

- 5 inci maddesinin ikinci fıkrasının (ç) bendinde yer alan “Değerleme, derecelendirme, destek hizmeti ile bağımsız denetim faaliyetlerinde veya gerekli teknik ve idari tedbirlerin alınması kaydıyla hizmet alımlarına yönelik işlemlerde kullanılmak üzere bu hizmeti sağlayanlara bilgi ve belge verilmesi.”,

- 5 inci maddesinin üçüncü fıkrasında yer alan “İkinci fıkranın (b) bendi kapsamında yapılacak paylaşımların, sadece söz konusu bentte belirtilen amaçlar ile sınırlı kılınması, gizlilik sözleşmesi yapılması, söz konusu sözleşme hükümleri ile karşı tarafın gerekli teknik ve idari tedbirleri alınmasının sağlanması koşuluyla, hakim ortak ile yapılması ya da hakim ortağın/ana ortaklığın belirleyeceği, konsolide finansal tablo hazırlama ya da konsolide risk yönetimi uygulamaları kapsamında hizmet aldığı bir grup şirketi ile yapılması sır saklama yükümlülüğüne aykırılık teşkil etmez.”,

- 5 inci maddesinin dokuzuncu fıkrasında yer alan “İkinci fıkranın (b) bendi ile üçüncü fıkra kapsamında yapılacak paylaşımlara ilişkin gizlilik sözleşmesinin bir örneği, gerçekleştirilen paylaşımın amaçları, sır kapsamındaki bilgilerin gizliliği ve güvenliğinin sağlanmasına yönelik hâkim ortak/ana ortaklık tarafından veya hâkim ortağın/ana ortaklığın bu kapsamda hizmet aldığı taraflarca alınan teknik ve idari tedbirler ile bu madde kapsamında banka sırrı ve müşteri sırrı niteliğindeki bilgilerin aktarıldığı tüm üçüncü tarafların unvanı ve bulunduğu ülke bilgileri, Kurumca uygun görülen biçim ve yöntemlere göre, altı aylık dönemler halinde ve kritik bir değişiklik olması durumunda söz konusu değişiklik özelinde derhal Kuruma raporlanır. Müşterinin kimliğini belirli veya belirlenebilir kılacak şekilde bu madde kapsamında yapılan tüm paylaşımlar banka nezdinde denetime hazır şekilde bulundurulur ve söz konusu bilgiler Kurumca uygun görülen biçim ve yöntemlere göre talebi halinde Kuruma gönderilir.”

hükümleri uyarınca bankalarca hizmet alımlarında paylaşılacak sır kapsamındaki bilgilerin gizliliği ve güvenliğinin sağlanmasına yönelik olarak gerekli teknik ve idari tedbirlerin alınması gerektiği düzenlenmektedir.

Bilindiği üzere, 15/03/2020 tarihli ve 31069 sayılı Resmî Gazete’de yayımlanan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelikte (BSEBY), bankaların faaliyetlerinin ifasında kullandıkları bilgi sistemlerinin yönetimi ile elektronik bankacılık hizmetlerinin sunulmasında ve bunlara ilişkin risklerin yönetiminde esas alınacak asgari usul ve esaslar ile tesis edilmesi gereken bilgi sistemleri kontrolleri düzenlenmektedir. Söz konusu bilgi sistemleri kontrolleri ile bankaların bilgi sistemlerinin ve bu sistemler üzerindeki verilerinin gizliliği, güvenliği, bütünlüğü ve erişilebilirliğine ilişkin gerekli görülen asgari teknik ve idari tedbirlerin neler olduğu da düzenlenmiş bulunmaktadır.

Bu çerçevede, Yönetmeliğin yukarıda yer verilen hükümlerinde belirtilen **“gerekli teknik ve idari tedbirler”** ifadelerinden, genel anlamda veri gizliliği ve güvenliğinin sağlanmasına yönelik olarak BSEBY’de düzenlenen hükümlerin anlaşılması gerekmekte olup, sır niteliğindeki verilerin paylaşıldığı karşı tarafça BSEBY’de düzenlenen bu hükümlere birebir uyulması beklenmemekte ve veri gizliliği ve güvenliği konusunda genel kabul görmüş standart ve çerçevelerin esas alınması suretiyle karşı tarafça alınabilecek teknik ve idari tedbirler ile de bu konulardaki BSEBY hükümlerinin karşılanması mümkün bulunmaktadır.

3. Sır Niteliğindeki Bilgilerin Paylaşılmasına İlişkin Genel İlkeler Hakkında Açıklamalar (Madde 6)

3.1. Yönetmeliğin 6 ncı maddesinin birinci fıkrasında paylaşımın yanı sıra belirtilmiş olan aktarımın, paylaşımından farkının ne olduğu:

Yönetmeliğin 3 üncü maddesindeki “veri işleme” tanımında da belirtildiği üzere aktarım da paylaşım gibi bir veri işleme faaliyetini ifade etmekte olup, Yönetmeliğin 6 ncı maddesinin birinci fıkrasında da 5 inci madde kapsamında yapılacak paylaşımlar da dâhil olmak üzere, müşteri sırrı ve banka sırrı niteliğindeki bilgilerin, sadece belirtilen amaçlarla sınırlı olmak ve ölçülülük ilkesine uygun olarak bu amaçların gerektirdiği kadar veriyi içermek kaydıyla paylaşılacağı ve bilginin aktarıldığı karşı tarafın bilgilerin içeriğine vakıf olup olmadığına bakılmaksızın sır kapsamındaki bilgilerin aktarılmasının da paylaşım olarak kabul edileceği ifade edilmektedir.

Bu çerçevede, Yönetmelikte belirtilen “aktarım” kavramı hem bir veri işleme hem de bir paylaşım metodu olup, bilginin aktarıldığı karşı tarafın bu verinin içeriğini öğrenip öğrenemediği fark

etmeksizin de sır niteliğindeki bilgilerin paylaşılmasına ilişkin Yönetmelik ile getirilen tüm yükümlülüklerin aktarım halinde de geçerli olacağı ifade edilmektedir.

Bu yönüyle, sır niteliğindeki verilerin karşı tarafa şifrelenmiş bir şekilde aktarılmış olması ya da yetkisiz erişimi engelleyici nitelikte erişim kontrollerinin uygulanmış olması, sadece Yönetmeliğin çeşitli hükümlerinde de belirtilen bir **“teknik tedbir”** niteliğinde olup, bu teknik tedbirlerin uygulanması suretiyle karşı tarafın kendisine aktarılan verilerin içeriğini öğrenmesinin engellendiğinin iddia edilmesi, bu suretle aktarılan sır niteliğindeki verilerin karşı taraf ile paylaşılmadığı anlamına gelmeyecek ve bilakis sır niteliğindeki bilgiler karşı taraf ile paylaşılmış kabul edilerek, Yönetmelikte belirtilen yükümlülüklerin yerine getirilmesi gerekecektir.

Diğer taraftan Yönetmelik ile sır niteliğindeki verilerin kendisine aktarılması halinde, paylaşım gerçekleştirilmiş olacağı için yükümlülük doğacağı belirtilen “karşı taraf” kavramının, elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten internet servis sağlayıcılar gibi yalnızca veri aktarımına aracılık eden tarafları kapsamayacağı tabiidir.

3.2. Yönetmeliğin 6 ncı maddesinin birinci fıkrasının (b) bendinde yer verilen “Paylaşımların içerdiği veri ya da veri setlerinin tamamının belirtilen amaçların gerçekleştirilmesi için gerekli olduğunun gösterilebilir olması.” hükmünün nasıl uygulanması gerektiği ve “gerekli olduğunun gösterilebilir” olmasından neyin kastedildiği:

Yönetmeliğin 6 ncı maddesinin birinci fıkrasının (b) bendinde belirtilen “gerekli olduğunun gösterilebilir olması şartı” ile, paylaşımın içerdiği veri ya da veri setlerinin, **paylaşım amacının yerine getirilmesi için gerekli olup olmadığının somut bir şekilde ortaya konulması kastedilmektedir.**

Örneğin, varlıkların satışı amacıyla yapılacak değerlendirme çalışmalarında kullanılması amacıyla yapılan bilgi paylaşımının, bu amacın gerçekleştirilmesi için gerekli olmayan bilgileri içermesi bahse konu hükme aykırılık teşkil edecektir. Benzer şekilde, harcama itirazına ilişkin bir uyuşmazlığın çözümü amacıyla yapılacak bilgi paylaşımında itiraz konusunun kapsamını aşacak şekilde kredi kartı harcamalarına ilişkin bilgi gönderilmesi mezkûr hükme aykırılık oluşturacaktır.

3.3. “Ana firma/ilişki grubu (Mastergrup)” düzeyinde çokuluslu şirketlerin ana merkezleri ile bu ana merkeze bağlı diğer grup şirketi ile tüm iştirak ve şubelerin “ortak müşteri” olarak kabul edilip edilemeyeceği ve risk yönetimi ve/veya konsolidasyon amacı ile bu şekildeki bir Master grubun iştiraki olan müşterinin bilgilerinin, müşterinin talimatı uyarınca ve talimatta açıkça belirlenen bilgiler ile sınırlı olarak banka ana ortaklığı ile paylaşılıp paylaşılamayacağı:

Kanunun 73 üncü maddesinin üçüncü fıkrası ve Yönetmelik hükümleri uyarınca, diğer kanunların emredici hükümleri saklı kalmak kaydıyla, müşteri sırrı niteliğindeki bilgiler, müşterinin açık rızası alınsa dahi, müşteriden gelen bir talep ya da talimat olmaksızın yurt içindeki ve yurt dışındaki üçüncü kişilerle paylaşılamaz ve müşterinin bilgilerini paylaşmaya dair açık rıza göstermesi veya talep ya da talimat vermesi bankanın vereceği hizmetler için bir ön şart haline getirilemez. Bu şartın istisnası ise Yönetmeliğin 5 inci maddesinde sayılan sır saklama yükümlülüğünden istisna tutulan hallerdir.

Bu kapsamda, banka müşterisi olan Türkiye’de yerleşik uluslararası iş yapan şirketlerin, müşteri bilgilerinin global anlamda bir risk yönetimi yapabilmek adına banka ana ortaklığı ile paylaşılabilmesinin, söz konusu müşterilerin bu konuda talep ya da talimatının alınması suretiyle yerine getirilmesi mümkün olmakla birlikte, Yönetmeliğin 5 inci maddesinin ikinci fıkrasının (b) bendi uyarınca; gizlilik sözleşmesi yapılması ve sadece belirtilen amaçlar ile sınırlı kılınması koşuluyla konsolide finansal tablo hazırlama çalışmaları, risk yönetimi ve iç denetim uygulamaları kapsamında bankaların sermayelerinin yüzde on veya daha fazlasına sahip olan yurt içinde veya yurt dışında yerleşik kredi kuruluşu ile finansal kuruluşlar da dâhil ana ortaklıklarına bilgi ve belge verilmesi sır saklama yükümlülüğünden istisna tutulmuş ve Yönetmeliğin 6 ncı maddesinin birinci fıkrası uyarınca, bilgisi paylaşılacak müşteri aynı zamanda ana ortaklık, hakim ortak ya da grup şirketinin de **ortak müşterisi değilse, bu taraflarla paylaşılacak söz konusu gerçek/tüzel kişi müşteriye ilişkin sır niteliğindeki bilgilerin**, anılan müşterinin kimliğini belirli veya belirlenebilir kılacak nitelikte olmaması ve bu tür paylaşımlar için anonimleştirme, kimliksizleştirme ve toplulaştırma gibi yöntemlerin kullanılması şart koşulmuştur.

Diğer taraftan, Yönetmeliğin 6 ncı maddesinin sekizinci fıkrasında ise;

“(8) 5 inci maddenin ikinci fıkrasının (b) bendi ile üçüncü fıkrası kapsamında, kredi karşılık hesaplamaları ile içsel sermaye yeterliliği hesaplamaları gibi çok sayıda müşteriye ilişkin kapsamlı veri paylaşımını gerektiren paylaşımlar ile karşı tarafın uyum riski amacıyla yapılacak paylaşımlar için, paylaşım öncesinde Kurumun uygun görüşünün alınmış olması şartıyla, birinci fıkranın (ç) bendi uygulanmaz. 5 inci maddenin ikinci fıkrasının (b) bendi ile üçüncü fıkrası kapsamında konsolide risk yönetimi amacıyla paylaşılacak verilerin, banka ana sermayesinin yüzde onu veya daha fazlası oranında kredi kullandırılmış bir gerçek ya da tüzel kişiye veya bir risk grubuna ait olması halinde ise, söz konusu veriler için paylaşım öncesinde Kurumun uygun görüşünün alınmış olması ve birinci fıkranın (ç) bendine uyum şartı aranmaz. Kurul bu fıkrafta yer alan sınırlamaları değiştirmeye ya da bu fıkrafta yer alan hususlara ilişkin yeni sınırlamalar getirmeye yetkilidir.” hükmüne yer verilmiştir.

Bu kapsamda, Yönetmeliğin 6 ncı maddesinin birinci fıkrasında belirtilen “ortak müşteri” kavramı aynı gerçek ya da tüzel kişi müşterinin eş anlı olarak hem bankanın hem de ana ortaklık, hakim ortak ya da grup şirketinin müşterisi olmasını ifade etmekte, dolayısıyla uluslararası bir grubun banka ana ortaklığının müşterisi olması ve bu uluslararası grubun Türkiye’deki iştirakinin de bankanın (ana ortaklığın Türkiye’deki iştiraki olan banka) müşterisi olması durumunda “ortak müşteri” şartı sağlanmış olmamaktadır.

Diğer taraftan yukarıda belirtildiği üzere, müşterinin talep ya da talimatına gerek olmaksızın Yönetmeliğin 5 inci maddesinin ikinci fıkrasının (b) bendi kapsamında yapılabilecek paylaşımlarda dahi, Yönetmeliğin 6 ncı maddesinin sekizinci fıkrasında Kurumun uygun görüşünün alınmasını şart koşan durumlar belirlenmiş olup, bu fıkraya uygulama alanı bırakmamak amacıyla bankalarca müşterinin talep ya da talimatının alınması yöntemine başvurulmasından imtina edilmesi gerekmektedir.

Ayrıca global anlamda bir risk yönetimi yapabilmek adına bu şekildeki bir paylaşım talebinin bankanın ana ortaklığı tarafından talep edildiği de dikkate alındığında, müşterinin kendisinden kaynaklanmayan veya normal şartlar altında ana ortaklığın risk yönetimi için müşterinin bizatihi kendisinden kaynaklanması ihtimal dahilinde olmayan bir talebin, müşterinin kendisinden kaynaklanan bir talepmiş gibi alınması, hatta aksi takdirde müşteriye ürün ve hizmet sunumundan imtina edileceğinin belirtilmesi, aynı zamanda Yönetmeliğin 6 ncı maddesinin üçüncü fıkrasına da aykırılık teşkil edecektir. **Bu kapsamda, söz konusu paylaşımın müşteriden talep ya da talimat alınmak suretiyle gerçekleştirilmek istenmesi halinde dahi, bu yöntem bankanın Yönetmeliğin 6 ncı maddesinin sekizinci fıkrasından kaynaklanan yükümlülüklerini ortadan kaldırmayacaktır.**

3.4. Yönetmeliğin 6 ncı maddesinin birinci fıkrasının (ç) bendinde yer verilen “Bilgisi paylaşılacak müşteri aynı zamanda ana ortaklık, hâkim ortak ya da grup şirketinin de ortak müşterisi değilse, bu taraflarla paylaşılacak söz konusu gerçek/tüzel kişi müşteriye ilişkin sır niteliğindeki bilgilerin, anılan müşterinin kimliğini belirli veya belirlenebilir kılacak nitelikte olmaması ve (c) bendinde belirtilen yöntemlerin kullanılması.” hükmünde yer alan “grup şirketi” ifadesi ile; sadece Yönetmeliğin 5 inci maddesinin üçüncü fıkrasında belirtilen “hakim ortağın/ana ortaklığın belirleyeceği, konsolide finansal tablo hazırlama ya da konsolide risk yönetimi uygulamaları kapsamında hizmet aldığı grup şirketinin” kastedilip kastedilmediği ve bankaların iştiraki konumunda olup, aynı zamanda aynı ana ortaklık/hakim ortağın dolaylı kontrolünde bulunan şirketlerle Yönetmeliğin 5 inci maddesinin ikinci fıkrasının (a) bendi ile tanınan istisna kapsamında bilgi paylaşımına devam edilip edilemeyeceği:

Yönetmeliğin 6 ncı maddesinin birinci fıkrasının (ç) bendinde yer verilen “*Bilgisi paylaşılacak müşteri aynı zamanda ana ortaklık, hâkim ortak ya da grup şirketinin de ortak müşterisi değilse, bu taraflarla paylaşılacak söz konusu gerçek/tüzel kişi müşteriye ilişkin sır niteliğindeki bilgilerin, anılan müşterinin kimliğini belirli veya belirlenebilir kılacak nitelikte olmaması ve (c) bendinde belirtilen yöntemlerin kullanılması.*” hükmünde yer alan “**grup şirketi**” ifadesi ile; sadece Yönetmeliğin 5 inci maddesinin üçüncü fıkrasında belirtilen “hakim ortağın/ana ortaklığın belirleyeceği, konsolide finansal tablo hazırlama ya da konsolide risk yönetimi uygulamaları kapsamında hizmet aldığı grup şirketi” kastedilmekte olup, söz konusu grup şirketinin hakim ortağın/ana ortaklığın belirleyeceği herhangi bir grup şirketi değil konsolide finansal tablo hazırlama ya da konsolide risk yönetimi uygulamaları kapsamında hizmet aldığı bir grup şirketi olması gerekmektedir.

Diğer taraftan, Yönetmeliğin 5 inci maddesinin ikinci fıkrasının (a) bendinde de belirtildiği üzere, gizlilik sözleşmesi yapılması ve sadece belirtilen amaçlar ile sınırlı kılınması koşuluyla, bankaların ve finansal kuruluşların, kendi aralarında doğrudan doğruya ya da Risk Merkezi veya en az beş banka ya da finansal kuruluş tarafından kurulacak şirketler vasıtasıyla yapılacak her türlü bilgi ve belge alışverişi sır saklama yükümlülüğünden istisna tutulmuş olup, bankaların iştiraki konumunda olan ve aynı zamanda ana ortaklığın/hakim ortağın da dolaylı kontrolünde bulunan **Türkiye’de yerleşik şirketlerin**, Kanunun 3 üncü maddesinde tanımlanan bir finansal kuruluş da olması halinde, bu şirketler ile yapılacak bilgi/belge paylaşımları da söz konusu istisnanın kapsamında değerlendirilebilecektir.

3.5. Yönetmeliğin 6 ncı maddesinin birinci fıkrasının (ç) bendinde belirtilen “ortak müşteri” tespitinin yapılabilmesi için dahi, ana ortaklık/hâkim ortak ile bilgi paylaşımı gerekebileceğinden, tespit yapılabilmesi için gerekli olan müşteri bilgilerinin paylaşımının kapsam dışı olup olmadığı:

Yönetmeliğin 6 ncı maddesinin birinci fıkrasının (ç) bendine göre bilgisi paylaşılacak müşteri aynı zamanda ana ortaklığın/hakim ortağın ya da grup şirketinin de ortak müşterisi değilse paylaşılacak söz konusu gerçek/tüzel kişi müşteriye ilişkin sır niteliğindeki bilgilerin, anılan müşterinin kimliğini belirli veya belirlenebilir kılacak nitelikte olmaması gerekmekte ve ayrıca Yönetmeliğin 6 ncı maddesinin sekizinci fıkrasında, sır niteliğindeki müşteri bilgilerinin açıktan paylaşılması için şart koşulan ortak müşteri olma şartının da hangi durumlarda aranmadığı düzenlenmektedir.

Söz konusu Yönetmelik hükümlerinin uygulanabilmesi için banka tarafından “ortak müşteri” kontrolünün yapılması şart olup, **söz konusu kontrol kapsamında ana ortaklık/hakim ortak ya da grup şirketi ile müşteri bilgilerinin paylaşılmasından önce bilgisi paylaşılması planlanan**

müşterilerin ana ortaklığın/hakim ortaklığın ya da grup şirketinin müşterisi olup olmadığına yönelik yapılacak bilgi teatisi çerçevesinde müşteri kimliğini belirli veya belirlenebilir kılacak nitelikte yapılacak paylaşımlar bu hükme aykırılık teşkil etmeyecektir. Ancak söz konusu "ortak müşteri kontrolü" kapsamında ana ortaklık/hakim ortak ya da grup şirketi ile yapılacak bilgi paylaşımında dahi Yönetmeliğin 6 ncı maddesinin birinci fıkrasında belirtilen diğer "ölçülülük" kriterlerine riayet edilmesi şart olup, örneğin müşteriyi tekil olarak tanımlayabilecek bir TCKN/ID/VKN numarası ile kontrol yapılabilmesi ve/veya bunun yanında müşteri ad/soyadı bilgilerinin de maskeli olarak karşı taraf ile paylaşılması mümkün iken söz konusu kontrolün gerektirdiği bilgi paylaşımından daha fazla ölçüde bir müşteri bilgisinin açıktan paylaşılması gerekmektedir. Benzer şekilde ana ortaklık/hakim ortak ya da grup şirketinden gelen bir talep doğrultusunda yapılacak paylaşımlarda, ortak müşteri kontrolünün mümkün olduğu ölçüde, kişi bilgisinin banka tarafından değil ana ortaklık/hakim ortak ya da grup şirketi tarafından iletilmesi suretiyle yapılması ve böylelikle karşı tarafın iletildiği kişi bilgilerinin aynı zamanda bankanın da müşterisi olup olmadığının kontrol edilmesi şeklinde gerçekleştirilmesi gerekmektedir.

3.6. Yönetmeliğin 6 ncı maddesinin ikinci fıkrasında yer verilen "Müşteri sırrı niteliğinde olsa dahi, sağlık ve cinsel hayata ilişkin kişisel veriler, sır saklama yükümlülüğünden istisna tutulan hallerden biri dayanak gösterilerek, yurt içindeki ya da yurt dışındaki taraflarla paylaşamaz." hükmünün nasıl uygulanması gerektiği ve müşterinin kendisi ile paylaşılacak verileri de kapsayıp kapsamadığı:

Yönetmeliğin 6 ncı maddesinin ikinci fıkrasında "Gerçek kişi müşterilere ilişkin sır niteliğindeki bilgilerin paylaşımında KVKK'nin 4 üncü maddesinde yer verilen genel ilkelere uyulması zorunludur. Müşteri sırrı niteliğinde olsa dahi, sağlık ve cinsel hayata ilişkin kişisel veriler, sır saklama yükümlülüğünden istisna tutulan hallerden biri dayanak gösterilerek, yurt içindeki ya da yurt dışındaki taraflarla paylaşamaz." hükmüne yer verilmiş olup, söz konusu hüküm ile gerçek kişi müşterilere ilişkin sağlık ve cinsel hayata ilişkin özel nitelikli kişisel verilerin, müşteri sırrı haline gelmiş olsa dahi, özel nitelikli bir kişisel veri olma yönünün daha ağır bastığı ve bu nedenle 5 inci maddede belirtilen sır saklama yükümlülüğünden istisna tutulan hallerden biri dayanak gösterilmek suretiyle herhangi bir sır kapsamındaki veriymiş gibi paylaşımına tabi tutulmaması amaçlanmaktadır.

KVKK'nin 6 ncı maddesinin üçüncü fıkrasında da yer verilen,

"(3) Birinci fıkrafta sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık

hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.”

hükmü uyarınca da, sağlık ve cinsel hayat dışındaki kişisel verilerin kanunda öngörülen hallerde ilgilinin açık rızası olmaksızın da işlenebilmesi mümkün olmakla birlikte, sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak bu hükümde belirtilen amaçlarla ve yine yalnızca bu hükümde belirtilen yetkili kişi, kurum ya da kuruluşlarca ilgilinin açık rızası alınmaksızın işlenebilmektedir.

Bu çerçevede, KVKK'nin 6 ncı maddesinin birinci fıkrasında belirtilen, sağlık ve cinsel hayata ilişkin veriler dışında kalan, özel nitelikli kişisel verilerin işlenebilmesinin kanunlarda öngörülen hallerde ilgilinin açık rızası bulunmaksızın işlenmesi mümkün olduğundan, söz konusu özel nitelikli kişisel verilerin aynı zamanda müşteri sırrı haline gelmesi halinde, KVKK ve ilgili mevzuatına da aykırılık teşkil etmediği müddetçe, Kanun uyarınca sır saklama yükümlülüğünden istisna tutulan hallerden biri dayanak gösterilerek müşterinin açık rızası alınmaksızın işlenebilmesinin önünde bir engel bulunmamaktadır.

Ancak hem Yönetmeliğin 6 ncı maddesinin ikinci fıkrası, hem de KVKK'nin 6 ncı maddesinin üçüncü fıkrası uyarınca, sağlık ve cinsel hayata ilişkin kişisel verilerin, müşteri sırrı haline gelmiş olsa dahi, ilgili müşterinin açık rızası alınmaksızın yurt içindeki ya da yurt dışındaki taraflarla sır saklama yükümlülüğünden istisna tutulan hallerden biri dayanak gösterilerek paylaşılması mümkün bulunmamaktadır.

Diğer taraftan sağlık ve cinsel hayata ilişkin kişisel verileri de barındırıyor olsa bile, müşteri sırrı niteliğindeki verilerin, müşterinin açık rızası ve kendi talep ya da talimatı çerçevesinde bankaya yapacağı başvuru üzerine, **bizatihi kendisi/temsilcisi ile ya da kendisine/temsilcisine ait olduğunu beyan ettiği bir iletişim adresi ile paylaşılması, sır niteliğindeki bir bilginin sır sahibinin kendisi ile paylaşılması anlamına geleceği için, Yönetmeliğin 6 ncı maddesinin ikinci fıkrasına aykırılık teşkil etmeyecektir. Ancak söz konusu temsil ilişkisinin kurulmasına yönelik müşteri tarafından yapılacak yetkilendirmede ve müşterinin bankaya iletileceği talep/talimatta, müşteri sırrı niteliğindeki bilgi ve belgelerin de temsilci ile paylaşılabilmesinin açıkça belirtilmesi gerekmektedir.**

3.7. Yönetmeliğin 6 ncı maddesinin üçüncü fıkrasında belirtilen müşteri talep talimatının nasıl, hangi yöntem ile müşterinin aktif rol oynamak suretiyle bankalarca temin edileceği, müşteri memnuniyeti ve süreç etkinliği bakımından bankaca sağlanacak örneklerin müşteri tarafından incelenip talimata dönüştürülmesi şeklinde veya “push notification” ile sağlanan metinler üzerinden müşterinin bu talimatı verip veremeyeceği:

Bilindiği üzere Kanunun 73 üncü maddesinin üçüncü fıkrasına 20/2/2020 tarihli ve 7222 sayılı Kanun ile "... Bankacılık faaliyetlerine özgü olarak bankalarla müşteri ilişkisi kurulduktan sonra oluşan gerçek ve tüzel kişilere ait veriler, müşteri sırrı hâline gelir. Diğer kanunların emredici hükümleri saklı kalmak kaydıyla, müşteri sırrı niteliğindeki bilgiler, bu maddede belirtilen sır saklama yükümlülüğünden istisna tutulan hâller haricinde, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca müşterinin açık rızası alınsa dahi, **müşteriden gelen bir talep ya da talimat olmaksızın yurt içindeki ve yurt dışındaki üçüncü kişilerle paylaşılabilir ve bunlara aktarılamaz...**" cümleleri eklenmiştir. Söz konusu değişiklik ile, sır saklama ödevinin yükümlüsü olan bankaların kanunların tanıdığı bir istisna ya da herhangi bir mecburiyet bulunmadığı halde, kendi belirleyecekleri amaç ve yöntemler için ve kendi hazırlayacakları rıza metinleri ile bu yükümlülüklerini dolanmalarını engellemek ve bu kapsamda sır saklama yükümlülüğünün bankanın aktif rol aldığı rıza metni yöntemiyle değil, sır sahibi müşterinin aktif rol aldığı "müşterinin talebi ya da talimatı" yöntemiyle kaldırılabilmesini sağlamak amaçlanmıştır.

Bu düzenleme ile, müşterinin sır niteliğindeki bilgileri, bu bilgilerin paylaşılmasına ilişkin talep veya talimatın alınması şartıyla ve bu talep veya talimat ile ölçülü olacak şekilde paylaşılabilir olup, bu doğrultuda, sır niteliğindeki bilgilerin paylaşımı müşterinin talebi veya talimatında belirtilen amaç ile sınırlı olacaktır.

Yönetmeliğin 6 ncı maddesinde de sır niteliğindeki bilgilerin paylaşılmasına ilişkin genel ilkeler düzenlenmiş olup, Kanunun 73 üncü maddesinde ve Yönetmeliğin 5 inci maddesinde yer alan, sır saklama yükümlülüğünden istisna tutulan hallerde de dahil olmak üzere, sır niteliğindeki bilgilerin paylaşımında "amaçla sınırlı olma" ve "ölçülülük ilkesine uygun olma" esaslarına uyulması gerekmektedir. Yönetmeliğin 6 ncı maddesinin üçüncü, dördüncü ve yedinci fıkralarında ise sırasıyla;

*"Diğer kanunların emredici hükümleri saklı kalmak kaydıyla, müşteri sırrı niteliğindeki bilgiler, 5 inci maddede belirtilen sır saklama yükümlülüğünden istisna tutulan hâller haricinde, müşterinin açık rızası alınsa dahi, **müşteriden gelen bir talep ya da talimat olmaksızın yurt içindeki ve yurt dışındaki üçüncü kişilerle paylaşılabilir ve müşterinin bilgilerini paylaşmaya dair açık rıza göstermesi veya talep ya da talimat vermesi bankanın vereceği hizmetler için bir ön şart haline getirilemez.**"*

*"Üçüncü fıkrada belirtilen müşterinin talep ya da talimatı yazılı şekilde alınabileceği gibi kanıtlanabilir nitelikte olmak kaydıyla kalıcı veri saklayıcısı yoluyla da alınabilir. Müşterinin talep ya da talimatı, talep ya da talimatın alındığı aynı yöntemlerle müşteri tarafından istenildiğinde iptal edilebilir veya değiştirilebilir olmak kaydıyla, birden çok işlemi kapsayabilir ve süreklilik arz eden işlemlere yönelik talep ya da talimat süresiz olabilir. Altıncı fıkrada belirtilen durumlar haricinde, **müşterinin vermiş olduğu talep ya da talimatlarını***

elektronik bankacılık hizmetlerine yönelik dağıtım kanalları üzerinden sorgulayabilmesi ve görüntüleyebilmesi esastır.”,

“Müşterinin, talep ya da talimatı üzerine yapılacak paylaşımlarda birinci fıkrada belirtilen ölçülülük ilkesine uyulup uyulmadığı, müşterinin talep ya da talimatına uyulup uyulmadığı ile sınırlı olarak değerlendirilir. Müşterinin paylaşılmasını talep ettiği veri seti içinde başka müşterilere ya da başka bankaların müşterilerine ilişkin sır kapsamındaki bilgilerin de olması halinde ise, birinci fıkradaki yükümlülüğe herhangi bir sınırlama olmaksızın uyulması zorunludur.”

hükümleri yer almaktadır.

Bu kapsamda, söz konusu hükümlerde müşterinin sır niteliğindeki bilgilerinin paylaşımına ilişkin talep veya talimatı konusunda belirlenen esaslara uyulması kaydıyla, banka tarafından belirlenecek açık ve anlaşılır örnek metinler üzerinden müşteri talep ya da talimatının alınması mümkündür. Ancak söz konusu örnek metinler bir sözleşme kapsamında alınıyor ise bu örnek metinlerin **sözleşme metninden açıkça ayırt edilebilir şekilde olması ve müşteri dikkatine sunulmasını müteakip, müşteri tarafından incelenip, müşterinin aktif rol alacağı şekilde bir talimata dönüştürülmesi gerekmektedir.** Müşterinin talep veya talimatının, doğrudan müşterinin sır niteliğindeki bilgilerinin paylaşılması yönündeki istek ve iradesini açıkça ortaya koyması gerektiğinden, bankanın hazırladığı örnek metnin müşteri talimatı haline dönüştürülmesinde, müşterinin aktif bir rol aldığı kabul edilebilmesi için,

- Söz konusu talep ya da talimatın yazılı olarak alındığı hallerde “müşterinin talep ya da talimatın içeriğini anladığına ve söz konusu talep/talimatın kendi isteğiyle verildiğini onayladığına” ilişkin yazılı beyanının alınması,

- Talep/talimatın kalıcı veri saklayıcısı üzerinden alındığı hallerde, örnek talep/talimat metninin müşterinin teyit edilmiş iletişim adresine gönderilmiş olması ve müşterinin kendisine iletilen bu örnek “talep/talimat metninin içeriğini anladığına ve söz konusu talep/talimatın kendi isteğiyle verildiğini onayladığına” ilişkin beyanının müşteriye ait teyit edilmiş aynı iletişim adresi üzerinden alınmış olması,

- Talep/talimatın internet bankacılığı ya da mobil bankacılık üzerinden alınması halinde ise, örnek talep/talimat metninin müşteriye söz konusu kanallar üzerinden gönderilmesi ve müşterinin kendisine iletilen bu örnek “talep/talimat metninin içeriğini anladığına ve söz konusu talep/talimatın kendi isteğiyle verildiğini onayladığına” ilişkin irade beyanının ve talep/talimatın kendisinin 01.04.2021 tarihli ve 31441 sayılı Resmî Gazete’de yayımlanan “Bankalarca Kullanılacak Uzaktan

Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik”in 12 inci maddesinin ikinci fıkrasına uygun olacak şekilde dijital olarak imzalanması şarttır.

Ayrıca, bu kapsamda yapılacak paylaşımın genel ilkelere uygun olabilmesi için, bilgi paylaşımının müşteri tarafından talep edilmesi; banka tarafından hazırlanmış örnek bir talep/talimat metni bulunsa da içeriğinin, müşterinin talep veya talimatını karşılayacak şekilde değiştirilebilir olması ve söz konusu paylaşımların istisnalar kapsamına girmeyen ve kanunen yetkili kılınmayan üçüncü kişilerle yapılacak nitelikte paylaşımlar olduğu da dikkate alınarak, bu paylaşımlar için alınacak talep ya da talimatların bankanın vereceği hizmetler için bir ön şart haline getirilmemesi ve **talep/talimat alınmasından önce** müşterinin bu hususlarda bilgilendirilmiş olması gerekmektedir.

Diğer taraftan, Yönetmeliğin 6 ncı maddesinin altıncı fıkrasında da belirtildiği üzere işlemin doğası gereği yurt içinde ya da yurt dışında kurulu banka, ödeme hizmeti sağlayıcısı, ödeme, menkul kıymet mutabakat veya mesajlaşma sistemleri ile etkileşimin gerekli olduğu ve işlemin tamamlanabilmesi için yurt içindeki ya da yurt dışındaki taraflarla müşteri sırrı niteliğindeki bilgilerin paylaşılmasının işlemin zorunlu unsuru olduğu, yurt içi/yurt dışı fon transferi, yurt dışı akreditif, teminat mektubu, referans mektubu gibi işlemler için, işlemin müşteri tarafından başlatılması ya da elektronik bankacılık hizmetlerine yönelik dağıtım kanalları üzerinden müşteri tarafından emir girilmesi, söz konusu paylaşımlar bakımından müşteri talep ya da talimatı olarak kabul edilmekte ve **işlemin doğası gereği bilgi paylaşımının zorunlu olduğu durumlarda bu hüküm uyarınca müşteriden ilave bir talep/talimat alınması gerekmemektedir.**

3.8. Yönetmeliğin 6 ncı maddesinin dördüncü fıkrasında yer verilen “... Altıncı fıkrada belirtilen durumlar haricinde, müşterinin vermiş olduğu talep ya da talimatlarını elektronik bankacılık hizmetlerine yönelik dağıtım kanalları üzerinden sorgulayabilmesi ve görüntüleyebilmesi esastır.” hükmünün kapsamının ne olduğu ve bu hüküm kapsamında müşterinin vermiş olduğu talep ya da talimatlarını internet ve mobil bankacılık (ATM, Çağrı merkezi hariç) kanalları üzerinden sorgulayabilmesine imkan tanınmasının Yönetmelik maddesinin gereğini karşılayıp karşılamayacağı:

Yönetmeliğin 6 ncı maddesinin dördüncü fıkrasında “Üçüncü fıkrada belirtilen müşterinin talep ya da talimatı yazılı şekilde alınabileceği gibi kanıtlanabilir nitelikte olmak kaydıyla kalıcı veri saklayıcısı yoluyla da alınabilir. Müşterinin talep ya da talimatı, talep ya da talimatın alındığı aynı yöntemlerle müşteri tarafından istenildiğinde iptal edilebilir veya değiştirilebilir olmak kaydıyla, birden çok işlemi kapsayabilir ve süreklilik arz eden işlemlere yönelik talep ya da talimat süresiz olabilir. **Altıncı fıkrada belirtilen durumlar haricinde,**

müşterinin vermiş olduğu talep ya da talimatlarını elektronik bankacılık hizmetlerine yönelik dağıtım kanalları üzerinden sorgulayabilmesi ve görüntüleyebilmesi esastır.” hükmü düzenlenmektedir.

Bilindiği üzere, BSEBY’de, bankaların faaliyetlerinin ifasında kullandıkları bilgi sistemlerinin yönetimi ile elektronik bankacılık hizmetlerinin sunulmasında ve bunlara ilişkin risklerin yönetiminde esas alınacak asgari usul ve esaslar ile tesis edilmesi gereken bilgi sistemleri kontrolleri düzenlenmektedir. Söz konusu düzenlemede, elektronik bankacılık hizmetleri, internet bankacılığı, mobil bankacılık, telefon bankacılığı, açık bankacılık servisleri ile ATM ve kiosk cihazları gibi müşterilerin, uzaktan bankacılık işlemlerini gerçekleştirebildikleri veya gerçekleştirilmesi için bankaya talimat verebildikleri her türlü elektronik dağıtım kanalı olarak tanımlanmakta ve mobil bankacılık dağıtım kanalının tanımında da söz konusu dağıtım kanalının özelleşmiş bir internet bankacılığı dağıtım kanalı olduğu ifade edilmektedir.

Bu çerçevede, Yönetmeliğin bahse konu hükmü kapsamında, müşterinin vermiş olduğu talep ya da talimatlarını elektronik bankacılık hizmetlerine yönelik dağıtım kanallarının en az biri üzerinden sorgulayabilmesi ve görüntüleyebilmesine imkan tanınması yeterli olmakla birlikte, söz konusu sorgulama ve görüntüleme hizmetinin öncelikle hem internet bankacılığı kanalı hem de bu kanalın özelleşmiş bir şekli olan mobil bankacılık kanalları üzerinden verilmesi gerekmekte, bu kanallardan söz konusu hizmetlerin sunulması sonrasında (ya da eş anlı olarak) diğer elektronik bankacılık dağıtım kanallarından da (ATM, kiosk gibi) bu hizmetlerin verilmesi mümkün bulunmaktadır.

Diğer taraftan, Yönetmeliğin 6 ncı maddesinin dördüncü fıkrasında yer verilen bu yükümlülük, Yönetmelik uyarınca alınmış olan müşteri talep/talimatlarını kapsamakta olup, Yönetmeliğin yürürlük tarihinden önce alınmış olan talep/talimatların yukarıda belirtilen dağıtım kanallarından sorgulanmasına gerek bulunmamaktadır. Ancak Yönetmeliğin yürürlük tarihinden sonra, kağıt ortamında alınanlar da dahil olmak üzere, Yönetmelik kapsamında gerçek ya da tüzel kişi ayrımı bulunmaksızın müşterilerden alınan talep/talimatların müşteri tarafından yukarıda belirtilen dağıtım kanallarından sorgulanabilmesinin sağlanması gerekmektedir.

3.9. Yönetmeliğin 6 ncı maddesinin beşinci fıkrasında yer verilen “İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan birincil sistemler kapsamında olmayan, destek hizmetlerine veya değerlendirme, derecelendirme ve bağımsız denetim dışındaki hizmet alımlarına ilişkin 5 inci maddenin ikinci fıkrasının (ç) bendi uyarınca yapılacak paylaşımlar için üçüncü fıkrada belirtilen “müşterinin talep ya da talimatının bulunması zorunludur. 5 inci maddenin yedinci fıkrası

kapsamında yapılan paylaşımlar için bu hüküm uygulanmaz.” hükmü uyarınca birincil sistemler kapsamında olmayan destek hizmeti veya hizmet alımlarında, müşterinin talep veya talimatının aranmasının gerekip gerekmediği:

Yönetmeliğin 6 ncı maddesinin beşinci fıkrasında,

“İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan birincil sistemler kapsamında olmayan, destek hizmetlerine veya değerlendirme, derecelendirme ve bağımsız denetim dışındaki hizmet alımlarına ilişkin 5 inci maddenin ikinci fıkrasının (ç) bendi uyarınca yapılacak paylaşımlar için üçüncü fıkrada belirtilen müşterinin talep ya da talimatının bulunması zorunludur. 5 inci maddenin yedinci fıkrası kapsamında yapılan paylaşımlar için bu hüküm uygulanmaz.” hükmüne yer verilmiştir.

Bahse konu hükümde mezkur maddenin üçüncü fıkrasında belirtilen müşterinin talep ya da talimatının bulunması zorunluluğu, İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan **birincil sistemler kapsamında olmayan, destek hizmetlerine veya** (değerleme, derecelendirme ve bağımsız denetim dışındaki) **hizmet alımlarına ilişkin yapılacak paylaşımlar** için aranmaktadır. Dolayısıyla, birincil sistemler kapsamında olmayan, tüm destek hizmetlerine ilişkin ya da (değerleme, derecelendirme ve bağımsız denetim dışındaki) tüm hizmet alımlarına ilişkin yapılacak paylaşımlarda bu zorunluluk aranmaktadır.

Ancak, Yönetmeliğin 5 inci maddesinin yedinci fıkrasında belirtildiği üzere bankanın taraf olduğu uyuşmazlıklarda bankayı temsil etmek üzere hizmet alınan taraflarla yapılacak bankanın iddia ya da savunmasının ispatı için zorunlu olan paylaşımlar için müşterinin talep ya da talimatının alınması zorunluluğu bulunmamaktadır.

3.10. Yönetmeliğin 5 inci maddesinin yedinci fıkrasında yer alan “bankayı temsil eden taraflarla” ifadesinden hukuki danışmanlık alınabilecek ve fakat bankayla bir temsil ilişkisi olmayan üçüncü tarafların da anlaşılmasının mümkün olup olmadığı ve bu durumda Yönetmeliğin 6 ncı maddesinin beşinci fıkrası uyarınca müşteri talep ya da talimatının gerekip gerekmediği:

Yönetmeliğin 5 inci maddesinin yedinci fıkrasında sır saklama yükümlülüğünden istisna tutulan hallerden biri *“Bankanın taraf olduğu uyuşmazlıklarda iddia ya da savunmasının ispatı için zorunlu olması halinde, söz konusu uyuşmazlığın tarafı olan gerçek veya tüzel kişilere ait müşteri sırrı niteliğindeki bilgilere veya banka sırrı niteliğindeki bilgilere ilişkin olarak, yurt içindeki ya da yurt dışındaki yargı makamları ile tahkim, arabuluculuk ve hakem heyeti gibi alternatif uyuşmazlık çözmeye yetkili makamlarla ya da bu makamlarla paylaşmak üzere söz konusu uyuşmazlıklarda bankayı temsil eden taraflarla yapılan paylaşımlar”* olarak belirtilmiştir.

Yönetmeliğin 5 inci maddesinin ikinci fıkrasının (ç) bendine göre gizlilik sözleşmesi yapılması ve sadece belirtilen amaçlar ile sınırlı kılınması koşuluyla gerekli teknik ve idari tedbirlerin alınması kaydıyla hizmet alımlarına yönelik işlemlerde kullanılmak üzere bu hizmeti sağlayanlara bilgi ve belge verilmesi de sır saklama yükümlülüğünden istisna tutulan hallerden biri olarak sayılmış olup **“hukuki danışmanlık”** gibi hizmet alımlarının da bu kapsamda ele alınması mümkün bulunmaktadır.

Ancak, Yönetmeliğin 6 ncı maddesinin beşinci fıkrasında yer verilen *“İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan birincil sistemler kapsamında olmayan, destek hizmetlerine veya değerlendirme, derecelendirme ve bağımsız denetim dışındaki hizmet alımlarına ilişkin 5 inci maddenin ikinci fıkrasının (ç) bendi uyarınca yapılacak paylaşımlar için üçüncü fıkrada belirtilen müşterinin talep ya da talimatının bulunması zorunludur. 5 inci maddenin yedinci fıkrası kapsamında yapılan paylaşımlar için bu hüküm uygulanmaz.”* hükmü uyarınca **“hukuki danışmanlık”** hizmetleri gibi İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan birincil sistemler kapsamında olmayan hizmet alımları için müşterinin talep ya da talimatının bulunması zorunlu olsa da aynı hükmün devamında 5 inci maddenin yedinci fıkrası kapsamında yapılan paylaşımlar için bu zorunluluğun aranmayacağı belirtilmiştir.

Söz konusu hükümler birlikte değerlendirildiğinde,

- **“Hukuki danışmanlık”** gibi hizmet alımları da Yönetmeliğin 5 inci maddesinin ikinci fıkrasının (ç) bendinde belirtilen bir hizmet alımı olması dolayısıyla anılan maddenin ikinci fıkrası uyarınca **gizlilik sözleşmesi yapılması ve sadece belirtilen amaçlar ile sınırlı kılınması koşulu bu tür hizmet alımları için yapılacak paylaşımlar için de zorunlu olmakla birlikte,** Yönetmeliğin 6 ncı maddesinin beşinci fıkrası uyarınca bu tür paylaşımlar için ilave olarak müşterinin talep ya da talimatının bulunması da gerekmektedir;

- Banka ile müşterileri arasındaki uyuşmazlıklarda yurt içindeki ya da yurt dışındaki yargı makamları ile tahkim, arabuluculuk ve hakem heyeti gibi alternatif uyuşmazlık çözmeye yetkili makamlar önünde bankayı temsil etme potansiyeli bulunan **ancak henüz bir “temsil ilişkisi bulunmayan” ve mevcut uyuşmazlığa ilişkin belge ve kayıtları incelemesi gerekip bu inceleme neticesinde bankaya görüşünü iletme üzere hukuki danışmanlık hizmeti alınan taraflarla yapılacak paylaşımlar için de Yönetmeliğin 6 ncı maddesinin üçüncü fıkrasında belirtilen müşterinin talep ya da talimatının alınmış olması gerekmektedir.**

Diğer taraftan, **“temsil ilişkisi bulunmadığı halde”** hukuki danışmanlık hizmeti alınan bu gibi taraflar ile, müşteri kimliğini belirli veya belirlenebilir kılacak şekilde bir paylaşım yapılmaması halinde ise, müşteriden talep ya da talimat alınmasına gerek bulunmamaktadır.

3.11. 5549 Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun ve bankaların tabi olduğu uluslararası AML/CTF düzenlemeleri kapsamında işlemleri tamamlamak için gereken, muhabir bankalarca talep edilen bilgilerin (işleme konu taraflara ait kimlik/adres/vatandaşlık/nihai faydalanıcı/meslek/faaliyet ve benzeri bilgileri ile tarafların ortakları veya ilişkili olduklarına ait kimlik/adres/vatandaşlık/nihai faydalanıcı/meslek/faaliyet ve benzeri gibi üçüncü taraf bilgileri) Yönetmeliğin 6 ncı maddesinin altıncı fıkrası kapsamında işlemin gerçekleştirilebilmesi için paylaşımı zorunlu olan bilgiler olarak değerlendirilip değerlendirilemeyeceği:

Yönetmeliğin 5 inci maddesinin sekizinci fıkrası uyarınca 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanunun 5 inci maddesi uyarınca finansal gruba bağlı kuruluşların, müşterinin tanınmasıyla hesap ve işlemlere ilişkin olarak grup içerisinde bilgi paylaşımı sır saklama yükümlülüğüne aykırılık teşkil etmemektedir.

Diğer taraftan, Yönetmeliğin 6 ncı maddesinin altıncı fıkrasında *“İşlemin doğası gereği yurt içinde ya da yurt dışında kurulu banka, ödeme hizmeti sağlayıcısı, ödeme, menkul kıymet mutabakat veya mesajlaşma sistemleri ile etkileşimin gerekli olduğu ve işlemin tamamlanabilmesi için yurt içindeki ya da yurt dışındaki taraflarla müşteri sırrı niteliğindeki bilgilerin paylaşılmasının işlemin zorunlu unsuru olduğu, yurt içi/yurt dışı fon transferi, yurt dışı akreditif, teminat mektubu, referans mektubu gibi işlemler için, işlemin müşteri tarafından başlatılması ya da elektronik bankacılık hizmetlerine yönelik dağıtım kanalları üzerinden müşteri tarafından emir girilmesi, söz konusu paylaşımlar bakımından üçüncü fıkra da belirtilen müşteri talep ya da talimatı yerine geçer.”* hükmüne yer verilmektedir.

Ancak bu hüküm dayanak gösterilerek müşteri tarafından başlatılan işlemler ya da girilen emirler kapsamında yurt içindeki ya da yurt dışındaki taraflarla müşteri sırrı niteliğindeki bilgilerin paylaşılabilmesi için, banka tarafından müşteriye kullanılan sistemin kuralları gereği söz konusu bilgi paylaşımının işlemin tamamlanabilmesi için zorunlu unsur olması gerekmektedir. Dolayısıyla müşteriye kullanılan sistem kurallarının zorunlu kılmadığı ancak yurt dışındaki muhabir banka gibi diğer tarafların kendi risk yönetim politikası veya sair diğer sebeplerle paylaşımı zorunlu kıldığı müşteri bilgilerinin, 2.2 başlığı altında yapılan açıklamalar saklı kalmak üzere, bu fıkra kapsamında değil Yönetmeliğin 6 ncı maddesinin üçüncü fıkrası kapsamında ele alınması gerekmektedir.

3.12. Banka müşterisi olan ve Türkiye’de faaliyette bulunan çok uluslu şirketlerin, muhasebe sistemleri üzerindeki banka hesap mutabakatı gibi bazı operasyonlarının yürütülmesi amacıyla içinde üçüncü taraf bilgilerinin de yer aldığı müşteri hesap hareketlerinin, müşterinin bağlı oldukları çok uluslu grubun hizmet merkezleri ile paylaşılması:

Yönetmeliğin 6 ncı maddesinde de belirtildiği üzere, sır niteliğindeki bilgilerin paylaşılmasına ilişkin genel ilkeler, paylaşımın, sadece belirtilen amaçlarla sınırlı olması ve ölçülülük ilkesine uygun olarak bu amaçların gerektirdiği kadar veriyi içermesi olup, paylaşımın ölçülü olabilmesi için yerine getirilmesi gereken asgari hususlar ise Yönetmeliğin 6 ncı maddesinin birinci fıkrasında sayılmaktadır.

Kanununun 73 üncü maddesinin üçüncü fıkrası ve Yönetmelik hükümleri uyarınca, diğer kanunların emredici hükümleri saklı kalmak kaydıyla, müşteri sırrı niteliğindeki bilgiler, müşterinin açık rızası alınsa dahi, müşteriden gelen bir talep ya da talimat olmaksızın yurt içindeki ve yurt dışındaki üçüncü kişilerle paylaşılabilir ve müşterinin bilgilerini paylaşmaya dair açık rıza göstermesi veya talep ya da talimat vermesi bankanın vereceği hizmetler için bir ön şart haline getirilemez. Bu şartın istisnası ise Yönetmeliğin 5 inci maddesinde sayılan sır saklama yükümlülüğünden istisna tutulan hallerdir.

Bu kapsamda, banka müşterisi olan şirketlerin, hesap hareketlerine ilişkin bilgilerin, yurt dışına, şirketin bağlı olduğu çok uluslu grubun paylaşımlı hizmet merkezlerine gönderilebilmesi için müşterinin bu konuda talep ya da talimatının alınması gerekmektedir.

Yönetmeliğin 6 ncı maddesinin *“Müşterinin, talep ya da talimatı üzerine yapılacak paylaşımlarda birinci fıkrada belirtilen ölçülülük ilkesine uyulup uyulmadığı, müşterinin talep ya da talimatına uyulup uyulmadığı ile sınırlı olarak değerlendirilir. Müşterinin paylaşılmasını talep ettiği veri seti içinde başka müşterilere ya da başka bankaların müşterilerine ilişkin sır kapsamındaki bilgilerin de olması halinde ise, birinci fıkradaki yükümlülüğe herhangi bir sınırlama olmaksızın uyulması zorunludur.”* hükmünü amir yedinci fıkrasında ise müşterinin talep ya da talimatı üzerine yapılacak paylaşımında başka müşterilere ilişkin sır kapsamındaki bilgilerin olması halinde, söz konusu paylaşımın Yönetmeliğin 6 ncı maddesinin birinci fıkrasında düzenlenen, *“amaçla sınırlı olmak”* ve *“ölçülülük ilkesine uygun olarak bu amaçların gerektirdiği kadar veriyi içermek”* esaslarına uygun şekilde yapılması ve paylaşımın ölçülü olabilmesi için anılan hükümde sayılan asgari hususların da yerine getirilmesi gerekmektedir.

Diğer taraftan Yönetmeliğin bu hükmü, içinde üçüncü taraf bilgilerinin de yer aldığı müşteri hesap hareketleri gibi müşteri bilgilerinin, müşterinin talep ya da talimatı üzerine, bizzat müşteri müşterinin kendisi/temsilcisi ile ya da kendisine/temsilcisine ait olduğunu beyan ettiği bir iletişim adresi ile paylaşılmasına engel teşkil etmemektedir. Ancak söz konusu temsil ilişkisinin kurulmasına yönelik müşteri tarafından yapılacak yetkilendirmede ve müşterinin bankaya ileteceği talep/talimatta, müşteri sırrı niteliğindeki bilgi ve belgelerin de temsilci ile paylaşılabilirliğinin açıkça belirtilmesi gerekmektedir. Bu gibi durumlarda müşterinin

paylaşılmasını talep ettiği veri seti içinde başka müşterilere ya da başka bankaların müşterilerine ilişkin sır kapsamındaki bilgilerin de olması nedeniyle bankanın, Yönetmeliğin 6 ncı maddesinin birinci fıkrasındaki yükümlülüğe herhangi bir sınırlama olmaksızın uyma yükümlülüğü bulunmamakta, 6 ncı maddenin yedinci fıkrasının birinci cümlesinde de belirtildiği şekilde **bu gibi durumlarda bankanın ölçülülük ilkesine uyup uymadığı hususu, müşterinin talep ya da talimatına uyulup uyulmadığıyla ya da diğer bir ifade ile bu talep/talimatın sınırlarını aşacak şekilde bizatihi bankanın paylaşım amaç ve yöntemlerini belirleme konusunda inisiyatif alıp almadığıyla sınırlı olacak şekilde değerlendirilmelidir.**

3.13. Ana ortaklığın müşterisi olmayan banka müşterileri ile ilgili Yönetmeliğin 5 inci maddesinin ikinci fıkrasının (b) bendi kapsamında (konsolide finansal tablo hazırlama çalışmaları, risk yönetimi ve iç denetim uygulamaları) veri paylaşılması halinde bu bilgilerin anonim halde gönderilmesinin gerekip gerekmediği ve anonimleştirme yapılması halinde yine de gizlilik sözleşmesi yapılmasına gerek olup olmadığı:

Yönetmeliğin 6 ncı maddesinin sekizinci fıkrasında belirtilen hallerde, Yönetmeliğin 5 inci maddesinin ikinci fıkrasının (b) bendi ve üçüncü fıkrası kapsamında aynı zamanda ana ortaklık, hakim ortak ya da grup şirketinin de müşterisi olmayan banka müşterileri ile ilgili olarak söz konusu taraflarla paylaşılacak müşteri sırrı niteliğindeki bilgilerin, müşterilerin kimliğini belirli veya belirlenebilir kılacak nitelikte olmasının önünde bir engel bulunmamaktadır.

Bu haller dışında ise, söz konusu taraflar ile yapılacak paylaşımların müşteri kimliğini belirli veya belirlenebilir kılacak nitelikte olmaması gerekmele birlikte, müşteri kimliğini belirli veya belirlenebilir kılmamak adına uygulanabilecek tek yöntem “anonimleştirme” yöntemi olmayıp, Yönetmeliğin 6 ncı maddesinin birinci fıkrasının (c) bendinde belirtilen diğer yöntemler olan “toplulaştırma ve kimliksizleştirme” yöntemlerinin de kullanılması mümkün bulunmaktadır.

Diğer taraftan, (b) bendi de dahil olmak üzere, Yönetmeliğin 5 inci maddesinin ikinci fıkrasında düzenlenen sır saklama yükümlülüğünden istisna tutulan tüm hallerde, paylaşımın müşterinin kimliğini belirli veya belirlenebilir kılacak nitelikte olup olmadığı fark etmeksizin, gizlilik sözleşmesinin yapılması gerekmektedir.

3.14. Yönetmeliğin 6 ncı maddesinin sekizinci fıkrasında belirtilen “Kurumun uygun görüşünün alınmış olması” şartı ile kastedilenin ne olduğu ve bu şartın bulunmasının bankanın sorumluluğunu ortadan kaldırıp kaldırmayacağı:

Yönetmeliğin 6 ncı maddesinin sekizinci fıkrasında; “(8) 5 inci maddenin ikinci fıkrasının (b) bendi ile üçüncü fıkrası kapsamında, kredi karşılık hesaplamaları ile içsel sermaye yeterliliği hesaplamaları gibi çok sayıda müşteriye ilişkin kapsamlı veri paylaşımını gerektiren paylaşımlar ile karşı tarafın uyum riski amacıyla yapılacak paylaşımlar için, **paylaşım öncesinde Kurumun uygun görüşünün alınmış olması şartıyla, birinci fıkranın (ç) bendi uygulanmaz.** 5 inci maddenin ikinci fıkrasının (b) bendi ile üçüncü fıkrası kapsamında konsolide risk yönetimi amacıyla paylaşılacak verilerin, banka ana sermayesinin yüzde onu veya daha fazlası oranında kredi kullandırılmış bir gerçek ya da tüzel kişiye veya bir risk grubuna ait olması halinde ise, söz konusu veriler için paylaşım öncesinde Kurumun uygun görüşünün alınmış olması ve birinci fıkranın (ç) bendine uyum şartı aranmaz. Kurul bu fıkra da yer alan sınırlamaları değiştirmeye ya da bu fıkra da yer alan hususlara ilişkin yeni sınırlamalar getirmeye yetkilidir.” hükmüne yer verilmiştir.

2.1 ve 2.2 numaralı başlıklarda da belirtildiği üzere, bu hüküm uyarınca Kuruma yapılacak başvurularda, uyum riski çerçevesinde ana ortaklık/hakim ortak ile yapılması planlanan paylaşım kapsamında hangi verilerin paylaşılacağı, paylaşılacak verilerin paylaşım amacının yerine getirilmesi için gerçekten gerekli olup olmadığı ve uyum riski yönetimi için talep edilen bilgilerin geçerli bir mevzuat hükmünden kaynaklanıp kaynaklanmadığının somut bir şekilde ortaya konulması gerekmekte ve uyum riskine konu yabancı mevzuat hükümlerinin orijinal metinleri ile birlikte Türkçe tercümelerinin de başvuru kapsamında Kuruma iletilmesi ve bu kapsamda bankanın Yönetmeliğin 7 nci maddesi uyarınca tesis edeceği Bilgi Paylaşım Komitesinin yapmış olduğu ölçülülük değerlendirmesinin ve paylaşım talebi hakkındaki kendi uygunluk görüşünün de Kuruma iletilmesi gerekmektedir.

Benzer şekilde söz konusu fıkra da belirtilen “çok sayıda müşteriye ilişkin kapsamlı veri paylaşımını gerektiren paylaşımlar” için Kuruma yapılacak başvurularda da, ana ortaklık/hakim ortak ile yapılması planlanan paylaşım kapsamında hangi verilerin paylaşılacağı ve paylaşılacak verilerin paylaşım amacının yerine getirilmesi için gerçekten gerekli olup olmadığının somut bir şekilde ortaya konulması gerekmekte olup, bu kapsamda bankanın Yönetmeliğin 7 nci maddesi uyarınca tesis edeceği Bilgi Paylaşım Komitesinin yapmış olduğu ölçülülük değerlendirmesinin ve paylaşım talebi hakkındaki kendi uygunluk görüşünün de Kuruma iletilmesi gerekmektedir.

Bu çerçevede, söz konusu Yönetmelik hükmünde belirtilen “Kurumun uygun görüşü”, paylaşımın içeriğinin, ölçülülüğünün ya da gerekliliğinin Kurum tarafından onaylandığını değil; banka tarafından başvuru kapsamında Kuruma iletilen bilgi, belge ve beyanların paylaşım yapılabilmesine izin vermeye yetecek detay ve kapsamda olduğuna ilişkin verilen bir uygunluk görüşüdür. Dolayısıyla söz konusu başvurular kapsamında Kurum tarafından verilen uygunluk

görüşü, bankanın Kanununun 73 üncü maddesi ve Yönetmelikten kaynaklanan uyum yükümlülüklerini ve sorumluluklarını kaldırmadığı gibi, paylaşımın ölçülü ya da gerekli olduğunun onayı manasına da gelmemektedir.

3.15. Yönetmeliğin 6 ncı maddesinin onuncu fıkrası uyarınca, Yönetmeliğin 5 inci maddenin ikinci fıkrasının (b) bendi ile üçüncü fıkrası kapsamında denetim çalışma kağıtları da dahil olmak üzere, iç denetim uygulamaları amacıyla yapılan paylaşımların müşterinin kimliğini belirli veya belirlenebilir kılacak veriler içermesi, ölçülülük ilkesinin düzenlendiği Yönetmeliğin 6 ncı maddesinin birinci fıkrasına aykırılık olarak kabul edilmekte olup, yurt dışında bulunan ana ortaklığın yerinde veya uzaktan denetim uygulamaları amacıyla müşteri bilgilerinin paylaşılması gerektiği durumlarda söz konusu denetimlerin etkin bir şekilde yerine getirebilmesi amacıyla bilgi paylaşımının nasıl yapılabileceği:

Yönetmeliğin 6 ncı maddesinin birinci fıkrasına göre bilgisi paylaşılacak müşteri aynı zamanda ana ortaklığın/hakim ortağın da ortak müşterisi değilse paylaşılacak söz konusu gerçek/tüzel kişi müşteriye ilişkin sır niteliğindeki bilgilerin, anılan müşterinin kimliğini belirli veya belirlenebilir kılacak nitelikte olmaması, diğer bir deyişle açık bir şekilde paylaşılmaması, gerekmektedir. Ayrıca, Yönetmeliğin 6 ncı maddesinin sekizinci fıkrası uyarınca, sır niteliğindeki müşteri bilgilerinin açık bir şekilde paylaşılabilmesi için zorunlu tutulan ortak müşteri olma şartı anılan Yönetmeliğin 5 inci maddesinin ikinci fıkrasının (b) bendi ile üçüncü fıkrası kapsamında yapılacak paylaşımlar için olmak üzere ve yalnızca aşağıdaki durumlarda aranmamaktadır:

1. Kurumun paylaşım öncesinde uygun görüşünün alınmış olması kaydıyla, kredi karşılık hesaplamaları ile içsel sermaye yeterliliği hesaplamaları gibi çok sayıda müşteriye ilişkin kapsamlı veri paylaşımını gerektiren paylaşımlar,

2. Kurumun paylaşım öncesinde uygun görüşünün alınmış olması kaydıyla, karşı tarafın uyum riski amacıyla yapılacak paylaşımlar,

3. Kurumun paylaşım öncesinde uygun görüşünün alınmış olmasına gerek olmaksızın, banka ana sermayesinin yüzde onu veya daha fazlası oranında kredi kullandırılmış bir gerçek ya da tüzel kişiye veya bir risk grubuna ait verileri içeren konsolide risk yönetimi amacıyla yapılacak paylaşımlar.

Söz konusu hükümden de anlaşılacağı üzere, Yönetmeliğin 5 inci maddesinin ikinci fıkrasının (b) bendi ile üçüncü fıkrası kapsamında yapılacak paylaşımlarda, yalnızca yukarıda sayılan durumlarda müşterinin kimliğinin belirli veya belirlenebilir kılacak şekilde paylaşılabilmesi için gerekli olan “ortak müşteri olma” şartının (Yönetmelik madde 6/1-ç) aranmadığı hükme bağlanmış olup, bu

durumlarda dahi ölçülülük ilkesi gereği Yönetmeliğin 6 ncı maddesinin birinci fıkrasının (c) bendinde belirtilen “Paylaşılacak veriler toplulaştırıldığında, kimliksizleştirildiğinde ya da anonim hale getirildiğinde söz konusu amaçlar yine de gerçekleştirilebiliyor ise bu yöntemlerin uygulanması.” ilkesine uyumun gözetilmesi gerekmektedir. Diğer bir ifade ile Yönetmeliğin 6 ncı maddesinin sekizinci fıkrasında belirtilen hallerde, aynı maddenin birinci fıkrasının (ç) bendinde belirtilen ortak müşteri olma şartının aranmaması nedeniyle toplulaştırma, kimliksizleştirme ya da anonim hale getirme yöntemlerinin kullanılma zorunluluğu bulunmasa dahi, anılan maddenin birinci fıkrasının (c) bendi uyarınca bu yöntemlerin uygulanması halinde paylaşım amaçları yine de yerine getirilebiliyor ise bu yöntemlerin uygulanmasına devam edilmesi gerekmektedir.

Dolayısıyla, iç denetim uygulamaları kapsamında yapılacak paylaşımlar da dahil olmak üzere ana ortaklık, hakim ortak ya da grup şirketi ile yapılacak paylaşımlarda, ortak müşteri olma şartı bulunsun ya da bulunmasın, müşteri bilgilerinin açık bir şekilde paylaşılması gerekmiyor ise paylaşımın bu şekilde yapılmaması ve yukarıda belirtilen yöntemlerin uygulanması beklenmektedir.

Diğer taraftan Yönetmeliğin 6 ncı maddesinin onuncu fıkrasında 5 inci maddenin ikinci fıkrasının (b) bendi ile üçüncü fıkrası kapsamında denetim çalışma kağıtları da dahil olmak üzere, iç denetim uygulamaları amacıyla yapılan paylaşımların müşterinin kimliğini belirli veya belirlenebilir kılacak veriler içermesinin, anılan maddenin birinci fıkrasında belirtilen “ölçülülük” ilkesine aykırılık teşkil edeceği açıkça belirtilmiş olduğundan ve iç denetim uygulamaları özelinde 6 ncı maddenin sekizinci fıkrasında herhangi bir istisna tanınmamış olduğundan, paylaşılacak müşteri bilgilerinin aynı zamanda ana ortaklık, hakim ortak ya da grup şirketinin de ortak müşterisi olmadığı durumlarda, iç denetim uygulamaları kapsamında ana ortaklık, hakim ortak ya da grup şirketi ile müşteri kimliğini belirli veya belirlenebilir kılacak şekilde bir bilgi paylaşımı yapılması mümkün bulunmamaktadır.

Ancak ana ortaklığın uyum riski yönetimi kapsamında, bankanın denetim çalışma kağıtlarında ya da iç denetim uygulamaları kapsamında yer verilen müşteri bilgilerine açık bir şekilde erişmesi gerektiğinin somut bir şekilde ortaya konulabilmesi durumunda, Yönetmeliğin 6 ncı maddesinin sekizinci fıkrası uyarınca Kuruma yapılacak başvuru üzerine, anılan maddenin birinci fıkrasının (ç) bendinin uygulanmaması ve dolayısıyla müşteri bilgilerinin toplulaştırma, kimliksizleştirme ya da anonim hale getirme gibi yöntemler uygulanmadan paylaşılması mümkün bulunmaktadır.

4. Bilgi Paylaşım Komitesine İlişkin Açıklamalar (Madde 7)

4.1. Yönetmeliğin 7 nci maddesinde yer verilen Bilgi Paylaşım Komitesinin, müşteri sırrı ve banka sırrı niteliğindeki bilgiler hakkında gelen tüm paylaşım taleplerini somut olay özelinde

değerlendirmesinin gerekip gerekmediği, komitenin genel olarak, yapılacak paylaşımların banka içinde nasıl yapılacağına ilişkin usul ve esasları oluşturup takibini yapmasının yeterli olup olmayacağı:

Yönetmeliğin 7 nci maddesinde Bilgi Paylaşım Komitesinin, Yönetmeliğin 5 inci madde kapsamında yapılacak paylaşımlar da dâhil olmak üzere, ölçülülük ilkesini dikkate alarak **bankaların yapacağı müşteri sırrı ve banka sırrı niteliğindeki bilgilerin paylaşımını koordine etmek, gelen paylaşım taleplerinin uygunluğunu değerlendirmek ve bu değerlendirmeleri kayıt altına almakla sorumlu olduğu** ifade edilmiştir.

Dolayısıyla Bilgi Paylaşım Komitesinin, tüm paylaşım taleplerini somut olay bazında değerlendirmesi gerekmele birlikte, aynı tür ve süreklilik arz eden paylaşım talepleri için genel bir değerlendirme yapmak suretiyle, bu türdeki paylaşımların nasıl ele alınması gerektiğini yapacağı bu genel değerlendirme ile belirlemesi mümkün bulunmakta ve bu şekilde genellik ve süreklilik arz eden her paylaşım talebi için ayrı ayrı değerlendirme yapması gerekmemektedir.

Diğer taraftan, yukarıda yer verilen 2.1 ve 2.2 başlıklı açıklamalarda da belirtildiği üzere, bankanın Yönetmeliğin 6 ncı maddesinin sekizinci fıkrası kapsamında yapacağı başvurularda, o başvuruya ilişkin her bir somut olay bazında yapılacak paylaşımlar için, bankanın Bilgi Paylaşım Komitesinin yapacağı ölçülülük değerlendirmesini ve paylaşım talebi hakkındaki kendi uygunluk görüşünü Kuruma iletmesi gerekmektedir.

USUL/ESASLAR VE DİĞER GENEL KONULAR

Bölüm İçeriği

- Kullanıcı Güvenliğine İlişkin Veri Sorumluları Tarafından Alınması Tavsiye Edilen Teknik ve İdari Tedbirler
- Katılım Belgesinin Verilmesine Dair Usul ve Esaslar
- Bağlayıcı Şirket Kuralları
- Veri Sorumluları İçin Bağlayıcı Şirket Kuralları Başvuru Formu
- Veri Sorumluları İçin Bağlayıcı Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin Yardımcı Doküman

Kullanıcı Güvenliğine İlişkin Veri Sorumluları Tarafından Alınması Tavsiye Edilen Teknik ve İdari Tedbirler

Kullanıcı Güvenliğine İlişkin Veri Sorumluları Tarafından Alınması Tavsiye Edilen Teknik ve İdari Tedbirlere İlişkin Kamuoyu Duyurusu

Yayınlanma Tarihi: 15.02.2022

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrasında “ veri sorumlusunun;

- a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
- c) Kişisel verilerin muhafazasını sağlamak

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu” hükme bağlanmıştır.

Mezkûr Kanunun amir hükmü kapsamında Son zamanlarda Kişisel Verileri Koruma Kurumuna intikal eden veri ihlal bildirimleri değerlendirilmiştir. Bu kapsamında; finans, e-ticaret, sosyal medya ve oyun gibi muhtelif sektörlerde faaliyet gösteren veri sorumlularının internet sitelerine giriş için kullanılan kullanıcı hesap bilgilerinin (kullanıcı adı ve parolalar) bazı internet sitelerinde herkese açık şekilde yayınlandığı görülmüştür. Söz konusu kullanıcı hesaplarını elde eden üçüncü kişilerce anılan veri sorumlularının internet sitelerine kullanıcıların haberi olmadan aktif bir şekilde giriş yapıldığı ve ilgili kişilere ait verilerin bu kapsamda görüntülenebildiği tespit edilmiştir.

Ayrıca farklı zamanlarda, veri sorumluları sistemlerinden veya son kullanıcı bilgisayarlarındaki güvenlik açıkları kullanılarak elde edilen kişisel verilerin, hukuka aykırı bir şekilde paylaşıldığı ve ekonomik bir değer karşılığında satışa sunulabildiği görülmektedir. Bununla birlikte ilgili kişilere ait bu veriler elden ele dolaşarak kötü niyetli kişilerce arşivlenerek daha büyük veri setleri halinde yeniden pazarlanabilmektedir.

Veri sorumluları ve veri işleyenler tarafından veri güvenliği kapsamında alınacak teknik ve idari tedbirlerin olası veri ihlal durumlarını ve ilgili kişiler üzerinde oluşturabileceği riskleri minimize edeceği muhakkaktır. Bu kapsamda yaygın olarak yaşanan ve veri ihlallerinin oluşmasına neden olan “aynı kullanıcı adı ve parolanın farklı platformlarda kullanılması, belirli zaman aralıklarında parola

değişiminin yapılmaması, iki kademeli kimlik doğrulama vb. giriş yöntemlerinin kullanılmaması” gibi teknik ve idari tedbir eksikliklerinin kişisel veri ihlallerine neden olabildiği görülmektedir.

Yukarıda belirtilen ve yaygın olarak yaşanan veri ihlallerini önlemek veya meydana gelmesi halinde ilgili kişiler üzerinde olumsuz sonuç doğurma olasılığının azaltılmasını teminen, veri sorumluları tarafından bir takım önlemlerin alınmasına ihtiyaç duyulmaktadır.

Bu kapsamda veri sorumlularının;

- Çift kademeli kimlik doğrulama (two-factor authentication) sistemlerini kurmaları ve kullanıcılarına üyelik başvurusu aşamasından itibaren alternatif güvenlik önlemi olarak sunmaları,
- Kullanıcıların hesaplarına sık erişim sağlayan cihazlar haricinde farklı cihazlar üzerinden giriş yapılması durumunda, giriş bilgilerinin e-posta/sms vb. yöntemlerle ilgili kişilerin iletişim adreslerine iletilmesinin sağlanması,
- Uygulamaların HTTPS (Hypertext Transfer Protocol Secure - Hiper Metin Aktarma Güvenli İletişim Kuralı) ile veya aynı güvenlik seviyesini sağlayacak bir şekilde koruma altına alınması,
- Kullanıcı parolalarının, siber saldırı yöntemlerine karşı korunmasını teminen, güvenli ve güncel karma (hashing) algoritmaların kullanılması,
- IP (Internet Protocol Address) adresinden yapılacak başarısız giriş denemesi sayısının sınırlandırılması,
- İlgili kişilerin en az son 5 adet başarılı ve başarısız giriş denemeleri ile ilgili bilgilerini görüntüleyebilmelerinin sağlanması,
- İlgili kişilere aynı parolanın birden fazla platformda kullanılmaması gerektiğinin hatırlatılması,
- Veri sorumluları tarafından parola politikasının oluşturulması ve kullanıcılara ait parolaların belirli aralıklarla değiştirilmesinin sağlanması veya bu hususun ilgili kişilere hatırlatılması,
- Yeni oluşturulan parolaların, eski parolalarla (en az son üç parolayla) aynı olmasının engellenmesi, kullanıcı hesaplarına girişlerde bilgisayar ile insan davranışlarını ayırt edici güvenlik kodu gibi teknolojilerin (CAPTCHA, dört işlem vb.) kullanılması, erişime izin verilen IP adreslerinin sınırlandırılması,
- Veri sorumlularının sistemlerine giriş yapılan parolaların uzunluğunun asgari 10 karakter olması, büyük-küçük harf, rakam ve özel karakterlerin bir arada kullanılmasına yönelik güçlü parola oluşturulmasının sağlanması,

- Veri sorumlularının sistemlerine giriş için üçüncü parti yazılımlar veya servisler kullanılıyorsa bu yazılımların ve servislerin güvenlik güncelleştirmelerinin düzenli olarak gerçekleştirilmesi ve gerekli kontrollerin yapılması

gibi teknik ve idari tedbirlerden kendi risk değerlendirmelerini yaparak uygun olanlarını almaları tavsiye edilmektedir.

Katılım Belgesinin Verilmesine Dair Usul ve Esaslar

Katılım Belgesinin Verilmesine Dair Usul ve Esaslar

Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğ, 06.12.2021 tarihli ve 31681 sayılı Resmî Gazete’de yayımlanarak yürürlüğe girmiştir. Tebliğin “Genel esaslar” başlıklı 5’inci maddesinin üçüncü fıkrasında “Katılım belgesine ilişkin usul ve esaslar Kurul tarafından belirlenerek ilan edilir.” ifadesine yer verilmiştir.

Bu doğrultuda, 23.12.2021 tarihli ve 2021/1296 sayılı Kişisel Verileri Koruma Kurulu Kararı ile katılım belgesine ilişkin usul ve esaslar belirlenmiştir.

Kamuoyuna saygıyla duyurulur.

KATILIM BELGESİNİN VERİLMESİNE DAİR USUL VE ESASLAR

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Usul ve Esasların amacı; Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğ kapsamındaki katılım belgesinin verilmesine dair usul ve esasları düzenlemektir.

Kapsam

MADDE 2 - (1) Bu Usul ve Esaslar, katılım belgesinin verilmesine dair şartları kapsar.

Dayanak

MADDE 3 - (1) Bu Usul ve Esaslar 06/12/2021 tarihli ve 31681 sayılı Resmî Gazete’de yayımlanan Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğin 5’inci maddesinin üçüncü fıkrasına dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Usul ve Esasların uygulanmasında;

- a) Eğitimci Kurum: Kurumu ya da Kurul tarafından temel eğitimi vermek ve temel eğitim sınavını gerçekleştirmek üzere bir protokolle yetkilendirilen kurum ve kuruluşu,
- b) Eğitim Tutanağı: Temel eğitimin düzenlendiği yer, tarih, katılımcıların adı, soyadı, imzası, eğitime devam durumu, eğiticinin adı, soyadı, imzası ile verdiği eğitimin konusu, süresi ve sınav sonucunu içeren tutanağı,
- c) Kanun: 24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununu,
- ç) Katılım Belgesi: Düzenlenen temel eğitimi tamamlayıp akabinde yapılacak sınavda başarılı olan kişilere Kurum tarafından verilen belgeyi,
- d) Kurul: Kişisel Verileri Koruma Kurulunu,
- e) Kurum: Kişisel Verileri Koruma Kurumunu,
- f) Sınav: Katılım Belgesi’ne sahip olmak amacıyla temel eğitimin sonunda gerçekleştirilen sınavı,
- g) Tebliğ: Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliği,
- ğ) Temel Eğitim: Ek-1’de belirlenen konulara ve sürelere uygun olarak verilen eğitimi

ifade eder.

(2) Bu Usul ve Esaslarda yer almayan tanımlar için Kanunda ve ilgili ikincil mevzuatta yer alan tanımlar geçerli olacaktır.

İKİNCİ BÖLÜM

Temel Eğitimin Planlanması ve Düzenlenmesi

Temel Eğitim

MADDE 5 - (1) Eğitici kurum;

- a) Temel eğitim için uygun yer, yeterli personel, eğitim materyali, araç ve gereçlerin temin edilmesini,
 - b) Katılımcıların temel eğitime katılmasını ve eğitim tutanağının düzenlenmesini,
- sağlar.

Temel eğitime katılım

MADDE 6 - (1) Temel eğitim, en geç eğitimin başlangıç tarihinden 15 gün önce eğitici kurum tarafından ilan edilmelidir.

(2) Temel eğitim ve sınav ücreti, Kurulun onayı ile eğitici kurum tarafından ayrı ayrı belirlenir.

Temel eğitimin prensipleri

MADDE 7 - (1) Temel eğitim; katılımcılara kişisel verilerin korunması mevzuatı alanında gerekli donanımın kazandırılmasını amaçlar.

(2) Temel eğitim, Ek-1'de belirtilen konulara göre teorik olarak düzenlenir.

(3) Temel eğitim, Kurum tarafından belirlenen yöntemlerle düzenlenir.

(4) Katılımcılar, temel eğitimde mazeretli veya mazeretsiz toplam ders saatinin %20'sini aşmayacak kadar devamsızlık hakkına sahiptir. Katılım zorunluluğuna aykırılığın tespiti halinde kişi hakkında katılım belgesi düzenlenmiş olsa dahi iptal edilir.

ÜÇÜNCÜ BÖLÜM

Sınav ve Belgelendirme

Sınav

MADDE 8 - (1) Temel eğitimin tamamlanmasının ardından katılımcıların bilgi düzeylerini ölçmek amacıyla eğitici kurum tarafından bir sınav gerçekleştirilir.

- (2) Temel eğitim sınav soruları Ek-1'de yer alan konulardan oluşacak şekilde hazırlanmalı ve soru dağılımı, eğitim konularının dağılımıyla aynı ağırlıkta olmalıdır.
- (3) Katılımcıların temel eğitim sınavında başarılı olması için soruların en az %70'ini doğru cevaplaması gerekmektedir.
- (4) Sınav 100 tam puan üzerinden değerlendirilir, her soru beş (5) seçenekli ve çoktan seçmeli olacak şekilde hazırlanır. Sınavda boş bırakılan veya yanlış cevaplandırılmış sorulardan dolayı herhangi bir puan indirimi yapılmaz.
- (5) Sınavların değerlendirilmesi ile ilgili bütün işlemler bittikten sonra eğitici kurum tarafından sonuçlar tutanak altına alınır ve katılımcılara duyurulur.
- (6) Eğitici kurum, soruların hazırlanmasına ilişkin iş ve işlemlerini gizlilik ilkesi içerisinde yürütür.
- (7) Her sınav salonunda en az iki gözetmen bulunur. Sınavı yapacak olan eğitici kurum sınav salonunun güvenliğini sağlamakla yükümlüdür.
- (8) Sınav gözetmenleri, sınavın başlama saatinden en geç 30 dakika önce görev yerinde hazır bulunur.
- (9) Sınav gözetmenleri; sınav sırasında, katılımcıları kontrol eder. Gözetmenler kopya çekmeye veya vermeye kalkışanları uyararak zorunda değildir, tüm sorumluluk katılımcılara aittir. Sınav sırasında kopya çektiği veya verdiği tespit edilen katılımcıların kimlik bilgileri ve yaşanan durum tutanak ile kayıt altına alınır ve bu katılımcılar sınavdan başarısız sayılır.
- (10) Katılımcılar sınava ilişkin itirazlarını, itiraz gerekçelerini de yazmak koşuluyla sınav sonuçlarının ilanından itibaren 30 gün içerisinde eğitici kuruma yapacaktır. Eğitici kurum ise, söz konusu itirazı 30 gün içerisinde sonuçlandırarak başvuran kişiye cevap verecektir.
- (11) Her temel eğitim sonunda katılımcıların üç sınav hakkı bulunmaktadır. Üç sınavdan başarısız olan katılımcılar, yeniden temel eğitimi tamamlamak zorundadır.

Eğitim tutanağı ve katılım belgesi

MADDE 9 - (1) Eğitim tutanağı, eğitici kurum tarafından düzenlenir.

(2) Katılım belgesinde yer alacak bilgiler ve şekil şartları Kurum tarafından belirlenir.

(3) Katılım belgesi, eğitici kurum tarafından düzenlenir ve Kurum tarafından onaylanır.

İstisnalar

MADDE 10 - (1) Temel eğitimden ve sınavdan istisna tutulacak kişiler, Kurul tarafından belirlenir.

(2) İstisna tutulacak kişilere katılım belgesi Kurum tarafından verilir.

Diğer Hususlar

MADDE 11 - (1) Bu Usul ve Esaslarda yer almayan ya da açıklık bulunmayan konularda ilgili mevzuat hükümleri çerçevesinde karar vermeye ve düzenleme yapmaya Kurul yetkilidir.

DÖRDÜNCÜ BÖLÜM

Son Hükümler

Yürürlük

MADDE 12 - (1) Bu Usul ve Esaslar, ilan edildiği tarihte yürürlüğe girer.

Yürütme

MADDE 13 - (1) Bu Usul ve Esasların hükümleri Kişisel Verileri Koruma Kurumu Başkanı tarafından yürütülür.

EK - 1

Sıra	Konu Başlıkları	Saat
1	Kanunun Kapsamı ve Amacı	2
2	Temel Kavramlar	2
3	Genel / Temel İlkeler	3
4	Kişisel Veri İşleme Şartları	4
5	Kişisel Verilerin Yurtiçinde Aktarılması	2
6	Kişisel Verilerin Yurtdışına Aktarılması	2
7	Aydınlatma Yükümlülüğü	2
8	İlgili Kişi Hakları	2
9	Veri Sorumlusuna Başvuru	2
10	Kurula Şikâyet	2
11	Kurumun Yapısı ve Kurul	2
12	Yaptırımlar	2
13	Tam ve Kısmi İstisnalar	2
14	Veri Güvenliği Tedbirleri/Teknik ve İdari Tedbirler	4
15	Veri İhlal Bildirimi Süreçleri	2
16	Silme, Yok Etme, Anonim Hale Getirme	2
17	Veri Sorumluları Siciline Kayıt	3
	Toplam	40

Bağlayıcı Şirket Kuralları

Bağlayıcı Şirket Kuralları Hakkında Duyuru

Yayınlanma Tarihi : 10.04.2020

Kişisel verilerin yurt dışına aktarılması, 6698 sayılı Kişisel Verilerin Korunması Kanununun (6698 sayılı Kanun) 9 uncu maddesi ile düzenlenmektedir. Anılan madde hükmüne göre, kişisel verinin aktarılacağı ülkede yeterli korumanın bulunmaması durumunda kişisel veriler, Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kişisel Verileri Koruma Kurulu'nun (Kurul) izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir.

Bilindiği üzere Kurul, Türkiye'de yerleşik veri sorumlusu tarafından yeterli veri koruması bulunmayan ülkelerde yerleşik veri sorumlusuna/veri işleyene kişisel verilerin aktarımında, ilgili tarafların yeterli bir korumayı yazılı olarak taahhüt etmelerine imkân sağlayan yöntemlerden birini "Taahhütnameler" olarak belirlemiş ve taraflarca hazırlanarak Kurul onayına sunulacak Taahhütnamelerde bulunması gereken asgari unsurları da belirleyerek ilan etmişti. Bu kapsamda söz konusu taahhütnamelerin Kurul tarafından onaylanması akabinde yurt dışına veri aktarımı mümkün olabilmektedir.

Bununla birlikte söz konusu taahhütnameler, genellikle şirketler arasında gerçekleştirilecek iki taraflı veri aktarımlarını kolaylaştırmakla birlikte çok uluslu şirket toplulukları arasında yapılacak veri aktarımları bakımından uygulama pratiğini sağlamakta yetersiz kalabilmektedir. Bu nedenle Kurul tarafından, söz konusu şirketler arasında gerçekleştirilecek uluslararası veri aktarımlarında kullanılmak üzere diğer bir yöntem olarak da "Bağlayıcı Şirket Kuralları" belirlenmiştir.

Bağlayıcı Şirket Kuralları, yeterli korumanın bulunmadığı ülkelerde faaliyet gösteren çok uluslu grup şirketleri için kişisel verilerin yurt dışına aktarımında kullanılan ve yeterli bir korumanın yazılı olarak taahhüt edilmesini sağlayan veri koruma kurallarıdır. Bu kapsama giren şirketlerin, ilgili formu doldurup gerekli talimatları izleyerek Kuruma, Bağlayıcı Şirket Kuralları başvurusu yapması gerekmektedir.

6698 sayılı Kanunun 9 uncu maddesinin (2) numaralı fıkrasının (b) bendi gereğince, söz konusu başvurular Kurul'un iznine tabidir.

Veri Sorumluları İin Baėlayıcı Őirket Kuralları Bařvuru Formu

Veri Sorumluları İin Baėlayıcı Őirket Kurallarında Bulunması Gereken Temel Hususlara İliřkin
Yardımcı Doküman

Veri Sorumluları İin Baėlayıcı Őirket Kuralları Bařvuru Formu

KVKK-BŐK/2020-1

KİŐİSEL VERİLERİ KORUMA KURUMU

BAėLAYICI ŐİRKET KURALLARI

BAŐVURU FORMU

Veri Sorumluları İin Baėlayıcı Őirket Kuralları Bařvuru Formu

Kişisel Verilerin Yurt Dışına Aktarımında Veri Sorumluları İçin Bağlayıcı Şirket Kuralları Başvuru Formu

AÇIKLAMALAR

6698 sayılı Kişisel Verilerin Korunması Kanununun (6698 sayılı Kanun) 9 uncu maddesi ile “Kişisel verilerin yurt dışına aktarılması” düzenlenmektedir. Kanunun 9 uncu maddesinin (2) numaralı fıkrasının (b) bendi gereğince, yeterli korumanın bulunmaması durumunda, kişisel veriler, Türkiye’deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kişisel Verileri Koruma Kurulu’nun (Kurul) izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir.

Kurul’un 02/04/2018 tarih ve 2018/33 numaralı kararı ile kişisel verilerin, Türkiye’de yerleşik veri sorumlusu tarafından yeterli veri koruması bulunmayan ülkelerde yerleşik veri sorumlusuna aktarımına ilişkin olarak 6698 sayılı Kanunun 9 uncu maddesinin (2) numaralı fıkrasının (b) bendine istinaden hazırlanacak taahhütnamelerde bulunması gereken asgari unsurlar belirlenmiştir. Bu taahhütnameler, genellikle şirketler arasında gerçekleştirilecek iki taraflı veri aktarımlarını kolaylaştırmakla birlikte çok uluslu şirket toplulukları arasında yapılacak veri aktarımları bakımından uygulama pratiğini sağlamakta yetersiz kalmaktadır. Bu nedenle, söz konusu şirketler arasında gerçekleştirilecek uluslararası veri aktarımlarında kullanılmak üzere bu başvuru formu oluşturulmuştur.

Bağlayıcı Şirket Kuralları, yeterli korumanın bulunmadığı ülkelerde faaliyet gösteren çok uluslu grup şirketleri için kişisel verilerin yurt dışına aktarımında kullanılan ve yeterli bir korumanın yazılı olarak taahhüt edilmesini sağlayan veri koruma politikalarıdır. Bu kapsama giren şirketlerin, bu formu doldurup gerekli talimatları izleyerek Kişisel Verileri Koruma Kurumuna (Kurum) Bağlayıcı Şirket Kuralları başvurusu yapması gerekmektedir.

6698 sayılı Kanunun 9 uncu maddesinin (2) numaralı fıkrasının (b) bendi gereğince, kişisel verilerin aktarılacağı ülkede yeterli korumanın bulunmaması durumunda, Türkiye’deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli korumayı sağlayacaklarına ilişkin olarak hazırladıkları yazılı taahhütler, Kurul’un iznine tabidir.

Kurul tarafından kabul edilen Bağlayıcı Şirket Kurallarının uygulanması süreye tabi değildir. Gerekmesi halinde Kurul tarafından Bağlayıcı Şirket Kurallarının uygulanması askıya alınabilir ya da feshedilebilir.

BAŞVURUYA İLİŞKİN USUL VE ESASLAR

1. Başvuruyu yapma yetkisi

Grubun Türkiye’de yerleşik merkezi var ise başvuruyu yapmaya burası yetkilidir.

Grubun Türkiye’de yerleşik merkezi yok ise Türkiye’de yerleşik bir Grup üyesi kişisel verilerin korunması konusunda yetkilendirilmelidir (Kısaca “Yetkili Grup Üyesi”). Bu durumda, Grup adına başvuru yapma yetkisini burası haizdir.

2. Başvuruda sunulacak bilgi/belgeler

- a. Başvuru Formu
- b. Bağlayıcı Şirket Kuralları metni
- c. Başvuru ile ilgili gördüğünüz diğer tüm bilgi ve belgeler

Başvurucu, başvuru belgelerini hazırlayarak başvuru aşmasında Kuruma sunar. Gerekmesi halinde Kurum başkaca bilgi ve belge talep edebilir.

3. Başvurunun yöntemi

Başvurular, Kuruma elden veya posta yolu ile iletilir.

4. Başvurunun sonuçlandırılması

Başvurular, Kurum tarafından, resmi başvuru tarihinden itibaren bir (1) yıl içerisinde değerlendirilerek sonuca bağlanır. Gerekmesi halinde bu süre, altı (6) aylık sürelerle uzatılabilir.

Başvurunun Kurulca onaylanması halinde, bu durum Kurum tarafından ilgisine bildirilir ve gerekmesi halinde ilan edilir.

TANIMLAR

Bağlayıcı Şirket Kuralları : Bir şirketler topluluğuna bağlı olarak Türkiye’de yerleşik bir veri sorumlusu tarafından, bu şirketler topluluğuna bağlı olarak yurtdışında bir veya daha fazla ülkede faaliyet gösteren şirketler, teşebbüsler ile ortak bir ekonomik faaliyette bulunan veya veri işleme faaliyetine ilişkin ortak bir karar mekanizması bulunan veri sorumlularına yapılacak olan kişisel veri aktarımları veya aktarım setlerinde uyulması gereken kişisel veri koruma kurallarını ifade eder.

Grup : Bir şirketler topluluğuna bağlı olarak faaliyet gösteren şirketler, teşebbüsler ile ortak bir ekonomik faaliyette bulunan veya veri işleme faaliyetine ilişkin ortak bir karar mekanizması bulunan veri sorumlularının tümünü ifade eder.

Grup üyesi : Şirketler topluluğuna bağlı bir şirket ya da teşebbüs ile ortak bir ekonomik faaliyette bulunan ya da veri işleme faaliyetine ilişkin ortak bir karar mekanizması bulunan bir gruptaki veri sorumlularını ifade eder.

Yetkili Grup üyesi : Grubun Türkiye’de yerleşik bir merkezinin bulunmadığı durumda kişisel verilerin korunması konusunda yetkilendirilen Türkiye’de yerleşik bir Grup üyesini ifade eder.

KISALTMALAR

6698 sayılı Kanun : 6698 sayılı Kişisel Verilerin Korunması Kanunu

BŞK : Bağlayıcı Şirket Kuralları

Kurul : Kişisel Verileri Koruma Kurulu

Kurum : Kişisel Verileri Koruma Kurumu

EKLER

Ek 1 : Baęlayıcı Őirket Kuralları Metni

Baęlayıcı Őirket Kuralları metninin bir asıl suretini ekleyiniz.

Dięer : Baęlayıcı Őirket Kuralları bařvurunuz için gerekli olduęunu dūřündüęünüz dięer tüm bilgi ve belgeleri burada listeleyerek bařvuruunuza ekleyiniz.

KİŞİSEL VERİLERİN YURT DIŞINA AKTARIMINDA

BAĞLAYICI ŞİRKET KURALLARI

BAŞVURU FORMU

I. BAŞVURUCU BİLGİLERİ

Bu bölümde, başvuruda bulunan çokuluslu şirketler topluluğu (Bundan sonra kısaca “Grup” olarak anılacaktır.), başvuruyu gerçekleştiren kişi ve Bağlayıcı Şirket Kuralları ile bağlı çokuluslu şirketler topluluğu bünyesinde yer alan her bir şirket (Bundan sonra kısaca “Grup üyesi” olarak anılacaktır.) bakımından sorular yer almaktadır.

A. Başvuruda Bulunan Şirketler Topluluğu Bakımından

Adı/Unvanı:

Genel Merkezinin Adresi:

Türkiye’de yerleşik Grup üyesinin adresi (Genel Merkezi Türkiye’de değilse):

B. Başvuru İşlemini Gerçekleştiren Bakımından

Başvurucunun Adı/Unvanı:

Varsa TCKN/VKN:

Başvurucunun Hukuki Statüsü (şirket, ortaklık vb.):

Başvurucunun Grup içerisindeki pozisyonu (Grubun Türkiye’de yerleşik merkezi veya Türkiye’de yerleşik merkezi yok ise kişisel verilerin korunması konusunda yetkilendirilmiş ve Türkiye’de yerleşik bir Grup üyesi):

Temas kişinin adı ve/veya birimi:

Adresi:

Telefon Numarası:

Faks Numarası:

Elektronik posta adresi:

C. Diğer Hususlar

1. Veri aktarımı Türkiye’den hangi ülkeye/ülkelere gerçekleştirilecek belirtiniz:

2. Bağlayıcı Şirket Kurallarının kapsayacağı tüm Grup üyeleri ile iletişim bilgilerini belirtiniz:

II. BAĞLAYICI ŞİRKET KURALLARINA YÖNELİK BİLGİLER

Bu bölümde, Bağlayıcı Şirket Kurallarının tüm Grup üyeleri ve Grup adına veri işleme faaliyetini gerçekleştirenler bakımından bağlayıcılığının nasıl sağlanacağı, etkili bir uygulamayı teminen öngörülen mekanizmalar, Kurum ile koordinasyon, kişisel verinin aktarılması ve işlenmesi ile ilgili detaylar, raporlama ve kayıt değişikliği mekanizmaları, veri güvenliği konuları, hesap verebilirlik, Bağlayıcı Şirket Kuralları başvurusuna ilişkin yardımcı bilgi ve belgeler hakkında sorular ile genel hükümler yer almaktadır.

A. BAĞLAYICILIK UNSURU

Bağlayıcı Şirket Kuralları başvurusunun uygun bulunabilmesi için ulusal mevzuata uygun olarak tarafları bağlayıcı bir etkiye sahip olması gerekmektedir. Bu bölümde yer alan sorular, söz konusu bağlayıcılık unsurunun bulunup bulunmadığına karar verilmesi bakımından gereklidir. Her alt başlık içerisinde, konu ile ilgili açıklamalarınızı açık ve anlaşılır bir dil ile ifade ediniz.

1. Grup Şirketleri Bakımından

- Grup üyeleri arasında Bağlayıcı Şirket Kurallarına uyma yükümlülüğü (Kısaca: bağlayıcılık) hangi yöntemle (örneğin Grup şirketleri arasında yapılacak sözleşmeler, tek taraflı taahhütnameler, taraflarca onaylanmış etik kurallar vb.) sağlanacak, açıklayınız:
- Grup içerisinde, söz konusu yöntemlere uygun davranılmamasının sonuçları nedir, açıklayınız:
- Bağlayıcı Şirket Kuralları, tüm Grubu kapsamakta mıdır, varsa muaf tutulan Grup üyesini belirterek sebebini açıklayınız:

2. Çalışanlar Bakımından²⁴

- Çalışanların, Bağlayıcı Şirket Kurallarına uyma yükümlülüğü nasıl sağlanacak, ilgili belgelere (iş sözleşmesi, toplu iş sözleşmesi, gizlilik sözleşmesi, etik kurallar, şirket politikaları, iş yeri yönergeleri, disiplin yönetmelikleri vb.) atıf yaparak kısaca özetleyiniz.
- Çalışanlar tarafından, Bağlayıcı Şirket Kuralları hükümlerinin ihlal edilmesi durumunda uygulayacağınız yaptırımları belirtiniz:

3. Veri İşleyenler Bakımından

²⁴ Çalışanların, Bağlayıcı Şirket Kurallarını okumaları ve ihtiyaç duydukları her an Bağlayıcı Şirket Kurallarına ulaşabilmelerinin sağlanması gerekmektedir.

- Veri işleyenlerin, kişisel verilerin güvenliğini sağlamaya yönelik önlemleri almasını zorunlu tutmak için uygulayacağınız yöntemleri (örneğin, sözleşmelerde yükümlülük getiren maddeler düzenlemek gibi) belirtiniz:

- Uygulayacağınız yöntem bakımından, veri işleyenler tarafından Bağlayıcı Şirket Kurallarına aykırı davranılmasının sonuçlarının ve yaptırımlarının neler olduğunu açıklayınız:

4. İlgili Kişinin Hakları ve Yasal İddialar Bakımından²⁵

- Grup üyeleri tarafından, ilgili kişinin 6698 sayılı Kanun kapsamında sahip olduğu hak ve yetkilerin (10 uncu, 11 inci, 13 üncü ve 14 üncü maddeleri gibi) temin edileceğini beyan ediniz:

- Bağlayıcı Şirket Kuralları kapsamında, ilgili kişilerin, 6698 sayılı Kanununun 11 inci maddesinin (ğ) bendinde yer alan zararın giderilmesini talep etme hakkı da dâhil olmak üzere her türlü zararının tazmini için açılacak davalar bakımından Türk mahkemelerine başvurulabileceğini, beyan ediniz:

- İlgili kişilerin hakları bakımından diğer ülkelerde açılacak davalarda ilgili kişiye tercüme, avukat sağlanması vb. her türlü yardımın sağlanacağını beyan ediniz:

- Grup içerisinde, ihlalin nereden kaynaklandığına bakılmaksızın, Bağlayıcı Şirket Kuralları hükümlerinin ihlalden kaynaklanan zararın, Grubun Türkiye’de yerleşik merkezi veya kişisel verilerin korunması konusunda yetkilendirilmiş Türkiye’de yerleşik bir Grup üyesi tarafından giderilmesi gerekmektedir. Bu kapsamda, yetkili Grup üyesini ve alınan finansal güvenceler dâhil olmak üzere uygun güvenceleri açıklayınız:

- İddianın nereden kaynaklandığına bakılmaksızın, Bağlayıcı Şirket Kuralları hükümlerinin ihlali iddiasıyla ilgili ispat yükünün, Grubun Türkiye’de yerleşik merkezinde veya Grubun merkezi Türkiye’de değil ise kişisel verilerin korunması konusunda yetkilendirilmiş Türkiye’de yerleşik Grup üyesinde bulunması gerekmektedir. Buna ilişkin süreci açıklayınız:

B. ETKİLİ UYGULAMA

²⁵ Bağlayıcı Şirket Kurallarında, 6698 sayılı Kanunun aşağıdaki hükümlerine asgari olarak yer verilmelidir:

- Madde 4 (Genel ilkeler),
- Madde 11 (İlgili kişinin hakları),
- Verinin aktarıldığı ülkede, Bağlayıcı Şirket Kurallarına uymayı engelleyen ulusal bir mevzuatın bulunup bulunmadığı ve bulunması halinde açıkça belirtilmesi,
- Grup üyelerinden birinin, üçüncü bir ülkede tabi olduğu ve Bağlayıcı Şirket Kuralları ile sağlanan teminatlar üzerinde önemli olumsuz etkileri olma ihtimali bulunan tüm yasal yükümlülüklerinin Kuruma bildirilmesi,
- Kurum ile koordinasyon,
- Madde 13 (Veri sorumlusuna başvuru).

Bağlayıcı Şirket Kurallarının, Grup tarafından etkili bir şekilde uygulanması önemlidir. Bu kısımda Bağlayıcı Şirket Kurallarının etkili bir şekilde uygulanabilmesini sağlamak için hangi mekanizmaları, nasıl kullandığınız hakkında sorular yer almaktadır. Grup içerisinde Bağlayıcı Şirket Kurallarının nasıl uygulamaya geçirileceği, özellikle, yurt dışına aktarılan veriler bakımından yeterli korumayı sağlayacak önlemlerin alınıp alınmadığının değerlendirilmesinde önemlidir.

1. Eğitim ve Farkındalık Çalışmaları (Çalışanlar Bakımından)

Bağlayıcı Şirket Kurallarının, çalışanlar tarafından uygun ve etkili bir şekilde uygulanmasını sağlamak üzere, aşağıdaki konularla ilgili yaptığınız ya da yapacağınız çalışmalar hakkında kısaca bilgi veriniz.

- Çalışanların, Bağlayıcı Şirket Kurallarını etkin bir şekilde uygulamasını ve kişisel verilerin korunması hakkına saygılı olmasını sağlamak üzere özel eğitim programlarınız var mı, açıklayınız:
- Çalışanların, kişisel verilerin korunması, veri güvenliği ve Bağlayıcı Şirket Kuralları hükümleri bakımından bilgi ve farkındalık seviyesinin takibi yapılmakta mı, açıklayınız:
- Bağlayıcı Şirket Kuralları metinlerinin tüm çalışanlara basılı veya çevrimiçi ortamda iletilmesi sağlanmakta mı, açıklayınız:
- Kişisel veri işleme faaliyetleri bakımından Grup içerisinde bu konuda yetkili kişilerin inceleme ve onayı söz konusu mu, açıklayınız:
- Çalışanların, işleri ile kişisel veri güvenliği arasındaki ilişkiyi kavramaları ve gerektiğinde harekete geçmeleri konusunda ne tür eğitimler öngörülmekte, açıklayınız:

2. Şikâyet Mekanizması

- Bağlayıcı Şirket Kurallarına uyumlu hareket edilmemesi halinde, bu durumu bildirmek üzere Grup içerisinde şikâyet mekanizması var mı, kısaca açıklayınız:

3. Uyumluluk Denetimi

- Her bir Grup üyesinin Bağlayıcı Şirket Kurallarına uyumunun denetimini yapmak veya yaptırmak için Grup tarafından hangi mekanizmalar kullanılmaktadır, açıklayınız:
- Uyumluluk denetimi mekanizmalarının Bağlayıcı Şirket Kuralları metninde nerede ve nasıl düzenlendiğini açıklayınız:
- Bağlayıcı Şirket Kuralları metninde, taahhüde uyumluluğu denetlemek üzere kimler görevlendirilmiştir, görev ve sorumlulukları nelerdir açıklayınız:

- Uyumluluk denetimi mekanizmalarının belirli aralıklarla gözden geçirilmesini/güncellenmesini sağlayacak düzenlemeleriniz bulunmakta mı, açıklayınız:

- Belirli aralıklarla, şeffaf ve açık bir raporlama öngörülmekte mi, açıklayınız:

4. Bağlayıcı Şirket Kurallarının Uygulanması Konusunda Görevli Personel

- Tüm Grup bakımından Bağlayıcı Şirket Kurallarına uyumun sağlanması ve bunun takibi için görevlendirilmiş uygun bir personel/birim yapılanması bulunuyor mu, açıklayınız:

- Bu personel/birim yapılanmasının oluşumu, görev ve sorumlulukları gibi hususları açıklayınız:

C. KURUM İLE KOORDİNASYON

Bu kısımda, Kurum ile koordinasyon konuları düzenlenmekte ve Bağlayıcı Şirket Kurallarının uygulanması bakımından Kurum ile gerçekleştirecek işbirliği hakkında bilgi talep edilmektedir.

- Kurum ile koordinasyonun nasıl sağlanacağını açıklayınız.

Ç. KİŞİSEL VERİLERİN İŞLENMESİ VE AKTARILMASI

Bu kısımda, Bağlayıcı Şirket Kurallarının, 6698 sayılı Kanun uyarınca kişisel verilerin aktarımında yeterli güvenceyi sağlayıp sağlamadığının Kurul tarafından değerlendirilmesini teminen Grup içerisindeki kişisel veri işleme süreçlerinin açık ve anlaşılır şekilde tanımlanması gereklidir.

- Aktarıma konu veri kategorilerini²⁶ (kimlik, iletişim, lokasyon, özlük gibi) belirtiniz:

- Her bir veri kategorisinde yer alan veriler bakımından verinin niteliğini (genel/özel nitelikli kişisel veri), aktarımın amaçlarını ve azami saklama sürelerini belirtiniz:

- Veri konusu kişi grubu veya gruplarını belirtiniz (çalışan, stajyer, ziyaretçi, ürün veya hizmet alan kişi gibi):

- Veri aktarımının hangi yöntemle (bulut ortamı, elektronik posta, taşınabilir depolama araçları vb.) gerçekleştirileceğini belirtiniz:

- Veri aktarımının hukuki sebebini/sebeplerini belirtiniz:

- Aktarılabilecek verilerin Grup içerisindeki dağılımını, ilgili Grup üyelerinin adı ve iletişim bilgilerini belirterek açıklayınız:

- Bu Bağlayıcı Şirket Kuralları, Türkiye ve yurt dışında bulunan bütün Grup şirketleri arasındaki veri aktarımlarında mı kullanılacak, açıklayınız:

²⁶ Veri kategorileri için VERBİS'teki sınıflandırma örnek alınmalıdır.

- İhtiyaç duyulması halinde, Türkiye’de yerleşik olmayan bir Grup üyesinden, grup üyesi olmayan herhangi bir şirkete yapılacak veri aktarımları (sonraki aktarım)²⁷ yapılacak ise bu konuda öngörülen aktarımları belirtiniz:

D. RAPORLAMA VE KAYIT DEĞİŞİKLİĞİ MEKANİZMALARI

Hem Grup üyeleri hem de Kurum, Bağlayıcı Şirket Kurallarında yapılacak herhangi bir değişiklik hakkında en kısa sürede bilgilendirilmelidir.

Bağlayıcı Şirket Kurallarının uygulanmasına hiçbir şekilde etki etmeyen, salt idari değişiklikler gibi hususlar hariç olmak üzere ilgili kişinin haklarına zarar verebilecek veya veri güvenliğini önemli ölçüde etkileyecek türden değişikliklerin önceden Kuruma bildirilmesi gerekmektedir.

Bu kısımda, Grubunuzun bu türden değişiklikleri bildirmek ve kaydını tutmak üzere uygulayacağı mekanizmaların açıklanması gerekmektedir.

- Bağlayıcı Şirket Kuralları metni veya Grubun üyeleri bakımından meydana gelebilecek değişikliklerden diğer grup üyeleri ve Kurumun nasıl haberdar edileceğini açıklayınız:

- Bağlayıcı Şirket Kuralları metni ve uygulanması bakımından meydana gelecek her türlü değişikliği kayıt altına alacak bir sisteminiz var mı, açıklayınız:

E. VERİ GÜVENLİĞİ²⁸

Bu bölümde, Bağlayıcı Şirket Kuralları kapsamında aktarılacak kişisel verilerin niteliğine uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirin nasıl ele alındığına dair detayların açıklanması gerekmektedir. Bağlayıcı Şirket Kurallarında, aşağıdaki konuların nasıl düzenlendiğini, varsa destekleyici dokümanları kullanarak ve uygun kısımlara atıf yaparak açıklayınız.

- Bağlayıcı Şirket Kuralları metninde, genel ilkelere uyum konusunun nerede ve nasıl değerlendirildiğini açıklayınız²⁹:

²⁷ Bu türden veri aktarımları için Kurulun 02/04/2018 tarih ve 2018/33 sayılı kararı ekinde yer alan “Taahhütnameler”in kullanılması gerekmektedir.

Taahhütnamelere <https://kvkk.gov.tr/Icerik/5255/Taahhutnameler> adresinden ulaşabilirsiniz.

²⁸ 6698 sayılı Kanun madde 9/2/b, 9/4/d, 12/1

²⁹ 6698 sayılı Kanun madde 4/2; “Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

a. Hukuka ve dürüstlük kurallarına uygun olma.

b. Doğru ve gerektiğinde güncel olma.

c. Belirli, açık ve meşru amaçlar için işlenme.

ç. İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

d. İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.”

- Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen uygun güvenlik düzeyini temin etmeye yönelik teknik tedbirleri (gerekli gördüğünüz durumlarda Grup üyelerini de belirterek) açıklayınız:

- Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen uygun güvenlik düzeyini temin etmeye yönelik idari tedbirleri (gerekli gördüğünüz durumlarda Grup üyelerini de belirterek) açıklayınız:

- 6698 sayılı Kanunun 6 ncı maddesinin 4 numaralı fıkrası gereğince, özel nitelikli kişisel verilerin işlenmesinde, Kurul tarafından belirlenen yeterli önlemlerin³⁰ alınması şarttır. Bu kapsamda aldığınız önlemleri açıklayınız:

- Diğer hususlar (varsa):

- Veri ihlal bildirimine³¹ ilişkin sürecinizi açıklayınız:

F. HESAP VEREBİLİRLİK VE DİĞER ESASLAR/ARAÇLAR

- Grup üyelerinin, Bağlayıcı Şirket Kurallarına nasıl uyum sağlayacağı ve bundan nasıl sorumlu tutulacağını açıklayınız:

- Grup üyeleri tarafından, her bir veri sorumlusu adına Bağlayıcı Şirket Kuralları kapsamında gerçekleştirilecek işleme faaliyetlerinin kaydının nasıl tutulacağını açıklayınız³²:

G. YARDIMCI BİLGİ VE BELGELER

1. Uluslararası Sözleşmelere Taraf Olma Durumu

³⁰ "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" başlıklı ve 31/01/2018 tarih ve 2018/10 sayılı Kurul Kararı

³¹ 6698 sayılı Kanun madde 12/5: "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir."

Kurulun 24.01.2019 tarih ve 2019/10 sayılı Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin kararı ile "en kısa süre" ifadesi 72 saat olarak belirlenmiştir. Kararı incelemek ve Kişisel Veri İhlali Bildirim Formu'na ulaşmak için <https://kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirim>

³² 30.12.2017 tarih ve 30286 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren Veri Sorumluları Sicili Hakkında Yönetmelik madde 4/1(h) ile kişisel veri işleme envanteri "Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter.." olarak tanımlanmaktadır. Bağlayıcı Şirket Kuralları bakımından hesap verebilirliğin sağlanması amacı ile söz konusu Yönetmelikte düzenlenen Kişisel Veri İşleme Envanterinin ("Envanter") hazırlanması gerekmektedir.

Aktarımın yapılacağı ülkelerin taraf olduğu, kişisel verilerin korunması konusunda hüküm içeren uluslararası sözleşmeleri, ilgili kısımlara atıf yaparak belirtiniz:

2. Verinin Aktarıldığı Ülke Mevzuatı ve Uygulaması

Kişisel verinin aktarılacağı ülkede, kişisel verilerin korunması konusunda ulusal mevzuat ve yetkili bir kişisel verileri koruma otoritesi var mı, varsa konuyla ilgili mevzuatı ve uygulamasını kısaca belirtiniz:

H. GENEL HÜKÜMLER

Bu kısımda, Bağlayıcı Şirket Kurallarına ilişkin genel düzenleyici hükümler yer almaktadır.

- Bağlayıcı Şirket Kuralları başvuru formu doldurulurken, her alt başlık içerisinde konu ile ilgili gerekli ve yeterli açıklamalar yapılarak açık ve anlaşılır bir dil kullanılmalıdır.

- Başvuru ve uygulama aşamasında, bir bütün olarak Grup ve Grup üyelerinden her biri Bağlayıcı Şirket Kurallarının yorumlanması ve uygulanmasıyla ilgili Kurumun talimatlarına uygun hareket etmeyi kabul eder.

- Bağlayıcı Şirket Kurallarının uygulanması bakımından, Bağlayıcı Şirket Kuralları başvurusunu yapmaya yetkili Grubun Türkiye’de yerleşik merkezi veya Grubun merkezi Türkiye’de değil ise kişisel verilerin korunması konusunda yetkilendirilmiş Türkiye’de yerleşik bir Grup üyesi muhataptır.

- Grup, Bağlayıcı Şirket Kuralları kapsamında aktarılan kişisel verileri, 6698 sayılı Kanuna ve Bağlayıcı Şirket Kurallarına uygun olarak işler, herhangi bir sebeple Kanuna ve Taahhüde uygunluk sağlanamazsa Kurumu konu ile ilgili derhal bilgilendirir. Bu durumda Kurumun, veri aktarımını askıya alma ve Bağlayıcı Şirket Kurallarını feshetme hakkına sahip olacağını kabul eder.

- Bağlayıcı Şirket Kuralları kapsamında işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, bu durum en kısa sürede Grubun Türkiye’de yerleşik merkezine veya Grubun merkezi Türkiye’de değil ise kişisel verilerin korunması konusunda yetkilendirilmiş Türkiye’de yerleşik bir Grup üyesine bildirilir. Bunlar ise söz konusu durumu en kısa sürede

ilgisine³³ ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.³⁴

- Bağlayıcı Şirket Kuralları, yalnızca bir bütün olarak Grup içerisinde ve Grup üyeleri arasındaki veri aktarımlarına ilişkindir. Bağlayıcı Şirket Kuralları kapsamında aktarımına izin verilen kişisel veriler, Grup üyeleri dışındaki kişilere aktarılamaz. Türkiye’de yerleşik olmayan bir Grup üyesinden, grup üyesi olmayan herhangi bir şirkete veri aktarımı (sonraki aktarım) yapılmasına ihtiyaç duyulması halinde Kurulun 02/04/2018 tarih ve 2018/33 sayılı kararı ekinde yer alan “Taahütname”in kullanılması gerekmektedir.

- Grup üyelerinden herhangi birinin Grupla bağının kesilmesi, Bağlayıcı Şirket Kurallarının herhangi bir sebeple sona ermesi gibi durumlarda, aktarıma konu kişisel veriler yedekleri ile Grubun Türkiye’de yerleşik merkezine veya Grubun merkezi Türkiye’de değil ise kişisel verilerin korunması konusunda yetkilendirilmiş Türkiye’de yerleşik bir Grup üyesine gönderilir ya da yedekleri ile birlikte tamamen yok edilir. Ulusal mevzuatta bu yükümlülüğün yerine getirilmesini engelleyen hükümler varsa, aktarıma konu kişisel verilerin gizliliğini güvence altına almak için gerekli idari ve teknik tedbirler alınarak veri işleme faaliyeti sınırlandırılır.

- Bir bütün olarak Grup ve Grup üyeleri, işledikleri kişisel verileri, 6698 sayılı Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamaz. Bu yükümlülük herhangi bir süre ile sınırlı değildir.

EK 1:

BAĞLAYICI ŞİRKET KURALLARI METNİ

Bağlayıcı Şirket Kuralları metninin bir suretini ekleyerek bu ekin, göndermek istediğiniz tüm yardımcı bilgi ve belgeleri içerdiğinden emin olunuz.

³³ Kurulun 24.01.2019 tarih ve 2019/10 sayılı Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin kararı gereğince, ihlal durumunun öğrenilmesinden itibaren veri sorumlusu tarafından gecikmeksizin ve en geç 72 saat içinde Kurula bildirim yapılması gerekmektedir. Detaylı bilgi için: Kurulun 24.01.2019 tarih ve 2019/10 sayılı Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin kararı <https://kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi>

³⁴ 6698 sayılı Kanun madde 12/5

**Veri Sorumluları İin Baėlayıcı Őirket Kurallarında Bulunması Gereken Temel Hususlara İliŐkin
Yardımcı Doküman**

KVKK-BŐK/2020-2

KİŐİSEL VERİLERİ KORUMA KURUMU

BAėLAYICI ŐİRKET KURALLARI

Veri Sorumluları İin Baėlayıcı Őirket Kurallarında Bulunması Gereken Temel Hususlara
İliŐkin Yardımcı Doküman

TANIMLAR

Bağlayıcı Şirket Kuralları : Bir şirketler topluluğuna bağlı olarak Türkiye’de yerleşik bir veri sorumlusu tarafından, bu şirketler topluluğuna bağlı olarak yurt dışında bir veya daha fazla ülkede faaliyet gösteren şirketler, teşebbüsler ile ortak bir ekonomik faaliyette bulunan veya veri işleme faaliyetine ilişkin ortak bir karar mekanizması bulunan veri sorumlularına yapılacak olan kişisel veri aktarımları veya aktarım setlerinde uyulması gereken kişisel veri koruma kurallarını ifade eder.

Grup : Bir şirketler topluluğuna bağlı olarak faaliyet gösteren şirketler, teşebbüsler ile ortak bir ekonomik faaliyette bulunan veya veri işleme faaliyetine ilişkin ortak bir karar mekanizması bulunan veri sorumlularının tümünü ifade eder.

Grup üyesi : Şirketler topluluğuna bağlı bir şirket ya da teşebbüs ile ortak bir ekonomik faaliyette bulunan ya da veri işleme faaliyetine ilişkin ortak bir karar mekanizması bulunan bir gruptaki veri sorumlularını ifade eder.

Yetkili Grup üyesi : Grubun Türkiye’de yerleşik bir merkezinin bulunmadığı durumda kişisel verilerin korunması konusunda yetkilendirilen Türkiye’de yerleşik bir Grup üyesini ifade eder.

KISALTMALAR

6698 sayılı Kanun : 6698 sayılı Kişisel Verilerin Korunması Kanunu

BŞK : Bağlayıcı Şirket Kuralları

Kurul : Kişisel Verileri Koruma Kurulu

Kurum : Kişisel Verileri Koruma Kurumu

KVKK : Kişisel Verileri Koruma Kurumu

AÇIKLAMALAR

Veri sorumluları için Bağlayıcı Şirket Kuralları, kişisel verilerin, Türkiye’de yerleşik veri sorumlularından aynı grup içerisindeki ve Türkiye dışındaki diğer veri sorumluları veya veri işleyenlere aktarımı için kullanılır.

Dolayısıyla, veri sorumluları için Bağlayıcı Şirket Kurallarında belirtilen yükümlülükler, aynı grupta veri sorumlusu olarak hareket eden kuruluşlar ve “dâhili” veri işleyen olarak hareket edenler için geçerlidir.

Bağlayıcılığın sağlanması amacı ile Bağlayıcı Şirket Kuralları kapsamında yer alacak veri sorumlusu ile veri işleyen arasında Türk hukukunda geçerli yasal bir sözleşme ya da diğer bir hukuki işlem düzenlenerek bunun tüm veri işleyenler tarafından imzalanması sağlanmalıdır (Hizmet Sözleşmesi³⁵). Veri sorumluları için Bağlayıcı Şirket Kuralları ile belirlenen yükümlülükler, Hizmet Sözleşmesine aykırı düşmeyecek şekilde, Grup içerisinde veri işleyen olarak veri aktarılan yapılara da uygulanır.

³⁵ Kişisel veri işleme faaliyetlerinde veri sorumlusunun veri işleyenle birlikte hareket ettiği durumlarda, aralarında yazılı bir sözleşme yapılması gereklidir. Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) (KVKK Yayınları, Ocak 2018, Ankara) adlı Rehber ile de veri sorumlusunun veri işleyenden alacağı hizmetler bakımından kişisel veriler konusunda en az kendileri tarafından sağlanan güvenlik seviyesinin sağlandığından emin olması gerektiği hatırlatılmaktadır. 6698 sayılı Kanun madde 12/2 gereğince, “Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.”. Bu bakımdan veri sorumlusu ile veri işleyen arasındaki ilişkiyi düzenleyen sözleşmenin yazılı olması, veri işleyenin sadece veri sorumlusunun talimatları doğrultusunda, sözleşmede belirtilen veri işleme amaç ve kapsamına uygun ve kişisel verilerin korunması mevzuatı ile uyumlu şekilde hareket edeceğine ilişkin hüküm içermesi ve Kişisel Veri Saklama ve İmha Politikasına uygun olması önerilmektedir.

Veri sorumlusunun özel ya da genel yazılı bir yetkilendirmesi ile Bağlayıcı Şirket Kuralları ile bağlı olan diğer BŞK üyeleri, veriyi başkaca veri işleyenlere işletebilir. Hizmet Sözleşmesinde, hizmetin başlangıcında genel bir ön izin verilesinin yeterli olup olmadığı ya da her bir yeni veri işleyen için spesifik bir izin gerekip gerekmediği belirtilecektir. Eğer genel bir izin verildiyse, veri işleyen diğer veri işleyenlere ilişkin değişiklikler hakkında veri sorumlusuna makul bir sürede bilgi verir, böylece veri sorumlusunun verinin yeni bir veri işleyene iletilmesinden önce değişikliğe itiraz edebilmesi ya da sözleşmeyi sonlandırılabilmesine imkân sağlanır.

Uygunluk Kriterleri	BŞK Metni İçin	Başvuru Formu İçin	İlgili yasal dayanaklar	Açıklamalar	Referanslar (Başvuru formu ve BŞK ye yapılacak referanslar başvuran tarafından tamamlanacaktır)
1. BAĞLAYICILIK UNSURU					
1.1 BŞK'ye uyma yükümlülüğü	EVET	EVET	6698 sayılı Kanun m. 9/2/b	BŞK hukuken bağlayıcı olmalı ve BŞK'ye uyma hususunda çalışanları da dâhil olmak üzere tüm grup üyelerine açık bir yükümlülük getirmelidir.	
1.2. Kuralların, grup içerisindeki BŞK üyeleri ve çalışanlarını nasıl bağladığına ilişkin açıklama	HAYIR	EVET	6698 sayılı Kanun m. 9/2	Grup, kuralların bağlayıcı niteliğini başvuru formunda açıklamak zorundadır: Gruptaki her üye için hukuken geçerli ve ispatlanabilir bir veya daha fazla yöntem ile BŞK'nin bağlayıcılığı sağlanmalıdır. Çalışanlar üzerinde bağlayıcılığın sağlanması için iş sözleşmesi, toplu iş sözleşmesi, gizlilik sözleşmesi, etik kurallar, şirket politikaları, iş yeri iç yönetmelikleri vb. yöntemlerden bir veya bir kaç kullanılabilir.	
1.3. İlgili kişinin hakları (üçüncü taraf yararlanıcı hakları) ve yasal iddialar (KVKK ve Mahkemeler nezdinde şikâyetle bulunma imkânı dâhil)	EVET	EVET	6698 sayılı Kanun m. 11, 13, 14	BŞK ile ilgili kişilerin hakları açıkça tanınmalıdır. BŞK'de, ilgili kişinin asgari olarak aşağıda sayılan maddelerin uygulanmasını isteme hakkı yer almalıdır; Genel ilkeler (m. 4), İlgili kişinin aydınlatılması (m. 10) Kişisel verilerin silinmesini, yok edilmesini talep etme hakkı (m. 7), İşlenen verilerin münhasıran otomatik sistemler	

			<p>vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme hakkı (m. 11/1/g),</p> <p>Verinin aktarıldığı ülkede, Bağlayıcı Şirket Kurallarına uymayı engelleyen ulusal bir mevzuatın bulunup bulunmadığı ve bulunması halinde açıkça belirtilmesi, Veri sorumlusuna başvuru hakkının tanınması (m. 13), Kurum ile koordinasyon yükümlülüğü,</p> <p>Grup üyelerinden herhangi birinin, yabancı bir ülkede tabi olduğu ve BŞK ile ilgili kişiye sağlanan teminatlar üzerinde önemli olumsuz etkileri olma ihtimali bulunan tüm yasal yükümlülüklerinin belirtilmesi,</p> <p>Yetki tespiti hükümleri (BŞK bakımından yetkili otorite KVKK'dır ve BŞK yetkili otorite olan KVKK'nın bu konuda yetkili birimi olan Kurula şikâyet hakkını ve mahkemelere başvuru hakkını tanımalıdır (m. 14)).</p> <p>BŞK ile ilgili kişilere 6698 sayılı Kanununun 11 inci maddesinin (ğ) bendinde yer alan zararın giderilmesini talep etme hakkı da dâhil olmak üzere her türlü yasal yolun kullanılabilmesi imkânı açıkça tanınmalıdır.</p> <p>BŞK metninde, tüm bu haklar yer almalıdır. Şirketler bunu, söz konusu hakların düzenlendiği BŞK hükümlerine/bölümlerine/pa rçalarına atıfta bulunmak veya ilgili kişilerin hakları kısmında hepsini listelemek suretiyle yapabilirler.</p> <p>Bu haklar, eğitim ve farkındalık çalışmaları, uyumluluk denetimi,</p>	
--	--	--	---	--

				BŞK'nin uygulanması konusunda görevli personel, kuralların güncellenmesi mekanizması gibi kurum içi mekanizmalarla ilgili olan BŞK düzenlemelerini kapsamaz.	
1.4. Grubun Türkiye'de yerleşik merkezi, kişisel verilerin korunması konusunda yetkilendirilmiş Türkiye'de yerleşik bir Grup üyesi veya veri aktaran veri sorumlusunun BŞK den kaynaklanan tazminatın ödenmesi ve ihlallerin giderilmesi konusundaki yükümlülüğünü kabul etmesi	EVET	EVET	6698 sayılı Kanun m. 11/1/ğ, 12/2, 14/3, 17	<p>Grubun Türkiye'de yerleşik merkezi veya Grubun merkezi Türkiye'de değil ise kişisel verilerin korunması konusunda yetkili ve Türkiye'de yerleşik bir Grup üyesinin, ülke dışında bulunan ve BŞK ile bağlı olan diğer Grup üyelerinin eylemlerinin düzeltilmesi için gerekli girişimlerde bulunması ve BŞK'nin ihlal edilmesinden kaynaklanacak maddi veya manevi zararların giderilmesi için tazminat ödemesi konusunda BŞK de bir yükümlülük bulunmalıdır.</p> <p>BŞK'de şu hususlar açıkça belirtilmelidir; Türkiye dışındaki bir BŞK üyesi BŞK'yi ihlal ederse, bu konuda yetki Türkiye'deki mahkemeler ve yetkili makamlarda olacaktır. İlgili kişinin, sanki ihlal yurtdışında değil Türkiye'de gerçekleşmiş gibi sorumluluk ve yükümlülüğü kabul etmiş olan BŞK üyesine karşı hak ve tazminatlarını talep etme yetkisi olacaktır.</p> <p>Tüm sorumluluğun belirli bir kişi tarafından üstlenilmesinin mümkün olmadığı kurumsal yapıya sahip bir Grup bakımından, özellikle Türkiye dışındaki herhangi bir BŞK ihlali durumunda, bir diğer seçenek olarak;</p> <p>Türkiye'de kurulu bir BŞK üyesinden veriyi alan,</p>	

				Türkiye dışında kurulu bir BŞK üyesi tarafından meydana getirilecek tüm ihlaller bakımından her bir BŞK üyesinin sorumlu olması sağlanabilir.	
1.5. Şirketin yeterli malvarlığının bulunması	HAYIR	EVET		Başvuru formu, BŞK ile bağlı Türkiye dışında kurulu bulunan diğer üyelerin fiilleri bakımından sorumluluğu kabul eden tüm BŞK üyelerinin, BŞK'nin ihlalinden kaynaklanan zararların tazmini için yeterli varlığa sahip olduğu yönünde bir taahhüt içermelidir.	
1.6. İspat yükünün bireysel değil şirket üzerinde olması	EVET	EVET	6698 sayılı Kanun m. 9/2-9/4	BŞK ile; ilgili kişi tarafından iddia edilen zararların yurt dışında bulunan üyeden kaynaklanıp kaynaklanmadığı konusunda, sorumluluğu alan BŞK üyesinin ispat külfetini kabul ettiği açıkça düzenlenmelidir. Sorumluluğu kabul eden BŞK üyesi, yurt dışındaki üyenin zarara yol açacak olayda sorumluluğu olmadığını kanıtlayabilirse kendisi de sorumlu olmaktan kurtulacaktır.	
1.7. İlgili kişilerin BŞK'ye kolay erişimi ve şeffaflığın sağlanması	EVET	HAYIR	6698 sayılı Kanun m. 10, 11,, 10/03/2018 tarih ve 30356 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve	İlgili kişi haklarından yararlanan kişilere, 6698 sayılı Kanun md. 11 ile düzenlenen hakları ve md. 10 ile düzenlenen veri sorumlusunun aydınlatma yükümlülüğü kapsamında yer alan hususlar başta olmak üzere kişisel verilerinin işlenmesiyle ilgili hakları, bu hakların kullanımı, sorumluluk, genel ilkeler konularında kapsamlı bir bilgilendirme sağlanmalıdır. Bağlayıcı Şirket Kuralları, her bir ilgili kişinin bu haklarına kolayca	

			Esaslar Hakkında Tebliğ	erişim hakkını içermelidir. Örneğin, Bağlayıcı Şirket Kurallarının ilgili kişileri ilgilendiren kısımlarının internet üzerinden yayımlanması gibi.	
2. ETKİLİ UYGULAMA					
2.1. Uygun eğitim ve farkındalık çalışmalarının bulunması	EVET	EVET	6698 sayılı Kanun m. 9, 12, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)	BŞK'nin, kişisel verilere sürekli veya düzenli erişime sahip olan, veri toplamaya dâhil olan veya kişisel verileri işlemek için kullanılan araçların geliştirilmesinde çalışan personele uygun eğitim programını içermesi gerekir. BŞK başvurusunu değerlendirecek olan Kurul, başvuru prosedürü sırasında eğitim programının örneklerini ve açıklamalarını isteyebilir. Eğitim programı başvuruda açıkça belirtilmelidir.	
2.2. Şikâyet mekanizmasının bulunması	EVET	EVET	6698 sayılı Kanun m. 13, 10/03/2018 tarih ve 30356 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Veri Sorumlusunun Başvuru Usul ve Esasları Hakkında Tebliğ	Herhangi bir ilgili kişinin kendi haklarını kullanabilmesi ve herhangi bir BŞK üyesi hakkında başvuruda bulunabilmesini sağlayacak dâhili bir şikâyet yönetimi süreci kurulmalıdır. Şikâyet kapsamında ilgili kişilerin talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde sonuçlandırılır. Başvuru formunda, şikâyet sisteminin uygulanma aşamaları hakkında ilgili kişilerin nasıl bilgilendirileceği açıklanmalıdır. Özellikle: Başvurunun nereye ve hangi formatta yapılacağı, Cevabın gecikmesi ile ilgili durumlar,	

				<p>Başvurunun reddedilmesi durumunda ortaya çıkacak sonuçlar,</p> <p>Başvuru hakkı bulunduğu ortaya çıkacak sonuçlar,</p> <p>İlgili kişinin verilen cevabı yetersiz bulması durumunda ortaya çıkacak sonuçlar (Kurula şikâyet, mahkemeler nezdinde hak talebi)</p>	
2.3.Uyumluluk denetiminin bulunması	EVET	EVET	6698 sayılı Kanun m. 9, 12/3	<p>BŞK, taahhüt edilen kurallara uygun hareket edilmesini sağlamak üzere düzenli olarak denetim yapılması/yaptırılması ve bu denetimi kimlerin yapacağı gibi konularda açıklamalar içermelidir.</p> <p>Uyumluluk denetim programı, düzeltici faaliyetlerin gerçekleşmesini sağlayacak yöntemler de dâhil olmak üzere BŞK'yi tüm yönleri ile kapsmalıdır. Ayrıca BŞK'de, denetim sonuçlarından Grup üyelerinin ilgili birim ve çalışanlarının haberdar edilmesi ile ilgili hususlar belirtilmelidir. Uygun durumlarda sonuçtan genel merkez yönetim birimi de haberdar edilir.</p> <p>BŞK'de, Kurumun talebi halinde denetim sonuçlarına erişme yetkisi ve Kuruma gerekli durumlarda herhangi bir BŞK üyesi üzerinde denetim yapma yetkisi tanınmalıdır.</p> <p>Başvuru formunda uyumluluk denetim sistemine ilişkin açıklamalar bulunmalıdır. Örneğin;</p> <ul style="list-style-type: none"> - BŞK ye uyumu denetlemek için hangi mekanizmaların kullanılacağı, - BŞK ye uyumluluğu denetlemek üzere kimlerin 	

				<p>görevlendirildiği, bunların görev ve sorumlulukları (hangi birimin denetim programına/planına karar vereceği, hangi birimin denetimi gerçekleştireceği, denetimin zamanı, denetimin kapsamı (uygulamalar, bilgi teknolojileri sistemleri, kişisel verileri işleyen veri tabanları, ileriye dönük transferler, yasaların BŞK ile uyumsuzluk gösterdiği hallerde alınacak önemli kararlar vb., denetimin sonuçlarını hangi birimin alacağı gibi))</p> <p>- Uyumluluk denetimi mekanizmalarının belirli aralıklarla gözden geçirilmesini/güncellenmesini sağlayacak düzenlemelerin olup olmadığı,</p> <p>- Belirli aralıklarla, şeffaf ve açık bir raporlama yapıp yapılmayacağı.</p>	
2.4. BŞK'nin Uygulanması Konusunda Görevli Personel yapılanmasının bulunması	EVET	HAYIR		<p>Tüm Grup bakımından BŞK'ye uyumun sağlanması ve bunun takibi için görevlendirilmiş uygun bir personel yapılanması bulunmalıdır. Uyumun takibini yapacak kişi veya birim yüksek dereceli yöneticiler tarafından desteklenmelidir.</p> <p>Bu görevliler, en yüksek yönetici kademesine doğrudan rapor verebilmelidir. BŞK' de bu personel yapılanmasının oluşumu, görev ve sorumlulukları gibi hususlar açıklanmalıdır. Söz konusu personel, üst yönetimi bilgilendirir ve tavsiyede bulunur, yetkili denetim otoritesinin incelemeleriyle ilgilenir, uyumluluğu izler ve grup düzeyinde yıllık olarak raporlar.</p>	

3. KURUM İLE KOORDİNASYON					
3.1. Kurum ile koordine çalışma görevi	EVET	EVET	6698 sayılı Kanun m. 9	Bağlayıcı Şirket Kuralları, gerekmesi halinde tüm üyelerin Kurum tarafından denetlenmesini ve bu kurullarla ilgili herhangi bir konuda Kurum'un tavsiyelerine uymayı kabul ettiğini içeren açık bir yükümlülük içermelidir.	
4. KİŞİSEL VERİLERİN İŞLENMESİ VE AKTARILMASI					
4.1. BŞK'nin içeriği hakkında açıklama	EVET	EVET	6698 sayılı Kanun m. 9/4	BŞK, üçüncü ülkelerde yürütülen işlemlerin uyumlu olup olmadığının Kurum tarafından değerlendirilmesini sağlamak üzere Kurulların kapsamı ve aktarımların genel bir tanımını içermelidir. BŞK; aktarıma konu kişisel verinin niteliği (genel/özel nitelikli kişisel veri), veri kategorileri (kimlik, iletişim, lokasyon, özlük gibi), aktarım amaçları ve süreleri, veri konusu kişi grubu veya grupları (çalışan, stajyer, ziyaretçi, ürün veya hizmet alan kişi gibi), veri aktarımının hangi yöntemle gerçekleştirileceği, veri aktarımının hukuki sebebi/sebepleri, aktarılacak verilerin grup içerisindeki dağılımı (ilgili Grup üyelerinin adı ve iletişim bilgilerini belirterek), sonraki aktarımlar gibi hususları içermelidir.	
4.2. BŞK'lerin yer bakımından kapsamı hakkında açıklama	EVET	EVET		BŞK'de, her bir grup üyesi dâhil olmak üzere grubun yapısı ve iletişim bilgileri açıkça belirtilmelidir.	

4.3. BŞK ile bağlı yapılar	HAYIR	EVET	6698 sayılı Kanun m. 9, 12	Grubun tanımlanmış bir temas kişinin, BŞK ile bağlı olan şirketlerin/varlıkların (iletişim bilgileri dâhil olmak üzere) tamamen güncellenmiş bir listesini tutma ve listede değişiklik yapılması durumunda Kurumu ve ilgili kişileri bilgilendirme yükümlülüğü konusunda bu kılavuzdaki madde 5.1'e bakınız.	
5. RAPORLAMA VE KAYIT DEĞİŞİKLİĞİ MEKANİZMALARI					
5.1. BŞK'ye ilişkin değişikliklerin raporlanması, kaydedilmesi ve bunların Kuruma bildirilmesi	EVET	EVET	6698 sayılı Kanun m. 9	<p>BŞK değiştirilebilir/güncellenebilir ancak değişikliklerin gecikmeksizin tüm BŞK üyelerine ve Kuruma bildirilmesi konusunda bir yükümlülük öngörülmelidir.</p> <p>Bununla birlikte aşağıdaki durumlarda tekrar bildirim yapmaya gerek bulunmamaktadır:</p> <p>Belirli bir kişi veya ekip/birim, BŞK üyelerinin tam ve güncel bir listesi ile kurallardaki güncellemelere dair kayıtları tutar, ilgili kişilere ve Kuruma talep üzerine gerekli bilgileri sağlar.</p> <p>Yeni Grup üyesine, BŞK'ye bağlılığı ve uyumu tam olarak sağlayıncaya kadar herhangi bir kişisel veri aktarımı yapılmaz.</p> <p>BŞK veya BŞK üyelerindeki herhangi bir değişiklik, güncellemeyi haklı kılan sebeplerin kısa bir açıklamasıyla birlikte Kuruma yılda bir kez bildirilir.</p> <p>BŞK'nin sunduğu koruma seviyesini veya BŞK'yi önemli şekilde etkileyen değişiklikler (bağlayıcılık niteliğini etkileyen</p>	

				değişiklikler gibi) derhal Kuruma bildirilir.	
6. VERİ GÜVENLİĞİ					
6.1 Türkiye'den aktarım ya da sonraki aktarımları kapsar şekilde veri koruma ilkelerine ilişkin bir açıklama	EVET	EVET	6698 sayılı Kanun m. 4, 9/4 c, d, md. 12	<p>BŞK açıkça şirket tarafından izlenecek aşağıdaki hususları içermelidir:</p> <p>Hukuka ve dürüstlük kurallarına uygun olma (6698 sayılı Kanun m. 4/2/a)</p> <p>Doğru ve gerektiğinde güncel olma (6698 sayılı Kanun m. 4/2/b)</p> <p>Belirli, açık ve meşru amaçlar için işleme (6698 sayılı Kanun m.4/2/c)</p> <p>İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma (6698 sayılı Kanun m. 4/2/ç)</p> <p>İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza etme (6698 sayılı Kanun m. 4/2/d)</p> <p>Özel kategorideki kişisel verilerin işleme</p> <p>Güvenlik; idari ve teknik tedbirler alınacaktır. Grup içerisindeki kişisel veri işleme faaliyetleri kapsamında veri işleyenlere yapacak aktarımlar bakımından, veri işleyenlerin BŞK ile öngörülen teknik ve idari tedbirlere uygun hareket etmeleri sağlanmalıdır.</p> <p>Ayrıca, bu teknik ve idari tedbirler herhangi bir kişisel veri ihlali durumunda şirketin Türkiye'de bulunan genel merkezine veya kişisel verilerin korunması konusunda yetkili Türkiye'de bulunan BŞK</p>	

				<p>üyelerine ve ilgili veri koruma birimi ile hak ve özgürlüklerinin ihlalden etkilenme riski bulunan ilgili kişilere gecikmeksizin bildirimde bulunma yükümlülüğünü de içermelidir.</p> <p>Tüm kişisel veri ihlalleri (kişisel veri ihlaliyle ilgili olaylar, etkileri ve yapılan müdahaleleri içerecek şekilde) belgelenmeli ve ilgili dokümanlar istenmesi halinde Kuruma sunulmalıdır.</p> <p>Grubun bir parçası olmayan veri işleyenlere ve veri sorumlularına yapılan aktarımlar ve sonraki aktarımlar üzerindeki kısıtlamalar (Veri sorumlusu olan BŞK üyelerinin, Türkiye dışında kurulu bulunan grubun dışındaki veri işleyenlere/veri sorumlularına veri aktarabilmeleri için 6698 sayılı Kanun m. 9 kapsamında yeterli bir korumanın sağlanmış olması gerekmektedir).</p> <p>BŞK'lerin temel ilkelerinin ifadeleri ve tanımları, 6698 sayılı Kanunun ifadeleri ve tanımları ile uyumlu olmalıdır.</p>	
6.2. Ulusal mevzuatın, grubun BŞK'ye uymasını engellediği durumlarda şeffaflık	EVET	HAYIR	6698 sayılı Kanun m. 9/4 ç	<p>Bir BŞK üyesinin uymakla yükümlü olduğu mevzuatta, şirketin BŞK'deki yükümlülüklerini yerine getirmesini engelleyen veya BŞK ile düzenlenen kuralların uygulanmasını önemli ölçüde etkileyen hükümler varsa, derhal Grubun Türkiye'de yerleşik merkezi veya Türkiye'de yerleşik merkezi yok ise kişisel verilerin korunması</p>	

			<p>konusunda yetkilendirilmiş ve Türkiye’de yerleşik bir Grup üyesi bilgilendirilmelidir.</p> <p>Ayrıca, bir BŞK üyesinin üçüncü bir ülkede tabi olduğu hukuki gerekliliklerin, BŞK’nin sağladığı garantiler üzerinde önemli bir olumsuz etkiye sahip olması durumu da Kuruma bildirilmelidir. Kanunla yetki verilen bir otorite veya milli güvenliği sağlamakla yükümlü bir kurum tarafından kişisel verilerin açıklanmasının istendiği talepler de bu duruma dâhildir. Böyle bir durumda, Kurumun, talep hakkında (talep edilen verilerin ne olduğu, talep edenin kimliği, talebin yasal dayanağı gibi hususlarda bilgi içerecek şekilde) açıkça bilgilendirilmesi gerekir.</p> <p>Askıya alma ve/veya bildirim yasaklanması gibi belirli durumlar bakımından BŞK’ler; BŞK üyesinin, mümkün olan en kısa sürede ve olabildiğince fazla bilgi vermek üzere bu yasaktan feragat etme hakkını elde etmek üzere elinden gelen çabayı göstereceği ve bunu ispat edeceğine ilişkin hüküm içermelidir.</p> <p>Eğer, yukarıdaki durumlarda, bilgi talep edilen BŞK üyesi tüm çabasına rağmen Kurumu bilgilendirebilecek bir konumda değilse, kendisine gelen talepler hakkında yıllık olarak Kuruma genel nitelikte bir bilgilendirmeyi (örneğin kişisel verilerin açıklanması için yapılan başvuru sayısı, talep edilen veri türü, mümkünse talep</p>	
--	--	--	--	--

				<p>sahibi vb.) sağlamayı BŞK'de taahhüt etmelidir.</p> <p>Her durumda BŞK'lerin şunu belirtmesi gerekir; Bir BŞK üyesi tarafından kişisel verilerin herhangi bir kamu otoritesine aktarılması, demokratik bir toplumda gerekli olanın ötesine geçecek şekilde büyük, orantısız ve rastgele şekilde yapılamaz.</p>	
6.3. Ulusal mevzuat ve BŞK arasındaki ilişkinin açıklanması	HAYIR (ihtiyari)	HAYIR (ihtiyari)		Zorunlu olmamakla birlikte, BŞK ve ilgili meri ulusal mevzuat arasındaki ilişkiyi belirlemek faydalı olacaktır.	
7. HESAP VEREBİLİRLİK VE DİĞER ARAÇLAR					
7.1. Hesap verebilirlik ve diğer araçlar	EVET	EVET	6698 sayılı Kanun m. 12	<p>Her bir veri sorumlusu BŞK'ye uyum göstermekle yükümlü ve sorumludur.</p> <p>Uyumun sağlanabilmesi için BŞK üyelerinin, tüm kategorilerdeki veri işleme faaliyetlerinin elektronik yöntemler de dâhil olmak üzere yazılı şekilde kaydını tutması ve talep halinde Kuruma sunması gerekmektedir.</p> <p>Uyumluluğun artırılması ve gerektiğinde, gerçek kişilerin hak ve özgürlükleri bakımından yüksek risk oluşturması muhtemel olan veri işleme faaliyetleri için risk analizi yapılmalıdır (Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler). Yapılan risk analizine göre, veri sorumlusu tarafından riski hafifletmek için gerekli tedbirlerin alınmamış olması ve veri işlemenin yüksek risk doğuracağına ortaya çıkması durumunda, veri</p>	

				<p>işleme faaliyetinden önce Kuruma danışılmalıdır.</p> <p>Veri koruma ilkelerini uygulamak ve uygulamada BŞK'ler tarafından belirlenen gereksinimlere uyumu kolaylaştırmak için uygun teknik ve idari tedbirler alınmalıdır.</p>	
8. YARDIMCI BİLGİ VE BELGELER					
8.1. Yardımcı bilgi ve belgeler	HAYIR (ihtiyari)	EVET (ihtiyari)		<p>Aşağıdaki hususlarda bilgi verilmesi zorunlu olmamakla birlikte başvurunun değerlendirilmesi bakımından faydalı olacaktır:</p> <p>Aktarımın yapılacağı ülkelerin taraf olduğu, kişisel verilerin korunması konusunda hüküm içeren uluslararası sözleşmelerin, ilgili kısımlara atıf yapılarak, belirtilmesi.</p> <p>Kişisel verinin aktarılacağı ülkede, kişisel verilerin korunması konusunda ulusal mevzuat ile yetkili bir kişisel verileri koruma otoritesinin varlığı ve varsa konuyla ilgili mevzuatı ve uygulamasının kısaca belirtilmesi.</p>	

İDARİ PARA CEZASI TUTARLARI

6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU'NDA DÜZENLENEN İDARİ PARA CEZALARI (TL)

Yıl	Oran %	Aydınlatma yükümlülüğünü yerine getirmeme (Madde 18/A - Aykırılık: Madde 10)		Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi (Madde 18/b - Aykırılık: Madde 12)		Kurul kararlarının yerine getirilmemesi (Madde 18/c - Aykırılık - Madde 15)		Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edilmesi (Madde 18/ç - Aykırılık Madde 16)	
2016	-	5.000	100.000	15.000	1.000.000	25.000	1.000.000	20.000	1.000.000
2017	3.83	5.191	103.830	15.574	1.038.300	25.957	1.038.300	20.766	1.038.300
2018	14.47	5.942	118.854	17.827	1.188.542	29.712	1.188.542	23.770	1.188.542
2019	23.73	7.352	147.058	22.057	1.470.583	36.762	1.470.583	29.410	1.470.583
2020	22.58	9.012	180.263	27.037	1.802.640	45.062	1.802.640	36.050	1.802.640
2021	9.11	9.832	196.684	29.500	1.966.860	49.167	1.966.860	39.334	1.966.860
2022	36.20	13.391	267.883	40.179	2.678.863	66.965	2.678.863	53.572	2.678.863
2023	122.93	29.852	597.191	89.571	5.971.989	149.285	5.971.989	119.428	5.971.989

Bölüm İçeriği

- Law on the Protection of Personal Data
- By-Law On Data Controllers Registry
- By-Law on Erasure, Destruction or Anonymization of Personal Data
- Communiqué on the Principles and Procedures for the Request to Data Controller
- Communiqué on Principles and Procedures to be Followed in Fullfillment of the Obligation to Inform

Law on the Protection of Personal Data

Law Number : 6698

Date of Ratification : 24.3.2016

Official Journal Date : 07.04.2016

Official Journal No : 29677

LAW ON THE PROTECTION OF PERSONAL DATA

CHAPTER ONE

Purpose, Scope and Definitions

Purpose

Article 1 - (1) The purpose of this Law is to protect fundamental rights and freedoms of people, particularly the right to privacy, with respect to processing of personal data and to set forth obligations, principles and procedures which shall be binding upon natural or legal persons who process personal data.

Scope

Article 2 - (1) The provisions of this Law shall apply to natural persons whose personal data are processed as well as to natural or legal persons who process such data fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means.

Definitions

Article 3 - (1) For the purposes of this Law the following definitions shall apply:

- a) Explicit consent: freely given, specific and informed consent,
- b) Anonymizing: rendering personal data impossible to link with an identified or identifiable natural person, even through matching them with other data,
- c) President: President of the Personal Data Protection Authority,
- ç) Data subject: the natural person, whose personal data is processed,

- d) Personal data: all the information relating to an identified or identifiable natural person,
- e) Processing of personal data: any operation performed upon personal data such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means,
- f) Board: the Personal Data Protection Board,
- g) Authority: the Personal Data Protection Authority,
- ğ) Processor: the natural or legal person who processes personal data on behalf of the controller upon his authorization,
- h) Data registry system: the registry system which the personal data is registered into through being structured according to certain criteria,
- i) Controller: the natural or legal person who determines the purpose and means of processing personal data and is responsible for establishing and managing the data registry system.

CHAPTER TWO

Processing of Personal Data

General principles

Article 4 - (1) Personal data may only be processed in compliance with the procedures and principles set forth in this Law and other laws.

(2) The following principles shall be complied within the processing of personal data:

- a) Lawfulness and conformity with rules of bona fides.
- b) Accuracy and being up to date, where necessary.
- c) Being processed for specific, explicit and legitimate purposes.
- ç) Being relevant with, limited to and proportionate to the purposes for which they are processed.
- d) Being retained for the period of time stipulated by relevant legislation or the purpose for which they are processed.

Conditions for processing of personal data

Article 5- (1) Personal data cannot be processed without the explicit consent of the data subject.

(2) Personal data may be processed without seeking the explicit consent of the data subject only in cases where one of the following conditions is met:

a) it is clearly provided for by the laws.

b) it is mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid.

c) processing of personal data belonging to the parties of a contract, is necessary provided that it is directly related to the conclusion or fulfilment of that contract.

ç) it is mandatory for the controller to be able to perform his legal obligations.

d) the data concerned is made available to the public by the data subject himself.

e) data processing is mandatory for the establishment, exercise or protection of any right.

f) it is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

Conditions for processing of personal data of special nature

Article 6- (1) Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data are deemed to be personal data of special nature.

(2) It is prohibited to process the personal data of special nature without explicit consent of the data subject.

(3) Personal data, excluding those relating to health and sexual life, listed in the first paragraph may be processed without seeking explicit consent of the data subject, in the cases provided for by laws. Personal data relating to health and sexual life may only be processed, without seeking explicit consent of the data subject, by any person or authorised public institutions and organizations that have confidentiality obligation, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

(4) It is stipulated that adequate measures determined by the Board are also taken while processing the personal data of special nature.

Erasure, destruction or anonymizing of personal data

Article 7- (1) Despite being processed under the provisions of this Law and other related laws, personal data shall be erased, destroyed or anonymized by the controller, ex officio or upon demand by the data subject, upon disappearance of reasons which require the process.

(2) Provisions of other laws concerning the erasure, destruction or anonymizing of personal data are reserved.

(3) Procedures and principles for the erasure, destruction or anonymizing of personal data shall be laid down through a by-law.

Transfer of personal data

Article 8- (1) Personal data cannot be transferred without explicit consent of the data subject.

(2) Personal data may be transferred without seeking explicit consent of data subject upon the existence of one of the conditions provided for in:

a) the second paragraph of Article 5,

b) the third paragraph of Article 6, provided that sufficient measures are taken.

(3) Provisions of other laws concerning transfer of personal data are reserved.

Transfer of personal data abroad

Article 9- (1) Personal data cannot be transferred abroad without explicit consent of the data subject.

(2) Personal data may be transferred abroad without explicit consent of the data subject provided that one of the conditions set forth in the second paragraph of Article 5 and the third paragraph of Article 6 exist and that;

(a) sufficient protection is provided in the foreign country where the data is to be transferred,

(b) the controllers in Turkey and in the related foreign country guarantee a sufficient protection in writing and the Board has authorized such transfer, where sufficient protection is not provided.

(3) The Board determines and announces the countries where sufficient level of protection is provided.

(4) The Board shall decide whether there is sufficient protection in the foreign country concerned and whether such transfer will be authorised under the sub-paragraph (b) of second paragraph, by evaluating the followings and by receiving the opinions of related public institutions and organizations, where necessary:

a) the international conventions to which Turkey is a party,

- b) the state of reciprocity concerning data transfer between the requesting country and Turkey,
 - c) the nature of the data, the purpose and duration of processing regarding each concrete, individual case of data transfer,
 - ç) the relevant legislation and its implementation in the country to which the personal data is to be transferred,
 - d) the measures guaranteed by the controller in the country to which the personal data is to be transferred,
- (5) In cases where interest of Turkey or the data subject will seriously be harmed, personal data, without prejudice to the provisions of international agreements, may only be transferred abroad upon the permission to be given by the Board after receiving the opinions of related public institutions and organizations.
- (6) Provisions of other laws concerning the transfer of personal data abroad are reserved.

CHAPTER THREE

Rights and Obligations

Obligation of Controller to Inform

Article 10- (1) Whilst collecting personal data, the controller or the person authorised by him is obliged to inform the data subjects about the following:

- a) the identity of the controller and of his representative, if any,
- b) the purpose of data processing;
- c) to whom and for what purposes the processed data may be transferred,
- ç) the method and legal reason of collection of personal data,
- d) other rights referred to in Article 11.

The Rights of Data Subject

Article 11- (1) Each person has the right to apply to the controller and

- a) to learn whether his personal data are processed or not,
- b) to request information if his personal data are processed,
- c) to learn the purpose of his data processing and whether this data is used for intended purposes,

- c) to know the third parties to whom his personal data is transferred at home or abroad,
- d) to request the rectification of the incomplete or inaccurate data, if any,
- e) to request the erasure or destruction of his personal data under the conditions laid down in Article 7,
- f) to request notification of the operations carried out in compliance with sub-paragraphs (d) and (e) to third parties to whom his personal data has been transferred,
- g) to object to the processing, exclusively by automatic means, of his personal data, which leads to an unfavourable consequence for the data subject,
- ğ) to request compensation for the damage arising from the unlawful processing of his personal data.

Obligations concerning data security

Article 12- (1) The controllers are obliged to take all necessary technical and administrative measures to provide a sufficient level of security in order to:

- a) prevent unlawful processing of personal data,
- b) prevent unlawful access to personal data,
- c) ensure the retention of personal data.

(2) In case of the processing of personal data by a natural or legal person on behalf of the controller, the controller shall jointly be responsible with these persons for taking the measures laid down in the first paragraph.

(3) The controller shall be obliged to conduct necessary inspections, or have them conducted in his own institution or organization, with the aim of implementing the provisions of this Law.

(4) The controllers and processors shall not disclose the personal data that they learned to anyone in breach of this Law, neither shall they use such data for purposes other than processing. This obligation shall continue even after the end of their term.

(5) In case the processed data are collected by other parties through unlawful methods, the controller shall notify the data subject and the Board within the shortest time. Where necessary, the Board may announce such breach at its official website or through other methods it deems appropriate.

CHAPTER FOUR

Application, Complaint and Registry

Application to the Controller

Article 13- (1) The data subject shall lodge an application in writing to the controller about his demands concerning the implementation of this Law or via other methods specified by the Board.

(2) The data controller shall conclude the demands involved in the applications within the shortest time possible depending on the nature of the demand and within thirty days at the latest and free of charge. However if the action in question incurs another cost, the price set by the Board may be collected.

(3) The data controller shall accept the application or decline it on justified grounds and communicate its response to data subject in writing or in electronic media. If the demand involved in the application found admissible, it shall be indulged by the data controller. Data subject shall be reimbursed for the application fee provided that the application has been lodged due to a mistake made by the controller.

Complaint to the Board

Article 14- (1) If the application is declined, the response is found unsatisfactory or the response is not given in due time, the data subject may file a complaint with the Board within thirty days as of he learns about the response of the controller, or within sixty days as of the application date, in any case.

(2) A complaint cannot be filed before exhausting the remedy of application to the controller under Article 13.

(3) The right to compensation under general provisions of those whose personal rights are violated is reserved.

Procedures and principles of examination ex officio or upon complaint

Article 15- (1) The Board shall make the necessary examination in the matters falling within its scope of work upon complaint or ex officio, where it learnt about the alleged violation.

(2) The notices and complaints not meeting the requirements laid down in Article 6 of the Law No. 3071 of 1/11/1984 on the Use of Right to Petition shall not be examined.

(3) Except for the information and documents having the status of state secret, the controller shall be obliged to communicate within fifteen days the information and documents related to the subject of examination which the Board has requested, and shall enable, where necessary, on-the-spot examination.

(4) The Board shall finalise the examination upon complaint and give an answer to data subjects. In case the Board fails to answer the data subject's application in sixty days as of the application date, it is deemed rejected.

(5) Following the examination made upon complaint or ex officio, in cases where it is understood that an infringement exists, the Board shall decide that the identified infringements shall be remedied by the relevant controller and notify this decision to all it may concern. This decision shall be implemented without delay and within thirty days after the notification at the latest,

(6) Following the examination made upon complaint or ex officio, in cases where it is determined that the infringement is widespread, the Board shall adopt and publish a resolution in this regard. Before adopting the resolution, the Board may also refer to the opinions of related institutions and organisations, if needed.

(7) The Board may decide that processing of data or its transfer abroad should be stopped if such operation may lead to damages that are difficult or impossible to recover and if it is clearly unlawful.

Registry of Controllers

Article 16- (1) The Presidency shall maintain a publicly accessible Registry of Controllers under the supervision of the Board.

(2) Natural or legal persons who process personal data shall be obliged to enrol in the Registry of Data Controllers before proceeding with data processing. However, by taking into account the objective criteria set by the Board such as the nature and quantity of the data processed, the legal requirement for data processing, or transferring the data to third parties, the Board may provide exception to the obligation of enrolment in the Registry of Data Controllers.

(3) Application for enrolling in the Registry of Data Controllers shall be made with a notification including:

- a) identity and address of the controller and of his representative, if any,
- b) purposes for which the personal data will be processed,
- c) explanations about group(s) of personal data subjects as well as about the data categories belonging to these people,
- ç) recipients or groups of recipients to whom the personal data may be transferred,
- d) personal data which is envisaged to be transferred abroad,

e) measures taken for the security of personal data.

(f) maximum period of time required for the purpose of the processing of personal data.

(4) Any changes in the information provided under the third paragraph shall be immediately notified to the Presidency

(5) Other procedures and principles governing the Registry of Data Controllers shall be laid down through a by-law.

CHAPTER FIVE

Crimes and Misdemeanours

Crimes

Article 17- (1) Articles 135-140 of Turkish Penal Code No. 5237 of 26/9/2004 shall apply in terms of the crimes concerning personal data.

(2) Those who fail to erase or anonymize personal data in breach of Article 7 herein shall be punished under Article 138 of the Law No. 5237.

Misdemeanours

Article 18- (1) For the purposes of this Law;

a) those who fail to comply with obligation to inform provided for in Article 10 herein shall be required to pay an administrative fine of 5.000 to 100.000 TL,

b) those who fail to comply with obligations related to data security provided for in Article 12 herein shall be required to pay an administrative fine of 15.000 to 1.000.000 TL,

c) those who fail to comply with the decisions issued by the Board under Article 15 herein shall be required to pay an administrative fine of 25.000 to 1.000.000 TL,

ç) those who fail to meet the obligations for enrolling in the Registry of Data Controllers and making a notification as provided for in Article 16 herein shall be required to pay an administrative fine of 20.000 to 1.000.000 TL.

(2) The administrative fines listed in this article shall be applicable to natural persons and private law legal persons who are controllers.

(3) Should the acts listed in the first paragraph be committed within the public institutions and organizations as well as professional associations having the status of public institution, disciplinary procedures shall be applied to the civil servants and other public officers employed in the relevant

public institutions and organisations and those employed in the professional associations having the status of public institution upon a notice by the Board and the result is communicated to the Board.

CHAPTER SIX

Personal Data Protection Authority and its Organization

Personal Data Protection Authority

Article 19- (1) Personal Data Protection Authority which is a public law body with public law legal personality having administrative and financial autonomy has been established to carry out duties provided by this Law

(2) The Authority is affiliated to the office of the Prime Minister

(3) The Headquarters of the Authority is in Ankara

(4) The Authority is composed of the Board and the Presidency. Decision making body of the Authority is the Board.

Duties of the Authority

Article 20 - (1) The duties of the Authority are as follows;

(a) to follow the latest developments in the legislation and practices, make evaluations and recommendations, conduct researches and analyses or have them conducted within its field of duty.

(b) to cooperate with public institutions and organisations, NGOs, professional associations or universities within its field of duty, if needed.

(c) to follow and evaluate the latest international developments on personal data; and within its field of duty cooperate with international organisations and participate to the meetings

(ç) to submit its annual activity report to the office of the President of Turkish Republic, the Committee on Human Rights Inquiry of Grand National Assembly of Turkey and office of the Prime Minister.

(d) to carry out other duties provided by laws.

Personal Data Protection Board

Article 21 - (1) The Board shall perform and exercise the duties and powers conferred on it by this law and other laws, independently and under its own responsibility. No body, authority, office or person shall give orders and instructions, recommendations or suggestions to the Board on matters falling within the scope of its duties and powers.

(2) The Board is composed of nine members. Five members of the Board shall be elected by the Grand National Assembly of Turkey, two members shall be elected by the President of Turkey and two members shall be elected by the Council of Ministers.

(3) The following conditions shall be met in order to be elected for the Board:

- a) Being informed on and being experienced in the issues falling within Authority's field of duty.
- b) Complying with the requirements set forth in points (1), (4), (5), (6) and (7) of sub-paragraph (A) of first paragraph of Article 48 of the Public Servants Law No. 657 of 14/7/1965.
- c) Not being a member of any political party.
- ç) Having been graduated from at least a four-year graduate program.
- d) Having been employed in public institutions and organisations, international organisations, non-governmental organisations, or professional associations having the status of public institution or in the private sector for at least ten years in total.

(4) Those who are elected for the membership should express their consent. Elections are held so as to pluralistical representation of those who are informed on and experienced in the issues falling within Authority's field of duty.

(5) Board members shall be elected by the Grand National Assembly of Turkey on the basis of the following procedure:

- a) Persons twice as many as the number of members to be determined in proportion to the number of deputies of political party groups shall be nominated for election and the members of the Board shall be elected by the Plenary of the Grand National Assembly from among these candidates on the basis of the number of deputies allocated to each political party. However, political party groups shall not negotiate or decide whom to vote for in the elections to be held in the Grand National Assembly of Turkey.
- b) The Board members shall be elected within ten days after the designation and announcement of the candidates. For the candidates designated by the political party groups, a composite ballot in the form of separate lists shall be prepared. Voting shall be cast by ticking of the specific space across the names of the candidates. The votes casted more than the numbers of the members to be elected for the Board from the political party quotas, determined in accordance with paragraph two, shall be deemed invalid.

c) Provided that the quorum is ensured, candidates the number of whom corresponds to the number of vacancies and who take most of the votes shall be deemed to have been elected.

ç) The election for the renewal of the members shall be held two months before the expiration of their term of office; should there be a vacancy in the memberships for any reason, there shall be an election within one month as of the date of vacancy; or if the date of vacancy coincides with the recess of the Grand National Assembly of Turkey, the election shall take place within one month from the end of the recess, by employing the same procedure. During these elections, the allocation of the vacant memberships to the political party groups shall be made by considering the number of the elected members from the political party groups' quotas in the first election and the current proportions of the political party groups.

(6) Forty-five days before the expiration of the term of office or in case of expiration of term of office by any reason of the members elected by the President of Turkey or the Council of Ministers, the Authority shall notify the situation in fifteen days to the office of the Prime Minister so as to be submitted to the office of the President of Turkey or the Council of Ministers; A new election shall take place one month before the expiration of term of office of the members. Should there be a vacancy in these memberships before the expiration of term of office, there shall be an election within fifteen days as of the date of notification.

(7) The Board shall designate the Head and the Second Head of the Board among its members. The Head of the Board is also the President of the Authority.

(8) Term of office of the Board members is four years. Members may be re-elected after expiration of their term of office. The person who is elected instead of the member whose post ends before the expiration of his/her term of office for any reason, shall complete the remaining term of office.

(9) Members of the Board shall take the following oath before Court of Cassation's Board of First Presidency: "I do solemnly swear on my honour and on my dignity that I will carry out my duties with absolute impartiality, bona fides, fairness and with sense of justice in line with the Constitution and the relevant legislation." Application to Court of Cassation for oath taking is deemed to be one of the pressing matters.

(10) Unless provided for by a specific law, the members shall not assume any public or private tasks other than those related with carrying out their official duties in the Board; shall not act as executives in associations, foundations, cooperatives and in similar bodies; shall not engage in commercial activities, shall not engage in self-employment, shall not act as arbitrators and expert witnesses.

However, Board members may prepare scientific publications, give lectures and attend conferences so as not to hinder their primary duties, and may receive copyrights and fees associated with those.

(11) Investigations into the claims about the crimes allegedly committed by the members in connection with their duties shall be conducted as per the Law No. 4483 of 2/12/1999 on Adjudication of Public Servants and Other Public Employees, and permission for investigation shall be granted by the Prime Minister.

(12) Provisions of the Law No. 657 shall apply to disciplinary investigations and prosecutions about the members of the Board.

(13) Members shall not be removed from their office by any reason before the expiration of their term of office. However, members of the Board may be removed from office by the Board decision if:

- a) it is found out subsequently that they do not meet the conditions required for their election,
- b) the verdict, which is rendered for crimes committed by them in connection with their duties, becomes final
- c) a medical report is issued by board of health to certify that they are not suitable for office,
- ç) it is ascertained that they were absent from work for fifteen consecutive days or for a total of thirty days within a year, without legitimate permission and excuse.
- d) it is ascertained that they fail to attend three Board meetings in one month and ten Board meetings in one year without any permission and excuse.

(14) Those who are appointed as the members of the Board shall be removed from their previous posts during their term of office in the Board. On the condition that they do not fail to meet the requirements of being employed as a civil servant, those who are assigned as Board members whilst on duty shall be appointed to posts that are appropriate for their vested positions and titles in one month, in case their term of office ends or they express their will to resign and lodge an application in this regard to their former institution within thirty days. Until the assignment, Authority shall continue to make any payment they are vested with. Until they take another post or take up another employment, Authority shall continue to make the payment of those who are appointed as Board members despite not being public servants and whose term of office terminated as stated hereinabove; and the payments to be made under this scope shall not exceed three months. With regard to personal and other rights, terms spent in the Authority shall be deemed to have spent in the previous institutions or organisations.

Duties and powers of the Board

Article 22 - (1) Duties and powers of the Board are as follows:

- a) to ensure that the personal data are processed in compliance with fundamental rights and freedoms.
- b) to conclude the complaints of those claiming that their rights with regard to personal data protection have been violated.
- c) to examine whether the personal data are processed in compliance with the laws, upon complaint, or ex officio where it learnt about the alleged violation, and to take temporary measures, if necessary.
- ç) to determine the adequate measures which are necessary for the processing of the data of special nature.
- d) to ensure that Registry of Controllers is maintained.
- e) to draft regulatory acts on the matters concerning the Board's field of duty and operation of the Authority.
- f) to draft regulatory acts in order to lay out the liabilities concerning data security.
- g) to draft regulatory acts on the matters concerning duties, powers and responsibilities of the Controller and of his representative.
- ğ) to decide on the administrative sanctions provided for in this Law.
- h) to deliver its opinion about the legislation drafted by other institutions or organizations that contain provisions on personal data.
- i) to conclude the Strategic Plan of the Authority; to determine the purpose, targets, service quality standards and performance criteria of the Authority.
- ii) to discuss and decide on Strategic Plan and the budget proposal of the Authority which are prepared in compliance with its purposes and targets.
- j) to approve and publish the draft reports on the performance, financial situation, annual activities and other matters related with the Authority.
- k) to discuss and decide on the recommendations as regards the purchase, sale and lease of immovable properties.
- l) to carry out other tasks provided for by laws.

Working Principles of the Board

Article 23 - (1) Head of the Board shall determine the dates and agenda of the meetings. The Board may be called for an extraordinary meeting by the Head, if necessary.

(2) The Board shall convene at least with six members, including the Head of the Board, and shall take decisions by simple majority of its total members. Members of the Board shall not cast abstaining vote.

(3) Members shall not attend and cast vote in meetings, which concern issues regarding themselves, their relatives by blood up to third degree and relatives by affinity of marriage up to second degree, their adopted children and their spouses even if the marriage has ended.

(4) Members of the Board shall not disclose the secrets they learned as to data subjects and third parties during their work to anyone other than legally authorized bodies, neither shall they use such secrets for their benefits. This obligation shall apply even after the end of their term of office.

(5) The outcome of the agenda of the Board shall be written down. The decisions and dissenting opinions, if any, shall be written within 15 days at the latest. The Board shall announce to public the decisions it deems necessary.

(6) The meetings of the Board are confidential unless decided otherwise

(7) Working procedures and principles of the Board and the writing procedure of the decisions and other issues shall be laid down through a by-law.

The President

Article 24 - (1) The President, as the head of both the Authority and the Board, is the highest-level official of the Authority, and organises and conducts the services of the Authority in accordance with the legislation, Authority's purpose and policies, Strategic Plan, performance criteria and service quality standards, and , ensures coordination between service units, as well.

(2) The President is responsible for the general management and representation of the Authority. This responsibility entails the duties and powers concerning regulation, execution, inspection, evaluation of Authority's work and, its announcement to the public, when necessary.

(3) The duties of the President are as follows;

a) to chair the Board's meetings.

b) to ensure the notification of Board decisions and public announcement of these when deemed necessary by the Board, and to monitor their implementation.

- c) to appoint Deputy President, Heads of Departments and Authority's personnel.
 - ç) to finalize the recommendations communicated by service units and submit them to the Board.
 - d) to ensure the implementation of the Strategic Plan and to establish the human resources and working policies in line with service quality standards.
 - e) to prepare the annual budget and financial tables of the Authority in line with the determined strategies, annual purposes and targets.
 - f) to ensure coordination in order for the Board and service units to work in harmony in an efficient, disciplined and well-ordered manner.
 - g) to maintain the relations of the Authority with other institutions.
 - ğ) to determine the scope of the duties and powers of the personnel authorized to sign on behalf of the President.
 - h) to carry out other duties related to the management and operation of the Authority
- (4) The Second President is entitled to act on behalf of the President in his absence.

Composition and Duties of the Presidency

Article 25 - (1) The Presidency is composed of Deputy President and service units. The Presidency shall fulfill the duties listed in paragraph four through the service units which are organized as departments. The number of departments shall not be more than seven.

(2) A Deputy President shall be appointed by the President in order to assist him in his administrative duties.

(3) The Deputy President and Heads of Departments shall be appointed by the President among those who have been graduated from at least a four-year higher education institution and worked in the public institutions for at least ten years.

(4) The duties of the Presidency are as follows,

- a) to maintain the Registry of Controllers.
- b) to carry out clerical services for the Authority and the Board.
- c) to represent the Authority through lawyers at the lawsuits and execution proceedings to which the Authority is a party; to follow up such lawsuits or have them followed up and carry out the legal services.

- ç) to carry out personnel-related services of the Board members and Authority's personnel.
 - d) to perform the duties foreseen by laws with regard to financial services and strategy development units.
 - e) to ensure that the information systems are established and used in order to carry out acts and actions of the Authority.
 - f) to draft reports on the annual activities of the Authority or on other issues which are deemed necessary, and submit them to the Board.
 - g) to draft the Strategic Plan of the Authority.
 - ğ) to determine the personnel policy of the Authority, prepare and implement the education and career-based plans for the personnel.
 - h) to carry out the appointment, transfer, discipline, performance, promotion, retirement and other similar procedures regarding the personnel.
 - ı) to determine the ethical principles for the personnel and give necessary training.
 - ı) to carry out the services with regard to purchasing, leasing, maintenance, repair, construction, archive, health and social issues and similar ones within the framework of the Public Financial Management and Control Law No. 5018 of 10/12/2003.
 - j) to keep record of the movable and immovable property of the Authority
 - k) to fulfill other duties conferred on it by the Board or the President.
- (5) Service units and their working procedures and principles shall be laid down through a by-law which is put into force by the Council of Ministers upon Authority's proposal drafted as per the field of activity, duties and powers stated in the Law herein.

The Personal Data Protection Experts and the Assistant Experts

Article 26 - (1) The Personal Data Protection Experts and the Assistant Experts may be recruited by the Authority. The experts and assistant experts who are appointed as Personal Data Protection Expert within the framework of additional Article 41 of the Law No. 657 shall receive one extra grade for once only.

Provisions on the Personnel and Personnel Rights

Article 27- (1) Personnel of the Authority shall be subject to the Law No. 657, excluding the matters regulated through the Law herein.

(2) Head and members of the Board and personnel of the Authority shall receive remunerations determined to be paid to the precedent personnel, within the scope of financial and social rights, as per Additional Article 11 of the Decree Law No. 375 of 27/6/1989, within the framework of the same procedures and principles applicable. Among the remunerations paid to the precedent personnel, those which are exempt from taxes and other legal deductions shall also be exempt from taxes and deductions as per the Law herein.

(3) Head and members of the Board and personnel of the Authority are subject to the sub-paragraph (c) of the first paragraph of Article 4 of the Social Insurance and Universal Health Insurance Law No. 5510 of 31/5/2006. Head and members of the Board and personnel of the Authority shall be considered equal with the precedent personnel in terms of retirement rights. Among the personnel who were appointed as Head and members of the Board when insured under sub-paragraph (c) of the first paragraph of Article 4 of the Law No. 5510, terms of office in these duties shall be considered while ascertaining acquired rights, salaries, grades and steps of those whose term of office ends or who express their will to resign. The relevant term of office of those who fall within the scope of Provisional Article 4 of the Law No. 5510 while on duty, shall be deemed as the period for which position and representation compensation should be paid. Removal from previous institutions and organisations of those who were appointed as Head and members of the Board when insured under sub-paragraph (a) of the first paragraph of Article 4 of the Law No. 5510, shall not entail receiving a severance pay or termination pay. In such a case, term of office qualified for a severance pay or termination pay, shall be added to the service periods spent as Head and member of the Board, and accepted as the period for which a retirement bonus.

(4) Civil servants working in public administrations attached to the centralized government, social security institutions, local administrations, administrations attached to local administrations, local administrative unions, revolving fund enterprises, funds established with laws, public entities, organizations more than 50% of whose capital belongs to public, public economic enterprises, state-owned economic enterprises, and associations and establishments attached to these, as well as other public officials may be seconded to the Authority upon the consent of their own institution, provided that their salaries, allowances, any increases thereof, compensations and other social and financial rights and aids are paid by their own institution. Requests of the Authority in this regard shall be concluded with priority by the related institutions and organizations. Personnel assigned accordingly shall be deemed on paid leave. During this leave, rights of the personnel and their connection with civil service shall be maintained, this period of leave shall be taken into account in promotions and

retirement, and they shall be promoted in due time without any need to further action. Periods spent in the Authority by those assigned under this Article shall be deemed to have been spent in their own institutions. Number of the personnel assigned accordingly shall not exceed ten per cent of the total number of posts for Personal Data Protection Experts and Personal Data Protection Assistant Experts, and the term of assignment shall not exceed two years. However, when deemed necessary, this term may be extended in one-year periods.

(5) Titles and numbers of posts regarding the personnel to be employed in the Authority are presented in the annexed Table (I). Changes in titles and grade; addition of new titles and annulment of vacant posts shall be realized upon the decision of the Board, provided that it shall not exceed the total number of posts, and shall be limited with the titles in the annexed tables of the Decree Law No. 190 on the General Posts and Procedures, dated 13/12/1983.

CHAPTER SEVEN

Miscellaneous

Exceptions

Article 28 - (1) The provisions of this Law shall not be applied in the following cases where:

a) personal data is processed by natural persons within the scope of purely personal activities of the data subject or of family members living together with him in the same dwelling provided that it is not to be disclosed to third parties and the obligations about data security is to be complied with.

b) personal data is processed for the purpose of official statistics and for research, planning and statistical purposes after having been anonymized.

(c) personal data is processed with artistic, historical, literary or scientific purposes, or within the scope of freedom of expression provided that national defence, national security, public security, public order, economic security, right to privacy or personal rights are not violated or they are processed so as not to constitute a crime.

(ç) personal data is processed within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations duly authorised and assigned to maintain national defence, national security, public security, public order or economic security.

(d) personal data is processed by judicial authorities or execution authorities with regard to investigation, prosecution, criminal proceedings or execution proceedings.

(2) Provided that it is in compliance with and proportionate to the purpose and fundamental principles of this Law, Article 10 regarding the data controller's obligation to inform, Article 11 regarding the rights of the data subject, excluding the right to demand compensation, and Article 16 regarding the requirement of enrolling in the Registry of Data Controllers shall not be applied in the following cases where personal data processing:

- a) is required for the prevention of a crime or crime investigation.
- b) is carried out on the data which is made public by the data subject himself.
- c) is required for inspection or regulatory duties and disciplinary investigation and prosecution to be carried out by the public institutions and organizations and by professional associations having the status of public institution, assigned and authorised for such actions, in accordance with the power conferred on them by the law,
- ç) is required for protection of State's economic and financial interests with regard to budgetary, tax-related and financial issues.

The Budget and the Revenues of the Authority

Article 29 - (1) The budget of the Authority shall be prepared and adopted in accordance with procedures and principles provided for in the Law No. 5018.

(2) The revenues of the Authority are as follows;

- a) Treasury grants from the general budget.
- b) The revenues from the movable and immovable properties of the Authority.
- c) Donations and grants received.
- ç) The revenues from the utilization of the revenues.
- d) Other revenues.

Amended and Inserted Provisions

Article 30 - (1) The following line was inserted into the Table (III) attached to the Law No. 5018:

“10) Personal Data Protection Authority”

(2) The phrase “Any person” in the second paragraph of Article 135 of the Law No. 5237 was amended as “Any personal data, any person”; and the phrase “Any person who records the information as personal data shall be punished according to the provisions of the above subsection.” as “the punishment to be given in accordance with the first paragraph is aggravated by half more.”

(3) The expression “children” in third paragraph of Article 226 of the Law No. 5237 was amended as “children, symbolic images of children or persons with a juvenile image”

(4) The expression “and” in first paragraph of Article 243 of the Law No. 5237 was amended as “or”, and the following paragraph was added.

“(4) Person who, by employing technical means, illegally monitors the data transfer carried out within an information system or between information systems without entering in the system, shall be punished with imprisonment from one year to three years”

(5) The following Article was inserted to follow Article 245 of the Law No.5237:

“Prohibited device or programmes”

Article 245/A- In case a device, computer programme, password or other security code are produced to commit the crimes inscribed exclusively within this Part and those that may be committed by using information system as a means, the person who produces, imports, dispatches, transfers, stores, accepts, sells, supplies, purchases, lends another person or possesses these shall be punished with imprisonment from one to three years and with a punitive fine up to five thousand days”

(6) Sub-paragraph (f) of the first paragraph of Article 3 of the Health Services Fundamental Law No 3359 of 7/5/1987 was amended as follows:

“f) With the aim of tracking the medical condition of everybody and to ensure that healthcare services are carried out in a more effective and rapid way, Ministry of Health and its associated institutions shall establish the required registration and notification system. This system may also be established in electronic environment in line with the e-State practices. To this end, a nationwide information system may be established by the Ministry of Health.”

(7) Article 47 of the Decree Law No 663 of 11/10/2011 on the Organization and Duties of the Ministry of Health and its Associated Institutions was amended as follows:

“ARTICLE 47- (1) Of those applying to the public or private health organizations and health professionals to receive health service, personal data provided compulsorily as a requirement of health service or provided in relation with the service they received may be processed.

(2) The Ministry may process the data obtained within the framework of the first paragraph in order to provide the health services, protect the public health, maintain the services of preventive medicine, medical diagnosis, treatment and care, and to plan the health services and calculate their cost. This

data shall not be transferred except for the conditions stipulated under the Law on the Protection of Personal Data.

(3) The Ministry shall establish a system that will enable the persons themselves or any third person authorized by them to access the personal data gathered and processed pursuant to the second paragraph,

(4) Standards relating to the security and reliability of the systems established as per the third paragraph shall be determined by the Ministry in compliance with the principles determined by the Personal Data Protection Board. The Ministry shall take the necessary measures to ensure the security of the personal health data obtained pursuant to the Law herein. To this end, the Ministry shall establish a security system enabling the supervision of the official and the purpose of using the registered data in the system.

(5) Public institutions and organizations, natural persons and legal entities under the private law employing health personnel shall be obliged to inform the Ministry about the personnel employed and the personnel movements.

(6) Other matters relating to the processing and security of personal health data and the implementation of the Article herein shall be governed through a by-law to be put into force by the Ministry.”

By-law

Article 31 - (1) By-laws related to the implementation of this Law shall be put into force by the Authority.

Transitional Provisions

PROVISIONAL ARTICLE - (1) The members of the Board shall be selected and the organizational structure of the Presidency shall be established within six months following the date of publication of this Law, as per the procedure stipulated in Article 21.

(2) Data controllers are obliged to enrol in the Registry of Data Controllers within the time specified and announced by the Board.

(3) The personal data that were processed before the publication date of this Law shall be rendered compatible with the provisions of this Law within two years as of its date of publication. The personal data which are found to be in breach of the provisions of this Law shall be immediately erased, destroyed or anonymized. However, consents duly taken before the publication date of this Law shall

be deemed compatible with the provisions of this Law, unless no declaration of intent is made to the contrary within one year.

(4) The by-laws provided for by this Law shall be put into force within one year as of the date of publication of this Law.

(5) A high-level executive, to ensure coordination with regard to the implementation of the Law in public institutions and organisations, shall be appointed and notified to the Presidency within one year as of the date of publication of this Law.

(6) The term of office for the first elected President, the Deputy President, and two members who are determined by ballot, shall be six years; this period shall be four years for the remaining five members.

(7) Until the budget of the Authority is allocated;

a) The expenditures of the Authority shall be reimbursed by the budget of the office of the Prime Minister.

b) All necessary support services such as the premises, equipment, furnishing and the hardware shall be provided by the office of the Prime Minister in order for the Authority to fulfill its duties.

(8) The clerical services of the Authority shall be carried out by the office of the Prime Minister until the service units of the Authority has become fully functional.

Entry into force

Article 32 - (1) For the purposes of this Law;

a) Articles 8, 9, 11, 13, 14, 15, 16, 17 and 18 shall enter into force after six months as of the date of its publication.

b) Other Articles shall enter into force on the date of its publication.

Enforcement

Article 33 - (1) The provisions of this law shall be enforced by the Council of Ministers.

By-Law On Data Controllers Registry

Official Journal Date : 30.12.2017

Official Journal No : 30286

BY-LAW ON DATA CONTROLLERS REGISTRY

CHAPTER ONE

Purpose, Scope, Legal Basis and Definitions Purpose

ARTICLE 1 - (1) The purpose of this By-law is to determine and ensure the implementation of procedures and principles related to the establishment and management of Data Controllers' Registry to be kept publicly available by Presidency under supervision of the Board pursuant to Personal Data Protection Law No. 6698 of 24/3/2016 and envisaged records to be entered into Data Controllers' Registry.

Scope

ARTICLE 2 - (1) This By-law shall apply to natural and legal persons who determine the purposes and means of personal data processing and are responsible for establishment and management of the data filing system.

Legal Basis

ARTICLE 3 - (1) This By-law has been prepared on the basis of Article 16(5) and subparagraphs (d) and (e) of Article 22(1) of Law No. 6698.

Definitions

ARTICLE 4 - (1) For the purposes of this By-law:

- a) "Recipient group" means category of natural and legal persons to which the personal data are transferred by the data controller,
- b) "President" means the President of Personal Data Protection Authority,
- c) "Presidency" means the Presidency of Personal Data Protection Authority,
- ç) (Amended: OG (Official Gazette) - 28/4/2019-30758) "Contact person" means the natural person notified by the data controller which is natural and legal person established in Turkey and by

representative who represents the data controller which is natural and legal person not established in Turkey during the registration with the Registry for communicating with the Authority relating to obligations within the scope of the Law and secondary legislation to be prepared in accordance with this Law,

d) "Law" means the Personal Data Protection Law No. 6698,

e) "Registration" means the notification made by data controllers who are obliged to register, in accordance with procedures and principles determined by this By-law.

f) "Obligation to register" means the obligation relating to registration to be fulfilled pursuant to the By-law,

g) "Registered e-mail address (KEP)" means the qualified form of electronic mail which provides legal evidence for the use of it, including sending and delivering of electronic messages,

ğ) "Personal data" means any information relating to an identified or identifiable natural person,

h) (Amended: OG-28/4/2019-30758) "Personal data processing inventory" means the inventory which are detailed by explanations of the followings; personal data processing operations performed by data controllers according to their business processes, purposes and legal basis of personal data processing, data category, recipient group, maximum storage period which is formed relating to the group of person subject to data and necessary for the purpose for which personal data are processed, personal data envisaged to be transferred to foreign countries, and measures taken relating to data security.

ı) "Personal data storage and disposal policy" means the policy which data controllers issue as a basis for erasure, destruction and anonymization of personal data and the determination of maximum storage period for the purpose for which personal data are processed.

ii) "Processing of personal data" means any operation which is performed on personal data, wholly or partially by automated means or non-automated means which provided that form part of a data filing system, such as collection, recording, storage, protection, alteration, adaptation, disclosure, transfer, retrieval, making available for collection, categorization, preventing the use thereof,

j) "Board" means the Personal Data Protection Board,

k) "Authority" means the Personal Data Protection Authority,

l) "Registry" means Data Controllers' Registry kept by the Presidency,

m) "Category of Data" means group of personal data related to group(s) of persons subject to data that are classified in accordance with their common features,

n) "Group of persons subject to the data" means category of the data subject whose personal data are processed by data controllers,

o) "Data Controllers' Registry Information System (VERBIS)" means information system that is accessible through the Internet, established and managed by the Presidency, that data controllers will use for the registration with the Registry and the other operations related to the Registry,

ö) "Data controller" means the natural or legal person who determines the purpose and means of processing of personal data and is responsible for establishment and management of the data filing system,

p) (Amended: OG-28/4/2019-30758) "Representative of the data controller" means the legal person established in Turkey or the natural person who is citizen of Republic of Turkey, minimum authorized to represent data controllers which are not established in Turkey within the scope of the issues specified in the third paragraph of Article 11 of this By-law,

(2) For the definitions not included in this By-law, the definitions in the Law shall apply.

CHAPTER TWO

Establishment, Management, Supervision of the Registry and Access to the Registry

Principle, rules and procedures

ARTICLE 5 - (1) Following principles, rules and procedures shall be applied in establishment, management and supervision of the Registry:

a) Data controllers are obliged to register with the Registry prior to the start of data processing.

b) Data controllers not established in Turkey are obliged to register with the Registry by their representatives prior to the start of data processing.

c) The Registry shall be kept publicly available. Board is authorized to determine the scope of this principle and derogations provided that the principle of making publicly available is ensured.

ç) (Amended: OG-28/4/2019-30758) Data controllers under registration obligation are obliged to prepare Personal Data Processing Inventory. The information to be entered in the application for the Registry is prepared based on Personal Data Processing Inventory.

d) The information entered into the Registry based on personal data processing inventory and published in the Registry, shall be the basis for the obligation to inform for data controllers referred

to in Article 10 of the Law, responses to the request of concerned data subjects referred to in Article 13 of the Law and the determination of the scope of explicit consent to be given by data subjects.

e) Data controllers shall be responsible for the information entered into the Registry and published in the Registry to be complete, accurate, up-to-date and lawful. Registration of the data controllers with the Registry shall not remove the other obligations under the Law.

f) Without prejudice to the conditions specified in Article 28 of the Law, the Board may provide derogation from the obligation to register for the data controllers meeting certain conditions on the basis of the objective criteria specified in Article 16 of the By-law. This derogation shall not remove the obligations of those data controllers under the Law.

g) The operations relating to the Registry shall be carried out by data controllers through VERBIS.

ğ) (Amendment: OG-28/4/2019-30758) - (1) Maximum storage period necessary for the purpose of processing of personal data entered by data controllers into the Registry and published in the Registry shall be basis for erasure, destruction and anonymization obligations of data controllers specified in Article 7 of the Law.

Establishment, Management and Supervision of the Registry

ARTICLE 6 - (1) Registry is established by Presidency. Presidency, for the establishment, management, protection of the Registry and maintaining it up-to-date, shall take necessary technical and organizational measures to establish and to operate VERBIS.

(2) Responsible department for establishment and management of the Registry is Department of Data Management.

(3) Supervision of the Registry is carried out by the Board. Activity report which has been prepared by Department of Data Management once a three month and whose scope determined by the Board, shall be transmitted to the Board.

Access to Registry

ARTICLE 7 - (1) The Presidency shall make current information in the Registry publicly available by the appropriate means to be determined pursuant to Board decisions.

(2) Among the information given in the Registry, the following shall be disclosed to the public:

a) (Amendment: OG-28/4/2019-30758) The data controller, representative of the data controller, if any, address and KEP (Registered E-Mail) address, if taken,

- b) The purposes for which the personal data will be processed,
- c) Group(s) of persons subject to the data and data categories relating to those persons,
- ç) Recipients and recipient groups to whom personal data may be transferred,
- d) Personal data which are envisaged to be transferred to foreign countries,
- e) Registration date and expiration date of the registration.
- f) Measures taken for the security of personal data,
- g) Maximum storage period necessary for the purposes for which personal data are processed.

CHAPTER THREE

Beginning of Registration Obligation, Information to be entered into VERBIS, Registration Application, Renewal and Erasure of Registration

Beginning of Registration Obligation

ARTICLE 8 - (1) Data controllers shall fulfil the obligation to register with the Registry prior to the start of data processing.

(2) If the data controllers, who are not under the registration obligation, become obliged to register later, they shall register with the Registry within thirty days following their entry into the obligation.

(3) Data controllers, who are obliged to register with the Registry, may request additional time for fulfilling their registration obligation from the Authority in cases where they cannot fulfil their obligation to register due to any technical, legal or actual impossibility on the condition that apply to the Authority in writing with justifiable grounds in not later than 7 work days. Authority may give additional time only once, not exceeding thirty days in any case.

Information to be entered within the scope of registration obligation

ARTICLE 9 - (1) Registration Application to the Registry includes the following information:

- a) The information included in the application form determined by the Board relating to the identity and address of the data controller, representative of the data controller, if any and contact person,
- b) The purposes for which the personal data will be processed,
- c) The explanations about group(s) of persons subject to the data as well as about the data categories belonging to these people,
- ç) The recipients or groups of recipients to whom personal data may be transferred,

- d) The personal data which are envisaged to be transferred abroad,
 - e) Measures taken as referred to in Article 12 of the Law and in accordance with the criteria determined by the Board,
 - f) Maximum storage period of personal data laid down by the legislation or for the purposes for which personal data are processed,
- 2) Information to be entered into the Registry by data controllers pursuant to subparagraphs (b), (c), (c) and (d) of the first paragraph; shall be transmitted through VERBIS to the Registry based on Personal Data Processing Inventory by using headings given in VERBIS.
- (3) Information to be entered into the Registry by data controllers pursuant to subparagraph (e) of the first paragraph shall be transmitted through VERBIS to the Registry in the manner that cover the issues specified in the Article 12 of the Law by using headings given in VERBIS.
- (4) Information relating to the maximum storage period laid down by the legislation or for the purposes for which personal data are processed relating to the personal data to be entered into the Registry by data controllers pursuant to the subparagraph (f) of the first paragraph, shall be entered into the Registry by matching them with data categories. Maximum storage period necessary for the purposes of processing of data categories entered into the Registry by the data controller may differ from the period envisaged in the legislation. In such cases, if maximum storage period is envisaged in the legislation, this period shall be entered into the Registry, if not envisaged, the longest storage period of this category shall be entered into the Registry. While determining the maximum storage period required for purposes for which personal data are processed, following issues shall be taken into account:
- a) The period generally accepted in the sector in which the data controller operates within the scope of purposes for processing relevant data category,
 - b) The period that requires processing of personal data in the relevant data category and to continue legal relationship with the data subject,
 - c) The period to be valid for the legitimate interest to be obtained by the data controller in accordance with lawfulness and fairness, depending on the purpose of processing relevant data category,
 - ç) The period in which the risks, costs and responsibilities arising from the storage of the relevant data category depending on the purpose of processing shall continue legally,

- d) Whether maximum storage period to be determined is appropriate to keep the relevant data category accurate and up-to-date where necessary,
- e) Time period in which the data controller is obliged to retain personal data given in the relevant data category pursuant to its legal obligation,
- f) Period of limitation determined by the data controller for assertion of a right relating to personal data in the relevant data category.

(5) Data controllers shall issue a personal data storage and disposal policy for defining maximum storage period of personal data for the purposes of processing, complying with this period indicated in personal data processing inventory and tracking whether these periods are exceeded or not and shall ensure the implementation of such policy.

(6) In cases where headings and contents given in VERBIS do not cover operations of the data controller and the information to be entered into the Registry, the data controller shall complete its registration by entering such information into "Others" section in VERBIS which is provided for such cases.

Application for Registration

ARTICLE 10 - (1) Data controllers shall be deemed to have fulfilled its registration obligation by entering the information specified in Article 9 into VERBIS.

(2) Data controllers, who have been given additional time by the Authority pursuant to third paragraph of Article 8, are obliged to complete registration before this time expires.

Obligations of the data controller, representative of the data controller and contact person

ARTICLE 11 - (1) Legal persons are themselves the data controllers for the legal persons. The data controller obligations of legal persons established in Turkey under the Law are fulfilled by capacity of competent to represent and bind the legal person or the person(s) specified in the relevant legislation pursuant to provisions of the relevant legislation. Competent representative may assign one or more persons for its obligations to be fulfilled for the implementation of the Law. This assignment does not remove the responsibilities of legal person pursuant to the provisions of the Law.

(2) Representatives of data controllers not established in Turkey shall submit certified copy of decision for the designation of a representative to be taken its competent or person to the Authority during application.

(3) Decision of designation for representative of the data controller shall be arranged to cover at least the following points:

a) to receive or accept notifications and correspondence made by the Authority on behalf of the data controller,

b) to transmit the demands made by the Authority to the data controller and to submit the responses of the data controller to the Authority,

c) to receive and transmit requests to be made by data subjects pursuant to first paragraph of the Article 13 of the Law on behalf of the data controller, in case no other principle has been determined by the Board.

ç) to transmit the response of the data controller to the data subjects pursuant to third paragraph of Article 13 of the Law, in case no other principle has been determined by the Board,

d) to perform operations relating to the Registry on behalf of the data controller.

4) (Amendment: OG-28/4/2019-30758), Data controllers established in Turkey and representatives of data controllers not established in Turkey shall enter contact person information into the Registry at the time of registration. Contact person is not authorized to represent data controllers in accordance with the provisions of the Law and the By-law.

5) (Amendment: OG-28/4/2019-30758) Contact person in the public institutions shall be head of department or higher executive to be assigned by the coordinating high level executive for the aim of communication with the Authority.

Communication

ARTICLE 12 - (1) Related to the implementation of the Law, the Authority shall use following means of communications with data controllers:

a) For legal persons established in Turkey; identity, address or KEP (registered e-mail address) address notified to the Registry,

b) For natural persons settled in Turkey; identity, address or KEP address notified to the Registry,

c) For data controllers not established in Turkey; representative of the data controller notified to the Registry.

Changes in Registry records

ARTICLE 13 - (1) (Amendment: OG-28/4/2019-30758) In case of any change in the Registry records, data controllers shall notify the Authority through VERBIS within seven days of the date of change.

Erasure of Registry records

ARTICLE 14 - (1) The data controller shall apply to the Authority relating to the erasure of their Registry records through VERBIS.

(2) If the obligation to register is relieved or terminated, Registry records shall be erased. These records shall be accessible in case of any request however they are kept in a manner that no changes can be made.

(3) Erasure of registry records does not relieve the data controller of the obligations during the period in which it is registered.

CHAPTER FOUR

Exemptions from Registration Obligation

Cases of exemptions

ARTICLE 15 - (1) In respect of the following personal data processing activities, data controllers are not obliged to register and notify these activities to the Registry:

- a) Data processing is necessary for the prevention of committing a crime or for crime investigation.
- b) Processing the data which are made public by the data subject himself/herself.
- c) Data processing is necessary for performance of supervision or regulatory duties and disciplinary investigation and prosecution to be carried out by the assigned and competent public institutions and organizations and by the public professional organizations, in accordance with the power conferred on them by the law,
- ç) Data processing is necessary for protection economic and financial interests of State related to budgetary, tax and financial matters.

Derogation criteria

ARTICLE 16 - (1) The Board may provide derogation from registration obligation by considering following criteria:

- a) The nature of personal data.
- b) The quantity of personal data.

- c) The purpose of processing of personal data.
 - ç) The field of activity where personal data are processed.
 - d) Transferring personal data to third parties.
 - e) The fact that the processing of data is laid down in the laws.
 - f) Storage period of personal data.
 - g) Group of persons subject to the data or categories of data.
 - ğ) (Annex: OG-28/4/2019-30758) The information of annual number of employees or annual financial balance sheet of the data controller.
- (2) Board has the authority to take decisions in order to determine principles and procedures of implementation and the scope of exemptions determined in the framework of criteria listed in the first paragraph. Board shall announce such decisions to public via appropriate means of communication.

CHAPTER FIVE

Miscellaneous

Administrative sanction

ARTICLE 17 - (1) Administrative fine referred to in sub-paragraph (ç) of Article 18(1) of the Law shall be imposed on data controllers who act contrary to the obligation to register and notify.

(2) In the event that the action to contrary to the obligation to register and notify is committed within the public institutions and organizations as well as the public professional organizations, the disciplinary provisions shall be applied to the civil servants and other public officers employed in the relevant public institutions and organisations and those employed in the public professional organizations upon the notice of the Board and the result is reported to the Board.

Clarifying the Doubts

ARTICLE 18 - (1) The Board is authorised to clarify the doubts and recover disruptions to occur during the implementation of this By-law, to direct the implementation, to determine the principles and standards and make necessary arrangements to ensure the unity of implementation, to demand any type of information and documentation in this regard and to take a decision within the framework of the relevant legislation on matters which are not included in this By-law.

Entry into force

ARTICLE 19 - (1) This By-law enters into force on 1/1/2018. Enforcement **ARTICLE 20 - (1)** The President shall enforce the provisions of this By-law.

	The By-law published in the Official Gazette	
	Date	Number
	30/12/2017	30286
	By-laws making amendments on the By-law published in the Official Gazette (s)	
Date	Number	
1.	28/4/2019	30758
2.		

By-Law on Erasure, Destruction or Anonymization of Personal Data

Official Journal Date : 28.10.2017

Official Journal No : 30224

BY-LAW ON ERASURE, DESTRUCTION OR ANONYMIZATION OF PERSONAL DATA

FIRST CHAPTER

Purpose, Scope, Legal Basis and Definitions

Purpose

ARTICLE 1 - (1) The purpose of this By-Law is to determine principles and procedures regarding erasure, destruction and anonymization of personal data processed wholly or partially by automated means or by non-automated means which provided that form part of a data filing system.

Scope

ARTICLE 2 - (1) Provisions of this By-Law shall apply to data controllers in accordance with Article 7 of the Personal Data Protection Law No. 6698 and of 24/03/2016.

Legal Basis

ARTICLE 3 - (1) This By-Law is issued on the basis of Article 7(3) and sub-paragraph (e) of Article 22(1) of Personal Data Protection Law No. 6698.

Definitions

ARTICLE 4 - (1) For the purposes of this By-Law:

- a) "Recipient group" means category of natural or legal persons to which the personal data are transferred by the data controller,
- b) "User concerned" means persons who process personal data within the organization of the data controller or upon authorization and instructions received from the data controller, other than the person or department which is responsible for the technical storage, protection and back up of personal data,
- c) "Disposal" means erasure, destruction or anonymization of personal data,
- ç) "Law": Personal Data Protection Law No. 6698 and of 24/3/2016,

d) "Recording medium" means any type of environment that keeps the personal data processed wholly or partially by automated means or non-automated means which provided that form part of a data filing system,

e) (Amendment:OG-28/4/2019-30758) "Personal data processing inventory" means the inventory which are detailed by explanations of the followings: personal data processing activities of data controllers according to their business processes; purposes and legal ground of personal data processing; data category; maximum data storage period required for the purposes formed relating to the recipient group to whom the data are transferred and with data subject groups, and for personal data processing; personal data envisaged to be transferred to foreign countries; and measures taken relating to the data security,

f) "Personal data storage and disposal policy" means the policy which data controllers issues as a basis for erasure, destruction and anonymization of personal data and determination of maximum storage period for the purpose for which personal data are processed,

g) "Board" means Personal Data Protection Board,

ğ) "Periodic Disposal" means the erasure, destruction or anonymization process which is determined in the personal data storage and disposal policy and to be carried out periodically ex officio, in the event that all of the conditions for processing laid down in the Law no longer exist,

h) "Registry" means Data Controllers' Registry kept by Personal Data Protection Authority,

ı) "Data filing system" means the filing system where personal data are processed by being structured according to specific criteria,

i) "Data Controller" means the natural or legal person who determines the purpose and means of processing personal data and is responsible for the establishment and management of the data filing system,

(2) For the definitions not included in this By-Law, the definitions in the Law shall apply.

CHAPTER TWO

Personal Data Storage and Disposal Policy

Principles regarding the Personal Data Storage and Disposal Policy

ARTICLE 5 - (1) Pursuant to Article 16 of the Law; data controllers who are obliged to register with Data Controllers' Registry system shall issue personal data storage and disposal policy in accordance with personal data processing inventory.

(2) To issue personal data storage and disposal policy shall not mean that personal data are stored, erased, destructed or anonymized in accordance with the Law and the By-Law. (3) For data controllers who are not obliged to issue personal data storage and disposal policy, the obligation of storage, erasure, destruction or anonymization of personal data shall continue pursuant to the Law and By-Law.

Scope of personal data storage and disposal policy

ARTICLE 6 - (1) Personal data storage and disposal policy shall at least include the following:

- a) Purpose of issuing personal data storage and disposal policy,
- b) Recording medium arranged in accordance with personal data storage and disposal policy,
- c) Definitions of technical and legal terms indicated in personal data storage and disposal policy,
- ç) Explanations relating to legal, technical or other reasons requiring storage and disposal of personal data
- d) Technical and organizational measures taken against unlawful processing of and access to personal data and for storing personal data securely,
- e) Technical and organizational measures taken for lawful disposal of personal data,
- f) Definitions of titles, units and tasks of those who are involved in personal data storage and disposal processes
- g) Table that shows storage and disposal periods,
- ğ) Time period for periodic disposal,
- h) Any alterations being made in the current personal data storage and disposal policy, if any.

CHAPTER THREE

Erasure, Destruction and Anonymization of Personal Data

Principles

ARTICLE 7 - (1) Personal data shall be erased, destructed or anonymized by the controller ex officio (by its own initiative) or upon the request of the data subject, in the event that all of the conditions for processing laid down in Article 5 and Article 6 of the Law no longer exist.

(2) It is mandatory to act in accordance with general principles of Article 4 of the Law, technical and organizational measures to be taken within the scope of Article 12, provisions of the relevant

legislation, Board decisions and personal data storage and disposal policy in erasure, destruction and anonymization of personal data.

(3) All operations relating to erasure, destruction and anonymization of personal data shall be recorded and those records shall be stored for minimum three years excluding other legal obligations.

(4) (Amendment: OG-28/4/2019-30758) The data controller is obliged to describe the methods used for the erasure, destruction and anonymization operations of personal data in the relevant policies and procedures.

(5) Unless otherwise decided by the Board, the data controller may choose one of the appropriate methods for periodic erasure, destruction or anonymization of personal data ex officio. Upon request of data subject, the data controller may choose appropriate method with justified grounds.

Erasure of personal data

ARTICLE 8 - (1) Erasure of personal data is the process of rendering personal data inaccessible and non-reusable for the users concerned, by no means.

(2) The data controller is obliged to take necessary technical and organizational measures required for ensuring erased data to be inaccessible and non-reusable for its users concerned.

Destruction of personal data

ARTICLE 9 - (1) Destruction is the process of rendering personal data inaccessible, irretrievable or non-reusable by anyone, by no means.

(2) The data controller is obliged to take any type of technical and organizational measures required for ensuring destruction of personal data.

Anonymization of personal data

ARTICLE 10 - (1) Anonymization is the process of rendering personal data impossible to link with an identified or identifiable natural person, even through matching them with other data.

(2) To anonymize the personal data, personal data shall be rendered impossible to relate to identified or identifiable person, even through using appropriate techniques in respect of the recording medium and relevant field of activity, such as recovery of data by the data controller, recipient or recipient groups and matching data with other data.

(3) The data controller is obliged to take any type of technical and organizational measures required for ensuring anonymization of personal data.

Time periods for ex officio erasure, destruction and anonymization of personal data

ARTICLE 11 - (1) The data controller, who has issued data storage and disposal policy, shall erase, destruct or anonymize the personal data in the first periodic disposal process following the date when obligation of erasure, destruction or anonymization of personal data arises.

(2) Time interval for periodic disposal shall be defined in personal data storage and disposal policy by the data controller. This time interval cannot exceed six months in any case.

(3) Data controllers who are not obliged to issue personal data storage and disposal policy, shall erase, destruct or anonymize personal data within three months following the date for obligation of erasure, destruction or anonymization of personal data arises.

(4) Board may shorten the durations specified in this Article in the case of irreparable or impossible damages, and in the event of explicit infringement of the law.

Time period for erasure and destruction of personal data upon request of data subject

ARTICLE 12 - (1) (Amendment- OG-28/4/2019-30758) When the data subject requests erasure or destruction of his/her personal data from the data controller, pursuant to Article 11 and 13 of the Law;

a) In the event that all of the conditions for the processing no longer exist; the data controller shall erase, destruct or anonymize the mentioned personal data which are subject to the request. The data controller shall act on the request of the data subject at the latest within thirty days and inform the data subject.

b) In the event that all of the conditions for the processing no longer exist and the personal data which are subject to the request have been transferred to any third party; the data controller shall notify the third party of such request and ensure the performance of necessary operations by the third party within the scope of this By-Law.

c) In the event that all of the conditions for the processing have not disappeared completely, the request may be rejected by the data controller in accordance with the Article 13(3) of the Law together with its justified grounds and such rejection shall be communicated to the data subject in writing or by electronic means at the latest within thirty days.

CHAPTER FOUR

Miscellaneous and Final Provisions

Clarifying Doubts

ARTICLE 13 - (1) The Board is authorised to clarify the doubts and recover disruptions to occur during the implementation of this By-Law, to direct the implementation, to determine the principles and standards and make necessary arrangements to ensure the unity of implementation, to demand any type of information and documentation in this regard and to take a decision within the framework of the relevant legislation on matters which are not included in this By-Law.

Entry into force

ARTICLE 14 - (1) This By-Law shall enter into force on 1/1/2018.

Enforcement

ARTICLE 8 - (1) The President of Personal Data Protection Authority shall enforce the provision of this By-Law.

	The By-law published in the Official Gazette	
	Date	Number
	28/10/2017	30224
	By-laws making amendments on the By-law published in the Official Gazette (s)	
Date	Number	
1.	28/4/2019	30758

Communiqué on the Principles and Procedures for the Request to Data Controller

Official Journal Date : 10.03.2018

Official Journal No : 30356

COMMUNIQUE ON THE PRINCIPLES AND PROCEDURES FOR THE REQUEST TO DATA CONTROLLER

Purpose and Scope

ARTICLE 1 - (1) This Communiqué has been prepared in order to determine the principles and procedures for the request to be made to the data controller and fee to be charged in cases where the process requires additional costs.

Legal Basis

ARTICLE 2 - (1) This Communiqué has been prepared on the basis of Article 13 and sub-paragraphs (e) and (g) of Article 22 (1) of Personal Data Protection Law No 6698 of 24/03/2016.

Definitions

ARTICLE 3 - (1) For the purposes of this Communiqué:

- a) "Request" means request made within the scope of Article 13 of the Law,
- b) "Secured Electronic Signature" means the electronic signature which exclusively belongs to the signatory, has been created by means of secured signature creation devices under exclusive disposition of the signatory, provides identification of the signatory via qualified electronic certificate, provides the determination whether any subsequent changes have been made in the signed electronic document,
- c) "Data subject" (natural person concerned) means the natural person whose personal data are processed,
- ç) "Law" means Personal Data Protection Law numbered 6698 of 24/03/2016,
- ç) "Board" means the Personal Data Protection Board,

d) "Recording medium" means any type of environment that keeps the personal data, processed wholly or partially by automated means or non-automated means which provided that form part of a data filing system,

e) "Registered electronic mail (KEP) address" means the qualified form of electronic mail which provides legal evidence for the use of it, including sending and delivering of electronic messages,

f) "Board" means the Personal Data Protection Board,

g) "Authority" means the Personal Data Protection Authority,

ğ) "Mobile signature" means electronic signature created by using a mobile device,

(2) For the definitions not included in this Communiqué, the definitions in the Law shall apply.

Right to Request

ARTICLE 4 - (1) Natural persons whose personal data are processed have right to request to the data controllers.

(2) Data subjects may benefit from this right provided that they make the requests in Turkish.

Procedures of Request

ARTICLE 5 - (1) Data subjects may make requests to data controllers within the scope of their rights specified in Article 11 of the Law, in writing or by registered electronic mail (KEP) address, secured electronic signature, mobile signature or by the e-mail address which has been previously recorded in the data controller's system or by means of a software or application designed for purposes of this request.

(2) The request must include the following;

a) Name, surname and signature, if the request is made in writing,

b) For Turkish Citizens, TC identity number; for foreigners, nationality, passport number or identity number if available,

c) Residential and business address subject to the notification,

ç) Electronic mail address, telephone, fax number subject to notification if available,

d) Subject of demand,

(3) Documents and information regarding the demand shall be attached to the request,

(4) In written request, the request date is the date that the document is notified to data controller or to its representative.

(5) In the case that the requests are made by other methods, requisition date is the date when the request is delivered to data controller.

Response to the Request

ARTICLE 6 - (1) The Data controller is obliged to take necessary organizational and technical measures to conclude the requests to be made by data subject within the scope of the Communiqué, effectively and in accordance with norms of lawfulness and fairness.

(2) The data controller shall act on the request or refuse it together with justified grounds.

(3) The data controller shall communicate its response to the subject in writing or by electronic means.

(4) Letter of response shall include the following:

a) Information regarding data controller or its representative,

b) The requester's name and surname, for Turkish citizens, TC identity number; for foreigners nationality, passport number or identity number if available, residential and business address subject to the notification, electronic mail address, telephone and fax numbers subject to notification if available,

c) Subject of demand,

ç) Explanations of data controllers regarding the request,

(5) Data controller shall conclude the demands set forth in the request within the shortest time by taking into account the nature of the demand and at the latest within thirty days and free of charge. However, if process requires additional costs, fees laid down in Article 7 may be charged. If the Request is made due to the fault of the data controller, the fee is refunded to data subject.

(6) In the case that the demand of the data subject is accepted by the data controller, the demand shall be fulfilled by the controller within the shortest time and information is communicated to data subject.

Fee

ARTICLE 7 - (1) If the request of the data subject is to be responded in writing, no fee will be charged up to ten pages. 1 Turkish Lira may be charged per page over ten pages.

(2) In cases where the request is responded by means of recording medium like CD, flash memory, fee to be charged by data controller cannot exceed the cost of the recording medium.

Entry into force

ARTICLE 8 - (1) This Communiqué shall enter into force on date of issue in the Official Gazette.

Enforcement

ARTICLE 9 - (1) The President of Personal Data Protection Authority shall enforce the provisions of this Communiqué.

Communiqué on Principles and Procedures to be Followed in Fullfillment of the Obligation to Inform

Official Journal Date : 10.03.2018

Official Journal No : 30356

**COMMUNIQUE ON PRINCIPLES AND PROCEDURES TO BE FOLLOWED IN
FULLFILLMENT OF THE OBLIGATION TO INFORM**

Purpose and Scope

ARTICLE 1 - (1) The purpose of this Communiqué is to determine the procedures and principles to be followed within the scope of the obligation to inform to be fulfilled by data controllers or persons authorized by them, pursuant to Article 10 of the Personal Data Protection Law No. 6698 of 24/3/2016.

Legal Basis

ARTICLE 2 - (1) This communiqué has been prepared on the basis of sub-paragraphs (e) and (g) of Article 22 (1) of the Personal Data Protection Law No. 6698.

Definitions

ARTICLE 3 - (1) For the purposes of this communiqué:

- a) "Recipient group" means the category of natural and legal person to which the personal data are transferred by the data controller,
- b) "Data subject (Natural person concerned)" means the natural person whose personal data are processed,
- c) "Law" means Personal Data Protection Law No. 6698 and of 24/3/2016,
- ç) "Board" means the Personal Data Protection Board,
- d) "Authority" means Personal Data Protection Authority,
- e) "Registry" means Data Controllers' Registry kept by Presidency,
- f) (Amendment: OG-28/4/2019-30758) "Data filing system" means filing system where personal data are processed by being structured according to specific criteria.

g) “Data controller” means the natural or legal person who determines the purposes and means of processing personal data and is responsible for establishment and management of the data filing system.

ğ) (Amendment: OG-28/4/2019-30758) “Representative of the data controller” means a legal person established in Turkey or a natural person who is citizen of Republic of Turkey, minimum authorized to represent data controllers not established in Turkey on issues specified in the third paragraph of Article 11 of By-law on Data Controllers’ Registry.

(2) For the definitions not included in this Communiqué, the definitions in the Law shall apply.

Scope of the Obligation to Inform

ARTICLE 4 - (1) Pursuant to Article 10 of the Law; data subjects shall be informed by data controllers or the person authorised by them at the time when personal data are obtained.

At the time when this obligation is being fulfilled, information to be given by data controllers or the person authorised by them shall at least include following issues:

- a) the identity of the data controller or its representative, if any,
- b) the purpose of processing of personal data,
- c) to whom and which purposes personal data may be transferred,
- ç) the method and legal basis of collection of personal data,
- d) other rights of data subject referred to in Article 11 of the Law.

Principles and procedures

ARTICLE 5 - (1) The following procedures and principles shall be followed at the time of the fulfilment of the obligation to inform by the data controller or the person authorized by it by using physical or electronic media such as oral or written statement, voice recording, call centre:

- a) The obligation to inform shall be fulfilled in any case of processing depending on the explicit consent of data subject or other conditions for processing in the Law.
- b) In case the purpose of personal data processing changes, the obligation to inform shall be fulfilled for this purpose prior to data processing operation, as well.
- c) (Repealed: OG-28/4/2019-30758)
- ç) If the data controller is obliged to register with the Registry, information to be given to data subject within the scope of the obligation to inform shall conform to those given in the Registry.

- d) Fulfilment of the obligation to inform does not depend on the request of data subject.
- e) Proof of fulfilment of the obligation to inform shall be under responsibility of the data controller.
- f) In the event that processing personal data is on the basis of explicit consent, procedures of the obligation to inform and obtaining explicit consent shall be performed separately.
- g) The purpose of processing personal data to be explained within the scope of the obligation to inform shall be specified, explicit and legitimate. While the obligation to inform is being fulfilled, general and ambiguous statements should be avoided. Statements which may raise opinions on processing of personal data for other possible purposes shall not be used.
- ğ) The notification to be given within the scope of the obligation to inform shall be performed by using intelligible, clear and plain language
- h) "Legal basis" mentioned in sub-paragraph (ç) of Article 10(1) of the Law means that personal data are processed on the basis of which processing conditions determined in the Article 5 and 6 of the Law within the scope of the obligation to inform. Legal basis shall be explicitly provided at the time of fulfilment of the obligation to inform.
- ı) Within the scope of the obligation to inform, the purpose of processing of personal data and recipient group to which personal data will be transferred shall be stated.
- ı) Within the scope of the obligation to inform, it shall be clearly stated by which method personal data are obtained from wholly or partially by automated means or by non-automated means which provided that form part of a data filing system.
- j) At the time of fulfilment of the obligation to inform; information that is incomplete, incorrect and misleading the data subjects shall not be used.

The Obligation to Inform in cases where personal data are not obtained directly from data subject

ARTICLE 6 - (1) In cases where personal data are not obtained directly from data subjects; the obligation to inform shall be fulfilled:

- a) within a reasonable time following the obtainment of the personal data,
- b) at the first instance of communication in case personal data are used to communicate with the data subject,
- c) at the time of the first transfer of personal data at the latest in case personal data are to be transferred.

Entry into force

ARTICLE 7 - (1) This Communiqué shall enter into force on the date of issue in the Official Gazette.

Enforcement

ARTICLE 8 - (1) The President of Personal Data Protection Authority shall enforce the provisions of this Communiqué.

	The By-law published in the Official Gazette	
	Date	Number
	10/03/2018	30356
	By-laws making amendments on the By-law published in the Official Gazette (s)	
	Date	Number
	28/4/2019	30758

KİŞİSEL VERİLERİ KORUMA KURULU İLKE KARARLARI

Bölüm İçeriği

- 2022/388 sayılı KVKK Kararı - Belediyelerin Ödeme Ve Borç Sorgulama Hizmetlerine İlişkin Karar
- 2021/1304 sayılı KVKK Kararı - Araç Kiralama Sektöründe Kara Liste Uygulamalarına İlişkin Karar
- 2020/966 sayılı KVKK Kararı - İletişim Bilgilerinin Doğrulanmasına İlişkin Karar
- 2020/481 sayılı KVKK Kararı - Unutulma Hakkı Kararı
- 2020/71 sayılı KVKK Kararı - Veri Sorumlusu ve Veri İşleyenin Tespitinde Göz Önünde Bulundurulması Gereken Hususlar
- 2019/308 sayılı KVKK Kararı - Hukuka Aykırı Verilere Dayalı Sorgulamalara İlişkin Karar
- 2019/271 sayılı KVKK Kararı - Veri İhlal Bildirimi Asgari Unsurlarına İlişkin Karar
- 2019/125 sayılı KVKK Kararı - Yeterli Korumaya Sahip Ülkelerin Belirlenmesinde Esas Alınacak Kriterler
- 2019/10 sayılı KVKK Kararı - Kişisel Veri İhlal Bildirimine İlişkin Karar
- 2018/119 sayılı KVKK Kararı - Ticari İletilere İlişkin Karar
- 2018/63 sayılı KVKK Kararı - Personelin Yetki Aşımına İlişkin Karar
- 2018/10 sayılı KVKK Kararı - Özel Nitelikli Kişisel Verilere İlişkin Yeterli Önlemlere İlişkin Karar
- 2017/62 sayılı KVKK Kararı - Banko, Gişe, Masa gibi Hizmet Alanlarına İlişkin Karar
- 2017/61 sayılı KVKK Kararı - Rehberlik Hizmetleri Veren İnternet Sitelerine İlişkin Karar

**2022/388 sayılı KVKK Kararı - Belediyelerin Ödeme Ve Borç Sorgulama Hizmetlerine İlişkin
Karar**

**Belediyelerin ödeme ve borç sorgulama hizmetleri hakkında Kişisel Verileri Koruma Kurulunun
21/04/2022 Tarihli ve 2022/388 sayılı İlke Kararı**

RG Tarih ve Sayı: 29.04.2022/31824

Karar Tarihi : 21/04/2022

Karar No : 2022/388

Konu Özeti : Belediyelerin ödeme ve borç sorgulama hizmetleri hakkında İlke Kararı

Kişisel Verileri Koruma Kurumuna iletilen çeşitli ihbarlarda belediyelerin çevrimiçi olarak sunmuş olduğu emlak vergisi ödeme/hızlı ödeme veya borç sorgulama sayfalarında yalnızca TC kimlik numarası girilerek vatandaşın emlak bilgilerine ulaşılmasının kişisel verilerin korunması açısından sorun teşkil ettiği ifade edilerek, konunun 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında incelenmesi talep edilmiştir.

Bilindiği üzere Kanununun 12 nci maddesinin (1) numaralı fıkrasında “Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.” hükmünü amirdir. Anılan maddenin (4) numaralı fıkrasında veri sorumluları ile veri işleyen kişilerin öğrendikleri kişisel verileri Kanun hükümlerine aykırı olarak başkasına açıklayamayacağı ve işleme amacının dışında kullanamayacağı; (5) numaralı fıkrasında ise işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunun bu durumu en kısa sürede ilgisine ve Kurula bildireceği, Kurulun, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebileceği hükümlerine yer verilmiştir.

Bu kapsamda, kişisel verilerin işlenmesi sürecinde veri sorumlularının alması gereken teknik ve idari tedbirler konusunda uygulamada açıklık sağlanması ve iyi uygulama örnekleri oluşturması amacıyla Kişisel Verileri Koruma Kurulu tarafından hazırlanarak Kurum internet sayfasında yayımlanan Kişisel Veri Güvenliği Rehberinde (Teknik ve İdari Tedbirler) kişisel verilere gerekli durumlarda

uzaktan erişilmesi halinde iki kademeli kimlik doğrulama kontrolünün uygulanması güvenliğin sağlanması adına alınması gereken tedbirler arasında sayılmaktadır. Bu itibarla kişisel verilere uzaktan erişilmesi halinde 3. kişilerin kolayca ulaşamayacağı şekilde iki aşamalı sorgulama sistemi kullanılması gerekli olup, örneğin kişinin TC kimlik numarası ve doğum günü bilgisinin sorgulanarak erişim imkânı veren sistemler tek kademeli doğrulama olarak belirlenirken, kişinin TC kimlik numarasının yanı sıra kişiye özel oluşturulmuş şifre ya da kişinin daha önce bildirmiş olduğu telefon numarasına iletilen SMS kodu ile erişim sağlanan sistemler iki kademeli doğrulama olarak kabul edilmektedir.

Kişisel Veri Güvenliği Rehberi'nin "Teknik ve İdari Tedbirler Mevcut Risk ve Tehditlerin Belirlenmesi" başlıklı 2.1 maddesinde de "*Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir. Bu riskler belirlenirken; kişisel verilerin özel nitelikli kişisel veri olup olmadığı, mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği, güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği dikkate alınmalıdır. Bu risklerin tanımlanması ve önceliğinin belirlenmesinden sonra; söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmeli, gerekli teknik ve idari tedbirler planlanarak uygulamaya konulmalıdır.*" ifadelerine yer verilmektedir. Buna bağlı olarak kişilerin bilgilerine kolayca erişilmesi riskini barındıran tek kademe doğrulama sistemlerinin yerine bu riski önemli ölçüde azaltacak ya da ortadan kaldıracak iki faktörlü doğrulama yöntemleriyle sorgulamaların uygulamaya konulması önem arz etmektedir.

Bu çerçevede belediyeler tarafından emlak vergisi ödeme/hızlı ödeme veya borç sorgulama vb sayfalar aracılığıyla çevrimiçi olarak sunmuş oldukları hizmetler kapsamında Kanunun 12 nci maddesinde yer alan yükümlülüklerin yerine getirilmesi ve herhangi bir veri ihlalinin önlenmesi amacıyla; çift faktörlü doğrulama için ilk doğrulamanın TC kimlik no, ad soyad, vergi no, sicil no gibi verilerle yapılırken ikincil düzeydeki doğrulamanın kişiye özel oluşturulmuş SMS ya da e-postaya iletilen şifre gibi bir sistemle gerçekleştirilmesi, ikincil düzeyde kişiye ait başkalarının da erişebileceği telefon no, doğum tarihi, anne baba adı, sicil no gibi bilgiler yerine sadece kişiye özel olarak belirlenecek ve sadece ilgili kişinin erişebileceği verilerin istendiği sistemler ya da üyelik sistemi ile söz konusu hizmetlerin sunulmasının uygun olacağı değerlendirilmektedir.

Bu değerlendirmeler ışığında;

- Belediyelerin emlak vergisi ödeme/hızlı ödeme ve borç sorgulama hizmetlerinde üyelik ve şifre ya da çift faktörlü doğrulama kullanmak sureti ile Kanunun 12 nci maddesi kapsamında gerekli teknik ve idari tedbirleri alması gerektiğine,
 - Söz konusu önlemleri almayan belediyeler hakkında iletilecek şikayet/ihbarlar doğrultusunda ilgili belediye hakkında Kanunun 18 inci maddesi hükümleri çerçevesinde işlem tesis edileceği hususunda kamuoyunun bilgilendirilmesine,
 - Belediyelerin emlak vergisi ödeme/hızlı ödeme ve borç sorgulama hizmetlerinde Kanunun 12 nci maddesi kapsamında “üyelik ve şifre” ya da “çift faktörlü doğrulama” kullanılması gerektiği hususunda Kanunun 15 inci maddesinin (6) numaralı fıkrası kapsamında İlke Kararı alınarak Resmi Gazetede ve Kurumun internet sayfasında yayımlanmasına
- oybirliği ile karar verilmiştir.

**2021/1304 sayılı KVKK Kararı - Araç Kiralama Sektöründe Kara Liste Uygulamalarına İlişkin
Karar**

Araç kiralama sektöründeki kara liste uygulamaları hakkında 23/12/2021 Tarihli ve 2021/1304 sayılı İlke Kararı

RG Tarih ve Sayı: 20.01.2022/31725

KURUL KARARI

Kişisel Verileri Koruma Kurumundan:

KARAR

Karar Tarihi : 23.12.2021

Karar No : 2021/1304

Toplantı Sıra Sayısı: 2021/59

Konu Özeti : Araç kiralama sektöründeki kara liste uygulamaları hakkında İlke Kararı

Toplantıya Katılan Üyeler

Başkan : Prof. Dr. Faruk BİLİR

Üyeler : İsmail AYDIN, Bayram ARSLAN, Hasan AYDIN, Şaban BABA, Murat KARAKAYA, Dr. Ayşenur KURTOĞLU, Dr. Cengiz PAŞAOĞLU

Kişisel Verileri Koruma Kurumuna intikal eden ihbarlar kapsamında Kanunun 15'inci maddesi çerçevesinde Kişisel Verileri Koruma Kurulu (Kurul) tarafından yürütülen incelemeler sonucunda araç kiralama sektöründe "kara liste" yazılımlarına/programlarına/uygulamalanna başvurulduğu anlaşılmıştır.

Araç kiralama sektöründe kullanılan bahse konu "kara liste" uygulamaları ile,

- Araç kiralama yazılımcısı ve satıcısı kişilerin araç kiralama firmalarına (veya araç kiralama işi yapan gerçek kişilere) "kara liste" özelliği de içeren araç kiralama yazılımları sundukları,

- Araç kiralama firmaları tarafından söz konusu yazılımlara kendi müşterileri olan araç kiralayan gerçek kişilerin kişisel verilerinin işlendiği; işlenen bu veriler arasında araçların kullanım sürecinde meydana gelen olumsuzlukları veya araç kiralama firmasının yorumlarını da içeren "kara liste" bilgilerinin yer aldığı,

- Bu bilgilerin araç kiralama firmaları tarafından sonraki kiralamalar için karar verirken kullanılmak üzere işlendiği,

- Öte yandan bahse konu yazılımların, bir araç kiralama firmasının kendi girdiği verileri diğer araç kiralama firmalarına da açmasına da olanak veren sistemler olarak tasarlandığı,

- Dolayısıyla araç kiralama firmasından yazılıma, yazılımdan ise söz konusu yazılımı kullanan diğer araç kiralama firmalarına kara listeye ilişkin veri akışı/paylaşımı sağlayan bir sistem oluşturulduğu, araç kiralayan ilgili kişilerin kişisel verilerinin de böylece karşılıklı olarak paylaşılmakta olduğu,

- Genel olarak yazılım şirketleri tarafından sunulan hizmetin, SaaS (Software as a Service) şeklinde olduğu, SaaS hizmetinin gereği olarak veri tabanı ve yazılımın yönetiminin yazılım şirketlerinde olup araç kiralama firmalarında ve gerektiğinde teknik destek ve geliştirme sağlayabilmesi için yazılım şirketlerinde admin yetkisine sahip kullanıcıların atandığı, sunulan hizmet türü hazır bir SaaS hizmeti olduğundan kaynak kod halinde sunulmadığı, araç kiralama firmalarının yazılım kodlarına müdahalesine izin verilmediği, bu sebeple araç kiralama firmalarının yetkilerinin içerik sağlamakla sınırlı olduğu,

- Araç kiralayan bir gerçek kişinin, müşterisi olduğu araç kiralama firmasına kiralama sözleşmesi kapsamında gerekli olan kişisel verilerini sağlarken, bu süreçte firmaya sağladığı verilerin, firma ile yaşadığı olumlu/olumsuz ilişkinin, araca verdiği zarar, ödeme sürecinde yaşanan sorunlar gibi kişisel verilerinin kara liste özelliği içeren yazılımlar vasıtasıyla müşterisi olduğu araç kiralama firması haricinde bilinmeyen sayıda kullanıcı ile paylaşıldığına dair bilgi sahibi olmadığı anlaşılmıştır.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) "Tanımlar" başlıklı 3'üncü maddesinin 1 numaralı fıkrasının (ç) bendinde ilgili kişi, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel veri, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesi, "Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem ", (1) bendinde veri sorumlusu,

“kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi” olarak tanımlanmıştır.

“Kişisel Verilerin İşlenme Şartları” başlıklı Kanun’un 5’inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hükme bağlanmıştır.

Kanunun 8’inci maddesinde “(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz. (2) Kişisel veriler; 5’inci maddenin ikinci fıkrasında, yeterli önlemler alınmak kaydıyla, 6’ncı maddenin üçüncü fıkrasında, belirtilen şartlardan birinin bulunması halinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir. (3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.” hükmü düzenlenmiştir.

Öte yandan, Kanun’un 11 ‘inci maddesi ilgili kişinin haklarını düzenlemekte olup maddenin 1 (g) bendi, "işlenen kişisel verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme" hakkını içermektedir.

Kanunun 12 inci maddesinde ise, veri sorumlularının kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda oldukları hüküm altın alınmıştır.

1774 sayılı Kimlik Bildirme Kanununun ilgili maddeleri gereğince araç kiralama faaliyetinin kolluk kuvvetlerine bildirilme zorunluluğu bulunmaktadır. Dolayısıyla, araç kiralama firmalarının Kiralık Araç Bildirim Sistemine (KABİS) veri girişi yapmaları bağlamında kişisel veri işlemleri, Kanunun 5’inci maddesinin 2 numaralı fıkrasının (a) bendinde yer alan “Kanunlarda açıkça öngörülmesi” işleme şartı ile (ç) bendinde yer alan “veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması” işleme şartları kapsamında değerlendirilebilecektir.

Ayrıca, araç kiralama işi taraflar arasında akdedilen bir sözleşme kapsamında gerçekleştirilmekte olduğundan Kanunun 5'inci maddesinin 2 numaralı fıkrasının (c) bendinde yer alan "bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması" işleme şartı kapsamında ilgili kişilerin kişisel verilerinin araç kiralama firmalarınca işlenmesi mümkündür.

Kara liste benzeri veri kayıtları bakımından ise kişisel verilerin işletme faaliyetleri ile sınırlı olmak üzere işlenmesi ile yazılım firmaları aracılığıyla diğer veri sorumlularına açılmasının farklılık arz edeceği değerlendirilmektedir. Kanun'un 5'inci maddesinin 2 numaralı fıkrasının (f) bendinde "ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" işleme şartı düzenlenmiş olup ilgili kişinin temel hak ve özgürlükleri ile veri sorumlusunun meşru menfaatleri arasında yapılacak denge testi sonucunda meşru menfaatin baskın gelmesi durumunda, işletme faaliyetleri ile sınırlı olmak kaydıyla, başka bir ifadeyle veri sorumlusu bünyesinde olmak üzere kara liste kaydı yapılmasının somut olaya göre ayrıca değerlendirilmek koşuluyla uygulanabilir olabileceği; ancak işlenen kişisel verilerin aynı yazılımı kullanan diğer veri sorumlularına (diğer araç kiralama firmalarına) açılması halinde ilgili kişinin temel hak ve özgürlüklerinin ihlal edilmeme şartının karşılanamayacağı değerlendirilmektedir.

Ayrıca bir araç kiralama firmasının işlediği kişisel verileri yazılım vasıtasıyla bilinmeyen sayıda araç kiralama firması ile paylaşmasının Kanunun 4'üncü maddesinde düzenlenen Genel İlkelerden "hukuka ve dürüstlük kurallarına uygun olma", "belirli, açık ve meşru amaçlar için işleme", "amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerine aykırılık teşkil edeceği değerlendirilmektedir.

Öte yandan, ihbara konu kara liste uygulamalarında araç kiralama firmaları, gerçek kişi müşterilerden kişisel verileri ilk elden toplayan veri sorumlularıdır. Ancak, kara liste kaydına erişimin bir firma ile sınırlı kalmadığı, yazılıma aktarılan kişisel verilere yazılımı kullanan diğer araç kiralama firmalarının da erişim sağlayabildiği ve veri üzerinde hakimiyetleri olduğu dikkate alındığında, kara liste kaydını kendi menfaatleri doğrultusunda kullanan araç kiralama şirketleri ile yazılım şirketlerinin ortak veri sorumluluğunun ortaya çıkacağı değerlendirilmektedir.

Ortak veri sorumlularına ilişkin sorumluluk ve kusur miktarlarının belirlenmesi açısından her halükarda olay bazında veri işleme süreçlerinin incelenmesi; kusurun ve söz konusu veri üzerindeki kontrolün kimde olduğunun tespiti gerekecektir. Ortak veri sorumluları arasında kusurluluk belirlenirken işlenen verinin ilk ve son kullanıcısının kim olduğu; veri girişini kimin yaptığı; hangi amaçla söz konusu verinin girildiği; verinin değiştirilmesine veya silinmesine yahut aktarılmasına

kimin karar verdiđi; veriyi toplayan dıřında kalan veri sorumlularının bu veri ile hangi faaliyetleri gerekleřtirdiđi vb. etkenlere dikkat edilecektir.

Ara kiralama sektöründe kara liste uygulamalarının ilgili kiřinin hakları bakımından da deđerlendirilmesi gerekmektedir. Kara liste kapsamında kiřisel veri iřlenmesi kiřilerin Kanun'un 11 'inci maddesinden kaynaklanan haklarını geređi gibi kullanabilmelerinin önünde engel teřkil edecektir. řöyle ki, bu tür bir veri iřleme kara liste uygulamalarının dođası geređi, kiři hakkında olumsuz bir sonuca ulařılmasını, bu olumsuz sonucun kara listeye iřlenmesini ve kiři hakkında bu olumsuz sonuca göre karar verilmesini içereceđi için, yapılan profillemeye neticesinde ilgili kiři hakkında olumsuz bir sonuç ortaya çıkacak; ancak ara kiralayan ilgili kiřinin kiřisel verilerinin paylařıldıđı diđer ara kiralama firmalarının kim olduđunu bilebilecek durumda olmaması nedeniyle, Kanunun 11 'inci maddesinden kaynaklanan haklarını bu veri sorumluları nezdinde ileri sürebilmesi güçleřecektir.

Tüm bu deđerlendirmeler iřığında;

- Kanunun 4'üncü maddesinde düzenlenen genel ilkelere, Kanun'un 5'inci maddesinde düzenlenen iřleme řartlarına ve Kanunun 8'inci maddesinde düzenlenen aktarıma iliřkin hükümlere aykırı olarak ara kiralama sektöründe kara liste uygulamaları kapsamında kiřisel verilerin iřlenmesi halinde, söz konusu veriler üzerinde hakimiyeti bulunan ara kiralama řirketlerinin yazılım řirketleri ile ortak veri sorumlusu olarak deđerlendirileceklerine,

- Hukuka aykırı bu gibi uygulamalara son verilerek, ara kiralama sektöründe kiřisel veri iřleme süreçlerinin Kanuna uygun olmasını teminen Kanun'un 12'nci maddesinde düzenlenen gerekli teknik ve idari tedbirlerin veri sorumlularınca alınması gerektiđine,

- Söz konusu önlemleri almaksızın ve Kanun hükümlerine aykırı řekilde ara kiralama sektöründe kara liste uygulamasına bařvuran veri sorumluları hakkında Kanunun 18 inci maddesi hükümleri çerçevesinde iřlem tesis edileceđi hususunda kamuoyunun bilgilendirilmesine,

- 6698 sayılı Kiřisel Verilerin Korunması Kanununun 15 inci maddesinin altıncı fıkrası hükmü

uyarınca alman bu İlke Kararının Resmi Gazete ile Kurumun internet sitesinde yayımlanmasına oybirliđi ile karar verilmiřtir.

2020/966 sayılı KVKK Kararı - İletişim Bilgilerinin Doğrulanmasına İlişkin Karar

Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına Kanuna aykırı şekilde gönderilen üçüncü kişilere ait kişisel veriler hakkında Kişisel Verileri Koruma Kurulunun 22/12/2020 Tarihli ve 2020/966 sayılı İlke Kararı

Karar Tarihi : 22.12.2020

Karar No : 2020/966

Konu Özeti : Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına Kanuna aykırı şekilde gönderilen üçüncü kişilere ait kişisel veriler hakkında İlke Kararı

RG Tarih ve Sayı: 15.01.2021/31365

Kişisel Verileri Koruma Kurumuna intikal eden şikâyet ve ihbarlar kapsamında; e-ticaret, telekomünikasyon, ulaşım, turizm gibi muhtelif sektörlerde faaliyet gösteren veri sorumlularınca, fatura, ekstre, rezervasyon belgesi gibi kişisel veri içeren dokümanların sms ve/veya e-posta vasıtasıyla gönderimini teminen ilgili kişilerden telefon numarası ve/veya e-posta adreslerini beyan etmelerinin istenildiği, bununla birlikte ilgili kişiler tarafından söz konusu bilgilerin beyanında yanlışlık olabildiği veya yine ilgili kişilerce üçüncü kişilere ait bilgilerin beyan edilmesi neticesinde, ilgili kişilere ait verileri içeren bahse konu dokümanların üçüncü kişilere iletildiği görülmektedir.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun 4 üncü maddesinin (1) numaralı fıkrasında kişisel verilerin ancak bu kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği hüküm altına alınmış ve (2) numaralı fıkrasında kişisel verilerin işlenmesinde "*a) Hukuka ve dürüstlük kuralına uygun olma b) Doğru ve gerektiğinde güncel olma. c) Belirli, açık ve meşru amaçlar için işlenme. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.*" ilkelerine uyulmasının zorunlu olduğu düzenleme altına alınmıştır.

Bu ilkeler arasında yer alan kişisel verilerin doğru ve gerektiğinde güncel bir şekilde tutulması, veri sorumlusunun çıkarına uygun olduğu gibi ilgili kişinin temel hak ve özgürlüklerinin korunması açısından da gerekli olup, veri sorumlusunun eğer kişisel verilere dayalı olarak ilgili kişiye dair bir sonuç oluşturuyor ve doğruruyorsa kişisel verilerin doğru ve gerektiğinde güncel olmasının

sağlanması noktasında aktif özen yükümlülüğü bulunmaktadır. Bunun dışında veri sorumlusunun her zaman ilgili kişinin bilgilerinin doğru ve gerektiğinde güncel olmasını temin edecek kanalları açık tutması önem arz etmektedir. Aksi takdirde, kişilerin, güncel olmayan veya yanlış tutulan kişisel verileri nedeniyle maddi ve manevi zarar görmesi gündeme gelebilecektir. Bu anlamda, kişisel verilerin doğru ve gerektiğinde güncel tutulabilmesini temin etmek amacıyla; kişisel verilerin elde edildiği kaynakların belirli olması ve kişisel verilerin toplandığı kaynağın doğruluğunun tespit edilmesi ile kişisel verilerin doğru olmamasından kaynaklı ilgili kişiler açısından olumsuz sonuçlar ortaya çıkmasının önlenmesi kapsamında ilgili kişilerce beyan edilen iletişim bilgilerinin doğrulanmasına yönelik (telefon numarası ve/veya e-posta adresine doğrulama kodu/linki gönderilmesi vb.) makul önlemler alınması gerekli görülmektedir.

Öte yandan, Kanunun 12 inci maddesinde veri sorumlularının kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda oldukları hüküm altına alınmıştır.

Bu kapsamda; veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına, 6698 sayılı Kişisel Verilerin Korunması Kanununa aykırılık oluşturacak şekilde üçüncü kişilerin kişisel verilerini içeren ekstre, fatura vb. belgelerin gönderilmesinin önlenmesini teminen; Kanunun 12 nci maddesinin (1) numaralı fıkrası gereğince veri sorumluları tarafından kendilerine bildirilen iletişim bilgilerinin doğruluğunu teyit edecek mekanizmaların oluşturulması adına gerekli idari ve teknik tedbirlerin alınması hususunda Kanunun 15 inci maddesinin 6 numaralı fıkrası uyarınca İlke Kararı alınmasına ve söz konusu İlke Kararının Kurumun internet sayfasında ve Resmi Gazetede ilan edilmesine oybirliği ile karar verilmiştir.

2020/481 sayılı KVKK Kararı - Unutulma Hakkı Kararı

Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına Yönelik Talepler ile ilgili olarak Kişisel Verileri Koruma Kurulunun 23/06/2020 Tarihli ve 2020/481 Sayılı Kararı

Karar Tarihi : 23.06.2020

Karar No : 2020/481

Konu Özeti : Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına Yönelik Talepler

Kurumumuza intikal eden muhtelif başvurularda, ilgili kişilerin medya kuruluşlarına ait çeşitli internet sitelerinde yer alan haberlerde geçen isim ve soy isimlerinin ya da haberlerin 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) hükümleri kapsamında silinmesinin talep edildiği, bunun yanı sıra bazı başvurularda ise söz konusu gazete arşivlerinin arama motorları tarafından indekslenmeyecek şekilde teknik düzenlemeye tabi tutulması hususunda gerekli kararların alınmasının istenildiği görülmekte olup Kurumumuza intikal eden bu yöndeki taleplerin “Unutulma Hakkı” kapsamında bir bütün olarak Kurulumuzca değerlendirilmesi gereği hasıl olmuştur.

Unutulma hakkının çeşitli yargı kararları ve uluslararası kurumların organlarının görüşleri doğrultusunda literatürde, “bireyin geçmişte hukuka uygun olarak yayılmış ve doğru nitelikteki bilgilerinin zamanın geçmesine bağlı olarak erişimden kaldırılmasını ya da gündeme getirilmemesini talep edebilmesi” olarak tanımlandığı görülmektedir.

Bilindiği üzere Anayasa’nın 20 nci maddesine 2010 Anayasa değişikliği ile eklenen “... Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.” hükmü ile bireylere kişisel verilerin silinmesini talep etme hakkı tanınmaktadır.

Öte yandan, Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinde kişisel verilerin işlenmesinde uyulması zorunlu ilkeler arasında doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme ve kişisel verilerin ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi sayılmış, ayrıca Kanunun 11 inci maddesinin birinci fıkrasının (e) bendinde ilgili kişiye kişisel verilerin silinmesini veya yok edilmesini isteme hakkının tanındığı, 7 nci maddesinde ise kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesinin düzenlendiği, mezkur hükümde; Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silineceği, bu hususta diğer kanunlarda yer alan hükümlerin saklı olduğu ve buna ilişkin usul ve esasların ise yönetmelikle düzenleneceğinin hükme bağlandığı görülmektedir.

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik’in 8 inci maddesinde kişisel verilerin silinmesinin kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi olarak tanımlandığı ve veri sorumlusunun bunu sağlamaya yönelik olarak gerekli her türlü teknik ve idari tedbirleri almakla yükümlü olduğu belirtilmektedir.

Diğer taraftan Kanunun yürürlüğe girmesinden önce dahi “unutulma hakkı”nın yargı kararlarına konu olduğu, internet haber arşivinde bulunan bir haberin içeriğinin yayından kaldırılması talebine ilişkin olarak Anayasa Mahkemesi’nin 03.03.2016 tarihli ve 2013/5653 Başvuru Numaralı Kararında, “bireyin geçmişte haber yapılmış ve gerçeğe aykırılığı ileri sürülmemiş davranışlarının artık hatırlanmasının engellenmesi”nin hukuki mesele olarak ortaya konulduğu, internet haber arşivlerindeki kişisel verilere erişimin engellenerek kişilerin yaptıklarının unutulmasının sağlanması yönündeki talebin unutulma hakkı olarak nitelendirildiği, ayrıca kararda; “Başvuru tarihi itibarıyla söz konusu haberin yaklaşık on dört yıl önceki bir olaya ilişkin olduğu ve böylelikle güncelliğini yitirdiği açıktır. İstatistiki ve bilimsel amaçlar yönünden de yukarıda ifade edilen gerekçelerle bu bilgilere internet ortamında kolaylıkla ulaşılmayı gerekli kılan bir neden bulunmamaktadır. Bu bağlamda kamu yararı bakımından siyasi veya medyatik bir kişiliğe sahip olmayan başvurucu hakkında internet ortamında yayınlanan haberlerin kolaylıkla ulaşılabilirliğinin başvurucunun itibarını zedelediği açıktır.” denilmek suretiyle unutulma hakkının nasıl ele alınması gerektiğine ilişkin kriterler belirlenerek haberlerin kişinin Anayasa’nın 17 nci maddesinde güvence altına alınan şeref ve itibarın korunması hakkını ihlal ettiğine karar verilmiştir.

Kararda ayrıca unutulmayı etkin kılacak yöntemlerden de söz edildiği, buna göre, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 9 uncu maddesinde erişimin engellenmesinin kapsamının kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL vb.) içeriğe erişimin engellenmesi yöntemiyle verileceği ve zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemeyeceği belirtilmiş olup buna ek olarak, *"... alınacak tedbirlerin kişinin şeref ve itibarına yönelik müdahaleleri unutulma hakkı gereğince engellemek için arşivde arama yapmaya imkân tanıyan haber ile kişi arasında ilişki kuran kişisel verilerin silinmesi, haberin anonim hâle getirilmesi, haber içeriğinin bir kısmına erişimin engellenmesi gibi birçok yöntem benimsenebilir. Bu bağlamda yargının görevinin, İnternet ortamının sağladığı kolaylıkla zamanla kişilerin itibarına yönelik müdahale oluşturan haberleri tamamen ortadan kaldırarak geçmişte meydana gelmiş olayların yeniden yazulmasını sağlamak olmadığı dikkate alınmalıdır. İnternet haber arşivinin bir bütün olarak basın özgürlüğünün koruması altında olduğu unutulmamalıdır..."* denilmek suretiyle kişisel verilerin silinmesine ve anonim hale getirilmesine yapılan atıfla erişimin kısmi olarak engellenmesi ve kişi ile haber arasında bağlantının koparılması yollarıyla söz konusu hakla basın özgürlüğü arasında nasıl denge kurulabileceğinin gösterildiği, burada Kanunun yürürlüğe girmesinden önce silme ve anonim hale getirmenin unutulma hakkını hayata geçirmeye yönelik bir yöntem olarak ifade edilmesinin önemli olduğu, zira Yüksek Mahkeme kararında unutulma hakkına bir üst kavram olarak yaklaşıldığı, silme ve anonim hale getirmeyi ise bu hakkı tesis etmeye yönelik bir yol olarak sunulduğu anlaşılmaktadır.

Yine davacının isminin rumuzlanmadan bir kitapta yer almasına ilişkin olarak verilmiş olan Yargıtay Hukuk Genel Kurulu'nun 17.06.2015 tarihli E:2014/4-56, K:2015/1679 sayılı Kararında unutulma hakkının; üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerin silinmesini ve yayılmasının önlenmesini isteme hakkı olarak ifade edildiği, bireyin geçmişinde yaşadığı olumsuz etkilerden kurtularak geleceğini şekillendirebilmesinin bireyin yararına olduğu gibi toplumun kalitesinin gelişmişlik seviyesinin yükselmesine de etkisinin tartışılmaz olduğu ifade edilerek unutulma hakkının gereği gibi sağlanmasının bireye faydası olduğu kadar topluma da faydası olduğunun vurgulandığı, bunun da ötesinde kararda unutulma hakkı tanımlarına bakıldığında her ne kadar dijital veriler için düzenlenmiş ise de, bu hakkın özellikleri ve bu hakkın insan haklarıyla arasındaki ilişkisi dikkate alındığında; yalnızca dijital ortamdaki kişisel veriler için değil, kamunun kolayca ulaşabileceği yerde tutulan kişisel verilere yönelik olarak da kabul edilmesi gerektiğinin ifade edildiği görülmektedir.

Unutulma hakkına ilişkin olarak Kanunun yürürlüğe girmesinin ardından verilen Yargıtay 19. Ceza Dairesi'nin 05.06.2017 tarihli E:2016/15510, K:2017/5325 sayılı kararında; bir internet sitesinde yer alan haberin güncellik değerini yitirdiği, dolayısıyla haberin o tarihte "gerçeklik ve doğruluk" kriterlerini karşılamaının artık bir önemi kalmadığı, adı geçen habere istenildiği zaman ulaşılmasının, toplum açısından yanlış algılamaya yol açabileceği, haberin yayında kalmasının toplumun ilerlemesi, gelişmesi için bir katkı sağlamayacağı, kamu yararına toplum hafızasında yer etmesi gibi bir etkisi olmadığı, haberin içeriğini oluşturan kişilerin toplumu temsil ve topluma hizmet etme gayesiyle seçilmiş veya atanmış siyasilerden olmadığı gibi, topluma kendini anlatma ve toplumu aydınlatma gayesiyle eser veren sanatçılardan veya aydınlardan da olmaması nedeniyle suç geçmişlerine dair bilgilerin kamuyu ilgilendirmediği belirtilerek unutulma hakkının ifade ve basın özgürlüğüne üstün tutulduğu, ayrıca kararda Kanuna atıf yapılmasa da unutulma hakkının kişisel verilerin korunması hakkı içinde ele alındığı anlaşılmaktadır.

Uluslararası hukukta unutulma hakkı Birleşmiş Milletler, Avrupa Konseyi ve Avrupa Birliği sistemleri yönünden ele alındığında öncelikle ilk iki sistem içinde mevzuat düzeyinde unutulma hakkının tanımlanmadığı, ancak anılan kurumların mevzuatlarında yer alan özel hayata saygı, şöhretin korunması, kişisel bilgilerin gizliliği gibi bazı haklar üzerinden unutulma hakkına ilişkin sonuçlara ulaşılan kararlara ya da raporlara rastlandığı görülmektedir. Öte yandan;

- Avrupa Birliği Adalet Divanının (ABAD) 2014 yılında verdiği Google İspanya kararında özetle; arama motorunda yapılan aramada çıkan sonuçların "geçersiz, eksik, tamamen ilgisiz veya sonradan ilgisiz hale gelmiş" ise arama motorları tarafından internet ortamına yüklenen amacını aşan söz konusu kişisel verilerin ve buna ilişkin sonuç listesinde yer alan bilgilerin silinmesi gerektiğinin belirtildiği, kararda ayrıca ilke olarak kişinin özel hayatının gizliliği hakkının, arama motorunun ekonomik çıkarı ile söz konusu kişi adına yapılan arama üzerine kamunun bilgiye erişim hakkının diğer bir ifadeyle bilgi alma hakkının üzerinde olduğu, bu kuralın yalnızca kamunun bilgiyi öğrenmede üstün bir yararı bulunmakta ise uygulanmayacağı ifade edildiği,
- 29. Madde Çalışma Grubu'nun ABAD'ın mezkur kararının uygulanmasına ilişkin rehber ilkelerinde de kavramsal olarak "unutulma hakkı"nın kullanılmadığı, burada daha çok indeksten çıkarılma hakkı, arama motoru sonuçlarındaki linklerin gizlenmesi gibi kavramlar üzerinden konunun ele alındığı,
- 25 Mayıs 2018 tarihinde yürürlüğe giren Avrupa Genel Veri Koruma Tüzüğü'nün (Tüzük) "Silme hakkı ("Unutulma Hakkı")" başlıklı 17 nci maddesindeki düzenlemenin incelenmesinden, unutulma hakkının ayrıca tanımlanmadığı ve "silme" yükümlülüğü kapsamında

değerlendirildiği, bu hakkın kullanımı bakımından Kanunun ilgili hükümlerine benzer şekilde veri işleme şartlarının ortadan kalkmış olması durumuna atıfta bulunulduğu ve bu hakkın istisnalarına (yasal yükümlülük, kamu yararına gerçekleştirilen bir görevin yerine getirilmesi, halk sağlığı alanındaki kamu yararı, kamu yararına arşivleme, bilimsel veya tarihi araştırma amaçları, istatistiki amaçlar, yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması) yer verildiği

görülmektedir.

Bu kapsamda, unutulma hakkının uygulanmasında mevzuatımızda kavramsal olarak söz konusu hakka yer verilmese bile hukukumuzda bu hakkı sağlamaya yönelik araçların bulunduğu açık olduğu, bu araçların örneğin, 5651 sayılı Kanunun özel hayatın gizliliği nedeniyle içeriğe erişimin engellenmesi yönündeki düzenlemesi olabileceği gibi Kanunun silmeyi düzenleyen 7 nci maddesi de olabileceği, bu itibarla, yukarıda yer verilen açıklamalardan hareketle, unutulma hakkının, Anayasanın 20 nci maddesinin üçüncü fıkrası hükmü ile 6698 sayılı Kanunun 4 üncü, 7 nci ve 11 inci maddelerinde ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 8 inci maddesinde yer verilen düzenlemelerle iç hukukumuz açısından karşılanabileceği ve ayrı bir hak olarak tanımlanmasına gerek olmadığı; öte yandan unutulma hakkını sağlamaya yönelik olarak veri işleme faaliyetinin durdurulması, silme, yok etme veya anonim hâle getirme ile indeksten çıkarma işleminden somut olaya göre en uygun olan araca karar verilebileceği, zira unutulma hakkı içinde pek çok hakkı barındıran bir üst kavramken, sayılanların bu hakkı tesis etmeye yönelik araçlar olarak ele alındığında Kanunla hedeflenen gayenin gerçekleşmesine de katkı sunulabileceği değerlendirilmektedir.

Bu çerçevede, Kurumumuza intikal eden medya kuruluşlarına ait çeşitli internet sitelerinde yer alan haberlerde yer verilmek suretiyle işlenen kişisel verilerinin kaynaktan silinmesine yönelik başvurular, bu basın organlarının veri sorumlusu olduğu noktasından hareketle Kanunun ilgili hükümleri çerçevesinde Kurulca değerlendirilerek karara bağlanmakla birlikte, kişilerin unutulma hakkı kapsamında ad ve soyadları üzerinden arama motorlarından yapılan aramalarda çıkan sonuçların indeksten çıkarılmasına yönelik talepleri kapsamında Kanunda ve ilgili alt düzenlemelerde herhangi bir açık hükme yer verilmediğinden, bu nitelikteki başvuruların ne şekilde ele alınacağı hususunun değerlendirilmesi gereği ortaya çıkmaktadır.

Yukarıda yer verilen değerlendirmeler çerçevesinde;

- Kurumumuza intikal eden başvurulara konu “Unutulma Hakkı”nın bir üst kavram olarak ele alınmak suretiyle Anayasanın 20 nci maddesinin üçüncü fıkrası hükmü ile 6698 sayılı Kanunun 4

üncü, 7 nci ve 11 inci maddelerinde ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 8 inci maddesinde yer verilen düzenlemeler çerçevesinde değerlendirildiği,

- Yine Kurumumuza yapılan başvurularda yer verilen arama motorlarından ad ve soyadı ile yapılan aramalarda kişinin kendisiyle bağlantılı sonuçlara ulaşılmamasını isteme hakkının indeksten çıkarılma talebi olarak nitelendirildiği,
- Bu kapsamda, arama motorlarının, üçüncü taraflara ait internette topladıkları verilerin işlenmesinin amaç ve vasıtalarını belirledikleri göz önünde bulundurularak Kanunun 3 üncü maddesinde yer verilen tanım çerçevesinde veri sorumlusu olarak kabul edildiği,
- Arama motorunun işletmecisinin otomatik, düzenli ve sistematik olarak internette yayınlanan bilgiyi bulduğu, daha sonra kendi indeksleme programları çerçevesinde alıp, kaydedip, organize ettiği kişisel verileri arama sonuçlarının listesi formunda düzenlediği, sunucuları üzerinde sakladığı, belirli durumlarda açıkladığı ve kullanıcılarına sunduğu dikkate alındığında arama motorları tarafından gerçekleştirilen faaliyetlerin Kanunun 3 üncü maddesi kapsamında ‘kişisel veri işleme’ faaliyeti olarak değerlendirildiği,
- Bu kapsamda, Kanunun başvuru ve şikâyet hakkına ilişkin hükümlerinde belirtilen usul ve süreler esas alınarak ilgili kişilerin, arama sonuçlarının indeksten çıkarılmasına yönelik talepleri ile ilgili olarak öncelikle arama motorlarına başvuruda bulunmaları, veri sorumlusu arama motorlarının söz konusu talepleri reddetmeleri veya başvuru sahibine cevap vermemeleri halinde ilgili kişilerce Kurula şikâyette bulunabilecekleri,
- İlgili kişilerce yapılacak başvurunun şekli ve istenilecek bilgi ve belgelerin arama motorları tarafından belirleneceği,
- İlgili kişinin arama motorları üzerinden kendi adı ve soyadı ile yapacağı bir arama sonucunda gösterilen sonuçların indeksten çıkarılmasına yönelik taleplerin değerlendirilmesinde, ilgili kişinin temel hak ve özgürlükleri ile kamunun söz konusu bilgiyi edinmesinden sağlayacağı menfaatler arasında bir denge testi yapılması, yarışan menfaatlerden hangisinin ağır bastığının gözetilmesi ve bu değerlendirme yapılırken öncelikli olarak aşağıda belirtilen linkte yer verilen açıklamaların dikkate alınması ancak bu konudaki şikâyetlerin değerlendirme sürecinde dikkate alınacak kriterlerin bunlarla sınırlı olmayacağı, her somut olay özelinde Kurulca ilave ölçütlerin de gündeme gelebileceği,
- İlgili kişilerin, arama motorları üzerinden kendi ad ve soyadları ile yapılacak aramalar neticesinde gösterilen sonuçların indeksten çıkarılmasına yönelik taleplerinin veri sorumlusu arama

motorları tarafından reddedilmesi veya taleplerine cevap verilmemesi halinde Kurula başvuruda bulunulurken aynı zamanda doğrudan yargı yoluna başvurularının da mümkün bulunduğu hususlarının kamuoyuna duyurulmasına,

Bu kararda yer alan usul ve esasların arama motoru işleticisi şirketlere bildirilmesi ve ilgili kişilerce internet siteleri üzerinden unutulma hakkının uygulanabilmesini teminen iletişim kanallarının ülkemiz vatandaşları tarafından da kullanılabilmesine yönelik gerekli aksiyonların alınmasının sağlanmasına

karar verilmiştir.

Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına İlişkin Değerlendirmede Dikkate Alınacak Kriterler

Aşağıda yer verilen kriterler Kişisel Verileri Koruma Kurulunca bu yöndeki şikayetlerin değerlendirilmesi sürecinde öncelikli olarak dikkate alınacak kriterler olarak belirlenmiş olup, ihtiyaç duyulması halinde güncellenmeleri söz konusu olabilecektir. Bu kriterlerin veri sorumlularına yapılacak başvuruların değerlendirilmesinde de dikkate alınmasında yarar görülmektedir.

1. İlgili kişi kamusal yaşamda önemli bir rol oynuyor mu?

Sıradan vatandaşlara göre kamusal yaşamda rolü olan vatandaşların bilgilerine erişimde daha fazla kamu yararı olduğu bir gerçektir. Bu anlamda, ilgili kişiye ilişkin internette bulunan arşiv kayıtlarının arama motorlarından bağlantısının kaldırılmasına ilişkin bir değerlendirme yapılırken kişinin kamusal yaşamda ayırt edilebilir bir rolünün olup olmadığının değerlendirilmesi önem arz etmektedir.

İlgili kişinin temel hak ve özgürlükleri ile karşılaştırıldığında arama sonuçlarından elde edilen bilgilere erişimde toplumun daha üstün menfaati olduğunu söyleyebilmek için bir kişinin sahip olması gereken rolü kesin hatları ile tanımlamak zor olabilmektedir. Bununla birlikte, siyasetçilerin, üst düzey kamu yöneticilerinin, iş adamlarının, ünlü sanatçı ve sporcuların, dini liderlerin ve bazı meslekleri icra eden kişilerin kamusal hayatta rol oynadıkları kabul edilmektedir. Ayrıca, açıklamaları ya da eylemleri nedeniyle medyada sıklıkla yer alan kişiler de bu kapsamda değerlendirilebilmektedir.

Kamusal yaşamda rol üstlenen kişilerin adı ile yapılacak aramalar vasıtasıyla ulaşılan sonuçlara erişim sağlanması, söz konusu arama sonuçlarının bu kişilerin profesyonel hayatları açısından

kamunun bilgisine sunulmasını gerektiren bazı bilgileri de içerebileceği ya da toplumu, bazı meslekleri icra eden profesyonellerin uygulamalarından koruyacağı düşünüldüğünden, kamusal yaşamda önemli rolü olan ilgili kişilerin bu kapsamda yapacakları başvuruların kabul görme olasılığı daha düşüktür.

Burada belirtmek gerekir ki, ilgili kişinin özel yaşamı ile ilgili bilgilere ilişkin başvuruların arama sonuçlarından kaldırılma olasılığı daha yüksektir. Bu nitelikteki veriler, kamusal yaşamda rolü olan kişiler hakkında da olsa arama sonuçlarından kaldırılabilir.

2. Arama sonuçlarının öznesi bir çocuk mu?

Bir kişi, kendisine ait bilginin yayımlanması sırasında yasal olarak reşit değilse, söz konusu bilgiye dayalı arama sonuçlarına ilişkin bağlantı kaldırılması talebinin kabul görme olasılığı yüksektir. Nitekim, reşit olmayanlara diğer bir ifade ile çocuklara ilişkin bu yöndeki taleplerin değerlendirilmesinde “çocuğun üstün (yüksek) yararı” ilkesi göz önünde bulundurulmalıdır.

3. Bilginin içeriği doğru mu?

Bilginin doğru olması gerçeğe uygun olması anlamına gelmektedir. Bu noktada, gerçeğin yorumlanması ile gerçeğin paylaşılması arasındaki farka dikkat edilmelidir. Bilginin doğru olmaması ya da yanıltıcı olması bu konudaki başvuruların kabul edilme olasılığını yükseltirken, bilginin doğru ve gerçeklere dayanması da başvuruların kabul edilme olasılığını düşürmektedir. Yayımlanan bilgi gerçeği yansıtmıyorsa ve bu durum ilgili kişi hakkında doğru olmayan ve yanıltıcı bir izlenim edinilmesine neden oluyorsa, söz konusu bilgiye ilişkin bağlantı kaldırılması taleplerinin uygun görülmesi daha olasıdır.

Burada önemle belirtmek gerekir ki, şikayet sahibi ilgili kişi, kendisi hakkında yanlış bir bilgi olduğunu ileri sürüyorsa, bu iddiasını ispat etmesi beklenmektedir.

Öte yandan, bilginin doğruluğu konusunda bir ihtilaf varsa, (örneğin ilgili kişi hakkında devam etmekte olan bir yargılama ya da polis soruşturması olduğunda), süreç tamamlanuncaya kadar bu hususta herhangi bir eylemde bulunulmaması yoluna gidilmesi de mümkündür.

4. Bilgiler kişinin çalışma hayatı ile mi ilgili?

Arama sonuçlarından bağlantı kaldırılmasına yönelik taleplerin değerlendirilmesinde dikkate alınması gereken diğer bir kriter ise bilginin ilgili kişinin iş yaşamı ile mi yoksa özel yaşamı ile mi ilgili olduğudur. Bir kişi ile ilgili tüm veriler kişisel veri olmakla birlikte, o kişiyle ilgili tüm veriler özel değildir. Genel olarak, bilginin ilgili kişinin iş yaşamı ile ilgili olması, bu bilginin arama

motorlarından bağlantısının kaldırılması talebinin kabul edilmesini zorlaştırmakta iken, özel yaşama dair olması bu yöndeki talebinin kabul edilmesinde önemli bir unsur olarak değerlendirilmektedir.

Doğaldır ki kamu hayatında rol oynamayan bir kişinin özel hayatına dair bilgiler alakasız olarak kabul edilmelidir. Bu açıdan bakıldığında kamunun bu bilgilere erişmesinde herhangi bir fayda bulunmadığı dikkate alınarak bu bilgilerin arama sonuçlarında yer almasının gerekli olmadığı değerlendirilebilecektir. Bununla birlikte, yukarıda yer verildiği üzere, belli durumlarda kamuya mal olmuş kişiler de, özel hayatlarına ilişkin bilgilerin yayılmamasını isteme hakkına sahiptirler.

Ancak, burada iki hususa dikkat edilmelidir. İlk olarak, kişinin halihazırda aynı işi yapıp yapmadığı ve ilgili kişinin işine ilişkin yayımlanan verilerin olması gerekenden fazla bilgi içerip içermediği, bu kriterin değerlendirilmesinde ayrıca göz önünde bulundurulmalıdır.

5. Arama sonuçlarında yer alan bilgi ilgili kişi hakkında hakaret, onur kırıcı, iftira niteliği taşıyor mu?

Arama motorunda listelenen sonuçlarda suç niteliği taşıyan kişi hakkında hakaret, nefret söylemi içeren, onur kırıcı ya da aşağılayıcı ifadeler bulunan içeriklerin bağlantılarının kaldırılması hususunda veri sorumlusuna yapılacak başvuruların reddedilmesi halinde Kişisel Verileri Koruma Kuruluna şikayet yoluna gidilmemesi, bu yöndeki başvuruların mahkemeler vasıtasıyla çözüme kavuşturulması daha doğru bir yaklaşım olacaktır.

6. Arama sonuçlarında yer alan bilgi özel nitelikli kişisel veri niteliği taşıyor mu?

Özel nitelikli kişisel veriler (hassas veri) öğrenildiği takdirde kişinin mağdur olabilmesine ya da ayrımcılığa maruz kalmasına neden olabilecek nitelikteki veriler olarak kabul edilmektedir. Bu kapsamda, kişilerin hassas (cinsel hayata, dini inancına, sağlığına ilişkin bilgiler vb) bilgilerinin arama motorlarından bağlantılarının kaldırılmasına yönelik taleplerin kabul görme olasılığı özel nitelikli olmayan kişisel verilere göre daha yüksektir.

Bununla birlikte, kamuya mal olmuş kişilerin özel nitelikli verileri söz konusu olduğunda ise toplumun bu bilgilere erişmedeki menfaatinin ilgili kişinin haklarına üstün gelip gelmediğinin ayrıca değerlendirilmesi gerekebilir.

Bunun yanı sıra özel nitelikli kişisel veri olmamakla birlikte, kişiyi tanımlayıcı bilgileri (adres, telefon numarası, parola vb), mali bilgileri gibi bireyin mahremiyetinin ön plana çıktığı bilgilere ilişkin bu yöndeki taleplerin kabul görme olasılığı da yine yüksek olarak değerlendirilmektedir.

7. Arama sonuçlarında ulaşılan bilgi güncel mi?

Arşiv kayıtlarının arama motorlarından bağlantısının kaldırılmasına yönelik taleplerin değerlendirilmesinde dikkate alınacak kriterlerden bir diğeri de verinin güncel olup olmadığı, başka bir ifade ile verinin yayımlanmasından sonra aradan geçen zamandır. Aradan geçen zaman verinin güncel olma özelliğini yitirmesine neden olabilmekte, ya da bilginin konu ile ilgisi azalabilmektedir. Bu durum da verinin işleme amacı ile olan bağınyı koparabilmektedir. Bu nedenle, aradan geçen zaman indeksten çıkarma taleplerinin kabul edilme ihtimalini artıran bir unsurdur.

Ancak, diğerkriterlerde de olduđu gibi aradan geçen zaman da mutlak bir kural değildir. Örneğın, politikacılara veya kamuoyunca tanınan kişilere ilişkin veriler ya da tarihsel ve bilimsel veriler üzerinde aradan geçen zamanın etkisi sınırlı olacaktır.

8. Arama sonucunda ulaşılan bilgi kişi hakkında önyargıya sebep oluyor mu?

İlgili kişinin arama sonucunda ulaşılan bilginin kendisi hakkında önyargıya sebep olduğunu iddia etmesi hali söz konusu bağlantının arama sonuçlarından kaldırılması yönünde bir talebin değerlendirilmesini gerektirir. Ancak söz konusu iddianın kanıtlanabilir nitelikte olması talebin kabul görme olasılığını artıracaktır.

9. Arama sonucunda yer alan bilgi kişi açısından bir risk doğuruyor mu?

Bir arama sonucu ulaşılan bilgiler kişiyi kimlik hırsızlığı veya takip edilme gibi risklere açık hale getiriyorsa, söz konusu bilgilerin arama motoru listelerinden kaldırılması olasıdır.

10. Bilgi kişinin kendisi tarafından mı yayımlandı?

İlgili kişi tarafından ya da onun açık rızası ile yayımlanan bilgilerin buldukları yerden kendileri tarafından kaldırılması imkanı bulunduğundan, arama sonuçlarından kaldırılmasına yönelik taleplerin kabul görme olasılığı azalmaktadır.

Eğer ilgili kişi bir verinin yayımlanmasına açık rıza vermiş ancak daha sonra kendisine açık rızasını geri alma imkanı tanınmamışsa veya verisinin işlenmemesine ilişkin talebi reddedilmişse, kişiye ilişkin söz konusu bilginin arama sonuçlarından bağlantısının kaldırılmasına yönelik taleplerde bu hususun da değerlendirilmesi gerekmektedir.

11. Orijinal içerik gazetecilik faaliyeti kapsamında işlenen verileri mi kapsıyor?

Bilginin kaynağı ve yayımlanma amacı da kişilerin kendilerine yönelik arama sonuçlarında bağlantılarının kaldırılmasına ilişkin taleplerin değerlendirilmesi sürecinde dikkate alınması gereken önemli bir etkidir.

Nitekim, ifade özgürlüğü çoğulcu ve anayasal demokrasilerin temel taşıdır. İfade özgürlüğü genel hatları ile, düşünce ve bilgiye ulaşma, edindiği fikir ve düşüncelerden dolayı kınanmama, bunları meşru yöntemlerle dışa vurabilme imkan ve serbestisi olarak tanımlanmaktadır.

Basın özgürlüğü de görüş ve düşünceleri, yazılı ve görsel biçimde, basın ve yayın yoluyla, yerli ve yabancı tüm muhataplarına açıklayabilme ve yayabilme hakkı şeklinde kendini gösteren bir temel hak ve özgürlüktür. Basın özgürlüğü kavramı, toplumun bilgiye ulaşması, yorum süzgecinden geçirdikten sonra kendi düşüncelerini ifade edebilmesi açısından ifade özgürlüğü kavramıyla bir bütün halinde değerlendirilmelidir.

Bu bağlamda, haber ve fikirlerin yayılmasını ve bunların kamunun ulaşmasını kolaylaştıran internetin toplum hayatındaki önemli rolü yadsınamaz. İnternet üzerinde arşiv oluşturma, aktüalitenin ve haberlerin saklanmasına ve erişilebilirliğine büyük ölçüde hizmet etmektedir. Bu nitelikteki arşivler özellikle doğrudan halkın erişimine açık ve genelde ücretsiz olmaları nedeniyle tarih eğitimi ve araştırma faaliyetleri için kaynak sunmaktadır. Öte yandan, demokratik bir toplumda basının ilk işlevi olan "gözetleyici" rolünün bir sonucu da arşivlerin halkın erişimine sunulmasıdır.

Bu sebeple Anayasada koruma altına alınan şeref ve itibarın korunmasını isteme hakkı ile basın özgürlüğü ve bu özgürlükle bağlantılı olarak ifade özgürlüğü arasında belli kriterler çerçevesinde bir denge kurulması gerekmektedir. Söz konusu haber ya da düşüncelerin kamu yararına ilişkin bir tartışmaya katkı yapması ya da konu alınan kişinin toplumdaki rol veya fonksiyonu ile röportaj ya da fotoğrafa konu faaliyetin niteliği bu kriterlere örnek gösterilebilir.

Bu kapsamda, kamunun arama sonuçlarına erişiminin sağlanması önemli olmakla birlikte, başkalarının özel ve aile hayatlarının korunması için konulan sınırların da aşılması gerekmektedir. Bu durumlarda, gazetecilik içeriğiyle ilgili olarak arama sonuçlarının kaldırılması da mümkün olabilecektir. Dolayısıyla, her bir şikayet özelinde yarışan menfaatler arasında bir değerlendirme yapılması gerekliliği gündeme gelecektir.

12. İlgili kişiye ilişkin bilgilerin yayımlanmasında yasal bir zorunluluk var mı?

Bir kamu kurumu ya da yasal bir zorunluluk nedeniyle kendisine yetki tanınan kuruluşlar tarafından belirli bir verinin yayımlanması zorunluluğu varsa ve bu zorunluluk geçerliliğini sürdürüyorsa, bu durum ilgili kişinin kendisi ile ilgili arama sonuçlarının kaldırılması yönündeki talebinin değerlendirilmesinde olumsuz bir etken olarak görülecektir. Bununla birlikte, her olayda konunun ayrıca değerlendirilmesi gerekliliği unutulmamalıdır.

13. İlgili kişiye ilişkin bilgi ceza gerektiren bir suçla mı ilgili?

Çok zaman önce meydana gelen göreceli olarak küçük suçlarla ilgili arama sonuçlarının listelerden bağlantılarının kaldırılmasına yönelik taleplerin, daha yakın zamanlarda meydana gelen daha ciddi olanlarla ilgili sonuçların listelerden bağlantılarının kaldırılmasına yönelik taleplere göre kabul görme olasılığı daha yüksektir. Ancak, bu kriter kesin bir kural şeklinde algılanmamalı ve her somut olay özelinde dikkatle incelenerek ele alınmalıdır.

**2020/71 sayılı KVKK Kararı - Veri Sorumlusu ve Veri İşleyenin Tespitinde Göz Önünde
Bulundurulması Gereken Hususlar**

Veri sorumlusu ve veri işleyenin tespitinde göz önünde bulundurulması gereken hususlar ile aydınlatma yükümlülüğünün kim tarafından yerine getirileceğine ilişkin Kişisel Verileri Koruma Kurulunun 30/01/2020 tarihli ve 2020/71 sayılı Karar Özeti

Karar Tarihi : 30.01.2020

Karar No : 2020/71

Konu Özeti : Veri sorumlusu ve veri işleyenin tespitinde göz önünde bulundurulması gereken hususlar ile aydınlatma yükümlülüğünün kim tarafından yerine getirileceği

1. Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 3 üncü maddesinin birinci fıkrasının (1) bendi uyarınca veri sorumlusu; “kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi”yi ifade etmektedir. Bu çerçevede, kişisel verilerin işlenmesine ilişkin kararları alma, işleme faaliyetinin amacı, bu faaliyetin ne zaman başlayacağı kimler tarafından gerçekleştirileceği ve benzeri hususlarda karar verme yetkisi veri sorumlusuna aittir. Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen veri sorumlusu, veri işleme faaliyetinin temel araçlarını ve amaçlarını; veri işleminin “neden” ve “nasıl” olacağını belirlemektedir. Diğer bir deyişle, teknik ve organizasyona ait araçların belirlenmesi, veriye kimin erişeceği, hangi verilerin işleneceği, bu verilerin ne kadar süre tutulacağı, ne şekilde saklanacağı gibi veri işlemeye ilişkin temel unsurlar veri sorumlusu tarafından belirlenmektedir. Bununla birlikte veri sorumlusu, kişisel verilerin korunmasına yönelik mevzuata uyumla ilgili tedbirlerin alınmasından, veri işleyeni denetimden ve ilgili kişilerin haklarını kullanabilmesini sağlamaktan sorumludur. Veri sorumlusunun özerk ve bağımsız olması da önem arz etmektedir. Veri sorumlusu kimseden emir ve talimat almayan, bilakis bir başka kişiye veri işletmesi halinde bu hususta emir ve talimat veren, veri işleme süreçlerinin her anında serbestçe karar verme yetkisine sahip olan gerçek veya tüzel kişilerdir.

29’uncu Madde Çalışma Grubu’nun veri sorumlusu ve veri işleyene yönelik yayınlamış olduğu 1/2010 sayılı tavsiye kararı uyarınca da veri sorumlusunun belirlenmesine yönelik çeşitli kriterler

getirilmiştir. Benzer şekilde, Avrupa Veri Koruma Denetmeni tarafından 7 Kasım 2019 tarihli “2018/1725 Numaralı Tüzük Kapsamında Veri Sorumlusu, Veri İşleyen ve Müşterek Veri Sorumlusu Kılavuzu” yayımlanmıştır. Bu kılavuz, 29’uncu Madde Çalışma Grubu tavsiye kararı ile de örtüşmektedir. İlgili düzenlemelerde de Kanunla benzer veri sorumlusu tanımı yapılarak veri sorumlusu kavramı irdelenmiştir. Sayılan ulusal ve Avrupa Birliğinde mevcut tüm düzenlemelerin değerlendirilmesi ışığında, veri sorumlusunun tespiti için aşağıdaki hususlara kimin karar verdiği belirleyici olmakta, bu kapsamda söz konusu kriterlerin çoğunu gerçekleştirenler, veri sorumlusu olarak değerlendirilmektedir.

- Kişisel verilerin toplanması ve toplama yöntemi,
- Toplanacak kişisel veri türleri,
- Hangi bireylerin kişisel verilerinin toplanacağı,
- Kişisel verinin işlenmesine ve kimin işleyeceğine karar verme,
- İşleme faaliyetinin temel unsurlarına karar verme (hangi kişisel verilerin toplanacağı, toplanan verilerin hangi amaçlarla kullanılacağı ve ne şekilde işleneceği, verilerin ne kadar süreyle saklanacağı, veri saklama politikasının ne şekilde olacağı, verilere kimlerin erişme yetkisi olacağı, alıcıların kim olacağı gibi hususlar işlemenin temel unsurlarına örnek olarak gösterilebilir)
- Toplanan verilerin paylaşılıp paylaşılmayacağı, paylaşılacaksa kiminle paylaşılacağı,
- Kişisel verilerin işlenmesinde üst düzeyde, herhangi bir emir ve talimat almadan karar verebilme,
- İlgili kişilerle doğrudan muhatap olma,
- Kendi adına veri işleme faaliyetini yürütecek bir veri işleyen atama,
- İşleme faaliyetinden menfaat sağlama.

2. Veri işleyen ise, Kanunun 3 üncü maddesinin birinci fıkrasının (ğ) bendinde “Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi” olarak tanımlanmıştır. Veri işleyenin faaliyetleri, veri işlemenin daha çok teknik kısımları ile ilgilidir. Kişisel verilerin işlenmesine ilişkin kararların alınması yetkisi ise veri sorumlusuna aittir. Veri işleyen, veri sorumlusu adına kişisel verileri işlemekte olup, veri sorumlusunun belirlemiş olduğu temel amaç ve araçlar ve veri sorumlusunun verdiği yetki doğrultusunda veri işleme faaliyetini gerçekleştirmektedir. Diğer bir deyişle veri işleyen, veri sorumlusunun çıkarlarını gözetken, kendisine verilen belirli görevleri aldığı talimatlar doğrultusunda yerine getirmekle yükümlü olan taraftır. Bu

çerçevede, veri işleyen verileri hukuka uygun olarak işlemesi veri sorumlusunun vermiş olduğu emir ve talimatlara uyduğu ölçüde gerçekleşecektir.

Belirtmekte fayda görülmektedir ki, veri sorumlusunun yetki vermesi halinde, veri işleyen veri işleme faaliyetleri esnasında önemli ölçüde bir özerkliğe sahip olabilir ve bu doğrultuda işleme faaliyetinin temel olmayan öğelerini de tanımlayabilir. Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi veri işleyen tarafından işlenmesi halinde; alınan her türlü teknik ve idari tedbirler hususunda bu kişilerle birlikte müştereken sorumludur. Bununla birlikte veri sorumlusu, yapacağı kişisel veri işleme sözleşmesi ile;

- Kişisel verilerin toplanması için hangi bilgi teknolojileri sistemlerinin veya diğer metotların kullanılacağı,
- Kişisel verilerin hangi yöntemle saklanacağı,
- Kişisel verilerin korunması için alınacak güvenlik önlemlerinin detayları,
- Kişisel verilerin aktarımının hangi yöntemle yapılacağı,
- Kişisel verilerin saklanmasına ilişkin sürelerin doğru uygulanabilmesi için kullanılacak metot,
- Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi yöntemleri

hususlarında karar verme yetkisini veri işleyene bırakabilir. Yani, özellikle bazı teknik konularda veri sorumlusunun menfaatlerine bağlı kalmak ve talimatlarına uymak koşuluyla, veri işleyen de bazı konularda karar verme yetkisini haiz olabilir. Diğer taraftan, veri işleyen için genel itibariyle;

- Kişisel veri işlemek için başkasından talimat alınması,
- Kişisel verilerin kişilerden toplanması sürecinde karar verme yetkisine sahip olmamak,
- Kişisel verilerin kullanım amaçlarının belirlenmemesi,
- Verilerin ne şekilde ifşa olabileceğine, kimlerin bu verilere erişebileceğine karar verme yetkisine sahip olmamak,
- Veri saklama sürecine karar verme yetkisine sahip olmamak,
- Veri işlemenin sonuçlarından sorumlu olmaması,
- Veri sorumlusu ile yapılacak sözleşme gibi yasal bağlayıcılığı olan anlaşmalar çerçevesinde veri sorumlusunun verdiği yetkiler çerçevesinde kişisel verilerin işlenmesine yönelik birtakım karar verme mekanizmalarının söz konusu olup olmadığı

hususları değerlendirilmek suretiyle yukarıda sayılanların çoğunun bulunması halinde veri işleme faaliyetini gerçekleştiren veri işleyen olarak kabul edilecektir.

3. Öte yandan, Kanunun muhtelif hükümlerinde veri sorumlusuna birtakım yükümlülükler getirilmiştir. Bu yükümlülükler başlıca “*aydınlatma yükümlülüğü, veri güvenliğine ilişkin yükümlülükler, ilgili kişiler tarafından yapılan başvuruların cevaplanması ve Kişisel Verileri Koruma Kurulunun (Kurul) kararlarının yerine getirilmesi yükümlülüğü, veri sorumluları siciline kaydolma yükümlülüğü*” olarak sayılabilir. Kanun koyucu kişisel verileri işlenen ilgili kişilere bu verilerinin kim tarafından, hangi amaçlarla ve hukuki sebeplerle işlenebileceği, kimlere hangi amaçlarla aktarılabilirliği hususunda bilgi talep etme hakkı tanımakta ve bu hususları, veri sorumlusunun aydınlatma yükümlülüğü kapsamında ele almaktadır. Buna göre veri sorumlusu, Kanunun 10 uncu maddesi çerçevesinde kişisel verilerin elde edilmesi sırasında **bizzat veya yetkilendirdiği kişi aracılığıyla** aşağıdaki bilgileri ilgili kişiye sağlamakla yükümlüdür:

- Veri sorumlusunun ve varsa temsilcisinin kimliği,
- Kişisel verilerin hangi amaçla işleneceği,
- Kişisel verilerin kimlere ve hangi amaçla aktarılabilirliği,
- Kişisel veri toplamanın yöntemi ve hukuki sebebi,
- 11 inci maddede sayılan diğer hakları.

Veri Sorumluları Siciline kayıt yükümlülüğünün bulunması durumunda aydınlatma yükümlülüğü çerçevesinde ilgili kişiye verilecek bilgiler, Sicile açıklanan bilgilerle uyumlu olmalıdır. Aydınlatma yükümlülüğünün yerine getirilmesi, ilgili kişinin onayına tabi değildir. Tek taraflı bir beyanla aydınlatma yükümlülüğü yerine getirilebilir. Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı ise veri sorumlusuna aittir. Ayrıca belirtmek gerekir ki, Kanunun 10 uncu maddesinde yer alan aydınlatma yükümlülüğü “*Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ*” (**Aydınlatma Tebliği**) hükümlerine uygun olarak yerine getirilmelidir. Her ne kadar aydınlatma yükümlülüğü veri sorumlusuna ait olsa da veri işleyene verdiği talimatlar doğrultusunda veri işleyen tarafından da aydınlatma yükümlülüğünün yerine getirilebileceği değerlendirilmektedir. Nitekim, Kanunun 10 uncu maddesinde “*kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi aracılığıyla*” denilmek suretiyle veri sorumlusuna aydınlatma yükümlülüğü konusunda iki seçenek tanınmıştır. Diğer bir deyişle, aydınlatma yükümlülüğünün bizzat veri sorumlusu tarafından mı yoksa yetkilendireceği kişi tarafından mı yerine getirileceği konusunda Kanun, veri sorumlusuna seçim hakkı tanımıştır.

Sonu olarak; Kanunun 10 uncu maddesinde dzenlenen “aydınlatma ykmllğ” bizzat veri sorumlusu tarafından veya veri sorumlusunun yetkilendirdiğ bir kiři tarafından yerine getirilebilir. Veri sorumlusu tarafından yetkilendirilen kiři de veri iřleyen olabilir.

2019/308 sayılı KVKK Kararı - Hukuka Aykırı Verilere Dayalı Sorgulamalara İlişkin Karar

Hukuka Aykırı Olarak Elde Edilen Veriler Üzerinden Vatandaşların Kimlik ve İletişim Bilgileri Gibi Kişisel Verilerinin Sorgulanmasına İmkân Tanıyan Yazılım/Program/Uygulamalara Yönelik Kişisel Verileri Koruma Kurulunun 18/10/2019 Tarihli ve 2019/308 Sayılı İlke Kararı

Karar Tarihi : 18.10.2019

Karar No : 2019/308

Konu Özeti : Hukuka Aykırı Olarak Elde Edilen Veriler Üzerinden Vatandaşların Kimlik ve İletişim Bilgileri Gibi Kişisel Verilerinin Sorgulanmasına İmkân Tanıyan Yazılım/Program/Uygulamalar Hakkında

RG Tarih ve Sayı: 21.11.2019/30955

Kişisel Verileri Koruma Kurumuna intikal eden ihbarlar kapsamında avukatlar/hukuk büroları ile finans, gayrimenkul danışmanlık, sigorta vb. sektörlerde faaliyet gösteren bazı kişi ve kuruluşlar tarafından muhtelif yollarla elde edilen veriler üzerinden vatandaşların kimlik ve iletişim bilgileri gibi kişisel verilerinin sorgulanmasına imkân tanıyan yazılım/program/uygulamaların kullanılmakta olduğu tespit edilmiştir. Yapılan değerlendirme sonucunda bu durumun, 6698 sayılı Kişisel Verilerin Korunması Kanununun veri sorumlularının veri güvenliğine ilişkin yükümlülüklerini düzenleyen 12 nci maddesi hükümlerine aykırılık oluşturduğu dikkate alınarak, yaşanabilecek veri güvenliği ihlallerinin önüne geçilmesini teminen;

- Bu mahiyetteki yazılımları/programları/uygulamaları kullandığı tespit edilenler hakkında Türk Ceza Kanunu kapsamında gerekli adli işlemlerin tesisi için konunun, 5271 sayılı Ceza Muhakemesi Kanununun 158 inci maddesi hükmü uyarınca ihbaren ilgili Cumhuriyet Başsavcılıklarına bildirileceği,

- Kişisel Verileri Koruma Kurulunun görev alanına giren yönüyle de veri sorumluları hakkında 6698 sayılı Kişisel Verilerin Korunması Kanununun 18 inci maddesi hükmü çerçevesinde idari işlem tesis edileceği hususlarında kamuoyunun bilgilendirilmesine,

- 6698 sayılı Kişisel Verilerin Korunması Kanununun 15 inci maddesinin altıncı fıkrası hükmü uyarınca alınan bu ilke kararının Resmi Gazete ile Kurumun internet sitesinde yayımlanmasına

oybirliđi ile karar verilmiřtir.

2019/271 sayılı KVKK Kararı - Veri İhlal Bildirimi Asgari Unsurlarına İlişkin Karar

Veri sorumlusu tarafından ilgili kişiye yapılan veri ihlali bildiriminde yer alması gereken asgari unsurlara ilişkin, Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararı

Karar Tarihi : 18.09.2019

Karar No : 2019/271

Konu Özeti : Veri sorumlusu tarafından ilgili kişiye yapılan veri ihlali bildiriminde yer alması gereken asgari unsurlara ilişkin, Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararı

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrasında veri sorumlusunun;

- a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
- c) Kişisel verilerin muhafazasını sağlamak

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu, (5) numaralı fıkrasında ise, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunun bu durumu en kısa sürede ilgisine ve Kurula bildireceği, Kurulun, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebileceği hükme bağlanmıştır.

Kişisel Verileri Koruma Kurulunun (Kurul) 24.01.2019 tarih ve 2019/10 sayılı kararı ile veri ihlali bildiriminin “Veri sorumlusunca söz konusu veri ihlalden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabilirse doğrudan, ulaşamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılmasına” karar verilmiştir.

Söz konusu hüküm ve Kurul kararı kapsamında Kuruma intikal eden veri ihlal bildirimlerinin değerlendirilmesi sürecinde; kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde veri sorumlusunun bu durumu Kurula ve ihlalden etkilenmiş kişilere bildirmesinde

amacın, ihlal nedeniyle bu kişiler hakkında ortaya çıkabilecek olumsuz sonuçların bir an önce önüne geçilmesi veya en aza indirilmesine imkan verecek önlemler alınmasını sağlamak olduğu dikkate alındığında veri sorumlularının söz konusu ihlale ilişkin ilgili kişilere yapacağı bildirimlerde hangi unsurların bulunması gerektiğinin açıkça düzenlenmesi gerekliliği doğmuştur.

Bu kapsamda Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararı ile;

Veri sorumlusu tarafından ilgili kişiye yapılacak olan ihlal bildiriminin açık ve sade bir dille yapılması ve asgari olarak;

- İhlalinin ne zaman gerçekleştiği,
- Kişisel veri kategorileri bazında (kişisel veri / özel nitelikli kişisel veri ayrımı yapılarak) hangi kişisel verilerin ihlalden etkilendiği,
- Kişisel veri ihlalinin olası sonuçları,
- Veri ihlalinin olumsuz etkilerinin azaltılması için alınan veya alınması önerilen tedbirler,
- İlgili kişilerin veri ihlali ile ilgili bilgi almalarını sağlayacak irtibat kişilerinin isim ve iletişim detayları ya da veri sorumlusunun web sayfasının tam adresi, çağrı merkezi vb. iletişim yolları

unsurlarına yer verilmesi gerektiğine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2019/125 sayılı KVKK Kararı - Yeterli Korumaya Sahip Ülkelerin Belirlenmesinde Esas Alınacak Kriterler

Yeterli Korumaya Sahip Ülkelerin Belirlenmesinde Esas Alınacak Kriterler

Karar Tarihi : 02.05.2019

Karar No : 2019/125

Konu Özeti : Yeterli korumanın bulunduğu ülkelerin tayininde kullanılmak üzere oluşturulmuş form

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 9 uncu maddesinde; kişisel verilerin, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamayacağı, kişisel verinin aktarılacağı yabancı ülkede yeterli korumanın bulunması veya yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kişisel Verileri Koruma Kurulunun (Kurul) izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın söz konusu verilerin yurt dışına aktarılacağı düzenlenmiştir. Ayrıca maddede yeterli korumanın bulunduğu ülkelerin Kurulca belirlenerek ilan edileceği ve söz konusu ülkelerin ilanında değerlendirilecek hususlar hüküm altına alınmıştır.

Bu kapsamda Kanunun 9 uncu maddesi uyarınca yeterli korumanın bulunduğu ülkelerin Kurulca belirlenmesinde kullanılmak üzere Kurulun 02/05/2019 tarih ve sayılı 2019/125 sayılı Kararında kabul edilen ilgili kriterlere aşağıda belirtilen bağlantı üzerinden erişim sağlanabilir.

Yeterli Korumaya Sahip Ülkelerin Belirlenmesinde Esas Alınacak Kriterler

YETERLİ KORUMAYA SAHİP ÜLKELERİN BELİRLENMESİNDE ESAS ALINACAK KRİTERLER

İNCELENEN ÜLKE:			
İNCELENEN ÜLKENİN İLGİLİ KURULUŞU:			
DEĞERLENDİRME			
KRİTERLER	VAR	YOK	AÇIKLAMA
1. Karşılıklılık durumu			
2. İlgili ülkenin kişisel verilerin işlenmesine ilişkin mevzuatı ve uygulanması			
2.1. Kişisel verilerin korunmasının Anayasal bir hak olması			
2.2. Kişisel verilerin korunmasına ilişkin temel bir kanunun bulunması			
2.3. Temel Kanunun yürürlük tarihi			
2.4. İkincil düzenlemeler ve bu düzenlemelerin ülkemiz mevzuatıyla uyumu			
2.5. Kişisel verilerin korunmasına ilişkin temel kavramlar			
2.6. Kişisel Verilerin Korunması ile ilgili Genel İlkeler			
2.7. Kişisel veri işleme şartlarının 6698 sayılı Kanunda yer alan kişisel veri işleme şartları ile uyumu			
2.8. Özel nitelikli kişisel verilerin işlenmesi konusunda özel işleme şartlarının ve ek güvenlik tedbirlerinin bulunması			
2.9. Kişisel veri işleme faaliyetinin şeffaflık ilkesine uygun olarak gerçekleştirildiğine yönelik hukuki teminatların varlığı			
2.10. Kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek ile kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirlerin alınması zorunluluğu			
2.10.1. Teknik tedbirler			
2.10.2. İdari Tedbirler			
2.11. Veri ihlallerine karşı idari ve/veya cezai yaptırımların uygulanma durumu ile veri ihlallerinin önüne geçilmesini sağlayacak diğer mekanizmalar			
2.12. İlgili kişinin hakları			
2.13. İlgili kişilerin veri sorumlusuna başvuru hakkı ve veri koruma otoritesine şikâyet hakkı			
2.14. Kişisel veriler ile ilgili hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı bulunması			
2.15. Referans niteliğinde uygulamaya ilişkin rehberler/yayınlar			

2.16. Kanunun uygulanmasına ilişkin istisnalar			
2.17. Veri aktarım sistemi			
3. Bağımsız veri koruma otoritesinin bulunması			
3.1. Yapısı			
3.2. Bağımsızlık durumu			
3.3. Görev ve yetkileri			
3.4. Denetim/inceleme yetkisi			
3.5. Kararlarına karşı başvuru yolunun bulunup bulunmadığı			
4. Kişisel verilerin korunması ile ilgili uluslararası antlaşmalara taraf olma ile uluslararası kuruluşlara üye olma durumu			
4.1. 108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi			
4.2. 181' No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınırşan Veri Akışına İlişkin Protokol			
4.3. Ceza İşlerinde Karşılıklı Yardım Avrupa Sözleşmesine Ek 2'nci Protokol (CETS 182)			
4.4. Avrupa İnsan Hakları Sözleşmesi			
4.5. International Conference of Data Protection and Privacy Commissioners (ICDPPC)			
4.6. Global Privacy Enforcement Network (GPEN)			
5. Ülkemizin üye olduğu küresel ve bölgesel örgütlere üye olma durumu			
6. İlgili ülke ile yürütülen ticaret hacmi			
7. Diğer			

2019/10 sayılı KVKK Kararı - Kişisel Veri İhlal Bildirimine İlişkin Karar

Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 Tarih ve 2019/10 Sayılı Kararına İlişkin Duyuru

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrasında veri sorumlusunun;

- a. Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- b. Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
- c. Kişisel verilerin muhafazasını sağlamak

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu, (5) numaralı fıkrasında ise, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunun bu durumu en kısa sürede ilgisine ve Kişisel Verileri Koruma Kuruluna (Kurul) bildireceği, Kurulun, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebileceği hükme bağlanmıştır.

Veri ihlal bildirimlerinde, Kurula ve ihlalden etkilenmiş kişilere bildirim yapılmasındaki amacın, ihlal nedeniyle bu kişiler hakkında ortaya çıkabilecek olumsuz sonuçların bir an önce önüne geçilmesi veya en aza indirilmesine imkan verecek önlemler alınmasını sağlamak olduğu, öte yandan 6698 sayılı Kanuna kaynak teşkil eden Avrupa Birliğinin 95/46/EC sayılı Direktifini ilga eden Avrupa Genel Veri Koruma Tüzüğünde de veri ihlal bildirimlerine ilişkin olarak Direktifin aksine detaylı düzenlemelere yer verildiği dikkate alındığında Kurul tarafından bu konuda alınacak kararlar arasında herhangi bir uyumsuzluğa mahal verilmemesi ve uygulamada bir standartlaşma sağlanabilmesini teminen; Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararı ile;

- Kanunun 12 nci maddesinin (5) numaralı fıkrasının “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir....” hükmünde yer alan “en kısa sürede” ifadesinin 72 saat olarak yorumlanmasına ve bu kapsamda veri sorumlusunun bu durumu öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirmesine, veri sorumlusunca söz konusu veri ihlalden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre

içerisinde, ilgili kişinin iletişim adresine ulaşılabilirse doğrudan, ulaşamazsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılmasına,

- Veri sorumlusu tarafından Kurula haklı bir gerekçe ile 72 saat içinde bildirim yapılamaması halinde, yapılacak bildirimle birlikte gecikmenin nedenlerinin de Kurula açıklanmasına,
- Kurula yapılacak bildirimde aşağıda yer verilen “Kişisel Veri İhlal Bildirim Form”unun kullanılmasına,
- Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bu bilgilerin gecikmeye mahal verilmeksizin aşamalı olarak sağlanmasına,
- Veri sorumlusu tarafından veri ihlallerine ilişkin bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurulun incelemesine hazır halde bulundurulmasına,
- Veri işleyen nezdinde bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri işleyen bu konuda herhangi bir gecikmeye yer vermeksizin veri sorumlusuna bildirimde bulunmasına,
- Veri ihlalinin yurtdışında yerleşik veri sorumlusu nezdinde yaşanması halinde, bu ihlalin sonuçlarının Türkiye’de yerleşik ilgili kişileri etkilemesi ve ilgili kişilerin sunulan ürün ve hizmetlerden Türkiye’de faydalanmaları durumunda, bu veri sorumlusu tarafından da aynı esaslar çerçevesinde Kurula bildirimde bulunulmasına,
- Veri ihlali gerçekleşmesi halinde veri sorumlusu tarafından kendi nezdinde kimlere raporlama yapılacağı, Kanun kapsamında yapılacak bildirimler ile veri ihlalinin olası sonuçlarının değerlendirilmesi hususunda, kendi nezdindeki sorumluluğun kimde olduğunun belirlenmesi gibi konuları içeren bir veri ihlali müdahale planı hazırlanarak belirli aralıklarla bu planın gözden geçirilmesine

karar verilmiştir.

Kişisel Veri İhlali Bildirim Formu

Kamuoyuna saygıyla duyurulur.

Not: Veri İhlali Bildirim formu yalnızca Veri Sorumlusu tarafından doldurulması gerekmektedir. Şikayet ve İhbar içerikli başvuruların Kurumumuza yazılı olarak veya <https://sikayet.kvkk.gov.tr> adresinden iletilmesi gerekmektedir.

2018/119 sayılı KVKK Kararı - Ticari İletilere İlişkin Karar

Kişisel Verileri Koruma Kurulunun 16/10/2018 Tarihli ve 2018/119 Sayılı İlke Kararı

Karar Tarihi : 16.10.2018

Karar No : 2018/119

Konu Özeti : Veri sorumluları ve veri işleyenler tarafından ilgili kişilerin e-posta adreslerine veya SMS ya da çağrı ile cep telefonlarına reklam bildirimleri/aramaları yönlendirilmesinin önüne geçilmesini teminen ilke kararı alınması

RG Tarih/Sayı : 01.11.2018/30582

6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) hükümlerine aykırı olarak ilgili kişilerin açık rızaları alınmaksızın e-posta adreslerine veya SMS veya çağrı ile cep telefonlarına reklam bildirimleri/aramaları geldiği hususunda Kişisel Verileri Koruma Kurumuna (Kurum) intikal eden çok sayıda başvuru ile bu kapsamda yürütülmekte olan incelemeler çerçevesinde ulaşılan tespitler dikkate alınarak;

- İlgili kişilerin rızalarını almadan veya Kanunun 5 inci maddesinin (2) numaralı fıkrasında hüküm altına alınan işleme şartlarını sağlamadan, telefon numaralarına SMS göndermek, arama yapmak veya e-posta adreslerine posta göndermek suretiyle reklam içerikli ileti yönlendiren veri sorumluları ile veri sorumluları adına reklam içerikli mesaj/e-posta göndermek veya arama yapmak amacıyla ilgili kişilerin açık rızaları bulunmaksızın bu verileri kullanan veri işleyenlerin söz konusu veri işleme faaliyetlerini Kanunun 15 inci maddesinin (7) numaralı fıkrası uyarınca derhal durdurması gerektiği,
- Kanunun 12 nci maddesi kapsamında veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu ve kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, anılan tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumlu olduğu,
- Belirtilen şekilde söz konusu faaliyetlerde bulunan veri sorumluları hakkında Kanunun 18 inci maddesi hükümleri çerçevesinde işlem tesis edileceği,

- Bahse konu şekilde işlenen kişisel verilerin hukuka aykırı olarak elde edilmiş olabileceği de göz önüne alınarak 5237 sayılı Türk Ceza Kanununun “Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme” başlıklı 136 ncı maddesi çerçevesinde ilgili veri sorumluları hakkında gerekli hukuki işlemlerin tesisi için konunun 5271 sayılı Ceza Muhakemesi Kanununun 158 inci maddesi uyarınca ihbaren ilgili Cumhuriyet Başsavcılığına bildirileceği

hususlarında kamuoyunun bilgilendirilmesine ve bu İlke Kararının Kurumun internet sitesi ile Resmi Gazetede yayımlanmasına oy birliği ile karar verilmiştir.

2018/63 sayılı KVKK Kararı - Personelin Yetki Aşımına İlişkin Karar

Veri sorumlusu nezdindeki kişisel verilere erişim yetkisi bulunan personelin yetkisi ve amacı dışında söz konusu verileri işlemesi hususunun değerlendirilmesine ilişkin 31/05/2018 tarih ve 2018/63 sayılı ilke kararı

Karar Tarihi : 31.05.2018

Karar No : 2018/63

Konu Özeti : Veri sorumlusu nezdindeki kişisel verilere erişim yetkisi bulunan personelin yetkisi ve amacı dışında söz konusu verileri işlemesi hususunun değerlendirilmesi

Veri sorumlusu nezdinde buldukları pozisyon veya görev itibariyle kişisel verilere erişime yetkisi olanlar tarafından, yetkilerini aşarak ve işleme amacı dışında söz konusu verilerin işlendiği hususunda Kuruma intikal eden ihbar ve şikayetlere ilişkin yapılan değerlendirme sonucunda, uygulamada yaşanan problemlerin önüne geçilebilmesini teminen;

- Bir veri sorumlusu nezdinde buldukları pozisyon veya görev itibariyle kişisel verilere erişim yetkisi olanlar tarafından, yetkileri aşmak ve/veya yetkilerini kötüye kullanmak suretiyle, kişisel amaçlara veya nedenlere bağlı olarak işleme amacı dışında söz konusu kişisel verilerin işlenmesi ve/veya bu verilerin üçüncü kişilerle paylaşılması 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrasına aykırılık teşkil edeceğinden, bu kapsamdaki eylemlerin önlenmesi amacıyla veri sorumlularınca uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirin alınması gerektiği hususunda veri sorumlularının bilgilendirilmesine,

- Kanunun 15 nci maddesinin (6) numaralı fıkrası uyarınca alınan bu ilke kararının Resmi Gazete ile Kurumun internet sitesinde yayımlanmasına,

oy birliği ile karar verilmiştir.

**2018/10 sayılı KVKK Kararı - Özel Nitelikli Kişisel Verilere İlişkin Yeterli Önlemlere İlişkin
Karar**

Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı

Karar Tarihi : 31.01.2018

Karar No : 2018/10

Konu Özeti : “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler” in görüşülmesi

RG Tarih ve Sayı: 07.03.2018/30353

Kanunun 6 ncı maddesinin (4) numaralı fıkrası ile 22 nci maddesinin (1) numaralı fıkrasının (ç) bendi kapsamında hazırlanan “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler” in ekte yer verilen şekilde kabulüne ve Resmi Gazetede yayımlanmasına oy birliği ile karar verilmiştir.

Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler

6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 6 ncı maddesinin (4) numaralı fıkrasında, “Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.” hükmü yer almaktadır.

Bu çerçevede, Kanunun 22 nci maddesinin (1) numaralı fıkrasının (ç) ve (e) bentleri uyarınca özel nitelikli kişisel veri işleyen veri sorumluları tarafından alınması gereken yeterli önlemler Kişisel Verileri Koruma Kurulu tarafından aşağıdaki şekilde belirlenmiştir:

- 1- Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi,
- 2- Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik,

- a) Kanun ve buna bağılı yönetmelikler ile özel nitelikli kişisel veri güvenliđi konularında düzenli olarak eđitimler verilmesi,
 - b) Gizlilik sözleşmelerinin yapılması,
 - c) Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,
 - ç) Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,
 - d) Görev deđişikliđi olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması.
- Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması,

3- Özel nitelikli kişisel verilerin işlendiđi, muhafaza edildiđi ve/veya erişildiđi ortamlar, elektronik ortam ise

- a) Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,
- b) Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,
- c) Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,
- ç) Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- d) Verilere bir yazılım aracılıđı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- e) Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik dođrulama sisteminin sağlanması,

4- Özel nitelikli kişisel verilerin işlendiđi, muhafaza edildiđi ve/veya erişildiđi ortamlar, fiziksel ortam ise

- a) Özel nitelikli kişisel verilerin bulunduğu ortamın niteliđine göre yeterli güvenlik önlemlerinin (elektrik kaçađı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındıđından emin olunması,
- b) Bu ortamların fiziksel güvenliđinin sağlanarak yetkisiz giriş çıkışların engellenmesi,

5- Özel nitelikli kişisel veriler aktarılacaksa

- a) Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması,

b) Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması,

c) Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımının gerçekleştirilmesi,

ç) Verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın "gizlilik dereceli belgeler" formatında gönderilmesi gerekir.

6- Yukarıda belirtilen önlemlerin yanı sıra Kişisel Verileri Koruma Kurumunun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate alınmalıdır.

2017/62 sayılı KVKK Kararı - Banko, Gişe, Masa gibi Hizmet Alanlarına İlişkin Karar

Banko, Gişe, Masa gibi Hizmet Alanlarında Kişisel Verilerin Korunmasına Yönelik Kişisel Verileri Koruma Kurulunun 21/12/2017 Tarihli ve 2017/62 Sayılı İlke Kararı

Karar Tarihi : 21.12.2017

Karar No : 2017/62

Konu Özeti : Banko, Gişe, Masa gibi Hizmet Alanlarında Kişisel Verilerin Korunması

Banko, gişe ve masa gibi vatandaşa hizmet sunulan alanlarda yaşanan kişisel veri güvenliği ihlallerine ilişkin olarak Kişisel Verileri Koruma Kurumuna intikal eden ihbarlar kapsamında yapılan değerlendirme sonucunda, uygulamada yaşanan problemlerin önüne geçilmesini teminen;

- Bankacılık ve sağlık sektörleri başta olmak üzere birden fazla çalışan ile birlikte bitişik düzende hizmet veren posta ve kargo hizmetleri, turizm acenteleri, zincir mağazaların müşteri hizmetleri bölümleri, çeşitli abonelik işlemlerinin yapıldığı kuruluşlar ile belediye, vergi ve nüfus ile ilgili işlemler gibi hizmetlerin verildiği kamu ve özel sektör kurum ve kuruluşlarının, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesi uyarınca kişisel verilerin korunması ile ilgili olarak; banko/gişe/masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda birbirlerine yakın konumda hizmet alanların birbirlerine ait kişisel verileri duymasını, görmesini, öğrenmesini veya ele geçirmesini engelleyecek nitelikte gerekli teknik ve idari tedbirleri almasına,

- Kanunun 15 inci maddesinin (6) numaralı fıkrası uyarınca alınan bu ilke kararının Resmi Gazete ile Kurumun internet sitesinde yayımlanmasına ve bu karara uymayanlar hakkında Kanunun 18 inci maddesi kapsamında işlem yapılacağına

oy birliği ile karar verilmiştir.

2017/61 sayılı KVKK Kararı - Rehberlik Hizmetleri Veren İnternet Sitelerine İlişkin Karar

Rehberlik Hizmeti Veren İnternet Sitelerinde/Uygulamalarda Kişisel Verilerin Korunmasına Yönelik Kişisel Verileri Koruma Kurulunun 21/12/2017 Tarihli ve 2017/61 Sayılı İlke Kararı

Karar Tarihi : 21.12.2017

Karar No : 2017/61

Konu Özeti : Rehberlik Hizmeti Veren İnternet Sitelerinde/Uygulamalarda Kişisel Verilerin Korunması

6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) hükümlerine aykırı olarak ilgili kişilerin açık rızalarını almaksızın isimden telefon numarası veya telefon numarasından isim sorgulanması şeklinde rehberlik hizmeti veren internet siteleri ve uygulamalara ilişkin olarak Kişisel Verileri Koruma Kurumuna intikal eden ihbar ve şikâyetler kapsamında yapılan değerlendirme sonucunda; çeşitli uygulamalar, internet siteleri veya sosyal medya hesapları üzerinden kişisel verileri toplayarak bu verilerin paylaşımını sağlayan, isim sorgulandığında telefon numarası bilgisine, telefon numarası sorgulandığında da isim bilgisine erişme ve başkalarının telefon rehberinde nasıl kayıtlı olduğunu öğrenme gibi konularda hizmet veren birçok uygulamanın ve internet sitesinin bulunduğu tespit edilmiştir.

Kanunun 3 üncü maddesinin (1) numaralı fıkrasının (e) bendinde “kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem” kişisel verilerin işlenmesi olarak düzenlenmiş olup sayılan eylemlerden birinin gerçekleştirilebilmesi için öncelikle Kanunun 5 ve 6 ncı maddelerinde sayılan işlenme şartlarından birinin bulunması, ayrıca Kanun ile öngörülen diğer yükümlülüklerin yerine getirilmesi gerekmektedir.

Bu kapsamda;

- Kanunda ve ilgili mevzuatta dayanađı bulunmaksızın ilgili kiřilerin iletiřim bilgilerinin paylařımını yapan internet siteleri ve mobil uygulamalar tarafından gerekleřtirilen veri iřleme faaliyetinin Kanunun 15 inci maddesinin (7) numaralı fıkrası uyarınca derhal durdurulması gerektiđi,

- Belirtilen řekilde sz konusu faaliyetlerde bulunan internet sitelerinin/uygulamaların faaliyetlerine son vermediđine iliřkin bilgi edinilmesi halinde bu internet sitelerine/uygulamalara eriřimin engellenmesi adına geređinin yapılmasını teminen yetkili kurumlara bařvuruda bulunulacađı, te yandan kiřisel verilerin hukuka aykırı olarak elde edilmiř olabileceđi de dikkate alınarak, 5237 sayılı Trk Ceza Kanununun “Verileri Hukuka Aykırı Olarak Verme veya Ele Geirme” bařlıklı 136 ncı maddesi erevesinde ilgili internet siteleri/uygulamalar hakkında gerekli hukuki iřlemlerin tesisi iin konunun Ceza Muhakemesi Kanununun 158 inci maddesi uyarınca ihbaren Cumhuriyet Bařsavcılıđına bildirileceđi

hususlarında kamuoyunun bilgilendirilmesine,

- Kanunun 15 inci maddesinin (6) numaralı fıkrası uyarınca alınan bu ilke kararının Resmi Gazete ile Kurumun internet sitesinde yayımlanmasına ve bu karara uymayanlar hakkında Kanunun 18 inci maddesi kapsamında iřlem yapılacađına

oy birliđi ile karar verilmiřtir.

KİŞİSEL VERİLERİ KORUMA KURULU KARARLARI

BÖLÜM İÇERİĞİ

2023/426 sayılı KVKK Kararı

Tüketici Finansman Kredisiyle Alışveriş İmkânı Sunan Şirket Tarafından İlgili Kişilerden e-Devlet Şifrelerinin Talep Edilmesi hakkında Kişisel Verileri Koruma Kurulu'nun 22/03/2023 tarihli ve 2023/426 sayılı Karar Özeti

2023/437 sayılı KVKK Kararı

Bir avukatlık ortaklığı tarafından borçlu ilgili kişiye kısa mesaj gönderilmesi suretiyle kişisel verilerinin işlenmesi hakkında Kişisel Verileri Koruma Kurulu'nun 22/03/2023 Tarihli ve 2023/437 Sayılı Kararı

2023/224 sayılı KVKK Kararı

Bir belediyenin meclis toplantısı videosunun sosyal medya hesabından paylaşılması suretiyle ilgili kişinin kişisel verilerinin hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 16/02/2023 tarih ve 2023/224 sayılı Karar Özeti

2023/134 sayılı KVKK Kararı

TikTok Pte. Ltd. hakkında Kişisel Verileri Koruma Kurulunun 2023/134 sayılı Karar Özeti

2023/86 sayılı KVKK Kararı

Veri sorumlusunun çalışanlarına tahsis ettiği kurumsal e-posta adresindeki içerikleri izleme, erişme ve depolama suretiyle kişisel verileri işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 19/01/2023 tarihli ve 2023/86 sayılı Karar Özeti

2023/78 sayılı KVKK Kararı

İlgili kişinin borç bilgisinin ortağı olduğu şirketin kurumsal numaralarına kısa mesaj olarak gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 19/01/2023 tarihli ve 2023/78 sayılı Karar Özeti

2023/67 sayılı KVKK Kararı

Veri sorumlusu bir banka tarafından ilgili kişinin para transferleri ile hesap bilgilerinin üçüncü kişiye ait e-postaya gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 12/01/2023 tarihli ve 2023/67 sayılı Karar Özeti

2023/4 sayılı KVKK Kararı

Bir kargo firmasının çapraz barkodlama hatası nedeniyle kişisel verilerin hukuka aykırı olarak paylaşımına sebep olması hakkında Kişisel Verileri Koruma Kurulunun 05/01/2023 tarihli ve 2023/4 sayılı Kararı

2022/1358 sayılı KVKK Kararı

Bir internet sitesinde yer alan çerezlere ilişkin aydınlatma ve açık rıza metinlerinin sunulmaması hakkında Kişisel Verileri Koruma Kurulunun 23/12/2022 tarihli ve 2022/1358 sayılı Karar Özeti

2022/1357 sayılı KVKK Kararı

Spor salonu işletmecisi olan veri sorumlusunun, özel nitelikli kişisel veri niteliğini haiz kan grubu verisini ilgili kişinin açık rızasını almaksızın işlemesi hakkında Kişisel Verileri Koruma Kurulunun 23/12/2022 tarih ve 2022/1357 sayılı Karar Özeti

2022/1281 sayılı KVKK Kararı

İcra takibi dolayısıyla veri sorumlusu avukat tarafından borçlunun borç bilgisinin oğlu ile paylaşılması ve kendisi ile borç bilgisi paylaşılan borçlunun oğlunun telefon numarasının bu suretle hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 01/12/2022 tarihli ve 2022/1281 sayılı Karar Özeti

2022/1249 sayılı KVKK Kararı

İlgili kişinin döviz bürosundaki güvenlik kamerası ile kayıt altına alınmış görüntülerinin haber ajansları ile paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 24/11/2022 tarihli ve 2022/1249 sayılı Karar Özeti

2022/1201 sayılı KVKK Kararı

İlgili kişinin Resmî Gazete'nin internet sayfasından erişilebilen bir ilana ilişkin olarak arama motorunda adı ve soy adı ile yapılan aramada ulaşılan sonuçların indeksten çıkarılması talebi hakkında Kişisel Verileri Koruma Kurulunun 10/11/2022 tarihli ve 2022/1201 sayılı Karar Özeti

2022/1147 sayılı KVKK Kararı

İlgili kişinin kişisel verilerinin iş akdinin feshinden sonra işveren tarafından işlenmeye devam edilmesi hakkında Kişisel Verileri Koruma Kurulunun 20/10/2022 tarihli ve 2022/1147 sayılı Karar Özeti

2022/1072 sayılı KVKK Kararı

İlgili kişinin kişisel verisi niteliğindeki e-posta adresinin reklam amaçlı ileti gönderilmesi suretiyle işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 07/10/2022 tarihli ve 2022/1072 sayılı Karar Özeti

2022/925 sayılı KVKK Kararı

İlgili kişinin e-posta adresine başka abonelere ait e-faturaların gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 08/09/2022 tarihli ve 2022/925 sayılı Karar Özeti

2022/923 sayılı KVKK Kararı

İlgili kişinin telefon numarasının hastaneden ayrılan doktor tarafından SMS gönderilmesi suretiyle işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 08/09/2022 tarihli ve 2022/923 sayılı Karar Özeti

2022/902 sayılı KVKK Kararı

İlgili kişinin açık rızası alınmadan pazarlama amacıyla kısa mesaj gönderilmesi suretiyle kişisel verilerinin işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 02/09/2022 tarihli ve 2022/902 sayılı Karar Özeti

2022/896 sayılı KVKK Kararı

Veri sorumlusu eski işveren tarafından ilgili kişinin kişisel verilerinin yer aldığı adli yazışma bilgilerinin kardeşi ile paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 02/09/2022 tarihli ve 2022/896 sayılı Karar Özeti

2022/863 sayılı KVKK Kararı

Bir bankanın müşteri hizmetlerinin aydınlatma yükümlülüğünü yerine getirmeden ve açık rızasını almadan ilgili kişiyi telefonla aramak suretiyle kişisel verilerini işleme hakkında Kişisel Verileri Koruma Kurulunun 01/09/2022 tarihli ve 2022/863 sayılı Karar Özeti

2022/861 sayılı KVKK Kararı

İlgili kişinin internet arama motorlarında yapılan aramalardan elde edilen iş yeri e-postasının açık rızası alınmaksızın veri sorumlusu bir pazarlama şirketi tarafından ticarî elektronik ileti gönderilmesi suretiyle işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 01/09/2022 tarihli ve 2022/861 sayılı Karar Özeti

2022/853 sayılı KVKK Kararı

Bir yasal bahis platformu tarafından ilgili kişinin e-posta adresinin işlenerek bir üyesinin kişisel verilerinin üçüncü şahıs konumundaki ilgili kişinin e-posta adresine gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 01/09/2022 tarihli ve 2022/853 sayılı Karar Özeti

2022/798 sayılı KVKK Kararı

İlgili kişinin bir şirket ile iş görüşmesi yaptığı bilgisi ile görüşmenin içeriği hakkındaki muhtelif bilgilerin iş görüşmesi yapılan şirket tarafından halihazırdaki iş yeri ile paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 04/08/2022 tarihli ve 2022/798 sayılı Karar Özeti

2022/790 sayılı KVKK Kararı

Bir üniversite hastanesi tarafından ilgili kişinin sağlık verilerinin idari bir davaya esas teşkil etmek üzere talebine binaen davalı kamu kurumuna aktarılması hakkında Kişisel Verileri Koruma Kurulunun 04/08/2022 tarihli ve 2022/790 sayılı Karar Özeti

2022/787 sayılı KVKK Kararı

Ev eşyası satan veri sorumlusu tarafından ilgili kişinin telefon numarasının üçüncü bir kişinin borcu için iletişim kurulmak suretiyle işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 04/08/2022 tarihli ve 2022/787 sayılı Karar Özeti

2022/776 sayılı KVKK Kararı

Veri sorumlusu bir pazarlama şirketi tarafından çocuğun kişisel verilerinin velisinin açık rızası alınmaksızın tanıtım amaçlı broşür gönderilmesi suretiyle işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 03/08/2022 tarihli ve 2022/776 sayılı Karar Özeti

2022/774 sayılı KVKK Kararı

Veri sorumlusu bir e-ticaret sitesinden alışveriş yapan üçüncü kişiye ait sipariş bilgilerinin ilgili kişinin e-posta adresine gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 03/08/2022 tarihli ve 2022/774 sayılı Karar Özeti

2022/768 sayılı KVKK Kararı

Veri sorumlusu banka tarafından ilgili kişinin kişisel verilerinin açık rızası alınmaksızın bir sigorta şirketine aktarılması hakkındaki Kişisel Verileri Koruma Kurulunun 03/08/2022 tarihli ve 2022/768 sayılı Karar Özeti

2022/655 sayılı KVKK Kararı

Tasfiye edilmiş şirketin yönetim kurulu üyeleri olan ilgili kişilerin kişisel verilerinin, şirket borcu kapsamında kısa mesaj gönderme ve arama suretiyle veri sorumlusu avukat tarafından hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 07/07/2022 tarihli ve 2022/655 sayılı Karar Özeti

2022/653 sayılı KVKK Kararı

İlgili kişinin, çevrimiçi alışveriş hizmeti veren veri sorumlusundan gerçekleştirdiği alışverişine ilişkin kredi kartı ve cep telefonu bilgilerinin kendisine bildirilmesi talebi hakkında Kişisel Verileri Koruma Kurulunun 07/07/2022 tarihli ve 2022/653 sayılı Karar Özeti

2022/630 sayılı KVKK Kararı

İlgili kişinin ameliyat sırasında çekilen fotoğraflarının veri sorumlusu hastanede çalışan bir doktorun sosyal medya hesabında paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 29/06/2022 tarihli ve 2022/630 sayılı Karar Özeti

2022/594 sayılı KVKK Kararı

Özel nitelikli kişisel sağlık verisi niteliğindeki bağımlılık yapıcı madde testinin sonuçlarının ilgili kişilerin açık rızası alınmaksızın veri sorumlusu özel bir sağlık kuruluşu tarafından ilgili kişilerin işyerinde görevli üçüncü bir kişiye ait e-posta adresine gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 22/06/2022 tarihli ve 2022/594 sayılı Karar Özeti

2022/545 sayılı KVKK Kararı

İlgili kişinin kişisel verilerinin hesabının bulunmadığı veri sorumlusu banka tarafından aydınlatma yükümlülüğü yerine getirilmeksizin ve açık rızası alınmaksızın işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 02/06/2022 tarihli ve 2022/545 sayılı Karar Özeti

2022/491 sayılı KVKK Kararı

Veri sorumlusu bir giyim mağazası için katalog modeli olarak çalışan ilgili kişinin fotoğraflarının, iş ilişkisinin sona ermesinden sonraki süreçte açık rızası olmaksızın veri sorumlusuna ait internet sitesinde yayınlanmaya devam etmesi hakkında Kişisel Verileri Koruma Kurulunun 18/05/2022 tarihli ve 2022/491 sayılı Karar Özeti

2022/489 sayılı KVKK Kararı

Kişisel Verileri Koruma Kurulunun 18/05/2022 tarihli ve 2022/489 sayılı Karar Özeti

2022/386 sayılı KVKK Kararı

Veri sorumlusu bünyesinde çalışan bir kişinin iş akdinin sonlandırılması hususunun veri sorumlusuna ait sosyal medya hesabında paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 21/04/2022 tarihli ve 2022/386 sayılı Karar Özeti

2022/328 sayılı KVKK Kararı

İlgili kişinin kişisel verilerinin yer aldığı ihtarnamenin, bordrolama hizmeti sunan veri sorumlusu tarafından başka çalışanlara da gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 07/04/2022 tarih ve 2022/328 sayılı Karar Özeti

2022/325 sayılı KVKK Kararı

İlgili kişi ile ilgisi bulunmayan bir işletme adına düzenlenmiş e-faturaların, ilgili kişinin e-posta adresine gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 07/04/2022 tarih ve 2022/325 sayılı Karar Özeti

2022/277 sayılı KVKK Kararı

İlgili kişiye ait kişisel verileri içeren bir kargo paketinin üçüncü bir şahsın eline geçmesi hakkında Kişisel Verileri Koruma Kurulunun 24/03/2022 tarihli ve 2022/277 sayılı Karar Özeti

2022/249 sayılı KVKK Kararı

Bir teknoloji řirketi tarafından ilgili kiřinin kiřisel verilerinin aık rızası olmaksızın yurt dıřına aktarılması hakkında Kiřisel Verileri Koruma Kurulunun 17/03/2022 tarihli ve 2022/249 sayılı Karar zeti

2022/662 sayılı KVKK Kararı

İlgili kiřinin 'el geometrisi' bilgisinin bir iřletmenin hizmet binasına giriř yapabilmek amacıyla veri sorumlusu tarafından aık rıza alınmaksızın iřlenmesi hakkındaki Kiřisel Verileri Koruma Kurulunun 07/07/2022 tarihli ve 2022/662 sayılı Karar zeti

2022/243 sayılı KVKK Kararı

Aynı isme sahip bir kiři tarafından internet üzerinden sipariř verilirken ilgili kiřinin e-posta adresinin kullanılması zerine faturanın ilgili kiřiye gnderilmesi suretiyle kiřisel verilerinin iřlenmesi hakkında Kiřisel Verileri Koruma Kurulunun 17/03/2022 tarihli ve 2022/243 sayılı Karar zeti

2022/229 sayılı KVKK Kararı

E-ticaret sektrnde faaliyet gsteren veri sorumlusu řirket tarafından internet sitesinde/mobil uygulamalarında kullanılan erezler aracılıęıyla hukuka aykırı olarak kiřisel veri iřlenmesi hakkında Kiřisel Verileri Koruma Kurulunun 10/03/2022 tarih ve 2022/229 sayılı Karar zeti

2022/224 sayılı KVKK Kararı

Bir bankanın aęrı merkezi tarafından ilgili kiřinin telefon numarasının nc kiřilerle paylařılması hakkında Kiřisel Verilerin Koruma Kurulunun 10/03/2022 tarihli ve 2022/224 sayılı Karar zeti

2022/184 sayılı KVKK Kararı

Bir alacak ynetim řirketi tarafından ilgili kiřinin bor bilgilerinin nc kiřilerle paylařılması hakkında Kiřisel Verileri Koruma Kurulunun 04/03/2022 tarihli ve 2022/184 sayılı Karar zeti

2022/172 sayılı KVKK Kararı

Yurt dışında mukim veri sorumlusunun Türkiye'deki irtibat bürosu tarafından işe alım sürecinde adaylardan özel nitelikli kişisel veri talep edilmesi hakkında Kişisel Verileri Koruma Kurulunun 24/02/2022 tarihli ve 2022/172 sayılı Karar Özeti

2022/137 sayılı KVKK Kararı

Veri sorumlusu bir alışveriş merkezi tarafından senetli alışverişler için ilgili kişilerden e-Devlet şifresi, internet sayfasında üyelik oluşturulması için ise T.C. kimlik numarası temin edilmesi suretiyle kişisel verilerin hukuka aykırı işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 17/02/2022 tarih ve 2022/137 sayılı Karar Özeti

2022/107 sayılı KVKK Kararı

Bir tasarruf finansman şirketi tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmaksızın işlenmesi ve ilgili numaraya reklam içerikli SMS gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 10/02/2022 tarihli ve 2022/107 sayılı Karar Özeti

2022/103 sayılı KVKK Kararı

Unvanında ilgili kişinin adının geçtiği bir şirket hakkında başlatılan icra takibine ilişkin dosya içeriğinin sosyal medyada paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 10/02/2022 tarihli ve 2022/103 sayılı Karar Özeti

2022/31 sayılı KVKK Kararı

Sağlık sektöründe faaliyet gösteren veri sorumlusu tarafından ilgili kişinin kişisel verilerinin açık rızası alınmaksızın ticarî elektronik ileti gönderilmesi amacıyla işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 18/01/2022 tarihli ve 2022/31 sayılı Karar Özeti

2022/13 sayılı KVKK Kararı

Yerel bir haber sitesi tarafından ilgili kişinin açık rızası olmaksızın sınav sonuç belgesinin paylaşılmasına ilişkin Kişisel Verileri Koruma Kurulunun 06/01/2022 tarihli ve 2022/13 sayılı Karar Özeti

2022/6 sayılı KVKK Kararı

İlgili kişinin eski ortağı olduğu şirketin sicil bilgilerinin görüntülediği internet adresinde kişisel verilerinin hukuka aykırı olarak paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 06/01/2022 tarih ve 2022/6 sayılı Karar Özeti

2021/1324 sayılı KVKK Kararı

Yemek Sepeti Elektronik İletişim Perakende Gıda Lojistik AŞ veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 23/12/2021 tarih ve 2021/1324 sayılı Karar Özeti

2021/1303 sayılı KVKK Kararı

Araç kiralama programları yazılımcısı ve satıcısı firmalar tarafından, ilgili kişilerin verilerinin işlenmesi ve bu verilerin araç kiralama firmaları arasında paylaşılmasını sağlayan bir kara liste programı oluşturulması” hakkında Kişisel Verileri Koruma Kurulunun 23/12/2021 tarihli ve 2021/1303 sayılı Karar Özeti

2021/1262 sayılı KVKK Kararı

Bir sigorta şirketi tarafından ilgili kişinin banka verilerinin işlenmesi hakkında” Kişisel Verileri Koruma Kurulunun 16/12/2021 tarihli ve 2021/1262 sayılı Karar Özeti

2021/1258 sayılı KVKK Kararı

İlgili kişinin kişisel verilerinin iş akdinin sona erdiği veri sorumlusu şirket tarafından hukuka aykırı olarak işlenmesi hakkında” Kişisel Verileri Koruma Kurulunun 16/12/2021 tarihli ve 2021/1258 sayılı Karar Özeti

2021/1243 sayılı KVKK Kararı

İlgili kişinin kişisel verisi niteliğindeki e-posta adresinin bir insan kaynakları firması tarafından reklam ve pazarlama amaçlı e-posta gönderilmesi amacıyla işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 09/12/2021 tarihli ve 2021/1243 sayılı Karar Özeti

2021/1239 sayılı KVKK Kararı

Veri sorumlusu Banka tarafından ilgili kişinin ailesinin telefonları üzerinden arama gerçekleştirilmesi suretiyle kişisel verilerinin paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 09/12/2021 tarihli ve 2021/1239 sayılı Karar Özeti

2021/1218 sayılı KVKK Kararı

İlgili kişi işçinin hakkında yürütülen kişisel verilerin işlenmesi faaliyetleri kapsamında yurtdışında mukim olan veri sorumlusu işverence aydınlatılmaması, ilgili kişiye ait kişisel verilerin Nisan 2021 sonrası dönemde veri sorumlusu tarafından hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 02/12/2021 tarihli ve 2021/1218 sayılı Karar Özeti

2021/1217 sayılı KVKK Kararı

İlgili kişi anne ve ilgili kişi sıfatını haiz çocuğunun fotoğrafları da kullanılmak suretiyle ilgili kişi hakkında gerçek dışı, şeref ve haysiyet kırıcı bir televizyon haberi yapıldığı iddiası hakkında Kişisel Verileri Koruma Kurulunun 02/12/2021 tarihli ve 2021/1217 sayılı Karar Özeti

2021/1214 sayılı KVKK Kararı

Bir üniversite tarafından verilen eğitimde, eğitim alan kişilerin kişisel verilerini içeren yoklama listesinin diğer katılımcılar tarafından görülebilir şekilde düzenlenmesi hakkında Kişisel Verileri Koruma Kurulunun 02/12/2021 tarihli ve 2021/1214 sayılı Karar Özeti

2021/1210 sayılı KVKK Kararı

İlgili kişinin kişisel verisi niteliğindeki cep telefonu numarasının, Digiturk kampanyaları hakkında bilgilendirmede bulunmak amacıyla aranması ve SMS gönderilmesi suretiyle işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 02/12/2021 tarih ve 2021/1210 sayılı Karar Özeti

2021/1187 sayılı KVKK Kararı

Veri sorumlusu işveren tarafından eski çalışanı olan ilgili kişinin kurumsal e-posta hesabına aydınlatma yapılmaksızın erişilmesi hakkında Kişisel Verileri Koruma Kurulunun 25/11/2021 tarihli ve 2021/1187 sayılı Karar Özeti

2021/1153 sayılı KVKK Kararı

Tıbbi ürünler satan veri sorumlusu tarafından ilgili kişiye reklam içerikli SMS gönderilmesi suretiyle kişisel verilerinin işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 11/11/2021 tarihli ve 2021/1153 sayılı Karar Özeti

2021/1127 sayılı KVKK Kararı

Veri sorumlusu Üniversitenin ilgili kişinin kişisel verilerini içeren belgeleri internet sitesinde yayımlaması hakkında Kişisel Verileri Koruma Kurulunun 04/11/2021 tarihli ve 2021/1127 sayılı Karar Özeti

2021/1111 sayılı KVKK Kararı

İlgili kişinin ceza mahkûmiyeti bilgisinin avukat olan veri sorumlusu tarafından hukuka aykırı olarak elde edilmesi ve mahkeme dosyasına sunulması hakkında Kişisel Verileri Koruma Kurulunun 02/11/2021 tarihli ve 2021/1111 sayılı Karar Özeti

2021/1110 sayılı KVKK Kararı

Veri sorumlusunun icra takibi başlattığı müşterilerinin kişisel verilerini herkesin erişimine açık bir internet sitesinde yayımlaması hakkında Kişisel Verileri Koruma Kurulunun 02/11/2021 tarih ve 2021/1110 sayılı Karar Özeti

2021/1107 sayılı KVKK Kararı

İlgili kişinin kredi notunun Banka tarafından düzeltilmemesi ve kişisel verilerinin üçüncü kişilerle paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 02/11/2021 tarihli ve 2021/1107 sayılı Karar Özeti

2021/1104 sayılı KVKK Kararı

Banka tarafından ilgili kişinin cep telefonu numarasına SMS gönderilmesi suretiyle kişisel verilerinin hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 02/11/2021 tarihli ve 2021/1104 sayılı Karar Özeti

2021/1069 sayılı KVKK Kararı

Bankanın avukatı tarafından borçlu yakını olan ilgili kişiye haciz ihbarnamesi gönderilmesi suretiyle kişisel verilerinin işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 21/10/2021 tarihli ve 2021/1069 sayılı Karar Özeti

2021/1051 sayılı KVKK Kararı

İş arama ve işe alım süreçlerini yürüten bir istihdam platformunun Kişisel Verilerin Korunması Kanunu'na aykırı uygulamalarda bulunması hakkında Kişisel Verileri Koruma Kurulunun 14/10/2021 tarihli ve 2021/1051 sayılı Karar Özeti

2021/909 sayılı KVKK Kararı

İlgili kişinin kardeşine ait borca dair yürütülen icra takibi kapsamında, veri sorumlusu avukat tarafından ilgili kişinin kişisel verilerinin İcra Müdürlüğüne iletilmesi hakkında Kişisel Verileri Koruma Kurulunun 09/09/2021 tarihli ve 2021/909 sayılı Karar Özeti

2021/925 sayılı KVKK Kararı

İlgili kişinin sendika üyeliği bilgisinin hukuka aykırı şekilde elde edilmesi ve paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 16/09/2021 tarihli ve 2021/925 sayılı Karar Özeti

2021/989 sayılı KVKK Kararı

İlgili kişiye ait görselin, açık rızası alınmaksızın bir internet sitesinde yer alan haber içeriğinde kullanılması hakkında Kişisel Verileri Koruma Kurulunun 30/09/2021 tarihli 2021/989 sayılı Karar Özeti

2021/993 sayılı KVKK Kararı

Veri sorumlusu kargo firması tarafından ilgili kişi adına sehven fatura düzenlenmesi hakkında Kişisel Verileri Koruma Kurulunun 30/09/2021 tarihli 2021/993 sayılı Karar Özeti

2021/889 sayılı KVKK Kararı

İlgili kişinin, bir spor tesisi tarafından açık rızası alınmaksızın yer aldığı müsabakaların kaydedilip yayınlanması hakkında Kişisel Verileri Koruma Kurulunun 03/09/2021 tarihli ve 2021/889 sayılı Karar Özeti

2021/859 sayılı KVKK Kararı

İlgili kişinin internet hizmeti aboneliğini sağlamak üzere evine gelen şirket yetkilisinin aboneliği oluşturmak adına ilgili kişiye ait kimliğin fotoğrafını cep telefonu aracılığıyla çekmesi suretiyle kişisel verilerini işlemesi hakkında Kişisel Verileri Koruma Kurulunun 26/08/2021 tarihli ve 2021/859 sayılı Karar Özeti

2021/850 sayılı KVKK Kararı

Şikayetçinin ablasının kimlik bilgilerinin numara taşıma işlemi adına bir telekomünikasyon şirketinin bayi çalışanına ait telefon marifetiyle fotoğraflanarak kullanılan sisteme yüklenmesi hakkındaki ihbara ilişkin Kişisel Verileri Koruma Kurulunun 26/08/2021 tarihli ve 2021/850 sayılı Karar Özeti

2021/847 sayılı KVKK Kararı

İlgili kişinin bir web sitesinden kişisel verilerinin silinmesi talebinin veri sorumlusu tarafından yerine getirilmemesi hakkında Kişisel Verileri Koruma Kurulunun 26/08/2021 tarihli ve 2021/847 sayılı Karar Özeti

2021/799 sayılı KVKK Kararı

İlgili kişinin uluslararası geçerliliği olan bir dil sınavı konusunda Türkiye'deki akredite kuruluş tarafından kişisel verilerinin hukuka aykırı işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 12/08/2021 tarihli ve 2021/799 sayılı Karar Özeti

2021/761 sayılı KVKK Kararı

Kişisel sağlık verilerinin hastanedeki yetkisiz çalışanlar tarafından velayete sahip olmayan ebeveyn ile paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 06/08/2021 tarihli ve 2021/761 sayılı Karar Özeti

2021/670 sayılı KVKK Kararı

İlgili kişinin veri sorumlusu bankaya yaptığı iş başvurusunun olumsuz sonuçlanması sonrası kişisel verilerinin işlenmeye devam etmesi hakkında Kişisel Verileri Koruma Kurulunun 06/07/2021 tarih ve 2021/670 sayılı Karar Özeti

2021/666 sayılı KVKK Kararı

Şikâyetçinin yeni doğan bebeğine ait doğum belgesinde yer alan kişisel verilerin üçüncü kişiler tarafından Özel Hastane olarak faaliyet gösteren veri sorumlusundan hukuka aykırı olarak ele geçirilmesi hakkında Kişisel Verileri Koruma Kurulunun 06/07/2021 tarihli ve 2021/666 sayılı Karar Özeti

2021/664 sayılı KVKK Kararı

İlgili kişinin, doğal gaz dağıtımı yapan bir şirket tarafından düzenlenen faturasında kişisel verisi niteliğindeki banka bilgisine yer verilmesi hakkında Kişisel Verileri Koruma Kurulunun 06/07/2021 tarihli ve 2021/664 sayılı Karar Özeti

2021/603 sayılı KVKK Kararı

İlgili kişinin internet alışveriş sayfası üzerinden ev adresine teslim talepli olarak vermiş olduğu siparişlerinin veri sorumlusu kargo şirketi tarafından, hiçbir suretle belirtmediği halde işyeri adresine

gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 22/06/2021 tarihli ve 2021/603 sayılı Karar Özeti

2021/584 sayılı KVKK Kararı

Sigortacılık ve bireysel emeklilik alanında faaliyet gösteren bir şirket tarafından ilgili kişiye ait kişisel verilerin hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 09/06/2021 tarihli ve 2021/584 sayılı Karar Özeti

2021/572 sayılı KVKK Kararı

İlgili kişinin fotoğrafının öğrencisi olduğu okul tarafından kullanılması hakkında Kişisel Verileri Koruma Kurulunun 09/06/2021 tarihli 2021/572 sayılı Karar Özeti

2021/548 sayılı KVKK Kararı

İlgili kişinin cep telefonu numarasının kampanya adı altında bir dijital platform bayisi tarafından edinilmesi, işlenmesi ve rızası olmaksızın arama yapılması hakkında Kişisel Verileri Koruma Kurulunun 04/06/2021 tarih ve 2021/548 sayılı Karar Özeti

2021/545 sayılı KVKK Kararı

Veri sorumlusu tarafından ilgili kişinin cep telefonu numarasına reklam amaçlı SMS gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 04/06/2021 tarihli 2021/545 sayılı Karar Özeti

2021/511-512-513 sayılı KVKK Kararı

Avukatların icra takip dosyalarındaki kişisel verilere vekâletname olmaksızın hukuka aykırı olarak erişim sağladığına ve Adalet Bakanlığı tarafından icra tevzi bürolarında görevli personel eliyle alacaklı vekili avukatlara borçluların alacaklı olduğu icra takip dosyalarında bulunan kişisel verilerin hukuka aykırı olarak aktarılmasına ilişkin ihbarlar hakkında Kişisel Verileri Koruma Kurulunun 20/05/2021 tarihli ve 2021/511-512-513 sayılı Karar Özeti

2021/424 sayılı KVKK Kararı

Bir bankanın, varlık yönetim şirketinin ve üç farklı avukatın borçlu olmayan ilgili kişinin kişisel verisini işleyerek icra takibi başlattıkları iddiası hakkında Kişisel Verileri Koruma Kurulunun 27/04/2021 tarihli ve 2021/424 sayılı Karar Özeti

2021/422 sayılı KVKK Kararı

İlgili kişinin fotoğraflarının veri sorumlusuna ait bir sosyal medya hesabında paylaşılması suretiyle gerçekleşen kişisel veri işleme faaliyeti hakkında Kişisel Verileri Koruma Kurulunun 27/04/2021 tarihli ve 2021/422 sayılı Karar Özeti

2021/470 sayılı KVKK Kararı

İlgili kişinin yemek kartı hesap hareketlerine ilişkin kişisel verilerine erişim talebinin veri sorumlusu tarafından yerine getirilmediği iddiası hakkında Kişisel Verileri Koruma Kurulunun 06/05/2021 tarihli ve 2021/470 sayılı Karar Özeti

2021/464 sayılı KVKK Kararı

Bir otoyol işletmesinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 16.06.2020 tarih ve 2021/464 sayılı Karar Özeti

2021/427 sayılı KVKK Kararı

Bir e-ticaret sitesi (veri sorumlusu) nezdinde gerçekleşen veri ihlali hakkında yapılan resen inceleme hakkında Kişisel Verileri Koruma Kurulunun 27/04/2021 tarih ve 2021/427 sayılı Karar Özeti

2021/426 sayılı KVKK Kararı

Yardım masası paneli hizmeti veren bir veri sorumlusunda gerçekleşen veri ihlali hakkında yapılan resen inceleme hakkında Kişisel Verileri Koruma Kurulunun 27/04/2021 tarihli ve 2021/426 sayılı Karar Özeti

2021/407 sayılı KVKK Kararı

Bir hastanenin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 20/04/2021 tarih ve 2021/407 sayılı Karar Özeti

2021/389 sayılı KVKK Kararı

Bir sigorta şirketi tarafından hizmetin açık rıza şartına bağlanması hakkındaki ihbar ile ilgili olarak Kişisel Verileri Koruma Kurulunun 20/04/2021 tarihli ve 2021/389 sayılı Karar Özeti

2021/361 sayılı KVKK Kararı

Bir bankanın mobil uygulamalar üzerinden ilgili kişiye rızası dışında tanıtım iletileri göndermesi hakkında Kişisel Verileri Koruma Kurulunun 13/04/2021 tarihli ve 2021/361 sayılı Karar Özeti

2021/359 sayılı KVKK Kararı

İlgili kişinin kişisel verilerinin site yönetim hizmetini sağlayan veri sorumlusu şirket tarafından bir mobil uygulama ile hukuka aykırı olarak paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 13/04/2021 tarihli ve 2021/359 sayılı Karar Özeti

2021/358 sayılı KVKK Kararı

İlgili kişiye bir banka tarafından SMS gönderilmesi ve ilgili kişinin bu banka nezdindeki kişisel verilerinin imha edilmesi talebinin yerine getirilmemesi hakkında Kişisel Verileri Koruma Kurulunun 13/04/2021 tarihli ve 2021/358 sayılı Karar Özeti

2021/333 sayılı KVKK Kararı

Bir sigorta şirketi tarafından işlenen kişisel verilerin üçüncü kişiye aktarılması ve ilgili kişiye veri aktarımına ilişkin aydınlatma yapılmaması hakkında Kişisel Verileri Koruma Kurulunun 05/04/2021 tarih ve 2021/333 sayılı Karar Özeti

2021/311 sayılı KVKK Kararı

Bir kozmetik şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 25.03.2021 tarih ve 2021/311 sayılı Karar Özeti

2021/242 sayılı KVKK Kararı

İlgili kişinin kişisel verilerinin bir tur şirketi tarafından üçüncü kişilerle paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 18/03/2021 tarihli ve 2021/242 sayılı Karar Özeti

2021/241 sayılı KVKK Kararı

Ölenin sigorta poliçesine yasal mirasçısının erişim talebinin sigorta şirketi tarafından reddedilmesi hakkında Kişisel Verileri Koruma Kurulunun 18/03/2021 tarihli ve 2021/241 sayılı Karar Özeti

2021/238 sayılı KVKK Kararı

Veri Sorumluları Siciline Kayıt Tarihlerinin Uzatılması İle İlgili Kişisel Verileri Koruma Kurulunun 11/03/2021 Tarihli ve 2021/238 Sayılı Kararı

2021/230 sayılı KVKK Kararı

İlgili kişinin kişisel verisinin kamu kurumu personeli olarak görev yapan eski eşi tarafından sorgulanarak elde edilmesi ve adli makamlar ile paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 11/03/2021 tarihli ve 2021/230 sayılı Karar Özeti

2021/228 sayılı KVKK Kararı

Hukuk Bürosu tarafından ilgili kişinin kişisel verilerinin muhatabı ve tarafı olmadığı icra takibi ile ilgili işlemlerde hukuka aykırı olarak işlenmesi ve icra dosyasına ilişkin ilgili kişinin telefon numaralarına mesajlar gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 11/03/2021 tarihli ve 2021/228 sayılı Karar Özeti

2021/227 sayılı KVKK Kararı

Bir eğitim kurumu tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmaksızın işlenmesi ve ilgili numaraya reklam içerikli SMS gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 11/03/2021 tarihli ve 2021/227 sayılı Karar Özeti

2020/216 sayılı KVKK Kararı

Bir bilişim şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 12/03/2020 tarih ve 2020/216 sayılı Karar Özeti

2021/205 sayılı KVKK Kararı

İşten çıkarma sürecinde veri sorumlusu işveren tarafından ilgili kişinin kişisel verilerinin hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 09/03/2021 tarihli ve 2021/205 sayılı Karar Özeti

2021/190 sayılı KVKK Kararı

Bankacılık sektöründeki veri sorumlusunun veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 04.03.2021 tarih ve 2021/190 sayılı Karar Özeti

2021/187 sayılı KVKK Kararı

Bir sigorta şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 04.03.2021 tarih ve 2021/187 sayılı Karar Özeti

2021/154 sayılı KVKK Kararı

Bir sigorta şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 25.02.2021 tarih ve 2021/154 sayılı Karar Özeti

2021/140 sayılı KVKK Kararı

Belediyeler tarafından sunulan internet hizmetlerine ilişkin Kişisel Verileri Koruma Kurulunun 25/02/2021 tarih ve 2021/140 sayılı Karar Özeti

2021/115 sayılı KVKK Kararı

Bankaya olan borcundan dolayı ilgili kişinin yakınına Bankanın sözleşmeli avukatı tarafından ilgili kişinin borç bilgisinin iletilmesi hakkında Kişisel Verileri Koruma Kurulunun 09/02/2021 tarihli ve 2021/115 sayılı Karar Özeti

2021/111 sayılı KVKK Kararı

İlgili kişinin telefon numarası bilgisinin farklı veri sorumluları tarafından hukuka aykırı olarak işlenmesine ilişkin Kişisel Verileri Koruma Kurulunun 09/02/2021 tarihli ve 2021/111 sayılı Karar Özeti

2021/85 sayılı KVKK Kararı

İlgili kişinin Kanununun 11 nci maddesi kapsamındaki başvurusuna veri sorumlusu tarafından verilen cevabın yeterli bulunmaması hakkında Kişisel Verileri Koruma Kurulunun 03/02/2021 tarihli ve 2021/85 sayılı Karar Özeti

2021/84 sayılı KVKK Kararı

Veri sorumlusu sabit telefon hizmeti sağlayan işletmeci tarafından bir hastanenin müşterilerinin kişisel verilerinin hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 03/02/2021 tarihli ve 2021/84 sayılı Karar Özeti

2021/79 sayılı KVKK Kararı

Veri sorumlusu banka tarafından ilgili kişinin verilerinin yakınları ile paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 03/02/2021 tarihli ve 2021/79 sayılı Karar Özeti

2021/78 sayılı KVKK Kararı

Telekomünikasyon hizmetleri sunan bir veri sorumlusunun ürün satışı esnasında müşterilerinin pasaport fotoğraflarını çekerek depolaması hakkında Kişisel Verileri Koruma Kurulunun 03/02/2021 tarihli ve 2021/78 sayılı Karar Özeti

2021/32 sayılı KVKK Kararı

İlgili kişinin kişisel verilerinin bilgisi dışında veri sorumlusu banka nezdinde sorgulanması hakkında Kişisel Verileri Koruma Kurulunun 12/01/2021 tarihli ve 2021/32 sayılı Karar Özeti

2020/957 sayılı KVKK Kararı

Bir ilaç şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 15/12/2020 tarih ve 2020/957 sayılı Karar Özeti

2020/935 sayılı KVKK Kararı

Bir sigorta şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 08/12/2020 tarih ve 2020/935 sayılı Karar Özeti

2020/934 sayılı KVKK Kararı

Enerji sektöründe faaliyet gösteren veri sorumlusunun veri ihlali bildirimini hakkında Kişisel Verileri Koruma Kurulunun 08/12/2020 tarih ve 2020/934 sayılı Karar Özeti

2020/927 sayılı KVKK Kararı

Unutulma hakkı kapsamında ilgili kişinin arama motorunda adı ve soyadı ile bağlantılı sonuçların kaldırılması talebine ilişkin Kişisel Verileri Koruma Kurulunun 08/12/2020 tarihli ve 2020/927 sayılı Karar Özeti

2020/915 sayılı KVKK Kararı

Belediyede memur olarak görev yapan ilgili kişinin, veri sorumlusu bünyesinde işe giriş çıkış takibinin biyometrik veri işlenerek yapılması hakkında Kişisel Verileri Koruma Kurulunun 01/12/2020 tarihli ve 2020/915 sayılı Karar Özeti

2020/905 sayılı KVKK Kararı

Bir sigorta şirketinin kişisel veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 24.11.2020 tarih ve 2020/905 sayılı Karar Özeti

2020/816 sayılı KVKK Kararı

Bir teknoloji şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 22/10/2020 tarih ve 2020/816 sayılı Karar Özeti

2020/787 sayılı KVKK Kararı

Sağlık sektöründe faaliyet gösteren bir şirketin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 09.10.2020 tarih ve 2020/787 sayılı Karar Özeti

2020/769 sayılı KVKK Kararı

İlgili kişinin eski çalışanı olduğu şirketi devralan veri sorumlusu şirket tarafından kanuna aykırı veri işleme faaliyetinde bulunulması hakkında Kişisel Verileri Koruma Kurulunun 08/10/2020 tarihli ve 2020/769 sayılı Karar Özeti

2020/766 sayılı KVKK Kararı

Bir Banka Tarafından Kurul Kararı ile Verilen Talimatların Gereğinin Yerine Getirilmemesi Hakkında Kişisel Verileri Koruma Kurulu'nun 08/10/2020 Tarihli ve 2020/766 Sayılı Karar Özeti

2020/765 sayılı KVKK Kararı

Bir Banka Tarafından Kurul Kararı ile Verilen Talimatın Gereğinin Yerine Getirilmemesi Hakkında Kişisel Verileri Koruma Kurulu'nun 08/10/2020 Tarihli ve 2020/765 Sayılı Karar Özeti

2020/763 sayılı KVKK Kararı

İnternette market alışveriş hizmeti veren veri sorumlusunun veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 01.10.2020 tarih ve 2020/763 sayılı Karar Özeti

2020/755 sayılı KVKK Kararı

İlgili kişinin aidat borcu bilgisinin site yönetimi tarafından ev sahibine iletilmesi hakkında Kişisel Verileri Koruma Kurulunun 29/09/2020 tarihli ve 2020/755 sayılı Karar Özeti

2020/746 sayılı KVKK Kararı

İlgili kişinin veri sorumlusu ile abonelik sözleşmesi kurma amacıyla gerçekleştirdiği telefon görüşmesi kayıtlarına erişim talebi hakkında Kişisel Verileri Koruma Kurulunun 29/09/2020 tarihli ve 2020/746 sayılı Karar Özeti

2020/744 sayılı KVKK Kararı

Bir Bankanın veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 29.09.2020 tarih ve 2020/744 sayılı Karar Özeti

2020/715 sayılı KVKK Kararı

Bir e-ticaret şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 17/09/2020 tarih ve 2020/715 sayılı Karar Özeti

2020/710 sayılı KVKK Kararı

İcra Müdürlükleri tarafından ilgili kişilerin yakınlarına haciz ihbarnamesi gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 17/09/2020 tarih ve 2020/710 sayılı Karar Özeti

2020/691 sayılı KVKK Kararı

İlgili kişinin cep telefonu numarasının, açık rızası olmaksızın bir dernek tarafından reklam içerikli SMS gönderimi için işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 10/09/2020 tarihli ve 2020/691 Sayılı Karar Özeti

2020/667 sayılı KVKK Kararı

Bir sigorta şirketinin ilgili kişiye vereceği hizmeti açık rıza şartına bağlaması sebebiyle Kuruma iletilen şikâyet hakkında Kişisel Verileri Koruma Kurulunun 03/09/2020 tarihli ve 2020/667 sayılı Karar Özeti

2020/649 sayılı KVKK Kararı

Biyometrik imza verisinin kullanılmasına ilişkin görüş talebi ile ilgili olarak Kişisel Verileri Koruma Kurulunun 27.08.2020 Tarihli ve 2020/649 Sayılı Karar Özeti

2020/622 sayılı KVKK Kararı

18 yaşını doldurmamış ilgili kişiye ait sağlık raporunun imha edilmesine yönelik ilgili kişinin babası tarafından veri sorumlusuna başvurulması ve cevap alınamaması üzerine ilgili kişinin kendisi tarafından Kurumumuza şikayette bulunulması hakkında Kişisel Verileri Koruma Kurulunun 11/08/2020 tarihli ve 2020/622 sayılı Karar Özeti

2020/608 sayılı KVKK Kararı

İlgili kişinin, bilet satın almamasına karşın bir havayolu şirketinden uçak bileti satın aldığına dair SMS alması hakkında Kişisel Verileri Koruma Kurulunun 11/08/2020 tarihli ve 2020/608 sayılı Karar Özeti

2020/567 sayılı KVKK Kararı

Bir oyuncak perakendecisi veri sorumlusunun veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 22/07/2020 tarih ve 2020/567 sayılı Karar Özeti

2020/560 sayılı KVKK Kararı

Site Yönetimlerine ilişkin 6698 sayılı Kişisel Verilerin Korunması Kanunu ile 634 sayılı Kat Mülkiyeti Kanunu çerçevesinde Kişisel Verileri Koruma Kurulu'nun 22.07.2020 tarihli ve 2020/560 sayılı Kararı'nda yer alan değerlendirmeler

2020/559 sayılı KVKK Kararı

Kişisel verilerin 108 sayılı Sözleşme dayanak gösterilerek yurt dışına aktarılması hakkında Kişisel Verileri Koruma Kurulunun 22/07/2020 tarih ve 2020/559 sayılı Karar Özeti

2020/542 sayılı KVKK Kararı

Aynı gerçek kişinin, yurt dışında yerleşik birden fazla veri sorumlusu için irtibat kişisi olarak atanması hakkındaki görüş talebi ile ilgili olarak Kişisel Verileri Koruma Kurulunun 16.07.2020 tarihli ve 2020/542 sayılı Karar Özeti

2020/532 sayılı KVKK Kararı

Bir sigorta şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 09/07/2020 tarih ve 2020/532 sayılı Karar Özeti

2020/530 sayılı KVKK Kararı

Bir bankanın veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 09/07/2020 tarih ve 2020/530 sayılı Karar Özeti

2020/511 sayılı KVKK Kararı

Bir sigorta şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 30.06.2020 tarih ve 2020/511 sayılı Karar Özeti

2020/508 sayılı KVKK Kararı

Bazı avukatların avukat sorgulama siteleri ile ilgili ihbar başvuruları hakkında Kişisel Verileri Koruma Kurulunun 30/06/2020 tarih ve 2020/508 sayılı Karar Özeti

2020/507 sayılı KVKK Kararı

Ölenin sağlık verisinin yasal mirasçısı tarafından talep edilmesi hakkında Kişisel Verileri Koruma Kurulunun 30/06/2020 tarihli ve 2020/507 Sayılı Karar Özeti

2020/504 sayılı KVKK Kararı

Veri sorumlusu bir havayolu şirketi tarafından ilgili kişiye ait çağrı merkezi görüşme kayıtlarının transkriptinin teslim edilmemesi hakkında Kişisel Verileri Koruma Kurulunun 30/06/2020 tarihli ve 2020/504 sayılı Karar Özeti

2020/494 sayılı KVKK Kararı

İlgili kişinin bir kargo şirketine karşı açtığı işe iade davasında, kişisel verisi olan kamera görüntülerinin kargo şirketi tarafından mahkemeye sunulması hakkında Kişisel Verileri Koruma Kurulunun 25/06/2020 tarihli ve 2020/494 sayılı Karar Özeti

2020/482 sayılı KVKK Kararı

Veri Sorumluları Siciline Kayıt Tarihlerinin Uzatılması ile İlgili Kişisel Verileri Koruma Kurulunun 23/06/2020 Tarihli ve 2020/482 Sayılı Kararı

2020/471 sayılı KVKK Kararı

Ülkemizde temsilciliği bulunan bir yabancı bankanın 6698 sayılı Kanun kapsamında veri sorumlusu sayılıp sayılmayacağı ve Veri Sorumluları Siciline kayıt yükümlülüğü hakkındaki görüş talebi ile ilgili olarak Kişisel Verileri Koruma Kurulunun 23.06.2020 tarihli ve 2020/471 sayılı Karar Özeti

2020/466 sayılı KVKK Kararı

Bir sigorta şirketinin acentesinde gerçekleşen veri ihlali hakkında Kişisel Verileri Koruma Kurulunun 16.06.2020 tarih ve 2020/466 sayılı Karar Özeti

2020/465 sayılı KVKK Kararı

Kurumsal yazılım hizmeti sunan bir veri sorumlusunun veri ihlali bildirimini hakkında Kişisel Verileri Koruma Kurulunun 16/06/2020 tarih ve 2020/465 sayılı Karar Özeti

2020/463 sayılı KVKK Kararı

İlaç sektöründe faaliyet yürüten bir veri sorumlusunun veri ihlali bildirimini hakkında Kişisel Verileri Koruma Kurulunun 16/06/2020 tarih ve 2020/463 sayılı Karar Özeti

2020/435 sayılı KVKK Kararı

Bir kargo firmasında çalışan ilgili kişinin iş akdinin haksız feshedilmesi sonrası özlük dosyası kapsamında yer alan kişisel verilerinin birer suretinin tarafına verilmesi talebine veri sorumlusu tarafından cevap verilmemesi hakkında Kişisel Verileri Koruma Kurulunun 28/05/2020 tarihli ve 2020/435 sayılı Karar Özeti

2020/429 sayılı KVKK Kararı

İlgili kişinin kişisel verilerinin, hakkında icra takibi yapan avukat tarafından hukuka aykırı olarak işlenmesi ve açıklanmasına ilişkin şikayet ile ilgili Kişisel Verileri Koruma Kurulunun 28/05/2020 Tarihli ve 2020/429 Sayılı Karar Özeti

2020/421 sayılı KVKK Kararı

Kişisel bakım sektöründe faaliyet yürüten bir veri sorumlusunun veri ihlali bildirimini hakkında Kişisel Verileri Koruma Kurulunun 22/05/2020 tarih ve 2020/421 sayılı Karar Özeti

2020/414 sayılı KVKK Kararı

Hakkında hüküm verildiği suçtan dolayı cezası infaz edilen ilgili kişiye ait haberin yayımlandığı gazetenin internet sitesinden kaldırılması talebi hakkında Kişisel Verileri Koruma Kurulunun 22/05/2020 tarihli ve 2020/414 sayılı Karar Özeti

2020/407 sayılı KVKK Kararı

İlgili kişinin tahlil sonuçlarının veri sorumlusu hastane tarafından hukuka aykırı şekilde üçüncü kişilere aktarılması hakkında Kişisel Verileri Koruma Kurulunun 20/05/2020 tarihli ve 2020/407 sayılı Karar Özeti

2020/404 sayılı KVKK Kararı

İşverenin, işçisine ait kişisel verileri ve özel nitelikli kişisel verileri; aydınlatma yükümlülüğünü yerine getirmeden ve hukuka aykırı işlemesi hakkında Kişisel Verileri Koruma Kurulunun 20/05/2020 tarihli ve 2020/404 sayılı Karar Özeti

2020/396 sayılı KVKK Kararı

İlgili kişinin, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili özel nitelikli kişisel verilerinin özlük dosyasından çıkarılması talebi hakkında Kişisel Verileri Koruma Kurulunun 20/05/2020 tarihli ve 2020/396 sayılı Kararı

2020/379 sayılı KVKK Kararı

Bir tıp merkezinin internet sitesinde video tanıtım bölümü içerisinde görsel ve işitsel kişisel verileri işlenen ilgili kişinin başvurusuna veri sorumlusu tıp merkezi tarafından cevap verilmemesi hakkında Kişisel Verileri Koruma Kurulunun 14/05/2020 tarihli ve 2020/379 sayılı Karar Özeti

2020/359 sayılı KVKK Kararı

Bir bankanın veri ihlali bildirimini hakkında Kişisel Verileri Koruma Kurulunun 07/05/2020 tarih ve 2020/359 sayılı Karar Özeti

2020/357 sayılı KVKK Kararı

Bir sigorta şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 07/05/2020 tarih ve 2020/357 sayılı Karar Özeti

2020/355 sayılı KVKK Kararı

İlgili kişiye ait Medula Eczane çıktılarının eczacının eşi tarafından kullanılması hakkında Kişisel Verileri Koruma Kurulunun 07/05/2020 Tarihli ve 2020/355 Sayılı Karar Özeti

2020/345 sayılı KVKK Kararı

Bilgisayar oyunları alanında faaliyet gösteren veri sorumlusunun veri ihlali bildirimini hakkında Kişisel Verileri Koruma Kurulunun 05/05/2020 tarih ve 2020/345 sayılı Karar Özeti

2020/344 sayılı KVKK Kararı

Bir bankanın veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 05.05.2020 tarih ve 2020/344 sayılı Karar Özeti

2020/335 sayılı KVKK Kararı

İlgili kişinin araç kiralama hizmeti alması esnasında kişisel verilerinin işlenmesine dair açık rıza vermemesi üzerine kiralama hizmetinden yararlandırılmamasına ilişkin Kişisel Verileri Koruma Kurulu'nun 05/05/2020 tarihli ve 2020/335 sayılı Karar Özeti

2020/336 sayılı KVKK Kararı

İlgili kişinin kendisine iletilmesi gereken cevap yazısının veri sorumlusu tarafından resmi yazı şeklinde, çalıştığı birime gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 05/05/2020 tarihli ve 2020/336 sayılı Karar Özeti

2020/325 sayılı KVKK Kararı

Kurumumuza Bir Şahıs Tarafından Vekaleten İntikal Ettirilen Usulen Eksik Nitelikteki Çok Sayıda Başvuru Hakkında Kişisel Verileri Koruma Kurulunun 30/04/2020 Tarihli ve 2020/325 Sayılı Karar Özeti

2020/315 sayılı KVKK Kararı

Veri Sorumluları Siciline Kayıt Yükümlülüğünden İstisna Tutulacak Veri Sorumluları ile ilgili Kişisel Verileri Koruma Kurulunun 22/04/2020 Tarihli ve 2020/315 Sayılı Kararı

2020/307 sayılı KVKK Kararı

Türkiye Ticaret Sicili Gazetesinde açık bir şekilde ilan edilmeyen kişisel verilerin, talepleri üzerine kamu kurum ve kuruluşlarıyla paylaşılması hususuna ilişkin Kişisel Verileri Koruma Kurulunun 22/04/2020 tarihli ve 2020/307 sayılı Karar Özeti

2020/286 sayılı KVKK Kararı

Bir oyun şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 16.04.2020 tarih ve 2020/286 sayılı Karar Özeti

2020/255 sayılı KVKK Kararı

Veri sorumlusu eğitim kurumu tarafından şikayetçinin çocuklarının özel nitelikli kişisel verilerinin hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 02/04/2020 tarihli ve 2020/255 sayılı Karar Özeti

2020/226 sayılı KVKK Kararı

İlgili kişinin, bir Valilikte görev yapmakta iken, Valilik çalışanı tarafından hukuka aykırı olarak elde edildiği iddia edilen kişisel verilerinin Valiliğe dijital ortamda sunulması hakkında Kişisel Verileri Koruma Kurulunun 19/03/2020 tarih ve 2020/226 sayılı Karar Özeti

2020/213 sayılı KVKK Kararı

Bir internet servis sağlayıcısının veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 12.03.2020 tarih ve 2020/213 sayılı Karar Özeti

2020/212 sayılı KVKK Kararı

Ses kayıt özelliği bulunan güvenlik kamerası kullanılması ile ilgili Kişisel Verileri Koruma Kurulunun 12/03/2020 tarihli ve 2020/212 sayılı Karar Özeti

2020/201 sayılı KVKK Kararı

Bir bankanın veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 03/03/2020 tarih ve 2020/201 sayılı Karar Özeti

2020/196 sayılı KVKK Kararı

İlgili kişiye ait kişisel verinin denetim faaliyeti kapsamında bir kamu kurumuna aktarılmasına ilişkin şikayet hakkında Kişisel Verileri Koruma Kurulunun 03/03/2020 Tarihli ve 2020/196 Sayılı Karar Özeti

2020/191, 2020/192, 2020/193, 2020/194 sayılı KVKK Kararları

Risk Merkezindeki verilerin muhtelif faktoring şirketleri tarafından ihlal edildiğinin ihbar edilmesine ilişkin Kişisel Verileri Koruma Kurulunun 03.03.2020 Tarihli ve 2020/191, 2020/192, 2020/193 ve 2020/194 Sayılı Karar Özeti

2020/187 sayılı KVKK Kararı

İlgili kişinin oturmakta olduğu binaya, komşusu tarafından kamera yerleştirilerek kayıt ve izleme gerçekleştirilmesi hakkında Kişisel Verileri Koruma Kurulunun 27/02/2020 tarihli ve 2020/187 sayılı Karar Özeti

2020/173 sayılı KVKK Kararı

Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/173 Sayılı Karar Özeti

2020/172 sayılı KVKK Kararı

İlgili kişinin cep telefonunun özel bir hastane tarafından izinsiz aranması hakkında Kişisel Verileri Koruma Kurulunun 27/02/2020 tarih ve 2020/172 sayılı Karar Özeti

2020/167 sayılı KVKK Kararı

Spor salonu hizmeti sunan veri sorumlusunun, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/167 Sayılı Karar Özeti

2020/166 sayılı KVKK Kararı

İlgili kişinin kullanımına izin vermediği kredi kartı bilgilerinin veri sorumlusu araç kiralama şirketi tarafından kullanılması hakkında Kişisel Verileri Koruma Kurulunun 27/02/2020 tarihli ve 2020/166 sayılı Karar Özeti

2020/145 sayılı KVKK Kararı

Veri sorumlusu tarafından ilgili kişilerin kişisel verilerinin hukuka aykırı şekilde internet gazetesi üzerinden yayımlanması hakkında Kişisel Verileri Koruma Kurulunun 18/02/2020 tarihli ve 2020/145 sayılı Karar Özeti

2020/138 sayılı KVKK Kararı

Veri sorumlusu işveren tarafından, iş sözleşmesi tek taraflı olarak feshedilen ve işe iade davası açan ilgili kişiye ait özlük dosyasında yer alan sağlık raporunun dava savunmasında kullanılmak suretiyle mahkemeye sunulması hakkında Kişisel Verileri Koruma Kurulunun 18/02/2020 tarihli ve 2020/138 sayılı Karar Özeti

2020/124 sayılı KVKK Kararı

Veri sorumlusu havayolu řirketi bünyesindeki alıřanın ilgili kiřiye ait kiřiisel verileri 6698 sayılı Kiřiisel Verilerin Korunması Kanununa aykırı řekilde řirket kayıtlarından elde etmesi hakkında Kiřiisel Verileri Koruma Kurulunun 13/02/2020 tarihli ve 2020/124 sayılı Karar Özeti

2020/120 sayılı KVKK Kararı

İlgili kiřilerin kiřiisel verileri olan banka hesap hareketlerinin, mevduat bilgilerinin, para yatırma ve ekme iřlemlerinin açık rızaları olmaksızın vergi müfettiř yardımcısı tarafından hukuka aykırı olarak iřlenmesi hakkında Kiřiisel Verileri Koruma Kurulunun 13/02/2020 tarihli ve 2020/120 sayılı Karar Özeti

2020/118 sayılı KVKK Kararı

İlgili kiřinin, veri sorumlusu bir banka nezdindeki kiřiisel verileri olan hesap ve kiralık kasa bilgilerinin aktarılması hakkında Kiřiisel Verileri Koruma Kurulunun 13/02/2020 tarihli ve 2020/118 sayılı Karar Özeti

2020/113 sayılı KVKK Kararı

Elektronik satıř hizmeti saęlayan bir řirketin veri ihlal bildirimini hakkında Kiřiisel Verileri Koruma Kurulunun 11/02/2020 tarih ve 2020/113 sayılı Karar Özeti

2020/108 sayılı KVKK Kararı

Veri sorumlusu saęlık firması tarafından eski alıřanı olan ilgili kiřinin kiřiisel verilerinin rızası alınmaksızın aktarımı hakkında Kiřiisel Verileri Koruma Kurulunun 11/02/2020 tarihli ve 2020/108 sayılı Karar Özeti

2020/103 sayılı KVKK Kararı

Bir Bankanın Potansiyel Müřteri Kazanımı Amacıyla İlgili Kiřinin Kiřiisel Verilerini Hukuka Aykırı řekilde İřleyerek Hesap Amasına İliřkin Olarak Kurula Yapılan Bařvuru Hakkında Kiřiisel Verileri Koruma Kurulunun 06/02/2020 Tarihli ve 2020/103 Sayılı Karar Özeti

2020/93 sayılı KVKK Kararı

Geçmiş sağlık verilerinin düzeltilmesine/silinmesine yönelik şikâyetler hakkında Kişisel Verileri Koruma Kurulunun 06/02/2020 tarihli ve 2020/93 sayılı Karar Özeti

2020/86 sayılı KVKK Kararı

Bir uçak bileti satış firması olan veri sorumlusu hakkındaki şikâyetle ilgili Kişisel Verileri Koruma Kurulunun 06.02.2020 Tarihli ve 2020/86 Sayılı Karar Özeti

2020/78 sayılı KVKK Kararı

Veri sorumlusu bankanın ilgili kişiye ait kredi kartı ekstresinde yer alan kişisel verileri yanlış e-posta hesabına göndermesi hakkında Kişisel Verileri Koruma Kurulunun 30/01/2020 tarihli ve 2020/78 sayılı Karar Özeti

2020/67 sayılı KVKK Kararı

İlgili kişiye rızası bulunmamasına rağmen bir gayrimenkul şirketi tarafından SMS aracılığıyla gönderilen reklam ve bildirimler hakkında Kişisel Verileri Koruma Kurulunun 27/01/2020 tarih ve 2020/67 sayılı Karar Özeti

2020/66 sayılı KVKK Kararı

İlgili kişinin irtibat numarasının bir elektrik dağıtım şirketi tarafından herhangi bir işleme şartına dayanılmaksızın işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 27/01/2020 tarihli ve 2020/66 sayılı Karar Özeti

2020/65 sayılı KVKK Kararı

Ulaşım hizmeti sunan bir mobil uygulama kapsamında işlenen kişisel veriler hakkında Kişisel Verileri Koruma Kurulunun 27/01/2020 tarih ve 2020/65 sayılı Karar Özeti

2020/63 sayılı KVKK Kararı

Veri sorumlusu hastanede uygulanan beyaz kod kapsamında ilgili kişinin işlenen kişisel verileri hakkında Kişisel Verileri Koruma Kurulunun 27/01/2020 tarihli ve 2020/63 sayılı Karar Özeti

2020/59 sayılı KVKK Kararı

İlgili kişinin ortağı olduğu şirkette kullandığı e-posta adresine izinsiz ve hukuka aykırı olarak erişildiği iddiası hakkında Kişisel Verileri Koruma Kurulunun 27/01/2020 tarihli ve 2020/59 sayılı Karar Özeti

2020/58 sayılı KVKK Kararı

Bir Sigorta Acentesinin müşterilerine ait kişisel verileri herkese açık sosyal medya platformlarında müşterilerinden habersiz olarak ve reklam amacıyla paylaşması hakkında Kişisel Verileri Koruma Kurulunun 27/01/2020 Tarihli ve 2020/58 Sayılı Karar Özeti

2020/50 sayılı KVKK Kararı

Bir perakende giyim firmasının veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 20/01/2020 tarih ve 2020/50 sayılı Karar Özeti

2020/43 sayılı KVKK Kararı

İlgili kişiye ait verilerin veri sorumlusu bir banka tarafından rızası olmaksızın babası ile paylaşılması karşısında kişinin Bankadan tazminat talep etmesi hakkında Kişisel Verileri Koruma Kurulunun 16/01/2020 Tarihli ve 2020/43 Sayılı Karar Özeti

2020/41 sayılı KVKK Kararı

İlgili kişinin kişisel verilerinin hukuka aykırı işlendiği iddiası kapsamında veri sorumlusu bankadan talep ettiği tazminat talebinin karşılanmaması hakkında Kişisel Verileri Koruma Kurulunun 16/01/2020 Tarihli ve 2020/41 Sayılı Karar Özeti

2020/34 sayılı KVKK Kararı

İlgili kişinin dergi aboneliği işlemleri ile ilgili bir çağrı merkezine vermiş olduğu telefon numarasının, anılan çağrı merkezi tarafından bir gıda şirketinin reklamının yapılması amacıyla aranması hakkında Kişisel Verileri Koruma Kurulunun 16/01/2020 Tarihli ve 2020/34 Sayılı Karar Özeti

2020/32 sayılı KVKK Kararı

Bir banka tarafından ilgili kişinin kredi kartının rızası dışında üçüncü kişilere teslim edilmesine ilişkin Kişisel Verileri Koruma Kurulu'nun 16/01/2020 Tarih ve 2020/32 Sayılı Karar Özeti

2020/26 sayılı KVKK Kararı

Kişisel verilerin veri sorumlusu bir avukat tarafından kısa mesaj yoluyla üçüncü kişilere ifşa edilmesi hakkında Kişisel Verileri Koruma Kurulunun 14.01.2020 Tarihli ve 2020/26 Sayılı Karar Özeti

2020/20 sayılı KVKK Kararı

Bir Eğitim Kurumu tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmaksızın işlenmesi ve ilgili numaraya reklam/bilgilendirme içerikli mesaj gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 14/01/2020 Tarihli ve 2020/20 Sayılı Karar Özeti

2020/13 sayılı KVKK Kararı

İlgili kişi ile veri sorumlusu şirket arasında gerçekleştirilen telefon görüşmelerine ilişkin kayıtların ilgili kişiye verilmesi yönündeki talebin reddedilmesi hakkında Kişisel Verileri Koruma Kurulunun 14/01/2020 Tarihli ve 2020/13 Sayılı Karar Özeti

2019/393 sayılı KVKK Kararı

Kişisel Veri Güvenliği Rehberinde geçen "personel gizlilik sözleşmesi" imzalatılmasının 657 sayılı Devlet Memurları Kanununa tabii olarak çalışanlar için gerekli olup olmadığı ile ilgili Kişisel Verileri Koruma Kurulunun 26/12/2019 tarihli ve 2019/393 sayılı Karar Özeti

2019/389 sayılı KVKK Kararı

Aday Puanlarının Rıza Alınmaksızın, İnternet Sitesinde Paylaşılması Hakkındaki Görüş Talebi ile ilgili Kişisel Verileri Koruma Kurulunun 26/12/2019 Tarihli ve 2019/389 Sayılı Karar Özeti

2019/387 sayılı KVKK Kararı

Veri Sorumluları Siciline Kayıt Yükümlülüğüne İlişkin Kurulca Belirlenen Sürelerin Uzatılması ile ilgili Kişisel Verileri Koruma Kurulunun 17/12/2019 Tarihli ve 2019/387 Sayılı Kararı

2019/276 sayılı KVKK Kararı

Sevinç Eğitim Kurumlarının kişisel veri işleme şartları olmaksızın ilgili kişinin cep telefonuna reklam amaçlı kısa mesaj göndermesi hakkında Kişisel Verileri Koruma Kurulunun 18.09.2019 Tarihli ve 2019/276 sayılı Karar Özeti

2019/372 sayılı KVKK Kararı

Bir gazete tarafından ilgili kişinin özel nitelikli kişisel verileri hakkında haber yapılmasına ilişkin Kişisel Verileri Koruma Kurulu'nun 09/12/2019 tarih ve 2019/372 sayılı Karar Özeti

2019/269 sayılı KVKK Kararı

Facebook hakkında Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/269 sayılı Karar Özeti

2019/353 sayılı KVKK Kararı

Dernek, Vakıf Ve Sendikaların Veri Sorumluları Siciline Kayıt Yükümlülüğü İstisnası Hakkında Kişisel Verileri Koruma Kurulunun 26.11.2019 Tarihli ve 2019/353 Sayılı Karar Özeti

2019/352 sayılı KVKK Kararı

Bir Banka Nezdinde Gerçekleşen Veri İhlali ile İlgili Olarak Kişisel Verileri Koruma Kurulunun 26/11/2019 Tarihli ve 2019/352 Sayılı Karar Özeti

2019/333 sayılı KVKK Kararı

Telekomünikasyon sektöründe faaliyet gösteren veri sorumlusu tarafından şikayetçiye, ad ve soyadı benzerliği olan başka bir abonesinin fatura bilgilerinin e-posta yoluyla iletilmesi hakkında Kişisel Verileri Koruma Kurulunun 07/11/2019 Tarihli ve 2019/333 Sayılı Karar Özeti

2019/332 sayılı KVKK Kararı

Bir doktor tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmaksızın işlenmesi ve ilgili numaraya reklam/bilgilendirme içerikli mesaj gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 07/11/2019 Tarihli ve 2019/332 Sayılı Karar Özeti

2019/331 sayılı KVKK Kararı

İlgili kişi tarafından alenileştirilen kişisel verinin, alenileştirme amacı dışında işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 07/11/2019 Tarihli ve 2019/331 Sayılı Karar Özeti

2019/316 sayılı KVKK Kararı

Bilimsel amaçlarla kayıt altına alınan bilimsel veri niteliğindeki kan, serum ve doku örneklerinin ihmal sonucu bozulması ve sonrasında imha edilmesi hakkındaki ihbara ilişkin Kişisel Verileri Koruma Kurulunun 30/10/2019 tarihli ve 2019/316 sayılı Karar Özeti

2019/297 sayılı KVKK Kararı

Veri sorumlusu tarafından ilgili kişiye gönderilen reklam amaçlı SMS'ler hakkında Kişisel Verileri Koruma Kurulunun 01/10/2019 Tarihli ve 2019/297 Sayılı Karar Özeti

2019/296 sayılı KVKK Kararı

Bir operatör şirketinin, ilgili kişinin internet sitesi üzerinden yapmış olduğu başvurusunu kimlik teyidi yapamadığı gerekçesiyle reddetmesine ilişkin olarak Kurula yapılan başvuru hakkında Kişisel Verileri Koruma Kurulunun 01/10/2019 Tarihli ve 2019/296 Sayılı Karar Özeti

2019/294 sayılı KVKK Kararı

Bir havayolu taşımacılık şirketinin (veri sorumlusu) sunduğu sadakat programını kullanan ilgili kişinin kullanıcı adı ve parola bilgilerini değiştirme talebi karşısında ilgili kişiden arkalı önlü kimlik görüntüsü talep eden veri sorumlusu hakkında Kişisel Verileri Koruma Kurulunun 01.10.2019 Tarihli ve 2019/294 sayılı Karar Özeti

2019/273 sayılı KVKK Kararı

Ölü kişilerin verilerine yakınlarının erişim talebi hakkında Kişisel Verileri Koruma Kurulunun 18/09/2019 Tarihli ve 2019/273 Sayılı Karar Özeti

2019/265 sayılı KVKK Kararı

"VERBİS Kayıt Sürelerinin Uzatılması" hakkında 03/09/2019 tarihli ve 2019/265 sayılı Kurul Kararı

2019/255 sayılı KVKK Kararı

Bir turizm şirketi hakkında Kişisel Verileri Koruma Kurulunun 27.08.2019 tarih ve 2019/255 sayılı Karar Özeti

2019/254 sayılı KVKK Kararı

S Şans Oyunları A.Ş hakkında Kişisel Verileri Koruma Kurulunun 27.08.2019 tarih ve 2019/254 sayılı Karar Özeti

2019/227 sayılı KVKK Kararı

Bir bankanın, ilgili kişinin cep telefonu numarasını bankaya veriliş amacı dışında kullanması hakkında Kişisel Verileri Koruma Kurulunun 18/09/2019 Tarihli ve 2019/227 Sayılı Karar Özeti

2019/225 sayılı KVKK Kararı

Yurtdışında yerleşik Tüzel kişilerin Türkiye'deki Şubeleri ile İrtibat Bürolarının Sicile Kayıt Yükümlülüğü Hakkındaki Görüş Talebi ile ilgili Kişisel Verileri Koruma Kurulunun 23/07/2019 tarih ve 2019/225 sayılı Kararı

2019/222 sayılı KVKK Kararı

Dubsmash Inc. hakkında Kişisel Verileri Koruma Kurulunun 17/07/2019 Tarihli ve 2019/222 Sayılı Karar Özeti

2019/206 sayılı KVKK Kararı

Veri sorumlusunun, web sitesinde kişisel verilerin işlenmesini hizmet şartı olarak talep ettiği ve aydınlatma yükümlülüğünü usulüne uygun yerine getirmediği iddiaları hakkında Kişisel Verileri Koruma Kurulunun 08/07/2019 tarih ve 2019/206 sayılı Karar Özeti

2019/204 sayılı KVKK Kararı

Bir yatırım şirketi tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmadan işlenmesi ve reklam/bilgilendirme amaçlı aranması hakkında Kuruma yaptığı başvuru ile ilgili Kişisel Verileri Koruma Kurulunun 08/07/2019 Tarihli ve 2019/204 Sayılı Karar

2019/198 sayılı KVKK Kararı

İlgili kişinin, bir sadakat programı kapsamında veri sorumlusunca hukuka aykırı kişisel veri işlendiği yolundaki ihbarı" hakkında Kişisel Verileri Koruma Kurulunun 05/07/2019 tarihli ve 2019/198 sayılı Karar Özeti

2019/188 sayılı KVKK Kararı

Öğrencilerin kişisel verisi niteliğindeki sınav sonuçlarını internet ortamında yayımlayan Mimar Sinan Güzel Sanatlar Üniversitesi'nin uygulaması hakkında Kuruma yapılmış olan başvuru hakkında Kişisel Verileri Koruma Kurulunun 01/07/2019 Tarihli ve 2019/188 Sayılı Karar

2019/170 sayılı KVKK Kararı

Bir perakende giyim firmasının veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 18/06/2019 tarih ve 2019/170 sayılı Karar Özeti

2019/166 sayılı KVKK Kararı

İlgili kişiye ait telefon numarasına kendisine ait olmayan içeriğin gönderilmesi ile ilgili Kişisel Verileri Koruma Kurulunun 31/05/2019 Tarihli ve 2019/166 Sayılı Karar

2019/162 sayılı KVKK Kararı

Bir anonim şirketin (veri sorumlusu) ilgili kişinin açık rızası dışı elektronik ticari ileti göndermesine ilişkin Kişisel Verileri Koruma Kurulunun 31.05.2019 Tarihli ve 2019/162 Sayılı Karar Özeti

2019/159 sayılı KVKK Kararı

Bir varlık yönetim şirketinin ilgili kişiye aynı konu ile ilgili birden çok mesaj gönderimine ilişkin Kişisel Verileri Koruma Kurulunun 31/05/2019 Tarihli ve 2019/159 Sayılı Karar

2019/157 sayılı KVKK Kararı

Kurumsal e-posta hizmetinin, Google (gmail) üzerinden yine aynı uzantıya sahip olarak kullanılıp kullanılmayacağı ilişkin Kişisel Verileri Koruma Kurulunun 31/05/2019 Tarihli ve 2019/157 Sayılı Karar

2019/144 sayılı KVKK Kararı

Cathay Pasific Airway Limited Hakkında Kişisel Verileri Koruma Kurulunun 16.05.2019 Tarih ve 2019/144 Sayılı Karar Özeti

2019/143 sayılı KVKK Kararı

Marriott International Inc. Hakkında Kişisel Verileri Koruma Kurulunun 16.05.2019 Tarih ve 2019/143 Sayılı Karar Özeti

2019/141 sayılı KVKK Kararı

Clickbus Seyahat Hizmetleri A.Ş. Hakkında Kişisel Verileri Koruma Kurulunun 16.05.2019 Tarih ve 2019/141 Sayılı Karar Özeti

2019/138 sayılı KVKK Kararı

Bir şirket sahibinin, çalışanının Whatsapp yazışmalarını hukuka aykırı olarak elde etmesi hakkında Kişisel Verileri Koruma Kurulunun 16/05/2019 Tarihli ve 2019/138 Sayılı Karar Özeti

2019/125 sayılı KVKK Kararı

Yeterli Korumaya Sahip Ülkelerin Belirlenmesinde Esas Alınacak Kriterler

2019/122 sayılı KVKK Kararı

İlgili kişinin yaptığı başvuruyu cevaplandırmayan ve internet sitesi üzerinden yayımladığı aydınlatma metni mevzuatta düzenlenen şartları taşımayan T.C. Ziraat Bankası A.Ş. hakkında Kişisel Verileri Koruma Kurulunun 02/05/2019 tarihli ve 2019/122 sayılı Karar Özeti

2019/104 sayılı KVKK Kararı

Facebook nezdinde gerçekleşen veri ihlalinin değerlendirilmesi ile ilgili Kişisel Verileri Koruma Kurulunun 11.04.2019 tarih ve 2019/104 sayılı Kararı Özeti

2019/82 sayılı KVKK Kararı

Bir market zincirinin sadakat kart uygulamasına ilişkin ihbar ve şikayetler hakkında” Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/82 sayılı Karar Özeti

2019/81, 2019/165 sayılı KVKK Kararı

Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Karar

2019/78 sayılı KVKK Kararı

Veri sorumlusunun kanuni yükümlülüğünü yerine getirmek için işlediği kişisel verileri meşru menfaat çerçevesinde kullanma talebiyle Kuruma yapmış olduğu başvuru Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/78 Sayılı Karar Özeti

2019/52 sayılı KVKK Kararı

Kurul kararının yerine getirilmemesi hakkında Kişisel Verileri Koruma Kurulunun 05/03/2019 tarihli ve 2019/52 sayılı Karar Özeti

2019/47 sayılı KVKK Kararı

Bir şahsın, kendisi ve ailesi hakkındaki kişisel bilgilere hukuk dışı yollarla erişerek rızası dışında yargıya ve üçüncü kişilere aktardığı iddiasıyla bir başka şahıs hakkında Kuruma yapmış olduğu şikayet hakkında Kişisel Verileri Koruma Kurulunun 01/03/2019 tarihli ve 2019/47 sayılı Karar Özeti

2019/23 sayılı KVKK Kararı

Teknik servis hizmeti veren firmanın müşterilerine verdiği form/takip numarasının son hanelerinin değiştirilmesi yoluyla farklı kişilere ait kişisel verilere ulaşıldığı yolunda Kuruma iletilen ihbarın incelenmesi ve ihbara ilişkin alınan Kurul Kararının yerine getirilmemesi hakkında Kişisel Verileri Koruma Kurulunun 14/02/2019 tarihli ve 2019/23 sayılı Karar Özeti

2019/9 sayılı KVKK Kararı

Veri Sorumlusuna Başvuru ve Kurula Şikayet Sürelerinin Hesaplanmasına İlişkin Kişisel Verileri Koruma Kurulunun 24/01/2019 tarih ve 2019/9 sayılı Kararı

2018/156 sayılı KVKK Kararı

Yargı mercilerinin görev alanına giren konularla ilgili Kuruma yapılan başvurular hakkında Kişisel Verileri Koruma Kurulunun 24/12/2018 tarihli ve 2018/156 sayılı Kararı Özeti

2018/143 sayılı KVKK Kararı

“Sağlık verilerini Kanununun 6 ncı maddesinde yer alan işleme şartlarından birine dayanmadan üçüncü bir kişiye aktaran veri sorumlusu hakkında” Kişisel Verileri Koruma Kurulunun 05/12/2018 Tarihli ve 2018/143 Sayılı Kararı

2018/142 sayılı KVKK Kararı

İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi gereğince kişisel verilerin silinmemesi hakkında Kişisel Verileri Koruma Kurulunun 05/12/2018 tarihli ve 2018/142 sayılı Kararı Özeti

2018/131 sayılı KVKK Kararı

Tüzel kişiliğe ait elektronik ortamda yer alan verilerin başka bir tüzel kişilik tarafından talep edilmesi hakkında Kişisel Verileri Koruma Kurulunun 19/11/2018 tarihli ve 2018/131 sayılı Kararı Özeti

2018/118 sayılı KVKK Kararı

Kurul Kararının gereğinin süresi içinde yerine getirilmemesi hakkında Kişisel Verileri Koruma Kurulunun 16/10/2018 tarihli ve 2018/118 sayılı Kararı Özeti

2018/106 sayılı KVKK Kararı

Kimliği belirsiz kişi/kişilerin veri sorumlusu olarak kabul edilemeyeceği hakkında Kişisel Verileri Koruma Kurulunun 13/09/2018 tarihli ve 2018/106 sayılı Kararı Özeti

2018/91 sayılı KVKK Kararı

Kişisel verilere hukuka aykırı erişilmesini önleme yükümlülüğünü yerine getiremeyen veri sorumlusu hakkında Kişisel Verileri Koruma Kurulunun 26/07/2018 Tarihli ve 2018/91 Sayılı Kararı

2018/90 sayılı KVKK Kararı

Veri sorumlusu tarafından aydınlatma yükümlülüğü ve açık rıza onayı alınması süreçlerinin ayrı ayrı yerine getirilmesi gerektiği ile ilgili Kişisel Verileri Koruma Kurulunun 26/07/2018 tarihli ve 2018/90 sayılı Kararı Özeti

2018/88 sayılı KVKK Kararı

Sicile Kayıt Yükümlülüğünün Başlama Tarihleri ile ilgili Kişisel Verileri Koruma Kurulunun 19/07/2018 Tarihli ve 2018/88 Sayılı Kararı

2018/87 sayılı KVKK Kararı

Veri Sorumluları Siciline Kayıt Yükümlülüğünden İstisna Tutulacak Veri Sorumluları ile ilgili Kişisel Verileri Koruma Kurulunun 19/07/2018 Tarihli ve 2018/87 Sayılı Kararı

2018/75 sayılı KVKK Kararı

Arabulucuların Veri Sorumluları Siciline Kayıt Zorunluluğundan İstisna Tutulması ile ilgili Kişisel Verileri Koruma Kurulunun 05/07/2018 Tarihli ve 2018/75 Sayılı Kararı

2018/69 sayılı KVKK Kararı

Sicil dosyalarındaki kişisel verilerin, işlenmelerini gerektiren sebeplerin ortadan kalkmaması sebebiyle, imha edilmemesi gerektiği hakkında Kişisel Verileri Koruma Kurulunun 28/06/2018 Tarihli ve 2018/69 Sayılı Kararı

2018/68 sayılı KVKK Kararı

Gümrük Müşavirlerinin Sicile Kayıt İstisnası Hakkında Görüş Talebi ile ilgili Kişisel Verileri Koruma Kurulunun 28/06/2018 Tarihli ve 2018/68 Sayılı Kararı

2018/32 sayılı KVKK Kararı

Veri Sorumluları Siciline Kayıt Yükümlülüğünden İstisna Tutulacak Veri Sorumluları ile ilgili Kişisel Verileri Koruma Kurulunun 02/04/2018 Tarihli ve 2018/32 Sayılı Kararı

2023/426 sayılı KVKK Kararı

Tüketici Finansman Kredisiyle Alışveriş İmkânı Sunan Şirket Tarafından İlgili Kişilerden e-Devlet Şifrelerinin Talep Edilmesi hakkında Kişisel Verileri Koruma Kurulu'nun 22/03/2023 tarihli ve 2023/426 sayılı Karar Özeti

Karar Tarihi : 22/03/2023

Karar No : 2023/426

Konu Özeti: Tüketici Finansman Kredisiyle Alışveriş İmkânı Sunan Şirket Tarafından İlgili Kişilerden e-Devlet Şifrelerinin Talep Edilmesi

Kuruma intikal ettirilen bir ihbar dilekçesinde özetle;

Tüketici finansman kredisiyle alışveriş imkânı sunan Şirketten senetle televizyon alındığı sırada kendisinden e-Devlet şifresinin talep edildiği,

Kuruma intikal ettirilen bir diğer ihbar dilekçesinde ise özetle;

- Şirketin ihbar edenden e-Devlet şifresini istediği, ihbar edenin ısrarlar sonucunda şifre almadığını söyleyerek talebi reddettiği,
- İhbar edenin kendisi dışında birçok vatandaştan da e-Devlet şifrelerinin alındığının bilindiği hususları belirtilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gerekli işlemlerin yapılması talep edilmiştir.

Konuya ilişkin başlatılan resen inceleme çerçevesinde ihbar edilen veri sorumlusu Şirketin savunması talep edilmiş olup veri sorumlusunun ilk ihbar dilekçesine ilişkin cevabî yazısında özetle;

- İhbar edenin veri sorumlusu ile tüketici finansman sözleşmesi akdetmiş olduğu, kredi puanı yetersiz görüldüğünden ve işyerinde sigorta girişinin yeni yapıldığını belirtmesi üzerine son altı aylık güncel sigorta hizmet dökümü belgesi ile şubeye müracaat edilmesinin istendiği ve fakat ihbar eden kişi tarafından sözleşmenin iptal edildiği,
- İhbar edenin ürün satın almak için başvuruda bulunduğu, işlem yapmak amacıyla açık rızası ile irtibat numarasını bildirmiş olduğu, Şirketin Tüketici Finansman Kredisi kullanılmasına ilişkin ihbar edenin yeni işe başladığını beyan etmesi üzerine işe başlama kaydının sigorta hizmet dökümü

üzerinden teyit edilmesi amacıyla müşterinin en yakın şubeye davet edildiği ve sigorta kayıtlarının beyan edilmesinin talep edildiği, bu bilgilerin e-Devlet sistemi üzerinden temin edileceğinin sabit olduğu, şirketin ihbar edenin e-Devlet şifresini talep etmediği, ilgili kişinin e-Devlet şifresinin bilinmediği, müracaat anında müşterinin sigorta hizmet dökümünü görüntülemek, işe başladığını teyit etmek ve öğrenebilmek adına kendi rızası olduğu takdirde ve kendi cep telefonundan kendisinin görebileceği şekilde e-Devlet üzerinden talep edilen kayıtların gösterilmesinin talep edildiği, müşteri/ihbar edenin ilgili kayıtları paylaşmadığı ve sözleşmenin iptalini talep ettiği,

- İhbar edenin kişisel verilerinin işlenmesinin gerekçelerinin ise; şirketin hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, tüketici sözleşmesinin kullanımı açısından sigorta hizmet dökümü bilgisinin talep edilmesinin zorunluluğu, bir hakkın tesisi, kullanılması veya korunması için bilgi talebi olması, şirketin meşru menfaatleri için bilgi talebinin gerekli olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait bilgi talebinin gerekli olması olduğu

belirtilmiştir.

Aynı konuya ilişkin veri sorumlusu Şirketin ikinci ihbar dilekçesine ilişkin cevabî yazısında ise özetle;

- Somut olayda ihbar edenin veri sorumlusu ile taksitli satış sözleşmesi akdettiği, sonrasında bozuk olan ürün yerine yeni ürünün ilgili kişiye teslim edildiği, ardından bu üründe de arıza olunca ürün satış işleminin iptal olduğu ve ücret ödemesinin ihbar edene iade edildiği,

- Veri sorumlusunun, ilgili mevzuat çerçevesinde yükümlülüklerini yerine getirmek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almış olduğu,

Müşterilerden/ilgili kişilerden e-Devlet şifresi talep edildiği yönündeki iddiaların gerçek dışı olduğu, veri sorumlusunun Kanun gereğince, tüketici işlemleri sırasında herhangi bir veri tutmadığı; kimlik aslının ve iletişim bilgilerinin ilgili kişilerden kontrol amacıyla alındığı ve yapılan kontrollerin ardından kimlik aslının geri verilip suretinin dahi sistemlerde kayıt altına alınmadığı,

- İddia edildiği gibi e-Devlet şifresi ile taksitli satış sözleşmesi arasında bir illiyet bağının olmadığı, e-Devlet şifresi ile satış sözleşmesi arasında birbiri ile ilişkili bir işlemin söz konusu olmadığı, e-Devlet şifresi ile yapılacak bir işlemin de bulunmadığı,

- Kişisel verilerin korunması ve işlenmesi konusunda azami düzeyde teknik ve idari tedbirleri alan veri sorumlusunun, e-Devlet gibi kişiye ait özel bir alanı kullandığı iddiasının Şirket politikası ve uygulamaları ile ters düşeceği, bu açıdan hiçbir müşteriden herhangi bir şifre talep etme durumunun

söz konusu olmadığı, somut durumlar karşısında Şirket açısından herhangi bir cezai yaptırım oluşturabilecek bir durumun söz konusu olmadığı belirtilmiştir.

Konuya ilişkin yapılan inceleme neticesinde, Kişisel Verileri Koruma Kurulunun 22/03/2023 tarihli ve 2023/426 sayılı Kararı ile;

- Kişilerin kendilerine ait ad-soyadı, iletişim numarası gibi tüketici işlemlerinde kullanılan bilgilerin veri sorumlusunun veri kayıt sisteminde işlenmesinden ötürü, Kanunun 2'nci maddesinde yer alan hüküm dikkate alındığında Kuruma yapılan ihbarların Kanun kapsamında olduğu,
- Kanunun 3'üncü maddesinin birinci fıkrasının (ç) bendi gereği Şirket'in veri kayıt sisteminde kişisel verileri tutulan ihbarda bulunanların ilgili kişi, (1) maddesi gereği ilgili kişilerin kişisel verilerinin işleme amaç ve vasıtalarını belirleyen, veri kayıt sisteminin tutulmasından ve yönetilmesinden sorumlu tüzel kişi olan Şirket'in ise veri sorumlusu olduğu,
- Kişisel verilerin işleme şartlarının Kanun'un 5'inci maddesinde düzenlendiği; buna göre maddenin birinci fıkrasında; kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, ikinci fıkrasında -Kanunlarda açıkça öngörülmesi, -Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, -Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, -Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, -İlgili kişinin kendisi tarafından alenileştirilmiş olması, -Bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması, -İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması hallerinden birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğunun düzenlendiği,
- İlgili kişinin Kuruma sunduğu ihbar dilekçesinde Şirketten senetle televizyon alındığı ve kendisinden e-Devlet şifresinin talep edildiğinin ifade edildiği, başvuru ekinde yer alan ve Şirket tarafından ilgili kişinin cep telefonu numarasına gönderildiği anlaşılan kısa mesajda "E-devlet şifreniz ile beraber en yakın şubemize gelmenizi rica ederiz. (Sipariş no, kayıt tarihi:16.01.2022, ürünler başlıkları ile)" ifadelerinin yer aldığı görüldüğü,
- Veri sorumlusunun savunmasında; ihbar edenin Şirket ile tüketici finansmanı sözleşmesi akdetmiş olduğu, kredi puanı yetersiz görüldüğünden ve işyerinde sigorta girişinin yeni yapıldığını belirtmesi

üzerine son altı aylık güncel sigorta hizmet dökümü belgesi ile şubeye müracaat etmesinin istendiği ve ilgili kişi tarafından sözleşmenin iptal edildiği, tüketici sözleşmesinin kullanımı açısından sigorta hizmet dökümü bilgisinin talep edilmesinin zorunlu olduğu, bu bilgilerin e-Devlet sistemi üzerinden temin edileceği, e-Devlet şifresinin talep edilmediği, müracaat anında müşterinin sigorta hizmet dökümünü görüntülemek, işe başladığını teyit etmek ve öğrenebilmek adına şifreyi kendi rızası olduğu takdirde ve kendi cep telefonundan kendisinin görebileceği şekilde e-Devlet üzerinden girmek suretiyle talep edilen kayıtların gösterilmesinin istendiği, ilgili kişinin kayıtları paylaşmadığı ve sözleşmenin iptalini talep ettiği hususlarını belirtmiş olduğu,

- İlgili kişi ve veri sorumlusunun beyanları ile Kuruma sunulan belgelerden; ilgili kişinin veri sorumlusu ile tüketici finansmanı (kredisi) sözleşmesi yaptığı, ilgili kişiye iletilen kısa mesajda ilgili kişinin e-Devlet şifresi ile beraber şubeye çağırıldığı, ilgili kişinin ise e-Devlet şifresinin kullanılmasına yönelik rızası olmadığından sözleşmeyi iptal etmek istediğinin anlaşılmakta olduğu,
- Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerektiği, bu riskler belirlenirken kişisel verilerin özel nitelikli kişisel veri olup olmadığı, mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği, güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliğinin dikkate alınması gerektiği, bu risklerin tanımlanması ve önceliğinin belirlenmesinden sonra söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatiflerinin maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmesi ve gerekli teknik ve idari tedbirlerin planlanarak uygulamaya konulması gerektiği,
- Bununla birlikte Kişisel Veri Güvenliği Rehberi'nde veri sorumlularınca alınabilecek idari tedbirlerin; "kişisel veri işleme envanteri hazırlanması, kurumsal politikalar (erişim, bilgi güvenliği, kullanım, saklama ve imha vb.), sözleşmeler (veri sorumlusu-veri sorumlusu, veri sorumlusu-veri işleyen arasında), gizlilik taahhütnameleri, kurum içi periyodik ve/veya rastgele denetimler, risk analizleri, iş sözleşmesi, disiplin yönetmeliği (kanuna uygun hükümler ilave edilmesi), kurumsal iletişim (kriz yönetimi, kurul ve ilgili kişiyi bilgilendirme süreçleri, itibar yönetimi vb.), eğitim ve farkındalık faaliyetleri (bilgi güvenliği ve kanun), veri sorumluları sicil bilgi sistemine (VERBİS) bildirim" şeklinde örnek teşkil etmesi amacıyla ifade edildiği,
- Bu kapsamda, ihbara konu edilen e-Devlet şifresi istenmesi beyanına ilişkin gerek resen inceleme kapsamındaki ihbarlar gerekse veri sorumlusuna ilişkin kamuya açık kaynaklarda yer alan şikayetler

ele alındığında veri sorumlusunun kişisel veri işleme faaliyetlerinin kontrolünü sağlayamadığına, dolayısıyla gerekli teknik ve idari tedbirleri almadığına ilişkin güçlü bir kanaat oluştuğu, bilhassa senetli alışverişlerde müşterilerin e-Devlet şifrelerinin temin edilmesi suretiyle ilgili kişilerin e-Devlet kapısında yer alan kendileriyle ilgili her türlü bilgiye veri sorumlusunca erişilebilme tehlikesi ile karşı karşıya kalacakları; ayrıca veri sorumlusunun ihbara konu olayda veri güvenliğinin sağlandığına yönelik yeterli bilgi ve belgeyi de sunamadığı,

- Öte yandan veri sorumlusunun e-Devlet şifrelerinin talep edilmesine ilişkin savunmasında, bir taraftan ilgili kişiler ile akdettiği tüketici kredisi sözleşmesi sebebiyle işe başlama kaydının sigorta hizmet dökümü üzerinden teyit edilmesi amacıyla müşteriyi en yakın şubeye davet ettiğini belirtirken diğer taraftan e-Devlet şifresi ile taksitli satış sözleşmesi arasında bir illiyet bağının olmadığını, e-Devlet şifresi ile satış sözleşmesi arasında birbiri ile ilişkili bir işlemin söz konusu olmadığını, e-Devlet şifresi ile yapılacak bir işlemin de bulunmadığını ifade etmiş olduğu,
- Resen inceleme kapsamındaki iki dosyaya ilişkin veri sorumlusunca -aynı konu kapsamında- Kuruma sunulan bilgi ve belgelerin bütünlük ve tutarlılık içinde olmadığı, kişisel verilerin işlenmesi suretiyle kurulan sözleşmelere ilişkin hususların Kanun kapsamında ifade edilemediği,
- Veri sorumlusu tarafından yürütülen veri işleme faaliyetlerinde ilgili kişilerden e-Devlet şifresi talep edilmesine ilişkin kamuoyuna yansıyan çok sayıda şikayet olduğu, resen inceleme dosyalarında veri sorumlusu tarafından e-Devlet şifresi hakkında sunulan beyanların da birbiri ile tutarlı bir çerçevede olmadığı, veri sorumlusunun ülkemizde çok sayıda mağazası olan - tüketici finansman kredisiyle alışveriş imkânı sunan/taksitle satış yapan- bir şirket olduğu, Kuruma sunulan ihbarlar dışında taksitli satışlarda ilgili kişilerden e-Devlet şifresi istendiğine ilişkin şifahi bilgiler de edinildiği, e-Devlet şifresinin ele geçirilmesi durumunun veri güvenliğine yönelik ciddi riskler ortaya çıkarabileceği hususlarının tümünün idari teknik tedbirleri alma noktasında eksikliği olduğu kanaatine varılan veri sorumlusu hakkında uygulanacak idari yaptırımında artırım sebepleri olarak ele alınabileceği,
- İnternette yer alan açık kaynaklarda, veri sorumlusundan yapılan taksitli alışverişlerde ilgili kişilerin e-Devlet şifrelerinin alındığına dair pek çok şikayet olduğunun görülmesi, konuya ilişkin Kuruma da intikal eden farklı şikayetler olması, e-Devlet şifrelerinin talep edildiği her olayda tüm müşterilerin e-Devlet şifrelerini kendi telefonlarından açıp göstermesinin söz konusu olmayabileceği dikkate alındığında Şirket bilgisayarları aracılığıyla görüntüleme yapılmış olmasının mümkün olduğu

değerlendirmelerinden hareketle;

- İlgili kişilerin e-Devlet şifrelerine erişim sağlandığı yönünde güçlü bir kanaat oluştuğu, ilgili kişilerin e-Devlet şifreleri talep edilerek hassas nitelikli olanlar da dahil pek çok kişisel veriye erişim sağlanabileceği sonucuna varıldığından veri sorumlusundan yapılan taksitli alışverişlerde e-Devlet şifrelerinin talep edilmesinin Kanun'un 5'inci maddesinde yer alan herhangi bir veri işleme şartına dayanmaması nedeniyle Kanun'un 12'nci maddesinin (1) numaralı fıkrasında yer alan yükümlülüklerini yerine getirmediği değerlendirilen veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 400.000 TL idari para cezası uygulanmasına,
- Hukuka aykırı işlendiği değerlendirilen kişisel verilerin Kanun'un 7'nci maddesi ile Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında Yönetmelik uyarınca imha edilerek sonucundan Kurula bilgi verilmesine

karar verilmiştir.

2023/437 sayılı KVKK Kararı

Bir avukatlık ortaklığı tarafından borçlu ilgili kişiye kısa mesaj gönderilmesi suretiyle kişisel verilerinin işlenmesi hakkında Kişisel Verileri Koruma Kurulu'nun 22/03/2023 Tarihli ve 2023/437 Sayılı Kararı

Karar Tarihi : 22/03/2023

Karar No : 2023/437

Konu Özeti: Bir avukatlık ortaklığı tarafından borçlu ilgili kişiye kısa mesaj gönderilmesi suretiyle kişisel verilerinin işlenmesi

Bir Avukatlık Ortaklığı tarafından vekili olduğu Şirket ve ilgili kişi arasındaki abonelik ilişkisi kapsamında, borcun takibi ve hatırlatılması amacıyla ilgili kişiye beş kez kısa mesaj gönderilmesi suretiyle gerçekleştirilen kişisel veri işleme faaliyeti ile ilgili olarak Kuruma intikal eden şikâyet dilekçesinde özetle;

- Veri sorumlusu olarak Avukatlık Ortaklığı tarafından Şirketten elde edilen kişisel veriler hakkında ilgili kişiyle iletişime geçildiği ilk anda aydınlatma yükümlülüğünün yerine getirilmemesi ve ayrıca çağrı merkezi vasıtasıyla yapılan görüşme bağlamında ses kaydı hakkında ses kaydı gerçekleşmeden önce aydınlatma yükümlülüğünün yerine getirilmemesi nedeniyle 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 18'inci maddesinin birinci fıkrasının (a) bendi uyarınca veri sorumlusu hakkında yaptırım uygulanması,
- Toplamda beş kez aynı konu ve içerikle ilgili kişiye kısa mesaj gönderilmesi nedeniyle Kanunun 18'inci maddesinin birinci fıkrasının (b) bendi uyarınca veri sorumlusu hakkında yaptırım uygulanması,
- Veri sorumlusunun "hukuka aykırı olarak elde edilen veriler üzerinden vatandaşların kimlik ve iletişim bilgileri gibi kişisel verilerin sorgulanmasına imkân tanıyan yazılım/program/uygulama" kullanıp kullanmadığı hususunda denetim yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup verilen cevapta özetle;

- Kurulun şikâyeti değerlendirmeye alarak taraflarından savunma, bilgi ve belge ibrazı talep etmesinin usul ve yasaya aykırı olduğu, ilgili kişi tarafından Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in 5'inci maddesinde öngörülen veri sorumlusuna başvuru usulüne uygun bir başvuru yapılmadığı ve Avukatlık Ortaklığının, veri işleyen olması nedeniyle ilgili kişinin Avukatlık Ortaklığına başvuru hakkı bulunmadığı,
- Şirket ile Avukatlık Ortaklığı arasındaki hukuki ilişkinin mahiyetine ilişkin olarak; Avukatlık Ortaklığının, Şirket ile arasında bulunan hizmet sözleşmesi ve vekalet ilişkisi kapsamında, alacakların tahsili için yasal takip hizmeti verdiği, Avukatlık Ortaklığının, Şirket tarafından abonelerin borçlarının tahsilat süreçlerinin yürütülmesi konusunda sınırlı olarak yetkilendirildiği, Şirket tarafından yönetilmekte olan sisteme sınırlı erişim hakkına sahip olduğu, Avukatlık Ortaklığının söz konusu sistem üzerinden sınırlı şekilde görüntülenen/erişilen kişisel veriler ve bu veriler kullanılarak Şirket borçlularıyla gerçekleştirilen telefon ve kısa mesaj ile iletişim kurma faaliyetlerine ilişkin olarak Kanun'un 3'üncü maddesinin birinci fıkrasının (ğ) bendi uyarınca "veri işleyen" konumunda olduğu, Şirket ile Avukatlık Ortaklığı arasında münakid Sözleşmenin ilgili maddesi uyarınca Avukatlık Ortaklığının veri işleyen olduğu, hal böyleyken gerek taraflar arasında akdedilen Sözleşme hükümleri gerek vekalet ilişkisi gerek ise Kanun hükümleri uyarınca işlemekte oldukları kişisel verilere ilişkin olarak veri işleyen sıfatı ile sorumlu olduklarının son derece açık olduğu,
- Kişisel verilerin veri sorumlusu tarafından işlenmesinin hukuki dayanağına ilişkin olarak; müvekkilli Şirketin gecikmiş alacaklarının tahsili amacı ile icra işlemlerini yürütmek üzere Avukatlık Ortaklığı ile kurulan vekalet ilişkisi ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yayımlanan Borç ve Alacak Bilgilerinin Sorgulanmasına İlişkin Usul ve Esasların yerine getirilmesi kapsamında icra takibi öncesi ve sonrasında borçlularla iletişim kurularak borç bilgisi, haciz bilgisi, faiz indirimi kampanyası ve ödeme kanalı gibi konularda bilgilendirme yapıldığı ve mümkün oldukça borçların uzlaşma ile tahsilatının sağlandığı,
- Diğer taraftan, borcun yasal yollara başvurulmadan ve borçlunun durumu ağırlaştırılmaksızın, mevzuata uygun ve Şirket ile Avukatlık Ortaklığı arasındaki vekalet ilişkisi ve sözleşmeler kapsamında tahsil edilebilmesi için 2004 sayılı İcra İflas Kanunu'nun temel ilkelerinden birisi olan "Alacağın tahsili için yapılacak işlemlerde borçlunun, borcunu arttıracak giderlerden kaçınılması" prensibi doğrultusunda hareket edilmesi gerektiği,

- Alacağın kısa sürede tahsili ile abonelerin/borçluların takip hukukundan kaynaklanan vekalet ücreti, faiz, harç ve masraf gibi borcun ferilerine ve haciz işlemlerine maruz kalmadan indirimli şekilde ödeme yapabilmesine olanak sağlanması ile dosya borcunun artmasının önüne geçilmesi, borçluların lehine olarak taksitlendirme imkanı ve banka, kredi kartı gibi ödeme kanalları hakkında açıkça bilgi verilmesi, ödemenin yapılmaması halinde alacağın tahsili amacıyla hakkında icra takibi başlatılacağı ve/veya başlatıldığı abonelere/borçlulara bildirilmesi, diğer bir deyişle borcun ödenmemesi durumunda maruz kalınabilecek hukuki riskler hakkında açıkça bilgi verilmesi, Şirketin talebi ve onayı doğrultusunda sulh görüşmelerinin gerçekleştirilmesi, ileride doğabilecek uyuşmazlıklarda bu bilgilendirmelerin delil olarak kullanılması adına aramaların gerçekleştirilebildiği ve kısa mesaj gönderilebildiği,
- Hukuka aykırı olarak kişisel veri elde etmek amacıyla herhangi bir yazılım/program/uygulama kullanılıp kullanılmadığına ilişkin olarak; Avukatlık Ortaklığı tarafından kişisel veri elde edilmesi amacıyla yasa dışı herhangi bir yazılım/uygulama, program yahut başka şekilde elde edilmiş veri kullanılmadığı, ilgili kişinin, “internet sitelerinin borçların ödenmesine özgülendiği” bu amaçla hukuka aykırı olarak çeşitli yazılımlarla borçlu verisi topladıkları iddialarının tamamen kötü niyetli olarak öne sürüldüğü, ilgili kişinin bu asılsız ve dayanağı olmayan iddiaları ile Avukatlık Ortaklığını zan altında bırakma çabası içinde olduğu, Avukatlık Ortaklığının web sitesinde borçluların borcunu kolayca ödemesi için ödeme kanallarının ve yöntemlerinin bulunduğu bir sekmenin mevcut olduğu ve web sitesinden borçlulara Türkiye Barolar Birliği tarafından sunulan BaroKart sistemi üzerinden taksitli borç ödeme imkanı, banka hesapları ve Şirketin ödeme kanalları, talep, itiraz, şikâyet yolları hakkında bilgi verildiği, web sitesinde yapılan bilgilendirmelerin Kanun ve buna ilişkin mevzuat ile bir ilgisi bulunmadığı, web sitesi üzerinden bir veri toplanmasının da söz konusu olmadığı, Avukatlık Ortaklığının mevcut olayda kişisel verilerin korunması hukuku çerçevesinde yasal mevzuatı ihlal edici nitelikte hiçbir icrai yahut ihmali davranışta bulunmadığı,
- Bu kapsamda, Avukatlık Ortaklığı olarak vekili oldukları Şirket adına, Şirketin haklarını ve menfaatlerini korumak amacıyla hareket ettikleri ve bu anlamda Avukatlık Kanunu’ndan kaynaklanan yükümlülükleri ve yürütmekte oldukları icra işlemleri bakımından İcra ve İflas Kanunu ile diğer mevzuattan kaynaklanan hukuki yükümlülüklerini yerine getirmek amacıyla ilgili kişiye ait kişisel verileri, Kanunun 5’inci maddesinin ikinci fıkrasında yer alan “bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması” ve “ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması” hukuki sebepleri çerçevesinde işledikleri,

- Avukatlık Ortaklığının kişinin borç bilgilerini müvekkili Şirketten temin ettiği; takip öncesi bilgilendirmeden maksadın yasal takip başlatmadan evvel makul bir süre bekleyerek karşı yanı borcuna eklenecek masraflardan korumayı amaçladığı, ilgili kişinin Avukatlık Ortaklığı tarafından kendisine beş kez kısa mesaj atıldığını ve Avukatlık Ortaklığının kendisini taciz ettiğini beyan ettiği, ancak kendisine ayda yalnızca 1 kereye mahsus olmak üzere, hafta içi, mesai saatleri içerisinde bilgilendirme dışında hiçbir ibare olmayan kısa mesaj gönderildiği, Türk Borçlar Kanunu'na, BTK Usul ve Esaslarına ve Kanunun 5'inci maddesinin ikinci fıkrasının (e) bendi kapsamında açık rıza aranmaksızın bilgilendirme haklarına dayalı olarak Avukatlık Ortaklığınca bilgilendirme saikiyle hareket edildiği

ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde, Kişisel Verileri Koruma Kurulunun 22/03/2023 tarihli ve 2023/437 sayılı Kararı ile;

- Kanun'un 3 üncü maddesinin birinci fıkrasının (1) bendi uyarınca veri sorumlusunun; "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi"yi ifade ettiği, bu çerçevede, kişisel verilerin işlenmesine ilişkin kararları alma, işleme faaliyetinin amacı, bu faaliyetin ne zaman başlayacağı, kimler tarafından gerçekleştirileceği ve benzeri hususlarda karar verme yetkisinin veri sorumlusuna ait olduğu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen veri sorumlusunun, veri işleme faaliyetinin temel araçlarını ve amaçlarını, veri işlemenin "neden" ve "nasıl" olacağını belirlediği, diğer bir deyişle, teknik ve organizasyona ait araçların belirlenmesi, veriye kimin erişeceği, hangi verilerin işleneceği, bu verilerin ne kadar süre tutulacağı, ne şekilde saklanacağı gibi veri işlemeye ilişkin temel unsurların veri sorumlusu tarafından belirlendiği, her ne kadar Avukatlık Ortaklığı ile Şirket arasındaki Sözleşmede Avukatlık Ortaklığının "veri işleyen" statüsünü haiz olduğu öngörülmüş ve ilgili kişinin şikâyetine konu kişisel veriler Şirket tarafından Avukatlık Ortaklığına aktarılmış olsa da kişisel verilerin korunması mevzuatı ve uygulanması bağlamında Avukatlık Ortaklığının sahip olduğu sıfatın fiili durumun şartları gözetilerek belirlenmesi gerektiği,

- Avukatlık Ortaklığının yetkilerinin, Şirket ile arasındaki vekalet ilişkisi ve Sözleşme kapsamında Şirketin alacaklarının tahsil ve takip işlemlerinin yürütülmesi ile sınırlı olsa dahi Şirket tarafından kendisine aktarılan kişisel veriler üzerinde gerçekleştirilecek işleme faaliyetlerini yönettiğinin görüldüğü, bu itibarla, avukatlık faaliyetleri çerçevesinde Avukatlık Ortaklığının kişisel veri işleme faaliyetleri bakımından serbestçe karar verme yetkisine sahip olduğu, ilgili kişinin şikâyetine konu

kişisel verilerinin işleme amaç ve vasıtalarını belirlediği ve veri sorumlusu olarak kabul edilmesi gerektiği,

- Veri sorumlusu tarafından avukatlık faaliyetleri kapsamında Şirketin alacaklarının borçlu ilgili kişiden tahsil edilebilmesi ve ilgili kişiye sağlanacak kolaylıklar ile borcun ödenmemesi durumunda ilgili kişinin maruz kalabileceği hukuki risklerin bildirilmesi amacıyla Kanunun 5'inci maddesinin ikinci fıkrasının (e) bendinde öngörülen "bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" işleme şartına dayanılarak kısa mesaj göndermek suretiyle ilgili kişinin kişisel verilerinin işlenmesinin mümkün olduğu;

- Bununla birlikte, şikâyete konu somut olayda veri sorumlusu tarafından benzer içerikli 5 kısa mesajın, yaklaşık 1 aylık periyotlarla ilgili kişiye gönderildiği, veri sorumlusunun Kurumu muhatap cevabi yazısında da belirtildiği üzere söz konusu mesajların, ayda yalnızca 1 kereye mahsus olmak üzere, hafta içi, mesai saatleri içerisinde ilgili kişiye gönderildiği, bu kapsamda, söz konusu işleme faaliyetinin Kanunun 4'üncü maddesinin ikinci fıkrasının (a) bendinde yer alan "hukuka ve dürüstlük kurallarına uygun olma" ve (ç) bendinde yer alan "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerine de aykırılık teşkil etmediği

değerlendirmelerinden hareketle,

- Veri sorumlusu tarafından ilgili kişinin telefon numarasının işlenmesi suretiyle gerçekleşen kişisel veri işleme faaliyetinin Kanun'un 5'inci maddesinin ikinci fıkrasının (e) bendinde yer alan bir hakkın tesisi, korunması veya kullanılması için veri işlemenin zorunlu olması hükmü kapsamında hukuka uygun olduğu değerlendirildiğinden söz konusu şikâyet kapsamında yapılacak bir işlem bulunmadığına,

- İlgili kişinin, veri sorumlusunun Şirketten elde ettiği kişisel veriler hakkında ilgili kişiyle iletişime geçildiği ilk anda aydınlatma yükümlülüğünün yerine getirilmemesi ve ilgili kişinin kendisine gönderilen kısa mesajlar hakkında bilgi almak üzere veri sorumlusunun çağrı merkezini araması sırasında alınan ses kaydı hakkında ses kaydı gerçekleşmeden önce aydınlatma yükümlülüğünün yerine getirilmemesi nedeniyle Kanun'un 18'inci maddesinin birinci fıkrasının (a) bendi uyarınca cezalandırılması talebine ilişkin olarak ilgili kişinin veri sorumlusuna başvurusunda söz konusu iddialara ilişkin bir açıklama veya talebin bulunmadığı anlaşıldığından Kanun kapsamında yapılacak bir işlem bulunmadığına,

- İlgili kişinin, veri sorumlusu nezdinde hukuka aykırı olarak elde edilen veriler üzerinden vatandaşların kimlik ve iletişim bilgileri gibi kişisel verilerin sorgulanmasına imkân tanıyan

yazılım/program/uygulama kullanıp kullanmadığı hususunda denetim yapılması talebine ilişkin olarak veri sorumlusunun cevabi yazısında ilgili kişinin bu iddiasının reddedilmiş olduğu ve ilgili kişi tarafından da iddiasını tevsik edici nitelikte herhangi bir bilgi, belge veya kaydın Kuruma iletilmemiş olduğu dikkate alındığında bahse konu talep hakkında Kanun kapsamında yapılacak bir işlem bulunmadığına

karar verilmiştir.

2023/224 sayılı KVKK Kararı

Bir belediyenin meclis toplantısı videosunun sosyal medya hesabından paylaşılması suretiyle ilgili kişinin kişisel verilerinin hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 16/02/2023 tarih ve 2023/224 sayılı Karar Özeti

Karar Tarihi : 16/02/2023

Karar No : 2023/224

Konu Özeti: Bir belediyenin sosyal medya hesabından meclis toplantısı videosunun paylaşılması suretiyle kişisel verilerinin paylaşılması

İlgili kişinin Kuruma intikal eden şikâyetinde özetle; bir ilçe belediyesinin sosyal medya hesabından paylaşılan olağan meclis toplantısı videosunda, kişisel verilerinin hukuka aykırı olarak işlendiği, bahse konu toplantıda belediye başkanı tarafından ilgili kişinin özel hayatına, kişisel verilerine ve bazı dava dosyaları ile ilgili adli işlemlere ilişkin bilgileri içeren bir konuşma gerçekleştirildiği ve bu konuşmanın belediyenin sosyal medya hesabından kamuoyu ile paylaşıldığı, bu çerçevede kişisel verilerinin ihlal edilmesine ilişkin olarak Belediyeye başvuruda bulunulduğu, ancak Belediye tarafından Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında herhangi bir hak ihlaline rastlanmadığı şeklinde cevap verildiği ifade edilerek gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- İlgili kişinin önceki yıllarda Belediye meclis üyesi olarak görev yaptığı, meclis üyeliği görevi çerçevesinde ilgili kişinin kişisel verilerinin yerel seçimleri müteakiben İlçe Seçim Kurulu tarafından Belediyeye iletilen asil ve yedek meclis üyelerinin isim listesi çerçevesinde işlenmeye başlandığı,

İlçe Seçim Kurulundan gelen verilerin yanı sıra mevzuat gereği belediye meclis üyesinin göreve başlayabilmesi için başta kimlik veri kategorisinde yer alan isim, soyisim ve T.C. kimlik numarası (kimlik fotokopisi) ile iletişim, özlük (mal bildirim formu), mesleki deneyim (meslek bilgileri), finans (banka hesap bilgileri), görsel ve işitsel kayıt (fotoğraf, imza ve paraf örneği, mazbata fotokopisi, belediye başkan ve meclis üyeleri bilgi formu) kategorilerinde yer alan verilerin ilgili kişinin kendisinden temin edildiği,

İlgili kişi hakkında Belediye Başkanı tarafından meclis toplantısında zikredilen dava dosyalarının Belediye Başkanının görevleri ile doğrudan ilgili olduğu ve hukuki çerçevede işlendiği, ... Cumhuriyet Başsavcılığı Avukat, Noter ve Memur Suçları Soruşturma Bürosu tarafından Belediyeye gönderilen soruşturma dosyasından haberdar olduğu ve Başsavcılığa gerekli bilgilerin ve soruşturma dosyası çerçevesinde şikayetçi sıfatıyla katılma talebinin iletildiği,

- Cumhuriyet Başsavcılığı Hazırlık Bürosundan taraflarına iletilen yazı ile Belediyeden çeşitli bilgi ve belge taleplerinde bulunduğu, Belediye Zabıta Müdürlüğünce hazırlanan yazı ile Başsavcılığa talepleri doğrultusunda bilgi ve belgelerin gönderildiği, soruşturmanın akabinde asliye ceza mahkemesinin dosyası ile dava açıldığı ve görülmekte olan davaya Belediye adına katılma talebinde bulunduğu,

- Belediye Başkanının meclis konuşmalarında değindiği; belediye meclis üyesinin belediye ile doğrudan veya dolaylı olarak iş ilişkisine giremeyeceğine yönelik beyanlarının dayanağının ve hukuki gerekçeleri ile dava dosyaları hakkında bilgilerin yukarıda belirtilen resmi süreçler dahilinde gerçekleştiği, bu çerçevede ilgili kişinin hukuki işlem kategorisinde yer alan verilerinin hukuka uygun olarak işlendiği,

- Toplantı sırasında Belediye Başkanı tarafından zikredilen cümlelerde mümkün olduğunca belli bir kişiyi işaret etmemek için özen gösterildiği, Başkan tarafından isim belirtilmeden zikredilen cümlelerin, ilgili kişinin kişilik hakları ile özel hayatının gizliliğini korumaya yönelik olduğu,

- Şikâyete konu meclis toplantısının çevrim içi ortamlardaki paylaşımının, Kurul tarafından yürütülen inceleme sona erene kadar, iyi niyetin bir göstergesi olarak geçici olarak kaldırıldığı,

- Kuruma sunulan aydınlatma metninde de görüleceği üzere Belediye meclis toplantılarında ses ve görüntü kaydının alındığı, bu verilerin ulusal ve yerel yayın organlarında yayımlandığına dair bilgi verildiği ve bu konuda bilgilendirmenin belediye meclis salonu girişinde herkese duyurulduğu,

- 5393 sayılı Belediye Kanunu'nun 20'nci maddesinin altıncı fıkrasının ikinci cümlesinde "Toplantılar, meclisin kararıyla sesli ve görüntülü cihazlarla da kaydedilebilir." hükmünün yer aldığı, bu hüküm doğrultusunda Belediyesi Meclisinin Kararı ile meclis toplantılarının kayıt altına alınmasına karar verildiği,

- 09/10/2005 tarihli ve 25961 sayılı Resmi Gazete'de yayımlanan Belediye Meclisi Çalışma Yönetmeliği'nin 11'inci maddesinin dokuzuncu fıkrasında "Meclis toplantıları halka açıktır. Meclis başkanı veya üyelerden herhangi birinin gerekçeli teklifi üzerine kapalı oturum yapılmasına karar verilebilir. (...)" hükmüne yer verildiği, hükümden de anlaşılacağı üzere meclis toplantılarının

şeffaflık ve katılımcılık ilkeleri gereği halka açık olduğu ve bu doğrultuda, meclis kararı ile toplantıda alınan kayıtların ulusal ve yerel kanallarda yayımlanmasının hukuka uygun olduğu, zira şikâyete konu meclis toplantısının kapalı oturum olarak yapılmasını gerektirecek herhangi bir meclis kararının da bulunmadığı,

- Belediyenin meclis toplantısını kayıt altına alması ve çeşitli araçlarla halk ile paylaşmasının bir hukuki yükümlülük gereği olduğu ve katılımcıların bu konuda açık rızasına ihtiyaç duyulmadığının düşünüldüğü,

- Belediye Başkanlığının kamu tüzel kişiliğini haiz bir kuruluş olduğu ve tüm iş ve işlemlerinde Anayasa ve kanunlara uygunluk ile kamu yararını en önde tuttuğu, Belediyenin sadece meclis görüşmelerini değil, yine şeffaflık ilkesi ve kamu yararının bir gereği olarak ihaleleri de kayıt altına alarak halkla paylaştığı,

ifade edilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulunun 16/02/2023 tarih ve 2023/224 sayılı Kararı ile;

- 6698 sayılı Kanun'da, kişisel verinin "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", ilgili kişinin "kişisel verisi işlenen gerçek kişi", kişisel verilerin işlenmesinin ise "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem" olarak tanımlandığı,

- Kişisel verilerin işlenmesinin Kanun kapsamında belirli işleme şartlarına bağlandığı, buna göre Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin;

(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

- c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- e) Bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması.
- f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

hükmünü haiz olduğu,

- Bu çerçevede, Belediye Meclis Toplantısında ilgili kişinin adına yer verilmesi ve öncesinde sıklıkla “eski meclis üyesi arkadaşımız” ifadesi ile anılması dolayısıyla ilgili kişiyi belirlenebilir kılan nitelikte bir bilgi paylaşımının söz konusu olduğu, bu anlamda meclis toplantısının kaydedilmesi işlemi ile birlikte Belediye Başkanlığı tarafından kişisel veri işleme faaliyetinde bulunulduğunun anlaşıldığı, Bahse konu Olağan Meclis Toplantısı videosu kaydı incelendiğinde; Belediye Başkanı tarafından ilgili kişinin dahil olduğu ve Belediyenin de müdahil olduğu dava sürecine ve dava dosyasında yer alan evraklara dair bilgiler verildiğinin tespit edildiği, aynı zamanda Belediye Başkanının yaptığı konuşma boyunca ilgili kişinin adı ve soyadının anılmadığı, sürekli olarak “eski meclis üyesi arkadaşımız” olarak bahse konu olduğu ve video kaydının bir yerinde “isim vermeyelim” uyarısında bulunulduğunun tespit edildiği, ek olarak yalnızca video kaydının bir yerinde Belediye Başkanının ilgili kişinin soyadına yer vermeksizin adını andığının tespit edildiği,
- İlgili kişinin Belediye Başkanı tarafından ifade edilen dava sürecine ilişkin ifadelerinin gerçek dışı olduğu yönünde bir iddiasının bulunmadığı esas alındığında ve veri sorumlusu tarafından Kuruma iletilen evraklardan da dava sürecine ilişkin ifadelerin gerçeği yansıttığı kanaatine varıldığı,
- İlgili kişinin önceden meclis üyeliği yaptığı ve ilgili kişinin bilgilerinin meclis toplantısında gündem olmasının meclis üyelerinin belediye ile doğrudan veya dolaylı şekilde iş ilişkisine giremeyeceği kuralının ihlal edildiği iddiası ile mahkeme süreci kapsamında gündeme geldiği dikkate alındığında kamuoyunun konuya ilişkin bilgilendirilmesinde ilgi ve yararının mevcut olduğunun anlaşıldığı,
- Diğer taraftan 5393 sayılı Belediye Kanunu’nun 20’nci maddesinin altıncı fıkrasında “Toplantılar, meclisin kararıyla sesli ve görüntülü cihazlarla da kaydedilebilir.” hükmü doğrultusunda Belediyesi Meclisinin Kararı ile meclis toplantılarının kayıt altına alınmasına karar verildiği,

- Belediye Meclisi Çalışma Yönetmeliği'nin 11 inci maddesinin dokuzuncu fıkrasında "Meclis toplantıları halka açıktır. Meclis başkanı veya üyelerden herhangi birinin gerekçeli teklifi üzerine kapalı oturum yapılmasına karar verilebilir. (...)" hükmüne yer verildiği, bununla beraber şikâyete konu meclis toplantısının kapalı oturum olarak yapılması yönünde herhangi bir meclis kararının da mevcut olmadığı anlaşıldığı,

- Bu çerçevede belediye başkanı tarafından ilgili kişinin dava sürecine ilişkin bilgilerinin paylaşılması ve ardından adının anılması şekilde gerçekleşen somut olay yukarıda yer verilen hukuki gerekçeler kapsamında değerlendirildiğinde; Belediye Meclisi Toplantısında ilgili kişinin kişisel verilerinin yer aldığı ilgili video kaydının sosyal medya platformu üzerinde yayımlanması yönündeki veri işleme faaliyetinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (ç) bendinde yer alan "veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için veri işlemenin zorunlu olması" hükmü kapsamında olduğu

değerlendirmelerinden hareketle;

- İlgili kişinin Belediyesi Meclis Toplantısında kişisel verilerinin Kanun'a aykırı olarak paylaşıldığı ve ilgili video kaydının sosyal medya platformu üzerinde yayımlandığı iddiasıyla Kurula intikal eden şikâyetinin incelenmesi neticesinde; ilgili kişinin eski meclis üyesi olduğu ve konuya ilişkin olarak kamuoyunun bilgilendirilmesinde kamu ilgi ve yararının mevcut olduğu, öte yandan 5393 sayılı Belediye Kanunu'nun 20'nci maddesinin altıncı fıkrasında "Toplantılar, meclisin kararıyla sesli ve görüntülü cihazlarla da kaydedilebilir." hükmüne, Belediye Meclisi Çalışma Yönetmeliği'nin 11'inci maddesinin dokuzuncu fıkrasında ise "Meclis toplantıları halka açıktır. Meclis başkanı veya üyelerden herhangi birinin gerekçeli teklifi üzerine kapalı oturum yapılmasına karar verilebilir. (...)" hükmüne yer verildiği dikkate alındığında söz konusu veri işleme faaliyetinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (ç) bendinde yer alan "veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için veri işlemenin zorunlu olması" hükmü kapsamında olduğu değerlendirildiğinden Belediye Başkanlığı hakkında Kanun kapsamında yapılacak bir işlem bulunmadığına

karar verilmiştir.

2023/134 sayılı KVKK Kararı

TikTok Pte. Ltd. hakkında Kişisel Verileri Koruma Kurulunun 2023/134 sayılı Karar Özeti

Karar No : 2023/134

Konu Özeti : TikTok Pte. Ltd nezdinde gerçekleşen veri ihlalinin değerlendirilmesi

İnternet ve sosyal medya platformlarında TikTok uygulaması ile ilgili olarak açık rızanın 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında usulüne uygun alınmadığı, kişisel verilerin elde edilmesi ve saklanması hususunda hukuka aykırılıkların bulunduğu ve yazılıma ait birçok güvenlik açığı olduğuna yönelik yer alan muhtelif haber ve şikayetlerden hareketle Kişisel Verileri Koruma Kurulu tarafından 6698 sayılı Kanun'un 15'inci maddesinin (1) numaralı fıkrası kapsamında resen inceleme başlatılmasına karar verilmiştir. Konuya ilişkin veri sorumlusundan alınan savunma yazıları ve bununla bağlantılı olarak Gizlilik Politikası ve Hizmet Koşullarının incelenmesi neticesinde, Kişisel Verileri Koruma Kurulu'nun 2023/134 sayılı Kararı ile;

- TikTok'un 2021 yılı Ocak ayında Gizlilik Politikasında güncelleme gerçekleştiği, güncelleme neticesinde metinde 13 ve 15 yaş aralığındaki kullanıcı hesapları için varsayılan gizlilik ayarının "özel" olarak değiştirildiği bu sayede, yalnızca kullanıcının onayladığı takipçilerin paylaştığı videoların görüntülenebileceği, videoları indirebilecek ve yorum yapabilecek kişilerin sınırlandırıldığı belirtilmekle birlikte; belirtilen güncelleme öncesinde varsayılan olarak profillerin herkese açık olarak görüntülenerek etkileşimde sınırlandırılma bulunmamasının, hassas yaş grubunda olan kullanıcıların verilerine erişilmesi kapsamında risk teşkil ettiği, ayrıca kullanıcılara ilişkin risklerin belirlenerek risklerin azaltılmasına dair yeterli tedbir alınmadığını gösterdiği,
- 2021 yılı Ocak ayında Gizlilik Politikasının güncellenmesi öncesinde uygulamayı kullanan 13 yaş altı çocukların kişisel bilgilerinin görüntülendiği ve uygun ebeveyn izni olmadan çocuklar hakkında veri toplandığı, dolayısıyla uygulamayı kullanmış olan çocuklar üzerinde olumsuz sonuç doğma riskinin bulunduğu,
- Veri sorumlusunun internet sitesinde yer alan Gizlilik Sözleşmesinde Kişisel Verilerin Korunması Kanunu'nun 5'nci maddesinde yer alan işleme şartlarının tümünün belirtildiği, ancak hangi kişisel verilerin hangi amaçla ve hangi işleme şartına dayanılarak işlendiği hakkında net bilgi verilmediği,

bu hususta veri sorumlusunca Kanun'un 4'üncü maddesinde yer alan "belirli, açık ve meşru amaçlar için işleme" ve "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerine aykırı hareket edildiği,

- TikTok hesabı oluşturulurken kullanıcıların hesap oluşturmaya devam etmeleri halinde Hizmet Koşulları (Kullanım Şartları) ile Gizlilik Politikasını kabul etmiş sayılacaklarının belirtildiği , ancak Hizmet Koşulları kısmında onay alınırken ilgili metnin henüz Türkçe'ye tercüme edilmediği, bu sebeple kullanıcılara içeriğin kolay anlaşılır bir biçimde sunulmadığı ve kullanıcıların kullanım şartlarını tam olarak anlayamadan kabul etmesinin ihtimal dahilinde olduğu,

- Platformda hesap oluştururken ya da hesap oluşturulup aktif olarak kullanılırken açık rıza alınmasına ilişkin herhangi bir durum ile karşılaşılmadığı, TikTok'un Gizlilik Politikasının, esasen aydınlatma yükümlülüğünü yerine getirmek için hazırlanmış bir metin olduğu, ancak açık rıza metni yerine de kullanıldığı, dolayısıyla, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in 5'inci maddesinin (f) bendine göre açık rıza şartına dayalı olarak gerçekleştirilen kişisel veri işleme faaliyetleri bakımından açık rızanın aydınlatma yükümlülüğünden ayrı olarak yerine getirilmesi şartının sağlanmadığı,

- Veri sorumlusu tarafından, profileme amacıyla çerezler kullanılarak gerçekleştirilen kişisel veri işleme faaliyetine ilişkin olarak ilgili kişilerden açık rıza alınmadığı, bu kapsamda yürütülen kişisel veri işleme faaliyetinin de hukuka uygun olmadığı

anlaşıldığından Kanun'un 12'nci maddesinin (1) numaralı fıkrasında yer alan kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almadığı tespit edilen veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 1.750.000 TL idari para cezası uygulanmasına,

Ayrıca veri sorumlusunun;

- İlgili kişilerin doğru bilgilendirilmesi adına Hizmet Koşullarının bir ay içerisinde Türkçeye çevrilmesi,

- İlgili kişilerin doğru bilgilendirilmesi için söz konusu Gizlilik Politikası metnlerinin üç ay içerisinde Kanuna uygun hale getirilmesi,

- Gizlilik Politikasının, aydınlatma metni yerine kullanıldığı ve geçerli bir aydınlatmanın unsurlarını taşımadığı anlaşıldığından, Kanun'un 10'uncu maddesi ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerine uygun bir aydınlatma yapılması

hususunda talimatlandırılmasına

karar verilmiştir.

2023/86 sayılı KVKK Kararı

Veri sorumlusunun çalışanlarına tahsis ettiği kurumsal e-posta adresindeki içerikleri izleme, erişme ve depolama suretiyle kişisel verileri işlemesi hakkında Kişisel Verileri Koruma Kurulunun 19/01/2023 tarihli ve 2023/86 sayılı Karar Özeti

Karar Tarihi : 19/01/2023

Karar No : 2023/86

Konu Özeti: Veri sorumlusunun çalışanlarına tahsis ettiği kurumsal e-posta adresindeki içerikleri izleme, erişme ve depolama suretiyle kişisel verileri işlemesi

Kuruma intikal eden şikâyetle özetle;

- İlgili kişinin veri sorumlusu şirkette iş akdinin feshedildiği, fesih sebebinin şirket içi verilerin şirketin tahsis etmiş olduğu e-posta adresi üzerinden kişisel e-posta adresine gönderilmesi ve şirketin bir başka çalışanı ile gerçekleştirilen telefon görüşmesinin gizlice kayıt altına alınarak yine kişisel e-posta adresi ile avukatının e-posta adresine gönderilmesi olduğu,
- Feshin geçersizliği ve istifaya zorlamak için uygulanan mobbing nedeniyle iş akdinin feshedildiği gerekçesiyle ilgili kişi tarafından işe iade davası açıldığı ve aynı zamanda 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 11'inci maddesi kapsamındaki hakları çerçevesinde veri sorumlusu şirkete başvuruda bulunulduğu,
- Şirket tarafından verilen cevabın yeterli olmadığı, ilgili kişi işe başlarken şirket tarafından imzalatılan formlarda bilgisayardaki tüm hareketler ve e-posta içeriği dahil olmak üzere kişisel veri işleme süreçlerine ilişkin düzenlemelerin yer almadığı, bu anlamda iş sözleşmesi ekinde yer alan formlar/taahhütnamelerin battaniye rıza niteliğinde olduğu ve belgelerde yer alan açıklamaların muğlaklıklar içerdiği, ayrıca bu durumun Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in 5'inci maddesine de aykırılık oluşturduğu,

Şirketin kendi yayınladığı iş sözleşmesi eki olan "Etik Kurallar ve Disiplin Yönetmeliği"ne de aykırı davrandığı, İş Kanunu'nun 26'ncı maddesinde ve ilgili Disiplin Yönetmeliği'ndeki 6 iş günlük ve 1 yıllık hak düşürücü sürelerin geçmesine rağmen fesih tarihinden 607 gün ve 149 gün önce elde edilen e-postaların fesih tarihinde kullanılmasının şirketin e-postaları izlediğinin, süresiz depoladığının ve

fesih konusu iddialarını oluşturan e-postalar üzerinde genel denetimde bulunduğu göstergesi olduğu, söz konusu e-postaların ve ses kaydının tarafına iletilmesini talep ettiği ancak veri sorumlusu tarafından iletilmediği,

- e-posta içeriklerinin izlenmesi, erişilmesi ve depolanması suretiyle kişisel verilerinin hukuka aykırı işlendiği ve söz konusu kişisel veri işleme faaliyetlerinin doğruluk, ölçülülük ilkelerine aykırılık barındırdığı, işe iade davasında şirket avukatları tarafından dava dosyasına iki adet belge sunulduğu ve üç ayrı belgenin sayfalarının değiştirilerek sanki ilgili kişiden onay alınmış, aydınlatma yapılmış veya ilgili kişi tarafından taahhüt verilmiş algısı oluşturulmaya çalışıldığı, “Bilgi Formu ve Muvafakatname” başlıklı belgenin 2. ve 3. sayfalarının başka belgelerden alındığı, dipnotu İşe Alım Süreci Aday KVKK Bilgi ve Onay Formu olan belgenin de çalışanlardan değil iş başvurusunda bulunan adaylardan alınan yazı olduğu ve bu sayfada imzasının bulunmadığı, dipnotu Çalışanlara Ait Kişisel Verilerin İşlenmesine ve Korunmasına İlişkin Bilgilendirme ve Muvafakatname olan yazının içeriğinde ise e-posta içeriklerinin izlendiğine dair bilgilendirme olmadığı,

- Bu kapsamda üç belgenin sayfaları değiştirilerek işe başvuran adaylardan alınan belgenin aydınlatma metni gibi gösterilmeye çalışıldığı, muvafakatnamenin ise açık rıza metni olarak gösterilmeye çalışıldığı

ifade edilerek 6698 sayılı Kanun kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabî yazıda özetle;

- İlgili kişinin şirket bünyesinde “Pazarlama ve İç İletişim Yöneticisi” olarak görev yaptığı ve iş akdinin haklı sebeple feshedildiği, tamamı ticari veri içeren şirket bilgilerini gizlilik önlemlerine aykırı davranarak kişisel e-posta adresine ilettiği, ayrıca bir şirket çalışanı ile gerçekleştirdiği telefon görüşmesini bu çalışanın bilgisi ve onayı olmaksızın gizlice kayıt altına aldığı ve yine kurumsal e-posta adresinden ilk olarak kişisel e-posta adresine sonra da üçüncü kişiye ait e-posta adresine ilettiği, şirketin bu eylemden denetim esnasında haberdar olduğu,

- İlgili kişinin gerek gizlilik ve kişisel verilerin korunması mevzuatına dair bilgilendirilmiş bir yönetici olması gerekse de uzun yıllardır çalışma hayatının içinde yer alması sebebiyle anılan işlemlerin hukuka ve etik kurallara aykırı olduğunu bilecek konumda olduğu, kendisinin işveren nezdinde, kişisel verilerin hukuka aykırı olarak işlenmesini ve kişisel verilerine hukuka aykırı olarak erişilmesini engellemek; kişisel verilere, üçüncü kişiler tarafından erişilmesini ve paylaşılmasını da engelleyerek güvenli bir şekilde korunmasını sağlamak; kişisel verilerin üçüncü bir tarafla

paylaşılması gereken süreçlerde gerek Kanun gerekse Kişisel Veri Koruma Politikası ile şirket tarafından belirlenen diğer ilke ve kararlar uyum hususunda azami özeni göstermek ve olağan iş akışı dışında değerlendirilebilecek şüpheli paylaşımları şirket içinde ilgili birimlere bildirmek hususunda görevlendirdiği kişi konumunda olduğu,

- İlgili kişinin bahse konu davranışının mevzuat hükümlerine, iş sözleşmesine, kişisel verilerin korunmasına ve gizlilik taahhütlerine, doğruluk borçlarına aykırılık teşkil ettiği ve iş akdinin haklı nedenle feshedildiği, ilgili kişinin iş akdinin feshi üzerine şirket aleyhine işe iade davası ikame ettiği,

- Kurumun ilgi yazısında dava dosyasına sunulan eklerin sayfalarının aldatma kastı ile değiştirildiği gibi yakışıksız bir iddianın öne sürüldüğü belirtilmekte ise de şirketlerinin bu gibi bir davranışa tevessül etmesinin mümkün olmadığı, bu iddianın ilgili kişinin ekleri fiziken karıştırmasından kaynaklandığını umdukları,

- İlgili kişinin kişisel verilerinin hukuka aykırı işlendiğine yönelik iddialarına ilişkin cevaplar ile işlemenin esasına, amacına ve hukuki sebeplerine ilişkin olarak; ilgili kişinin, ticari verileri havi kaydı şirket hakimiyet alanı dışına çıkarmak ve başka bir çalışanın ses kaydını izinsiz şekilde kayda alıp kendi şahsi e-posta hesabı ile üçüncü bir kişiye aktarmak şeklinde gerçekleşen hukuka aykırı tutumunu bastırmak ve hukuki ihtilafta lehine delil yaratmak adına, şirketlerinin bu olaya vakıf olma durumunu sorgulamakta olduğu,

- Buna karşın şirketlerinin ilgili kişinin verilerini otomatik olan ve/veya olmayan yöntemlerle işlemek suretiyle ilgili kişi aleyhine hiçbir dönem hukuka aykırı bir ihlal gerçekleştirmediği, nitekim şirketlerinin çalışanlarının mevzuata, şirket politikalarına, gizlilik yükümlülüklerine, bilgi güvenliği prosedürlerine, disiplin hükümlerine riayet ettiğini izlemek ve denetlemekle hem yetkili hem de görevli olduğu, mevcut çalışanları arasındaki ilişkileri gözetmek ve tüm çalışanlarının kişisel haklarını korumakla mesul olduğu, şirketlerinin iletişim sistemlerinin ve ekipmanlarının kullanımının, kurumsal e-posta hesabı üzerinden gerçekleştirilen yazışmaların güvenliğinin sağlanması, iş amacı dışındaki şahsi kullanımın tespiti, makul şüphe üzerine başlatılan disiplin soruşturmalarının karara bağlanması, bu sistem ve ekipmanların kullanımı yoluyla hukuka aykırı eylemlerin gerçekleştirilmesinin önüne geçilmesi/eylemlerin tespiti ve her halde iş yeri kurallarına uygunluğunun teyidi amacıyla izlenebileceği hususunda ilgili kişinin, Çalışanlara Ait Kişisel Verilerin İşlenmesine Dair Politika, Çalışan Aydınlatma Metinleri ve muhtelif iç düzenlemeler kapsamında müteaddit kereler bilgilendirildiği,

- Şirketlerinin mahrem bilgi ve sırları hakkında bilgi edinme olanağına sahip, bu bilgileri kendi veya rekabet gücü bulunan farklı bir firma adına ekonomik bir değer olarak kullanabilecek duruma gelen

çalışanlarına getirilen gizlilik yükümlülüklerinin şirket iç düzenlemelerinde ve ikili sözleşmelerde yer aldığı, bu düzenlemelere uyumun şirketlerinin ticari mevcudiyetini koruması, hizmet hacmi ve piyasadaki rekabet gücünde telafisi imkânsız zararların oluşmaması yönünden hayati önem taşıdığı, Şirketleri tarafından çalışanlarına zimmetli bilgisayar ve kurumsal e-postaların kullanımında hukuka ve işverenin haklı menfaatlerine uygun davranılması gerektiği, bu gerekliliğe paralel hükümlerin E-Posta Güvenliği Politikasında, Bilgi ve Yazılım Alışverişi Politikasında, Kabul Edilebilir Kullanım Politikasında düzenlendiği, tüm bu iç düzenlemelerinin çalışanların erişimine de açık halde tutulduğu,

- Nitekim, Kurulun da şirket sunucularından şirket e-posta hesabı üzerinden gerçekleştirilen yazışmalara erişim sağlanmasında hukuka aykırılık görülmediğine dair kararlarının mevcut olduğu ve bunlarda; "şirkete ilişkin iş ve işlemler için kullanıldığında şüphe bulunmayan e-postaların kişisel içerik taşımayacağı" vurgulandığı,

- Bu kapsamda iç düzenlemelere uyumun had safhada önem arz ettiği, şirket bilgilerinin, özel kalıp tasarımlarının şirket dışına aktarımı ve e-posta iletişim politikalarına uygunluğu kapsamında kişi bazında e-posta hesaplarının, şirket dışı iletişimleri ve aktarımlarının denetlenmesi yönünde örneklem tekniğiyle incelendiği, bu denetim sırasında çalışan kurumsal e-posta hesabı - çalışan şahsi e-posta trafiğinde şikayetçinin gerçekleştirdiği aktarım şüpheli görülerek, iki adet e-posta gönderisinin içeriğine girildiği ve netice ile mağaza bilgilerinin ilgili kişiye ait kurum e-posta adresinden ilgili kişinin kişisel e-posta adresine iletildiği ve şirket çalışanı ile gerçekleştirilen telefon görüşmesi kaydının yine kurumsal e-posta adresinden ilgili kişinin kişisel e-posta adresine ve üçüncü bir kişiye aktarıldığına dair bulguların elde edildiği,

- Kurumsal e-posta hesabının denetimine dair veri işleme faaliyetinin 6698 sayılı Kanun'un 5'nci maddesinin (2) numaralı fıkrasının (e) bendinde yer alan; "Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" ve (f) bendinde yer alan "İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" veri işleme şartlarına dayalı olarak gerçekleştirildiği ve Kanun'un ilgili maddelerindeki şartları sağlayan bu işleme faaliyeti için açık rıza alınmasını gerektirir hallerin istisnası kapsamında kaldığı, kaldı ki elde edilen bulgu ve olası sonuçlarının da, işleme faaliyetinin şirketlerinin haklı menfaatlerini korumak adına belirli, açık ve meşru bir amaç dahilinde gerçekleştirdiğini ortaya koyduğu kanaatinde oldukları,

- Şirket çalışanlarının e-posta adresleri üzerinde hangi işleme faaliyetlerinin, hangi veri işleme şartına dayalı olarak gerçekleştirildiği hususuna ilişkin olarak; güvenlik, iş amacı dışındaki şahsi kullanımın

tespiti, makul şüphe üzerine başlatılan disiplin soruşturmalarının karara bağlanması, bu sistem ve ekipmanların kullanımı yoluyla hukuka aykırı eylemlerin gerçekleştirilmesinin önüne geçilmesi/eylemlerin tespiti ve her halde iş yeri kurallarına uygunluğunun teyidi amacıyla izlenebildiği, bu işleme faaliyetine ilişkin çalışanlarına aydınlatma gerçekleştirildiği ve yine yukarıda bahsedilen muhtelif yollarla kurumsal e-postaların şahsi kullanımından kaçınılması gerekeceği, bu e-postaların denetlenebileceği hususunda bilgilendirme sağlandığı,

- Ayrıca bu denetim esnasında şüpheli olmayan yazışmaların içeriğinin tetkik edilmediği, sadece içerdiği anahtar kelimeler ve ekler uyarınca hassas görülen yazışmaların incelendiği, Kurumsal Denetim Aktivite Raporunun Teknoloji birimi/unvanlı Bilgi Güvenliği Teknoloji eğitimi almış çalışanları tarafından gerçekleştirildiği ve denetim talebinin doğrudan şirket üst yönetiminden gelmesinin öncelikli koşul olduğu

ifade edilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 19/01/2023 tarih ve 2023/86 sayılı kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, "belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza", (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi", (ğ) bendinde veri işleyenin "veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi" olarak tanımlandığı,

- Kanun'un "Genel İlkeler" başlıklı 4'üncü maddesinde, kişisel verilerin ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükmüne bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, buna göre, kişisel verilerin ancak; a) Hukuka ve dürüstlük kurallarına uygun olma, b) Doğru ve gerektiğinde güncel olma, c) Belirli, açık ve meşru amaçlar için işlenme, ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ile d) İlgili

mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceği,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi; fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin kendisi tarafından alenileştirilmiş olması; bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hükmünün yer aldığı,

- İlgili kişinin şikâyet dilekçesinde; veri sorumlusu tarafından şirket e-posta hesaplarının içeriklerine ulaşılması suretiyle gerçekleştirilen kişisel veri işleme faaliyetinin ve veri sorumlusu tarafından şirket e-posta hesaplarının içeriklerine ulaşılması neticesinde elde edilen kişisel verilerin fesih bildirimine konu edilmesi vasıtasıyla gerçekleştirilen kişisel veri işleme faaliyetinin hukuka aykırı olduğu iddialarının mevcut olduğu,

- İşveren tarafından işçilere kullanım amacıyla tahsis edilen iletişim araçlarının denetiminde işçinin kişisel verilerinin korunması hakkı ile işverenin; kaynakların verimli kullanılmasını sağlama, ticari gizliliği ve yönetim risklerini koruma, çalışanlar tarafından suç işlenmesini önleme, cezai ve hukuki sorumluluğa karşı korunma, bilgi akışının kontrolünü sağlama amaçları arasında menfaat dengesi kurulması gerektiği,

- 17/09/2020 tarih ve 2016/13010 başvuru numaralı Anayasa Mahkemesi Kararı ile Avrupa İnsan Hakları Mahkemesi'nin (AİHM) 12/01/2016 tarihli "Bărbulescu v. Romanya" Kararında değerlendirilen kriterlerin somut olay açısından da dikkate alınması gerektiği, bu kararlarda özetle işverenin hangi ilkeleri göz önünde bulundurarak denetim yapabileceğine ilişkin değerlendirmelere yer verildiği, bu bağlamda, işçinin kişisel verilerinin korunması hakkı ile işverenin denetim hakkı arasında denge kurulurken; işverenin iletişimi denetlemek için önlem alma olasılığı ve bu önlemlerin uygulanması konusunda çalışanı bilgilendirip bilgilendirmediği, bu bilgilendirmenin açık ve net olarak izleme öncesinde yapılıp yapılmadığı, işveren tarafından yapılan izlemenin kapsamı ve işçinin

mahremiyetine yapılan müdahalenin derecesi, iletişim akışı ve içeriklerin izlenmesi arasında bir ayırım yapıp yapılmadığı, iletişimin bir kısmı veya tamamının mı izlendiği, izlemenin zaman açısından sınırlı olup olmadığı, sonuçlara erişimi olan kişilerin sayısı, işverenin iletişimi denetlemek ve içeriğe erişmeyi haklı çıkarmak için meşru gerekçeler sunup sunmadığı, çalışanın iletişimlerinin içeriğine doğrudan erişmekten daha az müdahaleci yöntem ve önlemlere dayalı bir denetim mekanizmasının mümkün olup olmadığı, işçi için izlemenin sonuçları ve sonuçların bilgilendirmede bulunan amaca ulaşmak için kullanılıp kullanılmadığı, işverenin izleme faaliyetlerinin müdahaleci nitelikte olması durumunda işçiye yeterli güvence sağlanıp sağlanmadığı hususlarının dikkate alınması gerektiği, her bir olay özelinde bu hususların tek tek irdelenmesi gerektiği yönünde değerlendirme yapıldığı,

- Uluslararası Çalışma Örgütü'nün işçinin kişisel verilerinin korunmasına ilişkin kılavuzunda da işçiler izleniyorsa izleme nedenleri, zaman çizelgesi, kullanılan yöntem ve teknikler ile toplanacak veriler hakkında önceden bilgilendirilmesi ve işverenin işçilerin özel hayatına müdahaleyi en aza indirmesi gerektiği görüşünde olduğu,

- Madde 29 Çalışma Grubu'nun iş yerinde elektronik iletişimin gözetimi hakkında çalışma belgesinde bazı ilkeler belirlediği; izlemenin işçiler için şeffaf olup olmadığı, işveren açısından bu izlemenin gerekli bulunup bulunmadığı ve daha geleneksel yöntemlerle aynı sonuca ulaşıp ulaşılamayacağı, işlenecek olan kişisel verilerin çalışanlar açısından yasal olup olmadığı ve kişisel verilerin ulaşılması istenen amaçla orantılı olup olmadığı hususunda bir değerlendirme yapılması gerektiği,

- Veri sorumlusu tarafından e-posta denetimi aracılığıyla gerçekleştirilen kişisel veri işleme faaliyeti ile ilgili olarak aydınlatma yükümlülüğünün yerine getirilmesi hususuna ilişkin Kuruma intikal ettirilen Yazılım Alışverişi Politikası, Çalışanlara Ait Kişisel Verilerin İşlenmesi ve Korunması Politikası, Çalışanlara Ait Kişisel Verilerin İşlenmesi ve Korunmasına İlişkin Bilgilendirme, E-Posta Güvenliği, Pazarlama ve İç İletişim Yöneticisi Görev Tanımları, Taahhütname başlıklı metinler incelendiğinde; e-posta yazışmalarının işveren tarafından hangi amaçlarla işlenebileceği, hangi durumlarda e-postaların izlenmesi suretiyle kişisel veri işlenebileceği bilgilerine yer verildiği, iş yeri tarafından tahsis edilen kurumsal e-posta hesabının yalnızca iş amaçlı kullanılabilmesi, kişisel kullanımların en makul seviyede tutulması gerektiği hususlarına yer verildiği dikkate alındığında ilgili kişinin imzalamış olduğu metinlerde atıfta bulunulan hususların okunup anlaşıldığına ilişkin beyanda bulunmuş olduğu ve dolayısı ile bu metinlerde yer alan e-posta denetimi vasıtasıyla

işlenecek kişisel verilere ilişkin veri sorumlusu tarafından ilgili kişiye karşı Kanun'un 10'uncu maddesi çerçevesinde aydınlatma yükümlülüğünün yerine getirilmiş olduğu,

- Öte yandan, ilgili kişi tarafından aydınlatma ve açık rıza metinlerinde veri sorumlusunun yanıltıcı bir şekilde evrakları karıştırarak sunduğu iddiasına ilişkin olarak veri sorumlusu tarafından yanıltıcı bir izlenime sebebiyet verilmeye çalışıldığı hususunda somut bir emareye ulaşılamamış olup ilgili kişi tarafından imzalanan evrakların sahteliği hususunda bir iddia mevcut ise yargı yoluna başvurulmasının mümkün olduğu,

- E-posta denetimi aracılığıyla gerçekleştirilen kişisel veri işleme faaliyetlerinin amacı ve hukuki dayanağı hususlarına ilişkin olarak; veri sorumlusunun giyim sektöründe ticari faaliyette bulunan bir şirket olduğu, iş ile ilgili ticari sır veya herhangi bir bilginin üçüncü taraflarla paylaşılmamasını isteme noktasında ve kurumsal iletişim araçlarının kişisel amaçlarla kullanılmamasının sağlanması hususunda haklı menfaati bulunduğu, ayrıca ilgili kişinin yönetici pozisyonunda görev yaptığı ve bu anlamda şirketin gizli kalmasında menfaati bulunan bilgileri haiz olabileceği dikkate alındığında, İş Kanunu'nun 25'inci maddesinde yer alan "işverenin meslek sırlarını ortaya atmak gibi doğruluk ve bağlılığa uymayan davranışlar"ın tespiti ve Türk Borçlar Kanunu'nun 396'ncı maddesinde yer alan "işverene ait teknik sistemlerin usulüne uygun kullanılması ve iş sırları gibi bilgileri hizmet ilişkisinin devamı süresince kendi yararına kullanamayacağı ve başkalarına açıklayamayacağı" hususlarının tespiti amacıyla veri sorumlusunun e-posta denetimi suretiyle kişisel verileri işlemede haklı menfaati bulunduğu,

- Veri sorumlusunun e-posta denetimi aracılığıyla ulaşılması istenen amaç ile orantılı bir kişisel veri işleme faaliyetinde bulunup bulunmadığı ve söz konusu denetim gerçekleşmeksizin veri sorumlusunun amacına ulaşip ulaşamayacağı hususlarına ilişkin olarak; veri sorumlusu tarafından Kuruma intikal ettirilen Bilgi Güvenliği Yönetim Sistemi Kurumsal Mail Aktivite Denetim Raporu ve elde edilen bulgulara ilişkin ekran görüntüsü incelendiğinde veri sorumlusunun şüpheli konuya sahip ve kurumsal e-posta adresinden üçüncü şahıslar ve çalışanın şahsi e-posta adresine iletilen e-postaların tespit edildiği ve sonrasında iletişimin içeriğine ilişkin bir denetim gerçekleştirildiğinin anlaşıldığı, iletişimin denetlenmesi hususunda iletişim akışı ve iletişim içeriklerinin denetlenmesi arasında bir ayırım yapılmasının önem arz ettiği, iletişim içeriklerinin denetlenmesinin daha katı gerekçelere bağlı olduğu, e-posta kullanımının denetlenmesinde işverenin amacı elverdiği kadarıyla iletişimin içeriğinden ziyade öncelikli olarak işverenin menfaatine ters düşecek şekilde bir güvenlik, sadakat ve kullanım ihlali olabilecek durumların tespiti sonrasında iletişimin içeriğine ilişkin bir denetim yapılması gerektiği, veri sorumlusunun herhangi bir ihlalin gerçekleşip gerçekleşmediğini

ancak içerik denetimi ile ortaya koyabileceği dikkate alındığında veri sorumlusu tarafından yalnızca ilgili personelle ve amaca yönelik kişisel veri ile sınırlı tutularak ve yine yalnızca amaçlanan çerçevede bir kişisel veri işleme faaliyeti gerçekleştirildiği dolayısıyla söz konusu işlemenin Kanun'un Genel İlkeler başlıklı 4'üncü maddesinin (2) numaralı fıkrasının (ç) bendinde yer alan "işlendikleri, amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesine de aykırılık teşkil etmediği,

- Veri sorumlusu tarafından şirket e-posta hesaplarının içeriklerine ulaşılması neticesinde elde edilen kişisel verilerin fesih bildirimine konu edilmesi suretiyle gerçekleştirilen kişisel veri işleme faaliyetinin hukuka aykırı olduğu iddiasına ilişkin olarak; e-posta denetimi aracılığıyla elde edilen kişisel verilerin yukarıda yapılan değerlendirmeler çerçevesinde fesih konusu olayla birebir ilişkili olduğu, veri sorumlusunun işveren sıfatı ile iş sözleşmesinin feshi ile ilgili olarak açıklama ve ispat hakkını kullandığı, bu itibarla kişisel veri niteliğindeki e-posta denetimi suretiyle elde edilen kişisel verilerin fesih bildirimine konu edilmesinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (e) bendinde yer verilen "Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" hükmü kapsamında gerçekleştirildiği, öte yandan, Kanun'un Genel İlkeler başlıklı 4'üncü maddesinin (2) numaralı fıkrasının (ç) bendinde yer alan işlendikleri, amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine de aykırılık teşkil etmediği,

- Öte yandan, İş Kanunu'nun 26'ncı maddesinde ve ilgili Disiplin Yönetmeliği'ndeki 6 iş günlük ve 1 yıllık hak düşürücü süreler geçmesine rağmen fesih tarihinden 607 gün ve 149 gün önce elde edilen e-postaların fesih tarihinde kullanılmasının şirketin e-postaları izlediğinin, süresiz depoladığının ve e-postalar üzerinde genel denetimde bulunduğunun göstergesi olduğu iddiaları ile ilgili olarak; İş Kanunu'nun "Derhal fesih hakkını kullanma süresi" başlıklı 26'ncı maddesinde "24 ve 25 inci maddelerde gösterilen ahlak ve iyiniyet kurallarına uymayan hallere dayanarak işçi veya işveren için tanınmış olan sözleşmeyi fesih yetkisi, iki taraftan birinin bu çeşit davranışlarda bulunduğunu diğer tarafın öğrendiği günden başlayarak altı iş günü geçtikten ve her halde fiilin gerçekleşmesinden itibaren bir yıl sonra kullanılamaz." hükmünün yer aldığı, söz konusu maddede yer alan sürelerin fesih hakkının kullanılmasına ilişkin olarak düzenlenmiş süreler olduğu, e-posta verilerinin saklanması hususu ile ilgisinin bulunmadığı, e-posta verilerinin yaklaşık 2 yıllık bir süre ile saklanması suretiyle gerçekleştirilen kişisel verileri işleme faaliyetinin Kanun'un 4'üncü maddesinde düzenlenen genel ilkelere aykırılık barındırmadığı

değerlendirmelerinden hareketle;

- İlgili kişinin imzalamış olduğu metinlerde okunup anlaşıldığına ilişkin beyanda bulunduğu, dolayısıyla bu metinlerde yer alan e-posta denetimi vasıtasıyla işlenecek kişisel verilere ilişkin veri

sorumlusu tarafından ilgili kişiye karşı Kanun'un 10'uncu maddesi çerçevesinde aydınlatma yükümlülüğünün yerine getirildiği,

- Şirket tarafından e-posta denetimi aracılığıyla gerçekleştirilen kişisel veri işleme faaliyetinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (e) bendinde yer alan "bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" hükmü ile (f) bendinde yer alan "İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması." işleme şartları kapsamında gerçekleştirildiği,

E-posta denetimi aracılığıyla gerçekleştirilen kişisel veri işleme faaliyetinin Kanun'un Genel İlkeler başlıklı 4'üncü maddesinin (2) numaralı fıkrasının (ç) bendinde yer alan işlendikleri, amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine de aykırılık teşkil etmediği,

- İlgili kişinin e-posta ve ses kayıtlarının tarafına iletilmesi hususundaki talebini öncelikli olarak veri sorumlusuna yöneltmediği dikkate alındığında bu hususta Kanun kapsamında yapılacak bir işlem bulunmadığı,

- E-posta denetimi suretiyle elde edilen kişisel verilerin fesih bildirimine konu edilmesinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (e) bendinde yer verilen "Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" hükmü kapsamında gerçekleştirildiği, öte yandan, Kanun'un Genel İlkeler başlıklı 4'üncü maddesinin (2) numaralı fıkrasının (ç) bendinde yer alan işlendikleri, amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine de aykırılık teşkil etmediği değerlendirildiğinden şirket tarafından gerçekleştirilen kişisel veri işleme faaliyetinde herhangi bir hukuka aykırılık bulunmadığı hususları dikkate alındığında veri sorumlusu hakkında Kanun kapsamında yapılacak bir işlem bulunmadığına,

- Veri sorumlusu tarafından somut olayda yanıltıcı bir izlenime sebebiyet verilmeye çalışıldığı hususunda somut bir emareye ulaşılamamış olup ilgili kişi tarafından imzalanan evrakların sahteliği hususunda bir iddia mevcut ise yargı yoluna başvurulmasının mümkün olduğunun ilgili kişiye hatırlatılmasına,

- E-posta verilerinin yaklaşık 2 yıllık bir süre ile saklanması suretiyle gerçekleştirilen kişisel verileri işleme faaliyetinin Kanun'un 4'üncü maddesinde düzenlenen genel ilkelere aykırılık barındırmadığı, bu kapsamda, ilgili kişinin fesih için öne sürülen sebeplerden süresi uygun bulunmayanlar olduğuna ilişkin iddialarının yargı mercileri nezdinde ileri sürülmesi gerektiği hususunda ilgili kişinin bilgilendirilmesine

karar verilmiştir.

2023/78 sayılı KVKK Kararı

İlgili kişinin borç bilgisinin ortağı olduğu şirketin kurumsal numaralarına kısa mesaj olarak gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 19/01/2023 tarihli ve 2023/78 sayılı Karar Özeti

Karar Tarihi : 19/01/2023

Karar No : 2023/78

Konu Özeti: İlgili kişinin borç bilgisinin ortağı olduğu şirketin kurumsal numaralarına kısa mesaj olarak gönderilmesi

İlgili kişinin Kuruma intikal eden dilekçesinde özetle;

- İlgili kişi ile GSM operatörü veri sorumlusu arasında mobil internet hattına ilişkin yapılan sözleşmenin ilgili kişi tarafından iptal edilmesi sonucu tarafına borç çıkarıldığı,
- İlgili kişi adına çıkarılan borcun tahsili için GSM operatörünün bir avukatlık ortaklığına yetki verdiği, avukatlık ortaklığı tarafından borcun tahsilini sağlamak amacıyla ilgili kişinin ortağı olduğu şirkete ait 4 farklı cep telefonu numarasına ilgili kişinin soyadını maskeleyerek fakat adının açıkça görüneceği şekilde borçlu olduğu miktar hakkında icra takibi başlatılacağı bilgilerini içeren bir kısa mesaj gönderildiği,
- Bahsi geçen mesajlar nedeniyle, ilgili kişinin ortağı olduğu şirket hatlarını kullanan çalışanların konu ile ilgileri bulunmamasına karşın ilgili kişinin borç bilgilerinden haberdar olduğu, ayrıca şirkette ilgili kişiyle aynı ada sahip başkaca kimse bulunmadığından soyadı maskelenmiş olsa dahi bahsi geçen kısa mesajda kimliğinin bilinir kılındığı,
- Konuya ilişkin olarak avukatlık ortaklığına ve GSM operatörüne başvurduğu, verilen cevaplarda bilgi amaçlı gönderilen kısa mesajın maskelenerek paylaşıldığı belirtilmiş ise de ilgili kişiye ait kişisel verilerin, ilgili kişinin ortağı olduğu şirket hatlarına hangi amaçla iletildiğinin açıklanamadığı ifade edilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Söz konusu iddialara ilişkin başlatılan inceleme çerçevesinde öncelikle ilgili avukatlık ortaklığından savunması istenilmiş olup alınan cevabi yazıda özetle;

- GSM operatörü tarafından kendilerinin abonelerin borçlarının tahsilat süreçlerinin yürütülmesi konusuyla sınırlı olarak hizmet sözleşmesi ve vekâlet ilişkisi kapsamında yetkilendirildiği, GSM operatörü tarafından yönetilmekte olan sisteme sınırlı erişim hakkına sahip oldukları, bu doğrultuda taraflarının söz konusu sistem üzerinden sınırlı şekilde görüntülenen/erişilen kişisel veriler ve bu veriler kullanılarak gerçekleştirilen kısa mesaj gönderme faaliyetlerine ilişkin olarak Kanun'un 3'üncü maddesinin (1) numaralı fıkrasının (ğ) bendi uyarınca veri işleyen konumunda olduğu, ilgili kişinin avukatlık ortaklığına başvuru hakkı bulunmadığı ve şikâyetinin usulden reddinin gerektiği,
- Nitekim söz konusu şirket ile aralarında imzalanan sözleşmede de avukatlık ortaklığının veri işleyen sıfatı ile sorumlu olacağına ilişkin hükme yer verildiği,
- Avukatlık ortaklığı olarak vekili oldukları şirket adına, müvekkillerinin haklarını ve menfaatlerini korumak amacıyla ve bu anlamda Avukatlık Kanunu'ndan doğan yükümlülüklerini ve yürütmekte olduğu icra işlemleri bakımından 2004 sayılı İcra ve İflas Kanunu ile diğer mevzuattan kaynaklanan hukuki yükümlülüklerini yerine getirmek amacıyla borçluya ait kişisel verileri 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 5'inci maddesinin (2) numaralı fıkrasında yer alan "Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" ve "İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" hukuki sebepleri çerçevesinde işledikleri,
- Belirtilen 4 farklı telefon numarasının ilgili kişinin iletişim numarası olarak avukatlık ortaklığına veri sorumlusu GSM operatörü tarafından iletildiği ve avukatlık ortaklığının da "veri işleyen" sıfatıyla bu numaralara bilgilendirme kısa mesajı gönderdiği, bu bağlamda avukatlık ortaklığının söz konusu şirket tarafından erişim imkânı sağlanan borçlulara ait iletişim numaralarının kaynağını sorgulama yetkisinin bulunmadığı,
- İlgili kişinin iletişim numarası olarak bildirilen numaralara yalnızca bir kez kısa mesaj gönderimi yapıldığı, bu kısa mesajın içeriğinde ise ilgili kişiye ilişkin kişisel verilerin paylaşılmadığı ve ilgili kişinin isminin maskelenerek paylaşıldığı

ifade edilmiştir.

Söz konusu iddialara ilişkin başlatılan inceleme çerçevesinde veri sorumlusu GSM operatöründen de savunması istenilmiş olup alınan cevabi yazıda özetle;

- Veri sorumlusu olarak avukatlık ortaklığı ile hukuki ilişkileri kapsamında ve borcun tahsili amacıyla yalnızca ilgili kişi borçluya ilişkin kimlik, iletişim ve borç bilgilerini içeren verilerin paylaşıldığı,

- Şikâyete konu telefon numaralarının ilgili kişinin ortağı olduğu şirket adına kayıtlı kurumsal numaralar olduğu

ifade edilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 19/01/2023 tarih ve 2023/78 sayılı kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, "belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza", (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi", (ğ) bendinde veri işleyen "veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi" olarak tanımlandığı,

- Kanun'un "Genel İlkeler" başlıklı 4'üncü maddesinde, kişisel verilerin ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, buna göre, kişisel verilerin ancak; a) Hukuka ve dürüstlük kurallarına uygun olma, b) Doğru ve gerektiğinde güncel olma, c) Belirli, açık ve meşru amaçlar için işlenme, ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ile d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceği,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi; fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda

bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin kendisi tarafından alenileştirilmiş olması; bir hakkın tesisi, kullanılması veya korunması için veri işleminin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hükmünün yer aldığı,

- Şikâyete konu olayda avukatlık ortaklığı tarafından sunulan savunmada veri sorumlusu müvekkili ile aralarındaki sözleşme gereği veri sorumlusu sıfatını haiz olmadıkları belirtilmişse de veri sorumlusu sıfatını tayin etmede Kanun çerçevesinde yapılacak değerlendirme için bu sözleşmede yer alan nitelendirmenin esas alınamayacağı; bununla birlikte ilgili kişiye ilişkin kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan, ilgili kişinin ortağı olduğu şirkete ait iletişim numaralarını borcun tahsili amacı ile avukatlık ortaklığı ile paylaşan GSM operatörü şirketin, “veri sorumlusu”; veri sorumlusunun verdiği talimat çerçevesinde ilgili kişiye ait olduğu belirtilen iletişim numaralarına borcun tahsili amacıyla kısa mesaj gönderen avukatlık ortaklığının ise veri işleyen olarak tanımlanabileceği,

- Her ne kadar avukatlık ortaklığı tarafından ilgili kişi borçlunun soyadının yıldızlı bir şekilde yazıldığı ifade edilse de adının tamamı ve soyadının baş harfinin yer alması ile mesajın ilgili kişinin ortağı olduğu şirkete ait telefon numaralarına gönderilmesinin ilgili kişiyi belirlenebilir kıldığı,

- Kanun’da, kişisel verilerin sınırlı sayma yöntemi ile belirlenmediği, bir verinin kişisel veri olması için belirli ya da belirlenebilir gerçek kişiye ilişkin olma kriteri getirildiği; bu kapsamda, ilgili kişinin şirket hattı olan cep telefonu numaralarına gönderilen adı, soyadı, borçlu olduğu firma ve hakkında icra takip işlemlerinin başlatılacağı bilgilerini ihtiva eden kısa mesajın ilgili kişiye ait kişisel verileri içerdiğinin anlaşıldığı,

- Avukatlık ortaklığının savunmasında, veri sorumlusu ile arasındaki vekâlet ilişkisine binaen müvekkilinin alacaklarının takibini gerçekleştirdiği, ilgili kişiye ilişkin tüm iletişim numaralarının veri sorumlusu tarafından irtibat bilgisi olarak paylaşıldığının belirtildiği; veri sorumlusunun savunmasında ise alacağın tahsili için zorunlu olan veriler dışında avukatlık ortaklığına başkaca

kişisel veri aktarılmadığının, şikâyete konu GSM numaralarının ilgili kişinin ortağı olduğu şirket adına kayıtlı kurumsal numaralar olduğunun ifade edildiği,

- İlgili kişinin ortağı olduğu şirkete ait kurumsal iletişim numaralarının Kanun'un 5'inci maddesinin (1) numaralı fıkrası kapsamında veri sorumlusu ile arasındaki bireysel sözleşmelere ilişkin iletişim numarası olarak da kullanılabileceğine dair ilgili kişinin açık rızasının alındığını tevsik eden bilgi ve belgeye savunma ekinde rastlanmadığı,

- Her ne kadar Kanun kapsamında tüzel kişiye ait telefon numaraları kişisel veri olmasa da veri sorumlusu tarafından ilgili kişinin ortağı olduğu şirkete ait kurumsal telefon numaralarının ilgili kişinin iletişim numarası olarak avukatlık ortaklığı ile paylaşılmasının, Kanun'un 4'üncü maddesinin (2) numaralı fıkrasının (b) bendine aykırı olarak ilgili kişiye ilişkin kişisel verilerin doğru bir şekilde işlenmediği şeklinde değerlendirileceği, bu nedenle avukatlık ortaklığı tarafından ilgili kişiye ilişkin kişisel verileri içeren kısa mesajların şirkete ait iletişim numaralarına gönderilmesi neticesinde borca konu işlemle ilgisi olmayan üçüncü kişi şirket çalışanları ile ilgili kişiye ilişkin kişisel veri olan borç bilgisinin Kanun'un 5'inci maddesinde yer alan herhangi bir işleme şartı bulunmaksızın paylaşıldığı değerlendirmelerinden hareketle;

- İlgili kişinin ortağı olduğu Şirkete ait kurumsal iletişim numaralarının, veri sorumlusu ile arasındaki bireysel sözleşmelerde de iletişim numarası olarak kullanılmasının veri sorumlusu tarafından Kanun'un 4'üncü maddesinde yer alan Genel İlkelerden "doğru ve gerektiğinde güncel" olma ilkesine aykırılık teşkil ettiği anlaşılmış olup, bu hukuka aykırı veri işleme faaliyeti nedeniyle avukatlık ortaklığı tarafından ilgili kişiye ilişkin kişisel verileri içeren kısa mesajların şirkete ait iletişim numaralarına gönderilmesi neticesinde, borca konu işlemle ilgisi olmayan üçüncü kişi şirket çalışanları ile ilgili kişiye ilişkin kişisel veri olan borç bilgisinin Kanun'un 5'inci maddesinde yer alan herhangi bir işleme şartı bulunmaksızın paylaşıldığı gözetildiğinde; Kanun'un 12'nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülüklerini yerine getirmediği kanaatine varılan veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 85.000 TL idari para cezası uygulanmasına,

- Veri sorumlusu tarafından verilen talimat çerçevesinde borcun tahsili amacıyla ilgili kişiye ilişkin olduğu belirtilen telefon numaralarına bir adet kısa mesaj gönderen ve sınırlı yetkisi çerçevesinde söz konusu numaralara ilişkin doğrulama imkânı olmayan veri işleyen avukatlık ortaklığı hakkında Kanun kapsamında yapılacak bir işlem bulunmadığına

karar verilmiştir.

2023/67 sayılı KVKK Kararı

Veri sorumlusu bir banka tarafından ilgili kişinin para transferleri ile hesap bilgilerinin üçüncü kişiye ait e-postaya gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 12/01/2023 tarihli ve 2023/67 sayılı Karar Özeti

Karar Tarihi : 12/01/2023

Karar No : 2023/67

Konu Özeti: Bir banka tarafından ilgili kişinin para transferleri ile hesap bilgilerinin üçüncü kişiye ait e-postaya gönderilmesi

İlgili kişi tarafından Kuruma intikal ettirilen dilekçede özetle;

- Bir banka nezdindeki hesabına ilişkin ekstre ve anlık hesap hareketlerinin, ilgili kişinin bilgisi ve rızası dışında üçüncü bir kişinin e-posta adresine gönderildiği, bu suretle ilgili kişinin tüm para transferleri ile hesap bilgilerinin, üçüncü kişiler tarafından öğrenildiği, bu sebeple güvensizlik ve tedirginlik içinde olduğu, veri sorumlusu tarafından aydınlatma yükümlülüğünün yerine getirilmediği,
- Veri sorumlusuna yapılan başvuruya istinaden gönderilen cevabi yazıda üçüncü kişinin e-posta adresinin ilgili kişinin ortağı olduğu şirketin vekili tarafından 2017 yılında çek karnesi talebi için bankaya bildirildiği yönünde beyanda bulunulduğu, veri sorumlusu tarafından, 2018 yılına ilişkin bireysel emeklilik sözleşmesi teklifi ve 2020 yılına ilişkin hayat sigortası formlarında, söz konusu e-posta adresinin yer almasına karşın ilgili kişinin itiraz etmeksizin bu formlara onay verdiğinin öne sürüldüğü ve veri ihlali yaşanmadığının iddia edildiği,
- Hukuken temsilci, vekil, veli veya vasi aracılığıyla gerçekleştirilen işlemlerin asil tarafından yapılmış kabul edilmesi sebebiyle bu kişilere yapılacak aydınlatmanın kanunen yeterli görüldüğü ancak şirket vekilinin, ilgili kişinin şahsi vekili olmadığı, diğer taraftan uyuşmazlığa konu olan hususta, e-posta adresinin ilgili kişinin şahsına ait olduğu varsayımında dahi, yetkisiz temsilciye yapılan aydınlatmanın hukuken geçerli olmadığı, ayrıca gönderim yapılan e-posta adresi ilgili kişiye ait olmadığından hukuken geçerli bir aydınlatmaya dayanmaksızın alınan rıza beyanının da batıl olduğu,

- 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 4'üncü maddesi uyarınca kişisel verilerin doğru ve güncel olması gerektiği, bu hususta veri sorumlusunun aktif özen yükümlülüğünün bulunduğu, veri sorumlusu tarafından ilgili kişinin bilgilerinin doğru ve güncel olmasını temin edecek kanalların açık tutulması gerektiği, veri sorumluları tarafından üçüncü kişilerin telefon numarası, e-posta adresi gibi kanallarına, ekstreleri vb. kişisel veri içeren belgelerin gönderilmesini önlemek ve bu iletişim adreslerinin doğruluğunu teyit etmek amacıyla veri sorumluları tarafından gerekli idari ve teknik tedbirlerin alınmasının zorunlu olduğu, veri sorumlusu tarafından sistemde kayıtlı e-posta adresinin ilgili kişiye ait olup olmadığının teyit edilmediği,
- Veri sorumlusu tarafından daha sonraki tarihlerde ilgili kişiye sunulan tüm sözleşme, teklif ve formlarda e-posta iletişim bilgisinin basılı olarak yer alması nedeniyle e-posta adresindeki yanlışlığı fark etme ve düzeltme imkânının tanınmadığı

belirtilerek veri güvenliğinin ihlal edilmesi sebebiyle gereğinin yapılması talep edilmiştir.

Şikâyet dilekçesinde yer alan hususlara ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabî yazıda özetle;

- İlgili kişinin ortağı olduğu şirketin banka müşterilerinden biri olduğu, ilgili kişinin ortağı olduğu şirket için 2017 yılında çek karnesi talep edildiği ve o dönem çek karnesi için Findeks üyeliği gerektiğinden firmaya Findeks üyeliği oluşturulduğu, Findeks üyeliği oluşturmak için firma yetkililerinin iletişim bilgilerinin sisteme girilmesinin zorunlu tutulması nedeniyle ilgili kişinin hesabına, şikâyete konu olan e-posta adresinin tanımlandığı, Findeks üyelik formunun firma yetkililerinin banka sistemindeki iletişim bilgileri ile doldurulduğu ve firma yetkilileri tarafından imzalandığı,
- Somut olayda Findeks üyelik formunda ilgili kişiye ait iletişim bilgilerinin, ilgili kişinin ortağı olduğu şirketin vekili tarafından bankaya ibraz edildiği, söz konusu formda bu adresin açıkça ekstreler ile hesap hareketlerinin gönderildiği e-posta adresi olarak belirtildiği ve evrakın vekil tarafından imzalandığının tespit edildiği,
- İlgili e-posta adresi verisinin, Findeks üyelik sözleşmesinin ifası için alınması gereken zorunlu bir bilgi olduğu, bu kapsamda söz konusu kişisel verinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (c) bendi uyarınca işlendiği, dolayısıyla "açık rıza alınmadığı" şeklindeki iddiaların yersiz olduğu,
- Türkiye Bankalar Birliği öncülüğünde sektör ve Kurul tarafından hazırlanmış olan Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Kılavuz Taslağı'nda belirtildiği üzere; her

bir kredi kullandırma işlemi özelinde “risk grubu”nda bulunan ilgili kişilerin tek tek aydınlatılması suretiyle değil, kolayca erişilebilecek şekilde ve sadece “Risk Grubu” faaliyetleri bakımından genel bir aydınlatma yapılabildiği,

- Gayri nakdi kredi işlemi olan çek karnesi başvurusunda risk grubu içerisinde yer alan ilgili kişinin kişisel verisinin işlenmesine ilişkin aydınlatma yükümlülüğünün veri sorumlusunun internet sitesi aracılığıyla yerine getirildiği,
- İlgili kişinin, e-posta adresinin silinmesi talebini bankaya iletmesi üzerine aynı gün içerisinde ilgili kişinin hesabına kayıtlı e-posta adresinin silindiği ve yeni e-posta adresinin eklendiği, EFT ve havale bilgilendirme e-postalarının ilgili kişi tarafından aktif hale getirildiği, 2020 yılında ilk EFT ve havale bilgilendirme e-postalarının gönderilmiş olduğu, bu tarihe kadar olan süreçte, söz konusu hatalı e-posta adresine gönderilen e-postalar incelendiğinde, gönderilen e-postaların müşterinin ortağı olduğu firmaya ait ekstre, EFT/havale transfer limit değişiklik bilgilerini içerdiği ve müşteriye ait herhangi bir kişisel veri içermediğinin görüldüğü, bu yüzden şikâyetçinin kişisel verilerinin hukuka aykırı şekilde üçüncü kişilerle paylaşıldığı iddiasının mesnetsiz olduğu,
- İlgili kişinin onayı ve teyidi sonrası gönderilen e-postalar için Kanun’a ve Türk Ceza Kanunu’na (TCK) aykırılık iddiasının söz konusu olamayacağı, zira halihazırda Kanun’un 5’inci maddesinde yer alan hukuka uygunluk sebepleri çerçevesinde işlenmiş olan ve Kanun’un 11’inci maddesi çerçevesinde doğruluğu teyit edilmiş bir e-posta adresine gerekli tüm teknik ve idari tedbirler alınarak; veri sorumlusunun hukuki yükümlülüğü çerçevesinde, ilgili kişinin talebi doğrultusunda e-posta iletilmesinin hem Kanun hem de TCK kapsamında ihlal olarak değerlendirilemeyeceği,
- İlgili kişinin kişisel verisinin yanlış ibrazından haberi olmadığı ve fark etme/düzeltilme imkânı tanınmadığı iddiasının mesnetsiz olduğu,
- Doktrinde de açıkça ifade edildiği gibi ana kuralın ilgili tarafından doğru veri iletilmesi olduğu ve Kanun’un 11’inci maddesinin (1) numaralı fıkrasının (d) bendinde yer alan kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesi hakkının kullanılabilmesi için veri sorumlusunun ilgili kişiye gerekli ortamı sağlama yükümlülüğünün bulunduğu,
- Verinin doğruluğu ve güncelliği için ilgili kişiye her türlü imkânın sağlanarak başvuru kanalının açıldığı, ilgili kişinin imzaladığı evrakta gördüğü e-posta adresine işlem esnasında itiraz etme olanağının bulunduğu,

- Veri sorumlusunun kayıtlarında yapılan incelemede, şikâyete konu olan e-posta adresine ilk e-posta gönderiminin 2018 yılında gerçekleştiği, son e-posta gönderiminin ise 2021 yılında gerçekleştiğinin tespit edildiği,
- İlgili kişiye ilişkin hatalı e-posta adresine 2020 yılına kadar herhangi bir kişisel veri iletilmediği ve yalnızca tüzel kişiye ait bilgilerin iletildiği, bu yüzden Kanun kapsamında giren herhangi bir durumun söz konusu olmadığı, 2020 yılından sonra gönderilen e-postaların ise halihazırda onay ve teyit alınarak gönderildiği,
- Yapılan incelemelerde gönderilen e-postaların tamamının müşterinin sisteminde kayıtlı olan adresine sistem tarafından gönderilen e-postalar olduğunun belirlendiği, söz konusu e-posta adresine sistem haricinde personel tarafından herhangi bir gönderim yapılmadığının tespit edildiği,
- Tüm bu sebeplerle hukuka aykırı veri paylaşımı yapıldığı, ilgili kişiye kişisel verilerini düzeltme ve yanlışlığı fark etme imkânının tanınmadığı iddiasının gerçek dışı olduğu,
- Kişisel verilerin işlenmesi noktasında her türlü önlemin alındığı, Kanun'un 4'üncü maddesinde yer alan ilkelere uygun davranıldığı ve taleplerine ilişkin olarak ilgili kişilerin her türlü kanaldan ulaşması için imkân sağlandığı

hususları bildirilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 12/01/2023 tarih ve 2023/67 sayılı Kararı ile;

- Kanun'un, kişisel verilerin işlenmesine ilişkin "Genel İlkeler"i düzenleyen 4'üncü maddesinin (1) numaralı fıkrasında, "Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir." hükmünün yer aldığı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin; a) hukuka ve dürüstlük kurallarına uygun olma, b) doğru ve gerektiğinde güncel olma, c) belirli, açık ve meşru amaçlar için işlenme, ç) işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, d) ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,
- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin

gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu,

- Kişisel verilerin işlenmesinde Kanun'un 4'üncü maddesi uyarınca temel ilkelere uyumluluğun zorunlu olduğu, "doğru ve gerektiğinde güncel olma" ilkesinin de veri sorumluları tarafından uyulması zorunlu bu temel ilkelerden bir tanesini teşkil ettiği, Kurulun 22/12/2020 tarihli ve 2020/966 sayılı İlke Kararı'nda da "doğru ve gerektiğinde güncel olma" ilkesi doğrultusunda veri sorumlusunun makul önlemler alması gerektiğinin belirtildiği, anılan İlke Kararı ile veri sorumluları tarafından kendilerine bildirilen irtibat numaralarının doğruluğunu teyit edecek mekanizmaların oluşturulması adına gerekli idari ve teknik tedbirlerin alınmasına karar verildiği, kişisel verilerin doğru ve güncel bir şekilde tutulmasının, veri sorumlusunun çıkarına uygun olduğu gibi ilgili kişinin temel hak ve özgürlüklerinin korunması açısından da gerekli olduğu, kişisel verilerin doğru ve gerektiğinde güncel olmasının sağlanması noktasında aktif özen yükümlülüğünün; veri sorumlusunun bu verilere dayalı olarak ilgili kişiyle alakalı bir sonuç ortaya koyması halinde geçerli olduğunun değerlendirildiği, bunun dışında veri sorumlusunun her zaman ilgili kişinin bilgilerinin doğru ve güncel olmasını temin edecek kanalları açık tutması gerektiği,

- Şikâyete konu e-posta adresinin ilk olarak ilgili kişinin ortağı olduğu şirketin vekili tarafından banka ile paylaşıldığı, sonrasında ilgili kişinin bireysel emeklilik başvurusu sırasında kendisine sunulan formda yer alan söz konusu e-posta adresini formu imzalamak suretiyle onayladığı, öte yandan ilgili kişinin başvurusu üzerine veri sorumlusunun hemen aksiyon alarak e-posta adresinde gerekli düzeltmeyi yaptığı göz önünde bulundurulduğunda, somut olaya konu olan işleme faaliyetinin hukuka uygun yürütülmesi bakımından veri sorumlusunun özen yükümlülüğü çerçevesinde hareket ettiği,

- Öte yandan, hatalı e-posta adresine giden bildirimlerin kişinin hesap hareketlerinin üçüncü bir kişiye açıklanmasının yanı sıra olası dolandırıcılık olaylarında hesaptan, hesap sahibinin bilgisi dışında para çekilmesi gibi durumlardan haberdar olunamaması gibi sonuçlara yol açabileceğinin veri sorumlusu tarafından göz önünde bulundurulması gerektiği, ilgili kişi açısından para transferlerine ilişkin bilgilendirmelerin alnamamasının ve üçüncü kişiye gönderilmesinin hak kaybına sebebiyet verebileceği dikkate alındığında, veri sorumlusunun Kişisel Verileri Koruma

Kurulunun “22/12/2020 tarihli ve 2020/966 sayılı İlke Kararı” doğrultusunda, banka işlemlerinde kullanılan ilgili kişilerin iletişim bilgilerinin belirli periyotlarla doğrulanması ve güncelliğinin sağlanması hususunda gerekli mekanizmaları kurması gerektiği

değerlendirmelerinden hareketle

- Şikâyete konu e-posta adresinin ilk olarak ilgili kişinin ortağı olduğu şirketin vekili tarafından banka ile paylaşıldığı sonrasında ilgili kişinin bireysel emeklilik başvurusu sırasında kendisine sunulan formda yer alan söz konusu e-posta adresini formu imzalamak suretiyle onayladığı, öte yandan ilgili kişinin başvurusu üzerine veri sorumlusunun hemen aksiyon olarak e-posta adresinde gerekli düzeltmeyi yaptığı hususları dikkate alındığında şikâyet konusu ile ilgili olarak veri sorumlusu banka hakkında Kanun kapsamında yapılacak bir işlem olmadığına,
- “Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına Kanun’a aykırı şekilde gönderilen üçüncü kişilere ait kişisel veriler hakkında Kişisel Verileri Koruma Kurulunun “22/12/2020 tarihli ve 2020/966 sayılı İlke Kararı” doğrultusunda, banka işlemlerinde kullanılan ilgili kişilerin iletişim bilgilerinin belirli periyotlarla doğrulanması ve güncelliğinin sağlanması hususunda gerekli mekanizmaların kurulmasına ilişkin veri sorumlusunun uyarılmasına karar verilmiştir.

2023/4 sayılı KVKK Kararı

Bir kargo firmasının çapraz barkodlama hatası nedeniyle kişisel verilerin hukuka aykırı olarak paylaşımına sebep olması hakkında Kişisel Verileri Koruma Kurulunun 05/01/2023 tarihli ve 2023/4 sayılı Kararı

Karar Tarihi : 05/01/2023

Karar No : 2023/4

Konu Özeti: Bir kargo firmasının çapraz barkodlama hatası nedeniyle kişisel verilerin hukuka aykırı olarak paylaşımına sebep olması

İlgili kişinin şikayetinde özetle; bir e-ticaret firmasından satın aldığı ürünü tarafına teslim edecek kargo firmasının siparişi ilgili kişiye teslim etmesini müteakip ilgili kişi tarafından kargo paketinin üzerinde kendisi dışında isim benzerliği bulunan başka bir kişiye (üçüncü kişi) ait adres ve iletişim bilgilerinin yer aldığını gördüğü, veri sorumlusu kargo firmasına 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında başvuruda bulunarak kendisi dışında üçüncü kişiye ait kişisel verilerin hangi hukuki gerekçeyle tarafına gönderildiği, benzer şekilde kendisine ait kişisel verilerin de üçüncü kişilere aktarılıp aktarılmadığı ve aktarıldıysa hangi hukuki nedenlere dayanılarak aktarıldığı hususlarına ilişkin bilgi talep ettiği, veri sorumlusu tarafından verilen cevabi yazıda söz konusu durumun barkodlama işlemi sırasında gerçekleşen bir hata sonucunda meydana geldiğinin ve ilgili kişiye ait gönderinin üçüncü kişiden iade alınarak gönderici firmaya teslim edildiğinin belirtildiği, söz konusu beyanlardan hareketle veri sorumlusunun yapmış olduğu çapraz kargo gönderimi hatası nedeniyle ilgili kişiye teslim edilmesi gereken kargo paketinin üçüncü kişiye gönderildiği ve bu suretle ilgili kişiye ait kişisel verilerin üçüncü kişi ile paylaşıldığı sonucuna varıldığı, bu itibarla veri sorumlusunun hem ilgili kişiye hem de üçüncü kişiye ait kişisel verileri Kanun'un 8'inci maddesine aykırı olarak aktardığı belirtilerek gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusunun savunması talep edilmiş olup veri sorumlusundan alınan cevabi yazıda özetle;

- Şikâyete konu olayın meydana geliş şekline ilişkin olarak; veri sorumlusu tarafından ilgili kişiye gönderilmek üzere faturalandırılan gönderinin acente personeli tarafından toplu şekilde barkodlama

işlemi yapılırken aynı isimli başka bir müşteriye ait gönderi ile isim benzerliği nedeniyle karıştırıldığı ve çapraz barkodlama hatası yapıldığının tespit edildiği, bu nedenle bir diğer müşterileri olan üçüncü kişinin kargosunun ilgili kişiye, ilgili kişinin kargosunun ise üçüncü kişiye teslim edilmek üzere barkodlandığı ve bu şekilde ulaştırıldığı, işlemin fark edilmesiyle birlikte şikâyetçi müşteriye ait gönderinin diğer müşterileri olan üçüncü kişiden alınarak gönderici firmaya iade edildiği,

- Gerçekleştirilen bu eylemin sistematik bir hata olmadığı, veri sorumlusunun acente çalışanları tarafından manuel olarak gerçekleştirilen barkodlama işlemi sırasında bir kereye mahsus olmak üzere sehven ortaya çıkan bir olay olduğu,
- Veri sorumlusunun müşterilerine ait kişisel verileri yalnızca taşıma hizmetinin ifası için ilgili birimlerle, ifa yardımcısıyla, Bilgi Teknolojileri ve İletişim Kurumu, talep halinde Ulaştırma Denizcilik ve Haberleşme Bakanlığı ve kanunen kişisel verileri talep etmeye yetkili kamu kurumları ile paylaştığı,
- Bu çerçevede ilgili kişinin ve yine veri sorumlusundan hizmet alan hiçbir müşterinin kişisel verisinin istenmeden yaşanan münferit olay dışında üçüncü kişilerle paylaşılmadığı, bu güvenliğin sağlanabilmesi için idari ve teknik pek çok önlemin alındığı, söz konusu tedbirlerin günün gerekleri ve yürürlükteki mevzuat uyarınca gerekli oldukça geliştirildiği ve güncellendiği,
- Veri sorumlusunun taşıma hizmeti kapsamında belli bilgileri kargo/gönderi üzerine yazmasının Karayolu Taşıma Kanunu'nun 43'üncü maddesi gereğince bir yükümlülük olduğu, dolayısıyla alıcıların isim ve adres bilgilerinin kargo üzerinde yazdığı,
- Veri sorumlusunun belli taşıyıcılık faaliyetlerini, akdettiği acentelik sözleşmeleri vasıtasıyla yürüttüğü, şikâyete konu işlemin de bir acentenin istihdam ettiği personel tarafından yapıldığı,
- Veri sorumlusunun hizmetlerin güvenliği konusunda hassas davrandığı ve mezkûr vakiada da kasıtlı bir eyleminin bulunmadığı, kargo dağıtım süreçlerinde istemeden de olsa yaşanan bu gibi aksaklıkların önüne geçilebilmesi için acentelere ve ilgili tüm birim personeline gerekli bildirimlerin sıklıkla gerçekleştirildiği, çalışanlara yükümlülükleriyle ilgili düzenli eğitimlerin verildiği ve farkındalık çalışmaları yapıldığı, nitekim söz konusu acentenin çalışanlarına da kişisel verilerin korunmasına ilişkin muhtelif tarihlerde eğitimler verildiği, belirli aralıklarla hatırlatma SMS'leri gönderildiği,
- Veri sorumlusu tarafından kişisel verilerin korunmasına yönelik bilgilendirme ve aydınlatmaların yerine getirildiği, firmalarının bilgi ve kişisel veri güvenliği konusunda da uluslararası standartları

haiz bir kurum olduđu, kişisel verilerin korunmasının ve ilgili yasal mevzuata uyumun öncelikli önem verdiđi deđer ve politikalar arasında olduđu, bu konunun en önemli bölümlerinden birini müşterilerinin kişisel verilerinin korunmasının oluşturduđu,

- İzah ettikleri üzere yaşanan olayda veri sorumlusunun kasıtlı bir eyleminin bulunmadığı, tekrarlanmaması için gerekli hassasiyet ve özenin gösterileceđi bildirilmiştir.

Konuya ilişkin yapılan inceleme neticesinde, Kişisel Verileri Koruma Kurulunun 05/01/2023 tarihli ve 2023/4 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, "belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza", (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi", (ğ) bendinde veri işleyenin "veri sorumlusunun verdiđi yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi" olarak tanımlandığı,

- Kanun'un, kişisel verilerin işlenmesine ilişkin "Genel İlkeler"i düzenleyen 4'üncü maddesinin (1) numaralı fıkrasında, "Kişisel veriler, ancak bu Kanunda ve diđer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir." hükmünün yer aldığı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin; a) hukuka ve dürüstlük kurallarına uygun olma, b) doğru ve gerektiğinde güncel olma, c) belirli, açık ve meşru amaçlar için işlenme, ç) işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, d) ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceđi, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi; fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda

bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin kendisi tarafından alenileştirilmiş olması; bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hükmünün yer aldığı,

- Kanun'un 12'nci maddesinin (1) numaralı fıkrası gereğince veri sorumlusunun; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğunun, (5) numaralı fıkrası gereğince de işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunun bu durumu en kısa sürede ilgisine ve Kurula bildirmesi gerektiğinin hükme bağlandığı,

- İlgili kişiye ait isim, soy isim ve adres bilgilerinin ilgili kişiyi belirli veya belirlenebilir kılmaya yeterli olduğu, bu yüzden, bahsi geçen bilgilerin Kanun'un 3'üncü maddesindeki tanım uyarınca "kişisel veri" niteliğini haiz olduğu, ilgili kişiye ait mezkûr kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması, kullanılmasının engellenmesi ve sair fiillerin Kanun'un 3'üncü maddesindeki tanım kapsamında birer "kişisel verilerin işlenmesi" faaliyeti olduğu,

- Veri sorumlusu ile acente arasında akdedildiği belirtilen "acentelik sözleşmesi" de dâhil olmak üzere taraflarca dosyaya sunulan bilgi ve belgelerin, somut olayda mezkûr acentenin Kanun hükümleri karşısında "veri sorumlusu" olarak kabul edilebilmesine yetecek nitelikte olmadığı, zira taraflar arasında akdedilen acentelik sözleşmesinde söz konusu acentenin faaliyetlerini veri sorumlusunun nam ve hesabına yürüttüğünün açık bir şekilde düzenlenmiş olduğu, bu şartlarda acentenin, Kanun'un 3'üncü maddesinde yapılan tanımlar itibarıyla ancak "veri işleyen" sıfatını haiz olduğu,

- Veri sorumlusunun uhdesinde bulunan/işlenen kişisel verilerin güvenliğini sağlamak için gerekli her türlü teknik ve idari tedbiri almak konusunda Kanun'un 12'nci maddesinin (1) numaralı fıkrasından kaynaklanan bir zorunluluğu bulunduğu, bu yüzden, veri sorumlusunun savunmasında almış olduğunu beyan ettiği kişisel verilerin korunmasına ilişkin tedbirlerin Kanun'un 12'nci maddesinin (1) numaralı fıkrasının birer gereği olduğu,
- Somut olayda, ilgili kişiye ait isim, soy isim ve adres kişisel verilerinin, veri sorumlusunca türleri/nitelikleri dikkate alındığında ancak Kanun'un 5'inci maddesinde yer alan şartlardan en az birine dayanılarak ve 4'üncü maddesinde zikredilen genel ilkelere uygun olarak işlenebileceği,
- İlgili kişiye ait isim, soy isim ve adres kişisel verilerinin veri sorumlusu tarafından üçüncü şahısla paylaşılmasından ibaret olan kişisel veri işleme faaliyetinin yeni/müstakil bir kişisel veri işleme faaliyeti olduğu ve söz konusu kişisel veri işleme faaliyeti açısından da Kanun'un 5'inci maddesinde yer alan şartlardan en az birine dayanılmış olması gerektiği,
- Veri sorumlusunun 4925 sayılı Karayolu Taşıma Kanunu'nun 43'üncü maddesine atıf yaptığı savunmasından, veri sorumlusunca ilgili kişi hakkında yürütülen kişisel veri işleme faaliyetlerinde Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (a) bendindeki "kanunlarda açıkça öngörülmesi" hukuki şartına dayanıldığına anlaşıldığı, buna karşın, yapılan inceleme neticesinde, veri sorumlusunun atıf yaptığı 4925 sayılı Karayolu Taşıma Kanunu'nun toplamda 38 (otuz sekiz) maddeden ibaret olduğunun görüldüğü; bu yüzden de 4925 sayılı Karayolu Taşıma Kanunu içerisinde veri sorumlusunun beyan ettiği 43'üncü maddenin tespit edilemediği, ayrıca, taşıma hizmeti kapsamında alıcıların isim ve adres bilgilerinin kargo üzerine yazılmasını gerektiren bir yükümlülüğün mevzuatta öngörülmüş olmasının, veri sorumlularının somut olayda olduğu gibi kişisel verileri hatalı olarak işlediği (aslında kargoyla alakası olmayan ilgili kişilerin kişisel verilerinin kargo paketi üzerine yazıldığı) durumlarda geçerli bir kişisel veri işleme sebebi/şartı olarak kabul edilemeyeceği, dolayısıyla, somut olayda veri sorumlusu tarafından ilgili kişinin kişisel verilerinin "çapraz barkodlama hatası" yapılarak üçüncü bir kişi ile paylaşılması suretiyle yürütülen kişisel veri işleme faaliyetinde Kanun'un 5'inci maddesinde düzenlenen herhangi bir hukuki şartına dayanılmadığı sonucuna ulaşıldığı,
- Veri sorumlularının uhdelinde bulunan/işlenen kişisel verilerin güvenliğini sağlamak için gerekli her türlü teknik ve idari tedbiri almak konusunda Kanun'un 12'nci maddesinin (1) numaralı fıkrasından kaynaklanan zorunluluğa uymamaları halinde, ortaya bir veya daha fazla "kişisel veri ihlali" çıkmasının ihtimal dâhilinde olduğu, kişisel veri ihlali durumlarında ise veri sorumluları

tarafından Kanun'un 12'nci maddesinin (5) numaralı fıkrasında düzenlenen "veri ihlal bildirimini" yolunun işletilmesi ve "ilgili kişilere ve Kurula bildirim yükümlülüğü"ne uyulması gerektiği,

Bu çerçevede ilgili kişinin kişisel verilerinin üçüncü kişiyle paylaşılmasının yeni bir kişisel veri işleme faaliyeti olduğu, buna karşın söz konusu kişisel veri işleme faaliyetinin Kanun'da yer alan herhangi bir işleme şartına dayanmadığı, veri sorumlusunun anılan fiilinin ise Kanun'un kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirlerin alınmasını zorunlu kılan 12'nci maddesinin (1) numaralı fıkrasına aykırılık teşkil ettiği, öte yandan söz konusu durumun bir veri ihlali olmasına karşın veri sorumlusunun Kanun'un 12'nci maddesinin (5) numaralı fıkrası kapsamında Kurula veri ihlal bildiriminde bulunmadığı

değerlendirmelerinden hareketle;

- İlgili kişinin kişisel verilerinin üçüncü kişi ile paylaşılmasının yeni bir veri işleme faaliyeti olduğu, söz konusu veri işlemenin Kanun'da yer alan herhangi bir işleme şartına dayanmadığı, veri sorumlusunun anılan fiilinin Kanun'un veri güvenliğine ilişkin yükümlülüklerin düzenlendiği 12'nci maddesinin (1) numaralı fıkrasının (a) bendi hükmüne aykırılık teşkil ettiği, öte yandan söz konusu durumun bir veri ihlali olmasına karşın veri sorumlusunun Kanun'un 12'nci maddesinin (5) numaralı fıkrası kapsamında Kurula veri ihlal bildiriminde bulunmadığı da dikkate alındığında; Kanun'un 12'nci maddesinde yer alan yükümlülüklerini yerine getirmeyen veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendine istinaden 75.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2022/1358 sayılı KVKK Kararı

Bir internet sitesinde yer alan çerezlere ilişkin aydınlatma ve açık rıza metinlerinin sunulmaması hakkında Kişisel Verileri Koruma Kurulunun 23/12/2022 tarihli ve 2022/1358 sayılı Karar Özeti

Karar Tarihi : 23/12/2022

Karar No : 2022/1358

Konu Özeti: Bir internet sitesinde yer alan çerezlere ilişkin aydınlatma ve açık rıza metinlerinin sunulmaması

İlgili kişinin Kuruma intikal eden şikayetinde özetle; bir oyun platformunun internet sayfasına giriş yapıldığında çerez işleme süreçleriyle ilgili kullanıcılara aydınlatma yapılmadığı ve zorunlu olmayan çerezler için açık rıza alınmadığı, siteye üye olan kullanıcılardan kimlik ve iletişim bilgilerinin talep edildiği ancak aydınlatma ve açık rıza metinlerinin sunulmadığı, ilgili şirkete başvuru yapılmakla birlikte yeterli bir cevap alınamadığı ifade edilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde sitenin işletilmesinden sorumlu veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- Söz konusu internet sitesinin şirkete ait olduğu ancak Türkiye'deki operasyonlarından başka bir şirketin sorumlu olduğu,
- KVKK aydınlatma metnine sitede paylaşılan link aracılığı ile ulaşılabildiği ve bu metinde kişisel verilerin hangi amaçlarla işlendiğine dair kapsamlı bir açıklama sunulduğu,
- Sitede satıcılar için satış yapma ön şartı olan telefon ve kimlik onay zorunluluğu olduğu, bu bilgilerin satıcıların kendi kabulleri ile siteye girildiği ve yalnızca satış esnasında oluşan komisyon sözleşmesi sebebiyle alındığı, alınan bilgilerin yalnızca sözleşme kapsamında doğacak hukuki sorumluluk kaynaklı olarak talep edildiği ve satıcılar tarafından siteye iletildiği,
- İlgili kişinin site üzerinde bir sanal hesap satım işlemi gerçekleştirmesi neticesinde komisyon sözleşmesinden doğan sorumluluğun yanı sıra alıcının satış sonrası uğrayabileceği zararlardan

doğacak rücu hakkından dolayı muhtemel hukuki sorumluluğa karşı bu verilerin işlenmesinin veri sorumlusu açısından zaruri olduğu,

- Bu kapsamda internet sitesinde işlenen kişisel verilerin Kanun'un 5'inci maddesinin (2) numaralı fıkrasında yer alan "bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması" ile "veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" şartlarına dayanılarak işlendiği, ifade edilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulunun 23/12/2022 tarih ve 2022/1358 sayılı Kararı ile;

- Kanun'un 5'inci maddesinin kişisel verilerin işleme şartlarını düzenlediği, maddenin (1) numaralı fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin hüküm altına alındığı, (2) numaralı fıkrada ise, kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda olan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün korunması için veri işlemenin zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaati için veri işlenmesinin zorunlu olması hallerinde ilgili kişinin açık rızası olmaksızın kişisel verilerin işlenmesinin mümkün olduğunun hükme bağlandığı,

- Kanun'un "Veri Sorumlusunun Aydınlatma Yükümlülüğü" başlıklı 10'uncu maddesinin (1) numaralı fıkrasında kişisel verilerin elde edilmesi sırasında veri sorumlusunun veya yetkilendirdiği kişinin, ilgili kişilere; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, kişisel veri toplamanın yöntemi ve hukuki sebebi ve 11 inci maddede sayılan diğer hakları konusunda bilgi vermekle yükümlü olduğunun belirtildiği,

- Kanun'un "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12'nci maddesinin (1) numaralı fıkrasının ise; veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri almakla yükümlü olduğu hükmünü içerdiği,

- Öte yandan, bir internet sitesinin düzgün çalışması için zorunlu çerezler vasıtasıyla kişisel verilerin işlenmesinde kişilerin açık rızasına gerek duyulmayacak iken; reklam, pazarlama ve performans amacıyla çalışan çerezlerin kullanılmasının ilgili kişinin açık rızasına tabi olduğu, “kesinlikle gerekli çerezler”in internet sitesinin düzgün çalışması için gerekli çerezler olduğu, ilgili kişinin açık rızası olmaksızın Kanun’un 5’inci maddesinin (2) numaralı fıkrasında ve Kanun’un 6’ncı maddesinin (3) numaralı fıkrasında yer alan işleme şartlarından birine dayanılarak kişisel veri işleme faaliyeti gerçekleştirilebileceği, “kesinlikle gerekli çerezler” statüsünde olmayan çerezler ile kişisel veri işleme faaliyeti gerçekleştirilmesi ve Kanun’un 5’inci maddesinin (2) numaralı fıkrası ile 6’ncı maddesinin (3) numaralı fıkrasında yer alan işleme şartlarından birinin bulunmaması durumunda ilgili kişinin açık rızasına başvurulması gerektiği, veri sorumlusunun, internet sitesinde ve mobil uygulamalarında yer alan ve sitenin/uygulamanın düzgün çalışmasını sağlayan kesinlikle gerekli çerezler dışında yer alan işlevsel çerezler, performans-analitik çerezler, reklam/pazarlama çerezlerinin çalıştırılmasına ilişkin olarak açık rıza dışında bir veri işleme şartı bulunmuyor ise internet sitesini/mobil uygulamaları ziyaret eden kullanıcılardan internet sitesine/mobil uygulamaya giriş anında ilgili kişilerin iradi aktif hareketiyle söz konusu çerezlerin çalışmasına onay vermesini, dolayısıyla varsayılan ayar olarak çerezlerin çalışmamasını öngören “opt-in” mekanizmasına göre açık rıza alması gerektiği,

- İlgili kişinin iddiaları kapsamında yapılan incelemede sitenin ziyaret edilerek çok sayıda çerezin mevcut olduğunun görüldüğü bu çerçevede herhangi bir aydınlatma yapılmadığı, zorunlu olmayan ve kullanıcı hareketlerini reklam veya istatistik gibi amaçlar için takip eden çerezler için veri sorumlusu tarafından açık rıza alma yoluna gidilmediğinin tespit edildiği,

- Ayrıca veri sorumlusunun bahse konu internet sayfasında işlemekte olduğu çerez verilerine yönelik olarak kullanıcıların siteye ilk ziyareti sırasında Kanun’un 10’uncu maddesi uyarınca aydınlatma yükümlülüğünü yerine getirmesi gerektiği, sitede yer alan üyelik formu sayfasına KVKK Aydınlatma Metninin eklendiği ve link bağlantısı ile site ziyaretçilerine sunulduğu ancak metnin Kanun’da ve Tebliğde yer alan zorunlu unsurları taşımadığı ve kullanıcı verilerinin yurt dışına aktarıldığı

değerlendirmelerinden hareketle;

- Veri sorumlusu tarafından internet sayfasında herhangi bir işleme şartına dayanmadan reklam ve pazarlama amacı gibi zorunlu olmayan çerezler vasıtasıyla kişisel veri işlendiği, bu durumun ise Kanun’un 12’nci maddesinin (1) numaralı fıkrasında yer alan yükümlülüklerle aykırılık teşkil ettiği

dikkate alındığında veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 300.000 TL idari para cezası uygulanmasına,

- Sitede çerezlerle işlenen kişisel veriler bakımından Kanun'un 10'uncu maddesi ile Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in ilgili hükümlerine uygun biçimde ilgili kişilere yönelik aydınlatma yükümlülüğünün yerine getirilmesi ve sonucundan Kurula bilgi vermesi yönünde veri sorumlusunun talimatlandırılmasına,
- Kullanıcılara sunulan kayıt formunun doldurulması sırasında işlenen kişisel verilerle ilgili olarak sitede aydınlatma metninin sunulmakta olduğu anlaşılmış olmakla birlikte söz konusu aydınlatma metninde tespit edilen eksikliklerin Kanun'un 10'uncu maddesi ile Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in ilgili hükümlerine uygun biçimde düzenlenerek sonucundan Kurula bilgi vermesi yönünde veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2022/1357 sayılı KVKK Kararı

Spor salonu işletmecisi olan veri sorumlusunun, özel nitelikli kişisel veri niteliğini haiz kan grubu verisini ilgili kişinin açık rızasını almaksızın işlemesi hakkında Kişisel Verileri Koruma Kurulunun 23/12/2022 tarih ve 2022/1357 sayılı Karar Özeti

Karar Tarihi : 23/12/2022

Karar No : 2022/1357

Konu Özeti: Spor salonu işletmecisi olan veri sorumlusunun, özel nitelikli kişisel veri niteliğini haiz kan grubu verisini ilgili kişinin açık rızasını almaksızın işlemesi

İlgili kişinin Kuruma intikal eden şikâyetinde özetle; bir spor salonunun işletmecisi olan veri sorumlusunun spor salonundan hizmet alan kişilerin sağlık verilerini (detaylı yağ, kilo ve performans ölçümü, kan grubu, yıllık hastane ziyaret sayısı, içilen sigara bilgisi vb.), biyometrik verilerini (salona girişte alınan parmak izi) ve kamera görüntülerini işlediği ancak bu verilerle ilgili olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında aydınlatma yapılmadığı ve kişilerin açık rızalarının alınmadığı, ilgili kişinin kişisel verilerinin işlenmesine ilişkin soru ve taleplerini içeren e-postanın veri sorumlusu tarafından yasal süre içerisinde cevaplandırılmadığı, ilgili kişilere ait kişisel verileri içeren kartlara spor salonunda görevli herkesçe erişilebildiği ve bu bilgilerin güvenliğinin sağlanmadığı, sağlık verilerinin de aralarında bulunduğu bu kartların zaman zaman kaybolduğu ve kimlerin eline geçtiğinin belirsiz olduğu, spor salonu görevlilerinin kamera kayıtlarını izlediği ve ilgili kişilerin salon içerisindeki davranışlarıyla bu kayıtların eşleştirilmesi suretiyle yorum yapılabildiği belirtilerek veri sorumlusu hakkında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- İlgili kişinin iddialarının asılsız olduğu ve spor salonunda uygulanan COVID-19 tedbirlerine uymamak amacıyla şikâyette bulunduğu,
- İlgili kişinin spor salonunda hizmet almak üzere üyelik sözleşmesi imzaladığı ve bu sözleşmede yer alan kişisel verileri dışında başka verisinin işlenmediği,

- Üyelik sözleşmesinin ilk sayfasında yer alan “SMS pazarlama faaliyetlerini istiyorum” kısmına, ilgili kişinin “Okudum, anladım, onaylıyorum” şeklinde imzalı onay verdiği ve bu suretle söz konusu verilerin işlenmesinin kendisi tarafından da kabul edilmiş olduğu,
- Spor salonu üyelerinin kendi talepleri olmadıkça boy ve kilo gibi verilerinin alınmadığı, nitekim sözleşmede “anılan spor salonunun üyelere yönelik bir kilo kaybetme, kilo artışı veya sağlığının iyileştirilmesi gibi konularda herhangi bir yazılı veya sözlü taahhüdü bulunmamaktadır.” ibaresinin yer aldığı,
- Dolayısıyla veri sorumlusunun, üyelerin kilo ve boy gibi verilerini kaydetmediği, zira bu hususlarda bir yükümlülüğünün bulunmadığı, aksi bir durumun yalnızca üyenin talebi ve rızası ile mümkün olduğu ancak somut olayda ilgili kişiye ait bu nitelikte bir veri girişinin bulunmadığı ifade edilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulunun (Kurul) 23/12/2022 tarih ve 2022/1357 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun “Kişisel Verilerin İşlenme Şartları” başlıklı 5’inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi; fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin kendisi tarafından alenileştirilmiş olması; bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hükmünün yer aldığı,
- Kanun’un “Özel Nitelikli Kişisel Verilerin İşlenme Şartları” başlıklı 6’ncı maddesinin (2) numaralı fıkrasında özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğunun; (3) numaralı fıkrasında ise, birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel verilerin, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebileceğinin; sağlık ve cinsel hayata ilişkin kişisel verilerin ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis,

tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceğinin düzenlendiği,

- Kanun'un 10'uncu maddesinin (1) numaralı fıkrasında kişisel verilerin elde edilmesi sırasında veri sorumlusunun veya yetkilendirdiği kişinin, ilgili kişilere; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabilirliği, kişisel veri toplamanın yöntemi ve hukuki sebebi ile 11'inci maddede sayılan diğer haklar konusunda bilgi vermekle yükümlü olduğunun düzenlendiği,

- Kanun'un 12'nci maddesinin (1) numaralı fıkrası gereğince veri sorumlusunun; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğunun hükme bağlandığı,

- İlgili kişinin şikayetinde, üyeliği kapsamında özel nitelikli kişisel verileri dahil olmak üzere veri sorumlusu tarafından işlenen diğer kişisel verilerine yönelik Kanun'un 10'uncu maddesi kapsamında aydınlatmada bulunulmadığı ve sağlık verileri ile biyometrik veriler için de açık rıza alınmadığını iddia ettiği, ilgili kişi tarafından şikâyete ek olarak üyelik sözleşmesinin bazı sayfalarının bir örneğinin de Kuruma sunulduğu, bu çerçevede şikâyete konu olaydaki sözleşme incelendiğinde, işlenen kişisel verilere ilişkin herhangi bir aydınlatmanın yer almadığının görüldüğü, bu çerçevede Kanun'un 10'uncu maddesinde yer verilen yükümlülüğün yerine getirilmesi amacıyla üyelik sözleşmesi kapsamında işlenen kişisel veriler için sözleşme metninden ayrı olarak aydınlatma metninin veri sorumlusunca sunulması gerektiği,

- Diğer yandan sözleşmenin ilk sayfasında ilgili kişinin kimlik verilerinin yanı sıra sağlık verisi olan kan grubu bilgisinin de yer aldığı, özel nitelikli kişisel veri olarak sağlık verisi kategorisinde yer alan kan grubu bilgisinin spor salonu tarafından işlenmesi Kanun'un 6'ncı maddesinin (2) numaralı fıkrası uyarınca ilgili kişilerin açık rızası ile mümkün olmakla birlikte buna ilişkin bir açık rıza metninin sunulmadığı görüldüğünden veri sorumlusunun Kanun'da yer alan işleme şartına dayanmaksızın kişisel veri işlediğinin anlaşıldığı,

- Veri sorumlusunun savunmasında beyan edildiği üzere, sözleşme metninde yer alan "SMS pazarlama faaliyetlerini istiyorum" kısmına onay verilmesinin ilgili kişi tarafından kişisel verilerinin işlenmesine açık rıza verildiği anlamına gelmediği, bu ifadenin yalnızca pazarlama faaliyetleri kapsamında ilgili kişinin kişisel verisinin işlenmesiyle sınırlı bir beyandan ibaret olduğu, bununla

birlikte ilgili kişilerin tercihlerinin metne yansıtılmasını teminen söz konusu seçenikle birlikte “SMS pazarlama faaliyetlerini istemiyorum” seçeneğinin de üyelik sözleşmesinde sunulması gerektiği,

- Diğer yandan ilgili kişinin, yağ ve kilo performans ölçümleri, hastane ziyaret sıklığı, boy uzunluğu vb. verilerinin yanı sıra salon girişinde biyometrik veri olan parmak izinin alındığına yönelik iddiasını tevsik edememesi nedeniyle bu hususta herhangi bir tespitle bulunulmadığı,

- İlgili kişinin, spor salonu içerisinde üyelere ait bilgi kartlarının herkes tarafından kolayca ulaşılabilir durumda bulunduğu, bu kartların uygun biçimde saklanmadığı ve zaman zaman kaybolduğu, salon içerisindeki güvenlik kamerası görüntülerine yetkisiz kişilerce erişilebildiği ve ilgili kişinin birtakım davranışlarının bu görüntülerle eşleştirildiği yönündeki iddialarına ilişkin tevsik edici bilgi ve belge sunamadığı ve veri sorumlusundan alınan savunmada da bu iddiaların reddedildiği,

- Şikâyet konusu olaya ilişkin olarak ilgili kişi tarafından veri sorumlusuna gönderilen e-postaya herhangi bir cevap verilmediğinin bu anlamda veri sorumlusunun, kendisine yapılan başvuruyu Kanun’un 13’üncü maddesinin (2) numaralı fıkrası kapsamında sonuçlandırma yükümlülüğüne uygun davranmadığının görüldüğü,

değerlendirmelerinden hareketle;

- Spor salonu üyeliği için özel nitelikli kişisel veri niteliğindeki kan grubu verisinin işlendiği ve bu işleme için açık rıza alınmadığı dikkate alındığında Kanun’un 12’nci maddesinin (1) numaralı fıkrasında yer alan yükümlülüklerini yerine getirmeyen veri sorumlusu hakkında, veri sorumlusunca işletilen spor salonunun üyelik sözleşmesi kapsamında çok sayıda üyenin kişisel verilerinin işlendiği, bunlar arasında özel nitelikli kişisel verilerin de bulunmasının kullanıcıların mahremiyeti açısından önemli bir risk arz ettiği, veri sorumlusunca ilgili kişi başvurusunun cevapsız bırakıldığı, ve spor salonu işletmeciliğinin yanı sıra turizm ve otel işletmeciliği ile inşaat taahhüt gibi birçok sektörde faaliyet gösteren veri sorumlusunun ekonomik durumu da dikkate alınarak Kanun’un 18’inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 100.000 TL idari para cezası uygulanmasına,

- Aydınlatma ve açık rıza metinlerinin üyelere sunulan sözleşme metni içerisinde değil ayrıca düzenlenmesi, açık rızanın ilgili kişilere her bir faaliyet açısından onay verme ve vermeme seçeneklerini içerecek şekilde sunulması, aydınlatma metninin Kanun’un 10’uncu maddesinin yanı sıra Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ’in ilgili hükümlerine uygun şekilde düzenlenmesi ve yapılan işlemlerin sonucundan Kurulu bilgilendirmesi hususunda veri sorumlusunun talimatlandırılmasına,

- İlgili kişinin Kanun'un 11'inci maddesi uyarınca bilgi edinme talebinin cevapsız bırakıldığı anlaşıldığından bundan sonra söz konusu olabilecek ilgili kişi başvurularının uygun biçimde cevaplandırılmasında gerekli hassasiyetin gösterilmesi hususunun veri sorumlusuna hatırlatılmasına,

- İlgili kişilere ait bilgi kartlarında yer alan verilerin yanı sıra güvenlik kameraları ile işlenen görsel kayıtların güvenliğinin sağlanmadığı yönündeki şikâyet ile ilgili olarak eldeki mevcut bilgi ve belgeler kapsamında bu şekilde bir veri ihlali yaşandığı yönünde bir tespitle bulunulamamış olup bu hususta yapılacak bir işlem bulunmadığına

karar verilmiştir.

2022/1281 sayılı KVKK Kararı

İcra takibi dolayısıyla veri sorumlusu avukat tarafından borçlunun borç bilgisinin oğlu ile paylaşılması ve kendisi ile borç bilgisi paylaşılan borçlunun oğlunun telefon numarasının bu suretle hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 01/12/2022 tarihli ve 2022/1281 sayılı Karar Özeti

Karar Tarihi : 01/12/2022

Karar No : 2022/1281

Konu Özeti: İcra takibi dolayısıyla veri sorumlusu avukat tarafından borçlunun borç bilgisinin oğlu ile paylaşılması ve kendisi ile borç bilgisi paylaşılan borçlunun oğlunun telefon numarasının bu suretle hukuka aykırı olarak işlenmesi

İlgili kişilerin (borçlu ve oğlu) aynı konuya ilişkin Kuruma intikal eden şikayetlerinde özetle; borçlu hakkında başlatılan icra takibi ile ilgili olarak oğluna ait telefon numarasının veri sorumlusu avukat tarafından defalarca aranarak borca ilişkin bilgi verildiği, borçlunun hukuki işlem ve finansal bilgilerinin açık rızası olmaksızın üçüncü kişi konumundaki oğlu paylaşıldığı, öte yandan kendisi ile borç bilgisi paylaşılan borçlunun oğlunun ise telefon numarasının hukuka aykırı olarak elde edildiği ve kullanıldığı, konu ile ilgili olarak ilgili kişilerin veri sorumlusu avukata yaptıkları başvurunun veri sorumlusunca tebellüğ edilmesine rağmen cevaplandırılmadığı ifade edilerek, 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusu avukattan savunması istenilmiş olup alınan cevabi yazıda özetle;

- Keşidecisinin borçlu baba olduğu bono sebebiyle hakkında başlatılan ve kesinleşen icra takibi neticesinde borçlunun adreslerindeki menkul ve gayrimenkulleri ile üçüncü şahıslardaki hak ve alacaklarının haczi ve haczedilecek taşınır malların muhafaza altına alınması talebiyle icra müdürlüğüne başvurulduğu ve bu talebin kabul edildiği,
- Hukuk bürosunda çalışan bir avukat tarafından belirlenen tarihte haciz ve muhafaza işlemlerinin gerçekleştirilmesi adına haciz mahalli olan adrese gidilerek burada hazır bulunan borçlu ile oğluna

haciz memuru tarafından geliş sebebinin mahalde anlatıldığı, bu hususun haciz tutanakları ile de sabit olduğu,

- Söz konusu işlemler sürerken borçlunun haciz mahallini terk ettiği, sonrasında haciz mahallinde bulunan borçlunun oğlu tarafından “Ben borçlu şirketin yetkilisiyim, borçlu benim misafirim olarak geldi, borçlunun şirketle alâkası yoktur, haczedilen mallar şirkete aittir.” demek suretiyle istihkak iddiasında bulunduğu, haczedilen malların yediemin sıfatıyla kendisine bırakıldığı ve haciz tutanağının imzalandığı,

- Bu suretle borçlunun oğlunun kişisel verilerinin haciz işleminin gerçekleştirildiği tarihte icra memuru tarafından işlendiği, iddia edilenin aksine borçlunun borcu hakkında oğluna bilgi verilmediği, iki tarafın da hâlihazırda konudan haberdar oldukları,

- İlgili kişilerin veri sorumlusuna usulüne uygun başvuruda bulunmadıkları, borçlunun başvurusunda yer alan vekaletnamede kişisel verilerin korunması çerçevesinde veri sorumlusuna başvurulabilmesi için gerekli açık rızayı içeren özel bir hükmün bulunmadığı, borçlunun oğlunun başvurusunun ise başvuruda bulunan vekil ile vekaletnamede yer alan vekilin farklı olması nedeniyle usulsüz olduğu

ifade edilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulunun (Kurul) 01/12/2022 tarih ve 2022/1281 sayılı Kararı ile;

- Kanun’un “Kişisel verilerin işleme şartları” başlıklı 5’inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işleminin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanun'un "Veri güvenliğine ilişkin yükümlülükler"i düzenleyen 12'nci maddesinin (1) numaralı fıkrası uyarınca veri sorumlularının; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik her türlü teknik ve idarî tedbiri almakla mesul tutulduğu,
- Kanun'un "Veri sorumlusuna başvuru" başlığını hâiz 13'üncü maddesinin (1) numaralı fıkrasının, "İlgili kişi, bu Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir" hükmünü hâvî olmakla birlikte, anılan maddeye dayanılarak hazırlanan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in (Tebliğ) 5'inci maddesinin (1) numaralı fıkrasında, ilgili kişinin Kanun'un 11'inci maddesinde belirtilen hakları kapsamında taleplerini, yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna ileteceği, (2) numaralı fıkrasında, başvurularda; ad, soyad ve başvuru yazılı ise imza, Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyuşu, pasaport numarası veya varsa kimlik numarası, tebligata esas yerleşim yeri veya iş yeri adresi, varsa bildirim esas elektronik posta adresi, telefon ve faks numarası ile talep konusunun bulunmasının zorunlu olduğu, (3) numaralı fıkrasında ise konuya ilişkin bilgi ve belgelerin başvuruya ekleneceği hususlarının belirtildiği,
- Bahse konu Tebliğ'in "Başvuruya cevap" başlıklı 6'ncı maddesinde veri sorumlusunun, Tebliğ kapsamında ilgili kişi tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlü olduğunun hükme bağlandığı,
- Somut olayda veri sorumlusunun Kuruma ulaştırdığı belgeler arasında yer alan "Haciz Tutanağı"nda; borçlu ve oğlunun haciz mahallinde olduğu ve konuya ilişkin olarak haciz memuru tarafından kendisine bilgilendirmelerde bulunulduğu hususlarının kayıt altına alındığı, ayrıca söz konusu tutanakta "Yediemin" sıfatıyla oğlunun da imzasının yer aldığı, ilgili kişilerin Kuruma intikal ettirdiği şikâyet dilekçelerinin eklerinde yer alan arama kayıtlarının tarihlerinin ise haciz işleminin gerçekleştirildiği tarihten sonraki günlere ait olduğunun görüldüğü,
- Şu hâlde, veri sorumlusunun yaptığı aramalar sonrasında ilgili kişiler konumundaki oğlunun, babasına ait borç bilgisini ilk defa bu aramalar ile öğrenmesinin mümkün olmadığı, zira bu

aramalardan önce tanzim edilmiş olan haciz tutanağında kendisinin imzası bulunduğu, borçlunun oğlunun konuya hâlihazırda vakıf olup şikâyet konusu olan kişisel verinin, alenileştiği, aleni verinin ise alenileştirildiği kişiler bakımından gizliliğinin düşünülmemeyeceği,

- Borçlunun oğlunun da haciz tutanağına imza atmakla haciz işleminin bir tarafı hâline geldiği, birtakım hacizli mallar üzerine yediemin olarak tayin edildiği ve yetkilisi olduğunu iddia ettiği şirket adına söz konusu mallar üzerinde istihkak iddiasında bulunduğu, bu çerçevede Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (e) bendi uyarınca "Bir hakkın tesisi, kullanılması veya korunması için veri işleminin zorunlu olması" şartına dayanılarak, örneğin üzerine yediemin olarak tayin edildiği hacizli malların durumu vb. hakkında bilgi almak ve yürütülen hukuki işlemler hakkında kendisine bilgi vermek amacıyla kişisel verisi hüviyetinde olan şahsî cep telefonu numarasının, veri sorumlusu avukat tarafından, borçlunun oğlunun açık rızası olmaksızın, söz konusu amaçla sınırlı ve kısıtlı olmak üzere işlenebileceği, zira somut olayda alacaklı tarafın hak ve menfaatlerinin korunmasının, oğlunun üzerine yediemin bırakıldığı hacizli malların durumu ve bu konu hakkında kendisi ile irtibat kurulabilmesi ile yakından irtibatlı olduğu,

- Öte yandan borçlunun oğlunun cep telefonu numarasının veri sorumlusu tarafından hukuka aykırı bir şekilde elde edildiğine ilişkin Kuruma herhangi bir belge iletilmediği, yapılan inceleme sürecinde de böyle bir tespit bulunamadığı, veri sorumlusu tarafından borçlunun oğlunun kişisel verisi olan cep telefonu numarasının, aradaki hukuki ihtilafa ilişkin hususlarla sınırlı olmak üzere işlenmesinin hukuka aykırı olmadığı,

- Borçlunun oğlunun başvurusunda başvuruda bulunan vekil ile vekaletnamede yer alan vekilin farklı olması ve taraflar arasında düzenlenen bir yetki belgesi de veri sorumlusuna ya da Kuruma iletilmemiş olduğundan, söz konusu başvurunun yanıtlanmamasının hukuka aykırılık teşkil etmediği, bununla birlikte, ilgili kişinin başvurusunda yer alan vekaletnamede kişisel verilere ilişkin özel yetki yer almamasının, söz konusu taleplerin yanıtlanmaması noktasında bir engel teşkil etmediği

değerlendirmelerinden hareketle;

- Borçlunun oğlunun haciz esnasında haciz mahallinde olduğu ve haczedilen malların yediemin sıfatıyla kendisine bırakılmış olduğu da dikkate alındığında, eldeki mevcut bilgi ve belgelerden veri sorumlusunun borçlunun oğlunun telefon numarasını hukuka aykırı işlediğinin tevsik edilemediği anlaşıldığından söz konusu iddia hakkında Kanun kapsamında yapılacak bir işlem olmadığına,

- Veri sorumlusunun Kuruma iletteđi belgelerden, borçlunun ođlunun da söz konusu borcun hacizle tahsili sırasında haciz mahallinde bulunduđu ve Haciz Tutanađını imzaladıđı, dolayısıyla babasının borcu hakkında hâlihazırda bilgi sahibi olduđu, Őikâyet konusu aramalara dair kayıtların ise anılan Haciz Tutanađının tanzim edildiđi tarihin ertesi gününe ait olduđu, bu nedenlerle borçlunun “aynı zamanda da kişisel verisi olan, kendisinin borçlu olduđuna dair bilginin veri sorumlusu tarafından ođluna iletilmesi” Őeklindeki Őikâyetine iliŐkin olarak Kanun kapsamında tesis edilebilecek bir iŐlem olmadığına,

- Veri sorumlusunun kendisine Kanun ve Tebliđ kapsamında, vekilleri aracılıđıyla baŐvuruda bulunan ilgili kişilerden yasal bir mecburiyet bulunmamasına karŐın “kiŐisel verilere iliŐkin özel yetki” talep ettiđi, bu durumun ilgili kişilerin veri sorumlusuna baŐvuru yapmasını Tebliđ’in 5 ve 6’ncı maddeleri hükümlerine aykırı olarak zorlaŐtırdıđı dikkate alındıđında kendisine yapılacak baŐvuruları sonuçlandırma noktasında azami dikkat ve özeni göstererek ilgili kişilerin bizzat kendileri veya vekilleri aracılıđı ile yaptıkları baŐvuruları Kanun ya da Tebliđ’de bulunmayan, ayrıca herhangi bir yasal mesnede de dayanmayan ek külfetler getirmek suretiyle zorlaŐtırmamasına yönelik gerekli tedbirlerin alınması konusunda veri sorumlusunun uyarılmasına

karar verilmiŐtir.

2022/1249 sayılı KVKK Kararı

İlgili kişinin döviz bürosundaki güvenlik kamerası ile kayıt altına alınmış görüntülerinin haber ajansları ile paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 24/11/2022 tarihli ve 2022/1249 sayılı Karar Özeti

Karar Tarihi : 24/11/2022

Karar No : 2022/1249

Konu Özeti: İlgili kişinin döviz bürosundaki güvenlik kamerası ile kayıt altına alınmış görüntülerinin haber ajansları ile paylaşılması

İlgili kişinin şikâyetinde özetle;

- Veri sorumlusuna ait döviz bürosunda gişe görevlisi tarafından yapılan yanlış işlem sebebiyle ilgili kişiye fazla ödeme yapıldığı, fazla ödemenin ilgili kişi tarafından öğrenilmesi üzerine fazla ödenen kısmın iade edildiği, bununla birlikte döviz bürosunda bulunan güvenlik kamerası ile kayda alınmış ilgili kişiye ait görüntülerin haber ajans ve siteleri ile ilgili kişinin açık rızası alınmaksızın paylaşıldığı, Bahsi geçen haber sitelerinde ilgili kişinin görüntülerinin paylaşılması sebebiyle ilgili kişi hakkında rencide edici yorumların yapıldığı ve bu durumun ilgili kişinin manevi anlamda yıpranmasına sebep olduğu,
- Veri sorumlusunun iş yerinde görüntü kaydı yapıldığına ilişkin herhangi bir uyarı levhasının bulunmadığı,
- İlgili kişi tarafından 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 11'inci maddesindeki hakları uyarınca veri sorumlusuna yazılı şekilde başvuruda bulunulduğu ancak başvuru dilekçesindeki hususlara makul ve yeterli cevap verilmediği ve ihlal durumunun veri sorumlusunca reddedildiği

belirtilmiş ve gerekli işlemlerin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusunun savunması talep edilmiş olup veri sorumlusunun cevabi yazısında özetle;

- Kuruma yapılan başvurunun haksız ve mesnetsiz olduğu, veri sorumlusunca ilgili kişinin başvurusunun somut delillerle ve ilgili olaya ilişkin haber kayıtları, kamera kayıtları, kamera uyarı levhalarını gösteren fotoğraflarla birlikte tek tek ayrıntılı bir şekilde cevaplandırıldığı, buna rağmen ilgili kişi tarafından makul ve yeterli cevap bulunmadığı beyan edilerek Kuruma başvurulmasının anlamlandırılmadığı,
- İlgili kişinin veri sorumlusuna ait döviz bürosuna giderek döviz cinsinden para bozdurmak istediği ancak getirilen paraların rulo şeklinde ve buruşmuş olması sebebiyle para makinesinin para tutarını belirlerken yanıldığı ve vezne görevlisinin ekrandaki tutarı ilgili kişiye verdiği,
- Döviz bürosunda gün sonunda rutin olarak yapılan kasa sayımında para açığı olduğunun fark edildiği ve kamera kayıtlarının incelemesi neticesinde hatalı işlemin ve bu işlemin gerçekleştirildiği müşterinin tespit edildiği, bu tür hatalı işlemlerde sorumluluğun veznedarda olduğu ve kasa açığının veznedarın hesabına yazılıp siciline işlendiği,
- Fazla para ödenen ilgili kişinin fazla ödenen parayı veri sorumlusuna iade etmesinin beklendiği ancak makul süre geçmesine rağmen paranın iade edilmediği,
- Olayın gerçekleşmesinden bir gün sonra uluslararası yayın yapan bir televizyon kanalının her hafta rutin olarak gerçekleştirdiği ekonomi yorumu çekimi için döviz bürosuna geldiği, yayın yapılması esnasında bir önceki gün gerçekleştirilen hatalı işlemin gündeme geldiği, veznedarın kendi sorumluluğunun doğduğunu bildiği, paranın makul süre içerisinde iade edilmemesi nedeniyle yapılan hatalı işlemin ilgili kişi tarafından aslında kasten yapılmış olabileceği ihtimalinin de bulunduğu, bu durumda suç soruşturmasına neden olabileceği için savcılığa başvurmadan önce eğer ilgili kişi iyi niyetliyse iş savcılığa intikal etmeden bu sorunu çözmek istediği ancak müşteri ile irtibata geçebileceği isim-adres-telefon vb. bilgiler vasıtasıyla müşteriye başka türlü ulaşma imkanı bulunmadığı için ilgili kişinin kendileriyle irtibata geçebilmesi için müşterinin sadece şahsının kendisini tanıyabileceği, ilgili kişinin yalnızca göz çevresinin görüldüğü, görüntülerin kanala verildiği,
- İlgili kişinin kişisel verisi sayılabilecek nitelikte bir bilgisinin basına verilmediği, ekranda gösterilen videonun ilgili kişinin tanınabileceği bir kayıt olmadığı, söz konusu yayınlar yapıldıktan sonra ilgili kişinin yurtdışında bulunan kızının yayını izlediği ve annesine durumu ilettiği bu sayede veri sorumlusu ile iletişime geçtiği, ilgili kişinin Düzeltme/Teşekkür haberinin yapıldığı yayın esnasında bu durumu “kızım haber verdi geldim yoksa haberim olmazdı” şeklinde kendisinin açıkça beyan ettiği, ilan verilmeseydi ilgili kişinin veri sorumlusuna ulaşmayacağını anlaşıldığı, bu durumda eksik kalan para bedelinin veznedardan tahsil edileceği ve siciline işleyeceği, asgari ücretle hayatını

idame ettiren veznedarın ekonomik anlamda mahvına sebep olacak durumun korku ve paniği ile bu görüntüyü verirken kişiyi rencide etme ve aşağılama gibi bir düşüncesinin bulunmadığı yalnızca kişiye ulaşma ve fazla parayı geri alma amaç ve iyi niyetiyle verildiği, bu yönüyle incelendiği zaman ilgili olayın Kanunlarımızda hukuka uygunluk nedeni olarak düzenlenen daha üstün nitelikli kamusal veya özel yarar durumunu oluşturduğu,

- Veri sorumlusu tarafından konunun haber yapılması için kasten girişimde bulunulmadığı, haberi yayınlayan diğer basın organlarının haber içeriğini kopyalamak suretiyle veri sorumlusunun bilgisi ve kontrolü dışında yayın yaptıkları, haber içeriğinde şahsı rencide edici, küçük düşürücü hiçbir kelimenin kullanılmadığı, diğer internet sitelerinde haberin altına yapılan yorumların ise veri sorumlusunun kontrolü altında tutabileceği bir durum olmadığı, diğer internet sitelerince yapılan haberlerin veri sorumlusunun bilgisi dahilinde olmadığı, bu nedenle de usulsüz şekilde haberi yapan ve bu haberlere yorum yapan kişilerin cezai sorumluluklarının sadece kendilerini bağladığı, veri sorumlusuna bir kusur atfedilemeyeceği,

- Veznedarın bilgisi dâhilinde olan haber içeriğinin ilgili kişiye ulaşmak amacıyla ilan niteliğinde olduğu, haberin içerisinde kişilik haklarını zedeleyecek yahut taraflarca kötü bir anlam yüklenecek içeriğin oluşturulmadığı, döviz bozdurma işlemi sırasında müşterilerin adı ve soyadı ile işlem yapılmadığından ilgili kişiye doğrudan doğruya başvurulamayacağı ve başka şekilde ilgili kişiye ulaşma imkanının bulunmaması sebebiyle söz konusu olayda ilgili kişinin ismi verilerek değil tanıyanların kendisine iletmesi ve bu kişinin geri dönüşünün sağlanması için sadece gözleri belli olan video kaydının kullanıldığı, ses veya başkaca herhangi bir kişisel veri niteliği taşıyan hiçbir unsurun basın veya haber kuruluşuyla paylaşılmadığı,

- Olayın yerel basına yansımalarının akabinde ilgili kişinin karşı komşusu ile birlikte büroya geldiği, durumun kendisine kızı tarafından haber verildiğini ve eğer parayı getirmese veri sorumlusunun kendisini zor bulacağını beyan ettiği, her ne kadar ilgili kişiyi tanıyanların veri sorumlusuna başvurması için ilan niteliğinde bir yayın yapılsa da ilgili görüntülerde maske takıldığı ve ilgili kişinin gözlerinden başka hiçbir uzvu veya kendisinin tanınmasına yardımcı olacak bir özelliği belli olmadığı için başkaları tarafından tanınmasının imkansız olduğu, ilgili kişinin yayınlanan haberde siyah eşarp ve maske taktığı, kişinin yalnızca gözlerinin açıkta olduğu, adı/soyadı/herhangi bir spesifik özellik veya verisi verilmeyen ilgili kişinin yalnızca gözlerinden tanınmasının hayatın olağan akışına ters olduğu, mantık sınırları içerisinde olmadığı, zaten ilgili kişiyi bu haliyle tanıyan tek kişinin de birinci derece yakını olan kızından başkası olmadığı,

- İlgili kişinin fazla parayı, veri sorumlusuna hatalı işlemin tesis edildiği ve kendisinin parayı bankaya yatırdığı gün veya işlem gerçekleştikten sonraki üç gün içerisinde geri ödemediği, bu davranışlar bir bütün olarak ele alındığında ilgili kişinin gerçekleştirdiği davranışın açıkça kişinin gerçek niyetinin aslında paranın geri ödenmemesi yönünde olduğunun, makul ve dürüst bir insandan beklenebilecek bir davranış olmadığına göstergesi olduğu, eğer ki haber yapılmıyaydı ilgili kişinin döviz bürosuna gelerek hatalı işlemin düzeltilmesini hiçbir zaman talep etmeyeceği ve kişi zaten yurt dışında yaşadığı için kendisine ulaşamayacağı,
- Veri sorumlusunun ilgili kişiye teşekkür etmek için ilgili haberi yapan TV kanalına haber verdiği ve kanalın paranın iadesinin yapıldığına dair düzeltme niteliğinde haber yaptığı, veri sorumlusunun haber içeriğinde ilgili kişiyi rencide edecek nitelikte hiçbir imada bulunulmasa da güzel bir davranış gerçekleştirdiği ve durumun kamuoyu tarafından da öğrenilmesi için bir nevi teşekkür mahiyetinde ilgili kişinin iznini alarak TV kanalını aradığı, paranın geri getirildiği haberinin yapılmasını istediği, yayın yapılacağından ilgili kişinin haberdar olduğu, veri sorumlusunca teklif yapıldığında ilgili kişi tarafından hemen kabul edildiği, hatta haber ekiplerinin kayıta olduğu sırada parayı veznedara teslim ettiği, sonrasında kameranın önüne geçerek kendi hür iradesiyle röportaj verdiği, ilgili kişinin adının ve soyadının veri sorumlusunca açıklanmadığı, ilgili kişinin bu bilgileri röportaj esnasında özgür iradesiyle verdiği, ilgili kişinin isminin teşekkür haberinin yapıldığı sırada öğrenildiği,
- Tüm işlemlerin tamamlanmasını müteakip tarafların iyi bir şekilde ayrıldıkları ancak sonrasında ilgili kişinin birçok davranışının şüpheli ve tutarsız olduğu,
- Veri sorumlusu tarafından işlenen veri ve kayıtların hukuka uygun olarak kaydedildiği ve saklandığı, veri sorumlusuna ait büronun iki farklı yerinde kamera kaydı yapıldığına dair levhalar bulunduğu, levhaların kişilerin kolayca görebileceği yerlerde bulunduğu, kişilerin bu iş yerine girdikleri zaman kayıtlarının yapılmasını kabul ettiklerine karine teşkil etmesi sebebiyle hukuka uygunluk nedeni oluşturduğu, veri sorumlusunca tutulan, kayıt altına alınan ve saklanan kamera kayıtlarının hukuka uygun, hatta ilgili yasa ve mevzuat gereği zorunlu olduğu, nitekim döviz bürolarının Hazine ve Maliye Bakanlığına bağlı kurumlar olması sebebiyle iş ve işlemlerinin Bakanlığın denetimi altında gerçekleştirildiği, döviz bürolarının istenildiği zaman canlı izlendiği, döviz bürolarında kamera bulundurulmasının zorunlu olduğu, kamera takılmaması ve kamera kayıtlarının saklanmamasının ise döviz bürosunun kapatılması yaptırımına bağlandığı,
- Veri sorumlusu tarafından Kanun'un 10'uncu maddesine uygun olarak büronun kamera ile izlendiğine dair herkesin rahatlıkla görebileceği yerlerde bulunan uyarı levhaları ile aydınlatıldığı ve kamera ile izleme faaliyetine ilişkin birden fazla yöntem ile bildiride bulunulduğu, böylelikle ilgili

kişilerin temel hak ve özgürlüklerine zarar verilmesinin engellendiği, şeffaflığın ve ilgili kişilerin aydınlatılmasının hedeflendiği, ilgili kişinin de büroda kendisine ödeme yapılırken kameraya uzun süre baktığı, bu nedenle ilgili kişinin büroda kamera bulunduğunun farkında olduğu, bu kameraların tam alt kısmında kamera ile kayıt yapıldığına dair uyarı levhasının bulunduğu, güvenlik amacıyla kamera ile izleme faaliyetinin yürütülmesinde Kanun'da yer alan düzenlemelere uygun hareket edildiği, döviz bürosunun bina ve tesislerinde ilgililerin haklarının zedelenmemesi amacıyla yürürlükte bulunan ilgili mevzuatta öngörülen amaçlarla ve Kanun'da sayılan kişisel veri işleme şartlarına uygun olarak güvenlik kamerasıyla izleme faaliyetinde bulunulduğu, güvenlik kamerasıyla kişilerin görüntülerinin kayda alınmasıyla ilgili Anayasal düzenleme esas alındığında güvenlik kamerasıyla yapılan kayıtların kanunilik, ölçülülük ve maddede sayılmış olan bir ya da daha fazla amaç bakımından demokratik bir toplumda gerekli olması koşullarına uygun olduğu sürece bu kayıtların hukuka uygun olarak kaydedildiğinin kabul edildiği,

- Olayda Kanun'da belirtilen hukuka uygunluk sebeplerinin mevcut olduğu, döviz bürosunun Kanun'un 4'üncü maddesine uygun olarak kişisel verileri amaçla bağlantılı, sınırlı ve ölçülü bir biçimde işlediği, veri sorumlusunun güvenlik kamerasıyla izleme faaliyetinin sürdürülmesindeki amacın bu Kanun maddesinde sayılan amaçlarla sınırlı olarak ve bu doğrultuda, güvenlik kameralarının izleme alanları, sayısı ve ne zaman izleme yapılacağına güvenlik amacına ulaşmak için yeterli ve bu amaçla sınırlı olarak uygulanmaya alındığı, kişisel verilerin işlenmesiyle ilgili Avrupa İnsan Hakları Mahkemesi içtihatlarına bakıldığında mahkemenin özel hayata ait beklentilerin zayıf olduğu kamusal alanda kişinin sadece kayda alınmasının özel hayata müdahale olmadığını ifade edildiği,

- Kanun'un 5'inci maddesinde sayılan birden çok fıkranın büronun ilgili verileri işlemesini hukuka uygun hale getirdiği, Türk Parası Kıymetini Koruma Hakkında 32 Sayılı Karara İlişkin Tebliğ'in 26'ncı maddesi gereği döviz bürolarında kamera bulundurulmasının zorunlu olduğu, bu durumun kişisel veri işlemenin kanunlarda açıkça öngörülmesi, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması hükmü ile birebir örtüştüğü ayrıca veri sorumlusunun döviz bürosu olduğu ve yapılan işin önemi göz önünde bulundurulduğunda geri dönülmez zararlar olabileceği için bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması hükmü çerçevesinde veri sorumlusunca hukuka aykırı olarak herhangi bir veri kaydı yapılmadığının, tutulmadığının ve saklanmadığının görüleceği,

- Kanun'un hangi durumlarda kişisel verilerin aktarımı yapılabileceğini düzenlediği 8'inci maddesi uyarınca Kanun'un 6'ncı maddesinde zikredilen hususlar arasında biyometrik verilerin

işlenebileceğine ve aktarılabileceğine de yer verildiği, ayrıca Kanun'un 28'inci maddesinin (2) numaralı fıkrası gereğince suç işlenmesinin önlenmesi veya suç soruşturması için zorunlu olması durumunda bu verilerin aktarılabileceğinin düzenlendiği,

- İlgili kişinin hal ve hareketleri bir bütün olarak değerlendirildiğinde suç işlemiş olabileceği kanaatinin oluştuğu, toplumda makul, orta zekalı bir birey tarafından yorumlandığında da bu durumun bu şekilde yorumlanabileceği, bu nedenlerle ilgili kişinin kişisel verilerinin işlenmesinde hukuka aykırı hiçbir usulün izlenmediği, her şeyin usul ve kanuna uygun gerçekleştirildiği, ilgili kişinin bu olayda herhangi bir zararı olmadığı gibi bürodaki veznedarın bir yıllık maaşıyla ödenebilecek bir zararın kapatıldığı, bu durumun ilgili kişinin gönüllü olarak verdiği röportaj kapsamında TV'de yayınlandığı, açıklanan tüm bu nedenlerle ilgili kişinin görüntülerinin hukuka aykırı bir amaç güdülerek veyahut kişilik haklarına zarar verecek biçimde herhangi bir kurum/kuruluşa veya basın/yayın organına verilmediği, tüm kayıtların hukuka uygun şekilde tutulduğu ve işlemlerin bu doğrultuda tesis edildiği

bildirilmiştir.

Konuya ilişkin yapılan inceleme neticesinde, Kişisel Verileri Koruma Kurulunun 24/11/2022 tarihli ve 2022/1249 sayılı Kararı ile;

- Kanun'un 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, "belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza", (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi"

olarak tanımlandığı,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi; fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı

veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin kendisi tarafından alenileştirilmiş olması; bir hakkın tesisi, kullanılması veya korunması için veri işleniminin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hükmünün yer aldığı,

- Kanun'un "Kişisel Verilerin Aktarılması" başlıklı 8'inci maddesinde ise "(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz. (2) Kişisel veriler; a) 5 inci maddenin ikinci fıkrasında, b) Yeterli önlemler alınmak kaydıyla 6'ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir. (3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır." hükmüne yer verildiği

Bu çerçevede;

İlgili kişinin "veri sorumlusunun aydınlatma yükümlülüğünü yerine getirmediği" yönündeki şikâyeti ile ilgili olarak;

- İlgili kişinin görüntü kaydının alınması şeklindeki veri işleme faaliyetinin gerçekleştiği dönemde yürürlükte bulunan Tebliğ'in (Tebliğ No:2018-32/45) amir 26'ncı maddesinin incelenmesinden "Yetkili müesseseler işlem yapılan her bir vezne, para makinesi ile işlem yapan kişileri gösterecek şekilde yeterli sayıda kamera veya görüntü kayıt sistemini çalışır şekilde kurulu bulundurmak zorundadır." hükmünün yer aldığı görüldüğü, bu itibarla döviz bürolarında kamera bulundurulmasının hukuki bir yükümlülük olduğu, dolayısıyla kamera-video kaydı yapmak suretiyle ilgili kişinin görüntülerinin kaydedilmesinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasında yer alan "Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" işleme şartına dayandığı, öte yandan ilgili kişinin kamera kaydı yapıldığına ilişkin aydınlatma yapılmadığı iddiaları hakkında veri sorumlusunun savunması ekinde iletmış olduğu fotoğrafların incelenmesinden döviz bürosunun muhtelif yerlerinde "Bu iş yeri güvenliğiniz için 7/24 kamera ile izlenmektedir" levhalarının asılı olduğunun görüldüğü ve kamera kaydı yapıldığına ilişkin ilgililerin aydınlatılmasının sağlandığı kanaatinin hasıl olduğu,

İlgili kişinin veri sorumlusunca kamera kaydı neticesinde elde edilen görüntülerinin yerel televizyon kanalına aktarılması şikâyeti ile ilgili olarak;

- Kanun'un 8'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın aktarılamayacağını hükme bağlandığı, aynı maddenin (2) numaralı fıkrasında Kanun'un 5'inci maddesinin (2) numaralı fıkrasında belirtilen şartlardan birinin bulunması hâlinde ilgili kişinin kişisel verilerinin açık rızası aranmaksızın aktarılabilmesinin düzenlendiği,
- İlgili kişi ile irtibata geçilebilecek isim-adres-telefon vb. bir bilginin bulunmaması ve ilgili kişiye başka türlü ulaşma imkanı bulunmadığı için veri sorumlusunca ilgili kişinin sadece göz çevresinin görüldüğü görüntülerin TV kanalına verildiği, ilan verilmeseydi ilgili kişinin veri sorumlusuna ulaşmayacağını anlaşıldığı, bu durumda eksik kalan para bedelinin veznedardan tahsil edileceği ve siciline işleyeceği, asgari ücretle hayatını idame ettiren veznedarın ekonomik anlamda mahvına sebep olacağı, bu yönüyle incelendiği zaman ilgili olayın kanunlarımızda hukuka uygunluk nedeni olarak düzenlenen daha üstün nitelikli kamusal veya özel yarar durumunu oluşturduğu, haber içeriğinin ise ilgili kişiye ulaşmak amacıyla ilan niteliğinde olduğu beyanlarından hareketle somut olayın Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (f) bendinde yer alan ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlemenin zorunlu olması işleme şartı çerçevesinde incelendiği,
- Hükümün uygulanabilmesinin iki aşamalı bir değerlendirme gerektirdiği, ilk değerlendirmede veri sorumlusunun meşru menfaatinin varlığının tespit edilmesinin gerektiği, somut olayda veri sorumlusunun, fazla ödeme yapılan ilgili kişinin tespit edilmesi amacıyla ilgili kişiye ait görüntü kayıtlarını üçüncü kişi/kurumlara aktarması suretiyle gerçekleşen eylemde menfaatinin bulunduğunu "1- İlgili kişiye yapılan fazla-haksız ödemenin iadesinin sağlanması 2- İlgili kişiye ulaşamaması durumunda eksik kalan para bedelinin veznedardan tahsil edilmesi ve siciline işlenmesi sebebiyle veznedarın ekonomik anlamda mahvına sebep olması" şeklinde izah ettiği,
- Söz konusu menfaatler açısından bir değerlendirme yapıldığında; fiilin kasten yapılmış olabileceği şüphesinin mevcut olduğu da göz önünde bulundurulduğunda suç soruşturmasına neden olabileceği için veri sorumlusunca makul ve normal şartlarda beklenen hareket tarzının adli mercilere başvuruda bulunmak şeklinde olduğunun düşünüldüğü, bununla birlikte döviz bozdurma işlemi sırasında müşterilerin adları ve soyadlarıyla işlem yapılmadığından ad-soyad-iletişim bilgisi gibi ilgili kişiye ait herhangi bir kişisel veriye sahip olmadığı ve yapılan fazla/haksız ödemenin iadesinin sağlanmasında tek yol olarak görüldüğü dikkate alındığında söz konusu aktarımın kişinin kendisinin geri dönüşünün sağlanabilmesi adına yararlı olacağı düşüncesiyle ilgili kişiye ait göz çevresinin ve silüetinin görüldüğü görüntülerin, kendinin tanıyabileceği şekilde TV kanalına verilmesinde meşru olarak değerlendirilebilecek bir menfaatin varlığından söz edilebileceği,

- Bununla birlikte veri sorumlusunun elde edeceği faydanın; meşru, ilgili kişinin temel hak ve özgürlüğü ile yarışabilecek düzeyde etkin, belirli ve halihazırda mevcut olan bir menfaatinin ilişkili olması gerektiği, bu kapsamda menfaatin ilgili kişinin temel hak ve özgürlüklerine zarar verip vermeyeceği yönünde yapılan ikinci değerlendirilmede temel hak ve özgürlüklere konu olan kişisel verilerin korunması hakkına, ilgili kişinin şikâyetine ve aktarıma konu olan kamera kaydı görüntüleri incelendiğinde, ilgili kişinin maske takmasından dolayı gözünün, göz çevresinin ve silüetinin görünür olduğu görüntülerin, bir gerçek kişiyle ilişkilendirildiği ve ilgili kişiyi diğer bireylerden ayırmaya ve niteliklerini ortaya koymaya elverişli olduğu için kuşkusuz kişisel veri niteliğini haiz olduğu, buna karşın ilgili kişinin yalnızca göz, göz çevresinin ve silüetinin görünür olduğu görüntülerle ilgili kişiyi tanımlamanın mümkün olmadığı, bu verilerin tek başına ilgili kişiyi belirlemeye imkân sağlayacak nitelikte de olmadığı, kişileri doğrudan değil ama dolaylı yoldan belirlenebilir kılan veriler açısından da kişisel veriden bahsedilmekle birlikte bunların ilgili kişilerin temel hak ve hürriyetleri açısından yaratacağı risklerin daha az olduğundan söz edilebileceği, somut görüntülerin değerlendirilmesinden de ilgili kişinin yalnızca göz, göz çevresi ve silüetinin yer aldığı görüntülerin tek başına ilgili kişiyi belirlemeye imkân sağlayacak nitelikte olmadığından hareketle yukarıda belirtilen menfaatin gerçekleştirilmesinin bahsi geçen görüntülerin aktarılması karşısında yarışabilir nitelikte olduğu,

- Bu itibarla veri sorumlusu tarafından ilgili kişiye yapılan fazla-haksız ödemenin iadesinin sağlanabilmesini ve kaybın önlenmesini teminen ilgili kişinin göz çevresinin ve silüetinin görüntülediği kamera kaydı görüntülerinin ilan amacıyla yerel haber kanalına aktarılmasının, ilgili kişinin temel hak ve hürriyetleri ile yarışabilir nitelikte bir yarar sağladığı ve kişisel veri işlenmeksizin başkaca bir yol ve yöntemle bu yararın elde edilmesinin mümkün olmayacağı,

- Bu çerçevede, meşru menfaatin ortaya koyulmasına ilişkin olarak yukarıda yer verilen kriterler esas alınarak yapılan değerlendirme sonucu; veri sorumlusu tarafından ilgili kişiye yapılan fazla-haksız ödemenin iadesini sağlamak ve ekonomik kaybın önlenmesini teminen ilgili kişinin göz çevresinin ve silüetinin görüntülediği kamera kaydı görüntülerini ilan amacıyla yerel haber kanalına aktarılmasının Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (f) bendine göre, "İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" kapsamında olduğu,

- Öte yandan paranın iadesinin yapıldığına dair düzeltme niteliğinde haber yapıldığı, yayın esnasında ilgili kişinin parayı veznedara teslim ettiği, akabinde açıklamalarda bulunduğu da dikkate alındığında söz konusu şikâyette bulunmada hukuki bir yarar kalmadığı

değerlendirmelerinden hareketle;

- Döviz bürolarında kamera bulundurulmasının hukuki bir yükümlülük olduğu bu itibarla kamera-video kaydı yapmak suretiyle ilgili kişinin görüntülerinin kaydedilmesinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (ç) bendi kapsamında veri sorumlusunun hukuki yükümlülüğünün yerine getirilmesi işleme şartına dayandığı, öte yandan ilgili kişinin kamera kaydı yapıldığına ilişkin aydınlatma yapılmadığı iddialarına ilişkin olarak veri sorumlusunun savunması ve eklerinde iletmiş olduğu fotoğrafların incelenmesinden döviz bürosunun muhtelif yerlerinde "Bu iş yeri güvenliğiniz için 7/24 kamera ile izlenmektedir" levhalarının asılı olduğu görüldüğünden, kamera kaydı yapıldığına ilişkin ilgililerin aydınlatılmasının sağlandığı kanaati hasıl olmuş olup ilgili kişinin söz konusu şikâyeti hakkında Kanun kapsamında yapılacak bir işlem olmadığına,
- Veri sorumlusu tarafından ilgili kişiye yapılan fazla-haksız ödemenin iadesinin sağlanabilmesini ve ekonomik kaybın önlenmesini teminen ilgili kişinin göz çevresinin ve silüetinin görüntülediği kamera kaydı görüntülerinin ilan amacıyla yerel haber kanalına aktarılmasının Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (f) bendine göre, "İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" işleme şartı kapsamında olduğundan hareketle bu hususta Kanun kapsamında yapılacak bir işlem olmadığına

karar verilmiştir.

2022/1201 sayılı KVKK Kararı

İlgili kişinin Resmî Gazete'nin internet sayfasından erişilebilen bir ilana ilişkin olarak arama motorunda adı ve soy adı ile yapılan aramada ulaşılan sonuçların indeksten çıkarılması talebi hakkında Kişisel Verileri Koruma Kurulunun 10/11/2022 tarihli ve 2022/1201 sayılı Karar Özeti

Karar Tarihi : 10/11/2022

Karar No : 2022/1201

Konu Özeti: İlgili kişinin Resmî Gazete'nin internet sayfasından erişilebilen bir ilana ilişkin olarak bir arama motorunda adı ve soy adı ile yaptığı aramada ulaşılan sonuçların indeksten çıkarılması talebi

Kuruma yapılan şikâyette özetle; ilgili kişinin ismi ile veri sorumlusu arama motoru üzerinden arama yapıldığında https://www.resmigazete.gov.tr/arsiv/*****.pdf sayfasına ulaşıldığı, ilgili kişinin ismiyle yapılan arama sonucunda çıkan sayfanın "unutulma hakkı" kapsamında kaldırılmasının veri sorumlusundan talep edildiği, ancak taraflarına verilen yanıtta "içeriğin engellenmemesine" karar verildiğinin bildirildiği hususları beyan edilerek ilgili kişinin ismiyle veri sorumlusu arama motoru üzerinde arama yapıldığında ilgili adresin çıkmamasının sağlanması için gereğinin yapılması talep edilmiştir.

İlgili kişinin şikâyetine istinaden başlatılan inceleme çerçevesinde veri sorumlusunun savunması istenilmiş olup, verilen cevapta özetle;

- https://www.resmigazete.gov.tr/arsiv/*****.pdf uzantılı URL adresine ilişkin olarak ilgili kişinin öncelikle veri sorumlusu tarafından unutulma hakkına dayalı taleplerini iletmek isteyen ilgili kişiler için sağlanan etkili bir kanal olan çevrimiçi form aracılığıyla başvurduğu ve talebinin kayıt altına alındığı,

- Veri sorumlusu tarafından ilgili kişinin talebinin süresi içinde ve Kişisel Verileri Koruma Kurulunun (Kurul) 23/06/2020 tarihli ve 2020/481 sayılı kararında öngörülen kriterler kapsamında değerlendirildiği, ilgili kişinin adının arama sonuçlarından kaldırılmasındaki mahremiyet menfaati ile halkın bilgiye erişim hakkı dahil ifade özgürlüğü arasında denge testi yapıldığı, eldeki olaya ilişkin tüm koşulları değerlendirdikten sonra veri sorumlusunun menfaat dengesinin arama sonuçlarında

kalmasından yana olduđu sonucuna vardığı ve deęerlendirmenin sonucuna iliřkin olarak ilgili kiřiye bilgilendirdiđi,

- Veri sorumlusunun üçüncü kiři internet sayfalarında sunulan beyanların doęruluęunu veya yanlıřlığını deęerlendirmeye uygun bir konumda olmadıđı, dolayısıyla kamu menfaati için önem arz eden ancak halihazırda yanlıř veya hakaretamiz olduđu iddia edilen ifadelerin ele alınması için uygun yöntemin mahkemelerin delilleri deęerlendirmesi ve maddi gerçeklikleri tespit etmesi olduđu, unutulma hakkı konusunda rehber olarak Kurulun 23/06/2020 tarihli ve 2020/481 sayılı kararındaki kriterlerin dikkate alındıđı, bununla birlikte ilgili kiřinin bařvurusuna konu olan URL adresinin bir Resmî Gazete kaydı olduđu ve bir mahkumiyet kararıyla deęil ilgili kiřinin lehine verilen bir beraat kararıyla ilgili olduđu,

- İlgili kiřinin bařvurusuna konu olan https://www.resmigazete.gov.tr/arsiv/****.pdf uzantılı URL adresinin birden çok ilan içeren **/**/2000 tarihli Resmî Gazete'ye iliřkin olduđu, Resmî Gazete'nin **. sayfasında ilgili kiřinin bazı suçlara istinaden yapılan bir yargılamadan beraat ettiđine dair karara iliřkin bir tebliğın yer aldıđı, ayrıca ilgili kiřinin ikametgahının ve iř yeri adresinin tespit edilememesi nedeniyle kararın ilgili kiřiye tebliğ edilemediđinin ve 7201 sayılı Tebligat Kanunu'nun (Tebligat Kanunu) 28, 29 ve 31'inci maddeleri uyarınca kararın Resmî Gazete'de yayımı tarihinden itibaren 15 gün sonra davalıya tebliğ edilmiř sayılacađının belirtildiđi, bu kapsamda söz konusu içeriđin Resmî Gazete'de yayınlanan ve herkesin eriřimine açık bir ilan olduđu, Resmî Gazete'nin mevcut durumda olduđu üzere resmî tebligat veya kiřilerin yokluęunda bir bildirim aracı olduđu gibi belirli durumlarda hukukun uygulanmasının yanı sıra arřiv ve bilgi almanın temel bir aracı olduđu,

- Devlet kayıtlarının devletin kamu yararına olduđunu düřündüđü konular hakkında toplumu bilgilendirmekte çok önemli bir rol oynadıđı ve devletin bilgilerin arama motorları aracılıęıyla halk tarafından eriřilebilir olması gerektiđine dair kararının kendi deęerlendirmelerinde güçlü bir faktör olduđu, söz konusu URL adresinin bir kamu kurumu tarafından hukuki düzenlemeler kapsamında bařlıca görevi kamusal bilgi alınması olan bir internet sitesinde kamuya açıklanmıř ve arama motorlarında eriřilebilir kılınmaya devam eden verilere iliřkin olduđu, söz konusu içeriđin kanun hükmü sebebiyle var olan resmî bir kayıt olduđu ve açıklanacađı üzere kamu kurumu kaynaklarından bilgi alma hakkının temel bir hak olduđu,

- İçeriđin ilgili kanunların emrettiđi řekilde Resmî Gazete'de yayınlanan bir mahkeme kararı ilan olduđu dikkate alındıđında veri sorumlusunun aksi yönde bir eyleminin hukuk ve uygulaması açısından elzem bilgileri edinmek isteyebilecek çok sayıda kiřinin Anayasa'da düzenlenen temel haklarının ihlali sayılabileceđinin deęerlendirildiđi,

• Ayrıca kararın bir beraat kararı olduğunun içerikte açıkça belirtildiği ve ortalama bir okuyucunun söz konusu suçları ilgili kişiyle ilişkilendirmeyeceği, hatta herhangi bir yerde ilgili kişiye söz konusu suçları işlediğine dair iddiaların yöneltmesi halinde resmî kayıtların bu tip iddialara karşı kesin kayıt niteliğinde olacağı, ilanın dayanağı Tebligat Kanunu olduğundan bu bilginin işlenmesinin açıkça kanun tarafından öngörüldüğü ve işleme faaliyetinin aynı zamanda Kişisel Verilerin Korunması Kanunu'nun 28'inci maddesindeki muafiyetlerden "kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi" kapsamında değerlendirilebileceği

açıklamalarına yer verilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde, Kurulun 10/11/2022 tarihli ve 2022/1201 sayılı kararı ile;

• 6698 sayılı Kanun'un "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, "belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza", (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi" olarak tanımlandığı,

• Kanun'un 5'inci maddesinin kişisel verilerin işleme şartlarını düzenlediği, maddenin (1) numaralı fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin, (2) numaralı fıkrasında ise, kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda olan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün korunması için veri işlemenin zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaati için veri işlenmesinin

zorunlu olması hallerinde ilgili kişinin açık rızası olmaksızın kişisel verilerin işlenmesinin mümkün olduğunun hükme bağlandığı,

- 6698 sayılı Kanun'un "Şikâyet üzerine veya resen incelemenin usul ve esasları" başlıklı 15'inci maddesinin (5) numaralı fıkrasının ise "Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması hâlinde Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ eder. Bu karar, tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilir." şeklinde olduğu,

- Bu çerçevede, internette yer alan sayfalardaki kişisel veri barındıran içerikleri belirli bir sistematığe göre indeksleyerek arama sonuçlarında listelemesi suretiyle gerçekleştirilen işlemlerin "kişisel veri işleme faaliyeti" olduğu, internet sitelerinden topladığı verilerin işlenmesinin amaç ve vasıtalarını belirlediği dikkate alındığında arama motoru işleticisi şirketin "veri sorumlusu" sıfatını haiz olduğu, somut olayda işlenen kişisel verilerin ise ilgili kişinin adı soyadı ile yapılan arama sonucunda erişilen ad-soyad, anne-baba adı, doğum tarihi, ikametgah adresi ve beraate ilişkin bilgiler olduğu,

İlgili kişinin başvurusunda yer alan talep konusunun "İlgili kişinin adı ile arama motoru üzerinden yapılan aramada https://www.resmigazete.gov.tr/arsiv/*****.pdf uzantılı URL adresine ilişkin olarak ulaşılan sonucun arama motoru tarafından indeksten çıkarılması" yönünde olduğu,

- Tebligat Kanunu'nun "İlanen Tebligat" başlıklı 28'inci maddesinin "Adresi meçhul olanlara tebligat ilan edilir..." hükmünü, "İlan şekli" başlıklı 29'uncu maddesinin ise "İlan suretiyle tebliğ, tebliği çıkartacak merciin mucip sebep beyaniyle vereceği karar üzerine aşağıdaki şekilde yapılır. 1. İlan alakalının ıtılaina en emin bir şekilde vasil olacağı umulan ve varsa (...) (1) tebliği çıkaran merciin bulunduğu yerde intişar eden birer gazetede ve ayrıca elektronik ortamda yapılır. 2. Tebliğ olunacak evrak ve ilan sureti, tebliği çıkaran merciin herkesin kolayca görebileceği bir yerine de asılır. Merci, icabına göre ikinci defa ilan yapılmasına karar verebilir. İki ilan arasındaki müddet bir haftadan aşağı olamaz. Gerekirse ikinci ilan, yabancı memleket gazeteleriyle de yaptırılabilir." hükmünü haiz olduğu,

- Tebligat Kanunu'nun "İlanın ihtiva edeceği kayıtlar" başlıklı 30'uncu maddesinin "İlanda, alakalıların ad ve soyadları, işleri, ikametgâh veya mesken yahut iş yerleri, tebliğ olunacak evrak muhteviyatının hulasası, tebliğin anlaşılabilir şekilde mevzuu, sebebi, ilanın hangi merciden verildiği, ilan daveti tazammun ediyorsa nerede ve ne için, hangi gün ve saatte hazır bulunulacağı yazılmak lazımdır." ifadelerini, "İlanen tebligatta tebliğ tarihi" başlıklı 31'inci maddesinin ise "İlanen tebliğ, son ilan tarihinden itibaren yedi gün sonra yapılmış sayılır. İlanen tebliğe karar veren merci,

icabına göre daha uzun bir müddet tayin edebilir. Ancak, bu süre 15 günü geçemez.” ifadelerini içerdiği,

- Öte yandan, “Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına Yönelik Talepler” hakkında Kurul tarafından verilmiş olan 23/06/2020 tarihli ve 2020/481 sayılı kararda ile “kişilerin ad ve soyadı ile arama motorları üzerinden yapılan aramalarda çıkan sonuçların indeksten çıkarılmasına ilişkin değerlendirmede dikkate alınacak ve her somut olay üzerinde incelenecek kriterlerin” belirlendiği ve söz konusu kriterlerin “ilgili kişinin kamusal yaşamda önemli bir rol oynaması, arama sonuçlarının öznesinin çocuk olması, bilginin içeriğinin doğruluğu, bilginin kişinin çalışma hayatı ile ilgisi, bilginin ilgili kişi hakkında hakaret, onur kırıcı, iftira niteliğine sahip olması, bilginin özel nitelikli kişisel veri niteliği taşıması, bilginin güncelliği, bilginin kişi hakkında önyargıya sebep olması, bilginin kişi açısından risk doğurması, bilginin kişinin kendisi tarafından yayımlanma durumu, içeriğin gazetecilik faaliyeti kapsamında işlenen verileri kapsamaması, bilgilerin yayınlanmasında yasal zorunluluk olması, bilginin ceza gerektiren bir suçla ilgili olması” başlıkları ile belirlendiği, bu kapsamda somut olaya ilişkin şikâyetin söz konusu kriterler çerçevesinde değerlendirilmesine ihtiyaç duyulduğu,

- İlgili kişinin şikâyetinde yer alan https://www.resmigazete.gov.tr/arsiv/*****.pdf uzantılı URL adresinde ilgili kişiye ait açık kimlik ve hüküm özeti, beraat ve ilanen tebligat bilgilerinin bulunduğu,

- Somut olayın arama motoru üzerinden yapılan aramada çıkan sonuçların indeksten çıkarılmasına ilişkin olarak Kurulun 23/06/2020 tarihli ve 2020/481 sayılı kararı ile belirlenen kriterler çerçevesinde incelenmesi neticesinde; ilgili kişinin bir şirketin yönetim kurulu üyesi ve başkanı olduğu, bu kapsamda söz konusu içeriğin ilgili kişinin iş yaşamına ilişkin olmadığı, ayrıca içerikte yer alan verilerin işlenmesindeki amacın ilgili içeriğin kamu bilgisine sunulması değil ilgili kişiye tebliğinin sağlanması olduğu göz önünde bulundurulduğunda yayınlanmasında kamu yararının bulunmadığı, arama sonuçlarının öznesinin çocuk olmadığı açık olduğu, şikâyete konu URL adresinde yer alan Resmî Gazete'nin **/**/2000 ve mahkeme kararının da 1999 tarihli olduğu göz önüne alındığında 20 yıldan fazla sürenin geçmiş olduğu, bu anlamda içeriğin güncelliğini yitirdiği, her ne kadar içerikte yer alan bilgi ilgili kişinin üzerine atılı suçtan mahkeme kararıyla beraat ettiğinin teyidi olsa da ilgili kişi hakkında önyargıya sebep olabileceği, içeriğin ilgili kişinin kendisi tarafından yayınlanmadığı, içeriğin gazetecilik faaliyeti kapsamında işlenen verileri kapsamadığı,

- Öte yandan incelemeye konu şikâyet ile benzer olarak unutulma hakkına yönelik talebin yargı mercileri önüne taşındığı ilk davanın konusunun Costeja Gonzales'in arama motoru Google'da adını yazması sonucunda La Vanguardia isimli gazetenin iki farklı tarihli sayfasında çıkan kişinin sosyal

güvenlik borçlarını ödeyemediği için mülkünü satmak zorunda kalmasına ilişkin bilgilerin gazete sayfalarından ve Google ile Google İspanya arama sonuçlarından kaldırılmasını ve gizlenmesini talep etmesine ilişkin olduğu, Gonzales'in bu talebini temelde kendisiyle ilgili prosedürün yıllar önce sonuçlandığı ve artık bu haberlerin tamamen yersiz ve ilgisiz olduğu gerekçesine dayandırdığı,

İspanya Veri Koruma Otoritesi tarafından yapılan değerlendirmede; ulusal mevzuat çerçevesinde ilan verilmesinin zorunlu olduğu ve birçok kişinin bu bilgiye ulaşmasında veri sorumlusunun menfaatinin bulunduğu gerekçesi ile La Vanguardia hakkındaki şikâyetin reddedilmesine ama arama motoru işletmecilerinin veri koruma mevzuatına tabi oldukları gerekçe gösterilerek Google tarafından ilgili linklerin kaldırılmasına karar verildiği,

- Bunun üzerine Google'ın temyiz yoluna başvurduğu, İspanya Yüksek Ulusal Mahkemesinin de konu hakkında görüş bildirmesi için davayı Avrupa Birliği Adalet Divanı'na (ABAD) taşıdığı,

- ABAD'ın 2014 yılında verdiği kararında özetle; arama motorunda yapılan aramada çıkan sonuçlar "geçersiz, eksik, tamamen ilgisiz veya sonradan ilgisiz hale gelmiş" ise arama motorları tarafından internet ortamına yüklenme amacını aşan söz konusu kişisel verilerin ve buna ilişkin sonuç listesinde yer alan bilgilerin silinmesi gerektiğinin ifade edildiği, ayrıca kişinin özel hayatının gizliliği hakkının arama motorunun ekonomik çıkarı ile kamunun bilgiye erişim hakkının üzerinde olduğu değerlendirmesinde bulunulduğu, bu kuralın yalnızca kamunun bilgiyi öğrenmesinde üstün bir yararı var ise uygulanmayacağı, verilerin işleme amacı bakımından yetersiz, ilgisiz olması veya bu amacı aşması, güncellenmemesi ve gereğinden uzun tutulmaması gerekliliği gibi nedenlerle silme talebinde bulunulabileceğinin vurgulandığı, ABAD tarafından unutulma hakkına ilişkin verilen kararın 95/46/EC sayılı Direktif'in ilgili hükümlerine göre verildiği,

- İlerleyen süreçte Avrupa Birliği tarafından kişisel verilerin korunması alanında ortaya çıkan ihtiyaçları karşılamak üzere yürürlüğe giren Avrupa Genel Veri Koruma Tüzüğü'nün "Silme hakkı (Unutulma Hakkı)" başlıklı 17'nci maddesinde de unutulma hakkının ayrıca tanımlanmadığı ancak "silme" yükümlülüğü kapsamında değerlendirildiği, anılan düzenlemede bu hakkın kullanımı bakımından veri işleme şartlarının ortadan kalkmış olması gerektiği durumuna atıfta bulunularak hakkın istisnalarına (yasal yükümlülük, kamu yararına gerçekleştirilen bir görevin yerine getirilmesi, halk sağlığı alanındaki kamu yararı, kamu yararına arşivleme, bilimsel veya tarihi araştırma amaçları, istatistiki amaçlar, yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması) yer verildiği,

değerlendirmelerinden hareketle;

• Şikâyete konu Resmî Gazete sayfasının veri sorumlusu arama motoru üzerinden ilgili kişinin ismi ile ilişkilendirilerek indekslenmesindeki veri işleme faaliyetinin amacının ilgili içeriğin kamu bilgisine sunulması değil ilgili kişiye tebliğin yapılmasının sağlanması olduğu, bununla birlikte Tebligat Kanunu kapsamında ve Resmî Gazete’de belirtildiği üzere söz konusu içeriğin ilan tarihinden itibaren 15 gün sonra tebliğ edilmiş sayılacağı, bu anlamda ilgili kişiye tebliğ amacının gerçekleştiği, bununla birlikte ilgili kişinin bir şirketin yönetim kurulu üyesi ve başkanı olduğu ancak söz konusu içeriğin ilgili kişinin iş yaşamına ilişkin olmadığı, ayrıca içerikte yer alan verilerin işlenmesindeki amacın ilgili içeriğin kamu bilgisine sunulması değil ilgili kişiye tebliğinin sağlanması olduğu dikkate alındığında yayınlanmasında kamu yararı bulunmadığı, arama sonuçlarının öznesinin çocuk olmadığının açık olduğu, şikayete konu URL adresinde yer alan Resmî Gazetenin **/**/2000 ve mahkeme kararının da 1999 tarihli olduğu göz önüne alındığında 20 yıldan fazla süre geçmiş olduğu ve bu anlamda içeriğin güncelliğini yitirdiği, her ne kadar içerikte yer alan bilgi ilgili kişinin üzerine atılı suçtan mahkeme kararıyla beraat ettiğinin teyidi olsa da ilgili kişi hakkında önyargıya sebep olabileceği, içeriğin ilgili kişinin kendisi tarafından yayınlanmadığı, içeriğin gazetecilik faaliyeti kapsamında işlenen verileri içermediği değerlendirildiğinden, ilgili kişinin ad ve soyadıyla yapılan arama sonucunda çıkan https://www.resmigazete.gov.tr/arsiv/*****.pdf URL adresinin ilgili kişinin ad ve soy adıyla ilişkilendirilemeyecek şekilde indeksten çıkarılması hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2022/1147 sayılı KVKK Kararı

İlgili kişinin kişisel verilerinin iş akdinin feshinden sonra işveren tarafından işlenmeye devam edilmesi hakkında Kişisel Verileri Koruma Kurulunun 20/10/2022 tarihli ve 2022/1147 sayılı Karar Özeti

Karar Tarihi : 20/10/2022

Karar No : 2022/1147

Konu Özeti: İlgili kişinin kişisel verilerinin iş akdinin feshinden sonra işveren tarafından işlenmeye devam edilmesine ilişkin şikâyet

İlgili kişinin Kuruma intikal eden şikayetinde özetle;

- Mobilya-dekorasyon sektöründe faaliyet gösteren bir anonim şirket bünyesinde iç mimar olarak yaklaşık 3 yıl çalıştığı, iş akdinin feshi tarihinden sonra, pandemi döneminde veri sorumlusu şirket tarafından müşterilere yönelik olarak sosyal medya üzerinden gerçekleştirilen canlı yayınlardaki görüntüsünün TV reklamlarında, veri sorumlusu şirketin internet sitesinde, sosyal medya hesaplarında ve tanıtıma yönelik basılı materyallerde reklam ve pazarlama amacıyla kullanıldığı, görüntüsünün bu şekilde kullanımı ile ilgili olarak kendisine aydınlatma yapılmadığı, açık rızasının da alınmadığı,
- Öte yandan iş akdinin feshedildiği tarihten sonra veri sorumlusunun taşıma süreçlerine ilişkin kargolarda hala ilgili kişinin cep telefonu numarasının kullanıldığı,
- Yine iş akdinin feshedildiği tarihten sonra ilgili kişinin veri sorumlusu bünyesinde gerçekleştirilen satış ve tahsilat işlemlerinde işlemi gerçekleştiren kişi gibi görüldüğü,
- Şikayete konu durum ve delillerin Ankara 4. Fikri ve Sınai Haklar Hukuk Mahkemesinin 2022/... D.İş sayılı dosyası üzerinden Bilirkişi Raporu ile tespit edildiği,
- Veri sorumlusuna yapılan başvuruda ilgili kişiye ait kişisel verilerin imhası ve bu konuda kendisine bilgi verilmesinin talep edilmesine karşın veri sorumlusu tarafından bu konuda bir işlem yapılmayıp hatalı ve eksik bilgi verildiği, veri sorumlusu tarafından ilgili kişinin aydınlatma metnini imzaladığı ifade edilmiş ise de bu aydınlatma metninin iş akdi süresi içerisinde sınırlı olduğu, zira içerisinde

“Kişisel verileriniz, iş akdiniz devam ettiği sürece yukarıdaki amaçlarla ve bu amaçların gerektirdiği süre boyunca saklanacaktır.” ibaresinin yer aldığı,

- Veri sorumlusu tarafından ilgili kişiye çalıştığı süre boyunca iki adet şirket hattı tesis edildiği iddia edilmiş ise de kargo şirketine bildirilen numaranın, ilgili kişinin şahsî cep telefonu numarası olduğu, ilgili kişiye işten ayrıldıktan sonra gelen kargo SMS’lerinin de bunun kanıtı olduğu, şirket merkezinden ilgili kişinin çalıştığı mağazaya gönderilen ürünlerin kargolarında alıcı olarak halen ilgili kişinin telefon numarasının verildiği, bu durumun iş akdinin bitmesiyle birlikte hukuka aykırı hale geldiği,

ifade edilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması ve hukuka aykırı olarak işlenen kişisel verilerinin imha edilmesi talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- İlgili kişinin görev tanımında ana sorumluluğunun “... müşterileri satın almaya teşvik edecek en iyi atmosferi yaratmak...” olarak belirlendiği, dolayısıyla ilgili kişinin mesleğini, satışa yönelik pazarlama faaliyetleri çerçevesinde sunarak gerçekleştirmesinin, işe alındığı pozisyonun gereği olduğu ve görev kapsamı içerisinde bulunduğu, bu hususlarının tümünün ilgili kişiye imzalatılan iş akdinde yer aldığı,

- İlgili kişiye imzalatılan aydınlatma metninde bulunan “İşlenen kişisel verilerinizin yurt içindeki aktarımı” başlıklı maddenin altıncı bendinde “yazılım, kurumsal kaynak planlaması, raporlama, pazarlama vb. işlevlerin yerine getirilmesi amacıyla tedarikçi ve çözüm ortaklarıyla verilerin paylaşılabilmesi” hususunun yer aldığı, bu hukuki mesnede binaen ilgili kişinin şirket reklamlarında yer alarak pazarlama amacıyla kişisel verilerinin işlenmesine rıza vermiş sayılacağı, ilgili kişinin işi gereği şirketin tanıtım yüzlerinden biri olduğu, ilgili kişinin bu işi bilerek kabul etmesine karşın iş akdi feshedildikten sonra bu hükümleri kötü niyetle şirket aleyhinde yorumlamaya çalıştığı,

- İlgili kişinin “kargo paketi üzerinden görüldüğünden bahisle cep telefonu bilgisinin şirketçe işlenmeye devam edilmesi” iddiasının da izahtan varestede olduğu, bu konuda bir delil olmadığı, açıkça kötü niyetli bir iddia olduğu

ifade edilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulunun 20/10/2022 tarih ve 2022/1147 sayılı Kararı ile;

- Kanun'un, kişisel verilerin işlenmesine ilişkin "Genel İlkeler"i düzenleyen 4'üncü maddesinin (1) numaralı fıkrasında, "Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir." hükmü yer almakta olup bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin; a) Hukuka ve dürüstlük kurallarına uygun olma, b) Doğru ve gerektiğinde güncel olma, c) Belirli, açık ve meşru amaçlar için işlenme, ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,
- Kanun'un "Kişisel verilerin işleme şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,
- Kanun'un 7'nci maddesinde "Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi" hususu düzenlenmiş olup maddede; "(1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir. (2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır. (3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir." hükümlerine yer verildiği,
- Ayrıca 6698 sayılı Kanun'un "Veri güvenliğine ilişkin yükümlülükler"i düzenleyen 12'nci maddesinin (1) numaralı fıkrasının (a), (b) ve (c) bentleri uyarınca veri sorumlularının; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik her türlü teknik ve idarî tedbiri almakla mesul tutulduğu,

- Somut olaya ilgili kişinin reklam ve pazarlama amacıyla yayınlanan görüntülerinin ilgili kişinin veri sorumlusu bünyesinde çalışırken kendisinin iş tanımı kapsamı içerisinde alındığının anlaşıldığı ve bu nedenle söz konusu kişisel verilerin, veri sorumlusu bünyesindeki arşivlerde yasal süre müddetince muhafaza edilmesinin hukuka uygun olduğu kanaatine ulaşılmış ise de ilgili kişinin mesleğinin esas itibariyle mimarlık olup bu mesleğin icrasının ekran önünde görünmeyi gerektirmemesi ve ilgili kişi ile veri sorumlusu arasındaki çalışma akdinin hâlihazırda feshedilmiş olması, dolayısıyla ilgili kişinin başka bir şirket nezdinde çalışmaya başlaması veya kendi ticari faaliyetlerini yürütmeye karar vermesi gibi durumlarda veri sorumlusunun halen ilgili kişinin görüntülerini kullanarak reklam ve pazarlama maksatlı faaliyetler yürütmesinin hayatın olağan akışına aykırı olacağı,
- Veri sorumlusunun ilgili kişiye verdiği cevapta, her ne kadar söz konusu cep telefonu numarasının, ilgili kişi tarafından iş süreçlerinde kullanılması amacıyla kargo şirketlerine kendi iradesiyle verildiği iddia ediliyor ise de Kanun'un 4'üncü maddesinde düzenlenen genel ilkeler gereğince işlemekte olduğu kişisel verileri bu ilkelere uygun bir şekilde doğru ve güncel tutması, elde etme amaçlarına uygun bir şekilde kullanması ve yalnızca hukukî sebep bulunduğu durumlarda, yasal süre müddetince muhafaza etmesi hususunda aktif özen yükümlülüğü altında bulunan veri sorumlusunun, iş akdini feshettiği bir çalışanın cep telefonu numarasını kendisine ait iş süreçlerinde kullanmak suretiyle, uhdesinde işlediği kişisel verilerin doğru ve güncelliğini sağlayamamış olduğu, veri sorumlusunun, ilgili kişinin kargo şirketi nezdinde kayıtlı bulunan cep telefonu numarasını yeni yetkili kişinininki ile değiştirdiğini kargo şirketine bildirmediği ve ilgili kişinin kişisel verilerinin kullanımını sonlandırabilecek iken bunu yapmayarak ilgili kişinin kişisel verilerinin korunması adına gerekli hassasiyeti göstermediği,
- Zira şirket merkezinden ilgili kişinin çalıştığı mağazaya gönderilen ürünlerin kargolarının alıcısı olarak halen ilgili kişinin görüldüğü, bu sebeple kargo şirketi tarafından ilgili kişinin kayıtlı kişisel cep telefonu numarasına SMS gönderimi yapıldığının görüldüğü, bu nedenle veri sorumlusunun Kanun'un 4'üncü maddesinin (2) numaralı fıkrasının (b) bendinde gösterilen "Doğru ve gerektiğinde güncel olma" ilkesine aykırı davrandığı,
- Ankara 4. Fikri ve Sınai Haklar Hukuk Mahkemesinin 2022/... D. İş sayılı dosyasında yer alan Bilirkişi Raporundan ilgili kişinin iş akdinin fesih edildiği tarihten sonra yapılan pek çok satışta "işlemi gerçekleştiren" sorumlu personel olarak gösterildiğinin anlaşıldığı, bu minvalde işlemi yapan kişi olarak ilgili kişinin görüldüğü belgeler tanzim edildiği, ilgili kişinin kişisel verilerinin bu

bakımdan, veri sorumlusu nezdinde Kanun'un 4'üncü maddesinin (2) numaralı fıkrasının (b) bendinde gösterilen "Doğru ve gerektiğinde güncel olma" ilkesine aykırı bir şekilde işlendiği,

- 6698 sayılı Kanun'da gösterilen genel ilkeler ve veri işleme şartlarına aykırı bir şekilde işlenen kişisel verilerin; veri sorumlusunun, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12'nci maddesinin (1) numaralı fıkrasının (a) bendinde ifade olunan, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idarî tedbirleri almadığını gösterdiği,

değerlendirmelerinden hareketle,

- İlgili kişinin yer aldığı görüntülerin veri sorumlusunun arşivlerinde bulunmasının hukuka uygun olacağı ancak iş akdinin sona ermesinden sonra da söz konusu verilerin paylaşımına devam edilmesi suretiyle işlenmesinde Kanun kapsamında geçerli bir işleme şartının mevcut olmadığı, öte yandan ilgili kişinin kargo şirketleri nezdinde kayıtlı olan kişisel cep telefonu numarasının ve iş akdi feshedilmeden öncesinde çalıştığı mağazadaki dijital ödeme sistemleri, çeşitli evrak ve formlar içerisinde kayıtlı bulunan ve kendisini işlem yetkilisi olarak gösteren kişisel verilerinin Kanun'un 4'üncü maddesinde yer alan Genel İlkelerden "doğru ve gerektiğinde güncel olma" ilkesine aykırı şekilde işlendiği, bu verilerin işlenmesinde veri sorumlusunca bir başka hukuki nedenin de gösterilemediği görüldüğünden Kanun'un 12'nci maddesinin (1) numaralı fıkrasında yer alan yükümlülüklerini yerine getirmediği anlaşılan veri sorumlusu hakkında, ilgili kişinin hukuka aykırı olarak işlenen kimlik ve iletişim bilgileri kullanılarak yapılan satış, kargo gönderimi gibi yasal işlemlerin ilgili kişi üzerinde negatif sonuç doğurma riskinin yüksek olduğu hususu dikkate alınarak, Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 250.000 TL idarî para cezası uygulanmasına,

- Diğer taraftan, ilgili kişinin hukuka aykırı bir şekilde işlendiği anlaşılan şahsî cep telefonu bilgisinin veri sorumlusu ve kargo şirketi kayıtlarından, isim ve soy isim bilgilerinin ise iş akdi feshedilmeden öncesinde çalıştığı mağazadaki dijital ödeme sistemleri, çeşitli evrak ve formlar içerisinde imha edilmesi, buna ilişkin usule uygun bir şekilde düzenlenecek olan tutanakların ilgili kişi vekiline iletilmesi ve bu tutanaklar ile ilgili belgelerin muhatabınca tebellüğ edildiğine dair delillerin Kurula da gönderilmesi hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2022/1072 sayılı KVKK Kararı

İlgili kişinin kişisel verisi niteliğindeki e-posta adresinin reklam amaçlı ileti gönderilmesi suretiyle işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 07/10/2022 tarihli ve 2022/1072 sayılı Karar Özeti

Karar Tarihi : 07/10/2022

Karar No : 2022/1072

Konu Özeti: İlgili kişinin kişisel verisi niteliğindeki e-posta adresinin reklam amaçlı ileti gönderilmesi suretiyle işlenmesi

İlgili kişinin Kuruma intikal eden şikâyetinde özetle; ilaç sektöründe faaliyet gösteren bir şirketin çalışanı olduğu iddia edilen bir şahıstan e-posta aldığı, e-posta adresinin nasıl elde edildiğine ilişkin veri sorumluna başvurarak e-posta adresinin ecza depoları vasıtasıyla paylaşıldığı bilgisini edindiği ifade edilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- E-posta gönderen şahsın şirkette kısa bir süre çalıştığı ve daha sonra istifa ettiği, bahse konu yazışmaların şirketin bilgisi ve onayı dahilinde yapılmadığı, Kurum tarafından şirkete tebliğ üzerine konudan haberdar olunduğu,
- Söz konusu işlem, şirket eski çalışanı tarafından şirketin bilgisi ve onayı dışında yapılmış olduğundan hangi kişisel verinin hangi amaçla işlendiği konusunda bilgi sahibi olunmadığı,
- Dolayısıyla ilgili kişinin açık rıza beyanına ilişkin tevsik edici bir belgenin de mevcut bulunmadığı ifade edilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulunun 07/10/2022 tarih ve 2022/1072 sayılı Kararı ile;

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise

kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin düzenlendiği,

- Kurul tarafından “Veri sorumluları ve veri işleyenler tarafından ilgili kişilerin e-posta adreslerine veya SMS ya da çağrı ile cep telefonlarına reklam bildirimleri/aramaları yönlendirilmesinin önüne geçilmesini teminen” alınan 16/10/2018 tarihli ve 2018/119 sayılı İlke Kararı’nda; “İlgili kişilerin rızalarını almadan veya Kanun’un 5’inci maddesinin (2) numaralı fıkrasında hüküm altına alınan işleme şartlarını sağlamadan, telefon numaralarına SMS göndermek, arama yapmak veya e-posta adreslerine posta göndermek suretiyle reklam içerikli ileti yönlendiren veri sorumluları ile veri sorumluları adına reklam içerikli mesaj/e-posta göndermek veya arama yapmak amacıyla ilgili kişilerin açık rızaları bulunmaksızın bu verileri kullanan veri işleyenlerin söz konusu veri işleme faaliyetlerini Kanun’un 15’inci maddesinin (7) numaralı fıkrası uyarınca derhal durdurması gerektiği; Kanun’un 12’nci maddesi kapsamında veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu ve kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, anılan tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumlu olduğu; belirtilen şekilde söz konusu faaliyetlerde bulunan veri sorumluları hakkında Kanun’un 18’inci maddesi hükümleri çerçevesinde işlem tesis edileceği; bahse konu şekilde işlenen kişisel verilerin hukuka aykırı olarak elde edilmiş olabileceği de göz önüne alınarak 5237 sayılı Türk Ceza Kanunu’nun ‘Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme’ başlıklı 136’ncı maddesi çerçevesinde ilgili veri sorumluları hakkında gerekli hukuki işlemlerin tesisi için konunun 5271 sayılı Ceza Muhakemesi Kanunu’nun 158’inci maddesi uyarınca ihbaren ilgili Cumhuriyet Başsavcılığına bildirileceği” hususlarının karara bağlandığı,

- Kanun'un "Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi" başlıklı 7'nci maddesinde; bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silineceği, yok edileceği veya anonim hâle getirileceği ve kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu ibaresinin yer aldığı,

- Kanun'un 12'nci maddesinin (1) numaralı fıkrasının "Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır." hükmünü amir olduğu, bununla birlikte (2) numaralı fıkrasında; "Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur." ifadesi bulunurken (3) numaralı fıkrasında "Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır." hükmünün yer aldığı,

- Somut olaya konu reklam amaçlı e-postaların, somut olayın yaşandığı tarihte veri sorumlusu bünyesinde çalışan personel tarafından kurumsal e-posta adresi üzerinden ilgili kişinin elektronik posta adresine gönderildiği; veri sorumlusunun ilgili kişinin kişisel verisi niteliğindeki elektronik posta adresinin veri sorumlusunun çalışma alanı çerçevesinde reklam ve pazarlama amaçları doğrultusunda kullanıldığı ve ilgili kişinin açık rızasının alınmadığının anlaşıldığı, bu kapsamda ilgili kişinin e-posta adresine izinsiz reklam içerikli ileti gönderilmesi suretiyle kişisel verilerin işlenmesinde Kanun'un 5'inci maddesinde yer alan herhangi bir işleme şartının bulunmadığı değerlendirilmelerinden hareketle;

- Veri sorumlusu tarafından reklam ve pazarlama amaçlı, izinsiz ticari elektronik ileti gönderilmesi suretiyle ilgili kişinin kişisel verisi niteliğinde olan e-posta adresinin işlenmesinde Kanun'un "Kişisel verilerin işleme şartları" başlıklı 5'inci maddesinde öngörülen kişisel veri işleme şartlarının bulunmadığı ve bu kapsamda veri sorumlusunun Kanun'un 12'nci maddesinin (1) numaralı fıkrasının (a) bendi kapsamında kişisel verilerin hukuka aykırı işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı kanaatine varılması nedeniyle Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendine istinaden veri sorumlusu hakkında 50.000 TL idari para cezası uygulanmasına,

- Somut olayda ilgili kişinin kişisel verisi niteliğinde olan e-posta adresinin, hukuka aykırı olarak işlendiği dikkate alındığında; Kanun'un 7'nci maddesi ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'e uygun olarak ilgili kişinin kişisel verisinin imha edilmesi ve söz konusu imha işlemlerini tevsik edici belgelerin Kurula iletilmesi hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2022/925 sayılı KVKK Kararı

İlgili kişinin e-posta adresine başka abonelere ait e-faturaların gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 08/09/2022 tarihli ve 2022/925 sayılı Karar Özeti

Karar Tarihi : 08/09/2022

Karar No : 2022/925

Konu Özeti: İlgili kişinin e-posta adresine başka abonelere ait e-faturaların gönderilmesi

İlgili kişinin Kuruma intikal eden şikâyetinde özetle; ilgili kişinin daha önce veri sorumlusu telekomünikasyon şirketi hakkında kendisine ait e-posta adresine başka bir aboneye ait e-faturaların gönderilmesi nedeniyle şikâyette bulunduğu, bu kapsamda veri sorumlusu telekomünikasyon şirketi hakkında Kişisel Verileri Koruma Kurulu (Kurul) tarafından idari para cezası uygulanmasına ve kişisel verilerin güvenliğine ilişkin gerekli tüm idari ve teknik tedbirlerin alınması hususunda veri sorumlusunun talimatlandırılmasına karar verildiği ancak 2018 yılından beri 053.....4 numaralı hattın sahibinin e-faturalarının veri sorumlusu tarafından ilgili kişiye iletilmediği bununla birlikte 054.....9 numaralı hattın sahibinin e-faturalarının da kendisine iletmeye başlandığı ifade edilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- Öncelikle ilgili kişiye ait verilerin düzeltilmesini isteme hakkının yerine getirilmediği iddiasının gerçeği yansıtmadığı, ilgili kişinin şirkete yaptığı başvuru sonrasında 054.....9 numaralı hattın faturalama bilgilendirme tercihinin Mayıs 2020 dönemi ve sonrası için e-faturadan SMS'e çevrildiği; bu çerçevede, şirket sistemlerinde yapılan sorgulamada 054.....9 numaralı telefon numarasına ilişkin hazırlanan e-faturanın ilgili kişinin beyan ettiği e-posta adresine en son 30 Nisan 2020 tarihinde iletilmediğinin tespit edildiği,
- Aynı e-mail adresini beyan eden 053.....4 numaralı hat sahibine ise konuya ilişkin olarak ulaşılmaya çalışılmasına rağmen borcundan dolayı hattının erişime kısıtlı olması nedeniyle ulaşılamadığı, abonelik sözleşmesi kapsamında aynı e-posta adresini beyan eden hat sahibinin

değişikliğe ilişkin rızası alınmadığı için herhangi bir işlem yapılamadığı, hat sahibinin abonelik sözleşmesinde beyan ettiği bilgilerin hat sahibinin iradesi dışında değiştirilmesinin Kanun kapsamındaki haklarının ihlaline ve Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK) ilgili yönetmeliklerine aykırı hareket edilmesine sebep olacağı, zira kişisel verilerinin düzeltilmesinin kullanılması hakkının hat sahibine ait olduğu,

- İlgili kişinin ilk şikâyetini 11.01.2019 tarihinde Kuruma ilettiği, ilk başvurusunda, yalnızca 053.....7 numaralı hattın faturalarının kendisine gönderilmesi ve bu suretle e-posta adresinin hukuka aykırı işlendiğine ilişkin rahatsızlığını beyan ettiği ancak 053.....4 numaralı hatta ait faturaların da 2018 yılında aynı e-posta adresine iletilmekte olduğu görülmesine rağmen ilgili kişinin yaptığı 11.01.2019 tarihli ilk başvuruda 053.....4 numaralı hattın faturasına ilişkin rahatsızlık duyduğunu beyan etmediği, ilk başvurusunda yer vermediği bu numaraya yönelik rahatsızlığını yaklaşık 18 ay sonra iletme gereği duymasının diğer şikâyetlerinde kullanmak üzere numarayı elinde tutmayı tercih etmesi anlamına geldiği, gereksiz iş yükü getiren ve etik olmayan bu tercihin dürüstlük ilkesiyle bağdaşmadığı

ifade edilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kurulun 08/09/2022 tarih ve 2022/925 sayılı Kararı ile;

- Kanun'un "Genel İlkeler" başlıklı 4' üncü maddesinde "(1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir. (2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur: a) Hukuka ve dürüstlük kurallarına uygun olma. b) Doğru ve gerektiğinde güncel olma. c) Belirli, açık ve meşru amaçlar için işlenme. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme." hükmünün yer aldığı

- Kanun'un "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12'nci maddesinde; "(1) Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır." hükmüne yer verildiği,

- Somut olayda ilgili kişinin ilk başvurusuna istinaden verilen Kurul Kararı kapsamında veri sorumlusunun kişisel verilerin güvenliğine ilişkin gerekli tüm idari ve teknik tedbirlerin alınması hususunda talimatlandırılmasına rağmen, üçüncü kişilere ilişkin faturanın ilgili kişinin e-posta

adresine iletmeye devam edilmesinin ve yine üçüncü bir kişiye ait abonelik sözleşmesinde ilgili kişinin e-posta adresinin bildirilmiş olmasının, mevcut ve yeni üyelerin e-posta adresi gibi iletişim kanallarının doğrulanmasına yönelik bir mekanizmanın bulunmadığını gösterdiği,

- Veri sorumlusunun söz konusu kişisel verilerin doğruluğunu sağlamak amacıyla proaktif bir yaklaşımla gerekli tedbirleri almamasının Kanun'un 4'üncü maddesinin (2) numaralı fıkrasının (b) bendinde yer alan "doğru ve gerektiğinde güncel olma" ilkesine aykırılık teşkil ettiği, dolayısıyla veri sorumlusu tarafından kişisel verilerin işlenmesinde Kanun'un 12'nci maddesinin (1) numaralı fıkrası kapsamında uygun güvenlik düzeyini temin etmeye yönelik gerekli tedbirlerin alınmadığı kanaatine varıldığı

değerlendirmelerinden hareketle;

- İlgili kişinin e-posta adresinin üçüncü kişilere ait faturanın iletilmesi suretiyle işlenmesi ve bu durumun Kanun'un 4 üncü maddesinin (2) numaralı fıkrasının (b) bendinde yer alan "doğru ve gerektiğinde güncel olma" ilkesine aykırılık teşkil etmesi sebebiyle Kanun'un 12'nci maddesinin (1) numaralı fıkrasındaki yükümlülükleri yerine getirmediği kanaatine varılan veri sorumlusu hakkında, daha önce verilen Kurul Kararında abonelerin kişisel verilerinin güvenliğine ilişkin gerekli idari ve teknik tedbirlerin alınması hususunda talimatlandırıldığı da dikkate alınarak, Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 200.000 TL idari para cezası uygulanmasına,
- İlgili kişinin e-posta adresine üçüncü kişilere ait kişisel verilerin iletilmemesi amacıyla gerekli tedbirlerin alınması ve sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2022/923 sayılı KVKK Kararı

İlgili kişinin telefon numarasının hastaneden ayrılan doktor tarafından SMS gönderilmesi suretiyle işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 08/09/2022 tarihli ve 2022/923 sayılı Karar Özeti

Karar Tarihi : 08/09/2022

Karar No : 2022/923

Konu Özeti: İlgili kişinin telefon numarasının tedavi olduğu hastaneden ayrılan doktor tarafından SMS gönderilmesi suretiyle işlenmesine ilişkin şikâyet

Kuruma intikal eden şikâyetinde özetle ilgili kişinin;

- Ocak 2018 tarihinde hastanede bir doktor tarafından muayene edildiği, ilgili doktorun hastaneden ayrılarak özel muayenehane açtığı ve akabinde ilgili kişinin cep telefonu numarasına reklam amaçlı SMS gönderdiği, bu sebeple doktor tarafından hastaneden ayrılırken kişisel verilerinin hukuka aykırı olarak temin edildiğini düşündüğü,
- Konuya ilişkin ilgili doktora ve hastaneye başvurduğu, doktorun cevabında kendisine ait verilerini sağlık durumunun kontrolü amacıyla aldığını belirttiği, hastanenin cevabında ise başvurusuna konu ettiği kişisel verilerine ilişkin özel bilgi vermek yerine genel nitelikte ve konuya özgü olmayan bir cevap verildiği, bu çerçevede taraflardan yeterli bir cevabın alınmadığı,
- Kendisinin sadece yaklaşık 3 sene önce ilgili doktora bir kere muayene olduğu ve sonrasında hiçbir muayene ya da tedavinin söz konusu olmadığı, ne hastane nezdinde ne de doktor nezdinde devam eden ya da takip edilen hiçbir sağlık probleminin söz konusu olmadığı, bu sebeple ilgili doktorun hastaneden ayrılırken kendisine ait verileri usulsüz olarak ele geçirdiği ve kendi özel kliniğinde maddi çıkar sağlamak üzere kullandığı

ifade edilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında hastane ve doktor hakkında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde hastaneden ve ilgili doktordan savunması istenilmiş olup doktordan alınan cevabi yazıda özetle;

- Hastaneden ayrılırken rehberinde telefon numaraları bulunan hastalara artık mesleğini özel muayenehanede yürüteceğine dair bilgilendirme mesajı gönderdiği,
- Hastanede çalışmadığı konusunda hastaların bilgilendirilmesinin önem arz ettiği ve hastalara kolaylık sağladığı, bu hususun özellikle kadın doğum uzmanlığı gibi yüksek ihtisaslar için bir zorunluluk olduğu, somut durumda da ilgili kişinin iletişim bilgilerini kendisinin paylaşmış olduğu, bu açıdan hastaların bilgilendirilmesinin hayatın doğal akışına uygun ve mesleğin doğası gereği olduğu, ayrıca bu durumun mesleki bir sorumluluk olduğu,
- 2017-2020 arasındaki dönemde hastane ile arasında kurulan ilişkinin bir işçi-işveren ilişkisi olmadığı, tıp dünyasında genel geçer uygulamalara uygun olarak hastaların doktoru kendisi iken; hastaların barınma, yeme-içme, hastane hizmetlerinden faydalanma, yatış işlemleri gibi “hekimlik dışı” işlemlerinde, hastayla arasında ilişki kuran tarafın hastane olduğu, tüm sağlık sektöründe de işleyişin bu şekilde olduğu, hastanenin, hasta-doktor ilişkisinde sağlık ve bakım hizmetleri söz konusu olduğu durumda devreye giren bir süje olduğu,
- Bu kapsamda tıbbi bakım ve tedavi hizmetlerinin özünü sağlayanın hastane değil, hekim olduğu; bundan ötürü de hastanın her zaman doktorla iletişim kurmak ve onu takip etmek istediği, bu durumun sadece özel hastanelerde değil neredeyse tüm hasta-hekim ilişkisinin kurulduğu tıbbi yerleşkelerde söz konusu olduğu, somut olayda da şikayetçinin hastane bünyesinde bulunan ve yüksek ihtisasa sahip dört doktor arasından kendisiyle hasta-hekim ilişkisi kurmayı tercih ettiği,
- Bu minvalde meslek hayatı boyunca neredeyse tüm hastalarıyla iletişim bilgilerini memnuniyetle paylaştığı ve sadece hastalarıyla iletişim için kullandığı bir numarasının bulunduğu, özellikle de uzmanlık ihtisasının kadın doğum doktorluğu ve özel alanının ise tüp bebek uzmanlığı olması sebebiyle iletişimin hem mesleğin etik gereklilikleri hem de hastanın hassasiyeti ve beklentileri sebebiyle çok daha büyük bir önem arz ettiği,
- İlgili kişinin sadece adı-soyadı ile telefon numarası bilgilerinin mevcut olduğu, bu bilgilerin ilgili kişiyi muayene ettiği tarihte ilgili kişinin kendisi tarafından paylaşıldığı, bunun dışında ilgili kişinin sağlık verisi gibi bilgilerini kaydetmesinin ve saklamasının mümkün olmadığı, ilgili kişinin iletişim numarasının da doğrudan cep telefonu rehberine kaydedildiği ve üçüncü kişilerle paylaşılmadığı,
- İlgili kişinin başvurusunun ardından cep telefonu numarasının da silindiği

ifade edilmiştir.

Hastaneden alınan cevabi yazıda ise özetle;

- Doktor ile aralarındaki sözleşmenin Eylül 2020 tarihinde sona erdiği, bu tarihten itibaren doktorun hastane kayıt ve sistemlerine erişemediği, dolayısıyla Eylül 2020 tarihinden sonra doktor tarafından gerçekleştirilen herhangi bir haksız veri işleme faaliyetinden hastanenin sorumlu tutulamayacağı,
- Hastalara ait kişisel verilerin Hastane Bilgi Yönetim Sistemine (HBYS) kaydedildiği, ardından hasta tarafından randevu alınması halinde, ilgili hastanın HBYS'ye kaydedilmiş olan verilerinin muayenenin gerçekleştirilmesi amacıyla yine HBYS sistemi üzerinden hekimlerin erişimine açıldığı, bu sistemin yalnızca muayene işleminin gerçekleştirilmesi amacıyla çalıştığı,
- Bir hekimin hastasının iletişim bilgilerine erişiminin olmasının hayatın olağan akışı içerisinde oldukça normal bir durum olduğu ve hastanın menfaati için gerekli olduğu,
- Hastanın adı, soyadı, T.C. kimlik numarası, iletişim bilgileri, şikâyeti, özgeçmişi, öykü, soy geçmişi, bulgu bilgilerinin HBYS üzerinden yalnızca tedavinin sağlanması amacıyla görüntülenmek üzere söz konusu doktorun erişimine sunulduğu, log kayıtlarından da anlaşılacağı üzere doktorun epikriz raporu oluşturmak ve ilgili kişinin sağlık bilgilerini Hastane Bilgi Yönetim Sistemine kaydetmek üzere sisteme giriş yaptığı

ifade edilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulunun 08/09/2022 tarih ve 2022/923 sayılı Kararı ile;

- 6698 sayılı Kanun'un "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, "belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza", (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi" olarak tanımlandığı,
- Somut olayda, ilgili kişi tarafından şikayet dilekçesinde hastanede yer alan kişisel verilerinin doktor tarafından hukuka aykırı olarak temin edildiğinin iddia edildiği, hastanenin cevabında ilgili kişinin 16.01.2018 tarihinde hastanede görev yapmakta olan şikayete konu doktora muayene olduğu;

doktorun 01.09.2020 itibariyle hastane ile olan iş ilişkisinin sona erdiği ve bu tarihten itibaren hastane kayıt ve sistemlerine erişim imkanının kalmadığı; sisteme giriş kayıtlarında da (log) doktorun ilgili kişinin kaydına hastanede çalıştığı süre içerisinde sisteme giriş yetkisi bulunurken 12.01.2018, 19.01.2018 ve 27.06.2018 tarihlerinde giriş yaptığının görüldüğü,

- Doktor tarafından ise, ilgili kişinin kişisel verisi olan cep telefon numarasının hastane kayıtlarından temin edilmediği, aksine ilgili kişinin muayenesi esnasında branşının mahiyeti gereği iletişim kurulabilmesi amacıyla bizzat kişiden temin edilerek cep telefonuna kaydedildiği, hastaneden ayrılması akabinde de güncel adresi hakkında bilgi verilerek kendisiyle iletişim kurulabilmesi amacıyla telefon rehberinde kayıtlı olması sebebiyle ilgili kişiye de SMS gönderildiğinin beyan edildiği değerlendirildiğinde söz konusu kişisel verilerin hastanenin veri tabanından alındığının tevsik edilemediği,

- 6698 sayılı Kanun'un "Genel İlkeler" başlıklı 4'üncü maddesinde, kişisel verilerin ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verilerek bu çerçevede, kişisel verilerin ancak hukuka ve dürüstlük kurallarına uygun şekilde, belirli, açık ve meşru amaçlar kapsamında, doğru ve gerektiğinde güncel olma şartıyla, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun olarak işlenebileceğinin belirtildiği,

- Diğer taraftan, Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin "(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür: a) Kanunlarda açıkça öngörülmesi. b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması. c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması. ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması. d) İlgili kişinin kendisi tarafından alenileştirilmiş olması. e) Bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması. f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" hükmünü haiz olduğu,

- Veri sorumlusunca ilgili kişiye ait kişisel verilerin belirtilen amaçlar dışında başka amaçlarla işlenmemesi, amaçla sınırlı olma ilkesi uyarınca kişisel verilerin işlenmesinin belirlenen amaçların

gerçekleştirilmesine elverişli olması, amacın gerçekleşmesiyle ilgili olmayan kişisel verilerin işlenmesinden kaçınılması gerektiği,

- Kanun'un gerekçesinde de "(...) sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik veri işlenebilmesi için, işlemeye ilk kez başlıyor gibi, 5'inci maddede düzenlenmiş olan kişisel verilerin işleme şartlarından birinin gerçekleşmesi gerekecektir" ifadesinin yer aldığı, dolayısıyla veri sorumlusunun kişisel verileri ilk veriliş amacıyla uyumsuz bir şekilde işlememesi, farklı bir amaçla işleme durumu söz konusu ise bu işlemenin de ayrıca bir hukuka uygunluk sebebine dayanması gerektiği,

- Somut olayda, şikayet konusu SMS'in kendi mesleki faaliyeti kapsamında ilgili kişiye gönderilmesi özelinde veri sorumlusu olduğu anlaşılan doktorun ilgili kişiyi 2018 Ocak ayında, çalıştığı hastane bünyesinde muayene ettiği, ilgili kişi ile olan hasta-doktor ilişkisi kapsamında sistem bilgilerine hastane doktoru olarak en son 2018 Haziran ayında girdiği, bu tarihten sonra ilgili kişi ile doktor arasında tıbbi olarak bir temas sağlandığına yönelik herhangi bir kaydın ya da beyanın bulunmadığı, ancak veri sorumlusu doktor tarafından 2020 yılında, hastane ile olan iş ilişkisinin sona erdiği ve güncel adresinin değiştiği hakkında ilgili kişinin hastanede muayene olurken vermiş olduğu ve halihazırda doktorla bir hizmet ilişkisi de bulunmazken ilgili kişinin cep telefonuna kısa mesaj göndermek suretiyle ilgili kişinin kişisel verisi olan telefon numarasının işlendiğinin anlaşıldığı,

- İlgili kişinin 2018 Ocak ayından 2020 yılının Eylül ayına kadar olan süre içerisinde, doktor ile arasında aktif bir hasta-doktor ilişkisinin bulunmadığı, doktor tarafından telefon numarasının ilgili kişinin kendisinden alındığının beyan edildiği bu çerçevede söz konusu iletişim verisinin hasta doktor ilişkisi çerçevesinde muayene/televi süreçlerine ilişkin bilgilendirme amacıyla temin edildiğinin anlaşıldığı ancak daha sonra doktor tarafından reklam içerikli SMS göndermek amacıyla ilgili kişinin telefon numarasının işlendiği ve bu işlemenin de ilgili kişinin açık rızasına ya da Kanun'un 5'inci maddesinde yer alan diğer işleme şartlarından herhangi birine dayanmadığının anlaşıldığı

değerlendirmelerinden hareketle;

- Eldeki bilgi ve belgeler çerçevesinde söz konusu kişisel verilerin hastanenin veri tabanından alındığının tevsik edilemediği dikkate alındığında hastane hakkında Kanun kapsamında yapılacak bir işlem bulunmadığına,

- Veri sorumlusu doktor tarafından telefon numarasının ilgili kişinin kendisinden alındığının beyan edildiği bu çerçevede söz konusu iletişim verisinin hasta doktor ilişkisi çerçevesinde muayene/televi

süreçlerine ilişkin bilgilendirme amacıyla temin edildiğinin anlaşıldığı ancak daha sonra doktor tarafından reklam içerikli SMS göndermek amacıyla ilgili kişinin telefon numarasının işlendiği dikkate alındığında söz konusu kişisel veri işleme faaliyetinin Kanun'un 5'inci maddesinde yer alan herhangi bir işleme şartına dayanmadığına, bu kapsamda Kanun'un 12'nci maddesine aykırı uygulamada bulunan gerçek kişi veri sorumlusu doktor hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL idari para cezası uygulanmasına karar verilmiştir.

2022/902 sayılı KVKK Kararı

İlgili kişinin açık rızası alınmadan pazarlama amacıyla kısa mesaj gönderilmesi suretiyle kişisel verilerinin işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 02/09/2022 tarihli ve 2022/902 sayılı Karar Özeti

Karar Tarihi : 02/09/2022

Karar No : 2022/902

Konu Özeti: İlgili kişinin açık rızası alınmadan pazarlama amacıyla kısa mesaj gönderilmesi suretiyle kişisel verilerinin işlenmesi

Kuruma intikal eden şikâyetle özetle; veri sorumlusu şirket ile herhangi bir ticari faaliyette bulunulmamasına ve bu kapsamda iletişim onayı verilmemesine rağmen, aydınlatma yükümlülüğü yerine getirilmeden ve açık rızası alınmadan ilgili kişiye pazarlama amacıyla mesaj gönderildiği, veri sorumlusuna yapılan başvurunun cevabında, ilgili kişiden yanlışlık için özür dilenerek ilgili kişi tarafından pazar yerlerinden alışveriş yapılmış olması nedeniyle sistemin, cari kodunu sabit müşterileri gibi tanımlaması nedeniyle ilgili kişiye kısa mesaj gönderildiğinin ve başvuru akabinde gerekli düzeltmelerin yapıldığının belirtildiği ifade edilerek veri sorumlusu hakkında 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabî yazıda özetle;

- İlgili kişinin pazar yeri olarak hareket eden bir satış platformundaki veri sorumlusunun mağazasından alışveriş yaptığı ve kendilerindeki bilgilerin kaynağının bu alışverişe istinaden kesilen faturadan kaynaklı olduğu,
- Veri sorumlusu şirkete ait olan firmalardan birinin internet sitesinde kendi rızasıyla e-posta ya da kısa mesaj alabilmek için onay veren müşterilerine/üyelerine gitmesi gereken mesajın sehven veri sorumlusunun satış platformundaki mağazalarından alışveriş yapan müşterilerine gönderilmiş olduğu, yapılan yanlışın fark edilmesi üzerine iptal işleminin başlatıldığı fakat bazı müşterilere kısa mesaj gitmesine engel olunamadığı, gönderilen mesajların bazılarının iletildiği bazılarının iletilemediği,

- İlgili yazılım firması ile görüşüldüğü ve hatalı gönderim yapılsa dahi kısa mesaj ve e-posta gönderilmemesi için gerekli önlemlerin alındığı

ifade edilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 02/09/2022 tarih ve 2022/902 sayılı sayılı Kararı ile;

- Kanun'un "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, "belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza", (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi" olarak tanımlandığı,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi; fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin kendisi tarafından alenileştirilmiş olması; bir hakkın tesisi, kullanılması veya korunması için veri işleminin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hükmünün yer aldığı,

- Kanun'un "Veri Güvenliğine İlişkin Yükümlülükler" başlıklı 12'nci maddesinin (1) numaralı fıkrasında "Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri

almak zorundadır.” düzenlemesinin, (5) numaralı fıkrasında ise “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” düzenlemesine yer verildiği,

- Somut olayda veri sorumlusu firmaya ait internet sitesinden SMS/e-posta alabilmek için onay veren müşterilere gönderilmesi gereken mesajın sehven veri sorumlusunun satış platformundaki mağazalarından alışveriş yapan müşterilere gönderilmiş olduğu, yapılan yanlıştın fark edilmesi ile iptal işlemleri başlatılmışsa da bazı müşterilere kısa mesaj iletilmesine engel olunamadığı dikkate alındığında; veri sorumlusunun Kanun’un 5’inci maddesinde yer alan işleme şartlarından herhangi birine dayanmaksızın ilgili kişinin kişisel verisini işlediği, öte yandan şikâyet konusunun veri ihlal niteliği arz ettiği ancak bu hususta veri sorumlusunun Kanun’un 12’nci maddesinin (5) numaralı fıkrası kapsamında Kuruma bir bildirim yapmadığı

değerlendirmelerinden hareketle;

- Veri sorumlusu tarafından verilen yanıtta firmalarına ait olan internet sitesinde kendi rızasıyla e-posta/SMS alabilmek için onay veren müşterilerine/üyelerine iletilmesi gereken mesajın sehven satış platformundaki mağazalarından alışveriş yapan müşterilerine gönderilmiş olduğu, yapılan yanlıştın fark edilmesi üzerine iptal işleminin başlatıldığı fakat bazı müşterilere kısa mesaj gitmesine engel olunamadığının beyan edildiği dikkate alındığında veri sorumlusunun Kanun’un 5’inci maddesinde yer alan işleme şartlarından herhangi birine dayanmaksızın ilgili kişinin kişisel verisi niteliğindeki telefon numarasını işlediği, bu çerçevede Kanun’un 12’nci maddesinin (1) numaralı fıkrası kapsamında kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı, öte yandan şikâyet konusunun veri ihlal niteliği arz ettiği ancak veri sorumlusunun gerçekleşen veri ihlali ile ilgili Kanun’un 12’nci maddesinin (5) numaralı fıkrası kapsamında Kurula bir bildirim yapmadığı kanaatine varıldığından Kanun’un 18’inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca veri sorumlusu hakkında 30.000 TL idari para cezası uygulanmasına,

- Bundan sonraki süreçlerde meydana gelebilecek veri ihlallerinde Kanun’un 12’nci maddesinin (5) numaralı fıkrası kapsamında ilgili kişilere ve Kurula bilgi verilmesi gerektiği hususunun veri sorumlusuna hatırlatılmasına

karar verilmiştir.

2022/896 sayılı KVKK Kararı

Veri sorumlusu eski işveren tarafından ilgili kişinin kişisel verilerinin yer aldığı adli yazışma bilgilerinin kardeşi ile paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 02/09/2022 tarihli ve 2022/896 sayılı Karar Özeti

Karar Tarihi : 02/09/2022

Karar No : 2022/896

Konu Özeti: Veri sorumlusu eski işveren tarafından ilgili kişinin kişisel verilerinin yer aldığı adli yazışma bilgilerinin kardeşi ile paylaşılması

Kuruma intikal eden şikâyette özetle; ilgili kişi ile veri sorumlusu arasındaki iş akdinin haklı nedenle feshedildiği tarihe kadar geçen sürede bir iş ilişkisinin mevcut olduğu, bu doğrultuda veri sorumlusu tarafından ilgili kişiye ait kimlik, iletişim, özlük, mesleki deneyim, sağlık verileri gibi birtakım kişisel verilerin işlendiği, ancak bu kişisel veri işleme faaliyetlerine ilişkin ilgili kişiye herhangi bir aydınlatma yapılmadığı, ayrıca birtakım kişisel veriler işlenirken ilgili kişinin açık rızasının alınmadığı, bunların yanı sıra veri sorumlusu işveren tarafından ilgili kişinin adının geçtiği ceza soruşturma dosyasında yer alan adli yazışma bilgilerinin dosya ile herhangi bir bağlantısı olmadığı halde ilgili kişinin kardeşinin e-posta adresine iletildiği, ilgili hususta veri sorumlusuna başvuru yapılmışsa da cevap alınmadığı belirtilerek veri sorumlusu hakkında 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabî yazıda özetle;

- Veri sorumlusunun işçi-işveren ilişkisi kapsamında tutmuş olduğu özlük dosyasında ilgili kişiye ait kimlik, iletişim, özlük, mesleki deneyim, sağlık verileri gibi kişisel verileri Kanun'un kişisel verilerin işleme şartlarını düzenleyen 5'inci maddesinin (2) numaralı fıkrasının (a), (c), (ç), (e) ve (f) bentlerine ve İş Kanunu'na dayanarak işlediği,
- Yasal yükümlülükler gereği oluşturulan işçi özlük dosyası haricinde ilgili kişinin açık rızasına bağlı olarak herhangi bir verisinin işlenmediği, ilgili kişiye ait özel nitelikli hiçbir kişisel verinin işlenmediği, ilgili kişiye ait kişisel verilerin yurt dışına aktarılmadığı,

- İş Kanunu kapsamındaki yasal yükümlülük gereği kendilerinden hangi gerekçeyle evrak talep edildiğinin işçilere bildirilmesiyle sözlü olarak aydınlatma yükümlülüğünün yerine getirildiği, bununla birlikte yazılı bir aydınlatma metninin bulunmadığı,
- İlgili kişinin başvurusuna iş yoğunluğu sebebiyle yasal süresi içinde cevap verilemediği,
- İlgili kişinin diğer birkaç eski çalışan ile birlikte veri sorumlusunun markasına ait yazılım programlarını başka şirketlere sattığı, sahte imzalar atarak şirketin müşterileriyle akdettiği sözleşmeleri şirket yönetiminin bilgisi, onayı ve vekaleti olmaksızın başka bir paravan şirkete devrettiği, markanın çevrimiçi eğitim portallarını izinsiz olarak aktardığı ve bu yolla haksız kazanç elde ettiği, bu kapsamda ilgili kişinin iş sözleşmesindeki ticari sır saklama, şirket yazılımlarını üçüncü kişilerle paylaşmama, gizlilik anlaşmalarına aykırı davranmama vb. yükümlülüklerle aykırı davrandığı,
- Veri sorumlusunun bu durumu öğrenir öğrenmez ilgili kişinin iş sözleşmesini haklı sebeple feshettiği, ilgili kişinin ofisten ayrılırken şirketin kendisine tahsis ettiği iş bilgisayarında hem şahsi hem de şirketin sağladığı e-posta hesabının oturumunu açık unuttuğu, bahse konu hesaplardaki yazışmalar incelendiğinde ilgili kişinin şirketin yazılım ve ticari sırlarını çalarken şirket uzantılı e-posta adresinden kendi şahsi e-posta hesaplarına yönlendirmeler yaptığının anlaşıldığı ve akabinde ilgili kişi hakkında Cumhuriyet Başsavcılığına suç duyurusunda bulunulduğu

ifade edilmiştir.

Veri sorumlusu tarafından, ilgili kişi hakkında Cumhuriyet Başsavcılığına suç duyurusunda bulunmasının nedenleri açıklanmış olmakla beraber bu suç duyurusuna ilişkin bilgilerin ilgili kişinin kardeşine iletilip iletilmediği, iletiliyse bunun hukuki gerekçesinin ne olduğu sorusuna herhangi bir yanıt verilmediğinden veri sorumlusunu muhatap ikinci bir yazı ile söz konusu hususlarda bilgi talep edilmiş ancak veri sorumlusu tarafından bu yazıya cevap niteliğinde herhangi bir bilgi ya da belge Kuruma iletilmemiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 02/09/2022 tarih ve 2022/896 sayılı sayılı Kararı ile;

- 6698 sayılı Kanun'un "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, "belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza", (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt

sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem”, (1) bendinde veri sorumlusunun, “kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi” olarak tanımlandığı,

- Kanun’un “Kişisel Verilerin İşlenme Şartları” başlıklı 5’inci maddesinin “(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür: a) Kanunlarda açıkça öngörülmesi. b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması. c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması. ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması. d) İlgili kişinin kendisi tarafından alenileştirilmiş olması. e) Bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması. f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması” hükmünü haiz olduğu,

- Kanun’un “Veri Güvenliğine İlişkin Yükümlülükler” başlıklı 12’nci maddesinin (1) numaralı fıkrasında “Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.” düzenlemesinin, (5) numaralı fıkrasında ise “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” düzenlemesinin yer aldığı,

Bu çerçevede;

Veri sorumlusu firma tarafından ilgili kişiye ait kimlik, iletişim, özlük, mesleki deneyim, sağlık verileri gibi birtakım kişisel verilerin işlendiği ancak ilgili kişinin açık rızasının alınmadığı iddiasına ilişkin olarak;

- Veri sorumlusu ile ilgili kişi arasında iş sözleşmesinin kurulmuş olduğu, veri sorumlusunun ilgili kişiye ait kimlik bilgilerini 4857 sayılı İş Kanunu’nun “İşçi Özlük Dosyası” başlıklı 75’inci maddesinin 1’inci fıkrasında yer alan “İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu

dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır. İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür” düzenlemesi uyarınca 6698 sayılı Kanun’un 5’inci maddesinin (2) numaralı fıkrasının (a) bendinde düzenlenmiş bulunan “kanunlarda açıkça öngörülme” şartına dayalı olarak; özlük dosyasında bulundurulması gereken şikayete konu diğer kişisel verileri ise anılan maddenin (ç) bendinde yer alan “veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması” şartına dayalı olarak işlediği,

Kişisel veri işleme faaliyeti çerçevesinde veri sorumlusunun aydınlatma yükümlülüğünü yerine getirmediği iddiasına ilişkin olarak;

- Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ’in 5’inci maddesi uyarınca aydınlatma yükümlülüğünün, veri sorumlusu ya da yetkilendirdiği kişi tarafından ilgili kişinin açık rızasına veya Kanun’daki diğer işleme şartlarına bağlı olarak kişisel veri işlenen her durumda sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanılmak suretiyle yerine getirilmesi gerektiği ve ispatının veri sorumlusuna ait bir yükümlülük olduğu,

- veri sorumlusunun aydınlatma yükümlülüğünün yerine getirildiğine ilişkin Kuruma tevsik edici herhangi bir belge göndermediği, arama motorları üzerinden yapılan araştırmada veri sorumlusuna ait internet sitesi incelendiğinde aydınlatma metnine yer verildiğinin görüntülendiği,

Veri sorumlusunun, ilgili kişinin kardeşinin e-posta adresine, ilgili kişinin adının geçtiği Savcılık şikayet dilekçesini ilettiği iddiasına ilişkin olarak;

- İlgili kişinin adının geçtiği ceza soruşturma dosyasında yer alan adli yazışma bilgilerinin ilgili kişinin kardeşinin e-posta adresine hiçbir bağlantısı bulunmadığı halde iletildiği iddiası incelendiğinde; veri sorumlusundan ilgili kişinin kardeşine iletildiği belirtilen e-postaların içeriğinde “Bu doküman ekindeki yazışma ve kanıtlarla 500 sayfalık bir dosya ve kitapçık haline de getirildi, dava süreçleri yavaş işleyebilir, ama bu belgeler sizin eve, ana baba evlerinize, çalıştığınız şirkete özel olarak teslim ediliyor, adresleri ancak bulabildik.” ifadesine yer verildiği, aynı e-postanın ekinde bir hukuk bürosu tarafından Cumhuriyet Başsavcılığına iletilen şikayet dilekçesine yer verildiği, bahse konu şikayet dilekçesinin şüpheliler kısmında sadece ilgili kişiye değil, diğer pek çok gerçek ve tüzel kişiye ilişkin bilgilere de yer verildiğinin anlaşıldığı,

- Bununla birlikte veri sorumlusunun ilgili kişiye ait Savcılık şikayet dilekçesini hangi hukuki gerekçe ile ilgili kişinin kardeşi ile paylaştığı iddiasına cevap vermediği,

- İlgili kişinin kardeşinin e-posta adresine veri sorumlusu tarafından iletilen dosyalar incelendiğinde iletilerde dört farklı gerçek kişinin kişisel verilerinin de hukuka aykırı şekilde paylaşıldığının görüldüğü, paylaşma işleminin Kanun'un 5'inci maddesinde yer alan kişisel verilerin işlenmesi şartlarından herhangi birine dayanmadığı, bu kapsamda, veri sorumlusunun Kanun'un 12'nci maddesinin (1) numaralı fıkrasında yer alan kişisel verilerin hukuka aykırı olarak işlenmesini önlemeye yönelik gerekli her türlü teknik ve idari tedbirleri alma yükümlülüğüne aykırı hareket ettiği,

İlgili kişi tarafından yapılan başvurunun, veri sorumlusu tarafından cevapsız bırakıldığı iddiasına ilişkin olarak;

- Kanun'un "Veri sorumlusuna başvuru" başlıklı 13'üncü maddesinin (1) numaralı fıkrasında "İlgili kişi, bu Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir." düzenlemesi, (2) numaralı fıkrasında "Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır." ve (3) numaralı fıkrasında "Veri sorumlusu talebi kabul eder veya gerekçesini açıklayarak reddeder ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir." düzenlemesi ile Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in (Tebliğ), "Başvuruya cevap" başlıklı 6'ncı maddesinin (1) numaralı fıkrasında "Veri sorumlusu bu Tebliğ kapsamında ilgili kişi tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlüdür." düzenlemesi, 5'inci fıkrasında ise "Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır." düzenlemesine karşılık veri sorumlusunun Kanun'a ve Tebliğ'e aykırı davranarak ilgili kişinin başvurusuna yasal süreler içerisinde cevap vermediği

değerlendirmelerinden hareketle;

- Veri sorumlusu ile ilgili kişi arasındaki iş sözleşmesi kapsamında ilgili kişiye ilişkin kimlik bilgilerinin 6698 sayılı Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (a) bendinde düzenlenmiş bulunan "kanunlarda açıkça öngörülme" şartına dayalı olarak; özlük dosyasında bulundurulması gereken şikayete konu diğer kişisel veri içeren belgelerin ise anılan maddenin (ç) bendinde yer alan "veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" şartına dayalı

olarak işlendiği değerlendirildiğinden kişisel veri işleme faaliyeti açısından veri sorumlusu hakkında Kanun kapsamında herhangi bir işlem tesis edilmesine yer olmadığına,

- Veri sorumlusu tarafından ilgili kişiye ve başka gerçek kişilere ait kişisel verileri barındıran Savcılık şikayet dilekçesinin olayla herhangi bir ilgisi olmadığı anlaşılan ve ilgili kişinin kardeşi olduğu belirtilen üçüncü bir kişiye e-posta yoluyla iletilmesi işleminin, Kanun'un 5'inci maddesinde yer alan kişisel verilerin işlenmesi şartlarından herhangi birine dayanmadığı ve bu kapsamda veri sorumlusunun Kanun'un 12'nci maddesinin (1) numaralı fıkrasında yer alan kişisel verilerin hukuka aykırı olarak işlenmesini önlemeye yönelik gerekli her türlü teknik ve idari tedbirleri alma yükümlülüğüne aykırı hareket ettiği değerlendirildiğinden veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 150.000 TL idari para cezası uygulanmasına,

- İlgili kişinin kişisel verilerinin işlenmesine ilişkin aydınlatılmadığını iddia ettiği, veri sorumlusunun kişisel veri işlenmesine ilişkin sözlü olarak aydınlatma yapıldığını beyan ettiği ancak bu konuda tevsik edici bir belgenin Kuruma iletilmemiş olduğu, bununla birlikte Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin 5'inci maddesinin (1) numaralı fıkrasının (e) bendi uyarınca aydınlatma yükümlülüğünün yerine getirilip getirilmediğinin ispatının veri sorumlusuna ait bulunduğu hususları dikkate alındığında, veri sorumlusunun çalışanlara ilişkin kişisel veri içeren bilgi ve belgeleri özlük dosyasında muhafaza etmek suretiyle işleme hakkında ilgili kişileri aydınlatması gerektiği ve bu doğrultuda aydınlatma yükümlülüğünün Tebliğ'in ilgili hükümleri uyarınca yerine getirilmesinde gerekli dikkat ve özeni göstermesi hususunun veri sorumlusuna hatırlatılmasına,

- Veri sorumlusunun Kanun ve Tebliğ'den doğan "ilgili kişinin başvurusunun cevaplandırılması" yükümlülüğünü yerine getirmediği anlaşıldığından, veri sorumlusunun ilgili kişilerin yaptığı başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak ve Kanun ile Tebliğ'de öngörülen süreler içerisinde cevaplandırması gerektiği konusunda uyarılmasına; ayrıca ilgili kişinin taleplerinin yanıtı bırakıldığı dikkate alındığında veri sorumlusunun, ilgili kişiye başvurusunda talep ettiği hususlara ilişkin açıklayıcı ve detaylı bir şekilde cevap vermesi ve ilgili kişiye verilen cevaba ve cevabın ilgili kişi tarafından tebellüğ edilip edilmediğine ilişkin tevsik edici belgeyle birlikte Kurula bilgi vermesi gerektiği yönünde talimatlandırılmasına,

- Öte yandan veri sorumlusunun Kurumun ikinci yazısına da cevap vermediği dikkate alındığında bundan sonraki süreçte Kurumca istenilen bilgi ve belge taleplerine zamanında cevap verilmesi hususunda uyarılmasına,

- Őikâyet konusunun veri ihlali niteliđi arz ettiđi, bu çerçevede bundan sonraki süreçlerde meydana gelebilecek veri ihlallerinde Kanun'un 12'nci maddesinin (5) numaralı fıkrası kapsamında ilgili kişilere ve Kurula bilgi verilmesi gerektiđi hususunun veri sorumlusuna hatırlatılmasına karar verilmiştir.

2022/863 sayılı KVKK Kararı

Bir bankanın müşteri hizmetlerinin aydınlatma yükümlülüğünü yerine getirmeden ve açık rızasını almadan ilgili kişiyi telefonla aramak suretiyle kişisel verilerini işlemesi hakkında Kişisel Verileri Koruma Kurulunun 01/09/2022 tarihli ve 2022/863 sayılı Karar Özeti

Karar Tarihi : 01/09/2022

Karar No : 2022/863

Konu Özeti: Bir bankanın müşteri hizmetlerinin aydınlatma yükümlülüğünü yerine getirmeden ve açık rızasını almadan ilgili kişiyi telefonla aramak suretiyle kişisel verilerini işlemesi

Kuruma intikal eden şikâyetle özetle; ilgili kişinin başka bir bankada bulunan hesabından veri sorumlusu bankada bulunan üçüncü tarafa ait bir hesaba para gönderdiği, akabinde kendisiyle iletişim kurulmasına ilişkin rıza vermediği ve tarafına herhangi bir aydınlatma yapılmadığı halde veri sorumlusu banka tarafından tanıtım amacıyla aynı gün telefonla arandığı, ilgili hususta veri sorumlusu bankaya başvurduğu, posta gönderi takibinden banka tarafından başvurunun teslim alındığı görüntülenmişse de yasal süresi içerisinde cevap verilmediği belirtilerek veri sorumlusu hakkında 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabî yazıda özetle;

- Müşterilerin, Kanun kapsamındaki talep ve şikâyetlerini kimlik, tevsik edici belgeler ve talebi içeren dilekçe ile şubelere bizzat elden veya noter kanalıyla, KEP adresine, güvenli elektronik imza, mobil imza ya da bankaya daha önce bildirilen ve sistemlerinde kayıtlı bulunan elektronik posta adresleri kullanılmak suretiyle iletmeleri gerektiği, bu itibarla ilgili kişinin Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in (Tebliğ) 5'inci maddesine uygun olmayan başvurusu ile Kanun'un 14'üncü maddesi kapsamında Kurula şikâyet yoluna gitmesinin mümkün olmadığı,
- İlgili kişinin başvuru dilekçesinin bankaya tebliğ edilmesi ile birlikte, başvurunun Merkezi Operasyonlar Bölüm Başkanlığı tarafından Bildirim Yönetim Sistemine (BYS) aktarıldığı, ilgili kişinin

sistemde kayıtlı olan e-posta adresine “Dilekçenize konu hususlar ilgili birimimize iletilmiş olup, en kısa sürede tarafınıza dönüş gerçekleştirilecektir.” açıklaması ile e-posta gönderildiği,

- Müşteri bildirimının bankaya “posta” kanalı ile geldiği, dolayısıyla müşteri kimlik doğrulaması yapılan kanallar ile başvuru bankaya iletilmediğinden Kanun kapsamında değerlendirilebilmesi için başvurunun iletilmesi gereken kanallar hakkında ilgili kişiye bilgi vermek amacıyla cevabın ilgili kişinin banka sisteminde kayıtlı olan posta adresine iletilerek ilgili bildirim sonuçlandırıldığı,

- İlgili kişinin başvuru dilekçesinde yer alan posta ve e-posta adresinin banka kayıtlarında yer alan adreslerden farklı olduğu, banka kayıtlarında bulunan resmi imza örnekleri ile başvuru dilekçesinde yer alan imzaların da uyuşmadığı görüldüğünden banka cevabının müşterinin sistemde kayıtlı olan adresine gönderildiği, adi posta ile gönderildiğinden cevabın müşteriye ulaşıp ulaşmadığının teyit edilemediği,

- Pandemi süreci ile birlikte Bildirim Yönetim Sistemine gelen bildirimlerin geçen yıla oranla 3 kat arttığı, bildirim açıldığı tarih olan 06.07.2020 tarihi itibarıyla Bildirim Yönetim Sisteminde bulunan bildirim adedinin yaklaşık 47 bin olduğu, mevcut personel kadrosu ile bildirimlerin sonuçlandırılmaya çalışıldığı ancak gelen bildirim sayısındaki olağanüstü artış nedeni ile söz konusu bildirim farklı tarihlerde ara bilgilendirme ve sonuç bilgilendirmesi yapılabildiği,

- İlgili kişinin başvurusuna da her ne kadar Kanun kapsamında geçerli bir başvuru olmasa da gerekli işlem yapılarak akabinde müşteriye konu hakkında bilgi de verildiği, Kuruma yapılan şikayetten önce banka tarafından işlem yapıldığından, şikayetin konusuz kaldığı, haklı ve yasal dayanağın da bulunmadığı,

- Banka tarafından ilgili kişiye iki konu için arama yapıldığı; ilk aramanın ilgili kişinin açık rıza beyanının öğrenilmesi için Banka Müşteri İletişim Merkezi tarafından gerçekleştirildiği, söz konusu görüşmede ilgili kişinin onay vermeyeceğinin öğrenildiği ancak müşteriye doğrulamadan ret bilgisi banka tarafından sisteme kaydedilemeyeceğinden bilgi vermek için görüşmeye devam edilmek istendiği fakat ilgili kişi tarafından müşteri temsilcisinin konuşmasına fırsat verilmediği ve konuyla ilgili şubeden bilgi alabileceğinin belirtildiği esnada telefonun ilgili kişi tarafından kapatıldığı; ikinci aramanın ise internet bankacılığı ürünü sahibi olan ancak bu ürünü kullanmayan ve iletişim izni olan tüm müşterilere yapılan dış arama kapsamında gerçekleştirildiği, bu aramada müşterinin bir sorun yaşayıp yaşamadığının sorulduğu, şifresi yoksa şifre oluşturabileceği yönünde bilgi/hizmet verildiği, yeni bir ürün hizmet tanıtımı ya da satışının yapılmadığı, ancak ilgili kişinin detaylı bilgi vermeye fırsat vermeden onayı olmadan arandığı için şikayetini iletmediği,

- İlgili kişinin kişisel verilerinin banka tarafından işlenmesine yönelik hukuka aykırılığın bulunmadığı; müşterilerin kişisel verilerinin de banka ile girmiş oldukları sözleşmesel ilişki ve yasal yükümlülükler sebebi ile işlendiği, ilgili kişinin iletişim izni 01.08.2015 tarihinden bu yana “evet” olarak görüldüğünden banka tarafından ilgili kişinin açık rıza beyanının öğrenilmesi ve 12.01.2016 tarihinden itibaren sahip olduğu ve kullanmadığı internet bankacılığı ile ilgili bir sorun yaşayıp yaşamadığının öğrenilmesi amacıyla, banka ile ilgili kişi arasında mevcut olan sözleşmesel ilişki kapsamında arandığı,

- İlgili kişinin Kuruma iletilen şikâyet dilekçesindeki hususların gerçeği yansıtmadığı, başvurunun ilgili kişinin kötü niyetini açık bir şekilde ortaya koyduğu ifade edilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 01/09/2022 tarih ve 2022/863 sayılı sayılı Kararı ile;

- 6698 sayılı Kanun’un “Tanımlar” başlıklı 3’üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, “belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza”, (ç) bendinde ilgili kişinin, “kişisel verisi işlenen gerçek kişi”, (d) bendinde kişisel verinin, “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi”, (e) bendinde kişisel verilerin işlenmesinin, “kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem”, (ı) bendinde veri sorumlusunun, “kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi” olarak tanımlandığı,

- Kanun’un “Kişisel Verilerin İşlenme Şartları” başlıklı 5’inci maddesinin “(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür: a) Kanunlarda açıkça öngörülmesi. b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması. c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması. ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması. d) İlgili kişinin kendisi tarafından alenileştirilmiş olması. e) Bir hakkın tesisi, kullanılması veya korunması için veri

işlemenin zorunlu olması. f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması” hükmünü haiz olduğu,

- İlgili kişinin Kanun’un 13’üncü maddesi uyarınca veri sorumlusuna başvurusunu posta yoluyla yazılı olarak iletmediği, başvurusunda Tebliğ’in “Başvuru Usulü” başlıklı 5’inci maddesinde belirtilen ad-soyad, imza, T.C. kimlik numarası, e-posta adresi, tebligata esas yerleşim yeri adresi ile Kanun’un 11’inci maddesinde yer alan hakları çerçevesinde taleplerine ve başvuru ekinde de kimlik fotokopisine yer verdiği, veri sorumlusu tarafından ise ilgili kişinin başvurusunda yer alan adresten farklı olan ancak banka sistemlerinde kayıtlı olan adrese başvurunun zorunlu unsurlarının eksik olması sebebiyle kabul edilmediği şeklinde cevap verildiği, bahse konu yazının adi posta ile gönderilmiş olması sebebiyle ilgili kişiye ulaşım ulaşılmadığının banka tarafından tespit edilemediği, ilgili kişinin Kanun ve Tebliğ’e uygun olarak veri sorumlusuna başvurduğu, veri sorumlusunun cevabının otuz günlük yasal süreden sonra gönderildiği ve bu cevabın da ilgili kişiye tebliğ edildiğinin veri sorumlusunca ispat edilememiş olduğu dikkate alındığında ilgili kişinin Kanun’un 14’üncü maddesi uyarınca cevap verilmemiş olması gerekçesiyle “...başvuru tarihinden itibaren altmış gün içinde” Kuruma şikayette bulunmasında usul açısından herhangi bir hukuka aykırılık görülmediği,

- Öte yandan ilgili kişilerin Kanun’un 11’inci maddesi kapsamındaki başvurularına cevaben düzenlenen yazıların "adi posta" ile gönderilmesinin kişisel bilgi içeren söz konusu belgelerin ilgisi olmayan üçüncü kişilerin eline geçmesine ve dolayısıyla güvenlik açığına sebebiyet verebileceğinin değerlendirildiği,

- Kanun’un 5’inci maddesinde kişisel verilerin işleme şartlarından biri olarak sayılan açık rızanın Kanun’un 3’üncü maddesinde “belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza” şeklinde tanımlandığı ve dolayısıyla “belirli bir konuya ilişkin olma”, “bilgilendirmeye dayanma” ve “özgür iradeyle açıklanma” şeklinde üç unsuru bulunduğu, bu doğrultuda veri sorumlusu tarafından açık rıza beyanının hangi konuya ilişkin olarak istenildiğinin açıkça ortaya konulmasının ve ilgili kişinin özgür bir şekilde rıza gösterebilmesi için neye rıza gösterdiğini de bilmesi gerektiği, kişinin yalnızca konu üzerinde değil rızasının sonuçları üzerinde de tam bir bilgi sahibi olması gerektiği, bu sebeple bilgilendirmenin veri işleme ile ilgili bütün konularda açık ve anlaşılır bir biçimde gerçekleştirilmesi ve mutlaka kişisel verinin işlenmesinden önce yapılması gerektiği,

- 01.08.2015’ten bu yana ilgili kişinin iletişim izninin “evet” olarak görüldüğü, buna istinaden eksik olduğu anlaşılan açık rıza beyanının öğrenilmesi ve 12.01.2016’dan itibaren sahip olduğu ancak aktif

olarak kullanmadığı tespit edilen internet bankacılığı ile ilgili sorun yaşayıp yaşamadığının öğrenilmesi amacıyla iki defa arandığı, Kanun'un "Geçiş Hükümleri" başlıklı Geçici 1'inci maddesinin üçüncü fıkrasında "... Kanunun yayımı tarihinden önce hukuka uygun olarak alınmış rızalar, bir yıl içinde aksine bir irade beyanı bulunulmaması halinde, bu Kanuna uygun kabul edilir." hükmüne yer verildiği, Kanun'un yayımından önce mevcut hukuk kurallarına uygun olarak alınmış rızaların bir yıl içinde ilgili kişilerce aksi bir irade beyanında bulunulmadığı sürece geçerli olduğu, bu durumda yeni rıza alınmasına ya da güncellenmesine gerek olmadığı,

- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'un (6563 sayılı Kanun) "Tanımlar" başlıklı 2'nci maddesinde "ticari elektronik ileti"nin; telefon, çağrı merkezleri, faks, otomatik arama makineleri, akıllı ses kaydedici sistemler, elektronik posta, kısa mesaj hizmeti gibi vasıtalar kullanılarak elektronik ortamda gerçekleştirilen ve ticari amaçlarla gönderilen veri, ses ve görüntü içerikli iletiler olarak tanımlandığı, "Ticari elektronik ileti gönderme şartı" başlıklı 6'ncı maddesinin birinci fıkrasında "Ticari elektronik iletiler, alıcılara ancak önceden onayları alınmak kaydıyla gönderilebilir. Bu onay, yazılı olarak veya her türlü elektronik iletişim araçlarıyla alınabilir. Kendisiyle iletişime geçilmesi amacıyla alıcının iletişim bilgilerini vermesi hâlinde, temin edilen mal veya hizmetlere ilişkin değişiklik, kullanım ve bakıma yönelik ticari elektronik iletiler için ayrıca onay alınmaz." hükmüne yer verildiği,

- 6563 sayılı Kanun'a dayanılarak hazırlanan Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmeliğin (Ticari İletişim Yönetmeliği) "Onay gerektirmeyen durumlar" başlıklı 6'ncı maddesinde de "Alıcının kendisiyle iletişime geçilmesi amacıyla iletişim bilgilerini vermesi hâlinde, temin edilen mal veya hizmetlere ilişkin değişiklik, kullanım ve bakıma yönelik ticari elektronik iletiler için ayrıca onay alınmaz. Devam eden abonelik, üyelik veya ortaklık durumu ile tahsilat, borç hatırlatma, bilgi güncelleme, satın alma ve teslimat veya benzeri durumlara ilişkin bildirimleri içeren iletiler ile hizmet sağlayıcıya ilgili mevzuatla getirilen bilgi verme yükümlülüğü durumlarında önceden onay alma zorunluluğu aranmaz. Ancak bu tür bildirimlerde herhangi bir mal veya hizmet özendirilemez veya bunların tanıtımı yapılamaz." düzenlemesine yer verildiği,

- 6563 sayılı Kanun'un 6'ncı maddesi ile Ticari İletişim Yönetmeliği'nin 6'ncı maddesi uyarınca, devam eden abonelik sebebiyle, veri sorumlusu tarafından herhangi bir mal veya hizmet özendirilmesi ya da tanıtımı yapılmaksızın, ilgili kişinin kendisiyle iletişime geçilmesi amacıyla veri sorumlusu bankayla paylaşmış olduğu cep telefonu bilgisinin, banka tarafından ilgili kişinin eksik olduğu anlaşılan açık rızasının alınmasına yönelik bilgilendirilmesi ile 12.01.2016'dan bu yana sahip olunan internet bankacılığı hizmeti ile ilgili olarak yine farklı bir ürün tanıtımı yapılmaksızın

bilgilendirilmesi amacıyla aranmasının 6698 sayılı Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (a) bendinde yer alan "Kanunlarda açıkça öngörülme" hukuki işleme şartına dayalı olarak gerçekleştirildiği kanaatine varıldığı,

- İlgili kişinin veri sorumlusu tarafından kişisel verilerinin işlenmesine yönelik aydınlatılmadığını, veri sorumlusunun aydınlatma yükümlülüğünü yerine getirmediğini iddia ettiği, veri sorumlusu bankaya ilgili hususun sorulduğu ancak alınan cevabi yazıda buna ilişkin herhangi bir açıklamaya yer verilmediği,

- Veri sorumlularının aydınlatma yükümlülüğünün Kanun'un 10'uncu maddesinin (1) numaralı fıkrasında "Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; a) Veri sorumlusunun ve varsa temsilcisinin kimliği, b) Kişisel verilerin hangi amaçla işleneceği, c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi, d) 11 inci maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür" şeklinde düzenlendiği,

- Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'de (Aydınlatma Tebliği) de veri sorumluları veya yetkilendirdiği kişiler tarafından aydınlatma yükümlülüğü kapsamında uyulacak usul ve esaslar belirlenmiş olup anılan Tebliğ'in 5'inci maddesinin (1) numaralı fıkrasının (a) bendinde "İlgili kişinin açık rızasına veya Kanundaki diğer işleme şartlarına bağlı olarak kişisel veri işlendiği her durumda aydınlatma yükümlülüğü yerine getirilmelidir" hükmüne, (f) bendinde ise "Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir." hükmüne yer verildiği,

- İlgili kişinin kişisel verisi olan cep telefonu numarası bilgisinin tanıtım amacıyla açık rızasına ya da Kanun'da yer alan diğer işleme şartlarına dayalı olarak işlendiği hususunda aydınlatıldığına dair Kurumca talep edilmiş olmasına rağmen veri sorumlusu tarafından herhangi bir bilgi verilmemiş olması sebebiyle konu hakkında veri sorumlusunun web sitesi üzerinde inceleme yapıldığı, veri sorumlusunun web sitesinde "Bize Ulaşın" sekmesi altında "Kişisel Verilerin İşlenmesi ve Korunması Hakkında Bilgilendirme"nin bulunduğu, bu bölüme girildiğinde "Veri Sorumlusunun Aydınlatma Yükümlülüğü" başlıklı 10'uncu maddesi kapsamında veri sorumlusunun kimliğine, kişisel verilerin hangi amaçla işleneceğine, kişisel verilerin kimlere ve hangi amaçla aktarılabileceğine, kişisel veri toplamanın yöntemi ve hukuki sebeplerine, ilgili kişinin Kanun'un 11'inci maddesinde sayılan haklarına yönelik asgari bilgilere yer vermek suretiyle genel aydınlatma yükümlülüğünün yerine getirildiği kanaatine varıldığı,

• Daha önce belirtildiği üzere Kanun'un "Geçiş Hükümleri" başlıklı Geçici'1 inci maddesinin (3) numaralı fıkrasında "Bu kanunun yayımı tarihinden önce işlenmiş olan kişisel veriler, yayımı tarihinden itibaren iki yıl içinde bu Kanun hükümlerine uygun hale getirilir. Bu Kanun hükümlerine aykırı olduğu tespit edilen kişisel veriler derhal silinir, yok edilir veya anonim hale getirilir. Ancak Kanunun yayımı tarihinden önce hukuka uygun olarak alınmış rızalar, bir yıl içinde aksine bir irade beyanı bulunulmaması halinde, bu Kanuna uygun kabul edilir." hükmünün yer aldığı,

• Şikâyete konu somut olayda, ilgili kişinin kişisel verilerinin ilk elde edilmesinin 6698 sayılı Kanun'un yürürlük tarihi öncesi (01.08.2015) olduğu, ilgili kişinin iletişim izninin anılan tarihten itibaren evet olarak görüldüğü, Kanun'un yürürlük tarihinden sonraki bir yıl içinde ilgili kişinin aksi yönde bir irade beyanının bulunmadığı ve banka tarafından sözlü olarak yapılmaya çalışılan aydınlatmanın ise kabul edilmediğinin anlaşıldığı

değerlendirmelerinden hareketle;

• İlgili kişinin kendisiyle iletişime geçilmesi amacıyla veri sorumlusu bankayla paylaşmış olduğu cep telefonu bilgisinin, Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'un 6'ncı maddesi ile Ticari İletişim ve Ticari Elektronik İletiler Yönetmeliği'nin 6'ncı maddesinin (2) numaralı fıkrası uyarınca, devam eden müşteri ilişkisi sebebiyle, veri sorumlusu tarafından herhangi bir mal veya hizmet özendirilmesi ya da tanıtımı yapılmaksızın, kullanılmakta olan hizmete ilişkin bilgi verilmek amacıyla 6698 sayılı Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (a) bendinde yer alan "Kanunlarda açıkça öngörülme" hukuki işleme şartına dayalı olarak işlendiği kanaatine varıldığından, veri sorumlusu banka hakkında yapılacak bir işlem bulunmadığına,

• İlgili kişinin veri sorumlusuna posta yoluyla yazılı olarak ilettiği başvurusunun Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in 5'inci maddesinde belirtilen zorunlu unsurları içerdiği ve ilgili kişinin taleplerinin yanıtı bırakıldığı dikkate alındığında veri sorumlusunun Kanun'un 13'üncü maddesi kapsamında kendisine yapılan başvurulara ilişkin Tebliğ'in 6'ncı maddesine uygun olarak hareket etmesi gerektiği yönünde uyarıda bulunulmasına, ayrıca veri sorumlusunun, ilgili kişiye başvurusunda talep ettiği hususlara ilişkin açıklayıcı ve detaylı bir şekilde cevap vermesi ve ilgili kişiye verilen cevaba ve cevabın ilgili kişi tarafından tebellüğ edilip edilmediğine ilişkin tevsik edici (KEP Delili, e-posta ekran görüntüsü veya APS alımdısı niteliğindeki) belgeyle birlikte Kurula bilgi vermesi gerektiği yönünde talimatlandırılmasına,

• İlgili kişilerin Kanun'un 11'inci maddesi kapsamındaki başvurularına cevaben düzenlenen yazıların "adi posta" ile gönderilmesinin kişisel bilgi içeren söz konusu belgelerin ilgisi olmayan üçüncü kişilerin eline geçmesine ve dolayısıyla güvenlik açığına sebebiyet verebileceği değerlendirilmiş

olduğundan veri sorumlusunun Tebliğ'in 6'ncı maddesine uygun olarak ilgili kişilere göndereceği kişisel bilgi içeren cevapları daha güvenilir ve takip edilebilir bir yöntemle iletmesi hususunda uyarılmasına, ilgili kişinin 6698 sayılı Kanun'un yürürlük tarihi öncesi olan 2015 yılından beri bankanın müşterisi olduğu, iletişim izninin evet olarak görüldüğü, Kanun'un yürürlük tarihinden sonraki bir yıl içinde ilgili kişinin aksine bir irade beyanının bulunmadığı ve banka tarafından sözlü olarak yapılmaya çalışılan aydınlatmanın ise kabul edilmediği hususları dikkate alındığında, ilgili kişinin aydınlatma yükümlülüğünün yerine getirilmediği iddiasına yönelik veri sorumlusu banka hakkında yapılacak bir işlem bulunmadığına

karar verilmiştir.

2022/861 sayılı KVKK Kararı

İlgili kişinin internet arama motorlarında yapılan aramalardan elde edilen iş yeri e-postasının açık rızası alınmaksızın veri sorumlusu bir pazarlama şirketi tarafından ticarî elektronik ileti gönderilmesi suretiyle işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 01/09/2022 tarihli ve 2022/861 sayılı Karar Özeti

Karar Tarihi : 01/09/2022

Karar No : 2022/861

Konu Özeti: İlgili kişinin internet arama motorlarında yapılan aramalardan elde edilen iş yeri e-postasının veri sorumlusu bir pazarlama şirketi tarafından açık rızası alınmaksızın ticarî elektronik ileti gönderilmesi suretiyle işlenmesi

Kuruma intikal eden dilekçede özetle; ilgili kişinin herhangi bir bağlantısı olmadığı halde veri sorumlusu şirket tarafından ilgili kişinin iş e-posta adresine kampanya, reklam vb. içerikli e-posta gönderildiği, ilgili kişi tarafından veri sorumlusuna ait e-posta adresine başvuruda bulunularak iletişim bilgilerinin ve kimlik bilgilerinin nereden ve nasıl temin edildiğinin sorulduğu, tarafına reklam/kampanya içerikli e-postaların gönderilmemesinin, kişisel verilerinin imha edilmesinin ve imha edilen bilgiler hakkında tarafına bilgi verilmesinin talep edildiği ancak veri sorumlusu tarafından verilen cevapta sadece e-posta adresi ve bilgilerinin kayıtlardan silindiğinin belirtildiği, verilerinin nereden temin edildiğine ilişkin herhangi bir bilgi verilmediği ifade edilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin olarak başlatılan inceleme çerçevesinde veri sorumlusu şirketten savunması istenilmiş olup alınan cevabi yazıda özetle;

- Şirketlerinin avukat büroları için yazılımlar ürettiği ve pazarladığı, avukatlık bürolarına tanıtım faaliyetlerinde bulunmak için avukatlık bürolarında çalışan avukatların e-posta adreslerinin internet arama motorlarında yapılan aramalardan temin edildiği, burada bulunan bilgilerden kişinin sadece isim, çalıştığı büro adı ve e-posta adresi bilgilerinin sistemlerine kaydedildiği,
- Pazarlama içerikli e-postanın 6563 sayılı "Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'un 6'ncı maddesinde yer alan "Esnaf ve tacirlere önceden onay alınmaksızın ticari elektronik iletiler

gönderilebilir" hükmüne dayanılarak gönderildiği, ilgili e-postanın kişinin mesleği ile ilgili bir yazılım ürününün tanıtımı amaçlı olduğu,

- İlgili kişiye gönderilen e-postanın sonunda e-posta listesinden çıkılmasının talep edilebileceğine ilişkin "Bu E-Posta ile rahatsızlık verdiyse özür dileriz. E-Posta Listemizden Çıkmak için Tıklayınız" şeklinde bir metin ve bağlantının bulunduğu, ilgili kişinin bu bağlantıyı kullanarak firmaya talepte bulunduğu ve ilgili kişinin e-posta adresinin kayıtlardan silindiği, bünyelerindeki avukatlık büro adresleri ve kişisel verilerin başka hiçbir tüzel kişiliğe aktarılmadığı

ifade edilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 01/09/2022 tarihli ve 2022/861 sayılı Kararı ile;

- 6698 sayılı Kanun'un "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, "belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza", (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi" olarak tanımlandığı,

- Kanun'un 5'inci maddesinin kişisel verilerin işleme şartlarını düzenlediği, maddenin (1) numaralı fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin, (2) numaralı fıkrasında ise, kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda olan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün korunması için veri işlemenin zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaati için veri işlenmesinin

zorunlu olması hallerinde ilgili kişinin açık rızası olmaksızın kişisel verilerin işlenmesinin mümkün olduğunun hükme bağlandığı,

- İlgili kişinin kişisel verilerinin Kanuna aykırı olarak işlendiği iddiası bakımından yapılan incelemede; Karar tarihi itibarıyla arama motorlarında yapılan araştırmada, avukat sorgulamasına ilişkin hizmet veren çeşitli internet sitelerinde yer alan ilgili kişinin e-posta adresinin şikayet edilen adresten farklı olduğu, şikayete konu e-posta adresine internet ortamında erişilememiş olmakla birlikte şikayete konu olayın gerçekleştiği tarihte, veri sorumlusu tarafından belirtilen büroda çalıştığı ve veri sorumlusu tarafından bahse konu e-posta adresinin internet arama motorlarından temin edildiğinin beyan edildiği dikkate alındığında, şikayete konu e-posta hesabının da şikayet tarihinde internet arama motorları üzerinden herkesin erişimine açık olacak şekilde alenileştirildiği kanaatine varıldığı,

- Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (d) bendinde yer alan "ilgili kişinin kendisi tarafından alenileştirilmiş olması" şartı kapsamında kişisel verilerin açık rıza olmaksızın işlenmesinin mümkün olduğu, ancak ilgili verinin alenileştirilmiş olmasının diğer bir ifadeyle kamuya açık hale getirilmiş olmasının bu kişisel verilerin her türlü amaç için işlenebileceği anlamına gelmediği, ancak alenileştirme amacıyla bağlantılı ve amaçla sınırlı olarak işlenebileceği, şikayete konu somut olayda ise ilgili kişinin iş e-posta adresinin avukatlık mesleğine yönelik yapılacak iletişimler kapsamında aleni hale getirildiği, pazarlama/reklam amacıyla yapılacak işlemlere ilişkin bir alenileştirme iradesini içermediği,

- Diğer taraftan, veri sorumlusunun avukat olan ilgili kişinin e-posta adresini 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'un 6'ncı maddesinde yer alan "Esnaf ve tacirlere önceden onay alınmaksızın ticari elektronik iletiler gönderilebilir" hükmüne istinaden reklam amaçlı ileti göndermek suretiyle işlediğini belirtmesine karşın, 1136 sayılı Avukatlık Kanunu'nun "Avukatlıkla birleşemeyen işler" başlıklı 11'inci maddesinde "Aylık, ücret, gündelik veya kesenek gibi ödemeler karşılığında görülen hiçbir hizmet ve görev, sigorta prodüktörlüğü, tacirlik ve esnaflık veya meslekin onuru ile bağdaşması mümkün olmayan her türlü iş avukatlıkla birleşemez" hükmüne yer verilerek avukatların ne esnaf ne de tacir sıfatıyla hareket edemediği belirtildiğinden avukat olan ilgili kişiye bu hükme dayanılarak onay alınmaksızın ticari ileti gönderilemeyeceği,

- Dolayısıyla veri sorumlusunun Kanun'un 5'inci maddesi çerçevesinde herhangi bir kişisel veri işleme şartı bulunmaksızın veri işleme faaliyetinde bulunması sebebiyle Kanun'un 12'nci maddesinde yer alan "Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek" yükümlülüğüne aykırı davrandığı,

• Veri sorumlusu tarafından ilgili kişiye verilen yanıtın yetersiz olduğu iddiası bakımından yapılan incelemede; Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in (Tebliğ) 6'ncı maddesinin, "(1) Veri sorumlusu bu Tebliğ kapsamında ilgili kişi tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlüdür. (2) Veri sorumlusu, başvuruyu kabul eder veya gerekçesini açıklayarak reddeder. (3) Veri sorumlusu, cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir... (5) Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak, işlemin ayrıca bir maliyet gerektirmesi halinde, 7 nci maddede belirtilen ücret alınabilir. Başvurunun, veri sorumlusunun hatasından kaynaklanması hâlinde alınan ücret ilgiliye iade edilir." hükmünü haiz olduğu, veri sorumlusu tarafından ilgili kişinin başvurusuna verilen cevapta sadece kişisel verilerinin silindiği yönünde bilgi verildiği ancak ilgili kişinin Kanun'un 11'inci maddesi kapsamındaki diğer bilgi taleplerinin yanıtı bırakıldığı tespit edildiği,

• Veri sorumlusunun ilgili kişiye ve Kuruma ilettiği cevap yazılarında ilgili kişiye ait ve sistemlerinde kayıtlı olan kişisel verilerin sistem kayıtlarından silindiğini beyan etmesine karşılık silmeye ilişkin tevsik edici herhangi bir belge ibraz etmediği

değerlendirmelerinden hareketle;

• İlgili kişinin e-posta adres bilgisinin reklam ve pazarlama amacıyla işlenmesine yönelik herhangi bir platformda alenileştirme iradesinin bulunduğu dair veri sorumlusu tarafından kanıtlayıcı nitelikte bir belgenin Kuruma sunulmadığı, veri sorumlusunun ilgili kişinin kişisel verilerinin Kanunda yer alan işleme şartları kapsamında işlendiğine ilişkin açıklamalarının hukuki dayanaktan yoksun olduğu dikkate alındığında veri sorumlusunun Kanun'un 5'inci maddesi çerçevesinde herhangi bir kişisel veri işleme şartı bulunmaksızın veri işleme faaliyetinde bulunduğu kanaatine varıldığından veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 150.000 TL idari para cezası uygulanmasına,

• Veri sorumlusu tarafından ilgili kişinin başvurusuna verilen cevapta, ilgili kişinin Kanun'un 11'inci maddesi kapsamındaki bilgi taleplerinin yanıtı bırakılarak sadece kişisel verilerinin silindiği yönünde bilgi verilmesi sebebiyle Kanun'un 13'üncü maddesi kapsamında veri sorumlusunun kendisine yapılan başvurulara ilişkin Tebliğ'in 6'ncı maddesine uygun olarak hareket etmesi gerektiği yönünde uyarıda bulunulmasına; diğer taraftan ilgili kişiye başvurusunda talep ettiği hususlara ilişkin olarak açıklayıcı ve detaylı bir şekilde cevap vermesi ve ilgili kişiye verilen cevaba ve cevabın ilgili kişi tarafından tebellüğ edilip edilmediğine ilişkin tevsik edici (KEP Delili, e-posta

ekran görüntüsü veya APS alındısı niteliğindeki) belgeyle birlikte Kuruma bilgi vermesi gerektiği yönünde veri sorumlusunun talimatlandırılmasına,

- Veri sorumlusu tarafından Kuruma sunulan cevabi yazıda, ilgili kişinin talebi üzerine ilgili kişiye ait e-posta adresinin kayıtlardan silindiği bilgisi verilmekle birlikte silmeye ilişkin tevsik edici herhangi bir belgenin yazı ekinde sunulmadığı ve ilgili kişinin veri sorumlusuna başvurusunda kişisel verilerinin silinmesi talebini de iletmediğinden; veri sorumlusunun, ilgili kişinin kişisel verilerinin silinmesi, yok edilmesi veya anonim hâle getirilmesi ve buna ilişkin kayıtların Kuruma iletilmesi gerektiği yönünde talimatlandırılmasına

karar verilmiştir.

2022/853 sayılı KVKK Kararı

Bir yasal bahis platformu tarafından ilgili kişinin e-posta adresinin işlenerek bir üyesinin kişisel verilerinin üçüncü şahıs konumundaki ilgili kişinin e-posta adresine gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 01/09/2022 tarihli ve 2022/853 sayılı Karar Özeti

Karar Tarihi : 01/09/2022

Karar No : 2022/853

Konu Özeti: Bir yasal bahis platformu tarafından ilgili kişinin e-posta adresinin işlenerek bir üyesinin kişisel verilerinin üçüncü şahıs konumundaki ilgili kişinin e-posta adresine gönderilmesi

İlgili kişinin şikâyetinde özetle;

- Nisan 2022 içerisinde ilgili kişinin şahsi e-posta hesabı olan *****@gmail.com'a yasal bahis platformu olan *****.com tarafından bir e-postanın gönderildiği ve söz konusu e-postada özetle "Sayın ***** ***** , Üyelik işlemlerinizi ile ilgili detayları aşağıda bulabilirsiniz: Üye Numaranız: *****. Üye numaranız, kullanıcı adınız, TC kimlik numaranız ile *****.com hesabınıza giriş yapabilirsiniz. Güvenlik önlemi olarak *****.com'a giriş şifrenizi belirli aralıklarla değiştirmenizi tavsiye ediyoruz." denildiği, hemen ardından gelen ikinci bir e-posta ile ise "Sayın Üyemiz, E-posta adresinize reklam, promosyon vb. ticari elektronik iletilerin gönderilmesini onayladınız." denildiği,
- İlgili kişi tarafından *****.com sitesine herhangi bir üyeliğin asla gerçekleştirilmediği, bu çerçevede konuya ilişkin veri sorumlusuna başvurarak şahsına ait herhangi bir bilginin işlenmiş olması halinde, bunların derhal yok edilmesi talebinde bulunduğu ayrıca veri sorumlusunun sisteminde kullanıcılar tarafından girilerek beyan edilen e-posta adreslerinin doğruluğunu herhangi bir surette kontrol edilip edilmediğine yönelik sorularını yönelttiği,
- Veri sorumlusunun ise "İletmiş olduğunuz talebinize istinaden E-posta adresiniz kayıtlı olduğu üyelikten kaldırılmıştır." şeklinde cevap verdiği,
- Somut olayda 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) bakımından asıl sorunun veri sorumlusunun kişisel veriyi işlerken herhangi bir kontrol mekanizması oluşturmamış olması olduğu, üçüncü bir şahıs ilgili kişiye ait e-postayı sisteme üyelikte kullanmak istediğinde veri

sorumlusunun bunu doğrudan geçerli ve doğru kabul ederek ilgili kişinin e-posta adresine e-postalar göndermeye başlamakla hata yaptığı

beyan edilerek Kanun kapsamında gereğinin yapılması talep edilmiştir.

Yapılan şikâyete istinaden başlatılan inceleme çerçevesinde veri sorumlusu yasal bahis platformunu işleten şirketten savunması istenilmiş olup, alınan cevabi yazıda özetle;

- Şirketin ilgili mevzuat hükümleri uyarınca idareden aldığı yetki ile bizatihi idarenin düzenleyici olduğu bahis piyasasında faaliyet gösteren bir sanal ortam bayii olduğu,
- Şirketin yürüttüğü faaliyet kapsamında, kişisel verilerin korunmasına ilişkin mevzuata ilave olarak veri işleme bakımından iki önemli yükümlülüğünün bulunduğu, bu yükümlülüklerden ilkinin 18 yaşından küçük kimselerin şirket tarafından bayiliği yürütülen oyunları oynamalarının engellenmesi olduğu, ikinci yükümlülüğün ise suç gelirlerinin aklanmasına dair mevzuata uyum göstermek olduğu, bu çerçevede şirketin kendi nezdinde yapılan her türlü işlemde önce işlemi yapanların kimliklerini tespit etme ve gerekli diğer tedbirleri alma yükümlülüğünün bulunduğu,
- İlgili mevzuat kapsamında her bir üyelik başvurusunda şirket tarafından müşterinin (i) adı-soyadı, (ii) uyruğu ve (iii) T.C. kimlik numarası veya yabancı kimlik numarası bilgilerinin İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü veri tabanından teyit edildiği,
- Nisan 2022 içerisinde ilgili kişinin şikâyetine konu edilen e-posta adresi kullanılarak şirketin platformu üzerinden ***** numaralı üyeliğin oluşturulduğu,
- Söz konusu üyelik oluşturulurken cep telefonu numarasının doğrulandığı, kimlik bilgilerinin ise MERNİS sistemi üzerinden doğrulandığı, buna karşın e-posta adresinin kayıt aşamasında doğrulanmadığı,
- Sonrasında şikâyet sahibi ilgili kişi tarafından şirkete e-posta vasıtasıyla ulaşıldığı, söz konusu e-postada ilgili kişinin şirketin platformunda hesap açmadığını bildirdiği ve e-posta adresine ileti gönderilmemesini talep ettiği, ilgili kişiden gelen bildirim derhal işleme alındığı ve ilgili kişinin e-posta adresinin şirketin sistemlerinden kaldırıldığı,
- Akabinde ilgili kişiyle e-postasında paylaştığı telefon numarası üzerinden iletişime geçilerek konu hakkında bilgi verildiği, ayrıca ilgili kişinin talebi üzerine aynı bilgilerin yazılı olarak da ilgili kişiye gönderildiği,
- İlgili kişi tarafından Nisan 2022'de e-posta üzerinden şirkete yapılan talepte ilgili kişinin kimliğinin doğrulanmasını sağlayacak veri bulunmadığından tabii olarak taleplerinin tamamı hakkında ilgili

kişiyeye bilgi verilemediği, bununla birlikte şirketin tabi olduğu mevzuat gereğince uyguladığı risk temelli veri politikasına uygun olarak aynı gün içerisinde e-posta adresinin şirketin veri tabanından silindiği,

- Dolayısıyla ilgili kişi her ne kadar şirkete başvururken kendi kimliğinin tanımlanmasına imkân verecek bilgi paylaşmamışsa da yapmış olduğu başvuruda yer alan talebin tamamen karşılandığı ve 6698 sayılı Kanun'un 11'inci maddesinin (1) numaralı fıkrasının (d) bendi gereği yanlış işlendiği iddia edilen verinin aynı gün içerisinde Şirket tarafından silindiği,

- İlgili kişi tarafından -karşılanmış olan talebine ilişkin olarak Kanun'un 14'üncü maddesinde yer alan koşullar mevcut olmamasına rağmen- Kurula şikâyette bulunulduğu,

- Öncelikle ilgili kişinin veri sorumlusu sıfatıyla şirkete Nisan 2022 içerisinde göndermiş olduğu e-postada yer alan sorular kapsamındaki bilgilerin -ilgili kişi tarafından şirkete kimlik doğrulanmasına imkân verecek bir başvuru yapılmadığından- veri ihlâl riski nedeniyle paylaşılmadığı, bununla birlikte ilgili kişinin aslı talebi olan e-posta adresine bir daha gönderim yapılmaması talebinin şirketin veri yönetim politikası ile uyumlu olması nedeniyle derhal işleme alındığı ve ilgili kişinin talebinin aynı gün yerine getirildiği,

- İlgili kişi tarafından şirketin üye kaydı esnasında e-posta adresi verisini işlerken herhangi bir kontrol mekanizması işletmediğinin iddia edildiği, ayrıca e-posta adresinin bir iletişim verisi olduğunun ve kontrolsüzce kullanılmaya başlanmasının düşünülemeyeceğinin ifade edildiği,

- Öncelikle şirketin yürüttüğü faaliyetin ruhsata tabi bir faaliyet olduğunu, pek çok idari organın gözetim ve denetimi altında yürütüldüğünü ve özellikle de müşterinin kimlik doğrulaması ile ilgili olarak şirketin internet üzerinden servis sunan diğer veri sorumlularından ayrıştığını belirtmek istedikleri,

- Şirketin platformuna üye olabilmek için ilgili kişilerin ad soyad, doğum tarihi ve TC kimlik numarası verilerini doğru girmelerinin ve bu verilerin MERNİS üzerinden teyit edilmesinin zorunlu olduğu, dolayısıyla şirketin işlediği asgari sayıdaki veri içerisinde yer alan iletişim verilerinin kontrolsüzce işlenmediği, esasen pek çok çevrimiçi hizmet uygulaması üyeliğinin ötesinde bir kontrolden sonra toplandığı,

- Şirketin risk temelli veri güvenliği yaklaşımı uyarınca, üyelerin ana iletişim kanalı olarak cep telefonu numarasının kabul edildiği, bu nedenle de üyelik aşamasında öncelikle cep telefonu numarası verisinin doğrulamasının yapıldığı, sistemin ayrıca üyelik başvurusunda kullanılan cep

telefonu ve/veya elektronik posta adresinin başka bir üyelikte kullanılıp kullanılmadığını da otomatik olarak kontrol ettiği,

- Şirket veya herhangi bir yetkili sanal ortam bayi sistemindeki üyenin MERNİS üzerinden doğrulanan TC kimlik numarası ile uyuşmayan bir banka hesabından para yüklemesi veya para çekimi işlemi yapılamayacağından şirket bakımından teyidi ve korunması öncelikli olan verilerin ad-soyad, doğum tarihi ve TC kimlik numarası verileri olduğu, iletişim verilerinin ikincil önemi haiz olduğu,

- Öncelikle cep telefonu verisinin doğrulanmasının sebebinin ise şirket tarafından herhangi bir problem halinde müşteri ile ilk temas noktasının müşteri iletişim stratejisi gereği telefon aramaları olduğu, e-posta verisinin ikincil nitelikte olduğu,

- Şikâyete konu olayda da cep telefonu numarasının doğrulandığı ama e-posta adresinin doğrulanmadığı, e-posta adresinin doğrulanmaması halinde ilgili kişiye şirket tarafından yalnızca “Hoşgeldiniz” bilgilendirmesinin gönderildiği ve sistem üzerindeki panelde kişinin e-posta adresinin “Doğrulama Bekleniyor” aşamasında kaldığı, buna ilave olarak e-posta doğrulaması yapılmamış bir hesaptan şirketin platformuna her giriş yapıldığında ilgili kişiye e-posta doğrulamasına ilişkin uyarı penceresinin gösterildiği,

- E-posta doğrulaması yapıp yapılmadığından bağımsız olarak tüm üyelere ilk etapta yalnızca iki adet e-postanın gidebileceği, nitekim ilgili kişinin başvurusunda da bu iki e-postaya yer verildiği ve başkaca bir e-postanın sunulmadığı, bu nedenle kontrolsüzce e-posta ve hatta e-postalar gönderildiği iddiasının soyut ve dayanaktan yoksun olduğu,

- Şirket sistemi tarafından gönderilen e-postaların ilkinin “Hoşgeldiniz” bilgilendirmesi olduğu ve bu e-postanın üyeliğin başlatıldığına yönelik bilgilendirme içerdiği, “Hoşgeldiniz” bilgilendirmesinin içeriğinde yalnızca üyenin adı ve soyadı ile üyelik numarasının yer aldığı,

- Gönderimin amacının üyeliğin oluşturulduğuna dair bilgi vermek ve ilgili kişinin şirket hesabına nasıl giriş yapabileceğini açıklamak olduğu, ikinci olarak ise eğer üyelik başvurusu sırasında ilgili kişi ticari elektronik ileti gönderilmesine onay vermiş ise Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik’in 7’nci maddesinin (3) numaralı fıkrası uyarınca hukuki yükümlülüğün yerine getirilmesi adına ilgili kişiye ticari elektronik ileti onayının alındığı bilgisinin verildiği,

- Mezkûr madde uyarınca onayın elektronik ortamda alınması durumunda onayın alındığı bilgisinin reddetme imkânı da tanınmak suretiyle- alıcının elektronik iletişim adresine 24 saat içinde

iletilmesinin gerektiği, bu hükmün amacının esasen sehven bildirilen iletişim adreslerine ret imkânı sunmak olduğu,

- İkinci e-postanın bu kapsamda üyelik oluşturma sırasında ticari elektronik ileti gönderimine elektronik ortamda onay verilmiş olması sebebi ile iletildiği, nitekim gönderilen e-postada hatalı kayıt ihtimâline binaen çıkma hakkının tanındığı, bununla birlikte ticari elektronik iletinin alındığına ilişkin e-postada herhangi bir kişisel veriye yer verilmediği,
- Tekrar özetlemek gerekirse; şirketin platformuna üyelik başvurusu sırasında e-posta adresi verisi işlenirken öncelikle ilgili verinin şirket veri tabanında mevcut bir başka üye ile ilişkili olup olmadığının kontrol edildiği, eğer veri başka bir üyelik hesabı ile ilişkili değilse doğrulama zorunlu tutulmadan üyelik oluşturulduğu ve üyeye yalnızca yukarıda belirtilen iki bilgilendirme e-postasının iletilebildiği, üye ticari elektronik ileti onayı vermediyse kendisine yalnızca “Hoşgeldiniz” bildirimini yapıldığı,
- E-posta doğrulama işlemlerinin ise üyelik panelinde ilgili alandan doğrulama talebi yapıldığında e-posta adresine yönlendirilen iletideli adımlar izlenerek yapılabildiği, bu doğrulamaların üyenin bilgilendirme e-postalarını alabilmesinin ön şartı niteliğinde olduğu, dolayısıyla ilgili kişinin şikâyetinde iddia edildiği üzere şirket tarafından kontrolsüzce veri işlenmediği,
- Şirketin sistemi üzerinde üyelik esnasında verilen e-posta adresi için üyenin doğrulamaya zorlanmamasının başlıca nedeninin hesaba MERNİS sistemi ile uyuşacak şekilde para transferi yapılmadığı müddetçe salt şirket platformu üyeliğinin hüküm ifade etmemesi olduğu, daha açık bir ifadeyle herhangi bir üyenin şirketin platformu üzerinde işlem yaparak oyun oynayabilmesi için öncelikle platformdaki hesabına para transferi yapmasının gerektiği, bu aşamada para aktarımının üye tarafından yapıldığına MERNİS kontrolü neticesinde emin olunduğu,
- Yapılan işin doğası ve şirketin risk politikası gereğince para çekme veya yatırma işlemlerinde üyeye şirket uygulamaları haricinde iletişim kanallarından bilgilendirme yapılmadığı, para yatırma veya çekme gibi işlemlerde hiçbir şekilde şirket tarafından e-posta gönderilmediği ve yalnızca kuponlara isabet eden ikramiyeyle ilgili bilgilendirmeler ile oyunlara dair çeşitli bilgilerin e-posta adresinin doğrulanmış olması halinde yapıldığı, bu bilgilendirme tercihlerinin de üyelik paneli üzerindeki ayarlar sekmesinden kolaylıkla güncellenebildiği,
- Gönderilen “Hoşgeldiniz” e-postasının üyelik oluşturma sırasında sehven yanlış girilen bir e-postaya iletilmesi halinde de iletiyi alan kişinin bu hatayı düzeltme imkânının bulunduğu, şöyle ki gönderilen e-posta içerisinde müşteri hizmetleri numarasının yer aldığı ve bu numara üzerinden

müşteri hizmetlerinin her türlü soru, öneri ve şikâyet için 7 gün 24 saat hizmet vermekte olduğunun belirtildiği, nitekim şikâyet konusu olayda da ilgili kişinin şirkete e-posta vasıtası ile ulaşarak kendisinin şirketin platformu üzerinden hesap açmadığı bilgisini iletmiş ve e-posta adresine iletmemesini talep ettiği,

- Şirket tarafından ilgili kişiden gelen bildirim derhal işleme alındığı ve aynı gün ilgili kişinin e-posta adresinin şirket sistemlerinden kaldırıldığı, öte yandan yanlış e-posta adresi ile kaydolmuş üye bakımından ise durumun üyelik e-postasının gelmemesi ile fark edilebileceği,
- Huzurdaki incelemeye konu edilen şikâyeti kişisel verilerin korunması hukukuna hâkim ilkeler ışığında da ele almak istedikleri, bugün için kişisel verilerin korunması hukukunda veri sorumluları bakımından hâkim ilkenin “hesap verebilirlik” olduğunun kabul edildiği,
- Hesap verebilir olmanın bir diğer anlamının da veri sorumlularına proaktif bir özen yükümlülüğü yüklenmesi olduğu, Kurulun 2020/966 sayılı İlke Kararında da bu özen yükümlülüğünün özellikle vurgulandığı, burada veri sorumlusunun özen yükümlülüğünün sınırını çizerken veya 6698 sayılı Kanun’da geçen “gerekli her türlü teknik ve idari tedbir”, “makul önlemler” gibi ifadelerde yer alan sınırlayıcı gerekli veya makul gibi ifadelerin yorumlanmasında hesap verebilirlik ilkesinin özellikle dikkate alınmasının gerektiği,
- Kanun koyucunun veri sorumluları için getirdiği yükümlülüklerde “gerekli”, “makul” gibi sınırlamalar koyarken hesap verilebilirliği veri sorumlusunun faaliyetine bağlı olarak daralıp genişleyebilecek şekilde ölçülü olarak kurgulamayı amaçladığı, dolayısıyla veri sorumlusu tarafından alınacak önlemler veya uygulanacak teknik veya idari tedbirlerin veri sorumlusunun işlediği verilerle, tabi olduğu mevzuatla, işgal konusuyla ve verilerin tabi olduğu riskle yakın ilgisinin bulunduğu,
- Somut incelemede şirketin suç gelirlerinin aklanmasına ilişkin mevzuat ve şans oyunları mevzuatı gereği sıkı bir kimlik kontrolü yükümlülüğü altında olduğunun dikkate alınması gerektiği, bu yükümlülükleri kapsamında şirkete MERNİS üzerinden gerçekleşen kimlik kontrolü olmaksızın üyeliğin mümkün olmadığı, ayrıca şirketin işgal sahasının şans oyunları olması nedeniyle işlenen verinin mahremiyeti dikkate alınarak şirket politikası olarak e-posta veya SMS vasıtası ile üyelerle minimum iletişimde bulunduğu, bu çerçevede şirket bakımından gerekli idari ve teknik tedbirler ile makul önlemlerin sınırının özellikle e-posta adresi verisi gibi asgari düzeyde işlenen veriler bakımından daraldığı,

- Şirket tarafından her türlü kişisel verinin işlenmesinde genel ilkelere uyulmasında azami özen gösterildiği, bu kapsamda geliştirme ve iyileştirme çalışmalarında kimlik verilerine odaklanılmış olmakla birlikte iletişim verilerine ilişkin doğrulama süreçlerinin geliştirilmesine de devam edildiği, bununla birlikte mevcut durumda doğrulanmamış iletişim bilgilerine kişisel veri içeren bilgilendirmelerin yapılmaması için gerekli tedbirlerin alındığı,
- Kurulun 2020/966 sayılı İlke Kararına değinilecek olursa; söz konusu kararda özellikle bahsedilen verilerin fatura, ekstre, rezervasyon belgesi gibi pek çok kişisel veriyi ihtiva eden ve eksik/yanlış veri girişi nedeniyle üçüncü kişilere gönderilmesi mümkün olan veriler olduğunun anlaşıldığı, şirket tarafından yapılan iletişimde bu ve benzeri kişisel verilerin üyelere gönderilmediğinin detayıyla izah edildiği, dolayısıyla Kurulun 2020/966 sayılı İlke Kararı ile şikâyete konu olay arasında doğrudan bağ kurulmasının da hukuken mümkün olmadığı,
- Yapılan inceleme kapsamında tartışılabilir bir diğer hususun da şirketin gönderdiği “Hoşgeldiniz” e-postasında kişisel veri olup olmadığı konusu olduğu, 6698 sayılı Kanun’un 3’üncü maddesinde kişisel verinin “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” olarak tanımlandığı, bu tanım doğrultusunda öne çıkan hususun verinin bir kişiyi belirli ya da belirlenebilir kılması olduğu, veri kendi başına ilgili kişiyi tespit etmeye elverişli değilse ancak başka verilerle birleştirildiği takdirde kişi belirlenebiliyorsa belirlilikten değil belirlenebilirlikten bahis açıldığı ancak bu defa da kişinin elinde olmayan hangi veriler esas alınarak belirlenebilirliğin tartışılması gerektiği sorununun ortaya çıktığı,
- Şirketin gönderdiği “Hoşgeldiniz” e-postasında yer alan isim soy isim verisi ile üye numarası verisinin yanlış bir e-postaya gönderilmesi halinde ortada “belirlenebilir” bir kişisel veri olup olmadığının tartışılmasının gerekeceği, ad soyad verisinin pek çok halde herhangi bir tartışmaya mahal bırakmaksızın ilgili kişiyi doğrudan belirlenebilir kıldığı, ancak yine de bu savın her durumda geçerli olmadığı, pek çok kişinin aynı isim ve soy ismi taşıyabildiği, bu halde üçüncü kişi bakımından ad soyad verisinin tek başına ilgili kişiyi belirleyebilecek nitelikte olmayabileceği, öte yandan üyelik numarasının ise üçüncü kişi bakımından ilgili kişiyi belirleyebilecek nitelikte olmadığı, zira bu numaranın üyeye özel, üye tarafından değiştirilemez harf veya rakamlardan oluşan dizin olarak yalnızca şirket sistemi için anlamlı olduğu, ad soyad verisinin ise yalnızca şirketin iç sistemi için anlam ifade eden üye numarası verisi ile birlikte “belirlenebilir” olduğunun söylenemeyeceği kanaatinde oldukları, dolayısıyla gönderilen “Hoşgeldiniz” e-postasında her ne kadar isim soy isim verisi yer alsa da bu verinin belirlenebilir olmaması sebebiyle kişisel veri niteliğini haiz olmadığı,

- Son olarak, 6698 sayılı Kanun'un en önemli ilkelerinden biri olan ve 6698 sayılı Kanun'un 4'üncü maddesinin (2) numaralı fıkrasının (b) bendinde yer yer alan "doğru ve gerektiğinde güncel olma" ilkesinin veri sorumlusunun çıkarına uygun olduğu gibi ilgili kişinin temel hak ve özgürlüklerinin korunması açısından da gerekli olduğu,

- Kurum tarafından hazırlanan Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler Rehberinde de belirtilmiş olduğu üzere bu yükümlülüğün tesisindeki en önemli hususun her zaman ilgili kişinin bilgilerini doğru ve güncel olmasını temin edecek kanalların açık tutulması olduğu, nitekim şirket tarafından sağlanan platform üzerinden üyelik sırasında verilen iletişim bilgilerinin her zaman görüntülenerek değiştirilme/düzeltilme/güncellenme imkânının bulunduğu

ifade edilmiştir.

Taraflarca dosyaya sunulan tüm bilgi ve belgeler dâhilinde konuya ilişkin yürütülen inceleme neticesinde, Kurulun 01/09/2022 tarihli ve 2022/853 sayılı kararı ile;

- 6698 sayılı Kanun'un "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, "belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza", (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi" olarak tanımlandığı,

- Kanun'un "Genel İlkeler" başlıklı 4'üncü maddesinde, kişisel verilerin ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, buna göre, kişisel verilerin ancak; a) Hukuka ve dürüstlük kurallarına uygun olma, b) Doğru ve gerektiğinde güncel olma, c) Belirli, açık ve meşru amaçlar için işlenme, ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ile d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceği,

- Kanun'un 5'inci maddesinin kişisel verilerin işleme şartlarını düzenlediği, maddenin (1) numaralı fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin, (2) numaralı fıkrasında ise, kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda olan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün korunması için veri işlemenin zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaati için veri işlenmesinin zorunlu olması hallerinde ilgili kişinin açık rızası olmaksızın kişisel verilerin işlenmesinin mümkün olduğunun hükme bağlandığı,
- Kanun'un "Veri Güvenliğine İlişkin Yükümlülükler" başlıklı 12'nci maddesinin (1) numaralı fıkrasında "Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır." düzenlemesinin, (5) numaralı fıkrasında ise "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." düzenlemesinin yer aldığı,
- İlgili kişinin şikâyeti kapsamında savunması istenen şirket tarafından "Şirketin ilgili mevzuat hükümleri uyarınca idareden aldığı yetki ile bizatihi idarenin düzenleyici olduğu regüle bahis piyasasında faaliyet gösteren bir sanal ortam bayii olduğu, yürüttüğü regüle faaliyet kapsamında kişisel verilerin korunmasına dair mevzuata ilave olarak veri işleme bakımından iki önemli yükümlülüğünün bulunduğu ve sistemlerinin anılan yükümlülüklerle uyumlu olarak tasarlandığı"nın vurgulandığı, buna karşın şirketin faaliyet alanına ilişkin özel mevzuat hükümleri uyarınca çeşitli yükümlülüklerinin bulunmasının 6698 sayılı Kanun'dan kaynaklanan yükümlülüklerden muaf olmasını/tutulmasını sağlamayacağı,
- Bir gerçek kişinin kimliğini belirli veya belirlenebilir kılacak mahiyette olup da şirketin elektronik sistemlerinde kaydetme, depolama ve sair fiillere konu edilen isim-soy isim, e-posta adresi, telefon numarası, üyelik numarası gibi bilgilerin "kişisel veri" niteliğini haiz olduklarının açık olduğu, zira söz konusu bilgilerin şirket nezdinde üyelik hesabı bulunan herhangi bir kişinin kimliğini -Şirket

veya herhangi bir diğerk kişi tarafından kullanılabilir makul tüm araçlar dikkate alındığında- şirket veya başka herhangi bir kişi için belirlenebilir kılmaya yeterli olduklarının kabul edilmesinin gerektiği, böyle bir kabulün de gerek 6698 sayılı Kanun'un 3'üncü maddesindeki "kişisel veri" tanımıyla gerek ülkemizin taraf olması vesilesiyle kişisel verilerin korunması mevzuatımızın bir parçası olan ve kamuoyunda "108 sayılı Sözleşme" olarak bilinen Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "Tanımlar" başlıklı 2'nci maddesindeki "Kişisel veriler: Kimliği belirli veya belirlenebilir bir gerçek kişi (ilgili kişi) hakkındaki tüm bilgileri ifade eder." tanımıyla gerekse de Kurulun yerleşik uygulamalarıyla uyumlu olduğu, kaldı ki halen yürürlükte olmasa da 6698 sayılı Kanun'un yapım aşamasında örnek alınan düzenlemeler arasında bulunan 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi (Direktif) adlı Avrupa Birliği düzenlemesinin başlangıç/giriş bölümünde yer alan ve "kişisel veri" kavramına dair de açıklamalar içeren (26) numaralı resitalde/gerekçede de aynı hususun teyit edildiği,

- Her ne kadar şirket tarafından "ilgili kişiye gönderilen 'Hoşgeldiniz' mesajı içerisindeki verilerin somut olaydaki isim-soy isim bilgisinin yaygın olabileceğinden ve üyelik numarası bilgisinin de sadece şirket tarafından bilindiğinden bahisle kişisel veri niteliği taşımadığı" yönünde bir savunma yapılmışsa da söz konusu mesaj içerisinde beraber yer aldıkları görülen "isim-soy isim" ve "üyelik numarası" bilgilerinin somut olayda şirketin elektronik sistemine üye olan şahsı en azından şirket nezdinde belirlenebilir kılmaları dolayısıyla kişisel veri mahiyetinde oldukları, bununla birlikte belirli bir kişiye ait gibi görünen bilgilerin aslında yanlış olmaları (örneğin farklı bir kişiye ait olmaları) durumunda bu bilgilerin "kişisel veri" olma nitelikleri ortadan kalkmadığı için ilgili kişiye ait olduğu ama şirketin elektronik sistemine üyelik sahibi şahıs tarafından beyan edildiği anlaşılan e-posta adresi bilgisinin ilgili kişinin kişisel verisi olduğunun da unutulmaması gerektiği,

- Somut olayda kişisel verilerin şirketin elektronik sistemlerinde kaydetme, depolama, paylaşma, sınıflandırma, aktarma ve sair fiillere konu edilmesinin birer "kişisel veri işleme faaliyeti" olarak adlandırılması gerektiği, bu durumda hem anılan kişisel verileri işleme faaliyetlerinin amaçlarını ve vasıtalarını belirleme gücünü haiz olduğu hem de veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olduğu anlaşılan şirketin "veri sorumlusu" sıfatını taşıyacağı konusunda herhangi bir şüphenin bulunmadığı,

- Somut olayda veri sorumlusu tarafından ilgili kişinin e-posta adresine bilgisi ve rızası dışında iki adet e-postanın gönderildiğinin sabit olduğu, söz konusu gönderim kapsamında e-posta adresinin

işlenmesinden ibaret olan kişisel veri işleme faaliyetlerinin öncelikle 6698 sayılı Kanun'un 5'inci maddesinde düzenlenen hukuki şartlardan en az birine dayanmasının gerektiği, buna rağmen ilgili kişinin e-posta adresi kişisel verisinin üçüncü bir şahıs konumunda olan üyelik sahibi kişi tarafından veri sorumlusunun sistemine kaydedildiği dikkate alındığında veri sorumlusu tarafından ilgili kişi hakkında yürütülen mezkûr kişisel veri işleme faaliyetleri sırasında 6698 sayılı Kanun'un 5'inci maddesinde düzenlenen herhangi bir hukuki şarta dayanılmadığı, ayrıca somut olayda veri sorumlusunun elektronik sisteminde kaydı bulunan üyenin "isim-soy isim" ve "üyelik numarası" kişisel verilerinin ilgili kişiyle paylaşılmasından ibaret olan kişisel veri işleme faaliyeti açısından da anılan şartlardan herhangi birine dayanılmadığı,

- Şikâyete konu olayda asıl üyenin "isim-soy isim" ve "üyelik numarası" kişisel verilerinin 6698 sayılı Kanun'un 5'inci maddesinde düzenlenen herhangi bir hukuki şarta dayanılmadan ilgili kişi ile paylaşılmasının aynı zamanda bir "kişisel veri ihlali" niteliği taşıdığı göz önünde bulundurulduğunda; veri sorumlusu tarafından 6698 sayılı Kanun'un 12'nci maddesinin (5) numaralı fıkrası kapsamındaki "ilgili kişiye ve Kurula bildirim yükümlülüğü"ne de uyulmadığı sonucuna ulaşıldığı,

- İlgili kişinin şikâyetinde yer verdiği iddialara cevaben, veri sorumlusunca "Şirket tarafından sağlanan platform üzerinden üyelik sırasında verilen iletişim bilgilerinin her zaman görüntülenerek değiştirilme/düzeltilme/güncellenme imkânının mevcut olmasının şirketin 6698 sayılı Kanun'un 4'üncü maddesinin (2) numaralı fıkrasının (b) bendindeki 'Doğru ve gerektiğinde güncel olma' genel ilkesine uygun hareket ettiğini gösterdiği" yönünde bir savunma yapılmış olmasına karşılık; 6698 sayılı Kanun'un 4'üncü maddesinin (2) numaralı fıkrasının (b) bendindeki "Doğru ve gerektiğinde güncel olma" genel ilkesinin veri sorumlularının uyması gereken bir zorunluluğa işaret ettiği ve bu konuda gerekli tedbirleri almamış ya da alamamış olan veri sorumlularının "mezkûr zorunluluğa uyumlarını ilgili kişilerin uhdesine/keyfiyetine bırakmış oldukları" veya "ilgili kişilere iletişim bilgisi görüntüleme, değiştirme, düzeltme ve güncelleme imkânı verilmesinin mezkûr zorunluluklarına uyduklarını gösterdiği" yönünde savunmalar yaparak sorumluluktan kurtulmalarının bahsi geçen düzenlemenin sözüne ve ruhuna aykırı olacağı,

- Zaten Kurulun 22/12/2022 tarihli ve 2020/966 sayılı İlke Kararındaki ifadelerin de veri sorumlularının 6698 sayılı Kanun'un 4'üncü maddesinin (2) numaralı fıkrasının (b) bendindeki zorunluluğa uymak için aktif bir şekilde adımlar atması gerektiğine işaret ettiği, bu kapsamda kullanıma sunduğu sistem özelinde 6698 sayılı Kanun'un 4'üncü maddesinin (2) numaralı fıkrasının (b) bendindeki "Doğru ve gerektiğinde güncel olma" genel ilkesinden kaynaklanan zorunluluğa

uymak konusunda aktif adımlar atmadığı anlaşılan veri sorumlusunun somut olaydaki kişisel veri işleme faaliyetlerinin mezkûr genel ilkeye aykırı olduklarının açık olduğu,

- Veri sorumlusunun yukarıdaki bölümlerde “Şirketin kişisel veri işleme faaliyetleri sırasında ‘hesap verebilirlik’ yaklaşımını benimsediği, ilgili kişinin şikâyetinde atıf yaptığı Kurulun 2020/966 sayılı İlke Kararının -kararda özellikle bahsedilen verilerin fatura, ekstre, rezervasyon belgesi gibi pek çok kişisel veriyi ihtiva eden ve eksik/yanlış veri girişi nedeniyle üçüncü kişilere gönderilmesi mümkün olan veriler olması nedeniyle- somut olayda uygulama alanı bulmasının mümkün olmadığı” olarak özetlenen savunmasının da Kurulun 22/12/2022 tarihli ve 2020/966 sayılı İlke Kararında örnek kabilinden sayılan bilgi ve/veya belgelerin sınırlı sayıda olmaması, ilgili kişilerin hukuka aykırı kişisel veri işleme faaliyetleri sonucunda görebilecekleri zararların veri sorumlusunun öngörüsünün aksine sadece maddi değil manevi nitelik de taşıyabilecek olması, “698 sayılı Kanun’un 15’inci maddesinin (6) numaralı fıkrasına dayanan ilke kararlarının şikâyet üzerine veya resen yapılan inceleme sonucunda ihlalin yaygın olduğunun tespit edilmesi hâlinde Kurul tarafından alınıp yayımlanan ‘yol gösterici’ mahiyette kararlar olması ve inceleme konusu bir şikâyet kapsamında 6698 sayılı Kanun’un 4’üncü maddesinin uygulama alanı bulabilmesi için Kurulun almış olduğu bir ilke kararına dayanmak zorunda olmaması nedenleriyle geçerli bir savunma olmadığı,

- Veri sorumlusunun ilgili kişinin şikâyetine ilişkin savunmaları içerisinde “Şirket tarafından işlenen kişisel veriler kapsamında iletişim verilerinin şirketin risk politikası gereğince MERNİS üzerinden doğrulanan bazı kimlik verilerine kıyasla ikincil öneme sahip olduğu, buna rağmen şirketin üyelerinin iletişim verilerinin kontrollü bir şekilde işlenmesi için gerekli mekanizmalara sahip olduğu” yönündeki ifadeler ele alınacak olursa; 6698 sayılı Kanun’da kişisel verilerin veri sorumluları için taşıdıkları önem dereceleri gözetilerek sınıflandırılması gerektiğini ifade eden bir düzenlemenin bulunmadığı, dolayısıyla veri sorumlusunun “kendisi için daha çok önem arz eden verileri daha çok denetlediği ama iletişim verileri bakımından böyle bir denetimin o kadar da gerekli olmadığı” anlamına gelebilecek savunmalarının da kabul edilebilir nitelikte olmadığı, ayrıca günümüzde “ilgili kişi” sıfatını haiz kişilerin iletişim verileri kullanılarak yürütülen ve “ortalama” gibi yöntemlere dayanan çeşitli illegal faaliyetler sonucunda bazı mağduriyetlerin yaşanabildiği göz önüne alındığında iletişim verilerinin güvenliklerinin sağlanmasının önemsiz olduğunun söylenemeyeceği, öte yandan bir üyesi tarafından yanlış ve/veya hatalı bildirilmesi nedeniyle “üçüncü kişi” konumundaki ilgili kişiye e-postalar gönderdiği sabit olan veri sorumlusu için “üyelerinin iletişim verilerinin kontrollü bir şekilde işlenmesi için gerekli mekanizmalara sahip olduğu” yönünde bir niteleme yapabilmeyenin de mümkün olmadığı,

- Veri sorumlusunun ilgili kişinin şikâyetine ilişkin savunmaları kapsamında “veri sorumlusunun üyeleri ile ana iletişim kanalı olarak cep telefonu numarasını kabul ettiği, bu yüzden e-posta iletişim bilgisi için doğrulamanın üyelik başvurusu anında yapılmadığı ve e-posta iletişim bilgisini doğrulamayan üyelerin bildirdikleri e-posta adreslerine veri sorumlusu tarafından en fazla iki e-postanın gönderildiği, ayrıca hatalı bildirilen e-posta adresi sahiplerinin veri sorumlusu ile iletişime geçerek ret imkanına sahip oldukları” yönündeki beyanları karşısında; “veri sorumlusunun üyeleri ile ana iletişim kanalı olarak cep telefonu numarasını kabul ettiği, bu yüzden e-posta iletişim bilgisi için doğrulamanın üyelik başvurusu anında yapılmadığı” gibi bir savunmanın veri sorumlusu tarafından üyelerinin e-posta adresleri hakkında yürütülen kişisel veri işleme faaliyetleri bakımından kişisel verilerin korunması alanına hâkim olan ve 6698 sayılı Kanun’un 4’üncü maddesinin (2) numaralı fıkrasının (ç) bendinde düzenlenen “İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” genel ilkesi ile somutlaştırılan “veri minimizasyonu ilkesi”ne de uyulmadığını gösterdiği, zira ana iletişim kanalı olarak kullanılmayan ve aslında hiç işlenmemiş olsa da veri sorumlusunun üyelerine sunduğu hizmetleri aksatmayacağı anlaşılan bir iletişim verisinin veri sorumlusu tarafından işlenmesinin “veri minimizasyonu ilkesi”ne aykırı olacağı,

- Veri sorumlusunun “üyeleri ile ana iletişim kanalı olarak cep telefonu numarasını kabul ettiği, bu yüzden e-posta iletişim bilgisi için doğrulamanın üyelik başvurusu anında yapılmadığı ve e-posta iletişim bilgisini doğrulamayan üyelerin bildirdikleri e-posta adreslerine veri sorumlusu tarafından en fazla iki e-postanın gönderildiği, ayrıca hatalı bildirilen e-posta adresi sahiplerinin veri sorumlusu ile iletişime geçerek ret imkanına sahip oldukları” yönündeki savunması karşısında ayrıca; ilgili kişilere hukuka aykırı kişisel veri işleme faaliyeti teşkil edecek şekilde tek bir e-posta gönderilmesinin yeterli olduğu bu anlamda e-posta sayısının hukuka aykırılığın mevcudiyeti açısından herhangi bir fark yaratmayacağı, ilaveten veri sorumlusunun mevcut sisteminin veri sorumlusuyla herhangi bir ilişkisi bulunmayan ilgili kişileri veri sorumlusundan bildirim e-postaları almamak için aktif eylemlerde bulunmaya zorluyor olması sebebiyle 6698 sayılı Kanun’un 4’üncü maddesinin (2) numaralı fıkrasının (a) bendinde düzenlenen “Hukuka ve dürüstlük kurallarına uygun olma” genel ilkesine uygun olmadığına da kabul edilmesi gerektiği, bu durumda veri sorumlusunun “hatalı bildirilen e-posta adresi sahiplerinin veri sorumlusu ile iletişime geçerek ret imkanına sahip oldukları” yönündeki savunmasının da geçerli olmadığına açık olduğu,

- Veri sorumlusunca ilgili kişinin veri sorumlusuna kimliğinin doğrulanmasına imkân verecek bir başvuru yapmadığından bahisle “ilgili kişinin şikâyetinin 6698 sayılı Kanun’un 14’üncü maddesinde düzenlenen usule aykırı olduğu” yönündeki savunması karşısında; taraflarca dosyaya sunulan bilgi

ve belgelerden ilgili kişinin veri sorumlusuna e-posta üzerinden yaptığı başvurunun yukarıdaki bölümde paylaşılan mevzuat hükümlerine uygun bir başvuru olmadığı, bununla birlikte söz konusu e-posta başvurusuna cevaben veri sorumlusu tarafından gönderilecek bir e-posta marifetiyle “başvurunun işleme alınabilmesi için mevzuata uygun şekilde yapılması gerektiği” yönünde ilgili kişinin bilgilendirilmesi ve yönlendirilmesi imkânı varken ilgili kişinin başvurusunun veri sorumlusunca sanki hukuka uygun bir başvuruymuş gibi ele alındığı (konu hakkında ilgili kişinin e-postasında paylaşmış olduğu cep telefonu numarası üzerinden ilgili kişiye bilgi verildiği, ayrıca talep edilen hususlardan biri hakkında ilgili kişinin e-postasına yazılı olarak cevap da iletildiği) dikkate alındığında konuya ilişkin Kurulca bir inceleme başlatıldıktan sonra “ilgili kişi tarafından veri sorumlusuna yapılan başvurunun hukuka aykırı olduğu” itirazının ileri sürülmesinin 4721 sayılı Türk Medeni Kanunu’nun 2’nci maddesinde düzenlenen ve 6698 sayılı Kanun’un “Genel İlkeler” başlıklı 4’üncü maddesi çerçevesinde de her türlü veri işleme faaliyetinde esas alınması gerektiği şeklinde ifadesini bulan “dürüstlük kurallarına uygun hareket etme” yükümlülüğüne aykırı olacağı, dolayısıyla ilgili kişinin şikâyetine istinaden veri sorumlusu hakkında başlatılan incelemede usule dayanan herhangi bir hukuka aykırılığın bulunmadığı

değerlendirmelerinden hareketle;

- Veri sorumlusunun kişisel veri işleme faaliyetlerini yürüttüğü elektronik sistemi 6698 sayılı Kanun’un 4’üncü maddesinin (2) numaralı fıkrasında düzenlenen “Hukuka ve dürüstlük kurallarına uygun olma”, “Doğru ve gerektiğinde güncel olma” ve “İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” genel ilkelerine uygun tasarlamamış/tasarlatmamış olmasından dolayı hem ilgili kişinin kişisel verisi olan e-posta adresini 6698 sayılı Kanun’un 5’inci maddesinde öngörülen herhangi bir hukuki şarta dayanmaksızın işlediği hem de bir üyesinin “isim-soy isim” ve “üyelik numarası” kişisel verilerini 6698 sayılı Kanun’un 5’inci maddesinde öngörülen herhangi bir hukuki şarta dayanmaksızın “üçüncü şahıs” konumundaki ilgili kişi ile paylaştığı kanaatine varıldığından; veri sorumlusunun anılan fiillerinin 6698 sayılı Kanun’un veri güvenliğine ilişkin yükümlülüklerin düzenlendiği 12’nci maddesinin (1) numaralı fıkrasının (a) bendi hükmüne aykırılık teşkil ettiği dikkate alınarak 6698 sayılı Kanun’un 18’inci maddesinin (1) numaralı fıkrasının (b) bendine istinaden veri sorumlusu hakkında 250.000 TL idari para cezası uygulanmasına,
- Veri sorumlusunun şikâyete esas elektronik sisteminin 6698 sayılı Kanun’un 4’üncü maddesinin (2) numaralı fıkrasındaki genel ilkelere aykırılık teşkil ettiği değerlendirildiğinden; doğrulanmamış iletişim kanalına kişisel veri içerikli herhangi bir gönderi yapılmaması bu kapsamda söz konusu sistemin 6698 sayılı Kanun’a uyumlu hale getirilmesini teminen Kurulun 22/12/2020 tarihli ve

2020/966 sayılı İlke Kararı da dikkate alınarak gerekli çalışmaların yapılması ve sonuçtan Kurula bilgi verilmesi konusunda veri sorumlusunun talimatlandırılmasına,

- Şikâyete konu olayda asıl üyenin kişisel verilerinin şikâyetçi ile paylaşılmasının aynı zamanda kişisel veri ihlali niteliği taşıdığı dikkate alındığında bundan sonraki süreçlerde meydana gelebilecek veri ihlallerinde 6698 sayılı Kanun'un 12'nci maddesinin (5) numaralı fıkrası kapsamında ilgili kişilere ve Kurula bildirim yapılması gerektiği hususunun veri sorumlusuna hatırlatılmasına

karar verilmiştir.

2022/798 sayılı KVKK Kararı

İlgili kişinin bir şirket ile iş görüşmesi yaptığı bilgisi ile görüşmenin içeriği hakkındaki muhtelif bilgilerin iş görüşmesi yapılan şirket tarafından halihazırdaki iş yeri ile paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 04/08/2022 tarihli ve 2022/798 sayılı Karar Özeti

Karar Tarihi : 04/08/2022

Karar No : 2022/798

Konu Özeti: İlgili kişinin bir şirket ile iş görüşmesi yaptığı bilgisi ile görüşmenin içeriği hakkında muhtelif bilgilerin iş görüşmesi yapılan şirket tarafından halihazırdaki işyeri ile paylaşılması

Kuruma intikal eden şikayette özetle; ilgili kişinin halihazırda bir şirket bünyesinde çalışmakta iken başka bir şirkete iş görüşmesi yapmak maksadıyla davet edildiği ve iş görüşmesinin gerçekleştirildiği, iş görüşmesi yapan veri sorumlusu şirket tarafından, ilgili kişinin halihazırda çalışmakta olduğu şirket hakkında itibarını zedeler nitelikte birçok beyanda bulunduğu bilgisinin ilgili kişinin mevcut iş yeri ile paylaşıldığı, bunun neticesinde ilgili kişinin mevcut iş yeri tarafından ücretsiz izne çıkarıldığı, bu durum üzerine ilgili kişi tarafından iş sözleşmesinin feshi için ihtarname gönderildiği, iş yeri tarafından ihtarnameye verilen yanıtta ilgili kişinin başka bir şirket ile iş görüşmesi yaptığı, ayrıca ilgili kişinin halihazırdaki iş yeri hakkında bir takım söylemlerde bulunduğu, bu durumun iş görüşmesi yaptığı veri sorumlusu şirket tarafından kendilerine iletildiği bilgilerine yer verildiği, dolayısıyla ihtarnameye verilen yanıtta ilgili kişinin iddialarının tevsik edildiği, akabinde ilgili kişi tarafından kişisel verilerinin işlenip işlenmediği, kişisel verilerinin kimlerle paylaşıldığı konularında bilgi edinmek, ayrıca maddi ve manevi zararların tazmini ile kişisel verilerinin silinmesini talep etmek suretiyle iş görüşmesi yapan veri sorumlusuna başvuruda bulunulduğu ancak yasal süresi içerisinde yanıt verilmediği belirtilerek veri sorumlusu hakkında 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- Öncelikle ilgili kişinin başvurusuna cevap verilmediği iddiası ile ilgili olarak, ilgili kişinin vekili aracılığıyla tarafları aleyhine Cumhuriyet Başsavcılığına "Hukuka Aykırı olarak Kişisel Verileri

Kaydetmek, Özel Hayatın Gizliliğinin İhlal Etmek, Hukuka Aykırı Verileri Ele Geçirmek veya Yayımlamak” suçlamalarıyla yaptığı şikayet üzerine Başsavcılık Makamı tarafından soruşturma başlatıldığı, soruşturma dosyasının hukuken sonuca bağlanılmasının beklenilmesi nedeniyle ilgili kişinin başvurularına cevap verilmediği,

- Cumhuriyet Başsavcılığı tarafından soruşturmaya konu olayla ilgili olarak "Kovuşturmaya Yer Olmadığına Dair Karar” verildiği,

- Söz konusu Kararda “... paylaşılan bilginin müşterinin özel yaşam alanına ilişkin bir bilgi niteliğinde bulunmadığı gibi müşterinin sürekli denetim ve gözetim altına alınması sonucu elde edilmiş özel hayatın gizliliğini ihlale yol açan bir bilgi niteliğinde de olmadığı, TCK.nun 135 ve 136. maddelerinde düzenlenen 'Kişisel Verilerin Kaydedilmesi' ve 'Verileri hukuka aykırı olarak verme veya ele geçirme 'suçlarının konusunu oluşturan Kişisel Veri kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı, herkes tarafından bilinmeyen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan, kişinin ve onun niteliklerini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerektiği, kişinin özel hayata ilişkin olmayan bilgilerin rızaya aykırı olarak paylaşılmasının kişilik hakkını ihlal edeceği fakat şüphelinin eyleminin ancak özel hukuk yaptırımlarını gerektirebileceği, söz konusu kişilik hakkının ihlali, özel hayatın gizliliğini ihlal suçunu oluşturmayacağı, bu haliyle atılı suçların unsurlarının oluşmayacağı anlaşılmalı, ... 1-Soruşturmaya konu olayla ilgili olarak şüpheli hakkında kamu adına kovuşturma yapılmasına yer olmadığı, ...” hususlarına yer verildiği

- İşlenen verilerin ilgilinin kâğıt ortamında muhafaza edilen özgeçmişinde yer alan bilgiler olduğu, alınan CV ile dijital, mülakat esnasında başvuru formu üzerine bilgi işlemek suretiyle fiziksel ve kameralar vasıtasıyla da görsel veri toplamak suretiyle kişisel verilerin elde edildiği,

- Kanun’un 5’nci maddesinin (2) numaralı fıkrasının (c) bendinde yer alan “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” hükmü ve aynı fıkrasının (f) bendinde yer alan “İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.” hükmü uyarınca kişisel verilerin işlendiği,

- İnsan kaynakları süreçlerinin planlanması, çalışan ve stajyer adayı seçme ve yerleştirme süreçlerinin yürütülmesi, yeni eleman istihdam edilmesi, adayları inceleme ve istihdam edilecek yeni adayın

tespit edilmesi, çalışan adaylarının başvuru süreçlerinin yürütülmesi ve doğru değerlendirilebilmesi amaçlarıyla kişisel verilerin işlendiği,

- İlgili kişinin şirketlerince işlenen kişisel verilerinin herhangi bir üçüncü kişiye aktarılmadığı, bu iddia hakkında Başsavcılığın kararının da Kuruma iletildiği,

ifade edilmiştir.

Konuya ilişkin olarak yapılan incelemede Kişisel Verileri Koruma Kurulunun 04/08/2022 tarihli ve 2022/798 sayılı Kararı ile;

- Kanun'un "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi" olarak tanımlandığı,

- Kanun'un "Genel İlkeler" başlıklı 4'üncü maddesinde, kişisel verilerin ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, buna göre, kişisel verilerin ancak; a) Hukuka ve dürüstlük kurallarına uygun olma, b) Doğru ve gerektiğinde güncel olma, c) Belirli, açık ve meşru amaçlar için işlenme, ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ile d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceği,

- Kanun'un 5'inci maddesinin kişisel verilerin işlenme şartlarını düzenlediği, maddenin (1) numaralı fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin, (2) numaralı fıkrasında ise, kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda olan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün korunması için veri işlemenin zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine

getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaati için veri işlenmesinin zorunlu olması hallerinde ilgili kişinin açık rızası olmaksızın kişisel verilerin işlenmesinin mümkün olduğunun hükme bağlandığı,

- Kanun'un "Kişisel Verilerin Aktarılması" başlıklı 8'inci maddesinde ise "(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz. (2) Kişisel veriler; a) 5 inci maddenin ikinci fıkrasında, b) Yeterli önlemler alınmak kaydıyla 6'ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir. (3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır." hükmünün yer aldığı,

- İlgili kişinin şikâyet dilekçeleri incelendiğinde; 21.06.2021 ve 11.11.2021 tarihli dilekçeler ile veri sorumlusuna başvuruda bulunulduğu ve söz konusu başvuruların 23.06.2021 ve 16.11.2021 tarihlerinde veri sorumlusuna teslim edildiğinin posta alındıları ile tevsik edildiği,

- Veri sorumlusu tarafından Kuruma iletilen cevabi yazıda ilgili kişinin veri sorumlusunun yöneticisi aleyhine Cumhuriyet Başsavcılığına "Hukuka Aykırı olarak Kişisel Verileri Kaydetmek, Özel Hayatın Gizliliğinin İhlal Etmek, Hukuka Aykırı Veri Ele Geçirmek veya Yaymak" suçlamalarıyla yaptığı şikâyet üzere başlatılan soruşturmanın akıbetinin beklendiği iddia edilmekle birlikte söz konusu soruşturmanın şirket çalışanı ile ilgili olduğunun anlaşıldığı, ayrıca konu hakkında soruşturma yürütülmesinin Kanun ve Tebliğ hükümlerinin uygulanmayacağı anlamına gelmediği, bu çerçevede, ilgili kişinin Tebliğ'e uygun olarak veri sorumlusuna yapılmış başvurularına yasal süresi içerisinde cevap verilmemesi sebebiyle Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in 6'ncı maddesinin (1) numaralı fıkrasında yer alan "Veri sorumlusu bu Tebliğ kapsamında ilgili kişi tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlüdür." hükmüne aykırı davranıldığı,

- Öte yandan Cumhuriyet Başsavcılığının "Kovuşturmaya Yer Olmadığına Dair Karar"ı incelendiğinde ilgili kişinin söz konusu soruşturmada müşteki sıfatı ile yer aldığı, suç tarihinin ise 05.02.2021 olduğunun anlaşıldığı, söz konusu Kararda "kişinin özel hayata ilişkin olmayan bilgilerin rızaya aykırı olarak paylaşılmasının kişilik hakkını ihlal edeceği fakat şüphelinin eyleminin ancak özel hukuk yaptırımlarını gerektirebileceği, söz konusu kişilik hakkının ihlalinin, özel hayatın gizliliğini ihlal suçunu oluşturmayacağı.." belirtilerek şüpheli hakkındaki şikâyetin Türk Ceza Kanunu kapsamında suç unsuru barındırmadığı yönünde karar tesis edildiğinin anlaşıldığı,

- Şikâyete konu olay kapsamında, ilgili kişi tarafından şikâyet edilen tarafın veri sorumlusu sıfatı ile ilgili kişinin kişisel verilerini işlediği ve inceleme konusunun Kanun çerçevesinde değerlendirmeye tabi tutulacağı, bu kapsamda Cumhuriyet Başsavcılığı tarafından kovuşturmayaya yer olmadığına dair verilen kararın Türk Ceza Kanunu çerçevesinde yapılan değerlendirme sonucu verildiği, verilen Kararın Kurum tarafından yürütülen inceleme kapsamında bir etkisi bulunmadığı ayrıca Kararda “kişinin özel hayata ilişkin olmayan bilgilerin rızaya aykırı olarak paylaşılmasının kişilik hakkını ihlal edeceği” yönünde değerlendirmede bulunulduğunun görüldüğü,
- Bu çerçevede, ilgili kişi tarafından Kuruma iletilen şikâyet dilekçesinin ekleri incelendiğinde; mevcut işyeri tarafından ilgili kişiye iletilen cevabi ihtarnamede “...evden çalıştığınız bu süreçte sadakat yükümlülüğüne aykırı davrandığınız, başka şirketlerle iş görüşmeleri yaptığınız ve bu görüşmelerde müvekkilin sektör paydaşlarına karşı prestijini zarara uğrattığınız tespit edilmiştir. Halen müvekkil şirkette çalışmakta iken tarihinde Şirket ofisinde yaptığınız iş görüşmesinde müvekkil şirket ile ilgili oldukça kötü söylemlerde bulunduğunuz ... Şirket tarafından tarafımıza iletilmiştir...” ifadelerine yer verildiği,
- Şikâyete konu somut olayda ilgili kişinin veri sorumlusu ile iş görüşmesi gerçekleştirdiği ve bu görüşmede halihazırda çalışmakta olduğu iş yeri hakkında kötü söylemlerde bulunduğu bilgisinin veri sorumlusu tarafından üçüncü kişilerle paylaşıldığı iddiasına karşılık veri sorumlusu tarafından bu hususa ilişkin olarak; ilgili kişinin şirketlerince işlenen kişisel verilerinin herhangi bir üçüncü kişiye aktarılmadığı belirtilmekle birlikte ilgili kişinin çalışmakta olduğu şirket tarafından ilgili kişiye iletilen ihtarnamede bu hususlara açık bir şekilde yer verildiği,
- Veri sorumlusu tarafından ilgili kişinin mülakat esnasında başvuru formu üzerine bilgilerinin işlendiği ve özgeçmişinde yer alan bilgilerinin Kanun’un 5’nci maddesinin (2) numaralı fıkrasının (c) bendinde yer alan “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” hükmü ve aynı fıkrasının (f) bendinde yer alan “İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması” hükmü uyarınca kişisel verilerin işlendiğinin belirtilmekle birlikte işverenlerin işçi ile akdedilecek iş sözleşmesi çerçevesinde adayın pozisyona uygunluğunu tespit etmek amacıyla işin gerektirdiği menfaatler kapsamında birtakım kişisel verileri işlenmesinin mümkün olacağı, iş sözleşmesinin kuruluşu öncesinde işverenin yönetim hakkı kapsamında adayın uygunluğunu belirlemek amacıyla kişisel verileri işleme hakkı bulunduğu ancak söz konusu bilgilerin Kanun’un 4’üncü maddesinin (2) numaralı fıkrasının (ç)

bendinde yer alan “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkesine de uygun olarak işlenmesi gerektiği,

- Bu çerçevede veri sorumlusu tarafından ilgili kişinin kendileri ile iş görüşmesi yaptığı bilgisi ile iş görüşmesinde ilgili kişinin halihazırda çalışmakta olduğu iş yeri hakkında birçok beyanda bulunduğu bilgisinin ilgili kişinin çalıştığı şirkete hukuka aykırı olarak aktarıldığı, bu aktarımın Kanun’un 8’inci maddesinde yer alan veri aktarımına yönelik şartlarından herhangi birine dayanılmaksızın gerçekleştirildiği,

değerlendirmelerinden hareketle;

- İlgili kişinin Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ’e uygun olarak yapılmış başvurularına veri sorumlusu tarafından yasal süresi içerisinde cevap verilmemesi sebebiyle Tebliğ hükümlerinin uygulanmasına azami dikkat ve özen gösterilmesi hususunda veri sorumlusunun uyarılmasına,

- Veri sorumlusu tarafından ilgili kişinin şirketleri ile iş görüşmesi yaptığı bilgisi ile iş görüşmesinde ilgili kişinin halihazırda çalışmakta olduğu iş yeri hakkında birçok söz beyan ettiği bilgisinin aktarılması faaliyetinin Kanun’un 8’nci maddesine uygun şekilde gerçekleştirilmediği değerlendirilmekte olup bu durumun Kanun’un 12’nci maddesinde yer verilen “veri sorumlusu kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır” hükmüne aykırılık teşkil etmesi nedeniyle, veri sorumlusunun 1997 yılından beri faaliyet gösterdiği, Türkiye genelinde 7 ofis, 1 depo ve 135 çalışan ile lojistik faaliyetlerini yürüttüğü ve ilgili kişinin başvurularına yasal süresi içerisinde yanıt vermediği de dikkate alınarak veri sorumlusu hakkında Kanun’un 18’inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 100.000 TL idari para cezası uygulanmasına karar verilmiştir.

2022/790 sayılı KVKK Kararı

Bir üniversite hastanesi tarafından ilgili kişinin sağlık verilerinin idari bir davaya esas teşkil etmek üzere talebine binaen davalı kamu kurumuna aktarılması hakkında Kişisel Verileri Koruma Kurulunun 04/08/2022 tarihli ve 2022/790 sayılı Karar Özeti

Karar Tarihi : 04/08/2022

Karar No : 2022/790

Konu Özeti: Bir üniversite hastanesi tarafından ilgili kişinin sağlık verilerinin idari bir davaya esas teşkil etmek üzere talebine binaen davalı kamu kurumuna aktarılması

Kuruma iletilen şikayet dilekçesinde özetle; bir kamu kurumu ile ilgili kişi arasında idare mahkemesi nezdinde yürütülen dava dosyası ile ilgili olarak davalı kamu kurumu tarafından üniversite hastanesinden birtakım bilgilerin talep edildiği, söz konusu talep üzerine üniversite hastanesi tarafından ilgili kişiye ait sağlık verilerinin kamu kurumuna teslim edildiği, üniversitenin yapmış olduğu ihlal nedeni ile ilgili kişinin manevi zarara uğradığı ve bu kapsamda manevi tazminat talebinde bulunulduğu, üniversite tarafından yapılan hukuka aykırı eylem nedeni ile hastanede gerçekleşen muayenesi sonucunda ilgili kişi için düzenlenen hasta anamnez formunda belirtilen "... ara sıra tek tük esrar kullanmak zorunda kaldığını söylüyor" içerikli beyan üzerine hakkında Cumhuriyet Başsavcılığına suç duyurusunda bulunulduğu, ilgili kişinin gözaltında kaldığı, konutu ve arabasının arandığı, ilgili kişinin üniversite hastanesinde çalışmakta olan doktora böyle bir beyanda bulunmadığı, üniversite hastanesinde çalışmakta olan doktorun sorusuna verdiği cevabın doktor tarafından yanlış anlaşılacak hasta muayene bilgilerinin hikaye bölümüne yanlış şekilde yazıldığı, yapılan soruşturma neticesinde ilgili kişi hakkında kovuşturmayaya yer olmadığına dair karar verildiği, uyuşturucu madde kullanmadığının Cumhuriyet Başsavcılığının Kararı ile sabit olduğu, bu nedenle ilgili kişiye ait sağlık dosyasında "esrar maddesi kullanıldığına ilişkin verilerin ve bilgilerin silinmesi"nin talep edildiği, belirtilen taleplerine ilişkin olarak başvurusuna üniversite tarafından cevap verilmediği ifade edilerek üniversite hakkında 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Başlatılan inceleme çerçevesinde söz konusu iddialara ilişkin veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- Kamu kurumunun istemi üzerine ilgili kişiye ait üniversite hastanesi kayıtlarında mevcut olan İstirahat Raporu, Anamnez Formları, Epikriz Raporları, Konsültasyon Formları, Hasta Medikal Klinik Seyir Bilgileri, Patoloji Raporu, Radyoloji Raporlarının, 1 (bir) adet CD içeriğinde görevli personele teslim edildiği,
- İlgili kişinin manevi tazminat ödenmesi talebinin 2577 sayılı İdari Yargılama Usulü Kanunu'nun "İdari Makamların Sükutu" başlıklı 10'uncu maddesi kapsamında zımnen reddedildiği,
- Kişisel verilerin Kanun'un "Kişisel Verilerin Aktarılması" başlıklı 8'inci maddesinin (2) numaralı fıkrasının (b) bendine dayalı olarak aktarıldığı,
- İlgili kişinin kişisel verilerinin silinmesi için üniversiteye herhangi bir müracaatının bulunmadığı,
- İlgili veriler, Doktor-Hasta görüşmeleri neticesinde Hastane Bilgi Yönetim Sistemine girildiği için verilerin silinemediği

ifade edilmiştir.

Konuya ilişkin olarak yapılan incelemede Kişisel Verileri Koruma Kurulunun 04/08/2022 tarihli ve 2022/790 sayılı Kararı ile;

- 6698 sayılı Kanun'un "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi" olarak tanımlandığı,
- Kanun'un "Genel İlkeler" başlıklı 4'üncü maddesinde, kişisel verilerin ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, buna göre, kişisel verilerin ancak; a) Hukuka ve dürüstlük kurallarına uygun olma, b) Doğru ve gerektiğinde güncel olma, c) Belirli, açık

ve meşru amaçlar için işlenme, ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ile d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceği,

• Kanun'un "Özel Nitelikli Kişisel Verilerin İşlenme Şartları" başlıklı 6'ncı maddesinin

(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır. şekilde düzenlendiği,

• Veri sorumlusu tarafından kamu kurumuna teslim edilen istirahat raporu, anamnez formları, epikriz raporları, konsültasyon formları, hasta medikal klinik seyir bilgileri, patoloji raporu, radyoloji raporları ve 1 (bir) adet CD'de yer alan ilgili kişiye ilişkin sağlık verilerinin, Kanun'un 6'ncı maddesinin (1) numaralı fıkrasına göre özel nitelikli kişisel veri olduğu,

• Kanun'un 8'inci maddesinin (2) numaralı fıkrasının (b) bendinde belirtilen Kanun'un 6'ncı maddesinin (3) numaralı fıkrasında sağlık ve cinsel hayata ilişkin kişisel verilerin ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceğinin düzenlendiği,

• Kamu kurumunun yazısında söz konusu verilerin talep edilmesinin sebebinin "yürütülmekte olan bir İdari Davaya esas teşkil etmek üzere" şeklinde belirtildiği, öte yandan ilgili kişinin şikayet dilekçesinde idare mahkemesi nezdinde devam eden dava dosyasında davacı tarafın söz konusu kamu kurumunda çalışan ilgili kişi, davalı tarafın ise kamu kurumu olduğunun beyan edildiği, veri sorumlusunun Kanun'un 8'inci maddesinin (2) numaralı fıkrasının (b) bendine yönelik savunması

dikkate alındığında ilgili kişi ile kamu kurumu arasında devam eden idari dava nedeniyle talep edilen özel nitelikli kişisel verilerin veri sorumlusu üniversite tarafından kamu kurumuna aktarılmasına ilişkin işleme faaliyetinde Kanun'un 6'ncı maddesinde yer alan şartların mevcut olmadığı,

- Diğer taraftan, veri sorumlusu tarafından kamu kurumunun yazısında talep edilenden fazla bilgi ve belgenin tesliminin gerçekleştirildiğinin tespit edildiği, şöyle ki, kamu kurumunun yazısında ilgili kişinin belirtilen tarihlerde ameliyat işlemi geçirip geçirmediği, ameliyat geçirmedi ise rahatsızlığı ile ilgili hastanede tedavi ve tetkik işlemine tabi tutulup tutulmadığı, tedavi sürecinin ne kadar sürdüğü, tedavi sonrasında istirahat raporu verilmiş ise ne kadar süre verildiği ve hastane nezdinde resmi tatil günlerinde ne gibi durumlarda ameliyat işlemlerinin gerçekleştirildiğine dair ıslak imzalı olarak tanzim edilen evrakın talep edildiği, veri sorumlusu tarafından bu soruları aşacak nitelikte veri minimizasyonu ilkesine aykırı olarak, bu anlamda Kanun'un 4'üncü maddesinin (2) numaralı fıkrasının (ç) bendi gereğince kişisel verilerin işlenmesinde işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkeleri gözetilmeyerek ilgili kişiye ait hastane kayıtlarında mevcut olan istirahat raporu, anamnez formları, epikriz raporları, konsültasyon formları, hasta medikal klinik seyir bilgileri, patoloji raporu, radyoloji raporlarının, 1 (bir) adet CD içeriğinde teslimi ile talep edilenden fazla özel nitelikli kişisel veri aktarımının gerçekleştirildiğinin anlaşıldığı,

- İlgili kişinin şikayet dilekçesinde, doktorun teşhis koyma amaçlı olarak hastaya sorduğu sorular sonucu elde ettiği, hastanın mevcut ya da geçmiş hastalıkları hakkında kendisinden alınan bilgileri içeren hasta anamnez formunun hasta muayene bilgileri bölümüne doktor tarafından yanlış anlaşılacak "ara sıra tek tük esrar kullanmak zorunda kaldığını söylüyor" şeklinde yazıldığı belirtilen ifadeyi içeren formun kamu kurumuna teslimiyle birlikte, ilgili kişi hakkında Cumhuriyet Başsavcılığına suç duyurusunda bulunulduğu, yapılan soruşturma neticesinde ilgili kişi hakkında Cumhuriyet Başsavcılığının Kararı ile kovuşturmaya yer olmadığına dair karar verildiği,

- İlgili kişi tarafından, "esrar maddesi kullanıldığına ilişkin verilerin ve bilgilerin silinmesi" talebine veri sorumlusu tarafından cevap verilmediği, öte yandan 21.06.2019 tarihli ve 30808 sayılı Resmi Gazete'de yayımlanan Kişisel Sağlık Verileri Hakkında Yönetmelik'in 13'üncü maddesi kapsamında, ilgili kişinin kendisi hakkında sehven oluşturulduğunu iddia ettiği sağlık verilerine ilişkin öncelikle İl Sağlık Müdürlüğüne başvurulması gerekliliğine ve bu başvuru sonrasında sehven oluşturulan sağlık verilerinin düzeltilmesi için gerçekleştirilecek işlemlere yönelik bir düzenlemenin bulunduğu dikkate alındığında ilgili kişinin Kanun'un 11'inci maddesinin (1) numaralı fıkrasının (d) bendi kapsamında "Anamnez Formu"nda geçen "esrar maddesi kullanıldığına ilişkin verilerin

düzeltilmesi"ni, veri sorumlusunun bağlı bulunduğu il sağlık müdürlüğüne başvurmak suretiyle talep edebileceği,

- Veri sorumlusu tarafından 2577 sayılı İdari Yargılama Usulü Kanunu'nun "İdari Makamların Sükutu" başlıklı 10'uncu maddesi uyarınca ilgili kişinin başvurusuna cevap verilmeyerek zimnen reddedildiğinin belirtildiği, ancak Kanun'un 13'üncü maddesinin (2) numaralı fıkrasına göre, veri sorumlusunun başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırması gerektiği

değerlendirmelerinden hareketle;

- Kanun'un 8'inci maddesinin (2) numaralı fıkrasının (b) bendinde belirtilen özel nitelikli kişisel verilerin aktarılmasına ilişkin Kanun'un 6'ncı maddesinde yer alan şartlar ya da Kanun'un 8'inci maddesinin (1) numaralı fıkrasında belirtildiği üzere ilgili kişinin açık rızası mevcut olmadığı halde ilgili kişiye ilişkin özel nitelikli kişisel veri olan sağlık verilerinin Kanun'a aykırı olarak kamu kurumuna aktarıldığı, öte yandan talep edilen bilgiden daha geniş kapsamda bilgi paylaşıldığı dikkate alındığında veri sorumlusu üniversite hastanesinin Kanun'un 12'nci maddesinin (1) numaralı fıkrasına göre kişisel verilerin güvenliğine ilişkin gerekli her türlü teknik ve idari tedbiri alma yükümlülüğünü yerine getirmediği değerlendirildiğinden sorumlular hakkında Kanun'un 18'inci maddesinin (3) numaralı fıkrası çerçevesinde disiplin hükümlerine göre işlem yapılmasına ve yapılan işlem hakkında Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına,

- İlgili kişinin Kanun'un 11'inci maddesinin (1) numaralı fıkrasının (d) bendi kapsamında "Anamnez Formu"nda geçen "esrar maddesi kullanıldığına ilişkin verilerin" düzeltilmesini talep etme hakkı dikkate alındığında; Kanun'un 4'üncü maddesinin (2) numaralı fıkrasının (b) bendinde yer aldığı üzere "doğru ve gerektiğinde güncel olma" ilkesine uygun olarak Kişisel Sağlık Verileri Hakkında Yönetmelik'in 13'üncü maddesi kapsamında, veri sorumlusu tarafından gerek kendi bünyesinde ve gerektiği takdirde ilgili kişiyi de yönlendirmek suretiyle İl Sağlık Müdürlüğü nezdinde gerekli işlemlerin yapılması ve sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına,

- Şikayete konu edilen verilerin aktarıldığı kamu kurumu nezdinde de bu verilerin imha edilmesinin sağlanması hususunda gerekli işlemlerin tesis edilmesine ve yapılan işlemin sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına,

- İlgili kişilerin Kanun kapsamındaki taleplerini Kanun'a ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'e uygun olarak talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde sonuçlandırması gerektiğinin veri sorumlusuna hatırlatılmasına,
 - İlgili kişinin kişisel verilerinin hukuka aykırı olarak işlenmesi nedeniyle uğradığı zararlara ilişkin tazminat talepleri hakkında, genel hükümlere göre yargı mercilerine başvurabileceği konusunda ilgili kişiye bilgi verilmesine
- karar verilmiştir.

2022/787 sayılı KVKK Kararı

Ev eşyası satan veri sorumlusu tarafından ilgili kişinin telefon numarasının üçüncü bir kişinin borcu için iletişim kurulmak suretiyle işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 04/08/2022 tarihli ve 2022/787 sayılı Karar Özeti

Karar Tarihi : 04/08/2022

Karar No : 2022/787

Konu Özeti: Ev eşyası satan veri sorumlusu tarafından ilgili kişinin telefon numarasının üçüncü bir kişinin borcu için iletişim kurulmak suretiyle işlenmesi

Kuruma intikal eden şikâyetle özetle; ilgili kişinin ev eşyası satan bir veri sorumlusu tarafından arandığı, ertesi gün de cep telefonuna mesaj gönderildiği, mesajda şirket ile arasındaki sözleşmeden kaynaklanan borcun tahsili amacıyla hakkında icra takibine başlandığı, takip kapsamında ödeme emri gönderildiği halde bugüne kadar borcun ödenmediğinin tespit edildiği ve yasal takibin durması için hemen ödeme yapılması gerektiği ifade edilerek ödeme ve iletişim için "... Şirketi Hukuk Departmanını arayın" ifadesine yer verildiği, konu hakkında Cumhuriyet Başsavcılığına yapılan suç duyurularında kovuşturmayaya yer olmadığına karar verildiği, ancak bu karardan sonraki bir tarihte de veri sorumlusu tarafından üç kez arandığı ve yapılan son aramada veri sorumlusu tarafından alışveriş yapan kişinin numarasının sorulduğu, ilgili kişinin bu kişinin numarasını bilmediğini ve kendisinin herhangi bir borcunun ya da kefilliğinin bulunmadığını belirttiği ancak veri sorumlusu tarafından borçlu borcunu bitirene kadar sürekli rahatsız edileceğinin söylendiği, en son arandığında numarasının sistemden silinmesi talebine olumsuz cevap verildiği, ayrıca veri sorumlusuna yapılan silme talebini içeren yazılı başvuruya cevap verilmediği ve aramalara devam edildiği ifade edilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin olarak başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- İlgili kişinin 2018 yılı içerisinde şirket ile tüketici finansman sözleşmesi akdettiği, tüketici finansman sözleşmelerinde "Kişisel Verilerin Paylaşımı ve Ticari Elektronik Gönderim İzni" kutucuğunun

bulunduğu; müşterilerin bu şekilde muvafakat/rıza verdiği ve aynı zamanda sözleşmenin 13'üncü maddesinde de "izinli ticari iletişim bilgi verme, bilgi alma (kişisel veri paylaşımı)" hükmünün mevcut olduğu,

- Şirketten alışveriş yapan üçüncü kişi olan müşterinin irtibat numarası olarak ilgili kişinin telefon numarasını şirkete bildirdiği, borcun ödenmemesi sebebiyle söz konusu numara arandığında numaranın kullanıcısı ilgili kişinin üçüncü kişinin arkadaşı olduğunu beyan ettiği, bunun üzerine numara yanlış kaydedilmişse arkadaşı olan ve ilgili kişinin numarasını sözleşmeye kaydettiren müşteriyle irtibata geçmesi gerektiğinin ve sadece bu müşterinin talebi olması halinde iletişim numarasının değiştirilebileceğinin ilgili kişiye birden çok kez söylendiği,
- İlgili kişinin şirkete ulaşan yazılı bir başvurusu olmadığı için ilgili kişinin irtibat numarasının silinmediği, ancak Kurum tarafından gönderilen yazıdan sonra telefon numarasının hemen silindiği,
- İlgili kişiyi arayan hatların şirket adına kayıtlı olduğu, bunlardan birinin adres araştırması yapan bir personel tarafından kullanıldığı bir diğerinin gecikmiş ödemeleri hatırlatmak amacıyla kullanıldığı,
- İlgili kişinin kişisel verilerinin veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi, gecikmiş borç tahsili yapabilmesi çerçevesinde bir hakkın tesisi, kullanılması veya korunması, veri sorumlusunun meşru menfaatlerinin korunması ile bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesi şartlarına dayanılarak işlendiği

ifade edilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde, Kişisel Verileri Koruma Kurulunun 04/08/2022 tarihli ve 2022/787 sayılı Kararı ile;

- 6698 sayılı Kanun'un "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, "belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza", (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusunun, "kişisel

verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi” olarak tanımlandığı,

- Kanun’un “Genel İlkeler” başlıklı 4’üncü maddesinde, kişisel verilerin ancak bu Kanun’da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, buna göre, kişisel verilerin ancak; a) Hukuka ve dürüstlük kurallarına uygun olma, b) Doğru ve gerektiğinde güncel olma, c) Belirli, açık ve meşru amaçlar için işlenme, ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ile d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceği,

- Kanun’un 5’inci maddesinin kişisel verilerin işleme şartlarını düzenlediği, maddenin (1) numaralı fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin, (2) numaralı fıkrasında ise, kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda olan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün korunması için veri işlemenin zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaati için veri işlenmesinin zorunlu olması hallerinde ilgili kişinin açık rızası olmaksızın kişisel verilerin işlenmesinin mümkün olduğunun hükme bağlandığı,

- Kanun’un “İlgili Kişinin Hakları” başlıklı 11’inci maddesine göre herkesin, veri sorumlusuna başvurarak kendisiyle ilgili; kişisel veri işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, 7’nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, kişisel verilerin düzeltilmesi veya silinmesi/yok edilmesi ile ilgili yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme ve kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme haklarına sahip olduğu,

- Kanun'un "Veri Sorumlusuna Başvuru" başlıklı 13'üncü maddesi uyarınca; veri sorumlusunun, ilgili kişinin başvurusunda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırma, bu kapsamda talebi kabul etme veya gerekçesini açıklayarak reddetme ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirme yükümlülüğü olduğu, Veri Sorumlusuna Başvuru Usul ve Esasları hakkında Tebliğ'in (Tebliğ) 5'inci maddesinde "İlgili kişi, Kanununun 11'inci maddesinde belirtilen hakları kapsamında taleplerini, yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletir." hükmüne yer verildiği, Tebliğ'in 6'ncı maddesinde veri sorumlusunun, bu tebliğ kapsamında yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlü kılındığı,
- Veri sorumlusunun ilgili kişi tarafından yazılı bir başvuru yapılmadığı iddiası bakımından yapılan incelemede, ilgili kişi tarafından ibraz edilen posta takip kodunun sorgulanmasıyla yapılan başvurunun veri sorumlusuna tebliğ edildiği anlaşıldığından veri sorumlusunun ilgili kişinin başvurusunu cevaplandırmamasının Kanun ve Tebliğ'in ilgili maddelerine aykırı olduğu,
- İlgili kişinin kişisel verilerinin veri sorumlusu tarafından işleme şartlarına aykırı olarak işlenmeye devam edildiği ve kişisel verilerinin silinmesi talebinin yerine getirilmediği iddialarına ilişkin yapılan incelemede, öncelikle ilgili kişi ile veri sorumlusu arasında akdedilen sözleşmenin 13'üncü maddesinde "izinli ticari iletişim bilgi verme, bilgi alma (kişisel veri paylaşımı)" hükmünün mevcut olduğu ve sözleşmenin son kısmında yer alan "Kişisel Verilerin Paylaşımı ve Ticari Elektronik Gönderim İzni" kutucuğunun, ilgili kişi tarafından "Kabul Ediyorum" şeklinde işaretlenmiş olduğunun görüldüğü, ancak ilgili kişi tarafından sunulan irtibat numarası ve rıza gösterilen izinlerin, bizzat kendisinin taraf olduğu tüketici finansman sözleşmesiyle ilgili olduğunun vurgulanması gerektiği,
- Veri sorumlusunun Kuruma ilettiği savunmasında ayrıca, üçüncü bir kişi ile aralarında bir sözleşmesinin imzalandığını ve üçüncü kişi konumundaki müşterinin irtibat numarası olarak ilgili kişinin telefon numarasını kendilerine bildirdiğini ifade ettiği, ancak veri sorumlusunun üçüncü kişi müşteri ile aralarında yapılmış olan sözleşmenin incelenmesinden, irtibat numarası olarak ilgili kişinin numarasından farklı bir telefon numarasını bildirdiğinin görüldüğü, anılan sözleşme dışında,

üçüncü kişi müşterinin irtibat numarası olarak ilgili kişinin numarasını bildirdiğine ilişkin herhangi bir kanıtın Kuruma sunulmadığı,

- Bu çerçevede, veri sorumlusu tarafından iletilen cevap yazısında ilgili kişiyi arayan telefon hatlarının şirketlerine ait olduğunun kabul edildiği, veri sorumlusu ile üçüncü kişi arasında imzalanan sözleşmede ilgili kişinin numarasından farklı bir telefon numarasının olduğunun görüldüğü, veri sorumlusu tarafından üçüncü kişi müşterinin irtibat numarası olarak ilgili kişinin numarasının bildirildiğine ilişkin herhangi bir kanıt sunulmadığı, ilgili kişiye ait telefonun 2019 yılından 2021 yılına kadar veri sorumlusu tarafından pek çok defa arandığı, bahse konu numaranın asıl borçlu olan üçüncü kişiye ait olmayıp ilgili kişiye ait olduğunun öğrenilmesine rağmen ilgili kişinin silme talebinin reddedilmesi suretiyle ilgili kişinin aranmasına devam edildiği göz önüne alındığında, ilgili kişinin kişisel verisi niteliğindeki telefon numarasının Kanun'un 4'üncü maddesinde yer alan kişisel verilerin "doğru ve gerektiğinde güncel olma" ile "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerine ve Kanun'un 5'inci maddesinde yer alan kişisel verilerin işleme şartlarına aykırı olarak işlendiği,

- Ayrıca veri sorumlusunun Kuruma ilettiği cevap yazısında, Kurum tarafından gönderilen yazının ardından ilgili kişinin telefon numarasının hemen silindiğinin belirtilmesine karşın silme işlemi tevsik edici herhangi bir belge ibraz edilmediği

değerlendirmelerinden hareketle;

- Veri sorumlusunun Kanun'un 4'üncü maddesinde yer alan kişisel verilerin "doğru ve gerektiğinde güncel olma" ile "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerine aykırı olarak ve Kanun'un 5'inci maddesinde yer alan kişisel verilerin işleme şartlarından herhangi biri bulunmaksızın ilgili kişiye ait olmadığını bildiği bir borca ilişkin olarak ilgili kişiyi defaatle aramak suretiyle kişisel verisi niteliğindeki telefon numarasını işlemeye devam ettiği göz önünde bulundurulduğunda, Kanun'un 12'nci maddesinin (1) numaralı fıkrasında yer alan kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri alma yükümlülüğüne aykırı hareket ettiği kanaatine varıldığından, arama yapılan telefon numarasının takibi yapılan asıl borçluya değil, söz konusu borçla ilgisi olmayan ilgili kişiye ait olduğunu öğrenmesine rağmen veri sorumlusunun ilgili kişiyi aramaya devam ettiği ve veri sorumlusunun ekonomik durumu dikkate alınarak, hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 200.000 TL idari para cezası uygulanmasına,

- İlgili kişinin başvurusunun cevaplandırılmamasının Kanun ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'e aykırı olduğu değerlendirildiğinden, veri sorumlusunun kendisine yapılan başvurulara Kanun ve Tebliğ'in ilgili hükümlerine uygun şekilde cevap verilmesinde gerekli dikkat ve özeni göstermesi hususunda uyarılmasına,
- İlgili kişinin kişisel verisinin silinmesi talebinin yerine getirildiğinin tevsik edilmemesi sebebiyle Kanun'un 7 ve 11'inci maddeleri ile Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 7'nci maddesi uyarınca ilgili kişinin kişisel verilerinin silinmiş olduğunu kanıtlayan belgeleri Kuruma iletmesi yönünde veri sorumlusunun talimatlandırılmasına karar verilmiştir.

2022/776 sayılı KVKK Kararı

Veri sorumlusu bir pazarlama şirketi tarafından çocuğun kişisel verilerinin velisinin açık rızası alınmaksızın tanıtım amaçlı broşür gönderilmesi suretiyle işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 03/08/2022 tarihli ve 2022/776 sayılı Karar Özeti

Karar Tarihi : 03/08/2022

Karar No : 2022/776

Konu Özeti: Veri sorumlusu bir pazarlama şirketi tarafından çocuğun kişisel verilerinin velisinin açık rızası alınmaksızın tanıtım amaçlı broşür gönderilmesi suretiyle işlenmesi

Kuruma intikal eden dilekçede özetle;

- Pazarlama şirketine ait bir ürün için serbest girişimci olan gerçek kişi tarafından 8 yaşındaki çocuğa (ilgili kişi) mektup yoluyla tanıtım amaçlı broşür gönderildiği,
- Bunun üzerine, velisi tarafından mektupta telefon numarası bulunan gerçek kişiye telefonla ulaşılarak 8 yaşındaki kızının kişisel bilgilerine nereden ulaştığının sorulduğu, ancak yapılan bu görüşmede karşı tarafça kendisine bir bilgi verilmediği gibi kızının kişisel verileri ile ilgili herhangi bir işlemin yapılmadığı,
- Bu çerçevede velisi tarafından çocuğun ev adresi ve ismi gibi kişisel verilerine nasıl ulaşıldığına ilişkin pazarlama şirketine başvuru yapıldığı, yapılan başvuru neticesinde yine herhangi bir bilgi verilmediği,
- Velinin çocuğun kişisel verilerinin işlenmesine ilişkin herhangi bir rızası olmadığı ve ticari amaçla tanıtım yapmak amacıyla açık rıza olmaksızın çocuğun kişisel verilerinin işlendiği

belirtilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

- Konunun değerlendirilmesi neticesinde Kişisel Verileri Koruma Kurulu (Kurul) tarafından başlatılan inceleme çerçevesinde pazarlama şirketinden savunması istenilmiş olup alınan cevabi yazıda özetle;

Şirketin sağlık ve güzellik ürünleri gibi ürünlerin satışını yapan bir doğrudan satış şirketi olduğu,

Satış yapan gerçek kişi ile şirket arasında, “Başvuru Kuralları ve Koşulları”na uygun olarak şirket ürünlerini satın alma ve satma opsiyonu veren bir sözleşme ilişkisinin olduğu, bu sözleşme kapsamında satış yapan kişinin bağımsız bir iş sahibi/serbest girişimci olarak hareket ettiği ve şirketten bağımsız olduğu,

- Diğer bir ifade ile şirketin “Başvuru Kuralları ve Koşulları”na göre, serbest girişimcilerin şirket çalışanı, acentesi, temsilcisi, franchise (imtiyaz) alanı veya genel anlamda şirket ile bağımlı çalışan ilişkisi içerisinde faaliyet gösteren kişiler olmadığı,

- Şirket ürünlerini satmak isteyen kişilerin, şirkete başvuruda bulunarak serbest girişimci olabildiği,

- Serbest girişimcilerin yalnızca kendi menfaatleri doğrultusunda ve kendi programlarına göre faaliyet gösterdiği, bu kişilerin şirket ürünlerini tamamen kendi tercihlerine göre satın aldığı ve satış faturasının kendi müşterisine ibraz edildiği, doğrudan pazarlama amaçları da dahil olmak üzere, hizmet verdikleri müşterilerden elde ettikleri kişisel veriler bakımından serbest girişimcilerin tek başına ve bağımsız veri sorumlusu olarak hareket ettiği,

- Bu faaliyet çerçevesinde şirketin rolünün; ürünlerin ithalatı, serbest girişimcilere ürünlerin satışı ve ürünlerin müşterilere tesliminden yani bir doğrudan satış şirketi- doğrudan satıcı ilişkisinden ibaret olduğu,

- Somut olayda broşürün pazarlama şirketi tarafından gönderilmediği ve broşür göndermesi için serbest girişimciye şirket tarafından bir talimat verilmediği, broşürün daha önce bağımsız olarak topladığı kişisel veriler kullanılarak serbest girişimci tarafından gönderildiği,

- Şirket tarafından ilgili kişiye ait herhangi bir kişisel verinin işlenmediği ve bu verilerin serbest girişimciye aktarılmadığı,

- Şirketin, serbest girişimcilerin işlediği kişisel veriler bakımından veri sorumlusu olmamakla birlikte serbest girişimcileri gözetim altında tuttuğu ve sözleşme kapsamındaki kurallara aykırılık halinde yaptırım uyguladığı, şikâyet üzerine yapılan araştırma neticesinde serbest girişimcinin geçmişte internetten satış yaptığı müşterilerine broşür gönderdiği, alışveriş yapan kişinin 8 yaşındaki bir çocuk olduğunu bilmediği için bir yanlışlık olduğunun belirtildiği

ifade edilmiştir.

Akabinde konuya ilişkin olarak başlatılan inceleme çerçevesinde gerçek kişi serbest girişimciden savunması istenilmiş olup alınan cevabi yazıda özetle;

- Kendisinin internetten satış yaptığı dönemde ilgili kişinin kişisel verilerini bir e-ticaret sitesi üzerinden kendi nam ve hesabına sattığı şirket ürünlerinden temin ettiği, ilgili kişinin velisinin kendi kızı adına fatura hazırlattığı,

- E-ticaret sitesi üzerinden kendi adres ve iletişim bilgilerini rızaen kendisiyle paylaşan ilgili kişinin velisinin her ne kadar adres ve telefon bilgileri olarak kendi bilgilerini vermiş olsa da velisi olduğu çocuğunun ismini kullanarak sipariş verdiği ve bu sipariş dahilinde kendisine bu broşürün gönderildiği,

- Dolayısıyla söz konusu işlemin Kanun'un 28'inci maddesinin (1) numaralı fıkrasının (a) bendi kapsamında istisna olarak değerlendirilmesi gerektiği, konunun yanlış anlaşılardan kaynaklandığı ifade edilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde, Kişisel Verileri Koruma Kurulunun 03/08/2022 tarihli ve 2022/776 sayılı Kararı ile;

- Kanun'un "Tanımlar" başlıklı 3'üncü maddesinde "ilgili kişi"nin, kişisel verisi işlenen gerçek kişi; "kişisel veri"nin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi; "veri sorumlusu"nun, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi; "kişisel verilerin işlenmesi"nin, kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem" olarak tanımlandığı,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işleminin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından

birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğunun düzenlendiği,

- Kanun'un 12'nci maddesinin (1) numaralı fıkrasında ise veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu,

- Somut olayda öncelikle veri sorumlusunun tespitinin yapılmasının gerektiği, bu çerçevede şirket ile serbest girişimci gerçek kişi arasındaki sözleşmede, müşterilerle ilgili kişisel verilerin işleme amacını ve aracını belirlemek ve geçerli veri koruma hukuki yükümlülüklerine uyma hususunda serbest girişimcinin yükümlü olduğunun, şirket ile serbest girişimci arasındaki ilişkinin temsilcilik, işçi-işveren ilişkisi gibi bağımlı bir ilişki olmadığı ve serbest girişimcinin bağımsız bir sözleşmenin tarafı olduğu hükümlerine yer verildiği, bu hükümler dikkate alındığında gerçek kişi serbest girişimcinin pazarlama kapsamında kişisel veri işleme faaliyetinde şirketten bağımsız olarak hareket ettiği, kişisel veri işleme amaç ve araçlarının serbest girişimci gerçek kişi tarafından belirlendiği ve ilgili kişi ile ilişkisinde gerçek kişinin tek başına veri sorumlusu sıfatını haiz olduğu, söz konusu kişisel veri işleme faaliyetinde şirketin bir rolünün bulunmadığı,

- Veri sorumlusu tarafından bahse konu kişisel verilerin ilgili kişi tarafından veri sorumlusuna iletildiği ve broşürün iletilmesi suretiyle gerçekleştirilen kişisel veri işleme faaliyetinin Kanun'un 28'inci maddesinin (1) numaralı fıkrasının (a) bendinde yer alan "Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklerle uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi" istisna hükmü kapsamında değerlendirilmesi gerektiğinin iddia edildiği ancak hükümdeki düzenlemenin aynı konutta yaşayan aile fertlerinin, yine aile içindeki bireylerin kişisel verinin işlenmesine ilişkin olduğu, örneğin doğum günü gibi özel günlerde aile içinde çekilen fotoğrafların aile bireyleri tarafından işlenmesinin istisna kapsamında olduğu, incelemeye konu faaliyetin ise bir serbest girişimci tarafından broşür gönderimi suretiyle ilgili kişiye ait kişisel veri niteliğindeki isim ve adres bilgilerinin işlenmesi olduğu ve somut olayda aynı konutta yaşayan aile fertlerinin kişisel verilerinin yine aile bireyleri tarafından işlenmesi söz konusu olmadığından bu istisna hükmünün veri sorumlusu sıfatını haiz olan gerçek kişi bakımından uygulanamayacağı,

- Gerçek kişi veri sorumlusu tarafından, ilgili kişinin velisinin daha önce ilgili kişinin isim ve adres bilgilerini kullanarak bir e-ticaret sitesi üzerinden kendi nam ve hesabına sattığı şirket ürünlerine ilişkin sipariş oluşturduğu ve bu sipariş teslim edilirken broşürün de iletilmesine ilişkin iddiaları

bakımından yapılan incelemede, 213 sayılı Vergi Usul Kanunu'nun (VUK) 231'inci maddesinin 5'inci bendinin "Fatura, malın teslimi veya hizmetin yapıldığı tarihten itibaren azami yedi gün içinde düzenlenir. Bu süreler içerisinde düzenlenmeyen faturalar hiç düzenlenmemiş sayılır." hükmü ile Mesafeli Sözleşmeler Yönetmeliği'nin 16'ncı maddesinin somut olay tarihindeki birinci fıkrasında yer alan "Satıcı veya sağlayıcı, tüketicinin siparişinin kendisine ulaştığı tarihten itibaren taahhüt ettiği süre içinde edimini yerine getirmek zorundadır. Mal satışlarında bu süre her halükarda otuz günü geçemez." hükmünü haiz olduğu, bununla birlikte ilgili kişiye e-ticaret sitesi üzerinden gönderilen sipariş ile broşür arasında dört buçuk aylık bir süre olduğu, broşürün e-ticaret sitesi üzerinden verilerin sipariş ile birlikte iletilmediği, öte yandan veri sorumlusu tarafından tanıtım ve pazarlama amaçlı olarak kişisel veri işlenebilmesi için açık rıza alındığına dair ispat edici bir belge ibraz edilemediği göz önüne alındığında veri sorumlusunun tanıtım ve pazarlama amacıyla broşür göndermesi suretiyle ilgili kişinin kişisel veri niteliğindeki isim ve adres bilgilerini işlemesinin Kanun'un 5'inci maddesinde yer alan işleme şartlarından herhangi birine dayanmadığı değerlendirilmelerinden hareketle;

- İlgili kişiye broşürü gönderen gerçek kişinin şirketle imzalamış olduğu sözleşme koşullarına göre serbest girişimci olduğu, şirket ürünlerinin satışı konusunda müşterilerle hizmet ilişkisinde bulunurken şirketten bağımsız olarak hareket ettiği, dolayısıyla serbest girişimci gerçek kişinin, müşterilerine ait kişisel veri işleme faaliyetinde bulunurken şirketten bağımsız bir şekilde veri sorumlusu sıfatını haiz olduğu, bu çerçevede şirketin incelemeye konu kişisel veri işleme faaliyetine dair bir ilgisinin bulunmaması sebebiyle şirket hakkında Kanun kapsamında tesis edilecek herhangi bir işlem bulunmadığına,
- İlgili kişi adına mektup yolu ile tanıtım amaçlı broşürün gönderilmesi suretiyle ilgili kişinin kişisel verisi niteliğindeki isim ve iletişim bilgilerinin işlenmesinin veri sorumlusu tarafından ibraz edilen faturaya konu sipariş ile bir bağlantısı olmadığı, ilgili kişiye tanıtım amaçlı gönderilen broşürün faturada belirtilen sipariş ile birlikte gönderilmediği, incelemeye konu salt broşür gönderiminin Kanun'da tanımlı işleme şartlarından herhangi birine dayanılmaksızın gerçekleştirildiği, bu bakımdan Kanun'un 12'nci maddesinin (1) numaralı fıkrasındaki yükümlülüklerin yerine getirilmediği ve kabahate konu eylemin yalnızca bir kez gerçekleştirildiği kanaatine varıldığından, 5326 sayılı Kabahatler Kanunu'nun 17'nci maddesinin (2) numaralı fıkrası uyarınca işlenen kabahatin haksızlık içeriği ile veri sorumlusunun kusuru ve ekonomik durumu birlikte göz önünde bulundurulduğunda veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 30.000 TL idari para cezası uygulanmasına,

Tanıtım ve pazarlama amaçlarıyla kişisel verilerin işlenmesinde ilgili kişilerin açık rızalarının alınması ve Kanun hükümlerine riayet edilmesi gerektiğine ilişkin satış görevlilerinin bilgilendirilmesi gerektiği hususunun pazarlama şirketine bildirilmesine karar verilmiştir.

2022/774 sayılı KVKK Kararı

Veri sorumlusu bir e-ticaret sitesinden alışveriş yapan üçüncü kişiye ait sipariş bilgilerinin ilgili kişinin e-posta adresine gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 03/08/2022 tarihli ve 2022/774 sayılı Karar Özeti

Karar Tarihi : 03/08/2022

Karar No : 2022/774

Konu Özeti: Veri sorumlusu bir e-ticaret sitesinden alışveriş yapan üçüncü kişiye ait sipariş bilgilerinin ilgili kişinin e-posta adresine gönderilmesi

Kuruma intikal eden şikayette özetle; ilgili kişinin e-posta adresine bir e-ticaret sitesinden alışveriş yapan üçüncü bir kişinin sipariş bilgilerinin gönderildiği, söz konusu e-posta içeriğinde ödenen tutar, resimli olarak siparişin içeriği, gönderici adı soyadı, alıcının adı soyadı, adresi, telefon numarası gibi bilgilerin açık bir biçimde yer aldığı, ayrıca e-postada yer alan "Sipariş Takibi ve Güncelleme" adlı buton sayesinde tüm sipariş detaylarının görülebileceği bir sayfaya yönlendirme yapıldığı, bu sayfada ise gönderici ve alıcı bilgilerine ek olarak sipariş edilen ürünün içerik adı, ürün kodu, rengi ve gönderici tarafından alıcıyı muhatap gönderi notunun görüntülediği, gönderici veya alıcı bilgileri ile gönderi notu bilgilerinin düzenlenebilir durumda olmakla birlikte sipariş iptal butonunun da aktif olduğu, söz konusu olayların veri ihlali olduğunu tespit ederek ve şahsına ait kişisel verilerinin de belirttiği şekilde başkaları tarafından görülebileceğini düşünerek öncelikle e-ticaret sitesine ait müşteri hizmetleriyle canlı destek sistemi üzerinden irtibata geçtiği, müşteri hizmetleri tarafından müşterinin isim benzerliği neticesinde yanlış e-posta verdiği, bu sebeple söz konusu sipariş bildirimini iletildiğinin, bu sipariştan kendisine ait e-posta adresinin silindiğinin ve artık kendisine bildirim iletilmeyeceğinin ifade edildiği, ancak bahse konu e-posta adresine halen veri sorumlusu e-ticaret sitesi tarafından reklam içerikli e-postaların iletildiği, konunun hata olarak nitelendirilmesinin kişisel verilerin ihlali gerçeğini değiştirmede, bu itibarla veri ihlalinin önlemek adına güvenlik tedbirlerinin alınması konusunda tüm iletişim kanalları üzerinden veri sorumlusuna bilgilendirmede bulunmasına karşın kendisine herhangi bir dönüş yapılmadığı belirtilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- İlgili kişinin konu hakkında kendilerine başvurduğu ve başvuruya ilişkin cevabın ilgili kişinin ikamet adresine gönderildiği,
- İlgili kişinin 20.10.2014 tarihinde şikâyete konu edilenden farklı bir e-posta ile söz konusu e-ticaret sitesine üyelik oluşturduğu, e-ticaret sitesine kayıtlı tüm üyelerin bilgilerinde yapılan araştırmalar neticesinde şikâyete konu siparişte kullanılan e-posta adresi için bir üyelik hesabının bulunmadığı,
- Söz konusu siparişin, bir başka kullanıcı tarafından isim benzerliğinden kaynaklı olarak sehven ilgili kişiye ait e-posta adresinin bildirilerek üyelik hesabı açılmaksızın misafir müşteri girişi ile oluşturulduğu ve e-posta ile SMS gönderimi için açık rızanın verildiği,
- Üyelik hesabı açmadan oluşturulan siparişlerde kullanıcıların “Kişisel verileriniz, Kişisel Verilerin Korunmasına İlişkin Aydınlatma Metni kapsamında işlenmektedir.” bilgisi ile karşılaştığı ve burada aydınlatma yükümlülüğünün yerine getirilmesini sağlayan konularda bilgilendirmelerde bulunulduğu, ilgili kullanıcıların siparişin bir sonraki adımına geçmeyi kabul etmeleri hâlinde kişisel verilerinin işlendiği,
- İlgili kişinin veri sorumlusuna yaptığı başvuruda kendisine reklam içerikli e-posta gönderilmemesi ile ilgili olarak herhangi bir talepte bulunmadığı,
- Tüm müşterilere diledikleri zaman ticari elektronik ileti almayı reddetmeleri için imkân sağlandığı ve veri sorumlusu tarafından gönderilen tüm ticari elektronik iletilerde bu hususun yer aldığı, ayrıca bu yöndeki şikâyetlerin muhatabının da Kurum değil Ticaret Bakanlığının il ve ilçe müdürlükleri olduğu,
- Şikâyete konu somut olayda, bir başka gönderici tarafından sehven ilgili kişinin e-posta adresinin sisteme girilmesi, ilgili kişiye ait e-posta adresinin ilgili kişiye ait herhangi bir kayıtlı eşleşmemesi ve veri sorumlusunun bu olayda kastının bulunmadığı dikkate alındığında Kanun’un 12’nci maddesinin ihlal edildiğinden söz edilemeyeceği,
- Diğer yandan üye olmaksızın misafir müşteri girişi ile yapılan alışverişler esnasında alışveriş yapan kişi tarafından kendisine ait e-posta veya telefon numarası girilmek istenirken sehven hatalı olarak girilen başkalarına ait e-posta ve telefon numaralarının e-ticaret sitesi tarafından teyit edilebilmesine yönelik olarak da teknik geliştirme yapılması çalışmalarına başlandığı ve tamamen kontrol dışında gerçekleşen bu durumun önüne geçmek ve hatalı veri girişlerini engellemek amacıyla planlamaların yapıldığı

ifade edilmiştir.

Konuya ilişkin olarak yapılan incelemede Kişisel Verileri Koruma Kurulunun 03/08/2022 tarihli ve 2022/774 sayılı Kararı ile;

- 6698 sayılı Kanun'un "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, "belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza", (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi" olarak tanımlandığı,

- Kanun'un "Genel İlkeler" başlıklı 4'üncü maddesinde, kişisel verilerin ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, buna göre, kişisel verilerin ancak; a) Hukuka ve dürüstlük kurallarına uygun olma, b) Doğru ve gerektiğinde güncel olma, c) Belirli, açık ve meşru amaçlar için işlenme, ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ile d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceği,

- Kanun'un 5'inci maddesinin kişisel verilerin işlenme şartlarını düzenlediği, maddenin (1) numaralı fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin, (2) numaralı fıkrasında ise, kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda olan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün korunması için veri işlemenin zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaati için veri işlenmesinin

zorunlu olması hallerinde ilgili kişinin açık rızası olmaksızın kişisel verilerin işlenmesinin mümkün olduğunun hükme bağlandığı

Buna göre;

İlgili kişinin kişisel verisi niteliğindeki e-posta adresinin Kanuna aykırı bir biçimde işlendiğine yönelik iddiası hakkında;

- Veri sorumlusunun, müşterilerine üye olma seçeneği sunduğu, bu kapsamda üyelik oluşturan kişilerden manuel girilebilecek şekilde e-posta bilgisini beyan etmelerini istediği, veri sorumlusu tarafından üyeliği olmayan müşterilere de hizmet verildiği, üyelik kaydı bulunmaksızın sipariş oluşturan müşterilerden gerek hizmetin ifası gerekse e-faturanın gönderilmesi gibi amaçlarla e-posta bilgisinin yine manuel olarak girilebilecek şekilde beyan etmelerinin istendiği,
- Veri sorumlusu tarafından, ilgili kişinin üyelik bilgilerinde yalnızca “xxx” e-posta adresinin olduğu, ilgili kişi ile aynı isme sahip üçüncü kişinin üyelik oluşturmadan misafir müşteri girişi ile ilgili kişiye ait bir diğer e-posta adresi olan “yyy” adresini sehven girerek sipariş verdiği, “yyy” e-posta adresi için ilgili kişi veya bir başka kişi için üyelik hesabı bulunmadığı, e-postanın ilgili kişiye ait herhangi bir veriyle eşleşmediği veya ilgili kişiye ait kimlik bilgilerinin işlenmediği, misafir müşteri girişi ile yapılan alışverişler esnasında girilen e-posta ve telefon numaralarının teyit edilebilmesine yönelik olarak henüz bir kontrol mekanizmasının bulunmadığının belirtildiği, veri sorumlusunun cevabi yazı eki incelendiğinde de, ilgili kişinin üyelik bilgisinde “xxx” e-posta adresinin olduğu ve sistemlerinde “yyy” e-posta adresinin yer almadığının görüldüğü, diğer yandan ilgili kişinin şikâyet ekinde “yyy” e-posta adresine kendisi tarafından oluşturulmayan bir siparişe dair e-ticaret sitesi tarafından bilgilendirme e-postasının gönderildiğine ilişkin ekran görüntülerinin yer aldığı,
- İlgili kişiye gönderilen sipariş bilgilendirme e-postasında; söz konusu siparişe dair detayların bulunduğu, hediye olarak gönderilen bu siparişte gönderici adının ve cep telefonu numarasının yer aldığı, bunun yanında alıcı adının, cep telefonu numarasının ve adresinin açıkça yer aldığı,
- Bireyler tarafından manuel olarak yapılan bilgi girişlerinde yanlış beyanlarda bulunulabilmesinin muhtemel olduğu, veri sorumluları tarafından ise Kanun’un 12’nci maddesinin (1) numaralı fıkrasında tanımlanan kişisel verilerin hukuka aykırı olarak işlenmesini önlemeye yönelik idari ve teknik tedbirlerin alınması yükümlülüğü kapsamında, bu yanlış bilgi girişleri sebebiyle üçüncü kişilere ait kişisel verilerin hukuka aykırı bir biçimde işlenmesinin önüne geçilebilmesi adına, kendilerine bildirilen iletişim bilgilerinin doğruluğunu teyit edecek mekanizmaların oluşturulmasına yönelik gerekli idari ve teknik tedbirlerin alınması gerektiği,

- Dolayısıyla somut olayda şikâyete konu siparişin kendisi tarafından verilmemesine karşın ilgili kişinin kişisel verisi niteliğindeki “yyy” e-posta adresine veri sorumlusu tarafından bilgilendirme e-postası gönderilmek suretiyle kişisel veri işleme faaliyetinde bulunulduğu, bu işleme faaliyetinin Kanun’un 5’inci maddesinde yer alan işleme şartlarından herhangi birine dayanılmaksızın gerçekleştirildiği,

- Bu çerçevede söz konusu işlemde bir teyit mekanizmasının bulunmaması nedeniyle e-ticaret sitesine üye olmadan misafir girişi ile yapılan tüm alışveriş işlemlerinin veri ihlal riski taşıdığı,

- Bilgilendirme e-postalarının, gönderici ve alıcılara ait ad, soyad, T.C. kimlik numarası, adres, telefon, e-posta, sipariş bilgileri gibi bilgileri ihtiva edebileceği, bilgilendirme e-postasının konu ile ilgisiz üçüncü bir kişiye gönderilmesinin, konu ile ilgisiz üçüncü kişinin kişisel verisinin hukuka aykırı bir biçimde işlenmesi sonucunu doğurduğu gibi içerikte yer alan kişisel verilerin olduğu gibi üçüncü bir kişiye açıklanarak bu verilerin başkaları tarafından kötü niyetli olarak kullanılmasına da zemin hazırlayabileceği

İlgili kişinin Kanun kapsamında yaptığı başvuruya veri sorumlusu tarafından cevap verilmediğine yönelik iddiası hakkında:

- İlgili kişinin Kanun kapsamında başvuru yapmak maksadıyla doldurduğu başvuru formu ile veri sorumlusunun cevabi yazı ve ekinde yer alan bahse konu belgeler incelendiğinde ve gönderi takip formunda yer alan gönderi barkod numarası sorgulandığında; başvuruya verilecek yanıtın tarafına bildirilme yöntemi olarak yalnızca “Adresime gönderilmesini istiyorum” kutucuğunu işaretlediği, veri sorumlusu tarafından ilgili kişiye cevap verildiği, bu cevabın ilgili kişinin belirttiği şekilde adresine teslim edildiğinin görüldüğü, bu sebeple veri sorumlusu tarafından ilgili kişinin yaptığı başvuruya cevap verildiğinin anlaşıldığı,

İlgili kişinin e-posta adresine veri sorumlusu tarafından kendisine ait e-posta adresinin silindiğinin ve artık kendisine bildirim iletilmeyeceğinin ifade edilmesine rağmen hâlen reklam içerikli e-postaların iletildiğine yönelik iddiası hakkında:

- İlgili kişinin şikâyet dilekçesi ve ekinde; söz konusu siparişe dair gönderilen bilgilendirme e-postalarının, bunun üzerine e-ticaret sitesi asistanı üzerinden gerçekleştirmiş olduğu görüşme trafiğinin ekran görüntüsünün ve Kanun kapsamında yapmış olduğu başvurusunun yer aldığı görüldüğü, veri sorumlusunun cevabi yazı ekinde, bu belgelerin yanı sıra ilgili kişiye verilen yanıtın yer aldığı dokümanlar incelendiğinde; bahse konu sipariştten ilgili kişinin kişisel verisi niteliğindeki e-posta adresinin silindiğinin ve kendisine bildirim iletilmeyeceğinin müşteri hizmetleri ile yapılan

görüşmede ifade edildiği, bununla birlikte ilgili kişinin veri sorumlusuna başvurusunda hâlen kendisine reklam içerikli e-postanın iletmeye devam edildiğine dair bir ifadesine rastlanılmadığı ve ilgili kişinin Kuruma ilettiği şikayetinde reklam içerikli e-posta iletmeye devam edildiği iddiasına yönelik tevsik edici herhangi bir bilgi ve belgeye yer verilmediği,

Veri sorumlusunun tüm müşterilere diledikleri zaman ticari elektronik ileti almayı reddetmeleri için imkân sağlandığına, e-ticaret sitesi tarafından gönderilen tüm ticari elektronik iletilerde sunulan bu imkânın belirtildiğine, bu yöndeki şikâyetlerin muhatabının Kurumun değil Ticaret Bakanlığının il ve ilçe müdürlüklerinin olduğuna yönelik açıklamaları hakkında:

- Telefon ve e-posta bilgisinin bir iletişim bilgisi olduğu, bu iletişim bilgilerinin kişisel veri olduğu, kişisel veriler üzerinde Kanun'da belirtilen yollarla gerçekleştirilen her türlü işlemin bir işleme faaliyeti olduğu, bu bilgilerin kişiyi belirlenebilir kılmak maksatlı işlendiği, dolayısıyla SMS ya da e-posta yoluyla ticari elektronik ileti gönderilmesi suretiyle bir kişinin e-posta ya da cep telefonu bilgisinin kullanılmasının bir kişisel veri işleme faaliyeti olduğu ve kişisel verilerin hangi işleme şartlarına dayalı olarak işlenmesi gerektiğini düzenleyen Kanun kapsamında değerlendirileceği

değerlendirmelerinden hareketle;

- Veri sorumlusu tarafından taraflara yönelik bir teyit mekanizması kurulmadan satış sözleşmesi ile ilgisiz üçüncü kişi konumundaki ilgili kişiye sipariş bilgilendirmesine dair e-posta gönderilmesi suretiyle kişisel verisinin Kanun'un 5'inci maddesinde yer alan işleme şartlarından herhangi birine dayanılmaksızın işlendiği, bu bakımdan Kanun'un 12'nci maddesinin (1) numaralı fıkrasındaki yükümlülüklerin yerine getirilmediği kanaatine varıldığından, veri sorumlusunun 550+ çalışan ve 40.000+ tedarikçi açısından oluşan bir ekiple süreçlerini yürütmekte olduğu, şikayete konu olayda veri sorumlusunun Kanun'un 12'nci maddesindeki yükümlülüklerini yerine getirmeyerek ihmali davranışla e-postanın gönderileceği alıcı gruplarına yönelik bir teyit mekanizması kurmadan uzaktan satış sözleşmesinin tarafı olmayan ilgili kişinin e-posta adresinin işlenmesine, dolaylı olarak e-postada yer alan gönderici ve alıcıya ait bilgilerinin ise ilgili kişiye açıklanmasına sebebiyet verildiği, bu e-postanın yanlış muhataba gönderilmesi halinde hak kaybına yol açabileceği hususları da dikkate alınarak, veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 120.000 TL idari para cezası uygulanmasına,

- İlgili kişinin Kanun kapsamında yapmış olduğu başvuruya veri sorumlusu tarafından yasal süreler içinde cevap verildiğinin görülmüş olması sebebiyle ilgili kişinin veri sorumlusu tarafından

başvuruya cevap verilmediği iddiasına yönelik olarak veri sorumlusu hakkında Kanun kapsamında yapılacak herhangi bir işlem olmadığına karar verilmiştir.

2022/768 sayılı KVKK Kararı

Veri sorumlusu banka tarafından ilgili kişinin kişisel verilerinin açık rızası alınmaksızın bir sigorta şirketine aktarılması hakkındaki Kişisel Verileri Koruma Kurulunun 03/08/2022 tarihli ve 2022/768 sayılı Karar Özeti

Karar Tarihi : 03/08/2022

Karar No : 2022/768

Konu Özeti: Veri sorumlusu banka tarafından ilgili kişinin kişisel verilerinin açık rızası alınmaksızın bir sigorta şirketine aktarılması

İlgili kişinin Kuruma intikal eden şikâyet dilekçesinde özetle; şahsi telefonundan bir sigorta şirketince pek çok kez arandığı, sigorta şirketi ile yapılan görüşmede cep telefonu numarasının veri sorumlusu bir banka aracılığıyla elde edildiğini öğrendiği, veri sorumlusu bankada hesabının bulunduğu fakat veri sorumlusu dışında veri sorumlusuyla ilişkili başkaca bir kurum veya kuruluşla ilişkisinin bulunmadığı, bu çerçevede veri sorumlusuna başvuru yapıldığı ancak veri sorumlusu tarafından verilen cevabın 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 12'nci maddesine aykırılık teşkil ettiği ve yeterli olmadığı ifade edilerek Kanun kapsamında gereğinin yapılması talep edilmiştir.

Söz konusu iddialara ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişinin 2015 yılından beri veri sorumlusunun müşterisi olduğu, ilgili sigorta şirketi ile veri sorumlusunun arasında sigorta acentelik sözleşmesinin bulunduğu, bu kapsamda veri sorumlusunun, sigorta şirketinin ürünlerinin satış ve pazarlanması noktasında yetkili acente olarak hizmet verdiği,
- 5411 sayılı Bankacılık Kanunu'nun 73'üncü maddesi gereği bankaların hizmet ve destek hizmeti aldığı kuruluşlar ve finansal kuruluşlar ile müşteri sırrı niteliğindeki bilgi ve belgeleri yalnızca hizmetin kapsamı ile sınırlı olarak paylaşabildiği, bu durumun Kanun'un 5'inci maddesinin (2) numaralı fıkrasındaki işleme şartlarına dayandığı ve bu nedenle bankaların acentesi oldukları sigorta şirketi ile olan bilgi paylaşımının da bu yasal düzenlemeler çerçevesince gerçekleştiği,

- İlgili kişinin veri sorumlusu tarafından kampanya, hizmet ve ürünlerle ilgili kısa mesaj, e-posta, posta ve arama şeklinde ticari elektronik ileti gönderilmesine yönelik izninin ve bu amaçla kişisel verilerinin işlenmesi konusunda rızasının bulunduğu, bu kapsamda konut sigortası için acentecilik yetkisi doğrultusunda ilgili kişinin aranarak ürün teklifinde bulunulduğunun anlaşıldığı,
- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'un yürürlük tarihi olan 01.05.2015 tarihinden önce doğrudan hizmet teminine ilişkin kurulmuş bir ilişki çerçevesinde temin edilen iletişim bilgilerinin kullanılması sebebiyle Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik'in "Mevcut Veri Tabanı Kullanımı" başlıklı Geçici 1'inci maddenin ikinci fıkrası gereği müşteriye ait iletişim bilgisinin onaylı veri sayıldığı,
- Veri sorumlusu ile ilgili kişi arasında sözleşmesel ilişkinin mevcut olduğu, veri sorumlusunda halen açık ürün ve hesaplarının yer aldığı ve ilgili kişinin bu duruma ilişkin aksi yönde bir beyanının bulunmadığı,
- Kanun'un Geçici 1'inci maddesinin (3) numaralı fıkrasına göre Kanun'un yayımı tarihinden önce oluşturulan sözleşmesel ilişki ile ilgili kişi tarafından, veri sorumlusunca sunulan ürün, hizmet ve avantajlardan yararlanmak için söz konusu hizmet ve pazarlamanın gerektirdiği kapsamda kişisel verilerinin işlenmesi ve buna dair iletilerin gönderilmesi konusunda onay verildiğinden bu durumun Kanun'un 5'inci maddesine aykırılık oluşturmadığı, ilgili kişinin Kanun'un geçiş süresi dahilinde aksi bir irade beyanında bulunmadığı

ifade edilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 03/08/2022 tarih ve 2022/768 sayılı Kararı ile;

- 6698 sayılı Kanun'un "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi" olarak tanımlandığı,

• Kanun'un 5'inci maddesinin kişisel verilerin işleme şartlarını düzenlediği, maddenin (1) numaralı fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin, (2) numaralı fıkrasında ise, kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda olan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün korunması için veri işlemenin zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaati için veri işlenmesinin zorunlu olması hallerinde ilgili kişinin açık rızası olmaksızın kişisel verilerin işlenmesinin mümkün olduğunun hükme bağlandığı,

• Kanun'un "Kişisel Verilerin Aktarılması" başlıklı 8'inci maddesinde ise "(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz. (2) Kişisel veriler; a) 5 inci maddenin ikinci fıkrasında, b) Yeterli önlemler alınmak kaydıyla 6'ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir. (3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır." hükmünün yer aldığı,

• Ayrıca Kanun'un "Geçiş Hükümleri" başlıklı Geçici 1'inci maddesinin (3) numaralı fıkrasında; "Bu Kanunun yayımı tarihinden önce işlenmiş olan kişisel veriler, yayımı tarihinden itibaren iki yıl içinde bu Kanun hükümlerine uygun hâle getirilir. Bu Kanun hükümlerine aykırı olduğu tespit edilen kişisel veriler derhâl silinir, yok edilir veya anonim hâle getirilir. Ancak bu Kanunun yayımı tarihinden önce hukuka uygun olarak alınmış rızalar, bir yıl içinde aksine bir irade beyanında bulunulmaması hâlinde, bu Kanuna uygun kabul edilir." hükümlerinin bulunduğu,

• Bu çerçevede, veri sorumlusunun Kanun'un 8'inci maddesi kapsamında kişisel verilerin aktarımı hususuna gerekçe gösterebileceği üç durum bulunduğu, somut olayda veri sorumlusunun ilgili veri işleme faaliyetini Kanun'un 5'inci maddesinin (2) numaralı fıkrasında sıralanan veri işleme şartlarından birine dayandırmaması durumunda ilgili kişiden açık rıza alma yoluna gitmesi veya kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümleri gerekçe olarak sunması gerektiği,

• Bu bağlamda veri sorumlusunun Kuruma ilettiği savunmasında yer alan ilgili kişinin ticari elektronik ileti gönderimine izin verdiğini gösteren belgenin "Kampanya İletişim Tercihleri Talimatı" olduğu, ilgili talimatın incelenmesi neticesinde "Bankanızın tüm fırsat ve kampanyalarına ilişkin tüm

kanallardan tanıtım iletisi almak istiyorum” seçeneğinin, “İleti almak istediğim kanal/kanallar” başlığı altındaki “Hepsi, SMS, telefon, E-mail, adres” seçeneklerinden “Hepsi” seçeneğinin , “İleti almak istediğim ürün/ürünler” başlığı altında “Elementer Sigortayı” (Hayat sigortası dışındaki sigortaların genel adı) da içerecek şekilde yine “Hepsi” ibaresinin seçili olduğunun tespit edildiği, ilgili kişinin şikâyet konusu özelinde kişisel verilerinin aktarılacağı bilgisinin kendisine sunulmadığı ve bu durumun açık rızanın “bilgilendirmeye dayanma” ilkesine aykırılık teşkil ettiği ve dolayısıyla ilgili belgenin kişisel verilerin aktarılması kapsamında açık rıza örneği teşkil etmediği,

- İlgili talimat ekranının en alt kısmında “İşbu formda yer alan “tüm kanal ve ürünler” seçeneğinin seçilmesi suretiyle izin verilen kanal ve ürünler, formun imzalanmasından sonraki bir tarihte Bankaca kullanılabilir ve/veya tanımlanabilecek kanal ve ürünleri de kapsayacaktır.” ifadesinin yer aldığı, bu ifadenin açık rıza şartlarından “özgür iradeye dayanma” unsuruna uygun olmadığı, geleceğe yönelik muğlak bir ifade olduğu, aynı unsura aykırılık oluşturduğu izlenimi yaratan bir diğer hususun ise ilgili belgede kutucukların otomatik olarak doldurulduğunun gözlemlenmesi olduğu, bu kutucukların ilgili kişinin kendi iradesiyle doldurulduğunun şüphe barındırdığı, zira veri sorumluları tarafından ilgili kişilerden alınacak açık rıza beyanlarında opt-out yani bireyin önceden onayını almaksızın kişisel verilerinin işlenmesine otomatik onay verdiklerinin kabul edildiği ve bu kapsamda kişilere bu onayı kaldırmaları yönünde imkân veren bir sistemin değil, opt-in yani bireyin bilinçli eylemi ile kişisel verilerinin işlenmesine onay vereceği bir sistemin kullanılmasının gerekli olduğu; veri sorumlusunun savunmasında ise, kutucukların ilgili kişi tarafından doldurulduğunu ispatlayıcı herhangi bir ifadeye yer verilmediği,

- Yukarıda izah olunan nedenlerle veri sorumlusu tarafından Kuruma sunulan savunmada yer verilen belge ve ifadelerin gerek genel anlamda gerek somut olay özelinde kişisel verilerin aktarımına yönelik ilgilinin açık rızasının bulunduğu kanıtlar nitelik taşımadığı,

- Ek olarak, veri sorumlusunun Kuruma sunduğu savunmasında, 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun’un yürürlük tarihi olan 01.05.2015 tarihinden önce doğrudan hizmet teminine ilişkin kurulmuş bir ilişki çerçevesinde temin edilen iletişim bilgilerinin kullanılması sebebiyle Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik’in “Mevcut Veri Tabanı Kullanımı” başlıklı Geçici 1’inci maddesinin 2’nci fıkrası gereği ilgili kişiye ait iletişim bilgisini onaylı veri saydıkları, kişinin de 6698 sayılı Kanun’un geçiş süreci dahilinde aksi bir irade beyanında bulunmadığı ve dolayısıyla bu durumun Kanun’un Geçici 1’inci maddesinin (3) numaralı fıkrasına uygunluk teşkil ettiğinin belirtildiği ancak veri sorumlusunun bu noktadaki savunmasının asıl

şikayet konusu olan ilgili kişinin kişisel verisinin aktarımı hususuna uygun bir hukuki gerekçe sunmadığı,

- Öte yandan 5411 sayılı Bankacılık Kanunu'nun "Sırların Saklanması" başlıklı 73'üncü maddesinin göre "...bu maddede belirtilen sır saklama yükümlülüğünden istisna tutulan hâller haricinde, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca müşterinin açık rızası alınsa dahi, müşteriden gelen bir talep ya da talimat olmaksızın yurt içindeki ve yurt dışındaki üçüncü kişilerle paylaşılamaz ve bunlara aktarılamaz." şeklinde düzenlendiği,

- Yine ilgili Kanun'un "Tanımlar ve kısaltmalar" başlıklı 3'üncü maddesinde "Finansal Kuruluş" tanımının "Kredi kuruluşları dışında kalan ve sigortacılık, bireysel emeklilik veya sermaye piyasası faaliyetlerinde bulunmak veya bu Kanunda yer alan faaliyet konularından en az birini yürütmek üzere kurulan kuruluşlar ile kalkınma ve yatırım bankaları ve finansal holding şirketlerini ifade eder." şeklinde yapıldığı,

- Bununla beraber, Bankacılık Kanunu'nun 73'üncü maddesine dayanılarak hazırlanan Sır Niteliğindeki Bilgilerin Paylaşılması Hakkındaki Yönetmelik'in "Sır saklama yükümlülüğü" başlıklı 4'üncü maddesinin (4)'üncü bendinin "Kişisel veriler de dâhil olmak üzere, bankalar ile müşteri ilişkisi kurulmadan önce de var olan ve başka bir bankanın müşteri sırrı niteliğinde olmayan gerçek ve tüzel kişilere ilişkin veriler, tek başına sır kapsamında bulunmamakla birlikte, ilgili kişinin banka müşterisi olduğunu gösterecek şekilde, tek başına ya da üçüncü fıkrada belirtilen müşteri ilişkisinin kurulmasından sonra oluşan verilerle birlikte işlendiğinde, müşteri sırrı haline gelir. Söz konusu verilere ilişkin birinci fıkra kapsamındaki yükümlülük, bu verilerin müşteri sırrı haline gelmesinden itibaren başlar." ve "Sır saklama yükümlülüğünden istisna tutulan haller" başlıklı 5 inci maddesi "... (2) Gizlilik sözleşmesi yapılması ve sadece belirtilen amaçlar ile sınırlı kılınması koşuluyla banka sırrı ya da müşteri sırrı niteliğindeki bilgilerin aşağıdaki durumlarda paylaşımı sır saklama yükümlülüğüne aykırılık teşkil etmez: a) Bankaların ve finansal kuruluşların, kendi aralarında doğrudan doğruya ya da Risk Merkezi veya en az beş banka ya da finansal kuruluş tarafından kurulacak şirketler vasıtasıyla her türlü bilgi ve belge alışverişinde bulunması..." hükümlerini içerdiği,

- Somut olayda, veri sorumlusunun savunmasında şikâyet konusu veri işleme faaliyetine yönelik Kanun kapsamında bir açık rıza aldığına dair ve kişinin şikâyet konusu veri işleme faaliyeti yönünde bir talimatının veya talebinin olduğuna dair kanıtlayıcı bilgi ve/veya belgeye rastlanılmadığı, yukarıda ifade edilen ilgili Yönetmelik uyarınca veri sorumlusunun sır saklama yükümlülüğünden istisna tutulabilmesi adına sadece belirtilen amaçlarla sınırlı kalınması şartıyla düzenlemesi gereken

gizlilik sözleşmesine Kuruma sunulan bilgi ve belgeler arasında rastlanılmadığı, nihayetinde veri sorumlusunun ilgili kişinin kişisel verilerini ilgili sigorta şirketi ile paylaşması hususunda Kanun'un 8'inci maddesindeki şartları sağlamadığı

değerlendirmelerinden hareketle;

- İlgili kişinin kişisel verisi niteliğinde olan telefon numarasının, veri sorumlusu tarafından Kanun'un 5'inci maddesinde yer alan kişisel veri işleme şartlarından herhangi birine dayanılmaksızın ilgili sigorta şirketine Kanun'un 8'inci maddesine aykırı olarak aktarıldığı; bu minvalde Kanun'un 12'nci maddesinin (1) numaralı fıkrasında öngörülen kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli idari ve teknik tedbirlerin alınması yükümlülüğünün yerine getirilmediği göz önünde bulundurulduğunda veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 250.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2022/655 sayılı KVKK Kararı

Tasfiye edilmiş şirketin yönetim kurulu üyeleri olan ilgili kişilerin kişisel verilerinin, şirket borcu kapsamında kısa mesaj gönderme ve arama suretiyle veri sorumlusu avukat tarafından hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 07/07/2022 tarihli ve 2022/655 sayılı Karar Özeti

Karar Tarihi : 07/07/2022

Karar No : 2022/655

Konu Özeti: Tasfiye edilmiş şirketin yönetim kurulu üyeleri olan ilgili kişilerin kişisel verilerinin şirket borcu kapsamında kısa mesaj gönderme ve arama suretiyle veri sorumlusu avukat tarafından hukuka aykırı olarak işlenmesi

İlgili kişilerin vekillerinin Kuruma intikal eden şikâyet dilekçesinde özetle; ilgili kişilerin ortağı olduğu ve tasfiyesi gerçekleşmiş limited şirkete ait olduğu iddia edilen bir borç nedeniyle veri sorumlusu avukatın ve bünyesinde çalışanların ilgili kişilerle kısa mesaj gönderme ve arama yoluyla iletişim kurduğu ve bu kapsamda kişisel verilerinin işlendiği, konuya ilişkin yapılan başvuruya veri sorumlusunun verdiği cevap yazısında, ilgili kişilerin ortağı oldukları şirketin bir telekomünikasyon şirketine- veri sorumlusu bu şirketin vekilliğini yürütmektedir- olan borcundan ötürü icra takibi başlatılması nedeniyle Ticaret Sicil Gazetesi'nden ilgili şirketin ortaklarının kimlik bilgilerine, bilinmeyen numaralar hizmeti sunan operatörler aracılığıyla ise telefon numaralarına ulaşıldığı, yapılan başvuru neticesinde veri sorumlusunca ilgili telefon numaralarına erişimin engellendiği ve bu numaranın başka bir kişi ile paylaşımının mümkün olmadığı, işlenen verilerin ise geri dönülemez şekilde yok edilmiş olduğu yönünde açıklamada bulunulduğu, buna karşın şirket ortaklarının şirket borçlarından dolayı şahsi sorumluluklarının bulunmaması sebebiyle yapılan veri işleminin hukuki bir temeli olmadığı, kendilerini arayan veri sorumlusu çalışanlarına defaten şirketin tasfiye edildiği, alacağın zamanaşımına uğradığı ve aranmak istemedikleri belirtilse de şikâyete konu fiillerin devam ettirildiği ayrıca aydınlatma yükümlülüğünün her bir veri işleme faaliyeti yönünden yerine getirilmediği ifade edilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Söz konusu iddialara ilişkin başlatılan inceleme çerçevesinde veri sorumlusu avukattan savunması istenilmiş olup, Kuruma intikal eden cevabi yazıda özetle;

- Somut olaya konu telekomünikasyon şirketinin vekili olması nedeniyle ilgili şirketin borcuna ilişkin başlatılan icra takibi gereğince borcun tahsili amacıyla Ticaret Sicil Gazetesi üzerinden yapılan sorguda şirket ortağı olarak ilgili kişilerin adlarına ulaşıldığı, ilgili kişilere ait telefon numarası bilgilerinin ise icra dosyası borçlusunu olan şirketin ortağı olmaları sebebiyle Bilgi Teknoloji Kurumu tarafından yetkilendirilmiş rehberlik hizmeti sağlayan kuruluşlardan biri olan bilinmeyen numaralar hizmeti sunan operatörler kullanılarak elde edildiği,
- Benzer şekilde Türkiye Barolar Birliği (TBB) tarafından sunulan Ulusal Hukuk Ağı Projesi (UHAP) sistemi üzerinden sorgu ücreti ödemek suretiyle ad, soyadı ve/veya T.C. kimlik numarası ile GSM numaralarına erişilebildiği,
- İlgili kişilerin telefon numaralarına ulaşılmamasının ardından şirket borcundan dolayı ortakların sorumlu olduğu iddiasında bulunulmadığı, yalnızca yönetim kurulu üyelerine borç bildiriminde bulunulduğu,
- Şikâyetçilerin söz konusu telefon numaralarının bir defaya mahsus olmak üzere Avukatlık Kanunu'nun 35/A maddesi gereğince uzlaşma sağlamak amacıyla arandığı,
- İlgili kişilere ait başvurunun veri sorumlusuna ulaşması ile kişisel verilerinin silindiği ve sistemler üzerinden geri dönülemez biçimde yok edildiği,
- Danıştay 10. Dairesinin 2014/6559 esas ve 2015/874 sayılı kararında avukatlık mesleğini icra eden davacı avukatın davalıların iletişim bilgilerini öğrenmek için yapılan başvurusunun reddinin "hak arama özgürlüğünün ihlali" nedeniyle hukuka aykırı olduğu yönünde hüküm tesis edildiği, bu karar göz önünde bulundurulduğunda hukuk ofisinin müvekkillerin hukuki menfaatlerini korumak adına borçlunun iletişim bilgilerine ulaşma çabasının hak arama hürriyeti kapsamında değerlendirilmesi gerektiği,
- Vekâleten görülen işlerde karşı tarafa ait ad, soyadı, T.C. kimlik numarası, adres bilgisi, nüfus kayıt bilgileri, anne-baba adları, aylık kazançları, eğitim durumları ve telefon numaralarının işlendiği; yargısal faaliyette ise özellikle gizlilik kararı verilmemişse mahkemelerde ve icra müdürlüklerinde olan tüm dosyaların vekâlet ilişkisi olsun olmasın Avukatlık Kanunu gereğince tüm avukatlar tarafından incelenebildiği hatta avukat olsun olmasın tüm vatandaşların yargı faaliyetinin Türk Milleti adına yürütülmesi sebebiyle duruşmalara katılabildiği

ifade edilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 07/07/2022 tarih ve 2022/655 sayılı Kararı ile;

- 6698 sayılı Kanun'un "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi", (ğ) bendinde veri işleyenin, "veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi olarak tanımlandığı,

- Somut olayda, ilgili kişilere ait kişisel verilerin işlenmesinde işleme amacını (borcun tahsili amacıyla ilgili kişilerle iletişim kurulması/ bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması/ veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için vb.); işleme vasıtalarını (UHAP sistemi aracılığıyla/ bilinmeyen numaralar hizmeti sunan operatörler aracılığıyla vb.) ve işlenen verilerin ne kadar süre (borç tahsil edilinceye kadar/ silme, yok etme talebinde bulunulması halinde vb.) ile nasıl saklanılacağına (veri sorumlusunun işyerinde fiziken/ bilgisayarlarında vb.) karar vermesi hususunda avukatın veri sorumlusu olarak hareket ettiği,

- Kanun'un "Genel İlkeler" başlıklı 4'üncü maddesinde, kişisel verilerin ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, buna göre, kişisel verilerin ancak; a) Hukuka ve dürüstlük kurallarına uygun olma, b) Doğru ve gerektiğinde güncel olma, c) Belirli, açık ve meşru amaçlar için işlenme, ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ile d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceği,

- Kanun'un 5'inci maddesinin kişisel verilerin işlenme şartlarını düzenlediği, maddenin (1) numaralı fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin, (2) numaralı fıkrasında ise, kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda olan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün korunması için veri işlemenin zorunlu olması, bir sözleşmenin

kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaati için veri işlenmesinin zorunlu olması hallerinde ilgili kişinin açık rızası olmaksızın kişisel verilerin işlenmesinin mümkün olduğunun hükme bağlandığı,

- Avukatlık Kanunu'nun 2'nci maddesinde avukatlığın amacının; hukuki münasebetlerin düzenlenmesini, her türlü hukuki mesele ve anlaşmazlıkların adalet ve hakkaniyete uygun olarak çözümlenmesini ve hukuk kurallarının tam olarak uygulanmasını her derecede yargı organları, hakemler, resmi ve özel kişi, kurul ve kurumlar nezdinde sağlamak olarak tanımlandığı,

- Avukatlık Kanunu'nun 35/A maddesinde avukatların dava açılmadan veya dava açılmış olup da henüz duruşma başlamadan önce kendilerine intikal eden iş ve davalarda, tarafların kendi iradeleriyle istem sonucu elde edebilecekleri konulara inhisar etmek kaydıyla, müvekkilleriyle birlikte karşı tarafı uzlaşmaya davet edebileceğinin düzenlendiği,

- Somut olayda, ilgili kişilerin vekilinden alınan şikâyet dilekçesinde şirketin borçlu sıfatını haiz olduğu; ilgili kişilerin ise ad, soyadı, T.C. kimlik numarası, adresi, telefon numarası gibi verilerinin hiçbir hukuka uygunluk sebebi olmaksızın işlendiği, şirketin fesih edildiği, zaten limitet şirket ortaklarının borçtan şahsi sorumluluğu bulunmadığı ve borcun zaman aşımına uğradığı iddiaları bulunulduğunun anlaşıldığı,

- Öncelikle kişisel verilerin işlenmesinde işleme sebepleri olarak kabul edilen Kanun'un 5'inci maddesinde yer alan hallerin aynı zamanda birer "hukuka uygunluk sebebi" olarak karşımıza çıktığı, bu sebeplerin söz konusu veri işleme faaliyetini Kanuna aykırı olmaktan çıkardığı, diğer bir ifade ile fiile hukuk dünyasında uygun bir zemin yarattığı, kişisel verilerin korunması mevzuatında yer alan "sebepler" kavramından farklı olarak borcun varlığı yahut talep edilip edilemeyeceği hususlarının farklı maddi hukuk dallarının değerlendirme alanına girdiği,

- Borç zamanaşımına uğramış olsa bile bunun bir def'i olduğu ve taraflarca ileri sürülmedikçe borcun talep edilebileceği, talep edilebilirlik olgusunun bile başlı başına bir veri işleme sebebi olduğu, bir borcun varlığı açısından ise borcun bir limited şirkete ait olduğu, ilgili kişilerin borçlu olmadığını belirttiği ancak bu kişilerin yönetim kurulu üyesi olduğu düşünüldüğünde iletişim kurulması muhtemel tarafların kendileri olduğunun hayatın olağan akışına uygun düştüğü,

- Veri sorumlusu avukat açısından Ticaret Sicil Gazetesi'nde ortak olarak görülen ilgili kişilerin kişisel verilerinin, şirketin iflasından sonra borcun tahsil edilebilmesini sağlamak amacıyla taraflarla uzlaşma kurulmasını teminen Avukatlık Kanunu'nun 35'inci maddesi hükmü gereğince işlendiği, hali hazırda avukatların görevlerini ifa ederken Avukatlık Kanunu'nun 2'nci maddesine uygun olarak taraflarına tevdi edilen işleri yerine getirmek amacıyla – somut olayla telekomünikasyon şirketi ile arasında bulunan vekâlet ilişkisinden kaynaklanan borcun tahsil edilmesi amacıyla – karşı taraflara ve müvekkillerine ilişkin verileri işleminin makul bir beklenti olacağı,
- UHAP sisteminde avukatlara sistem üzerinden dava açma, icra dosyası açma, dilekçe gönderme, beyan/talep yollama, T.C. kimlik numarası ile telefon numarası sorgulaması ve T.C. kimlik numarasına kısa mesaj gönderimi vb. imkânlar sağlandığı, bu imkânların kullanılması sırasında tıpkı tevzi bürolarında olduğu gibi bir davanın açılması / talebin gönderilmesi / beyanda bulunulması vb. amaçlarla gerekli olan taraflara ait verilerin sorgulanmasının/edinilmesinin söz konusu olduğu,
- Bilinmeyen numaralara ilişkin sunulan rehberlik hizmetlerinin ise telefon işletmecilerinin numara veri tabanlarına erişerek elde edilen bilgilerin gerekirse işlenerek kullanıcılara ulaştırılması amacıyla hizmet ettiği,
- Yukarıda belirtilen yöntemlerin birer işleme sebebi olmayıp veri toplama yöntemi olduğu, bu anlamda bahsi geçen platformların mevzuata aykırı bir kullanımı (yetkisiz erişim/hatalı bilgi girişi/veri sızıntısı vb.) söz konusu olmadıkça ve aksi ispat edilmedikçe veri toplamanın yönteminin kârî olarak hukuka uygun kabul edileceği ve bu anlamda hem UHAP hem bilinmeyen numaralar servislerinin avukatların açık ve yetkileri oranında veri elde edebilecekleri platformlar olarak kabul edilebileceği,
- İlgili kişilerin vekilinin Kuruma sunduğu dilekçede yer alan veri sorumlusu adına arama gerçekleştiren çağrı merkezi çalışanlarına şirketin tasfiye edildiği ve bir daha aranmak istemediklerinin belirtilmesine rağmen ısrarla taciz boyutuna varacak şekilde arka arkaya aramalar yapıldığı iddiası ile ilgili olarak ise geçmiş tarihli birçok Kurul Kararında, araç ve amaç arasındaki dengede ölçsüz bir durum ortaya çıkarması ve veri sorumlusunun sahip olduğu hakkı kötüye kullanması sonucunu doğurması sebepleriyle söz konusu davranışın genel ilkelerden biri olan hukuka ve dürüstlük kurallarına uygun olma şartına aykırılık taşıyacağı yönünde değerlendirmede bulunulduğu, bununla birlikte Kuruma iletilen şikâyette aramalara ilişkin bir kayda yer verilmediği ve dolayısıyla ilgili kişilerin vekili tarafından iddia edilen “defaten/ısrarla” arama yapılması durumunun sunulan bilgi ve belgelerden anlaşılabilmesi sebebiyle söz konusu veri işleme

faaliyetinin Kanun'un 4'üncü maddesi gereğince hukuka ve dürüstlük kurallarına uygun olarak gerçekleşmediğinin ispat edilemediği,

- İlgili kişinin veri sorumlusu tarafından Kanun'un 10'uncu maddesi kapsamında aydınlatılmadığı iddiasına ilişkin olarak, ilgili kişilerin vekilinden alınan dilekçede, ilgili kişilerin Kanun'un 10'uncu maddesi uyarınca aydınlatılmadığına ilişkin bir iddia bulunmamakla birlikte veri sorumlusuna yapılan başvuruda da aydınlatma hususuna ayrıca değinilmediğinin görüldüğü; bunun yanı sıra Kuruma intikal ettirilen dilekçede veri sorumlusunun gerçekleştirdiği her bir veri işleme faaliyeti yönünden aydınlatma yükümlülüğünün yerine getirilmediği hususunun Kurulca resen değerlendirilmesinin talep edildiği,

- Bu kapsamda avukatların uzlaşma amacıyla karşı tarafla iletişim kurduğu anda kendini tanıtmayı, veriyi nereden temin ettiğinin, ne amaçla iletişim kurduğunun karşı tarafa bildirilmesi hayatın doğal akışı içerisinde değerlendirilebilecekken verilerin ne kadar süreyle işleneceği, hangi yöntemler kullanılarak dosyalandığı/saklandığı gibi hususların bildirilmesinin bu akış içerisinde mümkün olmayacağı, aynı hususun borçlu ilgili kişilere icra takibi başlatılması ya da dava açılması sürecinde müvekkilden elde edilen karşı taraf bilgilerinin yine vekâlet ilişkisinin yürütülmesi amacıyla işlenmesinde aydınlatma yükümlülüğünün bir veri sorumlusundan uygulanması gereken şekilde yerine getirilmesinin beklenemeyeceği değerlendirilmekle birlikte bu hususun avukatın aydınlatma yükümlülüğünden muaf olduğu anlamına gelmediği; avukatın, vekâlet ilişkisi kurduğu kişiyi-yani müvekkilini- Kanun'un 10'uncu maddesi hükmü gereğince aydınlatma yükümlülüğü bulunduğu ve bu veri işleme faaliyetini gerçekleştirirken öğrendiği diğer bilgiler açısından zaten Avukatlık Kanunu gereğince sır saklama yükümlülüğü altında olduğu

değerlendirmelerinden hareketle;

- İlgili kişilerin borcun doğduğu/icra takibinin başlatıldığı dönemde münfesiş şirketin yönetim kurulunda yer aldığı, bu hususun da Ticaret Sicil Gazetesi'nde aleni bir şekilde paylaşıldığı, veri sorumlusu avukatın Avukatlık Kanunu ve sair mevzuat çerçevesinde vekâlet ilişkisi içerisinde bulunan müvekkile ait alacağın tahsili amacıyla ilgili kişilerin ad, soyadı, T.C. kimlik numarası, adresi, telefon numarası gibi verilerini UHAP/bilinmeyen numara servisleri vb. mevzuata uygun faaliyet yürüten yasal platformlar üzerinden edinmesinin ve işleminin 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 5'inci maddesinin (2) numaralı fıkrasının (ç) bendi gereğince veri sorumlusunun vekâlet ilişkisinden doğan hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması şartına ve (e) bendi gereğince alacaklının hak arama hürriyetinin tesisi, kullanılması veya

korunması için veri işlemenin zorunlu olması şartına dayandığı dikkate alınarak bu iddia açısından Kanun kapsamında yapılacak bir işlem olmadığına,

- Veri sorumlusunca gerçekleştirildiği iddia edilen “defaten/ısrarla” arama yapılması durumunun ise Kuruma sunulan dilekçe ve eklerinde yer alan bilgi ve belgelerden anlaşılabilmesi sebebiyle söz konusu veri işleme faaliyetinin Kanun’un 4’üncü maddesi gereğince hukuka ve dürüstlük kurallarına uygun olarak gerçekleşmediğinin ispat edilemediği dikkate alınarak bu hususta yapılacak bir işlem olmadığına,

- İlgili kişilerce yapılan veri sorumlusu başvurusunda aydınlatma yükümlülüğüne ilişkin iddialara yer verilmemiş olması sebebiyle veri sorumlusuna tanınan savunma hakkının kısıtlanmasının önüne geçilmesi amacıyla söz konusu hususun inceleme kapsamına dahil edilemeyeceğine

karar verilmiştir.

2022/653 sayılı KVKK Kararı

İlgili kişinin, çevrimiçi alışveriş hizmeti veren veri sorumlusundan gerçekleştirdiği alışverişine ilişkin kredi kartı ve cep telefonu bilgilerinin kendisine bildirilmesi talebi hakkında Kişisel Verileri Koruma Kurulunun 07/07/2022 tarihli ve 2022/653 sayılı Karar Özeti

Karar Tarihi : 07/07/2022

Karar No : 2022/653

Konu Özeti: İlgili kişinin, çevrimiçi alışveriş hizmeti veren veri sorumlusundan gerçekleştirdiği alışverişine ilişkin kredi kartı ve cep telefonu bilgilerinin kendisine bildirilmesi talebi

İlgili kişinin Kuruma intikal eden dilekçesinde özetle;

- Veri sorumlusu şirketin sunduğu hizmetlerden biri olan çevrimiçi alışveriş platformu üzerinden gerçekleştirdiği alışveriş ile ilgili olarak, uygulamaya girdiği kredi kartı bilgilerinin ve sipariş teslimatı için verilen iletişim -cep telefonu numarası- bilgisinin 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) uyarınca veri sorumlusundan talep edildiği,
- Ancak, kredi kartı üzerinde yazan isim bilgisinin veri sorumlusuna ait sistemlerde tutulmadığı ve siparişe ilişkin telefon bilgisinin kendisiyle paylaşılmasının uygun olmadığı gerekçesiyle söz konusu talebin veri sorumlusu tarafından reddedildiği ancak savcılık kararının bulunması halinde ilgili kişiyle bu bilgilerin paylaşılabilirliğinin belirtildiği,
- Platform üzerinden gerçekleştirilen alışverişlerde her ne kadar ilgili banka sayfasına yönlendirme yapılsa da kredi kart bilgileri alanının ödeme aşamasının başında veri sorumlusunun internet sayfası üzerinden doldurulduğu ve kredi kartı bilgilerinin isteğe bağlı olarak kaydedilebildiği, bu sebeple kredi kartı bilgilerinin veri sorumlusunun sisteminde tutulmadığı iddiasının gerçeği yansıtmadığı, aydınlatma metninde internet sitesi/mobil uygulamalar üzerinden alışveriş yapanın/yaptıranın kimlik bilgilerini teyit etme ve bu kişiyle iletişim kurmak amaçlarıyla adres ile diğer gerekli bilgilerinin kaydedilmesi suretiyle kişisel veri işlendiğinin belirtildiği,
- Kayıt altına alındığı beyan edilen bilgilerin sisteme kayıtlı kullanıcı e-postası ve telefon yoluyla talep edilmesine rağmen bu bilgilerin kendisiyle paylaşılmamasının Kanun'a aykırı olduğu

ifade edilerek Kanun kapsamında gereğinin yapılması talep edilmiştir.

Söz konusu iddialara ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- İlgili kişinin platform üzerinden alışveriş yapabilmesi için kart bilgilerini girmesi gerektiği, daha sonraki alışverişlerinde kullanmak istemesi halinde kredi kartı bilgilerini kaydedebileceği, buna karşın kredi kartını kaydetmeyi seçse dahi veri sorumlusunun kredi kartı bilgilerine ilişkin verilerin tamamına erişemediği, PCI DSS Level-1 Sertifika uyumluluğu bulunması nedeniyle ilgili kişilerin ödeme yaptıkları kredi kartı bilgilerinin veri sorumlusu sistemlerinde maskeli olarak tutulduğu,
- İlgili kişinin somut olaya konu üç adet sipariştten 53.....8 ve 53.....4 numaralı siparişlerin ilgili kişinin üyelik hesabıyla yapıldığı, 54.....8 numaralı siparişin ise ilgili kişinin üyelik hesabından yapılmadığı ve bu siparişin başka bir üyenin hesabından yapıldığının tespit edildiği, yazı ekinde 54.....8 numaralı siparişin başka bir kişiye ait olduğunu tevsiken ekran görüntüsünün sunulduğu,
- Öte yandan bazı durumlarda üyelik hesabından yapılan işlemlerde üçüncü kişilere ait isim, soy isim ve telefon numarası bilgilerinin verildiği; somut olayda da 53.....8 ve 53.....4 numaralı siparişlerin ilgili kişinin üyelik hesabından yapılmasına rağmen üçüncü bir kişinin adı, soyadı ve telefon numarası bilgilerinin verildiğinin anlaşıldığı, bu bağlamda talep konusu siparişlerin üçüncü kişilere ait olması ve veri sorumlusu bünyesinde kredi kartı bilgilerinin bulunmaması nedeniyle ilgili kişinin talebinin yerine getirilmediği,
- İlgili kişinin üyeliği ile yapılan iki alışverişte üçüncü kişiye ait isim, soy isim ve telefon numarası bilgilerinin bulunmasının; aynı üyelik hesabının eş, anne, baba, kardeş gibi birden fazla kişi tarafından ortak kullanılması, üyenin kendi şifresini başka bir üçüncü kişiyle paylaşması, üyenin hediye almak istediği üçüncü kişinin teslimat bilgilerini teslimat amacıyla sisteme eklemesi gibi ilgili kişinin bilgisi dâhilindeki nedenlerden kaynaklanabileceği gibi başka bir cihazdan giriş yaptığı hesabını kapatmadan çıkması, üyelik hesabı oluşturduğu farklı platformlarda hep aynı şifreyi kullanması gibi ihmallerden kaynaklanabileceği,
- Kanun'un 11'inci maddesinde vurgulandığı üzere ilgili kişilerin "kendisiyle ilgili" kişisel verilere ilişkin bilgi talep etme hakkının olduğu, dolayısıyla veri sorumlusunun, üçüncü kişinin kişisel verisine ilişkin olarak ilgili kişiye herhangi bir bilgi verme yükümlülüğünün bulunmadığı,
- Ortak hesap kullanan kişilerin daha sonra ihtilafli hâle geldiği durumların, örneğin ortak hesap kullanan eşlerin siparişlere ilişkin bilgi talebinde bulunduğu durumların yaşanabildiği göz önünde bulundurularak ilgili kişi taleplerinin hassasiyetle incelendiği ve ilgili kişinin hakkında bilgi talep

etmiş olduğu sipariş kendi üyelik hesabından yapılsa dahi alışverişin başka bir kişi tarafından yapıldığı tespit edilmişse bilgi paylaşmama konusunda titizlikle hareket edildiği,

- Öte yandan kredi kartı numarası bilgilerine uluslararası güvenlik standartları nedeniyle maskeli olarak erişim sağlanabilmesi nedeniyle bu bilgileri paylaşmasının mümkün olmadığı, ilgili kişinin talep ettiği kart üzerindeki isim ve soy isim bilgisinin ise veri sorumlusu nezdinde maskeli olarak dahi saklanmadığı,
- İlgili kişinin, üyelik hesabından yapmış olduğu kendisine ait siparişlere yönelik bilgi talebinde bulunması halinde çağrı merkezi doğrulama soruları aracılığıyla bu talebinin karşılanabileceği, ilgili kişinin taleplerini yerine getirmemek adına değil yalnızca mevzuat hükümleri ve veri güvenliği tedbirleri doğrultusunda yanıt verildiği,
- İlgili kişinin bilgisi dışında bir işlem olması ihtimali göz önünde bulundurularak bu konu hakkında yetkili mercilere başvurması yönünde kendisine bilgi verildiği ve ilgili kişinin üyelik hesabının güvenlik nedeniyle işleme kapatıldığı,
- İlgili kişinin talebinin Kanun'un 11'inci maddesi kapsamında olmadığı, ilgili kişilere verilecek yanıtın Kanun'un diğer hükümlerine aykırılık teşkil etmesi hâlinde veri sorumlusunun Kanun'un 13'üncü maddesi uyarınca reddetme hakkının olduğu

ifade edilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 07/07/2022 tarih ve 2022/653 sayılı Kararı ile;

- Kanun'un "Tanımlar" başlıklı 3'üncü maddesinde "kişisel veri"nin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi; "ilgili kişi"nin, kişisel verisi işlenen gerçek kişi, "veri sorumlusu"nun kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi; "kişisel verilerin işlenmesi"nin kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı,
- Kanun'un "Genel İlkeler" başlıklı 4'üncü maddesinde, kişisel verilerin ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, buna göre, kişisel verilerin ancak; a)

hukuka ve dürüstlük kurallarına uygun olma, b) doğru ve gerektiğinde güncel olma, c) belirli, açık ve meşru amaçlar için işleme, ç) işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ile d) ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceği,

• Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiilî imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

• Ayrıca, Kanun'un "İlgili kişinin hakları" başlıklı 11'inci maddesinde, ilgili kişilerin haklarının sıralandığı, bu maddede "Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

a) Kişisel veri işlenip işlenmediğini öğrenme,

b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

c) Kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,

ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,

e) 7'nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,

f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme haklarına sahiptir."

hükümlerine yer verildiği,

- Somut olayda veri sorumlusu tarafından sunulan Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (Payment Card Industry –PCI- Data Security Standard –DSS-) Servis Sağlayıcıları Yerinde İncelemesi için Uygunluk Tasdiki (Attestation Of Compliance –AOC- For Onsite Assessments Service Providers) belgesinde yer aldığı üzere mobil ödeme teknolojisi sağlayıcısı aracı şirket tarafından; kartın fiziksel olarak bulunmadığı işlemlerin, tacirlerden veya müşterilerden alınarak üye iş yeri anlaşması yapan kuruluşa (acquirer) yönlendirildiği, aynı zamanda müşterilere dijital cüzdan hizmeti sağlandığı, kart hamili verisinin sistemlerinde saklandığı, GSM numarasının müşterileri benzersiz olarak tanımladığı,
- Mobil ödeme teknolojisi sağlayıcısı aracı şirketin 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun kapsamında bir ödeme hizmeti sağlayıcısı olmadığı, üye iş yeri için kart bilgilerini saklama ve sonraki ödemeler için saklanan bilgilerin kullanılmasına izin veren bir hizmet sağladığı,
- Banka Kartları ve Kredi Kartları Hakkında Yönetmelik'in 27/A maddesinin beşinci fıkrası hükmü uyarınca hassas ödeme verisinin üye işyerine (somut olayda veri sorumlusuna) hiç iletilmemesinin gerektiği; ayrıca ödeme teyidinin yapılması amacıyla bir veri gönderilmesi gerekmesi hâlinde ise hesap numarası veya hassas ödeme verisi yerine her ödeme için oluşturulan farklı bir token iletilerek daha sonraki ödemeler için oluşabilecek risklerin ortadan kaldırılabileceği,
- Mobil ödeme teknolojisi sağlayıcısı aracı şirketin hizmet sözleşmesi incelendiğinde üye işyeri ile hassas kart verisinin paylaşılmayacağı beyan ve taahhüt edildiği, kart bilgisi görüntüleme ve silme işlemleri dahil olmak üzere kart saklama hizmetinin ilgili şirket tarafından sağlandığı ve veri sorumlusunun hassas kart bilgilerine sahip olmadığı anlaşıldığı, nihayetinde ilgili kişinin kart bilgilerine erişim talebinin veri sorumlusu tarafından karşılanamayacağı,
- İlgili kişinin Kanun'un 11'inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında siparişe ilişkin bilgi talebinin reddedilmesine ilişkin olarak; telefon numarasına ilişkin talebinin "ilgili kişinin kendisiyle ilgili olması" kriteri çerçevesinde incelendiğinde, kişisel verilerin aynı anda birden fazla kişiyle ilgili olmasının mümkün olduğu, ilgili kişinin teslimatı için verilen iletişim adresi üçüncü kişiye ait olsa da ilgili kişinin üyelik hesabından yapılan alışverişle ilgili olarak söz konusu telefon numarasının aynı zamanda ilgili kişiye ilişkin olduğu,

- Avrupa Veri Koruma Kurulu'nun (EDPB) "İlgili Kişi Hakları- Erişim Hakkı Üzerine 01/2022 sayılı Rehber" ilkelerinde; ilgili kişinin, münhasıran başkasını ilgilendiren veriler hariç olmak üzere, yalnızca kendisiyle ilgili kişisel verilere erişme hakkına sahip olduğu, bununla birlikte verilerin ilgili kişiye ilişkin kişisel veri olarak sınıflandırılmasının, bu kişisel verilerin başka biriyle de ilgili olmasına bağlı olmadığı ifade edildiği, "kendisiyle ilgili kişisel veriler" ifadesinin kapsamının "çok kısıtlayıcı" yorumlanmaması gerektiğinin tavsiye edildiği, ayrıca rehberde kişisel verilerin hane halkı kapsamında işlenmesine yönelik istisna hükmünün kapsamına girmeyen haller için ilgili kişinin sağladığı kişisel veriyi başka amaçlarla kullanması halinde, ilgili kişinin kendisinin de veri sorumlusu olarak nitelendirilebileceği ve veri sorumlusunun bu konuda diğer ilgili kişiyi bilgilendirmesi gerektiğinin ifade edildiği, bu çerçevede söz konusu rehber ilkeler ile erişim hakkının sınırları hakkında yapılacak değerlendirmede;

- Hak ve özgürlükler üzerinde olumsuz bir etkisi olup olmadığı (diğer bireyler için risk olasılığı ve riskin öneminin değerlendirilmesi)

- Başkalarının hak ve özgürlüklerinin, ilgili kişinin hakkına üstün gelip gelmediği

dengeyi temel alınarak eğer kişisel verilere erişim hakkı çözümsüzlüğünde, örneğin bir ses kaydını yalnızca transkriptinin sağlanması gibi uygun formatta kişisel verilere erişim hakkı tanınarak uzlaşılması veya böyle bir uzlaşma sağlayacak bir yöntem bulunmadığı durumda, diğer kişinin hak ve özgürlüklerinin olumsuz etkilendiği ve kişisel verilere erişim hakkına üstün geldiği sürece ilgili kişiye erişim hakkının sağlanmamasının tavsiye edildiği,

- Somut olayda, veri sorumlusu tarafından teslimat için verilen iletişim adresinin farklı olması nedenleri arasında;

- Bir üyeliğin birden fazla kişi (aile üyeleri gibi) ile ortak kullanılması,

- Üyenin şifresini başka kişiyle paylaşarak üyelik hesabını kullanması,

- Hediye almak istediği üçüncü kişi bilgilerini teslimat amacıyla sisteme eklemesi,

- Kimlik veya hesap hırsızlığı

hususlarının sayıldığı, ayrıca veri sorumlusu tarafından üçüncü kişinin kişisel verisine ilişkin ilgili kişiye herhangi bir bilgi verme yükümlülüğünün bulunmadığının belirtildiği,

- Veri sorumlusunun platformu üzerinden üyelik hesabına giriş yapıldığında halihazırda verilen siparişin teslimatının yapılacağı kişinin bilgileri kapsamında üçüncü kişinin ismi, soy ismi ve adres bilgisine ulaşılabildiği, yalnızca telefon numarasının yıldızlanarak maskelendiğinin anlaşıldığı;

somut olayda ilgili kişinin üyelik hesabından verilen siparişin teslimatı için bildirilen telefon numarasının

- Üçüncü kişinin hak ve özgürlükleri üzerinde olumsuz bir etkisinin olup olmadığı (üçüncü kişi için risk olasılığı ve riskin öneminin değerlendirilmesi),

- Üçüncü kişi hak ve özgürlüklerinin, ilgili kişinin erişim hakkına üstün gelip gelmediği

arasında bir denge kurulmak suretiyle ilgili kişinin kişisel veriye erişim hakkının üstün geldiği kanaatine varılması halinde, ilgili kişinin üyelik hesabından verilen siparişlerde teslimat için bildirilen telefon numarasının, ilgili kişinin makul gerekçesi bulunması ve erişim talebiyle ilişkili dolandırıcılık riski bulunmaması şartıyla veri sorumlusu tarafından ilgili kişinin kimliğini doğrulayacak mekanizmalar aracılığıyla ilgili kişiye sağlanması gerektiği,

• Öte yandan, ilgili kişinin üyelik hesabı kullanılmaksızın verilen üçüncü siparişin ilgili kişi dışında üçüncü kişinin üyelik hesabından yapıldığı veri sorumlusunun sunduğu deliller ile kanıtlandığı dikkate alındığında, ilgili kişinin kişisel verisi olmaması nedeniyle kişisel verilere erişim hakkı kapsamında veri sorumlusu tarafından söz konusu siparişin teslimatı için verilen telefon numarasının ilgili kişiye sağlanamayacağı

değerlendirmelerinden hareketle;

• İlgili kişinin kredi kartı bilgilerinin mobil ödeme teknolojisi sağlayıcısı aracı şirket bünyesinde tutulduğu dikkate alındığında veri sorumlusu hakkında bu açıdan yapılacak bir işlem olmadığına,

• Üyelik hesabından giriş yapıldığında verilen siparişin teslimatının yapılacağı kişinin bilgileri kapsamında halihazırda üçüncü kişinin isim, soy ismi ve adres bilgisine ulaşabildiği, telefon numarasının ise maskeli olarak gösterildiği dikkate alındığında, ilgili kişinin erişim talebinin gerekçesinin makul olması ve bu talep ile bağlantılı dolandırıcılık riski bulunmaması halinde üçüncü kişinin hak ve özgürlüklerinin ilgili kişinin kişisel veriye erişim hakkına üstün gelmediği kanaatine varıldığından, ilgili kişinin üyelik hesabından verilen siparişlerin teslimatı için bildirilen telefon numarasının kimlik doğrulama mekanizmaları aracılığıyla ilgili kişiye sağlanması yönünde veri sorumlusunun talimatlandırılmasına,

• İlgili kişinin üyelik hesabı kullanılmaksızın verilen diğer siparişin ilgili kişi dışında üçüncü kişinin üyelik hesabından yapıldığının veri sorumlusunun sunduğu deliller ile kanıtlandığı dikkate alındığında, şikayetçinin kişisel verisi olmaması nedeniyle söz konusu siparişin teslimatı için verilen telefon numarasının ilgili kişinin erişim hakkı kapsamında bulunmadığı kanaatine varıldığından bu hususta veri sorumlusu hakkında yapılacak herhangi bir işlem bulunmadığına

karar verilmiştir.

2022/630 sayılı KVKK Kararı

İlgili kişinin ameliyat sırasında çekilen fotoğraflarının veri sorumlusu hastanede çalışan bir doktorun sosyal medya hesabında paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 29/06/2022 tarihli ve 2022/630 sayılı Karar Özeti

Karar Tarihi : 29/06/2022

Karar No : 2022/630

Konu Özeti: İlgili kişinin ameliyat sırasında çekilen fotoğraflarının veri sorumlusu hastanede çalışan bir doktorun sosyal medya hesabında paylaşılması

İlgili kişinin Kuruma intikal eden şikâyetinde özetle; özel bir hastanede gerçekleştirilen burun ameliyatı esnasında baygın olduğu sırada açık rızası alınmaksızın çekilen kişisel verisi niteliğindeki fotoğraflarının veri sorumlusu hastanede çalışan ve ameliyatı gerçekleştiren doktorun sosyal medya hesabında reklam amaçlı olarak paylaşıldığı ve söz konusu fotoğrafların yaklaşık iki yıl boyunca bu hesapta tutulduğu, doktor ile veri sorumlusu hastanenin gerçekleştirilen ameliyatları sosyal medya hesaplarında paylaşarak yeni müşteriler kazanmayı hedefledikleri, ilgili kişinin yaptığı başvuru sonrasında fotoğraflar kaldırılmış olmakla birlikte veri sorumlusu hastane tarafından ilgili kişiye verilen cevapta ilgili kişinin kişisel verilerinin hukuka uygun olarak işlendiğinin ispat edilemediğinin belirtildiği iddialarına yer verilmiş ve kişisel verilerinin reklam ve pazarlama amaçlı işlenmesinde açık rızasının bulunmadığı belirtilerek gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusu hastaneden savunması istenilmiş olup alınan cevabi yazıda özetle;

- Öncelikle ilgili kişinin, kişisel verisi niteliğinde olduğunu iddia ettiği görüntülerin kişisel veri niteliği taşımadığı, zira kişisel veriden söz edebilmek için verinin gerçek kişiye ilişkin olması ve bu gerçek kişinin kimliğinin belirli ya da belirlenebilir nitelikte olması gerektiği, ancak şikâyete konu görüntü ile ilgili kişinin ilişkilendirilmesinin mümkün gözükmediği, söz konusu görüntünün yalnızca operasyon yapılan burundan ibaret olduğu, burun dışında herhangi bir belirleyici unsur olmadığı, kişinin kimliğini belirlenebilir kılacak unsurların çekim açısı ve anonimleştirmeler yoluyla ortadan kaldırıldığı, bahse konu sosyal medya gönderisinde ilgili kişinin kimlik bilgilerinin, isim veya

soy isminin etiketleme yöntemi ile sosyal medya hesabında paylaşılmadığı, dolayısıyla yalnızca bahse konu görüntüye bakılarak herhangi bir kişinin tespit edilemeyeceği, ayrıca söz konusu ameliyatın bir estetik ameliyatı olduğu göz önünde bulundurulduğunda yapılan tıbbi müdahalenin gösterilebilmesi amacıyla uygulanan tedaviden hemen sonra çekilen fotoğrafın ilgili kişiyi tanımlamadığı,

- Öte yandan ilgili kişiye hastane bünyesinde uygulanan tıbbi tedavinin akabinde, hastane doktorlarından birisi tarafından ilgili kişinin bahse konu fotoğrafının çekildiği, ilgili kişinin başvuru dilekçesinin ekinde yer alan görsel dışında sistemlerinde ilgili kişinin bir görüntüsünün mevcut olmadığı, ilgili kişinin başvurusu üzerine ilgili görselin kaldırıldığı ve hastane bünyesinde çalışan bahse konu doktor tarafından da imha edildiği,

- Özel Hastaneler Yönetmeliği'nin 48'inci maddesi hükmü uyarınca düzenlenen hasta dosyasında ilgili kişinin çeşitli kişisel verilerinin işlendiği ve bu verilerin hukuka ve dürüstlük kuralına uygun şekilde, güncel ve doğru olmak şartıyla, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ve yönetilmesi amaçları doğrultusunda belirlenmiş olan meşru amaçlarla sınırlı olarak ölçülülük ilkesine uygun şekilde, 6698 sayılı Kanun'un 5 ve 6'ncı maddelerinde belirtilen şartlar dahilinde hukuka uygun olarak işlendiği,

- Bahse konu görselin, fotoğrafı çeken doktorun sosyal medya hesabında ilgili kişinin açık rızası alınarak paylaşıldığı, hastane tarafından hem sözlü hem de yazılı olarak ilgili kişinin açık rızasının alındığı, bu çerçevede ilgili kişinin tedavinin nitelikleri, özellikleri ve sonuçları bakımından kamunun bilgilendirilmesi amacıyla görsel olarak kullanılması yönünde açık rıza verdiğini gösteren belgenin Kuruma sunulduğu, dolayısıyla ilgili kişinin açık rızasının bulunmadığı yönündeki iddiasının gerçeği yansıtmadığı,

- Görüntünün paylaşım tarihinden iki yıl sonra ilgili kişinin, bahse konu fotoğrafı çeken doktora, fotoğrafının, kendisinin sosyal medya hesabından kaldırılması talebinde bulunarak açık rızasını geri alması üzerine söz konusu paylaşımın kaldırıldığı,

- İlgili kişinin bahsi geçen doktor tarafından ameliyat sonrasında düzenli olarak muayene edildiği, periyodik muayenelerde söz konusu paylaşımlar hakkında herhangi bir talebi bulunmayan ilgili kişinin tedavinin tamamlanması sonrasında itirazlarda bulunmasının kişisel fayda sağlayacağı umuduyla hareket ettiği anlamına geldiği ve ilgili kişi tarafından bahsi geçen doktora gönderilen ihtarnamede, fotoğraflarının sosyal medya platformlarından kaldırılması akabinde kendisine belli bir miktar manevi tazminat ödenmemesi durumunda yasal yollara başvurulacağını belirtilmesinin,

Kurum tarafından kesilen idari para cezasından kendisinin faydalanabileceği düşüncesi taşıdığı anlamına geldiği,

- Taraflarına yapılan başvuru sonrasında ilgili kişinin talebinin yerine getirilmesi ve fotoğrafların tüm alanlardan kaldırılmasının ardından Kurula şikâyetle bulunmuş olmasının ilgili kişinin açıkça kötü niyetli olduğunu gösterdiği

ifade edilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulunun 29/06/2022 tarih ve 2022/630 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, "belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza", (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ğ) bendinde "veri işleyen" in veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi, (ı) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi" olarak tanımlandığı,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi; fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin kendisi tarafından alenileştirilmiş olması; bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından

birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hükmünün yer aldığı,

- Kanun'un 12'nci maddesinin (1) numaralı fıkrası gereğince veri sorumlusunun; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğunun hükme bağlandığı,

- Somut olayda veri sorumlusu tarafından şikâyete konu görüntünün ilgili kişiyi tanımlamadığı, yalnızca operasyon öncesi ve sonrası burun görselinin bulunduğu, ilgili kişinin kimliğini belirlenebilir kılacak unsurların çekim açısı ve anonimleştirmeler yoluyla ortadan kaldırıldığı beyan edilmiş olmakla birlikte Kuruma intikal eden şikâyet dilekçesinin ekinde yer alan görüntüler incelendiğinde; ameliyat öncesi ve sonrasına ilişkin burun görselinin yer aldığı görüntüde ilgili kişinin gözlerinin görsel karakter kullanılmak suretiyle kapatıldığı, ancak görsel içeriğinin yalnızca burundan ibaret olmadığı, yüzün ilgili kişiyi tanımlayabilecek kaş, bıyık vb. bölümlerinin açıkça yer aldığı ve anonimleştirilmediği görüldüğünden bahsi geçen görsellerin ilgili kişinin kimliğini belirlenebilir kılabilme özelliğinde olduğu, yüzün açıkta kalan bölümlerinden görselde yer alan kişinin ilgili kişi olduğunun tespit edilebileceği, dolayısıyla ilgili kişiye ait kişisel veri niteliği taşıdığı,

- Veri sorumlusu, bahse konu görüntünün fotoğrafı çeken doktorun sosyal medya hesabında ilgili kişinin rızası alınarak paylaşıldığını, bu çerçevede hastane tarafından ilgili kişinin hem sözlü hem de yazılı olarak açık rızasının alındığını ve bu çerçevede ilgili kişinin tedavinin nitelikleri, özellikleri ve sonuçları bakımından kamunun bilgilendirilmesi amacıyla görsel olarak kullanılması yönünde açık rıza verdiğini gösteren muvafakatnamenin Kuruma sunulduğunu beyan etmiş olmakla birlikte bahse konu muvafakatname incelendiğinde; ilgili kişinin, kişisel verilerinin kullanılmasına açık rıza gösterdiği tarafın tedaviyi gerçekleştiren sağlık kuruluşu olduğunun görüldüğü ancak somut olayda ilgili kişinin ameliyat sırasında çekilen görsellerini sosyal medya hesabında paylaşan hastanede çalışan bir doktor olduğu,

- Bu doğrultuda ilgili kişinin kişisel verilerinin ameliyatının gerçekleştirildiği sağlık kuruluşu tarafından kullanılmasına rıza gösterdiği, ancak hastane doktorunun bu verileri kullanması yönünde bir rızasının bulunmadığı, bu nedenle fotoğrafları paylaşan doktor tarafından ilgili kişiye ait kişisel verilerin Kanun'da belirlenen işleme şartları sağlanmaksızın hukuka aykırı şekilde işlendiği,

- Veri sorumlusunun, bahsi geçen doktora ilgili kişi tarafından gönderilen ihtarnamede maddi taleplerin yer aldığı ve ihtarnameden, ilgili kişinin Kurum tarafından kesilen idari para cezasından faydalanabileceği düşüncesinde olduğunun anlaşıldığı yönündeki iddiası veri sorumlusunun cevap

yazısının ekinde yer alan belgelerden tevsik edilmiş olduğundan, veri sorumlusunun anılan iddialarına ilişkin olarak yargı yoluna başvurabileceği,

- Öte yandan, Kanun'un 17'nci maddesinde kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarih ve 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140'ıncı madde hükümlerinin uygulanacağını düzenlendiği, Türk Ceza Kanunu'nun 135, 136 ve 137'nci maddelerinde hukuka aykırı olarak kişisel verileri kaydetme, kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçuna ilişkin yaptırımların hükme bağlandığı ve böyle bir durumun varlığında kişisel verilere hangi yollarla ulaşıldığının tespiti ile bu kapsamda gerekli hukuksal işlemlerin tesisini teminen ilgili kişi tarafından konuya ilişkin yargı yoluna başvurulmasının mümkün olduğu

değerlendirmelerinden hareketle;

- İlgili kişinin, veri sorumlusu bünyesinde çalışan doktor tarafından burun estetiği ameliyatında baygın olduğu sırada çekilen görsellerinin açık rızası alınmaksızın sosyal medya hesabında paylaşıldığı iddiasına ilişkin olarak, ilgili kişinin açık rıza gösterdiği tarafın veri sorumlusu hastane olduğu, baygın olduğu esnada çekilen görsellerinin bahsi geçen doktor tarafından paylaşılması konusunda açık rıza beyanının bulunmadığı, bununla birlikte veri sorumlusu hastanenin söz konusu fotoğrafların adı geçen doktor tarafından sosyal medya hesabında paylaşıldığı hususunda bilgisinin bulunduğu, bu itibarla veri sorumlusunun ilgili kişinin kişisel verisi olan görselin adı geçen doktor tarafından sosyal medya hesabında paylaşılmasını önleyici gerekli idari ve teknik tedbirleri almadığı dikkate alındığında; Kanun'un 12'nci maddesinin (1) numaralı fıkrası çerçevesinde kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirleri yeterli düzeyde almadığı kanaatine varılması nedeniyle veri sorumlusu hastane hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 100.000 TL idari para cezası uygulanmasına,

- Veri sorumlusunun, ilgili kişinin kendisine maddi tazminat ödenmesi durumunda Kurula şikâyetle bulunmayacağına dair teklifine ilişkin yargı yoluna başvurulabileceği hususunda bilgilendirilmesine, Kişisel verilerini rızası olmaksızın şahsi sosyal medya hesabında paylaşmak suretiyle işleyen doktor hakkında Türk Ceza Kanunu'nun ilgili madde hükümleri kapsamında gerekli hukuksal işlemlerin tesisini teminen yargı yoluna başvurabileceği hususunda ilgili kişinin bilgilendirilmesine

karar verilmiştir.

2022/594 sayılı KVKK Kararı

Özel nitelikli kişisel sağlık verisi niteliğindeki bağımlılık yapıcı madde testinin sonuçlarının ilgili kişilerin açık rızası alınmaksızın veri sorumlusu özel bir sağlık kuruluşu tarafından ilgili kişilerin işyerinde görevli üçüncü bir kişiye ait e-posta adresine gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 22/06/2022 tarihli ve 2022/594 sayılı Karar Özeti

Karar Tarihi : 22/06/2022

Karar No : 2022/594

Konu Özeti: Özel nitelikli kişisel sağlık verisi niteliğindeki bağımlılık yapıcı madde testinin sonuçlarının ilgili kişilerin açık rızası alınmaksızın veri sorumlusu bir özel sağlık kuruluşu tarafından ilgili kişilerin işyerinde görevli üçüncü bir kişiye ait e-posta adresine gönderilmesi

Kuruma intikal eden dilekçelerde özetle;

- İlgili kişilerin, işveren bünyesinde tüm çalışanlar gibi hiçbir sebep ve açıklama olmaksızın baskıyla uyuşturucu testine zorlandığı, evlerinden çağrılarak veri sorumlusu özel sağlık kuruluşunda test yaptırıldığı,
- Testin yapılması sırasında ilgili kişilerin iletişim bilgileri alınmadığı gibi test sonuçlarının hukuka aykırı olarak ilgili kişilerin işyerindeki bir personele ait e-posta adresine gönderildiği, dolayısıyla kişisel sağlık verilerinin kendilerinden izin alınmaksızın ve hiçbir aydınlatma yapılmaksızın, açık rızaları dışında üçüncü bir kişiye aktarıldığı,
- Konu ile ilgili olarak yapılan başvurulara istinaden veri sorumlusu tarafından ilgili kişilere verilen cevapta ilgili kişilerin, çalıştıkları kurumun işvereni olarak bildirdikleri üçüncü kişi ile birlikte laboratuvar birimine gelerek bağımlılık yapıcı madde taraması yaptırmak istediklerini beyan ettikleri, her hastaya yapıldığı gibi kayıt aşamasında T.C. kimlik numarası, doğum tarihi, telefon numarası ve sonucun bildirileceği e-posta adresinin istenerek kayıt işlemlerinin yapıldığı, bahsi geçen hastaların ödemesinin beraber geldikleri işverenleri tarafından yapıldığı, hastaların yanında duyabilecekleri şekilde ve kameraların önünde kendi rızaları ile sözlü olarak onay alındıktan sonra işverene ait e-posta adresinin, sonuçların gönderilmesi için kayıtlara işlendiği ve ilgili kişilerin bu duruma hiçbir

itirazının olmadığı, kişisel verilerin işlenmesindeki amacın tüm sağlık kuruluşlarında olduğu gibi kişiye özel bir kayıt oluşturmak ve çalışan test sonuçlarını raporlamak olduğunun beyan edildiği,

- İlgili kişilerin diğer arkadaşlarından öğrendikleri şekliyle, test sonrasında şikâyetle belirtilen üçüncü kişinin sonuçların kendisine gönderilmesini istediğini ve kayıt alan kişinin de hiçbir açık rıza beyanı almaya gerek duymaksızın verilen bilgiyi kayda aldığı,

- Her ne kadar veri sorumlusu sağlık kuruluşu tarafından verilen cevap yazısında ilgili kişilerin işvereni olduğu belirtilse de söz konusu kişinin işverenleri olmadığı, sonuç olarak tetkik sonuçlarının taraflarına gönderilmek yerine üçüncü bir kişiye gönderildiği

ifade edilerek gereğinin yapılması talep edilmiştir.

İlgili kişilerin şikâyetine istinaden başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişilerin bağımlılık yapıcı madde tarama testi yaptırmak için şikâyetle belirtilen üçüncü kişi ile birlikte kliniğe başvurduğu, bunun ardından standart hasta kayıt kabul prosedürü gereği kayıt sürecinin başlatıldığı,

- İlgili kişilerden alınan bilgiler çerçevesinde kayıt oluşturularak işlemin başlatıldığı, tüm bilgilerin ilgili kişilerin açık beyanı üzerine kayıt altına alındığı, işlem ödemesinin anılan üçüncü kişi tarafından yapılacağı beyan edildiği, ilgili kişiler tarafından söz konusu testlerin rıza dışında yaptırıldığına ilişkin bir geri bildirimde bulunulmadığı, ödeme alınarak ve faturası ilgili adına düzenlenerek test sürecinin başlatıldığı,

- Laboratuvar işleyişinde ilgili kişilerin beyan ettiği adres, telefon ve e-posta adresi gibi bilgiler iletişim adresi kabul edilerek tüm bildirimlerin anılan adrese yapıldığı, ilgili kişilerin kayıt esnasında kendi rızasıyla üçüncü kişiye ait e-posta adresini verdiği,

- İlgili kişilerin veri sorumlusu hakkında somut olayla ilgili açtığı manevi tazminat davasının devam ettiği,

- Sağlık hizmeti sunucusunun banko, gişe ve masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda yakın konumda hizmet alanların birbirlerine ait kişisel verilerini duymalarını, görmelerini, öğrenmelerini veya ele geçirmelerini engelleyecek nitelikte gerekli fiziki, teknik ve idari tedbirleri almakla; tahlil ve tetkik sonuçları gibi hastaya ait kişisel sağlık verilerini içeren basılı materyal üzerinde gerekli kısmi kimliksizleştirme veya maskeleyen tedbirlerini

uygulamakla ve söz konusu materyalin yetkisiz kişilerin eline geçmesi halinde kime ait olduğunun tespit edilmesini zorlaştıracak tedbirleri almakla yükümlü olduğu,

- Kişisel sağlık verilerinin hasta yakınları ile paylaşımında, KVKK ilkelerine aykırılık teşkil etmeyecek şekilde, bilginin, mümkün olduğunca sade şekilde, tereddüt ve şüpheye yer verilmeden, hastanın sosyal ve kültürel düzeyine uygun olarak anlayabileceği şekilde verildiği,
- Hastanın kendisinin bilgilendirilmesinin esas olduğu, hastanın kendisi yerine bir başkasının yakınlarının bilgilendirilmesini talep etmesi halinde, bu talebin kişinin imzası ile yazılı olarak kayıt altına alınmak kaydıyla yerine getirildiği, bilgilendirmenin uygun ortamda ve hastanın mahremiyeti korunarak yapıldığı

hususları bildirilmiştir.

Bahse konu inceleme sürecinde ilgili sağlık kuruluşu tarafından da söz konusu uyuşturucu testlerinin sonuçlarının üçüncü kişiye ait e-posta adresine gönderildiği ifade edildiğinden, Kişisel Verileri Koruma Kurulu tarafından ilgili kişilerin işvereninden, anılan üçüncü kişinin şirketteki konumu hakkında bilgi temin edilmesine karar verilmiştir. Karara istinaden işveren tarafından gönderilen cevabi yazıda özetle;

- İşveren bünyesinde çalışan personelden edinilen bilgi ile mağazanın alt katındaki depodan koku geldiğinin öğrenildiği, bu kokunun uyuşturucu dumanı kokusu olabileceğinin anılan üçüncü kişi personele iletildiği, bu iddia karşısında personellerin uyuşturucu testi yaptırmasının uygun olacağına karşılıklı olarak kararlaştırıldığı,
- İki personelin yaşlarından, bir personelin ise durumu bildiren kişi olmasından ötürü test sürecinden hariç tutulduğu, diğer personelin gönüllü olarak uyuşturucu testi yaptırdığı, sonrasında test yapılacak beş personelin klinik testleri için randevu alındığı, beş personelden birinin hastalığını gerekçe göstererek test yaptırmadığı, kalan personelin ise ilgili testi yaptırdığı,
- Bahsi geçen personel test verdikten sonra sağlık kuruluşunda görevli bir kişinin test sonuçlarının hangi e-posta adresine gönderileceğini sorduğu, anılan üçüncü kişinin diğer personele test sonuçlarının onların e-posta adresine mi yoksa kendi e-posta adresine mi gönderilmesi istediklerini sorduğu, bunun üzerine personelin, test sonuçlarının anılan üçüncü kişinin e-posta adresine gösterilmesine sözlü olarak rıza gösterdikleri, bu sebeple anılan üçüncü kişinin e-posta adresini klinikteki görevliye verdiği,
- Test sonuçlarının gönderildiği tarihte veri sorumlusu tarafından test veren personele gösterildiği ve sonrasında test sonuçlarını içeren e-postanın anılan üçüncü kişi tarafından derhal silindiği,

Kanun'a aykırı bir durumun söz konusu olmadığı, personelin ilgili işlemi kendi rızaları ile yaptığı, ilgili tarihte anılan üçüncü kişinin herhangi bir yetkisinin bulunmadığı, mağaza çalışanı olarak görev yaptığı, üçüncü kişinin e-postasının kliniğe işveren tarafından bildirilmediği, işverenin olayla ilgili herhangi bir hukuki ve cezai sorumluluğunun bulunmadığı

ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 22/06/2022 tarih ve 2022/594 sayılı Kararı ile;

- 6698 sayılı Kanun'un "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, "Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza", (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi" olarak tanımlandığı,

- Kanun'un "Genel İlkeler" başlıklı 4'üncü maddesinde, kişisel verilerin ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, buna göre, kişisel verilerin ancak; a) Hukuka ve dürüstlük kurallarına uygun olma, b) Doğru ve gerektiğinde güncel olma, c) Belirli, açık ve meşru amaçlar için işlenme, ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ile d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceği,

- Kanun'un "Özel Nitelikli Kişisel Verilerin İşlenme Şartları" başlıklı 6'ncı maddesinin

(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir. (4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır. şeklinde düzenlendiği,

- Kişisel veri işleme faaliyeti bakımından açık rızanın hem özel nitelikli kişisel veriler hem de özel nitelikli olmayan kişisel veriler bakımından hukuka uygunluk sebeplerinden biri olduğu, açık rızanın ilgili kişinin işlenmesine izin verdiği verinin sınırlarını, kapsamını ve gerçekleştirilme biçimini de belirlemesini sağladığı ve rıza veren kişinin “olumlu irade beyanı”nu içermesi gerektiği, açık rızanın alındığına dair ispat yükünün ise veri sorumlusuna ait olduğu,

- Kanun’un 6’ncı maddesinin (4) numaralı fıkrası ile 22’nci maddesinin (1) numaralı fıkrasının (ç) bendi kapsamında Kişisel Verileri Koruma Kurulunun 31/01/2018 tarihli ve 2018/10 sayılı Kararı ile “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler”in belirlendiği,

- Şikâyete konu iddialara ilişkin olarak, veri sorumlusundan ve işverenden alınan cevap yazılarının incelenmesi neticesinde, “ilgili tarihte anılan üçüncü kişinin herhangi bir yetkisinin bulunmadığı, mağaza çalışanı olarak görev yaptığı” şeklindeki açıklamadan anlaşıldığı üzere veri sorumlusu tarafından ilgili kişiye ait özel nitelikli kişisel veri niteliğindeki test sonuçlarının gönderildiği üçüncü kişinin, Kanun’un 6’ncı maddesi kapsamında işveren bünyesinde çalışanların kişisel sağlık verilerini ilgili kişilerin açık rızası olmaksızın işleyebilecek sır saklama yükümlülüğü altında bulunan iş yeri hekimi olmadığı,

- Öte yandan, veri sorumlusu sağlık kuruluşu tarafından Kuruma intikal ettirilen cevabî yazıda belirtildiği üzere anılan üçüncü kişinin işveren olduğu düşünülerek söz konusu özel nitelikli kişisel verilerin bahsi geçen kişinin e-posta adresine gönderildiği dikkate alındığında veri sorumlusunun ilgili kişilere ait özel nitelikli kişisel verileri göndereceği e-posta adresinin Kanun kapsamında sır saklama yükümlülüğü altında bulunan iş yeri hekimine ait olup olmadığını tespit etmeden gönderdiğinin anlaşıldığı, her ne kadar veri sorumlusu tarafından ilgili kişilerin özel nitelikli kişisel verilerinin söz konusu e-posta adresine iletilmesi konusunda açık beyanlarının bulunduğu ifade edilse de Kuruma söz konusu hususu kanıtlayıcı mahiyette herhangi bir bilgi ya da belge iletilmediği,

- Bu kapsamda, veri sorumlusu sađlık kuruluřunun, ilgili kiřilerin sađlık verilerini üçüncü kiři ile paylaşması sureti ile gerekleřtirilen veri iřleme faaliyetinin Kanun'un 6'ncı maddesinde yer alan herhangi bir veri iřleme faaliyetine dayanmaksızın gerekleřtirdiđi dikkate alındıđında Kanun'un 12'nci maddesi kapsamındaki yükümlölüklerini ihlal ederek kiřisel verilerin hukuka aykırı olarak iřlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almadıđı kanaatine varıldıđı

deđerlendirmelerinden hareketle

- İlgili kiřilere ait özel nitelikli kiřisel verilerin veri sorumlusu sađlık kuruluřu tarafından ilgili kiřilerin iřyerinde görevli üçüncü bir kiřiye ait e-posta adresine gönderilmek suretiyle paylaşılması řeklindeki veri iřleme faaliyetine iliřkin olarak her ne kadar veri sorumlusu tarafından ilgili kiřinin özel nitelikli kiřisel verilerinin söz konusu e-posta adresine iletilmesi konusunda açık beyanının bulunduđu ifade edilse de söz konusu açık rızayı kanıtlayıcı mahiyette herhangi bir bilgi ya da belgenin Kuruma iletilmediđi bu anlamda veri sorumlusunun söz konusu veriyi Kanun'un 6'ncı maddesinde yer alan herhangi bir veri iřleme faaliyetine dayanmaksızın paylařtıđı, dolayısıyla kiřisel verilerin hukuka aykırı olarak iřlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almadıđı ve bu hususun Kanun'un 12'nci maddesinin (1) numaralı fıkrasına aykırılık teřkil ettiđi kanaatine varıldıđından, söz konusu ihlalden etkilenen kiři sayısının ilgili kiřilerle sınırlı kalmadıđı, ilgili veri iřleme faaliyetinde kiřilerin özel nitelikli kiřisel veri niteliđini haiz sađlık verilerinin iřlendiđi, veri sorumlusunun yaklaşık 600'e yakın alıřan ile birok ilde sađlık hizmetleri verdiđi hususları da dikkate alınarak, Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında veri sorumlusu hakkında 75.000 TL idari para cezası uygulanmasına

karar verilmiřtir.

2022/545 sayılı KVKK Kararı

İlgili kişinin kişisel verilerinin hesabının bulunmadığı veri sorumlusu banka tarafından aydınlatma yükümlülüğü yerine getirilmeksizin ve açık rızası alınmaksızın işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 02/06/2022 tarihli ve 2022/545 sayılı Karar Özeti

Karar Tarihi : 02/06/2022

Karar No : 2022/545

Konu Özeti: İlgili kişinin kişisel verilerinin hesabının bulunmadığı veri sorumlusu banka tarafından aydınlatma yükümlülüğü yerine getirilmeksizin ve açık rızası alınmaksızın işlenmesi

İlgili kişinin şikâyetinde özetle;

- Bir elektronik eşya mağazasından satın almak için baktığı ürünün ödeme seçeneklerini sorduğu sırada mağaza görevlisince veri sorumlusu banka tarafından verilebilecek kredi vasıtasıyla taksit yapılabildiği bilgisinin ilgili kişiye iletildiği,
- Bunun üzerine ilgili kişinin alabileceği kredi tutarını öğrenebilmek adına T.C. kimlik numarasını yazarak belirtilen numaraya SMS gönderdiği, veri sorumlusu banka tarafından verilen SMS yanıtında ilgili kişinin kredi limitinin belirtildiği,
- İlgili kişinin daha önce bu bankada hiçbir hesabının olmadığı ve hiçbir işlem yapmadığı, bankaya gönderilen T.C. kimlik numarası ve cep telefonu numarası için veri sorumlusu bankanın ilgili kişiye yönelik herhangi bir aydınlatmada bulunmadığı, bu banka ile irtibatı bulunmayan bir kişi olmasına karşın veri sorumlusunun ilgili kişiye kısa süre içerisinde kredi limiti belirleyebildiği, bu durumun veri sorumlusu banka tarafından ilgili kişinin kişisel verilerinin bilgisi olmaksızın daha önceden işleniyor olduğunu gösterdiği,
- Bu çerçevede veri sorumlusunun aydınlatma yükümlülüğünü yerine getirmediği, ilgili kişinin başvurusuna usulüne uygun bir yanıt verilmediği ve kişisel verileri işlenirken ilgili kişiden açık rıza alınmadığı

belirtilmiş ve gerekli işlemlerin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusunun savunması talep edilmiş olup veri sorumlusunun cevabi yazısında özetle;

- İlgili kişinin elektronik eşya mağazasında bulunduğu sırada almış olduğu bilgiye istinaden, bankalarına ait numaraya T.C. kimlik numarası bilgisini göndererek kredi başvurusunda bulunduğu, kayıtlarında daha önceden kendisine ait hiçbir bilgi ve belge olmadığı,
- Kredi sürecini SMS göndermek suretiyle ilgili kişinin başlattığı, talep ettiği bankacılık ilişkisi kurulmadan önce hukukî ve ticari risk analizleri yapabilmek, bankacılık mevzuatına göre bir risk grubuna ait olup olmadığını tespit edebilmek, müşteri ilişkilerini yürütebilmek için kara paranın aklanmasına yönelik düzenlemeler dâhil fakat bunlarla sınırlı olmamak üzere talebi için gerekli olan kişisel verilerinin işlenmesine ilişkin bilgilendirme metninin SMS yoluyla iletildiği,
- Veri sorumlusuna SMS göndermesinden sonra ilgili kişinin ilk olarak talebini değerlendiren ve sonrasında da limitini belirleyen kredi sürecinin başladığı,
- Bu sürecin karar ağacı formatında olduğu ve her bir kademedeki başvuru sahibinin kredibilitesini ölçmeye yarayan, saniyeler içerisinde ve otomatik çalışan, öngörüselle modellere dayanarak oluşturulan kredi politika kurallarından oluştuğu, dolandırıcılık ihtimalini ve suistimali önlemek amacıyla başvuran kişiye ait telefon numarası ile SMS içeriğinde kimlik numarasının eşleşip eşleşmediğinin kontrol edildiği, bu işlemin ilgili kişiye gönderilen bilgilendirme metninde de belirtildiği üzere, kişinin SMS gönderdiği telefon numarasının ve SMS içeriğinde yer alan kimlik numarasının Kredi Kayıt Bürosu'na aktarılması ile gerçekleştirildiği, akabinde başvuru sahibine ait kimlik numarasının kredi sorgulaması amacıyla Türkiye Bankalar Birliği Risk Merkezi'ne iletildiği, Bankanın kredi politikalarına uygun olan başvurular için ise kredi değerlendirme sistemi sayesinde söz konusu veriler ile her bir başvurunun risk seviyesi ve ödeyebileceği taksit tutarına göre kredinin ortalama 2,5 saniye içerisinde otomatik olarak hesaplandığı ve bunu müteakip başvurunun gerçekleştirildiği telefon numarasına sonucun iletildiği,

- Açıklanan nedenlerle ilgili kişinin iddialarının gerçeği yansıtmadığı

hususları bildirilmiştir.

Konuya ilişkin yapılan inceleme neticesinde, Kişisel Verileri Koruma Kurulunun 02/06/2022 tarihli ve 2022/545 sayılı Kararı ile;

"İlgili Kişiyeye Yapılan Aydınlatmanın Hukuka Uygunluğu" konusunda:

• 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) "Veri sorumlusunun aydınlatma yükümlülüğü"nü düzenleyen 10'uncu maddesinin, "Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; a) Veri sorumlusunun ve varsa temsilcisinin kimliği, b) Kişisel verilerin hangi amaçla işleneceği, c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi, d) 11 inci maddede sayılan diğer hakları konusunda bilgi vermekle yükümlüdür." hükmünü amir olduğu,

• Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in (Aydınlatma Tebliği) "Usul ve esaslar"ı düzenleyen 5'inci maddesinde yer alan (a) bendinde "İlgili kişinin açık rızasına veya Kanundaki diğer işleme şartlarına bağlı olarak kişisel veri işlendiği her durumda aydınlatma yükümlülüğü yerine getirilmelidir." hükmünün, (e) bendinde "Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı veri sorumlusuna aittir." hükmünün, (f) bendinde "Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir." hükmünün, (g) bendinde "Aydınlatma yükümlülüğü kapsamında açıklanacak kişisel veri işleme amacının belirli, açık ve meşru olması gerekir. Aydınlatma yükümlülüğü yerine getirilirken, genel nitelikte ve muğlak ifadeler yer verilmemelidir. Gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandıran ifadeler kullanılmamalıdır." hükmünün, (ğ) bendinde "Aydınlatma yükümlülüğü kapsamında ilgili kişiye yapılacak bildirim anlaşılır, açık ve sade bir dil kullanılarak gerçekleştirilmesi gerekmektedir." hükmünün, (h) bendinde "Kanun'un 10'uncu maddesinin birinci fıkrasının (ç) bendinde yer alan "hukuki sebep" ten kasıt, aydınlatma yükümlülüğü kapsamında kişisel verilerin Kanunun 5 ve 6'ncı maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiğidir. Aydınlatma yükümlülüğünün yerine getirilmesi esnasında hukuki sebebin açıkça belirtilmesi gerekmektedir." hükmünün, (ı) bendi ise "Aydınlatma yükümlülüğü kapsamında, kişisel verilerin aktarılma amacı ve aktarılacak alıcı grupları belirtilmelidir." hükmünün yer aldığı,

• Aydınlatma yükümlülüğünün amacının ilgili kişilerin kişisel verilerini belirli işlemler için veri sorumlularına vermeden önce kişisel verilerinin kullanımı, aktarımı, bu işlemlerin hukukî mesnetleri ve başvuru mercii olan veri sorumlusunun kimliği ile kendilerinin kişisel verileri üzerinde var olan haklarıyla alakalı olarak bilgilendirilerek, kişisel verileri üzerindeki hâkimiyetlerini tamamen yitirmelerini önlemek olduğu, aydınlatma yükümlülüğünün şeffaflık ilkesinin bir gereği olduğu, şeffaflığın şartının ilgili kişinin anlaşılabilir bir şekilde bilgilendiriliyor olması olduğu, aydınlatma metinlerinin her veri işleme faaliyetini kapsayacak şekilde yazılması halinde bu metinlerin çok uzun

ve karmaşık olması durumunun ortaya çıktığı, bu kapsamda çok aşamalı ve katmanlı, farklı hedef gruplara yönelik hazırlanmış ayrı aydınlatma metinlerinin bir çözüm alternatifi olarak görülebildiği, bu maksatla Kanun'un ilgili kişilere yönelik bir aydınlatmanın taşınması gereken asgari unsurları gösterdiği, "Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi"nde de "Kanun'un 4'üncü maddesinde yer alan temel ilkeler gereği veri sorumlularının, faaliyetleri kapsamında işlediği kişisel verileri, hangi işleme amacına dayanarak işlediğini kişisel veri bazında belirlemesi ve bu amacın da aydınlatma metinlerinde açıkça belirtilmesi gerekmektedir." denilerek aydınlatma yükümlülüğünün işlenecek kişisel veri bazında yerine getirilmesi gerektiğinin ifade edildiği,

- İlgili kişinin bahse konu numaraya SMS göndermek suretiyle kredi hesaplanması sürecini başlattığı, bu süreç devam ederken ilgili kişiye öncelikle kişisel verilerinin korunması ile ilgili olarak bir SMS gönderildiği ve bu SMS'te veri sorumlusunun aydınlatma metnine ulaşılmasını sağlayan bir bağlantının yer aldığı, sonrasında gelen SMS'te ise ilgili kişiye ait çekilebilecek kredi tutarının yer aldığı görüldüğü, şu hâlde ilgili kişinin iddiasının aksine veri sorumlusunun ilgili kişinin iradesiyle başlattığı veri işleme sürecini tamamlamadan evvel ilgili kişiye konuya ilişkin aydınlatmada bulunduğu görüldüğü, veri sorumlusunun ilgili kişinin başvuru sürecini sona erdirmesinden önce ilgili kişiye aydınlatmada bulunması gerektiği, nitekim Aydınlatma Tebliği'nin "Aydınlatma yükümlülüğünün kapsamı" başlığını haiz 4'üncü maddesinde yer alan "Kanunun 10'uncu maddesine göre; kişisel verilerin elde edilmesi sırasında veri sorumluları veya yetkilendirdiği kişilerce, ilgili kişilerin bilgilendirilmesi gerekmektedir." şeklindeki hüküm uyarınca kişisel verilerin işlenmesi sırasında ilgili kişilere bilgilendirme yapılmasının hukuka uygun olduğu,

- Veri sorumlusunun aydınlatma metni incelendiğinde; Kanun'un 10'uncu maddesinde gösterilen asgari unsurları karşıladığı görülmekle birlikte Aydınlatma Tebliği'ne birtakım aykırılıklar içerdiğinin tespit edildiği, geçerli ve hukuka uygun bir aydınlatmanın gerçekleştirilebilmesinin ilgili kişinin en azından kategorik olarak kişisel verileri üzerindeki hâkimiyetini yitirmemesine yani bu verilerin akıbetinden genel şekliyle haberdar olabilmesine bağlı olduğu, bunun da ancak işlenen veri kategorileri, bu kategorilerin hangi verileri içerdikleri, bu veri kategorilerinin işlenme/aktarıma amaçları ve hukukî mesnetleri arasındaki illiyet bağlarının veri sorumlusunca sunulan aydınlatma metninde gösterilmesi ile mümkün olabileceği, öte yandan şayet bir veri aktarımı yapılıyorsa aktarılan veri kategorilerinin hangi alıcı gruplarına aktarıldığının da aydınlatma metinlerinde sarih olarak ortaya konulmasının gerektiği, alıcı gruplarının; resmî merciler, iş ortakları vb. şekillerde sınıflandırılması mümkün olmakla birlikte bu alıcı gruplarının içerdiği üçüncü kişi ya da

kurum/kuruluşların da talep edildiği takdirde ilgili kişilerin sorularına yanıt verilebilmesini teminen veri sorumlusu nezdinde kayıtlı tutulmasının da büyük önem arz ettiği,

- Veri sorumlusunun aydınlatma metninde; hangi veri kategorisinin, hangi amaç ve hangi hukuka uygunluk sebebi kapsamında işlendiği arasında bir illiyet bağı kurulmadığı ve hangi veri kategorisinin hangi alıcı gruplarına hangi amaç ve hukuka uygunluk sebebi kapsamında iletildiğine yer verilmediği, bu bilgilerin oluşturulmasının ve kamuoyuna aydınlatma metinleri vasıtasıyla sunulmasının veri sorumluları için bir külfet oluşturmadığı,

- Veri sorumluları siciline (VERBİS) kayıt yaptırmakla yükümlü olan veri sorumlusunun Veri Sorumluları Sicili Hakkında Yönetmelik'in "İlke, usul ve esaslar"ı düzenleyen 5'inci maddesinin (1) numaralı fıkrasının (ç) bedinde yer alan "Sicile kayıtlı yükümlü olan veri sorumluları, Kişisel Veri İşleme Envanteri hazırlamakla yükümlüdür. Sicil başvurularında Sicile açıklanacak bilgiler Kişisel Veri İşleme Envanterine dayalı olarak hazırlanır." hükmü doğrultusunda kişisel veri işleme envanteri hazırlamış olması ve hâlihazırda aydınlatma metninde yer alan eksiklikleri bu envantere yer alan bilgiler doğrultusunda gidermiş olması gerekeceği,

- Bu minvalde, veri sorumlusunun ilgili kişiye yönelik aydınlatmada bulunduğu, bu aydınlatmanın Kanun'un 10'uncu maddesi uyarınca hukuken geçerli ve muteber olduğu, ancak içerisinde Aydınlatma Tebliği'nde düzenlenen detay konularda birtakım eksiklikler bulunduğu tespitinin yapıldığı,

"İlgili Kişinin Açık Rızası Olmaksızın Kişisel Verilerinin İşlenip İşlenmediği" konusunda:

- Veri sorumlusunun; ilgili kişinin T.C. kimlik numarası ve cep telefonu verisini Kimlik Paylaşım Sistemi (KPS) aracılığıyla MERNİS ve nüfus kayıtlarıyla eşleştirerek doğruladığı, bu bilgileri Kredi Kayıt Bürosu ve Türkiye Cumhuriyet Merkez Bankası'na aktararak kredi performansı ve çek, haciz bilgileri ile risk analizi yaptığı ve kredi sorgulaması amacıyla TBB Risk Merkezi'ne gönderdiği ve bu sonuçları otomatik algoritmalar ile hesaplayarak ilgili kişiye bir kredi miktarı çıkardığı, veri sorumlusunun bu hesaplamaları kendi nezdinde önceden tutulmuş hiçbir veri olmaksızın yaptığının anlaşıldığı, bu doğrultuda ilgili kişinin iddialarının gerçeği yansıtmadığı ve bu hususta bir hukuka aykırılık emaresine rastlanmadığı,

"İlgili Kişiye Usulüne Uygun Bir Yanıt Verilmemesi" konusunda:

- İlgili kişinin veri sorumlusuna yaptığı başvuruda; hangi kişisel verilerinin, hangi amaç ve hukukî sebeplere dayanılarak işlendiği, hangi tarihlerde işlenmeye başlandığı ve bu verilerin kimlerden temin edildiği, bu verilerin üçüncü kişilere aktarılıp aktarılmadığı, veri işlenmesi sırasında neden

aydınlatma yükümlülüğünün yerine getirilmediği, ilgili kişinin kredi limiti hesaplanırken hangi kişisel verilerine, hangi yöntemler ve kurumlar vasıtasıyla ulaşıldığı, ilgili kişinin kişisel verilerinin işlenmesi hususunda veri sorumlusuna verdiği bir açık rıza bulunup bulunmadığı hususlarında bilgi talep ettiği,

- Veri sorumlusunun ise verdiği yanıt içerisinde; ilgili kişinin kişisel verilerinin ilk olarak kendisi tarafından SMS gönderildiği tarihte işlendiği, bu SMS'te yer alan T.C. kimlik numarasının hukuki ve ticari risk analizleri yapabilmek amacıyla bankacılık mevzuatı uyarınca temin edildiği, ilgili kişiye SMS vasıtasıyla kademeli aydınlatma yapıldığı, ilgili kişinin verilerinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasında yer alan şartlar, 5411 sayılı Bankacılık Kanunu ve MASAK mevzuatı kapsamında işlendiği hususlarına yer verildiği, ayrıca ilgili kişinin bilgilerinin aktarıldığı kurum ve kuruluşlar hakkında bilgi verildiğinin görüldüğü,

- Bu kapsamda, ilgili kişiye hukuken muteber ve geçerli bir yanıt verilmiş ise de bu yanıtın aydınlatma yükümlülüğü ile ilgili yukarıda arz edilen detaylardan yoksun olduğunun ve bu haliyle ilgili kişinin taleplerine yönelik tam ve eksiksiz bir yanıt sağlamaktan uzak olduğunun görüldüğü, örneğin veri sorumlusu ilgili kişinin kişisel verilerinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasında gösterilen şartlar dâhilinde işlendiğini ifade etmekte ise de bu verilerin hangi veriler olduğunun ve ilgili maddede gösterilen hangi şarta dayalı olarak işlendiğinin meçhul olduğu, bu sebeplerle veri sorumlusunun ilgili kişiye karşı tam ve eksiksiz aydınlatma ile ilgili arz edilen şartları sağlayan bir metinle yanıt verme yükümlülüğünü ihlâl ettiğinin anlaşıldığı

değerlendirmelerinden hareketle;

- İlgili kişiye Kanun'un 10'uncu maddesi uyarınca hukuken geçerli bir şekilde aydınlatmada bulunulduğu fakat bu aydınlatmada Aydınlatma Tebliği ile düzenlenen bazı hususlarda giderilmesi gereken eksiklikler bulunduğu dikkate alındığında, aydınlatma metninin Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'e uygun hale getirilmesi ve sonucundan otuz günlük yasal süre içerisinde Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına,

- İlgili kişinin veri sorumlusuna yaptığı başvuruya verilen yanıtın; ilgili kişinin taleplerini karşılamaktan uzak ve eksik bir yanıt olduğu dikkate alındığından veri sorumlusunun ilgili kişilerin başvurularına, Kanun'a ve Tebliğ'e uygun şekilde yanıt vermesi hususunda azamî dikkat ve özeni göstermesi konusunda uyarılmasına

karar verilmiştir.

2022/491 sayılı KVKK Kararı

Veri sorumlusu bir giyim mağazası için katalog modeli olarak çalışan ilgili kişinin fotoğraflarının, iş ilişkisinin sona ermesinden sonraki süreçte açık rızası olmaksızın veri sorumlusuna ait internet sitesinde yayınlanmaya devam etmesi hakkında Kişisel Verileri Koruma Kurulunun 18/05/2022 tarihli ve 2022/491 sayılı Karar Özeti

Karar Tarihi : 18/05/2022

Karar No : 2022/491

Konu Özeti: Veri sorumlusu bir giyim mağazası için katalog modeli olarak çalışan ilgili kişinin fotoğraflarının, iş ilişkisinin sona ermesinden sonraki süreçte açık rızası olmaksızın veri sorumlusuna ait internet sitesinde yayınlanmaya devam etmesi

İlgili kişinin şikâyetinde özetle; veri sorumlusu bir giyim mağazası tarafından satışa çıkarılan ürünlerin tanıtım ve görsellerinin veri sorumlusuna ait internet sayfasında paylaşıldığı, ilgili kişinin bünyesinde katalog modeli olarak çalıştığı veri sorumlusu ile iş ilişkisinin sona ermesine rağmen fotoğraflarının açık rızası olmaksızın veri sorumlusuna ait internet adreslerinde yayınlanmaya devam edildiği, ilgili kişinin fotoğrafların kaldırılması talebiyle veri sorumlusuna başvuruda bulunmasına rağmen fotoğrafların yayınlanmasına devam edildiği belirtilerek gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusunun savunması talep edilmiş olup veri sorumlusunun cevabi yazısında özetle;

- İlgili kişinin, tarafları ile fotomodellik yapmayı üstlendiği bir eser sözleşmesinin mevcut olduğu, bu sözleşmenin doğası gereği ilgili kişinin fotoğraflarının çekildiği ve tanıtım amacıyla sergilenen ürünler stoklarda bitene kadar bu fotoğrafların sosyal medya hesaplarında paylaşıldığı,
- İlgili kişinin bu verilerinin paylaşılmasına açık rızasının olduğu, ilgili kişinin fotoğraflarının belirsiz süreli bir sözleşmesi kapsamında çekildiği, ilgili kişinin üzerinde taşıdığı ürünleri iyi görünecek şekilde taşımayı ve fotoğraflanmayı kabul ve taahhüt ettiği, fotoğraflarının kullanılması karşılığında ilgili kişiye ödeme yapıldığı,

- Açık rızanın, rıza veren kişinin “olumlu irade beyanı”nı içermesi gerektiği ve diğer mevzuattaki düzenlemeler saklı kalmak üzere açık rızanın yazılı şekilde alınmasına gerek olmadığı, ilgili kişinin rızası olmaksızın modellik yaparak fotoğraflarının çekilmesinin mümkün olmadığı,
- İlgili kişinin bir eser sahibi olması sebebiyle kendisine yapılan ödemeler ile eserin umuma arz edilmesine ve yayımlanmasına yönelik haklarının devredildiği,
- Yapılan bu işlemin hukuki ilişkiden kaynaklı olarak yapıldığı, fotoğrafların yalnızca ürünlerin tanıtımı amacıyla sınırlı bir zaman diliminde kullanıldığı ve stokların sona ermesi ile fotoğrafların ilgili mecralardan kaldırıldığı,
- İlgili kişinin Kanun kapsamındaki başvurusunda modellik yaptığı fotoğrafların kaldırılması talebinin bulunmadığı, ihtarname ile fotoğrafların kullanımı için ilgili kişinin tek tarafı olarak belirlediği miktarın ödenmesinin talep edildiği,
- İlgili kişinin fotoğraflarının hukuki ve ticari ilişki kapsamında açık rızasıyla çekildiği ve paylaşıldığı, ilgili kişi ile yazılı bir fotomodellik sözleşmesinin akdedilmediği ve taraflar arasında sözlü olarak devam eden uzun süreli ticari ilişkinin, karşılıklı güven esasına dayanan bir çalışma modelinin mevcut olduğu hususları belirtilmiş ve yazıları ekinde Kanun kapsamında kendilerine yapılan başvuruya ve verilen yanıtta, ayrıca muhtelif tarihlerde ilgili kişinin hesabına gönderilen paranın transferine ilişkin dekontlara yer verildiği görülmüştür.

Konuya ilişkin yapılan inceleme neticesinde, Kişisel Verileri Koruma Kurulunun 18/05/2022 tarihli ve 2022/491 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun (Kanun) “Tanımlar” başlıklı 3’üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, “belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza”, (ç) bendinde ilgili kişinin, “kişisel verisi işlenen gerçek kişi”, (d) bendinde kişisel verinin, “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi”, (e) bendinde kişisel verilerin işlenmesinin, “kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem”, (ı) bendinde veri sorumlusunun, “kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi” olarak tanımlandığı,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi; fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin kendisi tarafından alenileştirilmiş olması; bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hükmünün yer aldığı,
- Kanun'un "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi" başlıklı 7'inci maddesinin (1) numaralı fıkrasının "Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hale getirilir." hükmünü haiz olduğu,
- Kanun'un "İlgili Kişinin Hakları" başlıklı 11'inci maddesinde de herkesin, veri sorumlusuna başvurarak kendisiyle ilgili; kişisel verilerinin işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerinin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerinin aktarıldığı üçüncü kişileri bilme, kişisel verilerinin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme, 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerinin silinmesini veya yok edilmesini isteme, kişisel verilerinin düzeltilmesi veya silinmesi/yok edilmesi ile ilgili yapılan işlemlerin kişisel verilerinin aktarıldığı üçüncü kişilere bildirilmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme ve kişisel verilerinin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme haklarına sahip olduğunun hüküm altına alındığı,
- Somut olayda, ilgili kişi ile veri sorumlusu arasında iş ilişkisinden doğan yazılı olmayan bir sözleşmenin bulunduğu ve bu sözleşme kapsamında ilgili kişinin veri sorumlusu nezdinde fotomodellik yaptığı, söz konusu iş ilişkisinin sona ermesi nedeniyle ilgili kişinin veri sorumlusunun

internet adresinde yayınlanan fotoğraflarının kaldırılmasını talep ettiği, ilgili kişinin fotomodellik yaptığı kıyafetlerin stoklarının sona ermesinden sonra söz konusu fotoğrafların kaldırıldığının anlaşıldığı,

- Diğer yandan, ilgili kişinin şikâyet dilekçesinde yer verdiği linklerin incelenmesinden her bir linkin veri sorumlusu şirketin internet sitesinin ana sayfasına yönlendirildiğinin, dolayısıyla söz konusu linklerin açılmadığının görüldüğü,

- Bu kapsamda, ilgili kişinin fotoğraflarının ilgili kişi ile veri sorumlusu arasındaki sözleşmeye istinaden Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (c) bendinde yer verilen "Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması" şartı çerçevesinde internet sitesinde yayınlanmak suretiyle işlendiği kanaatine varıldığı

değerlendirmelerinden hareketle;

- İlgili kişinin iş ilişkisinin sona ermesi nedeniyle fotoğraflarının veri sorumlusu şirketin internet sayfasından kaldırılması talebi ile ilgili olarak veri sorumlusunun, kıyafetlerin stoklarının bitene kadar paylaşıldığı beyanı ve ilgili kişinin fotoğraflarının ilgili kişi ile veri sorumlusu arasındaki sözleşmeye istinaden Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (c) bendi çerçevesinde internet sitesinde yayınlamak suretiyle işlendiği dikkate alındığında veri sorumlusu şirket hakkında Kanun kapsamında yapılacak bir işlem bulunmadığına

karar verilmiştir.

2022/489 sayılı KVKK Kararı

Kişisel Verileri Koruma Kurulunun 18/05/2022 tarihli ve 2022/489 sayılı Karar Özeti

Karar Tarihi : 18/05/2022

Karar No : 2022/489

Konu Özeti: Kamu tüzel kişiliğini haiz Birlik tarafından ilgili kişinin kişisel verilerini içeren belgelerin Birliğin vekili tayin edilen avukat ile paylaşılması ve müteakiben söz konusu belgelerin avukat tarafından Baroya aktarılması

İlgili kişinin şikâyetlerinde özetle;

- Kendisinin avukatlık mesleğini icra ettiği, kamu tüzel kişiliğini haiz Birlik ile arasındaki hukuki danışmanlık ve avukatlık sözleşmesinin fesih görüşmeleri sırasında kendisini Birlik vekili olarak tanıtan bir avukatın ilgili kişiyi aradığı ve sözleşmeyi feshetmesini istediği,
- Bunun üzerine Birlik ile konu hakkındaki görüşmeleri devam ederken kendisini Birlik vekili gibi tanıttığı ve avukatlık meslek etiğine uygun olmayacak şekilde konuşması nedeniyle hakkında disiplin soruşturması yapılmasını teminen ilgili kişinin söz konusu avukatı Baroya şikâyet ettiği
- Avukatın Baro Başkanlığına sunduğu savunması ile ilgisi olmayan, sadece Birlikte asılları bulunan ve danışmanlık sözleşmesi kapsamında Birliğe kesilen serbest meslek makbuzu ve stopaj ödeme listesinin fotokopilerine savunma dilekçesi ekinde yer verdiği, bunun üzerine ilgili kişinin söz konusu avukata ve Birliğe başvuruda bulunduğu ancak yanıt alamadığı

belirtilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gerekli işlemlerin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde şikâyet edilen Birliğin ve avukatın ayrı ayrı savunması talep edilmiş olup veri sorumlusu Birliğin cevabi yazısında özetle;

- İlgili kişinin kurumlarına yapmış olduğu başvuruya cevap verilmediği hususunun gerçeği yansıtmadığı, ilgili kişiye ihtar ile cevap verildiği,

- Birlik Başkanlığı ile danışmanlık sözleşmesi kapsamında kesilen ve ilgili kişinin kişisel verilerini içeren stopaj ödeme listesinin fotokopilerinin Avukatlık Kanunu'na dayanılarak şikâyet edilen avukat ile paylaşıldığı,
- Söz konusu dönemde kurum vekili olarak görev yapan başka bir avukat tarafından verilen yetki belgesi kapsamında şikâyet edilen avukatın da kurum vekili olarak görevini ifa ettiği, bu hususun Avukatlık Kanunu'nun 56'ncı maddesinin (5) numaralı fıkrasında açıkça düzenlendiği, Türkiye Barolar Birliği Avukatlık Kanunu Yönetmeliği'nin 18'inci maddesinde "Avukatlar veya avukatlık ortaklıkları, başkasını tevkil etme yetkisini taşıdıkları tüm vekaletnameleri kapsayacak şekilde tek bir genel ya da ayrı ayrı özel yetki belgesi düzenleyerek; bir başka avukatı veya avukatlık ortaklığını müvekkilleri adına vekil tayin edebilirler. Vekaletname hükmünde olan bu yetki belgesi; tüm yargı mercileri ile resmi ve özel kişi, kurum ve kuruluşlar için hukuken vekaletname işlev ve etkisi taşır." hükmüne yer verildiği,
- İlgili kişi tarafından şikâyet edilen avukat aleyhine Baro Başkanlığına yapılan şikâyet doğrultusunda serbest meslek makbuzunun ve stopaj ödeme listesinin savunmaların delili mahiyetinde sunulduğu, Türk Borçlar Kanunu'nun 502'nci maddesi ve Avukatlık Kanunu hükümleri kapsamında şikâyet edilen avukat ile kurumları arasında vekalet sözleşmesi kurulduğu, bu kapsamda söz konusu belgelerin 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 5'inci maddesinin (2) numaralı fıkrasının (c) bendindeki açık rıza hususunun istinası niteliğini haiz olduğu belirtilmiştir.

Şikâyete istinaden savunması istenen avukatın cevabi yazısında ise özetle;

- İlgili kişinin başvurusuna Birlik tarafından yanıt verildiği, ilgili kişinin söz konusu başvuru konusuna ilişkin bilgilendirildiği için tekrar aynı sorulara cevap verilmesinde hukuki bir yararın bulunmadığı,
- Avukatlık Kanunu kapsamında hazırlanmış olan "yetki belgesi" ile Birliği temsil yetkisinin bulunduğu, yapılan tüm işlemlerin bu yetki belgesine dayanılarak gerçekleştirildiği, ilgili belge ve bilgilerin iddia edildiği gibi üçüncü kişilerle paylaşılmasının söz konusu olmadığı,

İlgili kişi ile müvekkili Birlik arasında avukatlık sözleşmesine dayalı bir ilişkinin bulunduğu dönemde ilgili kişinin Birliği stopajlı faturalar keserek zarara uğrattığı, bu kapsamda detaylı bir inceleme yapılması amacıyla şikâyete konu bilgi ve belge fotokopilerinin fiziki dosya şeklinde tarafına verildiği, bu süreçte ilgili kişi tarafından Baroya asılsız iddialara dayanan bir şikâyette

bulunulduğu, bu çerçevede savunma hakkını kullanmak ve iddialarını desteklemek için zaruri olması nedeniyle söz konusu stopaj listesi ve makbuz örneklerinin savunma dilekçesine eklendiği,

- Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (c) ve (e) bentleri ile 28'inci maddesinin (2) numaralı fıkrasının (c) bendi göz önüne alındığında söz konusu bilgi ve belgelerin savunmaya dayanak olarak Baro'ya sunulmasının Kanun hükümlerine aykırılık oluşturmadığı belirtilmiştir.

Konuya ilişkin yapılan inceleme neticesinde, Kişisel Verileri Koruma Kurulunun 18/05/2022 tarihli ve 2022/489 sayılı Kararı ile;

- Kanun'un 3'üncü maddesinde "veri sorumlusu"nun "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi" olarak tanımlandığı, veri sorumlusunun veri işleme faaliyetinin genel anlamda "neden" ve "nasıl" yapıldığını belirleyen kişi olduğu, "hangi kişisel verilerin toplanacağı, kişisel verilerin hangi amaçlarla işleneceği, hangi kişilerin kişisel verisinin toplanacağı, kişisel verilerin kimlere, hangi amaçla aktarılacağı, kişisel verilerin hangi süre ile saklanacağı" konularındaki kararların ancak veri sorumlusu tarafından alınabildiği,

- Genel Bütçe Kapsamındaki Kamu İdareleri ve Özel Bütçeli İdarelerde Hukuk Hizmetlerinin Yürütülmesine İlişkin Kanun Hükmünde Kararname'nin "Muhakemat hizmeti temini" başlıklı 5'inci maddesinin (3) numaralı fıkrasının "Birinci ve ikinci fıkraya göre muhakemat hizmetlerinin temin edilememesi veya özel uzmanlık gerektirdiği Cumhurbaşkanlığında Cumhurbaşkanı veya Cumhurbaşkanlığı İdari İşler Başkanının, bakanlıklarda ilgili bakanın onayı ile belirlenen hallerde muhakemat hizmetlerini yürütmek üzere Cumhurbaşkanı kararıyla belirlenen usul ve esaslar çerçevesinde, 4/1/2002 tarihli ve 4734 sayılı Kamu İhale Kanununun 22 nci maddesine göre doğrudan temin usulüyle serbest avukatlardan veya avukatlık ortaklıklarından hizmet satın alınabilir." hükmünü haiz olduğu,

- Serbest Avukatlardan Hizmet Satın Alınmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik'in 4'üncü maddesinin (1) numaralı fıkrasında ise "İdareler, muhakemat hizmetlerini kendi hukuk birimlerinden, bakanlıklarından veya bağlı kuruluşlarından ve Maliye Bakanlığından temin edemediği ya da hizmetin özel uzmanlık gerektirdiği ilgili bakan onayı ile belirlendiği hallerde, serbest avukatlardan hizmet satın alabilir." hükmüne yer verildiği,

- Öte yandan Avukatlık Kanunu'nun 56'ncı maddesinin (5) numaralı fıkrasında "Avukatlar veya avukatlık ortaklığı başkasını tevkil etme yetkisini haiz oldukları bütün vekâletnamelerini kapsayacak

şekilde bir başka avukata veya avukatlık ortaklığına vekâletname yerine geçen yetki belgesi verebilir. Bu yetki belgesi vekâletname hükmündedir.” hükmüne yer verildiği, Avukatlık Kanunu Yönetmeliği'nin 18'inci maddesinin (2) numaralı fıkrasında “Avukatlar veya avukatlık ortaklıkları, başkasını tevkil etme yetkisini taşıdıkları tüm vekaletnameleri kapsayacak şekilde tek bir genel ya da ayrı ayrı özel yetki belgesi düzenleyerek; bir başka avukatı veya avukatlık ortaklığını müvekkileri adına vekil tayin edebilirler. Vekaletname hükmünde olan bu yetki belgesi; tüm yargı mercileri ile resmi ve özel kişi, kurum ve kuruluşlar için hukuken vekaletname işlev ve etkisi taşır.” hükmünün düzenlendiği,

- Somut olayda, ilgili kişinin Birlik ile arasındaki hukuki danışmanlık sözleşmesinin feshedilmesinin ardından Birliğin anlaştığı avukatın düzenlediği yetki belgesi ile şikâyet edilen avukatın da Birliğin vekili konumuna geldiği, şikâyet edilen avukatın Birliğin vekili sıfatıyla ilgili kişiyi aradığı, söz konusu görüşme esnasında yaşanan anlaşmazlık sonucunda ilgili kişinin şikâyete konu avukatı, avukatlık meslek kurallarına aykırı davranışları nedeniyle Baroya şikâyet ettiği, bu olay sonucunda şikâyet edilen avukatın Baroya sunduğu dilekçe ekinde ilgili kişinin kişisel verilerini içeren belgelere de yer verdiği ve söz konusu belgeleri Birlikten edindiği hususları ile ilgili kişinin Birlik ile anılan avukatı ayrı ayrı şikâyet ettiği,

- Veri sorumlusunun tespiti kapsamında Birliğin kendi nezdinde bulunan ilgili kişinin kişisel verilerini içeren belgeleri hukuki danışmanlık hizmeti aldığı şikâyet edilen avukat ile paylaşması kapsamında kişisel verilerin işleme amaç ve vasıtasını belirlediğinden hareketle veri sorumlusu sıfatını haiz olduğu, diğer taraftan Birlik ile aralarındaki sözleşme kapsamında işin gereği olarak ilgili kişinin kişisel verilerini içeren şikâyet konusu belgeleri elde ederek daha sonra ilgili kişiyle yaşadığı anlaşmazlık sonrasında söz konusu belgeleri Baroya ileten dolayısıyla kişisel verilerin işlenmesinde amaç ve yöntemi belirleyen şikâyet edilen avukatın da somut olay nezdinde veri sorumlusu sıfatını haiz olduğu,

- Kanun'un “Kişisel verilerin işleme şartları” başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması

için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Birliğin ilgili kişinin kişisel verilerini içeren belgeleri, yetki belgesi ile Birliğin vekili tayin edilen şikâyet edilen avukat ile paylaşması kapsamında; Birliğin kamu tüzel kişiliğini haiz bir kurum olarak özel kanun ile taraflarına hasredilen görevleri yerine getirmeleri sürecinde dışarıdan avukatlık hizmeti aldıkları ve bu durumda hizmet aldıkları şikâyet edilen avukat ile ilgili kişiye ait kişisel verileri içeren belgeleri paylaşmalarının Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (e) bendinde yer alan "Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" şartı çerçevesinde değerlendirildiği,

- Veri sorumlusu sıfatını haiz şikâyet edilen avukatın Baroya sunduğu savunma dilekçesi ekinde ilgili kişiye ait kişisel verileri içeren belgelere de yer vermesine ilişkin olarak Birliğin "yetki belgesi" kapsamında temsil yetkisinin bulunduğu, ilgili belge ve bilgilerin iddia edildiği gibi üçüncü kişilerle paylaşılmasının söz konusu olmadığı, savunma hakkını kullanmak ve iddialarını desteklemek için zaruri olması nedeniyle stopaj listesinin ve makbuz örneklerinin ek olarak savunma dilekçesinde yer aldığı beyanlarından hareketle veri sorumlusu sıfatını haiz avukatın ilgili kişinin kişisel verilerini içeren belgeleri yürütülen soruşturma kapsamında Baroya aktarmasının Kanun'un 8'inci maddesine uygun olarak Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (e) bendi çerçevesinde gerçekleştirildiği kanaatine varıldığı

değerlendirmelerinden hareketle;

- Birlik Başkanlığının ilgili kişinin kişisel verilerini içeren belgeleri Birliğin vekili tayin edilen avukat ile paylaşması ile ilgili olarak; Birliğin kamu tüzel kişiliğini haiz bir kurum olarak taraflarına hasredilen görevleri yerine getirmeleri sürecinde dışarıdan avukatlık hizmeti aldıkları ve bu durumda söz konusu avukat ile ilgili kişiye ait kişisel verileri içeren belgeleri paylaşmalarının Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (e) bendi çerçevesinde değerlendirilebileceği kanaatine varıldığından ilgili kişinin Birlik hakkındaki şikâyeti ile ilgili olarak Kanun kapsamında yapılacak herhangi bir işlem bulunmadığına,

- Veri sorumlusu sıfatını haiz avukatın ilgili kişinin kişisel verilerini içeren belgeleri yürütülen soruşturma kapsamında Baroya aktarmasının Kanun'un 8'inci maddesine uygun olarak Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (e) bendi çerçevesinde gerçekleştirildiği kanaatine

varıldığından ilgili kişinin söz konusu avukat hakkındaki şikâyeti ile ilgili olarak Kanun kapsamında yapılacak herhangi bir işlem bulunmadığına karar verilmiştir.

2022/386 sayılı KVKK Kararı

Veri sorumlusu bünyesinde çalışan bir kişinin iş akdinin sonlandırılması hususunun veri sorumlusuna ait sosyal medya hesabında paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 21/04/2022 tarihli ve 2022/386 sayılı Karar Özeti

Karar Tarihi : 21/04/2022

Karar No : 2022/386

Konu Özeti: Veri sorumlusu bünyesinde çalışan bir kişinin iş akdinin sonlandırılması hususunun veri sorumlusuna ait sosyal medya hesabında paylaşılması

İlgili kişi tarafından Kuruma iletilen şikâyet dilekçesinde özetle; veri sorumlusu bünyesinde şirket müdürü olarak çalışmakta iken iş akdinin haksız şekilde sonlandırıldığı ve veri sorumlusuna ait sosyal medya hesabında "... Yaptığı usulsüzlükler nedeni ile işten ATILAN'ın sizlere vermiş olduğu rahatsızlıktan dolayı özür dileriz..." içerikli bir paylaşım yapıldığı, söz konusu paylaşımın silinmesi, durdurulması ve düzeltme metni yayınlanması için 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) gereği veri sorumlusuna ihtarda bulunduğu ancak tarafına cevap verilmediği, herhangi bir mahkeme kararı ve rızası olmadan yapılan bu duyurudan şikâyetçi olduğu belirtilerek Kanun kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması talep edilmiş olup alınan cevabi yazıda özetle;

- İlgili kişinin işten ayrıldıktan sonra taraflarını zarara uğratmak için çeşitli faaliyetlerde ve tarafları hakkında birtakım haksız şikâyetlerde bulunduğu; Kuruma iletilen şikâyetin de bu amacı taşıdığı,

İlgili kişi ile aralarında çeşitli hukuki süreçlerin devam ettiği; İş Mahkemesinde davalarının olduğu ayrıca ilgili kişi hakkında dolandırıcılık, resmî belgede sahtecilik, şirket bilgisi dışında şirket adına para çekmek ve kendi adına usulsüz ödeme yaptırmak ile verilen yetkiyi kötüye kullanmak suçlamaları ile soruşturmaların bulunduğu,

- İlgili kişinin, şirketlerinin ticari itibarlarını zedelemeye yönelik faaliyetlerinin olduğu, şirketin sahte kaşesini yaptırarak taraflarına haciz işlemi uygulatmaya çalıştığı konularında İcra Mahkemesinde davalarının olduğu ve şirket lehine sonuçlandığı,
- Sosyal paylaşım sitesindeki duyurunun ilgili kişinin şirketin bütün müşterilerine göndermiş olduğu “Kıymetli Musterimiz; Firmamız Mali Olarak Kapanmıştır. eski yerimize yakın farklı isimle hizmet veren firmayla BAGIMIZ YOKTUR (.....Bey)” şeklindeki gerçek olmayan beyanlar içeren SMS bildirimine karşı doğru ve gerçek durumu açıklamak amacıyla ve ilgili kişinin kendisi veya aile bireyleri için şirket adına müşterilerinden ödeme talep etmesinden dolayı müşterilerinin mağdur olmasını engellemeye yönelik bilgilendirme maksadı ile yapıldığı,
- İlgili kişi tarafından yapılan ve gerçeği yansıtmayan açıklamaya karşılık yapılan düzeltme mahiyetindeki söz konusu duyuru haricinde herhangi bir veri girişi yapılmadığı, depolanmadığı, ilgili kişinin müşteriler tarafından tanınmasından dolayı benzer bir durum yaşanmaması için ilgili kişinin sadece adının verildiği,
- İlgili kişinin ihtarnamesine aralarında devam eden dava ve soruşturmalar bulunması nedeni ile cevap verilmediği,
- Ayrıca ilgili kişi tarafından gönderilen ve gerçeği yansıtmayan mesajlara karşılık bir tedbir olarak sosyal paylaşım sitesinde yayınlanan yazının şikayetçi ile aralarındaki davaların devam etmesi nedeniyle ve herhangi bir zamanda benzer bir durum ile karşı karşıya kalınması halinde doğru bilginin öğrenilmesi adına silinmediği
- Duyurunun Kişisel Verilerin Korunması Kanunu’na aykırılık teşkil etmediği, Kanun’un “Genel ilkeler” başlıklı 4’üncü maddesinde kişisel verilerin hukuka ve dürüstlük kurallarına uygun şekilde, doğru ve gerektiğinde güncel kalma şartı ile açıklanabildiği, ceza hukukunda düzenlenen meşru savunma kurumunun da taraflarına bu hakkı verdiği, meşru savunmanın kişinin kendisine veya bir başkasına yönelmiş haksız bir saldırıya karşı o anki durum ve imkanlar çerçevesinde saldırı ile orantılı bir şekilde işlenen bir fiil olduğu

ifade edilmiştir.

Konuya ilişkin olarak yapılan incelemede Kişisel Verileri Koruma Kurulunun 21/04/2022 tarihli ve 2022/386 sayılı Kararı ile;

- Kanun’un “Tanımlar” başlıklı 3’üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, “belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza”, (ç) bendinde ilgili kişinin, “kişisel verisi işlenen gerçek kişi”, (d) bendinde kişisel verinin, “kimliği belirli veya

belirlenebilir gerçek kişiye ilişkin her türlü bilgi”, (e) bendinde kişisel verilerin işlenmesinin, “kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem”, (1) bendinde veri sorumlusunun, “kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi” olarak tanımlandığı,

- Kanun’un “Kişisel Verilerin İşlenme Şartları” başlıklı 5’inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi; fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin kendisi tarafından alenileştirilmiş olması; bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hükmünün yer aldığı,

- Hukuka uygun bir kişisel veri işleme faaliyetinin gerçekleştirilebilmesi için kişisel verilerin öncelikle Kanun’un 5’inci maddesindeki şartlardan birine dayanılarak işlenmesi gerekmekte olup, geçerli bir hukuki sebebi olan kişisel veri işleme faaliyetleri bakımından ise her hal ve şartta Kanun’un 4’üncü maddesinde sayılan temel ilkelere uygunluğun sağlanmasının veri sorumlusunun başlıca yükümlülükleri arasında olduğu,

- Somut olayda, ilgili kişinin açık ad ve soyadı ile ilgili kişi hakkındaki ithamları da içeren duyurunun sadece şirket müşterilerinin değil herkesin erişimine açık şekilde şirketin sosyal medyada yer alan kurumsal hesabında/sayfasında yayımlandığı, bu çerçevede, veri sorumlusunun sosyal medyadaki kurumsal hesabı/sayfasının sadece şirketin müşterilerine özel bir ortam olmadığı, herkese açık bir platform olduğu dikkate alındığında söz konusu eylemin Kanun’un 4’üncü maddesindeki ölçülülük ilkesine aykırılık teşkil ettiği ve ilgili kişinin kişisel verilerinin işlenmesine ilişkin Kanun’un 5’inci

maddesi kapsamındaki bir işleme şartına dayanıldığına dair Kuruma somut herhangi bir bilgi, belge sunulmadığı

değerlendirmelerinden hareketle;

- İlgili kişinin kişisel verilerinin Kanun'un 5'inci maddesinde yer alan herhangi bir işleme şartına dayanmaksızın veri sorumlusuna ait sosyal medya hesabında paylaşılmak suretiyle işlendiği kanaatine varıldığından, Kanun'un 12'nci maddesinin (1) numaralı fıkrasında yer verilen yükümlülüklerini yerine getirmediği değerlendirilen veri sorumlusu hakkında, şikayete konu olayda ilgili kişi hakkındaki duyurunun veri sorumlusu tarafından Kanun'un 4'üncü maddesine aykırı olarak herkese açık bir şekilde yapıldığı, veri işleme ile gerçekleştirilmesi istenen amaç arasında makul bir denge bulunmadığı, Kanun kapsamındaki bir işleme şartına dayanıldığına dair Kuruma somut herhangi bir bilgi, belge sunulmadığı hususları ile veri sorumlusunun ekonomik durumu dikkate alınarak, Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 30.000 TL idari para cezası uygulanmasına,

- İlgili sosyal medya paylaşımında yer verilen kişisel verilerin imha edilerek sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2022/328 sayılı KVKK Kararı

İlgili kişinin kişisel verilerinin yer aldığı ihtarnamenin, bordrolama hizmeti sunan veri sorumlusu tarafından başka çalışanlara da gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 07/04/2022 tarih ve 2022/328 sayılı Karar Özeti

Karar Tarihi : 07/04/2022

Karar No : 2022/328

Konu Özeti: İlgili kişinin kişisel verilerinin yer aldığı ihtarnamenin, bordrolama hizmeti sunan veri sorumlusu tarafından başka çalışanlara da gönderilmesi

Kuruma intikal eden şikâyetle özetle; ilgili kişinin ücretsiz izne gönderildiğine dair veri sorumlusu tarafından kendisine bir ihtarname ileildiği, söz konusu ihtarnamenin yedi kişiye daha gönderildiği, ihtarnamede T.C. kimlik numarası ve adresinin bulunması nedeniyle ilgili kişinin kişisel verilerinin alenen ifşa edildiği belirtilerek gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- İlgili kişinin esasen aynı grup şirketine ait başka bir şirketin çalışanı olduğu ve aynı grup şirketi çatısı altında yer almaları nedeniyle taraflarınca, söz konusu şirket çalışanlarının ücretleri ve çalışma süreleri kapsamında bordrolama hizmeti temin edildiği ve çalışanlara yönelik bordro oluşturma ve izin kullanım süreçlerinin denetlenerek bunların kontrol ve takip edilmesi hizmeti sunulduğu,
- COVID-19 pandemisinden dolayı alınan tedbirler kapsamında ücretsiz izin kullanımının iş yerinde zorunlu hale gelmesi nedeniyle istihdamın sonlanmaması ve iş yeri ile personel sağlığının tehlikeye düşmemesi adına, ilgili kişinin, asıl işvereni olan şirket tarafından ücretsiz izne çıkarıldığı ve bu kapsamda ilgili kişinin ad ve soyadı, T.C. kimlik numarası, adres bilgisi ve pandemi nedeniyle ücretsiz izin uygulanmasına dair bilgilerinin ilgili kişinin işvereni olan şirket tarafından kendilerine aktarıldığı,
- İlgili kişi ücretsiz izindeyken, izin süresinin uzatılması kararının kendisine ve onun gibi izinde olan diğer işçilere bildirilmesi için kendilerine telefonla ulaşılmaya çalışıldığı, ancak bu yolla ulaşılamayan işçilerin hem iş yerine gelmelerinde sağlık açısından sakınca bulunması hem de taraflarınca grup

şirketlerine sunulan personel izin takip hizmetleri dolayısıyla çalışana noter vasıtasıyla bildirim yapılmasının uygun olacağı düşüncesi ile taraflarının avukatına çalışanın ad ve soyadı, T.C. kimlik numarası, adres ve ücretsiz izin durumuna ilişkin bilgiler gönderilerek ücretsiz izin süresinin uzatıldığına ihtar edilmesinin istendiği,

- Bildirim yapılacak personel sayısının fazla olması sebebiyle, usul ekonomisi ve noterlikteki işlemlerin en uygun şekilde gerçekleştirilmesi adına avukatları tarafından vekâleten ihtarname düzenlenerek gönderildiği, noterlik nezdinde yapılan işlemlerde, sair bilgilerin ilgili noterliğe sağlanmasının Noterlik Kanunu ve ikincil mevzuattan kaynaklandığı, ihtarname keşide edilebilmesi için keşidecinin ve muhatabın/muhatapların ad ve soyadı ile T.C. kimlik numaralarının noterliğe sunulmasının, tebligatın sağlıklı yapılabilmesi için yine mevzuat gereğince zorunlu olduğu, bu nedenle birden çok muhatabın yer aldığı ihtarname içerisinde muhatabların bilgilerine yer verildiği ve ilgili kişisel verilerin noterlik ile paylaşıldığı,

- Yapılan bu işlemin meşru ve açık bir amaca dayalı olduğu, işleme amacı olan ücretsiz izin süresinin takibi ve çalışana bildirim yapılabilmesi amacı ile sınırlı olarak bahse konu verilerin işlendiği, aktarıldığı ve işlendikleri amaçla bağlantılı olmayan bir şekilde kullanılmadığı, veri işleme faaliyetinin ölçülü olduğu ve kişisel verilerin ihtarname keşide edilmesi için noterlik ile paylaşılmasının ilgili kişinin lehine ve izin durumunun bildirilmesine yönelik olduğu,

- İlgili kişiye ait kişisel verilerin, bordrolama destek hizmetleri çerçevesinde ilgili kişinin işvereni olan şirket tarafından kendilerine aktarıldığı ve bu aktarımın hukuki dayanağının 6698 sayılı Kişisel Verilerin Korunması Kanun'unun (Kanun) 5'inci maddesinin (2) numaralı fıkrasının (f) bendi olduğu ifade edilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulunun 07/04/2022 tarih ve 2022/328 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) "Genel İlkeler" başlıklı 4'üncü maddesinde, kişisel verilerin ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, buna göre, kişisel verilerin ancak; "a) Hukuka ve dürüstlük kurallarına uygun olma, b) Doğru ve gerektiğinde güncel olma, c) Belirli, açık ve meşru amaçlar için işlenme, ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ile d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" ilkelerine uygun olarak işlenebileceği,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi; fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin kendisi tarafından alenileştirilmiş olması; bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hükmünün yer aldığı,
- Kanun'un 12'nci maddesinin (1) numaralı fıkrası gereğince veri sorumlusunun; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğunun hükme bağlandığı,
- Diğer yandan 1512 sayılı Noterlik Kanunu'nun "Düzenleme Şeklinde Yapılması Zorunlu İşlemler" başlıklı 89'uncu maddesinde; "Niteliği bakımından tapuda işlem yapılmasını gerektiren sözleşme ve vekaletnamelerle, vasiyetname, mülkiyeti muhafaza kaydı ile satış, gayrimenkul satış va'di, vakıf senedi, evlenme mukavelesi, evlat edinme ve tanıma, mirasın taksimi sözleşmesi ve diğer kanunlarda öngörülen sair işlemler bu fasıl hükümlerine göre düzenlenir." hükmünün yer aldığı ve yine anılan Kanun'un "Onaylama" başlıklı üçüncü bölümünün "Şekil" başlığını taşıyan 90'ıncı maddesinin; "Hukuki işlemlerin altındaki imzanın onaylanması imzayı atan şahsa ait olduğunun bir şerhle belgelendirilmesi şeklinde yapılır. İmzası onaylanan iş kağıdının aslı ilgisine verilir ve imzalı bir örneği dairede saklanır. Bu örnek harca tabi değildir." hükmünü haiz olduğu,
- Somut olayda, veri sorumlusu tarafından ilgili kişinin ve diğer yedi çalışanın bilgilerine aynı ihtarnamede yer verildiğinin görüldüğü ve veri sorumlusu tarafından da bu durumun ikrar edildiği, Senetler düzenleme ve onaylama şeklinde hazırlanabilmekle birlikte söz konusu belgenin noterlik tarafından "onaylama" şeklinde gerçekleştirildiğinin görüldüğü ve ilgili kişinin kişisel verilerine ek olarak yedi çalışanın da kişisel verilerinin toplu bir şekilde aynı ihtarnamede yer almasından dolayı her birinin kişisel verilerinin birbirleriyle paylaşıldığının anlaşıldığı,

- İlgili kişinin ve diğer yedi çalışanın kimlik ve iletişim verisinin ihtarnamede yer alması suretiyle ilgili noterlikle paylaşılması Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (e) bendinde yer alan "bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" işleme şartı kapsamında yer almakla birlikte söz konusu çalışanların kimlik ve iletişim verisinin aynı ihtarnamede yer alması ve söz konusu ihtarname keşide edilirken herhangi bir şekilde karartma, muhataplara ayrı ayrı keşide etme vb. gibi bir işlem yapılmaması sebebiyle ilgili kişinin kişisel verilerinin diğer çalışanlarla paylaşıldığı ve bu suretle gerçekleşen kişisel veri işleme faaliyetinin Kanun'un 5'inci maddesinde yer alan kişisel veri işleme şartlarından herhangi birine dayanmadığı

değerlendirmelerinden hareketle;

- İlgili kişinin kişisel verilerinin yer aldığı ihtarnamenin veri sorumlusu tarafından yedi kişiye daha gönderildiği iddiasına ilişkin olarak; diğer yedi çalışanla birlikte ilgili kişinin kimlik ve iletişim verisinin aynı ihtarnamede yer alması ve söz konusu ihtarname keşide edilirken de herhangi bir şekilde karartma, muhataplara ayrı ayrı keşide etme vb. işlemin yapılmaması nedeniyle ilgili kişinin kişisel verilerinin diğer çalışanlarla paylaşıldığı, bu çerçevede Kanun'un 5'inci maddesinde yer alan herhangi bir işleme şartına dayanmaksızın gerçekleşen kişisel veri işleme faaliyetinin Kanun'un 12'nci maddesinin (1) numaralı fıkrası hükmüne aykırı olduğu değerlendirildiğinden veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL idari para cezası uygulanmasına,

- Diğer taraftan Karar hakkında Türkiye Noterler Birliğine bilgi verilmesine

karar verilmiştir.

2022/325 sayılı KVKK Kararı

İlgili kişi ile ilgisi bulunmayan bir işletme adına düzenlenmiş e-faturaların, ilgili kişinin e-posta adresine gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 07/04/2022 tarih ve 2022/325 sayılı Karar Özeti

Karar Tarihi : 07/04/2022

Karar No : 2022/325

Konu Özeti: İlgili kişi ile ilgisi bulunmayan bir işletme adına düzenlenmiş e-faturaların, ilgili kişinin e-posta adresine gönderilmesi

İlgili kişinin Kuruma intikal eden şikâyetinde özetle; bir pazarlama şirketinin Trabzon bölge müdürlüğü yetkilileri tarafından bir market adına düzenlenmiş e-faturaların ilgili kişinin kullanmakta olduğu e-posta adresine 13/01/2020 tarihinden 20/04/2020 tarihine kadar on beş kez gönderildiği, ilgili kişinin adına fatura düzenlenen market ile bir ilgisinin bulunmadığı, bu durum çeşitli iletişim kanalları üzerinden söz konusu şirkete bildirilmesine rağmen faturaların tarafına iletmeye devam ettiği belirtilerek gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde pazarlama şirketinden savunması istenilmiş olup alınan cevabi yazıda özetle;

- Faturaları gönderen yetkililerden birinin önceden şirketlerinin Trabzon eski baş bayisi olduğu ancak Kasım 2018 itibariyle ilişkilerinin kesildiği,
- İlgili kişinin başvurusunu yönelttiği e-posta adreslerinin bir kısmının domain'inin aktif olmadığı ve name server bilgilerinin şirketlerine ait olmadığı,
- Sistemlerinde ilgili kişinin e-posta adresine rastlanmadığı, bu nedenle herhangi bir ilişkileri bulunmayan işletme adına düzenlenen ve gerçek kişiye ait herhangi bir bilgi içermemesi nedeniyle kişisel veri ihlali teşkil etmeyecek fatura paylaşımının şirketleri tarafından gerçekleştirilmesinin mümkün olmadığı,

- Şirketlerinde herhangi bir üyelik sistemi bulunmadığından, doğrudan e-posta adresi ile başvuru yönteminin açık olmadığı ve ilgili kişi tarafından şirketlerine yapılan usulüne uygun bir başvuru tespit edilemediği

ifade edilmiştir.

Bahse konu cevabi yazının incelenmesinin ardından şirketin daha önce Trabzon baş bayisi olan fatura düzenleyen şahıstan şikâyet konusu olaya ilişkin savunması talep edilmiş olup bu kapsamda bahse konu şahıstan alınan cevabi yazıda özetle;

- Taraflarının adı geçen şirketin bayisi iken başka bir pazarlama şirketine devir teslim işlemi yapılmasının ardından yeni şirket ile bayilik sözleşmesi (yetkili satıcı) imzalandığı,
- E-fatura sistemine geçildiğinden dolayı, gazete dağıtımı yapan son satıcılardan e-posta ve telefon bilgilerinin güncellenmesinin talep edildiği, bunun üzerine bahsi geçen market tarafından güncellenmesi istenen e-posta adresinin taraflarına, ilgili kişinin adı ile soyadı arasına nokta konulmuş şekliyle (ad.soyad@... şeklinde) iletildiği,
- Ancak e-posta adresinin, el yazısıyla yazılarak taraflarına iletilmesi nedeniyle sistem üzerinde e-posta adresi kaydı yapılırken bahse konu adresin, ad ve soyadı arasına nokta işareti konulmadan (adsoyad@... şeklinde) kaydedildiği, söz konusu durumun tamamen yanlışlıkla meydana geldiği,

Şikâyet konusu olaya ilişkin olarak ilgili kişinin taraflarına ulaşmasının ardından sistemleri üzerinde düzeltme işlemi yapıldığı ve ilgili kişiye e-posta gitmesinin önlendiği

belirtilmiştir.

Bahse konu cevabi yazı incelendiğinde, son satıcı olan bayi bilgilerinin kaydedildiği sistemin yeni sözleşme imzalanan pazarlama şirketine ait olduğunun anlaşılması üzerine söz konusu şirketten de savunması istenilmiş olup alınan cevabi yazıda özetle;

- Şirketlerinin Türkiye'deki yazılı basın sektörünün tamamına hizmet vermek üzere Türkiye genelinde genel müdürlüğe bağlı bölge müdürlükleri ve bölge temsilcilikleri, bölge müdürlüklerine/temsilciliklerine bağlı yetkili satıcılar ile yetkili satıcılara bağlı son satıcılardan oluşan bir dağıtım ağı oluşturduğu,
- Şirketleri ile şikâyete konu fatura düzenleyen kişi arasında Temmuz 2018'de dağıtım yetkili satıcı sözleşmesi imzalandığı ve söz konusu kişinin yetkili satıcı olarak atandığı, adına fatura düzenlenen marketin ise söz konusu yetkili satıcının yayınlarının pazarlama, dağıtım ve satışını yaptığı son satıcılardan biri olduğu,

- Bu ilişkide şirketlerinin yayınları okuyuculara ulaştırılan son satıcılar ile herhangi bir sözleşmesel ilişki içerisinde girmediği ve son satıcılara yönelik herhangi bir dağıtım, pazarlama ve satış faaliyeti yürütülmediği, bu faaliyetlerin yürütülmesinin yetkili satıcıların uhdesine bırakıldığı,
- Atanan yetkili satıcılar tarafından yayınların Türkiye geneline dağıtımını, pazarlanması ve satış süreçlerinin sağlanması adına dağıtım bilgi sistemi (DBS) kullanıldığı, yetkili satıcıların DBS'ye tanımlanması ile erişim/kullanım hakkı tanındığı, yetkili satıcının yetkili olduğu il dahilinde yer alan son satıcıları kendi inisiyatifinde olmak üzere belirleyip anlaşma yaptığı ve son satıcılardan elde edilen bilgilerin DBS'ye girilmesi suretiyle son satıcı kayıtlarının yapıldığı,
- Yetkili satıcıların yalnızca kendileri tarafından kaydedilen bilgilere erişim imkânının bulunduğu, öte yandan son satıcıların DBS'ye herhangi bir erişiminin bulunmadığı,
- DBS'ye kaydedilen son satıcı bilgilerinin, şirketlerinden bağımsız bir şekilde ve herhangi bir emir veya talimat almadan ya da şirketleri tarafından herhangi bir yönlendirmede bulunulmadan elde edildiği,
- Yetkili satıcıların söz konusu veriler üzerinde tam bir hâkimiyete sahip oldukları, bu bilgileri kendi inisiyatif ve kararları doğrultusunda kendilerine ait süreçler/faaliyetler dahilinde belirledikleri amaçlar ile işledikleri, gerek gördüklerinde diledikleri gibi değiştirebildikleri ve silebildikleri,
- Şirketlerinin gerek DBS gerek başka bir vasıtayla yetkili satıcılara ve mevcut ya da potansiyel son satıcılara ilişkin herhangi bir bilgi toplamadığı ve aktarmadığı, dolayısıyla son satıcılara ait herhangi bir iletişim bilgisinin yetkili satıcılara sağlanması gibi bir uygulama bulunmadığı,
- DBS'ye girilen bilgilerin doğru, güncel ve eksiksiz olma sorumluluğunun son satıcılar ile doğrudan hukuki/ticari ilişki içerisinde bulunan yetkili satıcılara ait olduğu, zira DBS'ye şirket yetkilileri dışında yalnızca yetkili satıcıların doğrudan erişiminin olduğu ve DBS'nin sistem üzerinden son satıcılara ulaşılarak bilgi doğrulaması yapılmasına imkân sağlayacak bir alt yapıda kurulmadığı; ayrıca şirketlerinin yetkili satıcı sözleşmesi ile ilgili mevzuat hükümlerine uygun faaliyette bulunulması ve bu kapsamda gereken tedbirlerin alınması konusunda yetkili satıcılara sorumluluk yüklediği,
- DBS'nin, sunduğu raporlama imkânı ile yetkili satıcının planlama, dağıtım ve iade operasyonlarını yürütebilmesi bakımından kolaylık sağlandığı ancak yetkili satıcının doğrudan DBS üzerinden resmi bir irsaliye/fatura oluşturmasının mümkün olmadığı, DBS'nin irsaliye/faturaya konu satışın icmalini rapor olarak dökümünü ve resmi irsaliye/faturaya ticari içerik oluşturulmasını sağladığı, bu hususların DBS üzerinden yürütülmesi gibi bir zorunluluğun bulunmadığı,

- DBS üzerinden doğrudan son satıcılar ile iletişime geçilmesini sağlayan (e-mail gönderimi, fatura gönderimi, irsaliye gönderimi gibi) herhangi bir hizmetin de sunulmadığı, yine herhangi bir üçüncü parti yazılımı (e-fatura, e-arşiv sistemleri, CRM gibi) ile entegrasyonun da bulunmadığı,
- Şirketlerinin yetkili satıcıların son satıcılar nezdinde yapmış olduğu planlama, dağıtım ve iade operasyonlarını DBS üzerinden takip ettiği, bu operasyonlar dahilinde sisteme girilen satış bilgileri dikkate alınarak tiraj tahminlerini yaptığı, basım, üretim ve planlama süreçlerini yönettiği,
- Somut olayda da yetkili satıcının markete ilişkin kendi fatura süreçleri dahilinde ve veri sorumlusu olarak işlediği e-posta verisini yaptığı hata sonucu e-fatura hizmeti sistemine hatalı şekilde aktardığı, zira son satıcı bilgilerinin kaydedildiği DBS üzerinden yalnızca ön muhasebe işlemlerinin yapılabildiği, e-fatura işlemlerinin üçüncü taraflara ait sistemler üzerinden gerçekleştirildiği, e-posta adresinin DBS’de girilmesi zorunlu bir alan olmadığı, faturalama sistemine hatalı şekilde girilen kaydın, DBS’ye yapılan hatalı kayıttan ve DBS’nin tetiklediği herhangi bir gönderimden kaynaklanmadığı,
- Yetkili satıcının, yayınların son satıcılar nezdindeki planlama, dağıtım ve iade operasyonlarını yürütmesi kapsamındaki faturalama süreçlerinde ve dolayısıyla şikâyete konu olay özelinde e-posta verisinin işlenmesi faaliyeti bakımından şirketlerinden bağımsız şekilde ayrı bir veri sorumlusu sıfatı ile hareket ettiği, işlenecek kişisel veriler bakımından emir veya talimat almadığı, e-posta verisinin DBS dahilinde kaydedilmesi gereken zorunlu bir veri dahi olmadığı

ifade edilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulunun (Kurul) 07/04/2022 tarih ve 2022/325 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanun’unun (Kanun) “Tanımlar” başlıklı 3’üncü maddesinin (1) numaralı fıkrasının (ç) bendinde ilgili kişinin, “kişisel verisi işlenen gerçek kişi”, (d) bendinde kişisel verinin, “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi”, (e) bendinde kişisel verilerin işlenmesinin, “kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem”, (g) bendinde “veri işleyen”in veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi, (i) bendinde veri sorumlusunun, “kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt

sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi” olarak tanımlandığı,

- İlgili kişi, yetkili satıcının ilk sözleşme imzaladığı pazarlama şirketi hakkında Kurul’a şikâyette bulunmuş olmakla birlikte şikâyete konu faturayı düzenleyen kişi ile Kasım 2018 tarihi itibarıyla ilişkilerinin kesildiği ve fatura tarihinin Şubat 2020 olduğu göz önünde bulundurulduğunda söz konusu ilk sözleşme imzalanan pazarlama şirketinin veri sorumlusu sıfatını haiz olmadığı,

- İkinci sözleşme imzalanan pazarlama şirketi tarafından oluşturulan dağıtım ağında ilgili bölgelerde dağıtım, pazarlama ve satış hizmetlerinin sunulması adına aralarındaki sözleşme ile fatura gönderimi yapan kişinin yetkili satıcı olarak yetkilendirildiği, satıcının da bu yetkiye istinaden tüketiciye doğrudan satış ve pazarlama yapılması adına son satıcı olan market ile sözleşme kurduğunun anlaşıldığı,

- Yetkili satıcı sözleşmesi incelendiğinde yetkili satıcıların; son satıcıların açık isim ve adreslerinin yetkili satıcı dağıtım bilgi sistemine kaydedilmesi, son satıcılara teslim edilen ürünler için fatura düzenlenmesi ve tebliğ edilmesi, dağıtım, pazarlama ve bütün muhasebe işlemlerinde bilgisayar, modem vb. araçları ve ikinci pazarlama şirketinin gerekli gördüğü bilgisayar programlarının kullanılması ve bu bilgilerin tümünün şirketin kullanımına ve denetimine açık tutulması ile yükümlü olduğunun görüldüğü,

- Fatura işlemlerinin yetkili satıcı tarafından gerçekleştirildiği belirtilmekle birlikte söz konusu işlemlerin ikinci pazarlama şirketi ile yetkili satıcı aralarındaki sözleşmenin yerine getirilmesi amacıyla gerçekleştirildiği, DBS’ye hangi verilerin girişinin yapılacağına ikinci pazarlama şirketi tarafından karar verildiği, şirketin fatura düzenlenmesi ve tebliğ edilmesi sürecinde hangi teknik ve organizasyonel araçların kullanılacağını yetkili satıcının takdirine bırakmış olmasının yetkili satıcı bakımından ayrı bir veri sorumluluğu doğurmayacağı, yetkili satıcının fatura süreçleri kapsamında gerçekleştirdiği işlemlerde sözleşme maddelerinin dışına çıkarak kendi işleme amaçlarını belirlemediği dikkate alındığında ikinci pazarlama şirketinin veri sorumlusu, yetkili satıcının ise bu şirket adına veri işleyen olarak kişisel veri işlediğinin tespit edildiği,

- Son satıcılara yönelik bilgilerin kaydedildiği DBS’ye, veri işleyen tarafından hizmet verdikleri bir marketin e-posta adresinin, sehven ilgili kişinin e-posta adresi olarak kaydedildiği, bu sebeple son satıcı adına düzenlenen faturaların da ilgili kişiye gönderildiği ve bu hususta e-posta adresi düzeltilerek ilgili kişiye fatura gönderiminin durdurulduğunun anlaşıldığı,

- Bu çerçevede, veri işleyen tarafından ilgili kişinin e-posta adresinin sehven sisteme kaydedilmesi suretiyle herhangi bir kasıt bulunmaksızın işlendiği ve şikâyetle konu durumun düzeltildiği,
- Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına Kanuna aykırı şekilde gönderilen üçüncü kişilere ait kişisel veriler hakkında Kişisel Verileri Koruma Kurulunun 22/12/2020 tarih ve 2020/966 sayılı İlke Kararı kapsamında e-posta gönderilmesi hususunda gerekli teyit mekanizmalarının kurulmasının uygun olacağı değerlendirilmelerinden hareketle;
- Şikâyetle bulunulan ilk pazarlama şirketinin ilgili kişiye tarafı olmayan faturaların gönderilmesi faaliyetinde herhangi bir ilgisi ve sorumluluğunun bulunmadığı kanaatine varıldığından hakkında yapılacak bir işlem olmadığına,
- Son satıcı olan market sahibi ile ilgili kişinin e-posta adresi benzerliği sebebiyle veri işleyen yetkili satıcı tarafından sehven ilgili kişinin e-posta adresinin sisteme kayıt edilerek herhangi bir kasıt bulunmaksızın işlendiği ve ilgili kişinin faturaların tarafına gönderilmemesi yönündeki talebinin gerekli düzeltme yapılarak yerine getirildiği dikkate alındığında veri sorumlusu ikinci pazarlama şirketi hakkında Kanun kapsamında yapılacak bir işlem bulunmadığına,
- Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına Kanuna aykırı şekilde gönderilen üçüncü kişilere ait kişisel veriler hakkında Kişisel Verileri Koruma Kurulunun 22/12/2020 tarih ve 2020/966 sayılı İlke Kararı kapsamında e-posta gönderilmesi hususunda gerekli teyit mekanizmalarının kurulmasının uygun olacağına veri sorumlusu ikinci pazarlama şirketine hatırlatılmasına karar verilmiştir.

2022/277 sayılı KVKK Kararı

İlgili kişiye ait kişisel verileri içeren bir kargo paketinin üçüncü bir şahsın eline geçmesi hakkında Kişisel Verileri Koruma Kurulunun 24/03/2022 tarihli ve 2022/277 sayılı Karar Özeti

Karar Tarihi : 24/03/2022

Karar No : 2022/277

Konu Özeti: İlgili kişiye ait kişisel verileri içeren bir kargo paketinin üçüncü bir şahsın eline geçmesi

İlgili kişinin şikâyetinde özetle;

- İlgili kişinin kulaklığını onarım yapılması için bir elektronik perakende zincirinin AVM'deki şubesine teslim ettiği, mağaza yetkililerinin de kulaklığı distribütör firmaya iletmek üzere kargo şirketine teslim ettiği ama kargonun distribütör firma yerine konuyla ilgisiz üçüncü bir şahsa teslim edildiği, ilgili kişinin kargonun teslim edildiği üçüncü şahsın kendisine ulaşması üzerine konudan haberdar olduğu,
- Elektronik perakende zinciri yetkililerinin konu kapsamında herhangi bir suçlarının olmadığını ve hatanın tamamen kargo şirketinde olduğunu ileri sürdükleri, ancak taşınan kargonun içine ilgili kişiye ait isim, soy isim, cep telefonu numarası, e-posta adresi, ikamet ettiği il ve ilçe ile ödeme yaptığı kredi kartının ilk altı hanesi gibi bilgileri haiz belgelerin koyulduğu,
- Karşı tarafın art niyetli olması durumunda rahatça kötüye kullanılacak mezkûr bilgilerin konuyla ilgisiz üçüncü bir şahsın eline geçtiği, bu durumda ilgili kişinin maddi-manevi bir zarar görmemesinin tamamen o şahsın insaniyetine ve vicdanına kaldığı, elektronik perakende zinciri yetkililerinin bu durumun tamamen prosedür gereğince yapıldığını beyan ettikleri ve hatanın mesuliyetini kabul etmedikleri belirtilmiş ve konu hakkında 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gerekli işlemlerin yapılması talep edilmiştir.

İlgili kişinin şikâyetine istinaden başlatılan inceleme çerçevesinde veri sorumlusu sıfatını haiz olduğu anlaşılan elektronik perakende zincirinden savunması istenilmiş olup, verilen cevapta özetle;

- Şikâyete konu olayın, ilgili kişinin kulaklığını onarım yapılması için veri sorumlusunun bir AVM'deki şubesine teslim etmesi ve akabinde ürünün ilgili kişinin talebine uygun olarak onarım için veri sorumlusu tarafından distribütör firmaya kargo şirketi aracılığıyla gönderilmesi ile ilgili olduğu,
- Kargo içeriğinde, ürünün yanı sıra distribütör firma tarafından kulaklığın onarım işleminin yapılabilmesi için gerekli olan belgelerin bulunduğu,
- Kargonun söz konusu onarım işleminin yapılabilmesi için gerekli olan belgelerle birlikte distribütör firmaya gönderiminin sağlanması amacıyla alıcının adres bilgisi ve unvanı doğru bir şekilde girilerek kapalı ve paketlenmiş olarak kargo şirketine 31/08/2021 tarihinde teslim edildiği, bahsi geçen gönderime ilişkin doldurulan kargo formunun ve irsaliyenin görüntüsünün yazıları ekinde sunulduğu,
- Bununla birlikte, şikâyete konu kişisel verileri içeren paketin kargo şirketi tarafından veri sorumlusunun kargo üzerinde belirttiği adres dışında üçüncü bir kişiye/farklı bir adreste teslim edildiği, bu durumun kargo şirketinin hatalı teslimat yapması ve adreste bulunan kişinin kendisine ait olmayan hatalı gönderiyi kabul etmesi sebebiyle yaşandığı,
- Yaşanan hatalı teslimat durumundan ötürü taraflarının herhangi bir sorumluluğunun bulunmadığı, nitekim Kurumun Veri İşleyen ve Veri Sorumlusu Rehberinde de belirtildiği gibi kargo şirketlerinin sevkiyatı yönetmek için elde ettiği kişisel veriler bakımından 6698 sayılı Kanun uyarınca veri sorumlusu oldukları,
- Aynı doğrultuda, Kişisel Verileri Koruma Kurulunun (Kurul) 16/01/2020 tarihli ve 2020/32 sayılı Karar Özeti'nde de ifade edildiği üzere "Kurye'nin Karayolu Taşıma Yönetmeliği çerçevesinde gönderici ve alıcılara ilişkin ad ve soyad, unvan, gerçek kişilerde T.C. kimlik numarası bilgilerini tam ve doğru şekilde kaydetme yükümlülüğüne sahip olduğu, kurye firmalarının yükümlülükleri kapsamında sunacakları hizmeti tam ve doğru bir şekilde yerine getirmek amacı ile bu verileri kendi sistemlerine kaydetmekte olduğu, bu açıdan Kurye'nin bağlı olduğu mevzuat çerçevesinde işlediği kişisel veriler bağlamında veri sorumlusu olduğu"nun değerlendirildiği,
- İlgili kişinin kişisel verilerinin üçüncü bir kişinin eline geçmesinin kargo şirketinin teslimatı gönderim formunda veri sorumlusu tarafından alıcı olarak gösterilen tarafa yapmaması nedeniyle ortaya çıkan bir durum olduğu, yaşanan olayda taraflarının kişisel verilerin korunması mevzuatını ihlal edecek herhangi bir uygulamada ve işleme faaliyetinde bulunmadığı, dolayısıyla ilgili kişinin iddia ettiği gibi somut olayda gerçekleşen işleme faaliyetine ilişkin herhangi bir hukuka aykırılığın söz konusu olmadığı

ifade edilmiştir.

İlgili kişinin şikâyetinin ve veri sorumlusunun savunmasının Kurul tarafından değerlendirilmesi neticesinde; veri sorumlusu tarafından distribütör firmaya gönderilen kargo içerisinde yer alan ve ilgili kişinin bazı kişisel verilerini içeren belgelerin kargo şirketinin hatalı teslimat yapması nedeniyle gerçekleştiğinin beyan edildiği dikkate alınarak kargo şirketinin savunmasının alınması suretiyle incelemeye devam edilmesine karar verilmiştir.

Bu çerçevede, kargo şirketinin Kuruma ilettiği savunmasında özetle;

- Şikâyete konu ***** gönderi numaralı kargonun, taşınmasını gerçekleştirmek üzere taraflarına verildiğinin tespit edildiği, varış birimine ulaşan kargonun birim personeli tarafından 02/09/2021 tarihinde dağıtıma çıkarıldığı ve sehven üçüncü bir kişiye teslim edildiği, durumun kargonun teslim edildiği üçüncü kişinin bilgi vermesiyle anlaşıldığı,
- Kargo şirketinin akdettiği acentelik sözleşmesi ile taşımacılık faaliyeti kapsamında kendi nam ve hesabına taşıtların yükleme, boşaltma, gümrükleme ve pazarlama işlemleri ile diğer acentelik hizmetlerini acenteleri vasıtasıyla yürüttüğü, nitekim şikâyete konu gönderinin varış biriminin de acentesi olduğu ve olayın yaşandığı tarihte işlemi gerçekleştiren personelin söz konusu acentede istihdam edildiğinin tespit edildiği,
- Acentelik ilişkisine istinaden imzalanan acentelik sözleşmesinin ve güvenlik tedbirlerine ilişkin protokollerin yazıları ekinde, kargo şirketi tarafından kişisel verilerin korunmasına yönelik bilgilendirme ve aydınlatmaların yerine getirildiği,
- Teslime ilişkin bilginin alınmasıyla birlikte varış birimi/acente tarafından derhal teslim edilen adrese gidilerek kargonun alındığı ve aynı gün gönderici müşteri olan veri sorumlusuna iade edildiği, acentenin teslimatta görevli personelinin Eylül 2021'in sonlarında ayrıldığı bildirildiğinden teslimatın detayları hakkında bilgi temin edilemediği,
- Kargo şirketinin hizmetlerinin güvenliği konusunda oldukça hassas davrandığı ve insani bir hata olarak yapılan işlemle ilgili kasıtlı bir eyleminin söz konusu olmadığı, kargo dağıtım süreçlerindeki yoğunluk nedeniyle istemeden de olsa yaşanan bu gibi aksaklıkların önüne geçilebilmesi için personele gerekli bildirimlerin sıklıkla gerçekleştirildiği,
- Acentenin işlemi yapan personeli ile acente arasında akdedilen hizmet sözleşmesinde kişisel verilerin güvenliği, korunması ve gizlilik ile ilgili yükümlülükleri hakkında bilgilendirme yapılmakta olduğu,

- Tüm kargo şirketi çalışanlarına ve tedarikçi/acente çalışanlarına kişisel verilerin gizliliği ve bilgi güvenliği alanlarında hizmet öncesi eğitim verildiği, ilgili personele Nisan 2021 içerisinde toplam 32 saatlik hizmet öncesi eğitim, Mayıs 2021 ve Temmuz 2021 içerisinde iki kez olmak üzere birer saatlik Kişisel Verilerin Korunması ve Bilgi Güvenliği eğitimlerinin verildiği,
- Gönderi içeriği hakkında kargo şirketinin bilgisinin olup olmadığı sorusuna cevaben, gönderi içeriğinin kayıtlarda yer almadığı ve bu yüzden ilgili kişinin kişisel bilgilerinin gönderi içeriğinde bulunduğu dair taraflarının hiçbir bilgisinin bulunmadığı,
- Gönderici şirket tarafından ilgili kişiye ait kişisel bilgilerin prosedür gereği kargo içeriğine eklendiği beyan edilmekteyse de bu prosedürün dayanağının da açıklanması gerektiği, çünkü kargo içeriğinde bulunduğu belirtilen bilgilerin distribütör firma ile paylaşım yönteminin daha güvenli sistemler üzerinden iletililebilmesinin mümkün olduğu, gönderici şirketin kargonun kaybı veya zayıfatı risklerini basiretli bir tacir olarak öngörmesi ve önlemlerini almış olması gerektiği,
- Diğer taraftan kargonun sehven teslim edildiği ilgisiz üçüncü kişinin ise kendisine ait olmadığını bilmesine ve kargo paketinde alıcı olmadığını görmüş olmasına rağmen paketi hangi sebeple açtığına anlayamadığı, söz konusu şahsın kendisine ait olmadığını gördüğü anda kargo paketini açmadan tarafları ile ya da göndericiyle iletişime geçmiş olması durumunda bu olayın meydana gelmeyeceğinin açık olduğu,
- Bilgi güvenliği yönetimi, kişisel verilerin korunması ve ilgili yasal mevzuata uyum konularının ISO/IEC 27001 belgesine sahip olan kargo şirketinin öncelikle önem verdiği değer ve politikalar arasında olduğu, müşterilerin kişisel verilerinin korunmasına da bu kapsamda önem verildiği bildirilmiştir.

Tüm taraflarca dosyaya sunulan bilgi ve belgeler göz önünde bulundurularak konuya ilişkin yürütülen inceleme neticesinde, Kurulun 24/03/2022 tarihli ve 2022/277 sayılı Kararı ile;

- Kanun'un 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, "belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza", (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü

işlem”, (g) bendinde “veri işleyen”in veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi, (ı) bendinde veri sorumlusunun, “kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi” olarak tanımlandığı,

- Kanun’un “Kişisel Verilerin İşlenme Şartları” başlıklı 5’inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi; fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin kendisi tarafından alenileştirilmiş olması; bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hükmünün yer aldığı,

- Kanun’un “Kişisel Verilerin Aktarılması” başlıklı 8’inci maddesinde ise “(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz. (2) Kişisel veriler; a) 5 inci maddenin ikinci fıkrasında, b) Yeterli önlemler alınmak kaydıyla 6’ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir. (3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.” hükmüne yer verildiği

Bu çerçevede;

İlgili kişinin kargo paketi içerisine konulan belgelerde yer alan bilgilerinin ve distribütör firmaya gönderim de dâhil olmak üzere bu bilgilere ilişkin olarak veri sorumlusu tarafından yürütülen faaliyetlerin Kanun hükümleri karşısındaki durumu:

- Somut olayda, ilgili kişiye ait kulaklığın distribütör firma tarafından onarılabilmesi için kargo paketi içine konuldukları ifade edilen ve ilgili kişiye ait bazı kişisel verileri içeren belgelerin veri sorumlusu tarafından distribütör firmaya gönderilmesinden ibaret olan kişisel veri işleme/aktarım faaliyetinin Kanun’un 8’inci maddesinin (2) numaralı fıkrasının (a) bendi dikkate alınarak Kanun’un 5’inci maddesinde düzenlenen herhangi bir veri işleme şartına dayanıp dayanmadığı incelendiğinde; anılan kişisel veri işleme faaliyetinin Kanun’un 5’inci maddesinin (2) numaralı fıkrasının (c) bendinde düzenlenen “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla,

sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” ve (ç) bendinde düzenlenen “Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması” hukuki şartlarına dayandığı,

- Öte yandan veri sorumlusunca bir onarım işleminin yapılabilmesi için distribütör firmaya gönderilen belgelerde yer alan ilgili kişiye ait kişisel verilerin mahiyetleri ile ticari hayatın dinamik yapısı ve şartları dikkate alındığında hayatın olağan akışına uygun olduğunun rahatlıkla savunulabileceği düşünülen söz konusu kişisel veri işleme/aktarım faaliyeti bakımından Kanun’un 4’üncü maddesinde belirtilen genel ilkelere açık bir aykırılığın tespit edilemediği, bununla beraber gelecekte ürün onarımı amacıyla veri sorumlusu tarafından onarım firmalarına iletilebilecek kargo paketleri içindeki formlarda minimum düzeyde kişisel veri paylaşılmasını ve paylaşılan kişisel verilerin de mümkün olduğunca maskelenmesini teminen gerekli önlemlerin alınması gerektiği,

- İlgili kişinin bazı kişisel verilerini içeren belgelerin veri sorumlusu tarafından bir onarım işleminin yapılabilmesi için distribütör firmaya gönderilmesinden ibaret olan kişisel veri işleme/aktarım faaliyetine dayanan ve ilgili kişinin şikâyetine esas olan olay veri sorumlusunun Kanun’un 12’nci maddesinin (1) numaralı fıkrasından kaynaklanan yükümlülüğü kapsamında ele alındığında ise; veri sorumlusunun ilgili kişinin kişisel verilerini içeren kargo paketini “göndericisi veri sorumlusu, alıcısı ise distribütör firma” olacak şekilde kargo şirketine teslim etmiş olmasından dolayı Kanun’un 12’nci maddesinin (1) numaralı fıkrasına aykırı herhangi bir eyleminin mevcut olmadığı,

- Veri sorumlusu tarafından ilgili kişiye ait kulaklığın ve ilgili kişinin bazı kişisel verilerini içeren belgelerin distribütör firmaya gönderilmesinin amaçlandığı kargo gönderim işlemi kapsamında gerçekleşen hatalı teslimat işleminden haberdar olan veri sorumlusunun Kanun’un 12’nci maddesinin (5) numaralı fıkrasından kaynaklanan bildirim yükümlülüğü:

- Taraflarca dosyaya sunulan bilgi ve belgelerin incelenmesinden “somut olayda ilgili kişiye ait bazı kişisel verilerin hatalı kargo teslimatı yapılmış olması nedeniyle üçüncü bir şahısca elde edilmesinin ilgili kişi tarafından veri sorumlusundan önce öğrenilmiş olmasının kuvvetle muhtemel olduğu, durumu öğrenmesinden sonra ilgili kişinin veri sorumlusuna bir başvuru yaptığı, anılan başvuruyu takiben veri sorumlusunca ilgili kişiye hatalı kargo teslimat işlemi hakkında bilgi verildiği, ardından ilgili kişinin Kanun’un 14’üncü maddesine istinaden Kurula bir şikâyet ilettiği, söz konusu şikâyetin olayın ilgili kişi tarafından öğrenilmesinin üzerinden takriben 74 saat geçmişken Kurumun elektronik şikâyet sistemine intikal ettirilmiş olduğu ve konuya ilişkin şikâyetin ilgili kişi tarafından Kurumun elektronik şikâyet sistemine intikal ettirildiği an itibarıyla veri sorumlusunun olayı öğrenmesinin üzerinden henüz 72 saatin bile geçmemiş olabileceği” hususlarının anlaşıldığı,

Kanun'un "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12'nci maddesinin (5) numaralı fıkrasında "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." şeklinde hükme yer verildiği,

- Kurumun resmî internet sitesinde yayımlanan "Kişisel Veri İhlali Bildirim Usul Ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararına İlişkin Duyuru" başlıklı Kamuoyu Duyurusu'nda ise "(...) Veri ihlal bildirimlerinde, Kurula ve ihlalden etkilenmiş kişilere bildirim yapılmasındaki amacın, ihlal nedeniyle bu kişiler hakkında ortaya çıkabilecek olumsuz sonuçların bir an önce önüne geçilmesi veya en aza indirilmesine imkan verecek önlemler alınmasını sağlamak olduğu, öte yandan 6698 sayılı Kanuna kaynak teşkil eden Avrupa Birliğinin 95/46/EC sayılı Direktifini ilga eden Avrupa Genel Veri Koruma Tüzüğünde de veri ihlal bildirimlerine ilişkin olarak Direktifin aksine detaylı düzenlemelere yer verildiği dikkate alındığında (...)" ifadelerine yer verildiği ve Kanun'un 12'nci maddesinin (5) numaralı fıkrasında geçen "en kısa sürede" ibaresinin "72 saat" olarak yorumlanacağı, bu kapsamda veri sorumlusunun ihlal durumunu öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirimde bulunması gerektiğinin bildirildiği,
- Somut olayda ilgili kişinin bazı kişisel verilerini içeren belgelerin veri sorumlusu tarafından bir onarım işleminin yapılabilmesi için distribütör firmaya gönderilmesinde herhangi bir hukuka aykırılığın bulunmadığı sonucuna ulaşılmış olsa da; kargo paketinin kargo şirketi tarafından hatalı bir şekilde teslim edilmiş olmasından dolayı ilgili kişinin kişisel verilerinin kanuni olmayan bir şekilde üçüncü bir şahıs tarafından elde edildiğini öğrenmesini müteakip veri sorumlusunun Kanun'un 12'nci maddesinin (5) numaralı fıkrası uyarınca konu hakkında ilgili kişiye ve Kurula bildirimde bulunma yükümlülüğünün doğduğu,
- Ancak dosya kapsamındaki olgulara ilişkin yapılan tespit ve değerlendirmeler dikkate alındığında; ilgili kişinin şikâyetine esas olan ve ilgili kişinin dışında "ilgili kişi" sıfatını haiz olabilecek başka bir kişiyi doğrudan etkileme ihtimali de bulunmayan olay hakkında –ilgili kişinin başvurusuna cevaben da olsa- Kanun'un 12'nci maddesinin (5) numaralı fıkrası uyarınca en kısa sürede ilgili kişiye bildirimde bulunduğu kabul edilebilecek olan ama Kurula herhangi bir bildirimde bulunmadığı anlaşılan veri sorumlusunca, Kurula bir veri ihlal bildiriminde bulunulmuş olsaydı hatalı kargo teslimat işlemi sebebiyle ilgili kişi hakkında ortaya çıkabilecek olumsuz sonuçların bir an önce önüne geçilmesine veya en aza indirilmesine imkân verecek ve ilgili kişi tarafından Kurulun yönlendirmesi

olmadan düşünülemez ilave herhangi bir önlemin alınıp alınmayacağı konusunda bir çıkarımda bulunulmasının güç olduğu,

- Kanun'un 12'nci maddesinin (5) numaralı fıkrasında düzenlenen veri ihlal bildirimleri kapsamında Kurula ve ihlalden etkilenmiş kişilere bildirim yapılmasındaki amacın, ihlal nedeniyle bu kişiler hakkında ortaya çıkabilecek olumsuz sonuçların bir an önce önüne geçilmesine veya en aza indirilmesine imkân verecek önlemler alınmasını sağlamak olduğu, bununla birlikte mezkûr hükmün bir şekilde meydana gelmiş olsalar da ortaya çıkan her türlü veri ihlali vesilesiyle veri sorumlularını mutlak surette cezalandırmak olamayacağı", "somut olayda ilgili kişinin kişisel verilerinin kanuni olmayan bir şekilde üçüncü bir şahıs tarafından elde edildiğini öğrenmesinin üzerinden ortalama 72 saat geçmemişken –ilgili kişi tarafından yapılan başvuruya cevaben de olsa- ilgili kişiye bilgi verildiği", "yaşanan hatalı kargo teslimatından ilgili kişi dışında herhangi bir kişinin etkilenme ihtimalinin bulunmadığı", "olay sebebiyle ilgili kişi hakkında ortaya çıkabilecek olumsuz sonuçların bir an önce önüne geçilmesi veya en aza indirilmesine imkân verecek ve ilgili kişi tarafından Kurulun yönlendirmesi olmaksızın düşünülemez ilave bir önlemin bulunup bulunmadığı konusunun tartışmalı olduğu" ve "konu hakkında veri sorumlusunca Kurula bildirim yapılmamış olmasının ilgili kişinin kişisel verilerinin korunması bağlamında somut nitelikte bir tehlikeye yol açmayabileceği" hususları göz önünde bulundurulduğunda; gelecekte yaşanabilecek benzer olaylar için Kanun'un 12'nci maddesinin (5) numaralı fıkrası uyarınca ilgisine ve Kurula bildirimde bulunması konusunda veri sorumlusunun talimatlandırılmasının uygun olacağı,

- Veri sorumlusu tarafından ilgili kişiye ait kişisel verileri içeren belgelerin de distribütör firmaya gönderilmesinin amaçlandığı ama hatalı teslimatla sonuçlanan kargo gönderim işlemi kapsamında kargo şirketinin rolü ve yükümlülüklerinin Kanun hükümleri karşısındaki durumu:

- Somut olayda kargo şirketinin bahsi geçen kargo gönderim işlemindeki rolünün de Kanun hükümleri dikkate alınarak incelenmesinin gerektiği, kargo şirketinin ilgili kişinin şikâyetine esas kargo gönderim işlemi kapsamında Kanun'un 3'üncü maddesindeki tanımlar uyarınca "veri sorumlusu" veya "veri işleyen" sıfatını haiz olduğu bir senaryoda Kanun'dan kaynaklanan belli yükümlülüklerinin de gündeme gelebileceğinin açık olduğu,

- Gerek ilgili kişi ve veri sorumlusunca gerekse de kargo şirketi tarafından dosyaya sunulan bilgi ve belgelerden; şikâyete esas kargo gönderim işleminde tüzel kişiliği haiz veri sorumlusunun "gönderici" sıfatını, tüzel kişiliği haiz distribütör firmanın ise "alıcı" sıfatını haiz olduğu ve ilgili kişinin kargo gönderiminin tarafı olmadığı, buradan da somut olay özelinde kargo içeriğini

bilmesinin kendisinden beklenmeyen kargo şirketinin ilgili kişi hakkında veri sorumlusu veya veri işleyen sıfatıyla yürüttüğü herhangi bir kişisel veri işleme faaliyetinin bulunmadığı,

- Dolayısıyla Kanun'un "Kapsam" başlıklı 2'nci maddesindeki "Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır." hükmüne istinaden somut olaydaki kargo gönderim işlemi özelinde ilgili kişi hakkında doğrudan bir kişisel veri işleme faaliyeti yürütmediği anlaşılan kargo şirketi hakkında Kanun hükümleri uyarınca yapılabilecek herhangi bir işlemin bulunmadığı, zira Kurumun resmî internet sitesinde yayımlanan "Veri Sorumlusu ve Veri İşleyen" başlıklı Rehber'in "Örnekler: Kargo Firmaları" başlıklı alt bölümünde yer alan "Bir kargo firması, bir banka ile müşterilerin kredi kartlarını ilgisine ulaştırma hizmetini vermek üzere bir sözleşme yapmıştır. Kargo firması gönderenin adı, soyadı, alıcının adresi gibi sevkiyatı yönetmek için elde ettiği veriler bakımından veri sorumlusudur. Ancak, kargo firması her ne kadar kredi kartlarını fiziksel olarak elinde bulundursa da, söz konusu kredi kartı ile ilgili bilgilere ulaşması mümkün değildir. Bu durumda, dağıtım hizmeti sunucusu olarak hizmet veren kargo firması ne veri sorumlusu, ne de veri işleyen statüsündedir. Dolayısıyla, yalnızca taşıdığı fiziksel eşyanın güvenliğini sağlamakla yükümlü olup, kişisel verilerin işlenmesiyle ilgili uyması gereken herhangi bir yükümlülük yoktur." açıklamalarının da kargo içeriğine hâkim olması kendisinden beklenemeyecek kargo şirketlerinin kargo içeriği açısından veri sorumlusu veya veri işleyen sıfatlarını haiz olmayacağı ve bu yüzden de Kanun'dan kaynaklanan bir yükümlülüklerinin bulunmayacağı hususlarını teyit ettiği,

- Veri sorumlusu tarafından ilgili kişiye ait kulaklığın ve ilgili kişinin bazı kişisel verilerini içeren belgelerin distribütör firmaya gönderilmesinin amaçlandığı kargo gönderim işlemi kapsamında gerçekleşen hatalı teslimat işleminden sonradan haberdar olmuş olabilecek kargo şirketinin Kanun'un 12'nci maddesinin (5) numaralı fıkrasından kaynaklanan herhangi bir bildirim yükümlülüğünün de bulunmadığı, zira somut olayda Kanun'un 3'üncü maddesinde tanımlanan sıfatlardan herhangi birini haiz olmadığı,

değerlendirmelerinden hareketle;

- İlgili kişiye ait bazı kişisel verileri içeren belgelerin veri sorumlusunca bir onarım işleminin yapılabilmesi için distribütör firmaya gönderilmesinden ibaret olan kişisel veri işleme/aktarım faaliyetinin hukuka uygun olduğu dikkate alındığında, anılan faaliyetten ötürü veri sorumlusu hakkında Kurul tarafından Kanun kapsamında yapılacak herhangi bir işlemin bulunmadığına,

Somut olayda veri sorumlusunca bir onarım işleminin yapılabilmesi için distribütör firmaya gönderilen belgelerde yer alan ilgili kişiye ait kişisel verilerin mahiyetleri göz önünde bulundurularak veri sorumlusu hakkında Kanun kapsamında herhangi bir işlem tesis edilmesine gerek görülmemiş olsa da gelecekte onarım amacıyla veri sorumlusu tarafından onarım firmalarına iletilebilecek kargo paketleri içindeki formlarda minimum düzeyde kişisel veri paylaşılması ve paylaşılan kişisel verilerin de mümkün olduğunca maskelenmesini teminen gerekli önlemlerin alınması hususunda veri sorumlusunun uyarılmasına,

- Somut olayda veri sorumlusu tarafından ilgili kişiye ait kulaklığın onarımı için distribütör firmaya gönderilen ve ilgili kişiye ait bazı kişisel verileri içeren belgelerin de koyulduğu kargo paketinin kargo şirketinin hatasıyla konudan bağımsız üçüncü bir şahsa teslim edilmesi neticesinde ilgili kişinin kargo paketi içerisindeki kişisel verilerinin kanuni olmayan bir yolla konudan bağımsız üçüncü bir kişi tarafından elde edilmiş olduğu anlaşılmakla birlikte, olayın tüm şartları ve Kanun'un 12'nci maddesinin (5) numaralı fıkrasının amacı gözetildiğinde, ayrıca konuya ilişkin ilgili kişinin bilgisi olduğu dikkate alındığında; veri sorumlusu hakkında Kanun hükümleri dâhilinde yapılacak herhangi bir işlemin bulunmadığına, ancak gelecekte yaşanabilecek benzer olaylar için Kanun'un 12'nci maddesinin (5) numaralı fıkrası uyarınca en kısa sürede hem ilgisine hem de Kurula bildirimde bulunması konusunda veri sorumlusunun talimatlandırılmasına,

- İlgili kişinin şikâyetine esas olaylar ve bu olaylardaki rolü ile Kanun'un "Kapsam" başlıklı 2'nci maddesi dikkate alındığında, kargo içeriğine hâkim olması kendisinden beklenemeyecek kargo şirketinin kargo içeriği açısından veri sorumlusu veya veri işleyen sıfatlarını haiz olmayacağı ve bu yüzden somut olayda Kanun hükümlerine istinaden herhangi bir sorumluluğunun bulunmadığı anlaşılan kargo şirketi hakkında Kurul tarafından yapılacak herhangi bir işlemin bulunmadığına,

- Bunlarla birlikte, somut olayda ilgili kişinin hak mağduriyeti yaşamasına neden olabilecek hatalı bir kargo teslim işleminin bulunduğu göz önüne alındığında, anılan hatalı işlemde kaynaklanabilecek hukuki ve/veya cezai sorumluluğun takibi için yargı mercileri nezdinde girişimde bulunabileceği hususunda ilgili kişinin bilgilendirilmesine

karar verilmiştir.

2022/249 sayılı KVKK Kararı

Bir teknoloji řirketi tarafından ilgili kiřinin kiřisel verilerinin açık rızası olmaksızın yurt dışına aktarılması hakkında Kiřisel Verileri Koruma Kurulunun 17/03/2022 tarihli ve 2022/249 sayılı Karar Özeti

Karar Tarihi : 17/03/2022

Karar No : 2022/249

Konu Özeti: Bir teknoloji řirketi tarafından ilgili kiřinin kiřisel verilerinin açık rızası olmaksızın yurt dışına aktarılması

Kuruma iletilen řikayet dilekçesinde özetle; ilgili kiřinin veri sorumlusunun sistemine internet sitesi üzerinden üye olduđu, internet sitesinde çerez politikasının yer almadığı, aydınlatma metninde yurt dışına aktarım yapıldığının bildirildiği ancak ilgili kiřinin bu yönde bir açık rızasının olmadığı, bunun üzerine konuya ilişkin internet sitesinde yer alan aydınlatma metnindeki e-posta adresine başvuruda bulunduđu, bu başvuruda ilgili kiřinin hangi verilerinin kaydedildiği ve aktarıldığı hususlarında bilgi talep edilmişse de yasal süre olan 30 gün içerisinde veri sorumlusundan bir cevap alınmadığı ifade edilerek veri sorumlusu hakkında 6698 sayılı Kiřisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- Veri sorumlusunun, ilgili kiři başvurularına özgülediği bir e-posta adresi oluşturduđu, ancak bu e-posta adresine gönderilen ilgili kiři başvurusunun sehven gözden kaçırılması sebebiyle yanıtız kaldığı,
- Veri sorumlusunun internet sitesinde, gerek ilgili kiřinin başvuru tarihinde bulunan aydınlatma metninde gerekse de hali hazırda yürütölen KVKK Uyum Projesi kapsamında güncellenen aydınlatma metninde çerezler vasıtası ile işlenen kiřisel verilere ilişkin bilgilerin belirtildiği, konu ile ilgili aydınlatmanın 6698 Kanun'un 10'uncu maddesi kapsamında gerçekleştirildiği,
- Veri sorumlusunun İngiltere, Polonya, Çek Cumhuriyeti, Macaristan, Romanya, Suudi Arabistan, Mısır ve Türkiye'de hizmet vermekte olduđu, çok sayıda ölkede milyonlarca kullanıcının

menfaatlerinin en güvenli şekilde karşılanabilmesi için, veri sorumlusunun hizmetlerini yurt dışında bulunan bulut servis teknolojileriyle sağladığı, internet sitesinde bulunan aydınlatma metninde yer alan yurt dışına aktarım bildiriminin verilerin bu sunucuda tutulması sebebiyle gerçekleştirildiği, sistemlerinin Kanun ve Avrupa Veri Koruma Tüzüğü (GDPR) düzenlemelerinin yürürlüğe girmesinden önce bu mimari üzerinde geliştirilmeye başlandığı, anılan kanunlar ve kişisel verilerin korunmasına ilişkin mevzuatın yürürlüğe girmesi akabinde de KVKK ve GDPR ile uyumlu hale getirilmek üzere titizlikle yapılan çalışmaların devam ettirildiği,

- Günümüzde çok sayıda ülkede ve tüketiciye hizmet veren teknoloji girişimlerinin ihtiyaçları bağlamında Türkiye'de bulunan barındırma hizmetlerinin yetersiz olduğu, Türkiye'deki barındırma hizmetlerinde ihtiyaç duyulan modern altyapı teknolojilerinin büyük çoğunluğunun bulunmadığı, bulunan teknolojilerin de kapasite, güvenlik ve özellik olarak birçok eksikliğin olduğu, buna karşın yurtdışında bulunan söz konusu hizmet sağlayıcının altyapı teknolojilerine çok daha fazla yatırım yapma kapasitesinin olduğu, Türkiye'de bulunan bağımsız sunucu barındırma şirketlerinin benzer bir yatırım yapma kapasitesi olmadığı için altyapı teknolojilerinin avantajlı hale getirilmesinin son derece güç olduğu, bu sebeple Türkiye'de operasyonu bulunan birçok teknoloji şirketinin de kendilerinin çalıştığı şirketten hizmet aldığı,

- Veri sorumlusunun çok sayıda ülkede, çok sayıda tüketiciye hizmet sağlayabilmek için geliştirdiği teknolojilerin, kullandığı bulut servis sağlayıcının sunduğu altyapı teknolojilerinin üzerine inşa edildiği, veri sorumlusunun bu barındırma hizmetini tercih etmesindeki temel sebebin tüketicilerinin menfaatini üstün tutmak olduğu, siber saldırılar karşısında dahi tüketicilere kesintisiz hizmet verebildiği ve tüketicilerin verilerinin gizlilik ve güvenliğini bu saldırılara karşı koruyabildiği, veri sorumlusunun iş modeli çerçevesinde tüketicilerin ihtiyaçlarını karşılayabilmesinin de ancak bu firmanın sağladığı yenilikçi yapay zeka ve veri aktarımı teknolojileri sayesinde mümkün olabildiği, tüm sermayeleri ile Türkiye merkezli olarak kalmaya devam edebilmesi açısından yurt dışında bulunan servis veya muadillerini kullanmasının gerekli olduğu,

- Veri sorumlusunun barındırma hizmeti aldığı firma ile Kanun'un 9'uncu maddesinin (2) numaralı fıkrasının (b) bendi kapsamında bir taahhütname çalışmasını uzun zamandır sürdürmekte olduğu, söz konusu taahhütnameyi de en kısa sürede Kurulun onayına sunacağı

ifade edilmiştir.

Konuya ilişkin olarak yapılan incelemede Kişisel Verileri Koruma Kurulunun 17/03/2022 tarihli ve 2022/249 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, "belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza", (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (i) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi" olarak tanımlandığı,
- Şikâyet dilekçesinde veri sorumlusunun internet sitesinde gizlilik politikasının bulunmadığının belirtildiği, ancak veri sorumlularının Kanun'un 10'uncu maddesi kapsamında aydınlatma yükümlülüğünü yerine getirmekle yükümlü oldukları, her ne kadar uygulamada veri sorumluları tarafından gizlilik politikası adı altında belgeler hazırlanıp ilgili kişilerin dikkatine sunuluyor olsa da Kanun'da ve ilgili diğer mevzuatta veri sorumluları tarafından gizlilik politikası hazırlanmasına dair bir yükümlülüğün yer almadığı, ilgili kişilerin kişisel verilerinin işlenmesiyle ilgili bilgilendirilmesi hususunda veri sorumlularının asli sorumluluğunun; kişisel verilerin ilgili kişiden elde edildiği durumlarda kural olarak kişisel veri işleme faaliyetinden önce aydınlatma yükümlülüğünün yerine getirilmesi olduğu,
- İlgili kişinin Kanun'un 13'üncü maddesi kapsamında veri sorumlusuna yaptığı başvurunun sehven gözden kaçırıldığı dikkate alındığında, Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in 6'ncı maddesinin (1) numaralı fıkrasında düzenlendiği üzere, veri sorumlusu tarafından ilgili kişilerce yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirlerin alınmadığı kanaatine varıldığı,
- Yurt dışına aktarım iddialarıyla ilgili veri sorumlusu cevap yazısında özetle, barındırma hizmeti kullanımı dolayısıyla yurt dışındaki sunucularda verilerin saklandığı ve benzer güvenlik önlemlerini sunan bir mekanizmanın ülke içinde bulunmadığı gerekçesiyle böyle bir uygulamanın yapılmakta olduğunun belirtildiği, öncelikle kişisel verilerin yurt dışına aktarılmasının, Kanun'un 3 üncü maddesinde yer verilen "kişisel verilerin işlenmesi" tanımında da açıkça belirtildiği üzere bir işleme faaliyeti olduğu, diğer bir ifade ile kişisel verilerin yurt dışına aktarılmasının değiştirme, yeniden

düzenleme, kaydetme, depolama ve muhafaza etme gibi diğer kişisel veri işleme faaliyetlerinden bir farkı bulunmadığı,

- Kanun'un "Kişisel verilerin yurt dışına aktarılması" başlıklı 9'uncu maddesinin; (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamayacağını hükme bağlandığı, (2) numaralı fıkrasında ise Kanun'un 5'inci maddesinin (2) numaralı fıkrası ile özel nitelikli kişisel veriler bakımından 6'ncı maddesinin (3) numaralı fıkrasında belirtilen şartlardan birinin varlığı ve bu şartla birlikte, kişisel verinin aktarılacağı yabancı ülkede yeterli korumanın bulunması veya yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması hallerinde ilgili kişinin açık rızası aranmaksızın kişisel verilerin yurt dışına aktarılabilmesinin hükme bağlandığı,

- Kişisel verilerin yurt dışına aktarımının ayrı bir hükümde düzenlenmiş olmasının ve kişisel veri işleme şartlarından birinin varlığına ek olarak diğer bazı şartların aranmasının sebebinin ilgili kişinin kişisel verilerinin aktarıldığı ülkede de etkin olarak korunabilmesini sağlamak olduğu, bu düzenlemeyle yurt dışına aktarılmış kişisel verilerle ilgili olarak, ilgili kişinin sahip olduğu hakları etkin bir şekilde ve Kanun'un uygulamasına mümkün olabilecek en yakın seviyede kullanabilmesi ile aktarım yapılacak tarafın başta veri güvenliği olmak üzere ilgili kişiyi korumaya yönelik güvencelerin sağlanması hususunda yükümlü kılınmasının amaçlandığı,

- Kanunun 9'uncu maddesinin (3) numaralı fıkrası uyarınca yeterli korumanın bulunduğu ülkelerin ise henüz Kurul tarafından belirlenmediği, diğer taraftan, Kurulun yeterli koruma bulunmayan ülkelere yapılacak aktarımlarda yeterli korumayı taahhüt etme yollarını öngördüğü, bu kapsamda, veri sorumlusundan veri sorumlusuna ve veri sorumlusundan veri işleyene aktarımlarda kullanılmak üzere asgari şartları içerir iki adet taahhütname metni ve çok uluslu grup şirketleri arasında yapılacak aktarımlarda kullanılacak Bağlayıcı Şirket Kurallarına ilişkin başvuru formu ile Bağlayıcı Şirket Kurallarında bulunması gereken temel hususlara ilişkin yardımcı doküman hazırlanarak ilgililerin kullanımına sunulduğu, ayrıca, Kurulun yerleşik uygulamalarında da kişisel verilerin, dünyanın çeşitli yerlerinde bulunan veri merkezlerinde tutulmasının yurt dışına aktarım niteliğinde olduğuna ve sunucuları yurt dışında bulunan veri sorumlularından/veri işleyenlerden temin edilen saklama hizmetleri kapsamındaki kişisel veri işleme faaliyetlerinin de Kanun'un 9 uncu maddesine uygun olarak yerine getirilmesi gerektiğine karar verdiği,

- Veri sorumlusunun, Kurul tarafından onaylanmış taahhütname başvurusu bulunmamakla birlikte Kanun kapsamında yurt dışına aktarım faaliyetinin hukuka uygun olabilmesi için açık rızadan başka

bir hukuki sebep bulunmadığı, veri sorumlusu tarafından somut olayda yurt dışına aktarım faaliyeti kapsamında ilgili kişilerden belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan açık rıza alınması yoluna da başvurulmadığı

değerlendirmelerinden hareketle;

- Veri sorumlusu tarafından sunucuları yurt dışında bulunan sistemin kullanılması aracılığıyla kişisel verilerin yurt dışına aktarılması faaliyetinin gerçekleştirildiği, söz konusu faaliyet gerçekleştirilmeden önce aktarım yapılacak ülkede yeterli korumanın sağlanacağına ilişkin bir taahhütnamenin Kurula sunulmadığı, yurt dışına aktarım faaliyeti bakımından somut olayda açık rıza dışında bir hukuki sebep bulunmadığı, veri sorumlusu tarafından bu hususta ilgili kişilerden de açık rıza alınmadığı anlaşıldığından Kanun'un 12'nci maddesinin (1) numaralı fıkrası kapsamında uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirlerin alınmadığı kanaatine varılması sebebiyle, veri sorumlusu şirketin birçok ülkede faaliyet gösterdiği ve ekonomik durumu, kişisel verilerin işlenmesinde kullanılan uygulama ve internet sitesi aracılığıyla toplanan çok sayıda kişisel verinin hukuka aykırı olarak yurt dışına aktarıldığı, söz konusu fiilden etkilenen ilgili kişilerin fazla olduğu, yurt dışına kişisel veri aktarma fiilinin münferit bir olaydan kaynaklı olarak değil sistemli bir şekilde veri sorumlusu tarafından kasten ve icrai hareketle yapıldığının savunma dilekçesinde ikrar edildiği, kabahat teşkil eden ihlalin ticari amaç kapsamında gerçekleştirildiği ve 6698 sayılı Kanun'un yürürlüğe girdiği tarihin üzerinden 6 sene geçmiş olmasına rağmen yurt dışına aktarım faaliyetinin Kanun'a uygun hale getirilmemiş olduğu dikkate alınarak, veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 950.000 TL idari para cezası uygulanmasına,

- Kişisel verilerin yurt dışına aktarılmasına ilişkin işlemlerin Kanun'un 9'uncu maddesine uygun hale getirilmesini teminen gerekli düzenlemelerin ivedilikle yapılması ve sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına,

- Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ kapsamında ilgili kişiler tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri alması hususunda veri sorumlusunun uyarılmasına

karar verilmiştir.

2022/662 sayılı KVKK Kararı

İlgili kişinin 'el geometrisi' bilgisinin bir işletmenin hizmet binasına giriş yapabilmek amacıyla veri sorumlusu tarafından açık rıza alınmaksızın işlenmesi hakkındaki Kişisel Verileri Koruma Kurulunun 07/07/2022 tarihli ve 2022/662 sayılı Karar Özeti

Karar Tarihi : 07/07/2022

Karar No : 2022/662

Konu Özeti : İlgili kişinin 'el geometrisi' bilgisinin bir işletmenin hizmet binasına giriş yapabilmek amacıyla veri sorumlusu tarafından işlenmesi

Kuruma intikal eden şikâyette özetle; ilgili kişinin bir işletmeye kayıt yaptırırken hizmet alanına giriş yapabilmek için ilgili firma yetkililerince avuç içi ve parmak izi bilgisinin tarandığı ve bu verilerin şirket kayıtlarında işlendiği, hizmet alan kişilerin cihaza elini koyarak ve verilen şifreyi tuşlayarak hizmet alanına girişin sağlandığı, dolayısıyla ilgili kişinin Kanunen geçerli bir açık rızası olmaksızın avuç içi ve parmak izinin taratıldığı, sözleşmesinin feshedilmesinden sonra konuya ilişkin 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) uyarınca veri sorumlusu şirkete başvuruda bulunduğu, veri sorumlusu tarafından ilgili kişiye cevap verildiği ancak verilen cevabın yetersiz bulunduğu ifade edilerek konu hakkında gereğinin yapılması talep edilmiştir.

Şikâyet konusuna ilişkin başlatılan inceleme çerçevesinde veri sorumlusunun savunması talep edilmiş olup veri sorumlusundan alınan cevap yazısında özetle;

- İlgili kişinin şikâyetinin temel dayanağında; abonelerin işletmenin girişinde, bir cihaz vasıtasıyla parmak izi ve avuç izlerinin taranması suretiyle alana girilebildiği iddiasının bulunduğu,
- İşletme girişinde, kayıtlı abonelerin kimliğinin tanınması amacıyla "... El Geometrisi Terminali" adlı bir cihaz kullanıldığı, bu cihazın parmak veya avuç izi alımından farklı olarak kişilerin "el geometrilerini" sisteme kaydettiği,
- Bu noktada "el geometrisi" kavramını açıklamakta fayda olduğu, parmak izi ve avuç izinin kişiye özgü, bir başka ifadeyle başka bir kişide benzeri mümkün olmayan biyometrik veriler olduğu,

- El geometrisinde ise, cihaza okutulan elin, tarama sırasında parmakların uzunluğu, birleşme noktaları arasındaki uzaklıklar, parmaklardaki oynak yerlerin geometrisi gibi noktalara dikkat edildiği, elin geometrik yapısının, parmakların ve kemiklerin boyutlarının üç boyutlu ortamda bir formüle göre ölçülebildiği, cihaza konulan elin, yalnızca üst kısmının tarandığı, parmak izi veya avuç izinin bulunduğu elin iç kısmını tarayacak herhangi bir mekanizmanın cihazda bulunmadığı, bir başka ifadeyle, tıpkı bir insanın boyunun ölçülmesi gibi kişinin elinin ölçülerinin cihaz vasıtasıyla tarandığı,
- El geometrisi kavramının, parmak veya avuç izinden temel olarak farkının, parmak veya avuç izinin kişiye özel olmasına karşın, el geometrisinin bu tarz kişiye ait bir özelliğinin bulunmadığı, örneğin, X kişinin parmak izinin Y kişisiyle aynı olması mümkün değilken, X kişinin el geometrisinin Y kişisiyle aynı olmasının mümkün olabileceği, bu durum KVKK kapsamında değerlendirildiğinde, parmak veya avuç izi kişiye özel olduğu için özel nitelikli kişisel veri iken el geometrisinin başkaca iki insanda aynı çıkabileceği için sadece kişisel veri hükmünde bir veri olduğu, bir başka ifadeyle el geometrisinin, kişinin yaşı, adı soyadı, iletişim numarası gibi bir kişisel veri olduğu,
- Bu cihazın çalışma şekli bahsedildiğinde; abonelerin el geometrisinin alınmasının tek başına yeterli olmadığı, abonelerin öncelikle, sadece kendilerinin bildiği bir şifreyi, ilgili cihaza tanımladığı, daha sonrasında ise el geometrisinin ilgili cihaz tarafından çıkarıldığı, bu aşamadan sonra, abonenin cihazı her kullanımında şifresini cihaza girmesi ve ardından elini cihaza okutması gerektiği, diğere bir ifade ile kişinin el geometrisinin alınmasının, kişiyi doğru bir şekilde eşleştirmede tek başına yeterli bir husus olmadığı, bunun sebebinin de yukarıda bahsedildiği üzere, el geometrisinin ilgili kişiden başka biriyle de aynı olabileceği, ilgili kişinin ayrıca kendi belirlediği bir şifre ile cihazın kötüye kullanımının önüne geçildiği, el geometrisinin, parmak veya avuç iziyle aynı nitelikte olması halinde, kişiye özgü bir şifre belirlenmesi gibi ayrıca bir teyit işlemine gerek kalmadan, kişinin sadece el geometrisini cihaza okutmasının yeterli olacağı, fakat bu hususun bilimsel gerçekler karşısında mümkün olmayıp, el geometrisinin kişiye özgü olmamasından dolayı, bu kimlik doğrulama tekniğinin yanında şifre girilmesi gibi başkaca teyit mekanizmalarına da ihtiyaç duyulduğu,
- Bu hususlar göz önüne alındığında, şirketin abonelerinden aldığı, el geometrisi verisinin niteliği itibariyle özel nitelikli kişisel veri değil; normal bir kişisel veri olduğu, bu nedenlerle ilgili kişinin, şirketin abonelerinden parmak izi veya avuç izini aldığı iddiasının tamamıyla gerçek dışı bir iddia olduğu, yine ilgili kişinin üyelere şifre verildiği iddiasının da doğru olmadığı, abonelerin kendi şifrelerini kendilerinin oluşturduğu ve bu şifre ile el geometrisini cihaza girerek alana giriş yapabildiği,

• Bu kapsamda gerek el geometrisi alınmasının gerekse de kişilerin bu cihazı kullanırken kendilerine özgü şifre oluşturmasının amacının işletmeye ilgili kişiden başkasının girmesini önlemek, aboneliğin kötüye kullanımının önüne geçmek olduğu, şirket tarafından söz konusu önlemler alınırken gerek 6698 sayılı Kanunun herhangi bir hükmünün gerekse de Kurulun ilke kararlarından hiçbirinin ihlal edilmediği, ilgili kişinin kişisel verilerinin işlenmesi durumunun 6698 sayılı Kanun'un 5'inci maddesi kapsamında kaldığı ve bu verilerin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (c) bendi kapsamındaki gerekçeyle işlendiği, ilgili kişinin el geometrisi verisinin, ilgili kişinin üyeliğinin sonlanması akabinde ivedilikle silindiği

ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde, Kişisel Verileri Koruma Kurulunun 07/07/2022 tarihli ve 2022/662 sayılı Kararı ile;

• 6698 sayılı Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin;

(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

hükmünü haiz olduğu,

• 6698 sayılı Kanun'un "Özel Nitelikli Kişisel Verilerin İşlenme Şartları" başlıklı 6'ncı maddesinde de "... kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık

ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri”nin özel nitelikli kişisel veri olarak belirlendiği, maddenin devamında özel nitelikli kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenmesinin yasak olduğu, üçüncü fıkrasında da birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel verilerin, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebileceği, sağlık ve cinsel hayata ilişkin kişisel verilerin ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceğinin hükme bağlandığı, dolayısıyla veri sorumlusu tarafından Kanun’a uygun olarak kişisel verilerin işlenmesinin ancak Kanun’un 5’inci ve 6’ncı maddesinde yer verilen işleme şartlarının varlığında mümkün bulunduğu,

- Öncelikle şikâyete konu olan kişisel verinin niteliğinin, özel nitelikli kişisel veri olup olmadığının tespit edilmesi gerektiği, nitekim veri sorumlusundan alınan cevap yazısında; cihazın avuç içi veya parmak izi alımından farklı olarak kişilerin “el geometrilerini” sisteme kaydettiği, bu anlamda cihaz tarafından kaydedilen bilginin biyometrik niteliğe haiz olmayan “el geometrisi” bilgisi olduğu ve bu bilginin benzerinin başka bir kişide olma ihtimali bulunduğundan söz konusu bilginin kişinin yaşı, adı soyadı, iletişim numarası gibi bir kişisel veri niteliğinde olduğunun belirtildiği,
- Bu kapsamda veri sorumlusunun cevap yazısında yer verdiği abonelerin, veri sorumlusuna ait hizmet binasına girişlerinde, kimlik tanıma amaçlı kullandığı “... El Geometrisi Terminali” isimli cihazın ilgili kişilere ait hangi bilgiyi işlediği ve kişi ile eşleştirmede bulunulan bilginin niteliğinin belirlenmesi gerektiği,
- İlgili cihaz hakkında açık kaynaklar üzerinden araştırma yapıldığında; öncelikle cihazın isminin “... **Biyometrik** El Terminali” olduğunun görüldüğü ve el geometrisi okuma teknolojisinin, adından da anlaşılacağı gibi kullanıcıların el ve parmak gibi fiziksel karakteristiklerinin üç boyutlu bir ortamda ölçülebilmesi prensibine dayandığı, bu sistemde elin 31.000 noktadan üç boyutlu olarak taranarak, elin ve parmakların karakteristiklerinin analiz edildiği, tarama sırasında parmakların uzunluğu, birleşme noktaları arasındaki uzaklıklar, parmaklardaki oynak yerlerinin geometrisi gibi noktalara dikkat edildiği, elin geometrik yapısının, parmakların ve kemiklerin boyutlarının üç boyutlu ortamda bir formüle göre ölçülebildiği bilgilerine yer verildiğinin tespit edildiği, ayrıca açıklamalarda biyometrik sistemlerin vazgeçilmez özelliğinin doğru sonuç alınması olduğu vurgulanarak el geometrisinde her el için 9 karakterlik bir kodun mevcut olduğu, bu 9 karakterden

her birinin 10 rakam ve 26 harften oluşan toplam 36 olasılık içerdiği yani sistemin yanılma olasılığının $1/36 \times 36 \times 36 \times 36 \times 36 \times 36 \times 36 \times 36 \times 36 \times 36 = 1/101.559.956.668.416$ olduğunun belirtildiği, doğrulama işleminin nasıl yapılacağına ilişkin olarak ise; veri sorumlusu tarafından başka bir kişi ile eşleme ihtimaline binaen şifre ile ikincil bir doğrulama olduğu ifade edilse de cihaza ilişkin açıklamalarda önce kod girilerek kişinin kendisine ait görüntüyü çağırdığı ve elini cihazın altına koyduğu anda doğrulamanın 1 sn'nin altında bir hızla gerçekleştiğinin ifade edildiği,

- Kimlik doğrulamanın; bir kişinin belirli bir kimliğe sahip olduğunu ve/veya bir güvenlik alanına girme veya şikâyete konu somut olaydaki gibi hizmet alınan alana giriş gibi bazı eylemleri yapmaya yetkili olduğunu kanıtlayan bir prosedür olduğu, kimlik doğrulamaya ilişkin kanıtlama, şifre gibi yalnızca belirli bir kimliği veya yetkisi olan kişi tarafından bilinmesi gereken bilginin sorulmasıyla sağlanabileceği gibi somut olayın özelliklerine göre yüz tanıma, parmak izi gibi biyometrik verilerle de yapılabildiği,

- Danıştay'ın 15. Dairesinin 2014/4562 Esas sayılı Kararında; biyometrik yöntemlerin, ölçülebilir fizyolojik ve bireysel özellikleri aracılığıyla gerçekleştirilen ve otomatik şekilde doğrulanabilen kimlik denetleme tekniklerini ifade ettiği, bu yöntemler arasında parmak izi tanıma, avuç içi tarama, el geometrisi tanıma, iris tanıma, yüz tanıma, retina tanıma, DNA tanıma gibi yöntemlerin bulunduğu belirtilmiştir,

- Avrupa Genel Veri Koruma Tüzüğü'nün (GVKT), 4'üncü maddesinde de biyometrik verinin; "yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel veriler" olarak tanımlandığı, aynı zamanda Tüzüğü'nün Resital bölümünün 51'inci maddesinde de yalnızca gerçek bir kişinin benzersiz bir şekilde tanımlanmasına veya doğrulanmasına izin veren belirli bir teknik yöntemle işlendiğinde, bu verilerin biyometrik verilerin tanımı kapsamında kabul edileceği açıklamalarına yer verildiği, dolayısıyla bir verinin biyometrik veri kapsamında değerlendirilebilmesi için o verinin sadece o kişiyi tanımlayabilme ya da doğrulayabilme özelliğine sahip olmasının kriter olarak alındığı,

- Avrupa İnsan Hakları Mahkemesi'nin (AİHM) 4 Aralık 2008 tarihli S. ve Marper/Birleşik Krallık Kararında; parmak izleri, biyolojik örnekler ve genetik profillerin kişisel veri olarak nitelendirildiği, mahkemenin, kişisel verilerin kullanılmasının Sözleşme'nin 8'inci maddesinde yer alan güvencelere aykırılık teşkil etmesinin önüne geçilmesi amacıyla yeterli güvenceleri sağlayacak şekilde iç hukukta düzenlemeler yapılması gerektiğini belirttiği, AİHM'nin, bu tür güvencelere olan ihtiyacın önemini

otomatik olarak işlenen kişisel verilerin korunmasının söz konusu olduğu durumlarda daha da arttığını vurguladığı,

- Diğer taraftan Anayasa Mahkemesi'nin parmak izi kayıt sistemi ile mesai takibi yapılması nedeniyle özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiği yönündeki 2018/11988 başvuru numaralı ve 10/03/2022 tarihli Kararında; 6698 sayılı Kanun'un 6'ncı maddesinde özel nitelikli kişisel verilerin tahdidi olarak sayılmak suretiyle işlenmesini genel nitelikli verilere göre daha sıkı koşullara bağlandığını, özel nitelikli kişisel veri olarak kabul edilen biyometrik verinin **"bir kişinin diğer şahıslardan ayrılmasını ve bizzat kişinin kimliğinin tanımlanmasını sağlayan, bu kişiye ait bir biyolojik veya davranışsal bilgi içermesi nedeniyle önemine binaen özel nitelikli kişisel veri"** olarak kabul edildiğini belirttiği, aynı zamanda biyometrik yöntemlerin kullanılması için kural olarak meşru bir amacın varlığı, hak ve özgürlüklere daha az müdahale ile bu amacı gerçekleştirmeye elverişli başka bir yolun olmaması hâlinde ve amaçla sınırlı olmak üzere uygulanabileceğine, kişisel verilerin işlenmesi ve paylaşılmasını içeren yöntemlerin işyerinde kullanılması hâlinde çalışanın hak ve özgürlüklerini koruyacak anayasal güvencelerin de idare tarafından sağlanması gerektiğine dikkat çektiği,

- Şikayet konusu olayda; ilgili kişinin ve diğer abonelerin hizmet binasına giriş denetimlerinde, el geometrisi bilgisinin işlendiğinin anlaşıldığı, kişisel verilerin korunmasına yönelik düzenlemelerde biyometrik veri tanımının; parmak izi, avuç izi, yüz tanıma, iris tanıma gibi sayılarak sınırları ve çeşitlerinin belirlenmediği, öyle ki, biyometrinin "yaşayan bir organizmanın ölçümü"nü ifade ettiği dikkate alındığında fizyolojik olmayan davranışsal nitelikteki bilgilerin dahi biyometrik veri tanımına dahil olduğu, dolayısıyla veri sorumlusu tarafından el geometrisi bilgisinin ölçülebilir fizyolojik bir özellik olması nedeniyle otomatik şekilde doğrulanabilen kimlik denetleme tekniği ile işlendiğinin anlaşıldığı, her ne kadar veri sorumlusu tarafından el geometrisi bilgisinin parmak izi gibi kişiye ait bir özelliğinin bulunmadığı başka bir kişi ile aynı olmasının mümkün olabileceği ifade edilse de cihaz aracılığıyla elin 31.000 noktadan üç boyutlu olarak taranarak elin ve parmakların analizinin yapıldığı, ilgili kişiyle eşleşmeye ilişkin yanılma oranının çok düşük olduğunun matematiksel olarak açık ve net olduğu dikkate alındığında fizyolojik özellik aracılığıyla gerçekleştirilen ve otomatik şekilde doğrulanabilen bir kimlik denetleme yöntemi olduğu, sonuç olarak, veri sorumlusu tarafından hizmet abonelerinin ve ilgili kişinin el geometrisinin çıkarılması suretiyle biyometrik bir yöntemle kimlik doğrulaması yapıldığı, bu anlamda özel nitelikli kişisel veri işlendiği sonucuna varıldığı,

- Bu doğrultuda, 6698 sayılı Kanun'da özel nitelikli kişisel verilerin işlenmesinin, genel nitelikteki kişisel verilere nazaran daha sıkı koşullara bağlandığı, Kanun'un 6'ncı maddesi uyarınca; özel

nitelikli kişisel veri niteliğini haiz olan biyometrik verinin işlenmesinin ancak açık rızanın bulunması veya kanunlarda açıkça öngörülmesi halinde mümkün olabildiği, bu anlamda biyometrik verilerin kaydedilmesi yöntemiyle hizmet binasına giriş yönteminin uygulanabilmesi için kanunlarda düzenlenmeyen hâllerde kişinin açık rızasının mevcut olması gerektiği, bu kapsamda konuya ilişkin Kanunda öngörülen bir durumun söz konusu olup olmadığı incelendiğinde herhangi bir kanun hükmüne rastlanmadığı,

- Diğer taraftan somut olayda ilgili kişinin veri sorumlusu nezdindeki hizmet binasına girişlerde kullanılması amacıyla el geometrisi bilgisinin veri sorumlusu tarafından kaydedilmesine yönelik özel nitelikli kişisel verisinin işlenmesine rıza göstermediği hususunda da bir ihtilafın söz konusu olmadığı, nitekim ilgili kişinin Kuruma ilettiği şikâyet dilekçesinde de açık rızanın varlığından söz edebilmek için gerekli olan işlenecek kişisel verinin kapsamı, amacı, sınırları ve sonuçları hakkında ilgili kişiye önceden yeterli düzeyde bilgilendirilmediğinin anlaşıldığı,

- Tespitler ışığında, veri sorumlusu bünyesindeki hizmet binasına girişlerde denetimin sağlanması amacıyla özel nitelikli kişisel verilerin işlenmesine ve bu bağlamda biyometrik veri bazlı sistemlerin kullanılmasına dair herhangi bir hukuka uygunluk nedeni olmadığı, bu çerçevede ilgili kişinin özel nitelikli kişisel verisinin 6698 sayılı Kanun'da yer alan herhangi bir işleme şartı mevcut olmaksızın işlendiği sonucuna varıldığı,

- Bilindiği üzere 6698 sayılı Kanun'un "Veri Güvenliğine İlişkin Yükümlülükler" başlıklı 12'nci maddesinin;

"(1) Veri sorumlusu;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak,

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır." hükmünü haiz olduğu,

- Kanun'un "Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi" başlıklı 7'nci maddesinde kişisel verilerin Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silineceği, yok edileceği veya anonim hale getirileceğinin hüküm altına alındığı, bununla birlikte ilgili kişinin hakları hususunda düzenleme getiren Kanun'un

11'inci maddesinde de ilgili kişinin veri sorumlusuna başvurarak kendisiyle ilgili "7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerinin silinmesini veya yok edilmesini isteme" hakkına sahip olduğunun düzenlendiği,

- Kanun'un 15'inci maddesinin (5) numaralı fıkrasının "Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması hâlinde Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ eder. Bu karar, tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilir." hükmünü haiz olduğu,

- Diğer taraftan Kanun'un 15'inci maddesinin (7) numaralı fıkrasında "Kurul, telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması hâlinde, veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulmasına karar verebilir." hükmüne yer verildiği

değerlendirmelerinden hareketle;

- Kanun'un 6'ncı maddesinde yer alan işleme şartlarından herhangi biri bulunmaksızın veri sorumlusu tarafından ilgili kişinin özel nitelikli kişisel veri niteliğini haiz biyometrik veri kategorisindeki "el geometrisi" bilgisinin işlendiği, dolayısıyla veri sorumlusu tarafından Kanun'un 12'nci maddesinin (1) numaralı fıkrasında yer alan yükümlülüğe aykırı davranıldığı, tüm bu hususların ve kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu açısından; şikayete konu olan kişisel verinin özel nitelikli kişisel veri olması, ilgili kişi haricinde diğer abonelerin de özel nitelikli kişisel verilerinin Kanuna aykırı olarak işlendiğinden çok sayıda kişinin etkilenmesi ve kişisel verilerin korunması hakkına müdahalede bulunulması hususları göz önünde bulundurularak, Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca veri sorumlusu hakkında 100.000 TL idari para cezası uygulanmasına,

- İlgili kişinin veri sorumlusu bünyesinde bulunan kişisel verilerinin silinmesi talebine istinaden, veri sorumlusundan alınan cevap yazısında ilgili kişinin el geometrisi verisinin, ilgili kişinin üyeliğinin sonlanması akabinde ivedilikle silindiği ve el geometrisi bilgisi cihaza kaydedildiğinden ve yine cihaz üzerinden silindiğinden silme işlemine dair bir evrak göndermenin fiziken mümkün olmadığı ifade edildiğinden, veri sorumlusunun beyanı esas alındığında silme talebinin yerine getirildiği ve söz konusu kişisel verilerin silindiğine ilişkin ilgili kişinin bilgilendirilmesine,

- Giriş amacıyla biyometrik veri niteliğinde özel nitelikli kişisel veri işlenmesi uygulamasının Kanun'un 15'inci maddesinin 7'nci fıkrası kapsamında durdurulmasına, veri sorumlusu tarafından bugüne kadar işlenen ve muhafaza edilen "el geometrisi" ile ilgili verilerin Kanun'un 7'nci maddesi ile Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

hükümlerine uygun olarak ivedilikle yok edilmesi, eğer ilgili özel nitelikli verilerin üçüncü kişilere aktarılması söz konusu ise, yok etmeye yönelik işlemlerin bu verilerin aktarıldığı üçüncü kişilere ivedilikle bildirilmesinin sağlanması ve yapılan işlemlerin sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2022/243 sayılı KVKK Kararı

Aynı isme sahip bir kişi tarafından internet üzerinden sipariş verilirken ilgili kişinin e-posta adresinin kullanılması üzerine faturanın ilgili kişiye gönderilmesi suretiyle kişisel verilerinin işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 17/03/2022 tarihli ve 2022/243 sayılı Karar Özeti

Karar Tarihi : 17/03/2022

Karar No : 2022/243

Konu Özeti : Aynı isme sahip bir kişi tarafından internet üzerinden sipariş verilirken, ilgili kişinin e-posta adresinin kullanılması üzerine faturanın ilgili kişiye gönderilmesi suretiyle kişisel verilerinin işlenmesi

Kuruma intikal eden şikâyetle özetle; ilgili kişinin, kendisi ile aynı isme sahip bir şahsın internet üzerinden hizmet veren veri sorumlusuna üye olduğu ve sipariş verdiği, bu şahsın siparişi verirken ilgili kişiye ait e-posta adresini kullandığı, veri sorumlusunun e-posta adresinin doğruluğunu kontrol etmeden ve onaylamadan üyelik işlemini gerçekleştirmek suretiyle siparişe ilişkin faturayı ilgili kişiye gönderdiği belirtilerek veri sorumlusu hakkında 6698 sayılı Kanun kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin olarak başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- İlgili kişi ile aynı adı taşıyan bir kullanıcı tarafından isim benzerliğinden kaynaklı olarak Şirketlerine sehven “(...)@gmail.com” e-posta adresinin bildirilerek misafir müşteri girişi ile üyelik hesabı oluşturulmaksızın söz konusu siparişin verildiği, söz konusu e-posta adresi için ilgili kişi veya bir başka kişi adına üyelik hesabı bulunmadığı, e-postanın ilgili kişiye ait herhangi bir veriyle eşleşmediği veya kişiye ait kimlik bilgilerinin işlenmediği,
- Verilerin doğru ve gerektiğinde güncel olmasını sağlamak adına kullanıcılara, üyeliğe ilişkin kişisel verilerini, “hesabım” sayfasında yer alan “üyelik bilgilerim” kısmından değiştirme imkanı sağlandığı ancak Şirketin sisteminde üyelik, e-posta adresine bağlı oluşturulduğundan, mevcut üyelikler için e-posta adresinin değiştirilemediği, bu nedenle yeni bir e-posta adresi kullanmak isteyen kullanıcıların

internet sitesi ya da mobil uygulama üzerinden veya müşteri hizmetlerini arayarak kullanmak istedikleri e-posta adresi ile yeni üyelik açtırabilecekleri

- Üçüncü bir kişi tarafından ilgili kişiye ait e-posta adresi ile gerçekleştirdiği üyelik işlemi sırasında eğer ilgili kişiye ait e-posta adresi ile halihazırda bir üyelik oluşturulmuş ise yeni bir kullanıcının aynı e-posta adresi ile yeni bir üyelik oluşturamadığı ancak somut olayda ilgili kişinin “(...)@gmail.com” e-posta adresi ile üyelik hesabı bulunmadığı için başka bir kullanıcı tarafından misafir girişi yaparak isim benzerliği ile sehven bu e-posta adresinin kullanılarak sipariş oluşturulabildiği,

- Misafir girişlerinde, kullanıcıların internet sitesinde kendi istekleri doğrultusunda işlemleri gerçekleştirebilmeleri ve işlemlerin kolaylaştırılması amacıyla e-posta doğrulaması yapılmadığı, internet sitesinde üye olmaksızın misafir müşteri girişi ile yapılan alışverişler esnasında alışveriş yapan kişi tarafından kendisine ait e-posta veya telefon numarası girilmek istenirken, sehven hatalı olarak girilen başkalarına ait e-posta ve telefon numaralarının teyit edilebilmesine yönelik olarak teknik geliştirme çalışmalarına başlandığı, Kurulun 22.12.2020 tarihli ve 2020/966 sayılı İlke Kararı uyarınca alınacak teknik önlemlere ilişkin Kurulun da görüşüne başvurulduğu, tamamen kontrolleri dışında gerçekleşen bu durumun önüne geçmek ve sehven hatalı veri girişlerini engellemek amacıyla planlar yapıldığı,

- Bir başka gönderici tarafından sehven ilgili kişinin e-posta adresinin sisteme girilerek sipariş oluşturulduğu, ilgili kişiye ait e-posta adresi ile ilgili kişiye ait herhangi bir verinin eşleşmediği ve kişiye ait kimlik bilgilerinin işlenmediği, dolayısıyla işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinin somut olayda söz konusu olmadığı ve 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun (Kanun) 12’nci maddesinin (5) numaralı fıkrası hükmü ile Avrupa Genel Veri Koruma Tüzüğünde yer alan veri ihlali tanımı dikkate alınarak Kuruma veri ihlal bildiriminde bulunulmadığı

ifade edilmiştir.

Konuya ilişkin yapılan incelemede Kişisel Verileri Koruma Kurulunun 17/03/2022 tarihli ve 2022/243 sayılı Kararı ile;

- Kanun’un 3’üncü maddesinin (1) numaralı fıkrasının (ç) bendinde ilgili kişinin, “kişisel verisi işlenen gerçek kişi”; (d) bendinde kişisel verinin, “Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi”, (e) bendinde kişisel verilerin işlenmesinin, “Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi,

yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem,” (1) bendinde veri sorumlusunun, “kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi” olarak tanımlandığı;

- Bu çerçevede şikâyete konu olayda, şikayetçinin uzaktan satış sözleşmesinin tarafı olmayan ilgili kişi, şikayete konu olan ... A.Ş.’nin veri sorumlusu, ilgili kişinin e-posta adresinin kişisel veri, ilgili kişinin e-posta adresine veri sorumlusu tarafından ilgili kişiye ileti gönderilmesi suretiyle e-posta adresinin kullanılmasının da kişisel veri işleme faaliyeti olduğunun değerlendirildiği,

- Kanun’un, kişisel verilerin işlenmesine ilişkin “Genel İlkeler”i düzenleyen 4’üncü maddesinin (1) numaralı fıkrasında, “Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.” hükmünün yer aldığı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin;

a) Hukuka ve dürüstlük kurallarına uygun olma,

b) Doğru ve gerektiğinde güncel olma,

c) Belirli, açık ve meşru amaçlar için işlenme,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,

- Kanun’un “Kişisel Verilerin İşlenme Şartları” başlıklı 5’inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından

birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanun'un "Veri Güvenliğine İlişkin Yükümlülükler"i düzenleyen 12'nci maddesinin (1) numaralı fıkrasında veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idarî tedbirleri almak zorunda olduğunun hükme bağlandığı,

- Şikayete konu olayda, ilgili kişi ile aynı isme sahip bir kişinin üyelik oluşturmadan misafir müşteri girişi ile ilgili kişiye ait e-posta adresini sehven girerek sipariş verdiği, "(...)@gmail.com" e-posta adresi için ilgili kişi veya bir başka kişi için üyelik hesabı bulunmadığı, e-postanın ilgili kişiye ait herhangi bir veriyle eşleşmediği veya ilgili kişiye ait kimlik bilgilerinin işlenmediği, misafir müşteri girişi ile yapılan alışverişler esnasında girilen e-posta ve telefon numaralarının teyit edilebilmesine yönelik olarak henüz bir kontrol mekanizmasının bulunmadığı,

- Sipariş detayları incelendiğinde; gönderici adı, soyadı ve e-posta adresi olarak ilgili kişinin adı, soyadı ve "(...)@gmail.com" e-posta adresinin yer aldığı, bunun yanı sıra alıcı bilgisi olarak üçüncü bir kişinin adresinin açıkça faturada yer aldığı,

- Kişisel veri işleme faaliyetleri bakımından ise her hal ve şartta Kanun'un 4'üncü maddesinde sayılan temel ilkelere uygunluğun sağlanmasının veri sorumlusunun başlıca yükümlülükleri arasında olduğu, şikâyet konusu olayda üye olmadan misafir girişi ile verilen siparişlerde e-fatura gönderiminin temini için e-posta bilgisi beyan edilmeden alışveriş yapılamadığı,

- Öte yandan 05.03.2010 tarihinde yayımlanan 397 sıra numaralı Vergi Usul Kanunu Genel Tebliği ile elektronik fatura (e-fatura) uygulamasının vergi mevzuatımıza dahil edilmiş bulunduğu, söz konusu genel tebliğde belirtilen koşulları sağlayan mükelleflerin kendi istekleri ile seçebileceği bir uygulama olarak başlayan e-fatura uygulamasının zorunlu hale getirildiği, elektronik ticaret ortamı sağlayan gerçek ve tüzel kişi hizmet sağlayıcılarının da e-fatura uygulamasına geçiş yapma zorunluluğu bulunduğu, bu anlamda veri sorumlusu tarafından ilgili kişilere ait e-posta adresinin işlenmesinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (ç) bendi gereğince bir hukuki yükümlülüğün yerine getirilmesi amacıyla kişisel verilerin işlenmesi şartına uygun olarak veri işlendiği yönünde değerlendirilebileceği,

- Bununla birlikte faturanın, ticaret ve vergi mevzuatı bakımından işlemin tarafları arasında borç ilişkisinin varlığı veya akdin ifasını gösteren delil niteliğinde bir belge olup ispat ve itiraz aracı olarak

kullanılabildiği, çeşitli Yargıtay kararlarında da faturanın bu işlevine dikkat çekildiği, bu çerçevede faturanın doğru muhataba/adrese gönderilmesinin önem taşıdığı, elektronik ortamlar üzerinden yapılan alışverişlerde kişiler tarafından telefon veya e-posta bilgilerinin beyanında yanlışlık yapılması sık karşılaşılabilen bir durum olduğundan faturanın yanlış muhataba/adrese gönderilmesi durumunda hak kaybı yaşanmasının muhtemel olduğu, bu açıdan veri sorumlusunun e-posta adreslerinin işlenmesine yönelik olarak her ne kadar Kanun'un 5'inci maddesi gereğince bir işleme sebebine dayanması söz konusu ise de kişisel verilerin Kanun'un 4'ncü maddesinin (2) numaralı fıkrasının (b) bendinde yer alan "doğru ve gerektiğinde güncel olma" ilkesine uygun işlenmesi hususunda aktif özen yükümlülüğü bulunduğu da göz ardı edilemeyeceği,

- Veri sorumlusunun, e-posta adresinin alışveriş yapan kişi tarafından kullanılıp kullanılmadığını teyide yönelik gerekli tedbirleri/doğrulama mekanizmalarını uygulamaya alması gerekirken, buna yönelik bir doğrulama mekanizmanın devrede olmadığı, işlem kolaylığı açısından üye olmadan misafir girişi ile yapılan alışverişlerde e-posta doğrulaması yapılmadığının beyan edildiği,

- Söz konusu işlemde bir teyit mekanizmasının bulunmamasının, hak kaybına sebebiyet verebilmesinin yanı sıra internet sitesinde üye olmadan misafir girişi ile yapılan tüm alışveriş işlemlerinin veri ihlal riski taşıdığı anlamına da gelebileceği, faturaların gönderici ve alıcılara ait ad, soyad, T.C. kimlik numarası, adres, telefon, e-posta ve sipariş bilgilerini ihtiva edebildiği, faturanın konu ile ilgisiz üçüncü bir kişiye gönderilmesinin, içerikte yer alan kişisel verilerin olduğu gibi üçüncü bir kişiye açıklanarak bu verilerin başkaları tarafından kötü niyetli olarak kullanılmasına da zemin hazırlayabileceği, nitekim alıcının adresi ve sipariş bilgilerinin de ilgili kişi tarafından öğrenildiği,

- Bu çerçevede, veri sorumlusunun ilgili kişinin e-posta adresinin işlenmesinde Kanun'un 5'inci maddesindeki bir işleme şartına dayanmadığı, dolayısıyla Kanun'un 4'üncü maddesinin (2) numaralı fıkrasının (b) bendi ile Kanun'un 12'nci maddesinin (1) numaralı fıkrasında belirtilen uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik tedbirlerin alınması yükümlülüklerini yerine getirmediği

değerlendirmelerinden hareketle;

- Veri sorumlusunun faturanın gönderileceği alıcı gruplarına yönelik bir teyit mekanizması kurmadan uzaktan satış sözleşmesinin tarafı olmayan ilgili kişinin e-posta adresinin işlenmesine ve dolaylı olarak faturada yer alan gönderici ve alıcıya ait bilgilerinin ise ilgili kişiye açıklanmasına sebebiyet verdiği dikkate alındığında söz konusu işleme faaliyetinde Kanun'un 5'inci maddesinde yer alan herhangi bir işleme şartına dayanmadığı ve bu minvalde Kanun'un 12'nci maddesinin (1)

numaralı fıkrasındaki yükümlülüklerini yerine getirmediği değerlendirilen veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 100.000 TL idari para cezası uygulanmasına,

- "Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına Kanuna aykırı şekilde gönderilen üçüncü kişilere ait kişisel veriler hakkında" Kurulun 22.12.2020 tarihli ve 2020/966 sayılı İlke Kararının gereğini yerine getirmesi hususunda uyarılmasına,

- Veri sorumlusunun savunmasında Avrupa Birliği Genel Veri Koruma Tüzüğü'nün muhtelif hükümlerine ve değerlendirmelere yer verilmiş olduğu görülmüş olup Kanun hükümlerine uyumun sağlanmasının öncelikli olduğu hususunun veri sorumlusuna hatırlatılmasına

karar verilmiştir.

2022/229 sayılı KVKK Kararı

E-ticaret sektöründe faaliyet gösteren veri sorumlusu şirket tarafından internet sitesinde/mobil uygulamalarında kullanılan çerezler aracılığıyla hukuka aykırı olarak kişisel veri işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 10/03/2022 tarih ve 2022/229 sayılı Karar Özeti

Karar Tarihi : 10/03/2022

Karar No : 2022/229

Konu Özeti : E-ticaret sektöründe faaliyet gösteren veri sorumlusu şirket tarafından internet sitesinde/mobil uygulamalarında kullanılan çerezler aracılığıyla hukuka aykırı olarak kişisel veri işlenmesi

İlgili kişinin Kuruma intikal eden şikâyetinde özetle;

- Veri sorumlusu tarafından uygulanmakta olan çerez politikasının kişilerin temel hak ve özgürlükleri ile özel hayatın gizliliğine müdahaleci nitelikte olduğu,
- Çerez kullanımı hakkında internet sitesinde yer alan politikanın anlaşılabilir ve kapsamı belirtilmemiş bilgiler içermesi dolayısıyla çerezler hakkındaki aydınlatma yükümlülüğünün tam olarak yerine getirilmediği,
- Çerez kullanımına ilişkin işleme şartı olarak meşru menfaatin zorunlu olduğunun iddia edilebilmesinin hukuken mümkün olmadığı düşünülmesi ve veri sorumlusu tarafından ilgili kişinin açık rızasına dayanılarak da işleme faaliyetinin gerçekleştirilmediği,
- İnternet sitesinin faaliyetleri ya da kullanılan çerezler kapsamında işlenen kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 9'uncu maddesinde yer aldığı üzere yurt dışına aktarıldığı ve bu kapsamda ilgili kişinin açık rızasının alınmadığı,
- Kanun'un 11'inci maddesi uyarınca sahip olunan tüm haklar kapsamında veri sorumlusundan bilgi talebinde bulunulduğu; ancak veri sorumlusunun cevabında yalnızca çerez kullanımına ilişkin bilgi verildiği,

- Ayrıca ilgili kişinin, hangi veri konusu kişi grubuna dâhil olduğunun belirtilmediği, üye müşteri ve misafir müşteriyle ilgili olarak işlenen veri kategorileri ve veri tiplerinin işleme amaçlarının tam olarak açıklanmadığı ve kapsamlarının anlaşılmadığı,
- Pazarlama bilgisi veri kategorisi altında yer alan açıklamalardan hangi veri tipinin işlendiğinin anlaşılmadığı, ilgili kişinin ticari elektronik ileti onayı vermemiş olmasına rağmen “hedefleme ve analiz” çerezlerinin tarayıcıda ve uygulamada aktif olduğu, gerek platform gerek mobil uygulama üzerindeki üye müşteri deneyiminin iyileştirilmesi olarak sunulan veri işleme amacı için “hedefleme bilgilerinin” veya “beğenileri” gösteren değerlendirmelerin davranışsal reklamcılık çerezi işlevi kazandığı ve işlenmesine gerek olmadığı hâlde işlendiği, “üye müşterinin açık rızası doğrultusunda yeniden pazarlama, hedefleme, profillemeye ve analiz yapılarak üye müşterinin tercih ve beğenisi doğrultusunda uygulama, mal/ürün ve hizmetlerin tanıtımının ve pazarlamasının yapılması” amacı belirtilen veri kategorisi ve veri tipleri için en uygun amaç olmakla birlikte açık rızasının alınmadığı,
- Ziyaretçi için hedeflemeli çerezler aktifken hedeflemeli reklamcılık yapılmadığının belirtilmesinin doğru olmadığı, çevrim içi ziyaretçinin IP adresinin 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun sebebiyle işlendiği ve bunun politikada belirtildiği; ancak kişisel veri olan IP adresinin işlenmesi sırasında hedeflemeli reklamcılık çerezlerinin site üzerinde aktif hâlde bulunmasının hedefleme yapılmamasını imkânsız kıldığı,
- İnternet sitesinde yer verilen çerez politikasının gerçeği yansıtmadığı, çerezlerin ve üçüncü taraf çerezlerin özelliklerine tam ve doğru bir şekilde yer verilmediği, veri saklama sürelerinin sınırlı sayıda çerez için belirtildiği, bir sosyal medya platformu ile giriş sekmesi üzerinden üyelik oluşturulması ile bazı bilgilerin iki platform arasında paylaşılarak kullanıldığı,
- İşlevde olan çerezlerin ve işlenen kişisel verilerin sadece bir kısmı gösterilerek tam bilgi sunulmamasının çerezler konusundaki aydınlatma yükümlülüğünün yerine getirilmediğinin kanıtı olduğu,
- Ayrıca, tarayıcı veya mobilde çerezleri devre dışı bırakmanın bir önlem olarak sunulduğu, tarayıcıda çerezlerin devre dışı bırakılmasının kişinin tarayıcı deneyimini tamamen katlanılmaz hâle getirdiği, kullanıcının siteye ziyaret gerçekleştirmesinden önce tarayıcı ayarlarından çerez kullanımını engellemediği her hâlde kişisel verilerin işlenmiş olacağı,
- Üçüncü taraf analitik çerezlerin her zaman meşru sayılamayacağı, bu çerezlerin kullanıcı deneyimine yarar sağlamadığı, internet sitesinde 14 adet analitik çerez kullanılmak suretiyle yurt

dışına kişisel veri aktarılmasının Kanun'a uygun şekilde gerçekleştirilmediği, veri sorumlusunun cevabında Avrupa Birliği müktesebatında bu tür çerezlerin kullanılmasına ilişkin olarak e-Gizlilik Regülasyonunun henüz taslak aşamasında olduğunun vurgulandığı, ancak regülasyon olarak taslağı hazırlanan 2002/58 sayılı e-Gizlilik Direktifinin, 2009/136 sayılı Direktif düzenlemesi olarak güncel hâlde yürürlükte olduğu, davranışsal reklamcılık ve analitik çerezlerin uygulanmasında 2002/58 sayılı Direktifin 5'inci maddesinin (3) numaralı fıkrası ile kullanıcıya tanınması gereken "reddetme hakkı"nın, 2009/136 sayılı Direktifte tekrar düzenlendiği, hâlihazırda bu tür çerezlerin uygulanmasının, 95/46 sayılı Direktif'te tanımlandığı hâliyle "rıza"ya tabi olduğu, güncel durumun, bu rızanın artık Avrupa Birliği Genel Veri Koruma Tüzüğü'ne (GDPR) göre yorumlanması yönünde olduğu,

- Üye olmayan ya da üye olmadan alışveriş yapan ziyaretçilerin profillemeye veya segmentasyona tabi tutulmadığının belirtildiği ancak kullanılan çerezlerin büyük bir kısmının veriyi doğrudan ziyaretçiden topladığı ve ziyaretçi trafiğinin siteler arası davranışsal reklamcılık ile arttırılmasının sağlandığı, bu durumda ziyaretçilerin hedeflemeli reklamlara, segmentasyon veya profillemeye tabi tutulduğu

belirtilerek gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan konuya ilişkin savunması istenilmiş olup alınan cevabi yazıda özetle;

- İlgili kişinin internet sitesi üzerindeki çerezler kapsamında işlenen kişisel verileri açısından, ilgili kişinin tanınabilmesi amacıyla tarayıcısına yerleştirilen çerezler ve internet sitesinde kullanılan çerezler vasıtasıyla işlenen kişisel verilerinin "oturum belirteci (session token), alıcı numarası (Buyer ID), e-posta özet değeri (hashed e-mail), cinsiyeti, üyelik tarihi, sisteme son giriş tarihi, e-posta izni, alıcı VIP statüsü ve web/mobil web sitelerinde yer alan Çerez Politikası'nda belirtilen ve 'kesinlikle gerekli çerez' statüsünde olmayan çerezler" şeklinde olduğu ve bunların Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (f) bendi uyarınca meşru menfaatleri için veri işlenmesinin zorunlu olması şartı kapsamında işlenmekte olduğu,

- "Kesinlikle gerekli çerez" statüsünde olmayan çerezler dışında kalan diğer çerezlerin ise bilgi toplumu hizmet sağlayıcısı sıfatıyla çevrim içi bedelli olarak kullanıcılara sunulan elektronik ticaret hizmetinin sunulabilmesi için kesinlikle gerekli çerezler olduğu,

- "Kesinlikle gerekli çerezler" ve bilgi toplumu hizmetinin sunulması noktasında, kendilerinin bir bilgi toplumu hizmet sağlayıcısı olduğu ve bu kapsamda kullandıkları bazı çerezlerin hizmetin

sunumu açısından “kesinlikle gerekli çerezler” olduğu ve bunlar bakımından web sitesi veya mobil uygulama kullanıcılarından açık rıza alınmasının gerekli olmadığı ve bilgi toplumu hizmet sağlayıcısı olarak meşru menfaatlerine istinaden kişisel verilerin işlenmekte olduğu, bu kapsamdaki çerezlere örnek olarak kullanıcı girişi, kimlik doğrulama, güvenlik, ağ yönetimi ve kullanıcı tercihlerini saklamak için kullanılan oturum çerezlerinin verilebileceği,

- “Kesinlikle gerekli çerez” kategorisi dışında kalan analitik, kullanıcı davranışları takibi ve diğer online reklamcılık çerezlerinin kullanıldığı, bu çerçevede kullanıcıların internet sitesini ilk ziyaretleri akabinde pop-up şeklinde bir aydınlatma metni çıktığı, kullanıcıların internet sitesindeki Gizlilik ve Çerez Politikalarına yönlendirildiği, Çerez Politikasında da çerezlerin nasıl kullanıldığı, birinci ve üçüncü taraf çerez ayrımı ve işlevleri, üçüncü taraf çerezlerin reklam ve hedefleme amacıyla nasıl kullanıldığı, çerez sağlayıcı, çerez adı, çerez çeşidi, çerez amacı, çerez süresi ve detaylı olarak çerez yönetiminin nasıl yapılacağına ilişkin olarak kullanıcıya bilgi verildiği,

- Kullanılan çerezlerin sunulan hizmetin ön şartı olarak ileri sürülmediği, çerez uygulamalarının AB’de “çerez duvarları” (cookie walls) veya “takip duvarları” (tracking walls) olarak adlandırılan uygulamalardan farklı olarak, elektronik ticaret hizmetinin sunumunun bu çerezlerin kabulü şartına bağlanmadığı, bilakis ana sayfayı ziyaret eden kullanıcılara çerezlere ilişkin bilgilendirme yapıldığı ve çerezleri kabul etmeleri kaydıyla hizmeti kullanmalarının istenmediği,

- Çerez uygulamalarının GDPR’nin yürürlüğe girdiği tarihe kadar Avrupa’da kabul edilen bir uygulama olduğu, aynı uygulamanın Türkiye’de yerleşik birçok şirket tarafından benimsenmekte ve kullanılmakta olduğu, GDPR’nin yürürlüğe girmesi ile birlikte 2002/58 sayılı e-Privacy Direktifi ile düzenlenen “kesinlikle gerekli çerezler” dışında kalan izleme ve online reklamcılık çerezlerine ilişkin olarak kullanıcıdan rıza alınması şartı getirildiği, uygulamada özellikle AB menşeli veya çok uluslu şirketler tarafından GDPR uyumu doğrultusunda, çerezler için açık rıza alınması ve açık rıza yönetimi sağlayacak şekilde internet siteleri tasarlanmışken birçok şirketin çerez kullanımına ilişkin olarak hâlâ GDPR öncesi uygulamaya devam etmekte olduğu, bu duruma netlik kazandırmak için Kişisel Verileri Koruma Kurulu tarafından da veri sorumlularına yardımcı olarak nitelikte bir rehber yayınlanmasının elzem olduğu, ilgili kişi tarafından yapılan şikâyetten bağımsız olarak, çerez kullanımına ilişkin olarak açık rıza alınması hususunda ve rıza yönetimini sağlayacak teknik çözüm sunan firmalarla görüşmelerin başladığı, ticari anlaşmalar yapıldığında ise çerezler için açık rıza ve kullanıcı tercih yönetimi sağlayacak şekilde sayfalarının çalıştığına ilişkin bilgilerin Kurula sunulacağı,

- Çerezlerin yalnızca e-ticaret siteleri tarafından değil, tüm internet ekosisteminde kullanılmakta olduğu ve günümüz dünyasında çerez kullanımının internet deneyimi açısından temel standart hâline gelmiş bir uygulama olduğu, dolayısıyla özellikle de e-ticaret platformlarının çerez kullanmaksızın temel işlevlerini yerine getiremeyecekleri ve kullanıcılarına kaliteli bir hizmet sunamayacakları, çerezler sayesinde yerine getirilen işlevleri başka bir araçla ikame etmenin mümkün olmadığı ve bir e-ticaret platformu için çerez kullanımının zorunlu olduğu,
- Çerez kullanımında meşru menfaatlerinin bulunduğuna kuşku olmadığı, zira çerez kullanımının müşteri deneyiminin iyileştirilmesi, müşteri tercih ve beğenileri odaklı hizmet sunulması ve müşteri istekleri doğrultusunda ürün ve hizmet optimizasyonu yapılabilmesi gibi karar destek sistemlerini besleyen temel gerekliliklerden biri olduğu ve aksi bir durumun, kullanıcı deneyimini ve kendi faaliyetlerini derinden zedeleyeceği, Şirketlerini sektörel rekabetin dışına iteceği,
- Veri işleme sonucu elde edilen menfaatin ilgili kişilerin temel hak ve özgürlükleriyle yarışabilir düzeyde ve orantılı olduğu, çerezlerin kullanılmasının özünün kullanıcı deneyimini iyileştirmek ve ilgili internet sitesini kullanıcılarının en işine yarayacak ve en kolay şekilde kullanılmasını sağlamak olduğu, bu kapsamda çerezler vasıtasıyla kullanıcıların ilgi alanları ve istekleri göz önüne alınarak onlara özel bir deneyim sunulmasının amaçlandığı,
- Çerezler kapsamında gerçekleştirilen kişisel veri işleme faaliyetlerinin meşru menfaat denge testini sağladığı görüşünde bulunduğu; çerez ve benzeri teknolojilerin kullanımına ilişkin AB'nin GDPR ve e-Privacy Direktifi uygulamalarına paralel olarak "kesinlikle gerekli olmayan çerezler" için kullanıcının açık rızasının alınması ve rıza yönetimi süreçlerinin tasarlanmaya başlandığı,
- Ad-soyadı, iletişim bilgileri (telefon numarası, adres ve e-posta adresi) ve T.C. kimlik numarasının Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (c) bendi kapsamında işlendiği ve söz konusu kişisel verilerin yine aynı kapsamda satıcı ve kargo şirketi ile paylaşıldığı,
- Sunulan Gizlilik Politikası ile Çerez Politikasının birbirini tamamlayıcı nitelikte olduğu ve çerezlerin kullanımı kapsamında işlenen verilere ilişkin olarak detaylı açıklamaları barındırdığı, ilgili kişinin aydınlatmada bulunmadığını iddia ettiği hususların Gizlilik Politikasında mevcut olduğu, ek olarak, ilgili politikalarda Kanun'un 10'uncu maddesinde bulunan her türlü içeriğin yer aldığı
- İnternet sitelerinde ve mobil uygulamalarında "tracking wall" uygulamasının olmadığı ve çerezlerin Çerez Politikasında belirtilen şekilde kullanım dışı bırakılması durumunda da internet sitesinin işlediği ve etkin şekilde ziyaret edilmesinin mümkün olduğu,

- Çerez hizmeti sunan yerli bir sağlayıcı bulunmadığından, internet ortamında çerez kullanan tüm internet sitelerinin yurt dışına veri aktarımında bulunduğu, bu aktarıma ilişkin olarak gerek internet sitesinde bulunan politikalarında gerekse de Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) kaydında bilgilendirmenin yer aldığı ve ilgili kişilerin Kanun'un 10'uncu maddesi kapsamında bilgilendirildiği,
- Çerezlerin Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik'in kapsamının dışında yer aldığı ve söz konusu Yönetmelik hükümlerinin çerezler bakımından uygulama alanı bulmadığı, bu sebeple de çerez uygulamaları için ticari elektronik ileti onayı alınması gerekmediği ifade edilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulunun 10/03/2022 tarih ve 2022/229 sayılı Kararı ile;

- Bir internet sitesinin düzgün çalışması için zorunlu çerezlere ilişkin olarak ilgili kişilerin açık rızasına gerek duyulmayacak iken; reklam, pazarlama ve performans amacıyla çalışan çerezlerin kullanılmasının ilgili kişinin açık rızasına tabi olduğu,
- "Kesinlikle gerekli çerezler", internet sitesinin düzgün çalışması için gerekli çerezler olup ilgili kişinin açık rızası olmaksızın Kanun'un 5'inci maddesinin (2) numaralı fıkrasında ve Kanun'un 6'ncı maddesinin (3) numaralı fıkrasında yer alan işleme şartlarından birine dayanılarak kişisel veri işleme faaliyeti gerçekleştirilebileceği,
- "Kesinlikle gerekli çerezler" statüsünde olmayan çerezler ile kişisel veri işleme faaliyeti gerçekleştirilmesi ve Kanun'un 5'inci maddesinin (2) numaralı fıkrası ile 6'ncı maddesinin (3) numaralı fıkrasında yer alan işleme şartlarından birinin bulunmaması durumunda ilgili kişinin açık rızasına başvurulması gerektiği,
- Veri sorumlusu tarafından çerezler vasıtasıyla gerçekleştirilen veri işleme faaliyetinin dayanağı olarak Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (f) bendi gösterilmişse de kesinlikle gerekli çerezler statüsünde olmayan çerezler vasıtasıyla gerçekleştirilen işleme faaliyeti bakımından anılan bende dayanılmasının mümkün olmadığı ve ilgili kişinin açık rızasına başvurulması gerektiği,
- Veri sorumlusu tarafından ilgili kişilerin kullanıcı tercihlerinin kesinlikle gerekli çerezler kapsamında değerlendirildiği anlaşılacakla birlikte bu çerezlerin zorunlu çerezler dışında kalan işlevselliği sağlama amacı ile kullanıldığı, ilgili kişinin bilgi toplumu hizmetini açıkça talep ettiğinin net olmadığı durumlarda açık rızaya dayanılması gerekeceği,

- Veri sorumlusunun internet sitesinde yer alan Çerez Politikasında “...İlgi alanlarınıza ve size daha uygun içerik ve reklamları sunmak için, diğer bir ifade ile hedeflenmiş reklam/tanıtım amacıyla kullanır. Çerezler yoluyla elde edilen bilgileri sizlere ait diğer kişisel verilerle eşleştirerek; size daha uygun içerikleri, kişiye özel kampanya ve ürünleri sunar ve daha önceden istemediğinizi belirttiğiniz içerik veya fırsatları bir daha sunmaz.” ifadesinin yer aldığı, ayrıca veri sorumlusunun üçüncü taraf çerezlerini reklam ve yeniden hedefleme için nasıl kullandığına ilişkin açıklamaların bulunduğu, ilgili kişinin şikâyeti ekinde yer verilen veri sorumlusunun internet sitesinde bulunan çerezlere ilişkin listede de üçüncü taraf çerezlerin bulunduğu dikkate alındığında veri sorumlusu tarafından reklam/pazarlama çerezleri kullanılmak suretiyle kişisel veri işleme faaliyeti gerçekleştirildiğinin anlaşıldığı,
- Veri sorumlusunun internet sitesine girildiği anda sayfanın sol alt köşesinde çıkan bir pop-up ile “Çerez Kullanımı Çerezler (cookie), ...web sitesini ve hizmetlerimizi daha etkin bir şekilde sunmamızı sağlamaktadır. Detaylı bilgi için Gizlilik ve Kişisel Verilerin Korunması Politikası ile Çerez Politikasını inceleyebilirsiniz.” şeklinde açıklamalar barındıran kutucuk ile bilgi verildiği, kesinlikle gerekli olmayan çerezler bakımından ilgili kişilerin açık rızasına başvurulduğuna ilişkin herhangi bir emareye rastlanmadığı,
- Bununla birlikte, çerez politikası içerisinde bulunan Çerez Yönetimi başlığı altında internet tarayıcısının çeşidine göre çerezler hakkında bilgi edinilip izin verme veya reddetme hakkının kullanılabilmesini teminen yönlendirmelerin yapıldığının görüldüğü,
- Kanun kapsamında açık rızanın, “Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza” şeklinde tanımlandığı ve açık rızanın “aktif bir hareket” vasıtasıyla verileceğinin bir prensip olarak kabul edildiği göz önünde bulundurulduğunda veri sorumlusu tarafından kesinlikle gerekli olmayan çerezler kullanılması suretiyle Kanun’un 5’inci ve 6’ncı maddesinde yer alan kişisel veri işleme şartlarından herhangi birine dayanılmaksızın kişisel veri işleme faaliyeti gerçekleştirildiği ve bu işleme faaliyeti bakımından açık rıza mekanizmasının bulunmadığı,
- Veri sorumlusunun, internet sitesinde ve mobil uygulamalarında yer alan ve sitenin/uygulamanın düzgün çalışmasını sağlayan kesinlikle gerekli çerezler dışında yer alan işlevsel çerezler, performans-analitik çerezler, reklam/pazarlama çerezlerinin çalıştırılmasına ilişkin olarak açık rıza dışında bir veri işleme şartı bulunmuyor ise internet sitesini/mobil uygulamaları ziyaret eden kullanıcılardan internet sitesine/mobil uygulamaya giriş anında ilgili kişilerin iradi aktif hareketiyle söz konusu çerezlerin

çalışmasına onay vermesini, dolayısıyla varsayılan ayar olarak çerezlerin çalışmamasını öngören “opt-in” mekanizmasına göre açık rıza alması gerektiği,

- Kanun’un 9’uncu maddesi anlamında aktarıma ilişkin olarak veri sorumlusunun Kuruma taahhüname sunmadığı ve yeterli korumanın bulunduğu ülkelerin de belirlenmediği dikkate alındığında kişisel verilerin yurt dışına aktarılmasının yalnızca açık rıza şartına dayalı olarak gerçekleştirilebileceği; ancak veri sorumlusunun bu yönde ilgili kişilerin açık rızasını almadığı, bu çerçevede veri sorumlusunun çerezler vasıtasıyla yurt dışına kişisel veri aktarmak suretiyle gerçekleştirdiği faaliyetler Kanun’un 9’uncu maddesine uygun şekilde gerçekleştirilmediğinden, bu faaliyetlerin Kanun’un 9’uncu maddesine uyumlu hâle getirilmesi gerektiği,

- Veri sorumlusunun internet sitesine girildiği anda sayfanın sol alt köşesinde çıkan bir pop-up ile “Çerez Kullanımı Çerezler (cookie), ...web sitesini ve hizmetlerimizi daha etkin bir şekilde sunmamızı sağlamaktadır. Detaylı bilgi için Gizlilik ve Kişisel Verilerin Korunması Politikası ile Çerez Politikasını inceleyebilirsiniz.” şeklinde açıklamalar barındıran kutucuk ile bilgi verildiğinin görüldüğü, söz konusu politikaların her ikisinin de üzerine tıklanıldığında Gizlilik Politikalarının bulunduğu ana sayfaya yönlendirme yapıldığı ve bir süre sonra ilgili politikaların olduğu sayfanın ekranda belirdiği,

- Gizlilik ve Kişisel Verilerin Korunması Politikasında Çerezlere ilişkin olarak “...Çerez (Cookie) Kullanımı ve Yönetimi ... tarafından kullanılan çerezler, çerez çeşitleri, amaçları, saklama süreleri ve çerez yönetimi ile ilgili detaylı bilgi için Çerez (Cookie) Politikamızı inceleyebilirsiniz.” şeklinde bilgilendirme bulunduğu, söz konusu metin içerisinde direkt olarak ilgili kişileri Çerez Politikasına yönlendirebilecek bir bağlantı eklenmesinin çerezler konusunda aydınlatmanın daha kolay erişilebilir olması adına önem arz ettiği, bu nedenle söz konusu metne çerezlere direkt olarak yönlendirme yapılacak bağlantının eklenmesi yönünde güncelleme yapılması gerektiği,

- Veri sorumlusunun Gizlilik ve Kişisel Verilerin Korunması Politikasından ayrı olarak bir Çerez Politikası oluşturduğu, ilgili kişilerin de çerezler vasıtasıyla gerçekleştirilen kişisel veri işleme faaliyetleri bakımından bu metne yönlendirildiği dikkate alındığında veri sorumlusunun Gizlilik Politikasında çerezlerle ilgili yer vermiş olduğu bilgilerin Çerez Politikasında da yer alması gerektiği, ayrıca söz konusu metnin aydınlatma yükümlülüğünün düzenlendiği Kanun’un 10’uncu maddesi ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ’e (Tebliğ) uygun olması gerektiği,

- Bu çerçevede Çerez Politikasında, Tebliğ’in 4’üncü maddesi uyarınca veri sorumlusunun kimliğine ilişkin açıklamalara yer verildiği; ancak kişisel verilerin hangi amaçla işleneceği, kişisel verilerin

kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi ile ilgili kişinin Kanun'un 11'inci maddesinde sayılan diğer hakları konusunda doğru bir şekilde bilgilendirme yapılmadığı,

- Söz konusu Çerez Politikası Tebliğ'in 5'inci maddesinin (1) numaralı fıkrasının (g) bendi açısından değerlendirildiğinde, bu politikada kişisel veri işleme amaçlarının belirlendiği görülmekle birlikte hangi kişisel veri işleme faaliyetinin hangi işleme amacı ile örtüştüğüne ilişkin detaylı bilgilendirmeye yer verilmediği, öte yandan çerez çeşitlerinin her birine ilişkin amaçların tabloda gösterildiği anlaşılmalı beraber amacın ilgili kişiler tarafından anlaşılacak açıklıkta olmadığı görüldüğü,
- Tebliğ'in 5'inci maddesinin (1) numaralı fıkrasının (ğ) bendi kapsamında değerlendirildiğinde, çerezlerin niteliği itibariyle teknik bir konu olduğundan hareketle veri sorumlusunun Çerez Politikasında anlaşılır, açık ve sade bir dil kullandığının görüldüğü,
- Tebliğ'in 5'inci maddesinin (1) numaralı fıkrasının (h) bendi hükmü açısından değerlendirildiğinde, veri sorumlusunca düzenlenen Çerez Politikasında hangi kişisel verinin hangi işleme amacı ve hukuki sebep olan işleme şartı ile ilişkilendirildiğinin açıkça belirtilmediğinin; anılan düzenleme (i) bendi kapsamında değerlendirildiğinde ise hangi kişisel verilerin hangi yöntem ile elde edildiğinin Çerez Politikasında açıkça belirtilmediğinin görüldüğü,
- Veri sorumlusunun hâlihazırda internet sitesinde ve mobil uygulamada kullanılan tüm çerezlere ilişkin süreçlerin gözden geçirilerek Çerez Politikası ile uyumluluğunun sağlanması gerektiği, bu çerçevede söz konusu Çerez Politikasının Kanun'un 10'uncu maddesi ve Tebliğ'e uygun olarak güncellenmesi gerektiği

değerlendirmelerinden hareketle;

- Veri sorumlusu tarafından kişisel veri niteliğinde "kesinlikle gerekli olmayan" çerezler kullanılması suretiyle Kanun'un 5'inci ve 6'ncı maddesinde yer alan şartlarından herhangi birine dayanılmaksızın işleme faaliyeti gerçekleştirildiği, Kanun'un 9'uncu maddesinde yer alan aktarım usullerinden herhangi birine dayanılmaksızın kişisel veri aktarıldığı ve bu hususların Kanun'un 12'nci maddesinin (1) numaralı fıkrası hükmüne aykırılık teşkil ettiği değerlendirilmekte olup Kurul tarafından Kanun'un 12'nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri alma yükümlülüğünü yerine getirmeyen veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 800.000 TL idari para cezası uygulanmasına,

Ayrıca,

- Veri sorumlusu tarafından kesinlikle gerekli olmayan çerezler kullanılması suretiyle Kanun'un 5'inci ve 6'ncı maddesinde yer alan kişisel veri işleme şartlarından herhangi birine dayanılmaksızın kişisel veri işleme faaliyeti gerçekleştirildiği ve bu veri işleme faaliyeti bakımından açık rıza mekanizmasının da bulunmadığı değerlendirildiğinden veri sorumlusu tarafından internet sitesinde ve mobil uygulamalarında yer alan ve sitenin/uygulamanın düzgün çalışmasını sağlayan kesinlikle gerekli çerezler dışında yer alan İşlevsel Çerezler, Performans-Analitik Çerezler, Reklam/Pazarlama Çerezlerinin çalıştırılmasına ilişkin olarak açık rıza dışında bir veri işleme şartı bulunmuyor ise internet sitesini/mobil uygulamaları ziyaret eden kullanıcılardan internet sitesine/mobil uygulamaya giriş anında ilgili kişilerin iradi aktif hareketiyle söz konusu çerezlerin çalışmasına onay verilmesinin sağlanması ve dolayısıyla varsayılan ayar olarak çerezlerin çalışmamasını öngören "opt-in" mekanizmasına göre açık rıza alınması,

- Veri sorumlusunun çerezler vasıtasıyla yurt dışına kişisel verileri aktarmak suretiyle gerçekleştirdiği faaliyetlerin Kanun'un 9'uncu maddesine uyumlu hâle getirilmesi,

- Gizlilik ve Kişisel Verilerin Korunması Politikası içerisinde direkt olarak ilgili kişileri Çerez Politikasına yönlendirebilecek bir bağlantı eklenmesinin çerezler konusunda aydınlatmanın daha kolay erişilebilir olması adına önem arz ettiği dikkate alındığında söz konusu metne çerezlere direkt olarak yönlendirme yapılacak bağlantının eklenmesi yönünde güncelleme yapılması,

- Veri sorumlusunun hâlihazırda internet sitesinde ve mobil uygulamasında kullanılan tüm çerezlere ilişkin süreçlerin gözden geçirilerek Çerez Politikası ile uyumluluğunun sağlanması ve söz konusu Çerez Politikasının Kanun'un 10'uncu maddesi ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'e uygun olarak güncellenmesi,

Kullanıcı tercihleri ile ilgili çerezler zorunlu çerezlerin dışında kalan işlevselliği sağlama amacıyla kullanıldığından söz konusu çerezlerin kullanıcının talep etmiş olduğu bir bilgi toplumu hizmetinin yerine getirilebilmesi için zorunlu olarak kullanılıp kullanılmadığı hususunda veri sorumlusu tarafından değerlendirme yapılması suretiyle kişisel veri işleme şartının belirlenmesi, ilgili kişi tarafından bilgi toplumu hizmetinin açıkça talep edildiği net değil ise ilgili kişilerin açık rızasına başvurulması

hususlarında gerekli düzenlemelerin yapılarak Kurula en geç 30 gün içinde bilgi verilmesi yönünde veri sorumlusunun talimatlandırılmasına,

- Öte yandan ilgili kişinin Kanun'un 11'inci maddesi kapsamındaki bilgi taleplerinin veri sorumlusu tarafından yerine getirildiğine

karar verilmiştir.

2022/224 sayılı KVKK Kararı

Bir bankanın çağrı merkezi tarafından ilgili kişinin telefon numarasının üçüncü kişilerle paylaşılması hakkında Kişisel Verilerin Koruma Kurulunun 10/03/2022 tarihli ve 2022/224 sayılı Karar Özeti

Karar Tarihi: 10/03/2022

Karar No: 2022/224

Konu Özeti: Bir bankanın çağrı merkezi tarafından ilgili kişinin telefon numarasının üçüncü kişilerle paylaşılması

Kuruma intikal eden şikâyette özetle; ilgili kişi tarafından üçüncü bir kişinin kartının Banka ATM'sinde bulunduğu, akabinde veri sorumlusu Banka'nın çağrı merkezi ile iletişime geçildiği, görüşme sırasında çağrı merkezi yetkilisi tarafından ilgili kişinin telefon numarasını kart sahibi üçüncü kişiyle paylaşmak suretiyle, kartın ilgili kişiden teslim alınmasının önerildiği, bu çözüm önerisine ilgili kişinin rıza göstermediği ve çağrı merkezi yetkilisinin kartı havalimanındaki güvenlik görevlilerine teslim etmesini rica etmesi üzerine ilgili kişinin banka kartını görevlilere teslim ettiği, ancak ilerleyen saatlerde kart sahibi tarafından ilgili kişiye şahsi telefon numarası üzerinden mesaj gönderildiği, işlenen verilerin ilgili kişinin açık rızası olmamasına rağmen kart sahibine iletildiğinin anlaşıldığı, bu itibarla isim ve soy ismi ile telefon numarasının işlenmesine dair ilgili kişinin aydınlatılmadığı ve verilerinin aktarılmasına açık rıza göstermediği belirtilerek veri sorumlusu Banka hakkında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusunun savunması talep edilmiş olup veri sorumlusunun Kuruma intikal eden cevabi yazısında özetle;

- Çağrı Merkezi ile ilgili kişinin yapmış olduğu görüşmede kimlik verileri (adı, soyadı) iletişim verileri (telefon numarası) ve ses kaydı verisinin; Banka'nın internet sayfasında Bize Ulaşın bölümünü kullanarak ilettiği başvurusuna ilişkin kimlik verilerinin (adı, soyadı, TC kimlik numarası), iletişim verilerinin (telefon numarası ve e-posta adresi); Banka'nın şubesine ilettiği dilekçesinden ise söz konusu dilekçede yer alan bilgileri ile kimlik verilerinin (kimlik belge örneği) Banka tarafından işlendiği,

- İşlenen kişisel verilerin müşteri ilişkileri yönetimi süreçlerinin yönetimi ile buna bağlı olarak talep ve şikâyetlerin takibi, ilgili iletişim faaliyetlerinin yürütülmesi, bu faaliyetlerin bağlı olunan mevzuatta öngörülen uygun içerik ve detayda yürütülmesinin sağlanması, kayıtlara ilişkin mevzuatta emredilen şekilde saklama ve arşiv faaliyetlerinin gerçekleştirilmesi ve genel olarak müşteri güvenliğinin sağlanması amaçları ile işlendiği,

- Banka'nın aydınlatma metninin internet sitesinde herkes tarafından erişime açık şekilde yer aldığı, internet sayfasında 'Bize Ulaşın' bölümünü kullanarak iletilen başvurularda "Kişisel Verilerin Korunması Kanunu kapsamında yapılan Bilgilendirmeyi okudum, anladım" kutucuğu ile, Çağrı Merkezi arandığında ilk olarak kayıp/çalıntı/şüpheli işlem bildirimini işlemleri ile birlikte Kişisel Verilerin Korunmasına ilişkin bilgi alınması hususundaki işlem menüsüne yönlendirildiği, ilgili kişiye çağrı merkezi kanalıyla KVKK aydınlatma metni sunulduğu, ancak müşterinin dinlememeyi tercih ettiği, ilgili kişinin "Çağrı Merkezi" kanalıyla ve Banka web sayfasında 'Bize Ulaşın' bölümünde oluşturduğu başvurusunda 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 10'uncu maddesi gereğince verilerinin işlenmesi sürecine ilişkin olarak aydınlatma yükümlülüğünün yerine getirildiği,

- İlgili kişinin, müşterilerinin bankomat kartını bulduğunu haber vermek amacıyla çağrı merkezleriyle yaptığı görüşmede müşteri temsilcisinin "kart sahibine kartı sizin bulduğunuzu ileteceğim şeklinde" yaptığı bilgilendirmeye "tamam" cevabını vermesi üzerine kart sahibi ile ilgiliye ait kişisel verilerin sözlü olarak paylaşıldığı,

ifade edilmiş, ayrıca yazı ekinde, ilgili kişinin Çağrı Merkezi ile yaptığı görüşme kaydının yer aldığı CD sunulmuştur.

Konuya ilişkin yapılan inceleme neticesinde, Kişisel Verileri Koruma Kurulunun 10/03/2022 tarihli ve 2022/224 sayılı Kararı ile;

- Kanun'un amacının kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek olduğu, Kanun'un "Tanımlar" başlıklı 3'üncü maddesinde "ilgili kişi"nin, kişisel verisi işlenen gerçek kişi; "veri sorumlusu"nun ise kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlandığı,

- Kanun'un, kişisel verilerin işlenmesine ilişkin "Genel İlkeler"i düzenleyen 4'üncü maddesinin (1) numaralı fıkrasında, "Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve

esaslara uygun olarak işlenebilir.” hükmünün yer aldığı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin;

a) Hukuka ve dürüstlük kurallarına uygun olma,

b) Doğru ve gerektiğinde güncel olma,

c) Belirli, açık ve meşru amaçlar için işlenme,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,

• Kanun’un “Kişisel Verilerin İşlenme Şartları” başlıklı 5’inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

• Kanun’un “Veri Sorumlusunun Aydınlatma Yükümlülüğü” başlıklı 10’uncu maddesinde, veri sorumlusunun veya yetkilendirdiği kişinin, kişisel verilerin elde edilmesi sırasında ilgili kişilere; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, kişisel veri toplamanın yöntemi ve hukuki sebebi, 11 inci maddede sayılan diğer hakları konusunda bilgi vermekle yükümlü olduğunun düzenlendiği,

• Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ’de de veri sorumluları veya yetkilendirdiği kişiler tarafından aydınlatma yükümlülüğü kapsamında uyulacak usul ve esasların belirlendiği, anılan Tebliğ’in 5’inci maddesinin (1) numaralı fıkrasında; d) bendinde; “Aydınlatma yükümlülüğünün yerine getirilmesi, ilgili kişinin talebine bağlı değildir.”e)

bendinde; “Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı veri sorumlusuna aittir.” hükmünün yer aldığı,

- Kanun’un “Veri Güvenliğine İlişkin Yükümlülükler”i düzenleyen 12’nci maddesinin (1) numaralı fıkrasında ise veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idarî tedbirleri almak zorunda olduğunun hükme bağlandığı,
- Somut olayda, çağrı merkezi aracılığıyla banka ile iletişim kurulduğunda arayan kişiye KVKK aydınlatma metninin sunulduğunun tespit edildiği, aynı zamanda veri sorumlusu tarafından iletilen belgelerden; ilgili kişi, veri sorumlusunun internet sitesinde bulunan ‘bize ulaşın’ bölümünden başvuruda bulunurken, "Kişisel Verilerin Korunması Kanunu kapsamında yapılan Bilgilendirmeyi okudum, anladım" kutucuğunun işaretlendiği, bu anlamda veri sorumlusu Banka tarafından aydınlatma yükümlülüğünün yerine getirildiğinin anlaşıldığı,
- Kanun’da kişisel veri işleme şartlarından biri olarak düzenlenen “açık rıza”nın, Kanun’un 3 üncü maddesinde “belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza” şeklinde tanımlandığı, tanımda yer aldığı üzere, açık rızanın, “belirli bir konuya ilişkin olması”, “rızanın bilgilendirmeye dayanması” ve “özgür iradeyle açıklanması” şeklinde üç unsuru bulunduğu, bu kapsamda, veri işlemek üzere alınan açık rızanın geçerli olması için, açık rızanın öncelikle belirli bir konuya ilişkin ve o konu ile sınırlı olarak verilmesi, ayrıca kişinin neye rıza gösterdiğini de bilmesi gerektiği,
- Bu çerçevede, veri sorumlusu tarafından iletilen çağrı merkezi görüşme kaydı dinlendiğinde; görüşmenin son kısmında çağrı merkezi personelinin “... Kartın güvenliğini sağlıyorum. Gerekli bilgileri not aldım, müşterinin kendisi ile iletişime geçeceğim kartı sizin bulduğunuzu iletacağım.” şeklindeki ifadesinin üzerine ilgili kişinin “tamam” şeklinde yanıt verdiğinin tespit edildiği,
- Somut olayda verilen açık rıza değerlendirildiğinde; çağrı merkezi personelinin öncesinde kartın güvenliğini sağladığına ilişkin açıklamalarda bulunduktan sonra “... kart sahibine kartı sizin bulduğunuzu iletacağım ...” şeklindeki ifadesinden ilgili kişinin ad, soyadı ve telefon numarası bilgisinin kart sahibi üçüncü kişiyle paylaşılacağı çıkarımında bulunulmasının makul bir beklentiye uygun olmadığı, aynı ifadeden kart güvenliğinin sağlanması ile birlikte bir vatandaş tarafından kartın bulunduğu bilgisinin paylaşılacağına ilişkin anlaşıldığının daha beklenebilir bir durum olduğu,

- Buna ek olarak, görüşme kaydının tamamı göz önünde bulundurularak değerlendirme yapıldığında, ilgili kişiye kart sahibinin bilgilerinin verilerek kartın ilgili kişinin kendisi tarafından teslim edilmesine ilişkin öneriye karşılık, olumsuz cevap verilmesinden de ilgili kişinin kişisel verilerinin paylaşılması yönünde bir rızasının bulunmadığı çıkarımında bulunulmasının mümkün olabileceği,

- Sonuç olarak, ilgili kişinin kişisel verilerinin üçüncü kişiye açıklanması şeklinde gerçekleşen kişisel veri işleme faaliyetinin açık rızanın unsurlarını barındırmadığı, dolayısıyla veri sorumlusu tarafından Kanun'a aykırı olarak kişisel veri işleme faaliyetinde bulunulduğu kanaatine varıldığı,

- Bu çerçevede veri sorumlusu tarafından Kanun'un 5'inci maddesinde yer alan işleme şartlarından herhangi biri geçerli olmadan kişisel verilerin açıklanması suretiyle veri işleme faaliyetinde bulunulduğu anlaşıldığından Kanun'un 12'nci maddesinde yer alan "Kişisel verilere hukuka aykırı erişilmesini önlemek" ve "Kişisel verilerin muhafazasını sağlamak" yükümlülüğüne aykırı davranıldığı,

değerlendirmelerinden hareketle,

- İlgili kişinin kişisel verisi niteliğindeki ad, soyadı ve telefon numarası bilgilerinin Kanuna aykırı olarak üçüncü kişiyle paylaşılması nedeniyle veri ihlaline sebebiyet verildiği dikkate alındığında; Kanun'un 12'inci maddesi çerçevesinde veri sorumlusu Banka tarafından bünyesinde işlediği kişisel verilerin hukuka aykırı işlenmesini önlemek ve muhafazasını sağlamak adına yükümlülüklerinin gereği gibi yerine getirilmemesi nedeniyle Kanun'un 18'inci maddesi kapsamında veri sorumlusu hakkında idari yaptırım uygulanmasına,

- İlgili kişinin kişisel verilerinin işlenmesi sürecinde aydınlatma yükümlülüğünün yerine getirilmediği iddiasına ilişkin olarak; çağrı merkezi aracılığıyla banka ile iletişim kurulduğunda arayan kişiye KVKK aydınlatma metninin sunulduğunun tespit edildiği, aynı zamanda veri sorumlusu tarafından iletilen belgelerde, ilgili kişinin veri sorumlusunun internet sitesinde bulunan 'Bize Ulaşın' bölümünden başvuruda bulunurken, "Kişisel Verilerin Korunması Kanunu kapsamında yapılan Bilgilendirmeyi okudum, anladım" kutucuğunun işaretlendiği hususları dikkate alındığında, veri sorumlusu banka tarafından aydınlatma yükümlülüğünün yerine getirildiği anlaşıldığından söz konusu iddia hakkında Kanun kapsamında yapılacak bir işlem bulunmadığına

karar verilmiştir.

2022/184 sayılı KVKK Kararı

Bir alacak yönetim şirketi tarafından ilgili kişinin borç bilgilerinin üçüncü kişilerle paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 04/03/2022 tarihli ve 2022/184 sayılı Karar Özeti

Karar Tarihi : 04/03/2022

Karar No : 2022/184

Konu Özeti : Bir alacak yönetim şirketi tarafından ilgili kişinin borç bilgilerinin üçüncü kişilerle paylaşılması

Kuruma intikal eden şikâyet dilekçesinde özetle; ilgili kişinin kardeşi ve askeri personel olan eşi adına kayıtlı hatlara veri sorumlusu alacak yönetim şirketinin unvanını taşıyan bir başlık altında SMS gönderildiği, söz konusu SMS ile ilgili kişinin bir telekomünikasyon şirketine olan borcunun süresinin dolacağı ve ödenmemesi halinde icra işlemlerine başlanacağı bildirildiği; ilgili kişinin kişisel verilerinin ifşa edilmesinden ötürü ilgili alacak yönetim şirketinin hukuk bürosuna başvuruda bulunduğu ancak kendisine yazılı bir cevap verilmediği; akabinde ilgili kişinin eşine ait hattın hukuk bürosu çalışanı olduğunu söyleyen bir şahıs tarafından arandığı, konuşma esnasında konuyu hukuk yoluyla değil konuşarak çözelim nedir durum neden dilekçe yazdınız şeklinde hitapta bulunduğu; sonrasında ilgili kişinin eşinin, kişisel verileri istedikleri gibi ifşa edemeyeceklerini, bunun 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) uyarınca suç teşkil ettiğini, kendileri hakkında hukuki olarak gereken her türlü yasal yollara başvuracaklarını bildirdiği; ayrıca ilgili kişiye ait şahsi bilgilerin neden kendi telefonuna gönderilmediğinin sorulduğu ayrıca, istenildiği takdirde UYAP veya MERNİS'ten iletişim bilgilerine ulaşılabileceğinin söylendiği ve ilgili telefon numaralarına nasıl ulaşıldığı yönünde bilgi talep edildiğinde ise dolaylı yollardan bulduk, biz buluruz şeklinde cevap verildiği belirtilmiş; ilgili kişinin rızası olmadan kişisel verilerinin üçüncü kişilerle paylaşıldığı beyan edilerek Kanun kapsamında şikâyetçi olunduğu ifade edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusu alacak yönetim şirketinden savunması istenilmiş olup verilen cevabı yazıda özetle;

- Bir telekomünikasyon şirketi ile arasında alacak devir sözleşmesinin akdedilmiş olması sebebiyle bahsi geçen şirket tarafından icra dosya bilgileri, müşterilere ait faturalar, müşteriler tarafından telekomünikasyon şirketine verilen iletişim bilgileri vb. bilgilerin taraflarına iletildiği,
- İşlem yapılırken icra borçlularının telekomünikasyon firmasına iletildiği telefon numaralarının arandığı, taraflarınca herhangi bir iletişim bilgisi araştırma yükümlülüğünün olmadığı gibi, başkaca iletişim bilgisine ulaşma şanslarının olmadığı, ilgili kişi için de ifade edilen şekilde işlemlere başlanmış olduğu ve telekomünikasyon firmasının taraflarına iletildiği telefon numaralarının arandığı,
- Akabinde şikâyet dilekçesinde belirtilen hatlardan şirketlerinin çağrı merkezinin arandığı ve ilgili kişi olarak dosya hakkında bilgi almak istendiği, kullanılan çağrı merkezi sistemi tarafından şikâyete konu telefon numaralarının, ilgili kişi sıfatıyla aranıldığı için sisteme herhangi bir işlem yapmadan otomatik olarak kaydedildiği ve sistem tarafından söz konusu telefon numaralarına otomatik olarak SMS gönderimi gerçekleştirildiği,
- Taraflarınca hiçbir şekilde ilgili kişiye ait başka bir telefon numarası araştırması yapılmadığı gibi üçüncü kişilere de ulaşılmadığı ve üçüncü kişilere bilgi verilmediği, çağrı merkezini arayan kişilerin ilgili kişi olup olmadığı tespit edilemediğinden taraflarınca ilgili kişi sıfatıyla arandıkları telefon numaralarına işlem yapıldığı

beyan ve iddialarına yer verilmiştir.

Şikâyet dilekçesinde belirtilen hatlardan çağrı merkezinin arandığı ve ilgili kişi olarak dosya hakkında bilgi almak istendiği, kullanılan çağrı merkezi sistemi tarafından şikâyete konu telefon numaralarının, ilgili kişi sıfatıyla aranıldığı için sisteme herhangi bir işlem yapmadan otomatik olarak kaydedildiği hususlarına ilişkin kanıtlayıcı nitelikte imza ve kaşeli belgelerin Kurum'a gönderilmesinin istenmesi üzerine; veri sorumlusunca telekomünikasyon şirketi ile aralarında imzalanan sözleşme ile alacak devri sözleşmesi örneklerine yer verilmekle birlikte ilgili kişinin telekomünikasyon şirketine ilişkin ödenmemiş faturası dolayısıyla borcu olduğunu ve icra takibi başlatıldığını gösterir kayıtlar ile veri sorumlusunun alacakların tahsili için kullandığı çağrı merkezi sistemi aracılığıyla borçlular ile icra takibi sürecinde iletişim kurulması sonrası ilgili görüşmeye ilişkin ayrıntıların kaydedildiği sistemin ekran görüntülerine yer verilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 04/03/2022 tarihli ve 2022/184 sayılı kararı ile;

- Kanun'un amacının kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin

yükümlülükleri ile uyacakları usul ve esasları düzenlemek olduğu, Kanun'un "Tanımlar" başlıklı 3'üncü maddesinde "ilgili kişi"nin, kişisel verisi işlenen gerçek kişi; "veri sorumlusu"nun ise kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlandığı,

- Kanun'un, kişisel verilerin işlenmesine ilişkin "Genel İlkeler"i düzenleyen 4'üncü maddesinin (1) numaralı fıkrasında, "Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir." hükmünün yer aldığı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin;

a) Hukuka ve dürüstlük kurallarına uygun olma,

b) Doğru ve gerektiğinde güncel olma,

c) Belirli, açık ve meşru amaçlar için işlenme,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Öte yandan, "İlgili Kişinin Hakları"nı düzenleyen Kanun'un 11'inci maddesinin, "(1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

a) Kişisel veri işlenip işlenmediğini öğrenme,

b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

c) Kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp

kullanılmadığını öğrenme,

ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

d) Kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini

isteme,

e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok

edilmesini isteme,

f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü

kişilere bildirilmesini isteme,

g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle

kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde

zararın giderilmesini talep etme, haklarına sahiptir.”

hükmünü amir olduğu,

- Kanun'un "Veri Güvenliğine İlişkin Yükümlülükler"i düzenleyen 12'nci maddesinin (1) numaralı fıkrasında veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idarî tedbirleri almak zorunda olduğunun hükme bağlandığı,

- Somut olayda, ilgili kişinin kardeşi adına kayıtlı olan hatta ve eşine ait telefona ilgili kişinin telekomünikasyon şirketine olan borcunun süresinin dolacağına ilişkin bir SMS gönderildiği ifade edilerek rızası olmadan kişisel verilerinin üçüncü kişilerle paylaşıldığının beyan edildiğinin görüldüğü;

- Veri sorumlusu tarafından Kurum'a gönderilen savunma ekindeki belgeler incelendiğinde ilgili kişinin şikâyet dilekçesinde belirttiği borcun süresinin dolacağına ilişkin SMS'in gönderildiği tarihten önceki bir tarihte ilgili kişinin kardeşi adına kayıtlı telefon numarasından veri sorumlusunun aranarak dosya numarasının öğrenildiği, yine aynı tarihte söz konusu borca itiraz edildiği ve itirazın onaylandığı bilgisinin paylaşıldığı iddiası ile ilgili kişinin kardeşi adına kayıtlı telefon numarasından tekrar veri sorumlusunun arandığına ilişkin imzalı ve kaşeli ekran görüntülerinin bulunduğu;

bununla birlikte yine aynı tarihte ilgili kişinin eşine ait telefon numarasıyla görüşüldüğü, borç ve masraflarla ilgili bilgilendirme yapıldığının beyan edildiği;

- Veri sorumlusu tarafından Kurum'a iletilen savunma yazısında taraflarınca işlem yapılırken icra borçlularının telekomünikasyon şirketinin ilettiği telefon numaralarının arandığı, taraflarınca herhangi bir iletişim bilgisi araştırma yükümlülüğünün olmadığı gibi, başkaca iletişim bilgisine ulaşma şanslarının olmadığı, ilgili kişi için de ifade edilen şekilde işlemlere başlanmış olduğu ve telekomünikasyon şirketinin taraflarına ilettiği telefon numaralarının arandığı, akabinde şikâyet dilekçesinde belirtilen ilgili kişinin eşi ve kardeşinin telefon numaralarından çağrı merkezinin arandığı ve ilgili kişi olarak dosya hakkında bilgi almak istendiği, kullanılan çağrı merkezi sistemi tarafından şikâyete konu telefon numaralarının, ilgili kişi sıfatıyla aranıldığı için sisteme herhangi bir işlem yapmadan otomatik olarak kaydedildiği ve sistem tarafından söz konusu telefon numaralarına otomatik olarak SMS gönderimi gerçekleştirildiğinin beyan edildiğinin görüldüğü;

- Bu kapsamda veri sorumlusu tarafından Kurum'a iletilen cevap yazılarından; veri sorumlusunun çağrı merkezini arayarak bir borç hakkında bilgi talep edilmesi halinde arayan kişiye herhangi bir bilgilendirme yapılmaksızın ve Kanunun 5'inci maddesinde yer alan herhangi bir işleme şartına dayanmaksızın arayan kişilerin telefon bilgilerinin sisteme otomatik olarak kaydedilmek suretiyle işlenmesi ve bu kişilerle başka şahısların kişisel verisi niteliğindeki borç bilgisine ilişkin bilgi paylaşımında bulunduğu kanaatine varılması nedeniyle veri sorumlusunun Kanunun 12'nci maddesinin (1) numaralı fıkrası çerçevesinde kişisel verilerin hukuka aykırı işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı değerlendirilmelerinden hareketle;

- Veri sorumlusunu arayan telefon numaralarının ilgili kişinin telefon numarası olarak kaydedilmesi ve bu telefonların aranması suretiyle borç bilgilerinin üçüncü kişiler ile paylaşılmasında Kanunun 5'inci maddesi çerçevesinde bir işleme şartının geçerli olmadığı dikkate alındığında Kanunun 12'nci maddesinin (1) numaralı fıkrası çerçevesinde kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı tespit edilen veri sorumlusu hakkında Kanunun 18'inci maddesinin (1) numaralı fıkrasının (b) bendi çerçevesinde 50.000 TL idari para cezası uygulanmasına,

- Veri sorumlusunu bilgi almak amacıyla arayan kişilerin telefon numaralarının veri sorumlusu sistemlerine otomatik olarak borcu olan kişilerin iletişim bilgileri olarak kaydedilmesi uygulamasına son verilmesi ve sonucundan Kurul'a bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2022/172 sayılı KVKK Kararı

Yurt dışında mukim veri sorumlusunun Türkiye'deki irtibat bürosu tarafından işe alım sürecinde adaylardan özel nitelikli kişisel veri talep edilmesi hakkında Kişisel Verileri Koruma Kurulunun 24/02/2022 tarihli ve 2022/172 sayılı Karar Özeti

Karar Tarihi : 24/02/2022

Karar No : 2022/172

Konu Özeti : Yurt dışında mukim veri sorumlusunun Türkiye'deki irtibat bürosu tarafından işe alım sürecinde adaylardan özel nitelikli kişisel veri talep edilmesi

İlgili kişinin yurt dışında mukim veri sorumlusunun Türkiye'deki irtibat bürosu hakkındaki şikâyetinde özetle;

- İlgili kişinin işe kabulü yapılırken veri sorumlusunun irtibat bürosunca kendisinden adli sicil kaydı, sağlık raporu, akciğer filmi raporu, kan grubu belgesi, ehliyet fotokopisi, evlilik cüzdanı fotokopisi ve aile bireylerinin nüfus cüzdanı fotokopilerinin istenildiği ve ilgili kişi tarafından bu belgelerin teslim edildiği,
- İrtibat bürosunun bahse konu özel nitelikli kişisel verilerin işlenmesi için ilgili kişiden açık rıza almadığı,
- Aile bireylerinin nüfus cüzdanı bilgilerinin talep edilmesinin Kanun'un 4'üncü maddesinde yer alan genel ilkeler ile çeliştiği,
- Veri sorumlusunun özel nitelikli kişisel verilerin işlenmesinde Kişisel Verileri Koruma Kurulu'nun (Kurul) aldığı 31/01/2018 tarihli ve 2018/10 sayılı Kararda belirtilen hususları yerine getirmediği,

Veri sorumlusunun yurt dışında mukim olması sebebiyle, ilgili kişiye ait kişisel verilerin yurt dışına da aktarılmış olabileceği,

- İlgili kişinin başvurusuna veri sorumlusu tarafından 30 günlük yasal süre içinde herhangi bir yanıt verilmediği

hususları belirtilmiş ve 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) hükümleri uyarınca gerekli işlemlerin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusunun Türkiye'deki irtibat bürosuna yazılan yazı ile savunması istenilmiş olup, alınan cevabi yazıda özetle;

- Şikâyet edilenin, yurt dışı menşeli veri sorumlusunun Türkiye'deki irtibat bürosu olduğu, yasal kuruluş esasları gereği münferit bir tüzel kişiliği ve ticari faaliyeti haiz olmadığı,
- İlgili kişinin veri sorumlusu bünyesinde çalışmasının doğrudan yurt dışı merkezli yasal mevzuat hükümlerine göre belirlendiği ve buna göre iş yeri sicil dosyasının yurt dışında cari olan mevzuat hükümlerine göre oluşturulduğu,
- İlgili kişinin şikâyetine konu olan kişisel verilerin, ilgili kişinin yurt dışında mukim veri sorumlusunun çalışanı olması nedeniyle, iş yeri özlük dosyası kapsamında rızası ile ilgili kişiden temin edildiği, bu anlamda icazet olmaksızın söz konusu kişisel verilerin yurt dışına aktarılması gibi bir durumdan bahsedilemeyeceği,

Ş• ikâyete konu kişisel verilerin, iş akdi gereği, çalışma süresi boyunca şikâyet edilen irtibat bürosu uhdesinde "özlük dosyası" mahiyetinde, ilgili yasal mevzuat ile kanunlarda belirlenen meşru amaca uygun olarak muhafaza edildiği, iş akdinin sonlandırılmasını müteakip ilgili kişi tarafından açılan İş Mahkemesi nezdindeki dava dosyasının bir örneğinin sunulduğu, sonrasında yasal bir zorunluluk bulunmamasına karşın söz konusu kişisel verilerin irtibat bürosu ve yurt dışı birimleri kayıtlarında imha edildiği

belirtilmiştir

Konuya ilişkin yürütülen inceleme neticesinde, Kurulun 24/02/2022 tarih ve 2022/172 sayılı Kararı ile;

- Kanun'un amacının kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek olduğu, Kanun'un "Tanımlar" başlıklı 3'üncü maddesinde "İlgili kişi"nin, kişisel verisi işlenen gerçek kişi; "veri sorumlusu"nun ise kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlandığı,
- Kanun'un, kişisel verilerin işlenmesine ilişkin "Genel İlkeler"i düzenleyen 4'üncü maddesinin (1) numaralı fıkrasında, "Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir." hükmünün yer aldığı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin;

a) Hukuka ve dürüstlük kurallarına uygun olma,

b) Doğru ve gerektiğinde güncel olma,

c) Belirli, açık ve meşru amaçlar için işlenme,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanun'un "Veri Güvenliğine İlişkin Yükümlülükler"i düzenleyen 12'nci maddesinin (1) numaralı fıkrasında veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idarî tedbirleri almak zorunda olduğunun hükme bağlandığı,

- Öte yandan, 4857 sayılı İş Kanunu'nun ("4857 sayılı Kanun") "Tanımlar" başlıklı 2'nci maddesinin "Bir iş sözleşmesine dayanarak çalışan gerçek kişiye işçi, işçi çalıştıran gerçek veya tüzel kişiye yahut tüzel kişiliği olmayan kurum ve kuruluşlara işveren, işçi ile işveren arasında kurulan ilişkiye iş ilişkisi denir. İşveren tarafından mal veya hizmet üretmek amacıyla maddî olan ve olmayan unsurlar ile işçinin birlikte örgütlendiği birime işyeri denir... İşveren adına hareket eden ve işin, işyerinin ve işletmenin yönetiminde görev alan kimselere işveren vekili denir. İşveren vekilinin bu sıfatla işçilere karşı işlem ve yükümlülüklerinden doğrudan işveren sorumludur" hükümlerini ihtiva ettiği,

- 4875 sayılı Kanun'un "Tanımlar" başlıklı 2'nci maddesinde ise "Yabancı yatırımcı: Türkiye'de doğrudan yabancı yatırım yapan, 1) Yabancı ülkelerin vatandaşlığına sahip olan gerçek kişiler ile yurt

dışında ikamet eden Türk vatandaşlarını, 2) Yabancı ülkelerin kanunlarına göre kurulmuş tüzel kişileri ve uluslararası kuruluşları ifade eder” hükmünün bulunduğu,

- Bununla birlikte, Doğrudan Yabancı Yatırımlar Kanunu Uygulama Yönetmeliği'nin “İrtibat bürosu kuruluşu” başlığını haiz 6'ncı maddesinin “Bakanlık, yabancı ülke kanunlarına göre kurulmuş şirketlere, Türkiye'de ticari faaliyette bulunmamak kaydıyla irtibat bürosu açma izni vermeye ve bu izinlerin süresini uzatmaya yetkilidir...” hükmünü amir olduğu,

- Somut hadisede şikâyet olunan tarafın, yurt dışında yerleşik bir tüzel kişi olan veri sorumlusunun irtibat bürosu olduğunun görüldüğü, veri sorumlusunun internet sitesinden edinilen bilgilere göre veri sorumlusunun başka bir ülke merkezli bir yazılım şirketi tarafından satın alındığı, şu halde veri sorumlusunun Türkiye İrtibat Bürosu'nun; Türkiye'de ticarî faaliyet yürütmeyen, tüzel kişiliği bulunmayan, yalnızca “Haberleşme ve Bilgi Aktarımı” faaliyetinde bulunan bir irtibat bürosu olduğu ve yabancı sermaye mevzuatına tabi bulunduğu,

- Öte yandan irtibat bürolarının, 4857 sayılı Kanun'a göre “iş yeri” statüsüne dâhil olduğu, 4875 sayılı Kanun'a göre ise “yabancı yatırımcı”nın yabancı ülkelerin vatandaşlığına sahip olan gerçek kişiler ile yurt dışında ikamet eden Türk vatandaşlarını, yabancı ülkelerin kanunlarına göre kurulmuş tüzel kişileri ve uluslararası kuruluşları ifade ettiği,

- 4875 sayılı Kanun'da gösterilen yatırımcıların iş hukuku anlamında işveren sıfatını kazanacağına ulaşıldığı, bu surette irtibat bürosu çalışanlarını ve dolayısıyla da ilgili kişiyi istihdam eden işverenin; veri sorumlusunun irtibat bürosu değil, veri sorumlusunun kendisi olacağı,

- Bu sebeplerle, somut hadisede “veri sorumlusu” sıfatının yurt dışında yerleşik veri sorumlusunun Türkiye İrtibat Bürosu'na değil, yurt dışında mukim ve tüzel kişiliği haiz olan veri sorumlusunun kendisine atfedilebileceği kanaatine varıldığı,

- İlgili kişinin gönderdiği tebligatta “yetkili” sıfatı ile veri sorumlusunun şirket müdürüne yer verildiği, şirket müdürünün ise yurt dışında mukim olunan yer yetkili noteri tarafından onaylanan ve düzenlenen vekâletname ile veri sorumlusu adına yetkilendirildiğinin görüldüğü, şu halde ilgili kişinin veri sorumlusuna İrtibat Bürosu yetkilisi ve işveren vekili vasıtasıyla yaptığı tebligatın hukuken muteber ve geçerli olduğu, veri sorumlusunun da buna yanıt vermesi gerektiği, ancak veri sorumlusunun, ilgili kişinin başvurusuna yasal süre içerisinde herhangi bir yanıt vermediği, bu suretle veri sorumlusunun Kanun ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'de (“Tebliğ”) yer verilen ilgili kişilerin başvurularına yanıt verilmesine ilişkin hükümlere aykırı hareket ettiğinin tespit edildiği,

- İşveren sıfatının yurt dışı merkezli veri sorumlusunun üzerinde olduğu dikkate alındığında, çalışanlar ile akdedilen iş ilişkisi sözleşmelerinin irtibat bürosuyla değil, veri sorumlusunun kendisiyle akdedilmesinin icap edeceği, hâl böyle olunca bu iş ilişkisi kapsamında akdedilen sözleşme gereği, ilgili kişiye ait kişisel verilerin irtibat bürosu tarafından yurt dışında mukim veri sorumlusuna aktarılmasında herhangi bir hukuka aykırılığın bulunmayacağı zira sözleşmenin tarafının doğrudan yurt dışı merkezli veri sorumlusu olmasından dolayı “veri sorumlusu” sıfatının zaten yurt dışı merkezli şirkete ait olduğu,
 - İlgili kişinin yurt dışı menşeli veri sorumlusu bünyesinde çalışmak üzere iş akdi yaparken, veri sorumlusunun tabi olduğu yabancı mevzuat gereği kendisinden temin edilen bilgi ve belge mahiyetindeki kişisel verilerinin yurt dışında işleneceğini düşünmemesinin mümkün olmadığı, bir akdin gereğinin yerine getirilmesi için ilgili kişiden açık rıza temin etmekten başka hiçbir yasal yol olmaması durumunda bu akit kurulurken taraflardan açık rıza istenmesinin açık rızanın yasal unsurlarını sakatlamayacağı, zira ilgili kişinin bu akit kurulurken kişisel verilerinin akıbetine dair farkındalık sahibi olduğu,
 - Veri sorumlusu tarafından ilgili kişinin kişisel verilerinin tabi olunan yabancı ülke hukuku gereği, özlük dosyası oluşturmak amacıyla işlendiği iddia edilse de bu konudaki açıklamaları destekleyici bir bilgi ya da belgenin sunulmadığı, ayrıca veri sorumlusunun bu belgeleri hangi yasanın hangi hükmü uyarınca temin ettiğini Kurula açıklamadığı,
 - Öte yandan, veri sorumlusu tarafından şirket merkezi ve irtibat bürosu nezdinde ilgili kişiye ait tüm kişisel verilerin imha edildiği iddia edilmekle birlikte bunu destekleyen bir belgenin de Kuruma sunulmadığı, hâlbuki Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik’in “İlkeler”i düzenleyen 7’nci maddesinin (3) numaralı fıkrasındaki “Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.” hükmü uyarınca veri sorumlularının, yaptıkları silme işlemlerini evraka bağlamak ve söz konusu vesaiki talep edildiği takdirde resmî makamlara sunmak zorunda oldukları,
 - Veri sorumlusuna gönderilen bilgi ve belge talebi konulu yazıda, ilgili kişinin şikâyet dilekçesinde yer alan bütün iddialara yönelik yanıtlar ile bu yanıtları destekleyen kayıt ve belgelerin istendiği fakat veri sorumlusunun bu belgeleri Kurula sunmadığı
- değerlendirmelerinden hareketle;

- Somut olayda “veri sorumlusu” sıfatının irtibat bürosuna değil, bizzat yurt dışı merkezli şirkete ait olduğu,
 - İrtibat bürosu müdürünün aynı zamanda veri sorumlusunun işveren vekili olması sebebiyle, ilgili kişi tarafından irtibat bürosuna yapılan tebligatın hukuken muteber ve geçerli olduğu,
 - İlgili kişinin veri sorumlusuna yaptığı başvuruya Kanun ve Tebliğ hükümleri ihlal olunarak yasal süre dâhilinde herhangi bir yanıt verilmediği,
 - Şikâyet konusunu teşkil eden somut olayda yurt dışına veri aktarılmasının hukuka aykırı olmadığı, ilgili kişiye ait kişisel verilerin yurt dışında mukim veri sorumlusu tarafından iş ilişkisi kapsamında akdedilen sözleşme vasıtasıyla, yerleşik ülke hukuku doğrultusunda elde edildiği fakat bu mevzuat hükümlerine ilişkin olarak ilgili kişiye ve Kurula yeterli açıklamalarda bulunulmadığı,
 - Bahse konu iş akdinin ifası için ilgili kişiye ait kişisel verilerin yurt dışında işlenmesinin gerektiği ve bunun yegâne yolunun da ilgili kişinin açık rızasının alınması olduğu anlaşıldığından, ilgili kişiden alınan açık rızanın hukuka uygun olduğu,
 - İlgili kişinin kişisel verilerinin gerek şirket merkezi gerekse de irtibat bürosu nezdinde imha edildiğine dair destekleyici bir belgenin Kuruma intikal ettirilmediği anlaşıldığından, veri sorumlusunun;
 - İlgili kişilerin başvuruları konusunda azamî dikkat ve özeni göstermesi,
 - İlgili kişinin kişisel verilerinin şirket merkezi ve irtibat bürosu nezdinde imha edildiğini gösterir belgenin ilgili kişiye iletilerek bu hususu tevsik edici belge ile birlikte işlemin sonucundan Kurula bilgi vermesi
- hususlarında talimatlandırılmasına karar verilmiştir.

2022/137 sayılı KVKK Kararı

Veri sorumlusu bir alışveriş merkezi tarafından senetli alışverişler için ilgili kişilerden e-Devlet şifresi, internet sayfasında üyelik oluşturulması için ise T.C. kimlik numarası temin edilmesi suretiyle kişisel verilerin hukuka aykırı işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 17/02/2022 tarih ve 2022/137 sayılı Karar Özeti

Karar Tarihi : 17/02/2022

Karar No : 2022/137

Konu Özeti : Veri sorumlusu bir alışveriş merkezi tarafından senetli alışverişler için ilgili kişilerden e-Devlet şifresi, internet sayfasında üyelik oluşturulması için ise T.C. kimlik numarası temin edilmesi suretiyle kişisel verilerin hukuka aykırı işlenmesi

Kuruma intikal ettirilen ihbar dilekçesinde; veri sorumlusu bir alışveriş merkezinin internet sitesinde senet ile telefon satın alma başvurusu yapıldığı esnada ilgili kişilerden e-Devlet şifrelerinin istenildiği, bu durumun 6698 sayılı Kanuna aykırılık teşkil ettiği belirtilerek gereğinin yapılması talep edilmiştir. İhbar dilekçesinde ayrıca; veri sorumlusunun internet sitesinde 'Kasaya Git' sekmesi altındaki sayfada "Senetli alışverişte onay sürecinizin başarıyla tamamlanmasını istiyorsanız aşağıdaki alana e-Devlet şifrenizi giriniz. Siparişi onaylıyorum butonuna basıldığında otomatik olarak doğrulama yapılacaktır." şeklinde bilgilerin yer aldığı ekran görüntüsüne yer verildiği görülmüştür.

Konuya ilişkin başlatılan resen inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- Veri sorumlusunun gerek yerleşik olduğu iş yerlerinde gerekse de web sitesinde perakende satış hizmeti sunduğu ve bu hizmete ilişkin müşteri/ziyaretçi/üyelerden kanundan kaynaklanan veya satış sözleşmesinin gereklerinden kaynaklanan kişisel verileri satış sözleşmesini gereği gibi ifa etmek amacıyla otomatik olan yahut otomatik olmayan yollarla bir veri kayıt sisteminin parçası olmak üzere uhdesinde bulundurduğu,
- Ayrıca kredilendirmeye esas olarak senetle yapılan alışverişler için sözleşmenin kurulması ve ifasıyla doğrudan ilgili olan ilgili kişilere ait kişisel, mali ve ekonomik verilerin işlendiği, ilgili kişilerden istenen bu verilerin işleme ilkelerine tam olarak uyumlu olduğu,

Veri sorumlusu tarafından verilerin; kredilendirmeye esas teşkil etme, ilgili kişilerin kimlik bilgilerini, mali gücünü ve iletişim bilgilerini doğrulama, mal/hizmet satış süreçlerinin yürütülmesi, müşteri ilişkileri süreçlerinin yönetilmesi, sözleşme süreçlerinin yürütülmesi, talep/şikâyetlerin takibi, yetkili kişi, kurum ve kuruluşlara bilgi verilmesi, hukuk işlerinin takibi ve yürütülmesi amaçlarıyla işlendiği, saklandığı ve gerektiğinde imha edildiği,

- İnternet sitelerine üye olan kişilerin; ad-soyadı, iletişim, adres, parola, alışveriş bilgileri, ödeme yöntemleri bilgilerinin işlendiği, bu bilgilerin satış/pazarlama, pazarlama analiz çalışmalarının yürütülmesi, reklam/kampanya/promosyon süreçlerinin yürütülmesi, talep/şikâyetlerin takibi, ürün tanıtımı, hediye çeki, satış sözleşmesine hazırlık faaliyeti amaçlarıyla işlendiği, üye olmayıp yalnızca ziyaretçi olan kişilerin; IP adresi, site üzerinde gezinme bilgilerinin tanıtım yapmak, promosyonlar ve pazarlama teklifleri sunmak, sitenin içeriğini kullanıcılara göre iyileştirmek ve/veya tercihlerini belirlemek amacıyla işlendiği, alışveriş yapmak isteyen muhtemel müşteri/müşterilerin; ad-soyadı, iletişim, adres, parola, alışveriş bilgileri, ödeme yöntemleri, otomatik ödeme bilgilerinin satış/pazarlama, pazarlama analiz çalışmalarının yürütülmesi, reklam/kampanya/promosyon süreçlerinin yürütülmesi, talep/şikâyetlerin takibi, ürün tanıtımı, hediye çeki, satış sözleşmesine hazırlık faaliyeti amaçlarıyla işlendiği,

- Firmalarının mağaza satışlarının büyük kısmını oluşturan "Sözleşmeli Alışveriş"ler için internet üzerinden uygun bir ekran oluşturulmak istendiği, sözleşme ile alışverişin Türk Borçlar Kanununun (TBK) 8 inci maddesinde yer alan icaba davet niteliğinde bir faaliyet olduğu, bu alışveriş bakımından firmanın kendi iç bünyesinde kredilendirme çalışması yapıldığı, ilk olarak muhtemel müşteri ile iletişime geçilerek verilecek ürün ile ilgili ödeme gücünün tespit edildiği, internet sitesinde bulunan sözleşmeli satış ile ilgili olarak alınan verilerin yalnızca yukarıda belirtilen veriler olduğu, bunun haricinde e-Devlet şifresinin taraflarınca istenmediği ve ilgili alanın başkaca bir görselin parçası olduğu, format olarak dahi girilip doldurabilen bir alan olmadığı, jpg formatında olan bir alan olduğu ve taraflarınca fark edilmesiyle ivedilikle kaldırıldığı, bu alanda yer alan e-Devlet şifresi girişi için internet sitelerinde teknik donanım dahi bulunmadığı, bu hususla ilgili kurumun yapacağı her türlü denetime firmalarının açık olduğu, site üzerinde yer alan yazılımda ve veri tabanlarında bu hususa ilişkin hiçbir veri bulunmadığı, hiç kimsenin bu şekilde oldukça hassas ve kişiye özel olan verisinin işlenmediği, yalnızca icaba davet niteliğinde olacak şekilde genel nitelikli verilerin taraflarınca işlendiği ve kredilendirme yapma ve ödeme gücünün tespiti için iletişim numarasından kişi ile iletişime geçilerek bu şekilde kimlik doğrulaması yapıldığı, taraflarının e-Devlet şifresi alma gibi bir uygulaması bulunmadığından bu verilerle başkaca hiçbir verinin de elde edilmediği

belirilerek kişisel verilerin korunmasına ilişkin taraflarınca alınan idari ve teknik tedbirlerle ilgili başkaca bilgilere ve açıklamalara yer verilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulunun 17/02/2022 tarih ve 2022/137 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanununun “Tanımlar” başlıklı 3 üncü maddesinde; “kişisel veri”nin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi, “veri sorumlusu”nun, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi, “kişisel verilerin işlenmesi”nin ise kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı,

- Kanunun, kişisel verilerin işlenmesine ilişkin “Genel İlkeler”i düzenleyen 4 üncü maddesinin (1) numaralı fıkrasında, “Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.” hükmünün yer aldığı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkeler; hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işleme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,

- Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanunun “Veri Güvenliğine İlişkin Yükümlülükler” başlıklı 12 nci maddesinin (1) numaralı fıkrasında da “Veri sorumlusu; a) kişisel verilerin hukuka aykırı işlenmesini önlemek, b) kişisel verilere hukuka aykırı erişilmesini önlemek, c) kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.” hükmüne yer verildiği, mezkur maddenin (5) numaralı fıkrasında kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri sorumlusunun bu durumu en kısa sürede ilgisine ve Kurula bildireceğinin hüküm altına alındığı,
- Somut olayda veri sorumlusu tarafından internet sitesinde e-Devlet şifresinin talep edildiği alanın jpg formatında olduğu iddia edilmekle birlikte söz konusu internet sitesine ilişkin ekran görüntüsü incelendiğinde; Kasaya Git sekmesi altındaki sayfada kırmızı renk ile yazılmış “Dikkat Senetli alışverişte onay sürecinizin başarıyla tamamlanmasını istiyorsanız aşağıdaki alana e-Devlet şifrenizi giriniz. Siparişi Onaylıyorum butonuna basıldığında otomatik olarak doğrulama yapılacaktır.” bilgilendirmesinin yer aldığı ve e-Devlet şifresinin girilebildiği bir kutucuk ile SİPARİŞİ ONAYLIYORUM başlıklı bir bölüm olduğu, dolayısıyla, ihbar dilekçesi ekinde yer verilen ekran görüntüsünden yazı içeriğinde butona basılması ile otomatik olarak doğrulama yapılacağı belirtilmesi ve e-Devlet şifresinin girildiği bir alan olduğunun anlaşılması noktasından hareketle e-Devlet şifresi girileceği belirtilen alanın jpg formatında olmasının herhangi bir amaca hizmet etmeyeceği, nitekim veri sorumlusu da her ne kadar e-Devlet şifresinin taraflarınca istenmediğini, ilgili alanın başkaca bir görselin parçası olduğunu, doldurulamayacak ve jpg formatında bir alan olduğunu iddia etse de bu durumu tevsik edici bir belge sunmadığı, hatta ihbara konu ekran görüntüsünün taraflarınca fark edilmesiyle ivedilikle kaldırıldığını beyan ettiği,
- Bu kapsamda, ihbara konu ekran görüntüsünde yer alan sayfanın, veri sorumlusunun e-mağaza uygulamasında kontrolleri dışında görüntülenebilir olmasının mümkün olmayacağı, söz konusu olay bu şekilde vuku bulmuş olsa dahi bu durumun veri sorumlusunun kendi internet sitesinde gerçekleştirilmesi muhtemel kişisel veri işleme faaliyetlerinin kontrolünü sağlayamadığına, dolayısıyla gerekli teknik ve idari tedbirleri almadığına işaret ettiği, senetli alışverişlerde müşterilerin e-Devlet şifrelerinin temin edilmesi suretiyle, ilgili kişilerin e-Devlet kapısında kendileriyle ilgili yer alan her türlü bilgiye veri sorumlusunca erişilebilme tehlikesi ile karşı karşıya kalacakları,
- Öte yandan, söz konusu e-Devlet şifresinin bir anlam ifade edebilmesi için müşteriler tarafından öncelikle T.C. kimlik numarasının veri sorumlusuna sağlanmış olması gerektiği, veri sorumlusu tarafından üye olan kişilerin ad-soyadı, iletişim, adres, parola, alışveriş ve ödeme yöntemleri bilgilerinin işlendiği, alışveriş yapmak isteyen muhtemel müşteri/müşterilerin ise ad-soyadı, iletişim,

adres, parola, alışveriş, ödeme yöntemleri ve otomatik ödeme bilgilerinin işlendiği belirtilmekle birlikte Kuruma iletilen aydınlatma metinlerinde taraflarınca T.C. kimlik numarasının da alındığının beyan edildiği, bu hususa ilişkin olarak internet sitesinde yapılan incelemede Hesap Oluştur sayfasında üyelik için T.C. kimlik no, ad, soyadı, e-posta, telefon, adres (il, ilçe, mahalle, cadde, sokak, açık adres) ve parola bilgilerinin talep edildiği ve “TC Kimlik No bilgisi dışındaki diğer alanlar, Tc Kimlik No bilgisi girildikten sonra aktifleştirilecektir.” ifadelerine yer verildiği,

- Ayrıca, internet sitesine rastgele bir T.C. kimlik numarası ile üye olunmak istendiğinde “Girdiğiniz Tc kimlik numarası geçersizdir.” uyarısı ile karşılaşıldığı, söz konusu T.C. kimlik numaralarının geçerli ya da geçersiz olduğuna ilişkin doğrulamanın nasıl bir veri tabanı ile sağlandığının anlaşılamadığı,

- Üyelik oluşturma sayfasında T.C. kimlik numarası girilmesi gereken alanlara rastgele numaralar girilerek deneme yapıldığı, bu denemede ***** şeklinde bir numara girilmesi sonrasında aktifleşen alanlarda otomatik olarak A*** A*** İ*** Cad. S*** Sok. No:** bilgilerinin görüntülediği, bu şekilde birkaç tane daha deneme yapıldığı ve farklı kişilerin ad, soyadı ve adres bilgilerinin ekrana otomatik olarak yansıdığı, söz konusu T.C. kimlik numaralarının geçersiz olabileceği kanaatine varılmakla birlikte bu üyeliklerin veri sorumlusu tarafından doğrulama sistemi getirilmesi öncesinde müşteriler tarafından oluşturulan gerçek hesaplar veya veri sorumlusu tarafından deneme amaçlı oluşturulan hesaplar olabileceği,

- Söz konusu ihtimallere karşı geçerli bir T.C. kimlik numarası ile üyelik oluşturulduğu, sonrasında aynı T.C. kimlik numarasının hesap oluşturma sayfasına girildiği ve oluşturulan hesap bilgilerinin üyelik sayfasında otomatik olarak yer aldığı, buradan hareketle, yalnızca bir kişinin T.C. kimlik numarasını ve söz konusu sayfaya üye olduğunu bilen bir kişinin ilgili kişinin adres bilgilerine ulaşmasının olası olduğu,

- Bununla birlikte söz konusu güvenlik açığının veri sorumlusu nezdindeki kişisel verilere hukuka aykırı olarak üçüncü kişiler tarafından erişim sağlanmasına sebebiyet vermiş olduğu; ancak veri sorumlusu tarafından bu hususta Kanununun 12 nci maddesinin (5) numaralı fıkrası çerçevesinde Kurula bildirimde bulunma yükümlülüğünün yerine getirilmediği,

- Resen inceleme konusu çerçevesinde internette yapılan araştırmada; veri sorumlusunun internet sitesinden yaptıkları alışverişlerle ilgili yaşadıkları sorunları paylaşan farklı kişilerin olduğu, bu kişilerin şikâyetlerinde e-Devlet şifresini de veri sorumlusu ile paylaştıklarını ifade ettikleri ve bu durumdan endişe duyduklarının görüldüğü,

- Bu çerçevede resen incelemeye konu ihbar başvurusu, veri sorumlusu hakkında internet sayfalarında yer verilen şikâyetler ile veri sorumlusundan alınan bilgiler ışığında, veri sorumlusu tarafından ilgili kişilerden senetli alışveriş yapabilmek için e-Devlet şifresi, internet sayfasında üyelik oluşturabilmek için de T.C. kimlik numarası bilgisinin temin edilmesi suretiyle gerçekleştirilen kişisel veri işleme faaliyetlerinin Kanununun 5 inci maddesinin (2) numaralı fıkrasında yer alan veri işleme şartlarından herhangi birine dayanılmaksızın gerçekleştirildiği,
- Bununla birlikte, “T.C. kimlik numarası” ve “e-Devlet şifresi” bilgileri her ne kadar üye olmak ve/veya senetli alışveriş yapmak isteyen kişiler tarafından veri sorumlusu ile paylaşılıyor olması dolayısıyla, açık rıza kapsamında işleniyor gibi görünse de; açık rızanın Kanununun 3 üncü maddesinin (1) numaralı fıkrasının (a) bendinde ‘Belirli konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza’ şeklinde tanımlandığı, buna göre, açık rızanın ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı şeklinde anlaşılması gerektiği, rızanın özgür iradeyle verilmiş olmasının kişilerin verileri üzerinde kontrol hakkına sahip olması ve bireylere gerçek bir seçim hakkının tanınmış olması ile sağlandığı, birey rıza vermemenin sonucunda hizmetten yararlanamıyor ise yani reddin bir yaptırımını var ise bu bireyin karar verme mekanizmasını etkileyecek bir duruma sebebiyet verebileceği, somut olayda online bir alışveriş sitesine üye olmak ve senetli alışveriş yapmak için alınan kişisel verilerin sözleşmenin gerektirdiği nitelikteki verileri aşacak nitelikte olduğu, bu bilgiler verilmeden üye olunup, senetli alışveriş yapılamıyorsa (Veri Sorumlusunun hesap oluşturma sayfasında yer alan bilgi: “TC Kimlik No bilgisi dışındaki diğer alanlar, Tc Kimlik No bilgisi girildikten sonra aktifleştirilecektir.”, veri sorumlusunun Kasaya Git sekmesinde yer alan bilgi: Dikkat Senetli alışverişte onay süreciniz başarıyla tamamlanmasını istiyorsanız aşağıdaki alana e-Devlet şifrenizi giriniz.), bu durumda hizmetin sunumunun bu bilgilerin verilmesi yönündeki bir rızaya bağlandığı, burada bireyin üyeliği oluşturmak ve sonrasında sunulacak hizmetlerden yararlanabilmek için başka bir seçeneği bulunmadığı ve bireye gerçek bir seçim hakkı sunulmadığı, sonuç olarak, ilgili kişiler tarafından e-Devlet şifresi ve T.C. kimlik numarasının söz konusu internet sayfasına üye olabilmek ve senetli alışveriş yapabilmek için zorunlu bilgi olarak talep edilmesi neticesinde vermiş olabileceği rızasının geçerli bir rıza olmayacağı, bu çerçevede, ilgili kişilerden senetli alışverişlerde e-Devlet şifresinin, internet sayfasında üyelik oluşturulması için ise T.C. kimlik numarasının paylaşılmasının zorunlu kılınması suretiyle gerçekleştirilen kişisel veri işleme faaliyetlerinin Kanununun 5 inci maddesinde yer alan veri işleme şartlarına dayanılmaksızın gerçekleştirildiği,

• Öte yandan, veri sorumlusu tarafından kredilendirmeye esas olarak senetle yapılan alışveriş için ilgili kişilere ait sözleşmenin kurulması ve ifasıyla doğrudan ilgili olan kişisel, mali ve ekonomik verilerin işlendiği, verilerin ilgili kişilerin mali gücünü doğrulama amacıyla işlendiği, veri sorumlusu tarafından işlenen verilerin kanundan ve işin gereklerinden kaynaklanan veriler olduğu, muhtemel müşteri ile iletişime geçilerek verilecek ürün ile ilgili ödeme gücünün tespit edildiği gibi genel nitelikte ve muğlak ifadelerle yer verildiği görülmekte olup bu kapsamda ilgili kişilerin hangi verilerinin, Kanunda yer alan hangi veri işleme şartına dayalı olarak işlendiğinin anlaşılamadığı, bu kapsamda, veri sorumlusu her ne kadar sözleşmenin kurulması ve ifasıyla doğrudan ilgili olan veriler olduğunu iddia etse de ödeme gücü tespit edilmeksizin de sözleşmenin kurulmasının mümkün olabileceği ile söz konusu ödemenin aksaması/yapılmaması halinde hukuki yollara başvurulması suretiyle ödemenin yapılmasının sağlanabileceği kanaatine varıldığı, diğer bir deyişle, veri sorumlusu tarafından ilgili kişilerin ekonomik durumuna ilişkin kişisel verilerin işlendiği ve söz konusu verilerin işlenmesinin hukuka uygunluğu noktasında belirsizlik bulunduğu tespit ve değerlendirmelerinden hareketle;

• Veri sorumlusu tarafından senetli alışverişler için ilgili kişilerden e-Devlet şifresinin, internet sayfasında üyelik oluşturulması için de T.C. kimlik numarasının temin edilmesinin zorunlu kılınması suretiyle gerçekleştirilen kişisel veri işleme faaliyetlerinin Kanunun 5 inci maddesinde yer alan veri işleme şartlarından herhangi birine dayanılmaksızın gerçekleştirildiği, öte yandan veri sorumlusunun internet sitesindeki üyelik başvurusu ile ilgili sayfada T.C. kimlik numarası girilmek suretiyle daha önce internet sayfasına üye olan kişilerin kişisel verilerinin üçüncü kişilerce görüntülenebilir olması hususunun veri güvenliği açığına işaret ettiği sonucuna varılmakta olup bu hususların Kanunun 12 nci maddesinin (1) numaralı fıkrasına aykırılık teşkil etmesi nedeniyle, kişisel verilerin işlenmesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri alma yükümlülüğünü yerine getirmeyen veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 300.000 TL idari para cezası uygulanmasına,

• Veri sorumlusunun, bugüne kadar sözlü görüşmeler ve/veya internet sitesi aracılığıyla ilgili kişilerden temin ettiği e-Devlet şifrelerini ve T.C. kimlik numaralarını Kanunun 7 nci maddesine ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğe uygun bir biçimde imha etmesi ve imha işlemlerinin yapıldığını kanıtlar nitelikteki belgeler (log kaydı gibi) ile birlikte Kurula bilgi vermesi hususunda talimatlandırılmasına,

• Veri sorumlusunun internet sitesinde hesap oluşturma sayfasında sisteme daha önce üye olmuş kişilerin kişisel verilerinin görüntülenmesine sebebiyet veren güvenlik açığının ivedilikle giderilmesi,

T.C. kimlik numarası temin edilmeksizin üyelik oluşturulabilmesi adına sistemin güncellenmesi ile bu işlemlere ilişkin Kurula en geç otuz gün içinde bilgi verilmesi yönünde veri sorumlusunun talimatlandırılmasına,

- Öte yandan, söz konusu güvenlik açığının veri sorumlusu nezdindeki kişisel verilere hukuka aykırı olarak üçüncü kişiler tarafından erişim sağlanmasına sebebiyet vermiş olduğu; ancak veri sorumlusu tarafından bu hususta Kanunun 12 nci maddesinin (5) numaralı fıkrası çerçevesinde Kurula bildirimde bulunma yükümlülüğünün yerine getirilmediği dikkate alındığında, konuya ilişkin olarak Kanunun 15 inci maddesinin (1) numaralı fıkrası çerçevesinde resen inceleme başlatılmasına karar verilmiştir.

2022/107 sayılı KVKK Kararı

Bir tasarruf finansman şirketi tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmaksızın işlenmesi ve ilgili numaraya reklam içerikli SMS gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 10/02/2022 tarihli ve 2022/107 sayılı Karar Özeti

Karar Tarihi : 10/02/2022

Karar No : 2022/107

Konu Özeti: Bir tasarruf finansman şirketi tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmaksızın işlenmesi ve ilgili numaraya reklam içerikli SMS gönderilmesi

İlgili kişi tarafından Kuruma iletilen şikayet dilekçesinde özetle; veri sorumlusu bir tasarruf finansman şirketince kendisine birkaç kez kısa mesaj gönderildiği, bunun üzerine ilgili kişi tarafından kişisel verisi niteliğindeki cep telefonu numarasının açık rızası olmadan ne şekilde elde edildiği, nasıl ve hangi amaçla işlendiğine dair bilgi edinmek amacıyla veri sorumlusuna başvurulduğu, veri sorumlusu tarafından verilen cevapta özetle İleti Yönetim Sistemi (İYS) adı verilen sisteme kayıtlı kurumsal bir firma olduğunun, bu sisteme üyelerin rızası dahilinde veri girişi yapıldığının, istenildiği zaman İYS sisteminden çıkılabildiğinin, söz konusu mesaj içeriğinde ret imkanının bulunduğu ve sistemde kayıtlı ilgili kişiye ait telefon numarasının SMS gönderimine kapatıldığının belirtildiği, veri sorumlusu tarafından verilen cevapta belirtildiğinin aksine ilgili kişi tarafından İYS aracılığıyla veri sorumlusuna herhangi bir açık rıza veya onay verilmediği, ilgili kişinin kişisel verilerinin nasıl, hangi amaçlarla işlendiği ve kişisel verilerinin açık rızası olmadan işlenmesi konularında yeterli cevap verilmemesi ve kişisel veri güvenliğinin sağlanması konusunda yükümlülüğünün yerine getirilmemesi nedeniyle kişisel verilerinin 6698 sayılı Kişisel Verilerin Korunması Kanunu'na (6698 sayılı Kanun) aykırı olarak işlendiği ifade edilerek şirket hakkında Kanun kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun (6563 sayılı Kanun) uyarınca çıkarılan Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik'in (Yönetmelik) Geçici 2'nci

maddesinin (1) ve (2) numaralı fıkraları kapsamında İYS sistemine bildirdiği kayıtlar arasında ilgili kişinin telefon numarasına ilişkin kaydın da bulunduğu, ilgili kişinin anılan Yönetmelik'te belirtilen 16.01.2021 tarihine kadar İYS üzerinden veya ayrı bir kanaldan şirkete bildirdiği aksi yönde bir beyanının veri sorumlusu tarafından tespit edilemediği, bu durumda Yönetmelik uyarınca ilgili kişi tarafından verilmiş bu tarihten önceki onayın geçerli sayıldığı,

- Yönetmelik'in ilgili geçici maddesi uyarınca şirkete tanınan istisna düzenlemesine göre 16.01.2021 tarihine kadar bu izni kaldırdığını ispat yükünün ilgili kişinin üzerinde kaldığı,
- Yönetmelik hükümlerine uygun olarak ilgili kişinin cep telefonu numarasının ticari ileti gönderilmek amacıyla 6698 sayılı Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (a) bendi uyarınca "kanunlarda açıkça öngörülmesi" işleme şartına dayalı olarak işlendiği,
- Yönetmelik'in 13'üncü maddesinin (2) numaralı fıkrasında şirket gibi hizmet sağlayıcılara ticari iletişime ilişkin kayıtları 3 yıl süreyle saklama yükümlülüğü getirildiği,
- Şirketin, ilgili kişiden gelen talep üzerine yalnızca SMS gönderim faaliyetine son verdiği, bunu da ilgili kişiye verdiği cevabında açıkça belirtmiş olduğu,
- İlgili kişinin kayıtlarına bakıldığında kendisinin şirkete başvurduğu tarihte henüz SMS ret talebinde bulunmadığı, ilgili kişinin Kuruma şikayette bulduktan sonra dahi SMS onayı olduğunun görüldüğü, ilgili kişi tarafından verilen onaya ilişkin retlerin sonraki tarihte sisteme girildiği ifade edilmiştir.

Konuya ilişkin olarak yapılan incelemede Kişisel Verileri Koruma Kurulunun 10/02/2022 tarihli ve 2022/107 sayılı Kararı ile;

- Kanun'un "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, "belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza", (ç) bendinde ilgili kişinin, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel verinin, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesinin, "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusunun, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi" olarak tanımlandığı,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi; fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin kendisi tarafından alenileştirilmiş olması; bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hükmünün yer aldığı,
- Ticari elektronik iletiye ilişkin ayrı bir mevzuat bulunmakla birlikte somut olayda olduğu gibi ilgili kişiye ait cep telefon numarasının bir veri kayıt sisteminde depolanması suretiyle ticari nitelikli iletiler gönderilmesinin, bir kişisel veri işleme faaliyeti olduğu, dolayısıyla ticari nitelikli bir elektronik iletinin ticari elektronik ileti gönderilmesine ilişkin mevzuata uygun olarak gönderilmesi gerekmektedir birlikte, bu mesajların iletilmesi için kullanılan iletişim numarasının kişisel veri niteliğinde olması nedeniyle ticari elektronik iletilerin gönderilmesi süreçlerinin aynı zamanda kişisel verilerin korunması mevzuatına da uygun olması gerektiği,
- 6563 sayılı Kanun'un 11'inci maddesinin (4) numaralı fıkrasına göre Bakanlık'ın, ticari elektronik ileti onaylarının alınmasına ve reddetme hakkının kullanılmasına imkân tanıyan bir elektronik sistem kurmaya veya kurdurmaya yetkili olduğu, bu Kanun çerçevesinde alınan onayların Bakanlıkça belirlenen süre içinde sisteme aktarılması gerektiği, sisteme aktarılmayan onayların geçersiz kabul edileceği, alıcıların, sisteme kaydedilen onayları Bakanlıkça belirlenen süre içinde kontrol edeceği, bu sürenin bitiminden sonra gönderilen ticari elektronik iletilerin onaylı kabul edileceği, alıcılar tarafından reddetme hakkının bu sistem üzerinden kullanılacağı, sistemin kurulması, onayların sisteme aktarılması, saklanması, reddetme hakkının sistem üzerinden kullanılması ve sistemin işleyişine ilişkin diğer usul ve esasların yönetmelikle belirleneceği,
- Veri sorumlusu tarafından ilgili Yönetmelik'in "Mevcut veri tabanlarının İYS'ye yüklenmesi" başlıklı Geçici 2'nci maddesinin (2) numaralı fıkrası dikkate alındığında şirketin İYS sistemine bildirdiği kayıtlar arasında ilgili kişinin telefon numarasının bulunduğu ve ilgili kişi tarafından verilen onayın geri alınmasının Kuruma şikayet tarihinden sonra sisteme girildiğinin belirtildiği

ancak ilgili kişinin iddialarına karşı veri sorumlusu tarafından sunulan bilgi ve belgeler değerlendirildiğinde, ilgili kişinin cep telefonu numarasının İYS sistemine kaydının yapılmasına temel teşkil edecek nitelikte ilgili kişinin veri sorumlusu ile bir ilişkisinin olduğunun tespit edilemediği veya veri sorumlusunun sunduğu bilgi ve belgeler arasında, ilgili kişinin kişisel verisinin işlenmesi hususunda açık rızasının olduğuna ilişkin tevsik edici bilgi veya belge olmadığının tespit edildiği,

- Diğer taraftan ilgili kişi tarafından Kuruma yapılan şikâyetinde, kişisel verilerinin güvenliğinin sağlanması konusunda veri sorumlusunun yükümlülüklerini yerine getirmemesi (örneğin kişisel verinin başkasına aktarılması vb.) nedeniyle kişisel verilerinin Kanun'a aykırı işlendiği iddia edilmiş olsa da veri güvenliğine ilişkin bu hususun Kanun'un 11'inci maddesi kapsamında olmadığı ve ihlale ilişkin tevsik edici bilgi ve belge sunulmadığı

değerlendirmelerinden hareketle;

Somut olayda, veri sorumlusu tarafından sunulan bilgi ve belgeler çerçevesinde

- İYS sistemine kaydının yapılmasına temel teşkil edecek nitelikte ilgili kişinin veri sorumlusu ile bir ilişkisinin olduğunun tespit edilemediği veya veri sorumlusu tarafından ilgili kişinin kişisel verisinin işlenmesi hususunda açık rızasının olduğunun tevsik edilemediği dikkate alındığında, Kanun'un 12'nci maddesinin (1) numaralı fıkrası çerçevesinde gerekli teknik ve idari tedbirleri almadığı kanaatine varılan; veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 75.000 TL idari para cezası uygulanmasına,

- Hukuka aykırı işlendiği tespit edilen söz konusu kişisel verinin, başka bir işleme sebebi bulunmaması halinde, Kanun'un 7'nci maddesi ile Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında Yönetmelik hükümlerine uygun şekilde imha ederek sonucundan Kurula bilgi vermesi hususunda veri sorumlusunun talimatlandırılmasına,

- İlgili kişinin şikâyetinde belirttiği, veri sorumlusunun kişisel verilerinin güvenliğinin sağlanması konusundaki yükümlülüklerini yerine getirmediği iddialarının Kanun'un 11'inci maddesi kapsamında olmadığı dikkate alındığında bu hususta Kanun kapsamında yapılacak bir işlem olmadığına

karar verilmiştir.

2022/103 sayılı KVKK Kararı

Unvanında ilgili kişinin adının geçtiği bir şirket hakkında başlatılan icra takibine ilişkin dosya içeriğinin sosyal medyada paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 10/02/2022 tarihli ve 2022/103 sayılı Karar Özeti

Karar Tarihi : 10/02/2022

Karar No : 2022/103

Konu Özeti : Unvanında ilgili kişinin adının geçtiği bir şirket hakkında başlatılan icra takibine ilişkin dosya içeriğinin sosyal medyada paylaşılması

Kurum'a intikal eden şikâyet dilekçesinde özetle; bir tekstil firması (veri sorumlusu) ile yapılan alışveriş sonrasında veri sorumlusu tarafından ilgili kişinin adının geçtiği yedek parça şirketi (Şirket) hakkında icra takibi başlatıldığı, bu süreçte bir şahıs tarafından Facebook üzerinden herkese açık olan bir grupta "Şirketin aldığı maskelerin ödemesini yapmadığı, dolandırıcı olduğu, bu doğrultuda Şirket hakkında icra takibi başlatıldığı ve icraya ilişkin evrakların bu grupta paylaşılacağı" hususlarında herkese açık bir yorum yapıldığı, paylaşımı yapan şahıs adına internette yapılan araştırmalar neticesinde veri sorumlusu firmanın muhatabı olarak tanındığının tespit edildiği, bahsi geçen şahısla ilgili kişinin hiçbir ticari ilişkisi olmamasına rağmen icra dosyası içerisinde yer alan kişisel verilerinin üçüncü kişilerle paylaşılması suretiyle kişilik haklarının ihlal edildiği, veri sorumlusu firmanın ticaret sicil kaydında ismi geçmeyen ancak kendisini firma yetkilisiymiş gibi tanıtan söz konusu şahıs tarafından icra dosyası hakkında nasıl bilgi edinildiğinin anlaşılamadığı, bu hususta 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 11'inci maddesi kapsamındaki hakları uyarınca veri sorumlusuna başvuruda bulunulduğu ancak süresi içinde bir yanıt alınmadığı ifade edilerek, veri sorumlusu hakkında gereğinin yapılması talep edilmiştir.

Şikâyet dilekçesinde yer alan hususlara ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup verilen cevabî yazıda özetle;

- İlgili kişinin adının geçtiği Şirketin, şikâyete konu sosyal medya paylaşımlarına ilişkin Cumhuriyet Savcılığına intikal eden şikâyette taraf olduğu, şikâyete konu tarafın şahıs olmaması tüzel kişi olması

dolayısıyla ve suçun yasal unsurlarının oluşmadığı gerekçesiyle hakaret suçundan kovuşturma yapılmasına yer olmadığına karar verildiği,

- Savcılığa intikal eden şikâyete konu paylaşımları yapan şahsın o tarihlerde ilgili kişinin adının geçtiği şirketin yarı zamanlı çalışanı olduğu sonradan firmadan ayrıldığı, akabinde veri sorumlusu nezdinde çalışmaya başladığı,
- Şikâyetçi tarafın veri sorumlusu firmadan yüksek miktarda mal aldığı, bu süreçte Şirketin paylaşımları yapan şahsın müşterisi olduğu, ilgili ürünleri pazarlayan, sunan ve siparişi alanın da bu kişi olduğu, diğer bir ifade ile Şirketin bu şahsın portföyünde bulunduğu,
- Şirketin söz konusu mal alımına ilişkin ödeme yapmadığı, e-postalara ve telefonlara yanıt vermediği, Şirketle hiçbir şekilde irtibat sağlanamadığı, bunun üzerine Şirket hakkında icra takibi başlatıldığı,
- Veri sorumlusu adına açılmış sosyal medya hesaplarının bulunmadığı ve veri sorumlusunun unvanı altında paylaşım yapılmadığı,
- Bahsi geçen şahıs bu pazarlamadan çok zarar gördüğü için diğer firmaların da bu Şirketten zarar görmemesi adına üyesi olduğu bir Facebook grubunda ilgili kişinin adının geçtiği Şirket ile yaşanan durumu kısaca izah ettiği, ispat olarak dava dosyasının ön kapak görselini okunmayacak şekilde paylaştığı, ancak bu paylaşımın yayımlanmadan silindiği ve üçüncü şahısların söz konusu paylaşımı görmediği, olay sonrasında bahsi geçen şahsın gruptan çıkarılarak engellendiği

ifade edilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 10/02/2022 tarih ve 2022/103 sayılı kararı ile;

- Kanunun "Tanımlar" başlıklı 3'üncü maddesinde "kişisel veri"nin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi; "ilgili kişi"nin kişisel verisi işlenen gerçek kişi, "veri sorumlusu"nun kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi; "kişisel verilerin işlenmesi"nin ise kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı,

• 95/46/AT sayılı Veri Koruma Direktifine dayalı olarak hazırlanan ve “kişisel veri kavramı”nın ele alındığı Madde 29 Veri Koruma Çalışma Grubu’nun 04.06.2007 tarihli ve 4/2007 sayılı görüşünde; tüzel kişiler hakkında bilginin gerçek kişilerle “ilişkili olması” durumunun somut olay özelinde göz önünde bulundurulması gerektiği, tüzel kişilerin unvanının gerçek kişi isimlerinden türetildiği durumda kişisel veri olup olmadığının belirli kriterlere (içerik, amaç ve sonuç kriterlerine) göre değerlendirilmesi gerektiğinin belirtildiği, Madde 29 Veri Koruma Çalışma Grubu’nun söz konusu görüşü ile örneğin, bir şirket e-postasının belirli bir çalışan tarafından kullanılmasında veya küçük bir işletmenin sahibinin davranışlarını ifade eden bilgide bu durumun söz konusu olabileceği, “içerik”, “amaç” veya “sonuç” kriterlerine göre değerlendirildiğinde, işletme veya tüzel kişi hakkında bilginin gerçek kişiyle ilişkili olması mümkünse kişisel veri olarak düşünülebileceğinin ifade edildiği, söz konusu kriterlerin kümülatif olarak bulunmasının gerekli olmadığı, kriterlerin birbirinin alternatifi olarak düşünülebileceği, söz konusu görüşe göre; aynı bilginin aynı zamanda farklı unsurlar bakımından farklı kişilerle ilişkilendirileceğinin de değerlendirildiği, örneğin bir bilgi A kişisi hakkında ise içerik kriteri bakımından A kişisiyle, B kişisine belirli bir şekilde davranılması amacıyla kullanılması durumunda amaç kriteri bakımından B kişisiyle, C kişinin hak ve menfaatlerinde bir etkiye sahipse veya herhangi bir etkiye sahip olması muhtemelse “sonuç” kriteri bakımından C kişisiyle ilişkili olduğunun söylenebileceği,

• İlgili şirketin, yetkilisinin ismini ve soy ismini taşıdığı, somut olay özelinde şirket unvanının, Kanun’un 3’üncü maddesinin (1) numaralı fıkrasının (d) bendi uyarınca kişisel veri olup olmadığının göz önünde bulundurulması gerektiği, icra takibi evrakında bulunan tacirin unvanında ilgili kişinin isim ve soy ismi bulunsa da yapılan paylaşım ve yorumlarda tüzel kişiliğin hedeflendiği göz önünde bulundurulduğunda şirketin unvanının veya borç bilgisi, adresi, vergi kimlik numarası bilgisinin gerçek kişinin hak ve menfaatlerinde bir etkiye sahip olmadığı ya da gerçek kişiye belirli bir şekilde davranılması amacıyla kullanılmadığı kanaatiyle Kanun’da yer alan kişisel veri tanımını karşılamadığı,

• Kanun’un 2’nci maddesinin (1) numaralı fıkrası uyarınca, Kanun hükümlerinin kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanacağı,

• Somut olay özelinde, veri sorumlusunun çalışanı tarafından icra takip talebi evrakının fotoğraflanması suretiyle elde edilerek sosyal medya platformu aracılığıyla paylaşılması ile Şirket’e ait bazı bilgileri içeren yorumların sosyal medya platformunda paylaşılmasında, kişisel veri

işlenmemesi sebebiyle konunun Kanun'un 2'nci maddesinin (1) numaralı fıkrası uyarınca Kanun kapsamında olmadığı

değerlendirmelerinden hareketle;

- Her ne kadar şikâyete konu edilen Şirket adında ilgili kişinin ad ve soyadı geçse de, sosyal medyada yapılan paylaşımlarda tüzel kişiliğin hedeflendiği anlaşıldığından söz konusu veri gerçek kişiye değil tüzel kişiliğe ait veri olarak değerlendirildiğinden şikâyet konusunun Kanun kapsamında olmadığı kanaatine varılması nedeniyle yapılacak bir işlem olmadığına

karar verilmiştir.

2022/31 sayılı KVKK Kararı

Sağlık sektöründe faaliyet gösteren veri sorumlusu tarafından ilgili kişinin kişisel verilerinin açık rızası alınmaksızın ticarî elektronik ileti gönderilmesi amacıyla işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 18/01/2022 tarihli ve 2022/31 sayılı Karar Özeti

Karar Tarihi : 18/01/2022

Karar No : 2022/31

Konu Özeti : Sağlık sektöründe faaliyet gösteren veri sorumlusu tarafından ilgili kişinin kişisel verilerinin açık rızası alınmaksızın ticarî elektronik ileti gönderilmesi amacıyla işlenmesi

İlgili kişinin Kuruma intikal eden şikâyetinde özetle;

- e-posta adresine sağlık sektöründe faaliyet gösteren veri sorumlusu tarafından ticarî içerikli bir ileti gönderildiği, bu durumun 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'un (6563 sayılı ETK) 6'ncı maddesinin (1) numaralı fıkrasındaki "Ticarî elektronik iletiler, alıcılara ancak önceden onayları alınmak kaydıyla gönderilebilir..." hükmüne aykırılık teşkil ettiği,
- Öte yandan kişisel verilerin hukuka uygun olarak işlenebilmesi için 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (6698 sayılı Kanun) 5'inci maddesinin (1) numaralı fıkrası gereği ilgili kişinin açık rızasının alınmasının veya aynı maddenin (2) numaralı fıkrasında sayılan açık rızanın aranmadığı özel şartlardan birinin sağlanmasının gerektiği, ancak somut hadisede ne kendisinin açık rızasının alındığı ne de 6698 sayılı Kanun'da gösterilen özel şartların sağlandığı,
- 6698 sayılı Kanun'un 12'nci maddesinin (1) numaralı fıkrasının (a) bendinde; veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri almak zorunda olduğunun belirtildiği ancak kişisel verilerinin e-posta adresine ileti gönderilmek suretiyle işlenmesinden ötürü bu hükmün ihlal edildiğinin ortada olduğu,
- Veri sorumlusu tarafından ilgili kişiye verilen cevapta 6563 sayılı ETK ve Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik kapsamında herhangi bir bilgiye yer verilmediğinden, kampanya ve reklamcılık faaliyetleri çerçevesinde ticari elektronik ileti gönderimine ilişkin yapılan savunmanın yerinde olmadığı

hususları ifade edilmiş ve 6698 sayılı Kanun hükümleri uyarınca gerekli işlemlerin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusunun savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişinin e-posta adresinin, kendisi tarafından veri sorumlusunun şubesine başvuru yapması sonucunda elde edildiği ve bu bilginin hasta kayıt sürecinde Hastane Bilgi Yönetim Sistemi'ne (HBYS) kayıt edildiği,
- Bu veri işleme faaliyetinin, 6698 sayılı Kanun'un 5'inci maddesi uyarınca, ilgili kişi ile hastane arasında akdedilen sözleşme sebebiyle "bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması" şartına ve 2219 sayılı Hususi Hastaneler Kanunu ile 3359 sayılı Sağlık Hizmetleri Temel Kanunu uyarınca "veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için (veri işlemenin) zorunlu olması" şartına dayalı olarak gerçekleştirildiği,
- İlgili kişinin e-posta adresinin HBYS ve hastaneler arası iletişim ortamı olan MEDULA yazılımı aracılığı ile Sosyal Güvenlik Kurumu (SGK) sistemlerine aktarıldığı,
- İlgili kişinin başvurusuna verilen yanıtta belirtildiği üzere, söz konusu e-posta gönderiminin birimler arasındaki geçici koordinasyon eksikliğinden kaynaklandığı ve sehven ilgili kişinin onayı dışında gerçekleştiği,
- Mevcut durumun bir daha tekrar etmemesi adına, ilgili kişinin e-posta adresinin, kendisinin talebi üzerine, ticari elektronik ileti gönderimine onay veren kişiler listesinden çıkarıldığı ve ilgili kişiye bir daha e-posta gönderilmeyeceğinin taahhüt edildiği,
- İlgili personele uyarı yazısının verilmiş olmasının yanı sıra birtakım başka ek tedbirlerin de alındığı, örneğin artık hasta kaydı sırasında kişilerin HBYS kaydının tamamlanabilmesi ve aydınlatma yapılabilmesi adına, hasta kayıt işlemi yaptıran ilgili kişi alıcılara SMS gönderilmesi uygulamasına başlandığı, bahse konu SMS içeriğinde 6698 sayılı Kanun ile 6563 sayılı ETK kapsamında onay vermek isteyen ilgili kişiler için ayrı ayrı, iki adet tek kullanımlık onay kodunun yer almakta olduğu, bu kodların personele iletilmesi durumunda 6698 sayılı Kanun ve 6563 sayılı ETK kapsamında açık rıza ve onay alındığına dair HBYS üzerinde kayıt oluşturulduğu,
- Bununla birlikte, ilgili kişilerin hastaneye vermiş oldukları e-posta adresini doğrulamak üzere yeni bir sistemin ilerleyen süreçte kullanıma alınacağı, buna göre ilgili kişilerin vermiş oldukları e-posta

adresini doğrulamak üzere kendilerine doğrulama linki içeren bir e-posta gönderileceği, bu linke tıklanmaması halinde ilgili kişinin e-posta adresinin HBYS kayıtlarına alınmayacağı,

- Tüm bunların dışında; veri sorumlusunun hastanelerini ziyaret eden hastalara ait kişisel verilerin işlenmesini detaylıca ele alan aydınlatma metninin daha kapsamlı hale getirilerek veri sorumlusunun internet sitesinde yayınlandığı, ilgili kişilerle reklam amaçlı iletişime geçilmesine olanak tanıyan Misafir İletişim Açık Rıza Beyanı belgesinin düzenlenerek ilgili kişilere sunulduğu, personel eğitimlerine devam edildiği ve eğitim içeriklerinin Kurulun güncel kararları doğrultusunda periyodik olarak güncellendiği, veri sorumlusuna bağlı hastaneler ve genel merkezde faaliyet gösteren Kişisel Verilerin Korunması ve Bilgi Güvenliği Kurulunun teşkil edildiği, bu Kurula seçilenler için özel bir Görevlendirme ve Taahhütname belgesi hazırlandığı,

- Kişisel Verileri İşleme ve İmha Politikası başta olmak üzere tüm politikaların yeni ihtiyaçlar doğrultusunda güncellendiği

belirtmiştir.

Konuya ilişkin yürütülen inceleme neticesinde, Kişisel Verileri Koruma Kurulunun 18/01/2022 tarih ve 2022/31 sayılı Kararı ile;

- Kanun'un amacının kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek olduğu, Kanun'un "Tanımlar" başlıklı 3'üncü maddesinde "ilgili kişi"nin, kişisel verisi işlenen gerçek kişi; "veri sorumlusu"nun ise kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlandığı,

- Kanun'un, kişisel verilerin işlenmesine ilişkin "Genel İlkeler"i düzenleyen 4'üncü maddesinin (1) numaralı fıkrasında, "Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir." hükmünün yer aldığı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin;

a) Hukuka ve dürüstlük kurallarına uygun olma,

b) Doğru ve gerektiğinde güncel olma,

c) Belirli, açık ve meşru amaçlar için işlenme,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme

şeklinde sayıldığı,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işleminin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanun'un "Veri Güvenliğine İlişkin Yükümlülükler"i düzenleyen 12'nci maddesinin (1) numaralı fıkrasında veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idarî tedbirleri almak zorunda olduğunun hükme bağlandığı,

- İlgili kişinin şikâyeti hakkında veri sorumlusu tarafından "İlgili kişinin e-posta adresinin, kendisi tarafından veri sorumlusunun şubesine yapılan başvuru sırasında, hasta kaydı açılırken elde edildiği" bilgisinin verildiği,

- Bu durumun ise 6698 sayılı Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (c) bendinde yer alan "Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması" hükmü ile (ç) bendinde yer alan "Veri sorumlusunun hukukî yükümlülüğünü yerine getirebilmesi için zorunlu olması" hükmüne istinaden gerçekleştirildiğinin ifade edildiği,

- Hasta kaydı açılması sırasında ilgili kişinin veya refakatçilerinin iletişim bilgilerinin temin edilmesinin, 6698 sayılı Kanun ile birlikte diğer sair mevzuata da bir aykırılık teşkil etmediği, ancak somut hadisede ilgili kişinin iletişim bilgisinin, herhangi bir tıbbî bilginin kendisine veya yakınına iletilmesi için değil bir pazarlama faaliyetinde bulunmak amacıyla kullanıldığı, ilgili kişiye gönderilen e-posta içeriğinin bilgilendirme ve ticarî amaçlı olduğunun görüldüğü,

- 6698 sayılı Kanun'un 4'üncü maddesinin (2) numaralı fıkrasının (ç) bendinde, kişisel verilerin işlendikleri amaçla sınırlı, bağlantılı ve ölçülü şekilde işlenebileceğinin açıkça belirtildiği, veri sorumlusunun hasta kaydı açılırken ilgili kişiden iletişim bilgilerini temin etmesi hukuka uygun olsa da bahse konu olayda kişisel verilerin temin edildikleri andaki elde etme amacıyla bağlantısız bir şekilde e-posta adresine ticari amaçlı e-posta gönderilmesi suretiyle işlenmeleri nedeniyle ilgili hükmün ihlal edildiğinin görüldüğü

değerlendirmelerinden hareketle;

- İlgili kişinin kişisel verilerinin veri sorumlusu tarafından temin edilmesi hukuka uygun olsa da söz konusu kişisel verilerin elde edilme amaçlarıyla alakalı olarak kullanılmamasından ötürü şikâyet edilen veri işleme faaliyetinin hukuka aykırı olduğu, bu kapsamda veri sorumlusu tarafından bir veri işleme şartı olmaksızın ilgili kişinin e-posta adresine reklam ve pazarlama amacıyla bildirim gönderilmesi suretiyle kişisel verisinin işlenmesi sebebiyle 6698 sayılı Kanun'un 12'nci maddesinin (1) numaralı fıkrasının (a) bendi çerçevesinde kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli tedbirleri almadığı kanaatine varılan veri sorumlusu hakkında 6698 sayılı Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 100.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2022/13 sayılı KVKK Kararı

Yerel bir haber sitesi tarafından ilgili kişinin açık rızası olmaksızın sınav sonuç belgesinin paylaşılmasına ilişkin Kişisel Verileri Koruma Kurulunun 06/01/2022 tarihli ve 2022/13 sayılı Karar Özeti

Karar Tarihi : 06/01/2022

Karar No : 2022/13

Konu Özeti : İlgili kişinin açık rızası olmaksızın sınav sonuç belgesinin yerel bir haber sitesi tarafından paylaşılması

Kuruma intikal eden şikâyette; ilgili kişinin kişisel verisi niteliğindeki bilgilerinin yer aldığı Yükseköğretim Kurumları Sınavı (YKS) sınav sonuç belgesinin yerel haber sitesi tarafından açık rızası olmaksızın paylaşıldığı, kişisel verilerinin bu şekilde hukuka aykırı olarak işlenmesi sebebiyle 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) gereği veri sorumlusuna başvurarak bilgi talebinde bulunduğu, söz konusu başvurunun tebliğ edilmesine karşın başvurunun yanıtı bırakıldığı ifade edilerek konuya ilişkin Kanun kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde söz konusu iddialara ilişkin veri sorumlusundan savunması istenilmiş olup veri sorumlusu tarafından Kuruma herhangi bir cevap verilmemiştir.

Bu itibarla yapılan incelemede, Kişisel Verileri Koruma Kurulunun 06/01/2022 tarihli ve 2022/13 sayılı Kararı ile;

- Kanunun “Kişisel verilerin işleme şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise sayılan şartlardan birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğunun hüküm altına alındığı,
- Şikâyetin incelemeye alındığı tarihte veri sorumlusuna ait internet sitesinde yer alan haberde ilgili kişinin ad, soyad, fotoğraf, yerleştiği yükseköğretim programı ve yerleştirme puanından oluşan kişisel verilerinin işlendiğinin görüldüğü, şikayete konu iddialara ilişkin olarak veri sorumlusunun savunması ve savunmasına temel teşkil edecek bilgi ve belgelerin talep edildiği, veri sorumlusunu muhatap yazınının tebliğ edilmiş olmasına rağmen Kanunun 15 inci maddesinin (3) numaralı

fıkrasında öngörülen on beş günlük süre içerisinde Kuruma bir cevap verilmediği, dolayısıyla veri sorumlusunun ilgili kişinin kişisel verilerinin işlendiği iddiası hakkında savunma hakkını kullanmadığı ve bu nedenle ilgili kişinin sunmuş olduğu iddiasını tevsik edici belgeler ile şikâyetin sonuçlandırılmasının gerektiği,

- Kanunun “Tanımlar” başlıklı 3 üncü maddesinde kişisel verinin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlandığı, kişinin adı, soyadı ve fotoğrafının kişisel veri niteliğini haiz olduğu konusunda tereddüt olmamakla birlikte kişinin yerleştiği yükseköğretim programı ve yerleştirme puanını içerir sınav sonucu bilgilerinin kişisel veri niteliğine haiz olup olmadığı hususunun ayrıca değerlendirilmesi gerektiği, sınav sonucu bilgilerinin, ilgili kişinin belirli bir alandaki bilgi ve yeterliliğinin kapsamını ve bazı durumlarda zekasını, düşünce süreçlerini ve yargısını yansıttığı değerlendirildiğinden kişisel veri niteliğini haiz olduğu, ilgili kişinin yerleştiği yükseköğretim programının kişisel veri niteliğinde olan kişinin meslek bilgisine ilişkin kesin bir bilgi sağlamamakla birlikte kişinin ilgi alanlarına ilişkin bilgi vermesi nedeniyle kişisel veri niteliğini haiz olduğu,

- Öte yandan, Kanunun 28 inci maddesinin (1) numaralı fıkrasının (c) bendine göre; kişisel verilerin milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi hâlinde Kanun hükümlerinin uygulanmayacağına hüküm altına alınmış olduğu, Anayasanın 28 inci maddesinde düzenlenen basın özgürlüğünün Anayasanın 26 ncı maddesinde düzenlenen düşünceyi açıklama ve yayma özgürlüğünün bir yansıması olarak kabul edildiği, demokratik toplumlarda basının en önemli görevinin, kamu yararını ilgilendiren olay ve konularda haber ve bilgi vermek, açıklamalar yapmak, eleştiri ve değer yargıları sunmak suretiyle toplumu aydınlatmak ve kamuoyu oluşturmak olduğu ve yaptığı bu görev nedeniyle basına “haber verme hakkı ve görevi” tanınmış olduğu,

- Şikâyete konu olayda haberi yayınlayan veri sorumlusu açısından basın özgürlüğü söz konusu iken ilgili kişi açısından da kişisel verilerin korunmasını isteme hakkının söz konusu olduğu, dolayısıyla basın özgürlüğü ile kişisel verilerin korunmasını isteme hakkının karşı karşıya olduğu, haberden beklenen yarar ile ilgili kişinin kişisel verilerinin korunmasını isteme hakkından beklediği meşru çıkarın karşılaştırılması gerektiği ve bunun için temel ölçütün ise kamu yararı olduğu, gerek yazılı ve gerek görsel basın tarafından bu işlev yerine getirilirken, yayının kamu ilgi ve yararının bulunması ile gerçek ve güncel olmasının sağlanmasının ve haberi verirken öze biçim arasındaki dengenin korunmasının gerektiği,

- Haber başlığında ilgili kişinin yalnızca üniversiteyi kazanan gençlerin sevincinden bahisle T.C. kimlik numarası maskelenerek ilgili kişinin adı, soyadı, fotoğrafı, yerleştiği yükseköğretim programı ve yerleştirme puanını içeren sınav sonuç belgesine yer verilmiş olduğu, haberde başkaca bir bilgiye veya belgeye yer verilmediği, bu bilgilerin kullanılarak yapılan haber kapsamındaki kişisel verilerin kişilik haklarını ihlal etmemek kaydıyla ifade özgürlüğü kapsamında işlenip işlenmediğinin değerlendirilmesi gerektiği,
- Bu kapsamda, biçim ve öz arasındaki denge açısından haberlerde kullanılan dil ve ifadenin gerektirdiği ölçüde olduğu ve haberlerin verilmesinde gerekli, ilgili ve yararlı olmayan beyan ve değerlendirmelerde bulunulmadığı sonucuna varılması sebebiyle habere konu kişisel veriler açısından öz ile biçim arasındaki denge kriterine muhalefet edilmediği anlaşılmakla beraber, söz konusu haberin ilgili kişinin yüksek bir başarısı olduğundan bahisle yapılmadığı, yalnızca üniversiteyi kazanan gençlerden birinin örneğinin verildiğinin görüldüğü, bu sebeple haberin toplumda sık rastlanan bir olay olduğu ve haberdeki olayın toplumu konu üzerinde düşünmeye sevk etmediği ve dolayısıyla bir kamu yararı bulunmadığı kanaatine varılmış olup söz konusu haberde gerçekleştirilen kişisel veri işleme faaliyetinin Kanununun 28 inci maddesinin (1) numaralı fıkrasında düzenlenen ifade özgürlüğü kapsamında değerlendirilemeyeceği ve söz konusu kişisel veri işleme faaliyetinin istisna kapsamında olmadığı görüldüğü,
- Kanununun “Kişisel verilerin işleme şartları” başlıklı 5 inci maddesinin ikinci fıkrasının (d) bendinde “ilgili kişinin kendisi tarafından alenileştirilmiş olması”nın bir kişisel veri işleme şartı olarak düzenlendiği, Yükseköğretim Kurumları Sınavı Ölçme, Seçme ve Yerleştirme Merkezi tarafından yapılan bir sınav olup sınav sonucunun ancak kişinin oluşturduğu bir şifre ve T.C. kimlik numarası ile sorgulanabildiği, bu bilgiden hareketle ilgili kişinin adı, soyadı, fotoğrafı, yerleştiği yükseköğretim programı ve yerleştirme puanının ilk olarak ilgili kişi tarafından yayımlanması suretiyle alenileştirilmiş olabileceği ihtimalinin gündeme geldiği, ancak veri sorumlusunun şikâyete ilişkin bilgi ve belge talebine cevap vermeyerek savunma hakkını kullanmamış olması nedeniyle ilgili kişinin kişisel verilerinin nereden ve nasıl elde edildiği ve kişisel verilerinin hangi veri işleme şartına dayanılarak işlendiği bilgisine ulaşılamadığı, Kanununun kişisel verilerin işleme şartlarının düzenlendiği 5 ve 6 ncı maddelerinde kişisel verilerin işlenmesi bakımından hukuka uygunluk sebeplerinin, veri sorumlusu tarafından Kanunda yer alan hangi hukuka uygunluk sebebine dayanılarak kişisel veri işlendiğinin belirtilmemiş olması nedeniyle kişisel verilerin hukuka aykırı olarak işlendiği yönündeki karineye dayanarak veri sorumlusunun kişisel veri işleme faaliyetinin hukuka aykırı olduğu kanaatine varıldığı,

- Kanunun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesine göre veri sorumlusunun; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu, veri sorumlusunun ilgili kişinin kişisel veri niteliğini haiz adı, soyadı, fotoğrafı, yerleştiği yükseköğretim programı ve yerleştirme puanını hukuka aykırı olarak işleme nedeniyle Kanunun 12 nci maddesinde yer alan yükümlülüklerine aykırı hareket ettiği,

- 5326 sayılı Kabahatler Kanununun “İdari Para Cezaları” başlıklı 17 nci maddesinin ikinci fıkrasına göre idari para cezasının miktarı belirlenirken işlenen kabahatin haksızlık içeriği ile failin kusuru ve ekonomik durumunun birlikte göz önünde bulundurulacağı hüküm altına alındığı,

- Karar tarihi itibarıyla veri sorumlusuna ait internet sitesinde ilgili kişinin ad, soyad, fotoğraf, yerleştiği yükseköğretim programı ve yerleştirme puanının paylaşıldığı haberin kaldırılmış olduğunun görüldüğü

değerlendirmelerinden hareketle;

- Şikayete konu kişisel veri işleme faaliyetinin Kanunun 28 inci maddesinin (1) numaralı fıkrasında düzenlenen ifade özgürlüğü kapsamında değerlendirilemeyeceği, veri sorumlusuna ait internet sitesinde yer alan haberde ilgili kişinin kişisel verilerinin Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendine aykırı olarak işlendiği, karar tarihi itibarıyla söz konusu kişisel verilerin veri sorumlusuna ait internet sitesinden kaldırılmış olduğu hafifletici unsuru dikkate alınarak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca veri sorumlusu hakkında 30.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2022/6 sayılı KVKK Kararı

İlgili kişinin eski ortağı olduğu şirketin sicil bilgilerinin görüntülediği internet adresinde kişisel verilerinin hukuka aykırı olarak paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 06/01/2022 tarih ve 2022/6 sayılı Karar Özeti

Karar Tarihi : 06/01/2022

Karar No : 2022/6

Konu Özeti : İlgili kişinin eski ortağı olduğu şirketin sicil bilgilerinin görüntülediği internet adresinde kişisel verilerinin hukuka aykırı olarak paylaşılması

Kuruma intikal eden şikâyetle; ilgili kişinin eski ortağı olduğu şirkete ait sicil bilgilerinin yer aldığı "...” internet sayfasında eski ortaklar başlığı altında ad ve soyadının yazılı olduğu, şirketle herhangi bir hukuki veya idari bağının kalmadığı, dolayısıyla kişisel verilerinin üçüncü kişilerle izni olmaksızın paylaşılmasını istemediği, bu kapsamda veri sorumlusu Ticaret Odası’na sözlü ve yazılı olarak başvuruda bulunulduğu, Ticaret Odası tarafından ilgili kişinin talebinin Türk Ticaret Kanunu ve Ticaret Sicili Yönetmeliği gereğince yerine getirilemeyeceğinin belirtildiği ifade edilerek gereğinin yapılması talep edilmiştir.

Söz konusu iddialara ilişkin başlatılan inceleme çerçevesinde veri sorumlusu Ticaret Odası’ndan savunması istenilmiş olup alınan cevabî yazıda özetle;

- Türk Ticaret Kanunu hükümleri gereğince tescile tabi olan kayıt, değişiklik ve kayıt silme işlemlerinin Ticaret Sicili Müdürlükleri tarafından MERSİS (Merkezi Sicil Kayıt Sistemi) üzerinden yapıldığı, tescile ait ilan metinlerinin ise MERSİS'te üretilerek Türkiye Ticaret Sicili Gazetesinde yayınlandığı,
- Limited şirketlerin kuruluş işleminde ana sözleşmenin ve tüm ortakların tescilinin Türk Ticaret Kanunu’nun 587’nci maddesinde, payların geçiş hallerinin tescilinin ise 598’inci maddesinde düzenlendiği, bu çerçevede; tescile tabi ve üçüncü kişilerin incelemesine açık olan Türkiye Ticaret Sicili Gazetesinde yayınlanan limited şirketlerin pay devrine ilişkin tescillerine ait ilanlarda payı devir alan ortak ile payını devreden ortağa ait ad-soyad bilgisinin yer aldığı, kimlik numarası ve adres bilgisi gibi kişisel verilerin gizlenerek ilan edildiği,

- Şirketin ortaklık yapısının mevzuat gereği tescil edilip ilan edilmesi nedeni ile kişinin ortak olarak ya da eski ortak olarak görünmesinin aleni bir bilgi olduğu, kimlik numarası ve adresi gibi kişisel veri niteliği taşımadığı,

- Bu bağlamda, veri sorumlusunun internet sayfasındaki firma bilgileri içerisinde; Türk Ticaret Kanunu'nun 35 inci maddesi ile Ticaret Sicili Yönetmeliği'nin 15'inci maddesine göre mevzuatın izin verdiği ve Ticaret Sicili Gazetesinde yayınlanarak üçüncü kişilerin incelemesine açık olan bilgilerin yer aldığı

ifade edilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulu'nun 06/01/2022 tarih ve 2022/6 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) kişisel verilerin işlenmesine ilişkin "Genel İlkeler"i düzenleyen 4 üncü maddesinin (1) numaralı fıkrasında, "Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir." hükmünün yer aldığı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin; hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,

- Kanun'un, "Kişisel verilerin işlenme şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğunun hükme bağlandığı,

- Kanun'un 'Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi' başlıklı 7'inci maddesinin (1) numaralı fıkrasında bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silineceği, yok edileceği veya anonim hale getirileceği, (2) numaralı fıkrasında kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu, (3) numaralı fıkrasında ise kişisel verilerin silinmesine, yok edilmesine veya anonim hale getirilmesine ilişkin usul ve esasların yönetmelikle düzenleneceği,
- İlgili kişinin ad ve soyadının silinmesi talebinin bulunduğu internet sayfası incelendiğinde Ticaret Odası'nın Bilgi Bankasından Şirket bilgilerine göre bir sorgulama yapılabildiğinin görüldüğü, ilgili kişinin eski ortağı olduğu Şirket hakkında ilgili sayfada sorgulama yapıldığında Şirketin sicil numarası, oda sicil numarası, MERSİS numarası, firma unvanı, iş adresi, odaya kayıt tarihi, sermayesi, iş konusu gibi bilgilerin yanı sıra Tescil ve Gazete Bilgileri başlığı altında sicil gazetesine tescil edilen işlemlere ilişkin bilgi, ayrıca ortaklar ve eski ortakların adı, soyadı, görevi ve sermaye miktarına ilişkin bilgilere yer verildiğinin görüldüğü,
- İlgili kişinin şikâyetinde de ifade edildiği gibi söz konusu Şirketin eski ortağı olarak sorgulama sayfasında ilgili kişinin adı, soyadı ve sermaye miktarının yer aldığı görüldüğü,
- Öte yandan, Ticaret Sicili'nin tutulması hususuna ilişkin ilgili mevzuat incelendiğinde; 6102 sayılı Türk Ticaret Kanunu'nun "Ticaret Sicili-Kuruluş" başlıklı 24 üncü maddesinin "Gümrük ve Ticaret Bakanlığı tarafından il merkezindeki ticaret ve sanayi odaları ile ticaret odalarında faaliyet gösterecek şekilde ticaret sicili müdürlükleri kurulur. Bakanlık il merkezleri dışındaki odalarda ticaret sicili müdürlükleri kurabileceği gibi müdürlüklere bağlı şubeler de kurabilir. Ticaret sicili, Bakanlığın gözetim ve denetiminde ticaret sicili müdürlükleri ve şubeleri tarafından tutulur. Ticaret sicili kayıtlarının elektronik ortamda tutulmasına ilişkin usul ve esaslar Kanununun 26 ncı maddesine göre çıkarılacak yönetmelikte gösterilir. Bu kayıtlar ile tescil ve ilan edilmesi gereken içeriklerin düzenli olarak depolandığı ve elektronik ortamda sunulabilen merkezi ortak veri tabanı, Gümrük ve Ticaret Bakanlığı ile Türkiye Odalar ve Borsalar Birliği nezdinde oluşturulur. Ticaret sicili müdürlüğünün kurulmasında aranacak şartlar ve odalar arasında sicil işlemleri ile ilgili olarak varlığı gerekli işbirliğinin sağlanmasına ilişkin esaslar, Gümrük ve Ticaret Bakanlığınca çıkarılacak bir tebliğle düzenlenir. Ticaret sicili kayıt işlemlerinin elektronik ortamda yapılması için toplanması ve işlenmesi gerekli olan kişisel veriler, kişisel verilerin korunması ve bilgi güvenliğinin sağlanmasına ilişkin mevzuata uygun bir şekilde korunur." hükmünü haiz olduğu,

- Türk Ticaret Kanunu'nun "Açıklık" başlıklı 35'inci maddesinin "Tescil işleminin dayanakları olan dilekçe, beyanname, senetler, belgeler ve ilanları içeren gazeteler, üzerlerine sicil defterinin tarih ve numaraları yazılarak sicil müdürlüğüne saklanır. Herkes ticaret sicilinin içeriğini ve müdürlükte saklanan tüm senet ve belgeleri inceleyebileceği gibi giderini ödeyerek bunların onaylı suretlerini de alabilir. Bir hususun sicilde kayıtlı olup olmadığına dair onaylı belge de istenebilir. Tescil edilen hususlar, kanun veya Kanununun 26 ncı maddesine göre çıkarılacak yönetmelikte aksine bir hüküm bulunmadıkça ilan olunur. İlan, Türkiye genelinde sicil kayıtlarının ilanına özgü Türkiye Ticaret Sicili Gazetesi ile yapılır." hükmünü haiz olduğu,

- Türk Ticaret Kanunu'nun "Tescil ve İlan" başlıklı 587'nci maddesinde "Şirket sözleşmesinin tamamı, kurucuların imzalarının ticaret sicili müdürlüğünde yetkilendirilmiş personelin huzurunda imzalandığı tarihi izleyen otuz gün içinde, şirketin merkezinin bulunduğu yer ticaret siciline tescil ve Türkiye Ticaret Sicili Gazetesinde ilan olunur. Tescil ve ilan edilen şirket sözleşmesine, aşağıda sayılanlar dışında, 36'ncı maddenin birinci fıkrası hükmü uygulanmaz: Şirket sözleşmesinin tarihi, Şirketin ticaret unvanı ve merkezi, esas noktaları belirtilmiş ve tanımlanmış şekilde şirketin işletme konusu; şirket sözleşmesinde bu konuda bir hüküm varsa, şirketin süresi, esas sermayenin itibarî değeri, gerçek kişi ortağın adı ve soyadı, yerleşim yeri, tüzel kişi ortakların unvanı, merkezleri ve her ortağın üstlendiği esas sermaye payları, aynı sermayenin konusu ve bu tür sermayenin karşılığında verilecek esas sermaye payları; ..." şeklinde hüküm bulunduğu, aynı Kanun'un Tescil başlıklı 598'inci maddesinde ise "Esas sermaye paylarının geçişlerinin tescil edilmesi için, şirket müdürleri tarafından ticaret siciline başvurulur. Başvurunun otuz gün içinde yapılmaması hâlinde, ayrılan ortak, adının bu paylarla ilgili olarak silinmesi için ticaret siciline başvurabilir. Bunun üzerine sicil müdürü, şirkete, iktisap edenin adının bildirilmesi için süre verir. Sicil kaydına güvenen iyiniyetli kişinin güveni korunur." hükmünün yer aldığı,

- Türk Ticaret Kanunu'nun 26'ncı maddesine dayanılarak hazırlanan Ticaret Sicili Yönetmeliği'nin "Sicil kayıtlarına erişim hakkı" başlıklı 15'inci maddesi "Herkes, sicilin içeriğini ve müdürlükte saklanan tüm senet ve belgeleri inceleyebilir. Bu inceleme elektronik ortamda ve/veya müdürlükte yapılabilir... Bunların incelenmesinde müdür, kişisel verilerin korunmasına ilişkin hükümler çerçevesinde gerekli tedbirleri almak zorundadır. İnceleme esnasında müdürün vereceği talimatlara uyulması zorunludur. Aksi takdirde müdür defter ve belgeleri derhal kaldırabilir. Elektronik ortamda yapılacak olan incelemelerde de kişisel verilerin korunmasını ve bilgi güvenliğini sağlayacak tedbirler alınır." şeklinde düzenlendiği,

• Aynı Yönetmelik'in "Sicil İşlemlerinin Tabi Olduğu Hükümler" başlıklı 28'inci maddesi "(1) Sicile ait tescil, değişiklik ve silinmeler ile diğer iş ve işlemler Kanun ve bu Yönetmelik hükümlerine göre yapılır.(2) Tescil, bir olgunun sicile geçirilmesini; değişiklik, tescil edilmiş bir olgudaki değişiklik dolayısıyla sicildeki kayıtların değiştirilmesini veya düzeltilmesini; silinme ise tescil edilmiş olan bir olgunun ortadan kalkması veya sona ermesi sebebiyle ona ait kayıtların silinmesini ifade eder." hükmüne, "Tescil edilmiş olgularda değişiklikler" başlıklı 29'uncu maddesinin "Tescil edilmiş olgularda meydana gelen her türlü değişikliğin de tescil edileceğini, "Tescil ve ilanun üçüncü kişilere etkisi" başlıklı 30'uncu maddesinin ise bir olgunun tescil ile beraber derhal üçüncü kişiler hakkında sonuç doğuracağını belirten hükümlere sahip olduğu,

• Türkiye Cumhuriyeti Anayasası'nın "Kamu Kurumu Niteliğindeki Meslek Kuruluşları" başlıklı 135'inci maddesinde "Kamu kurumu niteliğindeki meslek kuruluşları ve üst kuruluşları; belli bir mesleğe mensup olanların müşterek ihtiyaçlarını karşılamak, mesleki faaliyetlerini kolaylaştırmak, mesleğin genel menfaatlere uygun olarak gelişmesini sağlamak, meslek mensuplarının birbirleri ile ve halk ile olan ilişkilerinde dürüstlüğü ve güveni hakim kılmak üzere meslek disiplini ve ahlakını korumak maksadı ile kanunla kurulan ve organları kendi üyeleri tarafından kanunda gösterilen usullere göre yargı gözetimi altında, gizli oyla seçilen kamu tüzel kişilikleridir." hükmünün yer aldığı,

• 5174 sayılı Türkiye Odalar ve Borsalar Birliği İle Odalar ve Borsalar Kanunu'nun "Odalar" başlıklı 4'üncü maddesinde odaların üyelerinin müşterek ihtiyaçlarını karşılamak, meslekî faaliyetlerini kolaylaştırmak, mesleğin genel menfaatlere uygun olarak gelişmesini sağlamak, mensuplarının birbirleri ve halk ile olan ilişkilerinde dürüstlüğü ve güveni hâkim kılmak üzere meslekî disiplin, ahlâk ve dayanışmayı korumak ve bu Kanunda yazılı hizmetler ile mevzuatla odalara verilen görevleri yerine getirmek amacıyla kurulan, tüzel kişiliğe sahip kamu kurumu niteliğinde meslek kuruluşları olduğunun belirtildiği,

• Türkiye Odalar ve Borsalar Birliği İle Odalar ve Borsalar Kanunu'nun "Odaların Görevleri" başlıklı 12 nci maddesinin "Odaların görevleri şunlardır:... Ticaret ve sanayiye ilgilendiren bilgi ve haberleri derleyerek ilgililere ulaştırmak, ilgili kanunlar çerçevesinde resmî makamlarca istenecek bilgileri vermek ve özellikle üyelerinin mesleklerini icrada ihtiyaç duyabilecekleri her çeşit bilgiyi, başvuruları durumunda kendilerine vermek veya bunların elde edilmesini kolaylaştırmak, elektronik ticaret ve internet ağları konusunda üyelerine yol gösterecek girişimlerde bulunmak, bu konularda gerekli alt yapıyı kurmak ve işletmek." şeklinde düzenlendiği,

- Bu çerçevede ticaret sicilinin, Ticaret Bakanlığının gözetim ve denetiminde ticaret sicili müdürlükleri ve şubeleri tarafından tutulacağı düzenlenmiş olup Ticaret Bakanlığı tarafından il merkezindeki ticaret ve sanayi odaları ile ticaret odalarında faaliyet gösterecek şekilde ticaret sicili müdürlükleri kurulacağı hükmünden de anlaşılacağı üzere ticaret sicili müdürlüklerinin il merkezindeki ticaret odasına bağlı olarak faaliyet gösterdiği,

- Öte yandan, kayıtlar ile tescil ve ilan edilmesi gereken içeriklerin düzenli olarak depolandığı ve elektronik ortamda sunulabilen merkezi ortak veri tabanının, Ticaret Bakanlığı ile Türkiye Odalar ve Borsalar Birliği nezdinde oluşturulduğu,

- Türk Ticaret Kanunu'nun ve Ticaret Sicili Yönetmeliği'nin ilgili maddeleri çerçevesinde, herkesin sicilin içeriğini ve müdürlükte saklanan tüm senet ve belgeleri inceleyebileceği ve bu incelemenin elektronik ortamda ve/veya müdürlükte yapılabileceği ile tescil edilmiş olgularda meydana gelen her türlü değişikliğin de tescil edileceği

anlaşmakta olup Şirketin pay devrine ilişkin değişikliğin ticaret sicili gazetesinde tescil edildiği, söz konusu ticaret sicilinin tutulmasından sorumlu ticaret sicil müdürlüklerinin de ticaret odalarına bağlı olarak faaliyet gösterdiği dikkate alındığında söz konusu bilgilerin ticaret odası bünyesinde hâlihazırda mevcut olduğu sonucuna varıldığı,

- Ayrıca, ticaret sicil gazetesinde yer alan bir bilginin ticaret odasının sayfasında bulunmasındaki amacın yine ticaret sicil işlemlerine ilişkin bilginin daha kolay ulaşılabilir olmasını sağlamak adına gerçekleştirildiği, bununla birlikte söz konusu bilgiye yalnızca ilgilileri tarafından ticaret odasının sayfasındaki bilgi bankası platformundan firma bilgileri girilmek suretiyle erişildiği, söz konusu bilginin ticaret sicil gazetesinde yayınlanma amacından farklı bir amaçla yayınlandığına ilişkin herhangi bir emare bulunmadığı dikkate alındığında söz konusu kişisel veri işleme faaliyetinin Kanun'un Genel İlkeler başlıklı 4 üncü maddesinde yer alan "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesine de aykırılık teşkil etmediği, diğer yandan söz konusu bilginin ilgili kişi tarafından da belirtildiği üzere doğru olduğu ve yayınlanmasında amaca aykırılık bulunmadığı,

- Diğer taraftan, Anayasa'da ve Türkiye Odalar ve Borsalar Birliği İle Odalar ve Borsalar Kanunu'nda yer aldığı üzere Kamu Kurumu niteliğindeki meslek kuruluşları ve üst kuruluşlarının; belli bir mesleğe mensup olanların müşterek ihtiyaçlarını karşılamak, mesleki faaliyetlerini kolaylaştırmak, mesleğin genel menfaatlere uygun olarak gelişmesini sağlamak amacıyla kurulan kamu tüzel kişilikleri olduğu,

- Türkiye Odalar ve Borsalar Birliđi ile Odalar ve Borsalar Kanunu'nda yer aldıđı üzere; ticaret ve sanayiye ilgilendiren bilgi ve haberleri derleyerek ilgililere ulařtırmak, ilgili kanunlar çerçevesinde resmî makamlarca istenecek bilgileri vermek ve özellikle üyelerinin mesleklerini icrada ihtiyaç duyabilecekleri her çeřit bilgiyi, başvuruları durumunda kendilerine vermek veya bunların elde edilmesini kolaylařtırmak, elektronik ticaret ve internet ađları konusunda üyelerine yol gösterecek giriřimlerde bulunmak, bu konularda gerekli alt yapıyı kurmak ve iřletmek řeklinde odalara görev ve sorumlulukların yüklendiđi

dikkate alındıđında ilgili Ticaret Odası tarafından "...”internet sayfasında Bilgi Bankası bölümünden firma bilgileri girilmek suretiyle sorgulama yapılmasına ve ticaret sicili gazetesindeki bilgilerin bu platformda yer alması suretiyle bilgiye ulařımın kolaylařtırılmasına imkân sađlanması suretiyle gerçekteřirilen kiřisel verileri iřleme faaliyetinin T.C. Anayasası ve 5174 sayılı Türkiye Odalar ve Borsalar Birliđi İle Odalar ve Borsalar Kanunu'nda ticaret odaları için öngörülen yükümlölükler kapsamında deđerlendirilebileceđi dikkate alındıđında söz konusu kiřisel veri iřleme faaliyetinin Kanun'un 5 inci maddesinin (2) numaralı fıkrasının (a) bendinde yer alan kanunlarda açıkça öngörölme ve aynı fıkranın (ç) bendinde yer alan veri sorumlusunun hukuki yükümlölüđünü yerine getirebilmesi için zorunlu olması řartlarına dayanılarak gerçekteřirildiđi sonucuna varıldıđı

deđerlendirmelerinden hareketle;

- Kanun'un "Kiřisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi" bařlıklı 7 nci maddesinde yer alan "Bu Kanun ve ilgili diđer kanun hükümlerine uygun olarak iřlenmiř olmasına rađmen, iřlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kiřisel veriler resen veya ilgili kiřinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir." hükmüne istinaden söz konusu kiřisel verilerin iřlenmesini gerektiren sebeplerin ortadan kalkmadıđı sonucuna varılmıř olup ilgili kiřinin bu yöndeki talebi ile ilgili olarak Kanun kapsamında tesis edilecek herhangi bir iřlem bulunmadıđına karar verilmiřtir.

2021/1324 sayılı KVKK Kararı

Yemek Sepeti Elektronik İletişim Perakende Gıda Lojistik AŞ veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 23/12/2021 tarih ve 2021/1324 sayılı Karar Özeti

Karar Tarihi : 23.12.2021

Karar No : 2021/1324

Konu Özeti : Yemek Sepeti Elektronik İletişim Perakende Gıda Lojistik AŞ (Yemeksepeti) veri ihlal bildirimini

Veri sorumlusunun Kuruma intikal eden veri ihlal bildiriminde;

- 18.03.2021 tarihinde kimliği tespit edilemeyen şahıs/shahıslar tarafından veri sorumlusuna ait bir web uygulama sunucusuna erişildiği,
- Normal şartlarda yetkisiz bir erişim olduğunda uyarı veren araç üzerinde sorun kaydı olduğu ancak bir aksaklık nedeniyle yetkisiz erişimin o an fark edilemediği,
- 25.03.2021 tarihinde gelen alarmlar incelediğinde şüpheli bir davranış olduğunun tespit edildiği,
- Aynı tarihte yapılan incelemede Yemeksepeti'ne ait bir web uygulama sunucusu üzerindeki açıktan yararlanmak suretiyle uygulama kurulduğu ve komut çalıştırılarak sunucuya erişildiği,
- İhlali gerçekleştiren şahsın/shahısların eriştiği sunucu üzerinde kullanıcı oluşturularak farklı araçlar vasıtasıyla veri toplamaya çalıştıkları ve uzaktaki sunuculara trafik gönderdiklerinin de ayrıca tespit edildiği,
- Saldırganların veriyi Fransa'da bulunan bir IP adresine/sunucuya ilettikleri ve bu iletilen trafiğin firewall (güvenlik duvarı) üzerinde izlerinin olduğu,
- İhlalden 21.504.083 Yemeksepeti kullanıcısının etkilendiği,
- İhlalden etkilenen kişisel verilerin kullanıcı adı, adres, telefon numarası, e-posta adresi, kullanıcı şifresi ve IP bilgileri olduğu

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 23/12/2021 tarih ve 2021/1324 sayılı Kararı ile;

- Veri sorumlusuna ait bir web uygulama sunucusu üzerindeki açık sebebiyle uygulama kurarak ve komut çalıştırmak suretiyle sunucuya erişildiği,
- İhlalden 21.504.083 Yemeksepeti kullanıcısının etkilendiği,
- Etkilenen kişisel verilerin kullanıcı adı, adres, telefon numarası, e-posta adresi, şifre ve IP bilgileri olduğu,
- İhlalden etkilenen kişi sayısının çok fazla olması ve neredeyse tüm müşteri veri tabanının dışarı sızdırıldığı dikkate alındığında ihlalin çok büyük çaplı olduğu,
- İhlalin boyutu, sızdırılan verinin büyüklüğü ve sızdırılan kişisel verilerin niteliği dikkate alındığında, ihlalin ilgili kişiler açısından kişisel veriler üzerinde kontrol kaybı gibi önemli riskler oluşturacağı,
- Sisteme giren kişi ya da kişilerce, zararlı yazılım ve araçlarla sisteme giriş yaptıktan sonra diğer sistemlere de erişilerek bilgi toplandığı, sisteme zararlı yazılımların yüklenip, çalıştırılmasının veri sorumlusunca 8 gün boyunca fark edilemediği dolayısıyla bilişim ağlarında hangi yazılım ve servislerin çalıştığı kontrol edilmesi ve bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi noktasında veri sorumlusunun kusurunun bulunduğu,
- 18.03.2021 tarihinden itibaren güvenlik yazılımlarında alarmlar oluştuğu, oluşan bu alarmların üçüncü parti firmalar tarafından izlenen ürünlerde Yemek Sepeti Güvenlik Ekiplerine ilgili bildirimler yapılamadan ve gerekli aksiyonlar alınmadan kapatıldığı ifade edildiği, 25.03.2021 tarihinde iletilen alarmların Yemek Sepeti Güvenlik Ekiplerince incelenmesi sonucu siber saldırının farkına varıldığı dikkate alındığında bu durumun veri sorumlusunun hizmet aldığı üçüncü parti firmalar üzerinde etkin bir denetim mekanizmasının bulunmadığının ve güvenlik yazılımlarının takibi ile güvenlik prosedürlerinin kullanılması noktasında da eksiklerinin bulunduğunun göstergesi olduğu,
- Saldırganların veri sorumlusundan elde ettikleri veriyi Fransa'da bulunan bir IP adresine/sunucuya ait lokasyona iletildiği, sistemden çıkan 28.2 GB'lık verinin/dışarı giden trafiğin veri sorumlusu tarafından fark edilemediği ve bu veri trafiğinin firewall (güvenlik duvarı) üzerinde izlerinin olduğu dikkate alındığında; firewall üzerinde izlerin olmasına rağmen bu boyutta verinin dışarı sızdırılmasının fark edilememesinin veri sorumlusu tarafından güvenlik kontrolleri ve veri güvenliği takibinin düzgün bir şekilde yapılmadığının göstergesi olduğu,
- Açıklık bulunan sunucunun sızma testinden geçen bir sunucu olduğunun ifade edildiği dikkate alındığında bu durumun veri sorumlusu tarafından sızma testlerinin etkin bir şekilde yapılmadığını/yaptırılmadığını gösterdiği,

- Büyük miktarda kişisel veri işleyen veri sorumlusunun bu boyutta bir ihlal yaşamasının ve müdahalede geç kalmasının mevcut risk ve tehditleri iyi belirlemediğinin göstergesi olduğu

hususları dikkate alındığında, 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (1) numaralı fıkrası hükmü çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca ihlalin boyutu, kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak 1.900.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2021/1303 sayılı KVKK Kararı

Araç kiralama programları yazılımcısı ve satıcısı firmalar tarafından, ilgili kişilerin verilerinin işlenmesi ve bu verilerin araç kiralama firmaları arasında paylaşılmasını sağlayan bir kara liste programı oluşturulması hakkında Kişisel Verileri Koruma Kurulunun 23/12/2021 tarihli ve 2021/1303 sayılı Karar Özeti

Karar Tarihi : 23/12/2021

Karar No : 2021/1303

Konu Özeti : Araç kiralama programları yazılımcısı ve satıcısı firmalar tarafından, ilgili kişilerin verilerinin işlenmesi ve bu verilerin araç kiralama firmaları arasında paylaşılmasını sağlayan bir kara liste programı oluşturulması

Kuruma intikal eden ihbarda özetle;

- İhbar edilen veri sorumlularının araba kiralama yazılımı üreticileri veya satıcıları olduğu,
- Bu yazılımları kullanan araba kiralama şirketlerinin müşterileri hakkında elde ettikleri tüm verileri bu yazılımlar vasıtasıyla kayıt altında tuttuğu, bu kapsamda aynı yazılımları kullanan diğer şirketlerin de, rızaları olmaksızın ilgili müşterilerin kişisel verilerini uygulamadaki kara liste havuzundan görebildiği ve böylece bu yazılımı kullanan diğer kullanıcılara verilerin ifşa edildiği,
- Bir araç kiralama firmasının kiraladığı aracına gelecek muhtemel zararlardan korunmak maksatlı bir takım önlemleri almasının ticaret hayatının olağan akışına uygun olduğu ancak müşterilerin rızası alınmaksızın bu yazılım vasıtasıyla kara listeye alındıkları ve böylece bu yazılımı kullanan diğer kullanıcılar ile kişisel verilerinin paylaşıldığı

ifade edilerek, yukarıda belirtilen hususların6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında incelenmesi ve gereğinin yapılması talep edilmiştir.

Söz konusu ihbara ilişkin olarak Kişisel Verileri Koruma Kurulu tarafından resen inceleme başlatılmasına karar verilmiş olup Kurum tarafından dilekçede belirtilen iddialar ile ilgili olarak gerekli incelemelerin yapılabilmesini teminen tespit edilebilen araç kiralama yazılımı üreticisi şirketleri muhatap bilgi, belge ve savunma talepli yazılar ile yukarıdaki iddialar çerçevesinde kişisel

veri işleme faaliyetlerinin detayı ve iddia edildiği üzere bir kara liste uygulamasının mevcut olup olmadığı yönünde bilgi talep edilmiştir. Bu çerçevede araç kiralama yazılımı üreticisi şirketler tarafından Kuruma gönderilen yazılarda genel olarak Şirketlerin yazdığı yazılım programlarının araç kiralama firmalarının operasyonlarını yönetebilmesi için hazırlandığı, bu yazılım programlarında araç kiralama sözleşmesi için zorunlu olan bilgiler ile kamu kurum ve kuruluşlarının zorunlu olarak istediği kimlik ve ehliyet gibi bir takım kişisel verilerin kaydedildiği, araç kiralama firmalarına sundukları işletme faaliyetlerinin; sözleşme kurulduktan sonra bu şirketlere kullanıcı adı ve şifre verilmesi, kullanıma başlanılmasını takiben araç kayıtlarının tutulması, kira sözleşmelerinin, rezervasyonların ve bunlarla ilişkili muhasebe işlemlerinin kaydının tutulması olduğu bilgilerine yer verilmiştir.

Ek olarak bazı yazılım şirketleri tarafından;

- Kişisel verilerin işlenmesinin amacının; üye araç kiralama firmalarının kendi müşterilerine kolay ulaşmak, onları kampanyalardan haberdar edebilmek, araç teslimi noktasında bilgilendirme amaçlı SMS gönderebilmek ve sorunlu olan müşteriler (aracı geç teslim eden, kendi kusurlarıyla kaza yapan, kiralama bedelini ödemeyen vb.) program üyesi başka araç kiralama firmalarından araç kiralamak istediğinde müşteri hakkında sorun arz eden uyarıyı ve yorumları ilgili araç kiralama firmasına iletmek olduğu; hukuki açıdan ise kişisel verilerin işlenmesindeki amaçlardan birinin aydınlatma metninde belirtilen müşteri memnuniyeti, firma zarar riski araç güvenirliliği sağlamak için müşteri hakkındaki iyi/kötü yorumların diğer program ortaklarıyla paylaşılabilmesi olduğu,
- Bu anlamda programların amacının araç kiralama firmalarını tek çatı altında toplamak, kendi aralarında bilgi akışını sağlamak, sisteme kaydettikleri araçların takibini, trafik ceza durumlarını vb. birçok hususu anlık görebildikleri dijital ortam yaratmak olduğu,
- Yazılım programlarının araç kiralama firmaları tarafından satın alınması ile kişisel veri sisteme işlendiğinden kişisel verilerin araç kiralama firmalarının müşterilerinin kendisi tarafından alenileştirildiği,
- İmzalanan sözleşmelerde "... araç kiralama sözleşmesi vasıtasıyla ilettiğim ve sair yöntemlerle vermiş olduğum kişisel bilgilerimin tek başına ve/veya başka kişisel verilerle birleştirilerek ticari olarak kullanılmak üzere toplanmasına, işlenmesine, bunu hakkımdaki iyi/kötü yorumlarla birlikte diğer program ortakları ile paylaşılmasına ve aksini yazılı olarak belirtmediğim sürece bu firmaların benimle SMS, internet, mektup, telefon vb. kanallardan temasa geçmelerine aşağıya attığım imza ile açıkça rıza ve muvafakat ederim." uyarısı ve müşteri rızası ile araç kiralama firmasının müşterisinin kişisel bilgilerinin üye araç kiralama firması tarafından program veri tabanına kaydedildiği,

- Müşterileri olan araç kiralama firmalarının hukuka aykırı kullanımlarından şirketlerinin sorumlu olmadığı,
- Program üyeleri ile yapılan üyelik sözleşmesinde veri sorumlularının sisteme ekledikleri veriler için muhakkak kişilerin açık rızasının alınması gerektiğinin düzenlendiği; yazılım şirketleri veri sorumlusu olmadığı için hangi verinin hukuka aykırı olarak eklendiğinin tespitinin mümkün olmadığı

açıklamalarına yer verilirken; diğer yazılım şirketleri tarafından ise

- Verilen kullanıcı adı ve şifrelerin her bir müşteri araç kiralama firmasına ayrı ayrı özgülendiği bu nedenle bir araç kiralama firması tarafından girilen araba kiralayan kişi veya kişilere ait verilere bir başka araç kiralama firması tarafından erişilmesinin mümkün olmadığı,
- Aynı zamanda bu firmaların üçüncü kişilere ait verilere müdahale hakkının bulunmadığı ve bunun yanı sıra araç kiralama firmalarının müşteri havuzlarının kara liste sistemleriyle bağlantılı olmadığı,
- Ürettikleri yazılım vasıtasıyla araç kiralama firmalarının müşteri bilgilerinin başka bir ortama aktarılmasının, başka firmalarca bu bilgilere ulaşılmasının veya şirketleri tarafından paylaşılmasının ya da ekran görüntüsü alınarak internet ortamlarında paylaşılmasının söz konusu olmadığı,
- Müşteri araç kiralama firmaları tarafından sisteme işlenen veriler yönünden bu firmaların, verisini işlediği gerçek veya tüzel kişiden açık rıza alma şartının aranabileceği, fakat yazılımcı olan şirketlerinin sadece araç kiralama firmalarının müşterilerine ait verileri gizli tutma yükümlülüğü nedeniyle gizlilik politikası uyarınca sorumlu olduğu,
- Araç kiralama firmalarının uygulama üzerinden kiralama bilgilerini doldurması ile programlar tarafından otomatik hazırlanan sözleşmeyi kendi müşterileriyle imza altına alarak kiralama işlemi gerçekleştirdiği,
- Yazılım şirketlerinin veri sorumlusu olmadığı ve veri girişi yapmadığı; veri sorumlularının kendi müşterileri ile sözleşme yapan ve açık rızalarını alan araç kiralama firmaları olduğu; yazılım şirketlerinin ise eklenen verileri sadece saklamak ve diğer program üyeleri ile paylaşmakla yükümlü olduğu,
- İlgili kişilerden elde edilen kimlik, adres ve telefon bilgilerinin ise Emniyet Genel Müdürlüğünün ve Kiralık Araç Bildirim Sisteminin (KABİS) oto kiralama firmalarına belirttiği şekilde saklandığı,
- Kişisel verilerin toplanması, toplama yöntemleri, toplanacak kişisel veri türleri, toplanan verilerin hangi amaç ile kullanılacağı ve hangi bireylerin kişisel verilerinin toplanacağına araç kiralama

firmalarınca karar verildiği; hizmet sözleşmeleri ile yükümlülüğün araç kiralama firmalarına bırakıldığı

ifadelerinin yer aldığı görülmüştür.

Konuya ilişkin yapılan inceleme neticesinde Kurulun 23.12.2021 tarihli ve 2021/1303 sayılı Kararı aşağıdaki değerlendirmelere ulaşılmıştır.

1. Araç Kiralama Programı Yazılım Şirketlerinin ve Araç Kiralama Firmalarının Veri Sorumluluğu Sıfatına İlişkin Değerlendirme

- 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Tanımlar" başlıklı 3'üncü maddesinin (1) numaralı fıkrasının (ç) bendinde ilgili kişi, "kişisel verisi işlenen gerçek kişi", (d) bendinde kişisel veri, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", (e) bendinde kişisel verilerin işlenmesi, "Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", (ı) bendinde veri sorumlusu, "kişisel verilerin işleme amacını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi", (ğ) bendinde veri işleyen, "veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi" olarak tanımlanmıştır.

- Kanun çerçevesinde bir işleme faaliyetinde veri sorumlusu veya veri işleyenin tespiti için işlenecek kişisel verileri, gerçekleştirilecek veri işleme faaliyetini, bu işlemenin amaçlarını ve şeklini kimin belirlediğinin göz önünde bulundurulması gerekmektedir. Bu çerçevede, veri işlemenin parçası olarak yalnızca veri sorumlusu tarafından:

- İşleme faaliyetinin yasal dayanağı,
- İşlenecek kişisel verilerin türleri,
- Verilerin kullanılacağı amaç(lar),
- İlgili kişilerin kimler olacağı (hedef kitle),
- Verilerin aktarılıp aktarılmayacağı ve aktarılacak ise kime aktarılacağı;
- Bireylerin hakları doğrultusunda veri sorumlusuna yapılan başvurulara nasıl cevap verileceği; verilerin ne kadar süreyle saklanacağı, değiştirileceği veya anonim hale getirileceği

hususlarına karar verilebilecekken, veri işleyen tarafından ise ancak, veri sorumlusu ile yaptığı sözleşme şartları içinde sınırlı olarak;

- Kişisel veri toplamak için bilgisayar teknolojisi sistemlerinin veya diğer hangi yöntemlerin kullanılacağı,
- Kişisel verilerin nasıl depolanacağı,
- Kişisel verileri korumak için alınacak güvenlik önlemlerinin ayrıntıları,
- Kişisel verilerin bir kuruluştan diğerine nasıl aktarılacağı,
- Belirli kişilerle ilgili kişisel verilerin nasıl elde edileceği (otomatik/otomatik olmayan yöntemler),
- Saklama sürelerine uyulmasının nasıl sağlanacağı; verilerin nasıl silineceği veya imha edileceği

hususlarına karar verebilir.

• Bu çerçevede ihbarda belirtilen iddialara ilişkin olarak öncelikle veri işleme faaliyetinin tayini ile veri sorumlusunun belirlenmesi gerekmektedir. Öyle ki kişisel verileri toplanan hedef kitle araç kiralama firmalarının müşterileri olup işleme faaliyetinin başlıca yasal dayanağı müşterilerle araç kiralama firmaları arasında imzalanan kira sözleşmesidir. Araç kiralama firmaları müşterilerine ait verileri toplamak için yazılım şirketlerine başvurarak özel bir yazılım geliştirilmesini talep etmiş yahut bu iş için kullanılmakta olan bir yazılımı satın almış olabilir. Diğer bir ifade ile araç kiralama firmaları ile bu yazılımları üreten şirketler arasındaki hukuki ilişki satış ya da hizmet sözleşmesi olarak adlandırılabilir. Her iki durumda da araç kiralama firmalarının müşterilerine ilişkin verileri kayıt altında tutacağı söz konusu yazılımların 'yaşayan birer organizma' olduğunu söylemek mümkündür. Öyle ki müşterilere ilişkin veri girişinin araç kiralama firmaları tarafından yapılıyor oluşu veri sorumlusu sıfatının tanımlanmasında tek başına yol gösterici bir belirteç değildir.

• Veri sorumlusu olmanın belirleyicilerinden biri hangi verilerin işleneceğine sürecin başından itibaren kimin karar verdiğiidir. Veri işleyen uhdesine bırakılacak işleme sürecinin teknik bilgi ve alanda uzmanlık gerektirmesi bu anlamda karar yetkisinin veri işleyende olduğu yanılığını beraberinde getirmektedir. Oysaki veri işleyen, kendi adına bu verileri kullanmadan, veri sorumlusundan gelen talimat üzerine verileri toplayıp işlemektedir.

• Bu anlamda, ortak bir amacın varlığı ve kişisel verilerin işlenmesindeki temel araçların birlikte belirlenmesi ortak veri sorumluluğunu beraberinde getirmekte olup ortak veri sorumlularından biri işlenmekte olan kişisel verilere erişemese dahi, bu erişememe durumu ortak veri sorumluluğunu etkilememektedir. İhbara konu yazılım şirketlerinin araç kiralama firmaları tarafından girilen verilere erişememesi bu anlamda tek başına veri sorumlusu olmayacağı anlamına gelmemektedir. Öyle ki bir araç kiralama firmasının kara listeye alarak kaydettiği bir müşterinin kişisel verilerinin bu yazılım şirketine ait internet sitesi/veri tabanı aracılığıyla bir bulutta toplanıyor olması durumunda, söz

konusu yazılım şirketlerinin depoladıkları bu verilere doğrudan erişimleri olmadan da onları kendi amaçları doğrultusunda kullandığı yorumunu yapmak mümkün olabilecektir.

- Ortak veri sorumlularının yükümlülüklerinin eşit olarak paylaşılması zorunlu değildir, araç kiralama hizmeti sunan yazılım şirketine ait internet sitesinin araç kiralama firmalarından, araç kiralama firmalarına yönelik aydınlatma metni sunması ve verinin aktarımına ilişkin açık rıza alması da mümkündür. Bu tarz bir ortaklıkta veri işleminin esaslarının belirlenebilmesi adına iki veri sorumlusu arasında söz konusu sürece ilişkin bir sözleşme yapılması sorumlulukların belirlenmesi (müşterek sorumluluk) açısından önem taşımaktadır, aksi takdirde herkes kusuru oranında ortaya çıkacak ihlallerden sorumludur. Bununla birlikte, yazılım şirketlerinin “Araç kiralama firmaları tarafından uygulama içerisine kaydedilen verileri depoluyor ve güvenliği sağlıyoruz, bu verilerin içeriğine erişimimiz yok” açıklaması ve sözleşme içeriğine “Yazılım ürünlerinin yanlış kullanılmasından, müşteriler tarafından kendi müşterileriyle alakalı fişlemeye girebilecek bilgilerin saklanmasından ve kullanılmasından yazılım şirketimiz sorumlu değildir” vb. kayıtlar koyması ile söz konusu uygulamaya girilen bu tarz kişisel verileri başka kullanıcıların (araç kiralama firmalarının) erişimine açıyor olması, araç kiralama firması ile yazılım şirketi arasında sorumluluğun sözleşme ile paylaşıldığı anlamına gelmemektedir.

- Öte yandan idari para cezaları için genel kanun niteliğinde olan 5326 sayılı Kabahatler Kanunu’nun genel hükümleri arasında yer alan “İdari Para Cezaları” başlıklı 17’nci maddesinin 2’nci fıkrasında, idari para cezasının, kanunda alt ve üst sınırı gösterilmek suretiyle de belirlenebileceği, bu durumda, idari para cezasının miktarı belirlenirken işlenen kabahatin haksızlık içeriği ile failin kusuru ve ekonomik durumunun birlikte göz önünde bulundurulacağı karara bağlanmıştır. Kurul tarafından idari para cezalarının miktarı belirlenirken de Kanunun 18’inci maddesi gereğince kabahat bazında bir ayrıma gidilmiştir. Ceza miktarının hesabında ihlalin niteliği, veri sorumlusunun niyeti, ilgili kişilere verilen zararı azaltmak için alınan önlemler, veri güvenliğine ilişkin alınan rutin önleyici tedbirler, inceleme faaliyeti sırasında veya ihlal sonrası Kurumla yapılan işbirliği ve ihlale konu veri türü gibi faktörler önemlidir.

- Ortak veri sorumlularına ilişkin sorumluluk ve kusur miktarlarının belirlenmesi açısından her halükarda olay bazında veri işleme süreçlerinin incelenmesi; kusur ve söz konusu veri üzerindeki kontrolün kimde olduğunun tespiti gerekmektedir. Hukuka aykırı bir fiilin sorumluluk gerektirebilmesi için kişinin kusurlu olması gerekir. Kusur hem ceza hukukunda hem medenî hukukta hem de idare hukukunda ortak bir konudur. 6098 sayılı Borçlar Kanununda kusurun, sorumluluğun kurucu unsurlarından bir tanesi olduğu belirtilmiştir. Temelde ise söz konusu hukuka

aykırı eylem bir haksız fiile vücut vermektedir. Kabahatler Kanununun 2'nci maddesine göre "Kabahat deyiminden; kanunun, karşılığında idarî yaptırım uygulanmasını öngördüğü haksızlık anlaşılır." Kabahatler Kanununun 9'uncu maddesi gereğince kabahatin işlenebilmesi için kasıt ya da taksir şartı aranmaktadır. Kabahatler Kanununun 12'inci maddesinde ise aksine hüküm bulunmayan hallerde TCK'daki hukuka uygunluk nedenleri ile kusurluluğu ortadan kaldıran nedenlerin kabahatler bakımından da uygulanması gerektiği öngörülmektedir. Anayasa'nın 38'inci maddesinin 7'nci fıkrasında ve TCK'nın 20'nci maddesinin 1'inci fıkrasında cezaların şahsiliği ilkesine yer verilmiş ve suçun işlenmesine bizzat veya dolaylı olarak katılmadıkça kimsenin bir suçtan dolayı sorumlu tutulamayacağı ifade edilmiştir. Bu doğrultuda, veri sorumlusu sıfatına sahip olan her kişi 6698 sayılı Kanunun 12'nci maddesi gereğince hukuka aykırı eylemlerinden dolayı cezai müeyyideye tabi olabilecektir.

- Ortak veri sorumluları arasında kusurluluk belirlenirken işlenen verinin ilk ve son kullanıcısının kim olduğu; veri girişini kimin yaptığı; hangi amaçla söz konusu verinin girildiği; verinin değiştirilmesine veya silinmesine yahut aktarılmasına kimin karar verdiği; veriyi toplayan dışında kalan veri sorumlularının bu veri ile hangi faaliyetleri gerçekleştirdiği vb. etkenlere dikkat edilmesi yerinde olacaktır. Örneğin araç kiralama firmalarına 2015 yılından beri Kiralık Araç Bildirim Sistemi (KABİS) kullanma zorunluluğu getirilmiştir. 1174 sayılı Kimlik Bildirme Kanunu Ek Madde 3'te "Araç kiralama firmalarının sorumlu işleticileri ve yöneticileri, kiralanan araç bilgileri ile aracı kiralayanların kimlik bilgileri ve kira sözleşmesi kayıtlarını usulüne uygun şekilde günü gününe tutmak ve bu kapsamda mevcut bilgi, belge ve kayıtları genel kolluk kuvvetlerinin her an incelemelerine hazır bulundurmak zorundadırlar. Ancak araç kiralayanın kamu kurum veya kuruluşu olması hâlinde sadece kamu kurum veya kuruluşuyla yapılan sözleşme ile araç bilgileri sisteme kaydedilir. Araç kiralama esnasında gerçeğe aykırı kimlik kullananlar ile birinci fıkra kapsamında elde edilen bilgi ve kayıtları, hukuka aykırı olarak kullanan, bir başkasına veren, yayan veya ele geçiren kişi, 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu hükümlerine göre cezalandırılır. Birinci fıkrada belirtilen yükümlülüklerle aykırı hareket edenlere beş bin Türk Lirası, gerçeğe aykırı kayıt tutan veya bilgi verenlere on bin Türk Lirası idari para cezası, mülki idare amirlerince verilir. Bu Kanuna göre verilen idari para cezaları tebliğinden itibaren 1 ay içinde ödenir. İşlenen bir suçun gizlenmesi amacıyla bilgilerin yok edilmesi hâlinde işletme ruhsatı iptal edilir. Bu fıkra göre idari yaptırımların uygulanması ceza soruşturması ve kovuşturması yapılmasına engel değildir." şeklinde bir düzenleme mevcuttur. Bu durumda mevzuat gereğince araç kiralama firmalarının tutmakla yükümlü olduğu verilerin hatalı ve eksik girilmiş veya girilmemiş olmasından araç kiralama firmaları sorumlu olacaktır. Araç kiralama firmaları ile birlikte ortak veri sorumlusu

kabul edilebilecek yazılım şirketlerinin bu süreçte veri işleme faaliyetinde bir sorumluluğu olmadığı değerlendirilmektedir. Kısacası belirtilen hal ve koşullar altında toplanan veri üzerinde, söz konusu veri ilk elden başka bir veri sorumlusu tarafından elde edilmiş olsa bile, ilerleyen süreçlerde söz konusu kişisel veriler ile ilgili veri sorumlusu gibi hareket eden herkes Kanun gereğince veri sorumlusunun yükümlülükleri ile bağlıdır.

2. Yazılım Şirketlerinin Sundukları Hizmeti Bulut Teknoloji Altyapısı ile Gerçekleştirmelerine İlişkin Değerlendirme

- İhbara konu olayda yazılım şirketleri çevrimiçi ağ (network) üzerinden bulut bilişim (BT) vasıtasıyla araç kiralama firmalarına hizmet sunmaktadır. Bulut bilişim, ağ tarayıcılarıyla erişilen siteler sayesinde uygulamaların internet üzerinden kullanılmasını sağlamaktadır. Bir şirket, bulut bilişim kullanmakta ise bu şirketin BT altyapısı şirket dışında bulut bilişim sağlayıcı tarafından muhafaza edilen bir veri merkezinde depolanmaktadır. Üç ana bulut servisi türü vardır: Yazılım Hizmetleri (SaaS), Platform Hizmetleri (PaaS) ve Altyapı Hizmetleri (IaaS).
- Standart süreçlerde yazılım şirketleri tarafından sunulan hizmetin, SaaS (Software as a Service) şeklinde şirketler tarafından geliştirilen yazılım üzerinden araç kiralama firmalarına bir nevi platform olarak hizmet sunulması olduğu anlaşılmıştır. SaaS hizmetinin gereği olarak veri tabanı ve yazılımın yönetimi yazılım şirketlerinde olup müşterilerde (araç kiralama firmalarında) ve gerektiğinde teknik destek ve geliştirme sağlayabilmesi için yazılım şirketlerinde "admin" yetkisine sahip kullanıcıların atandığı görülmüştür. Sunulan hizmet türü hazır bir SaaS hizmeti olduğundan kaynak kod halinde sunulmadığı, müşterinin yazılım kodlarına müdahalesine izin verilmediği, bu sebeple müşterinin yönetim yetkilerinin içerikle sınırlı olduğu, sistemin düzgün işlemesi için gerekli fonksiyonları değiştirmeye yetkisinin ise bulunmadığı tespit edilen bir başka husustur.

3. Veri İşleme Faaliyeti Sırasında İlgili Kişilerin Aleyhlerine Ortaya Çıkan Sonuçlara İtiraz Etme Haklarına ve Profillemeye İlişkin Değerlendirme

- Uluslararası uygulamada bireyin davranışlarının analiz edilerek bunu izleyen davranışları hakkında tahminlerde bulunmak adına bireyin kişisel verilerinin otomatik olarak işlenmesi "profillemeye" olarak adlandırılmaktadır. "Tahmin" kelimesinin kullanılması aslında profil oluşturmanın bir kişi hakkında bir tür değerlendirme veya yargı içerdiğini göstermektedir.
- Profillemenin her zaman olumsuz bir eylem olduğunu söylemek doğru değildir. Bireylerin temel haklarını ve güvenliklerini tehdit etmeyecek şekilde bir noktaya kadar profillerinin oluşturulması makul görülmektedir. Bireyin profiline ilişkin kullanılan kıstaslar ve işleme süreci hangi noktaya

kadar profillemeye izin verilebileceğinin olay bazında incelenmesi gereğini de birlikte getirmektedir. Söz konusu profil oluşturma sırasında istenmeyen/hedeflenmeyen sonuçların ortaya çıkması da muhtemeldir. Oluşturulan profil, ilgili kişiyi tek bir kategoriye sabitleyerek seçeneklerini kendisine önerilenlerle sınırlayabilir öyle ki hatalı tahminlere dayanan varsayımlar nedeniyle bir hizmetten kısmen veya tamamen yararlanamama sonucunda ilgili kişinin ayrımcılığa uğramasına ya da olumsuz bir sonuçla karşılaşmasına da sebebiyet verebilir.

- 6698 sayılı Kanun'un lafzında ilgili kişinin haklarının sayıldığı 11'inci maddeye bakıldığında ilgili kişilerin "işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme" hakkı olduğu görülmektedir. Yani mevzuatın, profillemeye faaliyeti için gerekli olan otomatik veri işleme nedeniyle olumsuz bir sonuç doğacağı durumlarda ilgili kişilere bu işlemeye itiraz etme hakkı tanıdığını söylemek mümkündür.

- Veri sorumluları genel ilkelere uygun hareket ettikleri ve kişisel verilerin işlenmesinde yasal bir temele sahip oldukları sürece profil oluşturma ve otomatik karar verme sistemleri kullanma hakkına sahiptir. Bu kapsamda, ilgili kişilerin, kara liste uygulaması amacıyla profillemeye tabi olduğu hallerde dahi olay özelinde bu durumu Kanununun 4'üncü maddesi gereğince genel ilkelere ve 5'inci maddesi gereğince belirtilen şartlara uygun veri işlendiği şeklinde yorumlamak mümkündür. Ancak 5'inci madde gereğince ilgili kişinin açık rızası dışında kalan hallerden olan "ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" hali tespit edilirken veri sorumluları tarafından;

- Kişisel verinin işlenmesi sonucunda elde edilecek menfaat ile ilgili kişinin temel hak ve hürriyetlerinin yarışabilir düzeyde olması,
- Söz konusu menfaate ulaşılabilmesi bakımından kişisel veri işlenmesinin zorunluluk arz etmesi,
- Meşru menfaatin hali hazırda mevcut, belirli ve açık olması,
- İlgili kişinin temel hak ve hürriyetleri ile yarışabilir nitelikte olan meşru menfaatin elde edilmesi halinde bir yarar sağlanacak olması ve kişisel veri işlenmeksizin başkaca bir yol ve yöntemle bu yararın ortaya çıkmasının mümkün olmaması,
- Meşru menfaat belirlenirken söz konusu yararın çok sayıda kişiyi etkilemesi, yalnızca kâr elde edilmesi ya da ekonomik yararın sağlanması amacına yönelik olmaması, iş süreçlerini ya da bir işleyişi kolaylaştırması (örneğin bir birim ya da az sayıda personel nezdinde değil, kurumsal olarak geneli etkileyecek şekilde) gibi şeffaf ve hesap verilebilir nitelikleri haiz kriterlerin esas alınması,

- Bu açıdan ilgili kişinin başta kişisel verilerinin korunması olmak üzere temel hak ve hürriyetlerinin zarar görmesini engellemek amacıyla öngörülebilir, açık ve yakın her türlü tehlikeden uzak tutulması,
- Kişisel verilerin bir veri kayıt sisteminde amaçla sınırlı olarak hukuka uygun işleyişinin temini ile zararı ve ihlalleri engellemek için her türlü teknik ve idari tedbirin alınması,
- Kişisel verilerin işlenmesinde genel ilkelere uygunluğun sağlanması,
- Bu kapsamda, kişinin temel hak ve hürriyetleri ile veri sorumlusunun meşru menfaatinin karşılaştırılarak denge testinin yapılması

hususlarının değerlendirilmesi gerekmektedir. Yapılacak değerlendirmede, ilgili kişinin temel hak ve özgürlükleri ile veri sorumlusunun söz konusu bilgiyi otomatik işleme tabi tutması ile sağlayacağı menfaatler arasında denge testi yapılırken yarışan menfaatlerden hangisinin ağır bastığı veri sorumlusunca tespit edilmelidir. Ancak bu konudaki şikâyetlerin değerlendirme sürecinde dikkate alınacak kriterlerin bunlarla sınırlı olmayacağı, her somut olay özelinde Kurulca ilave ölçütlerin de gündeme gelebileceği tabidir.

- İhbar konusu kapsamında ise söz konusu inceleme sırasında bazı araç kiralama firmalarının internet sitelerinde, kiralanan araçların bu yazılım üzerinden takip edilebileceği hususunda otomatik veri işleme faaliyeti gerçekleştirildiği beyan edilmektedir. Araçlarının konum bilgilerinin takip edildiği durumlarda veri sorumluları tarafından ilgili kişilerin kişisel verileri işlenirken, konum verilerinin işlenmesinin özellikle ilgili kişilerin yaşam alışkanlıklarını ortaya çıkarabileceği akılda tutulmalıdır. Kullanılan uygulamaların, gerçekleştirilen yolculukların, iş yeri ve ikamet yeri ile sürücünün ziyaret ettiği diğer yerlerin konum bilgilerinin öğrenilmesine olanak sağlamasının kişi hakkında bir profil çıkarılmasına ve yaşam alışkanlıklarından hareketle ilgili kişinin özel nitelikli verilerini de ihtiva edebilecek (dini, inancı, cinsel hayatına ilişkin bilgiler vb.) pek çok verisinin ortaya çıkmasına sebebiyet vererek ilgili kişi açısından olumsuz bir sonuç meydana getirebilecektir. Buna göre, konum verilerinin toplanması yoluna gidilmesinin istisnai olarak uygulanan bir durum olması gerektiği değerlendirilmektedir.

- Öte yandan konum bilgilerinin yanı sıra müşterilerin sözleşme ilişkisi boyunca kiraladığı araca verdiği zararın veya aracı teslim sürecinde yarattığı gecikmenin ya da ödeme konusunda yol açtığı sorunların veri sorumlusunca bir sisteme girilerek kaydediliyor oluşu, başlı başına konum izlemesinde olduğu gibi bir profillemeye faaliyetini gündeme getirmeyecektir. Çünkü öncelikle veri sorumlusu tarafından girilen verilerin otomatik işleme tabi tutularak ilgili kişiler hakkında mekanik bir sonucun çıkması profillemeye beklenen sonuçtur. Burada ise “A kişinin teslim ettiği aracın ön

camının çatlamış olduğu görüldü/ koltuklarda sigaradan kaynaklı olduğu tespit edilen yanıkların olduğu görüldü vb.” gibi hususların veri sorumlusunca “kara liste” başlığı altında kayıt altına alınması ancak kısmen otomatik olan bir veri işlemedir. Ancak, kara liste kaydı sonucunda kişi hakkında otomatik bir karara varılması söz konusu ise (bu kişiye araç kiralanamaz uyarısı vb.) bu durumda uygulamanın otomatik bir işleme olduğunu söylemek mümkün olacaktır.

- Kanunun 5’inci maddesi gereğince veri sorumlularının meşru menfaati gereği veri işleminin zorunlu olduğu durumlarda denge testi yapılması gerekmektedir. Araç kiralama firmalarının faaliyet alanları ile ilgili olarak, bu firmaların çalışanları ve akdi ilişkide oldukları gerçek ve tüzel kişilerce bilinen; işletmenin ticari başarısı ve verimliliği için önem arz eden; rakiplerine karşı kendisi için avantaj teşkil eden; gerek kamuya gerekse ilgisi olmayan şahıslara açıklanmaması gereken; firmanın iç işleyişi, mali ve iktisadi durumu, faaliyet hedef ve stratejisi, fiyatlandırma uygulaması bilgisi, pazarlama stratejisi ve taktikleri, müşteri potansiyeli ve ağ bilgisi, her türlü sözleşme, protokol bilgileri gibi bu türden tüm bilgi/belgeyi ifade eden ve kendisini zarara uğrattığını düşündüğü bu kişilere ilişkin oluşturduğu kayıtlar şirket ticari sırrı olarak kullanılabilir niteliktedir. TTK’nin 527’nci maddesi hükmü gereğince 404’üncü madde hükmü saklı kalmak üzere, görevi dolayısıyla incelemesine sunulan defter ve belgeleri inceleyenlerin, elde ettikleri veya verilen bilgilerden öğrendikleri iş ve işletme sırlarını açıklamaları yasaktır. Aksi hâlde bu kişiler şirketin maddi ve manevi zararını tazmin etmek zorundadır. TCK’nın 239’uncu maddesinde ise bu minvalden verileri yetkisiz kişilere verenler veya ifşa edenler hakkında cezai yaptırım uygulanacağı öngörülmüştür. Söz konusu ticari sırlar aynı zamanda müşterilere ilişkin kişisel veriler de içermektedir. Kanuni yükümlülükler gereğince de işletme faaliyetleriyle sınırlı olmak üzere kullanılacak bu verilerin sadece kişinin “kara liste”ye kaydedilmesine sebebiyet verecek bir davranışı olmasından bahisle kişinin özel hayatının gizliliğini ve kişisel verilerinin korunmasını isteme hakkını ihlal etmeyeceği değerlendirilmektedir. Ancak belirtilen alana girilecek verilerin sınırlı olmadığı düşünüldüğünde kişinin ayrımcılığa uğramasına sebebiyet verecek ve davranışsal durumlar haricinde kalan genel ve özel nitelikli verilere yer verilmesi durumunda artık bir ticari sırrın varlığından bahsetmek mümkün değildir (Örneğin; cinsel yönelimi sebebiyle kişinin kara listeye alınarak araç kiralama hizmetinden yararlandırılmaması). Elbette ilgili kişinin kara listeye alınması sebebi ne olursa olsun şunu belirtmekte fayda vardır ki bu sebebe erişim hakkı olan herkes kendi değerlendirme ve imtiyaz hakkına sahiptir, ilgili kişinin A firmasından hizmet alamıyor olması B firmasından da hizmet alamayacağı anlamına gelmemektedir. Bu kapsamda sisteme girilen verilerin mevzuata uygun edinilip işlendiği yönünde Kanun gereğince veri sorumlusu sıfatını haiz olan taraf araç kiralama firmalarıdır.

- Araç kiralama firmalarının acentelerinde veya şubelerinde söz konusu listede yer alan ilgili kişiler hakkında yaptığı yorumun görünür kılınması ise bu ticari sırrın kullanımından öteye gitmediği sürece meşru menfaat kıstasına uygun bir işleme olarak kabul edilebilir. Ancak söz konusu ihbarda yer alan yazılım şirketlerinin araç kiralama firmalarının müşterileri hakkında yaptığı yorumlara dayanan "kara liste" uygulamasını yine aynı yazılımı kullanmakta olan diğer araç kiralama firmalarınca da görünür kılması ve hatta bu özelliği bir pazarlama stratejisi olarak öne sürmesi ne meşru menfaat kıstası ne de araç kiralama firmalarının talimatı doğrultusunda yapılan hukuka uygun bir veri işleme olarak değerlendirilebilir.

4. Kişisel Verilerin Kara Liste Uygulaması ile Diğer Kullanıcıların Erişimine Açılmasına İlişkin Değerlendirme

- Kanununun 8'inci maddesinde "(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz. (2) Kişisel veriler; 5'inci maddenin ikinci fıkrasında, yeterli önlemler alınmak kaydıyla, 6'ncı maddenin üçüncü fıkrasında, belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir. (3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır." hükmü düzenlenmiştir.

- Kişisel verilerin "depolanması, muhafaza edilmesi ve aktarılması" eylemleri kişisel veriyle aracısız yapılan doğrudan işlemlerle ilgilidir. Veri sorumlusu aktarım için hizmet alabileceği gibi bu veriyi kendisi aktarmayı da seçebilir. Ancak veriyi aktaran kim olursa olsun (ister veri işleyen, ister veri sorumlusu) bu kişisel veriye erişebilir, onun ne olduğunu görebilir ve kullanabilir. Bu sebeple yapılacak nitelendirmeye göre veriyi aktarma yetkisi olan kişinin sorumluluğu belirlenmelidir.

- Araç kiralama firmalarının müşterileri hakkında yaptıkları değerlendirmelerin ortak bir veri tabanına kaydedilerek diğer firmalarca yapılan yorumların da bu alana eklenebiliyor olması hem müşteri sırrının (ticari sır) ifşası hem de kişisel verilerin ifşası anlamına gelmektedir. Bu kapsamda artık yalnızca araç kiralama firmalarının veri sorumlusu olduğundan bahsetmek mümkün değildir. Yazılımın özelliği olarak sunulan bu veri aktarım faaliyeti artık araç kiralama firmalarınca girilen ilgili kişilere ait kişisel verilerin yazılım şirketleri tarafından kullanılması anlamına gelmektedir. İlgili kişilere ait bu tarz verilerin aktarılabilmesi için Kanun'un 5 ve 6'ncı maddelerine dayanan bir hukuka uygunluk sebebi bulunmalıdır. "Kara liste" uygulamasının doğası gereği ilgili kişilerin bu duruma rızası olması beklenemeyeceğinden 5'inci maddenin (2) numaralı ya da 6'ncı maddenin (3) numaralı fıkrasındaki şartların varlığı gerekmektedir. Yazılım şirketlerinin araç kiralama firmalarının müşterilerine ait verileri işleme noktasında bir yasal yükümlülüğü bulunduğunu söylemek mümkün olmadığından bu tarz verilerin ancak yukarıda açıklanan meşru menfaat kıstası çerçevesinde söz

konusu araç kiralama firmasının “iş ortakları, şubeleri veya acenteleri” ile paylaşılmasının mevzuat uyarınca mümkün olacağı değerlendirilmektedir. Ancak burada aktarıma taraf olacak kişi ve kişi gruplarının veri sorumlusu sıfatıyla ilgili kişilere aydınlatma metni aracılığıyla aktarım öncesi bildirilmiş olması gerekmektedir. Oysaki görülen uygulamada söz konusu aktarım faaliyetinin araç kiralama firmalarınca direkt kendilerinden diğer firmalara değil öncelikli olarak yazılıma yapıldığı; bu durumun da araç kiralama firmalarınca paylaşımına açılan verilerin, hangi firmalarca görülebileceğinin öngörülememesine sebebiyet vermesinden ötürü başta veri işleminin temel ilkelerine sonrasında da veri aktarımının genel prensiplerine aykırılık oluşmasına neden olduğu değerlendirilmektedir.

Yukarıda yer alan açıklamalar ışığında veri işleme süreçlerinin fiziksel olarak nasıl yürütüldüğünün söz konusu ihbarda yer alan iddialar, veri sorumlularından alınan bilgi, belgeler ve ilgili mevzuat hükümleri çerçevesinde değerlendirilmesi neticesinde;

- Yazılım şirketlerinin sunduğu bulut tabanlı SaaS hizmetinin gereği olarak veri tabanını ve yazılımın yönetimini bünyesinde barındırması; müşterilerde (araç kiralama firmalarında) ve gerektiğinde teknik destek ve geliştirme sağlayabilmesi için kendi bünyesinde ‘admin’ yetkisine sahip kullanıcılar ataması; yazılım bakımı ve geliştirmesi için aylık olarak düzenli bir ücret alması ve sözleşmelerini belirli periyodlarla yenilemesi; söz konusu yazılımın telif haklarının bu Şirketlere ait olması ve kullanıcılarına lisans vererek ilgili programı kiralaması; sunulan hizmet türü hazır bir SaaS hizmeti olduğundan kaynak kod halinde sunulmaması, yazılım şirketlerinin müşteri olan araç kiralama firmalarının yazılım kodlarına müdahalesine izin verilmemesi, bu sebeple müşterinin yönetim yetkilerinin içerikle sınırlı olması, müşterinin sistemin düzgün işlemesi için gerekli fonksiyonları değiştirme yetkisinin ise bulunmaması ve elde edilen bulgulara göre şirketlerin uygulama içinde “kara kutu” bölümü oluşturarak araç kiralama firmalarınca girilen ilgili kişiler hakkındaki bu değerlendirmeleri uygulamalar vasıtasıyla diğer tüm kullanıcılara açılabilmesi; yazılım şirketleri her ne kadar araç kiralama firmalarıyla yaptığı sözleşmelerde olası kara liste uygulamaları için sorumsuzluk kaydı koymuşsa da, araç kiralama firmalarının uygulamaya girerek kaydettiği verileri, Kanunun 5’inci maddesinde yer alan herhangi bir işleme şartına dayanmaksızın kendi ticari faaliyetleri kapsamında kişisel verilerin bir kuruluştan diğerine nasıl aktarılacağına karar vermesi hallerinde 6698 sayılı Kanunun 3’üncü maddesi gereğince yazılım şirketlerinin veri sorumlusu olarak hareket edeceği kanaatine varılmıştır. Araç kiralama firmalarının ise belirtilen veriler üzerinde sorumlulukları yazılım şirketi ile elbirliği halinde devam edecektir.

- Kanunun 12'nci maddesi gereğince veri sorumlusu olarak hareket eden yazılım şirketlerinin müşterilere ilişkin araç kiralama firmalarınca ilk elden girilen verilere hukuka aykırı olarak erişilmesini önlemek; bu verilerin muhafazasını sağlamak yükümlülüklerine aykırı hareket ederek söz konusu verileri diğer müşterilerinin de erişimine açmış olacağı; aktarımın direkt veri sorumlusundan diğer araç kiralama firmalarına değil öncelikli olarak yazılıma yapıldığı; bu durumun da paylaşımına açılan verilerin hangi firmalarca görülebileceğinin bilinmemesine yol açacağı; veri işleyen veri sorumlusunun verdiği yetki dışında herhangi bir işlem yapma imkanı bulunmamasına rağmen yazılım şirketlerinin bu veriyi bilinmeyen sayıda ve nitelikte kullanıcıya açarak Kanunun 4'üncü maddesinin 2 numaralı fıkrası hükmü gereğince kişisel verilerin işlenmesinde "hukuka ve dürüstlük kurallarına uygun olma", "belirli, açık ve meşru amaçlar için işlenme" ve "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerine ve Kanunun 8'inci maddesinde belirtilen ilgili kişinin açık rızası ya da 5'inci maddenin 2'nci fıkrasında düzenlenen işleme şartlarından biri olmadığı halde üçüncü kişilere aktarım suretiyle hukuka aykırı olarak işlenmesine sebebiyet vereceği kanaatine varılmıştır.

Bu kapsamda;

- Araç kiralayan gerçek kişi müşterilerin kişisel verilerinin de yer aldığı "kara liste" uygulamaları ile Kanunun 12'nci maddesinde düzenlenen müşterilere ilişkin araç kiralama firmalarınca ilk elden girilen kişisel verilere hukuka aykırı olarak erişilmesini önlemek, bu verilerin hukuka aykırı olarak işlenmesini önlemek ve muhafazasını sağlamak yükümlülüklerine aykırı olarak söz konusu verilerin yazılım şirketlerinin müşterileri olan başka araç kiralama firmalarının erişimine de açılması; fiili durumun araç kiralama firmalarınca da bilinmesi; aktarımın direkt bir araç kiralama firmasından diğer araç kiralama firmasına değil öncelikli olarak yazılıma yapılması; yazılım şirketlerinin bu veriyi bilinmeyen sayıda ve nitelikte kullanıcıya (diğer araç kiralama firmalarına) açması halinde hem veri sorumlusu haline geleceği, hem de Kanunun 4'üncü maddesinin 2 numaralı fıkrası hükmü gereğince kişisel verilerin işlenmesinde "hukuka ve dürüstlük kurallarına uygun olma", "belirli, açık ve meşru amaçlar için işlenme" ve "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerine ve Kanunun 8'inci maddesinde belirtilen ilgili kişinin açık rızası ya da 5'inci maddenin (2) numaralı fıkrasında düzenlenen işleme şartlarından biri olmadığı halde üçüncü kişilere aktarmak suretiyle hukuka aykırı olarak işlenmesine sebebiyet vereceği dikkate alındığında, ihbar konusu olayda araç kiralama yazılımı üreten ve satan şirketlerin araç kiralama firmaları ile birlikte ortak veri sorumlusu olarak hareket ettiğine,

- Öte yandan bu minvalde işlenen kişisel verilerin Kanuna aykırılık doğuracağı dikkate alındığında bu yönde işlenmiş kişisel verilerin Kanununun 7'nci maddesinde düzenlenen hükümler ile Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik hükümlerine uygun şekilde imha edilmesi hususunda ihbar kapsamında incelenen veri sorumlularının talimatlandırılmasına

karar verilmiştir.

2021/1262 sayılı KVKK Kararı

Bir sigorta şirketi tarafından ilgili kişinin banka verilerinin işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 16/12/2021 tarihli ve 2021/1262 sayılı Karar Özeti

Karar Tarihi : 16/12/2021

Karar No : 2021/1262

Konu Özeti : Bir sigorta şirketi tarafından ilgili kişinin banka verilerinin işlenmesi

Kuruma intikal eden şikâyet dilekçesinde özetle; ilgili kişinin banka bilgilerini veri sorumlusu sigorta şirketi ile paylaşmadığı halde bu bilgilerin sigorta şirketi tarafından hukuka aykırı olarak işlendiği, ilgili kişinin konuya ilişkin olarak veri sorumlusundan vekili aracılığıyla bilgi talebinde bulunduğu, ayrıca kişisel verilerinin silinmesi veya yok edilmesinin talep edildiği ancak başvurusunun yanıtız bırakıldığı belirtilerek veri sorumlusu hakkında 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gerekli idari yaptırımların uygulanması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup verilen cevapta özetle;

- İlgili kişinin yazılı başvurusunun öncelikle usulü açıdan değerlendirildiği, ilgili kişinin kendilerine başvurusunda, dilekçe ekinde yer alan vekâletnamenin dava aşamasındaki yetkileri içeren “genel vekâletname” niteliğinde olduğu, vekaleten istenen bilgilerin kişiye sıkı sıkıya bağlı hak olarak değerlendirilen kişisel verilerin işlenmesine yönelik olduğundan ve kişisel veri ve daha hassas bir koruma gerektiren özel nitelikli kişisel verileri de içerebilme ihtimali bulunduğundan ilgili kişi adına bilgi talep eden ve Kişisel Verilerin Korunması Kanununun 11 inci maddesi kapsamındaki hakları ilgili kişi adına kullanan vekilin, bu hakları kullanabilmek için özel yetki içeren vekaletle sahip olması gerektiğinin değerlendirildiği,
- Açık bir şekilde özel vekaletname ile başvuru yapılabileceğinin “Başvuru Formu”nda yazılı olarak belirtilmesine rağmen, taraflarına usulüne uygun bir başvuru yapılmadığı; veri sorumlusuna başvuru yolunun tüketilmeden Kurula şikayette bulunulamayacağı bu nedenle Kanununun 14 üncü maddesi gereği ilgili kişinin şikayetinin reddedilmesi gerektiği,

- Taraflarının sigortacılık faaliyetlerini yürütmekte ve bu amaçla çeşitli sigorta acenteleri ile işbirliği yapmakta olduğu, şirketlerinde ilgili kişiye ait, acenteleri sıfatıylaBankası aracılığı ile yapılmış sigorta poliçelerinin olduğu ve söz konusu banka bilgilerinin poliçelerle bağlantılı olarak acenteleri ... Bankası tarafından sağlandığının tespit edildiği,
- Taraflarına iletilen banka bilgilerinin; hesap tipi, banka kodu, hesap türü, şube kodu, döviz bilgisi, hesap numarası, kullanım amacı, IBAN numarası bilgileri olduğu; anılan verilerin işleme amacının poliçe prim tahsilatının yapılabilmesi ve poliçeden doğan yükümlülüklerinin yerine getirilmesi olduğu,
- Şikâyete konu bilgi paylaşımının acenteleri sıfatıyla ... Bankası tarafından ilgili kişi için tanzim edilen poliçelere istinaden gerçekleştirildiği, bu doğrultuda satışını gerçekleştirdikleri poliçelere ilişkin hasarın tespiti ve tanzim edilmesinin hukuki bir zorunluluk olduğu,
- Şikayete konu olayda, ilgili kişiye ait kasko poliçesi kapsamındaki hasar talepleri için Tüketici Hakem Heyetine başvurulduğu, verilen kararda ilgili kişiye ödeme yapılmasına hükmedildiği, poliçeden doğan kesinleşmiş yargı kararı ile sabit hasarı tazmin etme yükümlülüğünün yerine getirilmesi amacıyla Kişisel Verilerin Korunması Kanununun 5 inci maddesinin (2) numaralı fıkrasının (c) bendinde belirtilen "Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması" ve (ç) bendinde belirtilen "Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" hukuki sebeplerine dayanılarak Şirket kayıtlarında bulunan banka hesabına ödeme yapılması suretiyle ilgili kişinin banka bilgilerinin işlendiği,
- Yapılan araştırmada, ilgili kişinin şikâyete konu bilgilerinin yurt içi ve yurt dışındaki herhangi bir kişi ya da kurumla paylaşılmadığının tespit edildiği, söz konusu verilerin yalnızca Tüketici Hakem Heyeti kararının yerine getirilmesi amacıyla, ilgili Banka nezdindeki sigorta şirketi hesaplarından şikâyete konu banka hesap numarasına ödeme işlemlerinin tamamlanması amacıyla işlendiği,
- Tüketici Hakem Heyeti kararının yerine getirilmesi amacıyla yapılan ödemeye ilişkin hesap bilgilerinin yasal yükümlülük gereği 10 yıl muhafaza edileceği ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde, Kişisel Verileri Koruma Kurulunun 16/12/2021 tarih ve 2021/1262 sayılı Kararı ile;

- Kanun'un "Tanımlar" başlıklı 3'üncü maddesinde "ilgili kişi"nin, kişisel verisi işlenen gerçek kişi; "veri sorumlusu"nun ise kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt

sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlandığı, bu çerçevede şikâyete konu olayda sigorta şirketinin veri sorumlusu olduğu, Bankanın sigorta acentesi olarak ilgili kişi ve veri sorumlusu arasında sözleşme ilişkisinin kurulmasında veri sorumlusu adına hareket ederek veri sorumlusuna veri işleyen olarak hizmet sunduğu,

- Kanun'un "Veri Sorumlusuna Başvuru" başlıklı 13'üncü maddesinde "(1) İlgili kişi, bu Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir. (2) Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır... (3) Veri sorumlusu talebi kabul eder veya gerekçesini açıklayarak reddeder ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir..." hükmünün yer aldığı,

- Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in (Tebliğ) "Başvuru Usulü" başlığını taşıyan 5'inci maddesinin birinci fıkrasında "İlgili kişi, Kanunun 11 inci maddesinde belirtilen hakları kapsamında taleplerini, yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletir." hükmü ifade edilerek başvuruda bulunması zorunlu unsurlar; ad, soyad, başvuru yazılı ise imza, Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarası, tebligata esas yerleşim yeri veya iş yeri adresi, varsa bildirim esas elektronik posta adresi, telefon ve faks numarası ile talep konusu olarak ayrıca sayıldığı,

- Tebliğ'in "Başvuruya cevap" başlıklı 6'ncı maddesinin "(1) Veri sorumlusu bu Tebliğ kapsamında ilgili kişi tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlüdür. (2) Veri sorumlusu, başvuruyu kabul eder veya gerekçesini açıklayarak reddeder. (3) Veri sorumlusu, cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. (4) Cevap yazısının; a) Veri sorumlusu veya temsilcisine ait bilgileri, b) Başvuru sahibinin; adı ve soyadını, Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarasını, yabancılar için uyruğunu, pasaport numarasını veya varsa kimlik numarasını, tebligata esas yerleşim yeri veya iş yeri adresini, varsa bildirim esas elektronik posta adresini, telefon ve faks numarasını, c) Talep konusunu, ç) Veri sorumlusunun başvuruya ilişkin açıklamalarını, içermesi zorunludur. (5) Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak, işlemin ayrıca bir maliyet gerektirmesi halinde, 7 nci maddede belirtilen ücret alınabilir. Başvurunun, veri

sorumlusunun hatasından kaynaklanması halinde alınan ücret ilgiliye iade edilir. (6) İlgili kişinin talebinin kabul edilmesi halinde, veri sorumlusunca talebin gereği en kısa sürede yerine getirilir ve ilgili kişiye bilgi verilir.” hükmünü haiz olduğu,

- Somut olayda, ilgili kişinin vekili aracılığıyla veri sorumlusuna ilettiği başvurunun veri sorumlusu tarafından teslim alınması ve özel yetki içeren vekâletname bulunmaması sebebiyle cevaplanmamasına karşılık, kişisel verilerin korunması mevzuatında ilgili kişilerin vekilleri aracılığıyla yapacakları başvurularda özel vekaletname gerektiğine ilişkin bir düzenleme bulunmadığından veri sorumlularınca vekâletnamede “özel yetki” şartı aranmaması gerektiği,

- Ayrıca Tebliğ’in “Başvuruya cevap” başlıklı 6’ncı maddesinin ikinci fıkrasında “Veri sorumlusu, başvuruyu kabul eder veya gerekçesini açıklayarak reddeder.” Hükmüne karşılık veri sorumlusunun ret gerekçesini ilgili kişiye bildirmediği anlaşıldığından veri sorumlusunun Tebliğ’e aykırı hareket ettiği,

- Öte yandan Kanun’un, kişisel verilerin işlenmesine ilişkin “Genel İlkeler”i düzenleyen 4’üncü maddesinin (1) numaralı fıkrasında, “Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.” hükmünün yer aldığı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin;

a) Hukuka ve dürüstlük kurallarına uygun olma,

b) Doğru ve gerektiğinde güncel olma,

c) Belirli, açık ve meşru amaçlar için işlenme,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,

- Kanun’un “Kişisel Verilerin İşlenme Şartları” başlıklı 5’inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması

için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanun'un "Veri Güvenliğine İlişkin Yükümlülükler"i düzenleyen 12'nci maddesinin (1) numaralı fıkrasında veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idarî tedbirleri almak zorunda olduğunun hükme bağlandığı,

- İlgili kişinin veri sorumlusundan sigortalı olduğu, poliçeden doğan ve Tüketici Hakem Heyeti kararı ile kesinleşen tazminatın ilgili kişiye ödenebilmesi amacıyla veri sorumlusunun Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (c) bendinde belirtilen "Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması" ve (ç) bendinde belirtilen "Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" hukuki sebeplerine dayanarak ilgili kişinin banka bilgilerini işlediği ve somut olayın hukuka aykırılık teşkil etmediği,

- Diğer taraftan veri sorumlusu ile ilgili kişi arasındaki sigorta sözleşmesinin/ilişkisinin sona erdiği gösterir herhangi bir belgenin Kuruma sunulmadığı hususları ile veri sorumlusunun hasar dosyası kayıtlarında Tüketici Hakem Heyeti kararının yerine getirilmesi amacıyla yapılan ödemeye ilişkin hesap bilgilerinin yasal yükümlülük gereği 10 yıl muhafaza edileceği beyanı dikkate alındığında Kanun'un 7'nci maddesinin (1) numaralı fıkrası uyarınca ilgili kişinin kişisel verilerinin işlenmesini gerektiren sebeplerin ortadan kalkmadığı

değerlendirmelerinden hareketle;

- Veri sorumlusunun yasal temsilci vekâletnamelerinde "özel yetki" aramaması hususunda uyarılması, vekâletnamelerde "özel yetki" bulunması gerektiğine dair veri sorumlusu tarafından tanzim edilen ilgili kişi başvuru formu, aydınlatma metni ve kişisel verilerin korunması ile alakalı diğer dokümanlardan bu ibarenin kaldırılarak Kurula bilgi verilmesi ile Tebliğ'in 6'ncı maddesi uyarınca başvuruların gerekçesi açıklanarak reddedilmesi hususlarında veri sorumlusunun talimatlandırılmasına,

- Veri sorumlusunun, ilgili kişinin kişisel verileri niteliğindeki banka bilgilerini Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (c) bendinde belirtilen "Bir sözleşmenin kurulması veya ifasıyla

doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması" ve (ç) bendinde belirtilen "Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" hukuki sebeplerine dayanarak işlediği değerlendirildiğinden şikâyete ilişkin Kurul tarafından tesis edilecek bir işlem bulunmadığına,

- Kişisel verilerin silinmesi veya yok edilmesi talebinin yerine getirilmediği iddiası bakımından, ilgili kişi ile veri sorumlusu arasındaki sigorta sözleşmesinin/ilişkisinin devam ettiği, veri sorumlusunun yasal yükümlülüğü gereği ilgili kişinin kişisel verilerini muhafaza etmesi gerektiği dikkate alındığında Kanun'un 7'nci maddesi uyarınca ilgili kişinin kişisel verilerinin işlenmesini gerektiren sebeplerin ortadan kalkmaması sebebiyle konu hakkında Kurul tarafından tesis edilecek bir işlem bulunmadığına

karar verilmiştir.

2021/1258 sayılı KVKK Kararı

İlgili kişinin kişisel verilerinin iş akdinin sona erdiği veri sorumlusu şirket tarafından hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 16/12/2021 tarihli ve 2021/1258 sayılı Karar Özeti

Karar Tarihi : 16/12/2021

Karar No : 2021/1258

Konu Özeti : İlgili kişinin kişisel verilerinin iş akdi sona erdiği şirket tarafından hukuka aykırı olarak işlenmesi

İlgili kişinin, Kuruma intikal eden şikayetinde özetle veri sorumlusu şirket nezdinde 10.12.2018 tarihinde işe başladığı, söz konusu görevden 30.12.2019 tarihinde ayrıldığı, kişisel verilerine yönelik olarak veri sorumlusu şirkete başvuru yapmak istediğinde şirketin bir başvuru formunun bulunmadığı gibi başvuru yollarının da tarafına bildirilmediği, aydınlatma yükümlülüğünün hukuka uygun olarak yerine getirilmediği, özel nitelikli kişisel verilerinin açık rızası olmaksızın işlendiği, veri sorumlusu şirkete parmak izi ve yüz tarama sistemi ile giriş yapıldığı, grup şirketinin farklı firmalarının yurt dışında şubesinin olduğu ve ilgili kişi yurt dışı şubesine ziyarete gittiğinde kişisel verilerinin açık rızası olmaksızın yurt dışına aktarılmış olduğu, kişisel verilerine yönelik yeterli teknik ve idari güvenlik tedbirlerinin alınmadığı, veri sorumlusu şirketin internet sitesinde gizlilik politikasının bulunmadığı hususları ifade edilerek veri sorumlusu şirket hakkında 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Söz konusu iddialara ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabî yazıda özetle;

- İlgili kişinin, şirkette “e-ticaret pazar yerleri yetkilisi” olarak işe başladığı ve daha sonrasında istifa ettiği, istifa süreci yaşanırken ilgili kişinin şirket ile rakip alanda faaliyet gösteren bir firmada çalışmak üzere istifa ettiği bilgisinin şirket tarafından öğrenildiği, bu nedenle ilgili kişiye keşide edilen 07.01.2020 tarihli ihtarname ile “muhatabın iş sözleşmesinin 7.7. maddesi uyarınca 3 yıllık çalışma süresi dolmayan çalışanın, ‘...’ eğitimi nedeniyle ödenen eğitim ücretinin iadesi ve ayrıca iş sözleşmesinin 8. maddesinde düzenlenen rekabet yasağına aykırı davranışları nedeniyle sözleşme

maddesi uyarınca son aylık brüt ücretinin 12 katı tazminat ödemesi gerektiği, aksi takdirde yasal yollara başvurulacağıın...” bildirildiği,

- İlgili kişi tarafından söz konusu ihtarnameye cevaben gönderilen 23.01.2020 tarihli ihtarname ile rekabet yasağı ihlali iddialarının kabul edilmediği, eğitim giderinden işçinin sorumlu tutulamayacağıın bildirildiği, Kanun’un 11’inci maddesi uyarınca veri sorumlusuna başvuru mahiyetinde Şirkete toplam 8 soru yöneltildiği,

- Şirket tarafından ilgili kişinin Kanun’un 11’inci maddesi uyarınca veri sorumlusuna başvuru mahiyetindeki sorularına cevap verildiği, söz konusu cevapta Şirket tarafından tüm çalışanlara ilişkin kişisel bilgilerin 6698 sayılı Kanun’daki önlemlere göre muhafaza edilmekte ve Kanun’dan doğan tüm yükümlülüklerin Şirket tarafından yerine getirilmekte olduğunun belirtildiği,

- Şikâyet dilekçesinde ileri sürülen “kişisel verilere yönelik başvuru yapılmak istendiğinde bir başvuru formunun olmadığı, başvuru yollarının bildirilmediği, aydınlatma yükümlülüğünün yerine getirilmediği” iddialarının tümünün gerçek dışı olduğu, ilgili kişinin imzaladığı iş sözleşmesinin “Kişisel Verilerin İşlenmesi ve Korunması” başlıklı 9’uncu maddesindeki ifadelerden Şirketin aydınlatma yükümlülüğünü yerine getirdiğinin görüleceği,

- Ayrıca, Şirket’in yalnızca kendi çalışanları için kurmuş olduğu sosyal bir ağ olan “...” adresinden de aydınlatma metninin yayınlanmış olduğu ve bu aydınlatma metninde kişisel verilere yönelik başvurunun nasıl yapılacağı ve başvuru yolları konusunda ayrıntılı bilginin yer aldığı,

- Parmak izi ve yüz tarama sisteminin Şirketin ve çalışanların güvenliğini sağlamak amacıyla kullanıldığı, ilgili kişiden de parmak izinin bu kapsamda alındığı, tanımlama sonrası bu verilerin üçüncü kişiler ile paylaşılmadığı ve Kanun doğrultusunda amaçla uygun ve sınırlı ölçüde kullanılmakta olduğu, bunlar haricinde ilgili kişiye ait Şirket tarafından işlenmiş olan bir özel nitelikli kişisel veri bulunmadığı,

- İlgili kişinin yurt dışına aktarılan bir kişisel verisinin bulunmadığı,

- Şikâyet dilekçesinde ileri sürülen kişisel verilere yönelik yeterli teknik ve idari güvenlik tedbirlerinin alınmadığı ve veri sorumlusunun internet sitesinde gizlilik politikasının bulunmadığı iddialarının kabulünün mümkün olmadığı, veri sorumlusunun hem çalışanlarının hem müşterilerinin kişisel verilerinin korunmasını sağlamak için gerekli tüm teknik ve idari güvenlik tedbirlerini almış olduğu

ifade edilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 16/12/2021 tarihli ve 2021/1258 sayılı Kararı ile;

- Kanunun, kişisel verilerin işlenmesine ilişkin “Genel İlkeler”i düzenleyen 4 üncü maddesinin (1) numaralı fıkrasında,

“Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.” hükmünün yer aldığı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin

a) Hukuka ve dürüstlük kurallarına uygun olma,

b) Doğru ve gerektiğinde güncel olma,

c) Belirli, açık ve meşru amaçlar için işlenme,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,

- Kanunun “Kişisel verilerin işlenme şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğunun hükme bağlandığı,

- Somut olayda, veri sorumlusu tarafından sadece şirket personelinin erişim sağlayabildiği bir sosyal medya platformunda veri sorumlusuna başvuru formunun ve aydınlatma metninin yer almakta olduğunun ifade edildiği, ancak söz konusu başvuru formuna savunma dilekçesi ekinde yer verilmediği, aydınlatma metninin ise sadece adı geçen platformdaki başlığının görüntüsünün savunma dilekçesi ekinde yer aldığı,

- Savunma dilekçesi ekinde yer alan ve ilgili kişiyle imzalanmış olan iş sözleşmesinin “Kişisel Verilerin İşlenmesi ve Korunması” başlıklı 9’uncu maddesiyle veri sorumlusunun aydınlatma yükümlülüğünü yerine getirmiş olduğunun iddia edildiği, ilgili kişinin imzalamış olduğu iş sözleşmesinin aydınlatma yerine geçtiği iddia edilen 9’uncu maddesinin hem aydınlatmaya yönelik hem de ilgili kişiden açık rıza alınmasına yönelik ifadeler içeren, aydınlatma ve açık rıza metnlerinin içermesi gereken asgari unsurları da tam olarak içermeyen karma bir metin şeklinde kaleme alındığı, bu nedenle, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin (Tebliğ) 5’inci maddesinin (1) numaralı fıkrasının (f) bendi gereğince kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekliliği sağlanmadığından şekli olarak aydınlatmanın usulüne uygun yapıldığından söz edilemeyeceği,
- Veri sorumlusu tarafından 2020 yılı Temmuz ayından itibaren ayrı ayrı hazırlanmış Çalışan Açık Rıza Metni ve Çalışan Aydınlatma Metninin personellere imzalatıldığı belirtilmiş olsa da Kuruma sunulan bu metinlerde ilgili kişinin imzasının bulunmadığı görülmüş olup ilgili kişinin şikayeti bakımından bu belgelerin esas alınamayacağı,
- Özel nitelikli kişisel veri işleminin açık rıza veri işleme şartına dayandırıldığı ancak “Açık rıza” kavramının Kanun’un 3 üncü maddesinin (1) numaralı fıkrasının (a) bendinde; “Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza” şeklinde tanımlandığı, ilgili kişilerin açık rızasının alınacağı hallerde; rızanın belirli bir konuya ilişkin olması, bilgilendirmeye dayanması ve özgür iradeyle açıklanması gerektiği, veri işlemek üzere verilen açık rızanın geçerli olması için, açık rızanın öncelikle belirli bir konuya ilişkin ve o konu ile sınırlı olarak verilmesi ve veri sorumlusu tarafından açık rıza beyanının hangi konuya ilişkin olarak istenildiğinin açıkça ortaya konulması gerektiği, bununla birlikte; açık rıza bir irade beyanı olduğundan, kişinin özgür bir şekilde rıza verebilmesi için neye rıza gösterdiğini de bilmesi ve kişinin sadece konu üzerinde değil, aynı zamanda rızasının sonuçları üzerinde de tam bir bilgi sahibi olması gerektiği, bu sebeple bilgilendirmenin; veri işleme ile ilgili bütün konularda açık ve anlaşılır bir biçimde, mutlaka verinin işlenmesinden önce yapılması, ayrıca açık rızanın geçerlilik kazanabilmesi için kişinin yaptığı davranışın bilincinde ve kendi kararı sonucunda olması ve açık rızanın özgür iradeyle açıklanmasının önem teşkil ettiği, herhangi bir hususun ilgili kişi tarafından açık rıza verilmesi şartına bağlanmaması, tarafların eşit konumda olmadığı veya taraflardan birinin diğeri üzerinde etkili olduğu durumlarda rızanın özgür iradeyle verilip verilmediğinin dikkatle değerlendirilmesi gerektiği,

- Şikayete konu olayda ise ilgili kişinin açık rızasının alınması için iş sözleşmesine bir madde eklenmesi yoluna gidildiği, ilgili kişiye, özel nitelikli kişisel verilerin işlenmesine dair açık rıza beyanının iş sözleşmesiyle birleşik olarak sunulması sebebiyle ilgili kişinin özel nitelikli kişisel verilerinin işlenmesinde açık rıza verip vermemek konusundaki kararının özgür iradeye dayandığından söz edilemeyeceği, ilgili kişinin iş sözleşmesini imzalamadan işe başlamak gibi bir şansı bulunmadığından; iş sözleşmesinde bir madde olarak yer alan açık rıza şartını kabul etmeme imkanının etkin bir biçimde ilgili kişiye tanınmadığı, bu anlamda veri sorumlusu tarafından dayanılan açık rıza veri işleme şartının hukuka aykırı olduğu,
- Öte yandan, Kanun'un "Genel İlkeler" başlıklı 4'üncü maddesinin (ç) bendinde belirtilen işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi gereği de işlenen verilerin belirlenen amaçların gerçekleştirilebilmesine elverişli olması, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirdiği, sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik olarak veri işlenmesi yoluna gidilmemesi gerektiği anlamına geldiği, ölçülülük ilkesinin ise, veri işleme faaliyeti ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması, diğer bir ifadeyle veri işlemenin amacı gerçekleştirecek ölçüde olması anlamına geldiği, bu kapsamda, kişisel veri işleme faaliyetinin gerçekleşmesi için gerekli olmayan kişisel verilerin toplanmaması ve/veya işlenmemesi gerektiği, veri sorumlusunun amacı çerçevesinde ölçülülük ilkesine uygun olarak ilgili kişiden minimum düzeyde bilgi talep etmesi, bunun dışındaki amaç için gerekli olmayan veri işlemeden kaçınmasının önem arz ettiği,
- Kişisel verilerin işlenmesinin ilgili kişinin iznine bağlı olarak gerçekleştirilse ve belirli bir amaca bağlı olsa bile açık rızanın, aşırı miktarda veri toplanmasını meşrulaştırmayacağı, buna göre kişisel verilerin yalnızca belirli amaçlar için ve gerektiği kadar toplanması, amacın gerektirdiği yerlerde kullanılması ve amaç için gerekli olandan uzun süre tutulmaması gerektiği, bu doğrultuda, ilgili kişiye ait parmak izi ve yüz tarama verilerinin işlenme sebebi olarak veri sorumlusu tarafından belirtilen şirket çalışanlarının güvenliğinin sağlanması ihtiyacı ile orantısız olduğu, aynı amaca biyometrik verilerin işlenmesini gerektirmeyen manyetik kart okuyucu ve kontrol listesi gibi yöntemlerle de ulaşılabilmesi mümkün iken veri sorumlusu tarafından biyometrik veri işlenmesi yoluna gidilmesinin Kanun'un genel ilkelerinden ölçülü olma ilkesine uygun olmadığı,
- Öte yandan, ilgili kişinin veri sorumlusu şirketin yurt dışında yer alan şubesine gittiği süreçte kişisel verilerinin açık rızası olmaksızın yurt dışına aktarıldığını iddia ettiği, veri sorumlusunun ise savunma dilekçesinde ilgili kişinin herhangi bir kişisel verisinin yurt dışına aktarılmadığını belirttiği, ancak

şikâyet dilekçesinde aktarım faaliyetine ilişkin somut bilgi ve belgelere yer verilmemiş olduğu ve bu nedenle bu iddialar bakımından Kanun kapsamında yapılacak bir işlem bulunmadığı,

- Şikâyet dilekçesinde veri sorumlusunun internet sitesinde gizlilik politikasının bulunmadığının da belirtildiği, veri sorumlularının Kanun'un 10'uncu maddesi kapsamında aydınlatma yükümlülüğünü yerine getirmekle yükümlü olduğu, her ne kadar uygulamada veri sorumluları tarafından gizlilik politikası adı altında belgeler hazırlanıp ilgili kişilerin dikkatine sunuluyor olsa da Kanun'da ve Kanun ile ilgili diğer mevzuatta veri sorumluları tarafından gizlilik politikası hazırlanmasına dair bir yükümlülük yer almadığı

değerlendirmelerinden hareketle;

- İlgili kişinin iş sözleşmesine bir madde olarak eklenen aydınlatma metninin aynı zamanda açık rıza metni niteliği de taşıyan karma nitelikte bir metin olduğu, aydınlatma metninin içermesi gereken asgari unsurları içermediği ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in 5'inci maddesinin (1) numaralı fıkrasının (f) bendi gereğince aydınlatmanın açık rıza beyanından ayrı olarak yerine getirilmediği dikkate alındığında aydınlatma yükümlülüğünün Kanun'un 10'uncu maddesi ve Tebliğ'e uygun şekilde düzenlenerek sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına,

- Veri sorumlusunun biyometrik veri işlemekte hukuki sebep olarak ileri sürdüğü iş sözleşmesinde bir madde olarak yer alan açık rıza metninin, ilgili kişinin iş sözleşmesini imzalamadan işe başlamak gibi bir şansı bulunmadığından, özgür irade ile imzalanmadığı, söz konusu açık rıza metnini kabul etmeme imkanının etkin bir biçimde ilgili kişiye tanınmamış olduğu, personelin işyerine giriş çıkışlarında kullanılan biyometrik verilerle ulaşılmak istenen amaca başka vasıtalarla ulaşılabilecek olmasına rağmen açık rıza şartına dayanılarak biyometrik veri işlenmesinin Kanun'un "Genel İlkeler" başlıklı 4'üncü maddesinde yer alan amaç ile ölçülü olma ilkesine aykırı olduğu gerekçeleriyle Kanun'un 12'nci maddesinin (1) numaralı fıkrasında yer alan kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri alma yükümlülüğüne aykırı hareket ettiği kanaatine varılan veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 125.000 TL idari para cezası uygulanmasına,

- Hukuka aykırı işlendiği tespit edilen biyometrik veri işleme faaliyetine son verilmesi, öte yandan söz konusu verilerin Kanun'un 7'nci maddesi ve Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesine Dair Yönetmelik hükümlerine uygun şekilde imha edilerek sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına,

karar verilmiştir.

2021/1243 sayılı KVKK Kararı

İlgili kişinin kişisel verisi niteliğindeki e-posta adresinin bir insan kaynakları firması tarafından reklam ve pazarlama amaçlı e-posta gönderilmesi amacıyla işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 09/12/2021 tarihli ve 2021/1243 sayılı Karar Özeti

Karar Tarihi : 09/12/2021

Karar No : 2021/1243

Konu Özeti : İlgili kişinin kişisel verisi niteliğindeki e-posta adresinin bir insan kaynakları firması tarafından reklam ve pazarlama amaçlı e-posta gönderilmesi amacıyla işlenmesi

Kuruma intikal eden şikâyet dilekçesinde özetle; veri sorumlusu bir insan kaynakları firması tarafından ilgili kişiye ticari tanıtım amaçlı e-postalar iletildiği, ilgili kişinin veri sorumlusu ile daha önceden herhangi bir hukuki işleminin bulunmadığı dolayısıyla kişisel verilerinin nereden ve nasıl temin edildiği hakkında bir bilgiye sahip olmadığı, kişisel verilerinin bu çerçevede işlenmesi yönünde açık rızasının bulunmadığı, veri sorumlusuna bu hususta başvuruda bulunduğu ve kişisel verilerinin silinmesini talep ettiği, ancak kişisel verilerinin nereden temin edildiği ve ne amaçla işlendiği hususlarında tarafına bir bilgi verilmediği ifade edilerek, veri sorumlusu hakkında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabî yazıda özetle;

- Veri sorumlusunun her nevi konferans, anket, tanıtım, reklam, konser organizasyonları düzenlemek ve bu işler için eleman sağlamak, bu organizasyonlar için ara teknik donanım kiralamak, bu işleri başkalarına yaptırmak, benzin istasyonu işletmesi ve çalışan temini, AVM işletmelerine çalışan temin etmek, hastane vb. sağlık kurumlarına çalışan temin etmek, inşaat vb. işletmelere çalışan temin etmek, lojistik sektörüne çalışan temin etmek, gemi işletmelerine çalışan temini hizmetleri vermek ve diğer her türlü sektörde ihtiyaç duyulan elemanları temin etmek, reklam, gösteri, kongre, konferans, ticari fuar, anket çalışmaları, pazarlama faaliyetlerine eleman tedarik etmek ve benzeri nitelikteki etkinliklerin organizasyon faaliyetlerini yürüttüğü,

- İlgili kişiye ait e-posta adresinin veri sorumlusunca yürütülen ekonomik faaliyetler (anket ve tanıtım işleri) kapsamında edinildiği,
- Söz konusu e-posta adresinin 6698 sayılı Kişisel Verilerin Korunması Kanunun'un (Kanun) 5'inci maddesinin (d) bendi kapsamında "İlgili kişinin kendisi tarafından alenileştirilmiş olması" şartına dayanarak işlendiği,
- Kişisel verilerin işlenmesinde Kanun kapsamında hareket edildiği, ilgili kişiye ilişkin hiçbir bilgi ve belge paylaşımının yapılmadığı

ifade edilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 09/12/2021 tarih ve 2021/1243 sayılı kararı ile;

- Kanun'un "Kişisel verilerin işleme şartları" başlıklı 5'inci maddesinde;

"(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması."

hükmüne yer verildiği,

- Veri sorumlusu tarafından ilgili kişiye ait e-posta adres bilgisinin ekonomik faaliyetleri çerçevesinde anket ve tanıtım işleri kapsamında edinildiği ve Kanun'un 5'inci maddesinin (d) bendi çerçevesinde "İlgili kişinin kendisi tarafından alenileştirilmiş olması" şartı kapsamında işlendiğinin ifade edildiği, ancak ilgili kişinin hangi yöntemle ve hangi platformda veya mecraada e-posta adres

bilgisini alenileştirme iradesinde bulunduğuna ilişkin veri sorumlusu tarafından herhangi bir açıklamaya, anket ve tanıtım işleri çerçevesinden nasıl elde edildiğine ilişkin olarak kanıtlayıcı nitelikte herhangi bir belgeye yazı ekinde yer verilmediği,

- Bu anlamda veri sorumlusunun ilgili kişinin kişisel verilerinin nasıl elde edildiği ve hangi işleme şartı kapsamında işlendiğine ilişkin açıklamalarının hukuki dayanaktan yoksun olduğu, dolayısıyla veri sorumlusunun Kanun'un 5'inci maddesi çerçevesinde herhangi bir hukuki işleme şartı bulunmaksızın veri işleme faaliyetinde bulunduğu,

- Diğer taraftan Kanun'n "Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi" başlıklı 7'nci maddesine göre kişisel verilerin Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silineceği, yok edileceği veya anonim hale getirileceğinin hüküm altına alındığı, bununla birlikte ilgili kişinin hakları hususunda düzenleme getiren Kanun'un 11'inci maddesinde de ilgili kişinin veri sorumlusuna başvurarak kendisiyle ilgili "7'nci maddede öngörülen şartlar çerçevesinde kişisel verilerinin silinmesini veya yok edilmesini isteme" hakkının düzenlendiği,

- Kanun'un 7'nci maddesinin (3) numaralı fıkrasına dayanılarak hazırlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 7'nci maddesinin "Kanunun 5 inci ve 6'ncı maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin veri sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hale getirilmesi gerekir." ve aynı maddenin (2) numaralı fıkrasının "Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Kanunun 4'üncü maddesindeki genel ilkeler ile 12'nci maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve kişisel veri saklama ve imha politikasına uygun hareket edilmesi zorunludur." hükmünü haiz olduğu,

- Bu kapsamda ilgili kişinin e-posta bilgisinin Kanun'a aykırı olarak işlendiği ve ilgili kişinin veri sorumlusuna başvurusunda, kişisel verilerinin silinmesi talebini de iletmiş olduğunu anlaşıldığı

değerlendirmelerinden hareketle;

- Veri sorumlusu tarafından ilgili kişinin kişisel verisi niteliğindeki e-posta adresinin ilgili kişiye ticari amaçlı bir e-posta gönderilmesi suretiyle işlendiği ancak Kanun'un 5'inci maddesinde yer alan işleme şartlarından herhangi birinin söz konusu olmadığı dolayısıyla, veri sorumlusu tarafından Kanun'un 12'nci maddesinin (1) numaralı fıkrası çerçevesinde "kişisel verilerin hukuka aykırı olarak işlenmesini

önlemek" yükümlülüğüne aykırı davranıldığı anlaşıldığından veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrası uyarınca 50.000 TL idari para cezası uygulanmasına,

- İlgili kişinin e-posta adresi bilgisinin Kanun'a aykırı olarak işlendiği ve ilgili kişinin veri sorumlusuna başvurusunda kişisel verilerinin silinmesi talebini de ilettiği anlaşıldığından veri sorumlusunun, ilgili kişinin kişisel verilerini imha ederek imha işlemine ilişkin log kayıtlarının da Kurum'a iletilmesi suretiyle Kurul'a bilgi vermesi yönünde talimatlandırılmasına

karar verilmiştir.

2021/1239 sayılı KVKK Kararı

Veri sorumlusu Banka tarafından ilgili kişinin ailesinin telefonları üzerinden arama gerçekleştirilmesi suretiyle kişisel verilerinin paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 09/12/2021 tarihli ve 2021/1239 sayılı Karar Özeti

Karar Tarihi : 09/12/2021

Karar No : 2021/1239

Konu Özeti : Veri sorumlusu Banka tarafından ilgili kişinin ailesinin telefonları üzerinden arama gerçekleştirilmesi suretiyle kişisel verilerinin paylaşılması

Kuruma intikal eden şikâyette özetle;

- Banka olarak faaliyet gösteren veri sorumlusu ile ilgili kişi arasında kredi sözleşmesi akdedildiği, sözleşmeye konu borca ilişkin olarak ilgili kişinin açık yazılı veya sözlü onayı olmamasına rağmen anne ve babasının sabit telefonları üzerinden ısrarla arandığı, aramaya gerekçe olarak şikayetçiye ulaşılamamasının gösterildiği,
- Veri sorumlusu tarafından yapılan aramalarda ilgili kişinin ailesine, ilgili kişiye ve ilgili kişinin de ortağı olduğu Şirketin ortaklarına ulaşılamadığının beyan edildiği, ayrıca ortaklarının isimlerinin verildiği, görüşmelerin sonunda bir telefon numarası bırakıldığı ve ilgili kişinin bu numarayı araması gerektiğinin söylendiği, ilgili kişinin aranan numaranın ailesinin kullanımında olduğunu müteaddit kez belirttiği, yapılan aramalar sonucu zor duruma düşüldüğü, ilgili kişiye ait kişisel verilerin açık rızası olmaksızın veri sorumlusu tarafından kullanılması suretiyle ihlal edilmiş olduğu,
- Bu ihlal dolayısı ile 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 14 üncü maddesinin (2) numaralı fıkrası gereğince veri sorumlusuna başvuru yapıldığı, Banka tarafından vekaletnamede Kanun kapsamında talepte bulunma yetkisinin olmadığı gerekçesiyle vekile bilgi verilmeyeceği, cevapların şikayetçi müvekkile tebliğ edileceğinin beyan edildiği, sonrasında cevabın hazır olduğu 10 gün içerisinde tebliğ edileceğinin şikayetçiye bildirildiği ancak herhangi bir tebligat yapılmadığı, bunun üzerine tekrar Kanun kapsamında talepte bulunmaya ilişkin yetki içerir vekaletname ile yeni bir başvuru yapıldığı, bu başvurunun da reddedildiğinin öğrenilmesi üzerine Kuruma başvuru zorunluluğunun hasıl olduğu

belirtilerek, veri sorumlusu hakkında gereğinin yapılması talep edilmiştir.

İlgili kişinin şikâyetine istinaden başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, verilen cevapta özetle;

- İlgili kişinin Banka nezdinde bireysel müşteri kaydı bulunduğu, bunun yanı sıra ilgili kişinin hakim ortağı olduğu (...) Anonim Şirketi'nin de Bankada ticari müşteri kaydının yer aldığı, (...) Anonim Şirketi için kredi teklifi yapılabilmesi amacıyla şirkete ticari müşteri kaydı oluşturulurken alınan kredi başvuru formunda, anılan şirketin hakim ortağı ve aynı zamanda yönetim kurulu başkanı olması nedeniyle ilgili kişiye ait bazı bilgilerin de alındığı, kredi başvuru süreçleri aşamasında şirkete limit çalışması ve ticari kart başvurusu yapılması kapsamında ilgili kişinin de hakim ortak olarak Risk Merkezi bilgisinin sorgulandığı, Risk Merkezi'nden alınan ev telefonu numarasının Banka veri tabanına kaydedildiği, ilgili kişinin bireysel müşteri kayıtlarının içerisinde e-posta adresinin yer almaması nedeni ile cevabî yazının "resmi adres ve ev adresi" olarak kayıtlı olan adresine PTT aracılığıyla iadeli taahhütlü posta olarak gönderildiği,

- 5411 sayılı Bankacılık Kanunu (5411 sayılı Kanun) ile alt düzenlemelerin belirlediği kapsamla sınırlı olacak şekilde ve yine bu düzenlemelerde yer verilen esas ve usullere uygun olarak, Banka müşterilerinin kredilendirme süreçlerinde kullanılmak üzere risk bilgilerini alabilmek amaçları ile Türkiye Bankalar Birliği Risk Merkezi'nden (Risk Merkezi) sorgulamalar yapılmakta olduğu, yapılan aramalarda müşteriye ulaşılamaması durumunda müşterilere ulaşabilmek amacıyla Risk Merkezi sorgulamasından elde edilen ve sistemlere "alternatif numara" olarak kaydedilmiş olan iletişim numaralarının da aranabildiği, bununla birlikte söz konusu alternatif numaraların aranması ve bu aramalara müşteri dışında üçüncü kişilerin yanıt vermesi durumunda üçüncü kişilerle hiçbir şekilde bilgi paylaşımı yapılmayıp, kendisine ulaşmak istenilen müşterilerin Bankayı geri araması hususunda not bırakıldığı,

- İlgili kişinin hakim ortağı ve yönetim kurulu başkanı olduğu (...) Anonim Şirketi'nin Banka nezdinde kullandığı kredilerde gecikme oluşması nedeniyle, bu müşteri için yapılan aramaların başlamış olduğu, ilgili kişinin Banka sisteminde kayıtlı olan cep telefonu üzerinden muhtelif tarihlerde defalarca yapılan aramalara rağmen kendisi ile temas kurulamadığı, kendisinin Risk Merkezi nezdinde ev telefonu numarası olarak kayıtlı olan telefon numarasından çeşitli tarihlerde arama yapılarak görüşme sağlandığı, bu tarihlerde yapılan hiçbir aramada ilgili kişiye ya da kendisinin hakim ortağı ve yönetim kurulu başkanı olduğu şirkete ilişkin olarak üçüncü kişilere herhangi bir bilgi paylaşımı yapılmadığı, bu aramalarda ilgili kişiye iletilmesi için üçüncü kişilere

sadece not bırakıldığı, ilgili kişinin yakınının bırakılan notu kendisine iletceğini ifade ettiği ve Banka tarafından bu hususla ilgili olarak aranmak istemediklerine ilişkin bir talep iletmedikleri,

- İlgili kişinin Bankayı araması ile yapılan görüşmede, aranan numarayı Bankaya vermediği ve ailesinin nasıl arandığını sorması üzerine, müşteri temsilcisi tarafından kendisine ulaşım sağlanamadığı zaman sistem tarafından otomatik olarak alternatif numaradan arama yapıldığı, Banka şubelerinden konuya ilişkin bilgi alınabileceği ve bununla ilgili olarak aranmak istemediği numaraları Banka kayıtlarından sildirebileceğinin belirtildiği, ilgili kişinin talebi üzerine kendisi ile görüşmeyi gerçekleştirmiş olan müşteri temsilcisinin söz konusu telefon numarasını, sistem üzerinde bu numaranın bir daha aranmamasını sağlayıcı aksiyon olarak “yanlış numara” şeklinde belirtmesi gerektiği halde, bu şekilde işlem yapmaması nedeni ile şikâyet konusu telefon numarasına yapılan aramaların devam ettiği, ilgili personelin konu hakkında uyarıldığı, sonraki bir tarihte ilgili kişinin yakınının bu telefon numarasından aranmak istemediğini belirtmesi üzerine telefon numarasının arama engelli listesine eklendiği,

- Şikâyete konu alternatif telefon bilgisinin, Risk Merkezi’nden yapılan sorgulama vasıtasıyla temin edilerek, ilgili kişiye ulaşılmak maksadı ile ve sadece bu amaçla sınırlı kalınarak kullanıldığı

belirtilmiş ve risk merkezi üzerinden yapılan sorgulama sonuçlarında şikâyete konu telefon numarasının “ev telefon numarası” olarak görünen şekilde Banka sistemine yansımaya ilişkin ekran görüntüsü paylaşılmıştır.

Konuya ilişkin yapılan incelemede Kişisel Verileri Koruma Kurulunun 09/12/2021 tarihli ve 2021/1239 sayılı Kararı ile;

- 6698 sayılı Kanun’un “Tanımlar” başlıklı 3’üncü maddesinde kişisel verinin: “Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi”, ilgili kişinin; “Kişisel verisi işlenen gerçek kişi”, kişisel verilerin işlenmesinin; “Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem”, veri sorumlusunun; “Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi” olarak tanımlandığı,

- Öte yandan, 6698 sayılı Kanun’un “Kişisel Verilerin İşlenme Şartları” başlıklı 5’inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı

fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğunun hükme bağlandığı,

- Öte yandan, 6111 sayılı Kanun ile, 5411 sayılı Bankacılık Kanunu'na ek 1 inci madde ve geçici 28 inci maddenin ilave edildiği, ek 1 inci madde ile Türkiye Bankalar Birliği nezdinde, kredi kuruluşları ile Bankacılık Düzenleme ve Denetleme Kurulunca uygun görülecek finansal kuruluşların müşterilerinin risk bilgilerini toplamak ve söz konusu bilgileri bu kuruluşlar ile gerçek veya tüzel kişilerin kendileriyle ya da onay vermeleri koşuluyla özel hukuk tüzel kişileri ve üçüncü gerçek kişileri ile de paylaşılmasını sağlamak üzere Risk Merkezi kurulduğu, Risk Merkezi Yönetmeliği'nin "Risk Merkezi üyelerinin sorumlulukları" başlıklı 17 nci maddesinin birinci fıkrasının (b) ve (c) bentleri kapsamında üyelerin, Risk Merkezi ile gizlilik sözleşmesi yapmak ve Risk Merkezinden temin ettiği her türlü bilgi ve belgenin gizliliğinin sağlanmasına yönelik her türlü önlemi almak ve Risk Merkezinden temin ettiği bilgileri yalnızca kendi iç işlemlerinde kullanmak, diğer üyeler dahil herhangi bir gerçek ve tüzel kişi ile paylaşmamakla sorumlu tutulduğu, ayrıca, "Gizlilik" başlıklı 19 uncu madde uyarınca; "(1) Risk Merkezinin tüm işlem ve kayıtları gizlidir. Risk Merkezinden temin edilen bilgiler yalnızca bilgiyi alan üyenin kendi iç işlemlerinde kullanılabilir, diğer üyeler dahil herhangi bir gerçek ve tüzel kişi ile paylaşamaz. (2) Risk Merkezi nezdinde bulunan sır niteliğindeki bilgileri, bu konuda kanunen yetkili kılınan mercilerden başkalarına açıklayanlar, hukuka aykırı olarak kendisi ya da başkası yararına kullananlar, yayanlar, verenler, aktaranlar veya ele geçirenler hakkında Kanunun 159 uncu maddesi hükümleri uygulanır" hükmünün düzenlendiği, bu doğrultuda, Risk Merkezinde bulunan sır nitelikli bilgilerin kanunen yetkili kılınan mercilerden başkalarına açıklanması durumunda 5411 sayılı Kanun'un 159'uncu maddesinde öngörülen yaptırımların uygulanacağını belirtildiği,

- Öte yandan, "Türkiye Bankalar Birliği Risk Merkezi Üyelerinin Müşterilerinin Risk Merkezi Nezdindeki Bilgilerinin Kendilerine ya da Onay Vermeleri Koşuluyla Belirledikleri Gerçek veya

Tüzel Kişilere Verilmesine İlişkin Esas ve Usuller Hakkında Yönetmelik” kapsamında, TBB Risk Merkezi üyelerinin müşterilerinin TBB Risk Merkezi nezdindeki bilgilerinin, kendilerine ya da onay vermeleri koşuluyla belirledikleri gerçek veya tüzel kişilere verilmesini teminen başvuru ve onay verme sürecine ilişkin esas ve usullerin düzenlendiği, Risk Merkezi’ndeki bilgilerin ne şekilde sorgulanabileceği ve temin edilebileceği hususlarının da ayrı bir yönetmelik kapsamında düzenlendiği,

- İlgili kişinin hakim ortak olduğu (...) Anonim Şirketi ile veri sorumlusu arasında kredi sözleşmesi olduğu, veri sorumlusu Banka ile kredi başvuru süreci yürütülürken ilgili kişinin bazı kişisel verilerinin işlendiği, anılan sözleşmeden kaynaklanan bir borcun/riskin oluştuğu, oluşan risk üzerine ilgili kişiye cep telefonu numarasından ulaşılamadığı ve Risk Merkezi’nden yapılan sorgulama neticesinde alternatif numara olan Risk Merkezi sisteminde aynı zamanda “ev telefon numarası” şeklinde kayıtlı olan numaradan aramalar yapıldığı, bu aramaların ilgili mevzuat ve Kurulun “Risk Merkezinden temin edilen telefon numarası üzerinden yapılan arama ile müşterinin Banka ile münasebetinin yakınları ile paylaşılmasına ilişkin” 05.03.2021 tarihli yazısı doğrultusunda gerçekleştirildiği, ilgili kişinin anne-babasının kullandığı belirtilen telefon numarasına çeşitli tarihlerde veri sorumlusunca yetkilendirilmiş kişilerce arama yapıldığı,

- İlgili kişinin talebi üzerine yanlış numara aksiyonu alınması gerekirken, aramaların devam ettiği ve ilgili personelin bu konuda uyarıldığı tarihte “yanlış numara aksiyonu” alındığı, bu durumun Kuruma sunulan evraklardan da anlaşıldığı, ilgili kişinin başvurusuna binaen cevabî nitelikli yazı gönderildiği, yazıda kısaca ilgili mevzuattan bahsedilip bahis konusu telefon numarası ile ilgili gerekli aksiyonun alındığını da kapsayan özür ifadesinin yer aldığı, veri sorumlusu tarafından Kuruma gönderilen ve şikayete konu telefon numarası ile yapılan görüşmeleri kapsayan dökümlerde, ilgili kişinin borç bilgilerine ilişkin bilgi verilmediği, veri sorumlusu adına bilgi aktarımında bulunulacağı ifade edildiği ve (...) Anonim Şirketinin ortaklarının isimlerinin verildiği,

- Veri sorumlusunun ilgili kişinin verilerini kendisinin hâkim ortak olduğu şirket, 5411 sayılı Kanun ve ilgili diğer mevzuat hükümleri çerçevesinde “Risk Grubu” içerisinde yer aldığı için işlediği, bu işlemin bankacılık faaliyetleri kapsamında, Banka bünyesinde kullanılmak ve Risk Merkezine aktarılmak amacıyla yapıldığı ve Kanun’un 5’inci maddesinin (2) numaralı fıkrasının (ç) bendi uyarınca “veri sorumlusunun hukuki yükümlülüklerinin yerine getirilmesi kapsamında” olduğu, şikayete konu telefon numarasına yapılan aramalar hakkında ilgili kişi tarafından, numaranın kendisine ait olmadığı, anne-babası tarafından kullanıldığı bildirimini yapıldığı, ilgili personelce

gerekli işlemlerin yapılması için bilgi verilmediğinden, sonraki bir tarihte “yanlış numara aksiyonu” alınabildiği, veri sorumlusu tarafından ilgili personelin uyarıldığı,

değerlendirmelerinden hareketle;

- Veri sorumlusu tarafından, oluşan riskten dolayı yapılan borçlu takibinin Risk Merkezi sisteminde kayıtlı telefon numarasına yönelik yapıldığı, eldeki mevcut bilgi ve belgelerden veri sorumlusu tarafından kişisel veri paylaşıldığına yönelik bir tespitte bulunulamadığı ve ilgili kişinin talebi üzerine aramalara ilişkin kısa sürede gerekli aksiyonun alındığı dikkate alındığında veri sorumlusu hakkında Kanun kapsamında yapılacak bir işlem olmadığına,

- Telefon aramalarında kişisel verilerin korunması yönünden daha dikkatli olunması ve personelin bu konuda bilgilendirilmesi hususunun veri sorumlusuna hatırlatılmasına

karar verilmiştir.

2021/1218 sayılı KVKK Kararı

İlgili kişi işçinin hakkında yürütülen kişisel verilerin işlenmesi faaliyetleri kapsamında yurtdışında mukim olan veri sorumlusu işverence aydınlatılmaması, ilgili kişiye ait kişisel verilerin Nisan 2021 sonrası dönemde veri sorumlusu tarafından hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 02/12/2021 tarihli ve 2021/1218 sayılı Karar Özeti

Karar Tarihi : 02/12/2021

Karar No : 2021/1218

Konu Özeti : İlgili kişi işçinin hakkında yürütülen kişisel verilerin işlenmesi faaliyetleri kapsamında yurtdışında mukim olan veri sorumlusu işverence aydınlatılmaması ve ilgili kişiye ait kişisel verilerin Nisan 2021 sonrası dönemde veri sorumlusu tarafından hukuka aykırı olarak işlenmesi

İlgili kişinin şikâyetinde özetle;

- Ekim 2020 ila Nisan 2021 tarihleri arasında yurtdışında mukim olan veri sorumlusunun İstanbul İrtibat Bürosu'nda görev yaptığı ve iş sözleşmesinin eylemli fesih yoluyla sona erdirildiği,
- Veri sorumlusunun İstanbul İrtibat Bürosu'nun, "iş sözleşmesinin devamı" ve "iş sözleşmesinin eylemli fesih yoluyla sona erdirilmesi" olmak üzere iki farklı dönemde, ilgili kişiye karşı 6698 sayılı Kişisel Verilerin Korunması Kanunu'ndan (Kanun) kaynaklanan yükümlülüklerini yerine getirmediği,
- İlgili kişi tarafından Kanun'un 13'üncü maddesine dayanılarak hazırlanan ve e-posta üzerinden veri sorumlusunun İstanbul İrtibat Bürosu'na yöneltilen 26/05/2021 tarihli İhtarname'ye cevaben iletilen 07/06/2021 tarihli e-postada açık ve doğru bilgi verilmediği,
- İlgili kişiye verilen cevapta "Halen istihdam altında bulunduğunuzdan, çalışanın iş ilişkisinin karşılıklı ifası için gerekli kişisel verilerin işlenmesi KVKK m. 5/2 kapsamında '...c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.' şeklindeki madde kapsamına girdiğinden, ayrıca aynı maddenin (e) ve (f) bentleri gereğince, iş akdinizin ifası çerçevesinde gerekli kişisel verileriniz KVKK'ya uygun şekilde işlenmektedir. Dolayısıyla, ilgili yasal mevzuata uygun olarak ücretsiz izne

çıkarıldığından ve halen çalışan statüsünde olduğunuzdan, Kişisel Verilerin Korunması Kanunu kapsamında hiçbir hukuka aykırılık da söz konusu olmadığından talebiniz kabul edilememektedir.” ifadelerine yer verildiği,

- İlgili kişiye iletilen metnin geçerli bir cevap olmadığı, zira ilgili kişi tarafından yöneltilen soruların geçirildiği, kaldı ki istihdam ilişkisinin devamının işverenin Kanun’dan kaynaklanan yükümlülüklerini yerine getirdiğine karine teşkil etmeyeceği ve çalışanın işverene karşı Kanun’dan doğan haklarını kullanmasının istihdam ilişkisinin sona ermesine bağlı olmadığı,
- İşverenlerin Kanun kapsamında çalışanların özlük dosyalarının düzenlenmesi bakımından “veri sorumlusu” sıfatını haiz oldukları, bu sıfatla da Kanun’un 10’uncu maddesi uyarınca “veri sorumlusunun ve varsa temsilcisinin kimliği”, “çalışanın kişisel verilerin hangi amaçla işleneceği”, “işlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı”, “kişisel veri toplamanın yöntemi ve hukuki sebebi” ve “ilgili kişi çalışanın bu kapsamdaki hakları” hakkında yazılı bir aydınlatma metni düzenlemek ve çalışanı bilgilendirmekle yükümlü oldukları,
- İlgili kişinin istihdam edildiği süreçte kişisel verilerinin işlenmesi faaliyetinin amacı, kapsamı, verilerinin kimlerle paylaşıldığı, nasıl ve hangi süre için saklandığı, hangi hukuki sebeplerle işlendiği, Kanun kapsamında veri sorumlusuna yöneltebileceği haklarının neler olduğu konularında bilgilendirilmediği,
- Veri sorumlusunun İstanbul İrtibat Bürosu’nun ilgili kişinin kişisel verilerinin hangi üçüncü kişilere aktarıldığı ve ilgili kişinin kişisel verilerinin yurtdışına aktarılıp aktarılmadığı konularında da ilgili kişiyi bilgilendirmediği, kişisel verileri yurt dışına aktarıyor ise bu hususta ilgili kişinin açık rızasının alınmadığı,
- İlgili kişinin özel nitelikli kişisel verilerinin işlenip işlenmediğinin de veri sorumlusunun İstanbul İrtibat Bürosu tarafından ilgili kişiye bildirilmediği, eğer özel nitelikli kişisel verileri işleniyor ise bu hususta ilgili kişinin açık rızasının alınmadığı,
- Veri sorumlusunun İstanbul İrtibat Bürosu’nun ilgili kişinin kişisel verilerinin işlenmesinde; “Kişisel Verileri Koruma Kurulu (Kurul) tarafından belirlenen yeterli ve gerekli önlemleri gözetip gözetmediği”, “hangi tedbirleri aldığı”, “kişisel verilerini hangi ortamda muhafaza ettiği ve sakladığı”, “uygun güvenlik düzeyini temin edip etmediği”, “herhangi bir teknik veya idari tedbir alıp almadığı” ve “Kanun ve ilgili mevzuatta belirtilen yasal sürelerle uygun olarak kişisel verilerini imha edip etmediği” hususlarında ilgili kişiyi bilgilendirmediği, ayrıca ilgili kişinin taleplerine ve

sorularına cevap vermeyerek Kanun'un 11'inci maddesi kapsamındaki her türlü bilgi alma hakkını ihlal ettiği,

- İlgili kişinin iş akdinin eylemli fesih yoluyla sona erdirilmesinden sonraki dönemde "hiçbir koşul altında iş yapmaması", "işyerine gitmemesi" ve "irtibat bürosunda faal olarak görev yapmaması" konularında yazılı olarak bilgilendirildiği, ancak ilgili kişinin fotoğrafının ve sair kişisel verilerinin iş akdinin feshinden sonraki dönemde de veri sorumlusunun kurumsal internet sitesinden kaldırılmadığı,

- Bahsi geçen internet sitesi yurtdışında bulunduğundan ilgili kişinin fotoğrafının ve sair kişisel verilerinin bu sitede tutulmasının ilgili kişinin açık rızasına bağlı olduğu ama ilgili kişinin bu yönde bir rızayı hiçbir zaman vermediği

hususları bildirilmiş olup, veri sorumlusunun İstanbul İrtibat Bürosu'nun ilgili kişinin taleplerini yerine getirerek belirtilen hususlarda açıklama yapmasının ve hukuka aykırılıkların giderilmesinin sağlanması ile veri sorumlusunun İstanbul İrtibat Bürosu'nun Kanun'un amir hükümlerine istinaden cezalandırılması talep edilmiştir.

Bu kapsamda, her ne kadar ilgili kişi tarafından veri sorumlusunun İstanbul İrtibat Bürosu hakkında şikâyette bulunmuş olsa da yabancı şirketlerin Türkiye'deki irtibat bürolarının tüzel kişiliklerinin bulunmadığı ve Kanun'un "Kapsam" başlıklı 2'nci maddesi uyarınca Kanun hükümlerinin sadece gerçek kişiler ile tüzel kişiler hakkında uygulanabileceği dikkate alınmış ve ilgili kişinin iddialarına istinaden yurtdışında mukim veri sorumlusu hakkında inceleme başlatılmasına karar verilmiştir. Akabinde, başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, verilen cevapta özetle;

- İlgili kişinin Londra'da mukim olan veri sorumlusu bünyesinde çalışmaya başladığı ve 01/10/2020 tarihinde veri sorumlusunun İstanbul'da açılan irtibat ofisinde görevlendirildiği,

- Kurulun "yurtdışında yerleşik tüzel kişilerin Türkiye'deki şubeleri ile irtibat bürolarının sicile kayıt yükümlülüğü hakkındaki görüş talebi" hakkında verdiği 23/07/2019 tarihli ve 2019/225 sayılı karar ile yasal mevzuat göz önünde bulundurulduğunda, yurtdışında yerleşik tüzel kişilerin Türkiye'deki irtibat bürolarının veri sorumlusuna ait yükümlülüklerinin bulunmadığının ve veri sorumlusu olarak gerekli yükümlülüklerin yurtdışında yerleşik tüzel kişilik tarafından yerine getirilmesi gerektiğinin ortada olduğu,

- Bu doğrultuda, veri sorumlusu tarafından ilgili kişiye veri sorumlusunun "Veri Koruma Politikası" çerçevesinde bilgilendirilmedi bulunulduğu, "İşçiler ve Taşeronlar için GDPR Gizlilik Bildirgesi"

imzalatıldığı ve GDPR ile uygulanabilir tüm yasal mevzuat kapsamında gerekli her türlü yükümlülüğün yerine getirildiği,

- İlgili kişinin veri sorumlusu ile olan iş ilişkisinin devamı esnasında tüm dünyayı etkisi altına alan COVID-19 virüsünün ortaya çıktığı pandemi döneminde Türkiye Cumhuriyeti'nin yasal mevzuatının uygun gördüğü şekilde ücretsiz izne çıkarıldığı, bu yüzden ilgili kişinin iddia ettiğinin aksine ilgili kişi ile veri sorumlusu arasındaki sözleşmenin eylemli fesih yoluyla sona erdirilmediği, buna dair hiçbir geçerli ve hukuki delilin de bulunmadığı,

- İlgili kişinin iş sözleşmesinin 01/07/2021 tarihinde kendisine gönderilen Fesih Bildirimi ile sona erdirildiği, ilgili kişinin avukatı tarafından veri sorumlusuna gönderilen 01/07/2021 tarihli e-postada da iş ilişkisinin daha önceki bir tarihte sonlandırılmamış olduğunun ikrar edildiği,

- İlgili kişinin veri sorumlusu ile aralarındaki iş sözleşmesinin eylemli fesih yoluyla sona erdirildiğini iddia etmesine rağmen 01/07/2021 tarihli Fesih Bildirimi'ni beklediği ve Fesih Bildirimi'nin kendisine tebliğinden hemen sonra başka bir firmanın internet sitesine fotoğrafının koyulduğu, bunun da ilgili kişinin veri sorumlusu ile arasındaki sözleşmenin eylemli fesih yoluyla sona erdirilmediğinin farkında olduğunu gösterdiği,

- İlgili kişinin fesih eyleminin bir an önce gerçekleşmesi konusundaki ısrarının diğer firmanın internet sitesinde yer almak için sabırsızlanmasından kaynaklandığı, ilgili kişinin haksız ve hukuka aykırı taleplerinin veri sorumlusunca kabul edilmemesinden dolayı öç alma güdüsüyle inceleme konusu şikâyeti yaptığı,

- Kanun'un 5'inci maddesinin (2) numaralı fıkrasında sayılan şartlardan birinin varlığı halinde ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu,

- Bu çerçevede, veri sorumlusu ile ilgili kişi arasındaki iş ilişkisinin devamı sırasında ilgili kişiye ait kişisel verilerin işlenmesinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (c) bendindeki "Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması" düzenlemesinin kapsamına girdiği, ayrıca iş sözleşmesinin ifasına ilişkin kişisel verilerin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (e) ve (f) bentleri gereğince hukuka uygun olarak işlendiği,

- İlgili kişinin iş sözleşmesinin sona erdirilmesinin akabinde, ilgili kişinin özlük dosyasında bulunan bilgilerin gelecekte veri sorumlusu aleyhine açılma ihtimali olan davalarda ispat kolaylığı sağlayacağından ötürü meşru menfaat çerçevesinde saklanmakta olduğu ve bu bilgilerin hiçbir

üçüncü şahısla paylaşılmadığı, bunun dışında iş sözleşmesinin sona erdirilmesi ile ilgili kişiye ait diğer kişisel bilgilerin veri sorumlusu tarafından silindiği ve yok edildiği,

- Netice olarak, veri sorumlusunun İngiltere sınırları içerisinde tabi olduğu GDPR ve uygulanabilir yasal mevzuat uyarınca ilgili kişinin kişisel verilerinin hukuka uygun işlendiği, ilgili kişi ile veri sorumlusu arasındaki iş ilişkisinin sona ermesinin ardından ilgili kişinin kişisel verilerinin mümkün olduğunca yok edildiği ve silindiği, ilgili kişinin şikâyet ettiği hususların haksız ve mesnetsiz olduğu, veri sorumlusunun tüm yükümlülüklerini yerine getirdiği ifade edilmiştir.

İlgili kişinin şikâyetinde yer alan iddialar ile veri sorumlusunun savunması birlikte incelenmiş olup, görülen lüzum üzerine “ilgili kişi ile veri sorumlusu arasındaki iş ilişkisinin başladığı yer ve tarihi”, “veri sorumlusunun İstanbul İrtibat Bürosu’nda çalıştığı zaman diliminde ilgili kişinin hangi kişisel verilerinin işlendiği ve bu işleme faaliyetinin amacı/amaçları ve hukuki sebebi/sebepleri”, “veri sorumlusunun İstanbul İrtibat Bürosu’nda çalıştığı zaman diliminde ilgili kişiye yönelik yürütülen kişisel veri işleme faaliyetleri kapsamında, ilgili kişiye Kanun’un 10’uncu maddesi gereğince aydınlatma yapılıp yapılmadığı”, “ilgili kişinin veri sorumlusunun İstanbul İrtibat Bürosu’nda çalıştığı zaman diliminde işlenen kişisel verilerinin yurtiçinde veya yurtdışında üçüncü bir kişiye aktarılıp aktarılmadığı ve eğer aktarılmışsa aktarımın hukuki sebebi/sebepleri”, “ilgili kişinin kişisel verilerinin veri sorumlusuna ait kurumsal internet sitesinde yayınlanıp yayınlanmadığı ve eğer yayınlandıysa hangi kişisel verilerin hangi tarihler arasında, hangi hukuki sebebe/sebeplere dayanılarak yayınlandığı” hususlarının açıklığa kavuşturulması veri sorumlusundan istenmiştir.

Açıklığa kavuşturulması istenen hususlara dair veri sorumlusunca iletilen yazıda ise özetle;

- Veri sorumlusunun İstanbul İrtibat Bürosu’nda çalıştığı zaman diliminde, ilgili kişinin adının, soyadının, telefon numarasının, e-posta adresinin, adresinin ve özlük dosyasında bulunan bilgilerin Türkiye’de faaliyet gösteren binlerce işverenin milyonlarca çalışanına yaptığı gibi işlendiği, bu kişisel verilerin işlenme amacının veri sorumlusunun ilgili kişi ile olan istihdam ilişkisinin yürütülmesini sağlamak ve veri sorumlusunun işveren olarak yükümlülüklerini yerine getirmekten ibaret olduğu,
- Veri sorumlusu ile ilgili kişi arasındaki iş ilişkisinin devamı sırasında, ilgili kişiye ait kişisel verilerin işlenmesinin Kanun’un 5’inci maddesinin (2) numaralı fıkrasının (c) bendindeki “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” düzenlemesinin kapsamına girdiği, ayrıca Kanun’un 5’inci

maddesinin (2) numaralı fıkrasının (e) ve (f) bentleri gereğince iş sözleşmesinin ifası çerçevesinde gerekli kişisel verilerin Kanun'a uygun olarak işlendiği,

- İlgili kişinin İstanbul İrtibat Bürosu'nda çalıştığı zaman diliminde işlenen kişisel verilerinin veri sorumlusu haricinde yurtiçinde veya yurtdışında üçüncü bir kişiye aktarılmadığı,
- İlgili kişinin adının, soyadının ve fotoğrafının veri sorumlusuna ait İngiltere'de bulunan merkez ofisin yönetimindeki kurumsal internet sitesinde iş ilişkisinin devamı süresince yayınlandığı, veri sorumlusunun İstanbul İrtibat Bürosu tarafından kullanılan herhangi bir internet sitesinin bulunmadığı, söz konusu bilgilerin iş akdinin feshi itibarıyla derhal internet sitesinden kaldırıldığı ve veri sorumlusu bünyesinden silindiği, ilgili kişiye veri sorumlusu tarafından imzalatılan onay formunun ekte sunulduğu

beyan edilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde, Kurulun 02/12/2021 tarihli ve 2021/1218 sayılı kararı ile;

- 6698 sayılı Kanun'un "Tanımlar" başlıklı 3'üncü maddesinde kişisel verinin: "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", ilgili kişinin; "Kişisel verisi işlenen gerçek kişi", kişisel verilerin işlenmesinin; "Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", veri sorumlusunun; "Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi" olarak tanımlandığı,
- Öte yandan, 6698 sayılı Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işleniminin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar

vermemek kaydıyla veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğunun hükme bağlandığı,

- Ayrıca, 6698 sayılı Kanun'un kişisel verilerin işlenmesine ilişkin "Genel ilkeler"i düzenleyen 4'üncü maddesinin (1) numaralı fıkrasında "Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir." hükmü yer almakta olup, bahsi geçen maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin "Hukuka ve dürüstlük kurallarına uygun olma", "Doğru ve gerektiğinde güncel olma", "Belirli, açık ve meşru amaçlar için işlenme", "İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ve "İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" olarak sayıldığı,

- Kanun'un "Veri sorumlusunun aydınlatma yükümlülüğü" başlıklı 10'uncu maddesinde ise "(1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; a) Veri sorumlusunun ve varsa temsilcisinin kimliği, b) Kişisel verilerin hangi amaçla işleneceği, c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi, d) 11 inci maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür." hükmüne yer verildiği,

- Ek olarak, ilgili kişilerin hakları Kanun'un 11'inci maddesinin;

"Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

a) Kişisel veri işlenip işlenmediğini öğrenme,

b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,

ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

d) Kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme,

e) 7'nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,

f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme haklarına sahiptir.” demek suretiyle düzenlendiği,

- Kanun’un ilgili hükümleri dikkate alındığında; ilgili kişinin adının ve soyadının, telefon numarasının, e-posta adresinin, adresinin, fotoğrafının ve özlük dosyasında bulunan bilgilerin ilgili kişinin kimliğini belirli veya belirlenebilir kılmaları nedeniyle kişisel veri niteliğini haiz oldukları, bu yüzden ilgili kişiye ait bahsi geçen kişisel verilerin veri sorumlusu tarafından elde edilmesi, depolanması, kullanılması, yayınlanması vb. fiillerin de Kanun kapsamında birer kişisel veri işleme faaliyeti teşkil ettiği ve böyle faaliyetlerin hem Kanun’da düzenlenen hukuki sebeplere dayanılarak hem de yine Kanun’da yer alan genel ilkelere uygun bir şekilde yürütülmesi gerektiği hususlarında herhangi bir şüphenin bulunmadığı,

- İlgili kişinin Kanun’un 11’inci maddesinde düzenlenen haklarına ilişkin olarak Kanun’un 13’üncü maddesine istinaden veri sorumlusuna yapmış olduğu başvurunun, Kanun’un yine 13’üncü maddesinde düzenlendiği şekilde veri sorumlusunca cevaplanması gerektiği,

- İlgili kişi tarafından yapılan şikâyetin “veri sorumlusunun aralarındaki iş sözleşmesinin devamı sırasında ilgili kişiye karşı Kanun’un 10’uncu maddesinden kaynaklanan aydınlatma yükümlülüğünü yerine getirmediği”, “veri sorumlusu ile olan iş sözleşmesinin eylemli fesih yoluyla sona erdirilmesinden sonra ilgili kişiye ait fotoğraf ve sair kişisel verilerin veri sorumlusunun internet sitesinde tutulmasına devam edildiği, söz konusu verilerin bu sitede tutulmasının ilgili kişinin açık rızasına bağlı olduğu ama konuya ilişkin olarak ilgili kişinin açık rızasının alınmadığı ve bu durumun da hukuka aykırı kişisel veri işleme faaliyeti teşkil ettiği” ve “ilgili kişinin Kanun’un 13’üncü maddesi uyarınca yaptığı başvuruya veri sorumlusu tarafından yeterli bir şekilde cevap verilmediği” yönündeki üç iddia üzerine yoğunlaştığı, bu yüzden inceleme konusu şikâyetin ilgili kişinin iddialarının yoğunlaştığı üç başlık altında değerlendirilmesinin yerinde olacağı,

“Veri sorumlusunun aralarındaki iş sözleşmesinin devamı sırasında ilgili kişiye karşı Kanun’un 10’uncu maddesinden kaynaklanan aydınlatma yükümlülüğünü yerine getirmediği” yönündeki iddia bakımından:

- Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi tarafından ilgili kişilere Kanun’un “Veri sorumlusunun aydınlatma yükümlülüğü” başlıklı 10’uncu maddesi uyarınca bilgi verilmesinin bir yükümlülük olduğu, söz konusu yükümlülük kapsamında uyulacak usul ve esasların belirlenmesi amacıyla çıkarılan Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ’in “Aydınlatma yükümlülüğünün kapsamı” başlıklı 4’üncü maddesinde, ilgili kişilere yapılacak bilgilendirmenin asgari olarak Kanun’un 10’uncu

maddesinde de sayılan beş hususu içermesi gerektiğinin hükme bağlandığı, “Usul ve Esaslar” başlıklı 5’inci maddesinde ise veri sorumlusu ya da yetkilendirdiği kişi tarafından aydınlatma yükümlülüğünün yerine getirilmesi esnasında uyulması gereken usul ve esasların düzenlendiği,

- Anılan mevzuat hükümleri uyarınca, ilgili kişiler hakkında yürütülen ve Kanun hükümlerinin uygulama alanı bulacağı kişisel veri işleme faaliyetleri kapsamında -kişisel verilerin elde edilmesi sırasında- veri sorumluları tarafından ilgili kişilere Kanun’un 10’uncu maddesi ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerine uygun olarak bilgilendirmede bulunulması gerektiği,

- Hâl böyle olmakla birlikte, dosyaya sunulan bilgi ve belgelerden; ilgili kişinin veri sorumlusunun Londra’da bulunan ofisinde işe başlaması nedeniyle ilgili kişiye Avrupa Birliği’nin birincil kişisel veri koruma düzenlemesi olan ve kısaca “GDPR” olarak bilinen Avrupa Birliği Genel Veri Koruma Tüzüğü’ne istinaden bilgilendirme yapıldığı, daha sonra ilgili kişinin Londra’daki görevinden ayrılarak veri sorumlusunun İstanbul’da bulunan irtibat ofisi bünyesinde görev yapmaya başladığı, dolayısıyla ilgili kişiye Avrupa Genel Veri Koruma Tüzüğü (GDPR) yükümlülükleri kapsamında yapılan bilgilendirmenin ilgili kişi hakkında veri sorumlusunca yürütülen kişisel veri işleme faaliyetleri açısından yeterli olduğu, ancak Türkiye’de işlenen kişisel veriler bakımından Kanun’un 10’uncu maddesine uygun olarak aydınlatma yükümlülüğünün yerine getirilmesi konusunda özen gösterilmesi hususunda veri sorumlusuna hatırlatmada bulunulmasının da uygun olacağı,

“Veri sorumlusu ile olan iş sözleşmesinin eylemli fesih yoluyla sona erdirilmesinden sonra ilgili kişiye ait fotoğraf ve sair kişisel verilerin veri sorumlusunun internet sitesinde tutulmasına devam edildiği, söz konusu verilerin bu sitede tutulmasının ilgili kişinin açık rızasına bağlı olduğu ama konuya ilişkin olarak ilgili kişinin açık rızasının alınmadığı ve bu durumun da hukuka aykırı kişisel veri işleme faaliyeti teşkil ettiği” yönündeki iddia bakımından:

- İlgili kişi ile veri sorumlusu arasındaki iş ilişkisinin ne zaman sona erdiği hususunda taraflar arasında bir uyuşmazlık olduğu (İlgili kişi veri sorumlusu ile olan iş ilişkisinin “eylemli fesih” yoluyla Nisan 2021’de sona erdirildiğinden bahsederken, veri sorumlusu tarafından ilgili kişi ile olan iş ilişkisinin bitiş tarihinin 01/07/2021 olarak bildirildiği),

- Taraflar arasında ilgili kişinin kişisel verilerinin veri sorumlusunun internet sitesinde Nisan 2021 öncesini kapsayan zaman diliminde yayınlanması konusunda herhangi bir ihtilafın bulunmadığı,

- Kişisel verilerinin veri sorumlusunun internet sitesinde yayınlanabilmesi için ilgili kişi tarafından başlangıçta bir açık rıza verilip verilmediği dosya kapsamına sunulan bilgi ve belgelerden tam olarak

anlaşılmasa da, söz konusu kişisel veri işleme faaliyetinin hukuki sebebinin Kanun'un 5'inci maddesinin (1) numaralı fıkrasında düzenlendiği şekliyle "açık rıza" olduğunun kabulü halinde, ilgili kişinin veri sorumlusuna iletildiği 26/05/2021 tarihli İhtarname'den sonra verilen açık rızanın geri alındığının da kabul edilmesinin gerektiği,

- İlgili kişinin kişisel verilerinin veri sorumlusunun internet sitesinde yayınlanmasının Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (f) bendindeki "İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" hukuki sebebine dayanmasının mümkün olabileceği, ancak bu hukuki sebebe dayanabilmesi için -somut olay özelinde tespit edilecek- veri sorumlusunun meşru menfaatleri ile ilgili kişinin temel hak ve özgürlükleri esas alınarak yapılacak bir "denge testi" sonucunda veri sorumlusunun meşru menfaatlerinin ağır basıyor olmasının gerektiği,

- Somut olayda, ticari hayatta meşru bir şirket olarak faaliyet gösteren veri sorumlusunun Türkiye'de bir irtibat ofisinin bulunduğunu ve bu ofiste kariyerli/yetkin kişilerin çalıştığını veya en azından kimlerin çalıştığını kamuoyuna açıklamakta meşru menfaatinin bulunduğu söylenebileceği ve böyle bir açıklamanın ilgili kişinin temel hak ve özgürlüklerine açıkça zarar verdiğinden de bahsedilemeyeceği,

- Taraflar arasındaki iş ilişkisinin -ilgili kişinin iddia ettiği gibi- Nisan 2021 itibarıyla sona erdiğinin kabul edilmesi halinde ise, ilgili kişinin kişisel verilerinin halen veri sorumlusunun internet sitesinde tutulmasının, mevcut iş ilişkisinin bitmesi sonrasında yeni iş arayışlarına girmesi noktasında ilgili kişinin Türkiye Cumhuriyeti Anayasası'nın 48'inci maddesinde düzenlenen "Çalışma ve sözleşme hürriyeti"ne zarar verebileceği ve ilgili kişi hakkında yürütülen kişisel veri işleme faaliyetlerinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (f) bendindeki "İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" hukuki sebebine dayanamayacağı savunulabileceği, zira iş aradığı sırada halen bir yerde çalışıyor görünen ilgili kişinin yapacağı iş başvurularının bu durumdan olumsuz etkilenmesinin ihtimal dâhilinde olduğu,

- Buna karşın, dosyaya sunulan tüm bilgi ve belgelerden, ilgili kişinin iş sözleşmesinin Nisan 2021 itibarıyla sona ermediği, ilgili kişinin Nisan 2021 ile Temmuz 2021 arasını kapsayan dönemde mevzuatın veri sorumlusuna Covid-19 salgınının ortaya çıkardığı şartlardan ötürü geçici olarak tanıdığı bir hak sayesinde alınabilen tek taraflı bir kararla ücretsiz izne çıkarıldığının anlaşıldığı ve mevzuattan kaynaklanan böyle bir durumda ilgili kişinin iş sözleşmesinin "eylemli fesih" yoluyla Nisan 2021'de sona erdirildiği iddiasının kabulünün mümkün görünmediği,

- Neticede, ilgili kişinin fotoğraf ve sair verilerinin Nisan 2021 sonrası dönemde veri sorumlusunun internet sitesinde yayınlanmasından ibaret olan kişisel veri işleme faaliyetinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (f) bendindeki "İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" hukuki sebebine dayanabileceği, bu yüzden de anılan faaliyeti dolayısıyla veri sorumlusu hakkında Kanun kapsamında yapılacak herhangi bir işlemin bulunmadığı,

"İlgili kişinin Kanun'un 13'üncü maddesi uyarınca yaptığı başvuruya veri sorumlusu tarafından yeterli bir şekilde cevap verilmediği" yönündeki iddia bakımından:

- Kanun'un "Veri sorumlusuna başvuru" başlıklı 13'üncü maddesinde ilgili kişilerin Kanun'un uygulanmasıyla bağlantılı olarak veri sorumlularına yapacakları başvuruların usul ve esaslarının ana hatlarıyla düzenlendiği,

- Bununla birlikte, veri sorumlusuna başvuru ve işlemin ayrıca bir maliyet gerektirmesi halinde alınacak ücret ile ilgili usul ve esasları belirlemek üzere hazırlanmış olan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in "Başvuru usulü" başlıklı 5'inci maddesinde "İlgili kişi, Kanununun 11 inci maddesinde belirtilen hakları kapsamında taleplerini, yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletir." ifadesine, "Başvuruya cevap" başlıklı 6'ncı maddesinde ise "Veri sorumlusu bu Tebliğ kapsamında ilgili kişi tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlüdür." ifadesine yer verildiği,

- İlgili kişinin Kanun'un 11'inci ve 13'üncü maddeleri ile Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in 5'inci maddesi uyarınca veri sorumlusuna yaptığı başvurunun, veri sorumlusu tarafından Kanun'un 13'üncü maddesi ile Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in 6'ncı maddesi çerçevesinde etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırılmadığı, zira veri sorumlusu tarafından ilgili kişinin 26/05/2021 tarihli başvurusuna cevaben iletilen 07/06/2021 tarihli e-postada ilgili kişinin Kanun'un 11'inci maddesi kapsamında yönelttiği bilgi taleplerinin tamamının cevaplanmadığı,

- Dolayısıyla, veri sorumlusunun ileride kendisine yapılabilecek ilgili kişi başvurularını mevzuata uygun şekilde cevaplandırması hususunda talimatlandırılmasının yerinde olacağı

değerlendirmelerinden hareketle;

- İlgili kişiye Avrupa Genel Veri Koruma Tüzüğü (GDPR) yükümlülükleri kapsamında bir bilgilendirme yapılmış olmakla birlikte Türkiye’de işlediği kişisel veriler bakımından Kanun’un 10’uncu maddesine uygun olarak aydınlatma yükümlülüğünü yerine getirmesi konusunda özen gösterilmesi hususunda veri sorumlusuna hatırlatmada bulunulmasına,
- Veri sorumlusu ile arasındaki iş ilişkisinden kaynaklanan uyuşmazlıkların çözümü için adli makamlar nezdinde girişimde bulunması gerektiği hususunda ilgili kişinin bilgilendirilmesine,
- İlgili kişiler tarafından kendisine Kanun’un 11’inci ve 13’üncü maddeleri ile Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ’in 5’inci maddesine istinaden yapılacak başvuruları Kanun’un 13’üncü maddesi ile Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ’in 6’ncı maddesi çerçevesinde etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırması hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2021/1217 sayılı KVKK Kararı

İlgili kişi anne ve ilgili kişi sıfatını haiz çocuğunun fotoğrafları da kullanılmak suretiyle ilgili kişi hakkında gerçek dışı, şeref ve haysiyet kırıcı bir televizyon haberi yapıldığı iddiası hakkında Kişisel Verileri Koruma Kurulunun 02/12/2021 tarihli ve 2021/1217 sayılı Karar Özeti

Karar Tarihi : 02/12/2021

Karar No : 2021/1217

Konu Özeti : İlgili kişi anne ve ilgili kişi sıfatını haiz çocuğunun fotoğrafları da kullanılmak suretiyle ilgili kişi hakkında gerçek dışı, şeref ve haysiyet kırıcı bir televizyon haberi yapılması

Kuruma yapılan şikâyetle özetle;

- “Veri sorumlusu” ve “hizmet sağlayıcı” sıfatlarını haiz olan bir medya şirketinin televizyon kanalının Ana Haber programında ilgili kişi ve 6698 sayılı Kişisel Verilerin Korunması Kanunu (6698 sayılı Kanun) hükümleri dâhilinde ilgili kişi sıfatını haiz çocuğunun fotoğrafları da kullanılmak suretiyle ilgili kişi anne hakkında gerçek dışı, şeref ve haysiyet kırıcı bir televizyon haberi yapıldığı,
- Söz konusu yayına ilişkin olarak medya şirketine yapılan başvuruda 6698 sayılı Kanun’un 11’inci maddesi uyarınca Ana Haber programında yer verilen kişisel verilerin yok edilmesinin, bu durumun kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesinin ve kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle uğranılan zararların giderilmesinin talep edildiği,
- Başvuruya konu Ana Haber programında, ilgili kişinin ve çocuğunun fotoğrafları kullanılarak ilgili kişinin ilk evliliğinden bir oğlunun ve bir kızının olduğu, altı yıldır da başkası ile evli olduğu ve ilk evliliğinden olan oğlunun ilgili kişiyi bıçakladığı, bıçak darbelerinden birinin ilgili kişinin kalbine geldiği, ilgili kişinin yaşam savaşı verdiği, canı evladın ise tutuklandığı ifadelerini içeren yayının yapıldığı,
- İlgili kişinin habere konu olayın geçtiği ilde ikamet etmediği, eşinden de boşanmadığı, ayrıca bıçaklanmasının da söz konusu olmadığı, dolayısıyla habere konu olayın da ilgili kişi ve çocuğu hakkında olmadığı, gerçeğe aykırı haber yapılırken ilgili kişinin Facebook sayfasından alınan fotoğrafın amacı dışında kullanılmasının ve yayılmasının hukuka açıkça aykırı olduğu,

- Hukuka aykırı olarak kullanılan fotoğrafla yapılan haber nedeniyle 5237 sayılı Türk Ceza Kanunu'nun 132 ila 138'inci maddelerinde düzenlenen suçların işlendiğinden bahisle Cumhuriyet Başsavcılığına suç duyurusunda bulunulduğu,

- Konuya ilişkin olarak medya şirketine yapılan başvuruya rağmen otuz günlük yasal süre içerisinde hukuka aykırılığın giderilmediği, başvuruçulara da bilgi verilmediği

hususları bildirilmiş olup; kişisel veri niteliğindeki fotoğrafın ve kimlik bilgilerinin kullanılması, yayılması ve ifşa edilmesi suretiyle 6698 sayılı Kanun'a aykırı hareket edildiğinden bahisle ilgili kişi tarafından bahsi geçen kişisel verilerin imha edilmesi, uğranılan zararların giderilmesi, ayrıca medya şirketi hakkında idari ve cezai yaptırım uygulanmasına karar verilmesi talep edilmiştir.

Yapılan şikâyete istinaden başlatılan inceleme çerçevesinde medya şirketinden savunması istenilmiş olup, verilen cevapta özetle;

- Kendilerinin 6112 sayılı Radyo ve Televizyonların Kuruluş ve Yayın Hizmetleri Hakkında Kanun (6112 sayılı Kanun) kapsamında kurulmuş, özel televizyon yayıncılığı alanında faaliyet gösteren, yayınları ve faaliyetleri 6112 sayılı Kanun'da belirlenen kurallara, yayın ilkelerine ve Radyo ve Televizyon Üst Kurulu (RTÜK) denetimine tabi bir şirket oldukları,

- Yayınlanan haberlere ilişkin düzeltme ve cevap metinlerinin 6112 sayılı Kanun'un "Düzeltilme ve cevap hakkı" başlıklı 18'inci maddesi uyarınca değerlendirildiği, gerçek ve tüzel kişiler tarafından iletilen metinde düzeltme yapılması gerekirse ya da hukuken geçerli bir talep olmadığı kanaatine varılırsa yayın kuruluşunun metni yayınlamak zorunda olmadığı, bu durumda ilgisinin yayın için gerekli sürenin bitiminden sonra süresi içerisinde görevli yargı merciine başvuracağı ve yayıncı kuruluşun ancak hakkında alınan cevap ve düzeltme metninin yayınına dair kesinleşmiş yargı kararından itibaren yedi gün içinde kararın gereğini yerine getirmek zorunda olduğu, aksinin RTÜK denetimi ve yaptırımını sonucunu doğuracağı,

- 6112 sayılı Kanun'un ilgili hükümleri gereğince yayınlanmasına kesin olarak karar verilmiş olan cevap ve düzeltme metninin yayınlanmaması halinde yayın kuruluşlarına RTÜK tarafından idari yaptırım uygulandığı,

- 6112 sayılı Kanun'un 18'inci maddesi uyarınca ihtarname üzerine cevap ve düzeltme metninin yayınlanmasının zorunlu olmadığı, aynı zamanda ilgili kişilerin ihtarname düzenlenmeksizin doğrudan genel yargı yoluna müracaat ederek bu haklarını kullanmalarının da mümkün olduğu, bu konuda esas yetkinin genel yargıda olduğu,

- Dosya kapsamında medya kuruluşuna çekilen ihtarname ekinde yer alan cevap ve düzeltme metninin yetkililerince incelendiği, metnin toplumu yanıltacak şekilde düzenlendiği kanaatine varılmasından ve 6112 sayılı Kanun gereğince metin üzerinde değişiklik yapılamayacağından dolayı yayınlanmaması kararının alındığı,
- Cevap ve düzeltme metninin yayınlanmamasına dair kararın hukuki gerekçelerinin bulunduğu, zira haberin içeriğinin DHA, İHA ve AA gibi ajanslardan alınan bilgiler ile olay yerinde ve çevresinde yapılan araştırma ve röportajlara dayandığı, tüm açılardan bakıldığında haber içeriğinin somut gerçeğe uygun olduğunun ve o aşamada yapılabilecek bir araştırmanın da bulunmadığının anlaşıldığı,
- Haber içeriğinde ne mağdur kadının ne de başka herhangi bir şahsın şeref ve haysiyetine veya kişilik haklarına saldırı teşkil edecek bir ifade veya yorumda bulunulmadığı, hatta haber ajanslarının mağdur kadın hakkında verdikleri detaylara dahi haberde yer verilmediği,
- Haberi yayınlayan muhabirin olay yerine gidip ilgililerle ve faili yakalayan emniyet mensuplarıyla görüştüğü, mağdur kadının eşi de dâhil olmak üzere görüşülen kişilerden alınan bilgi ve teyit üzerine yayınlanan haberde ilgili kişiye ve çocuğuna ait olduğu bildirilen fotoğrafların tamamen yüzleri kapatılarak izleyicilere sunulduğu,
- Haberde ilgili kişinin eşinin ve çocuğunun adlarının hiç geçmediği, ilgili kişi ile habere konu mağdur kadının isim ve soy isim benzerliği ile bilginin olay hakkında görüşülen emniyet mensuplarından alınması ve fotoğrafın teyidi karşısında esasen bu konuda kendilerine atfedilebilir bir kusurun bulunmadığı,
- Kendilerine iletilen Kurum yazısında özetlenen şikâyet dilekçesi kapsamında haberdeki fotoğrafın herkese açık olduğu anlaşılan Facebook sayfasında yer aldığı ifade edildiği, bu yüzden söz konusu fotoğrafın kanuna aykırı bir şekilde elde edilmediğinin veya gizli bir veri olmadığının açık olduğu, kaldı ki fotoğrafların tamamen kapatılarak yayınlandığı,
- Mağdur kadının eşinin belki benzerlikten dolayı belki de olayın şoku ile kendisine gösterilen ve onaylaması üzerine haberde kullanılan fotoğrafın mağdura ait olduğunu teyit ettiği, buna rağmen gerek annenin gerekse oğlunun yüzlerinin tamamen kapatılarak yayınlandığı,
- Orta düzeyde bir izleyicinin haberde yer alan fotoğraftaki kişinin talepte bulunan kişiye ait olduğunu anlamasının mümkün olmadığı, ayrıca olayın ilgili kişilerin ikamet etmedikleri bir ilde gerçekleşmiş olmasından ve olayın failinin açık kimliğinin ve görüntülerinin de haberde yer

almasından dolayı şikâyetçilerin habere konu kişiler olduğu sonucuna varılamayacağına açık olduğu,

- Bir an için haberde yer alan fotoğrafın talepte bulunana ait olduğu sadece kendisini tanıyanlar tarafından anlaşılrsa dahi bunun isim benzerliğine dayanan bir hatadan kaynaklandığının da hemen anlaşılacağı, nitekim mezkûr olayın gerçekleştiği yerin açık bir şekilde haberde yer aldığı ve fotoğrafların blurlanmış/buzlanmış şekilde yayında gösterildiği,
- Haberin içeriğinde yer verilen hiçbir unsurun şikâyetçilerin şeref ve haysiyetini ihlal eder nitelikte olmadığı, habere konu olayın tamamen gerçek olduğu, haberdeki tek hatanın mağdur kadının ismi ile olan benzerlik nedeniyle ilgili kişinin isminin bir kez haberde yer alması ve bu isimle muhabirlerine verilen fotoğrafların yüzleri tamamen kapatılarak haberde yer alması olduğu,
- Dolayısıyla, şikâyetçilerce “medya şirketi tarafından yalan ve yanlış bir haber yayınlanmış, olayın gerçekleştiği ilde bir oğul annesini bıçaklamamış gibi” hazırlanan cevap ve düzeltme metni üzerinde herhangi bir düzeltme yapılmasına imkân bulunmadığından yasal yollar tüketilmeden gönderilen metnin yayınlanmaması kararı alınmasının tamamen haklı ve hukuka uygun olduğu,
- Ancak şikâyetçinin RTÜK yerine doğrudan genel yargı yoluna başvurduğu ve mahkeme kararı üzerine süresi içerisinde cevap ve düzeltme metnini yayınladıkları, bu noktada Kişisel Verileri Koruma Kuruluna (Kurul) şikâyetin cevap ve düzeltme metninin yayınlanmasından sonra yapıldığının dikkat çekici olduğu,
- Cevap ve düzeltme metninin yayınlanmasıyla birlikte haber yayınındaki verilere ilişkin hatanın düzeltildiği ve bu düzeltmenin üçüncü kişilere yani ilk yayının ulaştığı izleyicilere bildiriminin tamamlandığının vakıa olduğu,
- Yayın kayıtlarını silmelerinin, yok etmelerinin veya üzerinde düzeltme yapmalarının tabi oldukları 6112 sayılı Kanun kapsamında mümkün olmadığı, zira 6112 sayılı Kanun’un “Yayın kayıtlarının muhafazası” başlıklı 25’inci maddesi gereğince yaptıkları her yayının kaydını bir yıl süreyle muhafaza etmekle yükümlü oldukları,
- Bu bakımdan haberdeki yüzleri kapatılmış fotoğrafın ve sadece bir kez geçen ismin silinmesine yönelik talebin kabulünün 6112 sayılı Kanun kapsamında bir yıldan önce mümkün olmadığı, ayrıca 6112 sayılı Kanun’un “Yayın kayıtlarının muhafazası” başlıklı 25’inci maddesinin son fıkrasında da “Yayının herhangi bir şekilde soruşturma veya kovuşturma konusu yapılması halinde, bu işlemlerin sonuçlandırılmasının yetkili mercilerce ilgili medya hizmet sağlayıcı kuruluşa yazılı olarak bildirilmesine kadar soruşturma veya kovuşturma konusu yayın kaydının saklanması zorunludur.” denildiği,

- 6698 sayılı Kanun'un "İstisnalar" başlıklı 28'inci maddesinin (1) numaralı fıkrasında yazılı basın ve televizyon faaliyetlerini de içine alan ifade özgürlüğü kapsamında kişisel verilerin işlenmesinin 6698 sayılı Kanun hükümlerinin uygulanması hususunda tam bir istisna hali olarak düzenlendiği,
- Anayasa'nın 26'ncı maddesinin de "Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet Resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. (...) Bu hürriyetlerin kullanılması, millî güvenlik, kamu düzeni, (...), başkalarının şöhret veya haklarının, özel ve aile hayatlarının yahut kanunun öngördüğü meslek sınırlarının korunması veya yargılama görevinin gereğine uygun olarak yerine getirilmesi amaçlarıyla sınırlanabilir." hükmünü içerdiği,
- Haber bültenlerinin kuşkusuz 6698 sayılı Kanun'un 28'inci maddesinde sayılan istisna kapsamına girdikleri, bu bakımdan yayınlanan haberin Anayasa'nın 26'ncı maddesi uyarınca güvence altına alınan "basın hürriyeti" ve "kamunun haber alma hakkı" kapsamında değerlendirilmesi gerektiği,
- İfade özgürlüğü ve basın hürriyetinin değerlendirmesi yapılırken ifade özgürlüğünü ve basın hürriyetini düzenleyen Anayasa'nın ilgili maddelerinin, taraf olduğumuz uluslararası sözleşmelerin, basın özgürlüğünün sınırlarına ilişkin Avrupa İnsan Hakları Mahkemesinin ("AİHM") yerleşik içtihatlarının ve kriterlerinin dikkate alınmasının zorunlu olduğu,
- Yargıtay ve doktrinde istikrar bulmuş görüşler uyarınca bir haberin ifade özgürlüğü kapsamında haber niteliği taşıyabilmesinin belirli bazı koşullara bağlı olduğu, bunların "haber (1) gerçek olması, (2) güncel olması, (3) verilisinde kamusal ilgi ve yararın bulunması, (4) düşünce ve ifade arasında düşünsel bağ bulunması" şeklinde belirlendiği, Kurulun 22/05/2020 tarihli ve 2020/414 sayılı kararında da 6698 sayılı Kanun'un 28'inci maddesinde istisna olarak kabul edilen ifade özgürlüğünün bir yansıması olan basın özgürlüğü ile kişilik hakları karşı karşıya geldiğinde "haber; kamu ilgi ve yararı taşıması, gerçek ve güncel olması, özü ile biçimi arasındaki denge" kriterleri kapsamında değerlendirilmesi suretiyle hangi hakka üstünlük tanınması gerektiğinin belirlenmesinin önem arz ettiğinin vurgulandığı,
- Kurulun 23/06/2020 tarihli ve 2020/481 sayılı kararında basın özgürlüğü ve toplumun bilgiye ulaşma hakkının önemine vurgu yapılarak yarışan haklar arasındaki dengenin somut olay özelinde değerlendirilmesi gerektiğinin belirtildiği,
- Keza Yargıtay 4. Hukuk Dairesinin 2016/5516 E., 2016/8275 K. ve 23/06/2016 tarihli kararında da basın özgürlüğü ile kişilik hakları çatışmasında izlenecek yol ve kriterler belirlenirken kamusal yarar kapsamında basın özgürlüğüne üstünlük tanınması gerekeceğinin "(...) O anda ve görünürde var

olup da sonradan gerçek olmadığı anlaşılan olayların yayınından da basın sorumlu tutulmamalıdır.” açıklamaları ile vurgulandığı,

- Yine Yargıtay 4. Hukuk Dairesinin 17/05/1999 tarihli ve 2683 E., 4551 K. sayılı hükmünde de “Hukuka uygunluk nedenlerinde, korunan kişinin (o an için) korunmakta ya bir çıkarı yoktur ya da korunan çıkar karşısında yer alan ve onunla çatışan değer daha üstünlük taşımaktadır. Bunun sonucunda da, daha az üstün yarar, daha çok üstün olanı karşısında, hukuk düzenince çiğnenmesi uygun görülmektedir. Böylece ya ‘çıkâr eksikliği veya yokluğuna dayanan hukuka uygunluk’ ya da ‘çıkâr üstünlüğüne dayanan hukuka uygunluk’ söz konusu olmaktadır.” vurgusunun yapıldığı,

- Avrupa Birliği Adalet Divanının (ABAD) bir kararında da, demokratik toplumda ifade özgürlüğünün önemli olduğunun, geniş yorumlanması gerektiğinin, kişisel verilerin korunması hakkı ile ifade özgürlüğü arasındaki dengede kişisel verilerin korunması hakkının istisnalarının ve sınırlamaların zaruri olduğu kadarının uygulanması gerektiğinin belirtildiği, bu bakımdan 6698 sayılı Kanun’un 28’inci maddesinde ifade özgürlüğüne tam istisna tanınmasında büyük bir isabet bulunduğu konusunda bir kuşkunun olmadığı,

- Her ne kadar 6698 sayılı Kanun özel bir usulle ve idari yaptırımlar yoluyla kişisel verileri korumayı amaçlamakta ise de somut olay özelinde olduğu gibi 6112 sayılı Kanun, Türk Medeni Kanunu ve daha pek çok kanunda yer alan düzenlemelerin ilgili kişileri koruyucu hükümler ve yaptırımlar içerdiği, dolayısıyla 6698 sayılı Kanun’un 28’inci maddesi ile getirilen tam istisna nedeniyle kişilerin korumasız kaldığı sonucunun da doğmadığı,

- Nitekim somut olayda şikâyetçilerin 6112 sayılı Kanun’un 18’inci maddesi uyarınca genel yargı yerine müracaat ettikleri ve verilen yargı kararıyla hatanın düzeltilmesini, bu şekilde de iddia olunan zararlarının giderilmesini temin ettikleri,

- Şikâyetçilerin lehlerine kesin karar almalarına karşın Kuruma aynı taleplerle şikâyetle bulunmalarının hukuken himaye edilemeyeceği, yargıya müracaat ile taleplerini karşılamış olan şikâyetçilerin varsa başkaca hakları bunu yine genel yargı yoluna müracaat ile sağlamaları gerekirken yargı yerine Kurul eliyle kendilerine menfaat sağlamak istemelerinin yargı denetiminden kaçınılması ve hakkın kötüye kullanılması mahiyetinde olduğu,

- 6698 sayılı Kanun özel bir usulle ve yaptırımlar yoluyla kişisel verileri korumayı amaçlamakta ise de 6112 sayılı Kanun’un da aynı amacı güden düzenlemeler içerdiği, kendilerinin yayınları üzerinde denetim yetkisinin de esasen özel yasa ile RTÜK’e verildiği ama cevap ve düzeltme metni yayınlanıp konu hakkında RTÜK’e bilgi verilmesine rağmen mezkûr yayın hakkında RTÜK tarafından herhangi

bir işlem tesis edilmediği, bununla birlikte RTÜK'ün dahi zarar tazmini gibi maddi konuların genel yargı tarafından çözülmesi gerektiğini kabul ettiği ve bu tür müracaatlara bu gerekçelerle olumsuz cevap verdiği,

- Tüm açıklamaların ve sunulan kanıtların şikâyet konusu yayın hakkında genel yargı yoluna müracaat edildiğini ve şikâyetçilerin kendi haklarını koruyabilme imkânına sahip olduklarını gösterdiği,
- Detaylı olarak açıklandığı üzere, şikâyete konu haberinin içerik olarak tamamen gerçeğe uygun olduğu, ayrıca yayınlanmasında kamu yararı bulunan güncel bir olayın öze biçim arasındaki denge bozulmaksızın haber konusu edildiği, ne var ki emniyet kaynaklı ve isim benzerliğine dayalı bir hatanın -herkese açık bir yerden elde edilen fotoğraf haberde tamamen yüzleri kapatılarak yayınlanmış olsa da- şikâyete konu olduğu, ancak cevap ve düzeltme metninin yayınlanması ile hatanın telafi edildiğinin de vakıa olduğu, zira inceleme konusu açısından kişisel verilerin aktarıldığı üçüncü kişiler olan izleyicilere bildirim yapıldığı ve uğranılan bir zarar varsa bunun da giderildiği,
- Düzenlenen ihtarnamede her ne kadar 6698 sayılı Kanun'un 11'inci maddesi uyarınca kişisel verilerin yok edilmesi talep edilse de şikâyetçilerin kişisel veri olarak belirttiği hususlar ile haber kaydının en az bir yıl süreyle tutulmasının 6112 sayılı Kanun'un ilgili hükümleri nedeniyle zorunlu olduğu, dolayısıyla bu konudaki talebin yerine getirilmesinin şu an için mümkün olmadığı,
- Görüleceği üzere, somut olayda genel bir kanun olan 6698 sayılı Kanun ile özel bir kanun olan 6112 sayılı Kanun arasında bir çatışmanın da söz konusu olduğu, ancak şikâyet konusu haber hakkında 6698 sayılı Kanun'un uygulama alanı bulamayacağı ve bu durumun da 6698 sayılı Kanun'un 28'inci maddesi ile getirilen tam istisnanın isabetinin bir kez daha tezahürü olarak kabul edilmesi gerektiği ifade edilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde, Kurulun 02/12/2021 tarihli ve 2021/1217 sayılı kararı ile;

- 6698 sayılı Kanun'un "Tanımlar" başlıklı 3'üncü maddesinde kişisel verinin: "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", ilgili kişinin; "Kişisel verisi işlenen gerçek kişi", kişisel verilerin işlenmesinin; "Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", veri sorumlusunun; "Kişisel

verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi” olarak tanımlandığı,

- Öte yandan, 6698 sayılı Kanun’un “Kişisel Verilerin İşlenme Şartları” başlıklı 5’inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğunun hükme bağlandığı,

- 6698 sayılı Kanun’un özel nitelikli kişisel verilerin işlenme şartlarının düzenlendiği 6’ncı maddesinin (1) numaralı fıkrasında özel nitelikli kişisel verilerin tanımlandığı, (2) numaralı fıkrasında özel nitelikli kişisel verilerin ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğunun hüküm altına alındığı, (3) numaralı fıkrasında özel nitelikli kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenebileceği durumların sayıldığı, (4) numaralı fıkrasında ise özel nitelikli kişisel verilerin işlenmesinde Kurul tarafından belirlenen yeterli önlemlerin ayrıca alınmasının şart olduğunun ifade edildiği,

- Ayrıca, 6698 sayılı Kanun’un kişisel verilerin işlenmesine ilişkin “Genel ilkeler”i düzenleyen 4’üncü maddesinin (1) numaralı fıkrasında “Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.” hükmü yer almakta olup, bahsi geçen maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin “Hukuka ve dürüstlük kurallarına uygun olma”, “Doğru ve gerektiğinde güncel olma”, “Belirli, açık ve meşru amaçlar için işlenme”, “İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ve “İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme” olarak sayıldığı,

- 6698 sayılı Kanun’un “İstisnalar” başlıklı 28’inci maddesinde ise 6698 sayılı Kanun’un hiçbir hükmünün uygulanmayacağı “tam istisna halleri” ile 6698 sayılı Kanun’un belli hükümlerinin uygulanmayacağı “kismî istisna halleri”nin düzenlendiği,

- Dosyaya sunulan bilgi ve belgeler, 6698 sayılı Kanun'un 1, 2, 3, 4, 5, 6 ve 8'inci madde hükümleri ışığında ele alındığında; ilgili kişinin isim ve soy isim bilgileri ile ilgili kişi ve çocuğuna ait bir fotoğrafın adı geçen kişilerin kimliklerini belirli veya belirlenebilir kılmaları nedeniyle "kişisel veri" niteliğini haiz olacakları, ayrıca ilgili kişinin isim ve soy isim bilgileri ile ilgili kişi ve 6698 sayılı Kanun hükümleri dâhilinde ilgili kişi sıfatını haiz olan ilgili kişinin çocuğuna ait fotoğrafın medya şirketi bünyesinde kayıt altına alma, depolama, yayınlama vb. fiillere konu edilmesinin 6698 sayılı Kanun uyarınca birer "kişisel veri işleme faaliyeti" teşkil edeceği, bahsi geçen kişisel veri işleme faaliyetlerini yürüten medya şirketinin 6698 sayılı Kanun önünde "veri sorumlusu" olacağı, bu durumda medya şirketi tarafından ilgili kişiler hakkında yürütülen kişisel veri işleme faaliyetlerinin 6698 sayılı Kanun'un 5'inci maddesinde yer alan şartlardan birine dayanarak ve 6698 sayılı Kanun'un 4'üncü maddesindeki genel ilkelere uygun şekilde yürütülmesinin gerekeceği konularında herhangi bir şüphenin bulunmadığı,
- İlgili kişilere ait fotoğrafın medya şirketi tarafından blurlanmak/buzlanmak suretiyle yayınlanmış olmasının somut olayda blurlanan/buzlanan fotoğraf ile "isim ve soy isim" gibi başka bilgilerin birleştirilmesi/eşleştirilmesi halinde ilgili kişilerin kimliklerinin belirlenebilmesinin mümkün olmasından ötürü mezkûr fotoğrafın kişisel veri niteliğini ortadan kaldırmadığı, zira ilgili kişinin haberde paylaşılan isim ve soy isim bilgileri ile arama motorlarından ve/veya -dosya kapsamına sunulan bilgi ve belgelerde belirtildiği üzere- Facebook adlı sosyal medya platformundan arama yapıldığında bu fotoğrafın blurlanmamış/buzlanmamış versiyonuna da erişimin mümkün olduğu,
- İlgili kişilerin haberde kullanılan fotoğrafının herkese açık olduğu anlaşılan Facebook sayfasında yer almasının (diğer bir deyişle alenileştirilmiş olmasının), bu fotoğrafın amacı dışında kullanılabilmesine cevaz vermeyeceği ve fotoğrafın işlenmesinin 6698 sayılı Kanun'da düzenlenen kişisel veri işleme şartlarına dayanması gerektiğinin açık olduğu, 6698 sayılı Kanun kapsamında "alenileştirme" kavramının, kişisel verinin herhangi bir şekilde kamuoyuna sunulmasından daha dar bir anlama sahip olduğu ve ilgili kişinin alenileştirme iradesi ve alenileştirme amacı ile yakın ilişki içerisinde bulunduğu,
- Tüm bunların yanı sıra; 6698 sayılı Kanun'un "İstisnalar" başlıklı 28'inci maddesinin (1) numaralı fıkrasının (c) bendinde 6698 sayılı Kanun hükümlerinin "Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi" halinde uygulanmayacağı düzenlendiği,

dolayısıyla inceleme konusu şikâyete esas haberden ibaret olan yayım faaliyetinin mezkûr hükmün kapsamına girip girmediğinin öncelikle değerlendirilmesi gerektiği,

- 6698 sayılı Kanun'un 28'inci maddesinin (1) numaralı fıkrasının (c) bendi düzenlemesinin kişisel verilerin işlendiği ve ifade özgürlüğü ile özel hayatın gizliliğinin veya kişilik haklarının çatıştığı hallerde haklar arasında bir denge testinin yapılmasını gerektirdiği ve sadece -yapılacak denge testinin ardından - çatışan haklar bakımından özel hayatın gizliliğinin veya kişilik haklarının ifade özgürlüğüne üstün geldiğinin anlaşıldığı durumların 6698 sayılı Kanun hükümlerine göre incelenip değerlendirilebileceği,

- Bu çerçevede, Kurulun 22/05/2020 tarihli ve 2020/414 sayılı kararında da belirtildiği üzere, ifade özgürlüğünün bir yansıması olan basın özgürlüğü ile kişilik hakları karşı karşıya geldiğinde haberin; a) Kamu ilgi ve yararı taşıması, b) Gerçek ve güncel olması, c) Özü ile biçimi arasındaki denge, kriterleri kapsamında değerlendirilmesi suretiyle hangi hakka üstünlük tanınması gerektiğinin belirlenmesinin önem arz ettiği,

- Haberin kamu ilgi ve yararı taşıyıp taşımadığının tespitinde, haberin kişilerin gereksiz merak duygularına mı yoksa yüksek ahlaki ve hukuki değerlerin korunmasına mı hizmet ettiğinin değerlendirilmesinin gerektiği,

Şikâyete esas haberin esasını oluşturan "bir gencin eşinden boşanıp bir başkası ile evlenen annesinin kapısına dayanarak onu kalbinden bıçakladığı" bilgisinin paylaşılmasında herhangi bir kamu ilgi ve/veya yararının bulunduğu bahsedilemeyeceği, buna karşın kamuoyu nezdinde "üçüncü sayfa haberi" olarak bilinen bu tarz haberlerin basında sıklıkla yer aldığı dikkate alındığında inceleme konusu haberin "haberin kamu ilgi ve yararı taşıyıp taşımadığı" kriteri kapsamındaki durumunun tartışmalı olduğu sonucuna ulaşıldığı,

- Haberin gerçek ve güncel olması kapsamında; gerçekliğin habere konu edilen olayın gerçek olması anlamına geldiği, ancak yerleşik yargı kararlarında gerçeklikten maddi gerçekliğin değil görünürdeki gerçekliğin anlaşılması gerektiği ve görünürdeki gerçekliğe uygun olarak yapılan haberlerden ötürü basının sorumlu tutulmamasının ihtimal dâhilinde olduğunun kabul edildiği,

- Bahsi geçen "maddi gerçeklik" kavramının haber konusu olayın haberde zikredildiği şekliyle gerçekleşip gerçekleşmediğini nitelemekte olduğu, "görünürdeki gerçeklik" kavramının ise haberin verildiği anda ve görünürde var olan olgulara uygunluğunu ifade ettiği,

- Diğer taraftan, bir haberin maddi gerçekliğe veya görünürdeki gerçekliğe uygun olup olmadığı konusunda bir değerlendirme yapılmadan önce, o habere konu bilgilerin gerçeğe uygun olup

olmadığının araştırılması hususunda ilgili basın kuruluşu tarafından gereken her türlü dikkat ve özenin gösterilip gösterilmediğinin ele alınması gerektiği,

- Zira haber yapılmadan önce ilgili basın kuruluşunca gereken her türlü dikkat ve özen gösterilmemişse, orada artık maddi gerçeklik veya görünürdeki gerçeklik tartışması yapılmasının herhangi bir fayda sağlamayacağı,

- İnceleme konusu haber bu bilgiler ışığında ele alındığında; haberin dayandırıldığı olay örgüsünün gerçek olduğu ama bir bütün olarak bakıldığında haberin doğru/gerçek olmadığı, zira haberde mağdurun adının yanlış aktarıldığı ve olayla alakasız bir kişi konumunda olan ilgili kişinin çocuğu ile birlikte olduğu bir fotoğrafının blurlanarak/buzlanarak da olsa kullanıldığı, bunun da yapılan haber yayınlanmadan önce medya şirketi tarafından haber içeriğindeki unsurlarının doğruluğuna ilişkin gereken her türlü dikkat ve özenin gösterilmediğine işaret ettiği,

- Medya şirketi “haber içeriğinin DHA, İHA ve AA gibi ajanslardan alınan bilgiler ile olay yerinde ve çevresinde yapılan araştırma ve röportajlara dayandığı, tüm açılardan bakıldığında haber içeriğinin somut gerçeğe uygun olduğu ve o aşamada yapılabilecek bir araştırmanın da bulunmadığı” yönünde bir savunma yapmış olsa da, yine medya şirketi tarafından Kuruma iletilen ve yapılan haberin kaynağı olarak gösterilen (İHA ve DHA haber ajanslarına ait) haberlerde mağdur kadının isminin doğru bir şekilde yazılmış olduğunun görüldüğü,

- Dolayısıyla, medya şirketince dikkatli ve özenli bir şekilde haber yapılmış olsa idi yapılan isim yanlışlığının en azından haberde görüntülerine yer verilen mağdur kadının eşinden teyit edilmek suretiyle düzeltilebileceğinin rahatlıkla söylenebileceği,

- Medya şirketi “mağdur kadının eşinin belki benzerlikten dolayı belki de olayın şoku ile kendisine gösterilen ve onaylaması üzerine haberde kullanılan fotoğrafın mağdura ait olduğunu teyit ettiği” yönünde bir savunma beyanında bulunmuş olsa da bu beyanın tevsik edici herhangi bir belge ile desteklenemediği, böyle bir eksikliğin ise medya şirketinin söz konusu beyanının salt olarak sorumluluktan kurtulmak amacıyla ortaya atılmış olabileceği izlenimini uyandırdığı,

- Zira medya şirketinin savunmasında bahsedildiği gibi bir “onay” işleminin mevcut olması durumunda, bahsi geçen onay işlemin işini dikkatli ve özenli yapan bir basın kuruluşu tarafından yazılı ve/veya görüntülü olarak kayıt altına alınmasının hayatın olağan akışına uygun olacağı ve haberin yapımı ve yayınlanması sürecini sekteye uğratacak ek bir külfet de getirmeyeceği,

- Öte yandan, “haber güncel olması” kriterinin somut olayın açıklandığı tarihlerde kamu yararının bulunması esasına dayandığı, üzerinden süre geçmiş ve açıklanmasında artık kamu yararı

bulunmayan bir olayın yayınlanmasında haber verme hakkından söz edilemeyeceğinin ve kişilik hakkına üstünlük tanınması gerekeceğinin savunulabileceği,

- Bu kapsamda, somut olayda habere konu olayın haberleştirilmesinde kamu yararının bulunup bulunmadığının tartışmalı olduğu düşünülse de, habere konu olayın gerçekleşme tarihi ile haberin veriliş tarihi göz önüne alındığında haberin güncel olduğunun söylenebileceği,
- Biçim ve öz arasındaki denge kriteri açısından; kullanılacak dil ve ifade ile yapılacak niteleme ve vurgunun haberin gerektirdiği biçim ve ölçü çerçevesinde kalmasının gerektiği (diğer bir deyişle, haberde kullanılan dil, ifade, resim/şekil/tablo ve fotoğrafların haberin veriliş biçiminin gerektirdiği ölçüde olması gerektiği),
- Haber verilirken gerekli, yararlı ve ilgili olmayan içeriklerin kullanılmasının kişilik haklarına ölçüsüz müdahale anlamına gelebileceği, bu yüzden inceleme konusu haberin verilişinin -kullanılan fotoğrafların blurlanmış/buzlanmış olması nedeniyle- ölçülü olduğunun ilk bakışta savunulabileceği,
- Ancak ilgili kişinin isim ve soy isim bilgisinin haber içeriğinde zikredilmesi ve bu isim-soy isim bilgileri kullanılarak fotoğrafların açık kaynaklardan teyit edilebilmesinin mümkün olması sebepleriyle, yapılan haberin biçimi ile özü arasında makul bir dengenin bulunmadığının, diğer bir ifadeyle haberin ölçüsüz olduğunun kabul edilmesi gerektiği, ayrıca haberin biçimi açısından anılan fotoğrafların blurlanmış/buzlanmış şekilde de olsa ekrana yansıtılmasının gerekli olmadığını da savunulabileceği,
- Yayınlanan bir haber kapsamında çatışan haklar konumundaki ifade özgürlüğü ile kişilik hakkı arasında yapılan denge testi neticesinde ifade özgürlüğüne öncelik tanınabilmesi için zikredilen üç kriterin de aynı anda karşılanmasının gerektiği, ancak inceleme konusu şikâyetin dayandığı haber bakımından bahsi geçen kriterlerin tamamını karşılanmadığı,
- Bu yüzden, veri sorumlusu tarafından ilgili kişi ile çocuğuna ait bilgiler ve fotoğraf da kullanılarak yapılan haberin 6698 sayılı Kanun'un 28'inci maddesinin (1) numaralı fıkrasının (c) bendi uyarınca 6698 sayılı Kanun hükümlerinden istisna tutulamayacağı,
- Veri sorumlu medya şirketinin ilgili kişiler hakkında yürüttüğü kişisel veri işleme faaliyetinin 6698 sayılı Kanun'un 28'inci maddesinin (1) numaralı fıkrasının (c) bendi uyarınca 6698 sayılı Kanun hükümlerinden istisna tutulamamasından ötürü söz konusu kişisel veri işleme faaliyetinin 6698 sayılı Kanun hükümlerine uygun olması gerektiği,
- Bununla birlikte, somut olayda veri sorumlusu tarafından ilgili kişiler hakkında yürütülen kişisel veri işleme faaliyetleri için 6698 sayılı Kanun'da düzenlenen herhangi bir hukuki sebebe

dayanılmadığının görüldüğü, bu durumun ise mezkûr kişisel veri işleme faaliyetini hukuka aykırı hale getirdiği,

- 6698 sayılı Kanun'un "Kurula şikayet" başlıklı 14'üncü maddesinin (3) numaralı fıkrasındaki "Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır." hükmü, 6698 sayılı Kanun'un "Şikayet üzerine veya resen incelemenin usul ve esasları" başlıklı 15'inci maddesindeki "(...) 1/11/1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanununun 6 ncı maddesinde belirtilen şartları taşımayan ihbar veya şikayetler incelemeye alınmaz. (...)" hükmü ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun'un "İncelenemeyecek dilekçeler" başlıklı 6'ncı maddesindeki "Türkiye Büyük Millet Meclisine veya yetkili makamlara verilen veya gönderilen dilekçelerden; (...) b) Yargı mercilerinin görevine giren konularla ilgili olanlar, (...), incelenemezler." düzenlemesi gereğince, ilgili kişilerin yargı mercilerinin görev alanına giren veri sorumlusundan tazminat talepleri konusunda Kurul tarafından yapılabilecek herhangi bir işlemin bulunmadığı,

- İnceleme konusu habere ilişkin olarak, bir yargı kararına istinaden veri sorumlusu tarafından süresi içerisinde cevap ve düzeltme metninin yayınlanması suretiyle yayının ilk ulaştığı izleyicilere haberde yapılan hata hakkında bildirimde bulunulmuş olmasının veri sorumlusu tarafından yürütülen hukuka aykırı kişisel veri işleme faaliyetini ortadan kaldırmayacağı,

- İlgili kişiler tarafından Kurula yapılan şikâyetin, mahkeme kararına istinaden bir cevap ve düzeltme metninin yayınlanmasından sonra yapılmış olmasının konuya ilişkin olarak 6698 sayılı Kanun hükümleri uyarınca yapılacak müstakil değerlendirmeleri etkilemeyeceği

değerlendirmelerinden hareketle;

- Mevcut tüm bilgi ve belgeler itibarıyla, ilgili kişilere ait kişisel verilerin veri sorumlusunca herhangi bir işleme şartına dayanmadan işlendiği, bu hususun ise veri güvenliğine ilişkin yükümlülüklerin düzenlendiği 6698 sayılı Kanun'un 12'nci maddesinin (1) numaralı fıkrasının (a) bendinde yer alan "Veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır." hükmüne aykırılık teşkil ettiği kanaatine varıldığından, veri sorumlusu hakkında 6698 sayılı Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 300.000 TL idari para cezası uygulanmasına,

- Veri sorumlularınca hukuka aykırı kişisel veri işleme faaliyetinde bulunduğundan bahisle ilgili kişiler tarafından öne sürülebilecek maddi ve/veya manevi tazminat talepleri için adli makamlar nezdinde girişimde bulunulabileceği konusunda ilgili kişilerin bilgilendirilmesine

karar verilmiştir.

2021/1214 sayılı KVKK Kararı

Bir üniversite tarafından verilen eğitimde, eğitim alan kişilerin kişisel verilerini içeren yoklama listesinin diğer katılımcılar tarafından görülebilir şekilde düzenlenmesi hakkında Kişisel Verileri Koruma Kurulunun 02/12/2021 tarihli ve 2021/1214 sayılı Karar Özeti

Karar Tarihi : 02/12/2021

Karar No : 2021/1214

Konu Özeti : Bir üniversite tarafından verilen eğitimde eğitim alan kişilerin kişisel verilerini içeren yoklama listesinin diğer katılımcılar tarafından görülebilir şekilde düzenlenmesi

Kuruma intikal eden şikâyet dilekçesinde özetle; ilgili kişinin Bakanlık tarafından eğitim verilmesi için görevlendirilen bir Üniversite Eğitim Merkezinin eğitim programına katıldığı, eğitim süresince kursiyerlerin isimlerinin ve T.C. kimlik numaralarının yer aldığı yoklama listelerinin elden elde dolaştırılarak imzalandığı, ayrıca Üniversite ve Bakanlık tarafından kişisel verilerin işlenmesine dair ilgili kişiye aydınlatma yapılmadığı, konuyla ilgili Bakanlığa ve Üniversiteye ayrı ayrı başvuruda bulunduğu, Bakanlığın başvuruya cevap vermediği, Üniversitenin cevabında ise yoklama listelerinin Bakanlık tarafından hazırlandığı ve imza alınmasının yükümlülükleri olduğunun ifade edildiği belirtilerek veri sorumlusu Bakanlık ve Üniversite hakkında 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gerekli idari yaptırımların uygulanması talep edilmiştir.

Şikâyete ilişkin başlatılan inceleme çerçevesinde Bakanlıktan ve Üniversiteden konuya ilişkin bilgi ve belge talep edilmiş olup Bakanlık tarafından verilen cevapta özetle;

- olarak görevlendirilecek kişilerin görevlerine başlamadan önce eğitim almalarının ve görev yaptıkları sürece eğitime tabi tutulmalarının sağlanacağına ilgili mevzuatta hüküm altına alındığı, şikâyet konusu olan eğitimin, üniversiteler tarafından verildiği, Bakanlık Genel Müdürlüğünün şartları haiz eğitim kuruluşlarına mevzuat uyarınca eğitim izni verdiği, dolayısıyla eğitim faaliyeti ve eğitimin düzenine ilişkin hususların eğitim kuruluşları tarafından yerine getirildiği, Bakanlık ile eğitim kuruluşları arasındaki ilişkinin ilgili yönetmelik hükümleri ile belirlendiği,

- Konuya ilişkin mevzuatta ancak eğitimini tamamlayanların mesleki sicile kayıt olabilmeleri için yazılı sınavda başarılı olmaları gerektiğinin düzenlendiği,
 - Eğitimlerinin etkin ve mevzuata uygun bir şekilde gerçekleştirilmesinin sağlanması amacıyla, ilgili mevzuat kapsamında, eğitim programlarının takibi, koordinasyonu ve denetimi için eğitim yönetim sistemi adlı bir yönetim paneli oluşturulduğu, eğitim kuruluşlarının, eğitimlerini mevzuatın gerektirdiği yükümlülüklerle uygun bir şekilde gerçekleştirmek durumunda olduğu,
- Bakanlığın söz konusu hususa ilişkin olarak, veri sorumlusu sıfatı ile sorumluluğunun bulunmadığı,
- İlgili Yönetmelik kapsamında eğitime katılanların, belgeye dayalı ve eğitim kuruluşlarınca kabul edilen haklı bir mazeretleri olmadıkça eğitim süresince verilen ders ve çalışmalara katılımlarının zorunlu olduğu ve adayın eğitimi başarıyla tamamlamasının, mevzuatta öngörülen sürede eğitime katılmış olması şartını sağlamasına bağlı olduğu,
 - Eğitiminin başarıyla tamamlanmasının, sınav ve sicile kayıt başvurusu için bir ön şart olduğu,
 - Sınav başvurusu ve şekline ilişkin usul ve esasların düzenlendiği Yönetmeliğin ilgili maddesi uyarınca ilgililer tarafından sınav müracaatında bulunulurken başvuruya T.C. kimlik numarası ve eğitimini tamamladığını gösteren katılım belgesi ile mezuniyet belgesi asılları veya onaylı suretlerinin eklenmesi gerektiğinin hüküm altına alındığı, bu çerçevede ilgilinin yazılı sınava girebilme hakkını taşıyıp taşımadığının Bakanlık tarafından incelendiği, başka bir ifade ile sınav başvurusunun adayın eğitimi başarıyla tamamlayıp tamamlamadığı ve öğrenim yönünden sınava girebilme şartlarını haiz olup olmadığı açısından değerlendirildiği,
 - Katılım belgesinin ise eğitimlerini başarı ile tamamlayan kişilere, eğitim kuruluşları tarafından düzenlenerek verildiği, Bakanlık tarafından, adayın, eğitimi başarıyla tamamlayıp tamamlamadığının ibraz ettiği bu katılım belgesi incelenerek denetlendiği, devam zorunluluğunu takip etme, aksi durumda eğitim programı ile ilişkisini kesme yükümlülüğünün ise Bakanlığa değil, eğitim kuruluşuna ait olduğu, bu nedenle ilgili mevzuat kapsamında adayların derslere devam durumunu gösteren çizelgenin eğitim kuruluşlarınca düzenlenmesi gerektiğinin hüküm altına alındığı,
 - Bakanlık tarafından sınava ve sicile başvuru esnasında devam çizelgesinin değil katılım belgesinin denetlendiği, ileride adayın devam durumuna ilişkin bir itirazının bulunması veya Bakanlığın aleyhine dava açılması ihtimallerine binaen, devam çizelgesinin bir örneğinin Bakanlığa gönderildiği, aslının ise eğitim kuruluşunda saklandığı, dolayısıyla devam çizelgesinin, sınav ve sicil başvurusu

esnasında adayın eğitimini başarıyla tamamladığını gösteren ve Bakanlık tarafından incelemesi yapılan katılım belgesine dayanak teşkil eden bir belge niteliğinde olduğu,

- Diğer yandan, ilgili kişinin Eğitim Merkezinin ilgili eğitim biriminin yoklama listelerini Bakanlık tarafından hazırlanan sistemden aldığı yönünde cevap verdiğine ilişkin beyanıyla ilgili olarak ise; Bakanlık tarafından eğitim kuruluşlarına adaylara ilişkin devam çizelgelerinin T.C. kimlik numaralarıyla birlikte imzalatılması ve sonrasında Bakanlığa gönderilmesi yönünde bir bildirimde bulunulmadığı gibi, hali hazırda devam çizelgesi hazırlama yükümlülüğünün de eğitim kuruluşunda olduğu, eğitim yönetim sistemi panelinde çıkan listede yer alan T.C. kimlik numaralarına, bir grupta aynı ad ve soyadında birden fazla adayın bulunması halinde çıkabilecek ihtilafın önlenmesi amacıyla yer verildiği, eğitim kuruluşlarının ilgili mevzuatta öngörülen devam çizelgesini düzenlemeyip, eğitim yönetim sisteminde yer alan listeyi kullanmak istemesi durumunda ise çizelgeyi, gerekirse T.C. kimlik numaralarını çıkartmak veya elden ele dolaştırmayarak, adayın eğitmenin yanına gelerek imzasını atmasını sağlamak gibi yöntemlerle ikmal edebileceğinin izahından varestede olduğu,

- Öte yandan, ilgili kişinin Bakanlığa yaptığı başvurusuna Bakanlık tarafından cevap verildiği, ilgili kişinin başvurusuna cevap verilmediğine yönelik iddiasının gerçeği yansıtmadığı

ifade edilmiştir.

Üniversite tarafından verilen cevapta ise özetle;

- Merkez bünyesinde eğitim alan katılımcıların kişisel verilerinin, Kanun'un 5'inci maddesinin (1) ve (2) numaralı fıkralarında yer alan maddelere dayanılarak işlendiği,

- Kişisel Verilerin Korunması Kanunu'nun 10'uncu maddesi ve tebliğ hükümleri gereğince kişisel verilerin işlenmesi sürecine ilişkin olarak, Sürekli Eğitim Merkezinde eğitim öncesinde diğer tüm katılımcılar gibi ilgili kişiyle de, Sözleşme imzalandığı, ilgili mevzuat çerçevesinde katılımcıların devam durumlarını takip etmek üzere yoklama alma zorunluluğu bulunduğu, katılımcıların bu hususları kabul ederek eğitime katıldığı,

- Yoklama listelerinin tamamının sınıf içerisinde ve her bir dersin sorumlu öğretim elemanının kontrolünde katılımcılara imzalatıldığı, yoklama listelerinin imzalatılmasının katılımcıların eğitime devam durumlarının kayıt altına alınabilmesi için kendilerinin hukuki yükümlülüğü olduğu,

- Kişisel Verilerin Korunması Kanunu'nun 12'nci maddesi çerçevesinde Merkezin söz konusu eğitime ve katılımcılarına ilişkin bilgi ve belgeleri belirli yöntemlerle topladığı, uhdesinde güvenli olarak sakladığı ve Bakanlık dışında hiçbir şekilde üçüncü kişilerle paylaşmadığı

ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde, Kişisel Verileri Koruma Kurulu'nun 02/12/2021 tarihli ve 2021/1214 sayılı Kararı ile;

- Kanun'un "Tanımlar" başlıklı 3'üncü maddesinde veri sorumlusu ve veri işleyen tanımlarına yer verilmekte olup "veri sorumlusu"nun kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlandığı,
- Şikâyete konu olan eğitimin, üniversiteler tarafından verilebildiği ve bu eğitimin verilmesi sürecinde Bakanlığın izin, takip, koordinasyon ve denetim yönünden yetkili olduğu, eğitim faaliyeti ve eğitimin düzenine ilişkin hususların ise izin verilen eğitim kuruluşları tarafından belirlendiği ve yerine getirildiği, aynı zamanda bu hususlara ilişkin Bakanlık ile eğitim kuruluşları arasındaki ilişkinin yönetmelik hükümleri ile belirlendiği anlaşıldığından şikâyete konu olay çerçevesinde; Bakanlık ve Üniversitenin kişisel veri işleme faaliyeti alanları kapsamında ayrı ayrı veri sorumlusu olarak faaliyette bulunduğu,
- Kanun'un "Veri Sorumlusuna Başvuru" başlıklı 13'üncü maddesinde " (1) İlgili kişi, bu Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir.(2) Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır... (3) Veri sorumlusu talebi kabul eder veya gerekçesini açıklayarak reddeder ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir..." hükmünün yer aldığı,
- Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in (Tebliğ) "Başvuru Usulü" başlıklı 5'inci maddesinde, ilgili kişinin Kanun'un 11'inci maddesinde belirtilen hakları kapsamında taleplerini yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletceği ve Tebliğ'in 6'ncı maddesinde veri sorumlusunun bu tebliğ kapsamında yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlü olduğu, veri sorumlusunun başvuruyu kabul edeceği veya gerekçesini açıklayarak reddedeceği ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildireceğinin hüküm altına alındığı,

- Üniversite tarafından ilgili kişinin başvurusuna cevap verildiği, fakat Bakanlık tarafından ilgili kişinin başvurusuna verilen cevabın Kanun'un 13'üncü maddesi uyarınca veri sorumlularına tanınan 30 günlük süre aşıldıktan sonra gerçekleştirildiğinin tespit edildiği,

- Diğer taraftan, ilgili kişinin şikâyetinin temel olarak ad, soyad ve T.C. kimlik numarasının bulunduğu devam çizelgesinin ve fatura teslim ve sertifika teslim listelerinin sınıf ortamında elden ele dolaştırılması suretiyle imza alınması nedeniyle T.C. kimlik numarası bilgisinin hukuka aykırı olarak üçüncü kişilerle paylaşıldığı, dolayısıyla kişisel verilerinin güvenliğinin sağlanmadığına ilişkin olduğu,

- 6698 sayılı Kanunun "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin;

"(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması."

hükmünü amir olduğu,

- Bu kapsamda ilgili kişinin eğitim hakkının gereği gibi yerine getirilmesi ve eğitim sürecinin gerekliliklerinin yerine getirilmesini teminen ilgili kişinin kişisel verilerinin işlenmesine ilişkin hukuki zemin irdelendiğinde; Bakanlığın söz konusu eğitim, sınav, görev ve sorumluluklar, denetim, eğitim verecek kişi, kurum ve kuruluşların nitelikleri ve denetimleri ile sicili, eğitim kurumlarının listelerinin düzenlenmesi, gibi hususlarda ilgili Kanun ile görevlendirildiğinin anlaşıldığı, bu

kapsamda ilgili Kanun ile görevlendirilen veri sorumlusu Bakanlığın, 6698 sayılı Kanununun 5'inci maddesinin (2) numaralı fıkrasının (a) bendinde düzenlenen "Kanunlarda açıkça öngörülmesi" ve (ç) bendinde düzenlenen "Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" hükmü çerçevesinde kişisel veri işleme faaliyetinde bulunduğu değerlendirildiği,

- Öte yandan, veri sorumlusu Üniversitenin ilgili Yönetmelikle kendisinden beklenen yükümlülüklerinin ve eğitim sürecinin gerekliliklerinin yerine getirilmesini teminen ilgili kişinin kişisel verilerini Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (ç) bendinde düzenlenen "Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" hükmü ile (e) bendinde düzenlenen "Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" hükmü çerçevesinde işlediği,

- Diğer taraftan Kanunun "Genel İlkeler" başlıklı 4 üncü maddesinde kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, bu çerçevede kişisel verilerin ancak,

a) Hukuka ve dürüstlük kurallarına uygun şekilde,

b) Belirli, açık ve meşru amaçlar kapsamında,

c) Doğru ve gerektiğinde güncel olma şartıyla,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme

ilkelerine uygun olarak işlenebileceğinin belirlendiği, "işlendikleri amaçla bağlantılı ve sınırlı olma ilkesi" uyarınca, işlenen kişisel verilerin belirlenen amaçların gerçekleştirilebilmesine elverişli olmasının, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirdiği, kişisel verilerin açıkça yer almasının zorunluluk teşkil etmemesi halinde veri işlenirken maskeleyme, anonimleştirme gibi yöntemlerin kullanılması gerektiği,

- Şikâyet konusu hakkında veri sorumlularından alınan bilgi ve belgeler ilgili mevzuat kapsamında değerlendirildiğinde, kullanılan devam takip çizelgesinde aynı ad ve soyadı bilgisine sahip kişilerin olması gibi durumlarda karışıklığın önlenmesini teminen, kişilerin ad ve soyadı bilgisinin yanı sıra kişiyi belirleyici kılan başka bir verinin (örneğin T.C. kimlik numarasının) kullanılmasının gerekmesi halinde ilgili verinin maskelenerek kullanılması gerektiği,

• Ayrıca Kanun'un "Veri sorumlusunun aydınlatma yükümlülüğü" başlıklı 10'uncu maddesinin; "(1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; a) Veri sorumlusunun ve varsa temsilcisinin kimliği, b) Kişisel verilerin hangi amaçla işleneceği, c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi, d) 11 inci maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür." hükmünü haiz olduğu,

• "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ"de (Aydınlatma Tebliği) de veri sorumluları veya yetkilendirdiği kişiler tarafından aydınlatma yükümlülüğü kapsamında uyulacak usul ve esasların belirlendiği, Aydınlatma Tebliği'nin 5'inci maddesinin (1) numaralı fıkrasının (a) bendinde ilgili kişinin açık rızasına veya Kanundaki diğer işleme şartlarına bağlı olarak kişisel veri işlendiği her durumda aydınlatma yükümlülüğünün yerine getirilmesi gerektiği; (d) bendinde aydınlatma yükümlülüğünün yerine getirilmesinin ilgili kişinin talebine bağlı olmadığı ve (e) bendinde aydınlatma yükümlülüğünün yerine getirildiğinin ispatının veri sorumlusuna ait olduğunun belirtildiği,

• Tebliğ'in "Aydınlatma yükümlülüğünün kapsamı" başlıklı 4'üncü maddesinde Kanun'un 10'uncu maddesine göre; kişisel verilerin elde edilmesi sırasında veri sorumluları veya yetkilendirdiği kişilerce, ilgili kişilerin bilgilendirilmesi gerektiği belirtilmiş ve bu yükümlülük yerine getirilirken veri sorumluları veya yetkilendirdiği kişilerce yapılacak bilgilendirmenin asgari olarak veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, kişisel verilerin kimlere ve hangi amaçla aktarılacağı, kişisel veri toplamanın yöntemi ve hukuki sebebi ve ilgili kişinin Kanununun 11 inci maddesinde sayılan diğer hakları konularını içermesi gerektiğinin ifade edildiği,

• Konuya ilişkin olarak Üniversiteden alınan yazıda; Kişisel Verilerin Korunması Kanunu'nun 10'uncu maddesi ve Tebliğ hükümleri gereğince kişisel verilerin işlenmesi sürecine ilişkin olarak, Sürekli Eğitim Merkezinde eğitim öncesinde diğer tüm katılımcılar gibi ilgili kişiyle de, sözleşme imzalandığının ifade edildiği, söz konusu sözleşme ile veri sorumlusu tarafından aydınlatma yükümlülüğünün gereği gibi yerine getirilip getirilmediği incelendiğinde; anılan sözleşmede aydınlatma yükümlülüğünün gereği gibi yerine getirilmesini sağlayıcı nitelikteki asgari unsurlar olan; kişisel verilerin hangi amaçla işleneceği, kimlere ve hangi amaçla aktarılacağı, kişisel veri toplamanın yöntemi ve hukuki sebebi ve ilgili kişinin diğer haklarına ilişkin bilgilendirmelere yer verilmediği görüldüğünden veri sorumlusu tarafından aydınlatma yükümlülüğünün gereği gibi yerine getirilmediği sonucuna varıldığı

değerlendirmelerinden hareketle;

- Bakanlık tarafından ilgili kişinin başvurusuna 30 günlük süreden sonra yanıt verildiği anlaşıldığından Kanun'un 13'üncü maddesi çerçevesinde yapılan başvurulara yanıt verilirken 30 günlük sürenin gözetilmesi yönünde hatırlatmada bulunulmasına,
- Veri sorumlusu Üniversite tarafından devam takibine yönelik hukuki yükümlülük yerine getirilirken kullanılan devam takip çizelgesinde kişilerin ad ve soyadı dışında kişiyi belirleyici başka bir veriye (T.C. kimlik numarası) yer verilmesinin gerekmesi halinde; ilgili verinin maskelenmesi bu kapsamda devam takip çizelgesinin tekrar gözden geçirilerek uygulamaya geçirilmesi yönünde veri sorumlusu Üniversitenin talimatlandırılmasına ve sonucundan Kurula bilgi verilmesine,
- İlgili eğitimi veren başka kuruluşların bulunduğu ve benzer uygulamaların söz konusu olabileceği hususları dikkate alındığında, bu eğitimi veren diğer eğitim kuruluşlarına da konu hakkında bilgi verilmesi yönünde Bakanlığa bilgilendirmede bulunulmasına,
- Kanun'un 15'inci maddesinin (5) numaralı fıkrası çerçevesinde; veri sorumlusu Üniversiteye eğitim verilirken kursiyerlere ait kişisel verilerin işlenmesi sürecinde Kanun'un "Veri sorumlusunun aydınlatma yükümlülüğü" başlıklı 10'uncu maddesi ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'de yer verilen hükümlere uygun olacak şekilde bir uygulama geliştirmesi ve bu hususa ilişkin olarak Kurula bilgi verilmesi yönünde talimat verilmesine

karar verilmiştir.

2021/1210 sayılı KVKK Kararı

İlgili kişinin kişisel verisi niteliğindeki cep telefonu numarasının, Digiturk kampanyaları hakkında bilgilendirmede bulunmak amacıyla aranması ve SMS gönderilmesi suretiyle işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 02/12/2021 tarih ve 2021/1210 sayılı Karar Özeti

Karar Tarihi : 02.12.2021

Karar No : 2021/1210

Konu Özeti : İlgili kişinin kişisel verisi niteliğindeki cep telefonu numarasının, Digiturk kampanyaları hakkında bilgilendirmede bulunmak amacıyla aranması ve SMS gönderilmesi suretiyle işlenmesi hakkında

İlgili kişinin Kuruma intikal eden şikâyetinde özetle; kullanmakta olduğu cep telefonu numarasına 0850 *** ** 77, 0216 *** ** 70 ve 0850 *** ** 15 numaralarından farklı tarihlerde aramalar gerçekleştirilerek Digiturk kampanyaları hakkında bilgilendirmede bulunulduğu, yapılan aramalarda kendilerinin Digiturk bayisi olunduğunun belirtildiği, akabinde Digiturk hizmetlerinin reklam ve pazarlamasının yapılması amacıyla 0850 *** ** 82 numaralı telefon üzerinden ilgili kişiye SMS gönderildiği, ancak iletişim bilgilerinin ticari elektronik ileti gönderilmesi suretiyle işlenmesi hususunda açık rızasının bulunmadığı, bu anlamda herhangi bir işleme şartına dayanmaksızın kişisel verilerinin hukuka aykırı olarak işlendiği, adı geçen Şirket'e 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 11 inci maddesindeki hakları kapsamında başvuruda bulunduğu, bu başvuruya karşılık verilen cevapta ilgili kişinin Şirket nezdinde abonelik kaydının bulunmaması nedeniyle ilgili kişinin herhangi bir kişisel verisinin sistemlerinde yer almadığı, söz konusu ticari iletilerin kendileri tarafından gönderilmediği ve başvuruda belirtilen telefon numaralarının Şirket'lerine ait olmadığı yönünde bilgi verildiği belirtilerek konu ile ilgili gerekli incelemenin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde konunun Digiturk'ü ilgilendiren boyutu dikkate alınarak Krea İçerik Hizmetleri ve Prodüksiyon Anonim Şirketi'nden (Krea İçerik Hizmetleri) savunması istenilmiş olup alınan cevabi yazıda özetle;

- Şirket nezdinde ilgili kişinin abonelik kaydının bulunmadığı ve ilgili kişinin Şirket'e yaptığı başvurudan önce Şirket sistemlerinde ilgili kişiye ait herhangi bir kişisel verinin yer almadığı,

- İlgili kişinin başvurusunda belirtilen telefon numaralarının Şirket'e ait olmadığı ve söz konusu aramalar ile SMS gönderimlerinin Şirket tarafından gerçekleştirilmediği,
- Söz konusu telefon numaralarının Şirket bayilerinden birine ait olup olmadığının tespit edilemediği, zira bayilerin Şirket'ten bağımsız şekilde telefon numaraları elde etmiş olabilecekleri,
- Şirket ürün ve hizmetlerinin son kullanıcılara satışının bir kısmına aracılık eden bayilerin tüm pazarlama süreçlerinde Şirket'ten bağımsız şekilde ayrı birer veri sorumlusu sıfatı ile hareket ettikleri, Şirket'ten herhangi bir emir veya talimat almadıkları ve bu konuda Şirket tarafından herhangi bir yönlendirmede bulunulmadığı, bu aramalar üzerinde Şirket'in herhangi bir denetim imkânının bulunmadığı ve dolayısıyla şikâyete konu olayda Şirket'in veri sorumlusu olarak hareket etmediği,
- Şirket tarafından bayilere mevcut ya da potansiyel müşterilere ilişkin herhangi bir kişisel veri aktarılmadığı ve ürünlerin pazarlanması amacıyla iletişim bilgisi listeleri sağlanması gibi uygulamaların söz konusu olmadığı

ifade edilmiş ve ilgili kişiye yapılan aramada belirtilen bayinin (Bayi) Şirket sisteminde hangi unvanla kayıtlı bulunduğu bilgisi Kurumumuzla paylaşılmıştır.

Krea İçerik Hizmetleri'nden alınan cevabi yazının incelenmesinin ardından, ilgili kişinin başvurusunda belirtilen telefon hatlarını tahsis eden işletmeciler tespit edilmiş ve söz konusu telefon hatlarının hangi kişi/şirketlere tahsis edildiği ile bu kapsamda yapılan sözleşmenin içeriği hususlarında bahse konu işletmecilerden bilgi ve belge talep edilmiştir. İlgili işletmecilerden alınan cevabi yazıların incelenmesi neticesinde, 0850 *** ** 77 numaralı hattın Krea İçerik Hizmetleri'nin cevabi yazısında da unvanı belirtilen Bayi'ye, 0216 *** ** 70 ve 0850 *** ** 15 numaralı hatların M.D. isimli şahsa (M. İletişim); 0850 *** ** 82 numaralı hattın ise M.A. isimli şahsa tahsis edildiği anlaşılmıştır.

İnceleme sürecinde ulaşılan bilgiler çerçevesinde, telefon hatlarının tahsis edildiği kişilerden şikâyet konusu olaya ilişkin savunmaları talep edilmiş olup bu kapsamda Bayi'den alınan cevabi yazıda özetle;

- Kendilerinin Krea İçerik Hizmetleri'nin bayisi olduğu,
- İlgili kişinin rızası olmaksızın aranmasının Şirket'in operatör-çağrı merkezi bölümünü ilgilendirdiği ve operatör hizmetinin M.D. isimli şahsa (M. İletişim) devredildiği,

- Taşeronun numaraları nasıl temin ettiği, görüşme içerikleri ve ilgili kişiye yönelik aramalar gerçekleştirip gerçekleştirmediği hususlarında bilgi sahibi olunmadığı ve bu konudaki tüm sorumluluğun taşeron firmaya ait olduğu

belirtilmiş ve taşeron M.D. (M.İletişim) ile aralarındaki taşeronluk sözleşmesi gönderilmiştir.

İşletmeciler ile yapılan yazışmalardan, 0216 *** ** 70 ve 0850 *** ** 15 numaralı hatların kendisine tahsis edildiği görülen ve Bayi'nin cevabi yazısından da Bayi'nin taşeronu olduğu anlaşılan M.D. isimli şahıstan (M.İletişim) alınan cevabi yazıda özetle;

- Krea İçerik Hizmetleri'nin söz konusu bayisine taşeron çağrı merkezi hizmeti verilmekte olduğu,
- İlgili kişinin telefon numarasına reklam ve tanıtım amaçlı arama yapıldığı,
- Sistemlerinde kayıtlı olan verilerin 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunun yürürlük tarihinden önce numara türetme yöntemiyle elde edilmiş olduğu,
- Şikâyete konu olayın 6698 sayılı Kanun kapsamı dışında olduğu ve 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun çerçevesinde değerlendirilmesi gerektiği

ifade edilmiştir.

M.A isimli şahıstan alınan cevabi yazıda ise özetle;

- Bazı dönemlerde sosyal medya hesapları üzerinden verilen reklamların, kişilerin sosyal medya hesaplarında karşılıklarına çıktığı ve bu kapsamda kendi istekleri ile form doldurmalarının ardından kendilerine kampanya duyurusu yapıldığı,
- İlgili kişinin bir internet sitesi üzerinden doldurduğu formun ekte sunulduğu

belirtilmiş ve kişilere arama yapılmasında kullanılan sistemin çalışma şekline ilişkin bilgi verilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulunun 02/12/2021 tarih ve 2021/1210 sayılı Kararı ile;

- Kanununun 3 üncü maddesinin (1) numaralı fıkrasının (1) bendinde veri sorumlusunun, *“kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi”*; (ğ) bendinde ise veri işleyenin, *“veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi”* şeklinde tanımlandığı; Kişisel Verileri Koruma Kurumu tarafından yayınlanan *“Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi”*nde söz konusu kavramların açıklandığı bölümde, veri işleyenin faaliyetlerinin veri işlemenin daha çok teknik kısımları ile sınırlı olduğunun, veri sorumlusunun ise kişisel verilerin

işlenmesine ilişkin karar alma yetkisine sahip olduğunun ve kişisel veri işleme faaliyetinin “neden” ve “nasıl” yapılacağını belirlediğinin ifade edildiği; bu kapsamda “*kişisel verilerin toplanması ve toplama yöntemi*”, “*toplanacak kişisel veri türleri*”, “*toplanan verilerin hangi amaçlarla kullanılacağı*”, “*hangi bireylerin kişisel verilerinin toplanacağı*”, “*toplanan verilerin paylaşılıp paylaşılmayacağı, paylaşılacaksa kiminle paylaşılacağı*” ve “*verilerin ne kadar süreyle saklanacağı*” gibi hususlara ilişkin karar alma yetkisinin kimde bulunduğu veri sorumlusunun tespitinde önem taşıdığı,

- Krea İçerik Hizmetleri ile Bayi arasındaki ilişkiye yönelik olarak bir değerlendirme yapıldığında, ilgili kişinin kişisel verisinin işlenmesi faaliyetine ilişkin karar alma ve talimat verme yetkisinin Krea İçerik Hizmetleri’nde bulunduğu durumda Krea İçerik Hizmetleri’nin veri sorumlusu, kendisine verilen talimatlar çerçevesinde hareket eden Bayi’nin ise veri işleyen sıfatını haiz olacağının düşünülebileceği; ancak konuya ilişkin olarak tarafların Kuruma sundukları beyanlar değerlendirildiğinde Krea İçerik Hizmetleri’nin somut olayda veri sorumlusu olarak hareket ettiğine dair bir tespit bulunamadığı,

- Öte yandan Bayi ile taşeronu M.D. (M. İletişim) arasındaki taşeronluk sözleşmesi incelendiğinde, Bayi nezdinde kayıtlı olan 0850 *** ** 77 numaralı hattın kullanımı için taşeron firmanın yetkilendirildiği, bu hattın kullanımı ile ilişkili sorumluluğun taşeronu bırakıldığı ve sözleşmenin içeriğinde taşeronun Bayi’nin verdiği talimatlar çerçevesinde faaliyette bulunduğunu gösterir nitelikte hükümlerin yer almadığı görüldüğünden, şikâyete konu olayda Bayi’nin veri sorumlusu olarak nitelendirilebileceğine yönelik bir tespit bulunamadığı,

- Diğer taraftan inceleme sürecinde ulaşılan bilgiler arasında, 0216 *** ** 70 ve 0850 *** ** 15 numaralı hatların somut olayda taşeron M.D. isimli şahsa (M. İletişim) tahsis edildiği bilgisinin bulunduğu, mevcut bilgi ve belgelerden söz konusu iki numaranın Bayi ile olan alt işveren ilişkisinden bağımsız olarak M.D. tarafından kullanılmakta olduğu sonucuna ulaşıldığı, ilgili kişinin söz konusu numaralar üzerinden kendisine arama yapıldığını belirttiği tarihler ile M.D. isimli şahsın (M. İletişim) savunmasında sunulan tarihlerin uyduğu ve sisteminde kayıtlı telefon numaralarının “numara türetme yöntemi” ile elde edilmiş olduğunun beyan edildiği,

- Bu kapsamda M.D.’nin (M. İletişim) söz konusu aramalara ilişkin olarak başka kişilerce talimatlandırıldığını gösteren bir bilgi ve belgenin mevcut olmadığı, irtibata geçilecek kişileri belirleme konusunda yetkinin kendisinde bulunduğu, kendi inisiyatifi ile numara türetmek suretiyle ilgili kişinin telefon numarası verisine ulaştığı ve işletmesinin 6102 sayılı Türk Ticaret Kanunu kapsamında tüzel kişiliği bulunmadığından hareketle M.D.’nin somut olayda veri sorumlusu sıfatını haiz olduğu,

- 0850 *** ** 82 numaralı hattın tahsis edildiği M.A. açısından bir değerlendirme yapıldığında ise M.A.'nın, ilgili kişinin bir internet sitesi üzerinden doldurduğunu iddia ettiği formu sunduğu, kendi veri tabanını oluşturan ve bu veri tabanını kullanmak suretiyle ilgili kişinin kişisel verisi olan telefon numarasını işleyerek kendisine ticari elektronik ileti gönderimi yapan M.A.'nın somut olay kapsamında veri sorumlusu sıfatını haiz olduğu,
- İlgili kişinin kişisel verisi niteliğindeki cep telefonu numarasının, ürün tanıtımı ve pazarlama yapılması amacıyla aranması /SMS gönderilmesi suretiyle işlenmesi, Kanunun 3 üncü maddesi uyarınca kişisel veri işleme faaliyeti teşkil ettiğinden bu işlemenin hukuka uygun şekilde gerçekleştirildiğinden bahsedebilmek için Kanunun 5 inci maddesinde sayılan şartlardan birinin bulunması gerektiği,
- Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin; (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi; fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin kendisi tarafından alenileştirilmiş olması; bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğunun düzenlendiği,
- Şikâyete konu kişisel veri işleme faaliyetinde veri sorumlularından biri olduğu değerlendirilen M.D. (M. İletişim) tarafından, somut olayın 6698 sayılı Kanunun kapsamı dışında olduğu ve 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun çerçevesinde ele alınması gerektiği iddia edilmekle birlikte ticari elektronik iletilerin gönderilmesi için kullanılan iletişim kanallarının kişisel veri niteliğinde olması nedeniyle ileti gönderim sürecinin kişisel verilerin korunmasına ilişkin mevzuata da uygun olmasının beklendiği ve M.D.'nin (M. İletişim) sisteminde kayıtlı verilerin numara türetme yöntemi ile elde edildiğine yönelik beyanı esas alındığında ilgili kişinin telefon numarasının işlenmesinde Kanunun 5 inci maddesinde yer alan herhangi bir işleme şartına dayanılmadığının anlaşıldığı,

- Şikâyete konu olayda diğere veri sorumlusu olduđu sonucuna varılan M.A. isimli şahsın kişisel veri işleme faaliyeti açısından bir değerlendirme yapıldığında ise ilgili kişinin bir internet sitesi üzerinden doldurduğu iddia edilen formun geçerliliğinin sorgulanmaya muhtaç olduğu, zira ilgili formun internet sitesinde gösterilen biçimde ve log kaydı veya benzeri bir formatta Kuruma sunulmadığı, bunun yerine ilgili kişinin cep telefonu numarasının ve başvuru tarihinin M.A.'nın el yazısı ile yazıldığı, "onay veriyorum" kutucuğunun işaretlendiği ve formun M.A.'nın ismi ve telefon numarası yazılarak yine M.A.'nın kendisi tarafından imzalandığı görüldüğünden M.A.'nın iddia ettiği üzere formun ilgili kişi tarafından doldurulduğuna yönelik yeterli kanaatin oluşmadığı ve sunulan bu formun hukuka uygun bir açık rıza olarak kabul edilemeyeceği

değerlendirmelerinden hareketle,

- Krea İçerik Hizmetleri ve Prodüksiyon Anonim Şirketi ile Bayi'nin somut olayda veri sorumlusu olarak hareket ettiklerine yönelik bir tespitte bulunulamadığından anılan Şirketler hakkında Kanunun 12 nci maddesi kapsamında tesis edilecek bir işlem bulunmadığına,

- İlgili kişinin kişisel verisi niteliğindeki telefon numarasının işlenmesinde Kanunun 5 inci maddesinde yer alan herhangi bir işleme şartına dayanılmadığı, dolayısıyla Kanunun 12 nci maddesinin (1) numaralı fıkrası hükmüne aykırı hareket edildiği kanaatine varıldığından veri sorumlusu M.D. hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında idari yaptırım uygulanmasına,

- Şikâyete konu olayda veri sorumlusu olarak değerlendirilen M.A. isimli şahsın Kuruma sunduğu formun hukuka uygun bir açık rıza olarak kabul edilemeyeceği dikkate alındığında, ilgili kişinin kişisel verisinin işlenmesine ilişkin Kanunun 5 inci maddesinde yer alan herhangi bir işleme şartına dayanmayan veri sorumlusu M.A. hakkında Kanunun 12 nci maddesinde yer alan veri güvenliğine ilişkin yükümlülüklerini yerine getirmemesi nedeniyle Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında idari yaptırım uygulanmasına,

- İlgili kişi tarafından kullanılmakta olan telefon numarası verisinin imha edilmesi ve sonucundan Kurula bilgi verilmesi hususunda M.D. ve M.A.'nın talimatlandırılmasına,

- Öte yandan, yeni müşteri kazandırma süreçlerinde Kanuna uyum hususunda azami dikkat ve özenin gösterilmesi hususunda bayilerini yönlendirmesi/bilgilendirmesi ve bayiler ile yapılacak sözleşmelerde veri sorumlusu ve veri işleyenin kim olduğu hususunda açık hükümlere yer verilmesi hususunda Krea İçerik Hizmetleri ve Prodüksiyon Anonim Şirketi'nin talimatlandırılmasına

karar verilmiştir.

2021/1187 sayılı KVKK Kararı

Veri sorumlusu işveren tarafından eski çalışanı olan ilgili kişinin kurumsal e-posta hesabına aydınlatma yapılmaksızın erişilmesi hakkında Kişisel Verileri Koruma Kurulunun 25/11/2021 tarihli ve 2021/1187 sayılı Karar Özeti

Karar Tarihi : 25/11/2021

Karar No : 2021/1187

Konu Özeti : Veri sorumlusu işveren tarafından eski çalışanı olan ilgili kişinin kurumsal e-posta hesabına aydınlatma yapılmaksızın erişilmesi

İlgili kişinin Kuruma intikal eden şikâyetinde özetle;

- Veri sorumlusu şirketin eski çalışanı olduğu, ilgili kişi ile veri sorumlusunun karşılıklı taraf oldukları dava dosyalarına sunulan delil listeleri içeriğinde, ilgili kişiye ait kişisel veri niteliğinde olan ilgili kişinin nişanlısı ile e-posta üzerinden yapmış olduğu konuşma içeriklerine, şahsi banka hesap dökümlerine ve yaptığı harcama kayıtlarına erişim sağlandığının görüldüğü,
- Veri sorumlusu tarafından, şirket çalışanlarına verilen e-posta adreslerinin sadece iş dolayısıyla kullanılması gerektiğini bildiren herhangi bir açıklama veya bildirim yapılmamış olduğu bu hususa dair denetim kriterlerinin de belirlenmediği, ilgili kişinin özel hayatına ilişkin e-posta içeriklerinin bilinçli bir şekilde kötü niyetli olarak veri sorumlusu tarafından ele geçirildiği,
- İlgili kişinin 16.11.2020 tarihi itibariyle tek taraflı olarak iş akdini feshettiği, buna rağmen işveren sıfatını haiz olmadığı dönem de olmak üzere veri sorumlusu tarafından ilgili kişiye ait kişisel verilerin işlendiği ve üçüncü kişilere aktarıldığı,
- Veri sorumlusu tarafından ilgili kişiye ait kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda (Kanun) öngörülen işleme şartlarına aykırı olarak işlendiği, üçüncü kişilere aktarıldığı, bu hususta ilgili kişiye bir aydınlatma yapılmadığı ve açık rıza metni sunulmadığı,
- Müşterilerinin ve çalışanlarının bilgilerinin muhafaza edildiği, söz konusu kişilerin iş ve işlemlerini gerçekleştirdiği platformun "cloud" olduğu ve söz konusu Cloud'un da Microsoft tarafından sağlanan OneDrive bulut sistemi olduğu, adı geçen hizmet sağlayıcı firmaların "server"larının yurtdışında

bulunuyor olmasından dolayı söz konusu işlemlerin Kanun'un 9'uncu maddesine uygun olarak gerçekleştirilmesi gerektiği,

- İlgili kişinin şirket e-posta hesabının veri sorumlusu tarafından tahsis edilmiş olduğu, bu e-posta hesabına kimlerin erişim sağladığı belirli olmamakla birlikte, veri sorumlusu tarafından sunulan cevabi yazının içeriğinden, söz konusu verilerin şirket hissedarı ve şirket yetkilisi ile diğer bazı işyeri çalışanlarının erişime açık bir halde olduğunun anlaşıldığı,

- Kanun'un 11'inci maddesi kapsamında veri sorumlusuna başvuruda bulunulduğu ve ayrıca Kanun'un 5'inci maddesinin (2) numaralı fıkrası kapsamında işleme şartı haiz olmadan işlenen kişisel verilerinin silindiğini veya yok edildiğini gösterir bilgi ve belgelerin iletilmesinin talep edildiği

ancak veri sorumlusu tarafından verilen cevabın maddi gerçekleri yansıtmadığı ve yetersiz görüldüğü hususları belirtilmiş ve Kanun hükümleri uyarınca gerekli işlemlerin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusunun savunması istenilmiş olup alınan cevabi yazıda özetle;

- İlgili kişi ile veri sorumlusu arasındaki ihtilafın esasen Kanun'dan kaynaklanan bir sorun olmadığı,
- Konunun işyerinde çalışan ve çalıştığı süre boyunca rakip firmalara iş kaydırarak işyerini ciddi şekilde zarar uğrattığı tespit edilen eski bir çalışan ile ciddi şekilde zarara uğrayan işveren arasında karşılıklı suçlama, talep ve davalarla devam etmekte olan hukuki bir ihtilaf olduğu, bu kapsamda ilgili kişi ile veri sorumlusu arasında süregelen sekiz adet dava ve ceza soruşturmasının bulunduğu,
- İlgili kişinin, veri sorumlusu bünyesinde bilişim faaliyetleri alanında teknik nitelikli bir personel olarak çalışmaya başladığı ve iş akdini tek taraflı irade beyanı ile feshettiği,
- İlgili kişiye ait yazışmaların söz konusu yargılama süreçlerine delil olarak sunulması nedeniyle, ilgili kişinin özel hayatını ilgilendiren şahsi e-posta içeriklerine veri sorumlusu tarafından hukuka aykırı olarak erişildiği ve Anayasa ile koruma altına alınan özel hayatın gizliliği ile haberleşme gizliliği hakkının ihlal edildiğinden bahisle veri sorumlusu ve veri sorumlusu şirket yetkilisi hakkında Başsavcılığa şikâyette bulunulduğu, ancak bu şikâyetin yürütülen soruşturma neticesinde kovuşturmayaya yer olmadığına dair karar verilerek reddedildiği,
- İlgili kişiye iş ilişkisi kapsamındaki kurumsal faaliyetlerde ve işin gerektiği ölçüde kullanılmak üzere bir kurumsal e-posta hesabının tahsis edildiği, iş ilişkisi kapsamında çalışana tahsis edilmiş olan kurumsal e-posta hesaplarının sadece işin ifası amacı ile kullanılacağına açık olduğu, bu

nedenle bilişim alanında uzman olarak çalışan bir personelin bu gerekliliğin bilincinde olması gerektiği, bu hususta ilgili kişiye ilave denetim kriterlerinin uygulanmasının hayatın olağan akışına aykırı olacağı ve ilgili kişinin kurumsal e-posta hesabını kullanmaması yönünde uyarılmasına ihtiyaç bulunmadığı,

- Şikâyete konu e-posta hesabının veri sorumlusuna ait olduğu, e-posta hesabının ilgili kişinin ad ve soyadı ile başlasa da veri sorumlusunun ticaret unvanı ile devam eden uzantıya sahip olduğu, veri sorumlusuna ait olan ve sadece iş amacı ile personele verilen e-posta adreslerinin Kanun kapsamında kişisel veri olmadığı,

- İlgili kişinin, tek taraflı olarak iş akdini feshetmesi ile eş zamanlı olarak veri sorumlusu bünyesindeki on iki yıllık ticari işlem geçmişini içeren kurumsal e-posta hesabını da sildiği, ilgili kişinin bu hareketinin veri sorumlusu bünyesinde ciddi bir şüphe uyandırdığı, ilgili kişinin söz konusu silme eylemi üzerine işyeri ile ilgili pek çok müşteri verisi barındıran e-posta hesabının geri getirilmesi durumunda kaldığı,

- Yapılan zorlu mücadelelerle e-posta hesabının geri kazanılması sonrasında oluşan şüphe üzerine ilgili kişinin sadakat yükümlülüğüne tamamen aykırı olarak haksız kazanç elde ettiği hususunun açık ve net şekilde tespit edildiği, geri getirme esnasında amaç ve hedefin ilgili kişinin şahsi verilerinin işlenmesi ya da alenileştirilmesi değil, ticari verilere ulaşmak olduğu,

- Yapılan işlemler esnasında, ilgili kişinin kendi rızasıyla ve bilinçli olarak kaydettiği şahsi nitelikli veri ve yazışmalarının da sunucudan diğer veriler ile birlikte otomatik olarak çekildiği, ilgili kişinin dilemesi halinde nişanlısı ile olan yazışmaları da dâhil olmak üzere özel yazışmalarını silip ticari yazışmaları gelen kutusunda bırakması mümkün iken bu yolu tercih etmeyerek tüm ticari geçmişini sildiği, bu nedenle özel veriler ihtiva eden bağımsız bir klasöre kaydedilmemiş olan ve ticari yazışmalar arasında dağınık halde bulunan verilerin kurumsal e-posta adresinin incelenmesi esnasında iş yazışmaları arasında tesadüfen elde edildiği, dolayısıyla söz konusu olayda ilgili kişinin kendi ihmali ve rızasının bulunduğu,

- Kurumsal e-posta içeriklerinin ilgili kişi tarafından silinmesinin akabinde söz konusu e-posta hesabının geri getirilmesi üzerine tüm verilerin silinmesinin uyandırdığı şüpheye dayalı olarak işe yönelik olduğu düşünülen ve sadece işe yönelik yazışmaların yapılmasının gerektiği ilgili kişi tarafından da malum olan e-posta içeriklerinin, ticari ve itibari açıdan zarara uğrama ihtimali oluşan veri sorumlusunun tek şirket yetkilisi tarafından işveren sıfatı ile incelendiği,

- İşyerinde ve iş saatlerinde söz konusu e-posta hesabı üzerinden özel yazışmaların yapıldığı, ilgili kişinin bu yazışmalarda yer alan verilerin olağan denetim yükümlülüğü kapsamında işverenin erişimine açık olabileceğini göz önünde bulundurması gerektiği, bu yüzden yapılacak yorumda ilgili kişinin söz konusu yazışmaları işleme ve kaydetme hususunda işverene açık rıza verdiğinin kabul edileceği, zira söz konusu verilerin ilgili kişinin kendisi tarafından alenileştirilmiş vaziyette olduğu,
- Şikâyete konu verilerin tamamına yakınının hâlihazırda ilgili kişi tarafından ikame olunan hizmet tespiti davasında bizzat ilgili kişi tarafından delil olarak sunulduğu ve alenileştirildiği, veri sorumlusu tarafından da bahse konu e-posta hesabındaki yazışmaların yalnızca iddia konusu olan zarar verici eylemlerin ispatı maksadı ile sınırlı ve ölçülü olmak kaydıyla ilgili Mahkemeye bildirildiği,
- İşveren sıfatına sahip olunmayan dönemde veri sorumlusu tarafından verilerin işlendiği iddiasına ilişkin olarak; söz konusu verilere ilgili kişinin şüpheli davranışı üzerine erişildiği, burada ilgili kişinin temel haklarına yönelik müdahalenin meşru amaca dayalı olduğu, işverenin yönetim yetkisi kapsamında kural olarak işçinin kullanımına sunduğu iletişim araçlarını denetleyebileceği ve kullanıma ilişkin sınırlamalar öngörebileceği, bununla birlikte bahsedilen tarihte iş sözleşmesinin haklı nedenle sona erip ermediğinin şu an için açılmış bulunan iş davasında ayrı bir ihtilaf konusu olduğu ve davanın henüz neticelendirilmediği,
- Verilerin yurt dışına aktarıldığı iddiasına ilişkin olarak; şirketin verilerin muhafazası için Microsoft Office ile çalıştığı, aradaki iş ilişkisi dâhilinde Microsoft Office firmasının geri getirilmiş olan verilerin yalnızca veri sorumlusunun şirket yetkilisiyle paylaşıldığı, başkaca bir aktarım veya verileri yayma durumunun olmadığı,
- İlgili kişinin verilerinin yetkisiz kişi erişimine açıldığı iddiasına ilişkin olarak; taraflarına ulaşan veri sorumlusuna başvuru metninin içeriğinde bu gibi bir iddianın mevcut olmadığı, dolayısıyla bu hususta Kanun kapsamında öncelikle kendilerine başvuru yapılması gerektiği, bununla birlikte söz konusu iddianın gerçeği yansıtmadığı, zira bahsi geçen verilere sadece veri sorumlusunun şirket yetkilisinin erişim sağladığı bu durumun veri sorumlusunun meşru hak ve menfaatlerinin korunmasının tabii bir sonucu olduğu belirtilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde, Kişisel Verileri Koruma Kurulu'nun (Kurul) 25/11/2021 tarihli ve 2021/1187 sayılı Kararı ile;

- Kanun'un amacının kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek olduğu, Kanun'un "Tanımlar" başlıklı 3'üncü maddesinde "ilgili kişi"nin, kişisel verisi işlenen gerçek kişi; "veri sorumlusu"nun ise kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlandığı,

- Kanun'un, kişisel verilerin işlenmesine ilişkin "Genel İlkeler"i düzenleyen 4'üncü maddesinin (1) numaralı fıkrasında, "Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir." hükmünün yer aldığı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin;

a) Hukuka ve dürüstlük kurallarına uygun olma,

b) Doğru ve gerektiğinde güncel olma,

c) Belirli, açık ve meşru amaçlar için işlenme,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanun'un "Veri Güvenliğine İlişkin Yükümlülükler"i düzenleyen 12'nci maddesinin (1) numaralı fıkrasında veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel

verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idarî tedbirleri almak zorunda olduğunun hükme bağlandığı,

- Somut olayda öncelikle söz konusu tarihte ilgili kişi ile veri sorumlusu arasındaki iş akdinin feshedilmiş olup olmadığının değerlendirilmesi gerektiği ama söz konusu hususa ilişkin henüz verilmiş bir mahkeme kararının da bulunmadığının görüldüğü,

- Bununla birlikte, veri sorumlusunun, çalışanlarına tahsis etmiş olduğu e-posta adresinin Kanun kapsamında kişisel veri olmadığı iddiasının Kanun'un 3'üncü maddesi kapsamındaki "kişisel veri" tanımı karşısında geçerli olmadığı, zira yalnızca ilgili kişinin adı, soyadı gibi sadece kimliğini ortaya koyan bilgilerin değil e-posta adresi, özel yazışmaları, şahsi banka hesap dökümleri, harcama kayıtları gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm verilerin de kişisel veri niteliğini haiz olduğu,

- Konu ile ilgili olarak; 17/09/2020 tarihli ve 2016/13010 başvuru numaralı Anayasa Mahkemesi (AYM) Kararı ile;

- "... Anayasa Mahkemesi daha önce iletişim araçlarının işveren tarafından denetlenmesi kapsamındaki uyuşmazlıklarda derece mahkemeleri tarafından devletin pozitif yükümlülükleri bağlamında çıkarların dengelenmesi ve müdahalenin ölçülülüğünün irdelenmesi kapsamında gözetilmesi gereken hususları genel olarak belirlemiş; buna göre somut olayın koşullarına göre iş sözleşmelerinde kısıtlayıcı ve zorlayıcı düzenlemelerin ne şekilde belirlendiği, tarafların bu düzenlemeler hakkında bilgilendirilip bilgilendirilmediği, çalışanların temel haklarına yönelik müdahalede bulunulmasına neden olan meşru amacın müdahale ile ölçülü olup olmadığı, sözleşmenin feshinin çalışanların eylem ya da eylemsizlikleri karşısında makul ve orantılı bir işlem olup olmadığı hususlarının uyuşmazlığın çözümünde gözetilmesi gerektiğini tespit etmiştir.

- ...Öncelikle somut olayda olduğu gibi teknolojik gelişmelerin imkanlarından yararlanmak isteyen işverenlerin bilgisayar, internet, e-posta gibi iletişim araç ve gereçlerini çalışanın kullanıma sunması nedeniyle oluşan uyuşmazlıklarda işverenin menfaatleri ile işçinin temel hak ve özgürlükleri arasında bir dengeleme yapma gerekliliği doğmaktadır.

- ...işyerinde kullanıma sunulan iletişim araçlarının işverene ait olduğu gözetilerek sırf bu nedenle bile işverenin iletişim araçları üzerinde sınırsız ve mutlak bir gözetleme ve denetleme yetkisinin olduğunu kabul etmek, işçinin demokratik bir toplumda temel hak ve özgürlüklerine işyerinde de saygı gösterilmesi gerektiği yönündeki haklı beklentisiyle uyuşmayacaktır.

- ...devletin pozitif yükümlülükleri kapsamında Anayasa Mahkemesinin özellikle derece mahkemelerinin -somut olayın koşullarına uygun düştüğü ölçüde- aşağıda belirtilen güvencelerin somut olayda hakka müdahale eden üçüncü kişi tarafından sağlanıp sağlanmadığını gereği gibi denetleyip denetlemediğini incelemesi gerekir:

i. İşverenin çalışanın kullanımına sunduğu iletişim araçlarının ve iletişim içeriklerinin incelenmesinin haklı olduğunu gösteren meşru gerekçeleri olup olmadığı denetlenmelidir. Bu durumda işverenin gerekçelerinin ifa edilen işin ve işyerinin özellikleri de gözetilerek meşru olup olmadığı irdelenmelidir. Bu denetlemede iletişim akışı ile iletişim içeriklerinin incelenmesi arasında ayırım yapılarak içeriklerin incelenmesi yönünden daha ciddi gerekçeler aranmalıdır.

ii. Demokratik bir toplumda iletişimin denetlenmesi ve kişisel verilerin işlenmesi süreci şeffaf bir şekilde gerçekleştirilmeli ve bunun bir gereği olarak da süreçle ilgili olarak çalışanlar işveren tarafından önceden bilgilendirilmelidir. Uluslararası hukuk ve karşılaştırmalı hukuk dikkate alındığında bu bilgilendirmenin -somut olayın özelliklerine uygun düştüğü ölçüde- en azından iletişimin denetlenmesi ile kişisel verilerin işlenmesinin hukuki dayanağı ve amaçları, denetlemenin ve veri işlemenin kapsamı, verilerin saklanacağı süre, veri sahibinin hakları, denetlemenin ve işlemenin sonuçları ile verilerin muhtemel yararlanıcıları hususlarını kapsaması gerekir. Ayrıca bildirimde iletişim araçlarının kullanımına ilişkin olarak işveren tarafından öngörülen sınırlamalara da yer verilmelidir. Bilgilendirmenin mutlaka belli şekilde yapılması şart olmayıp şeffaflığı sağlamak bakımından bireylere, kişisel verilerin işlenmesine ve iletişimin denetlenmesine ilişkin süreçten yukarıda belirtilen kapsamda haberdar olma imkanı sağlayan uygun bir yöntem tercih edilebilir.

iii. Çalışanın kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine işveren tarafından yapılan müdahale, ulaşılmak istenen amaç ile ilgili ve bu amacı gerçekleştirmeye elverişli olmalıdır. Ayrıca inceleme faaliyetiyle elde edilen verilerin işveren tarafından hedeflenen amaç doğrultusunda kullanılması gerekir.

iv. İşveren tarafından çalışanın kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine işveren tarafından yapılan müdahalenin gerekli kabul edilebilmesi için aynı amaca daha hafif bir müdahale ile ulaşılmaması mümkün olmamalı, müdahale ulaşılmak istenen amaç bakımından zorunlu olmalıdır. Çalışanın iletişiminin içeriğine girilmesi yerine onun kişisel verilerine daha az müdahale eden yöntem ve tedbirlerin uygulanmasının mümkün olup olmadığı denetlenmelidir. Bu kapsamda işverenin ulaşmak istediği amaca çalışanın iletişimi incelenmeden de erişilme imkanı olup olmadığı her bir vakianın somut özellikleri ışığında değerlendirilmelidir.

v. İşveren tarafından başvurucunun kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine yönelik müdahalenin orantılı kabul edilebilmesi için ise iletişimin denetlenmesi ile işlenecek veya herhangi bir şekilde yararlanılacak veriler ulaşılmak istenen amaçla sınırlı olmalı, bu amacı aşacak şekilde sınırlama ya da müdahaleye izin verilmemelidir.

vi. Ayrıca iletişimin incelenmesinin muhatabı olan çalışan üzerindeki etkisi ve çalışan bakımından sonuçları göz önünde tutularak tarafların çatışan menfaat ve haklarının adil bir biçimde dengelenip dengelenmediğine bakılması gerekmektedir...”

12.01.2021 tarihli ve 2018/31036 başvuru numaralı Anayasa Mahkemesi Kararı ile de;

- “...Tüm bu açıklamalar çerçevesinde devletin pozitif yükümlülükleri kapsamında Anayasa Mahkemesinin özellikle derece mahkemelerinin -somut olayın koşullarına uygun düştüğü ölçüde aşağıda belirtilen güvencelerin somut olayda hakka müdahale eden üçüncü kişi tarafından sağlanıp sağlanmadığını gereği gibi denetleyip denetlemediğini incelemesi gerekir:

i. İşverenin çalışanın kullanımına sunduğu iletişim araçlarının ve iletişim içeriklerinin incelenmesinin haklı olduğunu gösteren meşru gerekçeleri olup olmadığı denetlenmelidir. Bu durumda işverenin gerekçelerinin ifa edilen işin ve işyerinin özellikleri de gözetilerek meşru olup olmadığı irdelenmelidir. Bu denetlemede iletişim akışı ile iletişim içeriklerinin incelenmesi arasında ayırım yapılarak içeriklerin incelenmesi yönünden daha ciddi gerekçeler aranmalıdır.

ii. Demokratik bir toplumda iletişimin denetlenmesi ve kişisel verilerin işlenmesi süreci şeffaf bir şekilde gerçekleştirilmeli ve bunun bir gereği olarak da süreçle ilgili olarak çalışanlar işveren tarafından önceden bilgilendirilmelidir. Uluslararası hukuk ve karşılaştırmalı hukuk dikkate alındığında bu bilgilendirmenin -somut olayın özelliklerine uygun düştüğü ölçüde- en azından iletişimin denetlenmesi ile kişisel verilerin işlenmesinin hukuki dayanağı ve amaçları, denetlemenin ve veri işlemenin kapsamı, verilerin saklanacağı süre, veri sahibinin hakları, denetlemenin ve işlemenin sonuçları ile verilerin muhtemel yararlanıcıları hususlarını kapsamaması gerekir. Ayrıca bildirimde iletişim araçlarının kullanımına ilişkin olarak işveren tarafından öngörülen sınırlamalara da yer verilmelidir. Bilgilendirmenin mutlaka belli şekilde yapılması şart olmayıp şeffaflığı sağlamak bakımından bireylere, kişisel verilerin işlenmesine ve iletişimin denetlenmesine ilişkin süreçten yukarıda belirtilen kapsamda haberdar olma imkanı sağlayan uygun bir yöntem tercih edilebilir.

iii. Çalışanın kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine işveren tarafından yapılan müdahale, ulaşılmak istenen amaç ile ilgili ve bu amacı gerçekleştirmeye elverişli

olmalıdır. Ayrıca inceleme faaliyetiyle elde edilen verilerin işveren tarafından hedeflenen amaç doğrultusunda kullanılması gerekir.

iv. İşveren tarafından çalışanın kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine işveren tarafından yapılan müdahalenin gerekli kabul edilebilmesi için aynı amaca daha hafif bir müdahale ile ulaşılması mümkün olmamalı, müdahale ulaşmak istenen amaç bakımından zorunlu olmalıdır. Çalışanın iletişiminin içeriğine girilmesi yerine onun kişisel verilerine daha az müdahale eden yöntem ve tedbirlerin uygulanmasının mümkün olup olmadığı denetlenmelidir. Bu kapsamda işverenin ulaşmak istediği amaca çalışanın iletişimi incelenmeden de erişilme imkanı olup olmadığı her bir vakıanın somut özellikleri ışığında değerlendirilmelidir.

v. İşveren tarafından başvuruçunun kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine yönelik müdahalenin orantılı kabul edilebilmesi için ise iletişimin denetlenmesi ile işlenecek veya herhangi bir şekilde yararlanılacak veriler ulaşmak istenen amaçla sınırlı olmalı, bu amacı aşacak şekilde sınırlama ya da müdahaleye izin verilmemelidir.

vi. Ayrıca iletişimin incelenmesinin muhatabı olan çalışan üzerindeki etkisi ve çalışan bakımından sonuçları göz önünde tutularak tarafların çatışan menfaat ve haklarının adil bir biçimde dengelenip dengelenmediğine bakılması gerekmektedir. Taraflardan birine şahsi olarak aşırı bir külfet yüklendiğinin tespiti halinde devletin pozitif yükümlülüklerini yerine getirmediği sonucuna varılabilir.

- ... Öte yandan e-posta hesabı üzerinden yapılan iletişimin denetlenebileceğine ve iletişim araçlarının kullanım koşullarına ilişkin olarak önceden tam ve açık bir bilgilendirme yapılmadığı hallerde temel hak ve özgürlüklerinin işyerinde de korunacağı yönündeki haklı beklentiyle çalışan kişinin kurumsal e-posta üzerinden kişisel yazışmalar yapabileceğinin işveren tarafından da öngörülebilecek bir durum olduğu vurgulanmalıdır. Buradan hareketle çalışana açık bir bilgilendirmenin yapılmadığı hallerde hak ve özgürlüklerine bir müdahalede bulunulmayacağı hususunda çalışanların makul bir beklenti içinde olacaklarının kabul edilmesi, temel hak ve özgürlüklerin sağladığı güvencelerden yararlandırılması gerektiği söylenebilir.”

şeklindeki kriterlerin vurgulandığı,

- Öte yandan, Avrupa İnsan Hakları Mahkemesinin (AİHM), Bărbulescu/Romanya Kararı'nda çalışanın iletişiminin işveren tarafından denetlenmesiyle ilgili ilkelerin belirlendiği; AİHM tarafından olay değerlendirilirken bir taraftan, çalışanın özel hayatına ve yazışmalarına saygı gösterilmesi hakkına sahip olduğunun, diğer taraftan şirketin düzgün işlemesi adına işverenin de gerekli

önlemler alma hakkına sahip olduğunun ifade edildiği, ancak ulusal mahkemelerin bu yarışan çıkarlar konusunda adil bir denge kuramadığının belirtildiği, AİHM tarafından, mesajlaşmaların izlenebileceği konusunda çalışanın işvereni tarafından önceden haberdar edilmediğinin tespit edildiği ayrıca başvurucunun, izlemenin niteliği ya da kapsamı özellikle de işverenin mesajlarının içeriğine erişebilme ihtimali hakkında bilgilendirilmediğinin vurgulandığı, AİHM'e göre ulusal mahkemelerin, izleme tedbirlerini haklı gösterecek özel sebepleri tespit edemediği; ikinci olarak, çalışanın özel hayatına ve yazışmalarına daha az müdahale öngören tedbirlerin varlığının yeterince tartışılmadığı, üçüncü olarak ise mesajların içeriğine çalışanın ön bilgisi olmadan erişildiği, dolayısıyla, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde düzenlenen özel hayata saygı hakkının yeterince korunmadığına ve ihlal edildiğine karar verildiği,

- AİHM tarafından özellikle işverenin, çalışanlarının iletişimlerini takip etmek için tedbirler alması durumunda, bu tedbirlerin istismarına karşı uygun ve yeterli önlemleri de sağlaması gerektiğinin vurgulandığı; bu noktada Mahkemenin çalışanların özel hayata saygı hakkı ve kişisel verilerinin korunması konusunda özellikle işverenlere rehber olacak kriterlerini;

i. Çalışanın yazışmalarını ve diğer iletişimini izlemek için işveren tarafından kendisine bir ön bildirim yapılıp yapılmadığı,

ii. İletişimin denetlenmesinin kapsamı ve çalışanın mahremiyetine müdahalenin derecesinin belirlenmesi, bu bağlamda, iletişimin akışı ile içeriğinin denetlenmesi hususunun birbirinden farklı kavramlar olduğu,

iii. İletişimin denetlenmesi ve içeriğine erişilmesi konusunda işverenin meşru gerekçelere sahip olup olmadığı, özellikle iletişimin içeriğinin denetiminin daha net bir gerekçelendirme gerektirdiği,

iv. Doğrudan çalışanın yazışmalarının içeriğine erişmek yerine daha az müdahaleci yöntem ve tedbirlerin bulunup bulunmadığı,

v. Denetleme faaliyetinin sonuçları ve bu sonuçların işveren tarafından elde etme amacına uygun kullanılıp kullanılmadığı,

vi. Özellikle işverenin izleme faaliyeti müdahaleci bir nitelikte olduğunda, çalışan yeterli koruyucu önlemlere sahip olup olmadığı, nitekim bu koruyucu önlemler dahilinde çalışanın önceden bilgilendirilmediği durumda işverenin iletişimlerin içeriğine erişememesi gerektiği,

şeklinde belirttiği,

- Sonuç olarak, AİHM'in çalışanların iş yerinde dahi özel hayata sahip olabileceği ve bu kapsamda kişisel verilerin korunmasının son derece önemli olduğunu vurgulayan bir karar verdiği, AİHM'nin mezkûr kararının, işverenlerin çalışanlar üzerinde herhangi bir denetim mekanizmasından yoksun olduğunu göstermediği, ancak özellikle çalışanların gözetilmesi ve iletişimlerinin denetlenmesi faaliyetlerinin Mahkeme tarafından belirlenen kriterler ölçüsünde hassasiyetle uygulanması gerektiğinin ifade edildiği,
- Bu kapsamda, konu ile ilgili olarak değinilen AYM ve AİHM kararlarında yer verilen kriterler de göz önünde bulundurulduğunda, iş ilişkisi kapsamında ilgili kişiye veri sorumlusu tarafından kurumsal faaliyetlerde ve işin gerektirdiği ölçüde kullanılmak üzere bir kurumsal e-posta hesabının tahsis edildiği, ancak veri sorumlusunun cevabi yazısında da belirtildiği üzere ilgili kişiye söz konusu hesabın sadece işin ifası amacı ile kullanılacağına veya işveren tarafından çalışanların e-postalarının incelenebileceğine/denetlenebileceğine ilişkin olarak Kanun'un 10'uncu maddesi ile Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in (Tebliğ) 4'üncü maddesi kapsamında herhangi bir aydınlatma yapılmadığının görüldüğü,
- İlgili kişiye Kanun ve Tebliğ hükümleri kapsamında herhangi bir aydınlatma yapmaması nedeniyle veri sorumlusu tarafından ilgili kişinin e-postalarının incelenmesinin Kanun'un 5'inci maddesinde yer verilen herhangi bir işleme şartına dayanmadığı dikkate alındığında, Kanun'un 12'nci maddesi kapsamındaki yükümlülüklerin ihlal edildiği,
- Diğer taraftan, ilgili kişinin, verilerinin yetkisiz üçüncü kişilerin erişimine açıldığı iddiasına ilişkin olarak; veri sorumlusunun Kuruma intikal eden cevabi yazısından ve ilgili kişiye vermiş olduğu cevabi yazıdan anlaşıldığı üzere taraflarına ulaşan veri sorumlusuna başvuru metninin içeriğinde söz konusu iddianın mevcut olmadığı görüldüğünden ilgili kişinin bu husustaki iddialarını Kanun'un 14'üncü maddesi kapsamında öncelikle veri sorumlusuna iletmesi gerektiğinin hatırlatılmasının uygun olacağı,
- İlgili kişinin açık rızası olmaksızın işlenen özel hayatı ile ilgili e-posta içeriklerinin, şahsi banka hesap dökümlerinin, harcama kayıtlarının ve Kanun'un 5'inci maddesinin (2) numaralı fıkrası kapsamında işleme şartını haiz olmadan işlenen diğer kişisel verilerinin silinmesi veya yok edilmesi şeklindeki talebine ilişkin olarak; veri sorumlusunun ilgili kişiye verdiği cevapta; söz konusu kurumsal e-posta hesabında yer alan yazışmaların devam etmekte olan davada delil olarak mahkemeye sunulmuş olması sebebiyle silinemeyeceğinin belirtildiği dikkate alındığında, yargı konusu olan hususlara ilişkin inceleme yapılamayacağından hareketle ilgili kişinin söz konusu talebi çerçevesinde yapılacak işlem bulunmadığı,

- İlgili kişinin, veri sorumlusunun, müşterilerinin ve çalışanlarının bilgilerinin muhafaza edildiği hizmet sağlayıcı firma olan Microsoft serverlarının yurtdışında bulunuyor olmasından dolayı söz konusu işlemlerin Kanun'un 9'uncu maddesine uygun olarak gerçekleştirilmesi gerektiği iddiasına ilişkin olarak; konunun Kanun'un 15'inci maddesinin (1) numaralı fıkrası çerçevesinde resen inceleme kararı alınmasının uygun olacağı,
- Veri sorumlusunun, "işyerinde iş saatlerinde söz konusu e-posta hesabı üzerinden özel nitelikli yazışmalar yapan ilgili kişinin, bu verilerin işverenin olağan denetim yükümlülüğü kapsamında erişimine açık olabileceğini pekala göz önünde bulunduracağı ve bu durumun söz konusu yazışmaları işleme ve kaydetme hususunda ilgili kişinin işverene açık rıza verdiği şeklinde yorumlanacağı, bu nedenle söz konusu verilerin ilgili kişinin kendisi tarafından alenileştirilmiş vaziyette olduğu" yönündeki savunmasına karşılık, ilgili kişinin "şirket e-posta hesabında, eski nişanlısına gönderdiği özel e-posta içeriği ve şahsi banka hesap özeti bulunması nedeniyle herhangi bir alenileştirmeden bahsedilemeyeceği" yönündeki iddiasına ilişkin olarak kişisel verilerin alenileştirilmesi kavramına açıklık getirilmesinin faydalı olacağı,
- Kişisel Verileri Koruma Kurumu tarafından yayımlanan "6698 sayılı Kanunda Yer Alan Terimler" başlıklı rehberde "'Herkes tarafından bilinir kılma' anlamında olan alenileştirme kavramı, 6698 sayılı Kanunun 5. maddesinde, kişisel verilerin açık rıza aranmaksızın işlenebileceği hallerden biri olarak sayılmıştır. Buna göre, ilgili kişinin kendisi tarafından alenileştirilen, bir başka ifadeyle ilgili kişinin alenileştirme iradesi ile herhangi bir şekilde kamuoyuna açıklamış olduğu kişisel veriler, ayrıca ilgili kişinin açık rızası olmaksızın alenileştirme amacı ve Kanunun 4. maddesinde düzenlenen genel ilkeler kapsamında işlenebilecektir." şeklinde açıklanan "alenileştirme" kavramı ile ilgili olarak "Kişisel Verilerin İşlenme Şartları" başlıklı rehberde de "kişisel verinin aleni kabul edilebilmesi için ait olduğu kişinin aleni olmasını istemesi gerekir. Başka bir ifade ile, alenileştirmenin gerçekleştirilebilmesi için alenileştirme iradesinin varlığı gerekir. Yoksa bir kişinin kişisel verisinin herkesin görebileceği bir yerde olması aleni olmasını sağlamaz. Ayrıca, alenileştirme durumunda kişisel verinin amacı dışında da kullanılmaması gerekmektedir." şeklindeki açıklamaya yer verildiği,
- Dolayısıyla, somut olay kapsamında ilgili kişinin tüm yazışmalarını kurumsal e-posta adresi aracılığı ile yapmış olmasında ilgili kişinin verilerini kamuoyuna açıklama gibi bir iradesi bulunmadığından, kişisel verilerin alenileştirilmesinden bahsedilemeyeceği

değerlendirmelerinden hareketle;

İlgili kişiye Kanun ve Tebliğ hükümleri kapsamında herhangi bir aydınlatma yapılmaması dolayısıyla veri sorumlusu tarafından ilgili kişinin e-postalarının incelenmesinin Kanun'un 5'inci

maddesinde yer verilen herhangi bir işleme şartına dayanmadığı dikkate alındığında, Kanun'un 12'nci maddesinin (1) numaralı fıkrasına aykırılık teşkil eden uygulaması nedeniyle veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 250.000 TL idari para cezası uygulanmasına,

- İlgili kişinin, verilerinin yetkisiz üçüncü kişilerin erişimine açıldığı iddiasına ilişkin olarak; veri sorumlusunun Kuruma intikal eden cevabi yazısından ve ilgili kişiye vermiş olduğu cevabi yazıdan anlaşıldığı üzere taraflarına ulaşan veri sorumlusuna başvuru metninin içeriğinde söz konusu iddianın mevcut olmadığı görüldüğünden ilgili kişinin bu husustaki iddialarını Kanun'un 14'üncü maddesi kapsamında öncelikle veri sorumlusuna iletmesi gerektiğinin hatırlatılmasına,

- İlgili kişinin bahse konu verilerinin silinmesi talebi çerçevesinde, veri sorumlusunun "ilgili kişinin kurumsal e-posta hesabında yer alan yazışmaların devam etmekte olan davada delil olarak mahkemeye sunulmuş olması sebebiyle silinemeyeceği" yönündeki cevabı dikkate alındığında, yargı konusu olan hususlara ilişkin inceleme yapılamayacağından hareketle ilgili kişinin söz konusu talebi çerçevesinde yapılacak işlem bulunmadığına,

- Öte yandan, ilgili kişinin "müşterilerinin ve çalışanlarının bilgilerinin muhafaza edildiği hizmet sağlayıcı firma olan Microsoft serverlarının yurtdışında bulunuyor olmasından dolayı söz konusu kişisel veri işleminin Kanun'un 9'uncu maddesine uygun olarak gerçekleştirilmesi gerektiği" yönündeki iddiasına ilişkin olarak; Kanun'un 15'inci maddesinin (1) numaralı fıkrası kapsamında resen inceleme başlatılmasına

karar verilmiştir.

2021/1153 sayılı KVKK Kararı

Tıbbi ürünler satan veri sorumlusu tarafından ilgili kişiye reklam içerikli SMS gönderilmesi suretiyle kişisel verilerinin işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 11/11/2021 tarihli ve 2021/1153 sayılı Karar Özeti

Karar Tarihi : 11/11/2021

Karar No : 2021/1153

Konu Özeti : Tıbbi ürünler satan veri sorumlusu tarafından ilgili kişiye reklam içerikli SMS gönderilmesi

İlgili kişinin Kuruma intikal eden şikâyetinde özetle; kişisel verisi niteliğindeki cep telefonu numarasına tıbbi ürünler satan bir veri sorumlusundan reklam içerikli ticari elektronik ileti gönderildiği, bunun üzerine kişisel verilerinin işlenmesine ilişkin açık rızasının bulunmadığını beyan ederek kişisel verilerinin nasıl elde edildiği hakkında bilgi ve kişisel verilerinin silinmesi talepli dilekçe ile veri sorumlusuna başvuruda bulunduğu, başvurusuna karşılık iletilen cevapta ilgili kişinin telefon numarası dışında herhangi bir verisinin kendilerinde bulunmadığının, söz konusu cep telefonu numarasının veri sorumlusu bünyesinde kayıtlı başka bir hastanın iletişim bilgisi olarak verdiği numara olduğunun, bu hastanın reklam ve tanıtım mesajları alma konusunda onayının bulunduğu ve ilgili hastanın sehven ilgili kişinin numarasını vermiş olabileceğinin düşünüldüğünün belirtildiği; ancak veri sorumlusunca verilen bu cevabın yetersiz olduğu ve onay mekanizmasını doğrulama olmaksızın gerçekleştirmesi nedeniyle veri sorumlusunun söz konusu olayda ihmalinin bulunduğu ifade edilerek gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- İlgili kişinin başvurusunda bulunması gereken zorunlu unsurların tamamının yer almadığı, gerekli bilgilerin bulunmaması sebebiyle kimlik doğrulaması yapılamadığı, her ne kadar usulüne uygun bir başvuru olmasa da hak ihlaline sebebiyet vermemek adına ilgili telefon numarasının mesaj gönderilmemesi amacıyla sistem üzerinden engellendiği ve talebine ilişkin olarak ilgili kişiye yanıt verilerek söz konusu işlemin hata ile ortaya çıktığının ve düzeltmelerin yapıldığının bildirildiği;

ancak usulüne uygun olarak yapılmayan başvurudan kaynaklı şikâyet hakkının kullanılmasının mümkün olmadığı,

- Veri sorumlusu bünyesinde ilgili kişiye ait herhangi bir kayıt veya kişisel veri bulunmadığı, ilgili kişiye ait olduğu iddia edilen cep telefonu numarasının, veri sorumlusundan daha önce hizmet alan başka bir şahsın numarası olduğu ve bu cep telefonu numarasının reklam ve kampanya amaçlı bilgilendirme ve iletişim faaliyetlerinin yürütülebilmesi amacı ile 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 5'inci maddesinin (1) numaralı fıkrasına uygun olarak açık rıza işleme şartı kapsamında işlendiği, bu kapsamda söz konusu numaraya bilgilendirme mesajları gönderilmesi hususunda hastaya yeterli bilgilendirmelerin yapıldığı ve kendisi ile iletişime geçilmesine yönelik ıslak imzalı dilekçe ile açık rızasının alındığı,

- İlgili kişinin başvurusu üzerine bahse konu telefon numarasının, bilgileri kayıtlı olan hastanın iletişim bilgileri kısmından silinerek taraflarınca gerekli düzeltmelerin yapıldığı, ilgili kişiye de hatanın düzeltildiği yönünde bilgi verilerek bu tarihten sonra kendisine herhangi bir elektronik ileti gönderilmediği ve ilgili kişinin başka bir kişisel verisinin işlenmediği,

- Kişisel Verileri Koruma Kurulu'nun 22/12/2020 tarihli ve 2020/966 sayılı İlke Kararına uygun şekilde SMS doğrulama sistemine geçildiği ve kimlik doğrulaması ile ilgili kişilerin kişisel verilerinin tespit edilerek buna uygun şekilde açık rızaları doğrultusunda kendilerine SMS gönderildiği; ancak ilgili kişinin telefon numarasının SMS doğrulama sisteminden önce yazılı ve ıslak imzalı bir açık rıza metni olması sebebi ile onayı olduğu varsayılarak sisteme eklendiği ve bu açık rızaya dayalı olarak mesaj iletildiği

ifade edilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulu'nun 11/11/2021 tarihli ve 2021/1153 sayılı Kararı ile;

- Kanun'un "Veri Sorumlusuna Başvuru" başlıklı 13'üncü maddesine göre, ilgili kişinin bu Kanun'un uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna ileteceği; veri sorumlusunun başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandıracağı, talebi kabul edeceği veya gerekçesini açıklayarak reddedeceği ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildireceği hükmüne yer verildiği,

- Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in (Tebliğ) "Başvuruya Cevap" başlıklı 6'ncı maddesinin (1) numaralı fıkrasında veri sorumlusunun bu Tebliğ kapsamında ilgili kişi

tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlü olduğunun ve (2) numaralı fıkrasında veri sorumlusunun, başvuruyu kabul edeceğinin veya gerekçesini açıklayarak reddedeceğinin düzenlendiği,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi; fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin kendisi tarafından alenileştirilmiş olması; bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükmünün yer aldığı,

- Kanun'un "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi" başlıklı 7'nci maddesinin (1) numaralı fıkrasında, bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silineceği, yok edileceği veya anonim hâle getirileceğinin; (2) numaralı fıkrasında, kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğunun; (3) numaralı fıkrasında ise kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esasların yönetmelikle düzenlendiğinin hükme bağlandığı,

- İlgili kişinin veri sorumlusuna ilettiği başvuru incelendiğinde ad, soyad, imza, adres ve iletişim bilgisine yer verildiği görüldüğünden ilgili kişinin veri sorumlusu nezdinde herhangi bir kaydı bulunmaması nedeniyle kimlik tespiti yapılamaması gibi bir durumun söz konusu olmayacağı,

- Kanun'un 13'üncü maddesi ile Tebliğ'in 6'ncı maddesinin (2) numaralı fıkrası hükümlerine istinaden veri sorumlusunun, ilgili kişinin başvurusunu gerekçesini açıklayarak reddetmemek suretiyle cevaplandırmış olduğu göz önünde bulundurulduğunda ilgili kişinin Kurula başvuru şartını yerine getirdiği ve usulüne uygun bir başvurunun Kurul tarafından incelemeye alındığı sonucuna varıldığı,

- Veri sorumlusundan daha önce hizmet aldığı iddia edilen şahsa ilişkin bir cihaz satış belgesinin Kuruma iletildiği, söz konusu belgenin üzerindeki bilgilerden bu satışın 2019 yılında gerçekleştirildiğinin ve iletişim bilgisi olarak ilgili kişinin cep telefonu numarasının yer aldığı anlaşıldığı,
- Söz konusu cep telefonu numarası bahsi geçen müşteri yerine ilgili kişiye ait olsa da veri sorumlusu tarafından bu durumun bilinmediği ve söz konusu numaranın anılan müşteriye ilişkin bir veri olarak işlendiği, dolayısıyla ilgili kişinin cep telefonu numarasının veri sorumlusu kayıtlarında kendisi ile ilişkilendirilmiş bir veri olarak işlenmediği ve müşteri tarafından sehven hatalı numaranın bildirilmesi sonucu şikâyete konu olayın vuku bulduğu kanaatine varıldığı,
- Veri sorumlusu tarafından belirtilen müşterinin imzalamış olduğu dilekçeden, reklam ve pazarlama amaçlı olarak kendisine elektronik ileti gönderilmesi hususunda açık rızasının bulunduğu anlaşıldığı,
- Veri sorumlusunun Kuruma verdiği yanıtta, ilgili kişinin başvurusu üzerine söz konusu numaranın “kara liste”ye alındığı belirtilerek ilgili listeye ilişkin ekran görüntüsüne yer verilmişse de herhangi bir veri işleme şartına dayanılmaksızın işlenmiş olan kişisel verilerin kara listeye alınmak suretiyle kişisel veri işleme faaliyetine devam edildiği ve bu anlamda ilgili kişinin şikâyetine konu kişisel verisinin Kanun’un 7’inci maddesine uygun olarak imha edilmediği sonucuna varıldığı değerlendirilmelerinden hareketle;
- İlgili kişiye ticari elektronik ileti gönderilmesi suretiyle kişisel verilerinin hukuka aykırı olarak işlenmesi hususuna ilişkin olarak; söz konusu cep telefonu numarasının veri sorumlusu kayıtlarında kendisi ile ilişkilendirmiş bir veri olarak işlenmediği, bir müşteri tarafından sehven hatalı numaranın bildirilmesi sonucu şikâyete konu olayın vuku bulduğu ve bu hususların veri sorumlusu tarafından belgeleri ile tevsik edilebildiği kanaatine varılmış olup veri sorumlusu hakkında Kanun kapsamında tesis edilecek herhangi bir işlem bulunmadığına,
- Bununla birlikte, Kanun’un kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesini düzenleyen 7’nci maddesi ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi Hakkında Yönetmeliğe uygun bir biçimde ilgili kişinin kişisel verilerinin imha edilmesi ve bu hususta Kurula bilgi verilmesi yönünde veri sorumlusunun talimatlandırılmasına karar verilmiştir.

2021/1127 sayılı KVKK Kararı

Veri sorumlusu Üniversitenin ilgili kişinin kişisel verilerini içeren belgeleri internet sitesinde yayımlaması hakkında Kişisel Verileri Koruma Kurulunun 04/11/2021 tarihli ve 2021/1127 sayılı Karar Özeti

Karar Tarihi : 04/11/2021

Karar No : 2021/1127

Konu Özeti : Veri sorumlusu Üniversitenin ilgili kişinin kişisel verilerini içeren belgeleri internet sitesinde yayımlaması

İlgili kişinin Kuruma intikal eden şikâyetinde özetle, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) Başkanlığı tarafından kişisel verileri ihtiva eden 40 sayfalık yazının Yükseköğretim Kurulu (YÖK) Başkanlığına bilgi amaçlı gönderildiği, sonrasında ilgili yazının YÖK Başkanlığı Hukuk Müşavirliği tarafından üst yazı ile üniversitelere bilgi amaçlı gönderildiği, "GİZLİ" ibareli söz konusu yazı ve belgelerin veri sorumlusu Üniversite tarafından tüm Üniversite çalışanlarına akademik ya da akademik olmayan ilgili ya da ilgisiz tüm personele e-posta yoluyla gönderildiği, söz konusu belgelerin veri sorumlusu Üniversite Rektörlüğü tarafından internet sitesinde yayımlandığı, ilgili kişinin konuya ilişkin yaptığı başvuruya istinaden veri sorumlusunun verdiği cevapta bu durumun sehven yapıldığının ifade edildiği belirtilerek "GİZLİ" ibareli ve mevcut durumda dava süreci devam eden konuyla ilgili belgelerin ilgisiz üçüncü kişilerle hem e-posta hem internet sitesi aracılığıyla paylaşılması sebebiyle 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında veri sorumlusu hakkında gereğinin yapılması talep edilmiştir.

Konuya ilişkin olarak başlatılan inceleme çerçevesinde veri sorumlusu Üniversitenin savunması istenilmiş olup alınan cevabi yazıda özetle;

- YÖK Başkanlığı Hukuk Müşavirliği tarafından gönderilen üst yazı ekinde sunulan TÜBİTAK Başkanlığının yazısında özetle, TÜBİTAK Araştırma ve Yayın Etiği Kurulu tarafından yapılan incelemeler sonucunda 15 hakemli derginin imtiyaz sahibi ve yayıncısı olan ilgili kişinin "haksız yazarlık" yaptığının tespit edildiği ve bu doğrultuda kendisine 5 yıl süre ile yaptırım uygulanacağı ve ilgili kişinin sahibi ve yazarı olduğu dergilerin "yağmacı yayıncılık" açısından derin kuşkular

içermesi nedeniyle akademik teşvik, atama ve yükseltmelerde bu dergilerin değerlendirme dışı bırakılması için gerekli işlemlerin başlatılmasına karar verildiğinin belirtildiği,

- Üniversite Rektörlüğü tarafından TÜBİTAK tarafından verilen yaptırım kararı uyarınca "yağmacı yayıncılık" açısından şüpheli bulunan ve akademik teşvik, atama ve yükseltmelerde kullanılması yasaklanan dergilerin Üniversitenin ilgili akademik aktörleri ile paylaşılmasına, bu şekilde YÖK tarafından paylaşılan ilgili yazının gereğinin yerine getirilmesine karar verildiği,

- Ekinde TÜBİTAK Raporunu barındıran ilgili yazının öncelikle Üniversite içerisinde yalnızca fakülte dekanları ile kurum içi profesyonel haberleşme için kullanılan Elektronik Belge Yönetim Sistemi (EBYS) aracılığıyla paylaşıldığı, bunun dışında e-posta veya benzeri herhangi bir araç ile paylaşım yapılmadığı, söz konusu veri paylaşımının TÜBİTAK Araştırma ve Yayın Etiği Kurulu Kararının gereğinin yerine getirilmesi kapsamında Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (ç) bendi uyarınca hukuki yükümlülüğünün yerine getirilebilmesi için ilgili kişiye ait kişisel verilerin işlenmesinin zorunlu olması şartına ve Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (e) bendi uyarınca, akademik aktörlerin teşvik, atama ve yükseltme işlemlerinin tesis edilebilmesi için bir hakkın tesisi, kullanılması veya korunması için veri işleminin zorunlu olması şartına dayanılarak gerçekleştirildiği,

- Devam eden süreçte, Üniversitede akademik çalışmalar yürütmekte olan öğrenciler ile akademik personelin, "yağmacı yayıncılık" şüphesi kapsamında kullanımı yasaklanan ilgili dergileri çalışmalarına esas alması halinde ilgili kişilerin ve/veya Üniversitenin yaşayabileceği mağduriyet riskleri göz önüne alınarak akademik aktörler tarafından sıkça takip edilen Üniversite internet sitesi üzerinde yayımlanmasına karar verildiği, ilgili verilerin internet sitesinde paylaşılmasında ise, Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (f) bendi uyarınca gerek Üniversite gerek Üniversite bünyesindeki akademik aktörlerin hak kaybına uğramaması ve akademik çalışmaların mevzuata ve yetkili kurum kararlarına uygun yürütümünün sağlanması yönündeki meşru menfaatleri için veri paylaşımının zorunlu olması haline dayanıldığı, ilgili kişisel veri işleme şartı yönünden yapılan değerlendirmede ilgili kişinin temel hak ve özgürlüklerine zarar vermeme koşulunun da göz önüne alındığı, şikâyete konu olayın ulusal birçok gazete ve uluslararası platformda erişime açık birçok internet sitesinde yer alması ve kamuoyu tarafından bilinen bir olay olmasından ve paylaşılan bilgilendirmede bu olayı aşar nitelikte kişisel veri paylaşımına yer verilmediğinden hareketle ilgili kişinin temel hak ve özgürlüklerine zarar vermeyecek boyutta bir paylaşım olduğuna kanaat getirildiği,

- Veri işleme faaliyetinin TÜBİTAK Başkanlığı tarafından hazırlanan raporun Üniversite fakülte dekanlarıyla EBYS üzerinden paylaşılması ve internet sitesi üzerinden yayımlanması suretiyle gerçekleştirildiği, bu kapsamda ilgili kişiye ait ad-soyadı, unvan, adres bilgisi, imtiyaz sahibi yayıncısı ve/veya temsilcisi olduğu dergi bilgileri, akademik çalışma alanı bilgileri, taraf olduğu dosya ve soruşturma bilgileri, hakkındaki görüş yazıları ve hakkındaki komisyon görüşünün üçüncü kişiler ile paylaşıldığı,

- İlgili kişinin Üniversite internet sitesi üzerinden yapılan paylaşımına ilişkin olarak yaptığı başvuru doğrultusunda konunun tekrar incelendiği ve olayın üzerinden geçen süreden ve akademik aktörlerin geçen süre zarfında bu konuda bilgilenmiş olmalarından hareketle ilgili kişinin talebinin yerine getirildiği, internet sitesi üzerinden yapılan paylaşımın kaldırıldığı

ifade edilmiştir.

Konuya ilişkin yapılan incelemede Kişisel Verileri Koruma Kurulu'nun 04/11/2021 tarihli ve 2021/1127 sayılı Kararı ile;

- Kanunun "Tanımlar" başlıklı 3'üncü maddesinde kişisel verinin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi, veri sorumlusunun; kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi, kişisel verilerin işlenmesinin ise kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı,

- Yine Kanun'un 4'üncü maddesinin (1) numaralı fıkrasında kişisel verilerin, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği hükmüne, (2) numaralı fıkra gereğince ise kişisel verilerin işlenmesinde "Hukuka ve dürüstlük kurallarına uygun olma; doğru ve gerektiğinde güncel olma; belirli, açık ve meşru amaçlar için işlenme; işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma; ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme." ilkelerine uyulmasının zorunlu olduğu hükmüne yer verildiği,

"Kişisel Verilerin İşlenme Şartları" başlıklı Kanunun 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya

rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğunun hükme bağlandığı,

- Kanun'un "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12'nci maddesinin (1) numaralı fıkrasında da, veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri almakla yükümlü olduğu hükmünü içerdiği,

- İlgili kişinin Kanun kapsamındaki haklarının 11'inci maddenin (1) numaralı fıkrasında düzenlendiği, buna göre herkes veri sorumlusuna başvurarak kendisiyle ilgili;

a) Kişisel veri işlenip işlenmediğini öğrenme,

b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,

ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,

e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,

f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme

haklarına sahip olduğu,

• Öte yandan, akademik teşvik, atama ve yükseltmeler ve etik ihlaline ilişkin üniversiteler ve akademisyenler nezdinde dikkate alınması gereken yasal düzenlemeler incelendiğinde;

- 12.06.2018 tarihli ve 30449 sayılı Resmi Gazete’de yayımlanan Öğretim Üyeliğine Yükseltme ve Atama Yönetmeliği’nin 12’nci maddesinin birinci fıkrasında, “Profesör kadrolarına atanabilmek için doçentlik unvanını aldıktan sonra en az beş yıl açık bulunan profesörlük kadrosu ile ilgili bilim alanında çalışmış olmak, kendi bilim alanında uluslararası düzeyde orijinal eserler vermiş olmak ve uygulama alanı bulunan dallarda uygulamaya yönelik çalışmalarda bulunması gereklidir.” hükmüne,

- 18.02.1982 tarihli ve 17609 sayılı Resmi Gazete’de yayımlanan Üniversitelerde Akademik Teşkilat Yönetmeliği’nin 8’inci maddesinin (b) bendinin son paragrafında, “Dekan; fakültenin ve bağlı birimlerinin öğretim kapasitesinin rasyonel bir şekilde kullanılmasında ve geliştirilmesinde, gerektiği zaman güvenlik önlemlerinin alınmasıyla, öğrencilere gerekli sosyal hizmetlerin sağlanmasında, eğitim-öğretim, bilimsel araştırma ve yayın faaliyetlerinin düzenli bir şekilde yürütülmesinde, bütün faaliyetlerin gözetim ve denetiminin yapılmasında, takip ve kontrol edilmesinde ve sonuçlarının alınmasında Rektöre karşı birinci derecede sorumludur.” hükmüne,

- 15.04.2018 tarihli ve 30392 sayılı Resmî Gazete’de yayımlanan Doçentlik Yönetmeliği’nin 6’ncı maddesinin birinci fıkrasında, “Doçentlik değerlendirme jürisi, adayın başvuru dosyasını ilk olarak bilimsel araştırma ve yayın etiğine aykırılık bulunup bulunmadığı ve asgari başvuru şartlarının sağlanıp sağlanmadığı yönünden değerlendirir...” hükmüne yer verildiği,

• İlgili kişiye ait kişisel verileri içeren belgenin tüm üniversite çalışanlarına akademik ya da akademik olmayan ilgili ya da ilgisiz tüm personele e-posta olarak gönderildiği iddiasının değerlendirilmesi neticesinde; ilgili kişinin, kendisinin kişisel verilerini içeren belgenin veri sorumlusu tarafından tüm üniversite çalışanlarına, akademik ya da akademik olmayan ilgili ya da ilgisiz tüm personele e-posta olarak gönderildiğini iddia etmesine karşılık bu iddiasına ilişkin tevsik edici bilgi ve belge sunulmadığından ilgili kişiye ait kişisel verileri içeren belgenin EBYS aracılığıyla fakülte dekanlarına gönderildiği yönünde değerlendirme yapılmış olup mevzuatın incelenmesi neticesinde, akademik teşvik, atama ve yükseltmelere etki edecek nitelik taşıyan belgede yer alan ilgili kişiye ait kişisel verilerin veri sorumlusu Üniversite tarafından fakülte dekanları ile EBYS aracılığıyla paylaşılmasının Kanun’un 5’inci maddesinin ikinci fıkrasının (ç) ve (e) bentleri çerçevesinde veri sorumlusunun hukuki yükümlüğünü yerine getirebilmesi ve bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması işleme şartlarına dayanması sebebiyle Kanun’a aykırılık teşkil etmediği,

- İlgili kişiye ait kişisel verileri içeren belgenin üniversiteye ait internet sitesi üzerinden paylaşılmasına ilişkin değerlendirmede; TÜBİTAK Başkanlığı tarafından YÖK Başkanlığına gönderilen yazıda, ilgili kişinin sahibi ve yazarı olduğu ekli listede isimleri verilen dergilerin "yağmacı yayıncılık" açısından derin kuşkular içermesi nedeniyle akademik teşvik, atama ve yükseltmelerde söz konusu dergilerin değerlendirme dışı bırakılması için gerekli işlemlerin başlatılmasının ifade edildiği dikkate alındığında; fakülte dekanlarına ilgili belgenin gönderilmesine ilişkin incelenen ilgili mevzuat kapsamında, veri sorumlusunun savunmasında iddia ettiği üzere Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (f) bendinde yer alan meşru menfaat işleme şartı kapsamında değerlendirilememekle birlikte aynı fıkranın (e) bendine göre bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması şartına uygun olarak kullanımı yasaklanan söz konusu dergilerin çalışmalarda esas alınmaması adına veri sorumlusu Üniversitenin yüksek lisans ve doktora öğrencileri ile akademik personele bilgi vermesi gerekliliğinin mevcut olduğu kanaatine varılabileceği,

- Ancak her ne kadar veri sorumlusu Üniversite tarafından ilgili kişiye ilişkin kişisel verileri içeren belge, Üniversitenin herkesin ilk aşamada ulaşabileceği tanıtım ve bilgi amaçlı kullanılan ve tüm ziyaretçilere açık olan adresten farklı olarak bilimsel çalışmalarda bulunan akademik aktörler tarafından proje geliştirme amacıyla kullanılan akademik kullanım amaçlı site üzerinden yayımlanmış ve veri sorumlusu tarafından ilgili kişinin başvurusu sonrası paylaşımın sehven yapıldığı belirtilmek suretiyle kaldırılmış olsa da yüksek lisans ve doktora öğrencileri ile akademik personeli bilgilendirme amacını aşacak şekilde, TÜBİTAK Başkanlığı tarafından YÖK Başkanlığına "GİZLİ" olarak gönderilen belgede yer alan üçüncü kişilere ait kişisel verilerin, ilgili kişiye ait adres bilgisi, taraf olduğu soruşturma bilgileri, hakkındaki görüş yazıları ve komisyon görüşü gibi kişisel verilerin tamamının veri sorumlusu tarafından Üniversiteye ait internet sitesinde paylaşılması ile veri minimizasyonu ilkesine aykırı hareket edildiği, bu anlamda Kanun'un 4'üncü maddesinin ikinci fıkrasının (ç) bendi gereğince kişisel verilerin işlenmesinde işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkelerinin gözetilmediği

değerlendirmelerinden hareketle;

- Akademik teşvik, atama ve yükseltmelere etki edecek nitelikte belgede yer alan ilgili kişiye ilişkin kişisel verilerin fakülte dekanları ile Kurumun EBYS sistemi aracılığıyla paylaşılmasının Kanun'un 5'inci maddesinin ikinci fıkrasının (ç) ve (e) bentleri çerçevesinde veri sorumlusunun hukuki yükümlüğünü yerine getirebilmesi ve bir hakkın tesisi, kullanılması veya korunması için veri

işlenmesinin zorunlu olması işleme şartları kapsamında hukuka uygun olduğu değerlendirildiğinden bu hususta Kanun kapsamında yapılacak işlem olmadığına,

- Belgede yer alan ilgili kişiye ait kişisel verilerin akademik çalışmalar için kullanılan Üniversiteye ait internet sayfasında yayımlanmak suretiyle Kanun'un 5'inci maddesinin ikinci fıkrasının (e) bendine uygun olarak kullanımı yasaklanan söz konusu dergilerin çalışmalarda esas alınmaması adına veri sorumlusu Üniversitenin yüksek lisans ve doktora öğrencileri ile akademik personele bilgi vermesi gerekliliğinin Kanun'a uygun olduğu değerlendirilmekle birlikte veri sorumlusu tarafından bilgilendirme amacını aşacak nitelikte söz konusu belgede yer alan kişisel verilerin tamamının Üniversiteye ait internet sitesinde paylaşılmasının Kanun'un 4'üncü maddesinin (2) numaralı fıkrasının (ç) bendi gereğince kişisel verilerin işlenmesinde işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkelerine aykırılık teşkil ettiği ve bu doğrultuda Kanun'un 12'nci maddesinin birinci fıkrasına aykırı olarak veri sorumlusu Üniversite tarafından kişisel verilerin güvenliğine yönelik gerekli yükümlülüklerin yerine getirilmediği kanaatine ulaşıldığından sorumlular hakkında Kanun'un 18'inci maddesinin (3) numaralı fıkrası çerçevesinde işlem yapılması ve işlemin sonucu hakkında Kurula bilgi verilmesine

karar verilmiştir.

2021/1111 sayılı KVKK Kararı

İlgili kişinin ceza mahkûmiyeti bilgisinin avukat olan veri sorumlusu tarafından hukuka aykırı olarak elde edilmesi ve mahkeme dosyasına sunulması hakkında Kişisel Verileri Koruma Kurulunun 02/11/2021 tarihli ve 2021/1111 sayılı Karar Özeti

Karar Tarihi : 02/11/2021

Karar No : 2021/1111

Konu Özeti : İlgili kişinin ceza mahkûmiyeti bilgisinin avukat olan veri sorumlusu tarafından hukuka aykırı olarak elde edilmesi ve mahkeme dosyasına sunulması

İlgili kişinin şikâyetinde özetle;

- Veri sorumlusunun vekillik görevi üstlendiği işçilik alacakları davası kapsamında ilgili kişinin davalı tanığı olarak bilgi ve görgüsüne başvurulduğu,
- Daha sonra veri sorumlusunca mahkemeye sunulan beyan dilekçesinde ilgili kişi ile ilgili olarak "Ayrıca ... tanık ... hakkında daha önceden çok sayıda memur olmayan kişinin resmî belgede sahteciliği suçundan dolayı ceza davaları açılmıştır. Bu davalarda son olarak Ceza Mahkemesinde dosyada almış olduğu mahkûmiyet hükmü kesinleşmiştir." ifadelerine yer verilmek suretiyle ceza mahkûmiyeti bilgisinin paylaşıldığı ve mahkemeden ilgili kişinin tanıklığına itibar edilmemesinin talep edildiği,
- İlgili kişinin özel nitelikte kişisel verisi olan adli sicil kaydına ilişkin bilgilerin veri sorumlusu tarafından hukuka aykırı olarak ele geçirildiği ve ilgili kişinin onayı ve bilgisi olmadan mahkeme dosyasına sunulduğu,
- Veri sorumlusunca dosyaya sunulan ilgili kişiye ait adli sicil kaydı bilgilerinin dosyanın esasıyla ilgisinin bulunmadığı, bu bilgilerin dosyanın esas bakımından bir faydasının da bulunmadığı, zira ilgili kişinin dosyada sadece tanıklık yaptığı,

Veri sorumluları tarafından kullanılan üçüncü kişilere ait kişisel verilerin amaçla bağlantılı ve ölçülü olması gerektiği, ancak ilgili kişiye ait özel nitelikli kişisel verilerin veri sorumlusunca kullanımının amaçla bağlantılı ve ölçülü olmadığı,

- İlgili kişinin yıllar önce yaşamış olduğu ve cezasını çekmiş olduğu bir dosyanın tekrar gün yüzüne çıkmasıyla birlikte işverenine ve çalışma arkadaşlarına karşı rencide olduğu, küçük düştüğü ve bu olay neticesinde büyük bir üzüntü duyduğu, dolayısıyla da manevi olarak büyük bir kayıp yaşadığı ve psikolojisi ile sağlığının da olay nedeniyle bozulduğu,

- Konu hakkında veri sorumlusuna iletilen başvuru dilekçesiyle 6698 sayılı Kişisel Verilerin Korunması Kanununun (6698 sayılı Kanun) 11'inci ve 13'üncü maddeleri kapsamında bilgi talep edildiği, ancak veri sorumlusu tarafından bu başvuruya verilen cevapta başvuru dilekçesindeki hususlara ilişkin makul ve yeterli cevap verilmediği

hususları bildirilmiş olup; ilgili kişinin özel nitelikli kişisel verilerinin hukuka aykırı olarak ele geçirilmesi, bu verilerin ilgili kişinin onay ve rızası dışında beyan dilekçesinde mahkemeye sunulması suretiyle üçüncü kişilerle paylaşılması ve ilgili kişinin bu durumdan dolayı maddi ve manevi olarak yıpranması sebepleriyle veri sorumlusu hakkında 6698 sayılı Kanun uyarınca idari yaptırım uygulanması talep edilmiştir.

İlgili kişinin şikâyetine istinaden başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, verilen cevapta özetle;

- İlgili kişinin 6698 sayılı Kanun'a aykırılık iddialarının kabulünün mümkün olmadığı, zira ilgili kişinin mahkeme tarafından kendilerinin vekil olarak yer aldıkları bir duruşmada tanık olarak dinlendiği ve bu nedenle de T.C. kimlik numarası bilgilerinin duruşma tutanağında yer aldığı,

- Dosyada vekil olarak yer almaları nedeniyle ilgili kişinin T.C. kimlik numarasına erişimlerinin zaten mevcut olduğu, adli sicil verilerinin de avukatlar tarafından adliye kanalıyla kolayca erişilebilen veriler olduğu, işleri gereği bu bilgilere erişimlerinin olmasının hayatın olağan akışına uygun olduğu, kaldı ki ilgili kişinin vekil oldukları dosyada tanık sıfatıyla yer alarak dosyanın akıbetini etkileyecek bir konuma sahip olduğu ve bu kapsamda ilgili kişi hakkında araştırma yapmalarının hukuka aykırılık teşkil etmediği,

- Adli sicil verilerinin her avukat tarafından ilgili kişinin T.C. kimlik numarası aracılığıyla öğrenilebilecek bir husus olduğu,

- Şikâyete konu beyan dilekçelerinde ilgili kişinin bilgilerine yer vermelerinin yargılama gereği taraflarına verilen tanık beyanlarına karşı beyanda bulunma yasal haklarının kullanılmış olmasının bir sonucu olduğu,

- Dosya kapsamında tanık olarak dinlenmiş olan ilgili kişinin gerçeği yansıtmadığını düşündükleri beyanlarına itibar edilmemesi için taraflarınca kaleme alınan dilekçe ile iddialarının dayanağı olan bilgilerin mahkemece görülmesini sağlamayı amaçladıkları,
- İlgili kişinin şikâyetinde ilgili kişinin tanık olarak dinlenmesi nedeniyle adli sicil bilgilerinin dosyanın esasına bir etkisinin olmayacağı belirtilmiş olsa da bu beyanın yargılamada elzem değeri olan tanık delilinin önemini hiçe saymak olduğu, tanıklık sıfatının yargılamanın her kolunda önemli bir yere sahip olduğu ve dosyanın muhteviyatına göre yargılamanın yönünü belirlediği, bu nedenle yargılamada tanık beyanlarına itimat edilmesi hususunda tanığın doğru ifade verdiğinden emin olunması gerektiği ve tanıklık yapan kişinin adli geçmişinin de vereceği beyanlar kapsamında önem arz ettiği,
- 6698 sayılı Kanun'un 4'üncü maddesinin (2) numaralı fıkrasında verilerin işlenmesindeki esaslara yer verildiği, vekil olarak görev yaptıkları dosyanın akibeti hususunda mezkûr maddede geçtiği şekilde belirli, açık ve meşru olan amaçlarına uygun ve ölçülü olarak işleme faaliyetinde bulunulduğu, amaçlarının sadece mahkemenin tanık hakkında bilgilendirilmesi olduğu,
- İlgili kişinin adli sicil verilerinin taraflarınca hukuka aykırı şekilde elde edilmediği, aksine vekil olmaları dolayısıyla taraflarına açık olan bilgiler eşliğinde yine bir yargı organı vasıtasıyla elde edildiği, kaldı ki kişilerin adli sicil kayıtlarının UYAP vasıtasıyla hâkimler ve savcılar tarafından zaten ulaşılabilir veriler olduğu, dolayısıyla taraflarının mahkemeye bu bilgileri sunmasının 6698 sayılı Kanun'a aykırılık teşkil etmeyeceği,
- Avukatlığın hem bir kamu hizmeti hem de serbest meslek olduğu, 1136 sayılı Avukatlık Kanunu'nun (Avukatlık Kanunu) 2'nci maddesinde mesleğin amacının "Avukatlığın amacı; hukuki münasabetlerin düzenlenmesini, her türlü hukuki mesele ve anlaşmazlıkların adalet ve hakkaniyete uygun olarak çözümlenmesini ve hukuk kurallarının tam olarak uygulanmasını her derecede yargı organları, hakemler, resmi ve özel kişi, kurul ve kurumlar nezdinde sağlamaktır." olarak açıklandığı, avukatların bu yolda görev yaparken çoğu kez belirsizliklerle karşılaştıkları ve bu belirsizlikleri kendi imkânlarıyla çözmek zorunda oldukları,
- Bu nedenle avukatların bir olayın aydınlatılması için çeşitli kurum ve kuruluşlardan zaman zaman bilgi almalarının gerektiği, kanun koyucunun da Avukatlık Kanunu'nun 2'nci maddesinde "Yargı organları, emniyet makamları, diğer kamu kurum ve kuruluşları ile kamu iktisadi teşebbüsleri, özel ve kamuya ait bankalar, noterler, sigorta şirketleri ve vakıflar avukatlara görevlerinin yerine getirilmesinde yardımcı olmak zorundadır." hükmüne yer verdiği ve bu hükmün avukatların

mesleklerinin gereklerini yerine getirirken ihtiyaç duydukları bilgileri kendilerine sağlayabilecek kurumlara başvuru yapabilmelerine imkân sağladığı,

- Şikâyet konusu olayda adliye kanalıyla ilgili kişinin adli sicil verilerine ulaşmış ve sonrasında da bunu ilgili mahkemeye bildirmiş olmalarının vekillik görevleri gereği yargı organlarından yararlanmaktan başka bir şey olmadığı, hâl böyleyken avukat olarak mahkemeye sundukları verilerin 6698 sayılı Kanun'a aykırı olduğunu öne sürmenin hakkaniyete uygun olmayacağı, zira bahsi geçen olayda Avukatlık Kanunu'ndan kaynaklanan bir yetkinin kullanılmasının söz konusu olduğu,
- Meslekleri gereği kamu hizmeti yaptıkları da düşünülürse taraflarına kanunla sağlanan bir yetkinin kullanılması niteliğinde olan mevcut durumun ilgili kişi tarafından kötü niyetli olarak ve tamamıyla dürüstlük kurallarına aykırılık teşkil edecek şekilde kullanılıyor olmasının hukuk düzeni içerisinde kabul edilebilir olmadığı,
- İlgili kişinin adli sicil kayıtlarının sadece beyan dilekçesi içerisinde mahkemeye sunulduğu, herhangi bir üçüncü kişiyle paylaşılmadığı, aynı zamanda ilgili kişiye ait başka herhangi bir kişisel veri veya bilginin de elde edilmemiş olduğu,
- Yukarıda yer alan tüm bilgiler ve kanun maddeleri doğrultusunda ilgili kişinin iddia ettiği üzere 6698 sayılı Kanun'a aykırı bir unsurun bulunmadığı

beyan edilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde, Kişisel Verileri Koruma Kurulunun (Kurul) 02/11/2021 tarihli ve 2021/1111 sayılı kararı ile;

- 6698 sayılı Kanun'un "Tanımlar" başlıklı 3'üncü maddesinde kişisel verinin: "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", ilgili kişinin; "Kişisel verisi işlenen gerçek kişi", kişisel verilerin işlenmesinin; "Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem", veri sorumlusunun; "Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi" olarak tanımlandığı,
- Öte yandan, 6698 sayılı Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak

durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğunun hükme bağlandığı,

- 6698 sayılı Kanun'un özel nitelikli kişisel verilerin işleme şartlarının düzenlendiği 6'ncı maddesinin (1) numaralı fıkrasında özel nitelikli kişisel verilerin tanımlandığı, (2) numaralı fıkrasında özel nitelikli kişisel verilerin ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğunun hüküm altına alındığı, (3) numaralı fıkrasında özel nitelikli kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenebileceği durumların sayıldığı, (4) numaralı fıkrasında ise özel nitelikli kişisel verilerin işlenmesinde Kurul tarafından belirlenen yeterli önlemlerin ayrıca alınmasının şart olduğunun ifade edildiği,

- Ayrıca, 6698 sayılı Kanun'un kişisel verilerin işlenmesine ilişkin "Genel ilkeler"i düzenleyen 4'üncü maddesinin (1) numaralı fıkrasında "Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir." hükmü yer almakta olup, bahsi geçen maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin "Hukuka ve dürüstlük kurallarına uygun olma", "Doğru ve gerektiğinde güncel olma", "Belirli, açık ve meşru amaçlar için işleme", "İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ve "İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" olarak sayıldığı,

- 6698 sayılı Kanun'un ilgili hükümleri dikkate alındığında; ilgili kişinin adli sicil kaydı bilgilerinin veri sorumlusu tarafından tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, depolanması, kullanılması, aktarılması vb. fiillere konu edilmesinin "özel nitelikli kişisel verilerin işlenmesi faaliyeti" olarak niteleneceği ve bu tarz faaliyetlerin hem 6698 sayılı Kanun'un 6'ncı maddesindeki hukuki sebeplerden birine dayanılarak ve Kurul tarafından belirlenen yeterli önlemler alınarak hem de 6698 sayılı Kanun'un 4'üncü maddesindeki genel ilkelere uygun olarak yürütülmesi gerektiği konusunda herhangi bir şüphenin bulunmadığı,

- Bu kapsamda, somut olayda ilgili kişinin adli sicil kaydı bilgilerinin veri sorumlusunca elde edilmesinin 6698 sayılı Kanun'un 6'ncı maddesindeki hukuki sebeplerden birine dayanıp dayanmadığının öncelikle ele alınması gerektiği, zira ilgili kişinin adli sicil kaydı verilerinin veri sorumlusunca 6698 sayılı Kanun'un 6'ncı maddesindeki hukuki sebeplerden birine dayanılmadan elde edilmiş (ve sonrasında da kullanılmış/verilmiş) olması durumunda söz konusu fiillerin hukuka aykırı nitelikte birer veri işleme faaliyeti teşkil edeceği,
- Dosyaya sunulan bilgi ve belgelerden; ilgili kişinin adli sicil verilerinin işlenebilmesi için veri sorumlusuna vermiş olduğu bir açık rızanın bulunmadığının görüldüğü, veri sorumlusunun "ilgili kişinin adli sicil kaydı bilgilerinin Avukatlık Kanunu'na uygun olarak adliyeden temin edildiği, taraflarınca yapılan iş ve işlemlerde herhangi bir hukuka aykırılık bulunmadığı" yönündeki savunmasından ise ilgili kişi hakkında yürütülen kişisel veri işleme faaliyetinde 6698 sayılı Kanun'un 6'ncı maddesinin (3) numaralı fıkrasında düzenlenen "Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebilir." düzenlemesine dayanıldığının anlaşıldığı, bu yüzden de veri sorumlusunun savunmasında zikrettiği Avukatlık Kanunu'nun 2'nci maddesi hükmünün 6698 sayılı Kanun'un 6'ncı maddesinin (3) numaralı fıkrasında geçen "kanunlarda öngörülen haller" in kapsamına girip girmediğinin açıklığa kavuşturulması gerektiği,
- Avukatlık Kanunu'nun 2'nci maddesinde "Avukatlığın amacı; hukuki münasabetlerin düzenlenmesini, her türlü hukuki mesele ve anlaşmazlıkların adalet ve hakkaniyete uygun olarak çözümlenmesini ve hukuk kurallarının tam olarak uygulanmasını her derecede yargı organları, hakemler, resmi ve özel kişi, kurul ve kurumlar nezdinde sağlamaktır. (...) Yargı organları, emniyet makamları, diğer kamu kurum ve kuruluşları ile kamu iktisadi teşebbüsleri, özel ve kamuya ait bankalar, noterler, sigorta şirketleri ve vakıflar avukatlara görevlerinin yerine getirilmesinde yardımcı olmak zorundadır. Kanunlarındaki özel hükümler saklı kalmak kaydıyla, bu kurumlar avukatın gerek duyduğu bilgi ve belgeleri incelemesine sunmakla yükümlüdür. Bu belgelerden örnek alınması vekaletname ibrazına bağlıdır. (...)" ifadelerinin yer aldığı,
- 5352 sayılı Adlî Sicil Kanunu'nun ("Adlî Sicil Kanunu") "Adlî sicil bilgileri verilebilecek olanlar" başlıklı 7'nci maddesinde ise "(1) Adlî sicil bilgileri, kullanılış amacı belirtilmek suretiyle; a) İlgili kişiye veya vekaletnamede açıkça belirtilmek koşuluyla vekiline, b) Kamu kurum ve kuruluşlarına, kamu kurumu niteliğindeki meslek kuruluşlarına, verilebilir. (2) Yabancı devletler tarafından istenilen adlî sicil bilgileri mütekabiliyet esasına göre verilir." düzenlemesinin mevcut olduğu, ayrıca Adlî Sicil Kanunu'nun 15'inci maddesine dayanılarak çıkarılan Adlî Sicil Yönetmeliği'nin "Adlî sicil

bilgileri verilebilecek olanlar” başlıklı 9’uncu maddesinde de “Adli sicil bilgileri, kullanılış amacı ve verileceği merci belirtilmek suretiyle; ilgili kişiye veya vekaletnamede açıkça belirtilmek koşuluyla vekiline, kamu kurum ve kuruluşlarına, kamu kurumu niteliğindeki meslek kuruluşlarına verilebilir. Taleplerin yazılı olarak yapılması sırasında, adli sicil bilgisinin niçin istendiğinin belirtilmesi ve nüfus kimlik bilgilerini içeren belgenin dilekçeye eklenmesi; kamu kurum ve kuruluşları ile kamu kurumu niteliğinde meslek kuruluşlarınca da kimlik bilgilerinin tereddüde yer vermeyecek şekilde bildirilmesi zorunludur. (...)” denildiği,

- Mezkûr mevzuat hükümlerinin lafızlarına istinaden, Avukatlık Kanunu’nun 2’nci maddesinde yer alan düzenlemenin Adli Sicil Kanunu’nun 7’nci maddesinde mevcut olan “özel hüküm” karşısında bir “genel hüküm” niteliği taşıdığı açık olduğu ve avukatlara ilgili kişilerin adli sicil kaydı bilgilerine resen erişim yetkisi vermediği, dolayısıyla ilgili kişiye ait adli sicil bilgilerinin veri sorumlusu tarafından hukuka aykırı olarak elde edildiği, bu sebeple de veri sorumlusu tarafından ilgili kişi hakkında yürütülen kişisel veri işleme faaliyetinin hukuka aykırı olduğu sonucuna ulaşıldığı,

- İlgili kişinin -veri sorumlusu tarafından yürütülmüş olan kişisel veri işleme faaliyetlerine konu olan- özel nitelikli kişisel veri niteliğindeki adli sicil bilgilerinin en başta hukuka aykırı olarak elde edilmiş olmasının veri sorumlusunun tüm kişisel veri işleme faaliyetlerini başlangıçtan itibaren hukuka aykırı hale getirdiği, zira hukuka uygun olmayan bir şeyin üzerine meşru bir şeyin bina edilemeyeceği konusunda herhangi bir şüphenin bulunmadığı

değerlendirmelerinden hareketle;

- Mevcut tüm bilgi ve belgeler itibarıyla; ilgili kişinin adli sicil bilgisi kişisel verisinin işlenmesi faaliyetinde veri sorumlusu tarafından 6698 sayılı Kanun’un 6’nci maddesinde düzenlenen hukuki sebeplerden herhangi birine dayanılmadığı, bu hususun ise veri güvenliğine ilişkin yükümlülüklerin düzenlendiği 6698 sayılı Kanun’un 12’nci maddesinin (1) numaralı fıkrasının (a) bendinde yer alan “Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.” hükmüne aykırılık teşkil ettiği dikkate alındığında 6698 sayılı Kanun’un 18’inci maddesinin (1) numaralı fıkrasının (b) bendine istinaden veri sorumlusu hakkında 75.000 TL idari para cezası uygulanmasına,

- Veri sorumlusu tarafından ilgili kişi hakkında başlangıçtan itibaren hukuka aykırı nitelikte kişisel veri işleme faaliyetinde bulunduğu kanaatine ulaşıldığından, ilgili kişinin veri sorumlusu nezdinde tutulan ve hukuka aykırı işleme amacıyla bağlantılı kişisel verilerinin 6698 sayılı Kanun’un 7’nci maddesi ile Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında

Yönetmelik uyarınca imha edilmesi ve sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına,

- Söz konusu verinin paylaşılmasının 5237 sayılı Türk Ceza Kanunu hükümleri kapsamında suç unsuru barındırabileceği dikkate alındığında, bu hususta işlem tesis edilmesini teminen Cumhuriyet Başsavcılığına başvurulabileceği hususunda ilgili kişiye bilgi verilmesine

karar verilmiştir.

2021/1110 sayılı KVKK Kararı

Veri sorumlusunun icra takibi başlattığı müşterilerinin kişisel verilerini herkesin erişimine açık bir internet sitesinde yayımlaması hakkında Kişisel Verileri Koruma Kurulunun 02/11/2021 tarih ve 2021/1110 sayılı Karar Özeti

Karar Tarihi : 02/11/2021

Karar No : 2021/1110

Konu Özeti : Veri sorumlusunun icra takibi başlattığı müşterilerinin kişisel verilerini herkesin erişimine açık bir internet sitesinde yayımlaması

Kuruma intikal eden ihbarda özetle, bir holding bünyesinde faaliyet gösteren veri sorumlusu şirket tarafından icra takibi başlatılan müşterilerinin T.C. kimlik numarası, telefon numarası, araç plakası ve adres bilgisinin bir internet adresinde paylaşıldığı, bu işlemi yaparken amaçlarının internet adresini verdikleri şahısların burada yazan yakalama kararı olan araçları bulmaları halinde 155 ihbarı yaparak bu araçların yakalatılmasının ve trafikten men edilmesinin sağlanması olduğu ifade edilerek veri sorumlusu hakkında 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmektedir.

Konuya ilişkin olarak başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- İlgili kişinin Kanun'un 11 ve 14'üncü maddeleri uyarınca veri sorumlusuna başvuruda bulunmadığı, ilgili kişinin herhangi bir kişisel verisi işlenmediğinden hukuken başvuru için aranan ilgili kişi maddi unsurunun mevcut olmadığı, ilgili kişiye şirketleri tarafından herhangi bir araç satışının yapılmadığı, ilgili kişinin muhafaza edilen şirket bilgilerine erişebilecek imkâna sahip olmadığı,
- Şirketlerinin taksitle ve peşin olmak üzere ikinci el araç satışı yaptığı, taksit ödemeleri müşteriler tarafından yapılmadığı takdirde şirketlerince hukuki yollara başvurularak icra takibi başlatıldığı, müşteriler adına kayıtlı araçlarda haciz ve yakalama işlemlerinin icra müdürlüğü tarafından yapıldığı, yakalanan araçların icra mevzuatı gereğince Yediemin otoparklarına çekildiği, Yedieminlerin otoparka çekilen araçlarda icra dosyası alacaklısını görerek şirketlerine haber verdiği,

bunun dışında hiçbir Yediemin ya da üçüncü kişilerle müşterilerinin icra borcu bilgisinin paylaşılmadığı,

İlgili kişinin belirttiği internet adresi incelendiğinde böyle bir adresin sunucularında mevcut olmadığı ve internet adresinde ilgili kişinin iddialarını ispat edici bir içeriğin mevcut olmaması sebebiyle başvurunun reddinin gerektiği, müşterilere ait kişisel verilerin dijital güvenli bir sunucu ortamında aktarıldığı ve şirket sistemi içinde sadece yetkilendirilmiş kullanıcı adı ve şifresiyle giriş yapan personeller tarafından sorgulama yapılabildiği

ifade edilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 02/11/2021 tarih ve 2021/1110 sayılı Kararı ile;

- Kanun'un amacının kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek olduğu, Kanun'un "Tanımlar" başlıklı 3'üncü maddesinde "ilgili kişi"nin, kişisel verisi işlenen gerçek kişi; "veri sorumlusu"nun ise kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlandığı,

- Kanun'un, kişisel verilerin işlenmesine ilişkin "Genel İlkeler"i düzenleyen 4'üncü maddesinin (1) numaralı fıkrasında, "Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir." hükmünün yer aldığı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin;

a) Hukuka ve dürüstlük kurallarına uygun olma,

b) Doğru ve gerektiğinde güncel olma,

c) Belirli, açık ve meşru amaçlar için işlenme,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı

veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işleniminin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanun'un "Veri Güvenliğine İlişkin Yükümlülükler"i düzenleyen 12'nci maddesinin (1) numaralı fıkrasında veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idarî tedbirleri almak zorunda olduğunun hükme bağlandığı,

- Somut olayda, ihbar dilekçesinin Kurula Cumhurbaşkanlığı İletişim Merkezi (CİMER) üzerinden intikal ettiği, ilgili kişinin dilekçesinde kendisine ait herhangi bir verinin bu internet adresinde paylaşıldığını ya da başka bir suretle işlendiğini iddia etmediği, Kanun'un 15'inci maddesinin birinci fıkrasında yer alan "Kurul, şikayet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapar." hükmü gereğince Kurulun şikayet veya ihbar üzerine inceleme yapabileceği gibi şikayet veya ihbar olmasa dahi görev alanına giren konularda resen inceleme başlatmasının mümkün olduğu, bir veri ihlali iddiasıyla ilgili olarak Kurulun harekete geçmesi için ihlalden etkilenen ilgili kişilerin Kurula şikayet başvurusunda bulunmasının gerekmediği göz önünde bulundurulduğunda CİMER üzerinden iletilen dilekçenin ihbar niteliğinde kabul edilerek Kurulun konu hakkında inceleme başlatılmasına karar verdiği,

- İncelemeye konu internet adresinin veri sorumlusuna Kurum tarafından bilgi ve belge talebi gönderilmesinden önce incelenmesi neticesinde, internet adresinde ilgili kişilerin isimleri, T.C. kimlik numaraları, adresleri, yakalama kararı çıkartılan araçların plakaları ve modelleri ile icra dosyalarının hangi hukuk bürosu tarafından takip edildiği bilgilerinin yer aldığı ve bu bilgiler arasında araç plakası, şehir ve ilçeye göre arama yapılabildiğinin tespit edildiği, Kurum tarafından gönderilen bilgi ve belge talebi yazısı veri sorumlusuna tebliğ edildikten sonra söz konusu internet adresine ulaşılmaya çalışıldığında ise siteye ulaşılamadığı uyarısı alındığı,

- Veri sorumlusu tarafından İcra ve İflas Kanunu hükümleri çerçevesinde borçlu müşterilerden alacağını tahsil etmek için icra takibi başlatılması, malvarlığı sorgulaması sonucu haciz konulması

için kişisel veri işlenmesi Kanun'un 5'inci maddesinin ikinci fıkrasının (a) ve (e) bentlerinde düzenlenen kanunlarda açıkça öngörülme ve bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması hukuki sebeplerine dayanabilirse de bu verilerin herkesin erişimine açık internet ortamında veri sorumlusu tarafından yayımlanmasının herhangi bir veri işleme şartına dayanmadan yapılan hukuka aykırı bir veri işleme faaliyeti olduğu

değerlendirmelerinden hareketle,

- Söz konusu internet adresinde yer alan kişisel verilerin incelemenin başlatıldığı tarihte herkesin erişimine açık olan internet ortamında veri sorumlusu tarafından yayınlanmasının Kanun'un 5'inci maddesi kapsamında herhangi bir veri işleme şartına dayanmadığı kanaatine varıldığından Kanun'un 12'nci maddesinin (1) numaralı fıkrası kapsamında uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı değerlendirilen veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca, ihbara konu internet sitesinde yayınlanmakta olan kişisel verilerin çokluğu ve önemi ile bu verilerin internet ortamında ifşa edilmesi dolayısıyla hukuka aykırı veri işleme faaliyetinin arz ettiği güvenlik riskinin yoğunluğu da dikkate alınarak 200.000 TL idari para cezası uygulanmasına karar verilmiştir.

2021/1107 sayılı KVKK Kararı

İlgili kişinin kredi notunun Banka tarafından düzeltilmemesi ve kişisel verilerinin üçüncü kişilerle paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 02/11/2021 tarihli ve 2021/1107 sayılı Karar Özeti

Karar Tarihi : 02/11/2021

Karar No : 2021/1107

Konu Özeti : İlgili kişinin kredi notunun Banka tarafından düzeltilmemesi ve kişisel verilerinin üçüncü kişilerle paylaşılması

Kuruma intikal eden şikâyetle özetle; ilgili kişi tarafından bireysel kredi kartı ödemesi geciktirilmediği hâlde veri sorumlusu Banka tarafından kanuni takip başlatıldığı ve defalarca ilgili kişinin kredi notunu etkileyen hukuksuz işlemler yapıldığı, ilgili kişinin kredi notunun düşürüldüğü, yapılan itiraz üzerine Banka tarafından bu işlemin düzeltildiği ve kredi notunun yüksek düzeye yeniden çekildiği fakat bu işlemin takip eden aylarda Banka tarafından birkaç kez daha tekrarlandığı ve her seferinde ilgili kişinin ısrarlı tepkileri sonucunda düzeltildiği, finans bilgilerinin gerçeğe aykırı olarak hukuksuz bir biçimde paylaşıldığı, ilgili kişi ile hiçbir finans kurumu arasında kredi, bireysel kart vb. gibi işlemlerin yapılamadığı, ilgili kişinin itibarının zedelendiği ve Bankaya yapılan başvurulara yanıt verilmediği belirtilerek veri sorumlusu hakkında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusunun savunması talep edilmiş olup veri sorumlusunun Kuruma intikal eden cevabi yazısında özetle;

- İlgili kişinin bahsettiği tarihte başvurusunun bulunmadığı fakat başka bir tarihte kendilerine e-posta üzerinden bir şikâyet iletildiği ve aynı tarihte kendisi ile telefonla irtibata geçildiği fakat ilgili kişinin aramaları yanıtlamaması nedeniyle kendisine e-posta ile bilgi verilerek görüşme talebinde bulunduğu ancak Banka tarafından iletilen e-postaya ilgili kişiden herhangi bir yanıt alınmadığı ancak aynı konulu başka tarihteki şikâyetlerinin Banka Genel Müdürlüğüne iletilerek başka bir tarihte yanıtladığı,

• Banka ile kurumlar arasında imzalanan protokoller kapsamında kurumların fatura tahsilatlarına aracılık hizmetinin verildiği ve bu kapsamda ilgili kişinin imzalamış olduğu Bankacılık Hizmetleri Sözleşmesi çerçevesinde verdiği fatura ödeme talimatlarının yerine getirilebilmesi amacıyla fatura ödeme talimatı verilen kurumlarla müşteri işlem; Banka nezdinde kredi ürünlerine ilişkin olarak bankacılık sektörüne yönelik yasal düzenlemelere uyumun sağlanması, Bankanın risk izleme ve bilgilendirme yükümlülüklerinin yerine getirilmesi amacıyla Türkiye Bankalar Birliği Risk Merkezine kimlik, iletişim, müşteri işlem; Banka'nın acentesi olduğu ...Sigorta A.Ş. nezdindeki sigorta poliçelerinin prim ödemeleri ile ilgili olarak söz konusu Şirkete müşteri işlem; ilgili kişinin yasal takipte izlenen kredilerinden kaynaklanan Bankanın alacaklarının tahsili amacıyla anlaşmalı hukuk bürosuna kimlik, iletişim, müşteri işlem, hukuki işlem bilgilerine ilişkin olarak her bir konu özelinde, ilgili amacın gerçekleştirilmesiyle kısıtlı olacak şekilde veri aktarımının gerçekleştirildiği,

İlgili kişinin yurt dışına aktarılan kişisel verisinin bulunmadığı,

• 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu'nun Geçici 28'inci maddesinde Türkiye Cumhuriyet Merkez Bankası nezdinde izlenen risk verilerinin 5411 sayılı Kanun'a göre kurulmuş olan Risk Merkezine aktarılmasının düzenlendiği, aynı Kanun'un Ek 1'inci maddesinde ise; "Türkiye Bankalar Birliği nezdinde, kredi kuruluşları ile Kurulca uygun görülecek finansal kuruluşların müşterilerinin risk bilgilerini toplamak ve söz konusu bilgileri bu kuruluşlar ile gerçek veya tüzel kişilerin kendileriyle ya da onay vermeleri koşuluyla gerçek kişiler ve özel hukuk tüzel kişileri ile de paylaşılmasını sağlamak üzere Risk Merkezi kurulmuştur." düzenlemesinin yer aldığı, anılan hükümler ve Türkiye Bankalar Birliği tarafından yayımlanan Türkiye Bankalar Birliği Risk Merkezi Yönetmeliği ile üye bankaların Risk Merkezine bilgi paylaşımının kapsamı, biçimi ve içeriği ile tarafların yükümlülüklerinin düzenlendiği,

• İlgili kişinin talebi üzerine yapılan incelemede gerçek kişi tacir ilgili kişinin bireysel kredi kartı geri ödemelerinde gecikme olmamasına karşın ticari nitelikli kredi kartından kaynaklanan gecikme nedeniyle gecikme bildirimini yapıldığının anlaşıldığı,

• Bu durumun giderilmesine yönelik olarak gerekli sistem geliştirmesinin planlandığı ve 2020 yılı Mayıs ayı içerisinde gerçekleşecek sistem güncellemesi sonrasında aktif hale geleceği ve konu hakkında Kuruma ayrıca bilgi verileceği, çalışmalar tamamlanuncaya kadar ilgili kişiye ilişkin kayıtların manuel olarak kontrol edilmeye ve gerekirse düzeltilmeye devam edileceği,

Güncelleme işlemlerinin Türkiye Bankalar Birliği Risk Merkezine ait portal üzerinden, kullanıcı ve onaylayıcı olarak yetkilendirilmiş Banka çalışanlarının Bankanın sistemindeki güvenlik kontrollerine uygun şekilde giriş yapması sonrasında gerçekleştirilebildiği, Portaldaki "Acil Güncelleme

Sistemi"ne müşteri T.C. kimlik numarası bilgisinin girilerek gerekli düzeltmenin yapıldığı ve yetkilendirilmiş kullanıcının onayıyla sürecin tamamlandığı ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 02/11/2021 tarih ve 2021/1107 sayılı Kararı ile;

- Kanun'un amacının kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek olduğu, Kanun'un "Tanımlar" başlıklı 3'üncü maddesinde "ilgili kişi"nin, kişisel verisi işlenen gerçek kişi; "veri sorumlusu"nun ise kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlandığı,

- Kanun'un, kişisel verilerin işlenmesine ilişkin "Genel İlkeler"i düzenleyen 4'üncü maddesinin (1) numaralı fıkrasında, "Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir." hükmünün yer aldığı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin;

a) Hukuka ve dürüstlük kurallarına uygun olma,

b) Doğru ve gerektiğinde güncel olma,

c) Belirli, açık ve meşru amaçlar için işlenme,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek

kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanun'un "Kişisel verilerin aktarılması" başlıklı 8'inci maddesinde; kişisel verilerin ilgili kişilerin açık rızası olmaksızın aktarılamayacağı, özel nitelikli olmayan kişisel verilerin ancak Kanun'un 5'inci maddesinin (2) numaralı fıkrasında belirtilen şartlardan birinin varlığı halinde, özel nitelikli kişisel verilerin ise yeterli önlemler alınmak kaydıyla 6'ncı maddesinin (3) numaralı fıkrasında belirtilen şartlardan birinin bulunması halinde ilgili kişinin açık rızası aranmaksızın aktarılabilceğinin düzenlendiği,

- Kanun'un "Veri Güvenliğine İlişkin Yükümlülükler"i düzenleyen 12'nci maddesinin (1) numaralı fıkrasında veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idarî tedbirleri almak zorunda olduğunun hükme bağlandığı,

- 5411 sayılı Kanun'un Geçici 28'inci maddesinin üçüncü fıkrasında; "Merkez Bankası nezdindeki Risk Merkezi bilgileri, bu Kanuna göre kurulan Risk Merkezine aktarılır." hükmü ile aynı Kanun'un Ek 1'inci maddesinde; Risk Merkezine ilişkin ayrıntılı düzenlemelere yer verildiği, ilgili hükmün birinci fıkrası uyarınca Risk Merkezinin; Türkiye Bankalar Birliği nezdinde, kredi kuruluşları ile Bankacılık Düzenleme ve Denetleme Kurulu tarafından uygun görülecek finansal kuruluşların müşterilerinin risk bilgilerini toplamak ve söz konusu bilgileri bu kuruluşlar ile gerçek veya tüzel kişilerin kendileriyle ya da onay vermeleri koşuluyla gerçek kişiler ve özel hukuk tüzel kişileri ile de paylaşılmasını sağlamak üzere kurulmuş olduğu, bu maddenin ikinci fıkrası gereğince; kredi kuruluşları ile Bankacılık Düzenleme ve Denetleme Kurulu tarafından uygun görülecek finansal kuruluşların, Risk Merkezine üye olmak zorunda olduğu ve üye kuruluşların, Risk Merkezince istenilen, müşterileri ile ilgili her türlü bilgiyi vermekle yükümlü olduğunun düzenlendiği, bu açıklamalarda bahsi geçen kredi kuruluşlarının; 5411 sayılı Kanun'un 3'üncü maddesinde, mevduat bankaları ve katılım bankaları olarak açıklandığı,

- 10/04/2012 tarihli ve 28260 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Türkiye Bankalar Birliği Risk Merkezi Yönetmeliğinin (Risk Merkezi Yönetmeliği) 9'uncu maddesi gereğince; Risk Merkezine üye olanlar tarafından Risk Merkezine müşteri ve/veya hesap bazında değişiklikler göstermekle birlikte, kredi limiti, kredi riski, donuk alacak niteliğindeki kredi ve diğer alacaklar,

çekler ve çek hesabı sahibinin bilgileri vb. ile Risk Merkezi Yönetimi tarafından Risk Merkezinin kuruluş amaçları doğrultusunda belirlenen diğer bilgilerin bildirildiği,

- Risk Merkezi Yönetmeliğinin 10'uncu maddesinin birinci fıkrası uyarınca ise; kredi limiti ve kredi riski bilgilerinin müşteri bazında birleştirilerek bu müşteriler hakkında bildirimde bulunan üyelere bildirim dönemi itibariyle topluca bildirildiği, yine aynı Yönetmeliğin 17'nci maddesinin birinci fıkrasının (a) bendinde; Risk Merkezine üye olanların, Risk Merkezi tarafından bu Yönetmelik kapsamında talep edilen her türlü bilgi ve belgeyi zamanında, tam ve gerçeğe uygun olarak vermekle sorumlu olduklarının düzenlendiği,

- Somut olayda veri sorumlusunun, banka niteliğini haiz olmakla birlikte 5411 sayılı Kanun'un Ek 1'inci maddesi uyarınca Risk Merkezine üye olma zorunluluğunun bulunduğu ve gerek 5411 sayılı Kanun gerekse Risk Merkezi Yönetmeliği gereğince; Risk Merkezine müşterilerine ait kredi bilgisi, kredi riski vb. bilgileri bildirmesi gerektiği, bu kapsamda ilgili kişiye ait finans verilerinin veri sorumlusu tarafından Risk Merkezine bildirilmesinin Kanun'un 8'inci maddesi anlamında aktarım anlamına gelmekte olduğu ve söz konusu aktarım faaliyetinin Kanun'un 5'inci maddesinde yer alan işleme şartlarından birine dayanması gerektiği,

- Bu çerçevede, 5411 sayılı Kanun ile Risk Merkezi Yönetmeliği hükümleri kapsamında veri sorumlusunun söz konusu kişisel veri aktarım faaliyetini gerçekleştirmesi gerektiği, dolayısıyla veri sorumlusunun ilgili kişinin finans verilerini Risk Merkezine bildirmesinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (a) bendinde yer alan; "Kanunlarda açıkça öngörülmesi" ile (ç) bendinde yer alan "Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" şartları kapsamında olduğu,

- Kanun'un "Genel ilkeler" başlıklı 4'üncü maddesi uyarınca, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği ve kişisel verilerin işlenmesinde maddede; "a) Hukuka ve dürüstlük kurallarına uygun olma. b) Doğru ve gerektiğinde güncel olma. c) Belirli, açık ve meşru amaçlar için işlenme. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme." şeklinde sayılan ilkelere uyulmasının zorunlu olduğu, anılan madde hükmünden açıkça anlaşılacağı üzere, kişisel verilerin işlenmesinde her hal ve şartta Kanun'un 4'üncü maddesinde sayılan genel ilkelere uyulmasının hukuki bir gereklilik olduğu,

- Bu ilkelere "Doğru ve gerektiğinde güncel olma" ilkesinin, Kanun'un 11 inci maddesinde düzenleme altına alınan ve ilgili kişinin haklarından biri olan kişisel verilerin düzeltilmesini talep etme hakkı ile doğrudan ilgili olduğu, kişisel verilerin doğru ve gerektiğinde güncel olmasının

sağlanması noktasında aktif özen yükümlülüğünün; veri sorumlusu eğer bu verilere dayalı olarak ilgili kişiyle alakalı bir sonuç ortaya koyuyor ise geçerli olduğu (örneğin kredi verme işlemleri),

- Somut olay bakımından, kişisel verilerin doğru ve gerektiğinde güncel olmasının sağlanması bakımından, veri sorumlusu Banka'nın aktif özen yükümlülüğü altında olduğu, zira, kredi verme, kredi kartı kullanımı, hesap özeti çıkarılması gibi işlemler bakımından banka hesap bilgilerinin güncelliğinin önem arz ettiği,

- Söz konusu verilerin yalnızca veri sorumlusu bünyesinde tutulmadığı ve pek çok kredi ve finans kuruluşunun erişebildiği Risk Merkezine de aktarıldığı, bununla birlikte, veri sorumlusu Banka'nın, Risk Merkezi Yönetmeliğinin 17'nci maddesinin birinci fıkrasının (a) bendi gereğince de; Risk Merkezi tarafından bu Yönetmelik kapsamında talep edilen her türlü bilgi ve belgeyi zamanında, tam ve gerçeğe uygun olarak verme sorumluluğu bulunduğu,

- Öte yandan, Kanun'un "İlgili kişinin hakları" başlıklı 11'inci maddesi uyarınca; herkesin, veri sorumlusuna başvurarak kendisiyle ilgili; kişisel veri işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerinin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme, Kanun'un 7 nci maddesinde öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, 11 inci maddenin birinci fıkrasının (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme haklarına sahip olduğu ve bu kapsamda ilgili kişilerin, kişisel verilerinin eksik veya yanlış işlenmesi halinde, bunların düzeltilmesini talep etme hakkının bulunduğu,

- Somut olay bakımından, Kuruma intikal eden belgeler incelendiğinde, veri sorumlusu Banka tarafından ilgili kişiye cevap verildiği ancak konuyu aydınlatacak ve ilgili kişinin şikâyetini çözümleyecek derecede yeterli bir cevap verilmediği,

- Zira ilgili kişinin farklı zamanlarda veri sorumlusu ile e-posta yoluyla iletişime geçerek Risk Merkezine yanlış aktarılan finans verilerinin düzeltilmesini tekraren talep ettiğinin görüldüğü,

- İlgili kişi tarafından veri sorumlusuna iletilen, sair tarihlerdeki e-postaların tamamının aynı konuya ilişkin olduğu, veri sorumlusu tarafından bu durumun giderilmesine yönelik olarak gerekli sistem

geliştirmesinin planlandığı ve 2020 yılı Mayıs ayı içerisinde gerçekleşecek sistem güncellemesi sonrasında aktif hale geleceği ve konu hakkında Kuruma ayrıca bilgi verileceği ve çalışmalar tamamlanuncaya kadar ilgili kişiye ilişkin kayıtların manuel olarak kontrol edilmeye ve gerekirse düzeltilmeye devam edileceği belirtilmiş olup, yazının farklı birçok tarihe ilişkin “Acil Güncelleme Sistemi” ekran görüntülerine yer verildiğinin görüldüğü,

- Söz konusu ekran görüntüleri incelendiğinde; ilgili kişiye ait hesap kaydı detaylarının revize edildiği, veri sorumlusundan alınan yazıda bahsedilen sistem geliştirmelerinin tamamlandığı, yapılan geliştirmenin sonuçlarının titizlikle izlendiği ve bu süreçte, ilgili kişiye ilişkin Risk Merkezi bildirimlerinde düzeltme gerektiren bir hususa rastlanmadığı ve yapılan geliştirmenin başarılı olarak sonuçlandırıldığına teyit edildiğinin belirtildiği, bu kapsamda veri sorumlusu tarafından ilgili kişinin Risk Merkezine yanlış aktarılan kişisel verilerinin düzeltilmesi talebinin veri sorumlusu tarafından yerine getirildiği,

- Öte yandan, her ne kadar ilgili kişinin yanlış işlenen kişisel verileri veri sorumlusu tarafından ilgili kişinin talebi doğrultusunda düzeltilmiş olsa da başlangıçta gerçeğe aykırı olarak işlenen ve Risk Merkezine aktarılan kişisel veriler bakımından hukuka aykırı bir kişisel veri işleme faaliyetinin gerçekleştirildiği, veri sorumlusu tarafından gerek manuel düzeltmeler yapılması gerek sistemsel iyileştirmelere gidilmesi suretiyle ilgili kişinin talebi yerine getirilmiş olsa dahi, ilgili kişinin veri sorumlusunun bir dönem Kredi Kayıt Bürosuna yaptığı hatalı raporlamalar suretiyle kişisel verilerinin yanlış işlendiği dikkate alındığında veri sorumlusunun kişisel verilerin hukuka aykırı işlenmesini önlemek üzere gerekli idari ve teknik tedbirleri almadığının anlaşıldığı,

- Zira, Kanun’un 4’üncü maddesinde düzenlenen genel ilkelere bütün kişisel veri işleme faaliyetleri bakımından riayet edilmesi gerekmektedir, somut olay bakımından veri sorumlusunun işlediği kişisel verilerin doğru ve güncel tutulması bakımından aktif özen yükümlülüğünün bulunduğu,

- Bir kişisel veri işleme faaliyetinin hukuka uygunluk arz edebilmesi için gerek Kanun’un 5’inci ve 6’ncı maddesindeki işleme şartlarından birinin varlığı gerek Kanun’un 4’üncü maddesinde düzenlenen genel ilkelere uygunluğun sağlanması gerektiği, somut olay bakımından da, veri sorumlusu tarafından yanlış işlenen kişisel verilerin Risk Merkezine aktarılması sonucunda ortaya çıkan finansal durumdan ötürü ilgili kişinin mağduriyet yaşadığı ve zarara uğratıldığı

değerlendirmelerinden hareketle,

- İlgili kişiye ait kişisel veri niteliğini haiz kredi notu bilgisinin veri sorumlusu tarafından yanlış işlenmesi ve Risk Merkezine aktarılmasının Kanun’un 4’üncü maddesinde yer alan genel ilkelerden;

“dođru ve gerektiđinde güncel olma” ilkesine aykırılık teşkil ettiđi dikkate alındıđında, Kanun’un 12’nci maddesinin (1) numaralı fıkrasının (a) bendinde bulunan “...Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek...” yükümlülüđüne aykırı davranan veri sorumlusu hakkında;

- Veri sorumlusunun bankacılık sektöründe oldukça büyük bir güce sahip olması,
- Veri sorumlusunun oldukça fazla sayıda müşteri ve potansiyel müşteri ile irtibat halinde olması, çeşitlilik arz eden konulara yönelik iletişim kurabilmesi ve bu konularda ilgili kişiler hakkında işlem tesis edebilmesi,
- Veri sorumlusunun banka niteliđini haiz olması dolayısıyla, işlediđi kişisel veriler üzerinden ilgili kişiler hakkında sonuç elde etmesi ve bu sonuçlar doğrultusunda iş ve eylemlerini gerçekleştirmesi nedeniyle işlenen kişisel veriler bakımından doğruluk ve güncelliđin sağlanması adına aktif özen yükümlülüđünün bulunması,
- Veri sorumlusunun işlediđi kişisel verileri düzenli ve sistematik olarak Risk Merkezine bildirme yükümlülüđünün bulunması ve bu sisteme bildirilen veriler üzerinden, ilgili kişiler hakkında finansal anlamda önemli sonuçların oluşturulması nedeniyle yanlış bildirilen kişisel verilerin ilgili kişilerin mağduriyetlerine yol açabilmesi

hususları da göz önünde bulundurularak Kanun’un 18’inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 150.000 TL idari para cezası uygulanmasına,

- İlgili kişi başvurularına Kanun ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliđ’de belirlenen usule uygun ve yeterli bir cevap verilmesi gerektiđinin veri sorumlusuna hatırlatılmasına karar verilmiştir.

2021/1104 sayılı KVKK Kararı

Banka tarafından ilgili kişinin cep telefonu numarasına SMS gönderilmesi suretiyle kişisel verilerinin hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 02/11/2021 tarihli ve 2021/1104 sayılı Karar Özeti

Karar Tarihi : 02/11/2021

Karar No : 2021/1104

Konu Özeti : Banka tarafından ilgili kişinin cep telefonu numarasına SMS gönderilmesi suretiyle kişisel verilerinin hukuka aykırı olarak işlenmesi

İlgili kişinin Kuruma intikal eden şikâyetinde özetle; verilerinin silinmesi için veri sorumlusu Bankadan talepte bulunduğu, Banka tarafından verilen cevapta bu hususta gerekli işlemlerin yapıldığının belirtildiği, buna rağmen Bankadan SMS ve e-posta ile bilgilendirme mesajları gönderilmeye devam edildiği ve bu hususta Bankaya başvurulduğu, verilen yanıtta “Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik” düzenlemesinin gerekçe gösterildiği belirtilerek veri sorumlusu hakkında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusunun savunması talep edilmiş olup veri sorumlusu tarafından Kuruma intikal ettirilen cevabi yazıda özetle;

- Banka ile ilgili kişi arasındaki müşteri ilişkisinin 2005 yılında başladığı, ilgili kişinin talebi üzerine Banka nezdindeki aktif ürünlerinin 03.08.2019 tarihinde kapatıldığı,
- İlgili kişinin Banka nezdinde demografik bilgilerinin (ad, soyadı, T.C. kimlik no, baba adı, anne adı, doğum tarihi, cinsiyet, doğum, doğum ülkesi, yerleşik ülke, vergi kimlik numarası, öğrenim bilgisi, medeni durum), meslek bilgisinin, anne kızlık soyadının, iletişim adreslerinin (telefon, cep telefonu, adres, e-posta), hesap numarası/IBAN bilgisi, banka tarafından üretilen müşteri numarası, kredi kartı müşterisi olması sebebiyle kredi kartı numarası gibi kişisel verilerinin işlendiği,
- İlgili kişinin Bankadan almış olduğu ürün ve hizmetler nedeniyle kurduğu ilişki kapsamında; Kişisel Verilerin Korunması Kanunu’nun (Kanun) 5’inci maddesinin (2) numaralı fıkrasında yer alan; kanunlarda açıkça öngörülmesi, Banka ile imzalanan sözleşme veya bu sözleşmenin yerine getirilmesiyle doğrudan ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin

işlenmesinin gerekli olması, Bankanın hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, bir hakkın oluşması, kullanılması veya korunması için veri işlemenin zorunlu olması ve aynı maddede düzenlenen müşterilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Bankanın meşru menfaatleri için veri işlenmesinin zorunlu olması sebepleriyle; özel nitelikli kişisel veriler için ise Kanun'un 6'ncı maddesinin (2) numaralı fıkrasına göre müşterilerin açık rızasının bulunması hukuki sebepleriyle kişisel verilerinin işlendiği,

- İlgili kişinin 06.01.2020 tarihinde Banka'ya başvurarak, Banka'nın kredi kartı müşterisi olduğu, kredi kaydını kapattırması sebebi ile Banka nezdindeki tüm kişisel verilerinin silinmesini talep ettiği,
- 6102 sayılı Türk Ticaret Kanunu'nun 82'nci maddesi, 5411 sayılı Bankacılık Kanunu ile Bankacılık Düzenleme ve Denetleme Kurumu'nun Bankaların Muhasebe Uygulamalarına ve Belgelerin Saklanması İlişkin Usul ve Esaslar Hakkında Yönetmelik'in 17'nci maddesi gereğince, Bankaların müşterilerine ait her türlü bilgi ve belgeyi on yıl süreyle saklamakla yükümlü olduğu, on yıllık saklama süresinin son işlem tarihi olan hesap ve ürünlerin kapanma tarihinden itibaren başladığı,
- Banka nezdinde muhafaza edilen müşteri bilgilerine ilişkin 10 yıllık saklama süresinin henüz dolmadığı dikkate alınarak ilgili kişinin kişisel verilerinin silinmesi talebine olumlu yanıt verilemediği ancak kişisel verilerin ikincil amaçlarla işlenmemesi adına Banka nezdinde gerekli adımların atıldığı,
- 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 4'üncü maddesinde yer verilen genel ilkelere uygun olarak kişisel verilerin saklama amacı dışında işlenmemesi için gerekli tedbirlerin alındığı, ilgili kişinin ticari elektronik ileti gönderilmesine ilişkin tüm tercihlerinin hiçbir kanaldan ulaşılmaması yönünde güncellendiği, verilerinin saklanması için gerekli hukuki sebep haricinde pazarlama gibi ikincil amaçlarla işlenmemesinin sağlanacağı yönünde ilgili kişiye cevap verildiği,
- İçişleri Bakanlığı'nın ve İl Hıfzıssıhha Kurullarının, Umumi Hıfzıssıhha Kanunu hükümleri doğrultusunda ve Banka'nın uymakla zorunlu olduğu tedbirler kapsamında özellikle pandeminin ülkemizde görüldüğü ilk aylardan itibaren sokağa çıkma yasağı kısıtlaması bulunan illerdeki Banka şubelerinin çalışma gün ve saatleri, genel olarak tüm şubelerinin çalışma saatleri, salgının yayılmasını önlemeye yönelik ve toplum sağlığını korumaya destek olmak amacıyla Banka tarafından alınan önlemlerin geçmişte Bankadan hizmet almış eski müşterileri olmak üzere tüm müşterilerine duyurulması ve bu konuda bilgilendirme yapma ihtiyacının hasıl olduğu,

- Bu gerekçelerle ilgili kişi müşterinin Banka’da kayıtlı telefon numarasına koronavirüs salgınının yayılmasını önlemeye yönelik ve toplum sağlığını korumaya destek olmak amacıyla Banka tarafından alınan önlemlerin duyurulduğu birtakım bilgilendirme SMS'lerinin gönderildiği,
- Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik’e uygun olarak, Banka nezdinde yapılan zorunlu iletişim konularının; “ Ürün ve hizmetlerimize ilişkin değişiklik ve kullanıma yönelik iletiler, devam eden ürün ve hizmetlerle ilgili tahsilat, borç hatırlatma, bilgi güncelleme, satın alma ve teslimat veya benzeri durumlara ilişkin bildirimleri içeren iletiler, ilgili mevzuata göre bilgi verme yükümlülüğümüz bulunan durumlar” şeklinde tanımlandığı,
- Bankanın hukuken bilgi verme yükümlülüğünün bulunduğu durumlarda önceden onay alma zorunluluğunun bulunmadığı ve ilgili mevzuatta öngörülen bu durumlarda ilgili kişilerin de ret hakkını kullanamayacağına yukarıda sözü edilen Yönetmeliğin 9’uncu maddesinin 1’inci fıkrasında tekraren vurgulandığı, söz konusu hükme göre ilgili kişinin reddetme hakkını kullanmış olmasının hizmet sağlayıcı olarak Banka’nın tabi olduğu ilgili mevzuat hükümlerine göre alıcı sıfatını taşıyan kişilere gönderilmesi zorunlu olan bildirimlerin yapılmasına engel teşkil etmediği,
- Kanun’un 5’inci maddesinin (2) numaralı fıkrasının (a) bendinde düzenlenen kanunlarda açıkça öngörülmesi ve (ç) bendinde düzenlenen Bankanın hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması hukuki sebeplerinin ilgili kişilerin açık rızası olmadan kişisel verilerinin işlenebileceği durumları düzenlediği

ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 02/11/2021 tarih ve 2021/1104 sayılı Kararı ile;

- Kanun’un amacının kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek olduğu, Kanun’un “Tanımlar” başlıklı 3’üncü maddesinde “ilgili kişi”nin, kişisel verisi işlenen gerçek kişi; “veri sorumlusu”nun ise kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlandığı,
- Kanun’un, kişisel verilerin işlenmesine ilişkin “Genel İlkeler”i düzenleyen 4’üncü maddesinin (1) numaralı fıkrasında, “Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.” hükmünün yer aldığı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin;

a) Hukuka ve dürüstlük kurallarına uygun olma,

b) Doğru ve gerektiğinde güncel olma,

c) Belirli, açık ve meşru amaçlar için işleme,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işleme zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanun'un "Veri Güvenliğine İlişkin Yükümlülükler"i düzenleyen 12'nci maddesinin (1) numaralı fıkrasında veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idarî tedbirleri almak zorunda olduğunun hükmüne bağlandığı,

- Kanun'un 5'inci maddesi çerçevesinde kişisel veri işleme şartları mevcut olsa dahi, kişisel verilerin işlenmesinde aynı zamanda, Kanun'un 4'üncü maddesinde yer alan ilkelere de uygun hareket edilmesi gerektiği, aksi halde, kişisel verilerin işlenmesine ilişkin hukuki şartlar geçerli olsa dahi hukuka aykırı veri işleme durumunun söz konusu olacağı,

- Veri sorumlusunun, toplanan kişisel verilerin işleme amacını açık ve kesin olarak belirlemesi ve ilgili kişiye belirtilen amaçlar dışında başka amaçlarla kişisel verileri işlememesi gerektiği, amaçla sınırlı olma ilkesi uyarınca kişisel verilerin işlenmesinin belirlenen amaçların gerçekleştirilmesine

elverişli olması ve yine bu ilke uyarınca amaç için gerekli olan süreye uygun olarak da muhafaza edilmesi gerektiği, Kişisel Verilerin Korunması Kanunu'nun gerekçesinde "(...) sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik veri işlenebilmesi için, işlemeye ilk kez başlıyor gibi, 5 inci maddede düzenlenmiş olan kişisel verilerin işleme şartlarından birinin gerçekleşmesi gerekecektir" ifadesinin yer aldığı,

- Şikâyete konu SMS'lerin gönderildiği döneme ilişkin, yeni tip Covid 19 salgını ile mücadele kapsamında İçişleri Bakanlığı'nın 81 İl Valiliği'ne, büyükşehir statüsündeki 30 il ile Zonguldak'ta 30.04.2020 günü saat 24.00 ile 03.05.2020 günü saat 24.00 arasında sokağa çıkma kısıtlamasının uygulanacağına ilişkin 03.04.2020 tarih ve 6235 sayılı Sokağa Çıkma Kısıtlaması Genelgesini gönderdiği, genelgede bankalar başta olmak üzere yurt çapında yaygın hizmet ağı olan kurum, kuruluş ve işletmelerin bilgi işlem merkezleri ile çalışanlarının asgari sayıda olmak kaydıyla sokağa çıkma kısıtlamasından muaf tutulanlar listesinde belirtildiğinin görüldüğü,

- İlgili kişinin müşterisi olduğu Banka'ya kendisine ait iş ve işlemlerde ulaşılması adına vermiş olduğu telefon numarası bilgisinin, Banka nezdindeki hesaplarını kapatmış olmasına diğer bir ifadeyle pasif hale getirmiş olmasına ve Bankanın da kişisel verilerin saklama amacı dışında işlenmeyeceği yönünde ilgili kişiye cevap vermiş olmasına rağmen, veri sorumlusu tarafından başlangıçta alınan işleme amacından başka bir amaçla SMS göndermek suretiyle ilgili kişinin kişisel verilerini işleminin farklı bir işleme amacına hizmet ettiği,

- Kişisel verilerin işlenmesinde Kanun'un 5'inci maddesinde düzenlenen işleme şartlarından birine dayanılması gerektiği ancak somut olayda bilgilendirme içerikli mesajların iletilmesi suretiyle ilgili kişinin kişisel verisinin işlenmesinde Kanun'un 5'inci maddesinde yer alan herhangi bir işleme şartının bulunmadığı, öte yandan işlemin Kanun'un 4'üncü maddesinde yer alan kişisel verilerin işlenmesinde "belirli, açık ve meşru amaçlar için işleme" ve "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerine uyulması zorunluluğuna da aykırı olduğu dikkate alındığında Kanun'un 12'nci maddesinin (1) numaralı fıkrasının (a) bendi uyarınca veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almadığı kanaatine varıldığı,

- Diğer taraftan, 5411 sayılı Bankacılık Kanunu'nun 42'nci maddesinde; alınan yazıların ve faaliyetler ile ilgili belgelerin asıllarının veya bunun mümkün olmadığı hallerde sıhhatlerinden şüpheye mahal vermeyecek kopyalarının ve yazılan yazıların makine ile alınmış, tarih ve numara sırası verilerek düzenlenecek suretlerinin, usulleri çerçevesinde ilgili banka nezdinde on yıl süreyle saklanacağı hükme bağlandığı,

- 5411 sayılı Bankacılık Kanunu'nun 42'nci maddesine dayanılarak hazırlanan Bankaların Muhasebe Uygulamalarına ve Belgelerin Saklanması İlişkin Usul ve Esaslar Hakkında Yönetmelik'in 17'nci maddesinin (1) numaralı fıkrasında ise "Bankaların, müşterilerinden ve resmî ya da özel kurum ve kuruluşlardan aldıkları mektup, telgraf, elektronik posta mesajı, ilam ve tebligatlar ile diğer yazıları ve Bankaların İç Sistemleri Hakkında Yönetmelik uyarınca hazırlayacakları raporlar da dahil olmak üzere, faaliyetleri ile ilgili belgelerin asıllarını veya mümkün olmadığı hallerde sıhhatlerinden şüpheye mahal vermeyecek kopyalarını ve müşterilerine ve resmî ya da özel kurumlara yazdıkları yazıların makine ile alınmış, tarih ve numara sırası verilerek düzenlenecek suretlerini istenildiğinde ibraz edilebilecek şekilde nezdlerinde on yıl süreyle saklamaları zorunludur." hükmünün yer aldığı,

- Dolayısıyla veri sorumlusu tarafından ilgili kişinin kişisel verilerinin silindiğine ilişkin herhangi bir beyanda bulunulmadığı, sadece hesapların kapatıldığı ve pazarlama amaçlı olarak kişisel verilerin işlenmeyeceğine yönelik ticari ileti iletilmesine dair tercihlerin hiçbir kanaldan ulaşılmaması yönünde güncellendiği bilgisinin verildiğinin anlaşıldığı,

- Öte yandan veri sorumlusunun sunduğu belgeler ile 5411 sayılı Kanun'un 42'nci maddesinde belirtilen 10 yıl saklama süresi hükmü ve 6698 sayılı Kanun'un 4'üncü maddesinde belirtilen "İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" ilkesinin birlikte değerlendirilmesi neticesinde, ilgili kişinin banka nezdindeki son işleminin 03.08.2019'da gerçekleştirilen aktif ürünlerinin kapatılması işlemi olduğu ve dolayısıyla son işlem tarihi üzerinden 10 yıllık sürenin geçmemiş olduğu dikkate alındığında; ilgili kişinin kişisel verilerinin işlenmesini gerektiren sebeplerin henüz ortadan kalkmaması sebebiyle silme talebinin veri sorumlusu tarafından yerine getirilmemesinin hukuka aykırı olmadığı

değerlendirmelerinden hareketle,

- İlgili kişinin kişisel verilerinin silinmesi talebi ile ilgili olarak Bankanın kişisel verilerin saklama amacı dışında işlenmeyeceği yönünde ilgili kişiye verdiği cevaba rağmen Banka tarafından bilgilendirme amaçlı SMS göndermek suretiyle ilgili kişinin kişisel verilerini işleminin Kanun'un 5'inci maddesinde yer alan herhangi bir işleme şartına dayanmadığı dikkate alındığında, Kanun'un 12'nci maddesinin (1) numaralı fıkrasında yer alan yükümlülüklerini yerine getirmeyen veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 50.000 TL idari para cezası uygulanmasına,

- İlgili kişinin veri sorumlusu banka nezdindeki son işleminin 03.08.2019'da gerçekleştirilen aktif ürünlerinin kapatılması işlemi olduğu ve dolayısıyla son işlem tarihi üzerinden 10 yıllık sürenin

geçmemiş olduđu dikkate alındığında; ilgili kişinin kişisel verilerinin işlenmesini gerektiren sebeplerin henüz ortadan kalkmaması sebebiyle silme talebinin veri sorumlusu tarafından yerine getirilmemesinin hukuka aykırı olmadığı kanısına varıldığından bu hususta 6698 sayılı Kanun kapsamında yapılacak bir işlemin olmadığına

karar verilmiştir.

2021/1069 sayılı KVKK Kararı

Bankanın avukatı tarafından borçlu yakını olan ilgili kişiye haciz ihbarnamesi gönderilmesi suretiyle kişisel verilerinin işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 21/10/2021 tarihli ve 2021/1069 sayılı Karar Özeti

Karar Tarihi : 21/10/2021

Karar No : 2021/1069

Konu Özeti : Bankanın avukatı tarafından borçlu yakını olan ilgili kişiye haciz ihbarnamesi gönderilmesi suretiyle kişisel verilerinin işlenmesi

İlgili kişinin Kuruma intikal eden şikâyetinde özetle; borçlu yakını olarak bir Banka avukatınca kendisine İcra İflas Kanunu'nun 89'uncu maddesinin (1) numaralı fıkrası kapsamında gönderilen haciz ihbarnamesi ile kişisel verilerinin açık rızası alınmaksızın ihbarnamede yer alan üçüncü kişilerle paylaşıldığını tespit ettiği ve bu konuya ilişkin olarak hem Banka'ya hem de Banka avukatına başvurulduğu belirtilerek veri sorumlusu hakkında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde hem Banka'nın hem Banka Avukatının savunması talep edilmiş olup Banka tarafından Kuruma intikal eden cevabi yazıda özetle;

- Banka'nın alacağını tahsil etmek amacıyla 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 4'üncü maddesinde yer alan işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine uygun olarak yasal takip ve diğer hukuki işlemler için gerekli kişisel verileri işlediği,
- Söz konusu kişisel verilerin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (a) ve (ç) bentleri uyarınca kanunlarda açıkça öngörülmesi ve veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması hukuki sebeplerine dayanılarak Banka'nın sözleşmeli avukatına aktarıldığı,
- Gerek ilgili kişi gerek birinci haciz ihbarnamesi gönderilen üçüncü kişilere ait hiçbir kişisel verinin Banka tarafından paylaşılmadığı,

- İcra İflas Kanunu'nun 89'uncu maddesinde borçluya ait olmakla beraber üçüncü kişilerde bulunan hak ve alacakların haczinin düzenlendiği, birinci haciz ihbarnamesinin alacaklı vekilinin bildirdiği kişilere İcra Müdürlüklerince gönderildiği,
- Düzenlenen ve gönderilen birinci haciz ihbarnamesinin İcra Müdürlüğü tarafından bizzat düzenlendiği ve gönderildiği, bankanın sözleşmeli avukatının ihbarnameye müdahale imkânı olmadığı, ihbarnamenin elektronik imzalandığı, Banka'nın şikayet konusu hususta herhangi bir sorumluluğunun bulunmadığı,
- İlgili kişinin ürün ve hizmetleri kullanması nedeniyle başvurusu sırasında elde edilen kimlik bilgileri, iletişim bilgileri, finans bilgileri, müşteri işlem bilgileri kategorisindeki kişisel verilerinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (c) bendi uyarınca bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması hukuki sebebine dayalı olarak başvuru ürün ve hizmetleri (vadesiz TL, ATM kartı, fastpay, internet/mobil bankacılığı yetkisi, sigorta, maaş ödemesi, fatura ödemesi, EFT işlemleri) sunabilmek amacıyla işlendiği,
- Müşteriye sunulan aydınlatma metninde kişisel verilerin hangi amaç ve sebeplerle işlendiğinin belirtildiği ifade edilmiştir.

Bankanın avukatı tarafından Kuruma intikal eden cevabi yazıda ise özetle;

- Borçlunun borcunu ödememesi sebebiyle kendisine ihbarname gönderildiği, ihbarnameye rağmen borcun ödenmemesi üzerine müvekkili Banka'nın alacağını tahsil amacıyla borçlu hakkında icra takibi başlatıldığı, borcun ödenmemesi üzerine icra müdürlüğünden haciz işlemlerinin başlatılması için talepte bulunulduğu, ancak yapılan sorgular neticesinde borçlunun SGK, araç ve tapu kaydının pasif olduğunun tespit edildiği,
- Borçlunun üçüncü şahıslarda olan alacaklarının haczi için bankalara İcra İflas Kanunu'nun 89'uncu maddesinin (1) numaralı fıkrası kapsamında haciz ihbarnamesi gönderildiği ve bankalardan olumsuz cevapların geldiği,
- Menkul malların haczedilmesi için borçlunun adresine hacze gidildiği ancak adresten ayrıldığı tespit edildiği,
- Menkul haczinden sonra borçlunun MERNİS kaydını düşürdüğü ve şu anda MERNİS adresinin bulunmadığının UYAP sorgu sonucuyla sabit olduğu,

- Diğer tüm girişimlerin olumsuz çıkması sonucunda, müvekkilinin alacağı tahsili amacıyla borçlunun hak ve alacaklarının haczi için yapılan rutin işlemler arasında yer alan üçüncü kişilere haciz ihbarnamesi gönderilmesinin İcra Müdürlüğü'nden talep edildiği,
- Bu talebin hukuki gerekçesinin, para alış veriřlerinin aile bireyleri arasında çok sık rastlanılması ve ayrıca rızai miras sözleşmelerine çok sık rastlanılmasından kaynaklandığı,
- İcra müdürlüğü tarafından talebin uygun görülerek üçüncü kişilere İcra İflas Kanunu'nun 89'uncu maddesinin (1) numaralı fıkrası kapsamında haciz ihbarnamesi hazırlandığı ve gönderildiği,
- Haciz müzekkeresi icra müdürlüğü tarafından, matbu şablon müzekkere örneği üzerinden hazırlanmış olduğundan üçüncü kişilerin tamamına aynı müzekkere içerisinde haciz ihbarnamesi gönderildiği,
- Yapılan işlemlerin tamamında İcra Müdürlüğü'nün karar ve onayı olduğu,
- İcra müdürlüğünce hazırlanan haciz ihbarnamesinin, üçüncü kişilere Kanun'un 5'inci maddesinin (2) numaralı fıkrası kapsamında kanunlarda açıkça öngörölme şartına uygun olarak gönderildiği,
- İcra Müdürlüğü tarafından hazırlanıp gönderilen haciz ihbarnamesi haricinde üçüncü kişiler hakkında başka bir işlem yapılmadığı, bu nedenle kişisel verilerin işlenmesi gibi bir durumun söz konusu olmadığı ve müştekinin icra dosyasında taraf olarak yer almadığı için kişisel verilerin depo edilmesi gibi bir durumun da oluşmadığı
- İlgili kişi tarafından İcra Müdürlüğüne gönderilen haciz ihbarnamesine cevaben borçlunun kendisinde herhangi bir alacağı bulunmadığına ilişkin beyan dilekçesinin icra dosyasına sunulduğu, bu cevaba istinaden haciz ihbarnamesinin fekki için talepte bulunulduğu ve İcra Müdürlüğünce fek müzekkeresi hazırlanarak üçüncü kişilere tebliğ edildiği, bu nedenle kişisel verilerin saklanması, imha edilmemesi gibi bir durumun söz konusu olmadığı ve hiçbir kişisel verinin saklanmadığı ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde, Kişisel Verileri Koruma Kurulunun 21/10/2021 tarih ve 2021/1069 sayılı Kararı ile;

- Kanun'un amacının kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek olduğu, Kanun'un "Tanımlar" başlıklı 3'üncü maddesinde "ilgili kişi"nin, kişisel verisi işlenen gerçek kişi; "veri sorumlusu"nun ise kişisel

verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlandığı,

- Kişisel verilerin hangi amaç ve vasıtayla işleneceğini belirleyip veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olduğu tanımından hareketle somut olayda İcra İflas Kanunu'nun 89'uncu maddesinin (1) numaralı fıkrası kapsamında düzenlenen haciz ihbarnamesinde yer alan üçüncü kişilerin alacaklı vekili tarafından icra müdürlüğüne bildirilmesi nedeniyle veri sorumlusunun Banka Avukatı olduğunun görüldüğü,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi; fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin kendisi tarafından alenileştirilmiş olması; bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükmünün yer aldığı,

- İcra İflas Kanunu'nun 89'uncu maddesinde " (1) Hamiline ait olmıyan veya cirosu kabil bir senetle müstenit bulunmıyan alacak veya sair bir talep hakkı veya borçlunun üçüncü şahıs elindeki taşınır bir malı haczedilirse icra memuru; borçlu olan hakiki veya hükmi şahsa bundan böyle borcunu ancak icra dairesine ödiyebileceğini ve takip borçlusuna yapılan ödemenin muteber olmadığını veya malı elinde bulunduran üçüncü şahsa bundan böyle taşınır malı ancak icra dairesine teslim edebileceğini, malı takip borçlusuna vermemesini, aksi takdirde malın bedelini icra dairesine ödemek zorunda kalacağını bildirir (Haciz ihbarnamesi). Bu haciz ihbarnamesinde, ayrıca 2, 3 ve 4'üncü fıkra hükümleri de üçüncü şahsa bildirilir. (2) Üçüncü şahıs; borcu olmadığı veya malın yedinde bulunmadığı veya haciz ihbarnamesinin tebliğinden önce borç ödenmiş veya mal istihlak edilmiş veya kusuru olmaksızın telef olmuş veya malın borçluya ait olmadığı veya malın kendisine rehnedilmiş olduğu veya alacak borçluya veya emrettiği yere verilmiş olduğu gibi bir iddiada ise, keyfiyeti, haciz ihbarnamesinin kendisine tebliğinden itibaren yedi gün içinde icra dairesine yazılı veya sözlü olarak bildirmeye mecburdur. " hükmünün yer aldığı,

- Bu kapsamda, veri sorumlusunun vekili olduđu Banka adına borçlu tarafın yakınlarına 89/1 haciz ihbarnamesi göndermesinde, Bankanın haklarını ve menfaatlerini korumak amacıyla hareket ettiđi, bu anlamda Avukatlık Kanunu'ndan kaynaklanan yükümlülükleri ve yürütmekte olduđu icra işlemleri bakımından İcra İflas Kanunu ve ikincil mevzuat düzenlemelerinden kaynaklanan yükümlülüklerini yerine getirmek amacıyla ilgili birim/mercilere bildirme yetkisi olduđu ve bu bağlamda işlediđi kişisel verilerin Kanun'un 5' inci maddesinin (2) numaralı fıkrası çerçevesinde ilgili kişinin açık rızası olmaksızın işleminin kanuna uygun olacağı kanaatine varıldıđı

deđerlendirmelerden hareketle;

- Bankanın somut olayda veri sorumlusu olmaması nedeniyle Kanun kapsamında hakkında yapılacak bir işlem olmadığına,

- Avukat tarafından vekili olduđu bankanın alacağını tahsil etmek amacı ile yürütmekle yükümlü olduđu işlemlerin tesisi için üçüncü kişilere İcra ve İflas Kanunu'nun 89'uncu maddesinin (1) numaralı fıkrası kapsamında haciz ihbarnamesi gönderilmesi amacıyla ilgili kişinin adı, soyadı, kimlik numarası ve adres bilgisinin işlenmesi Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (e) bendinde yer alan "bir hakkın tesisi, kullanılması veya korunması için veri işleminin zorunlu olması hükmü" kapsamında Kanuna uygun olduđu deđerlendirildiđinden söz konusu şikâyet ile ilgili olarak veri sorumlusu Avukat hakkında da Kanun kapsamında tesis edilecek bir işlem olmadığına

karar verilmiştir.

2021/1051 sayılı KVKK Kararı

İş arama ve işe alım süreçlerini yürüten bir istihdam platformunun Kişisel Verilerin Korunması Kanunu'na aykırı uygulamalarda bulunması hakkında Kişisel Verileri Koruma Kurulunun 14/10/2021 tarihli ve 2021/1051 sayılı Karar Özeti

Karar Tarihi : 14/10/2021

Karar No : 2021/1051

Konu Özeti : İş arama ve işe alım süreçlerini yürüten bir istihdam platformunun Kişisel Verilerin Korunması Kanunu'na aykırı uygulamalarda bulunması

Kurum'a intikal eden şikâyet dilekçesinde özetle; veri sorumlusuna ait iş arama ve işe alım süreçlerini yürüten bir istihdam platformunda ilgili kişinin üyelik hesabı üzerinden yaptığı iş başvuruları ve iş görüşmeleri sonucunda işverenlere yönelik kişisel verilerinin gizliliği ve işlenmesi hususlarında veri sorumlusunun 6698 sayılı Kişisel Verilerin Korunması Kanunu'na (Kanun) aykırı uygulamalarda bulunduğu, ilgili kişinin iş başvuruları ve görüşme sonrasında ait işverenlere sunulan tüm bilgi ve belgelerin dijital bir örneğinin kendisine verilmesi hususundaki bilgi/erişim talebinin veri sorumlusunca yerine getirilmediği, ayrıca ilgili kişinin başvurusuna cevaben iletilen cevabi yazıda ilgili kişinin onayı olmaksızın verilerinin silineceğinin belirtildiği ifade edilmiş ve konu hakkında gerekli işlemlerin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup verilen cevabî yazıda özetle;

- İlgili kişiye cevap verilerek talebinin yerine getirilmiş olmasına rağmen ilgili kişi tarafından veri sorumlusunun cevabı beklenmeden Kurul'a şikâyette bulunulduğu;
- İlgili kişinin platformda bulunan iletişim kanalı üzerinden "İş başvuruları ve görüşme sonrasında sistemlerinde bulunan adayların değerlendirilmesine yönelik, işverenlere sunulan ilgili kişiye ait tüm verilerin ve verilerden türetilmiş bilgilerin Kanunun 11'inci maddesinin bentleri uyarınca paylaşılması" talebini müteakip veri sorumlusunca ilgili kişi ile iletişime geçildiği; ilgili kişinin işveren ile planladıkları mülakata gitmediği, işverenin "bu durumu diğer işverenlere belirteceğini" söylediği, ilgili kişinin verilerinin paylaşıldığı kişileri ve verilerinin (işverenin ilgili kişi hakkında veri

sorumlusu hizmet ortamında yaptığı değerlendirmeleri) diğer işverenler ile paylaşılıp paylaşılmadığını öğrenmek istediğini belirttiği; ilgili kişinin talebini yanıtlamak amacıyla öncelikle sözlü olarak iletişime geçilerek veri sorumlusu nezdinde işverenlerin adaylar hakkında gerçekleştirdiği değerlendirmelerin herhangi bir şekilde diğer işverenlerle paylaşılmadığının belirtildiği; ayrıca ilgili kişinin talebinin kayda sistematik olarak geçmesi amacıyla "Veri Sorumlusu Başvuru Formu" iletilmiş ve bu formun doldurularak veri sorumlusuna başvuruda bulunabileceğinin ifade edildiği;

- İlgili kişinin formu doldurarak veri sorumlusuna ilettiği, ilgili kişinin başvurusunda Kanun'un 11'inci maddesinin tüm bentlerindeki haklarını kullanma talebinde bulunması üzerine bir yandan talebi yerine getirilirken bir yandan da söz konusu sürede ilgili kişiye ait kişisel verilerin işlenmesinin durdurularak talebi doğrultusunda 30 gün içerisinde Kanun ve ikincil mevzuata uygun şekilde kişisel verilerinin imha edileceği bilgisinin iletilmiş, bunun üzerine ilgili kişinin kişisel verilerinin imha talebinde bulunmadığını, kişisel verilerinin aktarıldığı işverenlerin bilgilerini talep ettiğini ve veri sorumlusunun tutumunu Kurul'a şikâyet edeceğini belirttiği, aynı gün veri sorumlusunun ilgili kişi ile sözlü iletişime geçtiği ve talebinin karşılanacağını belirttiği, bununla birlikte ilgili kişinin veri sorumlusunun kasıtlı bir şekilde böyle cevap verdiğini ve Kurul'a şikâyette bulunduğunu ifade ettiği;
- Buna rağmen ilgili kişinin veri sorumlusu bünyesinde yer alan verilerine o güne kadar erişen tüm işverenlerin bilgisinin ilgili kişi ile paylaşıldığı ve bunun ardından herhangi bir iletişim kurulmadığı, ilgili kişinin mevcut durumda hala platform üyesi olduğu ve platformu kullanmaya devam ettiği;
- İlgili kişinin Kurum'a ilettiği şikâyet dilekçesinde yer alan ifadelerin aksine başvurusunun reddedilmediği, veri sorumlusunun ilgili kişinin talebini yerine getirmek adına başvuru sonrası derhal çalışmalara başladığı ve 7 gün gibi kısa bir süre içerisinde 2008 yılından bu yana işlenen çeşitli kişisel verileri ilgili kişinin kolayca ulaşabileceği bir formatta kendisine ilettiği;
- Veri sorumlusunun Kanun ve ikincil düzenlemeleri uyarınca yürürlüğe koyduğu Kişisel Veri İşleme, Saklama ve İmha Politikasını özenle uygulamakta olduğu, ilgili kişinin talebi üzerine kişisel verileri silme/imha etme işlemine başlandığı fakat böyle bir talebinin olmadığı anlaşıldığı anda işlemin durdurulduğu ve ilgili kişiye ilişkin herhangi bir kişisel veri kaybının söz konusu olmadığı;
- İşverenlerin çalışan adayları hakkında aldığı notların ve izlenimlerinin diğer işverenler ile paylaşılması gibi bir uygulamanın söz konusu olmadığı, işverenlerin yalnızca çalışan adaylarının platforma yüklediği bilgileri görebildiği, veri sorumlusu nezdinde çalışan adaylarının platforma yüklemiş olduğu kişisel verileri kullanılarak herhangi bir veri türetilmediği, yalnızca işverenlerin kendilerine başvuruda bulunan çalışan adaylarına ilişkin notlarını ve izlenimlerini platforma

yükleyebildiği ancak bu durumun tamamen işverenlerin takdirinde olduğu ve bu kişisel veriler için işverenlerin veri sorumlusu olup bu bilgilerin üretilmesine ilişkin kendilerinin herhangi bir dahlinin bulunmadığı;

- İlgili kişinin Kanun yürürlüğe girmeden evvel bir dönemde platforma üye olduğu ve yine Kanun'un Geçici 1'inci maddesi uyarınca da geçiş süreci içerisinde aksine bir irade beyanında bulunmadığı, yine de firmanın tüm veri işleme süreçlerine ilişkin kapsamlı bir uyum süreci başlattığı, VERBİS kaydını da zamanında tamamlayarak, şeffaf ve hesap verebilir şekilde kişisel verilerin korunması için gerekli teknik ve idari tedbirleri aldığı;

- Veri sorumlusunun ilgili kişiye sunduğu hizmetler sebebiyle ilgili kişiye ait kimlik bilgilerinin, iletişim bilgilerinin, mesleki deneyim bilgisinin, aldığı sertifika ve eğitim bilgilerinin, yabancı dil bilgisinin, kullanabildiği bilgisayar programlarının, görsel veri olarak özgeçmişte yer alan fotoğraf ve diğer bilgiler olarak da hobilerinin, ilgi alanları ve gerçekleştirilen projelere ilişkin bilgilerin işlendiği, ilgili kişilere sunulan "Kişisel Verilerinizin Korunması Hakkında Aday Aydınlatma Metni"nde (Aydınlatma Metni) platforma üye olan adayların hangi kişisel verilerinin işlendiğinin belirtildiği ancak Aydınlatma Metni'nde yer alan tüm veri kategorilerinin veri sorumlusunca işlenmediği, ilgili kişilerin iş ilanlarına başvurmak için hangi bilgileri paylaşacaklarını kendilerinin belirlediği;

- İlgili kişinin 21.03.2008 tarihinde "Hizmet Sözleşmesi"ni kabul ederek platforma üye olduğu, Hizmet Sözleşmesi uyarınca ve ilgili kişiye sunulan hizmet kapsamında Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (c) bendindeki "Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması" hükmü uyarınca işlendiği, zira platformun kullanım amacı ve üyelere sunulan hizmet kapsamında sayılan kişisel verilerin işlenmesinin zaruri olduğu, ayrıca üyelerin paylaşacakları kişisel verileri kendilerinin belirlediği, bu nedenle ilgili kişiden açık rıza alınmadığı ve yukarıda belirtilen hukuki sebebe dayanılarak kişisel verilerinin işlendiği;

- İlgili kişinin kişisel verilerinin platforma üye olan işverenler ile paylaşıldığı, adayların işverenler ile doğrudan özgeçmiş paylaşımı yapabildiği gibi işverenlerin de platform üzerinden adayların özgeçmişlerine erişebildiği, ilgili kişinin özgeçmişinde yer alan kişisel verilere hangi işverenlerin ne zaman eriştiği de belli olacak şekilde ilgili kişiye sunulduğu;

- Veri sorumlusunun ilgili kişileri aydınlattığı ölçüde ve Aydınlatma Metni'nde belirttiği amaçlar doğrultusunda kişisel verilerini kullandığı, bu amaçların dışında ve bu amaçları aşacak ölçüde kişisel veri kullanılmasına izin vermediği, ilgili kişinin talebinin yerine getirildiği ve kişisel verilerinin onayı olmadan silinmesi veya imha edilmesi gibi bir durumun söz konusu olmadığı

ifade edilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 14/10/2021 tarihli ve 2021/1051 sayılı Kararı ile;

- Kanun'un amacının kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek olduğu, Kanun'un "Tanımlar" başlıklı 3'üncü maddesinde "ilgili kişi"nin, kişisel verisi işlenen gerçek kişi; "veri sorumlusu"nun ise kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlandığı,

- Kanun'un, kişisel verilerin işlenmesine ilişkin "Genel İlkeler"i düzenleyen 4'üncü maddesinin (1) numaralı fıkrasında, "Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir." hükmünün yer aldığı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin;

a) Hukuka ve dürüstlük kurallarına uygun olma,

b) Doğru ve gerektiğinde güncel olma,

c) Belirli, açık ve meşru amaçlar için işlenme,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,

- Kanun'un "Kişisel Verilerin İşlenme Şartları" başlıklı 5'inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından

birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

• Öte yandan, “İlgili Kişinin Hakları”nı düzenleyen Kanun’un 11’inci maddesinin, “(1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

a) Kişisel veri işlenip işlenmediğini öğrenme,

b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,

ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

d) Kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme,

e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,

f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme, haklarına sahiptir.”

hükmünü amir olduğu,

• Kanun’un “Veri Güvenliğine İlişkin Yükümlülükler”i düzenleyen 12’nci maddesinin (1) numaralı fıkrasında veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idarî tedbirleri almak zorunda olduğunun hükme bağlandığı,

• Somut olayda, ilgili kişinin kişisel verilerine erişim talebinin yerine getirilmemesi konusundaki iddiasına ilişkin olarak; ilgili kişinin veri sorumlusunun ilk cevabından sonra talebinin karşılanmadığı düşüncesiyle Kurula şikâyette bulunduğu anlaşılmış olmakla birlikte, ilgili kişinin kişisel verilerine erişim talebinin Kurula şikâyette bulunma tarihinden sonra ve Kanun’un 13’üncü maddesinin (2) numaralı fıkrasına uygun şekilde “talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde” sonuçlandırıldığı dolayısıyla ilgili kişi tarafından yapılan iş başvurularına ilişkin bilgi

edinme talebinin veri sorumlusunun e-postası ile yerine getirildiği görüldüğünden, ilgili kişinin talebinin karşılanmadığına yönelik şikâyeti hakkında Kanun kapsamında yapılacak bir işlem bulunmadığı,

- İlgili kişinin talebi olmaksızın kişisel verilerinin veri sorumlusu tarafından silineceğinin / imha edileceğinin bildirilmesi hususundaki iddialarına yönelik olarak veri sorumlusunca ilgili kişinin başvurusunda Kanun'un 11'inci maddesinin (1) numaralı fıkrasının tüm bentlerindeki haklarını kullanma talebinde bulunması nedeniyle söz konusu fıkranın (e) bendinde yer alan kişisel verilerinin silinmesi talebinde de bulunduğu anlaşıldığı fakat ilgili kişinin cevabı üzerine böyle bir talebin olmadığı anlaşıldığı halde silme ve imhaya yönelik işlemin derhal durdurulduğu ve ilgili kişiye ilişkin herhangi bir kişisel veri kaybının söz konusu olmadığı belirtilmiştir; ilgili kişinin veri sorumlusu nezdindeki kişisel verilerinin silindiği/silineceği iddiasına yönelik veri sorumlusu beyanı aksine bir bilgi veya belgenin ilgili kişi tarafından Kurum'a sunulmaması, ilgili kişinin iş başvurusu bilgilerinin e-posta ile ilgili kişiye iletilmiş olması, ilgili kişinin şikâyet tarihinden sonra da veri sorumlusuna ait platformda iş başvurularına devam ettiği bilgisinin verilmesi ve ilgili kişinin başvurusu ile Kanun'un 11'inci maddesi kapsamındaki tüm haklarını kullanmak istediğini belirtmesi karşısında verilerinin silinmesini de talep ettiğinin anlaşılmasında veri sorumlusuna herhangi bir kusur yüklenemeyeceği değerlendirilerek; ilgili kişinin talebi olmaksızın kişisel verilerinin veri sorumlusu tarafından silineceğinin/ imha edileceğinin bildirilmesine yönelik şikâyeti hakkında Kanun kapsamında yapılacak bir işlem bulunmadığı,

- İlgili kişinin bilgisi ve onayı olmaksızın iş başvuruları ve iş görüşmelerine ilişkin kişisel verilerinin diğer işverenlerle paylaşılması iddialarına ilişkin olarak ilgili kişinin bu iddiaya yönelik şüphenin ötesine geçen herhangi bir tevsik edici bilgi veya belge sunması, veri sorumlusunun ise işverenlerin yalnızca çalışan adaylarının platforma yüklediği bilgileri görebildiğini, işverenlerin kendilerine başvuruda bulunan çalışan adaylarına ilişkin notlarını ve izlenimlerini platforma yükleyebildiği ancak bu durumun tamamen işverenlerin takdirinde olduğu ve işverenlerin çalışan adayları hakkında aldığı notların ve izlenimlerinin diğer işverenler ile paylaşılması gibi bir uygulamanın söz konusu olmadığını beyan etmesi karşısında; ilgili kişinin bu şikâyetiyle ilgili olarak Kanun kapsamında yapılacak bir işlem bulunmadığı

değerlendirmelerinden hareketle;

- İlgili kişinin veri sorumlusunun ilk cevabından sonra talebinin karşılanmadığı düşüncesiyle Kurul'a şikâyette bulunduğu, ilgili kişinin kişisel verilerine erişim talebinin Kurul'a şikâyette bulunma tarihinden sonra ve Kanun'un 13'üncü maddesinin ikinci fıkrasına uygun şekilde "talebin

niteliğine göre en kısa sürede ve en geç otuz gün içinde” sonuçlandırıldığı görüldüğünden, ilgili kişinin kişisel verilerine erişim talebinin karşılanmadığına yönelik şikâyeti hakkında Kanun kapsamında yapılacak bir işlem bulunmadığına,

İlgili kişinin veri sorumlusu nezdindeki kişisel verilerinin silindiği/silineceği iddiasına yönelik veri sorumlusunun beyanı aksine bir bilgi veya belgenin ilgili kişi tarafından Kuruma sunulmaması, ilgili kişinin iş başvurusu bilgilerinin e-posta ile ilgili kişiye iletilmiş olması, ilgili kişinin şikâyet tarihinden sonra da veri sorumlusuna ait platformda iş başvurularına devam ettiği bilgisinin verilmesi ve ilgili kişinin başvurusu ile Kanun’un 11’inci maddesi kapsamındaki tüm haklarını kullanmak istediğini belirtmesi karşısında verilerinin silinmesini de talep ettiğinin anlaşılmasında veri sorumlusuna herhangi bir kusur yüklenemeyeceği değerlendirilerek; ilgili kişinin talebi olmaksızın kişisel verilerinin veri sorumlusu tarafından silineceğinin/imha edileceğinin bildirilmesine yönelik şikâyeti hakkında Kanun kapsamında yapılacak bir işlem bulunmadığına,

- İlgili kişinin bilgisi ve onayı olmaksızın iş başvuruları ve iş görüşmelerine ilişkin kişisel verilerinin diğer işverenlere aktarıldığı iddiasına yönelik şüphenin ötesine geçen herhangi bir tevsik edici bilgi veya belge sunmamış olması, veri sorumlusunun ise işverenlerin yalnızca çalışan adaylarının platforma yüklediği bilgileri görebildiğini, işverenlerin kendilerine başvuruda bulunan çalışan adaylarına ilişkin notlarını ve izlenimlerini platforma yükleyebildiği ancak bu durumun tamamen işverenlerin takdirinde olduğu ve işverenlerin çalışan adayları hakkında aldığı notların ve izlenimlerinin diğer işverenlere aktarılması gibi bir uygulamanın söz konusu olmadığını beyan etmesi karşısında; ilgili kişinin bu şikâyetiyle ilgili olarak Kanun kapsamında yapılacak bir işlem bulunmadığına

karar verilmiştir.

2021/909 sayılı KVKK Kararı

İlgili kişinin kardeşine ait borca dair yürütülen icra takibi kapsamında, veri sorumlusu avukat tarafından ilgili kişinin kişisel verilerinin İcra Müdürlüğüne iletilmesi hakkında Kişisel Verileri Koruma Kurulunun 09/09/2021 tarihli ve 2021/909 sayılı Karar Özeti

Karar Tarihi : 09.09.2021

Karar No : 2021/909

Konu Özeti : İlgili kişinin kardeşine ait borca dair yürütülen icra takibi kapsamında, veri sorumlusu avukat tarafından ilgili kişinin kişisel verilerinin İcra Müdürlüğüne iletilmesi

Kuruma intikal eden şikâyet dilekçesinde özetle; bir avukat tarafından ilgili kişinin kardeşine ait borç için başlatılan icra takibi kapsamında, ilgili kişinin adresine İcra Müdürlüğü tarafından İcra ve İflas Kanununun (İİK) 89 uncu maddesinin (1) numaralı fıkrası gereği Birinci Haciz İhbarnamesi gönderildiği, icra dosyası kapsamında ilgili kişiye ait T.C. kimlik numarasının ve adresinin herhangi bir açık rıza ve aydınlatma onamı olmadan icra dairesine verildiği, veri sorumlusu avukata iadeli taahhütlü posta ile başvuru dilekçesi gönderildiği ancak başvurunun veri sorumlusuna iletilmesine rağmen başvuruya cevap verilmediği hususları ifade edilerek ilgili kişinin kişisel verilerini kanuna aykırı olarak işleyen ve rızası dışında kullanan veri sorumlusu avukat hakkında gerekli idari yaptırımların uygulanması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup verilen cevapta özetle;

- Müvekkilinin şikâyet sahibi ilgili kişinin kardeşinden alacaklı olduğu; borçlu hakkında İcra Ceza Mahkemesi tarafından 3 ay tazyik hapsine karar verildiği;
- Borçlunun ikamet adresinin bulunamadığı; yapılan UYAP sorgularında MERNİS adresinin "bilinmiyor" olduğu; dolayısıyla müvekkilinin alacağını tahsil etmek amacıyla ne bir haciz yapılabildiği ne de bir tebligat gönderilebildiği;
- İlgili kişinin kimlik bilgilerini, alacağını hiçbir şekilde tahsil edemeyen müvekkilinin kendisine verdiği; kendisinin de bu bilgileri İcra Müdürlüğüne dosyasına sunarak İİK'nın 89 uncu maddesinin (1) numaralı fıkrası kapsamında Birinci Haciz İhbarnamesi gönderilmesini talep ettiği;

- İcra Müdürlüğünün devletin resmi bir kurumu olduğu, alacaklının veya vekilinin, haczi üçüncü kişilere bildirmek maksadıyla herkese İİK'nın 89 uncu maddesinin (1) numaralı fıkrası kapsamında haciz ihbarnamesi gönderilmesini talep etme hakkı olduğu;
- Avukatların, mesleğin gereği olarak, müvekkillerine ve hatta davanın muhatabı olan karşı tarafa ait bir takım kişisel verilere erişmesinin ve bu verileri yargı nezdinde kullanmasının doğal olduğu;
- İİK'nın 89 uncu maddesinin (1) numaralı fıkrası hükmü gereği takibin kesinleşmesi üzerine ve alacaklının talebi ile icra dairesinin, borçlunun üçüncü kişideki alacağına haczine karar vererek, haciz tutanağı düzenleyeceği ve bu haczi üçüncü kişiye bir haciz ihbarnamesi göndermek suretiyle bildireceği; bu ihbarnameye birinci haciz ihbarnamesi dendiği;
- Bu ihbarnamenin içeriğinin İİK'nın 89 uncu maddesinin (1) numaralı fıkrası ve İcra İflas Kanunu Yönetmeliğinin 42 nci maddesinde düzenlendiği: buna göre ilgili maddede "Bu ihbarnamede dosya numarası; üçüncü kişinin kimlik ve adresi ile alacaklının, borçlunun kimlikleri, varsa vekilin/vekillerin kimlik ve adresi; alacak tutarı ile faiz ve giderler haczin ..hangi miktar için yapıldığı hakkındaki bilgiler bulunur. Ayrıca, haciz ihbarnamesi, üçüncü kişinin alacak tahsil edilinceye kadar borcunu yalnız haciz ihbarnamesini gönderen icra dairesinin banka hesabına yatırması gerektiği, borçluya yapılan ödemenin geçerli olmayacağı... ihtarını içerir. Bundan başka, üçüncü kişiye, takip borçlusunun kendisinden alacağı bulunmadığı veya takip borçlusuna daha önce ödediği veya borcun emrettiği kişiye ödendiği gibi bir iddiası varsa, icra dairesine (haciz ihbarnamesine) itiraz edebileceği (cevap verebileceği); aksi durumda, borcun zimmetinde sayılacağı ve bu miktarı icra dairesine ödemek zorunda kalacağı uyarısı yapılır." hükmüne yer verildiği
- Kanunun alacaklıya veya vekiline sağlamış olduğu yasal hakkı kullanarak üçüncü kişi olan ilgili kişiye İİK'nın 89 uncu maddesinin (1) numaralı fıkrası çerçevesinde haciz ihbarnamesi gönderilmesinde hiçbir hukuka aykırılığın söz konusu olmadığı; gönderilebilmesi için üçüncü kişinin adresi ve kimlik bilgisinin olması gerektiğinin ilgili Yönetmelikte de belirtildiği

ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde, Kişisel Verileri Koruma Kurulunun 09/09/2021 tarih ve 2021/909 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) "Tanımlar" başlıklı 3 üncü maddesi uyarınca kişisel verinin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi, veri sorumlusunun kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi, kişisel verilerin

işlenmesinin ise kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade ettiği,

- İcra ve İflas Hukuku gereğince ifası talep edilen hak ve borçların ancak yetkili devlet organlarına başvuru yoluyla ve yasal düzenlemelerde gösterilen usuller çerçevesinde cebri olarak takip edilebildiği, "haciz" in; kural olarak kesinleşmiş bir icra takibinin konusu olan belli bir para alacağının ödenmesini sağlamak için bu yolda talepte bulunan alacaklı lehine, söz konusu alacağı karşılayacak miktar ve değerdeki borçluya ait mal ve haklara icra dairesi tarafından hukuken el konulması olarak tanımlandığı, söz konusu mal ve hakların borçlunun elinde olabileceği gibi üçüncü bir kişide de bulunabildiği,

- Borçluya ait olmakla beraber üçüncü kişilerde bulunan hak ve alacakların haczinin İcra ve İflas Kanununun 89 uncu maddesinin (1) numaralı fıkrasında "Bu ihbarnamede dosya numarası; üçüncü kişinin kimlik ve adresi ile alacaklının, borçlunun kimlikleri, varsa vekilin/vekillerin kimlik ve adresi; alacak tutarı ile faiz ve giderler haczin hangi miktar için yapıldığı hakkındaki bilgiler bulunur. Ayrıca, haciz ihbarnamesi, üçüncü kişinin alacak tahsil edilinceye kadar borcunu yalnız haciz ihbarnamesini gönderen icra dairesinin banka hesabına yatırması gerektiği, borçluya yapılan ödemenin geçerli olmayacağı ihtarını içerir. Bundan başka, üçüncü kişiye, takip borçlusunun kendisinden alacağı bulunmadığı veya takip borçlusuna daha önce ödediği veya borcun emrettiği kişiye ödendiği gibi bir iddiası varsa, icra dairesine (haciz ihbarnamesine) itiraz edebileceği (cevap verebileceği); aksi durumda, borcun zimmetinde sayılacağı ve bu miktarı icra dairesine ödemek zorunda kalacağı uyarısı yapılır." hükmü ile düzenlendiği,

- İİK'nin 89 uncu maddesinin (1) numaralı fıkrası kapsamında borçlunun üçüncü kişilerdeki alacağının tahsili amacıyla alacaklı tarafından bildirilen gerçek veya tüzel kişilere İcra Müdürlüklerince birinci haciz ihbarnamesi gönderilmesinin alacaklı ile vekili arasındaki vekalet ilişkisi gereğince veri sorumlusu avukatın, müvekkili adına ilgili kişinin kişisel verilerini icra dairesine sunmak suretiyle gerçekleştirdiği bu kapsamda söz konusu veri işleme faaliyetinin hem Kanunun 5 inci maddesinin (2) numaralı fıkrasının (a) bendinde yer alan "Kanunlarda açıkça öngörülmesi" hükmüne hem de (e) bendinde yer alan "Bir hakkın tesisi, kullanılması, korunması için veri işlemenin zorunlu olması" hükmüne dayandığı

değerlendirmelerinden hareketle;

- İlgili kişinin kişisel verilerinin veri sorumlusu avukat tarafından icra dairesiyle izinsiz paylaşılması hususuna ilişkin olarak; İcra ve İflas Kanununun 89 uncu maddesi kapsamında borçlunun üçüncü kişilerdeki alacağının tahsili amacıyla alacaklı tarafından bildirilen gerçek veya tüzel kişilere İcra Müdürlüklerince birinci haciz ihbarnamesi gönderilmesi suretiyle alacaklı ve vekili arasındaki vekâlet ilişkisi gereğince alacaklı adına İcra Müdürlükleri nezdinde ilgili kişinin kişisel verilerinin işlenmesinin Kanunun 5 inci maddesinin (2) numaralı fıkrasının (a) ve (e) bentlerinde yer alan 'Kanunlarda açıkça öngörülme' ve 'Bir hakkın tesisi, kullanılması veya korunması için veri işleminin zorunlu olması' şartına dayanarak gerçekleştirildiği, bu çerçevede ilgili şikayete ilişkin olarak Kanun kapsamında tesis edilebilecek bir işlem bulunmadığına,
 - Öte yandan ilgili kişinin, kişisel verilerinin alacaklı tarafından hukuka aykırı ele geçirilmiş olduğu yönünde bir düşüncesi varsa bunu alacaklı bakımından Türk Ceza Kanunu hükümleri kapsamında yargıya intikal ettirebileceğinin hatırlatılmasına,
 - Bunun yanı sıra veri sorumlusu avukatın kendisine yapılan başvuruya süresi içinde cevap vermediği anlaşıldığından ilgili kişilerin kişisel verilerine ilişkin Kanunun 11 inci maddesi kapsamına giren taleplerine yine Kanunun 13 üncü maddesi gereğince süresi içinde cevap verilmesi gerektiğinin veri sorumlusuna hatırlatılmasına
- karar verilmiştir.

2021/925 sayılı KVKK Kararı

İlgili kişinin sendika üyeliği bilgisinin hukuka aykırı şekilde elde edilmesi ve paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 16/09/2021 tarihli ve 2021/925 sayılı Karar Özeti

Karar Tarihi : 16.09.2021

Karar No : 2021/925

Konu Özeti : İlgili kişinin sendika üyeliği bilgisinin hukuka aykırı şekilde elde edilmesi ve paylaşılması

İlgili kişinin Kuruma intikal eden şikâyetinde özetle; iki yıldır çalışmakta olduğu Şirkete dava açan bir çalışanın avukatı (veri sorumlusu) tarafından kaleme alınmış dava dilekçesinde, ilgili kişinin kendisine ve sendika üyesi diğer çalışanlara ait sendika üyelik bilgileri ile üyelik tarihlerine yer verildiği; sendika üyelik bilgisini daha önce kimseyle paylaşmadığı; konu hakkında veri sorumlusuna başvuruda bulunduğu ancak verilen cevabı yeterli bulmadığı ifade edilerek veri sorumlusu avukat hakkında 6698 sayılı Kişisel Verilerin Korunması Kanun (Kanun) kapsamında gerekli yasal işlemlerin yapılması talep edilmiştir.

Bu kapsamda başlatılan inceleme çerçevesinde söz konusu iddialara ilişkin veri sorumlusundan savunması istenilmiş olup alınan cevabi yazılarda özetle;

- İşyerinde çalışan işçilerin yasal sendikal faaliyetleri nedeniyle iş sözleşmelerinin feshedilmesi üzerine söz konusu işyerinde çalışan işçilerin %60-70 oranında katıldığı toplantılarda, iş yerinde yaşanan olumsuzluklar nedeniyle iş sözleşmesi feshedilen işçilerin yanında bir kısım işçilerin de işveren baskısı sonucu sendika üyeliğinden istifa ettikleri vb. bilgisinin verildiği; bu toplantıların ve verilen bilgilerin iş yerinde çalışan tüm işçilerin bildiği aleni bilgiler olduğu ve tamamen duyuma dayalı olduğu, bu nedenle bu bilgilere ulaşım yolunun hukuka uygun olduğu,
- Bu bilgiler çerçevesinde iş yerinde çalışırken iş sözleşmesi sendikal nedenlerle feshedilen davacı işçi adına, davalı işveren aleyhine sendikal tazminat talepli işe iade davası açıldığı,
- 4857 sayılı İş Kanununun (4857 sayılı Kanun) 20 nci maddesi ve 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununun (6356 sayılı Kanun) 25 nci maddesinin 6 ncı fıkrası uyarınca iş sözleşmesinin sendikal nedenlerle feshedildiğinin ispat külfetinin işçiye (yani davacı müvekkiline) ait olduğu,

Yargıtay'ın kararlarında da sendika üyesi olan, istifa eden ve baskıya uğrayan işçilerin somut olarak bu durumu ispatlamasının istendiği, yine Yargıtay'ın yerleşik kararlarına göre "...işçilerin birlikte hukuki işlemi aynı anda yapması, notere gitmesi, ihtarname çekmesi, sendika üyeliğinden istifa etmesi..." gibi işlemlerin işverenin yönlendirmesi ile yapıldığının karine olduğu,

- Yargılama aşamasında sendikanın iş yerinde çalışan işçilerden sendika üyesi olanlara ve sonradan sendika üyeliğinden istifa edenlere ilişkin bilgi sunacağı ve varsa üyelik ve istifa fişlerini ibraz edeceği; şikâyetçinin hangi tarihte istifa ettiğinin dava dilekçesinde tarih olarak belirtilmediği, süreç olarak anlatıldığı, istifa tarihinin yasal zorunluluk olarak yargılama sırasında Çalışma ve Sosyal Güvenlik Bakanlığı ile sendikadan tezkere ile isteneceği,

- Müvekkilinin iş sözleşmesinin sırf sendikal nedenlerle feshedilmiş olduğu, işyerinde yaşanan sendikal süreçte sendika üyelikleri tespit edilen işçilere, işveren tarafından yapılan baskılar sonucu bir kısım üye işçilerin de, sendika üyeliklerinden istifa ederek, işyerinde çalışmaya devam ettiklerinin tüm işçiler tarafından bilinen bir gerçek olduğu, dava dilekçesinde de şikâyetçi dahil bir kısım işçinin aynı dönemde işverenin baskısı ile istifaya zorlandıklarının belirtildiği, açılan davada dava dilekçesi ve eklerinin şikâyetçi işçiye gösterilmesinin işverenin halen işyerinde sendikal faaliyeti engellemeye çalıştığı açık bir göstergesi olduğu ve bu kapsamda şikâyetçinin başvurusunun da işverenin yönlendirmesiyle yapıldığı,

- Hukuka uygun elde edilen tüm aleni bilgilerin dava dilekçesinde paylaşılmasının kişisel verilerin hukuka aykırı paylaşımı anlamına gelmediği ve verilerin işlendiği iddialarının da geçerli olmadığı, dava dilekçesinin izah edilen süreç çerçevesince hazırlanmış olduğu ve gerçekleştirilen hukuki işlemlerin hiçbir aşamasında hukuka aykırı bir yol izlenmediği

ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 16/09/2021 tarihli ve 2021/925 sayılı Kararı ile;

- Kanunun "Özel Nitelikli Kişisel Verilerin İşlenme Şartları" başlıklı 6 ncı maddesinin (1) numaralı fıkrasında özel nitelikli kişisel verilerin "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri" olarak sayıldığı,

- Kanunun "Özel Nitelikli Kişisel Verilerin İşlenme Şartları" başlıklı 6 ncı maddesinin (2) numaralı fıkrasında özel nitelikli kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (3)

numaralı fıkrasında ise birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel verilerin, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebileceği hükümlerinin yer aldığı,

- 1136 sayılı Avukatlık Kanununun “Avukatlığın amacı” başlıklı 2 nci maddesinde; “Avukatlığın amacı; hukuki münasebetlerin düzenlenmesini, her türlü hukuki mesele ve anlaşmazlıkların adalet ve hakkaniyete uygun olarak çözümlenmesini ve hukuk kurallarının tam olarak uygulanmasını her derecede yargı organları, hakemler, resmi ve özel kişi, kurul ve kurumlar nezdinde sağlamaktır. Avukat bu amaçla hukuki bilgi ve tecrübelerini adalet hizmetine ve kişilerin yararlanmasına tahsis eder. Yargı organları, emniyet makamları, diğer kamu kurum ve kuruluşları ile kamu iktisadi teşebbüsleri, özel ve kamuya ait bankalar, noterler, sigorta şirketleri ve vakıflar avukatlara görevlerinin yerine getirilmesinde yardımcı olmak zorundadır. Kanunlarındaki özel hükümler saklı kalmak kaydıyla, bu kurumlar avukatın gerek duyduğu bilgi ve belgeleri incelemesine sunmakla yükümlüdür. Bu belgelerden örnek alınması vekâletname ibrazına bağlıdır. Derdest davalarda müzekkereler duruşma günü beklenmeksizin mahkemeden alınabilir.” hükümlerine yer verildiği,

- 6100 sayılı Hukuk Muhakemeleri Kanununun “Dava dilekçesinin içeriği” başlıklı 119 uncu maddesinin (1) numaralı fıkrasında ise dava dilekçesinde bulunacak hususların “... a) Mahkemenin adı. b) Davacı ile davalının adı, soyadı ve adresleri. c) Davacının Türkiye Cumhuriyeti kimlik numarası. ç) Varsa tarafların kanuni temsilcilerinin ve davacı vekilinin adı, soyadı ve adresleri. d) Davanın konusu ve malvarlığı haklarına ilişkin davalarda, dava konusunun değeri. e) Davacının iddiasının dayanağı olan bütün vakıaların sıra numarası altında açık özetleri. f) İddia edilen her bir vakıanın hangi delillerle ispat edileceği. g) Dayanılan hukuki sebepler. ğ) Açık bir şekilde talep sonucu. h) Davacının, varsa kanuni temsilcisinin veya vekilinin imzası.” şeklinde belirtildiği

- Bu çerçevede, ilgili kişinin özel nitelikli kişisel verisi olan sendikalı olma bilgisinin veri sorumlusu tarafından üçüncü bir tarafla paylaşılması da dahil olmak üzere dava dilekçesine eklenmek suretiyle işlenmesinin ancak açık rızanın bulunması ya da Kanunlarda öngörülen hallerde mümkün bulunduğu,

- Veri sorumlusu tarafından yazı ekinde gönderilen dava dilekçesinin incelenmesi neticesinde; ilgili İş Mahkemesine sunulmak üzere hazırlanan dilekçede sendikal sürece ve işveren ile işçiler arasında mevcut olduğu iddia edilen anlaşmazlıklara yer verildiği, ilgili kişinin sadece ad ve soyadının sendikadan istifa eden işçilerden biri olarak açıkça yazıldığı, ilgili kişi dışında farklı işçilerin ad ve soyadlarının da ilgili dava dilekçesinde yer aldığı ve söz konusu durumun tespiti amacıyla sendikadan istifa beyanlarının celbinin talep edildiğinin görüldüğü,

• Yargıtay 9. Hukuk Dairesinin E.2018/5445 K. 2018/17529 sayılı kararının gerekçe bölümünde “... Dairemizce, sendikal tazminat davalarında ispat yükünün işçide olduğu hallerde, işyerinde çalışan ve sendikaya üye olan işçilerin sayısı, hangi tarihlerde üye oldukları, üyelikten çekilen işçilerin olup olmadığı, işyerinde çalışmakta olan işçilerin bulunup bulunmadığı, aynı dönemde yetki prosedürünün işletilip işletilmediği, işyerinde önceki dönemlerde toplu iş sözleşmelerinin bağtlanıp bağtlanmadığı, yeni işçi alınıp alınmadığı ve alınmışsa yeni işçilerin sendikalı olup olmadığı gibi hususlarla, işverence ekonomik veya teknolojik nedenlere dayalı bir fesih yoluna gidilmesi durumunda teknik yönden bu durumun araştırılması gibi ölçütler belirlenmiştir.” hususlarına yer verilerek işveren tarafından gerçekleştirilen feshin geçersizliğine ve davacının işe iadesine karar verildiğinin görüldüğü,

• 4857 sayılı İş Kanununun 20 nci maddesinin (2) numaralı fıkrasının “Feshin geçerli bir sebebe dayandığını ispat yükümlülüğü işverene aittir. İşçi, feshin başka bir sebebe dayandığını iddia ettiği takdirde, bu iddiasını ispatla yükümlüdür” hükmünü haiz olduğu,

• 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununun 25 inci maddesinin (3) numaralı fıkrasında ise “İşçiler, sendikaya üye olmaları veya olmamaları, iş saatleri dışında veya işverenin izni ile iş saatleri içinde işçi kuruluşlarının faaliyetlerine katılmaları veya sendikal faaliyette bulunmalarından dolayı işten çıkarılamaz veya farklı işleme tabi tutulamaz.” hükmüne; (5) numaralı fıkrasında “Sendikal bir nedenle iş sözleşmesinin feshi halinde işçi, 4857 sayılı Kanunun (...) (2), 20 ve 21 inci madde hükümlerine göre dava açma hakkına sahiptir. İş sözleşmesinin sendikal nedenle feshedildiğinin tespit edilmesi halinde, 4857 sayılı Kanunun 21 inci maddesine göre işçinin başvurusu, işverenin işe başlatması veya başlatmaması şartına bağlı olmaksızın sendikal tazminata karar verilir. Ancak işçinin işe başlatılmaması halinde, ayrıca 4857 sayılı Kanunun 21 inci maddesinin birinci fıkrasında belirtilen tazminata hükmedilmez. İşçinin 4857 sayılı Kanunun yukarıdaki hükümlerine göre dava açmaması ayrıca sendikal tazminat talebini engellemez.” hükmüne, (6) numaralı fıkrasında ise “İş sözleşmesinin sendikal nedenle feshedildiği iddiası ile açılacak davada, feshin nedenini ispat yükümlülüğü işverene aittir. Feshin işverenin ileri sürdüğü nedene dayanmadığını iddia eden işçi, feshin sendikal nedene dayandığını ispatla yükümlüdür.” hükmüne yer verildiği,

• Öncelikle işçi sendikalarının işçilerin ekonomik ve sosyal haklarını korumak ve geliştirmek amacıyla kurulan örgütler olduğu ve bir sendikanın toplu iş sözleşmesi imzalayabilmesi için 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanunu gereğince işkolu ve işyeri barajlarını geçmesi gerektiği, sendika özgürlüğünün, mevzuatımızda Anayasanın 51 inci ve 6356 sayılı Sendikalar ve

Toplu İş Sözleşmesi Kanununun 23 ila 25 inci maddeleri arasında yer alan düzenlemeler ile güvence altına alındığı, kişinin dilediği sendikaya üye olması veyahut üye olmaması, sendikal faaliyette bulunması veya sendika kurması gibi özgürlüklerin sendika özgürlüğü kapsamında olduğu,

- Somut olayda konu edilen sendikal feshin ise, işçilerin bir sendikaya üye olmaları veya tam tersi işverenin istediği bir sendikaya üye olmamaları nedeniyle ya da sendikal faaliyetlere katılmaları nedeniyle işten çıkarılmalarını ifade ettiği, Sendikalar ve Toplu İş Sözleşmesi Kanununun 25 inci maddesinin, bu nedene dayalı olarak yapılacak fesihleri açık bir şekilde yasakladığı ancak yasağa rağmen yapılması halinde, iş sözleşmesi sendikal nedenle feshedilen kişinin dava açması gerektiği, açılan davada iş sözleşmesinin sendikal nedenlerle feshedildiğinin işçi tarafından ispat edilmesinin beklendiği

- Şikâyete konu somut olayda, iş sözleşmesinin sendikal nedenle feshedildiğini iddia eden bir işçi hakkında veri sorumlusu avukat tarafından açılan işe iade davasında ilgili kişinin ad soyadının ve sendikal olduğu bilgisinin paylaşılmasının; somut olayın başka bir işçi lehine açılmış bir işe iade davası olması ve davanın sendikal faaliyet üzerine kurulmuş olması, ayrıca bu husustaki ispat külfetinin veri sorumlusu avukata ait olduğu davada, aynı işyerinde çalışan ilgili kişinin sendikalılıktan ayrılmış olma bilgisinin dosyayla ilgili olması sebebiyle Avukatlık Kanununun 2 nci maddesinde yer alan hüküm ve Hukuk Muhakemeleri Kanununun 119 uncu maddesi uyarınca işe iade dava dilekçesinde kullanmasının Kanunun 6 ncı maddesine aykırılık teşkil etmediği

değerlendirmelerinden hareketle;

- Şikayet dilekçesinde yer verilen iddiaların Kanuna aykırılık teşkil etmediği sonucuna varıldığından bu hususta 6698 sayılı Kanun kapsamında yapılacak bir işlem bulunmadığına karar verilmiştir.

2021/989 sayılı KVKK Kararı

İlgili kişiye ait görselin, açık rızası alınmaksızın bir internet sitesinde yer alan haber içeriğinde kullanılması hakkında Kişisel Verileri Koruma Kurulunun 30/09/2021 tarihli 2021/989 sayılı Karar Özeti

Karar Tarihi : 30.09.2021

Karar No : 2021/989

Konu Özeti : İlgili kişiye ait görselin, açık rızası alınmaksızın bir internet sitesinde yer alan haber içeriğinde kullanılması

Kısıtlının (ilgili kişi) vasisinin Kuruma intikal eden şikâyetinde özetle; bir veri sorumlusu bünyesinde yer alan internet sitesinin haber içeriğinde kullanılan fotoğrafın ilgili kişi olan oğluna ait olduğu, ilgili görselin kullanılmasında açık rızasının bulunmadığı, ilgili kişinin haber içeriğinde beyan edildiği gibi evlat edinilen bir mahkûmun çocuğu olmadığı, gerçek dışı haber içeriği sonucu mağduriyet yaşadığı ve ilgili kişinin kişilik haklarının ihlal edildiği, bu konunun öğrenilmesi neticesinde suça konu haberi yayınlayan veri sorumlusuna başvuru yapıldığı, veri sorumlusu tarafından fotoğrafın kaldırıldığı taraflarına e-posta ile bildirilse de sadece bir URL'deki fotoğrafın kaldırıldığı, diğer URL'lerin tamamında fotoğrafa ulaşımın hâlâ sağlandığı ve mağduriyetin devam ettiği, bu kapsamda Ankara...Sulh Ceza Hakimliğine erişimin engellenmesi talebi ile başvuru yapıldığı, başvuru neticesinde bazı URL'lerin erişiminin engellendiği ancak bazı URL'ler açısından ihlâlin hâlâ devam etmekte olduğu, Savcılığa da ayrıca suç duyurusunda bulunulduğu ifade edilerek, ilgili kişinin vasisi tarafından 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınancevabi yazıda özetle;

- İnternet sitesinin haber paylaşımı, blog ve çeşitli içerikler sağlayan veya kullanıcılarına/üyelerine bu içerikleri üretip paylaşma imkânı tanıyan bir sosyal medya platformu olduğu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (5651 sayılı Kanun) uyarınca sitenin yer sağlayıcısı

olduğu, sitede yer alan içeriklerin veri sorumlusu çalışan editörler tarafından oluşturulabileceği gibi içerik üretmek ve sitede yayımlamak isteyen herkesin üye olarak kendi içeriğini herhangi bir müdahale, kontrol veya denetim olmadan da oluşturabileceği ve sitede yayımlayabileceği, bu kapsamda veri sorumlusunun kendisine bağlı olarak çalışan editörler tarafından üretilen içerikler için içerik sağlayıcı; kullanıcı/üyelerin oluşturup yayımladığı ve sitenin herhangi bir müdahalesi veya denetimi olmayan içerikler açısından ise yer sağlayıcı niteliğinde olduğu,

- Somut olayda haber içeriğinin ise sitenin bir kullanıcısı/üyesi tarafından siteden bağımsız bir şekilde oluşturulduğu, siteye yüklenip yayımlandığı, dolayısıyla ilgili içeriğin yayımlanması hususunda kendilerinin herhangi bir kontrol veya denetiminin olmadığı, 5651 sayılı Kanun uyarınca yer sağlayıcı olarak ilgili mevzuat uyarınca içeriğin sebep olduğu herhangi bir hukuka aykırılıktan sorumlu tutulamayacağı,

- Sitede yer alan Kullanıcı ve Gizlilik Sözleşmesinde de açıklandığı üzere, paylaşım yapacak üyelere sadece paylaşım yapmalarına imkân tanıyan bir sosyal ağ sağlandığı, ayrıca diğer maddelerde de açıkça paylaşım yapan kullanıcı/üyenin paylaştığı içerikten tamamen kendisinin sorumlu olduğu ve bu kapsamda kendilerine herhangi bir sorumluluk yüklenemeyeceğinin düzenlendiği,

- Öte yandan, söz konusu haber içeriğinin yayından kaldırılması amacıyla kendilerine yapılan başvuruda; Kanunun 11 inci maddesinde yer alan haklara ilişkin taleplerin yer almadığı, yer sağlayıcı olarak yükümlülüklerinin yerine getirilmesinin talep edildiği, bu kapsamda ilgili kişinin vasisi tarafından öncelikle Kanunun 13 üncü maddesinde belirtilen veri sorumlusuna başvuru yolunun tüketilmediği, bu çerçevede usulüne uygun bir başvuru yapılmadığından hareketle şikâyetin hukuka aykırı olduğu ve reddedilmesi gerektiği,

- Diğer taraftan, iddia edilenin aksine başvuru talebinin tamamen kabul edildiği ve söz konusu içeriğin yayından kaldırıldığı, diğer URL adreslerinin ise içeriğin sitede yer alan arama çubuğu aracılığıyla aratılarak görüntülenmesine ilişkin olduğu ve tamamen ilgili içeriğe bağlı olduğu, içeriğin kaldırılmasıyla birlikte diğer linklerin de erişilemez hale geldiği ve gereken önlemlerin alındığı,

- Bununla birlikte sitede yayımlanan içeriğin haber niteliği taşıdığı ve ifade özgürlüğü kapsamında yayımlandığı, bu sebeple ilgili veri işleme faaliyetinin Kanunun 28 inci maddesinin (1) numaralı fıkrasında sayılan Kanun kapsamı dışında kalan istisnalar içerisinde yer aldığı

ifadelerine yer verilmiştir. Bunun üzerine veri sorumlusundan şikâyete konu içeriklere ilişkin linklere yer verilmek suretiyle mezkûr içeriklerin site kullanıcısı/üyesi tarafından siteden bağımsız bir şekilde oluşturulduğu iddiasına ilişkin tevsik edici tüm belge ve kayıtların Kuruma gönderilmesi

istenilmiştir. Veri sorumlusundan alınan cevabi yazıda ise ilgili kullanıcı hesap bilgileri verilerek, söz konusu kullanıcının veri sorumlusu nezdinde editör pozisyonunda görev aldığı ve içerik ürettiği, bununla birlikte incelemeye konu haberlerde yer alan görsellerin tüm kamuoyunda aleni hale geldiği ve veri sorumlusunun haber tarihinden önce yapılan birçok haber internet sitesinde yayımlandığı belirtilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 30/09/2021 tarihli ve 2021/989 sayılı Kararı ile;

- Kanunun “Tanımlar” başlıklı 3 üncü maddesinde “kişisel veri”nin kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi; “ilgili kişi”nin ise kişisel verisi işlenen gerçek kişi olarak tanımlandığı, bu çerçevede, habere konu edilen küçüğün kişisel verileri işlenen ilgili kişi, şikâyete konu içerikte yer alan fotoğrafın kişisel veri niteliğinde olduğu,
- Öte yandan veri sorumlusuna yapılan başvurunun iddia edildiğinin aksine 6698 sayılı Kanun kapsamında olduğu ve ilgili kişinin/vasisinin açık rızası olmaksızın kişisel verisinin paylaşılması sebebiyle söz konusu fotoğrafın kaldırılması talebinin de Kanunun 11 inci maddesinde sayılan haklar kapsamında olduğu,
- Söz konusu fotoğrafın kaldırıldığı iddiasının aksine yalnızca bir URL adresindeki fotoğrafın kaldırıldığı, diğer URL adreslerinde ise halen yayımlanmaya devam edildiği,
- Sitenin kullanıcıları ile akdettiği Kullanıcı ve Gizlilik Sözleşmesinde yer alan bilgi, veri, yazı, fotoğraf, video, ses klibi, yorumlar, makaleler, yazılımlar, kodlar ve grafiklerin kısaca içerik olduğu ve bu içeriklerin üyeler tarafından girilebileceği gibi veri sorumlusunun editörleri tarafından da girilebileceği ibarelerine yer verildiği,
- Veri sorumlusunun Kurumu muhatap cevabi yazısında, sitede içerik yayımlamak isteyen herkesin üye olarak kendi içeriğini herhangi bir müdahale, kontrol veya denetim olmadan da oluşturabileceği, veri sorumlusunun kendisine bağlı olarak çalışan editörler tarafından üretilen içerikler için içerik sağlayıcı, kullanıcı/üyelerin oluşturup yayımladığı ve sitenin herhangi bir müdahalesi veya denetimi olmayan içerikler açısından ise yer sağlayıcı niteliğinde olduğu ifadelerine rastlandığı,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun (5651 sayılı Kanun) “Tanımlar” başlıklı 2 nci maddesinin (1) numaralı fıkrasının (f) bendinde içerik sağlayıcının, “İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler”, yer sağlayıcının ise “Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek

veya tüzel kişiler” olarak tanımlandığı, “İçerik sağlayıcının sorumluluğu” başlıklı 4 üncü maddenin (1) numaralı fıkrasında “İçerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur.” hükmünün, “Yer sağlayıcının yükümlülükleri” başlığını haiz 5 inci maddesinin (1) numaralı fıkrasında ise “Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir.” hükmünün düzenlendiği,

- Kuruma intikal eden belgeler incelendiğinde, fotoğrafın yer aldığı içeriğin veri sorumlusunun bünyesinde içerik üreten bir editör tarafından oluşturulduğunun anlaşıldığı, şikâyet konusu içeriğin bağımsız bir kullanıcı/üye tarafından değil çalışan tarafından oluşturulmak suretiyle internet sitesinde yayımlandığı dikkate alındığında Şirketin somut olay nezdinde 6698 sayılı Kanun kapsamında veri sorumlusu sıfatını haiz olduğu, dolayısıyla Kanun kapsamındaki yükümlülüklere tabi olacağı; fotoğrafın şikâyete konu içerikte yayımlanmasının ise kişisel veri işleme faaliyeti olduğu,

- Öte yandan, Kanununun 28 inci maddesinin (1) numaralı fıkrasının (c) bendinde “Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi” halinde Kanun hükümlerinin uygulanmayacağı belirtilmiştir,

- Bu kapsamda öncelikli olarak, başvuru konusunun Kanun hükümlerinin uygulama alanı dışında kalıp kalmadığının değerlendirilmesi gerektiği, bu çerçevede, ifade özgürlüğünün bir yansıması olan basın özgürlüğü ile kişilik hakları karşı karşıya geldiğinde haberin;

- Kamu ilgi ve yararı taşıması,

- Gerçek ve güncel olması,

- Özü ile biçimi arasındaki denge

kriterleri kapsamında değerlendirilmesi suretiyle hangi hakka üstünlük tanınması gerektiğinin belirlenmesi gerektiği,

- Kamu yararının tespitinde, haberin kişilerin merak duygularına mı yoksa yüksek ahlaki ve hukuki değerlerin korunmasına mı hizmet ettiğinin değerlendirilmesi gerektiği, örneğin; yasa dışı uygulamaların, rüşvet ve yolsuzlukların kamuoyuna iletilmesinde, eleştirilmesinde kamu yararı bulunduğu, öte yandan, kamu ilgi ve yararı kriteri kapsamında siyasetçiler ve kamu görevlilerine dair yapılan haberler bakımından basın özgürlüğüne yapılan sınırlamaların daha dar yorumlanmasının uygun olacağı,

- Öte yandan, haberin gerçek ve güncel olmasının ikinci kriter olduğu, gerçeklik unsurunun, somut gerçeğe değil, olayın, haberin verildiği andaki belirli biçimine uygunluk olarak anlaşılması gerektiği,
- Haberin güncel olmasının ise somut olayın açıklandığı tarihlerde kamu yararının bulunması esasına dayandığı, üzerinden süre geçmiş ve açıklanmasında artık kamu yararı bulunmayan bir olayın yayımlanmasında haber verme hakkından söz edilemeyeceğinden hareketle kişilik hakkına üstünlük tanınması gerekeceği,
- Biçim ve öz arasındaki denge kriteri açısından ise kullanılacak dil ve ifadenin, yapılacak nitelendirme ve vurgunun da haberin gerektirdiği biçim ve ölçü çerçevesinde kalmasının ve yasal fonksiyonun yönelik bulunduğu “amaç”a ulaşabilmek için en uygun ve en elverişli “araç”ın kullanılmasının gerekeceği,
- Bu hususlar doğrultusunda, haber içeriği kapsamındaki kişisel verinin, kişilik haklarını ihlal etmemek kaydıyla ifade özgürlüğü kapsamında işlenip işlenmediğinin değerlendirilmesi neticesinde; ilgili kişi açısından bahse konu olayda yer alan haber içeriğinin kamu ilgi ve yararının varlığına sebep olabilecek bir nitelik taşımadığı, haber içeriğinde yer alan bilgilerin ilgili kişi açısından doğru olmadığı ve kişilik haklarını ihlal ettiği hususları göz önünde bulundurulduğunda şikâyet konusu içeriğin Kanununun 28 inci maddesinin (1) numaralı fıkrasının (c) bendi uyarınca kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesinin Kanundan istisna tutulacağına ilişkin hükmü kapsamında ele alınamayacağı,
- Kanunun “Kişisel verilerin işleme şartları” başlıklı 5 inci maddesinde;

“(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

 - a) Kanunlarda açıkça öngörülmesi.
 - b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması. c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
 - ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
 - d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.” hükmünün yer aldığı,

- Bu kapsamda, ilgili kişiye ait fotoğrafın kendisi ile ilgisi olmayan bir içerikte kullanılmak suretiyle internet sitesinde yayımlandığı dikkate alındığında Kanunun 5 inci maddesinde yer alan işleme şartları olmaksızın veri işleme faaliyetinde bulunduğu dolayısıyla veri sorumlusunun Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendi uyarınca kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almadığı

değerlendirmelerinden hareketle;

- İlgili kişi açısından bahse konu olayda yer alan haber içeriğinin kamu ilgi ve yararının varlığına sebep olabilecek bir nitelik taşımadığı, zira Kuruma iletilen şikâyet dilekçesi ekinde yer verilen 19.03.2019 tarihli mahkeme kararından da ilgili kişinin annesinin tarafına vasi olarak tayin edildiği dolayısıyla ilgili kişinin adı geçen ünlü tarafından evlat edinilmediğinin açık olduğu dikkate alındığında; internet sitesinde yayımlanan söz konusu haber içeriğinde yer alan bilgilerin ilgili kişi açısından doğru olmadığı ve kişilik haklarını ihlal ettiği hususları göz önünde bulundurulduğunda şikâyet konusu içeriğin Kanunun 28 inci maddesinin (1) numaralı fıkrasının (c) bendi kapsamında değerlendirilemeyeceğine,

- İlgili kişinin adına vasisinin açık rızası ya da Kanunun 5 inci maddesinde yer alan diğer işleme şartlarından biri olmaksızın ilgili kişiye ait fotoğrafın veri sorumlusu bünyesinde çalışan bir editör tarafından ilgili kişi ile ilgili olmayan yanlış bir içerikle internet sitesinde yayımlandığı dikkate alındığında, veri sorumlusunun Kanunun “Veri Güvenliğine İlişkin Yükümlülükler” başlıklı 12 nci maddesinin (1) numaralı fıkrasının (a) bendinde öngörülen yükümlülüğünü yerine getirmediği sonucuna varılmış olup veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında idari para cezası uygulanmasına

karar verilmiştir.

2021/993 sayılı KVKK Kararı

Veri sorumlusu kargo firması tarafından ilgili kişi adına sehven fatura düzenlenmesi hakkında Kişisel Verileri Koruma Kurulunun 30/09/2021 tarihli 2021/993 sayılı Karar Özeti

Karar Tarihi : 30.09.2021

Karar No : 2021/993

Konu Özeti : Veri sorumlusu kargo firması tarafından ilgili kişi adına sehven fatura düzenlenmesi

İlgili kişinin Kuruma intikal eden şikâyetinde özetle; herhangi bir hizmet almamasına rağmen, veri sorumlusu kargo şirketi tarafından ilgili kişinin e-posta adresine kendisi adına düzenlenen bir fatura gönderildiği, kargo gönderim kodu ile yapılan sorguda faturanın bir firmaya teslim edilen kargo işlemine ait olduğunun görüldüğü, faturada yer alan ad, soyadı, adres, e-posta adresi, T.C. kimlik numarası gibi kişisel verilerinin, satın alma işlemi gerçekleştirilen firmaya aktarıldığı, konuya ilişkin veri sorumlusuna başvurduğu, verilen yanıtta ise faturalandırma işleminin sehven ilgili kişi adına yapıldığı ve ilgili kişinin bilgilerinin bir kamu kurumu niteliğindeki meslek kuruluşu (meslek kuruluşu) ile veri sorumlusu arasında imzalanan, ilgili meslek kuruluşuna kayıtlı üyelerin indirimli gönderim ücretlerinden yararlanmasını sağlayan sözleşme kapsamında Şirketleri arşivinde bulunduğu belirtiltiği, ilgili meslek kuruluşunun hukuka aykırı şekilde veri sorumlusuna aktardığı kişisel verilerin, veri sorumlusu tarafından kanuni işleme şartına dayanmaksızın işlendiği ve ilgili kişinin kişisel verilerinin silinmesi talebinin veri sorumlusu tarafından yerine getirilmediği ifade edilerek, 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında veri sorumlusu kargo şirketi hakkında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- İlgili kişinin 2018-2020 yılları arasında alıcı müşteri olarak kaydının bulunduğu, bu kayıtlarda ad, soyadı, adres, telefon numarası, T.C. kimlik numarası olmak üzere belirli kişisel verilerinin yer aldığı,
- Kargo gönderilerinin alıcı tarafına ait kişisel verilerin kargo taşıma sözleşmesinin gereği olarak işlendiği, bu kişisel verilerin 6475 sayılı Posta Hizmetleri Kanunu, Posta Sektörüne İlişkin Yetkilendirme Yönetmeliği, Posta Hizmetlerinin Sunulmasına İlişkin Yönetmelik, Posta

Gönderilerine İlişkin Güvenlik Tedbirlerine Yönelik Usul ve Esaslar başta olmak üzere ilgili mevzuat hükümleri uyarınca zorunlu olarak işlendiği, söz konusu kişisel verilerin Kanunun 5 inci maddesinin (1) numaralı fıkrasının (a) bendinde yer alan “Kanunlarda açıkça öngörülmesi”, (c) bendinde yer alan “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması”, (ç) bendinde yer alan “Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması”, (e) bendinde yer alan “Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması” hukuki sebeplerine dayanarak işlendiği,

- Türk Ticaret Kanununun 855 inci maddesi uyarınca ileride meydana gelmesi muhtemel uyuşmazlıklarda delil teşkil etmek üzere, her bir taşıma için ayrı ayrı olmak üzere 3 yıl, 5 yıl ve 10 yıllık sürelerle kişisel verilerin saklandığı,
- İlgili kişinin şikâyetine konu kişisel verilerinin, bir meslek kuruluşu ile imzalanan ve söz konusu meslek kuruluşunun üyelerinin indirimli gönderim ücretlerinden yararlanmasını sağlayan sözleşme kapsamında veri sorumlusunun arşivinde bulunduğu,
- Şirketin ana müşterisi olan meslek kuruluşu ile yapılan görüşmeler devam etmekle birlikte, söz konusu kayıtların arşivleme sürecinin başlatıldığı, bu kapsamda ilgili kişinin müşteri bilgilerinin söz konusu kampanya dahilinde bir daha gönderim yapılmaması adına gönderici/alıcıya kapatıldığı,
- Bu süreçte, söz konusu kampanya kapsamında veri sorumlusunca kişilerin T.C. kimlik numaraları ile meslek kuruluşu üyesi olup olmadıklarının sorgulanabilmesi için ilgili meslek kuruluşunun sağladığı bir sistemin hayata geçirildiği, bu sistemden veri sorumlusuna yalnızca ilgili kişinin meslek kuruluşuna üye olup olmadığını gösterir “True/False” yanıtının iletildiği, bunun dışında başka bir kişisel verinin kendilerine aktarılmadığı,
- Şikâyete konu faturalandırma işleminin veri sorumlusunun acentesi tarafından sehven gerçekleştirildiği, söz konusu faturanın iptal edildiği ve işlemi gerçekleştiren acente çalışanlarına gerekli uyarıların yapıldığı

ifade edilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 30/09/2021 tarihli ve 2021/993 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanununun “Tanımlar” başlıklı 3 üncü maddesinde “ilgili kişi”nin, kişisel verisi işlenen gerçek kişi; “veri sorumlusu”nun ise kişisel verilerin işleme amaçlarını

ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlandığı,

• Kanunun, kişisel verilerin işlenmesine ilişkin “Genel İlkeler”i düzenleyen 4 üncü maddesinin (1) numaralı fıkrasında, “Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.” hükmünün yer aldığı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin;

a) Hukuka ve dürüstlük kurallarına uygun olma,

b) Doğru ve gerektiğinde güncel olma,

c) Belirli, açık ve meşru amaçlar için işleme,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,

• Kanunun “Kişisel verilerin işleme şartları” başlıklı 5 inci maddesinde;

“(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması. c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.” hükmünün yer aldığı,

• Şikâyet dilekçesinde ilgili kişi tarafından kişisel verilerinin işlenmesinin Kanunda gösterilen hukuka uygunluk sebeplerine veyahut ilgili kişinin açık rızasına dayanmadan işlendiği, kişisel verilerinin Kanunda gösterilen hukuka uygunluk sebeplerine veyahut ilgili kişinin açık rızasına

dayanmadan veri sorumlusu kargo şirketi tarafından üçüncü kişi ile paylaşıldığı ve kişisel verilerinin silinmesi talebinin yerine getirilmediği iddialarında bulunduğu,

- Somut olayda veri sorumlusunun, ilgili kişinin kişisel verilerini veri işlemenin hukuki sebepleri kapsamında işlediği, söz konusu meslek kurulu ile yapılan kampanya kapsamında ilgili kişinin üye olup olmadığını tespit edilebilmesi için kullanılan sistem nezdinde işlenen kişisel verilerin Kanunun 5 inci maddesinin (1) numaralı fıkrasının (c) bendi kapsamında sözleşmenin ifasıyla doğrudan ilgili olması hukuki şartına dayanarak işlendiği, veri sorumlusunun kişisel veri işleminde hukuka aykırılığının bulunmadığı,

- Öte yandan ilgili kişinin gönderici veya alıcı sıfatlarıyla veri sorumlusu bünyesinde gerçekleştirdiği işlemlere ilişkin kişisel verilerinin işlenmesinin hukuka uygun olduğu, ancak ilgili kişinin satın almadığı bir hizmet için adına fatura düzenlenmesinin hukuka aykırı bir veri işleme faaliyeti olduğu, hatalı faturalandırma işlemi ile Kanunun 5 inci maddesinin (2) numaralı fıkrasında sayılan veri işleme şartları bulunmadan ilgili kişinin ad, soyadı, TC kimlik numarası, adresi ve e-posta adresi bilgilerinin işlenerek adına fatura düzenlenmesinin hukuka aykırılık oluşturduğu,

- İlgili kişinin veri sorumlusu tarafından gönderilen kargo zarfında hatalı tahakkuk ettirilen faturada kişisel verilerinin açıkça yer aldığı, dolayısıyla kişisel verilerinin üçüncü kişilerin eline geçtiği iddiasına karşılık bu hususta ilgili kişi tarafından kanıtlayıcı belge sunulmadığı, ancak kargo şirketlerinin gönderi paketleri üzerine gönderici ve alıcıya ait ad, soyadı, adres, telefon numarası gibi kişisel verileri içerir barkod etiketleri yapıştırma uygulaması bulunduğu bilindiği, buna rağmen, bu etiketlerde yer alan kişisel verilerin maskelenmiş/yıldızlanmış olması ihtimali de bulunduğu; ilgili kişinin kişisel verilerinin 3. kişilere aktarıldığı iddiasının kanıtlanamadığı,

- Veri sorumlusu tarafından verilen cevabi yazıda “işlenen kişisel verilerin sözleşmenin kurulması ve ifası ile ileride meydana gelmesi muhtemel uyuşmazlıklarda delil teşkil etmesi amacı ile sınırlı bir şekilde” 6102 sayılı Türk Ticaret Kanununun 855 inci maddesinin (1) numaralı fıkrası uyarınca 1 yıl, aynı maddenin (5) numaralı fıkrası uyarınca 3 yıl ve gerekli olması halinde genel zamanaşımı süresi olan 10 yıl boyunca muhafaza edildiği”, bu nedenle ilgili kişinin kişisel verilerinin anılan süreler sona erdiğinde arşivlenmek suretiyle silineceği veya erişime kapatılacağı belirtilmiştir,

- Bu kapsamda veri sorumlusunun, ilgili kişinin kişisel verilerini Kanunda belirtilen süreler boyunca muhafaza etmesinin hukuka uygun olduğu

değerlendirmelerinden hareketle;

- İlgili kişinin kişisel verilerinin veri sorumlusu tarafından temin edilmesi hukuka uygun olsa da, hukuka uygunluk sebebi bulunmaksızın ilgili kişi adına fatura düzenlenmesi suretiyle gerçekleştirilen kişisel veri işleme faaliyetinin hukuka aykırı olduğu, bu kapsamda veri sorumlusunun Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendi çerçevesinde kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı kanaatine varılması nedeniyle; veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında idari para cezası uygulanmasına,
 - Veri sorumlusunun ilgili mevzuat gereği, işlenen kişisel verileri belirli süreler boyunca muhafaza etmesi gerektiğinden, ilgili kişinin kişisel verilerinin silinmesi talebinin yerine getirilmemesinde bir hukuka aykırılık bulunmadığına
- karar verilmiştir.

2021/889 sayılı KVKK Kararı

İlgili kişinin, bir spor tesisi tarafından açık rızası alınmaksızın yer aldığı müsabakaların kaydedilip yayınlanması hakkında Kişisel Verileri Koruma Kurulunun 03/09/2021 tarihli ve 2021/889 sayılı Karar Özeti

Karar Tarihi : 03.09.2021

Karar No : 2021/889

Konu Özeti : İlgili kişinin, bir spor tesisi tarafından açık rızası alınmaksızın yer aldığı müsabakaların kaydedilip yayınlanması

İlgili kişinin Kuruma intikal eden ihbar başvurusunda özetle; Türkiye genelinde halı saha işletmeciliği alanında faaliyet gösteren veri sorumlusunun, spor tesislerinde görüntü kaydı yapmakta olduğu, ancak görüntü kaydının tesislerde spor yapanların rızaları alınmaksızın yapıldığı, bu nedenle söz konusu faaliyetin yasalara açıkça aykırılık teşkil ettiği, kayıtların veri sorumlusunun internet platformunda da yayımlandığı, bu uygulamanın kişilerin mahrem hayatını ihlal ettiği belirtilerek Kurum tarafından 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişinin İstanbul Tesisinde kendisinin de yer aldığı bir futbol maçında kaydedilen görüntülerinin yayından kaldırılmasını talep ettiği, söz konusu talebin kendilerine ulaşmasının ardından derhal silinmesi için talepte bulunan 2 adet maç kaydının yayından kaldırıldığı,
- Maçlardan önce maç kaydı alınmaması yönünde bir talebin gelmesi halinde söz konusu taleplerin derhal yerine getirildiği ve ilgili kişinin halı saha işletmesine kaydın durdurulması yönünde bir talepte bulunmadığı,
- Maçların 2016 yılından itibaren kayıt altına alındığına ve daha sonra izlenebileceğine ilişkin bilgilendirme brandalarının tesislere asıldığı ve brandaların eskidikçe yenilendiği, tesislerin kafe, soyunma odası ve koridor gibi sosyal alanlarında da poster ve afişlerle tesiste oynanan maçların

yayınlandığı hususunun tesise gelen her ziyaretçinin kolaylıkla fark edebileceği şekilde açıkça duyurulduğu, ilgili kişilerin bu yolla aydınlatılmış olduğu,

- İlgili kişinin Kuruma yaptığı başvuru tarihindeki yayın ve imha politikalarınca kullanıcıların tesislerde yapılan bilgilendirmeler sayesinde diledikleri takdirde maç kaydının alınmamasını kolaylıkla sağlayabildikleri, internet sitesinde yayınlanan tüm maç yayınlarının sadece 15 gün yayında kaldığı, sonrasında ise geri döndürülemeyecek şekilde imha edildiği, her maç videosunun altında yer alan bildir butonu aracılığı ile maç videosunun yayından kaldırılması talebinde bulunulabildiği, buna ek olarak halı saha işletmecilerinden gelen talepler ve kişilerden gelen mesajlar üzerine de yayınların derhal yayından kaldırıldığı, ayrıca kişisel verilerin hiçbir şekilde yurtdışına aktarılmadığı,

- Kayıtların düşük kalitede olması nedeniyle kişilerin kimliklerinin tespit edilmesinin mümkün olmadığı,

- Kayıtların alınabilmesi ve ilgili spor etkinliği saatinde tesiste olacak herkesten açık rıza alınabilmesi için açık rıza formlarının hazırlanarak pilot tesislerde uygulanmaya başlandığı

ifade edilmiştir.

Yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 03/09/2021 tarihli ve 2021/889 sayılı Kararı ile;

- Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanunun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (1) numaralı fıkrasında “Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel

verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.” hükmünün yer aldığı,

- Öte yandan Kanun çerçevesinde açık rızanın, kişinin sahip olduğu verinin işlenmesine, kendi isteği ile ya da karşı taraftan gelen istek üzerine, onay vermesi anlamını taşıdığı, açık rızanın bu anlamda, rıza veren kişinin “olumlu irade beyanı”nı içermesi gerektiği, diğer mevzuattaki düzenlemeler saklı kalmak üzere, açık rızanın alınmasının şekil şartına bağlı olmadığı, açık rızanın elektronik ortam ve çağrı merkezi gibi yollarla alınmasının da mümkün olduğu, ancak burada ispat yükümlülüğünün veri sorumlusuna ait olduğu,

- Somut olayda veri sorumlusu tarafından; kayıtların alınabilmesi ve ilgili spor etkinliği saatinde tesiste olacak herkesten açık rıza alınabilmesi için açık rıza formlarının hazırlanarak pilot tesislerde uygulanmaya başlandığının ifade edildiği, söz konusu ifadeden, anılan uygulamanın yakın zamanda hayata geçirilmeye başlandığı ve henüz tüm üye tesislerde uygulanmadığı, somut başvuru tarihinde de aynı şekilde bu tip bir uygulamanın henüz hayata geçirilmemiş olduğunun anlaşıldığı,

- Bu hususa paralel şekilde, somut olay tarihinde ilgili kişilerden açık rıza alındığına ilişkin veri sorumlusu tarafından herhangi bir tevsik edici bilgi veya belgeye cevabi yazı ekinde yer verilmediğinin görüldüğü,

- Veri sorumlusu tarafından kayıtlarının düşük kalitede olması nedeniyle kişilerin kimliklerinin tespit edilmesinin mümkün olmadığı ifade edilmiş olmakla birlikte, somut olayda veri sorumlusuna ait internet sitesinde yayınlanan kayıtlar incelendiğinde, kayıtlarda görüntüleri yer alan kişilerin fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin verilerinin, bu bireylerin özgün bir şekilde teşhis edilmesini sağlayabilecek nitelikte oldukları

değerlendirmelerden hareketle;

- İlgili kişinin kişisel verisi olan görüntüsünün Kanunda yer alan herhangi bir kişisel veri işleme şartına dayanmaksızın veri sorumlusu tarafından işlendiği dikkate alındığından veri sorumlusunun Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendi kapsamında kişisel verilerin hukuka aykırı işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı sonucuna varılması nedeniyle, veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca idari para cezası uygulanmasına,

- Öte yandan, söz konusu veri işleme faaliyetinin ancak ilgili kişilerin açık rızası kapsamında gerçekleştirilebileceği dikkate alındığında, bu yönde gerekli düzenlemelerin yapılarak sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına karar verilmiştir.

2021/859 sayılı KVKK Kararı

İlgili kişinin internet hizmeti aboneliğini sağlamak üzere evine gelen şirket yetkilisinin aboneliği oluşturmak adına ilgili kişiye ait kimliğin fotoğrafını cep telefonu aracılığıyla çekmesi suretiyle kişisel verilerini işlemesi hakkında Kişisel Verileri Koruma Kurulunun 26/08/2021 tarihli ve 2021/859 sayılı Karar Özeti

Karar Tarihi : 26.08.2021

Karar No : 2021/859

Konu Özeti : İlgili kişinin internet hizmeti aboneliğini sağlamak üzere evine gelen şirket yetkilisinin aboneliği oluşturmak adına ilgili kişiye ait kimliğin fotoğrafını cep telefonu aracılığıyla çekmesi suretiyle kişisel verilerini işlemesi

İlgili kişinin Kuruma intikal eden şikâyetinde özetle, internet hizmeti alımı talebini karşılamak amacıyla evine gelen internet hizmeti sağlayan şirket yetkilileri tarafından kimlik bilgilerinin sözleşme üzerine yazılmasına rağmen ayrıca kimlik fotoğrafının da çekilmesinin istendiği, kendisinin kimlik üzerine “Müstenidattır” yazısı ekleyerek fotoğraf çekmelerini istediyse de bunun firma tarafından kabul edilmediğinin ifade edildiği, bunun üzerine hizmet alımını reddetmesi sebebiyle yetkililerin evden ayrıldığı, ardından veri sorumlusundan kimlik bilgilerinin silinmesini talep ettiği, ancak talebinin şirketin daha sonraki olası işlemlerde kendisini hatırlaması amacıyla saklandığı hususları ifade edilerek, 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında konu hakkında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup verilen cevabî yazıda özetle;

- Şirket tarafından abonelere temel ve katma değerli elektronik haberleşme hizmetlerinin sunumu, faturalama, müşteri hizmetleri, şikâyetlerin yanıtlanması gibi amaçlar için gerekli olan hallerde her bir kategori bazında kişisel verilerin işlenebildiği,
- Kimlik bilgilerinin T.C. kimlik numarası, ad, soyad, doğum yeri ve tarihi, medeni durum, cinsiyet, kimlik belgesi örneği, fotoğraf gibi kişisel verileri, iletişim bilgilerinin ise adres, telefon/faks numarası, e-posta adresi gibi kişisel verileri ifade ettiği,

- Yukarıda sıralanan kişisel veri tiplerinin işleme gerekçesinin temel olarak abonelerin şirketle yaptığı abonelik sözleşmesi kapsamında, Kanunun 5 inci maddesinin (2) numaralı fıkrasının (c) bendinde ifade edilmiş olan “bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” hükmü uyarınca olduğu,

- Şirketin Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yetkilendirilmiş ve temel iştiğal alanınının 5809 sayılı Elektronik Haberleşme Kanunu ve ilgili mevzuat çerçevesinde elektronik haberleşme hizmetlerinin sunulması olduğu, bu kapsamda Şirketin tüm ürün ve hizmet süreçleriyle ilgili BTK düzenlemelerine uymakla yükümlü olduğu, 28 Ekim 2017 tarihli Resmi Gazete’de yayımlanarak yürürlüğe giren Bilgi Teknolojileri ve İletişim Kurumu, Elektronik Haberleşme Sektörüne ilişkin Tüketici Hakları Yönetmeliğinin 7 nci maddesinin altıncı fıkrasının

“...

(6) Abonelik sözleşmelerinin elle atılan imza ile kurulması halinde, işletmeci abonelik sözleşmesinin yanında;

a) Bireysel aboneliklerde T.C. Kimlik Numarası ile kimlik belgesinin,

b) Kurumsal aboneliklerde yetkili kişinin T.C. Kimlik Numarası ve kimlik belgesi ile temsile yetkili olduğuna dair belge ile imza sirkülerinin,

c) Yabancı uyrukluların aboneliklerinde geçerlilik tarihi uygun pasaport, uluslararası geçerliliği olan muadili belge veya ulusal geçerliliği olan kimlik muadili belgenin, birer örneğini almakla yükümlüdür. Abonelik tesisi için gerekli kimlik belgesi veya muadili belgelerin aslınının ibrazı istenir. İşletmeci tarafından bu belgelerin örneği asılları üzerinden ve yalnızca uygun elektronik ortama aktarılarak alınır.

(7) İşletmeciler, abonelik sözleşmelerini ve sözleşmenin tesisi için gerekli bilgi ve belgeleri kuruluş şekline uygun olarak muhafaza etmekle yükümlüdür.” hükümlerini içerdiği,

- Bu kapsamda, abonelik sözleşmesi yapılması için kimlik fotoğrafının çekilmesi uygulamasının Elektronik Haberleşme Sektörüne ilişkin Tüketici Hakları Yönetmeliğinin 7 nci maddesinin altıncı fıkrası gereğince yükümlülük olduğu,

- Bu yükümlülüğün yerine getirilebilmesi için şirket tarafından özel bir uygulama geliştirilmiş olduğu ve kimlik belgesinin fotoğrafının ilgili çalışan tarafından şirketin bu özel uygulaması ile çekildiği, bu uygulama ile çekilen fotoğrafların direkt olarak şirketin veri tabanına aktarıldığı,

herhangi bir cihaz içerisinde veya bayi sisteminde saklanmadığı, mevzuatın izin verdiği yahut yargı kararlarının öngördüğü haller dışında üçüncü kişilerle paylaşılmadığı,

- Uygulama üzerinden çekilen ve gönderilen fotoğrafın çalışanın cihazında muhafaza edilmesinin mümkün olmayıp, belge fotoğraflarının uygulama üzerinden ve usulüne uygun olarak gönderilip gönderilmediğinin evrak arşiv sistemlerinde düzenli olarak kontrol edildiği ve denetlendiği,
- Bu kapsamda kimlik belgesinin fotoğrafının çekilmesine ilişkin hukuki gerekçenin, Kanunun 5 inci maddesinin (2) numaralı fıkrasının (ç) bendinde ifade edilmiş olan “Veri sorumlusunun hukuki yükümlülüğünün yerine getirebilmesi için zorunlu olması.” hükmü olduğu,
- Öte yandan, kişisel verilerin, Kanun ve yukarıda sayılan mevzuat başta olmak üzere ve bunlarla sınırlı olmaksızın ilgili tüm mevzuata uygun olarak, ilgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda, taraflarınca re’sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak politikada belirtilen tekniklerle silindiği, yok edildiği veya anonim hale getirildiği,
- İlgili kişinin şikayetine ilişkin taraflarınca yapılan incelemelerde, ilgili kişinin talebi ile abonelik sözleşmesi yapılması için şirket yetkililerince evine gidildiği, ancak kimlik fotoğrafının çekilmesinin istememesi sebebiyle sözleşme kurulmadığı ve kimlik fotoğrafının çekilmediğinin anlaşıldığı,
- Bununla birlikte ilgili kişinin kendisinin veya diğer resmi kurum/adli mercilerin şirketten bu kişiyle ilgili bilgi talep etmesi durumunda, ilgili kişinin şirkete başvurusunun incelenip ilgili bilgilere ulaşılabilmesi, başvuru sahibinin kimliğinin teyit edilmesi ve şikayet konusuyla eşleştirilmesi, bir başka deyişle ilgili kişinin “tanınabilmesi” için gerekli kişisel verilerinin saklanması gerektiği,
- Şirketçe ilgili mercie şikayetçi bazında yanıt verilebilmesi ve bilgi/belge sunulabilmesi için ilgili kişilerin asgari olarak kimlik bilgilerinin tutulması gerektiği, Kurumun bilgi talepli yazısının cevaplanması için gerekli verilere ulaşılmasının dahi ilgili kişinin bu işlem için ihtiyaç olan kişisel verilerinin saklanması neticesinde mümkün olduğu, bu nedenlerle ilgili kişinin kişisel verilerinin silinmesine dair başvurusunun reddedildiği, ancak söz konusu verilerin bu işleme amaçları dışında işlenmesinin söz konusu olmayacağı

ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 26/08/2021 tarih ve 2021/859 sayılı Kararı ile;

• Kanunun Tanımlar” başlıklı 3 üncü maddesinde; “kişisel veri”nin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi, “veri sorumlusu”nun, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi, “kişisel verilerin işlenmesi”nin ise kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı,

• Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

• Elektronik Haberleşme Sektörüne İlişkin Tüketici Hakları Yönetmeliğinin 7 nci maddesinin altıncı fıkrasında yer alan hüküm uyarınca veri sorumlusu tarafından abonelik sözleşmesinin tesisi için gerekli kimlik belgelerinin asılları üzerinden elektronik ortama aktarılmasının zorunlu olduğunun anlaşıldığı, dolayısıyla ilgili kişilerin kimlik belgesinin fotoğrafının çekilmesi yönündeki kişisel veri işleme faaliyetinin Kanunun 5 inci maddesinin (2) numaralı fıkrasının (ç) bendinde yer alan “veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması” hükmü temelinde gerçekleştirildiği, bu anlamda söz konusu kişisel veri işleme faaliyetinde Kanuna aykırılık unsuru bulunmadığı,

• Somut olayda ise, veri sorumlusundan alınan cevap yazısında ilgili kişinin kimlik fotoğrafının çekilmediği ve yalnızca kimlik bilgilerinin ilgili kişi ile abonelik sözleşmesi yapılması için o aşamada işlendiğinin belirtildiği göz önünde bulundurulduğunda söz konusu kimlik bilgilerinin Kanunun 5

inci maddesinin (2) numaralı fıkrasının (c) bendinde yer alan “bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” hükmü uyarınca işlendiğinin anlaşıldığı,

- Bununla birlikte ilgili kişinin sonraki aşamada sözleşme yapmaktan vazgeçmesi üzerine bilgilerinin silinmesini talep ettiği, veri sorumlusu tarafından ise ilgili kişinin tüketici sıfatını kazanması nedeniyle veri sorumlusu bünyesinde kişinin kimlik teyidinin yapılması adına asgari düzeyde kimlik bilgilerinin işlenmesinin söz konusu şikayet süreçlerinin sağlıklı yürütülmesi ve şikayete ilişkin ilgili mercilere yanıt verilmesi adına işlenmeye devam edildiğinin beyan edildiği,

- Her ne kadar sözleşme taraflar arasında kurulmamış olsa dahi kişinin tüketici sıfatını kazanması nedeniyle şirket hakkında çeşitli mecralarda ileri sürebileceği şikayetlerin söz konusu olabileceği, bu anlamda veri sorumlusunun kendini savunma hakkının gündeme geldiği, Anayasanın 36 ncı maddesinde adil yargılanma hakkının; herkesin, meşru vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahip olması şeklinde düzenlendiği, savunma hakkının, suç islediği iddia edilen kişinin, devlet ya da bireyler tarafından kendi varlığına yöneltilen eylem ve işlemlere karşı kendisini korumak için yasal yollara başvurması veya yasal imkanlardan faydalanması olarak tanımlandığı,

- Bu kapsamda, ilgili kişinin talebi üzerine, veri sorumlusu şirket ile hizmet sözleşmesi kurulmasını teminen ilgili kişinin kimlik verilerinin işlendiği ancak ilgili kişi tarafından sonradan sözleşme kurulmasından vazgeçilmesi sebebiyle, Kanunun 5 inci maddesinin (2) numaralı fıkrasının (c) bendinde yer alan “bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” işleme şartının ortadan kalktığı, bunun yanı sıra şikayet süreçlerinin sağlıklı yürütülmesi adına kimlik bilgilerinin işlendiği ve ilgili kişinin veri sorumlusu hakkında muhtelif mercilere yapabileceği şikayetler kapsamında savunma hakkının gereği gibi sağlanabilmesini teminen asgari düzeydeki kimlik bilgilerinin işlenmesinin zorunlu olduğu dikkate alındığında Kanunun 5 inci maddesinin (2) numaralı fıkrasının (e) bendinde yer alan “bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması” hükmü uyarınca veri sorumlusu tarafından ilgili kişiye ait asgari düzeyde kimlik verisinin işlenmesinde hukuka aykırılık bulunmadığı, ancak söz konusu verilerin amaçla bağlantılı olarak asgari süreyle sınırlı olarak saklanması ve amacı dışında kullanılmaması ile veri sorumlusu tarafından sözleşme vasıtasıyla işlenen kişinin diğer verilerinin ise imha politikasına uygun bir şekilde imha edilmesinin önem arz ettiği

değerlendirmelerinden hareketle,

- İlgili kişinin talebi üzerine veri sorumlusu şirket ile hizmet sözleşmesi kurulmasını teminen ilgili kişinin kimlik verilerinin işlendiği ancak ilgili kişi tarafından sonradan sözleşme kurulmasından vazgeçilmesi sebebiyle verilerin silinmesi talebinde bulunulduğu, ancak ilgili kişinin veri sorumlusu hakkında muhtelif mercilere yapabileceği şikayetler kapsamında sınırlı düzeyde kişisel verilerinin işlenmesinin zorunlu olduğu dikkate alındığında Kanunun 5 inci maddesinin (2) numaralı fıkrasının (e) bendinde yer alan “bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması” hükmü uyarınca veri sorumlusu tarafından ilgili kişiye ait asgari düzeyde kimlik verisinin işlenmesinde hukuka aykırılık bulunmadığına, ancak söz konusu verilerin amaçla bağlantılı olarak asgari süreyle sınırlı olarak saklanması ve amacı dışında kullanılmaması ile veri sorumlusu tarafından sözleşme vasıtasıyla işlenen kişinin diğer verilerinin ise imha politikasına uygun bir şekilde imha edilmesi hususunda veri sorumlusunun talimatlandırılmasına karar verilmiştir.

2021/850 sayılı KVKK Kararı

Şikayetçinin ablasının kimlik bilgilerinin numara taşıma işlemi adına bir telekomünikasyon şirketinin bayi çalışanına ait telefon marifetiyle fotoğraflanarak kullanılan sisteme yüklenmesi hakkındaki ihbara ilişkin Kişisel Verileri Koruma Kurulunun 26/08/2021 tarihli ve 2021/850 sayılı Karar Özeti

Karar Tarihi : 26.08.2021

Karar No : 2021/850

Konu Özeti : Şikayetçinin ablasının kimlik bilgilerinin numara taşıma işlemi adına bir telekomünikasyon şirketinin bayi çalışanına ait telefon marifetiyle fotoğraflanarak kullanılan sisteme yüklenmesi

Kuruma intikal eden ihbarda özetle, şikayetçinin ablası adına kayıtlı hattın taşıma işlemi için bir telekomünikasyon şirketinin bayisine uğradığı, ablasının kimliğinin bayide çalışan bir şahsa ait olan telefon ile fotoğraflandığı, çalışanların fotoğrafı şirketlerine ait bir uygulama üzerinden sisteme yüklediklerini ifade ettikleri, bu uygulamanın şahsî telefonlar üzerinden kullanılmasının, daha sonra işten ayrılan bir şahsın elinde birçok bilginin olmasına sebep olabileceği ve kötü niyetli işlemler yapılabilme riski taşıdığı, telekomünikasyon alanında faaliyet gösteren bir diğer firmanın, benzer bir uygulamayı kurumsal olarak tanımlanmış, IP adresi belirlenmiş, güvenli ve takip edilebilir bir cihazla yaptığı, şikayetçinin bu hususta Bilgi Teknolojileri ve İletişim Kurumuna (BTK) başvurduğu ve şikayete konu şirketin verdiği yanıtta “.....2018 tarihi itibarıyla Kimliklerin Dijital Ortama Aktarılması projesini devreye aldığı, bu proje ile kimliklerin dijital ortama aktarılması işleminin gerçekleştirildiği, bu uygulamanın yalnızca mobil cihazlarda çalıştığı, her personelin kendi telefonu üzerinden kendi kullanıcı kodu ve şifresi ile bu sisteme girerek kimliği tarama işlemini gerçekleştirdiği, ancak kimliklerin telefonda saklanması, depolanması ve üçüncü kişilerle paylaşılması durumunun söz konusu olmadığı” ifadelerine yer verildiği, fakat ihbar sahibinin bu durumda dahi müşterilerin kimlik bilgilerinin, veri kurtarma bilişimi sebebiyle tehdit altında bulunduğunu düşündüğü ifade edilerek, konu hakkında gerekli incelemenin yürütülmesi talep edilmiştir.

Konuya ilişkin başlatılan resen inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabî yazıda özetle;

- Veri sorumlusunun telekomünikasyon sektöründe faaliyet göstermekte olduğundan, BTK mevzuatı kapsamında faaliyetlerini sürdürdüğü ve Numara Taşınabilirliği (hat taşıma) işleminin de ayrıntılı olarak 5809 sayılı Elektronik Haberleşme Kanunu ve ilgili mevzuatlar kapsamında düzenlendiği,
- Yine BTK tarafından yayımlanan “Numara Taşınabilirliği Uygulama Sürecine İlişkin Usul ve Esaslar” da numara taşıma işlemi sırasında alınacak bilgilerin, imzalanacak formların ve doğrulama süreci ile ilgili hususların ayrıntısı ile hüküm altına alındığı,
- Numara taşıma taleplerinde, Numara Taşıma Yönetmeliğinin 7 nci maddesi ve Numara Taşınabilirliği Uygulama Sürecine İlişkin Usul ve Esasların 5 inci maddesinin (2) numaralı fıkrasının a/2 bendi kapsamında; abone tarafından taşınacak olan numaranın, kimlik bilgilerinin, verici işletmeci bilgisinin, irtibat bilgilerinin ve tercih ettiği taşıma zamanının, doldurulan matbu bir form alıcı işletmeye bildirilmesi gerektiği, alıcı işletmecinin söz konusu talep formunu, kimlik bilgileri ve diğer ilgili bilgileri alarak verici işletmeye göndermek üzere söz konusu belgeleri numara taşınabilirliği sistemine yüklemekle yükümlü olduğu, bu kapsamda söz konusu bilgilerin yanı sıra dijital sisteme aktarılmak üzere abone kimliği ve söz konusu işletmeci ile taşıma işleminin gerçekleşmesinden itibaren geçerli olacak şekilde abonelik sözleşmesinin alındığı,
- Bu kapsamda Şirketin, abonenin numarasının taşınmasına ilişkin imzalı talep formu ile kimliğini, verici işletmeye göndermek üzere elektronik ortamda alarak numara taşıma sistemine ulaştırdığı,
- Diğer taraftan BTK'nin 28.10.2017 tarih ve 30224 sayılı Resmî Gazetede yayımlanan “Elektronik Haberleşme Sektörüne İlişkin Tüketici Hakları Yönetmeliği”nin “Abonelik sözleşmelerinin kuruluşu ve içeriği” başlıklı 7 nci maddesinin (6) ve (7) numaralı fıkralarının ilgili bentlerinde; abonelik sözleşmelerinin elle atılan imza ile kurulması halinde, işletmecinin, abonelik sözleşmesinin yanında, bireysel aboneliklerde T.C. kimlik numarası ile kimlik belgesinin birer örneğini almakla yükümlü olduğu ve abonelik tesisi için gerekli kimlik belgesi veya muadili belgelerin aslının ibrazını isteyeceği, işletmecinin bu belgelerin örneğini, asılları üzerinden ve yalnızca uygun elektronik ortama aktararak alacağı hükümlerinin yer aldığı,
- Dolayısıyla veri sorumlusunun, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) “Kişisel verilerin işleme şartları” başlığını haiz 5 inci maddesinin (2) numaralı fıkrasında yer alan (a), (c) ve (ç) bentlerinde ifade edilen; “Kanunlarda açıkça öngörülmesi”, “Bir sözleşmenin kurulması

veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” ve “Veri sorumlusunun hukukî yükümlülüğünü yerine getirebilmesi için zorunlu olması” şartlarına dayanarak söz konusu kişisel verileri işlediği,

- Veri sorumlusunun, bilgi güvenliği politikaları ve BTK düzenlemeleri kapsamında her türlü teknik ve idarî tedbiri aldığı ve bunların, ilgili kişinin başvurusunda belirttiği tedbirlerden daha ileri tedbirler olduğu,
- Abonelik veya numara taşımaya ilişkin bir başvuru esnasında müşteriden alınacak olan kimlik belgesi örneğinin, uygulama üzerinden elektronik ortamda alınarak veri sorumlusunun merkezî sunucularına aktarıldığı ve ilgili düzenleme gereği muhafaza edilecek şekilde aboneyle ilişkilendirildiği,
- Söz konusu uygulamanın yalnızca mobil telefonlarda çalışıyor olduğu ve anılan uygulamada gerekli güvenlik önlemlerinin alındığı, (Alınan güvenlik önlemlerinin ise detaylı şekilde açıklandığı ve tevsik edici belgelerin yazıları ekinde Kuruma sunulduğu görülmüştür)

ifade edilmiştir.

Veri sorumlusundan ilgili cevabın alınmasını müteakip 19.01.2021 tarih ve 2021/55 sayılı Kurul Kararı ile; “... konunun detaylarının ortaya koyulabilmesi adına üç operatör şirketini temsil eden Mobil Telekomünikasyon Operatörleri Derneği’nden (m-TOD) bilgi temin edilmek suretiyle incelemenin devamına...” karar verilmiş ve bahse konu Kurul Kararı uyarınca m-TOD’a başvuru konusu ile ilgili bilgilendirmeler yapılarak;

- İhbar sahibi tarafından Kuruma intikal ettirilen hususların veri güvenliği ihlali riski oluşturup oluşturamayacağı,
- Bayi personelinin şahsî cep telefonlarına müşterilerin kimlik fotokopilerini kaydetmesini önlemek maksadıyla, bu işlemin her bayide yalnızca bu işe özgülenen, kurumsal olarak takip edilebilen ve yetkisiz erişimi mümkün olmayan tablet veya cep telefonu gibi bir mobil cihaz vasıtasıyla ya da ilgili kişinin kendisi tarafından gerçekleştirilmesinin operatör şirketleri açısından mümkün olup olmadığı hususlarında bilgi talep edilmiştir.

m-TOD’un konuya ilişkin cevabî yazısında ise özetle;

- Derneğin tüm üyelerinin; ürün ve hizmet süreçleriyle ilgili olarak BTK düzenlemelerine uymakla yükümlü olduğu, BTK tarafından konuya ilişkin yönetmeliklerin dijitalleşme trendi göz önüne alınarak güncellendiği ve bu sebeple mobil operatörlerin, abonelik tesis ederken T.C. kimlik numarası

ile kimlik belgesini asıllarına uygun olarak elektronik ortama aktararak almak zorunluluğunun bulunduđu,

- Cep telefonlarının yalnızca mobil operatörlerinin bayi ađında deđil, birçok firmanın personeli tarafından iş amaçlı olarak yaygın bir şekilde kullanıldıđı, alınan tüm idarî ve teknik tedbirlere rađmen insan faktörü sebebiyle her iş sektörü için riskler doğabildiđi, mobil telekomünikasyon sektöründe karşılaşılabilecek risklerin, diđer sektörlerdeki herhangi bir güvenlik riskinden daha farklı olmayacağı, öte yandan kimlik fotokopisinin alındıđı geçmişteki uygulamalara nazaran şimdiki metodun en güvenli metot olduđu,

- Bayi kanalıyla yapılan abonelik süreçlerinde müşterilerin kimlik fotokopilerinin alınması sürecinin, işletme tarafından özel olarak tahsis edilmiş cihazlar ya da işletmecinin uygulamasının kurulmasının yapıldıđı şahsi cihazlar üzerinden yürütölmekte olduđu, bu iki yöntemin de güvenli olduđu, bununla birlikte işletmeci tarafından özel olarak tahsis edilmiş cihazların bayilerde gerçekleştirilen abonelik süreçlerinde kullanımının yaygınlığının artırılması yönündeki çalışmaların sürdüröldüđu,

- Abonelik ilişkisinin tesisi sırasında kurumsal cihazlar veya personele ait fakat içerisinde güvenlik tedbiri alınmış kurumsal yazılım bulunan şahsî cihazlar vasıtasıyla işlem yapılabilirdiđi ve bu iki usulün de güvenli olduđu ancak ilgili kişinin kendisi tarafından bu işlemlerin gerçekleştirilmesinin mümkün ve güvenli olmayacağı, zira bu suretle uygulamanın yetkisiz erişime açılmış olacağı ve kötü niyetli kullanım olasılıđının artacağı, uygulamanın uç tarafında ise işletme servisleriyle entegrasyon bulunduđu ve ilgili kişilerin bu sisteme erişmesinin yüksek dereceli güvenlik riski doğurabileceđi, ayrıca herkesin bu uygulamaları kullanmaya yetkin telefonunun olmaması nedeniyle sistemde yeknesaklık sağlanamayacağı

belirtilmiştir.

Söz konusu resen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 26/08/2021 tarihli ve 2021/850 sayılı Kararı ile;

- Kanunun, kişisel verilerin işlenmesine ilişkin “Genel İlkeler”i düzenleyen 4 üncü maddesinin (1) numaralı fıkrasında, “Kişisel veriler, ancak bu Kanunda ve diđer kanunlarda öngörölen usul ve esaslara uygun olarak işlenebilir.” hükmünün yer aldıđı, bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin;

a) Hukuka ve dürüstlük kurallarına uygun olma,

b) Doğru ve gerektiğinde güncel olma,

c) Belirli, açık ve meşru amaçlar için işlenme,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,

- Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanunun “Veri Güvenliğine İlişkin Yükümlülükler”i düzenleyen 12 nci maddesinin (1) numaralı fıkrasında veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idarî tedbirleri almak zorunda olduğunun hükme bağladığı, anılan maddenin (3) numaralı fıkrasında veri sorumlusunun, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak ile yükümlü kılındığı,

- İhbar sahibinin veri sorumlusu bünyesinde çalışan personellerin abonelik veya numara taşıma işlemleri sırasında müşterinin kimlik belgesinin fotoğrafını kendi şahsî cep telefonlarıyla çektiklerini ifade ederek, bu durumun veri güvenliğini tehlikeye düşürdüğünü iddia ettiği, veri sorumlusunun da bu metodu kullandığını doğruladığı fakat veri sorumlusunun; söz konusu kimlik bilgilerinin, konuyla ilgili mevzuattan kaynaklanan yasal zorunluluk gereği alınıp elektronik ortama aktarıldığını, bu aktarım işlemini gerçekleştiren uygulamayla ilgili her türlü teknik ve idarî tedbirin alındığını, müşteri kimlik bilgilerinin asla şahsî telefonlarda depolanmadığı ve uygulamadaki tedbirler

sayesinde veri sorumlusunun çalışanlarının çekilen kimlik fotoğraflarına tekrar erişemediği hususlarını ifade ederek, bu verileri işlemenin yasal ve güvenli olduğunu savunduğu,

- Veri sorumlusunun, ilgili verileri, Kanunun “Kişisel verilerin işleme şartları” başlığını haiz 5 inci maddesinin (2) numaralı fıkrasında yer alan (a), (c) ve (ç) bentlerinde ifade edilen; “Kanunlarda açıkça öngörülmesi”, “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” ve “Veri sorumlusunun hukukî yükümlülüğünü yerine getirebilmesi için zorunlu olması” şartlarına dayanarak işlediği ve bu yönden ilgili veri işleme faaliyetlerinin hukuka uygun olduğu,

- Öte yandan veri sorumlusunun, müşterilere ait kimlik belgelerinin üzerinden temin edildiği uygulamanın çalışmasına dair makul teknik tedbirleri aldığı ve bunun yanı sıra bahse konu uygulamayı kullanan personele yönelik de gizlilik taahhütnameleri imzalatmak, eğitim vermek, farkındalık duyuruları yayınlamak gibi idarî tedbirlere de başvurduğu, bu kapsamda veri sorumlusunun, Kanunun 12 nci maddesinde belirtilen yükümlülüklerini yerine getirdiği,

değerlendirmelerden hareketle,

- Numara taşıma işlemi sırasında ilgili kişilerin kimlik fotokopilerinin alınmasının mevzuatta öngörülmüş olması sebebiyle bahse konu durumun Kanuna ve ilgili mevzuata aykırılık teşkil etmediğine,

- Veri sorumlusu tarafından uygulamanın çalışmasına ilişkin alınmış olan teknik ve idarî tedbirlerin makul olduğu değerlendirildiğinden somut hadisede Kanunun 12 nci maddesinde belirtilen yükümlülüklerle aykırı bir husus bulunamadığına,

- Bununla birlikte, Kanunun 4 üncü maddesinin (2) numaralı fıkrası çerçevesinde, kişisel verilerin işlenmesindeki genel ilkelere uyum sağlanması noktasında veri sorumlusunun personelin şahsî cihazlarından ziyade bayilere tanımlanmış, düzenli olarak denetlenen ve takibi yapılan kurumsal cihazlar vasıtasıyla iş ve işlemlerinin yürütülmesi usulünün hızlandırılması hususunda talimatlandırılmasına,

- Öte yandan Kanunun 10 uncu maddesinde düzenlenen aydınlatma yükümlülüğünün gereklerinin yerine getirilmesini teminen bayilerde numara taşıma işlemi yapan ilgili kişilere kurumsal bir uygulama üzerinden kimlik fotokopilerinin kayıt edildiğine dair aydınlatmanın yapılması hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2021/847 sayılı KVKK Kararı

İlgili kişinin bir web sitesinden kişisel verilerinin silinmesi talebinin veri sorumlusu tarafından yerine getirilmemesi hakkında Kişisel Verileri Koruma Kurulunun 26/08/2021 tarihli ve 2021/847 sayılı Karar Özeti

Karar Tarihi : 26.08.2021

Karar No : 2021/847

Konu Özeti : İlgili kişinin bir web sitesinden kişisel verilerinin silinmesi talebinin veri sorumlusu tarafından yerine getirilmemesi

İlgili kişinin Kuruma intikal eden şikâyetinde özetle; bir şirkete ait web sitesi üzerinden daha önce kullandığı ancak şu anda kullanmadığı adres bilgilerinin silinmesini talep ettiği ancak bu yöndeki talebinin iki kez reddedildiği ve silme işleminin gerçekleştirilmeyeceğinin bildirildiği beyan ve iddiaları ile veri sorumlusu hakkında gerekli yasal işlemlerin yapılması talep edilmiştir.

Bu kapsamda başlatılan inceleme çerçevesinde söz konusu iddialara ilişkin veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- İlgili kişinin hesabına kayıtlı olan adreslerin silinmesine yönelik işlemlerin nasıl gerçekleştirileceğine dair sorusunun şirket yetkilisi tarafından fatura adreslerinin silinemeyeceği şeklinde cevaplandırıldığı; bu cevaba karşı ilgili kişinin yasal olarak kişisel bilgilerini istediği zaman istediği yerden silme hakkının mevcut olduğunu, bilgileri silinmezse hakkını yasal olarak aramak zorunda kalacağını belirttiği; bunun üzerine ilgili kişiye yetkili tarafından geçmiş dönem faturalardaki bilgilerinin silinemeyeceğinin iletildiği,
- 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 4 üncü maddesinde kişisel verilerin ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerektiğinin öngörüldüğü, faturaların 213 sayılı Vergi Usul Kanunu uyarınca gerekli vergi süreçlerinden kaynaklı saklama süresinin beş yıl olarak değerlendirilebileceği,
- Satış sözleşmesi uyarınca müşteri tarafından gerçekleştirilen ödemeleri göstermek üzere müşteriye verilen bir ticari vesika mahiyetinde olan fatura kapsamında işlenen kişisel verilerin, sözleşmenin

ifası esnasında tarafların yükümlülüklerini yerine getirdiğine yönelik bir dayanak oluşturmayı amaçladığı,

- Bundan dolayı fatura üzerindeki kişisel verilerin, Kanunun 5 inci maddesindeki kişisel veri işleme şartlarından “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.” veri işleme şartı kapsamında değerlendirildiği,

- 6098 sayılı Türk Borçlar Kanununca düzenlenen satış sözleşmesi kapsamında ifa edilen edimlere ilişkin bilgileri içeren faturanın, satış sözleşmesine aykırı davranışlarda ve sözleşmenin hiç veya gereği gibi yerine getirilmemesinden kaynaklanan anlaşmazlıkların gündeme gelmesi halinde, hak kaybı yaşanmaması amacıyla on yıl süreyle saklanması mevzuatta öngörülen zamanaşımı süreleri ile doğru orantılı olduğu,

- Dolayısıyla şirketlerince ilgili kişinin adres bilgilerinin güncellenmesine imkân verildiği; ancak geçmiş adres bilgilerinin detaylıca açıkladıkları mevzuat ve sözleşmesel ilişki gereği on yıl süre ile muhafaza edildiği,

- Üyelerin serbest bir şekilde güncel adreslerinde değişiklik yapma hakkına sahip olduğu ancak geçmişte yapılan satış/hizmet alım sözleşmelerinin her biri ayrı birer kurulu sözleşme sayılacağı için söz konusu adreslerin sistemlerinde saklandığı, kullanılan adresin silinmesinin muhasebesel olarak siparişi alınmış ürün ile ilgili kayıtların da silinmesi anlamına geleceği, bu durumun tüketicilere sözleşme öncesinde sunulan “Üyelik Sözleşmesi”nin açıklamalar kısmında da sabit olduğu

ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 26/08/2021 tarihli ve 2021/847 sayılı Kararı ile;

- Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinin (2) numaralı fıkrası uyarınca kişisel verilerin işlenmesinde: a) Hukuka ve dürüstlük kurallarına uygun olma. b) Doğru ve gerektiğinde güncel olma. c) Belirli, açık ve meşru amaçlar için işlenme. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uyulmasının zorunlu olduğu,

- Kanunun 7 nci maddesinin (1) numaralı fıkrasında “Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hale getirilir.” hükmünün, (2) numaralı fıkrasında ise “Kişisel verilerin silinmesi, yok

edilmesi veya anonim hale getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır.” hükmünün düzenlendiği,

- 213 sayılı Vergi Usul Kanununun 230 uncu maddesinde faturada bulunması gereken bilgiler arasında müşterinin adresinin de yer aldığı, bununla birlikte, 213 sayılı Kanunun 253 ve 254 üncü maddeleri uyarınca fatura belgelerinin beş yıl süre ile muhafaza edileceğinin düzenlendiği,
- Veri sorumlusu tarafından ise faturanın 6098 sayılı Türk Borçlar Kanununda düzenlenen satış sözleşmesine ilişkin bir sürecin parçası olduğu; satış sözleşmesine aykırı davranışlardan ve sözleşmenin hiç veya gereği gibi yerine getirilmemesinden kaynaklanan anlaşmazlıklara on yıllık genel zamanaşımı süresinin uygulanacağı, fatura üzerindeki kişisel verilerin, Kanunun 5 inci maddesindeki kişisel veri işleme şartlarından olan “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.” veri işleme şartı kapsamında değerlendirildiği,
- Bu kapsamda, adres bilgisinin hem fatura belgesi hem de satış sözleşmesinde olduğu gibi birden fazla amaca ve hukuki sebebe dayanarak işlenebileceği, farklı veri işleme faaliyetlerindeki aynı kişisel veriler için öngörülen saklama sürelerinin farklı olabileceği, bu doğrultuda, ilgili kişinin fatura belgeleri ve dolaylı olarak üzerinde yer alan adres bilgilerinin işlenmesi için geçerli bir işleme amacı ve hukuki gerekçenin bulunduğu, ayrıca veri sorumlusu tarafından belirlenen on yıllık saklama süresinin Türk Borçlar Kanununun 146 ncı maddesinde yer alan “Kanunda aksine bir hüküm bulunmadıkça, her alacak on yıllık zamanaşımına tabidir.” hükmü uyarınca mevzuatta öngörülen en uzun süreye uygun olarak belirlendiği, bu kapsamda veri sorumlusunun yazısı ekinde yer alan dokümanlar incelendiğinde ilgili kişiye ait 2012, 2016, 2018 ve 2021 tarihli fatura belgelerinin bulunduğu görüldüğü, her bir fatura belgesi tarihinin ayrı olarak değerlendirilmesi sonucunda fatura belgeleri ve dolaylı olarak adres bilgileri için veri sorumlusu tarafından belirlenen saklama süresinin henüz tamamlanmadığının anlaşıldığı,
- Bununla birlikte, ilgili kişinin bireysel hesabının ekran görüntüsü incelendiğinde; “Profil Bilgilerim” sayfasının “Fatura Adres Bilgilerim” başlığı altında varsayılan adres olarak bir adresin seçilebildiği ve adres üzerinde “Düzenle” ve “Sil” olmak üzere iki seçeneğin yer aldığı, “Diğer Kayıtlı Adresler” başlığı altında ise adresler üzerinde “Varsayılan Yap”, “Düzenle” ve “Sil” şeklindeki seçeneklerin yer aldığı görüldüğü, ancak, veri sorumlusunca söz konusu seçeneklerin yer almasına rağmen fatura adresi olarak kullanılmış adres bilgilerinin fatura belgeleri ile ilişkilendirilmesi sebebiyle ilgili kişinin hesabında “Profil Bilgileri” altında belirlenen saklama süresi boyunca yer almaya devam edeceği ve üzerinde bir işlem yapılamayacağı belirtilmiştir,

- Satış sözleşmesi kapsamındaki anlaşmazlıklara yönelik fatura belgelerinin saklanması ile söz konusu fatura adresi bilgilerinin ilgili kişinin bireysel hesabında da saklanmasının iki farklı veri işleme faaliyeti olduğu, veri sorumlusu tarafından belirtilen saklama süresinin ilgili kişiye ait fatura belgeleri veya satış sözleşmesinin saklanması için geçerli olduğu, bununla birlikte kullanıcıların bireysel hesaplarına kaydettikleri adres bilgileri üzerinde silme, güncelleme gibi çeşitli düzenlemeleri yapma hakkına sahip olduğu ve bu alanda güncel olan adres bilgilerinin yer almasının ilgili kişinin sorumluluğunda olduğu,

- Ancak veri sorumlusunun da verilerin doğru ve güncel olmasını sağlayabilecek imkânları ilgili kişilere sağlaması gerektiği, güncel olmayan adres bilgilerinin bireysel hesap üzerinde de saklanması ve fatura adresi olarak kullanılmaları gerekçesiyle bu adres bilgileri üzerinde herhangi bir işlem yapılamamasının Kanunun 4 üncü maddesinin (2) numaralı fıkrasının (b) bendi uyarınca kişisel verilerin doğru ve gerektiğinde güncel olma ilkesine aykırılık teşkil ettiği

değerlendirmelerinden hareketle;

- İlgili kişinin fatura belgelerinin veri sorumlusunun Türk Borçlar Kanunundan kaynaklanan yükümlülükleri kapsamında on yıl saklanabileceği, bununla birlikte bireysel hesap üzerinde güncel adres bilgilerinin bulunması gereken alanda hâlihazırda kullanılmayan adres bilgilerinin de yer aldığı ve bu adres bilgileri üzerinde ilgili kişiler tarafından herhangi bir işlem yapılmadığı dikkate alındığında Kanunun 4 üncü maddesinin (2) numaralı fıkrasının (b) bendinde yer alan kişisel verilerin “doğru ve gerektiğinde güncel olma” ilkesinin yerine getirilebilmesi ve bu kapsamda kişisel verilerin güncellenmesine/imha edilmesine ve güncel olmayan kişisel verilerin ilgili kişilere gösterilmemesine imkân sağlayacak kanalların oluşturulması ile imha edilen/edilmesi istenen kişisel verilerin saklama amacı dışında kullanılmamasına ilişkin gerekli tedbirlerin alınması ve sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2021/799 sayılı KVKK Kararı

İlgili kişinin uluslararası geçerliliği olan bir dil sınavı konusunda Türkiye'deki akredite kuruluş tarafından kişisel verilerinin hukuka aykırı işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 12/08/2021 tarihli ve 2021/799 sayılı Karar Özeti

Karar Tarihi : 12.08.2021

Karar No : 2021/799

Konu Özeti : İlgili kişinin uluslararası geçerliliği olan bir dil sınavı konusunda Türkiye'deki akredite kuruluş tarafından kişisel verilerinin hukuka aykırı işlenmesi

İlgili kişinin Kuruma intikal ettirdiği şikâyet dilekçesinde özetle; uluslararası geçerliliği olan bir dil sınavı konusunda ilgili akredite kuruluşun düzenlemiş olduğu sınava girdiği, bu sınav öncesinde herhangi bir veri işleme şartına dayanmaksızın ilgili kişiye ait özel nitelikli kişisel verisi olan görsel kaydının (biyometrik fotoğraf) ve parmak izinin alındığı, giriş kaydının alternatif yollarla sağlanmasının mümkün olduğu, bu kapsamda bahsi geçen kuruluşa başvuruda bulunarak 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 11 inci maddesi kapsamındaki hakları ve kişisel verilerinin saklama süresi sona erince ne şekilde imha edildiği hakkında bilgi edinme talebinde bulunduğu, ancak başvurusunun haksız ve mesnetsiz gerekçelerle reddedildiği, kuruluşun söz konusu uluslararası dil sınavına ilişkin olarak Türkiye'deki süreçleri yürüten ve çeşitli uluslararası kurum ve kuruluşların yetkilendirdiği bir tüzel kişilik olduğu, bu kapsamda sınava katılan adayların kişisel verilerinin yurt dışına aktarılmasının kaçınılmaz olduğu ancak aktarım hakkında bilgilendirilmediği, diğer taraftan iletişim bilgilerinin de reklam ve pazarlama amaçlı olarak açık rızası alınmaksızın ve aydınlatma yükümlülüğü yerine getirilmeksizin hukuka aykırı olarak işlendiği hususları ifade edilerek 6698 sayılı Kanun kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde söz konusu iddialara yönelik ilgili şirketten savunması istenilmiş olup, alınan cevabi yazıda özetle,

- Öncelikle ilgili kişinin başvurusunda ad-soyad bilgisinin hatalı yazılmış olması sebebiyle Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğe (Tebliğ) uygun olarak taraflarına başvuru yapılmadığı,

- Sınava başvuran adaylardan kimlik bilgileri (adı, baba adı, ana adı, doğum yeri, doğum tarihi vatandaşlık numarası, kimlik seri no, kimlik geçerlilik tarihi), iletişim bilgileri (iletişim adresi, e-posta adresi, telefon numarası, ülke, şehir, posta kodu, ilçe), login ve kullanıcı adı, cinsiyeti, banka hesap bilgileri, engellilik durumu, sağlık raporu, dijital fotoğrafı, dijital parmak taraması ve el yazısı verilerinin alındığı,
- İlgili kişi tarafından iddia edildiğinin aksine taraflarınca biyometrik değil çehre görüntüsü gibi herkes tarafından bilinen, görünen ve kamuya açık dijital vesikalık fotoğrafının hizmet ilişkisi kapsamında kayıt altına alındığı, bahse konu verilerin, sınava girmek isteyen kişinin kaydının oluşturulması ve sınav sürecinin yönetilmesi için alınmasının zorunlu olduğu, dolayısıyla bu verilerin şirketleri ve sınava girecek kişiler arasında 6698 sayılı Kanununun 5 inci maddesinin (2) numaralı fıkrasının (c) bendi uyarınca bir sözleşmenin kurulması ve ifasıyla doğrudan doğruya ilgili olması sebebiyle alınması zorunlu bilgilerden olduğu ve ilgili kişinin açık rızasına tabi olmadığı,
- Parmak tarama kayıtlarının ise sınav güvenliği ve kimlik doğruluğunu sağlamak adına alınmasının şart olduğu, bu kayıtların yurt içi ya da yurt dışına aktarılmadığı, bu sistemin hizmet kalitesini standart hale getirmek amacıyla tüm dünyada söz konusu dil sınavını yapan merkez tarafından zorunlu tutulduğu, küresel olarak belirlenmiş olan bahse konu dil sınavının Güvenlik Protokollerine tüm yetkili sınav uygulayıcılarının uymakla yükümlü olduğu, parmak izi taramasının parmak izi şeklinde olmadığı, "görüntü kaydı" yöntemiyle alındığı ve yalnızca eşleştirme yapıldığı, parmak izi taramasında mürekkep, sıvı ya da herhangi bir kimyasal içermeyen elektronik tarayıcı kullanıldığı, parmağın herhangi bir görüntüsünün alınmadığı ya da saklanmadığı bunun yerine adayı tanımlayacak benzersiz bir sayı dizisine dönüştürüldüğü, parmak taramasına onay verilmesinin sözleşmenin ifası açısından zorunlu bir unsur olmadığı, kişilerden açık rıza alınmadığı takdirde parmak tarama kayıtlarının işlenmediği, buna ilişkin gerekli bilgilendirmenin ilgili kişilere yapılarak açık rızalarının olup olmadığının öğrenildiği,
- Bu kapsamda, sınava girecek adaylardan Kanununun 5 inci maddesinin (2) numaralı fıkrasının (c) bendi kapsamında kişisel verilerin toplandığı, özel nitelikli kişisel veriler bakımından ise adaylardan rızalarının alındığı,
- Kişisel verilerin işlenmesi sürecinde Kanununun 10 uncu maddesi kapsamındaki aydınlatma yükümlülüğü ile ilgili olarak, gizlilik politikası ve kullanım koşulları metinleri ile toplanan kişisel verilere ilişkin bilgilendirme sağlamak adına söz konusu metinlerin internet sitesinde yayınlandığı, internet üzerinden sınav başvurusunda bulunan kişilerin üyelik formunu doldurmak zorunda

oldukları ve bu esnada ilgili metinlere link verildiği, internet üzerinden başvuru yapmayan adaylara ise iletişim adreslerine söz konusu link ve metinlerin gönderildiği,

- Öte yandan söz konusu sınava girişte elde edilen kişisel verilerin işleme amaçlarının ve vasıtalarının belirlenmesinden, veri kayıt sisteminin kurulmasından ve yönetilmesinden merkezi yurt dışından bulunan bir başka kuruluşun sorumlu olduğu, Türkiye’de kurulu bulunan şirketin tüm çalışma, pazarlama ve işletme esaslarının kurucu şirket tarafından belirlendiği,

- Elde edilen kişisel verilerden, kişinin kimlik ve iletişim bilgilerinin, pasaport bilgilerinin, login ve kullanıcı adı, ülke, şehir, posta kodu, ilçe, cinsiyet, dijital fotoğraf bilgilerinin yurt içi ve yurt dışı ile paylaşıldığı, yurt içi/yurt dışı aktarımların yalnızca topluluk şirketleri ile yapıldığı, şirketin her türlü işlem ve ilişkilerinde yurt dışı merkezli topluluk şirketlerine bağlı olması sebebiyle söz konusu paylaşımın hizmetlerin ifası bakımından şart olduğu, dil sınavının uygulaması ve hazırlanmasında ancak kendisine tanınan yetki sınırları içerisinde hareket edebildiği ve sözleşme kapsamında bağlı olduğu şirketlere aktarım yapmakla yükümlü olduğu, adayın talep ettiği hizmeti almasında bu aktarımın önem arz ettiği, edimin ifa edilmesi adına dil sınavı test ortaklarının bu bilgilere sahip olmak zorunda oldukları, verilerin aktarıldığı topluluk şirketlerinin GDPR’a tabi olduklarından güvenli ülke oldukları,

- Özel nitelikli kişisel verilerin ve parmak tarama kayıtlarının ise yurt dışına aktarımının söz konusu olmadığı,

- Sınav adaylarıyla yapılan görüşmeler esnasında adaya gönderilen ve imzalatırılan gizlilik ile kullanım koşulları metinlerinde yurt dışına aktarıma ilişkin bilgilendirme yapıldığı, verilerin aktarımı öncesinde mutlaka adaylardan rızalarının alındığı,

- Sınava girecek adayın sınav yeri ve sonuç bilgilerini öğrenme hakkı kapsamında e-posta adres bilgilerinin alındığı, bu kapsamda ilgili bilgilerin gönderildiği, ticari iletilerle ilgili olarak ise “Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik”in 6 ncı maddesi hükmü uyarınca temin edilen hizmetler kapsamında gönderilecek ticari iletiler bakımından tekrar onay alınması gerekmediği,

- Kişisel verilerin saklanma ve imhasına ilişkin olarak politikalarının bulunduğu, buna göre toplanan kişisel bilgilerin artık gerekli olmadığına, kişisel bilgilerin bir kopyasının saklanmayacağı veya bilgilerin yasalar tarafından gerekmedikçe imha edilmesi ve kimlik giderme politikasına uygun olarak yok edilmesinin, güvenli şekilde silinmesinin veya bilgilerin tanımlanmasının sağlanacağı, bilgilerin dil sınavı veya sınav hazırlama amaçları için toplanması halinde, sınava girdikten, hizmete

katıldıktan sonra veya son etkinlikten sonra 3 yıla kadar saklanacağı, parmak tarama verilerinin test tarihinden sonra 60 gün boyunca sadece bir binary large object dosyası olarak saklanacağı ifade edilmiştir.

Bu kapsamda, kişisel verilerin işleme amaçlarının ve vasıtalarının belirlenmesinden ve veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olduğu iddia edilen yurt dışında yerleşik bulunan şirkete de şikâyet dilekçesindeki iddialara yönelik olarak bilgi verilerek açıklamaları istenilmiş olup, bu kapsamda yurt dışında yerleşik bulunan şirketçe verilen cevabi yazıda özetle;

- Dil sınavının arka planına ve bağlamına ilişkin açıklamalara yer verildikten sonra, şikâyete konu (Türkiye’de bulunan) akredite kuruluşun yurt dışında yerleşik bulunan şirketlerinin iştiraki konumunda olduğu ve sınav ortakları tarafından ortaklaşa belirlenen ve Test Merkezleri Sözleşmesinde belirtilen şartlar altında çalışmakla yükümlü olduğu,
- Bahsi geçen ortakların sınava ilişkin şartları ve koşulları, gizlilik bildirimini ve kimlik doğrulama süreçleri dahil olmak üzere gereksinimleri ortaklaşa belirledikleri,
- Katılan için önemli sonuçları olan bir sınav olması sebebiyle, sınava giren kişinin kimliğinin kesin olarak doğrulanabilmesinin ve sonucunun sınava giren kişiyle ilişkilendirmesinin hem sınav katılımcılarının hem de kuruluşların yararına olduğu, buna göre, kimlik doğrulaması ve sınav günü fotoğrafının, sınava girenlerin sonuç formunda gösterilen sonuçlara ulaşan kişi olduklarını kanıtlamalarını sağladığı,
- Parmakla taramaya ilişkin olarak; test merkezlerine, sınava girenlerin kimliklerini kontrol etmeye dayalı bir alternatif sağlanması gerektiğini belirtir talimatlarının bulunduğu, Türkiye’de alternatifin sunulmadığı bir dönemin bulunduğu ancak Mart 2020’den itibaren Türkiye’deki şirketin uygulamasının parmak taraması yaptırmak istemeyen sınav katılımcılarına bir alternatif sunulması gerektiği yönünde olduğu, ancak bunun her zaman böyle olmadığı bu sebeple bunu düzeltmek için adımlar attıkları,
- Parmak taramasını içeren mevcut sürecin, aynı kişinin sınavın tüm bölümlerini aldığını teyit etmek ile sınav katılımcısının gizlilik hakları arasında en iyi dengeyi sağladığından seçildiği,
- Parmak izlerinin resimlerinin alınmadığı veya saklanmadığı, yalnızca baskının aynı kişiden olduğunu doğrulamak için kullanılabilen, ancak parmak izi görüntüleri olarak çoğaltılmayan İkili Büyük Nesne Dosyaları (BLOB) olarak adlandırılan sayısal dizeler şeklinde tutulduğu, bu dosyaların da yalnızca sınav merkezinin bilgisayar ekipmanında yerel olarak tutulduğu ve 60 gün sonrasında silindiği, yurt dışına aktarılmadığı, Türkiye’de, Mart 2020’den itibaren parmak taramasına alternatif

bir kimlik doğrulama sistemi sunulduğu ve Covid riski nedeniyle de o zamandan beri parmak taramasının hiç kullanılmadığı,

- Bir yan kuruluşu olarak Türkiye'deki iştiraklerinin rolünün, dil sınavının Türkiye'de test merkezlerinde sunulmasının sağlanması şeklinde olduğu,
- Tüm ülkelerdeki sınav katılımcılarından parmak taramalarının talep edildiği ancak bunun zorunlu olmadığı, alternatif olarak kayıt kimliğinin manuel olarak kontrol edilmesinin de mevcut olduğu,
- Bazı kişisel verilerin Gizlilik Bildiriminde açıklandığı üzere veri sorumlusuna aktarıldığı, ancak bu bilgilerin her kişi için toplanmadığı, sınava girme nedenine ve seçilen sınavın türüne bağlı olarak değiştiği, parmak taramasının ise yurt dışına aktarılmadığı,
- Yurt dışına aktarmak için ilgili kişilerin açık rızasının alındığı, Kurulun, taraflarının Kanuna ilişkin yorumlarına katılmaması halinde, özellikle "Yeterli Ülkelerin" herhangi bir onayı yoksa transfer için Kurul onayı alma sürecine katılabilecekleri

beyan edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 12/08/2021 tarih ve 2021/799 sayılı Kararı ile;

Veri sorumlusu sıfatının belirlenmesi açısından;

- 6698 sayılı Kişisel Verilerin Korunması Kanununun Tanımlar başlıklı 3 üncü maddesinde "veri sorumlusu"nun, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi; "veri işleyen"in ise veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi olarak tanımlandığı; veri sorumlusunun, veri işleme faaliyetinin genel anlamda "neden" ve "nasıl" yapıldığını belirleyen kişi olduğu, Kurumun internet sitesinde yayınlanan veri sorumlusu-veri işleyen rehberine göre veri işleyen ise, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen, veri sorumlusunun organizasyonu dışındaki gerçek veya tüzel kişiler olduğu; bu kişilerin, kişisel verileri kendisine verilen talimatlar çerçevesinde işleyen, veri sorumlusunun kişisel veri işleme sözleşmesi yapmak suretiyle yetkilendirdiği ayrı bir gerçek veya tüzel kişi olduğu; bu kapsamda, Türkiye'deki dil sınavlarında iştiraki olarak görev yapmakta olan şirketin ve yurt dışı merkezli şirketten alınan bilgi, belge ve beyanların değerlendirilmesi neticesinde, Türkiye'deki şirketin dil sınavının Türkiye'de uygulanmasında yetkili kılınan bir tedarikçi olduğu, sınavın uygulanmasına dair hizmet sözleşmesi kapsamında yurt dışı merkezli şirketin emir ve talimatlarıyla bağlı olduğu öte yandan adaylardan elektronik ortamda alınan kayıtların tutulduğu elektronik

sistemin yurt dışındaki şirkete ait olduğu ve Türkiye'deki şirketin söz konusu sisteme erişim imkanı olmadığı, bu minvalde bahse konu sınav hizmetinin sağlanması noktasında adaylardan/ilgili kişiden edinilen sınava ilişkin genel nitelikteki kişisel verilerin işlenmesi noktasında veri işleyen sıfatını haiz olduğu,

- Diğer taraftan, sınav güvenliğinin sağlanması noktasında adaylardan sınava giriş esnasında kimliklerinin doğrulanmasını teminen alınan parmak taraması uygulamasının Mart 2020'ye kadar Türkiye'de zorunlu olarak yapıldığı ancak bu tarihten itibaren parmak taramasına alternatif bir kimlik doğrulama sistemi sunulmasına yönelik test merkezlerine talimat verildiğinin beyan edilmesi ve şikâyete konu ilgili kişinin parmak tarama kayıtlarının 2018 yılında alındığı hususları birlikte değerlendirildiğinde, somut olay açısından Türkiye'deki şirketin, yurt dışı merkezli şirketin emir ve talimatlarıyla hareket etmek zorunda olduğu, bununla birlikte her ne kadar Mart 2020 tarihinden itibaren ve günümüz itibariyle adaylara, verilerinin işlenmesi noktasında seçenek sunulması talimatının verildiği ifade edilse de şikâyet tarihi itibariyle parmak taraması alınması yönündeki kişisel veri işleme faaliyetinin zorunlu olarak yapıldığı anlaşıldığından, somut olay açısından Türkiye'deki iştirakin yine veri işleyen, yurt dışı merkezli şirketin ise veri sorumlusu olduğu,

İlgili kişinin başvurusunun reddedilmesi açısından;

- İlgili kişinin Türkiye'deki şirkete yaptığı başvuruda ad-soyad bilgisini bir harf eksik olarak yanlış yazdığı ancak ilgili kişinin ad-soyad bilgisi kişi tarafından bir harf eksik olarak yazılmış olsa da kişinin kimliğinin teyit edilmesini sağlayacak T.C. kimlik numarasının tam olarak iletildiği diğer taraftan şirket ile yapılan yazışmalarda ilgili kişinin ad ve soyadının verilen cevap e-postalarında tam olarak görüntülenebildiği dolayısıyla söz konusu e-posta adresinin şirketin sisteminde kayıtlı olduğu anlaşılmış olduğundan bir harf sebebiyle ilgili kişinin başvurusunu reddetmesinin Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğin 6 ncı maddesinde belirtilen dürüstlük kuralına uygun olmadığı,

- Diğer taraftan, ilgili kişinin Kanununun 11 inci maddesi kapsamında bilgi edinmeye yönelik taleplerine, talebi olmayan bir içerikle Tebliğin 6 ncı maddesine uygun olmayacak bir şekilde cevap verildiği bu anlamda ilgili kişinin taleplerinin yanıtsız bırakıldığı, bununla birlikte ilgili kişinin başvurusunda yer alan taleplerini veri sorumlusu adına cevaplayabileceği dikkate alındığında veri işleyen Kanun kapsamında kendisine yapılan başvurulara cevap verirken 6698 sayılı Kanun ve Tebliğin ilgili hükümlerine uyum konusunda gerekli dikkat ve özeni göstermediği,

İlgili kişinin görsel kaydının ve parmak izinin herhangi bir veri işleme şartına dayanmaksızın alındığı iddiası açısından;

- Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinde kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, bu çerçevede, kişisel verilerin ancak,
 - a) Hukuka ve dürüstlük kurallarına uygun şekilde,
 - b) Belirli, açık ve meşru amaçlar kapsamında,
 - c) Doğru ve gerektiğinde güncel olma şartıyla,
 - ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,
 - d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmeilkelerine uygun olarak işlenebildiği, bu ilkelerden, “işlendikleri amaçla bağlantılı ve sınırlı olma ilkesi”nin; işlenen verilerin belirlenen amaçların gerçekleştirilebilmesine elverişli olmasını, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını öte yandan sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik olarak da veri işlenmesi yoluna gidilmemesini içerdiği,
- Ölçülü olma ilkesinin ise, veri işleme faaliyeti ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulmasını, diğer bir deyişle veri işlemenin amacı gerçekleştirecek ölçüde olmasını ifade ettiği, bu kapsamda, veri sorumlusunun amacı çerçevesinde ölçülü olma ilkesine uygun olarak ilgili kişiden minimum düzeyde bilgi talep etmesi bunun dışında, amaç için gerekli olmayan kişisel verilerin işlenmesi faaliyetinden kaçınması gerektiği,
- Kanunun “Özel Nitelikli Kişisel Verilerin İşlenme Şartları” başlıklı 6 ncı maddesinde “...(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır. (3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir. (4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.” hükümlerine yer verildiği,
- Somut olayda, sınavın güvenilirliğinin ve güvenliğinin sağlanması noktasında 2020 Mart dönemi öncesinde, adaylardan parmak taramalarının alınmasında ilgili kişiden/adaylardan alternatif yollar

yerine açık rızalarının alınması yoluna gidildiği dolayısıyla Kanunun 4 üncü maddesinde yer alan “ölçülü olma” ilkesine aykırı davranıldığı,

- Türkiye’de adaylara alternatifin sunulmadığı bir dönemin bulunduğu anlaşıldığından şikâyete konu somut olay açısından 2018 yılındaki parmak tarama kayıtlarının işlenmesi noktasında hizmetin açık rıza şartına bağlandığı, bu kapsamda açık rızanın Kanunda sayılan unsurları taşımadığı ve dolayısıyla söz konusu işlemenin Kanunda yer alan işleme şartlarına dayanmadan gerçekleştirildiği, İlgili kişinin kişisel verilerinin yurt içi ve yurt dışına aktarılmasına ilişkin bilgilendirilmediği iddiası hakkında:

- Kanunun “Kişisel Verilerin Yurt Dışına Aktarılması” başlıklı 9 uncu maddesinde kişisel verilerin ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamayacağı ancak, kişisel verilerin 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede; a) Yeterli korumanın bulunması, b) Yeterli korumanın bulunmaması durumunda Türkiye’deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılacağı hükümlerinin düzenlendiği,

- Taraflardan alınan savunma yazılarında ve internet sitelerinde yapılan incelemede kişisel verilerin yurt dışına aktarımına açık rıza verilmesi gerektiği, açık rıza verilmemesi halinde sınav hizmetinin ifa edilemeyeceği, hizmetin ifası için söz konusu kişisel verilerin test ortaklarına aktarılmasının zorunlu olduğunun beyan edildiği ancak genel nitelikli kişisel verilerin işlenmesinin Kanunun 5 inci maddesinin (2) numaralı fıkrasının (c) bendi kapsamında bir sözleşmenin kurulması ve ifasıyla doğrudan doğruya ilgili olması sebebiyle alınması zorunlu bilgiler olduğu ve adayların açık rızasına tabi olmadığı bununla birlikte aktarımın adayların açık rızaları kapsamında yapıldığının anlaşıldığı,

- Ayrıca, gerek internet sitesinde gerekse sunulan bilgi ve belgelerde açık rızanın sadece yurt dışına aktarıma yönelik olarak alınmadığı, yurt dışına aktarıma ilişkin rızanın sınava ilişkin diğer koşulların da yer aldığı “şartlar ve koşullar” metnine istinaden hizmetten faydalanmanın şartı olarak alındığı, somut olaya konu olan ilgili kişinin onayının da aynı şekilde alındığı ancak aradan geçen 3 yıllık süre ve Türkiye’deki şirketin adaylara ilişkin elektronik kayıtların tutulduğu söz konusu sisteme erişim imkanının bulunmaması sebebiyle ilgili belgeye erişemediği ve yurt dışı ile yürütülen görüşmeler neticesinde ilgili kişiye ait bahse konu kayıtların imha politikasına uygun şekilde yok edildiği bilgisini aldığı,

- Bu itibarla, hizmetin ifası kapsamında zorunlu olarak alınması gereken genel nitelikteki kişisel verilerin yurt dışına aktarılmasında açık rızanın sınava ilişkin şartlar ve koşulların yer aldığı metinler aracılığıyla genel olarak alınmasının açık rızayı sakatlayacağı dikkate alındığında; yurt dışına aktarımın Kanunun 9 uncu maddesinin (1) numaralı fıkrası gereğince açık rıza kapsamında yapılmaya devam edilmesinin tercih edilmesi halinde açık rızanın Kanunun 3 üncü maddesinde yer alan unsurlar ve Aydınlatma Tebliğinde yer verilen hükümler dikkate alınmak şartıyla yurt dışına aktarım özelinde münferiden alınması gerektiği ya da açık rıza almak yerine Kanunun 9 uncu maddesinin (2) numaralı fıkrası uyarınca "bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması" kapsamında yurt dışına aktarılmak istenmesinin tercih edilmesi halinde ise Kanunun 9 uncu maddesinin (1) numaralı fıkrasına uygun bir taahhütnamenin hazırlanarak Kurulun onayına sunulması gerektiği,

Reklam ve pazarlama içerikli e-postalara rıza vermediği ve bu konuda aydınlatılmadığı iddiası açısından;

- Konu hakkında ilgili kişinin veri sorumlusuna başvuruda bulunmamış olmasının Kanunda yer verilen usul şartlarına uygun olmadığı sonucuna varıldığı

değerlendirmelerinden hareketle;

- İlgili kişinin Türkiye'deki şirketin sisteminde kayıtlı olduğu ve ilgili kişinin kimliğinin tespit edilebileceği anlaşılmış olduğundan bir harf sebebiyle "...başvurucu ismi kayıtlarımızda bulunamamıştır..." şeklinde ilgili kişiye cevap verilmesinin Tebliğin 6 ncı maddesinde belirtilen dürüstlük kuralına uygun olarak değerlendirilmemesi sebebiyle Kanun kapsamında kendisine yapılan başvurulara cevap verirken 6698 sayılı Kanun ve Tebliğin ilgili hükümlerine uyum konusunda gerekli dikkat ve özeni göstermesi gerektiği konusunda uyarılmasının,

- Diğer taraftan ilgili kişinin taleplerinin Türkiye'deki şirket tarafından yanıtız bırakıldığı göz önüne alındığında ise ilgili kişinin başvurusunda yer alan taleplerini veri işleyen veri sorumlusu adına cevaplayabileceği dikkate alındığında, veri işleyen bu talepleri detaylı şekilde yanıtlaması ve sonucundan Kurula bilgi vermesi gerektiği yönünde talimatlandırılmasına,

- Sınava girişlerde parmak taraması kayıtlarının alınması uygulamasına ilişkin veri sorumlusu tarafından test merkezlerine, sınava girenlerin kimliklerini kontrol etmeye dayalı bir alternatif sağlanması gerektiğini belirtir talimat verildiğinin belirtildiği, Türkiye'de adaylara alternatifin sunulmadığı bir dönemin bulunduğu zira bu uygulamanın Türkiye'de Mart 2020'den itibaren değiştirildiği ve parmak taramasına alternatif bir kimlik doğrulama sisteminin sunulduğunun beyan

edildiđi, Őikâyete konu somut olay aısından ise 2018 yılındaki parmak tarama kayıtlarının iŐlenmesi noktasında hizmetin aık rıza Őartına bađlandığı, bu kapsamda aık rızanın Kanunda sayılan unsurları taŐımadığı ve dolayısıyla söz konusu iŐlemenin Kanunda yer alan iŐleme Őartlarına dayanmadan gerekleŐtirildiđi dikkate alındığında Kanunun 12 nci maddesinin (1) numaralı fıkrasında sayılan tedbirlerin alınmadığı kanaatine varıldığından, yurt dıŐı merkezli veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında idari para cezası uygulanmasına,

- Türkiye’de sınava giriŐte kimlik dođrulaması amacıyla adaylardan parmak taraması kaydı alınması uygulamasına alternatif bir kimlik dođrulama sisteminin kullanılması, bu kapsamda veri iŐleyen baŐta olmak üzere Türkiye’deki yetkili test merkezlerinin bu sisteme uymasının sađlanması ve sonucundan Kurula bilgi verilmesi gerektiđi yönünde veri sorumlusunun talimatlandırılmasına,

- İlgili kiŐinin Őikayet dilekesinde Kurula iletildiđi “reklam, pazarlama ve tanıtım amalı maillerin geldiđi, bu iŐleme faaliyetine rıza vermediđi ve söz konusu iŐleme faaliyeti konusunda aydınlatılmadıđı” iddialarına iliŐkin veri sorumlusuna baŐvuruda bulunmamıŐ olmasının Kanunda yer verilen usul Őartlarına uygun olmadığının deđerlendirilmesi sebebiyle, veri sorumlusunu muhatap baŐvurusunda talep etmediđi, ancak Kurula yaptıđı baŐvuruda talep ettiđi konuların inceleme sürecine dahil edilmediđi hususlarında ilgili kiŐiye bilgi verilmesine

karar verilmiŐtir.

2021/761 sayılı KVKK Kararı

Kişisel sağlık verilerinin hastanedeki yetkisiz çalışanlar tarafından velayete sahip olmayan ebeveyn ile paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 06/08/2021 tarihli ve 2021/761 sayılı Karar Özeti

Karar Tarihi : 06.08.2021

Karar No : 2021/761

Konu Özeti : Kişisel sağlık verilerinin hastanedeki yetkisiz çalışanlar tarafından velayete sahip olmayan ebeveyn ile paylaşılması

Kuruma intikal eden şikâyet dilekçesinde özetle;

- Şikayetçinin aralarında boşanma davası devam eden eşinin, müşterek çocuklarını taciz ettiği iddiasıyla yargılanmakta olduğu, dosyanın istinaf aşamasında bulunduğu, ilgili kişinin eşinin istinaf dilekçesi ve eklerinde müşterek çocuklarına ait sağlık ve epikriz raporlarına yer verildiği,
- Şikayetçinin karşı tarafın İstinaf Mahkemesine vermiş olduğu epikriz raporlarında oğlu hakkında “yalan söyler, hırsızlık yapar” gibi cümlelerin olduğunu gördüğü, oğlunu çocuk psikiyatrisi bölümüne sadece dikkat dağınıklığı için muhtelif zamanlarda toplamda 3-4 kez muayeneye götürdüğü, ancak hiçbir zaman oğlunu yalan söylemesinden bahisle hastaneye götürmediği, yine İstinaf Mahkemesine sunulan raporların özel hayatın gizliliği hiçe sayılarak ve usulsüz olarak konuyla alakasız kişiler tarafından kendisinin haberi olmadan alındığı, alınan raporda değişiklik yapılarak Mahkemeyi yanıltılmak amacıyla karşı tarafa verildiği,
- Bunun üzerine, söz konusu sağlık raporlarının şikayetçi annenin izni olmadan bir Eğitim ve Araştırma Hastanesi (“Hastane”) tarafından hapiste bulunan eşinin vekiline verildiğinin anlaşıldığı, vekilin vekaletnamesinde ise bu konuda özel bir iznin bulunmadığı,
- Başlatılan araştırmalar kapsamında edindiği bilgilerden; Hastanede Arşiv Memuru olarak çalışan kişinin söz konusu raporları kendisinden sadece Hastane şefinin talep ettiği, diğer kişilerle bu konuda bir görüşmesinin olmadığı, bu talep üzerine çıktılar aldığı bunun yolu olarak sistemde kaydet butonuna basarak epikriz formu oluşturduğu, bu işlem sırasında bulgular ya da tanıda herhangi bir değişiklik yapmadığı ve çıktığı aldığını beyan ettiği, Hastanede Şef olarak çalışan kişinin söz konusu

raporlara ilişkin talep üzerine ilk etapta belgeleri vermeyip amirine danıştığı, geçmişte konu ile ilgili mevcut olan bir görüş yazısı ve İl Sağlık Müdürlüğü'nün avukatı ile yaptığı görüşme üzerine raporları alma talebi ile başvuran kişilerin ikinci gelişlerinde bu raporları veremeyeceğini beyan ettiği, Çocuk Hastalıkları Uzmanı doktorunun ise söz konusu belgeleri şikayetçinin eşinin vekiline kendisi tarafından verildiğini kabul ettiği, başvuru esnasında avukatın kimliği, vekâletnamesi, nüfus kayıt örneği, babaya ait dilekçeleri inceleyerek uygun olduğunu gördüğü, belgelerin imzalanıp kaşelenmeden resmi hüviyet kazanamayacağı, idareden resmi onaylı nüshanın talep edilmesi gerektiği hususlarının avukata açıkça beyan edildiği,

- Ancak şikayetçinin çocuğunu söz konusu doktora hiç muayeneye götürmediği,
- Konu hakkında ilgili Cumhuriyet Başsavcılığına suç duyurusunda bulunulduğu, ancak doktorun açık ikrarına rağmen Valilikçe soruşturma izninin verilmediği

hususları ifade edilerek ilgili kişinin kişisel verilerini 6698 sayılı Kişisel Verilerin Korunması Kanununa (Kanun) aykırı olarak işleyen ve velisinin rızası dışında kullanan veri sorumlusu hakkında gerekli idari yaptırımların uygulanması talep edilmiştir.

Şikayet dilekçesinin ekinde yer alan ilgili Valilik İl İdare Kurulu Müdürlüğüne alınan Kararda özetle;

- İlgili kişinin çocuğuna ait olan 11 adet epikriz raporunun sisteme doktorlar tarafından eklenmesi gerekirken arşiv memuru tarafından eklendiği,
- Raporların log kayıtlarının incelendiği ve raporlarda değişiklik yapılmadığının görüldüğü,
- Hastane Bilgi İşlem Müdürlüğü tarafından söz konusu hastanedeki tüm poliklinik hasta kayıt personeli ve doktorların tüm hastaların dosyalarını görme yetkisine sahip olduğu, hastane otomasyon sisteminde ekleme, silme ve değiştirme işlemlerinde log kaydı tutulduğu, hastaların bilgilerinin görüntülenmesi noktasında ise log kaydı tutulmadığına ilişkin bilgi verildiği,
- Raporları vekile teslim eden doktorun, başvuran kişinin avukat olması ve müvekkilinin çocuğuna dair sağlık bilgilerini talep etmesi nedeniyle raporları teslim ettiğini belirttiği,
- Doktorun söz konusu belgeleri verdiği ikrarı ile bu davranışının gerekçelerinin birlikte değerlendirilmesi neticesinde; çocuk hastalıkları uzmanı olarak görev yapan hekimin yoğun poliklinik şartları, gece nöbetleri ve diğer görevleri esnasında, kendisine yapılan tüm taleplerle ilgili yasaları bilmesinin ve/veya hatırlamasının mümkün olmadığı, muhatap olduğu hastaların kendisini ifade edemeyecek, kendisi ile ilgili karar alamayacak durumda olan 18 yaşın altındaki bireylerden oluşması ve hastaları ile ilgili tüm bilgileri ve açıklamaları hastası konumundaki çocukların ailelerine

izah etme/belge verme zorunluluğunun olması, talep eden avukatın istediği belgeleri mahkeme yoluyla da elde edilebileceği, imzasız ve kaşesiz olarak bilgilendirme amacıyla verildiği, doktorun bilerek ve isteyerek bir kişinin mağduriyetine sebep olma isteği taşıyamayacağı anlaşıldığı

belirtilerek, Valilik tarafından soruşturma izni verilmemesine karar verildiği bilgileri yer almaktadır.

Bu çerçevede konuya ilişkin başlatılan inceleme çerçevesinde söz konusu şikayet dilekçesinde yer alan iddialar kapsamında Sağlık Bakanlığının açıklamalarına başvurulmuş olup, konuya ilişkin ilgili Valilik İl Sağlık Müdürlüğü tarafından verilen cevapta özetle;

- Şikayete konu doktor ve arşiv memurunun kamu personeli ve sağlık çalışanı olmaları nedeniyle sır saklama yükümlülüğü altında buldukları,
- Sağlık çalışanlarının hastalara ait kişisel verilere erişmelerinin sağlık hizmetinin sunulması için bir zorunluluk olduğu, erişim yetkisinin sağlık hizmetinin sunumu açısından zorunlu olması sebebiyle, şikayete konu olan kişilerin de dahil olduğu meslek grubu olan sağlık çalışanlarının ve kamu personelinin sır saklama yükümlülüklerinin pek çok temel mevzuatta düzenlendiği ve bu erişim yetkisinin hasta mahremiyetini zedeleyecek şekilde kötüye kullanılmasının yaptırımlara bağlandığı,
- Şikayete konu edilen olayın Bakanlığa bağlı bir hastanede gerçekleştiği, Bakanlığın veri işleme faaliyetinin sebebinin 6698 sayılı Kanununun 6 ncı maddesinde tanımlanan "tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi" dahilinde olduğu ve dolayısıyla da sağlık çalışanlarının hasta dosyalarına sağlık hizmetinin sunulması kapsamında erişimlerinin bulunmasının Kanun kapsamında hukuki dayanağının bulunduğu,
- 21.06.2019 tarihli Resmi Gazetede yayımlanan Kişisel Sağlık Verileri Hakkında Yönetmeliğin 6 ncı maddesinde, sağlık personelinin verilere erişimine ilişkin şartların belirlenmiş olduğu ve buna göre, sağlık hizmet sunumunda görevli kişilerin; ilgili kişinin sağlık verilerine ancak, verilecek olan sağlık hizmetinin gereği ile sınırlı olmak kaydıyla erişebileceğinin düzenlendiği,
- Şikâyete konu olaydan tamamen bağımsız olarak düşünüldüğünde, sağlık çalışanlarına, çalıştıkları pozisyon ve sahip oldukları unvan gereğince ve verilecek sağlık hizmetinin gereği ile sınırlı olmak kaydıyla hasta verilerine erişim yetkisi verilmesinin hukuka uygun olduğu,
- Hekimlerin hastaların sağlık verilerine geçmiş hastalık öykülerini, tedavilerini öğrenmek ve mevcut rahatsızlıkları için tedaviyi belirlemek adına erişim sağladıkları,
- Aynı şekilde arşiv memurlarının da, yaptıkları işle ilgili olarak hastaların dosyalarına erişim ihtiyacı olan sağlık çalışanları oldukları, bu kişilerin hasta dosyalarına erişiminin kısıtlanmasının,

sağlık hizmetinin sunumunu aksatacak, insan sağlığı açısından telafisi imkansız sonuçlara yol açabileceği,

- Dolayısıyla, bahsi geçen olaydaki meslek gruplarının, yani bir uzman doktorun ve arşiv memurunun hasta kayıtlarına meslekleri icabı erişme zorunluluğu bulunduğu, bu kişilerin, sağlık hizmetinin sunumu esnasında amaçla sınırlı olmak kaydıyla hasta kayıtlarına erişmelerinde kişisel verilerin korunmasına ilişkin mevzuata aykırı bir husus bulunmadığının değerlendirildiği,
- Nihai değerlendirmelerinde Sağlık Bakanlığının kişisel veri işleme faaliyetlerinin dayanağını yürürlükteki mevzuattan aldığı, sağlık hizmetinin sunumu ile bağlantılı konularda, bu amacı aşmamak kaydıyla sağlık çalışanlarının hasta kayıtlarına erişmesinin mümkün olduğu, hasta kayıtları üzerinde yapılan her türlü değişikliğin log kaydının tutulduğu,
- Hekimlerin sadece kendileri üzerinden kayıtları açılmış hastaların dosyalarına erişmesinin veya arşiv memurlarının erişebilecekleri hasta dosyalarının kısıtlanmasının, sağlık hizmetinin doğası ile bağdaşmadığı, bir hekimin, kendi hastası olmayan bir hastaya doğrudan veya dolaylı olarak sağlık hizmeti sunabildiği, bir başka hekime konsültasyon verebildiği, bu sebeple de hastanedeki hekimlerin ve hasta dosyalarının muhafazasından sorumlu arşiv memurlarının hasta dosyalarına erişmesinde hukuka aykırılık görülmediği,
- Başvuruya konu olan olayda hukuka aykırılık, eğer gerçekten vuku buldu ise (yargısal süreç halen devam etmekte olduğu belirtilmekte), insan faktöründen kaynaklandığı, sağlık sektörünün doğası gereği, insan faktörünün tamamen gözden çıkarılmadığı, bununla birlikte Sağlık Bakanlığının caydırıcılığını arttırmak ve hasta mahremiyetini sağlamlaştırmak için idari, hukuki, cezai müeyyidelerin takipçisi ve uygulayıcısı olduğu, sayısız resmi yazı ile sayısız kurum ve kuruluşa hasta mahremiyeti ve kişisel verilerin korunmasına ilişkin talimatlandırma yaptığı, tüm bunlar birlikte değerlendirildiğinde olayda Bakanlığa atfedilebilecek bir güvenlik açığı tespit edilmediğinin düşünüldüğü

hususları bildirilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 06/08/2021 tarih ve 2021/761 sayılı Kararı ile;

- Kanunun “Özel Nitelikli Kişisel Verilerin İşlenme Şartları” başlıklı 6 ncı maddesinin

(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır. şeklinde düzenlendiği,

• Kanunun 6 ncı maddesinin (4) numaralı fıkrası ile 22 nci maddesinin (1) numaralı fıkrasının (ç) bendi kapsamında Kişisel Verileri Koruma Kurulu tarafından hazırlanan “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler”de

1. Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi,

2. Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik olarak,

a) Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi,

b) Gizlilik sözleşmelerinin yapılması,

c) Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,

ç) Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,

d) Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması,

3. Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise

a) Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,

b) Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,

c) Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,

- ç) Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- d) Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- e) Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması gerekmektedir.

hususlarına yer verildiği,

- İlgili sağlık mevzuatı incelendiğinde; 01.08.1998 tarihli Resmi Gazete’de yayınlanan Hasta Hakları Yönetmeliğinin “Kayıtların İncelenmesi” başlıklı 16 ncı maddesinde “Hasta, sağlık durumu ile ilgili bilgiler bulunan dosyayı ve kayıtları doğrudan veya yetkili veya kanuni temsilcisi vasıtası ile inceleyebilir ve bir suretini alabilir. Bu kayıtlar, sadece hastanın tedavisi ile doğrudan ilgili olanlar tarafından görülebilir.” hükmü yer alırken yine aynı Yönetmeliğin 23 üncü maddesinde; “Sağlık hizmetinin verilmesi sebebiyle edinilen bilgiler, kanun ile müsaade edilen haller dışında, hiçbir şekilde açıklanamaz. Kişinin rızasına dayansa bile, kişilik haklarından bütünüyle vazgeçilmesi, bu hakların başkalarına devri veya aşırı şekilde sınırlanması neticesini doğuran hallerde bilginin açıklanması, bunları açıklayanın hukuki sorumluluğunu ortadan kaldırmaz. Hukuki ve ahlaki yönden geçerli ve haklı bir sebebe dayanmaksızın hastaya zarar verme ihtimali bulunan bilginin ifşa edilmesi, personelin ve diğer kimselerin hukuki sorumluluğunu kaldırmaz. Hukuki ve ahlaki yönden geçerli ve haklı bir sebebe dayanmaksızın hastaya zarar verme ihtimali bulunan bilginin ifşa edilmesi, personelin ve diğer kimselerin hukuki ve cezai sorumluluğunu da gerektirir.” hükmüne yer verildiği,
- Ayrıca, 21.06.2019 tarihli Resmi Gazete’de yayımlanan Kişisel Sağlık Verileri Hakkında Yönetmeliğin çocukların sağlık verilerine erişim başlıklı 8 inci maddesinin ikinci fıkrasında “Anne ve babanın boşanması halinde velayet hakkı üzerinde bırakılmayan taraf, çocuk ile velinin faydası gözetilmek suretiyle kişisel verilerin korunması mevzuatına uygun şekilde ve Genel Müdürlükçe belirlenen sınırlar çerçevesinde çocuğa ilişkin sağlık verilerine erişebilir.” hükmü yer alırken, aynı Yönetmeliğin Sağlık verilerine avukatların erişimi başlıklı 10 uncu maddesinde “Avukatlar, müvekkilinin sağlık verilerini genel vekaletname ile talep edemezler. Müvekkiline ait sağlık verilerinin avukata aktarılması için düzenlenmiş olan vekaletnamede, ilgili kişinin özel nitelikli kişisel verilerinin işlenmesi ve aktarılmasına ilişkin açık rızasını gösteren özel bir hüküm bulunması gerekir.” hükmüne yer verildiği,

- Yine aynı Yönetmeliğin “Sağlık verilerine hasta yakınlarının erişimi” başlıklı 9 uncu maddesinin ilk fıkrasında kişisel sağlık verilerinin hasta yakınları ile paylaşımında 6698 sayılı Kanunun ilkelerine aykırılık teşkil etmeyecek şekilde, 01/08/1998 tarihli Resmi Gazete’de yayımlanan Hasta Hakları Yönetmeliğinin 18 inci maddesinin üçüncü fıkrasına uygun hareket edileceğinin belirtildiği, Hasta Hakları Yönetmeliğinin söz konusu fıkrasında ise hastanın kendisinin bilgilendirilmesinin esas olduğu, hastanın kendisi yerine bir başkasının bilgilendirilmesini talep etmesi halinde, bu talebin kişinin imzası ile yazılı olarak kayıt altına alınmak kaydıyla sadece bilgilendirilmesi istenilen kişilere bilgi verileceğinin hüküm altına alındığı,
- Yine Sağlık Bilgi Sistemleri Genel Müdürlüğünün güncellemiş olduğu “Bilgi Güvenliği Politikaları Kılavuzu”nun 41. sayfasında; “3.7.4.1. Kişisel sağlık kayıtlarının (tüm tetkik sonuçları, hasta dosyaları, barkodlar, gözlem formları vb.) özel nitelikli kişisel veri kategorisinde olduğu ve 6698 sayılı Kanun ile özel koruma uygulanması gerektiği her zaman dikkate alınır.” ifadesinin, 64. sayfasında “Özel nitelikli kişisel verilere (kişisel sağlık verileri) erişim için KVKK’nın 2018/10 sayılı kararında belirtilen teknik ve idari tedbirlerin alınmış olması gerekir.” ifadesinin, 122. sayfasında ise “9.9.25. KVKK’nın 2018/10 sayılı kararı uyarınca özel nitelikli kişisel verilerin işlendiği yazılımlarda; veriler üzerinde gerçekleştirilen tüm hareketlerin iz kayıtlarının bir başka ortamda güvenli olarak saklanması gerekmektedir.” ifadesinin yer aldığı,
- Bununla birlikte, Kılavuzun çeşitli sayfalarında salt 2018/10 sayılı Karara atıfta bulunmanın yeterli olmadığı, söz konusu kararda da atıf yapılan Kişisel Veri Güvenliği Rehberinde, kişisel veri güvenliğinin sağlanması için veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açabileceği kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınmasının gerekmekte olduğu, risklerin tanımlanması ve önceliğin belirlenmesinden sonra risklerin azaltılması ya da ortadan kaldırılmasına yönelik teknik ve idari tedbirlerin planlanarak uygulamaya konulması gerektiğinin belirtildiği,
- Veri sorumlusu bünyesinde çalışanların kendilerine gelen özel nitelikli kişisel verilerin paylaşımı konulu bu tür talepler karşısında aksiyon alırken dikkatsizlik, dalgınlık veya tecrübesizlik gibi durumların önüne geçmek adına risklerin/tehditlerin henüz olaylar gerçekleşmeden önce değerlendirilerek takip edilmesi gereken sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politikanın belirlenmesi gerektiği,

- Somut olayda doktorun ilgili kişi çocuğa muayene ve tedavi hizmeti verdiği için epikriz formundan görüldüğü, ancak anılan doktorun ilgili kişiyi çocuk ve ergen psikiyatrisi olarak değil, çocuk hastalıkları kapsamında muayene ettiğinin görüldüğü,

- Bu kapsamda, veri sorumlusu nezdinde görevli çocuk doktorunun söz konusu bilgileri kendi branşı dışında görüntülemiş ve çıktısını almak suretiyle üçüncü bir kişiyle, gerek vekâletnamede avukat ile özel nitelikli kişisel verilerin paylaşılabilirliği yönünde özel bir hüküm bulunmaması gerekse de çocuğun geçici velayetinin o esnada annesinde bulunması bakımından Kanunun 8 nci maddesine aykırı bir şekilde paylaştığı, anılan doktorun söz konusu bilgi ve belgeleri paylaşımının hastanın muayene ve tedavisi amacıyla bağlantılı, sınırlı ve ölçülü olmadığı,

- Bir diğer konu olarak hastanedeki tüm poliklinik hasta kayıt personelleri ve doktorların tüm hastaların dosyalarını görme yetkisine sahip olmasının veri işleminin amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırı olduğu, kimin hangi veriyi görüntülediği noktasında log kaydı tutulmadığı için herhangi bir kontrolün de mümkün olmadığı bu bakımdan, hastanedeki tüm doktor ve hasta kayıt personellerinin tüm hasta kayıtlarına erişmesi yerine, hastaların muayene ve tedavisi ile ilgili olarak çalışan personelin ve doktorların söz konusu verilere erişmesinin uygun olabileceği, veri sorumlusunun kimlerin hasta verilerini görüntülenebileceğine dair yetki matrisini oluşturmak suretiyle olası hukuka aykırı veri işlemlerinin önüne geçebileceği, bu kapsamda veri sorumlusu Sağlık Bakanlığının cevabi yazısında bahsetmiş olduğu, uzman doktorların sadece kendi üzerlerine kayıtlı hastalara hizmet vermedikleri, planlı veya ani gelişen durumlarda başka hastalara da hizmet verdikleri, sağlık hizmetlerinin yoğun ekip çalışması gerektirmesi ve aciliyet arz eden durumların da dikkate alınabileceği,

- Ayrıca, hastanenin otomasyon sisteminden çıktı alma noktasında sadece belirli personele yetki verilmesinin güvenlik risklerini azaltacağı

değerlendirmelerinden hareketle

- Veri sorumlusu Sağlık Bakanlığı bünyesindeki çalışanların tereddütte kalmadan takip edebilecekleri sistemli, kuralları net, yönetilebilir ve sürdürülebilir ayrı bir politika hazırlaması gerektiği hususunda veri sorumlusunun talimatlandırılmasına,

- İdari bir tedbir olarak ilgili Eğitim ve Araştırma Hastanesi çalışanlarının kişisel verilerin korunması uyum çalışmaları kapsamında eğitim alması, bu eğitimde özel nitelikli kişisel verilerle muhatap olan hastane personelinin kişisel verilerin işlenmesinde yetki kapsamlarına açıkça yer verilmesi ve alınan eğitim belgelerinin Kuruma sunulması hususunda veri sorumlusunun talimatlandırılmasına,

- Kişisel verilerin güvenliğinin sağlanması açısından teknik bir tedbir olarak hastane otomasyon sisteminin erişim loglarının görüntüleme işlemi de dâhil olmak üzere tutulmasını sağlamak için sistemin güncellenmesi ve Kuruma bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına,
- Hastanedeki tüm doktor ve hasta kayıt personelinin tüm hasta kayıtlarına erişmesi yerine, yalnızca hastaların muayene ve tedavisi ile ilgili olarak çalışan personelin ve doktorların söz konusu verilere erişmesine dair yetki matrisinin net bir şekilde ortaya konulması hususunda veri sorumlusunun talimatlandırılmasına,
- Hastane otomasyon sisteminden hasta kayıt örneklerinin çıktı alınması konusunda belirli prosedürlerin ve yetkili personelin belirlenmesi hususunda veri sorumlusunun talimatlandırılmasına, bu çerçevede kişisel verilerin korunması hususunda verilen tüm talimatlara ilişkin yapılan işlemlerin sonucundan Kurula bilgi verilmesine,
- Veri sorumlusu bünyesinde çalışan kişinin, ilgili kişinin çocuğuna ait özel nitelikli kişisel verileri ilgili avukata 6698 sayılı Kanununun 8 inci maddesinde yer alan aktarım şartlarından herhangi birine dayanmadan aktardığı, bu çerçevede veri sorumlusu tarafından Kanununun 12 nci maddesi kapsamında gerekli idari ve teknik tedbirlerin alınmadığı kanaatine varıldığından, Kanununun 18 inci maddesinin (3) numaralı fıkrası uyarınca ilgili kamu kurum ve kuruluşundaki sorumlular hakkında disiplin hükümlerine göre işlem yapılmasına ve sonucundan Kurula bilgi verilmesine

karar verilmiştir.

2021/670 sayılı KVKK Kararı

İlgili kişinin veri sorumlusu bankaya yaptığı iş başvurusunun olumsuz sonuçlanması sonrası kişisel verilerinin işlenmeye devam etmesi hakkında Kişisel Verileri Koruma Kurulunun 06/07/2021 tarih ve 2021/670 sayılı Karar Özeti

Karar Tarihi : 06.07.2021

Karar No : 2021/670

Konu Özeti : İlgili kişinin veri sorumlusu bankaya yaptığı iş başvurusunun olumsuz sonuçlanması sonrası kişisel verilerinin işlenmeye devam etmesi

Kuruma intikal eden şikâyet dilekçesinde, ilgili kişinin veri sorumlusu tarafından kurulmuş olan internet sitesi üzerinden iş başvurusunda bulunduğu, bu sebeple söz konusu internet sitesi üzerinden kişisel verilerini içerir bilgileri veri sorumlusuyla paylaştığı, başvurunun akabinde mülakata alındığı ancak mülakat neticesinde başarılı olamadığı, bu sebeple de veri sorumlusuyla kişisel verilerini paylaşması anlamında bir neden kalmadığı, bu bağlamda söz konusu internet sitesine girerek oluşturduğu özgeçmişini sildiği, akabinde veri sorumlusunun sisteminde kalan tüm kişisel verilerinin silinmesi adına telefon ve e-posta yoluyla veri sorumlusuna başvuruda bulunduğu, ancak ilgili kişinin başvurusuna istinaden veri sorumlusu tarafından e-posta yoluyla yapılan bilgilendirmede ilgilinin kişisel verilerinin veri sorumlusuna yapacağı olası başvurular için saklanacağı bilgisinin tarafına iletildiği ifade edilerek, veri sorumlusuna ilişkin herhangi bir iş talebi, ilgisi ya da ilişkisi olmadığını iletmesine rağmen kişisel verilerinin veri sorumlusu tarafından silinmemesi nedeniyle Kuruma şikayette bulunarak 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde söz konusu iddialara ilişkin veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişinin söz konusu internet sitesi aracılığıyla iş başvurusunda bulunduğu, gerek sitede doldurduğu form aracılığıyla gerekse daha sonraki süreçlerde bankalarına yazılı olarak bildirdiği ve ilgili kişiyle gerçekleştirilen mülakatlar esnasında beyan ettiği kişisel verilerin, 6698 sayılı Kişisel

Verilerin Korunması Kanununun 10 uncu maddesine uygun şekilde kendisine gerekli aydınlatmalar yapılarak işlendiği,

- Söz konusu kişisel verilerin Kanunun 5 inci maddesinin (2) numaralı fıkrasının (c) bendinde yer alan "Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması" hukuki sebebi kapsamında ilgili kişinin iş başvurusunun incelenmesi ve iş sözleşmesinin kurulabilmesi için gerekli olan bilgilerin temini, işe yeterlilik değerlendirmesi ve sair testlerin yapılabilmesi; (e) bendinde yer alan "Bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması" hukuki sebebi kapsamında ilgili kişinin başvuru pozisyonuna uygunluğunun incelenmesi, iletilen bilgilerin doğruluğunun teyit edilebilmesi, gerekli mülakatların yapılabilmesi ve (f) bendine yer alan "İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" hukuki sebebi kapsamında ilgili kişinin şirket prensiplerine uygunluğunun değerlendirilebilmesi, diğer başvurularda iletilen bilgilerle eşleştirme yapılabilmesi amaç ve işleme şartlarına dayanarak işlendiği,

- Veri sorumlusu tarafından yapılan değerlendirmeler sonrasında ilgili kişinin iş başvurusunun kabul edilmemesinin akabinde; yukarıda sayılan amaçlarla işlenen kişisel verilerin, ilgili kişinin talebi üzerine Kanunun 7 nci maddesine uygun olarak işleme amacının ortadan kalkması sebebi ile silindiği ancak söz konusu kişisel verilerden yalnızca isim-soy isim ve kimlik numarası ile veri sorumlusunun başvuru değerlendirilmesine esas genel gerekçesinin muhafaza edildiği, bu verilerin muhafaza edilmesindeki amacın ise veri sorumlusuna iş başvurusunda bulunan kişilerin, reddedilen başvuru sonrasındaki dönemlerde yapacakları iş başvurularının değerlendirmesinde, önceki başvurusunun da dikkate alınabilmesi olduğu, zira bu şekilde sonraki başvurularda gerçeğe aykırı verilerle karşılaşmanın önüne geçilmesinin amaçlandığı ve bu saklama amacının ilgili kişinin Kanunun 11 inci maddesi uyarınca yaptığı başvurusunda ilgili kişiye iletildiği,

- İlgili kişinin ikinci başvurusunda, isim-soy isim ve kimlik bilgisi verilerinin de silinmesini talep ettiğinin anlaşıldığı, ilgili kişinin kişisel verisi üzerindeki tasarruf yetkisinin öncelikli olduğu düşüncesinden hareketle ilgili kişinin isim-soy isim ve kimlik bilgilerinin de silinmesi kararının alındığı ve ilgili kişiye kişisel verilerinin ilk periyodik imha işlemi silineceği bilgisinin iletildiği ifade edilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 06/07/2021 tarihli ve 2021/670 sayılı Kararı ile;

- Kanunun, kişisel verilerin işlenmesine ilişkin “Genel İlkeler”i düzenleyen 4 üncü maddesinin (1) numaralı fıkrasında, “Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.” hükmünün yer aldığı (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin; hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,
- Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,
- Kanunun kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi başlıklı 7 nci maddesinin “(1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hale getirilir. (2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır. (3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hale getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir.” hükmünü amir olduğu, bu çerçevede, Kişisel Verilerin Silinmesi Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin yürürlüğe girdiği,
- Kişisel Verilerin Silinmesi Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin kişisel verilerin silinmesine ilişkin 8 inci maddesinin (1) numaralı fıkrasında kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi olarak tanımlanırken (2) numaralı fıkrasında veri sorumlusunun, silinen kişisel verilerin ilgili

kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlü olduğunun ifade edildiği,

- Yönetmelik kapsamında kişisel verilerin silinmesinin iki şekilde düzenlendiği, ilk olarak kişisel verilerin veri sorumlusunca resen silinmesi haline, ikinci olarak da kişisel verilerin ilgili kişinin başvurusu kapsamında silinmesi haline ilişkin düzenleme yapıldığı,

- Yönetmeliğin “Kişisel verileri resen silme, yok etme veya anonim hale getirme süreleri başlıklı” 11 inci maddesinin “(1) Kişisel veri saklama ve imha politikası hazırlamış olan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir. (2) Periyodik imhanın gerçekleştirileceği zaman aralığı, veri sorumlusu tarafından kişisel veri saklama ve imha politikasında belirlenir. Bu süre her halde altı ayı geçemez. (3) Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden üç ay içinde, kişisel verileri siler, yok eder veya anonim hale getirir.” hükmünü haiz olduğu,

- Ayrıca aynı Yönetmeliğin, kişisel verilerin ilgili kişinin talebi çerçevesinde silinmesini düzenleyen “Kişisel verileri ilgili kişinin talep etmesi durumunda silme ve yok etme süreleri” başlıklı 12 nci maddesinde de;

“(1) İlgili kişi, Kanunun (Değişik ibare:RG-28/4/2019-30758) 11 inci ve 13 üncü maddelerine istinaden veri sorumlusuna başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

a) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Veri sorumlusu, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir.

b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa veri sorumlusu bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde bu Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.

c) Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep veri sorumlusunca Kanunun 13 üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.” düzenlemesinin yer aldığı,

• İlgili kişinin kendisine ait kişisel verilerin silinmesi hususunda veri sorumlusuna ilettiği talebin, karşılanmaması iddiasına ilişkin olarak veri sorumlusundan alınan cevabi yazıda ilgili kişiye ait kişisel verilerin Kanunun 5 inci maddesinin (2) numaralı fıkrasının (c), (e) ve (f) bentleri kapsamında, ilgili kişiye aydınlatma yapılması suretiyle işlendiği, söz konusu verilerin ilgili kişinin ilk başvurusu sonucu silindiği, ancak ad-soyad, kimlik bilgileri ve mülakata ilişkin değerlendirme notlarının veri sorumlusu tarafından muhafaza edilmeye devam edildiği, buradaki amacın ise veri sorumlusuna iş başvurusunda bulunan kişilerin, reddedilen başvurusu sonrasındaki dönemlerde yapacakları iş başvurularının değerlendirmesinde, önceki başvurusunun da dikkate alınabilmesi olduğu, bu verilerin Kanunun 5 inci maddesinin (2) numaralı fıkrasının (f) bendinde yer aldığı üzere, veri sorumlusunun “meşru menfaati” çerçevesinde depolanmaya devam edileceğinin bildirildiği ancak ilgili kişinin bu durumu kabul etmeyerek tekrar başvuruda bulunduğu ve başvurusunda veri sorumlusu banka ile ilgili herhangi bir kariyer planı ve olası iş başvurusu olmayacağını belirterek bankada muhafaza edilen tüm kişisel verilerinin silinmesini talep ettiği, bu talebe karşılık olarak da veri sorumlusunca yapılan değerlendirmeler sonucu ilgili kişinin kendisine ait kişisel verileri üzerindeki tasarruf yetkisini önceleyerek ilgili kişiye ait tüm kişisel verilerin ilk periyodik imha sürecinde Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin “Kişisel verileri resen silme, yok etme veya anonim hale getirme süreleri” başlıklı 11 inci maddesi gereği ilk periyodik imha işleminde silineceği hususunu ilgili kişiye ve Kuruma beyan ettiği,

• Ancak; ilgili kişinin Kuruma ilettiği şikayet ekinde de yer alan veri sorumlusuna yaptığı ilk müracaata istinaden veri sorumlusu banka tarafından verilen yanıtta yer alan “ilgili kişinin olası iş başvuruları adına kimlik bilgileri, ad, soyadı bilgilerinin bankanın meşru menfaati çerçevesinde saklanacağı” ifadesinde muğlaklık söz konusu olduğu, zira veri sorumlusunun Kanunun 5 inci maddesinin (2) numaralı fıkrasının (f) bendi kapsamında meşru menfaati çerçevesinde veri işleminin, veri sorumlusuna sınırsız bir alan tanımadığı,

• Bu çerçevede ilgili kişinin ileride yapacağı olası başvurular adına kişisel verilerinin bu başvurularda kullanılacak ve veri sorumlusuna bildirilecek kişisel verilerin teyit edilmesi amacıyla veri sorumlusu tarafından muhafaza edilmesi hususunda, veri sorumlusunun meşru menfaate dayanarak yaptığı savunmasının değerlendirilmesi gerektiği,

• Bu kapsamda, ilgili kişinin verilerinin tamamının silinmesi talebine karşın veri sorumlusunun bahse konu verileri ilk periyodik imhada dikkate alacağına yönelik açıklamasının veri sorumlusunun söz konusu menfaate ulaşılabilmesi bakımından kişisel veri işlenmesinin zorunluluk arz etmediğinin bir

göstergesi olduğu, kişisel verinin işlenmesi sonucunda elde edilecek menfaat ile ilgili kişinin temel hak ve hürriyetlerinin yarışabilir düzeyde olmadığı, ilgili kişinin verilerinin saklanması hususunda veri sorumlusunun meşru menfaatinin açık ve belirli olmadığı, veri sorumlusunun işleme faaliyetinden sağlaması beklenen yararın kişisel veri işlenmeksizin başkaca bir yol ve yöntemle elde edilebileceği ve söz konusu veri işleme faaliyetinin çok sayıda kişiyi etkileyecek şekilde kurumsal bir fayda sağlamadığı değerlendirildiğinden söz konusu kişisel verilerin işlenmesinde veri sorumlusunun meşru menfaatinin ilgili kişinin temel hak ve özgürlüklerine baskın gelmediği,

- İş başvurusunun kabul edilmemesi ile birlikte Kanunun 5 inci maddesinde yer alan veri işleme şartlarından herhangi birinin devam etmediği göz önünde bulundurulduğunda her ne kadar veri sorumlusu tarafından Kişisel Verilerin Silinmesi Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğinin 11 inci maddesi gereği ilk periyodik imha sürecinde imha talebinin yerine getirileceği bilgisi ilgili kişiye verilmiş olsa da verilerin imha talebinin ilgili kişi tarafından Kanunun 7 ve 11 inci maddesi kapsamında veri sorumlusuna yeniden iletildiği, söz konusu imha talebi göz önüne alındığında mezkur Yönetmeliğin 11 inci maddesi kapsamında veri sorumlusu tarafından hazırlanan imha politikasına dayanarak gerçekleştirilecek “resen” imha işleminin söz konusu olamayacağı, aksine aynı Yönetmeliğin 12 inci maddesi kapsamında ilgili kişinin talebi üzerinde imha işleminin gerçekleştirilmesinin gerektiği; bu itibarla da imha işleminin bu madde kapsamında ele alınması gerektiği

değerlendirmelerinden hareketle;

- İlgili kişinin veri sorumlusuna yaptığı iş müracaatının olumsuz sonuçlanması üzerine veri sorumlusu tarafından işlenen kişisel verilerinin silinmesi talebinin veri sorumlusu tarafından önce kısmen kabul görerek ad, soyadı ve kimlik bilgilerinin işlenmesine devam edilmesi, sonrasında ise ilgili kişinin veri sorumlusuna aynı bağlamda yapılan ikinci başvurusu sonucunda yapılan değerlendirmede, söz konusu verilerin veri sorumlusunun imha politikası çerçevesinde gerçekleştirilecek ilk periyodik imha sürecinde imha edileceği kararının alındığının bildirilmesi dolayısıyla ilgili kişinin talebine karşın kişisel verilerinin Kişisel Verilerin Silinmesi Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 12 inci maddesi gereğince 30 gün içerisinde silinmemiş olmasının ve Kanunun 5 inci maddesinde yer alan herhangi bir işleme şartına dayanmaksızın ilgili kişinin kişisel verilerinin işlenmeye devam edilmesinin veri sorumlusunun Kanunun 12 inci maddesinin (1) numaralı fıkrası kapsamında kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari

tedbirleri almadığını gösterdiği kanaatine varıldığından veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca idari para cezası uygulanmasına,

- İlgili kişinin kişisel verilerinin imha edilerek ilgili kişiye ve Kurula konu hakkında bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına,

- İş müracaatı olumsuz sonuçlanmış başka kişilerin bulunması durumunda onların da kişisel verilerinin Kanunun 7 nci maddesi hükümleri çerçevesinde imha edilmesi ve sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2021/666 sayılı KVKK Kararı

Şikâyetçinin yeni doğan bebeğine ait doğum belgesinde yer alan kişisel verilerin üçüncü kişiler tarafından Özel Hastane olarak faaliyet gösteren veri sorumlusundan hukuka aykırı olarak ele geçirilmesi hakkında Kişisel Verileri Koruma Kurulunun 06/07/2021 tarihli ve 2021/666 sayılı Karar Özeti

Karar Tarihi : 06.07.2021

Karar No : 2021/666

Konu Özeti : Şikâyetçinin yeni doğan bebeğine ait doğum belgesinde yer alan kişisel verilerin üçüncü kişiler tarafından Özel Hastane olarak faaliyet gösteren veri sorumlusundan hukuka aykırı olarak ele geçirilmesi

Kuruma intikal eden şikâyetle özetle; şikâyetçinin veri sorumlusu hastanede doğan oğluna ait doğum belgesinin yer aldığı bilgisayar ekran görüntüsünün boşanmış olduğu eski eşi tarafından hastaneden temin edildiği ve Aile Mahkemesinde tarafına açılan yargılamanın iadesi davasına ilişkin dosyada, içeriğinde oğlunun T.C. kimlik numarası, doğum tarihi, anne ve baba adı, hasta numarası vb. kişisel veriler içeren bilgisayar ekran görüntüsünün delil olarak kullanıldığı, konuya ilişkin hastaneye yazılı olarak başvurmasına rağmen başvurusuna, hastane tarafından herhangi bir cevap verilmediği belirtilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- Şikâyetçi ile hastane arasında şikâyet öncesinde ve sonrasında devam eden bir dava süreci bulunmadığı,
- Hastane bünyesinde sağlık ve destek ekipleri dahil olmak üzere toplam 653 personelin çalıştığı, bu nedenle kuruma çeşitli kanallardan gelen ve kurum tarafından gönderilen evrak ve taleplere ilişkin yoğun bir trafiğin mevcut olduğu, bu nedenle gün içerisinde kuruma gelen ve gönderilen evrak ve talep sayılarının değişkenlik göstermekle birlikte gün içerisinde yaklaşık olarak bu sayının yetmiş

bulduđu, evrak trafiđinin yođunluđu nedeniyle bir hata yařandığı ve bařvurunun ilgili birimlere iletilmesindeki aksaklık nedeniyle bařvuru sahibi kiřiye dönüş yapılamadığı,

- Cumhuriyet Bařsavcılıđınca hazırlanan iddianame ve ekinde yer alan görüntünün dođumhane/bebek odasındaki hastaların bilgilerinin takip edildiđi ekran görüntüsü olduđunun tespit edildiđi,
- Bu ekrana ilgili birimde alıřan yatan hasta misafir hizmetleri alıřanları ve hemřirelerin eriřim yetkisinin bulunduđu,
- Mevcut bölümde hizmet veren kiřilerin Kiřiisel Verilerin Korunması Kanunu ve buna bađlı yönetmelikler ile özel nitelikli kiřiisel veri güvenliđi konularında eđitim aldıđı,
- řikâyetçinin yapmış olduđu suç duyurusu üzerine adı geen iki kiřiden alınan ifadelerden de anlaşılacağı üzere her iki řüphelinin de görevliye fark ettirmeden gizlice ekran görüntüsünü ektikleri ve bu hususun zapt altına alındığı,
- Hastane olarak hasta bilgi gizliliđi, hasta mahremiyeti konularındaki prensipleri geređi hasta dosyalarının gizliliđi, hasta bilgilerinin paylaşılmaması, hastane dışına ıkarılmaması gerekliliđi vb. konularda oldukça detaylı idari ve teknik tedbirler alındığı

belirtilmiştir.

Konuya iliřkin yapılan inceleme neticesinde Kiřiisel Verileri Koruma Kurulunun 06/07/2021 tarihli ve 2021/666 sayılı Kararı ile;

- Kanunun "İlgili Kiřinin Hakları" bařlıklı 11 inci maddesinde herkesin, veri sorumlusuna bařvurarak kendisiyle ilgili; kiřiisel verilerinin işlenip işlenmediđini öğrenme, kiřiisel verileri işlenmişse buna iliřkin bilgi talep etme, kiřiisel verilerinin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadıđını öğrenme, yurt içinde veya yurt dışında kiřiisel verilerinin aktarıldığı üçüncü kiřileri bilme, kiřiisel verilerinin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme, 7 nci maddede öngörülen şartlar çerevesinde kiřiisel verilerinin silinmesini veya yok edilmesini isteme, kiřiisel verilerinin düzeltilmesi veya silinmesi/yok edilmesi ile ilgili yapılan işlemlerin kiřiisel verilerinin aktarıldığı üçüncü kiřilere bildirilmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kiřinin kendisi aleyhine bir sonucun ortaya ıkmasına itiraz etme ve kiřiisel verilerinin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme haklarına sahip olduđunun düzenlendiđi,

- Kanunun “Veri Sorumlusuna Başvuru” başlıklı 13 üncü maddesinin ise “İlgili kişi, bu Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kişisel Verileri Koruma Kurulu’nun (Kurul) belirleyeceği diğer yöntemlerle veri sorumlusuna iletir, veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır, talebi kabul eder veya gerekçesini açıklayarak reddeder ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. Ancak, başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hallerinde; ilgili kişi, Kanunun “Kurula Şikayet” başlıklı 14 üncü maddesi kapsamında veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve herhalde başvuru tarihinden itibaren altmış gün içinde Kurula şikayette bulunabilir.” hükmünü haiz olduğu,
- Somut olayda, ilgili kişinin Kanunun 13 üncü maddesi çerçevesinde yazılı olarak veri sorumlusu hastaneye yaptığı başvurunun PTT gönderi belgesi sorgulamasında veri sorumlusunun söz konusu başvuruyu teslim aldığı görüldüğü, ancak yasal süresi içinde başvuruya cevap verilmemesi üzerine şikâyetçi tarafından Kanunun 14 üncü maddesi uyarınca Kuruma şikâyetle bulunulduğunun anlaşıldığı,
- Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğin “Başvuru Usulü” başlıklı 5 inci maddesinde, ilgili kişinin Kanunun 11 inci maddesinde belirtilen hakları kapsamında taleplerini yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletileceğinin, Tebliğin 6 ncı maddesinde ise veri sorumlusunun bu tebliğ kapsamında yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlü olduğunun, veri sorumlusunun başvuruyu kabul edeceği veya gerekçesini açıklayarak reddedeceği ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildireceğinin hüküm altına alındığı,
- Veri sorumlusundan alınan cevap yazısında; hastaneye çeşitli kanallardan birçok evrak geldiği ve evrak trafik yoğunluğu nedeniyle bir hata yaşandığı bu nedenle ilgili kişiye cevap verilemediği yönünde savunmada bulunulduğunun görüldüğü, bu kapsamda veri sorumlusunun Kanun kapsamında kendisine yapılan başvurular ile ilgili olarak Kanunun 13 üncü maddesi ve Tebliğin 6 ncı maddesine uygun olarak hareket etmediği kanaatine varıldığı,
- Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda

bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- 6698 sayılı Kanunun “Özel Nitelikli Kişisel Verilerin İşlenme Şartları” başlıklı 6 ncı maddesinin (2) numaralı fıkrasında özel nitelikli kişisel verilerin ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğu, (3) numaralı fıkrasında birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel verilerin, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebileceği, sağlık ve cinsel hayata ilişkin kişisel verilerin ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceğinin hükme bağlandığı,

- Somut olayda, veri sorumlusu bünyesinde kayıt altına alınan kişisel verilerin yer aldığı ve doğumhane/bebek odasındaki hastaların bilgilerinin takip edildiği sisteme Kanuna aykırı olarak üçüncü kişiler tarafından erişim sağlandığı ve şikâyete konu olan ekran görüntüsünün çekildiği,

- Her ne kadar veri sorumlusu tarafından hasta bilgi gizliliği, hasta mahremiyeti, hasta dosyalarının gizliliği, hasta bilgilerinin paylaşılmaması, hastane dışına çıkarılmaması gerekliliği vb. konularda çalışanlara sürekli eğitimler verildiği ve sürece ilişkin yazılı kurumsal dokümanlar oluşturulduğu ifade edilse de söz konusu olayın meydana geldiği ve kişisel veri ihlaline neden olduğu,

- Veri sorumlusu hastane tarafından kişisel verilere hukuka aykırı erişimi önlemek adına alınan idari ve teknik tedbirlerin yetersiz kaldığı ve sonuç olarak şikâyetçinin velisi bulunduğu ilgili kişiye ait kişisel verilerin üçüncü kişilerce erişimine neden olduğu

değerlendirmelerinden hareketle;

- Şikâyete konu olan ekran görüntüsünün hastanenin veri kayıt sistemine ait ekrandan temin edildiği dikkate alındığında, bu konuda veri sorumlusu Hastanenin gerekli teknik ve idari tedbirleri almadığı; bu minvalde veri güvenliğine ilişkin yükümlülüklerin düzenlendiği Kanunun 12 inci

maddesinin (1) numaralı fıkrasına aykırı hareket ettiği değerlendirildiğinden, veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında idari para cezası uygulanmasına,

- Veri sorumlusu hastaneye çeşitli kanallardan birçok evrak geldiği ve evrak trafik yoğunluğu nedeniyle bir hata yaşandığı bu nedenle ilgili kişiye cevap verilemediği yönünde savunmada bulunduğu görüldüğünden veri sorumlusunun Kanun kapsamında kendisine yapılan başvurularda Kanunun 13 üncü maddesi ve Tebliğin 6 ncı maddesine uygun olarak hareket etmesi yönünde uyarıda bulunulmasına, bu minvalde ilgili kişinin başvurusunda talep ettiği hususlara ilişkin olarak cevap verilmesi ve ilgili kişiye verilen cevaba dair Kurula bilgi verilmesi hususlarında veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2021/664 sayılı KVKK Kararı

İlgili kişinin, doğal gaz dağıtımını yapan bir şirket tarafından düzenlenen faturasında kişisel verisi niteliğindeki banka bilgisine yer verilmesi hakkında Kişisel Verileri Koruma Kurulunun 06/07/2021 tarihli ve 2021/664 sayılı Karar Özeti

Karar Tarihi : 06.07.2021

Karar No : 2021/664

Konu Özeti : İlgili kişinin, doğal gaz dağıtımını yapan bir şirket tarafından düzenlenen faturasında kişisel verisi niteliğindeki banka bilgisine yer verilmesi

İlgili kişinin Kuruma intikal ettirdiği şikâyet dilekçesinde özetle; kendisinin de aboneliği olduğu doğal gaz dağıtım hizmeti veren şirketin (veri sorumlusu) düzenlediği faturalarda "Otomatik Ödeme Talimatı" bölümünde kişilerin ödeme yaptığı banka adı bilgisine yer verildiği, faturada bu bilgiye yer verilmesi sebebiyle ilgili kişinin hangi bankada hesabının bulunduğu açıkça anlaşıldığı, söz konusu bilginin kişisel veri niteliğini haiz olduğu, faturada bu bilgiye yer verilmesinin ilgili kişinin kişisel verisinin üçüncü kişilerle paylaşılması anlamına geldiği, bahsi geçen bilginin kötü niyetli kişilerin eline geçmesi halinde dolandırıcılığa yol açabileceği, bu çerçevede düzenlenen faturalardan banka adı bilgisinin silinmesi talebine yönelik olarak veri sorumlusuna başvuruda bulunmuş olmasına rağmen veri sorumlusu tarafından olumsuz yanıt verildiği ifade edilerek 6698 sayılı Kişisel Verileri Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde söz konusu iddialara yönelik veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle,

- EPDK'nın Doğal Gaz Piyasası Dağıtım ve Müşteri Hizmetleri Yönetmeliğinin ilgili hükümlerine göre hizmet sunulan müşteriler ile "müşteri sözleşmesi" imzalandığı, müşterilerce gerçekleştirilen tüketimlerin taraflarınca faturalandırıldığı, müşterilerin ise ödemelerini veri sorumlusunun vezneleri, PTT veya anlaşmalı bankalar kanalıyla gerçekleştirdikleri, müşterilerce banka kanalıyla gerçekleştirilen ödeme işlemlerinin de ilgili bankalara ait ATM, vezne ya da otomatik ödeme yöntemlerinden herhangi biri ile gerçekleştirildiği,

- Abonelerden, sözleşme tanzim edilmesi işlemleri esnasında “Otomatik Ödeme” ya da banka bilgisi talep edilmediği, talimat bilgi ve verisinin; ödemelerini otomatik ödeme kanalıyla gerçekleştiren müşterilerin çalıştıkları bankalar aracılığıyla, banka ile veri sorumlusu arasındaki sistem entegrasyonu kapsamında veri sorumlusuna aktarıldığı ve aktarılan bu bilgilerin Kanunun 4 üncü maddesi ile 5 inci maddesinin (2) numaralı fıkrasının (c) bendi kapsamında veri sorumlusunun sistemlerinde yer aldığı, söz konusu verilerin sistemlerinde yer almasının, sözleşme kapsamındaki işlerinin ifası için zorunlu olduğu, aksi durumda bazı sorunların oluşacağı,
- Bankaya verilen otomatik ödeme talimatı sonrasında ilgili bankanın veri sorumlusunun sisteminden talimat sahibi abonenin borç bilgisini anlık olarak çektiği ve faturanın son ödeme tarihinde abonenin hesabından tahsilatı yaparak, tahsilat bilgisini veri sorumlusunun sistemine aktardığı, bu işlemlerin yapılması için ilgili bankaların, veri sorumlusu şirketin veri tabanında kendi bankalarına ait koda ve veriye teknik olarak gereksinim duyduğu, dolayısıyla söz konusu verinin veri sorumlusunun sistemlerinde yer almaması halinde, ilgili bankaların sistemsel sıkıntılar yaşayacağı ve ödenemeyen borçlar sebebiyle müşterilerin gaz arzının durdurulması sonucunun doğacağı, bu durumun bir yandan abonelerin mağduriyet yaşamasına yol açacağı, diğer yandan da veri sorumlusu şirketin işinin ifasında sıkıntı oluşturarak meşru menfaatlerine zarar vereceği,
- Diğer taraftan, ilgili kişinin faturada “Otomatik Ödeme Talimatı” başlığı karşısında yer alan banka bilgisinin kaldırılması talebinin veri sorumlusu tarafından tüm müşterileri kapsayacak şekilde yerine getirildiği, faturalarını otomatik ödeme talimatı vermek suretiyle ödeyen tüm abonelerin faturalarında banka talimatı bölümünde banka adı yazma uygulamasının kaldırıldığı ve talimat varsa sadece “VAR” ifadesi yazılacak şekilde gerekli düzeltmelerin yapıldığı

ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 06/07/2021 tarih ve 2021/664 sayılı Kararı ile;

- Kanunun “Tanımlar” başlıklı 3 üncü maddesinde “kişisel veri”nin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi; “veri sorumlusu”nun kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi; “kişisel verilerin işlenmesi”nin ise kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da

kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı,

- Kanunun "Genel İlkeler" başlıklı 4 üncü maddesinde kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, bu çerçevede, kişisel verilerin ancak; hukuka ve dürüstlük kurallarına uygun şekilde, belirli, açık ve meşru amaçlar kapsamında, doğru ve gerektiğinde güncel olma şartıyla, işleneceği, amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun olarak işleneceği,

- Kanunun kişisel verilerin işleme şartlarının belirlendiği 5 inci maddesinin (1) numaralı fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği hüküm altına alınmış olmakla birlikte, (2) numaralı fıkrasında, sayılan hallerde ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesine imkan tanındığı, buna göre;

a) Kanunlarda açıkça öngörülmesi,

b) Fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması,

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması

hallerinden birinin varlığı durumunda ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün bulunduğu,

- İlgili kişinin şikâyetine konu olan veri sorumlusu tarafından adına düzenlenen faturada yer verilen kişisel veri niteliğindeki banka adı bilgisinin, doğrudan ilgili kişiden elde edilmediği, ilgili kişinin faturalarının ödenmesini teminen bankaya verdiği otomatik ödeme talimatı dolayısıyla banka tarafından veri sorumlusu şirkete aktarıldığı görüldüğünden; bu kapsamda söz konusu banka adı

bilgisinin veri sorumlusu ile ilgili kiři arasında dzenlenen Doęalgaz Abonelik Sözleşmesi kapsamında Kanunun 5 inci maddesinin (2) numaralı fıkrasının (c) bendinde yer alan “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.” şartı uyarınca veri sorumlusu tarafından işlenmesinin Kanuna uygun olduğu,

- Öte yandan, ilgili kişinin söz konusu banka adı bilgisinin faturada yer alması nedeniyle hâlihazırda herhangi bir hak ihlali yaşamadığı,

- İlgili kişinin dzenlenen faturalardan banka adı bilgisinin silinmesi talebine yönelik veri sorumlusuna yaptığı başvuruya veri sorumlusu tarafından olumsuz yanıt verildiği iddiasına ilişkin olarak, Kuruma iletilen fatura örnekleri incelendiğinde veri sorumlusunca talep sonrası dzenlenen hiçbir faturada banka adı bilgisine yer verilmediği, banka talimatı bölümünde banka bilgisine yer verilmeyip sadece “VAR” ifadesinin kullanıldığı görüldüğü bu kapsamda ilgili kişinin talebinin yerine getirildiği kanaatine varıldığı

deęerlendirmelerinden hareketle,

- İlgili kişinin kişisel verisi niteliğinde olan banka adı bilgisinin, ilgili kişinin faturalarının ödenmesini teminen bankaya verdiği otomatik ödeme talimatı dolayısıyla veri sorumlusu ile ilgili kiři arasında dzenlenen Doęalgaz Abonelik Sözleşmesi kapsamında Kanunun 5 inci maddesinin (2) numaralı fıkrasının (c) bendinde yer alan “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.” işleme şartına dayanılarak işlendiği; öte yandan ilgili kişinin söz konusu banka adı bilgisinin faturada yer alması nedeniyle herhangi bir hak ihlali yaşadığının tespit edilemediği ve veri sorumlusunun ilgili kişinin talebini yerine getirdiği hususları dikkate alındığında bu aşamada şikayete konu iddialar ile ilgili olarak Kanun kapsamında yapılacak bir işlem olmadığına

karar verilmiştir.

2021/603 sayılı KVKK Kararı

İlgili kişinin internet alışveriş sayfası üzerinden ev adresine teslim talepli olarak vermiş olduğu siparişlerinin veri sorumlusu kargo şirketi tarafından, hiçbir suretle belirtmediği halde işyeri adresine gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 22/06/2021 tarihli ve 2021/603 sayılı Karar Özeti

Karar Tarihi : 22.06.2021

Karar No : 2021/603

Konu Özeti : İlgili kişinin internet alışveriş sayfası üzerinden ev adresine teslim talepli olarak vermiş olduğu siparişlerinin veri sorumlusu kargo şirketi tarafından, hiçbir suretle belirtmediği halde işyeri adresine gönderilmesi hakkında

İlgili kişinin Kuruma intikal eden şikayet dilekçesinde özetle: internet alışveriş sayfası üzerinden ev adresine teslim talepli olarak sipariş verdiği, vermiş olduğu siparişlerinin kendisine gönderiminin hangi kargo firması ile gerçekleşeceğini sipariş formunda yer aldığı, bununla birlikte söz konusu siparişlerin gerek teslimat gerek fatura adresi olsun hiçbir suretle belirtmediği halde işyeri adresine gönderiminin yapıldığını tespit ettiği; 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 11 inci maddesi hükmü kapsamındaki hakları ve 13 üncü maddesi uyarınca taşımacılık sektöründe faaliyet gösteren veri sorumlusuna dilekçe ile iadeli taahhütlü olarak başvuru yaptığı, söz konusu başvurusunda hukuka aykırı olarak elde edilmiş kişisel verilerinin yok edilmesi, kişisel verilerinin kullanım amacına uygun olarak kullanılması, üçüncü kişilere aktarılmış olan kişisel verilerine dair yapılan işlemlere ilişkin ilgili üçüncü kişilere bilgi verilmesi ve kişisel verisi olan iş yeri adresinin yasal mevzuata ve hukuka uygun olarak işlenmişse dahi işlenmesini gerektirir sebebin ortadan kalkmış olduğunu düşündüğünden söz konusu kişisel verilerinin yok edilmesi talebinde bulunduğu; fakat veri sorumlusu tarafından bu başvurusuna 30 günlük süre içinde cevap verilmediği belirtilerek, konunun incelenmesi, kişisel verilerinin halen silinmemiş olması nedeniyle veri sorumlusuna talimat verilmesi ve hakkında gerekli işlemlerin tesis edilmesi talep edilmiştir.

Başlatılan inceleme çerçevesinde veri sorumlusu kargo şirketinden savunması istenilmiş olup, alınan cevabi yazıda özetle;

- Taraflarının, ilgili kişi başvurularını Kanuna ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğe uygunluk konusunda ön değerlendirmeye tabi tuttuğu, ancak söz konusu olayda ilgili kişinin başvuruyu posta yoluyla gerçekleştirmiş olduğu ve başvuru evrakında T.C. kimlik numarasının yer almadığı, ilgili kişinin kimliğinin doğruluğunu teyit etmeden yapılan her türlü bilgi paylaşımının kişisel veri güvenliği açısından riskli olacağı, bu nedenle ilgili kişi tarafından gönderilen yazının hukuki olarak veri sorumlusuna başvuruda bulunması gereken hukuki nitelikleri taşımadığı,
- Şikayete konu kargo gönderimi esnasında birbirine rakip internet satış şirketlerinin indirim yapması sonrası oluşan kargo yoğunluğu sebebiyle, ilgili kişinin paketinin sehven ev adresi yerine iş yeri adresine yönlendirilmiş olduğunun görüldüğü; ancak ilgili kişinin teslimat sırasında bu adreste bulunmaması nedeniyle bu adreste herhangi bir teslimatın gerçekleştirilmediği,
- Yazı ekinde yer alan sistem çıktılarında görüldüğü üzere ilgili kişinin iş yeri adresinin, iş yerine gönderilmek üzere talepte bulunduğu önceki tarihli kargoların kendisine teslimi amacıyla (bir sözleşmenin ifası kapsamında veri işleme şartına dayalı olarak) taraflarına iletilen bilgiler neticesinde elde edildiği,
- 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanunun "Muhafaza ve ibraz" başlıklı, 8 inci maddesinin "(1) Yükümlüler, bu Kanunla getirilen yükümlülüklerle ve işlemlerine ilişkin her türlü ortamdaki: belgeleri düzenleme tarihinden, defter ve kayıtları son kayıt tarihinden, kimlik tespitine ilişkin belgeleri ise son işlem tarihinden itibaren sekiz yıl süreyle muhafaza ve istenmesi halinde yetkililere ibraz etmekle yükümlüdür." şeklinde düzenlendiği, ayrıca Bilgi Teknolojileri ve İletişim Kurulunun 27/12/2016 tarih ve 2016/DK-YED/517 sayılı kararı ile düzenlenen Posta Gönderilerine İlişkin Usul ve Esaslar'ın Posta gönderilerinin kabulü ve teslimi aşamasında yapılacak işlemler başlıklı 4 üncü maddesinin "Hizmet sağlayıcılar tarafından, haberleşme gönderileri hariç, posta gönderilerinin kabulü aşamasında: asgari olarak;(...) alıcının adı-soyadı ve açık adres bilgisi (...) kayıt altına alınır, gerektiğinde ilgili mercilere sunulmak üzere gizliliği sağlanarak en az iki yıl süreyle saklanır." şeklinde olduğu ve bu nedenle gönderim esnasında taşıma işini gerçekleştirmek üzere veri sorumlusuna beyan edilmiş kişisel verilerin mevcut kayıtlarından yasal zorunluluk gereği silinemediği,
- İlgili kişiye ait kişisel verilerinin bulunduğu veri tabanında kayıtlı bütün cari hesapların pasif hale getirildiği, pasif hale getirilen hesapların sistem kaydı ekran görüntüsünün yazı ekinde sunulduğu, bu bilgilerin saha personeli tarafından görüntülenemez, kullanılamaz ve pasif durumu değiştirilemez olduğu, pasif durumda olan cari bilgilerin yalnızca merkez birimi tarafından değiştirilebildiği, bu hususun tekrar yaşanmaması adına sistemlerinde mevcut cari kayıtlar güncellenerek ilgili kişinin

yeni siparişlerinde vermiş olduğu güncel bilgiler doğrultusunda yeniden cari açılımı yapılarak kargo gönderimi gerçekleştirileceği ifade edilmiştir.

Konuya ilişkin olarak yapılan incelemede, Kişisel Verileri Koruma Kurulunun 22/06/2021 tarihli ve 2021/603 sayılı Kararı ile;

- Kanunun "Tanımlar" başlıklı 3 üncü maddesinde "kişisel veri"nin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi; "veri sorumlusu"nun kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi; "kişisel verilerin işlenmesi"nin ise kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı,

- Kişisel verilerin işlenme şartlarının ise Kanunun 5 inci maddesinde "(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması." şeklinde hüküm altına alındığı,

- Bu çerçevede, ilgili kişinin kişisel verilerinin hukuka aykırı işlendiğine ilişkin iddiaları ile ilgili olarak somut olayda veri sorumlusu tarafından gönderinin kabulü aşamasında ilgili kişinin adresinin kaydedilmesinin Kanunun 5 inci maddesinin (2) numaralı fıkrasının (ç) bendinde yer alan “Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması” şartına dayanılarak yapıldığının açık olduğu, buna karşın veri sorumlusu tarafından ilgili kişinin belirtmiş olduğu adresten farklı bir adrese (daha önce ilgili kişinin kargo teslimatlarının yapıldığı iş yeri adresi) teslimatın yönlendirilerek iletişim bilgisinin işlenmesinin Kanunun 5 inci maddesinde yer alan kişisel veri işleme şartlarından herhangi birine dayanmaksızın gerçekleştiği dolayısıyla veri sorumlusunun Kanunun “Veri Güvenliğine İlişkin Yükümlülükler” başlıklı 12 nci maddesinin (1) numaralı fıkrasında belirtilen yükümlülüğüne aykırı hareket ettiği,
- İlgili kişinin verilerinin silinmesine yönelik talebi ile ilgili olarak, veri sorumlusu tarafından, gönderim esnasında taşıma işini gerçekleştirmek üzere beyan edilmiş olan adresi, adı, soyadı ve irtibat telefon numarasının mevcut kayıtlarından yasal zorunluluk gereği silinemediği, kişisel verilerin korunması ve güvenliğinin azami ölçüde sağlandığı ve işlenen kişisel verilerin taraflar arası hukuki ilişkinin niteliği gözetilerek ve ilgili kanunlarda öngörülen yasal zorunluluk ve zaman aşımı süreleri ve diğer hukuki yükümlülükler dikkate alınarak gereken süre boyunca saklandığı ve akabinde silme, yok etme veya anonim hale getirme yöntemleri gözetilerek imha edildiği, bu çerçevede ilgili kişinin kişisel verilerinin bulunduğu (isim soy isim, adres, iletişim no vb.) veri tabanında kayıtlı bütün cari hesapların pasif hale getirildiği, pasif hale getirilen hesapların sistem kaydı ekran görüntüsünün savunma yazısı ekinde gönderildiği ve pasif hale getirilen cari bilgilerin saha personeli tarafından görüntülenemez, kullanılamaz ve pasif durumu değiştirilemez olduğu,
- Posta Gönderilerine İlişkin Usul ve Esaslar’ın Posta gönderilerinin kabulü ve teslimi aşamasında yapılacak işlemler başlıklı 4 üncü maddesinde gönderinin kabulü ve teslimi aşamasında en az 2 yıl süreyle saklanacak verilerin açıkça düzenlendiği, ilgili kişinin iş yeri adresine uygun olan son kargo hareketinin 26.02.2019 tarihli olduğu ve sehven yanlış adrese yapılan gönderimin ise 02.11.2019 tarihli olduğunun belirtildiği, bu çerçevede, Kanunun 7 nci maddesi kapsamında ilgili kişinin kişisel verilerinin silinmesini gerektiren sebebin ortadan kalkmadığı ve cari bilgilerin pasif hale getirildiği,
- İlgili kişinin veri sorumlusuna yapmış olduğu başvurusuna veri sorumlusu tarafından 30 günlük süre içinde cevap ve bilgi verilmemesi iddiasına ilişkin olarak, her ne kadar Tebliğin 5 inci maddesinin (2) numaralı fıkrasında T.C. kimlik numarasının bulunmasının zorunlu olduğu düzenlenmiş olsa da veri sorumlusuna tebliğ edildiği açık olan ilgili kişinin yazılı başvurusunun Kanuna uygun olarak cevaplandırılması için ilgili kişinin yönlendirilmediği, eksik hususların

tamamlanmasına yönelik ilgili kişiyi yönlendirici gerekli aksiyonun veri sorumlusu tarafından alınmadığı, bu kapsamda başvurusunun bu şekilde cevapsız bırakılmasının Tebliğin 6 ncı maddesinin (1) numaralı fıkrasına aykırılık teşkil ettiği

değerlendirmelerinden hareketle;

- Veri sorumlusu tarafından ilgili kişinin belirtmiş olduğu adresten farklı bir adrese (daha önce ilgili kişinin kargo teslimatlarının yapıldığı iş yeri adresi) teslimatın yönlendirilerek iletişim bilgisinin işlenmesinin Kanunun 5 inci maddesinde yer alan kişisel veri işleme şartlarından herhangi birine dayanmaksızın gerçekleştiği, dolayısıyla veri sorumlusunun Kanunun 12 nci maddesinin (1) numaralı fıkrasında belirtilen yükümlülüğe aykırı hareket ettiği kanaatine varılması nedeniyle veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı (b) bendi hükmü uyarınca idari para cezası uygulanmasına,

- İlgili kişinin kişisel verisi olan iş yeri adresinin silinmesi/yok edilmesi talebine ilişkin olarak veri sorumlusu bünyesinde Kanunun 7 nci maddesi kapsamında ilgili kişinin kişisel verilerinin işlenmesini gerektiren sebeplerin ortadan kalkmadığı ve cari bilgilerin pasif hale getirildiği dikkate alındığında Kanun kapsamında bu çerçevede yapılacak bir işlem olmadığına,

- Veri sorumlusuna tebliğ edildiği açık olan ilgili kişinin yazılı başvurusunun Kanuna uygun olarak cevaplandırılması için ilgili kişinin yönlendirilmediği, eksik hususların tamamlanmasına yönelik gerekli aksiyonun veri sorumlusu tarafından alınmadığı ve başvurusunun cevapsız bırakıldığı, dolayısıyla Tebliğin 6 ncı maddesinin (1) numaralı fıkrasında belirtildiği üzere, ilgili kişi tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almadığı değerlendirildiğinden veri sorumlusunun ilgili kişinin başvurusundaki eksik hususların tamamlanmasına yönelik gerekli aksiyonları alması ve Tebliğ hükümlerine azami özeni göstermesi hususunda talimatlandırılmasına

karar verilmiştir.

2021/584 sayılı KVKK Kararı

Sigortacılık ve bireysel emeklilik alanında faaliyet gösteren bir şirket tarafından ilgili kişiye ait kişisel verilerin hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 09/06/2021 tarihli ve 2021/584 sayılı Karar Özeti

Karar Tarihi : 09.06.2021

Karar No : 2021/584

Konu Özeti : Sigortacılık ve bireysel emeklilik alanında faaliyet gösteren bir şirket tarafından ilgili kişiye ait kişisel verilerin hukuka aykırı olarak işlenmesi

Kuruma intikal eden şikayet dilekçesinde özetle; Sigortacılık ve Bireysel Emeklilik alanında faaliyet gösteren bir şirket tarafından ilgili kişinin cep telefonu numarasına "Sayın, Sizinle görüşmemiz öncesinde, hakkımızdaki özet bilgilere aşağıda yer alan linki tıklayarak kolayca ulaşabilirsiniz... IPTAL: ... Ret yazıp ...'e gönderiniz. ONAY: ... Onay yazıp ...'e gönderiniz. Eğer bu mesaja 24 saat içerisinde tarafınızca herhangi bir <> yanıtı iletilmez ise, aranmak için olumlu yanıt verdiğiniz varsayılacaktır..." içerikli bir SMS gönderildiği, kişinin adı geçen şirket ile herhangi bir ilişkisinin olmadığı, veri sorumlusu tarafından ticari elektronik ileti gönderilmesi üzerine ilgili kişi tarafından veri sorumlusuna e-postayla başvuruda bulunulduğu, başvuruda telefon numarası, ad/ soyadının nasıl elde edildiği, başka kişisel verilerinin işlenip işlenmediği hakkında bilgi talebinde bulunduğu, şirket tarafından verilen cevapta SMS gönderen finansal danışmanın elindeki bir soğuk referans listesinden telefon numarasına ulaşıldığı, söz konusu iletinin tarafına tanıtım yapabilmek için izin amaçlı gönderildiği, GSM numarası ve isminin aranmayacak kişiler listesine alındığı, bilgilerin üçüncü şahıslara ya da herhangi bir platforma aktarılmadığı ve referans listelerinden silindiği, taraflarınca gerekli idari ve teknik önlemlerin alındığı bilgisinin verildiği, söz konusu şirket tarafından ilgili kişinin aranmayacak kişiler listesine aktarıldığı bilgisinden kişisel veri işlemeye devam edildiğinin anlaşıldığı, bununla birlikte verilen yanıtta ilgili kişinin ad ve soyadının nasıl elde edildiğine ilişkin bilgiye yer verilmediği, ayrıca, gönderilen iletide ilk 24 saat içinde iptal yanıtı verilmezse aranmak için olumlu yanıt verildiğinin varsayılacağı bilgisinin yer aldığı bu işleğin hukuka aykırı olduğu belirtilerek yukarıda yer verilen hususlara ilişkin olarak gerekli yaptırımın uygulanması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle,

- Veri sorumlusu tarafından ilgili kişinin adı soyadı ve telefon bilgisinin ürünlere ilişkin teklif araması yapılmadan önce gerçekleştirilen araştırmalar sonucunda bir Baronun resmi internet sitesi üzerinden temin edildiği, söz konusu sitede ilgili kişi gibi Baroya kayıtlı avukatların adı soyadı, telefon numarası ve e-posta adresi gibi iletişim bilgilerinin yer aldığı ve bu bilgilerin herkes tarafından ulaşılabilecek aleni veriler olduğu,
- Sigortacılık ve Bireysel Emeklilik alanında faaliyet gösteren veri sorumlusunun, poliçelerinin tanıtım ve satışını yaparak satış sonrasında sigortacılık konusunda müşterilerine hizmet verdiği, ilgili kişinin cep telefonuna gönderilen SMS'in de şirketlerinin faaliyet alanı ve meşru menfaatleri kapsamında ürün tanıtımı yapılmadan önce bu amaçla gönderildiği, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 4 üncü maddesinin (2) numaralı fıkrasında yer alan kişisel verilerin işlenmesine ilişkin ilkeler arasında yer aldığı üzere, şirketlerinin hukuka uygun bir şekilde "belirli, açık ve meşru amaçlar" çerçevesinde kişisel veri işlediği ve mevzuattan kaynaklanan idari ve teknik tedbirleri aldığı,
- Kanunun "Kişisel Verilerin İşlenme Şartları" başlıklı 5 inci maddesinde kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği (2) numaralı fıkrasının (d) bendinde ise "İlgili kişinin kendisi tarafından alenileştirilmiş olması" şeklinde kişisel verilerin açık rıza olmaksızın işlenmesinin mümkün olduğuna ilişkin düzenleme bulunduğu,
- Kanunun 5 inci maddesinin (2) numaralı fıkrasının (d) bendine ilişkin TBMM Kanun gerekçesinde "fıkranın (d) bendine göre, ilgili kişinin kendisi tarafından alenileştirilen bir başka ifadeyle herhangi bir şekilde kamuoyuna açıklanmış olan kişisel verileri işlenebilecektir. Çünkü ilgili kişi tarafından alenileştirilen ve böylelikle herkes tarafından bilinebilecek hale gelen bu tür verilerin işlenmesinde, korunması gereken hukuki yararın ortadan kalktığı kabul edilmektedir." ifadelerinin yer aldığı, TBMM gerekçesinde söz konusu fıkra amacından bahsedilirken, temel ölçüt olarak sayısı belirsiz kişi tarafından görülebilecek durumda olma unsurunun kabul edildiği ve "herhangi bir şekilde" ibaresi kullanılarak alenileşmenin meydana gelmesi için başka bir şart aranmadığının ifade edildiği, ayrıca gerekçede alenileştirilen verilerin işlenmesinde korunması gereken hukuki yararın ortadan kalktığının belirtildiği, zira artık ilgili kişinin kendisinin dahi verinin korunması için bir çaba sarf etmediği,

- Bu bağlamda ilgili kişinin söz konusu bilgilerinin, telefonla aranmadan önce zaten ilgili kişi tarafından alenileştirildiğinden açık rızası alınmadan işlenmesinin mevzuata aykırılık teşkil etmeyeceğinin değerlendirildiği,
- Öte yandan, Kişisel Verilerin Korunması Kanununun 5 inci maddesinin (2) numaralı fıkrasının (f) bendinde ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması halinde ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğunun düzenlendiği, veri sorumlusunun sigortacılık ve bireysel emeklilik alanında faaliyet gösteren, bu faaliyetleri sonucunda ticari kazanç elde etmeyi amaçlayan ve sektördeki diğer tüm şirketler gibi faaliyet alanında meşru çalışmalar yürüten bir tüzel kişilik olduğu, söz konusu faaliyetlerin yürütülmesi sırasında veri sorumlusunun var olma amaçlarından olan poliçe satış işleminin gerçekleştirilmesinin de veri sorumlusu için meşru bir menfaat olduğu, dolayısıyla şirketlerinin var olması için poliçe satışı yapmak zorunda olduğu, poliçe satışı yapmak için de teklif araması yapılması gerektiği ve teklif araması sırasında mesaj gönderilen kişinin ad, soyadı ve telefon numarası bilgilerinin önceden şirket uhdesinde bulunması zorunluluğunun da izahtan vareste olduğu, bu nedenle Kanunun 5 inci maddesinin (2) numaralı fıkrasının (f) bendinin de bu gibi durumlarda ilgili kişinin açık rızasının aranmasına gerek olmadığını belirttiği ve ticari hayatın olağan akışı içinde seyrine imkan tanıdığı, şirketlerinin meşru menfaatleri ve Kanunun meşru menfaat hükmü birlikte değerlendirildiğinde taraflarınca hukuka aykırı bir işlem yapılmadığı,
- İlgili kişi tarafından veri sorumlusuna yapılan başvuruya, verilerinin veri sorumlusunun faaliyet alanı çerçevesinde meşru amaçlar çerçevesinde kendisine ürün tanıtımı ve pazarlaması yapılması amacıyla, hangi kanaldan elde edildiği de belirtilerek yanıt verildiği, ilgili kişinin, başvurusu üzerine veri sorumlusu nezdinden tutulan "Aranmayacaklar Listesi"ne alındığının, bunun ötesinde verilerinin hiçbir şekilde işlenmediği, yurt içinde veya yurt dışında üçüncü kişiler ile paylaşılmadığının ifade edildiği, söz konusu liste ile kişisel verilerinin silinmesini veya kendisi ile iletişime geçilmemesini talep eden ilgili kişilerin verilerinin işlenmesinin engellendiği, bu şekilde veri sorumlusunun faaliyetlerine devam ederken uyması gereken bir diğer mevzuat olan Ticari Elektronik İletim mevzuatına da uygun hareket edildiği,
- Ticari İletişim ve Ticari Elektronik İletimler Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin "İspat yükümlülüğü ve kayıtları saklama süresi" başlıklı 13 üncü maddesinin ikinci fıkrası gereğince; hizmet sağlayıcıların onay kayıtlarının, onay geçerliliğinin sona erdiği tarihten; ticari elektronik ilettilere ilişkin diğer kayıtların ise kayıt tarihinden itibaren üç yıl süreyle saklanması

gerektiđi, ayrıca talep edildiđinde ilgili kayıtların Bakanlıđa sunulacađının düzenlendiđi, buna ek olarak hizmet sađlayıcılara bildirilen "ret" bildirimlerinin de İleti Yönetim Sistemine 3 iş günü içinde bildirilmesi gerektiđi, zira bu hakkın kullanılmasının 6698 sayılı Kanun kapsamında açık rızanın geri alınması ile eşdeđer olduđu, bahsi geçen "Aranmayacaklar Listesi" ile kendisine ticari elektronik ileti gönderimine onay vermeyen kişilerin yer aldıđı listenin iç içe bir bütün olduđu ve veri sorumlusu tarafından bu listenin mevzuattan kaynaklanan yükümlülükler çerçevesinde saklandıđı, mevzuat uyarınca saklama süreleri bittiđinde bu verilerin de Şirketleri tarafından imha edileceđi, ayrıca veri sorumlusu tarafından alınan teknik ve idari tedbirler çerçevesinde ilgili listenin sadece yaptıđı iş geređi erişimi zorunlu olan kişilere açılarak yetki verildiđi,

- İlgili kişiye SMS gönderimi yapılan tarihte henüz ticari elektronik ileti gönderiminden önce onay alınmasına ilişkin yürürlüğe giren bir zorunluluk bulunmadıđı, içinde bulunulan pandemi süreci nedeniyle ticari elektronik ileti gönderiminden önce onay alınması ve ilgili ret veya onayların tutulmasına ilişkin uygulamanın bir zorunluluk olarak yürürlüğe girişinin birden çok defa ertelendiđi,

- Şirketlerinin satış politikası geređince meşru faaliyet alanı çerçevesinde elde edilen kişisel veri olan iletişim bilgileri üzerinden müşteri adaylarına ticari elektronik ileti almak isteyip istemediđinin sorulması suretiyle veri sorumlusunun ilgili kişilere açık rıza gösterme hakkı sađladıđı ifade edilmiştir.

Konuya ilişkin olarak yapılan incelemede Kişisel Verileri Koruma Kurulunun 09/06/2021 tarihli ve 2021/584 sayılı Kararı ile;

- Kanunun, kişisel verilerin işlenmesine ilişkin "Genel İlkeler"i düzenleyen 4 üncü maddesinin (1) numaralı fıkrasında, "Kişisel veriler, ancak bu Kanunda ve diđer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir." hükmü yer almakta olup bahse konu maddenin ikinci fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin; hukuka ve dürüstlük kurallarına uygun olma, dođru ve gerektiđinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldıđı,

- Kanunun "Kişisel Verilerin İşlenme Şartları" başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceđi, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı

veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işleniminin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Öte yandan Kanunun 'Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi' başlıklı 7 inci maddesinin (1) numaralı fıkrasında bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silineceği, yok edileceği veya anonim hale getirileceğinin hüküm altına alındığı,

- Ayrıca, Kanunun "Veri Güvenliğine İlişkin Yükümlülükler" başlıklı 12 nci maddesinin (1) numaralı fıkrasında "Veri sorumlusu; kişisel verilerin hukuka aykırı işlenmesini önlemek, kişisel verilere hukuka aykırı erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır." hükmüne yer verildiği,

- Somut olayda, veri sorumlusu tarafından söz konusu cep telefonu numarasının elde edildiği kaynak olarak iddia edilen internet sitesinde her ne kadar ilgili kişinin cep telefonu numarasına rastlanılmasa da ilgili kişi tarafından bağlı bulunduğu Baronun resmi internet sayfasında söz konusu kişisel verinin alenileştirilmesi hususunda öncelikle ilgili kişinin söz konusu alenileştirme kapsamında iradesi olması gerektiği, bu anlamda, tek başına kişisel verinin kamuoyuna açık hale gelmesinin, örneğin herkesin görebileceği bir yerde olması ya da herkesin erişimine açık durumda bulunmasının alenileştirilmiş olması bakımından yeterli olmadığı; eylemin, ilgili kişinin iradesi ile de desteklenmesi gerektiği, söz konusu olay kapsamında, veri sorumlusu tarafından ilgili kişinin telefon numarasının ilgili kişinin kayıtlı olduğu Baronun internet sayfasından elde edildiği kanıtlanamamakla birlikte yapılan incelemede de bu numaraya rastlanılmadığı, dolayısıyla söz konusu cep telefonu numarasının ilgili kişinin kendi iradesi ile alenileştirildiği hususuna ilişkin kanıtlayıcı herhangi bir bilgi ve belgenin de mevcut olmadığı,

- Veri sorumlusu tarafından iddia edildiği üzere Baronun internet sayfasından cep telefonu numarası elde edildiği kabul edilse dahi ilgili kişinin ne amaç ile kişisel verilerini alenileştirdiğinin tespitinin

gerektiđi, bu bağlamda ilgili kiřinin kendisi tarafından alenileřtirilen, bir bařka ifadeyle herhangi bir řekilde kamuoyuna aıklanmıř olan kiřisel verileri iřlenebilecek olup sz konusu olayda da avukatın avukatlık faaliyeti kapsamında kendisiyle iletiřime geilmesi amacıyla iletiřim bilgilerini kamuya aık bir hale getirdiđi, alenileřtirme eylemi, ilgili kiřilerin kiřisel verilerini kamuoyu ile paylařma amacıyla sınırlı olup veri sorumlularının ilgili kiřinin alenileřtirme amacından farklı ya da bu amacı ařan řekilde kiřisel veri iřleme faaliyetinde bulunmalarının, bařkaca bir iřleme řartına dayanılmadıđı srece, Kanuna aykırılık oluřturacađı, bu kapsamda ilgili kiřinin kiřisel verisi niteliđindeki telefon numarasına gnderilen kısa mesajlar incelendiđinde ilgili kiřinin mesleki yetkinliđinden faydalanmak iin kendisine ulařılmaya alıřılmadıđı, aksine řirket faaliyetlerine iliřkin randevu talebi ile ilgili kiřiye ulařıldıđı, ieriklerin reklam, pazarlama ve bilgilendirme amalı olduđu deđerlendirilmekte olup bu erevede ilgili kiřinin telefon numarasının reklam, pazarlama ve bilgilendirme amacıyla kısa mesaj gnderilmek suretiyle iřlenmesinin Kanununun 5 inci maddesinin (2) numaralı fıkrasının (d) bendinde yer alan "İlgili kiřinin kendisi tarafından alenileřtirilmiř olması" hkm erevesinde deđerlendirilemeyeceđi sonucuna varıldıđı,

- Veri sorumlusunun, faaliyetleri sonucunda ticari kazanç elde etmeyi amalayan ve sektrdeki diđer tm řirketler gibi faaliyet alanında meřru alıřmalar yrten bir tzel kiřilik olduđu, sz konusu faaliyetlerin yrtlmesi sırasında řirketin var olma amalarından olan polie satıř iřleminin gerekleřtirilmesinin de řirketleri iin meřru bir menfaat olması sebebiyle bu kapsamda gerekleřtirilen kiřisel veri iřleme faaliyetlerinin Kanununun 5 inci maddesinin (2) numaralı fıkrasının (f) bendinde yer alan "İlgili kiřinin temel hak ve zgrlklerine zarar vermemek kaydıyla, veri sorumlusunun meřru menfaatleri iin veri iřlenmesinin zorunlu olması" řartı kapsamında ilgili kiřinin kiřisel verilerinin iřlendiđine iliřkin aıklamaları ile ilgili olarak ise, veri sorumlusu tarafından reklam ve pazarlama amacıyla kiřisel verilerin meřru menfaat kapsamında iřlenmesinin kiřilerin kiřisel verileri zerindeki denetiminin sađlanmasını engelleyeceđi, te yandan polie satıřının gerekleřtirilmesi iin kiřisel veri iřlenmesinin bir zorunluluk olmadıđı ve bařka yollarla da ticari anlamda kazanç sađlanmasının mmkn olduđu, ilgili kiřilerin bu řekilde ilgilendikleri veya ilgilenmedikleri alanlarda reklam ve pazarlama amacıyla aranma ve kısa mesaj almaya maruz bırakılmasının temel hak ve hrriyetlerinin zarar grmesine yol aacađı, sonu olarak salt ekonomik fayda elde etmek amacıyla kiřisel verilerin reklam, pazarlama ve bilgilendirme amacıyla iřlenmesinin Kanununun 5 inci maddesinin (2) numaralı fıkrasının (f) bendinde yer alan "İlgili kiřinin temel hak ve zgrlklerine zarar vermemek kaydıyla, veri sorumlusunun meřru menfaatleri iin veri iřlenmesinin zorunlu olması" hkm erevesinde deđerlendirilemeyeceđi,

- Veri sorumlusu tarafından finansal güvence danışmanlarının müşteri adayları ile iletişime geçmeden önce kontrol etmesi gereken bir “Aranmayacaklar Listesi” oluşturulduğu, kişisel verilerinin silinmesini veya kendisi ile iletişime geçilmemesini talep eden ilgili kişilerin verilerinin işlenmesinin böylelikle engellendiğinin iddia edildiği ancak herhangi bir veri işleme şartına dayanılmaksızın işlenmiş olan kişisel verilerin “Aranmayacaklar Listesi”ne alınmak suretiyle kişisel veri işleme faaliyetine devam edildiği, bu anlamda, reklam ve pazarlama amacıyla gerçekleştirilen aramalardan kişisel verisi hukuka uygun olarak elde edilmiş ilgili kişiler bakımından rızanın/onayın geri çekilmesi durumunda kişisel verilerin bu listeye eklenmesi anlaşılabilir olmakla birlikte, kişisel verileri hukuka aykırı olarak elde edilmiş olan ilgili kişilerin kişisel verilerinin burada işlenmeye devam etmesi hususunun Kanunun 5 inci maddesinde yer alan veri işleme şartlarından herhangi birine dayanılmaksızın gerçekleştirilmesinin hukuka aykırılık barındırdığı, bu çerçevede Kanunun 11 inci maddesinin (e) bendi kapsamında herkesin, veri sorumlusuna başvurarak kendisiyle ilgili; 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme hakkına sahip olduğu hükmü uyarınca ilgili kişinin kişisel verilerinin silinmesi talebinin veri sorumlusu tarafından yerine getirilmediği,

- İlgili kişiye SMS gönderimi yapılan 18.06.2020 tarihinde henüz ticari elektronik ileti gönderiminden önce onay alınmasına ilişkin yürürlüğe giren bir zorunluluk bulunmadığı, içinde bulunulan pandemi süreci nedeniyle ticari elektronik ileti gönderiminden önce onay alınması ve ilgili ret veya onayların tutulmasına ilişkin uygulamanın bir zorunluluk olarak yürürlüğe girişinin birden çok defa ertelendiği, bu doğrultuda ilgili kişiye SMS’lerin iletildiği tarihte ticari elektronik ileti gönderilmesinde onay alınmasına ilişkin mevzuattan kaynaklanan zorunluluk bulunmadığı iddia edilse de ilgili kişilerden onay alınmak suretiyle kişisel verisi niteliğinde olan cep telefonu numarasının işlenmesini mümkün kılan Elektronik Ticaretin Düzenlenmesi Hakkında Kanunun 05.11.2014 tarihinde, söz konusu Kanuna dayanılarak hazırlanan Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmeliğin ise 15.07.2015 tarihinde yürürlüğe girdiği, bu kapsamda şikayete konu ticari elektronik iletinin gönderilmiş olduğu 18.06.2020 tarihinde ticari elektronik ileti gönderilmesine ilişkin onay alınması zorunluluğunun bulunduğu, onaya ilişkin hususlarla ilgili olarak herhangi bir erteleme söz konusu olmadığı, veri sorumlusu tarafından ilgili kişinin onayına istinaden ticari elektronik ileti gönderiminde bulunduğu hususunu kanıtlayıcı herhangi bir bilgi ve belgenin mevcut olmadığı,

- Başvuru Usul ve Esasları Hakkında Tebliğin “Başvuruya Cevap” başlıklı 6 ncı maddesinin (4) numaralı fıkrasında ise cevap yazısının; veri sorumlusu veya temsilcisine ait bilgileri, başvuru

sahibinin; adı ve soyadını, Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarasını, yabancılar için uyruğunu, pasaport numarasını veya varsa kimlik numarasını, tebligata esas yerleşim yeri veya iş yeri adresini, varsa bildirim esas elektronik posta adresini, telefon ve faks numarasını, talep konusunu, veri sorumlusunun başvuruya ilişkin açıklamalarını içermesi zorunluluğunun düzenlenmiş olduğu, ilgili kişinin başvurusuna veri sorumlusu tarafından 23.06.2020 tarihinde e-posta adresi aracılığıyla verilen cevapta Tebliğde yer alan T.C. kimlik numarası, adres gibi unsurların yer almadığı görülmekle birlikte veri sorumlusunda bu bilgilerin bulunmadığı dikkate alındığında bu hususta herhangi bir hukuka aykırılık olmadığı, öte yandan Tebliğde yer alan “başvuruya ilişkin açıklamalar” unsurundan ilgili kişinin taleplerinden ad ve soyadı bilgilerine nasıl ulaşıldığına ilişkin olarak veri sorumlusu tarafından açık ve net bir bilgiye yer verilmediği

değerlendirmelerinden hareketle;

- İlgili kişinin kişisel verisi niteliğindeki telefon numarasının kısa mesaj gönderilmek amacıyla işlendiği iddiası incelendiğinde ilgili kişinin mesleki yetkinliğinden faydalanmak için kendisine ulaşılmaya çalışılmadığı, aksine şirket faaliyetlerine ilişkin randevu talebi ile ilgili kişiye ulaşıldığı değerlendirilmekte olup bu çerçevede ilgili kişinin kişisel verisi niteliğindeki telefon numarasının reklam, pazarlama ve bilgilendirme amacıyla kısa mesaj gönderilmek suretiyle işlenmesinin Kanunun 5 inci maddesinde yer alan herhangi bir işleme şartına dayanmaksızın gerçekleştirildiği dolayısı ile veri sorumlusunun Kanunun 12 nci maddesinde yer verilen veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri alma yükümlülüğüne aykırı davrandığı kanaatine varıldığından veri sorumlusu hakkında Kanunun 18 inci maddesi uyarınca idari para cezası uygulamasına,

- Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğin 6 ncı maddesine uyum konusunda gerekli hassasiyetin gösterilmesi hususunun hatırlatılmasına,

- Kanunun kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini düzenleyen 7 nci maddesi ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğe uygun bir biçimde ilgili kişinin kişisel verilerinin imha edilmesi ve imha edildiğine dair kanıtlayıcı belgeler (log kaydı, vs) ile birlikte bu hususta Kurula en geç otuz gün içinde bilgi verilmesi yönünde veri sorumlusu şirketin talimatlandırılmasına

karar verilmiştir.

2021/572 sayılı KVKK Kararı

İlgili kişinin fotoğrafının öğrencisi olduğu okul tarafından kullanılması hakkında Kişisel Verileri Koruma Kurulunun 09/06/2021 tarihli 2021/572 sayılı Karar Özeti

Karar Tarihi : 09.06.2021

Karar No : 2021/572

Konu Özeti : İlgili kişinin fotoğrafının öğrencisi olduğu okul tarafından kullanılması”

Kuruma intikal eden şikayette, ilgili kişinin öğrenci olarak öğretmenleri ile yaptığı bir görüşmede rızası olmaksızın fotoğrafının çekildiği, çekilen fotoğrafının ticari amaçla okul tarafından bastırılan broşürde kullanıldığı ve kendi internet sitesinde yayınlandığı, ilgili kişi ve velisinin kişisel verilerin işlenmesine, yayımlanmasına veya kullanılmasına zımni veya açık bir rıza vermediği, konuya ilişkin veri sorumlusuna başvuruda bulunulduğu ancak verilen cevabın yetersiz olduğu ifade edilerek, 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) uyarınca veri sorumlusu okul hakkında gerekli işlemlerin tesis edilmesi talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup verilen cevabî yazıda özetle;

- 2018-2019 döneminde öğrencileri olan ilgili kişinin fotoğrafının özel olarak çekilen bir fotoğraf olmadığı, tüm öğrencilerin katılmış olduğu ders ve etkinlikler sırasında çekilen bir fotoğraf olduğu, anılan dönemin sonunda öğrencinin okul değişikliği gerçekleştirdiği, mevcut durumda öğrencileri olmadığı,
- İlgili kişinin velisinden de izin alındığı, bahse konu fotoğrafın aktif olarak kullanımda olmadığı ve yeni bir paylaşım durumunun da olmadığı,
- İlgili kişinin avukatı tarafından gönderilen ihtarnameye istinaden velinin “Sosyal Medya Paylaşımı” konulu yazılı izninin bir örneğinin bulunduğu

ifade edilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 09/06/2021 tarih ve 2021/572 sayılı kararı ile;

- Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanunun 3 üncü maddesinde açık rızanın “belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza” şeklinde tanımlandığı, tanımda yer aldığı üzere, açık rızanın, “Belirli bir konuya ilişkin olması”, “Rızanın bilgilendirmeye dayanması” ve “Özgür iradeyle açıklanması” şeklinde üç unsuru bulunduğu, bu kapsamda, veri işlemek üzere verilen açık rızanın geçerli olması için, açık rızanın öncelikle belirli bir konuya ilişkin ve o konu ile sınırlı olarak verilmesi gerektiği, bu doğrultuda veri sorumlusu tarafından açık rıza beyanının hangi konuya ilişkin olarak istenildiğinin açıkça ortaya konulması gerektiği, bununla birlikte, açık rıza bir irade beyanı olduğundan, kişinin özgür bir şekilde rıza gösterebilmesi için, neye rıza gösterdiğini de bilmesi gerektiği, kişinin sadece konu üzerinde değil, aynı zamanda rızasının sonuçları üzerinde de tam bir bilgi sahibi olması gerektiği, bu sebeple, bilgilendirmenin, veri işleme ile ilgili bütün konularda açık ve anlaşılır bir biçimde gerçekleştirilmesi ve mutlaka verinin işlenmesinden de önce yapılması gerektiği,

- Açık rıza vermenin, kişiye sıkı sıkıya bağlı bir hak olduğundan, verilen açık rızanın geri alınabileceği, bu bağlamda kişisel verilerin geleceğini belirleme hakkı ilgili kişiye ait olduğundan, kişinin dilediği zaman veri sorumlusuna vermiş olduğu açık rızasını geri alabileceği ancak, geri alma işlemi ileriye yönelik sonuç doğuracağından, açık rızaya dayalı olarak gerçekleştirilen tüm faaliyetlerin geri alma beyanının veri sorumlusuna ulaştığı andan itibaren veri sorumlusu tarafından durdurulması gerektiği, başka bir diğer deyişle, geri alma beyanının veri sorumlusuna ulaştığı andan itibaren hüküm doğurduğu,

- 6698 sayılı Kanunun “İlgili Kişinin Hakları” başlıklı 11 inci maddesinde herkesin, veri sorumlusuna başvurarak kendisiyle ilgili; kişisel verilerinin işlenip işlenmediğini öğrenme, kişisel verileri

işlenmişse buna ilişkin bilgi talep etme, kişisel verilerinin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerinin aktarıldığı üçüncü kişileri bilme, kişisel verilerinin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme, 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerinin silinmesini veya yok edilmesini isteme, kişisel verilerinin düzeltilmesi veya silinmesi/yok edilmesi ile ilgili yapılan işlemlerin kişisel verilerinin aktarıldığı üçüncü kişilere bildirilmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme ve kişisel verilerinin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme haklarına sahip olduğunun düzenlendiği,

- Veri sorumlusunun internet sitesinde yapılan incelemede şikayete konu fotoğrafların yer aldığı iddia edilen okul broşürünün halihazırda internet sitesinde erişime açık şekilde “pdf” formatında yer aldığı, şikayet konusu fotoğrafların da anılan broşürün 6 ncı ve 9 uncu sayfalarında yer aldığının görüldüğü,

- Şikayetçi veli tarafından, ilgili kişinin fotoğraflarının veri sorumlusu tarafından açık rızası olmaksızın hukuka aykırı olarak işlendiği iddiası ile ilgili olarak veri sorumlusunun Kurumu muhatap cevap yazıları ve ekleri incelendiğinde; veri sorumlusu tarafından öğrencilerin kişisel verisi olan fotoğraflarının paylaşılacak suretiyle işlenmesine ilişkin “sosyal medya paylaşımı” konulu bir bilgilendirme metninin düzenlendiği, anılan metinde “Okulumuzda yapılacak etkinliklerde öğrencilerimizin fotoğraf ve videoları çekilmektedir. Öğrencilerimizin fotoğraf ve videolarının resmi web sitesinde sosyal medya hesaplarında, okul dergimiz ve okul panolarımızda paylaşılması ile ilgili aşağıdaki izin yazısını doldurarak sınıf/mentor öğretmeninize göndermenizi rica ederim” şeklinde bilgilendirmeye yer verildiği; söz konusu paylaşım izin verilmesine ilişkin olarak öğrenci velilerinden izin alınmasına yönelik bu metnin alt kısmında ayrı bir bölümün düzenlendiği, bu bölümde ise söz konusu sosyal medya paylaşım yazısının okunduğu ve okul bünyesinde yapılacak etkinliklerde çekilen fotoğraf ve videoların kullanılmasına izin verildiği ya da verilmediğine ilişkin iki seçeneğin sunulduğu; somut olayda ise şikayetçi veli tarafından ilgili kişinin fotoğraflarının belirtilen amaçlar kapsamında kullanılmak suretiyle işlenmesine izin verildiğine ilişkin seçeneğin seçildiği ve belgenin ıslak imza ile imzalanarak açık rıza verildiğinin görüldüğü,

- Şikayet dilekçesi ve eklerinden ilgili kişi vekilinin veri sorumlusundan, şikayete konu kişisel verilerinin silinmesini talep ettiği ancak veri sorumlusu tarafından Bahse konu fotoğrafın aktif olarak kullanımda olmadığı ve yeni bir paylaşım durumunun da söz konusu olmadığı hususlarına yer verilmiş olmasına rağmen şikayete konu fotoğrafların muhafaza edilme süresi ile silinmesi veya yok

edilmesine ilişkin herhangi bir bilgiye yer verilmediği, bu kapsamda ilgili kişinin okul ile öğrencilik ilişkisinin 2018-2019 yıllarında mevcut olduğu ve güncel durumda ise okul ile arasında öğrencilik ilişkisinin kalmadığı anlaşıldığından Kanunun 15 inci maddesinin (5) numaralı fıkrası uyarınca, şikayet konusu fotoğraftaki ilgili kişinin görüntüsünün ayrılabilir olup olmadığının veri sorumlusunca ele alınması gerektiği

değerlendirmelerinden hareketle;

- Şikayet konusu fotoğrafların paylaşılmasına yönelik veri işleme faaliyetinin Kanunun 5 inci maddesinin (1) numaralı fıkrasında yer alan ilgili kişinin/velisinin açık rızası hukuki dayanağı çerçevesinde gerçekleştirildiği kanaatine varılmış olup ilgili kişinin fotoğraflarının haksız ve hukuka aykırı olarak ticari amaçla bastırılıp dağıtıldığı ve internet sitesinde paylaşıldığı iddiası hakkında Kanun kapsamında yapılacak bir işlem bulunmadığına,
- Veri sorumlusu tarafından ilgili kişinin talepleri hakkında yeterli açıklamaya yer verilmediği dikkate alındığında veri sorumlusu okulun 6698 sayılı Kanun ve “Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ”in ilgili hükümlerine uyum konusunda gerekli dikkat ve özeni göstermesi gerektiği konusunda talimatlandırılmasına,
- İlgili kişinin okul ile öğrencilik ilişkisinin 2018-2019 yıllarında mevcut olduğu ve güncel durumda ise okul ile arasında öğrencilik ilişkisinin kalmadığı anlaşıldığından Kanunun 15 inci maddesinin (5) numaralı fıkrası uyarınca, şikayet konusu fotoğraftaki ilgili kişinin görüntüsünün ayrılabilir olup olmadığının veri sorumlusunca değerlendirilerek buzlanması ya da imha edilmesi ve sonucundan Kurula bilgi verilmesi yönünde veri sorumlusunun talimatlandırılmasına,
- Veri sorumlusuna tebliğ edilmesinden sonra geçerli olmak üzere, veri sorumlusu tarafından okul bünyesinde çekilen fotoğraf ve videoların çeşitli mecralarda paylaşılmasına ilişkin daha önce hazırlanmış olan aydınlatma ve açık rıza metinlerinin Kanunun 3 üncü maddesinde yer alan unsurlar ve Aydınlatma Tebliğinde yer verilen hükümler dikkate alınmak ve bu yönde alınacak açık rızanın okulu tanıtıcı basılı yayınlarda/broşürlerde, web sitesinde veya sosyal medya hesaplarında paylaşılmasına yönelik her bir işleme faaliyeti özelinde ilgili kişilere ayrı ayrı seçenek sunulmak suretiyle revize edilmesi gerektiği yönünde veri sorumlusunun bilgilendirilmesine

karar verilmiştir.

2021/548 sayılı KVKK Kararı

İlgili kişinin cep telefonu numarasının kampanya adı altında bir dijital platform bayisi tarafından edinilmesi, işlenmesi ve rızası olmaksızın arama yapılması hakkında Kişisel Verileri Koruma Kurulunun 04/06/2021 tarih ve 2021/548 sayılı Karar Özeti

Karar Tarihi : 04.06.2021

Karar No : 2021/548

Konu Özeti : İlgili kişinin cep telefonu numarasının kampanya adı altında bir dijital platform bayisi tarafından edinilmesi, işlenmesi ve rızası olmaksızın arama yapılması

İlgili kişiden alınan şikâyet dilekçesinde özetle;

- Şikâyet olunan dijital platform ile hiçbir ilişkisinin olmamasına karşın ilgili kişinin sürekli olarak 0850'li bir çağrı merkezinden arandığı ve tarafına, bu platforma üye olması yönünde pazarlama yapılmaya çalışıldığı,
- Bunun üzerine ilgili kişinin reklamı yapılan dijital platformun internet adresinde bulunan irtibat formu vasıtasıyla başvuruda bulunduğu, kendisine e-posta ile verilen yanıtta ise ilgili kişinin müşteri olarak herhangi bir kaydının şirket nezdinde bulunmadığı yanıtını aldığı ancak kendisinin kişisel verilerinin nasıl elde edildiği ve nerelerde kullanıldığına ilişkin sorularına herhangi bir yanıt verilmediği,
- Dolayısıyla işlenen suçun kabul edildiği ancak detay içermeyen bir cevap ile geçiştirilmeye çalışıldığı

hususları beyan edilerek konunun incelenmesi, şirketin ilgili kişinin kişisel verilerini nasıl elde ettiği hususunda kendisine bilgi vermesi konusunda talimatlandırılması ve gerekli cezai yaptırımın uygulanması talep edilmiştir.

Konuya ilişkin olarak başlatılan inceleme neticesinde, reklamı yapılan dijital platformdan bilgi ve belge talep edilmiş olup Kuruma ulaştırılan cevabî yazıda;

- İlgili kişinin hiçbir şekilde şirketin müşterisi olmadığı, şirket ile bir ilgisinin tespit edilemediği,

- Şikâyet edilen numaranın dijital platformun çağrı merkezi numarasının olmadığı, yapılan araştırmada ilgili kişiyi aradığı iddia edilen numaranın 21.12.2018 tarihinden 12.09.2019 tarihine kadar “..... Expert” unvanı ile faaliyet gösteren bir bayiye tahsis edildiği,

- İlgili kişinin adının sistemlerde hiçbir şekilde kayıtlı olmadığı, diğer bir ifade ile ilgili kişinin potansiyel bir müşteri olarak kayıtlı olmayıp herhangi bir elektronik ticari ileti izninin de bulunmadığı, bu sebeple ilgili kişinin kişisel verilerinin nereden ve ne şekilde temin edildiğinin bilinmediği,

Şayet bayii bu şekilde bir arama gerçekleştirmiş ise bunun kendilerinin bilgisi ve izni dâhilinde yapılmadığı

beyanlarına yer verildiği görülmüştür.

Bunun üzerine bahse konu dijital platformdan, ilgili kişiyi aradığı iddia olunan bayii ile şirketleri arasındaki iş ilişkisini tanımlayan bilgi ve belgelerin Kuruma iletilmesi talep edilmiş olup söz konusu talebe istinaden Kuruma iletilen cevap yazısında ise;

- Bayilik hizmeti kapsamında “...Expert” olarak görev yürüten bayiye ürün ve hizmetlerin pazarlanması, tanıtılması, satışı, söz konusu ürün ve hizmetlerle ilgili abonelik tesisi, abonelik uzatma, abonelik iptali, üst paketlere geçiş, satış sonrası hizmetler, tahsilat ve gerektiğinde kurulum ve montaj destek hizmetleri verilmesi ile sınırlı olmamak kaydıyla dijital platform tarafından bildirilecek diğer iş ve işlemler konusunda görev ve yetki tevdi edildiği,

- Bayii ile akdedilen abonelik sözleşmesi ve bu bayiliğin iptaline ilişkin e-posta çıktısının yazılarına eklendiği,

- Bayii tarafından kullanılan herhangi bir sistemin dijital platform tarafından kurulmayıp bayilerin kural olarak bayilik sözleşmesi ile görev ve yetkiler kapsamında kendisine sağlanan kullanıcı adı ve şifre bilgileri ile dijital platformun CRM Sistemine erişerek potansiyel müşteri oluşturabildiği,

- İlgili kişi ile ilgili olarak herhangi bir kayda rastlanılmadığı için kişisel verilerinin ne şekilde elde edildiği ve benzeri soruların cevaplandırılmasının mümkün olmayacağı

ifade edilmiştir.

Yukarıda yer verilen bilgi ve belgelerin değerlendirmesi neticesinde alınan 04/06/2021 tarih ve 2021/548 sayılı Kurul Kararında özetle;

- 6698 sayılı Kişisel Verilerin Korunması Kanununun 3 üncü maddesinde “ilgili kişi”nin, kişisel verisi işlenen gerçek kişi; “veri sorumlusu”nun, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen,

veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi; ve “veri işleyen”in ise veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi olarak tanımlandığı,

- Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- 6698 sayılı Kanunda veri işleyen; veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi olarak tanımlandığı, buna göre veri işleyen, veri sorumlusu adına, ondan aldığı yetki ve talimata göre kişisel veri işlemekte olduğu, bu minvalde “veri işleyen” sıfatının kazanılabilmesi için veri işleyen, veri sorumlusunun idarî yapısından ayrı bir hukukî varlığının olması; bir başka diğer deyişle, veri sorumlusunun birimleri içerisinde bulunmaması gerekmektedir birlikte veri işleyen, veri sorumlusundan ayrı bir hukuk kişisi olarak veri sorumlusunun talimatı, denetimi ve yetkilendirmesi dâhilinde kişisel veri işleme faaliyeti yürüteceği,

- Her ne kadar bayii ile dijital platform arasında akdedilen sözleşme hükümlerinden genel şekliyle dijital platformun veri sorumlusu, bayinin ise veri işleyen olarak belirlendiği görülmekte ise de somut hadisede bayinin veri işleyen sıfatından çıkarak veri sorumlusu hâline geldiği, zira dijital platformun merkezî CRM sisteminde müşteri/potansiyel müşteri olarak kaydı bulunmayan ilgili kişiyi dijital platformun talimatı veya bilgisi dâhilinde olmaksızın aradığının anlaşıldığı, bu telefon numarası bayiye dijital platform tarafından iletilmediğinden, bayinin veri işleyen olarak, veri sorumlusunun denetimi ve kontrolü altında kişisel veri işleme faaliyeti yürüttüğünden bahsedilemeyeceği,

- Somut olayda bayinin, kendi iradesiyle ve dijital platformdan bağımsız bir şekilde ilgili kişinin açık rızası veya Kanunun 5 inci maddesinin (2) numaralı fıkrasında yer verilen işleme şartlarına

dayanmaksızın ilgili kişinin kişisel verisi niteliğindeki telefon numarasını aramak suretiyle kişisel veri işleme faaliyetinde bulunmasından ötürü veri sorumlusu sıfatını haiz olduğu

değerlendirmelerinden hareketle;

- İlgili kişinin kişisel verisi olan telefon numarasının Kanunun 5 inci maddesinde yer alan herhangi bir işleme şartına dayanmaksızın hukuka aykırı elde edildiği ve işlendiği dikkate alındığında Kanunun 12 nci maddesinin (1) numaralı fıkrasında yer alan teknik ve idari tedbirleri almayan veri sorumlusu bayii hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında idarî para cezası uygulanmasına

karar verilmiştir.

2021/545 sayılı KVKK Kararı

Veri sorumlusu tarafından ilgili kişinin cep telefonu numarasına reklam amaçlı SMS gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 04/06/2021 tarihli 2021/545 sayılı Karar Özeti

Karar Tarihi : 04.06.2021

Karar No : 2021/545

Konu Özeti : Veri sorumlusu tarafından ilgili kişinin cep telefonu numarasına reklam amaçlı SMS gönderilmesi”

Kuruma intikal eden şikâyetle özetle, veri sorumlusu sıfatını haiz Hastane tarafından ilgili kişinin telefonuna reklam ve pazarlama amaçlı SMS gönderildiği, bununla birlikte ilgili kişi tarafından veri sorumlusuna kişisel verilerin işlenmesi konusunda açık rıza verilmediği ifade edilerek veri sorumlusu hakkında 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup verilen cevabî yazıda özetle;

- Söz konusu şikâyetçinin hastanede herhangi bir kaydı olmadığı, dolayısıyla tedavi kaydı bulunmayan kişinin kişisel verilerinin kaydedilmesinin de mümkün olamayacağı,
 - Şikâyetçi tarafından konuya ilişkin herhangi bir başvuru yapılmadığı,
 - Hastanede kaydı bulunan hastalara gönderilen SMS’lerin reklam yapmak amacı taşımadığı, gönderilen SMS’lerin asıl amacının Covid-19 sürecinde vatandaşlar için bilgilendirme amacı taşıdığı,
 - Gönderilen SMS’lerin iptali için ücretsiz gönderme seçeneği bulunduğu, iptal seçeneği kullanmayan kişilerin mesajların devamının zımnen kabul etmiş olduğu
- ifade edilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 04/06/2021 tarih ve 2021/545 sayılı kararı ile;

- Kanunun “Kişisel verilerin işlenme şartları” başlıklı 5 inci maddesinde;

“(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.” hükmüne yer verildiği,

- Veri sorumlusunun iddialarında yer verilen SMS içeriklerinin ilgili kişiye gönderilen SMS içerikleri ile uyduğu ve mesajda belirtilen MERSİS numarasının veri sorumlusuna ait olduğu,

- Veri sorumlusunun kendisine herhangi bir başvuru yapılmadığı iddiasına ilişkin şikâyetçi vekili tarafından veri sorumlusuna ihtarname gönderildiği ve ilgili barkod numaralı ihtarnamenin teslim alındığının anlaşıldığı

değerlendirmelerinden hareketle;

- Veri sorumlusunun, ilgili kişinin kişisel verisi niteliğindeki telefon numarasına Kanunun 5 inci maddesinde sayılan şartlardan birine dayanmaksızın SMS göndermesi suretiyle gerçekleşen kişisel veri işleme faaliyeti nedeniyle Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendi kapsamında kişisel verilerin hukuka aykırı olarak işlenmesi önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri alma yükümlülüğünü yerine getirmediği dikkate alındığında, Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca veri sorumlusu hakkında idari para cezası uygulanmasına,

- Veri sorumlusunun ilgili kişinin başvurusuna cevap vermediği dikkate alındığında Kanun kapsamında yapılan başvurulara cevap vermek konusunda gerekli dikkat ve özenin gösterilmesi hususunda veri sorumlusunun talimatlandırılmasına,

- Hukuka aykırı işlendiđi deęerlendirilen Őikâyete konu kiŐisel verinin imha edilmesi ve sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına karar verilmiŐtir.

2021/511-512-513 sayılı KVKK Kararı

Avukatların icra takip dosyalarındaki kişisel verilere vekâletname olmaksızın hukuka aykırı olarak erişim sağladığına ve Adalet Bakanlığı tarafından icra tevzi bürolarında görevli personel eliyle alacaklı vekili avukatlara borçluların alacaklı olduğu icra takip dosyalarında bulunan kişisel verilerin hukuka aykırı olarak aktarılmasına ilişkin ihbarlar hakkında Kişisel Verileri Koruma Kurulunun 20/05/2021 tarihli ve 2021/511-512-513 sayılı Karar Özeti

Karar Tarihi : 20.05.2021

Karar No : 2021/511-512-513

Konu Özeti : Avukatların icra takip dosyalarındaki kişisel verilere vekâletname olmaksızın hukuka aykırı olarak erişim sağlaması ve Adalet Bakanlığı tarafından icra tevzi bürolarında görevli personel eliyle alacaklı vekili avukatlara borçluların alacaklı olduğu icra takip dosyalarında bulunan kişisel verilerin hukuka aykırı olarak aktarılması.

Adalet Bakanlığı ve bir avukat hakkında Kuruma intikal ettirilen ihbarlarda özetle; alacaklı vekili avukatların, icra tevzi bürolarına başvuruda bulunup borçluların alacaklı olduğu icra takip dosyalarının bilgilerini haksız bir şekilde elde ettiği, ayrıca avukatların bu sayede, icra dairesinde diledikleri dosyaları da inceleyebildiği, her ne kadar avukatın dosyanın bir örneğini alması vekâlet sunmasına bağlı olsa da kişisel verilere yetkisiz kişilerin erişiminin engellenmesinin veri sorumlularına verilen görevlerden biri olduğu ve avukatlar ya da görevlendirdikleri kişiler tarafından, icra tevzi bürosu yetkilileri ve memurları aracılığıyla; borçluların alacaklı olduğu icra takip dosyalarında bulunan kişisel verilerin hukuka aykırı olarak ele geçirilmesi ile avukatların icra dairelerindeki diledikleri dosyaları vekâletname olmaksızın incelemelerinin 6698 sayılı Kişisel Verilerin Korunması Kanununa aykırılık teşkil ettiği belirtilerek; bu kapsamda icra tevzi bürosu çalışanları tarafından yapılan aktarımların ve avukatlar tarafından vekâletname olmaksızın icra takip dosyalarındaki kişisel verilere erişimin 6698 sayılı Kanuna aykırı olduğunun tespit edilmesi, bu durumun düzeltilmesi için Adalet Bakanlığı nezdinde ivedilikle girişimlerde bulunulması ve gerekli idari yaptırımların uygulanması talep edilmiştir. Yapılan ihbarlara binaen Kişisel Verileri Koruma Kurulu tarafından resen inceleme başlatılmasına karar verilmiştir.

Başlatılan inceleme çerçevesinde veri sorumlusu Adalet Bakanlığında konuya ilişkin bilgi ve belge talep edilmiş olup, alınan cevabi yazıda özetle;

- İlgili mevzuat ve içtihat çerçevesinde, alacağını tahsil etmek isteyen alacaklı veya vekilinin takibin kesinleşmesini müteakip borçlunun alacaklı olduğu dosyalar da dâhil olmak üzere borçlunun her türlü mal varlığını, hak ve alacağını sorgulama hakkının 2004 sayılı İcra ve İflas Kanunundan kaynaklandığının anlaşıldığı;
- Ayrıca avukatın veya stajyerlerinin dava takip dosyalarını vekâletname olmaksızın inceleme isteğinin ilgililerce yerine getirilmesinin 1136 sayılı Avukatlık Kanununda düzenlendiği; bu kapsamda avukatların ve stajyerlerinin alacağın tahsilini teminen borçlunun alacaklı olduğu dosyaları sorgulama ve kendilerine tanınan dosya inceleme hakkını icra dairelerinde tespit amacıyla bu işle görevlendirilen icra tevzi büroları vasıtası ile yapmasının uygun olacağı, icra dairesinde görevli personelin de vekâletname ibraz etmeksizin dosya incelemek isteyen avukat ve stajyerlerine bu isteklerini yerine getirmelerinin fotokopi ve benzeri yollarla örnek almamaları kaydı ile zorunlu olduğunun değerlendirildiği;
- Bu itibarla avukat veya stajyerlerinin müvekkillerinin alacağına kavuşmasını sağlamak için borçluların alacaklı olduğu dosyaları tespit etmesi ve tespit ettiği dosyaları incelemesi hususunun kanunlarda açıkça öngörülmesi ve yukarıda izah edilen nedenlerle 6698 sayılı Kanuna aykırılık kapsamında bulunmayacağı değerlendirildiği

ifade edilmiştir.

Yine, başlatılan inceleme çerçevesinde veri sorumlusu avukattan savunması istenilmiş olup, alınan cevabi yazıda özetle; Avukatlık Kanununun 46 ncı maddesinin 2 inci fıkrasında yer alan “*Avukat veya stajyer, vekaletname olmaksızın dava ve takip dosyalarını inceleyebilir. Bu inceleme isteğinin ilgililerce yerine getirilmesi zorunludur.*” hükmü sınırları kapsamında borçlunun alacaklı olduğu dosyaların tespit edildiği, bu dosyalara borçlunun alacaklı olduğu icra dosyalarından talepte bulunmak ve ilgili icra müdüründen karar aldırarak suretiyle haciz işlemi yapıldığı; bunun göreviyle ilgili bir iş olduğu; bu işlemlerin yapılmaması halinde işini gereği gibi yapmadığı için müvekkiline karşı sorumluluğun dahi gündeme geleceği ve bu kapsamda tüm işlemlerin yasalar çerçevesinde yürütüldüğü ifade edilmiştir.

İhbar başvuruları ile veri sorumlularından alınan bilgi ve belgelerin ilgili mevzuat çerçevesinde incelenmesi neticesinde Kurulun 20/05/2021 tarihli ve 2021/511-512-513 sayılı Kararları ile

- 2004 sayılı İcra ve İflas Kanununun “Taşınır ve taşınmaz malların haczi” başlıklı 85 inci maddesinin birinci fıkrasının “*Borçlunun kendi yedinde veya üçüncü şahısta olan taşınır mallarıyla taşınmazlarından ve*

alacak ve haklarından alacaklının ana, faiz ve masraflar da dahil olmak üzere bütün alacaklarına yetecek miktarı haczolunur. ” hükmünü amir olduğu; hükümde haciz yoluyla takip kapsamında borçlunun taşınır ve taşınmaz malları ile alacak ve haklarına haciz konulabileceğinin öngörüldüğü ve bu kapsamda, borçlunun alacaklı olduğu icra dosyalarına konu alacaklara da haciz konulmasının mümkün olduğu;

• Diğer taraftan, 1136 sayılı Avukatlık Kanununun 46 ncı maddesinin,

“İşlerin stajiyer veya sekreterle takibi, dava dosyalarının incelenmesi ve dosyadan örnek alma:

Madde 46 - (Değişik : 2/5/2001 - 4667/32 md.)

Avukat, işlerini kendi sorumluluğu altındaki stajyeri veya yanında çalışan sekreteri eliyle de takip ettirebilir, fotokopi veya benzeri yollarla örnek alabilir. Avukatın onanmasını istemediği örnekler harca tabi değildir.

Avukat veya stajyer, vekaletname olmaksızın dava ve takip dosyalarını inceleyebilir. Bu inceleme isteğinin ilgililerce yerine getirilmesi zorunludur. Vekaletname ibraz etmeyen avukata dosyadaki kağıt veya belgelerin örneği veya fotokopisi verilmez.” hükmünü,

2 nci maddesinin üçüncü fıkrasının ise,

“Avukatlığın amacı:

Madde 2 - (Değişik birinci fıkra : 2/5/2001 - 4667/2 md.) ...

(Değişik üçüncü fıkra: 2/5/2001 - 4667/2 md.) Yargı organları, emniyet makamları, diğer kamu kurum ve kuruluşları ile kamu iktisadi teşebbüsleri, özel ve kamuya ait bankalar, noterler, sigorta şirketleri ve vakıflar avukatlara görevlerinin yerine getirilmesinde yardımcı olmak zorundadır. Kanunlarındaki özel hükümler saklı kalmak kaydıyla, bu kurumlar avukatın gerek duyduğu bilgi ve belgeleri incelemesine sunmakla yükümlüdür. Bu belgelerden örnek alınması vekaletname ibrazına bağlıdır. Derdest davalarda müzekkereler duruşma günü beklenmeksizin mahkemeden alınabilir.” hükmünü amir olduğu;

Anılan hükümlerden avukatların vekâletname sunmasına gerek olmaksızın icra takip dosyalarını inceleyebileceğinin ve ilgili makamların da avukatlara bu konuda gerekli imkanları sağlamakla yükümlü kılındığının anlaşıldığı;

Bununla birlikte, 2004 sayılı İcra ve İflas Kanununun 8/a maddesinin altıncı fıkrası ile 22.07.2020 tarihli ve 7251 sayılı Kanunla değişik 78 nci maddesinin birinci fıkrasının;

“Elektronik işlemler:

Madde 8/a - (Ek: 2/7/2012-6352/3 md.)

...

(Ek fıkra:6/12/2018-7155/10 md.) Alacaklı, Ulusal Yargı Ağı Bilişim Sistemi üzerinden bu sisteme entegre bilişim sistemleri vasıtasıyla dosya safahat bilgileri ile borçlunun mal, hak veya alacağını elli kuruluş karşılığında sorgulayabilir. Bu miktar her yıl, bir önceki yıla ilişkin olarak 4/1/1961 tarihli ve 213 sayılı Vergi Usul Kanununun mükerrer 298 inci maddesi hükümleri uyarınca tespit ve ilan edilen yeniden değerlendirme oranında artırılır. Adalet Bakanlığı yeniden değerlendirme oranında artırılan ücreti beş katına kadar artırmaya ve azaltmaya ayrıca gün ve dosya esaslı olmak üzere belirli sayıdaki sorgulamayı ücretten istisna tutmaya yetkilidir. Genel yönetim kapsamındaki kamu idarelerinden bu ücret alınmayacağı gibi alacaklının bir gün içinde aynı dosya üzerinden beş kez yapacağı sorgudan da ücret alınmaz. Bu kapsamda alınacak ücret Adalet Bakanlığının belirleyeceği usule göre tahsil edilir ve takip gideri olarak borçluya yüklenemez.

...

II. HACİZ

Haciz:

1 - Talep Müddeti

Madde 78 - (Değişik: 3/7/1940-3890/1 md.)

(Değişik birinci fıkra:22/7/2020-7251/49 md.) Ödeme emrindeki müddet geçtikten ve borçlu itiraz etmiş ise itirazı kaldırıldıktan sonra mal beyanını beklemeksizin alacaklı, haciz konmasını isteyebilir. Ancak, alacaklı dilerse haciz talebinde bulunmaksızın Ulusal Yargı Ağı Bilişim Sistemi üzerinden, bu sisteme entegre bilişim sistemleri vasıtasıyla borçlunun mal, hak veya alacağını sorgulayabilir. Sorgulama sonunda Ulusal Yargı Ağı Bilişim Sistemi, varsa borçlunun mal, hak veya alacağının mahiyeti ve detayı hakkında bilgi verir ve bu durumda sistem üzerinden de haciz talep edilebilir. Bu takdirde icra dairesi, tespit edilen mal, hak veya alacağı elektronik ortamda haczeder. Sorgulama sonunda edinilen bilgiler hukuka aykırı olarak paylaşılamaz. Sorgulama ve haciz işlemlerinin yürütülebilmesi için kamu kurum veya kuruluşları ile 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununun 3 üncü maddesinde tanımlanan kredi kuruluşları ve finansal kuruluşlar, Ulusal Yargı Ağı Bilişim Sistemi ile kendi sistemleri arasında entegrasyonu sağlar. Sorgulamanın tür, kapsam ve sınırı ile diğer hususlar Adalet Bakanlığınca yürürlüğe konulan yönetmelikle belirlenir.""

şeklinde olduğu;

- Söz konusu hükümler uyarınca alacaklı vekili avukatların, Ulusal Yargı Ağı Bilişim Sistemi üzerinden borçlunun alacaklı olduğu icra dosyaları dahil olmak üzere mal, hak veya alacağı hakkında sorgulama yapabileceği;

değerlendirmelerinden hareketle;

• 2004 sayılı İcra ve İflas Kanununun 85 inci maddesi çerçevesinde borçlunun kendi veya üçüncü kişi nezdindeki alacaklarına haciz konulabileceği, 2004 sayılı Kanunun 8/a ve 78 nci maddeleri uyarınca Ulusal Yargı Ağı Bilişim Sistemi vasıtasıyla alacaklı tarafından borçluların mal, hak veya alacaklarının sorgulanabileceği, avukatların müvekkillerinin alacağını tahsil etmek amacıyla 1136 sayılı Avukatlık Kanununun 46 ncı maddesi uyarınca dava ve icra takibi dosyalarını vekâletname sunmaksızın inceleyebileceği ve bu kapsamda 6698 sayılı Kanunun 5 inci maddesinin ikinci fıkrasının (a) bendinde düzenlenmiş işleminin “kanunlarda açıkça öngörülmesi” şartına dayanılarak alacaklı vekili avukatlar tarafından borçlunun alacaklı olduğu icra dosyalarına ilişkin olarak kişisel veri işleme faaliyeti yürütebileceğinden avukatların vekâletname olmaksızın icra takip dosyalarındaki kişisel verilere hukuka aykırı olarak erişim sağladığı iddiası bakımından 6698 sayılı Kanun kapsamında yapılacak bir işlem bulunmadığına,

• 1136 sayılı Avukatlık Kanununun 2 nci maddesinde ilgili makamların avukatların görevlerini yapmak üzere ihtiyaç duyduğu bilgi ve belgeleri avukatların incelemesine sunmakla yükümlü olduğunun düzenleme altına alındığı ve bu kapsamda 6698 sayılı Kanunun 8 inci maddesinin üçüncü fıkrasında düzenlenmiş “Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.” düzenlemesi uyarınca Adalet Bakanlığı tarafından icra tevzi bürosunda görevli personel eliyle borçlunun alacaklı olduğu icra dosyaları hakkında bilgi ve belge sağlama amacıyla avukatlara görevlerini yerine getirebilmeleri için kişisel veri aktarımı yapılabileceğinden Adalet Bakanlığı tarafından alacaklı vekili avukatlara borçluların alacaklı olduğu icra takip dosyalarında bulunan kişisel verilerin hukuka aykırı olarak aktarılması iddiası bakımından 6698 sayılı Kanun kapsamında yapılacak bir işlem bulunmadığına

karar verilmiştir.

2021/424 sayılı KVKK Kararı

Bir bankanın, varlık yönetim şirketinin ve üç farklı avukatın borçlu olmayan ilgili kişinin kişisel verisini işleyerek icra takibi başlattıkları iddiası hakkında Kişisel Verileri Koruma Kurulunun 27/04/2021 tarihli ve 2021/424 sayılı Karar Özeti

Karar Tarihi : 27.04.2021

Karar No : 2021/424

Konu Özeti : Bir bankanın, varlık yönetim şirketinin ve üç farklı avukatın borçlu olmayan ilgili kişinin kişisel verisini işleyerek icra takibi başlattıkları iddiası

Kurumumuza intikal eden şikâyet dilekçesinde;

- İlgili kişiye yönelik olarak yetkili icra dairesi tarafından icra takibi başlatıldığı, ilgili kişinin bu durumu 2017 yılı Şubat ayında ev kredisi çekmek isterken öğrendiği, 2010 yılında ilgili kişinin evine gelen bir saha müfettişinin, ilgili Bankaya borçlu olduğunu ve bunu ödemesi gerektiğini söylediği,
- İlgili kişinin bu şahsa, kendisinin Bankaya hiçbir şekilde gitmediğini ve bahse konu Bankada bir hesabının da bulunmadığını söylediği, adresini ne şekilde öğrendiğini sorduğunda “biz buluruz” cevabını aldığı,
- İlgili kişinin Banka şubesi ile görüştüğü, şube personelinin ilgili kişiye ait kimlik fotokopisini alarak merkeze faks çektiği ve ilgili kişiye, Bankaya borçlu olan şahsın kendisi değil, bir erkek olduğunu söyledikleri fakat aradan geçen yıllar içerisinde Varlık Yönetimi Şirketi tarafından ilgili kişinin sürekli olarak arandığı ve ilgili kişinin o kişinin kendisi olmadığı bilgisini Varlık Yönetim Şirketine ilemesine karşın bu aramaların sürdürüldüğü,
- Söz konusu icra dosyasında gerçek borçluya ilişkin tüm bilgilerin bulunmasına karşın ilgili kişinin kimlik numarasını kullanarak Bankanın, Varlık Yönetim Şirketinin ve üç farklı avukatın borçlu olmayan ilgili kişiye icra takibi başlattıkları,
- İlgili kişinin konu hakkında BİMER’e bulunduğu şikâyet üzerine açılan soruşturma dosyasına Banka şubesinin verdiği cevapta ilgili kişinin 21.02.2017 tarihinde şubeye başvurması sonucu gerekli güncellemelerin yapılarak T.C. kimlik numarasının sistemden silindiği ve kredi kayıt bürosu (KKB)

kayıtlarının düzeltildiği, takip hesabının devir yapıldığı Varlık Yönetimi Şirketine ayrıca bilgilendirmenin yapıldığının belirtildiği,

- Varlık Yönetim Şirketinin söz konusu borcu ilgili kişinin T.C. kimlik numarası üzerinden kaldırmadığı, Banka tarafından düzeltilmediği iddia edilen KKB kayıtlarının düzeltilmediği, ilgili kişinin bu hususta aldığı TBB Risk Merkezi Raporunun bunu doğruladığı, BİMER vasıtasıyla alınan Banka yanıtının Varlık Yönetimi Şirketine faks yoluyla bildirilmesine karşın aramaların devam etmekte olduğu,

- Veri sorumlusu Banka, Varlık Yönetimi Şirketi ve avukatların ilgili kişinin T.C. kimlik numarasını nasıl ve nereden edindiğinin meçhul olduğu, bu bilgilerin üçüncü şahıslara verilerek ilgili kişinin mağdur edildiği, kara listeye alındığı ve dosya bilgilerinin incelenmeksizin ilgili kişiye icra takibi yapmakta ısrar edildiği

hususları ifade edilerek anılan taraflar hakkında 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme neticesinde Bankanın, Varlık Yönetim Şirketinin ve avukatların savunması istenilmiş olup, Bankadan alınan cevabi yazıda özetle;

- İlgili kişi ile Banka arasındaki müşteri ilişkisinin 23.06.2003 tarihinde kurulduğu ve kredinin 28.11.2007 tarihinde bankanın kanuni takip hesaplarına intikal ettiği, ödeme yapılmaması üzerine 09.02.2008 tarihinde yetkili İcra Müdürlüğünün dosyası ile kredili müşteri aleyhine icra takibi başlatıldığı, takip süreci içerisinde herhangi bir tahsilat sağlanamadığından kredi riskinin 05.01.2010 tarihinde Varlık Yönetim Şirketine temlik edildiği,

- 21.02.2017 tarihinde Bankanın ilgili şubesine şikayetçi tarafından başvuru yapılarak borçlu olarak görünen kişi ile isim benzerliği olduğunu ve hatanın düzeltilmesini talep ettiği, bunun üzerine yapılan kontrollerde, ilgili kişiye ait T.C. kimlik numarasının, borçlu adına tanımlı olduğunun ve ilgili kişi ile borçlunun Banka sistemlerinde sadece T.C. kimlik numarasının aynı olup diğer tüm verilerinin ise farklı olduğunun tespit edildiği, böylelikle takip borçlusu için 23.06.2003 tarihinde müşteri kaydı oluşturulduğu sırada T.C. kimlik numarası olarak sehven ilgili kişiye ait T.C. kimlik numarasının kaydedildiğinin anlaşıldığı,

- Veri sorumlusu Bankaya şikâyetin ulaştığı 21.02.2017 tarihinde derhal ilgili kişinin T.C. kimlik numarasının, borçlunun müşteri bilgileri altından silinmesinin sağlandığı, ayrıca Kredi Referans Sistemi (KRS) ekranlarında yapılan kontrollerde 5 yıl geçtiği için kayıtların da silindiğinin görüldüğü, Bankaca yapılan tespit üzerine, dosyanın temlik edildiği yeni alacaklı Varlık Yönetim Şirketine

bilgilendirme yapılarak borçlunun telefon numarası verisinin güncel ve doğru olmasına ilişkin sorumluluğunu yerine getirildiği,

- Yapılan incelemede ilgili kişinin 30.10.2019 tarihinde Bankaya ilettiği başvurusuna 12.11.2019 tarihinde yanıt verildiği ancak bu cevabın sehven farklı uzantılı bir e-posta adresi üzerinden iletmeye çalışıldığı fakat KEP uzantılı e-posta hesaplarına ancak KEP uzantılı e-postalar aracılığı ile gönderim yapılabildiğinden bahse konu cevabın ilgili kişiye ulaşmadığı

hususları ifade edilmiştir.

Veri sorumlusu Varlık Yönetim Şirketinden alınan cevabi yazıda özetle;

- Sözleşme kapsamında şirketin yeni alacaklısı konumunda olduğu kredi borcu bakımından alacağın takibine ve tahsiline yönelik hukuki işlemlerin temlik sözleşmesinin imzalanmasından önceki dönemde Banka tarafından başlatılmış olduğu ve borçlu taraf olarak ilgili kişi ile arasında isim benzerliği bulunan üçüncü kişinin gösterilmesi gerekirken ilgili kişinin borçlu taraf olarak gösterildiği,

- İcra Müdürlüğü dosyasında mevcut bulunduğu belirtilen müzekkerede borçluya ait kimlik bilgilerinin yer almasına karşın, borçlunun adresinin tespiti için 2009 yılında SSK Tahsisler Daire Başkanlığına yazılan yazıda, veri sorumlusu Banka tarafından ilgili kişiye ait olan T.C. kimlik numarasına yer verildiği, bu işlemlerin hepsinin Banka ile Şirketleri arasında akdedilen sözleşmenin imzasından önce gerçekleştirildiği,

- İlgili kişinin Haziran 2019 tarihine kadar Şirketlerine herhangi bir başvuruda bulunmadığı, bu tarihte iletilen şikâyet üzerine ivedilikle veri sorumlusu Banka ile iletişime geçerek bilgi talebinde bulunduğu, bunu müteakip veri sorumlusu Bankadan yapılan, ilgili kişinin T.C. kimlik numarasının sehven borçluya ait MBB numarasının üzerine kaydedildiği bilgilendirmesi üzerine veri sorumlusu şirket tarafından ilgili kişiye, dosyadan taraf kaydının ve T.C. kimlik numarasının silindiğine dair bilgilendirmede bulunulduğu, Banka tarafından iletilen bilgiler doğrultusunda ilgili kişinin kişisel verilerinin tahsilat sisteminden silindiği ve 29.07.2019 tarihinde TBB Risk Merkezi'nde ilgili kişinin kendilerine borçlu olmadığına dair güncelleme gerçekleştirildiği,

- Bu konulara ilişkin bilgilendirmenin ilgili kişiye noter ihtarnamesi vasıtasıyla yapıldığı, tahsilat sistemleri ve TBB Risk Merkezi bilgilerinde yapılan sorgular sonucunda ilgili kişiye ait bilgilerin sonuçlar arasında gösterilmediği ve "veri bulunamadı" sonucu alındığının doğrulandığı ve bu hususta ilgili kişiye bilgi verildiği,

• İlgili kişiye ait kişisel verilerin arşiv kayıtlarının saklanması hukukî mesnedinin ileride doğabilecek uyuşmazlıklarda delil teşkil etmesi bakımından ilgili mahkeme veya yetkili kurum ve kuruluşlara ibraz edilmesi amacıyla sınırlı olarak, Kanunun 5 inci maddesinin (2) numaralı fıkrasının (e) bendinde yer verilen kişisel verilerin işlenmesinin bir hakkın tesisi, kullanılması veya korunması için zorunlu olması hükmü olduğu

ifade edilmiştir.

İlk avukattan alınan yazıda özetle;

- Kendisinin 13 yıl kadar önce, 2007-2008 yılları içinde çok kısa bir dönem ilgili Bankanın vekillik görevini icra ettiği ve 2008 yılı içinde vekillik görevinden ayrılarak tarafınca açılan tüm dosyaları bankaya devir ve teslim ettiği, bu tarihten sonra bu dosyalarla ilgili hiçbir işlemin tarafı olmadığı,
- Söz konusu dönemde kendisi tarafından açılan icra takiplerine ilişkin ad, soyad, adres gibi bilgilerin tamamının Banka tarafından kendisine iletildiği ve buna göre icra takiplerinin başlatıldığı, bu bilgilerde bir hata var ise kendisinin bunu bilmesine imkân olmadığı

ifade edilmiştir.

İkinci avukattan alınan yazıda özetle,

- Şikâyete konu icra dosyasında avukatlığını yaptığı müvekkil şirketin bir varlık yönetimi şirketi olduğu ve bankaların tahsili gecikmiş alacaklarını ihale usulü ile satın alarak elde etmekte olduğu,
- Genel olarak bu tür dosyalarda yeni bir icra takip işleminin yapılmayıp bankaların daha önce açmış olduğu icra takipleri üzerinden işlemlere devam edilmekte olduğu, bu aşamada yeni bir takip yapılmadığından bankalarca icra dosyası açılırken girilen bilgilerin dosyanın devamında kullanılmakta olduğu,
- Müvekkil Şirketin bahse konu dosyadaki borçlunun mal varlığının tespiti için mal varlığı sorgulama işleminin yapılması talimatını verdiği,
- Kişisel verilerin kendisine ait hukuk bürosu uhdesinde kayıt altında tutulmadığı, müvekkil Şirket ile yapılan yazışmalarda da müvekkil Şirketin hem şirket bünyesinde hem de Bankada tutulan bilgilerin silinmesini sağladığı bilgilerinin kendilerine iletildiği

hususları ifade edilmiştir.

Üçüncü avukat tarafından ise Kurum yazısına herhangi bir cevap verilmemiştir.

Konuya ilişkin yapılan incelemede Kişisel Verileri Koruma Kurulunun 27/04/2021 tarihli ve 2021/424 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanununun “Tanımlar” başlıklı 3 üncü maddesinde ilgili kişinin, kişisel verisi işlenen gerçek kişi; veri sorumlusunun, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi; veri işleyen ise veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi olarak tanımlandığı,
- Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer almakta olduğu,
- Şikâyet konusu evrakta ilgili kişiye ait T.C. kimlik numarasının yer aldığı görülmekle birlikte cinsiyet, adres, anne ve baba adı gibi verilerin farklı olduğu, Emniyet Müdürlüğünün İcra Müdürlüğüne böyle bir kişinin belirtilen adreste bulunmadığı bilgisini ilettiği, bunun üzerine veri sorumlusu Banka tarafından borçlunun adres bilgilerinin tespiti için müzekkere yazdırıldığı, bu müzekerede de ilgili kişinin borçlu ile aynı olan isim, soy isim ve doğum tarihi bilgileri dışında T.C. kimlik numarasının da yer aldığı fakat doğum tarihi ve ana baba adı gibi verilerinin kendisine ait olmadığı tespit edildiği,
- İlgili kişinin dilekçe ile veri sorumlusu bankaya ve BİMER (CİMER) üzerinden savcılığa şikâyette bulunması üzerine Cumhuriyet Başsavcılığı tarafınca açılan Soruşturma Dosyası kapsamında veri sorumlusu Banka tarafından Başsavcılığa verilen yanıtta ilgili kişinin şubelerine başvurması sonucu gerekli güncellemelerin yapılarak T.C. kimlik numarasının sistemden silindiği, KKB kayıtlarının düzeltildiği, takip hesabının devir yapıldığı, Varlık Yönetim Şirketine ayrıca bilgilendirme

yapıldığı için veri sorumlusu Bankanın 2017 yılı içerisinde kendi içerisinde ve Varlık Yönetimi Şirketi ile yaptığı yazışmalardan görüldüğü,

- Öte yandan ilgili kişinin de 06.07.2017 tarihinde veri sorumlusu Varlık Yönetimi Şirketinin hattına, bankanın Cumhuriyet Başsavcılığına verdiği yanıtı faks gönderdiği, bununla birlikte 2017-2019 yılları arasında Varlık Yönetimi Şirketinin kurumsal hesabıyla WhatsApp uygulaması üzerinden yapılan yazışmalar ile, konuyu kendilerine intikal ettirmesine ve talebinin ilgili birime iletilmesine dair geri bildirim almasına karşın ilgili kişiye Varlık Yönetimi Şirketi tarafından yapılan aramaların 2019 yılı içerisinde dahi devam ettiği, ilgili kişiye ait borçların sistemden ve TBB Risk Merkezinden ilgili kişinin şikâyet kaydının oluşturulduğu Haziran-Temmuz 2019 tarihlerine kadar silinmediğinin anlaşıldığı,
- Somut olayda Banka ile Varlık Yönetimi Şirketinin Kanunun 3 üncü maddesi kapsamında veri sorumlusu sıfatını haiz olduğu, bununla birlikte veri sorumlusu Banka ve Varlık Yönetim Şirketi ile birlikte şikâyet olunan avukatların ise Bankanın/Varlık Yönetim Şirketinin dosya kapsamındaki vekilleri olduğu, kendilerinin veri sorumlusu Banka ile veri sorumlusu Varlık Yönetim Şirketinin talimatları altında kişisel veri işlediği ve birtakım yasal işlemleri yürütmekten ibaret olan vazifelerini yerine getirdikleri, şikâyet edilen avukatların kendi iradeleriyle “kişisel verilerin işleme amaçlarını belirleyerek” herhangi bir kişisel veri işleme faaliyeti yürüttüğüne dair tevsik edici bir belge Kuruma ulaşmamış olduğundan mezkûr şahısların veri sorumlusu sıfatını haiz olmadıklarının anlaşıldığı,
- Kanunun “Geçiş hükümleri” başlıklı Geçici 1 inci maddesinin (3) numaralı fıkrasının “Bu Kanunun yayımı tarihinden önce işlenmiş olan kişisel veriler, yayımı tarihinden itibaren iki yıl içinde bu Kanun hükümlerine uygun hâle getirilir. Bu Kanun hükümlerine aykırı olduğu tespit edilen kişisel veriler derhâl silinir, yok edilir veya anonim hale getirilir., “Yürürlük” başlıklı 32 nci maddesinin ise “Bu Kanunun; a) 8’inci, 9’uncu, 11’inci, 13’üncü, 14’üncü, 15’inci, 16’ncı, 17’nci ve 18’inci maddeleri yayımı tarihinden altı ay sonra, b) Diğer maddeleri ise yayımı tarihinde, yürürlüğe girer.” hükmünü amir olduğu,
- İlgili kişinin kişisel verilerinin veri sorumlusu Banka tarafından Kanun yürürlüğe girmeden önce işlendiği, akdedilen alacak temlik sözleşmesine dayanarak hukuka uygun olarak veri sorumlusu Varlık Yönetim Şirketine aktarıldığı, öte yandan Kanunun Geçici 1 inci maddesinin (3) numaralı fıkrasında yer alan “Kanunun yayımı tarihinden önce işlenmiş kişisel veriler yayımı tarihinden itibaren iki yıl içinde Kanuna uygun hale getirilir” hükmü çerçevesinde ilgili kişinin 2017 yılında yaptığı başvuruya istinaden ilgili kişinin kişisel verilerinin Banka tarafından düzeltilmediği,
- Bununla birlikte veri sorumlusu Bankanın, ilgili kişinin kendisine yaptığı başvuruya Kanun ve Tebliğ hükümleri kapsamında cevap vermediğinin görüldüğü,

- Veri sorumlusu Varlık Yönetimi Şirketinin, veri sorumlusu Banka tarafından akdedilen sözleşme kapsamında kendisine aktarılmış olan kişisel verileri kullandığı görülmekle birlikte, ilgili kişiye ait kişisel verilerin veri sorumlusu Banka tarafından veri sorumlusu Varlık Yönetimi Şirketine aktarımının, Kanununun 5 inci maddesinin (2) numaralı fıkrasının (e) bendinde ifade olunan “Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması” uyarınca hukuka uygun olduğu kanaatinin hâsıl olduğu,

- Ancak veri sorumlusu varlık yönetimi şirketinin ilgili kişi ve veri sorumlusu Banka tarafından 2017 yılı içerisinde yapılan e-posta, faks ve WhatsApp uygulaması yollarıyla yapılan bütün bildirimlere karşın ilgili kişinin dosyası hakkında bir şikâyet kaydı oluşturmadığı, bu sebeple ilgili kişinin aslında var olmayan borcunu ödemesi hususunda telefonla rahatsız edilmeye devam edildiği, şirket bünyesindeki kişisel verilerinin silinmeyip UYAP’tan taraf kaydının kaldırılmadığı, bu sebeple TBB Risk Merkezi veri tabanında ilgili kişiye kayıtlı borçların görüntülenmeye devam edildiği, bu durumun Kanununun 12 nci maddesini ihlâl ettiği

değerlendirmelerinden hareketle;

- İlgili kişinin kişisel verilerinin Banka tarafından Kanun yürürlüğe girmeden önce işlendiği, akdedilen alacak temlik sözleşmesine dayanarak hukuka uygun olarak Varlık Yönetim Şirketine aktardığı, öte yandan ilgili kişinin 2017 yılında yaptığı başvuruya istinaden ilgili kişinin kişisel verilerinin Banka tarafından düzeltildiği dikkate alındığında Veri sorumlusu Banka hakkında Kanun kapsamında yapılacak bir işlem olmadığına,

- Veri sorumlusu Bankanın ilgili kişilere yasal süre dâhilinde, Kanuna ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğe uygun bir şekilde cevap vermesi konusunda azami dikkat göstermesi hususunda talimatlandırılmasına,

- Varlık Yönetim Şirketinin ilgili kişinin gerçek borçlu olmadığına dair bilgileri 2017 yılı içerisinde gerek Bankadan gerekse de ilgili kişi cihetinden tarafına ulaşan bilgi ve belgeler vasıtasıyla edinmesine karşın ilgili kişinin kişisel verilerini işlemeye devam ederek borcun tahsili amacıyla ilgili kişinin aranması yoluna gidilerek 2019 yılı Haziran-Temmuz dönemine kadar veri tabanında, UYAP’ta ve TBB Risk Merkezindeki kayıtların düzeltilmediği, ilgili kişinin başvurusuna verilen yanıtta 29.07.2019 tarihinde TBB Risk Merkezindeki kayıtların güncellendiğinin ifade edilmesine karşın bu iddiayı tevsik edici bir belgenin Kuruma iletilmediği, ayrıca ilgili kişinin Kuruma intikal ettirdiği 04.12.2019 tarihli TBB Risk Merkezi Raporunda halen Varlık Yönetim Şirketine dosya bakımından borçlu olarak görüldüğü, bu kapsamda Şirketin Kanununun 5 inci maddesinde yer alan işleme şartlarına dayanmaksızın ilgili kişinin kişisel verilerini işlediği dikkate alındığında, Kanununun

12 nci maddesinin (1) numaralı fıkrasının (a) bendi çerçevesinde kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli tedbirleri almadığı kanaatine varılması nedeniyle Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında Varlık Yönetim Şirketi hakkında idari para cezası uygulanmasına,

- Şikâyet edilen diğer taraflar olan avukatların ise veri sorumlusu sıfatını haiz olmadıkları dikkate alındığında haklarında Kanun kapsamında tesis edilecek idarî bir işlemin bulunmadığına,
- İlgili kişinin maddî ve manevî zarara uğratıldığı yönündeki iddialarına ilişkin olarak adlî yargıya başvuru hakkının saklı olduğu hususunda bilgilendirilmesine,
- Veri sorumlusu Varlık Yönetimi Şirketinin ayrıca ilgili kişinin TBB Risk Merkezinde bulunan bilgilerini güncellediğini ve ilgili kişinin Risk Raporunda bulunan ve esasen kendisine ait olmayan borç bilgilerinin silindiğine dair tevsik edici bilgi, belge ve kayıtları, Kanunun 15 inci maddesinin (5) numaralı fıkrası uyarınca 30 (otuz) günlük yasal süre içerisinde Kurula iletmesi konusunda talimatlandırılmasına

karar verilmiştir.

2021/422 sayılı KVKK Kararı

İlgili kişinin fotoğraflarının veri sorumlusuna ait bir sosyal medya hesabında paylaşılması suretiyle gerçekleşen kişisel veri işleme faaliyeti hakkında Kişisel Verileri Koruma Kurulunun 27/04/2021 tarihli ve 2021/422 sayılı Karar Özeti

Karar Tarihi : 27.04.2021

Karar No : 2021/422

Konu Özeti : İlgili kişinin fotoğraflarının veri sorumlusuna ait bir sosyal medya hesabında paylaşılması suretiyle gerçekleşen kişisel veri işleme faaliyeti

Kuruma intikal eden şikâyet dilekçesinde özetle; ilgili kişinin veri sorumlusunun iş yerinde pilates eğitmeni olarak çalıştığı, iş ilişkisinin sona ermesinden sonraki tarihlerde veri sorumlusunun sosyal medya hesabından ilgili kişinin fotoğraflarını kullanarak herkese açık şekilde paylaşımlarda bulunduğu, bu sebeple veri sorumlusuna başvuruda bulunularak ilgili paylaşımının kaldırılması, fotoğrafların ilgili kişiye iade edilmesi, veri sorumlusunda bulunan fotoğrafların yok edilmesi ve veri sorumlusu nezdinde reklam veya başka bir amaçla sosyal medyada kullanılmamasının talep edildiği, veri sorumlusunun başvuruya cevabında söz konusu fotoğrafların kullanımından vazgeçildiğini belirtmesine karşın, herkes tarafından erişilebilir sosyal medya hesabında fotoğrafların yayınlanmaya devam ettiği, ilgili kişinin açık rızası alınmamasına rağmen fotoğrafların paylaşıldığı ve talebe rağmen sosyal medya platformundan kaldırılmadığı, paylaşılan fotoğrafla ilgili olarak ilgili kişiye hiçbir bilgilendirme yapılmadığı ve aydınlatma yükümlülüğünün de yerine getirilmediği, söz konusu fotoğraf paylaşımının 6698 sayılı Kişisel Verilerin Korunması Kanununa (Kanun) aykırı olduğu belirtilerek, veri sorumlusu hakkında gereğinin yapılması talep edilmiştir.

Başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş ancak veri sorumlusu tarafından savunma, bilgi ve belge talepli Kurum yazısına herhangi bir cevap verilmemiştir.

Bununla birlikte, ilgili kişinin şikâyeti neticesinde veri sorumlusunun ilgili kişiye ilettiği cevabı nitelikli yazısında; veri sorumlusunun eski çalışanı olan ve çalıştığı döneme ilişkin olarak veri sorumlusu reklamlarında şahsi hiçbir özelliği ön plana çıkarılmadan, şirket çalışanı olarak o tarihte kendi isteği ile reklam çekimlerinde yer alması nedeniyle ilgili kişiye ait fotoğrafların şirketin

tanıtımına ilişkin bölümlerde yer aldığı, tanıtım fotoğraflarında ilgili kişinin şahsına ilişkin bir kayıt ve bilgi bulunmadığı, fotoğrafların ilgili kişinin bilgisi ve izni ile çekildiği, ilgili kişinin şahsına ve kişilik haklarına ilişkin bir aykırılık bulunmadığı yine de ihtarname sonrası ilgili kişinin talebi doğrultusunda fotoğrafların kullanımından vazgeçildiği, ilgili kişinin izni ile reklam şirketi tarafından tanıtım amaçlı çekilen şirket faaliyetlerine ilişkin fotoğrafların şirket reklamlarındaki görsellerden kaldırılması nedeniyle şirket yönünden ayrıca bir zarar olduğu ifadelerine yer verildiği görülmüştür.

Eldeki bilgi ve belgeler çerçevesinde konuya ilişkin yapılan incelemede Kişisel Verileri Koruma Kurulunun 27/04/2021 tarihli ve 2021/422 sayılı Kararı ile;

- Kanunun “Kişisel verilerin işleme şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında belirtilen hallerden birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Diğer taraftan, Kanunun 7 nci maddesinde “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi” hususu düzenlenmiş olup maddede;

“(1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.

(2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır.

(3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir.”

hükümlerine yer verildiği,

- 28.10.2017 tarih ve 30224 sayılı Resmi Gazete’de yayımlanan "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin (Yönetmelik) “Kişisel Verileri İlgili Kişinin Talep Etmesi Durumunda Silme ve Yok Etme Süreleri” başlıklı 12 nci maddesinde ise;

“(1) İlgili kişi, Kanunun 13 üncü maddesine istinaden veri sorumlusuna başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

a) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Veri sorumlusu, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir.

b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa veri sorumlusu bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde bu Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.

c) Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep veri sorumlusunca Kanununun 13 üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.” hükmünün yer aldığı,

- Yönetmeliğin “Kişisel verilerin silinmesi” başlıklı 8 inci maddesinin (2) numaralı fıkrasının, “Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.”; “Kişisel verilerin yok edilmesi” başlıklı 9 uncu maddesinin (2) numaralı fıkrasının ise, “Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.” hükümlerini haiz olduğu,

- Şikâyet konusu sosyal medya hesabında, ilgili kişinin paylaşılan fotoğraflarının yayınlanmaya devam ettiği ve hesaptan kaldırılmadığı, 15.05.2019 tarihli paylaşımında ilgili kişinin fotoğrafının arka planda ve hafif bulanık şekilde paylaşıldığı, 20.05.2019 tarihli paylaşımında ilgili kişinin fotoğrafının net şekilde seçilebildiği,

- Veri sorumlusunun savunma, bilgi ve belge talepli Kurum yazısına yasal süre içerisinde herhangi bir cevap vermemesi karşısında, ilgili kişinin söz konusu veri işleme faaliyeti açısından açık rızasının alındığına ilişkin herhangi bir somut bilgi veya belge edinilemediği için, veri sorumlusunun Kanununun 5 inci maddesi kapsamında herhangi bir kişisel veri işleme şartına dayanmaksızın ilgili kişinin kişisel verilerini hukuka aykırı şekilde işlemek suretiyle Kanununun 12 nci maddesinin (1) numaralı fıkrası kapsamında uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı,

- Öte yandan ilgili kişinin talebi üzerine fotoğraflarının Yönetmeliğin 12 nci maddesinin (1) numaralı fıkrasının (a) bendinde öngörülen otuz günlük yasal süre içinde silinmesi/ yok edilmesi gerektiği, yasal süre geçtikten sonra halen devam eden veri işleme faaliyetinin bu kapsamda yine hukuka aykırı olduğu

değerlendirmelerinden hareketle;

- İlgili kişinin fotoğraflarının veri sorumlusuna ait sosyal medya hesabından kaldırılmaması nedeniyle veri sorumlusunun Kanunun 5 inci maddesi kapsamında herhangi bir kişisel veri işleme şartına dayanmaksızın kişisel verileri hukuka aykırı şekilde işlemek suretiyle Kanunun 12 nci maddesinin (1) numaralı fıkrası kapsamında uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı kanaatine varılması nedeniyle veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında idari para cezası uygulanmasına,
- Veri sorumlusunun sosyal medya hesabında bulunan ilgili kişiye ait tüm fotoğrafların kaldırılması ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik hükümleri uyarınca uygun usulle silinmesi/yok edilmesi, söz konusu fotoğrafların başka hiçbir mecrada kullanılmaması ve bu işlemlerin sonucundan Kurula bilgi verilmesi yönünde veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2021/470 sayılı KVKK Kararı

İlgili kişinin yemek kartı hesap hareketlerine ilişkin kişisel verilerine erişim talebinin veri sorumlusu tarafından yerine getirilmediği iddiası hakkında Kişisel Verileri Koruma Kurulunun 06/05/2021 tarihli ve 2021/470 sayılı Karar Özeti

Karar Tarihi : 06.05.2021

Karar No : 2021/470

Konu Özeti : İlgili kişinin yemek kartı hesap hareketlerine ilişkin kişisel verilerine erişim talebinin veri sorumlusu tarafından yerine getirilmediği iddiası

İlgili kişinin Kuruma intikal eden şikayetinde özetle; kendisine işvereni tarafından tahsis edilen yemek kartına ait hesap hareketlerinin tarafına iletilmesinin veri sorumlusu Şirketten talep edildiği, veri sorumlusu tarafından verilen cevapta ise istenilen bilginin sağlanması için kimliği doğrulayacak ilave bilgiler talep edildiği, bunun üzerine dilekçe ve kimlik görüntüsünün veri sorumlusuna e-posta aracılığıyla iletildiği, veri sorumlusu şirketin gönderdiği e-postada ise ilgili bilgilerin ekte paylaşıldığı ancak ilave güvenlik önlemi alınması nedeniyle ekte paylaşılan dokümana erişilebilmesi için e-postada yer alan cep telefonu numarasının aranması gerektiğinin belirtildiği, getirilen bu ilave güvenlik önleminin hukuka aykırı olup şahsına ait verilere erişmesinin engellendiği ve hesap hareketlerinin 6698 sayılı Kişisel Verilerin Korunması Kanunu'na (Kanun) uygun olarak paylaşılmadığı belirtilerek Kanun kapsamında gereğinin yapılması talep edilmektedir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişinin gmail adresinden veri sorumlusuna gönderdiği e-postada ... nolu yemek kartı kullanıcısı olduğunu belirterek Kanun'un 11'inci maddesi uyarınca tüm hesap hareketlerini ve işlenen verileriyle ilgili açıklamaları talep ettiği, yapılan inceleme sonucunda söz konusu e-posta adresi sistemde kayıtlı olmadığından, ilgili iletişim kanalının teyit edilemediği ve ayrıca ilgili kişi tarafından sunulan kart numarasının hatalı bir numara olduğunun görüldüğü,
- Veri sorumlusunun ilgili kişinin talebine verdiği cevapta, talebin ilgili kişi tarafından yöneltildiğinin ve ilgili kişi haricinde bir başka kişiye cevap verilmediğinin teyit edilebilmesi için

kimliğini doğrulayacak bazı ilave bilgiler istenildiği, veri sorumlusunun talebi üzerine ilgili kişi tarafından gönderilen e-postanın ekinde yer alan ıslak imzalı dilekçedeki talebin “Tarafıma ait .. numaralı kartın tüm hesap hareketlerinin ...@gmail.com e-posta adresine gönderilmesi için gereğinin yapılmasını arz ederim.” şeklinde olduğu, bildirilen e-posta adresine yanıt verildiği ve başvurunun konusu olan tüm bilgilerin e-postanın ekinde ilgili kişiyle paylaşıldığı,

- İlgili kişinin daha önce veri sorumlusu sisteminde tanımlı olmayan ve “gmail” gibi altyapısı yurtdışında barındırılan bir e-posta adresine kişisel verilerinin gönderilmesini talep etmesi nedeniyle risk değerlendirmesi yapılarak e-posta ortamında güvenliği en üst düzeyde temin etmek amacı doğrultusunda talebin yanıtlandığı ve ek olarak dosyanın şifrelendiği, ilgili kişinin dosya şifresinin kendisine verilmesi için doğrudan arayabileceği bir telefon numarasının kendisine bildirildiği ve bu güvenlik tedbirinin neden alındığının açıkça izah edildiği

ifade edilmiştir.

Konuya ilişkin olarak yapılan incelemede, Kişisel Verileri Koruma Kurulunun 06/05/2021 tarihli ve 2021/470 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun 11’inci maddesinin (1) numaralı fıkrasının (b) bendi hükmü kapsamında ilgili kişinin, kendisiyle ilgili kişisel veriler işlenmişse buna ilişkin bilgi talep etme hakkının, söz konusu veriye erişim hakkını da kapsadığı; erişim hakkının bilgi talep etme hakkını tamamlayarak ilgili kişinin kişisel verileri üzerindeki haklarını kullanabilmesi için kişisel verilerinin ne şekilde işlendiğine dair tam olarak bilgi sahibi olmasına imkan sağladığı,

- Kanun’un 12’nci maddesinin (1) numaralı fıkrası gereğince veri sorumlusunun; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu,

- Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ kapsamında, veri sorumlusunun ilgili kişi tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlü olduğu; ayrıca, Kurum tarafından veri güvenliğinin sağlanmasına atfedilen önem doğrultusunda yayımlanan Kişisel Veri Güvenliği Rehberi’nde (Teknik ve İdari Tedbirler) Kanun’un 12’nci maddesi kapsamında veri güvenliğini sağlamak amacıyla veri sorumlusunun temin etmesi gereken teknik ve idari tedbirlere ilişkin başlıca yöntemlerin bölümler halinde açıklandığı, hangi önlemlerin alınması gerektiği konusunda ise Rehber’de belirtildiği üzere öncelikle veri sorumlusu tarafından işlenen tüm kişisel

verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerektiği,

- Şifreleme yöntemi ile temel olarak haberleşen kişiler arasındaki veri alışverişinin, üçüncü kişilerin okuyamayacağı şekilde güvenli olarak yapılmasının amaçlandığı; veri sorumlusunun, ilgili kişinin kişisel verisine erişimini engellemekle birlikte ilgili kişi için orantısız bir külfete yol açmayacak şekilde e-posta aracılığıyla gönderilen dosyanın şifreli olarak gönderimini sağladığı ve şifrenin de e-postada yer alan telefon numarası arandığında kendisiyle paylaşılacağı belirtilmiştir,

- Veri sorumlusu tarafından yapılan risk analizi doğrultusunda, ilgili kişinin kullanımındaki yemek kartının hesap hareketleri ve yükleme bilgilerine ilişkin kişisel verileri içeren dosyanın ilgili kişi tarafından belirtilen ve alt yapısı yurt dışında olan "gmail" hesabına e-posta aracılığıyla gönderileceği için bu verileri içeren dosyanın şifrelenerek gönderilmesi ile veri güvenliğinin üst düzeyde sağlanmasının amaçlandığının ifade edildiği; Kurulun 31/05/2019 tarihli ve 2019/157 sayılı Kararında belirtildiği üzere, Google firmasına ait G-mail e-posta hizmeti altyapısının kullanılması durumunda gönderilen ve alınan e-postaların dünyanın çeşitli yerlerinde bulunan veri merkezlerinde tutulmasının söz konusu olacağı; bu doğrultuda, Kanunun 12'nci maddesinin (1) numaralı fıkrasının (b) bendi gereğince kişisel verilere hukuka aykırı olarak erişilmesini önleme yükümlülüğü altında olan veri sorumlusunun aldığı ilave güvenlik önleminin ilgili kişinin iddia ettiği üzere Kanuna aykırılık değil, Kanunun titizlikle uygulanması olduğu

değerlendirmelerinden hareketle;

- İlgili kişinin Kanun'un 11'inci maddesinin (1) numaralı fıkrasının (b) bendi doğrultusunda, kullandığı yemek kartının hesap hareketlerine ilişkin veri sorumlusu tarafından işlenen kişisel verilerine erişim talebi üzerine; veri sorumlusu tarafından e-posta aracılığıyla ilgili kişi tarafından belirtilen "gmail" adresine gönderilen ve kişisel verileri içeren söz konusu dosyanın şifrelenmesinin ilgili kişinin iddiasının aksine Kanun'un 12'nci maddesinin (1) numaralı fıkrasının (b) bendi gereğince kişisel verilere hukuka aykırı olarak erişilmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri alma yükümlülüğünü yerine getirmek adına makul bir tedbir olduğuna, alınan bu güvenlik tedbirine ilişkin gerekli açıklamanın ilgili kişiye yapıldığı ve e-posta içerisinde yer alan telefon numarası arandığında şifrenin ilgili kişiyle derhal paylaşılacağı belirtilmiştir dikkate alındığında kişisel verilere erişim hakkının engellenmediğine, bu doğrultuda veri sorumlusu hakkında Kanun kapsamında yapılacak bir işlem bulunmadığına

karar verilmiştir.

2021/464 sayılı KVKK Kararı

Bir otoyol işletmesinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 16.06.2020 tarih ve 2021/464 sayılı Karar Özeti

Karar Tarihi : 16.06.2020

Karar No : 2021/464

Konu Özeti : Bir otoyol işletmesinin veri ihlal bildirimini hakkında karar

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin; çalışanların kendi rıza ve talepleri ile yazılı ve imzalı olarak veri sorumlusuna ilettikleri kişisel e-posta adreslerinin sisteme işlenmesinden sonra bordro programı üzerinden bu hesaplara gönderilen bordrolarda, gönderilen kişilerin kendisine ait olmayan ancak aynı şirket çalışanı olan başka çalışanlara ait bordroyu ve dolayısıyla başkasına ait ad, soyad, TC Kimlik No ve sicil numarası görüntülemesi şeklinde gerçekleştiği, maaş bilgisinin ise herkeste aynı jenerik bilgisinin görüntülediği,
- İhlalin sistemsal bir hata sebebiyle hatalı e-posta gönderimi neticesinde meydana geldiği ve bu teknik hatanın da bordro sisteminde Türkçe dili için bir cihaz türü tanımlı olmaması nedeni ile programın bordro zarflarını anlık göndermek yerine öncelikle kuyruğa gönderip oradaki kayıtları sonrasında e-posta atmak yöntemini kullanması nedeniyle yaşandığı,
- İhlalden etkilenen kişi ve kayıt sayısının 489 olduğu,

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 25.03.2021 tarih ve 2021/311 sayılı Kararı ile;

- Yapılan inceleme sürecinde, kurul kararına istinaden veri sorumlusuna gönderilen tebligatta, *"...Çalışanların kendi rıza ve talepleri üzerine sundukları yazılı beyan dilekçesinde yer alan kişisel e-posta adreslerinin sisteme işlendiği ve bu kişisel e-postaların kullanıldığı, ancak neden kişisel e-posta yerine şirket e-postasına gönderim gerçekleştirilmediği..."* ile ilgili bilgi istenmiştir. Bu talebe cevaben veri sorumlusu, *"Şirketimiz, çalışanlarının büyük bir çoğunluğu sahada bulunan bir organizasyon yapısına sahiptir. Bu itibarla*

tüm çalışanlarımıza şirketimiz tarafından tanımlanmış bir e-posta hesabı bulunmadığı, keza şirket e-posta hesaplarına şirketin erişim olanağı bulunduğu da dikkate alınarak bu bildirimlerin çalışanlarımızın kişisel e-posta hesaplarına yapılmasının daha uygun olacağı değerlendirilmiştir.” şeklinde bir geri dönüş yapılmıştır. Bu durum, çalışanlara yanlışlıkla giden bordroların silinip silinmediğinin kişisel e-posta hesaplarından (birçok e-posta sunucusu içerdiği için) kontrol imkânı bulunmadığından ihlalin, aslında veri sorumlusunun belirttiği gibi sadece teknik aksaklık değil; söz konusu çalışanlara kurumsal e-posta hesabı açmayarak ve bu hesaplar üstünden bordro gönderimi yapmayarak ihlalin idari eksiklikten de kaynaklanmasına sebep olunduğu,

- Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) 3.2 maddesi Kişisel Veri Güvenliğinin Takibi başlığında “...Çalışanların sistem ve servislerdeki güvenlik zaafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulması gerekmektedir.” ifadesine ve 2.1. Mevcut Risk ve Tehditlerin Belirlenmesi başlığında “Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir...” ifadesine göre ihlale konu olan riskin veri sorumlusu tarafından değerlendirilmediği,

- Veri sorumlusu tarafından aydınlatma yükümlülüğüne uyularak ve ilgili kişilerin açık rızası alınarak e-postaların gönderildiği belirtilmekle birlikte aydınlatma metninin ilgili kişileri bu hususlara ilişkin olarak yeterince bilgilendiren bir metin olmadığı ve kişilere herhangi bir başka seçenek bırakmadığının görüldüğü,

- 31.05.2019 tarihli ve 2019/157 sayılı Kurul Kararında de belirtildiği üzere, kurumsal e-posta hizmetinin sunucularının yurt dışında olan veri sorumlularından/veri işleyenlerden temin edilmesi durumunda saklama hizmetlerinin de 6698 sayılı Kanunun 9 uncu maddesi hükümlerine uygun olarak gerçekleştirilmesi gerektiği, veri sorumlusu tarafından Kurumsal e-posta hizmeti alınmadan çalışanların şahsi e-posta hesaplarının çalıştıkları işlerle ilgili e-posta gönderiminde kullanılmasının verilerin farklı ülkelerde saklanması durumunu ortaya çıkarabileceği ve veriler üzerinde kontrol kaybına neden olabileceği

hususları dikkate alındığında, Kanun’un 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 60.000 TL idari para cezası uygulanmasına,

karar verilmiştir.

2021/427 sayılı KVKK Kararı

Bir e-ticaret sitesi (veri sorumlusu) nezdinde gerçekleşen veri ihlali hakkında yapılan resen inceleme hakkında Kişisel Verileri Koruma Kurulunun 27/04/2021 tarih ve 2021/427 sayılı Karar Özeti

Karar Tarihi : 27.04.2021

Karar No : 2021/427

Konu Özeti : Bir e-ticaret sitesi (veri sorumlusu) nezdinde gerçekleşen veri ihlali hakkında yapılan resen inceleme

Bir e-ticaret sitesindeki (veri sorumlusu) partner firmanın, e-ticaret sitesindeki müşteri hizmetleri paneli üzerinden üçüncü kişiler konumundaki firmaların bilgilerine erişmesiyle yapmış olduğu ihbar kapsamında konuya ilişkin olarak Kişisel Verileri Koruma Kurulu tarafından resen inceleme başlatılmıştır.

Partner firmasının Kurumumuza intikal eden yazılarında;

- Partner firmanın elektronik adisyon takip sistemi ve dokunmatik bilgisayar ürünlerinin internet ortamında satışına ilişkin, veri sorumlusu ile partner şirket olmak adına başvuruda bulunulduğu,
- Firmanın, ürünlerini sisteme yüklerken giriş yaptığı bölümün aktif olmadığını fark etmeleri üzerine e-ticaret sitesinin müşteri hizmetlerini arayarak durumu ilettiklerinde, partner sayfasındaki bildirim bölümünden konuya ilişkin iletişime geçilmesi gerektiğinin belirtildiği, firmanın bu doğrultuda bildirim paneline giriş yapıp bildirim göndermeye çalıştıklarında sürekli hata aldığı,
- Bu hatalardan dolayı Partner Firmanın bildirim linkini tarayıcıya yazıp giriş yapmaya çalıştığı, bu suretle veri sorumlusunun kullanmış olduğu müşteri hizmetleri (CRM) paneline erişildiği, açılan panelde tekrar kullanıcı adı ve şifre istendiği, mevcut kullanıcı adı ve şifreleriyle giriş yapılmaya çalışıldığı, erişim sağlanamayınca şifrelerinin bloke edildiği düşünülerek yeni şifre talep edildiği, e-posta adreslerine gelen şifre ile sisteme giriş yapıldığında veri sorumlusunun CRM paneline ulaşıldığı, bu sistem açığıyla ilgili veri sorumlusuna e-posta gönderildiği,

- Konuya ilişkin veri sorumlusunun avukatının kendilerini arayarak, belirli bir ücret karşılığında kendilerini danışman şirket olarak atayacaklarını, veri sorumlusu tarafından ilgili firmaya bir şifre verilerek sisteme giriş yapılacağını, veri sorumlusunun onayı ile sistem açığı bulunup bulunmadığına yönelik kontrol sağlamak amacıyla girdiğini gösterir bir senaryo hazırlayacaklarını ve söz konusu senaryoyu destekleyecek bir gizlilik sözleşmesi imzalayacaklarını belirttiği, veri sorumlusunun ofisinde bir toplantı gerçekleştirildiği, yapılan toplantıda güvenlik açığına ilişkin görüşme gerçekleştirildiği ve gizlilik sözleşmesinin imzalandığı

ifadelerine yer verilmiştir.

Veri sorumlusunun meydana gelen veri ihlali ile ilgili Kurumumuzun konuya ilişkin tebliğatlarına verilen cevap yazılarında ise;

- Pazar yeri modeli ile satış yapmak üzere kendilerine başvuran şahısların veri sorumlusu nezdinde satış yapabilmelerini teminen giriş yapmaları amacı ile kendilerine tahsis edilen kullanıcı adı ve şifre ile sisteme giriş sağladıkları,
- Şahısların daha sonra sistemde bir açık bulduklarını, kendilerine ait doküman yükleme sayfası dışında üçüncü kişiler konumundaki firmaların bilgilerine de eriştiklerini beyan ederek veri sorumlusuna müracaat ettikleri,
- Akabinde bahse konu veri güvenliği açığına ilişkin, veri sorumlusu ile şahıslar arasında kişisel verilerin korunması amacıyla firmanın sisteme ilk girdiği tarihten itibaren başlayacak şekilde bir gizlilik sözleşmesi imzalandığı, sözleşme ile bu şahısların, ellerindeki tüm verileri veri sorumlusuna teslim edeceklerini ve kendi sistemlerindeki yedekler dahil tüm veriyi imha edeceklerini, tüm sürecin gizliliğini de en üst düzeyde sağlayacaklarını taahhüt ettikleri,
- Söz konusu sözleşmenin başlangıç tarihi olayın oluş tarihi olduğundan firma tarafından bilgilere erişilmesinin veri sorumlusu ile firma arasında akdedilen sözleşme kapsamında gerçekleştiği ve bu anlamda herhangi bir hukuka aykırı erişimin bulunmadığı,
- Taraflar arasında bu minvalde bir sözleşme imzalanmışsa da daha sonra bu şahısların veri sorumlusundan şantaj yolu ile para istedikleri, veri sorumlusunun bu şahıslara herhangi bir ödeme yapmadıkları ve sonunda da Kişisel Verileri Koruma Kurumuna başvurdukları,
- İhlale konu olayın suç niteliği taşıması nedeniyle Kurumumuz tarafından re'sen incelemeye ilişkin karar verilemeyeceği zira konunun yargı organları tarafından değerlendirilmesi gerektiği,
- Konuya ilişkin Cumhuriyet Başsavcılığına suç duyurusunda bulunulduğu

belirtilmiştir.

Partner Firmanın yapmış olduğu ihbar bildiriminin ve veri sorumlusu yazılarının incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 27/04/2021 tarih ve 2021/427 sayılı Kararı ile;

A. Teknik ve idari tedbirler ile ilgili olarak;

- Veri sorumlusu tarafından kendi tedarikçisi konumunda olan firma yetkililerinin, veri sorumlusunun sistemine giriş yaptıklarında üçüncü kişilere ait kişisel verilere erişim sağladıkları ve erişimin sağlandığı ilk tarih itibariyle bu hususta yetkili olmadıkları, bu anlamda bahsi geçen “Gizlilik Sözleşmesi” öncesinde “veri sorumlusu uhdesinde bulunan kişisel verilere yetkisiz erişim sağlandığının anlaşıldığı, hukuka aykırı erişimin meydana gelmesinden sonra veri sorumlusu ile şahıslar arasında imzalanan gizlilik sözleşmesi ile geçmişe dönük olarak, meydana gelmiş olan veri ihlalinin ortadan kaldırılmasının hukuken mümkün olmadığı,

- İhlalin veri sorumlusu tarafından kendi tedarikçisi konumunda olan firmanın da bulunduğu tedarikçi grubuna “tüm bildirimlerde arama” yetkisinin verilmesi sonucunda oluştuğunun tespit edildiği, bu durumun yetkisiz erişime ilişkin düzenli kontrolün sağlanmadığının ve yetkilendirme süreçlerinin kontrol edilmeyerek veri ihlali öncesinde veri sorumlusu tarafından ilgili kişiler üzerinde oluşabilecek potansiyel zararları önlemek adına gerekli tedbirlerin alınmadığının göstergesi olduğu hususları dikkate alındığında, 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (1) numaralı fıkrasında kapsamında veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca, 600.000 TL idari para cezası uygulanmasına,

B. Kuruma ve ilgili kişilere yapılan bildirim ile ilgili olarak:

Veri sorumlusu nezdindeki kişisel verilere hukuka aykırı olarak erişilmesi dolayısıyla, Firma nezdinde erişimi gerçekleştirenler yönünden yürütülen cezai soruşturmaya konu fiil ile veri sorumlusunun veri güvenliğini sağlamaya ilişkin gerekli her türlü teknik tedbiri almaması nedeniyle oluşan veri ihlalini Kurula bildirme yükümlülüğünün farklı fiiller olduğu, ihlalin 22.10.2019 tarihinde gerçekleşmesi ve 22.10.2019 tarihinde tespit edilmiş olmasına rağmen

- Veri ihlalden etkilenen ilgili kişilere bildirimde bulunulmadığı,
- Kişisel Verileri Koruma Kuruluna ihlal bildiriminde bulunulmadığı

hususları dikkate alındığında Kanunun 12 nci maddesinin (5) numaralı fıkrası kapsamında Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararında belirlenen 72 saat içerisinde bildirimde bulunma yükümlülüğüne aykırı davranan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 200.000 TL idari para cezası uygulanmasına

- Kurumumuzun bilgi belge talep yazısına cevap verilmediği dikkate alındığında, Kanuna uyum konularında azami dikkat ve özenin gösterilmesi hususunda veri sorumlusunun talimatlandırılmasına,

karar verilmiştir.

2021/426 sayılı KVKK Kararı

Yardım masası paneli hizmeti veren bir veri sorumlusunda gerçekleşen veri ihlali hakkında yapılan resen inceleme hakkında Kişisel Verileri Koruma Kurulunun 27/04/2021 tarihli ve 2021/426 sayılı Karar Özeti

Karar Tarihi : 27.04.2021

Karar No : 2021/426

Konu Özeti : Yardım masası paneli hizmeti veren bir veri sorumlusunda gerçekleşen veri ihlali hakkında yapılan resen inceleme

Bir e-ticaret sitesindeki partner firmaya, e-ticaret sitesinin hizmet aldığı yardım masası panelinde yapılan toplu yetkilendirme çalışması esnasında, yanlış yetki verilmesi sonucunda üçüncü taraf diğer firmaların yardım masasında açtıkları bildirimlere erişim sağlamasıyla gerçekleşen veri ihlalinin, partner firma tarafından Kurumumuza bildirilmesi neticesinde Kişisel Verileri Koruma Kurulu tarafından resen inceleme başlatılmıştır.

Yardım masası paneli hizmeti veren veri sorumlusu nezdinde yapılan yerinde inceleme ve konuya ilişkin ifadelerinin yer aldığı tutanakta;

- Veri ihlalinin, veri sorumlusunun kendi yardım masası üzerinde yapılan toplu yetkilendirme çalışması esnasında veri tabanı katmanında çalıştırılan SQL Script kodundaki bir hata sonucu oluştuğu,
- Yapılan hata sonucu partner firmanın yer aldığı gruba yanlış yetki verilmesiyle, partner firmanın kendi yardım masası bildirimleri haricinde grup içerisinde yer alan diğer firmaların da yardım masası bildirimlerine ulaşabildiği,
- Veri sorumlusu tarafından yapılan analiz çalışması sonucunda, sadece söz konusu partner firmanın kendisi haricindeki diğer yardım masası bildirimlerine erişim sağladığının tespit edildiği,
- Durum tespit edilir edilmez partner firmaya ait yardım masası yetkisi veri sorumlusu tarafından kaldırılarak erişiminin engellendiği,

- Partner firma tarafından veri sorumlusuna gönderilen e-postada, ilgili hata sonucu diğer firmalara ait bilgileri görebildikleri, kendileri ile iletişime geçilmemesi durumunda ihbarda bulunulacağı ve veri sorumlusunun çalışmakta olduğu firmalarla iletişime geçileceğinin paylaşıldığı, veri sorumlusu avukatınca partner firmaya gerekli yasal hatırlatma yapılarak, erişilen verilerin silinmesinin talep edildiği,
- Veri ihlalden 13 farklı veri sorumlusu niteliği taşıyan firmanın etkilenmiş olduğu, veri sorumlusu tarafından ihlalden etkilenen veri sorumlularına gerçekleşen olay ile ilgili e-posta yoluyla bilgilendirme yapıldığı,
- Yazılım üzerindeki özelliklerin tüm veri sorumluları için standart olduğu, bu standardın belirlenmesinde yardım masası paneli hizmeti veren veri sorumlusunun karar verici pozisyonda olduğu, ancak gelen geri bildirimler (kullanıcı deneyimleri) çerçevesinde değerlendirme yapılarak ürün özelliği olarak versiyon planı dahilinde eklendiği, kullanıcıların esnek form ve iş akışları tasarlayabildikleri, böylelikle kendilerine özel ekranlar oluşturabildikleri ifade edilmiştir.

Yardım masası panelinin, veri sorumlusunun kendisi tarafından kurulan ve yönetilen bir platform olduğu, yazılım hizmetleri ile ilgili bakım ve destek hizmetlerini sağladığı, diğer veri sorumlularının sınırlı bir erişime sahip olduğu ve üzerinde doğrudan değişiklik yapmasının mümkün olmadığı değerlendirilmiştir.

İhlal ile ilgili 3 veri sorumlusu tarafından, Kurumumuza kişisel veri ihlal bildiriminde bulunulmuş, bildirimde bulunmayan 10 veri sorumlusu hakkında 22.04.2020 tarih ve 2020/311 sayılı Kurul Kararı ile resen inceleme başlatılmasına karar verilmiş olup, bunun üzerine söz konusu veri sorumlularından bilgi ve belge talep edilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 27/04/2021 tarih ve 2021/426 sayılı Kararı ile,

A) Teknik ve idari tedbirler ile ilgili olarak;

- Yardım masası panelinin, yazılım firmasından hizmet alan veri sorumlularının kullanıcı adı ve şifreleriyle giriş yapıp yardım taleplerini ilettikleri bir platform olduğu, söz konusu platform üzerinde verilen hizmetler açısından yazılım firmasının veri sorumlusu sıfatını haiz olduğu,
- Veri ihlalden 13 farklı veri sorumlusunun, 950'den fazla sayıda çalışanına ve müşterisine ait kimlik, iletişim ve müşteri işlem verilerinin etkilendiği,

- Veri ihlalinin, hatalı bir şekilde yapılan yetki düzenlemesinden ve veri sorumlusunun ihmalkarlığı sebebiyle yeterli güvenlik önlemlerini almamasından kaynaklandığı,
- Bilişim hizmeti yürüten bir veri sorumlusunun bilgi sistemleri güvenliğinde daha dikkatli olmasının beklenildiği, yazılım geliştirme süreçlerinin test platformunda yapılması gerekirken, veri tabanında gerçekleştirilen güncellemenin canlı ortamda yapılmış olması sebebiyle ihlalin gerçekleştiği,
- Veri sorumlusunun sistemlerinde kişisel veri içeren belgelerin bulunması halinde kişisel verileri maskeleyen etkin uygulama ve denetim araçlarının bulunmadığı

hususları dikkate alındığında, 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak (ihlalden etkilenen 950'den fazla kişinin bulunduğu, ihlale veri sorumlusunun ihmalkarlığının sebebiyet verdiği) Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca, **300.000 TL idari para cezasının uygulanmasına,**

B) Kurumumuza ve ilgili kişilere yapılan bildirim ile ilgili olarak;

- Veri ihlaliyle ilgili Kurula bildirim yapılmadığı dikkate alındığında Kanunun 12 nci maddesinin (5) numaralı fıkrası kapsamında Kişisel Verileri Koruma Kurulunun 24/01/2019 tarih ve 2019/10 sayılı Kararı ile belirlenen 72 saat içerisinde bildirim yükümlülüğünü yerine getirmeyen veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca, **100.000TL idari para cezasının uygulanmasına,**

C) Kurumumuza yönelik bilgi ve belge gönderimi hakkında;

- Bir kamu tüzel kişiliğine haiz veri sorumlusunun, söz konusu olay dahilinde kendilerinden bilgi/belge talebinde bulunulmasına rağmen Kurumumuza **herhangi bir cevap vermediği,**
- Bir özel hukuk tüzel kişiliğine haiz veri sorumlusunun, ihlale konu olayın suç niteliği taşıması nedeniyle Kurumumuz tarafından resen incelemeye ilişkin karar verilemeyeceği, zira olayın yargı organları tarafından değerlendirilmesi gerektiğini iddia ettiği ve Kurumumuza bir takım bilgi ve belge göndermiş olmakla birlikte; Kurulun, inceleme konusuyla ilgili istemiş olduğu; ihlalden etkilenen kişi sayısı, ihlalden etkilenen kişisel veriler gibi ihlal ile ilgili açıklayıcı **birçok bilgi ve belgeyi Kurumumuza göndermemiş olduğu**

hususları dikkate alındığında Kanunun 15 inci maddesinin (3) numaralı fıkrasında yer alan “Devlet sırrı niteliğindeki bilgi ve belgeler hariç; veri sorumlusu, Kurulun, inceleme konusuyla ilgili istemiş olduğu bilgi ve belgeleri on beş gün içinde göndermek ve gerektiğinde yerinde inceleme yapılmasına imkân sağlamak zorundadır.” hükmü çerçevesinde veri sorumluların **Kurulun bilgi belge talebine ilişkin cevap verilmesinde gerekli dikkat ve özenin gösterilmesi hususunda talimatlandırılmasına** karar verilmiştir.

2021/407 sayılı KVKK Kararı

Bir hastanenin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 20/04/2021 tarih ve 2021/407 sayılı Karar Özeti

Karar Tarihi : 20.04.2021

Karar No : 2021/407

Konu Özeti : Bir hastanenin veri ihlali bildirimini

Veri sorumlusu bir hastane tarafından Kuruma intikal ettirilen veri ihlal bildiriminde;

- Veri ihlalinin; hastanede çalışan hekimin hastalarına ait dosyaların arşivden alınarak kendisinin talimatıyla bazı hastane çalışanları aracılığıyla hastane dışına çıkarılmasıyla gerçekleştiği,
- Veri ihlalinin; dosyaları hastane dışına çıkarmaya teşebbüs eden bir çalışanın görülmesinden 17 gün sonra kamera kayıtlarının incelenmesi neticesinde tam olarak tespit edildiği,
- İhlalden; 789 hastanın etkilendiği,
- İhlalden; kimlik, iletişim, sağlık bilgileri ve genetik verilerin hasta kartında yer alan bilgiler (T.C Kimlik numarası, adı, soyadı, baba adı, ana adı, sosyal güvenlik numarası, özel sigorta, anlaşmalı kurum, çalıştığı kurum, uyruğu, doğum tarihi, cinsiyet, medeni hali, kan grubu, mesleği, vergi dairesi, vergi numarası, adres, posta kodu, e-posta, ev telefonu, iş telefonu, cep telefonu, son randevu cep ve ev telefonu, sigortalı durumu, emekli olup olmadığı, poliçe no, engel durumu, çalışan adı, tedavi olunan doktorlar ve branşlar gibi bilgiler) ile hasta dosyası anamnez içeriğinin (kullandığı ilaçlar, alışkanlıklar, alerjik öyküsü, soygeçmiş, psikolojik durum, bulgular, laboratuvar tetkikleri, öntanı, tanı, tedavi ve bakım planı, geçirmiş olunan hastalıklar, ameliyatlar vb. bilgiler) etkilendiği ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 20/04/2021 tarih ve 2021/407 sayılı Kararı ile,

- İhlalden 789 hastanın etkilendiği ancak karakol tutanağına göre tespit edilen 54 adet hasta dosyasının geri alınarak yedieminliğe teslim edildiği, geri kalan dosyaların akıbetinin ise bilinmediği dikkate alındığından hasta dosyalarının kaybolması durumunun önlenemediği ve bu durumun söz

konusu hasta dosyalarının kaybolmasına yönelik risklerin azaltılmasına dair yeterli tedbirlerin alınmadığını gösterdiği,

- İhlalden; kimlik, iletişim, lokasyon, özlük, genetik veri, sağlık verileri gibi veri kategorilerine ait çok sayıda kişisel verinin ve özel nitelikli kişisel verinin etkilenmiş olduğu hususunun ilgili kişilerin ihlal sebebiyle önemli olumsuz etkilere maruz kalmaları olasılığının bulunduğu göstergesi olduğu,

- İhlal ile ilgili olan çalışanların, sağlık verileri ve genetik veriler de dahil olmak üzere özel nitelikli çok sayıda kişisel verinin işleme sürecinde yer aldığı göz önünde bulundurulduğunda; veri sorumlusu tarafından çalışanlara tanımlanan kişisel verilerin korunması eğitiminin tamamlanmasının sağlanmadığı, eski çalışanın kişisel verilerin korunması ile ilgili eğitim almış olmasına rağmen arşiv odasındaki belgelerin taşınmasına yardım ettiğinin anlaşıldığı dikkate alındığında Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kararında yer alan "Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik, a) Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi,...gerekir." ifadesine aykırı olarak veri sorumlusu tarafından çalışanlara kişisel verilerin korunmasına yönelik yeterli eğitimin verilmediğinin göstergesi olduğu,

- İhlal şüphesini doğuran olayların bulunmasına rağmen; ihlalin 17 gün sonra tespit edilmesinin veri sorumlusu tarafından kişisel veri güvenliği politika ve prosedürlerinin iyi bir şekilde hazırlanmadığı veya takip edilmediği, ayrıca bu durumun alınan mevcut güvenlik önlemlerinin etkili kullanılmadığı hususlarının göstergesi olduğu

- İhlali gerçekleştiren ve diğer çalışanların Başhekimliğin izni ve onayı bulunmaksızın, eski çalışanın ve aynı yerde yer alan bir şirket çalışanın arşiv odasına girebildiği ve hasta dosyalarını dışarı çıkarabildiği, ayrıca söz konusu durumun kamera kayıtlarında görülmesine rağmen 1 ayı aşkın süre boyunca ihlalin devam ettiği ve kamera kayıtlarının ancak ihlal anlaşıldıktan sonra kontrol edildiği hususunun Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kararında yer alan "... Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi...gerekir." ifadesine aykırı olarak kamera kayıtlarının kontrolünün ve hastalara ait kayıtların tutulduğu arşiv odasına yetkili olmayan kişilerin girmemesini sağlayacak yeterli idari tedbirlerin alınmadığını gösterdiği,

- İhlalin gerçekleşmesinden önce, Kişisel Verileri Koruma ve Bilgi Güvenliği Kurulu oluşturulmasına, Veri İhlali Müdahale Planı hazırlanmasına ve KVKK kapsamında ilgili kişilerden

veya kurumlardan gelecek talepleri karşılamak üzere algoritma oluşturulmasına rağmen; yedieminliğe teslim edilen hasta dosyalarının hastane arşivindekilerden daha fazla veri içerdiğinin ihlalden sonra tespit edildiği hususlarının Kişisel Veri Güvenliği Rehberi'nin "Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Belirlenmesi" başlığı altında yer alan "Kişisel veri güvenliğine ilişkin belirlenecek doğru ve tutarlı politika ve prosedürler, veri sorumlusunun çalışma ve işleyişine uygun şekilde entegre edilmelidir. Veri sorumlularınca politika ve prosedürler iyi bir şekilde ve zamanında hazırlanamadığında, sorunlu alanlar belirlenemediğinde veya mevcut güvenlik önlemleri kullanılmadığında kişisel veri güvenlik seviyesi yeteri kadar sağlanamamaktadır." ifadelerinde yer aldığı üzere; veri sorumlusu tarafından alınan mevcut güvenlik önlemlerinin iyi bir şekilde hazırlanmaması veya kullanamaması nedeniyle ihlalin tespit edilmesi ve önlenmesine yönelik tedbirlerin zamanında ve yeterli ölçüde alınmadığı,

- İzinsiz olarak hastaneden çıkarılan birçok hasta dosyasının akıbetinin halen bilinmemesinin "Kişisel Veri Güvenliği Rehberi'nin "Mevcut Risk ve Tehditlerin Belirlenmesi" başlığı altında yer alan "Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir. Bu riskler belirlenirken; Kişisel verilerin özel nitelikli kişisel veri olup olmadığı, Mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği, Güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği dikkate alınmalıdır. Bu risklerin tanımlanması ve önceliğinin belirlenmesinden sonra; söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmeli, gerekli teknik ve idari tedbirler planlanarak uygulamaya konulmalıdır ..." ifadelerine aykırı olarak hasta dosyalarının kaybolması durumunun önlenemediği veya kaybolması halinde risklerin azaltılmasına dair yeterli tedbir alınmadığını gösterdiği

dikkate alındığında Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 450.000 TL,

- İhlalin tespit edilmesinden 25 gün sonra Kuruma bildirildiği,

- İlgili kişilerden hastaneye gelen bir kişi dışında, hiç birine ihlalin bildirilmemiş olduğu

hususları dikkate alındığında Kanunun 12 nci maddesinin (5) numaralı fıkrası hükmü ve Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararında yer alan 'en kısa sürede' ifadesinin 72 saat olarak yorumlanmasına yönelik ifadeleri çerçevesinde bildirim yükümlülüğünü yerine getirmeyen veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 150.000 TL olmak üzere toplam 600.000 TL idari para cezası uygulanmasına,

İlgili kişilere Kurulun 24.01.2019 tarih ve 2019/10 sayılı Kararında yer alan hususları içeren bir bildirim yapılarak sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2021/389 sayılı KVKK Kararı

Bir sigorta şirketi tarafından hizmetin açık rıza şartına bağlanması hakkındaki ihbar ile ilgili olarak Kişisel Verileri Koruma Kurulunun 20/04/2021 tarihli ve 2021/389 sayılı Karar Özeti

Karar Tarihi : 20.04.2021

Karar No : 2021/389

Konu Özeti : Bir sigorta şirketinin hizmeti açık rıza şartına bağlaması hakkında ihbar

Kuruma intikal eden bir ihbarda; ihbar eden ilgili kişinin bir sigorta şirketinden (Şirket) bireysel emeklilik sözleşmesi (BES) yaptırdığı, Şirketin internet sayfasından poliçe bilgilerine ulaşmak için giriş yapmaya çalıştığı bir onay kutucuğu sunularak kişisel verilerin işlenmesine rıza göstermek zorunda bırakıldığı, bu kutucuğu işaretlememesi halinde hiçbir işlem yapamayacağını anlaşıldığı, ancak kişisel verilerinin işlenmesine onay vermek zorunda bırakılmasının hukuka aykırı olduğu belirtilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle,

- İnternet sayfası üzerinden müşterinin kim olduğunun anlaşılması, kimlik doğrulamasının yapılabilmesi, tazminat taleplerinin alınabilmesi, poliçe/sözleşme ve teminatlarının kontrolü, hasar takibi, müşteri talebi doğrultusunda ya da otomatik olarak müşteriye e-posta ile bilgilendirme yapılması amaçlarına yönelik müşterilere ait kişisel veri ve özel nitelikli kişisel verilerin işlenebildiği, bu kişisel verilerin ise kimlik numarası, telefon numarası, doğum tarihi, baba adı, kişiye ait sağlık bilgileri, sağlık hizmeti faturaları ve buna bağlı sağlık harcama bedeli talepleri, e-posta adresi olarak sıralanabileceği ve bu verilerin Kanununun 5 inci maddesinin birinci fıkrası uyarınca, ilgili kişinin açık rızası olması halinde ve yine anılan maddenin ikinci fıkrasına göre açık rızanın aranmayacağı taahhidi olarak belirtilen hallerde Kanuna uygun olarak işlendiği,
- İnceleme konusu olan uygulamanın ilgili hizmetlerin verildiği tek mecra olmadığı ve söz konusu hizmetlerin kişisel verilerin işlenmesinde alınan açık rıza şartına bağlanmadığı,

- Şirketin hem kişisel verilerin korunmasına ilişkin mevzuat çerçevesinde hem de ticari elektronik iletiler hakkında mevzuat gereği, kişisel verileri işleme kapsam ve koşulları konusunda ilgilileri aydınlatma/bilgilendirme ve gerektiğinde bu aydınlatmanın yapıldığını da ispat etme yükümlülüğü bulunduğu, bu sebeple uygulama girişinde ilgililere aydınlatma metni ileildiği, sağlık verileri başta olmak üzere yukarıda belirtilmiş olan kişisel verilerin işlenmesi söz konusu olabileceğinden, bir kez sisteme bağlanan bir kullanıcının, web üzerinden sunulmakta olan başka hizmet(ler)i de almak isteyebileceğinin önceden öngörülmesi mümkün olmadığından, açık rıza talep edilmesi gerektiğinin düşünüldüğü,

- Şirket tarafından internet sayfası üzerinden sunulmakta olan ürün ve hizmetlere asıl erişimin Türkiye'nin hemen her noktasında faaliyet gösteren sigorta acenteleri aracılığı ile sağlandığı, çağrı merkezinin de müşterilere kesintisiz olarak hizmet verdiği; ayrıca, başka bir alternatif olarak da Şirketin kurumsal internet sayfası ve mobil uygulamaları ile müşterilere bir takım ürünlere elektronik ortamdan da erişme imkânı sunulduğu, dolayısıyla Şirketin internet sayfası üzerinden sunulan çeşitli hizmetlere ulaşılabilecek başka mecra ve kanalların da mevcut olduğu,

- Şirketin açık rıza bildirim ve aydınlatma bildirimlerinin internet sayfasında yer alan iki ayrı linkte yer aldığı

ifade edilmiştir.

Söz konusu ihbar dilekçesindeki iddialar, veri sorumlusunun savunması ve ilgili mevzuat hükümlerinin birlikte incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 20/04/2021 tarih ve 2021/389 sayılı Kararı ile;

A. Aydınlatma Metninin Mevzuata Uygunluğuna İlişkin Olarak:

- 6698 sayılı Kanununun 10 uncu maddesi uyarınca kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişinin ilgili kişileri kişisel verilerin işleme faaliyeti hakkında anılan maddede yer verilen unsurları içerecek şekilde bilgilendirmesi ve bu kapsamda, Kanununun 10 uncu maddesinde yer alan aydınlatma yükümlülüğünün, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ (**Tebliğ**) hükümlerine uygun olarak yerine getirilmesi gerektiği,

- Tebliğin 4 üncü maddesinde; aydınlatma yükümlülüğünün kapsamının, 5 inci maddesinde ise veri sorumlusunun aydınlatma yükümlülüğünü yerine getirirken uyması gereken hususların düzenleme altına alındığı,

- Sigorta faaliyetleri çerçevesinde sigortacının müşteriye karşı olan yükümlülüklerini ifa edebilmesi için çeşitli kişisel verilerin işlenmesi gerekli olabileceğinden, söz konusu kişisel verilerin işlenmesinde Kanuna ve Tebliğe uygun aydınlatmanın yapılmasının önem arz ettiği, Şirketin cevabi yazısında belirttiği linklerde, “Online İşlemler” sayfasında sisteme giriş için doldurulması gereken kutucukların alt kısmında “Gizlilik ve Kişisel Verilerin Korunması Esasları’nı okudum, kabul ediyorum. Burada paylaşmış olduğum kişisel/özel nitelikli kişisel verilerimin 6698 sayılı Kişisel Verilerin Korunması Kanunu ve sair mevzuat çerçevesinde işlenmesine açık rıza veriyorum.” ifadesine yer verildiği, “Gizlilik ve Kişisel Verilerin Korunması Esasları” ibaresinin üzerine tıklandığında ise aydınlatma metninin açıldığının tespit edildiği, veri sorumlusunun cevabi yazısında belirtilmiş olan her iki linkte de yer alan aydınlatma metinleri incelendiğinde, söz konusu metinlerin birebir aynı olduğunun anlaşıldığı,
- Bu çerçevede her iki aydınlatma metninde de “D-Kişisel Verileriniz Toplama Yöntemi ve Hukuki sebebi” başlığı altında “Sigorta poliçeleri ve emeklilik sözleşmelerinin taraflarına ait kişisel/özel nitelikli kişisel veriler; acentelerimiz, internet uygulamalarımız ve çağrı merkezimiz aracılığı ile doğrudan doğruya sizlerden ve sigorta sözleşmelerinden kaynaklanan yükümlülüklerin yerine getirilebilmesi için kamu kurumları tarafından tarafımıza erişim yetkisi verilen veri tabanlarından derlenmektedir.” ifadelerine yer verildiğinin görüldüğü,
- Metnin devamında kişisel verileriniz, “6698 sayılı Kişisel Verilerin Korunması Kanunu ve sair mevzuat çerçevesinde sadece sigortacılık faaliyetlerinin yürütülmesi amacı ile ve bu amacın gerektirdiği yasal sürelerle sınırlı olarak işlenmektedir.” şeklinde açıklama yapıldığı, ancak Tebliğin 5 inci maddesinin birinci fıkrasının (h) bendinde de düzenlendiği üzere, Kanunun 10 uncu maddesinin birinci fıkrasının (ç) bendinde yer alan “hukuki sebep”ten kastın, aydınlatma yükümlülüğü kapsamında kişisel verilerin Kanunun 5 ve 6 ncı maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiği olduğu, bu anlamda hukuki sebep olarak Kanunda düzenlenen 5 inci veya 6 ncı maddelerden hangisine veya hangilerine dayanıldığına ilişkin bir bilgilendirmede bulunulmadığının anlaşıldığı,
- Bununla birlikte, mezkûr metnin “C-Kişisel Verilerinizi Kimlere ve Hangi Amaçla Aktarıyoruz?” başlığı altında geçen “sigortacılık ve sair mevzuat” ibaresinin muğlak olduğu, zira kişisel verilerin aktarımı hangi mevzuat kapsamında gerçekleştiriliyor ise ayrı ayrı açıkça belirtilmesi gerektiği, ayrıca metinde yer alan kurum ve kuruluşların isimlerinin de güncellenmediğinin anlaşıldığı,
- Diğer taraftan, ihbar edenin başvurusuna konu online sisteme veri sorumlusunun hizmetlerinden faydalanmak amaçlı üyelik kurulduktan sonra müşteriye ait TC kimlik numarası ile cep telefonu numarasının girilmesi sureti ile giriş yapılabildiğinin görüldüğü, sisteme giriş için doldurulması gereken kutucuğun alt kısmında yer alan “Gizlilik ve Kişisel Verilerin Korunması Esasları’nı okudum,

kabul ediyorum. Burada paylaşmış olduğum kişisel/özel nitelikli kişisel verilerimin 6698 sayılı Kişisel Verilerin Korunması Kanunu ve sair mevzuat çerçevesinde işlenmesine açık rıza veriyorum.” ifadesine yer verildiği, dolayısıyla tek bir kutucuk işaretlendiğinde ilgili kişinin hem aydınlatma metnine hem de kişisel verilerinin işlenmesine onay verdiği, ancak Tebliğin 5 inci maddesinin birinci fıkrasının (f) bendine göre, kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerektiğinin hüküm altına alındığı, dolayısıyla kişisel verilerin işlenmesinin hukuki sebebinin açık rıza olduğu durumlar için ayrı bir açık rıza metninin de oluşturulması gerektiği

B. Açık Rızanın Hizmet Şartına Bağlanıp Bağlanmadığına İlişkin Olarak:

- Kanunun “Tanımlar” başlıklı 3 üncü maddesinin birinci fıkrasının (a) bendinde açık rızanın, “belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza” şeklinde tanımlandığı, bu anlamda açık rızanın öncelikle belirli bir konuya ilişkin ve o konu ile sınırlı olarak verilmesi bu doğrultuda veri sorumlusu tarafından açık rıza beyanının hangi konuya ilişkin olarak istenildiğinin açıkça ortaya konulması gerektiği, diğer bir deyişle, açık rıza beyanının genel nitelikte olmaması, belirli bir konuya özgülenmiş ve o konu ile sınırlı olması gerekmekte olup, açık uçlu veri işleme faaliyetlerine ilişkin rıza alınamayacağı, bununla birlikte, açık rıza bir irade beyanı olduğundan, kişinin özgür bir şekilde rıza gösterebilmesi için, neye rıza gösterdiğini de bilmesi gerektiği ayrıca kişinin sadece konu üzerinde değil, aynı zamanda rızasının sonuçları üzerinde de tam bir bilgi sahibi olmasının beklenildiği, bu sebeple, bilgilendirmenin, veri işleme ile ilgili bütün konularda açık ve anlaşılır bir biçimde gerçekleştirilmesi ve mutlaka verinin işlenmesinden önce yapılmasının önem arz ettiği, diğer yandan, açık rızanın geçerlilik kazanabilmesi için kişinin yaptığı davranışın bilincinde ve kendi kararı olması gerektiği, bu çerçevede açık rızanın özgür iradeyle açıklanması gerektiğinden, herhangi bir ürün ve/veya hizmetin sunumunun da (ya da herhangi bir üründen ve/veya hizmetten yararlandırılması) ilgili kişi tarafından açık rıza verilmesi şartına bağlanmaması, tarafların eşit konumda olmadığı veya taraflardan birinin diğeri üzerinde etkili olduğu durumlarda rızanın özgür iradeyle verilip verilmediğinin dikkatle değerlendirilmesi gerektiği,

- Diğer taraftan, kişisel verilerin işleme şartlarının düzenlendiği Kanunun 5 inci maddesinin birinci fıkrasında; kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, bununla birlikte ikinci fıkrasında belirtilen şartlardan (-Kanunlarda açıkça öngörülmesi, -Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, -Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin

tarafına ait kişisel verilerin işlenmesinin gerekli olması, -Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, -İlgili kişinin kendisi tarafından alenileştirilmiş olması, -Bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması, -İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması) birinin varlığı halinde ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğunun hükme bağlandığı,

- Bununla birlikte, Kanunun “Genel ilkeler” başlıklı 4 üncü maddesinde, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği, bu çerçevede kişisel verilerin işlenmesinde “a) Hukuka ve dürüstlük kurallarına uygun olma. b) Doğru ve gerektiğinde güncel olma. c) Belirli, açık ve meşru amaçlar için işlenme. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.” şeklinde sayılan ilkelere uyulmasının zorunlu olduğunun düzenleme altına alındığı, anılan madde hükmünden açıkça anlaşılacağı üzere, kişisel verilerin işlenmesinde her hal ve şartta Kanunun 4 üncü maddesinde sayılan genel ilkelere uyulmasının hukuki bir gereklilik olduğu,

- Öte yandan, 4682 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanununun (4682 sayılı Kanun) “Emeklilik sistemine katılma ve emeklilik sözleşmesi” başlıklı 4 üncü maddesinin birinci fıkrasına göre;

“(…) Sisteme katılmak için şirket ile emeklilik sözleşmesi akdedilir. Emeklilik sözleşmesi; şirket nezdinde bireysel emeklilik hesabı açılması, hesaba katkı payı ödenmesi, ödenen katkı paylarının tercih edilen fonlarda yatırıma yönlendirilmesi ve hesapta biriken paraların hak sahiplerine ödenmesine ilişkin esas ve usuller ile tarafların bu kapsamdaki diğer hak ve yükümlülüklerini düzenleyen sözleşmedir. Emeklilik sözleşmesi, katılımcı ile bireysel emeklilik sözleşmesi şeklinde veyahut bir istihdam ilişkisine dayalı olarak veya katılımcı adına bir kuruluş ile grup emeklilik sözleşmesi şeklinde yapılabilir. Emeklilik sözleşmesine ve emeklilik sözleşmesinde bulunacak hususlara ilişkin esas ve usuller Kurulun görüşü alınarak Müsteşarlık tarafından belirlenir.”

hükmünün düzenlendiği, 09.11.2012 tarihli Resmi Gazetede yayımlanan Bireysel Emeklilik Sistemi Hakkında Yönetmeliğin (BES Yönetmeliği) 3 üncü maddesinin birinci fıkrasının (z) bendine göre teklif formunun, emeklilik planına, plan kapsamında sunulan fonlara, yapılan kesintilere, katkı payı tutarına, emeklilik sözleşmesinin taraflarına ve katılımcının yatırım tercihlerine ilişkin hususlar ile benzeri bilgileri içeren form olarak tanımlandığı, yine, anılan Yönetmeliğin “Bilgilendirme, teklif ve sözleşmenin düzenlenmesi” başlıklı 5 inci maddesinde;

“Bilgilendirme, teklif ve sözleşmenin düzenlenmesi

MADDE 5 - (1) Şirket, bireysel emeklilik sistemine girmek isteyenlere, sisteme girme kararını etkileyebilecek hususlar hakkında bilgi verir; dürüstlük ilkeleri çerçevesinde, emeklilik sözleşmesinin müzakeresi ve düzenlenmesi sırasında katılımcıya veya sözleşmeyi düzenleyen sponsora veya işverene sistemin işleyişine ilişkin teknik konularda yardımcı olur, tarafların hak ve yükümlülüklerine ilişkin gerekli her türlü bilgiyi sağlar, yanıltıcı her türlü hâl ve davranıştan kaçınır. Bakanlık ilgililere yapılacak bilgilendirmenin asgari içeriğini ve yöntemini belirler.

(2) Şirket, kişinin emekliliğe yönelik beklentilerine, gelir düzeyine ve yaşına uygun bir emeklilik planı teklifi sunar. (...)"

hükmünün yer aldığı,

- Bu çerçevede, veri sorumlusunun internet sitesinde yer alan "Bireysel Emeklilik Sözleşmesi Teklif Formu"nun (Teklif Formu) incelenmesinden "İnternet Ortamında Sunulacak Hizmetlere İlişkin Hükümler" başlığı altında yer verilen ifadelerden ilgili kişi ile veri sorumlusu arasında akdedilen Hizmet Sözleşmesi ile ihbar konusu uygulamanın kullanımında talep edilen verilerin veri sorumlusunun internet üzerinden sunduğu hizmetlerde şifre dışında geliştirilen bir yöntem olarak görülebileceği, bu durumda, veri sorumlusunun anılan kişisel veriler için Kanunun 5 inci maddesinin ikinci fıkrasında yer alan "Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması" veri işleme şartına dayanacağı değerlendirildiğinden hizmetin açık rıza şartına bağlanmasından söz edilemeyeceği, bununla birlikte ihbara konu olayda söz konusu uygulamanın kullanımı için sunulan aydınlatma metninde aynı zamanda kişisel verilerin işlenmesi için açık rıza alındığı, dolayısıyla veri sorumlusunun savunmasında açık rıza ve aydınlatma kavramlarını iç içe geçmiş belirsiz bir biçimde kullandığının görüldüğü, bu noktada söz konusu kişisel veri işleme faaliyetinin hukuki sebebinin açık bir şekilde ifade edilmesinin veri sorumlusunun yükümlülüğü olduğunun altının çizilmesi gerektiği,

- Ayrıca söz konusu kişisel veri işleme faaliyeti, Kanunda yer alan açık rıza dışındaki şartlardan birine dayanıyorsa, bu durumda ilgili kişiden açık rıza alınmasına gerek bulunmadığı ve veri işleme faaliyetinin, açık rıza dışında bir dayanakla yürütülmesi mümkün iken açık rızaya dayandırılmasının, aldatıcı ve hakkın kötüye kullanımı niteliğinde olacağı ve bu durumun ise Kanunun 4 üncü maddesinin ikinci fıkrasının (a) bendinde düzenlenen "hukuka ve dürüstlük kurallarına uygun olma" ilkesine aykırılık teşkil ettiği

değerlendirmelerinden hareketle,

- Kanunun 5 inci maddesinde yer alan diğer işleme şartları mevcut iken ilgili kişilerin açık rızasının alınmasının Kanunun 4 üncü maddesinde yer alan “hukuka ve dürüstlük kurallarına uygun olma” ilkesine aykırı olduğu dikkate alındığında Kanunun 12 nci maddesinin (1) numaralı fıkrasında yer alan yükümlülüklerini yerine getirmeyen veri sorumlusu hakkında, Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca söz konusu uygulamanın ihbar eden dışında pek çok kişi üzerinde olumsuz etki doğurabileceği, veri sorumlusunun sunduğu hizmet bakımından geniş bir müşteri kitlesi bulunduğu, Şirketin kusuru, ekonomik durumu ve haksızlık içeriği gibi hususlar da göz önünde bulundurularak 250.000 TL idari para cezası uygulanmasına,
- Açık rıza alınması ile ilgili kişiye aydınlatma yapılması tek bir onaya bağlandığından açık rıza ve aydınlatma metinlerinin ayrı ayrı düzenlenmesi ve sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına,
- Aydınlatma metninde muğlak ifadeler yer verildiği dikkate alındığında veri sorumlusunun aydınlatma yükümlülüğünü Kanun ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümleri ile uyumlu olacak şekilde düzenlenmesi ve sonucundan Kurula bilgi verilmesi hususunda talimatlandırılmasına

karar verilmiştir.

2021/361 sayılı KVKK Kararı

Bir bankanın mobil uygulamalar üzerinden ilgili kişiye rızası dışında tanıtım iletileri göndermesi hakkında Kişisel Verileri Koruma Kurulunun 13/04/2021 tarihli ve 2021/361 sayılı Karar Özeti

Karar Tarihi : 13.04.2021

Karar No : 2021/361

Konu Özeti : Bir bankanın mobil uygulamalar üzerinden ilgili kişiye rızası dışında tanıtım iletileri göndermesi

Kuruma intikal eden şikâyet dilekçesinde özetle; ilgili kişinin maaş müşterisi olduğu veri sorumlusu banka tarafından sunulan 2 adet mobil uygulama üzerinden cep telefonuna tanıtım iletileri gönderildiği, veri sorumlusunun tanıtım iletileri gönderme işlemi sırasında 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunun (6563 sayılı Kanun) 6 ncı maddesi ile 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) ilgili maddeleri kapsamında ilgili kişinin açık rızasına başvurmadığı ve veri sorumlusu tarafından Kanunun 12 nci maddesi uyarınca kişisel verilerin hukuka aykırı biçimde işlenmesini önlemek adına gerekli teknik ve idari tedbirlerin alınmadığı, ilgili kişinin, tanıtım iletilerinden dolayı duyduğu rahatsızlığı dile getirmek üzere veri sorumlusuna yazılı başvuruda bulunduğu, ancak bu başvurunun cevabının gelmesinden önce veri sorumlusuyla çağrı merkezi üzerinden de iletişime geçerek tanıtım iletilerinin gönderilmesine konu olan kişisel verilerinin silinmesi talebini ilettiği, yapılan sözlü ve yazılı başvuruların ardından, ilgili kişinin veri sorumlusundaki hesabı ile kredi kartlarının tamamen iptal edildiği, ilgili kişinin veri sorumlusuna yaptığı ikinci başvuruda iptal sebebini sorduğu ve kendisine Kanun kapsamındaki talebi sebebiyle söz konusu iptal işleminin gerçekleştirildiği bilgisinin verildiği, hesabının silinmesi işleminin ilgili kişiyi maddi ve manevi zarara uğrattığı ve başlangıçtaki başvurusunun karşılanmamasının yanı sıra, hesabının kapatılmasının ikinci bir hukuka aykırılık teşkil ettiği belirtilerek veri sorumlusu hakkında gerekli incelemelerin yapılması ve idari para cezası uygulanması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, verilen cevapta özetle;

- Mobil uygulamaların, müşterilere yönelik pazarlama amaçlı tesis edilen bir iletişim kanalı olarak kullanıldığı ve bu uygulamaların ayarlarında, kullanıcıların ileti almamaya ilişkin tercih hakkının bulunduğu,
- Kullanıcıların akıllı telefonlarına uygulamayı indirdikten sonra, tanıtım iletisi gönderilmesi için tercihlerinin istenildiği ve izin verilmesi durumunda kendilerine pazarlama içerikli bildirimlerin gönderildiği,
- Kullanıcıların bu bildirimlere en başta izin vermeme veya herhangi bir zamanda bu bildirimleri kapatma haklarının her zaman mevcut olduğu,
- Şikâyete konu olayda, ilgili kişinin uygulama ayarlarını bildirim almaya izin verecek şekilde düzenlemesi neticesinde kendisine tanıtım iletilerinin gönderildiği,
- İlgili kişinin veri sorumlusuna yaptığı başvuruda Kanunun 11 inci maddesinin (1) numaralı fıkrasının (e) bendi uyarınca kişisel verilerinin silinmesini veya yok edilmesini istemesi üzerine, Kanunun 7 nci maddesinin (1) numaralı fıkrası uyarınca işlem yapılabilmesi için ilgili kişinin hesabının ve kredi kartlarının kapatıldığı,
- İlgili kişiye ait kişisel verilerin, Kanunun 5 inci maddesinin (2) numaralı fıkrasında yer verilen “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” ve “Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması” şartları kapsamında işlendiği ve yine kendisinin talebi doğrultusunda silindiği,
- Hesabının kapatılması sonrasında ilgili kişinin veri sorumlusuna tekrar başvuruda bulunduğu ve kendisine yeniden hesap açıldığı,
- Hesabının kapatılması neticesinde ilgili kişi açısından bir zararın oluşmadığının tespit edildiği bildirilmiştir.

Konuya ilişkin yapılan incelemede Kişisel Verileri Koruma Kurulunun 13/04/2021 tarih ve 2021/361 sayılı Kararı ile;

- 6698 sayılı Kanunun kişisel verilerin işlenmesine ilişkin “Genel İlkeler”i düzenleyen 4 üncü maddesinin (1) numaralı fıkrasında, “Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.” hükmü yer almakta olup bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin; (a) Hukuka ve dürüstlük kurallarına uygun olma, (b) Doğru ve gerektiğinde güncel olma, (c) Belirli, açık ve meşru

amaçlar için işlenme, (ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, (d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,

- Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanunun “Veri Güvenliğine İlişkin Yükümlülükler”i düzenleyen 12 nci maddesinin (1) numaralı fıkrasında ise veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idarî tedbirleri almak zorunda olduğunun hükme bağlandığı,

- Somut olayda cihazlarında Android işletim sistemi bulunan veri sorumlusu banka müşterilerinin, yükledikleri bankacılık uygulamasının ayarlarında elektronik ileti alma tercihinin otomatik olarak onaylı olmasının ve müşterilerin bu tercihi değiştirmedeği sürece onay tercihinin geçerli kabul edilmesinin ilgili mevzuata uygun olmadığı,

- Zira hizmet sunucuları tarafından mobil uygulamalar üzerinden kullanıcılara anlık olarak gönderilen ve “push bildirim” olarak adlandırılan bu tarz bildirimlerin mobil uygulamaların varsayılan ayarlarında onaylı olarak bulunmasının hem 6563 sayılı Kanunda belirtilen elektronik iletilerin alıcıların onaylarına tabi olacağı düzenlemesiyle çeliştiği hem de Kanunun 5 inci maddesinde yer verilen kişisel verilerin işlenmesinde açık rızaya dayanma şartını ihlal ettiği,

- Çok sayıda yerel şubesinin ve müşterisinin yanı sıra yurt dışı iştirak şubeleri de bulunan veri sorumlusunun bahsi geçen tasarrufu sebebiyle hukuka aykırı kişisel veri işleme faaliyetinin yaygın bir biçimde meydana geldiği ve ilgili kişi olan müşteriler bakımından veri güvenliği riskinin mevcut olduğu,

- Veri sorumlusunun, Android işletim sistemi kullanıcılarına yönelik olarak işletmekte olduğu mobil uygulamalar üzerinden tanıtım iletisi gönderme seçeneğini, açık rızanın Kanunda yer alan bütün unsurlarına yer verecek şekilde yeniden düzenlemesi ve bu kapsamda uygulamanın varsayılan ayarlarını tanıtım iletisi almama biçiminde kullanıma sunması gerektiği,

- Veri sorumlusunun ilgili kişilerden usulüne uygun şekilde açık rıza almaksızın tanıtım iletisi göndermek suretiyle hukuka aykırı olarak kişisel veri işleme faaliyetinde bulunmasının Kanunun 12 nci maddesinin (1) numaralı fıkrasında zikredilen uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığını gösterdiği

değerlendirmelerinden hareketle;

- Veri sorumlusunun mobil uygulamalar üzerinden usulüne uygun açık rızası alınmaksızın tanıtım iletileri göndermek amacıyla ilgili kişinin kişisel verilerini işleminin hukuka aykırı olduğu dikkate alındığında, Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı kanaatine varılan veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca idari para cezası uygulanmasına,

- Bununla birlikte veri sorumlusunun sahibi olduğu mobil uygulama süreçlerini usulüne uygun açık rıza alınabilecek şekilde düzenlemesi ve bu işlemin sonucundan Kurula bilgi verilmesi yönünde veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2021/359 sayılı KVKK Kararı

İlgili kişinin kişisel verilerinin site yönetim hizmetini sağlayan veri sorumlusu şirket tarafından bir mobil uygulama ile hukuka aykırı olarak paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 13/04/2021 tarihli ve 2021/359 sayılı Karar Özeti

Karar Tarihi : 13.04.2021

Karar No : 2021/359

Konu Özeti : İlgili kişinin kişisel verilerinin ikamet ettiği sitede yönetim hizmetleri veren veri sorumlusu şirket tarafından bir mobil uygulama ile hukuka aykırı olarak paylaşılması

İlgili kişinin Kuruma intikal eden şikayetinde özetle; oturduğu sitenin yönetiminden sorumlu şirketin kendisine ait telefon numarasını yönetim hizmetleri kapsamında kullanılan bir mobil uygulama ile rızası dışında paylaştığı ve ilgili uygulamadan kendisine bilgi mesajı gönderildiği belirtilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gerekli yaptırımların uygulanması talep edilmiştir.

Konuya ilişkin olarak başlatılan inceleme çerçevesinde ilgili sitenin yönetim işlemlerini yürüten şirket (Site Yönetim Hizmeti Sunan Şirket) ile aktarım yapılan uygulama ile ilgili hizmeti sunan şirketin (Uygulama Hizmeti Sunan Şirket) savunmaları istenilmiştir.

Bu kapsamda Yönetim Hizmeti Sunan Şirketten alınan cevabi yazıda özetle;

- İlgili kişinin ikamet ettiği Sitenin Temsilciler Kurulu ile Şirketleri arasında hizmet sözleşmesinin bulunduğu, mezkur sözleşme kapsamında yükümlülüklerinin Kat Mülkiyeti Kanunu ve Site Yönetim Kurulu kararlarına uygun olacak şekilde; sitenin ortak alanlarında çalışacak personelin tahsisi ve çalıştırılması, site yönetim faaliyetlerine danışmanlık verilmesi, sitenin finansal durumunun analizi ve bilanço hazırlanması, site denetim kurulunun denetim işlemleri sırasında refakat edilmesi, sitenin gelir-gider muhasebe işlemlerinin usule uygun olarak yapılması olduğu,
- Dolayısıyla Şirketlerinin, bir yönetim firması olduğu ve yönetim firması olması sebebiyle hizmetlerini sunarken birçok yönetim programından yararlandığı, kişisel verilerin aktarıldığı iddia edilen uygulamanın da Şirketin bu anlamda yönetim hizmetlerini verirken kullandığı bir program

olduğu, site sakinlerinin kişisel verilerinin kesinlikle üçüncü kişilerle paylaşılmadığı, muhtemel olarak ilgili kişinin kendisinin programa kaydolduğundan SMS ile bilgilendirme aldığı,

- Söz konusu uygulamayı sunan Şirket ile aralarında hizmet sözleşmesi bulunduğu, ilgili kişiye ait kişisel verilerin mezkur uygulamaya aktarılması ya da uygulamaya kaydının taraflarınca yapılması gibi bir durumun söz konusu olmadığı, Şirketlerine üçüncü bir taraftan gelen yüksek meblağlı bir ürünle ilgili indirim site sakinlerince yönetim hizmetlerinin gerçekleştirilmesi için hali hazırda kullanılan bir uygulama (ilk uygulama) üzerinden site sakinlerine bilgi verme amaçlı olarak bildirildiği, kişisel verilerin aktarıldığı iddia edilen yeni uygulamaya (ikinci uygulama) üye olmayı gerektiren bu indirimden yararlanabilmenin tamamen ilgili kişinin inisiyatifinde olduğu, ilgili kişinin kendi seçimi ile yeni uygulamaya/ikinci uygulamaya kaydolduğu, bu çerçevede aydınlatılmanın söz konusu uygulama ve ilgili kişinin arasında bir durum olduğu,

İlgili kişinin mezkur uygulamaya kaydının Şirketlerince yapılmadığı, ilgili kişinin uygulamaya kendi özgür iradesiyle kayıt olduğu şeklinde açıklamalara yer verilmiş ve yazıları ekinde hem halihazırda kullanılan ilk uygulama hizmetini sunan şirket hem de şikayet konusu kişisel verilerin aktarıldığı iddia edilen ikinci uygulama hizmetini sunan şirket ile imzalanan hizmet sözleşmelerine ve taraflar arasındaki KVKK Protokolüne yer verildiği görülmüştür.

Şikayet konusu Uygulama Hizmetini Sunan Şirketten alınan yazıda ise,

- Yönetim Hizmeti Sunan Şirket ile aralarında akdedilen hizmet sözleşmesi kapsamında bu Şirkete bulut hizmeti sağlandığı, sisteme kullanıcı kaydı ve girişi, hesap oluşturma ve sair tüm işlemlerin Yönetim Hizmeti Sunan Şirket tarafından oluşturulduğu, bu sebeple kendilerinin veri sorumlusu sıfatını haiz olmadığı, sağlanan bulut hizmetinin kapsamı gereği veri işleyen sıfatını haiz oldukları,
- Sunulan bulut program hizmetinin bir sözleşmenin kurulması veya ifası ile doğrudan doğruya ilgili olduğu, ilgili kişinin ikamet ettiği sitede 634 sayılı Kat Mülkiyeti Kanunundan kaynaklanan borç ve yükümlülüklerin gereklerinin ifası için sitede ikamet eden kişilerin verilerinin işlenmesinin zorunlu olduğu,
- İlgili kişinin kişisel verilerinin Kanunun 5 inci maddesinin (2) numaralı fıkrasının (f) bendi çerçevesinde işlenebileceği, bu kapsamda açık rıza aranması durumunun söz konusu olmadığı, böyle bir rızanın aranacağı düşünülse bile söz konusu aydınlatma ve açık rızanın alınması yükümlülüğünün Yönetim Hizmeti Sunan Şirkete ait olduğu,
- İlgili kişinin kişisel verilerinin Yönetim Hizmeti Sunan Şirket tarafından bulut sistemine girilmesi suretiyle elde edildiği, bu kapsamda ilgili kişiye ait kişisel verilerin Yönetim Hizmeti Sunan Şirket

tarafından elde edilerek bulut sisteme girişinin yapıldığı, Yönetim Hizmeti Sunan Şirket tarafından ilgili kişinin girişinin yapılmasının ardından bulut programının otomatik olarak ilgili kişiye kayıt mesajı gönderdiği,

- Yönetim Hizmeti Sunan Şirket ile aralarındaki hizmet sözleşmesi kapsamında gerçekleşecek platform değişikliği ve/veya ek platform kullanımı sebebiyle; halihazırda yönetim hizmetlerinin ifası için kullanılan ilk uygulamada kayıtlı verilerin şikayete konu edilen ikinci uygulamaya aktarılabilmesi için Yönetim Hizmeti Sunan Şirketin bilgisi ve isteği dahilinde Şirketlerine ilk uygulamaya giriş yetkisi tanımlaması yapıldığı ve bu tanımlama ile birlikte platform değişikliği ve/veya ek platform kullanımı sonucu ilk uygulamada kayıtlı verilerin ikinci uygulamaya otomatik olarak aktarıldığı,
- Yönetim Hizmeti Sunan Şirket tarafından ilk uygulamaya kaydı yapılan kullanıcıların bilgi aktarımının otomatik olarak ikinci uygulamaya yapıldığı ve ilgili kişinin sisteme giriş yapabilmesi için telefon numarasına bilgilendirme SMS'i gönderildiği

açıklamalarına yer verilmiştir.

Söz konusu iddialar, tarafların savunmaları ve ilgili mevzuat hükümlerinin birlikte incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 13/04/2021 tarih ve 2021/359 sayılı Kararı ile;

- Öncelikle somut hadisede ilgili kişinin şahsına ait telefon numarasının rızası dışında uygulama ile paylaşıldığı iddiası kapsamında veri sorumlusunun tespit edilmesi gerektiği, veri sorumlusunun tespit edilebilmesi adına Site Temsilciler Kurulu ile Yönetim Hizmeti Sunan Şirket arasındaki sözleşmelerin de incelendiği, bu doğrultuda Yönetim Hizmeti Sunan Şirketin Site Temsilciler Kurulu ile akdettiği sözleşme kapsamında ilgili kişinin ikamet ettiği sitede yönetim hizmetleri verdiği, bu anlamda söz konusu hizmetlerin ifası gereği Yönetim Hizmeti Sunan Şirketin 3. kişilerle sözleşme yapabileceği, bu sözleşmeler kapsamında sorumluluğun Yönetim Hizmeti Sunan Şirkete ait olduğu, Yönetim Hizmeti Sunan Şirketin kişisel verilerin aktarıldığı iddia edilen uygulama/ikinci uygulama ile hizmet sözleşmesi akdettiği ve bu sözleşmenin eki niteliğinde olan KVKK Protokolünde hizmet sözleşmesinde Yönetim Hizmeti Sunan Şirketin veri sorumlusu sıfatını haiz olduğuna yer verildiği dikkate alındığında Yönetim Hizmeti Sunan Şirketin kişisel verilerin aktarıldığı iddia edilen ikinci uygulama ile yaptığı sözleşme kapsamında kişisel verilerin işleme amaç ve yöntemini belirleyen kişi olarak veri sorumlusu sıfatını taşıdığı,
- Uygulama Hizmetini Sunan Şirketin ise Yönetim Hizmeti Sunan Şirketin verdiği yetki kapsamında onun adına veri işleme faaliyetini gerçekleştiren veri işleyen sıfatını haiz olduğu,

• Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

• Diğer taraftan veri sorumlusu Şirket ve veri işleyen Uygulama Hizmeti Sunan Şirket arasında akdedilmiş olan Protokolün “Protokol Koşulları” başlıklı maddesinde;

- Yönetim Hizmeti Sunan Şirketin hizmet sözleşmesi kapsamında uygulamayı kullanarak uygulama ile yazılı olarak, elektronik ortamda veya sair şekillerde bilgi, belge ve veri paylaşacağı,
- Yönetim Hizmeti Sunan Şirketin uygulama ile paylaşacağı her türlü verinin sözleşme ilişkisi kapsamında uygulamaya aktarıldığını ve KVKK anlamında gerekli kabul edilmesi halinde Protokolün paylaşılacak her türlü kişisel veri bakımından açık rıza niteliğinde olduğunu kabul, beyan ve taahhüt edeceği,
- İlgili kişilerin KVKK kapsamında açık rıza vermesi gerekli ise ilgili kişilerin verilerinin uygulama ile paylaşılması hususunda ilgili kişilerden açık rıza aldığını kabul beyan ve taahhüt edeceği

hususlarına yer verildiği,

• Bununla birlikte, şikayet konusu kapsamında Uygulama Hizmetini Sunan Şirketten alınan cevap yazısından; Yönetim Hizmeti Sunan Şirket ile aralarındaki hizmet sözleşmesi ile birlikte gerçekleştirilecek platform değişikliği ve/veya ek platform kullanımı sebebiyle; Yönetim Hizmeti Sunan Şirketin kullandığı ilk uygulamada kayıtlı verilerin ikinci uygulama ile paylaşılabilmesi için veri sorumlusu Şirketin bilgisi ve isteği dahilinde ikinci uygulamaya giriş yetkisi tanımlaması yapıldığı ve bu tanımlama ile birlikte platform değişikliği ve/veya ek platform kullanımı sonucu ilk

uygulamada kayıtlı verilerin otomatik olarak ikinci uygulama ile paylaşıldığı ve ilgili kişinin sisteme giriş yapabilmesi için telefon numarasına bilgilendirme SMS'i gönderildiği,

- Bu kapsamda, veri sorumlusu Yönetim Hizmeti Sunan Şirket her ne kadar ilgili kişinin kişisel verilerini ikinci uygulama ile paylaşmadığını iddia etse de, bu uygulama ile aralarında akdedilmiş olan Protokol maddelerine ve Uygulama Hizmeti Sunan Şirketten alınan cevap yazısına göre taraflar arasında söz konusu kişisel veri paylaşımı hususunun mümkün olduğu; keza Uygulama Hizmeti Sunan Şirketten alınan cevap yazısından da veri sorumlusu Şirketin kullanmış olduğu ilk uygulamada mevcut verilerin ikinci uygulama ile paylaşılması kapsamında veri sorumlusu Yönetim Hizmeti Sunan Şirket tarafından ikinci uygulamaya yetki tanındığı, bu yetki çerçevesinde aralarında ilgili kişinin de bulunduğu ilk uygulamadaki kullanıcı bilgilerinin ikinci uygulama ile paylaşıldığı,

- İkinci uygulamaya katılımın, site yönetim işlerinden ayrı bir amaca hizmet ettiği ve isteğe bağlı olduğunun anlaşıldığı, bu uygulamaya ilgili kişilerin katılımını sağlamak amacıyla kişisel verilerin işlenmesinin ise Kanunun 5 inci maddesinin (2) numaralı fıkrasında yer alan işleme şartlarına dayandırılmayacağı ancak ilgili kişinin açık rızası ile gerçekleştirilebileceği, diğer taraftan somut hadisede ise ilgili kişinin açık rızasının alınmadığı hususları göz önünde bulundurulduğunda kişisel verilerin hukuka aykırı işlendiği kanaatine varıldığı

değerlendirmelerinden hareketle;

- Kişisel verilerin aktarıldığı iddia edilen uygulamaya katılımın, site yönetim işlerinden ayrı bir amaca hizmet ettiği ve isteğe bağlı olduğu, bu uygulamaya ilgili kişilerin katılımını sağlamak amacıyla kişisel verilerin işlenmesinin Kanunun 5 inci maddesinin (2) numaralı fıkrasında yer alan işleme şartlarına dayandırılmayacağı ancak ilgili kişinin açık rızası ile gerçekleştirilebileceği, ilgili kişinin açık rızasının ise alınmadığı hususları göz önünde bulundurularak kişisel verilerin hukuka aykırı işlendiği kanaatine varılmış olup, bu çerçevede Kanunun 12 nci maddesinin (1) numaralı fıkrası hükmüne aykırı hareket eden veri sorumlusu Yönetim Hizmeti Sunan Şirket hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2021/358 sayılı KVKK Kararı

İlgili kişiye bir banka tarafından SMS gönderilmesi ve ilgili kişinin bu banka nezdindeki kişisel verilerinin imha edilmesi talebinin yerine getirilmemesi hakkında Kişisel Verileri Koruma Kurulunun 13/04/2021 tarihli ve 2021/358 sayılı Karar Özeti

Karar Tarihi : 13.04.2021

Karar No : 2021/358

Konu Özeti : İlgili kişiye bir banka tarafından SMS gönderilmesi ve ilgili kişinin bu banka nezdindeki kişisel verilerinin imha edilmesi talebinin yerine getirilmemesi hakkında

Kuruma intikal eden şikâyet dilekçesinde özetle; veri sorumlusu bir banka ile ilgili kişi arasındaki ilişkinin 22/11/2003 tarihinde müşteri numarasının oluşturulmasıyla kurulduğu, ilgili kişinin veri sorumlusu nezdindeki son işleminin de bu tarih olduğu, ilgili kişinin veri sorumlusuyla ilişkisinin 16 yıl önce kesilmiş olmasına rağmen kişisel verilerinin veri sorumlusu tarafından halen saklandığı, ilgili kişiye SMS'ler gönderildiği ve kredi kartı isteyip istemediğine ilişkin telefon aramalarının yapıldığı, ilgili kişinin bu kapsamda yaptığı başvurunun veri sorumlusuna tebliğ edildiği, ancak veri sorumlusu tarafından ilgili kişiye cevabın mevzuatta belirlenen süre sonrasında iletilmediği, veri sorumlusu tarafından verilen cevabın yetersiz olduğu, ilgili kişiye verilen cevapta kişisel verilerin yurt dışına aktarılabildiği hususuna yer verildiği, ancak bu konuda ilgili kişinin açık rıza vermediği ve veri sorumlusunun 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 9 uncu maddesi kapsamında yurt dışına veri aktarım istisnalarından yararlanıldığına dair herhangi bir bilgiye de yer verilmediği, veri sorumlusu ile ilgili kişi arasında 2003 yılında kurulmuş olan sözleşmesel ilişkinin sona ermiş olmasına rağmen ilgili kişinin kişisel verilerinin silinip silinmeyeceğinin açıkça belirtilmemesinin ve ilgili kişiye ait bilgilerin 10 sene daha saklanması açıkça mevzuata aykırı olduğu belirtilerek veri sorumlusu hakkında Kanun kapsamında gerekli tedbirlerin alınması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, verilen cevapta özetle;

- İlgili kişinin kendilerine tebliğ edilen başvurusuna verilen cevabın sehven ilgili kişiye 2 gün gecikmeli olarak gönderildiği, yapılan bu hatayla ilgili veri sorumlusu bünyesinde gerekli tedbirlerin alındığı,
- İlgili kişinin veri sorumlusu nezdindeki müşteri numarasının 2003 yılında oluşturulduğu, bu yıl ilk kredi kartı girişinin yapıldığı, bu çerçevede ilgili kişi ile veri sorumlusu arasında 18/11/2003 tarihli Kredi Kartı Başvuru Formu ve Bankacılık İşlemleri Sözleşmesinin ve 14/11/2011 tarihli Bilgi Güncelleme, Kimlik Adres Tespit Tutanağı ve Bankacılık İşlemleri Sözleşmesinin mevcut olduğu,
- Veri sorumlusu nezdinde ilgili kişiye ait herhangi bir açık hesap ya da ürünün bulunmadığı, ilgili kişiye müşteri ilişkisi çerçevesinde hizmet sağlanamıyor olsa da 5411 sayılı Bankacılık Kanunu kapsamında yükümlülüklerinin halen devam ediyor olması sebebiyle ilgili kişinin bilgilerinin veri sorumlusunun veri tabanında saklandığı,
- 08/11/2019 tarihinde Gelir İdaresi Başkanlığının bildirimine istinaden ilgili kişinin veri sorumlusunda hak ve alacağının olmaması nedeniyle e-haciz uygulanamamış olduğu, aynı gün yine kurumdan gelen iptal bilgisine istinaden kayıtlara geçen haciz bilgisi iptal işleminin veri sorumlusu sisteminde kayıtlı bulunan cep telefonuna “Değerli müşterimiz, hesap limitiniz üzerinde bulunan e-haciz kısıtı, KADIKÖY V.D.’den Bankamıza iletilen bildirim istinaden kaldırılmıştır” şeklinde yasal bilgilendirme içeren SMS’in gönderildiği,
- Elektronik Ticaretin Düzenlenmesi Hakkında Kanuna istinaden 01/05/2015 tarihinden itibaren iletişim izni olmayan müşterilere pazarlama, temenni, kutlama içerikli elektronik iletilerin gönderilmemesi gerektiği, ayrıca Ticari İletişim ve Ticari Elektronik İletiler Yönetmeliğinin 6 ncı maddesinin (2) numaralı fıkrası uyarınca iletilerin yasal bilgilendirme içermesi halinde bu konuda iletişim izni bulunmasına gerek olmadığı,
- Veri sorumlusu nezdinde, vergi dairelerinden dosya borçlusu kişiler aleyhine/adına gelen haciz bildirimleri için birbirini tetikleyen bir sürecin mevcut olduğu, bu süreçte bahse konu müşterilere konu hakkında bilgilendirme mesajlarının gönderilmesinin de yer aldığı, bu mesajların yasal bilgilendirme içeriyor olması sebebiyle de otomatik tetiklenen bilgilendirme SMS’lerinde müşterinin iletişim izni durumuna bakılmadığı,
- 5411 sayılı Bankacılık Kanununun “Belgelerin Saklanması” başlıklı 42 nci maddesi gereğince müşterilerin banka nezdinde yaptığı işlemlere ilişkin belgelerin, son işlem/talimat tarihinden itibaren 10 yıl süreyle saklandığı, 10 yıl hareketsiz kalan hesapların banka sistemlerinde taranarak 6 ayda bir periyodik silme işlemine tabi tutulduğu, bunun yanı sıra hesaba bağlı olmaksızın müşterilerden gelen

talepler için de son işlem tarihinden itibaren 10 yıl geçmesi akabinde veri sorumlusu nezdindeki verilerin silindiği,

- İlgili kişinin veri sorumlusu nezdindeki son işleminin 13/12/2013'te gerçekleştirilen kredi kartı kapatma işlemi olduğu, 16/12/2019 tarihinde ise daha önce izni bulunan kampanya bilgilendirmesine yönelik iznini iptal ettiği,
- Veri sorumlusunun hukuki yükümlülüklerini yerine getirebilmesi için zorunluluk halinin devam ettiği, diğer bir ifadeyle Kanunun 5 inci ve 6 ncı maddelerinde sayılan işleme şartlarının tamamen ortadan kalkmamış olması sebebiyle ilgili kişiye ait verilerin ancak veri sorumlusu nezdindeki son işlem tarihinden itibaren 10 yıl sonra silinebileceği,
- İlgili kişinin verilerinin Kanunun 9 uncu maddesinde yer alan ve açık rıza gerektiren haller kapsamında yurt dışına aktarılmadığı,
- Veri sorumlusu nezdinde işlenen kişisel verilerin Kanunun 12 nci maddesi kapsamında güvenlik düzeyini sağlamaya yönelik idari ve teknik tedbirlerin alındığı,

ifade edilmiştir.

Konuya ilişkin olarak yapılan incelemede Kişisel Verileri Koruma Kurulunun 13/04/2021 tarih ve 2021/358 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanununun "Kişisel Verilerin İşlenme Şartları" başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,
- Kanunun "Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi" başlıklı 7 nci maddesinin (1) numaralı fıkrasında ise, Kanun ve ilgili diğer kanun hükümlerine uygun olarak

işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silineceği, yok edileceği veya anonim hale getirileceği hüküm altına alınmış olmakla birlikte, (2) numaralı fıkrasında kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu hükümlerinin yer aldığı,

- Öte yandan Kanunun “İlgili Kişinin Hakları” başlıklı 11 inci maddesi gereğince herkesin, veri sorumlusuna başvurarak kendisiyle ilgili; kişisel verilerinin işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerinin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerinin aktarıldığı üçüncü kişileri bilme, kişisel verilerinin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme, 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerinin silinmesini veya yok edilmesini isteme, kişisel verilerinin düzeltilmesi veya silinmesi/yok edilmesi ile ilgili yapılan işlemlerin kişisel verilerinin aktarıldığı üçüncü kişilere bildirilmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme ve kişisel verilerinin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme haklarına sahip olduğu,

- Somut olayda, ilgili kişinin veri sorumlusu nezdinde tutulan cep telefon numarasının bir kişisel veri olduğu, kişiye SMS gönderilmesi suretiyle ise kişisel veri niteliğindeki cep telefonu numarası ile ilgili işleme faaliyeti gerçekleştiği,

- İlgili kişinin veri sorumlusuna yaptığı başvurunun veri sorumlusu tarafından Kanunda ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğde (Tebliğ) öngörülen süre içerisinde cevaplanmadığı,

- İlgili kişinin şikâyet dilekçesinde veri sorumlusu tarafından ilgili kişiye hukuka aykırı olarak mesajlar gönderildiği ve kredi kartı isteyip istemediğine yönelik telefon aramaları gerçekleştirildiği iddia edilse de, dilekçesinin ekinde sadece gönderilen bir adet SMS’e ilişkin görüntü kaydına yer verildiği, buna karşın aramalara ilişkin tevsik edici herhangi bir belgeye yer verilmediği ve ilgili kişi tarafından veri sorumlusuna yapılan başvuruda sadece gönderilen SMS’lerden bahsedildiği anlaşıldığından; ilgili kişinin veri sorumlusuna yöneltmediği ancak şikâyet başvurusunda değindiği “telefon aramaları”nın inceleme kapsamına alınmamasının uygun olacağı,

- Veri sorumlusu tarafından ilgili kişiye “Değerli müşterimiz, hesap limitiniz üzerinde bulunan e-haciz kısıtı, KADIKÖY V.D.’den Bankamıza iletilen bildirimden istinaden kaldırılmıştır” şeklinde olan iletinin gönderilmesi suretiyle kişinin telefon numarasının Kanunun “Kişisel Verilerin İşlenme

Şartları” başlıklı 5 inci maddesinin (2) numaralı fıkrasında yer alan “veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması” şartına dayalı olarak işlendiği, ilgili iletinin yasal bilgilendirme içermesi ve herhangi bir mal veya hizmetin tanıtımının da söz konusu olmaması sebebiyle ilgili kişinin rızasının/izninin alınmasına gerek olmadığı, dolayısıyla veri sorumlusu tarafından ilgili kişiye yasal bilgilendirme içerikli SMS’in gönderilmesi suretiyle telefon numarasının işlenmesinde herhangi bir hukuka aykırılık bulunmadığı,

- İlgili mevzuat hükümleri dikkate alındığında, ilgili kişinin kişisel verilerinin işlenmesini gerektiren sebeplerin henüz ortadan kalkmaması sebebiyle, ilgili kişinin silme talebinin veri sorumlusu tarafından yerine getirilmemesinin hukuka aykırı olmadığı,

İlgili kişinin kişisel verilerinin veri sorumlusu tarafından yurt dışına aktarıldığı iddiasına ilişkin olarak Kuruma tevsik edici bir bilgi veya belge sunulmadığı

değerlendirmelerinden hareketle;

- İlgili kişinin Kanun kapsamında yaptığı başvurusuna, kendisine ulaşmasına rağmen 30 günlük yasal süre geçtikten sonra cevap vermesi sebebiyle veri sorumlusunun Kanunun ve Tebliğin ilgili hükümlerine uyum konusunda gerekli dikkat ve özeni göstermesi gerektiği konusunda talimatlandırılmasına,

- Veri sorumlusu tarafından söz konusu iletinin gönderilmesi suretiyle ilgili kişinin kişisel verisi olan cep telefonu numarasının işlenmesinin Kanunun 5 inci maddesinin (2) numaralı fıkrasında yer alan “veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması” şartına dayandığı, öte yandan ilgili iletinin yasal bilgilendirme içermesi ve herhangi bir mal veya hizmetin tanıtımının da söz konusu olmaması sebebiyle ilgili kişinin rızasının/izninin alınmasına gerek olmadığı bu çerçevede veri sorumlusu tarafından ilgili kişiye yasal bilgilendirme içerikli SMS’in gönderilmesi suretiyle kişisel verilerinin işlenmesinde hukuka aykırılığın bulunmadığı kanısına varıldığından bu hususta Kanun kapsamında yapılacak bir işlemin olmadığına,

- İlgili kişinin veri sorumlusu nezdindeki son işlem tarihinin 13/12/2013’te gerçekleştirilen kredi kartı kapatma işlemi olduğu ve dolayısıyla son işlem tarihi üzerinden 10 yıllık sürenin geçmemiş olduğu dikkate alındığında; ilgili kişinin kişisel verilerinin işlenmesini gerektiren sebeplerin henüz ortadan kalkmaması sebebiyle silme talebinin veri sorumlusu tarafından yerine getirilmemesinin Kanunun 7 nci maddesi hükümleri dikkate alındığında hukuka aykırı olmadığı kanısına varıldığından bu hususta Kanun kapsamında yapılacak bir işlemin olmadığına,

- İlgili kişinin, kişisel verilerinin veri sorumlusu tarafından yurt dışına aktarıldığı iddiasına ilişkin olarak Kuruma tevsik edici bir bilgi veya belge sunmadığı dikkate alındığında söz konusu iddiaya ilişkin olarak Kanun kapsamında yapılacak bir işlem olmadığına karar verilmiştir.

2021/333 sayılı KVKK Kararı

Bir sigorta şirketi tarafından işlenen kişisel verilerin üçüncü kişiye aktarılması ve ilgili kişiye veri aktarımına ilişkin aydınlatma yapılmaması hakkında Kişisel Verileri Koruma Kurulunun 05/04/2021 tarih ve 2021/333 sayılı Karar Özeti

Karar Tarihi : 05.04.2021

Karar No : 2021/333

Konu Özeti : Bir sigorta şirketi tarafından işlenen kişisel verilerin üçüncü kişiye aktarılması ve ilgili kişiye veri aktarımına ilişkin aydınlatma yapılmaması

İlgili kişinin Kuruma intikal eden şikâyetinde özetle; maliki olduğu aracı ile geçirdiği trafik kazası sonrası veri sorumlusu sigorta şirketi tarafından kasko poliçesi kapsamında hasar dosyası açıldığı, bununla birlikte veri sorumlusunun çağrı merkezini aradığında aracının pert süreci işlemlerinin üçüncü bir şirket tarafından yapıldığı ve bu şirketin kendisi ile iletişime geçeceğinin söylendiği, söz konusu kasko poliçesinde ve sigorta genel şartları mevzuatında pert işleminde ya da herhangi bir hasar halinde hasarın ya da aracın rayiç değerinin ve sovtaj değerinin tespitinin tarafsız ve bağımsız sigorta eksperince yapılacağı belirtilmişti, bununla birlikte veri sorumlusu tarafından üçüncü kişi şirket ile onayı ve bilgisi olmadan kendisine ait aracın kaza fotoğraflarının, kimlik bilgilerini de içeren ruhsatın ve iletişim bilgilerinin paylaşıldığı, ancak üçüncü şirketin veri sorumlusu ile yapılan sözleşmenin tarafı olmadığı, sözleşmede adının geçmediği, rayiç tespiti ve sigortacılık işlemlerinin ilgili şirket ile yürütülmesinin poliçeye ve sigortacılık mevzuatına aykırı olduğu ve poliçe kapsamında kişisel verilerinin sadece sigorta eksperine ile paylaşılacağı, veri sorumlusu tarafından kişisel verilerinin işlenmesinde onay istenmediği ve bildirim yapılmadığı, ayrıca konuya ilişkin veri sorumlusuna yapmış olduğu başvuruya cevap verilmediği ifade edilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Başlatılan inceleme çerçevesinde söz konusu iddialara ilişkin olarak veri sorumlusu sigorta şirketinin savunması istenilmiş olup alınan cevabi yazıda özetle;

- Şirketlerinin sigortacılık faaliyetlerini gerçekleştirmek ve mevzuattan doğan yükümlülüklerini yerine getirmek amacıyla çeşitli tedarikçi şirketler ile hizmet satın alımı yoluyla iş birliği yaptığı, bu

hizmetlere ilişkin usul ve esasların düzenlendiği Sigortacılık Destek Hizmetleri Hakkında Yönetmeliğin “Hizmet konuları” başlıklı 4 üncü maddesinin (h) fıkrasında sovtaj yönetimi hizmetlerinin alınabilecek destek hizmetleri arasında sayıldığı,

- Bu çerçevede üçüncü kişi şirket ile Ağır Hasarlı Araç Satış Sözleşmesi düzenlendiği, söz konusu sözleşmenin 13.9. maddesinde sigortalı ya da üçüncü kişilerin kişisel verilerinin Kanun ve ilgili mevzuata göre saklanabileceği, toplanabileceği, işlenebileceği ve aktarılabilceğinin düzenlendiği, yürütülen işlemlerin sigorta mevzuatına uygun olarak eksiksiz bir şekilde yerine getirildiği, kişisel verilerinin sadece sözleşmenin ifası için, ölçülü bir şekilde, hukuka, Kanun ve ilgili mevzuata uygun bir şekilde işlendiği,

- Şikâyet konusu kişisel veri aktarımının poliçeden doğan hasarı tazmin etme yükümlülüğünü yerine getirmek amacıyla, Kanununun 8 inci maddesinin (2) numaralı fıkrasının (a) bendi atfıyla 5 inci maddesinin (2) numaralı fıkrasının (c) bendinde yer alan; “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” hukuki sebebine dayanılarak Ağır Hasarlı Araç Satış Sözleşmesinde tanımlanan yükümlülöklere uygun şekilde işlemlerin yürütölmesi amacıyla şirketleri adına veri işleyen sıfatıyla üçüncü kişi şirkete aktarımının yapıldığı,

- Şikâyete konu aktarım bakımından bilgilendirmenin verinin aktarılmasına başlanmadan önce ilgili kişiye gönderilen bilgilendirme formu aracılığıyla yapıldığı ve kişisel verilerinin poliçenin düzenlenebilmesi, risk deęerlendirmesi yapılabilmesi, tazminat deęerlendirmesi yapılabilmesi ve poliçedeki yükümlölüklerin yerine getirilebilmesi için şirketlerinin birlikte çalıştığı kuruluşlara aktarıldığı konusunda bilgilendirildiği,

- Aktarım tarihinde internet sitelerinde yer alan aydınlatma metninde şirketlerinin kişisel verileri “Teklif, risk yönetimi, reasürans, hasar inceleme, tespit, tazmin, tazminat, tahsil, transfer, rücu, asistans hizmeti ve benzer süreçlerin yürütölmesi” amacıyla işlediği ve “Kişisel Verilerin Kimlere ve Hangi Amaçla Aktarılacağı” başlığı altında kişisel verilerin sayılan amaçlarla bağlantılı olarak aktarıldığı konusunda ilgili kişilerin bilgilendirildiği,

- Güncel çağrı merkezi poliçe satış süreçlerinde de Kanun kapsamında aydınlatma ve bilgilendirmelerin kişisel verilerin elde edilmesi sırasında ilgili kişiye ön bilgilendirme yapılması suretiyle gerçekleştirildiği, ayrıca ilgili kişinin çağrı merkezi aracılığıyla kişinin internet sitesindeki aydınlatmaya yönlendirilmesi suretiyle katmanlı olarak bilgilendirme de yapıldığı

ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 05/04/2021 tarihli ve 2021/333 sayılı Kararı ile;

- Kanunun "Tanımlar" başlıklı 3 üncü maddesinin (1) numaralı fıkrasında "kişisel veri"nin; "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi, "ilgili kişi"nin; "kişisel verisi işlenen gerçek kişiyi", "veri sorumlusu"nun "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi", "veri işleyen" in ise "veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi" ifade ettiği, Kanunun 3 üncü maddesinde yer alan tanımlar uyarınca, ilgili kişiye ait olan kimlik ve iletişim gibi bilgilerin kişisel veri, ilgili kişinin söz konusu bilgileri üzerinde gerçekleştirilen her türlü işlemin kişisel veri işleme faaliyeti, kişisel verisi işlenen kişinin ilgili kişi ve kişisel verileri işleyen sigorta şirketinin veri sorumlusu, kişisel verilerin aktarıldığı üçüncü kişi şirketin ise veri işleyen olarak değerlendirildiği,

- 5684 sayılı Sigortacılık Kanununun "Tanımlar" başlıklı 2 nci maddesinde destek hizmeti kuruluşunun "Bu Kanun kapsamındaki kuruluşlara, faaliyet alanlarıyla ilgili konularda yardımcı veya tamamlayıcı nitelikte hizmet veren kuruluşlar", sigorta şirketinin ise, "Türkiye'de kurulmuş sigorta şirketi ile yurt dışında kurulmuş sigorta şirketinin Türkiye'deki teşkilâtı," olarak tanımlandığı,

- Sigortacılık Destek Hizmetleri Hakkında Yönetmelikte sigorta şirketlerinin ana faaliyet alanlarıyla ilgili konularda yardımcı veya tamamlayıcı nitelikte destek hizmeti alımına, destek hizmetlerinin verilmesine ve bu hizmetleri sunan destek hizmeti sağlayıcılarına ilişkin usul ve esasların düzenlendiği, anılan Yönetmeliğin 4 üncü maddesinin birinci fıkrasının (h) bendinde ise sovtaj yönetimi hizmetlerinin dışarıdan temin edilebilecek destek hizmetleri arasında sayıldığı, 5 inci maddede destek hizmeti sunumunda hizmetin kimin adına sunulduğunun açıkça belirtileceği ve destek hizmeti sağlayıcılarının bu işleri nedeniyle bilgi sahibi oldukları sigortalılara, hak sahiplerine ve katılımcılara ait sırların korunmasına yönelik gerekli tedbirleri alacağını hüküm altına alındığı,

- İlgili sigorta mevzuatı hükümleri uyarınca yardımcı veya tamamlayıcı nitelikteki sovtaj yönetimi hizmetlerinin destek hizmeti olarak alınabileceği, bu çerçevede ilgili kişinin, açık rızası alınmadan kişisel verilerinin işlenmesinin hukuka aykırı olduğu iddiasına ilişkin olarak, söz konusu veri işleme faaliyetinin sigorta poliçesindeki yükümlülüklerin yerine getirilebilmesini teminen Kanunun 5 inci maddesinin (2) numaralı fıkrasının (c) bendinde yer alan; "Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması." veri işleme şartına dayanılarak gerçekleştirildiği anlaşıldığından söz konusu işlemde hukuka aykırılık bulunmadığı,

- Veri sorumlusu ile veri işleyen üçüncü kişi Şirket arasında imzalanan Ağır Hasarlı Araç Satış Sözleşmesi incelendiğinde ise, üçüncü kişi şirketin veri sorumlusunun verdiği talimatlar doğrultusunda ve veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işlemesi sebebiyle veri işleyen olarak hareket ettiği anlaşıldığından, veri sorumlusu ile onun adına kişisel verileri işleyen arasında yapılan paylaşımların Kanunun 8 inci maddesi kapsamında ele alınamayacağı,

- İlgili kişiye kişisel verisinin aktarımına ilişkin aydınlatma yapılmadığı iddiasına ilişkin olarak aydınlatma metni incelendiğinde; “Kişisel Verilerinizin Kimlere ve Hangi Amaçla Aktarılabilceği” bölümünde yer alan “Kişisel Verilerin İşlenme Amaçları” başlığı altında “sayılan amaçlarla ve bunlarla sınırlı olmamak üzere kişisel verilerin aktarılabilceğinin” belirtildiği tespit edilmiş olup söz konusu ibarenin Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin (Tebliğ) 5 inci maddesinin (1) numaralı fıkrasının (g) bendinde yer alan; “Aydınlatma yükümlülüğü kapsamında açıklanacak kişisel veri işleme amacının belirli, açık ve meşru olması gerekir. Aydınlatma yükümlülüğü yerine getirilirken, genel nitelikte ve muğlak ifadelerle yer verilmemelidir.” hükmüne aykırı olduğu; ayrıca “Kişisel Veri Toplamının Yöntemi ve Hukuki Sebebi” başlığı altında hangi kişisel verinin hangi veri işleme şartına dayanılarak işlendiğinin açıkça ortaya konulmadığı, bununla birlikte veri sorumlusunca daha sonra internet sitelerinde yayımlanan aydınlatma metninin güncellendiği ancak hangi kişisel verinin hangi veri işleme şartına dayanılarak işlendiğinin hala net olarak ortaya konulmadığı

değerlendirmelerinden hareketle;

- Veri sorumlusunun kendisine yapılan başvuruları titizlikle kayıt altına alarak Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğe uygun şekilde ilgili kişilerin başvurularına yanıt vermesi konusunda talimatlandırılmasına,

- Şikâyete konu faaliyette veri sorumlusunun kişisel veri paylaşımı yaptığı üçüncü kişi şirketin veri işleyen olduğu dikkate alındığında, ilgili kişinin, açık rıza alınmadan kişisel verilerinin işlenmesinin hukuka aykırı olduğu iddiasına ilişkin olarak, söz konusu işlemin Kanunun 5 inci maddesinin (2) numaralı fıkrasının (c) bendinde yer alan “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” veri işleme şartına dayanılarak gerçekleştirildiği anlaşıldığından söz konusu işlemde hukuka aykırılık bulunmadığına,

- İlgili kişinin, tarafına aydınlatma yapılmadığı iddiasına ilişkin olarak, olay tarihinde yapılan aydınlatmanın usul açısından eksiklikler taşıdığı ancak sonrasında aydınlatma metninin

güncellendiđi, bununla birlikte söz konusu metinde hâlihazırda hangi kişisel verinin hangi veri işleme şartına dayanılarak işlendiđinin belli olmaması nedeniyle veri sorumlusunun metindeki bu eksikliđin giderilmesi hususunda talimatlandırılmasına karar verilmiştir.

2021/311 sayılı KVKK Kararı

Bir kozmetik şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 25.03.2021 tarih ve 2021/311 sayılı Karar Özeti

Karar Tarihi : 25.03.2021

Karar No : 2021/311

Konu Özeti : Bir kozmetik şirketinin veri ihlal bildirimini hakkında karar

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- 18.05.2020 tarihinde, veri sorumlusunun internet sitesinde yer alan yeni bir kampanya sebebiyle siteye yüksek erişim sağlandığı ve uygulama sunucularının yetersiz kaldığı,
- Veri işleyen tarafından yeni uygulama sunucuları eklenirken, sitenin çalışmaması ihtimali gözetilerek sitenin mevcut halinin kopyalarının çıkarıldığı,
- Bu işlem gerçekleştirilirken; sitenin statik sayfasının kopyasının alınmasının ve yeni uygulama sunucuları eklenirken müşterilere sayfanın statik kopyasının gösterilmesinin amaçlandığı,
- Bu işlem esnasında; DDos ataklarını önlemek için kullanılan ve veri işleyenin üçüncü kişiden aldığı hizmetin içinde tanımlandığı gibi çalışmayan bir fonksiyon sebebiyle yalnızca mevcut ara yüzün değil kullanıcı profillerinin de bir kopyasının olduğu ve üye olarak giriş yapan kullanıcılara rastgele kopyası alınan kullanıcı profillerinin bilgilerinin görünür olduğu,
- Görüntülenen profillerde adı-soyadı, e-posta, adres gibi kişisel veriler yer aldığı, kredi kartı gibi finansal hiçbir kişisel veri bulunmadığı,
- Sitenin olağan dışı davranışlarının tüketiciler ve merkez ofis ekip tarafından veri sorumlusunun çağrı merkezine gelen bildirimlerle kısa sürede fark edildiği ve düzeltmek için yapılan çalışmalar neticesinde, saat 17.00'de sitedeki sorunların giderildiği, 17.00'de erişime kapatılan sitenin, 17.48'de tekrar normal çalışma düzenine çekildiği,
- Bu 48 dakikalık süre zarfı boyunca, sitede üye girişi yapmış müşterilerin, kendi kişisel verileri yerine kopyalama yapıldığı ana denk gelen tüketicilerin kopyası alınan profillerindeki kişisel verilerini görmüş olma ihtimali bulunduğu,

- Ancak bu süreçte alınan kopyaların herhangi bir sistemde saklanmadığı için kaç kişinin hangi üyelerin profilini görmüş olabileceği hakkında net bir sayının belirtilemediği, toplamda 24 kişinin bilgisinin farklı üyeler tarafından görünür olduğunun öngörüldüğü

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 25.03.2021 tarih ve 2021/311 sayılı Kararı ile;

- Kaç kişinin hangi üyelerin profilini görmüş olabileceği hakkında net bir sayı belirtilemediği ve oluşan hatanın kampanya sırasında ve yoğunluğun yüksek düzeyde olduğu dakikalarda olmasından ötürü bu kişilerin kişisel verilerin çok sayıda kişi tarafından görünmüş olabileceği,

- Fonksiyonun canlı ortama alınmadan önce teste tabi tutulmuş olmasına rağmen bu testin sınırlı sayıda kullanıcı ile yapıldığı, veri sorumlusu tarafından kampanya sebebiyle yoğunluğun yüksek olacağı öngörülerek, bu yoğunluğa uygun bir şekilde yazılımın kontrollerinin gerçekleştirilmesinin ardından uygulamaya konulması gerektiği ayrıca veri sorumlusu tarafından sitede yapılacak değişiklik ve güncellemelerin sitenin yoğun çalıştığı zaman diliminde yapılmayıp siteye girişin en düşük olduğu saatlerde ve bu tarz ihlallerin yaşanmaması adına sitenin kapatılarak yapılması gerektiği ancak veri sorumlusunun ihlale sebebiyet veren olayda buna uymadığı, açıklanan bu durumların Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 3.5. Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı başlığı altında belirtilen "Veri sorumlusu tarafından yeni sistemlerin tedariği, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmalıdır. Uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontroller yapılmalı, doğru girilmiş bilginin işlem sırasında oluşan hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmaları yerleştirilmelidir. Uygulamalar, işlem sırasında oluşacak hataların veri bütünlüğünü bozma olasılığını asgari düzeye indirecek şekilde tasarlanmalıdır." ifadelerine uygun düşmediği,

- Bunların yanında veri sorumlusunun kullanıcıların kişisel verilerini maskeleyerek veya şifreleyerek saklaması gerekirken Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) 4.1. Teknik Tedbirler Özet Tablosu'nda da yer verilen "şifreleme ve veri maskeleyme" önlemlerini ancak ihlalden sonra almayı planladığı

- Yukarıda sayılan gerekçelerin veri sorumlusunun Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 2.1. Mevcut Risk ve Tehditlerin Belirlenmesi başlığı altında belirtilen "...bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi

durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir.” şeklinde belirtilen risk odaklı yaklaşım çerçevesinde ve veri sorumlusu yükümlülüklerine uygun hareket etmediğinin göstergesi olduğu,

dikkate alındığında, Kanununun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanununun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 200.000 TL idari para cezası uygulanmasına,

- Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde veri sorumlusunun Kuruma bildirimde bulunduğu,

- Veri sorumlusu tarafından veri ihlaline ilişkin bildirim yapılması amacıyla ilgili kişilere e-posta gönderildiği, gönderilen e-postanın Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararında belirtilen bildirimde bulunması gereken asgari unsurları taşıdığı

dikkate alındığında, Kanununun 12 nci maddesinin (5) numaralı fıkrası uyarınca, bu aşamada yapılacak bir işlem olmadığına

karar verilmiştir.

2021/242 sayılı KVKK Kararı

İlgili kişinin kişisel verilerinin bir tur şirketi tarafından üçüncü kişilerle paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 18/03/2021 tarihli ve 2021/242 sayılı Karar Özeti

Karar Tarihi : 18.03.2021

Karar No : 2021/242

Konu Özeti : İlgili kişinin kişisel verilerinin bir tur şirketi tarafından üçüncü kişilerle paylaşılması

Kuruma intikal eden şikâyetinde özetle; ilgili kişinin veri sorumlusu tur şirketinden tatil paketi satın aldığı ve ilgili tüm bilgilerini veri sorumlusu ile paylaştığı, paylaşılan bu verilerin veri sorumlusu tarafından üçüncü bir kişiye aktarıldığı, söz konusu üçüncü kişi tarafından bahsi geçen bilgilerin bir mahkeme dosyasına ve baro şikâyet dilekçesi ekine sunulduğu, veri sorumlusuna yapılan başvuruya verilen cevapta üçüncü kişilere hiçbir şekilde verilmediği söylenen kişisel verilerin mahkeme dosyasında nasıl yer aldığına açıklanmadığı, bu kapsamda ilgili kişinin rızası ve bilgisi olmaksızın kişisel verilerini üçüncü kişilerle paylaşmış olan veri sorumlusu hakkında 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gerekli hukuki ve cezai işlemlerin yapılması talep edilmiştir.

Konuya ilişkin olarak başlatılan inceleme çerçevesinde veri sorumlusunun savunması istenilmiş olup alınan cevabi yazıda özetle;

- Kanunun yürürlüğe girmesinden önce veri sorumlusunun sistemlerinde güvenlik ve önlem amaçlı log kayıtlarının tutulduğu, şirketleri ile rezervasyonun; çağrı merkezi, acente ya da internet sitesi üzerinden yapılabildiği, tüm bu kanallardan yapılan satış ve rezervasyonların tek bir satış altyapısında saklandığı, satış sürecinde oluşan kişi kartının, kişi ile iletişim kurulacak telefon numarası ve e-posta gibi iletişim bilgilerinin her seferinde tekrardan kişiden alındığı, böylelikle kişinin bir önceki seyahatinden farklı iletişim bilgileri ile (cep telefonu, e-posta vs.) yeni seyahatini planlayabildiği,
- İnternet sitesinden gerçekleştirilen bir seyahat alım sürecinde kredi kartı bilgileri kaydedilmeden banka sistemleri üzerinden işlem yapıldığı ve onay sürecinde bankanın paylaştığı son 4 hane ile ilk 6 haneyi içeren bilgiler ile kişi adı gibi detayların ödeme kısmında saklandığı,

- Çağrı merkezi ve acente sistemlerinin aynı altyapıda olduğu, çağrı merkezlerinin büyük ve online bir acente gibi işlem yaptığı; çağrı merkezinden yapılan alımlarda kişi kartlarındaki iletişim bilgilerinin Kanuna uygun olarak alınan teknik ve idari tedbirler kapsamında tamamen boş geldiği ve satış personelinin/müşteri temsilcisinin gereken bilgileri seyahat özelinde misafirden talep ederek ve talebe uygun olarak doldurduğu,

- Bu suretle, her bir rezervasyonda rezervasyon bilgilerinin iletileceği e-posta adresi ve telefon bilgilerinin güncellenmekte olduğu, misafir rezervasyonunun önceki kayıtlarda yer alan e-posta adresine veya telefon numarasına gönderilmesinin de önüne geçildiği; sistemde gerçekleştirilen bu kayıtlarda işlemi yapan temsilcinin giriş yaptığı/login olduğu kendisine ait hesap ile sisteme kaydedildiği/log kaydı alındığı, böylelikle ileride de temsilcinin oluşturduğu ya da sonradan görüntülediği şeklindeki bilgilere erişilebildiği,

- Yukarıda sayılan her bir satış kanalından yapılan rezervasyonlar için öncelikle ödemenin alındığına dair “alındı belgesi”, ardından da rezervasyon detaylarını ve şartlarını içeren “voucher” düzenlendiği, “voucher”in rezervasyonun onayı için hem ilgili tesisle hem de misafirin rezervasyon detayları ile bu rezervasyonun şartlarına hakim olmasını sağlamak amacıyla misafir ile paylaşıldığı, misafir ile paylaşım acente üzerinden yapılan satışlarda misafire elden imza karşılığı teslim edilerek yapılmakta iken, çağrı merkezi ve internet üzerinden gerçekleştirilen satışlarda rezervasyon sırasında bildirilen e-posta adresine gönderilmek suretiyle yapıldığı,

- Log mekanizmasında yazılımların içindeki erişim, değişiklik ve görüntülemelerin tarih, saat ve kişi bazlı olarak kayıt yapıldığı, yaşanabilecek siber saldırılardan korunmak için güvenlik duvarı sistemlerinin bulunduğu, güvenli paylaşımı sağlamak amacıyla güvenli bir dosya paylaşımı uygulamasının kullanıldığı, bu suretle veri sorumlusu tarafından yapılan paylaşımların kişi bazlı olarak gözlemlenebildiği, verilerin veri sorumlusu şirket içerisinde kullanılan cihazlardan USB, e-posta gibi yöntemlerle dışarı çıkarılmasının gerektiğinde engellenmesi ve yine log kaydı alınması için bir “Veri Kayıp Önleme” (DLP) ürününün satın alınıp kurumsal ekiplerinde konumlandırıldığı,

- Şikâyet konusu rezervasyonun Çağrı Merkezi üzerinden yapıldığı, rezervasyona ilişkin ilk e-posta gönderiminin 20.11.2018 tarihinde ilgili kişinin e-posta adresine rezervasyonun onaylanması için gönderildiği, bu işlemin onaylanmaması sebebiyle 21.11.2018 tarihinde tekrar e-posta gönderildiği, daha sonra konaklama tarihinin yaklaşması sebebiyle aynı adrese 05.12.2018 tarihinde rezervasyon hatırlatma e-postası gönderildiği

hususları belirtilerek veri sorumlusu tarafından ilgili kişi ile kurulan tüm iletişimin log kayıtlarına dair ekran görüntüleri Kurum ile paylaşılmıştır.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 18/03/2021 tarihli ve 2021/242 sayılı Kararı ile,

- Kanunun “Tanımlar” başlıklı 3 üncü maddesinde “kişisel veri”nin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi; “veri sorumlusu”nun, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi; “veri işleyen”in, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi; “kişisel verilerin işlenmesi”nin, kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı,

- Konaklama satın almaya ilişkin işlemlerin tur şirketinin kendisine ait çağrı merkezi üzerinden yürütülmesi; rezervasyon takibinin yapıldığı ve otel ile tur şirketi arasındaki ilişkiyi kuran satışa ilişkin tek bir satış altyapısının varlığı ve bunun kurulması ve yönetilmesinden tur şirketinin sorumlu olması sebebiyle tur şirketinin Kanunun 3 üncü maddesinde tanımlanan veri sorumlusu sıfatını taşıdığı,

- “Voucher” ve “alındı” belgelerinde kimlik bilgileri kategorisinde ilgili kişinin adı soyadı, doğum tarihi gibi kişisel verilerin yer aldığı,

- Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinde ise kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, bu çerçevede, kişisel veriler ancak; hukuka ve dürüstlük kurallarına uygun şekilde, belirli, açık ve meşru amaçlar kapsamında, doğru ve gerektiğinde güncel olma şartıyla, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceğinin düzenlendiği,

- Kanunun kişisel verilerin işleme şartlarının belirlendiği 5 inci maddesinin (1) numaralı fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmadan işlenemeyeceği hüküm altına alınmış olmakla birlikte, (2) numaralı fıkrasında, sayılan hallerde ilgili kişinin açık rızası olmadan kişisel verilerinin işlenmesine imkan tanıdığı, buna göre;

a) Kanunlarda açıkça öngörülmesi,

- b) Fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
- c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- d) İlgili kişinin kendisi tarafından alenileştirilmiş olması,
- e) Bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması,
- f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması

hallerinden birinin varlığı durumunda ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün bulunduğu,

- Kanunun 12 nci maddesinin (1) numaralı fıkrasında ise veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu hükmünün yer aldığı,
- Somut olayda, ilgili kişinin rezervasyonuna ilişkin log kayıtlarının ekran görüntülerine ilişkin detaylar incelendiğinde; rezervasyon işlemine ilişkin görüntüleme detaylarının 25 satırda takip edildiği, bunlardan ilk 16 adetinin ilgili kişinin veri sorumlusuna yaptığı başvuruya istinaden farklı saatlerdeki görüntüleme kayıtları olduğu, geri kalan 9 adetinin de Kurumdan gönderilen tebligata istinaden tekrar kontrol amaçlı olarak şirket içindeki görüntülemeye yönelik log kayıtlarının olduğu, her bir görüntüleme işlemine ilişkin olarak log kayıtlarının IP numarası dahil kullanıcı adını(USER_NAME) içerecek şekilde tutulduğu, yukarıda bahsi geçen 25 satırlık log kaydına ilişkin olarak 4 farklı kullanıcı tarafından rezervasyon ve sonrasındaki inceleme işlemlerine yönelik kaydın yer aldığı görüldüğü,
- İlgili kişiye gönderilen e-postaların iletim tarihi ve adresine ilişkin olarak log kayıtlarına bakıldığında, veri sorumlusu tarafından ilgili kişinin e-posta adresine 20.11.2018, 21.11.2018 ve 05.12.2018 tarihlerinde şikâyete konu rezervasyon için elektronik posta gönderildiği, bu mesajların içeriğine ilişkin log kayıtlarına bakıldığında; 20.11.2018 ve 21.11.2018 tarihinde gönderilen e-

postaların onay için olduđu, 05.12.2018 tarihinde gönderilen e-postada ise rezervasyona ilişkin bilgilendirme yapıldığı,

- Ayrıca, “voucher” dokümanının acente üzerinden yapılan satışlarda misafire elden imza karşılığı verilirken, çağrı merkezi ve internet üzerinden gerçekleştirilen satışlarda rezervasyon sırasında bildirilen e-posta adresine gönderildiği, benzer şekilde “alındı” dokümanının konaklamanın yapılacağı tesis ile paylaşılmadığı ve sadece misafir ile e-posta üzerinden paylaşıldığı

değerlendirmelerinden hareketle;

- Şikâyet dosyasında yer alan konaklamaya ilişkin detayları içeren “Alındı” belgesinin sadece konaklamayı satın alan tarafla paylaşılan bir doküman olduđu ve konaklamanın yapılacağı tesis ile paylaşılmadığı; veri sorumlusunun Kuruma sunduđu log kayıtlarında konaklamaya ilişkin gönderilen “voucher” ve “alındı” dokümanlarının sadece ilgili kişinin e-posta adresine iletildiğinin belirlendiği ve konaklamaya yönelik veri sorumlusu personelinin yaptığı görüntülemelerin her birinin söz konusu belgelerin mahkemeye sunulma tarihi olan 04.04.2019 tarihinden sonra ve ilgili kişinin başvurusuna ve/veya Kurum tarafından yapılan bilgi ve belge talebine istinaden yapılan görüntülemeler olduđu dikkate alındığında, ilgili kişinin verilerinin veri sorumlusu tarafından paylaşıldığını tevsik eden somut bilgi ve belge bulunmadığından ilgili şikâyet hakkında 6698 sayılı Kanun kapsamında tesis edilecek bir işlem bulunmadığına karar verilmiştir.

2021/241 sayılı KVKK Kararı

Ölenin sigorta poliçesine yasal mirasçısının erişim talebinin sigorta şirketi tarafından reddedilmesi hakkında Kişisel Verileri Koruma Kurulunun 18/03/2021 tarihli ve 2021/241 sayılı Karar Özeti

Karar Tarihi : 18.03.2021

Karar No : 2021/241

Konu Özeti : Ölenin sigorta poliçesine yasal mirasçısının erişim talebinin sigorta şirketi tarafından reddedilmesi

Kuruma intikal eden şikâyet dilekçesinde özetle; şikâyetçinin ölen eşi ile veri sorumlusu sigorta şirketi arasında Hayat Sigortası Sözleşmesi kurulduğu, şikâyetçinin eşinin ölüm sebebinin iş kazası olduğunun mahkeme ilamı ile kesinleşmesi üzerine iş kazası nedeni ile yapılması gereken ödeme miktarının tespit edilebilmesi için Poliçenin ibrazı gerekliliğinin hâsıl olduğu, bu kapsamda çeşitli tarihlerde gönderilen ihtarnamelerle veri sorumlusundan söz konusu Poliçenin tesliminin talep edildiği, ancak veri sorumlusunca ilgili kişiye gönderilen yazı ile Kişisel Sağlık Verileri Hakkında Yönetmeliğin 10 uncu maddesi uyarınca “avukatların, müvekkilin sağlık verilerini genel vekaletname ile talep edemeyeceği, ilgili kişinin özel nitelikli kişisel verilerin işlenmesi ve aktarılmasına ilişkin açık rızasını gösteren özel bir hükmün bulunmasının gerektiği ve bu sebeple yazı ekinde gönderilen vekaletnamenin genel vekaletname niteliğinde olduğundan KVKK ve ilgili yönetmelik uyarınca özel nitelikli kişisel veri olan sağlık verilerinin paylaşılmasının mümkün olmadığı” hususları belirtilerek talebin reddedildiği, bunun üzerine şikâyetçinin kendi adına yeniden ihtarname düzenleyip veri sorumlusuna başvurduğu ancak veri sorumlusunca talebin karşılanmayarak hak yoksunluklarına sebep olduğu belirtilmiş ve gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme kapsamında veri sorumlusu sigorta şirketinden savunması istenilmiş, alınan cevabi yazıda özetle;

- Şikâyetçinin eşinin sigorta ettireninin bir banka olduğu ve Grup Hayat Sigorta Poliçesi ile sigortalı olduğu,

- Veri sorumlusu sigorta şirketi ile sigorta ettiren arasında imzalanan Grup Sigortası Sözleşmesi kapsamında sigorta ettiren tarafından bildirilen SGK'lı çalışanların sigortalandığı, şikâyetçinin eşinin de bu çalışanlardan biri olarak Grup Hayat Sigorta Poliçesi ile sigortalandığı, bu kapsamda murislere toplamda 100.000,00 TL (poliçe teminatının tamamı) ödeme yapıldığı, Poliçe teminatının tamamının murislere ödenmesiyle veri sorumlusunun Poliçe kapsamındaki tüm yükümlülüklerini yerine getirdiği,
- Şikâyet konusu Poliçenin müteveffanın eşi varise verilmemesinin hukuki gerekçesi ile ilgili olarak Poliçenin, sigorta ettiren banka ile veri sorumlusu arasında imzalanan Grup Hayat Sigortası arasındaki Sözleşmeye istinaden düzenlenmiş olduğu, sigortalıların bu grup sözleşmesinin tarafı olmadığı, 6102 sayılı Türk Ticaret Kanununun (TTK) 1496 ncı maddesi uyarınca Grup Hayat Sigortası Sözleşmesine/Poliçesine istinaden sigortalılara ayrı ayrı Poliçeler yerine sertifikalar verildiği,
- Müteveffanın sigortalılığını, sigortalı olduğu dönemi ve sigorta teminatı ile kapsamı gösteren Grup Yıllık Yaşam Sigortası Sertifikasının da veri sorumlusu tarafından şikâyetçi ile paylaşıldığı,
- Diğer taraftan Grup Hayat Sigortası Sözleşmesinde sigorta ettiren bankaya ait ticari bilgilerin ve o sözleşmeyi imzalayanların kişisel verilerinin yer aldığı, dolayısıyla müteveffanın tarafı olmadığı Grup Hayat Sigortası sözleşmesinin ve buna istinaden düzenlenen Grup Poliçesinin de ne sigortalılarla ne de murisleri ile paylaşma yükümlülüklerinin bulunmadığı,
- Veri sorumlusunun tüm kanuni yükümlülüklerini yerine getirdiği ancak şikâyetçinin Poliçe kapsamındaki alacağın tam olarak ödenmediğine ilişkin bir kuşkusu varsa, bu Grup Sigortası Sözleşmesinin içeriğini sigorta ettiren ve müteveffanın işvereni olan bankadan talep edebileceği gibi şikâyet dilekçesinde bahsettiği dava dosyasının görülmesi sırasında mahkeme aracılığı ile de pekâlâ celp ettirebileceği, şikâyetçinin daha fazla alacağı olduğunu düşünüyorsa veri sorumlusu aleyhine yargı yoluna da başvurabileceği,
- Kanunun 11 inci maddesi gereği ilgili kişinin kural olarak kendisiyle ilgili konularda veri sorumlusuna başvurabilme hakkına sahip olduğu ancak şikâyetçinin, eşine ilişkin talep etmiş olduğu Poliçe bilgileri, sertifika, teminat ödemesi vb. hususları eksiksiz paylaşılmış olmasına ve ortada kendisine ait Kanuna aykırı işlenen veri bulunmazken, sigortacılık mevzuatı açısından da tüm yükümlülüklerini yerine getiren veri sorumlusuna yönelik yapılan şikâyetin haksız olduğu ifade edilmiştir.

Konuya ilişkin olarak yapılan değerlendirme neticesinde Kişisel Verileri Koruma Kurulunun 18/03/2021 tarih ve 2021/241 sayılı Kararı ile;

• 6698 sayılı Kanununun 3 üncü maddesinde ilgili kişinin “kişisel verileri işlenen gerçek kişi” olarak tanımlandığı, 4721 sayılı Türk Medeni Kanununun 28 inci maddesinde ise kişiliğin, çocuğun sağ olarak tamamıyla doğduğu anda başladığı ve ölümle sona erdiği hükmünün yer aldığı, diğer taraftan; Kişisel Sağlık Verileri Hakkında Yönetmeliğin 4 üncü maddesinde; kişisel sağlık verisinin kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgiler olarak tanımlamalara yer verildiği; anılan Yönetmeliğin “Ölünün sağlık verilerine erişim” başlıklı 11 inci maddesinde ise ölmüş bir kimsenin sağlık verilerini almaya, veraset ilamını ibraz etmek suretiyle mirasın yasal mirasçılarının münferit olarak yetkili olduğuna yer verildiği, ölen kişilere ilişkin kişisel veriler hakkında 6698 sayılı Kanunda doğrudan bir düzenleme bulunmamasıyla birlikte Kişisel Verileri Koruma Kurulunun “Ölü kişilerin verilerine, ölenin yakınlarının erişim talebi hakkındaki 18/09/2019 tarihli ve 2019/273 sayılı kararında “(...) talep edilen kişisel verilerin talep eden gerçek kişiye ilişkin olmaması ve ölmüş kişiye ait olması sebebiyle talebin, Kanununun 11’inci maddesi kapsamında bir talep olarak değerlendirilmeyeceği kanısına varıldığından bu hususta 6698 sayılı Kanun kapsamında yapılacak bir işlemin olmadığına” karar verildiği,

• Diğer taraftan 4721 sayılı Türk Medeni Kanununun 499 uncu maddesinde ise sağ kalan eşin, birlikte bulunduğu zümredeki oranlara göre mirasbırakana mirasçı olacağı; 599 uncu maddesinde “Mirasçılar, mirasbırakanın ölümü ile mirası bir bütün olarak, kanun gereğince kazanırlar. Kanunda öngörülen ayırık durumlar saklı kalmak üzere mirasçılar, mirasbırakanın aynî haklarını, alacaklarını, diğer malvarlığı haklarını, taşınır ve taşınmazlar üzerindeki zilyetliklerini doğrudan doğruya kazanırlar ve mirasbırakanın borçlarından kişisel olarak sorumlu olurlar.” hükmüne; “Özel durumlar” başlıklı 601 inci maddesinin ikinci fıkrasında ise “Kendisine mirasbırakanın ölümünde ödenecek bir sigorta alacağı vasiyet edilen kimse, sigorta sözleşmesinden doğan istem hakkını sigortacıya karşı doğrudan doğruya kullanabilir.” hükmüne yer verildiği, bu doğrultuda ölen eşin kişiliğinin de ölümle birlikte sona erdiği dikkate alındığında her ne kadar hayat sigortası ölen eşin adına yapılmış ve kişilik ölümle son bulduğundan ölen kişinin kişisel verilerine ilişkin talepler Kanun kapsamında değerlendirilemeyecek olsa da, hayat sigortasının lehtarlarının ölen kişinin kanuni mirasçıları olduğu, bu çerçevede ilgili Sigorta Poliçesinin lehtarı olmaları bakımından mirasçıların ilgili kişi niteliği kazandığı, bu sebeple başvurucu için de kanuni mirasçılıktan kaynaklı olarak, Poliçeyi özetler belgede yer alan verilerin kişisel veri niteliği taşıdığı kanaatine varıldığı,

• Kanununun 11 inci maddesinde de “(1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili; a) Kişisel veri işlenip işlenmediğini öğrenme, b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

c) Kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme haklarına sahiptir.” hükmünün düzenlendiği,

- Öte yandan, 6102 sayılı Türk Ticaret Kanununun (Ticaret Kanunu) “Grup sigortaları” başlıklı 1496 ncı maddesinde “(2) Grupta yer alan her kişiye poliçe içeriğini özetleyen bir belge verilir.” hükmüne yer verildiği, bu kapsamda, ilgili kişinin eşi adına yapılan sigortanın da grup sigortası olarak yapıldığı gözetildiğinde, 6698 sayılı Kanunun 11 inci maddesi kapsamında talep edilebilecek belgenin grup poliçesinin kendisi yerine “poliçeyi özetler nitelikteki belgenin/sertifikanın” olabileceği kanaatine varıldığı,

- Anayasanın 20 nci maddesinin (3) numaralı fıkrasında yer verilen düzenleme ile “(...) kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme (...)” hakkına sahip olduğu, Kanunun 11 inci maddesinin (1) numaralı fıkrasının (b) bendi çerçevesinde ise ilgili kişilerin kişisel verileri işlenmişse buna ilişkin bilgi talep etme hakkına sahip olduğu düzenlemelerinin yer aldığı, bu çerçevede ilgili kişinin eşinin kanuni mirasçılıktan kaynaklı olarak müteveffanın kişisel verisi niteliğindeki “poliçeyi özetler belgeye” erişme hakkının olduğu ve bu hakkını veri sorumlusuna karşı ileri sürebileceği dikkate alındığında veri sorumlusundan kişisel veri niteliğinde olan “poliçeyi özetler belgeyi” Kanunun 11 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında talep edebileceği ve somut olayda veri sorumlusu tarafından “Poliçeyi özetler belgenin/sertifika”nın ilgili kişiye verildiği; bu anlamda Kanunun 11 inci maddesinden kaynaklanan erişim hakkının kişiye sağlandığı

değerlendirmelerinden hareketle;

- 6698 sayılı Kişisel Verilerin Korunması Kanununun 3 üncü maddesinde ilgili kişinin “kişisel verileri işlenen gerçek kişi” olarak tanımlandığı, 4721 sayılı Türk Medeni Kanununun 28 inci maddesinde ise kişiliğin, çocuğun sağ olarak tamamıyla doğduğu anda başladığı ve ölümle sona erdiği hükmünün yer aldığı, ölen eşin kişiliğinin de ölümle birlikte sona erdiği dikkate alındığında her ne kadar hayat sigortası ölen eşin adına yapılmış ve kişilik ölümle son bulduğundan ölen kişinin kişisel verilerine

ilişkin talepler Kanun kapsamında değerlendirilemeyecek olsa da, hayat sigortasının lehdarlarının ölen kişinin kanuni mirasçıları olduğu, bu çerçevede ilgili Sigorta Poliçesinin lehdarı olmaları bakımından mirasçıların ilgili kişi niteliği kazandığı, bu sebeple ilgili kişi için de kanuni mirasçılıktan kaynaklı olarak, poliçeyi özetler belgede yer alan verilerin kişisel veri niteliği taşıdığı; öte yandan grup sigortalarına ilişkin hususların 6102 sayılı Türk Ticaret Kanununda düzenlendiği, sigortalanan kişilere poliçe yerine poliçeyi özetler belgenin verileceğinin anılan Kanunda hüküm altına alındığı ve somut olayda veri sorumlusu tarafından "Poliçeyi özetler belgenin/sertifika"nın ilgili kişiye verildiği; bu anlamda Kanunun 11 inci maddesinden kaynaklanan erişim hakkının kişiye sağlandığı dikkate alındığında söz konusu şikayet hakkında Kanun kapsamında yapılacak bir işlem olmadığına karar verilmiştir.

2021/238 sayılı KVKK Kararı

Veri Sorumluları Siciline Kayıt Tarihlerinin Uzatılması İle İlgili Kişisel Verileri Koruma Kurulunun 11/03/2021 Tarihli ve 2021/238 Sayılı Kararı

Karar Tarihi : 11.03.2021

Karar No : 2021/238

Konu Özeti : Veri Sorumluları Siciline kayıt tarihlerinin uzatılması

RG Tarih ve Sayısı: 16.03.2021/31425

Dünyada olduğu gibi ülkemizde de etkisini gösteren salgın nedeniyle Sicile kayıt yükümlülüğünün yerine getirilmesi hususunda zorluklar yaşandığı gerekçesiyle Sicile kayıt sürelerinin uzatılmasına ilişkin birçok veri sorumlusu veya bunların bağlı olduğu üst kuruluşlar ile bazı kamu kurumları ve kamu kurumu niteliğindeki meslek kuruluşları tarafından Kuruma intikal ettirilen taleplerin değerlendirilmesi neticesinde;

- Yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları ile yurtdışında yerleşik gerçek ve tüzel kişi veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.12.2021 tarihine,
- Yıllık çalışan sayısı 50'den az ve yıllık mali bilançosu 25 milyon TL' den az olup ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek ve tüzel kişi veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.12.2021 tarihine,
- Kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşu veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.12.2021 tarihine kadar uzatılmasına,
- Anılan kararın Kurum internet sayfasında duyurulması ve Resmi Gazetede yayımlanmasına oybirliği ile karar verilmiştir.

2021/230 sayılı KVKK Kararı

İlgili kişinin kişisel verisinin kamu kurumu personeli olarak görev yapan eski eşi tarafından sorgulanarak elde edilmesi ve adli makamlar ile paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 11/03/2021 tarihli ve 2021/230 sayılı Karar Özeti

Karar Tarihi : 11.03.2021

Karar No : 2021/230

Konu Özeti : İlgili kişinin kişisel verisinin kamu kurumu personeli olarak görev yapan eski eşi tarafından sorgulanarak elde edilmesi ve adli makamlar ile paylaşılması

Kuruma intikal eden şikâyet dilekçesinde özetle; ilgili kişinin kamu kurumu personeli olarak görev yapan, boşanma sürecinde olduğu eşi tarafından görevi kötüye kullanmak suretiyle kendisine erişim yetkisi verilen bir sistem üzerinden, maaş bilgilerinin sorgulandığı, boşanma davasına ilişkin yargılama sürecinde talep edilmemesine rağmen bu bilginin mahkeme ile paylaşıldığı, belirtilen bu program ya da sistemle T.C. kimlik numarası bilinen kişilerin maaşlarının öğrenilmesinin hem 4A/4B bilgisinin kişiselliğine hem de özel şirketlerdeki maaş gizliliğinin ihlaline sebebiyet verdiği hususları ifade edilerek Kanun kapsamında gereğinin yapılması talep edilmiştir.

İlgili kişinin şikâyeti hakkında Kurumca başlatılan inceleme çerçevesinde veri sorumlusu kamu kurumunun açıklamalarına başvurulmuş olup, alınan cevabi yazıda özetle;

- Konu ile ilgili olarak İl Müdürlüğünden bilgi ve belge talep edildiği,
- Tabi olunan mevzuat kapsamında, Kurumları ile Sosyal Güvenlik Kurumunun (SGK) görev-yetki alanına giren iş ve işlemlerin ilintili olması nedeniyle tüm personel tarafından ilgili Kurum Portalına erişim sağlanabildiği ve "kontrol arayüzü" üzerinden sınırlı şekilde iş ve işlemler gerçekleştirilebildiği,
- Bu sınırlı erişim içerisinde kişilerin kimlik numaraları ile çeşitli sorgulamalar yapılabildiğinden, adı geçen personel de dahil olmak üzere tüm personel tarafından hem rutin işler için hem de günlük rutin dışı talepler nedeniyle söz konusu sorgulamanın sürekli yapıldığı,
- Öte yandan anılan İl Müdürlüğünce, Kanun ile ilgili Kurumun tüm personelinin defaten bilgilendirildiği ve talimatlandırıldığı bildirildiği,

• Şikayete konu veri işleme faaliyetini gerçekleştiren personelin konuya ilişkin açıklamalarının alındığı, yapılan açıklamada söz konusu kişi tarafından rutin işinin bir parçası olarak bahsi geçen sorgulamaları sıkça yaptığı, eşinin memur maaş zammına ilişkin kendisini haberdar etmesi üzerine ve kendisinin bilgisi dâhilinde bahsi geçen bilgileri sorguladığı, söz konusu zaman diliminde evliliğin aynı çatı altında sürdüğü, Kanunen aynı konutta yaşayanların istisna kapsamında olduğu ve bahsi geçen bilgilerin eşin bilgisi dahilinde sorgulanmasının sakınca teşkil etmediğini düşündüğü, boşanma davasında eşinin iddiasının aksine maaş bilgisinin paylaşılmadığı, bu bilgileri eşi dışında hiç kimse ile paylaşmadığı ve bu hususta mahkemeden bilgi talep edilebileceği ayrıca söz konusu Portaldan sehven kişisel sorgulama yapması hasebiyle Hizmet Merkezlerince “yazılı olarak” uyarıldığı belirtilmiştir.

ifade edilmiştir.

Konuya ilişkin olarak yapılan incelemede Kişisel Verileri Koruma Kurulunun 11/03/2021 tarihli ve 2021/230 sayılı Kararı ile;

• Kanunun “Tanımlar” başlıklı 3 üncü maddesinde “kişisel veri”nin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi, “veri sorumlusu”nun, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi, “kişisel verilerin işlenmesi”nin ise kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı,

• Kanunun, kişisel verilerin işlenmesine ilişkin “Genel İlkeler”i düzenleyen 4 üncü maddesinin (1) numaralı fıkrasında, “Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.” hükmü yer almakta olup bahse konu maddenin (2) numaralı fıkrasında ise kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin;

a) Hukuka ve dürüstlük kurallarına uygun olma,

b) Doğru ve gerektiğinde güncel olma,

c) Belirli, açık ve meşru amaçlar için işlenme,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayıldığı,

- Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise Kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Somut olayda veri sorumlusu Kurum bünyesinde, kişilerin kimlik numaraları ile SGK Sorgulaması yapılması kapsamında kişisel verilerin işlenmesinin Kanunun 5 inci maddesinin 2 numaralı fıkrasının (ç) bendine göre veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olduğu, bununla birlikte veri sorumlusunun hizmetlerini elektronik ortamda sürdürmesine ilişkin mevzuatta “Kişisel Verilerin Korunması” başlıklı maddede sistemde yer alan kişisel verilerin kullanılmasında mevzuatta yer alan özel hayatın gizliliğine ilişkin hükümlerin esas alınacağı, ayrıca kullanıcılardan alınan bilgilerin, tanımlanmış hizmetler ve yasal mükellefiyetlerin yerine getirilmesi dışında başka bir amaçla kullanılamayacağı düzenlendiği,

- Bu doğrultuda ilgili kişinin kişisel verisinin, kendisi tarafından talep edilmeksizin görev yapan eski eşi tarafından Portal üzerinden sorgulanarak elde edildiği ve söz konusu kişisel verilerin mahkeme ile paylaşıldığı da dikkate alındığında, kişisel veri işleme faaliyetinde kişisel verilerin, hem üçüncü kişilere verildiği hem de görev yetkisi ve tanımlanmış hizmetin dışında bir işleme faaliyetinde işlendiği göz önünde bulundurulduğunda kişisel verilerin hukuka aykırı işlenmesi ve erişilmesini önlemek ile muhafazasını sağlamak amacıyla veri güvenliğine ilişkin yükümlülüklerle uyulmadığı sonucuna varıldığı,

değerlendirmelerinden hareketle,

- İlgili kişinin kişisel verisinin, veri sorumlusu bünyesinde çalışan bir personel tarafından tanımlanmış hizmetlerin ve yasal mükellefiyetlerin yerine getirilmesi dışında başka bir amaçla kullanılması suretiyle işlenmesinin Kanunun 5 inci maddesinde yer alan işleme şartlarından birine dayanmaması nedeniyle hukuka aykırı olduğu ayrıca Kanunun 4 üncü maddesinin (2) numaralı fıkrasının (ç) bendinde yer alan kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak işlenmesi ilkesine aykırı bir veri işleme faaliyetinin gerçekleştiği, bu kapsamda söz konusu faaliyetinin Kanunun 12 nci maddesinin (1) numaralı fıkrasına aykırılık teşkil ettiği değerlendirildiğinden Kanunun 18 inci maddesinin (3) numaralı fıkrası uyarınca veri sorumlusu bünyesinde görev yapan söz konusu personel hakkında disiplin hükümlerine göre işlem yapılması, öte yandan kişisel verilere erişim yetkisi bulunan personelin söz konusu verilere amacı dışında erişmesinin önlenmesi hususunda 31/05/2018 tarih ve 2018/63 sayılı Kişisel Verileri Koruma Kurulu İlke Kararı da dikkate alınarak gerekli tedbirlerin alınması ve yapılacak işlemlerin sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına karar verilmiştir.

2021/228 sayılı KVKK Kararı

Hukuk Bürosu tarafından ilgili kişinin kişisel verilerinin muhatabı ve tarafı olmadığı icra takibi ile ilgili işlemlerde hukuka aykırı olarak işlenmesi ve icra dosyasına ilişkin ilgili kişinin telefon numaralarına mesajlar gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 11/03/2021 tarihli ve 2021/228 sayılı Karar Özeti

Karar Tarihi : 11.03.2021

Karar No : 2021/228

Konu Özeti : Hukuk Bürosu tarafından ilgili kişinin kişisel verilerinin muhatabı ve tarafı olmadığı icra takibi ile ilgili işlemlerde hukuka aykırı olarak işlenmesi ve icra dosyasına ilişkin ilgili kişinin telefon numaralarına mesajlar gönderilmesi

Kuruma intikal eden şikayette özetle ilgili kişinin şahsına ait telefon numaralarına çeşitli tarihlerde, muhatabı ve tarafı olmadığı icra dosyası ile ilgili (alacaklı telekomünikasyon şirketi adına hareket eden) hukuk bürosu tarafından mesajlar gönderildiği, söz konusu mesajlarla ilgili herhangi bir muhataplık sıfatının, mesajda bahsi geçen icra dosyasında ise alacaklı ya da borçluluk sıfatının bulunmadığı, bunun üzerine gerek alacaklı telekomünikasyon şirketi gerek avukat-hukuk bürosuna yaptığı başvuruya yasal süre içerisinde yanıt alamaması nedeniyle Kişisel Verileri Koruma Kuruluna şikâyetle bulunulduğu belirtilmiştir.

Bu kapsamda başlatılan inceleme çerçevesinde söz konusu iddialara ilişkin veri sorumlusunun tespit edilebilmesini teminen alacaklı telekomünikasyon şirketi ve hukuk bürosundan savunması istenilmiştir.

Şikayet edilen telekomünikasyon şirketinden alınan cevabi yazıda özetle;

- İlgili kişinin telefon numaralarına mesajları ileten avukat ile telekomünikasyon şirketi arasında Avukatlık Sözleşmesi akdedildiği, bahsi geçen Avukatlık Sözleşmesi uyarınca avukatın, bu sözleşme ve yasal takip prosedürleri kapsamında şirkete dair her türlü icra, dava, tahsilat ve takip işlemlerini yürüttüğü ve buna istinaden taraflarca sözleşmede belirlenen ücrete hak kazandığı ve avukat ile paylaşılan tek bilginin borçlu tüzel kişi bilgisi ile borç bilgisi olduğu,

- Avukatın, hukuk bürosunda kendine özgü veri kayıt ortamında kendi belirlediği yöntemlerle ve vasıtalarla veri işleme faaliyetini gerçekleştirdiği, dolayısıyla şirket ile avukat arasında akdedilen vekâlet sözleşmesi uyarınca faaliyetlerini yürüten avukatın ayrı bir veri sorumlusu sıfatını haiz olup 6698 sayılı Kanun ve ikincil düzenlemeleri kapsamında gerçekleştireceği veri işleme faaliyetleri kapsamında şirketleri ile aynı yükümlülüklerle sahip olduğu,

- İlgili kişinin başvurusuna cevap verilmemesine ilişkin şirketin web sitesinde yer alan ve Kanununun 10 uncu maddesi kapsamında oluşturulmuş aydınlatma metninde ilgili kişilerin Kanununun “İlgili kişinin hakları” başlıklı 11 inci maddesi kapsamında başvurularını iletebilecekleri adreslere yer verildiği, ilgili kişinin söz konusu aydınlatma metninde belirtilen adreslerine/ilgili kanallarına herhangi bir başvurusunun bulunmadığının tespit edildiği, bu sebeple bahse konu taleplerinin değerlendirilemediği

ifade edilmiştir.

Şikâyet ile ilgili olarak Kurumca istenilen savunmasına istinaden alacaklı telekomünikasyon şirketi adına hareket ettiği belirtilen avukat tarafından Kuruma intikal ettirilen cevap yazısında ise özetle;

- İlgili kişi tarafından usulüne uygun olarak yapılan ve taraflarına tebliğ edilmiş bir başvurunun bulunmadığı, Tebligat Kanununun 32 nci maddesinde yer aldığı üzere tebliğ usule aykırı olmuş olsa dahi muhatabın tebliği öğrenmesi halinde tebliğin geçerli olacağı ancak taraflarına usulüne uygun bir tebligat yapılmadığından Kuruma şikayette bulunulmayacağı ve şikayetin incelenmesinin hukuken mümkün olmadığı,

- Borcun alacaklısı şirket ile aralarında vekâlet ilişkisi bulunduğu, bu itibarla alacaklı şirketin avukatlığı görevinin taraflarınca yürütüldüğü, aralarındaki vekâlet ilişkisi sebebiyle alacakların tahsil edilebilmesi için taraflarınca icra takipleri başlatıldığı ve avukat-müvekkil ilişkisi çerçevesinde tüm hukuki işlemlerin yürütüldüğü, avukatlık mesleği gereğince Avukatlık Kanunu ve ilgili diğer tüm mevzuat çerçevesinde avukatların vekil olarak müvekkillerinin her türlü hak ve menfaatlerini gözetmek durumunda olduğu,

- Şikayete konu icra dosyası ve borcun tahsili açısından dosya borçlusu şirket hakkında yapılan araştırma neticesinde Ticaret Sicil Gazetesi üzerinden borçlu şirketin ortağı olarak ilgili kişinin ismine ulaşıldığı, Bilgi Teknolojileri Kurumu tarafından yetkilendirilmiş rehberlik hizmeti sağlayan bir kuruluşun sunduğu hizmetten yararlanarak ilgili kişinin telefon numaralarına ulaşıldığı ve borçlu şirket yetkililerine borcun bildirildiği, kişilerin telefon numaralarına ulaşılmasının ardından şirket borcundan dolayı ortakların sorumlu olduğu iddiasında hiçbir zaman bulunulmadığı yalnızca şirket

borcundan dolayı şirket yetkililerine borç bildirildiği, söz konusu telefon numaralarının Avukatlık Kanununun 35/A maddesi gereğince uzlaşma sağlamak amacıyla arandığı ve mesaj gönderildiği, bununla birlikte, müvekkilin hukuki menfaatlerini korumak adına borçlunun iletişim bilgilerine ulaşma çabasının hak arama hürriyeti kapsamında değerlendirilmesi gerektiği

hususları belirtilmiştir.

Konuya ilişkin olarak yapılan değerlendirme neticesinde Kişisel Verileri Koruma Kurulunun 11/03/2021 tarih ve 2021/228 sayılı Kararı ile;

- Kanunun "Tanımlar" başlıklı 3 üncü maddesinde "kişisel veri"nin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi, "veri sorumlusu"nun, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi, "kişisel verilerin işlenmesi"nin ise kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı,

- Kanunun "Kişisel Verilerin İşlenme Şartları" başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanunun 12 nci maddesinde "(1) Veri sorumlusu; a) kişisel verilerin hukuka aykırı işlenmesini önlemek, b) kişisel verilere hukuka aykırı erişilmesini önlemek, c) kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. (2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya

tüzel kişi tarafından işlenmesi halinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur. (3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır...” hükümlerine yer verildiği,

- Somut olayda, Kuruma iletilen yasal takip otomasyon sistemlerine ilişkin ekran görüntülerinde yalnızca borçlu olan tüzel kişinin bilgisinin yer aldığı, herhangi bir iletişim bilgisinin yer almadığı görüldüğünden alacaklı telekomünikasyon şirketinin şikâyete konu olayda veri sorumlusu sıfatını haiz olmadığı,

- Bu doğrultuda veri sorumlusunun, vekil sıfatıyla taraflarına devredilen icra dosyası kapsamındaki veri işleme süreçlerinde serbestçe karar verme yetkisine sahip olan ve ilgili kişinin şikâyetine konu kişisel verilerinin işleme amaç ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan hukuk bürosu adına hareket eden ilgili avukat olduğu,

- Avukatların müvekkilleri adına, müvekkilin hak ve menfaatlerini korumak amacıyla hareket ettiği durumlarda Avukatlık Kanunundan kaynaklanan yükümlülükleri ve yürütmekte olduğu icra işlemleri bakımından İcra İflas Kanunu ve ikincil mevzuat düzenlemelerinden kaynaklanan hukuki yükümlülüklerini yerine getirmek amacıyla borçluya ait bilgileri, kanuna uygun olarak işleme ve ilgili birim/mercilere bildirme yetkisi olduğu ve bu bağlamda işlediği kişisel verileri Kanunun 5 inci maddesinin (2) numaralı fıkrası çerçevesinde ilgili kişinin açık rızası olmaksızın işleminin kanuna uygun olduğu,

- İlgili kişinin borçlu Şirket ile olan ilişkisine ilişkin, veri sorumlusunun yazı ekinde ilettiği Ticaret Sicil Gazetesinden ilgili kişinin borçlu Şirketin ortağı olduğunun görüldüğü, ancak bu kapsamda yapılan incelemede, ilgili kişinin hissesini devrettiği ve Şirket ortaklığının son bulduğunun değerlendirildiği, borçlu Şirket ortaklığının son bulduğu bilgisinin Ticaret Sicil Gazetesinde ilan edildiği,

- İncelemeye konu olayda, ilgili kişinin borçlu Şirket ortaklığının son bulduğu bilgisinin 31.03.2015 tarihinde Ticaret Sicil Gazetesinde ilan edildiği, ancak borçlu Şirketin icra takibine ilişkin mesajların ilgili kişiye 2019 tarihinde gönderildiği hususları göz önünde bulundurulduğunda bu süre zarfında veri sorumlusu tarafından Ticaret Sicil Gazetesi üzerinden yapılan araştırmada ilgili kişinin borçlu Şirket ortaklığının son bulduğu bilgisine de ulaşabileceği sonucuna varıldığı,

- İlgili kişi tarafından gönderilen başvuru dilekçesi ve dilekçenin tebliğine ilişkin PTT Gönderi Takip belgesinin incelenmesi neticesinde, başvurusunun veri sorumlusuna teslim edildiğinin anlaşıldığı

değerlendirmelerinden hareketle,

- Alacaklı telekomünikasyon şirketinin veri sorumlusu sıfatını haiz olmadığı değerlendirildiğinden hakkında yapılacak bir işlem olmadığına,
- Veri sorumlusu sıfatını haiz olduğu değerlendirilen avukat tarafından halihazırda herhangi bir ilgisinin bulunmadığı borçlu şirketin icra takibine ilişkin mesajlar gönderilmesi suretiyle ilgili kişinin kişisel verisi olan telefon numaralarının işlenmesinin Kanunun 5 inci maddesinde sayılan işleme şartlarından herhangi birine dayanmadığı değerlendirildiğinden Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendi kapsamında kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri alma yükümlülüğünü yerine getirmediği kanaatine varılan veri sorumlusu avukat hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca idari para cezası uygulanmasına,

İlgili kişilerin başvurularına Kanunun ilgili maddeleri ile Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğe uygun bir cevap verilmesi kapsamında gerekli dikkat ve özenin gösterilmesi hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2021/227 sayılı KVKK Kararı

Bir eğitim kurumu tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmaksızın işlenmesi ve ilgili numaraya reklam içerikli SMS gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 11/03/2021 tarihli ve 2021/227 sayılı Karar Özeti

Karar Tarihi : 11.03.2021

Karar No : 2021/227

Konu Özeti : Bir eğitim kurumu tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmaksızın işlenmesi ve ilgili numaraya reklam içerikli SMS gönderilmesi

Kuruma iletilen şikâyet dilekçesinde özetle; ilgili kişinin, şahsına ait cep telefonuna açık rızası olmaksızın bir eğitim kurumu tarafından reklam/bildirim amaçlı SMS gönderilmesi üzerine veri sorumlusuna yaptığı başvuruya yasal süre içerisinde yanıt alamadığı, ihlalin yaygın olduğu ve benzer mesajların herkese gönderildiğinin düşünüldüğü ifade edilerek eğitim kurumu hakkında gerekli işlemlerin tesis edilmesi istenilmiştir.

Bu kapsamda başlatılan inceleme çerçevesinde söz konusu iddialara ilişkin veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- Veri sorumlusunun SMS gönderme uygulamasının olmadığı ve ilgili kişiye mesaj gönderilmediği,
- Veri sorumlusu tarafından işletilen bir eğitim kurumu bulunmadığı, çeşitli kurumlar ile isim hakkı sözleşmesi düzenlendiği, bu anlamda isim hakkı sözleşmesi düzenlenen ve eğitim alanında hizmet sunan bir şirketin şikâyete konu SMS gönderim eylemini gerçekleştirdiği, söz konusu şirketin SMS gönderimini yasal olarak gerçekleştirdiklerini beyan ettikleri ve şikâyete ilişkin bilgi ve belgelerin bu firmadan talep edilmesi gerektiği ifade edilmiştir.

Bu kapsamda, ilgili kişinin şikâyeti hakkında bahsi geçen şirkete bilgi verilmiş, başvuruda belirtilen iddialara ilişkin savunması istenilmiş olup, alınan cevabi yazıda;

- Anket yapan firmalardan belirli aralıklarla sosyal medya ve SMS onayı veren kişilerin bilgilerinin alındığı; ancak bu bilgilerin alınabilmesi için anket dolduran kişilerin SMS ya da başka iletişim araçlarına onay vermiş olmasının şart olduğu,

- Şikâyete konu olaydaki telefon numarasının da bir medya anket şirketinden alındığı bununla birlikte sosyal medya ve toplu SMS anket formunu dolduran kişi tarafından, anketin doldurulması esnasında iletişim bilgisi olarak sehven şikâyetçinin iletişim bilgisinin verildiği, kendilerinin bunu denetleme imkanının olmadığı,

- Anket içeriğinde SMS gönderimine izin verildiği, şirketlerinin onay vermeyen kimseye SMS göndermediği; dolayısıyla şirketlerinin ihlal iddiasına ilişkin bir kusurunun bulunmadığı ifade edilmiştir.

Konuya ilişkin olarak yapılan değerlendirme neticesinde Kişisel Verileri Koruma Kurulunun 11/03/2021 tarih ve 2021/227 sayılı Kararı ile,

- Kanunun “Kişisel verilerin işleme şartları” başlıklı 5 inci maddesinde;“(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (2) Aşağıdaki şartlardan birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.” hükmünün yer aldığı,

- Kanunun “Tanımlar” başlıklı 3 üncü maddesinin (1) numaralı fıkrasının (a) bendinde açık rızanın, “belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza” olarak tanımlandığı, açık rızanın, Kanunda hukuka uygunluk sebeplerinden biri olduğu, Kurumca yayımlanan “Açık Rıza” Rehberine göre; açık rıza açıklamasının, ilgili kişinin işlenmesine izin verdiği verinin sınırlarını, kapsamını ve gerçekleştirilme biçimini de belirlemesini sağlaması, bu kapsamda açık rızanın, rıza veren kişinin “olumlu irade beyanı”nı içermesi gerektiği, açık rızanın alındığına dair ispat yükümlülüğünün veri sorumlusuna ait olduğu, kişisel veri işlemek üzere verilen açık rızanın

geçerli olması için açık rızanın belirli bir konuya ilişkin ve o konu ile sınırlı olması, veri sorumlusu tarafından açık rıza beyanının hangi konuya ilişkin olarak istenildiğinin açıkça ortaya konulması gerektiği, açık rıza bir irade beyanı olup, kişinin özgür bir şekilde rıza gösterebilmesi için, neye rıza gösterdiğini de bilmesi gerektiği, kişinin sadece konu üzerinde değil, aynı zamanda rızasının sonuçları üzerinde de tam bir bilgi sahibi olması gerektiği, bilgilendirme yapılırken elde edilecek kişisel verilerin hangi amaçlarla kullanılacağına açıkça belirtilmesinin önemli olduğu,

- Veri sorumlusunca anket yapan firmalardan belirli aralıklarla sosyal medya ve SMS onayı veren kişilerin bilgilerinin alındığı beyanı karşısında; yazıları ekinde gönderilen “Sosyal Medya ve Toplu SMS Anket Formu”nun incelenmesi sonucunda anketin 9 uncu sorusunun “Firmalardan ürünler hakkında bilgi ve tanıtımlarını SMS yoluyla almak ister misiniz” şeklindeki genel nitelikli bir sorunun, “Evet” olarak anlaşıldığı, veri sorumlusu tarafından iletilen belgede açık rızanın unsurlarının bulunmadığı, açık rızanın belirli bir konuya ilişkin olması gerektiği, belirli bir konu ile sınırlandırılmayan ve ilgili işlemle sınırlı olmayan genel nitelikteki açık rızaların “battaniye rızalar” olarak kabul edileceği ve hukuken geçersiz sayılacağı hususları doğrultusunda, söz konusu sosyal medya şirketi tarafından yapılan ankette yer alan genel bir soruya verilen cevabın açık rıza kapsamında değerlendirilemeyeceği,

- Ankette belirtilen numaranın anketi dolduran kişiden farklı bir kişiye ait olması ve veri sorumlusunun bu durumu kontrol etme şansının bulunmadığı iddiası karşısında; açık rızanın alındığına ilişkin ispat yükümlülüğünün veri sorumlusuna ait olması nedeniyle “belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza” tanımına uygun şekilde açık rızanın alınmamış olduğu, battaniye rızanın açık rıza olarak değerlendirilemeyeceği,

- Veri sorumluları tarafından kişilerin telefon numarası, e-posta adresi gibi iletişim kanallarına Kanuna aykırı şekilde gönderilen üçüncü kişilere ait kişisel veriler hakkında Kişisel Verileri Koruma Kurulunun 22/12/2020 tarihli ve 2020/966 sayılı İlke Kararı kapsamında; Kanunun 12 nci maddesinin (1) numaralı fıkrası gereğince veri sorumluları tarafından kendilerine bildirilen iletişim bilgilerinin doğruluğunu teyit edecek mekanizmaların oluşturulması adına gerekli idari ve teknik tedbirlerin alınması gerektiği,

- Ticari elektronik iletilere ilişkin alınacak onayların şekline ilişkin 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanununun 6 ncı maddesinin “Ticari elektronik iletiler, alıcılara ancak önceden onayları alınmak kaydıyla gönderilebilir.” hükmünü amir olduğu, 15.07.2015 tarihli ve 29417 sayılı Resmi Gazete’de yayımlanan Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmeliğin 7 nci maddesinin (1) numaralı fıkrasında “Onay, yazılı olarak veya her türlü elektronik iletişim

aracıyla alınabilir. Onayda, alıcının ticari elektronik ileti gönderilmesini kabul ettiğine dair olumlu irade beyanı, adı ve soyadı ile elektronik iletişim adresi yer alır.”, (3) numaralı fıkrasında “Onayın elektronik ortamda alınması durumunda, onayın alındığı bilgisi, reddetme imkanı da tanınmak suretiyle, alıcının elektronik iletişim adresine aynı gün içinde iletilir.”, (10) numaralı fıkrasında ise “Onayın alındığına ilişkin ispat yükümlülüğü hizmet sağlayıcıya aittir.” hükümlerinin yer aldığı değerlendirmelerinden hareketle;

- Veri sorumlusunun ticari elektronik ileti göndermesi suretiyle ilgili kişinin kişisel verisi olan telefon numarasını işleminin Kanunun 5 inci maddesinde sayılan şartlardan birine dayanmadığı dikkate alındığında Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendi kapsamında kişisel verilerin hukuka aykırı olarak işlenmesi önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almadığı kanaatine varılan veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca idari para cezası uygulanmasına,
- Hukuka aykırı işlendiği tespit edilen kişisel verilerin yok edilmesi hususunda veri sorumlusu eğitim kurumunun talimatlandırılmasına,
- Şikâyete konu olayda ismi geçen medya şirketi tarafından yapılan ankette “Firmalardan ürünler hakkında bilgi ve tanıtımlarını SMS yoluyla almak ister misiniz” şeklindeki sorunun belli bir şirketi işaret eder nitelikte olmadığı, genel nitelikte bir soru olduğu, bu anket kapsamında kişilerden alınan “evet” şeklindeki cevapların açık rıza olarak değerlendirilmesi suretiyle adı geçen eğitim kurumu ile paylaşıldığı, bu çerçevede anket firmasının veri sorumlusu olabileceğinden hareketle söz konusu şirket hakkında Kanunun 15 inci maddesinin (1) numaralı fıkrası kapsamında resen inceleme başlatılmasına

karar verilmiştir.

2020/216 sayılı KVKK Kararı

Bir bilişim şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 12/03/2020 tarih ve 2020/216 sayılı Karar Özeti

Karar Tarihi : 12.03.2020

Karar No : 2020/216

Konu Özeti : Bir bilişim şirketinin kişisel veri ihlali bildirimini

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Veri sorumlusu Şirketin sistemlerine siber saldırı gerçekleştirilerek sistemlerinde yer alan verilerin elde edilmeye çalışıldığı,
- Pilot adı verilen uygulamada debugging özelliğinin açık olduğu ve şirket için sistem geliştirmesi yapan geliştiricilerin bu özelliği kullanarak uygulamadaki hataları tespit ettiği ve iyileştirme gerçekleştirdiği,
- İhlale konu siber saldırı ile Pilot uygulamasına internet üzerinden erişim sağlamaya çalışan kişinin(lerin), uygulamaya daha önce giriş yapmış kişilere ait "PHPSESSID" değerini elde ettiği ve Pilot uygulamasına erişim sağladığı,
- Debugging özelliğinin açık olmasının sebebinin sisteme internet üzerinden erişilerek geliştirmelerin yapılmasına olanak sağlamak olduğu, ancak bu durumun internet üzerinden siber saldırılar gerçekleştirilerek sisteme erişilmesine olanak tanıdığı,
- Sistemde saldırganlar tarafından erişilen verilerin neler olduğunun net bir şekilde tespit edilemediği ancak veri sorumlusunun sistemlerinde yer alan verilerin tümü dikkate alındığında sistemde 65.993 kişinin yer aldığı, bu kişilerin sadece teklif almış, üyelik oluşturmuş, herhangi bir şekilde hizmet almış, aktif olan ve olmayan kişileri içerdiği,
- İlgili kişilere ilişkin sistemde yer alan kayıtların 1259 sözleşme, 701 alan adı başvuru dosyası (içerisinde imza sirküleri, vergi levhası ve kişi kimlik fotokopisi kayıtları) olduğu,

- Sistemde ayrıca elli bin kredi kartı bilgisi yer aldığı, ancak bu kredi kartı bilgilerinin büyük çoğunluğunun son kullanma tarihinin geçmiş olduğu ve kullanılamayacağı, sadece sekiz bin kartın aktif olduğunun tespit edildiği,
- İhlalden etkilenen kişi kategorilerinin müşteriler ve potansiyel müşteriler olduğu,
- Saldırganların hangi verilere eriştiklerinin tespit edilemediği, sistemde yer alan verilerin kimlik, iletişim, işlem güvenliği (kullanıcı adı ve parola bilgileri), ödeme Bilgileri (kredi kartı numarası) olduğu,
- Ele geçirilen kredi kartı bilgilerinin 2018 tarihi öncesinde veri sorumlusu Şirkete aktarılan bilgiler olduğu, 2016 tarihi itibari ile ödeme hizmetlerinde iyileştirme çalışmaları kapsamında bir proje başlatıldığı, 2018 yılı itibariyle kredi kartı bilgilerinin yetkilendirilmiş ödeme hizmet sağlayıcıları üzerinden toplanmakta ve onlar tarafından saklanmakta olduğu,
- Veri ihlalden doğrudan etkilenen özel nitelikli bir veri bulunmadığı, ancak tüzel kişi müşterilerin imza sirkülerinin ekinde yer alan eski kimlik fotokopilerinde kan grubu ve din bilgisi hanelerinin bulunduğu ve bazı imza sirkülerinde kimlik fotokopisinin arka yüzünün de yer alabildiği dikkate alınarak; bazı müşteriler için saldırırganların bu verilere de erişme ihtimali olabileceği,
- Sistemde yer alan tüm kayıtların incelendiği ve sayımlarda (imza sirkülerlerinde yer alan kimlik fotokopileri de dahil) 1.784 adet eski kimlik fotokopisinin arkalı önlü yüzünün bulunduğu tespit edildiği,
- İhlalden etkilenen tüm müşterilere e-posta göndermek suretiyle bildirimde bulunulduğu, bir kısım müşterilere mümkün olduğunca telefonla da bilgilendirme gerçekleştirildiği

ifadelerine yer verilmiştir.

Söz konusu bildirim incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 12/03/2020 tarih ve 2020/216 sayılı sayılı Kararı ile;

- Sistemde saldırırganlar tarafından erişilen verilerin neler olduğunun net bir şekilde tespit edilememesinin, veri sorumlusu tarafından sızma veya herhangi bir anomali olup olmadığının belirlenmesi noktasında kontrol ve uyarı mekanizmalarının etkin bir şekilde kullanılmadığının göstergesi olduğu,
- Veri sorumlusu tarafından hangi kişisel verilerin etkilendiğinin tespit edilemediği ancak sistemlerde 65.993 kişinin yer aldığı, bu kişilerin sadece teklif almış, üyelik oluşturmuş, herhangi bir

şekilde hizmet almış, aktif olan ve olmayan kişileri içerdiği, bu kişilerden 1.784 tanesinin eski kimlik fotokopisinin arkalı önlü yüzünün bulunduğu ayrıca elli bin kredi kartı bilgisi yer aldığı,

- Veri sorumlusunun kredi kartı bilgilerinin büyük çoğunluğunun son kullanma tarihinin geçmiş olduğu ve kullanılmayacağı, sadece sekiz bin kartın aktif olduğu, 2018 yılı itibariyle kredi kartı bilgilerinin yetkilendirilmiş ödeme hizmet sağlayıcıları üzerinden toplandığı ve onlar tarafından saklandığı bu çerçevede veri sorumlusunun ödeme sistemini değiştirmiş olmasına rağmen sistemde bulunan kredi kartı bilgilerini imha etmeyerek 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 4 üncü maddesinin (2) numaralı fıkrasının (b) ve (ç) bendine aykırı hareket ettiği,

- Şirket dışından erişim için güvenlik amacıyla VPN ile Şirket IP'sine bağlanıldığı ve kişilere özel kullanıcı adı ve VPN şifresi verildiği, saldırganların da sisteme SFTP ve VPN aracılığı ile bağlandığı, ihlalden sonra 29.01.2020 tarihinde yapılan ve veri sorumlusu tarafından Kurumumuza gönderilen sızma testinde özellikle web uygulamalarında yüksek ve orta seviyede açıklıkların tespit edildiği göz önüne alındığında bu durumun veri sorumlusu tarafından gerekli teknik tedbirlerin alınmadığının göstergesi olduğu,

- Veri sorumlusunun https://www.****.com.tr adresinde domain ve hosting hizmetlerinin satın alındığı ekranları incelendiğinde satın alma süreçlerinde kimlik ve iletişim bilgilerinin talep edildiği ancak herhangi bir aydınlatma metninin bulunmadığı göz önüne alındığında veri sorumlusunun 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında yükümlülüklerini yeterli seviyede yerine getirmediği kanaatine varıldığı,

- Veri sorumlusu tarafından ihlal öncesi alınması gereken teknik tedbirlerin (çift faktör özelliği olan sistemlerde bu özelliğin aktifleştirilmesi, VPN erişimde kullanılan sertifikaların yenilenmesi, çalışanlarının e-posta erişimlerinin iki aşamalı kimlik doğrulama olarak güncellenmesi, log kayıtlarının adli olaylarda kanıt niteliğinde kullanılabilmesi için zaman damgasıyla damgalanması, logların korelasyonunun sağlanması vb) ihlal sonrası devreye alınmasının gerekli teknik ve idari tedbirlerin alınmadığının göstergesi olduğu

değerlendirmelerinden hareketle, Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik tedbirleri almayan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 450.000 TL idari para cezasının uygulanmasına,

- Veri ihlalinin 09.10.2019 tarihinde 14:04'de gerçekleştiği, 11.10.2019 tarihinde saat 14.04'de veri sorumlusu tarafından tespit edildiği, 14.10.2019 tarihinde Kurula 72 saat içinde bildirildiği

dikkate alındığında bu hususta yapılacak bir işlem bulunmadığına karar verilmiştir.

2021/205 sayılı KVKK Kararı

İşten çıkarma sürecinde veri sorumlusu işveren tarafından ilgili kişinin kişisel verilerinin hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 09/03/2021 tarihli ve 2021/205 sayılı Karar Özeti

Karar Tarihi : 09.03.2021

Karar No : 2021/205

Konu Özeti : İşten çıkarma sürecinde veri sorumlusu işveren tarafından ilgili kişinin kişisel verilerinin hukuka aykırı olarak işlenmesi

İlgili kişinin Kuruma intikal eden şikâyetinde özetle; ilgili kişinin iş sözleşmesinin feshedildiği tarihe kadar veri sorumlusu şirketin bir çalışanı olduğu, veri sorumlusu tarafından ilgili kişiye noter aracılığıyla ihtarname gönderilerek iş sözleşmesinin haksız olarak sona erdirildiği, işten çıkarma sürecinde şahsına ait iş eşyalarının yanı sıra ailevi özel eşyalarına da el konulduğu, veri sorumlusu şirketin çalışanlarının iş yerindeki odasına girerek masasında yer alan şirket bilgisayarını izinsiz ve haber vermeden aldığı, e-posta hesabının kapatıldığı, e-postalarına erişiminin ve e-posta göndermesinin engellendiği, bilgisayar ve e-postalarına bakıldığı, ilgili kişinin odasında arama yapıldığı, bunların yanında ilgili kişinin şahsına ait kişisel harici hard diskin de alındığı, özel bilgi ve belgeleri, banka bilgileri ve şifreleri ile fotoğraflarının ekrana yansıtılmak suretiyle odasında bulunan kişilerce izlendiği ve bu suretle veri sorumlusu tarafından kişisel verilerine karşı ihlal gerçekleştirildiği ifade edilerek veri sorumlusu hakkında gerekli incelemenin yapılması talep edilmiştir.

Bu kapsamda başlatılan inceleme çerçevesinde söz konusu iddialara ilişkin veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- İlgili kişinin kişisel verilerinin, veri sorumlusunun eski çalışanı olması nedeniyle başta İş Kanununun 75 inci maddesi ve Sosyal Sigorta İşlemleri Yönetmeliğinin 107 nci maddesi olmak üzere sair mevzuat uyarınca tutulması gereken iş yeri belgelerinin 10 yıl süre ile saklanmasını gerektiren yasal zorunluluk ve ilgili kişi ile veri sorumlusu arasında halen devam etmekte olan davaların takibi

amacıyla tutulduğu, söz konusu kişisel verilerin saklama sürelerinin sonunda mevzuata uygun şekilde silineceği, yok edileceği veya anonim hâle getirileceği,

- İlgili kişinin veri sorumlusunun eski çalışanı olması sebebiyle işlenen ve ilgili kişiyle devam etmekte olan davalar nedeniyle tutulan kişisel veriler dışında, ilgili kişiye ait “özel hard disk” ve “şifrelerin” veri sorumlusu bünyesinde saklanmadığı veya sair yollarla taraflarınca işlenmediği,
- 7036 sayılı İş Mahkemeleri Kanununun İş Mahkemelerinin görevlerini düzenleyen 5 inci maddesinin birinci fıkrasının (a) bendinde yer alan “5953 sayılı Kanuna tabi gazeteciler, 854 sayılı Kanuna tabi gemi adamları, 22/5/2003 Tarihli ve 4857 sayılı İş Kanununa veya 11/1/2011 tarihli ve 6098 sayılı Türk Borçlar Kanununun İkinci Kısımının Altıncı Bölümünde düzenlenen hizmet sözleşmelerine tabi işçiler ile işveren veya işveren vekilleri arasında, iş ilişkisi nedeniyle sözleşmeden veya kanundan doğan her türlü hukuk uyuşmazlıklarına” ifadesi ile Türk Borçlar Kanununda yer alan hizmet sözleşmelerinin İş Mahkemelerinin görev alanında olduğunun anlaşıldığı,
- Türk Borçlar Kanununun İşçinin Kişiliğinin Korunması başlığı altında yer alan, Kişisel Verilerin Kullanılması alt başlıklı 419 uncu maddesinin “İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir.” şeklinde olduğu, bu düzenleme ile İş Mahkemelerinin görev alanında kişisel verilerin nasıl kullanılacağı (işleneceğinin) veya kullanılmayacağı (işlenemeyeceğinin) yer aldığı, mahkemenin bu konuda bir değerlendirmede bulunurken kişisel verilerin korunması ile ilgili tüm mevzuatı göz önünde bulunduracağı açık olduğu,
- Bununla birlikte mahkemenin ilgili kişi tarafından ileri sürülen bu iddialara herhangi bir sonuç bağlamadığı, yukarıda belirtilen davalardaki taleplerin reddedildiği göz önünde bulundurulduğunda ilgili kişinin iddialarının mahkeme tarafından haklı bulunmadığının görüleceği, kaldı ki davaların hala istinaf aşamasında olmasının ilgili kişinin mahkeme tarafından haklı bulunmayan kişisel verilerle ilgili iddialarının istinaf aşamasında tekrar ileri sürmesi için bir imkân olduğu,
- İlgili kişinin kişisel verilerinin hukuka aykırı işlenmesi ile ilgili iddialarının Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesinin (b) bendi kapsamında söz konusu davalarda da öne sürüldüğü ve konunun yargının görev alanına girdiği, şikâyetçinin dile getirdiği konuları daha önce dava konusu yapmış olmasının Kurulun bu konuda bir karar almasına engel olduğu,

- Veri sorumlusu tarafından ilgili kişiye kullanımı için verilmiş olan dizüstü bilgisayarın işten çıkış aşamasında geri alındığı, kişinin dizüstü bilgisayarındaki veriler teslim alındıktan sonra hiçbir verisi kopyalanmadan, geri döndürülemeyecek şekilde silindiği,
- İlgili kişinin şirkete ait e-posta hesabının işten ayrıldıktan sonra kapatılmasının, şirket hesabı ile şirket adına işlem yapılmasının engellenmesi amacıyla uygulanan standart bir prosedür olduğu ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 09/03/2021 tarihli ve 2021/205 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,
- Kanunun “Veri Güvenliğine İlişkin Yükümlülükler”i düzenleyen 12 nci maddesinin (1) numaralı fıkrasında ise veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğunun hükme bağlandığı,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesi kapsamında yargı mercilerinin görevine giren konularla ilgili olan dilekçelerin Kurum tarafından incelenemeyeceği,
- Somut olayda ilgili kişinin Kuruma vermiş olduğu şikâyet dilekçesinde iddia ettiği hususları veri sorumlusu ile aralarında devam etmekte olan davalarda belirtmişse de bu davaların işçilik alacağı ve işe iade talepli davalar olduğu, bu dava dilekçelerinde ilgili kişinin, kişisel verileriyle ilgili iddialarını

da belirttiği ancak kişisel verilerine ilişkin bir talep oluşturmadığı, ilgili kişi tarafından bu davaların ikame edilmesindeki amacın kişisel verilerine yönelik koruma talep etmek değil işe iade ve işçilik alacağı olduğu,

- Veri sorumlusu tarafından verilen cevaptan ilgili kişinin kişisel verilerinin Kanunun 5 inci maddesinin (2) numaralı fıkrasının (ç) bendinde yer alan “veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması” hükmüne ve (e) bendinde yer alan “bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması” hükmüne istinaden gerçekleştirildiğinin anlaşıldığı,

- Diğer taraftan iş sözleşmesi feshedildikten sonra ilgili kişinin kullanımına tahsis edilen şirket bilgisayarının formatlanması ve şirket e-postasının kapatılmasının Kanuna aykırılık teşkil etmediği, iş sözleşmesinin sonlanmasından sonra veri sorumlusu şirket tarafından, işçinin e-posta adresinin kapatılmasının ve işçinin kullanımına tahsis edilmiş bilgisayarın geri alınmasının hayatın olağan akışı gereği olduğu, ilgili kişi e-posta adresinin kapatılması suretiyle hesabına erişiminin engellendiğini belirtmişse de bu durumun Kanuna aykırılık teşkil etmeyeceği,

- Yargıtay 9. Hukuk Dairesinin 05/02/2007 tarihli E.2006/30107, K.2007/2011 sayılı kararında bilgisayar kaynaklarının amacına uygun kullanılması ile ilgili işyeri iç düzenlemesine rağmen, davacının şirket bilgisayarını mesai saatleri içinde kişisel mailinde kullandığı, davacının bu davranışının şirketin iç işleyişi ile ilgili düzenlenen kurala aykırı olduğu gibi, mesai saatleri içinde kişisel ihtiyaçlarında işyeri bilgisayarını kullanarak iş görme edimini yeterince yerine getirmediği, bu davranışının işyerinde olumsuzluklara neden olduğu, feshin geçerli nedene dayandığı sonucuna varıldığı, buradan hareketle işçinin kullanımına tahsis edilen bilgisayar ve e-posta adreslerinin sadece iş görme amacıyla kullanılması gerektiğinin değerlendirildiği, dolayısıyla ilgili kişinin e-posta adresinin sadece iş ile alakalı hususları içeriyor olması gerektiği, bu durumda ilgili kişi ile aralarında iş ilişkisi kalmayan veri sorumlusuna ait şirket e-posta hesabına ilgili kişinin ulaşmasında yararının bulunmadığının değerlendirildiği, dizüstü bilgisayar açısından da durumun benzer olduğu, veri sorumlusu tarafından dizüstü bilgisayarın içindeki verilerin geri döndürülemez şekilde formatlanmış olduğu belirtildiği, sadece iş ile ilgili hususları içerdiği varsayılan bu bilgisayarın iş ilişkisi sonlandıktan sonra ilgili kişiden alınmasının Kanuna aykırılık teşkil etmediği,

- İlgili kişinin, kişisel harici hard diskinin, şahsına ve ailesine ait özel bilgilerinin, banka bilgilerinin, banka şifrelerinin ve fotoğraflarının ekrana yansıtılmak suretiyle odasında bulunan kişilerce izlendiğine ilişkin iddialarıyla ilgili dosya kapsamında tevsik edici bir bilgi veya belgeye yer verilmediği

değerlendirmelerinden hareketle;

- Veri sorumlusu ile ilgili kişi arasındaki iş sözleşmesi feshedildikten sonra ilgili kişinin kullanımına tahsis edilen şirket bilgisayarının formatlanması ve şirket e-postasının kapatılması suretiyle hesabına erişiminin engellenmesinin Kanuna aykırılık teşkil etmediğine,

- İlgili kişinin, kişisel harici hard diskinin, özel bilgi ve belgelerinin, şahsına ve ailesine ait özel şeylerin, banka bilgilerinin, banka şifrelerinin ve fotoğraflarının ekrana yansıtılmak suretiyle odasında bulunan kişilerce izlendiğine ilişkin iddialarıyla ilgili dosya kapsamında tevsik edici bir bilgi veya belge bulunmadığından bu aşamada yapılacak bir işlem bulunmadığına

karar verilmiştir.

2021/190 sayılı KVKK Kararı

Bankacılık sektöründeki veri sorumlusunun veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 04.03.2021 tarih ve 2021/190 sayılı Karar Özeti

Karar Tarihi : 04.03.2021

Karar No : 2021/190

Konu Özeti : Bankacılık sektöründeki veri sorumlusunun veri ihlal bildirimini hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Bir müşteri şikayeti üzerine Banka tarafından yapılan inceleme neticesinde, bir şube çalışanın kendisine tanımlanan Müşteri Bilgileri ve Belgeleri gözlem yetkisini, Banka erişim ve bilgi güvenliği politikalarına, verilen sınıf içi ve çevrimiçi eğitimlere, Banka ile olan iş sözleşmelerine ve ilgili menüye erişmeden önce çıkan uyarı mesajına aykırı şekilde, söz konusu müşterinin kimlik görüntüsünün amacı dışında gözlemlemesi; müşteriye ait gözlemlenen bilgilerin çalışanın şahsi cep telefonu ile fotoğrafının çekilmesi ve çalışan tarafından üçüncü kişiyle paylaşması suretiyle veri ihlali gerçekleştiği,
- Söz konusu olayda Banka sistemleriyle ilgili herhangi bir güvenlik açığının bulunmadığı, ihlalin çalışanın münferit davranışlarından kaynaklı olduğu sonucuna varıldığı,
- Veri ihlalinin, bir şube çalışanın kendisine tanımlanan Müşteri Bilgileri ve Belgeleri gözlem yetkisini amacı dışında kullanmasından ve 1 (bir) müşterinin kimlik bilgilerini yetkisiz kişiyle paylaşmasından kaynaklandığı,
- İhlal ile ilgili olan çalışanların Bilgi Güvenliği Farkındalığı Eğitimi ve Kişisel Verilerin İşlenmesi ve Korunmasında Temel Kavramlar Eğitimi aldığı

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 04.03.2021 tarih ve 2021/190 sayılı Kararı ile;

- Bulduğu görev pozisyonundan yararlanarak olaya konu Takım Lideri'nin şikayette bulunan ilgili kişinin bilgilerine erişebildiği ve yetkisini kötüye kullanabildiği, bu durumun veri sorumlusu

tarafından verilen veri gizliliği ve güvenliği eğitimlerine rağmen söz konusu çalışanın rol ve sorumlulukları hakkındaki farkındalığının sağlanamadığı göz önünde bulundurulduğunda Kurumumuzun yayınlamış olduğu Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nin Çalışanların Eğitilmesi ve Farkındalık Çalışmaları başlığı altındaki "Veri sorumlusu nezdinde çalışan herkesin hangi konumda çalıştığına bakılmaksızın kişisel veri güvenliğine ilişkin rol ve sorumlulukları, görev tanımlarında belirlenmeli ve çalışanların bu konudaki rol ve sorumluluğunun farkında olması sağlanmalıdır." düzenlemelerine aykırılık teşkil ettiği,

- Bankada Takım Lideri olarak çalışan personelin veri ihlali öncesinde müşteri bilgilerini istenilen sıklıkta ve sayıda sorgulama yaparak görüntüleyebildikleri ve bu durumun çalışan personel tarafından müşterilerin kişisel verilerinin ihlaline sebebiyet verebilecek bir durum olduğu ve bu durumun Kurumumuzun yayınlamış olduğu Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nin Çalışanların Eğitilmesi ve Farkındalık Çalışmaları başlığı altındaki "... kişisel veri içeren ortamlara erişim hakkı verilirken veya bu konuda kurum kültürü oluşturulurken "Yasaklanmadıkça Her Şey Serbesttir" prensibi değil, "İzin Verilmedikçe Her Şey Yasaktır" prensibine uygun hareket edilmesine dikkat edilmelidir" hususuna aykırılık teşkil ettiği,

- Risk Merkezi verilerinin sorgulanmasına yönelik sorgulama yapılabilecek kayıt sayısı/kota belirleme işlemlerinin veri ihlalden önce yapılmadığı, söz konusu ihlalden ancak yaklaşık iki yıl sonra çalışanlar için sorgulama kota limiti oluşturulduğu ve diğer müşteri sorgulamalarına kota oluşturulmasına yönelik çalışmalara halen devam edildiği,

- Veri sorumlusu bünyesinde Çağrı Merkezi Takım Lideri olarak görev yapan çalışanların, müşterilerin rızası dışında, müşteri bilgilerine sınırsız sayıda sorgulama yaparak erişebildiği, söz konusu çalışanlar için gerekli ölçüde yetki verilmediği dikkate alındığında Kurumumuzun yayınlamış olduğu Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nin Siber Güvenliğin Sağlanması başlığı altındaki "... kişisel veri içeren sistemlere erişimin de sınırlı olması gerekmektedir. Bu kapsamda çalışanlara, yapmakta oldukları iş ve görevler ile yetki ve sorumlulukları için gerekli olduğu ölçüde erişim yetkisi tanınmalı ve ... ilgili sistemlere erişim sağlanmalıdır." tedbirlerine aykırılık teşkil ettiği,

- Veri ihlali sonrasında, başka şube müşterisinin bilgilerini sorgulamak isteyen çalışanlara erişecekleri verileri iş ihtiyacı kapsamında ve görev tanımıyla uyumlu bir şekilde kullanabileceklerine dair uyarı sisteminin geliştirildiği, veri ihlali öncesinde herhangi bir uyarı sistemi kullanılmadığı

hususları dikkate alındığında, Kanununun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında

Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL idari para cezası uygulanmasına karar verilmiştir.

2021/187 sayılı KVKK Kararı

Bir sigorta şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 04.03.2021 tarih ve 2021/187 sayılı Karar Özeti

Karar Tarihi : 04.03.2021

Karar No : 2021/187

Konu Özeti : Bir sigorta şirketinin veri ihlal bildirimini hakkında karar

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin nasıl gerçekleştiği hakkında;
 - Bir emeklilik hizmeti kapsamında veri sorumlusunun müşterisi olan bazı firmalara sigorta hizmetine dâhil olan çalışanlarına dair "Rapor" iletildiği,
 - Veri sorumlusunun bilgi sistemleri hizmeti aldığı destek hizmeti sağlayıcısında meydana gelen sistemsel hata nedeniyle;
 - Sistem hizmeti kapsamında veri sorumlusunun müşterisi olan bazı firmalar ile "Rapor" ilişkilendirmesinde teknik bir hata nedeniyle sorun yaşandığı,
 - Sistem hizmeti kapsamındaki 28 müşteri şirkete, diğer 31 müşteri şirketin sisteme dâhil çalışanlarına dair "Rapor" dosyası gönderildiği,
 - "Raporu" seçen sorgunun hatalı çalışması" neticesinde, sistem kapsamında olan 31 işveren şirketin çalışanı 681 adet gerçek kişi müşterisine alt bilgilerin, yine sistem kapsamındaki 28 işveren şirkete, sistemsel olarak hatalı şekilde gönderildiği,
- İhlalin raporu alan müşteri firmanın konu hakkında telefonda bilgi vermesi sonucu tespit edildiği,
- İlgili dosyaya erişim sağlayan ve ihlali veri sorumlusuna bildiren firmanın telefon kanalı ile yapılan çağrı esnasında 19.02.2020 saat 09.55'te ihlal hakkında bilgi verdiği,
- Bu firmaya da ihlalden etkilenen tüm firmalara olduğu gibi bilgilendirme yapıldığı ve sehven gönderilen bilgilerin silinmesi gerektiğinin tekrarlandığı,
- İhlale konu yazılımın canlıya alınmadan önce test edildiği,

• İhlalden etkilenen kişisel verilerin TCKN / Mavi Kart No, Ad - Soyad, Planlanan Ara Verme Bitiş Tarihi Sözleşme Durumu bilgilerinin olduğu ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 04.03.2021 tarih ve 2021/187 sayılı Kararı ile;

• Veri sorumlusunun bilgi sistem destek hizmeti aldığı veri işleyende meydana gelen sistemselsel bir hata sonucu sorgunun hatalı çalışması nedeniyle emeklilik hizmeti kapsamında müşteri olan 31 işveren şirketin çalışanı olan 681 ilgili kişinin kişisel verilerini yine emeklilik kapsamında müşterilere gönderdiği (müşteri olan 28 işveren şirkete gönderilmiştir),

• Veri ihlaline sebep olan sistemselsel hatanın uygulama yazılımından kaynaklanması sebebiyle, Kurumumuz tarafından yayınlanan Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 3.5. Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı başlığı altında yer alan "Veri sorumlusu tarafından yeni sistemlerin tedariki, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmalıdır. Uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontroller yapılmalı, doğru girilmiş bilginin işlem sırasında oluşan hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmaları yerleştirilmelidir." ifadesi gereği, bu tip hataların işlem yayına alınmadan evvel düzeltilmesi gerektiği, ihlale konu olaydan önce tespitinin yapılamadığı,

• İhlale konu olayın gerçekleşme tarihi (18.01.2018) ile tespit tarihi (19.02.2020) arasında yaklaşık 2 yıllık bir gecikmenin bulunduğu hususunun, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 3.2. Kişisel Veri Güvenliğinin Takibi başlığında "...raporlama sürecinde oluşturulacak raporlar, sistem tarafından oluşturulacak otomatik raporlar olabilir. Bu raporların sistem yöneticisi tarafından en kısa sürede toplulaştırılarak veri sorumlusuna sunulması gerekmektedir. Ayrıca güvenlik yazılımı mesajları, erişim kontrolü kayıtları ve diğer raporlama araçlarının düzenli olarak kontrol edilmesi, bu sistemlerden gelen uyarılar üzerine harekete geçilmesi..." ifadesi gereği veri sorumlusunun gerekli kontrol ve denetimleri zamanında yapmadığının göstergesi olduğu,

• İhlalin raporu alan müşteri firmanın konu hakkında veri sorumlusuna bilgi vermesi sonucu tespit edildiği, veri sorumlusu tarafından kendiliğinden tespit edilemediği, bu durumun da Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 3.2. Kişisel Veri Güvenliğinin Takibi başlığı altında belirtilen "Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi gerekmektedir" ifadesine uymadığının bir göstergesi olduğu

hususları dikkate alındığında, Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 125.000 TL idari para cezası uygulanmasına,

- İhlale sebep olan sistemdeki hatanın 18.01.2018 ve 19.02.2020 tarihleri arasında gerçekleştiği, 19.02.2020 tarihinde ilgili dosyaya erişim sağlayan Şirket tarafından veri sorumlusuna bilgi verilmesi sonucu ihlalden haberdar olduğu, 21.02.2020 tarihinde Kurumumuza e-posta yoluyla veri ihlal bildiriminde bulunulduğu, ilgili yazının Kurum kayıtlarına 24.02.2020 tarihinde girdiği, bu açıdan veri sorumlusunun Kurulun 24.01.2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde bildirim koşulunun sağlandığı,
- İhlalden etkilenen ilgili kişilere 28.02.2020 tarihinde e-posta olarak bildirim yapılmaya başlandığı, e-posta bilgisi olmayan kişilere arama yapıldığı, görüşme yapılan tarih ve saatler ile bilgilendirme metin örneğinin tarafımıza gönderildiği

görülmekle birlikte, ilgili kişilere yapılacak bildirim Kurulun 18.09.2019 tarih ve 2019/271 sayılı Kararı ile belirlenen asgari unsurlardan ihlalin ne zaman gerçekleştiği, kişisel veri kategorileri bazında (kişisel veri / özel nitelikli kişisel veri ayrımı yapılarak) hangi kişisel verilerin ihlalden etkilendiği, kişisel veri ihlalinin olası sonuçları, veri ihlalinin olumsuz etkilerinin azaltılması için alınan veya alınması önerilen tedbirler hususlarında eksiklikler olduğu dikkate alındığında bundan sonra ilgili kişilere yapılacak bildirimlerde Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararına uygun olarak bildirimde bulunulması hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2021/154 sayılı KVKK Kararı

Bir sigorta şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 25.02.2021 tarih ve 2021/154 sayılı Karar Özeti

Karar Tarihi : 25.02.2021

Karar No : 2021/154

Konu Özeti : Bir sigorta şirketinin veri ihlal bildirimini hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin; veri sorumlusunun eski bir çalışanın görevi gereği erişimi bulunan bazı müşterilere ait kişisel verileri kurumsal e-posta adresinden gmail uzantılı şahsi e-posta adresine 3 ayrı tarihte ve 3 ayrı excel dosyasında göndermesiyle gerçekleştiği,
- İhlalin; veri sorumlusu tarafından tespit edilemeyip, eski çalışanın ihlale konu kişisel verileri çalışmaya başladığı yeni işyeri e-posta adresine göndermesi üzerine yeni işveren tarafında tespit edildiği,
- İhlalden etkilenen kişisel verilerin kimlik, iletişim ve araç plaka numaraları olduğu,
- İhlalden etkilenen kişi sayısının 544 olduğu ve bu kişilerden 422'sine ulaşılarak ihlalin gerçekleşme tarihi, kapsamı ve muhtemel etkileri hakkında bizzat bilgi verildiği,
- Veri sorumlusunun acentelik faaliyetleri kapsamında, ilgili çalışanlar tarafından işleri gereği müşterilere poliçe gönderimleri yapılması nedeni ile yoğun bir şekilde şirket dışına eposta gönderiminin yapıldığı, bu nedenle ihlal kapsamına alınabilecek olayların bu dönemde derhal fark edilemediği

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 25/02/2021 tarih ve 2021/154 sayılı Kararı ile,

- İhlalin eski çalışanın işinden ayrıldıktan sonra çalışmaya başladığı şirketin ilgili birimleri tarafından tespit edilip veri sorumlusuna bildirdiği,

- İhlalden 544 müşteriye ait; kimlik, iletişim ve araç plaka numaralarının etkilendiği,
- DLP sistemleri ile; belirli adedin üstünde T.C. Kimlik Numarası, kredi kartı numarası, IBAN, telefon numarası, e-posta adresi gibi kişisel verilerin bulunduğu belgelerin e-posta ile kurum dışına gönderilmesinin engellenmesinin mümkün olduğu, hatta veri sorumlusunun 2017 yılında bazı çalışanlara göndermiş olduğu e-postada; TCKN bilgileri, Kredi Kartı bilgileri ve IBAN bilgilerinin kurum içindeki hareketini ve dışına çıkışının izleneceği ve engelleneceğinin ifade edilmiş olduğu hususlarına rağmen, veri sorumlusunun DLP sisteminin ihlale konu e-postaların gönderilmesini engelleyememiş olmasının "Kişisel Veri Güvenliği Rehberi"nin "Siber Güvenliğin Sağlanması" başlığı altında yer alan "...her yazılım ve donanımın bir takım kurulum ve yapılandırma işlemlerine tabi tutulması gerekmektedir." ifadesine aykırı olarak bu sistemin doğru yapılandırılmadığını gösterdiği,
- Eski çalışanın kendi kişisel e-posta adresine yapmış olduğu son e-posta gönderiminin, bu tarihten 1 ay sonra, işten ayrılmasından dolayı hesabının kapatılması nedeniyle DLP Raporuna yansımamasının "Kişisel Veri Güvenliği Rehberi"nin "Kişisel Veri Güvenliğinin Takibi" başlığı altında yer alan "Tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması..." gerekmektedir ifadesine aykırılık teşkil ettiği,
- İhlale konu e-posta gönderimlerinin; kasım ve aralık aylarında gerçekleştirilmesine rağmen, 24.12.2019 tarihine kadar tespit edilemediği ve bu tarihteki tespitin de yeni çalışmaya başladığı şirket tarafından yapılarak, veri sorumlusuna bildirilmiş olduğu hususu ile 2017 yılında bazı çalışanlara gönderilen e-postada; DLP raporlarının departman yöneticileri ile paylaşılacağı ve ilgili veri paylaşımlarından bilgileri olup olmadığı sorulacağı ifade edilmesine rağmen, 2018 yılına ait iki DLP raporunda da dosyaların bulunduğu e-postalar hakkında personelin yöneticisine bildirim yapılmadığı hususlarının Veri Güvenliği Rehberi"nin "Kişisel Veri Güvenliğinin Takibi" başlığı altında yer alan "...erişim kontrolü kayıtları ve diğer raporlama araçlarının düzenli olarak kontrol edilmesi... gerekmektedir." ifadesine aykırı olarak gerekli kontrollerin sağlanmadığını gösterdiği,
- İhlal ile ilgili olan eski çalışana online kişisel veri koruma eğitimi açılmasına rağmen çalışanın 2 ay boyunca bu eğitime başlamadan işten ayrıldığı, bunun yanında eski çalışanın da içinde bulunduğu kullanıcılar grubuna bilgilendirmeler yapılmakla birlikte ilk bildirimde bilgilendirmede kişisel verilere ilişkin tanımlara yer verilip Kurumumuz internet sayfasında yer alan videoların bağlantısının paylaşıldığı, ikinci bilgilendirmede ise sadece ilgili kişilerin hak ve yükümlülüklerinin yer aldığı dikkate alındığında "Kişisel Veri Güvenliği Rehberi"nin "Çalışanların Eğitilmesi ve Farkındalık Çalışmaları" başlığı altında düzenlenen "... çalışanların kişisel verilerin hukuka aykırı olarak

açıklanmaması ve paylaşılmaması gibi konular hakkında eğitim almaları, çalışanlara yönelik farkındalık çalışmaları yapılması ve güvenlik risklerinin belirlenebildiği bir ortam oluşturulması kişisel veri güvenliğinin sağlanması bakımından çok önemlidir.” ifadesine aykırı olarak çalışana yönelik yapılan bilgilendirmelerin kişisel verilerin korunması hakkında bir takım genel hükümlerden ibaret olup, çalışanların kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi örneklendirilen temel konuları dahi içermeyen hususlarının veri sorumlusunun kişisel verilerin korunması hakkında eğitim verilmesine yeterli önemi vermediğini gösterdiği

dikkate alındığında, Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca, 150.000 TL idari para cezası uygulanmasına

- İhlalin; 24.12.2019 tarihinde tespit edildiği ve 27.12.2019 tarihinde Kurumumuza bildirildiği dikkate alındığında Kurul’un 24.01.2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde bildirim koşulunun sağlandığı dolayısıyla Kanun kapsamında yapılacak bir işlem olmadığına,

- Öte yandan, veri sorumlusu tarafından bundan sonra ilgili kişilere yapılacak bildirimlerin Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararına uygun olarak yapılmasına dikkat edilmesi hususunun veri sorumlusuna hatırlatılmasına

karar verilmiştir.

2021/140 sayılı KVKK Kararı

Belediyeler tarafından sunulan internet hizmetlerine ilişkin Kişisel Verileri Koruma Kurulunun 25/02/2021 tarih ve 2021/140 sayılı Karar Özeti

Karar Tarihi : 25.02.2021

Karar No : 2021/140

Konu Özeti : Belediyeler tarafından sunulan internet hizmetleri

Kurumumuza iletilen çeşitli ihbarlarda belediyelerin internet üzerinden emlak vergisi veya beyan bilgisini sorgulama sayfalarında yalnızca TC kimlik numarası girilerek vatandaşın emlak bilgilerine ulaşılmasının kişisel verilerin korunması açısından sorun teşkil ettiği ifade edilmiş, konunun 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında incelenmesi talep edilmiştir.

Konuya ilişkin başlatılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 25/02/2021 tarih ve 2021/140 sayılı Kararı ile;

- Kanununun 12 nci maddesinin (1) numaralı fıkrasında “Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.” hükmüne, anılan maddenin (4) numaralı fıkrasında veri sorumluları ile veri işleyen kişilerin öğrendikleri kişisel verileri Kanun hükümlerine aykırı olarak başkasına açıklayamayacağı ve işleme amacının dışında kullanamayacağı hükmüne, (5) numaralı fıkrasında ise işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri sorumlusunun bu durumu en kısa sürede ilgisine ve Kurula bildireceği, Kurulun, gerekmesi halinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebileceği hükümlerine yer verildiği,
- Kurumumuz internet sayfasında da yayımlanan “Kişisel Veri Güvenliği Rehberi”nde kişisel veri içeren sistemlere erişimin sınırlı olması gerektiği, kişilere yetki ve sorumlulukları için gerekli olduğu ölçüde erişim yetkisi tanınması ve kullanıcı adı ve şifre kullanılmak suretiyle ilgili sistemlere erişim sağlanabileceği, ayrıca uzaktan erişim için iki kademeli kimlik doğrulama kontrolünün uygulanmasının önemli olduğu hususlarına yer verildiği,

- Yapılan incelemeler neticesinde bazı belediyeler tarafından internet üzerinden verilen vergi ödeme hizmetlerinin üyelik ve şifre ya da çift doğrulama yolu ile sisteme giriş yapılması sureti ile gerçekleştirildiği ve bu uygulamaların Kanuna uygun olduğu, ancak bazı belediyeler tarafından sunulan hızlı sorgulama ya da borç ödeme uygulamalarında sadece tek bir bilgi girilerek kişilerin borç bilgisine ulaşılabildiği; her ne kadar kişiye ait isim ya da mülke ilişkin bilgilere erişim mümkün olmasa da borca ilişkin bilgiye erişim sağlanabildiğinin anlaşıldığı, bu durumun Kanununun 12 nci maddesinin 1 numaralı fıkrasının (b) bendinde yer alan hükme aykırı olduğu

değerlendirmelerinden hareketle;

- Bazı belediyelerin bu yöndeki Kanuna aykırı uygulamaları nedeniyle konu hakkında Çevre ve Şehircilik Bakanlığına ve Türkiye Belediyeler Birliğine bilgi verilmesine,

- Diğer taraftan, yalnızca tek bir bilginin girilerek (örneğin TC kimlik no, vergi no gibi) kişilerin borç ya da emlak bilgilerine erişim sağlanmasına yönelik uygulamalar yerine belediyeler tarafından sunulan emlak vergisi, beyan bilgisi veya benzeri nitelikteki hizmetlere ilişkin sorgulama sayfalarında veri güvenliğini arttırmaya yönelik olarak gerekli idari ve teknik tedbirlerin alınması, bu bağlamda örneğin çift katmanlı doğrulamayı mümkün kılacak şekilde TC Kimlik numarası ya da vergi numarasının girilmesinin yanı sıra kişilerden farklı kişisel verilerin de talep edilmesi, SMS ile doğrulama, üyelik yapılması gibi yöntemlerin seçilmesi ve bu itibarla belediyelerin hizmet sunma yöntemlerinin kişisel verilerin korunması mevzuatı çerçevesinde yeniden değerlendirilerek gerekli önlemlerin alınması hususunda Belediyelerin talimatlandırılmasına

karar verilmiştir.

2021/115 sayılı KVKK Kararı

Bankaya olan borcundan dolayı ilgili kişinin yakınına Bankanın sözleşmeli avukatı tarafından ilgili kişinin borç bilgisinin iletilmesi hakkında Kişisel Verileri Koruma Kurulunun 09/02/2021 tarihli ve 2021/115 sayılı Karar Özeti

Karar Tarihi : 09.02.2021

Karar No : 2021/115

Konu Özeti : Bankaya olan borcundan dolayı ilgili kişinin yakınına, Bankanın sözleşmeli avukatı tarafından ilgili kişinin borç bilgisinin iletilmesi

Kuruma intikal eden şikâyetle ilgili kişi tarafından, Bankaya olan borcu sebebiyle kız kardeşinin cep telefonu numarasının Bankanın sözleşmeli avukatı tarafından aranması ve cep telefonu numarasına SMS gönderilmesi suretiyle kişisel verisinin avukat tarafından hukuka aykırı olarak paylaşıldığı belirtilerek, 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında veri sorumlusu hakkında gereğinin yapılması talep edilmiştir.

Konuya ilişkin olarak başlatılan inceleme çerçevesinde Bankanın sözleşmeli Avukatından savunması istenilmiş olup, alınan cevabi yazıda özetle;

- Bankanın gecikmiş alacaklarının gerek yasal gerek idari takibini gerçekleştirdiği, vekâlet ilişkisi çerçevesinde tarafınca ulaşılmaması beklenen müşterilere ait tüm iletişim numaralarının müvekkili Banka tarafından "irtibat bilgisi" olarak iletilmesi, söz konusu iletişim bilgilerinin müvekkili Banka tarafından borçlu adına olan numaraların sorgulanması neticesinde referans bilgileri olarak gönderilmesi sebebiyle iletişim numarasını kullanmakta olan kişilerin dosyayla olan ilgisinin bilinmesinin ilk aşamada mümkün olmadığı, başka bir deyişle tarafınca sadece tevdi alınan dosyalar ile birlikte iletilen iletişim numaraları üzerinden borçlulara ulaşıldığı, ne var ki ilk aşamada tespit edilebilmesi mümkün olmamasına karşın mevcut bir numaranın borçlu ile ilgisi olmadığının anlaşılması halinde ivedilikle durumun Bankaya bildirildiği ve borçluya ait olmayan numaranın sistemden çıkartıldığı,
- Banka ile arasında bir "vekâlet ilişkisi" nin söz konusu olduğu, Bankanın bankacılık faaliyetleri kapsamında müşterilerine ait birçok kişisel veriyi işlediği, Bankadan kredi kullanmış fakat

ödemesinde gecikmiş müşterilerin öncelikle uhdesinde bulunan bir ekip tarafından arandığı ve ödemeye davet edildiği, kendilerine tanınan süre içerisinde ödeme gerçekleştirilmeyen müşterilere ait dosyaların Bankanın kendisi gibi dışarıdan hizmet aldığı hukuk bürolarına yönlendirildiği ve Bankanın talimatlarıyla idari ve yasal takip sürecinin yürütüldüğü, Bankanın müşterilerine ait tüm kişisel verilerini yine Bankanın kendisi tarafından "Veri Sorumlusu" sıfatı ile işlediği, "Vekil" sıfatı ile takibini gerçekleştirdiği dosyalarda yer alan müşterilere ait tüm kişisel verilerin hukuk bürosuna yine Banka tarafından iletildiği,

- Vekilliği yürütülen Banka tarafından dosyaları hukuk bürosuna tevdi edilen müşterilere gerçekleştirilen ilk otomatik aramalarda hiçbir şekilde borçlu adı, borç miktarı yahut banka bilgisine yer verilmediği, otomatik aramalarda dinletilen metinlerin somut şikâyette olduğu gibi dosya ile ilgili olmayan bir kişiye ulaşılması ihtimalinde Kanunu ihlal edici bir fiilin meydana gelmemesi amacıyla tasarlandığı,

- Şikâyete konu iletişim numarasının Banka tarafından ilgili kişinin iletişim bilgisi olarak sisteme kaydedildiği, ilgili kişinin dosyasının hukuk bürosuna tevdi edilmesi ile birlikte tarafınca dosya içerisinde yer alan tüm iletişim numaralarından borçluya ulaşılmaya çalışıldığı, gerçekleştirilen ilk otomatik arama akabinde numaranın ilgili kişiye ait olmadığı anlaşıldığı ve Bankaya konu hakkında bilgi verilerek numaranın kayıtlardan çıkarıldığı, şahsı ve hukuk bürosunun mevcut olayda kişisel verilerin korunması hukuku çerçevesinde yasal mevzuatı ihlal edici nitelikte hiçbir icrai yahut ihmali fiilinin bulunmadığı, vekil sıfatı ile yürüttüğü işler kapsamında ilgili kişinin kız kardeşine ait olduğunu iddia ettiği numaranın sisteme kaydedilmiş olmasında hiçbir sorumluluğunun bulunmadığı, hukuk bürosunda Bankanın borçluları ile gerçekleştirilen ilk temasta hiçbir isim, borç yahut banka bilgisine yer verilmemesi ve tarafınca takibi gerçekleştirilen dosyalar açısından herhangi bir ihlale mahal vermemesi adına azami gayretin sarf edilmekte olduğu

ifade edilmiştir.

- Avukatın savunma, bilgi ve belge talebine vermiş olduğu cevabi yazısının Kuruma iletilmesini müteakip bahse konu başvuru hakkında Bankadan savunması talep edilmiş olup, Banka savunmasında özetle;

- Bankanın müşterisi olan ilgili kişinin ödenmemiş borçları sebebiyle 30.12.2016 ve 30.01.2017 tarihlerinde tasfiyeye alındığı, Bankanın alacaklarının tahsilatı için gerekli bilgilerin Banka alacaklarının tahsilatına ilişkin avukatlık hizmetlerinin gerçekleştirilmesine ilişkin olarak İcra Takibi Öncesi Tahsilat Hizmeti Sözleşmesi kapsamında Bankanın sözleşmeli hukuk bürosuna aktarıldığı,

- Yasal Takip Sisteminin Bankanın yasal takip sürecinde olan müşterilerinin bilgilerine sözleşmeli avukatların erişebildiği ve numara ekleme çıkarma yapabildikleri bir sistem olduğu, ilgili kişiye ait telefon numarasının bu sisteme 'Diğer Telefonu' olarak kaydedildiği, sözleşmeli avukatlar tarafından verilen hizmetlerde müşteri teyidinin yapılmadan müşteriye ait hiçbir bilginin verilmemesinin ana kuralları olduğu, Avukatın da beyan ettiği gibi teyit edilmeyen numaralar ile yapılan tüm iletişimde kişisel veriler ile ilgili her türlü tedbir alınarak hareket edilmesi gerektiği,
- Bu kapsamda Banka tarafından tasfiye dosyası aktarılan tüm hukuk bürolarına 02.09.2019 ve 21.11.2019 tarihlerinde borçluya, kefiller ve diğer tüm taraflara (rehin maliki, çeki senet cirantaları, keşidecileri, aval verenleri vb., aynı ve/veya şahsi olarak takip ve/veya davalara muhatap olan tüm ilgililer) ait kişisel verilerin 3. şahıslar ile paylaşılmaması, borçlu ve kefiller başta olmak üzere yukarıda yer verilen tüm taraflar ile iletişim kurulan tüm kanallarda kişisel verilerin gizliliğinin korunması yönünde gerekli tedbirlerin alınması hususlarında hassasiyet gösterilmesi konularında gerekli bilgilendirmelerin yapıldığı,
- İlgili kişinin Bankaya yapmış olduğu başvuru kapsamında Avukata ait hukuk bürosu ile irtibata geçilerek, ilgili kişinin hangi numaralardan arandığı, hangi telefonlara SMS gönderildiği hususlarında detaylı bilgi talep edilmesi sonrası, hukuk bürosundan ilgili kişinin daha önceden kendilerini arayarak kız kardeşinin cep telefonuna SMS ve arama gitmesinden dolayı şikayetini ilettiği, telefonu kardeşinin kullandığı ve kardeşi ile bilgilerinin paylaşıldığını iddia ettiği, söz konusu numaranın iletişim bilgilerinde yer aldığı ancak bu numara ile görüşme yapılmadığı, 3. şahsın sadece gönderilen SMS'lerden bilgi sahibi olmuş olabileceği iletirse de ilgili kişinin şikayetinin devam ettiği, numaranın Yasal Takip Sisteminden silindiği bilgisinin alındığı, söz konusu numaranın avukatlık bürosu tarafından Yasal Takip Sisteminden 22.11.2019 tarihinde kaldırıldığı

ifade edilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 09/02/2021 tarihli ve 2021/115 sayılı Kararı ile,

- Somut olayda, Avukatın Banka ile arasındaki vekâlet ilişkisine istinaden tarafınca Bankanın gecikmiş alacaklarının gerek yasal gerekse de idari takibini gerçekleştirdiği, vekalet ilişkisi çerçevesinde tarafınca ulaştırılması beklenen müşterilere ait tüm iletişim numaralarının müvekkili Banka tarafından "irtibat bilgisi" olarak iletildiği, dilekçesi ekinde yer alan belgelerden de incelemeye konu iletişim numarasının bizzat Banka tarafından işlerin takibinde kullanılan Yasal Takip Sistemine kaydedilmiş olduğunun anlaşıldığı, müşterilerin Bankayı sistemlerinde kayıtlı olan iletişim numarasından farklı bir numara ile aramaları durumunda, ilgili numaranın sistemlerine alternatif

numara olarak kaydedildiği, müşterilerin ödemelerinin gecikmesi durumunda, müşterilerine sistemde kayıtlı numaralarından ulaşılamadığında alternatif numaraların arandığının anlaşıldığı; bu çerçevede, Bankanın kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olduğu ve veri sorumlusu sıfatını haiz olduğu;

- İlgili kişinin kız kardeşine ait olan numarayı asla iletişim numarası olarak kullanmadığı şeklindeki iddiasına ilişkin olarak Bankanın müşterilerinin sistemlerinde kayıtlı olan iletişim numarasından farklı bir numara ile aramaları durumunda ilgili numaranın sistemlerine alternatif numara olarak kaydedildiği, müşterilerin ödemelerinin gecikmesi durumunda, müşterilerine sistemde kayıtlı numaralarından ulaşılamadığında, alternatif numaralar aranarak, hiçbir kişisel bilgi paylaşılmaksızın müşterilerinin Bankayı araması hususunda not bırakıldığı savunması ve Kanunun 3 üncü maddesinde unsurları belirtilen açık rızanın kişinin sahip olduğu verinin işlenmesine, kendi isteği ile hukuka uygun şekilde onay vermesi anlamını taşıdığı dikkate alındığında ilgili kişinin kız kardeşine ait olan telefon numarasının Bankanın sistemlerine kayıt edilmesi işleminin ilgili kişinin açık rızasına dayanılarak yapıldığı sonucuna varılamayacağı, diğer taraftan Kanunun 5 inci maddesinde yer alan diğer işleme şartlarından birine dayanılarak da yapılmadığı, bu kapsamda, ilgili kişinin kız kardeşine ait telefon numarasının Banka tarafından hukuka aykırı olarak işlendiğinin değerlendirildiği,

- Bankanın alacaklarının borçlu müşteriler aleyhinde icra takibine geçilmeden müşterilerle uzlaşarak tahsil edilebilmesi amacıyla icra takibi öncesinde tahsilat hizmeti aldığı ve kişisel verileri aralarında sözleşme imzaladıkları hukuk bürolarına aktardığını ifade ettiği; bu çerçevede, Bankanın müşterilerine ilişkin kişisel verileri hukuk bürolarına aktarmasının Kanunun 5 inci maddesinin (2) numaralı fıkrasının (c) bendinde yer alan “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” veya (e) bendinde yer alan “Bir hakkın tesisi, kullanılması veya korunması için veri işleminin zorunlu olması” çerçevesinde olduğu; dolayısıyla Bankanın alacaklarının borçlu müşterilerden tahsilini sağlamak üzere Avukata hukuka uygun şekilde erişim yetkisi verildiğinin değerlendirildiği; ancak Kanun hükümleri gereğince açık rıza aranmaksızın işlenecek kişisel verilerin borçluya ait olması gerektiği, bu kapsamda somut olayda Banka ile bağı olmayan ve bahse konu icra işlemine konu kişisel verisi bulunmayan ilgili kişinin kız kardeşinin cep telefonu numarasına erişim yetkisi verildiğinin anlaşıldığı, ancak Bankanın kendi bünyesinde oluşturduğu Yasal Takip Sisteminde yer alan ilgili kişinin kişisel verileri haricinde kız kardeşinin telefon numarasını Avukat ile paylaşmasının Kanun kapsamında gerçekleştirilebilecek bir kişisel veri işleme faaliyeti olmadığı ve hukuka aykırı

olduğunun değerlendirildiği, bu durumun Kanununun 12 nci maddesinin (1) numaralı fıkrasının (a) bendine aykırılık teşkil ettiği kanaatine varıldığı,

- Avukatın ise Avukatlık Kanunundan kaynaklanan yükümlülükleri ve yürütmekte olduğu icra işlemleri bakımından İcra İflas Kanunu ve ikincil mevzuat düzenlemelerinden kaynaklanan hukuki yükümlülüklerini yerine getirmek amacıyla Bankanın verdiği talimatlar çerçevesinde onun adına kişisel verileri işlediği ve somut olayda veri işleyen sıfatını haiz olduğu,

- Avukatın söz konusu Yasal Takip Sisteminde “diğer telefonu” olarak kayıtlı olan telefon numarasının ilgili kişinin kız kardeşinin telefon numarası olup olmadığını ilk anda bilecek durumda olmadığı, zira sistemde bu telefon numarasının ilgili kişi haricinde kime ait olduğunun belirtilmediği, ilgili kişinin kız kardeşine sırasıyla 01.07.2019, 18.09.2019, 19.09.2020 ve 13.11.2019 tarihinde SMS’ler gönderildiği, 21.11.2019 tarihinde otomatik aramanın gittiği ve ilk otomatik arama sonrasında numaranın ilgili kişiye ait olmadığını anlaşıldığı ve veri sorumlusuna konu hakkında bilgi verilerek numaranın kayıtlardan çıkarıldığı

değerlendirmelerinden hareketle;

- Banka tarafından ilgili kişinin kız kardeşinin cep telefonu numarasının Yasal Takip Sistemine kaydedilmesi işleminin ilgili kişinin açık rızasının alınması şartına dayanılarak yapılmadığı anlaşıldığından söz konusu kişisel verinin elde edilmesinin Kanununun 5 inci maddesine aykırı olduğu; diğer taraftan Bankanın söz konusu kişisel veriyi elde etmesinin akabinde kendi bünyesinde oluşturduğu Yasal Takip Sisteminde yer alan ilgili kişinin kişisel verileri haricinde kız kardeşinin telefon numarasını Avukat ile paylaşmasının hukuka aykırı olduğu değerlendirilmekte olup, bu durumun Kanununun 12 nci maddesinin (1) numaralı fıkrasının (a) bendine aykırılık teşkil ettiği kanaatine varıldığından Banka hakkında Kanununun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 175.000 TL idari para cezası uygulanmasına,

- Avukatın söz konusu Yasal Takip Sisteminde “diğer telefonu” olarak kayıtlı olan telefon numarasının ilgili kişinin kız kardeşinin telefon numarası olup olmadığını ilk anda bilecek durumda olmadığı, zira sistemde bu telefon numarasının ilgili kişi haricinde kime ait olduğunun belirtilmediği, ilgili kişinin kız kardeşine sırasıyla 01.07.2019, 18.09.2019, 19.09.2020 ve 13.11.2019 tarihinde SMS’ler gönderildiği, 21.11.2019 tarihinde otomatik aramanın gittiği ve ilk otomatik arama sonrasında numaranın ilgili kişiye ait olmadığını anlaşıldığı ve veri sorumlusuna konu hakkında bilgi verilerek numaranın kayıtlardan çıkarıldığı dikkate alındığında avukat hakkında yapılacak bir işlem olmadığına

karar verilmiştir.

2021/111 sayılı KVKK Kararı

İlgili kişinin telefon numarası bilgisinin farklı veri sorumluları tarafından hukuka aykırı olarak işlenmesine ilişkin Kişisel Verileri Koruma Kurulunun 09/02/2021 tarihli ve 2021/111 sayılı Karar Özeti

Karar Tarihi : 09.02.2021

Karar No : 2021/111

Konu Özeti : İlgili kişinin telefon numarası bilgisinin farklı veri sorumluları tarafından hukuka aykırı olarak işlenmesi

İlgili kişiden alınan şikâyet dilekçesinde özetle; cep telefonuna, kendisine ait herhangi bir içerik barındırmayan fakat yakınına ait bir borca ilişkin iki adet kısa mesaj (SMS) gönderildiği; konuya ilişkin olarak ilgili hukuk bürosuna ve alacak sahibi şirkete başvuruda bulunduğu ancak tarafına verilen yanıtların birbiri ile çelişkili ve yetersiz olduğu ifade edilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin olarak Kurul Kararı ile başlatılan inceleme çerçevesinde SMS'leri gönderen Hukuk Bürosu Avukatından ve alacak sahibi Şirketten savunması istenilmiştir.

Bu çerçevede alacak sahibi Şirketten alınan cevabi yazıda özetle;

- Şirket bünyesinde yapılan inceleme sonucunda, Şirketin müşteri bilgilerini derlediği, temel veri tabanı programında, ilgili kişiye ait GSM numarası ile yapılan sorgulamada şikâyetçi adına herhangi bir abonelik kaydının bulunmadığının görüldüğü, ilgili kişinin başvurusu haricinde geçmişte ilgili kişi ile herhangi bir temaslarının bulunmadığı, ilgili kişinin yakını olduğu anlaşılan aboneyle ise aralarında icra süreci devam eden bir borç ilişkisinin olduğu,
- İlgili kişiye ait GSM numarasının, programlarında ve Yasal Takip Sisteminde (YTS) kayıtlı olmayıp YTS sisteminin not kısmında yazıldığı, netice olarak ilgili kişiye ait irtibat bilgilerinin ilgili kişinin başvurusundan önce Şirketin sistemlerinde bulunmadığı,
- İlgili kişiye verilen yanıtta da belirttikleri üzere Şirket tarafından gerçekleştirilen olağan borç tahsilatında iki adımlı bir sürecin yürütüldüğü ve farklı hukuk ofislerinden bu kapsamda destek

alındığı, ilk adımda faturası üç ay üst üste ödenmemiş olan üyeliklerin sahiplerine borç hatırlatması yapılması ve borç tahsilat sürecinde onlara yol gösterilmesi amacıyla dış kaynak hizmet sağlayıcı hukuk ofislerinden (İdari Hukuk Büroları) destek alındığı,

- Dış kaynak hizmet sağlayan hukuk ofislerinin, kendilerine “bir hakkın tesisi, kullanılması veya korunması için veri işleminin zorunlu olması” kanuni veri işleme şartına dayalı olarak aktarılan ad, soyadı, birikmiş borç miktarı ve iletişim bilgilerine istinaden Şirkete borcu bulunan kişiler ile temas kurduğu ve borç hatırlatmaları yaptığı, ilgili hatırlatmalar sonucunda da borçların ödenmemesi durumunda ikinci adıma geçildiği, bu çerçevede söz konusu üyeliklere ilişkin borçların tahsil edilmesi amacıyla icra takiplerinin başlatılması ve bu süreçlerin takibi amacıyla yine dış kaynak hizmet sağlayıcı hukuk ofislerinin (İcra Hukuk Büroları) devreye girdiği ve icra takibi başlatılacağı hakkında borçlu üyelere bildirimler yapıldığı,

- İlgili kişiye ait olduğu tespit edilen GSM numarasının Şirkete ait programda kayıtlı olmadığı ve söz konusu irtibat bilgisinin kısa mesaj gönderimi yapan ilgili Hukuk Bürosuna Şirket tarafından sağlanmadığı,

- Nitekim Hukuk Bürosu tarafından ulaşılan ilgili kişinin irtibat bilgisinin ne şekilde elde edildiğine ilişkin incelemenin başvuru üzerine gerçekleştirildiği, bu incelemeler sonucunda ilgili kişiye ait olduğu beyan edilen GSM numarasının dosya idari takip sürecindeyken Şirketin dış hizmet sağlayıcısı olan diğer bir Hukuk Bürosu tarafından YTS sistemine bu Hukuk Bürosunun iş akdi feshedilmiş personeli tarafından alınan not ile girildiğinin görüldüğü,

- Söz konusu büroların Şirketin dış kaynak hizmet sağlayıcıları olarak hizmet vermelerine rağmen, borç hatırlatma ve borçların icra takibi hizmetleri kapsamındaki veri işlemlerine ilişkin Şirketten doğrudan talimat almadığı, bu hizmetler kapsamında gerçekleştirdikleri veri işleme faaliyetleri açısından Şirketin veri işleyeni konumunda değil bağımsız birer veri sorumlusu durumunda oldukları,

- Öte yandan Şirketin dış kaynak hizmet sağlayıcılarının müşteriler ile olan etkileşimlerinde Kanun başta olmak üzere tüm kişisel verilerin korunması mevzuatına uygun davranmalarına ilişkin her türlü hatırlatmanın düzenli olarak yapıldığı ve gerekli her türlü teknik ve idari tedbirin alındığı, bu kapsamda hukuk bürolarından aylık olarak talep edilen konuşma kayıtlarının Şirket tarafından incelendiği, abone dışındaki bir yakınına borç bilgilendirmesi yapılması durumunda uyarı ve bilgilendirme yapıldığı

ifade edilmiştir.

İlgili kişiye kısa mesaj gönderim işlemini yapan ilgili Hukuk Bürosu Avukatından alınan cevabi yazıda ise özetle;

- Kendisinin ilgili Şirketin bireysel üyelerinin faturalarından kaynaklanan ve bu üyeler tarafından ödenmemiş alacaklarının tahsili konusunda Şirketin icra takiplerini başlatmak suretiyle avukatlığını yaptığı,
- Şirketin bireysel üyelerinin ödenememiş faturalarından kaynaklanan alacaklarını, sözleşmeli avukatlar aracılığıyla takip edebilmek amacıyla; dosyaları Yasal Takip Sistemine yükleyerek bu sistem üzerinden Avukatlık Bürolarına gönderdiği,
- Şirketin alacaklarını tahsil etmek üzere özetle iki aşamalı bir süreci sözleşmeli avukatları aracılığı ile uyguladığı, bu süreçlerin 'idari takip aşaması' ve 'icra takip aşaması' olduğu, idari takip aşamasına geçilmeden önce üyelere ait bilgilerin müvekkil Şirket bilgi sisteminden YTS'ye aktarıldığı, idari takip aşamasında alacakların iki ay içinde telefon, mektup ya da SMS ile tahsil edilmesinin amaçlandığı, iki ay içerisinde dosya tahsilatla kapatılamamışsa, dosyanın o avukattan alınarak müvekkil Şirket merkezine çekilerek ilgili avukatlara icra takibi başlatmaları için gönderildiği, icra takibini yapan avukatın daha evvel o dosyayı idari takip aşamasında takip eden avukat olabileceği gibi icra takibi aşamasında başka bir avukatın da belirlenebileceği, sürecin tüm dosyalarda YTS üzerinden yürütüldüğü,
- Şikayete konu dosyanın Şirket tarafından Bürolarına ilk kez 13/11/2018 tarihinde atandığı, dolayısıyla büro tarafından bu dosyanın varlığından 13/11/2018 tarihinde önce haberdar olma, dosyada herhangi bir işlem yapma, veri girme, bir not ya da telefon işlenmesinin teknik ve fiziki olarak imkansız olduğu,
- Dosyanın taraflarına icra takibi başlatılması için gönderilmeden önce idari takip süreci için diğer bir Avukatlık Bürosuna gönderildiği, şikayete neden olan GSM numarasının bu Avukatlık Bürosu çalışanı tarafından 16/07/2018 tarihinde YTS'ye işlendiği, yani bu verinin dosyanın bürolarına gelmesinden yaklaşık 4 ay önce işlendiği, bu hususun YTS'de kayıt altına alındığı,
- Bilahare şikayetçi şahsın bu numaranın kendisine ait olduğunu Bürolarına bildirdiği 25/07/2019 tarihinde borçlu ile ilgisi olmadığı nazara alınarak büro çalışanı tarafından silindiği, bu itibarla bürolarına daha gelmeden dosyaya işlenmiş olan bir veriden dolayı büronun sorumlu tutulmasının mümkün olmadığı,
- Bu numaraya SMS gönderilme sebebinin dosyada numaranın işlenmiş olarak bürolarına gönderilmesi olduğu, numaranın YTS'ye neden işlendiğini bilmelerinin mümkün olmadığı, borçlu

olan abone tarafından irtibat numarası olarak verilmiş veya sonradan şikâyetçiye devrolunmuş bir numara da olabileceği,

- Bürolarına bir borçluya ait dosyada “Diğer GSM Nosu” olarak şikâyetçinin numarasının işlenmiş vaziyette gelmesinden sonra bu GSM numarasına dosyanın ilk geldiği tarihlerde borçlunun ismi belirtilerek ve borçluya gönderildiği düşüncesi ile iki tane SMS iletildiği, telefonla bir görüşme yapılmadığı, yaklaşık bir yıl sonra GSM numarasının kendisine ait olduğunu söyleyen şahsın şikâyet dilekçesinin tarafına geldiği gün bu yanlış kaydın taraflarınca silindiği, bu verinin yurtiçinde ve/veya yurtdışında hiç kimse ile paylaşılmadığı

ifade edilmiştir.

İlgili kişinin başvurusu ile ilgili olarak şikâyetine konu olan ilgili Şirket ve Hukuk Bürosu Avukatından alınan cevap yazıları ve ilgili dokümanların incelenmesi neticesinde; ilgili kişiye ait GSM numarasının, dosya ‘idari takip süreci’ndeiyken diğer bir Hukuk Bürosu çalışanı tarafından temin edildiği ve Yasal Takip Sistemine büro çalışanı personel tarafından kaydedildiği bilgisinin edinilmesi üzerine söz konusu kaydı gerçekleştiren Hukuk Bürosundan ayrıca savunma, bilgi ve belge talep edilmiştir. İlgili Hukuk Bürosu Avukatından alınan cevabi yazıda ise özetle;

- İlgili kişiye ilişkin dosyanın şu an ofisin sisteminde kayıtlı olmadığı, bahsi geçen dosyanın Şirket tarafından YTS kullanılarak atandığı, bu dosyaların ofisinde yer alan personellerce sistemde yer alan telefon numaraları kullanılarak arandığı ve fatura borçlarının ödenmesinin sağlandığı,

- Şikâyete konu olan dosyanın da bu şekilde taraflarına 2018 yılında atanmış bir dosya olduğu, Hukuk Bürolarında kaldığı süre boyunca borçluya sistemde yer alan telefonlarla ulaşılmaya çalışıldığı, dosyanın şu an kendisinin uhdesinde olmadığı için ne gibi işlemler yapıldığını görmesinin mümkün olmadığı,

- Müvekkil Şirket tarafından, ilgili kişiye ait telefon numarasının ofislerince sisteme kayıt edildiği bilgisinin tarafına iletildiği, Şirketin verdiği bilgiye göre eski bir personelin sisteme şikâyete konu olan numarayı işlediğini öğrenmiş bulunduğu, bu tespit sonucu eski çalışanı ile irtibata geçtiği,

- Eski çalışanın; 2018 yılının Haziran, Temmuz aylarında gerçekleşen olayda kişiyi hatırlamadığını, kişinin telefonu sistemde kayıtlı ise veya tarafınca kayıt edildiyse 118 sorgu gibi kamuya açık portallardan ya da borçlu şahıs veya yakınlarının paylaşması sonucu bu bilgiye ulaşmış olabileceğini, şikâyetçinin telefon numarasının müvekkil Şirketin borçlusu tarafından bürolarınca paylaşılabilceğini ve bu şekilde işlenebileceğini söylediği,

- Çalışanı tarafından şikâyetçiye ait telefon numarasının irtibat numarası olarak kayıt edilmediği, şahsın telefon numarasının kimse ile paylaşılmadığı, sadece kurumun yaptığı işlemi bilmesi adına not alındığı,

- Söz konusu GSM numarasının tarafınca işlenmediği, ofisinde çalışan personelin Şirkete ait sisteme giriş yaptığı ve borçlular ile yaptıkları görüşmelere istinaden bir takım notlar alabildiği, bu numaranın da eski çalışanın beyanına göre 118 sorgu siteleri gibi kamuya açık portallardan edinilmiş ya da borçlu şahsın kendisi tarafından personele verilmiş olabileceği, bu numaranın sadece müvekkil firmayı dosyada yapılan işlem açısından bilgilendirme amaçlı olarak görüşme yapıldığına ilişkin not düşüldüğü

ifade edilmiştir.

Bu çerçevede, konuya ilişkin olarak yapılan incelemede, Kişisel Verileri Koruma Kurulunun 09/02/2021 tarihli ve 2021/111 sayılı Kararı ile,

- Kanunun “Tanımlar” başlıklı 3 üncü maddesinde “veri sorumlusu” nun kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlandığı, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberinde de belirtildiği üzere veri sorumlusunun işleme faaliyetinin neden ve nasıl yapılacağı sorularına cevap veren kişi olduğu, bu doğrultuda, somut bir olayda veri sorumlusu belirlenirken kişisel verilerin toplanması ve toplama yöntemi, toplanacak kişisel veri türleri, toplanan verilerin hangi amaçlarla kullanılacağı, hangi bireylerin kişisel verilerinin toplanacağı, toplanan verilerin paylaşılıp paylaşılmayacağı, paylaşılacaksa kiminle paylaşılacağı ve verilerin ne kadar süreyle saklanacağına kimin karar verdiği hususlarının dikkate alındığı,

- Karara konu somut olayda, alacaklı Şirketin abonelerine ait borçların tahsilatına ilişkin olarak iki aşamalı bir süreci sözleşmeli avukatlar aracılığı ile uyguladığı, bu süreçlerin ‘idari takip aşaması’ ve ‘icra takip aşaması’ olarak adlandırıldığı, idari takip aşamasına geçilmeden önce üyelere ait bilgilerin Şirket tarafından Yasal Takip Sistemi adı verilen sisteme aktarıldığı ve alacağın tahsilini sağlamak üzere yapılan işlemlerin bu sistem aracılığıyla gerçekleştirildiği,

- Söz konusu olayda ilk Hukuk Bürosu avukatının ‘idari takip süreci’nde yer aldığı ve bu süre zarfında da ilgili kişiye ait iletişim bilgisinin Hukuk Bürosu çalışanı tarafından temin edilerek YTS isimli sisteme işlendiğinin gerek şirket gerek SMS gönderimi işlemi yapan ikinci Hukuk Bürosu Avukatı tarafından beyan edildiği, bununla birlikte Kuruma sunulan evraklarda da ilk Hukuk Bürosu çalışanı tarafından ilgili kişiye ait iletişim bilgisinin işlendiğinin tevsik edildiği,

- Bu kapsamda somut olayda ilgili kişiye ait telefon numarası Şirket tarafından alacağın tahsilini sağlamak üzere ilk Hukuk Bürosuna aktarılmadığı halde söz konusu Hukuk Bürosu çalışanı tarafından numaranın borçlu kişinin yakınına ait olduğunu belirli kılacak şekilde ‘not’ olarak kaydedildiği, dolayısıyla borçlu kişinin yakını olması nedeniyle ilgili kişiye ait telefon numarasının YTS sistemine işlendiğinin anlaşıldığı,
- Bu anlamda veri sorumlusu belirlenirken kişisel verilerin toplanması ve toplama yöntemi, hangi bireylerin kişisel verilerinin toplanacağı gibi hususları belirleyen konumunda olup olmadığı dikkate alındığında ilk Hukuk Bürosu çalışanının ilgili sistemde borçlu kişiye ait olmayan ve YTS sisteminde bulunmayan numarayı bir şekilde temin ederek işlediği anlaşıldığından ilk Hukuk Bürosu Avukatının olay özelinde veri sorumlusu olduğu,
- Diğer taraftan ikinci Hukuk Bürosu Avukatından alınan cevap yazısı ve ekinde yer alan belgeler incelendiğinde; “... ilk avukatlık bürosunun YTS’ye girmiş olduğu verilerle birlikte ...” sonraki aşamanın gerçekleştirilmesi için ikinci Hukuk Bürosuna gönderildiği, numaranın YTS sisteminde kişinin yakınına ait olduğu notu ile işlendiği ve bu bilginin de ikinci Hukuk Bürosu Avukatı ile paylaşıldığı anlaşıldığından, bahse konu telefon numarasının borçlu kişiye ait olmadığı bilgisinin mevcut ve açıkça belirli olduğu halde kullanılarak SMS gönderildiği hususu dikkate alındığında SMS gönderimi işlemini yapan ikinci Hukuk Bürosu Avukatının da YTS isimli kayıt sistemi çerçevesinde kişisel veri işleme faaliyetinde bulunduğu dolayısıyla veri sorumlusu olduğu,
- Bu çerçevede kişisel verilerin işleme amaç ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yürütülmesinden sorumlu olan Şirketin ve Şirket tarafından yürütüldüğü anlaşılan YTS isimli kayıt sistemine kendilerine tevdi edilen dosyalara ek veri girişinde bulunmak suretiyle kendi amaçları doğrultusunda etki yapan ve işleme faaliyetinin amaç ve araçlarının belirlenmesi sürecine katılan ilk Hukuk Bürosu Avukatının ve ilgili verileri amaçları doğrultusunda kullanmak suretiyle işleyen ikinci Hukuk Bürosu Avukatının sürecin belli aşamalarında veri işleme faaliyetine katıldığının anlaşıldığı, bu çerçevede Şirket ile birlikte ilgili hukuk büroları avukatlarının da veri sorumlusu olduğu sonucuna varıldığı,
- Diğer taraftan 6698 sayılı Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinde kişisel verilerin, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği ile kişisel verilerin işlenmesinde hukuka ve dürüstlük kurallarına uygun olma, **doğru ve gerektiğinde güncel olma**, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uyulmasının zorunlu olduğunun düzenlendiği, kişisel veri işleme faaliyeti

gerçekleştirilirken, veri işleme şartı sağlansa dahi kişisel verilerin işlenmesine ilişkin genel ilkelerin tüm kişisel veri işleme faaliyetlerinin özünde bulunması ve bu ilkelere uygun olarak kişisel veri işleme faaliyetlerinin gerçekleştirilmesinin gerektiği, söz konusu şikâyete konu olayda veri sorumlusu Şirket tarafından borç takibi yapılabilmesi amacıyla kullanılan sisteme ilk Avukat tarafından girilen verilerin doğruluğu ve güncelliği noktasında gerekli denetim ve kontroller yapılmaksızın dosyanın ikinci bir avukat ile paylaşıldığı anlaşıldığından söz konusu davranışın genel ilkelerden biri olan doğru ve gerektiğinde güncel olma ilkesine aykırılık teşkil ettiği,

- Öte yandan, Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin birinci fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, ikinci fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- İlgili kişinin kişisel verilerinin açık rızası olmaksızın işlendiği iddiası ile ilgili olarak ilk Hukuk Bürosu Avukatından alınan cevap yazısında; ilgili kişinin telefon numarasının nasıl temin edildiği konusunda 118 sorgu gibi kamuya açık portallardan edinilmesi ya da borçlu şahıs veya yakınlarının paylaşması sonucu bu bilgiye ulaşılmış olunabileceği açıklamalarına yer verildiği, dolayısıyla ileri sürülen olasılıkların açık rıza dışındaki işleme şartlarına ilişkin bir hukuki dayanak oluşturmadığı, aynı zamanda hukuki anlamda somut zemine oturan açıklamalar olmadığı anlaşıldığı, bu kapsamda Kanunun 5 inci maddesinin ikinci fıkrasında yer alan açık rıza dışındaki kişisel veri işleme şartlarından herhangi biri geçerli olmadığı halde kişisel veri niteliğinde olan ilgili kişiye ait iletişim bilgisinin, yakınının borcu olması dolayısıyla Avukat tarafından işlendiği sonucuna varıldığı,

- Diğer taraftan Hukuk Bürolarının ortak kullanımında olan YTS sisteminde ilgili kişiye ait telefon numarasının kişinin yakınına ait olduğu bilgisinin mevcut olmasına rağmen ikinci Hukuk Bürosu Avukatı tarafından ilgili kişiye SMS göndermek suretiyle Kanunun 5 inci maddesinde yer alan kişisel veri işleme şartlarından herhangi biri söz konusu olmadığı halde ayrıca işlendiği bu itibarla, avukat

tarafından kişisel verilerin hukuka aykırı işlenmesini önlemek adına gerekli dikkat ve özen yükümlülüğünün yerine getirilmeyerek hukuka aykırı kişisel veri işleme faaliyetinde bulunulduğu, değerlendirmelerinden hareketle;

- İlgili kişinin telefon numarasının ilk Hukuk Bürosu çalışanı tarafından temin edilmesi ve işlenmesine ilişkin olarak, veri sorumlusu Avukat tarafından ileri sürülen hususların Kanunun 5 inci maddesinin ikinci fıkrasında yer alan açık rıza dışındaki kişisel veri işleme şartlarından herhangi birine dayanak teşkil etmediği dolayısıyla veri sorumlusu Avukatın Kanunun “Veri Güvenliğine İlişkin Yükümlülükler” başlıklı 12 nci maddesinin birinci fıkrasının (a) bendinde öngörülen yükümlülüğü yerine getirmediği kanaatine varıldığından, veri sorumlusu Avukat hakkında, Kanunun 18 inci maddesinin birinci fıkrasının (b) bendi uyarınca 50.000 TL idari para cezası uygulanmasına,

- Şirket tarafından borç takibi yapılabilmesi amacıyla kullanılan sisteme ilk Avukat tarafından girilen verilerin Kanunun 4 üncü maddesi gereğince doğruluğu ve güncelliğini sağlama noktasında gerekli denetim ve kontroller yapılmaksızın ikinci Avukat ile paylaşılması sebebiyle veri sorumlusu Şirketin gerekli teknik ve idari tedbirleri almadığı dolayısıyla Kanunun “Veri Güvenliğine İlişkin Yükümlülükler” başlıklı 12 nci maddesinin birinci fıkrasında yer alan yükümlülüğünü yerine getirmediği kanaatine varıldığından, veri sorumlusu Şirket hakkında Kanunun 18 inci maddesinin birinci fıkrasının (b) bendi uyarınca 115.000 TL idari para cezası uygulanmasına,

- YTS sisteminde bulunan telefon numarasının, kişinin yakınına ait olduğu bilgisi mevcut olmasına rağmen veri sorumlusu Avukat tarafından ilgili kişiye SMS göndermek suretiyle Kanunun 5 inci maddesinde yer alan kişisel veri işleme şartlarından herhangi biri söz konusu olmadığı halde işlendiği bu itibarla, veri sorumlusu avukat tarafından Kanunun “Veri Güvenliğine İlişkin Yükümlülükler” başlıklı 12 nci maddesinin birinci fıkrasının (a) bendinde öngörülen yükümlülüğün yerine getirilmediği kanaatine varıldığından, veri sorumlusu Avukat hakkında, Kanunun 18 inci maddesinin birinci fıkrasının (b) bendi uyarınca, 50.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2021/85 sayılı KVKK Kararı

İlgili kişinin Kanunun 11 nci maddesi kapsamındaki başvurusuna veri sorumlusu tarafından verilen cevabın yeterli bulunmaması hakkında Kişisel Verileri Koruma Kurulunun 03/02/2021 tarihli ve 2021/85 sayılı Karar Özeti

Karar Tarihi : 03.02.2021

Karar No : 2021/85

Konu Özeti : İlgili kişinin Kanunun 11 nci maddesi kapsamındaki başvurusuna veri sorumlusu tarafından verilen cevabın yeterli bulunmaması

Kuruma intikal eden şikâyette; ilgili kişinin "...com.tr" adresinden ürün siparişi verdiği, bu işlem ve veri sorumlusunun e-bültenine kayıt olması esnasında kişisel verilerinin işlenmesine ilişkin bir aydınlatmanın sunulmadığı, 26.06.2019 tarihinde veri sorumlusuna; hangi kişisel verilerinin hangi amaçlarla işlendiği, hangi verilerinin ne kadar süre ile saklandığı ve bu kişisel verilerin üçüncü taraflarla paylaşılıp paylaşılmadığı hususlarının yanıtlanması için başvuruda bulunduğu, veri sorumlusunun bu hususlardaki yanıtlarını içeren cevabî yazısının, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 13 üncü maddesi uyarınca 30 günlük süre içerisinde 23.07.2019 tarihinde ilgili kişiye iletildiği ancak ilgili kişinin veri sorumlusunun cevabını yeterli bulmadığı zira;

- Veri sorumlusunun internet sitesinde bulunan "Kişisel Veriler Politikası" (Politika) bölümünün bir aydınlatma olmadığı, tüm siteyi kapsamaya çalışan karışık bir metin olduğundan ötürü "belirli ve açık" olmadığı,
- İlgili kişi veri sorumlusuna başvurduğunda kendisine verilen cevap ile veri sorumlusuna ait internet adresinde yer alan Politikanın kimi yerlerde çeliştiği; Politikada IP, Çerez gibi verilerin sayıldığı ancak ilgili kişiye verilen cevapta bu konularda bir bilgilendirmenin yapılmadığı,
- İlgili kişiye verilen cevap metni içerisinde kişisel verilerin, "idarî ve resmî makamlar ile taşıma şirketlerine sınırlı ve orantılı bir şekilde aktarıldığı"nın ifade edildiği fakat Politika metni içerisinde kişisel verilerin "yurt içi/yurt dışı kuruluşlar ile diğer üçüncü kişilere" aktarıldığının söylendiği,

- Politika metni içerisinde birçok veri ve veri aktarımından söz edildiği ancak veri bazında bir bilgilendirmenin yapılmadığı, örneğin kimlik bilgilerinin ya da adreslerin hangi şirketlere aktarıldığı hususunda bir açıklama yer almadığı

ifade edilerek veri sorumlusu hakkında gerekli işlemlerin tesis edilmesi talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusu şirketin savunması talep edilmiş olup veri sorumlusunun cevabi yazısında özetle;

- İlgili kişinin internet siteleri üzerinden üyelik kaydı oluşturarak ürün sipariş ettiği, Kanunun yürürlüğe girmesiyle birlikte veri sorumlusunun Kanun kapsamında bir kişisel verileri koruma politikası uygulamaya başladığı, ilgili kişinin başvuru tarihinden itibaren geçen süre içerisinde politika metninde iyileştirmeler yapıldığı ve “Kişisel Verilerin Korunması ve İşlenmesi Hakkında Aydınlatma Metni”nin veri sorumlusunun sitesinde yer aldığı, ilgili kişinin başvurusunda belirli ve açık olmadığını ileri sürdüğü metnin yeniden düzenlenerek daha açık bir anlama kavuşturulduğu,

- IP, Çerez gibi verilere ilişkin açıklamaların halihazırda Aydınlatma Metninde yer aldığı, veri sorumlusunun internet sitesinde ayrıca Çerez Politikasına da yer verildiği, metinde yer alan bilgilendirme ve açıklamaların Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin (Tebliğ) 4 üncü maddesine uygun kapsamda olduğu, 24.06.2019 tarihli Mesafeli Satış Sözleşmesi gereği ilgili kişinin siparişinin ulaştırılması için zorunlu olarak işlenen ve kargo firmasına aktarılan verileri dışında herhangi bir veri paylaşımının gerçekleştirilmediği

ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 03/02/2021 tarih ve 2021/85 sayılı Kararı ile;

- Kanunun “Veri sorumlusunun aydınlatma yükümlülüğü” başlığını haiz 10 uncu maddesinin (1) numaralı fıkrasının; “Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; a) Veri sorumlusunun ve varsa temsilcisinin kimliği, b) Kişisel verilerin hangi amaçla işleneceği, c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabilceği, ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi, d) 11 inci maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür.” hükümlerini amir olduğu,

- Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin 4 üncü maddesinde, Kanunun 10 uncu maddesine göre; kişisel verilerin elde edilmesi sırasında veri sorumluları veya yetkilendirdiği kişilerce ilgili kişilerin bilgilendirilmesinin gerektiği, 5 inci maddesinin (1) numaralı fıkrasının (f) bendinde kişisel veri işleme faaliyetinin açık rıza şartına dayalı

olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerektiği, (g) bendinde aydınlatma yükümlülüğü yerine getirilirken genel nitelikte ve muğlak ifadelerle yer verilmemesi gerektiği, (ğ) bendinde açık, anlaşılır ve sade bir dil kullanılması gerektiği, (h) bendinde “hukuki sebep”ten kastın, Kanunun 5 ve 6 ncı maddelerinde belirtilen işleme şartlarından hangisine dayanarak veri işlendiğinin olduğu, bu sebeple aydınlatma yükümlülüğünün yerine getirilmesi esnasında hukuki sebebin açıkça ifade edilmesinin gerektiği, (ı) bendinde aydınlatma yükümlülüğü kapsamında, kişisel verilerin aktarılma amacı ve aktarılacak alıcı gruplarının belirtilmesi gerektiği ve (j) bendinde aydınlatma yükümlülüğü yerine getirilirken eksik, ilgili kişileri yanıltıcı ve yanlış bilgilere yer verilmemesinin lüzumlu olduğu hükümlerinin bulunduğu,

- Kanunun veri sorumlusuna yüklediği “Aydınlatma Yükümlülüğü”nün amacının, ilgili kişilerin, kişisel verilerini belirli işlemler için veri sorumlularına vermeden önce; kişisel verilerinin kullanımı, aktarımı, bu işlemlerin hukukî mesnetleri ve başvuru mercii olan veri sorumlusunun kimliği ile kendilerinin kişisel verileri üzerinde var olan haklarıyla alakalı olarak bilgilendirilerek, kişisel verileri üzerindeki hakimiyetlerini tamamen yitirmelerini önlemek olduğu, aydınlatma yükümlülüğünün varlığı, şeffaflık ilkesinin bir gereği olup şeffaflığın şartının da ilgili kişinin anlaşılabilir bir şekilde bilgilendirilmesi olduğu,

- Bu doğrultuda hazırlanan bir Aydınlatma Metninin, ilgili kişilere, yaptıkları işlem bazında, söz konusu işlem dahilinde kullanılan kişisel verilerine ilişkin bilgilendirme sağlamanın beklendiği, veri sorumluları için genel hukukî metinler niteliğinde olan “Gizlilik Politikası”, “Veri İşleme Politikası” gibi metinlerin, karışık yapıları ve ilgili kişilerin ihtiyacı olan belirlilikteki bilgilendirmeleri sağlayamamaları nedenleriyle Aydınlatma Metni olarak kullanılmamaları gerektiği,

- Zira 26.06.2020 tarihinde Kurumun internet sitesinden yayınlanan “Aydınlatma Yükümlülüğünün Yerine Getirilmesi Hakkında Kamuoyu Duyurusu”nun (h) maddesinde de bu durumun, “İşleme faaliyeti ile sınırlı olmayan, veri sorumlusu için genel veri işleme belgesi niteliğinde olan gizlilik politikaları veya veri işleme politikaları, aydınlatma metinleri olarak kullanılmamalıdır.” şeklinde açıklandığı,

- Nitekim Kişisel Verileri Koruma Kurumu tarafından yayınlanan “Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi”nde de “Kanun’un 4’üncü maddesinde yer alan temel ilkeler gereği veri sorumlularının, faaliyetleri kapsamında işlediği kişisel verileri, hangi işleme amacına dayanarak işlediğini kişisel veri bazında belirlemesi ve bu amacın da aydınlatma metinlerinde açıkça belirtilmesi

gerekmektedir.” denilerek, aydınlatma yükümlülüğünün işlenecek kişisel veri bazında yerine getirilmesi gerektiğinin ifade edildiği,

- Veri sorumlusunun güncel Aydınlatma Metni incelendiğinde Kanunda ifade olunan asgari unsurlara (veri sorumlusunun kimliği, kişisel verilerin işlenme amaçları, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabilceği, kişisel veri toplamanın yöntemi ve hukuki sebebi ve 11 inci maddede sayılan diğer haklar) yer verildiğinin görüldüğü, ayrıca veri sorumlusunun işlediği kişisel verilerin de kategorik olarak Aydınlatma Metninde sunulduğu,

- Veri sorumlusunun internet sitesinden (...com.tr) sipariş verilmek istendiğinde iki seçenek olduğu; bunlardan birincisinin internet sitesine üye olarak siparişi gerçekleştirmek, diğerinin ise üye olmadan devam ederek siparişi tamamlamak olduğu; söz konusu internet sitesinde bulunan “Üye Ol” sayfasına tıkladığında “Kişisel Verilerin Korunması hakkındaki açık rıza metnini okudum, onaylıyorum” butonu aktif edilmeden siteye üye olunamadığı, bir Aydınlatma Metni hüviyetini taşımayan bu metnin de kendi içerisinde Gizlilik Politikası metnine bir bağlantı içermediği, üye olunmadan devam edildiği takdirde ise aydınlatmaya dair herhangi bir buton veya pop-up yardımıyla aydınlatmada bulunulmadığı,

- Açık Rıza Metinlerinin, ilgili kişilere, işlenecek kişisel verileri hakkında sade ve özet bilgiler sunan metinler olduğu; bununla birlikte detaylı bilgilendirme için veri sorumlularının ilgili kişileri Aydınlatma Metnine yönlendirdikleri, bu durumun aydınlatmanın kişisel verilerin işlenmesinden önce yapılması adına önemli bir gereklilik olduğu fakat veri sorumlusunun bu gerekliliği yerine getirmediğinin anlaşıldığı,

- Tebliğin “Usul ve esaslar” başlığını haiz 5 inci maddesinin (1) numaralı fıkrasının (e) bendine göre aydınlatma yükümlülüğünün yerine getirildiğinin ispatı veri sorumlusuna ait olduğundan, veri sorumlusunun internet sitesinin en alt bölümünde bir link olarak yer verdiği politika metninin internet sitesinden alışveriş yapan ilgili kişilerin aydınlatıldığını ispatta yetersiz kaldığı zira söz konusu Aydınlatma Metninin, ilgili kişilerin sipariş vermesi ve üye olması sırasında ekrana gelmediğinden ilgili kişilerin bahse konu metni okuyup okumadığının belirsiz olduğu, bu noktada, internet sitesinden sipariş verilmesi veya internet sitesine üye olunması gibi, ilgili kişilerin kişisel verilerinin işlenmesine sebebiyet verecek işlemler esnasında ilgili kişilere, gerçekleştirdikleri işlemler özelinde; işlenecek kişisel veri kategorileri, bu verilerin işlenme amacı, hangi veri kategorilerinin hangi alıcı gruplarına ne maksatla aktarıldığı, sipariş kapsamında gerçekleştirilen veri işleme faaliyetlerinin hukukî sebeplerinin belirtildiği bir metin vasıtasıyla, işlenecek kişisel veriler bazında

aydınlatma yapılarak sonrasında ilgili kişilere, veri sorumlusunun genel veri işleme politikasını yansıtan metnine, örneğin bir link eklenmesi vasıtasıyla yönlendirme yapılabileceği,

- Bu anlamda, veri sorumlusunun ilgili kişilere, kişisel verilerinin en geç elde edilmesi esnasında, bahse konu işlemler bazında, “belirli ve açık” bir aydınlatmada bulunmadığı ve Aydınlatma Metninde eksiklikler bulunduğu; bu sebeplerle de Tebliğin 5 inci maddesinin (1) numaralı fıkrasının; “Aydınlatma yükümlülüğü kapsamında açıklanacak kişisel veri işleme amacının belirli, açık ve meşru olması gerekir. Aydınlatma yükümlülüğü yerine getirilirken, genel nitelikte ve muğlak ifadelerle yer verilmemelidir. Gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandıran ifadeler kullanılmamalıdır.” şeklindeki (g), “Aydınlatma yükümlülüğü kapsamında ilgili kişiye yapılacak bildirim anlaşılır, açık ve sade bir dil kullanılarak gerçekleştirilmesi gerekmektedir.” hükmünü amir (ğ) ve “Aydınlatma yükümlülüğü yerine getirilirken eksik, ilgili kişileri yanıltıcı ve yanlış bilgilere yer verilmemelidir.” hükmünü ihtiva eden (j) bentlerine aykırı hareket ettiği

değerlendirmelerinden hareketle,

- Veri sorumlusunun, internet sitesi üzerinden sipariş verilmesi veya üye olunması gibi ilgili kişilerin kişisel verilerinin işlenmesine sebebiyet verecek işlemler esnasında, o anda ve sonrasında gerçekleştirilecek veri işleme faaliyetine ilişkin bir aydınlatmada bulunmadığı, ilgili kişilerin kişisel verilerinin kullanımı ile ilgili olarak bilgi alabilmek için kendilerinin bahse konu politika metnini arayıp bulmaları gerektiği, bu metnin de tüm siteyi kapsayan bir politika metni hüviyetinde olduğu ve bu durumun Tebliğin 5 inci maddesinin (1) numaralı fıkrasının (g), (ğ) ve (j) bentlerine aykırılık teşkil ettiği kanaatine varılmış olup Kanunun “Şikayet üzerine veya resen incelemenin usul ve esasları”nı düzenleyen 15 inci maddesinin (5) numaralı fıkrasının “Şikayet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması halinde Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ eder. Bu karar, tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilir.” hükmü uyarınca veri sorumlusunun, söz konusu hukuka aykırılıkların giderilmesi ve sonucundan Kurula bilgi vermesi hususlarında talimatlandırılmasına

karar verilmiştir.

2021/84 sayılı KVKK Kararı

Veri sorumlusu sabit telefon hizmeti sađlayan iřletmeci tarafından bir hastanenin mřsterilerinin kiřisel verilerinin hukuka aykırı olarak iřlenmesi hakkında Kiřisel Verileri Koruma Kurulunun 03/02/2021 tarihli ve 2021/84 sayılı Karar Özeti

Karar Tarihi : 03.02.2021

Karar No : 2021/84

Konu Özeti : Veri sorumlusu sabit telefon hizmeti sađlayan iřletmeci tarafından ilgili kiřilerin iletiřim verilerinin hukuka aykırı olarak iřlenmesi

Kuruma intikal eden bir řikâyette; bařvuru sahibi Hastanenin, kendilerine bařvuran hastalarla iletiřim kurmak amacıyla kayıt altına alınan telefon numaraları üzerinden hastalara SMS gönderilmesi için sabit telefon hizmeti sađlayan bir iřletmeci (1. STH) ile anlařma yaptığı, söz konusu anlařma kapsamında hastanelerinde tedavi gören hastalara ait telefon numaralarının 1. STH ile paylařıldığı ve içeriđi hastaneleri tarafından belirlenen SMS metinlerinin 1. STH tarafından hastalara gönderildiđi, bununla birlikte hastaneleri nezdinde kayıtlı bulunan hastalara ait telefon numaralarına, öncesinde hastanelerinde çalıřan ancak görevinden ayrılan bir doktora hasta sađlamak adına doktorun ismi ve soyismi bařlıđı altında geçiř yaptığı yeni hastanenin isim ve iletiřim bilgileri ile bařka bir STH'ye (2. STH) ait numara tařınabilirliđi yönlendirme kodunu içerir SMS'lerin gönderildiđi yönünde kendilerine pek çok řikâyet ulařtıđından hareketle Hastanelerinde tedavi gören hastalara ait çok sayıda telefon numarasının 1. STH tarafından 2. STH ile iřbirliđi yapmak suretiyle hukuka aykırı olarak iřlendiđi iddiaları ile anılan STH'ler hakkında Kanun çerçevesinde gerekli iřlemlerin tesis edilmesi talep edilmiřtir.

Konuya iliřkin bařlatılan inceleme neticesinde veri sorumlusu STH'lerden savunmaları istenilmiř olup, 1. STH'nin cevabi yazısında özetle; söz konusu iddiaların gerçeđi yansıtmadıđı, olayla hiřbir řekilde bilgilerinin ve bađlantılarının olmadıđı; 2. STH'nin cevabi yazısında ise özetle kendilerinin bařvuruya konu olayda yalnızca SMS trafiđini tařıma konusunda servis sađlayıcı hizmeti sunmakta oldukları, kendilerinin geçmiřte olan bu iřlemlerle ilgili yapmıř oldukları incelemeler sonrasında řikâyete konu kiřisel veri iřleme faaliyetinin geçmiřte alt bayileri olan ve řu an bayileri olmayan 1.

STH üzerinden gerçekleştiği, gönderilen SMS'lerin numaralarının kime ait olduğu, nereden temin edildiği sorumluluğunun hem aboneye ait hem de alt bayilerinin sorumluluğunda olduğundan dolayı bu konuda sorumlu tutulamayacakları ve bu hususun Bayi Sözleşmesinde "Bayi Yükümlülükleri" bölümünde de belirlendiği ifade edilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 03/02/2021 tarihli ve 2021/84 sayılı Kararı ile,

- 5/11/2014 tarihli ve 29166 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunun "Tanımlar" başlıklı 2 nci maddesinin birinci fıkrasının (c) bendinde ticari elektronik iletinin; *"Telefon, çağrı merkezleri, faks, otomatik arama makineleri, akıllı ses kaydedici sistemler, elektronik posta, kısa mesaj hizmeti gibi vasıtalar kullanılarak elektronik ortamda gerçekleştirilen ve ticari amaçlarla gönderilen veri, ses ve görüntü içerikli iletiler"*, (ç) bendinde hizmet sağlayıcının; *"Elektronik ticaret faaliyetinde bulunan gerçek ya da tüzel kişi"* (d) bendinde aracı hizmet sağlayıcının; *"Başkalarına ait iktisadi ve ticari faaliyetlerin yapılmasına elektronik ticaret ortamını sağlayan gerçek ve tüzel kişi,"* olarak tanımlanmış olduğu,

- Mezkur kanunun "Aracı hizmet sağlayıcıların yükümlülükleri" başlıklı 9 uncu maddesinin birinci fıkrasında; *"Aracı hizmet sağlayıcılar, hizmet sundukları elektronik ortamı kullanan gerçek ve tüzel kişiler tarafından sağlanan içerikleri kontrol etmek, bu içerik ve içeriğe konu mal veya hizmetle ilgili hukuka aykırı bir faaliyetin ya da durumun söz konusu olup olmadığını araştırmakla yükümlü değildir."* hükmünün yer aldığı, bu doğrultuda 2. STH'nin bir aracı hizmet sağlayıcı olarak değerlendirilmesi halinde, aracı hizmet sağlayıcının, haberleşme altyapısını kullanan hizmet sağlayıcısı tarafından sağlanan içeriği kontrol etmekle, bu içerik ve içeriğe konu mal veya hizmetle ilgili hukuka aykırı bir faaliyetin ya da durumun söz konusu olup olmadığını araştırmakla yükümlü kılınmamasından dolayı, somut şikâyet kapsamında, 2. STH yönünden Kanuna aykırılığın bulunmadığı,

- Öte yandan aralarındaki anlaşma çerçevesinde Hastane ile 1. STH arasında, Hastanenin hastalarına SMS metinlerinin gönderilmesi faaliyeti kapsamında bir veri sorumlusu-veri işleyen ilişkisinin mevcut olduğu, Kanunun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12 nci maddesinin dördüncü fıkrasında *"Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder."* hükmünün yer aldığı, 1. STH'nin Kanun hükümlerine aykırı olarak başvuru sahibi Hastanenin hastalarına ait iletişim verilerini işleme amacı dışında kullanmak suretiyle mezkûr Kanun hükmünde öngörülen yükümlülüğe aykırı hareket etmiş olduğu,

- Hastane müşterilerine ait telefon verilerinin 1. STH tarafından sağlandığı, 1. STH'nin sadece iletim görevini yerine getirmeyip kendi veri tabanını oluşturduğu, veri tabanında yer alan kişilere ticari elektronik ileti alma hususunda onaylarının bulunup bulunmadığına bakmaksızın hizmet verdiği ve bu yönüyle veri sorumlusu niteliğini haiz olduğu,

- STH'nin Kanununun 5 inci maddesinde hüküm altına alınan işleme şartlarını sağlamaksızın telefon numaralarına reklam içerikli ileti yönlendirmek suretiyle ilgili madde hükmüne aykırı hareket ettiği ve hastane müşterilerinin telefon numaralarını amacı dışında kullanarak Kanununun 12 nci maddesinin dördüncü fıkrasında öngörülen yükümlülüğe aykırı davrandığı kanaatine varıldığı

değerlendirmelerinden hareketle;

Hastane müşterilerinin kişisel verilerinin 1. STH tarafından hukuka aykırı bir biçimde işlendiği ve 1. STH'nin Kanununun 12 nci maddesinin birinci fıkrasının (a) bendi çerçevesinde kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı sonucuna varıldığından Kanununun 18 inci maddesinin birinci fıkrasının (b) bendi uyarınca 1. STH hakkında 125.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2021/79 sayılı KVKK Kararı

Veri sorumlusu banka tarafından ilgili kişinin verilerinin yakınları ile paylaşılması hakkında Kişisel Verileri Koruma Kurulunun 03/02/2021 tarihli ve 2021/79 sayılı Karar Özeti

Karar Tarihi : 03.02.2021

Karar No : 2021/79

Konu Özeti : Veri sorumlusu banka tarafından ilgili kişinin verilerinin yakınları ile paylaşılması hakkında

Kuruma intikal eden şikâyet; ilgili kişinin veri sorumlusu Bankanın kredi kartını kullandığı, veri sorumlusu tarafından ilgili kişinin kredi kartı borcuna ilişkin ilgili kişinin ablası ve babasına ait telefon numaralarının arandığı, ilgili kişinin bu hususta 15/11/2019 tarihinde veri sorumlusuna başvurarak ailesinin iletişim bilgilerine nasıl ulaşıldığı, kişisel verilerinin üçüncü kişilerle neden paylaşıldığı konularında bilgi talep ettiği, veri sorumlusunun 19/11/2019 tarihinde verdiği cevapta, ilgili kişinin kredi kartı borcu bilgilendirilmesi için arandığı ancak ulaşılamadığında alternatif telefon numaralarından da ilgili kişiye ulaşılmaya çalışıldığının, veri sorumlusu ile ilgili kişi arasında yapılan görüşme sonucunda ilgili kişinin veri sorumlusu bünyesinde kayıtlı olan cep telefonu dışındaki diğer numaralardan aranmaması için gerekli sistemsel güncellemelerin tamamlandığının ifade edildiği belirtilerek veri sorumlusu hakkında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusunun savunması talep edilmiş olup veri sorumlusu tarafından Kuruma intikal eden cevabi yazıda özetle;

- İlgili kişinin 2016 yılından bu yana beri veri sorumlusu bankaya ait kredi kartını kullandığı, söz konusu kredi kartının 25/08/2018 tarihinden başlayarak gecikmeye girdiği, ilgili kişinin kartının gecikmeye girmesi sebebiyle kendisi ile görüşüldüğü, ilgili kişinin gecikmede olan kartı için 23/10/2018, 28/12/2018 ve 28/03/2019 tarihlerinde, ilgili kişinin vermiş olduğu iletişim numarasından arandığı ancak ulaşılamadığı,
- İlgili kişiye bünyelerindeki iletişim numarasından ulaşmak mümkün olmayınca, 23/10/2018 tarihinde, sistemlerinde alternatif numara olarak tutulan ***10 numaralı telefon ile 28/12/2018 ve 28/03/2019 tarihlerinde ise ***55 numaralı telefonların arandığı ve söz konusu numaralar ile yapılan

görüşmelerde, ilgili kişinin kişisel verilerinin hiçbir şekilde üçüncü şahıslar ile paylaşılmadığı, sadece aranan kişilere, ilgili kişinin taraflarını geri araması için not bırakıldığı, yapılan görüşme kayıtlarına ilişkin dökümlerin yazıları ekinde Kuruma gönderildiği,

- Bankalarının tabi olduğu temel düzenleme olan 5411 sayılı Bankacılık Kanununun Ek 1 inci maddesinde " (...) Üye kuruluşlar, Risk Merkezince istenilen müşterileri ile ilgili her türlü bilgiyi vermekle yükümlüdür. (...) Risk Merkezi, nezdindeki her türlü bilgi alışverişini 73 üncü maddenin dördüncü fıkrası uyarınca en az beş banka tarafından kurulmuş şirketler aracılığı ile ve bu şirketlerle yapılacak sözleşmeler çerçevesinde de gerçekleştirebilir." hükmünün yer aldığı,

- Anılan madde kapsamında düzenlenen ve 10 Nisan 2012 tarihli, 28260 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren "Türkiye Bankalar Birliği Risk Merkezi Yönetmeliği" hükümleri uyarınca Risk Merkezi, Risk Merkezinin kuruluş amaçları doğrultusunda kanunlarda özel hayat ve aile hayatının gizliliğine ilişkin hükümler saklı kalmak kaydıyla özel hukuk tüzel kişileri ile kamu kurum ve kuruluşlarından, kamu kurumu niteliğinde meslek kuruluşları ve bunların üst kuruluşlarından bilgi talep etmeye ve kuruluş amaçları doğrultusunda özel hukuk tüzel kişileri ile kamu kurum ve kuruluşlarıyla, kamu kurumu niteliğinde meslek kuruluşları ve bunların üst kuruluşlarıyla Kurulun uygun görüşüne istinaden bilgi alışverişine yönelik sözleşmeler imzalamaya yetkili olduğu, bu çerçevede, Risk Merkezi Yönetiminin, özel hukuk tüzel kişileri, kamu kurum ve kuruluşları, kamu kurumu niteliğinde meslek kuruluşları ve bunların üst kuruluşlarından aldığı bilgiler ile bilgi alışverişine yönelik imzalanan sözleşmeler kapsamında temin ettiği bilgileri, üyelerinin maruz kalacakları riskleri ölçmek, karşı tarafın mali gücünü düzenli olarak analiz etmek ve izlemek için ihtiyaç duydukları gerekli bilgileri dikkate alarak paylaştığı,

- Risk Merkezi ile veri sorumlusu Banka arasında bu çerçevede bir gizlilik sözleşmesi akdedilmiş olduğu bahsi geçen yasal düzenlemeler ile alt mevzuatın belirlediği kapsamla sınırlı ve yine bu düzenlemelerde yer verilen esas ve usullere uygun olarak, müşterilerinin, kredilendirme süreçlerinde kullanabilmek ve risk bilgilerini alabilmek amaçları ile Risk Merkezinden sorgulamalar yapıldığı, bu çerçevede, ilgili kişinin bünyelerinde kayıtlı olan telefon bilgilerinin, Risk Merkezinden yapılan sorgulama vasıtasıyla temin edilerek, ilgili kişiye ulaşılmak maksadı ile ve sadece bu amaçla sınırlı kalınarak kullanıldığı,

- 15/11/2019 tarihinde ilgili kişi ile yapılan görüşme sonucunda, ilgili kişinin talebi üzerine, ilgili kişi ile yakınlarının kişisel verisi olan ***10 ve ***55 telefon numaralarından iletişime geçilmemesi için, 18/11/2019 tarihinde gerekli sistemsel güncellenmelerin gerçekleştirildiği

ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 03/02/2021 tarih ve 2021/79 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanunun “Veri Güvenliğine İlişkin Yükümlülükler” başlıklı 12 nci maddesinin (1) numaralı fıkrasında “Veri sorumlusu; a) kişisel verilerin hukuka aykırı işlenmesini önlemek, b) kişisel verilere hukuka aykırı erişilmesini önlemek, c) kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.” hükmüne yer verildiği,

- 5411 sayılı Bankacılık Kanununun 73 üncü maddesinde, (Değişik üçüncü fıkra: 13/2/2011-6111/146 md.) “Sıfat ve görevleri dolayısıyla bankalara veya müşterilerine ait sırları öğrenenler, söz konusu sırları bu konuda kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamazlar. Bu yükümlülük görevden ayrıldıktan sonra da devam eder. (Ek cümleler:20/2/2020-7222/10 md.) Bankacılık faaliyetlerine özgü olarak bankalarla müşteri ilişkisi kurulduktan sonra oluşan gerçek ve tüzel kişilere ait veriler, müşteri sırrı haline gelir. Diğer kanunların emredici hükümleri saklı kalmak kaydıyla, müşteri sırrı niteliğindeki bilgiler, bu maddede belirtilen sır saklama yükümlülüğünden istisna tutulan haller haricinde, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca müşterinin açık rızası alınsa dahi, müşteriden gelen bir talep ya da talimat olmaksızın yurt içindeki ve yurt dışındaki üçüncü kişilerle paylaşamaz ve bunlara aktarılamaz. Kurul ekonomik güvenliğe ilişkin yapacağı değerlendirme neticesinde, müşteri sırrı ya da banka sırrı niteliğinde olan her türlü verinin, yurt dışındaki üçüncü kişilerle paylaşılmasını ya da bunlara aktarılmasını

yasaklamaya, ayrıca bankaların faaliyetlerini yürütmede kullandıkları bilgi sistemleri ve bunların yedeklerinin yurt içinde bulundurulması hususunda karar almaya yetkilidir. Bu maddede belirtilen sır saklama yükümlülüğünden istisna tutulan hallerde yapılacak paylaşımlar da dahil olmak üzere, müşteri sırrı ve banka sırrı niteliğindeki bilgiler, sadece belirtilen amaçlarla sınırlı olmak ve ölçülülük ilkesine uygun olarak bu amaçların gerektirdiği kadar veriyi içermek kaydıyla paylaşılabilir...” hükmüne yer verildiği,

- Bankacılık Kanununun Ek 1’inci maddesinde “Risk Merkezi nezdinde bulunan sır niteliğindeki bilgileri, bu konuda kanunen yetkili kılınan mercilerden başkalarına açıklayanlar, hukuka aykırı olarak kendisi ya da başkası yararına kullananlar, yayanlar, verenler, aktaranlar veya ele geçirenler hakkında 159’uncu madde hükümleri uygulanır. Bu fıkrada tanımlanan suçların bir tüzel kişinin faaliyeti çerçevesinde işlenmesi halinde, ilgili tüzel kişi hakkında Türk Ceza Kanununun tüzel kişilere özgü güvenlik tedbirlerine hükmolunur.” düzenlemesinin yer aldığı,

- Bu çerçevede; veri sorumlusu tarafından ilgili kişinin kredi kartı borcuna ilişkin ilgili kişinin ablası ve babasına ait telefon numaralarının birkaç kere arandığı iddiası ile ilgili olarak, veri sorumlusundan alınan cevabi yazı ve ekindeki açıklamalar dikkate alındığında veri sorumlusu tarafından ilgilinin kişinin ablası ve babasının arandığı ikrar edilerek yapılan görüşme kayıtlarına ilişkin dökümlerin de ekte yer aldığı ve söz konusu kayıtlarda; ilgili kişinin ablasının bir defa, babasının ise iki defa arandığı, konuşma içeriğinde müşteri temsilcisi tarafından Bankanın Genel Müdürlüğünden arandığı ve ilgili kişinin taraflarına dönüş yapmasının söylendiği görüldüğünden ilgili kişinin ablası ve babasının Risk Merkezi üzerinden temin edilen telefon numarası üzerinden aranması suretiyle ilgili kişinin banka ile münasebetinin yakınları ile paylaşılmasının Kanunun 5 inci maddesinde yer alan kişisel veri işleme şartlarından herhangi birine dayanmaksızın gerçekleştirildiği

değerlendirmelerinden hareketle,

- Veri sorumlusu tarafından ilgili kişinin ablası ve babasının Risk Merkezi vasıtasıyla temin edilen telefon numarası üzerinden aranması suretiyle ilgili kişinin banka ile münasebetinin yakınları ile paylaşılmasının Kanunun 5 inci maddesinde yer alan kişisel veri işleme şartlarından herhangi birine dayanmaksızın, hukuka aykırı olarak gerçekleştirildiği dikkate alındığında veri sorumlusunun Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendinde öngörülen “Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek” yükümlülüğünü yerine getirmediği kanaatine varıldığından, veri sorumlusu hakkında, Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca idari para cezası uygulanmasına

karar verilmiştir.

2021/78 sayılı KVKK Kararı

Telekomünikasyon hizmetleri sunan bir veri sorumlusunun ürün satışı esnasında müşterilerinin pasaport fotoğraflarını çekerek depolaması hakkında Kişisel Verileri Koruma Kurulunun 03/02/2021 tarihli ve 2021/78 sayılı Karar Özeti

Karar Tarihi : 03.02.2021

Karar No : 2021/78

Konu Özeti : Telekomünikasyon hizmetleri sunan bir veri sorumlusunun ürün satışı esnasında müşterilerinin pasaport fotoğraflarını çekerek depolaması

Kuruma intikal eden bir ihbarda; veri sorumlusu tarafından İstanbul Havalimanı şubesinde dış hatlara gelen yolculara kontrollü hat satışı gerçekleştirilirken müşterilerin rızası olmadan, ileride eksik evrak cezası almamak için, müşteri pasaport fotoğraflarının çekilerek çalışanlardan oluşturulan bir whatsapp grubunda depolandığı ve üçüncü kişilerle paylaşıldığı, kendisinin de veri sorumlusunun eski bir çalışanı olarak söz konusu gruplara üye olduğu, bu kapsamda söz konusu gruplarda paylaşılan pasaport fotoğraflarının kendi telefonunda da depolandığı ifade edilerek başvuru ekinde söz konusu pasaport fotoğraflarının örneklerine yer verilmiş ve veri sorumlusu nezdinde gerekli denetimlerin yapılması talep edilmiştir.

Başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, veri sorumlusunun avukatı tarafından Kuruma intikal eden cevabi yazıda özetle;

- Veri sorumlusuna ait iş yerinin bir telekomünikasyon şirketi ile sözleşmesinin olduğu, sistemdeki her işlemin telekomünikasyon şirketi tarafından takip ve kontrol edildiği, hat açmak için Bilgi Teknolojileri ve İletişim Kurumu (BTK) düzenlemelerine uygun şekilde yeni müşterilere ait pasaport ve kimliklerin taratılarak sisteme yüklendiği, mağazada alınan kimlik bilgilerinin telekomünikasyon şirketinin depolama sistemine gönderilmesi nedeni ile çalışanlarının bu bilgilere tekrar ulaşmasının mümkün olmadığı,
- Veri sorumlusuna ait iş yerinin telekomünikasyon şirketi ile olan sözleşme ve kendi prosedürleri gereği 24 saat kamera ile izlendiği, çalışanlara yalnızca şirket bilgisayarını temin edilmekte olduğu ve bu bilgisayarlarda yapılan tüm işlemlerin kamera görüş açısında olduğu, şahsi telefonların mağaza

içerisinde kullanımının yasak olduğu, bilgisayarlarda ise telekomünikasyon şirketine ait sisteme giriş için her bir çalışana yalnızca kendisi tarafından bilinen bir kod verilmekte olduğu ve yapılacak her türlü işlemlerden sorumluluğu olduğu konusunda çalışanların bilgilendirildiği, sistemdeki her işlemin telekomünikasyon şirketi tarafından takip ve kontrol edildiği, hat açmak için BTK düzenlemelerine uygun şekilde yeni müşterilere ait pasaport ve kimliklerin taratılarak sisteme yüklendiği, bilgilerin sisteme yüklendikten sonra ancak iş gereği kullanılabilirdiği, bilgilerin kayıt edilmesinin mümkün olmadığı, sistemin aynı zamanda Emniyet Genel Müdürlüğü'ne de entegre olduğu, mağazada alınan kimlik bilgilerinin telekomünikasyon şirketinin depolama sistemine gönderilmesi nedeni ile şirket çalışanlarının bu bilgilere tekrar ulaşmasının mümkün olmadığı,

- Hat açma işlemlerinin akabinde müşteri bilgilerinin ve kontratın telekomünikasyon şirketi tarafından incelendiği ve eksik veya yanlış bilgi olması durumunda telekomünikasyon şirketi tarafından ceza kesildiği, veri sorumlusunun prim alabilmesinin yapılan satış adedine ve satışın BTK kurallarına uygun olarak eksiksiz yerine getirilmesine bağlı olduğu,

- Şikayetçinin veri sorumlusu bünyesinde çalıştığı sırada kişisel verilerin korunması konusunda uyarılmasına rağmen şirketi suçlayıcı gerçeğe aykırı beyanlarda bulunduğu, şikayetçinin dürüstlük kuralına, hukuka ve hakkaniyete aykırı davrandığı, iddiaların asılsız olduğunun yapılacak yerinde inceleme ile kolayca anlaşılabilirliği, ilgili telekomünikasyon şirketi tarafından veri sorumlusunun 9000 işleminin incelendiği ve hiçbir usulüz işleme rastlanılmadığı, şikayetçinin müşteri verilerini sisteme doğru işlememesinden doğan cezaların telekomünikasyon şirketi tarafından veri sorumlusuna rücu edildiği

ifade edilmiştir.

Bahse konu savunma üzerine, çalışanlara yönelik verildiği ifade edilen eğitimleri kanıtlayıcı nitelikte belgeler ile eğitimlerin içeriğine ilişkin bilgiler ve yürütüldüğü ifade edilen incelemelere ilişkin raporların birer örneği ile veri sorumlusunca Kanununun 12 nci maddesi kapsamında alınan tüm idari ve teknik tedbirlere ilişkin kanıtlayıcı nitelikte belgelerin Kuruma iletilmesi talep edilmiş olup veri sorumlusunun cevabi yazısında özetle; yeni işe başlayan çalışanlara yazıları ekinde sunulan kitapçığın verildiği, bu kitapçıkta yer alan oryantasyon konularından birinin de “kişisel verilerin korunması” olduğu, eğitimde müşterilerin kişisel verilerinin korunmasına ilişkin bilgilendirmelerin çalışanlara yapıldığı, çalışanların şahsi telefonlarını kullanmalarının yasak olduğu, bu nedenle şahsi telefonlarla fotoğraf çekilmediği ve ilgili kişilere ait kişisel verilerin whatsapp'ta depolanmadığı, telekomünikasyon şirketinin portalı üzerinden yapılan bu işlemlerin veri sorumlusunca saklanması mümkün olmadığı belirtilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 03/02/2021 tarih ve 2021/78 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) "Tanımlar" başlıklı 3 üncü maddesinde; "kişisel veri"nin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi; "kişisel verilerin işlenmesi"nin kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem, "veri sorumlusu"nun kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi, "veri işleyen" in veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi olarak tanımlandığı,

- Kanunun kişisel verilerin işleme şartlarına ilişkin 5 inci maddesinin (1) numaralı fıkrasının "Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez", (2) numaralı fıkrasının: "Aşağıdaki şartlardan birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür: a) Kanunlarda açıkça öngörülmesi. b) Fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması. c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması. ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması. d) İlgili kişinin kendisi tarafından alenileştirilmiş olması. e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması. f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" şeklinde düzenlendiği,

- Kanunun 12 nci maddesinin (1) numaralı fıkrasının "Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır." hükmünü amir olduğu, ayrıca anılan maddenin (3) numaralı fıkrasında veri sorumlusunun, kendi kurum veya kuruluşunda, Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorunda olduğu, (4) numaralı fıkrasında veri sorumluları ile veri işleyen kişilerin öğrendikleri kişisel verileri Kanun hükümlerine aykırı olarak başkasına açıklayamayacağı ve işleme amacının dışında

kullanamayacağı, (5) numaralı fıkrasında ise işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri sorumlusunun bu durumu en kısa sürede ilgilisine ve Kurula bildireceği, Kurulun, gerekmesi halinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebileceği hükümlerine yer verildiği,

- Somut olayda, pasaportların işlenmekte olduğu sistemin telekomünikasyon şirketi tarafından kurulan ve yönetilen bir sistem olduğu anlaşılmalı birlikte, pasaportların sisteme işlenmesini sağlayan çalışanların veri güvenliğine ilişkin yükümlülüklerine uymasını ve sisteme işleme sırasında kişisel verilerin güvenliğini sağlamak hususunda şikâyet olunan şirketin sorumluluğu olduğu kanaatine varıldığından şikâyet olunan şirketin somut olayda veri sorumlusu olduğu,

- Veri sorumlusu tarafından çalışanlara yalnızca şirket bilgisayarı temin edildiği, şahsi telefonların mağaza içerisinde kullanımının yasak olduğu, bilgisayarlarda ise telekomünikasyon şirketine ait sisteme giriş için her bir çalışana yalnızca kendisi tarafından bilinen bir kod verildiği ve yapılacak her türlü işlemlerden sorumluluğu olduğu konusunda çalışanların bilgilendirildiği, sistemdeki her işlemin telekomünikasyon şirketi tarafından takip ve kontrol edildiği, hat açmak için BTK düzenlemelerine uygun şekilde yeni müşterilere ait pasaport ve kimliklerin taratılarak sisteme yüklendiği ve çalışanlarının bu bilgilere tekrar ulaşmasının mümkün olmadığı belirtilmekle birlikte, ihbar ekinde, pasaport bilgilerinin bir grupta paylaşıldığını gösterir kanıtlayıcı nitelikte belgeler olduğu görüldüğünden söz konusu ihbara ilişkin olarak veri sorumlusu Şirketin Kanununun 12 nci maddesinin (1) numaralı fıkrası kapsamında kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı ve Kanununun 12 nci maddesinin (3) numaralı fıkrası kapsamında yer alan veri sorumlusunun, kendi kurum veya kuruluşunda, Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorunda olduğu hükmüne aykırı hareket ettiği,

- Öte yandan, veri sorumlusunun daha önce bir çalışanın müşteri verilerini sisteme doğru işlememesinden doğan cezaların telekomünikasyon şirketi tarafından veri sorumlusu şirkete rücu edildiği, bu çalışanın Kanuna aykırı davranışlarının kamera ile tespit edildiği ve söz konusu çalışandan kaynaklı olarak veri sorumlusu bünyesinde bir veri ihlali yaşandığı anlaşılmış olup söz konusu ihlal kapsamında Kurula yapılmış bir bildirim olmadığı dikkate alındığında veri sorumlusu tarafından Kanununun 12 nci maddesinin (5) numaralı fıkrasında yer verilen, “işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri sorumlusunun bu durumu en kısa sürede ilgilisine ve Kurula bildireceği, Kurulun, gerekmesi halinde bu durumu, kendi internet

sitesinde ya da uygun göreceği başka bir yöntemle ilan edebileceği” hükmüne uygun hareket edilmediği

değerlendirmelerinden hareketle,

- Veri sorumlusu tarafından sunulan belgelere karşın ihbar ekinde, pasaport bilgilerinin bir grupta paylaşıldığının anlaşılması nedeni ile ihbara ilişkin olarak veri sorumlusu Şirketin Kanununun 12 nci maddesinin (1) numaralı fıkrası kapsamında kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı ve Kanununun 12 nci maddesinin (3) numaralı fıkrası kapsamında yer alan veri sorumlusunun, kendi kurum veya kuruluşunda, Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorunda olduğu hükmüne aykırı harekete ettiği kanaatine varıldığından veri sorumlusu hakkında Kanununun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca idari para cezası uygulanmasına,

- Veri sorumlusunun daha önce bir çalışanın müşteri verilerini sisteme doğru işlememesinden doğan cezaların telekomünikasyon şirketi tarafından veri sorumlusuna rücu edildiği, yine söz konusu çalışana verildiği anlaşılan uyarı yazısında, çalışanın Kişisel Verilerin Korunması Kanununa aykırı davranışlarının kamera ile tespit edildiği, kişinin müşteri kimlik resimlerinin kaydını şahsi cep telefonunda muhafaza ettiğinin anlaşıldığına yönelik ifadelerin yer aldığı ve söz konusu çalışandan kaynaklı olarak veri sorumlusu bünyesinde bir veri ihlali yaşandığı anlaşılmış olup, söz konusu ihlal kapsamında Kurula yapılmış bir bildirim olmadığı dikkate alındığında veri sorumlusu tarafından Kanununun 12 nci maddesinin (5) numaralı fıkrasına uygun hareket edilmemiş olması nedeniyle Kanununun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında veri sorumlusu hakkında idari para cezası uygulanmasına,

- 5237 sayılı Türk Ceza Kanununun 136 ncı maddesinde düzenlenen “Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.” hükmü gereğince ihbara konu aykırılıkların sorumluları hakkında Türk Ceza Kanunu kapsamında ihbaren Cumhuriyet Başsavcılığına bildirimde bulunulmasına

karar verilmiştir.

2021/32 sayılı KVKK Kararı

İlgili kişinin kişisel verilerinin bilgisi dışında veri sorumlusu banka nezdinde sorgulanması hakkında Kişisel Verileri Koruma Kurulunun 12/01/2021 tarihli ve 2021/32 sayılı Karar Özeti

Karar Tarihi : 12.01.2021

Karar No : 2021/32

Konu Özeti : İlgili kişinin kişisel verilerinin bilgisi dışında veri sorumlusu banka nezdinde sorgulanması

İlgili kişi adına vekilinden alınan şikâyette, ilgili kişinin, şikâyet edilen veri sorumlusu banka bünyesinde müdür yardımcısı pozisyonunda çalışmakta olan eşi ile boşanma davasının mevcut olduğu, bu süreçte şikâyet edilen banka aracılığıyla, müvekkiline ait kişisel veri niteliğinde bilgilerin sorgulandığı ve bu bilgilerin boşanma davası dosyasına sunulduğu, bahse konu evrakın, müvekkilinin geçmiş yıllara ilişkin karşılıksız çek bilgileri ve yine müvekkili hakkındaki tedbir kararlarına ilişkin olduğu, bu bilgilerin ancak müvekkilinin izin ve onayı dâhilinde sorgulanabileceği, söz konusu sorgulamanın banka aracılığıyla yapılmış olmakla kalmayıp müvekkilinin kişisel verilerinin, kişisel çıkar amacıyla mahkemeye sunulmak suretiyle paylaşıldığı ve bu kapsamda özel hayatın gizliliğinin ihlal edildiği, bu durumun 6698 sayılı Kişisel Verilerin Korunması Kanununa (Kanun) aykırılık teşkil ettiği ve şikâyet edilen veri sorumlusu bankaya aykırılığı gidermesi ve söz konusu durumdan doğan zararları tazmin etmesi amacıyla iadeli taahhütlü başvuru yapılmasına rağmen 30 günlük yasal süre içerisinde herhangi bir cevap alınmadığı ifade edilerek, veri sorumlusu banka hakkında gerekli işlemlerin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusu Bankadan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişinin başvurusu üzerine Bankanın ilgili iş birimince gereken incelemenin yapıldığı, Şube Operasyon Yetkilisi'nin, eşi ve aynı zamanda Bankanın müşterisi olan ilgili kişinin istihbarat sorgusunu yaparak sonuçlarını ilgili kişinin bilgisi ve isteği dışında, katılma alacağı davasına ilişkin mahkemeye sunduğunun tespit edildiği, bu süre zarfında, ilgili kişinin avukatı ile iletişime geçilerek Bankanın ilgili birimi nezdinde inceleme başlatılmış olduğu,

- Banka tarafından yapılan inceleme sonucunda, İnsan Kaynakları Uygulama Esas ve Usulleri'nin (KINAMA) "9.4.... Bankaya veya Bankanın müşterilerine ait sırları açığa vurmamak, personele ait gizli belge ve bilgileri ilgisi olmayan kişilere vermek" maddesine temas etmesi nedeni ile; mahkemenin bu veriye ulaşmak istediği takdirde Bankadan temin edebileceği ve eşler arasında zaten bilinen bir konunun diğer eşin avukatı marifetiyle -konuyla ilgisiz üçüncü kişilere açık etmeksizin- mahkemeye sunması hususları bir arada değerlendirilerek, diğer eşin bir mektupla dikkatinin çekilmesine karar verildiği ve yazı ile müşteri başvurusunun yanıtlandığı, bu itibarla başvuru talebi doğrultusunda Kuruma başvurulmadan önce Banka tarafından gerekli işlemler tesis edildiğinden, Kuruma yapılan başvuruya ilişkin talebin konusuz kaldığı ve başvurunun haklı ve yasal dayanağının bulunmadığı,

- Bankanın müşterisi olan ilgili kişinin kişisel verilerinin Banka tarafından, kişisel verilerin işlenmesine dair hukuka uygunluk nedenleri çerçevesinde hukuka uygun olarak işlendiği ve kişisel verilerinin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirin alındığı,

- İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi şeklinde ortaya çıkan veri güvenliği ihlallerinin, veri sorumlusu sıfatını haiz Banka ya da yurtiçi iştirakinin yetkili veya çalışanları değil, bu verilere yetkisiz ve hukuka aykırı olarak erişen üçüncü kişiler tarafından gerçekleştirilebileceği, bu verilere görevinden kaynaklı olarak erişim yetkisi bulunmakta olan Banka personeli diğer eşin hukuka aykırı bir erişiminin söz konusu olmadığı,

- Diğer eşin şahsi görevinden kaynaklanmayan sebeplerle ilgili kişinin kişisel verilerine ulaşarak mahkemeye sunmasında Bankanın bir kusuru olmadığı ve bunun da ötesinde, Bankanın objektif olarak alabileceği bir güvenlik önleminin de bulunmadığı,

- Sonuç itibarıyla, Bankanın kişisel verilerin korunmasına ilişkin mevzuatı uygulama konusundaki azami dikkat ve hassasiyeti ile şikâyete konu ilgili kişinin talep doğrultusunda gerekli araştırmanın yapıldığı, Bankanın kişisel verilerin işlenmesinde hukuka aykırı herhangi bir iş ve işleminin bulunmadığı ve öngörülen veri güvenliğine ilişkin yükümlülüklerini yerine getiren Bankanın bir kusuru ve dolayısıyla sorumluluğu bulunmadığı

belirtilmiştir.

Konuya ilişkin olarak yapılan inceleme neticesinde, Kişisel Verileri Koruma Kurulunun 12/01/2021 tarih ve 2021/32 sayılı Kararı ile;

- Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinde kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, bu çerçevede, kişisel verilerin ancak; hukuka ve dürüstlük kurallarına uygun şekilde, belirli, açık ve meşru amaçlar kapsamında, doğru ve gerektiğinde güncel olma şartıyla, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun olarak işlenebildiği,
- Kanunun kişisel verilerin işlenme şartlarının belirlendiği 5 inci maddesinin (1) numaralı fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmadan işlenemeyeceği hüküm altına alınmış olmakla birlikte, (2) numaralı fıkrasında, sayılan hallerde ilgili kişinin açık rızası olmadan kişisel verilerinin işlenmesine imkân tanındığı, buna göre; a) Kanunlarda açıkça öngörülmesi, b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması d) İlgili kişinin kendisi tarafından alenileştirilmiş olması, e) Bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması, f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması hallerinden birinin varlığı durumunda ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün bulunduğu,
- Kanunun 12 inci maddesinin (1) numaralı fıkrasında veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu hükmünün, (5) numaralı fıkrasında ise işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunun bu durumu en kısa sürede ilgisine ve Kurula bildireceği ve Kurulun gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebileceği hükmünün yer aldığı,
- Kurulun 31/05/2018 tarih ve 2018/63 sayılı Kararı ile bir veri sorumlusu nezdinde buldukları pozisyon veya görev itibarıyla kişisel verilere erişme yetkisi olanlar tarafından, yetkileri aşmak ve/veya yetkilerini kötüye kullanmak suretiyle, kişisel amaçlara veya nedenlere bağlı olarak işleme amacı dışında söz konusu kişisel verilerin işlenmesi ve/veya bu verilerin üçüncü kişilerle

paylaşılmasının 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (1) numaralı fıkrasına aykırılık teşkil edeceğinden, bu kapsamdaki eylemlerin önlenmesi amacıyla veri sorumlularınca uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirin alınması gerektiği hususunda veri sorumlularının bilgilendirilmesine karar verildiği,

- Ayrıca, Kurul, 24.01.2019 tarih ve 2019/10 sayılı Kararı ile Kanunun 12 inci maddesinin (5) numaralı fıkrasında yer alan “en kısa sürede” ifadesinin 72 saat olarak yorumlanmasına ve bu kapsamda veri sorumlusunun “işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi” durumunu öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirmesine, veri sorumlusunca söz konusu veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılmasına karar verildiği,

- Somut olayda ilgili kişiye ait kişisel veri niteliğinde bilgilerin veri sorumlusu bünyesinde çalışan diğer eş tarafından sorgulandığı ve bu bilgilerin boşanma davası dosyasına sunulduğu iddiasının Banka bünyesinde yapılan inceleme sonucunda veri sorumlusu Banka tarafından da kabul edildiği ve bu kapsamda, Bankanın İnsan Kaynakları Uygulama Esas ve Usulleri'nin (KINAMA) “9.4... Bankaya veya Bankanın müşterilerine ait sırları açığa vurmamak, personele ait gizli belge ve bilgileri ilgisi olmayan kişilere vermek” maddesine temas etmesi nedeniyle veri sorumlusu tarafından Banka çalışanı diğer eşin bir mektupla dikkatinin çekilmesine karar verildiği,

- Veri sorumlusu Banka tarafından ilgili kişinin kişisel verilerinin hukuka uygun olarak işlendiği ve Kanunun 12 nci maddesi kapsamında kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirin alındığı, veri sorumlusu bünyesinde çalışan diğer eşin görevinden kaynaklı olarak erişim yetkisi bulunduğu ve şikâyet konusuna ilişkin olarak Bankanın objektif olarak alabileceği bir güvenlik önleminin bulunmadığı, Kişisel Verilerin Korunması Kanununa ve ikincil mevzuata uyum ve uygun veri güvenliği düzeyini temin etmeye ilişkin olarak düzenlemelerin hazırlandığı ve veri sorumlusu bünyesinde çalışan personele farkındalıklarının artması için eğitim verildiği hususları belirtilmekle birlikte Kişisel Verilerin Korunması Uygulama Esas ve Usulleri başlıklı idari ve teknik tedbirlerin listelendiği bir bölüme yer verilmesi dışında isimleri geçen düzenlemeler, personele verilen eğitimler ve veri sorumlusu nezdinde uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü idari ve teknik tedbirin alındığına ilişkin herhangi bir tevsik edici belgenin Kuruma sunulmadığı,

- Veri sorumlusu Banka tarafından işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi kapsamındaki ihlalin varlığından haberdar olunmasına rağmen Kanununun 12 inci maddesinin (5) numaralı fıkrası uyarınca ve Kurulun 24.01.2019 tarih ve 2019/10 sayılı Kararı kapsamında ilgisine ve Kurula herhangi bir veri ihlal bildirimini yapılmadığı

değerlendirmelerinden hareketle;

- İlgili kişinin kişisel verisi niteliğindeki kimlik, müşteri işlem ve finansal bilgilerinin (geçmiş yıllara ilişkin karşılıksız çek ve tedbir kararı bilgileri) veri sorumlusu bünyesinde çalışan kişi tarafından sorgulanıp mahkemeye sunulması nedeniyle söz konusu kişisel verilere kanuni olmayan yollarla başkaları tarafından erişim sağlandığı, Kurulun 31.05.2018 tarih ve 2018/63 sayılı “Veri Sorumlusu Nezdindeki Kişisel Verilere Erişim Yetkisi Bulunan Personelin Yetkisi ve Amacı Dışında Söz Konusu Verileri İşlemesi Hususunun Değerlendirilmesine İlişkin İlke Kararı”nda da düzenlenen bu hususun Kanununun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirlerin alınmadığının bir göstergesi olduğu dikkate alındığında, veri sorumlusu Banka hakkında idari yaptırım uygulanmasına

- Veri sorumlusunun kişisel verilerin güvenliğini tesis etmeye yönelik gerekli teknik ve idari tedbirleri aldığı hususunda tevsik edici belgeleri Kuruma iletmesi hususunda talimatlandırılmasına,

- Kişisel verilere kanuni olmayan yollarla başkaları tarafından erişim sağlanması halinde Kanununun 12 nci maddesinin (5) numaralı fıkrasında düzenlenen hüküm gereği bu durumun en kısa sürede ilgisine ve Kurula bildirilmesi gerektiği hususunda veri sorumlusuna hatırlatmada bulunulmasına,

- Ayrıca, 5237 sayılı Türk Ceza Kanununun “Verileri hukuka aykırı olarak verme veya ele geçirme” başlıklı 136 ncı maddesinde yer alan suçların işlenmiş olabileceği dikkate alınarak, Türk Ceza Kanununun 136 ncı maddesi çerçevesinde ilgili kişinin kişisel veri niteliğindeki kimlik, müşteri işlem ve finansal bilgilerinin (geçmiş yıllara ilişkin karşılıksız çek ve tedbir kararı bilgileri) sorgulayıp mahkemeye sunan veri sorumlusu bünyesinde çalışan şahıs hakkında gerekli hukuki işlemlerin tesisi için konunun Cumhuriyet Başsavcılığına bildirilebileceği yönünde ilgili kişinin bilgilendirilmesine karar verilmiştir.

2020/957 sayılı KVKK Kararı

Bir ilaç şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 15/12/2020 tarih ve 2020/957 sayılı Karar Özeti

Karar Tarihi : 15.12.2020

Karar No : 2020/957

Konu Özeti : Bir ilaç şirketinin veri ihlal bildirimini

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin güvenlik seviyesini artırmak amacıyla yeni bir sunucuya geçiş sürecinde sunucu parametreleri optimize edilmediği için aylık maaş bordrosu bildirimlerinin e-posta yoluyla bildirilmesinde sistemsal bir hata meydana gelmesi ile oluştuğu,
- Sistem tarafından otomatik olarak oluşturulan ve güncel maaş bordrolarını içeren e-postalarda meydana gelen hata nedeniyle, 337 çalışanın bordrosunun yanlış çalışanlara gönderildiği,
- İhlalin yanlış bordro giden bir çalışanın e-posta yoluyla İnsan Kaynakları Departmanına bilgi vermesi sonucu anlaşıldığı,
- İhlalin 27.11.2020 tarihinde gerçekleştiği ve aynı gün tespit edildiği,
- Teknik eşleştirme hatası nedeniyle çalışanın aylık bordrosuna, başka bir çalışan tarafından erişilebilmesinin mümkün olduğu,
- Bordroların, çalışanın o ayki maaş bilgisi ve ad- soyad, banka hesap numarası ve T.C. kimlik numarası gibi kişisel veriler içerdiği,
- İhlalden etkilenen kişi sayısının 337; kayıt sayısının 1348 olduğu

ifadelerine yer verilmiştir.

Söz konusu bildirim incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 15/12/2020 tarih ve 2020/957 sayılı Kararı ile;

- İhlalin, gerçekleşmesinden 13 dakika sonra tespit edildiği, gerçekleşmesinden 2 saat sonra ise sonlandırıldığı,

- İhlalin, güvenlik seviyesini arttırmak amacıyla yeni bir sunucuya geçiş sürecinde oluştuğu,
- İhlal veri sorumlusunun çalışanlarının bordro bilgilerinin diğer çalışanlara gönderilmesi şeklinde gerçekleştiğinden olumsuz etki doğurma olasılığının düşük olduğu,
- İhlale sebep olan e-postaların silinmiş olduğu ve e-postaların gönderildiği kişilere gerekli uyarının yapıldığı,
- İhlale sebep olan konuda ihlal sonrası gerekli teknik ve idari tedbirlerin alındığı

dikkate alındığında Kanununun 12 inci maddesinin (1) numaralı fıkrası kapsamında veri sorumlusu hakkında bu aşamada yapılacak bir işlem olmadığına,

- İhlalin tespit tarihinden sonra 72 saat içinde Kurula bildirilmemiş olduğu dikkate alındığında, Kanununun 12 nci maddesinin (5) numaralı fıkrası uyarınca işlenen verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde en kısa sürede ilgisine ve Kurula, Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararına uygun olarak bildirimde bulunması hususunda daha dikkatli olunması, ayrıca ilgili kişilere bildirim yapıldığına ve e-postanın gönderildiği kişilere e-postanın silinmesi yönünde uyarının yapıldığına ilişkin tevsik edici belgelerin Kurumumuza gönderilmesi hususlarında veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2020/935 sayılı KVKK Kararı

Bir sigorta şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 08/12/2020 tarih ve 2020/935 sayılı Karar Özeti

Karar Tarihi : 08.12.2020

Karar No : 2020/935

Konu Özeti : Bir sigorta şirketinin kişisel veri ihlali bildirimini

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Sağlık yenileme talebinde bulunan bir müşteriye, Müşteri İletişim Merkezi (Çağrı Merkezi) tarafından sehven başka bir müşterinin poliçe muafiyet bildirimini bilgisinin iletildiği,
- Dolayısıyla gerçek kişiye ait sağlık verisinin, konunun tarafı olmayan başka bir müşteri ile paylaşıldığı,
- Veri Kaybı Önleme Sistemi (DLP) düzenli kontrolleri sırasında, sistemi kontrol eden görevli tarafından veri ihlalinin tespit edildiği ve ilgili birimlere aksiyon alınması için iletildiği,
- Veri ihlalden kimlik, iletişim ve sağlık kategorilerindeki kişisel verilerin etkilendiği,
- Sehven iletilen poliçe muafiyet bildiriminde, ilgili kişinin sağlık poliçesi kapsamında olmayan rahatsızlıklarının belirtildiği,
- Bu rahatsızlıkların poliçe muafiyetinin, ilgili kişinin bu rahatsızlıklara sahip olması veya sahip olduğu şüphesi olması sebebiyle yazıldığından, ilgili kişinin sağlık verisinin işlendiği,
- Veri ihlalden veri sorumlusu müşterisi olan 1 kişinin etkilendiği,
- Veri sorumlusunun Müşteri İletişim Merkezi çalışanlarının müşteriyle direkt temasta olduklarından dolayı düzenli eğitimlere tabi olduğu

ifadelerine yer verilmiştir.

Söz konusu bildirim incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 08/12/2020 tarih ve 2020/935 sayılı Kararı ile;

- İhlalden 1 kişinin etkilendiği,

- İhlalden etkilenen kişisel verilerin kimlik, iletişim ve sağlık bilgileri olduğu,
- Veri sorumlusunun “en kısa sürede” (24.01.2019 tarih ve 2019/10 sayılı Kurul kararında belirtilen 72 saatlik süre içerisinde) Kurumumuza veri ihlalini bildirme yükümlülüğünü yerine getirdiği,
- İlgili kişilere ihlale ilişkin 03.12.2020 tarihinde bildirim yapılacağı belirtilmiştir

hususları dikkate alındığında veri sorumlusu hakkında 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 inci maddesi kapsamında bu aşamada yapılacak bir işlem bulunmadığına, öte yandan veri sorumlusu tarafından ilgili kişiye bildirim yapılması ve söz konusu bildirim yapıldığı ile bahse konu verilerin sehven gönderilen müşteri nezdinde silindiğine dair tevsik edici belgelerin Kurumuza iletilmesi hususunda talimatlandırılmasına karar verilmiştir.

2020/934 sayılı KVKK Kararı

Enerji sektöründe faaliyet gösteren veri sorumlusunun veri ihlali bildirimini hakkında Kişisel Verileri Koruma Kurulunun 08/12/2020 tarih ve 2020/934 sayılı Karar Özeti

Karar Tarihi : 08.12.2020

Karar No : 2020/934

Konu Özeti : Enerji sektöründe faaliyet gösteren veri sorumlusunun veri ihlali bildirimini hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlali bildiriminde;

- Veri sorumlusunun kurumsal internet sitelerinde yayınlama amacıyla kurum içinde hazırlanmış ürün katalogları, dokümanlar, resimler ve sertifikaların yer aldığı bir kurum içi arşiv platformunun bulunduğu,
- Yönetim tarafından kendisine verilen yetki kapsamında, platform kullanıcılarının eğitiminden sorumlu ve bu konuda yetkili bir çalışanın, platformunun kullanımı hakkında uygun şekilde eğitimi için profesyonel görevlerinin yürütülmesi amacıyla platform yöneticisiyle birlikte bir irtibat listesi hazırladığı,
- Eğitimi düzenleyen çalışanın platform yöneticisi tarafından sağlanan kullanıcı listesini, olağan iş koordinasyonu kapsamında yetkili üst düzey kullanıcıları tarafından erişim sağlanabilen bir ortak klasörde sakladığı,
- Bu kullanıcılardan bir tanesinin irtibat listesi ararken kullanıcı listesinde sehven şifre bilgilerinin de bulunduğunu fark ettiği ve durumu raporladığı,
- Söz konusu listede, sehven, kurum içi bir platformun kullanıcılarının şifrelerinin açık bir şekilde, kullanıcı adı, isim, profesyonel e-posta adresi gibi tanımlayıcılarla birlikte yer aldığı,
- İhlalden etkilenen kişi ve kayıt sayısının 2 olduğu,

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 05/05/2020 tarih ve 2020/345 sayılı Kararı ile;

- İhlalden Türkiye’den sadece iki (2) kullanıcının etkilenmiş olduğu,
 - İhlale ilişkin dosyanın erişimden kaldırılmadan önce yalnızca sekiz (8) kullanıcı tarafından erişilmiş olabileceği,
 - Söz konusu sekiz (8) kullanıcı ile görüşüldüğü tamamının gizlilik yükümlüklerini anladığını ve kabul ettiğini ve herhangi bir şifre bilgisini kullanmayacaklarını veya paylaşmayacaklarını teyit ettiği,
 - İhlale konu olan verilerin niteliği gereği olumsuz etki doğurma olasılığının düşük olduğu,
 - İhlalden sonra ilgili platformdaki şifrelerin maskelenmesinin sağlandığı, bunun da Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)’nde 4.1. Teknik Tedbirler Özet Tablosu’nda da yer aldığı üzere veri maskeleyme tedbirine uygun olduğu,
 - İhlal gerçekleşikten sonra tespit edilen dosyanın veri sorumlusu tarafından ivedilikle ortadan kaldırıldığı, bu durumun da Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)’nde 2.2. Çalışanların Eğitilmesi ve Farkındalık Çalışmaları başlığı altında yer alan *“Kişisel veri güvenliğini zedeleyecek saldırılar ile siber güvenliğe ilişkin, çalışanların sınırlı bilgileri olsa dahi ilk müdahaleyi yapmaları, kişisel veri güvenliğinin sağlanması konusunda büyük önem taşımaktadır.”* ifadesi kapsamında değerlendirilebileceği,
 - İhlalden etkilenen platform kullanıcılarının şifrelerinin yenilendiği ve ilgili kullanıcılara şifrelerini değiştirmeleri için bir uyarı e-postası gönderildiği, bu tedbirin de ihlal sonrasında kişisel verilerin olumsuz etki doğurma olasılığı düşük olsa da veri sorumlusunun Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)’nde 2.1. Mevcut Risk ve Tehditlerin Belirlenmesi başlığı altında yer alan *“risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmeli, gerekli teknik ve idari tedbirler planlanarak uygulamaya konulmalıdır”* tedbirini aldığı bir göstergesi olduğu
- hususları dikkate alındığında, Kanunun 12 nci maddesinin (1) numaralı fıkrası kapsamında bu aşamada yapılacak bir işlem bulunmadığı
- İhlalin 02.09.2019 ile 16.09.2019 arası gerçekleştiği, 16.09.2019 tarihinde tespit edildiği ve 24.10.2019 tarihinde Kurumumuza bildirildiği dikkate alındığında Kurul’un 24.01.2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde veri sorumlusunun bildirimde bulunmadığı,

- Bununla birlikte veri sorumlusunun çok uluslu bir yapısı olduğu ve etkilenen ilgili kişilerin bulunduğu ülkelerin tespit edilmesi ve ilgili ülkelerin bildirim yükümlülüklerinin tespit edilmesi ve değerlendirilmesi için gerekli süre göz önüne alındığında makul kabul edilebileceği,

- Etkilenme ihtimali olan mevcut tüm kullanıcıların e-posta mesajıyla bilgilendirildiği ve aynı şifreyi kullanmış olabilecekleri diğer platformlar da dâhil şifrelerini değiştirmeleri konusunda uyarıldığı, yapılan bilgilendirmenin Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararında belirtilen bildirimde bulunması gereken asgari unsurlardan kişisel veri kategorileri bazında hangi kişisel verilerin ihlalden etkilendiği, veri ihlalinin olumsuz etkilerinin azaltılması için alınan veya alınması önerilen tedbirler, ilgili kişilerin veri ihlali ile ilgili bilgi almalarını sağlayacak irtibat kişilerinin isim ve iletişim detayları ya da veri sorumlusunun web sayfasının tam adresi, çağrı merkezi vb. iletişim yolları hususlarını barındırdığı, ancak, ihlalinin ne zaman gerçekleştiği ve kişisel veri ihlalinin olası sonuçları hakkında yeterli bilgi verilmediği

dikkate alındığında, Kanununun 12 nci maddesinin (5) numaralı fıkrası uyarınca işlenen verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde en kısa sürede ilgisine ve Kurula, Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararına uygun olarak bildirimde bulunması hususunda daha dikkatli olunması yönünde talimatlandırılmasına

karar verilmiştir.

2020/927 sayılı KVKK Kararı

Unutulma hakkı kapsamında ilgili kişinin arama motorunda adı ve soyadı ile bağlantılı sonuçların kaldırılması talebine ilişkin Kişisel Verileri Koruma Kurulunun 08/12/2020 tarihli ve 2020/927 sayılı Karar Özeti

Karar Tarihi : 08.12.2020

Karar No : 2020/927

Konu Özeti : Üniversitede öğretim üyesi olarak görev yapmakta olan bir kişinin aynı üniversitede açılan akademik kadroya aile yakınının alınmasında usulsüzlük bulunduğu hususunda yapılan haberlerin arama motorunda ilgili kişinin adı ve soyadı ile arama yapıldığında listelenmemesine yönelik talebi

İlgili kişinin şikâyet başvurusunda özetle; üniversitede öğretim üyesi olarak görev yaptığı, görev yapmış olduğu bölümde akademik kadro ilanı verildiği, kadro için sınavların usulüne uygun şekilde yapıldığı ve kadro için aile yakınının sınavlarda başarılı olduğu, ancak sosyal medyada bu kadro işe alımı ile ilgili doğru olmayan haberlerin yapıldığı ve üniversitenin tepkiler üzerine soruşturma başlattığı, soruşturma sonucunda bir usulsüzlük olmadığına üniversite tarafından tespit edildiği, haberlerin kaldırılması talebi ile arama motoruna başvuruda bulunduğu ancak arama motoru tarafından URL'ler hakkında herhangi bir işlem yapılmamasına karar verildiği ve ilgili kişinin kaldırma talebini söz konusu siteyi kontrol eden web yöneticisine gönderebileceği bilgisinin tarafına iletildiği, dolayısıyla arama motoru tarafından ilgili kişinin talebinin karşılanmadığı, bu kapsamda yapılan haberlerin aile yakınının ve kendisinin kamuda görev yapmasını ve hayatını olumsuz yönde etkilediği belirtilerek söz konusu içeriklerin arama motorunda indekslenmeyecek şekilde teknik düzenlemeye tabi tutulması talep edilmektedir.

Bahse konu şikâyet başvurusuna ilişkin olarak ilgili mevzuat hükümleri çerçevesinde yapılan değerlendirme neticesinde Kişisel Verileri Koruma Kurulu tarafından alınan 08/12/2020 tarih ve 2020/927 sayılı Kararda aşağıdaki değerlendirmelere yer verilmiştir;

6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel

verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek olup Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır.

Kanunun “Tanımlar” başlıklı 3 üncü maddesinde kişisel verinin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi, veri sorumlusunun kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi, kişisel verilerin işlenmesinin ise kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade ettiği belirtilmiştir.

Kanunun “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi” başlıklı 7 inci maddesinin birinci fıkrası “Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.” hükmünü haizdir.

Kanunun “İlgili Kişinin Hakları” başlıklı 11 inci maddesinin birinci fıkrasında “Herkes, veri sorumlusuna başvurarak kendisiyle ilgili; a) Kişisel veri işlenip işlenmediğini öğrenme, b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme, c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir.” hükmü yer almaktadır.

Öte yandan, Kişisel Verileri Koruma Kurulunun “Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına Yönelik Talepler” e ilişkin olarak almış olduğu 23.06.2020 tarih ve 2020/481 sayılı Kararı ile;

- Arama motorlarının, üçüncü taraflara ait internette topladıkları verilerin işlenmesinin amaç ve vasıtalarını belirledikleri göz önünde bulundurularak Kanunun 3 üncü maddesinde yer verilen tanım çerçevesinde veri sorumlusu olarak kabul edilmesine,
- Arama motorunun işletmecisinin otomatik, düzenli ve sistematik olarak internette yayınlanan bilgiyi bulduğu, daha sonra kendi indeksleme programları çerçevesinde alıp, kaydedip, organize ettiği kişisel verileri arama sonuçlarının listesi formunda düzenlediği, sunucuları üzerinde sakladığı, belirli durumlarda açıkladığı ve kullanıcılarına sunduğu dikkate alındığında arama motorları tarafından gerçekleştirilen faaliyetlerin Kanunun 3 üncü maddesi kapsamında 'kişisel veri işleme'' faaliyeti olarak değerlendirilmesine,
- Kanunun başvuru ve şikâyet hakkına ilişkin hükümlerinde belirtilen usul ve süreler esas alınarak ilgili kişilerin, arama sonuçlarının indeksten çıkarılmasına yönelik talepleri ile ilgili olarak öncelikle arama motorlarına başvuruda bulunmaları, veri sorumlusu arama motorlarının söz konusu talepleri reddetmeleri veya başvuru sahibine cevap vermemeleri halinde ilgili kişilerce Kurula şikâyette bulunabileceklerine,
- İlgili kişinin arama motorları üzerinden kendi ad ve soyadı ile yapacağı bir arama sonucunda gösterilen sonuçların indeksten çıkarılması gerektiğine yönelik yapılacak değerlendirmede, ilgili kişinin temel hak ve özgürlükleri ile kamunun söz konusu bilgiyi edinmesinden sağlayacağı menfaatler arasında bir denge testi yapılması, yarışan menfaatlerden hangisinin ağır bastığının gözetilmesi ve bu değerlendirme yapılırken öncelikli olarak karar ekinde yer verilen açıklamaların dikkate alınması ancak bu konudaki şikâyetlerin değerlendirme sürecinde dikkate alınacak kriterlerin bunlarla sınırlı olmayacağı, her somut olay özelinde Kurulca ilave ölçütlerin de gündeme gelebileceğine,
- İlgili kişilerin, arama motorları üzerinden kendi ad ve soyadları ile yapılacak aramalar neticesinde gösterilen sonuçların indeksten çıkarılmasına yönelik taleplerinin veri sorumlusu arama motorları tarafından reddedilmesi veya taleplerine cevap verilmemesi halinde Kurula başvuruda bulunulurken aynı zamanda doğrudan yargı yoluna başvurmalarının da mümkün bulunduğuna karar verilmiştir.

Kişilerin ad ve soyadı ile arama motorları üzerinden yapılan aramalarda çıkan sonuçların indeksten çıkarılmasına ilişkin değerlendirmede dikkate alınacak ve her somut olay üzerinde incelenecek kriterler de Kurulun bahse konu Kararı ile belirlenmiş olup bunlar; ilgili kişinin kamusal yaşamda önemli bir rol oynaması, arama sonuçlarının öznesinin çocuk olması, bilginin içeriğinin doğruluğu,

bilginin kişinin çalışma hayatı ile ilgisi, bilginin ilgili kişi hakkında hakaret, onur kırıcı, iftira niteliğine sahip olması, bilginin özel nitelikli kişisel veri niteliği taşıması, bilginin güncelliği, bilginin kişi hakkında önyargıya sebep olması, bilginin kişi açısından risk doğurması, bilginin kişinin kendisi tarafından yayımlanma durumu, içeriğin gazetecilik faaliyeti kapsamında işlenen verileri kapsamaması, bilgilerin yayınlanmasında yasal zorunluluk olması, bilginin ceza gerektiren bir suçla ilgili olması şeklinde belirlenmiştir.

Bu kapsamda, ilgili kişinin arama motorundan adı ve soyadı ile bağlantılı sonuçların kaldırılmasına yönelik talebinin değerlendirilmesi neticesinde;

- İlgili kişinin kamu üniversitesinde görev yapmakta olduğu, başvuru konusu hususlarda ilgili kişinin aile yakınının işe alınması ile ilgili usulsüzlük iddiaları sonucunda üniversite tarafından soruşturma açıldığı bilgisinin doğru olduğu, söz konusu bağlantılarda yer alan haberin ilgili kişinin çalışma yaşamına ilişkin olduğu ve ilgili kişinin hâlihazırda aynı işi yaptığı, bilgilerin özel nitelikli kişisel veri niteliği taşımadığı, yapılan haberlerin 2020 tarihli olduğu, dolayısıyla güncel olduğu, bilginin kişi açısından risk doğurmadığı ve içeriklerin gazetecilik faaliyeti kapsamında değerlendirilebileceği, öte yandan, bilginin kişi hakkında ön yargıya sebep olabileceği ancak bunun kanıtlanabilir nitelikte olmadığı, ilgili kişiye ilişkin bilgilerin yayınlanmasında yasal zorunluluk bulunmadığı, bilginin kişinin kendisi tarafından yayımlanmadığı, bilginin ceza gerektiren bir suçla ilgili olmadığı hususları göz önünde bulundurularak ilgili kişi hakkında yayınlanan içeriklerin arama motorundan kaldırılması yönündeki talebine ilişkin olarak veri sorumlusu tarafından yapılan işlemin 23.06.2020 tarih ve 2020/481 sayılı Kurul Kararı ekinde yer alan kriterler açısından yerinde olduğuna, bu kapsamda söz konusu şikayet ile ilgili olarak Kanun kapsamında tesis edilecek bir işlem bulunmadığına,

- Diğer taraftan ilgili kişinin haber içeriğinin gerçeği yansıtmadığına yönelik iddialarının ise yargı mercileri nezdinde ileri sürülmesi gerektiğine

karar verilmiştir.

2020/915 sayılı KVKK Kararı

Belediyede memur olarak görev yapan ilgili kişinin, veri sorumlusu bünyesinde işe giriş çıkış takibinin biyometrik veri işlenerek yapılması hakkında Kişisel Verileri Koruma Kurulunun 01/12/2020 tarihli ve 2020/915 sayılı Karar Özeti

Karar Tarihi : 01.12.2020

Karar No : 2020/915

Konu Özeti : Belediyede memur olarak görev yapan ilgili kişinin, veri sorumlusu bünyesinde işe giriş çıkış takibinin biyometrik veri işlenerek yapılması

Kurula intikal eden şikâyette ilgili kişi tarafından veri sorumlusu bünyesinde 657 sayılı Devlet Memurları Kanunu kapsamında çalışan memur olduğu, veri sorumlusu bünyesinde personel giriş çıkışlarının takibi için parmak izi okuma cihazları ile kişisel verilerinin, her personel için parmak izi bilgilerinin alındığı ve sisteme tanıtıldığı, bu konudaki uygulama için kendisine ait olan parmak izi bilgilerinin veri sorumlusunun kayıt sisteminden, kağıt ortamından ve elektronik ortamdan silinmesi ve kendisine bilgi verilmesi talebiyle veri sorumlusuna başvuru yaptığı; kendisine verilen cevapta sistemlerinden bu bilgilerin silinemeyeceğinin beyan edildiği, parmak izi bilgilerinin onayı olmadan işlenemeyeceği ve resmi başvuru yapmasına rağmen verilerinin silinmesi isteğinin kabul edilmediği belirtilmiştir.

Başlatılan inceleme çerçevesinde söz konusu iddialara ilişkin olarak veri sorumlusunun savunması istenilmiş olup alınan cevabi yazıda

- Tüm birimlerde tutulan kişisel veriler üzerinde Kanun kapsamında çalışmalara 2018 yılında başlandığı, irtibat kişilerinin belirlenerek personelin bu konu hakkında eğitim, e-posta ve duyuru panolarına asılan aydınlatma metinleriyle bilgilendirildiği ve kişisel verilerin korunması ve işlenmesine dair politika ve prosedürlerin hazırlandığı, ayrıca yapılan işlemlerin tamamlanması ve devamında işletilmesi, 6698 sayılı Kanuna ve standartlara uygun yapıldığının ölçülebilmesi hususunda Bağımsız Denetim Firması tarafından denetlenerek BS10012-2009 Veri Koruma ve Kişisel Bilgi Yönetim Standardı Sertifikası ile belgelendirildikleri,

- Başkanlığa ait Kültür Merkezleri, Bilgi Evleri, Spor Salonları vb faaliyet gösteren çok sayıda tesisin bulunduğu, iştirak personeli dahil olmak üzere 2302 kişinin istihdamının sağlandığı, kişisel verilerin korunmasına yönelik yapılacak başvuru ve taleplerin usulüne ilişkin Belediyesi Kişisel Verilerin İşlenmesi Duyuru Aydınlatma Metninin, Başkanlığın resmi web sitesi üzerinden ilan edildiği, Belediyesi Kişisel Verilerin Korunması Başvuru Formunun doldurularak hangi yöntemlerle başvuru yapılacağına duyurulduğu, Başkanlık personeline ise hizmet içi eğitimlerle konuya ilişkin bilgilendirmenin yapıldığı,
- İlgili kişiye ait başvuruda Kişisel Verilerin Korunması Başvuru Formunun bulunmaması, başvurunun veri sorumlusu görevini yürütmekte olan personele ulaştırılmaması ve çalıştığı Müdürlüğe verilmiş olan dilekçenin İnsan Kaynakları ve Eğitim Müdürlüğüne Bilgi ve Belge Talebi konulu başvuru olarak gönderilmesi nedeniyle ilgiliye ait başvurunun Kanun kapsamında değerlendirilmediği, buna bağlı olarak verilen cevap yazısında kamu kaynaklarını etkin ve verimli kullanabilmek amacıyla personelin işe giriş çıkışlarının takibi için parmak izinin kullanıldığı herhangi bir şaibeye mahal vermeden verinin temin edildiği ve üçüncü kişilerle paylaşılmasının teknik olarak mümkün olmadığı bildirildiği, alınan parmak izi şablonunun silinemeyeceğine dair herhangi bir ifadenin ise kullanılmadığı,
- Başkanlıkça uygulanmakta olan PDKS sistemi gereği personelden alınan parmak izlerinin salt mesai kontrollerinde kullanıldığı, mesai kontrolü için ayrıca sicil numarası ve şifreli giriş, ıslak imzalı form yöntemlerinin kullanıldığı, covid-19 salgını sebebiyle halihazırda müdürlüklerde personel kontrolünün listelerin ıslak imzalanması metodu ile sağlandığı, parmak izi sisteminin devre dışı olduğu, parmak izi tanıma algoritmasının temel işlevinin parmak izinin çıkartılması ve karakterlerin eşleştirilmesi olduğu, parmak izinin çıkartılmasıyla kastedilenin parmak izinin temel karakteristik verilerinin şifrelenip karakteristik bir şablon haline getirilmesi olduğu, bir şablon haline getirilen parmak izinin daha sonra hiçbir şekilde görüntüsünün alınmadığı ve işlem yapılamadığı, kullanılan şifrelenmiş parmak izi şablonunun özel bir algoritma olduğu ve üçüncü kişilere tamamen kapalı olduğu, parmak izi şablonunun formatının teknik belgeler veya ürün kaynak kodları vasıtasıyla dahi herhangi biri tarafından öğrenilmesi veya başkalarının bilgisine açılmasının mümkün olmadığı ifade edilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 01/12/2020 tarihli ve 2020/915 sayılı Kararı ile,

- 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) “Tanımlar” başlıklı 3 üncü maddesinde “kişisel veri”nin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi;

“veri sorumlusu”nun kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi; “kişisel verilerin işlenmesi”nin ise kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı,

- Özel nitelikli kişisel veriler arasında yer alan biyometrik veri tanımına Kanunda yer verilmemekle birlikte, 25.05.2018 tarihinde yürürlüğe giren Avrupa Genel Veri Koruma Tüzüğünde (GDPR) biyometrik verinin; “yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel veriler” olarak tanımlandığı,

- GDPR’nin Recital bölümünün 51 inci maddesinde de fotoğrafların işlenmesinin doğrudan biyometrik veri olarak nitelendirilemeyeceği, yalnızca gerçek bir kişinin benzersiz bir şekilde tanımlanmasına veya doğrulanmasına izin veren belirli bir teknik yöntemle işlendiğinde, bu verilerin biyometrik verilerin tanımı kapsamında kabul edileceğine yönelik açıklamalara yer verildiği, dolayısıyla bir verinin biyometrik veri kapsamında değerlendirilebilmesi için o verinin sadece o kişiyi tanımlayabilme ya da doğrulayabilme özelliğine sahip olmasının kriter alındığının değerlendirildiği, yine Danıştay 15. Dairesinin 2014/4562 Esas sayılı kararında biyometrik yöntemlerin, ölçülebilir fizyolojik ve bireysel özellikleri aracılığıyla gerçekleştirilen ve otomatik şekilde doğrulanabilen kimlik denetleme tekniklerini ifade ettiği belirtilerek, bu yöntemler arasında parmak izi tanıma, avuç içi tarama, el geometrisi tanıma, iris tanıma, yüz tanıma, retina tanıma, DNA tanıma gibi yöntemlerin bulunduğu ifade edildiği dikkate alındığında, işe giriş çıkışlarda personelin parmak izinin taranması suretiyle kişilerin kimlik doğrulamasının yapılması hususunda adı geçen veri sorumlusunun özel nitelikli kişisel veri niteliğindeki biyometrik veri işleme faaliyetinde bulunduğu,

- Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinde yer alan ilkelerden, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi çerçevesinde işlenen verilerin belirlenen amaçların gerçekleştirilebilmesine elverişli olması, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasının gerektiği; ölçülülük ilkesinin ise, veri işleme faaliyeti ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması, diğer bir ifadeyle veri işlemenin amacı gerçekleştirecek ölçüde olması gerektiğine işaret ettiği; bu kapsamda, kişisel veri işleme faaliyetinin gerçekleşmesi için gerekli olmayan kişisel verilerin toplanmaması

ve/veya işlenmemesi gerektiği, veri sorumlusunun amacı çerçevesinde, ölçülülük ilkesine uygun olarak ilgili kişiden minimum düzeyde bilgi talep etmesi, bunun dışındaki amaç için gerekli olmayan veri işlemeden kaçınması gerektiği,

- Kişisel verilerin işlenmesi ilgili kişinin iznine bağlı olarak gerçekleştirilse ve belirli bir amaca bağlı olsa bile açık rızanın aşırı miktarda veri toplanmasını meşrulaştırmayacağı, buna göre kişisel verilerin yalnızca belirli amaçlar için ve gerektiği kadar toplanması ve amacın gerektirdiği yerlerde kullanılması gerektiği,

- Öte yandan, Danıştay 5. Dairenin 2013/5342 E. ve 2013/9525 K. sayılı Kararında “personelden kişisel veri alınması kapsamında olan "parmak izi tarama sistemi" ile mesai takibi uygulamasının, kamusal alanda da olsa "özel hayatın gizliliği" ilkesi kapsamında bulunduğu anlaşılmaması karşısında; uygulamanın sınırlarını usul ve esaslarını gösteren bir yasal dayanağının bulunmaması, toplanan verilerin ileride başka bir şekilde kullanılmayacağına dair bir güvencenin mevcut olmaması göz önüne alındığında, yukarıda belirtilen temel haklar ve Anayasal ilkelerle bağdaşmayan dava konusu işlemde hukuka uyarlık, davanın reddi yolunda verilen İdare Mahkemesi kararında hukuki isabet bulunmadığı anlaşılmıştır.” şeklinde hüküm tesis edilmiş olup bu kapsamda, mesai kontrolü için parmak izi alınması gibi çoğunlukla üstün güvenlik önlemi alınmasına ihtiyaç duyulan alanlarda kullanılan yöntem yerine alternatif yollara başvurulabileceği, dolayısıyla veri sorumluları bünyesinde mesai kontrolü amaçlı giriş ve çıkışlar için parmak izi okutma sisteminin kurulmasının Kanunun “Genel İlkeler” başlıklı 4 üncü maddesi kapsamında ele alınması gerektiği, üstün güvenlik önlemi alınmasına ihtiyaç duyulmayan alanlarda yalnızca mesai kontrolü amacıyla parmak izi alınmasına yönelik uygulamaların mezkur maddenin (ç) bendindeki ölçülülük ilkesine aykırı olduğu,

- Somut olayda ilgili kişinin veri sorumlusu tarafından kendisine ait olan parmak izi bilgilerinin hukuka aykırı olarak işlenmesine ilişkin şikâyeti ile ilgili veri sorumlusunun PDKS sistemi gereği personelden alınan parmak izlerinin salt mesai kontrollerinde kullanıldığı, parmak izi tanıma algoritmasının temel işlevinin parmak izinin çıkartılması ve karakterlerin eşleştirilmesi olduğu, parmak izinin çıkartılmasıyla kastedilenin parmak izinin temel karakteristik verilerinin şifrelenip karakteristik bir şablon haline getirilmesi olduğu, bir şablon haline getirilen parmak izinin daha sonra hiçbir şekilde görüntüsünün alınmadığı ve işlem yapılamadığı şeklindeki açıklamaları çerçevesinde veri sorumlusu bünyesinde çalışan personellerden işe giriş ve çıkışlarda parmak izlerinin kullanıldığının açıkça kabul edildiği, ilgili kişinin parmak izinin açık rızasına dayanılarak alınıp alınmadığı hususunun anlaşılamadığı; ancak işe giriş ve çıkışlarda söz konusu kişisel verisinin işlenmesinin devam etmesi noktasında ilgili kişinin onayı olmadan parmak izinin işlenemeyeceği

hususunda şikayeti bulunduğu dikkate alındığında ilgili kişinin parmak izi kullanılarak mesai kontrolü yapılması hususunda açık rızasının olmadığı kanaatine varıldığı,

- Öte yandan veri sorumlusu tarafından mesai kontrolü için parmak izi, sicil numarası ve şifreli giriş, ıslak imzalı form yöntemlerinin kullanıldığı, covid-19 salgını sebebiyle halihazırda müdürlüklerde personel kontrolünün ıslak imzalama metodu ile sağlandığı, parmak izi sisteminin devre dışı olduğuna yönelik savunması dikkate alındığında işe giriş ve çıkış kontrollerinin biyometrik verileri işlemenin haricinde alternatif yollar ile sağlanabildiği, dolayısı ile üstün güvenlik önlemleri alınmasını gerektirecek bir durumun da olmadığı görüldüğü, bu kapsamda veri sorumlusu bünyesinde mesai kontrolü amaçlı giriş ve çıkışlar için parmak izi okutma sisteminin kurulmasının Kanunun "Genel İlkeler" başlıklı 4 üncü maddesinin (ç) bendindeki ölçülülük ilkesine aykırı olduğu kanaatine varıldığı ve veri sorumlusunun söz konusu uygulamasının Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendine aykırılık teşkil ettiği,

- Öte yandan, ilgili kişinin Kanunun 7 nci ve 11 inci maddesi çerçevesinde veri sorumlusuna başvurmasına rağmen veri sorumlusu tarafından, söz konusu başvurunun Kişisel Verilerin Korunması Başvuru Formu ile yapılmaması, başvurunun veri sorumlusu görevini yürütmekte olan personele ulaştırılmaması ve çalıştığı Müdürlüğe verilmiş olan dilekçenin İnsan Kaynakları ve Eğitim Müdürlüğüne Bilgi ve Belge Talebi konulu başvuru olarak gönderilmesi nedeniyle ilgiliye ait başvurunun Kanun kapsamında değerlendirilmediği, buna bağlı olarak da verilen cevabi yazıyla kamu kaynaklarının etkin ve verimli kullanabilmek amacıyla personelin işe giriş çıkışlarının takibi için parmak izinin kullanıldığı, herhangi bir şaibeye mahal vermeden temin edildiği ve üçüncü kişilerle paylaşılmasının teknik olarak mümkün olmadığı bildirildiği, alınan parmak izi şablonunun silinemeyeceğine dair herhangi bir ifadenin kullanılmadığı şeklinde savunma yapıldığı görülmekle birlikte, ilgili kişinin Kanuna atıf yapıp taleplerini açıkça belirten ve tarafına talepleriyle ilgili bilgi verilmesine yönelik isteğini de içeren ıslak imzalı dilekçesini veri sorumlusuna sunduğu, bu anlamda ilgili kişinin kişisel verilerinin silinmesi yönünde talepte bulunduğu, öte yandan söz konusu evraka sayı numarası verildiğinin açık olduğu ancak veri sorumlusunun ilgili kişinin başvurusunu Kanun kapsamında değerlendirmeyip kişisel verisinin silinmesi hususunda herhangi bir ifadeye yer vermeyerek ilgili kişinin talebini cevaplamadığı, bu durumun dürüstlük kuralı ile bağdaşmadığı

değerlendirmelerinden hareketle;

- Veri sorumlusu bünyesinde mesai kontrolü amacıyla biyometrik veri olan parmak izinin işlenmesinin Kanunun "Genel İlkeler" başlıklı 4 üncü maddesinin (ç) bendindeki amaçla bağlantılı,

sınırlı ve ölçülü olma ilkesine aykırı olduğu, öte yandan söz konusu veri işleme faaliyetinin hukuka uygun bir veri işleme şartına dayanmadığı dikkate alındığında veri sorumlusunun söz konusu uygulamasının Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendine aykırılık teşkil ettiği değerlendirildiğinden Kanunun 18 inci maddesinin 3 üncü fıkrası hükmüne göre söz konusu veri sorumlusu bünyesinde görev yapan kişiler hakkında disiplin hükümlerinin işletilmesine ve sonucunun Kurula bildirilmesine,

- Veri sorumlusu tarafından bugüne kadar işlenen ve muhafaza edilen parmak izi ile ilgili verilerin Kanunun 7 nci maddesi ile Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik hükümlerine uygun olarak ivedilikle imha edilmesi, eğer ilgili özel nitelikli kişisel verilerin üçüncü kişilere aktarılması söz konusu ise, imha edilmesine yönelik işlemlerin bu verilerin aktarıldığı üçüncü kişilere ivedilikle bildirilmesinin sağlanması, işe giriş ve çıkış işlemlerinin salgın dönemi dışında da geçerli olmak üzere alternatif yollarla sağlanması, biyometrik veri ile giriş çıkış işlemleri yapılması uygulamasına son verilmesi ve mevcut sistemin kaldırılması hususlarında veri sorumlusunun talimatlandırılmasına,

- Öte yandan söz konusu sistemin kaldırıldığı ve kişisel verilerin imha edildiğini tevsik edici bilgi ve belgelerin Kurula gönderilmesi konusunda veri sorumlusunun talimatlandırılmasına,

- Veri sorumlusunun ilgili kişinin başvurusunu Kanun kapsamında değerlendirmeyip kişisel verisinin imhası hususunda herhangi bir ifadeye de yer vermemesinin dürüstlük kurallarıyla bağdaşmadığı, ilgili kişinin veri sorumlusu bünyesinde bulunan kişisel verilerinin imhası talebine istinaden, talebin yerine getirildiğine ve söz konusu kişisel verilerin imha edildiğine ilişkin ilgili kişinin bilgilendirilmesi ve söz konusu imha işlemine ilişkin tevsik edici bilgi ve belgelerin Kurula iletilmesi hususu ile ilgili kişilerin taleplerine Kanun kapsamında cevap verilmesi konusunda azami dikkat ve özenin gösterilmesi hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2020/905 sayılı KVKK Kararı

Bir sigorta şirketinin kişisel veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 24.11.2020 tarih ve 2020/905 sayılı Karar Özeti

Karar Tarihi : 24.11.2020

Karar No : 2020/905

Konu Özeti : Bir sigorta şirketinin kişisel veri ihlal bildirimini hakkında karar

Veri sorumlusu bir sigorta şirketinin Kuruma intikal eden yazılarında özetle;

- Veri sorumlusunun internet sayfasının bulunduğu test sunucusunun siber saldırıya uğradığı ve bu durumun aynı tarihte veri sorumlusu tarafından tespit edildiği,
- Test sunucusunda bulunan internet sayfasının kullanıcı giriş ekranından birden çok giriş denemesi yapılması sonucunda sisteme giriş sağlanabildiği,
- Gerçekleşen yetkisiz erişim sonucu uygulamanın bulunduğu veri tabanının silindiği ve silinen veri tabanı yerine fidye taleplerinin bulunduğu yeni bir veri tabanının sisteme yüklendiği,
- Veri tabanının silinmesi işleminden önce muhtemelen siber saldırıyı gerçekleştiren kişi/kişiler tarafından kopyalandığının veri sorumlusu tarafından düşünüldüğü,
- Giriş denemeleri belirli aralıklarla yapılmış olduğundan SIEM sistemi tarafından algılanmadığı,
- Yurtdışından çok fazla giriş denemesi gerçekleştiği ancak bunun herhangi bir anomaliye sebep vermediği,
- İhlalden etkilenen kişi sayısının 311 olduğu,
- İhlalden etkilenen kişisel verilerin T.C. kimlik no, isim, soy isim, e-posta, plaka bilgisi olduğu ifadelerine yer verilmiştir.

Söz konusu kişisel veri ihlali bildirimini incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun (Kurul) 24.11.2020 tarih ve 2020/905 sayılı Kararı ile;

- İhlale konu test sunucusunun, veri sorumlusu nezdinde yıllık olarak yapılan sızma testleri kapsamına alınmamasının söz konusu test sunucusunda gerekli kontrollerin yapılmadığının göstergesi olduğu,
- Veri sorumlusuna ait “BT Veri Güvenlik ve Veri İhlali Prosedürü”nde tedbirler kapsamında “Periyodik aralıklarla veya ihtiyaç duyulduğunda sızma testi hizmeti olarak sistem açıklarının kontrolü sağlanmalıdır.” ifadesinin bulunmasına rağmen test sunucularının prosedürdeki tedbirlere uygun bir şekilde kontrol edilmediği, söz konusu kontrollerin uygun bir şekilde yapılmadığı,
- Test sayfasının tüm dünyaya açık olarak ulaşılabilir olduğu, saldırganın 7 kez giriş denemesi sonucunda sisteme başarılı bir şekilde giriş yapmış olduğu, veri sorumlusu nezdinde kullanılan parolaların yeteri kadar karmaşık ve güçlü olmadığı,
- Veri ihlali öncesinde test aşamasında kullanılan kişisel verilerin test sunucusundaki veri tabanına kaydedildiği, veri ihlali sonrasında ise mevcut teknolojinin değiştirilerek test sunucusunda kişisel verilerin kaydedilmeden test işlemlerinin yapılabildiği dikkate alındığında veri sorumlusunun kişisel verileri veri tabanına kaydetmeden test işlemlerini yapmış olması durumunda gerçekleşen siber saldırı vakasında kişisel veri ihlalinin söz konusu olmayacağına görüldüğü,
- Veri ihlali öncesinde test sunucusuna yapılan erişimlerde sistemler arasında SSL VPN gibi güvenli iletişim sağlama yöntemlerinin kullanılmadığı, ayrıca ek güvenlik katmanı olarak erişimlerde İki Faktörlü Kimlik Doğrulama (2FA) gibi güçlü kimlik doğrulama yöntemlerinin kullanılmadığı,
- Veri ihlalinden etkilenen kişisel veriler arasında, T.C. kimlik numarasının bulunduğu, ilgili kişiler için önem arz eden bir veri olduğundan söz konusu veri grubu işlenirken verilerin şifrelenerek muhafaza edilmesi durumunda verilere yetkisiz olarak erişilse bile veri ihlalinin ilgili kişiler üzerindeki olası olumsuz etkilerinin azaltılabileceği, ancak veri sorumlusunun böyle bir eylemde bulunmadığı dikkate alındığında kişisel verilerin gizlilik derecesine göre muhafaza edilmesi konusunda veri sorumlusu tarafından yeteri kadar özen gösterilmediği

hususları dikkate alınarak 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari ve tedbirleri almayan Şirket hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 300.000 TL,

Kurula ve ilgili kişilere yapılan bildirim ile ilgili olarak;

- İhlalin 28.02.2020 tarihinde tespit edildiği ve 04.03.2020 tarihinde Kurula bildirildiği dikkate alındığında Kurulun 24.01.2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin

öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde veri sorumlusunun Kurula bildirimde bulunmadığı,

- Geç bildirimde bulunulmasına sebep olarak ilgili teknik çalışmaların (sunucu ve firewall log kayıtlarının incelenmesi işlemleri) gecikmesinin gösterildiği,
- Veri sorumlusu tarafından veri ihlaline ilişkin veri sorumlusunun internet sitesinde duyuru yapılmış olmasının, ilgili kişilerin tespit edilmiş olması nedeniyle ilgili kişilere bildirim şeklinde kabul edilemeyeceği,
- Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararına uygun olarak ilgili kişilere bildirim yapılmadığı

dikkate alınarak, veri sorumlusunun 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (5) numaralı fıkrasında yer verilen “en kısa sürede” (24.01.2019 tarih ve 2019/10 sayılı Kurul kararında belirtilen 72 saatlik süre içerisinde) bildirimde bulunma yükümlülüğüne aykırı hareket etmesi ve 18.09.2019 tarih ve 2019/271 sayılı Kurul Kararına uygun şekilde ilgili kişilere bildirimde bulunulmamış olması nedeniyle Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca veri sorumlusu hakkında 30.000 TL

olmak üzere toplam 330.000 TL idari para cezası uygulanmasına karar verilmiştir.

2020/816 sayılı KVKK Kararı

Bir teknoloji şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 22/10/2020 tarih ve 2020/816 sayılı Karar Özeti

Karar Tarihi : 22.10.2020

Karar No : 2020/816

Konu Özeti : Bir teknoloji şirketinin veri ihlal bildirimini

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin, mağazada yapılan bir alışveriş sonrasında adına e-fatura düzenlenen müşterinin sistemde kayıtlı e-posta adresine ilgili faturanın gönderilmesi neticesinde bu faturanın aynı ad ve soyada sahip farklı bir müşteriye ulaşması neticesinde gerçekleştiği,
- CRM sistemi üzerinde adına fatura düzenlenen müşterinin telefon numarasının aynı ad ve soyada sahip iki farklı müşteri adına oluşturulduğu ve kayıtlarda her ikisinde de yer aldığı,
- Bu durumun kişilerin GSM-1 ve GSM-2 olarak oluşturulan kayıtları arasına aynı telefon numarasının bir müşteri için GSM-1, diğer müşteri için GSM-2 olarak kaydedilmiş olması nedeniyle fatura gönderiminde hatalı e-posta adresine ulaşılması nedeniyle meydana geldiği,
- 15.10.2020 tarihinde kişisel verileri ihlal edilen müşteri ile aynı ad ve soyada sahip müşterinin müşteri hizmetlerini arayarak kendisine iletilmiş olan e-mailde yer alan faturanın kendisine ait olmadığı bilgisini vermesi üzerine sistem üzerinden kontroller gerçekleştirilerek ihlalin tespit edildiği,
- Kayıtlarda meydana gelen karışıklığın mağazadaki kayıt aşamasında hatalı bilgi girişinden mi yoksa CRM sistemindeki veri tekilleştirme özelliğinden mi kaynaklandığına ilişkin araştırmaların sürdüğü,
- İhlalin hemen ardından müşteri kayıtlarının sistem üzerinden düzeltildiği, hatalı faturanın diğer müşteriden geri alınmasının sağlandığı ve doğru bilgilerle doğru kişiye fatura düzenlendiği,
- İhlalden etkilenen kişisel verilerin; müşterinin adı soyadı, T.C. Kimlik Numarası, cep telefonu numarası ve fatura bilgileri olduğu,

- İhlal edilen kişisel verilerin olumsuz etki doğurması yüksek olmayan kişisel veriler olduğu ve aynı zamanda ihlalin etkisinin azaltılması amacıyla ilgili kişiye bildirim yapılması ve sehven gönderilen e-postanın silinmesi gibi gerekli işlemlerin gerçekleştirildiği,
- İhlalin 15.10.2020 tarihinde gerçekleştiği ve 16.10.2020 tarihinde tespit edildiği,
- İhlalden etkilenen kişi sayısının 1; kayıt sayısının 4 olduğu,
- İlgili kişiye telefon görüşmesi ile bildirim yapıldığı

ifadelerine yer verilmiştir.

Söz konusu bildirim incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 22/10/2020 tarih ve 2020/816 sayılı Kararı ile;

- İhlalden 1 kişiye ait kişisel verilerin etkilendiği,
- İlgili kişiye telefon yoluyla bildirim yapıldığı,
- İhlale konu kişisel verilerin ilgili kişi üzerinde olumsuz etki doğurma olasılığının düşük olduğu,
- İhlale konu e-postanın silinmesinin sağlandığı,
- Veri sorumlusunun ihlale kısa zamanda müdahale ettiği

hususları dikkate alındığında, bu aşamada veri sorumlusu hakkında 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesi kapsamında yapılacak bir işlem olmadığına karar verilmiştir.

2020/787 sayılı KVKK Kararı

Sağlık sektöründe faaliyet gösteren bir şirketin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 09.10.2020 tarih ve 2020/787 sayılı Karar Özeti

Karar Tarihi : 09.10.2020

Karar No : 2020/787

Konu Özeti : Sağlık sektöründe faaliyet gösteren veri sorumlusu şirketin kişisel veri ihlal bildirimini hakkında

Sağlık sektöründe faaliyet gösteren bir veri sorumlusu tarafından Kuruma intikal ettirilen kişisel veri ihlali bildiriminde özetle;

- İhlalin 30.09.2020 tarihinde başladığı,
- İhlalin 05.10.2020 tarihinde tespit edildiği ve yine aynı tarihte sona erdiği,
- Dünya genelinde yaygın olan ve veri sorumlusu tarafından da kullanılan bir uygulamada bulunan açıktan yararlanılarak, veri sorumlusu nezdinde söz konusu uygulamanın bulunduğu tek sunucuya zararlı bir yazılımın yüklendiğinin tespit edildiği,
- Veriye erişim/ulaşılabilirlik bakımından ihlalin etkisinin, sunucuda bulunan uygulamanın erişiminin gerektiği “xml” formatındaki bazı dosyalara ulaşılamaması sonucunda fonksiyonlarını yerine getirememesi olduğu,
- İhlalden etkilenen kişisel verilerin Kimlik Verisi (Ad-Soyad; Ticari Unvan, TCKN, Bağlı Olunan Vergi Dairesi), İletişim Verisi (Adres, E-Posta Adresi, Faks Numarası, Telefon Numarası), Müşteri İşlem Verisi (E-Faturanın Düzenlenme Tarihi ve Belge Numarası, Malın Nevi, Miktarı, Fiyatı ve Tutarı, Vergi Türü, Oranı ve Tutarı, Satılan Malların Teslim Tarihi ve İrsaliye Numarası, Fatura Tipi, Fatura Kayıt No. Ödeme Tarihi, Ödeme Şekli) olduğu,
- İhlalden etkilenen kişi sayısının 200 (1 müşteri ve 199 tedarikçi); kayıt sayısının ise 1187 olduğu,
- Fatura ilişkisi kapsamında hâlihazırda veri sorumlusunun veri kayıt sisteminde bulunan iletişim bilgileri vasıtasıyla ilgili kişilere bildirim en geç Kişisel Verileri Koruma Kuruluna ihlal bildirim yapıldığı tarihi takiben 3 (üç) iş günü içinde gerçekleştirileceği,

• **İhlal ile ilgili olan çalışanların son bir yıl içerisinde aldığı eğitimler hakkında;**

- ISO27001 uyumu ve sertifikası kapsamında bilgi güvenliği eğitimlerinin çalışanlar bakımından zorunlu eğitim statüsünde olduğu ve bu eğitimlerin her yıl güncel içerik ile tekrarlandığı,
- Ayrıca işe yeni giren çalışanlar bakımından da aynı eğitimlerin oryantasyon programları kapsamında verildiği,
- Veri sorumlusunun vermiş olduğu eğitimlerin, sunumların, katılım durumunu tevsik edici belgelerin ve log kayıtlarının münferit ekler olmak üzere veri ihlal bildirim formunun ekinde Kişisel Verileri Koruma Kurulunun bilgilerine sunulduğu,

• **İhlalden önce alınmış bulunan teknik tedbirler hususunda;**

- Ağ güvenliği ve uygulama güvenliği sağlandığı,
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemlerinin alındığı,
- Çalışanlar için yetki matrisi oluşturulduğu,
- Erişim loglarının düzenli olarak tutulduğu,
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin kaldırıldığı,
- Güncel anti-virüs sistemleri kullanıldığı,
- Güvenlik duvarlarının kullanıldığı,
- Kâğıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alındığı ve ilgili evrakın gizlilik dereceli belge formatında gönderildiği,
- Kişisel verilerin yedeklendiği ve yedeklenen kişisel verilerin güvenliğinin de sağlandığı,
- Kullanıcı hesap yönetimi ve yetki kontrol sisteminin uygulandığı ve bunların takibinin de yapıldığı,
- Mevcut risk ve tehditlerin belirlendiği,
- Her yıl sızma testi uygulandığı,
- Kullanıcı bilgisayarlarının USB'lerinin kapalı durumda olduğu, sadece özel üretim cihazlarında açık olduğu,
- Veri kaybı önleme yazılımlarının kullanıldığı,
- Saldırı tespit ve önleme sistemlerinin kullanıldığı,

• **İhlalden önce alınmış olan idari tedbirler ile ilgili olarak;**

- Çalışanlar için veri güvenliği hükümleri içeren disiplin hükümlerinin mevcut olduğu,
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlandığı ve uygulamaya başlandığı,
- Gizlilik taahhütnamele yapıldığı,
- Kişisel veri güvenliği politika ve prosedürlerinin belirlendiği,
- Kişisel veri güvenliği sorunlarının hızlı bir şekilde raporlandığı,
- Kişisel veri güvenliğinin takibinin yapıldığı,
- Kişisel verilerin mümkün olduğunca azaltıldığı,
- Kurum içi periyodik ve/veya rastgele denetimler yapıldığı ve yaptırıldığı,
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlendiği ve uygulandığı,

• **İhlalden sonra alınmış teknik tedbirler hakkında;**

- Zararlı yazılımın bulunduğu sunucunun host edildiği lokasyonun dış bağlantılara kapatıldığı,
- Adli bilişim yazılımları ile sistemin denetlendiği,
- Şirket dış bağlantıları kesilerek kontrollü olarak aktive edildiği,
- Sunucular üzerinde zararlı yazılımlar için forensik çalışması yapıldığı,
- Siber istihbarat verilerinin analiz edildiği,
- Gerçek zamanlı proses ve dosya hareketleri izlemeleri başlatıldığı,
- Kullanılan yedekleme sisteminin kontrollü bir lokasyona taşındığı,
- Veri sorumlusu bünyesinde daha önceden gerçekleşen ve kayıtları bulunan zararlı aktivitelerin detaylarının elde edilmesi sürecinin devam ettiği,
- Uç noktalarda (istemci ve sunucu) tehdit ve güvenlik zafiyeti avcılığına yönelik çalışmaların devam ettiği,
- Tehdit avcılığına yönelik kural tanımlarının yapılması işlemlerine devam edildiği,
- Uç nokta tespit ve müdahale aracının kurulması işlemlerinin devam ettiği,
- Uç nokta tespit ve müdahale aracına ait sensörlerin tüm uç noktalara dağıtılması işlemlerinin sürdüğü,
- Uç noktalardan verilerin sorunsuz gelmesi için gerekli konfigürasyonların düzenlemelerinin devam ettiği,

- İlk tespitlerde rastlanmamış olmasına karşın tekrardan hizmet temin edilen uzman firmadan alınan IOC bilgileri ve olaylara müdahale ekibi tarafından sağlanan kurallar aracılığıyla, sistemlerin ele geçirilmediğinin teyidinde devam edildiği,
- Ele geçtiği belirlenen uç noktalardan gerekli iz ve kayıtların toplanması sürecinin devam ettiği,
- Zararlı IP ve domainlerin belirlenmesi, sistem üzerindeki kalıcılık mekanizmalarının belirlenmesi, arka kapıların tespit edilmesi ve zararlı proseslerin tespit edilmesi işlemlerinin devam ettiği,

• **İhlalden sonra alınmış idari tedbirler hususunda;**

- Veri İhlali Müdahale Planı prosedürünün derhal olay özelinde uygulamaya alındığı,
- Yetkisiz erişim denemelerinin veri sorumlusunun bilgi teknolojileri birimi tarafından tespit edildiği an üst yönetime ve Şirket Kişisel Verilerin Korunması Komitesine ("Komite") raporlandığı,
- Komite ve üst yönetim tarafından derhal veri güvenliği ekibi kurulduğu,
- Veri ihlali yetkilisinin bu ekibe başkanlık etmek üzere atandığı,
- Siber güvenlik alanında uzman bir firma tarafından yetkilendirilen Siber Olaylara Müdahale Ekibinin, Veri Güvenliği Ekibine dâhil edildiği,
- Veri Sorumluları Sicili kaydına göre revize edilen politika, prosedür ve gizlilik taahhütlerinin güncel versiyonlarının çalışanlara iletildiği,
- Veri Sorumluları Sicili kaydına göre revize edilen politikaların güncel versiyonlarının internet sitesinde yayımlandığı

ifadelerine yer verilmiş; ihlal öncesi ve sonrası alınmış teknik ve idari tedbirlere ilişkin tevsik edici belgeler bildirim formunun ekinde Kurulun bilgilerine sunulmuştur.

Söz konusu bildirim incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 09.10.2020 tarih ve 2020/787 sayılı Kararı ile;

- İhlalin veri sorumlusunun tedbir eksikliğinden kaynaklanmayıp yaygın kullanılan bir uygulamadan kaynaklandığı; bu duruma veri sorumlusunun müdahale edemeyeceği,
- Veri sorumlusunun ihlali kısa zamanda fark etmiş olduğu,
- İhlalden etkilenen kişisel verilerin şahıs şirketi kaşelerinden ve kamuya açık kaynaklardan rahatlıkla elde edilebileceği,

- Veri sorumlusunun ihlalden etkilenen kişilere üç iş günü içerisinde bildirim gerçekleştireceğini belirttiği,
- İhlalin ilgili kişiler açısından olumsuz sonuçlar doğurma riskinin düşük olduğu,
- Veri sorumlusunun makul teknik ve idari tedbirleri almış olduğu

hususları dikkate alındığında, söz konusu ihlale ilişkin ilgili kişilere bildirim yapıldığını tevsik edici belgelerin Kuruma gönderilmesi suretiyle söz konusu veri ihlal bildirimini ile ilgili olarak Kanununun 12 nci maddesi kapsamında yapılacak ilave bir işlem bulunmadığına karar verilmiştir.

2020/769 sayılı KVKK Kararı

İlgili kişinin eski çalışanı olduğu şirketi devralan veri sorumlusu şirket tarafından kanuna aykırı veri işleme faaliyetinde bulunulması hakkında Kişisel Verileri Koruma Kurulunun 08/10/2020 tarihli ve 2020/769 sayılı Karar Özeti

Karar Tarihi : 08.10.2020

Karar No : 2020/769

Konu Özeti : İlgili kişinin eski çalışanı olduğu şirketi devralan veri sorumlusu şirket tarafından Kanuna aykırı veri işleme faaliyetinde bulunulması

İlgili kişinin Kuruma intikal eden şikayetinde özetle; eski çalışanı olduğu şirketin, başka bir şirkete bütün borç, ödev ve yükümlülükleri ile devrolduğu ancak kişisel verilerin elde edilmesi sırasında tarafına herhangi bir aydınlatma yapılmadığı, veri sorumlusu devralan şirketin internet sitesinde sunulan aydınlatma metninin açık ve belirli olmayan muğlak ifadeler içerdiği, şahsına ilişkin özlük dosyasında sağlık verilerinin de bulunduğu ve 6698 sayılı Kişisel Verilerin Korunması Kanununun 6 ncı (Kanun) maddesi uyarınca bu veri işleme faaliyeti için açık rızasının alınmadığı, öte yandan Kanunun 11 inci maddesi kapsamındaki haklarına ilişkin başvurusuna karşılık veri sorumlusunun cevabında yer alan kişisel verileri saklama sürelerine ilişkin 10 yıllık sürenin geçersiz olduğu ve İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği uyarınca 15 yıl saklanması gerektiği, ayrıca veri sorumlusu tarafından kendisine gönderilen ticari elektronik iletiler aracılığıyla herhangi bir hukuka uygunluk sebebi olmaksızın kişisel verilerinin işlendiği iddia edilerek veri sorumlusu hakkında gereğinin yapılması talep edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 08/10/2020 tarihli ve 2020/769 sayılı Kararı ile;

- Kanunun “*Kişisel Verilerin İşlenme Şartları*” başlıklı 5 inci maddesinin birinci fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, ikinci fıkrasında ise Kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan

doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Diğer taraftan, Kanunun “*Özel Nitelikli Kişisel Verilerin İşlenme Şartları*” başlıklı 6 ncı maddesinin birinci fıkrasında kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerinin özel nitelikli kişisel veri olduğunun belirtildiği, aynı maddenin ikinci fıkrasında özel nitelikli kişisel verilerin ilgilinin açık rızası olmaksızın işlenmesinin yasaklandığı, bununla birlikte üçüncü fıkrada da özel nitelikli kişisel verilerin açık rıza aranmadan işlenebileceği diğer haller sayıldığı, buna göre sağlık verilerinin ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından açık rıza aranmaksızın işlenebileceğinin belirtildiği, 4 üncü fıkrada ise özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şartının da getirildiği,

- İlgili kişinin kişisel verilerinin elde edilmesi sırasında tarafına herhangi bir aydınlatma yapılmadığı iddiasına ilişkin olarak veri sorumlusu tarafından verilen yanıtta veri sorumlusunun ilgili kişilerle hukuki ilişkilerinin sürmekte olduğu ve/veya doğrudan üçüncü taraflar vasıtasıyla temas etmekte olduğu faaliyetler bakımından 6698 sayılı Kanun uyarınca aydınlatma ve açık rıza alınmasına ilişkin yükümlülükler doğrultusunda uyumlaştırmaların gerçekleştirildiği ancak Şirketin aktif bir hukuki ilişki içerisinde olmadığı, ilgili mevzuatlar kapsamındaki saklama yükümlülükleri ile sınırlı olarak veri işleme faaliyeti gerçekleştirdiği eski çalışanlar bakımından aydınlatma yükümlülüğünün gerçekleştirilmesinin pratikte mümkün olmadığı belirtilmiştir,

- Veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen Kanunun 10 uncu maddesi uyarınca kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişinin, ilgili kişilere; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, kişisel veri toplamanın yöntemi ve hukuki sebebi, 11 inci maddede sayılan diğer hakları konusunda bilgi vermekle yükümlü olduğu, ilgili kişinin

şikayet başvurusu ve veri sorumlusunun cevabi yazısından anlaşıldığı üzere ilgili kişinin kişisel verilerinin 2014-2015 yıllarında işlendiği, 6698 sayılı Kişisel Verilerin Korunması Kanununun 07.04.2016 itibariyle yürürlüğe girdiği, bu çerçevede söz konusu tarihler itibariyle Kanunun yürürlüğe girmemiş olması sebebiyle kişisel verilerin elde edilmesi sırasında aydınlatma yükümlülüğünün yerine getirilmesinin de mümkün olmadığı sonucuna varıldığı,

- 4857 sayılı İş Kanununun 75 inci maddesinin “İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır.” hükmünü haiz olduğu,

- 5510 sayılı Sosyal Sigortalar Kanununun ‘Prim belgeleri ve işyeri kayıtları’ başlıklı 86 ncı maddesinde “İşveren, işyeri sahipleri; işyeri defter, kayıt ve belgelerini ilgili olduğu yılı takip eden yıl başından başlamak üzere on yıl süreyle, kamu idareleri otuz yıl süreyle, tasfiye ve iflâs idaresi memurları ise görevleri süresince, saklamak ve Kurumun denetim ve kontrol ile görevlendirilen memurlarınca istenilmesi halinde onbeş gün içinde ibraz etmek zorundadır.” şeklinde düzenlemenin yer aldığı,

- İşverenin çalışanlarının özlük dosyalarını düzenlemesi bakımından veri sorumlusu sıfatını haiz olduğu, bu kapsamda İş Kanunu ve Sosyal Sigortalar Kanunu kapsamındaki yükümlülükleri dolayısıyla veri işleme faaliyetinin gerçekleştirildiği, söz konusu veri işleme faaliyetinin Kanunun 5 inci maddesinin ikinci fıkrasının (a) bendinde yer alan ‘kanunlarda açıkça öngörülme’ ve aynı fıkranın (ç) bendinde yer alan ‘veri sorumlusunun hukuki yükümlülüğünün yerine getirilebilmesi için zorunlu olması’ şartlarına dayanılarak gerçekleştirildiği sonucuna varıldığı,

- İlgili kişinin açık rızası olmaksızın sağlık verilerinin işlenmesine ilişkin olarak;

- Çalışanlara ait sağlık verisi içeren kayıtların kişisel sağlık dosyalarında saklanmakta olduğu, kişisel sağlık dosyalarının yalnızca sır saklama yükümlülüğü altında bulunan iş yeri hekiminin erişimi ile sınırlı olarak saklanmakta olduğu ve Şirketin sistemlerinde kayıtlı olmadığı,

- İşyeri Hekimi ve Diğer Sağlık Personelinin Görev, Yetki, Sorumluluk ve Eğitimleri Hakkında Yönetmeliğin “İşyeri Hekiminin Yükümlülükleri” başlıklı 11 inci maddesinde “İşyeri hekimleri, bu Yönetmelikte belirtilen görevlerini yaparken, işin normal akışını mümkün olduğu kadar aksatmamak ve verimli bir çalışma ortamının sağlanmasına katkıda bulunmak, işverenin ve işyerinin meslek sırları, ekonomik ve ticari durumları hakkındaki bilgiler ile çalışanın kişisel sağlık dosyasındaki bilgileri gizli tutmakla yükümlüdürler.” hükmü uyarınca iş yeri hekimlerinin sır saklama yükümlülüğü altında bulunan kişilerden olduğu,

- Aynı Yönetmeliğin “İşyeri Hekimlerinin Görevleri” başlıklı 9 uncu maddesinin ikinci fıkrasının (c) bendinde yer aldığı üzere iş yeri hekiminin sağlık gözetimi kapsamında yapılacak işe giriş ve periyodik muayeneler ve tetkikler ile ilgili olarak çalışanları bilgilendirmek ve onların rızasını alma, çalışanların yapacakları işe uygun olduklarını belirten işe giriş ve periyodik sağlık muayenesi ile gerekli tetkiklerin sonuçlarını yönetmelik ekinde verilen örneğe uygun olarak düzenleme ve işyerinde muhafaza etme görevlerinin bulunduğu,
- Öte yandan Kanunun 6 ncı maddesinin üçüncü fıkrasında sağlık verilerinin ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından açık rıza aranmaksızın işlenebileceğinin düzenlendiği,
- Kanunun 6 ncı maddesinin dördüncü fıkrasında ise özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şartının bulunduğu, bu kapsamda “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler” ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 tarihli ve 2018/10 sayılı Kararı çerçevesinde yeterli önlemlerin belirlendiği

hususları dikkate alınarak Kurul tarafından özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemler alınmak suretiyle mevzuatta öngörülen görevleri kapsamında iş yeri hekimi tarafından sağlık verisinin işlenmesinin mümkün olduğu

değerlendirmelerinden hareketle

- Şikayet dilekçesi ve veri sorumlusunun cevaplarından ilgili kişinin kişisel verilerinin 2014-2015 yıllarında işlendiğinin anlaşıldığı, 6698 sayılı Kişisel Verilerin Korunması Kanununun 07.04.2016 itibarıyla yürürlüğe girdiği, bu çerçevede söz konusu tarihler itibarıyla Kanunun yürürlüğe girmemiş olması sebebiyle kişisel verilerin elde edilmesi sırasında aydınlatma yükümlülüğünün yerine getirilmesinin de mümkün olmadığı, dolayısıyla bu hususta Kanun kapsamında yapılacak bir işlem bulunmadığına,
- İşverenin çalışanlarının özlük dosyalarını düzenlemesi bakımından veri sorumlusu sıfatını haiz olduğu, bu kapsamda İş Kanunu ve Sosyal Sigortalar Kanunu kapsamındaki yükümlülükleri dolayısıyla veri işleme faaliyetinin gerçekleştirildiği, söz konusu veri işleme faaliyetinin Kanunun 5 inci maddesinin ikinci fıkrasının (a) bendinde yer alan ‘kanunlarda açıkça öngörülme’ ve aynı

fıkranın (ç) bendinde yer alan 'veri sorumlusunun hukuki yükümlülüğünün yerine getirilebilmesi için zorunlu olması' şartlarına dayanarak gerçekleştirildiğine,

- İlgili kişinin açık rızası olmaksızın sağlık verilerinin işlenmesine ilişkin olarak; İşyeri Hekimi ve Diğer Sağlık Personelinin Görev, Yetki, Sorumluluk ve Eğitimleri Hakkında Yönetmeliğin "İşyeri Hekiminin Yükümlülükleri" başlıklı 11 inci maddesi hükmü uyarınca iş yeri hekimlerinin sır saklama yükümlülüğü altında bulunan kişilerden olduğu, aynı Yönetmeliğin "İşyeri Hekimlerinin Görevleri" başlıklı 9 uncu maddesinin ikinci fıkrasının (c) bendinde yer aldığı üzere çalışanların yapacakları işe uygun olduklarını belirten işe giriş ve periyodik sağlık muayenesi ile gerekli tetkiklerin sonuçlarını yönetmelik ekinde verilen örneğe uygun olarak düzenleme ve işyerinde muhafaza etme görevlerinin bulunduğu, 6698 sayılı Kanununun 6 ncı maddesi uyarınca özel nitelikli kişisel veriler arasında sayılan sağlık verilerini içermesi sebebiyle gerek çalışan gerekse de eski çalışanlarına ait kişisel sağlık dosyalarının yalnızca sır saklama yükümlülüğü altında bulunan iş yeri hekiminin erişimi ile sınırlı olarak saklanmakta olduğunun beyan edildiği ve ilgili kişinin kişisel verilerinin güvenliğinin sağlanmadığına yönelik bir iddiası olmadığı hususları dikkate alınarak Kurul tarafından belirlenen özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemler alınmak suretiyle mevzuatta öngörülen görevleri kapsamında iş yeri hekimi tarafından sağlık verisinin işlenmesinin mümkün olduğuna,

- İlgili kişinin ticari elektronik ileti gönderilmek suretiyle kişisel verilerinin hukuka aykırı işlendiği iddiasına ilişkin olarak herhangi bir somut delile rastlanılmadığından bu aşamada Kurum tarafından yapılacak herhangi bir işlem bulunmadığına karar verilmiştir.

2020/766 sayılı KVKK Kararı

Bir Banka Tarafından Kurul Kararı ile Verilen Talimatların Gereğinin Yerine Getirilmemesi Hakkında Kişisel Verileri Koruma Kurulu'nun 08/10/2020 Tarihli ve 2020/766 Sayılı Karar Özeti

Karar Tarihi : 08.10.2020

Karar No : 2020/766

Konu Özeti : Bir banka tarafından Kurul Kararı ile verilen talimatların gereğinin yerine getirilmemesi hakkında

İlgili kişinin 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 11'inci maddesinde belirtilen hakları kapsamında yaptığı başvurusuna veri sorumlusu Banka tarafından verilen cevabı yetersiz bulduğuna; internet sayfasında aydınlatma metni yerine veri sorumlusunun Kişisel Verilerin İşlenmesi ve Korunması Politikasına link verdiğine, yirmi sayfalık söz konusu dokümanda ilgili kısımları bulabilmek için detaylı bir inceleme yapılması gerektiğine, aydınlatma yükümlülüğüne ilişkin Tebliğin birçok kuralına uyulmadığına, kişisel verilerin aktarıldığı kişiler listelenirken amaçlardan örnekler verildiğine ve bunlara benzer başka amaçların da olduğu izleniminin edinildiğine, kişisel verilerin işlenmelerindeki hukuki sebeplerden de bahsedilmediğine ilişkin Kişisel Verileri Koruma Kuruluna ilettiği şikayet dilekçesi ile ilgili olarak savunması alınan veri sorumlusu Bankaya *"aydınlatma metninde, gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandıran ifadeler kullanılması ve kişisel verilerin Kanunun 5 ve 6'ncı maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiğinin açıkça belirtilmemesi nedeniyle söz konusu metnin, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin 5'inci maddesinin birinci fıkrasının (g) ve (h) bentlerinde yer verilen hükümlere uygun olmadığı; söz konusu internet sitesinde yer alan aydınlatma metninin gözden geçirilerek "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ" in hükümlerine uygun hale getirilmesini teminen veri sorumlusu tarafından işlenen kişisel verilerin hangi kişisel veri işleme şartlarına dayanılarak işlendiğine ayrıntılı şekilde yer verilmesi, gizlilik politikası metninin aydınlatma yerine geçmeyeceği, aydınlatmanın kişisel verilerin elde edilmesi sırasında ve faaliyet bazlı olarak yerine getirilmesi gerektiği hususlarında gerekli düzenlemelerin yapılması"* gerektiği yönündeki talimatı içerir 06.02.2020 tarih ve 2020/98 sayılı Kurul

Kararı tebliğ edilmiş olup, tebliğ edilen Kurul kararı sonrası veri sorumlusundan alınan bilgi ve belgelerin birlikte incelenmesinden:

- Veri sorumlusu tarafından Kurul Kararı tebligatı sonrası Kuruma gönderilen cevap metni ekinde yer alan aydınlatma metni örneğinde, taraflarına Karar Tebligatı yapılmadan önce aydınlatma amacıyla kullandığı Gizlilik Politikası metninden farklı olarak yeni bir aydınlatma metni hazırlandığı, bu aydınlatma metninde “Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ”e uygun olarak hangi kişisel verilerin işlendiğine kategorik bazda ve ayrıntılı bir şekilde yer verildiği, kişisel verilerin hangi ortamlarda ve hangi şekilde elde edildiği, neden işlendiği, aktarıldığı, hangi hukuki gerekçelerle hangi kurum ve kişilere aktarım yapıldığı ve verilerin ne kadar süre ile işlenip, saklandığına ilişkin net, anlaşılır ifadelerle yer verilerek bilgi paylaşımında bulunulduğu,
- Ancak bahsi geçen aydınlatma metninde işlenen kişisel verilerin hangi kişisel veri işleme şartına dayanılarak işlendiğine dair Tebliğ hükümlerine uygun bir aydınlatma yapılmadığı,
- “Kişisel verilerinizi Hangi Hukuki Gerekçe ile İşliyoruz?” başlığı altında “6698 sayılı Kanun’un 5 ve 6’ncı maddeleri kapsamında, Bankamız tarafından kişisel verileriniz aşağıda belirtilen koşulların varlığı halinde işlenmektedir:

- Açık rızanızın bulunması,
- Kanunlarda veya yönetmelik, tebliğ, idari otorite kararı ve sair ikincil mevzuatta belirtilmiş hak veya yükümlülüklerimizin yerine getirilmesi,
- Bankamız ile akdettiğiniz sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla veri işlemenin gerekli olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- Temel hak ve özgürlüklerinize zarar vermemek kaydıyla Bankamızın meşru menfaati için veri işlemenin zorunlu olması.

Bununla birlikte, özel nitelikli kişisel verileriniz ancak açık rızanızın bulunması veya Bankamızın tabii olduğu kanunlarda açıkça öngörülmesi halinde işlenmektedir.” ifadelerine yer verildiği, veri sorumlusuna tebliğ edilen Karar’da açıkça “... veri sorumlusu tarafından işlenen kişisel verilerin hangi kişisel veri işleme şartlarına dayanarak işlediklerine ilişkin ayrıntılı şekilde yer verilmesi, ...” talimatı yer aldığı halde veri sorumlusu tarafından hazırlanan aydınlatma metninin bu husus kapsamında Tebliğ’e uygun olmadığı,

- Ayrıca veri sorumlusu tarafından Kuruma iletilen cevap metninde Kararda yer alan “... aydınlatmanın kişisel verilerin elde edilmesi sırasında ve faaliyet bazlı olarak yerine getirilmesi gerektiği...”

talimatına ilişkin herhangi bir ifadeye ve tevsik edici belgeye yer verilmediği görülmüş olup internet sayfasında yapılan incelemede kredi kartı başvurusu yapılmak istenildiğinde “HEMEN BAŞVUR” butonu seçildiğinde yönlendirilen sayfada “*Kişisel Verilerin Korunması Kanunu kapsamında hazırlanan Aydınlatma Metni’ni okudum.*” ifadesinin yer aldığı, aydınlatma metni linki seçildiğinde ise ekranda beliren aydınlatma metninin veri sorumlusunun anasayfasında “*Kişisel Verilerin Korunması*” başlığı altında yer alan aydınlatma metninden farklı olduğu görülmekle birlikte bahsi geçen aydınlatma metninin de kredi kartı başvurusuna özgü, sadece o işlem kapsamında işlenen kişisel verilere (kategorik olarak), işleme amaçlarına ve işlemenin dayandığı hukuki sebep ve diğer unsurlara yer verilmediği aksine genel nitelikli bir aydınlatma metni olduğu, bu aydınlatma metninde de Bankanın ana sayfasında yer alan aydınlatma metni gibi veri sorumlusu tarafından işlenen kişisel verilerin hangi kişisel veri işleme şartına dayanılarak işlendiğine ayrıntılı bir şekilde yer verilmemesi dolayısıyla Tebliğin “Usul ve esaslar” başlıklı 5’inci maddesinin (1) numaralı fıkrasının (h) bendinde yer alan hükme aykırı olduğu,

- Ayrıca veri sorumlusunun internet sayfasında konut kredisi başvurusu yapılmak istenildiğinde ise kredi kartı başvurusunda olduğu gibi bir uygulama ile karşılaşılmayıp yönlendirilen ilk sayfada sağ üst köşede “Gizlilik” butonunun yer aldığı, bu buton seçildiği takdirde “Gizlilik Politikası” sayfasına yönlendirildiği, “*Kişisel Verilerin İşlenmesine İlişkin Aydınlatma Metni*” sekmesine girildiğinde ise Kurul Kararı ardından Kurumumuza gönderilen güncellenmiş olan ve ana web sayfasında yer alan aydınlatma metni ile karşılaşıldığı, dolayısıyla konut kredisi başvurusu için bu başvuruya özgü, sadece o işlem kapsamında işlenen kişisel verilere (kategorik olarak), işleme amaçlarına ve işlemenin dayandığı hukuki sebep ve diğer unsurlara yer verilmediği aksine genel nitelikli bir aydınlatma metni ile aydınlatma yapıldığı

tespit edilmiş olup, mevcut durum 6698 sayılı *Kişisel Verilerin Korunması Kanunu ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ* hükümleri çerçevesinde değerlendirildiğinde;

- Veri sorumlusunun aydınlatma metninde *Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ* hükümlerine uygun olarak kişisel verilerin hangi kişisel veri işleme şartına dayanılarak işlendiğine ilişkin ayrıntılı bilgiye yer verilmediği, yalnızca Kanunun 5’inci ve 6’ncı maddelerinin ilgili fıkra ve bentlerine yer verilmesiyle yetinildiği,

- Aydınlatmanın kişisel verilerin elde edilmesi sırasında ve faaliyet bazlı olarak yerine getirilmesi gerektiği talimatına ilişkin olarak cevap yazısı ile ekinde herhangi bir ifadeye ve tevsik edici belgeye yer verilmediği ve ayrıca veri sorumlusunun internet sayfasında çeşitli bankacılık ürünlerine başvuru

yapılması sırasında o faaliyete özgü hazırlanmamış genel bir aydınlatma metnine yer verildiği ve bu metnin de Tebliğe uygun hazırlanmadığı

dikkate alındığında veri sorumlusu tarafından yayımlanan aydınlatma metninin Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerine uygun olarak düzenlenmediği, bu çerçevede Kurul Kararı ile verilen talimatın yerine getirilmeyerek veri sorumlusu tarafından Kanunun 15'inci maddesinin (5) numaralı fıkrasına aykırı hareket edildiği kanaatine varıldığından, Kanunun 18'inci maddesinin (1) numaralı fıkrasının (c) bendi uyarınca veri sorumlusu hakkında 120.000 TL idari para cezası uygulanmasına karar verilmiştir.

2020/765 sayılı KVKK Kararı

Bir Banka Tarafından Kurul Kararı ile Verilen Talimatın Gereğinin Yerine Getirilmemesi Hakkında Kişisel Verileri Koruma Kurulu'nun 08/10/2020 Tarihli ve 2020/765 Sayılı Karar Özeti

Karar Tarihi : 08.10.2020

Karar No : 2020/765

Konu Özeti : Bir banka tarafından Kurul kararı ile verilen talimatın gereğinin yerine getirilmemesi hakkında

İlgili kişinin 6698 sayılı Kişisel Verilerin Korunması Kanununun 11'inci maddesinde belirtilen hakları kapsamında veri sorumlusu Banka'ya yaptığı başvuruya Kanun'da düzenlenen otuz günlük süre içerisinde cevap verilmediği ve Bankanın internet sayfasında yayımlanan aydınlatma metninin de Kurum tarafından yayımlanan tebliğe uygun olmadığı, metinde kişisel verilerin işlenmesindeki sebeplerin belirtilmediği, ayrıca kişisel verilerin işleme amaçları için genel ifadeler kullanıldığına ilişkin Kişisel Verileri Koruma Kuruluna ilettiği şikayet dilekçesi ile ilgili olarak savunması alınan veri sorumlusu Bankaya "internet sayfasında yer alan Kişisel Verilerin Korunması Kişisel Verileriniz Koruma Altında!" başlıklı metnin Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerine uygun hazırlanmaması nedeniyle gözden geçirilmesi ve Tebliğ hükümlerine uygun hale getirilmesini teminen kişisel verilerin hangi kişisel veri işleme şartlarına dayanılarak işlendiğine metinde ayrıntılı şekilde yer verilmesi, bahse konu metnin aydınlatma yerine geçmeyeceği, aydınlatmanın kişisel verilerin elde edilmesi sırasında ve faaliyet bazlı olarak yerine getirilmesi gerektiği hususlarında gerekli düzenlemelerin yapılması" gerektiği yönündeki talimatı içerir 06.02.2020 tarih ve 2020/100 sayılı Kurul Kararı tebliğ edilmiş olup, bu çerçevede veri sorumlusundan alınan bilgi ve belgelerin birlikte incelenmesinden:

- Veri sorumlusu tarafından aydınlatma metnine, işlenen kişisel verilerin işleme amaçları ile ilgili olarak "Bankamızdan alacağınız ürün ve hizmetler nedeni ile kuracağınız ilişki çerçevesinde; Kişisel verileriniz aşağıda belirtilen hukuki sebeplere dayalı olarak işlenmektedir. Kanun'un: 5/2 (a) maddesinde düzenlenen kanunlarda açıkça öngörülmesi; 5/2 (c) maddesinde düzenlenen Bankamızla imzalanan sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin

gerekli olması; 5/2 (ç) maddesinde düzenlenen Bankamızın hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; 5/2 (e) maddesinde düzenlenen bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması; 5/2 (f) maddesinde düzenlenen sizlerin temel hak ve özgürlüklerinize zarar vermemek kaydıyla Bankamızın meşru menfaatleri için veri işlenmesinin zorunlu olması; son olarak özel nitelikli kişisel verileriniz ise; de 6/2 maddesine göre ancak açık rızanızla işlenebilmektedir.” şeklindeki paragrafın eklendiği,

- Aydınlatma metninde veri sorumlusu tarafından işlenen kişisel verilere (kategorik olarak) ayrıca yer verilmediği gibi metinde kişisel verilerin hangi kişisel veri işleme şartına dayanılarak işlendiğine ilişkin de ayrıntılı bir düzenleme yapılmadığı; yalnızca Kanunun 5’inci maddesinin (2) numaralı fıkrasının (a), (c), (ç), (e) ve (f) bentleri ile Kanunun 6’ncı maddesinin (2) numaralı fıkrasındaki hükümlerin sıralandığı,

- Aydınlatma metninde işleme amaçlarında bazı eklemeler yapılması ve başvuru sahiplerinin veri sorumlusuna başvurularını iletme yollarının yeniden düzenlenmesi dışında genel itibariyle aydınlatma metninin Tebliğe uygun hale getirilmesi amacıyla talimatta yer verilen ilgili değişikliklerin yapılmadığı,

- Ayrıca veri sorumlusu tarafından savunma metninde; 5411 sayılı Bankacılık Kanununda belirlenmiş olan ve Bankacılık Düzenleme ve Denetleme Kurumu tarafından ayrıca izin alınmış olan faaliyetleri de kapsayacak şekilde kişisel verilerin işleme amacını belirten tek bir aydınlatma metni ile ilgili kişilerin, kişisel verilerin elde edilmesi anında bilgilendirildiği ancak Bankanın yürüttüğü sosyal sorumluluk projeleri ve kurumsal marka çalışmaları ile reklam faaliyetleri gibi diğer faaliyetlerinde ise müşterileri dışındaki gerçek kişiler hakkında gerçekleştirdiği veri işleme faaliyetlerinde özel ve ayrı aydınlatma metinleri kullanıldığı ifadelerine yer verilmekle birlikte bu hususta Kuruma tevsik edici herhangi bir belge sunulmadığı,

- Bu kapsamda ilgili Karardaki “... aydınlatmanın kişisel verilerin elde edilmesi sırasında ve faaliyet bazlı olarak yerine getirilmesi gerektiği...” talimatına ilişkin olarak veri sorumlusunun internet sayfasında kredi kartı başvurusu yapılmak istenildiğinde “*Kişisel verilerimin neden ve nerelerden toplandığı, nasıl kullanıldığı ve diğer haklarımla ilgili olarak Kişisel Verilerin Korunması Kanunu uyarınca yapılan bilgilendirmeyi okudum.*” ifadesinin yer aldığı ve bilgilendirme linkinin seçilmesi halinde ise yönlendirilen sayfada “*Kişisel Verilerin Korunması*” başlıklı bir aydınlatma metninin yer aldığı, söz konusu aydınlatma metninin Bankanın anasayfasında Gizlilik Politikası sekmesi altında da yer alan genel aydınlatma metni olduğu ve “*Kredi Kartı Başvurusu*” sırasında gerçekleştirilen işleme faaliyetine özgülenmemiş, genel nitelikli bir aydınlatma metni olduğu,

- Ek olarak “İhtiyaç Kredisi Başvurusu” nda bulunulduğunda da yine aynı genel aydınlatma metni ile karşılaşılmış olup, kredi kartı başvurusu ve ihtiyaç kredisi başvurusu sırasında bu başvurulara özgü, sadece o işlem kapsamında işlenen kişisel verilerin işleme amaçlarına ve işlemenin dayandığı hukuki sebep ve diğer unsurlarına yer verilmeyen aksine genel nitelikli bir metin ile aydınlatma yapıldığı,

- Söz konusu aydınlatma metinlerinde de veri sorumlusu tarafından işlenen kişisel verilerin hangi kişisel veri işleme şartına dayanılarak işlendiğine ilişkin ayrıntılı bilgiye yer verilmemesi dolayısıyla Tebliğin “Usul ve esaslar” başlıklı 5’inci maddesinin (1) numaralı fıkrasının (h) bendinde yer alan hükme aykırılığın söz konusu olduğu

değerlendirilmiş olup, mevcut durum 6698 sayılı Kişisel Verilerin Korunması Kanunu ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümleri çerçevesinde değerlendirildiğinde;

- Veri sorumlusunun aydınlatma metninde Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerine uygun olarak kişisel verilerin hangi kişisel veri işleme şartına dayanılarak işlendiğine ilişkin ayrıntılı bilgiye yer verilmediği, yalnızca Kanunun 5’inci ve 6’ncı maddelerinin ilgili fıkra ve bentlerine yer verilmesiyle yetinildiği,

- Aydınlatmanın kişisel verilerin elde edilmesi sırasında ve faaliyet bazlı olarak yerine getirilmesi gerektiği talimatına ilişkin olarak tevsik edici belge sunulmamakla birlikte veri sorumlusunun savunma yazısında; kişisel verilerin işleme amacını belirten tek bir aydınlatma metni ile ilgili kişilerin kişisel verilerin elde edilmesi anında bilgilendirildiği ve veri sorumlusunun müşterileri dışındaki gerçek kişiler hakkında gerçekleştirdiği veri işleme faaliyetlerinde ise özel ve ayrı aydınlatma metinleri kullanıldığı ifadelerine yer verilmekle birlikte web sayfasında farklı bankacılık ürünlerine başvuru yapılması sırasında o faaliyete özgü hazırlanmamış genel bir aydınlatma metnine yer verildiği ve bu aydınlatma metninin de Tebliğe uygun olmadığı

dikkate alındığında veri sorumlusu tarafından yayımlanan aydınlatma metninin Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerine uygun olarak düzenlenmediği ve Kurul Kararı ile verilen talimatın yerine getirilmeyerek Banka tarafından Kanunun 15’inci maddesinin (5) numaralı fıkrasına aykırı hareket edildiği kanaatine varıldığından, veri sorumlusu hakkında Kanunun 18’inci maddesinin (1) numaralı fıkrasının (c) bendi uyarınca 120.000 TL idari para cezası uygulanmasına karar verilmiştir.

2020/763 sayılı KVKK Kararı

İnternette market alışveriş hizmeti veren veri sorumlusunun veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 01.10.2020 tarih ve 2020/763 sayılı Karar Özeti

Karar Tarihi : 01.10.2020

Karar No : 2020/763

Konu Özeti : İnternette market alışveriş hizmeti veren veri sorumlusunun veri ihlal bildirimini hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- 400 kişilik bir alıcı grubuna e-posta gönderimi yapılması sırasında alıcı e-posta adreslerinin gizliliğinin korunması amacıyla tüm alıcıların ilgili toplu e-postanın BCC kısmına eklendiği,
- Söz konusu işlem sırasında, e-posta gönderimini yapan çalışan tarafından e-postanın konu kısmına hataen 43 müşteriye ait e-posta adresinin eklendiği, bu nedenle, e-postanın konu kısmında e-posta adresi yer alan 43 alıcı bilgisinin, e-posta gönderimi yapılan 400 kişilik alıcı grubu ile paylaşıldığı,
- Söz konusu e-posta gönderimi yapılır yapılmaz, mailin hataen yukarıda belirtilen şekilde iletilmesinin çalışan tarafından tespit edildiği ve ivedi aksiyon alınması için Teknoloji Departmanından sorumlu kişilerle iletişime geçildiği, ancak e-postanın geri alınmasının mümkün olmayacağını öğrenildiği,
- İhlalden müşterilere ait e-posta adresi bilgilerinin etkilendiği, e-posta adreslerinin kişinin adı-soyadını da içerebildiği, bu nedenle ihlalden kimlik ve iletişim verilerinin etkilendiği,
- 43 ilgili kişinin söz konusu paylaşım hakkında bilgilendirildiği ve ilgili kişilerin ihlalden etkilenme düzeylerinin minimize edilmesinin sağlandığı,
- İhlin gerçekleşmesini takiben en kısa süre içerisinde (48 saat içerisinde) ilgili kişiler ile doğrudan e-posta adresleri üzerinden iletişime geçilerek 29.09.2020 tarihinde bildirim yapıldığı ifadelerine yer verilmiştir.

Söz konusu bildirim incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 01.10.2020 tarih ve 2020/763 sayılı Kararı ile;

- İhlalden 43 ilgili kişinin etkilenmiş olması,
- İhlalden etkilenen kişisel verilerin sadece müşterilere ait e-posta ve e-posta adreslerinin içerisinde geçen ad-soyad bilgilerinin olması,
- İlgili kişilere ihlale ilişkin 29.09.2020 tarihinde bildirimde bulunulmuş olması ve tevsik edici belgelerin Kurumumuza iletilmiş olması,
- İhlalden etkilenen ilgili kişiler üzerinde ihlalin olumsuz sonuç doğurma riskinin düşük olması,
- Hatalı e-posta gönderimi yapılan 400 müşteriden ihlale konu e-postanın imha edilmesinin talep edilmiş olması,
- Veri sorumlusunun “en kısa sürede” (24.01.2019 tarih ve 2019/10 sayılı Kurul kararında belirtilen 72 saatlik süre içerisinde) Kurumumuza veri ihlalinin bildirme yükümlülüğünü yerine getirmiş olması hususları dikkate alındığında bu aşamada veri sorumlusu hakkında Kanunun 12 nci maddesi kapsamında yapılacak bir işlem olmadığına karar verilmiştir.

2020/755 sayılı KVKK Kararı

İlgili kişinin aidat borcu bilgisinin site yönetimi tarafından ev sahibine iletilmesi hakkında Kişisel Verileri Koruma Kurulunun 29/09/2020 tarihli ve 2020/755 sayılı Karar Özeti

Karar Tarihi : 29.09.2020

Karar No : 2020/755

Konu Özeti : İlgili kişinin aidat borcu bilgisinin site yönetimi tarafından ev sahibine iletilmesi

İlgili kişi tarafından Kuruma intikal ettirilen şikâyet dilekçesinde özetle; kendisine ev sahibinden, aidatının bazı aylarda eksik, bazı aylarda ise hiç yatırılmadığına dair bir SMS iletildiği, bu SMS iletimi hadisesinin kendisine ait kişisel verilerin hukuka aykırı olarak işlendiğini ortaya koyduğu; ilgili kişinin, kişisel verilerinin site yönetimi tarafından ev sahibi ile paylaşılmasında hiçbir bilgisi ve rızasının bulunmadığı, bu doğrultuda veri sorumlusu site yönetimine başvurmak suretiyle 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 11 inci maddesinde gösterilen haklarını kullandığı ve işlenen/aktarılan kişisel verileri ile ilgili olarak tarafına bir aydınlatma yapıp yapılmadığı hususlarında bilgi talep ettiği, site yönetiminin ise verdiği yanıtta, ilgili kişinin aidat ödeme bilgilerinin ev sahibinin talebi doğrultusunda paylaşıldığının belirtildiği fakat ilgili kişiye aydınlatma yapıldığına veya kendisinden bu hususta açık rıza alındığına dair bir belge yahut herhangi bir hukuka uygunluk sebebinin de sunulmadığı belirtilerek veri sorumlusu site yönetimi hakkında idarî para cezası uygulanması talep edilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulunun 29/09/2020 tarihli ve 2020/755 sayılı Kararı ile;

- Kanunun “Kişisel verilerin işleme şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,

ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması artlarından birinin varlığı halinde ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerine yer verildiği,

- Öte yandan, 634 sayılı Kat Mülkiyeti Kanununun “Ortak Giderlerin Teminatı” başlığını hâiz 22 nci maddesinin, “*Kat malikinin, 20’nci madde uyarınca payına düşecek gider ve avans borcundan ve gecikme tazminatından, bağımsız bölümlerin birinde kira akdine, oturma (sükna) hakkına veya başka bir sebebe dayanarak devamlı bir şekilde faydalananlar da müştereken ve müteselsilen sorumludur. Ancak, kiracının sorumluluğu ödemekle yükümlü olduğu kira miktarı ile sınırlı olup, yaptığı ödeme kira borcundan düşülür...*” hükmünü amir olduğu,

- Söz konusu hüküm uyarınca ev sahibi ile kiracının ortak giderler ve gecikme tazminatından müştereken ve müteselsilen sorumlu olduğu dikkate alındığında, ev sahibinin, kiracısının oturduğu dairenin aidat gibi apartmanın ortak giderlerinden payına düşen kısımlarını ödeyip ödemediğinden haberdar olmasında gerek ev sahibi gerek site yönetiminin menfaati bulunduğu, dolayısıyla söz konusu veri işleme faaliyetinin; 6698 sayılı Kanunun 5 inci maddesinin (2) numaralı fıkrasının (e) bendi kapsamında *bir hakkın tesisi, kullanılması veya korunması* çerçevesinde gerçekleştirildiği,

- Bu itibarla veri sorumlusunun ilgili kişiye verdiği cevapta da ev sahibinin isteği üzerine ilgili kişinin borç bilgilerinin ev sahibi ile paylaşıldığının ifade edildiği dikkate alındığında ilgili kişiye veri sorumlusu tarafından verilen yanıtın, ilgili kişinin iddialarına konu hususları yeterli derecede açıklayıcı olduğu

değerlendirmelerinden hareketle;

- İlgili kişinin kişisel verisi niteliğinde olan aidat borç bilgilerinin, veri sorumlusu tarafından ev sahibinin isteği üzerine paylaşıldığı, bu paylaşımın 634 sayılı Kat Mülkiyeti Kanununun 22 nci maddesinde yer alan hüküm uyarınca gerçekleştirildiği dikkate alınarak, veri sorumlusu site yönetimi tarafından ilgili kişiye iletilen cevap metninde yer verilen açıklamaların ilgili kişinin iddiasına konu hususları açıklayıcı nitelikte olduğuna, bu çerçevede, söz konusu şikâyet hakkında Kanun kapsamında yapılacak bir işlem bulunmadığına karar verilmiştir.

2020/746 sayılı KVKK Kararı

İlgili kişinin veri sorumlusu ile abonelik sözleşmesi kurma amacıyla gerçekleştirdiği telefon görüşmesi kayıtlarına erişim talebi hakkında Kişisel Verileri Koruma Kurulunun 29/09/2020 tarihli ve 2020/746 sayılı Karar Özeti

Karar Tarihi : 29.09.2020

Karar No : 2020/746

Konu Özeti : İlgili kişinin veri sorumlusu ile abonelik sözleşmesi kurma amacıyla gerçekleştirdiği telefon görüşmesi kayıtlarına erişim talebi

Kuruma intikal ettirilen şikâyette özetle, hizmet alımı esnasında yaşadığı ihtilaf nedeniyle ilgili kişinin veri sorumlusuna ait kayıtlı elektronik posta (KEP) adresi üzerinden veri sorumlusu ile yapılan görüşmeye ait ses kayıtlarının talebine ilişkin başvuru gerçekleştirdiği, 25.08.2011 tarihli ve 28036 sayılı Resmi Gazetede yayımlanan Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 12 nci maddesinin ikinci fıkrası uyarınca iletinin okunduğunun kabul edildiği tarihten itibaren otuz gün içerisinde kendisine cevap verilmediği, bunun üzerine müşteri hizmetleri ile görüştüğü, görüşmede sözleşmenin (ses kayıtlarının) bir örneğinin tarafına verilmesi gerektiği ancak verilmediğini, bu verilerin ilgili kişiye ait kişisel veriler olduğunu, veri sorumlusunun hangi tarihte kaç kere aradığına dair kayıtlarının da tutulduğunu, ayrıca, bunların da kişisel veri niteliği taşıdığını, bu verileri bilmeye hakkı olduğunu belirterek bu sebeple, tarafına iletilmesini talep ettiği ancak verilmediği, müşteri hizmetleri ile yapılan görüşmede Cumhuriyet Savcılığına başvurulması gerektiği ve söz konusu kişisel verilerin kendisine verilemeyeceğinin belirtildiği ifade edilerek, konunun 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında incelenmesi talep edilmiştir.

Başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişinin başvurusunu yaptığı KEP adresinin kişisel verilere ilişkin başvuruların yapılması amacıyla tahsis edilmiş bir KEP adresi olmadığı, kişisel verilerle ilgili talep ve soruların ana ortaklığın

KEP adresine veya kendilerine ait <https://www.....net/tr/gizlilik-ve-guvenlik> linkinden iletilebileceği,

- Veri sorumlusu ve ilgili kişi arasında abonelik sözleşmesi kurulduğu, ilgili kişiye ait kişisel verilerin abonelik sözleşmesinin kurulmasıyla elde edildiği, abonelere ait kişisel verilerin abonelik ilişkisinin yanı sıra sunulan hizmetler kapsamında abonelik sözleşmesi, bayiler ve sair yüz yüze kanallar, çağrı merkezi, web sitesi, mobil uygulamalar, kısa mesaj, elektronik posta, sesli yanıt sistemi kanallarıyla elde edildiği,

- İlgili kişiye ait kişisel verilerin Kanunun 5 inci maddesinin ikinci fıkrasının (c) bendi kapsamında işlendiği,

- Müşteri Hizmetleri ile abonelerin yapmış olduğu görüşmelerin ses kayıtlarının müşterilere iletilmesi durumunda müşteriler tarafından farklı amaçlarla kullanıldığı, sosyal medyada yayımlandığı, soruşturmalar kapsamında ve adli makamlara üzerinde tahrifat yapılarak iletilmesi gibi güvenlik risklerinin oluşabileceği, müşteri hizmetleri ile yapılan görüşmelerin ses kayıtlarının görüşmeyi gerçekleştiren müşteri hizmetleri çalışanının da kişisel verileri içerdiği düşünüldüğünde söz konusu kayıtların ilgili kişilere iletilmesinin bu kişilerin hakkını da zedeleyebilecek ve bu kişiyi ifşa edebilecek şekilde kullanılması riskini de doğuracağı değerlendirildiği,

- Somut olayda ilgili kişinin müşteri hizmetleri ile gerçekleştirdiği görüşmeleri yanlış anlaması nedeniyle bir kampanyaya taahhüt vererek sözleşmenin kurulmuş olduğunu zannettiği ancak, esasen kurulmadığının kendisine daha sonra yapılan görüşmelerde izah edildiği, sonuç olarak aradaki yanlış anlamanın giderilerek ilgili kişinin veri sorumlusunca sunulan ... Kampanyası'na kendi isteği ile tekrar taahhüt verdiği ve hâlihazırda hizmet almaya devam ettiği,

- Veri sorumlusunun Kanun gereğince uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü idari ve teknik tedbiri alma yükümlülüğünün bulunduğu, bununla birlikte, veri sorumlusunun yükümlülüklerine uygun olarak ticari faaliyetlerini devam ettirme yönündeki genel prensibi uyarınca müşteri hizmetleri ile abonelerin yapmış olduğu görüşmelerin (ses kayıtları) sadece yetkili adli ve idari merciler tarafından yöneltilen yasal talepler çerçevesinde yetkili merciler ile paylaşıldığı

ifade edilmiştir.

Söz konusu iddiaların incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 29/09/2020 tarih ve 2020/746 sayılı Kararında;

- Kişisel verilerin işleme şartlarının düzenlendiği Kanunun 5 inci maddesinin (1) numaralı fıkrasında; kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin, (2) numaralı

fıkrasında ise kişisel verilerin kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işleniminin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğunun hükme bağlandığı,

- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunun "Amaç ve Kapsam" başlıklı 1 inci maddesinin ikinci fıkrasında elektronik iletişim araçlarıyla yapılan sözleşmelerin 6563 sayılı Kanun kapsamında olduğunun ifade edildiği, Avrupa Birliği Elektronik Ticaret Direktifi'nde olduğu gibi 6563 sayılı Kanunda da elektronik sözleşmenin tanımının yapılmadığı, ancak, "Tanımlar" başlıklı 2 nci maddesinin birinci fıkrasının (c) bendinde, ticari elektronik iletinin, "*Telefon, çağrı merkezleri, faks, otomatik arama makineleri, akıllı ses kaydedici sistemler, elektronik posta, kısa mesaj hizmeti gibi vasıtalar kullanılarak elektronik ortamda gerçekleştirilen ve ticari amaçlarla gönderilen veri, ses ve görüntü içerikli iletileri*" kapsadığı, bu doğrultuda, 6563 sayılı Kanunun 2 nci maddesinde yer alan ticarî elektronik ileti tanımından hareketle, telefon aracılığıyla yapılan sözleşmelerin 6563 sayılı Kanun kapsamında elektronik sözleşme olarak kabul edildiğinin anlaşıldığı, dolayısıyla, veri sorumlusu ve ilgili kişinin telefon aracılığıyla sözleşme kurmaya yönelik yaptıkları görüşmede Kanunun 5 inci maddesinin (2) numaralı fıkrasının (c) bendinde yer alan hüküm çerçevesinde kişisel verilerin işlenebileceği,

- 2010 yılında 5982 sayılı Kanunla Anayasanın 20 nci maddesine eklenen fıkra ile herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkının anayasal bir hak olarak teminat altına alındığı, bu bağlamda, kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkı hükme bağlanırken, kişisel verilerin korunmasına ilişkin usul ve esasların kanunla düzenleneceği,

- Diğer taraftan, Kanunun "İlgili Kişinin Hakları" başlıklı 11 inci maddesinde,

"(1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

a) Kişisel veri işlenip işlenmediğini öğrenme,

b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

- c) Kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
- e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
- f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir." hükümlerine yer verildiği,

- Bu doğrultuda, Kanunun "İlgili Kişinin Hakları" başlıklı 11 inci maddesinin birinci fıkrasının (b) bendi hükmü kapsamında ilgili kişinin, kendisiyle ilgili kişisel veriler işlenmişse buna ilişkin bilgi talep etme hakkını, söz konusu veriye erişim hakkını da kapsadığı ve erişim hakkının, bilgi talep etme hakkını tamamlayarak ilgili kişinin, kişisel verileri üzerindeki haklarını kullanabilmesi için, kişisel verilerinin ne şekilde işlendiğine dair tam olarak bilgi sahibi olmasına imkân sağlaması gerektiği,
- Ancak bu hakkın, veri sorumlusunun veri güvenliğine ilişkin yükümlülüklerinin de dikkate alınması suretiyle, işlenen kişisel verilerin, teknik/fiziki imkânların el verdiği ölçüde ve verinin muhtevasına/içeriğine makul bir şekilde ulaşılabilmesine imkân tanınarak kullanılması gerektiği,
- İlgili kişinin erişim hakkı ile veri sorumlusunun konuşma kayıtlarının kaydedildiği kayıt ortamının kendisinin ancak yasal makamlar tarafından talep edildiği takdirde teslim edilebileceği yönündeki makul kabul edilebilecek açıklaması arasındaki dengenin talep edilen ses kayıtlarına ilişkin kayıt ortamlarının doğrudan ilgili kişiye teslim edilmeden dökümlerine erişim hakkı sağlanarak gerçekleştirilebileceği,
- Diğer taraftan, Kanunun "Veri Sorumlusuna Başvuru" başlıklı 13 üncü maddesinin ikinci fıkrası gereğince, veri sorumlusunun ilgili kişinin başvurusunda yer alan talepleri, talebin niteliğine göre ve en geç otuz gün içerisinde sonuçlandırması gerektiği, öte yandan, Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğin (Tebliğ) 5 inci maddesinin (1) numaralı fıkrasında, "İlgili kişi, Kanunun 11 inci maddesinde belirtilen hakları kapsamında taleplerini, yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletir." hükmüne yer verildiği, ayrıca, Tebliğin 6 ncı maddesinin (2) numaralı fıkrasında, veri sorumlusunun başvuru

kabul edeceği ya da gerekçesini açıklayarak reddedeceği, üçüncü fıkrasında ise, cevabın ilgili kişiye yazılı olarak veya elektronik ortamda bildirileceği

değerlendirmelerinden hareketle;

- Kanunun 11 inci maddesinin (1) numaralı fıkrasının (b) bendi hükmü kapsamında ilgili kişinin, kendisiyle ilgili kişisel veriler işlenmişse buna ilişkin bilgi talep etme hakkının, söz konusu veriye erişim hakkını da kapsadığına ve erişim hakkının, bilgi talep etme hakkını tamamlayarak ilgili kişinin, kişisel verileri üzerindeki haklarını kullanabilmesi için, kişisel verilerinin ne şekilde işlendiğine dair tam olarak bilgi sahibi olmasına imkân sağladığı dikkate alındığında söz konusu dökümün, ilgili kişi dışında başkalarının kişisel verileri varsa bunlar çıkarılmak veya maskelenmek gibi önlemler alınarak ilgili kişiye gönderilmesi yönünde veri sorumlusunun talimatlandırılmasına,
- İlgili kişilerin Kanun kapsamındaki başvurularına Kanunun ilgili hükümleri ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ hükümleri uyarınca süresi içinde bir cevap verilmesi yönünde veri sorumlusunun talimatlandırılmasına,
- İlgili kişilerin Kanun kapsamındaki başvurularını ana ortaklığın KEP adresi yerine veri sorumlusuna ait KEP adresi üzerinden iletebilmeleri için kendi bünyesinde gerekli düzenlemeleri yapması yönünde veri sorumlusunun talimatlandırılmasına,

karar verilmiştir.

2020/744 sayılı KVKK Kararı

Bir Bankanın veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 29.09.2020 tarih ve 2020/744 sayılı Karar Özeti

Karar Tarihi : 29.09.2020

Karar No : 2020/744

Konu Özeti : Bir bankanın veri ihlal bildirimini hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Veri ihlalinin, Bankanın Veri Sızıntısı ekibi tarafından Teftiş Kurulu Başkanlığı'na iletilen bildirimde istinaden soruşturma çalışmalarına başlanılarak tespit edildiği,
- Çalışanın veri sorumlusu nezdinde kullandığı e-posta adresine gelen ve ilgili adresten iletilen e-postalara ilişkin kayıtların incelenmesi neticesinde çalışanın 346 müşteriye ait bilgileri bir word dokümanına işlediği ve söz konusu dokümanı e-posta ile bir yatırım firmasında çalıştığını ve arkadaşı olduğunu iddia ettiği 3. kişiye gönderdiği,
- Söz konusu müşterilerin hepsinin bir yatırım şirketine para transferlerinin bulunduğu,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, müşteri işlem ve finans verileri olduğu,
- Verileri paylaşılan müşterilerin ihlale sebebiyet veren çalışanın ilişkili olduğu şubenin müşterileri olmadığı, bu nedenle çalışanın verileri toplaması ve paylaşmasının mesnedinin bulunmadığı ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 29/09/2020 tarih ve 2020/744 sayılı Kararı ile,

- İhlalden 346 Banka müşterisinin şube no, hesap no, ad-soyadı, cep telefonu numarası ve bu müşterilerin Bankadaki hesaplarından bir yatırım firması hesabına gönderdikleri yatırım işlemi tutar bilgilerinin etkilendiği,

- İhlal ile ilgili olan personelin veri ihlalinin gerçekleşmesinden 1 seneyi aşkın süre önce 09.10.2018 tarihinde “Kişisel Verilerin Korunması Kanunu” eğitimini tamamlamış olmasına rağmen, bahse konu eğitimden sonra bizzat ihlali gerçekleştirmiş olmasının verilen eğitimin yeterli ve etkin olmadığı hususunda şüphe oluşturduğu,

- Banka dışına giden e-postalara ilişkin Veri Sızıntısı Tespit/Önleme Sisteminin mevcut olduğunun belirtilmesine rağmen söz konusu ihlale neden olan e-postanın DLP sistemleri tarafından engellenmemesi ve ihlale sebep olan çalışanın kişisel verilerin aktarımı gerçekleştirilebildiği dikkate alındığında, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)’nde “Mevcut Risk ve Tehditlerin Belirlenmesi” başlığı altında yer alan “*Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir. Bu riskler belirlenirken; - Kişisel verilerin özel nitelikli kişisel veri olup olmadığı, - Mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği, - Güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği dikkate alınmalıdır. Bu risklerin tanımlanması ve önceliğinin belirlenmesinden sonra; söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmeli, gerekli teknik ve idari tedbirler planlanarak uygulamaya konulmalıdır.*”, ifadeleri uyarınca yetkisiz olarak kişisel veri aktarımı önleme açısından veri sorumlusunun almış olduğu tedbirlerin yetersiz kaldığı,

- Banka tarafından alınan idari ve teknik tedbirlere rağmen Banka personelinin 346 müşteriye ait kişisel verileri, işleme amacı dışında üçüncü taraflara iletebildiği ve bu durumun, Kişisel Verileri Koruma Kurulu’nun 31/05/2018 tarih ve 2018/63 sayılı ilke kararında “...Bir veri sorumlusu nezdinde buldukları pozisyon veya görev itibarıyla kişisel verilere erişme yetkisi olanlar tarafından, yetkileri aşmak ve/veya yetkilerini kötüye kullanmak suretiyle, kişisel amaçlara veya nedenlere bağlı olarak işleme amacı dışında söz konusu kişisel verilerin işlenmesi ve/veya bu verilerin üçüncü kişilerle paylaşılması 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrasına aykırılık teşkil edeceğinden, bu kapsamdaki eylemlerin önlenmesi amacıyla veri sorumlularınca uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirin alınması gerektiği...” ifadelerine aykırı olarak veri güvenliğini sağlamaya yönelik veri sorumlusunun almış olduğu teknik ve idari tedbirlerin yetersiz kaldığının göstergesi olduğu

dikkate alındığında, Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin

haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 225.000 TL,

- İlgili kişilere gerekli bildirimlerin yapıldığı ve söz konusu bildirim örneklerinin tarafımıza gönderildiği,

- Ancak, ihlalin 31.10.2019 tarihinde gerçekleştiği ve Bankanın Teknoloji Veri Sızıntısı ekibi tarafından 04.11.2019 tarihinde Teftiş Kurulu Başkanlığı'na iletildiği, veri sorumlusunun Kurumumuza bildirimini 06.12.2019 tarihinde gerçekleştirdiği dikkate alındığında Kurul'un 24.01.2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde bildirim koşulunun sağlanmadığı

dikkate alındığında, Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen "en kısa sürede" (24.01.2019 tarih ve 2019/10 sayılı Kurul kararında belirtilen 72 saatlik süre içerisinde) bildirimde bulunma yükümlülüğüne aykırı hareket etmesi nedeniyle veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 50.000 TL

olmak üzere toplam 275.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2020/715 sayılı KVKK Kararı

Bir e-ticaret şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 17/09/2020 tarih ve 2020/715 sayılı Karar Özeti

Karar Tarihi : 17.09.2020

Karar No : 2020/715

Konu Özeti : Bir e-ticaret şirketinin veri ihlal bildirimini

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin, kaynağı ve zamanı tahmin edilemeyen şekilde internet üzerinde ifşa olmuş kullanıcı e-posta adresleri ve şifrelerinin, veri sorumlusunun internet sitesinin giriş ekranında, robot bir uygulama vasıtasıyla denenmesi şeklinde gerçekleştiği,
- İhlalin, veri sorumlusunun bilgi güvenliği ekibi tarafından, olayın gerçekleştiği gecenin sabahı, mesai başlangıcında yapılan rutin kontroller sırasında tespit edildiği, müteakiben vaka hakkında detaylı araştırma başlatıldığı,
- İhlalden etkilenen kişi ve kayıt sayısının 832 olduğu,
- İhlalle ilişkili 832 hesabın kullanıcılarına e-posta aracılığıyla bildirimde bulunduğu, bildirimlerin, olaya ilişkin inceleme ve tespitler tamamlandıktan sonra derhal yapıldığı,
- İhlale konu olan platformun işleyişi kapsamında, giriş yapmak isteyen kullanıcıların e-posta ve şifrelerini girerek ilk olarak ana ekrana, bu ana ekranı geçtikten sonra da üyelik hesaplarının bulunduğu ekranlara ulaşabildiği

ifadelerine yer verilmiştir.

Söz konusu bildirimincin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 17/09/2020 tarih ve 2020/715 sayılı Kararı ile;

- Veri sorumlusu tarafından her ne kadar bahsi geçen e-posta adreslerinin ve şifrelerinin internet sitesi üzerinden ele geçirilmediği ve ihlalden etkilenen herhangi bir kimlik, iletişim veya müşteri işlem bilgisinin bulunmadığı belirtilse de ilgili kişilerin hesaplarına yetkisiz kişilerce erişimde

bulunulduđu, kişisel verilerin gizliliđinin bozulduđu ve söz konusu durumun da veri ihlali oluşturduđu,

- Veri sorumlusunun aynı IP adresinden başarısız oturum açma girişim sayısının veri ihlalden sonra sınırlandırıldığı, bahsi geçen sınırlandırma tedbirini önceden almış olması halinde internet ortamında sıkça rastlanan saldırı neticesinde ihlalin gerçekleşmesinin önlenebileceđi ya da ihlalin etkisinin azaltılabileceđi, bunun da veri sorumlusunun veri ihlali öncesinde veri güvenliđini sağlamaya yönelik alması gereken teknik tedbirleri yeterli ve gerekli düzeyde almadığının göstergesi olduđu,

- İhlalden 832 kişiye ait e-posta adresi ve şifre bilgilerinin etkilenmiş olduđunun beyan edildiđi,

- Veri sorumlusu tarafından kullanıcıların belirli zaman aralıklarında şifrelerini deđiştirmelerinin sağlanmadığı,

- “Web uygulaması güvenlik duvarı” [WAF (Web Application Firewall)] üzerinde aynı IP ile başarılı oturum açma işleminin engellenmesi kural tanımının veri ihlali gerçekleşmeden önce alınması gerekirken veri ihlalinin gerçekleşmesinden sonra alındığı,

- İhale konu olayda ilgili kişiler önemli bir zarara uğramamış olsa da bahsi geçen internet sitesinin kullanım düzeyi ve içerisinde yer alan kişisel veriler düşünöldüğünde veri sorumlusunun ilgili tedbirleri almamasının ihlal sonucunda potansiyel tehdit açısından ciddi bir risk taşıdığı

deđerlendirmelerinden hareketle; 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliđini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriđi, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 165.000 TL idari para cezası uygulanmasına,

- İhlalin 17.12.2019 tarihinde gerçekleştiđi, 17.12.2019 tarihinde tespit edildiđi ve 20.12.2019 tarihinde Kurumumuza bildirildiđi dikkate alındığında Kanunun 12 inci maddesinin (5) numaralı fıkrası kapsamında Kurulun 24/01/2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde veri sorumlusunun bildirimde bulunduđu, öte yandan veri sorumlusu tarafından ilgili kişilere bildirim yapıldığı

dikkate alındığında, veri sorumlusu hakkında Kanunun 12 nci maddesinin (5) numaralı fıkrası kapsamında yapılacak bir işlem bulunmadığına

karar verilmiştir.

2020/710 sayılı KVKK Kararı

İcra Müdürlükleri tarafından ilgili kişilerin yakınlarına haciz ihbarnamesi gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 17/09/2020 tarih ve 2020/710 sayılı Karar Özeti

Karar Tarihi : 17.09.2020

Karar No : 2020/710

Konu Özeti : İcra dosyasının tarafı olan ilgili kişilerin icra takibi ile ilgisi bulunmayan akrabalarına İcra Müdürlükleri tarafından haciz ihbarnamesi gönderilmesi

Kuruma intikal eden şikâyet başvurusunda, ilgili kişiler hakkında yürütülen icra takibi esnasında söz konusu icra takibi ile ilgisi bulunmayan, borçlu durumunda olmayan akrabalarının kişisel bilgilerinin araştırılması, adres ve kimlik bilgilerinin İcra Müdürlüğünün görevi kapsamında bulunmadığı halde tespit edilmesi ve bu çerçevede kişisel verilerinin hukuka aykırı bir şekilde akrabaları ile paylaşılmasının 6698 sayılı Kişisel Verilerin Korunması Kanununa (Kanun) aykırılık teşkil ettiği ifade edilerek İcra Müdürlükleri hakkında gereğinin yapılması talep edilmiştir.

Bahse konu şikâyet dilekçesi ve eklerinin incelenmesinden ilgili kişiler tarafından veri sorumlusuna kişisel verilerinin hukuka aykırı bir şekilde akrabaları ile paylaşılması hakkında bilgi talebi ile başvuruda bulunulduğu, veri sorumlusunun cevabi yazısında ise, *“Alacaklı vekili tarafından bildirilen üçüncü şahıslara İcra ve İflas Kanunu (İİK) 89/1 Haciz ihbarnamesi gönderilmiş olup, haciz ihbarnamesi alacaklı ve borçlu dışında bulunan bütün üçüncü şahısları kapsamakta olduğundan Müdürlüğümüzce yapılan işlemde hukuka aykırılık bulunmamaktadır...”* ifadelerine yer verildiği görülmüştür.

Konuya ilişkin olarak yapılan değerlendirme neticesinde Kişisel Verileri Koruma Kurulunun 17/09/2020 tarih ve 2020/710 sayılı Kararı ile,

- Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin, (2) numaralı fıkrasında ise kişisel verilerin kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin

işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın işlenmesinin mümkün olduğunun hüküm altına alındığı,

- İcra ve İflas Hukuku gereğince iflası talep edilen borçluya ilişkin hak ve borçların ancak yetkili devlet organlarına başvuru yoluyla ve yasal düzenlemelerde gösterilen usuller çerçevesinde cebri olarak takip edilebildiği, haczin, kural olarak kesinleşmiş bir icra takibinin konusu olan belli bir para alacağının ödenmesini sağlamak için bu yolda talepte bulunan alacaklı lehine, söz konusu alacağı karşılayacak miktar ve değerdeki borçluya ait mal ve haklara icra dairesi tarafından hukuken el konulması olarak tanımlandığı, söz konusu mal ve hakların borçlunun elinde olabileceği gibi üçüncü bir kişide de bulunabileceği, borçluya ait olmakla beraber üçüncü kişilerde bulunan hak ve alacakların haczinin İcra ve İflas Kanununun (İİK) 89 uncu maddesinde düzenlendiği,

- Anılan maddede; *“Hamiline ait olmayan veya cirosu kabil bir senetle müstenit bulunmayan alacak veya sair bir talep hakkı veya borçlunun üçüncü şahıs elindeki taşınır bir malı haczedilirse icra memuru; borçlu olan hakiki veya hükmi şahsa bundan böyle borcunu ancak icra dairesine ödeyebileceğini ve takip borçlusuna yapılan ödemenin muteber olmadığını veya malı elinde bulunduran üçüncü şahsa bundan böyle taşınır malı ancak icra dairesine teslim edebileceğini, malı takip borçlusuna vermemesini, aksi takdirde malın bedelini icra dairesine ödemek zorunda kalacağını bildirir (Haciz ihbarnamesi). Bu haciz ihbarnamesinde, ayrıca 2, 3 ve 4 üncü fıkra hükümleri de üçüncü şahsa bildirilir. Üçüncü şahıs; borcu olmadığı veya malın yedinde bulunmadığı veya haciz ihbarnamesinin tebliğinden önce borç ödenmiş veya mal istihlak edilmiş veya kusuru olmaksızın telef olmuş veya malın borçluya ait olmadığı veya malın kendisine rehnedilmiş olduğu veya alacak borçluya veya emrettiği yere verilmiş olduğu gibi bir iddiada ise, keyfiyeti, haciz ihbarnamesinin kendisine tebliğinden itibaren yedi gün içinde icra dairesine yazılı veya sözlü olarak bildirmeye mecburdur. Üçüncü şahıs, haciz ihbarnamesinin kendisine tebliğinden itibaren yedi gün içinde itiraz etmezse, mal yedinde veya borç zimmetinde sayılır ve kendisine gönderilen haciz ihbarnamesine süresinde itiraz etmediği, bu nedenle de malın yedinde veya borcun zimmetinde sayıldığı ikinci bir ihbarname ile bildirilir. Bu ikinci ihbarnamede ayrıca, üçüncü şahsın ihbarnamesinin kendisine tebliğinden itibaren yedi gün içinde ikinci fıkrada belirtilen sebeplerle itirazda bulunması, itirazda bulunmadığı takdirde zimmetinde sayılan borcu icra dairesine ödemesi veya yedinde sayılan malı icra dairesine teslim etmesi istenir. İkinci ihbarnameye süresi içinde itiraz etmeyen ve zimmetinde sayılan borcu icra dairesine ödemeyen veya yedinde sayılan malı icra dairesine teslim etmeyen üçüncü şahsa on beş gün*

içinde parayı icra dairesine ödemesi veya yedinde sayılan malı teslim etmesi yahut bu süre içinde menfi tespit davası açması, aksi takdirde zimmetinde sayılan borcu ödemeye veya yedinde sayılan malı teslim zorlanacağı bildirilir. Bu bildirim alan üçüncü şahıs, icra takibinin yapıldığı veya yerleşim yerinin bulunduğu yer mahkemesinde süresi içinde menfi tespit davası açtığına dair belgeyi bildirim yapıldığı tarihten itibaren yirmi gün içinde ilgili icra dairesine teslim ettiği takdirde, hakkında yürütülen cebri icra işlemleri menfi tespit davası sonunda verilen kararın kesinleşmesine kadar durur. Bu süre içinde 106 ncı maddede belirtilen süreler işlemez. Bu davada üçüncü şahıs, takip borçlusuna borçlu olmadığını veya malın takip borçlusuna ait olmadığını ispat etmeye mecburdur. Üçüncü şahıs açtığı bu davayı kaybederse, mahkemece, dava konusu şeyin yüzde yirmisinden aşağı olmamak üzere bir tazminata mahkûm edilir. Bu fıkraya göre açılacak menfi tespit davaları maktu harca tabidir..." hükmüne yer verildiği,

- Borçlunun üçüncü kişilerdeki mal ve alacakları için İcra Müdürlüğüne el koyma imkânı bulunduğundan, üçüncü kişilerin bünyesinde bulunan mal ve alacakların haczinde, haczin etkisiz bırakılmasının önlenmesi amacıyla İİK'nın 89 uncu maddesinde yer alan kuralların düzenlendiği, bu hususta ilgili maddenin İcra Müdürlüğü tarafından uygulanabilecek usulü ve alacaklı ile üçüncü kişinin başvurabileceği imkânları düzenlediği, İİK'nın 89 uncu maddesinin borçlunun üçüncü kişilerdeki mal ve alacaklarının nasıl haczedileceğinden ziyade, yapılan haczin korunmasına yönelik muhafaza tedbirlerini düzenlediği, borçlunun üçüncü kişilerdeki alacağı kavramına; maaş veya ücreti, borçlunun bir bankadaki mevduatı, üçüncü kişiye ödünç vermiş olduğu para, satmış olduğu malın satış bedeli, kiraladığı taşınmazın kira bedeli, borçlunun bir şirketteki kâr veya tasfiye payı, taraf bulunduğu cari hesap sözleşmesinde diğer taraftan alacaklı olduğu hesap bakiyesinin örnek olarak gösterilebildiği,

- Benzer nitelikte bir olayda, Yargıtay 12. Hukuk Dairesinin 15.04.2013 tarihli ve E:2013/5621 K:2013/14186 sayılı kararında, " ... Buna göre kural olarak icra müdürünün haciz talebini yerine getirme konusunda herhangi bir takdir yetkisi bulunmadığının kabulü gerekir. ... Görüldüğü gibi burada tanınan takdir yetkisi, İİK'nın 82. maddesi kapsamında malın haczi kabil olup olmadığı ile sınırlı olup, icra müdürünün bunun dışında, örneğin malın 3. kişiye ait olduğu ya da somut olayda olduğu gibi haciz ihbarnamesi gönderilmesi istenen kişilerin borçluya nazaran 3. kişi sayılamayacakları gerekçesi ile haciz talebinin veya haciz ihbarı gönderilmesi isteminin yerine getirilmesi konusunda herhangi bir takdir yetkisinin bulunmadığı tartışmasızdır. Haczi talep edilen malın üçüncü kişiye ait olduğunun iddia edilmesi halinde istihkak prosedürünün uygulanacağı ya da kendisine haciz ihbarı gönderilen kişinin 3. kişi olmadığı yönündeki iddiasını İİK'nın 16. maddesi uyarınca şikayet yoluyla icra mahkemesinde ileri sürebileceği tabidir. ..." şeklinde açıklamalara yer verilerek, haciz ihbarnamesi gönderilmesi istenen kişilerin borçluya nazaran üçüncü kişi

sayılamayacakları gerekçesi ile haciz ihbarı gönderilmesi isteminin yerine getirilmesi konusunda İcra Müdürünün herhangi bir takdir yetkisinin bulunmadığı hususunun vurgulandığı

değerlendirmelerinden hareketle;

- İlgili kişilerin kişisel verilerinin üçüncü kişilerle paylaşılması hususuna ilişkin olarak; İcra ve İflas Kanununun 89 uncu maddesi kapsamında borçlunun üçüncü kişilerdeki alacağının tahsili amacıyla alacaklı tarafından bildirilen gerçek veya tüzel kişilere İcra Müdürlüklerince birinci haciz ihbarnamesi gönderilmesinde hukuken engel bulunmadığına, İcra Müdürlükleri nezdinde gerçekleştirilen ilgili kişilerin kişisel verilerinin işlenmesi faaliyetinin Kanunun 5 inci maddesinin (2) numaralı fıkrası kapsamında 'Kanunlarda açıkça öngörülme' şartına dayanılarak gerçekleştirildiğine, bu çerçevede söz konusu başvuruya ilişkin olarak Kanun kapsamında yapılacak bir işlem bulunmadığına karar verilmiştir.

2020/691 sayılı KVKK Kararı

İlgili kişinin cep telefonu numarasının, açık rızası olmaksızın bir dernek tarafından reklam içerikli SMS gönderimi için işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 10/09/2020 tarihli ve 2020/691 Sayılı Karar Özeti

Karar Tarihi : 10.09.2020

Karar No : 2020/691

Konu Özeti : İlgili kişinin cep telefonu numarasının, açık rızası olmaksızın bir dernek tarafından reklam içerikli SMS gönderimi için işlenmesi hakkında

Kurumumuza intikal eden şikayette ilgili kişinin cep telefonu numarasına bir dernek tarafından reklam içerikli SMS gönderildiği, ilgili kişinin bu tür mesajlardan rahatsız olması, derneğin kendisine ait kişisel verileri nereden elde ettiğini bilmemesi ve kişisel verilerinin kendisinin açık rızası olmaksızın kullanılması nedeniyle 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) uyarınca dernekten bilgi talebinde bulunduğu, söz konusu bilgi alma talebine 30 günlük yasal süre içinde herhangi bir yanıt verilmediği belirtilerek, veri sorumlusu dernek nezdinde gerçekleşen tüm usulsüzlüklerin ortaya çıkarılması ve gerekli yaptırımların uygulanması talep edilmiştir.

Söz konusu iddialara ilişkin veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- Şikayetçinin bilgi edinme başvurusunun kendilerine tebliğ edilmiş olmasına rağmen, idari bir sıkıntı sebebiyle cevabın tanzim ve tebliğ edilemediği,
- Şikayetçinin başvurusunu müteakip Şikayetçi adına kayıtlı olan telefon numarasının, derhal “pasif” konuma, diğer bir deyişle “gönderim yapılamaz” hale getirildiği,
- Şikayetçinin dernek nezdinde SMS reklamlarına yahut bildirimlerine onay verdiğine ilişkin bir rızasının tespit edilemediği,
- Dernek uhdesinde şikayetçinin telefon numarasından başka herhangi bir kişisel verisinin mevcut olmadığı,

- Şikayetçinin telefon numarasının evvelce SMS bağışısı yapması sebebiyle ellerinde bulunuyor olmasının kuvvetle muhtemel olduğu,
- Söz konusu SMS'in şikayetçiye dernek tarafından gönderildiği

ifade edilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 10/09/2020 tarihli ve 2020/691 sayılı Kararı ile,

- Kanunun 5 inci maddesinde kişisel verilerin işleme şartlarına yer verilmiş olduğu; bu maddenin birinci fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, ikinci fıkrasında belirtilen şartlardan (-Kanunlarda açıkça öngörülmesi, -Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, -Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, -Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, -İlgili kişinin kendisi tarafından alenileştirilmiş olması, -Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, -İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması) birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu,

- Hukuka uygun bir kişisel veri işleme faaliyetinin gerçekleştirilebilmesi için kişisel verilerin öncelikle Kanunun 5 inci maddesindeki şartlardan birine dayanılarak işlenmesi gerektiği, geçerli bir hukuki sebebi olan kişisel veri işleme faaliyetleri bakımından ise her hal ve şartta Kanunun 4 üncü maddesinde sayılan temel ilkelere uygunluğun sağlanmasının veri sorumlusunun başlıca yükümlülüklerinden olduğu, somut olayda; veri sorumlusu dernek tarafından şikayetçinin kişisel verisi niteliğindeki cep telefonu numarasının işleme sebebinin tevsik edilemediği gibi bu hususa ilişkin netlik içeren herhangi bir açıklama da yapılmadığı, veri sorumlusu tarafından yapılan "İlgili kişinin evvelce SMS bağışısı yapmış olduğunun kuvvetle muhtemel olduğu" şeklindeki açıklamanın ise hukuki zemine oturan bir açıklama olmadığı gibi geçerli bir açıklama olarak da kabul edilemeyeceği, veri sorumlusu tarafından ilgili kişinin SMS gönderimine ilişkin açık rızasının tespit edilemediğinin açıkça belirtildiği, bu çerçevede şikayetçinin kişisel verisi niteliğindeki cep telefonu numarasının elde edilmesi ve reklam içerikli SMS gönderimi için kullanılması şeklide gerçekleşen kişisel veri işleme faaliyetinin Kanuna aykırılık teşkil ettiği, bu durumun ise veri sorumlusu tarafından veri güvenliğine ilişkin yükümlülüklerin yerine getirilmediğinin göstergesi olduğu,

- Bununla birlikte, şikayete konu olayda, veri sorumlusu konumundaki derneğin ilgili kişinin bilgi edinme talebine yanıt vermediği ve yanıt vermeme sebebinin de “idari bir sıkıntı” şeklinde belirtildiği fakat bahsedilen idari sıkıntının ne olduğuna ilişkin aydınlatıcı bir açıklama yapılmadığı, Kanun ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğdeki düzenlemeler ışığında veri sorumlularının herhangi bir başvuru karşısında yapabileceği iki tür hareketin bulunduğu ve bu kapsamda söz konusu başvurunun veri sorumluları tarafından kabul edilmesinin ya da gerekçesinin açıklanarak reddedilmesinin gerektiği, somut olayda derneğin ilgili başvuru karşısında hiçbir harekette bulunmaması dolayısıyla derneğin ilgili kişinin başvurusuna cevap vermemesinin Kanuna aykırılık teşkil ettiği,

- Öte yandan, Kanunun 7 nci maddesinin birinci fıkrasının; “Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.” hükmünü amir olduğu, söz konusu hükmün kanunlara uygun şekilde işlenmiş olan kişisel verilerin daha sonraki süreçte silinmesi, yok edilmesi, anonim hale getirilmesi için açıklama getirdiği, bununla birlikte başlangıçtan itibaren hukuki sebepten yoksun olması dolayısıyla hukuka aykırı kişisel veri işlemenin söz konusu olması halinde bu kişisel verilerin derhal silinmesi gerektiği, zira başlangıçtan itibaren vuku bulmaması gereken ve halihazırda hukuka aykırılık arz eden bu durumun derhal ortadan kaldırılarak hukuka uygunluğun en kısa sürede tesis edilmesi gerektiği,

- Şikayete konu olay bakımından, bahse konu telefon numarasının kara listeye alınmasının hukuka aykırı olarak işlenen kişisel verinin silindiği anlamına gelmediği, hiçbir hukuki sebebe dayanmaksızın işlenen kişisel verinin halihazırda derneğin sistemlerinde kara listeye alınmış bir şekilde bekliyor oluşunun hukuka aykırı durumun devam ettiğini gösterdiği, söz konusu hukuka aykırılığın devam etmemesi adına bahse konu telefon numarasının imha edilmesi gerektiği

değerlendirmelerinden hareketle;

- Kanunun 12 nci maddesinin birinci fıkrasının (a) bendi çerçevesinde kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı kanaatine varıldığından, veri sorumlusu sıfatını haiz dernek hakkında Kanunun 18 inci maddesinin birinci fıkrasının (b) bendi uyarınca idari para cezası uygulanmasına,

- Veri sorumlusu dernek tarafından ilgili kişilerin Kanun kapsamındaki başvurularının Kanunda yer verilen yasal süre içerisinde yanıtlanmasına azami dikkat ve özenin gösterilmesi hususunda talimatlandırılmasına,

- İlgili kişinin halihazırda hukuka aykırı olarak elde edilmiş olan kişisel verisi niteliğindeki cep telefonu numarasının imha edilmesi hususunda veri sorumlusunun talimatlandırılmasına karar verilmiştir.

2020/667 sayılı KVKK Kararı

Bir sigorta şirketinin ilgili kişiye vereceği hizmeti açık rıza şartına bağlaması sebebiyle Kuruma iletilen şikâyet hakkında Kişisel Verileri Koruma Kurulunun 03/09/2020 tarihli ve 2020/667 sayılı Karar Özeti

Karar Tarihi : 03.09.2020

Karar No : 2020/667

Konu Özeti : Bir sigorta şirketinin ilgili kişiye vereceği hizmeti açık rıza temini şartına bağlaması

Kuruma intikal eden şikâyet dilekçesinde özetle; ilgili kişinin veri sorumlusu bir sigorta şirketine başvurarak ailesi adına düzenlediği sağlık sigortası poliçesini yenilemek istediği; ancak veri sorumlusunun kendisinden poliçeyi yenilemek için açık rıza almak istediği ifade edilmiş olup bu durumun 6698 sayılı Kişisel Verilerin Korunması Kanununa (Kanun) aykırı olduğu gerekçesi ile veri sorumlusu hakkında gereğinin yapılması talep edilmiştir.

Başvurunun değerlendirilmesi neticesinde Kişisel Verileri Koruma Kurulunun 03/09/2020 tarihli ve 2020/667 sayılı Kararı ile;

• Kanunun “*Özel Nitelikli Kişisel Verilerin İşlenme Şartları*” başlıklı 6 ncı maddesinin (1) numaralı fıkrasında özel nitelikli kişisel verilerin “*Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri*” olarak sayıldığı, özel nitelikli verilerin işlenmesine ilişkin ise; “(2) *Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır. (3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.*” hükümlerine yer verildiği,

• Bu kapsamda; sağlık sigortası poliçesinin özel nitelikli kişisel veri niteliğini haiz sağlık verilerini içerdiği, poliçede yer alan sağlık verilerinin ise Kanunun 6 ncı maddesinin (3) numaralı fıkrası

kapsamında işlenemeyeceđi, veri işlemenin ancak ilgili kişiden açık rıza alınması yoluyla gerçekleştirilebileceđi ve bu nedenle ilgili kişiden açık rıza alınması talebinin Kanuna aykırılık teşkil etmediđi

deđerlendirmelerinden hareketle söz konusu şikâyet ile ilgili olarak Kanun kapsamında tesis edilecek bir işlem bulunmadıđına karar verilmiştir.

2020/649 sayılı KVKK Kararı

Biyometrik imza verisinin kullanılmasına ilişkin görüş talebi ile ilgili olarak Kişisel Verileri Koruma Kurulunun 27.08.2020 Tarihli ve 2020/649 Sayılı Karar Özeti

Karar Tarihi : 27.08.2020

Karar No : 2020/649

Konu Özeti : 6698 sayılı Kişisel Verilerin Korunması Kanunu çerçevesinde biyometrik imza verisinin kullanılması hakkında.

Kurumumuza intikal eden bir başvuruda; 6098 sayılı Türk Borçlar Kanununun (6098 sayılı Kanun) sözleşmelerin şekillerine ilişkin esasların belirlendiği 14 üncü ve 15 inci maddelerinde imzaların yalnızca el ile atılma zorunluluğunun yer alması sebebiyle biyometrik imzaların 6698 sayılı Kişisel Verilerin Korunması Kanununun (6698 sayılı Kanun) 6 ncı maddesinin üçüncü fıkrası kapsamında değerlendirilip değerlendirilemeyeceği hususunda Kurumumuz görüşlerinin talep edilmesi üzerine Kişisel Verileri Koruma Kurulunun (Kurul) 27.08.2020 tarih ve 2020/649 sayılı kararında aşağıdaki değerlendirmelere yer verilmiştir.

Biyometrik veriler, herhangi bir müdahaleye gerek olmaksızın zahmetsiz bir şekilde elde edilen ve genel itibariyle ömür boyu değişmeden kalan veriler olup, bu verilerin değiştirilmesi veya unutulması mümkün değildir; çünkü birey ona ait özellikleri bizzat kendisi taşımaktadır. Fizyolojik nitelikli biyometrik veriler, insan vücudunun benzersiz özelliklerini içeren verilerdir. Bu çerçevede, kişilere ait iris, retina, parmak izi, yüz, avuç içi, damarlar gibi veriler fizyolojik nitelikte biyometrik verileri oluşturmaktadır. Diğer taraftan, davranışsal biyometrik veriler ise zaman, ruh hali, yaş ve benzeri faktörlere göre değişebilen dinamik yapıda özelliklere ilişkindir. Örneğin, kişilerin yürüyüş biçimi, klavyeye basış şekli, akıllı cihazları kullanırken uyguladığı basınç ve basış şekli, araba sürüş biçimi gibi veriler davranışsal nitelikte biyometrik verileri oluşturmaktadır.

Biyometrik imza, imza sahiplerinin belirli biyometrik verilerini kullanarak imzalarını özel bir tablet/ped üzerinde oluşturmaları ve genellikle bu verilerin imzalanan belgeye çözülemez biçimde bağlanmasıyla elde edilmektedir. Bu noktada belirtmekte fayda görülmektedir ki, her ne kadar biyometrik imza ile elle atılan ıslak imza arasında benzer yönler bulunsa da, her ikisi de farklı

kavramlardır. Biyometrik imza çözümleri belirli bir standart çerçevesinde tanımlanmadığından farklı kurgusal özelliklere sahiptir ve ıslak imza ile denk sayılmamaktadır. Biyometrik imza ile elle atılan imzanın bütün fonksiyonları bakımından aynı olmadığı hususuna Avrupa Sayısal Tek Pazarı'ndaki (Digital Single Market) elektronik ortamdaki işlemler için elektronik kimlik tanımlama ve güven hizmetleriyle ilgili Avrupa Birliği düzenlemesi standardı olan "Elektronik Kimlik Belirleme ve Güven Hizmetleri Düzenlemesi"nde (eIDAS) de değinilmiştir. Islak, elle atılan klasik imza, imzanın görselliğine dayanarak o imzanın statik veya geometrik özelliklerini dikkate almakta iken (imzanın nasıl görüldüğü ile alakalıdır); biyometrik imza ise imzanın dinamik özelliklerini (imzanın nasıl oluştuğu) dikkate almaktadır. Bu doğrultuda, biyometrik imzanın analizinde, biyometrik imza esnasında uygulanan basıncın miktarı, yazma açısı, kalemin hızı ve ivmesi, harflerin oluşumu, imzanın yönü ve benzer diğer kişinin sahip olduğu benzersiz dinamik özellikler kullanılmaktadır.

Bilindiği üzere, 6698 sayılı Kanunun 6 ncı maddesinde; biyometrik veri özel nitelikli kişisel veriler arasında sayılmış olup, biyometrik veriler açık rıza bulunmayan hallerde ancak kanunlarda öngörülmesi halinde işlenebilmektedir. Bu çerçevede, 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 67 nci maddesinde yer alan sağlık hizmetlerinden yararlanmak amacıyla biyometrik verinin alınmasına ilişkin düzenleme ve 5490 sayılı Nüfus Hizmetleri Kanununun 7 nci maddesinde yer alan, aile kütüklerinde biyometrik veri bilgisinin de bulunduğu düzenlemeler kanunlarda öngörülen hallere örnek teşkil etmektedir. Anılan örneklerden de görüldüğü üzere, başka kanunlarda biyometrik verilerin işlenmesine dair hükümlerin yer alması durumunda ilgili kanunlarda yer alan hükümler uygulanacaktır. Ancak biyometrik veri işlemenin kanunlarda öngörülmesi durumunda, söz konusu hükmün şüpheye yer bırakmayacak kadar açık olması gerektiği değerlendirilmektedir.

Öte yandan, 6098 sayılı Kanunun sözleşmelerin şekline ilişkin düzenlemeleri içeren kısmında yer alan 14 üncü ve 15 inci maddeleri;

"b. Unsurları

MADDE 14- Yazılı şekilde yapılması öngörülen sözleşmelerde borç altına girenlerin imzalarının bulunması zorunludur. Kanunda aksi öngörülmedikçe, imzalı bir mektup, asılları borç altına girenlerce imzalanmış telgraf, teyit edilmiş olmaları kaydıyla faks veya buna benzer iletişim araçları ya da güvenli elektronik imza ile gönderilip saklanabilen metinler de yazılı şekil yerine geçer.

c. İmza

MADDE 15- İmzanın, borç altına girenin el yazısıyla atılması zorunludur. Güvenli elektronik imza da, el yazısıyla atılmış imzanın bütün hukuki sonuçlarını doğurur. İmzanın el yazısı dışında bir araçla atılması, ancak örf ve âdetçe kabul edilen durumlarda ve özellikle çok sayıda çıkarılan kıymetli evrakın imzalanmasında yeterli sayılır. Görme engellilerin talepleri halinde imzalarında şahit aranır. Aksi takdirde görme engellilerin imzalarını el yazısı ile atmaları yeterlidir."

hükmünü amirdir. Bu noktada belirtmekte fayda görülmektedir ki, 6098 sayılı Kanunda yer alan "imza"ya ilişkin düzenlemenin kapsamı klasik imza ve güvenli elektronik imzadır. Her ne kadar güvenli elektronik imza ile klasik imza doğurduğu hukuki sonuçlar bakımından aynı olarak düşünülse de, kanun koyucunun hem klasik imzayı hem de güvenli elektronik imzayı ayrı ayrı düzenlediği görülmektedir. Bu kapsamda, 6098 sayılı Kanunun mezkûr hükümlerinde yer alan düzenlemeyi biyometrik imzayı kapsayacak şekilde yorumlamanın hem 6698 sayılı Kanunun 6 ncı maddesinin üçüncü fıkrasında yer alan "*kanunlarda öngörüldüğü haller*" istisnasının geniş yorumlamasına yol açacağı hem de ölçülülük ilkesine aykırı olacağı değerlendirilmektedir.

Bu itibarla, konuya ilişkin olarak yukarıda yer verilen mevzuat hükümleri ve açıklamalar ışığında;

- Biyometrik imzanın biyometrik veri niteliğini haiz olduğu,
- Bu nitelikteki verilerin işlenebilmesinin 6698 sayılı Kanunun 6 ncı maddesi uyarınca kanunlarda öngörülme şartının gerçekleşmesi ya da ilgili kişilerden açık rıza alınması ile mümkün olabileceği,
- 6098 sayılı Borçlar Kanununun 15 nci maddesinde yer alan hükmün 6698 sayılı Kanunun 6 ncı maddesinin 3 numaralı fıkrasında yer alan "*kanunlarda öngörülme*" şartına karşılık gelmediği,
- Bu sebeple söz konusu işlemin ancak ilgili kişilerden;

Açık rıza alınması,

6698 sayılı Kanunun 10 uncu maddesi kapsamında gerekli aydınlatmanın yapılmış olması,

6698 sayılı Kanunun 6 ncı maddesinin 4 üncü fıkrasına dayanarak Kurul tarafından belirlenen

"Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" in de dikkate alınması

şartıyla gerçekleştirilebileceği değerlendirilmiştir.

2020/622 sayılı KVKK Kararı

18 yaşını doldurmamış ilgili kişiye ait sağlık raporunun imha edilmesine yönelik ilgili kişinin babası tarafından veri sorumlusuna başvurulması ve cevap alınamaması üzerine ilgili kişinin kendisi tarafından Kurumumuza şikayette bulunulması hakkında Kişisel Verileri Koruma Kurulunun 11/08/2020 tarihli ve 2020/622 sayılı Karar Özeti

Karar Tarihi : 11.08.2020

Karar No : 2020/622

Konu Özeti : 18 yaşını doldurmamış ilgili kişiye ait sağlık raporunun imha edilmesine yönelik ilgili kişinin babası tarafından veri sorumlusuna başvurulması ve cevap alınamaması üzerine ilgili kişinin kendisi tarafından Kurumumuza şikayette bulunulması hakkında Kişisel Verileri Koruma Kurulunun Kararı

Gerçeğe aykırı olarak düzenlendiği iddia edilen 18 yaşını doldurmamış ilgili kişiye ait sağlık raporunun kayıtlardan imha edilmesine yönelik ilgili kişinin babası tarafından başvuruda bulunan veri sorumlusunun söz konusu talebe cevap vermemesi üzerine, ilgili kişinin kendisinin Kişisel Verileri Koruma Kuruluna (Kurul) yaptığı şikayetin Kurulca incelenmesi neticesinde alınan 11/08/2020 tarihli ve 2020/622 sayılı Kararda, ilgili kişinin 18 yaşını doldurmadığı dikkate alındığında öncelikli olarak Kurula şikayette bulunulmasına dair hakkın ilgili kişi tarafından kullanılıp kullanılmayacağı ile veri sorumlusuna başvuran ile Kurula şikayette bulunan kişilerin farklı olması nedeniyle söz konusu şikayetin mevzuatta yer alan usul şartlarını taşıyıp taşımadığı hususunun ele alınması gereğinin hasıl olduğundan hareketle aşağıdaki değerlendirmelere yer verilmiştir;

- Anayasanın “Temel Haklar ve Ödevler” başlıklı ikinci kısmının birinci bölümünde yer alan ve temel hak ve hürriyetlerin niteliğini açıklayan 12 nci maddesinde; herkesin kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlere sahip olduğunun düzenlendiği, takip eden maddelerde ise temel hak ve hürriyetlerin hangi koşullar altında sınırlanabileceği ya da durdurulabileceği ile temel hak ve hürriyetlerin neler olduğunun hüküm altına alındığı,
- 2010 Anayasa değişikliği ile hukukumuzda dâhil edilen “Kişisel verilerin korunmasını isteme hakkı”nın, Anayasanın “Kişinin Hakları ve Ödevleri” başlıklı ikinci bölümünde, temel bir hak ve

özgürlük olarak düzenlendiği, “Özel hayatın gizliliği” başlıklı 20 nci maddesinin üçüncü fıkrasında; herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu; bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığının belirtildiği; kişisel verilerin, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceğinin hüküm altına alındığı,

- Anayasanın mezkûr hükmü uyarınca 24.03.2016 tarihinde kabul edilen ve 07.04.2016 tarihli Resmi Gazetede yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanununun amacının, “Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek” olduğu

- 4721 sayılı Türk Medeni Kanununun 13 üncü maddesinde; yaşının küçüklüğü yüzünden veya akıl hastalığı, akıl zayıflığı, sarhoşluk ya da bunlara benzer sebeplerden biriyle akla uygun davranma yeteneğinden yoksun olmayan herkesin Türk Medeni Kanununa göre ayırt etme gücüne sahip olduğunun düzenlendiği, mezkûr Kanunun “Ayırt etme gücüne sahip küçükler ve kısıtlılar” başlıklı 16 ncı maddesinde ise ayırt etme gücüne sahip küçükler ve kısıtlıların, yasal temsilcilerinin rızası olmadıkça kendi işlemleriyle borç altına giremeyeceği düzenlenmekle birlikte karşılıksız kazanma ve **kişiyeye sıkı sıkıya bağlı hakları kullanmada** bu rızanın gerekli olmadığının hüküm altına alındığı; bu çerçevede, kural olarak sınırlı ehliyetsizlerin kişiyeye sıkı sıkıya bağlı haklarını kullanmada yasal temsilcinin rızasını almak zorunda olmadığı düzenlense de, kişiyeye sıkı sıkıya bağlı haklardan olup çok önemli sonuçlar doğurmaya elverişli olan bazılarının (Ergin kılınma-MK. m.12, nişanlanma- MK. m.118, evlenme MK. m.126,127, evlenmeye izin MK. m.124/II, evlatlığa alınma MK. m.308) istisnai olarak yasal temsilcinin rızasına tabi tutulduğunun görüldüğü (AKİPEK, Jale G./ AKINTÜRK, Turgut/ ATEŞ, Derya: Türk Medeni Hukuku Başlangıç Hükümleri, Kişiler Hukuku, I. Cilt, Yenilenmiş 12. Baskı, İstanbul 2015, s. 325, 326.); bu itibarla, kişiyeye sıkı sıkıya bağlı hakların kullanılmasına karar verme yetkisinin bizzat hak sahibi tarafından kullanılması gerektiği, hakkın kullanılmasına karar verme yetkisinin başkasına devredilemediği, bu yetkinin başkasına tanınmasının kişilik kavramı ile bağdaşmadığının öğretilde kabul gördüğü (OĞUZMAN, M. Kemal/ BARLAS, Nami: Medeni Hukuk, 18. Bası, İstanbul 2012, s. 171.),

- Diğer taraftan, 4721 sayılı Kanun başta olmak üzere mevzuatımızda, ne kişiyeye sıkı sıkıya bağlı hakkın ne de kişilik hakkının tanımına yer verildiği; bununla birlikte, kişilik hakkının, kişinin maddi

ve manevi varlıkları ile iktisadi bütünlüğü ve sır çevresi üzerinde sahip olduğu kişiye sıkı sıkıya bağlı bir hak olduğu, bu niteliği nedeniyle herkese karşı ileri sürülebilen bu hakkın başkasına devredilemez, vazgeçilemez ve zamanaşımına uğramaz nitelikte olduğu, kişiye sıkı sıkıya bağlı olan hakların bu niteliklerinden ötürü miras yoluyla mirasçılara geçmediği ve hak süjesinin ölümüyle kendiliklerinden ortadan kalktığı; bu anlamda, ilgili kişilerin kişisel verilerinin işlenmesi kapsamında sahip olduğu hakların da kişiye sıkı sıkıya bağlı haklardan olduğu; kişiye sıkı sıkıya bağlı hakların doktrinde mutlak ve nispi olarak ayrıldığı; nişanlanma, evlenme, evlilik dışı çocuğu tanıma, mal rejimi sözleşmesi yapma, derneğe üye olma, ölüme bağlı tasarrufta bulunma gibi mutlak kişiye sıkı biçimde bağlı hakların kullanılmasında karar verme yetkisi, velinin rızası koşuluyla bizzat hak sahibine tanınmışken (BAYGIN, Cem: Soybağı Hukuku, On iki Levha, İstanbul 2010, s. 314.); **kişiliği koruyucu davalar**, yaş ve isim düzeltme davalarını ikame etme gibi nispi kişiye sıkı biçimde bağlı hakların küçük tarafından bizzat kullanılabilmesi gibi, velinin de küçük adına ve hesabına kullanabildiği; bu anlamda 4721 sayılı Kanununun 16 ncı maddesinin birinci fıkrasında yer alan “*Ayırt etme gücüne sahip küçükler ve kısıtlılar, yasal temsilcilerinin rızası olmadıkça, kendi işlemleriyle borç altına giremezler. Karşılıksız kazanmada ve kişiye sıkı sıkıya bağlı hakları kullanmada bu rıza gerekli değildir.*” hükmündeki ayırt etme gücüne sahip küçüklerin kişiye sıkı sıkıya bağlı hakları kullanmalarında yasal temsilcilerinin rızasının gerekli olmadığına ilişkin kuralın çocuk için bir yetki kuralı olduğu, ancak veli için bir yasak kuralı olmadığı; velinin nispi kişiye sıkı biçimde bağlı hakları küçük adına ve hesabına kullanabildiği (SEROZAN, Rona; Çocuk Hukuku, Vedat Kitapçılık, İstanbul 2017, s. 282; BAYGIN: s. 315.); bu bakımdan söz konusu ayrıma göre, çocuğun üstün yararı da gözetilerek kişisel verilerin korunması hakkının da somut olay bakımından nispi kişiye sıkı biçimde bağlı hak kategorisinde ele alınmasının yerinde olacağı değerlendirildiği,

• Öte yandan, “Kişisel Sağlık Verileri Hakkında Yönetmelik”in (Yönetmelik), “Genel ilke ve esaslar” başlığını taşıyan 5 inci maddesinin altıncı fıkrasında herkesin, veri sorumlusuna başvurarak kendisiyle ilgili olarak 6698 sayılı Kanununun 11 inci maddesinde yer alan hakları kullanabileceğinin belirtildiği; Yönetmeliğin 8 inci maddesinin birinci fıkrasında ise ebeveynlerin, çocuklarına ilişkin sağlık kayıtlarına herhangi bir onaya ihtiyaç duymaksızın e-Nabız üzerinden erişebileceği, ayırt etme gücüne sahip çocukların, sağlık geçmişlerine ebeveynlerin erişimini e-Nabız üzerinden izne tabi tutabileceğinin hüküm altına alındığı; mezkûr Yönetmelik hükümleri uyarınca sınırlı ehliyetsizlerin de ayırtım gücüne sahip olmak koşuluyla Kanununun 11 inci maddesinde belirtilen hakları bizzat kullanabileceği, bunun yanında e-Nabız verilerine erişim hususunda küçük tarafından aksi öngörülmedikçe hem küçüğün hem velisinin yetkili kılındığının anlaşıldığı; anılan düzenlemenin somut olay bakımından kişisel verilerin korunması hakkının nispi kişiye sıkı biçimde bağlı hak

olduđu yönündeki deęerlendirme ile de uyumlu olduđu; zira her iki durumda da ayırtım gücüne sahip küçüğün söz konusu hakkı bizzat kullanabileceđi gibi velisinin de onun adına ve hesabına kullanımına olanak tanındığı

deęerlendirmelerine yer verilerek;

Bu kapsamda, küçüğün ayırt etme gücüne sahip olması koşuluyla, ilgili kiři küçük ve velisinin başvuru konusundaki iradelerinin örtüştüğü de dikkate alındığında, gerek veri sorumlusuna yapılan başvuru gerek Kurula intikal eden řikayet bakımından her iki tarafın da hakkı kullanmada yetkili kabul edilebileceđi deęerlendirildiğinden somut olayda ilgili kiři ve babasının söz konusu řikayet hakkını kullanmada yetkili olduđu kanaatine varılmış ve Kanunun 15 inci maddesinin (1) numaralı fıkrası kapsamında Kurula intikal eden dilekçe ile ilgili olarak inceleme başlatılmasına karar verilmiştir.

2020/608 sayılı KVKK Kararı

İlgili kişinin, bilet satın almamasına karşın bir havayolu şirketinden uçak bileti satın aldığına dair SMS alması hakkında Kişisel Verileri Koruma Kurulunun 11/08/2020 tarihli ve 2020/608 sayılı Karar Özeti

Karar Tarihi : 11.08.2020

Karar No : 2020/608

Konu Özeti : İlgili kişinin, herhangi bir şekilde bilet satın almamasına karşın bir havayolu şirketinden uçak bileti satın aldığına dair SMS alması

Kuruma intikal eden şikâyet dilekçesinde özetle; ilgili kişinin 05*****4 numaralı cep telefonuna 01.07.2019 tarihinde bir Havayolu Şirketi tarafından Umman'dan İzmir aktarmalı İstanbul'a uçak bileti satın alındığına dair bir SMS gönderildiği, ilgili kişinin mesajı görür görmez veri sorumlusunu aradığı ancak görüşme sağlayamadığı, bunun üzerine çevrimiçi şikâyet formu doldurduğu, bu başvurusunu müteakiben veri sorumlusu tarafından aranarak belirtilen biletin iptal edildiğinin kendisine söylendiği, ilgili kişinin bunun üzerine adını ve cep telefonu numarasını kullanarak kimin söz konusu uçak biletini satın aldığına tarafına yazılı olarak bildirilmesini talep ettiği ancak herhangi bir yanıt alamadığı belirtilmiş olup veri sorumlusu hakkında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup verilen cevabî yazıda özetle;

- İlgili kişi adına 02.01.2020 tarihinde oluşturulmuş bir üyelik hesabı olduğunun görüldüğü, şikâyet tarihi olan 20.08.2019'a kadar ilgili kişiye ait herhangi bir üyelik hesabı ve bu hesap altında üyelik bilgisinin kayıtlarında yer almadığı,
- Şikâyete konu PNR kapsamında yer alan ilgili kişiye ait tek kişisel verinin cep telefonu bilgisi olduğu, söz konusu PNR kaydına bu veri girişinin de bileti satın alan mobil uygulaması kullanıcısı tarafından yapıldığı, belirtilen ilgili kişinin telefon numarasının zorunlu veri girişi alanına değil tercihe bağlı olarak sunulan "ücretli SMS bildirim" alanına bu kullanıcı tarafından girildiği ve SMS içeriğinin iletimi için yalnızca telefon numarasının hat operatörü ile paylaşıldığı,

- PNR ile ilgili kişinin telefon numarasının sistemsal olarak eşleşmediği, mobil uygulama üzerinden bilet satışında ad, soyadı, cinsiyet, doğum tarihi, telefon numarası, e-posta ve ülke bilgisi girilmesinin zorunlu olduğu diğer yandan SMS bilgilendirme hizmetinin ise zorunlu olmadığı, dolayısıyla ilgili kişiye ait kimlik bilgilerinin ilgili PNR kapsamında işlenmediği,
- İlgili kişiye ait kişisel verilerin üçüncü kişilerle paylaşımının veya üçüncü kişilerce bu verilere erişimin söz konusu olmadığı,
- Bilet satın alımı sırasında girilen T.C. kimlik numaralarının doğruluğunun MERNİS üzerinden eşleştirilerek teyit edilmesine ilişkin bir sistem bulunmadığı ancak girilen numaranın mevcut bir numara olup olmadığını anlayan (Ulaştırma ve Altyapı Bakanlığı Sivil Havacılık Genel Müdürlüğü düzenlemeleri ile uyumlu olarak) bir algoritma kullanıldığı ifade edilmiştir.

Bu savunma üzerine Kurum tarafından veri sorumlusundan, mobil uygulama vasıtasıyla alınan bilete ait PNR numarasının, ilgili kişinin iletişim bilgileri ile eşleşmediği hususunu tevsik edici mahiyette bilgi ve belgelerin Kuruma sunulması istenilmiş olup veri sorumlusu tarafından verilen yanıtta; ilgili kişiye ait olmayan biletleme işlemindeki uçuş rezervasyonu oluşturulurken işlemi yapan kişi tarafından bilet bilgilerinin ücretli SMS olarak iletilmesi tercihinin işaretlendiği ancak ücretli SMS'in gönderileceği telefon numarasının rezervasyonda kayıtlı iletişim numarasından farklı olarak girildiği, bu numaranın da ilgili kişiye ait telefon numarası olduğu hususu belirtilmiş ve bu hususa dayanak olan bilgi ve belgeler Kuruma ulaştırılmıştır.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 11/08/2020 tarihli ve 2020/608 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanununun 3 üncü maddesinin (1) numaralı fıkrasının (d) bendi gereğince "kişisel verinin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" şeklinde tanımlandığı, bu kapsamda ilgili kişiye ait telefon numarasının, adı- soyadı ve TC kimlik numarası ile eşleştirilerek saklandığından ve kimliği belirlenebilir gerçek bir kişiye ulaşılması sonucu doğurduğundan kişisel veri niteliğinde olduğu, ancak somut olayda ilgili kişiye ait telefon numarasının kendisine ait herhangi bir kayıtlı ile eşleşmediği aksine sehven yazılmış olan numaranın bileti satın alan kişi tarafından veri sorumlusu sistemlerine girildiğinin anlaşıldığı,
- Söz konusu bilgi ve belgelerin incelenmesi neticesinde, veri sorumlusu kanalları üzerinden bilet almakta olan 05*****2 telefon numarasının kullanıcısı gerçek kişinin satın aldığı biletle ilişkili olarak ilgili kişiye ait 05*****4 telefon numarasını veri sorumlusu ile paylaştığının anlaşıldığı, bu

kapsamda veri sorumlusunun müşterilerine alınan biletlere ilişkin SMS hizmeti sunarken başka bir telefon numarasına SMS gönderilmesi seçeneği de sunduğu görülmüş olup alınan bilete ilişkin müşteri bilgilerinin ilgili kişiye ait olmadığı,

değerlendirmelerinden hareketle;

- Veri sorumlusu tarafından ilgili kişinin iletişim bilgilerinin başka bir kullanıcı tarafından sisteme girilmesi suretiyle ve kastı bulunmaksızın işlendiği; ayrıca söz konusu manuel veri girişlerine cevaz veren sisteme girilen telefon numaralarının kime ait olduğunun belirlenmesine ilişkin sistemsal bir eşleştirme yahut veri tabanı bulunmadığı dikkate alındığında Kanunun 12 nci maddesinde yer alan kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri alma yükümlülüğünü ihlal ettiği yönünde bir tespit bulunmadığından konuya ilişkin Kanun kapsamında tesis edilecek bir işlem olmadığına,
- İlgili kişiler tarafından Kanun çerçevesinde yapılan başvurulara süresi içinde ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğe uygun bir şekilde cevap vermesi hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2020/567 sayılı KVKK Kararı

Bir oyuncak perakendecisi veri sorumlusunun veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 22/07/2020 tarih ve 2020/567 sayılı Karar Özeti

Karar Tarihi : 22.07.2020

Karar No : 2020/567

Konu Özeti : Bir oyuncak şirketinin veri ihlal bildirimini

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Kötü niyetli kullanıcılar tarafından, başka internet sitelerinden elde edilen kullanıcı adı ve şifrelerin, veri sorumlusunun internet sitesinde yer alan “Üye Girişi” sekmesinde denenerek 29 adet müşterinin hesabına yetkisiz erişim gerçekleşmesi suretiyle meydana geldiği,
- İhlalden etkilenen kişisel verilerin 29 müşteriye ait ad, soyad, e-posta adresi, telefon numarası, kayıtlı adres, müşteri işlem kategorisinde daha önce satın alınan ürün bilgilerinin olduğu,
- Markaya ilişkin kurulmuş olan uyarılar doğrultusunda herhangi bir sitede markanın kullanılması halinde, Şirketin Bilgi İşlem Departmanına bir bildirim düştüğü ve bu bildirim ile adı geçen siteye yönlendirme yapılmakta olduğu,
- Şirkete ulaşan bir bildirim doğrultusunda bir internet sitesinde, veri sorumlusunun markasına ait 29 adet hesap ile ilgili bir içerikle karşılaşıldığı,
- Söz konusu içeriğe erişimin, ancak ilgili siteye üye olunduğu takdirde sağlanabildiği,
- Söz konusu internet sitesi yöneticilerine bir ihtar gönderilerek internet sitesinde yer alan ihlale konu sayfanın kaldırılmasının sağlandığı

ifadelerine yer verilmiştir.

Söz konusu bildirim incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 22/07/2020 tarih ve 2020/567 sayılı Kararı ile;

- Kişisel hesaplara erişim hususunda veri güvenliğinin sağlanması amacıyla kullanıcı kimliklerinin doğrulanması gerekmekte olup veri sorumlusunun veri ihlali öncesinde alması gereken güvenlik

önlemlerinden olan iki faktörlü kimlik doğrulama yöntemini (SMS/Captcha) veri ihlali sonrasında yayına almayı planladığı dikkate alındığında veri sorumlusunun veri güvenliğini sağlamaya yönelik gerekli teknik tedbirleri almadığı,

- İhlalden etkilenen ilgili kişilerin hesaplarının şifreleri incelendiğinde müşteriler tarafından kullanılan şifrelerin sadece rakamlardan ya da sadece harf dizilerinden oluşabildiği, müşterilere hesap açılırken müşterilerin güçlü şifre oluşturması için zorlanmadığı,

- Veri sorumlusu nezdinde gerçekleşen ihlal sırasında web uygulama güvenlik duvarının (WAF) yetkisiz erişim işlemi saldırı ya da normal kullanıcı girişi olup olmadığını tespit edene kadar saldırganların belli bir miktarda hesaba yetkisiz erişim sağlayabildiği dikkate alındığında veri sorumlusunun uygulama güvenliğini sağlayamadığı

hususları dikkate alındığında 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik tedbirleri almayan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 75.000 TL idari para cezası uygulanmasına,

- Kurulun 24/01/2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde veri sorumlusunun bildirimde bulunmadığı; ancak yaşanan 1 günlük bir gecikmenin pandemi süreci nedeniyle makul olduğuna ve bu çerçevede veri sorumlusu hakkında yapılacak bir işlem bulunmadığına,

- İlgili kişilere yapılan bildirim 18/09/2019 tarih ve 2019/271 sayılı Kurul Kararının gerekliliklerini tam anlamıyla karşılamadığı dikkate alındığında, veri sorumlusunun Kişisel Verileri Koruma Kurulunun 18/09/2019 tarih ve 2019/271 sayılı Kararına uygun bir şekilde ilgili kişilere ihlale ilişkin bildirim yapması hususunda talimatlandırılmasına

karar verilmiştir.

2020/560 sayılı KVKK Kararı

Site Yönetimlerine ilişkin 6698 sayılı Kişisel Verilerin Korunması Kanunu ile 634 sayılı Kat Mülkiyeti Kanunu çerçevesinde Kişisel Verileri Koruma Kurulu'nun 22.07.2020 tarihli ve 2020/560 sayılı Kararı'nda yer alan değerlendirmeler

Karar Tarihi : 22.07.2020

Karar No : 2020/560

Konu Özeti : Site Yönetimlerine ilişkin 6698 sayılı Kişisel Verilerin Korunması Kanunu ile 634 sayılı Kat Mülkiyeti Kanunu çerçevesinde Kişisel Verileri Koruma Kurulu'nun 22.07.2020 tarihli ve 2020/560 sayılı Kararı'nda yer alan değerlendirmeler

Kişisel Verileri Koruma Kurulu'na (Kurul) iletilen bir şikâyet dilekçesi ile ilgili olarak iddialara konu Site Yönetimi hakkında başlatılan res'en inceleme neticesinde Kurul tarafından alınan 22.07.2020 tarih ve 2020/560 sayılı kararda şikâyet ve resen inceleme konusu hususlara ilişkin yapılan değerlendirmelerin yanı sıra Site Yönetimlerinin 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) karşısındaki durumuna ilişkin değerlendirmelere de yer verilmiş olup buna göre söz konusu kararda;

- 6698 sayılı Kanunun "Tanımlar"ı düzenleyen 3'üncü maddesinde veri sorumlusunun, "*kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*"yi ifade ettiği,
- Öte yandan, 634 sayılı Kat Mülkiyeti Kanunu'nun; 27'nci maddesinin, "Ana gayrimenkul, kat malikleri kurulunca yönetilir ve yönetim tarzı, kanunların emredici hükümleri saklı kalmak şartıyla bu kurul tarafından kararlaştırılır." hükmünü, 28'inci maddesinin birinci fıkrasının, "*Yönetim planı yönetim tarzını, kullanma maksat ve şeklini yönetici ve denetçilerin alacakları ücreti ve yönetime ait diğer hususları düzenler. Yönetim planı, bütün kat maliklerini bağlayan bir sözleşme hükmündedir.*" hükmünü, aynı maddenin dördüncü fıkrasının, "*Yönetim planı ve bunda yapılan değişiklikler, bütün kat malikleriyle onların külli ve cüzi haleflerini ve yönetici ve denetçileri bağlar.*" hükmünü, 32'nci maddesinin, "Ana gayrimenkul kat malikleri kurulu tarafından, sözleşme, yönetim planı ve kanun hükümleri uyarınca verilecek kararlara göre yönetilir. Bütün kat malikleriyle külli ve cüzi halefleri, yönetici ve denetçiler, kat malikleri kurulunun kararlarına

uymakla yükümlüdürler. Ana gayrimenkulün kullanılmasından veya yönetiminden dolayı kat malikleri arasında veya bunlarla yönetici ve denetçiler arasında veya denetçilerle yöneticiler arasında çıkan anlaşmazlıklar, kat malikleri kurulunca çözülür ve karara bağlanır..." hükmünü, 34'üncü maddesinin birinci fıkrasının, "Kat malikleri, ana gayrimenkulün yönetimini kendi aralarından veya dışardan seçecekleri bir kimseye veya üç kişilik bir kurula verebilirler; bu kimseye (Yönetici), kurula da (Yönetim kurulu) denir." hükmünü, aynı maddenin beşinci fıkrasının, "Yönetici her yıl kat malikleri kurulunun kanuni yıllık toplantısında yeniden atanır; eski yönetici tekrar atanabilir." hükmünü amir olduğu,

- Bu hükümlere göre; gayrimenkulün bütünü için söz sahibi olan birim kat malikleri kurulu olup kat malikleri kurulunun, yönetici de dâhil kat maliklerini bağlayan bir sözleşme hüviyetinde olan yönetim planının içeriği ve kapsamını belirleyen merci olduğu ve yöneticinin görevinin, kat malikleri kurulunun aldığı kararlar çerçevesinde, bu kararları uygulayıcı olarak faaliyet göstermekten ibaret bulunduğu,
- Aynı şekilde, 634 sayılı Kanun'un 35'inci maddesi gereği, yöneticinin görevlerinin yönetim planında belirtildiği ve yönetim planında aksine hüküm olmadıkça yöneticiye tevdi edilen vazifelerden bir tanesinin de kat malikleri kurulunca verilen kararların yerine getirilmesi olduğu,
- Aynı Kanun'un 38'inci maddesinin birinci fıkrasında yöneticinin kat maliklerine karşı aynen bir vekil gibi sorumlu olduğunun belirtilmiş olduğu ve bahse konu Kanun'un 40'inci maddesinin, yöneticinin kaide olarak vekilin haklarına sahip olduğu hükmünü haiz olduğu,
- Öte yandan, bahse konu Kanun'un 41'inci maddesinde, kat malikleri kurulunun, yöneticinin bu görevdeki davranışlarını devamlı olarak denetleyeceği ve haklı bir sebebin ortaya çıkması hâlinde yöneticiyi her zaman değiştirebileceği düzenlemesine yer verildiği,
- Yöneticinin devamlı olarak kat malikleri kurulunun denetimi altında olduğu, kat malikleri kuruluna hesap vermesinin ve haklı sebebin varlığı hâlinde her zaman değiştirilebilmesinin, ana gayrimenkul üzerindeki asıl söz sahibinin kat malikleri kurulu olduğunu gösterdiği,
- Ayrıca, 634 sayılı Kanun'un 35'inci maddesinin birinci fıkrasında yöneticinin görevlerinin sayıldığı, aynı maddenin ikinci fıkrası uyarınca; yönetici ataması yapılmayan gayrimenkullerde birinci fıkrada sayılan işlerin yapılması noktasında kat maliklerinin müştereken sorumlu tutulduğu, müştereken sorumluluğun söz konusu olduğu hâllerde birden fazla kişinin; bir borcun ödenmesinde ve zararın giderilmesinde kendi payları oranında sorumluluğu paylaştığı,
- Yine 634 sayılı Kanun'un 34'üncü maddesinin ikinci fıkrasının; "Ana gayrimenkulün sekiz veya daha fazla bağımsız bölümü varsa, yönetici atanması mecburidir." hükmünü amir olduğu, kat mülkiyetine konu

gayrimenkulün bağımsız bölüm sayısının sekizden az olması durumunda yönetici atama zorunluluğunun bulunmadığının görüldüğü, sekiz bağımsız bölümden az bağımsız bölüme sahip bir gayrimenkulde yöneticinin atanmaması ihtimalinin varlığından da anlaşılacağı üzere; yöneticinin yahut yönetim kurulunun her hal ve şartta karşımıza çıkan bir yapı olmadığı, buna karşın kat malikleri kurulunun, bu kurulu oluşturan şahıslardan bağımsız olarak tamamen gayrimenkulün bağımsız bölümlerinin varlığından kaynaklanan bir yapı görünümü arz ettiği, sekiz bağımsız bölümden fazla olsun ya da olmasın her gayrimenkulün bağımsız bölümleri üzerinde kurulan mülkiyet sonucu oluşan kat malikleri kurulunun, mülkiyet hakkından kaynaklanan bir topluluk olduğu,

- 634 sayılı Kanun'un 20'nci maddesinin birinci fıkrası uyarınca, kat maliklerinin ortak giderlere kendi arsa payları oranında katılmakla yükümlü olduğu, aynı maddenin ikinci fıkrasında ise, gider ve avans payını ödemeyen kat maliki hakkında diğer kat maliklerinden her biri yahut yönetici tarafından dava açılabileceğinin ve icra takibi başlatılabileceğinin teminat altına alındığı,

- Bununla birlikte, 634 sayılı Kanun'un 66'ncı maddesi uyarınca toplu yapının, *"Bir veya birden çok imar parseli üzerinde, belli bir onaylı yerleşim plânına göre yapılmış veya yapılacak, alt yapı tesislerini, ortak kullanım yerlerini, sosyal tesis ve hizmetleri ile bunların yönetimi bakımından birbirleriyle bağlantılı birden çok yapıyı"* ifade ettiği, bahse konu Kanun'un 69'uncu maddesinin, blok yapıların her birinin, o blokta bulunan bağımsız bölüm maliklerinden oluşan blok kat malikleri kurulunca yönetileceği hükmünü haiz olduğu,

- Bu çerçevede, gerek veri sorumlusunun 6698 sayılı Kanun'da yer alan tanımının gerekse 634 sayılı Kanun'da yer alan düzenlemelerin bir arada değerlendirilmesinden; kat mülkiyetine konu olan gayrimenkulün bütünü için kararlar alan, işlerin nasıl yürütüleceğini belirleyen birimin kat malikleri kurulu olduğu, bununla birlikte; kat malikleri kurulunun tüzel kişiliği haiz olmaması dolayısıyla 6698 sayılı Kanun'un 3'üncü maddesindeki veri sorumlusu tanımının içerdiği kriterlerin tamamını taşımadığının görüldüğü, zira anılan tanımdan hareketle veri sorumlusu sıfatının bir gerçek yahut tüzel kişiye ait olabileceği sonucunun çıktığı, kat malikleri kurulunun tüzel kişiliğinin bulunmadığı hususunun çeşitli Yargıtay kararlarında da açıkça ifade edildiği (Yargıtay 1. Hukuk Dairesi T. 29.03.2004, E. 2004/3091, K. 2004/3556: *"Davada gerçek ve tüzel kişiler ya da bunların yasal temsilcileri taraf olma ehliyetine sahiptir. Apartman kat malikleri kurulunun (Yönetiminin) tüzel kişiliği ve bu nedenle taraf ehliyeti yoktur."* Yargıtay 1. Hukuk Dairesi E. 2007/10090, K. 2007/11914: *"Davada gerçek ve tüzel kişiler ya da bunların yasal temsilcileri taraf olma ehliyetine sahiptir. Apartman kat malikleri kurulunun (Yönetimin) tüzel kişiliği bu nedenle taraf ehliyeti yoktur."*),

- Ancak, durum böyle olsa bile 634 sayılı Kanun'un 35'inci maddesinde, yöneticinin, ana gayrimenkulün tamamını ilgilendiren tebligatı kabul etme yetkisi olduğunun belirtildiği ve kat malikleri kurulunun vekili olarak görev yapan yöneticinin bir gerçek kişi yahut bu konuda hizmet sunan şirketlerden profesyonel hizmet satın alınması durumunda ise tüzel kişi olabileceği,
- Bununla birlikte, her ne kadar yönetici kat malikleri kurulunun verdiği kararlarla bağlı olup bu kararlara uygun hareket etmek zorunda olsa da, her somut olay bakımından yöneticinin yahut yönetim kurulunun kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan bir rol üstlenmiş olması halinde ayrık durumların çıkabileceği, örneğin, bir site yönetiminin ayrı bir tüzel kişilik tarafından yürütülüyor olması durumunda, kişisel verilerin işlenmesi noktasında bu tüzel kişiliğin de veri sorumlusu olabileceği,
- Tüm bu açıklamalar doğrultusunda; Kanun'un "veri sorumlusu"na ilişkin getirdiği tanımın, hayatın olağan akışına uygunluğunun sağlanması ve pratikte ortaya çıkan sorunların çözülebilmesi adına geniş yorumlanması gerektiği; bu kapsamda her ne kadar tüzel kişiliği haiz olmasa da kural olarak apartman, site ve benzeri yapılar bakımından veri sorumlusu olarak kat malikleri kurulunun kabul edilebileceği, kat malikleri kurulunun ise Kanun'un veri sorumlusuna yüklediği yükümlülüklerin yerine getirilmesi bakımından bir kişiyi görevlendirebileceği, görevlendirilen bu kişinin yönetici olmasının mümkün olduğu gibi başka bir kat malikinin yahut iradi temsilcinin de olabileceği değerlendirilmekle beraber, uygulamada istisnai durumların da ortaya çıkabileceği gözetilerek nihai olarak kişisel veri işleme faaliyetinde veri sorumlusu sıfatını haiz olanların belirlenmesi için; her somut hadise açısından kişisel veri işlenmesine ilişkin kararları alan, veri kayıt sistemlerini kuran, uhdesinde bulunduran ve yöneten birimlerin tespit edilmesinin gerektiği değerlendirilmelerine yer verilmiştir.

2020/559 sayılı KVKK Kararı

Kişisel verilerin 108 sayılı Sözleşme dayanak gösterilerek yurt dışına aktarılması hakkında Kişisel Verileri Koruma Kurulunun 22/07/2020 tarih ve 2020/559 sayılı Karar Özeti

Karar Tarihi : 22.07.2020

Karar No : 2020/559

Konu Özeti : Kişisel verilerin 108 sayılı Sözleşme dayanak gösterilerek yurt dışına aktarılması hakkında karar

Otomotiv sektöründe faaliyet gösteren veri sorumlusu tarafından reklam/bilgilendirme amaçlı gönderilen bir kısa mesaj (SMS) hakkında ilgili kişinin şikayeti üzerine yürütülen inceleme sürecinde, veri sorumlusundan alınan savunma yazısında şirketleri tarafından pazarlama amacıyla işlenmesi yönünde rıza alınmış kişisel verilerin veri işleyen konumunda bulunan yurt dışındaki bir firmaya aktarılmasının ve sadece söz konusu hizmetin yerine getirilmesi amacıyla bu firma tarafından işlenmesinin, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 5 inci maddesinin (2) numaralı fıkrasının (f) bendi doğrultusunda “veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması” şartı kapsamında değerlendirildiğinin ifade edilmesine rağmen, aynı savunmada veri sorumlusunun “veri gizliliği metni”nin Şikayetçi tarafından onaylandığı diğer bir ifade ile verilerinin yurtdışına aktarımına rıza verildiğine yönelik bir önceki ifadesi ile çelişen açıklamaların yer aldığı tespit edilmiştir. Bu duruma istinaden Kişisel Verileri Koruma Kurulu’nun (Kurul) 08.07.2019 tarihli ve 2019/203 sayılı Kararı ile veri sorumlusu hakkında müşterilerinin kişisel verilerini yurtdışındaki veri tabanlarında saklaması ile ilgili olarak Kanunun 15 inci maddesinin (1) numaralı fıkrası kapsamında resen inceleme başlatılmasına karar verilmiştir.

Bu itibarla, 6698 sayılı Kanunun ilgili maddeleri hakkında veri sorumlusuna bilgi verilerek kişisel verilerin yurtdışına aktarılmasının Kanunun 9 uncu maddesindeki hangi hukuki gerekçeye dayandırıldığına dair açıklamaları ile konuya ilişkin tüm bilgi, belge ile kayıtların tarafımıza gönderilmesi talep edilmiştir. Konuya ilişkin veri sorumlusundan alınan savunma yazısında ise özetle;

- Şirket tarafından gerçekleştirilen dijital pazarlama iletişimlerinde web tabanlı bir yazılımın kullanıldığı, söz konusu yazılımın web tabanlı olması nedeniyle yazılım üzerinden müşterilerine e-posta/sms gönderimi yapılabilmesi için müşterilerin verilerinin sunucuları Avrupa Birliği üyesi bir ülkede bulunan bulut veri tabanına SFTP kullanılarak (Dış Kaynak Firma) aktarıldığı,
- Müşterilere ilişkin; (1) müşteri bilgisinin, (2) kendilerine e-posta ve SMS gönderim bilgisi dolayısıyla pazarlama bilgisinin ve (3) iletişim bilgisinin, dış kaynak firmaya aktarıldığı, Şirket tarafından yurtdışına herhangi bir özel nitelikli kişisel verinin ise aktarılmadığı,
- Kişisel verileri yurtdışındaki dış kaynak firma'ya aktarılan müşterilerden açık rızanın alındığı, söz konusu açık rızanın 2018 yılından itibaren güncellenmiş Müşteri Kişisel Verilerinin İşlenmesine İlişkin Aydınlatma Metni ve Rıza Metni ile alındığı,
- Veri işleyen konumundaki dış kaynak firmaya bu verilerin aktarılmasındaki hukuki gerekçenin ise Kanunun 5 inci maddesinin (2) numaralı fıkrasının (f) bendinde düzenlenen veri sorumlusu olarak Şirketin meşru menfaati için veri işleminin zorunlu olması şartına dayandığı,
- 6698 sayılı Kanunun 9 uncu maddesinde kişisel verilerin a) ilgili kişinin açık rızası ile ya da b) yeterli korumanın bulunması veya ilgili ülkede yeterli koruma bulunmuyorsa Kurulun izninin alınması suretiyle Kanunun 5 inci maddesinin (2) numaralı fıkrası ile 6 ncı maddesinin (3) numaralı fıkrasında belirtilen veri işleme şartlarına dayalı olarak yurtdışına aktarılabilmesinin düzenlendiği, Kurulun yabancı ülkede yeterli koruma bulunup bulunmadığına Kanunun 9 uncu maddesinin (4) numaralı fıkrasında yer alan hususlar çerçevesinde karar vereceğinin düzenlendiği, ancak Kurul tarafından bir yabancı ülkede yeterli koruma bulunup bulunmadığına henüz karar verilmemiş olduğu, bunun yanı sıra aynı maddenin (5) ve (6) numaralı fıkrasında kişisel verilerin yurtdışına aktarılmasında uluslararası sözleşmeler ile diğer kanun hükümlerinin saklı olduğunun ortaya konulduğu,
- “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi”nin (108 sayılı Sözleşme) iç hukuka aktarıldığı, tüm Avrupa Birliği üye devletlerinin 108 sayılı Sözleşmeye taraf olduğu, Türkiye'nin 108 sayılı Sözleşmenin taraflarına ilişkin “... Sözleşme'nin onaylanmasının geçerliliği bulunmayan “Kıbrıs Cumhuriyeti”nin anılan sözleşmeye taraf olan Güney Kıbrıs Rum Yönetimi tarafından temsil edildiği iddiasının herhangi bir biçimde kabulü anlamına gelmeyeceğini ve Türkiye’de sözde Kıbrıs Cumhuriyeti ile işbu Sözleşme kapsamında herhangi bir temasta bulunma yükümlülüğü getirmeyeceğini” beyan ettiği, bu beyan dışında 108 sayılı Sözleşme'nin taraflarına ilişkin Türkiye tarafından herhangi bir beyanda bulunulmadığı; Anayasanın 90 inci maddesinin son fıkrası uyarınca “usulüne göre yürürlüğe konulmuş Milletlerarası Antlaşmaların kanun hükmünde” olduğunun kabul edildiği, ayrıca ilgili fıkranın devamı hükmünde usulüne göre yürürlüğe konulmuş

temel hak ve özgürlüklere ilişkin Milletlerarası antlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyumsuzluklarda Milletlerarası antlaşma hükümlerinin esas alınacağı düzenlemesine yer verildiği dolayısıyla kişilerin temel hak ve özgürlüklerinden olan kişisel verilerin korunması hakkına ilişkin 108 sayılı Sözleşme ile diğer kanunlar arasında çıkan uyumsuzluklarda 108 sayılı Sözleşmenin esas alınması gerektiği kanısında olduğu,

- 108 sayılı Sözleşme'nin 12 nci maddesi uyarınca 108 sayılı Sözleşmenin taraflarına gerçekleştirilecek kişisel veri aktarımlarının (a) ve (b) bentlerinde sıralanan istisnalardan biri sağlanmadan yasaklanmaması veya özel izne tabi tutulmamasının 108 sayılı Sözleşmenin getirdiği açık kurallardan biri olduğu, Türkiye tarafından gerçekleştirilmiş herhangi bir sınırlandırma veya özel izne tabi tutulmaya ilişkin herhangi bir işlem bulunmadığı, bu kapsamda Kanununun 9 uncu maddesinin (5) ve (6) numaralı fıkraları da dikkate alındığında 108 sayılı Sözleşmenin 12 nci maddesine dayanılarak 108 sayılı Sözleşmenin Taraflarına veri aktarımı yapılmasına ilişkin herhangi bir hukuki sınırlandırma ve/veya engelin bulunmadığı kanısında olduğu,

- “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınırşan Veri Akışına İlişkin Protokol”ün 2 nci maddesinin (1) numaralı fıkrasında sınır aşan kişisel veri aktarımlarına ilişkin olarak taraf olmayanlara yapılacak aktarımlarda yeterli koruma sağlanıp sağlanmadığının değerlendirmesinin yapılacağı düzenlendiği, bu doğrultuda ilgili maddenin mefhumu muhalifinden taraf olanlara yönelik yeterli koruma değerlendirilmesinin yapılamayacağı anlaşıldığı, ek protokolün 2 nci maddesinin (2) numaralı fıkrasında ise (1) numaralı fıkraya hangi koşullarda çekince getirilebileceğinin düzenlendiği, buna karşın ülkemizin ilgili düzenleme hakkında herhangi bir beyanda bulunmadığı,

- Şirketin hukuki gerekçeler (6698 sayılı Kanununun 9 uncu maddesinin (5) ve (6) numaralı fıkraları ile 108 sayılı Sözleşmenin 12 nci maddesi) kapsamında 6698 sayılı Kanununun 9 uncu maddesinin (2) numaralı fıkrasının atfı ile 5 inci maddenin (2) numaralı fıkrasının (f) bendinde yer alan “ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması” hukuki gerekçesine dayanılarak gerekli tüm idari ve teknik tedbirler alınmak suretiyle veri işleyen konumundaki dış kaynak firmaya hukuka uygun olarak veri aktarımının yapıldığı

hususlarına yer verilmiştir. Resen inceleme konusu kapsamında veri sorumlusundan alınan bilgi ve belgelerin ilgili mevzuat çerçevesinde incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 22/07/2020 tarih ve 2020/559 sayılı Kararında aşağıdaki değerlendirmelere yer verilmiştir.

1. Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “**Kişisel Verilerin İşlenme Şartları**” başlıklı 5 inci maddesinin birinci fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, ikinci fıkrasında ise Kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümleri yer almaktadır.

Bu kapsamda kişisel veri işleme faaliyetinin öncelikli olarak açık rıza dışındaki işleme şartlarından birine dayanıp dayanmadığı değerlendirilmeli, eğer bu faaliyet Kanunda belirtilen açık rıza dışındaki şartlardan en az birine dayalı olarak gerçekleştirilemiyorsa, bu durumda veri işleme faaliyetinin devamı için kişinin açık rızasının alınması yoluna gidilmelidir. Açık rıza alınmasına gerek olmayan hallerden biri de resen incelemeye konu veri sorumlusu tarafından da belirtildiği üzere Kanunun 5 inci maddesinin (2) numaralı fıkrasının (f) bendinde yer alan “*ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması*” şeklinde belirtilen durumdur. Anılan bendin uygulanabilmesi için kişisel verilerin korunmasına ilişkin temel ilkelere uyulması, veri sorumlusunun meşru menfaati ile ilgili kişinin temel hak ve özgürlüklerinin gözetilmesi ve yarışan menfaatler arasında yapılacak olan değerlendirmenin sonucunda kişisel verilerin belirtilen fıkra kapsamında işlenip işlenemeyeceğine karar verilmesi gerekmektedir.

Bu minvalde, Kanunun 5 inci maddesinin (2) numaralı fıkrasının (f) bendinin uygulanabilmesi için iki aşamalı bir testin ele alınması gerekir. Yapılacak olan ilk değerlendirmede veri sorumlusunun meşru menfaatinin varlığı tespit edilmeli, ikinci olarak da, bu menfaatin ilgili kişinin temel hak ve özgürlüklerine zarar verip vermediği belirlenmelidir. Ancak, resen incelemeye taraf olan veri sorumlusu tarafından açık rıza dışındaki kişisel veriler açısından yurt dışına aktarımda Kanunun 5 inci maddesinin (2) numaralı fıkrasının (f) bendindeki işleme şartı dayanak gösterilirken meşru menfaatin ne olduğu hakkında ve bu menfaati ile kişilerin temel hak ve özgürlükleri arasında bir

denge testi uygulanıp uygulanmadığına ilişkin herhangi bir açıklamaya yer verilmediğinden, kişisel verilerin veri sorumlusu tarafından yurt dışına aktarılmak suretiyle işlenmesinde geçerli bir meşru menfaatin bulunduğu kanaati hasıl olmamıştır.

2. Bununla birlikte, 6698 sayılı Kanununun 3'üncü maddesinin (1) numaralı fıkrasının (a) bendinde tanımına yer verilen "açık rıza"nın özgür irade ile açıklama, bilgilendirmeye dayanma ve belirli bir konuya ilişkin olma şeklinde üç unsuru bulunmaktadır. Bu kapsamda eğer birden çok kategoriye ilişkin verinin işlenmesine dair açık rıza beyanında bulunulacaksa, açık rızanın hangi verilerin hangi amaçlarla işleneceği gibi hususlara ilişkin verilmiş olması gerekmektedir. Veri sorumlusunun, veriyi kullanımı sonrasında gerçekleştireceği ikincil işlemler için ise (örneğin yurtdışına veri aktarımı gibi) ayrıca açık rıza alması gerekmektedir. Bununla birlikte, kişisel veri işleme faaliyeti, Kanunda bulunan açık rıza dışındaki şartlardan birine dayanıyorsa, ilgili kişiden açık rıza alınması yoluna gidilmeyecektir. Nitekim, veri işleme faaliyetinin, açık rıza dışında bir dayanakla yürütülmesi mümkün iken açık rızaya dayandırılması, aldatıcı ve hakkın kötüye kullanımı niteliğinde olacaktır.

Veri sorumlusunun, Kurula verdiği savunma yazısında, kişisel verilerin işlenmesinin hukuki sebebinin "ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" şartına dayandığını belirtmekle birlikte; ilgili kişilere sunduğu aydınlatma ve rıza metninde "... Şirketimiz tarafından sunulan ürün ve hizmetlerin sizlerin beğeni, kullanım alışkanlıkları ve ihtiyaçlarınıza göre özelleştirerek sizlere önerilmesi ve tanıtılması, kabulünüz kapsamında paylaşmış olduğunuz iletişim bilgilerinize reklam, promosyon vb ticari elektronik ileti gönderilmesi, saklanması ve ... gönderim sağlanması için hizmet aldığı üçüncü kişilerle paylaşılması amaçlarıyla işbu metni kabul etmeniz halinde vermiş olduğunuz açık rızanız kapsamında işlenebilecektir." şeklinde bir bilgilendirmede bulunduğu dikkate alındığında, kişisel veri işleme faaliyetinin asıl olarak ve yalnızca ilgili kişilerin açık rızalarına dayanılarak gerçekleştirildiği izlenimine neden olduğu değerlendirilmiştir.

Bahse konu savunma yazısının devamında ise, yurt dışına veri aktarımının 6698 sayılı Kanununun 9 uncu maddesinin (2) numaralı fıkrasının atfı ile 5 inci maddenin (2) numaralı fıkrasının (f) bendinde yer alan "ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" hukuki gerekçesine dayanılarak dış kaynak firmaya yapıldığı; pazarlama iletişimlerine izin vermiş kişilere/müşterilere e-posta/sms gönderimi yapılabilmesi için müşteri verilerinin sunucuları Avrupa Birliği üyesi ülkede bulunan bir bulut veri tabanına aktarıldığı ifadelerine yer verildiği görülmüştür. Ancak, aydınlatma metninde ve açık rıza metninde ilgili kişiler tarafından pazarlama amaçlı ileti gönderilmesine rıza verilmesi

halinde bu kişisel verilerin yurtdışına bulunan bir firmaya aktarılacağına ilişkin herhangi bir açıklamaya yer verilmediğinden yurtdışına veri aktarımının veri sorumlusunun Kanunun 5 inci maddesinin (2) numaralı fıkrasında belirtilen açık rıza dışındaki meşru menfaatleri kapsamında mı yoksa, ilgili kişilerin açık rızalarına istinaden mi gerçekleştirildiğinin anlaşılır olmadığı ya da söz konusu kişisel verilerin hangilerinin meşru menfaat çerçevesinde hangilerinin ise ilgili kişilerin açık rızalarına istinaden işlendiğinin açıkça belirtilmemiş olduğu kanaatine varılmıştır.

3. Kanunun “**Kişisel Verilerin Yurt Dışına Aktarılması**” başlıklı 9 uncu maddesinde de kişisel verilerin ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamayacağı ancak, kişisel verilerin 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede; a) Yeterli korumanın bulunması, b) Yeterli korumanın bulunmaması durumunda Türkiye’deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kişisel Verileri Koruma Kurulu’nun (Kurul) izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılacağı hükümleri düzenlenmektedir. Anılan maddenin devamında ise,

“(3)Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir.

(4) Kurul yabancı ülkede yeterli koruma bulunup bulunmadığına ve ikinci fıkranın (b) bendi uyarınca izin verilip verilmeyeceğine; a) Türkiye’nin taraf olduğu uluslararası sözleşmeleri, b) Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu, c) Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işleme amaç ve süresini, ç) Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını, d) Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri, değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir.

(5) Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye’nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir.

(6) Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.” hükümlerine yer verilmiştir.

Veri sorumlusu tarafından Kurula sunulan bilgi, belge ve açıklamaların incelenmesi neticesinde, veri sorumlusunun dijital pazarlama iletişimlerinde web tabanlı bir yazılım kullandığı, söz konusu yazılım üzerinden müşterilerine e-posta/sms gönderimi yapılabilmesi için müşteri verilerini (müşterilere ilişkin; (1) müşteri bilgisi, (2) kendilerine e-posta ve SMS gönderim bilgisi dolayısıyla

pazarlama bilgisi ve (3) iletişim bilgilerini) sunucuları Avrupa Birliği üyesi bir ülkede bulunan ,bulut veri tabanına aktardığı anlaşılmıştır.

108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin (108 sayılı Sözleşme) “Kişisel Verilerin Sınır Ötesi Akışı ve İç Hukuk” başlıklı 12 nci maddesinde ise;

“(1) Otomatik işleme konu olan veya otomatik işleme konu olmak üzere toplanmış olan kişisel verilerin her türlü yoldan ulusal sınırların ötesine transferinde aşağıdaki hükümler uygulanır.

(2) Bir Taraf, münhasıran özel yaşamın korunması amacıyla kişisel verilerin diğer bir Tarafa sınır ötesi akışını yasaklayamaz veya özel müsaadeye tabi tutamaz.

(3) Bununla birlikte her bir Taraf, 2. fıkradaki hükümlere aşağıdaki durumlarda istisnalar getirebilir:

(a) Kendi mevzuatının, belli kişisel veri veya otomatik kişisel veri dosyası kategorileri için, bu verilerin veya dosyaların doğasından kaynaklanan özel düzenlemeler içermesi, diğer Tarafın düzenlemelerinin ise eşdeğer bir koruma içermemesi durumunda;

(b) Bu transferin bir Tarafın ülkesinden, bir diğer Taraf üzerinden Taraf olmayan bir devletin ülkesine yapılması durumunda, bu bendin başında atıfta bulunulan Tarafın mevzuatının boşluklarından yararlanmak üzere yapılacak bu tür transferleri engellemek amacıyla” hükümleri yer almaktadır.

Veri sorumlusu Kurula verdiği savunmasında; müşteri bilgilerinin dış firmaya aktarılmasındaki hukuki gerekçenin Kanunun 5 inci maddesinin (2) numaralı fıkrasının (f) bendi kapsamındaki “veri sorumlusunun meşru menfaati için veri işlemenin zorunlu olması” olduğu, Kanunun 9 uncu maddesindeki gerekçesine ilişkin olarak ise; tüm Avrupa Birliği üye devletlerinin iç hukukumuzda aktarılan 108 sayılı Sözleşmeye taraf olduğu, Anayasanın 90 ıncı maddesi uyarınca “usulüne göre yürürlüğe konulmuş Milletlerarası Antlaşmaların kanun hükmünde” olduğunun kabul edildiği ve Milletlerarası antlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyumsuzluklarda Milletlerarası antlaşma hükümlerinin esas alınacağı düzenlemesine yer verildiği, bu doğrultuda kişilerin temel hak ve özgürlüklerinden olan kişisel verilerin korunması hakkına ilişkin 108 sayılı Sözleşme ile diğer kanunlar arasında çıkan uyumsuzluklarda 108 sayılı Sözleşmenin esas alınması gerektiği kanısında olunduğu, Kanun hükmünde olan 108 sayılı Sözleşmenin, serbest aktarım ilkelerini benimseyen 12 inci maddesinin (3) numaralı fıkrasının (a) ve (b) bentleri istisnasına dayanılan herhangi bir sınırlandırma veya özel izne tabi tutulmaya ilişkin şu zamana kadar Türkiye tarafından yapılan herhangi bir işlem bulunmadığı, bu kapsamda Kanunun 9 uncu maddesinin (5) ve (6) numaralı fıkraları da dikkate alındığında 108 sayılı Sözleşmenin 12 nci maddesine dayanılarak

108 sayılı Sözleşmenin Taraflarına veri aktarımı yapılmasına ilişkin herhangi bir hukuki sınırlandırma ve/veya engelin bulunmadığı kanısında bulunduğu, bununla birlikte “*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol*”un 2 nci maddesinin (2) numaralı fıkrasında (1) numaralı fıkraya *hangi koşullarda çekince getirilebileceğinin düzenlendiği, buna karşın ülkemizin ilgili düzenleme hakkında herhangi bir beyanda bulunmadığı, Kurul tarafından yeterli koruma sağlayan ülkelere ilişkin somut değerlendirmenin de henüz yapılmamış olduğu, bu minvalde 108 sayılı Sözleşme’nin Taraflarından olan bir ülkede bulunan Dış Kaynak Firmaya yapılan kişisel veri aktarımının 108 sayılı Sözleşme ve ilgili Ek Protokol’de belirtilen hukuki gerekçelerle yapıldığı ifade edilmiştir.*

Öncelikle, 108 sayılı Sözleşmenin 12 nci maddesinde, Sözleşmeye taraf devletlerin yalnızca özel hayatın korunması gerekçesiyle diğer taraf devletlere gerçekleşecek kişisel veri aktarımlarını yasaklayamayacaklarını veya özel bir izin öngörmek suretiyle kısıtlayamayacaklarının öngörüldüğünü belirtmek yerinde olacaktır. 108 sayılı Sözleşmeye İlişkin Açıklayıcı Rapor’un (Açıklayıcı Rapor) ikinci fıkrasında, bu düzenlemenin amacının Sözleşmeye taraf ülkelerin kişisel verilerin korunması bakımından yeterli düzeyde güvenceleri sağladığı yönündeki ön kabulden hareketle taraf ülkeler arasında veri akışının kolaylaştırılması olduğu, bununla birlikte, bu hükmün taraf devletler arasındaki veri akışının bildirim tabi kılınmasına veya tarafların iç hukuklarında belirli durumlarda yurt içinde veya sınır aşan nitelikte aktarımları yasaklamaya yönelik düzenlemeler yapabilme imkanını ortadan kaldırmadığı öngörülmektedir. Bahse konu Açıklayıcı Raporda Sözleşmenin 12 nci maddesinin Avrupa Birliği’ndeki (AB) uygulamasına ilişkin olarak ise, AB’nin gerek mülga 95/46/AT sayılı Direktif gerek 27/04/2016 tarih ve 2016/679 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (Genel Veri Koruma Tüzüğü-GVKT) hükümleri uyarınca 108 sayılı Sözleşmeye taraf olan ülkeleri herhangi bir başka değerlendirmede bulunmadan yeterli korumaya sahip ülke olarak nitelendirmediği ve Sözleşmeye taraf olmayı yalnızca yeterlilik değerlendirmesinde dikkate alacağı bir kriter olarak kabul ettiği hususlarına yer verildiğini de belirtmekte fayda görülmektedir.

Bu kapsamda, Kanunun 9 uncu maddesinin ikinci fıkrasında öngörülen düzenleme uyarınca, Kurul tarafından güvenli ülke olarak ilan edilmemiş ülkelere ilgili kişinin açık rızası olmaksızın yapılacak kişisel veri aktarımlarının ancak Kanunun 5 inci maddesinin ikinci fıkrasında veya 6 ncı maddesinin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve tarafların yeterli korumayı yazılı olarak taahhüt etmeleri ve Kurul tarafından aktarıma izin verilmesi halinde gerçekleşmesine imkan tanındığını belirtmek yerinde olacaktır.

4. Kanunun 9 uncu maddesinin 4 üncü fıkrasının (a) bendinde, Kurulun veri aktarımına izin verip vermeyeceğine ilişkin değerlendirilmede ülkemizin taraf olduğu uluslararası sözleşmelerin de dikkate alınacağı hükme bağlanmıştır. Kişisel verilerin aktarılacağı ülkenin 108 sayılı Sözleşmeye taraf olması Kurulun değerlendirmesine esas teşkil edecek unsurlardan sadece bir tanesini oluşturmakta olup bu durum yeterli korumanın bulunduğu ülkelerin Kurulca belirlenmesinde kullanılmak üzere Kurulun 02.05.2019 tarihli ve 2019/125 sayılı Kararında da kabul edilen kriterler arasında yer almaktadır. Bununla birlikte anılan maddede aktarıma konu kişisel verilerin niteliği ile işleme amaç ve süresi, aktarımın yapılacağı ülkedeki veri koruma mevzuatı ve uygulaması ve bu ülkedeki veri sorumlusu veya veri işleyenin taahhüt edeceği önlemler gibi özellikle kişisel verilerin etkin bir biçimde korunmasını sağlamaya yönelmiş hususlar ve ülkemiz ile aktarımın yapılacağı ülke arasında veri aktarımına ilişkin karşılıklılık durumu da Kurulun değerlendirmesinde göz önünde bulundurulmuş diğer hususlardır.

Bu minvalde, sözleşmeye taraf devletlerin iç hukuklarında belirli durumlarda yurt dışına veri aktarımını yasaklamaya yönelik düzenleme yapabileceğine dair “108 sayılı Sözleşmeye İlişkin Açıklayıcı Rapor”da yer alan açıklama ile Kurulun yurt dışına veri aktarımına izin vermesine ilişkin yapacağı değerlendirmede gerek 108 sayılı Sözleşme gibi ülkemizin taraf olduğu uluslararası sözleşmeleri gerek kişisel verilerin korunması veya özel hayatın gizliliğini koruma amacını taşımadan aktarımın yapılacağı ülke ile karşılıklılık halini dikkate alacağına ilişkin Kanunun 9 uncu maddesinde yer verilen düzenleme göz önünde bulundurulduğunda 6698 sayılı Kanunda öngörülen kişisel veri aktarım rejiminin 108 sayılı Sözleşme ile uyumlu olduğu değerlendirilmektedir.

5. Kanunun 9 uncu maddesinin (6) numaralı fıkrasında ise “*Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.*” hükmüne yer verilmektedir. Bilindiği üzere, Anayasanın 90 ıncı maddesinde yer alan düzenleme uyarınca yürürlüğe konulmuş uluslararası antlaşmaların kanun hükmünde olduğu, bu anlamda 108 sayılı Sözleşmenin de hukukumuzda kanun niteliğini haiz olduğu, Anayasanın 90 ıncı maddesine 5170 sayılı Kanunun 7 nci maddesi ile yapılan ekleme ile temel hak ve özgürlüklere ilişkin uluslararası antlaşmalarla kanunların aynı konuya ilişkin farklı düzenlemeleri öngörmesi halinde uluslararası antlaşma hükümlerinin esas alınacağı öngörülmektedir. Ancak, bu maddenin gerekçesinde “*uygulamada usulüne göre yürürlüğe konulmuş insan haklarına ilişkin milletlerarası antlaşmalar ile kanun hükümlerinin çelişmesi halinde ortaya çıkacak bir uyumsuzluğun varlığı halinde hangisine öncelik verileceği konusundaki tereddütlerin giderilmesi amacıyla 90 ıncı maddenin son fıkrasına hüküm eklenmektedir*” açıklamasına yer verildiği, bunun uygulanabilmesi için de söz konusu uluslararası antlaşma hükümlerinin doğrudan uygulanabilir olması gerektiği,

diğer bir ifadeyle antlaşma hükmünün “*yeterince açık, kesin, koşulsuz ve uygulaması için devletin ilave bir tedbir almasını gerektirmeyecek nitelikte*” olması gerektiği belirtildiğinden, doğrudan uygulanabilir olmayan daha soyut ve genel bir uluslararası antlaşma hükmü ile bir kanun hükmü arasında oluşacak bir uyuşmazlığın Anayasanın 90 ıncı maddesinin beşinci maddesinde yer alan düzenleme bağlamında bir çatışma teşkil etmeyeceği ve bu sebeple Anayasanın anılan hükmünün uygulama alanı bulmayacağı dolayısıyla genel nitelikteki uluslararası antlaşma hükmü ile kanun hükmünün çelişmesi halinde çelişen kanun hükmünün esas alınarak uygulanması gerektiği değerlendirilmektedir.

108 Sayılı Sözleşmenin 4 üncü maddesinin birinci fıkrası da “*her Taraf, kendi iç hukukunda işbu bölümde yer alan verilerin korunmasına ilişkin temel ilkelere işlerlik kazandırmak amacıyla gerekli önlemleri alır*” hükmünü içermektedir. Diğer bir ifadeyle Sözleşme hükümleri taraf devletlerin iç hukukunda doğrudan hüküm ve sonuç doğurmamakta, ulusal veri koruma düzenlemelerine hakim olması gereken temel ilkeleri ve bu düzenlemeler vasıtasıyla ilgili kişilere sağlanacak güvenceye ilişkin usul ve esasları belirlemektedir. “108 sayılı Sözleşmeye İlişkin Açıklayıcı Rapor”da da, Sözleşmenin doğrudan uygulanabilir nitelikte olmadığı ve bu sebeple taraf devletlerin veri koruma hükümlerini iç hukuklarına dahil etmekle yükümlü kılındıkları ifade edilmektedir. Dolayısıyla 108 sayılı Sözleşmenin 12 nci maddesinin ikinci fıkrasında yer alan ve tarafların münhasıran özel hayatın gizliliğinin korunması amacıyla diğer bir taraf ülkeye kişisel veri aktarımını yasaklayamayacağına veya izin koşuluna bağlayamayacağına ilişkin hükmünün doğrudan uygulanabilir nitelikte olmadığı, bu minvalde söz konusu hükmün ne Kanunun 9 uncu maddesinin (6) numaralı fıkrası ne de Anayasanın 90 ıncı maddesinin (5) numaralı fıkrası uyarınca öncelikle uygulama alanı bulamayacağı; diğer taraftan Kanunun 9 uncu maddesinde öngörülen düzenlemenin 108 sayılı Sözleşmenin 12 nci maddesine de aykırılık teşkil etmediği ve bu itibarla her iki düzenlemenin birbirini tamamlayıcı nitelikte olduğu dikkate alındığında, 108 sayılı Sözleşmeye taraf olmanın AB uygulamasında olduğu gibi 6698 sayılı Kanun kapsamında güvenli ülke statüsü tayini bakımından tek başına yeterli olmadığı ancak Kurul tarafından yapılacak değerlendirmede olumlu bir unsur teşkil edeceğini belirtmekte fayda görülmektedir.

Bu itibarla, öncelikle 108 sayılı Sözleşmenin başlı başına kişisel verilerin yurt dışına aktarımına cevaz vermediği, veri sorumlusunun yurt dışına veri aktarımı yaparken Kanunun 9 uncu maddesinde belirtilen şartları sağlamaması halinde hukuka aykırı bir veri işleminin gündeme geleceği, bu minvalde açık rıza alınmasını gerektiren kişisel verilerin yurtdışına veri aktarımının yapılabilmesi için ilgili kişinin açık rızasının alınması; Kanunda belirtilen diğer kişisel veri işleme şartlarına

dayanılarak yurtdışına veri aktarımının yapılabilmesi için ise Kanunun 5 inci maddesinin (2) numaralı fıkrasında ve 6 ncı maddesinin (3) numaralı fıkrasında belirtilen şartlardan birinin varlığı, tarafların yeterli bir korumayı taahhüt etmeleri ve Kurul tarafından izin verilmesi halinde yurt dışına kişisel veri aktarımının gerçekleşebileceğini belirtmek gerekmektedir.

Veri sorumlusunun Kurumumuza verdiği bilgi, belge ve açıklamalardan, ilgili kişilerin pazarlama amacıyla işlenen kişisel verilerini açık rıza kapsamında, bunun dışında kalan kişisel verilerinin ise 6698 sayılı Kanunun 9 uncu maddesinin (2) numaralı fıkrasının atfı ile 5 inci maddenin (2) numaralı fıkrasının (f) bendinde yer alan **“ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması”** hukuki gerekçesi kapsamında 108 sayılı sözleşmenin 12 nci maddesine dayanılarak aktarıldığı anlaşılmıştır. Ancak, veri sorumlusu 108 sayılı sözleşme kapsamında aktarım yaptığını ifade ederken ilgili dış kaynak firmaya aktarım yapılabilmesine ilişkin taahhütname hazırlandığına/hazırlanacağına dair herhangi bir bilgiyi Kurula sunmamıştır. Kurum kayıtlarında da veri sorumlusu tarafından Karar tarihi itibarıyla taahhütnameye ilişkin herhangi bir başvuruya rastlanmamıştır.

Sonuç itibarıyla, veri sorumlusu tarafından gerek açık rızanın usulüne uygun ayrı bir metin olarak düzenlenmemiş olması gerek yurt dışına aktarım yapılacağına ilişkin ilgili kişilere açık ve anlaşılır şekilde beyan edilmemiş olması; öte yandan açık rıza dışındaki işleme şartlarına bağlı olarak gerçekleşecek yurt dışına aktarımlarda ise veri sorumlusu tarafından meşru menfaate ilişkin denge testinin yapılmamış olması ve aktarım yapılan ilgili firma ile yazılı taahhütname yapılarak Kurulun izni alınmak üzere taahhütnamenin bir örneğinin Kurumumuza iletilmemiş olması sebepleriyle, bahse konu aktarımın Kanunun 9 uncu maddesinde belirtilen şartları sağlamadığı dolayısıyla hukuka aykırı bir veri işlemenin mevcut olduğu kanaatine varılmıştır.

6. Diğer taraftan, Kanunun “Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi” başlıklı 7 nci maddesinde, *“(1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir. (2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır. (3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir.”* hükmü yer almaktadır. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik’in 7 nci maddesinde de Kanunun 5 inci ve 6 ncı maddelerinde yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin veri

sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi gerektiği düzenlemesine yer verilmektedir.

Bu kapsamda, veri sorumlusu tarafından yurt dışına veri aktarımı konusunda ilgili kişilerden hukuka uygun bir açık rıza alınmamış olduğu, açık rıza dışındaki işleme şartlarından ise geçerli bir meşru menfaatin bulunduğu dair denge testinin yapılmamış olduğu, bununla birlikte yurt dışına aktarımda Kanunun 9 uncu maddesine uygun olarak taahhütname hazırlanmamış ve Kurulun izni alınmak üzere Kurumumuza iletilmemiş olduğu dolayısıyla yurt dışına veri aktarmak suretiyle hukuka aykırı veri işlemenin söz konusu olduğu kanaatine varıldığından, veri sorumlusunun yurt dışına veri aktarımında geçerli bir hukuki işleme şartının bulunmaması sebebiyle Kanunun 7 nci maddesinin (1) numaralı fıkrası ve ilgili Yönetmelik uyarınca, bu kişisel verilerin silinmesi veya yok edilmesi gerektiği kanaatine varılmıştır.

7. Öte yandan, bilindiği üzere Kanunun “**Veri Sorumlusunun Aydınlatma Yükümlülüğü**” başlıklı 10 uncu maddesi, veri sorumlusu veya yetkilendirdiği kişinin, kişisel verilerin elde edilmesi sırasında ilgili kişilere “a) Veri sorumlusunun ve varsa temsilcisinin kimliği, b) Kişisel verilerin hangi amaçla işleneceği, c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi, d) 11 inci maddede sayılan diğer hakları” konusunda bilgi vermekle yükümlü olduğunu içermektedir. “Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ” de de (Aydınlatma Tebliği) veri sorumluları veya yetkilendirdiği kişiler tarafından aydınlatma yükümlülüğü kapsamında uyulacak usul ve esaslar belirlenmiştir.

Resen incelemeye konu olayda, veri sorumlusunun açık rıza alımında 2018 yılından itibaren güncellenmiş Aydınlatma Metni ve Rıza Metnini kullandığı görülmüş olup bahse konu metnin incelenmesi neticesinde;

- Aydınlatma metninin Kanunun 10 uncu maddesi ve Aydınlatma Tebliğinde belirtilen detayda düzenlenmediği,
- Aydınlatma Tebliği'nin 5 inci maddesinin (f) bendinde kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerektiği düzenlenmektedir. Veri sorumlusunun açık rıza şartına dayalı olarak gerçekleştirilecek veri işleme faaliyetinin, aydınlatma metninin içerisinde ayrı bir başlık altında ancak aydınlatma metni ile birlikte düzenlenmiş olduğu görüldüğünden, söz konusu uygulamanın Tebliğ'in 5 inci maddesine aykırılık oluşturduğu,

• Aydınlatma Tebliği'nin 5 inci maddesinin (h) bendinde; *“Kanununun 10 uncu maddesinin birinci fıkrasının (ç) bendinde yer alan “hukuki sebep” ten kasıt, aydınlatma yükümlülüğü kapsamında kişisel verilerin Kanununun 5 ve 6 ncı maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiğidir. Aydınlatma yükümlülüğünün yerine getirilmesi esnasında hukuki sebebin açıkça belirtilmesi gerekmektedir”* hükmüne yer verilmiştir. Veri sorumlusunun düzenlediği aydınlatma metninde ise kişisel verilerin toplanmasının hukuki gerekçesinin Kanununun 5 ve 6 ncı maddelerinde belirtilen işleme şartları olduğu şeklinde genel nitelikte ifadeye yer verildiği ancak bahse konu hukuki gerekçenin Tebliğ'de belirtildiği üzere Kanununun 5 inci ve 6 ncı maddelerindeki işleme şartlarından hangisine dayandığının açıkça belirtilmediği,

• Aydınlatma Tebliği'nin anılan maddesinin (j) bendinde; *“Aydınlatma yükümlülüğü yerine getirilirken eksik, ilgili kişileri yanıltıcı ve yanlış bilgilere yer verilmemelidir.”* hükmüne yer verilmiştir. Veri sorumlusunun aydınlatma metninde ise, kişisel verilerin ticari ileti gönderilmesi için hizmet alınan üçüncü kişilerle paylaşılması amaçlarıyla açık rıza kapsamında işleneceğine yer verilmiş olduğu ancak bahsedilen üçüncü kişinin yurtdışında bulunan ... isimli firma olduğundan bahsedilmediği, diğer bir ifadeyle bu verilerin yurt dışına aktarılacağına ilişkin açıklamaya yer verilmediği, kişisel verilerin yurtdışına aktarılmasına ilişkin eksik ve yanıltıcı bilgi verilmesi sebebiyle, ilgili kişinin neye rıza gösterdiği ve rızasının sonuçları hakkında tam bir bilgi sahibi olamadığı,

• Aydınlatma Tebliği'nin anılan maddesinin (a) bendinde; *“İlgili kişinin açık rızasına veya Kanundaki diğer işleme şartlarına bağlı olarak kişisel veri işlendiği her durumda aydınlatma yükümlülüğü yerine getirilmelidir.”*, (f) bendinde ise; *“Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir.”* hükümlerine yer verilmiştir. Ancak, veri sorumlusunun aydınlatma metni ve açık rıza alınmasını tek metinde düzenlediği dolayısıyla ilgili kişiye tercihte bulunma seçeneğini sunmadığı

anlaşıldığından veri sorumlusunun Aydınlatma Tebliği'ne uyumda da yeterli dikkat ve özeni göstermediği kanaatine varılmıştır.

Sonuç itibariyle;

1. Veri sorumlusunun, kişisel verilerin yurtdışına aktarılması ile ilgili olarak yurtdışına veri aktarımı konusunu düzenleyen Kanununun 9. maddesinde belirtilen hususlara uygun bir veri aktarımı gerçekleştirilmediği ayrıca 108 sayılı Sözleşmeye taraf olmanın AB uygulamasında olduğu gibi 6698 sayılı Kanun kapsamında güvenli ülke statüsü tayini bakımından tek başına yeterli olmadığı ancak Kurul tarafından yapılacak değerlendirmede olumlu bir unsur teşkil edeceği, dolayısı ile gerekli

řartlar saęlanmadan kiřisel verilerin yurt dıřına aktarılması suretiyle hukuka aykırı bir kiřisel veri iřleme faaliyeti gerekleřtirildięi, bu sebeple Kanunun "Veri Gvenlięine İliřkin Ykmllkler" bařlıklı 12 nci maddesinin birinci fıkrasının (a) bendinde ngrlen "Kiřisel verilerin hukuka aykırı olarak iřlenmesini nlemek" ykmllęnn yerine getirilmedięi kanaatine varıldıęından, tzel kiři veri sorumlusu hakkında, Kanunun "Kabahatler" bařlıklı 18 inci maddesinin birinci fıkrasının (b) bendi uyarınca 900.000 TL idari para cezası uygulanmasına,

2. te yandan, hukuka aykırı olarak yurtdıřına aktarılan sz konusu kiřisel verilerin 6698 sayılı Kanunun 7 inci maddesine uygun olarak silinmesi/yok edilmesi ve sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına,

3. Veri sorumlusunun, aydınlatma metnini 6698 sayılı Kanunun 10 uncu maddesi ve bu maddeye dayanarak ıkarılan Aydınlatma Ykmllęnn Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Teblięin 5 inci maddesinde belirtilen hkmlere uygun olacak řekilde gncellemesi ile aydınlatma ykmllę ve aık rızanın alınması iřlemlerini ayrı ayrı yerine getirmesi gerektięi ynnde talimatlandırılmasına

karar verilmiřtir.

2020/542 sayılı KVKK Kararı

Aynı gerçek kişinin, yurt dışında yerleşik birden fazla veri sorumlusu için irtibat kişisi olarak atanması hakkındaki görüş talebi ile ilgili olarak Kişisel Verileri Koruma Kurulunun 16.07.2020 tarihli ve 2020/542 sayılı Karar Özeti

Karar Tarihi : 16.07.2020

Karar No : 2020/542

Konu Özeti : Aynı gerçek kişinin, yurt dışında yerleşik birden fazla veri sorumlusu için irtibat kişisi olarak atanması talebi hakkında.

Kurumumuza gelen muhtelif başvurular ve kamuoyunda yer alan tartışmalarda; Türkiye’de yerleşik olmayan veri sorumlularınca 6698 sayılı Kişisel Verilerin Korunması Kanunu (6698 sayılı Kanun) ve ikincil mevzuat kapsamında Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) kaydı gerçekleştirilirken, aynı veri sorumlusu temsilcisinin birden fazla yurt dışında yerleşik veri sorumlusu adına girişinin yapılabildiği ancak aynı irtibat kişisinin birden fazla yurt dışında yerleşik veri sorumlusu adına girişinin yapılamadığı ve her bir yurt dışında yerleşik veri sorumlusu için farklı bir gerçek kişinin atanması gerektiğinden bu hususta zorlukla karşılaşıldığı belirtilerek bir gerçek kişinin, aynı veri sorumlusu temsilcisi tarafından yurt dışında yerleşik birden fazla veri sorumlusu için irtibat kişisi olarak atanabilmesi hususunda görüş ve teknik düzenleme yapılmasının talep edilmesi üzerine Kişisel Verileri Koruma Kurulunca (Kurul) yapılan değerlendirme neticesinde alınan 16.07.2020 tarih ve 2020/542 sayılı kararın özetine aşağıda yer verilmektedir.

Bilindiği üzere Veri Sorumluları Siciline (Sicil) kayıt yükümlülüğünün yerine getirilmesi esnasında veri sorumlularına rehberlik etmek amacıyla hazırlanarak Kurum internet sayfasında yayımlanan “Sorularla Veri Sorumluları Sicil Bilgi Sistemi” dokümanında 41 ve 42 nci sorulara verilen cevaplarda; bir gerçek kişinin aynı anda birden fazla veri sorumlusu tarafından irtibat kişisi olarak atanamayacağı, bir veri sorumlusunun da aynı anda birden fazla irtibat kişisi atayamayacağı ifade edilmiştir.

Ayrıca Türkiye’de yerleşik grup şirketlerinde ortak irtibat kişisi atanması hakkında görüş talebiyle ilgili olarak 18.10.2019 tarihli ve 2019/299 sayılı Kurul kararında irtibat kişisinin, veri sorumlusunun

Sicile kayıt yükümlülüğünü yerine getirebilmesi için kişisel veri işleme envanteri ve kişisel veri işleme faaliyetlerine ait doğru, güncel ve güvenilir bilgiye haiz olmasının gerektiği, veri sorumlusunun Kanun ve ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak Kurumla iletişimi sağlamak amacıyla atandığı, Sicile bildirilen bilgilerde değişiklik olması halinde bu değişikliğin meydana geldiği tarihten itibaren en geç 7 gün içinde VERBİS'te değişiklik yapması gerektiği, bu değişikliği süresinde sisteme girebilmesi için veri sorumlusunun kişisel veri işleme faaliyetlerini yakından takip etmesi gerektiğinden bir gerçek kişinin aynı anda sadece bir veri sorumlusu tarafından irtibat kişisi olarak atanabilmesinin uygun olduğu belirtilmiştir.

Öte yandan Sicile ilişkin usul ve esasları düzenleyen Veri Sorumluları Sicili Hakkında Yönetmeliğin (Yönetmelik) 4 üncü maddesinde veri sorumlusu temsilcisi, *“Türkiye’de yerleşik olmayan veri sorumlularını bu Yönetmeliğin 11 inci maddesinin üçüncü fıkrasında belirtilen konularda asgari temsile yetkili Türkiye’de yerleşik tüzel kişi ya da Türkiye Cumhuriyeti vatandaşı gerçek kişiyi ifade eder.”* şeklinde, irtibat kişisi de *“Türkiye’de yerleşik olan gerçek ve tüzel kişiler için veri sorumlusu tarafından, Türkiye’de yerleşik olmayan gerçek ve tüzel kişiler için de veri sorumlusu temsilcisi tarafından, Kanun ve bu Kanuna dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile iletişimi sağlamak amacıyla Sicile kayıt esnasında bildirilen gerçek kişi”* şeklinde tanımlanmıştır.

Aynı Yönetmeliğin 11 inci maddesi ikinci fıkrasında, *“Türkiye’de yerleşik olmayan veri sorumlusunun, veri sorumlusu temsilcisi atanmasına ilişkin yetkili organı veya kişisi tarafından alınacak kararın tasdikli örneği, kayıt başvurusu sırasında veri sorumlusu temsilcisi tarafından Kuruma sunulur.”* hükmü yer almış, üçüncü fıkrasında ise Türkiye’de yerleşik olmayan veri sorumlusunun, veri sorumlusu temsilcisi atamasına ilişkin atama kararında asgari olarak bulunması gereken hususlar sayılmıştır.

Buna göre, Türkiye’de yerleşik olmayan veri sorumluları için; Kurum tarafından yapılan tebligat veya yazışmaları onun adına tebellüğ veya kabul etmek, Kurum tarafından veri sorumlusuna yöneltilen talepleri veri sorumlusuna iletmek, veri sorumlusundan gelecek cevabı Kuruma iletmek, ilgili kişilerin Kanununun 13 üncü maddesinin birinci fıkrası uyarınca veri sorumlusuna yönelteceği başvuruları veri sorumlusu adına almak ve veri sorumlusuna iletmek, ilgili kişilere veri sorumlusunun cevabını iletmek ve veri sorumlusu adına Sicile ilişkin iş ve işlemleri yapmak görevleri Yönetmelikle veri sorumlusu temsilcisine verilmiştir.

Söz konusu görevleri yerine getirmekte olan veri sorumlusu temsilcilerine ilişkin Kurul tarafından yapılan değerlendirme sonucunda; Türkiye’de yerleşik bir tüzel kişi veya Türkiye Cumhuriyeti vatandaşı ve Türkiye’de yerleşik bir gerçek kişi olması, Türkiye’de yerleşik olmayan veri sorumlusu adına Sicile ilişkin iş ve işlemleri yapması, VERBİS’te güncelleme yapması ve veri sorumlusu adına

Kurum ve ilgili kişilerle iletişimi sağlaması gerektiğinden hem kişisel verilerin korunması mevzuatı konusunda hem de yurtdışında yerleşik veri sorumlularıyla iletişimi sağlayabilecek düzeyde uzmanlaşmış gerçek veya tüzel kişilerin tespit edilerek veri sorumlusu temsilcisi olarak atamasının zorluğu göz önüne alınarak aynı gerçek veya tüzel kişinin Türkiye’de yerleşik olmayan birden fazla veri sorumlusu tarafından veri sorumlusu temsilcisi olarak atanabilmesine imkân sağlanmıştır.

Bu kapsamda Türkiye’de yerleşik olmayan veri sorumluları adına gerek ilgili kişiler gerekse de Kurumla iletişimi sağlayacak asıl muhatabın veri sorumlusu temsilcisi olması, Türkiye’de yerleşik olmayan veri sorumluları için veri sorumlusu temsilcisi tarafından atanacak irtibat kişilerinin VERBİS işlemlerini gerçekleştirecek kişi olması nedeniyle aynı gerçek kişinin Türkiye’de yerleşik olmayan birden fazla veri sorumlusu için irtibat kişisi olarak atanması Kurul tarafından uygun bulunmuştur.

Yukarıda yer verilen açıklamalar doğrultusunda Kişisel Verileri Koruma Kurulunca yapılan değerlendirme sonucunda;

- Bir gerçek kişinin, yurt içinde yerleşik birden fazla veri sorumlusu için irtibat kişisi olarak atanmasının uygun olmadığına,
- Bir gerçek kişinin, yurt dışında yerleşik birden fazla veri sorumlusu için irtibat kişisi olarak atanmasının uygun bulunduğuna

karar verilmiştir.

2020/532 sayılı KVKK Kararı

Bir sigorta şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 09/07/2020 tarih ve 2020/532 sayılı Karar Özeti

Karar Tarihi : 09.07.2020

Karar No : 2020/532

Konu Özeti : Bir sigorta şirketinin veri ihlal bildirimini hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Veri sorumlusunun bilgi sistem destek hizmeti aldığı hizmet sağlayıcısında meydana gelen sistemsel bir hata sonucu akıbet dosyası seçen sorgunun hatalı çalışması nedeniyle Otomatik Katılım Sistemi (OKS) kapsamında kendisine bağlı 61 şirketin müşterisi olan 367 ilgili kişinin kişisel verilerini içeren akıbet dosyalarını söz konusu hata sebebiyle yanlış alıcılara gönderdiği,
- Veri ihlalden veri sorumlusunun müşterisi olan 61 şirketin toplam 367 çalışanın etkilendiği,
- Destek hizmeti sağlayıcısından iletilen bilgiye göre; hataya sebebiyet veren uygulama 2010 yılında geliştirilmiş olup geliştirmede eski bir programdan yararlanıldığı,
- Yapılan geliştirme 2011 yılında devreye alındığı için, 2010 yılı ve öncesinde bu hata oluşmadığı,
- Alt yapının ilk kez kurulmasından beri mevcut olan bir hatanın olduğu ve bu hatanın ilk kez içerisinde bulunduğumuz yıl bilgisinin son rakamının 0 (sıfır) olması sebebiyle gerçekleşebildiği, (Örneğin bu alt yapı, 2010 yılından önce geliştirilseydi ilk kez 2010 yılında karşılaşılabileceği ancak 2010 yılından sonra geliştirildiği için ilk problem 2020'de yaşandığı),
- İhlalden 367 gerçek kişiye ait kimlik (TCKN, ad soyad, doğum tarihi, SGK numarası), iletişim (telefon numarası, e-posta adresi), özlük (işe başlama tarihi) ve finans (IBAN numarası, katkı payı tutarı) verilerinin etkilendiği,
- İhlalden etkilenen kişilere ihlal sonrası e-posta ile bildirim yapıldığı, ihlalden etkilenme durumuna göre etkilenen kişi grupları 4'e ayrılarak her bir gruba ayrı bildirimler yapıldığı,
- Yanlış kişisel veri dosyasının gönderildiği 854 firmaya yapılan bildirim aramaları ve e-posta gönderimleri sonunda: 543 firmanın, verileri sildiklerine dair açık teyit verdiği, irtibat bilgilerindeki

sorunlar nedeniyle ulaşılamayan bütün firmalara da ayrıca posta yoluyla yazılı olarak bildirim yapılmış ve yanlış bilgilerin kaydedilmiş ise silindiğine dair teyitlerinin beklendiği beyan ettikleri, ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 09/07/2020 tarih ve 2020/531 sayılı Kararı ile;

- Veri ihlaline sebep olan sistemsel hatanın 2011 yılından itibaren kullanılmaya başlanan uygulama yazılımından kaynaklanması sebebiyle, Kurumumuz tarafından yayınlanan Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 3.5. Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı başlığında *“Veri sorumlusu tarafından yeni sistemlerin tedariki, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmalıdır. Uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontroller yapılmalı, doğru girilmiş bilginin işlem sırasında oluşan hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmaları yerleştirilmelidir.”* ifadesi gereği veri ihlaline sebep olan yazılımdaki sistemsel hatanın veri güvenliğinin sağlanması amacıyla sürekli olarak takibinin gerektiği,

- İhlale konu olayın gerçekleşme tarihi (01.01.2020) ile tespit tarihi (06.01.2020) arasında 5 günlük bir gecikmenin bulunduğu hususunun, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde 3.2. Kişisel Veri Güvenliğinin Takibi başlığında *“...raporlama sürecinde oluşturulacak raporlar, sistem tarafından oluşturulacak otomatik raporlar olabilir. Bu raporların sistem yöneticisi tarafından en kısa sürede toplulaştırılarak veri sorumlusuna sunulması gerekmektedir. Ayrıca güvenlik yazılımı mesajları, erişim kontrolü kayıtları ve diğer raporlama araçlarının düzenli olarak kontrol edilmesi, bu sistemlerden gelen uyarılar üzerine harekete geçilmesi...”* ifadesi gereği veri sorumlusunun gerekli kontrol ve denetimleri zamanında yapmadığının göstergesi olduğu,

- İhlale sebep olan hatanın istisnai bir durum olması ve uygulamanın ana fonksiyonları ile doğrudan ilişkili olmaması durumu ihlal bildiriminde belirtilse de sigortacılık işlemi yürüten bir kuruluşun bilgi sistemleri güvenliğinde daha dikkatli olması gerektiğinden, veri ihlaline sebep olan sistemsel hatanın işlem yayına alınmadan evvel düzeltilmesi gerektiği,

dikkate alındığında Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında ihlale sebep olan hatanın istisnai bir durum olması ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 30.000 TL idari para cezasının uygulanmasına,

- İhlale sebep olan sistemdeki hatanın 01 Ocak 2020 tarihinde gerekleŖtiđi, 06 Ocak 2020 tarihinde tespit edildiđi, 08 Ocak 2020 tarihinde Kurumumuza veri ihlal bildiriminde bulunulduđu, bu durumda Kurul'un 24.01.2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin renilmesinden itibaren baŖlayan 72 saatlik sre ierisinde bildirim koŖulunun sađlandığı,
- Veri sorumlusu tarafından ilgili kiŖilere posta gndermek suretiyle bildirim yapıldığı, sz konusu metnin tarafımızla paylaŖıldıđı

dikkate alındığında, veri sorumlusunun bildirimini Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen "en kısa srede" (24.01.2019 tarih ve 2019/10 sayılı Kurul kararında belirtilen 72 saatlik sre ierisinde) bildirimde bulunma ykmllđne uygun olması nedeniyle Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca yapılacak bir iŖlem bulunmadığına karar verilmiŖtir.

2020/530 sayılı KVKK Kararı

Bir bankanın veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 09/07/2020 tarih ve 2020/530 sayılı Karar Özeti

Karar Tarihi : 09.07.2020

Karar No : 2020/530

Konu Özeti : Bir bankanın kişisel veri ihlali bildirimini

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Bankanın denetim ekiplerinin aldıkları bir ihbar üzerine yaptığı inceleme sonucunda bir Banka personelinin, 23 adet Banka müşterisinin Türkiye Bankalar Birliği Risk Merkezi (KBB) skorlarını veya TCKN bilgisini 01.01.2019 ile 05.12.2019 tarihleri arasında Whatsapp uygulaması aracılığıyla bir tanıdığı (3. kişi) ile paylaştığının tespit edildiği,
- Personelin 23 Banka müşterisine ait paylaşımlardan menfaat temin ettiğine dair somut bir tespite ulaşılmadığı,
- 19 kişinin KKB, 4 kişinin TCKN, 1 kişinin doğum tarihi, 2 kişinin hesaplarına ilişkin bilgi, 1 kişinin kredi başvurusuna ilişkin bilgi, 23 kişinin isim, soyadı bilgileri olmak üzere toplamda 23 kişiye ait kişisel verilerin ihlalden etkilendiği, özel nitelikli kişisel verilerin etkilenmediği,
- İhlalden etkilenen ilgili kişi gruplarının müşteriler olduğu,
- İhlal ile ilgili olan personelin son bir yıl içerisinde kişisel veri koruma eğitimi aldığı ifadelerine yer verilmiştir.

Söz konusu bildirim incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 09/07/2020 tarih ve 2020/530 sayılı Kararı ile;

- İhlalden 19 kişinin KKB, 4 kişinin TCKN, 1 kişinin doğum tarihi, 2 kişinin hesaplarına ilişkin bilgi, 1 kişinin kredi başvurusuna ilişkin bilgi, 23 kişinin isim, soy isim bilgileri olmak üzere toplamda 23 kişiye ait kişisel verilerin etkilenmiş olduğunun belirtildiği; ancak ihlale sebebiyet veren personelin 01.01.2019-05.12.2019 tarihleri arasında 1.052 kişi için 10.529 adet KKB sorgulaması gerçekleştirdiği,

- Kiři sayısı göz önüne alındığında Kurumumuza gönderilen ekran görüntülerinde yer alan 23 kişiden daha fazla kişinin etkilenmiş olabileceđi, söz konusu sorgulama miktarı ile aynı bölgede yer alan diđer personeller içerisinde kişinin 1. sırada olduđu, personelin bu husus ile ilgili makul bir açıklamasının olmadığı, veri sorumlusu tarafından da personelin müşterilere ilişkin bilgileri Banka dışına sızdırmış olabileceđi yönünde řüphe oluřtuđu,
- İhlal öncesinde veri sorumlusu tarafından personelin KKB sorgularının sınırlandırılmadığı,
- İhlale sebebiyet veren kişinin bölge ortalamasından oldukça yüksek miktarda sorgulama yapması hususunun incelenmemesi ve durumun ihlalin bařlangıç tarihinden yaklaşık 1 yıl sonra ihbar sonucu öğrenildiđi göz önüne alındığında yeterince denetim ve gözetim yapılmadığı,
- Veri sorumlusunca gerçekleştirilen “Kişisel Verilerin Korunması Kanunu Eđitimi”nin yeterli olmadığı

kanaatine varıldığından Kanunun 12 nci maddesinin (1) numaralı fıkrası hükmü çerçevesinde veri güvenliđini sađlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriđi, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 200.000 TL idari para cezasının uygulanmasına karar verilmiştir.

2020/511 sayılı KVKK Kararı

Bir sigorta şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 30.06.2020 tarih ve 2020/511 sayılı Karar Özeti

Karar Tarihi : 30.06.2020

Karar No : 2020/511

Konu Özeti : Bir sigorta şirketinin veri ihlal bildirimini hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Sağlık sigortası müşterilerine yönelik eczane provizyon uygulamasının 2018 yılında değiştirilmesi esnasında, sürekli ilaç kullanım raporu olan 683 farklı müşterinin ilaç geçmişinin yeni sisteme aktarılması amacıyla toplu bir liste hazırlanması gerektiği,
- Bu amaçla ilgili kişilerin kimlik ve ilaç kullanım bilgilerinin yer aldığı bir excel dosyasının oluşturulduğu,
- Söz konusu dosyada yer alan bilgilerin provizyon uygulamasına kişi bazlı olarak girilir iken ilgili dosyanın aynı zamanda provizyon sistemine entegre olarak çalışan doküman yönetim sistemine excel dokümanı olarak sehven bütün halinde yüklendiği,
- İhlalden etkilenen kişi sayısının 683; kayıt sayısının 2413 olduğu,
- Etkilenen kişi kategorilerinin müşteriler olduğu,
- İhlalden etkilenen kişisel verilerin kimlik, müşteri işlem ve sağlık bilgileri olduğu,
- İhlale konu excel dosyasına erişimin yalnızca mobil uygulamanın “sağlık geçmişim/Eczane” bölümünden 11 sağlık müşteri açısından mümkün olduğu, bunlardan yalnızca iki kişinin uygulama kullanıcısı olduğunun tespit edildiği, söz konusu dosyaya erişimin mobil uygulama üzerinden bir kişi tarafından yapıldığı, diğer kullanıcının ilgili dosyaya herhangi bir erişiminin olmadığı,
- Diğer taraftan ilgili dosyaya erişim sağlayan kullanıcı ile irtibata geçildiği, kendisine ihlal ve sonuçlarına yönelik bilgilendirme yapıldığı, erişim sağladığı dosyanın acil olarak silinmesi konusunda talepte bulunulduğu, bu kapsamda ihlalin ilgili kişiler üzerindeki potansiyel etkilerinin oldukça sınırlı olduğunun değerlendirildiği

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 30/06/2020 tarih ve 2020/511 sayılı Kararı ile,

- İhlalin, veri sorumlusunun eczane provizyon ekranlarının değiştirilmesi esnasında, kişi bazında kimlik ve ilaç kullanım bilgilerinin yer aldığı excel dosyasının, yeni sisteme aktarılırken 11 sigortalı tarafından görüntülenebilir hale gelmesi sonucu gerçekleştiği, bunun sonucunda ihlalden ilgili kişilerin; kimlik, müşteri işlem ve özel nitelikli kişisel veri olarak da sağlık bilgileri gibi kişisel verilerinin etkilendiği,
- 25.04.2019 tarihinden 07.12.2019 tarihine kadar açıklığın devam ettiği ve dosyaya erişim sağlayan kişi tarafından bilgilendirilinceye kadar veri sorumlusunun açıklığı tespit edemediği, Kişisel Veri Güvenliği Rehberi'nin Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Belirlenmesi başlığı altında da belirtildiği üzere "...veri sorumlusunun hazırlanmış olan kişisel veri güvenliği politika ve prosedürleri kapsamında; uygulamanın düzenli olarak kontrollerini yapmak, yapılan kontrolleri belgelemek, geliştirilmesi gereken hususlar belirlemek ve gerekli güncellemeler yerine getirildikten sonra da düzenli olarak kontrollere devam etmek gibi yükümlülüklerini" yerine getirmediği,
- Ayrıca yine Kişisel Veri Güvenliği Rehberi'nin Kişisel Veri Güvenliğinin Takibi başlığı altında belirtilen "veri sorumlularının gizlilik ve bütünlüğü bozan ihlaller gibi istenmeyen olayların önüne geçilmesi adına veri sorumlusu tarafından düzenli olarak zaafiyet taramalarının yapılmadığının" göstergesi olduğu, Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması başlığı altında belirtilen "çalışanların sistem ağına erişim sağlaması da güvenlik ihlali riskini arttırdığından bunlar için yeterli güvenlik tedbirinin" alınmadığı,
- Veri sorumlusunun ihlale sebep olan kişisel veri içeren ve yetkisiz kişiler tarafından görüntülenebilir hale gelen excel dosyalarının doküman yönetim sistemine yüklenmesini engelleyecek herhangi bir teknik ve idari tedbir almadığı, bu durumun Kişisel Veri Güvenliği Rehberi'nin Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı başlığı altında da ifade edildiği üzere "veri sorumlusu tarafından yeni sistemin geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimlerinin göz önünde bulundurulmadığı, uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontrollerin yeterli ve gerekli ölçüde yapılmadığı, doğru girilmiş bilginin işlem sırasında oluşan hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmaları yerleştirilmediği ve belgelerin sisteme yüklenirken bir onay sürecinin işletilmediği",

- İhlalden etkilenen kişisel verilerin içinde özel nitelikli kişisel veriler olarak sağlık bilgilerinin bulunduğu, ihlale konu olan dosyanın içerisinde özel nitelikli kişisel verilerin de yer aldığı göz önünde bulundurulduğunda "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararında da belirtildiği üzere "özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi ve kriptografik anahtarların güvenli ve farklı ortamlarda tutulması gerekirken veri sorumlusu tarafından diğer kişisel verilere göre çok daha sıkı şekilde korunmaları gerektiğinin" göz önünde bulundurulmadığı,

- İhlale konu olayda ilgili kişiler önemli bir zarara uğramamış olsa da öğrenilmesi halinde ilgili kişiler hakkında mağduriyete neden olabilecek nitelikteki verilerin ihlale konu olduğu bu yüzden de ihlalin potansiyel tehdit açısından ciddi bir risk taşıdığı,

dikkate alındığında, Kanununun 12 nci maddesinin (1) numaralı fıkrası hükmü çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanununun 18 nci maddesinin (1) numaralı fıkrasının (b) uyarınca 100.000 TL idari para cezası uygulanmasına,

- 07.12.2019 tarihinde tespit edilen veri ihlalinin, Kurumumuza 10.12.2019 tarihinde (72 saatlik süre koşulunun içerisinde) bildirildiği ve ihlalden etkilenen 683 kişiye yeterli bildirim yapıldığı, bildirim örneklerinin Kurumumuza sunulduğu dikkate alındığında, Kanununun 12 nci maddesinin (5) numaralı fıkrası uyarınca yapılacak bir işlem bulunmadığına

karar verilmiştir.

2020/508 sayılı KVKK Kararı

Bazı avukatların avukat sorgulama siteleri ile ilgili ihbar başvuruları hakkında Kişisel Verileri Koruma Kurulunun 30/06/2020 tarih ve 2020/508 sayılı Karar Özeti

Karar Tarihi : 30.06.2020

Karar No : 2020/508

Konu Özeti : Bazı avukatların, avukat sorgulama siteleri ile ilgili ihbar başvuruları

Kuruma intikal eden ihbarlarda, ihbar başvurusu sahiplerinin muhtelif avukat sorgulama sitelerinde taraflarına ait ad soyadı, kayıtlı buldukları baro, baro ve Türkiye Barolar Birliği (TBB) sicil numaraları, e-posta adresleri ve fotoğraflarının yayımlandığı, söz konusu verilerin rızaları olmaksızın hukuka aykırı olarak elde edildiği, bahsi geçen internet sitelerince gerek taraflarına gerek çok sayıda avukata ait kişisel verilerin hukuka aykırı olarak elde edildiği ve bu suretle paylaşıldığı, söz konusu internet sitelerinde ve bu siteler ile ilişkili bulunan kurum/kuruluş ya da alan adında yer alan tüm profillerin kaldırılması gerektiği yönünde ihbarda bulunularak gereğinin yapılması talep edilmiştir.

Konuya ilişkin yapılan değerlendirmede, Kişisel Verileri Koruma Kurulunun 30/06/2020 tarih ve 2020/508 sayılı Kararı ile,

- 1136 sayılı Avukatlık Kanununun “Baroya yazılma istemi” başlıklı 6 ncı maddesinin, “4 üncü maddedeki koşulları taşıyanlar başvurdukları yer barosu levhasına yazılmalarını dilekçe ile isteyebilirler.” hükmünü, “Avukatlık yetkilerinin başkaları tarafından kullanılmaması” başlıklı 63 üncü maddesinin “... Baro levhasında yazılı bulunmayanlar avukatlık unvanını da taşıyamazlar...” hükmünü haiz olduğu, Avukatlık Kanununun “Levhaya yazılma yükümlülüğü” başlıklı 66 ncı maddesi uyarınca, her avukatın bölgesi içinde sürekli olarak avukatlık edeceği yerin baro levhasına yazılmakla yükümlü olduğu, dolayısıyla avukatlık görevini ifa edecek kişiler için baro levhasına yazılmanın kanuni bir yükümlülük olduğu, bu yükümlülüğü yerine getirmeden avukatlık görevini icra etmenin mümkün olmadığı,

- Avukatlık Kanununun “Avukatlar listesi” başlıklı 75 inci maddesinde, “Baro yönetim kurulu üç yılda bir bölgesi içinde bulunan ve baro levhasında yazılı olan bütün avukatların bir listesini son yılın 31 Aralık tarihine kadar düzenler. Listeye her avukatın alfabe sırasıyla adı, soyadı, büro ve konut adresi yazılır. Birlikte

çalışan avukatların büroları ve avukatlık ortaklıkları listede ayrıca belirtilir. Levhadaki değişiklikler her yıl sonunda düzenlenecek ek listede gösterilir. Bu listenin düzenlenme şekli Türkiye Barolar Birliğince tespit edilir. Listenin düzenlenmesinden sonra baro levhasına yazılanlara yeni listenin düzenlenmesine kadar kullanılacak geçici bir belge verilir. Listeden Anayasa Mahkemesine, Yüksek Mahkemelere, Adalet Bakanlığına, Türkiye Barolar Birliğine, diğer barolara, baronun bölgesi içinde bulunan mahkemelerle Cumhuriyet Savcılıklarına, en büyük idare amirine, diğer yargı mercilerine, noterlere ve icra ve iflas dairelerine yeteri kadar gönderilir.” düzenlemesinin yer aldığı, bu kapsamda, baro levhasının, her baronun bünyesinde bulunan avukatlar listesinin TBB ya da baroların internet sayfalarında yayımlanan tezahürü olduğu kanaatine varıldığı,

- Buna ek olarak TBB ve il barolarının internet sayfalarında yayımlanan avukat bilgilerinin genel olarak; fotoğraf (biyometrik veya normal), baro sicil numarası, birlik sicil numarası, ad, soyadı, adres, iş telefonu, fax numarası, cep telefonu, web adresi, e-posta adresi olduğu, bununla birlikte, yayımlanan bilgilerin barodan baroya farklılık gösterdiği ve bu yönde tek tip bir uygulama olmadığı, hangi bilgilerin yayımlanacağına ilişkin yukarıda ifade edilen hükümler dışında doğrudan bir yasal düzenleme bulunmadığının anlaşıldığı,
- Baroya yazılma istemiyle birlikte baroya iletilen bilgilerin baro levhasında doğrudan yayımlandığı fakat daha sonradan avukatların söz konusu baroya başvurarak bu bilgileri güncelleme ya da sildirme imkânı olduğunun anlaşıldığı,
- TBB Başkanlığının 08.04.2016 tarihli 2016/24 numaralı duyurusunda, avukatlıkla birleşmeyen bir işte çalıştığını ve bu nedenle avukatlık yapmayacağını belirten talep sahiplerinin sadece adına avukatlık ruhsatnamesi düzenlenmesini talep edebileceği ve baro levhasına yazılma talebinin olmadığını belirten bir dilekçe alınması gerektiğinin görüldüğü,
- Söz konusu sitelerden birçoğunda ‘*Bu siteye ulaşılamıyor*’ ibaresinin yer aldığı görüldüğü, erişilebilen siteler incelendiğinde; internet sitelerinin ana sayfasında il barolarına ait butonlar olduğu, söz konusu butonlara basıldığında o ilde kayıtlı avukatlar listesine ilçelere göre ayrılmış şekilde ulaşılabilirdiği, ilçe ismine tıkladığında ise adresi o ilçede görünen avukat isimlerinin listesinin çıktığı, herhangi bir avukat ismine tıkladığında söz konusu profilin altında “*Bu sayfada bulunan bilgiler ... levhasından alınmıştır*” şeklinde o avukat hangi il barosuna kayıtlı ise o baro levhasının belirtildiği, internet sitelerinin ana sayfasında “*Hakkımızda, Gizlilik, Hukuki Uyarı, Avukat Sorgula, İcra İban Numaraları, Avukat Ekle, İletişim*” sekmelerinin yer aldığı, kullanıcıların bahsi geçen internet sitelerine giriş yaptıktan sonra arama butonuna herhangi bir isim yazmasıyla otomatik olarak <https://cse.google.com.tr/cse/> uzantılı Google özel arama motoru (Google Custom Search) linkinin

açıldığı ve ismin bu link üzerinde aratıldığı, internet sitelerinin “Gizlilik” bölümündeki “Kişisel Verilerin Korunması” başlığı altında, 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) uyarınca, veri sorumlusu sıfatıyla, mevzuatın izin verdiği durumlarda yurt içinde ve dışında üçüncü kişilere aktarılabilceği, “Kişisel Verilerin İşlenme Amaçları” başlığı altında sitenin, avukatların iletişim bilgilerinin müvekkiller veya avukat arayışında olan kişiler tarafından daha kolay bulunabilmesini amaçladığı, bu doğrultuda avukat bilgilerinin güncel tutulmaya çalışıldığı, yanlış ya da hatalı bilgiler için “Avukat Düzelt” ya da “Sorun Bildir” butonuyla kişilere düzeltme ve sorun bildirme imkanı tanındığı ve “Kişisel Verilerin Toplanma Yöntemleri ve Hukuki Sebepleri” başlığı altında, avukatların kişisel verilerinin baroların internet sitelerinden, sosyal medya veya diğer kamuya açık mecralardan ve kendi istekleri ile ekleme yaptıkları ‘Avukat ekle’ sayfasından elde edildiği, kişisel verilerin Kanunun ilgili maddelerinde (4,5,6) belirtilen şartlar çerçevesinde bu bildirimim Kişisel Verilerin İşlenme Amaçları bölümünde sayılan amaçlar için toplandığı, işlendiği, aktarıldığı ve saklandığının belirtildiği,

- Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinde, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlanmış olup kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, bu çerçevede, kişisel verilerin ancak, hukuka ve dürüstlük kurallarına uygun şekilde, belirli, açık ve meşru amaçlar kapsamında, doğru ve gerektiğinde güncel olma şartıyla, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun olarak işlenebileceği,

- Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin birinci fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, ikinci fıkrasında ise Kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanunun “İstisnalar” başlıklı 28 inci maddesinin ikinci fıkrasında, bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddelerinin aynı fıkranın (b) bendinde yer alan ilgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi durumunda uygulanmayacağı belirtilmiştir,

- Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberinin ‘Kişisel Verilerin İlgili Kişi Tarafından Alenileştirilmiş Olması’ başlığı altında; *“İlgili kişinin kendisi tarafından alenileştirilen, bir başka ifadeyle herhangi bir şekilde kamuoyuna açıklanmış olan kişisel verileri işlenebilecektir. Bu duruma örnek olarak ise bir kişinin belirli hallerde kendisiyle iletişime geçilmesi amacıyla iletişim bilgilerini kamuya açık şekilde ilan etmesi verilebilir. Kurumsal internet sitelerinde, çalışanların işyeri telefon numaraları ve kurumsal elektronik posta adreslerinin üçüncü kişilerin erişimine açık şekilde paylaşılması halinde de alenileştirmeden söz edilebilir.”* ifadelerinin yer aldığı

değerlendirmelerinden hareketle;

- Bahsi geçen internet sitelerinden; birçoğuna ulaşamadığı, erişilebilen sitelerde ise ilgili kişilerden sadece birinin profilinin bulunduğu, bu profilde ise yalnızca ilgili kişinin e-posta adresinin yer aldığı ve bu bilginin, ilgili kişinin kayıtlı olduğu ilin baro levhası ve TBB resmi internet sitesindeki profilinde de yer aldığı ve bahsi geçen sitelerin ilgili kişinin e-posta adresini TBB resmi internet sitesinden çekmiş olabileceği hususunda ilgili kişinin kendisi tarafından alenileştirilen kişisel verilerinin işlenebileceği kanaatine varıldığı ve işlenen kişisel verinin Kanunun 4 üncü maddesindeki genel ilkelere aykırı bir işleme faaliyeti olmadığına,

- Bahsi geçen internet sitelerinde; il baroları levhalarında ve TBB internet sitelerinde yayımlanan bilgilerden farklı bir bilgi yayımlanmadığı, yayımlanan bilgilerin il baroları levhalarında ve TBB internet sitesinde yayımlanma amacından farklı bir amaçla yayımlandığına ilişkin bir tespit yapılamadığı, söz konusu kişisel verileri düzeltme veya silme imkânlarının ilgili kişilere tanındığı göz önünde bulundurulmakla mevcut ihbar başvuruları hakkında Kanunun 5 inci maddesinde yer verilen kişisel verilerin işleme şartlarına aykırı bir durumun gerçekleşmediği kanaatine varıldığından Kanun kapsamında yapılacak bir işlem bulunmadığına

karar verilmiştir.

2020/507 sayılı KVKK Kararı

Ölenin sağlık verisinin yasal mirasçısı tarafından talep edilmesi hakkında Kişisel Verileri Koruma Kurulunun 30/06/2020 tarihli ve 2020/507 Sayılı Karar Özeti

Karar Tarihi : 30.06.2020

Karar No : 2020/507

Konu Özeti : Ölenin sağlık verisinin yasal mirasçısı tarafından talep edilmesi

Kuruma intikal eden şikayette; ilgili kişinin vefat eden babasının mirasçısı olduğunu gösterir mirasçılık belgesi ile Kişisel Sağlık Verileri Hakkında Yönetmeliğin 11 inci maddesi uyarınca babasına ait kayıtlı her türlü sağlık verisinin tarafına iletilmesini ilgili kamu kurumundan talep ettiği fakat talebinin 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 8 inci maddesi ile 5502 sayılı Sosyal Güvenlik Kurumu Kanununun 35 inci maddesinin beşinci fıkrası dayanak gösterilerek ve 4721 sayılı Türk Medeni Kanununa ilişkin sükna hakkı, intifa hakkı ve nafaka alacağıının devredilmediği belirtilerek reddedildiği, ancak bu hususların talebi ile hiçbir ilgisinin olmadığı, ölen kişinin verisinin mirasçısına verilmesi ile ilgili açık mevzuat olmadığı sürece, idarenin emsal yolu ile sınırlama getirmesinin hukuka aykırı olduğu, kişinin tıbben ve hukuken ölümüyle gerçek kişiliğinin sona ermesi ile birlikte, ölenin sağlığında sahip olduğu tüm mal varlığı, hukuki hakları, borçları ve yükümlülüklerinin mirası reddetmemiş mirasçılara geçtiği, hukuki varlığı sona eren ölen bir kişinin 6698 sayılı Kanuna dayanılarak gerçek kişi ve ilgili kişi kavramları ile ilişkilendirilmesinin fiilen ve hukuken söz konusu olmadığı, Kişisel Sağlık Verileri Hakkında Yönetmeliğin 11 inci maddesi göz önüne alındığında verilerin sadece yargı yolu ile alınması gerektiğine ilişkin açık bir düzenleme, yöntem ya da kısıtlama bulunmadığı, veri sorumlusu kamu kurumu tarafından verilen yanıtta Kişisel Sağlık Verileri Hakkında Yönetmeliğin yalnızca Sağlık Bakanlığını bağladığının ifade edildiği ancak, bir yönetmeliğin yalnızca onu çıkaran Bakanlığı bağlayabileceğinin düşünülemeyeceği, bu yönetmeliğin vatandaşı doğrudan ilgilendiren ve idarenin uygulaması gereken açık bir düzenleme olduğu hususları belirtilerek söz konusu verilerin tarafına verilmesi talep edilmiştir.

İlgili kişinin dilekçesi ekinde yer alan veri sorumlusu kamu kurumu tarafından ilgili kişiye verilen cevap yazısında;

• 5502 sayılı Kanununun 35 inci maddesinin beşinci fıkrasında; *“Bu Kanun ve diğer mevzuatla verilen görevleri yerine getirmek amacıyla işlediği kişisel veriler ile ticari sır niteliğinde olan verileri, veri sahibinin noter onaylı muvafakati veya e-devlet uygulaması üzerinden kimlik teyidi ile verilen izni olmadan gerçek veya tüzel kişilerle paylaşamaz. ... Kurum, kişisel sağlık verilerini kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, verilen sağlık hizmetlerinin uygunluğunun ve yerindeliğinin takibi ve finansmanının planlanması amacıyla talebi halinde Sağlık Bakanlığı ile paylaşır....”* hükümlerine yer verildiği,

• Ayrıca veri sorumlusu kamu kurumunun hukuk müşavirliğinden alınan görüşte; *“... bir kişinin yaşamı sırasında üçüncü kişilerden bir çok hak ve alacağı olabilir. Bu haklardan intifa hakkı, sükna hakkı, nafaka alacağı gibi hak ve alacaklar hak sahibi kişinin ölümü ile kendiliğinden sona erer. Bu nedenle kendiliğinden sona eren bu tür hak ve alacaklar mirasçılara geçmez. ... Bu itibarla, ölen kişinin mirasçılara kişisel verilerinin... verilmesinin hukuken mümkün olmadığı ancak dava konusu yapılması durumunda mahkeme kanalıyla istenmesi halinde ... verilmesinin uygun olacağı”*na ilişkin mütalaa verildiği,

• Sağlık Bakanlığı tarafından çıkarılan Yönetmelik hükümlerinin normlar hiyerarşisi yönünden Sağlık Bakanlığını bağladığı, bu nedenlerle ilgili kişinin babasına ilişkin kişisel sağlık verilerinin ancak yargı makamları tarafından istenmesi halinde verilebileceğinin ifade edildiği görülmüştür.

Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulunun 30/06/2020 tarihli ve 2020/507 sayılı Kararı ile,

• Kanunun “Tanımlar” başlıklı 3 üncü maddesinde; *“kişisel veri”*nin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi; *“kişisel verilerin işlenmesi”*nin ise kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı,

• Kanunun gerekçesinde; sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgilerin değil, aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgilerin de bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade ettiğinden kişisel veri olarak tanımlandığı, diğer bir ifadeyle, kişinin fiziksel, ekonomik,

kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıyan veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsadığı, bu sebeple, isim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi verilerin dolaylı da olsa kişiyi belirlenebilir kılabilmek özellikleri nedeniyle kişisel veriler olarak değerlendirildiği,

- 4721 sayılı Türk Medeni Kanununun 28 inci maddesinde ise kişiliğin çocuğun sağ olarak tamamıyla doğduğu anda başladığı ve ölümle sona erdiği hükmünün yer aldığı,
- 21/06/2019 tarihli ve 30808 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren Kişisel Sağlık Verileri Hakkında Yönetmeliğin, "Ölünün sağlık verilerine erişim" başlıklı 11 inci maddesinin birinci fıkrasının; *"Ölmüş bir kimsenin sağlık verilerini almaya, veraset ilamını ibraz etmek suretiyle murisin yasal mirasçıları münferit olarak yetkilidir."* hükmünü amir olduğu,
- Söz konusu olaya benzer nitelikte bir başvuruya ilişkin olarak Kişisel Verileri Koruma Kurulunun vermiş olduğu 18/09/2019 tarih ve 2019/273 sayılı Kararı ile;

"...

-6698 sayılı Kişisel Verilerin Korunması Kanununun 3 üncü maddesinde ilgili kişinin "kişisel verileri işlenen gerçek kişi" olarak tanımlandığı, 4721 sayılı Türk Medeni Kanununun 28 inci maddesinde ise kişiliğin çocuğun sağ olarak tamamıyla doğduğu ve ölümle sona erdiği hükmüne yer verildiği dikkate alındığında başvuranın vefat eden eşine ilişkin kayıtları veri sorumlusundan talep etmesinin 6698 sayılı Kanunda yer alan ilgili kişi tanımı kapsamında değerlendirilemeyeceğine,

-Öte yandan 21.06.2019 tarihli ve 30808 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Kişisel Sağlık Verileri Hakkında Yönetmeliğin, "Ölünün sağlık verilerine erişim" başlıklı 11 inci maddesinin 1 inci fıkrasında *"Ölmüş bir kimsenin sağlık verilerini almaya, veraset ilamını ibraz etmek suretiyle murisin yasal mirasçıları münferit olarak yetkilidir"* hükmü kapsamında ... vefat eden eşi ... yasal mirasçısı olarak söz konusu verileri Kişisel Sağlık Verileri Hakkında Yönetmelik kapsamında adı geçen klinikten talep edebileceği hususunda başvuru sahibinin bilgilendirilmesine...karar verilmiştir."

değerlendirmelerinden hareketle,

- İlgili kişinin vefat eden babasının yasal mirasçısı olarak söz konusu verileri Kişisel Sağlık Verileri Hakkında Yönetmelik kapsamında talep edebileceğine ancak Kuruma yapmış olduğu başvurunun Kanun kapsamında değerlendirilemeyeceğine karar verilmiştir.

2020/504 sayılı KVKK Kararı

Veri sorumlusu bir havayolu şirketi tarafından ilgili kişiye ait çağrı merkezi görüşme kayıtlarının transkriptinin teslim edilmemesi hakkında Kişisel Verileri Koruma Kurulunun 30/06/2020 tarihli ve 2020/504 sayılı Karar Özeti

Karar Tarihi : 30.06.2020

Karar No : 2020/504

Konu Özeti : Veri sorumlusu bir havayolu şirketi tarafından ilgili kişiye ait çağrı merkezi görüşme kayıtlarının transkriptinin teslim edilmemesi

Kuruma intikal eden şikâyetle özetle; ilgili kişinin veri sorumlusu bir havayolu şirketinin çağrı merkezi ile gerçekleştirdiği görüşmeye ait olan ses kaydının 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 3 üncü maddesinin (d) bendi gereğince yazıya dökülmesi suretiyle bir nüshasının tarafına yazılı yahut e-posta yolu ile iletilmesinin istendiği, veri sorumlusu tarafından söz konusu talebin “ilgili ses kayıtlarının talebi şirket prosedürleri gereği yalnızca yasal merciler tarafından iletilmesi durumunda mümkün olduğu” gerekçesi ile reddedildiği, ancak Kanuna göre gerçek kişiye ait olan, gerçek kişiyi belirlenebilir kılan her türlü bilginin kişisel veri olduğu, ilgili kişiye ait olan ses kaydının da kişisel veri niteliğini haiz olduğu belirtilerek ilgili kişi tarafından talebini reddeden veri sorumlusunun Kanunun 13 üncü maddesi anlamında veri ihlaline sebep olduğu gerekçesiyle cezalandırılması ve ilgili görüşme kaydının kendisine teslim edilmesi talep edilmiştir.

Başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- Veri sorumlusu tarafından şikâyetin yanıtlandığı tarih itibarıyla, çağrı merkezi kayıtlarının ancak adli veya idari görevleri doğrultusunda bunları talep eden yetkili adli ve idari kurumlar ile paylaşıldığı, bunların dışında ise yetkilendirilmiş çağrı merkezi görevlilerinin erişimine açık olduğu,
- Veri sorumlusunun misafirlerine ilişkin yolcu rezervasyon numarası (PNR), ses kaydı, şikâyet kayıtları gibi farklı türde kişisel verilerinin benzeri platformlar üzerinde ve farklı düzende kayıt altında tuttuğu,

- Çoğu örnekte söz konusu kayıtların salt misafir kişisel verisinden ibaret olmadığı ve örneğin; PNR kayıtlarında biletleme veya havalimanında uçuşa kayıt (check-in) ve uçuşa kabul (boarding) işlemlerini yapan görevli kişiye, çağrı merkezi kayıtlarında şikâyet kaydı üzerinde işlem yapan yetkiliye ait bilgileri içerebildiği,
- Veri sorumlusunun Kanun kapsamındaki yükümlülüklerini; tüm ilgili kişiler için amaçla bağlantılı, sınırlı ve ölçülü olma ilkesini gözeterek yerine getirdiği ve ilgili kişilerin kişisel verileri işlenmişse buna ilişkin bilgi talep etme hakkının kullanımını da bu ilkeleri gözeterek karşıladığı,
- Talep kapsamında kişilerin işlemleri hakkında açık bir şekilde bilgilendirilmelerinin zaruri olduğu,
- Diğer yandan, veri sorumlusunun kayıtlarında yer alan veri setlerinin aynen başvuru sahipleri ile paylaşılmasının Kanun kapsamında farklı veri ihlali endişelerini beraberinde getirdiği,
- Çağrı merkezi görüşmelerinin çoğu örnekte, uçuş ve işlemlere ilişkin detaylı bilgi içermekte olduğu, talep ve sonuca ilişkin bilgilerin yazılı iletişim kanalları ile misafirlerine doğrudan aktarıldığı ve ilgili kişinin çağrı merkezi görüşme kayıtlarına ilişkin talebinin de bu nedenle ilgili tarihteki uygulama doğrultusunda olumsuz yanıtlandığı,
- Diğer yandan 13.03.2020 tarihinde Kurumun internet sitesinde yayımlanan 14.01.2020 tarih ve 2020/13 sayılı Kurul karar özeti doğrultusunda ilgili kişi ile tekrar iletişime geçilerek görüşme kaydının gerekli görülen maskeleye tedbirleri uygulanması suretiyle yazılı ortamda ilgili kişi ile paylaşıldığı; bu yönde iletilecek taleplerin benzer bir yaklaşımla ele alınması yönünde ilgili hizmet birimlerinin bilgilendirildiği ifadelerine yer verilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 30/06/2020 tarihli ve 2020/504 sayılı Kararı ile,

- Türkiye Cumhuriyeti Anayasasının “Özel hayatın gizliliği” başlıklı 20 nci maddesinin üçüncü fıkrası hükmüne göre; herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına ve bu anlamda bireylerin temel olarak, kendileri ile ilgili kişisel verilerin ilgisiz üçüncü kişilerin eline geçmemesi konusunda gerekli tedbirlerin alınmasını isteme hakkına sahip olduğu,
- Bu hakkın; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı,

- Bu anlamda bireylerin, hangi amaçla hangi kişisel verilerinin kullanıldığını öğrenme hakkına sahip olduğu gibi söz konusu kişisel verilerde herhangi bir yanlışlık bulunması halinde bu durumun düzeltilmesini ya da verilerinin silinmesini isteme hakkına da sahip olduğu,
- Zira Kanunun “İlgili Kişinin Hakları” başlıklı 11 inci maddesinin birinci fıkrasında “Herkes, veri sorumlusuna başvurarak kendisiyle ilgili; a) Kişisel veri işlenip işlenmediğini öğrenme, b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme, c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir.” hükmünün yer aldığı,
- Kanunun 11 inci maddesinin birinci fıkrasının (b) bendi hükmü kapsamında ilgili kişinin, kendisiyle ilgili kişisel veriler işlenmişse buna ilişkin bilgi talep etme hakkının, söz konusu veriye erişim hakkını da kapsadığı, erişim hakkının, bilgi talep etme hakkını tamamlayarak ilgili kişinin, kişisel verileri üzerindeki haklarını kullanabilmesi için, kişisel verilerinin ne şekilde işlendiğine dair tam olarak bilgi sahibi olmasına imkân sağladığı,
- Ancak bu hakkın, kişisel verilerin işlendiği veri kayıt sisteminin/kayıt ortamının doğrudan kendisine erişimini, bu kayıt ortamının kendisinin ilgili kişiye teslimini veya doğrudan verinin kendisinin “elde edilme”sini değil; veri sorumlusunun veri güvenliğine ilişkin yükümlülükleri de dikkate alınarak, işlenen kişisel verilerin, teknik/fiziki imkânların el verdiği ölçüde ve verinin muhtevasına/içeriğine ilgili kişi tarafından makul bir şekilde ulaşılabilmesine imkân tanınmasını kapsadığı,
- Kurum tarafından iletilen bilgi ve belge talebi konulu yazıyı takiben veri sorumlusunca ilgili kişiye, talep ettiği konuşmanın transkriptinin e-posta vasıtasıyla iletildiği ve Kuruma da redaksiyon ile kapatılmış bir versiyonunun gönderildiği,
- Ayrıca veri sorumlusu tarafından gönderilen evraklar içerisinde Operasyon Birimine hitaben yazılan ve Kanun kapsamında yeni süreçte Çağrı Merkezi ile yapılan görüşmelere ilişkin kayıt talep eden misafirlere, görüşmenin transkriptinin dokümanda belirtilen hususlara bağlı kalınması suretiyle paylaşılması talimatını içeren e-postaya da yer verildiği,

değerlendirmelerinden hareketle;

- İlgili kişinin kişisel verilerinin veri sorumlusu havayolu şirketi tarafından temin edilmesinin hukuka uygun olduğu,
- Somut olayda gerçekleşen herhangi bir kişisel veri işleme faaliyeti kapsamında, Kanunun 12 inci maddesinin (1) numaralı fıkrası uyarınca veri sorumlusu tarafından veri güvenliğine ilişkin yükümlülükler aykırı hareket edildiği sonucuna varılamayacağı
- Somut olayla benzerlik arz eden bir konuya ilişkin olarak alınan ve 13.03.2020 tarihinde Kurum internet sitesinde yayımlanan 14.01.2020 tarih ve 2020/13 sayılı Kurul Karar özeti dikkate alınarak veri sorumlusu tarafından ilgili kişinin talebi doğrultusunda ses kaydına ait transkriptin hâlihazırda gönderildiği,
- Veri sorumlusu bünyesindeki birimlerin, uygulamada artık ilgili kişilerin Kanuni talepleri doğrultusunda hareket edilmesi hususunda bilgilendirildiği

hususları göz önüne alındığında veri sorumlusu hakkında yapılacak bir işlem bulunmadığına karar verilmiştir.

2020/494 sayılı KVKK Kararı

İlgili kişinin bir kargo şirketine karşı açtığı işe iade davasında, kişisel verisi olan kamera görüntülerinin kargo şirketi tarafından mahkemeye sunulması hakkında Kişisel Verileri Koruma Kurulunun 25/06/2020 tarihli ve 2020/494 sayılı Karar Özeti

Karar Tarihi : 25.06.2020

Karar No : 2020/494

Konu Özeti : İlgili kişinin bir kargo şirketine karşı açtığı işe iade davasında, kendisine ait kamera görüntülerinin kargo şirketi tarafından mahkemeye sunulması

Kuruma intikal eden şikayette; ilgili kişinin veri sorumlusu kargo şirketi nezdinde çalıştığı, iş akdinin sonlandırılmasından sonra açtığı işe iade davasının görülmesi sırasında veri sorumlusunun ilgili kişiye ait kamera görüntülerini mahkemeye sunduğu, kamera görüntülerinin 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında kişisel veri niteliğini haiz olduğu ve Kanunun 5 inci maddesi uyarınca kişisel verilerin ilgili kişinin açık rızası olmadan işlenemeyeceği, bu hususa ilişkin olarak ilgili kişinin bir açık rıza beyanının bulunmadığı, konuya yönelik olarak veri sorumlusuna yapılan başvuruya cevaben veri sorumlusu tarafından ilgili kişinin kişisel verilerinin önceden ilgili kişi tarafından imzalanmış bir bilgilendirme metni kapsamında işlendiğinin belirtilmiş olmasına rağmen kendisinin böyle bir açık rıza beyanının bulunmadığı belirtilerek veri sorumlusu kargo şirketi nezdinde Kanun kapsamında gerekli yaptırımların uygulanarak hukuka aykırı olarak elde edilen kişisel verilerin silinmesi talep edilmiştir.

Şikayet dilekçesi ekinde yer alan veri sorumlusu tarafından ilgili kişiye verilen cevapta; ilgili kişinin daha önceden imzaladığı bilgilendirme metni kapsamında aktarma merkezinde kamera kaydının yapıldığına ilişkin ilgili kişinin bilgilendirildiği, veri sorumlusu tarafından kamera kayıtlarının ilgili kişinin imzaladığı bu aydınlatma bildirimine istinaden hukuken geçerli sebeplere dayanılarak işlendiği, söz konusu kamera görüntülerinin ilgili kişinin çalışma arkadaşına hakaret içerikli sözlerde bulunarak fiziksel şiddet uygulaması sonucu iş akdinin feshedilmesine ilişkin delil olarak mahkemeye sunulduğu belirtilmiştir.

- Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulunun 25/06/2020 tarihli ve 2020/494 sayılı kararı ile,
- Kanunun amacının; kişisel verilerin işlenmesinin disiplin altına alınması ile temel hak ve özgürlüklerin korunması, kişinin mahremiyet hakkı ile bilgi güvenliğinin korunması ve ayrıca kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek olduğu,
- Kanunun kapsamına ilişkin 2 nci maddesi uyarınca; Kanun hükümlerinin, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanacağı,
- Kanunun “Tanımlar” başlıklı 3 üncü maddesinde; “kişisel veri”nin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi; “ilgili kişi”nin kişisel verisi işlenen gerçek kişi, “veri sorumlusu”nun kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi; “kişisel verilerin işlenmesi”nin ise kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı,
- Kanunun 5 inci maddesinde kişisel verilerin işleme şartlarına yer verilmiş olduğu; buna göre maddenin (1) numaralı fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması hallerinden birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğunun hükme bağlandığı,

- Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinde, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği ve buna göre, kişisel verilerin ancak; “a) Hukuka ve dürüstlük kurallarına uygun olma, b) Doğru ve gerektiğinde güncel olma, c) Belirli, açık ve meşru amaçlar için işlenme, ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ile d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme” ilkelerine uygun işlenebileceği,
- İlgili kişinin Kuruma ilettiği şikayet başvurusundan, bahsi geçen kamera görüntülerinin ilgili kişinin çalışma arkadaşına hakaret içerikli sözlerde bulunarak fiziksel şiddet uygulaması sonucu iş akdinin haklı nedenle feshedildiğine dair delil olmak üzere işveren vekili tarafından mahkemeye sunulduğunun anlaşıldığı,
- Veri sorumlusu tarafından ilgili kişinin başvurusuna cevap olarak iletilen ihtarname örneğinde, ilgili kişinin imzaladığı kişisel veriler hakkında bilgilendirme metni gereğince aktarma merkezinde kamera kaydı alındığına ilişkin olarak ilgili kişiye bilgilendirme yapıldığı, ilgili kişinin imzaladığı bu aydınlatma bildirimine göre veri sorumlusunca kamera kayıtlarının hukuken geçerli sebeplere dayanılarak işlendiği ve Kanunun 5 inci maddesinin (2) numaralı fıkrasının (e) bendindeki; “Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması” hukuki sebebi uyarınca taraflar arasında görülen işe iade davasında, iş akdinin haklı nedenle fesih sebebinin kanıtlanması amacıyla mahkemeye sunulduğunun açıklandığı,
- 6100 sayılı Hukuk Muhakemeleri Kanununun “Dava dilekçesinin içeriği” başlıklı 119 uncu maddesinin;

“(1) Dava dilekçesinde aşağıdaki hususlar bulunur:

Mahkemenin adı.

Davacı ile davalının adı, soyadı ve adresleri.

Davacının Türkiye Cumhuriyeti kimlik numarası.

ç) Varsa tarafların kanuni temsilcilerinin ve davacı vekilinin adı, soyadı ve adresleri.

Davanın konusu ve malvarlığı haklarına ilişkin davalarda, dava konusunun değeri.

Davacının iddiasının dayanağı olan bütün vakıaların sıra numarası altında açık özetleri.

İddia edilen her bir vakıanın hangi delillerle ispat edileceği.

Dayanılan hukuki sebepler.

ğ) Açık bir şekilde talep sonucu.

Davacının, varsa kanuni temsilcisinin veya vekilinin imzası.

(2) Birinci fıkranın (a), (d), (e), (f) ve (g) bentleri dışında kalan hususların eksik olması hâlinde, hâkim davacıya eksikliği tamamlaması için bir haftalık kesin süre verir. Bu süre içinde eksikliğin tamamlanmaması hâlinde dava açılmamış sayılır.”

hükmünü haiz olduğu,

- 6100 sayılı Kanunun “Cevap dilekçesinin içeriği” başlıklı 129 uncu maddesinde;

“(1) Cevap dilekçesinde aşağıdaki hususlar bulunur:

a) Mahkemenin adı.

b) Davacı ile davalının adı, soyadı ve adresleri; davalı yurt dışında ise açılan dava ile ilgili işlemlere esas olmak üzere yurt içinde göstereceği bir adres.

c) Davalının Türkiye Cumhuriyeti kimlik numarası.

ç) Varsa, tarafların kanuni temsilcilerinin ve davacı vekilinin adı, soyadı ve adresleri.

d) Davalının savunmasının dayanağı olan bütün vakıaların sıra numarası altında açık özetleri.

e) Savunmanın dayanağı olarak ileri sürülen her bir vakıanın hangi delillerle ispat edileceği.

f) Dayanılan hukuki sebepler.

g) Açık bir şekilde talep sonucu.

ğ) Davalının veya varsa kanuni temsilcisinin yahut vekilinin imzası.

(2) 121 inci madde hükmü cevap dilekçesi hakkında da uygulanır.”

hükmünün yer aldığı,

- Bu kapsamda Kuruma iletilen şikayet başvurusundan, 6100 sayılı Hukuk Muhakemeleri Kanunu uyarınca hangi unsurları barındırması gerektiği belirlenen cevap dilekçesinde veri sorumlusunun savunmaya yönelik dayandığı vakıaları beyan dilekçesiyle mahkemeye sunduğunun anlaşıldığı, bu çerçevede Kanunun 8 inci maddesine uygun olarak Kanunun 5 inci maddesinin (2) numaralı fıkrasının (e) bendindeki; “Bir hakkın tesisi, kullanılması veya korunması için veri işleminin zorunlu olması” hukuki sebebi uyarınca söz konusu kamera kaydının mahkemeye sunulmasının hukuka uygun bir veri işleme faaliyeti olduğu,

- İlgili kişinin veri sorumlusu kargo şirketi tarafından açık rızası alınmaksızın kamera kaydının alındığı iddiası karşısında; veri sorumlusunun daha önceden, ilgili kişinin imzaladığı kişisel veriler hakkında bilgilendirme metni gereğince aktarma merkezinde kamera kaydı alındığına ilişkin olarak ilgili kişiye bilgilendirme yapıldığı, ilgili kişinin imzaladığı bu aydınlatma bildirimine göre veri sorumlusunca kamera kayıtlarının hukuken geçerli sebeplere dayanılarak işlendiği” beyanı çerçevesinde değerlendirme yapıldığında; veri sorumlusunun ilgili kişinin açık rızasının alındığını tevsik edici belgeyi sunmadığı, ancak veri sorumlusunun kargo şirketi olduğu göz önüne alındığında;

Bilgi Teknolojileri ve İletişim Kurulunun 2016/DK - YED/517 sayılı kararı ile onaylanan "Posta Gönderilerine İlişkin Güvenlik Tedbirlerine Yönelik Usul ve Esaslar" düzenlemesinin "Posta gönderilerinin görüntüleme cihazları ile kontrolü" başlıklı 6 ncı maddesinin ikinci fıkrasında yer alan, "Hizmet sağlayıcılarının posta gönderilerini kabul merkezlerinde kamera sistemi kurularak kayıtlar, gerektiğinde ilgili mercilere sunulmak üzere en az bir (1) ay süreyle saklanır." hükmü gereğince veri sorumlusu kargo şirketinin, Kanununun 5 inci maddesinin ikinci fıkrasının (a) bendinde yer alan; "Kanunlarda açıkça öngörülmesi" hukuki sebebine uygun olarak işleme yaptığı değerlendirmelerinden hareketle, söz konusu şikayet ile ilgili olarak Kanun kapsamında yapılacak bir işlem bulunmadığına karar verilmiştir.

2020/482 sayılı KVKK Kararı

Veri Sorumluları Siciline Kayıt Tarihlerinin Uzatılması ile İlgili Kişisel Verileri Koruma Kurulunun 23/06/2020 Tarihli ve 2020/482 Sayılı Kararı

Karar Tarihi : 23.06.2020

Karar No : 2020/482

Konu Özeti : Veri Sorumluları Siciline kayıt tarihlerinin uzatılması

RG Tarih ve Sayısı: 25.06.2020/31166

Tüm dünyada olduğu gibi ülkemizde de etkisini gösteren Covid-19 virüs salgını nedeniyle bazı işyerlerinin fiziksel olarak kapalı olduğu veya uzaktan / dönüşümlü çalışma modeli uygulandığı, bu nedenle veri sorumlularınca kişisel veri işleme envanteri hazırlama çalışmalarının yapılamadığı ve Veri Sorumluları Siciline (Sicil) kayıt yükümlülüğünün süresinde yerine getirilemediği gerekçesiyle Sicile kayıt sürelerinin uzatılmasına ilişkin Türkiye Odalar ve Borsalar Birliği (TOBB) ile muhtelif sektör temsilcileri tarafından Kuruma intikal ettirilen taleplerin değerlendirilmesi neticesinde;

- Yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları ile yurtdışında yerleşik gerçek ve tüzel kişi veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmeleri için belirlenen sürenin 30.09.2020 tarihine,
- Yıllık çalışan sayısı 50'den az ve yıllık mali bilançosu 25 milyon TL' den az olup ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek ve tüzel kişi veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.03.2021 tarihine,
- Kamu kurum ve kuruluşu veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.03.2021 tarihine,

kadar uzatılmasına,

- Anılan kararın Kurum internet sayfasında duyurulması ve Resmi Gazete'de yayımlanmasına oybirliği ile karar verilmiştir.

2020/471 sayılı KVKK Kararı

Ülkemizde temsilciliği bulunan bir yabancı bankanın 6698 sayılı Kanun kapsamında veri sorumlusu sayılıp sayılmayacağı ve Veri Sorumluları Siciline kayıt yükümlülüğü hakkındaki görüş talebi ile ilgili olarak Kişisel Verileri Koruma Kurulunun 23.06.2020 tarihli ve 2020/471 sayılı Karar Özeti

Karar Tarihi : 23.06.2020

Karar No : 2020/471

Konu Özeti : Ülkemizde temsilciliği bulunan bir yabancı bankanın, verdiği hizmetler kapsamında kişisel verilerin işlenmesi bakımından 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca veri sorumlusu statüsünü taşıyıp taşımayacağı ve Sicile kayıt yükümlülüğü hakkında

Kurumumuza iletilmiş olan; hizmet verdikleri tüzel kişiler bünyesinde çalışan gerçek kişilere ait kişisel verileri işlemekte olan ve ülkemizde temsilciliği bulunan bir yabancı bankanın, yürüttüğü bu işleme faaliyetleri sebebiyle 6698 sayılı Kişisel Verilerin Korunması Kanununa (Kanun) göre veri sorumlusu sıfatını haiz olup olmayacağı ve Veri Sorumluları Siciline (Sicil) kayıt yükümlülüğünün bulunup bulunmadığı hususundaki görüş talebinin Kişisel Verileri Koruma Kurulunca değerlendirilmesi neticesinde verilen kararın özetine aşağıda yer verilmektedir.

Bankacılık Düzenleme ve Denetleme Kurulunun iznine bağlı olarak açılabilen ve Bankacılık Düzenleme ve Denetleme Kurumunun resmi internet sitesinde bir liste halinde yayımlanan yabancı bankaların Türkiye temsilciliklerinde, 01/04/2008 tarihli ve 26834 sayılı Resmi Gazetede yayımlanan Türkiye'de Açılan Temsilciliklerin Faaliyetlerine İlişkin Usul ve Esaslar Hakkında Tebliğin "Yasaklar" başlıklı 9 uncu maddesinin birinci fıkrası uyarınca bağlı bulunulan banka veya bir başka banka veya finansal kuruluş adına mevduat veya katılım fonu kabul edilememekte, kredi kullandırılmamakta veya 5411 sayılı Bankacılık Kanununun 4 üncü maddesinde belirtilen diğer bankacılık faaliyetleri gerçekleştirilememektedir.

Öte yandan, anılan Tebliğin "Faaliyetlerin kapsamı" başlıklı 4 üncü maddesinde temsilciliklerde bağlı bulunulan banka adına, bankanın ve sunduğu hizmetlerin tanıtımı, Türkiye'de kurulu kredi

kuruluşları veya finansal kuruluşlarla olan ilişkilerin güçlendirilmesi, piyasa araştırması yapılması ve toplanan bilgilerin merkeze raporlanması faaliyetlerinin yürütülebileceği düzenlenmiştir.

Görüş talebinde bulunan bankanın, sağladığı finansman hizmetleri kapsamında Türkiye’de mukim ilgili kişilerin kişisel verilerini işlediği anlaşılmaktadır. Bu kapsamda, mezkûr bankanın temsilciliğinin ülkemizde gerçekleştirdiği faaliyetler, bu bankanın bankacılık faaliyetleri çerçevesinde gerçekleştirdiği kişisel veri işleme faaliyetlerinden ayrı tutulamayacaktır. Zira, anılan Tebliğin 4 üncü maddesinde de belirtildiği üzere temsilciliğin, bankanın sunduğu hizmetler hakkında ülkemizde tanıtım faaliyetlerinde bulunması ve piyasa araştırması yaparak bağlı bulunduğu bankaya elde ettiği bilgileri aktarması mümkündür. Bu etkinliklerin, yurt dışında yerleşik bankanın faaliyetlerine katkı yapacağı açıktır. Bu sebeple, temsilciliğin faaliyetlerinin bankanın kişisel veri işleme faaliyetleri ile sıkı bir bağlantı içerisinde olduğunun kabul edilmesi gerekmektedir.

Aynı doğrultuda Avrupa Veri Koruma Kurulunun Genel Veri Koruma Tüzüğü’nün (GVKT) yer bakımından uygulama kapsamına ilişkin 3/2018 sayılı Kılavuz İlkelerinde de, örneğin üçüncü ülkede yerleşik bir şirketin tanıtım ve piyasa araştırması ile ilgili faaliyette bulunan bir ofisinin Birlik sınırları içerisinde yerleşik olması ve bu ofisin faaliyetlerinin veri sorumlusu sıfatını haiz üçüncü ülkede yerleşik şirketin gelirlerini arttırmasını sağlaması halinde GVKT hükümlerinin yurt dışında yerleşik veri sorumlusunun kişisel veri işleme faaliyetlerine uygulanacağı ifade edilmiştir.

Diğer taraftan, temsilciliği aracılığıyla ülkemizdeki sürekli mevcudiyeti karşısında, bankanın yurtdışında yerleşik olması ve bütün kişisel veri işleme faaliyetlerini yurtdışında gerçekleştirdiği gerekçesiyle bu veri işleme faaliyetleri bakımından Kanunun uygulama alanı bulmayacağıın kabulü Kanunun amacıyla bağdaşmayacaktır.

Özellikle kişisel veri işleme süreçlerinin şeffaf bir biçimde yürütülmesine yönelik olarak Kanunun 16 ncı maddesinde öngörülen Sicile bildirim ve kayıt yükümlülüğü ile, ilgili kişilerin kişisel verileri üzerinde en üst düzeyde kontrolünün sağlanmasının amaçlandığı göz önünde bulundurulduğunda yurtdışında yerleşik veri sorumlusu bankanın işleme faaliyetleri bakımından Kanuna tabi olması gerektiği ve bu kapsamda Sicile kayıt yükümlülüğünün bulunduğu değerlendirilmektedir.

Ayrıca belirtmek gerekir ki, 30.12.2017 tarihli ve 30286 sayılı Resmi Gazetede yayımlanan Veri Sorumluları Sicili Hakkında Yönetmeliğin 5 inci maddesinin birinci fıkrasının (b) bendinde ülkemizde yerleşik olmayan veri sorumlularının kişisel veri işlemeye başlamadan önce temsilcileri vasıtasıyla Sicile kaydolmak zorunda oldukları hükme bağlanmıştır.

Öte yandan, Kurulun 24/01/2019 tarihli ve 2019/10 sayılı Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kararında da *“Veri ihlalinin yurtdışında yerleşik veri sorumlusu nezdinde yaşanması halinde, bu ihlalin sonuçlarının Türkiye’de yerleşik ilgili kişileri etkilemesi ve ilgili kişilerin sunulan ürün ve hizmetlerden Türkiye’de faydalanmaları durumunda, bu veri sorumlusu tarafından da aynı esaslar çerçevesinde Kurula bildirimde bulunulmasına (...) karar verilmiştir.”* ifadesine yer verilmiştir.

Yukarıda yer verilen açıklamalar doğrultusunda Kişisel Verileri Koruma Kurulunca yapılan değerlendirme sonucunda;

- kişisel verilerin korunmasını isteme hakkının Anayasanın 20 nci maddesinin üçüncü fıkrasında düzenlenmiş bir temel hak ve özgürlük olduğu,
- veri koruma düzenlemelerinin yer bakımından uygulama alanının belirlenmesinde, bireylere en üst düzeyde ve en geniş kapsamda korumayı sağlayan bir yaklaşımın benimsenmesi gerektiği,
- görüş talebinde bulunan yabancı bankanın temsilciliği vasıtasıyla ülkemizdeki sürekli mevcudiyeti hususları göz önünde bulundurulduğunda, mezkûr bankanın kişisel veri işleme faaliyetleri açısından 6698 sayılı Kanunun uygulama alanı bulacağına ve bu kapsamda söz konusu yabancı bankanın veri sorumlusu sıfatını haiz olduğuna ve Sicile kayıt yükümlülüğünün bulunduğuna karar verilmiştir.

2020/466 sayılı KVKK Kararı

Bir sigorta şirketinin acentesinde gerçekleşen veri ihlali hakkında Kişisel Verileri Koruma Kurulunun 16.06.2020 tarih ve 2020/466 sayılı Karar Özeti

Karar Tarihi : 16.06.2020

Karar No : 2020/466

Konu Özeti : Bir sigorta şirketinin acentesinde gerçekleşen veri ihlali hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin veri sorumlusu Sigorta şirketinin bir acentesinde işletmelerine ait bilgisayar ekranına bir hacker tarafından erişim sağlanmasıyla gerçekleştiği,
- İhlalin; veri işleyenin verdiği şikayetçi ifade tutanağı ile anlaşıldığı, ilgili tutanağa göre; Acente tarafından kullanılan bilgisayarlarda yazışma ekranının açıldığı, yetkisiz kişinin bu ekran aracılığıyla iletişim kurup fidye istediği, saldırının bu şekilde tespit edildiği,
- İhlalin 13.02.2020 tarihinde gerçekleştiği, 20.02.2020 tarihinde tespit edildiği ve 22.02.2020 tarihinde Kurumumuza bildirildiği,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik ve finans verileri olduğu,
- İhlalden etkilenen kişi sayısının 172 olduğu,
- Acente yetkilisinin ihlalin gerçekleşmesinden sonra kişisel verilerin korunması ile ilgili eğitim aldığı,

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 16.06.2020 tarih ve 2020/466 sayılı Kararı ile;

- Veri ihlalinin 13.02.2020 tarihinde veri işleyenin sistemlerine yetkisiz erişim sağlanmasıyla gerçekleştiği, ihlalin veri sorumlusu tarafından 20.02.2020 tarihinde tespit edildiği,
- Veri sorumlusu sigorta şirketinin, veri işleyen acenteye donanımı kendilerinin temin etmediği, vakaya konu bilgisayarın veri işleyen kendisine ait olduğu, bu nedenle bilgisayar üzerinde veri

işleyenin kendi aktivite ve kullanıcı kayıtlarının veri sorumlusu tarafından yönetilmediği ve sızma testlerinin yapılmadığı hususlarını belirtildiği, ayrıca; Acente Bilgi Güvenliği İlkeleri dokümanında; Acentelerin bilgi güvenliği politikasına uyumlu olmasını temin etmek için, Bilgi Güvenliği veya Risk Yönetimi ve İç Kontrol birimleri tarafından denetlemelerin yapılabileceği ve gerektiği takdirde ve periyodik olarak kurum dışı bağımsız kaynaklara güvenlik ile uyum test ve denetlemelerin yaptırıldığı ifadelerine de yer verilmiş olmasına rağmen veri işleyenin herhangi bir şekilde denetlenmemesinin, Kurumumuz tarafından yayınlanan Kişisel Veri Güvenliği Rehberinin (Teknik ve İdari Tedbirler-Rehber) 2.5 maddesinde “Veri İşleyenler ile İlişkilerin Yönetimi” başlığı altında; “...veri sorumlularının, hizmet alırken söz konusu veri işleyenlerin kişisel veriler konusunda en az kendileri tarafından sağlanan güvenlik seviyesinin sağlandığından emin olmaları gerekmektedir. Zira Kanununun 12 nci maddesinin ikinci fıkrası gereği veri işleyenler de kişisel verilerin güvenliğinin sağlanması konusunda veri sorumlusuyla müştereken sorumludur.” ifadelerine aykırılık teşkil ettiği,

- Veri sorumlusu tarafından; ilgili bilgisayar hemen olayın akabinde formatlandığı için herhangi bir araştırmanın yapılamadığı, herhangi bir kişisel veriye erişilip erişilmediğinin tespit edilmediği, veri işleyenin ifadesine istinaden araç ruhsatı üzerinde bulunan kimlik bilgileri ile kredi kartı bilgileri kategorilerinin seçildiği belirtilmiş olup bu durumun Rehber’in 3.6. maddesinde; “Kişisel Verilerin Yedeklenmesi” başlığı altında; “...Kişisel verilerin herhangi bir sebeple zarar görmesi, yok olması, çalınması veya kaybolması gibi hallerde veri sorumlularının yedeklenen verileri kullanarak en kısa sürede faaliyete geçmesi...” ifadelerine aykırılık teşkil ettiği,

- Acente yetkilisinin kişisel verilerin korunması ile ilgili eğitimi veri ihlalinin gerçekleşmesinden sonra almış olduğu, Rehber’in 2.2. maddesinde; “Çalışanların Eğitilmesi ve Farkındalık Çalışmaları” başlığının altında; “...çalışanların, kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi konular hakkında eğitim almaları, çalışanlara yönelik farkındalık çalışmaları yapılması ve güvenlik risklerinin belirlenebildiği bir ortam oluşturulması kişisel veri güvenliğinin sağlanması bakımından çok önemlidir. Veri sorumlusu nezdinde çalışan herkesin hangi konumda çalıştığına bakılmaksızın kişisel veri güvenliğine ilişkin rol ve sorumlulukları, görev tanımlarında belirlenmeli ve çalışanların bu konudaki rol ve sorumluluğunun farkında olması sağlanmalıdır.” ifadelerine aykırı olarak veri sorumlusu tarafından eğitim ve farkındalık çalışmalarının yapılmasının veri sorumlusu tarafından sağlanmadığı,

- Veri işleyenin Windows 7 Professional x64 işletim sistemini kullandığı, Windows’un resmi sayfası üzerinden yapılan duyuruda; Windows 7 işletim sisteminin 14.01.2020 tarihinden itibaren artık yeni Microsoft Security Essentials yüklemelerini desteklememekte olduğundan tüm müşterilerin en iyi

güvenlik seçeneği olan Windows 10 ve Windows Defender Virüsten Koruma'ya geçmelerini önerildiği, Rehber'in 2.3 maddesinde; Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Belirlenmesi başlığı altında; "...hemen hemen her yazılım ve donanımın bir takım kurulum ve yapılandırma işlemlerine tabi tutulması gerektiği, ancak yaygın şekilde kullanılan bazı yazılımların özellikle eski sürümlerinin belgelenmiş güvenlik açıkları bulunmakta..." olduğunun belirtildiği, bahsi geçen işletim sisteminin hâlihazırda eski bir sürüm olduğu ve 14.01.2020 tarihinden itibaren güvenlik korumasıyla ilgili güncellemeleri desteklemediği hususlarının gerekli güvenlik önlemlerinin veri sorumlusu ve veri işleyen tarafından tam olarak alınmadığını gösterdiği,

- Veri işleyen tarafından veri ihlali öncesinde anti-virüs yazılımının hiç kullanılmamakta olmasının Rehber'in 3.2 maddesinde "Siber Güvenliğin Sağlanması başlığı altında"; "...Kötü amaçlı yazılımlardan korunmak için ayrıca, bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden antivirüs, antispam gibi ürünlerin kullanılması gerekmektedir. Ancak bu ürünlerin sadece kurulumu yeterli olmayıp güncel tutularak gereken dosyaların düzenli olarak tarandığından emin olunmalıdır.", 27 Nisan 2020 tarihinde veri sorumlusunun acentelerin siber saldırılardan korunmalarına yönelik yapmış olduğu duyuruda; Tüm kullanıcı bilgisayarlarına anti-virüs yazılımlar yüklenmesi ve kullanıcılar anti-virüs yazılımlarını kapatmaması veya ayarlarını değiştirmemesinin gerektiği, 01.11.2019 tarihli ve veri sorumlusunun acentelerine 21.01.2020 tarihinde duyurulan Acente Bilgi Güvenliği İlkeleri dokümanında yer alan; tüm kullanıcı bilgisayarlarına anti-virüs yazılımlarının yüklendiği, acente kullanıcılarının anti-virüs yazılımlarını kapatmadığı veya ayarlarını değiştiremediği, ifadelerine aykırı olarak veri sorumlusu ve veri işleyen tarafından bahse konu güvenlik önlemlerinin yerine getirilmediği hatta veri sorumlusunun kendi hazırlamış olduğu dokümanların gereklerinin dahi sağlanmadığı

hususları dikkate alındığında, Kanun'un 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 172.000 TL idari para cezası uygulanmasına,

- Veri ihlalden etkilenen 172 ilgili kişiden 95 kişiye veri ihlalinin bildirilmediği,
- İhlalin bildirildiği 77 kişiden 33'üne bildirim 26.03.2020, 9'una 16.04.2020, 35'ine 20.04.2020 tarihinde yapıldığı, dolayısıyla ihlalin tespit tarihi ile bildirim tarihleri arasında 1 ayı aşkın süre bulunduğu

dikkate alındığında, Kanununun 12 nci maddesinin (5) numaralı fıkrasında yer verilen “en kısa sürede” (ilgili kişilere bildirim için) bildirimde bulunma yükümlülüğünün 24.01.2019 tarih 2019/10 sayılı Kararda yer verilen “ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılması” şeklinde de yapılabileceği hususunun veri sorumlusuna hatırlatılmasına

karar verilmiştir.

2020/465 sayılı KVKK Kararı

Kurumsal yazılım hizmeti sunan bir veri sorumlusunun veri ihlali bildirimini hakkında Kişisel Verileri Koruma Kurulunun 16/06/2020 tarih ve 2020/465 sayılı Karar Özeti

Karar Tarihi : 16.06.2020

Karar No : 2020/465

Konu Özeti : Kurumsal yazılım hizmeti sunan bir veri sorumlusunun veri ihlali bildirimini hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlali bildiriminde;

- Siber suçlularının “parola püskürtme” saldırısı ile veri sorumlusunun bilgi sistemleri iç ağına eriştiklerini bilgisinin 6 Mart 2019 tarihinde emniyet birimlerinin siber güvenlik uzmanları tarafından veri sorumlusuna bildirildiği,
- Bilgilendirme sonrası, veri sorumlusu siber suçluları kendi dahili sistemlerinden çıkarmak için harici adli bilişim ve güvenlik uzmanlarını görevlendirdiği ve ek güvenlik önlemleri aldığı, ayrıca önde gelen bağımsız bir siber güvenlik firması tarafından yönetilen kapsamlı bir adli soruşturma çalışması başlattığı,
- Parola püskürtme saldırılarının, saldırganların kurumsal kullanıcı hesaplarında başarıyla kimlik doğrulaması yapmasını sağladığı,
- Saldırganlar, 5 kullanıcı hesabı için kimlik doğrulama anahtarını kaydettiği, bu da bir cep telefonu ortamı dışındaki XenDesktop Sanal Masaüstü Altyapısı (VDI) ortamına erişimi mümkün kıldığı,
- Ekim 2018'den Mart 2019'a kadar altı ayrı durumda, Dosya Aktarım Protokolü (FTP) ve Güvenli Dosya Aktarım Protokolü'nü (SFTP) kullanarak verileri dışarı sızdırdığı,
- Veri sorumlusu soruşturma sırasında 6 terabayttan fazla verinin muhtemelen sistemlerinden dışarı sızdığını öğrendiği,
- 06.03.2019 tarihinde tespit edilen veri ihlali, 29.04.2020 tarihinde Kurumumuza bildirildiği,
- İhlalden 22 gerçek kişiye ait kimlik (ad soyad, TCKN), özlük (iş beyanları, müşteri bağlılık belgeleri) ve finans (satış kayıtları, pazarlama materyalleri, bordro) verilerinin etkilendiği,

- İhlalden etkilenen 18 çalışanına (7 eski çalışan, 11 halihazırda çalışıyor olan) ihlal sonrası posta yolu ile 29 Nisan 2019 tarihinde bildirim yapıldığı, fakat Türkiye’de ikamet ettikleri düşünülen 4 kişinin ise iletişim bilgileri kendilerinde mevcut olmadığı için bildirim yapamadıkları,

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 16/06/2020 tarih ve 2020/465 sayılı Kararı ile;

- Veri sorumlusunun veri ihlalini, gerçekleşme tarihinden yaklaşık 5 ay sonra 06 Mart 2019’ da tespit ettiği ve bu durumun; Kurumumuz tarafından yayınlanan Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)’nde 3.2. Kişisel Veri Güvenliğinin Takibi başlığında “... güvenlik yazılımı mesajları, erişim kontrolü kayıtları ve diğer raporlama araçlarının düzenli olarak kontrol edilmesi, bu sistemlerden gelen uyarılar üzerine harekete geçilmesi, bilişim sistemlerinin bilinen zaafiyetlere karşı korunması için düzenli olarak zaafiyet taramaları ve sızma testlerinin yapılması ile ortaya çıkan güvenlik açıklarına dair testlerin sonucuna göre değerlendirmeler yapılması gerekmektedir.” ifadesi gereği, veri sorumlusu tarafından gerekli güvenlik kontrol ve denetimlerinin zamanında yapılmadığının göstergesi olduğu,

- Parola püskürtme saldırıları, çok sayıdaki hesaba zayıf olarak nitelendirilen parolalar kullanarak erişen kullanıcıların, parolalarının saldırganlar tarafından şifre tahmini yöntemiyle ele geçirilmesi şeklinde gerçekleştiği, söz konusu ihlalin; Kurumumuz tarafından yayınlanan Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)’nde 2.2. Çalışanların Eğitilmesi ve Farkındalık Çalışmaları başlığında “... kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi konular hakkında eğitim almaları, çalışanlara yönelik farkındalık çalışmaları yapılması ve güvenlik risklerinin belirlenebildiği bir ortam oluşturulması kişisel veri güvenliğinin sağlanması bakımından çok önemlidir.” ifadesine göre, veri sorumlusunun son kullanıcıları tarafından parola güvenliği farkındalığının tam olarak oluşmamasından kaynaklandığı,

- Bir paylaşım sürücüsünde bulunan 6 TB’tan fazla verinin çalınmasının, bu paylaşım sürücüsünde yüksek miktarda veri depolanması durumundan kaynaklanması sebebiyle, Kurumumuz tarafından yayınlanan Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)’nde 2.1. Mevcut Risk ve Tehditlerin Belirlenmesi başlığında “Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir....Bu risklerin tanımlanması ve önceliğinin belirlenmesinden sonra; söz konusu risklerin azaltılması ya da

ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmeli, gerekli teknik ve idari tedbirler planlanarak uygulamaya konulmalıdır” ifadesi gereği, bu gibi saldırılara karşı veri kaybı riskini azaltmaya yönelik gerekli idari tedbirleri almadıkları,

dikkate alındığında Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 75.000 TL,

- 06.03.2019 tarihinde tespit edilen veri ihlali, veri sorumlusu tarafından 29.04.2019 tarihinde Kurumumuza bildirilmiş olup bu durumda Kurumumuza 55 günlük geç bildirimde bulunduğu,
- Veri sorumlusunun ihlalden etkilenen ilgili kişilere ihlal tespit edildikten 55 gün sonra bildirim yaptığı

dikkate alındığında, Kanunun 12’nci maddesinin (5) numaralı fıkrasında yer verilen “en kısa sürede” bildirimde bulunma yükümlülüğüne aykırılık teşkil etmesi nedeniyle veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 50.000 TL

olmak üzere toplam 125.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2020/463 sayılı KVKK Kararı

İlaç sektöründe faaliyet yürüten bir veri sorumlusunun veri ihlali bildirimini hakkında Kişisel Verileri Koruma Kurulunun 16/06/2020 tarih ve 2020/463 sayılı Karar Özeti

Karar Tarihi : 16.06.2020

Karar No : 2020/463

Konu Özeti : İlaç sektöründe faaliyet yürüten bir veri sorumlusunun veri ihlali bildirimini hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlali bildiriminde;

- Veri ihlalinin zararlı yazılımlardan ve fidye yazılımlarından kaynaklı bir siber saldırı olarak veri sorumlusunun yetkili kullanıcı şifresi ele geçirilerek sistemlerine erişimin engellenmesi şeklinde gerçekleştiği ve saldırının çalışanlarının sistemlere erişememesi sonucu tespit edildiği,
- Veri sorumlusunun faaliyetlerini sürdürmesi için kritik öneme sahip tüm sunucu ve verilerinin ve bunlara ek olarak diğer sunucuların yedek dosyalarının depolandığı Data Domain Sunucusu verilerinin silindiği,
- Yetkisiz erişim sağlama girişimlerinin 8 - 11 - 12 Ocak tarihlerinde gerçekleştiği, saldırının 12/01/2020 tarihinde tespit edildiği,
- Veri sorumlusunun yaptığı incelemede, saldırının, LDAP servislerinde kullanılan Domain Admin yetkili anonim isimli bir kullanıcı hesabı ile gerçekleştirildiği, ihlalin yapılmış olduğu bilgisayarın tespit edildiği ve şüpheliler aleyhine İstanbul Cumhuriyet Başsavcılığına şikâyette bulunulduğu,
- Saldırının veri sorumlusunun bizzat siber güvenlik desteği almakta olduğu firmaya ait IP adresi üzerinden ve firma çalışanı tarafından gerçekleştirildiğinin tespit edildiği ve bu tespitin firma tarafından kabul edildiği,
- İhlali gerçekleştiren siber güvenlik desteği alınan firmanın çalışanının aynı zamanda veri sorumlusu eski çalışanı olduğu,
- İhlalden etkilenen kişi ve kayıt sayısının tam ve kesin olarak belirlenememiş olduğu ancak 1000 kişi civarında olduğunun tahmin edildiği belirtilmekte olup bunlardan 297 kişinin şirket çalışanı olduğu; bunlar dışında kalanların ise tedarikçi, müşteri ve taşeronlara ait olduğu, ifadelerine yer verilmiştir.

- Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 16/06/2020 tarih ve 2020/463 sayılı Kararı ile;
- Veri sorumlusunun faaliyetlerini sürdürmesi için kritik öneme sahip tüm sunucu ve verilerinin ve bunlara ek olarak diğer sunucuların yedek dosyalarının depolandığı Data Domain Sunucusu verilerinin silindiği,
- İhlalden etkilenen kişi ve kayıt sayısının tam ve kesin olarak belirlenememiş olduğu ancak 1000 kişi civarında olduğu ve ihlalden özel nitelikli kişisel verilerinde etkilenmiş olabileceği,
- Veri sorumlusu, sistemlerine düzenlenen söz konusu saldırıyı şirket çalışanlarının sistemlere erişememesi sonucu tespit ettiği; özel nitelikli kişisel veriler üzerinde çalışan çok uluslu bir şirketin, böylesi saldırılar için sızma testleri ve risk analizleri yapıp tehditleri belirlemesi ve güvenlik açıklarını kapatması ve log kaydı takibi ile veri güvenliğini sağlayacak önlemler alması gerektiği ve bu durumun Kişisel Veri Güvenliği Rehberi 3.2. maddesinde; “Kişisel Veri Güvenliğinin Takibi” başlığı altında; “...güvenlik yazılımı mesajları, erişim kontrolü kayıtları ve diğer raporlama araçlarının düzenli olarak kontrol edilmesi, bu sistemlerden gelen uyarılar üzerine harekete geçilmesi, bilişim sistemlerinin bilinen zaafiyetlere karşı korunması için düzenli olarak zaafiyet taramaları ve sızma testlerinin yapılması ile ortaya çıkan güvenlik açıklarına dair testlerin sonucuna göre değerlendirmeler yapılması gerekmektedir...” ifadelerine aykırılık teşkil ettiği,
- Veri sorumlusunun, sunucularının yedek dosyalarının depolandığı Data Domain sunucusunda yer alan verilerinin de silinmesinin, Kişisel Veri Güvenliği Rehberi 3.6. maddesinde; “Kişisel Verilerin Yedeklenmesi” başlığı altında; “...veri sorumlusunu fidye ödemeye zorlayan kötü amaçlı yazılımlar olabilir. Bu tür kötü amaçlı yazılımlara karşı kişisel veri güvenliğini sağlamak için veri yedekleme stratejilerinin geliştirilmesi önerilmektedir. Öte yandan, yedeklenen kişisel veriler sadece sistem yöneticisi tarafından erişilebilir olmalı, veri seti yedekleri mutlaka ağ dışında tutulmalıdır. Aksi halde, veri seti yedekleri üzerinde kötü amaçlı yazılım kullanımı veya verilerin silinmesi ve yok olması durumlarıyla karşı karşıya kalınabilecektir...” ifadelerine aykırılık teşkil ettiği,

hususları dikkate alındığında, Kanun’un 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 125.000 TL idari para cezası uygulanmasına

- İhlalden etkilenen şirket çalışanlarına 13.01.2020 tarihinde e-posta ile bildirim yapıldığı buna yönelik tevsik edici belgenin gönderildiği, ihlalden etkilenen şirket çalışanı dışındaki kişilere ise web

sayfasından genel duyuru yapıldığı ve yapılan bu duyurunun ise Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararı gerekliliğine uygun olduğu,

- 11.01.2020 tarihinde gerçekleşen veri ihlali, 12.01.2020 tarihinde tespit edilmiş ve Kurumumuza 14.01.2020 tarihinde bildirilmiş olup veri sorumlusunun Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen “en kısa sürede” (24.01.2019 tarih ve 2019/10 sayılı Kurul kararında belirtilen 72 saatlik süre içerisinde) bildirimde bulunma yükümlülüğüne uygun hareket ettiği

hususları dikkate alındığında; Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen “en kısa sürede” (Kurul’a bildirim için 72 saat) bildirimde bulunma yükümlülüğüne uygun davranan veri sorumlusu hakkında bu konuda yapılacak bir işlem bulunmadığına

karar verilmiştir.

2020/435 sayılı KVKK Kararı

Bir kargo firmasında çalışan ilgili kişinin iş akdinin haksız feshedilmesi sonrası özlük dosyası kapsamında yer alan kişisel verilerinin birer suretinin tarafına verilmesi talebine veri sorumlusu tarafından cevap verilmemesi hakkında Kişisel Verileri Koruma Kurulunun 28/05/2020 tarihli ve 2020/435 sayılı Karar Özeti

Karar Tarihi : 28.05.2020

Karar No : 2020/435

Konu Özeti : Bir kargo firmasında çalışan ilgili kişinin iş akdinin haksız feshedilmesi sonrası özlük dosyası kapsamında yer alan kişisel verilerinin birer suretinin tarafına verilmesine yönelik talebine veri sorumlusu tarafından cevap verilmemesi

İlgili kişiden alınan şikayet dilekçesinde özetle;

- Bir kargo firmasında denetim uzmanı olarak görev yaparken iş akdinin haksız, geçersiz ve tazminatsız olarak feshedildiği; tehdit, baskı ve türlü vaatlerde bulunularak tarafından ileri tarihli istifa dilekçesinin alınması sonrası özlük dosyası kapsamında yer alan kişisel verilerinin birer suretini 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 11 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında veri sorumlusu kargo firmasından talep etmesine rağmen, tarafına 30 gün içerisinde herhangi bir cevap verilmediği ifade edilerek Kanuna aykırı uygulaması nedeniyle veri sorumlusu hakkında yaptırım uygulanması ve özlük dosyası kapsamında yer alan kişisel verilerinin birer suretinin tarafına verilmesi amacıyla veri sorumlusunun talimatlandırılması talep edilmiştir.

Konuya ilişkin olarak başlatılan inceleme çerçevesinde veri sorumlusu kargo firmasından alınan savunmada;

- İlgili kişi tarafından noter kanalıyla yapılan başvurunun Kanunun 11 inci maddesi kapsamında bir başvuru olmadığı bu nedenle cevap verilmediği, ilgili kişinin 1. Noterliğinden keşide edilen ihtarnamesi incelendiğinde; *“İhtarın Konusu; tarafınızca iş akdim feshedilmeden önce tarafımdan almış olduğunuz 30.09.2019 tarihli önlü arkalı yazılı savunmamın tarafınızca tarafıma zorla imzalatılan 18.10.2019 tarihli istifa dilekçemin ve iş akdimin 17.10.2019 tarihinde tarafınızca feshi gerçekleştirildikten sonra aynı gün*

elden vermiş olduğum 17.10.2019 tarihli istifa dilekçemin birer örneğinin KVKK madde 11/1-b kapsamında tarafıma ibrazına ilişkin ihtarnamemdir." şeklindeki talebinde veri sorumlusundan kişisel verilerine ilişkin bilgi talep etmediği, kendisi tarafından veri sorumlusuna verilen belgelerin birer örneğini talep ettiği, Kanununun 11 inci maddesinde ilgili kişinin haklarının düzenlendiği, ilgili kişinin veri sorumlusuna başvurarak kendisinden sadır olan belgelerin birer örneğini alabileceğine veya belge örneklerini isteyebileceğine ilişkin bir hakkın da madde metninde düzenlenmediği, bu nedenle ilgili kişinin başvurusu her ne kadar 11 inci maddeye dayandırılrsa da başvuruda yer alan talebin Kanunda düzenlenen haklara ilişkin olmadığı, başvuru Kanunda düzenlenmeyen bir konu olan belge örneği talebi içerdiği için talebinin Kanununun 11 inci maddesi kapsamında karşılanmasının mümkün olmadığı,

- Ayrıca, ilgili kişi tarafından veri sorumlusuna başvurularak örneği talep edilen veri sorumlusuna vermiş olduğu dilekçelerin Kanun kapsamında "tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla" işlenen bir veri de olmadığı,

- İlgili kişi tarafından veri sorumlusuna noter aracılığıyla yapılan başvurusunun veri sorumlusuna ulaşma tarihinin 26.11.2019 olduğu, ilgili kişi tarafından ihtarname keşide edildikten 8 gün sonra henüz cevap verme süresi dolmadan bu defa 04.12.2019 tarihinde arabulucuya başvurularak konunun yargıya intikal ettirildiği,

- İlgili kişinin Kanununun 11 inci maddesi kapsamında düzenlenen "bilgiye erişim hakkını" kullanmak amacıyla olmadığı, bu yolla kendisine delil elde etmek amacıyla olduğu, kıdem ve itibar tazminatı ile sair işçilik alacaklarının kendisine ödenmesi amacıyla ... 26. İş Mahkemesinde açılan dava dosyasına sunulan dava dilekçesinin 9. sayfasındaki 33 nolu paragrafta açık bir şekilde; "Kaldı ki, müvekkilimizden daha öncesinde alınan istifa dilekçesinin ve savunmasının işbu davada delil olarak kullanılabilmesi için müvekkilimiz davalı tarafa başvurmuş ve kendilerine Noterliği nezdinde ... tarihli ve ... yevmiye no.lu ihtarı keşide ederek işbu belgelerin kendisine verilmesini talep etmiştir." hususunun ikrar edildiği,

- Türkiye Cumhuriyeti Anayasasınının 38 inci maddesinin 5 inci fıkrasında "Hiç kimsenin kendisini ve kanunda gösterilen yakınlarını suçlayan bir beyanda bulunmaya veya bu yolda delil göstermeye zorlanmayacağı"nın hükme bağlandığı, taraflarının "susma hakkı" olarak da ifade edilen bu hakkı kullandığı,

- İlgili kişinin cevap verilmeyen Noterliğinden keşide edilen ihtarnamede taraflarına karşı suç isnadında bulunulduğu ve kendisinden zorla imza alındığının iddia edildiğinin de izahtan varest

olduđu, bu nedenle ilgili kiřinin bařvurusunun Dilekçe Hakkının Kullanılması Kanununa da aykırı olduđu,

- İlgili kiřinin Kuruma 30.12.2019 tarihinde bařvurduđu, bu tarihten önce ilgili kiřinin 04.12.2019 tarihinde arabulucuya bařvurduđu, Kiřisel Verileri Koruma Kurulunun 24.12.2018 tarih ve 2018/156 sayılı Karar özetinde; *“6698 sayılı Kiřisel Verilerin Korunması Kanununun 15 inci maddesinin (2) numaralı fıkrasında 01.11.1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesinde “Yargı mercilerinin grevine giren konularla ilgili olan ihbar veya Őikayetlerin incelemeye alınamayacađının hkme bađlandıđı, Őikayete konu iddiaların Trk Ceza Kanunu hkmleri uyarınca su unsuru barındırdıđı ve bunların da bireysel su niteliđinde olduđu, bu kapsamda ilgili kiři tarafından da konunun yargıya intikal ettirilmif olduđu dikkate alındıđında sz konusu bařvurusunun Kanun kapsamında deđerlendirilemeyeceđine”* karar verildiđi, ilgili kiři tarafından Őikayet konusu yapılan hususun yargı mercilerinin grevine giren konularla ilgili olduđu, bu nedenle Őikayetin reddinin gerektiđi

beyanlarına yer verilmiřtir.

Konuya iliřkin yapılan inceleme neticesinde Kiřisel Verileri Koruma Kurulunun 28/05/2020 tarih ve 2020/435 sayılı Kararı ile;

- Kanunun “Tanımlar” bařlıklı 3 nc maddesinde “kiřisel veri”nin kimliđi belirli veya belirlenebilir gerek kiřiye iliřkin her trl bilgi olarak tanımlandıđı, Kanunun gerekesinde, sadece bireyin adı, soyadı, dođum tarihi ve dođum yeri gibi onun kesin teřhisini sađlayan bilgilerin deđil, aynı zamanda kiřinin fiziki, ailevi, ekonomik, sosyal ve sair zelliklerine iliřkin bilgilerin de bir kiřinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir Őekilde bir gerek kiřiyle iliřkilendirilmesi suretiyle, o kiřinin tanımlanabilir hale getirilmesini ifade ettiđinden kiřisel veri olarak tanımlandıđı, diđer bir ifadeyle, kiřinin fiziksel, ekonomik, kltrel, sosyal veya psikolojik kimliđini ifade eden somut bir ierik tařıyan veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtle iliřkilendirilmesi sonucunda kiřinin belirlenmesini sađlayan tm halleri kapsadıđı,

- Bu erevede ncelikli olarak, veri sorumlusundan alınan cevap yazısında ilgili kiřinin kiřisel verilerine iliřkin bilgi talep etmediđi, ilgili kiřinin veri sorumlusuna verdiđi belgelerin birer rneđini talep ettiđi iddiasına yer verilmiř olmakla birlikte Kanunun byk lde esas alınarak hazırlandıđı 95/46/EC sayılı Kiřisel Verilerin İřlenmesi ve Serbest Dolařımı Bakımından Bireylerin Korunmasına İliřkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifinin 29 uncu maddesi uyarınca kurulmuř olan Madde 29 alıřma Grubunun, kiřisel veri kavramına iliřkin 20/06/2007 tarihinde yayınladıđı grřnde *“Bir doktorun yazdıđı ila reetesinde yer alan bilgiler, doktor aısından kiřisel veridir. İster kiřiye zg reete olsun, ister belirli bir grup hastaya yazılan reetelerden ıkartılan genel bilgi formatında olsun, ilgili*

hastalar ister belirli ister anonim olsun, doktorun kimliği belirlenebilir olduğu müddetçe reçete bilgileri doktor açısından kişisel veridir.” örneğine yer verildiği, bu minvalde, kişisel veri kavramının kimliği belirli veya belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade ettiği,

- Dolayısıyla, veri sorumlusunun ilgili kişiden 30.09.2019 tarihinde aldığı yazılı savunma ve 18.10.2019 ile 17.10.2019 tarihli istifa dilekçelerinin içerik itibarıyla kişiye ilişkin bilgiler içerdiği ve bu bilgilerin ilgili kişiyi belirli veya belirlenebilir kıldığı, bu kişisel veriler sayesinde ilgili kişiye ulaşılabilir olduğu hususu göz önünde bulundurulduğunda bu bilgilerin kişisel veri niteliğinde olduğu sonucuna varıldığı,
- Kanunun 3 üncü maddesinde ayrıca “ilgili kişi”nin kişisel verisi işlenen gerçek kişi; “veri sorumlusu”nun, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi; “veri işleyen”in, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi; “kişisel verilerin işlenmesi”nin ise kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı,
- Bu minvalde, şikayet başvurusunda bulunan kişinin ilgili kişi, kargo firmasının veri sorumlusu, ilgili kişiye ait istifa dilekçesinin özlük dosyası kapsamında muhafaza edilmesinin ise veri işleme faaliyeti olduğu,
- Kanunun 4 üncü maddesinin (2) numaralı fıkrasında kişisel verilerin işlenmesinde uyulması zorunlu ilkelerin “a) hukuka ve dürüstlük kurallarına uygun olma, b) doğru ve gerektiğinde güncel olma, c) belirli, açık ve meşru amaçlar için işleme, ç) işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, d) ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme” şeklinde düzenlendiği,
- Kanunun “Kişisel verilerin işleme şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise Kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,

ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Anayasanın 20 nci maddesinin (3) numaralı fıkrasında “Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.” hükmüne yer verildiği,

- Kanununun 11 inci maddesinde ise “(1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili; a) Kişisel veri işlenip işlenmediğini öğrenme, b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme, c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme haklarına sahiptir.” hükmünün düzenlendiği,

- Kanununun 13 üncü maddesinin (1) numaralı fıkrasında da ilgili kişinin, bu Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna ileteceği, aynı maddenin (2) numaralı fıkrasında ise veri sorumlusunun başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandıracağını düzenlendiği, bununla birlikte Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğin (Tebliğ) 6 ncı maddesinin (2) numaralı fıkrasında da “Veri sorumlusu, başvuruyu kabul eder veya gerekçesini açıklayarak reddeder.” hükmüne yer verildiği,

- Yukarıda anıldığı üzere Anayasanın 20 nci maddesinin (3) numaralı fıkrasında yer verilen düzenleme ile “... kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme...” hakkına sahip olduğu, Kanununun 11 inci maddesinin (1) numaralı fıkrasının (b) bendi çerçevesinde ise ilgili kişilerin kişisel verileri işlenmişse buna ilişkin bilgi talep etme hakkına sahip olduğunun

düzenlendiği, bu çerçevede, ilgili kişinin veri sorumlusundan kişisel veri niteliğinde olan yazılı savunmasını ve istifa dilekçelerini Kanununun 11 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında talep ettiği, yukarıda anılan mevzuat kapsamında ilgili kişinin kişisel verilerine erişme hakkının olduğu ve bu hakkını veri sorumlusuna karşı ileri sürebileceğinin değerlendirildiği,

- Ayrıca, veri sorumlusunun cevap yazısında; Türkiye Cumhuriyeti Anayasasının 38 inci maddesinin 5 inci fıkrasında *“hiç kimsenin kendisini ve kanunda gösterilen yakınlarını suçlayan bir beyanda bulunmaya veya bu yolda delil göstermeye zorlanmayacağına”* hükme bağlandığı, taraflarının *“susma hakkı”* olarak da ifade edilen bu hakkını kullandığı iddialarına yer verildiği görülmekle beraber Anayasa Mahkemesinin 2011/41 Esas sayılı ve 2012/25 Karar sayılı kararında *“Anayasa’nın 38. maddesinde suç ve cezalara ilişkin temel ilkelere yer verilmiş, beşinci fıkrasında ‘Hiç kimse kendisini ve kanunda gösterilen yakınlarını suçlayan bir beyanda bulunmaya veya bu yolda delil göstermeye zorlanamaz.’ denilmiştir. İnsan hakları arasında yer alan, manevi işkenceyi meneden, insan haysiyetinin ve kişi dokunulmazlığının teminatı olan bu düzenlemeye, ceza yasalarında sanığın ‘susma hakkı’ olarak yer verilmiştir.”* denildiği, dolayısıyla Anayasanın 38 inci maddesinin (5) numaralı fıkrasının Anayasa Mahkemesinin anılan kararından da anlaşılacağı üzere gerçek kişileri esas alan bir düzenleme olduğu ve temel insan hakları arasında bir hak olarak değerlendirildiğinin anlaşıldığı,

- Veri sorumlusunun cevap yazısında; ilgili kişinin Kuruma 30.12.2019 tarihinde başvurduğu, bu tarihten önce ilgili kişinin 04.12.2019 tarihinde arabulucuya başvurduğu, bu anlamda Kişisel Verileri Koruma Kurulunun 24.12.2018 tarih ve 2018/156 sayılı karar özetine atıf yapılmak suretiyle ilgili kişi tarafından şikayet konusu yapılan hususun yargı mercilerinin görevine giren konularla ilgili olduğu, bu nedenle şikayetin reddinin gerektiği iddialarına yer verildiği, ancak ilgili kişinin Kurumu muhatap başvurusunda, veri sorumlusundan Kanununun 11 inci maddesi kapsamında özlük dosyasında yer alan yazılı savunmasının ve istifa dilekçelerini talep ettiğini belirterek, Kurumdan söz konusu kişisel verilerinin birer suretinin tarafına ibraz edilmemiş olması nedeniyle veri sorumlusu hakkında yaptırım uygulanmasını ve özlük dosyası kapsamında yer alan kişisel verilerinin birer suretinin tarafına verilmesini talebinde bulunduğu anlaşıldığı, esasen Kuruma intikal eden şikayetin konusunun kişisel verilere ilişkin olduğu ve suç unsuru da barındırmadığı sonucuna varıldığı,

- İlgili kişinin veri sorumlusuna karşı açmış olduğu davanın konusunun ise *“Fazlaya ilişkin her türlü talep ve dava hakkımız saklı kalmak ile şimdilik; 100 TL kıdem tazminatı, 100 TL ihbar tazminatı, 100 TL maaşından kesilen yıllık izin alacağının faizleri ile birlikte davalı şirketten alınarak müvekkile ödemesi talebine ilişkindir.”* şeklinde olduğunun anlaşıldığı, bu minvalde, açılan davanın kişisel verilere ilişkin bir dava

olmaması sebebiyle konunun kişisel verilere ilişkin olan yönünün Kurum tarafından ele alınmasında bir sakınca olmadığı

değerlendirmelerinden hareketle,

- İlgili kişinin başvurusunun, Kanunda düzenlenen haklara ilişkin olmadığı ve başvurusunun Kanunda düzenlenmeyen bir konu olan belge örneği talebi içerdiği için Kanunun 11 inci maddesi kapsamında karşılanmasının mümkün olmadığı gerekçesiyle veri sorumlusu tarafından 30 günlük yasal süre içerisinde cevaplandırılmadığı dikkate alındığında, ilgili kişiye ait kişisel veri niteliğindeki bilgilerini içeren 30.09.2019 tarihli savunma yazısı ile 18.10.2019 tarihli ve 17.10.2019 tarihli istifa dilekçelerinin birer örneğinin ilgili kişiye verilmesi hususunda Kanunun 15 inci maddesinin (5) numaralı fıkrası kapsamında veri sorumlusunun talimatlandırılmasına,
- Veri sorumlusunun, ilgili kişiler tarafından Kanun kapsamında yapılan başvurulara yasal süresi içerisinde cevap vermesi noktasında azami dikkat ve özeni göstermesi gerektiği hususunda talimatlandırılmasına

karar verilmiştir.

2020/429 sayılı KVKK Kararı

İlgili kişinin kişisel verilerinin, hakkında icra takibi yapan avukat tarafından hukuka aykırı olarak işlenmesi ve açıklanmasına ilişkin şikayet ile ilgili Kişisel Verileri Koruma Kurulunun 28/05/2020 Tarihli ve 2020/429 Sayılı Karar Özeti

Karar Tarihi : 28.05.2020

Karar No : 2020/429

Konu Özeti : İlgili kişinin kişisel verilerinin, hakkında icra takibi yapan avukat tarafından hukuka aykırı olarak işlenmesi ve açıklanması ile ilgili şikayet

İlgili kişiden alınan şikayet dilekçesinde özetle;

- Kamu görevlisi olarak görev yaptığı ilde kamuya ait bir sosyal tesiste konakladığı; banka borcundan dolayı, hakkında bankanın vekili olan avukat tarafından icra takibi başlatıldığı; 27.11.2018 tarihinde kendisiyle birlikte aynı sosyal tesiste ikamet etmekte olan sayısını tam olarak bilmediği iş arkadaşlarının kendi üzerlerine kayıtlı cep telefonlarına ve ilgili kişinin ağabeyi üzerine kayıtlı cep telefonuna ilgili kişinin adını ve haciz talimatını içeren kısa mesajlar gönderildiği; konuya ilişkin olarak ayrıca Cumhuriyet Başsavcılığına başvurduğu belirtilerek avukat hakkında gereğinin yapılması talep edilmiştir.

Konuya ilişkin olarak 01.10.2019 tarih ve 2019/293 sayılı Kurul Kararı ile başlatılan inceleme çerçevesinde avukattan savunma sunması talep edilmiş, veri sorumlusu avukat savunmasında,

- İkrar veya kabul anlamına gelmemek kaydı ile; şikayetçinin kişisel e-posta hesabı yerine içerisinde ofise günlük gelen yüzlerce e-postanın bulunduğu e-posta adresine gönderdiğini iddia ettiği başvurunun okunma ihtimalinin olmadığı, konudan Kurumumuzun savunma talepli yazısının tebellüğ edildiği tarihte haberdar olunduğu, bu nedenle 30 günlük yasal sürenin dolmasına karşın cevap alınamadığı iddiasının doğru olmadığı,

- İlgili kişinin müvekkil Banka ile imzaladığı bireysel bankacılık hizmetleri sözleşmesine istinaden kredi kullandığı, kredi sözleşmesi kurulurken kimlik, adres, telefon ve maaş bilgilerini rızası ile paylaştığı,

- Kullandığı kredinin taksitlerini vadenin dolmasına ve akabindeki ihtara rağmen yerine getirmekten kaçındığı için hakkında takip kararı alındığı; çıkarılan ödeme emrinin adresinde bulunamadığı için Adres Kayıt Sistemindeki adres Mahalle Muhtarlığına; Tebligat Yasasının 21 inci maddesi gereğince tebliğ edildiği, süresinde itiraz olunmadığından takibin kesinleştiği, dosyanın derdest olduğu,
- Takibin üzerinden 5 yılı/60 ayı aşkın süre geçmesine ve aleyhindeki yasal takibe rağmen şikayetçinin aldığı krediyi ödemekten kaçınması ve bundan rahatsızlık duymaması; ancak gönderilen borç hatırlatma mesajından rahatsızlık duymasındaki samimiyetin düşündürücü olduğu; ayrıca söz konusu SMS'lerin, ilgili kişinin kendisini telefonda arayarak bizzat bilgi istemesi üzerine rızası ile gönderildiği,
- 5 yıllık süreçte farklı telefon numaraları üzerinden kendileriyle iletişime geçen ve aradığı değişik hatlar nedeni ile sistemde adına birden fazla bağlantı numarası olan şikayetçinin güncel bilgi talebi sonrasında sistemde kayıtlı numaralarına 27.11.2018 günü SMS gönderilmesini şikayet etmesinin hakkın kötüye kullanılması olduğu, - T.C. kimlik numarasına göre abonelik sorgulaması yapıldığında; beyanın doğruluğunun anlaşılacağı ve şikayetçi adına hayatın olağan akışına aykırı sayıda GSM hattı olduğunun ortaya çıkarılabileceği,
- Şikayetçinin dilekçesine yazmakla birlikte alenileştirdiği T.C. kimlik numarasına göre telefon operatörlerinin borç sorgulama sayfasına girildiğinde; adına toplam 16 adet hat olduğunun görüldüğü, hatırlatma mesajının gönderildiği hat ve Cumhuriyet Savcılığında ifade verirken bildirdiği hat dikkate alındığında adına kayıtlı 18 hat bulunduğu,
- 07.04.2016 tarihli Resmi Gazetede yayımlanmasına ve avukat olmasına karşın ancak hakkında yapılan şikayet üzerine inceleme fırsatı bulduğu 6698 sayılı Kişisel Verilerin Korunması Kanunundan kamuoyunun henüz haberdar olmadığı; toplumda "kişisel veri" ve bunun korunmasına ilişkin bilincin oluşması için ilgililer tarafından yapılması gerekli çalışmaların yeterli olmadığı,
- Kamuoyunun, 6698 sayılı Kanunu son yıllarda kanun koyucu tarafından ihdas olunan ve uygulaması artık yerleşen 6502 sayılı Tüketicinin Korunması Hakkında Kanun, 4054 sayılı Rekabetin Korunması Hakkındaki Kanun, 6112 sayılı Radyo ve Televizyonların Kuruluşu Hakkındaki Kanun, 5411 sayılı Bankacılık Kanunu, 6325 sayılı Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu, Enerji Piyasası Düzenleme Kanunu ve benzeri kanunlar kadar içselleştirmiş olmadığı,
- Müeyyideleri oldukça ağır bu Kanuna ilişkin bilgilendirme ve uygulamaların zaman içerisinde Kurum Başkanı ve mensupları tarafından kamuoyuna aktarılacağı muhakkak olsa da; bu sürecin henüz tamamlanmadığının bir vakıa olduğu,

- “Kanunu bilmemek mazeret sayılmaz” ilkesi genel bir kural olsa da; hukuk sistemimize tamamen yabancı ve uygulama için geçiş süresi tanınan bu Kanun ve onun uygulayıcısı Kurumun konulara daha toleransla yaklaşması gerektiği, Kuruma ait web sayfasında yayımlanan kararların sayısı ve içeriğinin bu iddiayı doğrulayacak istikamette olduğu,

- Nitekim; Kurulun “Veri Sorumluları Siciline Kayıt Yükümlülüğü”ne ilişkin 27.12.2019 tarih ve 2019/387 sayılı süre uzatım kararından; kendi hukuk büroları statüsünde olanların; sicile kayıt zorunluluk süresinin 30.09.2020 tarihine ötelendiği,

Konunun Kurumun görev/inceleme alanından çıktığı, şöyle ki,

- 6698 sayılı Kişisel Verilerin Korunması Kanununun (3071 sayılı yasaya atıfta bulunan) 15 inci maddesinin (2) numaralı fıkrasındaki “Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesinde belirtilen şartları taşımayan ihbar ve şikayetler incelemeye alınamaz” şeklindeki düzenlemenin belirttiği üzere 01.11.1984 gün 3071 sayılı yasanın madde 6(b) fıkrası gereğince; yargı mercilerinin görevine giren konularla ilgili dilekçelerin istisna kabul edilerek yasanın kapsamı dışına bırakıldığı,

- Şikayet dilekçesinin kapsamından da anlaşılacağı üzere; şikayetçinin aynı konuda aynı gerekçelerle 29.11.2018 tarihinde Cumhuriyet Başsavcılığına başvurarak şikayetçi olması sonucu; Adalet Bakanlığından alınan soruşturma izni ile “özel hayatın gizliliğini ihlal etmek, kişilerin huzur ve sükununu bozmak” suçlarından hakkında 2019/3709 sayılı evrak üzerinden yürütülen soruşturmanın devam ettiği, vaki şikayet üzerine konunun yargıya intikal etmiş olduğu ve soruşturmanın devam ettiği dikkate alındığında konunun kurumun görev/kapsama alanından çıktığı,

- Nitekim bu hususun Kurulun 24.12.2018 gün ve 2018/156 sayılı kararında, “... şikayete konu iddiaların Türk Ceza Kanunu hükümleri uyarınca suç unsuru barındırdığı ve bunların da bireysel suç niteliğinde olduğu, bu kapsamda ilgili kişi tarafından da konunun yargıya intikal ettirilmiş olduğu dikkate alındığında, söz konusu başvurunun Kanun kapsamında değerlendirilemeyeceğine” denilmek suretiyle açıkça ifade edildiği,

- Bu yüzden dosyanın; konu hakkında karar verilmesine yasal olanak bulunmadığı gerekçesi ile kapatılmasının gerektiği,

USULE İLİŞKİN OLARAK

Başvuru yolunun henüz tüketilmediği,

- info@... adresine gönderildiği iddia edilen e-postadan 02.01.2019 tarihinde değil ancak Kurumun savunma talep ettiği yazının tebliğ günü olan 16.12.2019 tarihinde haberdar olunduğundan; 6698 sayılı Kişisel Verilerin Korunması Kanununun 14/2 maddesindeki "... 13. madde uyarınca başvuru yolu tüketilmeden şikayet yoluna başvurulamaz..." hükmü karşısında; bu konu ile ilgili şikayetin cevap verilmediği takdirde 17.01.2020 tarihinden itibaren yapılabileceği ve ilgiliye de 13.01.2020 tarihinde yasal süre içerisinde yanıt verildiği gözetilerek; henüz başvuru yolu tüketilmediği için yersiz şikayetin reddine karar verilmesi gerektiği,

Şikayetin süresinde yapılmadığı,

- Şikayetçinin 02.01.2019 tarihinde gönderildiğini iddia ettiği e-postanın gönderilme günü ile Kuruma şikayet dilekçesi verdiği 06.02.2019 tarihi arasında 1 ay 4 gün yani 34 günlük sürenin geçtiği; 6698 sayılı Kişisel Verilerin Korunması Kanununun 14/1 maddesindeki "... Başvuruya cevap verilmemesi hallerinde; ilgili kişi veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz gün içinde Kurula şikayette bulunabilir" şeklinde düzenleme dikkate alındığında; 30 günlük yasal süre içinde başvuruda bulunmadığı anlaşılan şikayetçinin usulsüz başvurusunun reddine kadar verilmesi gerektiği,

Şikayetin reddedilmiş sayılması gerektiği,

- Kurumun; uymak zorunda olduğu varoluş yasasının 15 inci maddesinin (4) numaralı fıkrasındaki "... şikayet üzerine kurul talebi inceleyerek ilgililere bir cevap verir. Şikayet tarihinden itibaren 60 gün içerisinde cevap verilmezse talep reddedilmiş sayılır..." şeklindeki düzenleme göz önüne alındığında; Şikayet dilekçesinin Kuruma verildiği 06.02.2019 tarihi ile Kurumun inceleme kararı verdiği 01.10.2019 tarihi arasında 7 ay 25 gün geçtiği ve yasal 60 günlük süre içerisinde şikayetçiye cevap verilmediği anlaşıldığından; talebin reddedilmiş sayılması gerektiği,

ESASA İLİŞKİN OLARAK,

- Verinin işlenmesinin açık rızaya dayandığı,
- Şikayetçi ile Banka arasında sözleşme düzenlenirken şikayetçinin rızasıyla kimlik, adres, telefon ve maaş bilgilerini paylaşmış olduğu ve bunların banka kayıtlarına işlendiği,
- Kredi sözleşmesinde öngörülen vadenin dolmasına ve akabinde çekilen ihtara rağmen geri ödemesi gerçekleştirilmeyen gecikmiş borcun tahsili açısından alacaklı bankanın adına vekalet vermesinin ardından icra takibi aşamasına geçildiği,

- Kesinleşen icra takibinin ardından tahsilat aşamaları ilerletilirken; geri ödeme yapmayan borçlunun durumunun sorgulandığı ve müvekkil Bankaya olan ve ödenmeyen borç dışında başka dosyaların da olduğu, şikayetçi hakkında çok sayıda icra takibi bulunduğu tespit edildiği,
- İcra İflas Kanununun temel ilkelerinden birisinin, “Alacağın tahsili için yapılacak işlemlerde borçlunun, borcunu arttıracak giderlerden kaçınılması” ilkesi olduğu; diğer yandan avukatın müvekkilin çıkarlarını gözetmek zorunda olduğu, bu açıdan bakıldığında mezkur dosyada olduğu gibi “bırakınız krediden kaynaklanan alacağınızı tahsil etme üstüne bir de durmadan icraya gider yatırarak sürekli masraf yapılmasını olabildiğince engellemek” sorumluluğu altında olduğu,
- Bu sorumluluğun yasal dayanağını oluşturan Avukatlık Kanununun 35/A maddesinde; “Avukatlar dava açılmadan veya dava açılmış olup da henüz duruşma başlamadan önce kendilerine intikal eden iş ve davalarda, tarafların kendi iradeleriyle istem sonucu elde edebilecekleri konularla inhisar etmek kaydıyla, müvekkilleriyle birlikte karşı tarafı uzlaşmaya davet edebilirler.” hükmünün düzenlendiği,
- Metinden de anlaşılacağı üzere; avukatın, müvekkilinin haklarını himaye etmek amacı ile müvekkilinin de rızasını alarak karşı taraf ile iletişime geçebileceği, müvekkil bankanın tarafına sağlıklı iletişim kurma izni ile şikayetçinin borcunu icra takip masrafları ile arttırmaktan ziyade; kendisini Avukatlık Kanununun 35/A maddesi uyarınca uzlaşmaya yani belirli indirimler yaparak borcunu ödemede kolaylık sağlamaya davet etmesinin hukuka uygun olduğu,
- Kaldı ki; uzlaşma sağlanmasının alacaklı olan müvekkil bankadan ziyade borçlu şikayetçinin lehine olduğu; zira; borçlu adına kayıtlı tapu ve araçlara haciz şerhi eklenip satış talep edilerek, üzerine kayıtlı tüm mal varlığını satma imkanı kanun nezdinde tarafına verilmişken; bu yola tevessül edilmeyecek kişileri borçları yüzünden daha fazla mağduriyet yaşatmamak adına, hiçbir malın satışı talep edilmeyip iletişim yolu ile borca taksitlendirmeler yaparak tahsilat sağlanmaya çalışıldığı,
- Takibin her aşamasında borçlu ile iletişime geçme hak ve imkanının mevcut olduğu; belli bir süre sonra -ki bu dosyada takibin açılmasından 3 yıl yani 36 ay sonra- şikayetçi borçluyu öncelikli olarak telefonla arama ve yanıt verilmediğinden mesaj gönderme sureti ile ilgisini haberdar etme yönteminin tercih edildiği ve böylelikle İcra İflas Kanunundaki borçlu üzerindeki külfetin gereksiz yere artırılmasını engelleyen amir hükme uygun davranıldığı,
- Bu meyanda; genel olarak 5411 sayılı Bankacılık Kanunu ve 6098 sayılı Türk Borçlar Kanununun hükümleri çerçevesinde; alacaklı banka ve hukuk bürosu arasında akdedilen vekâlet ilişkisi gereğince alacakların tahsili çalışmalarına devam edildiği; ayrıca Avukatlık Kanununun 35/A maddesindeki yasal yükümlülük dikkate alınarak borçlulara ödemede sağlanacak kolaylıkların ve borcun

ödenmemesi halinde karşı karşıya kalınabilecek hukuki risklerin bildirilmesi açısından SMS gönderilmesi yönteminin uygun olacağı düşünülüyor,

- Devlet memuru olan şikayetçinin; maaş ve diğer sosyal haklarına ve aracına, iş yerine icra dairesi aracılığıyla sürekli haciz talebi gönderilmesinin mi, yoksa uzun aralıklarla telefonundan aranması veya SMS gönderilmesinin mi çıkarına olacağı, hangi durumda kişinin itibar güvenilirliğinin sarsılacağı Kurulun takdirinde olduğu,

- Derdest olan dosyada; İcra Müdürlüğü'nün borçlunun verilerini işlemiş olması dikkate alınarak; üstelik arandığında görüşmeyi kabul ederek onaylaması ve bilgi talep etmesi üzerine ödemede sağlanacak kolaylıklar ve ödenmemesi halinde karşılaşılabileceği hukuki risklerin SMS ile şikayetçi borçluya bildirildiği,

- Şikayetçi borçlunun; banka ile bireysel kredi sözleşmesi imzalanırken veri işlemeye gösterdiği rızanın açık olduğu ve bu anlamda hukuka uygun olduğu,

- Ayrıca Kanunun geçiş hükümlerini düzenleyen; Geçici 1 inci maddesinin (3) numaralı fıkrasında yer verilen "Ancak bu kanunun yayımı tarihinden önce hukuka uygun olarak alınmış rızalar, bir yıl içinde aksine bir irade beyanında bulunulmaması halinde, bu kanuna uygun kabul edilir" şeklindeki hüküm dikkate alındığında bu süre içerisinde aksine beyanda bulunduğunu kanıtlayamayan şikayetçinin rızasının devam ettiğinin kabul edilmesi gerektiği,

- Bu bağlamda şikayet hakkının bulunmadığı ve yersiz şikayetin reddine karar verilmesi gerektiği,

- Kanunun 5 inci maddesinin 2 numaralı fıkrasının (e) bendi dikkate alındığında; işlenen veri açısından şikayetçi borçlunun açık rızasına da gerek bulunmadığı,

- Şikayetçi borçlunun, bu verinin işlenmesine dair Banka ile imzalanan sözleşme sırasında verdiği ve tanınan bir yıllık geçiş süreci içinde de geri almadığı rızasına istinaden, geciktirilen geri ödeme nedeni ile alacağını tahsil etmek isteyen bankanın cebri icrada bulunabilmesi yani sözleşmeden doğan alacak hakkını kullanabilmesi için icra dosyasında borçlunun verilerinin işlenmesinin zorunlu olduğu,

- Nitekim bu hususun Kurulun 31.05.2019 tarih ve 2019/159 sayılı kararında, "... Şikayetçinin ilgili bankalardan kullanmış olduğu kredi borçlarının yeni alacaklısı olması, bu kapsamda 6098 sayılı kanunun 186. maddesi çerçevesinde borçlunun önceki alacaklılara karşı borcunu ifa etmesinin engellenmesi ve taraflarınca şikayetçiye sağlanacak kolaylıklar ile borcun ödenmemesi durumunda şikayetçinin maruz kalabileceği hukuki risklerin bildirilmesi amacıyla işlenmiş olmasının 6698 sayılı Kanunun 5 inci maddesinin (2) numaralı fıkrasının (e) bendi kapsamında şikayetçinin açık rızası

olmaksızın gerçekleşebilir olması nedeniyle veri sorumlusu hakkında yapılacak bir işlem bulunmadığına...” denilmek suretiyle açıkça ifade edildiği,

- Rıza var kabul edildiğinden şikayetin reddine karar verilmesi gerektiği,
- Verilmiş rızaya dayanarak işlenen verinin; 6698 sayılı Kişisel Verilerin Korunması Kanununun çizdiği çerçeve içinde kalınarak kullanılması halinde; hukuka aykırılıktan söz etmenin mümkün olmadığı,
- Müvekkil bankanın bireysel kredi sözleşmesinden doğan meşru alacağını tahsil edebilmek amacıyla icra müdürlüğü tarafından işlenmiş veri kullanılarak, şikayetçi-borçluya üstelik kendi talebi ile SMS gönderilmesinin hukuka uygun olduğu,
- Hiçbir şekilde ikrar anlamına gelmemek kaydıyla, 27.11.2018 tarihinde borçluya ait olduğu düşünülen hatlara, tek seferde yalnızca bir SMS gönderildiği,
- Bu durumun, işlenmiş verinin, yasal ve somut bir alacağı tahsil edebilme amacı ile ölçülü ve sınırlı bir şekilde kullanıldığını yani Kanunda aranan dürüstlük kurallarına uyulduğunu ispatladığı,
- Sonuç olarak gönderilen SMS’lerin, meşru temelli, makul sayıda ve ölçülü içerikte olup dürüstlük kuralları gözetilerek iletildikleri anlaşılacağından yersiz şikayetin reddine karar verilmesi gerektiği,
- Şikayetçinin aradan geçen 5 yıllık sürede farklı GSM hatlarından büroyu birden fazla kez aradığı ve kendisi ile çok sayıda görüşme gerçekleştirildiği,
- Ofis çalışanları tarafından, işin doğasına uygun olarak gelen aramaların ilgili kişinin bilgisine işlenmekte olduğu ve gerekli zamanlarda bu numaradan ulaşıldığı,
- Şikayet dilekçesinde, ekran çıktıları sunulan hatların bu tipten olabileceği gibi, sıkça rastlanan şekilde borçluların; hukuk bürosunu arkadaşlarına ait hatlardan aramaları veyahut nadiren de olsa ekonomik durumları hakkında kendilerine referans olacak arkadaşlarının numaralarını bildirmeleri yüzünden kayıtlarına girebildiği,
- Bireysel kredi sözleşmesinde şikayetçi borçlu dışında buna kefalet veren biri olmadığından, yani meslektaşlarından veya ağabeyinden borcu hukuken tahsil etme şansı bulunmadığından; adı geçenlere SMS göndermekte (yapılan masrafın dışında) bir çıkarları olmadığı, bu açıdan bakıldığında adı geçenlere kasıtlı olarak SMS gönderildiğini iddia etmenin abesle iştiğal olduğu, yegane amaçlarının borçluya ulaşmak ve onu bilgilendirmek olduğu; mesaj atılan iş arkadaşlarının ve ağabeyinin kullandığı cep telefonlarını araştırarak bulma ve SMS gönderme gibi özel bir kasıtlı hareket edilmediği,

- Yukarıda da açıklandığı üzere, T.C. kimlik numarasına göre abonelik araştırıldığında, hayatın olağan akışına aykırı sayıda GSM hattının adına kayıtlı olduğundan şüphe duyulan şikayetçinin, ofis arkadaşlarına ait hatlardan araması veyahut ekonomik durumu hakkında referans olmaları için meslektaşlarının numaralarını bildirmiş olmasının kuvvetle muhtemel olduğu,
- Ayrıca GSM hattının adına kayıtlı kişi dışında, aile fertlerinden bir başkası tarafından kullanılmasına Türkiye’de sıkça rastlandığının gözden kaçırılmaması gerektiği,
- Ofislerinde, ...Takip Sistemi ve 118 80 bilinmeyen numaralar ile internet üzerinden herkesin kolaylıkla ulaşabildiği kimlik, adres ve telefon bilgileri sorgulayan.... dışında program kullanılmadığı, bu hususta yerinde inceleme yapılmasının da mümkün olduğu,
- Kurumumuzun yazısı ekinde gönderilen “Veri Sorumlusu Tanıtım Formu”nun 30.09.2020 tarihine kadar yasal süresi içerisinde doldurularak “Veri Sorumluları Siciline Kayıt Yükümlülüğü”nün yerine getirileceği

belirtilerek, konunun yargıya intikal etmiş olması, usule ilişkin itirazları, Kurul aksi kanaatte ise esasa ilişkin açıklamaları dikkate alınarak yersiz olarak nitelendirdiği şikayetin reddedilmesi talep edilmiştir. Avukatın savunmasında ayrıca, şikayetçinin T.C. kimlik numarasına göre adına kayıtlı cep telefonu aboneliklerinin olanak varsa sorgulanması yoksa iletişim şirketlerine yazı yazılması; bu minvalde 01.11.2018 - 31.12.2018 tarihleri arasında adına kayıtlı hattı arayanlar listesinin de GSM şirketinden getirilmesi ve yapılacak incelemede değerlendirilmesi Kurumumuzdan talep edilmiştir.

Öte yandan, inceleme süreci devam ederken ilgili kişiden alınan ek beyanda, Kurumumuzun savunma istemesinden sonra şikayet ettiği veri sorumlusu avukat tarafından kendisine iletilen cevapta şahsına ait bir çok numaranın olduğu ve kişisel verilerini içeren mesajların atıldığı numaraların kendisine ait olduğunu düşündüğü ve bu amaçla bilgilendirme amaçlı mesaj attıklarını iddia ettiği, şahsına ait tüm hat dökümlerini abonelik başlangıç ve bitiş tarihleri ile tarafımıza sunduğu, kişisel verilerinin paylaşıldığı tarihte şahsına ait tek bir hattın olduğunun görüleceği; kişisel verilerinin banka ile yapmış olduğu sözleşme kapsamında alenileştirilmiş olduğu açıklamasının doğru olmadığı; mesaj atılan numaraların şahsına ait olduğunu düşündüğünü belirtmiş olmasına rağmen yazısı ekinde sunulan ekran görüntülerinden anlaşılacağı üzere ve Savcılıkta ifade veren iş arkadaşlarına gönderilen mesajlarda o dönem beraber görev yaptığı bir başka iş arkadaşının borç bilgilerinin de paylaşılmış olduğunun görülebileceği, hukuk bürosu çalışanları, söz konusu mesaj atılan numaraların şahsına ait olduğunu düşünüyor ise diğer kişinin borç bilgilerini neden aynı numaralara mesaj gönderdiklerinin sorgulanması gerektiği belirtilmiştir.

Bahse konu şikayet başvurusu ve ek beyanlar, ilgili kişinin iddiaları, veri sorumlusundan alınan bilgi ve belgeler ve ilgili mevzuat hükümleri çerçevesinde değerlendirilmesi neticesinde Kişisel Verileri Koruma Kurulunca alınan 28.05.2020 tarih ve 2020/429 sayılı Kararda aşağıdaki değerlendirmelere yer verilmiştir.

Şikayete konu olayda, bankaya borcu olan ve bu borca ilişkin işlemlerin yürütülmesini teminen kişisel verileri banka tarafından avukata aktarılan ve avukat tarafından kişisel verileri işlenen şikayetçinin “**ilgili kişi**”, Banka adına icra işlemlerini yürüten ve bu işlemle ilgili olmak üzere ilgili kişinin kişisel verilerini işlemesi gereken avukatın “**veri sorumlusu**”, ilgili kişinin bankaya olan borcunu tahsil edebilmek için avukat tarafından ilgili kişinin iletişim bilgileri ve diğer ilgili bilgilerinin işlenmesi eyleminin ise “**veri işleme faaliyeti**” olduğu değerlendirilmektedir. Diğer yandan Kanunda, kişisel veriler sınırlı sayma yöntemi ile belirlenmemiş, bir verinin kişisel veri olması için belirli ya da belirlenebilir gerçek kişiye ilişkin olma kriteri getirilmiştir. Bu bağlamda, ilgili kişinin ağabeyine ve iş arkadaşlarına gönderilen mesajın içeriği incelendiğinde, ilgili kişinin açık adını, borçlu olduğu bankayı ve icra dosyası borcuna ilişkin bilgileri ihtiva eden kısa mesajın, ilgili kişiye ait kişisel veri niteliğindeki bilgileri içerdiği anlaşılmaktadır.

Usule İlişkin Değerlendirme

Veri sorumlusunun iddiası, ilgili kişinin 02.01.2019 tarihli e-postasından haberdar olunmadığı, şikayetin varlığından Kurumumuzun bilgi belge talebi yazısı ile haberdar olunduğu, bu durumda ilgili kişiye cevap verme süresinin Kurumumuz yazısının tebellüğ tarihinden itibaren başladığı yönündedir. Ancak, Kanunun 13 üncü maddesinin (2) numaralı fıkrası, “Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır” hükmünü amir olup, bu hükümde belirtilen 30 günlük sürenin Kurum yazısının tebellüğ tarihinden başlaması mümkün değildir.

Usule ilişkin bir diğer iddia, e-posta tarihinin 02.01.2019, Kurula şikayet tarihinin 06.02.2019 olduğu, bu durumun ise Kanunun 14 üncü maddesinin (1) numaralı fıkrası hükmüne uygun olmadığı yönündedir. Bilindiği üzere, Kanunun “Kurula şikâyet” başlıklı 14 üncü maddesi, “Başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyette bulunabilir.” hükmünü amirdir. Şikayete konu olayda başvuruya cevap verilmediği için başvurudan itibaren 60 günlük süre kuralı geçerli olacaktır ki, ilgili kişinin Kurumumuza başvurusu, veri sorumlusuna başvuru tarihinden

sonra 34 üncü günde yapılmış olup, Kanunda belirlenen 60 günlük yasal süre içerisinde yapılmış bir başvurudur.

Son olarak, veri sorumlusu şikayetin üzerinden uzun zaman geçmiş olduğunu belirtmekte ve Kanunun 15 inci maddesinde yer alan “..... şikayet üzerine Kurul talebi inceleyerek ilgililere bir cevap verir. Şikayet tarihinden itibaren 60 gün içerisinde cevap verilmezse talep reddedilmiş sayılır....” hükmüne dayanarak şikayetin reddedilmiş sayılmasını talep etmektedir. Ancak, Kurumumuzun 03.04.2019 tarih ve 4485 sayılı yazısı ile, konuya ilişkin incelemenin sürdüğü ve sonuçlanmasını müteakip tarafına bilgi verileceği hususu ilgili kişiye tebliğ edilmiş olup, bu bilgilendirmenin yapılması hususunda Kanunun ilgili maddesinde belirtilen süre gözetilmiştir. Ayrıca, dosyaya ilişkin alınan 2019/293 sayılı ilk Kurul Kararı da ilgili kişiye tebliğ edilmiş olup, dosyanın safahat bilgileri ilgili ile paylaşılmıştır.

Bu değerlendirmeler ışığında, veri sorumlusunun usule ilişkin itirazlarının reddedilmesi kanaatine varılmıştır.

Esasa İlişkin Değerlendirme

Kanunun 5 inci maddesi, kişisel verilerin işleme şartlarını düzenlemekte olup, maddenin (1) numaralı fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği hüküm altına alınmış, (2) numaralı fıkrada ise, kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda olan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün korunması için veri işlemenin zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaati için veri işlenmesinin zorunlu olması hallerinde ilgili kişinin açık rızası olmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükme bağlanmıştır.

Somut olayda, veri sorumlusu bir avukat olup, vekili olduğu Banka adına, Bankanın haklarını ve menfaatlerini korumak amacıyla hareket ettiği, bu anlamda Avukatlık Kanunundan kaynaklanan yükümlülükleri ve yürütmekte olduğu icra işlemleri bakımından İcra İflas Kanunu ve ikincil mevzuat düzenlemelerinden kaynaklanan hukuki yükümlülüklerini yerine getirmek amacıyla borçluya ait bilgileri, kanuna uygun olarak işleme ve ilgili birim/mercilere bildirme yetkisi olduğu ve bu

bağlamda işlediği kişisel verileri Kanunun 5 inci maddesinin (2) numaralı fıkrası çerçevesinde ilgili kişinin açık rızası olmaksızın işlenmesinin kanuna uygun olduğu değerlendirilmektedir.

Ancak Kanun hükümleri gereğince açık rıza aranmaksızın işlenecek kişisel verilerin borçluya ait olması gerekmektedir. **Bu kapsamda ne banka ile ne de avukat ile bağı olan ve bahse konu icra işlemine konu kişisel verisi bulunmayan ilgili kişinin ağabeyi ve iş arkadaşlarının telefon numaralarının işlenmesi ve akabinde şikayetçi ilgili kişiye ait kişisel verilerin bu üçüncü kişilere ifşası Kanunun 5 inci maddesinin (2) numaralı fıkrası hükümleri kapsamında gerçekleştirilebilecek bir kişisel veri işleme faaliyeti değildir.** Somut olayda Avukat tarafından ilgili kişiye ait borç bilgilerinin ağabeyi ve iş arkadaşlarına kısa mesaj olarak gönderilmesi eylemi bakımından, ilgili kişinin ağabeyinin ve iş arkadaşlarının telefon numarasının hangi surette elde edildiği ve bu telefon numaralarının işlenmesinde Avukatın hangi hukuki gerekçeye dayandığının da değerlendirilmesi gerekmektedir. Avukat tarafından yapılan savunmada, şikayetçinin süreç içerisinde farklı GSM hatlarından büroyu birden fazla kez aradığı ve kendisi ile çok sayıda görüşme gerçekleştirildiği, ofis çalışanları tarafından, işin doğasına uygun olarak gelen aramaların ilgili kişinin bilgisine işlenmekte olduğu ve gerekli zamanlarda bu numaradan ulaşıldığı, şikayet dilekçesinde, ekran çıktıları sunulan hatların bu tipten olabileceği gibi, sıkça rastlanan şekilde borçluların; hukuk bürosunu arkadaşlarına ait hatlardan aramaları veyahut nadiren de olsa ekonomik durumları hakkında kendilerine referans olacak arkadaşlarının numaralarını bildirmeleri yüzünden kayıtlarına girebildiği şeklindeki açıklamasının, söz konusu üçüncü kişilerin telefon numaralarının avukat tarafından işlenmesi bakımından Kanunun 5 inci maddesi kapsamında bir dayanak teşkil etmeyeceğinden, ilgili kişinin ağabeyi ve iş arkadaşlarının telefon numarasının avukat tarafından işlenmesi suretiyle kısa mesaj gönderilmesinin hukuka uygun olmadığı kanaatine varılmaktadır.

Ayrıca, veri sorumlusunun savunmasında, borçluya ait olduğu düşünülen telefon hatlarına aynı gün, yani 27.11.2018 tarihinde tek seferde yalnızca bir SMS gönderildiği belirtilmektedir. İlgili kişinin iş arkadaşlarının Cumhuriyet Başsavcılığında verdikleri ifadelerde kendilerine 27.11.2018 tarihinde SMS gönderildiği belirtilmekle birlikte, ilgili kişinin ağabeyi tarafından verilen ifadenin ekinde yer alan ekran görüntüsü çıktılarında söz konusu SMS'lerin bu kişiye muhtelif tarihlerde pek çok kez gönderildiği anlaşılmaktadır. Diğer yandan, ilgili kişinin iş arkadaşlarının telefon ekran görüntüsünde, ilgili kişi dışında bir başka şahsın borç bilgilerinin de avukata/hukuk bürosuna ait olduğu anlaşılan numaradan bu kişiler ile paylaşıldığı görülmektedir.

Kanunun 12 nci maddesinde yer alan hüküm gereğince veri sorumlusu; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel

verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır. Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar.

Veri sorumlusu avukat tarafından, ilgili kişinin ağabeyi ve iş arkadaşlarının telefon numaralarının varsayımlara dayanan ve tam olarak ispatlanamayan bir şekilde elde edilmesi, akabinde şikayetçi ilgili kişiye ait borç bilgilerinin yani kişisel verilerin bu numaralarla paylaşılması Kanun hükümlerine aykırılık teşkil etmekte olup, bu suretle veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini önleme, kişisel verilere hukuka aykırı olarak erişilmesini önleme ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri alma yükümlülüğünü yerine getirmediği kanaatine varılmaktadır.

Öte yandan, veri sorumlusu avukatın savunmasında, ilgili kişinin hayatın olağan akışına aykırı şekilde fazla sayıda telefon hattı aboneliğine sahip olduğu belirtilerek, bu durumun, ilgili kişinin dilekçesine yazmak suretiyle alenileştirdiği T.C. kimlik numarası kullanılarak GSM operatörlerinin borç sorgulama sayfalarından tespit edildiği belirtilmiş ve bu sorgulamalara ilişkin internet sayfası çıktıları da savunmaya eklenmiştir. Öncelikle, veri sorumlusu avukatın görevi gereği edindiği veya ilgili kişinin veri sorumlusu avukata başvurmak amacıyla kendisine bildirmiş olduğu kişisel verilerin alenileştirilmiş veri olduğunu söylemek mümkün değildir. Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberinde de belirtildiği üzere, alenileştirmeden söz edilebilmesi için ilgili kişinin alenileştirme iradesinin bulunması ve ayrıca verinin alenileştirme amacı dışında kullanılmaması gerekmektedir. Ancak, avukatın başka bir vesile ile işlediği kişisel verileri kullanarak ilgili kişinin GSM aboneliklerini ve borçlarını sorgulaması bu bağlamda değerlendirilemeyecektir. Diğer yandan, bilindiği üzere, Kanunun genel ilkeler başlıklı 4 üncü maddesinde, kişisel verilerin işlenmesinde uyulması gereken ilkeler düzenlenmiş olup, maddenin (2) numaralı fıkrasında kişisel verilerin işlenmesinde “(c) belirli, açık ve meşru amaçlar için işleme, (ç) işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkelerine uyulması gerektiği hükme bağlanmıştır. Veri sorumlusunun icra işlemlerinde kullanmak üzere edindiği veya ilgili kişi tarafından kendisine bildirilen T.C. kimlik numarasını kullanarak GSM hattı sorgulaması yapmak suretiyle ikinci bir hukuka aykırı veri işleme eylemine sebebiyet verdiği değerlendirilmektedir.

Kanuna uyum konusunda genel değerlendirme

Veri sorumlusu avukat tarafından Kurumumuza iletilen savunmada, 6698 sayılı Kanun ve uygulamalarına ilişkin yanlış tespit ve değerlendirmeler olduğu anlaşılmış olup, bu hususta genel bir değerlendirme yapılması gereği hasıl olmuştur.

Kanunun kamuoyu tarafından bilinmediği, içselleştirilmediği şeklindeki açıklamaya karşılık olarak, Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 tarihinde yürürlüğe girmiş; geçiş hükümleri Kanunun Geçici 1 inci maddesinde düzenlenmiştir. Geçici 1 inci maddenin (3) numaralı fıkrasında “Kanunun yayımı tarihinden önce işlenmiş kişisel verilerin Kanunun yayımı tarihinden itibaren iki yıl içinde Kanuna uygun hale getirileceği belirtilmek suretiyle uyum için gerekli süre de hüküm altına alınmıştır. Söz konusu iki yıllık geçiş süresinin 7 Nisan 2018 tarihi itibari ile dolduğu dikkate alındığında, içinde bulunduğumuz tarih itibariyle, mesleği gereği mevzuat konularına hakim olması gereken veri sorumlusu avukatın söz konusu açıklamasının kabul edilebilir olmadığı değerlendirilmektedir.

Öte yandan, Kurulca alınan karar sayısının az olduğu değerlendirmesine karşılık olarak, Kurul tarafından alınan her Kararın değil, sadece yayımlanmasına Kurulca karar verilen Kararların, Kanunun 12 nci maddesinin (5) numaralı fıkrası ile yine Kanunun 23 üncü maddesinin (5) numaralı fıkrası hükümlerine istinaden yayımlandığını belirtmekte fayda görülmektedir.

Öte yandan, veri sorumlusu avukat, Kurumun savunma talebi yazısı ekinde matbu olarak tüm veri sorumlularına iletilen Veri Sorumlusu Tanıtım Formunu doldurmamış, savunmasında yasal süre olan 30.09.2020 tarihi itibariyle formun doldurulacağı ve VERBİS'e kayıt yükümlülüğünün yerine getirileceğini belirtmiştir. Bilindiği üzere, Kanunun “Veri Sorumluları Sicili” başlıklı 16 nci maddesinin (2) numaralı fıkrasında Kurul tarafından Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebileceği düzenlenmiş olup, söz konusu hükmün verdiği yetki çerçevesinde Kurul tarafından alınan 02.04.2018 tarih ve 2018/32 sayılı Karar uyarınca “19/3/1969 tarihli ve 1136 sayılı Avukatlık Kanunu uyarınca faaliyet gösteren avukatlar” VERBİS'e kayıt yükümlülüğünden istisna tutulmuştur. Bu anlamda, veri sorumlusunun bir avukat olduğu dikkate alındığında, avukatlık mesleği dışında bir veri sorumluluğu bulunup bulunmadığı ve VERBİS'e kayıt yükümlülüğü olup olmadığı tarafınca ayrıca değerlendirilmelidir.

Öte yandan, veri sorumlusunun savunmasında, ofislerinde kullandıkları bazı yazılımlardan söz edilmekte olup, bu hususta Kurul tarafından alınan “Hukuka Aykırı Olarak Elde Edilen Veriler Üzerinden Vatandaşların Kimlik ve İletişim Bilgileri Gibi Kişisel Verilerinin Sorgulanmasına İmkân Tanıyan Yazılım/Program/Uygulamalara Yönelik” 18/10/2019 tarihli ve 2019/308 sayılı İlke Kararının veri sorumlusunca dikkate alınması gerektiği değerlendirilmektedir.

Bu minvalde, veri sorumlusu avukatın savunmasında 6698 sayılı Kanun ve uygulamalarına ilişkin yer alan yanlış tespit ve değerlendirmeler dikkate alındığında, Kanuna uyum konusunda azami dikkat ve özenin gösterilmesi hususunda veri sorumlusunun talimatlandırılmasının uygun olacağı sonucuna ulaşılmıştır.

Konunun yargıya intikal etmiş olmasına ilişkin değerlendirme

Gerek ilgili kişi tarafından sunulan belgeler gerek veri sorumlusu avukatın savunması ve sunduğu belgeler, konunun ilgili kişi tarafından yargıya intikal ettirilmiş olduğunu göstermektedir. 1136 sayılı Avukatlık Kanununun “Soruşturmaya yetkili Cumhuriyet Savcısı” başlıklı 58 inci maddesinde, “Avukatların avukatlık veya Türkiye Barolar Birliği ya da baroların organlarındaki görevlerinden doğan veya görev sırasında işledikleri suçlardan dolayı haklarında soruşturma, Adalet Bakanlığının vereceği izin üzerine, suçun işlendiği yer Cumhuriyet savcısı tarafından yapılır” hükmü düzenlenmiş olup, avukat hakkındaki işlemin bu hüküm çerçevesinde yürütüldüğü anlaşılmaktadır. Ancak, ilgili Cumhuriyet Başsavcılığı tarafından hazırlanan Adalet Bakanlığı Ceza İşleri Genel Müdürlüğünü muhatap fezlekenin “Netice ve Kanaat” bölümünde **avukatın “kişilerin huzur ve sükununu bozma, görevi kötüye kullanma ve özel hayatın gizliliğini ihlal suçlarını işlediği hususunda yeterli şüpheye ulaşıldığı” ifadesi yer almakta olup**, avukatın savunması ekinde de görüleceği üzere söz konusu suçlar arasında kişisel verilere ilişkin suçlar bakımından bir değerlendirmeye gidilmemiş olup, bu anlamda şikayete konu eylemde hukuka aykırı bir kişisel veri işleme faaliyeti olduğu değerlendirildiğinden konunun Kurulun görev ve yetki alanında olduğu sonucuna varılmaktadır. **Ayrıca, ilgili kişinin ağabeyinin ve kendisiyle aynı yerde ikamet eden iş arkadaşlarının iletişim bilgilerinin kaydedilmesi ve bu kişilere SMS gönderilmesi şeklinde gerçekleşen kişisel veri işleme faaliyeti bakımından konunun yargıya intikal etmediği ve bu hukuka aykırı kişisel veri işleme faaliyetinin de Kurulun yetki ve görev alanında bulunduğu dikkate alındığında söz konusu şikayete ilişkin yapılan inceleme neticesinde Kurul tarafından Kanunda yer alan müeyyidelerin uygulanmasının önünde bir engel olmadığı değerlendirilmektedir.**

Sonuç olarak,

Bankaya olan borcuna ilişkin bilgilerin, icra işlemlerini yürüten avukat tarafından kendisi gibi kamu sosyal tesisinde konaklamakta olan iş arkadaşlarına ve ağabeyine SMS aracılığıyla gönderilmesi üzerine, ilgili avukatlık bürosuna başvuran ancak bir cevap alamayan ilgili kişinin şikayetinin incelenmesi neticesinde;

1. Veri sorumlusunun usule ilişkin itirazlarının yersiz olması nedeniyle reddedilmesine,

2. Veri sorumlusu avukat tarafından, ilgili kişinin ağabeyi ve iş arkadaşlarının telefon numaralarının varsayımlara dayanan ve tam olarak ispatlanamayan bir şekilde elde edilmesi, akabinde şikayetçi ilgili kişiye ait borç bilgilerinin yani kişisel verilerin bu numaralarla paylaşılmasının; ayrıca ilgili kişinin T.C. kimlik numarası kullanılmak suretiyle GSM aboneliklerinin ve borçlarının sorgulanmasının Kanun hükümlerine aykırılık teşkil ettiği, bu suretle kişisel verilerin hukuka aykırı olarak işlenmesini önleme ve kişisel verilere hukuka aykırı olarak erişilmesini önleme yükümlülüğünü yerine getirmediği ve genel ilkelere aykırı hareket ettiği dikkate alındığında, veri sorumlusunca yürütülen veri işleme faaliyetinin Kanunun 12 nci maddesinin (1) numaralı fıkrasına aykırılık teşkil etmesi nedeniyle Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca hakkında 125.000 TL idari para cezası uygulanmasına,

3. Veri sorumlusu avukatın savunmasında 6698 sayılı Kanun ve uygulamalarına ilişkin yer alan yanlış tespit ve değerlendirmeler dikkate alındığında, Kanuna uyum konusunda azami dikkat ve özenin gösterilmesi hususunda talimatlandırılmasına

karar verilmiştir.

2020/421 sayılı KVKK Kararı

Kişisel bakım sektöründe faaliyet yürüten bir veri sorumlusunun veri ihlali bildirimini hakkında Kişisel Verileri Koruma Kurulunun 22/05/2020 tarih ve 2020/421 sayılı Karar Özeti

Karar Tarihi : 22.05.2020

Karar No : 2020/421

Konu Özeti : Kişisel bakım sektöründe faaliyet yürüten bir veri sorumlusunun veri ihlali bildirimini hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlali bildiriminde;

- 06.03.2020 tarihinde veri sorumlusu e-posta adresine kimliği belirsiz bir şahıstan veri sorumlusu web sitesi üyelerinin e-posta adresini/şifrelerini ele geçirdiğine dair bir mesaj geldiği,
- Yapılan incelemelerde, veri sorumlusu ile herhangi bir ilişkisi olmayan üçüncü kişilerin veri sorumlusunun kullanımındaki veri tabanlarından herhangi bir sızıntı olmaksızın dışı kaynaklardan elde ettikleri elektronik posta adresleri/şifreler ile veri sorumlusuna ait internet sitesine giriş yaptıkları,
- 04.03.2020 tarihinde bu olayın meydana geldiği, anılan kişi veya kişilerin ellerindeki e-posta şifre bilgilerini 14.000'den fazla IP'den bağlantı kurarak ve 500.000'in üzerinde e-posta/şifre kombinasyonunun sitede denedikleri,
- Her başarısız denemeden sonra bir başka e-posta/şifre denemesi yaptıkları ve bu yolla 2092 site kullanıcısının hesaplarının şifrelerini doğruladıklarının tespit edildiği,
- İhlalden etkilenen kişisel verilerin müşterilere ait ad, soyad, cep telefonu numarası, e-posta adresi, cinsiyet, doğum günü, teslimat/fatura adresleri ve sipariş geçmişi bilgileri olduğu ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 22/05/2020 tarih ve 2020/421 sayılı Kararı ile;

- İhlalin 04.03.2020 tarihinde meydana geldiği, anılan kişi veya kişilerin ellerindeki elektronik posta şifre bilgilerini 14.000'den fazla IP'den bağlantı kurarak sitede denedikleri ve her denemeden sonra başka bir e-posta/şifre denemesi yaptıkları,

- Veri sorumlusu tarafından yapılan inceleme neticesinde bu denemelerin sonucunda 2092 kullanıcının hesaplarına başarılı şekilde giriş yapıldığı,
- İhlalden veri sorumlusu müşterilerine ait ad-soyad, e-posta, cep telefonu, cinsiyet, doğum günü, teslimat/fatura adresleri ve sipariş geçmişi bilgilerinin etkilendiği,
- Veri sorumlusunun kendi olağan trafiğine ek bu trafiğin veri sorumlusunca fark edilmediği ve ihlali gerçekleştiren kimliği belirsiz kişilerce gönderilen e-posta sonucunda ihlalin tespit edilebildiği,
- İhlali gerçekleştiren kişi ya da kişiler tarafından veri sorumlusu dışı kaynaklardan elde edildiği belirtilen 500.000'in üzerinde e-posta/şifre kombinasyonuna ilişkin denemeler yapıldığı veri sorumlusu tarafından belirtilmiş olup, Kurumumuz tarafından yayınlanan Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde yer alan 3.2. Kişisel Veri Güvenliğinin Takibi maddesinde veri sorumlularının sistemlerinin çoğunlukla hem içeriden hem de dışarıdan gelen saldırılar ve siber suçlara veya kötü amaçlı yazılımlara maruz kalmakta olduğu, çeşitli belirtilere rağmen bu durumun uzun süre fark edilemediği ve müdahale için geç kalınabildiği ifade edilmekte olup; hesabına giriş yapılan 2092 kullanıcı dışında başarısız denemelerin sayısının fazlalığının veri sorumlusu tarafından fark edilememesinin bilişim ağlarının izlenmesi ve olmaması gereken durumların fark edilmesi hususunda eksiklik olduğu

hususları dikkate alındığında Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 210.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2020/414 sayılı KVKK Kararı

Hakkında hüküm verildiği suçtan dolayı cezası infaz edilen ilgili kişiye ait haberin yayımlandığı gazetenin internet sitesinden kaldırılması talebi hakkında Kişisel Verileri Koruma Kurulunun 22/05/2020 tarihli ve 2020/414 sayılı Karar Özeti

Karar Tarihi : 22.05.2020

Karar No : 2020/414

Konu Özeti : Hakkında hüküm verildiği suçtan dolayı cezası infaz edilen ilgili kişiye ait haberin yayımlandığı gazetenin internet sitesinden kaldırılması talebi

İlgili kişinin vekilinden alınan şikayet dilekçesinde özetle;

Müvekkilinin yurtdışında başına gelen bir olay nedeniyle internet yayınlarında adı ve soyadının geçtiği, Google arama motorunda adı ve soyadının aratılması sonucunda veri sorumlusu Gazetenin internet sitesinin linkine ulaşıldığı, söz konusu haberde müvekkilinin hüküm giydiği suça ilişkin bilgilerin yer aldığı ve haberin 2009 Haziran dönemine ait olması sebebiyle yaklaşık 10 yıl öncesine ilişkin olduğu, söz konusu cezanın tamamının infaz edildiği, ulaşılan haberler nedeniyle müvekkilinin iş hayatı ve ailesinin bu durumdan olumsuz etkilendiği, veri sorumlusu Gazeteye başvurulduğu; ancak başvurusunun aynı gün reddedildiği ifade edilerek kişisel verileri ve özel nitelikli kişisel verilerini ihlal eden tarafların hukuka aykırı davranışlarına son verilerek haberlerin kaldırılması, ilgili kurumlara 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında idari para cezası verilmesi, telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması nedeniyle veri işlenmesinin ve verinin yurt dışına aktarılmasının durdurulması, ilgili kurumlar hakkında Savcılığa suç duyurusunda bulunulması talep edilmektedir.

Konuya ilişkin olarak başlatılan inceleme çerçevesinde veri sorumlusu Gazeteden savunma sunması talep edilmiş, veri sorumlusu Gazetenin savunmasında,

- Kanunun 'İstisnalar' başlıklı 28 inci maddesinin birinci fıkrasının (c) bendinde yer alan "Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi" ifadeleri ile

kişisel verilerin 'ifade özgürlüğü' kapsamında işlenmesinin 'hukuka uygunluk' nedeni olarak değerlendirileceğinin açıkça ifade edildiği,

- Türkiye Cumhuriyeti Anayasasının 26 ncı maddesinin birinci fıkrasında "Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar." şeklinde düzenlemenin yer aldığı, dolayısıyla haber alma ve vermenin ifade özgürlüğünün bir parçası olarak değerlendirildiği ve Anayasa tarafından doğrudan koruma altına alındığı,

- Bu açıklamalar doğrultusunda, şikâyet konusu yazının 'kamunun haber alma hakkı' kapsamında kaleme alındığı, kanun koyucu tarafından veri işleme kuralları istisnaları arasında olan 'ifade özgürlüğü' içerisinde değerlendirilmesi gerektiği,

- Şikâyet eden vekiline gönderilen cevabi yazıda yer alan yayın ilkelerine ilişkin olarak; basın ve genel manada medyanın yasama, yürütme ve yargıdan sonra 4. güç olarak değerlendirildiği ve AİHM Kararlarında ifade edildiği üzere 'Demokrasinin Bekçi Köpeği' olarak kabul edildiği, basın kuruluşlarının genel yargı denetimi dışında bir iç denetim mekanizması kapsamında 'yayın ilkeleri oluşturarak' bunları uyguladığı ve yürüttüğü,

- İlgili kişinin kişisel verilerinin internet sitesinden kaldırılmamasına ilişkin gerekçelerin 'kamunun haber alma hakkı' içerisinde yer alan 'basın özgürlüğü' çerçevesinde kaleme alınması ve 'hukuka uygunluk nedeni' içermesi ile bağlantılı olduğu,

- İlgili medya grubunun bünyesinde yer alan bütün yayın organları ile ilgili her gün onlarca 'içerikten çıkarma, değiştirme' taleplerinin taraflarına iletildiği, okuyucuların haberde bahsi geçen olgular tamamen görünürde gerçeğe uygun olsa dahi kişisel olarak rahatsız edici olduğu gerekçesi ile yayından kaldırma taleplerinin bulunduğu, medyanın kamuoyu üzerindeki haber verme hak ve görevi doğrultusunda özellikle yaşanan adli süreçler ile ilgili yapılan bu haberlerin, gelişigüzel ve üstün kamuoyu yararı dikkate alınmadan sadece ilgilisi tarafından rahatsız edici bulunduğu için kaldırılması dolayısıyla orta ve uzun vadede medyanın işlevsiz kalması anlamına geleceği ve kamunun haber alma hakkının zarar görebileceği,

- İlgilisi tarafından içeriğin kaldırılması talepli hususlar değerlendirilirken üstün kamu yararının dikkate alındığı ve bu husus çerçevesinde her somut olay için ayrı bir değerlendirmenin yapıldığı, şikayete konu olayda ise ilgili kişinin gerçekleştirmiş olduğu eylemin tarafsız bir mahkeme tarafından araştırıldığı ve nihayetinde mahkumiyet kararı verilerek bu kararın kamuya açık bir şekilde ilan

edildiği, dolayısıyla gizli bir bilginin taraflarınca ifşa edilmesinin söz konusu olmadığı gibi haberde bahsi geçen bilgilerin tamamının yargı makamları kararı ile kesinlik kazandığı, haber tarihi üzerinden belli bir zaman geçmiş olması gerekçesine dayanarak içeriklerin kaldırılması halinde medya kuruluşlarının arşivlerinin tamamen eriyeceği ve kamu denetimi için önemli olan toplumsal belleğin ortadan kalkacağı,

- Yayınların kaldırılması ile ilgili olarak 5651 sayılı Kanun ile 'erişim engelleme'nin mümkün kılındığı, ilgili Kanun kapsamında bir içeriğin 'kişilik haklarını ihlal ettiğini' iddia eden şahsa, bağımsız ve tarafsız mahkemeler aracılığıyla her somut olay için ayrı değerlendirme yapılması ve hakimler tarafından uygun görüldüğü takdirde erişim engelleme kararının verilmesini sağlayabilecek Sulh Ceza Hakimlikleri aracılığıyla talepte bulunma hakkının ihdas edildiği, bu minvalde alınacak kararların taraflarına tebliği sonrasında erişim engelleme kararının 4 saat içerisinde taraflarınca uygulandığı,

açıklamalarına yer verilmiş ve bu kapsamda, kamu yararı içeren bir haber ile ilgili olarak ilgili kişinin yargı yoluna başvurmayıp kanuni muvazaa yoluna giderek Kurula başvurusunun yargı denetiminden kaçması ve hakkını kötüye kullanmış olmasına sebebiyet verdiği ifade edilerek bu açıklamalar ve ilgili mevzuat doğrultusunda; Anayasa Mahkemesi'nin 03.03.2016 tarih ve 2013/5653 sayılı Kararında "...her ne kadar kişisel verilerin ancak Kanunla veya kişinin açık rızası ile işlenebileceği belirtilmiş ise de Anayasada tanımlanan ifade ve basın özgürlükleri kapsamında yapılan bir haberin anılan sınırların istisnası olacağı açıktır..." "...Unutulma hakkının internet gazete arşivlerindeki her türlü haber yönünden uygulanmasını beklemek mümkün değildir..." "...internetten tutulan arşivlerin, ifade ve basın özgürlükleri kapsamında olduğu açıktır. Dolayısıyla internette yayımlanan ve gazetecilik faaliyeti kapsamında kabul edilen bir haber arşivinin yayından kaldırılması basın özgürlüğüne yönelik bir müdahale teşkil eder." şeklinde yer aldığı, bu çerçevede şikayet sonucu başlatılan soruşturma neticesinde tarafları hakkında "6698 sayılı Kanuna aykırı bir işlemin bulunmadığı" yönünde karar verilmesi talep edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 22/05/2020 tarih ve 2020/414 sayılı Karar ile;

- Kanunun "Tanımlar" başlığını taşıyan 3 üncü maddesinde kişisel verinin "kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilgi", ilgili kişinin "kişisel verileri işlenen her türlü gerçek kişi", veri sorumlusunun ise "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi" olarak tanımlandığı,

- Diğer taraftan, Kanunun “İlgili Kişinin Hakları” başlıklı 11 inci maddesinde herkesin, veri sorumlusuna başvurarak kendisiyle ilgili; kişisel verilerinin işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerinin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerinin aktarıldığı üçüncü kişileri bilme, kişisel verilerinin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerinin silinmesini veya yok edilmesini isteme, kişisel verilerinin düzeltilmesi veya silinmesi/yok edilmesi ile ilgili yapılan işlemlerin kişisel verilerinin aktarıldığı üçüncü kişilere bildirilmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme ve kişisel verilerinin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme hakkına sahip olduğunun hükme bağlandığı,
- Kanunun 28 inci maddesinin birinci fıkrasının (c) bendine göre ise “Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi” halinde Kanun hükümlerinin uygulanmayacağını düzenlediği,
- İfade özgürlüğünün bir yansıması olan basın özgürlüğü ile kişilik hakları karşı karşıya geldiğinde haberin;
 - Kamu ilgi ve yararı taşıması,
 - Gerçek ve güncel olması,
 - Özü ile biçimi arasındaki denge
 - kriterleri kapsamında değerlendirilmesi suretiyle hangi hakka üstünlük tanınması gerektiğinin belirlenmesinin önem arz ettiği,
 - Bu kapsamda öncelikle kamu yararının tespitinde, haberin kişilerin gereksiz merak duygularına mı yoksa yüksek ahlaki ve hukuki değerlerin korunmasına mı hizmet ettiğinin değerlendirilmesinin uygun olacağı, bu anlamda, toplumsal ilgi uyandıran, kamuoyu üzerinde düşünmeye ve tartışmaya sevk eden, belli bir sorunun aydınlanmasına ve buna çözüm yollarının gösterilmesine hizmet eden olayların açıklamasında kamu yararının bulunduğu, örneğin, yasa dışı uygulamaların, rüşvet ve yolsuzlukların kamuoyuna iletilmesinde, eleştirilmesinde kamu yararı bulunduğu, öte yandan, kamu ilgi ve yararı kriteri kapsamında siyasetçiler ve kamu görevlilerine dair yapılan haberler bakımından

basın özgürlüğüne yapılan sınırlamaların daha dar yorumlanmasının uygun olacağını değerlendirildiği,

- Bu çerçevede, basın özgürlüğüne yapılan sınırlamanın daha dar yorumlanabilmesine olanak sağlayacak olan ilgili kişinin toplum tarafından tanınır, bilinir olma gibi siyasetçi, ünlü veyahut kamu görevlisi olma kriterlerinden birini taşıdığına dair herhangi bir bilgiye yapılan incelemelerde rastlanılmamış olmakla birlikte bahse konu olaya konu haberin kamu ilgi ve yararının yasa dışı uygulamalar, rüşvet ve yolsuzlukların kamuoyuna iletilmesi gibi değerlendirilebilecek olan insan kaçakçılığı suçunu işleyen failler hakkında olduğunun görüldüğü, bu kapsamda, haberin yayımlanması ile toplumun bilgilendirilmesi ve bu durumdan haberdar edilmesinin toplumsal bir faydaya yol açabileceğinin mümkün görüldüğü, dolayısıyla, söz konusu haber her ne kadar toplum tarafından tanınır olmayan bir vatandaş hakkında olmuş olsa dahi bu haberin kamuya duyurulmasında kamunun ortak menfaatinin bulunduğu sonucuna varıldığı,

- Karşı karşıya gelen hakların değerlendirilmesi açısından haberin gerçek ve güncel olması ikinci kriter olarak sayılmış olup gerçeklik unsurunun, somut gerçeğe değil, olayın, haberin verildiği andaki belirli biçimine uygunluk olarak anlaşılması gerektiği, haberin güncel olmasının ise somut olayın açıklandığı tarihlerde kamu yararının bulunması esasına dayandığı, üzerinden süre geçmiş ve açıklanmasında artık kamu yararı bulunmayan bir olayın yayımlanmasında haber verme hakkından söz edilemeyeceğinden, burada kişilik hakkına üstünlük tanınması gerekeceği, geçmişteki bir olayın gündeme getirildiği haberin, hukuka uygun kabul edilebilmesi için kamu yararı taşıması gerektiği,

- Bahse konu şikâyet başvurusunun, haberin ve veri sorumlusunun cevabi yazısının incelenmesi neticesinde; gerçeklik unsuruna ilişkin olarak ilgili kişinin şikâyet başvurusunda yer alan *"Müvekkilinin 2009 yılında İngiltere'de 3 sene hapis cezası ile cezalandırıldığı, Haziran 2009'da cezaevine girip Ekim 2010'da çıktığı, 1,5 yıl cezaevinde kalması sonrasında İngiliz Yasaları doğrultusunda kontrollü tahliye şeklinde kalan cezasını cezaevi dışında tamamladığı ve Nisan 2012 itibarıyla müvekkile verilen cezanın tamamının infaz edildiği..."* ifadelerinden de anlaşılacağı üzere habere konu olayın yargı tarafından verilen kararlar kanıtlanmış olduğu, öte yandan, haberin güncel olması kriterinin değerlendirilmesi kapsamında mevcut şartlar altında bahse konu haberin gündemde kalması hususunda ve kamunun bu haberi alma konusunda menfaatinin devam ettiği dolayısıyla hukuka uygunluk sebebi sayılabilecek kamu yararının söz konusu haberde bulunduğu sonucuna varıldığı,

- Biçim ve öz arasındaki denge kriteri açısından ise haberde kullanılan dil, ifade ve resimlerin haberin veriliş biçiminin gerektirdiği ölçüde olması, haberin verilişinde gerekli, ilgili ve yararlı olmayan

beyan ve deęerlendirmelerde bulunulmaması gerektięi, haberin özü ile biçimi arasında denge gözetilmesi gereklilięi bulunduęu,

- Söz konusu haberde, biçim ve öz arasındaki denge kriteri açısından ise kullanılan dil, ifade ve resimlerin haberin veriliş biçiminin gerektirdięi ölçüde olduęu, haberin verilişinde gerekli, ilgili ve yararlı olmayan beyan ve deęerlendirmelerde bulunmadıęı sonucuna varıldıęı,

deęerlendirmelerinden hareketle;

- İlgili kişinin kendisine ilişkin verinin söz konusu habere konu edilerek yayımlanmasında hâlihazırda kamu yararı bulunduęu ve bu itibarla çatışan haklar bakımından ifade özgürlüęünün kişilik haklarına üstün geldięi sonucuna varıldıęı ve söz konusu başvurunun Kanunun 28 inci maddesinin birinci fıkrasının (c) bendi çerçevesinde deęerlendirilmesi nedeniyle ilgili kişinin şikayeti ile ilgili olarak Kanun kapsamında yapılacak bir işlem bulunmadıęına karar verilmiştir.

2020/407 sayılı KVKK Kararı

İlgili kişinin tahlil sonuçlarının veri sorumlusu hastane tarafından hukuka aykırı şekilde üçüncü kişilere aktarılması hakkında Kişisel Verileri Koruma Kurulunun 20/05/2020 tarihli ve 2020/407 sayılı Karar Özeti

Karar Tarihi : 20.05.2020

Karar No : 2020/407

Konu Özeti : İlgili kişinin tahlil sonuçlarının veri sorumlusu Hastane tarafından hukuka aykırı şekilde üçüncü kişilere aktarılması

İlgili kişinin şikâyetinde özetle; şikayete konu hastanenin Tüp Bebek bölümüne tahlil için başvurduğu, tahlil sonuçlarının e-posta yoluyla kendisine iletiildiği, ancak aynı e-postanın başka bir e-posta adresine ve tanımadığı bir kişiye daha gönderildiğini fark ettiği, veri sorumlusu Hastanenin “Kişisel Verilerin Korunması ve İşletilmesi Politikası” kapsamında kişisel verilerinin muhafazasında gerekli tedbirleri almadığı, kişisel verilerinin işleme amacının gereklilikleri doğrultusunda üçüncü kişilere aktarılmasında ilgili mevzuata ve alt düzenlemelere uygun davranmadığı, bu sebeple veri sorumlusundan ihtarname ile bilgi talebinde bulunduğu, söz konusu talebine ilişkin veri sorumlusu tarafından hatanın kabul edildiğini içeren bir cevap verildiği belirtilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde şikayet dilekçesinde yer alan iddialara ilişkin veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişinin hastanenin Tüp Bebek Bölümüne tahlil için başvurduğu, tahlil sonuçlarının aynı gün aynı test için hastalarını hastane laboratuvarına yönlendirmiş olan başka bir doktorun özel asistanına ve hastaların kendilerine e-posta olarak iletiildiği,
- Özel ve genel nitelikteki kişisel verilerin muhafazasını sağlamak amacıyla Kanunun 12 nci maddesi kapsamında hukuka uygun güvenlik düzeyini temin etmeye yönelik hangi idari ve teknik tedbirlerin alındığına ilişkin olarak; sistemdeki bilgilerin hasta temsilcilerine görmesine kapatılması kararı alındığı, hekimlerin sadece kendi hasta bilgilerine, hemşirelerin görev yaptıkları servislerde yatan

hasta bilgilerine erişebilmesi kararı alındığı, tıbbi sekreterlik ve anlaşmalı kurumlar birimi çalışanlarına gerektiğinde erişim için özel yetkilendirme yapılacağı

ifade edilerek, Hastane tarafından veri sorumlusu olarak mesul müdürün gösterildiği Veri Sorumlusu Tanıtım Formu Kurumumuza intikal ettirilmiştir.

Konuya ilişkin olarak yapılan incelemede, Kişisel Verileri Koruma Kurulunun 20/05/2020 tarihli ve 2020/407 sayılı Kararı ile,

- Kanunun “Özel Nitelikli Kişisel Verilerin İşlenme Şartları” başlıklı 6 ncı maddesinin (1) numaralı fıkrasında özel nitelikli kişisel verilerin “*Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri*” olarak sayıldığı, bu minvalde ilgili kişinin tahlil sonuçlarının sağlıkla ilgili özel nitelikli kişisel veri olduğu,

- Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise Kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanunun 6 ncı maddesinde düzenlenen özel nitelikli kişisel verilerin işlenmesine ilişkin ise; “(2) *Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.*(3) *Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.*” hükümlerine yer verildiği, anılan maddenin (4) numaralı fıkrasında da, “*Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.*” hükmünün yer aldığı, bu çerçevede, Kanunun 22 nci maddesinin (1)

numaralı fıkrasının (ç) ve (e) bentleri uyarınca Kişisel Verileri Koruma Kurulunun 31/01/2018 tarihli ve 2018/10 sayılı Kararı ile “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler” belirlenerek Resmi Gazetede yayımlandığı,

• Kanunun 8 inci maddesinde “(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz. (2) Kişisel veriler; a) 5 inci maddenin ikinci fıkrasında, b) Yeterli önlemler alınmak kaydıyla, 6 ncı maddenin üçüncü fıkrasında, belirtilen şartlardan birinin bulunması halinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir.”

hükümlerine yer verildiği, bu çerçevede, kişisel verilerin herhangi bir veri sorumlusu tarafından üçüncü bir tarafla paylaşılması da dahil olmak üzere işlenmesinin ancak açık rızanın bulunması ya da Kanunda belirtilen açık rıza dışı diğer hallerin varlığında mümkün bulunduğu,

• Bu çerçevede başvuruya konu olayda, ilgili kişinin veri sorumlusu Hastanede bulunan tahlil sonuçlarının sağlığa ilişkin özel nitelikli kişisel veri olduğu dikkate alındığında, bahse konu tahlil sonuçlarının üçüncü bir taraf olarak, hastaneden bağımsız şekilde çalışan ve ayrı bir gerçek kişi veri sorumlusu olarak değerlendirilen doktorun asistanına mail atılmak suretiyle aktarılmasında Kanunun 8 inci maddesi kapsamında herhangi bir hukuki dayanak söz konusu olmadığından ve veri sorumlusu Hastane tarafından da söz konusu aktarımın sehven yapıldığının beyan edilmiş olmasından hareketle ilgili kişinin kişisel verilerinin hukuka aykırı olarak aktarıldığı kanaatine varıldığı

değerlendirmelerinden hareketle;

• Veri sorumlusu Hastane tarafından Kuruma iletilen Veri Sorumlusu Tanıtım Formunda veri sorumlusu olarak mesul müdürün gösterildiği ve bu kişiye ilişkin bilgilerin söz konusu forma işlendiği görüldüğünden, 6698 sayılı Kanunun 3 üncü maddesinde veri sorumlusunun, “Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi” olduğu, tüzel kişilerin, kişisel verileri işleme konusunda gerçekleştirdiği faaliyetler kapsamında bizatihi kendilerinin “veri sorumlusu” olduğu, ilgili düzenlemelerde belirtilen hukuki sorumluluğun da tüzel kişinin şahsında doğacağı, bu konuda kamu hukuku tüzel kişileri ve özel hukuk tüzel kişileri bakımından bir farklılık gözetilmediği, bahse konu hüküm çerçevesinde Hastanenin bizatihi veri sorumlusu olduğunun Hastaneye hatırlatılmasına,

• Veri sorumlusu Hastane tarafından, ilgili kişinin özel nitelikli kişisel verisinin 6698 sayılı Kanunun 8 inci maddesinde belirtilen ilgili kişinin açık rızası ya da 6 ncı maddede düzenlenen işleme şartlarından biri olmadığı halde üçüncü kişilere aktarılmak suretiyle hukuka aykırı olarak işlenmesi sebebiyle, Kanunun “Veri Güvenliğine İlişkin Yükümlülükler” başlıklı 12 nci maddesinin birinci

fıkrasına yönelik yükümlülüğünü yerine getirmediği kanaatine varılan veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2020/404 sayılı KVKK Kararı

İşverenin, işçisine ait kişisel verileri ve özel nitelikli kişisel verileri; aydınlatma yükümlülüğünü yerine getirmeden ve hukuka aykırı işlemesi hakkında Kişisel Verileri Koruma Kurulunun 20/05/2020 tarihli ve 2020/404 sayılı Karar Özeti

Karar Tarihi : 20.05.2020

Karar No : 2020/404

Konu Özeti : İşverenin, işçisine ait kişisel verileri ile özel nitelikli kişisel verileri; aydınlatma yükümlülüğünü yerine getirmeden ve hukuka aykırı işlemesi

Kuruma intikal eden şikâyet dilekçesinde özetle,

- İlgili kişinin çalışmakta olduğu veri sorumlusu şirketten 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 11 maddesi kapsamındaki hakları kapsamında bilgi talebinde bulunduğu, söz konusu talebine yeterli cevap alamadığı,
- Veri sorumlusu tarafından kendisine kişisel verilerinin işlenme amacıyla ilgili olarak genel nitelikli bir bilgilendirme yapıldığı, verilerin işlenme ve saklanma süreçlerine ilişkin bilgi verilmediği,
- Veri sorumlusunun cevap yazısında çalışanların bordro bilgileri ve disiplin süreçlerine ilişkin bilgilerin HR Yazılım Programında tutulduğunu; tüm özlük bilgilerinin ... Arşiv ve Dokümantasyon Programında tutulduğunu; performans değerlendirme süreçleri, disiplin süreçleri, masraf bilgilerine ait verilerin ... Yazılım aracılığı ile elektronik ortamda tutulduğu bilgisinin verildiği, ancak bu programa kimlerin erişiminin olduğu, yetki matrisi olup olmadığına dair bilgilendirmenin yapılmadığı, ayrıca adı geçen programlarda saklanan verilerin ne kadar süre sonra silindiğine dair bilgi verilmediği, tüm çalışanların erişim yetkisi olan İntranet ağında bulunan "Veri Güvenliği Politikası"nda da bu bilgilere yer verilmediği,
- Veri sorumlusu tarafından çalışanlarından elektronik ortamda KVKK Çalışma Muvafakatnamesi alındığı, söz konusu muvafakatnamenin çok geniş kapsamlı olduğu ve yeterli aydınlatmanın yapılmadığı, verilecek rızanın "battaniye rıza" olduğu, kendisinin bu muvafakatnameye onay vermekten imtina ettiği ancak onay vermek durumunda bırakıldığı,

- Tüm çalışanların parmak izinin alındığı, çalışanların bu veriyi vermek zorunda bırakıldığı, parmak izi alındığı sırada çalışanların açık rızalarının alınmadığı ve aydınlatma yükümlülüğünün de yerine getirilmediği, biyometrik verilerin üçüncü taraf bir şirket ile paylaşılıp paylaşılmadığı, yeterli güvenlik önlemleri ile saklanıp saklanmadığı hususlarında tarafına bilgi verilmediği

belirtilerek hukuka aykırı uygulamaları nedeniyle veri sorumlusu hakkında gerekli yaptırımların uygulanması talep edilmiştir.

Başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişinin hangi kişisel verilerinin hangi amaçlara dayanılarak işlendiğine dair detaylı bilginin ilgili kişiye verdikleri cevapta da yer aldığı,

- Şirketin kişisel verilerin gizliliğine ve güvenli şekilde saklanmasına önem verdiği, fiziki dosyaların yalnızca yetkili kişilerin erişimine açık olan kilitli dolaplarda ya da fiziki arşivlerde tutulduğu, fiziki olarak aktarılması gereken evrakların gizlilik dereceli belge olarak gönderildiği, elektronik ortamda tutulan kişisel verilerin ise sadece belirli kişilerin erişimine açık klasörlerde ve /veya şifreli yazılımlarda saklandığı, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin hukuka aykırı işlenmesinin önlenmesi, bilgi ve veri güvenliği ile alakalı mevzuatlar hakkında eğitimlerin verildiği, şirket içinde rastgele ve periyodik denetimler yapılarak bu ortamlara yetkisiz giriş ve çıkışların engellendiği,

- Açık rıza metinlerinde hangi kişisel verilerin hangi meşru amaçlarla işleneceği, kimlere hangi amaçlarla aktarılabilceği, hukuki sebepleri, toplama yöntemi, kişisel verilere ilişkin olarak çalışanların haklarının neler olduğunun detaylı olarak anlatıldığı,

- Hukuki dayanakların yerine getirilebilmesi için, çalışan muvafakatnamesinin ve açık rıza metninin her çalışandan ıslak imzalı şekilde temin edildiği; şayet çalışan tarafından onay verilmezse özlük dosyasının tamamlanmamış kabul edildiği,

- Çalışanların "http://.....com/" adresinden kişisel verilerin güvenli olarak saklanmasına ilişkin politika, prosedür ve kılavuzlara ulaşabildikleri, aynı şekilde yetki dereceleri matrisinin çalışanların erişimine açık olan bu adreste yayınlandığı, matriste herhangi bir değişiklik söz konusu olduğunda güncelleme duyurularının site üzerinden yapıldığı,

- Çalışan ve aday çalışanlarının her birine KVKK Aydınlatma Metni ve Açık Rıza metninin tebliğ edildiği ve çalışanların bu metinleri imza karşılığı olarak veri sorumlusuna teslim ettiği,

- Çalışanların parmak izlerinin acil durum yönetimi sürecinin yürütülmesi, fiziksel mekan güvenliği ve yetkili kurum ve kuruluşlara bilgi verilmesi amaçlarıyla kullanıldığı, parmak izlerinin kriptografik yöntemlerle muhafaza edildiği, bu sebeple bu verilerin biyometrik veri niteliği taşımadığı,
- Özel nitelikli verilerin işlenmesi kapsamında veri sorumlusu tarafından, taşınabilir bellek, CD veya VCD ile bunların taşınması gerektiğinde kriptografik yöntemlerle şifreleme yapıldığı, fiziken taşınması gerektiğinde ise gizlilik dereceli belge olarak gönderildiği,
- Veri sorumlusu tarafından Kanununun 12 nci maddesi kapsamında kişisel verilerin uygun güvenlik düzeyini temin etmek amacıyla çalışanlara kişisel verilerin hukuka aykırı işlenmesinin önlenmesi, bilgi ve veri güvenliği ile alakalı mevzuatlar hakkında eğitimlerin verildiği, çalışanlara gizlilik sözleşmesi imzalatıldığı, güvenlik prosedür ve politikalarına uymayan çalışanlara disiplin prosedürünün uygulandığı, çalışanlar için veri güvenliği hükümlerini içeren disiplin düzenlemelerinin mevcut olduğu, çalışanlar için veri güvenliği ile ilgili olarak eğitim ve farkındalık çalışmaları yapıldığı, aydınlatma yükümlülüğünün yerine getirildiği, erişim loglarının düzenli olarak tutulduğu, şirket içi rastgele denetimler yapıldığı, bilgi güvenliği, kullanımı, saklanması imhası konularında şirket politikaları hazırlandığı ve uygulandığı, verilerin saklandığı ortamlar için arttırılmış güvenlik önlemleri alındığı, bu alanlara yetkisiz giriş ve çıkışların önlendiği, ağ ve uygulama güvenliği sağlandığı, kişisel veri içeren evrakların fiziken gönderilmesi gerektiğinde gizlilik dereceli belgeler olarak gönderildiği, bulutta depolanan kişisel verilerin güvenliğinin yalnızca yetkili kişilerin ulaşabileceği biçimde ayarlandığı

ifade edilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 20/05/2020 tarihli ve 2020/404 sayılı Kararı ile;

- Kanunun "Veri Sorumlusunun Aydınlatma Yükümlülüğü" başlıklı 10 uncu maddesinin "(1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; a) Veri sorumlusunun ve varsa temsilcisinin kimliği, b) Kişisel verilerin hangi amaçla işleneceği, c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi, d) 11 inci maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür." hükmünü amir olduğu,
- Aydınlatma yükümlülüğünün gerek açık rıza alınacağı durumlarda gerek Kanundaki diğer kişisel veri işleme şartlarından bağımsız olarak yerine getirilmesi gereken bir yükümlülük olduğu, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin (Tebliğ) 5 inci maddesinin birinci fıkrasının (e) bendi uyarınca aydınlatma yükümlülüğünün yerine

getirilip getirilmediğinin ispatının veri sorumlusuna ait bulunduğu, veri sorumlusu tarafından aydınlatma yükümlülüğü yerine getirilirken; öncelikle veri sorumlusunun kimliğine, kişisel verilerin hangi amaçlarla işlendiğine, kişisel verilerin kimlere ve hangi amaçlarla aktarılabileceğine, elde edilecek kişisel verilerin toplanma yöntemlerine, işlemenin hukuki sebeplerine ve ilgili kişinin Kanununun 11 inci maddesindeki haklarına aydınlatma metninde yer verilmesi gerektiği,

- Veri sorumlusu tarafından Kuruma gönderilen savunma yazısında çalışan ve aday çalışanlarının her birine KVKK Aydınlatma Metni ve Açık Rıza metninin tebliğ edildiği ve çalışanların bu metinleri imza karşılığı olarak veri sorumlusuna teslim ettiği ifade edilmekle birlikte yazıları ekinde aydınlatma metnine yer verilmediği, öte yandan ilgili kişinin şikayet dilekçesi ekinde yer verilen “Kişisel Verilerin İşlenmesine İlişkin Çalışan Muvafakatnamesi”nin hem aydınlatma metni hem de açık rıza metni olarak düzenlendiği kabul edildiğinde; Tebliğin 5 inci maddesinin birinci fıkrasının (f) bendinde yer alan “*Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir.*” hükmü gereği şekli olarak aydınlatmanın usulüne uygun yapıldığından söz edilemeyeceği,

- Diğer taraftan, bu metnin içerik olarak da açık rıza kapsamında ilgili kişiyi bilgilendirdiğinden ya da aydınlatma yükümlülüğünü yerine getirdiğinden söz edilemeyeceği zira, metinde çeşitli kişisel veri kategorileri sıralandıktan sonra “(...) sayılan kişisel veriler dahil olmak üzere ancak bunlarla sınırlı olmaksızın (...)” ifadesine yer verildiği ve hangi kişisel verilerin işleneceği (kategorik olarak) hususunun muğlak bırakıldığı, işlenecek veri kategorileri sıralandıktan sonra veri işleme amaçları da art arda sıralanmak suretiyle hangi veri kategorisinin hangi amaçla işleneceğine dair herhangi bir açıklamaya yer verilmediği, metinde “... uygun gördüğü diğer üçüncü kişilere ve/veya yurt dışında paylaşılabileceği” ifadesinin yer aldığı bu kapsamda kimlere aktarım yapılacağı muğlak bir şekilde veri sorumlusuna bırakıldığı, ayrıca metinde biyometrik veri niteliğini haiz olan parmak izinin veri kategorileri içerisinde dahi sayılmadığı,

- “Açık rıza” kavramının Kanununun 3 üncü maddesinin birinci fıkrasının (a) bendinde; “*Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*” şeklinde tanımlandığı, ilgili kişilerin açık rızasının alınacağı hallerde; rızanın belirli bir konuya ilişkin olması, bilgilendirmeye dayanması ve özgür iradeyle açıklanması gerektiği, veri işlemek üzere verilen açık rızanın geçerli olması için, açık rızanın öncelikle belirli bir konuya ilişkin ve o konu ile sınırlı olarak verilmesi ve veri sorumlusu tarafından açık rıza beyanının hangi konuya ilişkin olarak istenildiğinin açıkça ortaya konulması gerektiği, bununla birlikte; açık rıza bir irade beyanı olduğundan, kişinin özgür bir şekilde rıza verebilmesi için, neye rıza gösterdiğini de bilmesi ve kişinin sadece konu üzerinde değil, aynı

zamanda rızasının sonuçları üzerinde de tam bir bilgi sahibi olması gerektiği, bu sebeple bilgilendirmenin, veri işleme ile ilgili bütün konularda açık ve anlaşılır bir biçimde, mutlaka verinin işlenmesinden önce yapılması gerektiği, ayrıca açık rızanın geçerlilik kazanabilmesi için kişinin yaptığı davranışın bilincinde ve kendi kararı sonucunda olması ve açık rızanın özgür iradeyle açıklanması gerektiğinden, herhangi bir hususun ilgili kişi tarafından açık rıza verilmesi şartına bağlanmaması, tarafların eşit konumda olmadığı veya taraflardan birinin diğeri üzerinde etkili olduğu durumlarda rızanın özgür iradeyle verilip verilmediğinin dikkatle değerlendirilmesi gerektiği, örneğin işçi-işveren ilişkisinde, işçiye rıza göstermeme imkânının etkin bir biçimde sunulmadığı veya rıza göstermemenin işçi açısından muhtemel bir olumsuzluk doğuracağı durumlarda, rızanın özgür iradeye dayandığının kabul edilemeyeceği,

- Somut olayda, veri sorumlusu tarafından açık rıza metninin onaylanması için çalışanlara e-postalar gönderildiği, metni imzalamayan çalışanların listesinin tutulduğu, bu listelerin başkaca çalışanlara gönderilmesi suretiyle metni imzalamayan çalışanların metni imzalamalarının sağlanmasının talep edildiğinin anlaşıldığı, bununla birlikte çalışan tarafından onayın verilmemesi sebebiyle özlük dosyasının tamamlanmamış kabul edildiği durumlarda; işçiye rıza göstermeme imkânının etkin bir biçimde sunulmamasından ötürü verilen rızanın, geçerli bir açık rıza beyanı olarak değerlendirilemeyeceği, öte yandan, işçinin eşine ve çocuğuna ait kişisel verilerin işlenmesi için açık rıza vermesinin geçerlilik taşımayacağı,

- Yine ilgili kişinin dilekçesinde; “ (...) parmak izinin alındığını, çalışanların bu veriyi vermek zorunda bırakıldığını, parmak izi alındığı sırada ilgili kişilerin açık rızalarının alınmadığını ve aydınlatma yükümlülüğünün de yerine getirilmediğini, biyometrik verilerin üçüncü taraf bir şirket ile paylaşılıp paylaşılmadığı, yeterli güvenlik önlemleri ile saklanıp saklanmadığı hususlarında tarafına bilgi verilmediğinin (...)” dile getirildiği, veri sorumlusunun ise, “(...) çalışanların parmak izlerinin acil durum yönetimi sürecinin yürütülmesi, fiziksel mekan güvenliği ve yetkili kurum ve kuruluşlara bilgi verilmesi amaçlarıyla kullanıldığını, parmak izlerinin kriptografik yöntemlerle muhafaza edildiğini, bu sebeple bu verilerin biyometrik veri niteliği taşımadığını (...)” belirttiği, biyometrik verilerin hash yöntemi ile saklandıklarında biyometrik veri olma niteliklerini kaybetmedikleri, bu bakımdan açık rızanın bulunmadığı hallerde biyometrik verilerin ancak Kanunun 6 ncı maddesinde öngörülen kanunlarda öngörülme şartı doğrultusunda işlenebileceği, bununla birlikte söz konusu verinin işlenme amacının da Kanunun genel ilkeleri arasında yer alan “İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkesine de aykırı olduğu, örneğin fiziksel mekan güvenliğinin sağlanabilmesi için giriş esnasında manyetik kart sistemi, RFID etiketi, cep telefonuna gönderilecek bir SMS’in sisteme girilmesi gibi alternatif yollar ile

sağlanması mümkünken çalışanların biyometrik veri niteliğindeki parmak izi verisinin alınmasının Kanunun 4 üncü maddesinin (2) numaralı fıkrasında yer alan “İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkesi ile bağdaşmadığı, bu çerçevede “acil durum yönetimi sürecinin yürütülmesi, fiziksel mekan güvenliği ve yetkili kurum ve kuruluşlara bilgi verilmesi amaçları”nın farklı yollarla da hasıl olması mümkünken söz konusu veri işleme faaliyeti ile orantısız bir veri işleme yapıldığının değerlendirildiği,

- İşlenen kişisel verilerin aktarıldığı üçüncü kişiler arasında “Bu bölümde sayılan şirketlerin yerini alabilecek diğer şirketler” benzeri ifadelerin yer alması halinde, işlenecek kişisel verilerin tam olarak nereye aktarılacağına rıza verecek ilgili kişi tarafından tam olarak bilinemeyebileceğinden, bu şekilde verilen rızanın açık rıza olarak değerlendirilmesinin mümkün olmayacağı,

- Öte yandan kişisel verilerin yurtdışında mukim üçüncü kişilere aktarılması durumunda Kanunun 9 uncu maddesi uygulama alanı bulacağı, “Kişisel verilerin yurtdışına aktarılması” başlıklı 9 uncu maddesinde kişisel verilerin, ilgili kişinin açık rızası olmaksızın yurtdışına aktarılamayacağı; kişisel verilerin, Kanunun 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede yeterli korumanın bulunması, yeterli korumanın bulunmaması durumunda ise Türkiye’deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabileceğinin hükme bağlandığı, bu çerçevede yurtdışına veri aktarımlarında açık rızanın olmadığı hallerde 9 uncu maddede öngörülen prosedürün işletilmesi gerektiği,

- Ayrıca, veri sorumlusunun “bulutta depolanan kişisel verilerin güvenliğini yalnızca yetkili kişilerin ulaşabileceği biçimde ayarlandığı” ifadesi ele alındığında daha önce Kurul tarafından alınan 31.05.2019 tarihli ve 2019/157 sayılı I Kararı ile; “Google firmasına ait G-mail e-posta hizmeti altyapısının kullanılması durumunda gönderilen ve alınan e-postaların dünyanın çeşitli yerlerinde bulunan veri merkezlerinde tutulması söz konusu olacağından, böyle bir durumda kişisel verilerin yurt dışına aktarılmış olacağına ve veri sorumlularının söz konusu uygulamayı 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) “Kişisel verilerin yurt dışına aktarılması” başlıklı 9 uncu maddesi hükümlerine uygun olarak gerçekleştirmesine;“Server”ları yurt dışında bulunan veri sorumlularından/veri işleyenlerden temin edilen saklama hizmetlerinin de Kanunun 9 uncu maddesi hükümlerine uygun olarak gerçekleştirilmesine” karar verildiği, bu kapsamda serverları yurt dışında bulunan hizmetlerin kullanımının yurt dışına kişisel veri aktarımı olduğu ve Kanunun 9 uncu maddesine uygun hareket edilmesi gerektiği,

- Yukarıda yer alan açıklamalar doğrultusunda, veri sorumlusunun çalışanlarının açık rızaları olmaksızın kişisel verilerini ve özel nitelikli kişisel verilerini işlediği ve bu verileri yine çalışanlarının açık rızası olmaksızın yurtiçi ve /veya yurtdışına aktardığının anlaşıldığı, Kanunun 12 nci maddesinin birinci fıkrasında; veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ile kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu hükme bağlandığı, ancak veri sorumlusunun Kanunla kendisine yüklenmiş olan bu yükümlülükleri yerine getirmediği

değerlendirmelerinden hareketle;

- Aydınlatma yükümlülüğünü yerine getirmediği kanaatine varıldığından veri sorumlusu hakkında Kanunun 18 inci maddesinin birinci fıkrasının (a) bendi uyarınca 50.000 TL idari para cezası uygulanmasına,

- Veri sorumlusunun çalışanlarının ve yakınlarının açık rızaları olmaksızın kişisel verilerini ve özel nitelikli kişisel verilerini işlediği, işlediği özel nitelikli kişisel veriler bakımından Kanunun 4 üncü maddesinde yer alan genel ilkelerden ölçülülük ilkesine aykırı hareket ettiği ve bu verileri yine çalışanlarının açık rızası olmaksızın yurtiçi ve /veya yurtdışına aktardığı görüldüğünden, Kanunun 12 nci maddesinin birinci fıkrasında yer alan kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ile kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri alma yükümlülüğüne aykırı hareket ettiği kanaatine varılan veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 200.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2020/396 sayılı KVKK Kararı

İlgili kişinin, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili özel nitelikli kişisel verilerinin özlük dosyasından çıkarılması talebi hakkında Kişisel Verileri Koruma Kurulunun 20/05/2020 tarihli ve 2020/396 sayılı Kararı

Karar Tarihi : 20.05.2020

Karar No : 2020/396

Konu Özeti : İlgili kişinin, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili özel nitelikli kişisel verilerinin özlük dosyasından çıkarılması talebi

Kuruma intikal eden şikâyet dilekçesinde özetle, ilgili kişinin memuriyete ilk giriş tarihinden önce hakkında verilmiş olan ceza kararının özlük dosyasında yer aldığı, verilen kararda yer alan beş yıllık denetim süresinin dolduğu ve davanın düşmesine karar verildiği, kararın adli sicil kaydından silindiği, bu itibarla özlük dosyasında yer alan mezkûr karar ve ilgili dosyanın kaldırılarak imha edilmesi için veri sorumlusu çalıştığı kuruma yapmış olduğu başvurunun reddedildiği; ancak söz konusu dosyanın açık rızası dâhilinde, resmi olarak güvenlik soruşturması yapılmadan, kurumunda çalışmaya ilk başladığı tarihte İl Yazı İşleri Müdürünün kendisine sözlü olarak güvenlik soruşturması yapması ve mahkeme sürecinin devam etmesi sebebiyle mahkeme kararını getirmesinin gerekmesi üzerine özlük dosyasına konulduğu, anılan verinin muhafazasını gerektiren bir sebebin bulunmadığı belirtilerek özlük dosyasında yer alan mahkeme dosyasının kaldırılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişinin atamasının yapılabilmesini teminen başvuru belgelerinin istendiği, bu kapsamda sunulan belgeler arasında yer alan "Güvenlik Soruşturması ve Arşiv Araştırması Formu"nda "*Hakkınızda Verilmiş Bulunan Mahkûmiyet Hükümü veya Halen Devam Eden Ceza Davası Bulunup Bulunmadığı*" kısmının "Var" olarak beyan edilmesi nedeniyle, ilgili kişi hakkında verilmiş hükümler veya devam eden cezaların 657 sayılı Devlet Memurları Kanununun 48 inci maddesinde yer alan şartlara engel teşkil edip etmediğinin tespiti amacıyla, söz konusu mahkeme kararlarının ilgili kişinin

kendi isteği ile ... Asliye Ceza Mahkemesinden talep edilerek atamasının yapılıp yapılamayacağı hususunun incelenmesini teminen Kurumuna sunulduğu,

- İlgili kararın atamaya engel teşkil edip etmediği hususunda gerekli değerlendirmenin yapılarak atamanın gerçekleştirildiği ve ilgili kişinin görevine başladığı, söz konusu kararların atama onayı ile ilişkilendirildiği ve Kamu Personeli Genel Tebliğinin (Seri No: 2) “Özlük Dosyasının Tutulmasına İlişkin Usul ve Esaslar” başlıklı D maddesinin 5 inci fıkrasının birinci bendi gereğince özlük dosyasına konulduğu, işlemin 2013 yılında gerçekleştiği; ancak 6698 sayılı Kişisel Verilerin Korunması Kanununun (**Kanun**) 07.04.2016 tarihinde yürürlüğe girdiği

ifade edilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 20/05/2020 tarihli ve 2020/396 sayılı Kararı ile;

- Kanunun 3 üncü maddesinin birinci fıkrasının (d) bendi uyarınca kişisel verinin; kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi, (e) bendi uyarınca kişisel verilerin işlenmesinin; kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi, (ç) bendi uyarınca ilgili kişinin; kişisel verisi işlenen gerçek kişiyi, (1) bendi uyarınca veri sorumlusu; kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişiyi ifade ettiği,

- Bu çerçevede, şikâyete konu başvuruyu yapan kişinin gerçek kişi olduğu ve bu itibarla, ilgili kişi sıfatını haiz bulunduğu; ilgili kişinin Kuruma yapmış olduğu başvuruya konu ettiği mahkeme kararlarının kişiyi belirli kılma niteliğinin bulunması sebebiyle kişisel veri olduğu; söz konusu mahkeme kararlarının Kanunun 6 ncı maddesi kapsamında özel nitelikli kişisel veri niteliğini haiz bulunduğu,

- Kanunun 6 ncı maddesinin birinci fıkrasında kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerinin özel nitelikli kişisel veri olduğu, ikinci fıkrasında özel nitelikli kişisel verilerin ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğu, üçüncü fıkrasında, birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel verilerin kanunlarda öngörülen hallerde, sağlık ve cinsel hayata ilişkin

kişisel verilerin ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceğinin hükme bağlandığı,

- İlgili kişinin, başvurusunda resmi dayanağı olmaksızın yapıldığını iddia ettiği güvenlik soruşturması evrakının 2013 yılına ait olduğu, söz konusu tarihte 03.11.1994 sayılı Resmi Gazetede yayımlanan 4045 sayılı “Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun” un yürürlükte bulunduğu, anılan Kanunun 1 inci maddesi uyarınca güvenlik soruşturması işleminin yapılabilmesinin ön koşulunun; ilgili personelin ya kamu kurum veya kuruluşlarında “gizlilik dereceli birim” olarak nitelendirilen birimlerde ya da düzenlemede sınırlı olarak sayılan kurumlarda yahut görevlerde çalıştırılacak olması durumlarından birisinin gerçekleşmesi olduğu,

- İlgili kişiye güvenlik soruşturması ve arşiv araştırması işleminin yapılabilmesinin, konuya ilişkin temel düzenleme vasfı taşıyan 4045 sayılı “Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun” kapsamında, ilgili kişinin “gizlilik dereceli birim” olarak ifade edilen birimlerde çalıştırılacak olması koşuluyla; 4045 sayılı Kanuna dayalı olarak çıkarılan “Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği” kapsamında ise “...ilk defa veya yeniden kamu hizmeti ve görevlerine atanacakları...” ifadesi kapsamında mümkün olabileceği, bunun dışındaki olasılıklarda ise şikâyete konu olay tarihinde yürürlükte bulunan mevzuata aykırılık teşkil edeceğinin değerlendirildiği, bu açıdan bakıldığında, 4045 sayılı Kanun hükümleri uyarınca ilgili kişinin atanmış olduğu kadronun, kanunda “yetkili olmayan kişilerin bilgi sahibi olmaları halinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler” şeklinde ifade edilen birimler arasında yer alıp almadığı hususunun, Kanuna uygun bir kişisel veri işleme faaliyetinin gerçekleştirilip gerçekleştirilmediği noktasında önem arz ettiğinin görüldüğü,

- Öte yandan, “Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği”nin “Tanımlar” başlığını taşıyan 4 üncü maddesinde “gizlilik dereceli birim” kavramının tanımına yer verildiği, düzenlemeden, “gizlilik dereceli birim ve kısım” olarak ifade edilen kavramın, gizlilik dereceli bilgi ve belgeler ile bağlantılı olduğunun anlaşıldığı; bu noktada, herhangi bir kamu kurum ve kuruluşunda görev

yapmakta olan personelin, hukuki anlamda olmasa da, fiili olarak gizlilik dereceli birim ve kısımda çalışıyor olarak kabul edildiği/varsayıldığının değerlendirildiği,

- İlgili kişinin 657 sayılı Devlet Memurları Kanununun 48 inci maddesinde yer verilen şartlar arasında gösterilen “Kamu haklarından mahrum bulunmamak” ve “Türk Ceza Kanununun 53 üncü maddesinde belirtilen süreler geçmiş olsa bile; kasten işlenen bir suçtan dolayı bir yıl veya daha fazla süreyle hapis cezasına ya da affa uğramış olsa bile devletin güvenliğine karşı suçlar, Anayasal düzene ve bu düzenin işleyişine karşı suçlar, zimmet, irtikâp, rüşvet, hırsızlık, dolandırıcılık, sahtecilik, güveni kötüye kullanma, hileli iflas, ihaleye fesat karıştırma, edimin ifasına fesat karıştırma, suçtan kaynaklanan malvarlığı değerlerini aklama veya kaçakçılık suçlarından mahkûm olmamak.” koşullarının adayda bulunup bulunmadığının tespit edilebilmesini teminen birtakım belgelerin, aday tarafından veri sorumlusuna sunulmasının gerektiği; ancak atamaya esas teşkil eden belgelerin neler olduğuna ilişkin olarak 657 sayılı Kanunda herhangi bir hükmün yer almadığı, bununla birlikte; özel nitelikli kişisel veri niteliğini haiz bulunan “Ceza Mahkûmiyeti ve Güvenlik Tedbirleri” bilgisinin 657 sayılı Kanun uyarınca atamayı yapacak kuruma sağlanması hususunda adli sicil bilgisinin talep edilmesinin, Kanuna aykırılık teşkil etmediğinin değerlendirildiği,

- Diğer taraftan ilgili kişinin, 657 sayılı Devlet Memurları Kanunundaki koşulları taşıyıp taşımadığının araştırılması noktasında yeterli olduğu düşünülen adli sicil kaydının, bilgi ve belge talepli Kurum yazısına veri sorumlusu tarafından gönderilen cevap ve ekinde yer almadığının görüldüğü, bu itibarla, söz konusu mahkeme kararlarının; adli sicil kaydı istenmeksizin/verilmeksizin, doğrudan mahkeme kararlarının talep edilmesi/verilmesi şeklinde gerçekleştiği; bununla birlikte durumun ilgili kişinin bilgisi ve talebi doğrultusunda gerçekleşmesi sebebiyle, Kanunun yürürlüğe girdiği tarihten önce gerçekleşen söz konusu olgunun, olayın gerçekleştiği tarihte yürürlükte bulunan mevzuat bakımından hukuka aykırılık içermediğinin değerlendirildiği,

- Söz konusu kararların, güvenlik soruşturması işlemi neticesinde elde edilen (istihbari vb.) kararlar olmadığı, atama işlemlerinin gerçekleştirilmesini teminen ilgili kişi tarafından veri sorumlusuna sunulan evraklar arasında yer alması sebebiyle özlük dosyasına girdiğinin taraf beyanlarından anlaşıldığı,

- 657 sayılı Devlet Memurları Kanununun 109 uncu maddesinin dördüncü fıkrası gereğince özlük dosyalarının tutulma esasları ile özlük dosyalarında yer alacak belgelere ilişkin usul ve esasların Devlet Personel Başkanlığınca (DPB) belirlendiği, bu sebeple, konuya ilişkin olarak memurların ilk veya naklen atanmalarına ilişkin belgeler ile memurun adaylık ve asli memurluğa atanmasına ilişkin

belgelerin neler olduđu, kamu kurumlarının/kuruluşlarının memurlardan ilk işe başlamaları sırasında istedikleri bilgi ve belgelerin neler olduđu ile bu belgelerin her kurum/kuruluşta farklılık gösterip gösteremeyeceđi hususları ile “yargı organlarınca memur hakkında verilmiş karar örnekleri” ifadesinin yargı organlarınca memurun çalışma hayatına ilişkin verilmiş karar örneklerini mi yoksa memur hakkında verilmiş tüm karar örneklerini mi kastettiđi hususuna ilişkin olarak Kurumca, Devlet Personel Başkanlığından görüş talep edildiđi ve Devlet Personel Başkanlığının Kuruma gönderdiđi cevabi yazıda; 2 Seri No’lu Kamu Personeli Genel Tebliğinin “Özlük dosyalarının tutulma esasları ile özlük dosyalarında yer alacak belgelere ilişkin usul ve esaslar” başlıklı bölümüne ilişkin düzenlemelere yer verildikten sonra, “Mezkûr Tebliğde memurun özlük dosyasının sekiz bölümden oluştuđu belirtilmekte, bölümlerde hangi konulara ilişkin belgelerin yer alması gerektiđi hususu düzenlenmekte olup, özlük dosyasında yer alan her bir bölüme ilişkin belgelerin tek tek zikredilmesinin mümkün bulunmadıđı, kurumlarca lüzum görülen tüm belgelerin ilgili bölümlere konulmasının uygun olacađı, dosyanın dördüncü bölümünde memurun yalnızca çalışma hayatına ilişkin değil yargı organlarınca memur hakkında verilen tüm karar örneklerinin bulunması gerektiđi değerlendirilmektedir” denilmekle birlikte, bahsi geçen kişisel verinin Kanunun 6 ncı maddesi kapsamında özel nitelikli kişisel veri olması ve ilgili kişinin, şikâyet başvurusuna konu etmiş olduđu mahkeme kararlarının işlenmesine ilişkin olarak hâlihazırda açık rızasının bulunmaması hususları birlikte değerlendirildiğinde, söz konusu verilerin işlenmesinde Kanunun 6 ncı maddesinin üçüncü fıkrasında yer alan “...sağlık ve cinsel hayat dışındaki veriler, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebilir...” düzenlemesi uyarınca kişisel verinin işlenebilmesinde “kanunlarda öngörülme” prensibi doğrultusunda hareket edileceđi ve söz konusu ifadenin, “maddi kanun” biçiminde anlaşılması gerektiđi, bu doğrultuda, DPB’nin Kurum görüş talebine verdiđi cevap ve 2 Seri No’lu Kamu Personeli Genel Tebliđi hükümleri uyarınca sözü edilen kararların özlük dosyasından çıkarılmasına yer olmadıđının değerlendirildiđi,

• Diğer taraftan, Kanunun 7 nci maddesinde “(1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir. (2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır” hükümlerine yer verdiđi, konuya ilişkin olarak 657 sayılı Kanunun “Memur Bilgi Sistemi, Özlük Dosyası” başlıklı 109 uncu maddesinde her memur için bir özlük dosyasının tutulacađı ve bu dosyada memurun mesleki bilgileri, mal bildirimleri; varsa inceleme, soruşturma, denetim raporları, disiplin cezaları ile ödül ve başarı belgelerine ilişkin bilgi ve belgelerin konulacađı; özlük dosyalarının tutulma esasları ile özlük dosyalarında yer alacak belgelere ilişkin usul ve esasların Devlet Personel Başkanlığınca belirleneceđinin belirtildiđi; Kamu Personeli Genel Tebliğinin (Seri No:

2) "D" bölümünde ise özlük dosyasının sekiz bölümden oluştuğu ve bölümlerde yer alan konulara ilişkin bilgi ve belgelerin saklanacağı hükümlerine yer verildiği,

• Öte yandan, 16.05.1988 tarihli ve 19816 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren mülga "Devlet Arşiv Hizmetleri Hakkında Yönetmelik" in "Tarifler" başlıklı 3 üncü maddesinde "arşiv malzemesi" ve "arşivlik malzeme" kavramlarının;

"a) Arşiv malzemesi: Türk Devlet ve Millet hayatını ilgilendiren ve en son işlem tarihi üzerinden otuz yıl geçmiş veya üzerinden onbeş yıl geçtikten sonra kesin sonuca bağlanmış olup, birinci maddede belirtilen kuruluşların işlemleri sonucunda teşekkül eden ve onlar tarafından muhafazası gereken, Türk Milletinin geleceğine tarihi, siyasî, sosyal, hukukî ve teknik değer olarak intikal etmesi gereken belgeler ve Devlet hakları ile milletlerarası hakları belgelemeye, korumaya, bunlarla ilgili işlem ve münasebetler bakımından tarihî, hukukî, idarî, askeri, iktisadî, dinî, ilmî edebî estetik, kültürel biyografik, jeneolojik ve teknik herhangi bir konuyu aydınlatmaya, düzenlemeye, tespite yarayan, ayrıca ait olduğu devrin ahlâk, örf ve âdetlerini veya çeşitli sosyal özelliklerini belirten her türlü yazılı evrak, defter, resim, plan, harita, proje, mühür, damga, fotoğraf, film, ses ve görüntü bandı, baskı ve benzeri belgeleri ve malzemeyi,

*b) Arşivlik malzeme: Yukarıdaki bentte sayılan her türlü belge ve malzemedan zaman bakımından henüz arşiv malzemesi vasfını kazanmayanlarla, son işlem tarihi üzerinden **yüzbir yıl geçmemiş memuriyet sicil dosyaları**, Devletin gerçek ve tüzel kişilerle veya yabancı devlet ve milletlerarası kuruluşlarla akdettiği ikili ve çok taraflı milletlerarası antlaşmalar, tapu tahrir defterleri, tapu ve nüfus kayıtları, aynı özellikteki vakfiyelerden ait oldukları kamu kurum ve kuruluşları ile il, ilçe, köy ve belediyelere ait sınırlı kâğıtları gibi belgeleri, ..." ifade ettiğinin belirtildiği, bu kapsamda son işlem tarihi üzerinden yüz bir yıl geçmemiş olan memuriyet sicil dosyalarının, "arşivlik malzeme" olarak kabul edildiği ve yüz bir yıl boyunca saklandığı, ancak söz konusu düzenlemenin, 16.07.2018 tarihli ve 30480 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren 11 sayılı "Devlet Arşivleri Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi" ne dayalı olarak çıkarılan ve 18.10.2019 tarihli ve 30922 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren "Devlet Arşiv Hizmetleri Hakkında Yönetmelik" in 32 nci maddesi uyarınca yürürlükten kaldırıldığı, mülga yönetmelikte düzenlenen "arşiv malzemesi" ve "arşivlik malzeme" kavramları, Devlet Arşiv Hizmetleri Hakkında Yönetmelik'te "arşiv belgesi" ve "arşivlik belge" olarak düzenleme altına alındığı, mezkûr kavramların,*

"Tanımlar

MADDE 4- (1) Bu Yönetmelikte geçen;

b) Arşiv belgesi: Son işlem tarihi üzerinden yirmi yıl geçmiş veya on beş yıl geçtikten sonra kesin sonuca bağlanmış bulunan ve günlük iş akışı içinde işlevi bulunmayan, varsa tâbi olduğu diğer mevzuatlar ile saklama planlarındaki saklama sürelerini tamamlayan, üretim biçimleri, donanım ortamları ne şekilde olursa olsun geleceğe, tarihi, siyasi, sosyal, kültürel, hukuki, idari, askeri, iktisadi, dini, ilmi, edebi, estetik, biyografik, jeneolojik ve teknik herhangi bir değer olarak intikal etmesi gereken ve bir bilgiyi içeren yazılmış, çizilmiş, resmedilmiş, görüntülü, sesli veya elektronik ortamlarda üretilmiş belgeyi,

c) Arşivlik belge: Süre bakımından arşiv belgesi vasfını kazanmayan veya bu süreyi doldurmasına rağmen güncelliğini kaybetmeyen, hizmetin yürütülmesi açısından işlevi olan belgeyi, ...ifade eder”

şeklinde düzenlendiği, mülga Yönetmelikte arşivlik malzeme olarak kabul edilen memuriyet sicil dosyalarının, yeni Yönetmelik kapsamında arşivlik belge olarak değerlendirilmediği ve memuriyet sicil dosyalarına ve bunların yüz bir yıl saklanacağına ilişkin düzenlemeye yer verilmediği, buna karşın, süre bakımından arşiv belgesi vasfını kazanamayan belgelerin arşivlik belge kabul edilmesi sebebiyle memuriyet özlük dosyalarının da bu kapsamda yer aldığı ve bunların imha işlemine tabi tutulmadığı

değerlendirmelerinden hareketle;

- Şikâyete konu kişisel verinin özel nitelikli kişisel veri olduğu ve ilgili kişinin söz konusu mahkeme kararlarının özlük dosyasında yer almasına ilişkin hâlihazırda açık rızasının bulunmadığı; bununla birlikte, Kanun bakımından söz konusu kişisel verinin işlenmesine ilişkin “kanunilik” unsurunun öğretide ifade edilen “maddi kanun” olarak değerlendirilmesi gerektiği kanaatine varıldığından DPB’nin Kurum görüş talebine verdiği cevap ve 2 Seri No’lu Kamu Personeli Genel Tebliği hükümleri uyarınca mer’i mevzuat bakımından sözü edilen kararların özlük dosyasından çıkarılmasına yer olmadığına karar verilmiştir.

2020/379 sayılı KVKK Kararı

Bir tıp merkezinin internet sitesinde video tanıtım bölümü içerisinde görsel ve işitsel kişisel verileri işlenen ilgili kişinin başvurusuna veri sorumlusu tıp merkezi tarafından cevap verilmemesi hakkında Kişisel Verileri Koruma Kurulunun 14/05/2020 tarihli ve 2020/379 sayılı Karar Özeti

Karar Tarihi : 14.05.2020

Karar No : 2020/379

Konu Özeti : Bir Tıp Merkezinin internet sitesinde pazarlama amaçlı olarak "Video Tanıtım" bölümü içerisinde görsel ve işitsel kişisel verileri işlenen ilgili kişinin başvurusuna veri sorumlusu Tıp Merkezi tarafından cevap verilmemesi

İlgili kişiden alınan şikayet dilekçesinde özetle; bir Tıp Merkezinin internet sitesinde pazarlama amaçlı olarak "Video Tanıtım" bölümü içerisinde görsel ve işitsel kişisel verilerinin işlendiği, akdedilen iş sözleşmesi sona ermiş olduğundan kullanılan bu verilerin işleme amacı veya konusunun kalmadığı gerekçesiyle veri işlemenin durdurulmasını ve verilerin kaldırılmasını talep ettiğini, bu çerçevede veri sorumlusuna başvurduğu, bildirimde bulunmasına rağmen yasal sürede ilgili kişiye bilgi verilmediği, internet sitesindeki videoların silinmediği ifade edilerek veri sorumlusu Tıp Merkezine ait internet sitesinde bulunan kişisel verilerinin silinmesi ve başkaca işlenen kişisel verilerinin bulunup bulunmadığı, hangi verilerinin hangi amaçla işlendiği hususlarında tarafına bilgi verilmesi talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde savunmasının alınmasına yönelik Kurum yazısı veri sorumlusuna 01.08.2019 tarihinde tebliğ edilmiş ancak veri sorumlusu tarafından Kurula herhangi bir savunma ve bilgi/belge iletilmemiştir. İlgili kişinin başvurusunda belirtilen ve veri sorumlusuna ait internet sitesi adresine girildiğinde, veri sorumlusu Tıp Merkezinin kim tarafından kurulduğuna ilişkin bilgi ve Merkezi Sicil Kayıt Sisteminde kayıtlı bulunduğu tespit edilmiş olup, eldeki bilgi ve belgeler çerçevesinde yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 14/05/2020 tarih ve 2020/379 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) “Tanımlar” başlıklı 3 üncü maddesinin (1) numaralı fıkrasının (ç) bendinde ilgili kişinin, “kişisel verisi işlenen gerçek kişi”; (d) bendinde kişisel verinin, “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi”, (e) bendinde, kişisel verilerin işlenmesinin, “kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılma sı ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem”, (1) bendinde veri sorumlusunun ise, “kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi” olarak tanımlandığı,
- Bu çerçevede şikâyete konu olayda, ilgili kişiye ait görüntülerin kişisel veri niteliğinde olduğu, şikâyet başvurusunda bulunanın gerçek kişi olması nedeniyle ilgili kişi sıfatını haiz olduğu, kişisel verilerin hangi amaçla ve araçla işleneceğini belirleyip veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olduğu için Tıp Merkezinin veri sorumlusu olduğu, veri sorumlusu tarafından reklam yapmak amacıyla ilgili kişinin görüntülerinin kullanılmasının kişisel veri işleme faaliyeti olduğu ,
- Kanunun “Veri Sorumlusuna Başvuru” başlıklı 13 üncü maddesinin (2) numaralı fıkrasında yer alan “Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır.” hükmü ile “Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ” gereği; ilgili kişinin veri sorumlusuna başvurduğu, başvurusunda veri sorumlusu tarafından kişisel verilerinin, işleme amacı veya konusu kalmadığından silinmesi ve ilgili kişinin başkaca işlenen kişisel verilerinin bulunup bulunmadığı, hangi verilerinin hangi amaçla işlendiği hususlarında tarafına bilgi verilmesinin talep edildiği, ilgili kişinin, başvurusunun veri sorumlusuna tebliğ edildiği 15.01.2019 tarihi itibarıyla 30 günlük yasal süre içerisinde veri sorumlusundan herhangi bir cevap alamadığının anlaşıldığı, bu nedenle veri sorumlusu tarafından ilgili kişinin başvurusunu cevaplama yükümlülüğünün yerine getirilmediği,
- Öte yandan Kurulun savunma, bilgi/belge talebini içeren resmi yazısının veri sorumlusuna 01.08.2019 tarihinde tebliğ edilmesine rağmen söz konusu tarih itibarıyla veri sorumlusu tarafından Kurula herhangi bir savunma ve bilgi/belge iletilmediği,
- Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinde;

“(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işleniminin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.” hükmünün yer aldığı,

• Kanunun “Veri Güvenliğine İlişkin Yükümlülükler” başlıklı 12 nci maddesinin (1) numaralı fıkrasında “Veri sorumlusu; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.” hükmüne yer verildiği,

• Kanunun “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi” başlıklı 7 nci maddesinin (1) numaralı fıkrasında yer alan “Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.” hükmü gereği veri sorumlusu tarafından ilgili kişiye ait kişisel verilerin işlenmesini gerektiren herhangi bir sebebin bulunmaması halinde ilgili kişinin başvurusunda belirttiği talep doğrultusunda tüm kişisel verilerinin silinmesi veya yok edilmesi gerektiği

değerlendirmelerinden hareketle;

• Kanunun 11 inci maddesi uyarınca, ilgili kişinin tüm kişisel verilerinin silinmesi veya yok edilmesi talebinin, işlenmesini gerektiren sebep ortadan kalktığı halde; Kanunun 7 nci maddesinin (1) numaralı fıkrası gereği veri sorumlusu tarafından yerine getirilmediği, kişinin silme talebinin üzerinden makul süre geçmesine rağmen söz konusu kişisel veri işleme faaliyetine Kanunun 5 inci maddesinde yer alan şartlarından herhangi birine dayanmaksızın devam edildiği, bu durumun ise Kanuna aykırılık teşkil ettiği, bu kapsamda Kanunun 12 nci maddesinin (1) numaralı fıkrası hükümleri gereğince, kişisel verilerin hukuka aykırı işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı kanaatine varılan veri

sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 75.000 TL idari para cezası uygulanmasına,

- Kanunun 7 nci maddesinin (1) numaralı fıkrası uyarınca ilgili kişinin talebi doğrultusunda işlenmesini gerektiren herhangi bir sebep bulunmaması durumunda veri sorumlusu tarafından ilgili kişiye ait işlenen tüm kişisel verilerin silinmesi veya yok edilmesi ve tevsik edici belgelerin ilgili kişiye ve Kurula gönderilmesi hususunda veri sorumlusunun talimatlandırılmasına,

- Kanunun 13 üncü maddesi kapsamında başvuruda bulunan ilgili kişilere cevap verilmesine ilişkin gerekli özeni göstermesi hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2020/359 sayılı KVKK Kararı

Bir bankanın veri ihlali bildirimini hakkında Kişisel Verileri Koruma Kurulunun 07/05/2020 tarih ve 2020/359 sayılı Karar Özeti

Karar Tarihi : 07.05.2020

Karar No : 2020/359

Konu Özeti : Bir bankanın veri ihlali bildirimini hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlali bildiriminde;

- İhlalin; KKB ekranında, Veri Sorumlusu Banka'nın eski çalışanınun işin gereğinden fazla adette sorgulama yapılması ile gerçekleştiği, çalışanın ifadesine göre; T.C. kimlik numaraları Banka dışından 3. şahıs tarafından iletilip kişilerin kredi skorlarının öğrenilmek istenildiği,
- İhlalin yıllık periyotlarla hazırlanan kontroller neticesinde veri ihlalinin gerçekleştiren çalışanın işin gereğinden fazla adette sorgulama yaptığının fark edilmesi üzerine hazırlanan Teftiş Raporu ile; çalışanın KKB sorgulamalarını ilgili kişilerin gıyabında gerçekleştirdiği, KKB sorgulamalarını gerçekleştirdiği esnada cep telefonu ile ilgilendiği ve KKB sorgulamalarını yaptıktan hemen sonra bir kağıda not aldığı, bazı tarihlerde bu kağıdın fotoğrafını çektiği ve/veya cep telefonu ile yazıştığının tespit edilmesiyle anlaşıldığı,
- İhlalin Temmuz 2018 ile Mayıs 2019 tarihleri arasında gerçekleştiği,
- İhlalden veri sorumlusunun müşterisi olan ve müşterisi olmayan toplam 5695 kişinin etkilendiği,
- İhlalden etkilenen kişisel verilerin, şahısların bankalardan kullanmış oldukları tüm kredili ürünlere ilişkin geçmişleri, ödeme performansları ve borç rakamları, adres, telefon vb. olduğu ifadelerine yer verilmiştir.

- Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 07/05/2020 tarih ve 2020/359 sayılı Kararı ile;
- 7305 adet KKB sorgulaması yapıldığı, bu sorgularda 5889 adet TC kimlik numarası sorguladığı, (mükerrer olanlar elendikten sonra 5695) bu TC kimlik numaralarının 3038'inin Banka müşterilerine ait olduğu, 2851'inin Banka müşterisi olmadığı,

• Veri ihlalinin Temmuz 2018 ile Mayıs 2019 arasında gerçekleştiği, ihlalin anlaşılmasını sağlayan KKB sorgulama sayısının tespit edilmesine yönelik kontrolün yıllık periyotlarla yapılıyor olması nedeniyle ihlalin 1 yıla yakın süre boyunca devam ettiği ve ancak 18 Temmuz 2019 tarihinde tespit edilebildiği hususlarının, “Kişisel Veri Güvenliği Rehberi”nin (Teknik ve İdari Tedbirler-Rehber) “*Kişisel Veri Güvenliğinin Takibi*” başlığı altında yer alan “*Veri sorumlularının sistemleri çoğunlukla hem içeriden hem de dışarıdan gelen saldırılar ve siber suçlara veya kötü amaçlı yazılımlara maruz kalmakta olup çeşitli belirtilere rağmen bu durum uzun süre fark edilememekte ve müdahale için geç kalınabilmektedir. Bu durumun önüne geçebilmek için; a) Bilişim ağlarında hangi yazılım ve servislerin çalıştığına kontrol edilmesi, b) Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi, c) Tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması (log kayıtları gibi), ç) Güvenlik sorunlarının mümkün olduğunca hızlı bir şekilde raporlanması, d) Çalışanların sistem ve servislerdeki güvenlik zaaflıklarını ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulması, gerekmektedir.*”, ifadelerine aykırı olarak veri sorumlusu tarafından kişisel verilerin korunmasına ilişkin kişisel veri güvenliği takibinin uygun zaman aralıklarıyla yapılmadığının göstergesi olduğu,

• Veri sorumlusu tarafından ihlal öncesi yapılması gereken; kullanıcı bazında log kayıtlarında yetki sınırlaması, ekranların gereksiz rollere kapatılması, kişisel verilerin korunması ile ilgili uyarı metnine yer verilmesi gibi kullanıcı yetki ve rollerine yönelik kontrollerin ve düzenlemelerin ihlal sonrasında gerçekleştirilmiş olmasının Rehber’in “*Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması*” başlığı altında “*Kişisel veriler elektronik ortamda ise, kişisel veri güvenliği ihlalinin önlemek için ağ bileşenleri arasında erişim sınırlandırılabilir veya bileşenlerin ayrılması sağlanabilir. Örneğin kullanılmakta olan ağın sadece bu amaçla ayrılmış olan belirli bir bölümüyle sınırlandırılarak bu alanda kişisel verilerin işleniyor olması halinde, mevcut kaynaklar tüm ağ için değil de sadece bu sınırlı alanın güvenliğini sağlamak amacıyla ayrılabilir.*”, ifadelerine aykırı olarak ilgili teknik ve idari tedbirlerin ihlalin öncesinde yeterince alınmadığının göstergesi olduğu,

• Veri ihlalden önce sorgulanabilecek kişi sayısının sınırlandırılmamış olduğu ve ancak ihlalin gerçekleşmesinden sonra 250 üzerinde sorgulama yapan kullanıcıların kamera kayıtları incelenerek veri ihlali oluşturacak bir durum olup olmadığının kontrol edildiği hususunun, Rehber’in “*Mevcut Risk ve Tehditlerin Belirlenmesi*” başlığı altında yer alan “*Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir. Bu riskler belirlenirken; - Kişisel verilerin özel nitelikli kişisel veri olup olmadığı, - Mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği, - Güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği dikkate alınmalıdır.*”

Bu risklerin tanımlanması ve önceliğinin belirlenmesinden sonra; söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmeli, gerekli teknik ve idari tedbirler planlanarak uygulamaya konulmalıdır.”, ifadelerine aykırı sorgulamada sınırlama (kota) bulunmamasından kaynaklandığı,

- Veri sorumlusuna ait çalışanlar için veri güvenliği ve Kişisel Verilerin Korunması Kanunu konusunda belli aralıklarla eğitim ve farkındalık çalışmalarının yapıldığı, çalışanların %86’sının konuyla ilgili bilgilendirme eğitimini tamamladığı, kalan kişilere ise eğitimin tekrar iletildiği ifade edildiği ancak bu hususta tevsik edici belge gönderilmediği hususlarının, Kişisel Verilerin Korunması Kanununun 2016 yılında kabul edildiği, Rehber’in 2018 yılının ocak ayında yayımlanmış olduğu ve “Çalışanların Eğitilmesi ve Farkındalık Çalışmaları” başlığının altında; “...çalışanların, kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi konular hakkında eğitim almaları, çalışanlara yönelik farkındalık çalışmaları yapılması ve güvenlik risklerinin belirlenebildiği bir ortam oluşturulması kişisel veri güvenliğinin sağlanması bakımından çok önemlidir. Veri sorumlusu nezdinde çalışan herkesin hangi konumda çalıştığına bakılmaksızın kişisel veri güvenliğine ilişkin rol ve sorumlulukları, görev tanımlarında belirlenmeli ve çalışanların bu konudaki rol ve sorumluluğunun farkında olması sağlanmalıdır.”, ifadelerine aykırı olarak gerçekleşen çalışanlara eğitim verilmesinin halen sağlanmadığı

hususları dikkate alındığında, Kanun’un 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 400.000 TL,

- 18.07.2019 tarihinde tespit edilmiş olan ihlalin 31.07.2019 tarihinde Kurula bildirildiği, geç bildirim sebebi olarak belirtilen Teftiş Raporunda yer alan bilgilerin hangilerinin paylaşıldığının net olmadığı ifade edilmesi, eldeki delillerin yetersizliği, olayın mahiyetinden emin olunmaması, müşteri şikayeti olmaması, dışarıdan gelen T.C. Kimlik numaralarına istinaden bu durumun ortaya çıkması gibi sebeplerle, bildirim gerekip gerekmediğinin kurum içinde değerlendirilmesi ve tüm ilgili ünitelerden görüş alınmasından kaynaklandığı sebebinin, 24.01.2019 Tarih ve 2019/10 sayılı Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kurul Kararı’nda yer alan “...Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bu bilgilerin gecikmeye mahal verilmeksizin aşamalı olarak sağlanmasına...” ifadeleri göz önünde bulundurulduğunda ilgili sebeplerin Kurula geç bildirimde bulunulması için geçerli bir mazeret niteliği taşımadığı,

- Veri ihlalden etkilenen 5695 kişi arasında sadece Bankada iletişim bilgileri bulunanlara veri ihlal bildiriminde bulunulduğu, bu kapsamda ilgili kişilerin tamamına bildirimde bulunmak adına makul çaba sarf edilmediği ve Kurumumuz tarafından talep edilmesine rağmen ihlalin bildirildiği kişi

sayısının ve bu kişilerin Banka müşterisi olup olmadığına hususlarına dair Kurumumuza bilgi verilmediği

hususları dikkate alındığında; Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen “en kısa sürede” (Kurul’a bildirim için 72 saat) bildirimde bulunma yükümlülüğüne aykırı davranan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 50.000 TL

olmak üzere toplam 450.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2020/357 sayılı KVKK Kararı

Bir sigorta şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 07/05/2020 tarih ve 2020/357 sayılı Karar Özeti

Karar Tarihi : 07.05.2020

Karar No : 2020/357

Konu Özeti : Bir sigorta şirketinin veri ihlal bildirimini hakkında karar

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Veri sorumlusunun Çağrı Merkezi Birimi tarafından Teftiş Kuruluna; Çağrı Merkezi Satış Temsilcisi olarak dış kaynak sözleşmesi çerçevesinde çalışmakta olan bir çalışanın veri sorumlusunun ana sigortacılık (Cool:Gen) ekranları vasıtasıyla müşterilerin poliçe bilgilerini, portföy takibi için kullandığı yönündeki tereddütlerin iletilmesi üzerine, Teftiş Kurulu Başkanlığınca inceleme yapılmasına karar verilmiş olduğu, bu çalışma çerçevesinde elde edilen bulgular neticesinde ihlalin gerçekleştiğinin anlaşıldığı,
- Veri sorumlusunun yapmış olduğu Teftiş Kurulu incelemesi neticesinde; sistemlerinde tutulmakta olan isim-soyisim, iletişim, plaka bilgilerinin yer aldığı listeyi taşeron çalışanın kendisine atanan kurum e-posta adresinden şahsi e-posta adresine 22.10.2019 ve 24.10.2019 tarihlerinde göndermesi sonucu veri ihlali gerçekleştiğinin tespit edildiği,
- İhlalden etkilenen kişi ve kayıt sayısının 91 olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin müşterilere ait kimlik, iletişim ve risk yönetimi bilgisi (poliçe süreçleri kapsamında elde edilen plaka bilgisi) olduğu,
- Veri sorumlusu nezdinde kullanılan veri sızıntısı önleme uygulamasının, belirli anahtar kelimeleri yakalamak üzere kurgulandığı ancak veri sızıntısına konu olan ihlal, bu anahtar kelimeleri içermediğinden herhangi bir uyarının oluşmadığı,
- Veri ihlal bildirimini yapıldığı tarih itibarıyla ihlal ile ilgili olan çalışanların tamamının kişisel veri koruma eğitimi almadığı, ancak çalışan/taşeron çalışan sayısının fazla olması ve şirketin iş faaliyetlerindeki yoğunluk nedeniyle ve ilgili eğitimler kapsamında azami faydayı sağlayabilmek

adına eğitimlerin tek bir seferde tüm çalışanlara bir arada değil de farklı gruplar halinde verilecek şekilde planlandığı, bu nedenle, ilgili sürecin veri sorumlusu çalışanlarının %92'si için tamamlanmış olduğu ve geriye kalan %8 için devam etmekte olduğu

ifadelerine yer verilmiştir.

Söz konusu bildirim incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 07/05/2020 tarih ve 2020/357 sayılı Kararı ile;

- Veri sorumlusunun sisteminde tutulmakta olan 91 müşteriye ait isim-soyisim, iletişim, plaka bilgilerinin yer aldığı listeyi taşeron çalışanın kendisine atanan kurum e-posta adresinden şahsi e-posta adresine 22.10.2019 ve 24.10.2019 tarihlerinde göndermesi sonucu veri ihlali gerçekleştiği,
- İhlal kapsamında etkilenen kişisel verilerin veri sızıntısı önleme uygulamasında yakalanmak üzere kurgulanmadığı ve bu sebeple ihlale konu olan e-posta iletiminin anahtar kelimeleri içermediğinden herhangi bir uyarının oluşmadığı, ihlal konusu olan kişisel verilerin veri sızıntısı önleme uygulamasında tanımlanabilir kişisel veriler olduğu dikkate alındığında bu durumun kişisel veri güvenliğine ilişkin doğru ve tutarlı bir prosedürün, veri sorumlusunun çalışma ve işleyişine uygun şekilde entegre edilmediğinin göstergesi olduğu,
- Teftiş Kuruluna; veri sorumlusunun ana sigortacılık ekranlarını kullanarak müşterilerin poliçe bilgilerini portföy takibi için kullanıldığı yönündeki tereddütlerin iletilmesi üzerine yapılan inceleme ile veri ihlalinin, gerçekleşmesinden yaklaşık iki ay sonra ancak tespit edilebildiği ve söz konusu tereddütlerin Teftiş Kuruluna bildirilmemesi durumunda veya tereddütlerin oluşmaması durumunda veri ihlalinin tespit edilemeyeceğinin anlaşıldığı dikkate alındığında alınacak tedbirlerin önceden belirlendiği iyi bir olay yönetiminin kurgulanmadığı ve bu nedenle veri sorumlusunun, Kurumumuzun yayınlamış olduğu "Kişisel Veri Güvenliği Rehberi"nde de belirtildiği üzere bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının takip edilmesi noktasında alınan teknik tedbirler açısından yetersiz kaldığı,
- Veri ihlali öncesinde veri ihlali ile ilgili çalışanların tamamının kişisel veri koruma eğitimi almadığı ve ihlali gerçekleştiren çalışan için de bu eğitiminin atanmış olduğu ancak almadığı dikkate alındığında bu durumun veri sorumlusu Şirketin kişisel veri güvenliğinin sağlanması bakımından yeterli idari tedbirleri almadığının göstergesi olduğu

değerlendirmelerinden hareketle 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik

tedbirleri almayan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 90.000 TL idari para cezası uygulanmasına,

- Kurulun 24.01.2019 tarih ve 2019/10 sayılı Kararı ile belirlenen veri ihlalinin öğrenilmesinden itibaren başlayan 72 saatlik süre içerisinde veri sorumlusunun Kurumumuza bildirimde bulunduğu, öte yandan ilgili kişilere gerekli bildirimlerin yapıldığı ve söz konusu bildirim örneklerinin Kurumumuza gönderildiği

dikkate alındığında veri sorumlusu hakkında Kanunun 12 nci maddesinin (5) numaralı fıkrası yapılacak bir işlem bulunmadığına

karar verilmiştir.

2020/355 sayılı KVKK Kararı

İlgili kişiye ait Medula Eczane çıktılarının eczacının eşi tarafından kullanılması hakkında Kişisel Verileri Koruma Kurulunun 07/05/2020 Tarihli ve 2020/355 Sayılı Karar Özeti

Karar Tarihi : 07.05.2020

Karar No : 2020/355

Konu Özeti : İlgili kişiye ait Medula Eczane çıktılarının eczacının eşi tarafından kullanılması suretiyle İl Sağlık Müdürlüğüne dilekçe sunulması hususunda Kuruma intikal eden ihbar başvurusu

İl Sağlık Müdürlüğü tarafından Kişisel Verileri Koruma Kurumuna yapılmış olan ihbarda özetle;

- İl Sağlık Müdürlüğüne verilen bir dilekçede, dilekçe sahibinin *“bir eczacının sağlık problemleri nedeniyle bu mesleği icra edecek bilgi, beceri yeteneğine sahip bulunmadığı, bu nedenle yeni adresinde eczane açılmasına izin verilmemesinin halk sağlığı açısından da yararlı olacağı”* hususlarını beyan ederek dilekçe ekinde de şikayet ettiği eczacı adına tanı ve ilaç bilgilerinin bulunduğu Medula Eczane çıktılarına yer verdiği,

- Dilekçe sahibinin eşinin eczacı olduğu göz önünde bulundurulduğunda, ilgili kişiye ait Medula Eczane çıktılarına eşinin eczanesinden ulaşılmış olacağı güçlü bir ihtimal olduğundan veri sorumlusu konumunda bulunan eczane hakkında 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gerekli değerlendirmenin yapılmasını teminen konunun Kişisel Verileri Koruma Kurumuna bildirilmesinin mütalaa edildiği

belirtilmiştir.

İlgili kişiye ait Medula Eczane çıktıların, dilekçe sahibinin eşinin eczanesinden alınarak kullanılması hakkındaki ihbar başvurusunun incelenmesi neticesinde

- İhbara konu olan Medula Sisteminin, Sağlık Hizmeti Sunucularının Faturalarının İncelenmesine ve Bedellerinin Ödenmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik’te sağlık hizmeti kullanım verisi toplamak ve bu verilere dayanarak faturalama işlemini gerçekleştirmek amacıyla Sosyal Güvenlik Kurumu (SGK) tarafından uygulanan ve işletilen elektronik bilgi sistemi olarak tanımlandığı,

- Medula Eczanenin ise, Genel Sağlık Sigortası hak sahiplerinin SGK ile sözleşmeli eczanelerden almış oldukları ilaçlara ait reçete bilgilerinin SGK tarafından belirlenmiş kurallara uygunluğunu on-line olarak denetleyerek elektronik ortamda kayda alınmasını ve faturalanmasını sağlayan bir bilgi teknolojileri servisi olduğu,

- SGK ile sözleşmeli olan eczanelerin bu sistemi kullanmaya yetkili olduğu, kişilerin T.C. kimlik numaraları ile sisteme giriş yaparak kişilere ait hem kişisel verilere hem de özel nitelikli kişisel verilere erişebildikleri göz önünde bulundurulduğunda eczacıların Medula sistemi kapsamında veri işleme faaliyetinde bulunabildikleri

değerlendirilmiş, Sosyal Güvenlik Kurumu'ndan alınan bilgiler doğrultusunda ise ihbara konu Medula Eczane çıktılarının şikayet sahibinin eşinin eczanesinden alındığı tespit edilmiş olup, Kurulun 07/05/2020 tarihli ve 2020/355 sayılı Kararı ile;

Kanunun 4 üncü maddesinin (2) numaralı fıkrasında kişisel verilerin işlenmesinde uyulması zorunlu ilkelerin "a) hukuka ve dürüstlük kurallarına uygun olma, b) doğru ve gerektiğinde güncel olma, c) belirli, açık ve meşru amaçlar için işleme, ç) işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, d) ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" şeklinde düzenlendiği,

Kanunun "Kişisel Verilerin İşlenme Şartları" başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise Kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı

Kanunun 6 ncı maddesinin (2) numaralı fıkrasında özel nitelikli kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (3) numaralı fıkrasında "Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması,

koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.” hükümlerinin düzenlendiği,

Öte yandan, Kanunun “Veri Güvenliğine İlişkin Yükümlülükler” başlıklı 12 nci maddesinin (1) numaralı fıkrasında veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğunun hükme bağlandığı dikkate alınarak;

- Dilekçe sahibinin İl Sağlık Müdürlüğünü muhatap dilekçesi eki Medula Eczane çıktılarını eşinin eczanesinden temin ettiği dikkate alındığında Eczanenin SGK ile yaptığı sözleşme çerçevesinde kullandığı Medula sistemine üçüncü kişilerin erişimini önlemek üzere gerekli güvenlik tedbirlerini almadığı dolayısıyla Eczane hakkında Kanunun 12 nci maddesinin (1) numaralı fıkrasına muhalefet etmesi nedeniyle Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 60.000 TL idari para cezası uygulanmasına,

- İl Sağlık Müdürlüğüne yaptığı başvurusunda ilgili kişiye ait Medula eczane çıktılarına yer veren eczacının eşi hakkında ise ilgili kişiye ait verileri ele geçirerek kullanması sebebiyle Türk Ceza Kanununun 136 ncı maddesinde belirtilen “Verileri hukuka aykırı olarak verme veya ele geçirme” suçunun oluştuğu kanaatine varıldığından bu kişi hakkında savcılığa ihbaren bildirimde bulunulmasına

karar verilmiştir.

2020/345 sayılı KVKK Kararı

Bilgisayar oyunları alanında faaliyet gösteren veri sorumlusunun veri ihlali bildirimini hakkında Kişisel Verileri Koruma Kurulunun 05/05/2020 tarih ve 2020/345 sayılı Karar Özeti

Karar Tarihi : 05.05.2020

Karar No : 2020/345

Konu Özeti : Bilgisayar oyunları alanında faaliyet gösteren veri sorumlusunun veri ihlali bildirimini hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlali bildiriminde;

- Yapılan rutin güvenlik denetimi sırasında eski bir veri sorumlusu çalışanı (web geliştiricisi) tarafından içerisinde kaynak kod ile veri dosyaları içeren bir klasörün yetkisiz olarak github.com internet sitesine yüklendiğinin tespit edildiği ve konu hakkında inceleme başlatıldığı,
- Yapılan incelemede klasör içerisinde yer alan birçok dosyada veri sorumlusu kullanıcılarının bir alt kümesinin kimliğini belirli kılabeleden bilgilerinin bulunabileceği tespit edilmiş olsa da, bu verilerin büyük bir kısmının veri sorumlusu hizmetlerinden men edilmiş sahte(bot) hesaplara ait olduğunun görüldüğü,
- İncelemenin detaylandırılmasından sonra 12 Ocak 2019 tarihinde verilerin hem sahte(bot) hesaplara hem de Türkiye’de mukim kullanıcılara ait gerçek hesapların birleşiminden oluştuğunun kesinleştiği,
- Yapılan çalışmalar sonucunda bilindiği kadarıyla söz konusu verilerin github’dan kaldırıldığı veya kamu erişimine kapalı hale getirildiği,
- İhlalden etkilenen kişi sayısının 62 olduğu,
- İhlalden kullanıcılar, müşteriler ve potansiyel müşteriler ile çocukların etkilendiği, ihlalden etkilenenlerin tamamına yakınının yetişkin olmakla birlikte az sayıda çocuğun da içlerinde yer aldığı,
- İhlalden etkilenen kişisel verilerin kimlik(doğum tarihi), iletişim(e-posta adresi), lokasyon(internet hizmet sağlayıcı ve kullanıcı kayıt tarihi ve saati) gibi bilgilerin olduğu

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 05/05/2020 tarih ve 2020/345 sayılı Kararı ile;

- Veri ihlalinin, veri sorumlusu ve eski bir çalışanı ile iş ilişkisinin sonlanmasının akabinde, bu kişinin yetkisiz bir biçimde kişinin işinin ürünü olan kaynak kodu ve veri dosyalarını içeren klasörü github.com'a (GitHub) yüklemesi ile gerçekleştiği, eski çalışanın kaynak kodları da github.com internet sitesine yüklemiş olmasının bir güvenlik açığı olduğu, bu kaynak kodların yetkisiz üçüncü kişiler tarafından analiz edilerek başka güvenlik açıklıklarına sebebiyet verebileceği dikkate alındığında kişisel veri güvenliği noktasında veri sorumlusu tarafından gerekli teknik ve idari tedbirlerin yeterince alınmamış olduğunun ve Kişisel Verileri Koruma Kurumunca yayınlanan Kişisel Veri Güvenliği Rehberinin(Teknik ve İdari Tedbirler) 2.2. numaralı "Çalışanların Eğitilmesi ve Farkındalık Çalışmaları" başlığı altında "...çalışanların, kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi konular hakkında eğitim almaları, çalışanlara yönelik farkındalık çalışmaları yapılması ve güvenlik risklerinin belirlenebildiği bir ortam oluşturulması kişisel veri güvenliğinin sağlanması bakımından çok önemlidir. Veri sorumlusu nezdinde çalışan herkesin hangi konumda çalıştığına bakılmaksızın kişisel veri güvenliğine ilişkin rol ve sorumlulukları, görev tanımlarında belirlenmeli ve çalışanların bu konudaki rol ve sorumluluğunun farkında olması sağlanmalıdır. Ayrıca kişisel veri içeren ortamlara erişim hakkı verilirken veya bu konuda kurum kültürü oluşturulurken "Yasaklanmadıkça Her Şey Serbesttir" prensibi değil, "İzin Verilmedikçe Her Şey Yasaktır" prensibine uygun hareket edilmesine dikkat edilmelidir." şeklinde açıklanan hususlara uygun davranmadığının göstergesi olduğu,

- İhlalin gerçekleşme tarihinin 19.04.2017, tespit tarihinin 09.01.2019, Kuruma bildirim tarihinin ise 28.02.2019 tarihi olduğu, aradan 2 yıla yakın süre geçtikten sonra 09.01.2019 tarihinde ihlalin tespit edilmesinin güvenlik kontrollerinin düzenli olarak yapılmadığının, dolayısıyla kişisel veri güvenliği takibi açısından veri sorumlusunun almış olduğu teknik ve idari tedbirlerin yetersiz kaldığının göstergesi olduğu,

- Personele veri sorumlusunun çok sayıda politikasının imzalatıldığının veri sorumlusu tarafından beyan edilmiş olmasına rağmen söz konusu çalışanın kişisel verileri de içeren dosyaları kendi taşınabilir depolama aygıtına kopyalamasının politikaların etkin şekilde uygulanmadığı ve farkındalık konusunda yeterli etkiyi sağlamadığının göstergesi olduğu

hususları dikkate alındığında, 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (1) numaralı fıkrası kapsamında veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL,

- 19.04.2017’de gerekleŒen veri ihlalinin 09.01.2019 tarihinde tespit edildiđi, Kuruma 28.02.2019 tarihinde bildirim yapıldıđı hususları dikkate alındıđında, veri sorumlusunun Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen “en kısa surede” bildirimde bulunma yukumlulne aykırılık teŒkil etmesi nedeniyle Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca veri sorumlusu hakkında 30.000 TL

olmak zere toplam 130.000 TL idari para cezası uygulanmasına

karar verilmiŒtir.

2020/344 sayılı KVKK Kararı

Bir bankanın veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 05.05.2020 tarih ve 2020/344 sayılı Karar Özeti

Karar Tarihi : 05.05.2020

Karar No : 2020/344

Konu Özeti : Bir bankanın veri ihlali hakkında Karar

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Bankanın Uyum ve İç Kontrol Grubu tarafından düzenli gerçekleştirilen iç kontrol faaliyetleri kapsamında, 2 ayrı şubesinde toplam 3 personel tarafından, Türkiye Bankalar Birliği Risk Merkezince Bankaya sağlanan bireysel nitelikteki kredi bilgilerini içeren KKB sorgu ekranlarından şüpheli sorgulamaların yapıldığının gözlemlendiği,
- Bu işlemlerin detaylı incelenmesi talebiyle konunun Teftiş Kurulu Başkanlığına ihbar edildiği,
- Teftiş Kurulu soruşturması sonucunda; Bireysel Müşteri ilişkileri Yöneticisi, Bireysel Müşteri İlişkileri Yönetici Yardımcısı, İşletme Müşteri İlişkileri Yönetici Yardımcısı unvanlarında çalışan ve olaya sebep olan 3 personelin görev ve iş tanımları gereği KKB sorgulama ekranına yetkileri bulunduğu, ancak söz konusu 3 personelin kendilerine tanımlanan KKB sorgulama yetkilerini Bankanın erişim ve bilgi güvenliği politikalarına aykırı şekilde amacı dışında kullandığı,
- Banka müşterisi olmayan toplam 7.706 kişinin bireysel nitelikteki kredi bilgilerine hukuka aykırı erişildiği,
- 3 personelin söz konusu sorgulamalara konu olan kişilerin TCKN'lerini şahsi telefonları üzerinden üçüncü kişi/kişilerden temin ettikleri, personelin söz konusu verileri bankanın sistemlerini kullanarak aktardığına ilişkin bir bulgu olmadığı ancak şahsi telefonları üzerinden elektronik haberleşme programları kullanarak Banka dışına aktarmış olabileceği

ifadelerine yer verildiğinden hareketle yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 05.05.2020 tarih ve 2020/344 sayılı Kararı ile;

- İhlalden 25.288 kişinin etkilendiği, etkilenen kişilerden 17.582'sinin Banka müşterisi olduğu, 7.706 kişinin Banka müşterisi olmadığı dikkate alındığında özellikle Banka müşterisi olmayan kişilere ait KKB sorgulamaları için Banka tarafından zamanında gerekli teknik ve idari tedbirlerin alınmadığının değerlendirildiği,

- Kişisel Veri Güvenliği Rehberinde teknik tedbirler arasında yer alan "Kişisel Veri Güvenliğinin Takibi" başlığı altında belirtilen hususların aksine, Bankanın şubelerinden birinde ihlale sebep olan personelin ihlal fiillerinin 10.07.2017 tarihinde başlamasına rağmen; bu ihlal fiilinin 08.07.2019 tarihinde tespit edildiği; benzer şekilde Bankanın başka bir şubesindeki ihlal fiillerinin başlangıç tarihleriyle tespit tarihleri arasında 18 ay gibi oldukça uzun bir süre bulunduğu, bu durumun kişisel veri güvenliği takibi noktasında veri sorumlusu tarafından güvenlik yazılımı mesajlarının, erişim kontrolü kayıtlarının ve diğer raporlama araçlarının düzenli olarak kontrol edilmediğinin göstergesi olduğu,

- Kişisel Veri Güvenliği Rehberinde idari tedbirler arasında yer alan "Çalışanların Eğitilmesi ve Farkındalık Çalışmaları" başlığı altında ifade edilen, veri sorumlusu nezdinde çalışan herkesin hangi konumda çalıştığına bakılmaksızın kişisel veri güvenliğine ilişkin rol ve sorumluluklarının, görev tanımlarında belirlenmesi ve çalışanların bu konudaki rol ve sorumluluğunun farkında olmasının sağlanması gerektiği, ancak bunun veri sorumlusu tarafından sağlanmadığının görüldüğü,

- Veri sorumlusu tarafından ihlal öncesi yapılması gereken kullanıcı yetki ve rollerine yönelik kontrollerin ve düzenlemelerin ihlal sonrasında gerçekleştirilmiş olmasının gerekli idari tedbirlerin zamanında alınmadığının göstergesi olduğu,

- Veri sorumlusu tarafından ihlal öncesi yapılması gereken KKB sorgulama limitlendirilmesi gibi kritik önemi haiz tedbirlerin ihlal sonrasında gerçekleştirilmiş olmasının gerekli teknik tedbirlerin yeterince alınmadığının göstergesi olduğu

dikkate alınarak, Kanunun 12 nci maddesinin (1) numaralı fıkrasına uygun olarak gerekli teknik ve idari tedbirleri almadığı kanaatine varılan veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 1.000.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2020/335 sayılı KVKK Kararı

İlgili kişinin araç kiralama hizmeti alması esnasında kişisel verilerinin işlenmesine dair açık rıza vermemesi üzerine kiralama hizmetinden yararlandırılmamasına ilişkin Kişisel Verileri Koruma Kurulu'nun 05/05/2020 tarihli ve 2020/335 sayılı Karar Özeti

Karar Tarihi : 05.05.2020

Karar No : 2020/335

Konu Özeti : İlgili kişinin araç kiralama hizmeti alması esnasında kişisel verilerinin işlenmesine dair açık rıza vermemesi üzerine kiralama hizmetinden yararlandırılmaması hakkındaki şikayeti

İlgili kişiden alınan 25/05/2018 tarihli şikâyet dilekçesinde özetle; veri sorumlusu araç kiralama şirketinin hizmet noktasında, yetkilisi olduğu şirket adına kısa süreli araç kiralamak istediği, araç kiralama sözleşmesi ve ilgili belgelerin yetkili tarafından imzalanmasının talep edildiği, imzalanması talep edilen evrakları incelendiğinde önceki kiralamalardan farklı olarak kişisel verilerinin işlenmesine dair açık rıza verdiğine ilişkin evrakın da içinde bulunduğunu tespit ettiği, bunun üzerine kişisel verilerinin işlenmesine rıza göstermek istemediğini, bu nedenle de ilgili evrakı imzalamayacağını çalışana beyan etmesi üzerine araç kiralama işleminin gerçekleştirilmediği, konuyla ilgili olarak veri sorumlusuna yetkilisi olduğu şirket tarafından 23/03/2018 tarihinde başvuruda bulunduğu, veri sorumlusu tarafından 29/03/2018 tarihinde cevap verildiği ancak taleplerine yönelik hiçbir cevap veya çözüm önerisi yer almadığı gerekçesiyle 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Bununla birlikte, veri sorumlusuna yapılan başvuruların ilgili kişinin yetkilisi olduğu Şirket veya Şirket çalışanları tarafından yapıldığı, veri sorumlusunun da Şirketi muhatap alarak cevap verdiği görüldüğünden Kanunun ilgili maddeleri hakkında bilgi verilerek Kanun kapsamında mağduriyet yaşamış olan Şirket yetkilisinin Kanunda belirtilen usul çerçevesinde öncelikle kendi adına veri sorumlusuna başvuruda bulunması sonrasında ise ilgili kişinin başvurusunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde ise; Kişisel Verileri Koruma Kuruluna (Kurul) şikâyette bulunulması durumunda konunun incelemeye alınabileceği hususunda bilgi verilmiştir.

Bu minvalde ilgili kiři tarafından Kuruma iletilen 26/09/2018 tarihli Őikayette, Kurumumuz yazısının ardından veri sorumlusuna ilgili kiři adına 03/08/2018 tarihinde bařvuruda bulunulduđu ancak 30 gnlk yasal sre iinde herhangi bir cevap verilmediđi ifade edilerek daha nce Kuruma intikal eden 25/05/2018 tarihli Őikayete konu aynı hususlara yer verilmiřtir.

Sz konusu iddialara iliřkin olarak veri sorumlusundan savunması istenilmiř olup, alınan cevabi yazıda zetle;

- Őirketin ara kiralama sektrnde nc konumda olmakla birlikte tekel niteliđinde olmadıđı, mřterilerin serbest piyasa kapsamında dilediđi bařka ara kiralama Őirketinden kiralama yapma olanađının bulunduđu,
- İlgili kiřinin veri sorumlusuna 23/03/2018 tarihinde yazılı bařvuruda bulunduđu, tarafına derhal yazılı cevap verildiđi, Őikayete konu edilen 03/08/2018 tarihli yazının ieriđi ile ilgili kiřinin 23/03/2018 tarihinde gnderdiđi ve veri sorumlusu tarafından cevaplanan yazının ieriđinin birebir aynı olduđu, bu nedenle ilgili kiřinin tekraren aynı talepleri iletmesinin masraf aısından taraflarınca uygun olmadıđının deđerlendirilerek cevap verilmediđi,
- Ara kiralama sektrnn giderek bymesi ve kiralık ara sayılarındaki artıř ile birlikte zellikle uyulurucuya iliřkin sular, gasp, hırsızlık ve terrle ilintili sularda kiralık araların kullanımının yaygınlařması zerine kanun koyucunun yasal dzenlemeye giderek kiralanan tm araların Kiralık Ara Bildirim Sistemine (KABİS) giriřini zorunlu hale getirdiđi,
- 6638 sayılı Kanun ile deđerliřik 1774 sayılı Kimlik Bildirme Kanununun ilgili hkmlerinin 04/04/2015 tarihinde yrrlđe girdiđi,
- 1174 sayılı Kimlik Bildirme Kanunu Ek Madde 3'te "*Ara kiralama Őirketlerinin sorumlu iřleticileri ve yneticileri, kiralanan ara bilgileri ile aracı kiralayanların kimlik bilgileri ve kira szleřmesi kayıtlarını usulne uygun řekilde gn gnne tutmak ve bu kapsamda mevcut bilgi, belge ve kayıtları genel kolluk kuvvetlerinin her an incelemelerine hazır bulundurmak zorundadırlar. Ancak ara kiralayanın kamu kurum veya kuruluřu olması hlinde sadece kamu kurum veya kuruluřuyla yapılan szleřme ile ara bilgileri sisteme kaydedilir. Ara kiralama esnasında geređe aykırı kimlik kullananlar ile birinci fıkrada kapsamında elde edilen bilgi ve kayıtları, hukuka aykırı olarak kullanan, bir bařkasına veren, yayan veya ele geiren kiři, 26/9/2004 tarihli ve 5237 sayılı Trk Ceza Kanunu hkmlerine gre cezalandırılır. Birinci fıkrada belirtilen ykmllklere aykırı hareket edenlere beř bin Trk Lirası, geređe aykırı kayıt tutan veya bilgi verenlere on bin Trk Lirası idari para cezası, mlki idare amirlerince verilir. Bu Kanuna gre verilen idari para cezaları tebliđinden itibaren 1 ay iinde denir. İřlenen bir suun gizlenmesi amacıyla bilgilerin yok edilmesi hlinde iřletme ruhsatı iptal edilir. Bu*

fıkraya göre idari yaptırımların uygulanması ceza soruşturması ve kovuşturması yapılmasına engel değildir.”
şeklinde düzenleme yapıldığı,

- Bu düzenlemeye aykırı hareket eden, araç kiralamalarını sisteme girmeyen, istendiğinde bilgileri paylaşmayanlar hakkında cezai yaptırımlar öngörüldüğü, buna göre bu bilgilerin araç kiralama şirketi olarak alınmasının zorunlu olduğu, bu bilgilerin bilişim sisteminde arşivlenmesi maksadıyla yüklüce masraf ve gider yapıldığı, ayrıca bunlara veri paylaşım izni verilmediği takdirde fiilen araç kiralaması yapılmasının mümkün olmayacağı,
- Şirketin müşteriler ile imzaladığı sözleşmelerden kaynaklanan ilişkilerden doğan kanuni zorunlulukları uyarınca bu evrakları saklama ve yargı makamlarınca celbi talep edildiğinde ibraz etme yükümlülüğünün bulunduğu,
- Şirketin bu şekilde kanuni zorunlulukları bulunması nedeniyle şirketin veri işleyen sıfatını haiz olduğu kiralama hizmetine ilişkin kişisel verileri temin etmesi ve saklaması gerektiği,
- Bu nedenle 6698 sayılı Kanununa aykırı olarak hareket etmemek saikiyle ilgili kişinin kiralama hizmetinden yararlandırılmadığı,
- Taraflarının 6698 sayılı Kanuna uygun hareket ettiği ve bu hususta da ilgili kişinin 29/03/2018 tarihli dilekçesine istinaden bilgilendirildiği, açıklanan tüm bu sebeplerle araç kiralaması yapmak isteyip kanunen zorunlu kişisel verilerinin işlenmesine muvafakat etmeyen ilgili kişi bakımından bu tutumun fiili ve hukuki imkansızlıklar nedeniyle mesnedi bulunmadığı

ifade edilmiştir.

Konuya ilişkin olarak yapılan incelemede, Kişisel Verileri Koruma Kurulunun 05/05/2020 tarihli ve 2020/335 sayılı Kararı ile,

- Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in (Tebliğ) “Başvuru Usulü” başlıklı 5 inci maddesinde, ilgili kişinin Kanunun 11 inci maddesinde belirtilen hakları kapsamında taleplerini yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletceği ve Tebliğin 6 ncı maddesinde de veri sorumlusunun bu Tebliğ kapsamında yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlü olduğu, veri sorumlusunun başvuruyu kabul edeceği veya gerekçesini açıklayarak

reddedeceği ve cevabımı ilgili kişiye yazılı olarak veya elektronik ortamda bildireceğinin hüküm altına alındığı,

- Veri sorumlusunun tarafından Kuruma verilen cevap yazısında şikayete konu edilen 03/08/2018 tarihli yazının içeriği ile ilgili kişinin 23/03/2018 tarihinde gönderdiği dilekçe içeriğinin birebir aynı olduğu, veri sorumlusu tarafından ilk dilekçeye verilen cevabın karşı tarafa iletilmesi konusunda ilgili masrafların taraflarınca karşılandığı, ilgili kişinin tekraren aynı talepleri iletmesinin masraf açısından taraflarınca uygun olmadığı değerlendirildiğinden cevap verilmediğinin ifade edildiği ancak, Tebliğin “Ücret” başlıklı 7 nci maddesinde, ilgili kişinin başvurusuna yazılı olarak cevap verilecekse on sayfaya kadar ücret alınmayacağı, on sayfanın üzerindeki her sayfa için ise 1 Türk Lirası işlem ücreti alınabileceğinin belirtildiği,

- Bununla birlikte başvuruların içeriği benzer olsa da 23/03/2018 tarihli başvurunun ilgili kişinin yetkilisi olduğu tüzel kişilik adına, 03/08/2018 tarihli ikinci başvurunun ise ilgili kişinin kendisi adına yapılmış olduğu dikkate alındığında, içerik açısından aynı olsa dahi başvuran kişiler açısından farklı olması sebebiyle iki başvurunun aynı nitelikte olmadığı bu sebeple ayrı bir başvuru olarak veri sorumlusu tarafından cevaplanması gerekirken herhangi bir cevap verilmediğinden veri sorumlusunun Kanun kapsamında kendisine yapılan başvurulara Tebliğe uygun olarak hareket etmediği,

- Diğer taraftan Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin birinci fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, ikinci fıkrasında ise Kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kanunun 5 inci maddesi çerçevesinde kişisel veri işleme şartları mevcut olsa dahi, kişisel verilerin işlenmesinde aynı zamanda, Kanunun 4 üncü maddesinde yer alan hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme,

işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine de uygun hareket edilmesi gerektiği,

- Şikayete konu somut olayla ilgili olarak 1174 sayılı Kimlik Bildirme Kanununun Ek 3 üncü maddesinin “Araç kiralama şirketlerinin sorumlu işleticileri ve yöneticileri, kiralanan araç bilgileri ile aracı kiralayanların kimlik bilgileri ve kira sözleşmesi kayıtlarını usulüne uygun şekilde günü gününe tutmak ve bu kapsamda mevcut bilgi, belge ve kayıtları genel kolluk kuvvetlerinin her an incelemelerine hazır bulundurmak zorundadır” hükmünü haiz olduğu, bu anlamda aracı kiralayan kişinin kişisel verilerinin ve kiralanan aracın bilgilerinin veri sorumlusu tarafından Emniyet Genel Müdürlüğü tarafından hazırlanan Kiralık Araç Bildirim Sistemine (KABİS) kaydının zorunlu olduğu, dolayısıyla Kanunun 5 inci maddesinin ikinci fıkrasının (a) bendinde yer alan “Kanunlarda açıkça öngörülmesi” hükmü ve verilen hizmetin ifası amacıyla aynı fıkranın (c) bendinde yer alan “bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” hükmü gereğince kişisel verilerinin işlendiğinin anlaşıldığı,

- Ancak ilgili kişinin başvurusunun ekinde yer alan ve veri sorumlusu tarafından imzalatılmak istenen yazının;

*“... olarak Kişisel verilerin korunması mevzuatına uygun hareket edebilmemizi teminen size hizmet sağlayabilme ve hizmetlerimizi geliştirebilme doğrultusunda yürüttüğümüz operasyonlarımız kapsamında **mevzuatın istisna kıldığı haller haricinde** kişisel verilerinizin işlenmesi ve aktarılması hususunda açık rızanızı almamız gerekmektedir.*

*... Kişisel verilerinizin yasa gereği sözleşmenin ifası için gerektiği ölçüde işlenmesi ve aktarılması halleri **haricinde**, işbu onayınız ile Şirketimize vereceğiniz kişisel verilerinizin yukarıda belirtilen bilgiler kapsamında işleneceğine, yurtiçi ve yurtdışındaki üçüncü kişilere aktarılacağına rıza göstermektedirsiniz.”*

şeklinde olduğu dikkate alındığında; Kanunun 5 inci maddesinin ikinci fıkrasının söz konusu olmadığı diğer hallerde açık rıza alınması yoluna gidilmesi yolunun seçildiği, şikayete konu olayda da açık rıza verilmemesi halinde hizmetten yararlandırılmadığı dolayısıyla hizmetin açık rıza şartına dayandırıldığı anlaşıldığı,

- Kanunun 3 üncü maddesinde açık rızanın, “belirli bir konuya ilişkin”, “bilgilendirmeye dayanan” ve “özgür iradeyle açıklanan” rıza şeklinde tanımlandığı, kişinin irade beyanı olan rızanın, kişinin yaptığı davranışın bilincinde ve kendi kararı olması halinde geçerlilik kazanacağından kişinin iradesini sakatlayacak her türlü fiilin, kişisel verilerin işlenmesi için verdiği açık rızayı da sakatlayacağı, bu anlamda açık rızanın özgür irade ile açıklanması gerektiğinden ilgili kişinin açık

rızasının alınmasının bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının ön şartı olarak ileri sürülmemesi gerektiği, kişisel verilerin veri sorumlusu tarafından Kanunun 5 inci maddesinin ikinci fıkrası kapsamında işlendiği haller haricinde kişisel verilerin işlenmesi ve yurtdışına aktarımın sağlanması amacıyla açık rıza alınmasının ayrıca açık rızanın hizmetin dolayısıyla sözleşmenin bir koşulu olarak dayatılmasının söz konusu olduğunun görüldüğü bununla birlikte diğer kişisel veri işleme şartlarının varlığı söz konusu iken açık rıza alınmasının, ilgili kişinin yanıtılması ve yanlış yönlendirilmesi dolayısıyla veri sorumlusunca hakkın kötüye kullanılması anlamına da geldiği

değerlendirmelerinden hareketle;

- Veri sorumlusuna başvuruların içeriği benzer olsa da 23/03/2018 tarihli başvurunun tüzel kişilik adına, 03/08/2018 tarihli ikinci başvurunun ise ilgili kişi adına yapıldığı dolayısıyla iki başvurunun aynı nitelikte olmadığı değerlendirildiğinden ve ilgili kişi tarafından ayrıca e-posta üzerinden başvurularının da mevcut olduğu göz önüne alındığında veri sorumlusunun Kanun kapsamında kendisine yapılan başvurulara Tebliğe uygun olarak cevap vermesi yönünde talimatlandırılmasına,
- Araç kiralama hizmeti alımı esnasında veri sorumlusu tarafından Kanunun 5 maddesinin ikinci fıkrasında yer alan işleme şartları dışındaki haller kapsamında hizmetten faydalanmak isteyen kişilerin kişisel verilerinin işlenmesi amacıyla toptan bir şekilde açık rıza alımı yoluna gidildiği, hizmetin ifası için gerekli olmamasına rağmen kişisel verilerin talep edildiği ve açık rıza verilmemesi durumunda da kişilere hizmet verilmediği dikkate alındığında; hukuka aykırı veri işleme faaliyetinin söz konusu olduğu bu durumun ayrıca Kanunun 4 üncü maddesinde yer alan hukuka ve dürüstlük kurallarına uygun olma ilkesine de aykırılık teşkil etmesi nedeniyle, veri sorumlusunun Kanunun 12 nci maddesinin birinci fıkrasının (a) bendinde öngörülen “Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek” yükümlülüğünü yerine getirmediği kanaatine varıldığından, veri sorumlusu hakkında Kanunun 18 inci maddesinin birinci fıkrasının (b) bendi uyarınca 50.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2020/336 sayılı KVKK Kararı

İlgili kişinin kendisine iletilmesi gereken cevap yazısının veri sorumlusu tarafından resmi yazı şeklinde, çalıştığı birime gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 05/05/2020 tarihli ve 2020/336 sayılı Karar Özeti

Karar Tarihi : 05.05.2020

Karar No : 2020/336

Konu Özeti : İlgili kişinin kendisine iletilmesi gereken cevap yazısının veri sorumlusu tarafından resmi yazı şeklinde, çalıştığı birime gönderilmesi

İlgili kişiden alınan şikâyet dilekçesinde özetle; daha önce personeli olduğu veri sorumlusu Üniversitenin Sanat Tarihi Bölümüne iletmış olduğu dilekçesinin akıbeti hakkında 4982 sayılı Bilgi Edinme Hakkı Kanunu kapsamında veri sorumlusundan kendisine bilgi verilmesini talep ettiği, bu kapsamdaki talebine ilişkin cevabın, doğrudan ve sadece kendisine verilmesi gerekirken başvurusunun halihazırda görevli olduğu aynı Üniversitenin Meslek Yüksekokulu Müdürlüğüne, tüm taraflara açık biçimde yazılmış ve personele iletilen alelade resmi yazı şeklinde iletildiği, üçüncü kişilerin erişimine açılan kişisel bilgilerinin 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında korunmasına yönelik olarak veri sorumlusundan gerekli tedbirleri almasını talep ettiği ancak yasal süre içinde gerekli tedbirlerin alınmadığı ve tarafına cevap verilmediği belirtilerek 6698 sayılı Kanun kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgilinin başvurusunda yazı içeriğinde kendisine ait ad, soyad, unvan ve sicil numarasına yer verilerek kişisel bilgilerinin üçüncü kişilerin erişimine açıldığının belirtildiği ancak ilgilinin zaten Üniversiteye bağlı bir birimde görevli olduğundan bu bilgilerin çalıştığı birimde bulunması zorunlu olan bilgiler olduğu, dolayısıyla kişisel bilgilerinin üçüncü kişilerin erişimine açıldığı iddiasının gerçek durumla bağdaşmadığının düşünüldüğü,

- İlgili kişinin gönderdiği dilekçenin geldiği sistem üzerinden bağlantı kurularak, dilekçesine herhangi bir kasıt olmaksızın cevapla butonu ile yanıt verildiği için doğrudan çalıştığı birime gitmesine neden olunduğu,

- Bu çerçevede kişilik haklarının korunması ilkesi doğrultusunda zedeleyici/yıpratıcı bir tutum sergilenmesinin söz konusu olmadığı

ifade edilmiştir.

Konuya ilişkin olarak yapılan incelemede, Kişisel Verileri Koruma Kurulunun 05/05/2020 tarihli ve 2020/336 sayılı Kararı ile,

- Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğin (Tebliğ) “Başvuru Usulü” başlıklı 5 inci maddesinde, ilgili kişinin Kanunun 11 inci maddesinde belirtilen hakları kapsamında taleplerini yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletceği ve Tebliğin 6 ncı maddesinde de veri sorumlusunun bu tebliğ kapsamında yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlü olduğu, veri sorumlusunun başvuruyu kabul edeceği veya gerekçesini açıklayarak reddedeceği ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildireceğinin hüküm altına alındığı,

- Nitekim veri sorumlusunun Kanunun 13 üncü maddesi kapsamında kendisine yapılan başvuruya cevap vermemesinin Tebliğin 6 ncı maddesinde yer alan başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırma yükümlülüğüne aykırı olduğu değerlendirildiğinden ilgili veri sorumlusu tarafından 6698 sayılı Kanun kapsamında kendilerine yapılan başvurulara Tebliğe uygun olarak cevap verilmesi hususunda azami dikkat ve özenin gösterilmediği,

- Diğer taraftan, Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin birinci fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, ikinci fıkrasında ise Kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması

için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Kişisel verilerin işlenmesi faaliyetinin Kanunun 3 üncü maddesinde kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı, bu çerçevede başvuruya konu olayda ilgili kişinin Bilgi Edinme Hakkı Kanunu kapsamında veri sorumlusuna başvurusuna verilen yanıtın, ilgili kişinin çalıştığı birime gönderilmesi suretiyle kişisel verilerinin açıklanmasında Kanunun 5 inci maddesi kapsamında herhangi bir hukuki dayanak söz konusu olmadığından veri sorumlusu tarafından Kanunun 12 inci maddesinin (1) numaralı fıkrası kapsamında kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirlerin alınmadığı kanaatine varıldığı,

- 6698 sayılı Kanunun 18 inci maddesinin birinci fıkrasının (b) bendinde Kanunun 12 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezası verileceği ile aynı maddenin üçüncü fıkrasında birinci fıkrada sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılacağı ve sonucunun Kurula bildirileceğinin hükme bağlandığı,

değerlendirmelerinden hareketle;

- Veri sorumlusunun 6698 sayılı Kanunun 13 üncü maddesi kapsamında kendisine yapılan başvuruya cevap vermemesinin Tebliğin 6 ncı maddesinde yer alan başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırma yükümlülüğüne aykırı olduğu değerlendirildiğinden veri sorumlusunun 6698 sayılı Kanun kapsamında kendilerine yapılan başvurulara Tebliğe uygun olarak cevap verilmesi hususunda azami dikkat ve özenin gösterilmesi konusunda talimatlandırılmasına,

- Veri sorumlusunun söz konusu uygulaması neticesinde yetkisi olmayan kişiler tarafından ilgili kişinin verilerine erişildiği dikkate alındığında veri sorumlusunca kişisel verilerin muhafazasına yönelik veri güvenliğine ilişkin gerekli yükümlülüklerin yerine getirilmediği kanaatine ulaşıldığından, veri sorumlusunun Kanunun 12 nci maddesinin birinci fıkrasına aykırılık teşkil eden uygulaması nedeniyle sorumlular hakkında Kanunun 18 inci maddesinin üçüncü fıkrası çerçevesinde işlem yapılmasına ve işlemin sonucu hakkında Kurula bilgi verilmesine karar verilmiştir.

2020/325 sayılı KVKK Kararı

Kurumumuza Bir Şahıs Tarafından Vekaleten İntikal Ettirilen Usulen Eksik Nitelikteki Çok Sayıda Başvuru Hakkında Kişisel Verileri Koruma Kurulunun 30/04/2020 Tarihli ve 2020/325 Sayılı Karar Özeti

Karar Tarihi : 30.04.2020

Karar No : 2020/325

Konu Özeti : Bir şahıs tarafından Kurumumuza vekaleten intikal ettirilen usulen eksik nitelikteki çok sayıda başvuru hakkında değerlendirme

Kurumumuza bazı ilgili kişiler adına bir şahıs tarafından vekaleten, bazı ilgili kişiler tarafından ise asaleten intikal ettirilen aynı biçim, içerik ve adres bilgisine sahip çok sayıda başvuruda özetle; 01/01/2018 tarihinde çıkarılan Avrupa Uyum Yasaları içerisinde “Otomatik Bilgi Paylaşımı” adı altında 116 ülke ile anlaşmalar yapıldığı ve bu anlaşmalar içinde Türkiye’nin de yer aldığı, bununla birlikte 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun (Kanun) 9’uncu maddesinde açıkça kişisel verilerin ilgili kişilerin açık rızası alınmadan yurtdışına aktarılamayacağına hükme bağlandığı ifade edilerek adına başvuru yapılan kişilerin özel bilgilerinin Avrupa ülkeleri ile paylaşılmasından tedirgin olmalarından ötürü dilekçelerinin dikkate alınması ve ilgili kişilerin emeklilikleri hakkında kendileri ve vekil tayin ettiği kişiler dışında kimseye bilgi verilmemesi talep edilmiştir.

Söz konusu her bir başvuruya cevaben, Kurumumuzca Kanun kapsamında inceleme yapılabilmesi için Kanun’un “Veri Sorumlusuna Başvuru” başlıklı 13’üncü maddesinin (1) numaralı fıkrasındaki, “İlgili kişi, bu Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir” hükmü gereği öncelikli olarak veri sorumlusuna başvurulması gerektiği; Kanun’un “Kurula Şikâyet” başlıklı 14’üncü maddesinde ise, “Başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyette bulunabilir. (2) 13 üncü madde uyarınca başvuru yolu tüketilmeden şikâyet yoluna başvurulamaz.” hükümlerine yer verildiği ve bu çerçevede Kanun kapsamındaki taleplerine ilişkin ilgili kişilerin emeklilik hakkındaki kişisel verileri açısından öncelikli olarak veri sorumlusu niteliğini

haiz T.C. Aile, Çalışma ve Sosyal Hizmetler Bakanlığı Sosyal Güvenlik Kurumuna başvurularını gerektiğinin açıklanmasına rağmen, gerek vekaleten gerek iletişim bilgisi olarak vekalet verilen şahsın iş adresi belirtilmek suretiyle diğer gerçek kişilerce imzalı aynı içerikteki usulen eksik nitelikteki başvuruların Kurumumuza gönderilmesine ısrarla devam edilmiştir.

Bu kapsamda, başvurulara cevaben iletilen yazılarımız dikkate alınmaksızın aynı nitelikteki başvuruların Kurumumuza gönderilmesine devam edilmesi sebebiyle vekaleten başvuruda bulunmaya devam eden şahsı muhatap yazımızda, kamu idaresinin yersiz ve boş yere meşgul edilmesine sebebiyet veren ve dilekçe hakkının kötüye kullanılmasını teşkil eden bu nitelikteki yazıların Kurumumuza gönderilmemesi gerektiği, aksi halde yargı yoluna başvurulacağı belirtildiği halde usulü şartlar tamamlanmaksızın aynı nitelikte başvuruların Kurumumuza gönderilmeye devam edildiği görülmüştür.

Anayasamızın "Dilekçe, Bilgi Edinme ve Kamu Denetçisine Başvurma Hakkı" başlıklı 74'üncü maddesinde, *"Vatandaşlar ve karşılıklılık esası gözetilmek kaydıyla Türkiye'de ikamet eden yabancılar kendileriyle veya kamu ile ilgili dilek ve şikayetleri hakkında, yetkili makamlara ve Türkiye Büyük Millet Meclisine yazı ile başvurma hakkına sahiptir. Kendileriyle ilgili başvuruların sonucu gecikmeksizin, dilekçe sahiplerine yazılı olarak bildirilir..."* düzenlemesi yer almaktadır. Bu kapsamda, dilekçe hakkının nasıl kullanılacağı 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun ile düzenlenmektedir.

Öte yandan, 4271 sayılı Türk Medeni Kanunu'nun "Dürüst Davranma" başlıklı 2'nci maddesi, *"Herkes, haklarını kullanırken ve borçlarını yerine getirirken dürüstlük kurallarına uymak zorundadır. Bir hakkın açıkça kötüye kullanılmasını hukuk düzeni korumaz."* hükmünü haizdir. Söz konusu hüküm, bir kamu düzeni kuralı olarak ele alınan ve genel olarak bir hakkın açıkça öngörüldüğü amaç dışında ve başkalarını zarara sokacak şekilde kullanılması olarak açıklanabilecek hakkın kötüye kullanılmasının hukuk düzenince himaye edilmeyeceğini ifade etmektedir. Bu bağlamda, 3071 sayılı Kanun'da öngörülen dilekçe hakkının kullanılma usulü ile 6698 sayılı Kanun'da öngörülen şikayet başvurusu usulünün amacına açıkça aykırı olan ve Kurumumuzun başvuruyu gereği gibi değerlendirmesini engelleyen davranışlar, başvuru hakkının kötüye kullanılması olarak değerlendirilmektedir.

Bu kapsamda, vekaleten yapılan başvurulara cevaben, gerekli usulü şartı taşımaması sebebiyle incelenemeyeceğinin ve başvuruların öncelikle Sosyal Güvenlik Kurumuna yapılması gerektiği hususunun Kurumumuzca pek çok defa bildirilmesine rağmen, hala ilgili kişiler adına vekaleten başvuruda bulunulmasının, bu başvurular neticesinde vekili olunan kişiler lehine bir durum yaratıyormuş gibi gözükme suretiyle ilgili kişilerden vekalet sözleşmesi adı altında haksız kazanç sağlanabileceği ve bu durumun da Türk Ceza Kanunu kapsamında suç teşkil edebileceği ve vekaleten

başvuruda bulunan şahsın Kurumumuza başvurularını yönlendirmeye devam ettiği hususu göz önüne alınarak; Kurulun 30/04/2020 tarih ve 2020/325 sayılı Kararı ile;

Bugüne kadar Kuruma intikal eden ve Karar tarihi itibariyle cevap verilmemiş vekaleten gönderilen başvurular ve aynı adres üzerinden gelen muhtelif kişilere ait başvurular ile bundan sonra Kuruma intikal edecek bu içerikle benzer nitelikteki diğer başvuruların değerlendirmeye alınmamasına ve konunun vekalet eden kişi açısından ilgili Kurumlara bildirilmesine

karar verilmiştir.

2020/315 sayılı KVKK Kararı

Veri Sorumluları Siciline Kayıt Yükümlülüğünden İstisna Tutulacak Veri Sorumluları ile ilgili Kişisel Verileri Koruma Kurulunun 22/04/2020 Tarihli ve 2020/315 Sayılı Kararı

Karar Tarihi : 22.04.2020

Karar No : 2020/315

Konu Özeti : Dernek, vakıf ve sendikaların Veri Sorumluları Siciline kayıt yükümlülüğünden istisna tutulması

I. Kararın Konusu ve Hukuki Dayanağı

6698 sayılı Kişisel Verilerin Korunması Kanununun (6698 sayılı Kanun) 16 ncı maddesinin ikinci fıkrasında yer alan “*Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir.*” hükmüne göre kural olarak kişisel veri işleyen gerçek ve tüzel kişilerin Veri Sorumluları Siciline (Sicil) kayıt yükümlülüğü bulunmakla birlikte Kişisel Verileri Koruma Kurulu (Kurul) tarafından bu yükümlülüğe istisna getirilebilmektedir.

6698 sayılı Kanunun 16 ncı maddesinin verdiği yetkiye dayanarak Sicile kayıt yükümlülüğüne istisna getirilen veri sorumluları ile ilgili 02.04.2018 tarihli ve 2018/32 sayılı Kurul kararı ile;

1. Herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler,
2. 18/01/1972 tarihli ve 1512 sayılı Noterlik Kanunu uyarınca faaliyet gösteren noterler,
3. 04/11/2004 tarihli ve 5253 sayılı Dernekler Kanununa göre kurulmuş derneklerden, 20/02/2008 tarihli ve 5737 sayılı Vakıflar Kanununa göre kurulmuş vakıflardan ve 18/10/2012 tarihli 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununa göre kurulmuş sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılara yönelik kişisel veri işleyenler,
4. 22/04/1983 tarihli ve 2820 sayılı Siyasi Partiler Kanununa göre kurulmuş siyasi partiler,

5. 19/3/1969 tarihli ve 1136 sayılı Avukatlık Kanunu uyarınca faaliyet gösteren avukatlar,
6. 1/6/1989 tarihli ve 3568 sayılı Serbest Muhasebeci Mali Müşavirlik ve Yeminli Mali Müşavirlik Kanunu uyarınca faaliyet gösteren Serbest Muhasebeci Mali Müşavirler ve Yeminli Mali Müşavirler

Sicile kayıt yükümlülüğünden istisna tutulmuştur.

Anılan Kurul kararının 3 üncü maddesinde yer alan “04/11/2004 tarihli ve 5253 sayılı Dernekler Kanununa göre kurulmuş derneklerden, 20/02/2008 tarihli ve 5737 sayılı Vakıflar Kanununa göre kurulmuş vakıflardan ve 18/10/2012 tarihli 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununa göre kurulmuş sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçalarına yönelik kişisel veri işleyenler” ifadesinin kapsamı, yorumlanması ve uygulamada yaşanan bazı tereddütler nedeniyle Kuruma iletilen görüş taleplerinin değerlendirilmesi sonucunda;

- Sicile kayıt yükümlülüğüne istisna getirilen 02.04.2018 tarihli ve 2018/32 sayılı Kurul kararının 3 üncü maddesinde yer alan “04/11/2004 tarihli ve 5253 sayılı Dernekler Kanununa göre kurulmuş derneklerden, 20/02/2008 tarihli ve 5737 sayılı Vakıflar Kanununa göre kurulmuş vakıflardan ve 18/10/2012 tarihli 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununa göre kurulmuş sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçalarına yönelik kişisel veri işleyenler.” ifadesinin “yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı olmak üzere kişisel veri işleyen Türkiye’de yerleşik dernek, vakıf ve sendikalar” şeklinde değiştirilmesinin,

Anılan Kararın Kurum internet sayfası ve Resmi Gazetede yayımlanmasının gerektiği kanaatine varılmıştır.

II. Sonuç

6698 sayılı Kanunun 16 ncı maddesi gereği Sicile kayıt yükümlülüğüne istisna getirilen 02.04.2018 tarihli ve 2018/32 sayılı Kurul kararının 3 üncü maddesinde yer alan dernek, vakıf ve sendikalarla ilgili istisna hususundaki başvurular üzerine Kurul tarafından yapılan değerlendirme sonucunda;

- Sicile kayıt yükümlülüğüne istisna getirilen 02.04.2018 tarihli ve 2018/32 sayılı Kurul kararının 3 üncü maddesinde yer alan “04/11/2004 tarihli ve 5253 sayılı Dernekler Kanununa göre kurulmuş derneklerden, 20/02/2008 tarihli ve 5737 sayılı Vakıflar Kanununa göre kurulmuş vakıflardan ve 18/10/2012 tarihli 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununa göre kurulmuş sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına

ve bağıřçularına yönelik kiřisel veri iřleyenler.” ifadesinin “yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı olmak üzere kiřisel veri iřleyen Tırkiye’de yerleřik dernek, vakıf ve sendikalar” olarak deęiřtirilmesinin,

- Anılan Kararın Kurum internet sayfası ve Resmi Gazetede yayımlanmasının

kabulüne oybirlięi ile karar verilmiřtir.

2020/307 sayılı KVKK Kararı

Türkiye Ticaret Sicili Gazetesinde açık bir şekilde ilan edilmeyen kişisel verilerin, talepleri üzerine kamu kurum ve kuruluşlarıyla paylaşılması hususuna ilişkin Kişisel Verileri Koruma Kurulunun 22/04/2020 tarihli ve 2020/307 sayılı Karar Özeti

Karar Tarihi : 22.04.2020

Karar No : 2020/307

Konu Özeti : Türkiye Ticaret Sicili Gazetesinde açık bir şekilde ilan edilmeyen şirket ortakları ve yetkililerine ait şahsi kimlik numaraları, şahsi adresleri gibi kişisel verilerinin paylaşılması hk.

a) Bilindiği üzere, 6102 sayılı Türk Ticaret Kanununun (**6102 sayılı Kanun**) 24 üncü maddesinin ikinci fıkrasında yer alan “Ticaret sicili, Bakanlığın gözetim ve denetiminde ticaret sicili müdürlükleri ve şubeleri tarafından tutulur.” şeklindeki hüküm ile ticaret sicilinin ticaret sicil müdürlükleri tarafından tutulduğu belirtilmiştir. 1 Numaralı Cumhurbaşkanlığı Kararnamesinin “İç Ticaret Genel Müdürlüğü” başlıklı 446 ncı maddesinin birinci fıkrasının (1) bendi ve Ticaret Sicili Yönetmeliğinin 13 üncü maddesi uyarınca da ticaret sicili işlemleri Merkezi Sicil Kayıt Sistemi (**MERSİS**) üzerinden gerçekleştirilmekte ve buna ilişkin sicil kayıtları MERSİS’te tutulmaktadır.

6102 sayılı Kanunun 24 üncü maddesine ait gerekçe metninde, MERSİS’in ticaret sicili kayıtlarının güvenli ve birbirinin yedeği olacak şekilde olmasını sağlayacağı ve ticaret sicili kayıtlarının aleniyetine imkân tanıyacağı belirtilmiştir. Bu anlamda, MERSİS ile getirilen aleniyetle gerçek anlamda şeffaflık sağlanarak kayıtlardaki yolsuzlukların, aykırılıkların ve düzensizliklerin önüne geçilmesi hedeflenmiştir.

b) Bilindiği üzere, ticaret sicili alenidir; diğer bir deyişle herkes ticaret sicilinin içeriğini ve dairede saklanan bütün senet ve belgeleri inceleyebilmekte, bunların onaylı suretlerini alabilmekte, bir hususun sicilde kayıtlı olup olmadığına dair onaylı belgenin verilmesini isteyebilmektedir. Nitekim, 6102 sayılı Kanunun 35 inci maddesinde,

“(1) Tescil işleminin dayanakları olan dilekçe, beyanname, senetler, belgeler ve ilanları içeren gazeteler, üzerlerine sicil defterinin tarih ve numaraları yazılarak sicil müdürlüğüne saklanır.

(2) Herkes ticaret sicilinin içeriğini ve müdürlükte saklanan tüm senet ve belgeleri inceleyebileceği gibi giderini ödeyerek bunların onaylı suretlerini de alabilir. Bir hususun sicilde kayıtlı olup olmadığına dair onaylı belge de istenebilir.

(3) Tescil edilen hususlar, Kanun veya Kanununun 26 ncı maddesine göre çıkarılacak yönetmelikte aksine bir hüküm bulunmadıkça ilan olunur.

(4) İlan, Türkiye genelinde sicil kayıtlarının ilanına özgü Türkiye Ticaret Sicili Gazetesi ile yapılır.”

düzenlemesine yer verilmek suretiyle ticaret sicili kayıtlarının aleni bir şekilde tutulduğu ve herkes tarafından sicil kayıtlarının onaylı suretlerinin alınabileceği hükme bağlanmıştır. Yine, Ticaret Sicili Yönetmeliğinin 15 inci maddesinde; “(1) Herkes, sicilin içeriğini ve müdürlükte saklanan tüm senet ve belgeleri inceleyebilir. Bu inceleme elektronik ortamda ve/veya müdürlükte yapılabilir.(...)” hükmüne yer verilmiştir. Mezkûr hükümle ticaret sicilinin herkes tarafından incelenebileceği ve kayıtların incelenme usulünün ne şekilde gerçekleştirilebileceğine ilişkin hususlar düzenlenmiştir.

c) Bilindiği üzere, Kanununun 3 üncü maddesinin birinci fıkrasının (d) bendi uyarınca **kişisel veri**; kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi, (e) bendi uyarınca **kişisel verilerin işlenmesi**; kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade etmektedir. Buna göre tacirlerin ya da şirket hissedarlarının isim, kimlik, adres ve benzeri bilgileri üzerinde Müdürlükler tarafından yapılan işlemlerin kişisel veri işleme faaliyeti olduğu açıktır.

Bu kapsamda, tescil ve ilanı öngörülen bilgiler, kişisel veri de içerdiği ve bu verilere herkes tarafından kolaylıkla ulaşılabildiği için bu verilerin kötü niyetli kullanımını engellemek amacıyla gerek 6102 sayılı Kanunda gerek Ticaret Sicili Yönetmeliğinde birtakım düzenlemeler öngörülmüştür. 6102 sayılı Kanununun 24 üncü maddesinin (5) numaralı fıkrasında, ticaret sicili kayıt işlemlerinin elektronik ortamda yapılması için toplanması ve işlenmesi gerekli olan kişisel verilerin, kişisel verilerin korunması ve bilgi güvenliğinin sağlanmasına ilişkin mevzuata uygun bir şekilde korunacağı hükme bağlanmıştır; Ticaret Sicili Yönetmeliğinin “Sicil kayıtlarına erişim hakkı” başlıklı 15 inci maddesinde de,

“(1) Herkes, sicilin içeriğini ve müdürlükte saklanan tüm senet ve belgeleri inceleyebilir. Bu inceleme elektronik ortamda ve/veya müdürlükte yapılabilir. (2) Defterler ve belgeler, sicil dairesinin bulunduğu kısımdan dışarıya

çıkarılamaz. Bunların incelenmesinde müdür, kişisel verilerin korunmasına ilişkin hükümler çerçevesinde gerekli tedbirleri almak zorundadır. İnceleme esnasında müdürün vereceği talimatlara uyulması zorunludur. Aksi takdirde müdür defter ve belgeleri derhal kaldırabilir. (3) **Elektronik ortamda yapılacak olan incelemelerde de kişisel verilerin korunmasını ve bilgi güvenliğini sağlayacak tedbirler alınır.**"

düzenlemesine yer verilmiştir. Yine anılan Yönetmeliğin "İlan" başlıklı 41 inci maddesinde bu Yönetmelik uyarınca tescil edilen gerçek kişilerin kimlik numaralarının ilan edilmeyeceği hususu düzenlenmiştir. Nitekim Türkiye Ticaret Sicili Gazetesinde yapılan ilanlarda T.C. kimlik numaraları maskelenmek suretiyle yayımlanmakta, gerçek kişilerin yerleşim yeri adresleri olarak yalnızca il ve ilçe bilgisi ilan edilmektedir.

Bu kapsamda önemle belirtmek gerekir ki, her ne kadar aleniyet gereği herkes ticaret sicilinin içeriğini ve müdürlükte saklanan tüm senet ve belgeleri inceleyebilecek olsa da, bu durumun anılan bilgilerin kişisel verilerin korunmasına ilişkin mevzuattan muaf olması anlamına gelmeyeceği; aynı şekilde, aleniyet kapsamında işlenen kişisel verilerin aleniyetin amacıyla örtüşmesi gerektiği ve aleniyet amacı dışında kalan durumlarda bu verilerin işlenmesinin hukuka aykırı olacağı değerlendirilmektedir.

d) Diğer taraftan, Müdürlükler nezdinde tutulan kişisel verilerin çeşitli kamu kurum ve kuruluşlarıyla paylaşılması bir "aktarım" faaliyeti olup, Kanunda yer alan kişisel verilerin işlenmesi tanımında da düzenlendiği üzere, kişisel verilerin aktarımı da bir kişisel veri işleme faaliyetidir. Bu çerçevede, kişisel verilerin yurt içinde aktarımını düzenleyen Kanunun "Kişisel verilerin aktarılması" başlıklı 8 inci maddesinde; kişisel verilerin, ilgili kişinin açık rızası olmaksızın aktarılamayacağı; ancak Kanunun 5 inci maddesinin ikinci fıkrasında ve özel nitelikli kişisel veriler bakımından yeterli önlemler alınmak kaydıyla 6 ncı maddesinin üçüncü fıkrasında belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilmesi, ayrıca kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümlerin saklı tutulduğu hüküm altına alınmıştır. Bu anlamda, ticaret sicili müdürlükleri nezdinde tutulan kişisel verilerin başka kamu kurum ve kuruluşlarıyla paylaşılmasında bir başka ifadeyle diğer kamu kurum ve kuruluşlarına aktarılmasında da 6698 sayılı Kanunun 8 inci maddesine uygun hareket edilmesi gerektiği açıktır.

Kişisel verilerin işleme şartlarının düzenlendiği Kanunun 5 inci maddesinin birinci fıkrasında ise, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği; ikinci fıkrasında belirtilen şartlardan birinin varlığı halinde ise, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hükme bağlanmıştır. Anılan işleme şartlarından "Kanunlarda açıkça

öngörülmesi”, veri sorumlusunun herhangi bir kanundaki düzenlemeye dayanarak kişisel veri işleyebilmesini ifade etmektedir. Örneğin, 6102 sayılı Kanunun 35 inci maddesine göre sicilin içeriğinin ve müdürlükte saklanan tüm senet ve belgelerin herkes tarafından incelenebileceği hüküm altına alınarak sicilin aleniyetine yönelik düzenlemeler yer almaktadır. Yine, 5490 sayılı Nüfus Hizmetleri Kanununun (5490 sayılı Kanun) “Gizlilik” başlıklı 9 uncu maddesi;

“(1) Nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Bunlar, yetkili ve sorumlu memurlar ile teftiş ve denetim yetkisi olanlar dışında kimse tarafından görülüp incelenemez. Mahkemeler bu hükmün dışındadır. (2) Nüfus kayıtlarına bu bilgileri işleyen memurlar ve Kimlik Paylaşımı Sistemi kapsamında nüfus kayıtlarından faydalanan diğer görevliler de bu gizliliğe uymak zorundadırlar. Bu yükümlülük, kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam eder.”

hükmünü amirdir. Benzer şekilde, 5490 sayılı Kanunun “Nüfus kayıt örneğini almaya yetkili olanlar” başlıklı 44 üncü maddesi;

“(1) Nüfus kayıt örneklerini; a) Bakanlık, (...) (ç) Adli makamlar, (...) nüfus müdürlüklerinden doğrudan almaya yetkilidirler.

(2) Birinci fıkrada sayılanlar dışında kalan kurumlar ve tüzel kişiler, yazılı olarak başvurmak ve istem nedenini açıkça belirtmek suretiyle Bakanlık veya mülki idare amirinin emri ile nüfus kayıt örneğini alabilirler. Bakanlık bu madde hükümlerini işletmek üzere Kimlik Paylaşımı Sistemi kurar.

(...)”

hükmünü amirdir. Belirtmek gerekir ki, anılan Kanunun 7039 sayılı Kanunla değişiklik yapılan 45 inci maddesinde de, yerleşim yeri ve diğer adres bilgilerini de içeren Kimlik Paylaşım Sisteminin kullanılmasına ilişkin usul ve esaslar hükmüne bağlanmıştır. Görüleceği üzere, kimlik bilgilerinin ve yerleşim yeri bilgilerinin paylaşımına ilişkin usul ve esasları belirleyen kanun olan 5490 sayılı Nüfus Hizmetleri Kanunu, bu verilerin paylaşımı noktasında özel düzenleme niteliğini haizdir.

Bu kapsamda, Nüfus Hizmetleri Kanununa göre kimlik bilgilerini paylaşmaya yetkili merci nüfus müdürlükleri olup, bu verilerin ticaret sicil müdürlüklerinden istenmesi hususunun Nüfus Hizmetleri Kanununa aykırı olduğu, bir başka ifadeyle, talep edilecek kişisel verilerin özel düzenleme niteliğini haiz ilgili mevzuat hükümlerinde belirtilen yetkili kamu kurumlarından temin edilmesi gerektiği değerlendirilmektedir.

e) Öte yandan, Kanunun “Genel ilkeler” başlıklı 4 üncü maddesinde, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği ve kişisel verilerin işlenmesinde maddede sayılan ilkelere uyulmasının zorunlu olduğu düzenleme altına

alınmıştır. Anılan madde hükmünden açıkça anlaşılacağı üzere, kişisel verilerin işlenmesinde her hal ve şartta Kanunun 4 üncü maddesinde sayılan genel ilkelere uyulması hukuki bir gerekliliktir. Bu ilkelerden “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması” ilkesine göre, işlenen veriler belirlenen amaçların gerçekleştirilmesine elverişli olmalı, amacın gerçekleştirilmesiyle ilgili olmayan veya sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik veri işleme yoluna gidilmemelidir. Burada önemli olan, amacı gerçekleştirmeye yönelik yeterli verinin temin edilmesi, bunun dışındaki amaç için gerekli olmayan veri işlemeden kaçınılmasıdır.

Sonuç olarak, yukarıda yer verilen açıklamalar çerçevesinde;

- Müdürlük tarafından tutulan ticaret sicilinin kişisel verileri içerdiği ve sicilde yer alan kişisel veriler bakımından Müdürlüğün kişisel veri işleme faaliyetini gerçekleştirdiği;
- Ticaret sicilinin aleni olmasının sicilde yer alan kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu hükümlerinden muaf olacağı anlamını taşımadığı,
- Bu kapsamda Müdürlük tarafından kamu kurum ve kuruluşlarına gerçekleştirilecek aktarımların Kanunun 8 inci maddesinde yer alan düzenlemeye uygun biçimde yapılması ve sicilde aleni olarak işlenen verilerin işlenmesi noktasında aleniyet amacına bağlı kalınması gerektiği;
- Aktarımı talep edilen kişisel verilerin, bu verileri işleme faaliyetinin özel olarak düzenlendiği ilgili mevzuatlarca yetkili kılınmış kuruluşlardan talep edilmesi,
- Her türlü kişisel veri işleme faaliyetinde özellikle Kanunun 4 üncü maddesinde yer alan “İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkesi ve veri güvenliğine ilişkin gerekli her türlü teknik ve idari tedbirlerin alınması yükümlülüğünün birlikte gözetilmesi gerektiği değerlendirilmektedir.

2020/286 sayılı KVKK Kararı

Bir oyun şirketinin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 16.04.2020 tarih ve 2020/286 sayılı Karar Özeti

Karar Tarihi : 16.04.2020

Karar No : 2020/286

Konu Özeti : Bir oyun şirketinin veri ihlal bildirimini hakkında karar

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Oyun şirketinin oyuncu verilerine yasal olmayan yollarla hackerlar tarafından iki farklı yerden hukuka aykırı erişim gerçekleştirildiği,
- Hackerların, şirketin bulut sistemlerine, belirli olmayan kaynaklardan temin ettikleri kimlik bilgileri kullanarak erişmiş olduğu,
- Hackerların, oyuncu verilerine erişim sağladıklarının log kayıtlarından tespit edildiği, bu yetkisiz erişimin tespit edilmesinden sonra sistemde oyuncu giriş bilgilerinin değiştirildiği,
- Türkiye’de ihlalden etkilenen kişi sayısının 39,995 olduğu,
- İhlalden etkilenen kişi kategorilerinin kullanıcılar olduğu,
- Etkilenen kişisel verilerin, isim, soy isim, posta kodu, mahalle ve/veya ikamet ettiği şehir, doğum tarihi, e-posta adresi, fotoğraf, oyuncu kullanıcı adı ve şifresi, telefon numarası ve Facebook tanımlayıcısı da dâhil, özel nitelikli olmayan kimlik, irtibat ve konum bilgileri olduğu,
- Belirtilen verilerin tamamının olayın kapsamına her aşamada dahil olmadığı, örneğin, Türkiye’de yerleşik 39.995 kişi içerisinde 1.527 kişinin telefon numaralarına ve 51 kişinin doğum tarihine erişim sağlandığının düşünüldüğü,
- Türkiye’de yerleşik kişilere e-posta yoluyla bildirimde bulunulduğu, ifadelerine yer verilmiştir.

ifadelerine yer verilmiştir.

Söz konusu bildirimincelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 16.04.2020 tarih ve 2020/286 sayılı Kararı ile;

- Türkiye’de ihlalden etkilenen kişi sayısının 39.995 olduđu,
- Etkilenen kişisel verilerin, isim, soy isim, posta kodu, mahalle ve/veya ikamet ettiđi şehir, doğum tarihi, e-posta adresi, fotoğraf, kullanıcı adı ve şifresi, telefon numarası ve Facebook tanımlayıcısı da dâhil, özel nitelikli olmayan kimlik, irtibat ve konum bilgileri olduđu,
- Bir bulut sistemi bulunan veritabanına saldırganlar tarafından erişim sağlanmasının yapılan zafiyet testlerin yetersiz olmasının ve gerekli önlemlerin alınmadığının göstergesi olduđu,
- Veri sorumlusu tarafından ihlal öncesi alınması gereken teknik tedbirlerin (güvenlik ajanının ağ sistemine konuşlandırılması, kötü niyetli IP adreslerinin sistemden engellenmesi, oyuncu hesaplarının yetkisiz erişimlerden korunması için gerekli önlemlerin alınması, hackerlar tarafından kullanılan mekanizmaların ve IP’lerin gözlenmesi için 7x24 gerçek zamanlı gözetleme sistemini de içeren, geliştirilmiş gözetleme ve alarm sistemlerinin faaliyete geçirilmesi) ihlal sonrası devreye alınmasının gerekli teknik ve idari tedbirlerin alınmadığının göstergesi olduđu

hususları dikkate alındığında,

- Kanununun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik tedbirleri almayan Şirket hakkında Kanununun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 1.000.000 TL,
- Kanununun 12 nci maddesinin (5) numaralı fıkrasında yer verilen “en kısa sürede” (24.01.2019 tarih ve 2019/10 sayılı Kurul kararında belirtilen 72 saatlik süre içerisinde) bildirimde bulunma yükümlülüğüne aykırı hareket eden Şirket hakkında Kanununun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL

olmak üzere toplam 1.100.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2020/255 sayılı KVKK Kararı

Veri sorumlusu eğitim kurumu tarafından şikayetçinin çocuklarının özel nitelikli kişisel verilerinin hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 02/04/2020 tarihli ve 2020/255 sayılı Karar Özeti

Karar Tarihi : 02.04.2020

Karar No : 2020/255

Konu Özeti : Veri sorumlusu eğitim kurumu tarafından ilgili kişilerin özel nitelikli kişisel verilerinin hukuka aykırı olarak işlenmesi

Kuruma intikal eden şikâyet; şikayetçinin velisi bulunduğu çocuklarının veri sorumlusuna ait okulda eğitim gördüğü, gerek bu öğrencilere gerekse de diğer öğrencilerin okulda eğitim gördükleri sırada velilerinden herhangi bir şekilde izin alınmadan, aydınlatma yükümlülüğü yerine getirilmeden veya açık rızaları alınmadan CAS (Cognitive Assessment System) Uygulama ve Değerlendirme testinin yapıldığı, CAS testinin klinik ve nörolojik değerlendirme yeteneği ile geniş yelpazede gelişimsel değerlendirme yapabilen güncel bir ölçek olduğu, çocukların bu test için Kişisel Verilerin Korunması Kanununun (Kanun) 6 ncı maddesi ile belirlenmiş özel nitelikli kişisel verilerinin kullanıldığı ve işlendiği, aynı madde hükmünce ilgili kişilerin veya velisinin açık rızası bulunmadan bu verilerin işlenmesinin kesinlikle yasaklandığı, veri sorumlusunun uzun süredir şikayetçinin velayeti altında bulunan çocuklara eğitim vermekte iken hiçbir kayıt işleminde kişisel verilerin işlenmesinden bahsetmediği, Kanunun 10 uncu maddesi hükümlerince aydınlatma yükümlülüğünün yerine getirilmediği, veri sorumlusuna başvuruda bulunulduğu ancak yeterli bir cevap alınamadığı bu çerçevede Kurula şikâyetle bulunulduğu belirtilerek, veri sorumlusunun Kanunun 18 inci maddesi uyarınca aydınlatma yükümlülüğü ve veri güvenliğine ilişkin yükümlülüklerini ihlal fiillerinden dolayı cezalandırılması, işlenen verilerin Kanunun 7 nci maddesi doğrultusunda silinmesi, yok edilmesi veya anonim hale getirilmesi ve yapılan yargılama masrafları vs. tüm giderlerin karşı tarafa yükletilmesine karar verilmesi talep edilmiştir.

Konuya ilişkin başlatılan inceleme neticesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- Öncelikle şikayetçinin iddialarının aksine sadece bir çocuğuna bahse konu testin uygulandığı,
- Şikayete konu edilen testin hukuki dayanağının; eğitim kurumlarında sunulacak rehberlik hizmetlerinin amaç, ilke, faaliyet ve çalışma yöntemlerini düzenleyen “Milli Eğitim Bakanlığı Rehberlik Hizmetleri Yönetmeliği” (10 Kasım 2017 tarihli ve 30326 sayılı R. G.) olduğu, söz konusu Yönetmeliğin 6 ncı maddesi uyarınca rehberlik hizmetlerinin eğitsel rehberlik, mesleki rehberlik ve kişisel/sosyal rehberlik olarak üç temel alana ayrıldığı,
 - Bu kapsamda eğitsel rehberliğin “bireyin yetenek, ilgi, ihtiyaç, değer, kişilik özellikleri, imkân ve koşullarıyla uyumlu eğitsel kararlar alması; eğitime ilişkin olumlu tutum geliştirmesi ve hayat boyu öğrenme sürecinde bireyin gelişimine destek olunması amacıyla bireye ve ailesine sunulan hizmet” (Madde 6 (1) (a)); kişisel/sosyal rehberliğin ise “bireyin bilişsel, sosyal, duygusal, ahlaki ve davranışsal gelişimini desteklemek amacıyla kendini tanıması; karar verme ve problem çözme gibi sosyal beceriler ile yaşam becerilerini geliştirmesi ve sorumluluk sahibi bir birey olarak hayatına devam edebilmesi için bireye ve ailesine sunulan hizmet” (Madde 6 (1) (c)) olarak tanımlandığı,
 - Aynı Yönetmeliğin 8 inci maddesinin (1) numaralı fıkrasının (b) bendinde “İlkokul kademesinde rehberlik hizmetleri; öğrencinin okula uyum sağlamasına, eğitim ortamlarına ve öğrenmeye yönelik olumlu tutum geliştirmesine; öğrenmeyi öğrenme ve öğrendiklerini aktarmaya yönelik bilişsel becerileri kazanmasına; etkili öğrenmeye yönelik stratejiler geliştirme, duyguları tanıma, kendini ifade etme gibi sosyal beceriler ile zorlu yaşam olaylarıyla baş etme becerileri kazanmasına; kişilik gelişimini ve mesleki gelişimlerini desteklemeye yönelik olarak eğitsel, mesleki ve kişisel/sosyal rehberlik hizmetleri kapsamında yürütülür.” hükmünün yer aldığı,
 - Bu çerçevede eğitim kurumlarında sunulan rehberlik hizmetinin amacının ölçme değerlendirme araçları ve diğer yöntemleri kullanarak öğrencilerin durumlarının tespit edilip desteklenmesi gereken alanlarda çalışma yürütmek olduğu,
 - Rehberlik hizmetlerinin yerine getirilebilmesi ve amaçlarının sağlanabilmesi için “bireyin tanınması”nın zorunlu olduğu ve öğretmenlerin görevleri arasında olduğu, Yönetmeliğin 9 uncu maddesinin (1) numaralı fıkrasına göre bireyi tanımanın, “bireyin kendi ilgi, yetenek, değer, tutum ve kişilik özelliklerini keşfetmesini ve gerçekçi kararlar almasını sağlamak amacıyla rehberlik öğretmeni, sınıf rehber öğretmeni ve diğer öğretmenler tarafından yürütülen bilgi toplama süreci” olarak tanımlandığı ve aynı maddenin aynı

fıkrasının (c) bendine göre bireyin tanınması sürecinde farklı ölçme araçlarının, yöntemlerinin ve tekniklerinin kullanılmasının mümkün olduğu,

- Yönetmelik ile “rehberlik ve araştırma merkezleri ile rehberlik servislerinin bireyi tanıma, tanılama, tarama ve inceleme çalışmalarında kullanabilecekleri çeşitli test, anket ve envanterler”in psikolojik ölçme araçları olarak tanımlandığı ve Yönetmeliğin 10 uncu maddesinde rehberlik hizmetlerinde bireyi tanıma çalışmalarında kullanılacak psikolojik ölçme araçlarının sağlanmasına ilişkin amaç ve uygulama ilkelerinin belirlendiği,

- Bu çerçevede testin amacının rehberlik faaliyeti kapsamında öğrenciye eğitsel, kişisel, sosyal rehberlik hizmeti ile sınırlı olduğu, yürütülen faaliyetin hukuka uygun, belirli, açık ve meşru olduğu, testin uygulanmasına ilişkin velilerin bilgisi ve onayının bulunduğu,

- Öğrencinin velisi ile veri sorumlusunun rehberlik servisi arasında yapılan rehberlik görüşmesinde; öğrencinin öfkeli ve kaygılı olduğu, konuşurken heyecanlandığı, ikinci defa tekrarlamak istemediği, arkadaşları tarafından alay edilebildiği, içe dönük yapısı olduğu gibi konularda dikkatli olunması gerektiği hususunda veli tarafından bilgilendirme yapıldığı, bunun üzerine rehberlik hizmetine başlandığı, akabinde veri sorumlusunun rehberlik servisi ile öğrencinin velileri (anne ve baba) arasında çeşitli tarihlerde rehberlik görüşmelerinin devam ettiği ve bu görüşmelere ilişkin velilerin imzasını da içeren Bireysel Görüşme Formlarının düzenlendiği,

- CAS testinin öğrencinin velisinin bilgisi ve onayı ile başlanan rehberlik faaliyeti çerçevesinde öğrencinin durumunu tespit etmek, öğrenciyi tanımak, öğrencinin yetenek ve ilgi alanlarını belirleyerek öğrencinin bilişsel ve akademik gelişmesini sağlayabilmek amacıyla uygulandığı ve şikayetçinin başvurusuna verilen cevapta da bunun belirtildiği,

- Testin sonucuna ilişkin değerlendirmelerin öğrencinin velisi ile paylaşıldığı, veli ile yapılan e-posta yazışmalarında veli tarafından kendisine iletilen söz konusu test değerlendirmelerinin öğrenciyi takip eden psikiyatrist ile de paylaşıldığının belirtilmesinin ve rehberlik birimine öğrencinin tedavisi ile ilgili bilgi verilmesinin, velinin CAS testinin uygulandığından haberdar olduğunu gösterdiği,

- Uygulanan testin milli eğitim mevzuatı çerçevesinde, rehberlik faaliyetlerinde uygulanmasına cevaz verilen psikolojik bir ölçme aracı olduğu ve öğrenciye ilişkin kişisel verilerin işlenmediği ve üçüncü şahıslarla paylaşılmadığı, söz konusu test kitapçığının Kuruma iletilendiği,

- Testin Milli Eğitim Bakanlığının Rehberlik Hizmetleri mevzuatı çerçevesinde, rehberlik hizmetleri amaçları doğrultusunda uygulandığı ve veri sorumlusu eğitim kurumunun mevzuat ile tanımlanmış görev ve yetkilerini aşmadığı, testin uygulanmasında Kanuna aykırı davranılmadığı

belirtilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 02/04/2020 tarihli ve 2020/255 sayılı Kararı ile,

- 6698 sayılı Kişisel Verilerin Korunması Kanununun “Tanımlar” başlıklı 3 üncü maddesinin (1) numaralı fıkrasının (ç) bendinde ilgili kişinin, “kişisel verisi işlenen gerçek kişi”; (d) bendinde kişisel verinin, “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi”, (e) bendinde kişisel verilerin işlenmesinin, “kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem”, (ı) bendinde veri sorumlusunun “kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi” olarak tanımlandığı,

- Bu çerçevede şikayete konu olayda, şikayetçinin velisi olduğu öğrencinin CAS testine tabi tutulması sonucunda ortaya çıkan verilerin kişisel veri niteliğinde olduğu, şikayetçinin velisi olduğu öğrencinin gerçek kişi olması nedeniyle ilgili kişi sıfatını haiz olduğu, bünyesindeki eğitim kurumlarında öğrenim görmekte olan öğrencilerinin kişisel verilerinin hangi amaçla ve araçla işleneceğini belirleyip veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olması nedeniyle eğitim kurumunun veri sorumlusu olduğu,

- Genel olarak, eğitim kurumlarının rehberlik servisleri tarafından uygulanan psikolojik testlerin çeşidi ne olursa olsun, öğrencinin bireysel olarak daha yakından tanınmasını sağlamayı amaçladığı dikkate alındığında; testin sonucunun yorumlanması neticesinde oluşturulan değerlendirme kapsamında öğrenciyi diğer öğrencilerden ayıran ve kimliğini belirli veya belirlenebilir hale getiren kişisel verilerin işlendiği,

- Bu kapsamda ilgili kişilere CAS testi uygulanması sonrasında, veri sorumlusunun rehberlik servisinde görevli rehberlik öğretmeni/ psikolojik danışman tarafından yapılan ve öğrenciye ilişkin duygu durum, davranış, bilişsel yetenekler vb. unsurları içerdiği kanaatine varılan test sonucuna ilişkin değerlendirmenin kişisel veri işleme faaliyeti kapsamında olduğu,

- Kanununun “Kişisel verilerin işleme şartları” başlıklı 5 inci maddesinde;

“(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işleniminin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.” hükmüne yer verildiği,

- “Özel nitelikli kişisel verilerin işleme şartları” başlıklı 6 ncı maddesinde ise;

“(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. (2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır. (3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir. (4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.” hükümlerinin yer aldığı,

- Söz konusu kişisel veri işleme faaliyeti kapsamında; veri sorumlusu ile veli arasında, bireysel görüşme formları ve e-posta yazışmaları yoluyla en az 7 ay süren rehberlik sürecinde ilgili kişi öğrencinin ruh sağlığına ilişkin bilgilerin paylaşıldığı ve CAS testinin uygulanması sonucunda dikkat eksikliği/ hiperaktivite bozukluğu/ kaygı bozukluğu gibi ilgili kişinin ruh sağlığına ilişkin özel nitelikli kişisel verilerin de işlendiği,

- Psikolojik testlerin ölçüm alanları itibariyle farklılık gösterdiği ve eğitim sürecinde; öğrencinin öğrenme becerilerinin geliştirilmesi, akademik performansının artırılması, sosyal faaliyetlere yönlendirilmesi, meslek seçimi vb. konulara yönelik çalışmalar yapılmasını desteklemek amacıyla öğrencinin kişilik özelliklerini, akademik başarısını, zeka düzeyini, yeteneklerini, ilgi alanlarını ölçen psikolojik testlerin uygulanması sonucunda elde edilen değerlendirmelerin dahi kişisel veri içerdiği,

Milli Eğitim Bakanlığı Rehberlik Hizmetleri Yönetmeliğinin 10 uncu maddesi çerçevesinde; bu kapsamdaki kişisel veri işleme faaliyetinin, veri sorumlusunun Kanunun 5 inci maddesinin (ç) bendinde yer alan *“veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması”* kişisel veri işleme şartına dayandırılabilceği,

- Bununla birlikte somut vakada, ilgili kişi öğrenciye CAS testinin uygulanması sonucunda, zekâ ve bilişsel becerilerin yanı sıra dikkat eksikliği ve hiperaktivite bozukluğu gibi öğrencinin ruh sağlığına ilişkin özel nitelikli kişisel verilerin de işlenmiş olduğu dikkate alındığında; Kanunun 6 ncı maddesinin (3) numaralı fıkrasında yer verilen *“kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi”* amaçları da bulunmadığından, veri sorumlusu tarafından söz konusu veri işleme faaliyetinin *“açık rıza”* şartına dayandırılması gerektiği sonucuna varılacağı,

- Kurula yapılan şikâyet başvurusunda; gerek velisi olunan öğrencilere gerek diğer öğrencilere okulda eğitim gördükleri sırada velilerinden herhangi bir şekilde açık rızaları alınmadan CAS testinin yapıldığı iddiası karşısında ek bilgi/belge talebi kapsamında, Kurumun yazısı ile testin uygulanması sürecinde ilgili kişilerin açık rızasının alınıp alınmadığına ilişkin bilgi, belge, kayıt vb. dokümanın Kuruma iletilmesinin talep edildiği, veri sorumlusu tarafından iletilen cevabi yazıda, CAS testinin velinin bilgi ve onayı dâhilinde uygulandığının ifade edildiği, bunun da daha önce iletilen velinin imzasının bulunduğu bireysel görüşme formları ve e-posta yazışmaları ile açıkça kanıtlandığı ancak açık rızanın alındığına veya talep edildiğine dair herhangi bir bilgi/ belge iletilmediği,

- Özel nitelikli kişisel veri olan *“sağlık verisi”* nin, ilgili kişinin açık rızasına dayanarak işlenebildiği ve ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğu, bu kapsamda veri sorumlusunun, ilgili kişilere CAS testi uygulanması sürecinde, ilgili kişilerin reşit olmaması nedeniyle velisinin açık rızasına dayanmadan özel nitelikli kişisel verilerini işlediği, ilgili kişilerin açık rızasının alınmadığı hususunda taraflar arasında ihtilaf olmadığı, söz konusu verilerin özel nitelikli verileri de içermesi nedeniyle ilgili kişilerin açık rızası olmadan gerçekleştirilen veri işleme faaliyetinin hukuka aykırı bir veri işleme faaliyeti olduğu,

- Kuruma intikal eden şikâyet başvurusunda; veri sorumlusu tarafından aydınlatma yükümlülüğü yerine getirilmeden gerek velisi olunan öğrencilere gerek diğer öğrencilere CAS testinin yapıldığının iddia edildiği, bu çerçevede veri sorumlusundan ek bilgi/belge talebi kapsamında, testin uygulanması sürecinde ilgili kişilere testle ilgili olarak aydınlatma yapılıp yapılmadığı, ayrıca test ve testin sonucuna ilişkin bilgilendirmenin yapılıp yapılmadığına ilişkin bilgi, belge, kayıt vb. dokümanın Kuruma iletilmesinin talep edildiği,

- Veri sorumlusu tarafından iletilen cevap yazısında, CAS testinin rehberlik hizmeti kapsamında velinin bilgisi ve onayı dahilinde uygulandığı, testin sonucuna ilişkin değerlendirmelerin öğrencilerin velisi ile paylaşıldığı, söz konusu test değerlendirmelerinin ilgili kişi tarafından ayrıca öğrenciyi takip eden psikiyatru ile de paylaşıldığı, bu hususların velinin imzasının bulunduğu bireysel görüşme formları ve e-posta yazışmalarında açıkça yer aldığı belirtilmekle birlikte aydınlatmanın yapıldığına dair herhangi bir bilgi/ belgenin Kuruma iletilmediği,
- Kanun uyarınca veri sorumlusu veya yetkilendirdiği kişi tarafından, kişisel verilerin elde edilmesi sırasında, ilgili kişinin talebine bağlı olmaksızın sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanılmak suretiyle aydınlatma yükümlülüğünün yerine getirilmesinin gerektiği ayrıca bu yükümlülüğün yerine getirildiğinin ispatının da veri sorumlusuna ait olduğu, bu nedenle somut olayda, veri sorumlusu her ne kadar CAS testinin uygulanması süreci ve testin sonucu hakkında velinin bilgisi ve onayının olduğunu kanıtlaya da, aydınlatma yükümlülüğünün yerine getirilmesi için Kanunda öngörülen gerekli şartlar ile Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğde yer alan usul ve esasları tam olarak yerine getirmediği,
- Bu kapsamda veri sorumlusunun rehberlik servisi tarafından; öğrencilere CAS testi uygulanması sürecinde veri sorumlusunun kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, kişisel veri toplamanın yöntemi ve hukuki sebebi ile Kanunun 11 inci maddesinde sayılan ilgili kişilerin diğer hakları konusunda öğrencinin velisine yeterli düzeyde bilgi sağlamamak suretiyle veri sorumlusunun aydınlatma yükümlülüğünü tam olarak yerine getirmediği sonucuna varıldığı,
- Şikâyet dilekçesinde veri sorumlusu tarafından işlenen kişisel verilerin Kanunun 7 inci maddesi gereğince silinmesi, yok edilmesi veya anonim hale getirilmesi gerektiği belirtilmekle birlikte veri sorumlusuna başvuruda bu hususta bir talepte bulunmadığı,
- Veri sorumlusunun savunmasında CAS testi yoluyla ilgili kişilerin kişisel verilerinin işlenmediği iddia edilerek verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi ile ilgili herhangi bir hususa yer verilmediği, öğrencilerin, velisi tarafından yeni eğitim öğretim yılında bir başka okula nakledildikleri dikkate alındığında; işlenmesinde Kanunun 5 inci ve 6 ncı maddelerinde belirtilen şartlardan herhangi birini karşılamayan kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi gerektiği,
- Yukarıda açıklandığı üzere, somut olayda gerçekleşen veri işleme faaliyetinde, ilgili kişilerin özel nitelikli kişisel veri kapsamında olan sağlık verisine ilişkin olarak; ilgili kişinin/velinin açık rızasının

alınmadığı, açık rızanın aranmadığı diğer durumların da bulunmadığı gerekçesiyle veri işleme faaliyetinin hukuka aykırı olduğu sonucuna varıldığı,

- Son olarak ilgili kişi tarafından şikâyet dilekçesinde, CAS testinin yalnızca velisi olduğu öğrencilere değil diğer öğrencilere de okulda eğitim gördükleri sırada velilerinden herhangi bir şekilde izin alınmadan, aydınlatma yükümlülüğü yerine getirilmeden veya açık rızaları alınmadan uygulandığının iddia edildiği, veri sorumlusunun bir eğitim kurumu olduğu dikkate alındığında, Milli Eğitim Bakanlığı Rehberlik Hizmetleri Yönetmeliği doğrultusunda öğrencilere yönelik bireysel veya grup rehberlik hizmetlerini yürütmek üzere CAS ve benzeri psikolojik ölçme araçlarını kullanarak öğrencilerinin kişisel verilerini/ özel nitelikli kişisel verilerini işlediği sonucuna varıldığı değerlendirmelerinden hareketle,

- Veri sorumlusu eğitim kurumu tarafından ilgili kişilerin özel nitelikli kişisel veri kapsamında olan sağlık verisine ilişkin olarak; ilgili kişinin/velinin açık rızasının alınmadığı, açık rızanın aranmadığı diğer durumların da bulunmadığı gerekçesiyle Kanunun 12 inci maddesi uyarınca; kişisel verilerin hukuka aykırı olarak işlenmesinin engellenmesini teminen gerekli idari ve teknik tedbirleri almadığı kanaatine varılan veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendinde gereğince 50.000 TL idari para cezası uygulanmasına,

- Kanunun “Özel nitelikli kişisel verilerin işleme şartları” başlıklı 6 ncı maddesi uyarınca, özel nitelikli kişisel veri kapsamında olan ilgili kişinin sağlık verisinin ilgili kişilerin/velinin açık rızası alınmadan işlenmesi nedeniyle hukuka aykırı bir şekilde veri işlendiği dikkate alınarak velilere ve öğrencilere sunulan rehberlik hizmeti sürecinin kişisel verilerin korunması mevzuatı ile uyumlu hale getirilmesi, hukuka aykırılıkların giderilmesi hususunda veri sorumlusunun talimatlandırılmasına,

- Veri sorumlusu tarafından gerçekleştirilen kişisel veri işleme faaliyetlerine ilişkin olarak aydınlatma yükümlülüğünün Kanunun 10 uncu maddesi ve ilgili Tebliğ hükümlerine uygun şekilde yerine getirilmesi hususunda veri sorumlusunun talimatlandırılmasına,

- Öte yandan, hukuka aykırı elde edilen verilerin Kanunun 7 nci maddesi kapsamında silinmesi, yok edilmesi veya anonim hale getirilmesi hususunda Şirketin talimatlandırılmasına,

- Diğer taraftan şikâyetçinin, yapılan yargılama masrafları vs. tüm giderlerin karşı tarafa yükletilmesine karar verilmesine yönelik talebinin Kanun kapsamında olmadığı dikkate alındığında bu hususta Kurulca yapılacak bir işlem bulunmadığına

karar verilmiştir.

2020/226 sayılı KVKK Kararı

İlgili kişinin, bir Valilikte görev yapmakta iken, Valilik çalışanı tarafından hukuka aykırı olarak elde edildiği iddia edilen kişisel verilerinin Valiliğe dijital ortamda sunulması hakkında Kişisel Verileri Koruma Kurulunun 19/03/2020 tarih ve 2020/226 sayılı Karar Özeti

Karar Tarihi : 19.03.2020

Karar No : 2020/226

Konu Özeti : İlgili kişinin, bir Valilikte görev yapmakta iken, Valilik çalışanı tarafından hukuka aykırı olarak elde edildiği iddia edilen kişisel verilerinin Valiliğe dijital ortamda sunulması

Kuruma intikal eden şikâyet başvurusunda, ilgili kişinin, veri sorumlusu bir Valilikte görev yapmakta iken, veri sorumlusunun bir çalışanı tarafından hukuka aykırı olarak elde edildiği iddia edilen kişisel verilerinin veri sorumlusuna dijital ortamda sunulduğu, söz konusu verilere dayanılarak ilgili kişi hakkında 657 sayılı Devlet Memurları Kanunu gereğince disiplin soruşturması başlatıldığı ve disiplin cezası aldığı, başka bir ilde alt kadroya atandığı, 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında İçişleri Bakanlığına müracaat ederek Kanuna aykırı olarak gerçekleştirilen disiplin soruşturması sonucunda tarafına verilen disiplin cezalarının ve atama işleminin iptali ve hukuka aykırı olarak elde edilen ve üçüncü şahıslara aktarılan kişisel verilerinin yok edilmesi talebinde bulunduğu, İçişleri Bakanlığının bu talebi veri sorumlusuna gönderdiği, veri sorumlusu tarafından disiplin cezalarının kaldırılması ve atama işleminin iptali ile ilgili talebe karşılık yetersiz bir cevap verildiği iddia edilerek gereğinin yapılması talep edilmiştir.

Konuya ilişkin olarak yapılan değerlendirme neticesinde Kişisel Verileri Koruma Kurulunun 19/03/2020 tarih ve 2020/226 sayılı Kararı ile,

- Kanununun 15 inci maddesinin (1) numaralı fıkrasında Kişisel Verileri Koruma Kurulunun şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapacağı; aynı maddenin (2) numaralı fıkrasında ise 1/11/1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanununun 6 ncı maddesinde belirtilen

Belli bir konuyu ihtiva etmeyen,

Yargı mercilerinin görevine giren konularla ilgili olan,

4 üncü maddede gösterilen şartlardan (dilekçe sahibinin adı soyadı ve imzası ile iş veya ikametgâh adresi) herhangi birini taşımayan

ihbar veya şikâyetlerin incelemeye alınmayacağına hükme bağlandı,

- Öte yandan, Kanunun 17 nci maddesinin (1) numaralı fıkrasında, kişisel verilere ilişkin suçlar bakımından 26.09.2004 tarih ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümlerinin uygulanacağı belirtilmekte olup, Türk Ceza Kanununun 135 inci maddesinde hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verileceği, 136 ncı maddesinde ise kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişinin, iki yıldan dört yıla kadar hapis cezası ile cezalandırılacağına hükme bağlandı,

- Diğer taraftan, Kanunun istisnalar başlıklı 28 inci maddesinin (2) numaralı fıkrasında, bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddelerinin aynı fıkranın (c) bendinde yer alan kişisel veri işleminin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması durumunda uygulanmayacağına belirtildiği

değerlendirmelerinden hareketle;

- Kişisel verileri hukuka aykırı olarak elde eden Valilik çalışanı açısından şikâyete konu iddiaların esasen Türk Ceza Kanunu hükümleri uyarınca değerlendirilmesi gerektiğinden 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesi de dikkate alınarak söz konusu başvurunun Kanun kapsamında değerlendirilemeyeceğine,

- Veri sorumlusunun işlediği kişisel verilerin disiplin soruşturma veya kovuşturması kapsamında Kanunun 28 inci maddesinin (2) numaralı fıkrasının (c) bendi kapsamında işlendiğinden bu aşamada Kanun çerçevesinde yapılacak bir işlem bulunmadığına,

- Öte yandan işlenen veriler ve yürütülen soruşturma sonucunda ilgili kişi hakkında uygulanan yaptırımların ise 657 sayılı Kanun gereğince özlük dosyalarında saklanması gerektiği, Kamu Personeli Genel Tebliğine (Seri No: 2) göre görevi herhangi bir şekilde sona eren memurların özlük dosyalarının kurumlarınca saklanacağı ve Devlet Arşiv Hizmetleri Hakkında Yönetmeliğe göre son işlem tarihi üzerinden yüz bir yıl geçmemiş memuriyet sicil dosyaları içerisinde yer aldığı dikkate alınarak, ilgili kişinin veri sorumlusu nezdindeki bahse konu verilerinin silinmesi talebinin de 6698

sayılı Kanunun 7 inci maddesinde belirtildiđi üzere kiřisel verilerin iřlenmesini gerektiren sebeplerin henüz ortadan kalkmaması dolayısıyla veri sorumlusu tarafından karşılanmasının mümkün olmadığına

karar verilmiştir.

2020/213 sayılı KVKK Kararı

Bir internet servis sağlayıcısının veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 12.03.2020 tarih ve 2020/213 sayılı Karar Özeti

Karar Tarihi : 12.03.2020

Karar No : 2020/213

Konu Özeti : Bir internet servis sağlayıcısının veri ihlali hakkında Karar

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Şirketin müşterilerinin paket değişikliği, fatura ödeme, arıza bildirim gibi abonelik işlemlerini yapmalarına olanak sağlayan ve kendilerine tanımlanan kullanıcı adı ve şifre ile giriş yapabildikleri bir Online İşlem Merkezi bulunduğu,
- Şirketin fatura ödeme sisteminde online (çevrimiçi) işlemlerde fatura ödemesi yapılamadığı ve sorunun Şirkete müşteriler tarafından bildirildiği,
- Müşterinin ödeme yaptığı sırada ekranda “fatura seçilmesi gerektiği” uyarısı belirdiği,
- Sorun giderilmek üzere çalışma yapılırken bir güvenlik açığının ortaya çıktığı,
- Güvenlik açığı sebebiyle müşterilerin kredi kartı bilgilerinin üçüncü taraflarca görüntülediği,
- İhlalin kök nedeninin uygulamaya bilgi kaydı (log) üreten özelliklerin eklenerek “debug” ile düzeltilmesi girişiminin olduğu,
- 69 kişiye ait kart bilgisinin 649 adet Şirket müşterisi tarafından görüntülediğinin tespit edildiği, ifadelerine yer verilmiştir.

Söz konusu bildirim incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 12.03.2020 tarih ve 2020/213 sayılı Kararı ile;

- Yazılım geliştiricilere sözlü olarak aktarılmış olan değişiklik talebinin test ortamında değil de gerçek ortamda yapılmasının, uygulamada yapılan değişikliklerin canlıya (gerçek/çalışır ortam) alma süreçleri ile ilgili prosedürlerin uygulanmadığının göstergesi olduğu bu durumun ise teknik ve idari tedbir eksikliği olduğu,

- Test süreçlerinin yetersizliği veri sorumlusunun kendisi tarafından belirtilmiş olup bu durumun uygulama güvenliği açısından veri sorumlusunun gerekli teknik ve idari tedbirleri almadığının göstergesi olduğu,
- Sistem ara yüzlerinde kişisel verilerin ya hiç gösterilmediğinin ya da maskelendiğinin şirket tarafından belirtilmiş olmasına rağmen müşterilere ait kimlik ve finans verilerinin yapılan hata sonucunda görüntülenebilmesinin teknik bir eksiklik olduğu,
- Veri sorumlusunun bir veri güvenliği politikasının bulunduğu ancak bu politikanın yürürlük tarihinin veri ihlalinin gerçekleştiği tarihten sonra olduğu

dikkate alınarak, 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan Şirket hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 300.000 TL idari para cezasının uygulanmasına karar verilmiştir.

2020/212 sayılı KVKK Kararı

Ses kayıt özelliği bulunan güvenlik kamerası kullanılması ile ilgili Kişisel Verileri Koruma Kurulunun 12/03/2020 tarihli ve 2020/212 sayılı Karar Özeti

Karar Tarihi : 12.03.2020

Karar No : 2020/212

Konu Özeti : Bir kamu kurumu olan veri sorumlusu tarafından ses kayıt özelliği bulunan güvenlik kamerası kullanılması hk.

6698 sayılı Kişisel Verilerin Korunması Kanununun 3 üncü maddesinin birinci fıkrasının (d) bendi uyarınca “kişisel veri”; “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi” ifade etmektedir. Aynı maddenin birinci fıkrasının (e) bendi uyarınca “kişisel verilerin işlenmesi” ise; “kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi”, (ç) bendi uyarınca “ilgili kişi”; “kişisel verisi işlenen gerçek kişiyi”, (ı) bendi uyarınca “veri sorumlusu”; “kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişiyi” ifade etmektedir. Görüldüğü üzere; Kanun kişisel veri işleme faaliyetini tanımlarken örnek olması adına birtakım işlemde bahsetmiş fakat işleme faaliyetini bunlarla sınırlı tutmamıştır. Bu anlamda, kişisel veriler üzerinde gerçekleştirilecek her türlü eylem, kişisel veri işleme faaliyeti olarak kabul edilecek ve Kanun kapsamında değerlendirilecektir.

Kanunun 5 inci maddesinde ise kişisel verilerin işlenme şartlarına yer verilmiş olup; bu maddenin birinci fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, ikinci fıkrasında belirtilen şartlardan (-Kanunlarda açıkça öngörülmesi, -Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, -Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, -Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, -İlgili kişinin kendisi

tarafından alenileştirilmiş olması, -Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, -İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması) birinin varlığı halinde ise, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hükme bağlanmıştır.

Kanunun "Genel ilkeler" başlıklı 4 üncü maddesinde, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği ve kişisel verilerin işlenmesinde maddede; "*Hukuka ve dürüstlük kurallarına uygun olma. -Doğru ve gerektiğinde güncel olma. -Belirli, açık ve meşru amaçlar için işlenme. -İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. -İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.*" şeklinde sayılan ilkelere uyulmasının zorunlu olduğu düzenleme altına alınmıştır. Anılan madde hükmünden açıkça anlaşılacağı üzere, kişisel verilerin işlenmesinde her hal ve şartta Kanunun 4 üncü maddesinde sayılan genel ilkelere uyulması hukuki bir gerekliliktir. Bu ilkelerden kişisel verilerin "*belirli, açık ve meşru amaçlar için işlenme*" ilkesi, kişisel veri işleme faaliyetlerinin ilgili kişi tarafından açık bir şekilde anlaşılır olmasını, kişisel veri işleme faaliyetinin hangi hukuki işleme şartına dayalı olarak gerçekleştirildiğinin tespit edilmesini, kişisel veri işleme faaliyetinin ve gerçekleştirilme amacının belirliliğini sağlayacak detayda ortaya konulmasını sağlar. Amacın meşru olması, veri sorumlusunun işlediği verilerin, yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması anlamına gelmektedir. Bir diğer önemli ilke olan "*işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması*" ilkesine göre, işlenen veriler belirlenen amaçların gerçekleştirilmesine elverişli olmalı, amacın gerçekleştirilmesiyle ilgili olmayan veya sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik veri işleme yoluna gidilmemelidir. Burada önemli olan, amacı gerçekleştirmeye yönelik yeterli verinin temin edilmesi, bunun dışındaki amaç için gerekli olmayan verilerin işlenmesinden kaçınılmasıdır. Ölçülülük ilkesi ise, veri işleme ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması yani veri işlemenin, amacı gerçekleştirecek ölçüde olması demektir.

Bu kapsamda kişisel verilerin korunması hakkı, Anayasanın "Özel hayatın gizliliği" başlıklı 20 nci maddesinin üçüncü fıkrasında; "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.*" şeklinde hüküm altına alınmıştır. Bu düzenleme ile kişisel verilerin korunması hakkına anayasal bir nitelik kazandırılmış olup; bir temel hak ve

özgürlük olan bu hakkın sınırlandırılması da ancak Anayasanın 13 üncü maddesine uygun bir şekilde gerçekleştirilecektir. Nitekim, Anayasanın 13 üncü maddesi; *“Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.”* hükmünü amirdir. Görüldüğü üzere; bir temel hak ve özgürlüğün sınırlandırılmasının söz konusu olduğu hallerde; hakkın özüne dokunulmaması ve sınırlamanın Anayasanın sözüne, ruhuna, demokratik toplum düzenine, laik Cumhuriyetin gerekleri ile ölçülülük ilkesine aykırı olmaması gerekmektedir.

Bu hususa ilişkin olarak Anayasa Mahkemesinin 28/09/2017 tarihli ve 2016/125 E. 2017/143 K. sayılı kararında da; *“...*

24. *Anayasa'nın 20. maddesinin üçüncü fıkrasında ise “Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.”* hükmü yer almaktadır.

25. *108 sayılı Sözleşme'nin 9. maddesinde de devlet güvenliği, kamu güvenliği, devletin ekonomik menfaatlerinin korunması ve suçlarla mücadele edilmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması ile verilerin istatistiki veya bilimsel amaçlarla kullanılması durumlarında kişisel verilerin korunmasına sınırlamalar getirilebileceği belirtilmektedir.*

26. *Ancak bu sınırlama yapılırken temel hak ve özgürlüklerin sınırlandırılması rejimini belirleyen Anayasa'nın 13. maddesine de uyulması gerekmektedir. Anayasa'nın 13. maddesinde “Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.”* denilmektedir. *Anayasa'nın 13. maddesi uyarınca özel hayatın gizliliği ve kişisel verilerin korunması hakları, yalnızca kanunla ve demokratik bir toplumda gerekli olduğu ölçüde sınırlanabilir. Ayrıca getirilen bu sınırlamalar hakkın özüne dokunamayacağı gibi Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamaz.*

27. *Temel hak ve özgürlükler özlerine dokunulmaksızın yalnızca Anayasa'da öngörülen sebeplerle ve ancak kanunla sınırlanabilir. Dokunulamayacak “öz”, her temel hak ve özgürlük açısından farklılık göstermekle birlikte kanunla getirilen sınırlamanın hakkın özüne dokunmadığının kabulü için temel hakların kullanılmasını*

ciddi surette güçleştirip amacına ulaşmasına engel olmaması ve etkisini ortadan kaldırıcı bir nitelik taşımaması gerekir.

28. Temel hak ve özgürlüklerin özlerine dokunulmaksızın yapılan sınırlamaların ise demokratik toplum düzeninin gerekleri ile ölçülülük ilkesine aykırı olamayacağı belirtilmiştir. Öze dokunma yasağını ihlal etmeyen müdahaleler yönünden gözetilmesi öngörülen “demokratik toplum düzeninin gerekleri” kavramı, öncelikle ilgili hak yönünden getirilen sınırlamaların zorunlu ve istisnai tedbir niteliğinde olmalarını gerektirmektedir. “Demokratik toplum düzeninin gerekleri”nden olma, bir sınırlamanın demokratik bir toplumda zorlayıcı bir toplumsal ihtiyacın karşılanması amacına yönelik olmasını ifade etmektedir.

29. Anayasa'nın 13. maddesinde ifade edilen “ölçülülük ilkesi”, temel hak ve özgürlüklerin sınırlandırılmasına ilişkin başvurularda dikkate alınması gereken bir diğer ilkedir. Demokratik toplum düzeninin gerekleri ve ölçülülük ilkeleri, iki ayrı kriter olarak düzenlenmiş olmakla birlikte bu iki kriter arasında sıkı bir ilişki vardır. Temel hak ve özgürlüklere yönelik herhangi bir sınırlamanın başvurulabilecek en son çare ya da alınabilecek en son önlem olarak temel haklara en az müdahaleye olanak veren ölçülü bir sınırlama niteliğinde olup olmadığının incelenmesi gerekir.

30. Demokratik toplum kişilerin temel hak ve özgürlüklerinin en geniş şekilde güvence altına alındığı bir düzeni gerektirir. Demokrasilerde devlete düşen görev temel hak ve özgürlükleri korumak ve geliştirmek, bunların etkili şekilde kullanılmasını sağlayacak tedbirleri almaktır. Bu kapsamda devlet, özellikle temel hak ve özgürlükleri ortadan kaldıracak veya bunlara ölçsüz müdahale teşkil edecek tutumlardan kaçınmalı ve başkalarından gelebilecek tehditlere karşı bireyleri korumalıdır.

31. Özel hayatın gizliliği ve kişisel verilerin korunması hakkı, temel hak ve özgürlükler arasında önemli bir yer alır. Özel hayatın gizliliğinin korunması, bu hayatın başkalarının gözleri önüne serilmemesi demektir. Kişinin özel hayatının, yalnız kendisi veya kendisinin bilmesini istediği kimseler tarafından bilinmesini isteme hakkı, kişinin temel haklarından biridir ve bu niteliği nedeniyle insan haklarına ilişkin beyanname ve sözleşmelerde yer almış; demokratik ülkelerin mevzuatında açıkça belirlenen istisnalar dışında devlete, topluma ve diğer kişilere karşı korunmuştur. Kişisel verilerin korunması hakkı ise özel hayatın gizliliği hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvencenin yaşama geçirilebilmesi için bu hakkı ilgilendiren yasal düzenlemelerin açık, anlaşılabilir ve kişilerin söz konusu haklarını kullanabilmelerine elverişli olması gerekir. Ancak böyle bir düzenleme ile kişilerin özel hayatlarını ilgilendiren veri ve bilgilerin resmî makamların keyfî müdahalelerine karşı korunması mümkün olabilir.

...” açıklamalarına yer verilmiştir.

Bu açıklamalardan da anlaşılacağı üzere, temel hak ve özgürlük niteliğini haiz kişisel verilerin korunması hakkının sınırlandırılmasının, demokratik bir toplumda gerekli olduğu ölçüde, hakkın kullanımının ciddi surette güçleştirilip amacına ulaşmasının engellenmemesi ve etkisinin ortadan kaldırılmaması şartıyla mümkün olmasının yanı sıra, Devlet'in de bu tür hakları ortadan kaldıracak veya bu haklara ölçsüz müdahale teşkil edecek tutumlardan kaçınması gerekmektedir. Dolayısıyla, kişisel verilerin korunması hakkını sınırlayan hükümlerin, hakkın kullanımını ciddi surette güçleştirip amacına ulaşmasını engelleyecek ve etkisini ortadan kaldıracak şekilde geniş yorumlanmaması, aksine bu hükümlerin bir Anayasal hakkın istisnası olduğu bilinci ile dar yorumlanması gerektiği değerlendirilmektedir.

Bu açıklamalar çerçevesinde, sesli kamera kaydının hukuka uygun bir kişisel veri işleme faaliyeti olarak değerlendirilebilmesi için Anayasada belirtilen temel hak ve özgürlüklerin sınırlandırılmasında gözetilmesi gereken ilkelere uygun olması gerekmektedir. Bu kapsamda söz konusu kayıt ile beklenen faydanın ses kaydı olmaksızın görüntü kaydı ile elde edilebileceği hallerde ses kaydının da yapılması, gerçekleştirilecek kişisel veri işleme faaliyeti ile ulaşılmak istenen amaç arasındaki dengenin bozulmasına yol açacağından ölçülülük ilkesine aykırılık teşkil edecektir. Bu anlamda, gözetim sistemlerinde görüntü kaydı ile birlikte ses kayıt sisteminin de kullanılmasının sadece görüntü kaydına göre çok daha müdahaleci olacağı açıktır. Diğer taraftan, kameralar vasıtasıyla görüntü ile birlikte ses kaydı yapılması, bireylerde her açıdan gözetim altında tutuldukları endişesi yaratabilecek olup, kişilerin kamusal alanda bile özel bir kısım diyaloglarının ya da yaşantı kesitlerinin bulunabileceği de dikkate alındığında bu yönde bir uygulamanın hakkın özüne zarar vereceği değerlendirilmektedir. Ayrıca belirtmek gerekir ki, güvenlik amacıyla kamu kurumunun halk girişine takılması yönünde ihtiyaç bulunduğu belirtilerek ses kaydı yapan kameraların kullanılması, benzer nitelikteki her türlü ortam açısından da gerekli olduğu yönünde genel bir değerlendirmeye neden olabileceğinden, kişisel verilerin korunması hakkına yönelik oldukça geniş nitelikte bir istisna oluşması sonucunu doğurabilecektir ki, bu hususun da hakkın özüne zarar vereceği değerlendirilmiştir.

2020/201 sayılı KVKK Kararı

Bir bankanın veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 03/03/2020 tarih ve 2020/201 sayılı Karar Özeti

Karar Tarihi : 03.03.2020

Karar No : 2020/201

Konu Özeti : Bir bankanın veri ihlal bildirimini

Veri sorumlusunun Kurumumuza intikal eden veri ihlali bildiriminde;

- İhlalin, şirket müşterilerinin finansman taksit ödemesi tahsilatlarının gerçekleştiğine ilişkin ilgili müşterilere gönderilmesi gereken 905 kişiye ait bildirim (e-posta ve kısa mesaj) işlem dışı ve Banka sisteminde kayıtlı diğer müşterilere gönderilmesi şeklinde gerçekleştiği,
- İhlalin gerçekleşme şekli ve yöntemi hakkında;
 - Sehven gönderildiği belirtilen bildirimlerin, Şirketin mail ve SMS gönderimleri için kullandığı bir "iç sistem uygulaması" ile yapıldığı,
 - "İç sistem uygulamasında" bir yazılım değişikliğine gidildiği,
 - Ancak geliştirme hatası sebebiyle müşterelik ilişkisi dışındaki ilişki tiplerine sahip müşterilere de sehven bildirim yapıldığı,
 - Teknik anlamda, kullanılması gereken fonksiyon ve metodun doğru kullanıldığı ancak parametrelerde yeterli kontrol konulmadığının anlaşıldığı,
 - "İç sistem uygulaması" üzerinden yapılan geliştirmeyle faydası amaçlanan işlemin gerçekleştiği fakat tüm senaryoların öngörülemediği için amaçlanandan daha fazla müşteriye bildirim yapılmasına sebep olduğu
- İlgili kişilere SMS ve e-posta kanalıyla bilgilendirmenin yapıldığı,
- İhlalden etkilenen kişi sayısının 905; kayıt sayısının 1831 olduğu,
- Etkilenen kişi kategorilerinin müşteriler olduğu,

- İhlalden etkilenen kişisel verilerin kimlik (isim-soy isim), müşteri işlem (cari hesap numarası, finansman hesap numarası, işlem tarihi) ve finans bilgileri (finansman taksit numarası, finansman taksit tutarı, finansman taksit tarihi) olduğu,

ifadelerine yer verilmiştir.

Söz konusu bildirim incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 03/03/2020 tarih ve 2020/201 sayılı Kararı ile;

- İhlalin, şirket müşterilerinin finansman taksit ödemesi tahsilatlarının gerçekleştiğine ilişkin, ilgili müşterilere gönderilmesi gereken 905 kişiye ait bildirim (e-posta ve kısa mesaj) işlem dışı ve Banka sisteminde kayıtlı, diğer müşterilere gönderilmesi şeklinde gerçekleştiği, bunun sonucunda ihalden ilgili kişilerin; kimlik (isim-soy isim), müşteri işlem (cari hesap numarası, finansman hesap numarası, işlem tarihi) ve finans bilgileri (finansman taksit numarası, finansman taksit tutarı, finansman taksit tarihi) gibi kişisel verilerinin etkilendiği,

- Sehven gönderildiği bildirilen bildirimlerin, veri sorumlusu mail ve SMS gönderimleri için kullandığı bir iç sistem uygulaması ile yapıldığı, ihlale konu olayda teknik anlamda, “kullanılması gereken fonksiyon ve metodun doğru kullanılmasına rağmen parametrelerde yeterli kontrol konulmadığının anlaşıldığı, ilgili geliştirmeyle faydası amaçlanan işlemin gerçekleştiği fakat tüm senaryoların öngörülemediği için amaçlanandan daha fazla müşteriye bildirim yapılmasına sebep olduğu”, bu teknik tedbir eksikliğinin de ihlale yol açtığı, bahsi geçen “Notification” uygulama sisteminin hata sonucu veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için yerleştirilen kontrol mekanizmasının yeterli düzeyde olmadığı, bu tip hataların test aşamasında tespit edilerek değişikliklerin yayına alınmadan evvel düzeltilmesi gerektiği

dikkate alındığında, Kanununun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanununun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 75.000 TL idari para cezasının uygulanmasına,

- İhlalin 05.07.2019 ile 08.07.2019 arasında gerçekleştiği, 08.07.2019 tarihinde tespit edildiği ve ihlal bildiriminin Kuruma 11.07.2019 tarihinde intikal ettiği, bu kapsamda bildirim 72 saat içinde gönderildiği, ayrıca veri sorumlusu tarafından ilgili kişilere bildirim yapılmış olduğu

dikkate alındığında, veri sorumlusu hakkında Kanununun 12 nci maddesinin (5) numaralı fıkrası uyarınca yapılacak bir işlem olmadığına

karar verilmiştir.

2020/196 sayılı KVKK Kararı

İlgili kişiye ait kişisel verinin denetim faaliyeti kapsamında bir kamu kurumuna aktarılmasına ilişkin şikayet hakkında Kişisel Verileri Koruma Kurulunun 03/03/2020 Tarihli ve 2020/196 Sayılı Karar Özeti

Karar Tarihi : 03.03.2020

Karar No : 2020/196

Konu Özeti : İlgili kişiye ait kişisel verinin denetim faaliyeti kapsamında bir kamu kurumuna aktarılmasına ilişkin şikayet başvurusu hakkında

Kurumumuza intikal eden şikayet başvurusunda; bir veri sorumlusuna ait internet sitesinin ana sayfasında yayımlanan haberin altına yapılan yorumlarla ilgili olarak, başlatılan idari soruşturma kapsamında veri sorumlusundan habere yapılan yorumların tamamı ve yorum yapan kullanıcı IP adreslerinin istenildiği, bunun üzerine veri sorumlusu tarafından ilgili kişinin kişisel verilerinin çalıştığı kamu kurumuyla paylaşıldığı ve bu nedenle ilgili kişinin çalıştığı kamu kurumunda idari soruşturmaya maruz kaldığı, cep telefonuna ait IP adresinin ilgili kurum ile paylaşılmasının hukuka, hakkaniyete ve ölçülülük ilkesine uygun olmadığından bahisle veri sorumlusu şirket hakkında Kanun kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin yapılan inceleme aşağıdaki hususlar tespit edilmiştir:

- Bir veri sorumlusuna ait internet sitesinin ana sayfasında yayımlanan haberin altına yapılan yorumlar ile ilgili olarak habere konu kamu kurumu nezdinde başlatılan idari soruşturma çerçevesinde söz konusu kamu kurumunda görevli denetçiler tarafından haberin altına yapılan tüm kullanıcı yorumları ve bu yorumları yapan kimselerin tüm IP adreslerinin talep edildiği ve bu talebe cevaben ilgili veri sorumlusunun, tüm kullanıcı yorum ve IP'lerinin diğer veri sorumlusuna aktarıldığı tespit edilmiştir.
- 6698 sayılı Kişisel Verilerin Korunması Kanununun "Kişisel Verilerin İşlenme Şartları" başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği hükme bağlanmıştır. Aynı maddenin (2) numaralı fıkrasında da ilgili kişinin açık rızasının aranmayacağı durumlar;

- a) Kanunlarda açıkça öngörülmesi.
- b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
- c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması

şeklinde sayılmıştır.

• Kanunun kişisel verilerin aktarılmasına ilişkin 8 inci maddesi “(1) *Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz. (2) Kişisel veriler; a) 5 inci maddenin ikinci fıkrasında, b) Yeterli önlemler alınmak kaydıyla, 6 ncı maddenin üçüncü fıkrasında, belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir. (3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.*” şeklinde düzenlenmiştir.

• Veri güvenliğine ilişkin yükümlülükler Kanunun 12 nci maddesinde hüküm altına alınmış olup, ilgili madde hükmü şu şekildedir;

“(1) *Veri sorumlusu;*

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.”

• Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinde, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verilmiştir. Bu çerçevede, kişisel veriler ancak; *hukuka ve dürüstlük kurallarına uygun şekilde, belirli, açık ve meşru amaçlar kapsamında, doğru ve gerektiğinde güncel olma şartıyla, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun*

işlenebilmektedir. İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi kapsamında, işlenen veriler belirlenen amaçların gerçekleştirilebilmesine elverişli olmalı, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılması gerekmektedir. Bu noktada önemli olan husus, amacı gerçekleştirmeye yönelik yeterli verinin elde edilip, bunun dışındaki amaç için gerekli olmayan veri işlemeden kaçınılmasıdır.

- 375 sayılı Kanun Hükmünde Kararnamenin Ek 24 üncü maddesinde "...Denetime tabi gerçek ve tüzel kişiler, denetim için gereken gizli dahi olsa bütün belge, defter ve bilgileri talep edildiği takdirde ibraz etmek, para ve para hükmündeki evrakı ve ayniyatı ilk talep halinde göstermek, sayılmasına ve incelenmesine yardımcı olmak zorundadır. Müfettiş, denetmen, denetçi, kontrolör ve aktüerler ile bunların yardımcısı ve stajyerleri, görevleri sırasında tüm resmi daire, kurum, kuruluş ve kamuya yararlı derneklerle, gerçek ve tüzel kişilerden gerekli yardım, bilgi, evrak, kayıt ve belgeleri istemeye yetkili olup, kanuni bir engel olmadıkça bu isteğin yerine getirilmesi zorunludur." hükmüne yer verilmiştir.

- Veri sorumlusu haberin altına yapılan kullanıcı yorumları ve bu yorumları yapan kimselerin IP adreslerini, kanuni yükümlülüklerini yerine getirmesi kapsamında ilgili veri sorumlusuna aktardığını beyan etmiştir.

Yukarıda verilen bilgiler çerçevesinde neticesinde Kişisel Verileri Koruma Kurulunun 03/03/2020 tarihli ve 2020/196 sayılı kararında;

Denetim için gerekli olan tüm bilgi ve belgelerin talep edilmesi şeklinde gerçekleşen kişisel veri işleme faaliyetinin, Kanunun 5 inci maddesinin 2 numaralı fıkrasının (a) bendinde yer alan "kanunlarda açıkça öngörülme" hükmü kapsamında olduğu, şirketin söz konusu verileri aktarmasının ise Kanunun 5 inci maddesinin 2 nci fıkrasının (ç) bendi hükmüne göre "veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması " hükmü kapsamında olduğu, bu çerçevede söz konusu verilerin bahse konu şirket tarafından, kamu kurumuna Kanunun 8 inci maddesinin 2 nci fıkrasının (a) bendi uyarınca aktarıldığı, ancak **söz konusu aktarım ile idari soruşturmanın konusu olmayan üçüncü kişilerin kişisel verilerinin** de veri sorumlusu şirket tarafından ilgili veri sorumlusuna aktarıldığı dikkate alındığında, idari soruşturma konusu olmayan kişisel verilerin aktarılmasının Kanunun 4 üncü maddesinin 2 numaralı fıkrasının (ç) bendinde yer alan "amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesine aykırı olduğu, bu hususun ise hukuka aykırı bir veri işleme faaliyeti olduğu bu itibarla Kanunun 12 nci maddesinin 1 numaralı fıkrasında yer alan veri güvenliğine ilişkin yükümlülükleri yerine getirmediği

değerlendirilen veri sorumlusu hakkında Kanunun 18 inci maddesinin 1 numaralı fıkrasının (b) bendi kapsamında 50.000 TL idari para cezası uygulanmasına,

- Kişisel veri aktarılan kamu kurumunun, denetim faaliyetlerinde 6698 sayılı Kanunun 4 üncü maddesinde yer alan Genel İlkeler başta olmak üzere kanun hükümlerine uyum hususunda azami dikkat ve özeni göstermesi, öte yandan, ve söz konusu soruşturma kapsamında elde edilmiş ve soruşturma konusuyla ilgili olmayan üçüncü kişilere ait kişisel verilerin Kanunun 7 nci maddesinde yer alan hükümler çerçevesinde silinmesi veya yok edilmesi ve sonucundan Kurula bilgi verilmesi hususlarında talimatlandırılmasına

karar vermiştir.

Risk Merkezindeki verilerin muhtelif faktoring şirketleri tarafından ihlal edildiğinin ihbar edilmesine ilişkin Kişisel Verileri Koruma Kurulunun 03.03.2020 Tarihli ve 2020/191, 2020/192, 2020/193 ve 2020/194 Sayılı Karar Özeti

Karar Tarihi : 03.03.2020

Karar No : 2020/191, 2020/192, 2020/193, 2020/194

Veri Sorumlusu: Muhtelif faktoring şirketleri

Konu Özeti : Risk Merkezindeki verilerin muhtelif faktoring şirketleri tarafından ihlal edildiğine ilişkin ihbar hakkında

Kuruma intikal eden ihbarda özetle; sorgu adetlerinde ilgi çekici değişim gözlemlenen Risk Merkezi üyeleri hakkında Risk Merkezi Yönetimi tarafından yapılan inceleme neticesinde, üyelerin bazı çalışanları tarafından Risk Merkezinden yapılan sorgulamaların kanunen yetkili olmayan kişilerle paylaşıldığının ve/veya amaç dışı kullanıldığının tespit edildiği belirtilmiştir. Konu hakkında başlatılan inceleme çerçevesinde;

- 5411 sayılı Bankacılık Kanununun “Risk Merkezi” başlıklı Ek 1 inci maddesinde;

“(1) Türkiye Bankalar Birliği nezdinde, kredi kuruluşları ile Kurulca uygun görülecek finansal kuruluşların müşterilerinin risk bilgilerini toplamak ve söz konusu bilgileri bu kuruluşlar ile gerçek veya tüzel kişilerin kendileriyle ya da onay vermeleri koşuluyla gerçek kişiler ve özel hukuk tüzel kişileri ile de paylaşılmasını sağlamak üzere Risk Merkezi kurulmuştur.

(2) Kredi kuruluşları ile Kurulca uygun görülecek finansal kuruluşlar, Risk Merkezine üye olmak zorundadır. Üye kuruluşlar, Risk Merkezince istenilen, müşterileri ile ilgili her türlü bilgiyi vermekle yükümlüdür. Risk Merkezi, bu yükümlülüğe uymayanlara bilgi akışını durdurmaya yetkilidir.

(...)

(4) Risk Merkezi yönetimi, Risk Merkezinin kuruluş amaçları doğrultusunda özel hukuk tüzel kişileri ile kamu kurum ve kuruluşlarından, kamu kurumu niteliğinde meslek kuruluşları ve bunların üst kuruluşlarından bilgi talep etmeye ve bunlarla Kurulun uygun görüşüne istinaden bilgi alış-verişine yönelik sözleşmeler imzalamaya yetkilidir. Özel hukuk tüzel kişileri ile kamu kurum ve kuruluşları, kamu

kurumu niteliğinde meslek kuruluşları ve bunların üst kuruluşları Risk Merkezi yönetimi tarafından talep edilen bilgileri vermekle yükümlüdürler. Kredi kuruluşları ile Kurulca uygun görülecek finansal kuruluşların müşterilerinin onay vermesi koşuluyla, Risk Merkezi ile bilgi alış-verişi sözleşmesi imzalayan özel hukuk tüzel kişileri ile kamu kurum ve kuruluşlarına kamu kurumu niteliğinde meslek kuruluşları ve bunların üst kuruluşlarına verilecek, müşterilerin bu kuruluşlar nezdindeki risk bilgileri Kanununun 73 üncü maddesinin dördüncü fıkrası kapsamında değerlendirilir.

(...)

(9) Risk Merkezinin bütün işlem ve kayıtları gizlidir. Sır sahibinin bilgilerinin açıklanması konusunda açıklı rızasının bulunması durumunda belirlediği kişiye risk bilgileri verilir. Kişinin rızasına dayanan bilgilerin verilmesine ilişkin usul ve esaslar, Kurulun ve Merkez Bankasının uygun görüşü, Türkiye Katılım Bankaları Birliğinin ve Kurulun belirleyeceği kurum ve kuruluşların görüşü alınarak Türkiye Bankalar Birliğince belirlenir ve Resmi Gazetede yayımlanır.

(10) Risk Merkezi nezdinde bulunan sır niteliğindeki bilgileri, bu konuda kanunen yetkili kılınan mercilerden başkalarına açıklayanlar, hukuka aykırı olarak kendisi ya da başkası yararına kullananlar, yayanlar, verenler, aktaranlar veya ele geçirenler hakkında 159 uncu madde hükümleri uygulanır. Bu fıkırada tanımlanan suçların bir tüzel kişinin faaliyeti çerçevesinde işlenmesi halinde, ilgili tüzel kişi hakkında Türk Ceza Kanununun tüzel kişilere özgü güvenlik tedbirlerine hükmolunur.

(11) Risk Merkezi, nezdindeki her türlü bilgi alış-verişini 73 üncü maddenin dördüncü fıkrası uyarınca en az beş banka tarafından kurulmuş şirketler aracılığı ile ve bu şirketlerle yapılacak sözleşmeler çerçevesinde de gerçekleştirebilir."

hükmüne yer verilmiş, bu çerçevede, Risk Merkezi tanımlanarak anılan merkezde yapılacak işlemler, sır saklama yükümlülüğü ve gizlilik gibi hususlara ilişkin ayrıntılar ilgili madde kapsamında düzenlenmiştir.

5411 sayılı Kanun'un 159 uncu maddesi ise sırların açıklanmasına ilişkin düzenlemeleri içermektedir. İlgili hüküm kapsamında;

"(1)Bu Kanununun 73 üncü maddesinin birinci ve üçüncü fıkralarında belirtilen yükümlülüğe uymayanlar için bir yıldan üç yıla kadar hapis ve bin günden ikibin güne kadar adli para cezası hükmolunur. Banka ve müşterilere ait sırları açıklayan üçüncü kişiler hakkında da aynı cezalar uygulanır.

(2) Yukarıdaki fıkırada belirtilen kimseler sırları kendileri ya da başkaları için yarar sağlamak amacıyla açıklamış olursa verilecek cezalar altıda bir oranında artırılır. Ayrıca, fiilin önemine göre sorumluların bu Kanun kapsamına giren kuruluşlarda görev yapmaları, iki yıldan aşağı olmamak üzere geçici veya sürekli olarak yasaklanır."

denilmek suretiyle anılan kanuna aykırı olarak sırları ifşa edenler hakkında ağır yaptırımlar öngörülmüş olup; sırların kendileri ya da başkaları için yarar sağlamak amacıyla açıklanmış olması durumunda da cezaların altıda bir oranında artırılacağı vurgulanmıştır.

Benzer şekilde, 5411 sayılı Kanununun 73 üncü maddesi sır yükümlülüğünü düzenlemektedir. “Sırların saklanması” başlıklı 73 üncü madde;

“ (1) Kurul başkan ve üyeleri ile Kurum personeli, Fon Kurulu başkan ve üyeleri ile Fon personeli görevleri sırasında öğrendikleri bankalara ve bunların bağlı ortaklık, iştirak, birlikte kontrol edilen ortaklıkları ve müşterilerine ait sırları bu Kanuna ve özel kanunlarına göre yetkili olanlardan başkasına açıklayamaz ve kendilerinin veya başkalarının yararlarına kullanamazlar. Kurumun dışarıdan destek hizmeti aldığı kişi ve kuruluşlar ile bunların çalışanları da bu hükme tâbidir. Bu yükümlülük görevden ayrıldıktan sonra da devam eder.

(...)

(3) Sıfat ve görevleri dolayısıyla bankalara veya müşterilerine ait sırları öğrenenler, söz konusu sırları bu konuda kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamazlar. Bu yükümlülük görevden ayrıldıktan sonra da devam eder. (...)

(4) Kurumun gözetim ve denetimine tabi kuruluşların, bunların ortaklarına, bağlı ortaklık, iştirak, birlikte kontrol edilen ortaklıklarının faaliyetlerine veya müşterilerine ilişkin yabancı ülke kanunlarına göre denetime yetkili ve Kurum muadili mercilerin taleplerinin Kurumca karşılanması, gizlilik sözleşmesi yapılması ve **sadece belirtilen amaçlar ile sınırlı kılınması koşuluyla** bankaların ve finansal kuruluşların, kendi aralarında doğrudan doğruya ya da risk merkezi veya en az beş banka ya da finansal kuruluş tarafından kurulacak şirketler vasıtasıyla yapacakları her türlü bilgi ve belge alışverişinin yanı sıra doğrudan veya dolaylı pay sahipliği yoluyla sermayelerinin yüzde onunu ve daha fazlasını temsil eden paylarının satışı amacıyla muhtemel alıcıların yapacakları değerlendirme çalışmalarında ya da sermayelerinin yüzde on veya daha fazlasına sahip olan yurt içinde veya yurt dışında yerleşik kredi kuruluşu ile finansal kuruluşlar da dâhil ana ortaklıkların konsolide finansal tablo hazırlama çalışmalarında, risk yönetimi ve iç denetim uygulamalarında veya kredileri de dâhil varlıklarının ya da bunlara dayalı menkul kıymetlerin satışı amacıyla yapılacak değerlendirme çalışmalarında ya da değerlendirme, derecelendirme veya destek hizmeti alınması ile bağımsız denetim faaliyetlerinde ve gerekli tedbirlerin alınması kaydıyla hizmet alımlarına yönelik işlemlerde kullanılmak üzere bilgi ve belge taleplerinin karşılanması sırasında banka ya da müşteri sırrı niteliğindeki bilgilerin öğrenilmesi sır saklama yükümlülüğü dışındadır.”

hükmünü amirdir. Anılan maddenin dördüncü fıkrasında yer alan hüküm ile sır saklama yükümlülüğünün istisna olduğu durumlar, “sadece belirlenen amaçlar ile sınırlı kılınması koşuluyla” söz konusu olmaktadır. Yani, amacı dışında işlenecek her türlü veri, istisna kapsamı dışında

değerlendirilecektir. Nitekim söz konusu ihbara konu olan eylemlerde de ihlale sebebiyet verdiği iddia olunan kişiler, belirtilen amaçlar ile sınırlı kalmaksızın birçok gerçek ve tüzel kişiye ilişkin verilere erişmiş; üstelik bazıları bu verileri de yetkisiz üçüncü kişilere aktarmışlardır. Anılan sebeplerle, söz konusu eylemlerin 5411 sayılı Kanunu da ihlal ettiği değerlendirilmektedir.

• Benzer şekilde, Türkiye Bankalar Birliği Risk Merkezi Yönetmeliği (**Risk Merkezi Yönetmeliği**), TBB Risk Merkezinin kuruluşuna, faaliyetine ve çalışmasına, Türkiye Bankalar Birliği Risk Merkezi yönetiminin oluşumuna, toplanmasına ve karar almasına, Türkiye Bankalar Birliği Risk Merkezine verilen bilgilerin kapsam, biçim ve içeriğine ve bunların paylaşılmasına, paylaşılacak bilgilerin kapsam ve içeriğine, ücretlendirilmesine ve üyelere ödenecek aidatların belirlenmesine ilişkin usul ve esasları düzenlemektedir. Risk Merkezi Yönetmeliği'nin "Tanımlar" başlıklı 3 üncü maddesinin birinci fıkrasının (j) bendi uyarınca üye; *"kredi kuruluşları ile Türkiye Bankalar Birliği Risk Merkezine Kurul tarafından üye olması uygun görülen her bir finansal kuruluş"* olarak tanımlanmıştır. Bu kapsamda, ihbara konu olan faktoring şirketlerinin her biri üye niteliğini haizdir. Yine, Risk Merkezi Yönetmeliği'nin "Risk Merkezi üyelerinin sorumlulukları" başlıklı 17 nci maddesinin birinci fıkrasının (b) ve (c) bentleri kapsamında üyeler, Risk Merkezi ile gizlilik sözleşmesi yapmak ve Risk Merkezinden temin ettiği her türlü bilgi ve belgenin gizliliğinin sağlanmasına yönelik her türlü önlemi almak ve Risk Merkezinden temin ettiği bilgileri yalnızca kendi iç işlemlerinde kullanmak, diğer üyeler dahil herhangi bir gerçek ve tüzel kişi ile paylaşmamak ile sorumlu tutulmuştur. Ayrıca, "Gizlilik" başlıklı 19 uncu madde uyarınca;

"(1) Risk Merkezinin tüm işlem ve kayıtları gizlidir. Risk Merkezinden temin edilen bilgiler yalnızca bilgiyi alan üyenin kendi iç işlemlerinde kullanılabilir, diğer üyeler dahil herhangi bir gerçek ve tüzel kişi ile paylaşamaz.

(2) Risk Merkezi nezdinde bulunan sır niteliğindeki bilgileri, bu konuda kanunen yetkili kılınan mercilerden başkalarına açıklayanlar, hukuka aykırı olarak kendisi ya da başkası yararına kullananlar, yayanlar, verenler, aktaranlar veya ele geçirenler hakkında Kanununun 159 uncu maddesi hükümleri uygulanır."

hükmü düzenlenmiştir. Bu doğrultuda, Risk Merkezi'nde bulunan sır nitelikli bilgilerin kanunen yetkili kılınan mercilerden başkalarına açıklanması durumunda 5411 sayılı Kanununun 159 uncu maddesinde öngörülen yaptırımların uygulanacağı belirtilmiştir.

Ayrıca, "Türkiye Bankalar Birliği Risk Merkezi Üyelerinin Müşterilerinin Risk Merkezi Nezdindeki Bilgilerinin Kendilerine ya da Onay Vermeleri Koşuluyla Belirledikleri Gerçek veya Tüzel Kişilere Verilmesine İlişkin Esas ve Usuller Hakkında Yönetmelik" kapsamında, TBB Risk Merkezi üyelerinin müşterilerinin TBB Risk Merkezi nezdindeki bilgilerinin, kendilerine ya da onay vermeleri koşuluyla

belirledikleri gerçek veya tüzel kişilere verilmesini teminen başvuru ve onay verme sürecine ilişkin esas ve usuller düzenlemektedir. Diğer bir ifade ile, Risk Merkezindeki bilgilerin ne şekilde sorgulanabileceği ve temin edilebileceği hususları da ayrı bir yönetmelik kapsamında düzenlenmektedir.

• 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) “Genel ilkeler” başlıklı 4 üncü maddesinde, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği ve kişisel verilerin işlenmesinde maddede; “a) Hukuka ve dürüstlük kurallarına uygun olma. b) Doğru ve gerektiğinde güncel olma. c) Belirli, açık ve meşru amaçlar için işlenme. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.” şeklinde sayılan ilkelere uyulmasının zorunlu olduğu düzenleme altına alınmıştır. Bu ilkelere kişisel verilerin “belirli, açık ve meşru amaçlar için işlenme” ilkesi, **kişisel veri işleme faaliyetlerinin ilgili kişi tarafından açık bir şekilde anlaşılır olmasını, kişisel veri işleme faaliyetinin hangi hukuki işleme şartına dayalı olarak gerçekleştirildiğinin tespit edilmesini, kişisel veri işleme faaliyetinin ve gerçekleştirilme amacının belirliliğini sağlayacak detayda** ortaya konulmasını sağlar. Amacın meşru olması, veri sorumlusunun işlediği verilerin, yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması anlamına gelmektedir. Bir diğer önemli ilke olan “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması” ilkesine göre, işlenen veriler belirlenen amaçların gerçekleştirilmesine elverişli olmalı, amacın gerçekleştirilmesiyle ilgili olmayan veya sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik veri işleme yoluna gidilmemelidir. Burada önemli olan, amacı gerçekleştirmeye yönelik yeterli verinin temin edilmesi, bunun dışındaki amaç için gerekli olmayan veri işlemeden kaçınılmasıdır. Ölçülülük ilkesi ise, veri işleme ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması yani veri işlemenin, amacı gerçekleştirecek ölçüde olması demektir. Anılan madde hükmünden açıkça anlaşılacağı üzere, **kişisel verilerin işlenmesinde her hal ve şartta Kanunun 4 üncü maddesinde sayılan genel ilkelere uyulması hukuki bir gerekliliktir.** Kanundaki düzenlemede yer alan “belirli, açık ve meşru amaçlar için işlenme” ve “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması” ilkeleri ile 5411 sayılı Kanunun 73 üncü maddesinin dördüncü fıkrasında yer verilen “sadece belirlenen amaçlar ile sınırlı kılınması koşuluyla” şartı benzerlik göstermektedir. Dolayısıyla, somut olay değerlendirilirken anılan kişisel verilerin işlenmesine ilişkin ilkeler özellikle önem teşkil edecektir.

• Kanunun 3 üncü maddesinin birinci fıkrasının (d) bendi uyarınca *kişisel veri; kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi*, (e) bendi uyarınca *kişisel verilerin işlenmesi; kişisel*

verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi, (ç) bendi uyarınca ilgili kişi; kişisel verisi işlenen gerçek kişiyi, (ı) bendi uyarınca veri sorumlusu; kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişiyi ifade etmektedir. Buna göre, ihbara konu olan factoring şirketleri veri sorumlusu niteliğini haiz olup ihlal iddiasına konu eylemler bakımından şirket çalışanı kişisel veri işleme faaliyetinde bulunmuştur. Bu veri işleme faaliyetinin de yetki sınırını aşmak suretiyle hukuka aykırı bir şekilde gerçekleştiği değerlendirilmektedir.

- Kanununun 12 nci maddesinin beşinci fıkrasında ise, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunun bu durumu en kısa sürede ilgisine ve Kurula bildireceği, Kurulun, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebileceği hükme bağlanmıştır. Ayrıca, Kurumumuz resmi internet sitesinde yayımlanan 24.01.2019 tarih ve 2019/10 sayılı Kurul kararıyla “en kısa sürede” ibaresinin “72 saat” olarak yorumlanmasına ve bu kapsamda veri sorumlusunun bu durumu öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirmesine, veri sorumlusunca söz konusu veri ihlalden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabilirse doğrudan, ulaşamazsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılmasına karar verilmiştir.

Bu itibarla;

Risk Merkezi üzerinden yapılan sorgu adetlerinde dikkat çekici değişiklik gözlenen Factoring Şirketleri hakkında Kurulumuza yapılan ihbarın incelenmesi neticesinde, ihbara konu kişisel veri işleme faaliyetlerinde; Kanununun 4 üncü maddesinde sayılan genel ilkelere riayet edilmediği; söz konusu faaliyetlerin Kanununun 12 inci maddesinin birinci fıkrasında düzenlenen kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak yükümlülüklerine aykırılık teşkil ettiği tespit edilmiş ve **veri ihlalinin süresi, veri ihlalden etkilenen kişi sayısı, ihlale ilişkin bildirimde bulunulmaması dikkate alınarak; Kişisel Verileri Koruma Kurulunun 03/03/2020 tarih ve 2020/191, 2020/192, 2020/193, 2020/194 kararları ile söz konusu 4 şirket hakkında**

- Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sađlamaya yönelik gerekli tedbirleri almadıkları gerekçesiyle Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi çerçevesinde toplam 950.000 TL,
- Kanunun 12 nci maddesinin (5) numaralı fıkrası uyarınca ihlale ilişkin Kuruma ve ilgili kişilere bildirim yapılmadığı gerekçesiyle Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi çerçevesinde toplam 450.000 TL

idari para cezası uygulanmasına karar verilmiştir.

2020/187 sayılı KVKK Kararı

İlgili kişinin oturmakta olduğu binaya, komşusu tarafından kamera yerleştirilerek kayıt ve izleme gerçekleştirilmesi hakkında Kişisel Verileri Koruma Kurulunun 27/02/2020 tarihli ve 2020/187 sayılı Karar Özeti

Karar Tarihi : 27.02.2020

Karar No : 2020/187

Konu Özeti : İlgili kişinin oturmakta olduğu binaya, komşusu tarafından kamera yerleştirilerek kayıt ve izleme gerçekleştirilmesi hakkında

Kuruma intikal eden şikâyet dilekçesinde özetle; ilgili kişinin oturmakta olduğu bina içerisine komşusu tarafından 2 tanesi dışarıyı, 1 tanesi apartman girişini, 1 tanesi kat arasını gösterecek şekilde 4 tane kamera yerleştirildiği, bu kameralarla kayıt ve izleme gerçekleştirildiği, kişilerin huzur ve sükûnunu bozma, hukuka aykırı olarak kişisel verileri kaydetme, özel hayatın gizliliğini ihlal etme suçlarının işlendiği, kameraları yerleştiren komşu hakkında savcılığa da şikâyette bulunulduğu ifade edilerek gereğinin yapılması, şahsın cezalandırılması ve kamera görüntülerinin tarafına iadesi talep edilmektedir.

Konuya ilişkin yapılan değerlendirme neticesinde, Kişisel Verileri Koruma Kurulunun 27/02/2020 tarihli ve 2020/187 sayılı kararı ile;

• 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 15 inci maddesinin birinci fıkrasında Kişisel Verileri Koruma Kurulunun, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapacağı; aynı maddenin ikinci fıkrasında ise; 1/11/1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesinde belirtilen;

a) Belli bir konuyu ihtiva etmeyen,

b) Yargı mercilerinin görevine giren konularla ilgili olan,

c) 4 üncü maddede gösterilen şartlardan (dilekçe sahibinin adı soyadı ve imzası ile iş veya ikametgâh adresi) herhangi birini taşımayan

ihbar veya şikâyetlerin incelemeye alınmayacağına hükme bağlandı,

Kanunun 17 nci maddesinin birinci fıkrasında kişisel verilere ilişkin suçlar bakımından 26/09/2004 tarih ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümlerinin uygulanacağına belirtildi,

- Türk Ceza Kanununun 135 inci maddesinde hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verileceğinin, 136 ncı maddesinde ise kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişinin, iki yıldan dört yıla kadar hapis cezası ile cezalandırılacağına hükme bağlandı,

hususlarından hareketle,

- İlgili kişinin, komşusu hakkındaki hukuka aykırı olarak kamera taktırılması ve görüntü kaydı alınmasına ilişkin şikâyetlerinin Türk Ceza Kanunu hükümleri çerçevesinde suç unsuru barındırabileceği ve bu çerçevede 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesi dikkate alınarak söz konusu şikâyetin Kanun kapsamında değerlendirilemeyeceğine karar verilmiştir.

2020/173 sayılı KVKK Kararı

Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/173 Sayılı Karar Özeti

Karar Tarihi : 27.02.2020

Karar No : 2020/173

Veri Sorumlusu: Amazon Turkey Perakende Hizmetleri Limited Şirketi

Konu Özeti : Amazon Turkey Perakende Hizmetleri Limited Şirketince işlenen kişisel veriler hakkında yapılan başvuru

Kurumumuza intikal eden bir ihbar dilekçesinde ve eklerinde özetle;

- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun (6563 sayılı Kanun) uyarınca hizmet sağlayıcı ve aracı hizmet sağlayıcı niteliğinde olan www.amazon.com.tr üzerinden yürütülen faaliyetlerin kişisel verilerin korunması mevzuatına uygun olması gerektiği; ancak ilgili site üzerinden yürütülen faaliyetler ile mevzuatın ihlal edildiği,
- Amazon.com.tr internet sitesi ve bağlı uygulamalar aracılığıyla sunulan hizmetlere ilişkin olarak ne üyelik hesabı oluşturulurken ne de alışveriş yapılırken, reklam, kampanya veya promosyon amacıyla elektronik ticari ileti gönderebilmek için açık rıza alınmadığı, açık rıza dışında bir işleme nedeninin varlığına ilişkin açıklama yapılmadığı,
- Sitenin "Kullanım ve Satış Şartları" sayfasının girişinde "*Amazon Europe Core SARL, Amazon Turkey Perakende Hizmetleri Limited Şirketi vel/veya iştirakleri ("Amazon"), Amazon.com.tr' yi (internet sayfası) ziyaret ettiğinizde veya burada alışveriş yaptığınızda, Amazon ürünlerini veya hizmetlerini kullandığınızda, mobil Amazon uygulamalarını kullandığınızda veya yukarıdakilerle bağlantılı olarak Amazon tarafından sunulan hizmetleri kullandığınızda (toplu olarak "Amazon Hizmetleri") size internet sayfası özellikleri ve diğer ürünler ve hizmetler sunmaktadır. Amazon Hizmetleri aracılığıyla kişisel bilgilerinizin nasıl toplandığını ve işlendiğini anlayabilmek adına lütfen Gizlilik Bildirimimizi ve Çerezler Bildirimimizi inceleyin.*" ifadesine yer verildiği,

- Elektronik İletişimler başlıklı birinci maddede “Herhangi bir Amazon Hizmeti’ni kullandığınızda veya masaüstünüzden veya mobil cihazınızdan bize e-postalar, SMS veya diğer iletişimler gönderdiğinizde bizimle elektronik olarak iletişim kurmuş olursunuz. Sizinle, örneğin e-posta, SMS, uygulama içi anlık iletişimler gibi çeşitli şekillerde veya internet sayfasında e-posta mesajları veya iletişimler göndererek veya yayınlayarak veya Mesaj Merkezimiz gibi diğer Amazon Hizmetleri aracılığıyla elektronik olarak iletişim kuracağız. Sözleşmesel amaçlı olarak, bizden elektronik olarak iletişim almaya onay vermektedir ve size elektronik olarak temin ettiğimiz tüm sözleşmelerin, bildirimlerin, açıklamaların ve diğer iletişimlerin, uygulanan kanunlar farklı bir iletişim şeklini öngörmediği sürece, söz konusu iletişimlerin yazılı olmasına ilişkin her türlü yasal gerekliliğe uygunluk gösterdiğini kabul etmektedir.” ifadesinin kullanıldığı,
- Bu ifadeler birlikte değerlendirildiğinde, amazon.com.tr sitesini sadece ziyaret eden bir kişinin ilgili hükümleri kabul ettiği ve sadece internet sitesini ziyaret etmekle elektronik olarak iletişim almaya onay verdiği şeklinde bir uygulamaya gidildiğinin görüldüğü,
- Amazon hizmetini kullanmak suretiyle elektronik iletişime onay vermiş sayılmanın ve bu nedenle kullanıcılara elektronik ticari ileti göndermenin 6698 sayılı Kanunun 5’inci maddesinin 2’inci fıkrasında yer alan “bir sözleşmenin kurulması ve ifasıyla doğrudan doğruya ilgili olması kaydıyla gerekli olma” şeklindeki hukuka uygunluk sebebi kapsamında değerlendirilemeyeceği,
- Alışveriş yapabilmek için zorunlu olan üye hesabı oluşturulması amacıyla “Kullanım ve Satış Şartları”nı kabul ederek elektronik iletişim izni verilmiş sayılmanın özgür irade ile verilmiş bir açık rıza olarak değerlendirilemeyeceği, nitekim Kişisel Verileri Koruma Kurumu (Korum) internet sitesinde yer verilen karar özetleri bölümünde, “Açık rızanın Hizmet Şartına Bağlanması” başlığı altında hizmetin açık rıza şartına bağlanmış olmasının açık rızayı sakatlayacağı belirtilmiştir,
- amazon.com.tr “Gizlilik Bildirimi” sayfasının “Amazon Kişisel Bilgilerinizi Paylaşıyor mu?” kısmının “Kişisel Bilgilerin Türkiye Dışına Aktarılması” alt başlığı altında “Kişisel bilgilerinizi saklamak ve işbu Gizlilik Bildirimi’nde açıklanan amaçlar çerçevesinde işlemek için Avrupa Birliği’ne ve Avrupa Birliği’nden Amerika Birleşik Devletleri’ne aktarabiliriz.” şeklindeki ifadeden kişisel verilerin yurt dışına aktarıldığının anlaşıldığı; ancak hâlihazırda amazon.com.tr internet sitesi ve bağlı mobil uygulamalar aracılığı ile sunulan hizmetlere ilişkin ne üyelik hesabı oluşturulurken ne de alışveriş yapılırken, kişisel verilerin yurt dışına aktarılması için açık rıza alınmadığı,
- Yurt dışına aktarıma ilişkin olarak Kurul izni alınmamış ise, herhangi bir açık rıza da alınmadığından 6698 sayılı Kanunun 9’uncu maddesinin ihlal edilmiş olacağı, bunun da Kurulca yapılacak inceleme ile ortaya çıkarılabileceği

ifade edilerek, yukarıda belirtilen hususlar doğrultusunda konunun Kurumumuzca incelenmesi ve gereğinin yapılması talep edilmektedir.

Söz konusu başvuruya ilişkin olarak Kişisel Verileri Koruma Kurulunun 16.05.2019 tarih ve 2019/140 sayılı Kararı ile resen inceleme başlatılmasına karar verilmiş olup, Kurumumuz tarafından 27.06.2019 tarihli dilekçede belirtilen iddialar ile ilgili olarak gerekli incelemelerin yapılabilmesini teminen veri sorumlusundan söz konusu iddialar karşısındaki savunması ve savunmasına esas bilgi ve belgeler istenilmiştir.

Veri sorumlusundan 17.07.2019 tarihinde alınan yazıda ise özetle;

- Hukuka aykırı olarak ticari elektronik ileti gönderildiğine ilişkin iddiaların dayanaktan yoksun olduğu, herhangi bir kanıtlayıcı belgeye dayanmadığı ve başvuranın söz konusu taleplerini Ticaret Bakanlığına iletmesi gerektiği,
- Kurulun ticari elektronik iletiler gibi ilke kararlarını ve Kurulun bu alandaki yetkisini kabul etmek ve saygı göstermekle birlikte, konuya ilişkin usul ve esasların münferiden elektronik ticarete ilişkin mevzuat kapsamında düzenlenmiş olduğu, ihbar edenin bu mevzuat kapsamındaki şikayet mekanizmasını kullanmak yerine şikayetini varsayımsal tahminlere dayandırarak Kurumumuza iletmiş olduğu,
- Amazon Turkey'in, müşterilerinin kişisel verilerini yürürlükteki mevzuata uygun işlemek konusunda şeffaflık sağlamak amacıyla "Kullanım Koşulları" ve "Gizlilik Bildirimi" metinlerini sunduğu,
- Yalnız hesap oluşturulmasından sonra kayıtlı müşterilerle Amazon ürün ve hizmetlerine ilişkin elektronik iletişim kurulduğu; Amazon hesabı oluşturulduğunda ilgili müşterinin "Amazon Hesabınızı Oluşturun" sekmesine tıklayarak "Gizlilik Bildirimi"ni de kabul ettiği ("*Hesap oluşturarak işbu Gizlilik Bildirimi'nde belirtilen uygulamaları kabul etmektesiniz.*"); aynı şekilde kayıtlı bir müşteri site üzerinden sipariş verdiğinde kendisine "Gizlilik Bildirimi"nin kabul edildiğine dair tekrar hatırlatma yapıldığı ("*Sipariş verdiğinizde Amazon.com.tr'nin Gizlilik Bildirimini, Kullanım ve Satış Koşullarını ve Çerez Bildirimini kabul etmiş olursunuz.*"),
- Amazon Turkey'in ayrıca kayıtlı müşterilerine ticari elektronik ileti almak istedikleri alanları kolayca seçmeleri, sınırlandırmaları veya diledikleri zaman ticari elektronik ileti almayı reddetmeleri için imkan sağladığı,
- Kayıtlı müşterilerin kişisel verilerinin Türkiye dışına aktarıldığından/aktarılabileceğinden sadece haberdar olmadığı ayı zamanda "Gizlilik Bildirimi"ni onaylayarak bu hususu kabul etmiş olduğu,

- Amazon Turkey'in yurt dışına veri aktarım taahhütnameleri ile ilgili yazışmaların Kurumumuzla sürdürülmekte olduğu,
- Yukarıda yer alan açıklamalar ışığında Amazon Turkey'in kişisel verileri yurtdışına hukuka aykırı aktardığı, e-ticaret mevzuatına aykırı hareket ettiği iddialarının asılsız olduğu ve varsayımlara dayandığı

ifade edilerek, ihbarın dayanaktan yoksun olması nedeniyle reddedilmesi gerektiği belirtilmiştir.

Öte yandan, konuya ilişkin olarak Kurumumuza ihbarda bulunan şahsın Ticaret Bakanlığı'na yapmış olduğu Amazon.com.tr uygulamalarının elektronik ticaret ve kişisel verilerin korunması mevzuatı hükümlerine aykırılık teşkil ettiği yönündeki başvurusu Bakanlığın 17.04.2019 tarihli 43541135 sayılı yazısı ile "konunun KVKK çerçevesinde değerlendirilmesi" talebiyle Kurumumuza iletilmiştir.

Kurumumuza intikal eden ihbar, ilgili kişinin iddiaları, veri sorumlusundan alınan bilgi ve belgeler ve ilgili mevzuat hükümleri çerçevesinde aşağıda başlıklar halinde değerlendirilmiştir.

1. 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 5'inci maddesinin (1) numaralı fıkrası hükmü gereğince kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. Maddenin (2) numaralı fıkrasında ise, ilgili kişinin açık rızası olmaksızın kişisel verilerin hangi hallerde işlenebileceği düzenlenmiştir.

Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmeliğin 5'inci maddesinin (1)'nci fıkrası hükmü gereğince hizmet sağlayıcının, mal ve hizmetlerini tanıtmak, pazarlamak, işletmesini tanıtmak ya da kutlama ve temenni gibi içeriklerle tanınırlığını artırmak amacıyla alıcıların elektronik iletişim adreslerine gönderdiği ticari elektronik ileteler için kendisi tarafından önceden onay alınır. Onay, reddetme hakkı kullanılıncaya kadar geçerlidir. Bu madde kapsamında alınacak onayın ise yine Yönetmeliğin 7'inci maddesinin (1)'inci fıkrası hükmü gereğince yazılı olarak veya her türlü elektronik iletişim aracıyla alınabilmesi öngörülmüştür. Onayda ise alıcının ticari elektronik ileti gönderilmesini kabul ettiğine dair olumlu irade beyanı, adı ve soyadı ile elektronik iletişim adresi yer alır. Yine bu doğrultuda Yönetmeliğin 12'inci maddesinin (2)'nci fıkrası gereğince kişisel verilerin; üçüncü kişilerle paylaşılabilmesi, işlenebilmesi ve başka amaçlarla kullanılabilmesi için ilgili kişiden önceden onay alınması gerekir.

Kişilerin iletişim bilgilerinin pazarlama amaçlı ileteler göndermeden önce veya en geç elektronik ileti gönderme onayının alındığı sırada işlenmesinin Kanunun 5'inci maddesinde yer alan işleme şartlarından açık rıza kapsamında olduğu değerlendirilmekte olup, ilgili kişilerin açık rızaları veya Kanunun 5'inci maddesinin 2'nci fıkrasında yer alan işleme şartlarından herhangi biri olmaksızın e-postalarına veya telefonlarına ileteler gönderilmesi Kişisel Verileri Koruma Kurulunun 16.10.2018

tarikh ve 2018/119 sayılı İlke Kararında da düzenlenerek belirtilen şekilde faaliyetinde bulunan veri sorumluları hakkında Kanunun 18'inci maddesi kapsamında işlem tesis edileceđi hususu belirtilmiştir.

Veri Sorumlusunun iddiası, ticari elektronik iletilerin Elektronik Ticaretin Düzenlenmesi Hakkında Kanun ve Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik hükümleri kapsamında değerlendirilmesi gerektiđi ve söz konusu mevzuat kapsamında şikayet mekanizmasının Ticaret Bakanlığının sorumluluğunda olduđu, şikayet başvurusunda bulunabilmek için gerekli hususların Kurumumuza intikal ettirilen başvuruda yer almadığı ve bu konudaki sorumluluğun da Kurumumuzda olmadığı yönündedir.

Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmeliğin amacı, 1'inci maddede, *“elektronik iletişim araçlarıyla yapılan ticari iletişime dair bilgi verme yükümlülüklerine ve ticari elektronik iletilerde uyulması gereken hususlara ilişkin usul ve esasları düzenlemek”* olarak belirlenmiş olup, yönetmeliğin tanımlar başlıklı 4'üncü maddesinde ticari elektronik ileti, *“Telefon, çağrı merkezleri, faks, otomatik arama makineleri, akıllı ses kaydedici sistemler, elektronik posta, kısa mesaj hizmeti gibi vasıtalar kullanılarak elektronik ortamda gerçekleştirilen ve ticari amaçlarla gönderilen veri, ses ve görüntü içerikli iletiler”* olarak tanımlanmıştır.

Ticari elektronik iletiye ilişkin ayrı bir mevzuat bulunmakla birlikte, telefon numarası, e-posta adresi gibi bilgilerin bir veri kayıt sisteminde depolanması suretiyle kişilere ticari nitelikli iletiler gönderilmesi, bir kişisel veri işleme faaliyetine işaret etmektedir. Dolayısıyla ticari nitelikli bir elektronik iletinin ticari elektronik ileti gönderilmesine ilişkin mevzuata uygun olarak gönderilmesi gerekmektedir, bu mesajların iletilmesi için kullanılan iletişim kanallarının kişisel veri niteliğinde olması nedeniyle ticari elektronik iletilerin gönderilmesi süreçlerinin aynı zamanda kişisel verilerin korunması mevzuatına da uygun olması gerekmektedir. Bu bağlamda, Kurulun konuya ilişkin almış olduđu ilke kararı, ticari elektronik iletilerin gönderilmesine ilişkin değil, kişisel verilerin işlenmesi süreçlerine ilişkin bir karardır.

Somut olayda, veri sorumlusu hakkında Kurumumuza ihbarda bulunan şahıs tarafından Kurumumuzun yanı sıra Ticaret Bakanlığına da başvuruda bulunulmuş olup, Ticaret Bakanlığı söz konusu başvuruyu *“kişisel verilerin korunması mevzuatı kapsamında değerlendirilmek üzere”* Kurumumuza intikal ettirmiş olup, bu durumun, söz konusu başvurunun kişisel verilerin korunması düzenlemeleri bağlamında ele alınması gerekliliğini ortaya koyduđu değerlendirilmektedir.

Diğer yandan, Kurumumuz tarafından veri sorumlusu şirkete yönelik başlatılan inceleme, Kurumumuza intikal eden ihbarın değerlendirilmesini müteakip, Kanunun 15'inci maddesinin 1 numaralı fıkrasında verilen yetki çerçevesinde Kurulun resen başlatmış olduğu bir incelemedir.

Tarafımızca yapılan incelemede, www.amazon.com.tr sayfasında bir üyelik profili oluşturulmak suretiyle, iletişim bilgisinin pazarlama amaçlı iletiler gönderilmesi amacıyla işlenmesi hususunda ilgili kişilerin açık rızasının alınıp alınmadığı kontrol edilmiş olup, üyelik yapılabilmesi için gerekli bilgilerin girilmesi sırasında herhangi bir açık rıza alınmadığı, üyelik sürecinin tamamlanmasının ardından girilen "Hesabım" sekmesinde "İletişim Tercihleri" bölümünde Genel Ayarlar" başlığında, "e-postalar şu anda E-posta adresine gönderiliyor" açıklamasının yer aldığı, "Promosyon E-postaları" başlığına tıkladığında ise "haberdar olmak istediğiniz tüm iletişim kategorilerini seçin" ifadesine yer verilmekle birlikte, 10 adet başlığın önceden tıklanmış olarak ekranda belirlediği, bu bölümün en altında ise "lütfen bana artık pazarlama e-postaları göndermeyin" kutucuğunun yer aldığı görülmektedir.

Kanunun Tanımlar başlıklı 3'üncü maddesinin 1 numaralı fıkrasının (a) bendinde açık rıza, belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür irade ile açıklanan rıza" olarak tanımlanmıştır. Kanunda yer verilen tanım çerçevesinde veri sorumluları tarafından ilgili kişilerden alınacak açık rıza beyanlarında opt-out yani bireyin önceden onayını almaksızın kişisel verilerinin işlenmesine otomatik onay verdiklerinin kabul edildiği ve kişilere bu onayı kaldırmaları yönünde imkân veren bir sistemin değil, opt-in yani bireyin bilinçli eylemi ile kişisel verilerinin işlenmesine onay vereceği bir sistemin kullanılması gerekmektedir.

Veri sorumlusunca Gizlilik Bildiriminde yapılan açıklamada, "Amazon.com.tr'yi ziyaret ederek işbu Gizlilik Bildiriminde belirtilen uygulamaları kabul etmekte ve onaylamaktasınız" ifadesinin yer aldığı, böylece ilgili kişilerin kişisel verilerinin işlendiğinden sadece haberdar olmadığı ayı zamanda "Gizlilik Bildirimi"ni onaylayarak bu hususu kabul etmiş olduğu iddiası yer almaktadır. Ancak, üyelik oluşturulurken herhangi bir aşamada açık rıza alınması yoluna gidilmediği tarafımızca yapılan incelemede tespit edilmiştir. Gizlilik bildirimindeki ifade, aydınlatma yapılırken aynı zamanda kişilerden açık rıza alınması yoluna gidildiği izlenimini yaratmaktadır. Bilindiği üzere açık rıza dışında işleme nedenlerinin varlığı halinde açık rıza alınması yoluna gidilmesi, dürüstlük kuralına aykırılık şeklinde yorumlandığı gibi, diğer yandan açık rıza gerektiren veri işleme süreçleri bakımından da aydınlatmanın yapılması ile açık rızanın alınmasının birlikte yapılması yürürlükteki mevzuata uygun kabul edilmemektedir. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin 5'inci maddesinin 1'inci fıkrasının (f) bendinde, kişisel

veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerektiği düzenlenmiştir. Bu kapsamda veri sorumlusunca web sitesinde yayımlanan “Gizlilik Bildirimi”, birçok bilgi içermesi, veri işlemeye ilişkin genel bir bilgilendirme olması nedeniyle kişisel verilerin işlenmesine ilişkin ilgili kişilere aydınlatma yapıldığı ve açık rıza alındığı anlamına gelmemektedir.

Bu kapsamda, veri sorumlusunun ilgili kişilerin iletişim bilgilerini işlemek suretiyle ticari elektronik ileti göndermek hususunda ilgili kişilerin açık rızasını almadığı, açık rıza dışında da bir işleme nedenine dayanmadığı dikkate alındığında Kanunun 12’nci maddesinde yer alan kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri alma yükümlülüğünü yerine getirmediği kanaatine varılmaktadır.

2. Yine Kanunun 4’üncü maddesinin 2 numaralı fıkrası hükmü gereğince *kişisel verilerin işlenmesinde “hukuka ve dürüstlük kurallarına uygun olma”, “belirli, açık ve meşru amaçlar için işlenme” ve “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma”* ilkelerine uyulması zorunludur.

Veri sorumlusu, “Gizlilik Bildirimi” metninde “Belirli bilgileri vermemeyi tercih edebilirsiniz, ancak bu durumda Amazon Hizmetlerinin çoğundan yararlanamazsınız.” ya da “Çerezlerimizi engellerseniz veya reddederseniz alışveriş sepetinize ürün ekleyemez, satın alma aşamasına geçemez veya oturum açmanızı gerektiren herhangi bir Amazon hizmetini kullanamazsınız.” diyerek kişisel verilerin işlenmesini hizmet şartına bağlamaktadır. Kurumumuzun internet sayfasında da yayımlanan kararda sözleşmenin taraflarına ait kişisel veri işlenmesi durumunda ayrıca açık rıza alınması ve de açık rızayı üyeliğin ve hizmetin dolayısıyla sözleşmenin bir koşulu olarak dayatılmasının; diğer kişisel veri işleme şartlarının varlığı durumunda açık rıza alınmasının ilgili kişinin yanıtılması ve yanlış yönlendirilmesi dolayısıyla veri sorumlusunca hakkın kötüye kullanılması anlamına geleceği ve ayrıca hizmetin açık rıza şartına bağlanmış olmasının açık rızayı sakatlayacağı dikkate alındığında, bu durumun Kanunun 4’üncü maddesinde yer alan hukuka ve dürüstlük kurallarına uygun olma ve işlenme amacı ile bağlı, sınırlı ve ölçülü olma ilkelerine aykırılık teşkil ettiği değerlendirilmektedir.

Amazon.com.tr’nin topladığını beyan ettiği veriler ise şunlardır: “ad, adres, telefon numarası, ödeme bilgileri; yaş; konum bilgisi; satın alımların gönderildiği kişiler; 1-Tık ayarlarında listelenen kişiler (adresler ve telefon numaraları dâhil); arkadaşların ve diğer kişilerin e-posta adresleri; veri sorumlusuna gönderilen değerlendirmelerin ve e-postaların içeriği; profildeki kişisel bilgiler ve fotoğraflar; Amazon hizmetleri ile bağlantılı olarak saklanan resimler ve video, kimlik ve duruma ilişkin bilgiler ve belgeler; kurumsal ve finansal bilgiler; kredi geçmişi bilgileri; KDV numaraları.” İlgili kişinin arkadaşlarının bilgileri, kendisi

bakımından kişisel veri olmakla birlikte ayrıca bu bireylere ait birer kişisel veri niteliğini de taşımaktadır. Böylece üye ile Amazon.com.tr arasında bir sözleşmenin ifası veya üyenin açık rızası kapsamında, üyenin temas kişilerine ait e-posta adresleri de bu kişilerin açık rızalarına dayanmaksızın işlenmektedir. Öte yandan “kredi geçmişi bilgileri, duruma ilişkin bilgiler, kurumsal ve finansal bilgiler” Kanunda yer alan genel ilkeler bağlamında değerlendirildiğinde, bu verilerin orantılı ve sınırlı bilgiler olmadığı, işlenen verilerin ilgili kişiler tarafından en azından öngörülebilir olması gerekmekte olup veri sorumlusunca “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkesine aykırı hareket edildiği değerlendirilmektedir.

3. Kanunun 8 inci maddesinde “(1) *Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz. (2) Kişisel veriler; 5’inci maddenin ikinci fıkrasında, yeterli önlemler alınmak kaydıyla, 6’ncı maddenin üçüncü fıkrasında, belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir. (3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.”* hükmü düzenlenmiştir.

Veri sorumlusunun “Gizlilik Bildirimi” incelendiğinde ‘Amazon Kişisel Bilgilerinizi Paylaşıyor mu?’ başlığı altında açıklanan şekillerde paylaşım yapıldığı belirtilerek son maddede “*Yukarıda belirtilenler haricinde, hakkımızdaki kişisel bilgiler üçüncü taraflarla paylaşıldığında, bir bildirim alacaksınız ve bu bilgileri paylaşmamayı seçme şansınız olacaktır.*” ifadesine yer verilmiştir. Metinde yer aldığı şekilde ilgili kişinin kişisel verilerini paylaşmamayı tercih etme şansının mümkün olması, ancak ilgili kişinin açık rızasına istinaden verilerinin işlenmesi halinde geçerli olabilecektir. Çünkü Kanunun 8’inci maddesinin 2 ve 3 numaralı fıkraları kapsamında gerçekleştirilen veri aktarımı işlemlerinde ilgilinin açık rızası aranmayacağı gibi (Kanunun 5’inci maddesinin 2 numaralı fıkrası, 6’ncı maddesinin 3 numaralı fıkrası ve diğer kanunlarda öngörülen hallerde yapılan işlemler), bu durumlarda ilgili kişinin verilerini paylaşmamayı tercih etme şansı da bulunmayacaktır. Öte yandan, açık rızanın en geç aktarma faaliyeti gerçekleştiği sırada alınması lazımdır, bundan sonra alınacak açık rıza mevzuata uygun kabul edilemez. Dolayısıyla, aktarım faaliyetinin gerçekleşmesinden sonra rızanın geri alınabileceğinin söylenmesi kanun lafzının tersine yorumlanması olarak değerlendirilmektedir. Açık rıza alınmadan aktarılan verilerin rıza geri alındıktan sonra akıbetinin ne olacağının bilinmemesi de ayrı bir tartışma konusudur. Dolayısıyla kişisel verilerin aktarılmasına ilişkin gizlilik bildiriminde yer alan muğlak ifadeler, aktarıma ilişkin Kanun hükümlerine aykırı hareket edildiği kanaati uyandırmaktadır.

4. Kanunun 9’uncu maddesi, “(1) *Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz. (2) Kişisel veriler, 5’inci maddenin ikinci fıkrası ile 6’ncı maddenin üçüncü fıkrasında belirtilen şartlardan*

birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede; yeterli korumanın bulunması, yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması, kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir. (3) Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir." hükmünü içermektedir.

Yapılan incelemede veri sorumlusunun yurtdışına veri aktarımını sağlamak amacıyla Kurulun onayını almak üzere taahhütname mektuplarını Kurula sunduğu görülmüştür. Ancak Kurulun henüz bu yönde bir karar vermediği ve yeterli korumaya sahip ülkelerin de henüz belirlenmediği değerlendirildiğinde kişisel verilerin yurtdışına aktarılması için tek yöntem ilgilinin açık rızasının alınması olarak değerlendirilmektedir.

Veri sorumlusundan alınan yazıda hali hazırda mevzuata uygun olarak yurtdışına veri aktarım faaliyeti yapıldığı belirtilmiş olsa da "Amazon Hesabınızı Oluşturun" sekmesine tıklayarak "Gizlilik Bildirimi"nin de kabul edildiği ("*Hesap oluşturarak işbu Gizlilik Bildirimi'nde belirtilen uygulamaları kabul etmektesiniz.*") aynı şekilde kayıtlı bir müşteri, site üzerinden sipariş verdiğinde kendisine "Gizlilik Bildirimi"nin kabul edildiğine dair tekrar hatırlatma yapıldığı ("*Sipariş verdiğinizde Amazon.com.tr'nin Gizlilik Bildirimini, Kullanım ve Satış Koşullarını ve Çerez Bildirimini kabul etmiş olursunuz*") belirtilerek ilgili kişilerin rızasının alındığı veri sorumlusunca iddia edilmekle birlikte, zımni irade beyanı ile onay alınmasının mevzuata uygun kabul edilemeyeceği değerlendirilmektedir. Kanun çerçevesinde açık rıza, kişinin sahip olduğu verinin işlenmesine, kendi isteği ile ya da karşı taraftan gelen istek üzerine, onay vermesi anlamını taşımaktadır. Açık rıza, ilgili kişinin, işlenmesine izin verdiği verinin sınırlarını, kapsamını ve süresini de belirlemesini sağlayacaktır. Belirli bir konu ile sınırlandırılmayan ve ilgili işlemle sınırlı olmayan genel nitelikteki açık rızalar "battaniye rızalar" olarak kabul edilmekte ve hukuken geçersiz sayılmaktadır. Bu kapsamda "Gizlilik Bildirimi"ne onay verildiği yönünde yapılacak bilgilendirme ile "veri işleme" kapsamına giren bütün fiillerin (çerezlerle izleme, aktarma, paylaşma, depolama vb.) tek bir rıza beyanı ile onaylanmasının hukuka uygun olmadığı mütalaa edilmektedir. Mevcut hukuki düzenlemeler çerçevesinde veri sorumlusunun kişisel verilerin yurtdışına aktarılması konusunda Kanunun 9'uncu maddesinin 1 numaralı fıkrasında yer aldığı üzere ilgili kişilerin açık rızasını alması gerektiği, ancak veri sorumlusunun yurt dışına aktarıma ilişkin bir açık rıza alma yoluna gitmediği, yalnızca amazon hizmetlerinin kullanılması suretiyle gizlilik bildiriminde yer alan hususların kabul edilmiş olduğu varsayımının Kanuna uygun bir açık rıza olarak nitelendirilemeyeceği, bu durumun Kanunun 12'nci maddesinde yer alan veri güvenliğine ilişkin yükümlülüklerle aykırılık oluşturduğu kanaatine varılmıştır.

5. Kanunun 10'uncu maddesinde yer alan hüküm gereğince, "kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, kişisel veri toplamanın yöntemi ve hukuki sebebi, 11'inci maddede sayılan diğer hakları konusunda bilgi vermekle yükümlüdür."

Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin 5'inci maddesinin 1'inci bendinin f fıkrasına göre "Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir."

Veri sorumlusunun internet sitesindeki "Kullanım ve Satış Şartları" metni incelendiğinde Amazon Europe Core SARL, Amazon Turkey Perakende Hizmetleri Limited Şirketi ve/veya iştirakleri ("Amazon"), **Amazon.com.tr (internet sayfası) ziyaret edildiğinde** veya buradan alışveriş yapıldığında; Amazon ürünleri, hizmetleri, mobil Amazon uygulamaları veya yukarıdakilerle bağlantılı olarak Amazon tarafından sunulan hizmetler kullanıldığında (**toplu olarak "Amazon Hizmetleri"**) ilgili kişilere internet sayfası özelliklerinin, diğer ürünlerin ve hizmetlerin sunulduğu beyan edilmiştir.

Anlaşıldığı üzere yapılan işleme faaliyeti site ziyaret edildiğinde başlamaktadır. Öyle ki çerezler hakkında hazırlanan metinde *siteyi ziyaret eden kişilerin tarayıcılarını veya cihazını tanımak, ilgileri hakkında daha fazla bilgi sahibi olmak; gerekli özellik, hizmetleri sağlamak ve aşağıda sayılanların da aralarında bulunduğu ek amaçlar için çerezlerin, piksellerin ve diğer teknolojilerin (hep birlikte "çerezler" olarak anılacaktır)* kullanıldığı beyan edilmiştir. Bu durumda sitede gerekli metinlere yer verildiği savından yola çıkılarak Kanunda hüküm altına alınan aydınlatma yükümlülüğünün yerine getirildiği sonucuna varmak mümkün değildir. Siteyi ilk defa ziyaret eden bir kişinin daha henüz veri sorumlusu ile bir sözleşme ilişkisi içine girip girmeyeceğinin ya da kişisel verilerinin işlenmesine açık rızası olup olmayacağının belirli olmaması düşünüldüğünde yalnızca siteye girmiş olması ile verilerinin işlenmesi yönünde açık iradesini beyan ettiği düşünülemeyecektir. Farklı veri işleme araçları kullanılarak site ziyareti ile birlikte veri işlenmeye başlanması için aydınlatmanın öncelikle web sitesine giriş aşamasında yapılması gerekmektedir. Ancak site girişinde farklı araçlarla (ör. Çerezler) kişisel verilerin işlendiğine dair bir bilgilendirme sunulmamakla birlikte (ör. pop-up mesajlar) yapılan işleme için izin verilmesine dair bir istem de mevcut değildir (ör. Sitemizde gezinmeye devam etmek için çerez bildirimimize onay vermelisiniz). Bu durum hem işleme faaliyetindeki açık rıza şartına hem aydınlatma yükümlülüğüne aykırılık teşkil etmekte olup, web

sitesine girişle birlikte kişisel verilerin işlenmeye başlamasına karşın aydınlatmanın yapılmaması, veri sorumlusunun çerezler vasıtasıyla işlenen söz konusu kişisel verilere ilişkin aydınlatma yükümlülüğünü Kanunun 10'uncu maddesinde ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğde düzenlendiği şekilde yerine getirmediği kanaatini oluşturmuştur.

www.amazon.com.tr'ye ilişkin yürütülen resen inceleme neticesinde yukarıda yer verilen değerlendirmeler sonucunda

- Veri sorumlusunun ilgili kişilerin iletişim bilgilerini işlemek suretiyle ticari elektronik ileti göndermek hususunda ilgili kişilerin açık rızasını usulüne uygun olarak almadığı, açık rıza dışında da bir işleme nedenine dayanmadığı, diğer yandan üyenin temas kişilerine ait e-posta adreslerinin de bu kişilerin açık rızalarına dayanmaksızın işlendiği, ayrıca veri sorumlusu tarafından Kanunun 4'üncü maddesinde yer alan genel ilkelere aykırı hareket edildiği,

- Veri sorumlusunun "Gizlilik Bildirimi"nde 'Amazon Kişisel Bilgilerinizi Paylaşıyor mu?' başlığı altında "Yukarıda belirtilenler haricinde, hakkınızdaki kişisel bilgiler üçüncü taraflarla paylaşıldığında, bir bildirim alacaksınız ve bu bilgileri paylaşmamayı seçme şansınız olacaktır." ifadesine yer verildiği, metinde yer aldığı şekilde ilgili kişinin kişisel verilerini paylaşmamayı tercih etme şansının mümkün olmasının, ancak ilgili kişinin açık rızasına istinaden verilerinin işlenmesi halinde geçerli olabileceği, ancak usulüne uygun bir açık rıza alınmadığı dikkate alındığında, kişisel verilerin aktarılmasına ilişkin Kanun hükümlerine aykırı hareket edildiği,

- Kişisel verilerin yurt dışına aktarılması konusunda Kanunun 9'uncu maddesinde yer alan yeterli korumanın bulunduğu ülkelerin Kurulca henüz belirlenmediği, veri sorumlusunun yazılı taahhüdünün Kurum tarafından onaylanmadığı da dikkate alındığında, veri sorumlusunun kişisel verilerin yurtdışına aktarılması konusunda Kanunun 9'uncu maddesinin (1) numaralı fıkrasında yer aldığı üzere ilgili kişilerin açık rızasını alması gerektiği, ancak veri sorumlusunun yurt dışına aktarıma ilişkin usulüne uygun bir açık rıza alma yoluna gitmediği, yalnızca amazon hizmetlerinin kullanılması suretiyle gizlilik bildiriminde yer alan hususların kabul edilmiş olduğu varsayımının Kanuna uygun bir açık rıza olarak nitelendirilemeyeceği

dikkate alındığında veri sorumlusu tarafından Kanunun 12'nci maddesinin (1) numaralı fıkrasındaki yükümlülüklerin yerine getirilmemesinden dolayı Kanunun 18'inci maddesinin (1) numaralı maddesinin (b) bendi kapsamında 1.100.000 TL idari para cezası uygulanmasına,

- Veri sorumlusunca web sitesinde yayımlanan “Gizlilik Bildirimi”nin, birçok bilgi içermesi, veri işlemeye ilişkin genel bir bilgilendirme olması nedeniyle kişisel verilerin işlenmesine ilişkin ilgili kişilere aydınlatma yapıldığı anlamına gelmediği göz önünde bulundurulduğunda ihbar edilen web sitesine girişle birlikte çerezler vasıtasıyla kişisel verilerin işlenmeye başlamasına karşın, çerezler, üyelik girişi gibi veri işlemenin başladığı hiçbir aşamada aydınlatma yükümlülüğünün, Kanununun 10’uncu maddesinde ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğde düzenlenen usul ve esaslara uygun olarak yerine getirilmediği kanaati olduğundan Kanununun 10’uncu maddesinde düzenlenen Aydınlatma Yükümlülüğünü yerine getirmeyen veri sorumlusu hakkında Kanununun 18’inci maddesinin (1) numaralı fıkrasının (a) bendi uyarınca 100.000 TL idari para cezası uygulanmasına,
 - Veri sorumlusunun yukarıda tespit edilen ihlaller göz önünde bulundurularak kişisel veri işleme süreçlerini ve bununla uyumlu şekilde “Gizlilik Bildirimi”, “Kullanım ve Satış Şartları” ve “Çerez Bildirimi” metinlerini güncelleyerek web sitesini ve uygulamalarını Kanuna uygun hale getirerek sonucundan Kurula bilgi vermesi yönünde talimatlandırılmasına,
 - Söz konusu Kararın Kanununun 23’üncü maddesinin (5) numaralı fıkrası çerçevesinde Kurumun internet sayfasında yayımlanmasına
- karar verilmiştir.

2020/172 sayılı KVKK Kararı

İlgili kişinin cep telefonunun özel bir hastane tarafından izinsiz aranması hakkında Kişisel Verileri Koruma Kurulunun 27/02/2020 tarih ve 2020/172 sayılı Karar Özeti

Karar Tarihi : 27.02.2020

Karar No : 2020/172

Konu Özeti : İlgili kişinin cep telefonunun özel bir hastane tarafından izinsiz aranması

İlgili kişinin şikâyet başvurusunda, Hastane tarafından şahsına ait cep telefonunu, Hastane adına bir şahsın aradığı ve Hastanenin reklamını yapmaya çalıştığı, fakat kendisinin bu tip reklamlardan rahatsız olması sebebiyle konuşmak istemediğini dile getirerek telefonu kapattığı, akabinde, Hastanenin e-posta adresine yazılı olarak 6698 sayılı Kişisel Verilerin Korunması Kanununa (Kanun) istinaden başvurarak bilgi talep ettiği, kendisini Hastanenin bir çalışanın aradığı ve bu konuyu konuşmak istediğini söylediği, ancak kendisinin sözlü değil de yazılı cevap talep etmesi üzerine kendisine e-posta yolu ile cevap verildiği, konu ile alakalı olarak gelen bu cevabı yeterli bulmayınca Kuruma şikâyet hakkının gündeme geldiği belirtilerek Kanun kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde Hastaneden savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişinin, tarafları nezdinde SMS gönderimine ilişkin herhangi bir açık rızasının bulunmadığı,
- İlgili kişinin kişisel verilerinin hiçbir şekilde taraflarınca işlenmediği
- İlgili kişinin kişisel verilerinin yurt içinde ve yurt dışında hiç kimseye aktarılmadığı, çünkü ilgili kişinin kişisel verilerinin bünyelerinde işlenmediği,
- Reklam içerikli telefon aramalarından herhangi bir şekilde haberlerinin olmadığı, ilgili kişinin kişisel verilerinin bünyelerinde bulunmadığı, bu nedenle herhangi bir kişiden temin de edilmediği,
- Arama yapan numaranın taraflarına ait bir hat olmadığı, ilgili kişinin başvurusuna ilişkin kayıtlarında ilgili kişiye ait herhangi bir bilgi, arama vb. bilgi, belgenin mevcut olmadığı, ilgili kişiye yapılan aramanın Hastaneleri bilgisi dâhilinde gerçekleştirilmediğinden ilgili kişinin şikâyetine konu

iddialarının muhatabının da taraflarının olmadığı, bu nedenle ilgili kişinin kişisel verilerinin bünyelerinde bulunmadığı yani hiçbir zaman işlenmediği ve yurt içi ve yurt dışında herhangi bir kuruma aktarılmadığı

ifade edilmiştir.

Bununla birlikte, şikâyete konu telefon numarası arandığında hattın Hastanenin checkup departmanına ait olduğu ve çalışanların diğer müşterilere hizmet vermekte olması nedeniyle kısa sürede arayana dönüş sağlanacağını belirten sesli bir mesajla açıldığının görüldüğü, Hastanenin internet sitesinin iletişim bölümünde yer alan numara arandığında ise karşı tarafça şikâyete konu telefon numarasının da Hastanenin checkup merkezi olarak açıldığı yönünde bilgi verildiğinden, Hastaneyi, muhatap ikinci bir yazı ile şikâyete konu telefon numarasının hangi şirkete ait olduğu, checkup hizmetleri başta olmak üzere hasta yönlendirme, reklam ve tanıtım vb. konularda çeşitli firmalardan hizmet alıp almadığı, alıyorsa bu hizmetlere ilişkin sözleşme örnekleri ile sözleşme kapsamında yapılan aramalarda veya SMS gönderiminde kullanılan telefon numaralarının nasıl temin edildiği hususlarındaki açıklamaların tevsik edici belge ve bilgilerle birlikte Kuruma iletilmesi talep edilmiştir.

Hastane tarafından Kuruma iletilen cevap yazısında özetle:

- Şikâyete konu telefon numarasının taraflarına ait olmadığı ancak yaptıkları inceleme sonrasında ilgili numaranınSağlık ve Danışmanlık Hizmetlerinin kullandığı bir numara olduğunun tespit edildiği, ilgili firma ile yapılan sözleşmenin ekte sunulduğu,
- Sözleşmenin, Firma ile taraflarının üçüncü kişilere checkup hizmetinin pazarlanması ve satışı ile Hastanenin checkup hizmetini ilgili Firmanın bulmuş olduğu müşterilere sağlamasına ilişkin olduğu, ilgili sözleşmenin 4. maddesinde Firmanın müşteri bulurken Kanundan ve sözleşmeden kaynaklanan yükümlülükleri riayet etme zorunluluğunun bulunduğu, sözleşmede bahse konu maddeye aykırı davranılması halinde doğacak tüm zarardan Firmanın sorumlu olduğunun belirtildiği,
- Müşterilerin Hastane tarafından bulunmadığı bu nedenle ilgili kişinin herhangi bir bilgisinin bünyelerinde bulunmadığı, Firmanın ilgili kişinin bilgilerini ne şekilde bulduğu, bulup bulmadığı vb. konularda taraflarının bilgilendirilmediği,
- Hastane bünyesinde ilgili kişinin bilgilerinin bulunması ve gerekli onayı almış olması halinde taraflarının bu kişiyi direkt arayacağı ve checkup ile ilgili bilgileri bildireceği, başka bir firmanın checkup hizmeti için taraflarına hasta yönlendirmesi halinde komisyon aldığı dikkate alındığında

Hastanenin kendi bünyesinde bulunan bilgileri bir başka firma ile paylaşmasının da hukuki ve mantıken açıklanabilecek yönünün de bulunmadığı,

- Firmanın, Hastaneye bağlı bir firma veya Hastanenin checkup departmanının da olmadığı, Firmanın sadece taraflarına kanuna uygun olarak hasta bulmakta olduğu, Firmanın kendisini Hastanenin checkup departmanı gibi yani kendilerine bağlı bir firma gibi tanıttığının tespit edilmesi halinde konu ile ilgili de Firma ile hukuki girişimlere başlanılacağı,

- Hastanenin kişisel verilerini kullanacağı her kişiden açık yazılı onay aldığı, ilgili kişinin taraflarında kayıtlı hiçbir bilgisinin bulunmadığı gibi hiçbir zaman taraflarından tedavi hizmeti almadığı, Firmanın ilgili kişi ile temasa geçti ise hukuka uygun olarak mı yoksa uygun olmadan mı temasa geçtiğinin taraflarınca bilinmediği, Firmanın hukuka ve sözleşmeye uygun olarak taraflarına hasta yönlendirme hizmeti vermekte olduğu sözleşme gereğince de hasta temin etme hususunda hukuka aykırı bir işlem yapması halinde Firmanın sorumlu olacağına açıkça düzenlendiği

açıklamalarına yer verilmiştir.

Müteakiben, söz konusu iddialara ilişkin Firmadan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişiye ilişkin Hastane adına arama yapıldığı, taraflarının hastanelerin hastalarıyla olan randevu takibini yapmakta olduğu, ancak ilgili kişinin Hastanenin hastası olmayıp yanlışlıkla arandığı, durumun fark edilmesi ile telefon görüşmesinin sonlandırıldığı, bünyelerinde kişisel verilerin tutulmadığı, çalışılan hastanelerin tuttuğu kişisel verilerin ilgili hastanenin yazılı onayı ile kullanılarak randevuların düzenlediği, bu nedenlerle yurt içine ya da yurt dışına herhangi bir kişisel veri aktarımının söz konusu olmadığı, bu açıklamalar doğrultusunda şikâyetin reddine karar verilmesinin talep edildiği

ifade edilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 27/02/2020 tarih ve 2020/172 sayılı Kararı ile,

- Öncelikle, ilgili kişinin aranması ile ilgili olarak sorumluluğun kimde olduğunun tespit edilmesi amacıyla Hastane ile Firma arasındaki sözleşme incelenmiş olup inceleme neticesinde;

- Sözleşme konusunun, Hastanenin bünyesinde sunulan checkup panelinin Firma tarafından üçüncü kişilere pazarlanması ve satışı ile yapılan satıştan sonra Hastanenin bu hizmeti karşılması ve aradaki ticari işlemleri kapsadığı,

- Firmanın bu satışı ilgili kanunlar çerçevesinde elektronik posta, posta, kapıdan dağıtım, kapıdan satış, internet üzerinden satış, telefonla satış, medya üzerinden satış ve sair yollarla yapabileceği,
- Firmanın kendisi için tasarlanmış checkup panelini piyasa şartları çerçevesinde Hastaneden yazılı onay almak suretiyle kendisinin belirleyebileceği, satışı artırmak için gerekli noktalarda kampanyalar ve aktiviteler düzenleyebileceği,
- Hastanenin sözleşmede belirtilen ürünlerle ilgili SMS gönderme yetkisini de Firmaya verdiği,
- Firmanın bu sözleşme devam ettiği sürece bu ürünü ister web sitesi aracılığı ile ister kapıdan satış yöntemi ile, ister kurumsal satış şekliyle, isterse tele marketing yoluyla, yazılı, işitsel ve görsel medya yoluyla veya başka bir yolla pazarlayabileceği ve satabileceği,
- Satış esnasında kanundan ya da sözleşmeden kaynaklı yükümlülöklere riayet etmemesi sebebiyle doğacak tüm zararlar nedeniyle Hastanenin Firmaya rücu hakkına sahip olduğu,
- “Gizlilik Yasağı” başlıklı sözleşme maddesi altında Hastanenin müşteri verilerini Firmanın kullanımına açabileceği, Firmanın hem Hastanenin eski müşterilerine hem de kendi oluşturacağı yeni müşterilere checkup panelini satacağı, Firmanın Hastaneden aldığı datayı üçüncü kişilerle paylaşamayacağı, dağıtamayacağı, yayınlamayacağı, böyle bir durumun tespiti halinde Hastanenin sözleşmeyi derhal fesih hakkının bulunduğu ve bu sebeple uğrayacağı maddi zararın karşılanmasını Firmadan talep edebileceği, benzer şekilde Hastanenin de Firmanın Hastaneye kazandırdığı yeni hastaları başka çağrı merkezleri ile paylaşamayacağı, bu durumda da Firmanın zararının tazmin edilmesini talep hakkı bulunduğu hususlarının düzenlendiği,
- Firma teknik altyapısının SSL protokollerini desteklediği ve firewall ile IP Authentication yöntemi kullanılarak giriş yapıldığı ve sadece yöneticilerin erişebildiği server’ların kullanıldığı, müşteri bilgilerine yalnızca yetkilendirilmiş kişilerin erişebildiği,
- Müşteri temsilcilerinin sadece otomatik çağrı sistemi üzerinden ekranına gelen “aranan numara” bilgisini görmekte olduğu ve kişisel bilgilere erişemedikleri,
- Tüm arama, satış, backoffice, teslim ve takip adımlarının giriş ve yönetiminin dijital ortamda yapıldığı, ofiste müşteri bilgi güvenliğini tehlikeye sokacak gereksiz matbu formların kullanılmadığı

şartlarına yer verildiğinin görüldüğü,

- Kanununun 3 üncü maddesinde “veri sorumlusu”nun, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak “veri işleyen”in ise, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi olarak tanımlandığı, veri sorumlusunun, veri işleme faaliyetinin genel anlamda “neden” ve “nasıl” yapıldığını belirleyen kişi olduğu, diğer bir ifadeyle, “hangi kişisel verilerin toplanacağı, kişisel verilerin hangi amaçlarla işleneceği, hangi kişilerin kişisel verisinin toplanacağı, kişisel verilerin kimlere, hangi amaçla aktarılacağı, kişisel verilerin hangi süre ile saklanacağı” konularındaki kararların ancak veri sorumlusu tarafından alınabildiği, ancak veri sorumlusunun, akdedeceği bir sözleşme ile “kişisel verilerin toplanmasında hangi bilişim sistemlerinin kullanılacağı, kişisel verilerin nasıl saklanacağı, veri güvenliğinin sağlanmasının detayları, kişisel verilerin bir şirketten diğerine aktarılmasında hangi yöntemin kullanılacağı, veri saklama periyoduna uyulmasını sağlamak için kullanılacak yöntemin ne olduğu, kişisel verilerin silinmesinde hangi yöntemin kullanılacağı” gibi konularda karar alma yetkisini veri işleyene bırakabildiği,

- Kurum tarafından yayımlanan Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular rehberinde de çağrı merkezinin veri işleyen olduğu; “... veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına faaliyet gösteren, dışarıdan hizmet alınması suretiyle çağrı merkezi hizmeti veren bir şirket bu faaliyet kapsamında veri işleyen olarak kabul edilecektir. Burada önemli olan, veri işleyenin bu kapsamdaki kişisel veri işleme faaliyetlerini veri sorumlusundan aldığı talimatlar doğrultusunda gerçekleştirmesidir.” şeklinde açıklandığı,

- Bununla birlikte Madde 29 Çalışma Grubu’nun WP 169 sayılı Veri Sorumlusu ve Veri İşleyen Hakkında Görüşünde de çağrı merkezinin veri işleyen olduğunun “Veri sorumlusu bazı işlerini çağrı merkezine bırakır ve çağrı merkezine veri sorumlusunun müşterilerini veri sorumlusunun kimliğini kullanarak arama talimatı verir. Bu durumda müşterilerin beklentileri ve veri sorumlusunun kendisini dış kaynak firması aracılığıyla sunma şekli dış kaynak firmasının veri sorumlusu adına bir veri işleyen olarak hareket ettiği sonucunu doğurur.” şeklindeki örnekle açıklandığı,

- Firmanın Hastane adına hareket ederek hem hastanenin eski müşterilerine hem de kendi bulduğu müşterilere checkup panelini pazarlayan bir çağrı merkezi olduğunun anlaşıldığı, sözleşmede bulunan, Firmanın bu satışı ilgili kanunlar çerçevesinde elektronik posta, posta, kapıdan dağıtım, kapıdan satış, internet üzerinden satış, telefonla satış, medya üzerinden satış ve sair yollarla yapabileceği; bu ürünü ister web sitesi aracılığı ile, ister kapıdan satış yöntemi ile, ister kurumsal satış şekliyle, isterse tele marketing yoluyla, yazılı, işitsel ve görsel medya yoluyla veya başka bir yolla

pazarlayabileceği ve satabileceği; sözleşmede belirtilen ürünlerle ilgili SMS gönderebileceği hükümleri ile satış esnasında kanundan ya da sözleşmeden kaynaklı yükümlülüklere riayet etmemesi sebebiyle doğacak tüm zararlar nedeniyle Hastanenin Firmaya rücu hakkına sahip olduğu hükmü dikkate alındığında Hastanenin checkup hizmetinin pazarlanması ve satışı için Firmaya yetki verdiği; bu kapsamda yeni müşterilerin nereden bulunacağı ve bu müşterilere ürünlerin hangi yollarla pazarlanacağına ilişkin karar verme yetkisinin Firmaya bırakıldığı, bu sebeple Hastanenin checkup panelinin Hastanenin kayıtlarında bulunan müşterilerine pazarlanmasına yönelik kişisel veri işlenmesinde Firma **veri işleyen** olarak değerlendirilirken; Hastane kayıtlarında bulunmayan ancak Firmanın kendisi tarafından bulunan yeni müşterilerin pazarlama amacıyla aranarak kişisel verilerinin işlenmesinde Firmanın **veri sorumlusu** olduğu kanaatine varıldığı,

- Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin birinci fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin, ikinci fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, Hastanenin hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, Hastanenin meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğunun hükme bağlandığı,

- Firmadan alınan yazıda ilgili kişinin Hastanenin müşterisi olmadığı, kendileri tarafından yanlışlıkla arandığı belirtilmiş olmakla birlikte Hastane ve Firma arasında imzalanan sözleşme gereğince Hastaneye ait ürünün Hastane adına pazarlanması ve satışı için Firmaya yetki verilmiş olsa da; Firmanın sözleşmede yer alan “Satış esnasında kanundan ya da sözleşmeden kaynaklı yükümlülüklere riayet etmemesi sebebiyle doğacak tüm zararlar nedeniyle Hastanenin Firmaya rücu hakkına sahip olduğu” hükmü ile “Firmanın Hastaneden aldığı datayı üçüncü kişilerle paylaşamayacağı, dağıtamayacağı, yayınlamayacağı, böyle bir durumun tespiti halinde Hastanenin sözleşmeyi derhal fesih hakkının bulunduğu ve bu sebeple uğrayacağı maddi zararın karşılanmasını Firmadan talep edebileceği” hükmüne muhalefet ederek Hastane tarafından kendisine bildirilmemiş olan ilgili kişinin cep telefonuna erişmesi ve kişinin cep telefon

numarasını, Kanunun 5 inci maddesinde belirtilen açık rıza ya da diğer işleme şartlarından herhangi biri geçerli olmadığı halde aramak suretiyle işleminin Kanunun 5 inci maddesine aykırı olduğu değerlendirmelerinden hareketle;

- İlgili kişinin kişisel verisi olan cep telefonu numarasının veri sorumlusu Firma tarafından reklam amacıyla aranması suretiyle kullanılmasının, kişisel verilerin korunması mevzuatı açısından bir veri işleme faaliyeti olduğu, bu işlemin Kanunun 5 inci maddesinde düzenlenen işleme şartlarından herhangi birine dayanılarak yapılmaması sebebiyle de Kanunun “Veri Güvenliğine İlişkin Yükümlülükler” başlıklı 12 nci maddesinin (1) numaralı fıkrasının (a) bendinde öngörülen “Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek” yükümlülüğünün yerine getirilmediği kanaatine varıldığından, incelemeye konu olay açısından veri sorumlusu olarak kabul edilen Firma hakkında, Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi hükmü uyarınca 50.000 TL idari para cezası uygulanmasına karar verilmiştir.

2020/167 sayılı KVKK Kararı

Spor salonu hizmeti sunan veri sorumlusunun, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/167 Sayılı Karar Özeti

Karar Tarihi : 27.02.2020

Karar No : 2020/167

Konu Özeti : Spor salonu hizmeti sunan sorumlusunun, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun Kararı

Spor salonu hizmeti sunan şirketin (veri sorumlusu), üyelerinin giriş-çıkış kontrolünde el okutma sistemine geçilmesi gibi biyometrik verileri içeren bazı özel nitelikli kişisel verileri işlemesi ve bu bilgilerin güvenli şekilde muhafaza edildiğinden şüphe duyulması üzerine ilgili kişilerce Kuruma intikal ettirilen şikâyetin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 27/02/2020 tarih ve 2020/167 sayılı Kararı ile;

- 6698 sayılı Kanunun “Özel nitelikli kişisel verilerin işleme şartları” başlıklı 6 ncı maddesinde kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerinin özel nitelikli kişisel veri olarak belirlendiği, özel nitelikli kişisel veriler arasında yer alan biyometrik veri tanımına ise Kanunda yer verilmemekle birlikte, 25.05.2018 tarihinde yürürlüğe giren Avrupa Genel Veri Koruma Tüzüğünde (GDPR) biyometrik verinin; “yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel veriler” olarak tanımlandığı,

GDPR’ın Recital bölümünün 51 inci maddesinde de biyometrik verilerle ilgili açıklamalara yer verildiği ve fotoğrafların işlenmesinin doğrudan biyometrik veri olarak nitelendirilemeyeceği, yalnızca gerçek bir kişinin benzersiz bir şekilde tanımlanmasına veya doğrulanmasına izin veren belirli bir teknik yöntemle işlendiğinde, bu verilerin biyometrik verilerin tanımı kapsamında kabul edileceği açıklamalarına yer verildiği, dolayısıyla bir verinin biyometrik veri kapsamında

değerlendirilebilmesi için o verinin sadece o kişiyi tanımlayabilme ya da doğrulayabilme özelliğine sahip olmasının kriter alındığının değerlendirildiği,

Danıştay 15. Dairesinin 2014/4562 Esas sayılı kararında ise biyometrik yöntemlerin, ölçülebilir fizyolojik ve bireysel özellikleri aracılığıyla gerçekleştirilen ve otomatik şekilde doğrulanabilen kimlik denetleme tekniklerini ifade ettiği belirtilerek, bu yöntemler arasında parmak izi tanıma, avuç içi tarama, el geometrisi tanıma, iris tanıma, yüz tanıma, retina tanıma, DNA tanıma gibi yöntemlerin bulunduğu ifade edildiği

hususlarından hareketle bir spor tesisine giriş esnasında el ve parmak izinin taranması suretiyle kişilerin kimlik doğrulamasının yapılması hususunda adı geçen veri sorumlusunun özel nitelikli kişisel veri niteliğindeki biyometrik veri işleme faaliyetinde bulunduğu değerlendirildiği,

- Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinde de, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin ancak hukuka ve dürüstlük kurallarına uygun şekilde, belirli, açık ve meşru amaçlar kapsamında, doğru ve gerektiğinde güncel olma şartıyla, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceğinin düzenlendiği,

Bu ilkelerden, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesinin, işlenen verilerin belirlenen amaçların gerçekleştirilebilmesine elverişli olması, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirdiği, sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik olarak veri işlenmesi yoluna gidilmemesi gerektiği,

Ölçülülük ilkesinin ise, veri işleme faaliyeti ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması, diğer bir ifadeyle veri işlemenin amacı gerçekleştirecek ölçüde olması anlamına geldiği, bu kapsamda, kişisel veri işleme faaliyetinin gerçekleşmesi için gerekli olmayan kişisel verilerin toplanmaması ve/veya işlenmemesi gerektiği, veri sorumlusunun amacı çerçevesinde ölçülülük ilkesine uygun olarak ilgili kişiden minimum düzeyde bilgi talep etmesi, bunun dışındaki amaç için gerekli olmayan veri işlemeden kaçınması gerektiği, kişisel verilerin işlenmesinin ilgili kişinin iznine bağlı olarak gerçekleştirilse ve belirli bir amaca bağlı olsa bile açık rızanın, aşırı miktarda veri toplanmasını meşrulaştırmayacağı, buna göre kişisel verilerin yalnızca belirli amaçlar için ve gerektiği kadar toplanması, amacın gerektirdiği yerlerde kullanılması ve amaç için gerekli olandan uzun süre tutulmaması gerektiği,

dikkate alındığında spor salonuna giriş için veri sorumlusu tarafından uygulanan “el ve parmak izi taraması” sisteminin, üyelerin açık rızası olsa bile hizmetten faydalanmak için üyelere sunulmasının, kişisel verilerin işlenmesinde ölçülülük ilkesi ışığında ilgili kişilerden minimum düzeyde veri talep etme ilkesi ile uyumlu olmadığı değerlendirilmiş olup, **bu itibarla**;

- Spor kulübüne giriş ve çıkışların kontrolü amacıyla getirilen avuç içi izinin taranması suretiyle kişilerin kimlik doğrulamasının yapılmasının, biyometrik veri kapsamında değerlendirilmeyeceği ve bu sistemin yanı sıra dileyen üyelerin kart göstermek suretiyle tesisten faydalandıkları iddia edilse de avuç içi tarama sisteminin biyometrik veri tanımını karşıladığı, bu sistemin yanı sıra seçimlik hak sunulsa bile biyometrik veri içeren bir sistemin tesis giriş ve çıkışlarında kullanılmasının Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinin (2) numaralı fıkrasının (ç) bendindeki ölçülülük ilkesine aykırı olduğu kanaatine varılması nedeniyle Şirketin söz konusu uygulamasının Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendine aykırılık teşkil ettiği sonucuna varıldığından, Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında veri sorumlusu hakkında 225.000 TL idari para cezası uygulanmasına,

- Veri sorumlusu tarafından bugüne kadar işlenen ve muhafaza edilen el, parmak ve avuç izi ile ilgili verilerin Kanunun 7 nci maddesi ile Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik hükümlerine uygun olarak ivedilikle yok edilmesi, eğer ilgili özel nitelikli verilerin üçüncü kişilere aktarılması söz konusu ise, yok etmeye yönelik işlemlerin bu verilerin aktarıldığı üçüncü kişilere ivedilikle bildirilmesinin sağlanması ve biyometrik veri ile giriş çıkış işlemleri yapılmasının ve biyometrik veri işleminin durdurulması hususunda veri sorumlusunun talimatlandırılmasına,

- İlgili kişinin veri sorumlusuna bünyesinde bulunan kişisel verilerinin silinmesi talebine istinaden, talebin yerine getirildiğine ve söz konusu kişisel verilerin silindiğine ilişkin ilgili kişinin bilgilendirilmesi ve söz konusu silme işlemine ilişkin tevsik edici bilgi ve belgelerin Kurumumuza iletilmesi hususunda Şirketin talimatlandırılmasına,

- Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerinin de hatırlatılması suretiyle veri sorumlusunun Aydınlatma Metninin usulüne uygun olarak güncellenmesi hususunda talimatlandırılmasına

karar verilmiştir.

2020/166 sayılı KVKK Kararı

İlgili kişinin kullanımına izin vermediği kredi kartı bilgilerinin veri sorumlusu araç kiralama şirketi tarafından kullanılması hakkında Kişisel Verileri Koruma Kurulunun 27/02/2020 tarihli ve 2020/166 sayılı Karar Özeti

Karar Tarihi : 27.02.2020

Karar No : 2020/166

Konu Özeti : İlgili kişinin kullanımına izin vermediği kredi kartı bilgilerinin veri sorumlusu araç kiralama şirketi tarafından kullanılması

Kuruma intikal eden şikayette; ilgili kişi ile veri sorumlusu araç kiralama şirketi arasında imzalanan araç kiralama sözleşmesi kapsamında ilgili kişinin 1 günlük süreyle araç kiraladığı ve söz konusu sözleşme uyarınca araç kiralama bedeli ve provizyonun çekilmesi için ...22 ile biten kredi kartının kullanımına onay verildiği, kiralama süresi içerisinde 1 kez HGS kullandığı ve kiralama süresi sona erdiğinde aracı teslim ettikten sonra telefonuna gelen SMS ile söz konusu HGS bedelinin ...67 ile biten başka bir kredi kartından tahsil edilmeye çalışıldığını fark ettiği, bunun üzerine müşteri temsilcisini aradığında “araç kira bedeli ödemesi hangi kredi kartı ile yapılmış ise HGS bedelinin de aynı kredi kartından yapılması gerektiği” bilgisini edindiği, yaşadığı olay ile ilgili olarak kişisel veri güvenliğinin ihlal edildiği gerekçesi ile tarafına açıklama yapılması için müşteri hizmetleri ile birçok kez görüşme yaptığı ve konuya ilişkin şikâyetlerini elektronik posta yolu ile de müşteri hizmetlerine bildirdiği, müşteri hizmetleri tarafından konunun hukuk birimine yönlendirildiğinin belirtildiği ancak olayın üzerinden 2 ay geçmesine rağmen kendisine son yazışma tarihinden itibaren hiç bir geri dönüş yapılmadığı, bu durumun 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 13 üncü maddesine aykırılık teşkil ettiği, sözleşmede belirtilen ...22 ile biten kredi kartı yerine, hiçbir şekilde onayının ve bilgisinin bulunmadığı belirtilerek, kullanımına izin vermediği ...67 ile biten diğer kredi kartı bilgilerini alan ve kullanan veri sorumlusu araç kiralama şirketi hakkında gerekli yaptırımın uygulanarak kendisine bilgi verilmesi talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişinin ...67 ile biten kredi kartı bilgilerinin araç kiralama sözleşmesinden önce yapılan başka bir kiralama sözleşmesinde ilgili kişi tarafından kendilerine bildirildiği ve kira sözleşmesi gereği, sözleşme ile bildirilen kredi kartından yine kiracının yazılı onayı ile *“bu sözleşmeyi imza etmekle arka sayfada belirtilmiş olan ... standart kiralama kural ve koşullarını okuduğumu ve kabul ettiğimi beyan ederim. Aracın aylık kullanım limitinin 3.000 km olup aşıldığı takdirde ücretlendirmeyi, bu kiralamadan doğan ve doğacak olan her türlü ödemenin ... bildirdiğim kredi kartımdan tahsil edilmesini kabul ve beyan ederim.”* diyerek kira sözleşmesindeki bu onayı ile kredi kartı veri işlemi olduğu,
- Araç kiralama sözleşmesi gereği tahsil edilmek istenen bedelin bir önceki sözleşmede bildirilen kredi kartından çekilmesi işleminin hukuki dayanağını; kira sözleşmesinin *“Madde 2 - Ödeme”* başlığı altında yer alan *“kiracı tarafından bildirilen kredi kartından tahsilat yapılmadığı durumlarda; kiracının kiralayan ile yapmış olduğu başkaca araç kiralama sözleşmelerinde bildirdiği kredi kartı ve/veya nakit hesaplarından, kiralayanın tahsil etme hakkı saklıdır”* şartının oluşturduğu, bu nedenle daha önceki kira sözleşmelerinde bildirilen kredi kartlarının mevcut sözleşme şartı gereği daha sonraki kiralamalarında kullanıldığı, ilgili kişi tarafından kullanılmaması talep edildiğinde ise kullanılmadığı,
- Veri sorumlusu tarafından kişisel veri işlenmesinin hukuki gerekçelerinin;
 - 6698 sayılı Kanun Madde 5 (2) (c) - *“bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması”* ve
 - 6698 sayılı Kanun Madde 5 (2) (f) - *“ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması”* olduğu,
- İlgili kişinin araç kiralama sözleşmesi kapsamında aracı kiraladığı süre içerisinde oluşan HGS geçiş ücretinin bir önceki kira sözleşmesinde bildirdiği ...67 ile biten kredi kartından tahsil edilme girişiminde bulunulduğu ancak bu karttan bir çekim olmadığı, aynı gün içinde araç kiralama sözleşmesi ile bildirilen ...22 ile biten kredi kartından çekimin yapıldığının tespit edildiği,
- Kişinin ...67 ile biten kredi kartının kullanılmaması yönünde şirketlerine başvuru yaptığı, kişiye müşteri hizmetleri tarafından hukuk biriminden bilgi iletileceğinin bildirildiği ancak müşteri hizmetlerinin bir anlık dalgınlığı nedeniyle sehven konunun hukuk birimine aktarılmadığının tespit edildiği,
- Kira sözleşmelerinde yer alan açık hüküm sebebiyle şirketin tahsilat yapma hakkı olmasına rağmen kişinin bu talebinin özel kabul edilerek ve Kanun önemsenerek sistemde bulunan tüm kredi kartı bilgilerinin silindiği, silme işleminin Kanuna uygun olarak gerçekleştirildiği, silme işlemine ilişkin

olarak şirketin genel müdürü ve yazılım yetkilileri arasındaki e-posta yazışmalarının ekte sunulduğu, yedeklemeler ile de silme işleminin iptal edildiğinin ispat edildiği; yedekleme verisinin içerisinde başka kişisel veriler olduğu için Kuruma iletilemediği, aynı şekilde veri silme işlemine ilişkin veri tabanı görüntülerinin de başkaca kişisel veriler bulunması sebebiyle sunulamadığı,

- Yine kira sözleşmelerinin içerisinde kişiye ait başkaca kişisel verilerin bulunması sebebiyle şu an sunulamadığı ancak Kurumun talebi halinde bu dokümanların sunulmaya hazır olunduğu belirtilerek veri sorumlusu tarafından ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla kredi kartı bilgisinin kira sözleşmesi gereği kullanıldığı ve meşru menfaatler çerçevesinde işlem yapıldığı, ayrıca kişinin talebi üzerine 7 gün içerisinde veri tabanından tüm kredi kartı bilgileri silindiği

ifadelerine yer verilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 27/02/2020 tarihli ve 2020/166 sayılı Kararı ile,

- İlgili kişinin 1 günlük araç kiralamak amacıyla veri sorumlusunun web sayfası üzerinden rezervasyon yaptığı, rezervasyon sırasında kiralama ücretinin ön provizyon olarak, kira sözleşmesi kapsamında kendisinin kullanımına rıza gösterdiği ve onay verdiği ...22 ile biten kredi kartından tahsil edildiği, söz konusu kiralama süresi içerisinde ortaya çıkan HGS ücretinin (4.13 TL) ise veri sorumlusu tarafından ilgili kişinin daha önceki farklı bir kiralama sözleşmesi kapsamında kullanımına onay verdiği ...67 ile biten kredi kartından tahsil edilmeye çalışıldığı ancak söz konusu kredi kartının internetten alışveriş işlemlerine kapalı olduğu için işlemin gerçekleştirilemediği, bu nedenle söz konusu HGS ücretinin yine aynı gün içinde, mevcut sözleşmesinde bildirdiği ...22 ile biten kredi kartından tahsil edildiği,

- Veri sorumlusu tarafından ilgili kişi ile yapılan araç kiralama sözleşmesinde yer alan *“kiracı tarafından bildirilen kredi kartından tahsilat yapılamadığı durumlarda; kiracının kiralayan ile yapmış olduğu başkaca araç kiralama sözleşmelerinde bildirdiği kredi kartı ve/veya nakit hesaplarından, kiralayanın tahsil etme hakkı saklıdır”* maddesine dayanılarak HGS ücretinin ilgili kişi ile yapılan daha önceki bir sözleşme kapsamında bildirilen kredi kartından tahsil edilmeye çalışıldığının belirtildiği, ancak veri sorumlusu tarafından mevcut sözleşme kapsamında yer alan *“bu sözleşmeyi imza etmekle arka sayfada belirtilmiş olan ... standart kiralama kural ve koşullarını okuduğumu ve kabul ettiğimi beyan ederim. Aracın aylık kullanım limitinin 3.000 km olup aşıldığı takdirde ücretlendirmeyi, bu kiralamadan doğan ve doğacak olan her türlü ödemenin ... bildirdiğim kredi kartımdan tahsil edilmesini kabul ve beyan ederim”* maddesi gereği; ilgili kişinin kullanımına onay verdiği kredi kartının geçerliliğinin ön provizyon bedeli alınarak

onaylandığı ve bu karttan kiralama ücreti ve diğer ücretlerin tahsilatının yapılabildiği, bu nedenle somut vakada, söz konusu sözleşme maddesinde belirtilen *“kiracı tarafından bildirilen kredi kartından tahsilat yapılamaması”* durumu gerçekleşmediği için, veri sorumlusunun 4.13 TL olan HGS bedelini daha önceki araç kiralama sözleşmesi kapsamında bildirilen farklı bir kredi kartından tahsil etmeye çalışmasının gerekçesi ve hukuki dayanağını bu maddenin oluşturamayacağı,

- Ayrıca hem ilgili kişinin müşteri temsilcisi ile yaptığı görüşme sonucunda edindiği *“araç kira bedeli ödemesi, hangi kredi kartı ile yapılmış ise HGS bedelinin de aynı kredi kartından yapılması gerektiği”* bilgisi, hem de veri sorumlusunun web sayfasında yer alan *“Araç Kiralama Koşulları”* metninde ödemeye ilişkin başlıklar altında yapılan açıklamalar dikkate alındığında; ödemenin mevcut sözleşme kapsamında bildirilen ve kullanımına onay verilen kredi kartından tahsil edileceğinin anlaşıldığı, araç kira sözleşmesinde yer aldığı iddia edilen *“daha önce yapılan bir sözleşme kapsamında bildirilen başkaca bir kredi kartından da tahsil edilebileceği”* bilgisine yer verilmediği,

- Diğer taraftan, *“Tüketici Sözleşmelerindeki Haksız Şartlar Hakkında Yönetmelik”*in (17.06.2014 tarihli ve 29033 sayılı R.G.) *“Haksız Şart”* başlıklı 5 inci maddesinde *“(1) Tüketici ile kurulan sözleşmelerde yer alan bir şartın haksız şart olarak kabul edilebilmesi için; a) Tüketicikle müzakere edilmeden sözleşmeye dahil edilmesi, b) Tarafların sözleşmeden doğan hak ve yükümlülüklerinde dürüstlük kuralına aykırı düşecek biçimde tüketici aleyhine dengesizliğe neden olması, unsurlarının bir arada bulunması gerekir. (2) Bir sözleşme şartının önceden hazırlanması ve standart sözleşmede yer alması nedeniyle tüketicinin sözleşmenin içeriğine etki edememesi durumunda, o sözleşme şartının tüketicikle müzakere edilmediği kabul edilir. Sözleşmeyi düzenleyen, bir standart şartın münferiden müzakere edildiğini iddia ediyorsa bunu ispatla yükümlüdür”* ve *“Haksız Şartların Sözleşmeye Etkisi”* başlıklı 7 nci maddesinin 1. fıkrasında ise *“Tüketicikle kurulan sözleşmelerde yer alan haksız şartlar kesin olarak hükümsüzdür. Ancak sözleşmenin haksız şartlar dışındaki hükümleri geçerliliğini korur. Bu durumda sözleşmeyi düzenleyen, kesin olarak hükümsüz sayılan şartlar olmasaydı diğer hükümlerle sözleşmeyi yapmayacak olduğunu ileri süremez”* hükümlerinin yer aldığı, bu çerçevede söz konusu kira sözleşmesinde yer alan *“kiracı tarafından bildirilen kredi kartından tahsilat yapılamadığı durumlarda; kiracının kiralayan ile yapmış olduğu başkaca araç kiralama sözleşmelerinde bildirdiği kredi kartı ve/veya nakit hesaplarından, kiralayanın tahsil etme hakkı saklıdır”* hükmünün somut vaka itibarıyla ilgili kişi aleyhine bir durum oluşturduğu ve ilgili kişinin makul beklentisini ve çıkarlarını göz önüne almayarak dürüstlük kurallarına aykırılık teşkil ettiği,

- Veri sorumlusunun savunmasında, kira sözleşmelerinin içeriğinde ilgili kişiye ilişkin başkaca kişisel verilerin bulunması sebebiyle şu an sunulmadığı, ancak Kurumun talebi halinde sunulmaya hazır olduğunun belirtildiği, buna istinaden Kurumun ek bilgi/belge talebini içeren resmi yazısının

tebliğ tarihi itibarıyla veri sorumlusu tarafından Kuruma herhangi bir bilgi/belge iletilmediği, Kurum tarafından ek bilgi belge kapsamında talep edildiği halde veri sorumlusu tarafından gönderilmeyen söz konusu kira sözleşmesinin, tüketici ile hizmet sunucu arasındaki sözleşmelere ilişkin genel uygulamalar da dikkate alınarak, ilgili kişi ile müzakere edilmeksizin tek taraflı olarak hazırlandığı ve matbu bir şekilde ilgili kişiye sunulduğu kanaatine varıldığı,

- Tüm bu nedenlerle sözleşmede yer alan söz konusu maddenin uygulanmasına yer olmadığı ve ayrıca "haksız şart" niteliğine uyduğu değerlendirilmekte olup veri sorumlusunun ilgili kişinin eski sözleşmesinde yer alan kredi kartı bilgilerini kullanmaya devam etmesini, ilgili sözleşme hükmünü işaret ederek *"bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması"* kişisel veri işleme şartına dayandırmasının uygun olmadığı,

- Aynı şekilde somut olayda, veri sorumlusunun mevcut durumda ön provizyon işlemi ile geçerliliğini ve limitini onayladığı ilgili kişinin sözleşme kapsamında kullanımına izin verdiği kredi kartı bilgisine sahip olduğu ve ödemeyi bu kredi kartından tahsil edebileceği halde daha önce elde ettiği başka bir kredi kartı bilgisini kullanmaya çalışması ve ilgili kişiye ait toplam üç kredi kartına ilişkin bilgilerin daha sonra kullanılabilmesi düşüncesiyle sisteminde saklaması faaliyetine ilişkin olarak; menfaatlerin yarışabilir olmadığı, kişinin hem ilgili kişi hem de tüketici olarak zayıf konumda olan taraf olduğu, dolayısıyla temel hak ve hürriyetlerinin ihlale açık olduğu ve ilerde söz konusu veri işleme faaliyetinden (haber verilmeksizin kredi kartından tahsilat/ çekim vb. yapılabilmesi suretiyle) zarar görebileceği hususları dikkate alınarak yapılan değerlendirme ile, söz konusu veri işleme faaliyetinin *"ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması"* kişisel veri işleme şartına dayandırılmasının da uygun olmadığı, söz konusu veri işlemenin açık rızaya veya diğer kişisel veri işleme şartlarından herhangi birine dayandırılmayacağı ve hukuka aykırı bir veri işleme olduğu kanaatine varıldığı,

- Söz konusu veri işleme faaliyetinin; kira sözleşmesinin yukarıda bahsi geçen ilgili hükmünün haksız şart niteliğine uyması ve somut vakanın kişinin makul beklentisi dışında aleyhine bir sonuç ortaya çıkarması nedeniyle *"hukuka ve dürüstlük kurallarına uygun olma"*; kiralama süreci sonrasında araç tesliminin gerçekleşmesi ve bütün bedellerin tahsil edilmesiyle birlikte sözleşmenin sona ermesi, veri işleme amacının ortadan kalkması ve mevcutta olmayan ve sonradan gerçekleşmesi düşünülen amaçlarla kişisel veri işlenmeye devam edilmesi nedeniyle *"işledikleri amaçla bağlantılı, sınırlı ve ölçülü olma"* ilkelerine aykırılık teşkil ettiği,

değerlendirmelerinden hareketle;

İlgili kişinin veri sorumlusu ile daha önce yaptığı araç kiralama sözleşmesi kapsamında kullanımına onay verdiği kredi kartı bilgilerinin; veri sorumlusu tarafından daha sonra gerçekleştirilmesi düşünülen amaçlar doğrultusunda kullanılmak üzere sistemde saklanarak, haksız şart niteliği gösteren sözleşme hükmüne dayanmak suretiyle somut vakada kişinin makul beklentisine ve çıkarına aykırı olumsuz bir durum oluşturarak haklı bir gerekçe olmaksızın kullanılmasına ilişkin kişisel veri işleme faaliyetinin Kanunun “Kişisel verilerin işleme şartları” başlıklı 5 inci maddesinde yer alan şartlardan herhangi birine dayandırılmayacağı ve Kanunun “Genel ilkeler” başlıklı 4 üncü maddesi uyarınca “hukuka ve dürüstlük kurallarına uygun olma” ile “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkelerine aykırılık teşkil ettiği kanaatine varılmış olup bu itibarla, Kanunun 12 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülüklerini yerine getirmemiş olması nedeniyle veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 75.000 TL idari para cezası uygulanmasına karar verilmiştir.

2020/145 sayılı KVKK Kararı

Veri sorumlusu tarafından ilgili kişilerin kişisel verilerinin hukuka aykırı şekilde internet gazetesi üzerinden yayımlanması hakkında Kişisel Verileri Koruma Kurulunun 18/02/2020 tarihli ve 2020/145 sayılı Karar Özeti

Karar Tarihi : 18.02.2020

Karar No : 2020/145

Konu Özeti : Veri sorumlusu tarafından ilgili kişilerin kişisel verilerinin hukuka aykırı şekilde internet gazetesi üzerinden yayımlanması

Kuruma intikal eden şikâyet; ilgili kişilerin yönetim kurulu üyesi olduğu bir şirket hakkında şikâyetle bulunulan veri sorumlusu ...Medya Yayıncılık A.Ş.'ye bağlı olarak yayın yapan ...Medya isimli internet gazetesi üzerinden asılsız ve gerçeğe aykırı beyanlarda bulunduğu, ilgili kişilerin yönetim kurulu üyesi olduğu şirket tarafından noter aracılığı ile veri sorumlusuna tezip ihtarnamesinin gönderildiği, veri sorumlusunun ilgili kişiler tarafından gönderilen ihtarnamenin fotoğrafını çekmek suretiyle yeni bir haber şeklinde olduğu gibi yayımladığı, ilgili ihtarnamenin sonunda ilgili kişilerin T.C. kimlik numaralarının, nüfus kayıt bilgilerinin, anne-baba isimlerinin ve adres bilgilerinin yer aldığı, ilgili ihtarnamenin fotoğrafının çekilip olduğu gibi haberin içinde yayımlanması nedeniyle ilgili kişilerin kişisel bilgilerinin hukuka aykırı bir şekilde kamuya ifşa edildiği, kişisel verilerin hukuka aykırı şekilde yayımlanması nedeniyle veri sorumlusuna tekrar ihtarname gönderildiği ve bunun üzerine ihtarnamenin kişisel verilere ilişkin kısmının haber metninden çıkarıldığı ancak 10 gün boyunca ilgili kişilere ait kişisel verilerin hukuka aykırı şekilde yayımlanarak kamuya ifşa edildiği, veri sorumlusunun ilgili kişilerin şahsi kimlik bilgilerini kamuya açık alanda kasten yayımlayarak Kişisel Verilerin Korunması Kanununa (Kanun) aykırı davrandığı hususları belirtilerek T.C. kimlik numaraları, nüfus bilgileri, anne baba ismi ve adres bilgisi gibi kişisel verilerini hukuka aykırı şekilde internet gazetesi üzerinden yayımlayan böylece güvenliklerini tehlikeye düşürdüğü kadar ilgili kişilere ait kişisel verileri rızaları ve bilgileri dışında kullanarak üçüncü kişilerce dolandırılmalarına sebebiyet verecek işlemlerin önünü açan veri sorumlusu hakkında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişilerin yönetim kurulu üyesi oldukları şirketin anonim şirkete dönüşmek üzere genel kurula gittiği, haberi yapan ve aynı zamanda ilgili yayın grubunun da yöneticisi olan kişinin ilgili sektörü takip eden bir gazeteci olarak söz konusu genel kurul toplantısını izlemek istediği ancak toplantıyı izlemesine izin verilmediği, toplantıda iki farklı düşüncede grubun olduğu,
- Genel kurulun muhalif kanadının toplantı ile ilgili kendisine bilgi verdikleri, isimleri belli bir kesimin görüşlerini yayın grubunda yayınladığı, sonrasında olayın diğer tarafı, muhalif kesimin iddialarını cevaplamak için kendisine noter kanalıyla açıklama metinlerini gönderdikleri, bu açıklamaların cevap hakkı niteliğinde olması nedeniyle, zorunlu olmamasına rağmen etik gazetecilik anlayışı çerçevesinde açıklamaların önemli bölümlerinin yayın grubunun internet sitesinde kullanıldığı,
- Kendilerinin 10 satırlık haber yaptıkları, şirket yöneticilerinin ise 4-5 sayfalık açıklama metni gönderdiği, bunları baştan yazmanın çok zaman alacağından dolayı kendilerine “açıklamalarını mail yolu ile göndermeleri halinde tümünün yayımlanacağını” bildirildiği, noter kanalıyla gelmeye devam eden açıklamaların aynen eksiksiz olarak kullanılmasının istendiği, bu yüzden kendilerinin de metnin tamamını internet sitelerinde yayımladıkları, kaldırılması talebi üzerine hemen kaldırdıkları, bu açıklamanın kimlik bilgilerini içerdiği, bunu fark ettikleri anda hemen kaldırdıkları,
- Bu bilgilerin sitede kullanıldığına dair karşı tarafın bir kanıtının olmadığı, kendilerinde de bu ekran görüntüsünün bulunmadığı, kendilerinin kullanmadıklarını söylemeleri halinde karşı tarafın hiçbir kanıtının olmadığı; diğer yandan konunun yargıya gittiği, mahkeme huzuruna çıktığı ve beraat ettiği ifadelerine yer verilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 18/02/2020 tarihli ve 2020/145 sayılı Kararı ile,

- Kanunun “Tanımlar” başlıklı 3 üncü maddesinde; “kişisel veri”nin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi, “veri sorumlusu”nun, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi ve “kişisel verilerin işlenmesi”nin, kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi,

sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı,

- Bu minvalde, ilgili kişilerin şikayet konusu tekzip ihtarnamesinde yer alan ad, soyadı, T.C. kimlik numaraları, nüfus kayıt bilgileri, anne-baba isimleri, adres bilgilerinin birer kişisel veri, veri sorumlusu medya şirketinin, kişilere ait bu verilerin internet gazetesinde yayımlanması işleminin de kişisel veri işleme faaliyeti olduğu,

- Kanununun 4 üncü maddesinin (2) numaralı fıkrasında kişisel verilerin işlenmesinde uyulması zorunlu ilkelerin “a) hukuka ve dürüstlük kurallarına uygun olma, b) doğru ve gerektiğinde güncel olma, c) belirli, açık ve meşru amaçlar için işleme, ç) işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, d) ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme” şeklinde düzenlendiği,

- Kanununun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin, (2) numaralı fıkrasında ise Kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işleminin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Öte yandan, Kanununun 28 inci maddesinin (1) numaralı fıkrasının (c) bendinde “*Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi*” halinde Kanun hükümlerinin uygulanmayacağı belirtilmiştir,

- 5187 sayılı Basın Kanununun 14 üncü maddesinde ise “*Sürelî yayınlarda kişilerin şeref ve haysiyetini ihlâl edici veya kişilerle ilgili gerçeğe aykırı yayım yapılması halinde, bundan zarar gören kişinin yayım tarihinden itibaren iki ay içinde göndereceği suç unsuru içermeyen, üçüncü kişilerin hukuken korunan menfaatlerine aykırı olmayan düzeltme ve cevap yazısını; sorumlu müdür hiçbir düzeltme ve ekleme*

yapmaksızın, günlük süreli yayınlarda yazıyı aldığı tarihten itibaren en geç üç gün içinde, diğer süreli yayınlarda yazıyı aldığı tarihten itibaren üç günden sonraki ilk nüshada, ilgili yayının yer aldığı sayfa ve sütunlarda, aynı puntolarla ve aynı şekilde yayımlamak zorundadır” düzenlemesine yer verildiği,

- Sorumlu müdürün, Basın Kanunundan kaynaklı olarak düzeltme metnini veya cevap yazısını hiçbir düzeltme ve ekleme yapmaksızın yayımlama yükümlülüğünün bulunduğu, ancak bu amaç yerine getirilirken sorumlu müdürün bu amaçla bağlantılı, sınırlı ve ölçülü olacak şekilde hareket etmesi beklendiği, diğer bir ifadeyle, düzeltme metni yayımlanırken, haberle ve metnin içeriğiyle ilgisi olmayan ve yayımlanması halinde kişilerin kişilik haklarının zarara uğramasına sebep olacak kişisel verileri içeren kısımların yayımlanması, amaç ile orantılı olarak değerlendirilmediğinden söz konusu düzeltme metninin kişilik haklarını ihlal ederek internet sitesinde yayımlanmasının, Kanunun 28 inci maddesinin (1) numaralı fıkrasının (c) bendi kapsamında değerlendirilmeyerek şikâyetin incelemeye alındığı,

- Veri sorumlusunun bahse konu olan tekzip ihtarnamesini yayımlamasının, 5187 sayılı Basın Kanununun 14 üncü maddesinde yer alan yükümlülüğünü yerine getirmek amacıyla Kanunun 5 inci maddesinin 2 numaralı fıkrasının (ç) bendinde yer alan “veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için veri işlemenin zorunlu olması” hükmü doğrultusunda hukuka uygun olduğu, ancak ilgili ihtarnamenin kişisel verilere ilişkin bölümünü herhangi bir güvenlik önlemi almaksızın olduğu gibi yayımlanmasının, daha sonra bu bölüm internet sitesinden kaldırılmış olsa dahi Kanunun genel ilkeler başlıklı 4 üncü maddesinde düzenlenen “amaçla bağlantılı, sınırlı ve ölçülü olma” ilkesi ile bağdaşmadığı dikkate alındığında bu durumun veri sorumlusu tarafından kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirlerin alınmadığının göstergesi olduğu

değerlendirmelerinden hareketle;

- Veri sorumlusunun bahse konu tekzip ihtarnamesinin yayımlamasının, Kanunun 5 inci maddesinin 2 numaralı fıkrasının (ç) bendinde yer alan “veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için veri işlemenin zorunlu olması” hükmü kapsamında hukuka uygun olduğu, ancak ilgili ihtarnamenin kişisel verilere ilişkin bölümünün olduğu gibi yayımlanmasının, daha sonra bu bölümü internet sitesinden kaldırmış olsa dahi, Kanunun genel ilkeler başlıklı 4 üncü maddesinde düzenlenen “amaçla bağlantılı, sınırlı ve ölçülü olma” ilkesi ile bağdaşmadığı dikkate alındığında bu durumun Şirketin kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almadığına işaret ettiği ve bu kapsamda Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendinde öngörülen

yükümlülüğünü yerine getirmediği kanaatine varılan veri sorumlusu hakkında Kanunun 18 inci maddesinin birinci fıkrasının (b) bendi hükmü uyarınca 55.000 TL idari para cezası verilmesine karar verilmiştir.

2020/138 sayılı KVKK Kararı

Veri sorumlusu işveren tarafından, iş sözleşmesi tek taraflı olarak feshedilen ve işe iade davası açan ilgili kişiye ait özlük dosyasında yer alan sağlık raporunun dava savunmasında kullanılmak suretiyle mahkemeye sunulması hakkında Kişisel Verileri Koruma Kurulunun 18/02/2020 tarihli ve 2020/138 sayılı Karar Özeti

Karar Tarihi : 18.02.2020

Karar No : 2020/138

Konu Özeti : Özlük dosyasında yer alan sağlık raporunun veri sorumlusu tarafından dava savunmasında kullanılmak üzere mahkemeye sunulması

Kuruma intikal eden şikâyette özetle, ilgili kişinin iş akdinin tek taraflı feshi nedeniyle veri sorumlusu işveren hakkında açtığı işe iade davasında, dava içeriği ile ilgili olmamasına rağmen özlük dosyasında yer alan kendisine ait özel nitelikli kişisel verilerinin mahkemenin talebi olmadığı hâlde dava dosyasına sunulduğu, sağlık durumu hakkında özellikle ilgili sağlık kurumu tarafından bir tanı konulmamış olmasına rağmen sağlık raporlarında yer alan “uzman” veya “bilirkişi” gibi ifadelerin büyük harfler içine alınarak psikolojik tanı koymaya yetkili bir kurum veya kişi sıfatı ile raporların davaya konu edilmesinin kişilik haklarının ihlal edilmesine sebebiyet verdiği ifade edilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) uyarınca veri sorumlusu hakkında gerekli işlemlerin tesis edilmesi talep edilmiştir.

Konuya ilişkin olarak Kurul Kararı ile başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İşverenin 6331 sayılı İş Sağlığı ve Güvenliği Kanununun 15 inci maddesine göre çalışanın sağlık muayenelerini yapmasını sağlamak zorunda olduğu, İş Sağlığı ve Güvenliği Yönetmeliğinin 7 nci maddesinde yer alan hüküm uyarınca işten ayrılma tarihinden itibaren en az 15 yıl süreyle çalışanların kişisel sağlık dosyalarının saklanacağı, bu sebeple çalışanın sağlık verilerinin anılan Kanun ve Yönetmelik hükümlerince işlendiği,
- Söz konusu raporların herhangi bir gerekçe ile talep edilmeksizin izin taleplerinin bir mazereti olarak bizzat ilgili kişinin kendisi tarafından ibraz edildiği, ilgili kişinin tüm uyarılara rağmen görev

ve sorumluluklarının gereğini yerine getirmemesi ile birlikte işyerinde sergilediği olumsuz tutum ve beyanlar nedeniyle işyerinin çalışma düzenine ve iş huzurunun bozulmasına sebebiyet verdiği, bu nedenle 4857 sayılı İş Kanununun 25 inci maddesi uyarınca iş akdinin feshedildiği,

- Mahkeme tarafından ilgili kişiye ait özlük dosyasının tüm içeriğinin kendilerine gönderilmesinin istendiği, bu bağlamda mahkeme tarafından talep edilen özlük dosyasının tüm içeriğinin şikâyete konu sağlık raporları da dâhil olmak üzere herhangi bir bilgi ve belge ayırt edilmeksizin mahkeme ile paylaşıldığı, mahkeme emrinin yerine getirilmesini müteakip şikâyete konu raporların şirket savunması ve iş akdi feshi sebebine ilişkin maddi vakıaların ispatı amacıyla hukuka ve dürüstlük kurallarına uygun ve işlendiği amaç ile bağlantılı, sınırlı ve ölçülü olarak cevap dilekçesine de eklenerek mahkemeye sunulduğu

ifade edilmiştir.

Konuya ilişkin yapılan inceleme neticesinde: Kişisel Verileri Koruma Kurulunun 18/02/2020 tarih ve 2020/138 sayılı Kararı ile;

- Kanunun 3 üncü maddesinin (1) numaralı fıkrasının (ç) bendi uyarınca “ilgili kişi” tanımlaması, kişisel verisi işlenen gerçek kişiyi ifade ederken; (ı) bendi uyarınca “veri sorumlusu” tanımlamasının, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi; (e) bendi uyarınca da “kişisel verilerin işlenmesi” tanımlamasının, kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade ettiği,

- Kanunun “Genel ilkeler” başlıklı 4 üncü maddesi hükmü uyarınca kişisel verilerin, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği ve kişisel verilerin işlenmesinde

“a) Hukuka ve dürüstlük kurallarına uygun olma.

b) Doğru ve gerektiğinde güncel olma.

c) Belirli, açık ve meşru amaçlar için işlenme.

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme” ilkelerine uyulmasının zorunlu olduğu,

- Kanunun “Kişisel verilerin işleme şartları” başlıklı 5 inci maddesi hükmü uyarınca da kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemeyeceği ancak,

“a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işleminin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.” şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu,

- Kanunun 6 ncı maddesinin (1) numaralı fıkrasında ise kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerinin özel nitelikli kişisel veri olduğu, (2) numaralı fıkrasında özel nitelikli kişisel verilerin ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğu, (3) numaralı fıkrasında, birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel verilerin kanunlarda öngörülen hallerde, sağlık ve cinsel hayata ilişkin kişisel verilerin ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceğinin hükme bağlandığı,
- 4857 sayılı İş Kanununun işçi özlük dosyası başlıklı 75 inci maddesine göre; işverenin çalıştırdığı her işçi için bir özlük dosyası düzenlediği, bu dosyada, işçinin kimlik bilgilerinin yanında, bu kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorunda olduğu, ayrıca idari para cezası başlıklı 104 üncü maddesinde Kanunun 75 inci maddesinde belirtilen işçi özlük dosyalarını düzenlemeyen işveren veya işveren vekiline idari para cezası verileceği, ancak sağlık raporlarının işçiye ait özlük dosyasının içerisinde yer alıp alamayacağı hususuna ilişkin ise gerek 4857 sayılı İş Kanununda gerekse 6331 sayılı İş Sağlığı ve Güvenliği Kanununda özel bir hüküm bulunmadığı,

- Dięer yandan 6100 sayılı Hukuk Muhakemeleri Kanununun 219 uncu maddesinin 1 inci fıkrası uyarınca, tarafların, kendilerinin veya karşı tarafın delil olarak dayandıkları ve ellerinde bulunan tüm belgeleri mahkemeye ibraz etmek zorunda olduęu, bununla birlikte, anılan Kanunun 220 nci maddesinin 3 üncü fıkrası uyarınca, belgeyi ibraz etmesine karar verilen tarafın, kendisine verilen sürede belge ibraz edilmez ve aynı sürede, delillerle birlikte ibraz edilmemesi hakkında kabul edilebilir bir mazeret gösterilmez ya da belgenin elinde bulunduęu inkâr edilirse, mahkemenin, duruma göre belgenin içerięi konusunda dięer tarafın beyanını kabul edebileceęi,
 - 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun “İncelenemeyecek Dilekçeler” başlıklı 6 ncı maddesinde, Türkiye Büyük Millet Meclisine veya yetkili makamlara verilen veya gönderilen dilekçelerden yargı mercilerinin görevine giren konularla ilgili olanların incelenemeyeceęinin hüküm altına alındığı,
 - Somut olayda mahkemenin davaya ilişkin olarak yazmış olduęu müzekkerede davalı veri sorumlusundan davacı ilgili kişiye ait özlük dosyasının tüm içerięinin tasdikli bir suretinin gönderilmesini istedięinin görüldüğü
- deęerlendirmelerinden hareketle
- 6698 sayılı Kanunun 28 inci maddesinin (1) numaralı fıkrasının (d) bendinde yer alan “Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi” hükmü ile 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun’un “İncelenemeyecek Dilekçeler” başlıklı 6 ncı maddesinin (b) bendi dikkate alındığında konuya ilişkin Kurul tarafından tesis edilecek bir işlem bulunmadığına karar verilmiştir.

2020/124 sayılı KVKK Kararı

Veri sorumlusu havayolu şirketi bünyesindeki çalışanın ilgili kişiye ait kişisel verileri 6698 sayılı Kişisel Verilerin Korunması Kanununa aykırı şekilde şirket kayıtlarından elde etmesi hakkında Kişisel Verileri Koruma Kurulunun 13/02/2020 tarihli ve 2020/124 sayılı Karar Özeti

Karar Tarihi : 13.02.2020

Karar No : 2020/124

Konu Özeti : Veri sorumlusu bünyesindeki çalışanın ilgili kişiye ait kişisel verileri 6698 sayılı Kişisel Verilerin Korunması Kanununa aykırı şekilde şirket kayıtlarından elde etmeleri hakkında.

İlgili kişi tarafından Kuruma intikal ettirilen şikâyette özetle, veri sorumlusu bünyesindeki çalışanın ilgili kişiye ait uçuş bilgilerini şirket kayıtlarından elde ettiği, bunu da bir başka çalışanla paylaştığı, bu çalışanın da söz konusu bilgileri ilgili kişiye iletmediği, aralarındaki husumet nedeniyle ilgili kişinin her uçuş sonrası aranarak verileri elde eden çalışan tarafından rahatsız edildiği, durumun veri sorumlusuna e-posta ile bildirildiği, ancak, aramalara devam edilmesi üzerine noter aracılığıyla veri sorumlusuna ihtarname gönderildiği, veri sorumlusunun vermiş olduğu cevapta çalışanın kişisel verileri elde ettiğinin tespit edildiği, fakat çalışan hakkında bir işlem yapılmadığının belirtildiği, daha sonrasında, aramaların devam ettiği, ilgili kişinin hakaret ve tehditlere maruz kaldığı, bunun üzerine, yetkili makamlara bildirimde bulunduğu, ancak yaptığı başvurular çerçevesinde veri sorumlusu tarafından verilen cevabın ve alınan aksiyonların yetersiz olduğu belirtilerek konunun 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında incelenmesi talep edilmiş ve yazı ekinde ayrıca her iki çalışan ile gerçekleştirdiği kişisel telefonuna ait whatsapp konuşma görüntüleri, telefon çağrı geçmişi kayıtları ve PNR bilgileri sunulmuştur.

Kuruma intikal eden şikâyet dilekçesi ekinde yer alan veri sorumlusunun ilgili kişiye verdiği cevapta özetle,

- Kişisel verileri elde eden çalışanın görevi gereği yolcu bilgilerine erişim yetkisinin olduğu, bu çalışanın bilgiye erişim kayıtlarının incelenmesi neticesinde gerekli yaptırımların uygulandığı,
- Şikâyete konu kişiler arası görüşmelerin içeriğinin tespit edilemediği,

- Değerlendirmeler sonucunda, ilgili kişiye ait kişisel verilerin bazı ek kontroller uygulanmadan güvenlik amacıyla görüntülenmesini engelleyecek ek tedbirlerin uygulamaya alındığı, Kanunda belirtilen amaçlar ve yasal dayanaklara istinaden veri sorumlusu tarafından saklanan ilgili kişiye ait kişisel verilerin herhangi bir yetkisiz erişime konu olmadığı, kişisel verilerin gerekli teknik ve idari tedbirler uygulanarak muhafaza edildiği

ifade edilmiştir.

Başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişinin ilk olarak çalışanlar hakkında veri sorumlusuna dolandırıcılık ve haksız menfaat iddiasıyla şikâyette bulunduğu,

- Şikâyetin aynı gün iç denetim birimlerine iletildiği ve konu hakkında soruşturma başlatıldığı, ilgili kişi ve çalışanlarla yapılan görüşmeler ile veri sorumlusunun kayıtlarının incelenmesi sonucunda hiçbir aşamada dolandırıcılık, tehdit ve benzeri bir eylem tespit edilemediği,

- Ardından ilgili kişinin göndermiş olduğu ihtarnamenin veri sorumlusuna ulaştığı, şikâyetçi olduğu kişilere ait özel hayatın gizliliğini ihlal eder nitelikteki bazı görsel kayıtların da bizzat ilgili kişi tarafından veri sorumlusuna iletildiği, gerçek kişiler arasındaki bu durumun birden fazla adli sürece konu olduğu ve devam ettiği, bununla birlikte, kişilerin karşılıklı olarak 6284 sayılı Ailenin Korunması ve Kadına Karşı Şiddetin Önlenmesine Dair Kanun kapsamında adli tedbir talep ettiği, bu durumda ilgili kişilerin birbirlerine ait kimlik ve iletişim bilgilerine şirketlerinin müdahalesi ve kayıtları dışında sahip oldukları ve veri sorumlusunun ilgili kişi ile çalışanlar arasındaki kişisel ilişkilerin tarafı olmadığı, bu nedenle, veri sorumlusunun yürüttüğü incelemenin PNR kayıtlarına erişim ve bunların kullanımı üzerine olduğu,

- İlgili kişinin çalışanlar tarafından arandığının tevsiki için bildirdiği telefon numarasının veri sorumlusuna ait olmadığı ve telefon görüşmelerinin içeriğine yönelik şikâyetlerin soruşturma kapsamında değerlendirilmediği,

- Yapılan incelemeler neticesinde veri sorumlusu çalışanın ilgili kişiye ait PNR kayıtlarına yönelik sistemde arama yaptığının tespit edildiği,

- yöneticisi olan çalışanın uçuş operasyonlarına yönelik emniyet risklerini, güvenlik tehditlerini ve üst düzey yönetim adına güvenlik yönetim sistemi operasyonunun günlük işleyişini yönetmek ve izlemekten sorumlu olduğu,

- Erişim yetkisinin kişinin görev tanımı gereği ve 2920 sayılı Türk Sivil Havacılık Kanununun 40 ıncı maddesi dördüncü fıkrasında yer alan “*Havayolu ile seyahat edecek kişilerin bilgileri kişilerin seyahatini kolaylaştırmak veya güvenlik ve risk değerlendirmesi yapmak amacıyla Kanun çerçevesinde toplanabilir, kaydedilebilir, işlenebilir, paylaşılabilir, havacılık güvenliği ve emniyetini sağlamak üzere değerlendirilerek gereken tedbirler alınabilir*” hükmü doğrultusunda tanımlamış olması nedeniyle hukuka aykırı bir erişimin söz konusu olmadığı,
- Değerlendirmeler sonucunda ilgili kişiye ait kişisel verilerin saklanması ve erişim yetkilerinin tanımlanması konusunda hukuka aykırı bir durum olmadığı,
- Yürütülen soruşturma kapsamında görev gereği erişim yetkisi bulunan kişisel verileri kişisel çıkarlar doğrultusunda görüntülemenin Kanunda yer alan ilkelere aykırı olduğu, bununla birlikte, Kanuna aykırı olarak görüntülenen kişisel verilerin yetkisiz üçüncü kişiler ile paylaşılmadığı,
- Kişisel verilerin iş amacı dışında kullanılması sonucu oluşan bir zarar tespit edilmediği,
- Kişisel verilerin veri sorumlusu tarafından işlenmesine devam edilmesi nedeniyle ilgili kişinin temel hak ve hürriyetlerine yönelik veya mevcut bir durum nedeniyle ilgili kişi haricindeki yolculara ait kişisel verilere yönelik herhangi bir ihlal tespit edilmediği,
- Kanuna aykırı olarak kişisel verileri görüntüleyen çalışan hakkında yazılı uyarı verildiği ve yetkilerinin iptal edilerek görevleri kapsamındaki tüm sorgulama taleplerinin ayrı bir departman üzerinden gerçekleştirilmesinin sağlandığı,
- Veri sorumlusu bünyesinde farkındalığın artırılması adına çalışanlara yönelik çevrim içi eğitim gerçekleştirildiği,
- İç denetim birimleri tarafından yapılan kontroller sonucunda şikâyet bildiriminden sonra herhangi bir sorgulama gerçekleştirilmediği, bu nedenle, alınan tedbirlerin olumlu sonuç doğurduğu,
- İlgili kişinin, 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı maddeleri kapsamında kişisel verilerin hukuka aykırı olarak ele geçirildiği iddiasıyla suç duyurusunda bulunduğu ve soruşturmanın halen devam ettiği,
- Çalışanlara yönelik veri güvenliği konusunda belirli aralıklarla eğitim ve farkındalık çalışmaları yürütüldüğü, bu kapsamda, soruşturması yapılan çalışanların eğitimlerini başarı ile tamamladığı ifade edilmiştir.

Söz konusu iddiaların incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 13/02/2020 tarih ve 2020/124 sayılı Kararında;

- Kişisel Verilerin Korunması Kanununun 12 inci maddesinin veri sorumlusunun veri güvenliğine ilişkin yükümlülüklerini düzenlediği, buna göre “(1) Veri sorumlusu;

Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

Kişisel verilerin muhafazasını sağlamak,

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

(2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

(3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

(4) Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.” hükmüne yer verildiği,

- Somut olayda, veri sorumlusunun yürüttüğü soruşturma kapsamında kişisel verileri elde eden çalışanın ifadesine başvurulduğu, bu doğrultuda, şikâyete konu çalışanın, ilgili kişinin kişisel verilerinin paylaşıldığı diğer çalışanın uçuşlarına katılacağı düşünerek, sistem üzerinden arama gerçekleştirdiğini kabul ettiği, diğer taraftan, ilgili kişi ile arasında hâlihazırda dava durumu söz konusu olduğu, mahkeme sürecinin başladığı, bunun yanı sıra, ilgili kişiye hiçbir müdahalede bulunulmadığı,

- Dilekçe ekinde yer verilen söz konusu Whatsapp konuşma ve telefon çağrı geçmişi görüntülerinin veri sorumlusu çalışanlarına ait olup olmadığı konusunda herhangi bir bilginin bulunmadığı, bununla birlikte, veri sorumlusunun soruşturma raporuna göre kişisel verileri elde eden çalışanın bu iddiaları kabul etmediği dikkate alındığında, ilgili kişinin telefonunda yer alan kişisel telefon kayıtlarının tevsik edici belge olarak değerlendirilemeyeceği,

- Diğer taraftan, veri sorumlusu tarafından şikâyete konu olan kişiler arası görüşmelerin içeriğinin tespit edilemediği, telefon görüşmelerine ilişkin şikâyetlerin olaya konu olan kişiler arasındaki bireysel ilişkilerin geçmişinden kaynaklanma ihtimalinin yüksek olduğunun belirtildiği,

- Erişim yetkisinin görev tanımı gereği ve 2920 sayılı Türk Sivil Havacılık Kanununun 40 ıncı maddesinin dördüncü fıkrasında yer alan “Havayolu ile seyahat edecek kişilerin bilgileri kişilerin seyahatini kolaylaştırmak veya güvenlik ve risk değerlendirmesi yapmak amacıyla Kanun çerçevesinde toplanabilir, kaydedilebilir, işlenebilir, paylaşılabilir, havacılık güvenliği ve emniyetini sağlamak üzere değerlendirilerek gereken tedbirler alınabilir” hükmü doğrultusunda tanımlandığı,
- Her ne kadar çalışanlar eğitime tabi tutulmuş ve bu eğitimleri başarıyla tamamlamış olsalar da olay öncesinde eğitimlerin seyrek düzenlenmiş olduğu,
- Ayrıca, çalışanın görev tanımı gereği yetkisi çerçevesinde PNR sorgulaması gerçekleştirdiği ancak Kasım 2018 tarihinde bir adet, Aralık 2018 tarihinde on iki adet, Ocak 2019 tarihinde beş adet, Mart 2019 tarihinde on adet sorgulama yapıldığı, veri sorumlusunun PNR sorgulama sayısına bir sınırlama getirmediği veya gözetim mekanizması geliştirmemiş olduğunun anlaşıldığı, veri sorumlusu tarafından her ne kadar log kayıtları tutuluyor olsa da, bu kayıtlarda sıra dışı aktivitelerin gözlemlenebilir olması ve bu kayıtların analiz edilmesi ile kişisel verilerin hukuka aykırı işlenmesinin ve erişilmesinin tespitinin önem arz ettiği dolayısıyla, veri sorumlusunun Kanunun 12 nci maddesi kapsamında aldığı idari ve teknik tedbirlerin yeterli olmadığı,
- Çalışanın yetkisini kötüye kullandığını kabul ettiği, bu nedenle, hakkında yazılı uyarı verildiği ve yetkilerinin iptal edildiği, sorgulama işlemlerinin ayrı bir Genel Müdür Yardımcılığına bağlı farklı bir departmana verildiği ve bunun sonucunda sunulan log kayıtlarında PNR sorgulamasının yapılmadığının anlaşıldığı, öte yandan, kişisel verilerin hukuka aykırı olarak işlenmemesine yönelik özel koruyucu düzenlenmelere yer verildiği, ancak, soruşturma sonucu çalışanın yetkilerine ilişkin yaptırımların yeterli ve caydırıcı olmadığı, bu tür zafiyetlerin yaşanma riski göz önünde bulundurularak, alınması gereken tedbirlerin geliştirilmesi gerektiği,
- Kanunun 17 nci maddesi (1) numaralı fıkrası uyarınca ise kişisel verilere ilişkin suçlar bakımından 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümlerinin uygulandığı, veri sorumlusunun savunma yazısında, ilgili kişinin, çalışanlar ile birlikte veri sorumlusu hakkında 5237 sayılı Kanunun 135 ila 140 ıncı maddeleri kapsamında suç duyurusunda bulunduğu ve soruşturmanın halen devam ettiği, bu doğrultuda, 5237 sayılı Kanun kapsamında yürütülmekte olan bir soruşturmanın bulunması sebebiyle, 5237 sayılı Kanununun ilgili hükümleri çerçevesinde işlem tesis edilmesini teminen 5271 sayılı Ceza Muhakemesi Kanununun 158 inci maddesi hükmü uyarınca konunun Cumhuriyet Başsavcılığına bildirilmesine gerek olmadığı

değerlendirilmiş olup bu doğrultuda, veri sorumlusu tarafından kişisel verilere erişim ile ilgili sınırlama getirilmemesi ve çalışanlara verilen eğitimin yetersiz olması sebebiyle Kanunun 12 nci

maddesinde yer alan veri güvenliđinin sađlanmasına ynelik gerekli idari ve teknik tedbirlerin alınmadıđı kanaatine varıldıđından Kanununun 18 inci maddesinin birinci fıkrasının (b) bendi çerçevesinde veri sorumlusu hakkında 100.000 TL idari para cezası uygulanmasına karar verilmiřtir.

2020/120 sayılı KVKK Kararı

İlgili kişilerin kişisel verileri olan banka hesap hareketlerinin, mevduat bilgilerinin, para yatırma ve çekme işlemlerinin açık rızaları olmaksızın vergi müfettiş yardımcısı tarafından hukuka aykırı olarak işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 13/02/2020 tarihli ve 2020/120 sayılı Karar Özeti

Karar Tarihi : 13.02.2020

Karar No : 2020/120

Konu Özeti : İlgili kişilerin kişisel verileri olan banka hesap hareketlerinin, mevduat bilgilerinin, para yatırma ve çekme işlemlerinin açık rızaları olmaksızın vergi müfettiş yardımcısı tarafından hukuka aykırı olarak işlenmesi

Kuruma intikal eden şikayet dilekçesinde özetle; ilgili kişilerin çalışmakta olduğu mükellef kurum hakkında Vergi Müfettiş Yardımcısı tarafından yapılmış olan bir vergi incelemesi sonucunda düzenlenen "Vergi Tekniği Raporunda" (Rapor) kendileri ile ilgili bir vergi incelemesi olmamasına rağmen şahıslarına ait kişisel veri olan banka hesap hareketlerinin, mevduat bilgilerinin, para yatırma ve çekme işlemlerinin rızaları olmaksızın hukuka aykırı olarak işlendiği belirtilerek, veri sorumlusu ile ilgili olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Bu kapsamda, başlatılan inceleme çerçevesinde veri sorumlusu Bakanlıktan şikâyete konu Raporda adı geçen şikâyetçilerin yapılan vergi incelemesinin konusu olup olmadığı; şikâyetçilerin şahıslarının vergi incelemesinin konusu olmamasına rağmen banka hesap hareketlerine, mevduat bilgilerine, para yatırma ve çekme işlemlerine bakılmış olması halinde bunun hangi yasal gerekçelerle yapıldığı hususlarının açıklanması istenilmiştir. Veri sorumlusundan alınan cevabi yazıda;

- Vergi Denetim Kurulu Maltepe Küçük ve Orta Ölçekli Mükellefler Grup Başkanlığının görevlendirme yazılarında, mükellef şirketin 2012 ila 2016 yılları arası ihracat teslimleri nedeniyle KDV iadesi yönünden incelenmesinin istendiği,
- Herhangi bir hazine zararı doğmaması adına kapsamlı bir araştırma yapıldığı ve yapılan araştırmada, mükellefin banka hesaplarında normal hayata ve ticari icaplara uymayan şekilde, banka

şubesinde yüklü miktarlarda elden para yatırma işlemlerinin tespit edildiği; söz konusu işlemleri mükellefin %100 ortağı olan şahıs ve bu şahıs tarafından kurumu temsile vekil tayin edilen şikayetçi ilgili kişilerin gerçekleştirdiği,

- İlgili kişiler tarafından yatırılan paraların yine aynı gün içinde çek keşide edilmek suretiyle borcun ödenmesinde kullanıldığı; yapılan araştırmada, çekin mükellef şirket tarafından borçluya verildiği gün birçok firma tarafından, tek elden çıkmış gibi ciro edildiği ve aynı gün para yatırılan banka şubesinde, herhangi bir mükellefiyeti olmayan alakasız kişiler tarafından tahsil edildiğinin tespit edildiği,

- Ciro silsilesinde yer alan firmalar hakkında olumsuz tespitler bulunması üzerine 213 sayılı Vergi Usul Kanununun 3 üncü maddesi gereğince olayın gerçek mahiyetini ortaya çıkarmak üzere 178 sayılı Maliye Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 39 uncu maddesi ile 31/10/2011 tarihli ve 28101 sayılı Resmi Gazetede yayımlanan Vergi Denetim Kurulu Yönetmeliğinin 80 inci maddesine dayanılarak hazırlanan “Vergi İncelemeleri ile İlgili Bilgi Taleplerinde Uyulacak Usul ve Esaslara İlişkin Yönerge”nin 6 ncı maddesi hükmü gereğince ilgili kişilerin, sadece mükellef kurumun çek ödemesi olarak kullandığı bankalarda bulunan hesapları hakkında bilgi talebinde bulunulduğu,

- Banka hesaplarının incelenmesi neticesinde şüphelerin yerinde olduğunun görüldüğü, mükellef şirketin çekleri tahsil edilir iken, tahsil edilen tutarlar bazında, ilgili kişiler tarafından şahsi banka hesaplarına kimi zaman aynı tutar kimi zaman ise farklı tutarların geri yatırıldığına tespit edildiği ve pek çok çekin tahsilatı sırasında ilgili kişilerin aynı şubede bulunup işlem gerçekleştirdiğinin anlaşıldığı,

- Bakanlık Vergi Müfettişlerinin, yürüttükleri vergi incelemeleri ile ilgili bilgi istemelerinin esas olduğu, müfettiş tarafından istenen bilgilerin gerek mükellef şirket tarafından adı geçen iki şahsa vekâlet verilmesi gerek incelenen mükellefin işlemlerinde önemli bir yer teşkil etmesi nedenleriyle, incelemenin dışına çıkılması ve ilgisiz kişilerin banka hesaplarının istenmesi anlamını taşımadığı, diğer bir deyişle yapılan işlemin yasal olduğu

ifadelerine yer verilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 13/02/2020 tarih ve 2020/120 sayılı Kararı ile,

- 213 sayılı Vergi Usul Kanununun (213 sayılı Kanun) “Vergi Kanunlarının uygulanması ve ispat” başlıklı 3 üncü maddesinin B fıkrasına göre, vergiyi doğuran olay ve bu olaya ilişkin her türlü işlemin

yemin dışındaki her türlü delille ispatlanabileceği, olayın özelliğine göre mutad olmayan bir durumun iddia olunması halinde ispat külfetinin iddia edende olduğu

- 213 sayılı Kanunun “İncelemeye yetkililer” başlıklı 135 inci maddesine göre vergi incelemesinin; vergi müfettişleri, vergi müfettiş yardımcıları, ilin en büyük mal memuru veya vergi dairesi müdürleri tarafından yapıldığı,
- Benzer şekilde, 213 sayılı Kanunun “İncelemede uyulacak esaslar” başlıklı 140 inci maddesinin yedinci fıkrası çerçevesinde vergi raporlarının hukuka aykırı olmaması bakımından katı ve çok aşamalı prosedürlerin öngörüldüğü,
- Yine, anılan maddenin on birinci fıkrasının; “*Bu maddede belirlenen esaslar çerçevesinde, vergi incelemelerinde uyulacak diğer usul ve esaslar, komisyonların teşekkülü ile çalışma usul ve esasları ve Merkezi Rapor Değerlendirme Komisyonu tarafından doğrudan değerlendirmeye tabi tutulacak vergi inceleme raporlarının tutarları, Maliye Bakanlığınca çıkarılan yönetmelikle belirlenir.*” hükmünü; 178 sayılı “Maliye Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname”nin “Bakanlığın düzenleme görev ve yetkisi” başlıklı 39 uncu maddesi ise; “*Bakanlık, kanunla yerine getirmekle yükümlü olduğu hizmetleri tüzük, yönetmelik, tebliğ, genelge ve diğer idari metinlerle düzenlemekle görevli ve yetkilidir.*” hükmünü amir olduğu,
- Anılan düzenlemelere dayanarak yayımlanan “Vergi İncelemelerinde Uyulacak Usul ve Esaslar Hakkında Yönetmelik”in (**Yönetmelik**) amacının, vergi incelemelerinde uyulacak usul ve esasları düzenlemek olduğu, Yönetmeliğin “Vergi inceleme görevinin verilmesi” başlıklı 6 ncı maddesi uyarınca;

“(1) Vergi inceleme görevi yazı ile verilir. İnceleme görevi yazılarında; nezdinde inceleme yapılacak kişilere ve konulara ilişkin bilgilere, incelemenin türüne, gerekçesine, dönemine ve süresine ilişkin hususlara yer verilir. İnceleme görev yazısı ekinde yer alan belgeler, elektronik ortamda inceleme yapmaya yetkili olanlara gönderilebilir.

(...)

(3) Vergi incelemesi, sadece inceleme görev yazısında belirtilen konu ve döneme ilişkin olarak yapılır. İnceleme konusu ve dönemi ile ilgili olmayan herhangi bir hususa ilişkin mükelleften bilgi ve belge talebinde bulunulamaz. Yürütülmekte olan incelemeler sırasında, görevlendirme yazısında belirtilenden farklı bir konu veya döneme ilişkin eleştiriyi gerektiren hususların tespiti durumunda söz konusu durum inceleme görevini verenlere bildirilir. Görevlendirme yazısında yer alan inceleme konusuna giren tespitlerin, bu yazıda yer almayan farklı vergi türlerine ilişkin olarak da rapor yazılmasını gerektirmesi durumunda, bu husus yeni bir görevlendirme gerektirmez.

(4) Yürütülmekte olan incelemeler sırasında farklı bir mükellef nezdinde inceleme yapılma ihtiyacı duyulduğunda durum gerekçeleri ile birlikte bağlı olunan birime bildirilir. (...)” hükmünün düzenlendiği,

• Diğer bir deyişle, vergi incelemesi esnasında görevlendirmede yer alandan farklı bir konu veya döneme ilişkin eleştiriyi gerektiren hususlar tespit edilirse, herhangi bir yeni görevlendirmeye gerek olmaksızın bu durum inceleme görevini verene bildirilerek o konuya ilişkin araştırma yapılabileceği, kaldı ki, Vergi Müfettiş Yardımcısı tarafından düzenlenen cevabi yazıda yapılan kişisel veri işleme faaliyetinin inceleme kapsamında kaldığının ifade edildiği,

• Yönetmeliğin “İnceleme tutanakları” başlıklı 16 ncı maddesinde;

“MADDE 16 - (...)”

(4) Tutanakta yer alan hususların vergi kanunları karşısında yapılması muhtemel işlemler bakımından ispatlama vasıtası olduğu ve yapılması muhtemel işlemlerin neler olduğu mükellefe izah edilir.

(5) Vergi incelemesi yapmaya yetkili olanlar, ilgilileri tutanakları imzalamaları için zorlayamazlar. İlgililer tutanakları imzalamaktan çekindikleri takdirde tutanakta bahis konusu edilen olaylar ve hesap durumlarını ihtiva eden defter ve belgeler, nezdinde inceleme yapıldan rızasına bakılmaksızın alınır ve inceleme neticesinde tarh edilen vergiler ve kesilen cezalar kesinleşinceye kadar geri verilmez. İlgililer her zaman bu tutanakları imzalayarak defter ve belgeleri geri alabilirler.

(6) Suç delili olan defter ve belgeler mükellefin rızasına bakılmaksızın alıkonulur. (...)”

hükmüne yer verildiği,

• Bu kapsamda, mükellef tutanakları imzalamaktan imtina etse dahi tutanakta yer alan olayları ve hesap durumlarını içeren defter ve belgelerin mükellefin rızası olmaksızın alıkonulacağı, benzer şekilde, suç delili niteliğinde olan defter ve belgelerin de mükellefin rızası olmaksızın alıkonulabileceği,

• Öte yandan, Yönetmeliğin 17 nci maddesinin birinci fıkrasının (c) bendinde “vergilendirme ile ilgili olaylar ve/veya hesap durumları”nın vergi inceleme tutanaklarında yer alacağı hususunun da düzenlendiği,

• Söz konusu Rapor bakımından yapılan işlemlerin kişisel veri işleme faaliyeti olduğu ve bu kapsamda Bakanlığın veri sorumlusu; vergi müfettiş yardımcısının ise Bakanlığın çalışanı olduğu, Kanunun 5 inci maddesinin (1) numaralı fıkrasında; kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği; (2) numaralı fıkrasında belirtilen şartlardan birinin varlığı halinde ise, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğunun hükme

bağlandıđı, vergi incelemesine ilişkin olarak bu incelemenin amacı ve gerçekleştirilmesine yönelik 213 sayılı Kanunda ve ilgili Yönetmelikte detaylı düzenlemelere yer verildiđi, bu çerçevede, somut olay bakımından yapılan incelemede işlenen kişisel verilerin Kanunun 5 inci maddesinin (2) numaralı fıkrasının (ç) bendinde yer alan “Veri sorumlusunun hukuki yükümlülüđünü yerine getirebilmesi için zorunlu olması” şartı kapsamında işlendiđinin deđerlendirildiđi,

- Öte yandan, Kanunun “İstisnalar” başlıklı 28 inci maddesinin ikinci fıkrasının (c) bendinde kişisel veri işlemenin kanunun verdiđi yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliđindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması halinde, Kanunun veri sorumlusunun aydınlatma yükümlülüđünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüđünü düzenleyen 16 ncı maddelerinin uygulanmayacađının hükme bağlandıđı,

- Bu kapsamda incelemeye konu edilen yazı bağlamında Kanunun “İstisnalar” başlıklı 28 inci maddesinin (2) numaralı fıkrasının (c) bendinin uygulanıp uygulanmayacađı deđerlendirildiđinde kamu kurumu niteliđini haiz Bakanlıđın, 213 sayılı Kanunun verdiđi yetkiye dayanarak denetleme görevi kapsamında kişisel verileri işlediđinin anlaşıldıđı, somut olayda veri işleme şartları bulunmakla birlikte kısmi istisna olarak sayılan Kanunun 28 inci maddesinin (2) numaralı fıkrasının (c) bendinin uygulanacak olması dolayısıyla söz konusu kişisel veri işleme faaliyetleri bakımından Kanunun veri sorumlusunun aydınlatma yükümlülüđünü düzenleyen 10 uncu, veri sorumluları sicilinde kayıt yükümlülüđünü düzenleyen 16 ncı ve zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci maddelerinin uygulama alanı bulmayacađı ancak veri sorumlusunun Kanunun diđer hükümleri ile bađlı olacađı,

- Ayrıca, Kanunun “Genel ilkeler” başlıklı 4 üncü maddesinde ise, kişisel verilerin ancak bu Kanunda ve diđer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceđi ve kişisel verilerin işlenmesinde maddede; “a) Hukuka ve dürüstlük kurallarına uygun olma. b) Doğru ve gerektiđinde güncel olma. c) Belirli, açık ve meşru amaçlar için işlenme. ç) İşlendikleri amaçla bađlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.” şeklinde sayılan ilkelere uyulmasının zorunlu olduđunun düzenleme altına alındıđı, anılan madde hükmünden açıkça anlaşılaçađı üzere, kişisel verilerin işlenmesinde her hal ve şartta Kanunun 4 üncü maddesinde sayılan genel ilkelere uyulmasının hukuki bir gereklilik olduđu,

- Bakanlıđın cevabi yazısı ve eki evrakta, üç farklı görevlendirme yazısına istinaden, mükellef kurumun 2012 ila 2016 yılları arası ihracat teslimleri nedeniyle KDV iadesi yönünden incelenmesi

sürecinde; mükellef kurumun banka hesaplarında normal hayata ve ticari icaplara uymayan şekilde, banka şubelerinden yüklü miktarlarda elden para yatırma işlemlerinin gerçekleştirildiğinin ve bu işlemlerin de mükellef kurumun %100 ortağı olan şahıs tarafından kurumu temsile vekil tayin edilen ilgili kişiler tarafından gerçekleştirildiğinin tespit edilmesi üzerine, 213 sayılı Kanununun 3 üncü maddesi gereğince olayın gerçek mahiyetini ortaya çıkarmak amacıyla, adı geçen kişilerin sadece mükellef kurumun çek ödemesi olarak kullandığı bankalarda bulunan hesaplarının inceleme sürecine dâhil edildiğinin belirtildiği, bu çerçevede, başvuran ilgili kişilerin kişisel verilerinin hukuka ve ölçülülük ilkesine uygun olarak işlendiği,

- 213 sayılı Kanununun “Vergi mahremiyeti” başlıklı 5 inci maddesi uyarınca vergi muameleleri ve incelemeleri ile uğraşan memurların görevleri dolayısıyla, mükellefin ve mükellefle ilgili kimselerin şahıslarına, muamele ve hesap durumlarına, işlerine, işletmelerine, servetlerine veya mesleklerine ilişkin olmak üzere öğrendikleri sırları veya gizli kalması lazım gelen diğer hususları ifşa edemeyecekleri ve kendilerinin veya üçüncü şahısların nef’ine kullanamayacakları hususunun hüküm altına alındığı, ayrıca, bahsi geçen yasağın bu kişiler görevlerinden ayrılışları dahi devam edeceği de aynı hüküm altında vurgulandığı, ilgili düzenlemeden de görüleceği üzere, inceleme kapsamında mükellefle ilgili kimselerin hesap durumlarının elde edilebileceği gibi; bu görevi ifa eden memurların da konuya ilişkin sır saklama yükümlülüğü bulunduğu, başvuran ilgili kişilerin mükellef kurumun %100 ortağı olan kişi tarafından kendilerine vekâlet verilmesi suretiyle şirketi temsile haiz olmaları nedeniyle bu kişilerin “mükellefle ilgili kimseler” kapsamında değerlendirileceği, dolayısıyla, başvuranlara ait kişisel veri olan hesap numaralarının incelemeye konu olabileceği değerlendirmelerinden hareketle,

- Vergi Usul Kanunu ve sair mevzuat hükümleri de incelendiğinde, şikâyete konu veri işleme faaliyetinde; vergi incelemesi kapsamında mükellefle ilgili kimselerin hesap durumlarının elde edilebileceği, bu nedenle ilgili kişilerin mükellefin %100 ortağı tarafından kendilerine vekâlet verilmesi suretiyle şirketi temsile haiz olmaları nedeniyle bu kişilerin “mükellefle ilgili kimseler” kapsamında değerlendirilebileceğine, bu noktada tüm mükellef şirket çalışanlarının değil şirketi temsile yetkili kişilerin mükellefin çek ödemesi olarak kullandığı banka hesaplarıyla sınırlı olarak kişisel verilerinin işlenmesinin ölçülülük ilkesine uygun olduğuna, bu çerçevede, Kanununun 28 inci maddesinin (2) numaralı fıkrasının (c) bendi uyarınca yapılan kişisel veri işleme faaliyetinin Kanununun 5 inci maddesinin (2) numaralı fıkrasının (ç) bendi kapsamında veri sorumlusunun hukuki yükümlülüğü çerçevesinde yerine getirildiğine ve şikâyete konu kişisel verilerin açık rıza olmaksızın işlenebileceğine karar verilmiştir.

2020/118 sayılı KVKK Kararı

İlgili kişinin, veri sorumlusu bir banka nezdindeki kişisel verileri olan hesap ve kiralık kasa bilgilerinin aktarılması hakkında Kişisel Verileri Koruma Kurulunun 13/02/2020 tarihli ve 2020/118 sayılı Karar Özeti

Karar Tarihi : 13.02.2020

Karar No : 2020/118

Konu Özeti : İlgili kişinin veri sorumlusu bir banka nezdindeki kişisel verileri olan kiralık kasa bilgilerinin aktarılması

Kuruma intikal eden şikayet dilekçesinde özetle; ilgili kişiye karşı İcra ve İflas Kanunu hükümlerine aykırı ve haksız bir şekilde icra takibine geçildiği, Tebligat Kanununa aykırı tebligat hileleri yapılarak ilgili kişi adına ödeme emrinin kesinleştirildiği, bunun üzerine şikayete konu bankaya birinci haciz ihbarnamesi gönderildiği ve Bankanın şubelerinden birinde yer alan kiralık kasasına fiili haciz uygulandığı, ayrıca icra takibinde borçlu konumunda olan ilgili kişinin iş yaptığı kişi ve şirketler, çalışma arkadaşları, ortak olduğu şirketler, şirket bilgilerinin resmi olmayan yollarla ele geçirildiği, kimse tarafından bilinmeyen kişisel verisi olan banka hesap ve kiralık kasa bilgisinin paylaşıldığı hususları belirtilerek 6698 sayılı Kişisel Verilerin Korunması Kanununun (**Kanun**) 11 inci maddesi kapsamında ilgili kişinin hesap ve kiralık kasa bilgilerinin işlenip işlenmediği, işlenme amacı ve bu amaca uygun kullanılıp kullanılmadığı, yurt içi ve yurt dışındaki üçüncü kişilere aktarma yapıp yapılmadığı hususlarının tespiti ile hukuka aykırılıklar nedeniyle veri sorumlusu hakkında gereğinin yapılması talep edilmiştir.

Başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenmiş olup verilen cevabî yazıda;

- İlgili kişi hakkında İstanbul İcra Dairesince 2019/... sayılı dosya ile icra takibinin başlatıldığı, icra takibi sürecinde borçluların bankalar nezdindeki hak ve alacakları üzerine haciz tatbik etmek üzere İcra ve İflas Kanununun (İİK) 89 uncu maddesi uyarınca bankalara haciz ihbarnameleri gönderilmesi yönteminin uygulandığı, bu kapsamda yirmi iki banka ile birlikte kendi bankalarına da birinci haciz ihbarnamesi gönderildiği, bankalarının üçüncü kişi konumunda bulunduğu, icra takibinin haksız olduğu savının muhatabının kendileri olmadığı, bankanın icra takiplerinin haklılık

ve hukukilik denetimini yapmak gibi bir sorumluluğunun bulunmadığı, bankanın borçlunun alacaklı tarafından bilinen bir hesabı olmaması halinde, sistemde kayıtlı bankalara icra dosyasından ihbarname gönderilebildiği, ilgili kişinin hesap bilgilerinin, takip alacaklısına banka tarafından iletilmesinin söz konusu olmadığı, birinci haciz ihbarnamesine cevap verildiği, birinci haciz ihbarnamesine cevap verilmesinin her gün binlercesi yapılan işlemlerden olduğu, ilgili kişinin hesaplarının yer aldığı banka şubesi çalışanlarının anılan işlem süreçlerine katılmadığı, kiralık kasa haczi ve çilingir marifetiyle açılma işlemleri için alacaklı tarafından altı banka nezdinde talepte bulunulduğu ve İcra Müdürlüğü tarafından iki bankada haciz kararı verildiği, İcra İflas Kanununun 367 nci maddesi uyarınca Bankanın yasal yükümlülüklerini yerine getirdiği ifadelerine yer verilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 13/02/2020 tarih ve 2020/118 sayılı kararı ile;

- Kanunun amacının kişisel verilerin işlenmesinin disiplin altına alınması ile temel hak ve özgürlüklerin korunması, kişinin mahremiyet hakkı ile kişisel veri güvenliğinin korunması ve ayrıca kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek olduğu,
- Diğer taraftan; kişisel verilerin işlenme şartlarının belirlendiği Kanunun 5 inci maddesinin (1) numaralı fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmadan işlenemeyeceği hüküm altına alınmış olmakla birlikte, (2) numaralı fıkrasında, sayılan hallerde ilgili kişinin açık rızası olmadan kişisel verilerinin işlenmesine imkân tanındığı,
- İcra Dairelerinin 2004 sayılı İcra ve İflas Kanununun 1 inci maddesinde düzenlenen kanunen yetkili mercilerden olduğu, haciz işleminin, belli bir para alacağının ödenmesini sağlamak için borçluya ait mal ve haklara icra dairesi tarafından el konulması olarak tanımlandığı, haciz işlemlerini, alacaklının haciz istemi üzerine yetkili icra dairelerinin yerine getirdiği, somut olayda, haciz işleminin yetkili İcra Dairesi tarafından gerçekleştirildiği, yine, ilgili kişiye ödeme emrinin tebliğinin İcra Dairesi tarafından 7201 sayılı Tebligat Kanununa göre yapıldığı,
- Bu anlamda ilgili kişinin şikâyet başvurusunda belirttiği gibi haksız bir şekilde icra takibine geçildiği, haczin haksız olduğu ve tebligatın Tebligat Kanunu hükümlerine aykırı yapıldığı iddialarının veri sorumlusu tarafından yapılmış işlemlere ilişkin olmadığı, İcra Dairesi tarafından yasal olarak yapılmış işlemler ile ilgili olduğu, veri sorumlusu bankanın icra ve iflas hukuku bağlamında üçüncü kişi konumunda olduğu,

- Yine şikâyetçinin başvurusunda belirttiği söz konusu İcra Hukuk Mahkemesinin haciz işleminden sonraki tarihte, tebligatın usulsüz olduğu ve itiraz ile takibin kaldırılması kararı dolayısıyla icra takibinin ve haczin yasal dayanağı olmadığı iddiasının, şikâyet edilen veri sorumlusunun yasal yükümlülüğünden kaynaklanan kiralık kasa bilgisinin paylaşılmasına ilişkin olmadığı, Kurumun görev alanı ve kişisel verilerin korunması mevzuatı kapsamında bulunmadığı,
- Öte yandan, 2004 sayılı İcra ve İflas Kanununun “Borçlunun mevcudu hakkında malûmat vermek mecburiyeti” başlıklı 367 nci maddesinin “*İcra veya İflas dairelerinin borçlunun mevcuduna dair isteyeceği bütün malûmatı hakiki ve hükmi her şahıs derhal vermeğe ve talep halinde mevcudu bu dairelere teslim mecburdur.*” hükmü nedeniyle veri sorumlusunun borçlunun kişisel verilerini İcra Dairesine vermekle yükümlü olduğu, diğer bir ifade ile bankanın, bankacılık işlemleri anlamında ilgili kişinin kişisel verilerini işlediği, bu kapsamda veri sorumlusu sıfatını haiz olduğu ve kişisel veri olan hesap ve kiralık kasa bilgilerini İcra ve İflas Kanununun ilgili hükmü dolayısıyla İcra Dairesine aktardığı,
- Veri sorumlusunun cevap yazısında da belirttiği üzere, uygulamada haciz işleminin aşamalarından haciz ihbarnamesi gönderilmesinde icra daireleri tarafından mevzuata uygun olarak borçlunun alacaklı tarafından bilinen bir hesabının olmaması halinde, sistemde kayıtlı tüm bankalara haciz ihbarnameleri gönderildiği ve veri sorumlusunun ihbarname gönderilen ilgili bankalardan biri olduğu,
- Yine, İcra İflas Kanununun “Taşınır ve taşınmaz malların haczi” başlıklı 85 inci maddesinde “*Borçlunun kendi yedinde veya üçüncü şahısta olan taşınır mallarıyla taşınmazlarından ve alacak ve haklarından alacaklının ana, faiz ve masraflar da dahil olmak üzere bütün alacaklarına yetecek miktarı haczolunur.*” hükmünün yer aldığı,
- Aynı Kanunun 89 uncu maddesi uyarınca da malı elinde bulunduran üçüncü şahsın bundan böyle taşınır malı ancak icra dairesine teslim edebileceği, bu çerçevede ve ilgili Kanunun 367 nci maddesi hükmü nedeniyle, somut olayda veri sorumlusunun kiralık kasa bilgilerini icra dairesine aktarmasının ve haciz işlemi yapılmasının Kanunda açıkça öngörülen bir yükümlülük olduğunun anlaşıldığı,
- Veri sorumlusunun cevap yazısından, ilgili kişi tarafından öne sürüldüğü şekliyle kiralık kasa bilgisinin veri sorumlusu nezdinde bankacılık ve kişisel verilerin korunması mevzuatına aykırı bir biçimde elde edildiği iddiasına karşılık; alacaklı vekili, icra memuru ve veri sorumlusunun Şube yöneticisi, Operasyon yetkilisi ve diğer personelin ilk kez haciz işlemi sırasında karşılaştığının, alacaklı vekili ve memur tarafından ilgili kişinin Şube nezdinde kiralık kasanın olup olmadığının sorulması üzerine sistem üzerinden tespit yapıldığının ve polis nezaretinde kiralık kasanın çilingir

marifetiyle açıldığının anlaşıldığı, bu noktada İcra ve İflas Kanununa ve yasal usule uygun hareket edildiği

değerlendirmelerinden hareketle;

- Tebligat ve icra iflas mevzuatı yönünden inceleme yapıldığında, veri sorumlusu olarak şikâyet edilen bankanın, İcra Dairesince ödeme emrinin tebliğ edilmesi ve kiralık kasaya haciz konulması işlemleri nedeniyle kişisel verilerin korunması mevzuatından kaynaklanan bir sorumluluğunun bulunmadığı ve icra ve iflas hukuku bakımından üçüncü kişi konumunda olduğu,
- Kişisel veri olan hesap ve kiralık kasa bilgisinin veri sorumlusu nezdinde bankacılık ve kişisel verilerin korunması mevzuatına aykırı bir biçimde elde edildiğini gösteren bir bulguya rastlanılmadığı,
- Veri sorumlusu tarafından, ilgili kişinin kişisel verisi olan hesap ve kiralık kasa bilgilerinin, 2004 sayılı İcra İflas Kanununun 89 uncu ve 367 nci madde hükümleri çerçevesinde Kanunun 5 inci maddesinin (2) numaralı fıkrasının (ç) bendinde yer alan *“hukuki yükümlülüğün yerine getirilmesi”* şartına dayalı olarak Kanunun 8 inci maddesine uygun olarak icra iflas mevzuatı çerçevesinde aktarıldığı

hususları dikkate alındığında mezkûr iddialarla ilgili olarak Kanun kapsamında yapılacak bir işlem bulunmadığına karar verilmiştir.

2020/113 sayılı KVKK Kararı

Elektronik satış hizmeti sağlayan bir şirketin veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 11/02/2020 tarih ve 2020/113 sayılı Karar Özeti

Karar Tarihi : 11.02.2020

Karar No : 2020/113

Konu Özeti : Elektronik satış hizmeti sağlayan bir şirketin veri ihlali bildirimini

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Veri sorumlusu Şirketin e-ticaret sektöründe faaliyet göstermekte olduğu,
- Veri sorumlusunun internet sitesinden ve mobil uygulaması üzerinden ticari faaliyet amacı olmayan satıcılara ikinci el ürünlerini satmaları için bir aracı hizmet sağlayıcısı olarak teknik alt yapı sunduğu,
- Şirkete, internet sitesinin hacklendiği iddiasının iletildiği,
- Veri sorumlusunun personeli tarafından zaman zaman halka açık bağlantıların paylaşıldığı kafe ortamlarından çalışıldığı, ağ dinlemesinin de bu sırada gerçekleşmiş olabileceği,
- Azami 257.000 kişinin etkilenme ihtimalinin bulunduğu ancak veri sorumlusu tarafından 25 kişi dışında kimsenin veri ihlalden etkilenmiş olduğuna dair kayıt tespit edilmediği,
- İhlalden etkilenen ilgili kişi kategorilerinin kullanıcılar olduğu,
- İhlalden etkilendiği belirtilen kişisel verilerin ad, soyadı, e-posta adresi, kriptolanmış kullanıcı hesabı şifreleri olduğu, 973.147 üyeye kadar olan kullanıcılardan 172.490 adedinin sisteme Facebook profili üzerinden kayıt olduğu için e-posta adreslerinin sistemde bulunmadığı, ancak veri ihlalinin gerçekleştirildiği e-posta adresi ile Şirket arasında yapılan konuşmalarda; tüm veri tabanları, kaynak kodlar, dosya ve müşteri verilerinin ele geçirildiğinin iddia edildiği,
- İhlalden özel nitelikli kişisel verilerin etkilenmediği,
- Kayıtlı kullanıcılara bildirimde bulunulduğu

ifadelerine yer verilmiştir.

Söz konusu bildirim incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 11/02/2020 tarih ve 2020/113 sayılı sayılı Kararı ile;

Veri ihlalden önce veri sorumlusuna ait internet ağı dışında halka açık bağlantıların paylaşıldığı kafe ortamlarından sisteme herhangi bir kısıt bulunmaksızın erişildiği, sızma testlerinin ihlalden sonra yapıldığı, ihlal öncesi sistemlerinde kritik bilgilere erişime neden olabilecek SQL Injection, Cross Site Scripting gibi zafiyetlerin bulunduğu, mobil uygulama içerisine tanımlanmış SSL Sertifikası olmamasından dolayı uygulama trafiğinin rahatlıkla dinlenebildiği, politikaların ve müdahale planlarının ihlal gerçekleştikten sonra oluşturulduğu, veri ihlali gerçekleşmeden önce kurumsal eğitim ve farkındalık faaliyetlerinin düzenlenmediği ve veri ihlalinin ancak veri ihlalinin gerçekleştirilen kişinin veri sorumlusu ile iletişime geçmesi neticesinde tespit edilebildiği dikkate alınarak 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 200.000 TL idari para cezası uygulanmasına karar verilmiştir.

2020/108 sayılı KVKK Kararı

Veri sorumlusu sađlık firması tarafından eski alıřanı olan ilgili kiřinin kiřisel verilerinin rızası alınmaksızın aktarımı hakkında Kiřisel Verileri Koruma Kurulunun 11/02/2020 tarihli ve 2020/108 sayılı Karar zeti

Karar Tarihi : 11.02.2020

Karar No : 2020/108

Konu zeti : Veri sorumlusu sađlık firması tarafından eski alıřanı olan ilgili kiřinin kiřisel verilerinin rızası alınmaksızın aktarımı hakkında

Kuruma intikal eden Őikayette zetle;

- İlgili kiřinin sađlık alanında faaliyet gsteren veri sorumlusu Őirket bnyesinde belirli tarihler arasında alıřtıđı ve alıřma iliřkisini veri sorumlusu ile mutabık kalarak sonlandırmak suretiyle bařka bir Őirkette iře bařladıđı,
- İlgili kiřinin yeni iře bařladıđı Őirketin yetkilileri ile yapılan toplantıda, veri sorumlusu tarafından ilgili kiřinin ocuklarının ve eřinin uzun bir sredir Almanya'da yařadıkları ve ilgili kiřinin de bu lkeye tařınacađı, Trkiye'de fazla kalmayacađı gibi bilgilerin kendileri ile paylařıldıđı, ayrıca, ilgili kiřinin aldıđı maař, prim ve zel deme kořullarına riayet etmeksizin veri sorumlusu eski alıřtıđı Őirketten ayrıldıđı gibi iddiaların kendilerine iletildiđi belirtilerek ilgili kiřinin cevabının talep edildiđi,
- İlgili kiři hakkındaki bu bilgilerin veri sorumlusu eski alıřtıđı Őirket tarafından talep olmaksızın, ilgili kiřinin yeni iře bařladıđı Őirkete nce telefon ardından iki adet e-posta vasıtasıyla aktarıldıđının đrenildiđi,
- Bunun zerine konuyla ilgili olarak veri sorumlusu Őirkete ihtarname gnderildiđi, ilgili kiřinin yeni alıřmaya bařladıđı Őirketin bir talebi olmamasına rađmen ilgili kiřinin ailesi ve veri sorumlusu ile olan maddi iliřkilerinin, veri sorumlusu tarafından sz konusu Őirkete aktarılmasına esas teřkil eden bir sebep bulunmaması veya ilgili kiřinin ıkarları ve makul beklentilerinin gz nne alınmamasının, bu konuda herhangi bir haklı gerekeye dayanılmamasının, *"hukuka ve drstlk kurallarına uygun olma"* ilkesine aykırılık teřkil ettiđi, yine sz konusu Őirket ile ilgili kiřinin aık rızası

olmaksızın kişisel verilerinin paylaşılmasındaki amacın anlaşılmadığı ve tüm şartlar göz önüne alındığında hukuken korunan meşru bir amaç güdülmeyeceğinin de aşikâr olduğu, bu durumun “*belirli, açık ve meşru amaçlar için işleme ilkesi*” ile uyumlu olmadığı, Kişisel Verilerin Korunması Kanununun (Kanun) 8 inci maddesinde ilgili kişinin açık rızası olmaksızın kişisel verilerin üçüncü kişilere aktarılamayacağına hüküm altına alındığı, bu kapsamda ilgili kişinin kendisi ve ailesine ilişkin kişisel verilerinin üçüncü kişilerle paylaşılmasına yönelik açık veya zımni rızasının bulunmadığı,

- İlgili kişinin rızası alınmaksızın yapılan bu veri aktarımının veri sorumlusu tarafından Kanunun 5 inci maddesinde sayılan kişisel veri işleme şartlarından “*ilgili kişinin kendisi tarafından alenileştirilmiş olma*” koşuluna dayandırıldığı, ancak ilgili kişinin rızası olmaksızın paylaşılan kişisel verilerin ilgili kişi tarafından herhangi bir şekilde kamuoyuna açıklanmış yani ilgili kişi tarafından alenileştirilen ve böylelikle herkes tarafından bilinebilecek hale getirilmiş bir bilgi niteliğini haiz olmadığı, söz konusu yeni işe başladığı şirket yetkililerinin ilgili kişinin çocukları ve eşinin yurt dışında yaşayıp yaşamadıklarını ve özel ödeme koşullarına ilişkin veri sorumlusu eski şirketin iddialarını teyit etmeye yönelik sorular sormalarının da söz konusu kişisel verilerin aleni olmadığı ve herkesçe bilinmediğinin göstergesi olduğu, ayrıca alenileştirmenin gerçekleştirilebilmesi için alenileştirme iradesinin varlığının gerektiği ancak ilgili kişinin bu yönde bir iradesinin bulunmadığı,

- Öte yandan Kanunun 12 nci maddesi kapsamında, veri sorumlusunun Kanunun kendisine yüklediği sorumluluklara aykırı davranarak, kişisel verilere erişme yetkisi olanlar tarafından yetkilerin kötüye kullanılması ile işleme amacı dışında ilgili kişinin ve ailesinin kişisel verilerini üçüncü kişilerle paylaşması suretiyle Kanunu ihlal ettiği ve bu ihlallerin gerçekleşmesini önlemek için uygun güvenlik düzeyini temin etmeye yönelik gerekli herhangi bir teknik ve idari tedbir almadığı belirtilerek, konuya ilişkin gerekli yaptırımların uygulanması talep edilmiştir.

Başlatılan inceleme çerçevesinde söz konusu iddialara ilişkin veri sorumlusundan (eski işveren) savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişinin hem veri sorumlusuna hem de Kuruma yaptığı başvuru dikkate alındığında şirketlerinin olağan iş süreçlerine ilişkin veri işleme sürecine yönelik bir uyuşmazlık bulunmadığı, şikâyet konusunun eski çalışana (ilgili kişiye) ilişkin kişisel verilerin yeni işvereni ile paylaşılıp paylaşılmadığı ve paylaşılmış ise bu paylaşımın hukuki gerekçesi üzerinde toplandığı,

- Bu kapsamda, ilgili kişinin yeni işvereni ile gerçekleştirdiği toplantıda gündeme gelen; eşinin ve çocuklarının yurtdışında yaşadığı ve kendisinin de bu ülkeye taşınacağı, ilgili kişinin maaş ve özel

ödeme koşullarına riayet etmeksizin veri sorumlusu bünyesinden ayrıldığı şeklindeki bilgilerin neredeyse hiç birinin veri sorumlusu tarafından yeni işveren ile paylaşılmadığı,

- Pek çok sektörde olduğu gibi ilgili sektörde de yer alan insanların birbirlerini tanıdığı, sektörde yer alan şirketlere veya çalışanlara ilişkin gelişmelerin insanlar arasında konuşulabildiği, bu minvalde ilgili kişinin kendisi ile ilgili bilgileri sektörde yer alan diğer insanlara aktarmış olabileceği de göz önünde bulundurulduğunda; söz konusu toplantıda ilgili kişiye yöneltilen soruların, bu sorulara dayanak oluşturan verilerin ve bu verilerin kimden ne şekilde elde edildiğinin veri sorumlusunun bilgisi dâhilinde olmadığı, söz konusu verilerin şirketleri tarafından yeni işverene sağlandığı iddiasının tahmine dayalı ve şirketlerini zan altında bırakan bir iddia olduğu, ilgili kişi tarafından bu iddiaların gerçekliğini ortaya koyacak bilgi ve belgelerin tereddütsüz bir şekilde sunulması gerektiği,
- Bununla birlikte; ilgili kişinin yeni şirketinde çalışmaya başladığına ilişkin duyurunun yeni işveren şirketin kurumsal hesabından duyurulduğu, söz konusu duyuruda ilgili kişinin daha önce veri sorumlusu bünyesinde direktör seviyesinde çalıştığı bilgisine yer verildiğinin fark edildiği, bu verilerin ilgili kişinin kendi iradesiyle ve iradesine uygun olarak alenileştirilen ve bu vesileyle tüm tarafların bilgisinde olan bilgiler olduğu, ancak bu bilginin gerçeği yansıtmadığı, ilgili kişinin veri sorumlusu nezdinde hiçbir dönemde bu seviyede üst düzey bir pozisyonda çalışmadığı, bu nedenle ilgili kişinin gerçeğe aykırı beyanlarının sebep olduğu bu durumdan yeni işverenin e-posta yoluyla haberdar edildiği,
- Veri sorumlusu tarafından yeni işveren ile paylaşıldığı belirtilen bu bilgiler (ilgili kişinin şirketlerinde daha önce direktör seviyesinde çalışmadığı ve işten ayrılış sebebi) dışında ilgili kişiye ilişkin kişisel verilerin yeni işvereni ile paylaşılmasının söz konusu olmadığı,
- İlgili kişinin, veri sorumlusunun adını kullanarak etik olmayan, hukuka ve gerçeğe aykırı bir bilgi ile işvereni nezdinde kendisi lehine haksız bir menfaat sağlaması, veri sorumlusunun haklarını ve menfaatlerini ihlal etmesi nedeniyle; ilgili kişinin yeni işvereni ile yapılan bilgi paylaşımı ile yalnızca gerçeğe aykırı olarak beyan edildiği anlaşılan hususların açıklığa kavuşması, bu durumun düzeltilmesi ve hukuki etkilerinin ortadan kaldırılmasının amaçlandığı,
- İlgili kişinin yeni işvereni ile sınırlı bir veri paylaşımı olduğu ve bu bilgi paylaşımının yapılmasında;
 - Veri sorumlusunun adı kullanılarak etik olmayan, hukuka ve gerçeğe aykırı bilginin düzeltilmesi ve ihlalin kaldırılması bakımından şirketleri için,
 - Gerçeğe aykırı beyan ile menfaat temini nedeni ile mevzuattan kaynaklanan haklarının kullanılabilmesi bakımından yeni işveren için,

- Gerçeğe aykırı beyan ile menfaat elde edilemeyeceği ve bu durumun aykırılık olarak kabul edilmesi bakımından

- kamusal anlamda korunmaya değer daha üstün bir menfaat bulunduğu,
- Söz konusu üçüncü kişilere veri aktarımının hukuki dayanağını Kanunun 5 inci maddesinin (2) numaralı fıkrasında belirtilen kişisel veri işleme şartlarından “(e) bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması” ve “(f) ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için veri işleminin zorunlu olması”nın oluşturduğu,
- Veri sorumlusu tarafından alınan idari ve teknik tedbirlere yönelik açıklamalar kapsamında; bünyelerinde irtibat kişinin atandığı, veri envanterinin hazırlandığı, kişisel verilerin korunmasına yönelik farkındalığı arttırmak için veri sorumlusu içerisinde tüm çalışanlara eğitimler verildiği, konuyla ilgili çok sayıda politika ve dokümanın hayata geçirildiği, savunma ekinde de yer verilen idari ve teknik tedbirler listesinde yer alan pek çok tedbirin uygulandığı

ifadelerine yer verilmiştir.

Konuya ilişkin yapılan incelemede, Kişisel Verileri Koruma Kurulunun 11/02/2020 tarihli ve 2020/108 sayılı Kararı ile,

- İlgili kişi ve veri sorumlusu (eski işveren) arasında üçüncü kişilere veri aktarımından kaynaklanan şikâyetin temelini, ilgili kişinin eski işyerinde çalıştığı son iş pozisyonunu yeni işyerine yönetici pozisyonu olan “Etik Direktörü” olarak belirtmek suretiyle yanlış beyanda bulunması, ayrıca eski işyerine işten ayrılma sebebini yurtdışına taşınması olarak ifade etmesinin oluşturduğu,
- İlgili kişinin “çocuklarının ve eşinin uzun bir süredir yurtdışında yaşadıkları ve ilgili kişinin de bu ülkeye taşınacağı, Türkiye’de fazla kalmayacağı gibi bilgilerin paylaşıldığı, ayrıca, ilgili kişinin veri sorumlusundan aldığı maaş, prim ve özel ödeme koşullarına riayet etmeksizin veri sorumlusu bünyesinden ayrıldığı” iddialarını doğrulayacak herhangi bir bilgi, belge ve benzeri dokümanın ilgili kişi tarafından Kuruma sunulmadığı, yalnızca veri aktarımının telefon görüşmesi ve iki adet e-posta ile gerçekleştiği bilgisinin verildiği,
- Söz konusu e-posta yazışmalarının, şikâyet edilen veri sorumlusu tarafından savunma yazısı ekinde sunulmuş olduğu ve yazışmalardan, yalnızca ilgili kişinin eski işvereni şirkette hangi tarihler arasında hangi iş pozisyonlarında çalıştığı ve yeni işverenin ilgili kişinin işten ayrılma nedenine ilişkin soruya cevaben ailevi nedenlerden dolayı yurtdışına taşınacağı bilgisinin verildiğinin anlaşıldığı,

- İlgili kişinin eski işyerinde çalıştığı tarihler ve iş pozisyonları ile işten ayrılma sebebine ilişkin olarak, veri sorumlusu ile yeni işverenin İnsan Kaynakları Departmanları arasında e-posta yazışmaları yoluyla sınırlı bir veri aktarımının yapıldığının anlaşıldığı,
- İlgili kişinin veri sorumlusuna ayrılma nedenini “ailevi sebeplerden dolayı yurtdışına taşınma” ve yeni işverene de daha önce çalıştığı iş pozisyonunu “Etik Direktörü” olarak beyan etmiş olması dikkate alındığında; her iki işverenin de yanlış bilgilerle yanıltılmış olması nedeniyle, veri sorumlusunun bu bilgilerle ilgili düzeltme yapmasının kişinin makul beklentisine aykırı olmadığı ve temel hak ve hürriyetlerini de ihlal etmediği sonucuna varıldığı,
- Ayrıca veri sorumlusu tarafından ilgili kişinin şirketlerinde çalıştığı iş pozisyonuna ilişkin gerçeği yansıtmayan bilginin düzeltilmesi, şirket itibarının korunması, şirketlerinin adı kullanılarak yanlış bilgi üzerinden menfaat temin edilmesinin önlenmesi, gerçeğe aykırı beyandan ötürü şirket alacağının tahsil edilmesi yönünde hukuki sürecin başlatılması, ilgili kişinin daha önce çalıştığı işyerindeki iş pozisyonu için yeni işvereni yanıltması sonucunda yeni işverenin mevzuattan kaynaklanan haklarını kullanabilmesi ve iş yaşamında dürüstlük ve etik ilkelerin teşvik edilmesi amacıyla gerçekleştirilen söz konusu veri aktarımının hukuki gerekçesinin, Kanunun 5 inci maddesinin (2) numaralı fıkrasının (f) bendinde öngörülen “*ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.*” kişisel veri işleme şartına dayandığı kanaatine varıldığı,
- Diğer taraftan yeni işverenin, ilgili kişinin kendi şirketlerinde işe başlamasına ilişkin kurumsal web sitesinde yaptığı duyuruda, ilgili kişinin yeni görevi, eğitim durumu ve daha önce çalıştığı işyerleri ve iş pozisyonlarının belirtildiği, yapılan web araştırması sonucunda, yeni işveren tarafından alenileştirilen bu bilgilerin ilgili kişinin kendisi tarafından da profesyonel sosyal iletişim ağı hesabında herkesin erişimine açık bir şekilde alenileştirildiğinin belirlendiği, bu doğrultuda veri sorumlusu tarafından ilgili kişinin açık rızası alınmaksızın gerçekleştirilen veri aktarımının Kanunun 5 inci maddesinin (2) numaralı fıkrasının (d) bendinde öngörülen “*ilgili kişinin kendisi tarafından alenileştirilmiş olma*” kişisel veri işleme şartına uygun olduğunun değerlendirildiği,
- Veri aktarımı olarak gerçekleşen söz konusu veri işleme faaliyetinin; yanlış bilginin düzeltilmesi gibi haklı bir gerekçeye dayandığı, veri aktarımının amacının belirli, açık ve meşru olduğu ve belirtilen amaç ile sınırlı olduğu ve ilgili kişi tarafından iddia edildiği üzere “*hukuka ve dürüstlük kurallarına uygun olma*” ve “*belirli, açık ve meşru amaçlar için işleme ilkesi*” ne aykırılık teşkil etmediğinin değerlendirildiği,

• Ayrıca 4857 sayılı İş Kanununun 25/II-a maddesi gereğince “işçinin iş sözleşmesi yapıldığı sırada bu sözleşmenin esaslı noktalarından biri için gerekli vasıflar veya şartlar kendisinde bulunmadığı halde bunların kendisinde bulunduğunu ileri sürerek yahut gerçeğe uygun olmayan bilgiler veya sözler söyleyerek işvereni yanıltması”nın haklı nedenle derhal fesih sebebi olarak hüküm altına alındığı, yine aynı Kanunun 426 ncı maddesinde “*İşveren, işçinin isteği üzerine her zaman, işin türünü ve süresini içeren bir hizmet belgesi vermekle yükümlüdür. İşçinin açıkça istemde bulunması hâlinde, hizmet belgesinde onun iş görmedeki becerisi ile tutum ve davranışları da belirtilir. Hizmet belgesinin zamanında verilmemesinden veya belgede doğru olmayan bilgiler bulunmasından zarar gören işçi veya işçiyi işe alan yeni işveren, eski işverenden tazminat isteyebilir.*” hükümlerinin yer aldığı,

• Bu hükümler her ne kadar doğrudan yeni işvereni ve çalışanı ilgilendiriyor gibi görünse de, eski işveren için de talep olmasına gerek olmaksızın sorumluluk doğurduğu kanaatine varılmış olup veri sorumlusunun eski çalışanın kendi şirketinde çalıştığı iş pozisyonuyla ilgili yanlış bilgiyi düzelterek yeni işvereni bilgilendirme sorumluluğu hissetmesinin, makul ve olağan bir davranış olduğu sonucuna ulaşıldığı,

• Diğer taraftan iş etiği açısından bakıldığında, aynı sektörde faaliyet göstermelerinin doğal sonucu olarak, veri sorumlusunun eski çalışanı hakkındaki yanlış bilgidan haberdar olduğu halde doğru bilgiyi yeni işvereni ile paylaşmamasının ahlak, iyi niyet ve dürüstlük kurallarına da uygun olmayacağı değerlendirildiği,

• İlgili kişinin “*kişisel verilere erişme yetkisi olanlar tarafından yetkilerini kötüye kullanmak suretiyle ve işlenme amacı dışında ilgili kişinin ve ailesinin kişisel verilerini üçüncü kişilerle paylaşarak Kanunu ihlal ettiği ve bu ihlallerin gerçekleşmesini önlemek için uygun güvenlik düzeyini temin etmeye yönelik gerekli herhangi bir teknik ve idari tedbir almadığı*” yönündeki iddiası dikkate alındığında; e-posta yazışmaları yoluyla gerçekleşen veri aktarımının eski işveren ile yeni işverenin insan kaynakları müdürleri arasında yapılması ve insan kaynakları departmanının temel görevlerinden birisinin de kişilerin özlük dosyalarını tutmak olması nedeniyle veri sorumlusunun Kanunun 12 inci maddesi uyarınca veri güvenliğine ilişkin yükümlülüklerini ihlal etmediği

değerlendirmelerinden hareketle;

• Şikâyete konu kişisel veri işleme faaliyetinin hem kişisel verilerin korunması hem de iş mevzuatının ilgili maddelerine aykırılık teşkil etmediği, veri sorumlusu tarafından gerçeği yansıtmayan bilginin düzeltilmesi, şirket itibarının korunması, şirket adı kullanılarak yanlış bilgi üzerinden menfaat temin edilmesinin önlenmesi, ilerde oluşabilecek hukuki etkilerinin ortadan kaldırılması, iş yaşamında dürüstlük ve etik ilkelerin teşvik edilmesi amacıyla gerçekleştirildiği belirtilen söz konusu veri

aktarımının Kanunun “Kişisel verilerin işleme şartları” başlıklı 5 inci maddesinin (2) numaralı fıkrasının (f) bendi uyarınca “ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için veri işleminin zorunlu olması” kişisel veri işleme şartına dayandığı, bu kapsamda Kanunun “Kişisel verilerin aktarılması” başlıklı 8 inci maddesi kapsamında söz konusu veri aktarımının hukuka aykırı bir veri işleme olmadığı sonucuna varıldığından veri sorumlusu hakkında herhangi bir müeyyide uygulanmasına yer olmadığına,

- Bununla birlikte Kanunun “İlgili kişinin hakları” başlıklı 11 inci maddesi uyarınca, ilgili kişinin kişisel verilerinin rızası dışında üçüncü kişilere aktarımına ilişkin talebinin veri sorumlusu tarafından yeterli düzeyde karşılanmadığı, bu çerçevede ilgili kişinin talebi doğrultusunda “belirli tarihler arasında veri sorumlusu İnsan Kaynakları Departmanı çalışanları tarafından kanunlarda açıkça öngörülmesi ve Kanun kapsamında veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması durumları haricinde, ilgili kişiye ait kişisel verilerin ilgili kişinin açık rızası dışında herhangi bir iletişim aracı vasıtasıyla herhangi bir gerçek ve/veya tüzel kişiye aktarılıp aktarılmadığı; böyle bir aktarım yapıldıysa, yapılan bu aktarımın hangi amaçla yapıldığını, aktarımın içeriğini, aktaran ve aktarılan kişileri de gösterir orijinal metnin kopyasını içeren bilgi, belge vb. dokümanın” Kuruma sunulduğu üzere ilgili kişiye de sunulması ve akabinde söz konusu bilgi, belge vb. dokümanın ilgili kişiye sunulduğuna dair Kuruma bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2020/103 sayılı KVKK Kararı

Bir Bankanın Potansiyel Müşteri Kazanımı Amacıyla İlgili Kişinin Kişisel Verilerini Hukuka Aykırı Şekilde İşleyerek Hesap Açmasına İlişkin Olarak Kurula Yapılan Başvuru Hakkında Kişisel Verileri Koruma Kurulunun 06/02/2020 Tarihli ve 2020/103 Sayılı Karar Özeti

Karar Tarihi : 06.02.2020

Karar No : 2020/103

Konu Özeti : Bir Bankanın potansiyel müşteri kazanımı amacıyla ilgili kişinin kişisel verilerini hukuka aykırı şekilde işleyerek hesap açmasına ilişkin olarak Kurula yapılan başvuru hakkında

İlgili kişinin 2018 yılı sonunda bir Banka şubesinde mevduat hesabı açtırmak istediğinde aynı Bankanın başka bir ildeki şubesinde Ocak 2016'da açılan bir ticari hesabının olduğu, anne kızlık soyadı dahil tüm kimlik bilgilerinin bahsi geçen Banka şubesindeki hesapta görüldüğü bilgisini edinmesi karşısında, adına hesap açılan şubenin bulunduğu yere daha önce hiç gitmemiş olması ve yine hiç ticari faaliyet yürütmemesine rağmen Banka nezdinde kişisel verilerinin hukuka aykırı olarak işlenmesi suretiyle adına hesap açılması hakkında Kişisel Verileri Koruma Kuruluna ilettiği şikayet başvurusunun Bankadan alınan bilgi ve belgelerle birlikte incelenmesi neticesinde:

Veri sorumlusu Bankanın, potansiyel müşteri kazanımı amacıyla yapılan bir çalışmada üçüncü bir taraftan temin edilen liste vasıtasıyla ilgili kişinin bilgilerine ulaştığı ve müşteri numarasının oluşturulduğu ancak, Temel Bankacılık Hizmet Sözleşmesi imzalanmadan müşteri numarası aktif hale gelemeyeceğinden ilgili kişinin müşteri numarasının da aktif bir hesap haline gelmediği beyanı karşısında;

Müşteri numarasının oluşturulduğunun iddia edildiği Ocak 2016'da 07/04/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) yürürlükte olmamakla birlikte, Bankanın ilgili kişiye vermiş olduğu 2018 yılına ait cevap içeriğinden ilgili kişinin verilerinin halen veri sorumlusu nezdinde bulunduğu anlaşıldığından ilgili kişiye yönelik kişisel veri işleme faaliyetinin Kanununun 5 inci maddesinin (1) numaralı fıkrasında yer alan açık rıza şartı yerine getirilmeksizin ve (2) numaralı fıkrada sayılan hallerden biri mevcut olmaksızın gerçekleştirilmiş olması sebebiyle Bankanın Kanuna aykırı veri işleme faaliyetinde bulunduğu, öte yandan Kanununun Geçici 1 inci maddesinin (3) numaralı

fıkrasına aykırı şekilde ilgili kişiye ait kişisel verilerin derhal silinmediği, yok edilmediği veya anonim hale getirilmediği, bu nedenle veri sorumlusu Bankanın Kanununun 4 üncü maddesindeki genel ilkelere de aykırı bir şekilde ilgili kişinin kişisel verileri olan kimlik ve adres bilgilerini işlediği,

hususları dikkate alınarak; anılan Bankanın Kanununun 12 nci maddesinin (1) numaralı fıkrasının (a) bendindeki kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli idari ve teknik tedbirlerin alınması yükümlülüğüne aykırı hareket ettiği kanaatine varıldığından hakkında Kanununun 18 inci maddesinin (b) bendi kapsamında 210.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2020/93 sayılı KVKK Kararı

Geçmiş sağlık verilerinin düzeltilmesine/silinmesine yönelik şikâyetler hakkında Kişisel Verileri Koruma Kurulunun 06/02/2020 tarihli ve 2020/93 sayılı Karar Özeti

Karar Tarihi : 06.02.2020

Karar No : 2020/93

Konu Özeti : Geçmiş sağlık verilerinin düzeltilmesine/silinmesine yönelik şikâyetler

İlgili kişilerden alınan şikâyet dilekçelerinde özetle; geçmişte çeşitli sebeplerle kaydedilen sağlık raporlarının ve özellikle psikiyatrik hastalık tanılarının yaşamlarında sorun teşkil ettiği ve girmiş oldukları ve/veya girmeyi planladıkları çeşitli sınavların bu kayıtlardan dolayı olumsuz sonuçlandığı ve/veya sonuçlanacağı, ancak bu rapor/tanıların gerçeği yansıtmadığı ifadelerine yer verilerek söz konusu kişisel verilerin sağlık kayıtlarından düzeltilmesi ya da silinmesi talep edilmiştir.

Konuya ilişkin olarak başlatılan inceleme çerçevesinde veri sorumlusu Bakanlıktan alınan yazıda;

- Anayasanın 20 nci maddesinde kişisel verilerin korunmasını isteme hakkının kişisel verilerin silinmesini talep etme hakkını da kapsadığı ifade edilse de kişisel verilerin korunmasına ilişkin usul ve esaslarının kanunla düzenleneceğinin öngörüldüğü ve buna ilişkin usul ve esasların 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) ile belirlendiği,
- Kanunun 7 nci maddesi hükmünden de anlaşılacağı üzere Anayasanın 20 nci maddesinde yer alan kişisel verilerin silinmesini talep etme hakkının mutlak hak olmayıp bu hakkın ileri sürülmesinin belirli şartların varlığına bağlandığı, Kanun ve ikincil düzenlemelerle belirlenen bu şartların dayanağının yine Anayasanın 20 nci maddesinin son fıkrasında bulunan "*Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.*" hükmü olduğu,
- Buna ilaveten, 28.10.2017 tarihli ve 30224 sayılı Resmi Gazetede yayınlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 12 nci maddesinde

"1) İlgili kişi, Kanununun 13 üncü maddesine istinaden veri sorumlusuna başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Veri sorumlusu, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir. b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa veri sorumlusu bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde bu Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder. c) Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep veri sorumlusunca Kanununun 13 üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.” hükmünün bulunduğu, dolayısıyla kişisel veri işleme şartlarının tamamının ortadan kalkmadığı gerekçesiyle ilgili kişilerin kişisel verilerinin silinmesi taleplerinin veri sorumlusu tarafından reddedilebileceği, bu Yönetmelik ile de bunun hüküm altına alındığı,

- Anılan mevzuat hükümleri çerçevesinde kişilere kendi verilerini silme hakkının verilmediğinin değerlendirildiği, bu hususun Kanun ve ikincil düzenlemelerden de anlaşıldığı, veri silme taleplerinin ilgili kişi tarafından veri sorumlusuna iletilebileceği ve ancak belirli şartların varlığı halinde kişisel verilerin silinebileceğinin düzenlendiği,
- Bu kapsamda, kişilerin sağlık geçmişlerinde yer alan psikiyatrik tanuların silinmesi halinde kamu güvenliği ve kamu düzeni bakımından çok ciddi tehditlerin gündeme gelebileceği, kişilerin kendilerine konulan psikiyatrik tanular nedeniyle alamadıkları sürücü ehliyeti ve silah ruhsatı gibi belgeleri almaya hak kazanabilecekleri, gerçekte var olmasına ya da var olmadığı ispat edilmemiş olmasına rağmen silinen rahatsızlıkların etkileri ile istenmeyen olayların yaşanabileceğinin değerlendirildiği,
- Kanunun tam muafiyet hallerinin düzenlendiği 28 inci maddesinin birinci fıkrasında kamu güvenliği ve kamu düzenine yer verildiği ve önemlerine binaen bu şartlardan herhangi birisinin varlığı durumunda Kanunun uygulanmayacağına yer verildiği,
- Ayrıca Kanunun 6 ncı maddesinin üçüncü fıkrasında yer alan “...Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.” hükmü kapsamında, sağlığa ilişkin verilerin tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi amacıyla ilgili kişilerin açık rızaları olmaksızın Bakanlıklarınca işlenebileceği, bu durumda verilerin işleme sebeplerinin açık rıza değil, Kanunun 6 ncı maddesinin üçüncü fıkrasında yer alan amaçlar olduğu,

• Sonuç olarak, ilgili kişilerin sağlık geçmişlerinde yer alan psikiyatrik tanuların, Bakanlıklarınca resen veya ilgili kişinin başvurusu üzerine kamu güvenliği ile kamu düzeni bakımından büyük bir tehdit doğuracağı ve bu sebeple ilgili tanuların silinmesinin uygun olmayacağı değerlendirildiği,

• Diğer taraftan, Bakan Yardımcılığının 17.05.2019 tarihli Makam Oluru kapsamında sehven konulan tanuların silinmesi için tanı girişi yapan hekimin tanının hatalı kaydedildiğini bildiren yazısı, tanı girişinin yapıldığı sağlık tesisinin başhekim onaylı resmi yazısı veya hatalı kaydedildiği belirtilen tanının silinmesine ilişkin ilgili il sağlık müdürlüğünün ya da ilgili Genel Müdürlük yazısının Genel Müdürlüklerine iletilmesi gerektiği;

• Sehven kaydedildiği kanıtlanmamış tanular için ise ilgili il sağlık müdürlüğüne başvurulması ve bünyesinde kurulan bir komisyon ya da ilgili il sağlık müdürlüğü tarafından görevlendirilen hekim vasıtası ile hatalı kaydedildiği iddia edilen tanının araştırılması, araştırma sonucunda tanının hatalı kaydedildiği sonucuna ulaşılması halinde düzenlenecek raporda “ilgili tanının kişide bulunup bulunmadığının” net şekilde ifade edilmesi ya da bu hususta bir eğitim araştırma hastanesinden alınacak heyet raporu ile birlikte sağlık tesisinin bağlı bulunduğu il sağlık müdürlüğüne başvuru yapılması gerektiği; bu sürecin takip edilmesi sonucunda sehven konulan tanularla belirli bir muayene neticesinde konulmasına karşın kişi üzerindeki etkisi devam etmeyen tanuların silinmesinin mümkün bulunduğu

belirtilmiştir.

Bahse konu şikayet başvurularının incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 06/02/2020 tarih ve 2020/93 sayılı Kararı ile;

• 6698 sayılı Kanunun amacı kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek olup, Kanunun 3 üncü maddesinde kişisel verinin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi şeklinde tanımlandığı,

• Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinde, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, bu çerçevede, kişisel verilerin ancak,

a)Hukuka ve dürüstlük kurallarına uygun şekilde,

b)Belirli, açık ve meşru amaçlar kapsamında,

c)Doğru ve gerektiğinde güncel olma şartıyla,

ç)İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve

d)İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceği,

- Kanunun 6 ncı maddesinde ise özel nitelikli kişisel verilerin işlenme şartları düzenlenmiş olup, anılan maddenin;

“(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.” şeklinde hüküm altına alındığı,

- Kanunun 7 nci maddesinin (1) numaralı fıkrasında, bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silineceği, yok edileceği veya anonim hale getirileceğinin hükme bağlandığı,

- Kişisel Verilerin Silinmesi Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin kişisel verilerin silinmesine ilişkin 7 nci maddesinin (1) numaralı fıkrasında Kanunun 5 inci ve 6 ncı maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin veri sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi gerektiği; 8 inci maddesinin (1) numaralı fıkrasında kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi olarak tanımlanırken (2) numaralı fıkrasında veri sorumlusunun, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlü olduğunun düzenlendiği,

- Yönetmeliğin 12 nci maddesinin (1) numaralı fıkrasında ise ilgili kişinin, Kanunun 11 inci ve 13 üncü maddelerine istinaden veri sorumlusuna başvurarak kendisine ait kişisel verilerin silinmesini

veya yok edilmesini talep ettiğinde; kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusunun talebe konu kişisel verileri sileceği, yok edeceği veya anonim hale getireceği, ayrıca veri sorumlusunun, ilgili kişinin talebini en geç otuz gün içinde sonuçlandıracağı ve ilgili kişiye bilgi vereceğinin belirlendiği,

- Kanunun 11 inci maddesinde ise ilgili kişilerin hakları sıralanmış olup, maddede “Herkes, veri sorumlusuna başvurarak kendisiyle ilgili; a) Kişisel veri işlenip işlenmediğini öğrenme, b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme, c) Kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme haklarına sahiptir” hükmüne yer verildiği,

- 21.06.2019 tarihli ve 30808 sayılı Resmi Gazetede yayınlanan Kişisel Sağlık Verileri Hakkında Yönetmeliğin 4 üncü maddesinin birinci fıkrasının (k) bendinde kişisel verilerin imha edilmesinin; kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi şeklinde tanımlandığı,

- Anılan Yönetmeliğin “Kişisel Sağlık Verilerinin Düzeltilmesi” başlıklı 13 üncü maddesinin;

“(1) İlgili kişi, kendisi hakkında sehven oluşturulan sağlık verilerinin düzeltilmesi hususunda sağlık verisinin oluşturulduğu sağlık hizmeti sunucusunun bağlı bulunduğu il sağlık müdürlüğüne başvurur. İl sağlık müdürlüğü, ilgili sağlık hizmeti sunucusunda yapacağı araştırma neticesinde sağlık verisinin sehven oluşturulduğu bilgisine ulaşırsa resmi yazı ile Genel Müdürlüğe başvurur ve sehven oluşturulan sağlık verisinin düzeltilmesini ister.

(2) Genel Müdürlük tarafından tesis edilecek işlem, sağlık hizmeti sunucusunun kendi veri tabanında da gerçekleştirilir.

(3) Genel Müdürlük, sağlık hizmeti sunucuları tarafından oluşturulan sağlık verilerinin kendileri tarafından düzeltilebileceği tarihi belirler ve bu tarihi ihtiyaca göre günceller. Genel Müdürlükçe belirlenen bu tarihten sonra oluşturulan sağlık verileri ilgili sağlık hizmeti sunucusu tarafından; bu tarihten önce oluşturulan sağlık verileri ise ilgili il sağlık müdürlüğünün talebi üzerine Genel Müdürlükçe düzeltilir.”

ve kişisel sağlık verilerinin imha edilmesi başlıklı 14 üncü maddesinin “(1) Kişisel verilerin imha edilmesinde, Kanunun 7 nci maddesi ile Kurum tarafından hazırlanarak 28/10/2017 tarihli ve 30224 sayılı

Resmî Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik hükümlerine riayet edilir.” hükmünü amir olduğu

değerlendirmelerinden hareketle;

- İlgili kişilerin kişisel sağlık verilerinin düzeltilmesi talepleri hususunda, Kişisel Sağlık Verileri Hakkında Yönetmeliğin 13 üncü maddesi kapsamında ilgili il sağlık müdürlüklerine başvuruda bulunmaları ve il sağlık müdürlükleri tarafından başvurularına olumsuz cevap verilmesi sebebiyle Kurula yaptıkları şikâyetler kapsamında; kişisel sağlık verilerinin işleme şartlarının “kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi” şartının ortadan kalkmaması sebebiyle kaydedilen sağlık verilerinin bu amaca hizmet ettiği dikkate alındığında bahse konu şikâyetler ile ilgili olarak Kanun kapsamında yapılacak bir işlem olmadığına,
- İlgili kişilerin kişisel sağlık verilerinin silinmesine ilişkin talepleri hususunda kişisel sağlık verilerinin işleme şartlarından “kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi” şartının ortadan kalkmaması sebebiyle kaydedilen sağlık verilerinin bu amaca hizmet ettiği dikkate alındığında bu verilerin Bakanlık tarafından Kanunun 6 ncı maddesinin üçüncü fıkrası kapsamında işlendiği ve söz konusu işleme şartlarının ortadan kalkmaması nedeniyle Kanun kapsamında yapılacak bir işlem olmadığına

karar verilmiştir.

2020/86 sayılı KVKK Kararı

Bir uçak bileti satış firması olan veri sorumlusu hakkındaki şikayetle ilgili Kişisel Verileri Koruma Kurulunun 06.02.2020 Tarihli ve 2020/86 Sayılı Karar Özeti

Karar Tarihi : 06.02.2020

Karar No : 2020/86

Konu Özeti : Bir uçak bileti satış firması olan veri sorumlusu hakkındaki şikayet başvurusu.

İlgili kişinin “....com” internet adresi üzerinden hizmet veren bir uçak bileti satış firması olan veri sorumlusunun sistemlerinde@outlook.com şeklinde kayıtlı olan üyelik e-posta adresinin ...@gmail.com olarak güncellenmesini talep ettiği; ancak söz konusu talebinin, üyelik e-posta adresleri üzerinde değişiklik işlemi yapılamadığı ve kullanılmak istenilen e-posta adresiyle yeni bir üyelik başlatılabileceği gerekçe gösterilerek reddedilmesi nedeniyle Kurumumuza yaptığı Eylül 2018 tarihli başvuru ile ilgili yürütülen incelemede veri sorumlusu tarafından Kurumumuza iletilen savunma yazısında, ilgili kişinin başvurusunun, esasen sisteminde kayıtlı olmayan bir e-posta adresinden gönderildiği ve bu başvurunun tebliğde sayılan yöntemlerin herhangi biri ile gerçekleşmemiş olması sebebiyle reddedildiği açıklamasında bulunmuş olup, bu kapsamda ilgili kişinin başvurusunun veri sorumlusunun cevabı ile birlikte değerlendirilmesi neticesinde 01/03/2019 tarih ve 2019/48 sayılı Kişisel Verileri Koruma Kurulu Kararı ile

- Mevzuatla belirlenen usule uygun olmayan başvurusu nedeniyle kişinin kimliğinin tanımlanamadığı noktasından hareketle, ilgili kişinin talebini reddeden veri sorumlusunun bu eylemine ilişkin olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) hükümleri kapsamında yapılacak bir işlem bulunmadığına,
- Bununla birlikte, veri sorumlusu tarafından ilgili kişinin başvurusunun Kuruma yapılan açıklamada olduğu gibi sistemlerinde kayıtlı olmayan bir e-posta adresi üzerinden yapılması nedeniyle kişinin kimliğinin belirlenemediği gerekçesiyle değil üyelik e-posta adresleri üzerinde değişiklik işlemi yapılamadığı gerekçesiyle reddedilmesi karşısında veri sorumlusunun, Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ kapsamında ilgili kişi tarafından yapılan bir başvuruyu dürüstlük kuralına uygun olarak sonuçlandırmadığı dikkate alınarak, bundan böyle

Tebliğ kapsamında ilgili kişiler tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri alması hususunda Şirketin talimatlandırılmasına

karar verilmiş olup, bu karar ilgili kişiye ve veri sorumlusuna tebliğ edilmiştir.

Müteakiben, ilgili kişinin aynı veri sorumlusu hakkındaki ikinci şikayet başvurusunda özetle,

- İlgili kişinin 12.04.2019 tarihinde KEP hesabını kullanarak veri sorumlusunun KEP adresi olan "...@...kep.tr" adresine e-posta göndererek sistemlerinde kayıtlı "...@outlook.com" adresinin "...@gmail.com" olarak güncellenmesini talep ettiği,
- Kayıtlı elektronik posta aracılığıyla gönderilen e-postanın aynı gün içerisinde veri sorumlusu tarafından okunduğu ancak 30 gün içerisinde ilgili kişiye veri sorumlusu tarafından cevap verilmediği

belirtilerek, 6698 sayılı Kanun kapsamında gereğinin yapılması talep edilmiştir.

Veri sorumlusu savunmasında özetle;

- "...@gmail.com" adlı e-posta adresinden müvekkili firmaya bir e-posta gönderilerek bu e-postada sisteme kayıtlı bir kullanıcı olan ilgili kişinin bir takım kişisel verisini yazarak sistemdeki e-posta adresinin güncellenmesini talep ettiği,
- İlgili kişinin, veri sorumlusuna ilk başvurusunun, veri sorumlusunun sisteminde kayıtlı olmayan bir e-posta adresinden gönderilen ve kayıtlı bir kullanıcının hesap yönetimini talep eden bir e-posta olduğundan şikayete konu başvurunun tebliğde sayılan yöntemlerin herhangi biri ile gerçekleşmemiş olduğunu, bu sebeple söz konusu e-posta adresi değişikliği talebinin işleme alınmadığı,
- Daha sonra ilgili kişinin KEP adresi yoluyla 12.04.2019 tarihinde veri sorumlusuna tekrar başvuruda bulunduğu ancak yoğunluk sebebi ile başvurunun bir süre sonra gözden kaçtığı, ilgili kişinin talebi fark edildiğinde yerine getirilerek e-posta adresinin talebi doğrultusunda güncellendiği ve bu güncellemenin ilgili kişiye de bildirildiği, ilgili kişinin "...@gmail.com" e-posta adresiyle sisteme giriş yapabilmekte olduğu

belirtilmiştir.

Konunun incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 06.02.2020 tarih ve 2020/86 sayılı Kararı ile;

- Kanunun 13 üncü maddesi ile Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğin 6 ncı maddesinde veri sorumlusunun ilgili kişi başvurularını etkin bir şekilde sonuçlandırma yükümlülüğünün düzenlediği, veri sorumlusu tarafından ilgili kişinin başvurularına cevap verilmemesi ya da cevabın yetersiz bulunması halinde ilgili kişiye Kurula şikayet hakkı tanınmışsa da sadece başvuruya cevap verilmemesi sebebiyle veri sorumlusuna uygulanabilecek bir idari yaptırım türüne Kanunda yer verilmediği,

- Ancak, somut olaydaki başvurunun, ilgili kişinin veri sorumlusuna yaptığı ikinci başvuru olduğu, ilk başvuru sonrasındaki şikayet doğrultusunda Kurul tarafından alınan 01/03/2019 tarihli ve 2019/48 sayılı Kararda veri sorumlusunun, Tebliğ kapsamında ilgili kişiler tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri alması hususunda talimatlandırılmasına karar verildiği,

- Şikayet dilekçesi ekinde sunulan KEP delilinden veri sorumlusunun ilgili kişinin başvurusunu, kendisine iletilmesinden yedi dakika sonra okuduğunun anlaşıldığı, Kurulun talimatına rağmen ilgili kişinin KEP adresinden yaptığı ikinci başvurusunun cevaplandırılmadığı, başvurunun cevaplandırılmamasının ise veri sorumlusunun savunmasında, yoğunluk sebebiyle gözden kaçtığı şeklinde gerekçelendirildiği, buna göre, veri sorumlusu tarafından başvuruların etkin, hukuka ve dürüstlük kuralına uygun cevaplandırılması için gerekli idari tedbirlerin alınmadığı ve Kurul tarafından verilen talimata uygun davranılmadığı

değerlendirilmiş olup, Kanunun 15 inci maddesinin (5) numaralı fıkrası hükümlerine aykırı hareket eden veri sorumlusu hakkında Kanunun 18 inci maddesinin 1 inci fıkrasının (c) bendi uyarınca 50.000 TL idari para cezası uygulanmasına karar verilmiştir.

2020/78 sayılı KVKK Kararı

Veri sorumlusu bankanın ilgili kişiye ait kredi kartı ekstresinde yer alan kişisel verileri yanlış e-posta hesabına göndermesi hakkında Kişisel Verileri Koruma Kurulunun 30/01/2020 tarihli ve 2020/78 sayılı Karar Özeti

Karar Tarihi : 30.01.2020

Karar No : 2020/78

Konu Özeti : Veri sorumlusu bankanın ilgili kişiye ait kredi kartı ekstresinde yer alan kişisel verileri yanlış e-posta hesabına göndermesi

İlgili kişinin Kuruma intikal eden şikayetinde özetle; müşterisi olduğu bankanın, kendisine ait kredi kartının ekstresini kendisine ait olmayan bir e-posta adresine göndererek şahsına ait bilgileri üçüncü kişilerle paylaştığı, veri sorumlusuna konuya ilişkin hem e-posta hem de dilekçe ile başvuruda bulunduğu, başvuru tarihinin üzerinden bir ay geçmiş olmasına rağmen kendisine yazılı bir dönüş yapılmadığı belirtilerek veri sorumlusu hakkında 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) çerçevesinde gerekli işlemlerin yapılması talep edilmiştir.

Söz konusu şikâyeti takip eden süreçte ilgili kişinin Kuruma intikal eden ek dilekçesinde ise özetle; veri sorumlusu bankanın kendisine ait aynı kredi kartının ekstresini, kendisine ait olmayan bir e-posta adresine tekrar göndererek şahsına ait bilgileri tekrar üçüncü kişilerle paylaştığı, kendisinin Kuruma göndermiş olduğu dilekçe aracılığıyla veri sorumlusundan şikâyetçi olduğu belirtilerek veri sorumlusu hakkında Kanun çerçevesinde gerekli işlemlerin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişinin talebine istinaden tarafına kredi kartı tahsis edildiği, müşterinin ayrıca “.... Adi Ortaklığı” firma unvanı ile firma ortağı olarak veri sorumlusunun ticari müşterisi olduğu, şikâyet yazısında üçüncü bir kişinin e-postası olarak ifade edilen y...@gmail.com e-posta adresinin, aynı zamanda veri sorumlusunun kayıtlarında müşterinin ortağı olduğu firmanın iletişim adresi olduğu, firmanın talimatı doğrultusunda firmaya ve ortaklarına tahsis edilen ticari kredi kartlarının ekstrelerinin söz konusu e-posta adresine gönderilmekte olduğu,

- Mevcut durumda ilgili kişinin kredi kartı ekstrelerinin veri sorumlusu nezdinde kayıtlı h...@gmail.com e-posta adresine gönderilmekte olduğu, ilgili kişinin şikâyetinde belirttiği kredi kartı ekstresinin, y...@gmail.com e-posta adresine gönderilmesine ilişkin yapılan inceleme sonucunda; ilgili şube personelleri tarafından, başvuru sahibinin ortağı olduğu firma ve kendi adına düzenlenen ticari kredi kartlar için e-ekstre gönderimine yönelik tanımlamalar yapılırken, sehven müşterinin bireysel ürünü olan kredi kartı ekstresi için de e-ekstre talimatının güncellendiğinin belirlendiği, bu nedenle e-ekstre ortağı olduğu firma üzerinde tanımlı olan y...@gmail.com e-posta adresine gönderildiği, başvuru sahibinin şube aracılığıyla ulaşan talebi doğrultusunda e-posta adresinin güncelleme işleminin yapıldığı ve kendisinin sonraki dönemlere ait kredi kartı ekstrelerinin h...@gmail.com e-posta adresine yönlendirildiği,

- İlgili kişinin şikâyet başvurularının veri sorumlusu tarafından işleme alındığı ve ilgili birime yönlendirildiği, e-posta adres değişikliğinin ne şekilde yapıldığının belirlenmesinden sonra, ilgili kişinin şube personelleri tarafından telefonla aranarak konu hakkında bilgilendirildiği, ancak e-posta güncelleme işleminin sehven atlandığının anlaşıldığı, şube tarafından e-ekstre gönderiminin h...@gmail.com e-posta adresine yapılması yönünde oluşturulan talep doğrultusunda gerekli güncellenmenin yapıldığı ve başvuru sahibinin e-posta adresine ekstrenin gönderileceğine ilişkin bilgilendirmenin yapıldığının belirlendiği,

ifade edilmiştir.

Konuya ilişkin olarak yapılan incelemede, Kişisel Verileri Koruma Kurulunun 30/01/2020 tarihli ve 2020/78 sayılı Kararı ile;

- Kanunun 3 üncü maddesinin birinci fıkrasının (d) bendi uyarınca kişisel verinin; kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi, (e) bendi uyarınca kişisel verilerin işlenmesinin; kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem, (ç) bendi uyarınca ilgili kişinin; kişisel verisi işlenen gerçek kişi, (1) bendi uyarınca veri sorumlusunun; kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi olarak tanımlandığı,

- Kanunun “Genel ilkeler” başlıklı 4 üncü maddesinde ise, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği ve buna göre kişisel verilerin

işlenmesinde “a) Hukuka ve dürüstlük kurallarına uygun olma. b) Doğru ve gerektiğinde güncel olma. c) Belirli, açık ve meşru amaçlar için işlenme. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.” şeklinde sayılan ilkelere uyulmasının zorunlu olduğunun düzenleme altına alındığı, anılan madde hükmünden açıkça anlaşılacağı üzere, kişisel verilerin işlenmesinde her hal ve şartta Kanunun 4 üncü maddesinde sayılan genel ilkelere uyulmasının hukuki bir gereklilik olduğu,

- Kişisel verilerin işlenme şartlarının düzenlendiği Kanunun 5 inci maddesinin (1) numaralı fıkrasında; kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin, (2) numaralı fıkrasında ise belirtilen şartlardan kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması hallerinden birinin varlığı durumunda, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğunun hükme bağlandığı,

- İlgili kişilerin açık rızasının alınacağı hallerde, rızanın belirli bir konuya ilişkin olması, bilgilendirmeye dayanması ve özgür iradeyle açıklanması gerektiği, veri işlemek üzere verilen açık rızanın geçerli olması için, açık rızanın öncelikle belirli bir konuya ilişkin ve o konu ile sınırlı olarak verilmesinin zorunluluk arz ettiği, bu doğrultuda veri sorumlusu tarafından açık rıza beyanının hangi konuya ilişkin olarak istenildiğinin açıkça ortaya konulması bununla birlikte, açık rıza bir irade beyanı olduğundan, kişinin özgür bir şekilde rıza gösterebilmesi için, neye rıza gösterdiğini de bilmesi gerektiği, kişinin sadece konu üzerinde değil, aynı zamanda rızasının sonuçları üzerinde de tam bir bilgi sahibi olmasının önem arz ettiği, bu sebeple, bilgilendirmenin, veri işleme ile ilgili bütün konularda açık ve anlaşılır bir biçimde gerçekleştirilmesi ve mutlaka verinin işlenmesinden de önce yapılması gerektiği, diğer yandan, açık rızanın geçerlilik kazanabilmesi için kişinin yaptığı davranışın bilincinde ve kendi kararı olmasının şart olduğu, açık rızanın özgür iradeyle açıklanması gerektiğinden, herhangi bir ürün ve/veya hizmetin sunumunun (ya da herhangi bir üründen ve/veya hizmetten yararlandırılması) ilgili kişi tarafından açık rıza verilmesi şartına bağlanamayacağı,

tarafların eşit konumda olmadığı veya taraflardan birinin diğeri üzerinde etkili olduğu durumlarda rızanın özgür iradeyle verilip verilmediğinin dikkatle değerlendirilmesi gerektiği,

- Kanunun “kişisel verilerin işlenmesi” başlıklı 5 inci maddesi ve “kişisel verilerin aktarılması” başlıklı 8 inci maddesi hükümleri çerçevesinde; tarafların Kuruma ilettiği yazılarında yer alan beyanları incelendiğinde; veri sorumlusunun, ilgili kişinin kendisine ait olan kredi kartı ekstresini kendisine ait olmayan bir mail adresine (y...@gmail.com) göndermek suretiyle ilgili kişiye ait kişisel verilerin veri sorumlusu tarafından üçüncü kişilerle paylaşıldığı iddiasına aksi yönde bir beyanının olmadığı, şube personellerinin sehven başvuru sahibinin bireysel ürünü olan kredi kartı ekstresinin, başvuru sahibinin e-ekstre ortağı olduğu firma üzerinde tanımlı olan y...@gmail.com e-posta adresine gönderilmesi yönünde talimatlandırma yaptığının ifade edildiğinin görüldüğü, şikâyete konu olayda veri sorumlusunun ilgili kişinin kredi kartı ekstresinde yer alan kişisel verilerini, kendisine ait olmayan bir e-posta adresine göndermek suretiyle Kanunun 5 inci maddesinde düzenlenen kişisel veri işleme şartlarından biri bulunmaksızın üçüncü kişilerle paylaştığı ve bu yönüyle Kanunun 8 inci madde hükmüne aykırı bir kişisel veri aktarımı gerçekleştirdiği sonucuna varıldığı,

- Ayrıca ilgili kişinin, veri sorumlusunun Genel Müdürlüğüne konuya ilişkin hem e-posta hem de dilekçe aracılığıyla başvuruda bulunduğunu, ancak belirtilen tarihin üzerinden bir ay geçmiş olmasına rağmen kendisine yazılı bir dönüş yapılmadığını iddia ettiği, veri sorumlusunun, başvuru sahibinin, şube personelleri tarafından telefonla aranarak konu hakkında bilgilendirildiğini ifade ettiği görülmekle beraber bu noktada Kanunun “Veri sorumlusuna başvuru” başlıklı 13 üncü maddesinin üçüncü fıkrasında yer alan; *“Veri sorumlusu talebi kabul eder veya gerekçesini açıklayarak reddeder ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. Başvuruda yer alan talebin kabul edilmesi hâlinde veri sorumlusunca gereği yerine getirilir. Başvurunun veri sorumlusunun hatasından kaynaklanması hâlinde alınan ücret ilgiliye iade edilir.”* hükmünden hareketle, ilgili kişinin, veri sorumlusu Banka tarafından telefonla aranmak suretiyle bilgilendirilmesinin Kanunun ilgili hükmü kapsamında usulüne uygun bir bildirim niteliğini haiz olmadığı

değerlendirmelerinden hareketle;

- Veri sorumlusunun, ilgili kişinin şikâyet talebine yönelik cevabını, başvuru sahibini telefonla aramak suretiyle bildirmesinin Kanunun “Veri sorumlusuna başvuru” başlıklı 13 üncü maddesinin üçüncü fıkrası kapsamında usulüne uygun bir bildirim niteliğini haiz olmadığına, bu kapsamda Kanunun 15 inci maddesinin beşinci fıkrasında yer alan; *“Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması hâlinde Kurul, tespit ettiği hukuka aykırılıkların veri*

sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ eder. Bu karar, tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilir.” hükmü uyarınca da ilgili kişilerin başvurularının değerlendirilmesi ve yanıtlanmasında Kanun 13 üncü maddesi ve ilgili Veri Sorumlusuna Başvuru Usul ve Esasları Hakkındaki Tebliğ hükümlerine azami dikkat ve özeni göstermesi hususunda veri sorumlusunun talimatlandırılmasına,

- Veri sorumlusu Bankanın ilgili kişinin bireysel ürünü olan kredi kartı ekstresindeki kişisel verilerini, Kanunda sayılan işleme şartları olmaksızın bireysel mail adresi yerine e-ekstre ortağı olduğu firma üzerinde tanımlı olan e-posta adresine göndermek suretiyle Kanunun 8 inci maddesine aykırı bir kişisel veri aktarımı gerçekleştirmiş olduğu ve bu yönüyle veri sorumlusu Bankanın Kanunun 12 nci maddesinin birinci fıkrası kapsamında kişisel verilerin hukuka aykırı işlenmesini önlemek ve muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı kanaatine ulaşıldığından Kanunun 18 inci maddesinin birinci fıkrasının (b) bendi hükmü uyarınca hakkında 60.000 TL idari para cezası uygulanmasına karar verilmiştir.

2020/67 sayılı KVKK Kararı

İlgili kişiye rızası bulunmamasına rağmen bir gayrimenkul şirketi tarafından SMS aracılığıyla gönderilen reklam ve bildirimler hakkında Kişisel Verileri Koruma Kurulunun 27/01/2020 tarih ve 2020/67 sayılı Karar Özeti

Karar Tarihi : 27.01.2020

Karar No : 2020/67

Konu Özeti : İlgili kişiye rızası bulunmamasına rağmen bir gayrimenkul şirketi tarafından SMS aracılığıyla gönderilen reklam ve bildirimler hakkında

Kurumumuz intikal eden bir başvuruda ilgili kişi tarafından kendisine bir gayrimenkul şirketi tarafından SMS aracılığıyla gönderilen reklam ve bildirimlere ait açık rızasının bulunmadığı ve bu kapsamda gereğinin yapılması talebini içeren başvurusu ile ilgili Kurumumuzca istenilen savunmasına istinaden veri sorumlusundan alınan yazıda;

- Kayıtlarında tutulan kişisel verilerin ad, soyadı ve cep telefonu numarasından ibaret olduğu,
- Kayıtlarında tutulan kişisel verilerin ilgili kişiyle reklam, kampanya ve tanıtım amaçlı olarak irtibata geçilmesi amacıyla işlendiği,
- Kişisel verilerin internet üzerinden herkese açık bilgi kaynaklarından temin edildiği
- Ancak şu an söz konusu bilgi kaynaklarına ulaşamadığı, bu linklerin şu an aktif olmadığını ve kaldırıldığını tahmin ettikleri, ilgili kişinin yapmış olduğu başvuru neticesinde, kişisel verilerin sistemden derhal silindiğini ve kendisiyle bir daha iletişime geçilmediği

ifade edilmiştir.

Yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 27/01/2020 tarih ve 2020/67 sayılı Kararı ile;

- Kişisel verilerin işleme şartlarının düzenlendiği Kanunun 5 inci maddesinin birinci fıkrasında; kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, ikinci fıkrasında belirtilen şartlardan (-Kanunlarda açıkça öngörülmesi, -Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının

hayatı veya beden bütünlüğünün korunması için zorunlu olması, -Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, -Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, -İlgili kişinin kendisi tarafından alenileştirilmiş olması, -Bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması, -İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması) birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğunun hükme bağlandığı,

- Somut olayda Kurumun bilgi, belge talebine ilişkin olarak veri sorumlusu tarafından verilmiş olan cevap yazısında, ilgili kişiye ait kişisel verilerin herkese açık bilgi kaynaklarından elde edildiği ve ilgili kişinin açık rızasının bulunmadığının anlaşıldığı,

- Kanunun 5 inci maddesinin 2 nci fıkrasının (d) bendinde yer alan alenileştirme ilkesi gereğince, ilgili kişinin kendisi tarafından alenileştirilen, bir başka ifadeyle herhangi bir şekilde kamuoyuna açıklanmış olan kişisel verileri işlenebileceği, bu duruma örnek olarak ise bir kişinin belirli hallerde kendisiyle iletişime geçilmesi amacıyla iletişim bilgilerini kamuya açık şekilde ilan etmesinin verilebileceği,

- Alenileştirmenin gerçekleştirilebilmesi için alenileştirme iradesinin ne olduğuna bakılması gerektiği, zira bir kişinin kişisel verisinin herkesin görebileceği bir yerde olmasının aleni olmasını sağlamayacağı, alenileştirme durumunda kişisel verinin alenileştirme amacı kapsamında kullanılması gerektiği, somut olayda, alenileştirme bulunuyor olsa dahi ilgili kişinin reklam faaliyetleriyle ilgili kendisiyle iletişim kurulması amacıyla söz konusu kişisel verileri alenileştirmemiş ise, gerçekleştirilecek olan kişisel veri işleme faaliyetinin hukuka uygun olmayacağının değerlendirildiği,

- Somut olayda işlenen kişisel verilere yönelik olarak ilgili kişinin açık rızasının alınmadığı, açık rızanın aranmadığı diğer hallerin ise bulunmadığı, bu kapsamda ilgili kişinin kişisel verilerinin Kanunun 5 inci maddesinde yer alan şartlar yerine getirilmeden reklam içerikli iletiler gönderilmesi amacıyla kullanılmasının Kanunun 12 nci maddesinin 1 inci fıkrasının (a) bendine aykırılık teşkil ettiği

hususlarından hareketle veri sorumlusu hakkında Kanunun 18 inci maddesinin 1 inci fıkrasının (b) bendi uyarınca 50.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2020/66 sayılı KVKK Kararı

İlgili kişinin irtibat numarasının bir elektrik dağıtım şirketi tarafından herhangi bir işleme şartına dayanılmaksızın işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 27/01/2020 tarihli ve 2020/66 sayılı Karar Özeti

Karar Tarihi : 27.01.2020

Karar No : 2020/66

Konu Özeti : İlgili kişinin irtibat numarasının herhangi bir veri işleme şartına dayanılmaksızın işlenmesi

Kuruma intikal eden bir şikâyette özetle; ilgili kişinin irtibat numarasına, bir elektrik dağıtım firması tarafından kendisine ait olmayan birkaç elektrik abone numarasına ilişkin farklı konularda bilgilendirme amaçlı SMS'ler gönderildiği, söz konusu aboneliklere dair bilgilendirme mesajı almak istemediği, kendisine ait irtibat numarasının söz konusu sözleşmelerin iletişim bilgilerinden silinmesi ve başvurusunun sonucu hakkında yazılı olarak haberdar edilmesi konusunda veri sorumlusuna abone numarası sayısı kadar başvuruda bulunulduğu, ancak veri sorumlusu tarafından başvuru kapsamında herhangi bir işlem yapılmadığı ve kendisine cevap verilmediği, buna karşın irtibat numarasına hâlen bilgilendirme mesajı gönderildiği belirtilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gerekli işlemin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda; incelemeye konu talep değerlendirilmiş olup ilgili kişi adına kayıtlı olan irtibat numarasında güncelleme yapıldığı ifade edilmiş ancak bu durumu tevsik edici herhangi bir doküman gönderilmemiştir.

İlgili kişinin şikayeti, veri sorumlusunun savunması ve ilgili mevzuat hükümlerinin birlikte incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 27/01/2020 tarih ve 2020/66 sayılı Kararı ile;

- Kanununun 3 üncü maddesinin (1) numaralı fıkrasının (d) bendi uyarınca kişisel verinin; kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi, (e) bendi uyarınca kişisel verilerin işlenmesinin; kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt

sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi, (ç) bendi uyarınca ilgili kişinin; kişisel verisi işlenen gerçek kişiyi, (ı) bendi uyarınca veri sorumlusunun; kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişiyi ifade ettiği,

- Yukarıda aktarılan “kişisel veri” tanımına istinaden cep telefonu numarasının kimliği belirli bir gerçek kişiye ulaşılmasını sağladığından, şikâyette bulunanın ilgili kişi sıfatını ve şikâyet edilen elektrik dağıtım şirketinin veri sorumlusu sıfatını haiz olduğu,

- Kanunun “İlgili Kişinin Hakları” başlıklı 11 inci maddesinde, *“herkes, veri sorumlusuna başvurarak kendisiyle ilgili;*

a)Kişisel veri işlenip işlenmediğini öğrenme,

b)Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

c)Kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,

ç)Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

d)Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,

e)7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,

f)(d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

g)İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

ğ)Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme haklarına sahiptir.” hükmüne yer verildiği,

- İlgili kişinin veri sorumlusuna yaptığı başvuruda talebi, her ne kadar cep telefonu numarasının kendisine ait olmayan aboneliklere yönelik veri işleme faaliyetlerine ilişkin olarak silinmesi olarak belirtilse de, yukarıda aktarılan Kanunun 11 inci maddesi bağlamında bu talebin *“kişisel verilerin eksik ya da yanlış işlenmiş olması halinde düzeltilmesini isteme”* hakkıyla örtüştüğü, zira Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 8 inci maddesinin (1) numaralı fıkrasında kişisel verilerin silinmesinin, *“kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir”* şeklinde tanımlandığı bu bakımdan, ilgili kişinin veri sorumlusunun dağıtımını üstlendiği elektrik hizmetinden yararlanmaya devam eden bir

sözleşmesinin olup olmadığı bilinemediğinden ve veri sorumlusunun, kendisinden istenilen bilgi ve belge talebinde bu hususta bir açıklama yapmadığından talebin Kanun kapsamındaki silme işlemi değil “...düzeltmesini isteme” olarak değerlendirilmesi kanaatine varıldığı,

- Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğin 6 ncı maddesinin (1) numaralı fıkrasında “Veri sorumlusu bu Tebliğ kapsamında ilgili kişi tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlüdür.” (2) numaralı fıkrasında “Veri sorumlusu, başvuruyu kabul eder veya gerekçesini açıklayarak reddeder.” (5) numaralı fıkrasında “Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak, işlemin ayrıca bir maliyet gerektirmesi hâlinde, 7 nci maddede belirtilen ücret alınabilir. Başvurunun, veri sorumlusunun hatasından kaynaklanması hâlinde alınan ücret ilgiliye iade edilir.” düzenlemelerine yer verildiği,

- Veri sorumlusunun ilgili kişinin Tebliğ hükümlerine göre yaptığı başvuruya kendisine tanınan 30 günlük süre içerisinde cevap vermediğinden Tebliğin 6 ncı maddesinin (2) ve (5) numaralı fıkralarına aykırılık ortaya çıktığı, ilgili kişinin başvurusuna neden cevap verilmediğinin veri sorumlusuna gönderilen bilgi, belge yazısında sorulduğu, ancak veri sorumlusunun bu hususta herhangi bir cevap vermediği,

- Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinde ise kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, bu çerçevede, kişisel verilerin ancak; hukuka ve dürüstlük kurallarına uygun şekilde, belirli, açık ve meşru amaçlar kapsamında, doğru ve gerektiğinde güncel olma şartıyla, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceği,

- Kanunun kişisel verilerin işleme şartlarının belirlendiği 5 inci maddesinin (1) numaralı fıkrasında, kişisel verilerin ilgili kişinin açık rızası olmadan işlenemeyeceği hüküm altına alınmış olmakla birlikte, (2) numaralı fıkrasında, kişisel verilerin

a) Kanunlarda açıkça öngörülmesi,

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,

- ç)Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- d)İlgili kişinin kendisi tarafından alenileştirilmiş olması,
- e)Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- f)İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde ilgili kişinin açık rızası aranmaksızın işlenebileceğinin hükme bağlandığı,

• İlgili kişinin irtibat numarasının kendisine ait olmayan aboneliklerde kullanıldığına dair veri sorumlusu tarafından Kuruma herhangi bir açıklama yapılmadığı, ayrıca Kuruma intikal eden cevabi yazısında belirttiği hususa dair destekleyici bir doküman sunulmadığı, bu sebeple ilgili kişinin irtibat numarasının işlenmesine ilişkin Kanunun 5 inci maddesinde belirtilen kişisel veri işleme şartlarının bulunup bulunmadığının tespitine imkân tanınmadığı, ancak mezkûr cevabi yazıda ilgili kişi adına sistemde kayıtlı olan telefon numarasında güncelleme yapıldığı açıklamasından hareketle, veri sorumlusu tarafından ilgili kişinin irtibat numarasının kişisel veri işleme faaliyetine dâhil edildiği,

• Kanunda belirtilen veri işleme ilkelerinden “Doğru ve Gerektiğinde Güncel Olma İlkesi” uyarınca, veri sorumlusunun her zaman ilgili kişinin bilgilerinin doğru ve güncel olmasını temin edecek kanalları açık tutması gerektiği, bu ilkenin aslında kişisel verilerin düzeltilmesini isteme hakkıyla ilişkili olduğu, bu bakımdan, ilgili kişinin dilekçe ile yaptığı başvuruların işleme alınmasında zorluk çıkarılması ve kabul edildikten sonra süresi içinde ilgili kişiye talebine ilişkin olarak dönüş yapılmamasının bu ilkeye aykırı olarak hareket edildiğinin ve ilgili kişinin hakkını kullanamamasına yol açığının bir göstergesi olduğu

değerlendirmelerinden hareketle

• Kanunun 13 üncü maddesinin (2) numaralı fıkrasında “*Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak, işlemin ayrıca bir maliyet gerektirmesi halinde, Kurulca belirlenen tarifedeki ücret alınabilir*” hükmü ile Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğin 6 ncı maddesinin (1) numaralı fıkrasındaki “*Veri sorumlusu bu Tebliğ kapsamında ilgili kişi tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlüdür.*” hükmüne istinaden ilgili kişinin başvurusunu süresi içinde cevaplamayan veri sorumlusunun Kanun kapsamında yöneltilecek başvuruları zamanında, tam ve eksiksiz olarak cevaplaması hususunda talimatlandırılmasına,

• Mevcut bilgi ve belgeler bir bütün olarak değerlendirildiğinde; veri sorumlusu tarafından ilgili kişinin cep telefonu numarasının, Kanunun 4 üncü maddesinde belirtilen “*Belirli, açık ve meşru amaçlar*

için işlenme” ilkesi göz önünde bulundurulduğunda, Kanunun 5 inci maddesinde belirtilen kişisel veri işleme şartlarına dayanmadan işlendiği, bu hususun ise veri güvenliğine ilişkin yükümlülüklerin düzenlendiği Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendinde yer alan “*Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır*” hükmüne aykırılık teşkil ettiği değerlendirildiğinden, Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendine istinaden veri sorumlusu hakkında 100.000 TL idari para cezası uygulanmasına,

- İlgili kişinin talebinin yerine getirildiğine yönelik veri sorumlusunun, gerekli bilgi, belge ve kayıtları ilgili kişiye iletmesi ve yine söz konusu hususları yerine getirdiğine dair bilgi, belge ve kayıtları Kanunun 15 inci maddesinin (5) numaralı fıkrası uyarınca 30 gün içinde Kurula sunması hususunda talimatlandırılmasına

karar verilmiştir.

2020/65 sayılı KVKK Kararı

Ulaşım hizmeti sunan bir mobil uygulama kapsamında işlenen kişisel veriler hakkında Kişisel Verileri Koruma Kurulunun 27/01/2020 tarih ve 2020/65 sayılı Karar Özeti

Karar Tarihi : 27.01.2020

Karar No : 2020/65

Konu Özeti : Bir mobil uygulama kapsamında işlenen kişisel veriler hakkında Kuruma yapılan başvuru.

İlgili kişinin, ulaşım hizmeti sunan bir platform vasıtasıyla yaptığı yolculukların şoförler tarafından puanlandığını öğrenmesi, kendi yolculuklarına ait bu puanlara kendisi tarafından erişilememesi ve bu tip bir puanlama yapılacağı hususunda veri sorumlusunun aydınlatma metninde herhangi bir bilginin yer almaması neticesinde, veri sorumlusu statüsüne sahip ulaşım hizmeti sunan platforma 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 11 inci maddesinin 1 inci fıkrasının (b) bendinde yer alan “Kişisel veri işlenmişse buna ilişkin bilgi talep etme” hakkından hareketle, Kanunun 13 üncü maddesine istinaden yaptığı başvurunun cevapsız kaldığı iddialarına ilişkin Kuruma intikal eden dilekçeye istinaden veri sorumlusunun savunması istenilmiş, alınan cevabi yazıda;

- Veri sorumlusu tarafından kullanıcıya ait verilerin uygulamaya kayıt esnasında toplanarak üyelik sözleşmesinin kurulması ve ifasıyla doğrudan doğruya ilişkisi olması sebebiyle işlendiğini, <http://www.....com/gizlilik-politikasi> adresinde yer alan kişiselveriler@....com e-posta adresine ilgili kişiler tarafından taleplerin iletilebileceğini belirten veri sorumlusu tarafından bu taleplerin en kısa süre cevaplandığını,
- İlgili kişi tarafından kullanılan uygulamada ortalama puanın 5 üzerinden kaç olduğunun sorulduğuna ve “sehven süresi içinde talebe cevap verilmemiş olsa da” sonrasında yazılı olarak dönüş yapıldığı ifade edilmiştir.

Konunun incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 27/01/2010 tarih ve 2020/65 sayılı Kararı ile;

1- Kanunun 13 üncü maddesinin 2 inci fıkrasında “Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak, işlemin ayrıca bir maliyet gerektirmesi halinde, Kurulca belirlenen tarifedeki ücret alınabilir” hükmüne ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğin” 6 ıncı maddesinin (1) numaralı fıkrasındaki “Veri sorumlusu bu Tebliğ kapsamında ilgili kişi tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlüdür.” hükmüne yer verildiği,

- Veri sorumlusunun “Kullanım Koşulları” başlıklı dokümanında yer alan hükümlere istinaden ilgili kişinin talebini süresi içinde cevaplamayan veri sorumlusunun Kanun kapsamında yöneltilen başvuruları gerek bu Kanunun 15 inci maddesinin 5 inci fıkrasına istinaden gerekse kendisi tarafından duyurulan koşullara uygun olarak zamanında, tam ve eksiksiz olarak cevaplaması hususunda talimatlandırılmasına,

2- Bu noktada ikinci olarak, bahse taşıma/ulaşım hizmeti ile ilgili kişinin iddia ettiği ve veri sorumlusunun daha sonra Kurumun bilgi ve belge talebine yönelik yazısına cevaben gönderdiği yazı ve ekinde belirttiği üzere ilgili kişilerin puanlaması işleminin sözleşmenin kurulması veya ifasıyla doğrudan doğruya bir ilişkisinin olup olmadığının incelenmesi gerektiği,

- Müşterilerin/yolcuların yaptığı seyahatlerin şoförler tarafından puanlanmasına ve bu puanların ortalamasının alınmasına dayanan veri işleme faaliyetinin, Kanunun 5 inci maddesinin 2 inci fıkrasının (c) bendinde yer alan “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” şartı kapsamında sözleşmenin ifasına ilişkin ana kurucu öge olmadığı veya sözleşmenin ifasıyla doğrudan doğruya bir ilişkisinin var olmaması sebebiyle ve bu veri işleme faaliyetinin aynı maddede belirtilen diğer veri işleme şartlarından herhangi birine dayanmadığı dikkate alındığında veri sorumlusunun Kanunun 12 inci maddesinin 1 inci fıkrasının a bendinde yer alan “veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır” hükmüne aykırı hareket ettiği kanaatine varıldığından hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının b bendine istinaden 100.000 TL idari para cezası uygulanmasına,

3- İlgili kişinin veri sorumlusunun Aydınlatma Metninde müşteriler/yolcular hakkında bir puanlama yapıldığına dair her hangi bir bilginin bulunmadığına dair iddiasına ilişkin olarak, “Kişisel Verilerin Korunması Hakkında Bilgilendirme” başlıklı dokümanının incelendiği, “Kişisel Verilerin Korunması Hakkında Bilgilendirme” başlıklı bu dokümanda, “...’nin kişisel verilerinizi işleme amacı:

- *Kimliğinizi doğrulamak*
- *Müşteri desteği sağlamak ve sorun gidermek*
- *Servis güncellemeleri ve hatalar hakkında sizi bilgilendirmek*
- *Uygulama ve kampanyalar hakkında sizi bilgilendirmek*
- *Sürücünün yolculukla ilgili olarak size ulaşması gereken durumlarda sizi arayabilmesini sağlamaktır...”*

şeklinde açıklandığı,

- *Veri işleme amaçları arasında yolcuların puanlanıp sürücüler tarafından bunun görülebileceğine ilişkin bir açıklama bulunmadığı,*

• *“Kullanım Koşulları” dokümanında ise “Veri sorumlusu Sıfatıyla İşlenen Veriler” başlıklı maddesinde bu verilerin*

- *Tanımlama bilgileri (ad, soyad, cep telefonu numarası, e-posta adresi).*
- *Kullandığımız mobil aygıtın işletim sistemi versiyonu bilgisi.*
- *Kullandığımız mobil aygıttan edinilen konum bilgileri.*
- *Yolculuk sonunda sürücüye verilen oylama bilgisi ve yorumlar.*
- *Uygulama içindeki “Öneri ve Şikâyet” bölümünde iletilen yorumlar.”*

olarak sayıldığı,

- *Bu sebepten dolayı, ne aydınlatma metninde (Kişisel Verilerin Korunması Hakkında Bilgilendirme) ne de kullanıcı sözleşmesinde (Kullanım Koşulları) müşterilerin puanlanmasına ilişkin bir bilgilendirme bulunmadığı,*

• *Bu durumda, müşterilerin puanlanmasına dayanan veri işleme faaliyetinin Kanunun 4 maddesinde belirtilen kişisel verilerin işlenmesine ilişkin genel ilkelerden ilk olarak “Hukuka ve Dürüstlük Kurallarına Uygun Olma” ilkesine aykırılık teşkil ettiği, zira veri sorumlusunun sözü geçen kişisel veri işleme faaliyetine ilişkin olarak ilgili kişi ile hiçbir bilgi paylaşmadığı, konu “Belirli, Açık ve Meşru Amaçlar İçin İşlenme” ilkesi bakımından değerlendirildiğinde, veri sorumlusunun aydınlatma metninde ve kullanım koşullarına ilişkin metinde belirtilen amaçların müşterilerin puanlanmasına dayanan kişisel veri işleme faaliyetinin asıl amacının ne olduğunu açıklayamadığı,*

• *Bu kapsamda, söz konusu uygulamanın yüklenmesi akabinde üye olunması esnasında ilgili kişilere bir aydınlatma gerçekleştirilmediği ve ilgili kişinin yolculuklarının şoförler tarafından değerlendirilerek çıkarılacak bir puanlamaya dayalı veri işleme faaliyetine, internet sitesinde yer alan veri sorumlusunun aydınlatma metni yerine geçen “Kişisel Verilerin Korunması Hakkında*

Bilgilendirme" dokümanında ve Kullanım Koşulları başlıklı belgede yer verilmemesi sebebiyle, Kanunun 10 uncu maddesinde yer alan "Veri Sorumlusunun Aydınlatma Yükümlülüğü"nü yerine getirmemiş olduğu kanaatine varılmasından ötürü Kanunun 18 inci maddesinin (1) numaralı fıkrasının (a) bendi kapsamında veri sorumlusu hakkında 10.000 TL idari para cezası uygulanmasına,

4- Puanlamaya dayalı veri işleme faaliyetine devam edebilmesi için veri sorumlusunun Kanunun "Kişisel Verilerin İşlenmesi Şartları" başlıklı 5 inci maddesinde kapsamında uygun bir veri işleme şartı belirlemesi, buna istinaden aydınlatma metnini güncellemesi ve sayılan hususları tamamladığına ilişkin destekleyici belge ve kayıtları Kanunun 15 inci maddesinin 5 numaralı fıkrası hükümlerine istinaden 30 gün içinde Kurula sunması hususunda talimatlandırılmasına karar verilmiştir.

2020/63 sayılı KVKK Kararı

Veri sorumlusu hastanede uygulanan beyaz kod kapsamında ilgili kişinin işlenen kişisel verileri hakkında Kişisel Verileri Koruma Kurulunun 27/01/2020 tarihli ve 2020/63 sayılı Karar Özeti

Karar Tarihi : 27.01.2020

Karar No : 2020/63

Konu Özeti : Beyaz Kod uygulaması kapsamında işlenen kişisel veriler

İlgili kişi tarafından Kuruma yapılan şikâyette özetle, babasının tedavisi için gittikleri hastanede hastane görevlileri ile arasında yaşadığı tartışma sonucunda barkot alamadan hastaneden ayrılmak durumunda kaldığı, bahse konu hastane görevlilerinin yaşanan tartışma olayından 1 yıl 3 ay sonra tutanak tuttuğu, daha sonra bu tutanak aracılığıyla savcılığa suç duyurusunda bulunulduğu, bu sebeple adli para cezasına mahkûm edildiği ve vekâlet ücreti ödemek zorunda kaldığı, hastane görevlilerinin kamu gücünü kullanarak ilgili kişinin açık rızası olmaksızın adı, soyadı ve T.C. kimlik numarası bilgilerini hastane verilerinden alarak olay yeri tutanağına işlediği, bu durumun 6698 sayılı Kişisel Verilerin Korunması Kanununa (Kanun) aykırılık teşkil ettiği belirtilerek, konunun incelenmesi talep edilmiştir.

Şikâyet dilekçesi ekinde yer alan veri sorumlusunun konuya ilişkin yapmış olduğu başvuru çerçevesinde ilgili kişiye verdiği cevapta özetle,

- Hasta kayıt sürecinde yaşanan olay ile ilgili olarak tutanak tutulduğu, Sağlık Bakanlığının Hukuk Müşavirliğinin Hukuki Yardım ve Beyaz Kod Uygulamasına dair 2016/3 Genelgesine göre işlem başlatılarak, Cumhuriyet Savcılığına bildirim yapıldığı,

- Ayrıca Kanununun 6 ncı maddesi gereğince, kişisel verilerin sadece sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından paylaşıldığı

ifade edilmiştir.

Başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- Hastanede yaşanan tartışma sonucunda veri giriş elemanı tarafından Beyaz Kod verildiği, bu sebeple, Beyaz Kod tutanağının tutulduğu, söz konusu tutanak tutulurken ilgili kişinin kimlik bilgilerinin tutanağa işlendiği, kimlik bilgileri işlenmeden Beyaz Kod tutanağının tutulmasının mümkün olmadığı,

- Kanunun "Kişisel Verilerin İşlenme Şartları" başlıklı 5 inci maddesinin ikinci fıkrasında yer alan hüküm ile söz konusu kişisel verilerin işlenmesinin mümkün olduğu ifade edilmiştir.

Söz konusu iddiaların incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 27/01/2020 tarih ve 2020/63 sayılı Kararında;

- Kişisel verilerin işlenme şartlarının düzenlendiği Kanunun 5 inci maddesinin birinci fıkrasında; kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin, ikinci fıkrasında ise kişisel verilerin *kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde ilgili kişinin açık rızası aranmaksızın işlenmesinin mümkün olduğunun hükme bağlandığı,*

- Taraflar arası yaşanan tartışma sonucunda veri sorumlusu nezdinde Beyaz Kod uygulaması kapsamında hastane görevlileri tarafından ilgili kişiye ait kişisel verilerin işlendiği,

- Öte yandan, 2/11/2011 tarih ve 28103 mükerrer sayılı Resmi Gazetede yayımlanan Sağlık Alanında Bazı Düzenlemeler Hakkında Kanun Hükmünde Kararnamenin "Hukuki Yardım" başlıklı 54 üncü maddesinin birinci fıkrasında, "*Bakanlık ve bağlı kuruluşlarında; sağlık hizmeti sunumu sırasında veya bu görevlerden dolayı personele karşı işlenen suçlar sebebiyle ceza hukuku kapsamında yürütülmekte olan işlemler ve davalarda personelin talebi üzerine Bakanlık ve bağlı kuruluşlarınca hukukî yardım yapılır. Bakanlık ve bağlı kuruluşları merkez ve taşra teşkilatı ile döner sermaye teşkilatı kadrolarında bulunan hukuk birimi amirleri, hukuk müşavirleri ve avukatlar, ayrıca vekâletname ibraz etmeksizin ilgili personeli vekil sıfatı ile temsil eder. Bu yardımın usûl ve esasları Bakanlıkça belirlenir.*" hükmünün yer aldığı,

- Bununla birlikte, Sağlık Bakanlığı Hukuk Müşavirliğinin Hukuki Yardım ve Beyaz Kod Uygulamasına dair 2016/3 Genelgesi ile Beyaz Kod uygulamasına başlandığı, bu doğrultuda, sağlık personelinin hukuki yardımdan faydalanabilmesi adına "Beyaz Kod Kullanım Kılavuzu 2.0" kapsamında, şiddete maruz kalan çalışanın, adli süreçlerde kanıt teşkil etmesi açısından olaya tanık olan diğer personel ile birlikte, olayı anlatan ve belgeleyen bir tutanak düzenlemesi gerektiğinin ifade edildiği,

- Uygulamada yürütme organının Anayasada öngörölmüş düzenleyici işlemlere ek olarak, genel, soyut ve objektif hukuk kuralları öngörebildiği, bu tür düzenleyici işlemlere "adsız düzenleyici işlemler" denildiği, genelgelerin de bunlardan biri olduğu

değerlendirmelerinden hareketle,

- İlgili kişi ile hastane görevlileri arasında yaşanan tartışma neticesinde yaşanan olayla ilgili hastane görevlilerince tutanak tutulduğu, sonrasında hastane görevlilerince ilgili kişi hakkında Savcılığa suç duyurusunda bulunulduğu, bu kişilerce kamu gücü kullanılarak açık rızası olmaksızın ad, soyad ve T.C. kimlik numarası bilgilerinin hastane verilerinden alınarak olay yeri tutanağına 1 yıl 3 ay sonra işlendiği, bu şekilde temel hak ve özgürlüklerinin ihlal edildiği gerekçesiyle hastaneye başvurduğu; hastanenin vermiş olduğu cevapta ise, ilgili kişinin babasının tedavisinin eksiksiz planlanıp yapıldığı, olay ile ilgili tutanağın 1 yıl 3 ay sonra değil, olayla aynı gün tutulduğu, Sağlık Bakanlığı Hukuk Müşavirliği Hukuki Yardım ve Beyaz Kod Uygulamasına dair 2016/3 Genelgesine göre işlem başlatılarak Cumhuriyet Savcılığına bildirildiği; ayrıca Kanunun 6 ncı maddesi uyarınca kişisel verilerin, hastane kapsamında sır saklamakla yükümlü bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından paylaşıldığı yanıtları karşısında ilgili kişinin Kuruma yaptığı şikâyet başvurusunun, veri sorumlusundan alınan bilgi ve belgeler ve yukarıda belirtilen hukuki gerekçeler çerçevesinde incelenmesi sonucunda; söz konusu kişisel verilerin Kanunun 5 inci maddesinin (2) numaralı fıkrasının (ç) bendi uyarınca veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi kapsamında işlendiği kanaati olduğundan, söz konusu şikâyete ilişkin Kanun kapsamında yapılacak bir işlem olmadığına karar verilmiştir.

2020/59 sayılı KVKK Kararı

İlgili kişinin ortağı olduğu şirkette kullandığı e-posta adresine izinsiz ve hukuka aykırı olarak erişildiği iddiası hakkında Kişisel Verileri Koruma Kurulunun 27/01/2020 tarihli ve 2020/59 sayılı Karar Özeti

Karar Tarihi : 27.01.2020

Karar No : 2020/59

Konu Özeti : İlgili kişinin ortağı olduğu şirkette kullandığı e-posta adresine izinsiz ve hukuka aykırı olarak erişilmesi

Kuruma intikal eden bir şikâyette, ilgili kişinin ortağı bulunduğuLtd. Şti bünyesinde kullanmakta olduğu (ismininbaşharfivesoyadı)@şirketadı.com.tr şeklindeki ve kişisel verilerinin de bulunduğu kişisel e-posta hesabına izinsiz ve hukuka aykırı olarak erişildiği, erişim ayarlarının değiştirildiği, söz konusu e-posta hesabına ait tüm verilerin silinmesi ve kaldırılması konusunda bu e-posta hesabının bulunduğu IP adreslerinin sahibi veri sorumlusu ... Menkul Kıymetler AŞ'den noter kanalıyla talepte bulunulduğu; ancak, talebin reddedildiği belirtilerek, söz konusu hususlara ilişkin 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde e-posta hesabının bulunduğu IP adreslerinin sahibi veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- Şikâyet edilen veri sorumlusunun Genel Müdürünün aynı zamanda ilgili kişinin ortak olduğuLtd. Şti'nin diğer ortağı ve yetkili müdürü olduğu,
- Ticari işlerin takip edilmesi için ortağı olduğu şirketin müdürü sıfatıyla söz konusu e-posta adresinin ilgili kişiye tahsis edildiği, ortağı olduğu şirkete ait işlemlerin ilgili kişi tarafından takip edilmekte olmasına rağmen ilgili kişinin gerçekleştirdiği işlem ve kayıtlar hakkında hiçbir bilgi vermemesi, genel kurul davetine de icabet etmemesi üzerine şirket Genel Müdürünün, ilgili kişinin gerçekleştirdiği işlemleri ve yazışmalarını bulmak amacıyla şirket e-posta sunucusundan şirkete ait info@şirketadı.com.tr e-posta adresinin yazışmalarına bakıldığı, Asliye Ticaret Mahkemesinin dosyasına konu ve şirket gelirlerinin suiistimaline ilişkin e-posta yazışmalarına, ilgili kişinin hesabına

erişilmek suretiyle değil ilgili kişinin kendisinin talebiyle önceden dâhil edildiği e-posta hesabının sunucu yedeklerinden ulaşıldığı,

- E-posta ve eki kayıtları, yevmiye defteri ve fatura kayıtları ile şirketin gelirlerinin yatırıldığı banka kayıtlarının karşılaştırılması sonucunda, ilgili kişinin geçmiş yıllarda müdürlük görevini kötüye kullanarak şirket gelirlerinden bir kısmını muhtelif banka hesaplarına transfer ettiğinin tespiti üzerine Asliye Ticaret Mahkemesi nezdinde dava açıldığı,

- E-posta hesabının bulunduğu IP adreslerinin sahibi veri sorumlusu şirket genel müdürü hakkında, ilgili kişinin söz konusu e-posta hesabının izinsiz olarak ele geçirildiği ve söz konusu hesaptaki kişisel bilgilerinin tümünün alenileştirildiği ve başkaca kişilerle paylaşıldığı, böylece ilgili kişinin 6698 sayılı Kanun kapsamındaki haklarının açıkça ihlal edildiği yönünde Savcılığa yaptığı şikâyet başvurusuna ilişkin olarak, “şirket ortakları tarafından şirkete ilişkin iş ve işlemler için kullanıldığında şüphe bulunmayan maillerin kişisel içerik taşımayacağı, şirket serverlarından elde edilen bilgilerin hukuk ve ceza yargılamasına delil olarak sunulmasının suç teşkil etmeyeceği, müştekinin şirket iş ve işlemleri dışındaki kişisel verilerinin başkaca bir ortamda kullanıldığı, yayıldığı vb. bir iddiasının da bulunmadığı, yine şirket mail içeriklerinden özel hayatına ilişkin bilgi ve veri elde edildiğine dair bir iddiasının da bulunmadığı, iddia edilen suçların ise unsurları itibariyle oluşmadığı” gerekçesiyle kovuşturma yapılmasına yer olmadığına karar verildiği,

- Mülkiyeti, ortağı olduğu şirkete ait olan ve faturası şirket tarafından ödenen e-posta hesabının ilgili kişiye, şirkete ait işlemlerin takibi ile sözleşme ve ödeme işlemleri için tahsis edildiği ve kişisel bir e-posta hesabı olmadığı,

- İddia edildiği gibi, söz konusu şirket uzantılı e-posta adresine hukuka aykırı bir erişimin gerçekleşmediğinin gerek Asliye Ticaret Mahkemesinin gerekse Savcılığın kararları ile sabit olduğu ve “server yedek” kayıtlarından elde edilen e-postaların, ilgili kişinin müdürlükten azil, şirketi uğrattığı zararın tazmini ve ticari kayyım atanması talepli açılan davalarda delil olarak yalnızca Mahkemeye ve suç duyurusu esnasında da Savcılığa sunulduğu,

- İlgili kişinin, müdürlük yetkisinin tedbiren kaldırılması ve yerine yönetici kayyım atanması sonrasında söz konusu adresine erişildiği ve erişim ayarlarının değiştirildiği iddiasının gerçeğe aykırı olduğu ve Kurumu yanıltmaya yönelik olduğu; bu yöndeki iddianın Mahkeme ve Savcılık tarafından reddedildiği,

- İlgili kişinin söz konusu e-posta adresine ait tüm verilerin yedekleriyle kopyalarının silinmesi yönündeki talebinin, şirket mailini kullanarak şirket aleyhine işlemiş olduğu zarar doğurucu, şirket

gelirlerini zimmete geçirme ve suç teşkil eden fiillerine ilişkin delilleri Mahkemede ortadan kaldırma, bu delilleri karartma, hukuken geçersiz kılabilmek amacıyla dönük olduğundan reddedildiği ve bunun hukuka uygun olduğu,

- Şikayet edilen e-posta hesabının bulunduğu IP adreslerinin sahibi şirketin Kanun ve Türk Ceza Kanunu (TCK) uyarınca işlediği bir suç veya kabahatinin bulunmadığı, TCK'nın 26/1 maddesi gereğince, hakkını kullanan kimseye ceza verilemeyeceği; şikayet edilen şirket genel müdürünün, aynı zamanda ilgili kişinin ortak olduğu şirketin de ortağı ve yetkili müdürü olması sebebiyle, Türk Ticaret Kanununun 626 ncı maddesi hükmü uyarınca müdürlük görevini yerine getirebilmek ve şirket menfaatini korumak için şirkete ait sözleşme ve müşteri yazışmalarını denetlemek yükümlülüğünün bulunduğu, şirketin diğer müdürü olan ilgili kişinin hesap vermekten kaçınması üzerine, şirket uzantılı mail adresinin yedek kayıtlarının denetlenmesinin Kanuna ve hukuka uygun olduğu

belirtilmiştir.

İlgili kişinin şikayeti, veri sorumlusunun savunması ve ilgili mevzuat hükümlerinin birlikte incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 27/01/2020 tarih ve 2020/59 sayılı Kararı ile;

- Kanunun 4 üncü maddesinde kişisel verilerin işlenmesinde uyulacak genel ilkelerin, 5 inci ve 6 ncı maddelerinde de kişisel veriler ile özel nitelikli kişisel verilerin işlenme şartlarının belirlendiği, bu çerçevede, ad, soyad, adres, telefon numarası, Türkiye Cumhuriyeti kimlik numarası, doğum tarihi gibi kişisel verilerin herhangi bir veri sorumlusu tarafından işlenmesinin ancak açık rızanın bulunması ya da Kanunda belirtilen açık rıza dışı diğer hallerin varlığında mümkün bulunduğu,

- Kanunun "Kişisel verilerin işlenme şartları" başlıklı 5 inci maddesi hükmü uyarınca, kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemeyeceği; ancak kişisel verilerin

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması” şartlarından birinin varlığı halinde ilgili kişinin açık rızası aranmaksızın işlenebileceğinin hükme bağlandığı

değerlendirmelerinden hareketle;

- Kişinin ortağı olduğu şirkete ilişkin hakların korunması amacıyla söz konusu e-posta adresine ilişkin sunucu yedek kayıtlarından elde edilen kişisel verilerin Kanununun 5 inci maddesinin (2) numaralı fıkrasının (e) bendinde yer alan “... bir hakkın tesisi, kullanılması ve korunması kapsamında veri işlemenin zorunlu olması” kapsamında işlendiği ve kişisel veriler kullanılarak Asliye Ticaret Mahkemesi nezdinde açılan dava nedeniyle gerçekleştirilen kişisel veri işleme faaliyetinin ise Kanununun 28 inci maddesinin 1 numaralı fıkrasının (d) bendi hükmü kapsamında olduğu değerlendirildiğinden söz konusu şikayet ile ilgili Kanun kapsamında yapılacak bir işlem bulunmadığına karar verilmiştir.

2020/58 sayılı KVKK Kararı

Bir Sigorta Acentesinin müşterilerine ait kişisel verileri herkese açık sosyal medya platformlarında müşterilerinden habersiz olarak ve reklam amacıyla paylaşması hakkında Kişisel Verileri Koruma Kurulunun 27/01/2020 Tarihli ve 2020/58 Sayılı Karar Özeti

Karar Tarihi : 27.01.2020

Karar No : 2020/58

Konu Özeti : Bir Sigorta Acentesinin müşterilerine ait kişisel verileri herkese açık sosyal medya platformlarında müşterilerinden habersiz olarak ve reklam amacıyla paylaşması hakkında

Kurumumuza intikal eden bir ihbarda, bir Sigorta Acentesinin müşterilerine ait kişisel verileri herkese açık sosyal medya platformlarında müşterilerinden habersiz olarak reklam amacıyla paylaştığı, bu hususta poliçe sahiplerinin izninin olmadığı belirtilerek gerekli yasal işlemin yapılması talep edilmiş, ihbarı destekler nitelikte olan, ilgili sosyal medya paylaşımlarına ayrıca dilekçe ekinde yer verilmiştir.

Konuya ilişkin Veri Sorumlusu Sigorta Acentesinden ihbarda yer verilen iddialara ilişkin savunması istenilmiş, alınan cevabi yazıda

- Müşterilere ait kişisel verilerin herkese açık sosyal medya hesapları üzerinden paylaşıldığı ancak bu paylaşımlar yapılırken program özelliği ya da kağıt gibi vasıtalarla kişisel verilerin gizlenmeye çalışıldığı ancak kimi paylaşımlarda bu hususun dikkatsizlik ve acelecilik gibi nedenlerle gözden kaçırıldığı,
- Kurumumuzca yazısı alındıktan sonra gözden kaçan ilgili paylaşımların silindiği,
- Ayrıca poliçe kayıtlarının tutulduğu sistemde, kullanılan sistemin özelliği gereği, kimlik numaraları kapatıldığı için hiçbir zaman kimlik numaralarını içeren paylaşım yapılmadığı,
- Konuya ilişkin eksikliğin bilgisizlikten kaynaklandığı ve belirtilmesi halinde gerekli düzeltmeleri yapabilecekleri

belirtilmiştir.

Yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 27/01/2020 tarih ve 2020/58 sayılı Kararı ile,

- Veri sorumlusu Sigorta Acentesinin yaptığı sosyal medya paylaşımlarda müşterilerinin adları, adresleri ve maskelenmiş biçimde kimlik numaralarının yer aldığı, bunların dışında bazı hallerde kişisel veri niteliği arz edebilecek plaka numaraları ile birlikte aracın rengi, markası ve modeli, müşterinin ödemesi gereken prim, toplam prim gibi ayrıntılara da yer verildiği,
- Veri sorumlusu tarafından ilgili paylaşımların şahsi Facebook hesabından ve “.....sigorta” adıyla açtığı ve poliçe paylaşımlarıyla birlikte çeşitli özel gün kutlamaları ve şahsi fotoğraflarını da paylaştığı, hesabın açıklama kısmında kendi adına da yer verdiği Instagram hesabından yapıldığı,
- Kişisel verilerin işleme şartlarının düzenlendiği 6698 sayılı Kişisel Verilerin Korunması Kanununun 5 inci maddesinin birinci fıkrasında; kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, ikinci fıkrasında belirtilen şartlardan (-Kanunlarda açıkça öngörülmesi, -Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, -Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, -Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, -İlgili kişinin kendisi tarafından alenileştirilmiş olması, -Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, -İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması) birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğunun hükme bağlandığı,
- Öte yandan, Kanunun 12 nci maddesinin birinci fıkrasında; veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ile kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğunun ifade edildiği,
- Bu doğrultuda veri sorumlusunun müşterilerine ait kişisel verileri, onların açık rızası olmaksızın paylaştığının anlaşıldığı ve bu çerçevede Kanunun 12 nci maddesi ile veri sorumlusuna yüklenmiş olan yükümlülükleri yerine getirmediği kanaatine varıldığı

hususlarından hareketle müşterilerine ait kişisel verileri herkese açık sosyal medya platformlarında müşterilerinden habersiz olarak ve reklam amacıyla paylaşan veri sorumlusu hakkında Kanunun 18

inci maddesinin birinci fıkrasının (b) bendinde kapsamında 22.500 TL idari para cezasının uygulanmasına karar verilmiştir.

2020/50 sayılı KVKK Kararı

Bir perakende giyim firmasının veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 20/01/2020 tarih ve 2020/50 sayılı Karar Özeti

Karar Tarihi : 20.01.2020

Karar No : 2020/50

Konu Özeti : Bir perakende giyim firmasının kişisel veri ihlali bildirimini

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin bazı müşterilerin yeni bir hesap açarken kişisel verilerinin yanlışlıkla bir URL üzerinden veri sorumlusunun iç sistemlerine ve çalıştığı bazı üçüncü taraf satıcı/sağlayıcılara aktarılması şeklinde gerçekleştiği ve bu durumun veri sorumlusunun olağan bir denetimi esnasında tespit edildiği,
- Kurumumuza veri ihlaline ilişkin bildirim yapıldığında, veri sorumlusunun iki uygulama analizi sağlayıcısından (analytics provider) verilerin hâlihazırda otomatik olarak silinmiş olduğuna dair teyit aldığı,
- İlk bulgulardan sonra konunun daha detaylı araştırılması için gerçekleştirilen soruşturma kapsamında başka yedi adet URL tarafından da sehven veri toplandığı ve bunların veri sorumlusunun etiket yönetim sistemine (tag management system) yönlendirildiğinin öğrenildiği (Türkiye'deki ilgili kişilerin bu yedi adet URL'den iki tanesinde gerçekleşen hatadan etkilendiği),
- İhlalden etkilenen ilgili kişi sayısının 44 olduğu,
- İhlalden etkilenen kişi kategorilerinin aboneler/üyeler, müşteriler/potansiyel müşteriler olduğu,
- Şirketin Kurumumuzu muhatap 10.06.2019 tarihli ilk yazısında, ihlalden etkilenen kişisel verilerin, zorunlu alan olan e-posta adresi, doğum tarihi, açık metin şeklinde şifre verilerinin olduğu, ancak zorunlu alan olmayan ad soyad verilerinin de etkilenmiş olabileceği,
- İlgili kişilere 23.07.2019 tarihinde e-posta yoluyla bildirim yapıldığı

ifadelerine yer verilmiştir.

Veri ihlal bildiriminin Kurumumuzun yetki ve görev alanı çerçevesinde incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 20/01/2020 tarih ve 2020/50 sayılı Kararı ile;

- 01.08.2018 ve 21.10.2018 tarihlerinde gerçekleşen veri ihlallerinin tespitinin yaklaşık bir yıl sonra 02.07.2019 tarihinde yapılmış olmasının, gerçekleştirilen işlemlere dair Şirketin log kaydı/takip alarm sistemlerinin bulunmadığının ya da etkin bir şekilde kullanılmadığının ve Şirket tarafından gerekli kontrollerin yapılmadığının göstergesi olduğu,
- URL üzerinden kişisel verilerin üçüncü taraf satıcı/sağlayıcılar tarafından görülmesinin web sayfası tasarım aşamasında iken yapılan testlerin yetersiz olduğunun veya gerekli testlerin yapılmadığının göstergesi olduğu

kanaatine varıldığından Web sayfası tasarım aşamasında iken yapılan testlerin yetersiz olması, gerçekleşen işlemlere dair takip/alarm sistemlerinin bulunmamasından kaynaklı ihlal tespitinin geç yapılmış olması sebebiyle, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 50.000 TL idari para cezası uygulanmasına,

- İhlalin veri sorumlusu tarafından 29.05.2019 tarihinde tespit edildiği, 06.06.2019 tarihinde Kurula bildirim yapıldığı görülmekle birlikte yurtdışında mukim veri sorumlusu tarafından tespit tarihinden sonra söz konusu ihlalden Türkiye'deki ilgili kişilerin de etkilenip etkilenmediğine yönelik araştırma yapıldığı

dikkate alındığında bu sürenin makul olduğu değerlendirildiğinden bu hususta Kanun kapsamında yapılacak bir işlem bulunmadığına

karar verilmiştir.

2020/43 sayılı KVKK Kararı

İlgili kişiye ait verilerin veri sorumlusu bir banka tarafından rızası olmaksızın babası ile paylaşılması karşısında kişinin Bankadan tazminat talep etmesi hakkında Kişisel Verileri Koruma Kurulunun 16/01/2020 Tarihli ve 2020/43 Sayılı Karar Özeti

Karar Tarihi : 16.01.2020

Karar No : 2020/43

Konu Özeti :İlgili kişiye ait verilerin bir banka tarafından rızası olmaksızın babası ile paylaşılması karşısında Bankadan tazminat talep etmesi hakkında

Kurumumuza intikal eden bir başvuruda ilgili kişiye ait verilerin bir Banka tarafından rızası olmaksızın babası ile paylaşıldığı, veri sorumlusu Banka tarafından düzenlenen belgede babasına, ilgili kişi ile risk grubu oluşturduğu ve ilgili kişinin kredi aksamaları bulunması sebebiyle kendisine kredi kullanılmadığına ilişkin bir yazı verildiği, ilgili kişi tarafından veri sorumlusuna başvuru dilekçesi gönderilerek oluşan manevi zararın tazmini için 30.000 TL'nin ilgili banka hesabına ödenmesi aksi takdirde yasal yollara başvurularak alacağın tahsili yoluna gidileceğinin belirtildiği bununla birlikte Banka tarafından 30 gün içinde başvuruya yönelik bir cevap alınmadığı, bu nedenle de Kurumumuza başvuru yapma gereğinin hasıl olduğu belirtilmiştir.

Konuya ilişkin veri sorumlusu Bankanın savunması istenilmiş, alınan cevabi yazıda;

- İlgili şubenin yaptığı istihbarat sorgulamasının, ilgili kişi ile aynı evde ikamet eden ve 5411 sayılı Bankacılık Kanununun 49 uncu maddesi kapsamında adı geçen ile aynı risk grubunda yer alan oğlunun kredi aksamaları bulunması sebebiyle olumsuz olarak sonuçlandığı, müşteriye de istihbarat olumsuzluğu sebebiyle kredi talebinin uygun görülmediği yönünde şifahi olarak bilgi verildiği,
- 5411 sayılı Bankacılık Kanununun "Risk Grubu" başlıklı 49 uncu maddesinde yer alan "Bir gerçek kişi ile eşi ve çocukları, bunların yönetim kurulu üyesi veya genel müdürü oldukları veya bunların ya da bir tüzel kişinin birlikte veya tek başlarına, doğrudan ya da dolaylı olarak kontrol ettikleri ya da sınırsız sorumlulukla katıldıkları ortaklıklar bir risk grubunu oluşturur. ... Bu maddenin uygulanmasında aralarında birinin ödeme güçlüğüne düşmesinin diğer bir veya birkaçının ödeme güçlüğüne düşmesi sonucunu doğuracak boyutta kefalet, garanti veya benzeri ilişkiler bulunan

gerçek ve tüzel kişiler ilgili risk gruplarına dahil edilir.” hükmü gereğince ilgili kişinin babasının kredi talebinin reddedilmesinin sebebinin aynı evde ikamet ettiği ve aynı risk grubunda yer alan oğlunun kredilerindeki aksamalar olduğu ve oğluna ilişkin genel nitelikteki aksama bilgisinin babasının kredi talebinin reddedilmesi olarak gösterilmesinin zorunlu olduğunun değerlendirildiği,

- Diğer yandan, 6698 sayılı Kişisel Verilerin Korunması Kanununun 5 inci maddesinin 2 nci fıkrasının (a) bendinde de belirtildiği üzere kanunlarda açıkça öngörülmesi durumunda ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu,

- Ayrıca Banka internet sitesi aracılığıyla kamuoyuna duyurulan “.....Bankası Kişisel Verilerin Korunmasına ve İşlenmesine İlişkin Aydınlatma (Bilgilendirme) Metni”nin “Risk Gruplarının Tespiti ve Değerlendirilmesine İlişkin Özel Durum” başlıklı bölümünde de risk grubu kapsamına girecek kişiler -müşteri olmasalar dahi- bankacılık mevzuatına göre bir risk grubuna kullanılacak kredi sınırlarının tespiti için dahil olunacak risk grubunun belirlenebilmesi, izlenebilmesi, raporlanabilmesi, kontrol edilmesi amacıyla kişisel verilerin işlenebileceği açıkça belirtilip, ilan edilerek ilgili kişilerin bu hususta da aydınlatılması yoluna gidildiği,

- Dolayısıyla müşterinin kredisinin reddine dayanak oluşturacak bilgiyle sınırlı olarak aynı risk grubunda bulunanlara ilişkin aksama bilgisinin detay içermeyecek şekilde verilmesinin 6698 sayılı Kanun kapsamında veri ihlali olmadığı düşünülüyor

belirtilmiştir.

Konuya ilişkin yapılan inceleme neticesinde alınan Kişisel Verileri Koruma Kurulunun 16/01/2020 tarih ve 2020/43 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanununun “kişisel verilerin işleme şartları” 5’inci maddesi gereğince kural olarak kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemeyeceği, ancak;

a) Kanunlarda açıkça öngörülmesi,

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması,

- e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

hallerinde ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkün olduğu,

- Risk grubunun 5411 sayılı Bankacılık Kanununda tanımlandığı, 5411 sayılı Bankacılık Kanunu ve ilgili diğer mevzuat hükümleri çerçevesinde “Risk Grubu” içerisinde yer alan kişilerin kişisel verilerinin, ancak bankacılık faaliyetleri kapsamında, kendi bankası bünyesinde kullanılmak ve Risk Merkezine aktarılmak amacıyla işlenmesinin, 6698 sayılı Kişisel Verilerin Korunması Kanununun 5 inci maddesinin ikinci fıkrasının (ç) bendi uyarınca bankaların hukuki yükümlülüklerinin yerine getirilmesi kapsamında olduğunun değerlendirilmesi gerektiği,
- Kişisel Verilerin Korunması Kanununun 12 nci maddesinde “veri güvenliğine ilişkin yükümlülükler” belirlenmiş olup, maddenin 1 numaralı fıkrasında, veri sorumlusunun, (a) “kişisel verilerin hukuka aykırı olarak işlenmesini önlemek”, (b) “kişisel verilere hukuka aykırı olarak erişilmesini önlemek”, (c) “kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak” zorunda olduğunun düzenlendiği, aynı maddenin 4 numaralı fıkrasında ise, veri sorumluları ile veri işleyenlerin, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamayacağı ve işleme amacı dışında kullanamayacağının hüküm altına alındığı,
- Bankacılık Kanununun 76 ncı maddesinde “bankalar, müşterilerinin, verilen hizmetlerden kaynaklanan her türlü sorularına cevap verecek bir sistem kurmakla ve bu hizmetle ilgili bilgiyi müşterilerine bildirmekle yükümlüdür. Bankalar, kredi sözleşmelerinin onaylı bir örneğini müşterilerine vermek zorundadır. Talepleri hâlinde müşteri ile yapılan diğer işlemlere ilişkin her türlü belgenin bir örneği de müşterilere verilir.” hükmü düzenlenmiş olmakla birlikte Bankanın, söz konusu borç bilgisini paylaşmasının, kanun gereğince hizmetle ilgili bilgiyi müşterilerine bildirme yükümlülüğünü yerine getirmesi olarak değerlendirilmesinin uygun olmayacağı,
- Zira Bankacılık Kanununun 73 üncü maddesinin (3) numaralı fıkrası gereğince “Sıfat ve görevleri dolayısıyla bankalara veya müşterilerine ait sırları öğrenenler, söz konusu sırları bu konuda kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamazlar.” hükmü düzenlenmiş olup aynı husus Bankacılık Kanununun 159’uncu maddesinde de “Bu Kanunun 73’üncü maddesinin birinci ve üçüncü fıkralarında belirtilen yükümlülüğe uymayanlar için bir yıldan üç yıla kadar hapis ve bin günden ikibin güne kadar adlî para cezası hükmolunur. Banka ve müşterilere ait sırları açıklayan üçüncü kişiler hakkında da aynı cezalar uygulanır” şeklinde düzenlendiği,

- Aynı zamanda Bankacılık Kanununun Ek 1'inci maddesinde "Risk Merkezi nezdinde bulunan sır niteliğindeki bilgileri, bu konuda kanunen yetkili kılınan mercilerden başkalarına açıklayanlar, hukuka aykırı olarak kendisi ya da başkası yararına kullananlar, yayanlar, verenler, aktaranlar veya ele geçirenler hakkında 159'uncu madde hükümleri uygulanır. Bu fıkrada tanımlanan suçların bir tüzel kişinin faaliyeti çerçevesinde işlenmesi halinde, ilgili tüzel kişi hakkında Türk Ceza Kanununun tüzel kişilere özgü güvenlik tedbirlerine hükmolunur." düzenlemesine yer verildiği,

- Söz konusu verilerin kanuna aykırı olarak üçüncü kişilerle paylaşılması durumunda bu fiili gerçekleştiren kişiler için Türk Ceza Kanununun 136'ncı maddesi gereğince kişisel verilerin hukuka aykırı olarak verilmesi suçunun vücut bulacağı, ayrıca Türk Ceza Kanununun 239/1'inci maddesinde "Sifat veya görevi, meslek veya sanatı gereği vakıf olduğu ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgeleri yetkisiz kişilere veren veya ifşa eden kişi, şikayet üzerine, bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır." hükmü gereğince somut olayda müşteri sırrının ifşasının da söz konusu olacağı

hususlarından hareketle,

- İlgili kişinin başvurusunda manevi zarara uğradığı yönünde bir iddia ve buna ilişkin bir tazminat talebinin söz konusu olduğu dikkate alınarak, Kanunun 14 üncü maddesinin (3) numaralı fıkrasında yer alan "Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır." hükmü çerçevesinde, söz konusu talebini genel mahkemeler huzurunda kullanması gerektiğinden, bu hususta Kanun kapsamında Kurul tarafından tesis edilecek bir işlem bulunmadığına,

- Diğer yandan, ilgili kişinin vekili tarafından yapılan şikayet başvurusu yalnızca tazminat talebine yanıt verilmemiş olmasını içermekte ise de, yapılan incelemede Kanunun 12 nci maddesi hükümlerinin ihlal edildiği kanaati olduğundan veri sorumlusu bünyesinde söz konusu ihlale neden olanlar hakkında Kanunun 18 inci maddesinin hükmü kapsamında işlem tesis edilmesine,

- İlgili kişinin tarafına ait borç bilgilerinin rızası ve bilgisi dışında üçüncü kişilerle paylaşıldığı iddiası, sair mevzuat kapsamında hukuka aykırı bir fiil olduğundan ve bu fiiller Bankacılık Kanunu ve Türk Ceza Kanununun ilgili hükümlerinde de düzenlenmiş olduğundan, ilgili Banka ve personel hakkında Bankacılık Kanunu ve Türk Ceza Kanunu kapsamında işlem tesis edilmesi hususunun değerlendirilmesini teminen konunun Bankacılık Düzenleme ve Denetleme Kurumuna intikal ettirilmesine

karar verilmiştir.

2020/41 sayılı KVKK Kararı

İlgili kişinin kişisel verilerinin hukuka aykırı işlendiği iddiası kapsamında veri sorumlusu bankadan talep ettiği tazminat talebinin karşılanmaması hakkında Kişisel Verileri Koruma Kurulunun 16/01/2020 Tarihli ve 2020/41 Sayılı Karar Özeti

Karar Tarihi : 16.01.2020

Karar No : 2020/41

Konu Özeti :İlgili kişinin kişisel verilerinin hukuka aykırı işlendiği iddiası kapsamında veri sorumlusu Bankadan talep ettiği tazminat talebinin karşılanmaması hakkında

Kurumumuza intikal eden bir şikayet başvurusunda kişinin bir Bankaya kredi borcu olduğu, muhtelif nedenlerle borcunu ödeyemediği ve Bankanın yasal takip başlattığı, 2018'in ikinci yarısında sigortalı olarak bir işe girdiği ve sigortası başlar başlamaz cep telefonundan arandığında cevap vermesine rağmen Bankanın iş yerini aradığı ve aile bilgilerinin sorgulandığı, ödeme yapıp yapmayacağını iş yeri sekreterine defaten sorulduğu, aramalardan sonra aynı yıl içinde iş akdinin firma tarafından sonlandırıldığı belirtilerek konuyla ilgili Bankaya mail yoluyla başvurduğu ve 100.000 TL maddi manevi tazminat isteminde bulunduğu belirtilmiş ve Kurumumuzca gereğinin yapılması talep edilmiştir.

Konuya ilişkin yapılan değerlendirme neticesinde 16/01/2020 tarih ve 2020/41 sayılı Kişisel Verileri Koruma Kurulu Kararı ile;

• 6698 sayılı Kişisel Verilerin Korunması Kanununun 11 inci maddesinin (1) numaralı fıkrasında ilgili kişinin haklarının düzenlendiği buna göre herkesin veri sorumlusuna başvurarak kendisiyle ilgili;

- a) Kişisel veri işlenip işlenmediğini öğrenme,
- b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- d) Kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme,

- e) 7'inci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
- f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması haline zararın giderilmesini talep etme

haklarına sahip olduğu,

- İlgili kişinin veri sorumlusuna başvurusunun 11 inci madde kapsamında bir talep içermediği ve Kuruma şikayetinde de iddialarını kanıtlayıcı bir belge de sunmadığının görüldüğü,
- Ayrıca zarara uğradığı ve buna yönelik bir tazminat talebi söz konusuysa, Kanunun 14'üncü maddesinin (3) numaralı fıkrasında yer alan "Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır." hükmü çerçevesinde, söz konusu talebini genel mahkemeler huzurunda kullanması gerektiği,

hususlarını göz önünde bulundurarak Kanun kapsamında yapılacak bir işlem bulunmadığına karar verilmiştir.

2020/34 sayılı KVKK Kararı

İlgili kişinin dergi aboneliği işlemleri ile ilgili bir çağrı merkezine vermiş olduğu telefon numarasının, anılan çağrı merkezi tarafından bir gıda şirketinin reklamının yapılması amacıyla aranması hakkında Kişisel Verileri Koruma Kurulunun 16/01/2020 Tarihli ve 2020/34 Sayılı Karar Özeti

Karar Tarihi : 16.01.2020

Karar No : 2020/34

Konu Özeti : İlgili kişinin dergi aboneliği işlemleri ile ilgili bir çağrı merkezine vermiş olduğu telefon numarasının anılan çağrı merkezi tarafından bir gıda şirketinin reklamının yapılması amacıyla aranması hakkında

Kurumumuza intikal eden şikayette ilgili kişinin bir gıda şirketi adına 053..... nolu telefonundan arandığını, şirketin internet sitesinin “bize ulaşın” bölümünden kişisel verisinin nasıl elde edildiğine ilişkin başvuruda bulunduğunu ancak kendisine herhangi bir geri dönüşte bulunulmadığını, bunun üzerine ticari işletmeye aynı taleple yazılı olarak da başvurduğunu, çağrı merkezi işiyle iştigal eden bir gerçek kişiden gelen cevabi yazıda;

- Kendisinin 2008 yılından beri yetki aldığı firmaların ürünlerinin çağrı merkezi işi ile uğraştığını, 2013-2014-2015 yıllarında bir spor kulübünün kendisine verdiği yetki uyarınca dergi aboneliği olan kişilerin abonelik süresini uzatmaya yönelik arama hizmeti gerçekleştirdiğini,
- Şikayetçinin söz konusu spor dergisi aboneliği olması dolayısıyla server sisteminde telefon bilgisinin yer aldığı, ilgili kişinin telefon bilgisinin dergi aboneliğinin gerçekleştiği tarihte 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanununun 10. maddesine uygun olarak saklandığı, veri sorumlusunun 2017 yılından bu yana bir gıda markasıyla çeşitli doğal gıda ürünlerinin internet üzerinden satış ve pazarlama işini yürüttüğü,
- Veri sorumlusunun kullanmakta olduğu server arama sisteminin hata sonucu ilgili kişinin numarasının silinmesine karşın sistemin numarayı aradığının tespit edildiği, yapılan yanlışlık akabinde ilgili kişiye yazılı özür cevabı verilerek Kanununun 7 inci maddesi uyarınca kişisel verisinin geri dönülmez şekilde yok edildiği

bilgisinin verildiği, bu çerçevede söz konusu dergiye yapmış olduğu aboneliği kapsamında sisteme kaydedilen verilerin amacı dışında kullanıldığı ifade edilerek 6698 sayılı Kanun kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin yapılan incelemede Kişisel Verileri Koruma Kurulunun 16/01/2020 tarih ve 2020/34 sayılı Kararı ile,

• 6698 sayılı Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinde, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin işlenmesinde uyulması zorunlu ilkelere yer verildiği, bu çerçevede, kişisel verilerin ancak,

- a) Hukuka ve dürüstlük kurallarına uygun şekilde,
- b) Belirli, açık ve meşru amaçlar kapsamında,
- c) Doğru ve gerektiğinde güncel olma şartıyla,
- ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve
- d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme

ilkelerine uygun işlenebileceği,

• Kanunun kişisel verilerin işleme şartlarına ilişkin 5 inci maddesinin (1) numaralı fıkrasında “Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez”, (2) numaralı fıkrasında ise “Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür: a) Kanunlarda açıkça öngörülmesi. b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması. c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması. ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması. d) İlgili kişinin kendisi tarafından alenileştirilmiş olması. e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması. f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması”. hükümlerine yer verildiği,

• Kanunun 7 nci maddesinin (1) numaralı fıkrasında, bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen işlenmesini gerektiren sebeplerin ortadan kalkması halinde

kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silineceği, yok edileceği veya anonim hale getirileceğinin hükme bağlandığı,

- Kanunun Geçiş Hükümlerine ilişkin Geçici 1 inci maddesinin 3 üncü fıkrasında “(3) Bu Kanunun yayımı tarihinden önce işlenmiş olan kişisel veriler, yayımı tarihinden itibaren iki yıl içinde bu Kanun hükümlerine uygun hâle getirilir. Bu Kanun hükümlerine aykırı olduğu tespit edilen kişisel veriler derhâl silinir, yok edilir veya anonim hâle getirilir. Ancak bu Kanunun yayımı tarihinden önce hukuka uygun olarak alınmış rızalar, bir yıl içinde aksine bir irade beyanında bulunulmaması hâlinde, bu Kanuna uygun kabul edilir.” hükmüne yer verildiği,

- Kanunun yürürlük tarihinden önce ilgili kişi tarafından spor dergisi aboneliği sırasında paylaşılan kişisel verilerin o dönemde söz konusu spor kulübü adına dergi aboneliği olan kişilerin abonelik süresini uzatmaya yönelik arama hizmeti gerçekleştiren kişi (veri sorumlusu) tarafından işlendiği, veri sorumlusu tarafından kayıtlarında yer alan bilgilerin başka bir tarihte yine veri sorumlusu tarafından bu kez bir başka Şirket adına işlenerek arandığı, dolayısı ile verinin ilk işleme amacından farklı olarak başka bir amaç için kullanıldığı yani kişisel verilerin Kanunun 4 üncü maddesinde yer alan verinin işlendikleri amaçla bağlantılı ve sınırlı olma ilkesine aykırı hareket edildiği kanaatine varıldığı,

- Öte yandan Kanunun Geçiş Hükümlerine ilişkin Geçici 1 inci maddesinin 3 üncü fıkrasında yer alan “Kanunun yayımı tarihinden önce işlenmiş olan kişisel veriler, yayımı tarihinden itibaren iki yıl içinde bu Kanun hükümlerine uygun hâle getirilir” hükmü kapsamında söz konusu verilerin Kanunun yayınlanma tarihinden sonraki iki yıl içerisinde Kanuna uygun hale getirilmesi amacıyla; spor dergisi aboneliği için çağrı merkezi hizmeti vermeye ilişkin veri sorumlusu ile ilgili spor kulübü arasında imzalanan sözleşmenin 2015 yılında bitmesinin ardından söz konusu verilerin işleme amaçları ortadan kalktığından verilerin silinmesi gerektiği, verinin veri sorumlusu tarafından farklı amaçlarla işlenmesinin sürdürmesi amaçlanıyor ise de ilgili kişinin işleme amaçlarına ilişkin açık rızasının alınması gerektiği ancak bu işlemlerin gerçekleştirilmediğinin anlaşıldığı,

- Her ne kadar veri sorumlusu tarafından ilgili kişinin numarasının silinmesine karşın sistemin numarayı bir hata sonucu aradığı beyan edilse de ilgili kişinin numarasının aranmasının silinme işleminin gerektiği gibi gerçekleştirilmediğinin göstergesi olduğu ve bu kapsamda veri sorumlusunun Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendine yer alan “kişisel verilerin hukuka aykırı olarak işlenmesini önlemek” hükmüne aykırı davrandığının değerlendirildiği hususlarından hareketle veri sorumlusu hakkında, Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 18.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2020/32 sayılı KVKK Kararı

Bir banka tarafından ilgili kişinin kredi kartının rızası dışında üçüncü kişilere teslim edilmesine ilişkin Kişisel Verileri Koruma Kurulu'nun 16/01/2020 Tarih ve 2020/32 Sayılı Karar Özeti

Karar Tarihi : 16.01.2020

Karar No : 2020/32

Konu Özeti : İlgili kişinin kredi kartının rızası dışında üçüncü kişilere teslim edilmesi.

İlgili kişi tarafından Kurumumuza intikal eden şikayet dilekçesinde; yenilenen kredi kartının rızası dışında üçüncü kişilere teslim edilerek kişisel bilgilerinin açığa çıkmasına neden olduğu belirtilmekte olup, Banka hakkında 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında gereğinin yapılması talep edilmiştir.

Yapılan incelemede kişinin yenilenen kredi kartının Banka sisteminde kayıtlı bulunan birinci adresine Kurye tarafından dağıtımına çıkarıldığı ancak kişiye ulaşamadığı, kayıtlı telefon numarasına da Kurye Şirketi tarafından bilgilendirme SMS'lerinin gönderildiği ancak telefon numarasının servis dışı olması sebebiyle SMS'lerin kişiye iletilemediği, birinci adrese teslimat sağlanamadığından Banka sisteminde kayıtlı bulunan ikinci adrese dağıtımına gidildiği ve kartın burada bir kişiye teslim edildiği ancak teslim statüsünün hatalı olması sebebiyle kişiye SMS ile bilgilendirme yapılmadığı, daha sonra kişinin müşteri iletişim merkezi ile yaptığı görüşmelerde kredi kartının aslında birinci adrese teslim edildiğinin sisteme işlendiği, bu adresin doğru olduğu ancak teslim edilen kişinin tanınmıyor olmasının beyan edilmesi üzerine kartın güvenlik altına alınarak kapatıldığı, kartın aslında kişinin ikinci adresi olan eski işyeri adresine teslim edildiği anlaşılmıştır.

Söz konusu başvuru hakkında Kişisel Verileri Koruma Kurulu'nun 16/01/2020 tarih ve 2020/32 sayılı kararı ile,

- Bankanın ilgili kişi tarafından gerekli adres güncellemelerinin yapılmadığına dair savunması karşısında, her ne kadar ilgili kişi bilgileri güncellememiş olsa da kurye tarafından emtianın teslim edilmesi sırasında yeterli kontrolün yapılmadığı, Bankanın da ilgili kişiye ait verilerin güncelliğini sağlamak açısından yeterli ve makul çabayı göstermediği,

- Bankanın ilgili kişinin kredi kartına ilişkin bilgileri kendi veri kayıt sisteminde kendi belirlediği amaçlar ve vasıtalar ile tutmakta olduğundan veri sorumlusu olduğu, Bankanın bu verileri yine müşterisine sunmakta olduğu hizmet kapsamında kredi kartının asıl kart sahibine teslimini gerçekleştirilmesi amacı ile aralarında imzalanan sözleşme kapsamında Kurye ile paylaştığı, söz konusu bu bilgilerin kartın teslimi için gerekli olan ad, soyad, adres gibi bilgileri içerdiği, kredi kartı numarası, son kullanma tarihi CCV numarası gibi kredi kartına ilişkin diğer bilgilerin ise kapalı zarfta yer aldığı ve Kurye firmasının bu bilgilere erişimi olmadığı dolayısı ile bu verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydı ile Kurye tarafından işlenemeyeceği, bu bakımdan Kurye'nin zarfın içerisinde yer alan bilgiler açısından veri sorumlusu olmadığı,

- Kurye'nin Karayolu Taşıma Yönetmeliği çerçevesinde gönderici ve alıcılara ilişkin ad ve soyad, unvan, gerçek kişilerde T.C. kimlik numarası bilgilerini tam ve doğru şekilde kaydetme yükümlülüğüne sahip olduğu, kurye firmalarının yükümlülükleri kapsamında sunacakları hizmeti tam ve doğru bir şekilde yerine getirmek amacı ile bu verileri kendi sistemlerine kaydetmekte olduğu, bu açıdan Kurye'nin bağlı olduğu mevzuat çerçevesinde işlediği kişisel veriler bağlamında veri sorumlusu olduğu,

- Öte yandan somut olayda Banka ile Kurye arasında imzalanan sözleşme kapsamında Kuryenin kredi kartının teslim edilebileceği kişilerin tespitinde sözleşmede yer alan hükümlere aykırı davranmış olduğu, bu hususun Banka ve Kurye arasında 6098 sayılı Borçlar Kanunu çerçevesinde çözüme bağlanması gereken bir durum olduğu,

- Somut olay açısından Bankanın kart teslimi sırasında kişisel verilerin muhafazasını sağlamaya yönelik yükümlülükleri doğrultusunda yeterli idari ve teknik tedbirleri almadığı, ilgili kişiye ait verilerin güncelliğini sağlamak açısından yeterli ve makul çabayı göstermediği,

değerlendirilmiş olup, bu durumun Kanununun 12 nci maddesinin (1) numaralı fıkrasına aykırılık teşkil ettiği kanaatine varılması nedeniyle Kanununun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında Banka hakkında 50.000 TL idari para cezasına hükmedilmesine

karar vermiştir.

2020/26 sayılı KVKK Kararı

Kişisel verilerin veri sorumlusu bir avukat tarafından kısa mesaj yoluyla üçüncü kişilere ifşa edilmesi hakkında Kişisel Verileri Koruma Kurulunun 14.01.2020 Tarihli ve 2020/26 Sayılı Karar Özeti

Karar Tarihi : 14.01.2020

Karar No : 2020/26

Konu Özeti : Kişisel verilerin bir avukat tarafından kısa mesaj yoluyla üçüncü kişilere ifşa edilmesi hakkında

İlgili kişiden alınan şikayet dilekçesinde ve eklerinde özetle;

- Bankaya olan borcundan dolayı veri sorumlusu avukat tarafından İcra Dairesinde icra takibi başlatıldığı,
- İcra takibi başlatılmasından itibaren söz konusu avukatlık bürosu çalışanları tarafından münferit zamanlarda haciz işlemlerinin başladığına ilişkin arandığı ve mesajlar aldığı,
- Aynı içerikteki mesajın yıllardır görüşmediği kardeşine de gönderilmesi üzerine kardeşinin aldığı ekran görüntüsünü kendisine yolladığı,
- Bunun üzerine kişisel verilerinin üçüncü kişilerle paylaşılıp paylaşılmadığını öğrenmek adına kendisine ait mail adresinden veri sorumlusu avukata e-posta gönderdiği,
- Avukatın verdiği cevapta Bankacılık Kanunu ve diğer mevzuatlar gereği borçluya ait telefon numarası veya ikamet adresi bilgilerinin tespit edilememesi ve ulaşılamaması durumunda başkaca tespit ettikleri telefon numarası veya adreslere bilgilendirme mesajı ve bilgilendirme mektubu gönderildiğinin belirtildiği, ancak veri sorumlusunun cevabında yer verilen şahsına ait bir telefon numarasına ulaşılmadığı bilgisinin doğru olmadığı, adına kayıtlı ve kullanmakta olduğu iki adet telefon numarası daha bulunduğu, bu numaralardan hiçbirine bilgilendirme mesajı gelmezken kardeşine ait telefon numarasına mesaj gitmesinin tarafını rencide etmeye yönelik olduğu,

• Ayrıca kardeşine gönderilen mesaja ilişkin ekran görüntüsünün mevcut olmasına rağmen, veri sorumlusu tarafından gönderilen mailin devamında kendisinin kullanmış olduğu telefon numarası dışında hiçbir kişi veya kuruluş ile irtibata geçilmediği yönünde beyanda bulunulduğu

ifade edilerek, yukarıda belirtilen hususlar doğrultusunda konunun Kurumumuzca incelenmesi ve gereğinin yapılması talep edilmiştir.

Kurumumuz tarafından dilekçede belirtilen iddialar ile ilgili olarak veri sorumlusundan savunması istenilmiş, alınan cevabi yazıda özet olarak;

• Avukatlık mesleği itibariyle kişilerin kişisel verilerinin öğrenilmesinin veri işleme faaliyeti olmadığı ve hukuk bürosu olarak kimsenin verilerinin kendilerince işlenmediği,

• Kişisel Verilerin Korunması Kanununun 28 inci maddesinin 1 numaralı fıkrasının (d) bendi hükmü gereğince avukatların da yargı makamı sayılması ve kanun kapsamında istisna tutulması gerektiği,

• İlgili kişinin T.C. kimlik numarası, adres, malvarlığı vb. bilgilerinin bankaya verilmesi suretiyle alenileştirilmiş olduğu,

• İlgili kişinin kardeşine SMS gönderim tarihinden önce ilgili kişinin yakını olduğunu söyleyen bir şahsın ofise geldiği ve borçla ilgili bilgi almak istediği, bu şahsa ilgili kişiye ulaşabilecekleri başka bir yöntem olup olmadığı sorulduğunda şikayete konu telefon numarasını verdiği ve ilgili numaranın da sistemlerine böylece girdiği, zaten ilgili kişinin kardeşiyle iletişime geçilmesinin akabinde talep üzerine telefon numarasının sistemden çıkarıldığı,

• Şikayetçinin müşteri sırrı kapsamındaki bilgi ve belgelerinin yasal mevzuat uyarınca yetkilendirilmiş kişi ve kurumlar hariç olmak üzere üçüncü kişiler ile paylaşılmamasına dair bankaya talimat vermemiş olduğu,

• Gönderilen SMS'in kullanılan kredi türü yahut borç miktarı gibi bir bilgiyi içermediği, tamamen borçluyu borcu ödemeye ve müvekkil banka ile uzlaşmaya davet etmekten ibaret olduğu,

ifade edilerek, Kişisel Verilerin Korunması Kanunu kapsamında hareket ederek, kişiye ilişkin hiçbir bilgi ve belge paylaşımı yapmadığı belirtilmiştir.

Konuya ilişkin Kurulca yapılan inceleme neticesinde alınan 14/01/2020 tarih ve 2020/26 sayılı Karar ile;

• Şikayete konu olayda, Bankaya borçlu olan ve bu borca ilişkin işlemlerin yürütülmesini teminen kişisel verileri Banka tarafından avukata aktarılan ve avukat tarafından kişisel verileri işlenen "ilgili kişi", Banka adına icra işlemlerini yürüten ve bu işlemle ilgili olmak üzere ilgili kişinin kişisel

verilerini işleyen avukatın “veri sorumlusu”, ilgili kişinin bankaya olan borcunu tahsil edebilmek için avukat tarafından ilgili kişiye ait iletişim bilgileri ve diğer ilgili bilgilerinin işlenmesi eyleminin ise veri işleme faaliyeti olduğu,

- Diğer yandan, Kanunda, kişisel verilerin sınırlı sayma yöntemi ile belirlenmediği, bir verinin kişisel veri olması için belirli ya da belirlenebilir gerçek kişiye ilişkin olma kriteri getirildiği, bu bağlamda, ilgili kişinin kardeşine gönderilen mesajın içeriği incelendiğinde, ilgili kişinin açık adını, borçlu olduğu bankayı ve icra dosyası borcuna ilişkin bilgileri ihtiva eden kısa mesaj içeriğinin, ilgili kişiye ait kişisel veri niteliğindeki bilgileri içerdiği,

- Somut olayda, veri sorumlusu bir avukat olup, vekili olduğu Banka adına, Bankanın haklarını ve menfaatlerini korumak amacıyla hareket ettiği, bu anlamda Avukatlık Kanunundan kaynaklanan yükümlülükleri ve yürütmekte olduğu icra işlemleri bakımından İcra İflas Kanunu ve ikincil mevzuat düzenlemelerinden kaynaklanan hukuki yükümlülüklerini yerine getirmek amacıyla borçluya ait bilgileri, kanuna uygun olarak işleme ve ilgili birim/mercilere bildirme yetkisi olduğu ve bu bağlamda işlediği kişisel verilerin Kanunun 5 inci maddesinin 2 numaralı fıkrası çerçevesinde ilgili kişinin açık rızası olmaksızın işlenmesinin kanuna uygun olacağı,

- Ancak Kanun hükümleri gereğince açık rıza aranmaksızın işlenecek kişisel verilerin borçluya ait olması gerektiği, bu kapsamda ne banka ile ne de avukat ile bağı olan ve herhangi bir hukuksal işleme konu kişisel verisi bulunmayan ilgili kişinin kardeşinin telefon numarasının kanuna aykırı olarak ele geçirilmesinin akabinde ilgili kişiye ait kişisel verilerin üçüncü bir kişiye ifşasının Kanunun 5 inci maddesi hükümleri kapsamında değerlendirilemeyeceği,

- Avukat tarafından yapılan savunmada, büroya gelen kimliği belirsiz bir kişiden numaranın temin edildiği açıklamasının, Kanunun 5 inci maddesi kapsamında bir dayanak teşkil etmeyeceğinden, ilgili kişinin kardeşinin telefon numarasının avukat tarafından işlenmesi suretiyle kısa mesaj gönderilmesinin hukuka uygun olmadığı,

- Veri sorumlusu avukat tarafından her ne kadar ilgili kişinin kardeşine ait telefon numarasının büroya gelen ve kimliği bilinmeyen bir kişi tarafından verildiği, bunun ilgili kişiye ait olmadığı tespitini takiben talep üzerine numaranın silindiği beyan edilmiş olsa da sair mevzuat gereğince ilgili kişiye ait olup olmadığı bilinmeyen bir numaranın yine kimliği bilinmeyen bir kişi vasıtasıyla edinilmesi üzerine, ilgili kişiye ait verinin bu numarayla paylaşılmasının Kanun hükümlerine aykırılık teşkil ettiği ve bu suretle kişisel verilerin hukuka aykırı olarak işlenmesini önleme ve kişisel verilere hukuka aykırı olarak erişilmesini önleme yükümlülüğünü yerine getirmeyen veri

sorumlusunun Kanununun 12 nci maddesinde düzenlenen veri güvenliğine ilişkin yükümlülüklere aykırı davrandığı,

- Avukat tarafından yapılan savunmada, Avukatlık Kanununun 1 inci maddesi gereği, avukatların yargının kurucu unsuru olduğu ve bu bağlamda mesleki faaliyetleri gereği elde edilen bilgilerin kişisel verilerin işlenmesi olarak tanımlanmasının hukuken mümkün olmaması gerektiği yönünde ifadeler yer verildiği, Kanununun 28 inci maddesi kapsamında bir istisnadan söz edebilmek için, veri işlemenin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olması; ayrıca veri işlemenin yargı makamları veya infaz mercilerince işlenmesi gerektiği, maddede belirtilen yargı makamlarının tanımlaması yapılmamış olsa da, Devletin yasama ve yürütme faaliyetleri dışında kalan yargı organlarının bu kapsama girdiği, ayrıca, şikayete konu olayda, kişinin borcuna dair bilgilerin kardeşinin telefonuna kısa mesaj olarak iletilmesi; yani borcunu ödemeye ikna etmek amacıyla caydırıcı bir unsur oluşturmak niyetiyle bir yakınıyla paylaşılmasının, Kanununun 28 inci maddesinde sayılan soruşturma, kovuşturma, yargılama ve infaz işlemlerine ilişkin bir işlem olarak kabul edilmesinin mümkün olmadığı

değerlendirildiğinden, ilgili kişiye ait olup olmadığı bilinmeyen bir numaranın yine kimliği bilinmeyen üçüncü bir kişi vasıtasıyla edinilmesi ve ilgili kişiye ait verinin bu numaranın sahibi üçüncü kişi ile paylaşılması nedeniyle Kanununun 12 nci maddesinde düzenlenen veri güvenliğine ilişkin yükümlülükler aykırı hareket eden veri sorumlusu hakkında Kanununun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 50.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2020/20 sayılı KVKK Kararı

Bir Eğitim Kurumu tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmaksızın işlenmesi ve ilgili numaraya reklam/bilgilendirme içerikli mesaj gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 14/01/2020 Tarihli ve 2020/20 Sayılı Karar Özeti

Karar Tarihi : 14.01.2020

Karar No : 2020/20

Konu Özeti : Eğitim Kurumu tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmaksızın işlenmesi ve ilgili numaraya reklam/bilgilendirme içerikli mesaj gönderilmesine ilişkin şikâyet hakkında

İlgili kişinin şahsına ait cep telefonuna açık rızası olmaksızın bir eğitim kurumu tarafından bilgilendirme/reklam amaçlı mesaj gönderilmesi üzerine veri sorumlusuna yaptığı başvuruya yanıt alamaması nedeniyle Kişisel Verileri Koruma Kuruluna ilettiği şikâyet başvurusunun incelenmesi neticesinde; Kişisel Verileri Koruma Kurulunun 14/01/2020 tarih ve 2020/20 sayılı Kararı ile

Eğitim Kurumundan konuya ilişkin gerekli bilgi ve belgelerin istenilmesine ilişkin Kurumumuz yazısının işyerinde daimi çalışana teslim edilmesine rağmen, veri sorumlusu tarafından gerek ilgili kişiye gerek Kurumumuza bahse konu başvuru kapsamında herhangi bir cevap verilmediği dikkate alınarak, mevcut bilgi ve belgeler bir bütün halinde değerlendirildiğinde; Eğitim Kurumu tarafından ilgili kişinin açık rızası veya Kanunun 5 inci maddesinin (2) numaralı fıkrasında sayılan diğer işleme şartları olmaksızın cep telefonuna reklam amaçlı mesaj gönderilmesi suretiyle kişisel verilerinin işlenmesi nedeniyle, Kanun'un 12 nci maddesinin (1) numaralı fıkrasının (a) bendi kapsamında kişisel verilerin hukuka aykırı işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı kanaatine varılan Eğitim Kurumu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 50.000 TL idari para cezası uygulanmasına karar verilmiştir.

2020/13 sayılı KVKK Kararı

İlgili kişi ile veri sorumlusu şirket arasında gerçekleştirilen telefon görüşmelerine ilişkin kayıtların ilgili kişiye verilmesi yönündeki talebin reddedilmesi hakkında Kişisel Verileri Koruma Kurulunun 14/01/2020 Tarihli ve 2020/13 Sayılı Karar Özeti

Karar Tarihi : 14.01.2020

Karar No : 2020/13

Konu Özeti : Sermaye piyasası mevzuatı çerçevesinde, veri sorumlusu şirket ile ilgili kişi arasında imzalanan aracılık sözleşmesine ilişkin işlemlerle bağlantılı olarak ilgili kişiyle yapılmış olan telefon görüşmesi kayıtlarına erişim talebinin reddedilmesi hakkında.

İlgili kişi tarafından Kuruma yapılan şikâyet başvurusunda sermaye piyasası mevzuatı çerçevesinde alım-satım aracılık faaliyeti kapsamında, veri sorumlusu ile imzalanan sözleşme uyarınca işlenen kişisel verilerinden, ilgili kişi ile yapılan telefon görüşmesi kayıtlarının tarafına verilmesi talebinde bulunulduğu ancak, söz konusu telefon görüşmelerine ilişkin kayıtların taraflarına verilmesi yönündeki talebinin reddedildiği belirtilerek, konunun 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında incelenmesi talep edilmiştir.

Söz konusu iddiaların incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 14/01/2020 tarih ve 2020/13 sayılı Kararı ile;

Türkiye Cumhuriyeti Anayasasının “Özel hayatın gizliliği” başlıklı 20 nci maddesinin üçüncü fıkrası hükmüne göre; herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına ve bu anlamda bireylerin temel olarak, kendileri ile ilgili kişisel verilerin ilgisiz üçüncü kişilerin eline geçmemesi konusunda gerekli tedbirlerin alınmasını isteme hakkına sahip olduğu, bu hakkın; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı, bu anlamda bireylerin, hangi amaçla hangi kişisel verilerinin kullanıldığını öğrenme hakkına sahip olduğu gibi söz konusu kişisel verilerde herhangi bir yanlışlık bulunması halinde bu durumun düzeltilmesini ya da verilerinin silinmesini isteme hakkına da sahip olduğuna

6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 11 inci maddesinin birinci fıkrasının (b) bendi hükmü kapsamında ilgili kişinin, kendisiyle ilgili kişisel veriler işlenmişse buna ilişkin bilgi talep etme hakkının, söz konusu veriye erişim hakkını da kapsadığına ve erişim hakkının, bilgi talep etme hakkını tamamlayarak ilgili kişinin, kişisel verileri üzerindeki haklarını kullanabilmesi için, kişisel verilerinin ne şekilde işlendiğine dair tam olarak bilgi sahibi olmasına imkân sağladığına,

Ancak bu hakkın, kişisel verilerin işlendiği veri kayıt sisteminin/kayıt ortamının doğrudan kendisine erişimi, bu kayıt ortamının kendisinin ilgili kişiye teslimini veya doğrudan verinin kendisinin “elde edilme”sini değil; veri sorumlusunun veri güvenliğine ilişkin yükümlülükleri de dikkate alınarak, işlenen kişisel verilerin, teknik/fiziki imkânların el verdiği ölçüde ve verinin muhtevasına/içeriğine ilgili kişi tarafından makul bir şekilde ulaşılabilmesine imkân tanınmasını kapsadığına,

Şikâyetçi ilgili kişinin, veri sorumlusu tarafından işlenen kişisel verilerinin içeriğine, içeriğin tam olarak anlaşılmasına imkan tanıyacak şekilde erişim hakkı ile veri sorumlusunun, teknolojik olarak müdahale ve tahrif edilerek aleyhe kullanılabilir olan ve şikâyetçi dışındaki kişilerin de hassas nitelikli verisini içeren konuşma kayıtlarının kaydedildiği kayıt ortamının kendisinin, ancak yasal makamlar tarafından talep edildiği takdirde teslim edilebileceği yönündeki, makul kabul edilebilecek açıklaması arasındaki dengenin, şikâyetçi ilgili kişi tarafından veri sorumlusundan talep edilen ses kayıtlarına ilişkin kayıt ortamlarının doğrudan ilgili kişiye teslimi suretiyle değil; ancak, talep edilen ses kayıtlarının dökümlerine, verilerin içeriğinin ilgili kişi tarafından tam olarak anlaşılmasına imkan tanıyacak şekilde, erişim hakkı sağlanarak gerçekleştirilebileceğine,

Bu çerçevede, Kanunun 15 inci maddenin 5 inci fıkrasında yer alan; “Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması hâlinde Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ eder. Bu karar, tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilir.” hükmü uyarınca, şikâyet başvurusuna konu telefon görüşmesi kayıtlarına ilişkin dökümün, veri sorumlusu tarafından veri güvenliğine ilişkin yükümlülükler de dikkate alınarak, ilgi kişiye gönderilmesine ve tesis edilen işlemler hakkında da Kurula bilgi verilmesine

karar verilmiştir.

2019/393 sayılı KVKK Kararı

Kişisel Veri Güvenliği Rehberinde geçen “personel gizlilik sözleşmesi” imzalatılmasının 657 sayılı Devlet Memurları Kanununa tabii olarak çalışanlar için gerekli olup olmadığı ile ilgili Kişisel Verileri Koruma Kurulunun 26/12/2019 tarihli ve 2019/393 sayılı Karar Özeti

Karar Tarihi : 26.12.2019

Karar No : 2019/393

Konu Özeti : 657 sayılı Devlet Memurları Kanununa tabii olarak çalışanlara “Personel Gizlilik Sözleşmesi” imzalatılması hakkında.

- Bilindiği üzere Anayasanın 128 inci maddesi; “Devletin, kamu iktisadi teşebbüsleri ve diğer kamu tüzelkişilerinin genel idare esaslarına göre yürütmekle yükümlü oldukları kamu hizmetlerinin gerektirdiği asli ve sürekli görevler, memurlar ve diğer kamu görevlileri eliyle görülür. Memurların ve diğer kamu görevlilerinin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülükleri, aylık ve ödenekleri ve diğer özlük işleri kanunla düzenlenir. Ancak, malî ve sosyal haklara ilişkin toplu sözleşme hükümleri saklıdır.” hükmünü, 129 uncu maddesi ise; “Memurlar ve diğer kamu görevlileri Anayasa ve kanunlara sadık kalarak faaliyette bulunmakla yükümlüdürler.” hükmünü amirdir. Anılan Anayasa maddeleri, kamu hizmetlerinin Devlet memurları ve diğer kamu görevlileri eliyle yürütüleceğini, memurların bu görevleri yürütürken Anayasa ve kanunlara sadık kalma zorunluluğunu haiz olduğunu ve memurlara ilişkin haklar ve yükümlülüklerin kanunla düzenleneceğini açıkça hükme bağlamıştır. Konuya ilişkin ayrıntılı düzenlemelere ise 657 sayılı Devlet Memurları Kanununda yer verilmiştir.
- 657 sayılı Kanunun “Kapsam” başlıklı 1 inci maddesine göre, bu Kanunun kapsamına; Genel ve Katma Bütçeli Kurumlar, İl Özel İdareleri, Belediyeler, İl Özel İdareleri ve Belediyelerin kurdukları birlikler ile bunlara bağlı döner sermayeli kuruluşlarda, kanunlarla kurulan fonlarda, kefalet sandıklarında veya Beden Terbiyesi Bölge Müdürlüklerinde çalışan memurlar girmektedir. Sözleşmeli ve geçici personel için ise, 657 sayılı Kanunda belirtilen özel hükümler uygulanacaktır. 657 sayılı Kanunun 2 nci maddesi gereğince, bu Kanunun amacı; Devlet memurlarının hizmet şartlarını, niteliklerini, atanma ve yetiştirilmelerini, ilerleme ve yükselmelerini, ödev, hak, yüküm ve sorumluluklarını, aylıklarını ve ödeneklerini ve diğer özlük işlerini düzenlemektir. 657 sayılı

Kanunun "Ödevler ve Sorumluluklar" başlıklı İkinci Bölümünde, Devlet memurlarına ilişkin oldukça ayrıntılı düzenlemelere yer verilmiştir. Bu Kanunun 6 ncı maddesi; "Devlet memurları, Türkiye Cumhuriyeti Anayasasına ve kanunlarına sadakatla bağlı kalmak ve milletin hizmetinde Türkiye Cumhuriyeti kanunlarını sadakatla uygulamak zorundadırlar. Devlet memurları bu hususu "Asli Devlet Memurluğuna" atandıktan sonra en geç bir ay içinde kurumlarınca düzenlenecek merasimle yetkili amirlerin huzurunda yapacakları yeminle belirtirler ve özlük dosyalarına konulacak aşağıdaki "Yemin Belgesi"ni imzalayarak göreve başlarlar." hükmünü; 11 inci maddesi; "Devlet memurları kanun ve diğer mevzuatta belirtilen esaslara uymakla ve amirler tarafından verilen görevleri yerine getirmekle yükümlü ve görevlerinin iyi ve doğru yürütülmesinden amirlerine karşı sorumludurlar." hükmünü; 12 nci maddesi; "Devlet memurları, görevlerini dikkat ve itina ile yerine getirmek ve kendilerine teslim edilen Devlet malını korumak ve her an hizmete hazır halde bulundurmak için gerekli tedbirleri almak zorundadırlar." hükmünü amirdir. Anayasanın 128 inci ve 129 uncu maddeleri ile paralellik arz eden bu hükümlerle, Devlet memurlarının görevlerini icra ederken kanun ve diğer mevzuatla bağlı oldukları açıkça düzenlenmiştir.

• Devlet memurlarının görevleri sebebiyle bir zarara sebebiyet vermeleri halini ise, 657 sayılı Kanunun 12 nci ve 13 üncü maddeleri düzenlemiş olup, anılan maddelerde; "Devlet memurunun kasıt, kusur, ihmal veya tedbirsizliği sonucu idare zarara uğratılmışsa, bu zararın ilgili memur tarafından rayiç bedeli üzerinden ödenmesi esastır." ve "Kişiler kamu hukukuna tabi görevlerle ilgili olarak uğradıkları zararlardan dolayı bu görevleri yerine getiren personel aleyhine değil, ilgili kurum aleyhine dava açarlar. Ancak, Devlet dairelerine tevdi veya bu dairelerce tahsil veya muhafaza edilen para ve para hükmündeki değerli kağıtların ilgili personel tarafından zimmete geçirilmesi halinde, zimmete geçirilen miktar, cezai takibat sonucu beklenmeden Hazine tarafından hak sahibine ödenir. Kurumun, genel hükümlere göre sorumlu personele rücu hakkı saklıdır." hükümleri yer almaktadır. Görüldüğü üzere; Devlet memurlarının idare nezdinde bir zarara sebebiyet vermesi halinde, bu zararın giderilmesine ilişkin açık bir kanun hükmünün olmasının yanı sıra; memurlarca kişilere zarar verilmesi hali de ayrıca düzenlenmiştir. Kişilerin bir zarara uğraması halinde, memur hakkında değil ilgili idare hakkında dava açılmakta ve daha sonra o idare ilgili memura rücu edebilmektedir. 13 üncü maddenin gerekçesinde; "Bu madde, kamu hukukuna tabi görevler bakımından idare edilenlere verilecek zararlar konusundaki sorumluluğu düzenlemekte ve bu bakımdan «idare ile memur» arasındaki sorumluluk münasebetlerini düzenleyen 11 inci maddeden farklı bir nitelik taşımaktadır. Buradaki esas, yalnız memurların görevleri dolayısıyla değil, kamu hukukuna tabi bütün görevler dolayısıyla mevcut olduğu için, bu maddede «Devlet memuru» deyimini yerine «personel» deyimini kullanılmıştır. Hususi hukuka tabi hizmetlerde çalışan personel bakımından, tabî, hususi hukuk esasları uygulanacaktır."

Maddedeki teminat iki açıdan incelenmelidir. Her şeyden önce, idare edilenler lehine bir teminat mevcuttur. İdare edilenler, kamu hukukuna tabi görevler dolayısıyla kendilerine verilmiş olan zararlarda, doğrudan doğruya görev sahibi kurum aleyhine dâva açabilecekler ve böylece asıl ödeme kabiliyeti olan bir davalı bulmuş olacaktırlar. Aksi takdirde, özellikle büyük zararlar bakımından, davayı kazansalar bile, ödeme kabiliyeti olmayan bir memurla karşı karşıya kalmaları mümkündür. Halbuki maddedeki şekliyle, her zaman için karşılarında ödeme kabiliyetine sahip bir kurum bulabileceklerdir.

İkinci teminat, memur, daha doğrusu «Kamu hukukuna tabi hizmetlerle görevli personel» bakımındandır. Bu gibi personel, görevlerini yerine getirirken, daimî bir tazminat tehdidi altında kalmayacaklar ve dolayısıyla kamu hizmetlerinin çok ağır görülmesi gibi bir sakıncayla karşılaşılacaktır. Ancak, daimî olarak ve ilk elden dava tehdidi altında bulunmamak, memurların tamamıyla sorumsuz hareket edebilecekleri şeklinde anlaşılmalıdır. Bu madde ile memur, mütemadiyen mahkemelerde kendi aleyhine açılmış davalarla uğraşmaktan korunmuştur ama görevleri dolayısıyla idareye vermiş olduğu zararlardan ötürü idareye karşı olan sorumluluğu devam etmektedir. Zira, 11 inci maddedeki «Zarar», memurun gerek doğrudan doğruya idareye vereceği zararları, gerekse başkalarına zarar ıka etmek ve idareyi bu zararı tazmin mecburiyetinde bırakmak suretiyle sebep olacağı zararları kapsamaktadır. Bu son durumda, 12 nci maddenin son fıkrası hükmüne göre, idarenin haksız fiil sonucundaki genel hükümler çerçevesinde sorumlu personele rücu hakkı saklı kalmaktadır.” açıklamaları yer almaktadır. Bu açıklamalardan anlaşılacağı üzere; memurun bir zarara sebep olması halinde, bu zararın tazmini için doğrudan memur aleyhine değil de idare aleyhine dava açılmasının temelinde, hem zarara uğrayanın zararını tazmin kuvvetini haiz bir kişi ile karşılaşmasının istenilmesi hem de memurun görevini ifa ederken sürekli olarak tazmin baskısı altında hissetmesinin önlenmesinin istenilmesi yatmaktadır. Bu açıklamalar doğrultusunda görülmektedir ki; gerek Anayasa gerek 657 sayılı Kanun, yukarıda yer verilen hükümleri çerçevesinde, gizlilik sözleşmesi ile ulaşılmak istenen amacı karşılayacak nitelikte düzenlemeyi haizdir.

• 657 sayılı Kanun hükümlerinin yanı sıra, Devlete ve Kişilere Memurlarca Verilen Zararların Nevi ve Miktarlarının Tespiti, Takibi, Amirlerinin Sorumlulukları, Yapılacak Diğer İşlemler Hakkında Yönetmelik’in (Yönetmelik) 4 üncü maddesi; “Memurlar görevlerini dikkat ve itina ile yerine getirmek; Devlet malını korumak ve her an hizmete hazır halde bulundurmak için gerekli tedbirleri almakla görevli ve sorumludurlar. Memurlar, bu görev ve sorumlulukların yerine getirilmemesi sebebiyle doğan zararları bu yönetmelikte belli edilen usul ve esaslar uyarınca tazminle mükelleftirler.” hükmünü amir olup; Yönetmeliğin devamında yer alan maddelerde memurlarca verilen zararların giderilme usul ve esasları ayrıntılı olarak düzenlenmiştir. Kaldı ki, Anayasanın 40 inci maddesinde de; “Kişinin, Resmî

görevliler tarafından vaki haksız işlemler sonucu uğradığı zarar da, kanuna göre, Devletçe tazmin edilir. Devletin sorumlu olan ilgili görevliye rücu hakkı saklıdır.” denilmek suretiyle memurun tesis ettiği bir işlem dolayısıyla kişilerin bir zarara uğraması halinde, bu zararın Devlet tarafından tazmin edileceği, yani doğrudan ilgili memura başvurulmayacağı, gerekmesi halinde zararı tazmin eden Devletin ilgili memura rücu edeceği hükme bağlanmıştır. Böylelikle hem Anayasada hem 657 sayılı Kanunda hem de Yönetmelikte memurların görevleri sebebiyle bir zarara sebebiyet vermeleri hali ayrıntılı olarak düzenlenmiş olup; bu zararın giderilmesi Devlete yükletilmiştir. Bu noktada belirtmek gerekir ki, kamu kurum ve kuruluşlarında 6698 sayılı Kişisel Verilerin Korunması Kanununun (**Kanun**) ilgili maddeleri çerçevesinde kişisel verilerin işlenmesi, aktarılması vb. durumlarda bir veri güvenliği ihlali olması, bundan ötürü kişilerin yahut idarenin zarara uğraması halleri de yukarıda açıklanan hükümler çerçevesinde değerlendirilebileceğinden 657 sayılı Kanun kapsamında çalışan kişilerle ayrıca bir personel gizlilik sözleşmesinin imzalatılması suretiyle bu sorumluluğun düzenlenmesi uygun olmayacaktır.

- 657 sayılı Kanunun 16 ncı maddesinde yer alan; *“Devlet memurları görevleri ile ilgili resmi belge araç ve gereçleri, yetki verilen mahaller dışına çıkaramazlar, hususi işlerinde kullanamazlar. Devlet memurları görevleri icabı kendilerine teslim edilen resmi belge, araç ve gereçleri görevleri sona erdiği zaman iade etmek zorundadırlar. Bu zorunluluk memurun mirasçılara da şamildir.”* düzenlemesi ile Devlet memurları için görevlerine ilişkin resmi belgelerin yetki verilen mahallerin dışına çıkarmaması ve görevlerinin sona ermesi ile bu belgeleri teslim etmesi zorunluluğu getirilmiştir. Böylelikle, göreve ilişkin resmi belgelerin güvenliği temin edilmek istenilmiştir.

- Bununla birlikte, gerek Kişisel Veri Güvenliği Rehberinde gerek Kişisel Verileri Koruma Kurulunun 31/01/2018 tarihli 2018/10 sayılı Kurul kararında bahsi geçen personel gizlilik sözleşmesi imzalatılması hususu, daha ziyade bir işverenin emir ve talimatları doğrultusunda iş akdine bağlı olarak çalışanlar yahut kamu kurum ve kuruluşlarında 657 sayılı Kanuna tabi olmaksızın çalışanlar için uygulanabilecektir.

- Sonuç olarak; Anayasa, 657 sayılı Kanun ve ilgili ikincil mevzuat kapsamında Devlet memurunun başlıca ödevi (yükümlülüğü) Anayasaya, kanunlara sadık kalarak görevini ifa etmektir. Dolayısıyla, kişisel verilere ilişkin tesis edilen iş ve işlemlerde de 6698 sayılı Kanun hükümlerine uygun davranma yükümlülüğü, bu yükümlülüğe aykırı davranması halinde gerek idareye gerek kişilere verdiği zararlardan ötürü sorumluluğu söz konusudur. Bir başka ifadeyle, bu kişilerin yükümlülükleri hâlihazırda 657 sayılı Kanun ve ilgili yönetmeliklerle belirlenmiş olup; 6698 sayılı Kanun ve ilgili yönetmeliklere uygun hareket etmeleri görevlerini ifa ederken uymaları gereken başlıca

yükümlülüklerindedir. Yukarıda yer verilen gerekçelerle, kamu kurumu nezdinde 657 sayılı Kanun kapsamında çalışan ve kişisel veri işleyen personele kişisel verilerin korunmasına yönelik ayrıca bir gizlilik sözleşmesi imzalatılması uygun olmayacaktır. Ancak bu noktada önemle belirtmek gerekir ki, kişisel verilerin korunması hakkının bir temel hak ve özgürlük olarak yakın tarihte iç hukukumuzda düzenleme altına alınmış olduğu gözetildiğinde, 657 sayılı Kanun kapsamında çalışan personele, kişisel verilerin korunması hakkı kapsamında uymaları gereken usul ve esaslara dair bilgilendirici mahiyette bir metin tebliğ edilmesi ve bu konuda periyodik eğitimler düzenlenmesi uygun olacaktır.

2019/389 sayılı KVKK Kararı

Aday Puanlarının Rıza Alınmaksızın, İnternet Sitesinde Paylaşılması Hakkındaki Görüş Talebi ile ilgili Kişisel Verileri Koruma Kurulunun 26/12/2019 Tarihli ve 2019/389 Sayılı Karar Özeti

Karar Tarihi : 26.12.2019

Karar No : 2019/389

Konu Özeti : Öğretim görevlisi ve araştırma görevlisi kadrolarına yapılacak atamalarda adaylardan talep edilen kişisel veri niteliğindeki bilgilerin internet ortamında yayımlanması uygulaması hakkında

Kurumumuza iletilen; öğretim görevlisi ve araştırma görevlisi kadrolarına yapılacak atamalarda uygulanacak “Öğretim Üyesi Dışındaki Öğretim Elemanı Kadrolarına Yapılacak Atamalarda Uygulanacak Merkezi Sınav ile Giriş Sınavlarına İlişkin Usul ve Esaslar Hakkında Yönetmelik” (Yönetmelik) hükümleri doğrultusunda değerlendirme puanlarının, veri sorumlusunun internet sitesi aracılığıyla kamuoyuyla paylaşılmasınının 6698 sayılı Kişisel Verilerin Korunması Kanununa (Kanun) uygun olup olmadığı konusundaki görüş talebinin incelenmesi neticesinde;

Öncelikli olarak belirtilen ilanın, mevzuatta öngörülen süre kadar; böyle bir düzenleme yoksa veri sorumlusu tarafından işlendiği amaç için gerekli olduğu değerlendirilen süre ile sınırlı olması gerektiği, bununla birlikte söz konusu kişisel verilerin, internet ortamında ya da diğer fiziki ortamlarda ilanı halinde üçüncü kişiler tarafından tüm unsurlarıyla bilinir hale gelmesinde bir yarar bulunmadığı dikkate alındığında,

İnternet ortamında yayımlanan kişisel verilerin tamamen kaybolmadığı göz önüne alındığında değerlendirme puanlarının, Kanunun 4 üncü maddesinde yer alan genel ilkelere uyumlu şekilde, yalnızca akademik kadrolara müracaat eden ilgili kişilerce görüntülenebileceği bir yöntemle ve kimlik doğrulaması yapılmak suretiyle sorgulamasına imkân verecek şekilde ilan edilmesi gerektiğine,

İlgili kişiler ile sınav puanları arasındaki bağlantının, maskeleyme (kişisel verilerin belli alanlarının kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin çizilmesi, boyanması ve yıldızlanması gibi işlemler) yöntemleriyle kaldırılmasınının uygun olacağına, bu kapsamda adaylara ait ad- soy ad, T.C. kimlik numarası gibi verilerin, kişiyi belirli ya da

belirlenebilir kılabilme özelliğinin ortadan kaldırılabilmesi adına, anılan bilgilerin açık şekilde yazılması yerine, kişinin kendisinin anlayabileceği şekilde harflerin ya da rakamların "A**** B**** , 11*****11" şeklinde yıldızlanarak yukarıda sözü edilen yöntemlerle yayımlanabileceğine,

Kanununun 10 uncu maddesinde hükme bağlanan aydınlatma yükümlülüğü kapsamında, üniversiteler tarafından söz konusu kişisel veri işleme faaliyetine ilişkin olarak ilgili kişilerin aydınlatılması gerektiğine

karar verilmiştir.

2019/387 sayılı KVKK Kararı

Veri Sorumluları Siciline Kayıt Yükümlülüğüne İlişkin Kurulca Belirlenen Sürelerin Uzatılması ile ilgili Kişisel Verileri Koruma Kurulunun 17/12/2019 Tarihli ve 2019/387 Sayılı Kararı

Karar Tarihi : 17.12.2019

Karar No : 2019/387

Konu Özeti : VERBİS'e kayıt tarihlerinin uzatılması

I. Kararın Konusu

Bilindiği üzere 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 16 ncı maddesi gereği, kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır.

Veri Sorumluları Sicili, Kişisel Verileri Koruma Kurulu (Kurul) gözetiminde Başkanlık tarafından kamuya açık olarak tutulmaktadır. Bu amaçla oluşturulan ve kısa adı VERBİS olan Veri Sorumluları Sicil Bilgi Sistemine, kayıt yükümlülüğü kapsamındaki veri sorumlularınca işlemekte oldukları kişisel verilerle ilgili bilgi girişi yapılması gerekmektedir.

Veri Sorumluları Sicilinin kamuya açık olarak tutulması; kişisel verisi işlenen gerçek kişilere, kendi verileri üzerinde kontrolün sağlanabilmesi imkânı sunduğundan VERBİS, şeffaflık ve hesap verebilirlik özelliği ile ön plana çıkmaktadır.

Sicile kayıt yükümlülüğü, kişisel veri işlemekte olan gerçek veya tüzel kişiler için Kanunla getirilmiş bir yükümlülük olup bu yükümlülüğe uyulmaması halinde yaptırım öngörülmüş olmakla birlikte asıl hedeflenen; kişisel verilerin işlenmesinde şeffaflığın sağlanması, veri sorumlularının Kanuna uyumu konusunda özen göstermeleri, kişisel veri işlenmesinin disiplin altına alınması, kişisel verisini işlediği kişilere hesap verebilmesi, kişisel verilerin gelişigüzel işlenmesinin önüne geçilmesi ve bu konuda bir kültür ve farkındalık oluşmasının sağlanmasıdır.

Kayıt yükümlülüğünün yerine getirilmesi ile ilgili tarihler de Kanunun geçici 1. maddesine istinaden Kurul tarafından belirlenerek aşağıdaki gibi ilan edilmiştir:

Veri Sorumluları	Başlama Tarihi	Verilen Süre	Son Tarih
Yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları	01.10.2018	15 ay	31.12.2019
Yurtdışında yerleşik gerçek ve tüzel kişi veri sorumluları	01.10.2018	15 ay	31.12.2019
Yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25 milyon TL'den az olup ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek ve tüzel kişi veri sorumluları	01.01.2019	15 ay	31.03.2020
Kamu kurum ve kuruluşu veri sorumluları	01.04.2019	a5 ay	30.06.2020

II. Kararın Hukuki Dayanağı ve Sonuç

Bilindiği üzere, Kanunun 16 ncı maddesinde, istisna kapsamında olmayan veri sorumluları için getirilmiş olan yükümlülük, kayıt ve bildirim yükümlülüğünün yerine getirilmesidir. Bu kapsamda veri sorumlularının, önce VERBİS'e giriş yaparak başvuru formunu sistem üzerinden oluşturması ve bu formun Kuruma kargo / posta / elden iletilmesi veya Kayıtlı Elektronik Posta (KEP) aracılığıyla iletilmesi gerekli görülmektedir. Başvuru formunun iletilmesi üzerine Kurum tarafından kendisine iletilen "kullanıcı adı" ve "parola" ile VERBİS'e giriş yaparak bildirim yapması gerekmektedir.

VERBİS üzerinden yapılan değerlendirme sonucunda, bazı veri sorumlularınca söz konusu başvuru formlarının Başkanlığımıza iletilmesi ile yükümlülüğün yerine getirilmiş olduğu düşünüldükçe bildirim yapılmadığı gözlemlenmektedir. İrtibat kişisi tarafından "Sicile kayıt" butonu ile giriş yapılarak bildirim tamamlanması ve sistem üzerinden iletilmediği takdirde Sicile kayıt ve bildirim yükümlülüğünün yerine getirilmemiş olacağının bilinmesinde fayda görülmektedir.

Öte yandan, Sicile kayıt yükümlüsü olan veri sorumlularınca, Kurul kararında öngörülen sürede kayıt ve bildirim yükümlülüğünü yerine getirmek amacıyla son günlerde yoğun bir şekilde başvuru ve VERBİS üzerinden bildirim iletildiği gözlemlenmektedir.

Veri sorumlularına, 6698 sayılı Kanunla Sicile kayıt ve bildirim yükümlülüğü getirilmiş olmasının amacı;

- Kişisel verilerin işlenmesinde şeffaflığın,
- Kişisel verilerin gelişigüzel işlenmesinin önüne geçilerek bu alanda veri sorumlularının kişisel veri işleme faaliyetlerinin disiplin altına alınmasının,
- Kişisel verilerin korunması alanında toplumun tüm kesimlerinde kültür ve farkındalık oluşmasının, veri sorumlularının kişisel verisini işlediği kişilere hesap verebilmesinin,
- Veri sorumlularının Kanuna uyumunun,
- İstisna kapsamında olmayan tüm veri sorumlularının Sicile kaydolmasının

sağlanmasıdır.

Bu amaçlardan da anlaşılacağı üzere Sicile kayıt ve bildirim yükümlülüğü, sadece süresinde VERBİS'e kayıt olunmasını değil, bununla birlikte VERBİS'e beyan edilen bilgilerin tüm kişisel veri işleme faaliyetlerini kapsayacak şekilde doğru, güncel ve güvenilir bilgilerin de beyan edilmesini kapsamaktadır.

VERBİS veri tabanı üzerinden özellikle son günlerde iletilen bildirimlerle ilgili olarak yapılan araştırmada, bazı bildirimlerde işlendiği beyan edilen kişisel verilerle işleme amaçlarının, aktarım gerçekleştirildiği beyan edilen alıcı/alıcı gruplarının, veri konusu kişi gruplarının, alınan teknik ve idari tedbirlerin, özel nitelikli kişisel veriler için alınması gereken yeterli önlemlerin, yurtdışına veri aktarımının ve saklamaya ilişkin beyan edilen sürelerin örtüşmediği, bu konuda ciddi yanlışlıkların ve Kanuna/yönetmeliklere aykırılıkların olduğu görülmektedir.

Bu durumun nedenlerinden birisinin de Kanunun 18 inci maddesinde öngörülen yaptırımlarla karşılaşmamak adına Kurul tarafından belirlenen süre içerisinde bir kayıt gerçekleştirmek olduğu anlaşılmaktadır.

Kanunun 16 ncı maddesinde Sicile ilişkin bazı hükümler yer almış olup diğer usul ve esasların da yönetmelikle düzenleneceği ifade edilmiştir. Buna istinaden 31.12.2017 tarihli Resmi Gazetede yayımlanarak yürürlüğe giren Veri Sorumluları Sicili Hakkında Yönetmeliğin 5 inci maddesinde;

“ç) Sicile kayıtla yükümlü olan veri sorumluları, Kişisel Veri İşleme Envanteri hazırlamakla yükümlüdür. Sicil başvurularında Sicile açıklanacak bilgiler Kişisel Veri İşleme Envanterine dayalı olarak hazırlanır.

d) Kanununun 10 uncu maddesinde veri sorumluları için belirtilen aydınlatma yükümlülüğünde, Kanununun 13 üncü maddesinde belirtilen ilgili kişi başvurularının yanıtlanmasında ve ilgili kişiler tarafından açıklanacak açık rızanın kapsamının belirlenmesinde kişisel veri işleme envanterine dayalı olarak Sicile sunulan ve Sicilde yayınlanan bilgiler esas alınır.

e) Veri sorumluları, Sicile sunulan ve Sicilde yayınlanan bilgilerin eksiksiz, doğru, güncel ve hukuka uygun olmasından sorumludur. Veri sorumlularının Sicile kaydolması Kanun kapsamındaki diğer yükümlülüklerini ortadan kaldırmaz.”

hükümleri yer almıştır.

Buna göre, veri sorumlularının VERBİS'e kayıt ve bildirim yükümlülüğünü yerine getirirken öncelikle kişisel veri işlenmekte olan tüm süreçleri içerecek şekilde kişisel veri işleme envanteri hazırlanması ve VERBİS'e bildirim yapılırken gelişigüzel değil mutlaka söz konusu envanter baz alınarak giriş yapılması gerekmektedir.

Ayrıca, Kanununun 16 ncı maddesinde Sicile girilen bilgilerde meydana gelen değişikliklerin derhâl Başkanlığa bildirileceği hükmü ile Veri Sorumluları Sicili Hakkında Yönetmeliğin 13 üncü maddesinde yer alan “Veri sorumluları, Sicilde kayıtlı bilgilerde değişiklik olması halinde meydana gelen değişiklikleri, değişikliğin meydana geldiği tarihten itibaren yedi gün içerisinde VERBİS üzerinden Kuruma bildirir.” hükmü gereği gerekli güncellemelerin belirtilen sürede yapılması gerekmektedir.

Veri sorumlularınca Sicile kayıt ve bildirim yükümlülüğünün yerine getirilmesi amacıyla VERBİS'e girilen bilgiler üzerinden Kurul tarafından yapılan araştırma ve değerlendirme sonucunda;

a) Sicile kayıt ve bildirim yükümlülüğünün yerine getirilmesi kapsamında;

- Bazı veri sorumlularının sadece kayıt başvuru formunu ilettiğinin görüldüğü, Kanununun 16 ncı maddesinde yer alan yükümlülüğün kayıt ve bildirim kapsadığı, bu nedenle Kurumca iletilen “kullanıcı adı” ve “parola” ile VERBİS'e giriş yapılarak kişisel veri işleme faaliyetlerine ilişkin bildirim tamamlanması gerektiğinin,

- Sicile kayıt ve bildirim yükümlülüğünün asıl amacının kişisel veri işlemede şeffaflık, kişisel verilerin gelişigüzel işlenmesinin önüne geçilerek kişisel veri işleme faaliyetlerinin disiplin altına alınması, bu alanda kültür ve farkındalık oluşması, veri sorumlularının kişisel verisini işlediği kişilere

hesap verebilmesi, veri sorumlularının Kanuna uyumu ve istisna kapsamında olmayan tüm veri sorumlularının Sicile kaydolmasının sağlanması olduğunun,

- Sicile kayıt ve bildirim yükümlülüğünün sadece Kanunda öngörülen yaptırımlarla karşılaşmamak adına süresi içerisinde bir kayıt gerçekleştirmek olarak anlaşılması gerektiği, bu amaca yönelik kayıt ve bildirimlerin Kanuna aykırılık teşkil edeceğinin,
- Özellikle son zamanlarda VERBİS'e iletilen bildirimler incelendiğinde, birçok bildirimde kişisel veriler ile işleme amaçları, alıcı/alıcı grupları, veri konusu kişi grupları, alınan teknik ve idari tedbirler, yeterli önlemler, yurtdışına veri aktarımı ve saklama sürelerinin örtüşmediği, bu konuda ciddi yanlışlıklar ve mevzuata aykırılıklar olduğunun görüldüğünün,
- VERBİS'e beyan edilen bilgilerin doğru ve güncel olması gerektiği, bu bilgilerden ilgili veri sorumlusunun sorumlu olduğunun,
- Sicile kayıtle yükümlü olan veri sorumlularının Veri Sorumluları Sicili Hakkında Yönetmelik gereği kişisel veri işleme envanteri hazırlamak zorunda olduğunun ve VERBİS'e girilen bilgilerin bu envantere dayalı olarak hazırlanması gerektiğinin,
- Veri sorumlularının VERBİS'e kayıt ve bildirim yükümlülüğünü yerine getirirken öncelikle kişisel veri işlenmekte olan tüm süreçleri içerecek şekilde kişisel veri işleme envanteri hazırlaması ve VERBİS'e bildirim yapılırken gelişigüzel değil mutlaka söz konusu envanter baz alınarak giriş yapılması gerektiğinin,
- Sicilde kayıtlı bilgilerde değişiklik olması halinde meydana gelen değişiklikleri, değişikliğin meydana geldiği tarihten itibaren yedi gün içerisinde VERBİS üzerinden Kuruma bildirilmesi gerektiğinin,

tüm veri sorumlularına hatırlatılmasına,

b) Yukarıda yer verilen açıklamalar doğrultusunda kişisel veri işleme envanteri hazırlamadan gelişigüzel VERBİS'e kayıt ve bildirim gerçekleştiren veri sorumluları ile envanter hazırlama süreçlerini tamamlayamadığı için süresinde kayıt ve bildirim yükümlülüğünü yerine getiremeyecek olan veri sorumluları dikkate alınarak, VERBİS'e girilmiş olan bilgilerde herhangi bir hata veya Kanuna aykırılık varsa bu durumun bir an önce düzeltilmesi için gerekli çalışmaların yapılabilmesini teminen 6698 sayılı Kanununun Geçici 1 inci maddesi gereği Sicile kayıt ve bildirim yükümlülüğü için belirlenen tarihlerin;

- Yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları için Sicile kayıt ve bildirim yükümlülüğünü yerine getirmeleri için belirlenen sürenin 30.06.2020 tarihine,
- Yurtdışında yerleşik gerçek ve tüzel kişi veri sorumluları için Sicile kayıt ve bildirim yükümlülüğünü yerine getirmeleri için belirlenen sürenin 30.06.2020 tarihine,
- Yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25 milyon TL'den az olup ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek veya tüzel kişi veri sorumluları için Sicile kayıt ve bildirim yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.09.2020 tarihine,
- Kamu kurum ve kuruluşu veri sorumluları için için Sicile kayıt ve bildirim yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.12.2020 tarihine,

kadar uzatılmasına

c) Bu kararın Kurum internet sayfasında duyurulması ve Resmî Gazete'de aşağıdaki gibi yayımlanmasına

oybirliği ile karar verilmiştir.

“Veri sorumlularınca Sicile kayıt ve bildirim yükümlülüğünün yerine getirilmesi amacıyla VERBİS'e girilen bilgiler üzerinden Kurul tarafından yapılan araştırma ve değerlendirme sonucunda;

Yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları için Sicile kayıt ve bildirim yükümlülüğünü yerine getirmeleri için belirlenen sürenin 30.06.2020 tarihine,

Yurtdışında yerleşik gerçek ve tüzel kişi veri sorumluları için Sicile kayıt ve bildirim yükümlülüğünü yerine getirmeleri için belirlenen sürenin 30.06.2020 tarihine,

Yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25 milyon TL'den az olup ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek veya tüzel kişi veri sorumluları için Sicile kayıt ve bildirim yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.09.2020 tarihine,

Kamu kurum ve kuruluşu veri sorumluları için için Sicile kayıt ve bildirim yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.12.2020 tarihine,

kadar uzatılmasına

Bu kararın Kurum internet sayfasında duyurulması ve Resmî Gazete'de yayımlanmasına

oybirliği ile karar verilmiştir.”

2019/276 sayılı KVKK Kararı

Sevinç Eğitim Kurumlarının kişisel veri işleme şartları olmaksızın ilgili kişinin cep telefonuna reklam amaçlı kısa mesaj göndermesi hakkında Kişisel Verileri Koruma Kurulunun 18.09.2019 Tarihli ve 2019/276 sayılı Karar Özeti

Karar Tarihi : 18.09.2019

Karar No : 2019/276

Veri Sorumlusu: Sevinç Eğitim Kurumları

Konu Özeti : Bir eğitim kurumunun kişisel veri işleme şartları olmaksızın ilgili kişinin cep telefonuna reklam amaçlı kısa mesaj göndermesine ilişkin yapılan şikayet hk.

Bir eğitim kurumunun kişisel veri işleme şartları olmaksızın ilgili kişinin cep telefonuna reklam amaçlı kısa mesaj göndermesine ilişkin yapılan şikayet hk.

Bu çerçevede;

- 6698 sayılı Kişisel Verilerin Korunması Kanununun “Tanımlar” başlıklı 3 üncü maddesinde; kişisel verilerin işlenmesi, kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı,
- Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise Kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek

kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- 28.09.2018 tarihli ve 2018/112 sayılı Kurul Kararına istinaden Sevinç Eğitim Kurumları nezdinde yapılan yerinde inceleme esnasında istenilen ve 05.08.2019 tarihine kadar Kuruma gönderilmesi tebliğ edilen bilgi ve belgelerin eğitim kurumu tarafından Kuruma iletilmediği de dikkate alındığında,

anılan eğitim kurumu tarafından Şikayetçinin açık rızası veya Kanunun 5 inci maddesinin (2) numaralı fıkrasında sayılan diğer işleme şartları olmaksızın cep telefonuna reklam amaçlı mesaj gönderilmesi suretiyle kişisel verilerinin işlenmesi nedeniyle anılan eğitim kurumunun Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendi kapsamında kişisel verilerin hukuka aykırı işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı kanaatine varılması sebebiyle, Sevinç Eğitim Kurumları hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi hükmü gereğince 50.000 TL idari para cezası uygulanmasına karar verilmiştir.

2019/372 sayılı KVKK Kararı

Bir gazete tarafından ilgili kişinin özel nitelikli kişisel verileri hakkında haber yapılmasına ilişkin Kişisel Verileri Koruma Kurulu'nun 09/12/2019 tarih ve 2019/372 sayılı Karar Özeti

Karar Tarihi : 09.12.2019

Karar No : 2019/372

Konu Özeti : Bir gazete tarafından ilgili kişinin özel nitelikli kişisel verileri hakkında haber yapılması

Kurumumuza intikal eden bir şikayet dilekçesinde;

- Bir Gazetede şikayet sahibinin oğluna yönelik yer alan köşe yazısında, babasının kanser tedavisi nedeniyle bir süre önce görevine ara verdiğiine ilişkin bir habere yer verildiği dolayısı ile ilgili kişinin özel nitelikli kişisel verisi olan sağlık verilerinin rızası dışında işlendiği ve üçüncü kişilerle paylaşıldığı,
- İlgili kişinin bu tarihe kadar kanser tedavisi gördüğünü bilmediği, rahatsızlığından ötürü psikolojisinin ve moralinin bozulması istenmediğinden bu bilginin ailesi tarafından kendisinden saklandığı, ancak haber tarihinden sonra ilgili kişinin geçmiş olsun dilekleri ile arandığı, hastalığını öğrenerek ölüm korkusu yaşadığı, ilgili kişinin kanser olduğunu Gazeteden ve üçüncü kişilerden öğrenmesinden dolayı içine kapandığı ve ailesiyle iletişimini kestiği, ölüm korkusu nedeniyle ayrıca psikolojik tedavi görmeye başladığı ve kanser tedavisini reddettiği

ifade edilerek Kanun çerçevesinde Kurumumuzca yasal işlemlerin yapılması talep edilmiştir.

Söz konusu başvuru hakkında Kişisel Verileri Koruma Kurulu'nun 01.07.2019 tarih ve 2019/186 sayılı kararı ile, özel nitelikli kişisel veri niteliğindeki sağlık verisinin söz konusu köşe yazısına konu edilerek yayımlanmasında halihazırda kamu yararı bulunmadığı, bu itibarla çatışan haklar bakımından kişilik haklarının ifade özgürlüğüne üstün geldiği kanaatine varıldığından, konunun 6698 sayılı Kanununun 28 inci maddesinin (1) numaralı fıkrasının (c) bendi çerçevesinde değerlendirilemeyeceğine ve bu itibarla söz konusu başvurunun 6698 sayılı Kanununun 15 inci maddesinin (1) numaralı fıkrası çerçevesinde incelemeye alınmasına karar verilmiş olup yapılan

inceleme çerçevesinde Kişisel Verileri Koruma Kurulunun 09/12/2019 tarih ve 2019/372 sayılı kararı ile;

- Gazete tarafından Kanunun 6 ncı maddesinde sayılan şartlardan birine dayanmaksızın ilgili kişinin özel nitelikli kişisel verilerinin, köşe yazısında paylaşılmasının Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendine aykırılık teşkil ettiği kanaatine varıldığından, Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında söz konusu Gazete hakkında 125.000 TL idari para cezasının uygulanmasına, karar vermiştir.

2019/269 sayılı KVKK Kararı

Facebook hakkında Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/269 sayılı Karar Özeti

Karar Tarihi : 18.09.2019

Karar No : 2019/269

Konu Özeti : Facebook “Başkasının Gözünden Gör” uygulaması üzerinden gerçekleşen veri ihlali hakkında Karar

Facebook temsilcisi tarafından Kurumumuza gönderilen 14.10.2018 tarihli e-posta ile Facebook sisteminin birbirinden farklı üç özelliği olan “başkasının gözünden gör”, “doğum günü kutlayıcı” ve “video yükleyicinin” etkileşimi sonucunda oluşan bir hatadan kaynaklanan veri ihlaline ilişkin bilgi verilmiştir. Facebook temsilcisinin göndermiş olduğu e-postada özetle;

- Facebook Inc. nezdinde 14-28 Eylül 2018 tarihleri arasında access token (erişim jetonları) kullanılmak suretiyle Facebook platformları üzerinden çeşitli Facebook hesabı bilgilerinin ele geçirildiği,
- 25 Eylül 2018 tarihinde saldırganların erişim jetonları elde etmek için sistemleri üzerindeki üç hata arasındaki kompleks etkileşimden doğan bir zafiyetten faydalandıklarının tespit edildiği,
- Erişim jetonlarının, aynı dijital bir anahtar gibi, Facebook platformları üzerinden çeşitli bilgilerin elde edilebilmesi için kullanıldığı,
- İncelemeler sonucunda, ilgili zafiyetin Facebook’un kodu içerisinde 21 Temmuz 2017 tarihinde meydana geldiğinin tespit edildiği, ancak erişim jetonlarına yetkisiz olarak erişilmesine sebep olan bu saldırının 14 Eylül 2018 tarihinde başladığı kanaatini taşıdıkları, zira (25 Eylül 2018 tarihinde gerçekleştirilen incelemeler kapsamında) beklentinin üzerinde bir “View As” (Başkasının Gözünden Gör) trafiği artışının bu tarihte başladığının tespit edildiği,
- 28 Eylül 2018 tarihinde kod üzerindeki zafiyetin düzeltilerek saldırının durdurulduğu, bununla birlikte ihlal hakkındaki incelemelerin devam ettiği,

• İlgili zafiyetin, üç ayrı hatanın birbiri ile etkileşiminin bir sonucu olarak meydana geldiği, buna göre etkileşen üç hatanın; 1) “Başkasının Gözünden Gör” ara yüzünün, kullanıcıların kendi profillerinin başkaları tarafından nasıl görüntülendiğini görebildiği bir gizlilik özelliği olduğu, “Başkasının Gözünden Gör” özelliğinin yalnızca bir görüntüleme arayüzü olarak tasarlandığı, ancak kişilerin Facebook’a içerik yüklemesini sağlayan bir kutucuk (composer) üzerinden (spesifik olarak, kişilerin arkadaşlarının doğum günlerini kutlamalarını sağlayan versiyon üzerinden) “Başkasının Gözünden Gör” arayüzünde video yüklenmesi imkanının yanlışlıkla sağlandığı, 2) Video yükleyicisinin Temmuz 2017’de hayata geçirilen yeni bir versiyonunun (ilk hata sebebiyle uygulamaya konulan yeni arayüz), hatalı bir şekilde, Facebook mobil uygulamasının izinlerini taşıyan bir erişim jetonu oluşturduğu, bu erişim jetonunun sayfanın HTML kodunda görüntülenmekte olduğu, 3) Video yükleyicisinin “Başkasının Gözünden Gör” ekranının bir parçası olarak görüntülendiğinde, görüntüleyene ait erişim jetonu yerine görüntülediğiniz kullanıcıya ait erişim jetonunu oluşturduğu, ve bu üç hatanın bir araya gelmesi ile ilgili zafiyetin ortaya çıktığı, kişinin bir arkadaşının gözünden profilini görüntülemesini sağlayan “Başkasının Gözünden Gör” özelliğini kullanırken, uygulama kodunun kişilerin başkalarının doğum gününü kutlamalarını sağlayan kutucuğu kaldırmadığı, video yükleyicisinin yaratmaması gerekirken bir erişim jetonu yarattığı ve yaratılan erişim jetonunun kullanıcının kendisine değil görüntülenen kişiye ait olduğu,

• İlgili erişim jetonunun ise sayfanın HTML kodu üzerinden görüntülenebildiği, saldırganların bu erişim jetonunu buradan elde etmeleri, daha sonra saldırganların bu erişim jetonunu kullanarak bir diğer hesaba eriştikleri ve aynı adımları izleyerek bu hesapla ilişkili olan diğer hesapların erişim jetonlarını ele geçirdikleri,

ifadelerine yer verilmiştir.

Facebook temsilcisi tarafından gönderilen 14.10.2018 tarihli e-postada bilgilendirmenin takip eden hafta içinde yazılı olarak Kurula arz edileceğinin ifade edilmesine rağmen 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (5) numaralı fıkrasında yer alan “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir....” hükmü uyarınca Facebook tarafından Kurul’a herhangi bir bildirim yapılmamıştır. Bunun üzerine Kurul, Kanun’un 15 nci maddesinin (1) numaralı fıkrasında yer alan “Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapar.” hükmü kapsamında resen inceleme yapma kararı almıştır.

Kurul tarafından yapılan inceleme neticesinde,

1. Veri ihlalinin, Facebook sisteminin birbirinden farklı üç özelliği olan Başkasının Gözünden Gör modu, Doğum Günü Kutlayıcı ve Video Yükleyicinin etkileşimi sonucunda oluşan bir zafiyetten kaynaklandığı, bu durumun bir kullanıcının kendi profilini Başkasının Gözünden Gör modunda görüntülediğinde;

a. Gelen ekranda kullanıcının doğum gününün görünür olduğu arkadaşlarına doğum günü mesajı gönderme opsiyonunun verildiği,

b. Doğum günü mesajı gönderme opsiyonunun Video Yükleyici ile kullanıldığı takdirde, Başkasının Gözünden Gör modu için video yükleyicisinin bir erişim jetonu ürettiği,

c. Bu erişim jetonunun doğum günü mesajının gönderileceği kullanıcının arkadaşına ait olduğu,

d. Üretilen bu erişim jetonu sonucunda karşı tarafın profil bilgilerini elde etmek üzere kullanılabilirdiği,

göz önünde bulundurulduğunda, bu tip hataların test aşamasında tespit edilerek değişiklik yayına alınmadan evvel düzeltilmesi gerektiği dikkate alınarak Şirketin bahse konu veri ihlali kapsamında Kanunun 12 inci maddesinin (1) numaralı fıkrasında belirtilen teknik ve idari tedbirleri almakta kusurlu olduğu,

2. İlgili zafiyetin 21 Temmuz 2017 tarihinden 27 Eylül 2018 tarihine kadar yaklaşık 14 ay boyunca devam etmesinin gerekli denetim ve kontrollerin yapılmadığının göstergesi olduğu, bu durumun ise 6698 sayılı Kanunun 12 inci maddesinin (1) ve (3) numaralı fıkralarında belirtilen tedbirlerin alınması hususunda Facebook'un kusurlu olduğunu gösterdiği,

3. İlgili zafiyetten kaynaklı olarak ihlalin 14 - 27 Eylül 2018 tarihleri arasında 13 gün boyunca gerçekleştiği Şirket tarafından belirtilmiş olup,

a. 27 Eylül 2018 tarihinde güvenlik açığına yönelik yama geliştirildiği ancak 25 Eylül 2018 tarihinde Facebook tarafından ihlalin tespit edilmesine rağmen 2 gün boyunca ihlalin devam ettiği,

b. 28 Eylül 2018 tarihinde geçici olarak "Başkasının Gözünden Gör" özelliğinin bütünüyle devre dışı bırakıldığı, bahse konu devre dışı bırakma işleminin tespitten itibaren 3 gün sonra yapılmış olduğu,

c. Potansiyel olarak etkilendikleri belirlenen hesaplara ait erişim jetonlarının (yaklaşık 90 milyon) 27 Eylül 2018 tarihinden başlayarak 29 Eylül 2018 tarihine kadar devre dışı bırakıldığı,

d. 14 Eylül 2018 tarihinde başlamış olan olağandışı bir aktivite sonrası ihlalin tespit edilmiş olduğu, olağandışı aktivitenin olmadığı 21 Temmuz 2017 - 14 Eylül 2018 tarihleri arasında da veri ihlalinin gerçekleşmiş olabileceği

göz önüne alındığında, ihlale zamanında müdahale edilmediği ve bu konuda teknik ve idari tedbirlerin alınmasında eksikliklerin göstergesi olduğu, bu durumun ise veri sorumlusunun Kanunun 12 inci maddesinin (1) numaralı fıkrasında belirtilen teknik ve idari tedbirleri almakta kusurlu olduğunu gösterdiği,

4. İhlalinden etkilenen ve Facebook'u Türkçe olarak kullanan 280.959 kullanıcıdan;

- 133.510 kullanıcının (Grup 1) temel profil bilgilerine (isim, telefon numarası veya eposta bilgileri) ulaşıldığı,

- 143.974 kullanıcı (Grup 2) için yukarıda yer alan temel profil bilgilerine ek olarak, aşağıda yer alan bilgilere de erişilmiş olunabileceği (ilgili alanlarda kullanıcı tarafından bilgi sağlanmış olması şartıyla);

- Kullanıcı adı, Ad [profilinde kullanıcı tarafından belirlenmiş olan takma ad (eğer mevcutsa)]
- Cinsiyet [kullanıcı tarafından profilde belirlendiği üzere]
- Yerel ayarlar [kullanıcı tarafından seçilen dil]
- İlişki durumu [kullanıcı tarafından profilde belirlendiği üzere]
- Din bilgisi [kullanıcı tarafından profilde tanımlandığı üzere]
- Memleket [kullanıcı tarafından profilde belirlendiği üzere]
- Konum [yaşanılan şehir, kullanıcı tarafından profilde belirlendiği üzere]
- Doğum günü [kullanıcı tarafından profilde belirlendiği üzere]
- Cihazlar [kullanıcı tarafından Facebook'a erişmek için kullanılan cihazlar - alanlar işletim sistemi (örn. iOS) ve donanım (örn. iPhone) bilgilerini içermektedir]
- Eğitim geçmişi [kullanıcı tarafından profilde belirlendiği üzere]
- İş geçmişi [kullanıcı tarafından profilde belirlendiği üzere]
- Web sitesi [kullanıcı tarafından profilinde yer alan web sitesi alanına girilmiş olan sayfa adları]
- Kimlik doğrulama [bu, Facebook'un ilgili kullanıcının söylediği kişi olduğuna dair kuvvetli göstergelere sahip olduğunu gösteren bir işareti ifade eder]
- Kullanıcının son zamanlarda bulunduğunu bildirdiği yerlerin listesi [bu yerler gönderilerin içinde geçen yer isimlerinden belirlenmektedir (önemli bir yapı ya da bir restoran gibi) ve bir cihazdan sağlanan konum bilgisi değildir]
- Facebook'ta son zamanlarda yapılan aramalar
- Kullanıcının takip ettiği 500'e kadar başlıca hesaplar

3.475 kullanıcının (Grup 3) ise ilk iki grubun erişilen veri türlerine ilave olarak profil sayfalarındaki verilerinin de riske maruz kaldığı,

göz önünde bulundurulduğunda, Facebook kullanıcılarına ait kişisel verileri ile özel nitelikli kişisel verilerine bu zafiyeti kullanan kişiler tarafından erişilebildiği, bu durumun “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler” ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 tarihli ve 2018/10 sayılı Kararının (3) numaralı maddesine ve Kanununun 12 inci maddesinin (1) numaralı fıkrasına aykırılık teşkil ettiği,

5. İhlalden etkilenen kişilere ait çok sayıda kişisel verilerin elde edildiği dikkate alındığında, bu verilere yetkisiz bir şekilde erişenler tarafından ilgili kişiler hakkında profillemeye yapılabileceği ve bu faaliyetlerin bu kişilerin aleyhine bir sonuç oluşturabileceği,

6. Veri ihlali hakkında Facebook tarafından Kurum’a bildirim yapılmadığı,

tespit edilmiş olup, bu kapsamda

- Şirketin bahse konu veri ihlali kapsamında Kanununun 12 inci maddesi (1) numaralı fıkrasında belirtilen teknik ve idari tedbirlerde kusurunun bulunması nedeniyle, Kanununun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca Şirket hakkında 1.150.000 TL,

- Söz konusu veri ihlalinin 25 Eylül 2018 tarihinde tespit edilmesine rağmen Kanununun 12 nci maddesinin (5) numaralı fıkrası gereğince veri ihlali hakkında Kuruma bildirim yapılmadığı hususu da dikkate alınarak, Şirket hakkında Kanununun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 450.000 TL,

idari para cezası uygulanmasına,

oy birliğiyle karar verilmiştir.

2019/353 sayılı KVKK Kararı

Dernek, Vakıf Ve Sendikaların Veri Sorumluları Siciline Kayıt Yükümlülüğü İstisnası Hakkında Kişisel Verileri Koruma Kurulunun 26.11.2019 Tarihli ve 2019/353 Sayılı Karar Özeti

Karar Tarihi : 26.11.2019

Karar No : 2019/353

Konu Özeti : Vakıf ve derneklerin Sicile kayıt yükümlülüğünden istisna tutulduğu 2018/32 sayılı Kurul Kararında yer alan "... yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılara yönelik kişisel veri işleyenler" ifadesinin kapsamıyla ilgili bilgi talebi hakkında başvuru

Bilindiği üzere 6698 sayılı Kanununun 16 ncı maddesinin ikinci fıkrasında "*Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir.*" hükmü yer almaktadır.

Buna göre, genel kural olarak kişisel veri işleyen gerçek ve tüzel kişilerin Veri Sorumluları Siciline (Sicil) kayıt yükümlülüğü bulunmakla birlikte bu yükümlülüğe Kişisel Verileri Koruma Kurulu (Kurul) tarafından istisna getirilebilmektedir.

Maddenin verdiği yetkiye dayanarak Sicile kayıt yükümlülüğüne istisna getirilen veri sorumluları ile ilgili olarak alınan 2018/32 sayılı Kurul Kararınının 3 üncü maddesinde; "*04/11/2004 tarihli ve 5253 sayılı Dernekler Kanununa göre kurulmuş derneklerden, 20/02/2008 tarihli ve 5737 sayılı Vakıflar Kanununa göre kurulmuş vakıflardan ve 18/10/2012 tarihli 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununa göre kurulmuş sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılara yönelik kişisel veri işleyenler*" ifadesi yer almaktadır.

Anılan Kurul kararında yer alan "*yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılara yönelik kişisel veri işleyenler*" ifadesinde veri konusu kişi grubu sınırlı sayma yöntemiyle belirlenmiş olup bu durumda dernek ve

vakıflardan sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılara yönelik kişisel veri işleyenler Sicile kayıt yükümlülüğünden istisna kapsamında değerlendirilmiştir.

Söz konusu vakıf, dernek ve sendikaların Sicile kayıt yükümlülüğünden istisna tutulduğu 2018/32 sayılı Kurul Kararında yer alan “... yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılara yönelik kişisel veri işleyenler” ifadesinin kapsamı ile ilgili bilgi almak amacıyla Kuruma yapılan başvurunun incelenmesi neticesinde Kurul tarafından;

2018/32 sayılı Kurul Kararının 3 üncü maddesinde yer alan “04/11/2004 tarihli ve 5253 sayılı Dernekler Kanununa göre kurulmuş derneklerden, 20/02/2008 tarihli ve 5737 sayılı Vakıflar Kanununa göre kurulmuş vakıflardan ve 18/10/2012 tarihli 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununa göre kurulmuş sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılara yönelik kişisel veri işleyenler” ifadesinin, “kendisine bağış yapılanları” da kapsadığı ve bu hususun “faaliyet alanlarıyla sınırlı” ifadesine dâhil olarak yorumlanması gerektiğine,

karar verilmiştir.

2019/352 sayılı KVKK Kararı

Bir Banka Nezdinde Gerçekleşen Veri İhlali ile İlgili Olarak Kişisel Verileri Koruma Kurulunun 26/11/2019 Tarihli ve 2019/352 Sayılı Karar Özeti

Karar Tarihi : 26.11.2019

Karar No : 2019/352

Konu Özeti : Bir banka nezdinde gerçekleşen veri ihlali hakkında Karar

Bir Bankanın, Kurum kayıtlarına intikal eden Kişisel Veri İhlali Bildirim Formu ile yazısında;

- Banka personelinin iki farklı tarihte üç farklı müşterinin kritik bilgilerini (nüfus cüzdanı, bakiye, kimlik, iletişim vb. bilgileri) şahsi e-posta adresine iletildiği, ilgili müşterilerden birinin hesabından sahte belgelerle para çekildiği, somut olarak veri sızdırdığı belirlenememekle birlikte ilgili müşterilerden farklı üç başka müşterinin bilgilerinin de (nüfus cüzdanı, bakiye, kimlik, iletişim vb. bilgileri) aynı personel tarafından mesnetsiz olarak görüntülediği,
- Personelin en az 6 müşterinin verilerini Banka dışarısına çıkartarak yüksek miktartlı dolandırıcılık eylemlerine aracı olduğu ve menfaat sağlamış olmasının da kuvvetle muhtemel olduğu kanaatine ulaşıldığı,
- İhlalden etkilenen kişi sayısının 6 (altı), kayıt sayısının 24 (yirmi dört) olduğu,
- İhlalin sonucunda personelin usulsüz eylemleri nedeni ile Banka ile iş akdinin feshedildiği, personel ve olaya karışan tüm şahıslar hakkında dolandırıcılık ve zimmet suçlarından Savcılığa suç duyurusunda bulunulduğu,
- Bu kapsamda, müşterilerin hesaplarından kendi bilgileri dışında işlem gerçekleştirildiği ve müşteri zararı oluştuğu, müşterilerin tüm zararlarının Banka tarafından tazmin edildiği

belirtilmiştir.

Bankanın, Kurum kayıtlarına intikal eden veri ihlal bildiriminin incelenmesi neticesinde Kurulun 26/11/2019 tarih ve 2019/352 sayılı Kararı ile;

- Çalışanlar tarafından Banka dışına gönderilen e-postalara ilişkin Veri Sızıntısı Tespit/Önleme Sisteminin mevcut olduğunun belirtilmesine rağmen söz konusu ihlale neden olan kurumsal e-postadan kişisel veri sızıntısının olduğu ve alınan tedbirlerin bu ihlali engellemeye yeterli olmadığı,
- Bankanın teknik tedbir olarak belirttiği “Kredi Kartı numarası içeren e-postaların Banka dışına gönderilmek istenmesi durumunda, kart sayısı belirli bir adedin üzerinde ise bu e-postanın karantinaya alındığı ve gönderilemediği”, tedbirinin bu tür ihlaller konusunda kötü niyetli kişilerce kolayca aşılabilecek düzeyde olduğu,
- İhlalden etkilenen kişilerin nüfus cüzdanı, bakiye, kimlik, iletişim, kredi kartı numarası vb. bilgilerinin sızdırıldığı ve bu bilgiler aracılığıyla sahte belge hazırlanarak yüksek miktarda dolandırıcılık eylemlerine aracı olunduğu,
- Belirtilen tedbirlerin müşteri bilgisi olmadan yüksek miktarda para çekim işlemlerine ve sahte belge düzenlemeye engel teşkil etmediği,

hususları dikkate alındığında;

- 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari ve tedbirleri almayan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 70.000 TL,
- Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen “en kısa sürede” (24.01.2019 tarih ve 2019/10 sayılı Kurul kararında belirtilen 72 saatlik süre) bildirimde bulunma yükümlülüğüne uygun hareket etmeyen veri sorumlusu hakkında Kanunun 18’nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 30.000 TL

olmak üzere toplam 100.000 TL idari para cezası uygulanmasına,

karar verilmiştir.

2019/333 sayılı KVKK Kararı

Telekomünikasyon sektöründe faaliyet gösteren veri sorumlusu tarafından şikayetçiye, ad ve soyadı benzerliği olan başka bir abonesinin fatura bilgilerinin e-posta yoluyla iletilmesi hakkında Kişisel Verileri Koruma Kurulunun 07/11/2019 Tarihli ve 2019/333 Sayılı Karar Özeti

Karar Tarihi : 07.11.2019

Karar No : 2019/333

Konu Özeti : Telekomünikasyon sektöründe faaliyet gösteren veri sorumlusu tarafından şikayetçiye, ad ve soyadı benzerliği olan başka bir abonesinin fatura bilgilerinin e-posta yoluyla iletilmesi hakkında

Kurumumuza intikal eden bir şikayet başvurusunda özete;

- İlgili kişinin bir telekomünikasyon firması adına kayıtlı 05.....7 numaralı hattı için e-faturalı aboneliği kapsamında@gmail.com e-posta adresini kullandığı, 2018 yılı Ağustos ayından itibaren kendi faturaları ile birlikte isim benzerliği dolayısıyla başka bir abonenin faturalarının da tarafına e-posta ile gönderildiği,
- Kişisel verilerinin işleme sürecinde ortaya çıkan bu hatanın düzeltilmesi, kişisel verilerinin hangi amaçlarla işlendiği, yurt içi ve yurt dışında verilerinin aktarıldığı üçüncü kişiler hakkındaki bilgi taleplerini içeren e-postasını veri sorumlusuna göndererek başvuruda bulunduğu, aynı gün içinde tarafına gönderilen e-postada talebi ile ilgili olarak bir iş günü içerisinde yanıt verileceğinin ifade edilmesine rağmen herhangi bir cevap verilmediği,
- Öte yandan başvurusunun akabinde yanlış e-fatura gönderiminin tekrar gerçekleştiği belirtilerek Kanun kapsamında gereğinin yapılması talep edilmiştir.

Bu çerçevede Kurumumuz tarafından veri sorumlusunun konuya ilişkin savunması istenilmiş, alınan cevabi yazıda özetle;

- Şikayetçi ile şirketlerinin aynı isme sahip bir başka abonesinin fatura detaylarının şikayetçi kişiye iletilmesi konusuna ilişkin olarak Şirketlerinin imtiyaz sözleşmesi kapsamında mobil elektronik

haberleşme hizmeti veren bir işletme olduğu, bu kapsamda Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK) düzenlemelerine tabi olduğu,

- BTK Tüketici Hakları Yönetmeliğinin (THY) "Abone sözleşmelerinin kuruluşu ve içeriği" başlıklı 7 inci maddesinin (1) numaralı fıkrasının "İşletmecinin dönemsel ya da sürekli olarak bir hizmeti yerine getirmeyi veya mal teminini üstlendiği durumlarda tarafların birbirine uygun karşılıklı rızası ile abonelik sözleşmesi yapılır. Abonelik sözleşmeleri, elle atılan imza ve güvenli elektronik imza ile yapılabilir." şeklinde düzenlendiği, bu çerçevede Şirketlerinin aboneleri ile yaptığı Mobil Abonelik Sözleşmesi'ne göre aboneler tarafından iletilen bilgiler kapsamında hizmetlerin sunulduğu,

- Bununla birlikte THY'nin "Fatura gönderme yükümlülüğü" başlıklı 19 uncu maddesinin (1) numaralı fıkrasının "İşletmeciler, abonenin ispatlanabilir beyanı doğrultusunda; mali mevzuata uygun olarak düzenlenen faturayı posta veya elektronik posta yöntemlerinden birisini kullanarak veya asgari olarak fatura tutarı ve son ödeme tarihini içeren fatura bilgilerini kısa mesaj yöntemi ile son ödeme tarihinden önce abonelere ulaşacak şekilde ücretsiz olarak göndermekle yükümlüdür. Fatura veya fatura bilgisinin, elektronik posta veya kısa mesaj ile gönderilmesi durumunda söz konusu gönderme işlemi son ödeme tarihinden en az yedi gün önce aboneye ulaşacak şekilde ücretsiz olarak gönderilir." şeklinde düzenlendiği, bu çerçevede ilgili maddeye göre faturasını e-posta ile almak isteyen abonelerin kendi beyanları doğrultusunda ilettikleri e-posta adreslerine faturalarının elektronik ortamda gönderildiği,

- Şikayet konusuna ilişkin yapmış oldukları inceleme doğrultusunda Şikayetçi ile isim benzerliği bulunan Şirketlerinin başka bir abonesi olan kişinin Mobil Abonelik Sözleşmelerinin ayrı ayrı incelendiği ve her iki abonenin de sözleşmelerinde aynı e-posta adresini beyan ettiklerinin görüldüğü,

- Aboneleri tarafından Şirkete iletilmiş olan e-posta adreslerine faturaları, THY'nin 19 uncu maddesinin (1) numaralı fıkrası gereğince "Fatura gönderme yükümlülüğü" nün yerine getirilmesi amacıyla elektronik posta yöntemiyle iletilmiş olduğu ve Şirket tarafından mevzuata uygun hareket edildiği,

- Diğer taraftan şikayetin giderilmesi amacıyla müşteri memnuniyeti çerçevesinde ve ilgililerin iletişim bilgilerinin güncel tutulmasını teminen Şirketin abonesi olan ve aynı e-posta adresini beyan eden diğer kişi ile birçok kez iletişime geçilmeye çalışıldığı ancak hattında bulunan kısıtlama sebebi ile kendisine ilk etapta ulaşılamadığı, daha sonra devam eden aramalarda bahsi geçen kişiye bir kez ulaşılabildiği ve e-posta adresine ilişkin şikayet konusu durum aktarılarak mevzuata uygun bir şekilde güncelleme yapması gerektiği konusunda bilgi verildiği, gelinen aşamada abonenin söz

konusu güncellemeyi yapmaması ve şikayet konusu durumun devam etmesi nedeni ile konunun çözüme kavuşturulması amacıyla ilgili e-posta adresinin sistemden kaldırılarak Şikayetçiye ilgili e-postaların gitmesinin sonlandırıldığı,

• İlgili kişi tarafından yapılan başvuruya ilişkin olarak Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in "Başvuru usulü" başlıklı 5 inci maddesinin "(1) İlgili kişi, Kanununun 11 inci maddesinde belirtilen hakları kapsamında taleplerini, yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletir.

(2) Başvuruda;

a) Ad, soyad ve başvuru yazılı ise imza,

b) Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarası,

c) Tebligata esas yerleşim yeri veya iş yeri adresi,

ç) Varsa bildirme esas elektronik posta adresi, telefon ve faks numarası,

d) Talep konusu,

bulunması zorunludur.

(3) Konuya ilişkin bilgi ve belgeler başvuruya eklenir.

(4) Yazılı başvurularda, veri sorumlusuna veya temsilcisine evrakın tebliğ edildiği tarih, başvuru tarihidir.

(5) Diğer yöntemlerle yapılan başvurularda; başvurunun veri sorumlusuna ulaştığı tarih, başvuru tarihidir." şeklinde düzenlendiği,

• Şirket tarafından Kişisel Verilerin Korunması Kanununun "Veri sorumlusuna başvuru" başlıklı 13 üncü maddesinde düzenlenen yükümlülükler kapsamında hassasiyetle gereği gibi etkin, hukuka ve dürüstlük kurallarına uygun olarak işlemleri sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirlerin alındığı,

• Başvuruda Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in 5 inci maddesine uygun biçimde zorunlu olarak yer verilmesi gereken başta TC Kimlik Numarası olmak üzere tebligata esas yerleşim yeri veya işyeri adresi, varsa bildirme esas elektronik posta adresi, telefon ve faks numarası gibi kendisini doğrulamaya yarayacak olan herhangi bir bilgi vermediği ve bu çerçevede, kimlik teyidinin yapılamadığı, teknik anlamda güvenli olmaması sebebi ile e-posta ortamında cevap verilmesinin veri güvenliği açısından risk arz edeceğinin değerlendirildiği ve somut olaydaki şekilde birden fazla abonenin aynı e-posta adresini kullanabilmesinden mütevellit veri güvenliğinin

sağlanmasını teminen Kurumumuz düzenlemelerine de aykırı şekilde gerçekleştirilmiş olan bu başvuruya dönüş yapılamadığı ifadelerine yer verilmiştir.

Konuya ilişkin yapılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 07/11/2019 tarih ve 2019/333 sayılı Kararı ile;

- Veri sorumlusunun Şikayetçi ile aynı isme sahip bir başka Şirket abonesinin fatura detaylarının Şikayetçi kişiye iletilmesi konusuna ilişkin açıklamaları Kanun ve ilgili alt düzenleme hükümleri çerçevesinde değerlendirildiğinde; her iki müşteri ile yapılan Abonelik Sözleşmeleri incelendiğinde aynı e-posta adresinin iki kişi tarafından da beyan edildiği, Şikayetçinin 2013 yılına ait Abonelik Sözleşmesinin el yazısı ile doldurulduğu, diğer müşterinin 2018 yılına ait Abonelik Sözleşmesinin ise elektronik ortamda doldurulduğu, iki kişinin aynı e-posta adresini almasının teknik açıdan mümkün olmadığı, kayıt sırasında bir yazım yanlışı yapılmasının ihtimal dahilinde olduğu,
- Müşteri memnuniyeti çerçevesinde Şirketin diğer abonesi ile hangi tarihlerde iletişime geçilmeye çalışıldığı ve hangi tarihte kendisiyle görüşüldüğünün belirtilmediği, bahsi geçen müşterinin e-posta adresine ilişkin şikayet hakkındaki bilgilendirme sonrası herhangi bir güncelleme yapmaması sebebi ile şikayet konusu e-postanın hangi tarihte sistemlerinden kaldırıldığı bilgilerinin tarafımıza gönderilen cevap metninde paylaşılmadığının tespit edildiği,
- Bu çerçevede bir müşterinin abonelik kaydı oluşturulurken sistemde kayıtlı bulunan bir e-posta adresi yazıldığında bu e-postanın hali hazırda kayıtlı bir müşteri için var olduğu uyarısının kayıt yapılan sistem tarafından verilmemesi dolayısıyla veri sorumlusunun veri güvenliğine ilişkin gerekli teknik tedbirleri almadığı, sistemindeki verilerin doğru ve gerektiğinde güncel olmadığı ve müşterilerinin verilerini başka müşteriler ile paylaşabildiğinden bünyesinde barındırdığı kişisel verilerin güvenliğini sağlayamadığı kanaatine varıldığı,
- Veri sorumlusunun ilgili kişinin başvurusuna cevap vermemesi ile ilgili olarak halihazırda veri kayıt sisteminde kayıtlı olan bir abonenin Abonelik Sözleşmesi yapılması sırasında beyan ettiği e-posta adresi üzerinden yaptığı başvurusu için kimlik teyidi yapılamadığı gerekçesinin kabul edilebilir olmadığı, iki abonenin de aynı e-posta ile kayıtlı olmasından ötürü karışıklık yaşanabileceği kanaatine varılmış olsa da şikayet başvurusuna Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğe uygun başvuru koşulları hatırlatılarak verilecek bir cevap ile kimlik teyidinin vatandaşı mağdur etmeden yapılabileceğinin değerlendirildiği,

- Ayrıca kişinin yaptığı başvuruya ilişkin olarak veri sorumlusunun e-posta adresinden talebin bir iş günü içerisinde cevaplanacağına ilişkin Şikayetçiye gönderilen cevap postasının hemen altında yer verilen “Etkileşim Kanallarımız” başlıklı bölümde yer verilen e-posta adresi üzerinden ve yine daha önce veri sorumlusuna bildirilen e-posta adresi ile şikayet başvurusunda bulunduğundan ötürü veri sorumlusunun e-posta ortamından gelecek şikayet taleplerinin alınması ve cevap verilmesinin veri güvenliği açısından risk içereceğinden dolayı cevap verilmediğine ilişkin savunmasının yukarıda yer verilen bilgiler ışığında gerçekçi bir savunma niteliği taşımadığı kanaatine varıldığı,

- Veri sorumlusunun ilgili kişinin başvurusuna “Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ”e uygun olmadığı gerekçesi ile cevap verilmemesinin Tebliğin 6’ncı maddesinde yer alan hukuka uygunluk ve dürüstlük kuralı ile bağdaşmayacağı

sonucuna varılmış olup, bu kapsamda;

- Şikayetçiye, ad ve soyadı benzerliği olan başka bir abonenin fatura bilgilerinin e-posta yoluyla iletilmesinin Kanununun 12 nci maddesinin (1) numaralı fıkrasına aykırı olduğu kanaatine varılmasından ötürü, Kanununun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca veri sorumlusu hakkında 50.000 TL idari para cezası uygulanmasına,

- Bununla birlikte “Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ”in hükümlerine uyum konusunda azami dikkat ve özenin gösterilmesi ve bu karar çerçevesinde abonelerin kişisel verilerinin güvenliğine ilişkin gerekli tüm idari ve teknik tedbirlerin alınması hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2019/332 sayılı KVKK Kararı

Bir doktor tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmaksızın işlenmesi ve ilgili numaraya reklam/bilgilendirme içerikli mesaj gönderilmesi hakkında Kişisel Verileri Koruma Kurulunun 07/11/2019 Tarihli ve 2019/332 Sayılı Karar Özeti

Karar Tarihi : 07.11.2019

Karar No : 2019/332

Konu Özeti : Bir doktor tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmaksızın işlenmesi ve ilgili numaraya reklam/bilgilendirme içerikli mesaj gönderilmesine ilişkin şikayet hakkında

İlgili kişinin şahsına ait cep telefonuna açık rızası olmaksızın bir doktor tarafından bilgilendirme/reklam amaçlı mesaj gönderilmesi üzerine veri sorumlusuna yaptığı başvuruya yanıt alamaması nedeniyle Kişisel Verileri Koruma Kuruluna ilettiği şikayet başvurusunun incelenmesi neticesinde, Şikayete konu olayın değerlendirilmesi amacıyla Kişisel Verileri Koruma Kurumu'nun bilgi, belge ve savunma talep edilen yazısına da veri sorumlusu Doktor tarafından cevap verilmemesi sonucunda;

6698 sayılı Kişisel Verilerin Korunması Kanununun "Kişisel Verilerin İşlenme Şartları" başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise Kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili

kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerine yer verildiği dikkate alınarak,

İlgili kişinin veri sorumlusu Doktor hakkındaki başvurusunda yer alan iddialar ile ilgili olarak Kurulun 11/04/2019 tarihli ve 2019/98 sayılı Kararı ile başlatılan inceleme kapsamında veri sorumlusundan konuya ilişkin gerekli bilgi ve belgelerin istenilmesine ilişkin Kurumumuzun 18/06/2019 tarihli yazısının 20/06/2019 tarihinde aynı konutta bir yakınına teslim edilmesine rağmen, bugüne kadar herhangi bir cevap verilmediği de dikkate alınarak, veri sorumlusu Doktor tarafından ilgili kişinin açık rızası veya Kanunun 5 inci maddesinin (2) numaralı fıkrasında sayılan diğer işleme şartları olmaksızın cep telefonuna reklam amaçlı mesaj gönderilmesi suretiyle kişisel verilerinin işlenmesi nedeniyle adı geçen veri sorumlusu hakkında Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendi kapsamında kişisel verilerin hukuka aykırı işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almadığı kanaatine varılmasından ötürü, anılan veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 50.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2019/331 sayılı KVKK Kararı

İlgili kişi tarafından alenileştirilen kişisel verinin, alenileştirme amacı dışında işlenmesi hakkında Kişisel Verileri Koruma Kurulunun 07/11/2019 Tarihli ve 2019/331 Sayılı Karar Özeti

Karar Tarihi : 07.11.2019

Karar No : 2019/331

Konu Özeti : İlgili kişi tarafından alenileştirilen cep telefonu numarasının, bir sigorta şirketi tarafından alenileştirme amacı dışında işlenmesi hk.

İlgili kişinin bir Sigorta Şirketi (Şirket) tarafından açık rızası alınmadan sigortacılık faaliyetleri konusunda aranması hususunda Kurula yapmış olduğu şikâyet başvurusu ile ilgili olarak Şirketten alınan yazısında, Şikâyetçinin ad, soyadı ve telefon bilgisinin finansal güvence danışmanlarınca teklif araması yapılmadan önce gerçekleştirilen araştırmalar sonucunda ...uzantılı internet sitesinden bulunduğu, Şikâyetçinin taraflarınca ulaşılan ad, soyad ve telefon numarası bilgisinin belirtilen sitede halka açık bir şekilde yer aldığı şeklindeki savunmasının değerlendirilmesi sonucunda,

Şikâyetçinin kişisel verilerine kendisi tarafından daha önce alenileştirilen internet sitesinden ulaşılması halinde dahi Şirket tarafından Şikâyetçinin bu bilgilerinin internet sitesinde bulunma ve alenileştirilme amacıyla kullanılmadığı, diğer bir deyişle Şikâyetçinin mesleki yetkinliğinden faydalanmak için kendisine ulaşılmaya çalışılmadığı, aksine Şirket faaliyetlerine ilişkin randevu talebi ile Şikâyetçinin arandığı anlaşıldığından, Şirket tarafından gerçekleştirilen veri işleme faaliyetinin 6698 sayılı Kişisel Verilerin Korunması Kanununun 5 inci maddesinin (2) numaralı fıkrasının (d) bendi çerçevesinde değerlendirilemeyeceği kanaatine varılmış olup, bu kapsamda Şirketin kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almayarak Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendine aykırı davranmış olması nedeniyle Şirket hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2019/316 sayılı KVKK Kararı

Bilimsel amaçlarla kayıt altına alınan bilimsel veri niteliğindeki kan, serum ve doku örneklerinin ihmal sonucu bozulması ve sonrasında imha edilmesi hakkındaki ihbara ilişkin Kişisel Verileri Koruma Kurulunun 30/10/2019 tarihli ve 2019/316 sayılı Karar Özeti

Karar Tarihi : 30.10.2019

Karar No : 2019/316

Konu Özeti : Bilimsel amaçlarla kayıt altına alınan bilimsel veri niteliğindeki kan, serum ve doku örneklerinin ihmal sonucu bozulması ve sonrasında imha edilmesi hakkındaki ihbar

Bir hastanede çalışan doktordan alınan ihbar dilekçesinde özetle; hastanede çalıştığı dönemde idarenin önerisi ile kronik hastalıklar ile ilgili yan dal polikliniklerini kurarak hasta verilerini, poliklinik bilgisayarını ve hastane veri sistemine klinik olarak, uzmanlar ve yan asistanları ile kaydetmeye başladıkları, ayrıca hastane idaresinin bilgisinde, etik kurul onayları alınmış ve bazılarında bilimsel araştırma projelendirmelerinde projelendirilmiş olarak, hastalara ait kan, serum ve doku örneklerini de -80 derecede derin soğutucuda toplamaya başladıkları, geçici görevinin bitmesi sonucu hastaneden ayrıldıktan sonra ilgili Hastane başhekimlerine veriler hakkında bilgi verildiği, ancak bilgilendirmelere rağmen ülkemizdeki tek doku ve kan bilimsel materyallerinin olduğu -80 derece dondurucuların gözden uzak klimasız bir odaya aktarıldığı, sonrasında da erimiştir denilerek ve kıymetli doku materyallerinin bilimsel hayata tekrar kazandırılıp kazandırılmayacağına araştırılmadan tutanak altında çöpe atıldığı dolayısıyla bilimsel verilerin korunmasında ihmalkar davranıldığı ve 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinde belirtilen veri güvenliğine ilişkin yükümlülüklerin yerine getirilmediği belirtilerek Kanun kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İhbarda bulunan doktorun görev yaptığı dönemde de bundan sonraki süreçte de hasta kayıtlarının devamlılık esasına dayanılarak Gastroenteroloji Polikliniğinde tutulmaya devam edildiği ve hastaların takip ve tedavilerinin halen devam ettiği, bu hastaların Gastroenteroloji Kliniğine

başvuruda bulunan, teşhis ve tedavileri yapılmış ve halen tedavi takipleri yapılan hastalar olduğu, kayıtlarının Sağlık Bakanlığının talimatları doğrultusunda elektronik olarak tutulduğu, hasta mahremiyeti esası ile hasta bilgilerinin, takip eden doktorlar ve ailesi dışında kimse ile paylaşılmadığı,

- Buzdolaplarının 08.03.2018 tarihinde arıza verene kadar herhangi bir şekilde kullanılmadığı, arıza tutanaklarının tutulduğu, arıza esnasında Başhekimliğin bilgilendirildiği, buzdolaplarındaki materyallerin eridiğinin görüldüğü ve ilgili branşlara bu örneklerin kullanılıp kullanılmayacağı sorulduğu, bu işlemlerin de tutanak altına alındığı, bu esnada buzdolaplarının nasıl alındığının bilinmediği, Başhekimliğin bilgisinin olmadığı ve demirbaş kaydının alınmadığının görüldüğü, Başhekimliğin durumdan haberdar edilip onamları alınarak buzdolabı içindekilerin imha edildiği, Başhekimlik talimatı ile buzdolaplarının biyokimya laboratuvarına teslim edildiği,

- Örneklerin Hastane yöneticiliğinin bilgisi ve talimatı doğrultusunda imha edildiği, hasta bilgilerinin ve tarafına teslim edilen bilimsel çalışmalarda kullanılmak üzere hastalar tarafından bilgilendirilmiş onam formlarının olmaması ve örneklerin bozulmuş olması nedeniyle kimlik bilgileri ile eşleştirme yapılmasının da bilimsel bir anlamının olmadığı,

- Örneklerin arıza nedeniyle erimiş olması nedeniyle bunlarla ilgili analiz yapılmadığı, yapılsa dahi bilimsel etik kuralları gereği hasta onamları olmaması nedeniyle hükümsüz olacağı, bu örneklerin başka araştırmalarda kullanılmadığı, örneklerin hastaların tedavisini etkilemek veya değiştirmek amacıyla değil olası bilimsel çalışmalar için toplandığının tahmin edildiği, toplanan örneklerin etik kurul onayları ve belgelendirilmiş onamları ile ilgili herhangi bir devir teslim yapılmadığı

ifade edilmiştir.

Konuya ilişkin olarak yapılan incelemede Kişisel Verileri Koruma Kurulunun 30/10/2019 tarihli ve 2019/316 sayılı Kararı ile,

- “Bilimsel veri, kan ve doku bankası” olarak adlandırılan ve dilekçe ekinde yer alan doküman ve resimlerden hastalara ilişkin örnekler üzerinde çeşitli barkodların olduğunun görülmesi ile doku ve kan bankasındaki listede bu örneklerin, isim ve ependorf (tüp) sayılarına göre dolaplara yerleştirildiğinin anlaşılması nedeniyle anılan örneklerin hasta kişilerin kimliğine ulaşılmasını sağlayabilecek olmasından hareketle kişisel veri, bu verilerin belirli kriterlere göre sınıflandırılarak kayda alınması işleminin ise kişisel veri işleme faaliyeti olarak değerlendirildiği,

- Bununla birlikte, Kanunun “İstisnalar” başlıklı 28 inci maddesinin (1) numaralı fıkrasının (c) bendi uyarınca kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini,

ekonomik güvenliđi, özel hayatın gizliliđini veya kiřilik haklarını ihlal etmemek ya da suç teřkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi durumunda, bu Kanun hükümlerinin uygulanmayacağı

deđerlendirmelerinden hareketle;

- Hastalardan alınan kan, serum ve doku örneklerinin bilimsel amaçlarla kaydedildiđi Kanunun 28 inci maddesi kapsamında bu verilerin işlenmesinin millî savunmayı, millî güvenliđi, kamu güvenliđini, kamu düzenini, ekonomik güvenliđi, özel hayatın gizliliđini veya kiřilik haklarını ihlal etmediđi ya da suç teřkil etmediđi deđerlendirildiđinden řikâyet hakkında bu aşamada yapılacak bir işlem olmadığına karar verilmiştir.

2019/297 sayılı KVKK Kararı

Veri sorumlusu tarafından ilgili kişiye gönderilen reklam amaçlı SMS'ler hakkında Kişisel Verileri Koruma Kurulunun 01/10/2019 Tarihli ve 2019/297 Sayılı Karar Özeti

Karar Tarihi : 01.10:2019

Karar No : 2019/297

Konu Özeti : Veri sorumlusu tarafından ilgili kişiye gönderilen reklam amaçlı SMS'ler hakkında

Kurumumuza iletilen bir şikayet başvurusunda özetle:

- Otomotiv sanayi sektöründe faaliyet gösteren veri sorumlusu tarafından ilgili kişinin numarasına reklam içerikli SMS gönderildiği, kendisinin bu şekilde yapılan reklamlardan rahatsızlık duyduğu ve kişisel verilerinin açık rızası olmaksızın işlendiğini düşünmesi sebebiyle 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) çerçevesinde veri sorumlusuna başvurduğu veri sorumlusunun başvuruya yazılı olarak cevap verdiği, kendisinin bu cevabı yeterli bulmadığı, bu anlamda kişisel verilerinin açık rızası olmaksızın işlendiği düşünerek Kurula şikayette bulunmuştur.

Kurul tarafından eldeki bilgi ve belgeler değerlendirilerek;

- 6698 sayılı Kanununun Geçici 1 inci maddesinin (3) numaralı fıkrasında, "Bu Kanunun yayımı tarihinden önce işlenmiş olan kişisel veriler, yayımı tarihinden itibaren iki yıl içinde bu Kanun hükümlerine uygun hâle getirilir. Bu Kanun hükümlerine aykırı olduğu tespit edilen kişisel veriler derhâl silinir, yok edilir veya anonim hâle getirilir. Ancak bu Kanunun yayımı tarihinden önce hukuka uygun olarak alınmış rızalar, bir yıl içinde aksine bir irade beyanında bulunulmaması hâlinde, bu Kanuna uygun kabul edilir." hükmüne yer verildiği,

- Buna ilaveten, 15/07/2015 tarihli Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik'in Geçici 1/2 maddesinde, "Kanunun yürürlük tarihinden önce, hizmet sağlayıcı ve alıcı arasında doğrudan mal veya hizmet teminine yönelik işlemler sırasında alıcının elektronik iletişim adresini vermesi ile oluşturulan veri tabanlarının onaylı olduğu kabul edilir. Bu şekilde verildiği kabul edilen onay; acente, özel yetkili ya da bayi işletme için verilmiş ise sözleşmenin diğer tarafı için de verilmiş kabul edilir." hükmünün yer aldığı,

- Başvuruya konu olay incelendiğinde; veri sorumlusu tarafından, 2012 yılında ilgili kişinin başvurusunda belirttiği telefon numarasından Firma Merkezini arayarak motosikleti için İngilizce kullanım kılavuzu talep ettiğinin, bu talebiyle beraber şahsıyla e-posta, SMS ve telefon ile iletişime geçilmesine izin verdiğinin, ayrıca ilgili kişinin 2013 yılında motosikleti için Firmadan yedek parça ve servis hizmeti satın aldığı, bu duruma ilişkin olarak fatura cari kaydının bulunduğu görüldüğü,
- Firmanın, ilgili kişinin başvurusuna cevaben, söz konusu iddialarını tevsik etmek üzere satın alınan ürün ve hizmetin fatura bilgisini gösterir ekran görüntülerinin sunulduğunun, ilgili kişinin başvuru dilekçesinde de Firmanın iddialarının doğru olmadığına yönelik bir beyanın olmadığı,
- Açıklanan mevzuat hükümleri uyarınca, veri sorumlusu tarafından ilgili kişiye verilen cevapta belirtildiği üzere ilgili kişinin kişisel verilerinin, 2012 yılında Firma Merkezini arayarak motosikleti için İngilizce kullanım kılavuzu talep etmesi ve bu talebiyle beraber şahsıyla e-posta, SMS ve telefon ile iletişime geçilmesine izin vermesi, ayrıca ilgili kişinin 2013 yılında motosikleti için Firmadan yedek parça ve servis hizmeti satın almasına binaen işlendiğinin beyan edilmesi ve başvuru sahibince aksinin iddia edilmemesi sebebiyle, bahsi geçen satın alma işleminin Kanunun yürürlüğe girmesinden önce gerçekleştiği anlaşıldığından şikayete ilişkin 6698 sayılı Kanun kapsamında yapılacak herhangi bir işlem bulunmadığına karar verilmiştir.

2019/296 sayılı KVKK Kararı

Bir operatör şirketinin, ilgili kişinin internet sitesi üzerinden yapmış olduğu başvurusunu kimlik teyidi yapamadığı gerekçesiyle reddetmesine ilişkin olarak Kurula yapılan başvuru hakkında Kişisel Verileri Koruma Kurulunun 01/10/2019 Tarihli ve 2019/296 Sayılı Karar Özeti

Karar Tarihi : 01.10.2019

Karar No : 2019/296

Konu Özeti : Bir operatör şirketinin ilgili kişinin internet sitesi üzerinden yapmış olduğu başvurusunu kimlik teyidi yapamadığı gerekçesiyle reddetmesine ilişkin olarak Kurula yapılan başvuru hakkında

İlgili kişinin bireysel olarak faturalı telekomünikasyon ve buna bağlı hizmetler aldığı Operatör Şirketine (Şirket) internet sitesi üzerinden yapmış olduğu başvurusunun, Şirketin internet sitesinde bulunan KVKK başvuru formunun doldurularak noter aracılığıyla veya elektronik imzalı e-posta ile iletilmediğinden bahisle kimlik teyidi yapılamadığı gerekçesiyle reddedilmesi sonucu Kişisel Verileri Koruma Kuruluna ilettiği şikayet başvurusunun incelenmesi neticesinde,

Şikayete konu olayda veri sorumlusundan alınan bilgiler ışığında; Şirketin internet sitesinde yer alan Gizlilik Politikasında ilgili kişi tarafından Şirkete yapılacak başvurunun KVKK talep formunun doldurularak Şirket adresine “noter kanalı vb. yollarla” gönderilmesi gerektiği doğrultusunda bilgilendirme mahiyetinde açıklamada bulunulduğu ve söz konusu formun Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ’e (Tebliğ) uygun bir formatta sunulduğu, Şirketin yapılacak başvurularda belirtilen şekilde başvuruyu aramasının nedeni olarak kişilerin kimlik tespitinin amaçlandığı, Şirket tarafından başvuran kişi ile bilgisi talep edilenin aynı kişi olup olmadığı hususunda Tebliğ’de belirtilen yöntemlere ek bir kontrol mekanizması daha oluşturulduğu, ilgili kişinin başvurusunun Şirket tarafından belirtilen yöntem üzerinden değil Şirketin müşteri hizmetlerine elektronik ortamda yapıldığı, ilgili kişinin başvurusunu ilettiği formda ise Şirketin başvuru amacına yönelik oluşturduğu KVKK talep formunun aksine kimlik teyidini sağlayacak TC kimlik numarası, adres gibi bilgilerin istenmediği, yalnızca ad soyad, telefon, e-posta adresi gibi

bilgilerin zorunlu olarak yer aldığı ve bu sebeplerle bahsi geçen şikayet başvurusunun Tebliğ'e uygun olmadığı anlaşılmış olup,

6698 sayılı Kanun'un "Veri Sorumlusuna Başvuru" başlıklı 13'üncü maddesinin (1) numaralı fıkrasında, ilgili kişinin bu Kanun'un uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna ileceği, bu kapsamda Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in "Başvuru Usulü" başlıklı 5'inci maddesinde, ilgili kişinin Kanun'un 11'inci maddesinde belirtilen hakları kapsamında taleplerini yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna ileteceği ve Tebliğ'in 6'ncı maddesinde veri sorumlusunun bu tebliğ kapsamında yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlü tutulduğu hükümlerine yer verildiği dikkate alınarak;

- Şirketçe kimlik teyidi sağlamak amacıyla yalnızca noter kanalı veyahut e-imza ile başvuruda bulunabileceğinin bildirilmesi sonucu Kanun'da ya da Tebliğ'de öngörülmeven maddi bir külfet getirilmesinin ve ilgili kişinin bu şekilde yanlış yönlendirilmesi suretiyle söz konusu KVKK talep formunu doldurarak usule uygun bir başvuru yapma hakkının engellenmesinin Tebliğ'in 6'ncı maddesinde sayılan hukuka uygunluk ve dürüstlük kuralı ile bağdaşmayacağı dikkate alındığında, Tebliğ hükümlerine uyum konusunda azami dikkat ve özenin gösterilmesi hususunda Şirketin talimatlandırılmasına,

- İlgili kişiye ise 6698 sayılı Kanun'un 11'inci maddesi kapsamında ilgili kişinin hakları ile Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in ilgili maddelerinin hatırlatılmasına karar verilmiştir.

2019/294 sayılı KVKK Kararı

Bir havayolu taşımacılık şirketinin (veri sorumlusu) sunduğu sadakat programını kullanan ilgili kişinin kullanıcı adı ve parola bilgilerini değiştirme talebi karşısında ilgili kişiden arkalı önlü kimlik görüntüsü talep eden veri sorumlusu hakkında Kişisel Verileri Koruma Kurulunun 01.10.2019 Tarihli ve 2019/294 sayılı Karar Özeti

Karar Tarihi : 01.10.2019

Karar No : 2019/294

Konu Özeti : Bir havayolu taşımacılık şirketinin (veri sorumlusu) sunduğu sadakat programını kullanan ilgili kişinin kullanıcı adı ve parola bilgilerini değiştirme talebi karşısında ilgili kişiden arkalı önlü kimlik görüntüsü talep eden, ilgili kişinin kimlik görüntülerinin silinmesi talebine ise verilerin sistemlerinde tutulmadığı ve üçüncü kişilerle paylaşılmadığı yanıtını veren veri sorumlusu hakkında yapılan şikayet hk.

Bir havayolu taşımacılık şirketinin (veri sorumlusu) sunmuş olduğu sadakat programını kullanırken kullanıcı adı ve parola bilgilerini değiştirme talebiyle veri sorumlusuna başvuran ilgili kişiye, arkalı önlü kimlik görüntüsünü iletmesi halinde talebinin yerine getirileceği cevabının verilmesi, o sırada bilet bilgilerine erişmek için kimlik görüntüsünü elektronik olarak ileten, ancak daha sonra veri sorumlusuna başvurmak suretiyle kimlik görüntülerinin silinmesi ve kişisel verileri üçüncü kişilere aktarıldıysa, verilerin aktarılan üçüncü kişilerin kayıtlarından da silinmesi talebine kişisel verilerinin sistemlerinde tutulmadığı ve üçüncü kişilerle paylaşılmadığı yanıtını alan ilgili kişinin Kuruma yaptığı başvurunun incelenmesi neticesinde,

- İlgili kişinin kimlik görüntüsünde yer alan bilgilerin “kan grubu” ve “din” bilgilerini de içermesi nedeniyle arkalı önlü kimlik görüntüsünde yer alan verilerin özel nitelikli kişisel veri niteliğinde olduğu, bu nedenle Kanunun 5 inci ve 6 ncı maddelerinde düzenlenen hükümlerin birlikte dikkate alınması gerektiği, söz konusu verilerin özel nitelikli verileri de ihtiva etmesi nedeniyle ilgili kişinin açık rızası olmadan gerçekleştirilen veri işleme faaliyetinin hukuka aykırı bir işleme olduğu,
- Başvuruya konu olay Genel İlkeler bakımından değerlendirildiğinde,

- Arkalı önlü kimlik görüntüsünün işlenmesinin, Kanununun 5 inci ve 6 ncı maddeleri kapsamında kişisel verilerin işleme şartlarına uygun olmayan bir işleme faaliyeti olduğu değerlendirildiğinden, hukuka uygunluk ilkesine aykırı olduğu; öte yandan veri sorumlusunun kimlik görüntüsünün muhafaza edilmesine rağmen kayıt altına alınmadığı yönünde ilgili kişiye cevap vermesinden dolayı şeffaf olmadığı, bu nedenlerle de dürüstlük kuralına aykırı veri işleme faaliyetinde bulunduğu,
 - Veri sorumlusunun kimlik görüntülerini işlemede hangi hukuki işleme şartına dayandığı hususunun ilgili kişiye verilen cevaptave kurumumuza intikal eden yazıda belirtilmediği, bu nedenle veri sorumlusunun veri işleme faaliyetinin belirli, açık ve meşru amaçlar için işleme ilkesine aykırı olduğu,
 - Kimlik doğrulama işlemi için daha az verinin işlenmesinin mümkün olduğundan hareketle veri sorumlusunun somut olayda işlediği kimlik görüntüsünün işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırı olduğu,
 - Veri sorumlusunun kimlik görüntüsünü işlediği gibi, kimlik doğrulama işlemi bittikten sonra bu verileri silmediği, Kurumumuzca bilgi belge talep edilmesi üzerine sildiğini beyan ettiği gerçeğinden yola çıkarak, veri sorumlusunun veri işleme faaliyetinin ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesine de aykırı olduğu,
- İlgili kişinin, amacın ortadan kalktığı gerekçesi ile kişisel verilerini içeren nüfus cüzdanı görüntüsünün silinmesi veya yok edilmesi ile kişisel verilerinin silinmesi veya yok edilmesi işlemlerinin kişisel verilerinin aktarıldığı üçüncü kişilere de bildirilmesini talep ettiği, veri sorumlusunun ise güvenlik sebebi ile alınan kimlik kartı, pasaport ya da kimlik görüntüsü gibi bilgilerin kayıt altına alınmadığı ve üçüncü kişiler ile paylaşılmadığı şeklinde elektronik posta vasıtasıyla yanıt verdiği, ancak daha sonra Kurumumuzun bilgi ve belge talep etmesi üzerine veri sorumlusu tarafından yapılan incelemede ilgili kişi ile iletişim halinde olan çağrı merkezi ekibi tarafından ilgili kişinin ilk başvurusu işleme alınırken kimlik doğrulama sürecinin Şirket kurallarına uygun olarak yürütülmediği, kimlik görüntülerinin alınmasına dair şikayetin içeriğinin doğru tahlil edilemediği, ilgili kişinin, kimlik görüntülerinin kaydedilmediği ve üçüncü kişilerle paylaşılmadığı şeklinde hatalı bilgilendirildiği ve yazılı çalışma kurallarının aksine talep değerlendirme, görüş ve destek birimlerinin yeterli bilgisi olmadan şikayetlerin yanıtladığının tespit edildiği, ilgili kişinin iletmış olduğu kimlik görüntülerinin şikayet modülü yazılım firmasının sunucuları üzerinde bulundurulduğu, kimlik görüntülerinin silinmediğinin tespit edildiği, dolayısıyla inceleme neticesinde işlem yapan çağrı merkezi personelinin başvuru sahibi ilgili kişiyi kişisel verilerinin

saklandığı yerler ve paylaşıldığı üçüncü kişiler hakkında yanlış bilgilendirdiğinin ve bilgi eksikliği nedeniyle verilerinin silinmesine ve veri işleyenleri öğrenmeye yönelik taleplerini işleme almadığının tespit edildiğinin belirtildiği, bu nedenle veri sorumlusunun, ilgili kişinin veri sorumlusuna başvuru hakkına riayet etmediği, diğer bir deyişle, veri sorumlusunun ilgili kişinin başvurusuna hukuka ve dürüstlük kuralına uygun bir yanıt vermediği,

- Diğer yandan, veri sorumlusunun, Kanun kapsamındaki başvurusuna cevap verebilmek amacıyla ilgili kişinin kimliğinin teyidi noktasında ek bilgi istemesinin yerinde olduğu değerlendirilmekle birlikte, ilgili kişinin din ve kan grubu gibi özel nitelikli kişisel verilerini de içeren arkalı önlü kimlik görüntüsünün talep edilmesinin, Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinde düzenlenen “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkesine uygun olmadığı gibi, Kanunun özel nitelikli kişisel verilerin işlenmesini düzenleyen 6 ncı maddesine de uygun olmadığı, zira veri sorumlusunun da yapığı savunmada, somut olayda çağrı merkezi ekibi tarafından yazılı çalışma kurallarına aykırı şekilde kimlik belgesi talep edildiğini belirterek, olaya ilişkin ikrarda bulunduğu,

- Yukarıda açıklandığı üzere somut olayda işlenen kimlik görüntüsüne yönelik olarak ilgili kişinin açık rızasının alınmadığı, açık rızanın aranmadığı diğer hallerin bulunmadığı, genel ilkelere uyulmadığı ve ilgili kişinin haklarına riayet edilmediği gerekçesiyle veri işleme faaliyetinin hukuka aykırı olduğu, bu çerçevede kişisel verilerin hukuka aykırı işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olan veri sorumlusunun veri güvenliğine ilişkin yükümlülüğüne aykırı davrandığı

tespit edilmiş olup, bu itibarla,

- Kanunun 12 inci maddesinin (1) numaralı fıkrasında yer alan veri güvenliğine ilişkin yükümlülükleri yerine getirmediği değerlendirilen Veri Sorumlusu hakkında Kanunun 18 inci maddesinin 1 numaralı fıkrasının (b) bendi uyarınca 100.000 TL idari para cezası uygulanmasına,

- Veri sorumlusunun Kurumumuza iletteği yazıda, kişisel verilerinin silindiği hususunda ilgili kişinin bilgilendirileceğini belirtmiş olmasına rağmen, inceleme sürecinde bu bilgilendirmenin yapıldığına dair taraflardan gelen herhangi bir bildirim olmadığı dikkate alındığında, ilgili kişinin kimlik görüntüsünü içeren kişisel ve özel nitelikli kişisel verilerinin veri sorumlusu ve veri işleyenlerin sistemlerinden silindiği bilgisinin ilgili kişiye bildirilerek Kurumumuza bilgi verilmesi, önceden bildirildi ise bunu tevsik edecek bilgi ve belgelerin Kurumumuza iletilmesi konusunda veri sorumlusunun talimatlandırılmasına,

- Kişisel verileri işlenen müşterilerin bundan sonraki taleplerinde benzer karışıklıklara meydan vermemek amacıyla, sadakat kart uygulaması ve diğer hizmetlerin sunulması sürecinde kendi adına veya bir başkası adına kişisel verilere ilişkin talepte bulunan kişilerin kimliklerinin teyit edilmesi noktasında uygulanacak yöntem ve bu durumda işlenecek kişisel verilere ilişkin kurumsal düzenlemeleri Kanun kapsamında gözden geçirerek, ilgili birimleri ile veri işleyenleri bilgilendirmesi hususunda veri sorumlusunun talimatlandırılmasına, karar verilmiştir.

2019/273 sayılı KVKK Kararı

Ölü kişilerin verilerine yakınlarının erişim talebi hakkında Kişisel Verileri Koruma Kurulunun 18/09/2019 Tarihli ve 2019/273 Sayılı Karar Özeti

Karar Tarihi : 18.09.2019

Karar No : 2019/273

Konu Özeti : Ölü kişilerin verilerine yakınlarının erişim talebi hakkında

Ölü bir kişinin eşinin Kurumumuza yaptığı başvurusunda özetle;

- 2018 yılında vefat eden eşinin yasal mirasçısı olarak eşinin İstanbul'da tedavi görmüş olduğu Klinikten tüm medikal ve diğer bilgilerini talep ettiğini, bu talebini içeren bir mektubu taahhütlü posta ile bahse konu Kliniğe ilettiğini, postanın karşı tarafça alındığını, ancak kendisine bir yanıt verilmediğini,
- Bunun üzerine bahse konu taleplerini içeren bir epostayı Kliniğin elektronik ortamdaki adresine ilettiğini ve yanıt olarak resmi olmayan yollarla kendisi ile veri paylaşamayacağını iletilmesini ifade ederek, eşinin başvurusunda yer alan verilerine erişim talebinde bulunmuştur.

Konuya ilişkin yapılan değerlendirme neticesinde Kişisel Verileri Koruma Kurulunun 18/09/2019 tarih ve 2019/273 sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 3 üncü maddesinde ilgili kişinin "kişisel verileri işlenen gerçek kişi" olarak tanımlandığı,
- 4721 sayılı Türk Medeni Kanununun 28 inci maddesinde ise kişiliğin, çocuğun sağ olarak tamamıyla doğduğu anda başladığı ve ölümle sona erdiği hükmünün yer aldığı,
- Kanunun 11. maddesine göre ilgili kişinin kendisi ile ilgili kişisel veriler hakkında bilgi talep edebileceği,

hususları bir bütün olarak değerlendirildiğinde; talep edilen kişisel verilerin talep eden gerçek kişiye ilişkin olmaması ve ölmüş kişiye ait olması sebebiyle talebin, Kanunun 11. maddesi kapsamında bir talep olarak değerlendirilmeyeceği, kanısına varıldığından bu hususta 6698 sayılı Kanunun kapsamında yapılacak bir işlemin olmadığına

karar verilmiştir.

2019/265 sayılı KVKK Kararı

"VERBİS Kayıt Sürelerinin Uzatılması" hakkında 03/09/2019 tarihli ve 2019/265 sayılı Kurul Kararı

Karar Tarihi : 03.09.2019

Karar No : 2019/265

Konu Özeti : VERBİS Kayıt Sürelerinin Uzatılması

Türkiye Odalar ve Borsalar Birliği (TOBB) ile muhtelif sektör temsilcileri tarafından Kuruma intikal ettirilen Veri Sorumluları Siciline (Sicil) kayıt sürelerinin uzatılmasına ilişkin taleplerin değerlendirilmesi neticesinde;

- Yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları ile yurtdışında yerleşik gerçek ve tüzel kişi veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.12.2019 tarihine kadar uzatılmasına,
- Bu kararın Kurum internet sayfasında duyurulması ve Resmî Gazete'de yayımlanmasına oybirliği ile karar verilmiştir.

2019/255 sayılı KVKK Kararı

Bir turizm şirketi hakkında Kişisel Verileri Koruma Kurulunun 27.08.2019 tarih ve 2019/255 sayılı Karar Özeti

Karar Tarihi : 27.08.2019

Karar No : 2019/255

Konu Özeti : Bir turizm şirketinin veri ihlali hakkında Karar

Şirket tarafından Kurumumuza iletilen bildirim incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 27.08.2019 tarih ve 2019/255 sayılı Kararı ile;

- Şirket yetkilileri ve bilgi işlem uzmanlarının incelemeleri neticesinde Şirketin Local Area Network (LAN-Yerel Alan Ağı) üzerinden, ilgili şifrelerin ele geçirilmesi yoluyla yetkisiz şifre girişi ile siber saldırı yapıldığı ve söz konusu olayın Şirketin Genel alanlarda bulunan bir çalışan bilgisayarından üzerinden çalışan ağına sızılarak gerçekleştirilmesi şeklinde olduğu,

- Etkilenen kişisel verilerin;

Personel Verileri: Ad, soyad, TC kimlik numarası, doğum tarihi, medeni durum, eş çalışma bilgisi, çocuk sayısı, anne adı, baba adı, adresi, GSM numarası, banka hesap bilgileri

Müşteri Verileri: Ülke/eyalet, uyruk, doğum tarihi(DB-Veri tabanı seviyesinde şifreli), ad, soyad, telefon numarası, eposta adresi, mektup adresi, kredi kart numarası ve son kullanım tarihi(DB-Veri tabanı seviyesinde şifreli), firma ise vergi numarası, TC/Pasaport No(DB-Veri tabanı seviyesinde şifreli), cinsiyet

olduğu,

- Etkilenen kişisel veriler arasında özel nitelikli kişisel veri bulunmadığı,
- Genel alanlarda bulunan bir çalışan bilgisayarına Şirket çalışanı olmayan yetkisiz 3. kişilerce erişilebilmesinin idari bir tedbirsizlik olduğu,
- Genel alanlarda bulunan, sunuculara erişimi olan çalışan network bağlantılarının ihlal gerçekleşikten sonra kapatıldığı ve bu hususun da sunucu güvenliği noktasında bir aksaklık teşkil ettiği,

- Güvenlik duvarının ihlal gerçekleştiikten sonra yenilenmesinin sađlandıđı ve güvenlik duvarının güncel durumda bulunmamasının teknik bir eksiklik olduđu,
- Çalışanların ihlal gerçekleştiikten sonra güvenlik eğitiminin sađlandıđı ve daha önce böyle bir eğitim almadıkları anlaşılmiş olup bu durumun da kişisel veri güvenliđi sađlanması ve farkındalıđı noktasında idari bir eksikliđin göstergesi olduđu,
- İhlali gerçekleştiren kişinin önce Şirket içindeki sunuculara erişim sađladıđı, daha sonra dikkat çekmemek için Şirketten ayrıldıđı ve bir sunucuya yüklediđi uzaktan erişim yazılımı ile işlemlerini gerçekleştirdiđi,
- Bilişim ađlarında sızma veya olmaması gereken bir hareket olup olmadıđının Şirket IT sistemleri tarafından fark edilmemesinin teknik bir eksiklik olduđu, - Sunucu üzerindeki verilerin geri getirilemez şekilde ihlali gerçekleştiren kişi tarafından yok edildiđi,
- Söz konusu olayın Bilgi İşlem Birimine Şirketin diđer birimlerinde çalışanlar tarafından bildirilmesinin Şirketin Bilgi İşlem Biriminin ve Bilgi Sistemlerinin düzgün olarak çalışmadıđı ve işlemediđinin bir göstergesi olduđu

dikkate alınarak;

6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrasında yer alan “..veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sađlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.” hükmü ile, (3) numaralı fıkrasında yer alan “Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sađlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.” hükmü çerçevesinde veri güvenliđini sađlamaya yönelik gerekli teknik ve idari ve tedbirleri almayan Şirket hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 400.000 TL idari para cezası uygulanmasına,

Şirket tarafından tespit edilen ihlale ilişkin ilgili kişilere bildirim yapılmadıđı ve Kuruma yapılan bildirim Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen “en kısa sürede” bildirimde bulunma yükümlülüđüne aykırılık teşkil etmesi nedeniyle Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL idari para cezası uygulanmasına

karar verilmiştir.

2019/254 sayılı KVKK Kararı

S Şans Oyunları A.Ş hakkında Kişisel Verileri Koruma Kurulunun 27.08.2019 tarih ve 2019/254 sayılı Karar Özeti

Karar Tarihi : 27.08.2019

Karar No : 2019/254

Konu Özeti : S Şans Oyunları A.Ş.'nin veri ihlali hakkında Karar

S Şans Oyunları Şirket'inin Kurum kayıtlarına 17.09.2018, 27.09.2018, 11.10.2018 ve 02.05.2019 tarihlerinde giren yazılarda özetle;

- S Şans Oyunları A.Ş.'nin Spor Toto Teşkilat Başkanlığı'ndan almış olduğu izin doğrultusunda sanal bayi olarak www.tuttur.com alan adlı web sitesinde faaliyet gösterdiği,
 - Veri sızıntısından, şirketin üyelerinden birinin, 14.09.2018 tarihinde taraflarına ulaşarak bazı kullanıcılara ait telefon numaralarının ve şifrelerini kaybetmeleri durumunda SMS firması tarafından yollanan üye numaralarının yer aldığı bir Excel listesinin internet ortamındaki illegal sitelerde dolaştığı bilgisini paylaşmasıyla haberdar oldukları,
 - Veri ihlalinin gerçekleşme tarihinin bilinmediği,
 - İhlalden etkilenen kişi sayısının belirlenmediği,
 - İhlalden etkilenen ilgili kişi gruplarının şirket üyeleri/müşteriler olduğu,
 - İhlalden etkilenen kişisel veri kategorilerinin kullanıcıların ad ve soyadları ile cep telefonu numaraları olduğu,
 - Söz konusu listede yer alan SMS'lerin incelenmesinde ise 2015 Mart ile 2017 Ocak tarihleri arasında sistemden gönderilen kısa mesajlar olduğunun tespit edildiği
- ifadelerine yer verilmiştir.

Söz konusu bildirim incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 27.08.2019 tarih ve 2019/254 sayılı Kararı ile;

- İhlalin gerçekleşme tarihinin belirlenememesinin, veri sorumlusunun gerekli gözetim, denetim ve kontrolleri yapmadığının göstergesi olduğu,
- İhlale konu olan Excel listesinde yer alan verilerin ne zaman sistemden çekildiği ve ne zaman veri işleyene aktarıldığının tespit edilememesinin teknik ve idari bir kusur olduğu,
- Listede yer alan üyelerin %90'ının sisteme hiç giriş yapmadığının Şirket tarafından beyan edilmiş olmasına rağmen ihlalden etkilenen kişi sayısının tespit edilememesinin teknik ve idari tedbirlerin tam olarak alınmadığının veya uygulanamadığının göstergesi olduğu,
- Şirketin veri ihlaliyle alakalı olarak ilgili kişilere bildirim yapma hususunda faaliyete geçemediği, bu durumun idari tedbirlerin tam olarak alınmadığının veya uygulanamadığının göstergesi olduğu, Şirket tarafından ihlalin tespit edilememesi, veri sorumlusunun beyanında olduğu üzere ihlalin veri işleyen nezdinde gerçekleşme ihtimali olsa dahi veri sorumlusu açısından Kanun hükümleri çerçevesinde gerekli her türlü teknik ve idari tedbirleri alma konusunda yükümlülüklerini ortadan kaldırmadığı dikkate alındığında , 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (1) numaralı fıkrasında ifade edilen teknik ve idari ve tedbirleri almayan Şirket hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 150.000 TL idari para cezası uygulanmasına,

Kanunun 12 nci maddesinin (5) numaralı fıkrası kapsamında ilgili kişilere bildirim yapılmaması sebebiyle adı geçen Şirket hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 30.000 TL idari para cezası uygulanmasına,

karar verilmiştir.

2019/227 sayılı KVKK Kararı

Bir bankanın, ilgili kişinin cep telefonu numarasını bankaya verilmiş amacı dışında kullanması hakkında Kişisel Verileri Koruma Kurulunun 18/09/2019 Tarihli ve 2019/227 Sayılı Karar Özeti

Karar Tarihi : 18.09.2019

Karar No : 2019/277

Konu Özeti : İlgili kişinin, kişisel verisi olan cep telefonu numarasının bir banka tarafından verilmiş amacı dışında kullanılması hakkında

Şikâyetçinin bir banka çalışanının kendisini arayarak eşinin müdürü olduğu Şirket ile ilgili olarak eşine ulaşamadığını ve eşiyile iletişime geçebilmesi konusunda kendisine yardımcı olmasını talep ettiği, bunun üzerine müşterisi olarak Bankaya kendisiyle ilgili işlemlerde kullanılması için vermiş olduğu iletişim bilgilerine amacı dışında nasıl ve neden ulaşıldığı hakkında bilgi almak için Bankaya başvuru yaptığı ve Bankanın kendisine yazılı bir cevap vermediği iddiasıyla yapılan başvurusunun incelenmesi sonucunda;

Şikâyetçinin talebini Bankaya e-posta yoluyla ilettiği ancak Bankadan cevap verilmediği yönündeki iddiası ile ilgili olarak Bankanın Şikâyetçinin e-posta adresine mesaj gönderdiği ve gönderilen mesajda "... paylaşımınız hakkında detaylı bilgilendirme yapabilmek amacıyla iletişim numaranız üzerinden size ulaşmayı denedik ancak yanıt alamadık. İşleminiz ile ilgili detayları ...Hizmet Hattı'nı arayarak öğrenebilirsiniz..." ifadelerine yer verilerek şikâyetçinin bilgilendirilmesi yoluna gidildiği görülmüştür.

Bu çerçevede;

- Banka tarafından, Şikâyetçiye gönderilen e-posta mesajında başvurusuna ilişkin detayları Banka Hizmet Hattını arayarak öğrenebileceğine dair bilgilendirme yoluna gidilmesinin, veri sorumlusunca Şikâyetçiye başvurusunda talep ettiği hususları açıklayıcı nitelikte yazılı veya elektronik ortamda bir cevap olarak değerlendirilemeyeceği kanaatine ulaşılmış olduğundan, Şikâyetçinin başvurusuna Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ hükümlerine uygun cevap verilmemiş olması nedeniyle Bankaya Kanun ve Tebliğ hükümlerine uyum hususunda azami dikkat ve özenin gösterilmesi konusunda hatırlatmada bulunulmasına,,

- Şikâyetçinin müşterisi olduğu Bankaya kendisine ait iş ve işlemlerde ulaşılması adına vermiş olduğu telefon numarası bilgisinin, eşine ulaşılmasında yardımcı olunabilmesi adına işlenmesinin, 6698 sayılı Kanununun 4 üncü maddesinin (2) numaralı fıkrasının (c) ve (ç) bentlerinde yer alan kişisel verilerin işlenmesinde “belirli, açık ve meşru amaçlar için işleme ve işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkelerine uyulması zorunluluğuna aykırı olduğu ve bu çerçevede Kanununun 12 nci maddesinin birinci fıkrasının (a) bendi uyarınca veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almadığını göstermesi nedeniyle Banka hakkında Kanununun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL idari para cezası uygulanmasına karar verilmiştir.

2019/225 sayılı KVKK Kararı

Yurtdışında yerleşik Tüzel kişilerin Türkiye'deki Şubeleri ile İrtibat Bürolarının Sicile Kayıt Yükümlülüğü Hakkındaki Görüş Talebi ile ilgili Kişisel Verileri Koruma Kurulunun 23/07/2019 tarih ve 2019/225 sayılı Kararı

Karar Tarihi : 23.07.2019

Karar No : 2019/225

Konu Özeti : Yurtdışında Yerleşik Tüzel Kişilerin Türkiye'deki Şubeleri ile İrtibat Bürolarının Veri Sorumlusu Sifatını Taşıyıp Taşımayacağı ve Sicile Kayıt

Kurumumuza iletilen; yurtdışında yerleşik tüzel kişilerin Türkiye'de işlemekte oldukları kişisel veriler nedeniyle;

- yurtdışında yerleşik tüzel kişiler,
- yurtdışında yerleşik tüzel kişilerin Türkiye'deki şubeleri ve
- yurtdışında yerleşik tüzel kişilerin Türkiye'deki irtibat bürolarının

6698 sayılı Kanuna göre veri sorumlusu sıfatına haiz olup olmayacağı, Sicile kayıt yükümlülüğü ve istisna kriterleri açısından değerlendirilmesi konusundaki görüş talebinin incelenmesi neticesinde;

Yurtdışında yerleşik tüzel kişiler açısından;

6698 sayılı Kişisel Verilerin Korunması Kanununda (Kanun) veri sorumlusu, "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi" olarak tanımlanmış olup bunlar gerçek kişiler olabileceği gibi kamu kurumları, şirketler, dernekler veya vakıflar gibi tüzel kişiler de olabilecektir.

Bu kapsamda bir kişisel veri işleme etkinliğinde veri sorumlusunun tespiti için veri sorumlusu tanımında yer alan kişisel verilerin işleme amaçlarını ve vasıtalarını belirleme, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olma ve ayrı bir gerçek veya tüzel kişi olma kriterleriyle birlikte, kişisel verilerin ilk aşamada elde edilmesi ve bunun yasal dayanağı, hangi kişisel verilerin hangi amaçla işleneceği ve kişisel veri elde etme yöntemleri, işlenecek kişisel veri türleri, kimlerin kişisel verilerinin işleneceği, ilgili kişinin erişimi ve diğer hakların kullanılıp kullanılmadığı, kişisel

verilerin paylaşılıp paylaşılmayacağı, paylaşılacaksa kimlerle paylaşılacağı ve kişisel verilerin ne kadar süre muhafaza edileceği gibi hususlarda kimin karar verdiği dikkate alınabilecektir.

Bunlara ek olarak, merkez şirketten bağımsız olarak tabi olunan hukuki yükümlülükler, merkezden bağımsız olarak doğrudan kişisel verileri işlenen kişilere uygulanan kendi hüküm ve şartlarının mevcudiyeti gibi unsurlar da veri sorumlusunu belirlemek bakımından önem arz etmektedir.

Bununla birlikte ifade etmek gerekir ki, yurt içinde ve yurt dışında faaliyet gösteren ticari işletmeler, Türkiye'deki iş ilişkilerini yürütmek açısından çeşitli seçeneklere sahiptir. Bu seçeneklerden birisi şube açmak, diğeri de irtibat bürosu kurmaktır.

Bu açıdan ilgili seçenekler değerlendirilirken faaliyet çerçevesinin belirlenmesi önem taşımaktadır. Uygulamada genellikle, şirketler yürüttükleri faaliyetlerin kapsamı arttıkça işlerini merkezden yönetmek yerine, kuracakları yarı bağımsız birimler yani şubeler aracılığı ile mahallinden yönetmeyi tercih etmektedirler.

Yurtdışında yerleşik tüzel kişilerin Türkiye'deki şubeleri açısından;

6102 sayılı Türk Ticaret Kanununun (TTK) "Tescil" başlıklı 40 ıncı maddesinin üçüncü fıkrasında "Merkezi Türkiye'de bulunan ticari işletmelerin şubeleri de buldukları yerin ticaret siciline tescil ve ilan olunur. Ticaret unvanına ve imza örneklerine ilişkin birinci ve ikinci fıkra hükümleri bu işletmelere de uygulanır. Kanunda aksine hüküm bulunmadıkça merkezin bağlı olduğu sicile geçirilen kayıtlar şubenin bağlı bulunduğu sicile de tescil olunur. Ancak, bu hususta şubenin bulunduğu yer sicil müdürlüğünün ayrı bir inceleme zorunluluğu yoktur." hükmü, 4 üncü fıkrasında ise "Merkezleri Türkiye dışında bulunan ticari işletmelerin Türkiye'deki şubeleri, kendi ülkelerinin kanunlarının ticaret unvanına ilişkin hükümleri saklı kalmak şartıyla, yerli ticari işletmeler gibi tescil olunur. Bu şubeler için yerleşim yeri Türkiye'de bulunan tam yetkili bir ticari mümessil atanır. Ticari işletmenin birden çok şubesi varsa, ilk şubenin tescilinden sonra açılacak şubeler yerli ticari işletmelerin şubeleri gibi tescil olunur" hükmü yer almaktadır.

5174 Sayılı Türkiye Odalar ve Borsalar Birliği ile Odalar ve Borsalar Kanununun 9 uncu maddesinin 2 nci fıkrasında ise "Bir merkeze bağlı olduğu halde, ister merkezin bulunduğu odanın, ister başka odanın çalışma alanı içinde olan müstakil sermayesi ve müstakil muhasebesi bulunan ve/veya muhasebesi merkezde tutulduğu ve müstakil sermayesi bulunmadığı halde kendi başına sınaî faaliyet ve ticarî muamele yapan yerler ve satış mağazaları bu Kanunun uygulanması bakımından şube sayılır" denilerek odalara kayıt zorunluluğunun kapsamı belirlenirken şubenin tanımına da yer verilmiştir.

5411 sayılı Bankacılık Kanununun 3 üncü maddesine göre de şube; “elektronik işlem cihazlarından ibaret birimleri hariç olmak üzere, bankaların bağımlı bir parçasını oluşturan ve bu kuruluşların faaliyetlerinin tamamını veya bir kısmını kendi başına yapan, sabit ya da seyyar bürolar gibi her türlü iş yeri” olarak ifade edilmiştir.

Ticaret Sicili Yönetmeliğinin 118 inci maddesinin 1 inci fıkrasında ise şube, “bir ticari işletmeye bağlı olup ister merkezinin bulunduğu sicil çevresi içerisinde isterse başka bir sicil çevresinde olsun, bağımsız sermayesi veya muhasebesi bulunup bulunmadığına bakılmaksızın kendi başına sınai veya ticari faaliyetin yürütüldüğü yerler ve satış mağazaları” olarak tanımlanmıştır.

Bu çerçevede, bir yerin şube sayılabilmesi için merkeze bağımlı olma, dış ilişkilerde bağımsızlık, yer ve yönetim ayrılığı gibi kriterlere de bakmak gerekir.

Merkeze bağımlı olmak, şubenin merkeze ticari bir işletmenin parçası olarak bağlı olması anlamına gelmekte olup şube ile merkezin aynı gerçek veya tüzel kişiye ait olması gerekir. Bu bağımlılık nedeniyle şubenin, merkezden ayrı bir işletme politikası olamaz, şubenin kâr ve zararı merkeze aittir. Şube aracılığıyla elde edilen hakların, üstlenilen borçların sahibi de şube değil merkezdir. Ayrıca şube, ancak merkez nam ve hesabına üçüncü kişilerle iş ve işlem yaptığından şube tarafından yürütülen faaliyetten doğan hak ve yükümlülüklerin muhatabı da merkez, bir diğer ifade ile işletme sahibi olmaktadır. Bu bağlamda, merkez ile şube iktisadi bir bütün oluşturarak ortak bir işletme politikası yürütmektedir.

Dış ilişkide bağımsızlık, şubenin merkezin yaptığı işlemler türünden işlemleri üçüncü kişilerle kendi başına yapma yetkisine sahip olmasını ifade etmektedir. Yer ayrılığı ilkesine göre, şube ticari işletmenin genişleyen faaliyetlerinin mahallinden daha kolay biçimde yürütülmesi amacıyla açıldığında merkez ile şube arasında kural olarak yer ayrılığı olmalıdır. Ancak bu hususu çok dar ve kesin biçimde yorumlamamak gerekir.

Yönetim ayrılığı ise, şubenin kendi başına ticari işlem yapmaya yetkili olduğundan merkezden ayrı bir yönetime sahip olması gerekliliğini ifade etmektedir.

Öte yandan, Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GDPR) 3 üncü maddesinin (1) numaralı fıkrasında “Bu Tüzük, işleminin Birlik dahilinde gerçekleştiğine bakılmaksızın, kişisel verilerin bir veri sorumlusunun veya veri işleyenin Birlik dahilindeki işletmesinin faaliyetleri kapsamında işlenmesine uygulanır.” düzenlemesine yer verilmiştir.

Söz konusu hükme göre, Avrupa Birliği'nde (AB) bulunan şubenin / irtibat bürosunun kendisinin veri işleyip işlemediği önemli değildir. Yabancı şirket, AB'de bulunan şubesinin / irtibat bürosunun

faaliyetleri çerçevesinde veri işleme gerçekleştirdiği takdirde GDPR hükümlerine tabi olmaktadır. Bu kapsamda, AB’de bulunan işletme ile AB dışında bulunan veri sorumlusunun veri işlemesi arasında açık bir bağ olduğunun tespit edilmesi halinde, AB dışında bulunan veri sorumlusunun GDPR hükümlerine tabi olacağı sonucuna varılmaktadır. Burada, AB dışında bulunan şirketlerin, veri sorumlusu / veri işleyen olarak GDPR hükümlerine tabi olmasına ilişkin bir kriter olarak “işletme” kavramı dikkat çekmektedir. Yani GDPR’ın sınır aşan şekilde uygulanmasına ilişkin olarak, yabancı veri sorumlusu / veri işleyen bir girişimin / oluşumun (şirket vb.), AB’de bulunan işletmesi aracılığıyla (bu işletmenin faaliyetleri çerçevesinde) GDPR hükümlerine tabi olması sonucu doğabilmektedir.

Yine GDPR’ın 4 üncü maddesinin 7 inci fıkrasında veri sorumlusu (kontrolör); “yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçlar ve yöntemleri belirleyen gerçek veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır; söz konusu işleme amaçları ve yöntemlerinin Birlik ya da üye devlet hukukuna göre belirlenmesi durumunda, kontrolör veya kontrolörün belirlenmesine özgü kriterler Birlik ya da üye devlet hukukuna göre belirlenebilir” şeklinde 6698 sayılı Kanunda yer alan veri sorumlusu tanımı ile benzer şekilde ve daha kapsamlı olarak tanımlanmıştır. Bu çerçevede veri sorumlusu, kişisel verileri elinde bulundurması dolayısıyla bu sıfatı kazanmakta, kişisel verilerin işleme amaçlarını ve vasıtalarını belirlemekle veri sorumlusu haline gelmektedir.

Bu açıdan değerlendirildiğinde, her ne kadar Sicile kayıt yükümlülüğü için 6698 sayılı Kanuna göre veri sorumlusu sıfatını haiz olması yani tüzel ya da gerçek kişi olması kriterini de taşıması gerekmekte ise de, yurt dışında yerleşik tüzel kişilerin Türkiye’deki şubelerinin ayrı bir tüzel kişilikleri bulunmasa da TTK 40 inci maddesine göre şubelerin yerli ticari işletmeler gibi tescil oldukları ve GDPR’ın 4 üncü maddesindeki veri sorumlusu olma kriterleri arasında “tüzel kişi” olmanın şart olarak öngörülmediği göz önünde bulundurulduğunda, kişisel veri işleme süreçleri bakımından merkezden bağımsız bir şekilde Türkiye’de veri sorumlusu kriterlerine uygun olarak hareket eden bu şubelerin veri sorumlusu sayılacağı değerlendirilmektedir.

Yurtdışında yerleşik tüzel kişilerin Türkiye’deki irtibat büroları açısından;

4875 sayılı Doğrudan Yabancı Yatırımlar Kanununda yabancı yatırımlar ile ilgili düzenlemeler bulunmakta olup bu doğrultuda, doğrudan yabancı yatırıma ilişkin esaslar arasında, yatırım planlanan ülkeye irtibat bürosu kurma da yer almaktadır.

4875 sayılı Doğrudan Yabancı Yatırımcılar Kanunu Uygulama Yönetmeliğinin 6 ncı maddesinin 1 inci fıkrasında “Bakanlık, yabancı ülke kanunlarına göre kurulmuş şirketlere, Türkiye’de ticari faaliyette

bulunmamak kaydıyla irtibat bürosu açma izni vermeye ve bu izinlerin süresini uzatmaya yetkilidir.” düzenlemesine yer verilmiştir.

Yukarıda yer verilen açıklamalar çerçevesinde yapılan değerlendirme sonucunda;

1. Türkiye’de doğrudan veya şubeleri aracılığıyla kişisel veri işleme faaliyetinde bulunan yurt dışında yerleşik veri sorumlularının Sicile kayıt olmalarının gerektiğine,

2. Yurt dışında yerleşik tüzel kişilerin Türkiye’deki şubelerinin, Kanunda yer alan veri sorumlusu tanımı gereği kişisel verilerin işleme amaçlarını ve vasıtalarını belirlemesi ve veri kayıt sisteminin kurulması ile yönetilmesinden sorumlu olması halinde yurt dışında yerleşik tüzel kişiden ayrı olarak Türkiye’de yerleşik veri sorumlusu olarak değerlendirileceğine, bu durumda olan yurt dışında yerleşik tüzel kişilerin Türkiye’deki şubeleri için Kişisel Verileri Koruma Kurulunun 2018/88 sayılı ve 2019/265 sayılı kararlarında yer alan “yıllık çalışan sayısı” ve “yıllık mali bilanço toplamı” kriterleri açısından yapılacak değerlendirme sonucunda Sicile kayıt yükümlülüğü bulunup bulunmadığına karar verileceğine, bu durumda olmayan yurt dışında yerleşik tüzel kişilerin Türkiye’deki şubelerinin ise Sicile kayıt yükümlülüğünün bulunmadığına,

3. Türkiye’de irtibat bürosu açılabilmesi için şirket tüzel kişiliklerinin yabancı ülke kanunlarına göre kurulması ve kurulan irtibat bürolarının Türkiye’de ticari faaliyette bulunmaması gerektiği, irtibat bürolarının ticari faaliyet dışında haberleşme, fizibilite araştırması yapma, sosyal ve kültürel alanlarda bazı çalışmalarını yürütme, şirketler arasında birleşme ve devirler için ön hazırlık yapma, tanıtım ve reklam, ülkedeki iş olanaklarının yakından takip etme ve bu konular hakkında merkez firmaya bilgi verme amacı doğrultusunda açılan bürolar olması ve şube özelliği bulunmadığı hususu dikkate alındığında söz konusu irtibat bürolarının Sicile kayıt olma yükümlülüğünün bulunmadığına,

karar verilmiştir.

2019/222 sayılı KVKK Kararı

Dubsmash Inc. hakkında Kişisel Verileri Koruma Kurulunun 17/07/2019 Tarihli ve 2019/222 Sayılı Karar Özeti

Karar Tarihi : 17.07.2019

Karar No : 2019/222

Konu Özeti : Dubsmash Inc.'in veri ihlal bildirimini hakkında bilgilendirme

Kurum kayıtlarına 08.04.2019 ve 25.06.2019 tarihlerinde intikal eden, Dubsmash Inc.'i temsil eden Lewis Brisbois Bisgaard & Smith LLP'nin yazlarında özetle;

- 8 Şubat 2019 tarihinde Dubsmash'in, gazeteci olduğunu iddia eden bir kişiden gelen e-posta vasıtasıyla veri ihlalden haberdar olduğu, söz konusu gazetecinin ise karanlık ağda (Darknet) Dubsmash kullanıcılarının kişisel bilgilerine sahip olduğunu iddia eden bir kişi tarafından haberdar edildiği,
- İddiaları soruşturmak için bir dijital adli tıp firması ile anlaşıldığı ve inceleme başlatıldığı, 11 Şubat 2019'da Dubsmash'ın kullanıcı bilgilerini içeren veri tabanı kopyasının satın alındığı,
- Satın alınan veri tabanında bulunan kişilerin sayısına dayanarak, olayın Kasım 2018'de meydana geldiğinden şüphelenildiği,
- Dubsmash'ın incelemesi sonucunda, halka açık profilinde ilişkili ülke olarak Türkiye'yi tanımlayan 679.269 kişiye ait bilgilerin satın alınan veri tabanında yer aldığı,
- İhlalin tekrar yaşanmaması, güvenlik tedbirlerinin güçlendirilmesi, ağ ve sistemlerin güvenli olması da dahil olmak üzere gerekli adımların atıldığı,
- Dubsmash'ın kullanıcı sorularına cevap vermek için bir çağrı merkezi kurduğu, çağrı merkezi için yerli ve uluslararası telefon numaraları sağlandığı,

ifadelerine yer verilmiştir.

Söz konusu bildirimincin incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 17.07.2019 tarih ve 2019/222 sayılı Kararı ile;

Lewis Brisbois Bisgaard & Smith LLP'nin, Dubsmash Inc (ABD)'nin yasal temsilcisi olduğuna dair tevsik edici belgenin Kurum'a iletilmediği,

- Hem IOS hem de Android işletim sistemlerinde çalışabilen uygulamanın dünya çapında yaklaşık 162 milyon civarındaki kullanıcı hesabına ait bilgilerinin Darknet web'te satıldığı,
- Bu bilgiler arasında kullanıcıların kullanıcı adı, şifreler, doğum tarihi, telefon numarası, e-mail adresi, ülkesi/dili gibi gerçek kişiye ait verilerin olduğu,
- Bu verilerin Kasım 2018 Şubat ayından beri satışta olduğunun tahmin edildiği,
- Veri ihlalinin nasıl gerçekleştiğinin bilinmediği, - Veri ihlalden bir gazeteci vasıtasıyla haberdar olmasının Dubsmash'ın teknik ve idari tedbirler bakımından kusurlu olduğunu gösterdiği,
- Dubsmash'ın büyük çaptaki bu veri ihlaline rağmen kullanıcılarını bu konuda bilgilendirmediği,
- Dubsmash kullanıcılarının ancak belli bazı sitelerden verilerinin ihlal edilip edilmediğini öğrenebildikleri

hususları dikkate alınarak,

- Kanunun 12 nci maddesinin (1) numaralı fıkrasında yer alan veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almadığı kanaatine varılan Şirket hakkında, Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca, 680.000 TL,
- 08.02.2019 tarihinde tespit edilen veri ihlalinin 27.02.2019 tarihinde Kuruma bildirildiği dikkate alındığında, Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer alan "en kısa sürede bildirim" yükümlülüğüne aykırılık teşkil eden uygulaması nedeniyle Şirket hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 50.000 TL,

olmak üzere toplam 730.000 TL idari para cezası uygulanmasına,

- İhlalden, halka açık profilinde ilişkili ülke olarak Türkiye'yi tanımlayan 679.269 kişinin etkilendiği dikkate alındığında, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12 nci maddesinin (5) numaralı fıkrasında yer alan "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." hükmü gereğince söz konusu ihlalin Kurumun internet sitesinde ilan edilmesine

karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2019/206 sayılı KVKK Kararı

Veri sorumlusunun, web sitesinde kişisel verilerin işlenmesini hizmet şartı olarak talep ettiği ve aydınlatma yükümlülüğünü usulüne uygun yerine getirmediği iddiaları hakkında Kişisel Verileri Koruma Kurulunun 08/07/2019 tarih ve 2019/206 sayılı Karar Özeti

Karar Tarihi : 08.07.2019

Karar No : 2019/206

Konu Özeti : Veri sorumlusunun, web sitesinde kişisel verilerin işlenmesini hizmet şartı olarak talep ettiği ve aydınlatma yükümlülüğünün usulüne uygun yerine getirmediği iddiaları hakkında

Kurumumuza intikal eden ihbar başvurusunda özetle, veri sorumlusunun hizmet sunduğu web sayfasına girildiğinde, giriş yapılması için zorunlu bir alan çıktığı ve e-posta adresinin talep edildiği, istenilen kişisel veriler verilmeden ana sayfaya geçiş imkânının bulunmadığı ve bu bakımdan söz konusu kişisel verinin verilmesinin bir hizmet şartı olarak talep edildiği; kişisel veri talebi sırasında aydınlatma yükümlülüğü kapsamında sunulan metnin, işlenen kişisel verileri ve hukuki sebeplerini açıkça ortaya koymadığı iddia edilmekte olup, konuya ilişkin olarak başlatılan resen inceleme çerçevesinde alınan 08/07/2019 tarih ve 2019/206 sayılı Kurul Kararı ile;

1- 6698 sayılı Kişisel Verilerin Korunması Kanunu çerçevesinde açık rızanın, kişinin sahip olduğu verinin işlenmesine, kendi isteği ile ya da karşı taraftan gelen istek üzerine, onay vermesi anlamını taşıdığı, kişinin açık rıza açıklaması ile aslında veri sorumlusuna kendi hukuksal değerine ilişkin verdiği kararı bildirdiği ve açık rıza açıklamasının, ilgili kişinin, işlenmesine izin verdiği verinin sınırlarını, kapsamını ve gerçekleştirilme biçimini de belirlemesini sağlayacağı, açık rızanın bu anlamda, rıza veren kişinin “olumlu irade beyanı”nı içermesi gerektiği,

Kanununun 3 üncü maddesinde yer verilen açık rıza tanımı kapsamında açık rızanın “belirli bir konuya ilişkin olması, rızanın bilgilendirmeye dayanması ve özgür iradeyle açıklanması” şeklinde üç unsurunun bulunduğu,

Açık rızanın özgür irade ile açıklanması gerektiğinden, ilgili kişinin açık rızasının alınmasının, bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının ön şartı olarak

ileri sürülmemesi gerektiği, Kurumumuza intikal eden ihbarda bahse konu web sayfasının, kişisel verinin işlenmesini bir hizmet şartı olarak talep ettiğinin iddia edildiği,

Bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının açık rıza şartına dayandırılmasının, açık rızanın özgür iradeyle açıklanmış olması kuralına aykırılık teşkil edecek olmakla birlikte, incelemeye konu web sitesinin, site bünyesinde kullanıcılara sunulan çeşitli alanlardaki mal ve hizmetlerin doğrudan tedarikçisi/sağlayıcısı niteliğinde olmadığı; farklı illerde, farklı sektörlerde ve farklı hizmet sağlayıcıları tarafından sunulan çeşitli hizmetlerin, indirimli fiyatlar üzerinden üyeler tarafından satın alınmasını sağlayan bir aracı firma/hizmet sağlayıcı rolü üstlendiğinin görüldüğü,

Bu çerçevede söz konusu Sitenin, farklı illerde, farklı sektörlerde ve farklı hizmet sağlayıcıları tarafından sunulan çeşitli hizmetler açısından üyelerine artı bir menfaat/avantaj sağladığı; siteye üye olmak istemeyen müşterilerin, söz konusu site bünyesinde yer almakla birlikte, farklı illerde, farklı sektörlerde ve farklı hizmet sağlayıcıları tarafından sunulan çeşitli hizmetlere erişim, bu ürünleri ya da hizmetleri satın alma imkânlarının da ortadan kaldırılmadığı;

Bu anlamda iddiaya konu hususta, bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının açık rıza şartına dayandırılmasından ziyade Site bünyesinde sunulan indirimli fiyatların ve avantajların yalnızca üye olanlara sunulmasının söz konusu olduğu

değerlendirmelerinden hareketle, iddiaya konu hususa ilişkin olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında tesis edilecek herhangi bir işlem bulunmadığına,

2- İkinci olarak Kanununun 10 uncu maddesi hükmü uyarınca, kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişinin, ilgili kişilere; a) Veri sorumlusunun ve varsa temsilcisinin kimliği, b) Kişisel verilerin hangi amaçla işleneceği, c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi, d) 11 inci maddede sayılan diğer hakları konusunda bilgi vermekle yükümlü olduğu,

“Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ”in; 5 inci maddesinin birinci fıkrasının

(f) bendinde; *“Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir.”* hükmünün,

(g) bendinde; *“Aydınlatma yükümlülüğü kapsamında açıklanacak kişisel veri işleme amacının belirli, açık ve meşru olması gerekir. Aydınlatma yükümlülüğü yerine getirilirken, genel nitelikte ve muğlak*

ifadelere yer verilmemelidir. Gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandıran ifadeler kullanılmamalıdır.” hükmünün,

(ğ) bendinde; “Aydınlatma yükümlülüğü kapsamında ilgili kişiye yapılacak bildirim anlaşılır, açık ve sade bir dil kullanılarak gerçekleştirilmesi gerekmektedir.” hükmünün,

(h) bendinde; “Kanununun 10 uncu maddesinin birinci fıkrasının (ç) bendinde yer alan “hukuki sebep” ten kasıt, aydınlatma yükümlülüğü kapsamında kişisel verilerin Kanununun 5 ve 6 ncı maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiğidir. Aydınlatma yükümlülüğünün yerine getirilmesi esnasında hukuki sebebin açıkça belirtilmesi gerekmektedir.” hükmünün,

(j) bendinde ise; “Aydınlatma yükümlülüğü yerine getirilirken eksik, ilgili kişileri yanıltıcı ve yanlış bilgilere yer verilmemelidir.” hükmünün

yer aldığı,

İhbara konu web adresi üzerinden erişim sağlanan “GİZLİLİK ve KVK Politikamız” başlıklı metin, söz konusu mevzuat düzenlemeleri çerçevesinde incelendiğinde;

Web sitesinin ilgili kişiler hakkında işlediği ad, soyadı, doğum tarihi, cep telefonu numarası, e-posta, cinsiyet, adres, sosyal medya hesaplarıyla bağlanması durumunda üyenin o kanallar aracılığıyla paylaşılmasına onay verdiği bilgilerin, üyenin tüm alışveriş bilgilerinin, yani hangi üye işyeri, alışveriş noktası ve zamanı, ne kadar ödeme yaptığı, hangi kampanyadan faydalandığı, aldığı indirim tutarı, alışverişindeki ürün bilgileri, uygulama üzerindeki gezinme ve tıklama bilgilerinin, uygulamayı açtığı lokasyon bilgilerinin, “ilgili mevzuat”tan kaynaklanan yasal yükümlülük çerçevesinde mi yoksa ilgili kişilerin açık rızalarına istinaden mi işlendiğinin ya da söz konusu kişisel verilerin hangilerinin “ilgili mevzuat”tan kaynaklanan yasal yükümlülük çerçevesinde hangilerinin ise ilgili kişilerin açık rızalarına istinaden işlendiğinin açıkça belirtilmemiş olduğu,

İlgili kişilerin kişisel verilerin işlenmesinin hukuki sebebi olarak “ilgili mevzuattan kaynaklanan yasal yükümlülük”ten bahsedildikten sonra, aydınlatma metninin devamında, “... söz konusu amaç ve yasal yükümlülüklerini yerine getirebilmeyi sağlayacak kişisel verilerinizi ... sizlerden talep etmektedir. Bu kişisel veriler veri sorumlusunun sunmuş olduğu hizmetlerden yararlanabilmeniz adına, **açık rızanıza istinaden, ... işlenecek ve saklanacaktır.**” şeklinde bir bilgilendirmede bulunularak, kişisel veri işleme faaliyetinin asıl olarak ve yalnızca ilgili kişilerin açık rızalarına dayanılarak gerçekleştirildiği izlenimine neden olduğu,

Oysa kişisel veri işleme faaliyetinin, Kanunda bulunan açık rıza dışındaki şartlardan birine dayanıyorsa, bu durumda ilgili kişiden açık rıza alınmasına gerek bulunmadığı ve veri işleme

faaliyetinin, açık rıza dışında bir dayanakla yürütülmesi mümkün iken açık rızaya dayandırılmasının, aldatıcı ve hakkın kötüye kullanımı niteliğinde olacağı; nitekim ilgili kişi tarafından verilen açık rızanın geri alınması halinde veri sorumlusunun diğer kişisel veri işleme şartlarından birine dayalı olarak veri işleme faaliyetini sürdürmesinin hukuka ve dürüstlük kurallarına aykırı işlem yapılması anlamına geleceği,

dikkate alındığında, bahse konu web adresi üzerinden erişim sağlanan "GİZLİLİK ve KVK Politikamız" başlıklı metnin, "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ"e uygun düzenlenmediği, bu kapsamda söz konusu metnin Tebliğde yer verilen hükümler dikkate alınmak suretiyle güncellenmesi, ayrıca aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerektiği yönünde Şirketin talimatlandırılmasına

karar verilmiştir.

2019/204 sayılı KVKK Kararı

Bir yatırım şirketi tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmadan işlenmesi ve reklam/bilgilendirme amaçlı aranması hakkında Kuruma yaptığı başvuru ile ilgili Kişisel Verileri Koruma Kurulunun 08/07/2019 Tarihli ve 2019/204 Sayılı Karar

Karar Tarihi : 08.07.2019

Karar No : 2019/204

Konu Özeti : Bir yatırım şirketi tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmadan işlenmesi ve reklam/bilgilendirme amaçlı aranması hakkında Kurula yaptığı başvuru

İlgili kişinin şahsına ait cep telefonunun açık rızası olmaksızın bir yatırım ve menkul değerler şirketi tarafından bilgilendirme/reklam amaçlı aranması üzerine veri sorumlusuna yaptığı başvuruya yeterli yanıt alamaması nedeniyle Kişisel Verileri Koruma Kuruluna ilettiği şikayet başvurusunun incelenmesi neticesinde,

Şikayete konu olayda veri sorumlusundan alınan bilgiler ışığında; Şikayetçinin müşterisi olduğu personelin daha önce başka bir yatırım şirketinde çalıştığı, bu şirketin faaliyetlerine son verilip kapatılmasının ardından 2017 yılında bahse konu personelin yine aynı alanda faaliyet gösteren veri sorumlusu şirkette çalışmaya başladığı, dolayısıyla şikayetçinin telefon numarası bilgisine bu şekilde vakıf olduğu ve sonrasında veri sorumlusunun bir personeli tarafından ilgili kişinin reklam ve bilgilendirme amacıyla arandığı anlaşılmış olup,

6698 sayılı Kanunun "Kişisel Verilerin İşlenme Şartları" başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise Kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,

ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işleminin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerine yer verildiği dikkate alınarak,

- Şikayete konu başvuru, veri işleme şartları açısından değerlendirildiğinde Şirketin Şikayetçinin telefon numarasını işleminin 6698 sayılı Kanununun 5 inci maddesinde sayılan şartlardan herhangi birine dayanmaması nedeniyle Şirketin hukuka aykırı bir veri işleme faaliyetinde bulunduğu sonucuna ulaşıldığından, Kanununun 12 nci maddesinin (1) numaralı fıkrasının (a) bendine aykırı hareket etmesi nedeniyle Kanununun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi gereğince Şirket hakkında 75.000 TL idari para cezası uygulanmasına,

- Şirketin beyanlarında yer alan; Şikayetçinin Şirketin bir pazarlama personelinin başka bir şirkette çalışırken müşterisi olması nedeniyle, bu personelin yeni işyeri olan Şirkete bu verileri aktardığına ilişkin iddialarına ilişkin olarak; Şikayetçinin Türk Ceza Kanununun 136 ncı maddesi hakkında bilgilendirilmesine,

- Şikayetçinin Şirketi muhatap başvurusunda yer alan kişisel verilerinin kimlerden ne şekilde elde edildiğine dair bilgi talebine Şirketçe cevap verilmemiş olması nedeniyle Şirketin Kanuna uyum konusunda gerekli hassasiyeti ve özeni göstermesi yönünde uyarılmasına ve söz konusu hususlarda Şirketin Kurumu muhatap yazısında belirtildiği şekliyle Şikayetçiye bilgi vermesi yönünde talimatlandırılmasına

karar verilmiştir.

2019/198 sayılı KVKK Kararı

İlgili kişinin, bir sadakat programı kapsamında veri sorumlusunca hukuka aykırı kişisel veri işlendiği yolundaki ihbarı hakkında Kişisel Verileri Koruma Kurulunun 05/07/2019 tarihli ve 2019/198 sayılı Karar Özeti

Karar Tarihi : 05/07/2019

Karar No : 2019/198

Konu Özeti : İlgili kişinin, bir sadakat programı kapsamında veri sorumlusunca hukuka aykırı kişisel veri işlendiği yolundaki ihbarı

Kuruma intikal eden dilekçede özetle; veri sorumlusunun mağazasında satılan bazı ürünlere sadakat karta özel indirim uygulandığı, böylece özel indirimlerin şarta bağlandığı, söz konusu sadakat programına üyelik ve kart temini için de müşterinin kişisel verilerinin talep edildiği ve açık rızanın koşul olarak dayatıldığı belirtilerek veri sorumlusu hakkında ihbarda bulunulmuştur.

İhbarda yer alan konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabî yazıda özetle;

- Sadakat programına dahil olmak isteyen ilgili kişilere sunulan açık rıza metninde açık rızanın hangi amaçları içerdiği açıkça sıralanarak açık rızanın belirli bir konuya ilişkin olma unsurunun karşılandığı,
- İlgili kişilere açık rıza metni sunulmakla birlikte ayrıca kişisel verilerinin işlenmesine ve haklarına ilişkin olarak mevzuata uygun şekilde aydınlatma yapıldığı,
- Sadakat programı dahilinde açık rıza vermek istemeyen ilgili kişilere mağazalarından ve internet siteleri üzerinden her daim alışveriş imkanı sunulduğu, ürün ve hizmetlerinin herkesin erişimine açık olduğu ve belirlenen fiyatlar üzerinden herkes tarafından temin edilebildiği, bu ürün veya hizmetlerde yapılan indirimlerin ise ürün veya hizmetin rayiç bedelinin altında ve ek bir menfaat niteliğinde olduğu,
- Program dahilinde ve ilgili kişiler tarafından açık rıza verilmesi halinde yararlanılabilen indirimlerin ana ürün veya hizmetin sunumuna ilişkin olmayıp ek menfaat niteliğinde olduğu ve bu

durumun ilgili kişinin açık rızasının alınmasının, bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının ön şartı olarak ileri sürülmediğini gösterdiği,

- Ek menfaatlerin açık rıza koşuluna bağlanmasının “açık rızanın özgür irade ile verilmesi” koşulunu ortadan kaldırmayacağını mehz Avrupa Birliği mevzuatında da açıkça kabul edildiği ve bu durumun Avrupa Birliği Veri Koruma Hukuku Hakkında El Kitabında (Handbook on European Data Protection Law) “... rıza vermeme sonucunda negatif sonuçlar doğacak olması rızanın geçerli olmayacağı anlamına gelmemektedir. Örneğin eğer süpermarket müşteri kartına rıza verilmemesi yalnızca belirli ürün fiyatlarına küçük bir miktar indirim elde edilmemesi sonucunu doğuruyorsa söz konusu kartı almaya rıza veren müşterilerin kişisel verilerinin işlenmesi açısından rıza geçerli bir hukuki sebep olarak değerlendirilebilecektir. Müşteri ile şirket arasında bir altüst bağı yoktur ve rıza verilmemesinin sonuçları veri sahibinin özgür iradesini etkileyecek kadar ciddi değildir (ürün üzerinde yapılacak olan indirim veri sahibinin özgür iradesini etkilemeyecek kadar küçük miktardadır). ...” şeklindeki açıklama ile ortaya koyulduğu

ifade edilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 05/07/2019 tarih ve 2019/198 sayılı sayılı Kararı ile;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun 3’üncü maddesinin (1) numaralı fıkrasının (a) bendi hükmü uyarınca açık rızanın belirli bir konuya ilişkin olma, bilgilendirmeye dayanma, özgür irade ile açıklanma şeklinde üç unsuru olduğu,

- İncelemeye konu ihbar niteliğindeki dilekçede yer alan bilgiler çerçevesinde veri sorumlusunun 99,99 TL olan ürünün fiyatını sadakat karta özel indirim kapsamında 79,99 TL olarak belirlediğinin ve satışa sunduğunun anlaşıldığı,

- Sadakat kart programına dahil olmak istemeyen ve/veya söz konusu program dahilinde açık rıza vermek istemeyen ilgili kişilerin veri sorumlusunun mağazalarından alışveriş yapma imkanının ortadan kaldırılmadığı ve sadakat programına üye olmayan müşterilere indirimsiz fiyatlar üzerinden satış yapılmaya devam edildiği,

- Sadakat programı kapsamında ürün/hizmetlerin ek menfaat ile indirimli olarak sunulmasının açık rızanın koşul olarak dayatılması anlamına gelmediği

değerlendirmelerinden hareketle;

- Veri sorumlusunun mağazalarında sunulan ürün veya hizmetlerin, gerçekleştirilen kampanyalar dahilinde ve veri sorumlusu şirketin sadakat programına özel indirimli fiyatlar üzerinden ek bir menfaate sunuluyor olmasının, açık rızanın koşul olarak dayatılması ve bu anlamda ilgili kişinin açık rızasının bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının ön şartı olarak ileri sürülmesi olarak kabul edilemeyeceğinden, söz konusu dilekçeye ilişkin olarak Kanun hükümleri kapsamında yapılacak bir işlem olmadığına karar verilmiştir.

2019/188 sayılı KVKK Kararı

Öğrencilerin kişisel verisi niteliğindeki sınav sonuçlarını internet ortamında yayımlayan Mimar Sinan Güzel Sanatlar Üniversitesi'nin uygulaması hakkında Kuruma yapılmış olan başvuru hakkında Kişisel Verileri Koruma Kurulunun 01/07/2019 Tarihli ve 2019/188 Sayılı Karar

Karar Tarihi : 01.07.2019

Karar No : 2019/188

Konu Özeti : Öğrencilerin kişisel verisi niteliğindeki sınav sonuçlarını internet ortamında yayımlayan Mimar Sinan Güzel Sanatlar Üniversitesi'nin uygulaması hakkında Kuruma yapılmış olan başvuru hakkında

Mimar Sinan Güzel Sanatlar Üniversitesinde sınava girmiş kişilerin sınav sonuçlarının Yükseköğretim Kurulunun sınav sonuçlarına ilişkin düzenlemeleri çerçevesinde alenen duyurulduğu ve sonuçların internette aramaya açık biçimde yayınlandığı, arama motorlarında sorgulama yapıldığında bu sonuçlara kolayca ulaşılabildiği, üniversite bitirilmiş ve aradan yıllar geçmiş olsa dahi sonuçların üçüncü kişilerin erişimine açık olduğu, ancak bu uygulamanın 6698 sayılı Kişisel Verilerin Korunması Kanununa (Kanun) aykırılık teşkil ettiği belirtilerek, söz konusu uygulamanın düzeltilmesi, üniversitedeki sınav sonuçlarının kullanıcı adı-şifre ile giriş yapılan güvenli bir sistem ile açıklanması talebine ilişkin Kurumumuza intikal eden bir başvuru ile ilgili olarak;

Kişisel Verileri Koruma Kurulu (Kurul) Kararı ile başlatılan incelemeye istinaden veri sorumlusu Mimar Sinan Güzel Sanatlar Üniversitesi'ne iletilen bilgi belge talebi yazısına Kanunda belirtilen yasal süre içinde yanıt verilmediği de dikkate alınarak yapılan değerlendirme neticesinde;

- Yükseköğretim Kuruluna iletilen bilgi talebi yazısına cevaben Kurumumuza gönderilen yazıda üniversitelerin sınav sonuçlarını ne şekilde duyurması ve bu sonuçları ne kadar süre ile erişime açık tutması gerektiğine ilişkin düzenlemelerin Üniversitelerin kendi mevzuatlarında yer aldığı ve konuya ilişkin karar verme yetkisinin de Üniversitelerde olduğu sonuç ve kanaatine varıldığı ifade edildiği,

- “Mimar Sinan Güzel Sanatlar Üniversitesi Lisansüstü Öğretim Yönetmeliği” nin 8 inci maddesinin “Lisansüstü programlara kabul edilen öğrencilerin listesi enstitü yönetim kurulu kararı ile kesinleşir ve enstitü müdürlüğü tarafından duyurulur.” şeklinde düzenlendiği,

- Söz konusu düzenlemenin somut olayda Mimar Sinan Güzel Sanatlar Üniversitesi tarafından sonuçların internette aramaya açık biçimde yayınlanarak, üniversite bitirilmiş ve aradan yıllar geçmiş olsa dahi sonuçların üçüncü kişilerin erişimine açık ve arama motorlarında sorgulama yapıldığında bu sonuçlara kolayca ulaşılabilir tarzda bir duyuru yönteminin benimsenerek yerine getirildiği, ancak söz konusu duyuru yönteminin Kanun hükümleri çerçevesinde değerlendirildiğinde kişisel veriler bağlamında mahremiyet odaklı olmayıp, sınava giren bireylerin kişisel verilerinin herhangi bir işleme şartına dayanmaksızın üçüncü kişilerin de kolaylıkla ulaşabileceği şekilde açıklandığı kanaatine varıldığı,

- Bu kapsamda, sınav sonuç duyuru sisteminin Üniversite tarafından tekrar gözden geçirilerek kimlik doğrulama yöntemi şeklinde sadece sınava giren bireyin kendi TC Kimlik numarası ve doğrulama kodu ile yalnızca kendi sonuç verilerine ulaştığı, ÖSYM'nin sonuç açıklama yöntemi gibi bir düzenleme ile kişisel verilerin paylaşımında mahremiyet odaklı bir anlayışı uygulamaya koyması gerektiği,

değerlendirmelerinden hareketle;

- Mimar Sinan Güzel Sanatlar Üniversitesi'ne Kurumumuzca iletilen bilgi belge talebi yazısının Kanunda belirtilen yasal süre içinde yanıtlanmaması suretiyle ilgili Kurul Kararının gereğinin yerine getirilmemesinin Kanununun 15 inci maddesinin (3) numaralı fıkrasına aykırılık oluşturduğu dikkate alınarak, kamu kuruluşu olarak değerlendirilen Mimar Sinan Güzel Sanatlar Üniversitesinde görev yapan sorumlular hakkında Kanununun 18 inci maddesinin (3) numaralı fıkrası çerçevesinde disiplin hükümlerine göre işlem yapılmasına,

- Öte yandan Mimar Sinan Güzel Sanatlar Üniversitesi sınav sonuç duyuru sisteminin tekrar tasarlanarak kimlik doğrulama yönteminin benimsendiği, sadece sınava giren bireyin kendi TC Kimlik numarası ve doğrulama kodu ile yalnızca kendi sonuç verilerine ulaştığı bir duyuru sisteminin kullanılması yönünde Üniversitenin talimatlandırılmasına

karar verilmiştir.

2019/170 sayılı KVKK Kararı

Bir perakende giyim firmasının veri ihlal bildirimini hakkında Kişisel Verileri Koruma Kurulunun 18/06/2019 tarih ve 2019/170 sayılı Karar Özeti

Karar Tarihi : 18.06.2019

Karar No : 2019/170

Konu Özeti : Bir perakende giyim firmasının kişisel veri ihlali bildirimini

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin bazı müşterilerin yeni bir hesap açarken kişisel verilerinin yanlışlıkla bir URL üzerinden veri sorumlusunun iç sistemlerine ve çalıştığı bazı üçüncü taraf satıcı/sağlayıcılara aktarılması şeklinde gerçekleştiği ve bu durumun veri sorumlusunun olağan bir denetimi esnasında tespit edildiği,
- Kurumumuza veri ihlaline ilişkin bildirim yapıldığında, veri sorumlusunun iki uygulama analizi sağlayıcısından (analytics provider) verilerin hâlihazırda otomatik olarak silinmiş olduğuna dair teyit aldığı,
- İlk bulgulardan sonra konunun daha detaylı araştırılması için gerçekleştirilen soruşturma kapsamında başka yedi adet URL tarafından da sehven veri toplandığı ve bunların veri sorumlusunun etiket yönetim sistemine (tag management system) yönlendirildiğinin öğrenildiği (Türkiye'deki ilgili kişilerin bu yedi adet URL'den iki tanesinde gerçekleşen hatadan etkilendiği),
- İhlalden etkilenen ilgili kişi sayısının 44 olduğu,
- İhlalden etkilenen kişi kategorilerinin aboneler/üyeler, müşteriler/potansiyel müşteriler olduğu,
- Şirketin Kurumumuzu muhatap 10.06.2019 tarihli ilk yazısında, ihlalden etkilenen kişisel verilerin, zorunlu alan olan e-posta adresi, doğum tarihi, açık metin şeklinde şifre verilerinin olduğu, ancak zorunlu alan olmayan ad soyad verilerinin de etkilenmiş olabileceği,
- İlgili kişilere 23.07.2019 tarihinde e-posta yoluyla bildirim yapıldığı ifadelerine yer verilmiştir.

Söz konusu bildirim incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 18/06/2019 tarih ve 2019/170 sayılı Kararı ile;

- 01.08.2018 ve 21.10.2018 tarihlerinde gerçekleşen veri ihlallerinin tespitinin yaklaşık bir yıl sonra 02.07.2019 tarihinde yapılmış olmasının, gerçekleştirilen işlemlere dair Şirketin log kaydı/takip alarm sistemlerinin bulunmadığının ya da etkin bir şekilde kullanılmadığının ve Şirket tarafından gerekli kontrollerin yapılmadığının göstergesi olduğu,

- URL üzerinden kişisel verilerin üçüncü taraf satıcı/sağlayıcılar tarafından görülmesinin web sayfası tasarım aşamasında iken yapılan testlerin yetersiz olduğunun veya gerekli testlerin yapılmadığının göstergesi olduğu

kanaatine varıldığından Web sayfası tasarım aşamasında iken yapılan testlerin yetersiz olması, gerçekleşen işlemlere dair takip/alarm sistemlerinin bulunmamasından kaynaklı ihlal tespitinin geç yapılmış olması sebebiyle, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 50.000 TL idari para cezası uygulanmasına,

- İhlalin veri sorumlusu tarafından 29.05.2019 tarihinde tespit edildiği, 06.06.2019 tarihinde Kurula bildirim yapıldığı görülmekle birlikte yurtdışında mukim veri sorumlusu tarafından tespit tarihinden sonra söz konusu ihlalden Türkiye'deki ilgili kişilerin de etkilenip etkilenmediğine yönelik araştırma yapıldığı

dikkate alındığında bu sürenin makul olduğu değerlendirildiğinden bu hususta Kanun kapsamında yapılacak bir işlem bulunmadığına

karar verilmiştir.

2019/166 sayılı KVKK Kararı

İlgili kişiye ait telefon numarasına kendisine ait olmayan içeriğin gönderilmesi ile ilgili Kişisel Verileri Koruma Kurulunun 31/05/2019 Tarihli ve 2019/166 Sayılı Karar

Karar Tarihi : 31.05.2019

Karar No : 2019/166

Konu Özeti : İlgili kişiye ait telefon numarasına kendisine ait olmayan içeriğin gönderilmesi ile ilgili Kurul kararı

İlgili kişinin, şahsına ait telefon numaralarına gönderilen ve kendisine ait olmayan içerik barındıran kısa mesaj (SMS) nedeniyle veri sorumlusuna başvurduğu; veri sorumlusu tarafından verilen cevapta, bu gönderimin personel hatasından kaynaklandığı ve başka bir aboneye ait giriş yapılırken 1 rakam hatası sonucunda ilgili kişiye SMS gönderildiği tespit edilerek yanlışlığın derhal düzeltildiğinin belirtildiği; ancak, kendisine gönderilen SMS'te kişisel verileri yer alan kişinin yeğeni olduğunu ve yeğenin telefon numarası ile kendisine ait telefon numarasının 1 rakam değişikliği / yanlışlığı ile karıştırılmasının mümkün olmadığını belirterek veri sorumlusu hakkında gereğinin yapılmasını talep ettiği başvurusunun incelenmesi neticesinde,

Gerek bir şirketler grubuna borçlu olduğu belirtilen ve şikayetçinin yeğeni olduğu anlaşılan şahsa ait ad, soyad ve hizmet numarasının şikayetçiye ait hatta gönderilmesi, gerekse şikayetçiye ait telefon numarasının, Kanunda düzenlenen işleme şartlarından herhangi birine dayanmadan işlenmesi şeklindeki tek bir harekete bağlı iki farklı veri işleme faaliyeti sonucunda Kanunun 12 nci maddesinin birinci fıkrasının (a) bendinde öngörülen "Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek" yükümlülüğünü yerine getirmediği anlaşılan veri sorumlusu avukat hakkında, Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 50.000 TL idari para cezası uygulanmasına karar verilmiştir.

2019/162 sayılı KVKK Kararı

Bir anonim şirketin (veri sorumlusu) ilgili kişinin açık rızası dışı elektronik ticari ileti göndermesine ilişkin Kişisel Verileri Koruma Kurulunun 31.05.2019 Tarihli ve 2019/162 Sayılı Karar Özeti

Karar Tarihi : 31.05.2019

Karar No : 2019/162

Konu Özeti : Bir anonim şirketin (veri sorumlusu) ilgili kişinin açık rızası dışı elektronik ticari ileti göndermesine ilişkin şikâyet hakkında

• Veri sorumlusu tarafından şikâyetçiye ait telefon numarasına reklam amaçlı bir kısa mesajın (SMS) gönderilmesi üzerine ilgili kişinin kişisel verilerinin nasıl ve nereden temin edildiğini bilmemesi ve buna ilişkin olarak da kişisel verilerinin açık rızası olmaksızın kullanılması dolayısıyla veri sorumlusundan 6698 sayılı Kişisel Verilerin Korunması Kanununa (Kanun) istinaden bilgi talebinde bulunduğu ancak yasal süre içerisinde tarafına herhangi bir cevap verilmediği,

• Kanun kapsamında veri sorumlusuna yaptığı başvuruya yasal süresi içerisinde cevap verilmemesi neticesinde de Kurula şikâyette bulunduğu ve bu başvurusunda (1) Veri sorumlusu nezdinde kendisine reklam/bildirim içerikli SMS gönderimi konusunda herhangi bir açık rızasının olup olmadığı, (2) kişisel verilerinin işlenip işlenmediği, işlenmişse ne amaçla işlendiği, (3) kişisel verilerinin yurt içinde kimlere aktarıldığı, (4) kişisel verilerinin yurt dışına aktarılıp aktarılmadığı, aktarılmış ise kimlere aktarıldığı, (5) gelen SMS'lerden Şirketin haberdar olup olmadığı hususlarında bilgi almak istediği,

şeklindeki talepler birlikte incelenmiş ve yapılan inceleme neticesinde,

- Şikâyetçinin kişisel verisi olan cep telefonu numarası bilgisinin Şirket tarafından kendisine reklam içerikli mesaj gönderilmesi suretiyle kullanılmasının, kişisel verilerin korunması mevzuatı açısından bir veri işleme faaliyeti olduğu, veri işlemenin ise Kanunun 5 ve 6. maddelerinde yer alan işleme şartlarında birine dayanması gerektiğini, ancak şikâyet konusu mesaj gönderiminin herhangi bir işleme şartına dayanmadığı değerlendirildiğinden , kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari

tedbirleri almadığı için veri sorumlusu hakkında Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendinde aykırı davranmış olması nedeniyle Şirket hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 50.000 TL idari para cezası uygulanmasına karar verilmiştir.

2019/159 sayılı KVKK Kararı

Bir varlık yönetim şirketinin ilgili kişiye aynı konu ile ilgili birden çok mesaj gönderimine ilişkin Kişisel Verileri Koruma Kurulunun 31/05/2019 Tarihli ve 2019/159 Sayılı Karar

Karar Tarihi : 31.05.2019

Karar No : 2019/159

Konu Özeti : Bir varlık yönetim şirketinin ilgili kişiye aynı konu ile ilgili birden çok mesaj gönderimine ilişkin Kurul kararı

İlgili kişinin,

- Veri sorumlusu varlık yönetim şirketi tarafından ilgili kişiye ait telefon numarasına açık rızası olmaksızın kısa mesajların (SMS) gelmesi ve SMS'lerde ret bildiriminin bulunmaması, ayrıca Şirketin, kişisel verilerini nereden, kimlerden ve nasıl temin ettiğini bilmemesi,
- 6698 sayılı Kişisel Verilerin Korunması Kanununun (6698 sayılı Kanun) ilgili maddelerine istinaden veri sorumlusuna yapmış olduğu başvurusuna herhangi bir cevap alamaması sebebiyle Kişisel Verileri Koruma Kuruluna (Kurul) şikayette bulunması üzerine yapılan inceleme neticesinde,
- Şikayetçinin yapmış olduğu ve veri sorumlusu tarafından teslim alınan bilgi talebi başvurusuna 30 günlük yasal süre içerisinde cevap verilmediği iddiasına ilişkin olarak, veri sorumlusundan alınan cevabi yazı ekinde ilgili kişiye cevap verdiği, bu cevabi yazının Şikayetçi tarafından teslim alındığının veri sorumlusu tarafından Gönderi Takibi ile tevsik edildiği ve yazısında Şikayetçinin bilgi talebinde bulunduğu tüm hususlara cevap verdiği dikkate alınarak veri sorumlusu hakkında yapılacak bir işlem olmadığına,
- Şikayetçinin geri ödemesi gerçekleştirilmeyen tahsili gecikmiş alacakların ilgili bankalar ile veri sorumlusu arasında akdedilmiş bulunan sözleşmeler kapsamında 5411 sayılı Bankacılık Kanunu (5411 sayılı Kanun) ve 6098 sayılı Türk Borçlar Kanunu (6098 sayılı Kanun) hükümleri çerçevesinde veri sorumlusu şirketçe devir ve temlik alındığı, Şikayetçinin kişisel verisi olan telefon numarası verisinin veri sorumlusunun, Şikayetçinin ilgili bankalardan kullanmış olduğu kredi borçlarının yeni alacaklısı olması, bu kapsamda 6098 sayılı Kanununun 186 ncı maddesi çerçevesinde borçlunun önceki alacaklılara karşı borcunu ifa etmesinin engellenmesi ve taraflarınca Şikayetçiye sağlanacak kolaylıklar ile borcun ödenmemesi durumunda Şikayetçinin maruz kalabileceği hukuki risklerin

bildirilmesi amacıyla işlenmiş olmasının 6698 sayılı Kanununun 5 inci maddesinin (2) numaralı fıkrasının (e) bendi kapsamında Şikayetçinin açık rızası olmaksızın gerçekleştirilebilir olması nedenleriyle veri sorumlusu hakkında yapılacak bir işlem bulunmadığına,

- Ancak 6698 sayılı Kanun kapsamında kişisel verilerin kullanılmasının da bir veri işleme faaliyeti olduğu, bu anlamda Şirket tarafından ilgili kişinin telefon numarasına aynı içerikteki mesajların farklı tarihlerde birden fazla gönderilmesinin veri sorumlusunun sahip olduğu hakkı kötüye kullanımı olarak değerlendirilmesi ve bu durumun Kanununun 4 üncü maddesinin (2) numaralı fıkrasının (a) bendinde yer alan kişisel verilerin işlenmesinin hukuka ve dürüstlük kurallarına uygun olma ilkesine aykırılık teşkil etmesi, hususları göz önünde bulundurularak, Kanununun 12 nci maddesinin (1) numaralı fıkrasının (a) bendinde yer alan kişisel verilerin hukuka aykırı olarak işlenmesini önlemeye yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanununun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 20.000 TL idari para cezası uygulanmasına karar verilmiştir.

2019/157 sayılı KVKK Kararı

Kurumsal e-posta hizmetinin, Google (gmail) üzerinden yine aynı uzantıya sahip olarak kullanılıp kullanılmayacağı ilişkin Kişisel Verileri Koruma Kurulunun 31/05/2019 Tarihli ve 2019/157 Sayılı Karar

Karar Tarihi : 31.05.2019

Karar No : 2019/157

Konu Özeti : Kurumsal e-posta hizmetinin, Google (gmail) üzerinden yine aynı uzantıya sahip olarak kullanılıp kullanılmayacağı ilişkin başvuru hakkında

Veri sorumlusunun ücretsiz bir kurumsal e-posta hizmeti sunan açık kaynak kodlu Zimbra aracılığıyla uzantılı kurumsal e-posta adreslerinin, Google (gmail) üzerinden yine aynı uzantıya sahip olarak kullanılıp kullanılmayacağı hususunda Kurumumuz görüşlerini talep eden yazısının incelenmesi neticesinde Kurul tarafından,

Google firmasına ait G-mail e-posta hizmeti altyapısının kullanılması durumunda gönderilen ve alınan e-postaların dünyanın çeşitli yerlerinde bulunan veri merkezlerinde tutulması söz konusu olacağından, böyle bir durumda kişisel verilerin yurt dışına aktarılmış olacağına ve veri sorumlularının söz konusu uygulamayı 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) "Kişisel verilerin yurt dışına aktarılması" başlıklı 9 uncu maddesi hükümlerine uygun olarak gerçekleştirmesine;

"Server"ları yurt dışında bulunan veri sorumlularından/veri işleyenlerden temin edilen saklama hizmetlerinin de Kanunun 9 uncu maddesi hükümlerine uygun olarak gerçekleştirilmesine

karar verilmiştir.

2019/144 sayılı KVKK Kararı

Cathay Pasific Airway Limited Hakkında Kişisel Verileri Koruma Kurulunun 16.05.2019 Tarih ve 2019/144 Sayılı Karar Özeti

Karar Tarihi : 16.05.2019

Karar No : 2019/144

Konu Özeti : Cathay Pasific Airway Limited'in veri ihlal bildirimini hakkında bilgilendirme

Cathay Pasific Airway Limited'in (Cathay Pasific) 25.10.2018 ve 08.03.2019 tarihlerinde Kurumuza intikal eden yazılarında özetle;

- 13.03.2018 tarihinde bilgisayar ağları üzerinden yolcu bilgilerini içeren bilgi sistemlerine yetkisiz erişim gerçekleştiği,
- Şirket tarafından yapılan inceleme sonucunda yetkisiz erişimin 07.05.2018 tarihinde tespit edildiği,
- Saldırganın Cathay Pasific'in ortamına uzaktan eriştiği ve Müşteri Sadakat Sisteminin kısmi veri tabanı yedeği olarak hitap edilebilecek belgeleri ele geçirdiği,
- Saldırgan tarafından, müşteri ödemesi ile işlem verisini görmek ve veri tabanının yedeğini dışarı almak amacıyla web sitesi yönetici konsoluna ulaşıldığı,
- Cathay Pasific tarafından yapılan inceleme sonucunda ihlalin yetkisiz erişim nedeniyle olduğu ve kullanılan araç, taktik ve prosedürlere dayanarak iki farklı grubun saldırısı olabileceğinden şüphelenildiği,
- Birinci Grup'un BRIO sunucusunu Müşteri Bilgi Sistemine ulaşmak için kullandığı,
- Cathay Pasific'in Birinci Grup'un Cathay ağına zorla girişini belirleyemediği,
- Birinci Grup'un ağ içerisinde yanlamasına hareket ettiklerinden şüphelenildiği,
- İkinci Grup'un Müşteri Sadakat Sistemi ve Online İş Hizmeti Platformunun yedek belgelerine ve web sitesi yönetici konsoluna erişim sağlandığı,

- Bahse konu veri ihlalden Cathay Pacific yolcularının kişisel verilerinin yanı sıra bağlı kuruluşu Hong Kong Dragon Airlines Limited yolcuları ile Asia Miles ve Marco Polo Club üyelerinin kişisel verilerinin de etkilendiği,
- Şirket tarafından yapılan incelemede Türkiye’de toplam 1.286 kişinin söz konusu ihlalden etkilendiği, diğer taraftan Türkiye’de toplam 155 kişinin pasaport numarasına erişildiği,
- Yetkisiz erişim sağlanmış olan kişisel veriler arasında yolcu ismi, uyruğu, doğum tarihi, telefon numarası, elektronik posta adresi, pasaport numarası, kimlik kartı numarası, “frequent flyer” üyelik numarası, müşteri hizmetleri notları ve geçmiş seyahat bilgileri bulunduğu, öte yandan erişilen kişisel veri türü ve sayısının etkilenen her yolcu özelinde değişiklik gösterdiği,
- Veri ihlalden etkilenen ilgili kişilere doğrudan (e-posta vb.) ve web sitesi (“https://infosecurity.cathaypacific.com” adresi üzerinden) üzerinden ulaşmakta oldukları,
- Türkiye’ye özel 1 (bir) aylığına müşteri hizmetleri merkezi ve ücretsiz müşteri hattı ile ilgili kişilere özel “ infosecurity@cathaypacific.com” e-posta adresi tahsis edildiği,

ifadelerine yer verilmiştir.

Söz konusu bildirim incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 16.05.2019 tarih ve 2019/144 sayılı Kararı ile;

- 13.03.2018 tarihinde gerçekleşen ihlale ilişkin, şüpheli hareketlerden Cathay’ın Mart 2018 tarihinde haberdar olmasına rağmen ihlalin yaklaşık 2 ay sonra 07.05.2018 tarihinde tespit edildiği, bu durumun bir güvenlik açığı olduğu, öte yandan Şirket tarafından gerekli denetimlerin ve kontrollerin yapılmadığı,
- Şirket tarafından ihlalden önce alındığı belirtilen güvenlik önlemleri ve bildirim ekinde gönderilen kötücül yazılımların listesi incelendiğinde; saldırganların sistemler üzerinde yatay bir şekilde hareket ederek Müşteri Sadakat Sistemi (CLS), Online İş Hizmeti Platformu (EBSP), web sitesi yönetici konsolu (iRedeem), Müşteri Bilgi Sistemi’ni (CIS) etkilenmesinin Şirket bünyesinde bulunan donanım ve yazılımların yapılandırmalarının doğru bir şekilde yapılmadığının ve alınan güvenlik önlemlerinin yetersiz olduğunun göstergesi olduğu

hususları dikkate alınarak

- 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari ve tedbirleri almayan Şirket hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 450.000 TL,

- Öte yandan Şirket tarafından 07.05.2018 tarihinde gerçekleşen siber saldırıya ilişkin Kurula 25.10.2018 tarihinde bildirim yapılmasının, ihlalden etkilenen ilgili kişilere ise 25.10.2018 tarihinden itibaren bildirim yapmaya başlanmasının, Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen "en kısa sürede" bildirimde bulunma yükümlülüğüne aykırılık teşkil etmesi nedeniyle, Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca Şirket hakkında 100.000 TL, olmak üzere toplam 550.000 TL idari para cezası uygulanmasına, karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2019/143 sayılı KVKK Kararı

Marriott International Inc. Hakkında Kişisel Verileri Koruma Kurulunun 16.05.2019 Tarih ve 2019/143 Sayılı Karar Özeti

Karar Tarihi : 16.05.2019

Karar No : 2019/143

Konu Özeti : Marriot International Inc.'nin veri ihlal bildirimini hakkında bilgilendirme

Marriott International Inc'in (Marriott) 04.12.2018 ve 28.03.2019 tarihlerinde Kurumumuza intikal eden yazılarında özetle;

- 2016 yılı Eylül ayında Marriott'un önceden halka açık ve ayrı bir konaklama şirketi olan Starwood Hotels & Resorts Worldwide Inc'i (Starwood) devralma işlemi gerçekleştirdiği,
- Starwood otel markaları arasında St. Regis, Sheraton Hotel & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton and Design Hotels'in bulunduğu,
- Starwood misafir veritabanının tutulduğu ağa Temmuz 2014'ten beri yetkisiz erişim olduğu,
- Starwood misafir veritabanına yetkisiz erişimin 08.09.2018'de tespit edildiği,
- Starwood müşteri rezervasyon veri tabanının Marriott otelleri için değil sadece Starwood otellerindeki rezervasyonlar için kullanıldığı,
- Marriott'un yaklaşık 383 milyon müşteri kaydı arasında ülke/bölge adresi Türkiye olan yaklaşık 1.24 milyon müşteri kaydının bulunduğu,
- Saldırganın web sunucusuna bir komut istemi yüklediği ve Starwood ağına girdiğinin Marriot tarafından tespit edildiği,
- Web sunucusuna erişimin sağlanmasının ardından, saldırgan tarafından web sunucusuna uzaktan erişim sağlayan bir truva atı (RAT) yüklendiği,

- İhlal hakkında otel müşterilerini aydınlatmak için, özel bir web sitesinin (info.starwoodhotels.com) kurulduğu

ifadelerine yer verilmiştir.

Söz konusu bildirim incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 16.05.2019 tarih ve 2019/143 sayılı Kararı ile;

- Starwood otel markaları arasında Türkiye’de faaliyet gösteren, St. Regis, Sheraton Hotel & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton and Design Hotels’in bulunduğu,

- İhlalden etkilenen veri tabanının tutulduğu Starwood Hotels ağına 2014'ten beri yetkisiz erişim olduğu, 2016 yılı Eylül ayında Marriott’un önceden halka açık ve ayrı bir konaklama şirketi olan Starwood’u devralma işlemi gerçekleştirdikten sonra da ihlalin 19.11.2018 tarihine kadar yaklaşık 4 yıl sürmesinin çok ciddi bir güvenlik açığı olduğu ve Şirket tarafından gerekli denetimlerin ve kontrollerin yapılmadığının göstergesi olduğu,

- İhlalden etkilenen veriler arasında müşterilere ait ad, soyad, posta adresi, telefon numarası, doğum tarihi, cinsiyet, pasaport numarası, Starwood Preferred Guest (“SPG”) hesap bilgileri, otel ödül bilgileri, otele giriş ve çıkış bilgileri, ödeme kartı numaraları ve ödeme kartı son kullanma tarihleri, rezervasyon tarihi ve iletişim tercihlerini içeren bilgilerin olduğu,

- Sistemde şifrelenmiş ödeme kartı bilgilerinin yanında çok sayıda şifrelenmemiş ödeme kartı numaralarının da bulunmasının sistemin tasarım aşamasından itibaren doğru bir şekilde planlanmadığı ve gerekli kontrollerin yapılmadığının göstergesi olduğu, bu durumun ilgili kişiler açısından olumsuz etki oluşturabilecek bir güvenlik açığı olduğu,

- İhlalden etkilenen müşterilere ait bilgiler arasında ülke/bölge adresi Türkiye olan yaklaşık 1.24 milyon müşteri kaydının bulunduğu, ancak aynı müşteri için birden fazla kayıt bulunduğu için ihlalden etkilenen Türk müşterilerin sayısının tam olarak tespit edilemediği,

- Saldırmanın web sunucusuna bir komut istemi yükleyerek Starwood ağına girdiğinin tespit edildiği ve web sunucusuna erişimin sağlanmasının ardından, saldırgan tarafından web sunucusuna uzaktan erişim sağlayan bir truva atı (RAT) yüklendiği, saldırganın daha sonra kimlik bilgilerini toplayan ilave araçlar yüklediği ve sonrasında Starwood ağındaki diğer cihazlara erişim sağlayabilmek için kimlik bilgilerini ve iç ağ bağlanabilirliğini kullandığının tespit edilememesinin alınan teknik ve idari tedbirlerin yetersizliğinin göstergesi olduğu,

- 2014 yılından itibaren mevcut olan yetkisiz erişim ve komut isteminin kurulumunu gösteren web olay günlüklerinin (log kayıtları) olmasına rağmen, olayın tespit edilememesinin Şirket tarafından alınması gereken teknik ve idari tedbirlerin alınmadığının somut bir göstergesi olduğu

hususları dikkate alınarak

- 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari ve tedbirleri almayan Şirket hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 1.100.000 TL,

- Şirket tarafından 08.09.2018 tarihinde tespit edilen ihlale ilişkin Kuruma 03.12.2018 tarihinde bildirim yapılmasının, ihlalden etkilenen kişilere ise 30.11.2018 tarihinden sonra bildirimde bulunulmaya başlanmasının, Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen “en kısa sürede” bildirimde bulunma yükümlülüğüne aykırılık teşkil etmesi nedeniyle, Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca Şirket hakkında 350.000 TL,

olmak üzere toplam 1.450.000 TL idari para cezası uygulanmasına,

karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2019/141 sayılı KVKK Kararı

Clickbus Seyahat Hizmetleri A.Ş. Hakkında Kişisel Verileri Koruma Kurulunun 16.05.2019 Tarih ve 2019/141 Sayılı Karar Özeti

Karar Tarihi : 16.05.2019

Karar No : 2019/141

Konu Özeti : Clickbus Seyahat Hizmetleri A.Ş.'nin veri ihlal bildirimini hakkında bilgilendirme

Clickbus Seyahat Hizmetleri Anonim Şirketi'nin 07.02.2019 ve 29.03.2019 tarihlerinde Kurumumuza intikal eden yazılarında özetle;

- Clickbus tarafından Amazon Web Services (AWS) tarafından internet sistemlerinden biri üzerinde zararlı bir işlem olabileceğine ilişkin aldığı uyarı üzerine, internet platformları ile bağlantılı bazı şüpheli faaliyetlerin tespit edildiği,
- Clickbus tarafından, bilgi sistemlerinde veri güvenliğini tehlikeye sokabilecek faaliyetlerden şüphelenilerek, alanında uzman adli bilişim uzmanlarının yardımları ile iç inceleme başlatıldığı,
- Clickbus'ın görevlendirdiği adli bilişim uzmanlarının yaptıkları inceleme ile ilgili nihai bir rapor oluşturulduğu,
- Clickbus'ın adli bilişim uzmanlarının yardımlarını alarak gerçekleştirdiği ön incelemede, incelenen sunucularda bazı zararlı dosyaların bulunduğu ve bazı meşru kaynak kod dosyalarının Clickbus'ın sunucularına uzaktan erişim sağlanmasına izin veren zararlı kodları içerecek şekilde modifiye edildiğinin tespit edildiği,
- Clickbus'ın AWS sisteminde yer alan log ve sistemler üzerinde yaptığı analiz sonrasında, Clickbus kaynaklarından veri sızıntısının 25 Eylül 2018'den 25 Kasım 2018'e kadar geçen sürede gerçekleştiği sonucuna varıldığı ifadelerine yer verilmiştir.

ifadelerine yer verilmiştir.

Söz konusu bildirim incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 16.05.2019 tarih ve 2019/141 sayılı Kararı ile;

- Söz konusu ihlalden Türkiye'de yerleşik 67.519 kişinin etkilendiği,

- İhlalden etkilenmiş kişilerin farklı kategorilerde ve sayıda kişisel verileri arasında kimlik bilgileri (cinsiyet, ad, soyad, T.C. kimlik numarası, doğum tarihi), iletişim bilgileri (cep telefonu ülke kodu, cep telefonu numarası, sabit hat ülke kodu, sabit hat numarası, sabit hat uzantısı/dahilisi, e-posta adresi, sms gönderi izni, ticari elektronik ileti izni), müşteri işlemleri (ödeme anahtarı, yolculuk numarası, sepet numarası, sipariş numarası, toplam tutar, seyahat türü/kullanılacak araç, kalkış/varış yer ve saati, yolcu başına ücret referans numarası, yolcu türü, oturum simgesi, hata sebebi (uygulanabilir olduğu ölçüde hangi doğrulama adımının hataya sebep verdiği), segmentler), işlem güvenliği bilgileri (ödeme bilgileri; kart üzerinde yazan isim, kart numarası, kartın son kullanma tarihindeki ay ve yıl, kart güvenlik kodu, taksit bilgisi, indirim kodu, seyahat sigortası alınıp alınmadığına ilişkin bilgi, site kullanım koşullarının kullanılma bilgisi) verilerinin olduğu,
- İhlalin 25 Eylül 2018'den 25 Kasım 2018'e kadar geçen dönemde 2 (iki) ay boyunca devam etmesinin Şirket tarafından gerekli denetimlerin ve kontrollerin yapılmadığının göstergesi olduğu,
- İhlalin 21 Kasım 2018 tarihinde tespit edilmesine rağmen 25 Kasım 2018 tarihine kadar 4 (dört) gün daha devam etmesinin Şirket tarafından alınan idari tedbirlerin yeterince alınmadığının göstergesi olduğu,
- Söz konusu yetkisiz kişi veya kişilerin ayrıca Şirketin kaynak koduna (source code) ulaşarak değişiklik yapmasının ciddi bir güvenlik açığı olduğu

hususları dikkate alınarak

- 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari ve tedbirleri almayan Şirket hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 450.000 TL,

- Öte yandan Şirket tarafından 21.11.2018 tarihinde tespit edilen siber saldırıya ilişkin Kurula 07.02.2019 tarihinde bildirim yapılmasının, ihlalden etkilenen ilgili kişilere ise 25.02.2019 tarihinde bildirim yapılmasının; Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen "en kısa sürede" bildirimde bulunma yükümlülüğüne aykırılık teşkil etmesi nedeniyle Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca Şirket hakkında 100.000 TL,

olmak üzere toplam 550.000 TL idari para cezası uygulanmasına,

karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2019/138 sayılı KVKK Kararı

Bir şirket sahibinin, çalışanın Whatsapp yazışmalarını hukuka aykırı olarak elde etmesi hakkında Kişisel Verileri Koruma Kurulunun 16/05/2019 Tarihli ve 2019/138 Sayılı Karar Özeti

Karar Tarihi : 16.05.2019

Karar No : 2019/138

Konu Özeti : Bir şirket sahibinin, çalışanın Whatsapp yazışmalarını hukuka aykırı olarak elde etmesi hakkında

Şikâyetçinin rızası dışında kendisine ait Whatsapp yazışmalarının, çalıştığı şirketin sahibi tarafından hukuka aykırı olarak elde edilmesi ve üçüncü kişilerle paylaşılmasına ilişkin iddiaları ile ilgili olarak şikayette bulunması üzerine yapılan inceleme neticesinde; Kişisel Verileri Koruma Kurulunun 16/05/2019 tarih ve 2019/138 sayılı Kararı ile;

- Kanununun 15 inci maddesinin (1) numaralı fıkrasında Kişisel Verileri Koruma Kurulunun, şikayet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapacağı; aynı maddenin (2) numaralı fıkrasında ise 1/11/1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanununun 6 ncı maddesinde belirtilen a) Belli bir konuyu ihtiva etmeyen, b) Yargı mercilerinin görevine giren konularla ilgili olan, c) 4 üncü maddede gösterilen şartlardan (dilekçe sahibinin adı soyadı ve imzası ile iş veya ikametgâh adresi) herhangi birini taşımayan ihbar veya şikâyetlerin incelemeye alınmayacağına hükme bağlandığı,

- Diğer taraftan, Kanununun 17 nci maddesinin (1) numaralı fıkrasında kişisel verilere ilişkin suçlar bakımından 26.09.2004 tarih ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümlerinin uygulanacağı belirtilmekte olup, Türk Ceza Kanununun 136 ncı maddesinde kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişinin, iki yıldan dört yıla kadar hapis cezası ile cezalandırılacağına hükme bağlandığı

değerlendirilmelerinden hareketle;

- Şikayet edilenin Whatsapp grubunun kullanıcılarından biri olan bir çalışanın işyerindeki bilgisayarı üzerinden yazışmaları okuyup, fotoğraflarını çekmesinin ve/veya ekran görüntülerini kaydetmesinin TCK kapsamında değerlendirilmesi gerektiği,

- Őikayet edilen tarafından rızası dıŐında kendisine ait Whatsapp yazıŐmalarının hukuka aykırı olarak elde edilmesi ve üçüncü kişilerle paylaşılmasına ilişkin iddiaları ile ilgili olarak; Őikayetçi tarafından Türk Ceza Kanununun ilgili hükümleri kapsamında İstanbul Anadolu Cumhuriyet Başsavcılığına suç duyurusunda bulunulduđu ve sürecin devam ettiđi dikkate alındığında, Kanunun 15 inci maddesinin (1) numaralı fıkrası çerçevesinde ilgili başvurunun Kanun kapsamında değerlendirilemeyeceđine karar verilmiŐtir.

2019/122 sayılı KVKK Kararı

İlgili kişinin yaptığı başvuruyu cevaplandırmayan ve internet sitesi üzerinden yayımladığı aydınlatma metni mevzuatta düzenlenen şartları taşımayan T.C. Ziraat Bankası A.Ş. hakkında Kişisel Verileri Koruma Kurulunun 02/05/2019 tarihli ve 2019/122 sayılı Karar Özeti

Karar Tarihi : 02.05.2019

Karar No : 2019/122

Konu Özeti : İlgili Kişinin T.C. Ziraat Bankası A.Ş.'ye Yaptığı Başvurunun Cevaplandırılmaması ve Veri Sorumlusu Tarafından İnternet Üzerinden Yayımlanan Aydınlatma Metninin Mevzuatta Düzenlenen Şartları Taşımaması Hakkında

6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 11 inci maddesinde belirtilen hakları kapsamındaki taleplerini içeren kayıtlı elektronik posta (KEP) aracılığıyla veri sorumlusu T.C. Ziraat Bankası A.Ş.'ye (Banka) başvuran ancak, Kanunda düzenlenen otuz günlük süre içerisinde başvurusu cevaplandırılmayan ilgili kişinin gerek bu konuda gerekse veri sorumlusunun, internet sitesi üzerinden yayımladığı aydınlatma metninin mevzuatta düzenlenen şartları taşımadığı hususunda Kuruma yapılan şikâyet başvurusu hakkında;

- Şikâyete konu hususlarda açıklamalarına başvurmak üzere Bankaya gönderilen Kurum yazısının "İŞYERİNDE AMİRİNE TESLİM" açıklamasıyla Bankaya teslim edildiği görülmekle birlikte, söz konusu Kurum yazısına bugüne kadar herhangi bir cevap vermeyen Banka nezdinde, Kanunun 18 inci maddesinin üçüncü fıkrası çerçevesinde ihlale sebebiyet veren sorumlular ile gerekli tedbirleri almak ve denetimleri yapmakla yükümlü kişiler hakkında disiplin hükümlerine göre işlem yapılmasına,
- İlgili kişinin Kanunun uygulanmasına yönelik taleplerine ilişkin başvurusuna Banka tarafından cevap verilmesi; ayrıca, mevzuat hükümlerine uyumda azami dikkat ve özen göstermesi hususunda Bankanın talimatlandırılmasına,
- Bankanın internet sitesinde yer alan aydınlatma metninde, Bankanın kişisel veri işleme amaçlarının, ilgili kişilerin kişisel verilerinin Kanunun 5 inci ve 6 ncı maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiğine yönelik hukuki sebep açıkça belirtilmeksizin sıralandığı; kişisel

veri işleme amaçları sıralandıktan sonra metin içerisinde yer verilen “gibi amaçlar kapsamında işlenmektedir” ifadesinin ise, gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandırır nitelikte olduğu; bu çerçevede söz konusu aydınlatma metninin “Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ”in (Tebliğ) 5 inci maddesinin birinci fıkrasının (g) ve (h) bentlerinde yer verilen hükümlere uygun hazırlanmaması nedeniyle, Bankanın internet sitesinde yer alan aydınlatma metninin yeniden gözden geçirilerek Tebliğ hükümlerine uygun hale getirilmesi yönünde talimatlandırılmasına

karar verilmiştir.

2019/104 sayılı KVKK Kararı

Facebook nezdinde gerçekleşen veri ihlalinin değerlendirilmesi ile ilgili Kişisel Verileri Koruma Kurulunun 11.04.2019 tarih ve 2019/104 sayılı Kararı Özeti

Karar Tarihi : 11.04.2019

Karar No : 2019/104

Konu Özeti : Facebook nezdinde gerçekleşen veri ihlalinin değerlendirilmesi

Kamuoyuna yansıyan ve “Fotoğraf API” olarak adlandırılan Facebook veri ihlali, Facebook Mühendislik Direktörü Tomer Bar tarafından 14.12.2018 tarihinde <https://developers.facebook.com/blog/post/2018/12/14/notifying-our-developer-ecosystem-about-a-photo-api-bug/> adresinden “Geliştirici ekosistemimizin bir fotoğraf API’si hatası hakkında bilgilendirme” başlığıyla duyurulmuştur. Duyuruda;

- Facebook kullanıcı fotoğraflarına erişmek için üçüncü taraf uygulamalara izin veren bir fotoğraf API hatası keşfedildiği,
- Sorunun çözüldüğü, ancak bu kusur nedeniyle 13 Eylül - 25 Eylül 2018 tarihleri arasında bazı üçüncü taraf uygulamaların 12 gün boyunca yetkisini aşan düzeyde fotoğraflara erişmiş olabileceği,
- Üçüncü parti bir uygulamaya Facebook platformu üzerinden Facebook kullanıcısı tarafından fotoğraflarına erişim izni verildiğinde sadece zaman çizelgesinde paylaştığı fotoğraflara erişim sağlaması gerekirken, açıklanan kusurdan kaynaklı Marketplace veya Facebook Stories’de paylaşılan diğer fotoğraflara da üçüncü parti uygulamaların erişim sağladığı,
- Ayrıca söz konusu kusurun Facebook kullanıcılarının Facebook’a taslak olarak yüklediği ve henüz paylaşımına açmadığı fotoğrafları da etkilediği,
- Açıklanan kusurun 6,8 milyon kullanıcıyı ve 876 geliştirici tarafından oluşturulan 1.500 uygulamayı etkilemiş olabileceği,
- Açıklanan kusurun, Facebook’un fotoğraf API’sine erişmek için izin alan ve kişilerin fotoğraflarına erişebilen uygulamaları etkilediği,

- Facebook uygulama geliştiricilerinin, uygulamalarını kullanan ve bu kusurdan etkilenen kişileri belirlemelerine imkân sağlayacak araçların geliştirileceği, ifadelerine yer verilmiştir.

Yukarıda ifade edilen durumun “veri gizliliğine/mahremiyetine” aykırı bir husus olması sebebiyle veri ihlali olduğu ve bu ihlalin 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (5) numaralı fıkrasında yer alan “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir...” hükmü uyarınca Facebook tarafından Kurul’a bildirilmesi gerektiği ancak herhangi bir bildirim yapılmadığı tespit edilmiştir. Bunun üzerine, Kanun’un 15 nci maddesinin (1) numaralı fıkrasında yer alan “Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapar.” hükmü kapsamında resen inceleme yapma kararı almıştır.

Yapılan inceleme neticesinde,

- Facebook kullanıcı fotoğraflarına erişmek için üçüncü taraf uygulamalara izin veren bir fotoğraf API hatası keşfedildiği, Facebook tarafından yapılan inceleme sonrası bu durumu potansiyel bir yazılım bozukluğu olarak rapor ettiği,
- API hatasının 13 Eylül - 25 Eylül 2018 tarihleri arasında 12 gün boyunca gerçekleştiği, bahse konu API hatasına Facebook tarafından zamanında müdahale edilmemesi bu konuda teknik ve idari tedbirlerin alınmasında eksikliklerin göstergesi olduğu,
- Üçüncü taraf bir uygulamaya Facebook platformu üzerinden Facebook kullanıcısı tarafından fotoğraflarına erişim izni verildiğinde sadece zaman çizelgesinde paylaştığı fotoğraflara erişim sağlaması gerekirken, açıklanan ihlalden kaynaklı Marketplace veya Facebook Stories’de paylaşılan diğer fotoğraflara da üçüncü taraf uygulamaların erişim sağladığı, ayrıca Facebook kullanıcılarının Facebook’a taslak olarak yüklediği ve henüz paylaşımına açmadığı fotoğraflara da söz konusu üçüncü taraf uygulamaların erişim sağladığı dikkate alındığında, Facebook kullanıcılarının genel olarak izin vermiş olduğu kapasiteden çok daha fazla sayıda fotoğraflara erişim sağlanmasının, Kanunun 12 nci maddesinin (1) numaralı fıkrasına ve 4 üncü maddesinin (2) numaralı fıkrasının (a) bendinde belirtilen “Hukuka ve dürüstlük kurallarına uygun olma” ve (ç) bendinde belirtilen “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkelerine aykırılık teşkil ettiği,
- Facebook’un bahsi geçen üçüncü taraf uygulamaların normalde erişime izin verilmiş olan sayıdan daha fazla spesifik fotoğrafa gerçekten erişip erişemediklerini belirleyemediği dikkate alındığında,

bu durumun Facebook'un kendi platformundaki veri akışını kontrol etme noktasında sıkıntılar yaşadığı ve bu kapsamdaki hususun Kanunun 12 nci maddesinin (1) numaralı fıkrasında öngörülen veri güvenliğine ilişkin yükümlülüklerle aykırılık teşkil ettiği,

- Facebook platformu uygulamaları daha ilk aşamada “Arkadaşların, bağlantıların ve birlikte oyun oynadığın diğer kişiler senin oyun hareketlerini görebilecek. Oyunun senin herkese açık profiline ve bu oyunu oynayan tanıdığın kişilere erişimi vardır” ifadesini kullanarak, kullanıcının arkadaş bilgilerine veya diğer bilgilere kişi istemese bile ulaşabilecek şekilde çalışması hususunda izin almaktadır. İlgili kişilerin uygulamada paylaşmaya izin verecekleri kişisel verilerinin neler olması gerektiği ve yükleme aşamasında gizlilik ayarlarıyla ilgili seçimlere imkân sağlamayarak, kişisel verilerin bu şekilde işlenmesini açık rızaya dayandırmaktadır. Açık rızanın özgür irade ile açıklanması gerektiğinden, ilgili kişinin açık rızasının alınması, bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının ön şartı olarak ileri sürülmemelidir. Bu durumun Kanunun 4 üncü maddesinin (2) numaralı fıkrasının (a) bendine belirtilen “Hukuka ve dürüstlük kurallarına uygun olma” ilkesine aykırılık teşkil ettiği,

- Açıklanan ihlalin 6,8 milyon kullanıcıyı ve 876 geliştirici tarafından oluşturulan 1.500 uygulamayı etkilemiş olabileceği,

- Türkiye’de bulunan yaklaşık 300 bin kullanıcının veri ihlalinin etkilenmiş olabileceği,

- Kamuoyuna yansıyan ve “Fotoğraf API” olarak adlandırılan Facebook veri ihlali, Facebook Mühendislik Direktörü Tomer Bar tarafından 14.12.2018 tarihinde <https://developers.facebook.com/blog/post/2018/12/14/notifying-our-developer-ecosystem-about-a-photo-api-bug/> adresinde söz konusu Facebook uygulamasından kaynaklanan ihlalin “Geliştirici ekosistemimizi bir fotoğraf API'si hatası hakkında bilgilendirme” başlığıyla duyurmasının böyle bir ihlalin varlığı ve Facebook tarafından kabulü anlamına geleceği

hususları dikkate alınarak

1) Yukarıda gerekçeleriyle ortaya konulan durumun bir veri ihlali olduğu ve ihlalin oluşmaması için Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde gerekli teknik ve idari tedbirleri almadığı anlaşılan Facebook hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 1.100.000 TL oy birliğiyle,

2) Söz konusu veri ihlalinin 19.09.2018 tarihinde tespit edilmesine rağmen Kuruma bildirim yapılmadığının ve 13.09.2018 - 25.09.2018 tarihleri arasında gerçekleşen veri ihlalinin ilgili kişilere 17.12.2018 tarihinde bildirilmeye başlandığının tespit edildiği, bu çerçevede Kanunun 12 inci

maddesinin (5) numaralı fıkrasında yer alan en kısa sürede bildirim yapılması gerektiđi hükmüne aykırı hareket eden Őirket hakkında Kanununun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 550.000 TL oy birliđiyle idari para cezası uygulanmasına, karar verilmiŐtir.

2019/82 sayılı KVKK Kararı

Bir market zincirinin sadakat kart uygulamasına ilişkin ihbar ve şikayetler hakkında” Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/82 sayılı Karar Özeti

Karar Tarihi : 25.03.2019

Karar No : 2019/82

Konu Özeti : Bir market zincirinin sadakat kart uygulamasına ilişkin ihbar ve şikayetler hakkında

• Bir marketin mağazalarından temin edilen ve bazı alışveriş/ hizmet alımlarında indirim ve puan biriktirme avantajı sağlayan sadakat kart ile ilgili internet sitesine giriş yapıldığı esnada ekranlara gelen uyarı metninde “..... Kart avantajlarından faydalanmaya devam edebilmek için Kişisel Verilerin Korunması Kanunu kapsamında veri işleme iznini vermen yeterli...iznin yoksa karşına çıkacak olan üyelik ve rıza beyanı metnini okuyarak onayla.” ya da Kart tarafından kişilerin cep telefonlarına gönderilen kısa mesajlarda “Kişisel Verilerin Korunması Kanunu kapsamında izninizi lütfen güncelleyiniz. İzni güncel olmayan müşterilerimiz, kişisel bilgileri silineceği için kasalarımızdan cep telefonu söyleyerek alışveriş yapamayacaklar.” şeklinde açıklamalara yer verildiği, bu anlamda açık rızanın bir ürün veya hizmetin sunulmasına ilişkin koşul olarak ileri sürüldüğünden bahisle 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gerekli işlemlerin tesis edilmesi talebiyle Kuruma yapılan şikayet,

• Buna ilaveten Kuruma söz konusu market tarafından düzenlenen perakende satış fişlerinde, sadakat kart kullanımı ile ilgili Kanun kapsamında müşterilerden açık rıza alınması esnasında “Veri İzni Alma Uygulaması” adı altında 0,01 TL hizmet bedeli alındığı yolunda Kuruma intikal eden ihbarlar

• Öte yandan, yukarıda yer verilen hususlara ilişkin olarak yapılan değerlendirme esnasında söz konusu sadakat karta ilişkin olarak internet sitesinde yayımlanan “.... Kart Üyelik ve Rıza Beyanı” başlıklı metinde, “Üye; Program kapsamında otomatik ve otomatik olmayan yollarla edinilen mevcut ve/veya yeni kişisel bilgilerinin (Alışveriş bilgisi, isim, soyisim, rumuz, cep telefon numaraları, e-mail adresleri, doğum tarihi, yaşadığı şehir, cinsiyet, medeni durum, eğitim düzeyi, ilgi alanları, zevk ve beğenileri gibi) ve elektronik programlar nedeniyle ulaşılabilen lokasyon bilgisinin, kişisel olmayan

bilgilerinin, Program kapsamında mal ve hizmetlerini tanıtmak, üyelerini tanımak ve iletişimini arttırmak, imajını arttırmak, ürün, hizmet ve iletişimini geliştirmek, kulüplere üye kaydetmek, müşteri memnuniyeti uygulamaları ve bilgilendirmeleri yapabilmek, denetim, veri analizi, araştırma, trendleri anlama, pazarlama ve reklam hizmetlerinde de kullanılmak üzere toplanmasına, veri kayıt sisteminde muhafaza edilmesine, sayılan amaçlarla Ailesi ile “yurtiçinde ve yurtdışında ilgili yasal mevzuatın öngördüğü azami süreleri aşmamak üzere paylaşılmasına ve işlenmesine izin verir. Ailesi olarak bahsedilen kurumlar, Yönetim Hissedarları, Yönetim Hissedarlarının ve Şirket’in bağlı şirketleri, iştirakleri, alt kuruluşları, işletmeleri, Şirketin her türlü temsilcisi, hizmet sağlayıcısı ve/veya alt yüklenicisi ve bağlı şirketleri, GSM Operatörleri /Sosyal Paylaşım Siteleri ile Şirketin hak ve/veya görevlerini devretmeyi teklif ettiği her türlü kişilerdir.” gibi genel nitelikte ifadeler

birlikte incelenmiş ve yapılan inceleme neticesinde,

- Müşterinin Sadakat Kart Programına üye olmadığı durumda Şirketin sunduğu ürüne ve kişiye özel fırsat dünyasından faydalanamadığı ancak bu durumun hiçbir şekilde herhangi bir müşterinin Şirketin sunduğu alışveriş ortamından faydalanmasını engellemediği dolayısıyla, veri sorumlusu Şirket tarafından hizmet sunumu kapsamında Sadakat Kart Programına katılımın müşteriler açısından zorunlu tutulmadığı, söz konusu Programa üye olmayan müşterilere hizmet sunulmaması gibi bir durum ortaya çıkmadığı dikkate alındığında, Sadakat Kart Programına üye olunması sırasında kişilerin açık rızalarına başvurulması aksi takdirde söz konusu programdan yararlanılmaması hususunda Şikayetçinin Şirket tarafından bir hizmet veya ürün sunulmasının açık rıza şartına bağlandığı iddiası ile ilgili Kurumca yapılacak bir işlem bulunmadığına,
- Şirketten alınan savunmada, öncelikle Kanuna uygun üyelik onayları teyit edilemeyen müşterilere özel olarak 07.04.2018 tarihine kadar çeşitli kanallardan duyuru yapılan kişilerin daha öncesinde rızalarının alınmadığı değil, yıpranmış, eksik, imzasız vs. gibi durumlar ile karşılaşılması nedeniyle ileride doğabilecek hukuki ihtilaflarda ispat külfeti kapsamında söz konusu rızaların yenilenmesi yoluna gidildiğinin ifade edildiği, bu çerçevede, Şirket tarafından hukuka uygun olmayan bir şekilde elde edilen kişisel verilere hukuki meşruiyet kazandırılması için ilgili kişilerden açık rıza alınması şeklinde bir yola başvurulmadığı, aksine daha önce kişisel verilerin işlenmesine yönelik alınan rızalara ilişkin matbu formlardaki muhtelif eksiklik ya da tahrifatlar nedeniyle bu rızaların iki yıl içinde Kanun hükümlerine uyumlu hale getirilmesinin amaçlandığı dikkate alındığında, Kanunun Geçici 1 inci maddesinin (3) numaralı fıkrası çerçevesinde Kurumca yapılacak bir işlem bulunmadığına,

- “Aydınlatma Metni”nin incelenmesinden ucu açık ifadeler yer verildiği, öte yandan Sadakat Kart Programına üye olunması aşamasında elde edilen kişisel veriler ve bunların aktarıldığı taraflar hususları başta olmak üzere, “Üyelik ve Rıza Metni” ile “Aydınlatma Metni” arasındaki tutarsızlıklar bulunduğu, nitekim, elde edilen kişisel verilerin sosyal paylaşım siteleri ile paylaşılacağı hususunda kişilerin aydınlatılmasına rağmen yapılan güncelleme neticesinde “Üyelik ve Rıza Beyanı”nda bu ifadenin metinden çıkarılması ile birlikte söz konusu paylaşım için kişilerin açık rızalarının alınmadığı bir durumun oluşmasına sebebiyet verildiği,
- Ayrıca, aydınlatma metninde Şirketleri tarafından özel nitelikli kişisel verilerin de (sendika/dernek/vakıf üyeliklerine ilişkin bilgiler, ceza mahkûmiyeti, güvenlik tedbirleriyle ilgili veriler, cinsel hayat, biyometrik veri ve sağlık durumunuza ilişkin bilgiler gibi) işlenebileceği ifadelerine yer verildiği görülmüş olup, Şirketin temel faaliyet alanının gıda ve ihtiyaç maddelerinin perakende olarak tüketicilere ulaştırılması olduğu, Şirkete ait tüm işyerlerinde sunulan Sadakat Kart uygulamasının ise bir pazarlama programı olarak tasarlandığı dikkate alındığında, ceza mahkûmiyeti, güvenlik tedbirleriyle ilgili veriler gibi özel nitelikli kişisel verilerin işlenmesinin veri sorumlusunun faaliyetleri kapsamında amaçla bağlantılı, sınırlı ve ölçülü olmadığı değerlendirildiğinden, “Üyelik ve Rıza Beyanı” ile “Aydınlatma Metni” arasındaki tutarsızlıkların giderilmesi ve Şirketin Aydınlatma Metninin Kanununun temel ilkeleri ve Tebliğ hükümleri de dikkate alınmak suretiyle güncellenmesi gerektiği hususunda Şirketin talimatlandırılmasına,
- Öte yandan, Şirketin savunmasında kişisel verilerin anonim hale getirilerek sosyal paylaşım sitelerine aktarıldığı ifadelerine yer verildiğinin görüldüğü, bununla birlikte Kanunun 3 üncü maddesinde anonim hale getirmenin: kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi olarak tanımlandığı, bu kapsamda, anonim veriler diğer bir ifade ile kişiler ile ilişkilendirilemeyecek veriler üzerinden kişiye özel bir pazarlamanın gerçekleştirilemeyeceği göz önüne alındığında, Şirket uygulamasının Kanunda yer alan anonimleştirme tanımı ile bağdaşmadığına bu nedenle anonimleştirmenin Kanuna uygun olarak gerçekleştirilmesi gerektiği yönünde Şirketin talimatlandırılmasına,
- Son olarak, Şirket tarafından düzenlenen perakende satış fişlerinde, “Veri İzni Alma Uygulaması” altında 0,01 TL hizmet bedeli alındığı iddiaları kapsamında Şirketten alınan savunmada, müşterilere kasada alışveriş yaparken gerekli bilgiyi vermek ve dilerse açık rızasını verebileceği üyelik linkini SMS gönderebilmek için alışveriş kasalarına bilgi teknolojileri sistemi kurulduğu, bir teknik problem nedeni ile bazı fişlerde çalışmadığı ve müşterilere sehven 1 kuruşluk bir bedel yansıdığı, bilgi

teknolojileri hatası nedeni ile gerçekleşen bu olayda müşterilerden toplamda 91.502 fişte 910,52 TL'lik ücret alındığı ancak bu ödemelerin telafisi olarak müşterilerin kartına aynı tutarda indirim yüklendiği ve sistemsal bir hatadan kaynaklanan bu durumun derhal telafi edildiği hususları dikkate alındığında, konuya ilişkin Kanun kapsamında Kurumca yapılacak bir işlem bulunmadığına karar verilmiştir.

2019/81, 2019/165 sayılı KVKK Kararı

Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Karar

Karar Tarihi : 25.03.2019 ve 31.05.2019

Karar No : 2019/81 ve 2019/165

Konu Özeti : Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kurul Kararları

Konu Özeti

Spor salonu hizmeti sunan iki ayrı şirketin (veri sorumluları), üyelerinin giriş-çıkış kontrolünde el-avuç okutma sistemine geçilmesi, kaydı tutulan üyelere ait vesikalık fotoğraf, son ziyaret saati gibi bilgilerin herkesin görebileceği bir TV ekranında yansıtılması gibi biyometrik verileri de içeren bazı özel nitelikli kişisel verileri işlemesi ve bu bilgilerin güvenli şekilde muhafaza edildiğinden şüphe duyulması üzerine ilgili kişilerce Kuruma intikal ettirilen muhtelif ihbar ve şikayetlerin incelenmesi neticesinde yapılan değerlendirmede:

1- 6698 sayılı Kanunun “Özel nitelikli kişisel verilerin işleme şartları” başlıklı 6 ncı maddesinde kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerinin özel nitelikli kişisel veri olarak belirlendiği, özel nitelikli kişisel veriler arasında yer alan biyometrik veri tanımına ise Kanunda yer verilmemekle birlikte, 25.05.2018 tarihinde yürürlüğe giren Avrupa Genel Veri Koruma Tüzüğünde (GDPR) biyometrik verinin; “yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemekten kaynaklanan kişisel veriler” olarak tanımlandığı,

GDPR’ın Recital bölümünün 51 inci maddesinde de biyometrik verilerle ilgili açıklamalara yer verildiği ve fotoğrafların işlenmesinin doğrudan biyometrik veri olarak nitelendirilemeyeceği, yalnızca gerçek bir kişinin benzersiz bir şekilde tanımlanmasına veya doğrulanmasına izin veren

belirli bir teknik yöntemle işlendiğinde, bu verilerin biyometrik verilerin tanımı kapsamında kabul edileceği açıklamalarına yer verildiği, dolayısıyla bir verinin biyometrik veri kapsamında değerlendirilebilmesi için o verinin sadece o kişiyi tanımlayabilme ya da doğrulayabilme özelliğine sahip olmasının kriter alındığının değerlendirildiği,

Danıştay 15. Dairenin 2014/4562 Esas sayılı kararında ise biyometrik yöntemlerin, ölçülebilir fizyolojik ve bireysel özellikleri aracılığıyla gerçekleştirilen ve otomatik şekilde doğrulanabilen kimlik denetleme tekniklerini ifade ettiği belirtilerek, bu yöntemler arasında parmak izi tanıma, avuç içi tarama, el geometrisi tanıma, iris tanıma, yüz tanıma, retina tanıma, DNA tanıma gibi yöntemlerin bulunduğu ifade edildiği

hususlarından hareketle bir spor tesisine giriş esnasında el ve parmak izinin taranması suretiyle kişilerin kimlik doğrulamasının yapılması hususunda adı geçen veri sorumlusunun özel nitelikli kişisel veri niteliğindeki biyometrik veri işleme faaliyetinde bulunduğu değerlendirildiği,

2- a) Kanunun "Genel İlkeler" başlıklı 4 üncü maddesinde de, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin ancak hukuka ve dürüstlük kurallarına uygun şekilde, belirli, açık ve meşru amaçlar kapsamında, doğru ve gerektiğinde güncel olma şartıyla, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceği,

Bu ilkelerden, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesinin, işlenen verilerin belirlenen amaçların gerçekleştirilebilmesine elverişli olması, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirdiği, sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik olarak veri işlenmesi yoluna gidilmemesi gerektiği,

Ölçülülük ilkesinin ise, veri işleme faaliyeti ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması, diğer bir ifadeyle veri işlemenin amacı gerçekleştirecek ölçüde olması anlamına geldiği, bu kapsamda, kişisel veri işleme faaliyetinin gerçekleşmesi için gerekli olmayan kişisel verilerin toplanmaması ve/veya işlenmemesi gerektiği, veri sorumlusunun amacı çerçevesinde ölçülülük ilkesine uygun olarak ilgili kişiden minimum düzeyde bilgi talep etmesi, bunun dışındaki amaç için gerekli olmayan veri işlemeden kaçınması gerektiği, kişisel verilerin işlenmesinin ilgili kişinin iznine bağlı olarak gerçekleştirilse ve belirli bir amaca bağlı olsa bile açık rızanın, aşırı miktarda veri toplanmasını meşrulaştırmayacağı, buna göre kişisel verilerin yalnızca belirli amaçlar

için ve gerektiği kadar toplanması, amacın gerektirdiği yerlerde kullanılması ve amaç için gerekli olandan uzun süre tutulmaması gerektiği,

Nitekim Danıştayın 2017/816 Esas sayılı kararında, davalı idarenin toptancı hali biriminde görev yapan personelin mesai takibinin sağlanması amacıyla başlatılan yüz tarama sistemi uygulamasına son verilmesi talebinin ilgili İdare Mahkemesinde reddedilmesi işleminin iptali istemiyle açılan davada, davalı idarenin tüm birimlerinin mesai takibinde anılan yöntemin kullanılmadığı, uygulamanın gerçekleştirildiği birimin konumu ve vardiyalı çalışma sistemi sebebiyle personelin kontrol ve denetiminde güçlük yaşanması karşısında bahse konu uygulamaya geçildiği, yüz tanıma sisteminde personelin yüz görüntüsünün sayısal kodlara çevrilerek karşılaştırma yapmak suretiyle çalıştığı göz önünde bulundurulduğunda yapılan uygulamanın veri kaydetme olarak nitelendirilemeyeceği gerekçesiyle hukuka aykırı bulunmadığı sonucuna varılan davaya konu işlemin iptali istemiyle açılan davanın İdare Mahkemesince reddi yönündeki kararı hukuka uygun bulunmadığı,

Yine Danıştayın 2014/2242 Esas sayılı, 2014/4562 Esas sayılı kararlarında da “parmak izi ya da yüz tarama sistemi” gibi biyometrik yöntemlerin, kamusal alan da olsa “özel hayatın gizliliği” ilkesi kapsamında bulunduğu ve toplanan verilerin ileride başka bir şekilde kullanılmayacağına dair bir güvencenin mevcut olmadığı göz önünde tutularak hukuka aykırı bir işlem olarak değerlendirildiği, Benzer şekilde, Avrupa İnsan Hakları Mahkemesi de 4 Aralık 2008 tarihli S. ve Marper / Birleşik Krallık kararında kişilere ait parmak izi, hücre örneği ve DNA profillerinin saklanması, başvuru sahiplerinin özel yaşamının gizliliği hakkına yönelik orantısız, aşırı bir müdahale olduğu ve demokratik bir toplumda gerekli bir müdahale olarak kabul edilemeyeceğini vurgulayarak uygulamanın Avrupa İnsan Hakları Sözleşmesinin 8 inci maddesini ihlal ettiğine hükmettiği,

Öte yandan, Article 29 Working Party tarafından hazırlanan WP193 sayılı “Opinion 3/2012 on Developments in Biometric Technologies” başlıklı dokümanda, yer alan örnekte bir fitness kulübüne ya da spor salonuna sadece üyelerin girişini ve ilgili hizmetlere erişimini sağlamak için tüm müşterilerin ve personelin parmak izinin depolanarak işlenmesi, kulübe erişimi kolaylaştırma ve abonelikleri yönetme ihtiyacı ile orantısız olarak değerlendirildiği ve böyle bir uygulama yerine, basit bir kontrol listesi ya da RFID etiketlerinin kullanımı ya da biyometrik verilerin işlenmesini gerektirmeyen bir manyetik bantlı kart gibi farklı önlemler kullanılarak da aynı ihtiyaçların karşılanabileceği ifadelerine yer verildiği

dikkate alındığında spor salonuna giriş için veri sorumluları tarafından uygulanan “el ve parmak izi taraması” sisteminin, hizmetten faydalanmak için zorunlu ve tek yol olarak üyelere sunulmasının,

kişisel verilerin işlenmesinde ölçülülük ilkesi ışığında ilgili kişilerden minimum düzeyde veri talep etme ilkesi ile uyumlu olarak değerlendirilmediği,

b) Bunlara ek olarak, Spor kulüplerinde giriş çıkış kontrolünün sağlanması hususunda özel nitelikli kişisel verilerin işlenmesinin kanunlarda açıkça öngörülmediği dikkate alındığında veri sorumluları tarafından el ve parmak izinin işlenmesi için ilgili kişilerin açık rızalarının alınması yoluna gidildiği iddiası ile ilgili olarak;

Kanunun “Özel Nitelikli Kişisel Verilerin İşlenme Şartları” başlıklı 6 ncı maddesinin (1) numaralı fıkrasında özel nitelikli kişisel veriler “Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri” olarak sayıldığı ve özel nitelikli kişisel verilerinin aynı maddede

“(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.”

hükümlerine yer verildiği

Spor kulüplerinde giriş çıkış kontrolünün sağlanması hususunda özel nitelikli kişisel verilerin işlenmesinin kanunlarda açıkça öngörülmediği dikkate alındığında veri sorumluları tarafından avuç izinin işlenmesi için ilgili kişilerin açık rızalarının alınması yoluna gidildiğinin anlaşıldığı,

6698 sayılı Kanunun 3 üncü maddesinde açık rızanın “belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza” şeklinde tanımlandığı, tanımdan da anlaşılacağı üzere açık rızanın, “Belirli bir konuya ilişkin olması”, “Rızanın bilgilendirmeye dayanması” ve “Özgür iradeyle açıklanması” şeklinde üç unsuru bulunduğu, veri işlemek üzere verilen açık rızanın geçerli olması için, açık rızanın öncelikle belirli bir konuya ilişkin ve o konu ile sınırlı olarak verilmesi gerektiği, bu doğrultuda veri sorumlusu tarafından açık rıza beyanının hangi konuya ilişkin olarak istenildiğinin açıkça ortaya konulması gerektiği, bununla birlikte, açık rıza bir irade beyanı olduğundan, kişinin özgür bir şekilde rıza gösterebilmesi için, neye rıza gösterdiğini de bilmesini zorunlu olduğu, kişinin sadece konu üzerinde değil, aynı zamanda rızasının sonuçları üzerinde de tam bir bilgi sahibi olması gerektiği, bu sebeple, bilgilendirmenin, veri işleme ile ilgili bütün konularda açık ve anlaşılır bir

biçimde gerçekleştirilmesi ve mutlaka verinin işlenmesinden de önce yapılması gerektiği, diğer yandan, açık rızanın geçerlilik kazanabilmesi için kişinin yaptığı davranışın bilincinde ve kendi kararı olması gerektiği, aksi durumlarda, kişinin iradesini sakatlayacak cebir, tehdit, hata ve hile gibi hallerde açık rıza da sakatlanacağından kişinin özgür biçimde karar vermesinden de söz edilemeyeceği,

Bu bağlamda, herhangi bir ürün ve/veya hizmetin sunumunun, açık rıza verme ön şartına bağlanmaması gerektiği ve eğer yapılan seçimin sonuçları, kişisel veri sahibinin seçim özgürlüğünü etki altında bırakıyorsa, bu durumda rızanın özgürce verildiğini söylemenin mümkün bulunmadığı, dikkate alındığında bahse konu somut olayda, üyelere sunulan online üyelik sözleşmesinde, özel nitelikli kişisel veri olan avuç içi izinin alınmasına onay verilmesinin sözleşmenin kurulması için zorunlu bir şart olarak sunulduğu ve kurala uyulmaması halinde firmaya fesih hakkı tanınmış olduğu hususları birlikte değerlendirildiğinde üyelerin kulüplere girişlerde avuç içi izi bilgilerinin alınmasına rıza göstermemeleri halinde söz konusu hizmetten yararlanamayacakları dikkate alındığında, üyeler tarafından verilen açık rızaların özgür iradeye dayalı olduğunu söylemenin mümkün bulunmadığı bu kapsamda veri sorumlusu tarafından hizmetin sunulmasının açık rıza şartına bağlandığının değerlendirildiği

bu itibarla ilgili veri sorumluları hakkında,

- Spor kulübünde giriş çıkış kontrolünün yapılabilmesi ve kulüp hizmetlerinden faydalanmak isteyen kişilere ilişkin giriş kontrolünün alternatif yollar ile sağlanması mümkün iken kişilerin biyometrik veri niteliğindeki avuç içi izi verisinin alınmasının 6698 sayılı Kişisel Verilerin Korunması Kanununun 4 üncü maddesinin (2) numaralı fıkrasında yer alan “İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkesi ile bağdaşmadığı, öte yandan özel nitelikli kişisel verilerin Kanun kapsamında ancak ilgili kişilerin açık rızasına ya da Kanunun 6 ncı maddesinin (3) numaralı fıkrasında sayılan şartlar çerçevesinde işlenebileceği, bu kapsamda adı geçen veri sorumlusu tarafından avuç içi izi verisinin işlenmesi için kişilerden açık rızalarının alınması yoluna gidildiği ancak açık rıza verilmemesi durumunda kulüp hizmetlerinden yararlanamadıkları dikkate alındığında üyelere alınan açık rızanın Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendine aykırılık teşkil etmesi nedeniyle Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında idari para cezası uygulanmasına,

- Kişisel Verileri Koruma Kurulunun 21/12/2017 tarih ve 2017/62 sayılı “Banko, Gişe, Masa Gibi Hizmet Alanlarında Kişisel Verilerin Korunması”na ilişkin Kararı çerçevesinde üyelere ait kişisel bilgilerin üçüncü kişiler tarafından görülmesini önleyecek gerekli teknik ve idari tedbirleri almadığı

kanaatine varılan veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (c) bendi kapsamında idari para cezası uygulanmasına,

- Spor Kulübünde giriş çıkış kontrolünün ve kulüp içerisindeki güvenliğin temini noktasında kulüp hizmetlerinden faydalanmak isteyen kişilere ilişkin giriş kontrollerinin biyometrik verileri işlemenin haricinde alternatif yollar ile sağlanması, biyometrik veri ile giriş çıkış işlemleri yapılmasının ve biyometrik veri işlemenin ivedilikle durdurulması hususunda veri sorumlularının talimatlandırılmasına;

- Veri sorumluları tarafından bugüne kadar işlenen ve muhafaza edilen el, parmak ve avuç izi ile ilgili verilerin Kanunun 7 nci maddesi ile Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik hükümlerine uygun olarak ivedilikle yok edilmesi, eğer ilgili özel nitelikli verilerin üçüncü kişilere aktarılması söz konusu ise, yok etmeye yönelik işlemlerin bu verilerin aktarıldığı üçüncü kişilere ivedilikle bildirilmesinin sağlanması hususunda veri sorumlularının talimatlandırılmasına

karar verilmiştir.

2019/78 sayılı KVKK Kararı

Veri sorumlusunun kanuni yükümlülüğünü yerine getirmek için işlediği kişisel verileri meşru menfaat çerçevesinde kullanma talebiyle Kuruma yapmış olduğu başvuru Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/78 Sayılı Karar Özeti

Karar Tarihi : 25.03.2019

Karar No : 2019/78

Konu Özeti : Veri sorumlusunun kanuni yükümlülüğünü yerine getirmek için işlediği kişisel verileri meşru menfaat çerçevesinde kullanma talebiyle Kuruma yapmış olduğu başvuru

5015 sayılı Petrol Piyasası Kanunu gereğince, “Dağıtıcı Lisansı” kapsamında petrol piyasasında faaliyet gösteren Şirketin,

- Enerji Piyasası Düzenleme Kurulu (EPDK) Kararı ile getirilen yükümlülük çerçevesinde, bayi pompa satış hareketlerini, “plaka, akaryakıt türü, miktar, fiyat, zaman (saat, dakika ve saniye)” bilgilerini içerecek şekilde sorgulama imkanı veren ve ilgili Kurumun anlık erişimine açık olan bir otomasyon sistemi kurduğu,
- EPDK’nın anlık erişimine açık tutulan bu verilerden “plaka ve akaryakıt tipi”ne ilişkin verileri, araç sahipleri, akaryakıt bayileri ve akaryakıt dağıtım firmaları için sektörde büyük bir sorun haline gelen “hatalı akaryakıt dolumlarının” önüne geçmek için Şirketleri tarafından geliştirilen “Araç Tanıma Projesi” için kullanmak istedikleri,
- Araç Tanıma Projesinin hayata geçirilmesi ile birlikte, akaryakıt ikmal edecek aracın plaka verileri ile kullandığı yakıt türünün (benzin veya motorin) sistemde otomatik olarak eşleştirilerek kaydedileceği; böylece yanlış akaryakıt alımının otomatik olarak engelleneceği,
- Şirketin ve bayilerin tüketiciye akaryakıt satışı esnasında kurulan satış sözleşmesini doğru ifa edebilmesi ve doğru ürün tedarikini gerçekleştirmesi için tüketicinin araç plakasını kullanmasının bir gereklilik haline geldiği, Araç Tanıma Projesinin gerçekleştirilmesinin hatalı akaryakıt ikmalinden kaynaklanan problemleri sonlandıracağı ve böylece Şirketin ve bayilerin meşru menfaatlerinin korunmuş olacağı,

belirtilerek, bu kapsamda şirketin otomasyon sistemi için işlediği bazı verileri, ilgili kişilerin açık rızası olmaksızın Araç Tanıma Projesi için kullanmasının 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 5 inci maddesinin (2) numaralı fıkrasının (ç) ve (f) bentleri kapsamında değerlendirilip değerlendirilemeyeceği talebiyle yapmış olduğu başvuru hakkında Kurul tarafından:

- EPDK'dan almış olduğu lisanslar çerçevesinde "Akaryakıt Dağıtım Firması" olarak faaliyet gösteren Şirketin, 5015 sayılı Petrol Piyasası Kanunu ve ilgili mevzuatlarda düzenlenen denetim sistemi kurma zorunluluğu çerçevesinde araç sahiplerinin kişisel verilerini işlemesinin, 6698 sayılı Kanunun 5 inci maddesinin ikinci fıkrasının (ç) bendinde düzenlenen kişisel veri işlenmesinin "veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" hali sayıldığı; bu kapsamda kişisel veri işlenmesi halinde ilgili kişinin açık rızasının aranmadığı,

- Bununla birlikte, 6698 sayılı Kanunun 5 inci maddesinin ikinci fıkrasının (f) bendine göre "*ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması*" hali tespit edilirken veri sorumluları tarafından;

- Kişisel verinin işlenmesi sonucunda elde edilecek menfaat ile ilgili kişinin temel hak ve hürriyetlerinin yarışabilir düzeyde olması,
- Söz konusu menfaate ulaşılabilmesi bakımından kişisel veri işlenmesinin zorunluluk arz etmesi,
- Meşru menfaatin halihazırda mevcut, belirli ve açık olması,
- İlgili kişinin temel hak ve hürriyetleri ile yarışabilir nitelikte olan meşru menfaatin elde edilmesi halinde bir yarar sağlanacak olması ve kişisel veri işlenmeksizin başkaca bir yol ve yöntemle bu yararın ortaya çıkmasının mümkün olmaması,
- Meşru menfaat belirlenirken söz konusu yararın çok sayıda kişiyi etkilemesi, yalnızca kâr elde edilmesi ya da ekonomik yararın sağlanması amacına yönelik olmaması, iş süreçlerini ya da bir işleyişi kolaylaştırması (örneğin bir birim ya da az sayıda personel nezdinde değil, kurumsal olarak geneli etkileyecek şekilde) gibi şeffaf ve hesap verilebilir nitelikleri haiz kriterlerin esas alınması,
- Bu açıdan ilgili kişinin başta kişisel verilerinin korunması olmak üzere temel hak ve hürriyetlerinin zarar görmesini engellemek amacıyla öngörülebilir, açık ve yakın her türlü tehlikeden uzak tutulması,
- Kişisel verilerin bir veri kayıt sisteminde amaçla sınırlı olarak hukuka uygun işleyişinin temini ile zararı ve ihlalleri engellemek için her türlü teknik ve idari tedbirin alınması,
- Kişisel verilerin işlenmesinde genel ilkelere uygunluğun sağlanması,

- Bu kapsamda, kişinin temel hak ve hürriyetleri ile veri sorumlusunun meşru menfaatinin karşılaştırılarak denge testinin yapılması

hususlarının değerlendirilmesi gerektiği,

- Öte yandan, kişisel verilerin ilk kez işlenmesi için gereken amaçtan farklı olarak başka bir amaca yönelik yeni bir veri işleme faaliyetinin gerçekleştirilmesinin, Kanunun 5 inci maddesinde sayılan veri işleme şartlarından en az birine dayanması ve ilk amaçtan bağımsız olarak Kanunun 4 üncü maddesinde sayılan kişisel verilerin işlenmesinde aranan ilkelerin tümüne uyumlu olması gerektiği

- Şirketin Araç Tanıma Projesi uygulaması kapsamında, halihazırda Petrol Piyasası mevzuatı gereği kayıtlarında bulunan tüketicilere ait araç plaka ve ürün tipi bilgilerini otomatik olarak Araç Tanıma Projesi sistemine entegre etmesi de yeni bir kişisel veri işleme faaliyeti sayıldığı,

hususlarından hareketle; Akaryakıt istasyonlarına gelen araçlara tüketicinin talep ettiği üründen farklı bir ürün ikmal edilmesi nedeniyle oluşan araç arızalarından dolayı tüketicilerin uğramış olduğu zararlar ile bu zararlardan 6502 sayılı Tüketicinin Korunması Hakkında Kanun gereğince işletici ile birlikte başvuranın da dağıtıcı şirket olarak müteselsilen sorumluluğunun bulunduğu, bu yöndeki yargı kararları da dikkate alındığında durumun hem tüketicinin hem de dağıtıcı şirketin maddi kaybı ile birlikte şirket marka değeri ve hizmet kalitesinde de kayıplara yol açabileceğinin anlaşıldığı, dikkate alınarak,

- Bu çerçevede, meşru menfaatin ortaya konulmasına ilişkin olarak yukarıda yer verilen kriterler esas alınarak yapılan değerlendirme sonucu 6698 sayılı Kanunun 5 inci maddesinin ikinci fıkrasının (f) bendine göre veri sorumlusunun, tüketicilere ait plaka ve ürün tipi bilgilerini kullanmasının “İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması” kapsamında olduğu,

- Bu itibarla Şirketin, erişilebilir ve görünür bir şekilde aydınlatma yükümlülüğünü yerine getirmek ve başka bir amaçla kullanmamak kaydıyla ilgili kişilerin (kişisel verisi işlenen gerçek kişi tüketicilerin) açık rızasını almaksızın bahse konu sistemi kullanmasında 6698 sayılı Kanun yönünden hukuken bir engel bulunmadığına

karar verilmiştir.

2019/52 sayılı KVKK Kararı

Kurul kararının yerine getirilmemesi hakkında Kişisel Verileri Koruma Kurulunun 05/03/2019 tarihli ve 2019/52 sayılı Karar Özeti

Karar Tarihi : 05.03.2019

Karar No : 2019/52

Konu Özeti : Kurul kararının yerine getirilmemesi hakkında

2019/23 sayılı Kurul kararının şirkete tebliği sonrasında Şirket internet sitesi üzerinde muhtelif tarihlerde herhangi bir form numarasının son iki hanesinin değiştirilmesi suretiyle farklı form numaraları ile yapılan sorgulamalarda;

- Başka cihazlara ait sorgulamaların halen gerçekleştirilebildiği ve başka bir güvenlik doğrulamasının da yapılmadığı,
- Yapılan sorgulama sonucunda açılan sayfada kişilerin isim ve soy isimleri, IMEI numaraları ile cihazın sevk edildiği adresin baş ve son harfleri hariç maskelendiği, IMEI numaralarının, sorgulama yapılan ilk sayfada maskelenmiş şekilde gösterilmekle birlikte, aynı sayfada yer alan “Cihaz Kayıt Görüntüleri için Tıklayınız” linki seçildiğinde açılan yeni pencerede kamera görüntülerine ulaşabilmek için yönlendirilen linkin uzantısında IMEI numaralarının halen açık şekilde gösterildiği, söz konusu sayfada numaranın kime ait olduğuna ilişkin tanımlayıcı bir bilgiye yer verilmediği ancak, sorgu sayfasının aşağısında yer alan “Kargonuzu Görüntülemek İçin Tıklayınız” linki seçildiğinde gönderinin yapıldığı kargo firmasına yapılan yönlendirme ile ulaşılan sayfada gönderiyi teslim alan kişinin adı ve soyadı açıkça yer aldığından gönderiyi kendisi teslim alan müşteriler açısından IMEI numaraları ile cihaz sahibinin eşleştirilmesinin mümkün olabileceği, görülmüş olup, söz konusu sorgulamalara ilişkin ekran çıktıları alınmış ve tutanağa bağlanmıştır.

Bu itibarla,

- 2019/23 sayılı Kurul Kararı çerçevesinde Şirkete tebliğ edilen “...söz konusu aykırılığın ivedilikle giderilmesi, bahse konu aykırılığın giderildiği hususunun Kurula tevsiki sağlanıncaya kadar işbu Kararda yer alan linklerin kullanımının derhal durdurulması...” şeklindeki talimatın Şirket tarafından

Kurul Kararına uygun olarak yerine getirilmediđi dikkate alındıđında, Kanunun 15 inci maddesine aykırı olarak uyarınca Kurul tarafından verilen kararı yerine getirmeyen Őirket hakkında Kanunun 18 inci maddesi çerçevesinde 50.000 TL idari para cezası uygulanmasına,

- Öte yandan, Őirkete ait internet sitesinde herhangi bir sorgu numarasının son iki hanesini deđiřtirmek suretiyle bařka cihaz ve sahiplerine iliřkin sorgulamaların halen yapılabildiđi dikkate alındıđında, asıl güvenlik ağıının giderilmediđi bu kapsamda, cihaz takibi için sorgulama yapılabilmesine imkan veren sistemin deđiřtirilmesi, diđer taraftan halihazırda sorgulama yapılan sisteme eriřimin ivedilikle kapatılması hususunda Őirketin talimatlandırılmasına

karar verilmiřtir.

2019/47 sayılı KVKK Kararı

Bir şahsın, kendisi ve ailesi hakkındaki kişisel bilgilere hukuk dışı yollarla erişerek rızası dışında yargıya ve üçüncü kişilere aktardığı iddiasıyla bir başka şahıs hakkında Kuruma yapmış olduğu şikayet hakkında Kişisel Verileri Koruma Kurulunun 01/03/2019 tarihli ve 2019/47 sayılı Karar Özeti

Karar Tarihi : 01.03.2019

Karar No : 2019/47

Konu Özeti : Bir şahsın, kendisi ve ailesi hakkındaki kişisel bilgilere hukuk dışı yollarla erişerek rızası dışında yargıya ve üçüncü kişilere aktardığı iddiasıyla bir başka şahıs hakkında Kuruma yapmış olduğu şikayet hakkında

Başvuranın, isimli şahsın (şikayet edilen) kendisi ve ailesi hakkındaki bilgilere hukuk dışı yollarla erişerek, rızası dışında yargıya ve üçüncü kişilere aktardığı, bahse konu bilgilere İcra Müdürlükleri kanalıyla usulsüzce ulaştığı iddiası hakkında Kuruma yaptığı başvurusunun incelenmesi neticesinde,

- Şikayet edilen şahsın, başvuranın ailesi hakkındaki bilgilere hukuk dışı yollarla erişerek, rızası dışında yargıya ve üçüncü kişilere aktardığı iddiaları ile ilgili olarak, kişisel verilerin paylaşımının muhtelif mercilere yazılan dilekçelerden oluştuğu ve bu anlamda şikayet edilen tarafından kısmen ya da tamamen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla gerçekleştirilen bir kişisel veri işleme faaliyetine rastlanılmadığı, bu çerçevede şikayet edilenin veri sorumlusu olarak nitelendirilmesinin mümkün bulunmadığı, diğer taraftan şikayet edilen tarafından başvuran ve ailesine ait kişisel verilerin hukuka aykırı bir şekilde elde edildiği iddiasının Türk Ceza Kanunu kapsamında bir suç niteliği taşıdığı göz önüne alındığında söz konusu iddiaya ilişkin Kanun kapsamında yapılacak bir işlem bulunmadığına,

- Öte yandan, şikayet dilekçesinde şikayet edilenin, başvuranın kişisel verilerine İcra Müdürlükleri kanalıyla ulaştığı düşüncesinde olduğu iddiasının ilgili kişinin şahsi kanaatine dayandığı ve bu durumu tevsik edici herhangi somut bir bilgi veya belgeyle de tevsik edilmediği dikkate alındığında, söz konusu iddia ile ilgili olarak Kurulca yapılacak bir işlem bulunmadığına

karar verilmiştir.

2019/23 sayılı KVKK Kararı

Teknik servis hizmeti veren firmanın müşterilerine verdiği form/takip numarasının son hanelerinin değiştirilmesi yoluyla farklı kişilere ait kişisel verilere ulaşıldığı yolunda Kuruma iletilen ihbarın incelenmesi ve ihbara ilişkin alınan Kurul Kararının yerine getirilmemesi hakkında Kişisel Verileri Koruma Kurulunun 14/02/2019 tarihli ve 2019/23 sayılı Karar Özeti

Karar Tarihi : 14.02.2019

Karar No : 2019/23

Konu Özeti : Teknik servis hizmeti veren firmanın müşterilerine verdiği form/takip numarasının son hanelerinin değiştirilmesi yoluyla farklı kişilere ait kişisel verilere ulaşıldığı yolunda Kuruma iletilen ihbar hakkında

Teknik servis hizmeti veren veri sorumlusu firmanın, servise cihaz girişi yapıldığına ilişkin müşterilerine bir form numarası verdiği, form numarası sorgulaması ile kişilerin kendi telefonlarının servisteki durumlarına ilişkin bilgilere ulaşabildiği ancak form numaralarının birbirini takip eden sayılar olması nedeniyle ilgili kişiye verilen sorgu numarasının bir öncesi veya bir sonrasındaki sayının girilmesi suretiyle farklı numara girişlerinde farklı kişilere ait kişisel verilere erişildiği yolundaki ihbarın incelenmesi neticesinde,

- Veri sorumlusundan alınan bilgide, ilgili internet adresi üzerinden kişilerin servise bıraktıkları cihazları ile ilgili olarak yapılan sorgulamada cihaz sahiplerinin kişisel verilerine erişimin mümkün olmadığına belirtilmesine rağmen yapılan incelemede söz konusu internet sitesinde herhangi bir sorgu numarasının son iki hanesini değiştirmek suretiyle başka cihaz ve sahiplerine ilişkin de sorgulamalar yapılabildiği, söz konusu sorgulamalar neticesinde açılan sayfada yönlendirilen muhtelif linklerin seçilmesi suretiyle de bu kişilere ait isim, soy isim, adres ve sahip oldukları cihaz IMEI numarası bilgilerine erişim sağlanabildiği dikkate alınarak, anılan Şirket tarafından 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (1) numaralı fıkrasına aykırı olarak kişisel verilerin muhafazasının sağlanmasını teminen gerekli idari ve teknik tedbirlerin alınmaması nedeniyle, söz konusu aykırılığın Karar tarihi itibarıyla yapılan sorgulamalarda devam ettiği de göz

önünde bulundurulduğunda, veri sorumlusu hakkında Kanunun 18 inci maddesi çerçevesinde 150.000 TL idari para cezası uygulanmasına,

- Öte yandan, söz konusu aykırılığın giderilmesi yönünde veri sorumlusunun talimatlandırılmasına ve Kanunun 15 inci maddesinin (7) numaralı fıkrası uyarınca, söz konusu aykırılığın giderildiği hususunun Kurula tevsiki sağlanıncaya kadar işbu Kararda yer alan linklerin kullanımının durdurulmasına

karar verilmiştir.

2019/9 sayılı KVKK Kararı

Veri Sorumlusuna Başvuru ve Kurula Şikâyet Sürelerinin Hesaplanmasına İlişkin Kişisel Verileri Koruma Kurulunun 24/01/2019 tarih ve 2019/9 sayılı Kararı

Karar Tarihi : 24.01.2019

Karar No : 2019/9

Konu Özeti : Veri Sorumlusuna Başvuru ve Kurula Şikâyet Sürelerinin Hesaplanması

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) “Veri Sorumlusuna Başvuru” başlıklı 13 üncü maddesinin (1) numaralı fıkrasında ilgili kişinin Kanunun uygulanmasına yönelik taleplerini yazılı olarak veya Kişisel Verileri Koruma Kurulunun (Kurul) belirlediği diğer yöntemlerle veri sorumlusuna iletmesi, (2) numaralı fıkrasında ise veri sorumlusunun başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırması gerektiği hükme bağlanmıştır.

Öte yandan, Kanunun “Kurula Şikâyet” başlıklı 14 üncü maddesinin (1) numaralı fıkrasında da başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; ilgili kişinin, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyette bulunabileceği ifade edilmiştir.

Bu kapsamda, Kurumumuza intikal eden şikâyet başvurularının incelenmesi neticesinde veri sorumlusuna başvuru yolunu tüketen ilgili kişiler tarafından Kurula şikâyette bulunulması sürecinde Kanunda yer alan sürelerin yorumlanmasında farklılıklar olduğu görülmüştür. Bu itibarla Kanunun 14 üncü maddesinin (1) numaralı fıkrası uyarınca;

İlgili kişi tarafından yapılan başvuruya veri sorumlusunca 30 gün içinde bir cevap verilmesi halinde ilgili kişinin veri sorumlusunun cevabını müteakip 30 gün içerisinde şikâyette bulunabileceği, bu itibarla söz konusu hallerde ilgili kişinin veri sorumlusuna başvurduğu tarihten itibaren 60 günlük süresinin bulunmadığı,

İlgili kiři tarafından yapılan bařvuruya veri sorumlusunca bir cevap verilmedięi durumda ise ilgili kiřinin veri sorumlusuna bařvurduęu tarihten itibaren 60 gn iinde Kurula Őikâyette bulunabileceęi, İlgili kiři tarafından yapılan bařvuruya veri sorumlusunca Kanunda tanınan 30 gnlk sre sonrasında bir cevap verilmesi halinde ilgili kiřinin, Kanunda veri sorumlusuna tanınan 30 gnlk sre sonrasında verilecek cevabı beklemele ykml olmadıęı ve veri sorumlusuna tanınan srenin dolması ile birlikte Kurula Őikâyette bulunabileceęi gz nne alınarak, ilgili kiřinin veri sorumlusunun kendisine cevap verdięi tarihten itibaren 30 gn deęil, veri sorumlusuna bařvurduęu tarihten itibaren 60 gn iinde Kurula Őikâyette bulunabileceęi

hususlarının Kiřisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/9 sayılı Kararı ile kamuoyuna duyurulması uygun grlmřtir.

Kamuoyuna saygıyla duyurulur.

2018/156 sayılı KVKK Kararı

Yargı mercilerinin görev alanına giren konularla ilgili Kuruma yapılan başvurular hakkında Kişisel Verileri Koruma Kurulunun 24/12/2018 tarihli ve 2018/156 sayılı Kararı Özeti

Karar Tarihi : 24.12.2018

Karar No : 2018/156

Konu Özeti : Yargı mercilerinin görev alanına giren konularla ilgili Kuruma yapılan başvurular hakkında

İlgili kişinin, adı, soyadı, yerleşim yeri, boy, kilo, tip gibi kişisel bilgilerinin kullanılarak cinsel, siyasi, dini, arkadaşlık vb. içerikli yorumların ve paylaşımların yapıldığı hususu ile ilgili Kişisel Verileri Koruma Kurumuna yaptığı başvuru hakkında;

6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 15 inci maddenin (1) numaralı fıkrasında Kurulun, şikayet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapacağı; aynı maddenin (2) numaralı fıkrasında ise 01.11.1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesinde belirtilen;

a) Belli bir konuyu ihtiva etmeyen,

b) Yargı mercilerinin görevine giren konularla ilgili olan,

c) 4 üncü maddede gösterilen şartlardan (dilekçe sahibinin adı soyadı ve imzası ile iş veya ikametgâh adresi) herhangi birini taşımayan

ihbar veya şikâyetlerin incelemeye alınmayacağı hükme bağlanmıştır.

Diğer yandan, Kanunun 17 nci maddesinin (1) numaralı fıkrasında kişisel verilere ilişkin suçlar bakımından 26.09.2004 tarih ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümlerinin uygulanacağı belirtilmekte olup, Türk Ceza Kanununun 136 ncı maddesinde ise kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişinin, iki yıldan dört yıla kadar hapis cezası ile cezalandırılacağı hükme bağlanmıştır.

Bu kapsamda, kişinin ad-soyadı, yerleşim yeri, boy, kilo, tip gibi kişisel bilgilerinin kullanılarak çeşitli içerikli internet sitelerinde hakkında yorumların ve paylaşımların yapılmasına ilişkin şikayetini içeren ve yargıya intikal etmiş olan başvurunun değerlendirilmesi neticesinde;

6698 sayılı Kişisel Verilerin Korunması Kanununun 15 inci maddenin (2) numaralı fıkrasında 01.11.1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesinde “Yargı mercilerinin görevine giren konularla ilgili olan” ihbar veya şikâyetlerin incelemeye alınmayacağına hükme bağlandığı, şikayete konu iddiaların Türk Ceza Kanunu hükümleri uyarınca suç unsuru barındırdığı ve bunların da bireysel suç niteliğinde olduğu, bu kapsamda ilgili kişi tarafından da konunun yargıya intikal ettirilmiş olduğu dikkate alındığında, söz konusu başvurunun Kanun kapsamında değerlendirilemeyeceğine,

Öte yandan kişiye verilecek cevapta Kişisel Verilerin Korunması Kanunu kapsamında Kuruma yapılacak başvurularda izlenilmesi gereken yolun hatırlatılmasına

karar verilmiştir.

2018/143 sayılı KVKK Kararı

“Sağlık verilerini Kanunun 6 ncı maddesinde yer alan işleme şartlarından birine dayanmadan üçüncü bir kişiye aktaran veri sorumlusu hakkında” Kişisel Verileri Koruma Kurulunun 05/12/2018 Tarihli ve 2018/143 Sayılı Kararı

Karar Tarihi : 05.12.2018

Karar No : 2018/143

Konu Özeti : Sağlık Verilerinin Kanunun 6 ncı Maddesinde Yer Alan İşleme Şartlarından Birine Dayanmadan Üçüncü Kişilere Aktarımı Hakkında

Doktor kontrolünde ilaç kullanan ilgili kişinin, özel nitelikli bu sağlık verisinin ilaçların temin edildiği eczane tarafından her hangi bir işleme şartına dayanmadan üçüncü kişiyle paylaşılması hususunda Kuruma yapılan şikâyet başvurusu hakkında;

6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) “Özel nitelikli kişisel verilerin işleme şartları” başlıklı 6 ncı maddesinin (1) numaralı fıkrasında kişilerin sağlık verilerinin özel nitelikli kişisel veri olduğu belirtilmiştir. Mezkur maddenin (2) numaralı fıkrasında özel nitelikli kişisel verilerin ilgilinin açık rızası olmaksızın işlenmesi yasaklanmış bununla birlikte, (3) numaralı fıkrada özel nitelikli kişisel verilerin açık rıza aranmadan işlenebileceği diğer haller sayılmıştır. Buna göre sağlık verilerinin ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından açık rıza aranmaksızın işlenebileceği belirtilmiştir. Kanunun “Kişisel verilerin aktarılması” başlıklı 8 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın aktarılamayacağı hükme bağlanmış olup, anılan maddenin (2) numaralı fıkrasında ise kişisel verilerin açık rıza aranmaksızın aktarılabileceği haller Kanunun 5 inci maddesinin (2) numaralı fıkrası ile 6 ncı maddesinin (3) numaralı fıkrasına atıfta bulunmak suretiyle belirlenmiştir.

Öte yandan, Kanunun 12 nci maddesinin (1) numaralı fıkrası, veri sorumlusunun;

Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

Kişisel verilerin muhafazasını sağlamak

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğunu düzenlemektedir. Anılan maddenin (4) numaralı fıkrasında ise veri sorumluları ile veri işleyen kişilerin öğrendikleri kişisel verileri Kanun hükümlerine aykırı olarak başkasına açıklayamayacağı ve işleme amacının dışında kullanamayacağı hükmüne yer verilmiştir.

Bu kapsamda, doktor kontrolünde ilaç kullanan ilgili kişinin sağlığı ile ilgili özel nitelikli kişisel verilerinin, ilaçları temin ettiği eczane tarafından 6698 sayılı Kişisel Verilerin Korunması Kanununun 8 inci maddesinde sayılan şartlar sağlanmadan üçüncü kişiyle paylaşılmasının Kanunun 12 nci maddesinin (4) numaralı fıkrasına aykırılık teşkil etmesi nedeniyle veri sorumlusu eczane hakkında Kanunun 18 inci maddesi uyarınca idari para cezası uygulanmıştır.

2018/142 sayılı KVKK Kararı

İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi gereğince kişisel verilerin silinmemesi hakkında Kişisel Verileri Koruma Kurulunun 05/12/2018 tarihli ve 2018/142 sayılı Kararı Özeti

Karar Tarihi : 05.12.2018

Karar No : 2018/142

Konu Özeti : Kişisel Verilerin Silinmesi Talebi Hakkında

Veri sorumlusu bir Bankaya ait veri kayıt sisteminde yer alan kişisel verilerin silinmesi yönündeki ilgili kişi talebinin veri sorumlusu tarafından yerine getirilmemesi sebebiyle Kuruma yapılan başvuru hakkında;

6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) “Genel İlkeler” başlıklı 4 üncü maddesinin (2) numaralı fıkrasının (d) bendinde, kişisel verilerin ancak “İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza” edilebileceği hükme bağlanmıştır.

Diğer yandan Kanunun “Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi” başlıklı 7 nci maddesinin (1) numaralı fıkrasında, Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silineceği, yok edileceği veya anonim hâle getirileceği hüküm altına alınmış olmakla birlikte, (2) numaralı fıkrasında kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu hükümleri yer almaktadır.

5411 sayılı Bankacılık Kanununun 42 nci maddesi, alınan yazıların ve faaliyetler ile ilgili belgelerin asıllarının veya bunun mümkün olmadığı hâllerde sıhhatlerinden şüpheye mahal vermeyecek kopyalarının ve yazılan yazıların makine ile alınmış, tarih ve numara sırası verilerek düzenlenecek suretlerinin, usulleri çerçevesinde ilgili banka nezdinde on yıl süreyle saklanacağı hükmünü haizdir.

Ayrıca Bankaların Muhasebe Uygulamalarına ve Belgelerin Saklanması İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 17 nci maddesinin (1) numaralı fıkrasında da “Bankaların, müşterilerinden ve Resmî ya da özel kurum ve kuruluşlardan aldıkları mektup, telgraf, elektronik posta mesajı, ilam

ve tebligatlar ile diđer yazıları ve Bankaların İç Sistemleri Hakkında Yönetmelik uyarınca hazırlayacakları raporlar da dâhil olmak üzere, faaliyetleri ile ilgili belgelerin asıllarını veya mümkün olmadığı hâllerde sıhhatlerinden şüpheye mahal vermeyecek kopyalarını ve müşterilerine ve Resmî ya da özel kurum ve kuruluşlara yazdıkları yazıların makine ile alınmış, tarih ve numara sırası verilerek düzenlenecek suretlerini istenildiğinde ibraz edilebilecek şekilde nezdlerinde on yıl süreyle saklamaları zorunludur.” hükmüne yer verilmiştir.

Bu kapsamda, veri sorumlusu banka nezdinde bulunan kişisel verilerin silinmesi ile ilgili Kuruma yapılan başvuru hakkında; 6698 sayılı Kanunun ilgili maddesi ile 5411 sayılı Bankacılık Kanununun 42 nci maddesi göz önünde bulundurulduğunda; ilgili kişinin bankalar nezdindeki son işlemi üzerinden 10 yıllık saklama süresi geçmediği dikkate alındığında, şikayetçinin talebine yönelik Kurumumuzca yapılacak bir işlem bulunmadığına

karar verilmiştir.

2018/131 sayılı KVKK Kararı

Tüzel kişiliğe ait elektronik ortamda yer alan verilerin başka bir tüzel kişilik tarafından talep edilmesi hakkında Kişisel Verileri Koruma Kurulunun 19/11/2018 tarihli ve 2018/131 sayılı Kararı Özeti

Karar Tarihi : 19.11.2018

Karar No : 2018/131

Konu Özeti : Tüzel kişiliğe ait elektronik ortamda yer alan verilerin başka bir tüzel kişilik tarafından talep edilmesi hakkında

Bir tüzel kişiliğe ait elektronik ortamda yer alan verilerin veri sorumlusu tarafından başka bir veri sorumlusuna aktarılması talebi ile ilgili tüzel kişi şirket tarafından Kişisel Verileri Koruma Kurumuna (Kurum) yapılan başvuru hakkında;

6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 2 nci maddesinde Kanun hükümlerinin, kişisel verileri işlenen gerçek kişiler hakkında uygulanacağı belirtilmiş, "Tanımlar" başlıklı 3 üncü maddesinin (d) bendinde de kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmıştır. Bu sebeple, gerçek kişilere ait veriler Kanun kapsamında bulunurken, tüzel kişilere ait veriler ise Kanun kapsamında bulunmamaktadır.

Kanunun ilgili kişilerin haklarının düzenlendiği 11 nci maddesine göre ise herkesin, veri sorumlusuna başvurarak kendisiyle ilgili kişisel veri işlenip işlenmediğini öğrenme ve kişisel verileri işlenmişse buna ilişkin bilgi talep etme hakkı bulunmaktadır. Ayrıca söz konusu madde metninden de bu hakların, gerçek kişiye ait kişisel verileri kapsadığı ve bu hakkın da bizzat ilgili kişi veya yasal temsilcisi tarafından kullanılabilmesi anlaşılmaktadır.

Bu çerçevede,

Kurumumuza intikal eden söz konusu başvuruda yer alan, tüzel kişiliğe ait verilere erişilmesi yönündeki talebin Kanunun 2 nci maddesi gereğince Kanun kapsamında değerlendirilemeyeceğine,

Şirket ortak ve yetkilisi gerçek kişilere ilişkin verilere erişim sağlanması talebinin ise ilgili kişilerin kendileri tarafından değil Şirket tüzel kişiliği tarafından talep edilmesi sebebiyle söz konusu başvurunun Kanununun 11 ve 13 inci maddeleri kapsamında değerlendirilemeyeceğine karar verilmiştir.

2018/118 sayılı KVKK Kararı

Kurul Kararının gereğinin süresi içinde yerine getirilmemesi hakkında Kişisel Verileri Koruma Kurulunun 16/10/2018 tarihli ve 2018/118 sayılı Kararı Özeti

Karar Tarihi : 16.10.2018

Karar No : 2018/118

Konu Özet : Kurul Kararlarının Kanunun 15 inci Maddesi Uyarınca 30 Günlük Süre İçerisinde Yerine Getirilmemesi Hakkında

İlgili kişinin, veri kayıt sisteminde mevcut bulunan kişisel verilerinin silinmesi amacıyla veri sorumlusuna yaptığı başvuruya tatminkar bir cevap alamaması üzerine Kişisel Verileri Koruma Kurumuna (Kurum) yaptığı başvuru neticesinde, konu ile ilgili Kurul tarafından alınan kararın ilgili veri sorumlusu tarafından süresinde yerine getirilmemesi hakkında;

6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) “Şikâyet üzerine veya resen incelemenin usul ve esasları” başlıklı 15 inci maddesinin (5) numaralı fıkrası, şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması hâlinde Kurulun, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ edeceği, bu kararın da tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirileceği hükmünü haizdir.

Kanunun “Kabahatler” başlıklı 18 inci maddesinin (1) numaralı fıkrasının (c) bendinde ise Kanunun 15 inci maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar, idari para cezası verileceği (3) numaralı fıkrasında ise birinci fıkrada sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılacağı ve sonucunun Kurula bildirileceği hüküm altına alınmıştır.

Şikâyetçinin Kurula yapmış olduğu başvurunun incelenmesi neticesinde alınan Kurul Kararı 02.07.2018 tarihinde veri sorumlusuna tebliğ edilmiştir. Bu kapsamda veri sorumlusunun, Kurul Kararı kapsamında 16.08.2018 tarihinde şikâyetçiye bilgi verdiği, bu hususun da 17.08.2018 tarihli

yazı ile Kurula bildirildiği görülmekte olup, Şirket tarafından ilgili mevzuat hükümleri çerçevesinde en geç 01.08.2018 tarihinde yapılması gereken işlemin 16.08.2018 tarihinde yapıldığı; diğer yandan şikâyetçinin, veri sorumlusu nezdinde bulunan kişisel verilerinden asgari saklama süresi tamamlanmış olanlarının Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 11 inci maddesinin (1) numaralı fıkrası gereğince ilk periyodik imha işleminde, kalanların da yasal saklama yükümlülüğünün dolmasını müteakiben yapılacak periyodik imha işlemi dönemlerinde silinmesine ve gerçekleştirilecek silme işlemleri hakkında Şikâyetçiye bilgi verilmesi ayrıca, söz konusu kişisel verilerin saklama amacı dışında işlenmemesi hususunda veri sorumlusunun talimatlandırılmasına karar verilmiş olmasına rağmen Şirketin şikâyetçiyi muhatap 16.08.2018 tarihli yazısında Kurul Kararının bu maddelerine ilişkin herhangi bir açıklamada bulunmadığı tespit edilmiştir.

Bu çerçevede kamu kuruluşu olarak değerlendirilen veri sorumlusuna tebliğ edilen Kurul Kararının gereğinin Kanunun 15 inci maddesinin (5) numaralı fıkrasında belirtilen 30 günlük yasal süre içerisinde yerine getirilmemesi ve şikâyetçiye gönderilen bilgilendirme yazısında Kurul Kararında belirtilen hususlara yer verilmemiş olması nedenleriyle;

Şirket hakkında Kanunun 18 inci maddesinin (3) numaralı fıkrası çerçevesinde işlem tesis edilmesine, Şikâyetçinin, Şirket nezdinde saklanmakta olan verileri ile ilgili olarak Kurul Kararı kapsamında yapılacak iş ve işlemler hakkında bilgilendirilmesi hususunda Şirkete talimat verilmesine karar verilmiştir.

2018/106 sayılı KVKK Kararı

Kimliđi belirsiz kiři/kiřilerin veri sorumlusu olarak kabul edilemeyeceđi hakkında Kiřisel Verileri Koruma Kurulunun 13/09/2018 tarihli ve 2018/106 sayılı Kararı Özeti

Karar Tarihi : 13.09.2018

Karar No : 2018/106

Konu Özeti : Kimliđi belirsiz kiři/kiřilerin veri sorumlusu olarak kabul edilemeyeceđi

İlgili kiřinin görevi nedeniyle imzalamıř olduđu evrakın kimliđi belirsiz kiři/kiřilerce internet ortamında paylaşılması üzerine Kuruma yapmıř olduđu bařvuru hakkında,

6698 sayılı Kiřisel Verilerin Korunması Kanununun (Kanun) ‘‘Kapsam’’ bařlıklı 2 nci maddesinde, Kanun h k mlerinin, kiřisel verileri iřlenen ger ek kiřiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin par ası olmak kaydıyla otomatik olmayan yollarla iřleyen ger ek ve t zel kiřiler hakkında uygulanacađı ile ‘‘Tanımlar’’ bařlıklı 3 nc  maddesinin (1) numaralı fıkrasının (1) bendinde veri sorumlusunun kiřisel verilerin iřleme ama larını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve y netilmesinden sorumlu olan ger ek veya t zel kiřiyi ifade ettiđi belirtilmektedir.

Bu kapsamda;

řik yet inin bařvurusu incelendiđinde, kiřinin görevi nedeniyle imzalamıř olduđu bir evrakın hukuka aykırı bir řekilde elde edilip kimliđi belirsiz kiři veya kiřilerce internet ortamında paylařıldıđı ve aynı kullanıcı ismiyle řik yet inin isim ve soy isminin bař harflerinin yazılarak kiři hakkında bir takım iftira i erikli metinlere yer verildiđi anlařılmıř olup, kimliđi belirsiz kiři veya kiřilerin veri sorumlusu olarak tanımlanamayacađı

Kanunun ‘‘Su lar’’ bařlıklı 17 nci maddesinin (1) numaralı fıkrası geređi, kiřisel verilere iliřkin su lar bakımından 5237 sayılı T rk Ceza Kanununun 135 ila 140 ıncı madde h k mlerinin uygulanacađı

hususlarından hareketle, řik yete konu olayın T rk Ceza Kanunu h k mleri uyarınca su  unsuru barındırması ve konuya iliřkin gerekli hukuki iřlemlerin tesisini teminen konunun řik yet i

tarafından yargıya intikal ettirilmiş olması nedenleriyle Şikâyetçi hakkında ilgili uygulama üzerinden yapılan paylaşımlar kapsamında Kurumca yapılacak bir işlem bulunmadığına karar verilmiştir.

2018/91 sayılı KVKK Kararı

Kişisel verilere hukuka aykırı erişilmesini önleme yükümlülüğünü yerine getiremeyen veri sorumlusu hakkında Kişisel Verileri Koruma Kurulunun 26/07/2018 Tarihli ve 2018/91 Sayılı Kararı

Karar Tarihi : 26.07.2018

Karar No : 2018/91

Konu Özeti : Kişisel Verilere Hukuka Aykırı Erişilmesini Önleme Hakkında

Bir hazır giyim firmasının internet sitesi üzerinden üyelik bilgileri ile alışveriş yapan kişinin teslimat adresi, ad, soyadı, adres ve telefon numarası gibi kişisel bilgilerinin şirkete ait bu internet sitesi üzerinden alışveriş yapan üçüncü kişilerce erişilebilir hale gelmesi sebebiyle Şirkete başvuruda bulunarak kişisel verilerinin sistemlerinden silinmesini, yok edilmesini, ulaşılamaz hale getirilmesini, yurtiçi ve yurt dışında başka bir kurumla paylaşıldı ise o kurumlar nezdinde de silinmesini ve yok edilmesini talep etmesi üzerine Şirketten aldığı cevabı yetersiz bulması neticesinde Kuruma yapılan başvuru hakkında;

6698 sayılı Kişisel Verilerin Korunması Kanununun 7 nci maddesi “(1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir. (2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır” hükmünü amirdir.

Kanunun “İlgili Kişinin Hakları” başlıklı 11 inci maddesinin (1) numaralı fıkrasında ise herkesin, veri sorumlusuna başvurarak kendisiyle ilgili; yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme hakları düzenlemektedir.

Diğer yandan, Kanunun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (1) numaralı fıkrasında veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu hüküm altına alınmıştır.

Bir hazır giyim firmasının internet sitesi üzerinden üyelik bilgileri ile alışveriş yapan kişinin teslimat adresi, ad, soyadı, adres ve telefon numarası gibi kişisel bilgilerinin şirkete ait bu internet sitesi üzerinden alışveriş yapan üçüncü kişilerce erişilebilir hale gelmesi sebebiyle Şirkete başvuruda bulunarak kişisel verilerinin sistemlerinden silinmesini, yok edilmesini, ulaşılamaz hale getirilmesini, yurtiçi ve yurt dışında başka bir kurumla paylaşıldı ise o kurumlar nezdinde de silinmesini ve yok edilmesini talep etmesi üzerine Şirketten aldığı cevabı yetersiz bulması neticesinde Kuruma yapılan başvuru kapsamında;

- Şikâyetçinin kişisel verilerinin alışveriş işlemleri için girildiği, ancak anılan bilgilerin aynı zamanda başka müşterilerin alışverişe ilişkin işlemleri sırasında görülebilir hale geldiği, Şirket tarafından Kuruma sunulan savunma ve belgelerde, şirketin şikâyete konu durumdan olayla birlikte haberdar olduğu, olayın sistemselsel bir hatadan kaynaklandığının tespit edildiği, ilgili departmanlar arasında istişarelerde bulunularak başka müşterilerin de mağduriyet yaşamamaları amacıyla bir takım önlemlerin alındığı ve derhal uygulama sürümünün çıkarıldığı hususlarına ilişkin açıklamaları birlikte değerlendirildiğinde Şirket tarafından bahsi geçen mağduriyet öncesinde Kanunun 12 nci maddesinin (1) numaralı fıkrası kapsamında kişisel verilerin muhafaza edilmesi ve kişisel verilere hukuka aykırı erişilmesini önleme amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirlerin alınmadığı sonucuna varıldığından; Şirket hakkında Kanunun 18 inci maddesi uyarınca idari para cezası uygulanmasına,

- Şikâyetçinin her türlü kişisel verisinin Şirket sistemlerinden silinmesi, yok edilmesi, ulaşılamaz hale getirilmesi, yurtiçi ve yurt dışında başka bir kurumla paylaşıldı ise o kurumlar nezdinde de silinmesi ve yok edilmesi talebiyle ilgili olarak Şirketin taraflarınca yapılan işlemler hakkında açıklamalarını, tevsik edici belgelerle birlikte Kanunun 15 inci maddesinin (5) numaralı fıkrası gereğince kararın tebliğinden itibaren 30 gün içerisinde Şikâyetçiye iletmesi yönünde talimatlandırılmasına

karar verilmiştir.

2018/90 sayılı KVKK Kararı

Veri sorumlusu tarafından aydınlatma yükümlülüğü ve açık rıza onayı alınması süreçlerinin ayrı ayrı yerine getirilmesi gerektiği ile ilgili Kişisel Verileri Koruma Kurulunun 26/07/2018 tarihli ve 2018/90 sayılı Kararı Özeti

Karar Tarihi : 26.07.2018

Karar No : 2018/90

Konu Özeti : Veri sorumlusu tarafından aydınlatma yükümlülüğü ve açık rıza onayı alınması süreçlerinin ayrı ayrı yerine getirilmesi gerektiği ile ilgili

Online platformda iş başvurusu alan veri sorumlusu şirketler topluluğunun kişisel veri işleme süreçlerinin Kurul tarafından re'sen incelenmesini teminen yapılan başvuru neticesinde,

Online platformda iş başvurusunda bulunurken üyelik kaydı yapılmasının zorunlu olduğu, üyelik kaydı yapılması sırasında ise, aynı kutucuğun işaretlenmesi yoluyla hem aydınlatma metninin okunduğuna, hem de kişisel verilerin işlenmesi hususunda açık rıza verildiğine ilişkin onay alınması yoluna gidildiği tespit edilmiştir.

Bu kapsamda;

Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin 5 inci maddesinin (1) numaralı fıkrasının (f) bendinde kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerektiği hükme bağlanmıştır

Ayrıca, veri sorumlusu tarafından aydınlatma yükümlülüğünün yerine getirilmesi herhangi bir onaya bağlı değildir. Aydınlatma yükümlülüğünün yerine getirilmesindeki amaç kişisel verilerin işlenmesi noktasında ilgili kişinin bilgi sahibi olmasının temin edilmesidir. Açık rıza alınmasında amaç ise, veri sorumlusu tarafından kişisel verilerinin işlenmesinin hukuki bir gerekçeye dayandırılmasıdır. Bu sebeple, ilgili kişi aydınlatma metni sayesinde kişisel veri işleme faaliyeti ile ilgili olarak bilgi edinmiş olmakla birlikte, söz konusu metinde yazılanlara açık rıza vermek zorunda değildir.

Tüm bu hususlar bir arada değerlendirildiğinde; söz konusu uygulamanın 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) amacına ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin 5 inci maddesinin (1) numaralı fıkrasının (f) bendinde yer alan hükme uygun olmadığı, bu itibarla aydınlatma metninin okunduğuna ilişkin geri bildirim alınması ile ilgili kişilerin kişisel verilerinin işlenmesi hususunda gerekli seçimlik haklarının da tanındığı açık rıza metninin onaylandığının ispatını sağlayacak mekanizmaların ayrıştırılması hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

2018/88 sayılı KVKK Kararı

Sicile Kayıt Yükümlülüğünün Başlama Tarihleri ile ilgili Kişisel Verileri Koruma Kurulunun 19/07/2018 Tarihli ve 2018/88 Sayılı Kararı

Karar Tarihi : 19.07.2018

Karar No : 2018/88

Konu Özeti : Sicile kayıt yükümlülüğünün başlama tarihleri

6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 16 ncı maddesinin (2) numaralı fıkrasında yer alan “Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir.” hükmü ile Kanunun Geçici 1 inci maddesinin 2 nci fıkrasında yer alan “Veri sorumluları, Kurul tarafından belirlenen ve ilan edilen süre içinde Veri Sorumluları Siciline kayıt yaptırmak zorundadır.” hükmü göz önünde bulundurularak;

- Yıllık çalışan sayısı 50’den çok veya yıllık mali bilanço toplamı 25 milyon TL’den çok olan gerçek ve tüzel kişi veri sorumluları için Veri Sorumluları Siciline kayıt yükümlülüğü başlangıç tarihinin 01.10.2018 olması ve Sicile kayıt yaptırmaları için bu veri sorumlularına 30.09.2019 tarihine kadar süre verilmesinin kabulüne,

- Yurtdışında yerleşik gerçek ve tüzel kişi veri sorumluları için Veri Sorumluları Siciline kayıt yükümlülüğü başlangıç tarihinin 01.10.2018 olması ve Sicile kayıt yaptırmaları için bu veri sorumlularına 30.09.2019 tarihine kadar süre verilmesinin kabulüne,

- Yıllık çalışan sayısı 50’den az ve yıllık mali bilanço toplamı 25 milyon TL’den az olmakla birlikte ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek ve tüzel kişi veri sorumluları için Veri Sorumluları Siciline kayıt yükümlülüğü başlangıç tarihinin 01.01.2019 olması ve Sicile kayıt yaptırmaları için bu veri sorumlularına 31.03.2020 tarihine kadar süre verilmesinin kabulüne,

- Kamu kurum ve kuruluđu veri sorumluları için Veri Sorumluları Siciline kayıt yükümlülüđu başlangıç tarihinin 01.04.2019 olması ve Sicile kayıt yaptırmaları için bu veri sorumlularına 30.06.2020 tarihine kadar süre verilmesinin kabulüne
- Bu kararın Kurum internet sayfası ile Resmi Gazetede yayımlanmasına oybirliđi ile karar verilmiştir.

2018/87 sayılı KVKK Kararı

Veri Sorumluları Siciline Kayıt Yükümlülüğünden İstisna Tutulacak Veri Sorumluları ile ilgili Kişisel Verileri Koruma Kurulunun 19/07/2018 Tarihli ve 2018/87 Sayılı Kararı

Karar Tarihi : 19.07.2018

Karar No : 2018/87

Konu Özeti : Yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25 milyon TL'den az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanların Sicile kayıt yükümlülüğünden istisna tutulması

6698 sayılı Kişisel Verilerin Korunması Kanununun 16 ncı maddesinin (2) numaralı fıkrasında yer alan "Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir." hükmü ile 30 Aralık 2017 tarih ve 30286 sayılı Resmî Gazetede yayımlanarak yürürlüğe giren Veri Sorumluları Sicili Hakkında Yönetmeliğin "İstisna Kriterleri" başlıklı 16 ncı maddesi göz önünde bulundurularak; 02.04.2018 tarihli ve 2018/32 sayılı Kurul Kararı ile istisna tutulan veri sorumlularına ilave olarak, yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25 milyon TL'den az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanların; Veri Sorumluları Siciline kayıt yükümlülüğünden istisna tutulmasına ve bu kararın Kurum internet sayfası ile Resmi Gazetede yayımlanmasına oybirliği ile karar verilmiştir.

2018/75 sayılı KVKK Kararı

Arabulucuların Veri Sorumluları Siciline Kayıt Zorunluluğundan İstisna Tutulması ile ilgili Kişisel Verileri Koruma Kurulunun 05/07/2018 Tarihli ve 2018/75 Sayılı Kararı

Karar Tarihi : 05.07.2018

Karar No : 2018/75

Konu Özeti : Adalet Bakanlığı Hukuk İşleri Genel Müdürlüğü Arabuluculuk Daire Başkanlığından alınan Arabulucuların Veri Sorumluları Siciline kayıt zorunluluğundan istisna tutulmasına ilişkin 25/05/2018 tarih ve 9235 sayılı görüş talebi

Adalet Bakanlığı Hukuk İşleri Genel Müdürlüğü Arabuluculuk Daire Başkanlığından alınan Arabulucuların Veri Sorumluları Siciline kayıt zorunluluğundan istisna tutulmasına ilişkin 25.05.2018 tarih ve 9235 sayılı taleplerinin incelenmesi neticesinde;

6698 sayılı Kişisel Verilerin Korunması Kanununun 16 ncı maddesinin (2) numaralı fıkrasında yer alan “Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir.” hükmü ile 30 Aralık 2017 tarih ve 30286 sayılı Resmî Gazetede yayımlanarak yürürlüğe giren Veri Sorumluları Sicili Hakkında Yönetmeliğin “İstisna Kriterleri” başlıklı 16 ncı maddesi göz önünde bulundurularak; Arabulucular bakımından Veri Sorumluları Siciline kayıt yükümlülüğüne istisna getirilmesine ve Kararın Resmi Gazete ile Kurumun internet sayfasında yayımlanmasına oy birliği ile karar verilmiştir.

2018/69 sayılı KVKK Kararı

Sicil dosyalarındaki kişisel verilerin, işlenmelerini gerektiren sebeplerin ortadan kalkmaması sebebiyle, imha edilmemesi gerektiği hakkında Kişisel Verileri Koruma Kurulunun 28/06/2018 Tarihli ve 2018/69 Sayılı Kararı

Karar Tarihi : 28.06.2018

Karar No : 2018/69

Konu Özeti : Sicil Dosyalarındaki Kişisel Verilerin İmha Edilmesi Hakkında

Devlet memurlarının, memuriyet döneminde haklarında açılmış inceleme-soruşturma dosyalarına ilişkin evrakların imha edilmesi talebinin veri sorumlusu kamu kurumunca yerine getirilmemesi üzerine Kuruma yapılan başvuru hakkında;

6698 sayılı Kişisel Verilerin Korunması Kanununun 7 nci maddesinde “(1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir. (2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır” hükümlerine yer verilmiştir.

Öte yandan, 657 sayılı Kanunun “Memur Bilgi Sistemi, Özlük Dosyası” başlıklı 109 uncu maddesinde “Memur Bilgi Sistemi, Özlük Dosyası” başlıklı 109 uncu maddesinde her memur için bir özlük dosyasının tutulacağı ve bu dosyada memurun mesleki bilgileri, mal bildirimleri; varsa inceleme, soruşturma, denetim raporları, disiplin cezaları ile ödül ve başarı belgelerine ilişkin bilgi ve belgelerin konulacağı hükmüne; Kamu Personeli Genel Tebliğinin (Seri No: 2) “D” bölümünde ise görevleri herhangi bir şekilde sona eren memurların özlük dosyalarının kurumlarınca saklanacağı hükmüne yer verilmiştir.

Buna ek olarak, 16.05.1988 tarihli ve 19816 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren Devlet Arşiv Hizmetleri Hakkında Yönetmelik’in “Tarifler” başlıklı 3 üncü maddesinin

- (a) bendinde “Arşiv malzemesi: Türk Devlet ve Millet hayatını ilgilendiren ve en son işlem tarihi üzerinden otuz yıl geçmiş veya üzerinden onbeş yıl geçtikten sonra kesin sonuca bağlanmış olup,

birinci maddede belirtilen kuruluşların işlemleri sonucunda teşekkül eden ve onlar tarafından muhafazası gereken, Türk Milletinin geleceğine tarihi, siyasî, sosyal, hukukî ve teknik değer olarak intikal etmesi gereken belgeler ve Devlet hakları ile milletlerarası hakları belgelemeye, korumaya, bunlarla ilgili işlem ve münasebetler bakımından tarihî, hukukî, idarî, askeri, iktisadî, dinî, ilmî edebî estetik, kültürel biyografik, jeneolojik ve teknik herhangi bir konuyu aydınlatmaya, düzenlemeye, tespite yarayan, ayrıca ait olduğu devrin ahlâk, örf ve âdetlerini veya çeşitli sosyal özelliklerini belirten her türlü yazılı evrak, defter, resim, plan, harita, proje, mühür, damga, fotoğraf, film, ses ve görüntü bandı, baskı ve benzeri belgeleri ve malzemeyi”,

- (b) bendinde “Arşivlik malzeme: Yukarıdaki bentte sayılan her türlü belge ve malzemedan zaman bakımından henüz arşiv malzemesi vasfını kazanmayanlarla, son işlem tarihi üzerinden yüzbir yıl geçmemiş memuriyet sicil dosyaları, Devletin gerçek ve tüzel kişilerle veya yabancı devlet ve milletlerarası kuruluşlarla akdettiği ikili ve çok taraflı milletlerarası antlaşmalar, tapu tahrir defterleri, tapu ve nüfus kayıtları, aynı özellikteki vakfiyelerden ait oldukları kamu kurum ve kuruluşları ile il, ilçe, köy ve belediyelere ait sınır kâğıtları gibi belgeleri”,

- (c) bendinde “Birim arşivi: Kurum ve kuruluşların görev ve faaliyetleri sonucu kendiliğinden teşekkül eden ve bu kuruluşların çeşitli birimlerinde, aktüalitesini kaybetmemiş olarak aktif bir biçimde ve günlük iş akımı içinde kullanılan arşivlik malzemenin belirli bir süre saklandığı arşiv birimlerini (Mükelleflerin taşra, bölge ve yurt dışı kuruluşlarında bulunan arşivler de birim arşivi sayılır.)”,

- (d) bendinde “Kurum arşivi: Kurum ve kuruluşların, merkez teşkilâtları içinde yer alan ve arşiv malzemesi ile arşivlik malzemenin, birim arşivlerine nazaran daha uzun süreli saklandığı merkezî arşivleri”,

- (e) bendinde ise “Mükellefler: 28/9/1988 tarihli ve 3473 sayılı Muhafazasına Lüzum Kalmayan Evrak ve Malzemenin Yok Edilmesi Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabulü Hakkında Kanununun 1 inci maddesinde sayılan kurum ve kuruluşları”

şeklinde tanımlanmıştır.

Bu çerçevede, 3473 sayılı Muhafazasına Lüzum Kalmayan Evrak ve Malzemenin Yok Edilmesi Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabulü Hakkında Kanunun “Amaç ve Kapsam” başlıklı 1 inci maddesinde “Bu Kanunun amacı, genel ve katma bütçeli dairelerle (saklama, ayıklama ve imha işlemleri kendi mevzuatına tabi olmak kaydıyla Cumhurbaşkanlığı, Türkiye Büyük Millet Meclisi, Genelkurmay Başkanlığı, Milli Savunma Bakanlığı, İçişleri Bakanlığı, (Ek ibare:

1/2/2000 - 4516/1 md.) Dışışleri Bakanlıđı ve Milli İstihbarat Teşkilatı hariç) mahalli idareler, üniversiteler ve bunlara bađlı sabit ve döner sermayeli kuruluşlar, kamu iktisadi teşebbüsleri, özel kanunlarla kurulan kamu bankaları ve teşekkülleri elinde bulunan ve arşivlerinde arşiv malzemesi ve arşivlik malzeme niteliđi taşımayan, muhafazasına lüzum görülmeyen, yok edilecek evrak ve her türlü malzemenin, ayıklama ve imha işlemlerine dair usul ve esasları düzenlemektir." hükmü yer almakta olup, bu tanımdan hareketle genel bütçe kapsamındaki kamu idarelerinden olan Bakanlık da mükellef olarak deđerlendirilmektedir.

Buna ek olarak, Devlet Arşiv Hizmetleri Hakkında Yönetmelik'in "Birim ve Kurum Arşivleri" başlıklı 5 inci maddesinde mükelleflerin, belirli bir süre saklayacakları arşivlik malzeme için birim arşivlerini, daha uzun bir süre saklayacakları arşiv malzemesi veya arşivlik malzeme için kurum arşivlerini kuracakları ve ellerinde bulunan arşivlik malzemelerin birim arşivlerinde 1-5 yıl süre ile saklanacağı ile "Kurum Arşivine Devredilecek Malzemenin Ayrılması" başlıklı 19 uncu maddede de birim arşivinde saklanma süresini tamamlayan arşivlik malzemenin, "Kurum Arşivine Devredilecek" olanlar şeklinde ayrılacağı hüküm altına alınmıştır.

Devlet memurlarının, memuriyet döneminde haklarında açılmış inceleme-soruşturma dosyalarına ilişkin evrakların imha edilme talebinin veri sorumlusu kamu kurumunca yerine getirilmemesi üzerine Kuruma yapılan başvuru kapsamında, imha edilmesi talep edilen kişisel bilgilerin, ilgili kişinin devlet memuru olduğu dönemde hakkında açılmış inceleme-soruşturma dosyalarına ilişkin evraklar olması ve bu itibarla söz konusu evrakların, 657 sayılı Kanun geređince özlük dosyalarında saklanması gerektiđi, Kamu Personeli Genel Tebliđine (Seri No: 2) göre özlük dosyalarının dördüncü bölümünde yer alacağı ile görevi herhangi bir şekilde sona eren memurların özlük dosyalarının kurumlarınca saklanacağı ve Devlet Arşiv Hizmetleri Hakkında Yönetmeliđe göre son işlem tarihi üzerinden yüz bir yıl geçmemiş memuriyet sicil dosyaları içerisinde yer aldığı hususlarından hareketle, 6698 sayılı Kanunun 7 inci maddesinde belirtildiđi üzere kişisel verilerin işlenmesini gerektiren sebeplerin de henüz ortadan kalkmaması dolayısıyla şikayetçinin talebinin veri sorumlusu tarafından karşılanmamasının uygun olduğuna karar verilmiştir.

2018/68 sayılı KVKK Kararı

Gümrük Müşavirlerinin Sicile Kayıt İstisnası Hakkında Görüş Talebi ile ilgili Kişisel Verileri Koruma Kurulunun 28/06/2018 Tarihli ve 2018/68 Sayılı Kararı

Karar Tarihi : 28.06.2018

Karar No : 2018/68

Konu Özeti : Gümrük Müşavirlerinin Sicile Kayıt İstisnası Hakkında görüş talebi

Ankara, Bursa, İstanbul, İzmir ve Mersin Gümrük Müşaviri Derneklerinin 25.05.2018 tarihli yazısında belirtilen, Kişisel Verileri Koruma Kurulunun 15.05.2018 tarihli Resmi Gazetede yayımlanan ve bazı veri sorumlularının Veri Sorumluları Siciline kayıt yükümlülüğünden istisna tutulabileceğine ilişkin olarak verdiği karara istinaden gümrük müşavirleri ve yetkilendirilmiş gümrük müşavirlerinin de istisna kapsamına alınmasına ilişkin taleplerinin incelenmesi neticesinde;

6698 sayılı Kişisel Verilerin Korunması Kanununun 16 ncı maddesinin (2) numaralı fıkrasında yer alan “Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir.” hükmü ile 30 Aralık 2017 tarih ve 30286 sayılı Resmî Gazetede yayımlanarak yürürlüğe giren Veri Sorumluları Sicili Hakkında Yönetmeliğin “İstisna Kriterleri” başlıklı 16 ncı maddesi göz önünde bulundurularak 4458 sayılı Gümrük Kanunu uyarınca faaliyet gösteren gümrük müşavirleri ve yetkilendirilmiş gümrük müşavirleri bakımından Veri Sorumluları Siciline kayıt yükümlülüğüne istisna getirilmesine ve Kararın Resmi Gazete ile Kurumun internet sayfasında yayımlanmasına oy birliği ile karar verilmiştir.

2018/32 sayılı KVKK Kararı

Veri Sorumluları Siciline Kayıt Yükümlülüğünden İstisna Tutulacak Veri Sorumluları ile ilgili Kişisel Verileri Koruma Kurulunun 02/04/2018 Tarihli ve 2018/32 Sayılı Kararı

Karar Tarihi : 02.04.2018

Karar No : 2018/32

Konu Özeti : 6698 sayılı Kişisel Verilerin Korunması Kanununun 16 ncı maddesinin ikinci fıkrası ile Veri Sorumluları Sicili Hakkında Yönetmeliğin 16 ncı maddesi uyarınca Veri Sorumluları Siciline kayıt yükümlülüğüne getirilecek istisnaların belirlenmesi

6698 sayılı Kişisel Verilerin Korunması Kanununun 16 ncı maddesinin ikinci fıkrası ile 30/12/2017 tarihli ve 30286 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren Veri Sorumluları Sicili Hakkında Yönetmeliğin 16 ncı maddesine istinaden Veri Sorumluları Siciline kayıt yükümlülüğünden istisna tutulacak veri sorumlularının ekte yer verildiği şekilde belirlenmesine ve Kararın Resmi Gazete ile Kurumun internet sitesinde yayımlanmasına karar verilmiştir.

02/04/2018 tarih ve 2018/32 sayılı Karar Eki Liste

Herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler.

18/01/1972 tarihli ve 1512 sayılı Noterlik Kanunu uyarınca faaliyet gösteren noterler.

04/11/2004 tarihli ve 5253 sayılı Dernekler Kanununa göre kurulmuş derneklerden, 20/02/2008 tarihli ve 5737 sayılı Vakıflar Kanununa göre kurulmuş vakıflardan ve 18/10/2012 tarihli 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununa göre kurulmuş sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçalarına yönelik kişisel veri işleyenler.

22/04/1983 tarihli ve 2820 sayılı Siyasi Partiler Kanununa göre kurulmuş siyasi partiler.

19/3/1969 tarihli ve 1136 sayılı Avukatlık Kanunu uyarınca faaliyet gösteren avukatlar

1/6/1989 tarihli ve 3568 sayılı Serbest Muhasebeci Mali Müşavirlik ve Yeminli Mali Müşavirlik Kanunu uyarınca faaliyet gösteren Serbest Muhasebeci Mali Müşavirler ve Yeminli Mali Müşavirler.

YURTDIŐINA KİŐİSEL VERİ AKTARMA TAAHHÜTNAMELERİ

Bölüm İçeriđi

- Veri Sorumlusundan Veri Sorumlusuna Aktarım
- Veri Sorumlusundan Veri İŐleyene Aktarım
- Otokoç Otomotiv Ticaret ve Sanayi A.Ő. Taahhütname Başvurusu
- Türkiye Futbol Federasyonu Taahhütname Başvurusu
- Decathlon Türkiye Taahhütname Başvurusu
- TEB Arval Taahhütname Başvurusu
- Amazon Taahhütname Başvurusu

Veri Sorumlusundan Veri Sorumlusuna Aktarım

Konu: 24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununun (bundan sonra "6698 sayılı Kanun" olarak anılacaktır) 9 uncu maddesinin ikinci fıkrasının (b) bendi kapsamında kişisel verilerin yurtdışına aktarılmasında veri sorumlularının yapacağı yazılı taahhüt.

Kişisel verilerin Türkiye'de yerleşik veri sorumlusu tarafından yeterli veri koruması bulunmayan ülkelerde yerleşik veri sorumlusuna aktarımına ilişkin olarak, 6698 sayılı Kanunun 9 uncu maddesinin ikinci fıkrasının (b) bendine istinaden hazırlanacak sözleşmede aşağıdaki hususlara asgari olarak yer verilmesi zorunlu olup, bu sözleşme hükümleri ile taraflar kişisel verilerin aktarımında kişisel verilerin korunması için gereken yeterli korumayı tesis edeceklerini taahhüt ederler.

Madde 1- Veri Aktaran Veri Sorumlusunun Yükümlülükleri

Veri aktaran veri sorumlusu (bundan sonra "veri aktaran" olarak anılacaktır), aşağıda belirtilen yükümlülükleri yerine getirdiğini ve getireceğini taahhüt eder:

- a) Kişisel veriler, 6698 sayılı Kanun ve ilgili diğer mevzuata uygun olarak işlenmiş ve aktarılmış olacaktır.
- b) Veri aktaran; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla kişisel verinin niteliğine göre uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almalı ve veri alıcısı olan veri sorumlusu (bundan sonra "veri alıcısı" olarak anılacaktır) tarafından da bu tedbirlerin alındığından emin olmalıdır.
- c) Veri aktaran, veri alıcısına; aktarılan kişisel verilerin 6698 sayılı Kanun ile bu sözleşme hükümlerine uygun olarak işleneceğini bildirir.
- d) Veri aktaran, veri alıcısına, tabi olduğu 6698 sayılı Kanun ve ilgili diğer veri koruma düzenlemeleri hakkında bilgi verir.
- e) Veri aktaran; veri alıcısına, aktarılan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede kendisine bildirmek zorunda olduğu hakkında bilgi verir. Veri aktaran bu durumu en kısa sürede ilgisine ve Kişisel Verileri Koruma Kuruluna (bundan

sonra “Kurul” olarak anılacaktır) bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.

f) Veri aktaran, veri alıcısından aldığı bildirimleri, ilgili mevzuat hükümleri çerçevesinde Kurula iletir.

g) Veri aktaran, bu sözleşmede yer alan hükümlerin veri alıcısı tarafından yerine getirilmesi ile ilgili ortaya çıkan sorunlar hakkında en kısa sürede Kurula derhal bilgi verir.

h) Veri aktaran; veri alıcısının, ilgili kişilerden ve Kuruldan gelen sorulara cevap vereceği konusunda anlaşmaya varılmış olmasına rağmen cevap vermesinin mümkün olmaması halinde, elinde bulunan tüm bilgi ve belgeler ışığında makul bir süre içerisinde ilgili kişi veya Kurula cevap verir.

i) Veri aktaran; veri alıcısının bu sözleşmede belirtilen yükümlülüklerini ihlâl etmesi halinde, söz konusu ihlâl düzeltilene dek veri aktarımını askıya alabilir ya da sözleşmeyi feshedebilir.

j) Veri aktaran, veri aktarımının askıya alınması ya da sözleşmenin feshedilmesi halinde bu durumu en kısa sürede Kurula bildirir.

k) Veri aktaran; veri alıcısının, bu maddelerden doğan yükümlülüklerini yerine getirebilecek idari ve teknik yeterliliğe sahip olduğunu taahhüt eder.

l) Veri aktaran, 6698 sayılı Kanun gereğince veri aktarımına başlamadan önce, bu taahhütnameyi Kurula onaylatır.

Madde 2- Veri Alıcısının Yükümlülükleri

Veri alıcısı, aşağıda belirtilen yükümlülükleri yerine getirdiğini ve getireceğini taahhüt eder:

a) Veri alıcısı; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla kişisel verinin niteliğine göre uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri alır.

b) Veri alıcısı, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, (a) bendinde belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur. Veri işleyenler de dâhil olmak üzere veri alıcısının yetkisi altında faaliyet gösteren kişiler, kişisel verileri ancak ve sadece veri alıcısından aldıkları talimatlara uygun olarak işlemekle yükümlüdür.

c) Veri alıcısı; kişisel verileri 6698 sayılı Kanuna ve veri aktaranla arasındaki sözleşmeye uygun olarak işler, herhangi bir sebeple Kanuna ve sözleşmeye uygunluk sağlanamazsa, veri aktaranı konu ile ilgili

derhal bilgilendirir. Bu durumda veri aktaranın veri aktarımını askıya alma ve sözleşmeyi feshetme hakkına sahip olacağını kabul eder.

d) Veri alıcısı, sözleşmeye istinaden aktarılacak kişisel verilere ilişkin olarak, sözleşmeye aykırı herhangi bir ulusal düzenleme olmadığını kabul, beyan ve taahhüt eder. Sözleşme süresince veri alıcısının, sözleşmede yer alan taahhütlerini yerine getirmesini etkilemesi muhtemel bir mevzuat değişikliği yapılması hallerinde, durumu veri aktarana derhal bildirir ve bu durumda veri aktaranın veri aktarımını askıya alma ve sözleşmeyi feshetme hakkına sahip olacağını kabul eder.

e) Veri alıcısı; aktarılan kişisel verilere ilişkin olarak adli bir makamdan gelen talepleri, derhal veri aktarana bildirir. Bu durumda veri aktaranın talebin niteliğine göre sözleşmeyi askıya alma veya feshetme hakkına sahip olacağını kabul eder.

f) Veri alıcısı, sözleşme kapsamında veri aktarandan gelen soruları mümkün olan en kısa sürede usulüne uygun olarak cevaplandırır ve aktarıma konu kişisel verilerin işlenmesi hususunda Kurulun karar ve görüşlerine uyar.

g) Veri alıcısı, veri aktaranın, taahhüt ve yükümlülüklerin yerine getirilip getirilmediğine yönelik denetim yapma ve yaptırma yetkisine sahip olduğunu kabul eder ve bu yönde gerekli kolaylığı sağlar.

h) Veri alıcısı; bu sözleşmenin feshedilmesi veya yürürlük süresinin sona ermesi halinde, veri aktaranın tercihine bağlı olarak, aktarıma konu kişisel verileri yedekleri ile birlikte veri aktarana geri göndereceğini ya da kişisel verileri tamamen yok edeceğini, mevzuatta veri alıcısının bu yükümlülüğü yerine getirmesini engelleyen hükümler varsa, aktarıma konu kişisel verilerin gizliliğini güvence altına almak için gerekli idari ve teknik tedbirleri alacağını ve veri işleme faaliyetini durduracağını kabul eder.

i) Veri alıcısı, bu maddelerden doğan yükümlülüklerini yerine getirebilecek idari ve teknik yeterliliğe sahip olduğunu kabul eder.

j) Veri alıcısı sözleşme konusu hizmeti ifa ederken, sözleşmeye konu kişisel verileri, bir alt işverene aktarması gereken hallerde, veri aktaranı ispat edilebilir şekilde bilgilendirmeli ve onayını almalıdır. Veri alıcısının alt işveren ile yapacağı sözleşmenin, asgari olarak veri aktaran ile veri alıcısı arasındaki sözleşme ve bu taahhütnamedeki hükümleri içermesi şarttır.

Madde 3- Ortak Hükümler

a) Veri aktaran ve veri alıcısı, işledikleri kişisel verileri, 6698 sayılı Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar.

b) Veri aktaran ve veri alıcısı için bu yükümlülük herhangi bir süre ile sınırlı değildir.

Veri aktaran adına:

Veri alıcısı adına:

Ad Soyad:

Ad Soyad:

Açık Adres:

Açık Adres:

İrtibat Numarası:

İrtibat Numarası:

E-posta:

E-posta:

(Varsa sözleşmenin bağlayıcı olması için belirtilmesi gereken diğer bilgiler.)

(Varsa sözleşmenin bağlayıcı olması için belirtilmesi gereken diğer bilgiler.)

İmza/Kaşe

İmza/Kaşe

EK 1

(Taraflarca doldurulacaktır)

Veri konusu kiři grubu ve grupları

Aktarılan kişisel veriler, aşağıda belirtilen kiři grubu ve grupları (örneğin; çalışan verisi, müşteri verisi gibi) ile ilgilidir:

Veri kategorileri

Aktarılan kişisel veriler, aşağıda belirtilen veri kategorileri (kişisel veri veya özel nitelikli kişisel veri) ile ilgilidir:

Veri aktarımının amaçları

Veri aktarımı, aşağıda belirtilen amaçlarla yapılmaktadır:

Veri aktarımının hukuki sebebi

Alıcı ve alıcı grupları

Aktarılan kişisel veriler, sadece aşağıda belirtilen alıcılarla paylaşılabilir.

Veri alıcısı tarafından alınacak teknik ve idari tedbirler

Özel Nitelikli Kişisel veriler için alınan ek önlemler

Veri aktaranın Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) Bilgileri

(Kayıt yükümlülüğünün bulunması halinde)

Ek faydalı bilgiler

(Saklama süreleri ve ilgili diğer bilgiler)

İrtibat kişisi iletişim bilgileri

Veri Sorumlusundan Veri İşleyene Aktarım

Konu: 24/03/2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanununun (bundan sonra “6698 sayılı Kanun” olarak anılacaktır) 9 uncu maddesinin ikinci fıkrasının (b) bendi kapsamında kişisel verilerin yurtdışına aktarılmasında veri sorumlusu ile veri işleyenin yapacağı yazılı taahhüt.

Kişisel verilerin, Türkiye’de yerleşik veri sorumlusu tarafından yeterli veri koruması bulunmayan ülkelerde yerleşik veri işleyene aktarımına ilişkin olarak, 6698 sayılı Kanunun 12 nci maddesinin ikinci fıkrasına istinaden hazırlanacak sözleşmede asgari olarak aşağıdaki hususlara yer verilmesi zorunlu olup, bu sözleşme hükümleri ile taraflar kişisel verilerin aktarımında kişisel verilerin korunması için gereken yeterli korumayı tesis edeceklerini taahhüt ederler.

Madde 1- Veri Sorumlusunun Yükümlülükleri

Veri sorumlusu, aşağıda belirtilen yükümlülükleri yerine getirdiğini ve getireceğini taahhüt eder.

- a) Kişisel veriler, 6698 sayılı Kanun ve ilgili diğer mevzuata uygun olarak işlenmiş ve aktarılmış olacaktır.
- b) Veri sorumlusu; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla kişisel verinin niteliğine göre uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almalı ve veri işleyen tarafından da bu tedbirlerin alınmasını sağlamalıdır.
- c) Veri sorumlusu, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, durumu en kısa sürede ilgisine ve Kişisel Verileri Koruma Kuruluna (bundan sonra “Kurul” olarak anılacaktır) bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.
- d) Veri sorumlusu veri işleyene, aktarılan kişisel verilerin yalnızca kendi adına ve 6698 sayılı Kanun ile sözleşme hükümlerine uygun olarak işleneceği yönünde talimat verir.
- e) Veri sorumlusu, veri işleyenden aldığı ihlal bildirimlerini en kısa sürede ilgisine ve Kurula bildirir.
- f) Veri sorumlusu, bu sözleşmede yer alan hükümlerin veri işleyen tarafından yerine getirilmesi ile ilgili ortaya çıkan sorunlar hakkında Kurula en kısa sürede bilgi verir.

g) Veri sorumlusu, veri işleyen bu maddelerden doğan yükümlülüklerini yerine getirebilecek yeterliliğe sahip olduğunu taahhüt eder.

h) Veri sorumlusu, 6698 sayılı Kanun gereğince veri aktarımına başlamadan önce bu taahhütnameyi Kurula onaylatır.

Madde 2- Veri İşleyen Yükümlülükleri

Veri işleyen, aşağıda belirtilen yükümlülükleri yerine getirdiğini ve getireceğini taahhüt eder.

a) Veri işleyen; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla kişisel verinin niteliğine göre uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri alır.

b) Veri işleyen; kişisel verileri veri sorumlusu adına, onun verdiği talimatlara ve sözleşmeye uygun olarak işler. Herhangi bir sebeple veri sorumlusunun talimatlarına ve sözleşmeye uygunluk sağlanamazsa, veri sorumlusunu konu ile ilgili en kısa sürede bilgilendirir. Bu durumda veri sorumlusunun veri aktarımını askıya alma ve sözleşmeyi feshetme hakkına sahip olacağını kabul eder.

c) Veri işleyen, aktarılan kişisel verilere ilişkin olarak; sözleşme tarihinde sözleşmeye aykırı ulusal düzenleme olup olmadığını araştırır, böyle bir düzenlemenin bulunduğunu fark etmesi ya da sözleşmede yer alan taahhütlerini yerine getirmesini etkilemesi muhtemel bir mevzuat değişikliği yapılması hallerinde durumu veri sorumlusuna en kısa sürede bildirir ve bu durumda veri sorumlusunun veri aktarımını askıya alma ve sözleşmeyi feshetme hakkına sahip olacağını kabul eder.

d) Veri işleyen; bu sözleşmenin feshedilmesi veya yürürlük süresinin sona ermesi halinde, veri sorumlusunun tercihine bağlı olarak, aktarıma konu kişisel verileri yedekleri ile birlikte veri sorumlusuna geri göndereceğini ya da kişisel verileri tamamen yok edeceğini, mevzuatta veri işleyen bu yükümlülüğü yerine getirmesini engelleyen hükümler varsa, aktarıma konu kişisel verilerin gizliliğini güvence altına almak için gerekli her türlü teknik ve idari tedbiri alacağını ve veri işleme faaliyetini durduracağını kabul eder.

e) Veri işleyen; kişisel verilerin adli bir makamdan gelen ve kişisel verilerin söz konusu adli makama açıklanmasını gerektiren yasal olarak bağlayıcı talepleri ve kişisel verilere yetkisiz kişilerce erişilmesi durumunu en kısa sürede veri sorumlusuna bildirir.

f) Veri işleyen, sözleşme kapsamında veri sorumlusundan gelen soruları mümkün olan en kısa sürede usulüne uygun olarak cevaplandırır ve aktarıma konu kişisel verilerin işlenmesi hususunda Kurulun karar ve görüşlerine uyar.

g) Veri işleyen, taahhüt ve yükümlülüklerinin yerine getirilip getirilmediğine yönelik veri sorumlusunun denetim yapma ve yaptırma yetkisine sahip olduğunu kabul eder ve bu yönde gerekli kolaylığı sağlar.

h) Veri işleyen sözleşme konusu hizmeti ifa ederken, sözleşmeye konu kişisel verileri, bir alt işverene aktarması gereken hallerde, veri sorumlusunu ispat edilebilir şekilde bilgilendirmeli ve onayını almalıdır. Veri işleyenin alt işveren ile yapacağı sözleşmenin, asgari olarak veri sorumlusu ile veri işleyen arasındaki sözleşme ve bu taahhütnamedeki hükümleri içermesi şarttır.

Madde 3- Ortak Hükümler

a) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, belirtilen idari ve teknik tedbirlerin alınması hususunda veri işleyenle birlikte müştereken sorumludur.

b) Veri sorumlusu ve veri işleyen, işledikleri kişisel verileri 6698 sayılı Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar.

c) Veri sorumlusu ve veri işleyen için bu yükümlülük herhangi bir süre ile sınırlı değildir.

Veri sorumlusu adına:	Veri işleyen adına:
Ad Soyad:	Ad Soyad:
Açık Adres:	Açık Adres:
İrtibat Numarası:	İrtibat Numarası:
E-posta:	E-posta:
(Varsa sözleşmenin bağlayıcı olması için belirtilmesi gereken diğer bilgiler.)	(Varsa sözleşmenin bağlayıcı olması için belirtilmesi gereken diğer bilgiler.)
İmza/Kaşe	İmza/Kaşe

EK 1

(Taraflarca doldurulacaktır)

Veri sorumlusu

(Veri aktarımı ile ilgili faaliyetlerinizi kısaca belirtiniz.)

Veri işleyen

(Veri işleme ile ilgili faaliyetlerinizi kısaca belirtiniz.)

Veri aktarımının hukuki sebebi

Veri konusu kişi grubu ve grupları

İşlenecek kişisel veriler, aşağıda belirtilen kişi grubu ve grupları (örneğin; çalışan verisi, müşteri verisi gibi) ile ilgilidir

Veri kategorileri

İşlenecek kişisel veriler, aşağıda belirtilen veri kategorileri (kişisel veri veya özel nitelikli kişisel veri) ile ilgilidir.

İşleme faaliyetleri

Aktarılan kişisel veriler, aşağıda belirtilen temel işleme faaliyetlerine tâbi tutulacaktır: (Açıkça belirtiniz.)

Veri işleyen tarafından alınacak teknik ve idari tedbirler

Özel nitelikli kişisel veriler için alınacak ek önlemler

Veri sorumlusunun Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) Bilgileri

(Kayıt yükümlülüğünün bulunması halinde)

Ek faydalı bilgiler

(Saklama süreleri ve ilgili diğer bilgiler)

İrtibat kişisi iletişim bilgileri

Otokoç Otomotiv Ticaret ve Sanayi A.Ş. Taahhütname Başvurusu

Taahhütname Başvurusu Hakkında Duyuru

Yayınlanma Tarihi: 30.03.2023

Veri sorumlusu Otokoç Otomotiv Ticaret ve Sanayi Anonim Şirketi tarafından yurtdışına kişisel veri aktarımı yapılması hususundaki Taahhütname başvurusu Kişisel Verileri Koruma Kurulu tarafından 6698 sayılı Kişisel Verilerin Korunması Kanununun 9 uncu maddesinin 2 nci fıkrasının (b) bendi kapsamında değerlendirilmiş ve söz konusu veri aktarımına 30.03.2023 tarihinde Kurul tarafından izin verilmiştir.

Türkiye Futbol Federasyonu Taahhütname Başvurusu

Taahhütname Başvurusu Hakkında Duyuru

Yayınlanma Tarihi: 18.01.2022

Veri sorumlusu Türkiye Futbol Federasyonu tarafından yurtdışına kişisel veri aktarımı yapılması hususundaki Taahhütname başvurusu Kişisel Verileri Koruma Kurulu tarafından 6698 sayılı Kişisel Verilerin Korunması Kanununun 9 uncu maddesinin 2 nci fıkrasının (b) bendi kapsamında değerlendirilmiş ve söz konusu veri aktarımına 18.01.2022 tarihinde Kurul tarafından izin verilmiştir.

Decathlon Türkiye Taahhütname Başvurusu

Taahhütname Başvurusu Hakkında Duyuru

Yayınlanma Tarihi : 23.06.2021

Veri sorumlusu Turksport Spor Ürünleri San. Tic. Ltd. Şti. (Decathlon Türkiye) tarafından yurtdışına kişisel veri aktarımı yapılması hususundaki Taahhütname başvurusu Kişisel Verileri Koruma Kurulu tarafından 6698 sayılı Kişisel Verilerin Korunması Kanununun 9 uncu maddesinin 2 nci fıkrasının (b) bendi kapsamında değerlendirilmiş ve söz konusu veri aktarımına 22.06.2021 tarihinde Kurul tarafından izin verilmiştir.

TEB Arval Taahhütname Başvurusu

Taahhütname Başvurusu Hakkında Duyuru

Yayınlanma Tarihi : 09.02.2021

Veri sorumlusu TEB Arval Araç Filo Kiralama Anonim Şirketi tarafından yurtdışına kişisel veri aktarımı yapılması hususundaki Taahhütname başvurusu Kişisel Verileri Koruma Kurulu tarafından 6698 sayılı Kişisel Verilerin Korunması Kanununun 9 uncu maddesinin 2 nci fıkrasının (b) bendi kapsamında değerlendirilmiş ve söz konusu veri aktarımına 09.02.2021 tarihinde Kurul tarafından izin verilmiştir.

Amazon Taahhütname Başvurusu

Taahhütname Başvurusu Hakkında Duyuru

Yayınlanma Tarihi : 04.03.2021

Veri sorumluları Amazon Turkey Perakende Hizmetleri Ltd. Şti. ve Amazon Turkey Yönetim Destek Hizmetleri Ltd. Şti. tarafından yurtdışına kişisel veri aktarımı yapılması hususundaki Taahhütname başvuruları Kişisel Verileri Koruma Kurulu tarafından 6698 sayılı Kişisel Verilerin Korunması Kanununun 9 uncu maddesinin 2 nci fıkrasının (b) bendi kapsamında değerlendirilmiş ve söz konusu veri aktarımına 04.03.2021 tarihinde Kurul tarafından izin verilmiştir.

KİŞİSEL VERİ İHLAL BİLDİRİMİ FORMU

KİŞİSEL VERİ İHLALİ BİLDİRİM FORMU

A) HAKKINIZDA

1. Veri sorumlusunun unvanı/ ismi:

2. Veri sorumlusunun adresi:

3. Bu bildirim hazırlayan kişinin

Adı ve Soyadı:

Görevi:

E-postası:

Telefonu:

B) İHLAL HAKKINDA

1. Bildirim türü: İlk bildirim Takip bildirimi: _____

(Takip Bildirimlerinde varsa takip numarasını ekleyiniz)

2. İhlalin gerçekleşme tarihi ve saati:

3. İhlalin tespit tarihi ve saati:

4. İhlal hakkında bilgi veriniz.

5. İhlalin kaynağı (Birden çok uyan seçenek bulunması halinde hepsini işaretleyiniz)

Kişisel verilerin yanlış alıcılara gönderilmesi

Belge/cihaz hırsızlığı veya kaybolması

Verilerin güvensiz ortamlarda depolanması

Zararlı yazılımlar

Sosyal mühendislik

Sabotaj

- Kaza/ İhmal
- Diğer (Cevabınızı detaylandırınız):

6. İhlalden etkilenen kişisel veri kategorileri

(Birden çok uyan seçenek bulunması halinde hepsini işaretleyiniz)

Kişisel Veri	Özel Nitelikli Kişisel Veri
<input type="checkbox"/> Kimlik	<input type="checkbox"/> Irk ve Etnik Köken
<input type="checkbox"/> İletişim	<input type="checkbox"/> Siyasi Düşünce
<input type="checkbox"/> Lokasyon	<input type="checkbox"/> Felsefi İnanç, Din, Mezhep ve Diğer İnançlar
<input type="checkbox"/> Özlük	<input type="checkbox"/> Kılık ve Kıyafet
<input type="checkbox"/> Hukuki İşlem	<input type="checkbox"/> Dernek Üyeliği
<input type="checkbox"/> Müşteri İşlem	<input type="checkbox"/> Vakıf Üyeliği
<input type="checkbox"/> Fiziksel Mekan Güvenliği	<input type="checkbox"/> Sendika Üyeliği
<input type="checkbox"/> İşlem Güvenliği	<input type="checkbox"/> Sağlık Bilgileri
<input type="checkbox"/> Risk Yönetimi	<input type="checkbox"/> Cinsel Hayat
<input type="checkbox"/> Finans	<input type="checkbox"/> Ceza Mahkumiyeti ve Güvenlik Tedbirleri
<input type="checkbox"/> Mesleki Deneyim	<input type="checkbox"/> Biyometrik Veri
<input type="checkbox"/> Pazarlama	<input type="checkbox"/> Genetik Veri
<input type="checkbox"/> Görsel ve İşitsel Kayıtlar	
<input type="checkbox"/> Diğer (Detayları belirtiniz):	

7. İhlalden etkilenen tahmini kişi ve kayıt sayısı

Tahmini Kişi Sayısı: _____ Tahmini Kayıt Sayısı: _____

8. İhlalden etkilenen ilgili kişi grupları ve etkileri (Birden çok uyan seçenek bulunması halinde hepsini işaretleyiniz)

İlgili Kişi Grupları	İlgili Kişiler Üzerindeki Etkileri
<input type="checkbox"/> Çalışanlar <input type="checkbox"/> Kullanıcılar <input type="checkbox"/> Aboneler/Üyeler <input type="checkbox"/> Öğrenciler <input type="checkbox"/> Müşteriler ve potansiyel Müşteriler <input type="checkbox"/> Hastalar <input type="checkbox"/> Çocuklar <input type="checkbox"/> Korunmaya muhtaç yetişkinler <input type="checkbox"/> Henüz bilinmiyor	<input type="checkbox"/> Kişisel veriler üzerinde kontrol kaybı <input type="checkbox"/> Kimlik hırsızlığı <input type="checkbox"/> Ayrımcılık <input type="checkbox"/> Hakların kısıtlanması <input type="checkbox"/> Dolandırıcılık <input type="checkbox"/> Finansal kayıp <input type="checkbox"/> İtibar kaybı <input type="checkbox"/> Kişisel verilerin güvenliği kaybı
<input type="checkbox"/> Diğer (Detayları belirtiniz):	

9. Bildirimin yapılmasında herhangi bir gecikme yaşandıysa sebebini açıklayınız.

(Yalnızca ilk bildirimler için)

C) OLASI SONUÇLAR

1. İhlalin potansiyel etkileri hakkında bilgi veriniz.

(İhlalin ilgili kişiler üzerinde doğurabileceği etkileri tarif ediniz. Eğer halihazırda ilgili kişiler üzerinde bir zarar meydana geldiyse belirtiniz.)

2. İhlal sebebiyle ilgili kişilerin önemli olumsuz etkilere maruz kalma olasılığı *

- Yüksek
- Orta
- Düşük
- Daha bilinmiyor (Cevabınızı detaylandırınız):

3. İhlalin organizasyonunuza olan etkileri

Etkisi	Açıklama
<input type="checkbox"/> Yüksek	Tüm kullanıcılarınıza her türlü önemli hizmeti sunma yetinizi kaybettiniz.
<input type="checkbox"/> Orta	Bazı kullanıcılarınıza önemli bir hizmeti sunma yetinizi kaybettiniz.
<input type="checkbox"/> Düşük	Herhangi bir etkinlik kaybı söz konusu değil ya da çok düşük bir etkinlik kaybı var ve tüm kullanıcılarınıza tüm önemli hizmetleri sunabiliyorsunuz.
<input type="checkbox"/> Bilinmiyor	

4. İyileşme zamanı ile ilgili bilgiler

<input type="checkbox"/> Normal	Var olan kaynaklarınızı kullanacaksınız ve iyileşme zamanınızı öngörebiliyorsunuz.
<input type="checkbox"/> Destekli	Ek kaynaklar kullanacaksınız ve iyileşme zamanınızı öngörebiliyorsunuz.
<input type="checkbox"/> Uzatılmış	Ek kaynaklara ihtiyacınız var ve iyileşme zamanınızı öngöremiyorsunuz
<input type="checkbox"/> Geri Dönülmez	Saldırıdan geri dönüş imkansız (örn. yedekler yok edilmiş)
<input type="checkbox"/> Tamamlanmış	İyileşme tamamlandı

D) VARSA SİBER SALDIRIYA ÖZGÜ SONUÇLAR

1. Bilgi sistemleriniz siber saldırıdan etkilendi mi?

- Evet
 Hayır

2. Evet seçeneğini işaretlediyseniz, siber saldırı sonucu gerçekleşen ihlal unsurunu belirtiniz. (Birden çok uyan seçenek bulunması halinde hepsini işaretleyiniz)

- Veri gizliliği Veri bütünlüğü
 Veriye erişim Diğer (Cevabınızı detaylandırınız):

3. Siber saldırıların organizasyonunuza olan etkileri

Etkisi	Açıklama
<input type="checkbox"/> Yüksek	Tüm kullanıcılarınıza bilgi sistemleri aracılığıyla vermiş olduğunuz hizmetleri sunma yetinizi kaybettiniz.
<input type="checkbox"/> Orta	Bazı kullanıcılarınıza bilgi sistemleri aracılığıyla vermiş olduğunuz hizmetleri sunma yetinizi kaybettiniz.
<input type="checkbox"/> Düşük	Herhangi bir etkinlik kaybı söz konusu değil ya da çok düşük bir etkinlik kaybı var ve tüm kullanıcılarınıza bilgi sistemleri aracılığıyla vermiş olduğunuz hizmetleri sunabiliyorsunuz.
<input type="checkbox"/> Bilinmiyor	

4. İyileşme zamanı ile ilgili bilgiler

<input type="checkbox"/> Normal	Ek bilişim kaynakları kullanacaksınız ve iyileşme zamanınızı öngörebiliyorsunuz.
<input type="checkbox"/> Destekli	Var olan kaynaklarınızı kullanacaksınız ve iyileşme zamanınızı öngörebiliyorsunuz.

<input type="checkbox"/> Uzatılmış	Ek bilişim kaynaklarına ihtiyacınız var ve iyileşme zamanınızı öngöremiyorsunuz
<input type="checkbox"/> Geri Dönülmez	Saldırıdan geri dönüş imkansız (örn. yedekler yok edilmiş)
<input type="checkbox"/> Tamamlanmış	İyileşme tamamlandı

E) ÖNLEMLER

1. İhlal ile ilgili olan çalışanlar son bir yıl içerisinde kişisel veri koruma eğitimi aldı mı?

- Evet Hayır

2. Bu tür ihlalleri engellemek için ihlalin gerçekleşmesinden önce almış olduğunuz idari ve teknik tedbirlerini belirtiniz.

3. İhlalin sonucu olarak almış olduğunuz veya almayı planladığınız idari ve teknik tedbirleri belirtiniz.(Problemi çözmek ve olumsuz etkilerini ortadan kaldırmak adına almış olduğunuz önlemleri belirtiniz; örneğin yanlışlıkla gönderilmiş olan verilerin yok edilmesi, parolaların güvenliğinin sağlanması, veri güvenliği eğitimi planlanması vb.)

4. İhlalin tekrarlanmaması için atılan adımlar ve bunların tahminen ne zaman tamamlanacağı hakkında bilgi veriniz.

5. İlgili kişilere ihlal bildirim yapıldı mı?

- Evet, etkilenen ilgili kişilere bildirim yapıldı
- İlgili kişilere bildirim yapılmak üzere veya halihazırda bildirim gerçekleştiriyoruz
- Hayır, zaten bilgileri var
- Hayır, ancak bildirilecek
- Diğer (Aşağıda detayları belirtiniz)

6. İlgili kişilere hangi yöntemle bildirim yapıldığı/yapılacağı hakkında detaylı bilgi veriniz.

7. İlgili kişilerin veri ihlali ile ilgili bilgi almalarını sağlayacak kişinin adı-soyadı ve iletişim bilgisi ya da veri sorumlusu web adresi

8. Yurtdışında bulunan diğer organizasyon veya kurumlara ihlal hakkında bilgi verildi mi veya vermeyi düşünüyor musunuz?

(Örn. polis, diğer denetim ya da gözetim kurumları. Diğer kurumlar ile iletişime geçmeniz gerekebilir.)

<input type="checkbox"/> Evet	Evet seçeneğini işaretlediyseniz açıklayınız:
<input type="checkbox"/> Hayır	

9. Yurtdışında bulunan diğer veri koruma otoriteleri veya ilgili kurumlara ihlal hakkında bilgi verildi mi veya vermeyi düşünüyor musunuz? (Örn. polis, diğer denetim ya da gözetim kurumları.)

<input type="checkbox"/> Evet	Evet seçeneğini işaretlediyseniz açıklayınız:
<input type="checkbox"/> Hayır	

EK 1- VERİ İHLAL BİLDİRİM FORM REHBERİ

1. Eğer bu ilk bildirim ise doldurulan formu ihlalbildirimi@kvkk.gov.tr adresine “Kişisel veri ihlali bildirim” konulu bir e-posta ekiyle gönderiniz.

(e-posta yolu ile göndereceğiniz form ve eklerinin güvenli şekilde Kurumumuza ulaştırılmasının sorumluluğunun sizde olduğunu unutmayınız.)

2. Eğer bu bir takip bildirim ise bu formu ilk bildirimde göndermiş olduğumuz e-postanın ekine ekleyiniz. (e-postadaki konu satırını olduğu gibi bırakınız, bu sayede takip bildiriminiz olayınıza eklenebilecektir.)

3. Bu formu posta ile göndermek istemeniz durumunda onaylı olarak aşağıda belirtilen adresimize gönderiniz.

Kişisel Verileri Koruma Kurumu Nasuh Akar Mahallesi 1407. Sok. No:4, 06520 Balgat-Çankaya / Ankara

4. Varsa formda yer verilen bilgileri destekleyici dokümanları da (İnceleme raporu, ilgili kişilere bildirim yapıldığını tevsik edici belgeler vb.) forma eklemeyi unutmayınız.

5. Eğer bildiriminiz halihazırda mevcut bir olaya ilişkinse, olayınızla ilgilenen kişilerin bilgi sahibi olabilmesi için bildiriminiz olay dosyasına eklenecektir.

6. Atacağınız bir sonraki adımı belirlemek için 24.01.2019 tarih ve 2019/10 sayılı Kişisel Verileri Koruma Kurulu Kararını okumanızı tavsiye ederiz.

7. Eğer bu formu doldurma konusunda yardıma ihtiyacınız varsa ALO VERİ KORUMA 198 numaralı yardım hattımıza ulaşabilirsiniz.

*İlgili Soru	Açıklama
1. İhlal sebebiyle ilgili kişilerin önemli olumsuz etkilere maruz kalma olasılığı	<p>Gerçekleşen veri ihlalinin düzeyinin belirlenmesinde ilgili kişiler üzerinde ne kadar bir potansiyel etkiye neden olduğunun değerlendirilmesi gerekmektedir. Söz konusu potansiyel etkinin değerlendirilmesinde ise ihlalin niteliği, ihlalin nedeni, ihlale maruz kalan verinin türü, ihlalin etkisinin azaltılmasında alınan önlemler ile ihlalden etkilenen ilgili kişi kategorileri göz önünde bulundurulmalıdır. Risk düzeyinin belirlenmesinde aşağıdaki açıklamalar dikkate alınır.</p> <p>Düşük düzeyde risk: İhlal ilgili kişiler üzerinde olumsuz herhangi bir etkiye neden olmamakta ya da bu etki ihmal edilebilir düzeyde kalmaktadır.</p>

	<p>Orta düzeyde risk: İhlal ilgili kişiler üzerinde olumsuz etkilere neden olabilir fakat bu etki büyük değildir.</p> <p>Yüksek düzeyde risk: İhlal etkilenen kişiler üzerinde ciddi düzeyde olumsuz etkilere neden olmaktadır.</p>
--	---

VERİ İHLALİ BİLDİRİMLERİ

Bölüm İçeriği

- 2023/638 - Beytıp Sağlık Hizmetleri Ltd. Şti.
- 2023/504 - Sahibinden Bilgi Teknolojileri Paz. ve Tic. A.Ş.
- 2023/503 - Destek Bilgisayar ve İletişim Hizmetleri Tic. A.Ş.
- 2023/496 - Getir Perakende Lojistik Anonim Şirketi – Bitaksi Mobil Teknoloji Anonim Şirketi
- 2023/463 - Akbank T.A.Ş.
- 2023/375 - Marifet Saatçilik Kuym. Teks. Tur. Gıda İnş. Taah. San. ve Tic. Ltd. Şti.
- 2023/56 - Yalova Uzmanlar Sağlık Hizmetleri San.Paz.Tic.A.Ş
- 2023/55 - Reon Sağlık Hizmetleri İnş. Tur. San ve Tic. A.Ş.(Özel Aktif Hastanesi)
- 2023/54 - Okko Sağlık Turizm İnşaat San. ve Tic. A.Ş.
- 2022/1332 - Sital Çizgi İnşaat Turizm ve Tekstil Anonim Şirketi
- 2022/1271 - Pamukkale Belediyesi
- 2022/1264 - Shangai Moonton Technology Co Ltd
- 2022/1197 - Aktif İnş. Taşımacılık Paz. San. ve Tic. AŞ
- 2022/1196 - Aliza Otelcilik Turizm ve Tic. AŞ
- 2022/1195 - AES Otelcilik Turizm ve Tic. AŞ
- 2022/1194 - Baykar Motorlu Araçlar A.Ş.
- 2022/1138 - Denizli Özel Egekent Hastanesi
- 2022/1096 - Quick Sigorta Anonim Şirketi
- 2022/1032 - Flo Mağazacılık ve Pazarlama A.Ş.
- 2022/1018 - Özel Keystone Eğitim ve Eğitim Dan. A.Ş.
- 2022/990 - Marmara Üniversitesi
- 2022/987 - Fuudy Elektronik İletişim Perakende Gıda Lojistik Anonim Şirketi
- 2022/882 - Biblos Alaçatı Turizm Yatırımları A.Ş.
- 2022/891 - Posta ve Telgraf Teşkilatı Biriktirme ve Yardım Sandığı
- 2022/850 - Güreli Yeminli Mali Müşavirlik ve Bağımsız Denetim Hizmetleri Anonim Şirketi
- 2022/831 - AstraZeneca İlaç San. ve Tic. Ltd. Şti.
- 2022/757 - NeoPets Inc
- 2022/722 - Surtaş Otomotiv ve Servis Hizmetleri Sanayi Ticaret Limited Şirketi

- 2022/687 - Knauf İnşaat ve Yapı Elemanları San. ve Tic. A.Ş ile Knauf Insulation Izolation San. ve Tic. A.Ş
- 2022/686 - Türkiye Elektrik Dağıtım A.Ş.
- 2022/685 - Meklas Otomotiv San. ve Tic. A.Ş.
- 2022/649 - Tofisa Tekstil Sanayi ve Ticaret Limited Şirketi
- 2022/646-647-648 - ARG Denizcilik İnşaat Otomotiv Sanayi ve Ticaret Ltd. Şti, İstek Gemi İnşaa Bakım İnşaat Hırdavat Sanayi ve Ticaret Ltd. Şti, Safter Ulubay
- 2022/? - Barçın Spor Malzemeleri Ticaret ve Sanayi Anonim Şirketi
- 2022/569 - Pegasus Hava Taşımacılığı Anonim Şirketi
- 2022/554 - MBtech Mühendislik ve Danışmanlık Ltd. Şti.
- 2022/536 - Baydöner Restoranları A.Ş.
- 2022/535 - ZkSoftware The Advanced Biometric Solution Elektronik San. ve Tic. Ltd. Şti.
- 2022/478 - Yıldız Teknoloji Geliştirme Bölgesi Teknopark AŞ
- 2022/446 - Keyubu İnternet ve Bilişim Hizmetleri
- 2022/441 - Paketman E-Ticaret Sanayi Ticaret AŞ
- 2022/440 - Magna Ventures Yazılım ve Teknoloji Girişimleri Ticaret Anonim Şirketi
- 2022/404 - Villacım Emlak Turizm İnşaat Sanayi ve Ticaret Limited Şirketi
- 2022/334, 335,336 ve 337 - Yıldızlar Yatırım Holding AŞ, Yıldız Demir Çelik Sanayi AŞ, Yıldız Entegre Ağaç Sanayi AŞ, İstanbul Gübre Sanayi AŞ (İGSAŞ)
- 2022/304 - Yonca Sağlık Hizmetleri Ltd. Şti.
- 2022/209 - Martı İleri Teknoloji A.Ş.
- 2022/157 - Arı İnovasyon ve Bilim Eğitim Hizmetleri Anonim Şirketi (İTÜ ETA Vakfı Doğa Koleji)
- 2022/156 - Kentyol Kent Hizmetleri AŞ
- 2022/155 - Şişli Belediye Başkanlığı
- 2022/154 - T.C. Acıbadem Mehmet Ali Aydınlar Üniversitesi
- 2022/124 - Kent Konut İnşaat Sanayi ve Ticaret Anonim Şirketi
- 2022/94 - Pizza Restaurantları AŞ (Dominos Pizza)
- 2022/93 - Moncler İstanbul Giyim ve Tekstil Ticaret Ltd. Şti.
- 2022/92 - Industries S.p.A.
- 2022/16 - Logo Yazılım Sanayi ve Ticaret AŞ
- 2021/1327 - Eureko Sigorta AŞ
- 2021/1326 - GoDaddy.com, LLC ("GoDaddy")
- 2021/1231 - T.C. İstanbul Kültür Üniversitesi

- 2021/1175 - Media Markt Turkey Ticaret Limited Şirketi
- 2021/1168-1174 - May Şirketler Grubu
- 2021/1146 - Tasfiye Halinde Hedefevim Gayrimenkul ve Otomotiv Tic. AŞ
- 2021/1099 - İzmir Bakırçay Üniversitesi
- 2021/1027 - Panasonic Business Support Europe GmbH
- 2021/983 - Elginkan Topluluğu Şirketleri
- 2021/977 - Art Sistem Bilgisayar ve Güvenlik Teknolojileri Ltd. Şti
- 2021/951 - Arvato Lojistik Dış Ticaret ve E-Ticaret Hizmetleri AŞ
- 2021/895 - AK Gıda Sanayi ve Ticaret AŞ
- 2021/875 - MNG Kargo Yurtiçi ve Yurtdışı Taşımacılık AŞ
- 2021/874 - Sinoz Kozmetik Sanayi Ticaret AŞ
- 2021/844 - Subway International B.V.
- 2021/843 - Pied Piper Fansub (piedpiperfb.com)
- 2021/787 - Oriflame Kozmetik Ürünleri Ticaret Limited Şirketi
- 2021/758 - Motor Trend Group LLC
- 2021/752 - Timurlar Sigorta Aracılık Hizmetleri Ltd. Şti.
- 2021/729 - Özel Dentapoint Dış Sağlığı Polikliniği
- 2021/725 - Webhosting Bilişim Teknolojileri AŞ
- 2021/677 - T. Garanti Bankası AŞ
- 2021/675 - Cosmolog Kozmetik Sanayi ve Ticaret AŞ
- 2021/633 - INTERGEN Genetik ve Nadir Hastalıklar Tanı Araştırma & Uygulama Merkezi
- 2021/593 - Prof. Dr. Birol CİVELEK
- 2021/728 - Düzen Biyolojik Bilimler Araştırma Geliştirme ve Üretim A.Ş.
- 2021/517 - Pakten Sağlık Ürünleri Sanayi ve Ticaret AŞ (onlemmarket.com)
- 2021/537 - Rahmet Rağıp Kuğu (Serbest Muhasebeci Mali Müşavir)
- 2021/502 - Eliptik Yazılım ve Ticaret AŞ (BtcTurk)
- 2021/498 - E-Data Teknoloji Pazarlama Anonim Şirketi
- 2021/517 - Pakten Sağlık Ürünleri Sanayi ve Ticaret AŞ (onlemmarket.com)
- 2021/272 - Acer Bilişim Teknolojileri Limited Şirketi
- 2021/271 - Acer Sales International SA
- 2021/222 - Adım Adım Oluşumu
- 2021/329 - Air India Limited

- 2021/414 - Akademisyen Yayınevi Kitabevi Dağıtım Bilgisayar Tercümanlık İth. İhr. Tic. AŞ
(www.nobelkitabevi.com.tr)
- 2020/486 - Avivasa Emeklilik ve Hayat A.Ş.
- 2020/487 - Avon Kozmetik Ürünleri Sanayi ve Ticaret A.Ş.
- 2020/631 - Barilla Gıda A.Ş.
- 2021/463 - Bulut Elektromarket Bilgi Teknolojileri ve Dış Tic. AŞ
- 2020/863 - Çizgi Telekomünikasyon A.Ş.
- 2021/462 - ClearVoiceResearch.com, LLC
- 2020/635 - Dap Rotana Dalga ve Vazo Rezidans Toplu Yapı Yöneticiliği
- 2020/737 - PSL Elektronik San. ve Tic. A.Ş.
- 2020/636 - Rezzan Günday (Şimşek Eczanesi)
- 2020/485 - Sezgi Dental Ağız ve Diş Sağlığı Polikliniği
- 2021/382 - Sine İtiryat Par. Tem. Ür. Gıd. İnş. Mim. Müh. İth. İhr. ve Tic. AŞ
- 2021/132 - So CHIC Mağazacılık San. ve Tic. AŞ
- 2021/18 - T.C. Özyeğin Üniversitesi
- 2020/207 - Türk Ekonomi Bankası A.Ş.
- 2020/290 - Turkon Holding A.Ş. ve Grup Şirketleri
- 2020/984 - UiPath SRL
- 2020/848 - UPI Trans Dış Ticaret AŞ
- 2020/789 - Vatan Bilgisayar Sanayi ve Ticaret AŞ
- 2021/326 - West Gate Toplu Yapı Sitesi Yöneticiliği
- 2020/675 - Yalova Belediyesi
- 2021/376 - Yapı ve Kredi Bankası AŞ
- 2021/321 - Yemek Sepeti Elektronik İletişim Perakende Gıda Lojistik AŞ
- 2020/830 - Hanon Automotive Climate Sys. Manufacturing Industrial and Commercial Co.
- 2021/351 - Pierre Fabre Dermokozmetik Ltd. Şti.
- 2021/350 - Pierre Fabre İlaç AŞ
- 2019/286 - Gardrops Elektronik Hizmetler ve Ticaret Anonim Şirketi
- 2021/444 - DLSY Adi Ortaklığı
- 2020/206 - Doğa Sigorta A.Ş.
- 2020/540 - Doktor Atadan Egemen KOYUNCU
- 2020/443 - EasyJet Plc
- 2020/46 - Exeltis İlaç Sanayi ve Ticaret A.Ş.

- 2021/194 - Fibabanka AŞ
- 2020/1011 - Ficosa International Otomotiv San. ve Tic. AŞ
- 2020/987 - Ficosa Otomotiv San. ve Tic. AŞ
- 2020/555 - Fluke Corporation ve Fluke Electronics Corporation
- 2021/323 - Generali Sigorta AŞ
- 2020/211 - Gratis İç ve Dış Tic. A.Ş.
- 2020/600-601-602-603-604 - Penti Giyim Sanayi ve Ticaret Anonim Şirketi ve İştirakleri
- 2020/554 - Mert Grup Sigorta Aracılık Hizmetleri Ltd. Şti.
- 2021/192 - Oto Rapor Araç Muayene ve Ekspertiz Hizmetleri San. ve Tic. AŞ
- 2020/82 - Microsoft Corporation
- 2020/468 - Halk Sigorta A.Ş.
- 2020/986 - Otokur Otomotiv İnşaat Turizm Sanayi ve Ticaret A.Ş.
- 2020/857-858-859-860-861-862 - Kale Holding A.Ş. ve Grup Şirketleri
- 2019/406-407-408-409-410 - CM Holding A.Ş. ve Grup Şirketleri
- 2021/386 - Karacabay Turizm San. ve Dış Tic. Ltd. Şti.
- 2020/634 - Kariyer.net Elektronik Yayıncılık ve İletişim Hiz. A.Ş.
- 2019/384 - Küçükçekmece Belediyesi
- 2019/381 - T. Garanti Bankası A.Ş.
- 2019/401 - Doğu Planet Elektronik Ticaret ve Bilişim Hizmetleri A.Ş. (n11.com)
- 2019/360 - Edenred Kurumsal Çözümler A.Ş.
- 2019/313 - EDS Enjeksiyon Dök. San. Tic. AŞ.
- 2019/311 - Premierdc Veri Merkezi A.Ş.
- 2019/286 - Gardrops Elektronik Hizmetler ve Ticaret Anonim Şirketi
- 2019/285 - Zynga Game Ireland Limited
- 2019/281 - Furtrans Denizcilik Ticaret ve San. A.Ş.
- 2019/268 - Türkiye İş Bankası A.Ş.
- 2019/267 - FER Gayrimenkul Geliştirme ve İnş. A.Ş.
- 2019/230 - DenizBank A.Ş.
- 2019/219 - Türk Ekonomi Bankası A.Ş.
- 2019/190 - Pizza Restaurantları A.Ş. (Domino's Pizza)
- 2019/181 - Metro Grosmarket Bakırköy Alışveriş Hiz.Tic.Ltd.Şti.
- 2019/178 - Vodafone Telekomünikasyon A.Ş.
- 2019/169 - Bartu Turizm Yatırımları A.Ş.

- 2019/130 - Microsoft Corporation
- 2019/74 - Hunko Motorlu Araçlar San. Ve Tic. Ltd. Şti.
- 2019/73 - ASF Otomotiv A.Ş.
- 2019/72 - Kaya Seyehat Turizm San. Ve Dış. Tic. Ltd. Şti.
- 2019/67 - Turmobil Turizm Rent a Car Taşımacılık ve Nakliyat San. Tic. Ltd. Şti.
- 2019/56 - Adnan Özen İnşaat Taah. En. Turz. Tiç. ve San. A.Ş.
- 2019/43 - ING Bank A.Ş.
- 2019/35 - Borlease Otomotiv A.Ş.
- 2019/32 - Garanti Filo Yönetim Hizmetleri A.Ş.
- 2019/30 - Derindere Turizm Otomotiv San. ve Tic. A.Ş.
- 2019/29 - Clickbus Seyahat Hizmetleri A.Ş. (Nereden Nereye)
- 2019/28 - Enterprise (“Yes Oto”)
- 2019/27 - Arkas Otomotiv Servis ve Ticaret A.Ş. (“Arkas Otomotiv”)
- 2019/20 - Holiday Inn İstanbul - Şişli
- 2019/17 - Hedef Araç Kiralama ve Servis A.Ş. (HedefFilo)
- 2019/16 - Optimum Otomotiv Satış Sonrası Çözümleri Tic. A.Ş. (OPTİMUM)
- 2019/15 - TEB Arval Araç Filo Kiralama A.Ş.(TEB ARVAL)
- 2019/14 - ALD Automotive Turizm Ticaret A.Ş. (ALD AUTOMOTIVE)
- 2019/13 - ANIMOTO Inc. (Animoto)
- 2018/147 - Marriott International Inc
- 2018/124 - Cathay Pacific Airways Limited
- 2018/72 - Ticketmaster UK (Ticketmaster İngiltere) adına Biletix Bilet Dağıtım Basım ve Tic. A.Ş.
- 2018/45 - Careem Networks Teknoloji A.Ş.

Veri İhlali Bildirimi - Beytıp Sağlık Hizmetleri Ltd. Şti.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Beytıp Sağlık Hizmetleri Ltd. Şti. tarafından Kurula iletilen veri ihlal bildiriminde özetle:

- 18.02.2023 tarihinde tıp merkezi bünyesinde işlem gören hastalar ve yakınları ile ilgili tıbbi hususlardaki tüm işlemlere ilişkin kayıtların tutulduğu program ile programa giriş sağlanan bazı bilgisayarların açılmadığı, veri sorumlusu bilgisayarları ile bu bilgisayarların bağlı olduğu ağa ve bilişim sistemine kimliği belirsiz kişilerce izinsiz olarak girildiği, bahse konu programa erişimin şifrelendiği,
- İhlalden etkilenen kişisel verilerin kimlik, iletişim, özlük, hukuki işlem, müşteri işlem, işlem güvenliği, risk yönetimi, finans, pazarlama, görsel ve işitsel kayıtlar, ırk ve etnik köken ve sağlık bilgileri olduğu,
- İhlalden etkilenen kişi sayısının tam olarak bilinmediği; ancak tahmini olarak 5000 olduğu ve son bir yıla ait kayıtların etkilendiği,
- İhlalden etkilenen ilgili kişi grubunun çalışanlar, kullanıcılar ve hastalar olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 13.04.2023 tarih ve 2023/638 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Sahibinden Bilgi Teknolojileri Paz. ve Tic. A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Sahibinden Bilgi Teknolojileri Paz. ve Tic. AŞ (Sahibinden) tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusunun siber saldırıya uğraması sonucu veri ihlali gerçekleştiği,
- İhlalden etkilenen kişisel verilerin internette paylaşıldığının 27.03.2023 tarihinde tespit edildiği, ancak ihlalin başlama tarihinin henüz tam olarak tespit edilemediği,
- Yapılan araştırmada;
 - Sahibinden mağaza verilerinin (e-posta adresi verileri dışında kalan veriler) Sahibinden’in internet sitesi ve mobil uygulamasındaki ara yüzlerin çalışması için gerekli web service içeriklerinin kopyalanması suretiyle elde edildiğinin anlaşıldığı,
 - Kurumsal kullanıcılara ait e-posta adresi verilerinin kötü niyetli üçüncü kişilerce kullanıcılara şifre yenileme iletileri gönderilmesi suretiyle şifre yenileme servisinin sonuç çıktısından elde edildiğinin anlaşıldığı,
- İhlalden etkilenen kişisel verilerin genel kapsamda Sahibinden mağaza bilgileri ve kurumsal kullanıcılara ait e-posta adresi olmak üzere; kullanıcı ID, kullanıcı adı, soyadı, mağaza adı, telefon numarası, e-posta adresi, hesap kayıt tarihi, konum, kullanıcı tipi, mağaza numarası, paket kategorisi, paket statüsü, paket periyodu, mağaza ürün türü, kayıt periyodu, açılış tarihi, mağaza taahhüt başlangıç tarihi bilgileri olduğu,
- İhlalden veri sorumlusunun kurumsal kullanıcılarının etkilendiği, bu kapsamda şahıs şirketlerine ait verilerin de etkilendiği,
- İhlalden etkilenen tahmini ilgili kişi sayısının tahmini 71.422 olduğu,
- İhlalden etkilenen ilgili kişilerin ihlale ile ilgili bilgiyi “yaziliiletisim@sahibinden.com” e-posta adresi veya çağrı merkezi telefon numarası (0850 222 44 45) aracılığıyla alabileceği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 30.03.2023 tarih ve 2023/504 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Destek Bilgisayar ve İletişim Hizmetleri Tic. A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Destek Bilgisayar ve İletişim Hizmetleri Tic. A.Ş tarafından Kurula iletilen kişisel veri ihlali bildiriminde özetle;

- İhlalin; veri sorumlusunun kullanmakta olduğu sunucu, depolama üniteleri ve bazı kullanıcı makinelerindeki veri şifrenmesi ve silinmesi ile sistemde kayıtlı olan verilerin dışarı çıkarılması ve karşılığında fidye talep edilmesi şeklinde gerçekleştiği,
- Veri ihlalinin 23.03.2023 tarihinde başladığı ve aynı tarihte tespit edildiği,
- İhlalden etkilenen kişi sayının şifreleme ve blokajdan dolayı henüz tespit edilemediği,
- İhlalden etkilenen kişisel veri kategorilerinin finans, pazarlama, mesleki deneyim, görsel ve işitsel kayıtlar olduğu,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, müşteriler ve potansiyel müşteriler olduğu,
- İlgili kişilerin www.destek.as, info@destek.as, kvk@destek.as, callcenter@destek.as adreslerinin yanı sıra (yardım masası), müşteri hizmetleri numarası 0312 473 51 00 ile çağrı merkezi numarası 444 37 85 üzerinden bilgi alabilecekleri

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 30.03.2023 tarih ve 2023/503 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Getir Perakende Lojistik Anonim Şirketi – Bitaksi Mobil Teknoloji Anonim Şirketi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Getir Perakende Lojistik Anonim Şirketi (Getir) ve Bitaksi Mobil Teknoloji Anonim Şirketi (BiTaksi) tarafından Kurula iletilen veri ihlal bildirimi ve takip bildiriminde özetle;

- 11.03.2023 tarihinde Getir’in üst yönetimine ulaşan bir e-postada, kötü niyetli üçüncü bir şahsın BiTaksi (Getir’in kurucusu tarafından kurulan bir teknoloji şirketi) kullanıcılarına ait bazı kişisel verileri elinde bulundurduğunu iddia ettiği ve örnek olarak bazı veri satırlarını paylaştığı,
- 23.03.2023 tarihinde bir Getir yetkilisine ve 25.03.2023 tarihinde Getir’in kurumsal e-posta adresine kötü niyetli üçüncü kişi tarafından iletilen iki ayrı e-postada, darkwebde Getir hakkında kişisel verilerin ihlale uğradığına dair iddialara yer verildiği ve Getir müşterilerine ait olduğu iddia edilen kişisel veri içeren bağlantıların (URL) paylaşıldığı,
- Darkwebde yer alan içeriklerin Getir bünyesindeki müdahale ekibi tarafından incelenmeye başlandığı; log kayıtlarının aktarıldığı yazılımların birinde yer alan verilerin, ilgili darkweb gönderilerinde yer alan verilerle örtüştüğünün tespit edildiği,
- Öte yandan, darkwebde paylaşılan verilerin Bitaksi sistemlerinde yer alan verilerle örtüşmediği ve Bitaksi kullanıcılarının kişisel verilerinin ihlal edilmediği,
- İhlalden etkilenen kişisel verilerin, Getir kullanıcıları için; kimlik (ad, soyad, TC kimlik numarası, cinsiyet), iletişim (GSM numarası, e-posta adresi, teslimat adresi) hesap (Getir müşteri numarası ve hesap oluşturma tarihi), müşteri işlem (Getir uygulamasından verilen son sipariş tarihi ve numarası, sipariş verilen Getir dikeyi [Getir, Getir Büyük, Getir Yemek vb.], sipariş içeriği, iptal edilen sipariş sayısı ve toplam sipariş sayısı), diğer (Getir uygulamasına son giriş yapılan tarih ve konum, Getir’e verilen iletişim izinleri) bilgiler olduğu, Getir bayilerine hizmet veren kuryeler için ise; kimlik (ad, soyad), iletişim (GSM numarası), görsel ve işitsel kayıtlar (profil fotoğrafı), diğer (anlık konum bilgisi ve Getir çalışan numarası) bilgiler olduğu,

- İhlalden etkilenen tahmini kiři sayısının 5098 olduđu; ancak etkilenen her veri kategorisinin tüm ilgili kişiler için geçerli olmadığı,
- İlgili kişilerin ihlal ile ilgili olarak kisiselveriler@getir.com e-posta adresinden veya Etiler Mah. Tanburi Ali Efendi Sok. Maya Residences Sitesi, T Blok, No:13 İç Kapı NO:334 Beşiktaş/İstanbul adresinden bilgi alabilecekleri

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 30.03.2023 tarih ve 2023/496 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Akbank T.A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Akbank T.A.Ş. tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin; veri sorumlusu tüzel kişi müşterilerinin hesap açılış işlemleri için oluşturulan bir projenin kodunun yazımı sırasında mail adresi değişkeninin dinamik yazılması gerekirken statik yazılması neticesinde gerçekleştiği,
- 27.08.2022 ile 18.10.2022 tarihleri arasında hesap açılışı gerçekleştirilen bazı müşterilere ait elektronik hesap cüzdanlarının, bu müşteriler yerine hataen yine Banka müşterisi olan 20 adet tüzel kişi müşteriye (her birine farklı sayılarda) gönderildiği,
- İhlalden 5.847 banka müşterisinin etkilendiği,
- İhlalden etkilenen kişisel verilerin; kimlik, müşteri işlem ve finans kategorileri dahilinde; ad ve soyad, TC kimlik numarası, müşteri no, vergi dairesi, bireysel bankacılık hizmet sözleşmesi numarası ve tarihi, hesap numarası, şube adı, döviz kodu, IBAN, ürün adı, faiz oranı, açılış ve vade tarihi ile hesap açılış tutarı bilgileri olduğu,
- İhlalden etkilenen ilgili kişilerin akbank.com internet sitesi ve 4442525 telefon numarasından bilgi alabileceği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 22.03.2023 tarih ve 2023/463 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Marifet Saatçilik Kuym. Teks. Tur. Gıda İnş. Taah. San. ve Tic. Ltd. Şti.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Marifet Saatçilik Kuym. Teks. Tur. Gıda İnş. Taah. San. ve Tic. Ltd. Şti. tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin 07.03.2023 tarihinde başladığı ve 08.03.2023 tarihinde sona erdiği,
- İhlalin veri sorumlusunun müşterilerine mesaj göndermek için kullanmış olduğu uygulamaya ait bilgilerin yetkisiz kişiler tarafından elde edilmesi neticesinde 1.513.947 kişiye SMS gönderilmesi ile gerçekleştiği,
- Veri sorumlusunun uygulamada kayıtlı 66.000 müşterisinin bulunduğu bu sebeple SMS gönderilen telefon numaralarının uygulamayı ele geçiren kişiler tarafından sisteme yüklenildiğinin düşünüldüğü,
- İhlalin müşterilerin yaptığı geri dönüşler sonucu tespit edildiği,
- İhlalden etkilenen kişisel veri kategorisinin iletişim bilgisi olduğu,
- İlgili kişilerin veri ihlali ile ilgili olarak <https://www.marifetkuyumcu.com/> adresi ve 444 9 778 telefon numarası aracılığıyla bilgi alabileceği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 16.03.2023 tarih ve 2023/375 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Yalova Uzmanlar Sağlık Hizmetleri San.Paz.Tic.A.Ş

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Yalova Uzmanlar Sağlık Hizmetleri San.Paz.Tic.A.Ş tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- Veri sorumlusu tarafından personel ve muhasebe işlemleri için kullanılan programın veri sorumlusunun bir şubesine kurulumu sırasında kısa süreli port açıklığı sebebiyle siber saldırıya uğradığı,
- Siber saldırı sonucu program içeriğindeki verilerin silindiği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar ve hastalar olduğu,
- İhlalden çalışanlara ait ad-soyad, T.C. kimlik numarası, adres, fotoğraf, mesleki bilgiler ve kan grupları kişisel verilerinin etkilendiği, hastalara ait fatura bilgilerinin içerisinde yer alan ad, soyad bilgilerinin etkilendiği,
- İlgili programın 2012 yılından beri kullanıldığı, söz konusu programın içeriğinde tahmini 2.000.000 kayıt bulunduğu,
- İlgili kişilerin 0226-811-22-44 telefon numarasından ve info@oyh.com.tr adresinden bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 05.01.2023 tarih ve 2023/56 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Reon Sağlık Hizmetleri İnş. Tur. San ve Tic. A.Ş.(Özel Aktif Hastanesi)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Reon Sağlık Hizmetleri İnş. Tur. San ve Tic. A.Ş. (Özel Aktif Hastanesi) tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- Veri sorumlusu tarafından personel ve muhasebe işlemleri için kullanılan programın veri sorumlusunun bir şubesine kurulumu sırasında kısa süreli port açıklığı sebebiyle siber saldırıya uğradığı,
- Siber saldırı sonucu program içeriğindeki verilerin silindiği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar ve hastalar olduğu,
- İhlalden çalışanlara ait ad-soyad, T.C. kimlik numarası, adres, fotoğraf, mesleki bilgiler ve kan grupları kişisel verilerinin etkilendiği, hastalara ait fatura bilgilerinin içerisinde yer alan ad, soyad bilgilerinin etkilendiği,
- İlgili programın 2012 yılından beri kullanıldığı, söz konusu programın içeriğinde tahmini 2.000.000 kayıt bulunduğu,
- İlgili kişilerin 0226-811-22-44 telefon numarasından ve info@oyh.com.tr adresinden bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 05.01.2023 tarih ve 2023/55 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Okko Sağlık Turizm İnşaat San. ve Tic. A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Okko Sağlık Turizm İnşaat San. ve Tic. A.Ş.tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- Veri sorumlusu tarafından personel ve muhasebe işlemleri için kullanılan programın veri sorumlusunun bir şubesine kurulumu sırasında kısa süreli port açıklığı sebebiyle siber saldırıya uğradığı,
- Siber saldırı sonucu program içeriğindeki verilerin silindiği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar ve hastalar olduğu,
- İhlalden çalışanlara ait ad-soyad, T.C. kimlik numarası, adres, fotoğraf, mesleki bilgiler ve kan grupları kişisel verilerinin etkilendiği, hastalara ait fatura bilgilerinin içerisinde yer alan ad, soyad bilgilerinin etkilendiği,
- İlgili programın 2012 yılından beri kullanıldığı, söz konusu programın içeriğinde tahmini 10.000 kayıt bulunduğu,
- İlgili kişilerin 0226-811-22-44 telefon numarasından ve info@oyh.com.tr adresinden bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 05.01.2023 tarih ve 2023/54 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Sital Çizgi İnşaat Turizm ve Tekstil Anonim Şirketi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Sital Çizgi İnşaat Turizm ve Tekstil Anonim Şirketi tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusunun 05.12.2022 tarihinde fidye yazılımı saldırısına maruz kalması sonucu sunuculara erişilemediği ve bir kısım kişisel verilerin sızma ihtimalinden şüphelenilmekte olduğu,
- İhlalden çalışanlar ve müşterilerin etkilendiği,
- İhlalden etkilenen ilgili kişi sayısının henüz tespit edilemediği,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, özlük, müşteri işlem bilgileri olduğu
- İlgili kişilerin veri ihlali ile ilgili olarak www.uki.com.tr adresinden bilgi alabileceği

ifadelerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 08.12.2022 tarih ve 2022/1332 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Pamukkale Belediyesi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Pamukkale Belediyesi tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusunun web sitesine 18.11.2022 tarihinde SQL saldırısı girişiminde bulunulduğu,
- USOM bünyesinde yürütülen tehdit istihbaratı faaliyetleri kapsamında, veri sorumlusuna ait olduğu değerlendirilen bazı bilgilerin saldırganlar tarafından internette çeşitli forum sitelerinde yayımlandığının tespit edildiği ve SOME tarafından gelen uyarı ve bilgilendirme mesajı ile ihlalden haberdar olunduğu,
- İhlal ile birlikte web sitesi veri tabanında bulunan burs ve esnaf yardımı tablolarında yer alan TC kimlik numarası, adres, iletişim, ad, soyad verilerinin sızma ihtimalinden şüphelenildiği,
- İhlalden etkilenen kişi sayısının 11.000 olduğu;
- İhlalden etkilenen ilgili kişi gruplarının öğrenciler ve diğer (esnaf) kategorileri olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 24.11.2022 tarih ve 2022/1271 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Shangai Moonton Technology Co Ltd

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Shangai Moonton Technology Co Ltd tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusunun işletmekte olduğu Mobile Legends isimli oyun ile ilgili tartışma forum sitesine üye olan kullanıcılara ait verilerin bir web sitesinde paylaşılması sebebiyle veri ihlali meydana geldiği,
- Veri ihlalinin 12.09.2022 tarihinde başladığı, 15.09.2022 tarihinde sona erdiği ve 03.11.2022 tarihinde tespit edildiği,
- Veri ihlalinden 3.375 kullanıcı ve forum sitesi üyesinin etkilendiği,
- Veri ihlalinden kimlik, iletişim(e-posta), işlem güvenliği ve diğer (kullanıcı kimliği, kullanıcı adı, alan ziyaretleri, cinsiyet, kullanılan alan, puanlar, itibar, varlık, katkı puanı, kayıt tarihi, son ziyaret zamanı, kayıt sırasında kullanılan IP, son ziyaret IP'si ve son etkinlik zamanı) verilerinin etkilendiği,
- İlgili kişilerin veri ihlali ile ilgili mobilelegendsgame@moonton.com e-posta adresinden bilgi alabilecekleri

açıklamalarına yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 24.11.2022 tarih ve 2022/1264 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Aktif İnş. Taşımacılık Paz. San. ve Tic. AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Aktif İnş. Taşımacılık Paz. San. ve Tic. AŞ tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusunun 28.10.2022 tarihinde siber saldırıya maruz kalması sonucu sunucudaki muhasebe, insan kaynakları ve müşteri kayıtlarına ilişkin verilerin ve programların silindiği,
- İhlalin veri sorumlusu bünyesindeki yazılımların çalışmaması üzerine yapılan inceleme sonucunda aynı gün tespit edildiği,
- İhlalden etkilenen ilgili kişi sayısının henüz tespit edilemediği,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, özlük, hukuki işlem, müşteri işlem, işlem güvenliği, finans, mesleki deneyim, pazarlama, sağlık bilgileri ile ceza mahkumiyeti ve güvenlik tedbirleri olduğu,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, müşteriler, çocuklar ve bazı gerçek kişi tedarikçiler olduğu,
- İhlalden etkilenen ilgili kişilerin ihlale ile ilgili bilgiyi “aktif.group@hs03.kep.tr” KEP adresi, “m.bayyigit@metropolitanhotels.com.tr” e-posta adresi veya 0212 313 4242 numaralı telefondan alabileceği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 01.11.2022 tarih ve 2022/1197 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Aliza Otelcilik Turizm ve Tic. AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Aliza Otelcilik Turizm ve Tic. AŞ tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusunun 28.10.2022 tarihinde siber saldırıya maruz kalması sonucu sunucudaki muhasebe, insan kaynakları ve müşteri kayıtlarına ilişkin verilerin ve programların silindiği,
- İhlalin veri sorumlusu bünyesindeki yazılımların çalışmaması üzerine yapılan inceleme sonucunda aynı gün tespit edildiği,
- İhlalden etkilenen ilgili kişi sayısının henüz tespit edilemediği,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, özlük, hukuki işlem, müşteri işlem, işlem güvenliği, finans, mesleki deneyim, pazarlama, sağlık bilgileri ile ceza mahkumiyeti ve güvenlik tedbirleri olduğu,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, müşteriler, çocuklar ve bazı gerçek kişi tedarikçiler olduğu,
- İhlalden etkilenen ilgili kişilerin ihlale ile ilgili bilgiyi “aliza@hs03.kep.tr” KEP adresi, “kenan.done@metropolitanbosphorus.com” e-posta adresi veya 0212 334 3232 numaralı telefondan alabileceği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 01.11.2022 tarih ve 2022/1196 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - AES Otelcilik Turizm ve Tic. AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz AES Otelcilik Turizm ve Tic. AŞ tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusunun 28.10.2022 tarihinde siber saldırıya maruz kalması sonucu sunucudaki muhasebe, insan kaynakları ve müşteri kayıtlarına ilişkin verilerin ve programların silindiği,
- İhlalin veri sorumlusu bünyesindeki yazılımların çalışmaması üzerine yapılan inceleme sonucunda aynı gün tespit edildiği,
- İhlalden etkilenen ilgili kişi sayısının henüz tespit edilemediği,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, özlük, hukuki işlem, müşteri işlem, işlem güvenliği, finans, mesleki deneyim, pazarlama, sağlık bilgileri ile ceza mahkumiyeti ve güvenlik tedbirleri olduğu,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, müşteriler, çocuklar ve bazı gerçek kişi tedarikçiler olduğu,
- İhlalden etkilenen ilgili kişilerin ihlal ile ilgili bilgiyi “aes.otelcilik@hs03.kep.tr” KEP adresi veya “a.akpınar@metropolitanhotels.com.tr” e-posta adresi veya 0312 295 45 45 numaralı telefondan alabileceği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 01.11.2022 tarih ve 2022/1195 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Baykar Motorlu Araçlar A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Baykar Motorlu Araçlar A.Ş. (Peugot Bursa Bölge Bayisi) tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusu sistemlerine 14.10.2022 tarihinde siber saldırı gerçekleştiği ve sistemlerin kullanılmasının engellendiği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, kullanıcılar ve müşteriler/potansiyel müşteriler olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, özlük, hukuki işlem, müşteri işlem, işlem güvenliği, finans, mesleki deneyim, pazarlama, görsel işitsel kayıtlar ile özel nitelikli kişisel verilerden sağlık, ceza mahkûmiyeti ve güvenlik tedbirleri ile ilgili bilgiler olduğu,
- İhlalden etkilenen kişi sayısının henüz tespit edilemediği,
- İlgili kişilerin; info@baykar.biz e-posta adresinden, baykar@hs02.kep.tr Kayıtlı Elektronik Posta adresinden veya 0224 211 16 66 telefon numarasından bilgi alabilecekleri

ifadelerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 01.11.2022 tarih ve 2022/1194 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Denizli Özel Egekent Hastanesi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Denizli Özel Egekent Hastanesi tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusunun 10.10.2022 tarihinde fidye yazılımı saldırısına maruz kalması sonucu sistemlerinin şifrelendiği ve hastane sistemlerine erişim sağlanamadığı,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, kullanıcılar, aboneler, öğrenciler, müşteriler, hastalar, çocuklar, korunmaya muhtaç yetişkinler olduğu
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, lokasyon, özlük, hukuki işlem, müşteri işlem, fiziksel mekân güvenliği, işlem güvenliği, risk yönetimi, finans, mesleki deneyim, pazarlama bilgileri ile görsel ve işitsel kayıtlar olduğu,
- İhlalden etkilenen tahmini kişi sayısının 295 olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 14.10.2022 tarih ve 2022/1138 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Quick Sigorta Anonim Şirketi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Quick Sigorta Anonim Şirketi tarafından Kurula iletilen veri ihlal bildirimlerinde özetle;

- Veri sorumlusunun anlaşmalı olduğu yazılım firması tarafından yönetilen hasar yönetimi programında yer alan maddi araç hasarlarına ilişkin görsellerin yer aldığı URL'nin yetkisiz kişiler tarafından ele geçirildiği,
- Yetkisiz kişiler tarafından çeşitli ihbar ID numaraları denenerek görsellere erişilmesi ile ihlalin gerçekleştiği,
- Yapılan incelemelerde saldırganın sisteme giriş yapma denemelerinin 18.08.2022 tarihinde başarılı olduğu ve 21.08.2022 tarihinde veri çekme girişimlerine başladığının anlaşıldığı,
- İlgili programın çoğunlukla, kazaya karışmış hasarlı araçlara ait görüntülerden oluştuğu; halihazırda konuya ilişkin inceleme devam etmekle birlikte, hasar dosyasında yer alan bilgiler kapsamında:
 - Sürücülerin kimlik görseli iletmesi halinde; isim, soyisim, T.C kimlik numarası, doğum yeri, doğum tarihi, anne adı, baba adı, cinsiyeti ve fotoğrafı,
 - Sürücülerin ehliyet görseli iletmesi halinde; isim, soyisim, doğum tarihi, doğum yeri, T.C. kimlik numarası, kan grubu ve fotoğrafı,
 - Trafik kaza tespit tutanağı kapsamında adres bilgisinin bulunduğu,
- İhlalden etkilenen ilgili kişi sayısını tespit çalışmalarının devam etmekte olduğu,
- İhlalden etkilenen ilgili kişi grubunun müşteriler/potansiyel müşteriler ve trafik kazasına karışan taraflar olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 07.10.2022 tarih ve 2022/1096 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Flo Mağazacılık ve Pazarlama A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Flo Mağazacılık ve Pazarlama A.Ş. hakkında Kurumumuza iletilen ihbar sonucu yapılan değerlendirmede;

- Veri sorumlusuna ait instreet.com.tr internet sayfasının kullanıcılarına ait kişisel verilerin herkes tarafından ulaşılabilir bir internet sayfasında yayınlandığı,
- İhlalden etkilenen kişisel verilerin ad, soyad, kullanıcı adı, kullanıcı şifresi ve bu kullanıcılardan 380 kişiye ait olmak üzere kredi kartı ilk 4 ve son 4 hanesiyle bu kredi kartlarının hangi bankaya ait olduğunu gösteren bilgiler olduğu,
- İhlalden etkilenen ilgili kişi sayısının yaklaşık 3500 kişi olabileceği

tespit edilmiştir.

Söz konusu ihbar ile ilgili olarak Kişisel Verileri Koruma Kurulunun 27.09.2022 tarih ve 2022/1032 sayılı Kararı ile Kanunun 15 inci maddesinin (1) numaralı fıkrası kapsamında resen inceleme başlatılmış olup ayrıca veri sorumlusu kullanıcı bilgilerinin yayınlandığı internet sitesinde yer alan kişisel veri işleme faaliyetlerinin durdurulabilmesini teminen Sulh Ceza Hakimliğine müracaat edilmesine ve söz konusu veri ihlalinin Kurumumuzun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Özel Keystone Eğitim ve Eğitim Dan. A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Özel Keystone Eğitim ve Eğitim Dan. A.Ş tarafından Kurula iletilen veri ihlal bildiriminde özetle:

- İhlalin veri sorumlusu nezdinde çalışan eski bir öğretmenin kapatılmış e-posta adresinin açılarak, tüm okul veli ve personeline okulun muhasebe kayıtlarının, Drive'da bulunan ücret skala bilgilerinin, veli ve öğrenci isimlerinin e-posta gönderilmesi suretiyle gerçekleştiği,
- İhlalin 22.09.2022 tarihinde gerçekleştiği ve aynı gün tespit edildiği,
- İhlalden etkilenen kişisel verilerin kimlik, iletişim, özlük, hukuki işlem, işlem güvenliği, risk yönetimi, finans bilgileri ve diğer kategorilerinden oluştuğu,
- İhlalden etkilenen kişi ve kayıt sayısının henüz tespit edilemediği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, kullanıcılar, aboneler/üyeler, öğrenciler ve müşteriler/potansiyel müşteriler olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 23.09.2022 tarih ve 2022/1018 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Marmara Üniversitesi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Marmara Üniversitesi tarafından Kurula iletilen veri ihlal bildirimlerinde özetle;

- 15.09.2022 tarihinde veri sorumlusunun Bilgi Yönetim Sistemi (BYS) içerisindeki SMS gönderim servisindeki yetkili kullanıcı hesabının yetkisiz bir kişi tarafından elde edilerek SMS gönderilmesi suretiyle ihlalin gerçekleştiği,
- Ele geçirilen kullanıcı hesabının yeni kullanıcı hesapları tanımlama yetkisi olduğundan 3 yeni kullanıcı hesabı tanımı yapıldığının da tespit edildiği,
- Yetkisiz erişime konu dinamik raporlama ekranı üzerinden “toplu sms gönderimi” yapılabildiği ve üniversitede çalışan akademik ve idari personelin kimlik, iletişim ve özlük bilgilerine erişim sağlanabildiği,
- İhlalden etkilenen kişi sayısının 5698 olduğu,
- İhlalden etkilenen ilgili kişi grubunun çalışanlar ve kullanıcılar olduğu
- İhlal ile ilgili olarak ilgili kişilerin 0216 7771590 numaralı telefonu arayarak veya bidb@marmara.edu.tr adresine e-posta göndererek bilgi alabilecekleri

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 22.09.2022 tarih ve 2022/990 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Fuudy Elektronik İletişim Perakende Gıda Lojistik Anonim Şirketi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Fuudy Elektronik İletişim Perakende Gıda Lojistik Anonim Şirketi tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin hangi tarihte başladığının henüz tespit edilemediği, veri sorumlusu tarafından ihlalin 12.09.2022 tarihinde tespit edildiği,
- Veri sorumlusu kurumsal e-posta adresine ihlal iddiasına ilişkin bir e-posta gönderildiği,
- İhlal iddiasına ilişkin e-postada yer alan kayıtların Fuudy bünyesindeki kayıtlarla eşleştiği,
- İhlali gerçekleştiren kişi veya kişilerin bu bilgileri nasıl elde ettiği ve ihlalin hangi yöntemle gerçekleştirildiğinin henüz tespit edilemediği, ihlalin nasıl gerçekleştiği ile ilgili tespit çalışmalarının devam ettiği,
- İhlalden etkilenen kişisel verilerin sistemin test kısmında yer alan ad, soyadı, e-posta adresi, cep telefonu numarası ve adres ID’si olduğu, bu kişisel veriler arasında yer alan adres ID’sinin güncel nitelikte olmadığı,
- İhlalden etkilenen tahmini kişi sayısının yaklaşık olarak 81.452 olduğu, tam kişi sayısının tespitine yönelik çalışmaların devam ettiği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 22.09.2022 tarih ve 2022/987 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Biblos Alaçatı Turizm Yatırımları A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Biblos Alaçatı Turizm Yatırımları A.Ş. tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin kaynağının fidye yazılımı saldırısı ve parola saldırısı olduğu,
- İhlalin 19.08.2022 tarihinde başladığı, aynı tarihte veri sorumlusunun iş telefonlarına gönderilen mesajlar ve personeline gönderilen e-postalar aracılığıyla siber saldırının tespit edildiği,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, müşteri işlem, finans, pazarlama, görsel ve işitsel kayıtlar olduğu,
- İhlalden etkilenen özel nitelikli kişisel veri kategorilerinin sağlık bilgileri ve biyometrik veriler olduğu,
- Öte yandan insan kaynakları, ön büro ve finans departmanlarında kullanılan programlar vasıtasıyla personel bordro kayıtlarının, misafir verilerinin ve şirketin mali verilerinin ihlale maruz kalmasının ihtimal dahilinde olduğu,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, müşteriler ve potansiyel müşteriler olduğu,
- İhlalden etkilenen tahmini kişi sayısının 450 olduğu, ancak siber saldırıya uğrayan programlar ve verilerle ilgili envanter çalışmasının devam ettiği,
- İlgili kişilere ait verilerin siber saldırı sonucunda silinmesi nedeniyle bildirim yapılamadığı

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 01.09.2022 tarih ve 2022/882 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2022/891 - Posta ve Telgraf Teşkilatı Biriktirme ve Yardım Sandığı

Veri İhlali Bildirimi - Posta ve Telgraf Teşkilatı Biriktirme ve Yardım Sandığı

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Posta ve Telgraf Teşkilatı Biriktirme ve Yardım Sandığı tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Zararlı yazılımlar vasıtasıyla üyelerin bilgilerinin bulunduğu sisteme yetkisiz erişim sağlandığı,
- Yetkisiz kişiler tarafından, anne kızlık soyadı, cilt seri no gibi PTT çalışanlarının kişisel verilerinin, 3.2 gb veri tabanı yedeğinin ve sitenin tüm dosyalarının ele geçirildiğinin iddia edildiği,
- İhlalin 29.08.2022 ile 30.08.2022 tarihleri arasında gerçekleştiği ve 30.08.2022 tarihinde tespit edildiği,
- İhlalden etkilenen kişisel verilerin kimlik ve üyelik işlemlerine ait bilgiler olduğu,
- İhlalden yaklaşık 38.000 kaydın etkilendiği,
- İhlal ile ilgili çalışmaların devam etmekte olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 01.09.2022 tarih ve 2022/891 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Güreli Yeminli Mali Müşavirlik ve Bağımsız Denetim Hizmetleri Anonim Şirketi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Güreli Yeminli Mali Müşavirlik ve Bağımsız Denetim Hizmetleri Anonim Şirketi tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri ihlalinin, veri sorumlusu dosya sunucularına yapılan fidye yazılımı saldırısı sonucu gerçekleştiği,
- İhlalin 16.07.2022 tarihinde başladığı ve dosyaların çalındığı ile fidye istendiğine ilişkin metin dosyalarının bilgi sistemleri sorumlusu tarafından fark edilmesi üzerine 09.08.2022 tarihinde tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının müşteriler ve potansiyel müşteriler olduğu,
- İhlalden yeminli mali müşavirlik ve bağımsız denetim faaliyetleri kapsamında tüzel kişi müşterilerden elde edinilen ticari veriler içinde bulunan kimlik (ad, soyad), iletişim (e-posta adresi, telefon numarası) ve finans (fatura, ticari kayıtlar) kategorilerinde yer alan kişisel verilerin etkilenmiş olabileceğinin düşünüldüğü,
- İhlalden etkilenen kişi ve kayıt sayısının henüz tespit edilemediği, tespit ile ilgili çalışmaların devam ettiği,
- İhlale ilişkin olarak ilgili kişilerin kvk@gureli.com.tr e-posta adresi ile 444 9 475 - (0212) 285 01 50 telefon numaralarından bilgi alabileceği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 16.08.2022 tarih ve 2022/850 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - AstraZeneca İlaç San. ve Tic. Ltd. Şti.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz AstraZeneca İlaç Sanayi ve Ticaret Limited Şirketi tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Çalışan adaylarının, “AstraZeneca”daki açık pozisyonlara başvurabilmelerini sağlayan, veri işleyen (Workday Limited) sisteminde ihlal gerçekleştiği,
- Bir adayın kendi hesabına giriş yapmadan iş başvurusu gönderebilmesi için Workday’in, kullanıcı oturumuna ilişkin verileri izlemek adına bir JavaScript değişkeni kullandığı, bu değişkenin HTML kaynağına dahil edildiği, değişkenin değerinin, harici kariyer sitesi için HTML kaynağını inceleyen, örneğin tarayıcının "Kaynağı Görüntüle" özelliğini kullanan kullanıcılar tarafından görülebilir hale geldiği,
- Bahse konu durumdan dolayı, 13 Temmuz 2022 saat 23:53 (İstanbul saati) ila 14 Temmuz 2022 saat 05:32 arasında ve/veya 20 Temmuz 2022 saat 22:06 ila 1 Ağustos 2022 saat 23:15 arasında iş başvurusu yapan çalışan adaylarının kişisel verilerinin kısa süreliğine erişilebilir hale geldiği,
- İhlalin 31 Temmuz 2022 tarihinde tespit edildiği,
- İhlalden etkilenen kişi grubunun çalışan adayları olduğu,
- İhlalden tahmini 981 kişinin etkilendiği,
- İhlalden etkilenen kişisel verilerin; ülke, isim, e-posta, telefon numarası, maaş beklentisi, mevcut maaş bilgisi, var ise “AstraZeneca” ile önceki iş ilişkisi bilgisi, vize durumu, mevcut veya önceki işveren ile ilgili kısıtlayıcı maddelerin ayrıntıları olduğunun tahmin edildiği, buna ek olarak, çalışan adaylarının veri işleyen sistemi üzerinden gönüllü olarak da kişisel URL, iş deneyimi, eğitim, dil, yetenekler ve özgeçmiş verilerini sağlayabildiği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 11.08.2022 tarih ve 2022/831 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - NeoPets Inc.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan NeoPets Inc. tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin 17.07.2022 tarihinde gerçekleştiği ve 20.07.2022 tespit edildiği,
- Veri sorumlusunun sistemlerinin bir kısmına yönelik siber saldırı gerçekleştiğini tespit ettiği; daha sonra bir forum sitesinde saldırgan tarafından, veri sorumlusuna ait online platformdan yaklaşık 69 milyon mevcut ve eski kullanıcının verilerinin ele geçirildiğine dair paylaşım yapıldığı ve söz konusu paylaşımında kaynak kodlarını ve veri tabanını satmak amacıyla ilan yayımladığı,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim ve işlem güvenliği olduğu ancak bu konuda araştırmaların devam ettiği,
- İhlalden kullanıcılara, abonelere/üyelere ve çocuklara ait verilerinin etkilendiği,
- İhlalden etkilenen kişi ve kayıt sayısının henüz tespit edilemediği ancak ihlale konu olan online platforma kayıtlı 3.5 milyon aktif ve 65 milyon aktif olmayan hesabın bulunduğu
- Veri sorumlusunun; veri sızıntısının ne zaman ve nasıl gerçekleştiği ile ihlalden hangi verilerin etkilendiğini tespit etmek için bir adli bilişim firması ile çalışmaya başladığı

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 28.07.2022 tarih ve 2022/757 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Surtas Otomotiv ve Servis Hizmetleri Sanayi Ticaret Limited Şirketi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Surtas Otomotiv ve Servis Hizmetleri Sanayi Ticaret Limited Şirketi tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin 16.07.2022 tarihinde gerçekleştiği ve aynı gün tespit edildiği,
- İhlalin veri sorumlusu çalışanına gönderilen SMS onay kodunun kendisini yetkili olarak tanıtan kişiye telefonla bildirmesi üzerine veri sorumlusunun online işlemler sisteminin ve akabinde çalışanın telefonundaki anlık bir haberleşme uygulamasının kontrolünün ele geçirilmesi suretiyle gerçekleştiği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, müşteriler ve potansiyel müşteriler olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik (isim-soy isim), iletişim (telefon numarası), görsel ve işitsel kayıtlar (profil fotoğrafı) olduğu,
- İhlalden etkilenen kişi sayısının tahmini 1200 olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 21.07.2022 tarih ve 2022/722 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2022/687 - Knauf İnşaat ve Yapı Elemanları San. ve Tic. A.Ş ile Knauf Insulation Izolation San. ve Tic. A.Ş

Veri İhlali Bildirimi - Knauf İnşaat ve Yapı Elemanları San. ve Tic. A.Ş ile Knauf Insulation Izolation San. ve Tic. A.Ş

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Knauf İnşaat ve Yapı Elemanları San. ve Tic. A.Ş ile Knauf Insulation Izolation San. ve Tic. A.Ş tarafından Kurula iletilen veri ihlal bildirimlerinde özetle;

- Veri sorumlularının hissedarı olan veri işleyen Knauf Gips KG'in Almanya sunucularına 29.06.2022 tarihinde fidye yazılımı saldırısı gerçekleştirildiği,
- İhlalden etkilenen kişi sayısı henüz tespit edilememiş olmakla birlikte herhangi bir veri ihlalinin yaşanmamış olmasının da muhtemel olduğu; zira sorumlu olunan kişisel verilerin bulunduğu sunucuya erişim sağlanmamış olmasının ihtimal dahilinde olduğu,
- Veri sorumlularının e-posta hizmetinin bir bölümü, websitesi vasıtasıyla yürütülen süreçlerin (pazarlama, iletişim formu süreci, iş başvuru süreci vb) verileri ile iş/staj başvuru/kabul ve özlük dosyası oluşturma, muhasebe ve AGİ, izin/ mesai takip, sözleşme akdetme, mal/hizmet alım ve satış, bayilik başvuru/kabul gibi süreçlerde toplanan veriler veri işleyen sunucularında barındırıldığından ilgili kişilere ilişkin kimlik, iletişim, özlük, hukuki işlem, müşteri işlem, fiziksel mekan güvenliği, işlem güvenliği, risk yönetimi, mesleki deneyim, finans, pazarlama, görsel ve işitsel kayıtlar, sendika üyeliği, diğer, felsefi inanç, din, mezhep ve diğer inançlar, ceza mahkumiyeti ve güvenlik tedbirleri ve sağlık bilgilerinin veri ihlalden etkilenmiş olma ihtimali bulunduğu; etkilenen verilere dair detayların teknik çalışma neticesinde tespit edileceği,
- İhlalden etkilenen ilgili kişi grubu henüz tespit edilememiş olmakla birlikte veri işleyen sunucusunda verisi barındırılan ilgili kişi gruplarının: ticari ilişki kurulan gerçek kişi veya tüzel kişi ilgilisi, ziyaretçi, başvuruda bulunan kişi, çalışan adayı, çalışan adayı referansı, stajyer adayı, stajyer, tedarikçi çalışanı, sözleşme yapılan tüzel kişi yetkilisi, bayi çalışanı, çalışan ailesi olduğu bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 07.07.2022 tarih ve 2022/687 ve 2022/688 sayılı Kararları ile söz konusu veri ihlal bildirimlerinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2022/686 - Türkiye Elektrik Dağıtım A.Ş.

Veri İhlali Bildirimi - Türkiye Elektrik Dağıtım A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Türkiye Elektrik Dağıtım AŞ tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusuna ait bir çalışanın kullanıcı adı ve parolasının belirlenemeyen bir şekilde ele geçirildiği ve o kullanıcı hesabı ile sistemde kayıtlı diğer kullanıcı verilerinin bir e-posta adresine gönderim yolu ile sızdırıldığı,
- İhlalin, Bakanlık Siber Güvenlik Operasyon Merkezi tarafından Dark Web’de yapılan istihbarat çalışmaları sırasında tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar ve vatandaşlar olduğu,
- İhlalden etkilenen kişisel verilerin ad, soyad, e-posta ve cep telefonu numarası olduğu,
- İhlalden etkilenen kişi sayısının 208.000 olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 07.07.2022 tarih ve 2022/686 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Meclas Otomotiv San. ve Tic. A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Meclas Otomotiv San. ve Tic. A.Ş. tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin fidye yazılımı saldırısı ile verilerin bir kısmının şifrelenmesi suretiyle gerçekleştiği,
- İhlalin 29.06.2022 tarihinde gerçekleştiği ve aynı gün veri sorumlusuna iletilen e-posta ile tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, kullanıcılar, müşteriler ve potansiyel müşteriler olduğu,
- İhlalden etkilenen kişi ve kayıt sayısının en az 142 olduğu, sunuculara kısıtlı erişim sağlanması nedeniyle ihlalden etkilenen kişi sayısının tam olarak tespit edilemediği,
- İhlalden etkilenen kişisel veri kategorilerinin; kimlik, iletişim, özlük, işlem güvenliği, finans, pazarlama, görsel ve işitsel kayıtlar; özel nitelikli kişisel veri kategorilerinin ise sağlık bilgileri, felsefi inanç, din, mezhep bilgileri olduğu,
- İlgili kişilerin veri ihlali ile ilgili <https://www.meklas.com/tr/kvkk/> adresi aracılığıyla bilgi alabileceği

belirtilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 07/07/2022 tarih ve 2022/685 sayılı Kararı ile söz konusu veri ihlal bildirimlerinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Tofisa Tekstil Sanayi ve Ticaret Limited Şirketi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Tofisa Tekstil Sanayi ve Ticaret Limited Şirketi tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusu çağrı merkezine müşterilerden gelen aramalarda, teslim almadıkları kargo bedellerine ilişkin icra takibi başlayacağına ilişkin çeşitli hukuk bürolarından mesaj ve arama aldıkları bilgisinin verildiği,
- Yapılan kontroller sonucunda çağrı merkezini arayanların, veri işleyen (Dolunay Kargo Lojistik Otomotiv İnşaat Sanayi ve Ticaret Limited Şirketi) ile paylaşılan kişiler olduklarının tespit edildiği,
- Veri sorumlusunun veri işleyen ile iletişime geçmek istediği ancak başarısız olduğu,
- Veri sorumlusu tarafından ilgili kişilere ait isim, soyisimleri, telefon numaraları, e-posta adreslerinin veri işleyen ile paylaşmakta olduğu, ilgili kişilerin isim, soyisim ve telefon numaralarının hukuka aykırı olarak kullanıldığı,
- İhlalden etkilenen ilgili kişi gruplarının müşteriler ve potansiyel müşteriler olduğu,
- İhlalden etkilenen kişi sayısının 42.373 olduğu, bu sayının veri işleyen kayıtlarında bulunan kargo teslimi yapılmayan kişi sayısı olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 29.06.2022 tarih ve 2022/649 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

**2022/646-647-648 - ARG Denizcilik İnşaat Otomotiv Sanayi ve Ticaret Ltd. Şti, İstek Gemi İnşaa
Bakım İnşaat Hırdavat Sanayi ve Ticaret Ltd. Şti, Safter Ulubay**

**Veri İhlali Bildirimi - ARG Denizcilik İnşaat Otomotiv Sanayi ve Ticaret Ltd. Şti, İstek Gemi İnşaa
Bakım İnşaat Hırdavat Sanayi ve Ticaret Ltd. Şti, Safter Ulubay**

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz ARG Denizcilik İnşaat Otomotiv Sanayi ve Ticaret Ltd. Şti, İstek Gemi İnşaa Bakım İnşaat Hırdavat Sanayi ve Ticaret Ltd. Şti ve Safter Ulubay tarafından Kurula iletilen veri ihlal bildirimlerinde özetle;

- İhlalin bilgisayardaki dosyalara erişimin engellenmesi suretiyle gerçekleştiği,
- İhlalin kaynağının sabotaj olarak belirtildiği,
- İhlalin 21.06.2022 tarihinde gerçekleştiği ve aynı gün tespit edildiği,
- İhlalden veri sorumlusu çalışanlarına ait kimlik, iletişim ve özlük bilgilerinin etkilendiği,
- Her bir veri sorumlusu için ihlalden etkilenen kişi sayısının tahmini 2000 olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 29.06.2022 tarih ve 2022/646-647-648 sayılı Kararları ile söz konusu veri ihlal bildirimlerinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2022/? - Barçın Spor Malzemeleri Ticaret ve Sanayi Anonim Şirketi

Veri İhlali Bildirimi - Barçın Spor Malzemeleri Ticaret ve Sanayi Anonim Şirketi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz tarafından Barçın Spor Malzemeleri Ticaret ve Sanayi Anonim Şirketi tarafından Kurula iletilen veri ihlal bildirimlerinde özetle;

- 187.930 ilgili kişiye ait kişisel verilerin bulunduğu excel formatındaki dosyanın csv formatına dönüştürülmesi için kullanılan ara yazılım program aracılığıyla verilerin üçüncü kişiler tarafından elde edildiği,
- İhlalin bir internet sitesinde yer alan haber aracılığıyla öğrenildiği,
- İhlalden etkilenen ilgili kişi gruplarının kullanıcılar ve müşteriler ve potansiyel müşteriler olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik (isim, soyisim, cinsiyet), iletişim (telefon numarası, e-mail adresi), müşteri işlem (müşteri id'si) ve diğer (siteye üye olduğu tarih) bilgileri olduğu,
- Üçüncü kişilerin eline geçmiş olan excel tablosunda yer alan müşteri id'lerinin veri sorumlusu sistemlerimizdeki müşteri id'leriyle uyuşmadığı,
- İhlalden etkilenen kişi sayısının 187.930 olduğu,
- İlgili kişilerin veri sorumlusuna ait çağrı merkezi, whatsapp destek hattı, sosyal medya kanalları ve e-mail adresi aracılığıyla bilgi alabileceği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 22.06.2022 tarih ve 2022/... sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Pegasus Hava Taşımacılığı Anonim Şirketi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz tarafından Pegasus Hava Taşımacılığı Anonim Şirketi tarafından Kurula iletilen veri ihlal bildirimlerinde özetle;

- Veri sorumlusu tarafından istihdam edilen uçuş ekiplerinin uçuş planlamalarının yapılması ve gerekli koordinasyonun sağlanması amacıyla kurulan servisin tarayıcı listeleme özelliğinin açık olması sebebi ile sistemlere yetkisiz erişim söz konusu olduğu,
- 21.03.2022 tarihinde söz konusu sistemde bulunan ve açık olduğu tespit edilen browser listening (tarayıcı listeleme) özelliğinin 24.03.2022 tarihinde kapatılarak güvenlik açığının giderildiği,
- İhlalin ise daha sonra bilgi güvenliği istihbarat servisleri izleme araçları üzerinden 31.05.2022 tarihinde tespit edildiği, ayrıca sosyal medya hesapları ve bazı internet sitelerinde, konu hakkında yetkisiz erişim yapan kişilerce kendilerini tanıtıcı metinler yayımlandığı,
- Yetkisiz erişim sağlayan üçüncü kişilerin paylaşımları üzerine, kendileri ile iletişime geçilerek, erişilen kişisel verilerin imha edilmesinin talep edildiği;
- İhlalden etkilenen kişisel verilerin kimlik, iletişim ve lokasyon kategorileri dahilinde; pilot ve kabin ekibi çalışanlarının adı, soyadı, telefon numarası, e-posta adresi, unvanı, geçmiş tarihlerde yapmış oldukları uçuş bilgileri, uçuş lokasyonları ile bu çalışanların bir kısmının fotoğraf ve imza görselleri olduğu,
- Veri ihlalinden etkilenen kişi sayısının henüz tespit edilemediği ve bu konuda çalışmaların devam ettiği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 07.06.2022 tarih ve 2022/569 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - MBtech Mühendislik ve Danışmanlık Ltd. Şti.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz MBTech Mühendislik ve Danışmanlık Ltd. Şti. tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusunun fidye yazılımı saldırısına maruz kaldığı,
- 28.05.2022 tarihide tespit edilen ihlalin başlama tarihinin araştırıldığı,
- İhlalden etkilenen kişisel veri kategorilerinin; kimlik, iletişim, lokasyon, özlük, müşteri işlem, finans, mesleki deneyim ve görsel ve işitsel kayıtlardan oluştuğu; bu verilere ilişkin detayların hala araştırıldığı,
- İhlalden etkilenen kişi sayısının 500 olduğu; bu kişilerin çalışanlar, kullanıcılar ve müşteriler/potansiyel müşteriler olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 02.06.2022 tarih ve 2022/554 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Baydöner Restoranları A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Baydöner Restoranları A.Ş. tarafından Kurula iletilen veri ihlal bildirimlerinde özetle;

- İhlalin veri sorumlusunun Bilgi İşlem Yöneticisinin bilgisayarının zararlı bir yazılım ile saldırıya uğraması ve web servis şifrelerinin ele geçirilmesi sonucu gerçekleştiği,
- İhlalin 21.05.2022 tarihinde gerçekleştiği ve 22.05.2022 tarihinde tespit edildiği,
- İhlalden etkilenen kişi gruplarının çalışanlar, kullanıcılar ve aboneler/üyeler olduğu,
- İhlalden etkilenen kişisel verilerin; müşterilerin isim, e-posta, cep telefonu, cinsiyet, yaşadığı şehir bilgileri olduğu,
- İhlalden etkilenen kişi sayısının 505.337 olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 26.05.2022 tarih ve 2022/536 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - ZkSoftware The Advanced Biometric Solution Elektronik San. ve Tic. Ltd. Şti.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz ZkSoftware The Advanced Biometric Solution Elektronik San. ve Tic. Ltd. Şti. tarafından Kurula iletilen veri ihlal bildirimlerinde özetle;

- Veri sorumlusunun iki veri depolama alandaki dosyalarının crypto şifreleme ile kilitlendiği,
- İhlalin 22.05.2022 tarihinde gerçekleştiği ve 23.05.2022 tarihinde sunucu bilgisayarında bulunan muhasebe yazılımımıza erişilememesi ile tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının veri sorumlusu çalışanları ve müşteriler olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin; Kimlik (T.C kimlik numarası, ad ve soyad), İletişim (e-posta adresi ve telefon numarası), Özlük (personale ait özgeçmiş bilgileri), Müşteri İşlem (müşterilerin geçmişte satın aldığı ürünlere ait fatura ve sipariş bilgileri), Finans (müşterilerin alacakları ya da borç bilgileri), Pazarlama bilgileri (müşterilerin satın aldığı ürün bilgileri) olduğu
- İhlalden yaklaşık olarak 1000 gerçek kişinin etkilendiği,
- İlgili kişilerin ihlal ile ilgili info@zksoftware.tr e-posta adresinden ve 0850 811 11 95 telefon numarasından bilgi alabilecekleri

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 26.05.2022 tarih ve 2022/535 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Yıldız Teknoloji Geliştirme Bölgesi Teknopark AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Yıldız Teknoloji Geliştirme Bölgesi Teknopark AŞ tarafından Kurula iletilen veri ihlal bildirimlerinde özetle;

- İhlalin 03.05.2022 tarihinde veri sorumlusuna ait sistemlere siber saldırı gerçekleştirilmesi neticesinde sistemlerin devre dışı bırakılması ile gerçekleştiği,
- 05.05.2022 tarihinde fidye talep edilen bir not bulunması sonucu veri ihlalinin tespit edildiği,
- İhlalden etkilenen sistemlerin, veri sorumlusuna ait Argeportal, EBYS, eBA, PDKS, Logo yazılım ve şirket içi ortak alan olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, lokasyon, özlük, müşteri işlem, finans, mesleki deneyim bilgileri olduğu,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, kullanıcılar ve müşteriler olduğu,
- İhlalden etkilenen kişi sayısının henüz tespit edilemediği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 12.05.2022 tarih ve 2022/478 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Keyubu İnternet ve Bilişim Hizmetleri

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Keyubu İnternet ve Bilişim Hizmetleri (Keyubu) tarafından Kurumumuza gönderilen veri ihlali bildiriminde özetle;

- Veri sorumlusunun kullandığı sunucular üzerinde kurulu OnatWeb Auto VM sanal sunucu yönetimi yazılımında meydana gelen bir açık nedeniyle siber saldırı düzenlendiği ve tüm sunuculardaki verilerin imha edildiği,
- İhlalin 18.04.2022 tarihinde gerçekleştiği ve aynı gün tespit edildiği,
- İhlalden etkilenen ilgili kişi grubunun müşteriler olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, müşteri işlem ve işlem güvenliği bilgileri olduğu,
- Bunun yanında Keyubu üzerinden web hosting ve sanal sunucu alan kullanıcıların burada barındırdığı verilerin de imha edildiği ancak içeriğinde kaç kişiye ilişkin ne tür verilerin bulunduğu veri sorumlusunca tespit edilemediği,
- İhlal ile ilgili info@keyubu.com e-posta adresi üzerinden bilgi alınabileceği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 28.04.2022 tarih ve 2022/446 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Paketman E-Ticaret Sanayi Ticaret AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Paketman E-Ticaret Sanayi Ticaret Anonim Şirketi tarafından Kurumumuza iletilen veri ihlal bildirimlerinde özetle;

- Siber saldırganlar tarafından veri sorumlusuna ait veri tabanı sistemine bir siber saldırı gerçekleştirilerek, veri tabanı içerisindeki verilerin silinmesi, söz konusu verilerin saldırganlarca ele geçirilmesi ve sonrasında fidye talep edilmesi suretiyle veri ihlali olduğu,
- İhlalin 21.04.2022 tarihinde gerçekleştiği ve aynı gün tespit edildiği,
- İhlalden etkilenen kişisel verilerin kimlik (ad, soyad), iletişim (e-posta, telefon) ve lokasyon (adres) verileri olduğu,
- İhlalden etkilenen ilgili kişi sayısının 1.362 olduğu,
- İhlalden etkilenen ilgili kişi grubunun kullanıcılar olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 28.04.2022 tarih ve 2022/441 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Magna Ventures Yazılım ve Teknoloji Girişimleri Ticaret Anonim Şirketi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Magna Ventures Yazılım ve Teknoloji Girişimleri Ticaret Anonim Şirketi tarafından Kurumumuza gönderilen veri ihlali bildiriminde özetle;

- Veri sorumlusu ürünlerinden biri olan ve internet erişimi ile farklı lokasyonlarda, internete bağlı olarak kişiye özel çalışma alanı sunan Poda Mobil Uygulamasına yetkisiz kişilerce erişildiği,
- Sisteme yetkisiz erişim sağlayan kişilerce veri tabanı şifresinin ele geçirildiği,
- 20.04.2022 tarihinde tespit edilen ihlalin ne zaman gerçekleştiğinin bilinmediği,
- Uygulamaya üye olan kullanıcıların ad, soyad, e-posta adresi ve telefon numaralarına erişildiği,
- Uygulamaya 7823 üye kaydının bulunduğu,
- İhlalden etkilenen ilgili kişi grubunun üyeler olduğu,
- İhlalden etkilenen kişilerin olduğunun tespit edilemediği, tespit edilmesi halinde gerekli bildirimlerin poda@poda.com.tr e-posta adresi ve 0850 290 30 90 whatsapp çağrı merkezi aracılığı ile yapılacağı

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 28.04.2022 tarih ve 2022/440 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Villacım Emlak Turizm İnşaat Sanayi ve Ticaret Limited Şirketi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Villacım Emlak Turizm İnşaat Sanayi ve Ticaret Limited Şirketi tarafından Kurula iletilen veri ihlal bildirimlerinde özetle;

- Veri sorumlusuna ait internet sitesi (“<https://www.villacim.com.tr/>”) üzerinden Cross Site Scripting saldırısı gerçekleştirilerek müşterilere ait telefon numarası bilgilerinin ele geçirildiği ve saldırganlar tarafından müşterilere bir kampanya mesajı gönderildiği, akabinde veri sorumlusundan fidye talebinde bulunulduğu,
- İhlalin 12.04.2022 tarihinde gerçekleştiği ve aynı gün tespit edildiği,
- Veri sorumlusu tarafından ilgili kişilere ait ad, soyad, TC kimlik numarası, telefon ve adres bilgilerinin işlendiği belirtilmiş olup saldırganların elinde hangi verilerin olduğunun tam olarak tespit edilemediği,
- İhlalden etkilenen ilgili kişi sayısının tahmini 35.956 olduğu,
- İhlalden etkilenen ilgili kişi grubunun müşteriler olduğu,
- İlgili kişilerin veri ihlali ile ilgili bilgiyi +90 850 532 6802 numaralı telefon veya info@villacim.com.tr e-posta adresi üzerinden alabileceği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 21.04.2022 tarih ve 2022/404 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2022/334, 335,336 ve 337 - Yıldızlar Yatırım Holding AŞ, Yıldız Demir Çelik Sanayi AŞ, Yıldız Entegre Ağaç Sanayi AŞ, İstanbul Gübre Sanayi AŞ (İGSAŞ)

Veri İhlali Bildirimi - Yıldızlar Yatırım Holding AŞ, Yıldız Demir Çelik Sanayi AŞ, Yıldız Entegre Ağaç Sanayi AŞ, İstanbul Gübre Sanayi AŞ (İGSAŞ)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Yıldızlar Yatırım Holding AŞ, Yıldız Demir Çelik Sanayi AŞ, Yıldız Entegre Ağaç Sanayi AŞ ve İstanbul Gübre Sanayi AŞ (İGSAŞ) tarafından Kurula iletilen veri ihlal bildirimlerinde özetle;

- Kimliği belirsiz siber saldırganların, henüz tespit edilemeyen bir yöntem ile veri sorumlularına ait sunucuları şifrelediği; fiziksel sunucuyu yönetmekte kullanılan yönetici parolasını değiştirerek sunucuya erişimi imkansız hale getirdiği; dosya sunucusunun olduğu alana fidye talep etmek için not bıraktığı,
- İhlalin 03.04.2022 tarihinde başladığı ve aynı gün tespit edildiği,
- Veri sorumlularına ait e-fatura, e-defter, muhasebe, lojistik, stok, personel, insan kaynakları, üretim, yönetim ve benzeri sistemlerin tamamına ilişkin verilerin şifrelendiği; şifrelenen tüm dosyaların kullanılamaz ve erişilemez halde olduğu,
- Olay müdahale ve analiz çalışmalarına devam edildiği

beyan edilmiş olup, ihlalden etkilenen kişisel veri kategorilerine, ilgili kişi gruplarına ve kişi sayısına ise bildirimde yer verilmemiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 07.04.2022 tarih ve 2022/334, 335,336 ve 337 sayılı Kararları ile söz konusu veri ihlal bildirimlerinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Yonca Sağlık Hizmetleri Ltd. Şti.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Yonca Sağlık Hizmetleri Ltd. Şti. tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusu sistemlerine siber bir saldırı gerçekleştirildiği, gerçekleştirilen saldırının tipik Ransomware, dDos, vb. gibi bir saldırı olmadığı, saldırı tipinin tespiti için incelemelerin devam ettiği,
- İhlalin 15 Mart 2022 tarihinde başladığı ve 16 Mart 2022 tarihinde tespit edildiği,
- İhlalin veri sorumlusu bünyesinde bilgi işlem müdürü olarak çalışan personele iletilen bir e-posta ile öğrenildiği,
- Saldırmanın bir metin dosyası halinde tüm klasörlerin listesini veri sorumlusuna iletmek suretiyle veritabanı ve birçok dokümanı ele geçirdiğini belgelediği,
- Saldırılan kişi veya kişilerin, klasörlerin içeriğine erişebilip erişemediği konusunda danışmanlık şirketi tarafından incelemenin devam ettiği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar ve hastalar olduğu,
- İhlalden etkilenen kişisel verilerin kimlik, iletişim, özlük, finans, mesleki deneyim, pazarlama bilgileri olduğu, ihlalden etkilenen özel nitelikli kişisel verilerin ise sağlık, ceza mahkumiyeti ve güvenlik tedbirlerine ilişkin bilgiler ile genetik veri olduğu,
- İhlalden etkilenen tahmini kişi sayısının 500.000 ve tahmini kayıt sayısının 2.500.000 olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 24.03.2022 tarih ve 2022/304 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Martı İleri Teknoloji A.Ş.

Bilindiđi üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceđi başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Martı İleri Teknoloji AŞ tarafından Kuruma iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusu sistemlerine yetkisiz kişi/kişiler tarafından erişilmesi suretiyle veri ihlalinin gerçekleştiđi,
- Veri ihlalinin yetkisiz erişen kişi/kişiler tarafından iletilen e-posta üzerine 27.02.2022 tarihinde tespit edildiđi,
- İhlalden etkilenen ilgili kişi grupları ve kişi sayısının henüz belirlenemediđi,
- İhlalden etkilenen kişisel veri kategorilerinin henüz belirlenemediđi,
- İhlalin kaynađı ve gerçekleşme yöntemine ilişkin araştırmaların devam ettiđi

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 04.03.2022 tarih ve 2022/209 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2022/157 - Arı İnovasyon ve Bilim Eğitim Hizmetleri Anonim Şirketi (İTÜ ETA Vakfı Doğa Koleji)

Veri İhlali Bildirimi - Arı İnovasyon ve Bilim Eğitim Hizmetleri Anonim Şirketi (İTÜ ETA Vakfı Doğa Koleji)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Arı İnovasyon ve Bilim Eğitim Hizmetleri Anonim Şirketi tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusu sistemlerinde yetkili bir kullanıcıya ait e-posta erişim şifresinin ele geçirildiği,
- Saldırganın e-posta şifresini elde ettikten sonra bu Portal uygulamasına giriş yaparak diğer uygulamalara erişim sağladığı ve kullanıcı yetkilerine bağlı olarak bilgilere eriştiği ve verileri sızdırdığı,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, öğrenciler ve öğrenci velileri olduğu,
- İhlalden; çalışanlara ait ad, soyad, TC kimlik numarası, çalıştığı birim ve brüt ücretleri; öğrencilere ait ad soyad, TC kimlik numarası, anne-baba adı; öğrenci velilerine ait ad, soyad, TC kimlik numarası, meslek ve kayıt tutarları bilgilerinin etkilendiği,
- İhlalden etkilenen kişi sayısının 79.997 olduğu,
- İlgili kişilerin kisiselverilerim@dogakoleji.k12.tr e-posta adresinden ihlale ilişkin bilgi alabilecekleri

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 17.02.2022 tarih ve 2022/157 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Kentyol Kent Hizmetleri AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Kentyol Kent Hizmetleri AŞ tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusunun kullanmış olduğu sunucu ve istemcilere fidye yazılımı yüklemek suretiyle bir siber saldırı gerçekleştiği ve bu saldırı sonucu dosyaların ve klasörlerin şifrelendiği,
- Veri ihlalinin 12.02.2022 tarihinde gerçekleştiği ve aynı gün tespit edildiği,
- İhlalden etkilenen kişi sayısının yaklaşık 2100 olduğu,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, kullanıcılar ve müşterilere olduğu,
- İhlalden etkilenen veri kategorileri hakkında bilgi verilmediği, uzman incelemesinin devam ettiği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 17.02.2022 tarih ve 2022/156 sayılı Kararları ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Şişli Belediye Başkanlığı

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Şişli Belediye Başkanlığı tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusunun kullanmış olduğu sunucu ve istemcilere fidye yazılımı yüklemek suretiyle bir siber saldırı gerçekleştiği ve bu saldırı sonucu dosyaların ve klasörlerin şifrelendiği,
- Veri ihlalinin 12.02.2022 tarihinde gerçekleştiği ve aynı gün tespit edildiği,
- İhlalden etkilenen kişi ve kayıt sayısının henüz tespit edilemediği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, kullanıcılar ve üyeler olduğu,
- İhlalden etkilenen veri kategorileri hakkında bilgi verilmediği, uzman incelemesinin devam ettiği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 17.02.2022 tarih ve 2022/155 sayılı Kararları ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - T.C. Acıbadem Mehmet Ali Aydınlar Üniversitesi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan T.C. Acıbadem Mehmet Ali Aydınlar Üniversitesi tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusunun fidye yazılımı saldırısına uğraması sebebiyle sunucularına kesintili olarak erişim sağlayabildiği,
- Siber saldırının 09.02.2022 tarihinde gerçekleştiği ve aynı gün tespit edildiği,
- Veri ihlali bildiriminin yapıldığı tarih itibariyle öğrenci yönetim uygulaması, sınav sistemi ve santralin tamamen sorunsuz ve erişilebilir hale getirildiği,
- Tüm sistemlerin eksiksiz çalıştırılması ile ilgili çalışmaların devam ettiği, • İhlalden etkilenen ilgili kişi grubunun kullanıcılar olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin tespit edilemediği,
- Veri sorumlusu tarafından konu ile ilgili incelemelerin devam ettiği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 17.02.2022 tarih ve 2022/154 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Kent Konut İnşaat Sanayi ve Ticaret Anonim Şirketi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Kent Konut İnşaat Sanayi ve Ticaret Anonim Şirketi tarafından Kurula iletilen veri ihlal bildiriminde özetle:

- Veri sorumlusunun fidye yazılımı ve ayrıca hizmet dışı bırakma (DoS-DDoS) saldırılarına maruz kaldığı,
- İhlalin savcılık soruşturması kapsamında yapılan çalışmalar sırasında 31.01.2022 tarihinde tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar ve müşteriler olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin; kimlik, iletişim, özlük, müşteri işlem, finans, görsel ve işitsel kayıtlar ile biyometrik veri olduğu,
- İhlalden etkilenen kişi sayısının 1000 olduğu,
- İhlal ile ilgili Kocaeli Cumhuriyet Başsavcılığına suç duyurusunda bulunulduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 10.02.2022 tarih ve 2022/124 sayılı Kararı ile söz konusu kişisel veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2022/94 - Pizza Restaurantları AŞ (Dominos Pizza)

Veri İhlali Bildirimi - Pizza Restaurantları AŞ (Dominos Pizza)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Pizza Restaurantları AŞ tarafından Kurula iletilen veri ihlali bildiriminde özetle;

- Veri sorumlusuna ulaşan bir e-posta ile 3 müşteri ve 1 eski çalışanın verilerinin ele geçirildiğinin tespit edildiği
- belirtilmiş olup söz konusu veri ihlali bildirim hakkında Kişisel Verileri Koruma Kurulunun 18.01.2022 tarih ve 2022/55 sayılı Kararı ile incelemenin devam ettirilmesine karar verilmiştir.
- İlk bildirim ardından veri sorumlusu tarafından Kurula iletilen takip bildiriminde özetle;
- Veri sorumlusuna yeni bir e-posta daha gönderildiği ve bu e-posta içinde veri sorumlusu müşterilerine ait kişisel verilerin bulunduğu,
- İhlalden etkilenen ilgili kişi grubunun müşteriler olduğu,
- İhlalden etkilenen kişisel verilerin doğum yılı, ad, soyad, cep telefonu numarası, e-posta adresi ve müşteri ID bilgileri olduğu,
- İhlalden etkilenen kişi sayısının 180.000 olduğu,
- İlgili kişilerin dominoskvk@dominospizza.com.tr e-posta adresinden ihlale ilişkin bilgi alabilecekleri

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 27.01.2022 tarih ve 2022/94 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Moncler İstanbul Giyim ve Tekstil Ticaret Ltd. Şti.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Moncler İstanbul Giyim ve Tekstil Ticaret Ltd. Şti. tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- 22 Aralık 2021 tarihinde veri sorumlusunun bağlı bulunduğu ana şirket olan Industries S.p.A bilgisayar sistemlerine yapılan bir fidye yazılımı saldırısının tespit edildiği,
- Yapılan inceleme sonucunda bilgisayar sistemlerinde yer alan bir takım verilerin şifrelendiği ve bu verilerin sızmış olabileceği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, müşteriler, iş ortakları ve sağlayıcılar olduğu,
- İhlalden etkilenen verilerin müşterilere ait kimlik, iletişim ve alışveriş geçmişi bilgileri, çalışanlara ilişkin kimlik, iletişim ve bordro verileri ile iş ilişkisi ile ilgili olabilecek sağlık bilgileri ile sağlayıcı ve iş ortaklarına ilişkin kimlik, ticari bilgiler ve iletişim bilgileri olduğu,
- İhlalden etkilenen kişi sayısının 20005 olduğu,
- İlgili kişilerin client.service_us@moncler.com e-posta adresinden ihlale ilişkin bilgi alabilecekleri bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 27.01.2022 tarih ve 2022/93 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Industries S.p.A.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Industries S.p.A. tarafından Kurula iletilen veri ihlali bildiriminde özetle;

- 22 Aralık 2021 tarihinde veri sorumlusunun bilgisayar sistemlerine yapılan bir saldırının tespit edildiği,
- Söz konusu saldırının bir Ransomware saldırısı olduğunun daha sonra tespit edildiği,
- Veri sorumlusu tarafından saldırıya anında reaksiyon gösterildiği, tüm sistemlerin kapatıldığı ve kötücül yazılımın yayılmasının engellendiği,
- Yapılan inceleme sonucunda bilgisayar sistemlerinde yer alan bir takım verilerin şifrelendiği ve bu verilerin sızmış olabileceği,
- İhlalden etkilenen ilgili kişi grubunun müşteriler olduğu,
- İhlalden etkilenen verilerin müşterilere ait kimlik, iletişim ve alışveriş geçmişine ilişkin bilgiler olduğu,
- İhlalden etkilenen kişi sayısının 31748 olduğu,
- İlgili kişilerin client.service_us@moncler.com e-posta adresinden ihlale ilişkin bilgi alabilecekleri

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 27.01.2022 tarih ve 2022/92 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Logo Yazılım Sanayi ve Ticaret AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Logo Yazılım Sanayi ve Ticaret AŞ tarafından Kurula iletilen veri ihlal bildiriminde özetle:

- Bir şahsın, veri sorumlusuna bir e-posta göndererek, bir veri sızıntısı olayı ile ilgili görüşmek istediğini belirttiği, bunun üzerine ilgili şahıs ile çevrimiçi bir görüşme gerçekleştirildiği, ilgili şahıs tarafından sızıntı olduğunun iddia edilen verilerin veri sorumlusuna iletildiği,
- Yapılan inceleme sonucunda verilerin veri sorumlusu sistemlerine ait olduğunun ve hukuka aykırı olarak ele geçirilerek ihlalin gerçekleştiğinin tespit edildiği,
- İhlalin tüm detaylarına ilişkin tespit çalışmalarının uzman kuruluşlarla beraber devam ettiği, konu ile ilgili Gebze Cumhuriyet Başsavcılığına suç duyurusunda bulunulduğu,
- İhlalden etkilenen ilgili kişi gruplarının kullanıcılar ve müşteriler/potansiyel müşteriler olduğu,
- İhlalden etkilenen kişi ve kayıt sayısını tespit çalışmalarının devam ettiği,
- Etkilenen verilerin veri sorumlusunun şahıs şirketi müşterilerine ait ad, soyad, unvan, TC kimlik numarası/vergi kimlik numarası, iletişim, finans ve müşteri işlem bilgilerinin olabileceğinin düşünüldüğü

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 06.01.2022 tarih ve 2022/16 sayılı Kararı ile söz konusu kişisel veri ihlallerinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Eureko Sigorta AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Eureko Sigorta AŞ tarafından Kuruma gönderilen veri ihlali bildiriminde özetle;

- Daha önce düzenli olarak manuel gönderilen daini mürtehinli dosyalara ait raporun sistemsel gönderiminin yapılmasına yönelik çalışıldığı, bu çerçevede testlerle sürecin başarılı olarak çalıştığının teyit edildiği, ancak parametreler canlı ortamda çalışması için taşınırken sisteme yansımaması sonucu hazırlanan raporun filtrelenmeden alıcılara gönderilmesi sebebiyle veri ihlali gerçekleştiği,
- İhlalin 17.12.2021 tarihinde gerçekleştiği ve aynı gün tespit edildiği,
- İhlalden etkilenen ilgili kişi grubunun müşteriler ve potansiyel müşteriler olduğu,
- İhlalden 601 kişinin etkilendiği,
- İhlalden etkilenen kişisel verilerin ad, soyad, TC kimlik numarası, banka, şube, poliçe bilgileri olduğu,
- İlgili kişilerin veri ihlali hakkında “esmusterihizmetleri@eurekosigorta.com.tr” iletişim kanalı üzerinden bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 23.12.2021 tarih ve 2021/1327 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - GoDaddy.com, LLC ("GoDaddy")

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12 nci maddesinin (5) numaralı fıkrası "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan GoDaddy.com, LLC ("GoDaddy") tarafından Kuruma gönderilen veri ihlali bildiriminde özetle;

- Veri sorumlusunun kullanıcılarına hizmet verdiği bir ortamda şüpheli etkinlikler tespit etmesi sonucu inceleme başlatıldığı ve 06.09.2021 tarihinde veya bu tarih yakınlarında yetkisiz kişilerce kullanıcılara ait birtakım kişisel verilere erişilmesiyle veri ihlali gerçekleştiğinin anlaşıldığı,
- İhlalin veri sorumlusu tarafından 17.11.2021 tarihinde tespit edildiği,
- İhlalden Türkiye'de bulunan 13.382 kullanıcının etkilendiği, bu kullanıcıların içerisinde tüzel kişilerin de bulunduğu,
- İhlalden veri sorumlusu tarafından atanan müşteri numarası, e-posta adresi, varsayılan WordPress yönetici (admin) oturum açma bilgileri, güvenli dosya aktarım protokolü (sFTP) ve veritabanı kullanıcı adları ve şifrelerinin etkilendiği,
- İlgili kişilerin veri ihlali hakkında "+1 480 505 8870" numaralı telefonla GoDaddy çağrı merkezi kanalı üzerinden bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 23.12.2021 tarih ve 2021/1326 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi- T.C. İstanbul Kültür Üniversitesi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan T.C. İstanbul Kültür Üniversitesi tarafından Kuruma gönderilen veri ihlali bildiriminde özetle;

- Veri sorumlusuna ait bazı kişisel verilerin karaborsada satışa çıkarıldığı öğrenilmesi üzerine yapılan araştırma sonucu ihlalin tespit edildiği,
- İhlalin Üniversite çalışanının kullandığı bilgisayarın şifresinin ele geçirilmesi sonucu öğrenci bilgilerinin yer aldığı listenin çalınması suretiyle gerçekleştiği,
- İhlalden etkilenen ilgili kişi grubunun öğrenciler olduğu,
- İhlalden 15.967 kişinin etkilendiği,
- İhlalden etkilenen kişisel verilerin; T.C. kimlik numarası, doğum tarihi, uyruk, cinsiyet, telefon numarası, kurum e-posta adresleri, ödeme durumu, öğrenci adı soyadı, öğrenci danışman adı soyadı, YÖK burs oranı bilgileri olduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 02.12.2021 tarih ve 2021/1231 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Media Markt Turkey Ticaret Limited Şirketi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Media Markt Turkey Ticaret Limited Şirketi tarafından Kuruma gönderilen veri ihlali bildiriminde özetle;

- Veri sorumlusunun bağlı olduğu Media-Markt Saturn perakende grubu ve ulusal şirketleri tarafından kullanılan sistemlerin bir siber saldırının hedefi olduğu,
- Media-Markt Saturn’ün operasyonlarının bulunduğu ülkelerde fiziksel ve çevrimiçi mağazalardaki sunucular dâhil olmak üzere yaklaşık 3200 Windows sunucusunun söz konusu ihlalden etkilendiği, bununla birlikte Linux sunucularının etkilenmediği,
- İhlalden, veri sorumlusuna ait sunucu bilgisayarın da etkilendiği ve verilerin şifrelendiği,
- Sistemde bulunan verilerin kopyalandığına veya verilerin gizliliğinin ifşa edildiğine dair hiçbir belirtinin bulunmadığı,
- 08.11.2021 tarihinde tespit edilen veri ihlalinin, 08.11.2021 tarihinde başlayıp 10.11.2021 tarihinde sona erdiği,
- Veri ihlalden etkilenen kişi gruplarının ve kişi sayısının henüz tespit edilemediği,
- Veri ihlalden etkilenen kişisel verilerin tespit edilemediği,
- Teknik inceleme ve analiz çalışmalarının devam ettiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 11.11.2021 tarih ve 2021/1175 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - May Şirketler Grubu

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

May Şirketler Grubu bünyesinde faaliyet gösteren veri sorumluları; Maykim Yağ ve Kimya Sanayi Ticaret AŞ, Maysa Yağ Sanayi AŞ, Intertank Lojistik Sanayi ve Ticaret AŞ, Maypa İç ve Dış Ticaret AŞ, Oleo Yağ ve Kimya Sanayi Ticaret AŞ, Unimar Pazarlama Ticaret AŞ ve Enviro Yağ ve Enerji Sanayi Ticaret AŞ'nin Kuruma intikal eden veri ihlal bildirimlerinde özetle:

- 01.11.2021 tarihinde sistemlerin çalışmadığının fark edilmesi üzerine fidye yazılımı saldırısına maruz kalındığının tespit edildiği,
- Dosya sistemi, elektronik posta sistemi, muhasebe ve insan kaynakları departmanının kullandığı ERP sistemi, özlük dosyaları ile resmi ve özel dosyaların şifrelendiği,
- İhlalden etkilenen verilerin kimlik, iletişim, özlük, hukuki işlem, müşteri işlem, işlem güvenliği, risk yönetimi, finans, pazarlama, görsel ve işitsel kayıtlar, ceza mahkumiyeti ve güvenlik tedbirleri kategorileri altında; veri sorumluları sunucularında bulunan tüm kişisel verilerden oluştuğu,
- İhlalden etkilenen ilgili kişilerin; çalışanlar, kullanıcılar ve müşteriler/potansiyel müşteriler olmak üzere veri sorumlularının süregelen faaliyetleri çerçevesinde verileri sistemde bulunan tüm kişiler olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 11.11.2021 tarih ve 2021/1168, 1169, 1170, 1171, 1172, 1173, ve 1174 sayılı Kararları ile söz konusu kişisel veri ihlallerinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2021/1146 - Tasfiye Halinde Hedefevim Gayrimenkul ve Otomotiv Tic. AŞ

Veri İhlali Bildirimi - Tasfiye Halinde Hedefevim Gayrimenkul ve Otomotiv Tic. AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Tasfiye Halinde Hedefevim Gayrimenkul ve Otomotiv Tic. AŞ tarafından Kuruma gönderilen veri ihlali bildiriminde özetle;

- Veri ihlalinin 29.09.2021 tarihinde veri sorumlusu çalışanları tarafından sisteme giriş yapılamadığı ve bu nedenle yazılım sistemine girilmesi gereken bilgilerin girişinin sağlanamadığının bildirilmesi ile tespit edildiği,
- Bir bilişim firmasından yardım alınarak sistemdeki sorunun tespit edilmesinin istenildiği ve bu firmanın hazırladığı rapora göre sunucu üzerinde bulunan uygulamadaki veri dosyalarının (datafile) silindiğinin tespit edildiği,
- Silinen diskte veri kurtarma uygulamaları ile yapılan çalışmalardan sonuç alınamadığı,
- Şirketin mevcut durumundan dolayı ihlalden kaç kişinin etkilediğinin tespit edilemediği ancak yaklaşık olarak 10.000 kişiye ait verilerin silinmiş olabileceğinin düşünüldüğü,
- İhlalden müşterilerin kimlik, müşteri işlem, finans verilerinin etkilendiği,
- Müşteri verilerinin çalınmış olma olasılığının bulunduğu,
- İhlale ilişkin 27.10.2021 tarihinde suç duyurusunda bulunulduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 04.11.2021 tarih ve 2021/1146 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - İzmir Bakırçay Üniversitesi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan İzmir Bakırçay Üniversitesi tarafından Kuruma gönderilen veri ihlali bildiriminde özetle;

- Veri sorumlusu kullanıcılarına ait e-posta hesaplarının şifrelerinin ele geçirilmesi amacıyla kaba kuvvet saldırısı (Brute-Force Attack) yapıldığı, bazı kullanıcıların ele geçirilen şifre bilgileri ile Üniversite Bilgi Yönetimi Sistemi (UBYS) yazılımına giriş yapıldığı ve şifresi ele geçirilen kullanıcıların üzerinden servis çağruları yapılarak rapor çıktıları elde edilmeye çalışıldığı,
- Servis çağrılarından elde edilen rapor çıktılarının da bir forum sitesinde satışa çıkarıldığı,
- İhlalin bir sosyal medya sitesi üzerinden içerik metninde üniversite isminin geçmesinin fark edilmesiyle öğrenildiği,
- İhlalin 13.10.2021 tarihinde başladığı, 14.10.2021 tarihinde sona erdiği ve 20.10.2021 tarihinde tespit edildiği,
- İhlalden öğrencilere ait ad-soyad, Türkiye Cumhuriyeti kimlik numarası, kurumsal e-posta adresleri, kayıtlı buldukları program, öğrenci kimlik ve telefon numaralarının etkilendiğinin tespit edildiği,
- Veri sorumlusu bünyesinde çalışan tüm akademik ve idari personelin ise ad-soyad, Türkiye Cumhuriyeti kimlik numarası, kurumsal e-posta adresleri ve telefon numaralarının ihlalden etkilendiğinin tahmin edildiği,
- İhlalden etkilenen kişi sayısının 5389 öğrenci ve 425 personel olmak üzere toplam 5814 kişi olduğu ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 26.10.2021 tarih ve 2021/1099 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Panasonic Business Support Europe GmbH

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Panasonic Business Support Europe GmbH tarafından Kuruma gönderilen veri ihlali bildirimlerinde özetle;

- Veri sorumlusunun sistemlerine gerçekleştirilen yetkisiz erişim neticesinde 19.07.2021, 16.08.2021 ve 17.09.2021 tarihlerinde ihlalin gerçekleştiği,
- İhlalden etkilenen kişi sayısının belirlenemediği,
- İhlalden etkilenen kayıt sayısının 71.000 olduğu,
- İhlalden etkilenen kişisel verilerin kimlik (ad, soyad) iş iletişim bilgileri (adres, telefon numarası, e-posta adresi), iletişim bilgileri (adres, telefon numarası, e-posta adresi), fotoğraf (çok az kişi için), video (4 kişi - belirli bir şirket, kişi veya yerle ilişkili değil) olduğu,
- İhlalden etkilenen ilgili kişilerin Türkiye'deki Panasonic Telefon Yardım Hattı ile Aralık 2009 ve Mayıs 2012 arasında iletişime geçen tüketiciler, 2012 ve 2014 yılları arasında Panasonic ürünleri için servis talepleri olan tüketiciler, 2009 ve 2014 yılları arasında Panasonic için çalışan servis merkezleri çalışanları olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 07.10.2021 tarih ve 2021/1027 sayılı Kararları ile söz konusu veri ihlali bildirimlerinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi- Elginkan Topluluğu Şirketleri

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Elginkan Topluluğu Şirketleri tarafından Kuruma gönderilen veri ihlali bildirimlerinde özetle;

- Siber saldırganlarca yapılan fidye yazılımı saldırısı sonucu veri sorumlularına ait sunucu, kişisel bilgisayarlar, ERP sistemlerine erişimin engellendiği ve aynı zamanda yedek sunucularında kilitlendiği,
- Elginkan Topluluğu Şirketleri bünyesinde bulunan 23 şirketin; Elginkan Vakfı, Elginkan Holding AŞ, AR Muslukçuluk Sanayi AŞ, E.C.A. Presdöküm Sanayi AŞ, EKE İnşaat Sanayi ve Tic. AŞ, Elba Basınçlı Döküm Sanayii AŞ, Elba Basınçlı Döküm Sanayii AŞ Odöksan Osmaneli Şubesi, Eleks Dış Tic. AŞ, Elgin Seyehat ve Turizm Acenteliği, Elmor Tesisat Malzemesi Tic. AŞ, Elper Sigorta Acenteliği AŞ, Elper Yatırım Holding AŞ, Elsan Hammadde Sanayi AŞ, Elsel Gaz Armatürleri San. ve Tic. AŞ, Emar Satış Sonrası Müşteri Hiz. Sanayi ve Tic. AŞ, Emas Makina Sanayi AŞ, Matel Hammadde Sanayi ve Tic. AŞ, S.S. Elginkan Topluluğu Personeli Tüketim Kooperatifi, Serel Seramik Kaplama Malzemeleri San. ve Tic. AŞ, Tezel Gıda Maddeleri İmalat ve Satış AŞ, Teztaş Tüm Eczacılık Tic. Ve San. AŞ, Valf Sanayi AŞ ve Valfsel Armatür Sanayi AŞ veri ihlalden etkilendiği,
- İhlalin 21.09.2021 tarihinde gerçekleştiği,
- İhlalden etkilenen veriler arasında ilgili kişilere ait kimlik, iletişim, özlük verileri, işlem güvenliği ve finans verilerinin bulunduğu,
- Bunların yanı sıra özel nitelikli kişisel veri olan ilgili kişilere ait sendika üyeliği bilgisinin de ihlalden etkilendiği,
- Saldırının nedeni, sonuçları ve ilgili kişiler üzerinde potansiyel etkileri hakkında veri sorumluları nezdinde araştırmaların devam ettiği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 28.09.2021 tarih ve 2021/983 sayılı Kararları ile söz konusu veri ihlali bildirimlerinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi- Art Sistem Bilgisayar ve Güvenlik Teknolojileri Ltd. Şti

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Art Sistem Bilgisayar ve Güvenlik Teknolojileri Ltd. Şti tarafından Kuruma gönderilen veri ihlali bildiriminde özetle;

- Veri sorumlusunun kendi sistemlerine girişinin yetkisiz kişi veya kişiler tarafından engellendiği, yetkisiz erişim sonucunda bir kısım yedeklerin silindiği ve bir kısım dosyaların da şifrelendiği,
- İhlalin; 15.09.2021 tarihinde saat 07:00’da başladığı ve saat 07:15’te sunucudan gelen uyarı ile tespit edildiği, 16.09.2021 saat 18:05’a kadar ihlalin devam ettiği,
- İhlalden etkilenen ilgili kişi grubunun müşteriler ve potansiyel müşteriler olduğu,
- İhlalden etkilenen kişisel verilerin; kimlik, iletişim, lokasyon, müşteri işlem ve pazarlama verileri olduğu,
- İhlalden etkilenen kişi sayısının tespit edilemediği,
- İlgili kişilerin veri ihlali hakkında veri sorumlusuna ait 0212 552 52 42 numarası ile info@artsistem.com iletişim kanalı üzerinden bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 21.09.2021 tarih ve 2021/977 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2021/951 - Arvato Lojistik Dış Ticaret ve E-Ticaret Hizmetleri AŞ

Veri İhlali Bildirimi - Arvato Lojistik Dış Ticaret ve E-Ticaret Hizmetleri AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Arvato Lojistik Dış Ticaret ve E-Ticaret Hizmetleri AŞ tarafından Kurumumuza gönderilen veri ihlali bildiriminde özetle;

- Veri sorumlusu bünyesindeki bilişim sistemlerine hukuka aykırı bir şekilde üçüncü kişi veya kişiler tarafından girilmesi ve veri sorumlusundan fidye istenmesi suretiyle 11.09.2021 tarihinde bir veri ihlali gerçekleştiği,
- Söz konusu veri ihlalinin veri sorumlusunun Logipark Tuzla’da bulunan tesisinde kullanmış olduğu bilgisayarlarda fidye talep sayfasının açılması ile 11.09.2021 tarihinde tespit edildiği,
- İhlalden etkilenen kişi ve kayıt sayısı tespit çalışmalarının devam ettiği,
- İhlalden etkilenen kişisel veri kategorilerinin tespitine dair çalışmaların devam ettiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 16.09.2021 tarih ve 2021/951 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - AK Gıda Sanayi ve Ticaret AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan AK Gıda Sanayi ve Ticaret AŞ tarafından Kuruma gönderilen veri ihlali bildiriminde özetle;

- İhlalin 25.08.2021 ile 26.08.2021 tarihleri arasında gerçekleştiği ve 26.08.2021 tarihinde tespit edildiği,
- İhlalin veri sorumlusuna ait DMZ (Savunmasız Bölge) networkünde çalışan İş Akış Süreç uygulamasının önceki versiyonlarında kullanılan ve halihazırda aktif olmayan “endpoint”in kodlarda yer almasından kaynaklanan zafiyet sebebiyle siber saldırıya maruz kaldığı ve bazı verilerinin çalındığı,
- İhlalden 185.492 müşterinin etkilendiğini,
- İhlalden etkilenen kişisel verilerin kimlik (ad, soyad, TC Kimlik No) ve iletişim (e-posta, telefon) verileri olduğu,
- İlgili kişilerin veri ihlaliyle ilgili olarak kvkk@akgida.com.tr ve www.akgida.com.tr adresinin duyurular kısmından bilgi alabilecekleri

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 03.09.2021 tarih ve 2021/895 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2021/875 - MNG Kargo Yurtiçi ve Yurtdışı Taşımacılık AŞ

Veri İhlali Bildirimi - MNG Kargo Yurtiçi ve Yurtdışı Taşımacılık AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan MNG Kargo Yurtiçi ve Yurtdışı Taşımacılık AŞ tarafından Kuruma gönderilen veri ihlali bildiriminde özetle;

- İhlalin veri sorumlusunun kurumsal müşterilere sunduğu web servis üzerinden, kurumsal müşteriye/müşterilere ait kullanıcı adı ve şifrenin elde edilmesinden kaynaklı olarak, kurumsal müşterinin/müşterilerin hesaplarına yetkisiz erişim gerçekleştiren kişi/kişiler üzerinden sızma şeklinde olduğunun ve sistemden kaynaklı bir açık olmadığı düşünülmesi,
- İhlalin 15.08.2021 tarihinde başladığı ve 23.08.2021 tarihinde sona erdiği,
- 15.08.2021 tarihinde veri sorumlusunun kurumsal bir müşterisinden gelen sözlü bildirim sonucunda aynı gün içerisinde sızma testi çalışmasına başlandığı, yapılan incelemeler sonucunda 23.08.2021 tarihinde ihlalin tespit edildiği,
- İhlalden kargo alıcılarına ait "ad-soyad, adres, telefon numarası" bilgilerinin etkilendiği,
- İhlalden etkilenen kişi sayısının belirlenemediği,
- İlgili kişilerin veri ihlali ile ilgili <https://www.mngkargo.com.tr/iletisim> internet sayfası, 0(850) 222 06 06 numaralı çağrı merkezi ve kisiselveri@mngkargo.com.tr e-posta adresinden bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 26.08.2021 tarih ve 2021/875 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2021/874 - Sinoz Kozmetik Sanayi Ticaret AŞ

Veri İhlali Bildirimi - Sinoz Kozmetik Sanayi Ticaret AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Sinoz Kozmetik Sanayi Ticaret AŞ tarafından Kurumumuza 26.08.2021 tarihinde gönderilen veri ihlal bildiriminde özetle;

- Veri tabanı güncellemesi sırasında dışarıya açık durumda olan porttan sızıntı ile veri tabanındaki müşteri bilgilerinin ele geçirildiği,
- İhlalin 23.08.2021 tarihinde gerçekleştiği,
- İhlalin güncelleme sonrası yapılan veri tabanı taraması sırasında log kayıtlarının incelenmesiyle tespit edildiği,
- İhlalden etkilenen ilgili kişi grubunun müşteriler/potansiyel müşteriler olduğu,
- İhlalden 1.352.358 kişinin etkilendiği,
- İhlalden etkilenen kişisel verilerin müşteriler ve potansiyel müşterilere ait ad, soyad, eposta ve mobil telefon bilgileri olduğu,
- İlgili kişilerin veri ihlali ile ilgili kvkk@sinoz.com.tr mail adresinden bilgi talebinde bulunabilecekleri

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 26.08.2021 tarih ve 2021/874 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Subway International B.V.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Subway International B.V. tarafından Kurumumuza gönderilen veri ihlal bildiriminde özetle;

- 13.08.2021 tarihinde, veri sorumlusuna ait “www.subwaysiparis.com” alan adlı uzaktan sipariş sitesinde bir veri ihlali gerçekleştiğinin tespit edildiği,
- Veri ihlalinin SQL veri tabanının bir kopyasının ele geçirilmesiyle meydana geldiği,
- İhlalin 03.07.2021 tarihinde gerçekleştiği ve 13.08.2021 tarihinde bir sosyal medya paylaşımı üzerine yapılan inceleme sonucunda tespit edildiği,
- İhlalden etkilenen kişi grubunun uzaktan sipariş sitesine üye olan kullanıcılar/aboneler olduğu,
- İhlalden etkilenen kişi sayısının 51.295 olduğu,
- İhlalden ilgili kişilere ait ad, soyad, e-posta adresi, uzaktan sipariş hesabının şifresi, telefon numarası, adres ve önceki siparişlere ait bilgilerin etkilendiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 18.08.2021 tarih ve 2021/844 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Pied Piper Fansub (piedpiperfb.com)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Pied Piper Fansub (piedpiperfb.com) tarafından Kuruma gönderilen veri ihlali bildiriminde özetle;

- İhlalin kurucunun tüm kullanıcı verilerinin yer aldığı sunucu hesabını bir saldırganaya vermesi ve bu verilerin yedeklerinin alınıp taşınması sırasında sızdırılması ile gerçekleştiği,
- İhlalin eski site yöneticisinin verilerin satılık olduğunu fark etmesi ile tespit edildiği,
- İhlalin 14.11.2020 tarihinde gerçekleştiği ve 14.08.2021 tarihinde tespit edildiği,
- İhlalden etkilenen kişi sayısının 50.000 olduğu,
- İhlalden etkilenen kişi gruplarının kullanıcılar ve aboneler/üyeler olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin; kimlik, iletişim, lokasyon, özlük, işlem güvenliği, mesleki deneyim, siyasi düşünce, felsefi inanç, din mezhep ve diğer inançlar, cinsel hayat, genetik veri ve diğer olduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 18.08.2021 tarih ve 2021/843 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Oriflame Kozmetik Ürünleri Ticaret Limited Şirketi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Oriflame Kozmetik Ürünleri Ticaret Limited Şirketi tarafından Kurumumuza gönderilen veri ihlal bildiriminde özetle;

- Veri ihlalinin, veri sorumlusunun ağ sunucularından birine trojan virüsü bulaştırılmasıyla gerçekleştiği,
- İhlalin 31.07.2021-01.08.2021 tarihleri arasında gerçekleştiği ve 02.08.2021 tarihinde tespit edildiği,
- Veri sorumlusunun e-posta adreslerine bir fidye e-postası gönderildiği, söz konusu fidyenin ödenmemesi halinde ele geçirildiği iddia edilen kişisel verilerin satışa çıkarılacağı tehdidinde bulunduğu,
- İhlalden etkilenen ilgili kişi grubunun çalışanlar ve müşteriler olduğu,
- İhlalden etkilenen kişi sayısının 21.655 olduğu,
- İhlalden veri sorumlusunun Türkiye’de yerleşik yabancı marka elçilerinin kimlik bilgileri ile çalışanların ad, soyad, e-posta ve telefon bilgilerinin etkilendiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 06.08.2021 tarih ve 2021/787 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Motor Trend Group LLC

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Motor Trend Group LLC tarafından Kurumumuza gönderilen veri ihlal bildiriminde özetle;

- Veri ihlalinin, veri sorumlusunun bulut sunucularına ve depolama konumlarına bilinmeyen bir üçüncü tarafın erişim sağlamasıyla gerçekleştiği,
- Saldırganlar tarafından toplam 14 veri tabanına ile bir dizi ek dosyalara erişildiği ve söz konusu verilerin sızdırıldığı,
- İhlalin 20.06.2021 tarihinde gerçekleştiği ve aynı tarihte tespit edildiği,
- İhlalden tahmini olarak 2.977 ilgili kişinin etkilendiği,
- İhlalden etkilenen ilgili kişi grubunun kullanıcılar ve üyeler/aboneler olduğu,
- İhlalden kimlik, cinsiyet bilgisi, doğum tarihi, e-posta adresi, kimlik belirleme verileri (örneğin kullanıcı adları ve şifreler), tahmini coğrafi konum hakkında genel bilgiler ve yaklaşık 5 kişi için şifre sıfırlama güvenlik sorularının cevaplarına ilişkin bilgilerin etkilendiği,
- İlgili kişilerin veri sorumlusunun internet adresi, çağrı merkezi ve e-posta adresi aracılığıyla veri ihlali hakkında bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 03.08.2021 tarih ve 2021/758 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Timurlar Sigorta Aracılık Hizmetleri Ltd. Şti.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Timurlar Sigorta Aracılık Hizmetleri Ltd. Şti. tarafından Kuruma gönderilen veri ihlal bildiriminde özetle;

- Veri sorumlusunun sigortacılık faaliyeti kapsamında sigorta teklif işlemleri için dışardan bir firmadan yazılım sistemi alıp kullanmakta olduğu,
- Yazılım sistemine yapılan siber saldırı sonucunda admin yetkisine sahip olunarak müşteri bilgilerine erişildiği,
- İhlalin 25.07.2021 tarihinde başladığı ve aynı gün saldırganlar tarafından para talep edilmesiyle ihlalin tespit edildiği,
- İhlalden etkilenen ilgili kişi grubunun müşteriler ve potansiyel müşteriler olduğu,
- İhlalden etkilenen kişi sayısının bilinmediği,
- İhlalden etkilenen kişisel verilerin; ad soyadı, kimlik numarası, telefon numarası, doğum tarihi, adres ve meslek bilgileri olduğu, ancak doğum tarihi, adres ve meslek bilgileri alanlarının doluluk oranının yüzde on civarında olduğu,
- Konuya ilişkin Cumhuriyet Başsavcılığına suç duyurusunda bulunulduğu,
- İlgili kişilerin veri ihlali hakkında veri sorumlusuna ait 0312 354 10 12 numaralı iletişim kanalı üzerinden bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 03.08.2021 tarih ve 2021/752 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2021/729 - Özel Dentapoint Diş Sağlığı Polikliniği

Veri İhlali Bildirimi - Özel Dentapoint Diş Sağlığı Polikliniği

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Özel Dentapoint Diş Sağlığı Polikliniği (İzmir) tarafından Kurumumuza gönderilen veri ihlali bildiriminde özetle;

- 12.07.2021 tarihinde yapılan siber saldırı sonucu hasta bilgilerini barındıran bilgisayarların şifrelenerek erişimin engellendiği,
- İhlalden etkilenen ilgili kişi gruplarının hastalar, müşteriler ve potansiyel müşteriler olduğu,
- İhlalden etkilenen kişisel verilerin kimlik, iletişim, lokasyon, müşteri işlem, işlem güvenliği, finans, görsel ve işitsel kayıtlar olduğu, ihlalden etkilenen özel nitelikli kişisel verilerin ise ırk ve etnik köken bilgisi ile sağlık bilgileri olduğu,
- İhlalden etkilenen kişi sayısının tahmini 14.000 olduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 19.07.2021 tarih ve 2021/729 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Webhosting Bilişim Teknolojileri AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Webhosting Bilişim Teknolojileri AŞ tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- 09.07.2021 tarihinde yurtdışı kaynaklı bir sitede 2020 yılı aralık ayına ait verilerin olduğu düşünülen kayıtların paylaşıldığı ve konuya ilişkin veri sorumlusu tarafından araştırma yapıldığı,
- Yapılan kontroller neticesinde 27.12.2020 tarihinde bir sızıntı olduğunun, log kayıtlarında ilgili tarihte müşteri verilerinin toplu olarak yurtdışında bir IP adresine gönderildiğinin ve veri sızıntısının bir kez gerçekleştiğinin tespit edildiği,
- Bir yazılım açığı sebebiyle sızıntının oluştuğunun tahmin edildiği ancak detaylı incelemenin devam ettiği,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, müşteri işlem, finans ve diğer (Müşterilerin hizmetlere ait detaylar, hizmetlere ilişkin bazı şifreleri içeren e-posta içerikleri, .tr uzantılı alan adı kayıtlarına ilişkin kimlik, şirket belgeleri, imza sirküleri, vergi levhası gibi belgeler. 15 Kasım 2020 ile 27 Aralık 2020 tarihleri arasında log kayıtlarının sehven açık bırakılması nedeniyle oluşan 3027 adet kredi kartı bilgisi) olduğu,
- Kredi kartı verisinin önemi nedeniyle ilk aşamada kart numaralarının tespit edildiği ve ödeme kuruluşuna bildirildiği,
- İhlalden etkilenen kişi sayısının henüz tespit edilemediği,
- İhlalden etkilenen kişi gruplarının çalışanlar, kullanıcılar ve müşteriler/potansiyel müşteriler olduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 13.07.2021 tarih ve 2021/725 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - T. Garanti Bankası AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan T. Garanti Bankası AŞ tarafından Kuruma gönderilen 2 adet veri ihlali bildiriminde özetle;

- Banka sistemi üzerinden Kredi Kayıt Bürosu (KKB) ekranlarına yönelik yapılan görüntülemelere ilişkin Teftiş Kurulu Başkanlığı tarafından 01.04.2020 - 15.03.2021 dönemi için uzaktan gerçekleştirilen incelemelerde, 2 farklı banka şubesinde görev alan 2 çalışanın gerçekleştirdiği görüntülemelerin dikkat çekici bulunması üzerine incelemelerin genişletildiği,
- Veri sorumlusu tarafından yapılan değerlendirme sonucu çalışanların sorgulamalara istinaden elde etmiş oldukları muhtelif müşterilere ait bilgileri 3. şahıslar ile paylaşmış olabilecekleri konusunda güçlü kanaate varıldığı,
- Bir şube çalışanın, %85'i şube müşterisi olmayan ve % 90'ı farklı müşteri segmentlerinden 3277 farklı kişiye ait KKB (Kredi Kayıt Bürosu) kaydını görüntülediği, Akyazı şubesinde bir çalışanın ise %90'ının şube müşterisi olmayan ve %70'i farklı bir şehirde ikamet eden müşterilerden 5079 farklı kişiye ait KKB (Kredi Kayıt Bürosu) kaydı görüntülemesi yaptığı,
- İhlalden etkilenen kişisel veri kategorisinin finans bilgileri olduğu,
- İlgili kişilerin veri ihlali ile ilgili www.garantibbva.com.tr, banka şubeleri ile bankanın çağrı merkezinden bilgi alabileceği

ifade edilmiştir. Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 06.07.2021 tarih ve 2021/677 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Cosmolog Kozmetik Sanayi ve Ticaret AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Cosmolog Kozmetik Sanayi ve Ticaret AŞ tarafından Kurumumuza gönderilen veri ihlali bildiriminde özetle;

- Veri sorumlusu kayıtlarında veri ihlali olduğuna ilişkin iddiaların iki adet internet sitesinde 17-18 Haziran 2021 tarihinde duyurulduğu, 25 Haziran 2021 tarihinde veri sorumlusuna haber verilmesiyle konu hakkında incelemelerin başlatıldığı,
- Yapılan incelemelerde veri sorumlusunun sistemde oluşturduğu raporların, rapor isimlerinin/URL isimlerinin herhangi bir kişi tarafından bilinmesi durumunda söz konusu raporlara erişim yetkisi verilmeyen 3. kişilerce erişilebileceğinin tespit edildiği,
- İhlalin 02.07.2021 tarihinde sona erdiği,
- İhlalinden etkilenen kişi sayısının 36.116 kişi olduğu,
- İhlalden etkilenen ilgili kişi gruplarının müşteriler olduğu,
- İhlalden etkilenen kişisel verilerin kimlik (ad-soyad), iletişim (e-posta ve adres) bilgileri olduğu,
- İlgili kişilerin veri ihlali ile ilgili guvenlik@cosmolog.com.tr e-posta adresinden bilgi alabileceği ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 06.07.2021 tarih ve 2021/675 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - INTERGEN Genetik ve Nadir Hastalıklar Tanı Araştırma & Uygulama Merkezi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan INTERGEN Genetik ve Nadir Hastalıklar Tanı Araştırma & Uygulama Merkezi tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- İşten ayrılan bilgi işlem çalışanı tarafından bulunduğu departman itibariyle yetkilerini kötüye kullanarak işten ayrılmadan önce verilerin kopyalandığı,
- İhlalden etkilenen kişi grupları arasında çalışanlar, kullanıcılar, hastalar ve çocukların olduğu,
- Adli bilgi işleme başvurulduktan sonra gelen rapor neticesinde verilerin kopyalandığının tespit edildiği,
- İhlalden etkilenen kişisel veri kategorilerinin tespit edilemediği, ihlalden etkilenmiş olabilecek kişisel veri kategorilerinin kimlik, iletişim, özlük, hukuki işlem, müşteri işlem, işlem güvenliği, risk yönetimi, finans, görsel ve işitsel kayıtlar ile özel nitelikli kişisel veri kategorilerinden sağlık bilgileri ve genetik veri kategorileri olduğu,
- İhlalden etkilenen kişi sayısının yaklaşık 10.000 olduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 28.06.2021 tarih ve 2021/633 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Prof. Dr. Birol CİVELEK

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Prof. Dr. Birol CİVELEK tarafından Kurumumuza gönderilen veri ihlali bildiriminde özetle;

- İhlalin 10 Haziran 2021 tarihinde gerçekleştiği,
- Siber saldırı sonucu, muayenehane hastalarına ait tıbbi amaçla yalnızca sır saklama yükümlülüğü altında bulunan ve doktor tarafından erişilebilen bulut ortamında yer alan fotoğrafların çalındığı,
- İhlali gerçekleştiren kişi tarafından çeşitli iletişim yolları ile tehdit mesajları alınmaya başlanması ile ihlalin tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının hastalar olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik (hastanın ismi), görsel ve işitsel kayıtlar (kaydedilen sağlık hizmetine ait öncesi sonrası fotoğraflar) olduğu,
- İhlalden etkilenen kişi sayısının 600 olduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 14.06.2021 tarih ve 2021/593 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Düzen Biyolojik Bilimler Araştırma Geliştirme ve Üretim A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Düzen Biyolojik Bilimler Araştırma Geliştirme ve Üretim A.Ş. tarafından Kuruma gönderilen veri ihlal bildiriminde özetle;

- Veri işleyen konumundaki Fransa’daki Cerba Laboratuvarında yer alan kişisel verilerin yetkisi olmayan kişiler tarafından ulaşılabilir hale geldiğinin veri sorumlusuna bildirildiği,
 - İhlalin 09.06.2021 tarihinde başladığı ve 24.06.2021 tarihinde sona erdiği,
 - Bu tarihler arasında veri sorumlusunun Cerba Laboratuvarına 991 adet numune iletmediği, ancak belirtilen tarihler arasındaki kayıtların ne kadarına ulaşıldığı veya ulaşıp ulaşılmadığının bilinmediği,
 - İhlalden etkilenen kişisel verilerin ad, soyad, doğum tarihi, cinsiyet, istenen tetkik bilgileriyle birlikte tetkik sonucu olduğu,
 - İhlalden etkilenen kişi gruplarının hastalar olduğu,
 - İlgili kişilerin veri sorumlusunun çağrı merkezinden bilgi alabileceği
- ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 13.07.2021 tarih ve 2021/728 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Pakten Sağlık Ürünleri Sanayi ve Ticaret AŞ (onlemmarket.com)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Pakten Sağlık Ürünleri Sanayi ve Ticaret AŞ tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- SQL Injection saldırısıyla veri sorumlusu internet sitesinin veri tabanı yönetim bilgilerinin ele geçirildiği,
- Saldırganlar tarafından fidye talebiyle mesaj gönderilmesiyle ihlalin tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının müşteriler olduğu,
- İhlalden siteye üye olan müşterilerin ad-soyad, adres, e-posta ve telefon numarası bilgilerinin etkilendiği,
- İhlalden etkilenen kişi sayısının 2541 olduğu,
- İlgili kişilerin e-posta: bilgi@onlem.com.tr, çağrı merkezi: 0850 201 75 40, Whatsapp Hattı: 0535 830 93 23 vasıtası ile söz konusu ihlale ilişkin bilgi alabilecekleri

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 20.05.2021 tarih ve 2021/517 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2021/537 - Rahmet Ragıp Kuğu (Serbest Muhasebeci Mali Müşavir)

Veri İhlali Bildirimi - Rahmet Ragıp Kuğu (Serbest Muhasebeci Mali Müşavir)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Rahmet Ragıp Kuğu (Serbest Muhasebeci Mali Müşavir) tarafından Kurumumuza gönderilen veri ihlali bildiriminde özetle;

- Veri sorumlusunun bilgisayar ve internet sisteminin fidye yazılımı saldırısına maruz kaldığı,
- Bilgisayar korsanlarına fidye ödenmesiyle ihlale konu sistemlerin kullanıma açıldığı,
- İhlalin 31.03.2021-06.04.2021 tarihleri arasında gerçekleştiği ve 04.04.2021 tarihinde tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, kullanıcılar, müşteriler ve potansiyel müşteriler olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, özlük, hukuki işlem, müşteri işlem, işlem güvenliği, finans, mesleki deneyim, görsel ve işitsel kayıtlar olduğu,
- İhlalden etkilenen ilgili kişi ve kayıt sayısının tam olarak tespit edilemediği, ancak yaklaşık olarak 130 gerçek ve tüzel kişi müşterinin ihlalden etkilenmiş olduğunun tahmin edildiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 27.05.2021 tarih ve 2021/537 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Eliptik Yazılım ve Ticaret AŞ (BtcTurk)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Eliptik Yazılım ve Ticaret AŞ (BtcTurk) tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- 2018 yılında kimliği belirlenemeyen bir hacker grubu tarafından illegal bir veri paylaşımı sitesinde BtcTurk sistemlerinde yer alan bazı kişisel verilerin yayımlandığı,
- Veri sorumlusunun sosyal medya platformları üzerinden konuya ilişkin etiketlenmesiyle olaydan haberdar olduğu ve konu hakkında inceleme başlattığı,
- Yapılan inceleme ve denetim neticesinde, yayınlanan bu örnek verilerin iş ortaklığı içerisinde olunan kurumlar ile kişisel verilerin korunması kapsamında yapılan sözleşmelere uygun olarak paylaşılmasından önce, Temmuz 2018 tarihinde sistem dışına çıkartılan veri setlerinden birinin taslak hali (veritabanından alınan ilk hali) olduğunun değerlendirildiği, bahse konu veri setinin depolandığı ortamda oluşan bir güvenlik ihlali neticesinde şirket dışına çıktığının düşünüldüğü,
- İhlalden etkilenen verilerin; kullanıcıların BtcTurk sistemlerinde kayıtlı kimlik verileri (ad-soyadı, doğum tarihi, TC Kimlik Numarası ve Kullanıcı numaraları / ID’si), kullanıcıların BtcTurk sistemlerinde kayıtlı, olay tarihinden önceki döneme ait iletişim verileri (e-posta adresi, cep telefonu numarası, adresi), kullanıcıların BtcTurk nezdindeki işlem güvenliği verileri (kullanıcıların olay tarihinden önceki döneme ait IP adresi, BtcTurk hesaplarına olay tarihinden önceki son giriş tarihi, kullanıcıların, mevcut teknolojik imkânlarla geri döndürülemez şekilde PBKDF2 algoritması ile maskelenmiş olay tarihinden önceki döneme ait giriş şifreleri) olduğu,
- İhlalden etkilenen kişi sayısının 516.954 olduğu,
- İhlal ile ilgili bilgi almak isteyen ilgili kişilerin “kisiselveri@btcturk.com” e-posta adresinden veya “Nispetiye Caddesi, Akmerkez E-Blok Kat:9 Beşiktaş/İstanbul” adresine iletecekleri talepler ile her zaman bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 18.05.2021 tarih ve 2021/502 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - E-Data Teknoloji Pazarlama Anonim Şirketi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan E-Data Teknoloji Pazarlama Anonim Şirketi tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- Veri ihlalinin, veri sorumlusunun “www.bayipazar.com” internet sitesine ait veri tabanının SQL injection açıklığının kullanılması sonucu kullanıcı bilgilerini içeren veri tabanına erişilmesiyle gerçekleştiği,
- Veri tabanından elde edilen kullanıcı adı ve şifre bilgileriyle internet sayfasına giriş yapıldığı,
- İhlalden etkilenen ilgili kişi sayısının 721 olduğu,
- İhlalden etkilenen kişisel verilerin ad, soyad, e-posta adresi, kullanıcı adı ve şifre bilgilerinin olduğu,
- İlgili kişilerin “kvkk@e-data.com.tr” ve “dmflegal@dmflegal.com.tr” e-posta adreslerinden veri ihlali ile ilgili bilgi edinebileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 18.05.2021 tarih ve 2021/498 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Pakten Sağlık Ürünleri Sanayi ve Ticaret AŞ (onlemmarket.com)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Pakten Sağlık Ürünleri Sanayi ve Ticaret AŞ tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- SQL Injection saldırısıyla veri sorumlusu internet sitesinin veri tabanı yönetim bilgilerinin ele geçirildiği,
- Saldırganlar tarafından fidye talebiyle mesaj gönderilmesiyle ihlalin tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının müşteriler olduğu,
- İhlalden siteye üye olan müşterilerin ad-soyad, adres, e-posta ve telefon numarası bilgilerinin etkilendiği,
- İhlalden etkilenen kişi sayısının 2541 olduğu,
- İlgili kişilerin e-posta: bilgi@onlem.com.tr, çağrı merkezi: 0850 201 75 40, Whatsapp Hattı: 0535 830 93 23 vasıtası ile söz konusu ihlale ilişkin bilgi alabilecekleri

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 20.05.2021 tarih ve 2021/517 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Acer Bilişim Teknolojileri Limited Şirketi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Acer Bilişim Teknolojileri Limited Şirketi tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- İhlalin, veri sorumlusunun, EMEA Bölgesindeki (Avrupa, Ortadoğu, Afrika- Türkiye de dahil) yerel sunucularına 14.03.2021 tarihinde bir fidye yazılımı saldırısı yapılarak EMEA Bölgesinde kullanılan sistemlerde bulunan verilerin yaklaşık yarısının şifrelenmesi sonucu gerçekleştiği,
- İhlalin nedeni, sonuçları ve ilgili kişiler üzerinde potansiyel etkileri hakkında veri sorumlusu nezdinde araştırmaların devam ettiği,
- İhlalden etkilenen kişi grubunun çalışanlar olduğu,
- İhlalden, kimlik, iletişim, özlük verileri ve özel nitelikli kişisel veri olan sendika üyeliği verilerinin etkilendiği,
- İhlalden etkilenen kişi sayısının tespit edilemediği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 18.03.2021 tarih ve 2021/272 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Acer Sales International SA

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Acer Sales International SA tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- İhlalin, veri sorumlusunun, EMEA Bölgesindeki (Avrupa, Ortadoğu, Afrika- Türkiye de dahil) yerel sunucularına 14.03.2021 tarihinde bir fidye yazılımı saldırısı yapılarak EMEA Bölgesinde kullanılan sistemlerde bulunan verilerin yaklaşık yarısının şifrelenmesi sonucu gerçekleştiği,
- İhlalin nedeni, sonuçları ve ilgili kişiler üzerinde potansiyel etkileri hakkında veri sorumlusu nezdinde araştırmaların devam ettiği,
- İhlalden etkilenen kişi grubunun müşteriler olduğu,
- İhlalden, kimlik, iletişim, müşteri işlem ve finans verilerinin etkilendiği,
- İhlalden etkilenen kişi sayısının tespit edilemediği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 18.03.2021 tarih ve 2021/271 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Adım Adım Oluşumu

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Adım Adım Oluşumu tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- İhlalin, siber saldırganların ipk.adimadim.org web sayfası veri tabanına yetkisiz erişim sağlayarak kişisel verilere hukuka aykırı erişimleri sonucu gerçekleştiği,
- İhlalin, bir internet sitesinde veri sorumlusuna ait verilerin yayınlanmasının sosyal medyadaki paylaşımlar sonucunda fark edilerek veri tabanında inceleme başlatılması ile tespit edildiği,
- İhlalin kaynağı hakkında teknik incelemelerinin devam ettiği,
- İhlalden etkilenen verilerin kimlik, iletişim, müşteri işlem, işlem güvenliği, mesleki deneyim, diğer (Eğitim bilgisi, forma ebatları ve ilgili kişilerin adına koştugu Sivil Toplum Kuruluşu'na ilişkin bilgiler) bilgiler olduğu,
- İhlalden etkilenen kişi grubunun kullanıcılar ve aboneler/üyeler olduğu,
- Etkilenen kişi sayısının henüz tam olarak tespit edilemediği ve bu konuda çalışmaların devam ettiği, etkilenen kayıt sayısının tahmini 733.000 olduğu,
- İlgili kişilerin veri ihlali ile ilgili olarak www.adimadim.org internet sayfası, iyilikpesindekos@adimadim.org e-posta adresi, sosyal medya hesapları ve 0532 623 39 02 nolu telefondan bilgi alabilecekleri

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 09.03.2021 tarih ve 2021/222 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Air India Limited

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Air India Limited tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- İhlalin, Hindistan Havayolları yolcu hizmet sistemi hizmet sağlayıcısı olarak faaliyet gösteren SITA Passenger Service System Inc'nin ("SITA") (veri işleyen) 24.02.2021 tarihinde siber saldırıya uğraması sonucu 26.08.2011 - 20.02.2021 tarihleri arasında sık uçuş gerçekleştiren kişilere ait kişisel verilerin etkilenmesi ile gerçekleştiği,
- İhlalden etkilenen kişisel verilerin 26.08.2011 - 20.02.2021 tarihleri arasında sık uçuş gerçekleştiren kişilere ait id, üyelik durumu, kullanıcı adı, toplanılan uçuş puanı, üyelik seviyesi, e-posta adresi, telefon, uçuş kodu, doğum tarihi, cinsiyeti, genel bilgiler, kredi kartı bilgileri (kredi kartı sahibinin adı, kart numarası ve karta ilişkin son kullanma tarihi) olduğu,
- İhlalden Türkiye’de kaç kişinin etkilendiği belirtilmemekle beraber etkilenen;
 - bilet sayısının 1.301.814,
 - kredi kartı sayısının 311.435,
 - sadakat kart numarasına ilişkin sayının 106.775,
 - etkilenen veri kayıt sayısının 3.639.702olduğu,
- Konuya ilişkin SITA ve adli bilişim uzmanları tarafından soruşturmaya devam edildiği ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 01.04.2021 tarih ve 2021/329 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Akademisyen Yayınevi Kitabevi Dağıtım Bilgisayar Tercümanlık İth. İhr. Tic. AŞ (www.nobelkitabevi.com.tr)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Akademisyen Yayınevi Kitabevi Dağıtım Bilgisayar Tercümanlık İth. İhr. Tic. AŞ (www.nobelkitabevi.com.tr) tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- İnternet sitesi veri tabanında bulunan tüm kullanıcı bilgilerinin kopyalandığı ve silindiği, dosyalarının silinmesi sebebiyle internet sitesinin çalışmadığının tespit edildiği,
- İhlalin 17.04.2021 tarihinde başladığı, 19.04.2021 tarihinde sona erdiği ve 18.04.2021 tarihinde tespit edildiği,
- İhlalden etkilenen kişi gruplarının kullanıcılar, aboneler/üyeler, müşteriler ve potansiyel müşteriler olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, lokasyon ve müşteri işlem bilgileri olduğu,
- İhlalden etkilenen kişi sayısının 63.294; kayıt sayısının 316.470 olduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 20.04.2021 tarih ve 2021/414 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Avivasa Emeklilik ve Hayat A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Avivasa Emeklilik ve Hayat A.Ş. (Avivasa) tarafından Kurumumuza gönderilen yazı ve ekinde özetle;

- Bir e-posta kullanıcısı tarafından 12 Haziran 2020 tarihinde Avivasa’ya iletilen ihbar sonucu inceleme çalışmalarının başlatıldığı, iletilen ihbarda bir internet sitesi üzerinden Avivasa’ya ait kişisel verilerin para karşılığında satıldığı iddiasının yer aldığı,
- İhlalden etkilenen kişisel veri kategorilerine yönelik ihbarda bilgi bulunmadığı,
- İhlalden etkilenen kişi ve kayıt sayısının bilinmediği,
- Konunun aynı zamanda adli makamlara da iletildiği,
- İlgili Sulh Ceza Hakimliğinin söz konusu internet sayfasına yönelik erişim engelleme Kararının bulunduğu

bilgilerine yer verilmiş olup, yazı ekinde yer alan ilgili erişim engelleme Kararında “...erişimin engellenmesi talebine konu olan içerik incelendiğinde, içerikte talepte bulunan şirketin müşterilerine ait olduğu değerlendirilen müşterilerin yaşadıkları şehir, yaş ve cep telefonu numarası gibi kişisel nitelikteki bir kısım verilerin liste halinde siteye konulduğu...” tespitlerinin yer aldığı anlaşılmıştır.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 23.06.2020 tarih ve 2020/486 sayılı Kararı ile söz konusu veri ihlali bildirimiminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Avon Kozmetik Ürünleri Sanayi ve Ticaret A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Avon Kozmetik Ürünleri Sanayi ve Ticaret A.Ş (Avon Türkiye) tarafından Kurumumuza gönderilen yazıda özetle;

Avon Türkiye'nin bağlı olduğu İngiltere'de yerleşik Avon Cosmetics Limited'e (Avon Global) 7 Haziran 2020 tarihinde fidye yazılımı saldırısının gerçekleştiği,

Saldırının bazı sistemlerin kesintiye uğramasına ve Türkiye'de dahil Avon'un uluslararası operasyonlarında belirli verilerin şifrelenmesine neden olduğu, etkilenen sistemlerdeki belirli verilerin tehdit aktörü tarafından kopyalanmış olması ve bu verilerin kişisel veriler içermesi ihtimalinin bulunduğu,

- Avon Türkiye'nin bağlı bulunduğu İngiltere'de yerleşik Avon Global ile aynı yazılımları kullandığı,
- Etkilenen kişisel veri kategorisi belirleme çalışmalarının devam ettiği,
- Etkilenen kişi sayısı ve kişilere ait kayıt sayısını belirleme çalışmalarının devam ettiği,
- Avon Türkiye'nin ağırlıklı olarak çalışanların ve Avon ürünlerini doğrudan satış yolu ile tüketicilere tali satıcılığını yapmakta olan Avon temsilcilerinin verilerine sahip olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 23.06.2020 tarih ve 2020/487 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Barilla Gıda A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Barilla Gıda A.Ş. tarafından Kurumumuza gönderilen yazıda özetle;

- İhlalin; 12.08.2020 tarihinde gerçekleştirilen siber saldırı ile sunucularda fidye yazılımı çalıştırılarak dosyaların ve disklerin erişilemez olmasının sağlandığı,
- Fidyecilerin bildirim ve IBM’in yaptığı incelemeye göre 4 GB kadar bir verinin dışarıya çıkartıldığı,
- Verinin içeriğinin henüz saptanamadığı, incelemelerin devam ettiği,
- İhlalden etkilenen ilgili kişi gruplarının, kişi sayısının ve ihlalden etkilenen kişisel verilerin henüz tespit edilemediği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 18.08.2020 tarih ve 2020/631 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Bulut Elektromarket Bilgi Teknolojileri ve Dış Tic. AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Bulut Elektromarket Bilgi Teknolojileri ve Dış Tic. AŞ tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- Veri sorumlusunun sunucularına bir siber saldırı gerçekleştirildiği ve saldırı sonucunda sunuculara erişimin engellendiği,
- İhlalden çalışanlar ve müşterilerin etkilendiği,
- İhlalden etkilenen kişi ve kayıt sayısının henüz bilinmediği, tespit çalışmalarının devam ettiği,
- İhlalden kimlik, iletişim, lokasyon, özlük, hukuk, işlem, müşteri işlem, işlem güvenliği, fiziksel mekan güvenliği, işlem güvenliği, risk yönetimi, finans, mesleki deneyim ve pazarlama verilerinin etkilendiği,
- Özel nitelikli kişisel veriler arasında sağlık bilgileri ve ceza mahkumiyeti ve güvenlik tedbirlerine ilişkin verilerin etkilendiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 04.05.2021 tarih ve 2021/463 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir. Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Çizgi Telekomünikasyon A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Çizgi Telekomünikasyon A.Ş. tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- 7 Kasım 2020 tarihli hafta sonu vardiyası için şirkete gelen görevli çalışanın, rutin kontrolleri yapmak için sunucuya uzaktan bağlandığında sunucu masaüstünde bir mesaj bulduğu, bunun üzerine yapılan inceleme neticesinde, müşteri bilgilerinin bulunduğu şirket sunucularında bazı kötü amaçlı yazılımların bulunduğu aynı gün tespit edildiği,
- İhlalden, T.C. kimlik numarası, ad ve soyadı, e-posta ve ev adresi, müşteri işlem detayları (kredi kartı bilgileri gibi), müşterinin satın aldığı hizmetler ve bu hizmetlere ilişkin işlemlere konu tarih-saat bilgileri gibi müşteri bilgilerinin etkilenmiş olabileceği,
- İhlalden etkilenen kişilerin şirketten hizmet alan müşteriler olduğu,
- İhlalden etkilenen kişi ve kayıt sayısının henüz bilinmediği,
- İhlal hakkında incelemenin devam ettiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 12.11.2020 tarih ve 2020/863 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - ClearVoiceResearch.com, LLC

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan ClearVoiceResearch.com, LLC tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- İhlalin yetkisiz bir kullanıcı tarafından 2015 Ağustos ve Eylül aylarına ait yedeklerin herkese açık hale getirilmesi sonucunda meydana geldiği,
- 17 Nisan 2021 tarihinde yetkisiz bir kullanıcı tarafından, ClearVoice'un 2015'teki anket katılımcılarının profil bilgilerini içeren eski veritabanlarından birine ilişkin, yedek dosyasına eriştiğini belirten bir e-posta alınması ile ihlalin tespit edildiği,
- İhlalden kimlik, iletişim, doğum tarihi, 2015 yılına ait şifreler, ırk ve etnik köken, siyasi düşünce, sendika üyeliği, sağlık bilgilerine ilişkin kişisel verilerin etkilendiği,
- İhlalden etkilenen Türkiye’de yerleşik kişi sayısının 184.205 olduğu,
- İhlalden etkilenen ilgili kişi grubunun çalışanlar olduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 04.05.2021 tarih ve 2021/462 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2020/635 - Dap Rotana Dalga ve Vazo Rezidans Toplu Yapı Yöneticiliği

Veri İhlali Bildirimi - Dap Rotana Dalga ve Vazo Rezidans Toplu Yapı Yöneticiliği

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Dap Rotana Dalga ve Vazo Rezidans Toplu Yapı Yöneticiliği tarafından Kurumumuza gönderilen yazıda özetle;

- İhlalin; kat maliklerine ait kişisel verilerin bir çalışan tarafından üçüncü kişiler ile paylaşılması neticesinde gerçekleştiği,
- İhlalin 05.03.2020 tarihinde saat 9:00 ile 17:00 arasında gerçekleştiği ve 13.08.2020 tarihinde bilişim hizmeti alınan şirketten rapor istenilmesi ve gelen rapor üzerine yönetim kurulunun bilgilendirilmesiyle tespit edildiği,
- İhlalden etkilenen kişisel verilerin; kimlik, iletişim, lokasyon ve hukuki işlem veri kategorileri (ad, soyadı, T.C. Kimlik numarası, adres, cep telefonu ve varsa araç plaka bilgileri) olduğu,
- İhlalden etkilenen kişilerin kat malikleri ve sakinlerinden oluştuğu,
- İhlalden etkilenen kişi sayısının 2328, kayıt sayısının 11640 olduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 18.08.2020 tarih ve 2020/635 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - PSL Elektronik San. ve Tic. A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan PSL Elektronik San. ve Tic. A.Ş. tarafından Kurumumuza gönderilen yazıda özetle;

- İhlalin; Şirketin kullanmış olduğu server cihazında çalışan çeşitli yazılımların ve bu yazılımlarda üretilen bilgilerin yer aldığı dosyaların şifrenmesi suretiyle gerçekleştiği,
- İhlalin 20.09.2020 tarihinde saat 01:00’de gerçekleştiği ve mesai başlangıcında sistemin kontrol edilmesi üzerine 21.09.2020 tarihinde saat 08:00’de tespit edildiği,
- İhlalden kimlik, iletişim, özlük, hukuki işlem, müşteri işlem, finans, mesleki deneyim, pazarlama verilerinin etkilendiği,
- İhlalden etkilenen özel nitelikli kişisel verilerin ırk ve etnik köken bilgileri olduğu,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, kullanıcılar ile müşteri ve potansiyel müşteriler olduğu,
- İhlalden etkilenen kişi sayısının bu aşamada tespit edilemediği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 24.09.2020 tarih ve 2020/737 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Rezzan Günday (Şimşek Eczanesi)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Rezzan Günday (Şimşek Eczanesi) tarafından Kurumumuza gönderilen yazıda özetle;

- İhlalin; veri sorumlusunun eski çalışanı tarafından ilaçların tedarikinin başka eczanelerden sağlanması amacıyla, hastalara ait T.C. kimlik numaralarının bir şekilde (cep telefonu ile ekran görüntüsünün alınması, kağıda not edilmesi gibi) elde edilerek, “Medula Sistemi”ne girilmesi için hastaların bilgisi olmaksızın bir başka eczaneye aktarılması ile pandemi döneminde ise elde edilmiş olan T.C. kimlik numaralarının “Devam Reçetesi” uygulaması üzerinden kullanılarak ilaç tedarik edilmesiyle gerçekleştiği,
- İhlalin en az 2019 yılının Ekim ayından bu yana gerçekleştiği ve 11.08.2020 tarihinde bir hastanın ilaçlarına ulaşamaması üzerine eczane içinde durumun araştırılması ve bazı hastaların ifadeleri üzerine tespit edildiği,
- İhlalden etkilenen kişisel verilerin; T.C. kimlik numarası, telefon numarası, hastanın statüsü (emekli, çalışan), kurum adı (Bağkur Genel Müdürlüğü, Sosyal Güvenlik Kurumu, 60/G Sigortalılar) olduğu,
- İhlalden etkilenen özel nitelikli kişisel verilerin; sağlık bilgileri (hastalık bilgileri, hastalık raporları, hastaların kullandığı ilaçlar) olduğu,
- İhlalden etkilenen kişilerin hastalar olduğu,
- İhlalden etkilenen kişi sayısının bilinmediği,
- İhlale konu olay hakkında Cumhuriyet Başsavcılığına suç duyurusunda bulunulduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 18.08.2020 tarih ve 2020/636 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Sezgi Dental Ağız ve Diş Sağlığı Polikliniği

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Sezgi Dental Ağız ve Diş Sağlığı Polikliniği (Sezgi Dental) tarafından Kurumumuza gönderilen yazıda özetle;

- Sezgi Dental eski çalışanı diş hekiminin işten çıkartılması sonrasında poliklinik hastaları ile ilgili verileri yetkisiz olarak elde ettiği ve işten ayrıldığı,
- İşten ayrılan diş hekiminin Sezgi Dental kliniği hastalarına yeni açmış olduğu iş yeri ile ilgili tanıtıcı reklam amaçlı mesaj gönderdiği,
- Klinikte hasta kayıtlarının barındırıldığı bir otomasyon sisteminin kullanıldığı, bu otomasyon sisteme tüm diş hekimlerinin kendilerine özel olarak verilen kullanıcı adı ve şifre ile erişim sağlandığı,
- Söz konusu diş hekiminin çalıştığı dönem içerisinde bu otomasyon sistemine erişim yetkisinin bulunduğu, kendisine işten çıkartılması ile ilgili bildirim yapılmasından sonra hasta verilerini kopyalamış olduğunun tahmin edildiği,
- İhlalin 02.06.2020 tarihinde tespit edildiği,
- İhlalden etkilenen kişisel verilerin, kimlik ve iletişim verileri olduğu,
- İhlalden etkilenen kişi sayısının tahmini 2.500 olduğu, otomasyon sistemine kayıtlı bulunan tüm hastalara sms gitmemesi sebebiyle kişi ve kayıt sayısının tespit edilemediği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 23.06.2020 tarih ve 2020/485 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Sine İtiryat Par. Tem. Ür. Gıd. İnş. Mim. Müh. İth. İhr. ve Tic. AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Sine İtiryat Par. Tem. Ür. Gıd. İnş. Mim. Müh. İth. İhr. ve Tic. AŞ tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- İhlalin; 08.04.2021 tarihinde gerçekleştirilen siber saldırı sonucunda veri sorumlusunun sistem dosyalarına erişiminin engellenmesiyle gerçekleştiği,
- İhlalden; çalışanlar, kullanıcılar ve müşterilerin etkilendiği,
- İhlalden etkilenen kişisel verilerin; kimlik, iletişim, özlük, müşteri işlem, işlem güvenliği ve finans verileri olduğu,
- İhlalden etkilenen kişi sayısının henüz tespit edilemediği,
- İhlal ile ilgili olarak ilgili kişilerin info@madam10.com e-posta adresi ile 0 (850) 840 8503 numaradan bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 13.04.2021 tarih ve 2021/382 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - So CHIC Mağazacılık San. ve Tic. AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan So CHIC Mağazacılık San. ve Tic. AŞ tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- Bilgi Teknoloji ve İletişim Kurumu tarafından 08.02.2021 tarihinde tebliğ edilen yazıda şirketleri ile ilişkili olduğu iddia edilen bazı bilgilerin saldırganlar aracılığıyla internet üzerinden bir forum sitesinde satılmaya çalışıldığı bilgisinin verildiği,
- İhlalin kaynağının henüz tespit edilemediği, ihlalin 31.01.2021 tarihinde başladığının düşünüldüğü ve konuya ilişkin araştırmaların devam ettiği,
- İhlalden 4792 kişinin etkilendiği,
- İhlalden etkilenen kişisel verilerin isim-soyisim, e-posta bilgisi, %1,3 oranında adres bilgisi, %0,63 oranında T.C. kimlik numarası bilgisi, kullanıcı kayıt ve son giriş tarihi bilgisi, sipariş sayısı, sipariş tutarları, kullanıcıların iletildiği onaylara dair verilerin olduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 16.02.2021 tarih ve 2021/132 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - T.C. Özyeğin Üniversitesi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan T.C. Özyeğin Üniversitesi tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- Üniversitenin kurumsal internet sitesi olan www.ozyegin.edu.tr üzerindeki bir form alanından girilen bilgilerin tutulduğu bir tabloya saldırı yapıldığı, olayın oluş şekline bir SQL injection atağı yaşanmış olabileceğinin değerlendirildiği,
- İhlalden, 28.12.2020 Pazartesi günü saat 16.10’da USOM’da görevli operatörün telefon ile bildirim sonucunu haberdar olunduğu,
- Uzman şirket ve danışman vasıtasıyla adli bilişim ve bilgi güvenliği incelemelerinin başlatıldığı,
- Yapılan ilk inceleme neticesinde ihlalden etkilenen veri kategorilerinin www.ozyegin.edu.tr internet sitesindeki form alanından veri giren ilgili kişilere ait ad-soyad, telefon, T.C. kimlik numarası, mezun olunan lise ve doğum tarihi bilgileri olduğunun tespit edildiği,
- İhlalden 1665 kişinin etkilendiği, ilgili kişilerin bir kısmının yabancı uyruklu olduğu uyruk bakımından sayıların kesinleştirilmeye çalışıldığı

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 05.01.2021 tarih ve 2021/18 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlal Bildirimi- Türk Ekonomi Bankası A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Türk Ekonomi Bankası AŞ tarafından Kurumumuza gönderilen 05.03.2020 tarihli yazılarında özetle;

- İhlalin 01.01.2018 ile 28.01.2020 tarihleri arasında gerçekleştiği ve 02.03.2020 tarihinde tespit edildiği,
- İhlalin Banka çalışanlarının kendilerine tanımlanan Kredi Kayıt Bürosu skoru olarak da bilinen Türkiye Bankalar Birliği Risk Merkezi Raporu sorgulama sonuç bilgilerini şahsi telefonları aracılığıyla üçüncü kişilerle paylaşması şeklinde gerçekleştiği,
- İhlalden etkilenen kişisel verilerin, ilgili kişilerin kredibiliteleri hakkındaki bilgiler (Kredi Verilebilir, Kredi Verilemez) olduğu,
- İhlalden etkilenen ilgili kişi sayısının tam olarak tespit edilemediği ancak Banka müşterisi olmayan 2.317 kişinin, Banka müşterisi olan 6.917 kişinin ihlalden etkilenmiş olabileceği,
- İlgili kişilerin veri ihlaliyle ilgili olarak Müşteri Memnuniyeti Departmanı/Çağrı Merkezi (0850 200 0 666), kvkkbasvuru@teb.com.tr e-posta adresinden ve www.teb.com.tr internet adresinden bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 09.03.2020 tarih ve 2020/207 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Turkon Holding A.Ş. ve Grup Şirketleri

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Turkon Holding A.Ş. ve grup şirketleri olan Turkon Konteyner Taşımacılık ve Denizcilik A.Ş., Turkon Demiryolu Taşımacılık A.Ş., Turkon Lojistik A.Ş., Turkon Taşımacılık A.Ş., Anadolu Turizm Yatırımları A.Ş., Kanlıca Denizcilik ve Ticaret A.Ş. ve Kaşif Denizcilik A.Ş. tarafından Kurumumuza gönderilen 13.04.2020 tarihli yazılarda özetle;

- Terminal sunucu üzerindeki bir kullanıcının ortalama saldırısına maruz kalması sonucu, Turkon lokal ağında yer alan sunucu ve yedekleme sistemlerinin şifrelenmesi neticesinde ihlalin gerçekleştiği,
- İhlalin 05.04.2020 tarihinde gerçekleştiği ve 06.04.2020 tarihinde tespit edildiği,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, hukuki işlem, müşteri işlem, finans, pazarlama ile görsel ve işitsel kayıtlar olduğu,
- İhlalden etkilenen tahmini kişi ve kayıt sayısının henüz tespitinin yapılmadığı

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 16.04.2020 tarih ve 2020/290 sayılı Kararı ile söz konusu veri ihlal bildirimlerinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - UiPath SRL

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan UiPath SRL tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- Veri sorumlusunun, kullanıcıların UiPath yazılımını öğrenmelerini sağlayan UiPath Akademisinin(Akademi) idaresi amacıyla, Akademiye katılan kullanıcıların kayıt bilgilerini içeren bir dosya tuttuğu, veri sorumlusu çalışanın söz konusu dosyayı kullanıcıların kaydını tutmak amacıyla bir tedarikçinin yazılım platformuna yüklediği,
- Yetkisiz bir kullanıcının, dosya izin ayarlarında kazara gerçekleştirilen yanlış bir yapılandırma nedeniyle dosyaya eriştiği,
- Veri ihlalinin 01.12.2020 tarihinde, bir üçüncü tarafın veri sorumlusuna etkilenen dosyanın halka açık bir internet sitesinde ulaşılabilir durumda olduğunu bildirmesiyle tespit edildiği,
- İhlalden kişilerin ad ve soyadı, kullanıcı adı, eposta adresi, duruma göre kullanıcının işvereni olan şirketin ismi, kullanıcının ülkesi, veri sorumlusu tarafından verilen UiPath Akademi sertifikasyon düzeyi ve artık şirket tarafından kullanılmamakta olan UID kodu bilgilerinin etkilenmiş olabileceği,
- İhlalden etkilenen kişi grubunun kullanıcılar olduğu,
- İhlalden Türkiye’yi kendi ülkesi olarak belirten 4,692 kişinin etkilendiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 22.12.2020 tarih ve 2020/984 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - UPI Trans Dış Ticaret AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan UPI Trans Dış Ticaret AŞ tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- İhlalin; Şirket sunucularının siber saldırı (fidye yazılımı) sonucu şifrelenmesi ve verilere ulaşılamaması şeklinde gerçekleştiği,
- İhlalin 29.10.2020 tarihinde saat 10:00’da gerçekleştiği ve aynı tarihte tespit edildiği,
- İhlalden etkilenen kişisel verilerin; kimlik, iletişim, özlük, hukuki işlem, müşteri işlem, finans, pazarlama verileri ile görsel ve işitsel kayıtlar olduğu,
- İhlalden etkilenen özel nitelikli kişisel verilerin; felsefi inanç, din, mezhep ve diğer inançlar, sağlık bilgileri ile ceza mahkûmiyeti ve güvenlik tedbirlerine ilişkin veriler olduğu,
- İhlalden çalışanlar, kullanıcılar, müşteriler ve potansiyel müşteriler ile henüz tespit edilemeyen kişilerin etkilendiği,
- İhlalden tahmini 50 kişinin etkilendiği, ancak kişi sayısının tam olarak tespit edilemediği ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 06.11.2020 tarih ve 2020/848 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Ver İhlal Bildirimi - Vatan Bilgisayar Sanayi ve Ticaret AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Vatan Bilgisayar Sanayi ve Ticaret AŞ tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- İhlalin; başka bir kaynaktan elde edildiği değerlendirilen kullanıcı adı (e-posta) ve şifrelerin veri sorumlusunun internet sitesinde geçerli olup olmadığının denemesi sonucu, başarılı olan kullanıcı adı ve şifrelerin bir web sitesinde yayınlanması şeklinde gerçekleştiği,
- Giriş denemelerinin vatanbilgisayar mobil arayüzünde kullanılan bir web servis altındaki api ile programatik olarak denendiği,
- İhlalin 05.10.2020 tarihinde saat 01:30’da gerçekleştiği ve bir güvenlik firmasından gelen uyarı e-maili ile 05.10.2020 tarihinde saat 17:04’te tespit edildiği,
- İhlalden etkilenen kişisel verilerin www.vatanbilgisayar.com üye kullanıcı adı (e-posta adresi) ve bu kullanıcıların www.vatanbilgisayar.com’da yer alan şifreleri olduğu,
- İhlalden 27.143 vatanbilgisayar.com üyesinin etkilendiği,
- İlgili kişilerin veri ihlaliyle ilgili olarak kisiselverim@vatanbilgisayar.com uzantılı e-posta adresinden bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 09.10.2020 tarih ve 2020/789 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - West Gate Toplu Yapı Sitesi Yöneticiliği

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan West Gate Toplu Yapı Sitesi Yöneticiliği tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- İhlalin 25.02.2021 tarihinde veri sorumlusunun bir çalışanın, site yönetiminde kullanılan bir yazılım programında kendisine ait kullanıcı adı ve şifresini yetkisiz üçüncü kişilerle paylaşması sonucu kat maliklerine ve bağımsız bölüm kullanıcılarına ait kişisel verilerin ele geçirilmesi neticesinde gerçekleştiği,
- İhlalden etkilenen kişi grubunun West Gate Toplu Yapı Sitesi Bağımsız Bölüm Kullanıcıları ile Kat Maliklerinin olduğu,
- İhlalden kimlik, iletişim, lokasyon, hukuki işlem, müşteri işlem, fiziksel mekan güvenliği, işlem güvenliği, finans veri kategorilerinin etkilendiği,
- İhlalden 2.220 kişinin etkilendiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 29.03.2021 tarih ve 2021/326 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Yalova Belediyesi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Yalova Belediyesi tarafından Kurumumuza gönderilen yazıda özetle;

- Sunucularında yapılan inceleme sonucunda fidye yazılımıyla dosyaların şifrelendiğinin tespit edildiği, Belediye veri tabanında bulunan vatandaş bilgilerine erişimde kısıt oluştuğu,
- İhlalin 30.08.2020 tarihinde 01:00-09:00 saatleri arasında gerçekleştiği, bazı sunucuların çalışmaması üzerine 30.08.2020 tarihinde saat 09:00’da tespit edildiği,
- Sunucular ve firewall incelendiğinde dışarıya bir veri akışına rastlanmadığı,
- İhlalden çalışanlar, kullanıcılar ve müşterilere ait kimlik, iletişim, lokasyon, müşteri işlem ve finans verilerinin etkilendiği,
- İhlalden etkilenen tahmini kişi sayısının bu aşamada belirlenemediği, araştırmalara devam edildiği,

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 03.09.2020 tarih ve 2020/675 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlal Bildirimi- Yapı ve Kredi Bankası AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Yapı ve Kredi Bankası AŞ tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- Bir çalışanın, kendisine görevi nedeniyle tanımlanan Bankalar Birliği Risk Merkezi istihbarat kayıtları sorgulama yetkisini görevi dışında kullanarak, sorgulamalar yaptığı ve edindiği bu bilgileri üçüncü kişilere aktardığı,
- İhlalin Türkiye Bankalar Birliği'nin veri sorumlusuna gönderdiği 10.02.2021 tarihli yazıya istinaden soruşturma başlatılması sonucunda 05.04.2021 tarihinde tespit edildiği,
- İhlalden tahmini olarak 2484 kişinin etkilendiği,
- İhlalden TC kimlik numarası, ad, soyad, iletişim bilgileri, kredi risk ve teminat durumu, ödeme performans bilgileri, karşılıksız çek ve protestolu senet ödeme bilgilerinin etkilendiği,
- İhlalden etkilenen ilgili kişi gruplarının henüz bilinmediği, tespit çalışmalarının devam ettiği ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 13.04.2021 tarih ve 2021/376 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Yemek Sepeti Elektronik İletişim Perakende Gıda Lojistik AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Yemek Sepeti Elektronik İletişim Perakende Gıda Lojistik A.Ş. tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- 18.03.2021 tarihinde kimliği veri sorumlusunca belirlenemeyen şahıs ya da şahıslarca Yemek Sepetine ait bir web uygulama sunucusuna erişildiği,
- Normal şartlarda yetkisiz bir erişim olduğunda uyarı veren araç üzerinde sorun kaydı olduğu ancak bir aksaklık nedeniyle yetkisiz erişimin o an fark edilemediği,
- 25.03.2021 tarihinde gelen alarmlar incelendiğinde şüpheli bir davranışın tespit edildiği,
- Yemek Sepetine ait bir web uygulama sunucusu üzerinde bir açıklık bulunduğu, bu açıklıktan yararlanılarak, uygulama kurulduğu ve komut çalıştırılmak suretiyle sunucuya erişilebildiği,
- Saldırıyı yapanlar tarafından sunucu üzerinde kullanıcı oluşturularak veri toplanmaya çalışıldığı ve uzaktaki sunuculara trafik gönderildiği,
- İhlalden 21.504.083 kişinin etkilendiği,
- İhlalden etkilenen kişisel verilerin kısmi olarak veri sorumlusunca belirlendiği ve söz konusu verilerin kullanıcı adı, adres, telefon, e-posta, şifre, IP bilgileri olduğunun değerlendirildiği,
- Kredi kartı ya da finansal verilerin etkilenmediğinin belirtildiği, kredi kartı saklama hizmetinin veri sorumlusundan bağımsız Mastercard tarafından sağlandığı,
- İlgili kişilerin ihlal ile ilgili olarak info@yemeksepeti.com e-mail adresi üzerinden bilgi alabileceği, ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 29.03.2021 tarih ve 2021/321 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Hanon Automotive Climate Sys. Manufacturing Industrial and Commercial Co.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Hanon Automotive Climate Sys. Manufacturing Industrial and Commercial Co. tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- 04.10.2020 tarihinde şirketin küresel sunucularının çoğundaki dosyaları şifreleyen bir fidye yazılımı saldırısına uğradığı,
- İhlalden etkilenen kişisel verilerin henüz bilinmediği,
- İhlalden etkilenen kişi ve kayıt sayısının henüz bilinmediği,
- İhlalden etkilenen ilgili kişi gruplarının henüz bilinmediği,
- İhlalin ilgili kişilere yönelik olumsuz sonuç doğurma olasılığının henüz bilinmediği,
- İhlal etkisine yönelik değerlendirme çalışmalarının devam ettiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 27.10.2020 tarih ve 2020/830 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Pierre Fabre Dermokozmetik Ltd. Şti.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Pierre Fabre Dermokozmetik Ltd. Şti tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- İhlalin, veri sorumlusunun Fransa’daki genel merkezine bir siber saldırı sonucu gerçekleştiği ve etkilerinin araştırıldığı,
- İhlalden etkilenen kişi ve kayıt sayısının tespit edilemediği,
- İhlalden çalışanlar, kullanıcılar ile müşteriler ve potansiyel müşterilerin etkilendiği,
- İhlalden kimlik, iletişim, lokasyon, özlük, hukuk, işlem, müşteri işlem, işlem güvenliği, risk yönetimi, finans, mesleki deneyim ve pazarlama ve dernek üyeliği verilerinin etkilendiği,
- İhlal sebebiyle ilgili kişilerin önemli olumsuz etkilere maruz kalma olasılığının henüz bilinmediği ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 05.04.2021 tarih ve 2021/351 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Pierre Fabre İlaç AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Pierre Fabre İlaç AŞ tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- İhlalin, veri sorumlusunun Fransa’daki genel merkezine bir siber saldırı sonucu gerçekleştiği ve etkilerinin araştırıldığı,
- İhlalden etkilenen kişi ve kayıt sayısının tespit edilemediği,
- İhlalden çalışanlar, kullanıcılar ile müşteriler ve potansiyel müşterilerin etkilendiği,
- İhlalden kimlik, iletişim, lokasyon, özlük, hukuk, işlem, müşteri işlem, işlem güvenliği, risk yönetimi, finans, mesleki deneyim ve pazarlama ve dernek üyeliği verilerinin etkilendiği,
- İhlal sebebiyle ilgili kişilerin önemli olumsuz etkilere maruz kalma olasılığının henüz bilinmediği ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 05.04.2021 tarih ve 2021/350 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir. Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Gardrops Elektronik Hizmetler ve Ticaret Anonim Şirketi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Gardrops Elektronik Hizmetler ve Ticaret Anonim Şirketi tarafından Kurumumuza gönderilen 23.09.2019 tarihli yazıda özetle;

- Şirkete 13.09.2019 tarihinde bir e-posta adresinden internet sitesinin hacklendiği iddiasının iletildiği,
- Sistemi hacklediğini iddia eden kişi ile yapılan yazışmalar sonucu 25 kişinin verisinin ihlale uğradığının 17.09.2019 tarihinde Şirket tarafından öğrenildiği,
- İhlalden etkilenen kişisel verilerin kullanıcılara ait ad, soyad, e-posta adresi ve şifrelenmiş (encrypted) kullanıcı hesabı şifreleri olduğu,
- Şirket teknik ekibi tarafından, mevcut güvenlik önlemleri sayesinde iddia sahibinin verilerin tamamını çekemediğinin tespit edildiği,
- Yapılan teknik araştırmalara dayanarak azami 257.000 kullanıcının veri sızıntısından etkilenmiş olabileceği ve nihai tespit çalışmalarının devam ettiği,

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 26.09.2019 tarih ve 2019/286 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - DLSY Adi Ortaklığı (Daelim İnşaat Geliştirme AŞ, Limak İnşaat Sanayi ve Ticaret AŞ, SKEC Anadolu Mühendislik ve İnşaat Ltd. Şti., SK Engineering & Construction Co. Ltd. ve Yapı Merkezi İnşaat ve Sanayi AŞ)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan DLSY Adi Ortaklığı (Daelim İnşaat Geliştirme AŞ, Limak İnşaat Sanayi ve Ticaret AŞ, SKEC Anadolu Mühendislik ve İnşaat Ltd. Şti., SK Engineering & Construction Co. Ltd. ve Yapı Merkezi İnşaat ve Sanayi AŞ) tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- Veri sorumlusuna ait bazı sunucu ve dosyaların saldırganlar tarafından şifrelenerek fidye talebinde bulunulduğu,
- İhlalin 24.04.2021 tarihinde başladığı ve yine aynı tarihte tespit edildiği,
- Saldırıdan etkilenen sunuculardaki kişisel veri kategorilerinin kimlik, iletişim, lokasyon, özlük, hukuki işlem, fiziksel mekan güvenliği, işlem güvenliği, finans, mesleki deneyim, görsel ve işitsel kayıtlar, dernek üyeliği, vakıf üyeliği, sendika üyeliği, sağlık bilgileri, ceza mahkumiyeti ve güvenlik tedbirleri olabileceği, ancak hangi kategorideki kişisel verilerin etkilendiğinin kesin olmadığı,
- İhlalden etkilenen kişi ve kayıtların net bir şekilde tespitinin yapılamamış olduğu ancak ihlalden etkilenen tahmini kişi sayısının 20.000 olduğu,
- İhlalden adi ortaklık çalışanları, adi ortaklık çalışan yakınları ve taşeron çalışanlarının etkilendiğinin düşünüldüğü,
- İhlale ilişkin araştırmaların devam ettiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 27.04.2021 tarih ve 2021/444 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Doğa Sigorta A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Doğa Sigorta AŞ tarafından Kurumumuza gönderilen 06.03.2020 tarihli yazıda özetle;

- İhlalin 28.02.2020 tarihinde gerçekleştiği ve aynı gün tespit edildiği,
- İhlalin, Şirketin web sayfasına ait test sunucusunun hacklenmesi dolayısıyla gerçekleştiği,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, araç plakası, araç ruhsat, elektronik posta ve finans olduğu,
- İhlalden etkilenen tahmini kişi sayısının 300 olduğu,
- İlgili kişilerin veri ihlaliyle ilgili olarak www.dogasigorta.com adresinden bilgi alabilecekleri

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 09.03.2020 tarih ve 2020/206 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Doktor Atadan Egemen KOYUNCU

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Doktor Atadan Egemen KOYUNCU tarafından Kurumumuza gönderilen yazıda özetle;

- Hasta bilgilerinin tutulduğu sistemin 05.07.2020 tarihinde bir siber saldırıya (fidye saldırısı) maruz kaldığı,
- İhlalin 06.07.2020 tarihinde hasta programının silindiğinin fark edilmesi sonucu tespit edildiği,
- İhlalden etkilenen kişi sayısının tahmini 10.000 olduğu, hasta programına girilemediği için tam sayının bilinmediği,
- İhlalden etkilenen kişisel verilerin hastalara ait kimlik bilgileri, e-posta adresleri, telefon numaraları, sağlık ile ilgili detaylı bilgiler, tıbbi geçmişler, muayene bulguları, laboratuvar sonuçları ve cinsel sorunları içeren veriler olduğu,

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 09.07.2020 tarih ve 2020/540 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Veri İhlali Bildirimi - EasyJet Plc

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan EasyJet Plc (EasyJet) tarafından Kurumumuza gönderilen 26.05.2020 tarihli yazıda özetle;

- EasyJet’in üst düzey saldırganlar tarafından gerçekleştirilen ve kişisel verilere erişilmesine yol açan bir bilgi güvenliği sorununa maruz kaldığı,
- İhlalin 17.10.2019 ile 04.03.2020 tarihleri arasında gerçekleştiği,
- EasyJet’in sistemlerine yetkisiz erişimden ilk olarak 22.01.2020 tarihinde haberdar olduğu, 10.03.2020 tarihinde yolcu rezervasyon bilgilerini elde eden özel üretim bir kötü amaçlı yazılımın tespit edildiği,
- 20.05.2020 tarihinde saldırıdan etkilenen kişiler arasında 6.846 tanesinin Türkiye’de mukim olduğunun (müşteriler tarafından rezervasyon yapılırken bildirilen fatura adreslerine istinaden) tespit edildiği,
- İhlalden Türkiye’de mukim 3 kişinin irtibat bilgileri (adı, soyad ve e-posta adresi), uçuş bilgileri (uçak kalkış tarihi, kalkış noktası, varış noktası ve bilet referansı), işlem bilgileri (işlem tutarı ve cinsi) ve ödeme bilgilerinin (bilet alan kişinin tokenlaştırılmamış düz metin halinde kart numarası, son kullanma tarihi ve cvv bilgisi) etkilendiği, 6843 kişinin ise irtibat bilgileri (adı, soyad ve e-posta adresi), uçuş bilgileri (uçak kalkış tarihi, kalkış noktası, varış noktası ve bilet referansı), işlem bilgilerinin (işlem tutarı ve cinsi) etkilendiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 28.05.2020 tarih ve 2020/443 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Exeltis İlaç Sanayi ve Ticaret A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Exeltis İlaç Sanayi ve Ticaret A.Ş. tarafından Kurumumuza gönderilen 14.01.2020 tarihli yazıda özetle;

- İhlalin zararlı yazılımlardan ve fidye yazılımlarından kaynaklı bir siber saldırı olarak şirketin yetkili kullanıcı şifresi ele geçirilerek meydana geldiği,
- İhlalin 11.01.2020 tarihi saat 22.00’da başladığı, 12.01.2020 tarihi saat 03.00’da sona erdiği ve 12.01.2020 tarihi saat 13.05’te tespit edildiği,
- İhlalden etkilenen kişisel verilerin kimlik, iletişim, lokasyon, özlük, hukuki işlem, müşteri işlem, işlem güvenliği, risk yönetimi, finans ve pazarlama bilgileri; ihlalden etkilenen özel nitelikli kişisel verilerin ise sağlık, ceza mahkûmiyeti ve güvenlik tedbirleri bilgileri olduğu,
- İhlalden etkilenen kişilerin çalışanlar, kullanıcılar, müşteriler ve potansiyel müşteriler olduğu,
- İhlalden etkilenen tahmini kişi sayısının yaklaşık 1.000 civarı olduğu ve kesin sayının henüz tespit edilemediği,
- İlgili kişilerin veri ihlaliyle ilgili olarak Bilişim Departmanı yardım masası veya KVKK Komitesi’nden e-posta veya telefon ile bilgi alabilecekleri

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 16.01.2020 tarih ve 2020/46 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Fibabanka AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Fibabanka AŞ tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- Banka personelinin yapmış olduğu Kredi Kayıt Bürosu (KKB) sorguları neticesinde ulaştığı kişisel verileri kendi iletişim yolları (telefon, elektronik haberleşme programı vs.) aracılığı ile üçüncü kişilere 1 Ocak 2019 ve 16 Şubat 2019 tarihleri arasında ilettiği,
- İhlalin Banka çağrı merkezine gelen ihbar nitelikli arama sonrasında Banka Teftiş Kurulu Başkanlığı tarafından yapılan incelemeler sonucunda tespit edildiği,
- İhlalden kimlik ve finans verilerinin etkilendiği,
- İhlalden tahmini olarak 13500 kişinin etkilendiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 04.03.2021 tarih ve 2021/194 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Ficosa International Otomotiv San. ve Tic. AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Ficosa International Otomotiv San. ve Tic. AŞ tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- Veri sorumlusunun sunucularına 16.12.2020 tarihinde fidye saldırısının gerçekleştirildiği ve dosyaların şifrelendiği,
- İhlalin log kayıtlarında bir problem olduğunun fark edilmesiyle tespit edildiği,
- İhlalden etkilenen kişisel verilerin; ad, soyadı, e-posta ve/veya telefon numarası olduğu ancak bilişim incelemesinin devam ettiği,
- İhlalden çalışanların, müşterilerin, tedarikçiler ve hizmet sağlayıcıların etkilendiği
- İhlalden tahmini 1084 kişinin etkilendiği, incelemenin devam ettiği dolayısıyla kişi ve kayıt sayısının tam olarak bilinmediği,

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 29.12.2020 tarih ve 2020/1011 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Ficosa Otomotiv San. ve Tic. AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Ficosa Otomotiv San. ve Tic. AŞ tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- Veri sorumlusunun sunucularına 16.12.2020 tarihinde fidye saldırısının gerçekleştirildiği ve dosyaların şifrelendiği,
- İhlalin log kayıtlarında bir problem olduğunun fark edilmesiyle tespit edildiği,
- İhlalden etkilenen kişisel verilerin; ad, soyadı, e-posta ve/veya telefon numarası olduğu ancak bilişim incelemesinin devam ettiği,
- İhlalden çalışanların, müşterilerin, tedarikçiler ve hizmet sağlayıcıların etkilendiği
- İhlalden tahmini 976 kişinin etkilendiği, incelemenin devam ettiği dolayısıyla kişi ve kayıt sayısının tam olarak bilinmediği,

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 22.12.2020 tarih ve 2020/987 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Fluke Corporation ve Fluke Electronics Corporation

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Fluke Corporation ve Fluke Electronics Corporation tarafından Kurumumuza gönderilen yazıda özetle;

- İhlalin, veri sorumlusunun web servisi yönetici hesabının ele geçirilmesi ve Fluke Connect ortamına erişilmesi ile gerçekleştirildiği,
- Veri ihlalinin gerçekleşme tarihinin belirsiz olduğu, bu hususta araştırmaya devam edildiği, ihlalin 29.06.2020 tarihinde tespit edildiği,
- İhlalden etkilenen kişisel verilerin, e-posta adresleri, telefon numaraları, şirket adları, kişisel ve/veya şirket adresleri, iletişim bilgileri, Fluke Connect el aletlerinden ve Fluke Connect Sensörlerinden elde edilen ölçüm verileri, abonelik bilgileri ve şifrelenmiş parolaların olduğu,
- Veri sorumlusunun kayıtlarına göre ihlalden etkilenen kişi sayısının Türkiye’de yerleşik 4.282 kullanıcı olduğu,
- İlgili kişilerin veri ihlaliyle ilgili olarak connect@fluke.com adresinden bilgi alabilecekleri ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 16.07.2020 tarih ve 2020/555 sayılı Kararı ile söz konusu veri ihlali bildirimiminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Generali Sigorta AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Generali Sigorta AŞ tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- İhlalin, veri sorumlusunun tamamlayıcı sağlık sigortası teklifi alınan internet sayfası üzerinden TC kimlik numaralarının otomatik yazılımlar ve botlar aracılığıyla olağandışı sorgulama yapılması suretiyle gerçekleştiği,
- 21.03.2021 ve 24.03.2021 tarihleri arasında gerçekleşen veri ihlalinin 24.03.2021 tarihinde tespit edildiği,
- İlgili teklif formu sayfasının ihlalin tespitinin ardından veri sorumlusu tarafından kullanıma kapatıldığı,
- İhlalden etkilenen kişisel verilerin ad, soyad, doğum tarihi ve cinsiyet bilgisi olduğu,
- İhlalden 951 kişinin etkilendiği,
- İhlale ilişkin incelemelere veri sorumlusu tarafından devam edildiği

ifade edilmiştir. Konuya ilişkin inceleme devam etmekle birlikte,

Kişisel Verileri Koruma Kurulunun 29.03.2021 tarih ve 2021/323 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Gratis İç ve Dış Tic. A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Gratis İç ve Dış Tic. AŞ tarafından Kurumumuza gönderilen 09.03.2020 tarihli yazıda özetle;

- İhlalin 04.03.2020 ile 06.03.2020 tarihleri arasında gerçekleştiği ve 06.03.2020 tarihinde tespit edildiği,
- 06.03.2020 tarihinde Şirket e-posta adresine kimliği belirsiz bir şahıstan Şirket web sitesi üyelerinin e-posta adresinin/şifrelerinin ele geçirildiğine dair bir elektronik posta geldiği,
- Şirket dışı kaynaklardan elde edilen e-posta adresleri/şifreler ile şirkete ait Gratis.com sitesine birden fazla IP'den giriş denemeleri yapıldığı, her başarısız denemeden sonra bir başka elektronik e-posta/şifre denemesi yapıldığı, bu yolla 2092 site kullanıcısının site hesaplarının şifrelerini doğruladıkları,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim ve müşteri işlem verileri olduğu,
- İhlalden 2092 kişinin etkilendiği,
- İlgili kişilerin veri ihlaliyle ilgili olarak info@gratis.com aracılığıyla ve 0 850 210 69 00 telefon numarası vasıtası ile çağrı merkezinden bilgi alabilecekleri

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 09.03.2020 tarih ve 2020/211 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Penti Giyim Sanayi ve Ticaret Anonim Şirketi ve İştirakleri

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Penti Giyim Sanayi ve Ticaret Anonim Şirketi (Türkiye) ve iştirakleri olan Penti Çorap Sanayi ve Ticaret Anonim Şirketi (Türkiye), SC Penti World SRL (Romanya), Penti World LLC (Kazakistan) ve Penti Giyim Ticaret Anonim Şirketi (Kuzey Kıbrıs Türk Cumhuriyeti) tarafından Kurumumuza gönderilen yazılarda özetle;

- İhlalin; Penti Giyim Sanayi ve Ticaret Anonim Şirketinin sistemlerine yapılan fidye saldırısı neticesinde gerçekleştiği,
- İhlalin 31.07.2020 tarihinde gerçekleştiği ve aynı tarihte tespit edildiği,
- İhlal sonucunda; Penti Giyim Sanayi ve Ticaret Anonim Şirketinin tahmini 650 kullanıcıya ait kimlik ve iletişim verilerinin, Penti Çorap Sanayi ve Ticaret Anonim Şirketinin tahmini 130 kullanıcıya ait kimlik ve iletişim verilerinin, SC Penti World SRL'nin tahmini 45.228 çalışan, müşteri ve potansiyel müşterilerine ait kimlik, iletişim ve müşteri işlem verilerinin, Penti World LLC'nin tahmini 14 çalışanına ait kimlik ve iletişim verilerinin, Penti Giyim Ticaret Anonim Şirketinin tahmini 4 kullanıcıya ait kimlik, iletişim ve müşteri işlem verilerinin etkilendiği,
- İncelemelerin devam ettiği ihlalden etkilenen kişi sayısının henüz tespit edilemediği,
- İhlal hakkında incelemenin Penti Giyim Sanayi ve Ticaret Anonim Şirketi nezdinde devam ettiği,

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 06.08.2020 tarih ve 2020/600-601-602-603-604 sayılı Kararları ile söz konusu veri ihlali bildirimlerinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Mert Grup Sigorta Aracılık Hizmetleri Ltd. Şti.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Mert Grup Sigorta Aracılık Hizmetleri Ltd. Şti. (Mert Grup) tarafından Kurumumuza gönderilen yazıda özetle;

- Mert Grup’un acentesi olduğu Atlas Mutuel Sigorta ile Corpus Sigorta sistemlerine girilerek bazı kişilerin kredi kartlarından 1,5,10,15,25,30,50 TL gibi tutarların çekildiği,
- İhlalin 11.07.2020 tarihinde gerçekleştiği ve 13.07.2020 tarihinde tespit edildiği,
- İhlalden etkilenen kişisel verilerin kimlik, iletişim ve finans verileri olduğu,
- İhlalden etkilenen kişi sayısının 707 olduğu

ifade edilmiştir.

Konuya ilişkin ilgili veri sorumluları hakkında inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 16.07.2020 tarih ve 2020/554 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2021/192 - Oto Rapor Araç Muayene ve Ekspertiz Hizmetleri San. ve Tic. AŞ

Veri İhlal Bildirimi- Oto Rapor Araç Muayene ve Ekspertiz Hizmetleri San. ve Tic. AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Oto Rapor Araç Muayene ve Ekspertiz Hizmetleri San. ve Tic. AŞ tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- 22 Şubat 2021 tarihinde veri sorumlusuna, sistemlerine girildiğine ve bunun karşılığında kripto para olarak fidye istendiğine dair bir e-posta gönderildiği,
- İhlalden etkilenen kişi ve kayıt sayısının henüz bilinmediği,
- İhlalden kimlik, iletişim ve müşteri işlem bilgilerinin etkilendiği,
- İhlalin kaynağının henüz tespit edilemediği ve konu ile ilgili araştırmanın devam ettiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 04.03.2021 tarih ve 2021/192 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlal Bildirimi- Microsoft Corporation

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Microsoft Corporation tarafından Kurumumuza gönderilen 29.01.2020 tarihli yazılarında özetle;

- İhlalin 05.12.2019 ile 31.12.2019 tarihleri arasında gerçekleştiği ve 26.01.2020 tarihinde tespit edildiği,
- İhlalin güvenlik kurallarının yanlış yapılandırılması nedeniyle Microsoft destek hizmetleri temsilcilerinin müşteriler ile gerçekleştirdikleri etkileşimlere ilişkin bilgileri içeren bir veri tabanının internet vasıtasıyla erişilebilir olması dolayısıyla gerçekleştiği,
- İhlalden etkilenen kişisel veri kategorilerinin iletişim, müşteri işlem, işlem güvenliği, finans verileri olduğu,
- İhlalden etkilenen tahmini kişi sayısının Türkiye’den 158 kullanıcı olduğu,
- İlgili kişilerin veri ihlaliyle ilgili olarak <https://msrc-blog.microsoft.com/2020/01/22/access-misconfiguration-for-customer-support-database/> adresinden bilgi alabilecekleri

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 04.02.2020 tarih ve 2020/82 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Halk Sigorta A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Halk Sigorta A.Ş. (Halk Sigorta) tarafından Kurumumuza gönderilen yazıda özetle;

- İhlalin, istifa ederek iş akdi sona erdiren bir çalışanın, iş ilişkisi sona erdikten sonra daha önce sorgu yapmak için yetkili olduğu yazılımdaki trafik ve kasko sigortası dosyalarına yetkisiz bir şekilde erişmesi sonucu meydana geldiği,
- İhlalin 30.01.2020 ve 08.04.2020 tarihleri arasında gerçekleştiği,
- İhlalin 10.04.2020 tarihinde Halk Sigorta tarafından yapılan periyodik kontrol sırasında tespit edildiği,
- İhlalden etkilenen kişi gruplarının, sigortalılar, kaza mağdurları, eksperler, acente çalışanları, sürücüler, servis çalışanları, tedarikçi çalışanları olduğu,
- İhlalden etkilenen kişisel verilerin, sigorta hasar dosyasında bulunan ad, soyad, adres, telefon no, vergi kimlik numarası, T.C. kimlik numarası, plaka, şase no, ruhsat, eski hasar bilgileri ve ehliyet bilgisi olduğu, ihlalden etkilenen özel nitelikli kişisel verilerin ise engellilik bilgisi, sağlık bilgisi ve alkol raporu olduğu,
- İş akdi sona erdirilen kişiye ait kullanıcı bilgisi ile işten ayrılma tarihinden sonra 6933 adet farklı eksper dosyasına erişim gerçekleştirildiği,
- İhlali gerçekleştiren kişi hakkında savcılığa suç duyurusunda bulunulduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 16.06.2020 tarih ve 2020/468 sayılı Kararı ile söz konusu veri ihlali bildirimiminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2020/986 - Otokur Otomotiv İnşaat Turizm Sanayi ve Ticaret A.Ş.

Veri İhlali Bildirimi - Otokur Otomotiv İnşaat Turizm Sanayi ve Ticaret A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz Otokur Otomotiv İnşaat Turizm Sanayi ve Ticaret A.Ş. tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- Veri sorumlusu bünyesinde çalışan satış sonrası hizmetler müdürünün yetkisini kötüye kullanarak verileri raporlar halinde aldığı,
- Müşteri şikayetiyle ihlalin farkına varıldığı ve log kayıt kontrollerine göre ihlalin tespit edildiği,
- İhlalin 16.12.2019 tarihinde başladığı, 19.12.2019 tarihinde sona erdiği ve 18.12.2020 tarihinde tespit edildiği,
- İhlalden etkilenen kişi sayısının 17.092 olduğu,
- İhlalden etkilenen kişisel verilerin kimlik, iletişim, müşteri işlem verileri ve müşteri kartında yer alan notlar olduğu,

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 22.12.2020 tarih ve 2020/986 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Kale Holding A.Ş. ve Grup Şirketleri

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Kale Holding A.Ş. ve grup şirketleri olan Bodur Gayrimenkul Geliştirme A.Ş., Kale Nakliyat Seyahat ve Turizm A.Ş., Kalekim Kimyevi Maddeler Sanayi ve Ticaret A.Ş., Kalemaden Endüstriyel Hammaddeler Sanayi ve Ticaret A.Ş., Kaleseramik Çanakkale Kalebodur Seramik Sanayi A.Ş. tarafından Kurumumuza gönderilen kişisel veri ihlali bildirimlerinde özetle;

- Sunucu üzerindeki bazı veri tabanlarının şifrelenmesi şeklinde meydana gelen kişisel veri ihlalinin 04.11.2020 tarihinde gerçekleştiği,
- İhlalden etkilenen kişisel verilerin henüz tespit edilemediği,
- İhlalden etkilenen kişi ve kayıt sayısının henüz tespit edilemediği,
- İhlalden etkilenen kişi gruplarının henüz bilinmediği,
- İhlal hakkında veri sorumluları tarafından incelemenin devam ettiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 12.11.2020 tarih ve 2020/857-858-859-860-861-862 sayılı Kararları ile söz konusu veri ihlali bildirimlerinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - CM Holding A.Ş. ve Grup Şirketleri

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan CM Holding A.Ş. ve grup şirketleri olan Lotus Teknik Tekstil Sanayi ve Tic. A.Ş., Multipark Ambalaj Sanayi ve Tic. A.Ş., Sapro Temizlik Ürünleri Sanayi ve Tic. A.Ş. ve Tetra Paz. ve Dış Tic. A.Ş. tarafından Kurumumuza gönderilen 25.12.2019 tarihli yazılarında özetle;

- İhlalin 23.12.2019 tarihinde gerçekleştiği ve aynı gün tespit edildiği,
- İhlalin IFS Proud sunucusunun Cryptolocker olarak tabir edilen hack saldırısı ile dosyaların şifrelenmesi şeklinde gerçekleştiği,
- İhlalden etkilenen kişisel veri kategorilerinin henüz tespitinin yapılmadığı,
- İhlalden etkilenen tahmini kişi ve kayıt sayısının henüz tespitinin yapılmadığı

anlaşılmıştır.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 26.12.2019 tarih ve 2019/406-407-408-409-410 sayılı Kararları ile söz konusu veri ihlali bildirimlerinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Karacabay Turizm San. ve Dış Tic. Ltd. Şti.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Karacabay Turizm San. ve Dış Tic. Ltd. Şti. tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- İhlalin; veritabanı ve yedeklerin bulunduğu sunucuların fidye saldırısı neticesinde şifrelenmesi sonucunda gerçekleştiği,
- İhlalin; 06 Nisan 2021 tarihinde veri sorumlusunun otelcilik işletmelerinden olan Hotel Levni'nin otel programına giriş sağlanamaması neticesinde tespit edildiği,
- İhlalden; çalışanlar ve müşterilerin etkilendiği,
- İhlalden etkilenen kişisel verilerin; kimlik ve özlük verileri olduğu,
- İhlalden etkilenen kişi sayısının tespit edilemediği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 13.04.2021 tarih ve 2021/386 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Kariyer.net Elektronik Yayıncılık ve İletişim Hiz. A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Kariyer.net Elektronik Yayıncılık ve İletişim Hiz. AŞ tarafından Kurumumuza gönderilen yazıda özetle;

- İhlalin Kariyer.Net’e tedarikçi olarak hizmet veren bir danışman tarafından 12 Ağustos 2020 tarihinde Kariyer.net’in bir çalışanına, adı geçen sitede üyeliği bulunan 50.000 kişiye ait olduğu iddia edilen bir dosyanın aynı gün internette bir siteye yüklendiği bilgisinin aktarılmasıyla tespit edildiği,
- İhlalin 10.08.2020 tarihinde gerçekleştiği, Kariyer.net tarafından 12.08.2020 tarihinde tespit edildiği,
- İhlalden etkilenen verilerin, “email adresi”, “kullanıcı şifresi”, “isim soyad”, “doğum tarihi”, “telefon numarası”, “profil fotoğrafı” URL link bilgisi, “yaşadığı il”, “yaşadığı ilçe” bilgileri olduğu,
- İhlalden etkilenen kişi sayısının 40.955, kayıt sayısının 53.149 olduğu,
- İlgili kişilerin veri ihlaliyle ilgili olarak adaydestek@kariyer.net adresinden ve 0 216 468 76 00 numarasından bilgi alabilecekleri

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 18.08.2020 tarih ve 2020/634 sayılı Kararı ile söz konusu veri ihlali bildirimiminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2019/384 - Küçükçekmece Belediyesi

Veri İhlali Bildirimi - Küçükçekmece Belediyesi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Küçükçekmece Belediyesi tarafından Kurumumuza gönderilen 13.12.2019 tarihli yazıda özetle;

- İhlalin Küçükçekmece Belediyesi'nin SMS hizmeti aldığı yüklenici firmanın web ara yüzünden kullanıcı adı ve parola ele geçirilerek servis üzerinde kayıtlı olan herkese SMS gönderilmesi şeklinde meydana geldiği,
- İhlalin 12.12.2019 tarihinde 05:42' de gerçekleştiği ve aynı gün saat 06:30' da tespit edildiği,
- İhlalden etkilenen kişisel verilerin iletişim bilgileri olduğu,
- İhlalden etkilenen tahmini kişi sayısının 285.000 olduğu,
- İhlalden etkilenen kişilerin ilçe vatandaşı olduğu,

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 17.12.2019 tarih ve 2019/384 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - T. Garanti Bankası A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan T. Garanti Bankası A.Ş. tarafından Kurumumuza gönderilen 06.12.2019 tarihli yazıda özetle;

- Bir Banka personelinin, 346 adet banka müşterisinin şube no, hesap no, cep telefonu numarası ve bu müşterilerin Banka hesaplarından bir yatırım firması hesabına gönderdikleri yatırım işlemi tutarı bilgilerini, bir yatırım firmasında çalıştığını ve arkadaşı olduğunu iddia ettiği bir kişinin e-posta adresine gönderdiği,
- İhlalin 31.10.2019 tarihinde gerçekleştiği ve 04.12.2019 tarihinde tespit edildiği,
- Banka harici bir adrese gönderilen e-postaların kontrolüne yönelik iç süreçlerin dizayn edildiği süreçte ihlalin tespit edildiği,
- İhlalden 346 müşteriye ait kimlik, iletişim, müşteri işlem, finans verilerinin etkilendiği,

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 12.12.2019 tarih ve 2019/381 sayılı Kararı ile söz konusu veri ihlali bildirimiminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Dođuş Planet Elektronik Ticaret ve Bilişim Hizmetleri A.Ş. (n11.com)

Bilindiđi üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceđi başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Dođuş Planet Elektronik Ticaret ve Bilişim Hizmetleri A.Ş. tarafından Kurumumuza gönderilen 20.12.2019 tarihli yazıda özetle;

- Şirket ile bağlantısı olmayan üçüncü kişiler tarafından 832 adet n11.com üyesine ait e-posta adreslerinin internet ortamında ele geçirildiđi,
- Söz konusu e-posta adresleri kullanılarak şifre deneme yoluyla üyelerin n11.com hesaplarına giriş yapıldığı,
- İhlalden etkilenen kişisel verilerin kimlik, iletişim ve müşteri işlem bilgileri olduđu,
- İhlalin 17.12.2019 tarihinde gerçekleştiđi ve aynı gün tespit edildiđi,
- Konu ile ilgili araştırmaların devam ettiđi,
- İlgili kişilerin veri ihlaliyle ilgili olarak kisiselverilerim@n11.com e-posta adresinden bilgi alabilecekleri

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 26.12.2019 tarih ve 2019/401 sayılı Kararı ile söz konusu veri ihlali bildirimiminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Edenred Kurumsal Çözümler A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Edenred Kurumsal Çözümler A.Ş. tarafından Kurumumuza gönderilen 26.11.2019 tarihli yazıda özetle;

- 21.11.2019 saat 17:00’da Şirket’in dahil olduğu şirketler grubunun (“Edenred Global”) bilişim sistemlerine bir şifreleme virüsü saldırısı (cryptolocker attack, ransomware) gerçekleştirildiği,
- Siber saldırıdan, Türkiye dahil Edenred Global yapısı içinde dünyanın çeşitli ülkelerinde bulunan aktif iş birimlerine ait bilgisayar ve sunucuların etkilendiği,
- Siber saldırının, hem Edenred Türkiye hem de Edenred Global bünyesinde yer alan mevcut çalışanların iş için tahsis edilen bilgisayarlarında bulunan belgelere erişememesi sonucu anlaşıldığı,
- İhlalden etkilenen kişi sayısı, tahmini kayıt sayısı ve kişisel veri kategorilerini belirlemek için incelemelerin devam ettiği,
- İlgili kişilerin, kişisel verilerin korunması ile ilgili her türlü taleplerini ve sorularını yazılı olarak Esentepe Mahallesi Talatpaşa Cad. No:5 Kat:1, 34394, Şişli, İstanbul adresine veya 0947004343100016.edenred@hs02.kep.tr kayıtlı elektronik posta adresine veya bilgi-tr@edenred.com elektronik posta adresine elektronik posta yoluyla iletebileceği,

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 26.11.2019 tarih ve 2019/360 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - EDS Enjeksiyon Dök.San.Tic.AŞ.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan EDS Enjeksiyon Dök.San.Tic.AŞ. tarafından Kurumumuza gönderilen 17.10.2019 tarihli yazıda özetle;

- Şirket sunucularına girilerek dosyaların şifrelendiği ve sistemin kullanım dışı bırakıldığı,
- İhlalin 10.10.2019 tarihinde gerçekleştiği ve bu durumun 11.10.2019 tarihinde tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, kullanıcılar ve müşteriler olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, lokasyon, özlük, müşteri işlem, finans, pazarlama ile görsel ve işitsel kayıt bilgileri olduğu,
- İhlalden etkilenen kişi sayısı ve tahmini kayıt sayısının tam olarak bilinmediği ancak 400 GB boyutunda verinin etkilendiği,

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 18.10.2019 tarih ve 2019/313 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2019/311 - Premierdc Veri Merkezi A.Ş.

Veri İhlali Bildirimi - Premierdc Veri Merkezi A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Premierdc Veri Merkezi A.Ş.tarafından Kurumumuza gönderilen 14.10.2019 tarihli yazıda özetle;

- Bir kısım kişi ya da kişiler tarafından Şirket’in güvenlik duvarı yıkılarak tüm bilgi ve belgelere ulaşıldığının düşünüldüğü,
- Veri ihlalinin kaynağının araştırılmakta olduğu,
- İhlalin 09.10.2019 tarihinde gerçekleştiği ve bu durumun 11.10.2019 tarihinde tespit edildiği,
- İhlalden etkilenen kişisel veri kategorilerinin tespit edilmeye çalışıldığı,
- İhlalden etkilenen kişi sayısı ve tahmini kayıt sayısının henüz tespit edilemediği,
- İhlal ile ilgili tespit çalışmalarının devam ettiği,

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 18.10.2019 tarih ve 2019/311 sayılı Kararı ile söz konusu veri ihlali bildirimiminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Gardrops Elektronik Hizmetler ve Ticaret Anonim Şirketi

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Gardrops Elektronik Hizmetler ve Ticaret Anonim Şirketi tarafından Kurumumuza gönderilen 23.09.2019 tarihli yazıda özetle;

- Şirkete 13.09.2019 tarihinde bir e-posta adresinden internet sitesinin hacklendiği iddiasının iletildiği,
- Sistemi hacklediğini iddia eden kişi ile yapılan yazışmalar sonucu 25 kişinin verisinin ihlale uğradığının 17.09.2019 tarihinde Şirket tarafından öğrenildiği,
- İhlalden etkilenen kişisel verilerin kullanıcılara ait ad, soyad, e-posta adresi ve şifrelenmiş (encrypted) kullanıcı hesabı şifreleri olduğu,
- Şirket teknik ekibi tarafından, mevcut güvenlik önlemleri sayesinde iddia sahibinin verilerin tamamını çekemediğinin tespit edildiği,
- Yapılan teknik araştırmalara dayanarak azami 257.000 kullanıcının veri sızıntısından etkilenmiş olabileceği ve nihai tespit çalışmalarının devam ettiği,

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 26.09.2019 tarih ve 2019/286 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Zynga Game Ireland Limited

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Zynga Game Ireland Limited tarafından Kurumumuza gönderilen 23.09.2019 tarihli yazıda özetle;

- Kullanıcı adı ve şifrelerini içeren oyuncu hesap bilgilerinin hackerlar tarafından yasa dışı olarak erişilebilmiş olabileceğinin tespit edildiği,
- İhlalin 31 Ağustos 2019 tarihinde gerçekleştiği ve bu durumun 2 Eylül 2019 tarihinde tespit edildiği,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim ve lokasyon bilgileri olduğu,
- Etkilenen kişisel verilerin kimlik, iletişim ve konum bilgilerinin olduğu, © İhlalden 34.000 Türk vatandaşının etkilendiği, etkilenen kayıt sayısının bu aşamada bilinmediği,
- İlgili kişilerin www.zynga.com web adresi üzerinden ihlal hakkında bilgi alabileceği,

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 26.09.2019 tarih ve 2019/285 sayılı Kararı ile söz konusu veri ihlali bildirimiminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Furtrans Denizcilik Ticaret ve San. A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Furtrans Denizcilik Ticaret ve San. A.Ş. tarafından Kurumumuza gönderilen 12.09.2019 tarihli yazıda özetle;

- Şirket sistemlerine siber saldırı gerçekleştiği ve bu durumun 10.09.2019 tarihinde tespit edildiği,
- Siber saldırı sonucu Şirketin verilere ulaşımının engellendiği,
- İhlalden etkilenen tahmini kişi sayısının 500 olduğu,
- İhlalden etkilenen ilgili kişi gruplarının; çalışanlar, kullanıcılar, aboneler/üyeler, öğrenciler, müşteriler olduğu
- İhlalden etkilenen kişisel verilerin; kimlik, iletişim, lokasyon, özlük, hukuki işlem, müşteri işlem, fiziksel mekan güvenliği, işlem güvenliği, risk yönetimi, finans, mesleki deneyim, görsel ve işitsel kayıt bilgileri, sağlık bilgileri ve biyometrik veri olduğu,
- Verilerin kopyalanmış olabileceği veya üçüncü kişilere aktarılma ihtimalinin olduğu,

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/281 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Türkiye İş Bankası A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Türkiye İş Bankası A.Ş. tarafından Kurumumuza gönderilen 09.09.2019 tarihli yazıda özetle;

- Bankada yürütülen veri sızıntısı önleme çalışmaları kapsamında bir şube çalışanınun ekinde Risk Merkezi sorgularını içeren e-postaları Banka dışı kullanıcılara iletildiğinin belirlendiği,
- Banka tarafından yapılan ön incelemede kişinin görevini kötüye kullanarak elde ettiği raporları para karşılığı üçüncü taraflara aktardığının tespit edildiği,
- İhlalden etkilenen verilerin kimlik ve finans bilgileri olduğu,
- İlgili kişilerin tespitine yönelik incelemelerin devam ettiği,
- Bankaya ait <https://www.isbank.com.tr/TR/bize-ulasin/Sayfalar/iletisim-formu.aspx> adresinden ilgili kişilerin veri ihlali ile ilgili bilgi alabilecekleri,

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 12.09.2019 tarih ve 2019/268 sayılı Kararı ile söz konusu veri ihlali bildirimiminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - FER Gayrimenkul Geliştirme ve İnş. A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan FER Gayrimenkul Geliştirme ve İnşaat A.Ş. tarafından Kurumumuza gönderilen 09.09.2019 tarihli yazıda özetle;

- 28.08.2019 ile 02.09.2019 tarihleri arasında bir veri ihlali gerçekleştiği,
- İhlalin Şirket kütüklerine girilmesi suretiyle gerçekleştirilen bir siber saldırı olduğu,
- İhlal neticesinde bir takım verilere ilişkin kontrol kaybı yaşandığı,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar ve müşteriler olduğu,
- Müşteri verileri arasında tüzel kişiler ve tüzel kişilerle ilgili kişilere ait kişisel verilerin olduğu,
- İhlalden etkilenen kişisel verilerin kimlik, iletişim ve finans bilgileri olduğu,
- İhlalden etkilenen tahmini kişi sayısının 1100-1200 olduğu,

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 12.09.2019 tarih ve 2019/267 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - DenizBank A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan DenizBank A.Ş. tarafından Kurumumuza gönderilen 31.07.2019 tarihli yazıda özetle;

- DenizBank A.Ş. Teftiş Kurulu Başkanlığı tarafından düzenli gerçekleştirilen kontroller kapsamında, Bankanın Beylerbeyi Şubesinde Müşteri İşlem ve Satış Sorumlusu olarak görev yapan Banka çalışanı tarafından, bireysel nitelikli kredi bilgilerini içeren sorgu ekranlarından, işin gereğinden fazla adette sorgulama yapıldığının tespit edildiği ve gerekli incelemelerin başlatıldığı,
- Görevi gereği sorgulama ekranına erişim yetkisi bulunan söz konusu çalışanın, bu yetkiyi; Bankanın erişim ve bilgi güvenliği politikalarına aykırı şekilde amacı dışında kullandığı,
- Temmuz 2018 - Mayıs 2019 tarihleri arasında gerçekleşen ihlalden Banka müşterisi olan 3.038 kişinin ve Banka müşterisi olmayan 2.851 kişinin etkilendiği bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 31.07.2019 tarih ve 2019/230 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Türk Ekonomi Bankası A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Türk Ekonomi Bankası A.Ş. (TEB) tarafından Kurumumuza gönderilen 08.07.2019 tarihli yazıda özetle;

- Bankanın Uyum ve İç Kontrol Grubu tarafından düzenli gerçekleştirilen iç kontrol faaliyetleri kapsamında, 2 ayrı şubesinde (Alanya ve Gebze Akse Sapağı Şubesi) toplam 3 personel tarafından, Türkiye Bankalar Birliği Risk Merkezince Bankaya sağlanan bireysel nitelikteki kredi bilgilerini içeren Kredi Kayıt Bürosu (KKB) sorgu ekranlarından şüpheli sorgulamaların yapıldığının gözlemlendiği,
- Bankanın Teftiş Kurulu soruşturması sonucunda; Bireysel Müşteri ilişkileri Yöneticisi, Bireysel Müşteri İlişkileri Yönetici Yardımcısı, İşletme Müşteri İlişkileri Yönetici Yardımcısı unvanlarında çalışan ve olaya sebep olan 3 personelin görev ve iş tanımları gereği KKB sorgulama ekranına yetkileri bulunduğu, ancak söz konusu 3 personelin kendilerine tanımlanan KKB sorgulama yetkilerini Bankanın erişim ve bilgi güvenliği politikalarına aykırı şekilde amacı dışında kullandığı,
- 3 personelin söz konusu sorgulamalara konu olan kişilerin T.C. Kimlik Numaralarını şahsi telefonları üzerinden üçüncü kişi/kişilerden temin ettikleri, personelin söz konusu verileri bankanın sistemleri kullanarak aktardığına ilişkin bir bulgu olmadığı ancak şahsi telefonları üzerinden elektronik haberleşme programları kullanarak Banka dışına aktarmış olabileceği,
- 10 Temmuz 2017 ve 26 Haziran 2019 tarihleri arasında gerçekleşen ihlalden tahmini olarak Banka müşterisi olan 17.582 kişinin ve Banka müşterisi olmayan 7.706 kişinin etkilendiği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 17.07.2019 tarih ve 2019/219 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2019/190 - Pizza Restaurantları A.Ş. (Domino's Pizza)

Veri İhlali Bildirimi - Pizza Restaurantları A.Ş. (Domino's Pizza)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12 nci maddesinin (5) numaralı fıkrası "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Pizza Restaurantları A.Ş. (Domino's Pizza) tarafından Kurumumuza intikal ettirilen 26.06.2019 tarihli yazıda özetle;

- Şirkete ait dominos.com.tr internet sitesine giriş ve site üzerinden pizza veya diğer ürün siparişleri için kullanılan, müşterilerin kendileri tarafından belirlenen kullanıcı adı ve şifrenin sızdığına ilişkin şüphe oluştuğu,
- Yapılan detaylı teknik inceleme neticesinde 5225 adet müşteriye ait kullanıcı adı ve şifreye deneme yoluyla (brute-force attack) üçüncü kişiler tarafından hukuka aykırı olarak erişildiği ve internet ortamında paylaşıldığının tespit edildiği,
- İhlalden etkilenen verilerin kimlik, iletişim, internet sitesi girişi için kullanılan kullanıcı adı (e-posta adresi) ve şifresi, hediye pizza ve indirim hakkı olup olmadığı bilgileri olduğu,
- İlgili kişilerin dominoskvk@dominospizza.com.tr e-posta adresinden veri ihlali ile ilgili bilgi alabileceği,

ifadelerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 01.07.2019 tarih ve 2019/190 sayılı Kararı ile söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2019/181 - Metro Grosmarket Bakırk y Alışveriř Hiz.Tic.Ltd.řti.

Veri İhlali Bildirimi - Metro Grosmarket Bakırk y Alışveriř Hiz.Tic.Ltd.řti.

Bilindiđi  zere, 6698 sayılı Kiřisel Verilerin Korunması Kanununun “Veri g venliđine iliřkin y k ml l kler” bařlıklı 12 nci maddesinin (5) numaralı fıkrası “İřlenen kiřisel verilerin kanuni olmayan yollarla bařkaları tarafından elde edilmesi h linde, veri sorumlusu bu durumu en kısa s rede ilgisine ve Kurula bildirir. Kurul, gerekmesi h linde bu durumu, kendi internet sitesinde ya da uygun g receđi bařka bir y ntemle ilan edebilir.” h km n  amirdir.

Veri sorumlusu sıfatını haiz olan Metro Grosmarket Bakırk y Alışveriř Hiz. Tic. Ltd. řti. tarafından Kurumumuza intikal ettirilen 14.06.2019 tarihli yazıda  zetle;

- řirketin bazı mađazalarından 31.05.2019-12.06.2019 tarihleri arasında alışveriř yapan MetroCard sahibi olmayan g nl k kart m řterilerinin e-arřiv faturalarının sehven yanlış alıcı adreslerine (8 farklı e-posta hesabına) g nderildiđi,
- 658 kiřiye ait toplam 806 adet e-arřiv faturasında, m řterilerden řifahi beyan alınmak suretiyle elde edilmiř olan kimlik bilgilerinin (isim, soy isim ve T.C. Kimlik numarası) yer aldıđı,
- İlgili kiřilerden řifahi olarak alınan bu verilerin dođruluđu, kimlik kontrol  herhangi bir y ntemle teyit edilemediđi,
- İlgili kiřilerin iletiřim bilgileri olmadıđından dođrudan bildirim yapılamadıđı

bilgilerine yer verilmiřtir.

Konuya iliřkin incelemeler devam etmekle birlikte, Kiřisel Verileri Koruma Kurulunun 18.06.2019 tarih ve 2019/181 sayılı Kararı ile bu ařamada s z konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiřtir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Vodafone Telekomünikasyon A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Vodafone Telekomünikasyon A.Ş. (Vodafone) tarafından Kurumumuza intikal ettirilen 10.06.2019, 13.06.2019 ve 17.06.2019 tarihli yazılarda özetle;

- Vodafone ile yarı münhasır bayilik ilişkisi bulunan bir bayinin (Lotus Telekom) çalışanı tarafından MERNİS (Merkezi Nüfus ve İdare Sistemi) kullanıcı adı ve şifresinin üçüncü bir şahısla paylaşıldığı ihbarı alındığına,
- İhbar üzerine Şirket tarafından suç duyurusunda bulunulduğuna,
- Bayi çalışanı tarafından, GSM hattı abonesi olmak isteyen kişilerin verdiği kimlik fotoğraflarına ait ekran görüntülerinin kopyalandığına,
- İhlalden etkilenen kişisel verilerin kimlik bilgileri olduğuna,
- Kimlik bilgilerinin bayi çalışanı tarafından yasa dışı bahis oynatan siteler için bazı kişilere satıldığına,
- İhlal ile ilgili inceleme ve araştırmaların tamamlanmasının beklendiğinden ilgili kişilere herhangi bir bildirim yapılmadığına,
- Elde edilen bilgilere göre ihlalden etkilenen kişi sayısının yaklaşık 5-6 bin civarında olduğuna,

yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 18.06.2019 tarih ve 2019/178 sayılı Kararı ile söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2019/169 - Bartu Turizm Yatırımları A.Ş.

Veri İhlali Bildirimi - Bartu Turizm Yatırımları A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Bartu Turizm Yatırımları A.Ş. tarafından Kurumumuza intikal ettirilen 10.06.2019 tarihli yazıda özetle;

- İhlalin 05.06.2019 tarihinde Şirkete gönderilen ve doğrulanmayan tehdit ve şantaj içerikli e-posta mesajı ile öğrenildiği,
- İhlalin bir hacker grubu tarafından Şirket sistemlerine sızılarak gerçekleştirildiği,
- İhlalden etkilenen ilgili kişilerin, şirket yetkilileri, çalışanları ve Şirket ile ilgisi tespit edilemeyen üçüncü kişiler olduğu,
- İhlalden etkilenen tahmini kişi sayısının 52 ve bu kişilerin Şirket çalışanı olduğu,
- Hacker grubu tarafından Şirkete gönderilen e-postada ise 70 binin üzerinde kişiye ait kimlik bilgisinin elde edildiği,
- İhlalden etkilenen kişisel veriler arasında kimlik bilgileri ve iletişim bilgilerinin olduğu,

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 18.06.2019 tarih ve 2019/169 sayılı Kararı ile söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Microsoft Corporation

Yayınlanma Tarihi: 10 Mayıs 2019

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Microsoft Corporation tarafından Kurumumuza gönderilen 08.05.2019 tarihli yazıda özetle;

- Microsoft’un bir hizmet sağlayıcısının bünyesinde çalışan çağrı destek yöneticisine ait kimlik bilgilerinin ele geçirildiği,
- Bu sayede Microsoft ile bağı olmayan kişilerin Microsoft kullanıcılarının e-posta hesaplarındaki bilgilere erişebildiği,
- İlgili yöneticinin Microsoft Politikası’na aykırı olarak, hesap login bilgilerini kendisine bağlı 13 destek temsilcisiyle paylaştığının tespit edildiği,
- İhlalin yöneticiye bağlı bu kişilerden birinin, e-dolandırıcılık saldırısına maruz kalması sonucu olabileceği gibi; doğrudan bu kişilerden birisinin fiili sonucunda gerçekleşmiş olabileceği,
- İhlal tespitinin ardından, hesap login bilgilerinin derhal sonlandırıldığı,
- İhlalden etkilenen Türkiye’de yerleşik kişi sayısının tahmini 1.820 olduğu,
- Bu yetkilendirilmemiş erişim neticesinde 01.01.2019 ve 28.03.2019 tarihleri arasında e-postaların veya eklerin içeriği hariç e-posta adresi, klasör adları, e-postaların konu satırları, iletişim kurulan diğer e-posta adreslerinin adına erişilmiş veya bu bilgilerin görüntülenmiş olabileceği,
- Türkiye’de etkilenen kişilerden sayıca çok az kısmının yukarıda sayılan bilgilere ek olarak, e-posta hesaplarının ekler de dahil içeriklerine yetkisiz kişiler tarafından erişilmiş olabileceği,
- İhlalin e-posta adreslerini içeriyor olması sebebiyle kullanıcıların e-dolandırıcılık (phishing) saldırılarına maruz kalma ihtimallerinin bulunduğu,

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 10.05.2019 tarih ve 2019/130 sayılı Kararı ile söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Hunko Motorlu Araçlar San. Ve Tic. Ltd. Şti.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Hunko Motorlu Araçlar San. Ve Tic. Ltd. Şti. tarafından belirli konularda hizmet aldığı Optimum Otomotiv Satış Sonrası Çözümleri Tic. A.Ş. nezdinde gerçekleşen veri ihlali ile ilişkili olarak Kurumumuza 14.03.2019 tarihinde intikal ettirilen ihlal bildiriminde özetle;

- Veri ihlalinin 22-29 Aralık 2018 tarihlerinde meydana geldiği,
- Yetkisiz web arayüzü kullanıcısı ile sisteme erişildiği, müşterilere ait resim dosyalarının ve kişisel verilerin sızdırıldığı,
- İhlalden etkilenen kişisel verilerin kimlik, iletişim, görsel ve işitsel kayıtlar, araç ruhsatı, trafik poliçesi, kaza tespit tutanağı, alkol raporu, beyan dilekçesi ve özel nitelikli kişisel veri olarak sağlık verileri olduğu,
- İhlalden etkilenen kişi sayısının 697 olduğu,

bilgilerine yer verilmiştir.

Konuya ilişkin incelemeler devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 19.03.2019 tarih ve 2019/74 sayılı Kararı ile bu aşamada söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - ASF Otomotiv A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan ASF Otomotiv A.Ş. tarafından belirli konularda hizmet aldığı Optimum Otomotiv Satış Sonrası Çözümleri Tic. A.Ş. nezdinde gerçekleşen veri ihlali ile ilişkili olarak Kurumumuza 13.03.2019 tarihinde intikal ettirilen ihlal bildiriminde özetle;

- Veri ihlalinin 22-29 Aralık 2018 tarihlerinde meydana geldiği,
- Yetkisiz web arayüzü kullanıcısı ile sisteme erişildiği, müşterilere ait resim dosyalarının ve kişisel verilerin sızdırıldığı,
- İhlalden etkilenen kişisel verilerin kimlik, iletişim, araç ruhsatı, trafik poliçesi, kaza tespit tutanağı, alkol raporu, beyan dilekçesi ve özel nitelikli kişisel veri olarak sağlık bilgileri olduğu bilgilerine yer verilmiştir.

Konuya ilişkin incelemeler devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 19.03.2019 tarih ve 2019/73 sayılı Kararı ile bu aşamada söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Kaya Seyehat Turizm San. Ve Dış. Tic. Ltd. Şti.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Kaya Seyehat Turizm San. Ve Dış. Tic. Ltd. Şti. tarafından belirli konularda hizmet aldığı Optimum Otomotiv Satış Sonrası Çözümleri Tic. A.Ş. nezdinde gerçekleşen veri ihlali ile ilişkili olarak Kurumumuza 13.03.2019 tarihinde intikal ettirilen ihlal bildiriminde özetle;

Veri ihlalinin 22-29 Aralık 2018 tarihlerinde meydana geldiği,

İhlalden etkilenen kişisel verilerin kimlik, iletişim, lokasyon, müşteri işlem, işlem güvenliği, finans, mesleki deneyim, pazarlama, görsel ve işitsel kayıtlar, araç ruhsatı, trafik poliçesi, kaza tespit tutanağı, alkol raporu, beyan dilekçesi ve özel nitelikli kişisel veri olarak sağlık verileri olduğu,

İhlalden etkilenen tahmini kişi sayısının 1000’den fazla ve kayıt sayısının 10000 olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin incelemeler devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 19.03.2019 tarih ve 2019/72 sayılı Kararı ile bu aşamada söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Turmobil Turizm Rent a Car Taşımacılık ve Nakliyat San. Tic. Ltd. Şti.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Turmobil Turizm Rent a Car Taşımacılık ve Nakliyat San. Tic. Ltd. Şti. tarafından belirli konularda hizmet aldığı Optimum Otomotiv Satış Sonrası Çözümleri Tic. A.Ş (Optimum) nezdinde gerçekleşen veri ihlali ile ilişkili olarak Kurumumuza 07.03.2019 tarihinde intikal ettirilen ihlal bildiriminde özetle;

- Veri ihlalinin 22-29 Aralık 2018 tarihlerinde meydana geldiği,
- Yetkisiz web arayüzü kullanıcısı ile sisteme erişildiği ve müşterilere ait resim dosyaları ile kişisel verilerin sızdırıldığı,
- Veri ihlalinden etkilenen kişisel verilerin kimlik, iletişim, araç ruhsatı, trafik poliçesi, kaza tespit tutanağı, alkol raporu, beyan dilekçesi ve özel nitelikli kişisel veri olarak sağlık verileri olduğu, bilgilerine yer verilmiştir.

Konuya ilişkin incelemeler devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 08.03.2019 tarih ve 2019/67 sayılı Kararı ile bu aşamada söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Adnan Özen İnşaat Taah. En. Turz. Tiç. ve San. A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Adnan Özen İnşaat Taah. En. Turz. Tiç. Ve San. A.Ş. unvanlı şirket tarafından Kurumumuza 01.03.2019 tarihinde intikal ettirilen veri ihlal bildiriminde özetle;

- Adnan Özen İnşaat Taah. En. Turz. Tiç. Ve San. A.Ş. hasar onarım destek hizmeti alınan Optimum Otomotiv Satış sonrası Çözümleri Tic. A.Ş. nezaretinde yetkisiz web arayüz kullanımı ile sistemlerine erişerek müşterilere ait resim dosyalarının sızdırıldığı,
- Söz konusu verilerin kimlik, iletişim, araç ruhsatı, trafik poliçesi, kaza tespit tutanağı, alkol raporu ve beyan dilekçesinin olduğu,
- Veri ihlalinin 22-29 Aralık 2018 tarihlerinde meydana geldiği,
- Veri ihlalden etkilenen 750 kişinin olduğu ve 5700 kişinin de kullanılan mevcut kayıt sisteminde bulunduğu

bilgilerine yer verilmiştir.

Konuya ilişkin incelemeler devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 05.03.2019 tarih ve 2019/56 sayılı Kararı ile bu aşamada söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - ING Bank A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan ING Bank A.Ş (ING Bank) tarafından Kurumumuza gönderilen 21.01.2019 tarihli yazıda özetle;

- Türkiye Bankalar Birliği (TBB) tarafından Risk Merkezi nezdinde bilgi güvenliğine yönelik yapılan çalışmalarda, bir ING Bank çalışanının yapmış olduğu sorguların şüpheli olduğunun tespit edildiği ve bu işlemlerin olası bir veri sızıntısına yol açıp açmadığının belirlenmesi amacıyla ilgili Banka nezdinde denetim ekiplerince soruşturma yapılması gerektiğinin 19.10.2018 tarihinde ING Bank A.Ş. Genel Müdürlüğüne tebliğ edildiği,
- Bu doğrultuda ING Bank Teftiş Kurulu tarafından veri ihlaline sebep olan şahsa tahsis edilen Banka cihazlarına el konularak mevcut ve silinen e-postaları ile ilgili cihazlar üzerinden gerçekleştirdiği her tür işleme yönelik inceleme/soruşturma çalışması başlatıldığı,
- Soruşturma safhasında veri ihlaline sebep olan şahsın şüpheli beyanları ve cihazlarında yapılan incelemeler kapsamında oluşan ön bulgularda 5411 sayılı Bankacılık Kanununun Müşteri Sırrının ifşasına yönelik hükümleri çerçevesinde veri sızıntısı teşkil edebilecek unsurlar bulunduğuna yönelik kuvvetli emareler tespit edildiği,
- Veri sızıntısına neden olan şahsın ING Bank A.Ş.’nin uygulaması olan Finsoft sisteminde üzerinde tanımlı yetkileri uyarınca Ticari Nitelikli Kredi Bildirimi ve Paylaşımı (KRM) sorgusu yapamadığı halde, yetkilendirme sistemini devre dışı bırakacak bir yöntem ile yetki aşımı yaparak TBB Risk Merkezi web sitesine Banka kullanıcı olarak doğrudan erişim sağlayabildiği,
- Bu kapsamda toplanan ve incelenebilen Banka sistem logları, tanık beyanları ve sair deliller ışığında yapılan değerlendirmeler sonucu veri sızıntısına sebep olan şahsın dışında Banka bünyesinde yapılan geniş kapsamlı incelemelerde bu eyleme iştirak eden veya benzer şekilde hareket eden başka bir personelin bulunduğuna yönelik şüpheli başka bir durum olmadığı sonucuna ulaşıldığı,

- Veri sızıntısına sebep olan şahsın 2018 yılı içinde birçok kez Türkiye Bankalar Birliği Risk Merkezi sistemleri üzerinden usulsüz şekilde, çoğunluğu ING Bank müşterisi olmayan bir kısım şirketlere ait dışarıdan temin ettiği düşünülen TC kimlik numarası (TCKN) ve vergi kimlik numarası (VKN) bilgileriyle sorgular yaptığı ve söz konusu sorgular sonucu oluşan verilerin elektronik haberleşme yollarıyla Banka dışına çıkarttığı,
- ING Bank tarafından gerçekleştirilen inceleme, soruşturma çalışmaları ve yapılan değerlendirmeler neticesinde şu ana kadar ulaşılan bilgiler ışığında şirketlere ait sorgu yapılmış olmasına rağmen gerçek kişi tacir (şahıs firması) bilgilerinin de sorgularda yer aldığı tespit edildiği,
- Bilgilerine ulaşılan gerçek kişi tacirlerin ve tüzel kişi tacirlerin büyük çoğunluğunun banka müşterisi olmadığından dolayı söz konusu TCKN ve VKN verilerinin dışarıdan temin edilmiş olduğu sonucuna varıldığı,
- ING Bank A.Ş. müşterisi olan az sayıda şirketin VKN'lerinin de dışarıdan gelen listelerden alındığının tahmin edildiği,
- Şahsın bireysel kredibilite bilgisine bakabilen bireysel nitelikli kredi kayıtlarına değil, gerçek kişi tacir ve tüzel kişi tacirlere sorgu yapabilen KRM kayıtlarına ulaştığı,
- KRM sorgulama özet raporunda (KRM + çek rapor sorgusunun seçilmesi durumunda), sorgu yapılan firmaya ilişkin olarak; Bankalar nezdindeki kredi limiti, risk ve teminatlarına ilişkin rakamsal bilgileri, firmanın kuruluş tarihi, çalışan sayısı, geçmiş döneme ilişkin ciro bilgisi, telefon ve adresi, firma sahibinin ortaklarının isimleri, ortaklık payları ve ortakların TC kimlik numaraları, ihale yasağına ilişkin notlar, firma tarafından ibraz edilen çeklere ilişkin muhtelif bilgiler (ödenen çek adedi ve tutarı, arkası yazılan çek adedi ve tutarı, son 1 ay, 3 ay ve 12 ay içinde ödenen / arkası yazılan çek adet ve tutarı, çek hesabının bulunduğu bankaların isimleri), firma sahibi ve ortaklarının firma ile ilişki durumu (kefalet/ortaklık/yöneticilik v.s.) ve firma kredi skorları bilgilerine ulaşılabildiği,
- 1.172 adet gerçek kişi ticari işletmesinin KRM raporları ile adres ve telefon verilerinin, ilave olarak KRM raporlarında yer alan tüzel kişilikleri oluşturan gerçek kişilere ilişkin bilgiler kontrol edildiğinde toplam 19.055 adet gerçek kişinin TCKN ve isim bilgilerinin banka dışına aktarıldığının anlaşıldığı,
- İNG Bank A.Ş tarafından kontrolü mümkün alanlara yönelik olarak denetim, tespit ve farkındalık artırıcı unsurların değerlendirme altına alınarak, yetki denetimini devre dışında bırakmak için kullanılan yöntemin engellendiği,

- Eski personelin hukuka aykırı edimleri dâhilinde veri güvenliği ihlali gerekleştikine dair bu durumdan etkilenen gerek kiři ticari iřletmelere mevzuat geređi yapılacak bildirimlerin usulü ve ieriđine iliřkin olarak alıřmanın TBB Risk Merkezi ile koordineli řekilde bařlatıldıđı

bilgilerine yer verilmiřtir.

Bu kapsamda, Kiřisel Verileri Koruma Kurulunun 01.03.2019 tarih ve 2019/43 sayılı Kararı ile söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiřtir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Borlease Otomotiv A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Borlease Otomotiv A.Ş. (Borlease) unvanlı şirket tarafından Kurumumuza gönderilen 18.02.2019 tarihli yazıda özetle;

Borlease Otomotiv A.Ş. ile Optimum Otomotiv Satış Sonrası Çözümleri Tic. A.Ş. (OPTİMUM) arasında iş ilişkisi olduğu,

OPTİMUM nezdinde bir veri ihlali gerçekleştiği,

Veri ihlalinden etkilenen tahmini kişi sayısının 4.000 olduğu,

Veri ihlali sonuçlarının henüz net olarak ortaya çıkmadığı

bilgilerine yer verilmiştir.

Konuya ilişkin incelemeler devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 25.02.2019 tarih ve 2019/35 sayılı Kararı ile bu aşamada söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Garanti Filo Yönetim Hizmetleri A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Garanti Filo Yönetim Hizmetleri A.Ş. (Garanti Filo) unvanlı şirket tarafından Kurumumuza gönderilen 20.02.2019 tarihli yazıda özetle;

- Garanti Filo'nun sürdürmekte olduğu ticari faaliyet kapsamında, müşterilerine kiralamış olduğu araçların kazaya karışması halinde hasar onarımlarının ve buna ilişkin ihtiyaçlarının (çekici, ikame araç, servis yönlendirmesi gibi) karşılanması ve bahse konu hizmetlerin daha etkin sürdürülmesi amacı ile Optimum Otomotiv Satış sonrası Çözümleri Tic. A.Ş.'den (OPTİMUM) destek aldığı,
- OPTİMUM tarafından Garanti Filo'ya, bilgisayar sistemlerine yapılan bir siber saldırı sonucunda sistemlerinde kayıtlı bir kısım verilerin yetkisiz kişilerin eline geçmiş olabileceğinin aktarıldığı,
- Kiraya verilen araçlara ait plaka bilgileri ve hizmet koşullarına ilişkin bilgiler ile kiracılara ait isim ve unvan bilgilerinin OPTİMUM ile paylaşıldığı,
- Gerçek kişi müşterilerinin isim ve soy isim, tüzel kişi müşterilerinin ise unvan bilgisinin OPTİMUM ile paylaşıldığı,
- Garanti Filo'dan OPTİMUM'a doğrudan aktarılan yaklaşık 90 gerçek kişi müşteriye ait kişisel verinin (isim, soy isim) yetkisiz kişilerin eline geçtiğinin değerlendirildiği,
- Garanti Filo haricinde; OPTİMUM'un iş birliği yaptığı, çalıştığı diğer şirket/kuruluşlar vasıtası ile de OPTİMUM'un yine Garanti Filo müşterisi olan gerçek kişilere ait kişisel verileri topladığı ve bu kişisel verilerin (kimlik, ehliyet, kaza tutanağı, kazaya ilişkin beyan evrakı, alkol raporu, adres ve iletişim bilgisi) yetkisiz kişilerin eline geçmiş olabileceğinin değerlendirildiği

bilgilerine yer verilmiştir.

Konuya ilişkin incelemeler devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 25.02.2019 tarih ve 2019/32 sayılı Kararı ile bu aşamada söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Derindere Turizm Otomotiv San. ve Tic. A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Derindere Turizm Otomotiv San. ve Tic. A.Ş. (DRD) unvanlı şirket tarafından Kurumumuza gönderilen 18.02.2019 tarihli yazıda özetle;

- Derindere Turizm Otomotiv San. ve Tic. A.Ş.’nin müşterilerine kiralık olarak kullandırdığı araçlar ve süreçler ile ilgili Optimum Otomotiv Satış Sonrası Çözümleri Tic. A.Ş.’den (OPTİMUM) hasar yönetim sistemi desteği, yedek parça tedarik sistem hizmeti ve sistem entegrasyon hizmeti aldığı,
- DRD çalışanları, DRD müşteri ve çalışanları, araç kullanıcıları, servis tedarikçi ve çalışanları, sigorta hizmeti sağlayan sigorta şirketleri ve çalışanları, araçların karşılaştığı kazalarda karşı taraf sürücüleri ve diğer bütün ilgili kişiler hakkındaki kişisel verileri DRD adına işletmekte olan OPTİMUM sunucularına yetkisiz erişimin gerçekleştiği,
- Yetkisiz erişim sonrasında hangi kişisel verilerin nasıl etkilendiğine ilişkin DRD’ye henüz bilgi verilmediği

bilgilerine yer verilmiştir.

Konuya ilişkin incelemeler devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 25.02.2019 tarih ve 2019/30 sayılı Kararı ile bu aşamada söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2019/29 - Clickbus Seyahat Hizmetleri A.Ş. (Nereden Nereye)

Veri İhlali Bildirimi - Clickbus Seyahat Hizmetleri A.Ş. (Nereden Nereye)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Clickbus Seyahat Hizmetleri A.Ş. (“ClickBus”) unvanlı şirket tarafından Kurumumuza gönderilen 07.02.2019 tarihli yazıda özetle;

- Ekim ve Kasım 2018 tarihlerinde ClickBus sunucularında bazı olağan dışı faaliyetler gerçekleştiği,
- Yapılan incelemede, 25 Eylül 2018’den 25 Kasım 2018’e kadar geçen dönemde ClickBus’ı kullanan müşterilerinin bilgilerinin yer aldığı bilgi sistemlerine izinsiz erişim sağladığı yönünde kanıtlar tespit edildiği,
- Veri ihlalden 67.519 kişinin etkilenmiş olabileceği,
- Veri ihlaline konu olan veriler içerisinde; Ödeme Anahtarı, Yolculuk Numarası, Sepet Numarası, Sipariş Numarası, Toplam Tutar, Seyahat Türü, Her Yolcunun Kimlik Bilgileri (Cinsiyet, Ad, TCKN, Doğum tarihi, Kalkış/varış yer ve saati, Yolcu başına ücret, Referans numarası ve Yolcu türü), İletişim Bilgileri (Cep telefonu ülke kodu, Cep telefonu numarası, Sabit hat ülke kodu, Sabit hat numarası, Sabit hat uzantısı/dahilisi, E-posta adresi, Sms gönderi izni, Ticari elektronik ileti izni), Ödeme Bilgileri (Kart üzerinde yazan isim, Kart numarası, Kartın son kullanma tarihindeki ay/yıl, Kartın güvenlik kodu, Taksit bilgisi, İndirim kodu, Seyahat sigortası alınıp alınmadığına ilişkin bilgi, Site kullanım koşullarını kabul bilgisi), Segmentler, Ödeme Seçenekleri, Hata Sebebi, Oturum Kimliği (Session ID), Oturum simgesi (Session token) gibi kişisel verilerin olduğu,
- ClickBus tarafından herhangi bir kişisel verinin kötüye kullanıldığına dair bir kanıt rastlanmadığı

bilgilerine yer verilmiştir.

Konuya ilişkin incelemeler devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 14.02.2019 tarih ve 2019/29 sayılı Kararı ile bu aşamada söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2019/28 - Enterprise ("Yes Oto")

Veri İhlali Bildirimi - Enterprise ("Yes Oto")

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12 nci maddesinin (5) numaralı fıkrası "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Yes Oto Kiralama ve Turizm Yatırımları A.Ş. (Enterprise - Yes Oto) unvanlı şirket tarafından Kurumumuza gönderilen 31.01.2019 tarihli yazıda özetle;

- Enterprise (Yes Oto) ile Optimum Otomotiv Satış sonrası Çözümleri Tic. A.Ş. (OPTİMUM) arasında iş ilişkisinin bulunduğu,
- OPTİMUM'un siber saldırıya uğradığı,
- Müşteri ve evrak bilgilerinin yetkisiz kişiler tarafından alındığı,
- Siber saldırı neticesinde Enterprise (Yes Oto) şirketine ait herhangi bir verinin alınıp alınmadığına dair OPTİMUM tarafından net bir ifade kullanılmadığı

bilgilerine yer verilmiştir.

Konuya ilişkin incelemeler devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 14.02.2019 tarih ve 2019/28 sayılı Kararı ile bu aşamada söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Arkas Otomotiv Servis ve Ticaret A.Ş. ("Arkas Otomotiv")

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12 nci maddesinin (5) numaralı fıkrası "İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Arkas Otomotiv Servis ve Ticaret A.Ş. ("Arkas Otomotiv") unvanlı şirket tarafından Kurumumuza gönderilen 06.02.2019 tarihli yazıda özetle;

- Arkas Otomotiv ile Optimum Otomotiv Satış sonrası Çözümleri Tic. A.Ş. (OPTİMUM) arasında iş ilişkisinin bulunduğu,
- OPTİMUM sunucularına yetkisiz şifre girişi ile siber saldırı yapıldığı,
- Siber saldırı neticesinde veri kopyalama yapıp yapılmadığı, yapıldı ise hangi verilerin kopyalandığına ilişkin OPTİMUM tarafından veri sorumlusu ile bilgi paylaşılmadığı ve halihazırda belirgin olmadığı,

bilgilerine yer verilmiştir.

Konuya ilişkin incelemeler devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 14.02.2019 tarih ve 2019/27 sayılı Kararı ile bu aşamada söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Holiday Inn İstanbul - Şişli

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Şişli Turizm Yatırımları İnşaat San. ve Tic. A.Ş. (Holiday Inn İstanbul - Şişli) unvanlı şirket tarafından Kurumumuza gönderilen 05.02.2019 tarihli yazıda özetle;

- Şişli Turizm Yatırımları İnşaat San. ve Tic. A.Ş. tarafından işletilen ve 19 Mayıs Mahallesi, Halaskargazi Cd. No:206 34360 Şişli/İstanbul adresinde mukim otelin (Holiday Inn İstanbul - Şişli) 1 Ocak 2019 tarihinde siber saldırıya maruz kaldığı,
- Siber saldırı sonrasında ilgili yedek verilerin saldırıyı yapan kişiler tarafından silindiği,
- Siber saldırıya ilişkin şirket teknik ekibi tarafından detaylı bir rapor çalışmasına başlandığı

bilgilerine yer verilmiştir.

Konuya ilişkin incelemeler devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 06.02.2019 tarih ve 2019/20 sayılı Kararı ile bu aşamada söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

2019/17 - Hedef Araç Kiralama ve Servis A.Ş. (HedefFilo)

Veri İhlali Bildirimi - Hedef Araç Kiralama ve Servis A.Ş. (HedefFilo)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Veri sorumlusu sıfatını haiz olan Hedef Araç Kiralama ve Servis A.Ş. (HedefFilo) unvanlı şirket tarafından Kurumumuza gönderilen 25.01.2019 tarihli yazıda özetle;

- Hedef Araç Kiralama ve Servis A.Ş. ile Optimum Otomotiv Satış sonrası Çözümleri Tic. A.Ş. (OPTİMUM) arasında iş ilişkisinin bulunduğu,
- OPTİMUM sunucularına yetkisiz şifre ile siber saldırı yapıldığı,
- Siber saldırının HedefFilo tüzel kişi müşterilerinin gerçek kişi çalışanlarını kapsayıp kapsamadığının henüz belirlenmemiş olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin incelemeler devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 06.02.2019 tarih ve 2019/17 sayılı Kararı ile bu aşamada söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Optimum Otomotiv Satış Sonrası Çözümleri Tic. A.Ş. (OPTİMUM)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

OPTİMUM OTOMOTİV SATIŞ SONRASI ÇÖZÜMLERİ TİC. A.Ş. (OPTİMUM) unvanlı şirket tarafından Kurumumuza gönderilen 23.01.2019 tarihli yazıda;

- Aralık 2018 tarihinde sunucu (server) sistemlerine yetkisiz şifre girişi ile yapılan siber saldırının bilgi işlem uzmanları tarafından tespit edildiği,
- Gerçekleştirilen siber saldırıya ilişkin hangi kişisel verilerin ele geçirildiği ve kimlere ait olduğu hakkında şirket teknik ekibi tarafından detaylı bir rapor çalışmasına başlandığı ancak konunun teknik boyutu nedeniyle çalışmanın henüz sonuçlanmadığı,
- Siber saldırının hangi müşterileri ve veri gruplarını etkilediğinin kesin olarak belirlenemediği,
- Siber saldırıdan kendi çalışanlarının verilerinin de etkilenmiş olabileceği

bilgilerine yer verilmiştir.

Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/16 sayılı Kararı ile söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - TEB Arval Araç Filo Kiralama A.Ş.(TEB ARVAL)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

TEB ARVAL ARAÇ FİLO KİRALAMA A.Ş. (TEB ARVAL) unvanlı şirket tarafından Kurumumuza gönderilen 21.01.2019 tarihli yazıda;

- TEB ARVAL şirketinin müşterilerine kiraladığı araçların hasar ve kaza süreçlerini yönetmek amacıyla Optimum Otomotiv Satış Sonrası Çözümleri Tic. A.Ş.’den (“OPTİMUM”) taraflar arasında 13 Eylül 2013 tarihinde imzalanan sözleşme kapsamında dış kaynak destek hizmeti aldığı,
- TEB ARVAL şirketinin OPTİMUM şirketine ait Optimum Çözüm uygulamasını kendi operasyonlarında yürütmede kullandığı,
- Optimum Çözüm uygulamasının temel olarak hasar veya kaza durumlarında onarım ve ödeme süreçlerinin yürütülmesi ve takibi amacıyla kullanıldığı,
- Optimum Çözüm uygulamasının müşteri, sürücü, tedarikçi ve üçüncü kişi bilgilerini içerebildiği,
- Optimum Çözüm uygulamasının yazılım, geliştirme, barındırma hizmetleri ve işletilmesinin bizzat OPTİMUM şirketi tarafından sağlandığı,
- 11.01.2019 tarihinde, bilinmeyen kişiler tarafından TEB ARVAL kurumsal internet sitesinde yer alan müşteri iletişim formu kullanılarak; Optimum Çözüm uygulamasına yetkisiz şekilde erişildiği ve şirketlerine ait verilerin ele geçirildiği mesajı iletildiği, bu mesajın alınmasını müteakip konunun veri güvenliği ve diğer ilgili birimler tarafından incelenmeye başlandığı,
- Optimum Çözüm uygulamasının kullanılmaya başlandığı 13 Eylül 2013 tarihinden itibaren TEB ARVAL’den Optimum Çözüm uygulamasını kullanarak hasar ve kaza yönetimi hizmeti almış olan müşteriler, sürücüler, tedarikçiler ve TEB ARVAL’e ait araçların dahil olduğu kazaya karışmış olan üçüncü şahısların söz konusu veri sızıntısından etkilenmiş olabileceğinin değerlendirildiği,
- OPTİMUM şirketinden alınan hizmetin kapsamı gereği, veri sızıntısına konu kişisel verilerin temel olarak; ehliyet, nüfus cüzdanı, pasaport, kaza tespit tutanağı, kaza beyanı, araç ruhsatı,

polis/jandarma kaza tutanakları, trafik sigortası ve diđer ilgili sigorta poliçeleri, kazalı araçların ve olay yerini fotoğrafları, varsa sađlık raporu, sigorta eksperleri raporları, hasar onarım ve/veya yedek parça faturaları, hasar veya kaza ile ilgili varsa diđer belgeler ile sürücülerin e-posta adresleri olduğunun deđerlendirildiđi,

bilgilerine yer verilmiştir.

Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/15 sayılı Kararı ile söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - ALD Automotive Turizm Ticaret A.Ş. (ALD AUTOMOTIVE)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

ALD AUTOMOTIVE TURİZM TİCARET A.Ş. (ALD AUTOMOTIVE) unvanlı şirket tarafından Kurumumuza gönderilen 22.01.2019 tarihli yazıda;

- Veri sorumlusu sıfatını haiz olan ALD AUTOMOTIVE’in müşterilerine kiralık olarak kullandığı araçlar ve süreçler ile ilgili Optimum Otomotiv Satış sonrası Çözümleri Tic. A.Ş. (OPTİMUM) şirketinden Hasar Yönetim Sistem Desteği, Yedek Parça Tedarik Sistem Hizmeti, Anlaşmalı Servis Yönetim Sistem Desteği, Hasar Uzmanı Outsource Hizmeti, Mekanik Bakım Onarım Sistem Hizmeti, Sistem Entegrasyonu, İkame Araç Modülü, Servis Network Yönetimi hizmetlerini aldığı,
- OPTİMUM tarafından yönetilen sistemde veri sorumlusu ve çalışanları, veri sorumlusu müşterileri ve çalışanları, veri sorumlusu araç kullanıcıları, veri sorumlusu servis tedarikçileri ve çalışanları, veri sorumlusu sigorta hizmetlerini gören sigorta şirketleri ve çalışanları, veri sorumlusunun araçlarının karıştığı kazalarda karşı taraf sürücülerini ve diğer bütün ilgili kişiler hakkındaki kişisel verilerin işlendiği,
- OPTİMUM şirketinin web sitesine yasa dışı yollarla (siber saldırı) girilmiş olduğu ve bu vesile ile sunucu (server) sistemine ulaşıldığına ilişkin OPTİMUM tarafından ALD AUTOMOTIVE’e detay verilmeden 14.01.2019 tarihinde telefon ile 15.01.2019 tarihinde ise e-posta ortamında bilgi verildiği,
- Siber saldırı neticesinde birçok kişi, şirket, kurum kuruluşa ait kişisel verilerin kopyalanmış olabileceği,
- Siber saldırı sonucunda veri kopyalama yapıp yapılmadığı, yapıldı ise hangi verilerin kopyalandığına ilişkin ALD AUTOMOTIVE ile bilgi paylaşılmadığı ve halihazırda belirgin olmadığı,
- Siber saldırı ile ele geçirildiği belirtilen veriler ile ilgili kesin bir durumun olmadığı,

- Veri ihlali sebebiyle ele geçirilen veri olup olmadığı, varsa bu verilerin hangi firmanın müşterisi olduğu veya kimlerin verilerinin ele geçirildiğinin tespit edilmeye çalışıldığı

bilgilerine yer verilmiştir.

Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/14 sayılı Kararı ile söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - ANIMOTO Inc. (Animoto)

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

ANIMOTO Inc. (Animoto) unvanlı şirket adına Kurumumuza gönderilen 15.01.2019 tarihli yazıda;

- Animoto’nun 10 Temmuz 2018 tarihinde sunucularında alışılmışın dışında ağ trafiği farketmediği,
- 6 Ağustos 2018 tarihinde Animoto’nun veri ihlali yaşanmış olabileceği ihtimalini tespit ettiği,
- Veri ihlalden dünya çapında 22 milyon kişinin etkilenmiş olabileceği,
- Türkiye’de veya başka bir şekilde coğrafi olarak Türkiye içinde konumlandırılmış yaklaşık 90.000 kişinin veri ihlalden etkilenmiş olabileceği,
- Animoto’nun, Türkiye’de tam fatura adresi bilgisine sahip olduğu yaklaşık 1.500 abonesinin bulunduğu,
- Veri ihlalden etkilenmiş olabilecek verilerin müşterinin adı soyadı, kullanıcı adı (e-posta adresi), özetlenmiş (hashed) ve tuzlanmış (salted) şifreler, yüksek seviye coğrafi konum bilgisi (şehir ve ülkeye denk gelecek şekilde), cinsiyet ve doğum tarihi olduğu,
- Saldırganların şifre tuzuna (salt) erişmiş olabileceği,
- Türkiye’de yerleşik Animoto kullanıcılarının kişisel verilerinin ele geçirildiğine ilişkin kesin bir tespiti yapılmadığı,
- Yetkisiz veri sızıntısını gösteren kesin bir delil olmadığı,

bilgilerine yer verilmiştir.

Yapılan değerlendirmeler neticesinde, Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/13 sayılı Kararı ile ANIMOTO Inc. nezdinde gerçekleşen söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Marriott International, Inc.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

ABD merkezli otel zinciri olan Marriott International, Inc. (Şirket) unvanlı şirketten alınan 04.12.2018 tarihli yazıda;

- 8 Eylül 2018 tarihinde, kurum içi güvenlik aracından Starwood konuk rezervasyon veri tabanına erişim girişimi ile ilgili uyarı aldıkları,
 - Yaptıkları inceleme sırasında 2014 yılından itibaren Starwood ağına yetkisiz erişim olduğu,
 - Yetkisiz erişim yapan tarafın bilgileri kopyalayarak şifrelediği,
 - 19 Kasım 2018 tarihinde Şirket tarafından bilgilerin şifresinin çözüldüğünü ve içeriğin Starwood konuk rezervasyon veri tabanından alındığı,
 - 20 Eylül 2018 tarihinde veya öncesinde bir Starwood tesisinde rezervasyon yapmış olan ve sayıları yaklaşık 500 milyonu bulan konuğa ilişkin bilgilerin yer aldığı,
 - Bu konuklardan yaklaşık 327 milyonuna ilişkin bilgiler arasında ad soyad, posta adresi, telefon numarası, e-posta adresi, pasaport numarası, Starwood Tercih Edilen Konuk (“SPG”) hesabı bilgileri, doğum tarihi, cinsiyet, varış ve ayrılış bilgileri, rezervasyon tarihi ve iletişim tercihlerinin çeşitli kombinasyonlarının yer aldığı,
 - Bazı kişilere ilişkin bilgiler arasında İleri Şifreleme Standardı ile şifrelenmiş ödeme yapılan kartların numaraları ve bu kartların son kullanma tarihlerinin bulunduğu, ancak bu şifrelerin çözülüp çözülemediğini söyleyemedikleri,
 - Starwood markalı; W Hotels, St. Regis, Sheraton Hotel & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton and Design Hotels ve devremülk tesisleri olduğu,
- bilgilerine yer verilmiştir.

Yapılan deęerlendirmeler neticesinde, Kişisel Verileri Koruma Kurulunun 05.12.2018 tarih ve 2018/147 sayılı Kararı ile Marriott International, Inc. ve baęlı kuruluşları nezdinde gerçekleşen söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Öte yandan, konuya ilişkin sorular için info.starwoodhotels.com internet sitesinin ziyaret edilmesi mümkün bulunmaktadır.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Cathay Pacific Airways Limited

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Hong Kong merkezli havayolu şirketi Cathay Pacific Airways Limited (Şirket) unvanlı şirketten alınan 25.10.2018 tarihli yazıda;

- 13 Mart 2018 tarihinde bilgisayar ağları üzerinden yolcu bilgilerini içeren bilgi sistemlerine yetkisiz erişim sağlandığı, (Şirket tarafından yapılan inceleme sonucunda konuya ilişkin tespitlerin 7 Mayıs 2018 tarihinde ortaya çıktığı)
- Bahse konu veri ihlalden Cathay Pacific Airways Limited yolcularının kişisel verilerinin yanı sıra bağlı kuruluşu Hong Kong Dragon Airlines Limited yolcuları ile Asia Miles ve Marco Polo Club üyelerinin kişisel verilerinin de etkilendiği,
- Şirket tarafından yapılan incelemede Türkiye’de 1.286 kişinin söz konusu ihlalden etkilendiği, diğer taraftan Türkiye’de 155 kişinin pasaport numarasına erişildiği,
- Yetkisiz erişim sağlanmış olan kişisel veriler arasında yolcu ismi, uyruğu, doğum tarihi, telefon numarası, elektronik posta adresi, pasaport numarası, kimlik kartı numarası, “frequent flyer” üyelik numarası, müşteri hizmetleri notları ve geçmiş seyahat bilgileri bulunduğu, öte yandan erişilen kişisel veri türü ve sayısının etkilenen her yolcu özelinde değişiklik gösterdiği

bilgisine yer verilmiştir.

Yapılan değerlendirmeler neticesinde, Kişisel Verileri Koruma Kurulunun 30.10.2018 tarih ve 2018/124 sayılı Kararı ile Cathay Pacific Airways Limited ve bağlı kuruluşları nezdinde gerçekleşen söz konusu veri ihlalinin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Öte yandan, konuya ilişkin sorular için infosecurity.cathaypacific.com internet sitesinin ziyaret edilmesi veya infosecurtiy@cathaypacific.com e-posta adresi üzerinden destek alınması mümkün bulunmaktadır.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Ticketmaster UK

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Ticketmaster UK (Ticketmaster İngiltere) adına Biletix Bilet Dağıtım Basım ve Tic. A.Ş. (Biletix A.Ş.) tarafından 28.06.2018 tarihinde Kurumumuza yapılan bildirimde;

- 23 Haziran 2018 tarihinde Ticketmaster İngiltere firmasına dış kaynaklı hizmet sunan Inbenta Technologies tarafından sağlanan ve müşteri destek hizmetleri için kullanılan ürün üzerinde kötü amaçlı bir yazılım tespit edildiği,
- Inbenta Technologies tarafından sunulan bu ürünün tüm Ticketmaster International web sitelerinde kullanılmış olması sebebiyle bazı müşterilerin kişisel verilerine ve ödeme bilgilerine tanımlanmamış üçüncü kişiler tarafından izinsiz olarak erişilmiş olabileceği,
- Türkiye’de kredi kartı ve debit kart numaralarına ilişkin potansiyel bir tehlike olup olmadığının tespit edilmesi için Ticketmaster İngiltere tarafından adli müfettişlerle gerçekleştirilen çalışmaların devam ettiği,
- Bu anlamda, Türkiye’de Biletix A.Ş. aracılığıyla bilet almış veya almayı denemiş kullanıcıların verilerine erişildiğine ilişkin herhangi bir kanıt bulunmamakla birlikte, Eylül 2017 ile 23 Haziran 2018 tarihleri arasında işlem yapan kullanıcılara azami tedbiri almak adına bir bilgilendirme maili gönderildiği

bilgisine yer verilmiştir.

Yapılan değerlendirmeler neticesinde, Kişisel Verileri Koruma Kurulunun 29.06.2018 tarih ve 2018/72 sayılı Kararı ile bu aşamada Biletix A.Ş. kullanıcılarının söz konusu yetkisiz erişimden etkilenip etkilenmediği hususunda kesin bir bilgi bulunmamakla birlikte, Biletix A.Ş.’nin de Ticketmaster İngiltere ile aynı yazılımı kullandığı göz önüne alındığında, ilgili kişiler açısından olası bir güvenlik riskine karşın bilgi sahibi olunabilmesini ve Biletix A.Ş. tarafından yapılan yönlendirmeler çerçevesinde gerekli tedbirlerin alınabilmesini teminen Ticketmaster İngiltere nezdinde gerçekleşen ve Türkiye’deki Biletix A.Ş. kullanıcılarının da etkilenmiş olabileceği söz konusu yetkisiz erişimin

6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (5) numaralı fıkrası çerçevesinde Kurumun internet sitesinde ilan edilmesine karar verilmiştir.

Öte yandan, konuya ilişkin sorular için <https://guvenlik.biletix.com> internet sitesinin ziyaret edilmesi veya fan.help@biletix.com e-posta adresi üzerinden destek alınması mümkün bulunmaktadır.

Kamuoyuna saygıyla duyurulur.

Veri İhlali Bildirimi - Careem Networks Teknoloji A.Ş.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

Araç çağırma hizmeti sunmak üzere Türkiye’deki faaliyetlerini Careem Networks Teknoloji A.Ş. aracılığıyla yürüten Dubai merkezli Careem Inc. (Şirket) unvanlı şirketten alınan 18.04.2018 tarihli yazıda;

- Müşteri ve sürücü bilgilerinin tutulduğu bilgisayar sistemlerine 14.01.2018 tarihinde yetkisiz üçüncü kişilerce erişim sağlandığı, (yapılan inceleme sonucunda konuya ilişkin tespitlerin 21.03.2018 tarihinde ortaya çıktığı,)
- Şirket tarafından adli bilişim incelemesi başlatıldığı ve önde gelen bir siber güvenlik şirketinin konu ile ilgili görevlendirildiği,
- Söz konusu yetkisiz erişimden Türkiye’de mukim 103.337 müşteri ile 900 araç sürücüsünün etkilendiği,
- Yetkisiz erişim sağlanmış olan kişisel veriler arasında müşterilerin isim, telefon numarası, kredi kartı bilgisi, e-posta adresi, kayıtlı konum bilgisi ve yolculuk özeti bilgisi ile araç sürücülerine ait isim telefon numarası, araç modeli, plaka numarası, yolculuk özeti, uluslararası banka hesap numarası, T.C. kimlik numarası ve ehliyet numarası bilgilerinin olabileceği

bilgisine yer verilmiştir.

Yapılan değerlendirmeler neticesinde, Kişisel Verileri Koruma Kurulunun 02.05.2018 tarih ve 2018/45 sayılı Kararı ile Careem Inc. nezdinde gerçekleşen söz konusu yetkisiz erişimin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Öte yandan, konuya ilişkin sorular için <https://blog.careem.com/security> internet sitesinin ziyaret edilmesi veya infosupport@careem.com e-posta adresi üzerinden destek alınması mümkün bulunmaktadır.

Kamuoyuna saygıyla duyurulur.

DİĞER KURUL KARARLARI VE DUYURULARI

Bölüm İçeriği

- 27.03.2023 - Vekaleten Yapılacak Şikayetlerin Elektronik Ortamda Kurula İletilmesine İlişkin Kamuoyu Duyurusu
- 23.03.2023 - Seçim Faaliyetleri Kapsamında Siyasi Partiler ve Bağımsız Adaylar Tarafından İşlenen Kişisel Veriler Hakkında Kamuoyu Duyurusu
- 09.02.2023 - Depremden Etkilenen İlgili Kişilere Ve Veri Sorumlularına Yönelik Kamuoyu Duyurusu
- 17.12.2021 - Mağazalarda SMS Doğrulama Duyurusu
- 21.04.2022 - VERBİS Ceza Duyurusu
- 04.01.2022 - Verbis Duyurusu
- 17.12.2021 - Mağazalarda SMS Doğrulaması Duyurusu
- 10.12.2021 - Veri Koruma Görevlisi Hakkında Kamuoyu Duyurusu
- 07.12.2021 - Sertifikasyon Duyurusu
- 05.11.2021 - Belediyeler Duyurusu
- 28.09.2021 - Covid-19 PCR Test Sonucu ve Aşı Bilgisi Uygulamaları
- 03.09.2021 - WhatsApp (3)
- 09.08.2021 - Yurt Dışında Yaşayan Türkiye Cumhuriyeti Vatandaşlarının Kişisel Verilerinin Yurt Dışına Aktarılmamasına İlişkin Talepleri
- 25.06.2021 - Ortaklıkların VERBİS'e Kayıt Yükümlülüğü
- 25.06.2021 - Dernek, Vakıf ve Sendikalara Ait İktisadi İşletmelerin VERBİS'e Kayıt Yükümlülüğü
- 30.03.2021 - Kurumumuza Yapılan Şikayetlerin Usul Şartları
- 11.03.2021 - VERBİS'e Kayıt Sürelerinin Uzatılması
- 12.01.2021 - WhatsApp (2)
- 12.01.2021 - WhatsApp (1)
- 26.10.2020 - Yurtdışına Veri Aktarımı
- 01.10.2020 - Sicile Kayıt Yükümlülüğü
- 17.07.2020 - Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına Yönelik Talepler
- 23.06.2020 - VERBİS'e Kayıt Sürelerinin Uzatılması

- 07.05.2020 - Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlar
- 18.03.2020 - COVID-19 Tedbirleri
- 06.01.2020 - Kişisel Veri İhlali Bildirimlerinin Elektronik Ortamda Kurula İletilmesi
- 08.11.2019 - Veri Sorumlularının GDPR Atıfları
- 06.11.2019 - Kişisel Verilerin Korunması Kanunu Uyum Süreci
- 05.09.2019 - VERBİS'e Kayıt Süresinin Uzatılması
- 12.10.2018 - VERBİS'e Yapılan Kayıt Başvuruları
- 16.05.2018 - Yurtdışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurlar
- 06.04.2018 - Kanuna Uyum Süreci (Geçici 1. madde)
- 28.03.2018 - Rehberlik Hizmeti Veren İnternet Siteleri ve Uygulamalar

**27.03.2023 - Vekaleten Yapılacak Şikayetlerin Elektronik Ortamda Kurula İletilmesine İlişkin
Kamuoyu Duyurusu**

**Vekaleten Yapılacak Şikayetlerin Elektronik Ortamda Kurula İletilmesine İlişkin Kamuoyu
Duyurusu**

Yayınlanma Tarihi: 27.03.2023

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 15. maddesinde "Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapar." hükmü yer almakta olup, bu kapsamda Kurumumuza intikal eden şikayetler Kişisel Verileri Koruma Kurulu tarafından sonuçlandırılmaktadır.

Halihazırda şikayet dilekçeleri Kişisel Verileri Koruma Kurulu'na elden, posta veya kargo yoluyla iletilebildiği gibi www.kvkk.gov.tr adresinde hizmete sunulan "Şikayet Modülü" aracılığıyla elektronik ortamda da iletilebilmektedir.

Bu kapsamda, vekaleten yapılacak şikayetlerin daha hızlı ve etkin bir şekilde Kurumumuza iletilebilmeleri ve takip edebilmelerini teminen 27.03.2023 tarihi itibarıyla "Şikayet Modülü" sistemi avukatların da vekaleten yapacakları şikayetleri iletilebileceği şekilde güncellenmiş olup, söz konusu şikayet modülüne <https://sikayet.kvkk.gov.tr> internet bağlantısından ulaşılabilmektedir.

Kamuoyuna saygıyla duyurulur.

**23.03.2023 - Seçim Faaliyetleri Kapsamında Siyasi Partiler ve Bağımsız Adaylar Tarafından
İşlenen Kişisel Veriler Hakkında Kamuoyu Duyurusu**

Seçim Faaliyetleri Kapsamında Siyasi Partiler ve Bağımsız Adaylar Tarafından İşlenen Kişisel Veriler Hakkında Kamuoyu Duyurusu

Yayınlanma Tarihi: 23.03.2023

10 Mart 2023 tarih ve 32128 sayılı Mükerrer Resmi Gazete’de yayımlanan 2023/121 sayılı Cumhurbaşkanlığı Kararı ile Türkiye Cumhuriyeti Anayasasının 116’ncı maddesi uyarınca Türkiye Büyük Millet Meclisi genel seçimi ile Cumhurbaşkanlığı seçiminin yenilenmesine karar verilmiş olup ilgili Cumhurbaşkanlığı Kararı uyarınca seçimlerin düzenlenmesine ilişkin süreç resmi olarak başlamıştır.

Bilindiği üzere, seçim faaliyetleri kapsamında muhtelif kişisel veriler işlenmektedir. 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun 3’üncü maddesinde veri sorumlusu, “Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi” olarak tanımlanmış olup, bu kapsamda siyasi partiler başta 2820 sayılı Kanun olmak üzere ilgili kanunlar gereğince kuruluş, üyelik, seçimlerde aday belirleme faaliyetleri, yetkili organlarının seçimi ve bunların ilgili mercilere bildirim vb. işlemler kapsamında kişisel verileri işlemektedir. Dolayısıyla siyasi partiler yürüttükleri faaliyetler nedeniyle işledikleri kişisel veriler bakımından 6698 sayılı Kanun kapsamında yer alan veri sorumlularından biridir.

Siyasi partilerin ve bağımsız adayların kişisel veri işleme faaliyetlerinde, işlenecek kişisel verinin niteliğine göre 6698 sayılı Kanun’un kişisel verilerin işlenme şartları başlıklı 5’inci ve özel nitelikli kişisel verilerin işlenme şartları başlıklı 6’ncı maddelerinde belirtilen veri işleme şartlarına dayalı olarak kişisel veri işlemesi gerekmektedir. Bu hususta, Kişisel Verileri Koruma Kurumu tarafından bir bilgi notu hazırlanmış olup seçim süreçlerinde kişisel veri işleme faaliyetlerinde söz konusu hususlara uygun hareket edilmesi önem arz etmektedir.

Kamuoyuna saygıyla duyurulur.

T.C.

KİŞİSEL VERİLERİ KORUMA KURUMU

Seçim Faaliyetlerinde Kişisel Verilerin Korunması İçin Siyasi Partiler ve Bağımsız Adaylar Hakkında Bilgi Notu

Seçimler, siyasal hakların kullanılması, vatandaşların yönetime doğrudan ve/veya dolaylı olarak katılımı açısından sağlıklı ve iyi işleyen demokrasilerin önemli unsurlarından birisidir. Ülkemizde Anayasa ve kanunlarda gösterilen şartlara uygun olarak, Anayasa değişikliklerine ilişkin kanunların halkoyuna sunulması, Cumhurbaşkanı seçimi, milletvekili genel seçimi, mahalli idareler ile mahalle muhtarlıkları ve ihtiyar heyetleri seçimleri yapılmaktadır.

Seçim faaliyetleri (seçmen kütüğünün düzenlenmesi, güncellenmesi, askıya çıkartılması, aday adaylığı, aday gösterme, kesin aday listelerinin ilanı, seçim propagandası, kamuoyu araştırmaları, oy verme vb.) kapsamında kamu kurumları ve siyasi partilerce kişisel verilerin işlenmesi zorunlu ve kaçınılmazdır. Bu kapsamda seçim süreçlerinde kişisel verilerin işlenmesinin ilgili diğer kanunların yanı sıra 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) hükümlerine de uygun olması gerekmektedir.

2820 sayılı Siyasi Partiler Kanunu ile siyasi partilerin kurulmaları, teşkilatlanmaları, faaliyetleri, görev, yetki ve sorumlulukları, mal edinimleri ile gelir ve giderleri, denetlenmeleri, kapanma ve kapatılmalarıyla ilgili hükümler düzenlenmiştir. Aynı Kanunun 3'üncü maddesinde siyasi partiler, "Anayasa ve kanunlara uygun olarak; Cumhurbaşkanı, milletvekili ve mahalli idareler seçimleri yoluyla, tüzük ve programlarında belirlenen görüşleri doğrultusunda çalışmaları ve açık propagandaları ile milli iradenin oluşmasını sağlayarak demokratik bir Devlet ve toplum düzeni içinde ülkenin çağdaş medeniyet seviyesine ulaşması amacını güden ve ülke çapında faaliyet göstermek üzere teşkilatlanmış tüzel kişiliğe sahip kuruluşlar" olarak tanımlanmıştır.

Kanunun 3 üncü maddesinde veri sorumlusu, "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi" olarak tanımlanmaktadır. Siyasi partiler başta 2820 sayılı Kanun olmak üzere ilgili kanunlar gereğince kuruluş, üyelik, seçimlerde aday belirleme faaliyetleri, yetkili organlarının seçimi ve bunların ilgili mercilere bildirim vb. işlemler kapsamında kişisel verileri işlemekte, bu verileri yine ilgili hükümler çerçevesinde aktarabilmektedir. Dolayısıyla, siyasi partiler yürüttükleri faaliyetleri nedeniyle işledikleri kişisel veriler bakımından Kanun'a göre "veri sorumlusu" dur.

A. Kişisel Verilerin ve Özel Nitelikli Kişisel Verilerin İşlenmesi Şartları

Türkiye Cumhuriyeti Anayasası, 2820 sayılı Siyasi Partiler Kanunu, 298 sayılı Seçimlerin Temel Hükümleri ve Seçmen Kütükleri Hakkında Kanun, 2839 sayılı Milletvekili Seçimi Kanunu, 2972 sayılı Mahalli İdareler ile Mahalle Muhtarlıkları ve İhtiyar Heyetleri Seçimi Hakkında Kanun ve 6271 sayılı Cumhurbaşkanı Seçim Kanununun ilgili maddelerinde yer alan hükümler çerçevesinde Siyasi Partiler kişisel veri ve özel nitelikli kişisel veri işleyebilmektedir.

Kişisel verilerin işlenmesi şartları Kanunun 5 nci maddesinde, özel nitelikli kişisel verilerin işlenmesi şartları ise Kanunun 6 ncı maddesinde düzenlenmiştir. Siyasi Partiler tarafından ilgili mevzuat hükümlerine göre işlenen ve aktarılan kişisel verilerin bir bölümü Kanun'un 5 inci maddesinin (2) numaralı fıkrasında hukuka uygunluk nedenlerinden (a) bendinde yer alan "kanunlarda açıkça öngörülme" ve ilgili kişinin özel nitelikli kişisel verisi olan "siyasi düşüncesi"nin işlenmesine neden olan kişisel veri işleme faaliyetleri bakımından ise Kanunun 6 ncı maddesinin (3) numaralı fıkrasında yer alan "sağlık ve cinsel hayat dışındaki verilerin, Kanunlarda öngörülen hallerde ilgili kişinin açık rızası olmaksızın işlenmesi mümkündür" hükmü gereğince işlenebilmektedir. Bu durumda, ilgilinin açık rızası aranmaksızın kişisel verilerin işlenmesi mümkün olmaktadır.

2/6

Siyasi partiler aşağıda yer alan mevzuat hükümleri gereği kişisel verileri işlemektedir:

Örnek 1: Siyasi partilerin kuruluş bildiri ve belgelerinde: Siyasi partiler, aşağıda belirtilen bildiri ve belgelerin, İçişleri Bakanlığına verilmesiyle tüzel kişilik kazanırlar.

Bildiride, kurulacak siyasi partinin adı, genel merkez adresi, kurucuların adı, soyadı, doğum yeri ve tarihi, öğrenim durumları, meslek veya sanatlarıyla ikametgahlarının belirtilmesi ve bu bildirin bütünü kurucular tarafından imzalanması ve bildiriye beşer adet olmak üzere kurucuların nüfus kayıt örnekleri, adli sicil belgeleri ve kurucuların ayrı ayrı düzenledikleri siyasi parti kurucusu olabilme şartlarını taşıdıklarını belirten imzalı beyannameler ile kurucular tarafından imzalanmış parti tüzüğü ve programının eklenmesi şarttır.

Bilgi ve belgelerin alındığı anda, İçişleri Bakanlığınca bir alındı belgesi verilir.

İçişleri Bakanlığı, kuruluş bildirisi ve alındı belgesinin onaylı birer örneği ile bildiri eklerinin birer takımını üç gün içinde Cumhuriyet Başsavcılığı ile Anayasa Mahkemesine gönderir. (2820 sayılı Kanunun 8 inci maddesi).

Örnek 2: Siyasi parti sicili: Cumhuriyet Başsavcılığınca her siyasi parti için bir sicil dosyası tutulur.

Bu sicil dosyasında:

- a) Kuruluş bildirisi ve ekleri;
 - b) (Değişik: 21/5/1987 - 3370/2 md.) Merkez organları ile, teşkilat kurdukları il, ilçe ve beldeleri, bunların organlarında görev alanların adlarını, soyadlarını, doğum yer ve tarihlerini, meslek veya sanatlarını ve ikametgahlarını gösterir onaylı listeleri,
 - c) Partinin faaliyetlerini düzenleyen her türlü yönetmelikler ve diğer yayınları,
 - d) Partiye kayıtlı üyelerin, ilçelere göre (b) bendindeki bilgileri içeren listeleri,
- bulunur.

Cumhuriyet Başsavcılığınca istenilen sicille ilgili diğer bilgi ve belgeler de bu dosyaya konulur.

Siyasi partiler, (b) ve (c) bentlerindeki bilgi ve belgeler ile bunlarda ve parti tüzük ve programlarında yapılan değişiklikleri, yayın veya değişiklik tarihinden itibaren on beş gün içinde; (d) bendindeki listeler ile bunlarla ilgili değişiklikleri ise, altı ayda bir Cumhuriyet Başsavcılığına gönderirler.

Siyasi partilerin kapatılmaları veya kapanmaları sicillerine işlenir.

Bu sicil herkese açıktır. Soruşturma ile ilgili bilgilerin gizliliğine ilişkin hükümler saklıdır. (Ek:31/3/1988 - 3420/2. md.) Siyasi Partilerin bu Kanuna göre yapacakları kongre delege seçimlerinde ve ön seçimlerde (b) ve (d) bentleri gereğince Cumhuriyet Başsavcılığına bildirilmiş üye listeleri esas alınır. (2820 sayılı Kanununun 10 uncu maddesi).

Örnek 3: Seçimlerin yapılması: Seçim yapılacak büyük kongreyle il ve ilçe kongrelerinin toplantılarından en az on beş gün önce, kongreye katılacak parti üyelerini belirleyen listeler, büyük kongreyle il kongreleri için Yüksek Seçim kurulunun önceden belirleyeceği seçim kurulu başkanına, ilçe kongreleri için o yer ilçe seçim kurulu başkanına ilçede birden fazla ilçe seçim kurulunun bulunması halinde birinci ilçe seçim kurulu başkanına iki nüsha olarak verilir.

Seçim kurulu başkanı, gerektiğinde ilgili kayıt ve belgeleri de getirtip incelemek suretiyle varsa noksanları tamamlattırdıktan sonra seçime katılacakları belirleyen liste ile yukarıdaki fıkrada belirtilen diğer hususları onaylar. Onaylanan liste ile toplantıya ilişkin diğer hususlar kongrenin toplantı tarihinden yedi gün önce siyasi partinin ilgili teşkilatının bulunduğu binada asılmak suretiyle ilan edilir. İlan süresi üç gündür.

3/6

İlan süresi içinde, listeye yapılacak itirazlar hakim tarafından incelenir ve en geç iki gün içinde kesin olarak karara bağlanır. Bu suretle kesinleşen listeler ile toplantıya ilişkin diğer hususlar, hakim tarafından onaylanarak siyasi partinin ilgili teşkilatına gönderilir.

(Değişik: 31/10/1990 - 3673/1 md.) Listede adı yazılı bulunmayanlar oy kullanamazlar. Oylar, oy verenin nüfus hüviyet cüzdanı veya resimli üyelik kimlik kartı veya kimlik tespiti amacıyla düzenlenmiş resmi belge ile ispat edilmesinden ve listedeki isminin karşısındaki yerin imzalanmasından sonra kullanılır. (2820 sayılı Kanununun 21/2-3-4-8 inci maddesi).

Örnek 4: Organlarda görev alanların ilgili makamlara bildirilmesi: Parti kongreleri hariç olmak üzere, her kademedeki parti organlarıyla parti tüzüğünde belirtilen bir göreve getirilenlerin adları, soyadları, doğum yer ve tarihleri, meslek veya sanatları, ikametgahları ve nüfus cüzdanı örnekleri; o mahallin en büyük mülki amirliğine seçim veya atanmadan başlayarak on beş gün içinde yazı ile bildirilir. Valiliklerce birleştirilen bu bilgi ve belgeler İçişleri Bakanlığına ve Cumhuriyet Başsavcılığına gönderilir.

Merkez organlarında görevlendirilenlerle ilgili bilgi ve belgeler de aynı süre içinde doğrudan İçişleri Bakanlığına ve Cumhuriyet Başsavcılığına verilir. (2820 sayılı Kanununun 33 üncü maddesi).

Örnek 5: Parti adaylarının tespiti: Siyasi partiler, milletvekilliği genel veya ara seçimlerinde, adaylık için müracaat eden ve adaylığı uygun bulunanlar arasından, adayların tespitini; serbest, eşit, gizli oy, açık tasnif esasları çerçevesinde, tüzüklerinde belirleyecekleri usul ve esaslardan herhangi biri veya birkaçı ile yapabilirler (2820 sayılı Kanununun 37 inci maddesi).

26 Nisan 1961 tarihli ve 298 sayılı Seçimlerin Temel Hükümleri ve Seçmen Kütükleri Hakkında Kanununun bu Kanuna aykırı olmayan hükümleri, önseçimlerde ve kullanılacak parti seçmen kütükleri hakkında da uygulanır (2820 sayılı Kanununun 38 inci maddesi).

Siyasi partilerin genel başkanlığı; partilerinin, aday adayları listelerini ve seçim çevrelerini önseçimin yapılacağı tarihten en az yirmi gün önce saat on yediye kadar Yüksek Seçim Kuruluna ve ilgili il ve ilçe seçim kurullarına bildirir. Kurullarca ilgiliye bir alındı belgesi verilir (2820 sayılı Kanununun 40 ıncı maddesinin altıncı fıkrası)

Örnek 6: Parti seçmen listesi: Siyasi partilerin ilçe teşkilatı, kendi çevrelerindeki üyelerini muntazam kayıt ve sıra numarası ve partiye giriş çıkış tarihleri ve üye hakkında diğer bilgileri ihtiva eden bir üye kayıt defterine kaydederler.

Üye Kayıt Defterinde Parti üyesi olarak kayıtlı bulunan ve Cumhuriyet Başsavcılığınca seçim kurullarına gönderilen listelerde yer alan üyeler önseçimde oy kullanabilir.

Siyasi Partiler kayıtlı üyelerin tamamı dışında başka bir usulle aday yoklaması yapacaksa bu halde oy kullanacak seçmen listelerini önseçimden en az otuz gün önce ilçe seçim kurulu başkanlığına üye kayıt defterleri ile birlikte vermek zorundadırlar.

Bu listeler önseçim tarihinden 25 gün önce parti yönetim kurulu ve ilçe seçim kurulu binaları önüne asılır. Sekizinci fıkradaki itiraz süresinden sonra kesinleşen listelere göre parti seçmen kartları ilçe seçim kurulu başkanlığınca her üyeye dağıtılır.

Parti üyeleri, parti seçmen listesine, asıldığı tarihten itibaren on beş gün içinde yazıyla itiraz edebilirler. İtirazlar ilçe seçim kurulu tarafından incelenir ve en geç iki gün içinde kesin olarak karara bağlanır. İtirazın yerinde görülmesi halinde parti seçmen listesi düzeltilir (2820 sayılı Kanununun 42 nci maddesinin bir, üç altı ve sekiz numaralı fıkraları).

4/6

Örnek 7: Önseçimde propaganda ile ilgili hükümler: Siyasi partiler, tüzüklerinde gösterilmek kaydıyla aday adayları için bunların vereceği bilgileri de esas alarak aday adaylarının meslek veya sanat hayatlarındaki derece, başarı ve eserlerini, memlekete yaptığı hizmetleri gösterir, vesikalık fotoğraflarını taşıyan matbualar bastırıp dağıtabilir. Aday adaylarının soyadı alfabe sırasına göre düzenlenecek benzer bilgileri içeren matbualar sandık başlarına asılabilir (2820 sayılı Kanununun 43 üncü maddesinin ikincifıkrası).

Örnek 8: Kimliğin tespiti: Önseçimlerde oy vermek için parti seçmen kartının gösterilmesi şarttır. Bu belgeyi göstermeyenlerden veya belgenin sahibi olduğunda tereddüt edilenlerden parti hüviyet cüzdanı, o da yoksa nüfus hüviyet cüzdanı istenir (2820 sayılı Kanununun 47 nci maddesi).

Örnek 9: Son işlemler: Yüksek Seçim Kurulu, il seçim kurullarından gelen önseçimle tespit edilmiş parti adayları listelerinin tasdikli birer örneğini derhal ilgili partilerin genel başkanlıklarına teslim eder. Parti genel başkanlıkları, 38 inci madde ve parti mevzuatı gereğince merkez aday olarak seçilen parti adaylarını bu listelere dahil ederek seçim çevrelerine göre düzenleyecekleri parti aday cetvellerini, kanun hükümlerine göre Yüksek Seçim Kuruluna süresi içerisinde bildirirler. (2820 sayılı Kanununun 48 inci maddesi).

Örnek 10: Önseçim evrakının saklanması: Hesaba katılan, katılmayan ve itiraza uğramış olan oy pusulaları; sayım ve döküm cetvelleri ve adaylığa seçilme tutanaklarıyla diğer her türlü evrak, milletvekili seçimlerinin kesin sonuçlarının ilanı tarihinden itibaren üç ay süreyle ilçelerde ilçe seçim kurulu başkanı ve illerde il seçim kurulu başkanı tarafından saklanır.

Bu evrak, Yüksek Seçim Kurulunun istemi olmaksızın hiçbir yere gönderilmez (2820 sayılı Kanununun 49 uncu maddesi).

Örnek 11: Tutulacak defter ve kayıtlar: Her kademedeki parti organları üye kayıt defteri, karar defteri, gelen ve giden evrak kayıt defteri, gelir ve gider defteri ile demirbaş eşya defteri tutmak zorundadırlar. Üye kayıt defteri, mahalle ve köy esasına göre tutulur.

Partiye giriş işlemlerini gösteren üyelik beyannamelerinin birer örneği ilçe ve il kademesinde, alfabetik sıra esasına göre tasnif edilmiş olarak ayrı bir dosyada saklanır. Bu evrak, Yüksek Seçim Kurulunun istemi olmaksızın hiçbir yere gönderilmez (2820 sayılı Kanununun 60 ıncı maddesinin bir,iki ve yedi numaralı fıkraları).

Örnek 12: Defter, sicil ve kayıtların tutulma usulü: Bu Kanuna göre tutulacak sicil, dosya, defter ve kayıtlar elektronik ortamda da tutulabilir. Ancak form veya sürekli form şeklinde tutulacak defterler, kullanılmaya başlanmadan önce her bir sayfasına numara verilerek ve onaylatılarak kullanılabilir. Onaylı sayfalar kullanıldıktan sonra defter hâline getirilerek muhafaza edilir.

Yargıtay Cumhuriyet Başsavcılığı siyasi parti sicillerine işlenmek üzere elektronik ortamda veri aktarımı, ancak siyasi parti genel merkezleri tarafından ve bu işlemlerle görevlendirilecek kişilerce yerine getirilir. (2820 sayılı Kanununun Ek 7 nci maddesi).

Örnek 13: Siyasi partilerin aday listelerini vermeleri: Siyasi partilerin genel merkezleri, seçime katılacakları seçim çevrelerine ait aday listeleri (...) Yüksek Seçim Kuruluna (...) alındı belgesi karşılığında ön seçim gününden en geç on gün sonraki gün, saat 17.00'ye kadar verirler.

Yüksek Seçim Kurulu, bunları derhal il seçim kurullarına bildirir. Yüksek Seçim Kurulu, bütün siyasi partilerin aday listelerini Resmi Gazete ve radyo ile il seçim kurulları da kendi çevrelerine ait olanları alışılmış araçlarla geçici listeler halinde ilan ederler (2839 sayılı Kanununun 20 inci maddesi)..

Örnek 14: Siyasi partilerce aday gösterilme: Türkiye Büyük Millet Meclisinde grubu bulunan siyasi partiler grup kararıyla, diğer siyasi partiler ise tüzüklerinde gösterilen yetkili organlarının kararıyla Cumhurbaşkanlığına aday gösterebilirler.

5/6

Yüksek Seçim Kurulu tarafından ilân edilen süre içinde, adayların isimleri, muvafakat belgeleri ve gerekli diğer belgelerle birlikte Yüksek Seçim Kuruluna başvurularak aday gösterilmiş olur. Her siyasi parti veya parti grubu ancak bir aday için başvuruda bulunabilir. Bir kişiyi birden fazla siyasi parti grubu veya siyasi parti aday gösterebilir.

Adaylarla ilgili bilgi ve belgelerde eksiklik tespit edilmesi hâlinde, Yüksek Seçim Kurulunca, ilgili siyasi partilere eksikliklerin giderilmesi için beş günlük süre verilir.

Eksiklikleri, verilen süre içinde gidermeyen siyasi partiler, aday göstermekten vazgeçmiş sayılır (6271 sayılı Kanun'un 8 inci maddesi).

Diğer taraftan, siyasi partilerin kişisel veri işleme faaliyetlerinde işlenecek verinin türüne göre Kanunun 5 inci ve 6 ncı maddelerinde belirtilen veri işleme şartlarına uygun hareket etmesi gerekmektedir. İlgili kişilerden açık rıza alınması gerekiyor ise Kanun 3 üncü maddesinde yer verilen açık rıza tanımı kapsamında,

- Belirli bir konuya ilişkin olarak,
- Bilgilendirmeye dayalı olarak,
- Özgür iradeyle dayalı olarak ilgili kişilerin açık rızası alınmalıdır.

Öte yandan, ilgili kişi, kişisel verilerin geleceğini belirleme hakkına sahip olup, dilediği zaman veri sorumlusuna vermiş olduğu açık rızasını geri alabilir. Bununla birlikte, açık rızanın geri alınması ileriye yönelik sonuç doğuracaktır bir başka deyişle, açık rızaya dayalı olarak gerçekleştirilen tüm faaliyetler geri alma beyanının veri sorumlusuna ulaştığı andan itibaren veri sorumlusu tarafından durdurulmalıdır. Yani, geri alma beyanı veri sorumlusuna ulaştığı andan itibaren hüküm doğurur.

298 sayılı Seçimlerin Temel Hükümleri ve Seçmen Kütükleri Hakkında Kanunun "Seçim Propagandası" başlıklı ikinci kısmında siyasi partilerin seçim propaganda usulleri belirlenmiş olup, anılan Kanunun 49 uncu maddesine göre seçim propaganda süresi "oy verme gününden önceki onuncu günün sabahında başlar ve oy verme gününden önceki günün saat 18.00'inde sona erer" denilerek sınırlandırılmıştır. Bahse konu Kanunun "Basın, iletişim araçları ve internette propaganda" başlıklı 55/B maddesinin birinci fıkrasında "Seçime katılan siyasi partiler ve bağımsız adaylar, seçim propaganda süresinin sona ermesine kadar, yazılı basında ilan ve reklam yoluyla veya internet sitesi açarak sözlü, yazılı veya görüntülü propaganda yapabilirler" ifadesine, ikinci fıkrasında ise vatandaşların, elektronik posta adreslerine gönderilecek mesajlarla, taşınabilir veya sabit telefonlarına sesli, görüntülü veya yazılı mesaj göndermek suretiyle propaganda yapılamayacağı ancak siyasi partilerin kendi üyelerine gönderdiği sesli, görüntülü veya yazılı mesajların her zaman serbest olduğu hususuna yer verilmektedir. 6698 sayılı Kanunun 5 inci maddesinin (2) numaralı fıkrasında ilgili kişinin açık rızasının aranmayacağı durumlar arasında "a) Kanunlarda açıkça öngörülmesi" sayılmakta olup her iki Kanun birlikte değerlendirildiğinde siyasi partilerin sadece kendi üyelerine sesli, görüntülü veya yazılı mesajlar göndermek amacıyla kişisel veri olan iletişim verisini işleminin mümkün olduğu değerlendirilmektedir.

298 sayılı Kanunun 55/B maddesi doğrultusunda bağımsız adayların vatandaşlara sesli, görüntülü veya yazılı mesajlar gönderemeyecekleri anlaşılmakta olup, bağımsız adaylar vatandaşların kişisel verilerini bu amaçla işlememelidir.

Konuya 298 sayılı Kanun ve YSK tarafından alınan muhtelif kararlar bağlamında yaklaşıldığında, kişilerin iletişim bilgilerini işleyerek mesaj göndermek suretiyle propoganda yapılamayacağı düzenlenmiş olduğu dikkate alındığında, bağımsız adayların kişilerin iletişim bilgilerini işlemek suretiyle veri sorumlusu olabilmesinin hukuki bir dayanağı bulunmadığı değerlendirilmektedir.

6/6

B. Aydınlatma Yükümlülüğü

Kanunun 10 uncu maddesi hükmü çerçevesinde, siyasi partiler kişisel veri işleme faaliyetleri sırasında ilgili kişileri aydınlatmakla yükümlüdürler. Siyasi partiler, aydınlatma yükümlülüklerini yerine getirirken Kanunun ilgili hükmü ile “Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ” e uygun olarak hareket etmelidirler.

C. İlgili Kişinin Hakları

Siyasi partilerin, Kanunun 11 inci maddesinde düzenlenen ilgili kişinin hakları konusunda da yükümlülükleri bulunmakta olup, bu bağlamda Kanunun 13 üncü ve 14 üncü maddelerinde düzenlenen hükümler kapsamında Kanunun uygulanmasıyla ilgili olarak kendilerine yapılan başvuruları süresi içinde ve gerektiği şekilde yanıtlamaları gerekmektedir.

D. Veri Güvenliğine İlişkin Yükümlülükler

Siyasi partiler veri sorumlusu olarak, 6698 sayılı Kanun’un 12’nci maddesinde düzenlenen “Veri Güvenliğine İlişkin Yükümlülükler”i yerine getirmekle yükümlüdür. Bu kapsamda;

- Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
- Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

E. VERBİS’e Kayıt Yükümlülüğü

Kanunun 16 ncı maddesinde düzenlenen VERBİS’e kayıt yükümlülüğüne ilişkin olarak Kişisel Verileri Koruma Kurulu’nun 02.04.2018 tarih ve 2018/32 sayılı kararında, 2820 sayılı Siyasi Partiler Kanununa göre kurulmuş siyasi partiler “Veri Sorumluları Sicili” ne (VERBİS) kayıt

yükümlülüğünden istisna tutulmuş olan veri sorumluları arasında sayıldığından siyasi partilerin sicile kayıt yükümlülüğü bulunmamaktadır.

**09.02.2023 - Depremden Etkilenen İlgili Kişilere Ve Veri Sorumlularına Yönelik Kamuoyu
Duyurusu**

Depremden Etkilenen İlgili Kişilere Ve Veri Sorumlularına Yönelik Kamuoyu Duyurusu

Yayınlanma Tarihi: 09.02.2023

06.02.2023 tarihinde Kahramanmaraş'ın Pazarcık ve Elbistan ilçeleri merkezli olarak gerçekleşen iki büyük deprem felaketi nedeniyle 08.02.2023 tarihli Resmî Gazetede yayımlanan 6785 sayılı Cumhurbaşkanı Kararı ile Anayasanın 119 uncu maddesi ile 2935 sayılı Olağanüstü Hal Kanununun 3 üncü maddesinin birinci fıkrasının (a) bendine göre Adana, Adıyaman, Diyarbakır, Gaziantep, Hatay, Kahramanmaraş, Kilis, Malatya, Osmaniye ve Şanlıurfa illerinde 08.02.2023 Çarşamba günü saat 01.00'dan itibaren üç ay süreyle olağanüstü hâl ilan edilmesine karar verilmiştir.

Deprem bölgesindeki arama-kurtarma çalışmaları devam ederken kamu kurumları, kendi sorumluluk alanlarıyla ilgili ilave tedbirler almakta ve kamuoyuna duyurmaktadır. Bu itibarla Kurumumuz tarafından 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında şikâyet, ihbar, veri ihlal bildirimleri ve diğer yükümlülükler hakkında veri sorumluları ve ilgili kişilerce dikkate alınması gereken sürelerle ilişkin olarak açıklama yapılması gereği ortaya çıkmıştır.

Bu çerçevede, Kişisel Verileri Koruma Kurulu tarafından

Deprem sebebiyle olağanüstü hâl ilan edilen illerde bulunan veya diğer illerde bulunmakla birlikte depremden etkilenen ilgili kişiler ya da veri sorumluları,

Deprem sebebiyle olağanüstü hâl ilan edilen il barolarına bağlı olarak görev yapan veya diğer il barolarına bağlı olarak görev yapmakla birlikte depremden etkilenen avukatlar tarafından temsil edilen ilgili kişiler ya da veri sorumluları

açısından Kanunda ve ilgili alt düzenlemelerde yer alan sürelerin değerlendirilmesinde depremin sebep olduğu olağanüstü koşulların gözetileceği hususu kamuoyuna saygıyla duyurulur.

17.12.2021 - Mağazalarda SMS Doğrulama Duyurusu

Mağazalarda Alışveriş Sırasında İlgili Kişilere SMS ile Doğrulama Kodu Gönderilmesi Suretiyle Kişisel Verilerin İşlenmesine İlişkin Kamuoyu Duyurusu

Yayınlanma Tarihi: 17.12.2021

Kurumumuza intikal eden muhtelif sayıda şikâyet ve ihbarda, mağazalarda gerçekleştirilen alışveriş müteakip kasa işlemleri esnasında ilgili kişilere SMS ile doğrulama kodu gönderildiği ve ödemelerinin tamamlanması ya da bilgilerinin güncellenmesi için gerekli olduğu gerekçesi ile söz konusu kodun kasa görevlisine bildirilmesinin istenildiği, ancak bahse konu işlemin akabinde ilgili kişilere söz konusu mağaza faaliyetleri ile ilgili ticari elektronik ileti gönderildiği iddialarına yer verildiği görülmektedir. Kişisel Verileri Koruma Kurulu tarafından söz konusu şikâyet ve ihbarlara yönelik yapılan incelemelerde ilgili kişilere ödeme işlemleri esnasında doğrulama kodu gönderilen SMS içeriklerinde ya da SMS gönderimi öncesinde veri sorumlusunca herhangi bir aydınlatma yapılmadığı ve/veya söz konusu kodun ödeme işlemlerinin tamamlanması ya da bilgilerinin güncellenmesi için gerekli olduğu gerekçesi ile istenilmesine rağmen veri sorumlusu tarafından bu yolla ticari elektronik ileti gönderimine ilişkin açık rıza alınması suretiyle ilgili kişilerin yanıltıldığı tespit edilmiştir.

Bilindiği üzere, kişisel verilerin işlenmesi 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 5 inci maddesinde düzenlenmiş olup, buna göre Kanunun 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği hükme bağlandıktan sonra (2) numaralı fıkrasında ise ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu işleme şartları sayılmıştır.

Kanunun 3 üncü maddesinde ise açık rıza; “belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza” şeklinde tanımlanmış olup, söz konusu tanımdan açık rızanın taşınması gereken üç unsurunun bulunduğu görülmektedir. Öncelikle, alınan açık rızanın belirli bir konuya ilişkin ve o konu ile sınırlı olması, diğer bir ifade ile veri sorumlusu tarafından açık rıza beyanının hangi konuya ilişkin olarak istenildiğinin açıkça ortaya konulması gerekmektedir. Eğer birden çok kategoriye ilişkin verinin işlenmesine dair açık rıza beyanında bulunulacaksa, açık rızanın hangi verilerin ve ne amaçlarla işleneceği gibi, işlemin farklı noktaları açısından da verilmiş olması zorunluluk arz etmektedir. Öte yandan, açık rıza bir irade beyanı olup, kişinin özgür bir şekilde rıza gösterebilmesi için neye rıza gösterdiğini de bilmesi, bu anlamda kişinin sadece konu üzerinde değil,

aynı zamanda rızasının sonuçları üzerinde de tam bir bilgi sahibi olması gerekmektedir. Son olarak kişinin irade beyanı olan rıza, kişinin yaptığı davranışın bilincinde ve kendi kararı olması halinde geçerlilik kazanacaktır. Kişinin iradesini sakatlayacak her türlü fiil, kişisel verilerin işlenmesi için verdiği açık rızayı da sakatlayacaktır. Cebir, tehdit, hata ve hile gibi iradeyi sakatlayan hallerde, kişinin özgür biçimde karar vermesi mümkün değildir. Dolayısıyla, bu gibi durumlarda bir özgür irade açıklamasından bahsedilemeyecektir. Ayrıca, açık rızanın özgür irade ile açıklanması gerektiğinden, ilgili kişinin açık rızasının alınması, bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının ön şartı olarak ileri sürülmemelidir.

Öte yandan Kanunun 10 uncu maddesi çerçevesinde, kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi tarafından, ilgili kişilere maddede sayılan hususlarda bilgi verilmek suretiyle aydınlatma yükümlülüğünün yerine getirilmesi gerekmektedir. Bu kapsamda, aydınlatma yükümlülüğü gerek açık rıza gerekse de Kanundaki diğer kişisel veri işleme şartlarından bağımsız olarak yerine getirilmesi gereken bir yükümlülüktür. Bununla birlikte, kişisel veri işleme faaliyetinin ilgili kişinin açık rızasına dayanarak gerçekleştirilmesi durumunda, veri sorumlusu tarafından aydınlatma yükümlülüğü ile açık rıza alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir.

Bu kapsamda, Kişisel Verileri Koruma Kurulu tarafından yapılan incelemeler neticesinde;

- Kişilerin telefonuna gönderilecek olan SMS'in amacının ne olduğu ve bu SMS ile iletilen kodun verilmesi halinde ne gibi sonuçlar doğuracağı hususunun, katmanlı aydınlatmanın bir gereği olarak ilk aşamada veri sorumlusunun mağazalarda yetkilendirdiği kişiler tarafından ilgili kişilere açık ve anlaşılır bir biçimde aktarılması, ayrıca aydınlatma yükümlülüğünün yerine getirilebilmesini teminen yine söz konusu SMS içeriklerinde de gerekli kanalların sağlanması,
- Mağazalarda gerçekleştirilen alışverişler ile ilgili ödeme esnasında ilgili kişilere SMS ile doğrulama kodu gönderilerek üyelik sözleşmesi, kişisel verileri işleme izni, ticari elektronik ileti onayı vb. birbirinden farklı işleme faaliyetlerinin tek bir eylemle gerçekleştirilmesine yönelik uygulamalara son verilmesi, söz konusu işleme faaliyetlerine yönelik seçenek sunulmak suretiyle ayrı ayrı açık rıza alınması,
- Bunun yanı sıra, veri sorumlularınca açık rıza alınması ve aydınlatma yükümlülüğü işlemlerinin birlikte gerçekleşmesine neden olabilecek durumlardan kaçınılması,
- Ticari elektronik ileti gönderimi için açık rıza alınmasını teminen SMS doğrulama kodu gönderilmesine yönelik bir uygulamaya gidilmesi halinde ise söz konusu işlemde alınacak açık rızanın tüm unsurları kapsamı

önem arz etmektedir.

Kamuoyuna saygıyla duyurulur.

21.04.2022 - VERBİS Ceza Duyurusu

Kamuoyu Duyurusu (VERBİS)

Yayınlanma Tarihi: 21.04.2022

Bilindiği üzere 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 16'ncı maddesinde "(1) Kurulun gözetiminde, Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili tutulur. (2) Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır." hükmü ile Geçici 1 inci maddesinin (2) numaralı fıkrasında "Veri sorumluları, Kurul tarafından belirlenen ve ilan edilen süre içinde Veri Sorumluları Siciline kayıt yaptırmak zorundadır." hükmü yer almaktadır.

Bu hükme istinaden Kurulun 11/03/2021 tarihli ve 2021/238 sayılı Kararı ile; yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları ile yurtdışında yerleşik gerçek ve tüzel kişi veri sorumlularının, yıllık çalışan sayısı 50'den az ve yıllık mali bilançosu 25 milyon TL' den az olup ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek ve tüzel kişi veri sorumlularının, kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşu veri sorumlularının Sicile kayıt ve bildirim yükümlülüğünü yerine getirmeleri için 31.12.2021 tarihine kadar süre verilmiştir.

Kanun'un 18'inci maddesinin (1) numaralı fıkrasında yer alan "(ç) 16 ncı maddesinde öngörülen Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezası verilir." hükmü ile aynı maddenin (3) numaralı fıkrasında yer alan "Birinci fıkrada sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu Kurula bildirilir." hükmü gereği Sicile kayıt ve bildirim yükümlülüğünü yerine getirmeyen veri sorumluları hakkında Kurul tarafından re'sen idari yaptırım uygulanabilecektir.

Bu kapsamda Sicile kayıt ve bildirim yükümlülüğünü yerine getirmediği tespit edilen veri sorumluları hakkında Kanun'un 18'inci maddesi uyarınca idari yaptırım uygulanmasına başlanmıştır.

Kamuoyuna saygıyla duyurulur.

Veri Sorumluları Siciline Kayıt Hakkında Kamuoyu Duyurusu

Yayınlanma Tarihi: 04.01.2022

Bilindiği üzere Veri Sorumluları Sicili Hakkında Yönetmelik'in (Yönetmelik) 5 inci maddesinde veri sorumlularının, Sicile sunulan ve Sicilde yayınlanan bilgilerin eksiksiz, doğru, güncel ve hukuka uygun olmasından sorumlu olduğu, Sicile açıklanacak bilgilerin Kişisel Veri İşleme Envanterine dayalı olarak hazırlanması gerektiği ve veri sorumlularının Sicile kaydolmasının Kanun kapsamındaki diğer yükümlülüklerini ortadan kaldırmayacağı belirtilmektedir.

Aynı Yönetmelik'in 9 uncu maddesinde ise Sicile yapılan kayıt başvurusunun; başvuru formunda yer alan bilgiler, kişisel verilerin işleme amacı, veri konusu kişi grupları, kişisel verilerin aktarıldığı alıcı grupları, yabancı ülkelere aktarım öngörülüp öngörülmediği, alınan veri güvenliği tedbirleri ile saklama sürelerine ilişkin bilgileri içereceği hükmü yer almaktadır.

Bu kapsamda Kurumumuzca yapılan değerlendirme sonucunda, aşağıdaki hususların tekrar hatırlatılmasında fayda görülmektedir:

1. Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) kayıt başvuru formunun sadece sisteme girilmesi veya Kuruma posta, kargo, kurye, KEP ile iletilmesi ya da elden teslim edilmesi Sicile kayıt ve bildirim yükümlülüğünün yerine getirilmiş olduğu anlamına gelmemektedir. Sicile kayıt ve bildirim yükümlülüğünün yerine getirilmiş olması için VERBİS'e kayıt başvuru formunun Kuruma posta, kargo, kurye veya KEP ile iletilmesi ya da elden teslim edilmesi ve Kurumca onaylanması akabinde başvuru formunda belirtilen elektronik posta adresine iletilen "kullanıcı adı" ve "parola" ile VERBİS ana sayfada yer alan "Veri Sorumlusu Yönetici Giriş" butonu aracılığıyla giriş yaparak bir "irtibat kişisi" atanması, atanan irtibat kişisi tarafından da yine VERBİS ana sayfada yer alan "Sicile Kayıt" butonu aracılığıyla giriş yapılması ve ilgili veri sorumlusu için "bildirim" düzenlenerek sistem üzerinden bildirim onaylanması gerekmektedir.

2. VERBİS; kesintisiz olarak erişim, başvuru ve bildirim düzenlemesine açık olup hâlihazırda sistem üzerinden başvuru yapılabilmesi ve bildirim düzenlenmesi imkânı bulunmaktadır. Bu nedenle eksik başvuru ve bildirimlerin bir an önce tamamlanması önem arz etmektedir. Ayrıca, Yönetmelik'in 13 üncü maddesinde yer alan "Veri sorumluları, Sicilde kayıtlı bilgilerde değişiklik olması halinde

meydana gelen deęişiklikleri, deęişiklięin meydana geldięi tarihten itibaren yedi gn ierisinde VERBİS zerinden Kuruma bildirir.” hkm gereęi VERBİS zerinden giriř yapılarak “bildirim gncellemesi” yapılması mmkndr.

3. VERBİS'e kaydolmak haricinde, Kanun ve ikincil mevzuatta getirilen dięer ykmllkler de bulunmakta olup veri sorumlularının dięer ykmllklere de uyması gerektięi tabiidir.

Kamuoyuna saygıyla duyurulur.

17.12.2021 - Mağazalarda SMS Doğrulaması Duyurusu

Mağazalarda Alışveriş Sırasında İlgili Kişilere SMS ile Doğrulama Kodu Gönderilmesi Suretiyle Kişisel Verilerin İşlenmesine İlişkin Kamuoyu Duyurusu

Yayınlanma Tarihi: 17.12.2021

Kurumumuza intikal eden muhtelif sayıda şikâyet ve ihbarda, mağazalarda gerçekleştirilen alışveriş müteakip kasa işlemleri esnasında ilgili kişilere SMS ile doğrulama kodu gönderildiği ve ödemelerinin tamamlanması ya da bilgilerinin güncellenmesi için gerekli olduğu gerekçesi ile söz konusu kodun kasa görevlisine bildirilmesinin istenildiği, ancak bahse konu işlemin akabinde ilgili kişilere söz konusu mağaza faaliyetleri ile ilgili ticari elektronik ileti gönderildiği iddialarına yer verildiği görülmektedir. Kişisel Verileri Koruma Kurulu tarafından söz konusu şikâyet ve ihbarlara yönelik yapılan incelemelerde ilgili kişilere ödeme işlemleri esnasında doğrulama kodu gönderilen SMS içeriklerinde ya da SMS gönderimi öncesinde veri sorumlusunca herhangi bir aydınlatma yapılmadığı ve/veya söz konusu kodun ödeme işlemlerinin tamamlanması ya da bilgilerinin güncellenmesi için gerekli olduğu gerekçesi ile istenilmesine rağmen veri sorumlusu tarafından bu yolla ticari elektronik ileti gönderimine ilişkin açık rıza alınması suretiyle ilgili kişilerin yanıltıldığı tespit edilmiştir.

Bilindiği üzere, kişisel verilerin işlenmesi 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 5 inci maddesinde düzenlenmiş olup, buna göre Kanunun 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği hükme bağlandıktan sonra (2) numaralı fıkrasında ise ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu işleme şartları sayılmıştır.

Kanunun 3 üncü maddesinde ise açık rıza; “belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza” şeklinde tanımlanmış olup, söz konusu tanımdan açık rızanın taşınması gereken üç unsurunun bulunduğu görülmektedir. Öncelikle, alınan açık rızanın belirli bir konuya ilişkin ve o konu ile sınırlı olması, diğer bir ifade ile veri sorumlusu tarafından açık rıza beyanının hangi konuya ilişkin olarak istenildiğinin açıkça ortaya konulması gerekmektedir. Eğer birden çok kategoriye ilişkin verinin işlenmesine dair açık rıza beyanında bulunulacaksa, açık rızanın hangi verilerin ve ne amaçlarla işleneceği gibi, işlemin farklı noktaları açısından da verilmiş olması zorunluluk arz etmektedir. Öte yandan, açık rıza bir irade beyanı olup, kişinin özgür bir şekilde rıza

gösterebilmesi için neye rıza gösterdiğini de bilmesi, bu anlamda kişinin sadece konu üzerinde değil, aynı zamanda rızasının sonuçları üzerinde de tam bir bilgi sahibi olması gerekmektedir. Son olarak kişinin irade beyanı olan rıza, kişinin yaptığı davranışın bilincinde ve kendi kararı olması halinde geçerlilik kazanacaktır. Kişinin iradesini sakatlayacak her türlü fiil, kişisel verilerin işlenmesi için verdiği açık rızayı da sakatlayacaktır. Cebir, tehdit, hata ve hile gibi iradeyi sakatlayan hallerde, kişinin özgür biçimde karar vermesi mümkün değildir. Dolayısıyla, bu gibi durumlarda bir özgür irade açıklamasından bahsedilemeyecektir. Ayrıca, açık rızanın özgür irade ile açıklanması gerektiğinden, ilgili kişinin açık rızasının alınması, bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının ön şartı olarak ileri sürülmemelidir.

Öte yandan Kanunun 10 uncu maddesi çerçevesinde, kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi tarafından, ilgili kişilere maddede sayılan hususlarda bilgi verilmek suretiyle aydınlatma yükümlülüğünün yerine getirilmesi gerekmektedir. Bu kapsamda, aydınlatma yükümlülüğü gerek açık rıza gerekse de Kanundaki diğer kişisel veri işleme şartlarından bağımsız olarak yerine getirilmesi gereken bir yükümlülüktür. Bununla birlikte, kişisel veri işleme faaliyetinin ilgili kişinin açık rızasına dayanarak gerçekleştirilmesi durumunda, veri sorumlusu tarafından aydınlatma yükümlülüğü ile açık rıza alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir.

Bu kapsamda, Kişisel Verileri Koruma Kurulu tarafından yapılan incelemeler neticesinde;

- Kişilerin telefonuna gönderilecek olan SMS'in amacının ne olduğu ve bu SMS ile iletilen kodun verilmesi halinde ne gibi sonuçlar doğuracağı hususunun, katmanlı aydınlatmanın bir gereği olarak ilk aşamada veri sorumlusunun mağazalarda yetkilendirdiği kişiler tarafından ilgili kişilere açık ve anlaşılır bir biçimde aktarılması, ayrıca aydınlatma yükümlülüğünün yerine getirilebilmesini teminen yine söz konusu SMS içeriklerinde de gerekli kanalların sağlanması,
- Mağazalarda gerçekleştirilen alışverişler ile ilgili ödeme esnasında ilgili kişilere SMS ile doğrulama kodu gönderilerek üyelik sözleşmesi, kişisel verileri işleme izni, ticari elektronik ileti onayı vb. birbirinden farklı işleme faaliyetlerinin tek bir eylemle gerçekleştirilmesine yönelik uygulamalara son verilmesi, söz konusu işleme faaliyetlerine yönelik seçenek sunulmak suretiyle ayrı ayrı açık rıza alınması,
- Bunun yanı sıra, veri sorumlularınca açık rıza alınması ve aydınlatma yükümlülüğü işlemlerinin birlikte gerçekleşmesine neden olabilecek durumlardan kaçınılması,

- Ticari elektronik ileti gönderimi için açık rıza alınmasını teminen SMS doğrulama kodu gönderilmesine yönelik bir uygulamaya gidilmesi halinde ise söz konusu işlemde alınacak açık rızanın tüm unsurları kapsamı

önem arz etmektedir.

Kamuoyuna saygıyla duyurulur.

10.12.2021 - Veri Koruma Görevlisi Hakkında Kamuoyu Duyurusu

Veri Koruma Görevlisi Hakkında Kamuoyu Duyurusu

Yayınlanma Tarihi: 10.12.2021

06.12.2021 tarih ve 31681 sayılı Resmi Gazete'de yayınlanarak yürürlüğe giren Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğde ve Veri Koruma Görevlisi Belgelendirme Programında yer alan şartları haiz olan ve yapılacak sınav sonucunda başarılı olan kişilerin Veri Koruma Görevlisi (VKG) Sertifikası almaya hak kazanacağı belirtilmiştir.

Gönüllülük esasına dayalı olan sertifikasyon mekanizmasını düzenleyen Tebliğin 6 ncı maddesinin 2 nci fıkrasında veri koruma görevlisinin sertifikalandırıldıkları program kapsamında kişisel verilerin korunması mevzuatı açısından yeterli bilgiye sahip olduğunun kabul edileceği açıkça belirtilmekte olup, bu kişilere herhangi bir yetki verilmediği gibi bir görev tanımı da yapılmamıştır.

Tebliğ kapsamında kazanılacak olan bu unvanın kamuoyunda Avrupa Birliği Genel Veri Koruma Tüzüğünde bahsi geçen ve Tüzükte görev, yetki ve sorumlulukları tanımlanan Data Protection Officer (DPO) ile karıştırıldığı görülmüştür.

Avrupa Birliği Genel Veri Koruma Tüzüğünde geçmekte olan ancak ulusal mevzuatımızda yer almayan DPO ile Tebliğ uyarınca VKG Sertifikası verilecek kişi birbirinden farklılık arz etmektedir.

Sertifikasyon sürecinin yürütülmesine ilişkin diğer hususlar ayrıca duyurulacaktır.

Kamuoyuna saygıyla duyurulur.

07.12.2021 - Sertifikasyon Duyurusu

Sertifikasyon Duyurusu

Yayınlanma Tarihi: 07.12.2021

Kurumumuz tarafından Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğ kapsamında yapılacak olan sertifikasyon faaliyetine ilişkin olarak Veri Koruma Görevlisi Belgelendirme Programı hazırlanmıştır. 25.11.2021 tarihli ve 2021/1178 sayılı Kişisel Verileri Koruma Kurulu Kararı ile Veri Koruma Görevlisi Belgelendirme Programı'nın yürürlüğe konulmasına ve Kurumumuzun internet sayfasında yayımlanmasına oy birliği ile karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

VERİ KORUMA GÖREVLİSİ BELGELENDİRME PROGRAMI

1. AMAÇ

Bu programın amacı, 06/12/2021 tarihli ve 31681 sayılı Resmî Gazete’de yayımlanan Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğ kapsamında belgelendirilmek üzere TS EN ISO/IEC 17024 standardına göre akredite edilmiş ve Kurum tarafından yetkilendirilmiş Personel Belgelendirme Kuruluşu’na müracaat eden adayların başvurularının değerlendirilmesi, sınavların yapılması ve değerlendirilmesi, Veri Koruma Görevlisi veya Veri Koruma Görevlisi adayının belgelendirilmesi veya yeniden belgelendirilmesi ve belgelendirme yöntemi ile ilgili bütün esasların belirlenmesidir.

2. KAPSAM

Bu program, Personel Sertifikasyon Mekanizmasına İlişkin Usul ve Esaslar Hakkında Tebliğ çerçevesinde yapılacak belgelendirme faaliyetlerini kapsar.

3. TANIMLAR

Aday: Veri Koruma Görevlisi veya Veri Koruma Görevlisi adayını,

Akreditasyon: Türk Akreditasyon Kurumu tarafından; belgelendirme, doğrulama, yeterlilik testi sağlama ile diğer uygunluk değerlendirme kuruluşlarının ulusal ve uluslararası kabul görmüş teknik kriterlere göre değerlendirilmesini, yeterliğinin onaylanmasını ve düzenli aralıklarla denetlenmesini,

Değerlendirici/Sınav Yapıcı: Bu programda yer alan ölçütleri karşılayan ve Personel Belgelendirme Kuruluşu tarafından adayların teorik bilgi düzeylerini programda tanımlanan şartlar doğrultusunda ölçmek ve değerlendirmek üzere görevlendirilen kişiyi,

Gözetmen: Gerçekleştirilen sınavları kamera kaydına almak ve sınav düzenini sağlamak üzere Personel Belgelendirme Kuruluşu tarafından görevlendirilen, değerlendirici ölçütleri aranmayan, kuruluştaki tam ya da kısmi zamanlı çalıştırılan ve görev tanımına uygun olarak eğitilmiş personeli,

Kanun: 24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununu,

Katılım Belgesi: Kişisel Verileri Koruma Kurulu tarafından usul ve esasları belirlenen temel eğitim sürecini tamamlayanlara Kurum tarafından verilen belgeyi,

Kurul: Kişisel Verileri Koruma Kurulunu,

Kurum: Kişisel Verileri Koruma Kurumunu,

Personel Belgelendirme Kuruluşları: Türk Akreditasyon Kurumu tarafından (TS) EN ISO/IEC 17024 standardı kapsamında akredite edilen, sertifikasyona ilişkin ilgili sınavlarda başarılı olanları belgelendirmeye yetkili kuruluşları,

Program: Kurul tarafından ana hatları belirlenerek yayımlanan Veri Koruma Görevlisi'nin sertifikasyon faaliyetlerine ilişkin şartların belirlendiği dokümanı,

Sertifikasyon: Kanun ve ilgili mevzuat çerçevesinde, sertifika almak için gereken şartları taşıyan ve sınavda başarılı olanların belgelendirilmesi işlemi,

Sınav: Adayların bilgi, beceri ve yetkinliklerinin değerlendirilmesi amacıyla Personel Belgelendirme Kuruluşları tarafından belgelendirme programına ve akreditasyon kurallarına göre gerçekleştirilen değerlendirme sürecini,

TS EN ISO/IEC 17024: Uluslararası Standardizasyon Teşkilatı tarafından kabul edilen "Uygunluk Değerlendirmesi - Personel Belgelendirmesi Yapan Kuruluşlar için Genel Şartlar" standardını,

Veri Koruma Görevlisi (VKG): Sınavda başarılı olarak Veri Koruma Görevlisi unvanını kullanmaya hak kazanan gerçek kişiyi ifade eder.

4. İŞ VE GÖREV TANIMI

Katılım belgesine sahip kişilerden sınavda başarılı olanlar Veri Koruma Görevlisi sertifikası almaya hak kazanırlar.

Veri Koruma Görevlilerinin sertifikalandırıldıkları işbu program kapsamında kişisel verilerin korunması mevzuatı açısından yeterli bilgiye sahip olduğu kabul edilir.

5. YETERLİLİK ŞARTLARI

Sınav tarihinden önceki son 4 yıl içerisinde Katılım Belgesi almış olanlar veya başvuru tarihinde geçerli bir Veri Koruma Görevlisi Sertifikasına sahip olanlar sınava başvurabilirler.

Sınavda başarılı olanlar ise Veri Koruma Görevlisi olmaya hak kazanırlar.

6. BELGELENDİRME

6.1. BELGE DÜZENLEME

Sınavda başarılı olan adaylara Personel Belgelendirme Kuruluşu tarafından Kurumun şekil şartlarına uygun şekilde Veri Koruma Görevlisi Sertifikası düzenlenir.

6.2. ÜCRETLER

Tebliğ’de belirtildiği üzere, bu program kapsamında takvim yılı başında Kurumun internet sitesinden yayınlanan Kurul tarafından belirlenmiş ücret tarifeleri geçerlidir.

6.3. BELGE SÜRESİ

Veri Koruma Görevlisi Sertifikasının geçerlilik süresi sınav sonuçlarının ilanından itibaren 4 yıldır. Süre sonunda yeniden belgelendirme süreci mevcut programa ve yönetime göre baştan yapılır.

6.4. BELGENİN ASKIYA ALINMASI VE/VEYA İPTALİ

Veri Koruma Görevlisi Sertifikası sahibi olan Veri Koruma Görevlisinin,

- Veri Koruma Görevlisinin kendi talebiyle,
- Gerekli koşullardan herhangi birini taşımadığı halde, gerçeğe aykırı beyanda bulunduğu tespit edilmesi halinde,
- Belgeyi kötü amaçla veya yanıltıcı bir biçimde kullandığının tespiti halinde,
- Veri Koruma Görevlisi hakkında bildirilen şikâyetin değerlendirilmesi sonrasında Kurum veya ilgili mahkemelerce aleyhinde bir karar alındığında,
- Belge üzerinde oynandığının tespiti durumunda,

Personel Belgelendirme Kuruluşu tarafından Veri Koruma Görevlisi Sertifikası askıya alınır ve/veya iptal edilir.

6.5. ÖĞRENME ÇIKTILARI

6.5.1. Kanunun amacını ve kapsamı bilir.

6.5.2. Kanunda yer alan temel kavramlara hâkimdir.

6.5.3. Kanunda yer alan genel/temel ilkeler ile kişisel veri işleme şartlarına hâkimdir.

6.5.4. Kişisel verilerin korunması alanında uluslararası mevzuatı bilir.

6.5.5. Silme, yok etme ve anonim hale getirme kavramlarının neler olduğunu ve hangi durumlarda uygulanması gerektiğini bilir.

6.5.6. Kişisel verilerin yurt içinde ve yurt dışına aktarım konusuna hâkimdir.

6.5.7. Aydınlatma yükümlülüğüne dair bilgi sahibidir.

6.5.8. İlgili kişinin hakları, veri sorumlusuna başvuru ve Kurula şikâyet konularına hâkimdir.

6.5.9. Veri güvenliğine ilişkin teknik ve idari tedbirler ve veri ihlal bildirim süreçleri

hakkında neler yapılması gerektiğini bilir.

6.5.10. Veri Sorumluları Siciline Kayıt noktasında bilgi sahibidir.

6.5.11. Yaptırımlar, Kurumun yapısı, Kurul, tam ve kısmi istisnalar hakkında bilgi sahibidir.

7. SINAV

7.1. SINAV İLANI

Personel Belgelendirme Kuruluşlarınca yapılacak olan sınavlar, en geç sınavdan 15 gün önce akredite edilmiş Personel Belgelendirme Kuruluşu tarafından ilan edilmelidir.

7.2. BAŞVURU

Veri Koruma Görevlisi Sertifika sınavına, yurt içindeki üniversitelerin veya diploma denkliği Yükseköğretim Kurulu tarafından onaylanmış olmak kaydıyla yabancı üniversitelerin, en az dört yıllık lisans eğitimi veren fakültelerinden mezun olanlardan sınav tarihinden önceki son 4 yıl içerisinde Katılım Belgesi almış olan veya geçerli bir Veri Koruma Görevlisi Sertifikasına sahip olanlar başvuru yapabilir.

7.3. TEORİK SINAV

7.3.1. . Teorik sınav, Personel Belgelendirme Kuruluşu tarafından yapılır. Aday, 80 adet sorudan oluşan Teorik sınava tabi tutulur. Sınav dili Türkçedir.

Kitapçıkların 12 Punto'dan küçük olmamak kaydıyla Times New Roman yazı fontunda oluşturulmuş olması, aynı oturumda yer alan adayların aynı soru setine tabi tutulması ve soru kitapçıklarının gruplandırılması esastır.

Adaylar cevaplarını kurşun kalemle işaretlemelidir. Aday tarafından kullanılan soru kitapçığında ve cevap kâğıdında aday kimlik numarası, adı, soyadı ve imzası bulunmalıdır.

Sınava ilişkin puanlama sonucu ve puanlamayı yapan kişinin adı-soyadı, imzası ve tarihi cevap kâğıdı üzerine tükenmez kalemle kayıt edilmiş olmalıdır.

Sınav sonuçlarının optik okuyucular tarafından gerçekleştiriliyor olması durumunda optik sistemin doğru bir şekilde cevap kâğıtlarını okuduğunu kontrol eden kişinin adı-soyadı ve imzası bulunmalıdır.

Adaylar sınav süresince birbirleri ile konuşamaz, birbirlerinden sınav gereci veya yardım isteyemez.

Değerlendiriciler veya gözetmenler kopya çekmeye veya vermeye kalkışanları uyarmak zorunda değildir, sorumluluk adaylara aittir. Sınav sırasında kopya çektiği veya kopya verdiği tespit edilen adayların kimlik bilgileri ve yaşanan durum tutanak ile kayıt altına alınır ve bu adaylar sınavdan başarısız sayılır.

Sınav soru kitapçığında kitapçık türü (örn. A Kitapçığı), soru sayısı, program adı, revizyon numarası ve sınav süresi belirtilmelidir.

Sınav bitiminde adayların cevap kâğıtları ve kitapçıkları uygun şekilde teslim alınarak güvenliği sağlanır. (Kapalı zarf vb. yöntem)

7.3.2. Yetkilendirilmiş Personel Belgelendirme Kuruluşlarının sınav ve belgelendirme süreçlerini tarafsız, adil, geçerli ve güvenilir bir şekilde yürüttüğünün kontrolünü sağlamak amacıyla, sınav esnasında adayların görebileceği şekilde Kanun gereği adaylara aydınlatma yapılmak suretiyle sınav salonuna kamera yerleştirilir. Sınavda ses ve görüntü kaydı sınav başlangıcından son adayın sınavının bitimine kadar devam ettirilmelidir. Sınav kâğıtlarının dağıtıldığı, kimlik kontrolünün ve imzalı sınav yoklamasının yapıldığı, sınav kâğıtlarının değerlendiricilere veya gözetmenlere teslim edildiği ve sınavın sonlandırıldığı kayıt altına alınmalıdır. Sınavlarda kamera, tüm adayların, değerlendirici veya gözetmenlerin net bir şekilde görüntülenmesini sağlayacak uygun bir yere konumlandırılmalıdır.

Söz konusu kayıtlar, Personel Belgelendirme Kuruluşu tarafından sınavın gerçekleştirildiği tarihten itibaren sınava itiraz süresi içerisinde ve sınava itiraz edildiği takdirde Kurum tarafından gerçekleştirilecek incelemenin sonucu kesinleşinceye kadar saklanır ve Kurum tarafından talep edildiği takdirde bir örneği Kuruma teslim edilir. Kayda alınan görüntüler Kurum, yargı organları ve mevzuatın yükümlü kıldığı taraflar hariç, hiçbir kişi, kurum ve kuruluşla paylaşamaz.

Sınav başlangıcında değerlendirici veya gözetmen tarafından, adaylara sınav ile ilgili kapsamlı açıklama yapılmalıdır. Değerlendirici ve gözetmen;

- Sınavın yapıldığı sınav merkezi ve sınavın yapıldığı tarih hakkında bilgi vermelidir.
- Programın ismini açıklamalıdır.
- Kendilerini tanıtmalıdır.
- Katılan aday sayısı hakkında bilgi vermelidir.

□ Sınavda uyulması gereken kurallar hakkında bilgi vermelidir. (Örneğin cep telefonlarının kapalı şekilde uzakta tutulması, sınav esnasında yardımlaşmama ve birbirleriyle iletişime geçmeme, kopya çekmeme, vb.)

Belirtilen hususlara ilişkin uygunsuzluk tespit edilmesi halinde bu durum tutanakla kayıt altına alınır. Kurumun gerekli görmesi halinde belgelendirme kuruluşuna denetim düzenlenir.

7.3.3. Sınav 100 puan üzerinden değerlendirilir, her soru beş (5) seçenekli, çoktan seçmeli ve 1,25 puan ağırlığına sahiptir. Bu sınavda boş bırakılan veya yanlış cevaplandırılmış sorulardan herhangi bir puan indirimi yapılmaz. Sınav soruları Sınav Konuları listesindeki ilgili tüm bilgi ifadelerini ölçmelidir. Sınavdan 70 puan veya üzerinde puan alınması ve her bölümdeki soruların en az %60'ının doğru cevaplanması durumunda aday başarılı olarak kabul edilir.

7.3.4. Sınav sonuçları akredite edilmiş Personel Belgelendirme Kuruluşları tarafından akreditasyon ve program kuralları çerçevesinde değerlendirilir. Sınav sonuçları sınavdan sonra 1 ay içinde Personel Belgelendirme Kuruluşunun resmi internet adresinde Kanuna uygun bir şekilde ilan edilir ve SERTABİS'e aktarılır.

7.3.5. Teorik sınav soruları ve puanlarının konulara göre dağılımı ile asgari geçme kuralları şu şekilde tanımlanmıştır:

	TEORİK SINAV KONULARI	SORU DAĞILIMI %	SORU SAYISI
En az 14 doğru olmalı	I.BÖLÜM (%30)		
	1. Kanunun Kapsamı ve Amacı	4	3
	2. Temel Kavramlar	6	5
		Kişisel Veri	
		Kişisel Verilerin İşlenmesi	
		Veri Sorumlusu / Veri İşleyen	
		Kişisel Veri - Özel Nitelikli Kişisel Veri	
		Açık Rıza	
	3. Genel / Temel İlkeler	5	4
	4. Kişisel Veri İşleme Şartları	10	8

		Açık Rıza Metinleri		
	5. Kişisel verilerin korunması alanında uluslararası mevzuatı (108 sayılı sözleşme, 95/46/EC Direktif, GDPR)		5	4
		Uluslararası Kuruluşlar		
En az 22 doğru olmalı	II.BÖLÜM (%45)			
	6. Kişisel Verilerin Yurtiçinde Aktarılması		1	1
	7. Kişisel Verilerin Yurtdışına Aktarılması		4	3
		Standart Sözleşmeler		
		Bağlayıcı Şirket Kuralları		
	8. Aydınlatma Yükümlülüğü		10	8
		Usul ve Esaslar		
		Aydınlatmada Kullanılan Yöntemler		
		Aydınlatma Metinleri		
		Veri İşleme / Gizlilik Politikası		
		Çalışanlarla Gizlilik Sözleşmesi		
		Veri İşleyenle Gizlilik Sözleşmesi		
		Üçüncü Kişilerle Gizlilik Sözleşmesi		
	9. İlgili Kişi Hakları		3	2
	10. Veri Sorumlusuna Başvuru		6	5
	11. Kurula Şikâyet		6	5
	12. Kurumun Yapısı ve Kurul		6	5
		Tarihçe		
		Kurumun Teşkilat Yapısı		
		Yönetmelikler		
		İlke Kararları		
	13. Yaptırımlar		3	2

		Suçlar		
		Kabahatler		
	14. Tam ve Kısmi İstisnalar		6	5
En az 12 doğru olmalı	III. BÖLÜM (%25)			
	15. Veri Güvenliği Tedbirleri/Teknik ve İdari Tedbirler		11	9
		Veri Güvenliğine İlişkin İdari Tedbirler		
		Veri Güvenliğine İlişkin Teknik Tedbirler		
		Yeterli Önlemler		
		Kişisel Veri İşleme Envanteri		
		Kişisel Veri Saklama ve İmha Politikası		
	16. Veri İhlal Bildirimi Süreçleri		4	3
	17. Silme, Yok Etme, Anonim Hale Getirme		6	5
		Periyodik İmha / Saklama Süreleri		
	18. Veri Sorumluları Siciline Kayıt		4	3
	TOPLAM			80 soru

7.4. TEORİK SINAV YERİ VE DÜZENİ

Sınavlar sınıf düzenine sahip akredite edilmiş ortamlarda gerçekleştirilir. Teorik sınava katılım sağlayan adaylar sınav salonunda tek sıra oturma düzeni içerisinde yerleştirilir. Adaylar arasında adayların kopya çekmelerini engelleyecek şekilde en az 1 metre boşluk bırakılır. Paravan vb. şekillerde bölünmüş sınav alanlarının kullanıldığı sınavlarda söz konusu koşul aranmaz. Teorik sınav, sınav süresi boyunca görevlendirilen değerlendiriciler ve sınav gözetmenlerinin kontrolü altında yapılır.

7.5. SORU BANKASI

Teorik sınava ilişkin soru bankası, Personel Belgelendirme Kuruluşu tarafından hazırlanır ve Kurum tarafından talep edildiği takdirde elektronik ortamda ve yazılı olarak Kurum ile paylaşılır.

Soru Bankası analizi her sene en az 1 defa sınav sıklığına göre artacak şekilde Personel Belgelendirme Kuruluşu tarafından yapılır ve soruların doğruluğu, kullanılabilirliği, zorluk seviyeleri kontrol edilir. Her sene en az 1 defa soru bankalarında yer alan soru setleri yenilenir.

Personel Belgelendirme Kuruluşu tarafından hazırlanan sorular zorluklarına göre sınıflandırılmalı her soru setinde %30 kolay, %40 orta ve %30 zor güçlük seviyelerinde sorular yer alması sağlanmalıdır.

7.6. TEORİK SINAV SÜRESİ

Teorik sınav süresi 120 dakikadır.

7.7. SINAV GÖREVLİLERİ İLE İLGİLİ ŞARTLAR

Programda aksi belirtilmedikçe, aday sayısının 36'nın altında olduğu teorik sınavlar için (36 dâhil) birer değerlendirici ve gözetmen görevlendirilmesi yeterlidir. Tek seferde sınava alınacak aday sayısının 36'dan fazla 72'den az olduğu durumlarda (72 dâhil) değerlendirici ve gözetmene ilave olarak bir değerlendirici veya gözetmen görevlendirilmesi gerekmektedir. Aday sayısının 72'den fazla olduğu durumlarda ise her 36 adaya bir değerlendirici veya gözetmen olacak şekilde sayı artırılır. Her halükarda teorik sınavlarda en az bir değerlendirici ve bir gözetmen bulunmalıdır.

Değerlendiricilerin; Yükseköğretim kurumlarında öğretim elemanı olarak görev yapıyor olması ve bunu belgeliyebilmeleri gerekmektedir.

Yukarıdaki özelliklere sahip olan ve ölçme ve değerlendirme sürecinde görev alacak değerlendiricilere; Personel Belgelendirme Kuruluşları tarafından kişinin görev alacağı program ve ölçme-değerlendirmede kalite güvencesi konularında eğitim sağlanmalıdır.

7.8. SINAV MATERYALLERİ

Teorik sınav materyalleri aşağıdakilerden oluşur:

- Sınav Soru Kitapçığı.
- Sınav Cevap Kâğıdı.
- Sınav Yoklama Formu.
- Sınav Tutanak Formu.
- Değerlendirici Sonuç Raporu.
- Kurşun kalem, silgi ve kalem tıraş.
- Personel Belgelendirme Kuruluşu tarafından hazırlanan sınav yönergesi.

- Belgelendirme Karar Formu

7.9. SINAV SONUÇLARINA İTİRAZ

Aday, sınav sonuçlarına itirazları, itiraz gerekçelerini de yazmak koşuluyla 30 gün içerisinde akredite edilmiş Personel Belgelendirme Kuruluşuna yapacaktır. Personel Belgelendirme Kuruluşu ise, söz konusu itirazı 30 gün içerisinde sonuçlandırarak başvuran kişiye cevap verir.

05.11.2021 - Belediyeler Duyurusu

Kamuoyu Duyurusu (Belediyeler)

Yayınlanma Tarihi: 05.11.2021

Kurumumuza iletilen çeşitli ihbarlarda belediyelerin internet üzerinden emlak vergisi veya beyan bilgisini sorgulama sayfalarında yalnızca TC kimlik numarası girilerek vatandaşın emlak bilgilerine ulaşılmasının kişisel verilerin korunması açısından sorun teşkil ettiği ifade edilmiş, konunun 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında incelenmesi talep edilmiştir.

Söz konusu talepler kapsamında Kişisel Verileri Koruma Kurulu (Kurul) tarafından alınan **25/02/2021 tarih ve 2021/140 sayılı Karar ile** "...bazı belediyeler tarafından internet üzerinden verilen vergi ödeme hizmetlerinin üyelik ve şifre ya da çift doğrulama yolu ile sisteme giriş yapılması sureti ile gerçekleştirildiği ve bu uygulamaların Kanuna uygun olduğu, ancak bazı belediyeler tarafından sunulan hızlı sorgulama ya da borç ödeme uygulamalarında sadece tek bir bilgi girilerek kişilerin borç bilgisine ulaşılabilirdiği; her ne kadar kişiye ait isim ya da mülke ilişkin bilgilere erişim mümkün olmasa da borca ilişkin bilgiye erişim sağlanabildiği anlaşılmış olup, bu durumun Kanununun 12 nci maddesinin 1 numaralı fıkrasının (b) bendinde yer alan kişisel verilere hukuka aykırı olarak erişilmesini önlemek hükmüne aykırı olduğu değerlendirilmekte birlikte bahse konu uygulamalara ilişkin olarak belirli bir belediye hakkında Kurumumuza iletilmiş herhangi bir şikayet bulunmadığı dikkate alındığında bir hak mahrumiyetinin oluşmadığı, ancak Kanuna aykırı uygulamaların devam ediyor olması nedeniyle konu hakkında Çevre ve Şehircilik Bakanlığına ve Türkiye Belediyeler Birliğine bilgi verilmesine

- Diğer taraftan Belediyelerce sunulan söz konusu uygulamaların yeniden düzenlenmesi hususunda Belediyelere 3 (üç) ay süre verilmesine ve Kanununun 18 inci maddesinde yer alan yaptırımlara ilişkin hükümlerin Belediyelere hatırlatılmasına..."

karar verilmiştir. İlgili Karar kapsamında 09.04.2021 tarih ve 52863 sayılı yazımız ile tüm büyükşehir belediyelerine, il belediyelerine, ilçe belediyelerine ve belde belediyelerine "söz konusu uygulamaları yürüten belediyelerin bu yazı tarihinden itibaren 3 ay içerisinde bu uygulamaları sonlandırmaları ve Kanuna aykırı veri işleme faaliyetlerini durdurmalarına" karar verildiği, "Kanuna aykırı veri işleme faaliyetini sürdüren Belediyeler hakkında Kanununun 18 inci maddesi kapsamında idari işlem uygulanacağı" hususları iletilmiştir.

Bilindiği üzere, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) kapsamında kişisel verilere gerekmesi halinde uzaktan erişim için iki kademeli kimlik doğrulama kontrolünün uygulanması önerilmektedir. Bu kapsamda başkalarının kolayca ulaşabileceği örneğin kişinin TC kimlik numarası ve doğum günü bilgisinin sorgulanarak erişim imkânı veren sistemler tek kademeli doğrulama olarak kabul edilirken, kişinin TC kimlik numarasının yanı sıra kişiye özel oluşturulmuş şifre ya da kişinin daha önce bildirmiş olduğu telefon numarasına iletilen SMS kodu ile erişim sağlanan sistemler iki kademeli doğrulama olarak kabul edilmektedir. Bu çerçevede 1398 adet büyükşehir belediyesi ile bağlı ilçeleri, il belediyeleri ile bağlı ilçe ve belde belediyelerinin internet siteleri üzerinden verdikleri emlak vergisi borç sorgulama ve ödeme-hızlı ödeme sistemlerinde yapılan incelemede çift faktörlü doğrulamaya bakılırken ilk doğrulamanın TC kimlik no, ad soyad, vergi no gibi verilerle yapılırken ikincil düzeydeki doğrulamanın kişiye özel oluşturulmuş üyelik, SMS ya da e-postaya iletilen şifre gibi bir sistemle gerçekleştirilip gerçekleştirilmediği, ikincil düzeyde kişiye ait başkalarının da erişebileceği telefon no, doğum tarihi, anne baba adı gibi bilgiler yerine sadece kişiye özel olarak belirlenecek ve sadece ilgili kişinin erişebileceği verilerin istendiği sistemlerin varlığı incelenmiştir.

Kurulun 25.02.2021 tarih ve 2021/140 sayılı Kararı ile belirlenen 3 aylık sürenin dolmasını müteakip yapılan inceleme neticesinde Kurulun 21.10.2021 tarih ve 1077 sayılı Kararı ile Belediyelere iletilen yazılar uyarınca bazı belediyelerin gerekli değişiklikleri yaptığı, ancak birçok Belediyenin ilgili Karar çerçevesinde gerekli güvenlik tedbirlerini almadığı ve halihazırda emlak vergisi borç sorgulama ve ödeme hizmetleri sunumunda “tek faktörlü doğrulama” uyguladığı tespit edilmiş olup, Kanununun 12 nci maddesinin 1 numaralı fıkrasının (b) bendinde yer alan kişisel verilere hukuka aykırı olarak erişilmesini önlemek hükmüne aykırı uygulamalara devam ettiği anlaşılan belediyeler ile ilgili olarak 25.02.2021 tarih ve 2021/140 sayılı Kurul Kararının gereğinin yerine getirilmediği değerlendirilmesinden hareketle bahse konu aykırılığa sebebiyet verenler hakkında Kanununun 18 inci maddesinin (3) numaralı fıkrası kapsamında disiplin hükümlerine göre işlem yapılması ve sonucundan Kurula bilgi verilmesi hususunda ilgili belediyelerin talimatlandırılmasına karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

28.09.2021 - Covid-19 PCR Test Sonucu ve Aşı Bilgisi Uygulamaları

Covid-19 PCR Test Sonucu ve Aşı Bilgisi Uygulamalarına İlişkin Kamuoyu Duyurusu

Yayınlanma Tarihi: 28.09.2021

Kurumumuza gerek yazılı olarak gerek ALO 198 çağrı hattı vasıtasıyla intikal eden PCR testi ve/veya aşı bilgisi taleplerine ilişkin 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) çerçevesinde nasıl bir yol izlenmesi gerektiğine ilişkin olarak Kurumumuz görüşlerinin talep edilmesi üzerine, konunun ülke genelinde gerçekleştirilecek yaygın bir uygulamaya inhisar edeceği dikkate alınarak, Kanun kapsamında bir değerlendirme yapılmasını teminen Kişisel Verileri Koruma Kurulu'nun gündemine alınmasına karar verilmiş ve Kurul'un 28/09/2021 tarihli ve 2021/980 sayılı Kararı ile aşağıda yer verilen değerlendirmenin Kurum resmi internet sitesinde yayınlanmasına karar verilmiştir.

Dünya genelinde çeşitli varyantlarının da etkisiyle yayılma hızı giderek artış gösteren Covid-19 virüsünün neden olduğu hastalıklardan korunmak adına, değişen koşulları da dikkate almak suretiyle ülkemizin de aralarında bulunduğu tüm devletler, çeşitli tedbirler almaya devam etmekte olup; karantina, sosyal mesafe ve sosyal izolasyon gibi temel tedbirlerin alınmasının yanı sıra, yapılan bilimsel çalışmalar neticesinde Covid-19 aşuları geliştirilerek kullanıma sunulmuştur. Covid-19 aşısının, koronavirüsün yayılımını önlediği, hastalığın etkilerini de önemli ölçüde azalttığı bilinmekte olup; bu bilimsel gerçeklikten hareketle devletler, kamu sağlığının korunmasını teminen işyerleri de dâhil olmak üzere toplu halde bulunulacak alanlarda, Covid-19 aşı bilgisi ve/veya PCR testi sonuçlarının işlenmesi zorunluluğu getirmektedirler.

Nitekim ülkemizde de İçişleri Bakanlığınca 81 İl Valiliğine gereği, ilgili Bakanlıklara da bilgi için gönderilen 20.08.2021 tarihli yazıda; salgının toplum sağlığı ve kamu düzeni açısından oluşturduğu riskin asgari seviyeye düşürülmesi için konser, sinema, tiyatro ve toplu ulaşım araçları gibi insanların toplu olarak bulunduğu faaliyetlere katılım sağlamak isteyen kişilere Covid-19 aşı bilgisi ve/veya negatif sonuçlu PCR test bilgisinin bildirilmesi zorunluluğu getirilmiştir.

Çalışma ve Sosyal Güvenlik Bakanlığının 81 İl Valiliğine gereği için, ilgili Bakanlıklara da bilgi için gönderdiği 02.09.2021 tarihli yazıda ise işyerlerinde karşılaşılabilecek sağlık ve güvenlik risklerine yönelik koruyucu ve önleyici tedbirler kapsamında; Covid-19 aşısı olmayan işçilerden zorunlu olarak

haftada bir kez PCR testi yaptırmalarının işyeri/işveren tarafından istenebileceği ve test sonuçlarının gerekli işlemler yapılmak üzere kayıt altında tutulacağı ifade edilmiştir.

Öncelikle belirtmek gerekir ki; kişilerin tahlil, görüntüleme, test, rapor, aşı durumu gibi sağlık durumlarına ilişkin bilgileri Kanunun 6 ncı maddesine göre kişisel sağlık verisi niteliğini haiz olup, özel nitelikli kişisel veri kategorisinde bulunmaktadır. Bu sebeple, söz konusu bilgilerin Kanunun 6 ncı maddesinde yer verilen işleme şartlarına uygun olarak işlenmesi gerekmektedir.

Öte yandan, Covid-19 salgınının dünya çapındaki gerek sağlık, gerek sosyal hayat gerek ekonomi üzerindeki etkileri dikkate alındığında, bu salgınla mücadele kapsamında aşı durumu ve PCR test sonucu gibi Covid-19'a ilişkin kişisel sağlık verilerinin; kamu sağlığının, kamu güvenliğinin ve kamu düzeninin korunması amacıyla işlenmesi gerekliliğinin ortaya çıkması kaçınılmazdır.

Bilindiği üzere Kanunun 28 inci maddesinin birinci fıkrasının (ç) bendinde, *“Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi”* halinde Kanun hükümlerinin uygulanmayacağı düzenlenmiştir.

Bu noktadan hareketle salgın hastalık gibi kamu güvenliği ve kamu düzenini tehdit eden durumlarda bu tehdidi ortadan kaldırabilmek amacıyla salgın hastalığın bulaşıcılığının önüne geçilebilmesini teminen kanunla yetki verilmiş kamu kurum ve kuruluşlarınca yürütülen faaliyetler kapsamında kişisel verilerin işlenmesinin de Kanunun 28 inci maddesinin birinci fıkrasının (ç) bendi kapsamında değerlendirilmesi gerektiği düşünülmektedir.

Bu kapsamda Covid-19'un sebebiyet verdiği salgın hastalığın kamu güvenliği ve kamu düzenini tehdit etmesi sebebiyle hastalığın yayılımını engellemek amacıyla Covid-19 aşı bilgisi ve/veya negatif sonuçlu PCR test bilgisinin anılan madde hükmü kapsamına giren kamu kurum ve kuruluşlarınca yürütülen önleyici ve koruyucu faaliyetler kapsamında işlenmesinin önünde bir engel bulunmadığı, dolayısıyla söz konusu kişisel veri işleme faaliyetlerinin Kanunun 28 inci maddesinin birinci fıkrasının (ç) bendi kapsamında gerçekleştirilebileceği, bununla birlikte, Covid-19 salgını kapsamında yürütülen kamu güvenliğini ve kamu düzenini koruma amacına yönelik faaliyetler dışında kalan ya da bu amacı aşan nitelikteki kişisel veri işleme faaliyetlerinin Kanun kapsamında yer alacağı değerlendirilmektedir.

Kamuoyuna saygıyla duyurulur.

03.09.2021 - WhatsApp (3)

WHATSAPP UYGULAMASI HAKKINDA YÜRÜTÜLEN RESEN İNCELEMeye İLİŞKİN KAMUOYU DUYURUSU

Yayınlanma Tarihi: 03.09.2021

WhatsApp LLC (WhatsApp/veri sorumlusu) tarafından, WhatsApp uygulamasını kullanmak isteyen kullanıcıların kişisel verilerinin işlenmesine ve yurtdışında bulunan üçüncü taraflara aktarılmasına açık rıza verilmesini içerecek şekilde Hizmet Koşullarının ve Gizlilik İlkesinin güncellendiği, bu kapsamda açık rıza vermeyen kullanıcıların uygulamayı kullanamayacağına ve hesaplarının silineceğine dair bilgilendirme iletildiği tespit edilmiştir.

Kişisel Verileri Koruma Kurulunun 12.01.2021 tarihli ve 2021/28 sayılı Kararı ile 09.02.2021 tarihli ve 2021/120 sayılı Kararı çerçevesinde, yurtdışına veri aktarımı, hizmetin açık rıza şartına bağlanması ve genel ilkelere uygunluk hususları başta olmak üzere WhatsApp hakkında 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 15'inci maddesinin (1) numaralı fıkrası kapsamında resen inceleme başlatılmasına karar verilmiş ve konuya ilişkin WhatsApp'tan alınan savunma yazıları ve bununla bağlantılı olarak WhatsApp Hizmet Koşullarının ve Gizlilik İlkesi metinlerinin incelenmesi neticesinde; temel olarak veri sorumlusu tarafından kullanıcılara sunulan Hizmet Koşullarının kullanıcı ile yapılan bir sözleşme olarak tanımlandığı, Gizlilik İlkesinin ise şeffaflığı sağlamaya yönelik bir metin olarak, hangi verilerin hangi amaçlarla işleneceğini göstermekle birlikte esasen Hizmet Koşullarının bir parçası olarak ifade edildiği ayrıca Hizmet Koşullarına onay verilmeden sözleşmenin yürürlüğe giremeyeceğinin belirtildiği görülmüştür.

Bu kapsamda; Kişisel Verileri Koruma Kurulu'nun 03.09.2021 tarih ve 2021/891 sayılı Kararı ile;

- Veri sorumlusu tarafından söz konusu uygulama kapsamında çeşitli kişisel veri işleme faaliyetleri bakımından farklı veri işleme şartlarına dayanıldığı ve kişisel veri işlemeye yönelik açık rıza şartının ise istisna olarak başvurulmuş bir şart olduğu belirtilse de Hizmet Koşullarının kullanıcı ile

yapılan bir sözleşme olarak tanımlaması nedeniyle sözleşmeye onay verilmesi suretiyle ilgili kişilerin açık rızasının alınması yoluna gidildiği, bu çerçevede kullanıcılardan kişisel verilerinin işlenmesine ve yurtdışında yerleşik üçüncü taraflara aktarılmasına seçimlik hak sunulmaksızın tek bir açık rıza alındığı, sözleşmeye aktarıma ilişkin hüküm koymak suretiyle işleme ve aktarım faaliyetlerinin, tek metinde birbirinden ayrılmaz bir biçimde ilgili kişiye sunulduğu dikkate alındığında, açık rızanın “özgür iradeyle açıklanması” unsurunun zedelendiği,

- Veri sorumlusu tarafından Hizmet Koşulları ve Gizlilik İlkesinde yer alan “aktarım” a ilişkin ifadelerin müzakereye kapalı nitelikte sunularak ilgili kişilerin sözleşmeye bir bütün olarak onay vermeye zorlandığı, bu suretle açık rızanın saf dışı bırakılmaya çalışıldığı, uygulamanın kullanılmasının aktarım şartına bağlandığı, bu kapsamda ilgili kişilerin çıkarları ve makul beklentileri göz önüne alınmaksızın hareket edildiği dikkate alınarak veri sorumlusunun bu uygulamasının Kanunun 4’üncü maddesinde yer alan “Hukuka ve dürüstlük kurallarına uygun olma” ilkesine aykırılık teşkil ettiği,
- İşlenen tüm kişisel verilerin aktarımına ilişkin açık rıza istenildiği, ancak bu verilerin işlendikleri amaçla orantılı ve sınırlı bilgiler olmadığı gibi hangi verinin hangi amaçla aktarılacağına da bahse konu metinlerde net olarak ortaya konulmadığı, bu hususta veri sorumlusunca Kanunun 4’üncü maddesinde yer alan “belirli, açık ve meşru amaçlar için işlenme” ve “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkelerine aykırı hareket edildiği,
- WhatsApp tarafından kişisel verilerin işlenmesinin sözleşmenin bir parçası haline getirilmek suretiyle ilgili kişilerden sözleşmeye onay vermelerinin istenildiği ve sonrasında “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” şartı başta olmak üzere diğer kişisel veri işleme şartlarına dayanılarak kişisel verilerinin işlendiğinin beyan edildiği ancak görünen işlem sözleşmeye onay verme olsa da asıl yapılan işlemin kişisel verilerin işlenmesine açık rıza alınması niteliğinde olduğu, bu bakımdan sözleşmenin içerisine derç edilerek hizmetin bir koşulu olarak dayatılması suretiyle alınan açık rızanın, “özgür iradeyle açıklanması” unsurunun zedelendiği,
- Veri sorumlusunun Türkiye’de bulunan ilgili kişilerden elde ettiği kişisel veriler üzerinde, bu verileri elde ettikten sonra yapmış olduğu kaydetme, depolama, değiştirme, aktarma gibi her türlü işleme faaliyetinin, sunucuları Türkiye’de bulunmadığı sürece kişisel verilerin yurt dışına aktarımı anlamına geldiği, dolayısıyla söz konusu aktarımın, Kanunun “Kişisel verilerin yurt dışına aktarılması” başlıklı 9 uncu maddesine uygun olarak yapılmasının zorunluluk arz ettiği ancak veri sorumlusu tarafından aktarım faaliyetleri için hiçbir şekilde açık rızaya başvurulmadığının beyan edildiği, bununla birlikte veri sorumlusunca Kurulumuza bir

taahhütname başvurusunda da bulunulmadığı dikkate alındığında, veri sorumlusu tarafından Kanunun 9 uncu maddesine uygun hareket edilmediği,

- Veri sorumlusu tarafından, profillemeye amacıyla çerezler aracılığıyla yapılacak kişisel veri işleme faaliyetine ilişkin olarak ilgili kişilerden açık rıza alınmadığı, bu kapsamda yürütülen kişisel veri işleme faaliyetinin de hukuka uygun olmadığı

anlaşıldığından Kanunun 12 nci maddesinin (1) numaralı fıkrasında yer alan kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almadığı tespit edilen veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 1.950.000 TL idari para cezası uygulanmasına, Ayrıca veri sorumlusunun;

- Uygulamaya konulmadığı belirtilen 04.01.2021 tarihli Hizmet Koşulları ve Gizlilik İlkesi metinlerinin, halihazırda kullanıcılara geçerli sürüm olarak sunulduğu anlaşıldığından, ilgili kişilerin doğru bilgilendirilmesi için söz konusu metinlerin üç ay içerisinde Kanuna uygun hale getirilmesi,
- Gizlilik İlkesinin, aydınlatma metni yerine kullanıldığı ve geçerli bir aydınlatmanın unsurlarını taşımadığı anlaşıldığından, Kanunun 10'uncu maddesi ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerine uygun bir aydınlatma yapılması

ve söz konusu işlemlerin sonucundan Kurula bilgi verilmesi hususunda talimatlandırılmasına karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

09.08.2021 - Yurt Dışında Yaşayan Türkiye Cumhuriyeti Vatandaşlarının Kişisel Verilerinin Yurt Dışına Aktarılmamasına İlişkin Talepleri

Yurt Dışında Yaşayan Türkiye Cumhuriyeti Vatandaşlarının Kişisel Verilerinin Yurt Dışına Aktarılmamasına İlişkin Talepleri Hakkında Kamuoyu Duyurusu

Yayınlanma Tarihi : 09.08.2021

Kişisel verilerin yurtdışına aktarılmasına yönelik hükümler 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 9 uncu maddesinde Kanunun kişisel veri işleme şartlarına ilişkin maddelerine atıf yapılmak suretiyle belirtilmiştir. Bu kapsamda;

- Yurt dışında ikamet eden Türkiye Cumhuriyeti vatandaşları tarafından Kurumumuza, gerek Cumhurbaşkanlığı İletişim Merkezi (CİMER) üzerinden gerekse yazılı olarak ayni ve nakdi kişisel verilerinin başta Avrupa Birliği üyesi ülkeler olmak üzere diğer ülkelerin kurum ve kuruluşlarıyla paylaşılmamasını konu alan birçok başvuru intikal etmektedir. Kurumumuza intikal eden dilekçelerin bazılarında vatandaşların finansal hesap bilgilerinin yurt dışına aktarılmaması taleplerinin açıkça belirtildiği görülmekte olup bu nitelikteki dilekçelerin esas olarak ülkemizin de dahil olduğu Ekonomik Kalkınma ve İşbirliği Teşkilatı'na (OECD) üye ülkeler tarafından 3 Kasım 2011 tarihinde imzalanan ve 03.05.2017 tarihli ve 7018 sayılı Kanunla onaylanması uygun bulunan "Vergi Konularında Karşılıklı İdari Yardımlaşma Sözleşmesi" (Sözleşme) ile bu sözleşme kapsamında 2017 yılında imzalanan, 31.12.2019 tarihli ve 30995 sayılı Resmi Gazete'de yayımlanan "Finansal Hesap Bilgilerinin Otomatik Değişimine İlişkin Çok Taraflı Yetkili Makam Anlaşması" (Anlaşma) sebebiyle gerçekleştirildiği anlaşılmıştır. Türkiye'de söz konusu Anlaşma kapsamında otomatik bilgi değişimi için bilgileri toplamaya ve paylaşmaya yetkili makam, Hazine ve Maliye Bakanlığına bağlı Gelir İdaresi Başkanlığı olarak belirlenmiş olduğundan bu nitelikteki dilekçeler ilgisi nedeniyle anılan Bakanlığa intikal ettirilmiştir.

- Diğer taraftan, yurt dışında ikamet eden vatandaşların dilekçelerinin bazılarında ise herhangi bir ayırım yapılmaksızın genel olarak kişisel bilgilerinin yurt dışına aktarılmamasının talep edildiği görülmüştür.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Veri Sorumlusuna Başvuru" başlıklı 13 üncü maddesinin (1) numaralı fıkrasında; ilgili kişinin, bu Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletacağı;

Kanunun “Kurula Şikâyet” başlıklı 14 üncü maddesinin birinci fıkrasında da başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; ilgili kişinin, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde Kişisel Verileri Koruma Kurulu’na (Kurul) şikâyette bulunabileceği, ikinci fıkrasında ise 13 üncü madde uyarınca başvuru yolu tüketilmeden Kurula şikâyet yoluna başvurulamayacağı hükümleri yer almaktadır.

Kanunun 13 üncü maddesine dayanılarak hazırlanan “Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ”in (Tebliğ) “Başvuru Usulü” başlığını taşıyan 5 inci maddesinin birinci fıkrasında ise “İlgili kişi, Kanunun 11 inci maddesinde belirtilen hakları kapsamında taleplerini, yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletir” hükmüne yer verilerek başvuruda bulunması zorunlu unsurlar ad, soyadı, başvuru yazılı ise imza, T.C. Kimlik No., tebligata esas yerleşim yeri veya iş yeri adresi, varsa bildirim esas e-posta adresi ve talep konusu olarak sayılmıştır.

Bu çerçevede, genel olarak kişisel verilerinin yurt dışına aktarılmaması taleplerini içeren bu nitelikteki dilekçeler hakkında ise, ilgili kişilere kişisel verilerin korunması konusundaki talepleri ile ilgili olarak hak arama yöntemlerini içeren Kanunun 13 ve 14 üncü maddeleri hakkında bilgi verilmiştir.

• Ancak, mevcut durumda yurt dışında yaşayan Türkiye Cumhuriyeti vatandaşları tarafından benzer nitelikte çok sayıda dilekçenin Kurumumuza intikal etmesi sebebiyle konu Kişisel Verileri Koruma Kurulu tarafından değerlendirilmiş olup, alınan 07/07/2021 tarihli ve 693 sayılı Kurul Kararı ile;

- İlgili kişiler tarafından Kurumumuza intikal eden ve kişisel verilerin yurt dışına aktarılmamasını konu edinen genel nitelikteki başvuruların, herhangi bir veri sorumlusuna işaret etmemesi, taleplerin soyut nitelikte olması ve bu kapsamda 6698 sayılı Kanunun 13 ve 14’üncü maddelerinde yer alan veri sorumlusuna başvuru şartının yerine getirilmemiş olması nedeniyle usulü şartları taşımadığı değerlendirilmiş olduğundan Kuruma intikal eden bu yöndeki başvuruların incelemeye alınamayacağına,

- Öte yandan, ilgili kişiler tarafından Kurumumuza intikal eden ve “Otomatik Bilgi Paylaşımına” atıfta bulunulan başvurulara ilişkin olarak ise otomatik veri paylaşımına ilişkin hususların “Finansal Hesap Bilgilerinin Otomatik Değişimine İlişkin Çok Taraflı Yetkili Makam Anlaşması”nda düzenlendiği ve Anlaşma hükümlerinin ülkemiz nezdinde uygulanması bakımından yetkili makamın Hazine ve Maliye Bakanlığı’na bağlı Gelir İdaresi Başkanlığı olduğu değerlendirildiğinden bu minvaldeki başvuruların esasen başvuru sahipleri

tarafından ilgili Bakanlığa intikal ettirilmesi gerektiğinden hareketle söz konusu dilekçelere ilişkin olarak 6698 sayılı Kanun kapsamında yapılacak bir işlem olmadığına

karar verilmiştir.

Anılan Kurul Kararı çerçevesinde, Kurumumuza bugüne kadar intikal eden ve bundan sonra intikal edecek olan mezkur nitelikteki başvurular, Kurul Kararında yer verilen gerekçelerle değerlendirmeye alınmayacak olup başvuru sahiplerine de Kurumumuz tarafından ayrıca bir yanıt verilmeyeceği kamuoyuna saygıyla duyurulur.

25.06.2021 - Ortaklıkların VERBİS'e Kayıt Yükümlülüğü

Ortaklıkların VERBİS'e Kayıt Yükümlülüğü Hakkında Duyuru

Yayınlanma Tarihi : 25.06.2021

Kurumumuza iletilen yazılı ve şifahi görüş taleplerinde; iş ortaklığı / konsorsiyum / adi ortaklıkların Veri Sorumluları Siciline (Sicil) kayıt yükümlülükleri hususunda tereddütler yaşandığı ifade edilmiştir.

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 16 ncı maddesinde öngörülen Sicile kayıt yükümlülüğünün asıl amacı, kişisel veri işleme süreçlerinin şeffaf ve ilgili kişilere hesap verebilir nitelikte yürütülmesi ile ilgili kişilerin kendi kişisel verileri üzerinde en üst düzeyde kontrol sağlamasıdır.

Bu bakımdan iş ortaklığı / konsorsiyum / adi ortaklık gibi yapılar altında gerçekleştirilen faaliyetlerde işlenen kişisel verilerin Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) bilgi girişi olarak yansıtılması önem arz etmektedir.

Bu kapsamda, Kişisel Verileri Koruma Kurulunun 09/06/2021 tarihli ve 2021/569 sayılı kararı ile;

- Ortaklığı oluşturan ortaklardan hâlihazırda Sicile kayıt yükümlülüğü bulunanların VERBİS'e kayıtları esnasında kendi faaliyetleri ile birlikte ortaklık faaliyetleri kapsamında işledikleri kişisel verilere ilişkin olarak da bilgi girişi yapması gerektiğine

karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

25.06.2021 - Dernek, Vakıf ve Sendikalara Ait İktisadi İşletmelerin VERBİS'e Kayıt

Yükümlülüğü

Dernek, Vakıf ve Sendikalara Ait İktisadi İşletmelerin VERBİS'e Kayıt Yükümlülüğü Hakkında Duyuru

Yayınlanma Tarihi : 25.06.2021

Kurumumuza iletilen yazılı ve şifahi görüş taleplerinde; dernek, vakıf ve sendikalara ait iktisadi işletmelerin Veri Sorumluları Siciline (Sicil) kayıt yükümlülükleri hususunda tereddütler yaşandığı ifade edilmiştir.

6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 16 ncı maddesi gereğince; Kişisel Verileri Koruma Kurulu (Kurul), Veri Sorumluları Sicili Hakkında Yönetmeliğin 16 ncı maddesinde yer alan kriterleri göz önüne alarak Sicile kayıt yükümlülüğüne istisna getirebilmekte, istisnaların kapsamı ve uygulanmasına ilişkin usul ve esasları belirlemek amacıyla karar alabilmektedir.

Kurulun 22/04/2020 tarihli ve 2020/315 sayılı Kararı ile değişik 02/04/2018 tarihli ve 2018/32 sayılı Kararı uyarınca *"yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı olmak üzere kişisel veri işleyen Türkiye'de yerleşik dernek, vakıf ve sendikalar"* için Sicile kayıt yükümlülüğüne istisna getirilmiştir.

Kanunun 16 ncı maddesinde öngörülen Sicile kayıt yükümlülüğünün asıl amacı, kişisel veri işleme süreçlerinin şeffaf ve ilgili kişilere hesap verebilir nitelikte yürütülmesi ile ilgili kişilerin kendi kişisel verileri üzerinde en üst düzeyde kontrol sağlamasıdır.

Bununla birlikte dernek, vakıf ve sendikaların Sicile kayıt yükümlülüğüne istisna getirilmesine ilişkin kriterler açısından yapılan değerlendirme sonucunda; gelir elde etmek amacıyla yürüttükleri ticari faaliyetleri nedeniyle dernek, vakıf ve sendikaların iktisadi işletmeleri için söz konusu istisnanın uygulanması uygun görülmemektedir.

Bu bakımdan dernek, vakıf ve sendikalara ait iktisadi işletmelerin bünyesinde gerçekleştirilen faaliyetlerde işlenen kişisel verilerin Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) bilgi girişi olarak yansıtılması önem arz etmektedir.

Bu kapsamda, Kurulun 09/06/2021 tarihli ve 2021/571 sayılı kararı ile;

- 22/04/2020 tarihli ve 2020/315 sayılı Karar ile deęişik 02/04/2018 tarihli 2018/32 sayılı Kurul Kararında yer alan *“yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı olmak üzere kişisel veri işleyen Türkiye’de yerleşik dernek, vakıf ve sendikalar”* ifadesinin *“yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı olmak üzere kişisel veri işleyen Türkiye’de yerleşik dernek, vakıf ve sendikalardan kendisine baęlı herhangi bir iktisadi işletmesi bulunmayanlar”* olarak deęiştirilmesine,
- Yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı olmak üzere kişisel veri işleyen Türkiye’de yerleşik dernek, vakıf ve sendikalardan kendisine baęlı herhangi bir iktisadi işletmesi bulunanların Sicile kayıt olmaları ile Sicile kayıtları esnasında yalnızca iktisadi işletmelerin faaliyetlerine ilişkin bilgi giriři yapmalarının gerektiğine,
- Anılan Kararın Kurum internet sayfası ve Resmi Gazetede yayımlanmasına

karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

30.03.2021 - Kurumumuza Yapılan Şikayetlerin Usul Şartları

Kurumumuza Yapılan Şikayetlerin Usul Şartlarına İlişkin Kamuoyu Duyurusu

Yayınlanma Tarihi : 30.03.2021

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 'İlgili Kişinin Hakları' başlıklı 11 inci maddesinde " (1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili; a) Kişisel veri işlenip işlenmediğini öğrenme, b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme, c) Kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme haklarına sahiptir" hükmüne yer verilmiştir.

İlgili kişinin hak arama yöntemleri ise Kanunun 13 ve 14 üncü maddelerinde belirlenmiş olup buna göre, Kanunun "Veri Sorumlusuna Başvuru" başlıklı 13 üncü maddesinin (1) numaralı fıkrasında; *"İlgili kişi, bu Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir"* hükmü yer almaktadır.

Bahse konu maddeye dayanılarak hazırlanan "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ" in (Tebliğ) "Başvuru Usulü" başlığını taşıyan 5 inci maddesinin birinci fıkrasında "İlgili kişi, Kanunun 11 inci maddesinde belirtilen hakları kapsamında taleplerini, yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletir" hükmüne yer verilerek başvuruda bulunması zorunlu unsurlar ad, soyadı, başvuru yazılı ise imza, T.C. Kimlik No., tebligata esas yerleşim yeri veya iş yeri adresi, varsa bildirim esas e-posta adresi ve talep konusu olarak sayılmıştır.

Kanunun “Kurula Şikâyet” başlıklı 14 üncü maddesinin (1) numaralı fıkrasında ise “Başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyette bulunabilir” hükmüne, (2) numaralı fıkrasında ise “13 üncü madde uyarınca başvuru yolu tüketilmeden şikâyet yoluna başvurulamaz” hükmüne yer verilmiştir.

Kanunun “Şikâyet Üzerine veya Resen İncelemenin Usul ve Esasları” başlıklı 15 inci maddesinin (1) numaralı fıkrası Kurulun, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapacağı, (2) numaralı fıkrası da 01.11.1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesinde belirtilen şartları taşımayan ihbarların veya şikâyetlerin incelemeye alınmayacağı hükümlerini haizdir.

Öte yandan, 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesinde ise; “Türkiye Büyük Millet Meclisine veya yetkili makamlara verilen veya gönderilen dilekçelerden;

- a) Belli bir konuyu ihtiva etmeyenler,
- b) Yargı mercilerinin görevine giren konularla ilgili olanlar,
- c) 4 üncü maddede gösterilen şartlardan herhangi birini taşımayanlar incelenemezler.” hükmüne yer verilmiştir.

Bu itibarla yukarıda sayılan mevzuat hükümleri çerçevesinde usul şartlarını taşımayan şikâyetler Kurul tarafından esas yönünden değerlendirmeye alınamayarak reddedilmekte olup, şikâyetlerin daha etkin ve kısa sürede sonuçlanmasını teminen;

Veri sorumlusuna yapılacak başvurularda:

Kanunun 13 üncü maddesi ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğde belirlenen yöntem ve esaslara dikkat edilmesi, bu kapsamda;

- Veri sorumlusuna yapılacak başvuruların yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla yapılması
- Başvuru veri sorumlusuna ilgili kişinin KEP adresi dışında bir e-posta adresi üzerinden iletilecek ise mutlak surette veri sorumlusuna daha önce bildirilmiş ve veri sorumlusu nezdinde kayıtlı bulunan e-posta adresinin kullanılması

- Veri sorumlusuna başvuru yazılı yapılmış ise mutlak surette başvuruda imzaya yer verilmesi, vekil aracılığı ile yapılan başvurularda vekaletname örneğinin iletilmesi
- Yapılan her başvurunun ad, soyad, T.C. Kimlik No., tebligata esas yerleşim yeri veya iş yeri adresi, varsa bildirim esas e-posta adresi ve talep konusu içermesi
- Yapılan başvuruların Kanununun 11 inci maddesinde yer verilen ilgili kişinin hakları kapsamında olması gerekmektedir.

Kurula yapılacak şikayetlerde;

- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun gereğince yazılı başvurularda mutlak surette ad, soyad, imza, iş veya ikametgah adresine yer verilmesi
- Vekil aracılığı ile yapılan başvurularda başvuru ekinde ilgili kişiye ait vekâletnamenin eksiksiz bir şekilde ve süresine dikkat edilerek sunulması
- Kanun kapsamındaki talepler ile ilgili olarak Kurula şikayette bulunmadan önce veri sorumlusuna başvuru yolunun tüketilmesi,
- Veri sorumlusuna yapılmış başvuruya, başvurunun veri sorumlusuna iletildiğine dair kanıtlayıcı belgeye (örneğin PTT gönderi belgesi) ve gerekmesi halinde başvuru yöntemine ilişkin bilgi ve belgeye (örneğin e-posta ya da bir uygulama aracılığı ile başvuruldu ise bu yöntemin anlaşılır ve kanıt taşıyıcı nitelikte sunulması) yer verilmesi
- Veri sorumlusu tarafından ilgili kişiye cevap verilmiş ise verilen cevabın dilekçe ekinde yer alması ve varsa ilgili kişi tarafından cevabın ne zaman alındığını gösterir belgenin iletilmesi
- Kanununun 14 üncü maddesinde Kurula şikayette bulunabilmek için öngörülen sürelerle riayet edilmesi, bu kapsamda ilgili kişilerce
 - Veri sorumlusundan başvuru tarihinden itibaren en geç otuz gün içinde yanıt alındığı durumlarda veri sorumlusunun cevabının öğrenildiği tarihten itibaren otuz gün içinde Kurula şikayetin iletilmesi
 - Veri sorumlusunun yanıtının başvuru tarihinden itibaren otuz günden daha geç alınması halinde ilk başvuru tarihinden itibaren altmış gün içinde Kurula şikayetin iletilmesi
 - Veri sorumlusundan yanıt alınmadığı durumlarda başvuru tarihinden itibaren altmış gün içinde Kurula şikayetin iletilmesi

- Veri sorumlularının kendilerine başvurulduđu tarihten itibaren 30 gnlk cevap verme sresinin olduđu dikkate alındıđında veri sorumlusuna yapılan başvurudan itibaren 30 gn beklenilmesi, yanıt alınmaması durumunda Kurula Őikayette bulunulması
- Kanunun 14 nc maddesinde yer verilen srelerin hesaplanabilmesini teminen Kurula iletilen dilekelerin, veri sorumlusuna yapılan başvuruların, alınan cevapların ve bu belgelere dair gnderi belgelerinin tarihlerinin aık ve anlaŐılır olması
- 3071 sayılı Dileke Hakkının Kullanılmasına Dair Kanun geređince Őikyete konu edilen iddiaları tevsik edici belgelerin dilekeye ilave edilmesi
- 3071 sayılı Dileke Hakkının Kullanılmasına Dair Kanun geređince Őikyet konusunun ve talebin aık olarak belirtilmesi
- Konunun yargı mercilerine de intikal ettirilmesi halinde bu hususta detaylı bilgi ve dokmana yer verilmesi
- Kurumun grev alanı dıŐında taleplere yer verilmemesi

hususlarına dikkat edilmesi nem arz etmektedir.

Kamuoyuna saygıyla duyurulur.

11.03.2021 - VERBİS'e Kayıt Sürelerinin Uzatılması

VERBİS'E KAYIT SÜRELERİNİN UZATILMASI HAKKINDA DUYURU

Ülkemizde halen etkisini göstermeye devam eden Covid-19 virüs salgını nedeniyle Veri Sorumluları Siciline (Sicil) kayıt yükümlülüğünün gereği gibi yerine getirilmesi hususunda zorluklar yaşandığı gerekçesiyle Sicile kayıt sürelerinin uzatılmasına ilişkin birçok veri sorumlusu veya bunların bağlı olduğu üst kuruluşlar, muhtelif sektör temsilcileri ile bazı kamu kurumları ve kamu kurumu niteliğindeki meslek kuruluşları tarafından Kuruma intikal ettirilen taleplerin değerlendirilmesi neticesinde Kişisel Verileri Koruma Kurulunun 11/03/2021 tarihli ve 2021/238 sayılı Kararı ile;

- Yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları ile yurtdışında yerleşik gerçek ve tüzel kişi veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.12.2021 tarihine,
- Yıllık çalışan sayısı 50'den az ve yıllık mali bilançosu 25 milyon TL' den az olup ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek ve tüzel kişi veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.12.2021 tarihine,
- Kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşu veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.12.2021 tarihine

kadar uzatılmasına,

- Anılan Kararın Kurum internet sayfası ve Resmi Gazetede yayımlanmasına

oybirliği ile karar verilmiştir.

WHATSAPP Uygulaması Hakkında Kamuoyu Duyurusu

Yayınlanma Tarihi : 12.01.2021

Bilindiği üzere; 7 Nisan 2016 tarihli Resmi Gazete’de yayınlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 2 nci maddesinde “Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır” hükmü yer almaktadır.

Kişisel verilerin işlenebilmesi için ise, Kanunun 5 inci ve 6 ncı maddelerinde yer alan işleme şartlarından herhangi birinin mevcut olması gerekmektedir. Kanunun 5 inci maddesinin (2) numaralı fıkrasına göre; *“kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması,”* işleme şartlarından herhangi birinin varlığı halinde kişisel veriler işlenebilecektir. Bu şartların bulunmadığı durumlarda ise kişisel veriler ancak ilgili kişinin açık rızası alınmak suretiyle işlenebilecektir.

Kanunun 3 üncü maddesinde açık rıza; “belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza” olarak tanımlanmış olup, buna göre açık rızanın üç unsuru bulunmaktadır:

- Belirli bir konuya ilişkin olması,
- Rızanın bilgilendirmeye dayanması,
- Özgür iradeyle açıklanması.

Söz konusu unsurlar açısından değerlendirildiğinde açık rıza, kişinin sahip olduğu verinin işlenmesine, kendi isteği ile hukuka uygun şekilde onay vermesi anlamını taşımaktadır. Açık rızanın bir diğer önemi de veri sorumlusuna, gerçekleştireceği kişisel veri işleme faaliyeti konusunda yol

göstermesidir. Kişi açık rıza açıklaması ile aslında veri sorumlusuna kendi hukuksal değerine ilişkin verdiği kararı bildirmiş olmaktadır. Açık rıza, ilgili kişinin işlenmesine izin verdiği verinin sınırlarını, kapsamını, gerçekleştirilme biçimini ve süresini de belirlemesini sağlayabilmektedir. Bu anlamda açık rıza, rıza veren kişinin olumlu irade beyanını içermelidir.

Kişisel verilerin işlenmesine açık rıza vermek, kişiye sıkı sıkıya bağlı bir hak olduğundan verilen açık rıza geri alınabilir. Bu bağlamda kişisel verilerin geleceğini belirleme hakkı ilgili kişiye ait olup, kişi dilediği zaman veri sorumlusuna vermiş olduğu açık rızasını geri alabilir. Ancak, geri alma işlemi ileriye yönelik sonuç doğuracağından, açık rızaya dayalı olarak gerçekleştirilen tüm faaliyetler geri alma beyanının veri sorumlusuna ulaştığı andan itibaren veri sorumlusu tarafından durdurulmalıdır. Bir diğer deyişle, geri alma beyanı veri sorumlusuna ulaştığı andan itibaren hüküm doğurur.

Kişisel verilerin işlenmesinde hukuki sebep olarak “açık rıza”nın belirlenmesinin söz konusu olduğu ve verilen hizmetin açık rıza şartına bağlandığı hususlara ilişkin olarak 2 Ağustos 2018 tarihinde Kurum internet sayfasında, Kişisel Verileri Koruma Kurulunun (**Kurul**) 16.02.2018 tarihli ve 2018/19 sayılı Kararının özeti yayınlanmıştır. Söz konusu Kurul kararında da belirtildiği üzere, öncelikle kişisel verilerin işlenmesi sırasında ilgili kişilerden alınan açık rıza, veri sorumluları tarafından bir hizmetin ifası için ön şart olarak ileri sürülemeyecektir.

Kanunun 4 üncü maddesi uyarınca kişisel verilerin, hukuka ve dürüstlük kurallarına uygun, belirli, açık ve meşru amaçlarla ve işlenme amacı ile bağlı, sınırlı ve ölçülü olma ilkelerine uygun olarak işlenmesi, hangi kişisel verilerin işleneceği veya hangi amaçlarla kimlere aktarılacağı hususlarında gerekli bilgilendirmenin yapılmış olması ve her bir işleme/aktarma faaliyetine yönelik seçenek sunulmak suretiyle ayrı ayrı açık rıza alınması gerekmektedir.

Diğer taraftan, Kanunun “*Kişisel verilerin yurt dışına aktarılması*” başlıklı 9 uncu maddesinde; kişisel verilerin, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamayacağı; ancak anılan hükmün ikinci fıkrası uyarınca Kanunun 5 inci maddesinin ikinci fıkrası ile özel nitelikli kişisel veriler bakımından 6 ncı maddesinin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede yeterli korumanın bulunması, yeterli korumanın bulunmaması durumunda Türkiye’deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurul izninin bulunması kaydıyla kişisel verilerin ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilmesi düzenlenmiştir.

WhatsApp Inc. tarafından, WhatsApp uygulamasını kullanmak isteyen kullanıcıların kişisel verilerinin işlenmesine ve yurtdışında bulunan üçüncü taraflara aktarılmasına rıza verilmesini içerecek şekilde kullanım şartlarının güncellendiği, bu kapsamda rıza vermeyen kullanıcıların

uygulamayı kullanamayacağına ve hesaplarının silineceğine dair kullanıcılara bilgilendirme iletildiği tespit edilmiştir.

Söz konusu bilgilendirme metninde yönlendirme yapılan Gizlilik Politikasında ise, hangi verilerin hangi amaçlarla işleneceği ifade edilmekle birlikte, işlenen kişisel verilerin WhatsApp Inc. tarafından yurtdışında yerleşik bulunan hizmet aldığı ve hizmet verdiği Facebook grup şirketleri, tedarikçileri, iş ortakları, hizmet sağlayıcıları ve diğer üçüncü taraf veri sorumluları gibi net olarak belirli olmayan taraflara teknik destek, teslimat ve diğer hizmetleri sağlamak, araştırma yapmak, pazarlama ve anket vb. gibi yine belirli olmayan amaçlarla aktarılacağı ifade edilmekte olduğu görülmektedir.

Kişisel verilerin, yurtdışında yerleşik bir veri sorumlusu olan WhatsApp Inc. tarafından işlenmesine ve yurtdışında yerleşik başka veri sorumlularına aktarılmasına ilişkin açık rıza alınması hususunda yapılan ön değerlendirme sonucunda;

- Kullanıcılardan kişisel verilerinin işlenmesine ve yurtdışında yerleşik üçüncü taraflara aktarılmasına yönelik rıza alınması işleminin ayrıştırılmadığı ancak kullanıcıların kişisel verilerinin işlenmesine rıza verirken yurtdışında başka bir veri sorumlusuna aktarılmasına rıza vermeyebileceği dikkate alındığında söz konusu uygulamanın kullanım yaygınlığı da göz önünde bulundurularak bu durumun Kanunda belirlenen açık rızanın unsurlarından “özgür iradeyle açıklanması” açısından bir ihlal oluşturup oluşturmadığı,
- Yurtdışında bulunan başka bir şirkete aktarım yapılmak şartıyla uygulamanın kullanılmasına izin verilmesinin Kanunun 4 üncü maddesinde sayılan ilkelerden “hukuka ve dürüstlük kurallarına uygun olma”, “belirli, açık ve meşru amaçlar için işleme” ve “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkeleri açısından bir ihlale sebebiyet verip vermediği,
- Sunulan hizmetin açık rıza şartına bağlanmış olmasının verilen açık rızayı sakatlayabileceği bu durumun da kişisel verilerin hukuka aykırı işlenmesi sonucunu doğurabileceği dikkate alındığında Whatsapp Inc. tarafından yapılan güncelleme ile hizmetin rıza şartına bağlanması durumunun ortaya çıkıp çıkmadığı,
- WhatsApp Inc. tarafından yurtdışında yerleşik veri sorumlularına yapılacak aktarım hususunda Kanunun 9 uncu maddesi hükümlerine aykırılık olup olmadığı

hususları açısından, Kişisel Verileri Koruma Kurulunun 12.01.2021 tarihli ve 2021/28 sayılı Kararı ile WhatsApp Inc. hakkında resen inceleme başlatılmasına karar verilmiştir.

Sürece ilişkin olarak 08.02.2021 tarihinde Kurul tarafından yeni bir değerlendirme yapılacaktır.

Kamuoyuna saygıyla duyurulur.

WHATSAPP Uygulaması Hakkında Kamuoyu Duyurusu

Ülkemizde son günlerde basına da yansıyan çeşitli haberlerden; Whatsapp Inc tarafından WhatsApp uygulamasını kullanmak isteyen kullanıcıların kişisel verilerinin işlenmesine ve yurtdışında bulunan tedarikçi, iş ortakları, hizmet sağlayıcıları ve diğer üçüncü taraflara aktarılmasına rıza verilmesini içerecek şekilde kullanım şartlarının güncellendiği, bu kapsamda rıza vermeyen kullanıcıların bu uygulamayı kullanamayacağı ve hesaplarının silineceğine dair kullanıcılara bilgilendirme iletildiği anlaşılmaktadır.

Bu kapsamda, Kişisel Verilerin Korunması Kanununun 15 inci maddesi uyarınca Kişisel Verileri Koruma Kurulunun 12.01.2021 tarihli toplantısında konu, kişisel verilerin korunması mevzuatı genel hükümleri ile Kanunun açık rıza, veri işleme şartları, yurtdışına veri aktarımı ve temel ilkeler yönünden değerlendirilecek olup, gelişmeler hususunda kamuoyu ayrıca bilgilendirilecektir.

Kamuoyuna saygıyla duyurulur.

26.10.2020 - Yurtdışına Veri Aktarımı

Yurtdışına Veri Aktarımı Kamuoyu Duyurusu

Yayınlanma Tarihi : 26.10.2020

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanunu (**Kanun**) 07.04.2016 tarihli ve 29677 sayılı Resmi Gazetede yayımlanmıştır. Kanunun 32 nci maddesi uyarınca Kanunun 8 inci, 9 uncu, 11 inci, 13 üncü, 14 üncü, 15 inci, 16 ncı, 17 nci ve 18 inci maddeleri yayımı tarihinden altı ay sonra, diğer maddeleri ise yayımı tarihinde yürürlüğe girmiştir. Bununla birlikte, Kanunun “Geçiş hükümleri” başlıklı Geçici 1 inci maddesinin üçüncü fıkrasında Kanunun yayımı tarihinden önce işlenmiş olan kişisel verilerin, yayımı tarihinden itibaren 2 yıl içerisinde Kanun hükümlerine uygun hale getirileceği düzenlenmiştir. Bu anlamda, kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenleyen Kanuna uyum için makul bir süre hem Kanunda yer alan düzenlemelerle hem de Kurumumuzun işbirliğine dayalı anlayışı ile kişisel veri işleme faaliyetinde bulunan ilgililere tanınmıştır.

Kurumumuz faaliyete geçtiği günden bu yana, kişisel verilerin korunmasına yönelik farkındalık yaratmak ve ilgililerin iş süreçlerini Kanuna uygun olarak yeniden tasarlayabilmeleri adına Ülkemizin her bölgesine yayılan organizasyonlar gerçekleştirmekte, ilgili meslek örgütleri ve sivil toplum kuruluşları ile sürekli olarak bilgi alışverişinde bulunmakta, veri sorumluları ile veri işleyenleri yönlendirmekte ve ilgili paydaşlardan gelen talepleri uygun düştüğü ölçüde karşılamaktadır. Bu kapsamda, eğitim programları düzenlenmekte ve Kanuna etkili bir uyumun sağlanabilmesi için işleme faaliyetinde bulunan aktörlere kolaylık sağlanmaya çalışılmaktadır. Ayrıca yine önemle ifade etmek gerekir ki, başta Türkiye Odalar ve Borsalar Birliği ve muhtelif sektör temsilcileri olmak üzere çeşitli paydaşların talebi doğrultusunda Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğünün yerine getirilmesi için tanınan süre kapsamlı uyum sürecinin gerektirdiği özen, Sicile kayıt uygulamasıyla kişisel verileri işlenen ilgili kişiler bakımından sağlanması amaçlanan şeffaflığın tam anlamıyla gerçekleşmesi gereği ve COVID-19 salgınının etkileri dikkate alınarak üç kere uzatılmıştır. Yine, COVID-19 salgını sürecinde uzaktan ve/veya dönüşümlü çalışma uygulamalarının neden olabileceği zorluklar; her bir başvuru ya da veri ihlal bildirimi özelinde, veri sorumlularının uymakla yükümlü oldukları sürelerin değerlendirilmesi açısından Kişisel Verileri Koruma Kurulu (**Kurul**) tarafından göz önünde bulundurulmuştur.

Kurumumuz, Anayasada öngörülen özel hayatın gizliliği ile temel hak ve özgürlüklerin korunması kapsamında, Ülkemizde kişisel verilerin korunmasını sağlamanın ve buna yönelik farkındalık oluşturarak bilinç düzeyini geliştirmenin yanında, veri temelli ekonomide özel ve kamusal aktörlerin uluslararası rekabet kapasitelerini artırıcı bir ortam oluşturmayı da misyon olarak benimsemektedir. Kişisel verilerin hukuka uygun, bireylerin kontrolünden ödün vermeden ve şeffaf bir biçimde işlenmesi sonucu elde edilecek katma değer büyük bir önem arz etmektedir. Nitekim Kurumumuz da bu farkındalığa sahip olarak kişisel verilerin korunması ve dijital dönüşümün çok yoğun bir şekilde yaşandığı günümüzün gereklerine uygun olarak kişisel verilerin önemli bir parçasını teşkil ettiği verimi yüksek ve avantajlı iş süreçlerinin sürdürülebilmesi arasında bir denge gözetmektedir. Ancak takdir edilecektir ki, Kurumumuz Kanunda öngörülen görev ve yetkileri çerçevesinde faaliyetlerini sürdürmektedir. Bu anlamda, kişisel verilerin Kanunda yer verilen usul ve esaslara uygun olarak işlenmesinin sağlanması ve zorunlu izin ve/veya yetkilendirme süreçlerinin işletilmesi Kurumumuzun asli yükümlülüğüdür. Ancak bu noktada belirtilmesinde fayda görülmektedir ki, ilgili mevzuat hükümleri çerçevesinde Kurumumuz çağdaş hukuk düzenlerinde yürürlükte bulunan kişisel verilerin korunması ile ilgili düzenlemeler ve bunlara ilişkin uygulama ile aynı doğrultuda etkinlik göstermektedir.

Öte yandan, çeşitli özel sektör temsilcileri ve akademik kuruluşlardan Kanun ve ilgili ikincil mevzuatın uygulanmasına ve Kurumumuzun yürüttüğü faaliyetlere ilişkin birtakım eleştirilerde bulunulduğu görülmektedir. Söz konusu eleştiriler, çoğulcu bir yaklaşımla kişisel verilerin korunması alanında daha uygulanabilir modellerin oluşturulması imkânını tanıması bakımından Kurumumuz tarafından olumlu karşılanmakla birlikte, ilgililer nezdinde oluşabilecek yanlış anlaşılmanın giderilmesi gerektiği değerlendirilmektedir. Bu Kamuoyu Duyurusu da kişisel verilerin yurt dışına aktarılması özelinde Kurumumuzun çalışmalarını ve bakış açısını ortaya koyarak bu yanlış anlaşılmanın önüne geçilmesi amacıyla yayınlanmaktadır.

a) Kişisel Verilerin Yurt Dışına Aktarımına İlişkin Kanunda Öngörülen Düzenleme

Kişisel verilerin yurt dışına aktarımına ilişkin usul ve esaslar, Kanunun 9 uncu maddesinde düzenlenmekte olup; söz konusu maddede, kişisel verilerin ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamayacağı; ancak Kanunun 5 inci maddesinin ikinci fıkrası ile özel nitelikli kişisel veriler bakımından 6 ncı maddesinin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede yeterli korumanın bulunması halinde; yeterli korumanın bulunmaması durumunda ise Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli korumayı yazılı

olarak taahhüt etmeleri ve Kurulun izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilceği hükme bağlanmıştır.

Kişisel verilerin yurt dışına aktarılması, Kanunun 3 üncü maddesinde yer verilen “kişisel verilerin işlenmesi” tanımında da açıkça belirtildiği üzere bir işleme faaliyetidir. Yani, kişisel verilerin yurt dışına aktarılmasının değıştirme, yeniden düzenleme, kaydetme, depolama ve muhafaza etme gibi diğerk kişisel veri işleme faaliyetlerinden bir farkı bulunmamaktadır. Nitekim özel olarak Kanunun 9 uncu maddesinde düzenlenmiş olsa da ilgili hükümde Kanunun 5 inci ve 6 ncı maddelerinde düzenlenmiş kişisel verilerin işlenme şartlarına atıf yapılmaktadır.

Diğerk taraftan belirtmek gerekir ki, kişisel verilerin yurt dışına aktarımının ayrı bir hükümde düzenlenmiş olmasının ve kişisel veri işleme şartlarından birinin varlığına ek olarak diğerk bazı şartların aranmasının sebebi ilgili kişinin kişisel verilerinin aktarıldığı ülkede de etkin olarak korunabilmesinin sağlanmasıdır. Bu düzenlemeyle yurt dışına aktarılmış kişisel verilerle ilgili olarak, ilgili kişinin sahip olduğu hakları etkin bir şekilde ve Kanunun uygulamasına mümkün olabilecek en yakın seviyede kullanabilmesi ile aktarım yapılacak tarafın başta veri güvenliği olmak üzere ilgili kişiyi korumaya yönelik güvencelerin sağlanması hususunda yükümlü kılınması amaçlanmaktadır. Bu bağlamda, kişisel verilerin yurt dışına aktarımına ilişkin düzenlemeler ve bu düzenlemeler çerçevesinde Kurumumuz tarafından benimsenen yaklaşım ve yürütülen faaliyetler küreselleşme ve teknolojik gelişmeler sonucu her an daha da artan bir miktarda gerçekleşen sınır ötesi aktarımları engellemeyi değil; temel hak ve özgürlüklerin korunması temelinde öngörülebilir ve şeffaf bir aktarım rejimini oluşturmayı hedeflemektedir.

b) Yeterli Koruma Bulunan Ülkelerin (Güvenli Ülkelerin) Belirlenmesi

b-1) İlgili Ülkede Yeterli Koruma Bulunup Bulunmadığına İlişkin Değerlendirme

Kanunun 9 uncu maddesinin üçüncü fıkrasında yeterli korumanın bulunduğu ülkelerin Kurul tarafından belirlenerek ilan edileceği düzenleme altına alınmıştır. Bununla birlikte, anılan maddenin dördüncü fıkrasında, Kurulun yabancı ülkede yeterli koruma bulunup bulunmadığına; Türkiye'nin taraf olduğu uluslararası sözleşmeleri, kişisel verilerin aktarılacağı ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu, kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını değerlendirmek suretiyle karar vereceği hükme bağlanmıştır. Nitekim Kurulun 02.05.2019 tarihli ve 2019/125 sayılı kararı ile de, yeterli korumanın bulunduğu ülkelerin tayininde kullanılmak üzere oluşturulan form Kurumumuz resmi internet sitesinde yayımlanmış olup, söz konusu forma göre yeterli korumanın bulunduğu ülkelerin belirlenmesinde, karşılıklılık durumu, ilgili ülkenin kişisel verilerin işlenmesine ilişkin mevzuatı ve uygulaması, bağımsız veri koruma

otoritesinin bulunup bulunmadığı, kişisel verilerin korunması ile ilgili uluslararası antlaşmalara taraf olma ile uluslararası kuruluşlara üye olma durumu, Ülkemizin üye olduğu küresel ve bölgesel örgütlere üye olma durumu ve ilgili ülke ile yürütülen ticaret hacmi gibi kriterlerin dikkate alınacağı belirtilmiştir.

Kurul tarafından yeterli koruma bulunup bulunmadığına ilişkin yapılacak değerlendirme; çeşitli ve birbirinden oldukça farklı ulusal hukuk düzenlerinin varlığı, değerlendirmeye konu ülkede genel nitelikte bir veri koruma düzenlemesinin bulunmaması veya yalnızca belirli alanları kapsayan düzenlemelerin bulunması ve federal devletlerde eyaletler arasındaki farklılıklar göz önünde bulundurulduğunda titizlikle yürütülmesi gereken yoğun ve uzun bir süreç sonrasında sonuçlandırılabilir (Madde 29 Çalışma Grubu, Working Document Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive, s. 26, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf). Öte yandan, “yaşayan” birer doküman olarak nitelendirilebilecek yeterlilik kararları, periyodik gözden geçirmelere tabi tutulacak ve değişen koşullara göre söz konusu yeterlilik kararları değiştirilebilecek, askıya alınabilecek veya kaldırılabilir. Dolayısıyla, güvenli ülke statüsü tayini, ilgili ülke ile yakın işbirliği ve diyalog mekanizmalarının kurulmasını içeren, kapsamlı ve çok boyutlu değerlendirmelerin yapılması ile sağlanan koruma düzeyinin sürekliliğinin takip edilmesini gerektiren dinamik bir süreci ifade etmektedir (Avrupa Komisyonu, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Exchanging and Protecting Personal Data in a Globalised World, s. 8-9, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN>).

b-2) Güvenli Ülke Statüsünün Karşılıklı Olarak Tanınmasının Önemi

Kanunun 9 uncu maddesinin dördüncü fıkrasının (b) bendi uyarınca Kurul, yabancı ülkede yeterli koruma bulunup bulunmadığına ilişkin yapacağı değerlendirmede ilgili ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu dikkate alacaktır. Bu noktada belirtmek gerekir ki, Dışişleri Bakanlığı ile güvenli ülke statüsü tayinine ilişkin yapılan bütün yazışmalarda mütekabiliyet hususu ön plana çıkmakta ve yürütülecek müzakerelerin her hal ve şartta karşılıklı yeterlilik kararı verilmesi üzerine olması gerektiği vurgulanmaktadır.

Öte yandan, kişisel verilerin korunması bakımından güvenli ülke statüsünün değerlendirmeye konu ülke ile karşılıklı olarak tanınması Ülkemizde faaliyet gösteren veri sorumlusu ve veri işleyenlerin kişisel verilerin güvenli, maliyetsiz ve hızlı bir biçimde aktarım olanağından aynı şekilde

yararlanabilmeleri, ekonomik kazanç sağlayabilmeleri ve bu anlamda tek taraflı bir tanınmanın yaratacağı asimetri nedeniyle dezavantajlı konumda bulunmamaları için de büyük bir önem arz etmektedir.

b-3) Kurumumuz Tarafından Yürütülen Güvenli Ülke Statüsü Tayini Çalışmaları

Hâlihazırda güvenli ülke statüsü tayini için diğer devletlerden Kurumumuza iletilmiş herhangi bir talep bulunmamakla birlikte, mevcut ve potansiyel ticari ilişkiler, coğrafi ve/veya kültürel bağlar ve siyasi/diplomatik ilişkiler dikkate alınarak çeşitli ülkelerle görüşmeler gerçekleştirilmekte ve bu kapsamda çalışmalar yoğun bir şekilde sürdürülmektedir. Diğer taraftan, diğer kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri ve diğer paydaşlar tarafından hakkında yeterlilik kararı verilmesinin yararlı olacağı değerlendirilen ülkelere ilişkin önerilerde bulunulması halinde Kurumumuz çalışmalarını uygun düştüğü ölçüde yönlendirmektedir. Ayrıca belirtmek gerekir ki, güvenli ülke statüsü tayinine ilişkin çalışmalar Adalet Bakanlığı, Dışişleri Bakanlığı ve Ticaret Bakanlığı ile yakın iş birliği içerisinde yürütülmektedir. Bu çerçevede; Kurumumuz tarafından güvenli ülke statüsü tayini ile ilgili olarak muhtelif ülkelerle görüşmelerimiz devam etmekte olup, Avrupa Birliği (AB) ile hem resmi hem de gayri resmi nitelikte yapılan görüşmeler kapsamında gerek karşılıklı yeterlilik kararı verilmesi gerek Ülkemizde yürürlükte olan kişisel verilerin korunması mevzuatının AB müktesebatına uygun olarak güncellenmesi konularında istişarelerde bulunulmaktadır. Bununla birlikte, Kurumumuz üye devletler adına yeterlilik kararı vermeye yetkili Avrupa Komisyonunun ve Avrupa Komisyonuna yeterli koruma değerlendirmesi hususunda görüş veren Avrupa Veri Koruma Kurulunun konuya ilişkin çalışmalarını ve dokümanlarını yakından takip etmekte ve bu süreçte tesis edilen yeterlilik kararlarını inceleyerek potansiyel müzakereler için hazırlıklarını tamamlamaktadır. Bu kapsamda, Kurumumuz; ilgili diğer kamu kurum ve kuruluşları ile koordinasyon içerisinde Avrupa Komisyonu ile karşılıklı güvenli ülke görüşmelerinin yürütülebilmesi için gerekli her türlü tedbiri almış durumdadır.

b-4) Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (108 sayılı Sözleşme)

b-4-1) 108 sayılı Sözleşmenin 12 nci maddesinin Ülkemizdeki uygulamasına ilişkin olarak:

Bilindiği üzere, 108 sayılı Sözleşmenin “Kişisel verilerin sınır ötesi akışı ve iç hukuk” başlıklı 12 nci maddesi,

“1) Otomatik işleme konu olan veya otomatik işleme konu olmak üzere toplanmış kişisel verilerin her türlü yoldan ulusal sınırların ötesine transferinde aşağıdaki hükümler uygulanır.

2) Bir Taraf, münhasıran özel yaşamın korunması amacıyla kişisel verilerin diğer bir Tarafa sınır ötesi akışını yasaklayamaz veya özel müsaadeye tabi tutamaz.

3) Bununla birlikte her bir Taraf, 2 nci fıkradaki hükümlere aşağıdaki durumlarda istisna getirebilir:

a) Kendi mevzuatının, belli kişisel veri veya otomatik kişisel veri dosyası kategorileri için, bu verilerin veya dosyaların doğasından kaynaklanan özel düzenlemeler içermesi, diğer Tarafın düzenlemelerinin ise eşdeğer bir koruma içermemesi durumunda;

b) Bu transferin bir Tarafın ülkesinden, bir diğer taraf üzerinden Taraf olmayan bir devletin ülkesine yapılması durumunda, bu bendin başında atıfta bulunulan Tarafın mevzuatının boşluklarından yararlanmak üzere yapılacak bu tür transferleri engellemek amacıyla."

hükümünü amir bulunmakta olup, düzenlemede Sözleşmeye taraf devletlerin yalnızca özel hayatın korunması gerekçesiyle diğer taraf devletlere gerçekleştirilecek kişisel veri aktarımlarını yasaklayamayacakları veya özel bir izin mekanizması öngörmek suretiyle kısıtlayamayacakları öngörülmüştür. 108 sayılı Sözleşmeye ilişkin Açıklayıcı Raporda da (Rapor) hükmün ikinci fıkrasında yer alan düzenlemenin amacının, Sözleşmeye taraf ülkelerin kişisel verilerin korunması bakımından yeterli düzeyde güvenceleri sağladığı yönündeki ön kabulden hareketle taraf ülkeler arasında veri akışının kolaylaştırılması olduğu belirtilmiştir. Bununla birlikte, hükmün taraf devletler arasındaki veri akışının bildirim tabi kılınmasına veya tarafaların iç hukuklarında belirli durumlarda yurt içinde veya sınıraşan nitelikte aktarımları yasaklamaya yönelik düzenlemeler yapabilmeye imkânını ortadan kaldırmadığı açıklaması da yapılmıştır (Avrupa Konseyi, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Paragraf 67. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900016800ca434>).

Öte yandan, Kanununun 9 uncu maddesinin dördüncü fıkrasının (a) bendinde Kurulun veri aktarımına izin verip vermeyeceğine ilişkin yapacağı değerlendirmede Ülkemizin taraf olduğu uluslararası sözleşmelerin dikkate alınacağı hükme bağlanmıştır. Bu anlamda, kişisel verilerin aktarılacağı ülkenin 108 sayılı Sözleşmeye taraf olmasının Kurulun değerlendirmesine esas teşkil edecek unsurlardan biri olduğu anlaşılmaktadır. Nitekim 108 sayılı Sözleşmeye taraf olma durumu, yeterli korumanın bulunduğu ülkelerin Kurulca belirlenmesinde kullanılmak üzere Kurulun 02/05/2019 tarihli ve 2019/125 Kararında kabul edilen kriterler arasında da yer almaktadır. Bununla birlikte, maddede aktarıma konu kişisel verilerin niteliği ile işleme amaç ve süresi, aktarımın yapılacağı ülkedeki veri koruma mevzuatı ve uygulaması ve bu ülkedeki veri sorumlusu veya veri işleyenin taahhüt edeceği önlemler gibi özellikle kişisel verilerin etkin bir biçimde korunmasını sağlamaya

yönelmiş hususlar ile Ülkemiz ile aktarımın yapılacağı ülke arasında veri aktarımına ilişkin karşılıklılık durumunun da Kurulun değerlendirmesinde göz önünde bulundurulacağı düzenlenmiştir.

Bu çerçevede, yukarıda belirtildiği üzere, sözleşmeye taraf devletlerin iç hukuklarında belirli durumlarda yurt dışına veri aktarımını yasaklamaya yönelik düzenleme yapabileceğine ilişkin Raporda yer alan açıklama ve Kurulun yabancı ülkede yeterli koruma bulunup bulunmadığına ilişkin yapacağı değerlendirmede hem 108 sayılı Sözleşme gibi Ülkemizin taraf olduğu uluslararası sözleşmeleri hem de kişisel verilerin korunması veya özel hayatın gizliliğini koruma amacını taşımadan aktarımın yapılacağı ülke ile karşılıklılık halini değerlendireceğine ilişkin Kanunun 9 uncu maddesinde yer verilen düzenleme dikkate alındığında Kanunda öngörülen kişisel veri aktarım rejiminin 108 sayılı Sözleşme ile uyumlu olduğu açıktır.

b-4-2) 108 sayılı Sözleşmenin 12 nci maddesinin AB'deki uygulamasına ilişkin olarak:

AB hem mülga 95/46/AT sayılı Direktif hem de Gerçek Kişilerin Kişisel Verilerin İşlenmesi Bakımından Korunması ve Bu Verilerin Serbest Dolaşımı Hakkında ve 95/46/AT sayılı Direktifi Yürürlükten Kaldıran 27/04/2016 tarihli ve (AB) 2016/679 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (**Genel Veri Koruma Tüzüğü-GVKT**) hükümleri uyarınca 108 sayılı Sözleşmeye taraf olan ülkeleri herhangi başka bir değerlendirmede bulunmadan yeterli korumaya sahip ülke olarak nitelendirmemekte ve Sözleşmeye taraf olmayı yalnızca yeterlilik değerlendirmesinde dikkate alacağı bir kriter olarak kabul etmektedir. Nitekim 108 sayılı Sözleşmeye taraf olsa dahi bir ülkenin ancak yeterli koruma sağlayıp sağlamadığına ilişkin hakkında yapılacak ayrı bir değerlendirme sonrasında güvenli ülke olarak ilan edildiği görülmektedir(*Örnek: İsviçre*). Öte yandan AB, 108 sayılı Sözleşmeye ek Denetleyici Makamlar ve Sınırışan Veri Akışına İlişkin Protokolün yürürlüğe girmesinden sonra da Sözleşmeye ve Protokole taraf ülkeler için aynı süreci işletmiştir (*Örnek: Andorra*).

Kurulun "Kişisel verilerin 108 sayılı Sözleşme dayanak gösterilerek yurt dışına aktarılması" hakkında 22.07.2020 tarihli ve 2020/559 sayılı Kararında yukarıdaki değerlendirmeler çerçevesinde 108 sayılı Sözleşmenin 12 nci maddesi hükmünü gerekçe göstererek Kanunun 9 uncu maddesinin ikinci fıkrası uyarınca aktarım tarafları arasında düzenlenmiş yazılı bir taahhütnamenin ve Kurulun izninin bulunmaması nedeniyle yurt dışına kişisel veri aktarımını gerçekleştiren bir veri sorumlusu hakkında idari para cezasına hükmedilmiştir. Ancak belirtilmesinde fayda görülmektedir ki, söz konusu karar birtakım eleştirilerde ifade edildiği gibi yurt dışına veri aktarımını imkânsız hale getirmemektedir. Kararla, Ülkemizin taraf olduğu 108 sayılı Sözleşme ve Sözleşmeye Ek Protokolün uygulamasına Kurumumuzun yaklaşımı açıklanmakta ve 108 sayılı Sözleşmeye taraf olma durumunun Kurumumuz tarafından güvenli ülke statüsü tayini için yeterli olmadığı vurgulanarak veri

sorumlularının Kanunun 9 uncu maddesi uyarınca yazılı bir korumayı taahhütte bulunarak kişisel veri aktarımlarını gerçekleştirmeleri gerektiği belirtilmektedir.

c) Yeterli Koruma Bulunmayan Ükelere Kişisel Veri Aktarımı

Kanunun 9 uncu maddesinin ikinci fıkrasının (b) bendi kapsamında yeterli korumanın bulunmadığı ülkelere aktarımın gerçekleştirilebilmesi için aktarım taraflarının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun aktarıma izin vermesi gerekmektedir. Kurul öncelikle, yurt dışına kişisel veri aktarımında veri sorumlusu tarafından hazırlanacak taahhütnamelerde yer alacak asgari unsurları belirlemiştir. Daha sonrasında ise çok uluslu şirket topluluklarını oluşturan şirketler arasında gerçekleştirilecek topluluk içi aktarımlarda Bağlayıcı Şirket Kuralları alternatif bir yeterli koruma sağlama yolu olarak belirlenmiştir.

c-1) Taahhütnameler

Kurumumuz tarafından hem veri sorumlusundan veri sorumlusuna hem de veri sorumlusundan veri işleyene gerçekleştirilecek yurt dışına kişisel veri aktarımlarında kullanılmak üzere iki tür taahhütname hazırlanmıştır. Ancak, Kurumumuza veri sorumluları tarafından yapılan başvurularda taahhütnamelerin ekinde yer alan söz konusu kişisel veri aktarımının dayandığı işleme şartına, amacına, aktarıma konu veri kategorilerine, veri konusu kişi grubuna veya gruplarına, aktarım yapılacak tarafın alacağı idari ve teknik tedbirlere ve saklama süresi gibi unsurlar ile ilgili açıklamaların aktarıma izin verilip verilmeyeceğine ilişkin değerlendirmeye esas teşkil edilebilecek detayda ve açıklıkta olmadığı görülmüştür. Ayrıca, yapılan başvuruların idari makamlara yapılacak başvurularda riayet edilmesi gereken usul ve esaslara uygun olmadan gerçekleştirildiği tespit edilmiştir. Bunun üzerine bahse konu taahhütnamelerin hazırlanmasında veri sorumluları tarafından dikkat edilmesi gereken gerek usule gerek esasa ilişkin hususlar ile ilgili detaylı bir kamuoyu duyurusu hazırlanarak Kurumumuzun resmi internet sitesinde yayımlanmıştır.

Diğer taraftan belirtmek gerekir ki, yurt dışına kişisel veri aktarımı gerçekleştirmek amacıyla yapılan başvurular, Kurumumuzun ilgili tüm birimleri tarafından hem hukuki hem teknik boyutlarıyla titizlikle incelenmekte ve mümkün olan en kısa süre içerisinde başvuruculara geri dönüş yapılarak eksikliklerin tamamlanması veya düzeltmelerin yapılması için ek süre tanınmaktadır. Bu anlamda, başvurucular desteklenmekte ve iş süreçlerinin aksamaması adına gerekli yönlendirmeler yapılmaktadır. Dolayısıyla, Kurumumuzun taahhütnamelerin onaylanması ve aktarıma izin verilmesi sürecinde zorlaştırıcı bir yaklaşım benimsediği eleştirisi gerçeği yansıtmamaktadır.

c-2) Bağlayıcı Şirket Kuralları

Kurumumuz tarafından veri sorumlularının organizasyonlarının ve iş süreçlerinin farklılık gösterdiği dikkate alınarak kişisel verilerin yurt dışına aktarılabilmesi için uygun güvencelerin oluşturulması gereğini karşılayacak alternatif bir yöntem olarak Bağlayıcı Şirket Kuralları oluşturulmuştur. Bu kapsamda, çok uluslu grup şirketleri arasında yapılacak aktarımlarda kullanılacak Bağlayıcı Şirket Kurallarına ilişkin başvuru formu ve Bağlayıcı Şirket Kurallarında bulunması gereken temel hususlara ilişkin yardımcı doküman yayımlanarak ilgililerin kullanımına sunulmuştur. Çok uluslu grup şirketlerinin, kendilerine özgü yapılarına, ihtiyaçlarına ve faaliyet gösterdikleri sektörün gereklerine uygun olarak hazırladıkları ve birbirleri arasında gerçekleştirilecek yurt dışına veri aktarımlarında uymayı taahhüt ettikleri kuralların Kurul tarafından uygun bulunması halinde Kanunun 9 uncu maddesinin ikinci fıkrasının (b) bendinde düzenlenmiş yeterli korumayı taahhüt etme yükümlülüklerini yerine getirmiş olacaklardır. Ayrıca belirtmek gerekir ki, söz konusu yöntem AB’de kişisel verilerin korunmasında temel düzenleme niteliği haiz Genel Veri Koruma Tüzüğünde de hakkında yeterlilik kararı verilmemiş ülkelere yapılacak aktarımlarda kullanılacak uygun güvenlik düzeyini sağlama yöntemlerinden biri olarak öngörülmektedir.

d) Kişisel Verilerin Yurt Dışına Aktarımına İlişkin Diğer Kanunlarda Öngörülen Düzenlemeler

Kanunun 4 üncü maddesinin birinci fıkrası “Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.” hükmünü amirdir. Bu anlamda, Kanun çerçeve düzenleme niteliğini haiz olarak yurt dışına aktarım dâhil olmak üzere kişisel verilerin işlenmesine ilişkin temel usul ve esasları belirlemekte; sektörlere ilişkin farklı düzenlemelerin bulunması halinde bu düzenlemeleri tamamlayıcı bir rol üstlenmektedir. Diğer bir deyişle, farklı alanlarda sürdürülen kişisel veri işleme faaliyetlerinin tabi olduğu kanuni düzenlemeler Kanun ile beraber uygulanmakta ve bu şekilde söz konusu faaliyetlerin kendine özgü yapısından kaynaklanan gereklilikler de yerine getirilmiş olmaktadır. Kurumumuz da bütüncül bir bakış açısıyla hem mevzuatı tümüyle göz önünde bulundurarak hem de söz konusu kişisel veri işleme faaliyeti özelinde dikkate alınması gereken diğer unsurları tespit ederek faaliyetlerini yürütmektedir.

Yine Kanunun 9 uncu maddesinin altıncı fıkrasında “Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.” düzenlemesine yer verilmiştir. Anayasanın 90 ıncı maddesinin beşinci fıkrasında ise; “Usulüne göre yürürlüğe konulmuş milletlerarası antlaşmalar kanun hükmündedir. (...)” denilmek suretiyle milletlerarası antlaşmaların usulüne uygun olarak iç hukukumuza dâhil edilmesi halinde kanun hükmünde sayılacağı açıkça düzenlenmiştir. Bu çerçevede, kanunlarda ve usulüne göre yürürlüğe konulmuş milletlerarası antlaşmalarda kişisel verilerin yurt dışına aktarımına ilişkin bir düzenlemenin mevcut olması halinde, bu düzenlemeye

göre hareket edilecektir. Nitekim Kurulun bankacılık sektörüne ilişkin olarak vermiş olduğu bir kararında 5411 sayılı Bankacılık Kanununun 73 üncü maddesinde öngörülen düzenleme çerçevesinde yapacağı aktarımların Kanunun diğer hükümleri ile bağlı kalınmak şartıyla Kanunun 9 uncu maddesinin altıncı fıkrası uyarınca gerçekleştirilebileceği ifade edilmiştir.

SONUÇ

Kişisel verilerin korunmasını isteme hakkı, Anayasanın “Temel Haklar ve Ödevler” başlıklı ikinci kısmının “Kişinin Hakları ve Ödevleri” başlıklı ikinci bölümünde yer alan 20 nci maddenin üçüncü fıkrasında,

“IV. Özel hayatın gizliliği ve korunması

A. Özel hayatın gizliliği

Madde 20 - ...

(Ek fıkra: 7/5/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.”

şeklinde düzenlenerek bir temel hak ve özgürlük olarak tanınmıştır. Bu anlamda, Kurumumuz her geçen gün daha fazla tehdit altında olan bir temel hak ve özgürlüğün korunması amacına hizmet etmektedir. Diğer ülkelerde faaliyet gösteren veri koruma otoriteleri gibi Kurumumuz da bu bilince sahip olarak kişisel veri işleme faaliyetinde bulunan aktörleri eğitici ve yönlendirici çalışmalarda bulunmakla birlikte gereken durumlarda bir kanun uygulayıcısı olarak bu aktörler hakkında idari yaptırım da tesis etmekte olup, Kurumumuzun sürdürdüğü faaliyetler bireyleri en üst düzeyde korumaya yönelmiş bulunmaktadır. Bununla birlikte, teknolojik gelişmeler sonucu ortaya çıkan olanaklardan Ülkemizin de faydalanabilmesi adına söz konusu gelişmeler takip edilerek kişisel verilerin korunması hukukuna uygun şekilde uygulamaların geliştirilmesine de katkı sağlanmaya çalışılmaktadır. Bu kapsamda, kişisel verilerin yurt dışına aktarılmasına ilişkin olarak Kurumumuzca yürütülen güvenli ülke çalışmaları devam etmektedir. Bu noktada önemle ifade etmek gerekir ki, kamuoyunda sorun olarak görülen yurt dışına veri aktarımında Kurul’un iznini öngören süreç, Kanunun 9 uncu maddesinde emredici bir şekilde hükme bağlanan düzenlemenin bir sonucudur.

Kamuoyuna saygı ile duyurulur.

01.10.2020 - Sicile Kayıt Yükümlülüğü

Sicile Kayıt Yükümlülüğü Hakkında Kamuoyu Duyurusu

Yayınlanma Tarihi : 01.10.2020

Bilindiği üzere 6698 sayılı Kişisel Verilerin Korunması Kanununa (Kanun) göre kişisel verileri işleyen gerçek ve tüzel kişilerin Veri Sorumluları Siciline (Sicil) kayıt olması gereken tarihler Kişisel Verileri Koruma Kurulunca (Kurul) ilan edilmiştir.

Başkanlığımızca Hazine ve Maliye Bakanlığından elde edilen 2019 yılı verilerine göre yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olduğu görülmesine rağmen 01.10.2020 tarihi itibarıyla henüz Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) kayıt başvurusunda bulunmayan veya başvuruda bulunduğu halde bildirimini tamamlamayan veri sorumlularının olduğu tespit edilmiştir.

Bu tesbite istinaden Kişisel Verileri Koruma Kurulu tarafından yapılan inceleme ve değerlendirme sonucunda; COVID-19 ile mücadele kapsamında fiili, teknik ya da hukuki imkânsızlık nedeniyle bazı veri sorumlularının Sicile kayıt yükümlülüğünü yerine getiremediği göz önüne alınarak, Veri Sorumluları Sicili Hakkında Yönetmeliğin 8 inci maddesi uyarınca ve Kanunun Geçici 1 inci maddesiyle Kurula verilmiş olan yetki çerçevesinde, Sicile kayıt yükümlülüğünü yerine getirmemiş olan veri sorumlularına bu durumun bir yazı ile bildirilmesi Kurulun 01.10.2020 tarihli ve 2020/760 sayılı kararı ile uygun bulunmuştur.

Söz konusu yazıyla Kurul tarafından kendilerine bildirilen süre içerisinde, ilgili veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmeleri gerekmektedir.

Kamuoyuna saygıyla duyurulur.

NOT: VERBİS'e kayıt işlemleri halen devam etmektedir.

17.07.2020 - Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına Yönelik Talepler

Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına Yönelik Talepler Hakkında Kamuoyu Duyurusu

Yayınlanma Tarihi : 17.07.2020

Kurumumuza ilgili kişilerin ad ve soyadları ile arama motorları üzerinden yapacakları aramalar neticesinde çıkan sonuçların indekslenmeyecek şekilde teknik düzenlemeye tabi tutulması hususunda iletilen ve “Unutulma Hakkı” kapsamında değerlendirilmesi talep edilen başvuruların Kişisel Verileri Koruma Kurulu tarafından değerlendirilmesi neticesinde Kurulun 23.06.2020 tarih ve 2020/481 sayılı Kararı ile;

- Kurumumuza intikal eden başvurulara konu “Unutulma Hakkı”nın bir üst kavram olarak ele alınmak suretiyle Anayasanın 20 nci maddesinin üçüncü fıkrası hükmü ile 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 4 üncü, 7 nci ve 11 inci maddelerinde ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 8 inci maddesinde yer verilen düzenlemeler çerçevesinde değerlendirildiğine,
- Kurumumuza yapılan başvurularda yer verilen arama motorlarından ad ve soyadı ile yapılan aramalarda kişinin kendisiyle bağlantılı sonuçlara ulaşılmamasını isteme hakkının indeksten çıkarılma talebi olarak nitelendirildiğine,
- Arama motorlarının, üçüncü taraflara ait internette topladıkları verilerin işlenmesinin amaç ve vasıtalarını belirledikleri göz önünde bulundurularak Kanunun 3 üncü maddesinde yer verilen tanım çerçevesinde veri sorumlusu olarak kabul edilmesine,
- Arama motorunun işletmecisinin otomatik, düzenli ve sistematik olarak internette yayınlanan bilgiyi bulduğu, daha sonra kendi indeksleme programları çerçevesinde alıp, kaydedip, organize ettiği kişisel verileri arama sonuçlarının listesi formunda düzenlediği, sunucuları üzerinde sakladığı, belirli durumlarda açıkladığı ve kullanıcılarına sunduğu dikkate alındığında arama motorları tarafından gerçekleştirilen faaliyetlerin Kanunun 3 üncü maddesi kapsamında ‘kişisel veri işleme’ faaliyeti olarak değerlendirilmesine,

- Kanunun başvuru ve şikâyet hakkına ilişkin hükümlerinde belirtilen usul ve süreler esas alınarak ilgili kişilerin, arama sonuçlarının indeksten çıkarılmasına yönelik talepleri ile ilgili olarak öncelikle arama motorlarına başvuruda bulunmaları, veri sorumlusu arama motorlarının söz konusu talepleri reddetmeleri veya başvuru sahibine cevap vermemeleri halinde ilgili kişilerce Kurula şikâyette bulunabileceklerine,
- İlgili kişilerce yapılacak başvurunun şekli ve istenilecek bilgi ve belgelerin arama motorları tarafından belirleneceğine,
- İlgili kişinin arama motorları üzerinden kendi adı ve soyadı ile yapacağı bir arama sonucunda gösterilen sonuçların indeksten çıkarılmasına yönelik yapılacak değerlendirmede, ilgili kişinin temel hak ve özgürlükleri ile kamunun söz konusu bilgiyi edinmesinden sağlayacağı menfaatler arasında bir denge testi yapılmasına, yarışan menfaatlerden hangisinin ağır bastığının gözetilmesine ve bu değerlendirme yapılırken öncelikli olarak aşağıda belirtilen linkte yer verilen açıklamaların dikkate alınmasına ancak bu konudaki şikâyetlerin değerlendirme sürecinde dikkate alınacak kriterlerin bunlarla sınırlı olmayacağına, her somut olay özelinde Kurulca ilave ölçütlerin de gündeme gelebileceğine,
- İlgili kişilerin, arama motorları üzerinden kendi ad ve soyadları ile yapılacak aramalar neticesinde gösterilen sonuçların indeksten çıkarılmasına yönelik taleplerinin veri sorumlusu arama motorları tarafından reddedilmesi veya taleplerine cevap verilmemesi halinde Kurula başvuruda bulunulurken aynı zamanda doğrudan yargı yoluna başvurmalarının da mümkün bulunduğuna,
- Bu kararda yer alan usul ve esasların arama motoru işleticisi şirketlere bildirilmesine ve ilgili kişilerce internet siteleri üzerinden unutulma hakkının uygulanabilmesini teminen iletişim kanallarının ülkemiz vatandaşları tarafından da kullanılabilmesine yönelik gerekli aksiyonların alınmasının sağlanmasına

karar verilmiştir.

Kamuoyuna saygı ile duyurulur.

23.06.2020 - VERBİS'e Kayıt Sürelerinin Uzatılması

VERBİS'e Kayıt Sürelerinin Uzatılması Hakkında Duyuru

Yayınlanma Tarihi : 23.06.2020

Tüm dünyada olduğu gibi ülkemizde de etkisini gösteren Covid-19 virüs salgını nedeniyle bazı işyerlerinin fiziksel olarak kapalı olduğu veya uzaktan / dönüşümlü çalışma modeli uygulandığı, bu nedenle veri sorumlularınca kişisel veri işleme envanteri hazırlama çalışmalarının yapılamadığı ve Veri Sorumluları Siciline (Sicil) kayıt yükümlülüğünün süresinde yerine getirilemediği gerekçesiyle Sicile kayıt sürelerinin uzatılmasına ilişkin Türkiye Odalar ve Borsalar Birliği (TOBB) ile muhtelif sektör temsilcileri tarafından Kuruma intikal ettirilen taleplerin değerlendirilmesi neticesinde Kişisel Verileri Koruma Kurulunun 23/06/2020 tarihli ve 2020/482 sayılı Kararı ile;

- Yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları ile yurtdışında yerleşik gerçek ve tüzel kişi veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmeleri için belirlenen sürenin 30.09.2020 tarihine,
- Yıllık çalışan sayısı 50'den az ve yıllık mali bilançosu 25 milyon TL' den az olup ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek ve tüzel kişi veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.03.2021 tarihine,
- Kamu kurum ve kuruluşu veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.03.2021 tarihine,

kadar uzatılmasına,

- Anılan kararın Kurum internet sayfasında duyurulması ve Resmi Gazete'de yayımlanmasına oybirliği ile karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

07.05.2020 - Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlar

Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyuru

Yayınlanma Tarihi : 07.05.2020

A-USULE İLİŞKİN DİKKAT EDİLMESİ GEREKEN HUSUSLAR

1. Kurumumuza, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 9 uncu maddesinin (2) numaralı fıkrasının (b) bendi uyarınca yapılacak yurt dışına veri aktarımı izin başvurularında, başvuruya yetkili kişinin adı soyadı, adresi, imzası gibi hususlarla birlikte imzaya yetkili olduğuna dair tevsik edici belgelerin de eklenmesi gerekmektedir. Bu kapsamda, tüzel kişiler tarafından yapılacak başvuruların, ilgili veri sorumlusunu bu konuda temsil ve ilzama yetkili kişiler tarafından yapılması ile başvuruya bu hususu tevsik edici belgelerin eklenmesi; ayrıca, vekil marifetiyle yapılacak başvurularda da vekâletname aslı veya onaylı örneğinin bulunması gerekmektedir.
2. Taahhütname ve ekinin sonunda imza ve kaşe; her bir sayfasında ise imzacıların parafı bulunmalıdır.
3. İmzacıların yetkisini göstermesi bakımından, Taahhütname ekine Türkiye’de mukim şirketler bakımından imza sirkülerinin aslı veya onaylı örneği, Yabancı Resmî Belgelerin Tasdiki Mecburiyetinin Kaldırılması Sözleşmesine taraf olan ülkelerde mukim veri alıcısı bakımından ise imzalayanın imzaya yetkili olduğunu gösterir apostil şerhli belgenin aslı veya onaylı örneği eklenmelidir. Anılan Sözleşmeye taraf ülkelerin resmi makamlarınca hazırlanmış her belgede apostil şerhi bulunmalı, Sözleşmeye taraf olmayan ülkeler bakımından ise, belgelerin Türkiye’de hukuken geçerli olmasına ilişkin süreç işletilmelidir.
4. Yabancı dildeki her belgenin noter onaylı çevirisi bulunmalıdır.
5. Taahhütname hazırlanırken, Kurumumuz resmi internet sitesinde yayımlanan Taahhütname örneklerinde yer alan (Veri Sorumlusundan Veri Sorumlusuna Aktarım, Veri Sorumlusundan Veri İşleyene Aktarım) hükümlere asgari olarak aynen yer verilmeli, ilave hükümlere yer verilecek olması halinde ise, bu hükümlere “İlave Hükümler” başlığı altında ayrıca yer verilmelidir.

Taahhüt içeren cümlelerde gelecek zaman kullanılmalıdır. Örneğin “Veri aktaran, veri alıcısına; aktarılan kişisel verilerin 6698 sayılı Kanun ile bu sözleşme hükümlerine uygun olarak işleneceğini bildirecektir.” Gibi.

B-ESASA İLİŞKİN DİKKAT EDİLMESİ GEREKEN HUSUSLAR

I. Taahhütname Düzenlenirken Dikkat Edilmesi Gereken Hususlar

1. Aktarımın tarafları arasındaki ilişki doğru bir şekilde belirlenmeli ve alıcı tarafın niteliğine göre Kurumumuz resmi internet sitesinde yayımlanan Taahhütname örneklerinden uygun olan kullanılmalıdır.

2. Kanunun 3 üncü maddesinin birinci fıkrasının (1) bendi uyarınca veri sorumlusu; kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade etmektedir. Bu çerçevede, kişisel verilerin işlenmesine ilişkin kararları alma, işleme faaliyetinin amacı, bu faaliyetin ne zaman başlayacağı kimler tarafından gerçekleştirileceği ve benzeri hususlarda karar verme yetkisi veri sorumlusuna aittir. Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen veri sorumlusu, veri işleme faaliyetinin temel araçlarını ve amaçlarını; veri işlemenin “neden” ve “nasıl” olacağını belirlemektedir. Diğer bir deyişle, teknik ve organizasyona ait araçların belirlenmesi, veriye kimin erişeceği, hangi verilerin işleneceği, bu verilerin ne kadar süre tutulacağı, ne şekilde saklanacağı gibi veri işlemeye ilişkin temel unsurlar veri sorumlusu tarafından belirlenmektedir. Bununla birlikte veri sorumlusu, kişisel verilerin korunmasına yönelik mevzuata uyumla ilgili tedbirlerin alınmasından, veri işleyeni denetimden ve ilgili kişilerin haklarını kullanabilmesini sağlamaktan sorumludur. Veri sorumlusunun özerk ve bağımsız olması da önem arz etmektedir. Veri sorumlusu kimseden emir ve talimat almayan, bilakis bir başka kişiye veri işletmesi halinde bu hususta emir ve talimat veren, veri işleme süreçlerinin her anında serbestçe karar verme yetkisine sahip olan gerçek veya tüzel kişilerdir.

Veri işleyen ise, Kanunun 3 üncü maddesinin birinci fıkrasının (ğ) bendinde “Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi” olarak tanımlanmıştır. Veri işleyen faaliyetleri, veri işlemenin daha çok teknik kısımları ile ilgilidir. Kişisel verilerin işlenmesine ilişkin kararların alınması yetkisi ise veri sorumlusuna aittir. Veri işleyen, veri sorumlusu adına kişisel verileri işlemekte olup, veri sorumlusunun belirlemiş olduğu temel amaç ve araçlar kapsamında ve veri sorumlusunun verdiği yetki doğrultusunda veri işleme faaliyetini gerçekleştirmektedir. Diğer bir deyişle veri işleyen, veri sorumlusunun çıkarlarını gözetken, kendisine verilen belirli görevleri aldığı talimatlar doğrultusunda yerine getirmekle yükümlü olan taraftır.

Yukarıda yer alan açıklamalar ışığında, veri sorumlusundan veri işleyene aktarımlarda, veri sorumlusunun ve veri işleyenin gerçekleştirmekte olduğu hizmetler ile veri aktarımına ilişkin faaliyetlerinin, net bir şekilde anlaşılabilmesini teminen anlaşılır detayda açıklama yapılması gerekmektedir.

Sonuç olarak, veri sorumlusundan veri sorumlusuna veya veri sorumlusundan veri işleyene yapılacak aktarımlarda tarafların hukuki statülerine ilişkin anlaşılır detayda açıklamalara yer verilmesi ve aradaki ilişkiyi gösteren tevsik edici herhangi bir belgenin (sözleşme vb.) bulunması halinde Taahhütname ile gönderilmesi önem arz etmektedir.

3. Kanunda yer alan terminoloji birebir kullanılmalı, yapılacak tanımlar Kanunda ya da ikincil düzenlemelerde yer alan tanımlarla uyumlu olmalıdır.

4. Birbiriyle ilişkili başlıklar arasında bağ kurulmalıdır. Bu anlamda, hangi veri konusu kişi grubunun, hangi kişisel verilerinin, hangi amaca ve hukuki sebebe bağlı olarak aktarılacağı hususu, söz konusu başlıklar arasında bağ kurulmak suretiyle anlaşılır detayda açıklanmalıdır.

5. Açık rıza şartına dayalı gerçekleştirilecek olan yurt dışı kişisel veri aktarımları Taahhütname konusu edilemeyecektir.

6. Kanunun "*Genel ilkeler*" başlıklı 4 üncü maddesinde, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği ve kişisel verilerin işlenmesinde maddede; "*Hukuka ve dürüstlük kurallarına uygun olma, -Doğru ve gerektiğinde güncel olma, -Belirli, açık ve meşru amaçlar için işlenme, -İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, -İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme*" şeklinde sayılan ilkelere uyulmasının zorunlu olduğu düzenleme altına alınmıştır. Diğer bir deyişle, Kanunun 4 üncü maddesinde sayılan genel ilkelerin kişisel veri işleme faaliyetinin tüm süreçlerinde, her hal ve şartta uygulanması hukuki bir gerekliliktir.

Anılan maddenin ikinci fıkrasının (c) bendinde yer alan "*Belirli, açık ve meşru amaçlar için işlenme*" ilkesi, kişisel veri işleme faaliyetlerinin ilgili kişi tarafından açık bir şekilde anlaşılır olmasını, kişisel veri işleme faaliyetinin hangi hukuki işleme şartına dayalı olarak gerçekleştirildiğinin tespit edilmesini, kişisel veri işleme faaliyetinin ve gerçekleştirilme amacının belirliliğini sağlayacak detayda ortaya konulmasını sağlar. Amacın meşru olması, veri sorumlusunun işlediği verilerin, yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması anlamına gelmektedir.

Diğer taraftan, anılan maddenin ikinci fıkrasının (ç) bendinde yer alan “İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması” ilkesine göre ise, işlenen veriler belirlenen amaçların gerçekleştirilmesine elverişli olmalı, amacın gerçekleştirilmesiyle ilgili olmayan veya sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik veri işleme yoluna gidilmemelidir. Burada önemli olan, amacı gerçekleştirmeye yönelik yeterli verinin temin edilmesi, bunun dışındaki amaç için gerekli olmayan veri işlemeden kaçınılmasıdır. Diğer bir deyişle ölçülülük ilkesi, veri işleme ile gerçekleştirilmesi istenen amaç arasında makul bir denge kurulması yani veri işlemenin, amacı gerçekleştirecek ölçüde olması demektir.

Bu çerçevede, Taahhütname ve ekinde yer verilen belgeler düzenlenirken kişisel verilerin işleme amacına ilişkin yukarıda belirtilen ilkeler başta olmak üzere, Kanunun 4 üncü maddesinde yer alan genel ilkelerin gözetilmesi gerekmektedir.

II. EK-1’de Yer Alan Başlıklar Altında Yer Verilen Açıklamalarda Dikkat Edilmesi Gereken Hususlar

1. Veri konusu kişi grubu ve grupları

Veri konusu kişi ve kişi grupları belirtilirken “gibi, ve benzeri, olası, muhtemel, ...” gibi muğlak ifadelerin kullanımından kaçınılmalı; veri konusu kişi grubu ve grupları net bir şekilde ortaya konulmalıdır.

2. Veri kategorileri

“Veri kategorileri” belirlenirken, özellikle Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinin ikinci fıkrasının (ç) bendinde yer alan “İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkesine riayet edilmelidir. Bu anlamda, ancak belirli, açık ve meşru bir veri aktarımı amacıyla bağlantılı, sınırlı ve ölçülü olacak şekilde veri kategorileri belirlenmelidir. Veri kategorileri ifade edilirken muğlak, anlaşılması zor ve geniş ifadelerden kaçınılmalı, kategoriler anlaşılır detayda ortaya konulmalıdır.

Aktarılacak kişisel verilerin, “Veri konusu kişi grubu ve grupları” başlığı ile bağ kurulmak suretiyle, bu başlık altında sayılan kişi gruplarından hangisine ait olduğu açıkça belirtmeli ve herhangi bir muğlak ifadeye yer verilmemelidir.

3. Veri aktarımının amaçları

Veri aktarımının amaçları, “Veri Kategorileri” başlığında belirtilen veri kategorileri ile bağ kurulmak suretiyle açıklanmalıdır. Bununla birlikte, Kanunun 4 üncü maddesine göre kişisel veriler belirli, açık ve meşru amaçlar için işlenmelidir. Belirli, açık ve meşru amaçlar için işleme ilkesi, kişisel veri işleme

faaliyetlerinin ilgili kişi tarafından açık bir şekilde anlaşılır olmasını, kişisel veri işleme faaliyetinin hangi hukuki işleme şartına dayalı olarak gerçekleştirildiğinin tespit edilmesini, kişisel veri işleme faaliyetinin ve gerçekleştirilme amacının belirliliğini sağlayacak detayda ortaya konulmasını sağlar. Amacın meşru olması, veri sorumlusunun işlediği verilerin, yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması anlamına gelmektedir. Bu çerçevede, ilgili bölümde kişisel verilerin işleme amacı sınırları belirli ve açık bir şekilde anlaşılır detayda açıklanmalıdır.

4. Veri aktarımının hukuki sebebi

Taahhütnameye konu kişisel veri aktarım faaliyetinin Kanunun 5 inci maddesinin ikinci fıkrası ile 6 ncı maddesinin üçüncü fıkrasında belirtilen kişisel veri işleme şartlarından hangisine dayalı olarak gerçekleştirildiğinin; “*Veri Kategorileri*” başlığı altında yer verilecek unsurlar ile bağ kurularak, ayrı ayrı gerekçeli ve anlaşılır detayda ortaya konulması gerekmektedir.

Kanunun 6 ncı maddesinin birinci fıkrasında kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerinin özel nitelikli kişisel veri olduğu, ikinci fıkrasında özel nitelikli kişisel verilerin ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğu, üçüncü fıkrasında, birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel verilerin kanunlarda öngörülen hallerde, sağlık ve cinsel hayata ilişkin kişisel verilerin ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgili kişinin açık rızası aranmaksızın işlenebileceği hükme bağlanmıştır. Bu anlamda, sağlık verilerinin ve diğer özel nitelikli kişisel verilerin ilgili kişilerin açık rızası olmaksızın yurt dışına aktarımında öncelikli olarak 6698 sayılı Kanunun 6 ncı maddesinin üçüncü fıkrasında tahdidi olarak sayılan işleme şartlarından birinin mevcut olması gerekmektedir. Bu çerçevede, söz konusu işleme şartlarının mevcut olmadığı durumlarda, özel nitelikli kişisel verilerin yurt dışına aktarımı ancak ilgili kişilerin hukuka uygun bir şekilde açık rızalarının alınması ile mümkün olabilecektir ki, açık rıza şartına dayalı gerçekleştirilecek olan yurt dışı kişisel veri aktarımları Taahhütname konusu edilmemektedir.

“İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması” şartına dayanılarak gerçekleştirilecek aktarımlarda, Kurumumuz resmi internet sitesinde yayımlanan Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/78 sayılı kararında yer verilen denge testi uygulanmalı ve çıkan olumlu sonuç ortaya konulmalıdır. Bu

kapsamda, veri sorumluları tarafından; söz konusu veri işleme/aktarım faaliyetinin ilgili kişilerin temel hak ve özgürlüklerine zarar vermeyeceği hususu, veri işleme/aktarımı dolayısıyla veri sorumlusu olarak ilgili kişinin temel hak ve özgürlükleriyle yarışır düzeyde ne tür bir meşru menfaatin elde edileceği, veri işlemeden/aktarımından elde edilecek meşru menfaatin tesisi için söz konusu veri işleminin/aktarımının neden zorunlu olduğunun her bir veri konusu kişi grubu ve veri kategorisi bakımından somut faaliyet özelinde anlaşılır detayda açıklanması gerekmektedir.

5. Alıcı ve alıcı grupları

“Alıcı ve alıcı grupları”, veri alıcısı tarafından örneğin verilerin ifşası veya aktarılması suretiyle gerçekleştirilecek sonraki devam eden aktarımlarda veri alıcısının bulunduğu ülkede mukim olan veri sorumlusu veya veri işleyeni ifade etmektedir. Ayrıca belirtmekte fayda görülmektedir ki, sonraki devam eden aktarıma taraf veri sorumlularının veri alıcısının mevzuatta öngörülen hukuki yükümlülükleri gereğince aktarım gerektiren yetkili kurum ve kuruluşlar kapsamında olması gerekmektedir. Örneğin, aktarımın gerçekleşeceği ülkede yetkili kamu kurum ve kuruluşları ile mahkemeler bu kapsamda değerlendirilmektedir. Bununla birlikte, yetkili kamu kurum ve kuruluşlarının rekabet, telekomünikasyon otoritesi gibi belirlenebilir olması halinde bunların açıkça ortaya konulması gerekmektedir.

Öte yandan, Taahhütnameye taraf veri alıcısından, alıcının mukim olduğu ülkede yerleşik başka yukarıda belirtilenlerden farklı bir veri sorumlusuna ya da veri alıcısının mukim olduğu ülkeden başka bir ülkede yerleşik veri sorumlusu veya veri işleyene, Taahhütname kapsamında sonraki devam eden veri aktarımı gerçekleşemeyecektir. Bu durumdaki veri sorumluları veya veri işleyenlerle ayrıca taahhütname imzalanması gerekmektedir. Böyle bir durumda, aktarımın amacı ve niteliğine uygun düştüğü ölçüde, farklılıklar varsa bu farklılıklar da her bir veri sorumlusu ya da veri işleyen bakımından açık ve net bir şekilde ortaya konulmak suretiyle tek bir taahhütname metninin veri aktarılan veri alıcısı ile söz konusu veri sorumluları ya da veri işleyenler tarafından birlikte imzalanması da mümkündür.

6. Veri alıcısı tarafından alınacak teknik ve idari tedbirler

İlgili bölüm düzenlenirken, kişisel verilerin işlenmesi sürecinde veri sorumlularının alması gereken teknik ve idari tedbirler konusunda uygulamada açıklık sağlanması ve iyi uygulama örnekleri oluşturması amacıyla hazırlanan ve Kurumumuz resmi internet sitesinde yayımlanan “*Kişisel Veri Güvenliği Rehberi (Teknik Ve İdari Tedbirler)*”nin dikkate alınması, taahhüt edilen teknik ve idari tedbirlerin ayrı başlıklar halinde açıklanarak, bu tedbirlere ilişkin tevsik edici belgelerin de başvuruya eklenmesi gerekmektedir.

7. Özel Nitelikli Kişisel veriler için alınan ek önlemler

İlgili bölüm düzenlenirken, Kişisel Verileri Koruma Kurulunun 31/01/2018 tarihli ve 2018/10 sayılı “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler” başlıklı kararı ile belirlenen ve özel nitelikli kişisel verilerin işlenmesi sırasında alınması zorunlu olan teknik ve idari tedbirlere yer verilmesi ve söz konusu tedbirleri tevsik edici belgelerin de başvuruya eklenmesi gerekmektedir.

8. Veri aktaranın Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) Bilgileri

Kayıt yükümlülüğünün bulunup bulunmadığı bilgisinin gerekçesi ile birlikte açıklanması ve kayıt yükümlülüğünün bulunması halinde VERBİS bilgilerine bu başlık altında yer verilmesi gerekmektedir.

9. Ek faydalı bilgiler

Saklama süreleri ve ilgili diğer bilgilere bu başlık altında yer verilecek olup; kişisel verilerin işleme süresinin en azından azami süreyi gösterecek şekilde gerekçesine de yer verilmek suretiyle belirtilmesi gerekmektedir. Ayrıca, sürelerin belirlenmesinde Kanununun 4 üncü maddesinin ikinci fıkrasının (d) bendinde yer alan, “İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.” ilkesinin gözetilmesi gerekmektedir.

Mevzuattan kaynaklı bir sürenin mevcut olması durumunda, sürenin hangi mevzuat hükmüne dayandırıldığı belirtilmesi gerekmektedir.

Taahhütname ekinde yer alan başlıklar dışında ayrıca belirtmek istenen hususlar “Ek faydalı bilgiler” başlığı altında açıklanmalıdır.

10. İrtibat kişisi iletişim bilgileri

İrtibat kişisine ait bilgiler bu başlık altında yer almalıdır.

11. “Veri Sorumlusundan Veri İşleyene Aktarım” başlıklı Taahhütname örneği EK-1’de yer alan “Veri Sorumlusu” ve “Veri İşleyen” başlıkları

Bu başlıklar altında yapılacak açıklamalarda veri sorumlusu ve veri işleyenin faaliyet alanlarının açıklanması ile veri sorumlusunun veri aktarımına, veri işleyenin ise aktarım sonrasında gerçekleştireceği işleme faaliyetlerine ilişkin açıklamaların anlaşılır detayda ortaya konulması gerekmektedir.

12. “Veri Sorumlusundan Veri İşleyene Aktarım” başlıklı Taahhütname örneği EK-1’de yer alan “İşleme faaliyetleri” başlığı

Aktarılan kişisel verilerin aktarım amacıyla bağlantılı olacak şekilde ne tür bir işleme faaliyetine tabi tutulacağı hususu somut aktarım özelinde anlaşılır detayda ve netlikte ortaya konulmalıdır.

Kamuoyu Duyurusu

Yayınlanma Tarihi : 18.03.2020

Bilindiği üzere Kurula şikayet başvuruları ve veri ihlal bildirimleri elden, posta veya kargo yoluyla iletilebildiği gibi www.kvkk.gov.tr adresinde hizmete sunulan “şikayet modülü” ve “ihlal bildirimi modülü” aracılığıyla elektronik ortamda da iletilebilmektedir.

Ayrıca Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) kayıt başvuru formları da elden, posta veya kargo yoluyla iletilebildiği gibi Kayıtlı Elektronik Posta (KEP) adresi aracılığıyla da iletilebilmektedir.

Ancak yakın tarihlerde ülkemizde de görülmekte olan Yeni Tip Koronavirüsün (COVID-19) yayılmasını önlemek amacıyla tüm kamu kurum ve kuruluşlarında tedbirler alınmaya devam edilmektedir.

Bu kapsamda; şikayet, veri ihlal bildirimi ve VERBİS'e kayıt başvuru formlarının ELDEN iletilmemesi, bunun yerine Şikayet başvurularının; posta, kargo veya <https://sikayet.kvkk.gov.tr/> adresinde hizmete sunulan şikayet modülü aracılığıyla, Veri ihlali bildirimlerinin e-posta (ihlalbildirimi@kvkk.gov.tr) veya <https://ihlalbildirim.kvkk.gov.tr/> adresinde hizmete sunulan modül aracılığıyla, VERBİS'e kayıt başvuru formlarının ise posta, kargo veya KEP aracılığıyla iletilmesi önem arz etmektedir.

Kamuoyuna saygıyla duyurulur.

06.01.2020 - Kişisel Veri İhlali Bildirimlerinin Elektronik Ortamda Kurula İletilmesi

Kişisel Veri İhlali Bildirimlerinin Elektronik Ortamda Kurula İletilmesine İlişkin Duyuru

Yayınlanma Tarihi : 06.01.2020

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrasında veri sorumlusunun;

- a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
- c) Kişisel verilerin muhafazasını sağlamak

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu, (5) numaralı fıkrasında ise, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunun bu durumu en kısa sürede ilgisine ve Kurula bildireceği, Kurulun, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebileceği hükme bağlanmıştır.

Bu kapsamda 24.01.2019 tarih ve 2019/10 sayılı Kurul kararı ile Kurula yapılacak veri ihlal bildiriminde kullanılmasına karar verilen “Kişisel Veri İhlal Bildirim Form”unun <https://ihlalbildirim.kvkk.gov.tr/> internet bağlantısı yoluyla da Kurula iletilebilmesi mümkün hale getirilmiştir.

Kamuoyuna saygıyla duyurulur.

Kişisel Veri İhlali Bildirim Formu Kılavuzu

Not: Veri İhlali Bildirim formu yalnızca Veri Sorumlusu tarafından doldurulması gerekmektedir. Şikayet ve İhbar içerikli başvuruların Kurumumuza yazılı olarak veya <https://sikayet.kvkk.gov.tr> adresinden iletilmesi gerekmektedir.

Kamuoyu Duyurusu

Yayınlanma Tarihi : 08.11.2019

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun 'Veri Sorumlusunun Aydınlatma Yükümlülüğü' başlıklı 10 uncu maddesi "(1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; a) Veri sorumlusunun ve varsa temsilcisinin kimliği, b) Kişisel verilerin hangi amaçla işleneceği, c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi, d) 11 inci maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür." hükmünü amirdir.

Kurumumuzca yapılan incelemelerde başta medya kuruluşları olmak üzere muhtelif kurum/kuruluş/firma vb veri sorumlularının internet sayfalarında sunulan aydınlatma metinlerinde kişisel verilerin işlenmesi hususunda uygulanan politika ve kurallara yönelik açıklamalarda doğrudan Avrupa Genel Veri Koruma Tüzüğüne (GDPR) atıf yapıldığı görülmektedir.

Bu kapsamda Kişisel Verileri Koruma Kurulunun 30.10.2019 tarih ve 2019/315 sayılı Kararı uyarınca; bahse konu veri sorumluları tarafından aydınlatma yükümlülüğünün yerine getirilmesi amacıyla hazırlanan metinlerde GDPR'a uyum sağlandığına yönelik ifadelere yer verilmesinin, veri sorumlularının 6698 sayılı Kişisel Verilerin Korunması Kanununa karşı yükümlülüklerini ortadan kaldırmadığının, bu itibarla GDPR'a yapılan atıfların yanı sıra söz konusu aydınlatma metinlerinde belirtilen politika ve kuralların öncelikle 6698 sayılı Kişisel Verilerin Korunması Kanununa uygun olduğunun belirtilmesi gerektiğinin hatırlatılmasında fayda görülmektedir.

Diğer taraftan veri sorumlularınca yayımlanan aydınlatma metinlerinde Kanunun 10 uncu maddesi ile Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin 4 üncü maddesi hükümlerine uygun şekilde;

- Veri sorumlusunun ve varsa temsilcisinin kimliği,
- Kişisel verilerin hangi amaçla işleneceği,
- Kişisel verilerin kimlere ve hangi amaçla aktarılacağı,
- Kişisel veri toplamanın yöntemi ve hukuki sebebi (Kanunun 5 ve 6 ncı maddesinde yer alan işleme şartlarından hangisine dayanıldığına açıkça belirtilmesi)

- İlgili kişinin Kanununun 11 inci maddesinde sayılan diğer hakları

hususlarına açıkça yer verilmesi, muğlak ve belirsiz ifadelerden mutlak surette kaçınılması gerekmektedir.

Kamuoyuna saygıyla duyurulur.

06.11.2019 - Kişisel Verilerin Korunması Kanunu Uyum Süreci

Kişisel Verilerin Korunması Kanunu Uyum Sürecine İlişkin Duyuru

Yayınlanma Tarihi : 06.11.2019

6698 sayılı Kişisel Verilerin Korunması Kanunu, bununla ilişkili ikincil mevzuat ve Kişisel Verileri Koruma Kurulu'nun vermiş olduğu kararlar çerçevesinde veri sorumlularının yükümlülükleri belirlenmiştir. Bu kapsamda, veri sorumlularının hukuka uygun veri işleme "Veri Sorumluları Sicil Bilgi Sistemine" (VERBİS) kayıt, buna bağlı olarak "Kişisel Veri İşleme Envanteri" ile "Saklama ve İmha Politikası" hazırlama ve kişisel veri güvenliğine ilişkin teknik ve idari tedbirleri almak gibi yükümlülükleri bulunmaktadır.

Veri işleme faaliyetinin yukarıda belirtilen mevzuatlara uyumlu olarak gerçekleştirilmesi için veri sorumlularının ve veri işleyenlerin bu yükümlülüklerin kaynağı olan başta kişisel verilerin işleminin genel ilkeleri olmak üzere kişisel veri koruma alanında genel bir bilgi sahibi olması gerektiği yadsınamaz. Bu sebeple, Kişisel Verileri Koruma Kurumu tarafından veri sorumlularının bu yükümlülüklerle uyumunu kolaylaştırmak amacıyla birçok rehber, kılavuz ve doküman hazırlanmış ve www.kvkk.gov.tr adresinde paylaşılmıştır. Kurum, ayrıca, ilgili kişileri ve veri sorumlularını aydınlatmak ve hızlı bir şekilde sorularının cevaplanması amacıyla "VERİ Koruma Hattı" (ALO 198) adı ile bir bilgi danışma hattı kurmuştur. Bu çalışmalar, Kurum tarafından düzenli olarak yapılan farkındalık artırma ve bilgilendirme faaliyetleri vasıtasıyla da farklı platformlarda desteklenmektedir.

Kurul, şikâyet üzerine ya da re'sen yaptığı incelemelerde veri sorumlularının bu yükümlülükleri yerine getirip getirmediğini hukuki ve teknik açıdan birçok unsuru içeren geniş bir perspektiften değerlendirmekte ve karar vermektedir. Bu noktada Kurulun, sadece Kanun ve ikincil mevzuatta belirtilen yükümlülüklerle uyumu göz önünde bulundurduğunun ve bu uyum çalışmalarının veri sorumlusu bünyesinde ya da dışarıdan destek almak suretiyle yürütülüp yürütülmediği konusunda bir değerlendirmede bulunmadığının belirtilmesi gerekmektedir.

Nihayetinde, veri sorumlularının tabi olduğu yükümlülüklerin çeşitliliği gereği bu yükümlülüklerin ancak disiplinler arası ortak bir çalışmanın neticesinde yerine getirilebilir olduğu hususu da göz önünde bulundurulmalıdır.

Kurum tarafından gerekleřtirilen yukarıda belirtilen alıřmaların neticesinde vatandařlar ile zel sektr ve kamu kurumlarının temsilcileri arasında kiřisel verilerin korunması alanındaki bilgi birikimi son dnemde hızla artmakta ve bu durum kamuoyunda genel farkındalık dzeyine katkı saęlamaktadır.

nmzdeki dnemde Kurum; lkemizdeki farkındalık seviyesi, veri sorumluları-veri iřleyenler- ilgili kiřilerin beklentileri, kiřisel verilerin korunması alanında mevcut uygulama rnekleri, kamu kurumlarının yetki ve grevleri erevesindeki rolleri gibi unsurları da gz nne alarak veri sorumluları ve veri iřleyenlerin kurumsal kapasitelerinin arttırılması yoluyla ykmllklerini yerine getirmesini kolaylařtıran ve ilgili kiřilere kiřisel verilerinin iřlenmesi srecinde gven veren bir sertifikalandırma mekanizması zerinde alıřmalarını srdrmektedir. Kurum, bu alıřma ile ilgili detayları nmzdeki dnemde kamuoyu ile paylařacaktır.

Kamuoyuna saygı ile duyurulur.

05.09.2019 - VERBİS'e Kayıt Süresinin Uzatılması

VERBİS'e Kayıt Süresinin Uzatılması Hakkında Duyuru

Yayınlanma Tarihi : 05.09.2019

Türkiye Odalar ve Borsalar Birliđi (TOBB) ve muhtelif sektör temsilcileri tarafından Kurumumuza intikal ettirilen Veri Sorumluları Siciline kayıt sürelerinin uzatılmasına ilişkin taleplerin deđerlendirilmesi neticesinde Kişisel Verileri Koruma Kurulunun 03.09.2019 tarihli ve 2019/265 sayılı Kararı ile;

- Yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları ile yurtdışında yerleşik gerçek ve tüzel kişi veri sorumlularının Veri Sorumluları Siciline kayıt yükümlülüđünü yerine getirmeleri için belirlenen sürenin 31.12.2019 tarihine kadar uzatılmasına,
- Bu kararın Kurum internet sayfasında duyurulması ve Resmi Gazetede yayımlanmasına

karar verilmiştir.

Kamuoyuna saygıyla duyurulur.

12.10.2018 - VERBİS'e Yapılan Kayıt Başvuruları

VERBİS'e Yapılan Kayıt Başvuruları Hakkında Duyuru

Yayınlanma Tarihi : 12.10.2018

6698 sayılı kişisel Verilerin Korunması Kanunu gereği, kişisel veri işleyen gerçek ve tüzel kişilerin Veri Sorumluları Siciline kayıt yükümlülüğü bulunmakta olup Kişisel Verileri Koruma Kurulu tarafından bazı kriterler gözönüne alınarak veri sorumluları için kayıt yükümlülüğü başlama tarihleri ilan edilmiştir.

Buna göre, yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları ile yurtdışında yerleşik gerçek ve tüzel kişi veri sorumluları için Sicile kayıt yükümlülüğü başlangıç tarihi 01.10.2018 olarak belirlenmiştir.

Bu kapsamda, söz konusu kriterleri taşıyan veri sorumlularının, Sicile kayıt yükümlülüğünü yerine getirmesi amacıyla Başkanlığımızca hazırlanan Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) 01.10.2018 tarihi itibarıyla kullanıma açılmış ve kayıt yapılmaya başlanmıştır.

Bununla birlikte VERBİS'e yapılan kayıt başvuruları üzerinde Başkanlığımızca yapılan değerlendirmede, VERBİS Anasayfada yer alan "Veri Sorumlusu Yönetici Girişi" butonu ile giriş yapıldığında bazı tüzel kişi veri sorumluları için "Veri Sorumlusunun Vergi Kimlik Numarası" alanına veri sorumlusu olan tüzel kişiliğin değil de tüzel kişilik tarafından bu konuda görevlendirilmiş olan gerçek kişilere (çalışan, yönetici, yetkili vb.) ait T.C. kimlik numarası bilgisinin girildiği tespit edilmiştir.

Önemle belirtmek gerekir ki tüzel kişiliklerde veri sorumlusu; bu tüzel kişilikte çalışan, yönetici gibi bir gerçek kişi değil tüzel kişiliğin bizzat kendisi olduğundan Sicile kayıt yükümlülüğü de bu tüzel kişiliktir. Dolayısıyla, tüzel kişilik olan bir veri sorumlusunun Sicile kayıt başvurusu da bu tüzel kişiliğin vergi kimlik numarası ve unvanı ile yapılacaktır.

Bu şekilde hatalı kayıt yapılmış olması, söz konusu tüzel kişiliğin sorumluluğunu ortadan kaldırmayacağından bu durumda olan kayıt varsa ilgili tüzel kişilik için yeniden VERBİS'e başvuru yapılması önerilmektedir.

16.05.2018 - Yurtdışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurlar

Yurtdışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurlar

Yayınlanma Tarihi : 16.05.2018

6698 sayılı Kişisel Verilerin Korunması Kanununun 9 uncu maddesinin (2) numaralı fıkrasının (b) bendi kapsamında, yurtdışına veri aktarımında veri sorumlularınca hazırlanacak taahhütnamede yer alacak asgari unsurlar.

Veri Sorumlusundan Veri Sorumlusuna Aktarım

Veri Sorumlusundan Veri İşleyene Aktarım

06.04.2018 - Kanuna Uyum Süreci (Geçici 1. madde)

Kanuna Uyum Süreci (Geçici 1.madde) ile İlgili Duyuru

Yayınlanma Tarihi : 06.04.2018

Son günlerde medyada yer alan bazı haberler ile Kurumumuza şifahi olarak iletilen sorular neticesinde, 6698 sayılı Kişisel Verilerin Korunması Kanununun Geçici 1 inci maddesinin uygulanmasıyla ilgili tereddütler yaşandığı görülmüştür. Söz konusu tereddütlerin önüne geçilmesi ve kamuoyunun doğru bilgilendirilmesini teminen konuya ilişkin açıklama yapılması gereği doğmuştur.

Bilindiği üzere, Kanunun Geçici 1 inci maddesinin üçüncü fıkrasında; Kanunun yayımı tarihinden önce işlenmiş olan kişisel verilerin, yayımı tarihinden itibaren iki yıl içinde (7 Nisan 2018) Kanun hükümlerine uygun hale getirileceği, Kanun hükümlerine aykırı olduğu tespit edilen kişisel verilerin derhal silineceği, yok edileceği veya anonim hale getirileceği, ancak bu Kanunun yayımı tarihinden önce hukuka uygun olarak alınmış rızaların, bir yıl içinde (7 Nisan 2017) aksine bir irade beyanında bulunulmaması halinde, bu Kanuna uygun kabul edileceği hükme bağlanmıştır.

Bu itibarla, Kanunun yayımı tarihinden önce yürürlükte bulunan mevzuat çerçevesinde hukuka uygun olarak alınmış rızaların, ilgili kişilerce aksi belirtilmediği sürece, yukarıda yer verilen hüküm uyarınca Kanuna uygun olduğu kabul edildiğinden, veri sorumlularınca bu şartlar dâhilinde alınmış mevcut rızaların güncellenmesine veya yeniden ilgili kişilerden açık rıza alınmasına gerek bulunmamaktadır. Dolayısıyla, ilgili kişilerce Kanunun yayımı tarihinden itibaren bir yıl içerisinde aksine bir irade beyanında bulunulmamış ise, bu kişisel verilerin de silinmesi veya yok edilmesi gerekmemektedir.

Unutulmamalıdır ki kişisel verilerin işlenmesi için yegane şart açık rıza değildir. Kişisel veri işleme şartları, Kanunun 5 inci ve 6 ncı maddesinde açıklıkla belirtilmiştir. Bu bağlamda; Kanunun yayımından önce toplanmış kişisel veriler açık rıza dışındaki Kanunun 5 inci ve 6 ncı maddesindeki şartlar dairesinde işleniyorsa, bu işleme faaliyetleri için de açık rıza alınmasına ve bu faaliyetlerin de açık rızaya dayalı olarak yürütülmesine gerek yoktur.

Kamuoyuna saygıyla duyurulur.

Rehberlik Hizmeti Veren İnternet Siteleri ve Uygulamalara Yönelik Kamuoyu Duyurusu

Yayınlanma Tarihi : 28.03.2018

Bilindiği üzere, Kişisel Verileri Koruma Kurulunun 21.12.2017 tarihli ve 2017/61 sayılı Kararı ile, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuatta dayanağı bulunmaksızın ilgili kişilerin iletişim bilgilerinin paylaşımını yapan internet siteleri ve uygulamalar tarafından gerçekleştirilen kişisel veri işleme faaliyetinin Kanunun ilgili hükmü uyarınca derhal durdurulmasına, kişisel verilerin hukuka aykırı olarak elde edilmiş olabileceği de dikkate alınarak ilgili internet siteleri ve uygulamalar hakkında gerekli hukuki işlemlerin tesisi için adli ve idari süreçlerin başlatılacağına karar verilmiştir.

Bu çerçevede, ilgili kişilerin açık rızaları alınmaksızın isimden telefon numarası veya numaradan isim sorgulanması şeklinde rehberlik hizmeti veren internet siteleri ve uygulamalara yönelik Kurumumuza ulaşan şikayet ve ihbarlar ile çeşitli basın organlarında yer alan haberler kapsamında Kurumumuz, yetkili kurumlarla işbirliği içerisinde incelemelerini sürdürmektedir.

Belirtmek gerekir ki, bu kapsamda faaliyet gösteren internet siteleri ve uygulamalar; telefon rehberinde yer alan kişilerin ad-soyad ve telefon numarası gibi kişisel verilerini üçüncü kişilere aktarmakta olup söz konusu aktarma faaliyetinin, Kanunda belirtilen kişisel veri işleme şartlarına dayanmaması halinde bu durumun Kanuna açıkça aykırılık teşkil edeceğinin hatırlatılmasında fayda görülmüştür.

Bu süreçte, vatandaşlarımızın da çeşitli uygulamalar, internet siteleri ve sosyal medya hesapları üzerinden kişisel verileri toplayarak bu verilerin paylaşımını sağlayan, isim sorgulandığında telefon numarası bilgisine telefon numarası sorgulandığında da isim bilgisine erişme ve başkalarının telefonunda nasıl kayıtlı olduğunun öğrenilmesine yönelik faaliyette bulunan internet siteleri ve uygulamaların kullanılmasının hukuka aykırılık teşkil edebileceği göz önünde bulundurularak, bu konuda gerekli dikkat ve özeni göstermeleri önem arz etmektedir.

Kamuoyuna saygıyla duyurulur.

İNGİLİZCE DUYURULAR

Bölüm İçeriği

- Board Resolution on Protecting Personal Data at Service Areas such as the Counters, Box Offices and Desks
- The Transfer of Personal Data Abroad on the Basis of Convention No. 108
- Search Engine Delist Criteria
- Board Decision about Cathay Pasific Airway
- Board Decision about Clickbus Travel Services
- Board Decision on Minimum Elements that Should be Included in the Communication of the breach by the Data Controller to the Data Subject
- Board Decisions on Providing Derogations from The Obligation of Registration with the Data Controllers' Registry
- Board Resolution on Preventing Data Controllers and Data Processors From Forwarding Advertising Messages/Calls to Email Addresses of Data Subjects or to Their Phones By Sms or Phone Calls
- Protection of Personal Data During the Fight Against COVID-19
- Public Announcement - Microsoft Corporation
- Public Announcement on Application for Commitment
- Public Announcement on Covid-19
- Public Announcement on Distance Learning Platforms
- Public Announcement on the Commitment Application
- Public Announcement on the Extension of the Registration Periods to Verbis (Data Controllers Registry)
- Public Announcement on Whatsapp Application
- Regarding Processing of Location Data and Tracking Mobility of Individuals to Combat Covid-19
- The Board Decision No. 2019/10 of 24.01.2019 about Procedures and Principles of Personal Data Breach Notification
- The Board Decision No. 2019/125 of 02/05/2019 about the form prepared to be used in the determination of the countries having adequate level of protection
- The Decision of Personal Data Protection Board No. 2018/88 of 19/07/2018 on "The Starting Dates of Obligation to Register with the Data Controller's Registry"

- Fulfilment of Obligation to Inform

Board Resolution on Protecting Personal Data at Service Areas such as the Counters, Box Offices and Desks

Board Resolution on Protecting Personal Data at Service Areas such as the Counters, Box Offices and Desks

Decision Date: 21/12/2017

Decision No : 2017/62

Summary : Protecting Personal Data at Service Areas Like the Counters, Box Offices and Desks

As a result of the assessment made within the scope of notices submitted to the Turkish Data Protection Authority regarding personal data security breaches in the areas where the service offered to citizens such as the counters, box offices and desks, The Board has unanimously adopted the following decisions.

Institutions, especially those in the banking and health sector, that provide services by more than one employee in an open-plan office (where employees sit shoulder to shoulder at communal desks) like posting and cargo service providers, tourism agents, customer services departments of the chain stores, institutions that carry out subscription processes, and public and private sector institutions that provides services such as municipalities, tax and civil registration services shall take necessary organizational and technical measures pursuant to Article 12 of the Personal Data Protection Law numbered 6698 in order to prevent unauthorized persons to enter counter, box office and desk areas and to restrain persons, who gets services in close areas, from hearing, seeing, learning or acquiring each other's personal data.

This resolution that is undertaken in accordance with the Article 15 (6) of the Law is published in the official gazette and announced on the website of the Authority and Pursuant to the Article 18 of the law, The legal action shall be taken against for those who do not comply with this regulation

Binding Corporate Rules Application Form

PDPA-BCRs/2020-1

PERSONAL DATA PROTECTION AUTHORITY

BINDING CORPORATE RULES

APPLICATION FORM

Application Form of Binding Corporate Rules for Data Controllers

Application Form for Approval of the Data Controller Binding Corporate Rules for the Transfer of Personal Data

INTRODUCTION

“Transfer of personal data abroad” is regulated with the Article 9 of the Personal Data Protection Law No. 6698 (Law No. 6698). Pursuant to subparagraph (b) of Article 9(2) of Law No. 6698, in the event that adequate level of protection is not provided in the country to which personal data to be transferred, such data may be transferred abroad without explicit consent of the data subject upon the existence of commitment for adequate level of protection in writing by data controllers in Turkey and abroad and the authorization of the Personal Data Protection Board (the Board).

The Board determined the minimum elements that must be included in the Commitments to be prepared based on subparagraph (b) of Article 9(2) of the Law No. 6698 with the Decision No. 2018/33 dated 02/04/2018. These commitments generally make the bilateral transfers to be made between the companies easier, but they may remain incapable in providing a practical implementation with respect to the transfers of data to be made between the multinational group of companies. For this reason, this application form is established to be used in the international transfers of data to be made between these companies.

Binding Corporate Rules are data protection policies used for the transfer of personal data for the multinational group of companies operating in countries where adequate level of protection is not provided and that enable them to commit adequate level of protection in writing. Companies that are

within this scope need to make an application for Binding Corporate Rules to the Authority by filling out the relevant form and following the instructions required.

Pursuant to subparagraph (b) of Article 9(2) of Law No. 6698, in the event that adequate level of protection is not provided in the country to which personal data to be transferred, the commitments will be prepared by data controllers in Turkey and foreign countries relating to ensuring adequate level of protection are subject to the approval of the Board.

Binding Corporate Rules approved by the Board are not subject to the time period. If it is necessary, the application of Binding Corporate Rules may be suspended or rescinded by the Board.

PRINCIPLES AND PROCEDURES RELATING TO THE APPLICATION

1. The Competence to Apply

If the Group has its headquarters in Turkey, that entity is authorized to apply.

If the Group has its headquarters outside Turkey, then a Group member established in Turkey should be authorized in terms of the protection of personal data (Shortly "Authorized Group Member"). In that case, that entity is authorized to apply on behalf of the Group.

2. Information/Documents submitted in the application

- a. Application Form
- b. Binding Corporate Rules Text
- c. All the other information and documents relating to the application

Applicant prepares the application documents and submits them to the Authority during the application process. If necessary, the Authority may demand other information and documents.

3. Application Method

Applications shall be delivered to the Authority by hand or sent by post.

4. The Finalization of Application

Applications are assessed and finalized by the Board in one year from the official date of application. If necessary, this period may be extended for periods not exceeding six months.

In case the application is approved by the Board, this situation is notified to the relevant person and if necessary, it is announced.

DEFINITIONS

Binding Corporate Rules: Personal data protection policies to be adhered to by a data controller within a group of undertakings established in Turkey for transfers or a set of transfers of personal data to companies and enterprises operating abroad in one or more countries within the same group of companies and to data controllers that engage in a joint activity or have a joint decision making mechanism regarding data processing activities.

Group: The companies and enterprises that operate within a group of companies and all data controllers engaged in a joint economic activity or have a joint decision-making mechanism regarding data processing activities.

Group Member: Data controllers within a group that has a joint economic activity with a company or enterprise within a group of company or that has a joint decision mechanism regarding data processing activities.

Authorized Group Member: A group member established in Turkey that is authorized for protection of personal data in cases where the group has no headquarters in Turkey.

ABBREVIATIONS

Law No. 6698: Personal Data Protection Law No. 6698

BCR: Binding Corporate Rules

The Board: Personal Data Protection Board

The Authority: Personal Data Protection Authority

APPENDIX

Appendix 1: Binding Corporate Rules Text

Attach certified copy of Binding Corporate Rules text.

Other: Attach all other information and documents that you think are necessary for the application by listing.

BINDING CORPORATE RULES

APPLICATION FORM

FOR TRANSFER OF PERSONAL DATA ABROAD

I. APPLICANT INFORMATION

In this section, there are questions in terms of International Group of Multinational Companies (Hereinafter, it will be called as “the Group”) that apply, to the person who carries out the application and each company (Hereinafter, it will be called as “Group member”) that is in the group of multinational companies subject to Binding Corporate Rules.

A. In terms of the Group of Companies That Apply

Name/Title:

Headquarters Address:

Address of Group member established in Turkey (If the Headquarters is not in Turkey):

B. In terms of those carrying out application procedures

Applicant’s Name/Title

If any, Citizenship ID/Tax ID:

Legal Status of Applicant (company, partnership etc.):

The Position of Applicant in the Group (The headquarters of Group established in Turkey or if there is not, a group member established in Turkey that is authorized in terms of the protection of personal data.):

Name/Department of Contact Person:

Address:

Telephone Number:

Fax Number:

E-Mail Address:

C. Other Issues

1. Please indicate to which country/countries personal data to be transferred from Turkey:

2. Please indicate the contact information of all Group members that is involved in Binding Corporate Rules:

II. INFORMATION ABOUT BINDING CORPORATE RULES

This section contains the questions and general provisions on how the binding nature of Binding Corporate Rules is ensured for all Group members and for whom process personal data on behalf of the Group, envisaged mechanisms in order for an efficient implementation, coordination with the Authority, the details relating to transfer and processing of personal data, mechanisms for reporting and recording changes, data security issues, accountability, information and ancillary documents relating to the Binding Corporate Rules application.

A. THE ELEMENT OF BINDING NATURE

The application of Binding Corporate Rules shall have a binding effect on the parties as in accordance with the national legislation for approval. The questions in this section are necessary for deciding whether aforementioned binding nature is available or not. In all sub-titles, please state your explanations about the subject in clear and plain language.

1. In terms of Group Companies

- In which method (e.g. contracts between Group companies, unilateral commitments, ethical rules approved by the parties etc.), the obligation to obey Binding Corporate Rules (binding nature) between Group members will be ensured, explain:

- What are the consequences of not being in compliance with the methods in the Group, please explain:

- Does Binding Corporate Rules embrace the whole Group, if any, please explain Group member exempted and the reasons of exemptions:

2. In terms of Employees[1]

- How will the obligation of employees to obey Binding Corporate Rules be ensured, please summarize by referring relevant documents (labour contract, collective agreement, privacy contract, ethical rules, company policies, workplace directives, disciplinary regulations etc.):

- In the event that the provisions of Binding Corporate Rules are infringed by employees, please explain the sanctions that will be imposed:

3. In terms of Data Processors

- Please explain the methods (for example, regulating articles in the contract that bring obligations) to be implemented to make taking safeguards obligatory to data processors about ensuring personal data security:

- In terms of methods that will be implemented, please explain the consequences and sanctions of the violation of Binding Corporate Rules by data processors:

4. In terms of Data Subject Rights and Legal Claims[2]

- Please declare that the data subject rights and powers within the scope of Law No. 6698 (e.g. Article 10, 11, 13 and 14) will be ensured:

- Please declare that within the scope of Binding Corporate Rules, applying to the Turkish courts is possible for compensation of all kinds of damages including the right to claim compensation for the damage in the subparagraph (ğ) of the Article 11(1) of Law No. 6698:

- Please declare that all kind of help like translation, legal aid etc. will be ensured in cases to be filed in other countries about data subject rights:

- In the Group, regardless of the source of the violation, the damage from the violation of provisions of Binding Corporate Rules should be compensated by the headquarters of the Group established in Turkey or a Group member established in Turkey that is authorized in terms of the protection of personal data. In this context, please explain the authorized group member and adequate safeguards taken including financial safeguards:

- Regardless of the source of the claim, burden of proof about the claim of violation of Binding Corporate Rules shall be on the headquarters of the Group established in Turkey or a Group member established in Turkey that is authorized in terms of the protection of personal data. Please explain the process:

B. EFFECTIVENESS OF BCRs

It is important that the Binding Corporate Rules are effectively enforced by the Group. This section contains questions about which mechanisms and how you implement them to ensure that the Binding Corporate Rules are effectively enforced. How the Binding Corporate Rules will be implemented within the group is particularly essential in assessing whether measures have been taken to ensure adequate protection in terms of data transferred abroad.

1. Training and Awareness Raising (In Terms of Employees)

Please briefly explain the activities you do or will do on the followings in order to ensure that the Binding Corporate Rules are applied in an appropriate and effective manner by the employees.

- Do you have special training programs to ensure that employees enforce the Binding Company Rules effectively and respect the right to personal data protection?
- Is the level of knowledge and awareness of the employees monitored in terms of the protection of personal data, data security and provision of the Binding Corporate Rules?
- Are BCRs communicated to all employees on paper or on-line?
- In terms of personal data processing activities, is there any review and approval by authorised persons within the Group?
- What kind of trainings are planned for the employees to understand the relationship between their work and personal data security and to take action when necessary:

2. Complaint Handling Mechanism

- In case of non-compliance with the Binding Corporate Rules, is there a Complaint Handling Mechanism within the Group to notify this situation:

3. Verification of Compliance

- Please specify what verification mechanisms does your Group have in place to audit each member's compliance with the Binding Corporate Rules:
- Describe where and how verification of compliance mechanisms are regulated in the Binding Corporate Rules text:
- Who has been appointed to monitor commitment compliance, what are his duties and responsibilities
- Do you have any arrangements to review / update the verification of compliance mechanisms periodically, please explain:
- Is a transparent and clear reporting envisaged at certain intervals, explain:

4. Staff Responsible for the Enforcement of the Binding Corporate Rules

- For the whole Group, is there a suitable staff / unit structure assigned to ensure compliance with the Binding Corporate Rules and to follow it:
- Please describe the issues such as the structure of the unit/staff or its duties and responsibilities:

C. COOPERATION WITH THE AUTHORITY

In this section, issues on coordination with the Authority are regulated and information is requested on cooperation with the Authority in order to implement the Binding Corporate Rules.

- Explain how to coordinate with the institution.

Ç. PROCESSING AND TRANSFER OF PERSONAL DATA

In this section, it is necessary to define the personal data processing processes in the Group in a clear and intelligible manner so that the Board can assess whether the Binding Company Rules provide adequate protection in the transfer of personal data in accordance with the Law No. 6698.

- Specify the data categories^[3] (such as identity, communication, location, personality) subject to the transfer
- Indicate the quality of the data (general / sensitive data), the purposes of the transfer and the maximum retention periods in terms of the data in each data category
- Specify the group or groups of data subject (such as employee, trainee, visitor, product or service recipients)
- Specify the method of data transfer (cloud environment, e-mail, portable storage devices, etc.)
- Indicate the legal bases of data transfer
- Explain the distribution of the data to be transferred within the Group by specifying the name and contact information of the concerned Group members
- Are these Binding Corporate Rules will be used for data transfers among all the Group companies which are in Turkey or abroad, please explain
- When needed, please explain the envisaged transfer if the data transfer will be made from a group member which is not established in Turkey to a company which is not a group member (onward transfers)^[4].

D. THE MECHANISMS FOR REPORTING AND RECORDING CHANGES

Both group members and the Authority shall be notified about any changes to be made in Binding Corporate Rules within the shortest time.

The outside of the solely administrative changes that have no effect on the implementation of Binding Corporate Rules, the changes that can damage the rights of data subjects or have important effect on data security shall be notified to the Authority initially.

In this section, the mechanisms that will be implemented by the Group for notifying these kind of changes and keep records of them shall be explained.

- Please explain, how will the other Group members and the Authority be notified about Binding Corporate Rules and the possible changes with respect to the Group members:

- Please explain, whether you have any system that will record all kind of changes about Binding Corporate Rules and the implementation of it:

E. DATA SECURITY[5]

In this section, it is necessary to explain the details about how taking all necessary technical and organizational measures to provide an appropriate level of security for personal data to be transferred within the scope of Binding Corporate Rules will be ensured. Please explain that how the topics below are regulated in Binding Corporate Rules by using the ancillary documents and referring the appropriate sections.

- Please explain that where and how the issue of the compliance with general principles is evaluated in Binding Corporate Rules text:[6]

- Please explain (if it is necessary, by specifying the Group members) technical measures to provide an appropriate level of security committed by the data controller in the country to which personal data to be transferred:

- Please explain (if it is necessary, by specifying the Group members) organizational measures to provide an appropriate level of security committed by the data controller in the country to which personal data to be transferred:

- Pursuant to Article 6(4) of Law No. 6698, adequate measures [7] determined by the Board shall be also taken while processing the special categories of personal data. Please explain the measures taken within this scope:

- Other issues (if any):

- Please explain the process relating to the data breach notification.[8]

F. ACCOUNTABILITY AND OTHER PRINCIPLES/TOOLS

- Please explain that how the Group members comply with Binding Corporate Rules and to be held accountable.

- Please explain that how the records of operations of personal data processing will be keeping by Group members on behalf of each data controller.[9]

G. SUPPORTING INFORMATION AND DOCUMENTS

1. The Condition of Being a Party to International Conventions

Please state the international conventions to which the countries where the transfer will be made are parties and that include provisions about the protection of personal data, by referring to relevant sections.

2. The Legislation of Country to which personal data to be transferred and its implementation

In the country to which personal data to be transferred, are there any national legislation about the protection of personal data and any competent personal data protection authority, if any, please state briefly relevant legislation and implementation of it:

H. GENERAL PROVISIONS

In this section, there are general regulatory provisions relating to Binding Corporate Rules.

- While filling the Binding Corporate Rules application form, clear and plain language shall be used by making necessary and sufficient explanations relating to the topic under each sub-titles.

- In the level of application and implementation, the Group and each of the Group members as a whole agree that comply with the instructions of the Authority relating to the interpretation and implementation of Binding Corporate Rules.

- In terms of the implementation of Binding Corporate Rules, the headquarters established in Turkey of the Group that is competent to apply for Binding Corporate Rules or if its headquarters is not established in Turkey, a Group member established in Turkey that is authorized about the protection of personal data are addressed.

- The Group shall process personal data transferred within the scope of Binding Corporate Rules as complied with Law No. 6698 and Binding Corporate Rules. If the compliance with Law and Commitment may not be ensured, the Group give information to the Authority immediately. In this context, it accepts that the Authority has rights to suspend and rescind Binding Corporate Rules.

- In case the data processed within the scope of Binding Corporate Rules are obtained by others by unlawful means, this situation shall be communicated to the headquarters of the Group established in Turkey or the Group member established in Turkey that is authorized in terms of protection of personal data if the headquarters of the Group not established in Turkey within the shortest time.

Then they shall communicate the situation in question to whom it may concern and notify to the Board within the shortest time . Where necessary, the Board may announce such breach at its official website or through in any other way it deems appropriate[11].

- Binding Corporate Rules are only relating to the transfer of data as a whole in the Group and between the Group members. Personal data that are permitted to transfer within the scope of Binding Corporate Rules shall not be transferred to the persons out of the Group members. In the event that it necessitates the transfer of data (following transfer) from a Group member not established in Turkey to any company not the member of the Group, the usage of Commitments that are in the attachment of the Board Decision No. 2018/33 of 02/04/2018 shall be necessary.

- In the event that like the disengagement of any one of the Group member from the Group or the termination of Binding Corporate Rules for any reason, personal data subject to transfer and their backups shall be sent to the headquarters of the Group established in Turkey or if the headquarters not established in Turkey, to the Group member established in Turkey that is authorized in terms of the protection of personal data or these personal data shall be destructed with their backups wholly. In the case that there are provisions in national legislation that prevent the fulfilment of these obligations, the processing of data shall be restricted by taking necessary organizational and technical measures to ensure the privacy of personal data subject to transfer.

- The Group and Group members as a whole shall not disclose the personal data that they have learned to anyone contrary to the provisions of this Law, neither shall they use such data for purposes other than that for which the personal data have been processed. This obligation is not limited to any time.

ANNEX 1:

BINDING CORPORATE RULES TEXT

Please attach a copy of Binding Corporate Rules text and be sure that it includes all ancillary information and documents that you want to send.

[1] Reading Binding Corporate Rules and when it is necessary, accessing Binding Corporate Rules by employees shall be ensured.

[2] In Binding Corporate Rules, provisions of Law No. 6698 below mentioned should be included as a minimum:

- Article 4 (General Principles),
- Article 11 (Data Subject Rights),
- Whether presence of national legislation in the country to which personal data to be transferred or not that prevent obeying the Binding Corporate Rules and if it is available, the clear explanation of it,
- The notification of all legal obligations that one of the Group member is subject to in a third country and there is the possibility of important effects on the assurances that are ensured by Binding Corporate Rules to the Board.
- Coordination with the Authority,
- Article 13 (Request to the Data Controller)

[3] Classification provided in VERBIS should be taken as an example for the data categories.

[4] For such data transfers, the "Commitments" included in the annex of the Board's decision of 02.04.2018 and No. 2018/33 should be used. You can reach the commitments at <https://kvkk.gov.tr/Icerik/5255/Taahhutnameler>

[5] Articles 9/2/b, 9/4/d, and 12/1 of Law No. 6698.

[6] Article 4/2 of Law No. 6698; " The following principles shall be complied within the processing of personal data:

- a) Lawfulness and fairness.
- b) Being accurate and kept up to date where necessary.
- c) Being processed for specified, explicit and legitimate purposes.
- ç) Being relevant, limited and proportionate to the purposes for which they are processed.
- d) Being stored for the period laid down by relevant legislation or the period required for the purpose for which the personal data are processed."

[7] The Board Decision No. 2018/10 of 31/01/2018 on The Adequate Measures Necessary to be Taken By Data Controllers for Processing of the Special Categories of Personal Data.

[8] Article 12/5 of Law No. 6698: "In case the data processed are obtained by others by unlawful means, the data controller shall communicate the breach to the data subject and notify it to the Board within the shortest time. Where necessary, the Board may announce such breach at its official website or through in any other way it deems appropriate."

Pursuant to the Board Decision No. 2019/10 of 24.01.2019 about Principles and Procedures of the Personal Data Breach Notification, the data controller shall notify the Board without delay and not later than 72 hours after having become aware of the breach. To view the Board Decision and access to Personal Data Notification Breach Form; <https://kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi>

[9] Article 4/1(h) of By-law on Data Controllers Registry that is entered into force by being published in the Official Gazette No. 30286 of 30.12.2017 defines personal data processing inventory as “the inventory which are detailed by explanations of the followings; personal data processing operations performed by data controllers according to their business processes, purposes and legal basis of personal data processing, data category, recipient group, maximum storage period which is formed relating to the group of person subject to data and necessary for the purpose for which personal data are processed, personal data envisaged to be transferred to foreign countries, and measures taken relating to data security.”. Personal Data Processing Inventory (“Inventory”) that is regulated in aforementioned By-Law shall be necessary to be prepared to ensure the accountability in terms of Binding Corporate Rules.

[10] Pursuant to the Board Decision No. 2019/10 of 24.01.2019 about Principles and Procedures of the Personal Data Breach Notification, the data controller shall notify the Board without delay and not later than 72 hours after having become aware of the breach. For detailed information: The Board Decision No. 2019/10 of 24.01.2019 on Principles and Procedures of Personal Data Breach Notification <https://kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi>

[11] Article 12(5) of Law No. 6698

The Transfer of Personal Data Abroad on the Basis of Convention No. 108

Summary of the Decision of the Personal Data Protection Board dated 22/07/2020 and numbered 2020/559 regarding “the transfer of personal data abroad on the basis of Convention No. 108”

Decision Date: 22/07/2020

Decision No : 2020/559

Summary : Decision on the transfer of personal data abroad based on Convention No. 108

In the process of examining a short message (SMS) sent by the data controller operating in the automotive industry for advertising/information purposes, upon the complaint of the data subject, in the defence letter received from the data controller, although it is stated that the transfer of personal data, which has been consented to be processed by the companies for marketing purposes, to a company abroad, which is in the data processing position, and only to be processed by this company for the purpose of performing the service in question, are considered under the condition that "data processing is mandatory for the legitimate interests of the data controller" in line with Article 5, subparagraph 2 (f) of the Law on the Protection of Personal Data (Law) No. 6698, in the same defence, it was determined that the data controller's "data privacy text" was approved by the Complainant, in other words, there were statements that contradicted his/her previous statement regarding the consent to the transfer of his/her data abroad. Based on this situation, with the decision of the Personal Data Protection Board (Board) dated 08.07.2019 and numbered 2019/203, it was decided to initiate an ex officio investigation regarding the data controller to store personal data of its customers in foreign databases within the scope of paragraph (1) of Article 15 of the Law.

In this respect, the data controller was informed about the relevant articles of the Law No. 6698 and the explanations on the legal grounds in Article 9 of the Law on the transfer of personal data abroad and all information, documents and records related to the subject were requested to be sent to us. In the defence letter received from the data controller on the subject, in summary, the following issues are included;

In digital marketing communications carried out by the company, a web-based software was used, and since the software was web-based, customers' data were transferred to the cloud database located

in a European Union member country by using SFTP (Outsourcing Company) to send e-mail / SMS to customers via software,

Regarding customers; (1) customer information, (2) marketing information due to e-mail and SMS sending information and (3) contact information were transferred to the outsourcing company, and any sensitive personal data was not transferred abroad by the Company,

Explicit consent from customers whose personal data was transferred to the outsourcing company abroad was obtained, and the said explicit consent was obtained with the Informing Text on the Processing of Customer Personal Data and Consent Text updated since 2018,

The legal basis for the transfer of this data to the data processing company is based on the condition that data processing is mandatory for the legitimate interest of the Company as the data controller regulated in Article 5, subparagraph 2 (f) of the Law,

In Article 9 of Law No. 6698, it is regulated that personal data can be transferred abroad by a) the explicit consent of the data subject, or b) there is sufficient protection or if there is not sufficient protection in the relevant country, by obtaining the permission of the Board, based on the data processing conditions specified in paragraph (2) of Article 5 and Article 6 (3) of the Law, the Board will decide whether there is sufficient protection in the foreign country within the framework of the matters in the paragraph (4) of Article 9 of the Law, however, it has not yet been decided by the Board whether there is sufficient protection in a foreign country, in addition, it is stated in the paragraphs (5) and (6) of the same article that the provisions of international conventions and other laws are reserved for the transfer of personal data abroad,

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the Convention No. 108) is transported to the domestic laws, all European Union member states became a party of the Convention No.108, concerning the parties to the Convention No. 108 Turkey has declared that "... The claim that the "Republic of Cyprus", whose ratification of the convention is not valid, is represented by the Greek Cypriot Administration of Southern Cyprus, which is a party to the said convention will not mean acceptance in any form and in the so-called Republic of Cyprus and Turkey will not make any contact to bring liability under this Agreement", Turkey has not made any statements regarding the parties to the Convention No. 108 out of this declaration, in accordance with the last paragraph of Article 90 of the Constitution, it is accepted that "International Treaties duly put into effect" have the force of law, and also, it is believed that international treaties on fundamental rights and freedoms duly put into effect as per the continuation of the relevant paragraph and the regulation that the provisions of the international treaty will be based on the disputes that may arise

due to the different provisions of the laws on the same subject, therefore, in disputes between the Convention No. 108 on the right to the protection of personal data, which is one of the fundamental rights and freedoms of persons and other laws, Convention No. 108 should be taken as basis,

In accordance with Article 12 of Convention No. 108, it is believed that it is one of the clear rules of Convention No. 108 that personal data transfers to be made to the parties of Convention No. 108 are not prohibited or subject to special permission without one of the exceptions listed in subparagraphs (a) and (b), for any action that does not subjected to any restrictions or special permission has been carried out by Turkey, in this context, considering the paragraphs (5) and (6) of Article 9 of the Law, there is no legal restriction and/or obstacle regarding the transfer of data to the Parties of the Convention No. 108 based on Article 12 of the Convention No. 108,

In the paragraph (1) of Article 2 of the “Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows”, it is regulated that it will be assessed whether sufficient protection is provided for non-party transfers regarding cross-border personal data transfers, accordingly, it is understood that sufficient protection assessment cannot be made for those who are parties to the notion of the relevant article, in the paragraph (2) of the Article 2 of the additional protocol, regulates the conditions under which a reservation can be made to the paragraph (1), however, our country does not make any declaration about the relevant regulation,

Within the framework of the legal grounds (paragraphs (5) and (6) of Article 9 of Law No.6698 and Article 12 of the Convention No. 108), on the basis of the legal ground “provided that the fundamental rights and freedoms of the data subject is not harmed, data processing is mandatory for the legitimate interests of the data controller” in the sub-paragraph (f) of paragraph (2) of Article 5 referring to the paragraph (2) of Article 9 of Law No. 6698, data transfer is made to the outsourcing company in the position of data processing in accordance with the law by taking all necessary administrative and technical measures.

As a result of the examination of the information and documents received from the data controller within the scope of ex officio examination within the framework of the relevant legislation, the following evaluations are included in the decision of the Personal Data Protection Board dated 22/07/2020 and numbered 2020/559.

1. As it is known, in the first paragraph of Article 5 titled “Conditions for Processing Personal Data” of the Law No.6698 on the Protection of Personal Data, the personal data cannot be processed without the explicit consent of the data subject, in the second paragraph, it is clearly provided for by the laws,

it is mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid, processing of personal data belonging to the parties of a convention, is necessary provided that it is directly related to the conclusion or fulfilment of that convention, it is mandatory for the controller to be able to perform his legal obligations, he data concerned is made available to the public by the data subject himself, data processing is mandatory for the establishment, exercise or protection of any right, it is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

In this context, it should be evaluated whether the personal data processing activity is based on one of the processing conditions other than explicit consent, if this activity cannot be performed based on at least one of the conditions other than explicit consent, in this case, the explicit consent of the person should be obtained for the continuation of the data processing activity. One of the situations in which explicit consent is not required is as stated by the data controller subject to ex officio examination, as stated in the sub- paragraph (f) of paragraph (2) of Article 5 of the Law, "it is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject." In order to apply the aforementioned paragraph, it is necessary to comply with the basic principles of the protection of personal data, to observe the fundamental rights and freedoms of the data subject with the legitimate interest of the data controller, and to decide whether the personal data can be processed within the scope of the specified paragraph as a result of the evaluation to be made among competing interests.

In this respect, a two-stage test should be considered in order to apply the subparagraph (f) of paragraph (2) of Article 5 of the Law. In the first assessment to be made, the existence of the legitimate interest of the data controller should be determined, and secondly, it should be determined whether this interest harms the fundamental rights and freedoms of the data subject. However, when the processing condition in subparagraph (f) of paragraph (2) of Article 5 of the Law is based on the transfer of personal data other than explicit consent by the data controller who is a party to the review ex officio, since there is no explanation as to what the legitimate interest is and whether a balance test has been applied between this interest and the fundamental rights and freedoms of individuals, it has not been concluded that there is a valid legitimate interest in the processing of personal data by transferring it abroad by the data controller.

2. However, "explicit consent", whose definition is included in subparagraph (a) of paragraph (1) of Article 3 of Law No.6698, has three elements: disclosure with free will, relying on information and

being related to a specific subject. In this context, if an explicit consent is to be made for the processing of data for more than one category, the explicit consent must be given regarding which data will be processed for what purposes. The data controller must also obtain explicit consent for secondary transactions (such as data transfer abroad) to be performed after using the data. However, if the personal data processing activity is based on one of the conditions other than explicit consent in the Law, explicit consent will not be obtained from the data subject. As a matter of fact, basing data processing on explicit consent while it is possible to carry out a basis other than explicit consent will be deceptive and abuse of the right.

In the defence letter of the data controller to the Board, it is stated that the legal reason for the processing of personal data is based on the condition that "it is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject"; in the informing text and consent text provided to the data subjects, considering that the information "you accept this text for the purpose of recommending and promoting the products and services offered by our company by customizing them according to your taste, usage habits and needs, sending commercial electronic messages such as advertising, promotions, etc. to your contact information you have shared within the scope of your acceptance, storing and ... can be processed within the scope of your explicit consent." is included, it has been evaluated that the personal data processing activity is mainly based on the explicit consent of the data subjects.

In the continuation of the aforementioned defence letter, the transfer of data to abroad was made to the outsourcing company on legal grounds "it is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject." specified in the paragraph (2) of Article 9 of Law No.6698 and subparagraph (f) of paragraph (2) of Article 5; in order to send e-mails/SMS to people/customers who have authorized marketing communications, it is observed that customer data is transferred to a cloud database whose servers are located in a member country of the European Union. However, since there is no explanation in the informing text and the explicit consent text to send a message for marketing purposes by the data subjects, this personal data will be transferred to a company abroad, it has been concluded that it is not clear whether it is within the scope of their legitimate interests or based on the explicit consent of the data subjects, or whether the personal data in question were processed within the framework of legitimate interests and which were based on the explicit consent of the data subjects.

3. The following provisions are regulated In Article 9 of the Law titled “Transfer of Personal Data Abroad”: personal data cannot be transferred abroad without explicit consent of the data subject, however Personal data may be transferred abroad without explicit consent of the data subject provided that one of the conditions set forth in the second paragraph of Article 5 and the third paragraph of Article 6 exist and that; (a) sufficient protection is provided in the foreign country where the data is to be transferred, (b) the controllers in Turkey and in the related foreign country guarantee a sufficient protection in writing and the Board has authorized such transfer, where sufficient protection is not provided.

“(3) The Board determines and announces the countries where sufficient level of protection is provided.

(4) The Board shall decide whether there is sufficient protection in the foreign country concerned and whether such transfer will be authorised under the sub-paragraph (b) of second paragraph, by evaluating the followings and by receiving the opinions of related public institutions and organizations, where necessary: a) the international conventions to which Turkey is a party, b) the state of reciprocity concerning data transfer between the requesting country and Turkey, c) the nature of the data, the purpose and duration of processing regarding each concrete, individual case of data transfer, ç) the relevant legislation and its implementation in the country to which the personal data is to be transferred, d) the measures guaranteed by the controller in the country to which the personal data is to be transferred,

(5) In cases where interest of Turkey or the data subject will seriously be harmed, personal data, without prejudice to the provisions of international agreements, may only be transferred abroad upon the permission to be given by the Board after receiving the opinions of related public institutions and organizations.

(6) Provisions of other laws concerning the transfer of personal data abroad are reserved.” provisions are included.

As a result of the examination of the information, documents and explanations submitted to the Board by the data controller, it was understood that the data controller used a web-based software in digital marketing communications, data controller has transferred customer data (regarding customers; 1) customer information, (2) marketing information due to e-mail and SMS sending information and (3) contact information) to a cloud database whose servers are located in a European Union member country so that they can send e-mails / SMS to their customers via the software.

In Article 12 titled "Transborder flows of personal data and domestic law" of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No. 108, the following provisions are included;

(1) The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.

(2) A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.

(3) Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:

(a) insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;

(b) when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

In the defence letter of the data controller to the Board; it is stated that the legal reason for the transfer of customer information to the outsourcing company is that "data processing is mandatory for the legitimate interest of the data controller" within the scope of subparagraph (f) of paragraph (2) of Article 5 of the Law, regarding the reason in the Article 9 of the Law all European Union member states are a party to Convention No. 108, which has been transferred to our domestic law, it is accepted that, "International Treaties duly put into effect have the force of law" pursuant to Article 90 of the Constitution and in disputes that may arise due to the fact that international treaties and laws contain different provisions on the same subject the regulation based on the provisions of international treaties is included, accordingly, it is believed that in disputes between the Convention No. 108 and other laws regarding the right to protect personal data, which is one of the fundamental rights and freedoms of persons, Convention No. 108 should be taken as basis, there is no transaction carried out by these time by Turkey regarding Any restriction or special permission based on the exception of subparagraphs (a) and (b) of paragraph (3) of Article 12, which adopts the principles of free transfer of the Convention No. 108, which has the force of law, in this context, considering the paragraphs (5) and (6) of Article 9 of the Law, based on Article 12 of Convention No. 108 it is believed that there is no legal limitation and/or obstacle regarding the transfer of data to the Parties of the Convention No.

108, in addition to this, it is regulated under the conditions under which a reservation can be made to the paragraph (1) of the paragraph (1) of the Article 2 (2) of the “Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows”, however, our country does not make any declaration about the relevant regulation, a concrete assessment of the countries providing sufficient protection by the Board has not yet been made, in this respect the transfer of personal data to an Outsourcing Company located in a country that is a Party of Convention No. 108 is made for the legal reasons specified in Convention No. 108 and the relevant Additional Protocol.

First of all, in Article 12 of Convention No. 108, it would be appropriate to state that it is stipulated that the states party to the convention cannot prohibit or restrict the transfer of personal data to other state parties solely on the grounds of the protection of private life, or by prescribing a special permission. In the second paragraph of the Explanatory Report on the Convention No. 108 (Explanatory Report), the purpose of this regulation is to facilitate the data flow between the parties, based on the pre-acceptance that the Contracting Parties provide sufficient safeguards for the protection of personal data, however, it is foreseen that this provision does not eliminate the possibility of subjecting the data flow between the parties to the notification or making arrangements in the domestic laws of the parties to prohibit domestic or transboundary transfers in certain cases. Regarding the implementation of Article 12 of the Convention in the European Union (EU) in the said Explanatory Report, in accordance with the provisions of the abolished Directive 95/46/EC of the EU and the European Parliament and Council Regulation (General Data Protection Regulation-GDPR) dated 27/04/2016 and numbered 2016/679, it is also worth noting that it does not qualify the countries that are parties to the Convention No. 108 as countries with sufficient protection without any further evaluation and that it accepts being a party to the Convention only as a criterion to be considered in the qualification assessment.

In this context, in accordance with the regulation stipulated in the second paragraph of Article 9 of the Law, it would be appropriate to state that personal data transfers to countries that have not been declared as safe countries by the Board, without the explicit consent of the data subject, can only be made if one of the conditions specified in the second paragraph of Article 5 or the third paragraph of Article 6 of the Law, and if the parties undertake sufficient protection in writing and the transfer is allowed by the Board.

4. In the subparagraph (a) of paragraph 4 of Article 9 of the Law, it has been stipulated that international conventions to which Turkey is a party shall be taken into account in the assessment of

whether the Board will allow data transfer or not. The fact that the country to which personal data will be transferred is a party to Convention No. 108 is only one of the elements that will constitute the basis for the assessment of the Board, and this situation is among the criteria adopted in the decision of the Board dated 02.05.2019 and numbered 2019/125 to be used in determining the countries with sufficient protection by the Board. However, in the mentioned article, especially matters aimed at ensuring the effective protection of personal data such as the nature of the personal data subject to transfer and the purpose and duration of the processing, data protection legislation and implementation in the country where the transfer will be made and the measures to be committed by the data controller or data processor in this country and the reciprocity status regarding data transfer between our country and the country of transfer are other matters taken into account in the evaluation of the Board.

In this respect, with the explanation in the “Explanatory Report of the Convention No. 108”, which states that the contracting states may make a regulation in their domestic law to prohibit data transfer abroad, in the evaluation of the Board regarding the permission to transfer data abroad, considering both the international conventions to which our country is a party, such as the Convention No. 108, and the regulation included in Article 9 of the Law that it will take into account the state of reciprocity with the country where the transfer will be made without the purpose of protecting personal data or protecting the privacy of private life, it is considered that the personal data transfer regime stipulated in Law No. 6698 is in compliance with Convention No. 108.

5. In paragraph (6) of Article 9 of the Law, the provision “Provisions of other laws concerning the transfer of personal data abroad are reserved.” is included. As it is known, it is foreseen that international treaties put into effect pursuant to the regulation in Article 90 of the Constitution have the force of law, in this sense the Convention No. 108 has the nature of law in our law, the provisions of international treaties will be based on if the laws provide for different regulations on the same subject from international treaties on fundamental rights and freedoms with the addition made to Article 90 of the Constitution by Article 7 of Law No. 5170. However, in the justification of this article, the explanation “The provision is added to the last paragraph of Article 90 in order to eliminate the hesitations about which one will be given priority in the event of a conflict that will arise in case of conflict with the international treaties on human rights duly put into effect in practice and the provisions of the law” is included, for this to be implemented, the provisions of the said international treaty must be directly applicable, in other words, since it was stated that the provision of the treaty should be “sufficiently clear, precise, unconditional and not requiring the state to take any additional

measures for its implementation”, it is considered that a conflict between a more abstract and general international treaty provision that is not directly applicable and a provision of law will not constitute a conflict within the context of the regulation in the paragraph 5 of Article 90 of the Constitution and for this reason, the aforementioned provision of the Constitution will not find a field of application; therefore, if the provision of a general international treaty conflicts with the provision of law, it should be applied on the basis of the conflicting provision of law.

First paragraph of Article 4 of Convention No. 108 includes the provision “Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.” In other words, the provisions of the Convention do not have direct provisions or consequences in the domestic law of the parties, and determines the basic principles that should be mastered on national data protection regulations and the procedures and principles regarding the assurance to be provided to the data subjects through these regulations. In the “Explanatory Report on the Convention No. 108”, it is stated that the convention is not directly applicable and therefore the parties are obliged to include data protection provisions in their domestic laws. Therefore it is worth noting that the provision in the second paragraph of Article 12 of the Convention No. 108, which the parties cannot prohibit the transfer of personal data to another party country or subject to permission conditions, exclusively to protect the privacy of private life, is not directly applicable; in this respect the aforementioned provision cannot primarily be applied in accordance with paragraph (6) of Article 9 of the Law or paragraph (5) of Article 90 of the Constitution; on the other hand, the regulation provided for in Article 9 of the Law does not contradict Article 12 of the Convention No. 108 and in this respect, considering that both regulations are complementary to each other, being a party to the Convention No. 108 is not sufficient by itself in determining the status of a safe country within the scope of Law No. 6698 as in EU practice, however, it will constitute a positive element in the assessment to be made by the Board.

In this respect, first of all, it should be noted that the Convention No. 108 does not permit the transfer of personal data abroad, if the data controller does not fulfil the conditions specified in Article 9 of the Law while transferring data abroad, an illegal data processing will be brought to the agenda, in this respect, obtaining the explicit consent of the data subject in order to transfer data abroad of personal data that requires explicit consent, in order to transfer data abroad based on other personal data processing conditions specified in the Law, the existence of one of the conditions specified in paragraph (2) of Article 5 and paragraph (3) of Article 6 of the Law, if the parties undertake an sufficient protection and are given permission by the Board, personal data can be transferred abroad.

From the information, documents and explanations given by the data controller to our Authority, it is understood that the personal data of the data subjects processed for marketing purposes were transferred within the scope of explicit consent, and that other personal data were transferred based on the Article 12 of the Convention No. 108 within the scope of the legal justification "it is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject", referring to paragraph (2) of Article 9 of Law No. 6698 and in sub- paragraph (f) of paragraph (2) of Article 5. However, while the data controller stated that it made a transfer within the scope of the Convention No. 108, it did not submit any information to the Board regarding the preparation of a commitment for transferring to the relevant outsourcing company. As of the date of the decision, no application regarding the undertaking has been encountered by the data controller in the Authority records.

As a result, both the explicit consent should not be duly drafted as a separate text by the data controller, and the data subjects did not clearly and understandably declare the transfer abroad; on the other hand, in international transfers that will take place depending on the processing conditions other than explicit consent, the balance test regarding the legitimate interest has not been carried out by the data controller and a copy of the letter of undertaking has not been sent to our Authority in order to obtain the permission of the Board by making a written undertaking with the relevant company. It has been concluded that there is an illegal data processing due to the fact that it does not meet the conditions specified in Article 3.

6. On the other hand, in Article 7 of the Law titled "Erasure, destruction or anonymizing of personal data", the provisions are included: "(1) Despite being processed under the provisions of this Law and other related laws, personal data shall be erased, destroyed or anonymized by the controller, ex officio or upon demand by the data subject, upon disappearance of reasons which require the process. (2) Provisions of other laws concerning the erasure, destruction or anonymizing of personal data are reserved. (3) Procedures and principles for the erasure, destruction or anonymizing of personal data shall be laid down through a by-law." In the Article 7 of the Regulation on the Erasure, Destruction or Anonymizing of Personal Data, in the event that all the conditions for processing personal data in Articles 5 and 6 of the Law are eliminated, it is stated that the personal data must be erased, destroyed or anonymized by the data controller ex officio or upon the request of the data subject.

In this context, since an explicit consent in accordance with the law has not been obtained from the data subjects for the data transfer abroad by the data controller, the balance test has not been carried out indicating that there is a valid legitimate interest for processing conditions other than explicit

consent, however, a letter of undertaking has not been prepared in accordance with Article 9 of the Law and has not been submitted to our Authority in order to obtain the Board's permission, it is concluded that illegal data processing is in question by transferring data abroad, it has been concluded that this personal data should be deleted or destroyed in accordance with paragraph (1) of Article 7 and the relevant Regulation, due to the fact that the data controller does not have a valid legal processing requirement for data transfer abroad.

7. On the other hand, as it is known, Article 10 of the Law titled "Obligation of Controller to Inform" includes that whilst collecting personal data, the controller or the person authorised by him is obliged to inform the data subjects about the following: a) the identity of the controller and of his representative, if any, b) the purpose of data processing; c) to whom and for what purposes the processed data may be transferred, ç) the method and legal reason of collection of personal data, d) other rights referred to in Article 11. In the "Communiqué On Principles And Procedures To Be Followed In Fulfilment Of The Obligation To Inform (Communiqué to Inform)", the procedures and principles to be followed by the data controllers or the person authorised by him within the scope of the obligation to inform are determined.

In the incident subject to ex officio review, it was seen that the data controller used the Informing Text and Consent Text updated since 2018 for obtaining explicit consent, as a result of the examination of the text in question;

it has been concluded that the data controller does not show sufficient attention and care in compliance with the Communiqué to Inform by understanding that;

The informing text is not regulated in the detail specified in the Article 10 of the Law and the Communiqué to Inform,

In the paragraph (f) of Article 5 of the Communiqué to Inform, it is regulated that in the event that processing personal data is on the basis of explicit consent, procedures of the obligation to inform and obtaining explicit consent shall be performed separately. Since it is seen that the data processing activity to be carried out based on the explicit consent of the data controller is arranged under a separate heading but with the informing text within the informing text, the said application constitutes a violation of the Article 5 of the Communiqué,

In the paragraph (h) of the Article 5 of the Communiqué; the provision ""Legal basis" mentioned in sub-paragraph (ç) of Article 10(1) of the Law means that personal data are processed on the basis of which processing conditions determined in the Article 5 and 6 of the Law within the scope of the

obligation to inform. Legal basis shall be explicitly provided at the time of fulfilment of the obligation to inform." is included. In the informing text prepared by the data controller, there is a general statement that the legal reason for the collection of personal data is the processing conditions specified in Articles 5 and 6 of the Law, however, it is not clearly stated which of the processing conditions in Articles 5 and 6 of the Law, as stated in the Communiqué, the legal justification is based on,

In the paragraph (j) of the mentioned article of the Communiqué to Inform, "At the time of fulfilment of the obligation to inform; information that is incomplete, incorrect and misleading the data subjects shall not be used." In the informing text of the data controller, it is stated that the personal data will be processed within the scope of explicit consent for the purpose of sharing the service with third parties to send commercial messages, but the third person mentioned is a company named ..., in other words, there is no explanation that this data will be transferred abroad, due to incomplete and misleading information regarding the transfer of personal data abroad, the data subject does not have complete information about what the person consented to and the consequences of his/her consent,

In the paragraph (a) of the mentioned article of the Communiqué to Inform, "The obligation to inform shall be fulfilled in any case of processing depending on the explicit consent of data subject or other conditions for processing in the Law.", in the paragraph (f), "In the event that processing personal data is on the basis of explicit consent, procedures of the obligation to inform and obtaining explicit consent shall be performed separately." However, the data controller regulates the informing text and obtaining explicit consent in a single text, so it does not offer the option to make a choice to the data subject.

As a result, it has been decided that;

1. The data controller has not made a data transfer in accordance with the provisions specified in Article 9 of the Law regulating the issue of data transfer abroad regarding the transfer of personal data abroad, in addition, being a party to the Convention No. 108 is not sufficient on its own in determining the status of a safe country within the scope of Law No. 6698, however it will constitute a positive element in the evaluation to be made by the Board, therefore, an illegal personal data processing activity is carried out by transferring personal data abroad without meeting the necessary conditions, for this reason, since it is concluded that the obligation of "preventing the illegal processing of personal data" stipulated in the sub-paragraph (a) of the first paragraph of Article 12 of the Law titled "Obligations Regarding Data Security" has not been fulfilled, an administrative fine of 900.000 TL in accordance with subparagraph (b) of the first paragraph of Article 18 titled "Misdemeanors" of the Law on the legal person data controller,

2. On the other hand, it is necessary to instruct the data controller to delete / destruct the personal data in question illegally transferred abroad in accordance with Article 7 of Law No. 6698 and to inform the Board of the result,

3. It is necessary to instruct the data controller to update the disclosure text in accordance with the provisions of Article 10 of the Law No. 6698 and the provisions of Article 5 of the Communiqué On Principles And Procedures To Be Followed In Fulfilment Of The Obligation To Inform issued based on this article, and to instruct that the obligation to inform and obtaining explicit consent must separately fulfil.

Search Engine Delist Criteria

Public Announcement on The Criteria to Be taken into Account When Assessing Requests to Delist the Results Displayed Following a Search Made Based on Person's Name and Surname from a Search Engine's Index

As a result of the evaluation of the applications which were submitted to our Authority about the searches made by the name and surnames of the data subjects through search engines and which are requested to be evaluated within the scope of the "Right to be Forgotten" by Personal Data Protection Board, The Board adopted the decision dated 23.06.2020 and numbered 2020/481.

In accordance with this Decision, it has been decided that:

- "Right to Be Forgotten" subject to the applications submitted to our Authority has been evaluated by considering it as a top concept within the framework of the provision of the third paragraph of Article 20 of the Constitution, the regulations in the Articles 4, 7 and 11 of the Law No. 6698 and Article 8 of The Regulation on the Erasure, Destruction or Anonymization of the Personal Data,
- The right to request that the results related to the person not be achieved in searches made by the name and surname of the search engines included in the applications made to our Authority, is defined as a request to be removed from the index,
- Considering that search engines determine the purposes and means of processing the data collected by third parties on the internet, they are accepted as data controller within the scope of the definition in Article 3 of the Law,
- Considering that the operator of the search engine automatically, regularly and systematically finds the information published on the Internet, then organizes personal data in the form of a list of search results, stores it on its servers, discloses it in certain situations and presents it to its users, activities of the search engines are evaluated as 'personal data processing' within the scope of Article 3 of the Law,
- Based on the procedures and periods specified in the provisions of the Law on the right of application and complaint, the data subjects should first apply to the search engines regarding their requests to remove the search results from the index, if the data controller search engines refuse such requests or do not respond to the applicant, then they can complain to the Board,

- The form of the application to be made by the data subjects and the information and documents to be requested will be determined by the search engines,
- In the evaluation of the requests to be made by the data subjects for the removal of the results displayed from the index following a search made based on their name and surname through the search engines, conducting a balancing test between the fundamental rights and freedoms of the data subject and the interests that the public will obtain from the information in question, observing which of the competing interests outweigh, it is important to take into account the explanations given in the annex while making this evaluation, but the criteria to be taken into consideration in the evaluation process of complaints about this issue will not be limited to these, additional criteria may be brought up by the Board in each specific case,
- It is also possible for the data subjects to apply directly to the judiciary while applying to the Board if their requests for the removal of the results shown as a result of the searches made with their own names and surnames through the search engines are rejected by the data controller search engines or if their requests are not answered,
- Ensuring that necessary actions are taken to ensure that the procedures and principles in this decision are notified to the search engine operator companies and that the necessary actions are taken to ensure that the communication channels are used by the citizens of our country in order to ensure that the right to be forgotten is exercised by the data subjects through their websites.

Respectfully announced to the public.

The Criteria to Be Taken into Account When Assessing Requests to Delist the Results Displayed Following a Search Made Based on Person's Name and Surname from a Search Engine's Index

The criteria listed below are determined by the Personal Data Protection Board as the criteria to be taken into account primarily when assessing the complaints submitted in this regard and may be updated when needed. Taking these criteria into consideration in the assessment of the requests to be made to the data controller will be beneficial.

1. Does the individual play a role in public life?

It is true that there is a stronger public interest in people accessing to information about citizens that have a role in public life than information about ordinary citizens. In this respect, it is important to evaluate whether the person has a discernable role in public life when assessing the delisting of the archive records relating to the data subject from the search engines on the internet.

It can be challenging to define comprehensively the type of role that an individual must have to be able to say that the public interest is stronger in having access to the results displayed following a search when it is compared to an individual's fundamental rights and freedoms. However, politicians, senior public officials, business people, famous artists and athletes, religious leaders, and members of some professions are considered to have a role in public life. This also includes the persons who, due to their roles or activities, frequently appear in the media.

Requests to be made in this context by the individuals having a role in public life are less likely to be accepted in that granting access to results, which are obtained through a search made on the basis of person's name who plays a role in public life, may include some information that needs to be presented to the public for these people's professional lives or that it would protect the public against the practices of the people performing certain professions.

It should also be noted that information about individuals' private life is more likely to be removed from the list of search results. Data of this nature may be removed from the search results, even if they are about people who have a role in public life.

2. Is the subject of the search result a child?

If an individual is not of legal age at the time of the publication of the data relating to him or her, requests to be made for delisting the link of such search results concerning the data in question are more likely to be accepted. In fact, the principle of "best (high) interests of the child" should be taken into consideration in the assessment of the requests of minors, in other words, children.

3. Is the data accurate?

Accuracy of the information means to be accurate as to a matter of fact. At this point, attention should be paid to the difference between the interpretation of a fact and publishing a fact. Inaccurate or misleading information raises the probability of acceptance of the delisting requests, while accurate information based on the facts decreases the possibility of acceptance of the requests. If the information does not reflect the truth and if this presents an inaccurate and misleading impression of an individual, it is more likely that the requests for delisting the link of the information in question will be accepted.

It is important to note here that if a data subject objects to a search result on the grounds that the information is inaccurate, the complainant is expected to prove his or her claim.

On the other hand, in cases where a dispute about the accuracy of information is still on-going, (for example an on-going court case or police investigation), no action may be taken on this matter until the process is complete.

4. Does the data relate to individual's working life?

Another criterion that should be taken into account while assessing the requests for the removal of links from the search results is whether the information is related to the professional life or private life of the data subject. Although all data relating to a person is personal data, not all data about a person is private. As a general rule, information relating to the professional life of a data subject makes it difficult to accept the delisting requests, while information relating to the private life is considered as an important factor in the acceptance of the request. Normally, information relating to the private life of an individual who does not play a role in public life should be considered irrelevant. From this point of view, considering that access to such information has no benefit for the public, it can be evaluated that it is not necessary to include this information in the search results. Additionally, as stated above, in certain circumstances public figures also have a right to request that information relating to them not be spread.

However, two issues should be noted here to be taken into account in the assessment of this criterion: Firstly, is the data subject still engaged in the same professional activity? Secondly, is data about a person's work-related activity excessive, containing more information than necessary?

5. Is the information in the search results insulting, degrading, and slander about the data subject?

In cases of refusal of the request made to the data controller about the removal of the links containing insulting, degrading, derogatory statements or hate speech about the data subject, which constitutes

a crime, from the listed results in the search engine, it would be a more appropriate approach to contact a court rather than lodging a complaint about refusals with the Personal Data Protection Board.

6. Does the information in the search results fall within the scope of special categories of personal data?

Special categories of personal data (sensitive data) are the data that may open the individual to discrimination or make him or her suffer. Within this framework, it is more likely to accept the requests for delisting the links of sensitive data (sexual life, religious beliefs, health, etc.) from the search engine than ordinary personal data.

Nonetheless, when it comes to the special categories of personal data of public figures, reassessment may be needed to see if the interest of the public overrides the rights of the data subject.

In addition, although they are not special categories of personal data, delisting requests for the data about the privacy of the individual such as information identifying the person (address, phone number, password, etc.) and financial information are more likely to be accepted.

7. Is the information displayed in search results up to date?

Another criterion to be taken into account in the assessment of the delisting requests is to determine whether the data is up-to-date, in other words, the period of time after publishing the data. Over the course of time, data may become out-of-date or the relevance of the information to the subject may decrease, which can break the link to the data with the purpose of processing. For this reason, the course of time is a factor that increases the probability of accepting delisting requests from the index. However, this is not an absolute rule, as in any other criterion. For example, the impact of time on data relating politicians or public figures or historical and scientific data will be limited.

8. Is the information displayed in search results causing prejudice to the individual?

When the individual claims that the information in the search results causes prejudice about him or her, request for removing the link in question from the search results must be evaluated. Nonetheless, the provable nature of the claim will increase the probability of acceptance of the request.

9. Does the information in the search result put the individual at risk?

Delisting of the search results is likely to be required where the information in the search result leaves the individual open to risks such as identity theft or stalking.

10. Was the information published by the data subject?

Since the information published by the data subject or with his or her explicit consent can be removed by the data subject from where it is located, requests for removal from search results are less likely to be accepted.

If the data subject consented to the original publication, but has not been given the opportunity to withdraw his or her consent, or his or her request for not processing the data has been refused, then this issue should be also considered in requests for removal of the information in question from search results.

11. Does the original content include the data processed in a journalistic context?

Source of the information and publishing purposes are two other important factors to be taken into account when assessing the requests for removal of the links from the search results.

After all, freedom of expression is the keystone of pluralist and constitutional democracy. Freedom of expression is defined as the opportunity and freedom to have access to thoughts and information, not to be condemned because of the ideas and thoughts, and to express them with legitimate methods.

Similarly, freedom of the press is a fundamental right and freedom that manifests itself in the form of the right to express and spread opinions and thoughts to all domestic and foreign interlocutors in written and visual form. The concept of freedom of the press should be evaluated as a whole with the concept of freedom of expression in terms of public's access to the information and the opportunity to express their own thoughts after filtering such information with their interpretation.

In this context, the important role of the internet in social life, which facilitates the spread of news and ideas and their access to the public, cannot be denied. Archiving on the Internet serves substantially the storage and accessibility of the current events and the news. Archives of this nature provide resources for history, education and research activities, especially because they are directly accessible to the public and generally free. On the other hand, a result of the "observer" role, which is the first function of the press in a democratic society, is to make the archives available to the public.

For this reason, within the framework of certain criteria, it is necessary to establish a balance between the right to request the protection of honour and dignity, which is under protection in the Constitution, and freedom of the press and freedom of expression in connection with this freedom. Examples of these criteria are: that the news or ideas in question contribute to a discussion of the public interest, or the role or function of the person in society, and the nature of the activity subject to an interview or photograph.

Within this context, it is important to ensure that the public has access to search results, but the limits for the protection of private and family lives of others should not be exceeded. In such cases, search result relating to journalistic content may be delisted. Therefore, it will be necessary to make an evaluation among the competing interests in each complaint.

12. Is there any legal obligation to publish the data relating to the data subject?

If certain information must be published by a governmental institution or other bodies authorized due to a legal obligation and if this legal obligation is still on-going, delisting of search results relating to the data subject is less likely to be required. However, it should be noted that each issue must be assessed on a case-by-case basis.

13. Does the information relate to a criminal offence?

Requests for delisting of search results relating to relatively minor offences that happened a long time ago have higher chances to be accepted than that of relating to more serious ones that happened more recently. However, this criterion should not be considered as an absolute rule and should be handled carefully in each specific event on a case-by-case basis.

Board Decision about Cathay Pasific Airway

Personal Data Protection Board Decision No. 2019/144 of 16/05/2019 about Cathay Pasific Airway

As a result of examination regarding the data breach which stems from hardware and software misconfigurations and

inadequate security measures and notified to the Board in 25.10.2018, the Board decided;

1. to impose an administrative fine of 450.000 TL to the Company for not taking necessary technical and

organizational measures to ensure data security within scope of the Article 12(1) of the Law.

2. to impose an administrative fine of 100.000 TL to the Company for not notifying the breach to the Board within

the shortest time in line with the Article 12(5) of the Law.

Board Decision about Clickbus Travel Services

Personal Data Protection Board Decision No. 2019/141 of 16/05/2019 about Clickbus Travel Services

As a result of examination regarding the data breach caused by malware and affected 67.519 people's information such

as identity, contact and process security data in Turkey, the Board decided;

1. to impose an administrative fine of 450.000 TL to the Company for not taking necessary technical and

organizational measures to ensure data security within scope of the Article 12(1) of the Law

2. to impose an administrative fine of 100.000 TL to the company for not notifying the breach to the Board within

the shortest time in line with the Article 12(5) of the Law.

Board Decision about Marriott International Inc.

Personal Data Protection Board Decision No. 2019/143 of 16/05/2019 about Marriott International Inc.

As a result of examination regarding the data breach, which causes large number of data violation, lasted approximately

4 years and shows that the system is problematic by design, and notified to the Board in 03.12.2018, the Board decided;

1- to impose an administrative fine of 1.100.000 TL to the Company for not taking necessary technical and

organizational measures to ensure data security within scope of the Article 12(1) of the Law.

2- to impose an administrative fine of 350.000 TL to the Company for not notifying the breach to the Board within the

shortest time in line with the Article 12(5) of the Law.

Board Decision No. 2019/104 on Facebook

Turkish Personal Data Protection Board Decision Summary on Facebook No. 2019/104 of 11/04/2019

As a result of the examination regarding the data breach which occurred before Facebook about a photo API bug which

grants permission to third-party apps to access Facebook users photos, the Board decided;

1. to impose an administrative fine of 1.100.000 TL to the Company for not taking necessary technical and

organizational measures to ensure data security within scope of the Article 12(1) of the Law.

2. to impose an administrative fine of 550.000 TL to the Company for not notifying the breach to the Board within

the shortest time in line with the Article 12(5) of the Law.

Board Decision No. 2019/269 on Facebook

Turkish Personal Data Protection Board Decision Summary on Facebook No. 2019/269 of 18/09/2019

As a result of the examination regarding the data breach occurred in consequence of the vulnerability which arose from

the interaction of three distinct features of Facebook system such as "View as", "Birthday Celebrator" and "Video

Uploader", the Board decided;

1. to impose an administrative fine of 1.150.000 TL to the Company for not taking necessary technical and

organizational measures to ensure data security within scope of the Article 12(1) of the Law.

2. to impose an administrative fine of 450.000 TL to the Company for not notifying the breach to the Board within

the shortest time in line with the Article 12(5) of the Law.

Board Decision on Data Controllers to be Derogated from the Obligation of Registration with the Data Controllers' Registry

Decision Date : 19/07/2018 Decision Number : 2018/87

Subject Summary : Natural or legal person data controllers who have fewer than 50 annual employees and whose annual financial balance sheet is less than 25 million TL will be derogated from the registration obligation, as long as their primary activity is not processing special categories of personal data.

Having regard to the provision in the Article 16(2) of the Personal Data Protection Law No. 6698 *“Natural or legal persons who process personal data shall register with the Data Controllers' Registry prior to the start of data processing. However, by taking into account the objective criteria set by the Board such as the nature and quantity of the data processed, that data processing is laid down in a law, or transferring the data to third parties, the Board may provide derogation from the obligation of registration with the Data Controllers' Registry.”* and by taking into consideration the Article 16 titled 'Derogation Criteria' of By-Law on the Data Controllers' Registry which entered into force by being published in the Official Gazette No. 30286 of 30.12.2017; in addition to data controllers that are provided with derogation by the Decision of Board No. 2018/32 of 02/04/2018, the Board unanimously decided that natural or legal person data controllers who have fewer than 50 annual employees and whose annual financial balance sheet is less than 25 million TL will be derogated from the registration obligation, as long as their primary activity is not processing special categories of personal data and this Decision will be published on the Official Website of The Authority and in the Official Gazette.

Board Decision on Minimum Elements that Should be Included in the Communication of the breach by the Data Controller to the Data Subject

The Board Decisions No. 2019/271 of 18.09.2019 regarding minimum elements that should be included in the communication of the breach by the data controller to the data subject

As known, pursuant to paragraph (1) of article 12 of the Personal Data Protection Law No. 6698 the data controller is obliged to take all necessary technical and organisational measures to ensure the appropriate level of security, so as to:

- a. Prevent unlawful processing of personal data,
- b. Prevent unlawful access to personal data,
- c. Ensure protection of personal data.

According to Article 12(5), in case the data processed are obtained by third parties by unlawful means, the data controller shall communicate the breach to the data subject (natural person concerned) and notify it to the Board within the shortest time. Where necessary, the Board may announce such breach on its official website or through in any other way it deems appropriate.

The decision of the Personal Data Protection Board (Board) of 24.01.2019 and No. 2019/10 states that “Data subjects should be communicated about breach in the shortest reasonable period of time. If the contact address of the data subject can be reached, notification should be made directly, or if it cannot be reached, notification should be made by appropriate methods such as the publication on the data controller’s website”

During assessment process of the data breach notifications submitted to the Authority within the scope of the stated provision and Board decision; Considering the purpose of the notification to the Board and to persons affected by the breach is to ensure that measures are taken to prevent or mitigate the adverse consequences of such violations, it is necessary to clearly state which elements should be included in the notifications of the data controller to the data subjects.

Within this scope , Personal Data Protection Board Decision No. 2019/271 of 18.09.2019 states that;

- The communication of the breach to be made by the data controller to the data subject should be made in a clear and plain language and include at least;
- Time of the data breach occurred,

- Categories of personal data that are affected by the breach (by distinguishing between personal data / special categories of personal data)
- Possible consequences of personal data breach,
- Measures that have been taken or advised to be taken by the data subject after the breach to mitigate the negative effects of data breach,
- The contact ways to provide information to the data subjects about the data breach such as the name and contact details of the contact persons, or the link of the data controller's web page, call center number and so on.

Respectfully announced to the public.

Board Decisions on Providing Derogations from The Obligation of Registration with the Data Controllers' Registry

The Board Decision No. 2018/32 of 02/04/2018 provides derogation to the following data controllers from the obligation of registration with the Data Controllers' Registry:

Persons processing personal data by non-automated means which provided that form part of a data filing system.

1. Notaries who operate according to the Notary Public Law No. 1512 of 18.01.1972.
2. Only associations which are established pursuant to the Law of Associations No. 5253 of 04/11/2004, foundations which are established pursuant to the Law of Foundations No. 5737 of 20/02/2008 and trade unions which are established pursuant to the Law on Trade Unions and Collective Labor Agreements No. 6356 of 18/10/2012 which process personal data that are in compliance with relevant legislation and purposes, limited to its field of activity and towards their employees, members and donators.
3. Political parties that are established pursuant to the Law on Political Parties No. 2820 of 22/04/1983.
4. Lawyers who operate according to the Attorneyship Law No.1136 of 19/3/1969.
5. Certified Public Accountants and Sworn-in Certified Public Accountants who operate according to the Law of Accounting Profession No. 3568 of 1/6/1989.

The Board Decision No. 2018/68 of 28/06/2018 provides derogation to customs advisors from the obligation of registration with the Data Controllers' Registry.

The Board Decision No. 2018/75 of 05/07/2018 provides derogation to mediators from the obligation of registration with the Data Controllers' Registry.

Board Resolution on Preventing Data Controllers and Data Processors From Forwarding Advertising Messages/Calls to Email Addresses of Data Subjects or to Their Phones By Sms or Phone Calls

Board Resolution on Preventing Data Controllers and Data Processors From Forwarding Advertising Messages/Calls to Email Addresses of Data Subjects or to Their Phones By Sms or Phone Calls

Decision Date : 16/10/2018

Decision Number : 2018/119

Summary : Resolution on Preventing Data Controllers and Data Processors from Forward Advertising Messages/Calls to email address of data subjects or to their phones by SMS or phone calls
By taking into consideration the large number of requests to the Turkish Data Protection Authority regarding advertising messages/calls that are forwarded to email addresses of data subjects or to their phones by SMS or phone calls without obtaining their explicit consent contrary to the provisions of Personal Data Protection Law No. 6698, and considering the findings reached within the scope of the examinations carried out, it is unanimously decided to inform the public opinion on the issues listed below and to publish the Resolution on the web site of the Authority and on the Official Gazette;

- Data controllers who forward advertising messages/calls to email addresses of data subjects or to their phones by SMS or phone calls without obtaining their explicit consent and not providing conditions of processing stated in Article 5 of the Protection of Personal Data Law (the “Law”), and data processors who use such data without the explicit consent of the data subjects for the purposes of sending messages/e-mails or making calls with advertising content on behalf of the data controllers shall immediately cease the mentioned data processing activities pursuant to Article 15(7) of the Law,
- In accordance with the Article 12 of the Law data controller is obliged to take all necessary technical and organizational measures to provide an appropriate level of security for the purposes of preventing unlawful processing of personal data, preventing unlawful access to personal data and ensuring protection of personal data, and in case the processing of personal data is carried out by another natural or legal person on behalf of the data controller, the data controller shall jointly be responsible with these persons for taking such measures.

- Within the scope of provisions of the Article 18 of the Law, a legal action will be taken against the data controllers who engage in such activities
- Considering that mentioned personal data processed might have been obtained unlawfully, the Chief Public Prosecutor's Office will be informed with a notice pursuant to Article 158 of the Code of Criminal Procedure to take necessary legal actions against the relevant data controllers in accordance with Article 136 titled “Unlawful Delivery and Acquisition of Data” of the Turkish Criminal Code No. 5237.

Protection of Personal Data During the Fight Against COVID-19

PUBLIC ANNOUNCEMENT

On Protection of Personal Data During the Fight Against COVID-19

Public institutions and organisations are taking necessary steps and fighting against the virus by taking various measures in order to prevent the spread of COVID-19 outbreak, which has affected the whole world and our country, and to mitigate its impact. While taking these measures, many personal data (ID no, name, address, workplace, travel information) including special categories of data (data concerning health, etc.) are inevitably processed in many cases.

In this process, providing health services and protecting public health are essential. Within the scope of the Personal Data Protection Law No.6698 (Law), in cases where personal data, in particular the data relating to health, of the individuals need to be processed, it is important to ensure that such activities are carried out in accordance with the provisions of the Law and that necessary technical and organizational measures relating to data security are taken by the data controllers and data processors.

It should be noted that even in such exceptional times, data controllers and data processors are obliged to ensure the security of personal data of the data subjects. Therefore, it is important that the personal data are processed in accordance with the law and the measures taken in this regard comply with the general principles of the law, and that irreversible damages do not arise in terms of fundamental rights and freedoms of the individuals in this framework. In this regard, personal data processing activities carried out within the scope of the measures taken against the COVID-19 virus must be necessary, relevant with, limited and proportionate to the purpose. Decisions taken in this regard should be under the guidance and/or instructions of the public health institutions, particularly the Ministry of Health, or other relevant institutions and organizations.

In this context, data controllers must pay attention to the following points when processing personal data, especially the data relating to health.

General Principles of Personal Data Processing

The general (basic) principles in processing of personal data are lawfulness and fairness, being accurate and kept up to date where necessary, being processed for specified, explicit and legitimate

purposes, being relevant, limited and proportionate to the purposes for which they are processed and is stored for the period laid down by relevant legislation or required for the purpose for which the personal data are processed. In the event that the reasons for processing no longer exist, such data should be erased, destructed or anonymised.

Within the scope of fight against COVID-19, these principles must be at the core of all personal data processing activities and all personal data processing activities must be carried out in accordance with these principles.

Lawfulness

Conditions for the processing of personal data are laid down in Article 5 and conditions for the processing of special categories of personal data, including data relating to health, are specified in Article 6 of the Personal Data Protection Law No.6698.

Article 6 of the Law stipulates that it is prohibited to process special categories of personal data without explicit consent of the data subject, however; personal data, except for data concerning health and sexual life, may be processed without seeking explicit consent of the data subject, in the cases provided for by laws and for the data concerning health and sexual life may only be processed, without seeking explicit consent of the data subject, by the persons subject to secrecy obligation or competent public institutions and organizations, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

Also, with the decision of the Personal Data Protection Board, Decision No.2018/10 of 31/01/2018 on "Adequate Measures to Be Taken By The Data Controllers" is determined.

At this point, it should be remembered that personal data should be processed in accordance with the conditions specified in Article 5 and/or Article 6 of the Law.

Within this framework, seeking the consent of the employee may be preferred, especially for the processing of data concerning health, or considering the spreading rate of the pandemic, the employee will also be able to report the disease with his/her own consent. Under the conditions other than explicit consent, data concerning health may be processed by the physicians of the workplace. During this period, not every processed data will be special categories of personal data (such as the last travel destination of the persons). In such cases, conditions for the processing of personal data specified in Article 5 of the Law should be taken into account.

On the other hand, subparagraph (ç) of Article 28(1) of Law No.6698 stipulates that the provisions of Law do not apply in cases where personal data are processed within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations duly authorised and assigned by law to maintain national defence, national security, public security and public order or economic security. In this context, since the current situation threatens public security and public order, there is no obstacle to the processing of personal data by the Ministry of Health and public institutions and organizations which fall under the above-mentioned article.

Obligation to Inform (Transparency)

Another important point deserving to be reminded here is that obligation to inform regarding the personal data processed has been fulfilled. In this sense, data controllers who process personal data should be transparent regarding the measures they implement, including the reasons for collecting personal data and their storage period. The information to be given to the individuals relating to processing of personal data should be short, easily accessible, understandable and made by using a clear and plain language.

Privacy

Within the context of preventing the spread of COVID-19 virus, necessary technical and organizational measures should be taken to ensure the data security in any data processing activity, especially the data concerning health, by the data controllers and data processors. Data relating to the affected people should not be disclosed to any third party without any clear and compulsory reason.

Data minimisation

As in any data processing activity, every processing activity carried out to prevent the spread of COVID-19 virus should be relevant with and limited to the purpose and excessive processing should be avoided. In order to achieve the goal, the most non-intrusive path possible should be preferred.

Frequently Asked Questions

Can a healthcare organisation contact individuals in relation to COVID-19 without having prior permission?

Governments have obligations to ensure public health and public order in situations that reach the global epidemic dimension, such as the COVID-19 virus. Public institutions and organizations may additionally need to collect and share personal data to combat serious threats to public health.

Within this context, Personal Data Protection Law does not stop relevant health institutions and organizations from sending public health messages to people, either by phone, text or e-mail.

It is known that more of the employees work from home during the pandemic. What kind of security measures should be taken during this period?

The legislation on protection of personal data is not a barrier to working from home. During the pandemic, employees may work from home and they can use their own device or communication equipment. The legislation on protection of personal data does not prevent that, but necessary technical and organizational measures must be taken to ensure the security of personal data.

In order to minimise the risks that may arise during remote working, all employees related to the topic should be carefully informed in terms of taking all kinds of precautions and about the security of personal data, mainly ensuring that the data traffic between the systems is carried out with secure communication protocols and it does not bear any weaknesses, and anti-virus systems and firewalls are kept up-to-date.

However, It should not be forgotten that the measures to be taken by the employees do not eliminate the responsibility of the data controllers to ensure the security of personal data under the Law.

Can an employer disclose to her/his colleagues/other employees that an employee is infected with the virus?

An employer should keep employees informed about cases. While providing this information, giving names is not necessary and more information than necessary should not be given. In cases where it is necessary to disclose the name of the infected employee in terms of taking the protective measures, it is beneficial to inform the relevant employees in advance about the issue. Employers have an obligation to ensure the health and safety of their employees, as well as to fulfill their duty of care.

In this context, employers can make their initial announcements as in the following: " We would like to inform you a colleague working on the 5th floor tested positive for COVID-19. After determining those who contacted our infected friend during the dates he/she was in the building, we will inform them about the situation."

As in the example above, for the announcements to be made in an institution, organization or a company, other employees should be informed that there is a COVID-19 infected employee and whether he/she is working from home or on leave; however, unless it is mandatory, details that will directly identify who that employee is, such as the internal level or team, should not be shared.

Can an employer request all employees and visitors to provide information about their travels to affected countries and virus symptoms, such as fever?

Employers have a legal obligation to protect employee health and ensure a safe workplace. In this regard, and under the current circumstances, employers will have their justified reasons to request the employees and visitors to provide information on whether they have visited a place affected by the virus and/or they show COVID-19 symptoms.

This information request must have a strong rationale based on necessity and proportionality and risk management. In this case, certain factors should be taken into account, such as the travel of the employees due to their tasks, existence of people with chronic illnesses in the workplace or those who have the possibility of being affected by the virus more severely, and the instructions or guidance from public health officials.

In cases where adequate measures needed to be taken based on the existence of people have recently traveled to a country which is affected by the virus and/or show symptoms related to the disease, there is no harm in bringing certain recommendations to the attention of employees and visitors terms of personal data protection legislation.

Can an employer share the health data of the employees with authorities for public health purposes?

Within the framework of Article 8 of the Law and the provisions of other laws on the contagious diseases, personal data relating to those who carry the contagious diseases can be shared with the relevant authorities by the employer.

During the pandemic, when the organizations are temporarily closed or the capacity of the data controllers to fulfill the requests of the data subjects is restricted due to COVID-19, are the periods determined in the Personal Data Protection Law and relevant legislation within the scope of the obligation to respond to requests of the data subjects and responsibilities to our Institution still valid?

Under the legislation on protection of personal data, in relation to the complaints, notices, and data breach notifications submitted to our Authority, various periods are determined both in the Law and relevant secondary legislation regarding the obligations of data controllers to data subjects and our Authority, and the compliance with these periods by the data controllers is important.

It is not possible to extend the periods determined in the Law and relevant legislation; however, in these extraordinary conditions our country is in, by taking into account that various operational

applications (remote working, shift working etc.) are used with respect to the measures taken by data controllers, for each complaint or data breach notification, the extraordinary conditions we are in will be observed by the Personal Data Protection Board in terms of evaluating the periods that data officers are obliged to comply with.

PUBLIC ANNOUNCEMENT (DATA BREACH NOTIFICATION)

Gratis Domestic and Foreign Trade Inc.

As known, according to Article 12(5) of Law No. 6698, in case the processed data are obtained by third parties by unlawful means, the data controller shall communicate the breach to the data subject (natural person concerned) and notify it to the Board within the shortest time. Where necessary, the Board may announce such breach at its official website or through in any other way it deems appropriate.

Briefly, in the letter dated 09.03.2020 sent to the Personal Data Protection Authority by Gratis Domestic and Foreign Trade Inc. as the data controller, the following issues are reported;

- The breach occurred between 04.04.2020 and 06.03.2020 and was detected on 06.03.2020,
- In 06.03.2020, an e-mail from an unidentified person about the obtainment of the email addresses/passwords of the Web Site members of the Company was received
- More than one entry attempts are made with the e-mail addresses/passwords obtained by the sources out of the Company and after every unsuccessful attempt, another e-mail/password attempts are made. Hence, passwords of accounts of 2092 web site users were verified,
- Personal data categories affected by the breach are identity, contact and transaction data of customer,
- 2092 persons have been affected by the breach, • Data subjects can get information about the data breach from info@gratis.com and the call center by means of the telephone number of 0 850 210 69 00.

While the examination on the subject is continuing, it was decided to announce the notification of the data breach on the website of the Authority pursuant to the Decision of the Personal Data Protection Board dated 09.03.2020 and numbered 2020/221.

Respectfully announced to the public.

Public Announcement - Microsoft Corporation

Public Announcement - Microsoft Corporation

As known, according to Article 12(5) of Law No. 6698, in case the processed data are obtained by third parties by unlawful means, the data controller shall communicate the breach to the data subject (natural person concerned) and notify it to the Board within the shortest time. Where necessary, the Board may announce such breach at its official website or through in any other way it deems appropriate.

Briefly in the letters dated 29.01.2020 sent to Personal Data Protection Authority by Microsoft Corporation as the data controller the following issues are;

- The breach occurred between 05.12.2019 and 31.12.2019 and was detected on 26.01.2020,
- The breach occurred due to the incorrect configuration of security rules, hence the availability of a database , containing information about Microsoft support services representatives' interactions with customers, via Internet,
- Personal data categories affected by the breach are contact, customer transaction, transaction security and finance data,
- 158 users from Turkey have been affected by the breach,
- Data subjects can obtain information about the data breach from <https://msrc-blog.microsoft.com/2020/01/22/access-misconfiguration-for-customer-support-database/>

While the examination on the subject is continuing, it was decided to announce the notification of the data violation on the website of the Authority pursuant to the Decision of the Personal Data Protection Board dated 04.02.2020 and numbered 2020/82.

Respectfully announced to the public.

Public Announcement on Application for Commitment

Public Announcement on Application for Commitment

The application made by the data controller, TEB Arval Vehicle Fleet Leasing Corporation, for the Commitment with regard to the transfer of personal data abroad was evaluated within the scope of Article 9(2) of the Personal Data Protection Law No 6698, and permission for the data transfer in question was granted by the Board on 09.02.2021.

Public Announcement on Covid-19

Public Announcement on Covid-19

The various measures are taken against Covid-19 virus that take hold of all over the world and our country, by data controllers which operate both in public and private sectors. While these developments continue, a statement become necessary to be made with respect to the periods that are necessary to be taken into account by data controllers in terms of complaints, notices and data breach notifications submitted to the Authority within the scope of Personal Data Protection Law No. 6698.

As known, relating to the complaints, notices and data breach notifications submitted to the Authority within the scope of the legislation on the protection of personal data, various periods are determined both in the Law and relevant legislation with regard to the obligations of data controllers to either the Authority or data subjects. The compliance with these periods by data controllers is important.

On the other hand, in this extraordinary conditions that our country is in, by taking into account that the different operational implementations (remote working, shift working etc.) are used with respect to the measures taken by data controllers, for each complaint or data breach notification, it is announced to the public respectfully that the Personal Data Protection Board will pay regard to the extraordinary conditions that we are in with respect to the consideration of the periods that data controllers are obliged to comply with.

Public Announcement on Distance Learning Platforms

Public Announcement on Distance Learning Platforms

It is seen that, in distance learning platforms, personal data such as names and surnames of the students as well as some special categories of data that can be evaluated within the scope of biometric data such as voice and image, are processed.

Article 5 of Personal Data Protection Law No.6698 specifies the conditions for the processing of personal data and Article 6 of the same Law determines the conditions for special categories of personal data including biometric data. With regards to this, personal data should be processed in accordance with the conditions specified in Article 5 and/or Article 6 of the Law.

Furthermore, it is observed that much software that is used for distance learning provides services through cloud service providers and the data centers of such software are mostly located abroad. It should be noted that transfers that do not comply with the conditions set out in Article 9 of the Personal Data Protection Law may be in a violation of the Law, due to the fact that transfer of personal data abroad would come into question in case platforms with data centers abroad are used.

In this regard, "Personal Data Security Guide (Technical and Organisational Measures)" prepared by the Personal Data Protection Board and the Board Decision No. 2018/10 of 31/01/2018 on "Adequate Measures to be taken for the Processing Special Categories of Personal Data by Data Controllers" should be taken into consideration regarding whether these platforms used for distance learning services take necessary data security measures.

Public Announcement on the Commitment Application

Public Announcement on the Commitment Application

Commitment application regarding transfer of personal data abroad by data controllers Amazon Turkey Retail Services Co. Ltd. and Amazon Turkey Management Support Services Co. Ltd. was evaluated by the Personal Data Protection Board within the scope of paragraph 2 (b) of the Article 9 of the Personal Data Protection Law No.6698 and the data transfer in question was permitted by the Board on 04.03.2021.

Public Announcement on the Extension of the Registration Periods to Verbis (Data Controllers Registry)

Public Announcement on the Extension of the Registration Periods to Verbis (Data Controllers Registry)

Due to Covid-19 pandemic, which has an effect in our country as in the whole world, some workplaces are physically closed or a remote /alternate working model is applied, on the grounds that it is not possible to prepare personal data processing inventory for the data controllers, and the controllers could not fulfil the obligation to register to the Data Controllers Registry in due time, as a result of the evaluation of the requests conveyed to Authority for the extension of the registration periods to the Registry by Turkish Union of Chambers and Commodity Exchanges (TOBB) and various industry representatives, with the decision of Personal Data Protection Board dated 23.06.2020 numbered 2020/482; it has been decided unanimously that;

- For the natural and legal person data controllers and the natural and legal person data controllers abroad, whose annual number of employees is more than 50 or the annual financial balance sheet total more than 25 million TL, the date to fulfil obligation to register in the Registry has been extended to 30.09.2020,
- For the natural and legal person data controllers whose main field of activity is processing of sensitive personal data and whose annual number of employees is less than 50 or the annual financial balance sheet total less than 25 million TL, the date to fulfil obligation to register in the Registry has been extended to 31.03.2021,
- For the public institutions and organizations, the date to fulfil obligation to register in the Registry has been extended to 31.03.2021,
- Announcement of the mentioned decision shall be published on the website of the Authority and in the Official Gazette.

Respectfully announced to the public.

Public Announcement on Whatsapp Application

Public Announcement on Whatsapp Application

As is known, Article 2 of Personal Data Protection Law No.6698, which entered into force after being published in the Official Gazette of 7 April 2016, states that “The provisions of this Law shall apply to natural persons whose personal data are processed and to natural or legal persons processing such data wholly or partially by automated means or by non-automated means which provided that form part of a data filing system.”

Furthermore, in order to process personal data, any of the processing conditions specified in Articles 5 and 6 of the Law must be in place. Pursuant to Article 5(2) of the Law, personal data can be processed in cases where one of the following conditions is met: “Processing is expressly provided for by the laws; it is necessary for the protection of life or physical integrity of the person himself/herself or of any other person who is unable to explain his/her consent due to the physical disability or whose consent is not deemed legally valid; processing of personal data of the parties of a contract is necessary; provided that it is directly related to the establishment or performance of the contract, it is necessary for compliance with a legal obligation to which the data controller is subject; personal data have been made public by the data subject himself/herself; data processing is necessary for the establishment, exercise or protection of any right; processing of data is necessary for the legitimate interests pursued by the data controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.” In the absence of these conditions, personal data can only be processed by obtaining the explicit consent of the data subject.

Explicit consent is defined as “ the freely given, specific and informed consent” in Article 3 of the Law, and accordingly, explicit consent has three elements:

- It is related to a specific subject,
- Consent is based on information,
- Freely given

When evaluated in terms of the elements mentioned above, explicit consent means that the person gives consent to the processing of his or her data in accordance with the law. Another importance of the explicit consent is that it guides the data controller about the data processing activity that it will carry out. With the explicit consent expressed, the person actually informs the data controller about

his or her legal value. Explicit consent can also enable the data subject to determine the limits, scope, form and duration of processing of data that he/she permits to be processed. In this sense, explicit consent must include the positive declaration of the will of the person who gives the consent.

By reason of the fact that explicit consent to the processing of personal data is a strictly personal right, the explicit consent given can be withdrawn. In this context, the right to determine the future of personal data belongs to the data subject, and the person can withdraw his or her explicit consent given to the data controller at any time. However, since the withdrawal process will have forward-looking results, all activities carried out based on the explicit consent must be stopped by the data controller as soon as the withdrawal statement reaches the data controller. In other words, the withdrawal statement becomes effective from the moment it reaches the data controller.

On August 2, 2018, summary of Decision No 2018/19 of the Personal Data Protection Board of 16.02.2018 was published on the Authority's website regarding the issues where "explicit consent" is determined as a legal reason for the processing of personal data and service provided is subject to the explicit consent. As stated in the Board Decision, the explicit consent obtained from the data subjects during the processing of personal data cannot be put forward by the data controllers as a prerequisite for the performance of a service.

Pursuant to Article 4 of the Law, personal data must be processed in accordance with the principle of lawfulness and fairness; processed for specified, explicit and legitimate purposes; and the processing must relevant, limited and proportionate to the purposes for which they are processed; the necessary information must be provided about which personal data will be processed or to whom and for what purposes it will be transferred, and it is necessary to obtain explicit consent separately by offering the option for each processing/transfer activity.

On the other hand, Article 9 of the Law, titled "transfer of personal data abroad" states that personal data shall not be transferred abroad without explicit consent of the data subject; however, according to the paragraph 2 of the same article, personal data may be transferred abroad without explicit consent of the data subject upon the existence of one of the conditions referred to in Article 5(2) and, in terms of the sensitive data, Article 6(3) of the Law, and provided that in the country where personal data are to be transferred adequate protection is provided, and where the adequate protection is not provided, upon the existence of commitment for adequate protection in writing by the data controllers in Turkey and in the relevant foreign country and authorisation of the Board.

It has been found that WhatsApp Inc. has updated the terms of use to include consent to the processing of personal data of the users who would like to use the WhatsApp application and to the

transferring of their data to third parties abroad, and within this context, the users are informed that the ones who do not give consent will not be able to use the application and their accounts will be deleted.

The Privacy Policy referred to in the information text in question states which data will be processed for what purposes; however, it is also seen that personal data processed will be transferred by WhatsApp Inc. to not-explicitly-specific parties such as the Facebook group companies established abroad from which WhatsApp Inc. receives and provides services, suppliers, business partners, service providers and other third party data controllers in order to provide, again, not-explicitly-specific services such as technical support, delivery and other services, conduct researches, surveys and marketing.

As a result of the preliminary evaluation regarding obtaining explicit consent for the processing of personal data by WhatsApp Inc., a data controller established abroad, and for their transfer to other data controllers established abroad, considering the following issues;

- The process of obtaining consent from the users for the processing of their personal data and their transfer to third parties established abroad is not separated; however, considering that users may not consent to their personal data being transferred to another data controller abroad while giving their consent to the processing, taking into account the prevalence use of the application in question, whether this situation constitutes a breach in terms of being “freely given” from the elements of explicit consent specified in the Law,
- Whether allowing the use of application provided that the data are transferred to another company established abroad constitutes a violation in terms of the principles listed in Article 4 of the Law, as “compliance with the lawfulness and fairness”, “being processed for specified, explicit and legitimate purposes”, and “being relevant, limited and proportionate to the purposes for which they are processed”,
- Considering that the fact that the service provided is subject to the explicit consent may interfere with the explicit consent given, which may result in the unlawful processing of personal data, whether the service will still be subject to the consent, with the update made by WhatsApp Inc.,
- Whether there is a violation of Article 9 of the Law regarding the transfer to be made by WhatsApp Inc. to the data controllers established abroad,

It has been decided to launch an ex officio investigation on WhatsApp Inc. with the Decision No 2021/28 of Personal Data Protection Board of 12.01.2021.

A new evaluation will be made by the Board on 08.02.2021 regarding the process.

Respectfully announced to the public.

Regarding Processing of Location Data and Tracking Mobility of Individuals to Combat Covid-19

As known, all countries all over the world, including Turkey, have taken various measures and precautions to protect against the disease caused by COVID-19 (Coronavirus) virus that has spread worldwide. At this point, besides traditional measures such as quarantine, social distancing and social isolation, it is also seen that technological facilities are being used.

Within this scope, in order to prevent the spread of coronavirus in various countries; personal data such as health, location and contact information of data subjects are being processed by methods like mobile applications for purposes of such as identifying the people who contacted with the carriers or those who are at risk of carrying the virus, implementation of treatment and quarantine by mapping the spread of the virus, control of those under quarantine, implementation of curfew, detection of crowded places.

In circumstances such as an epidemic disease, it is legally possible for the competent institutions and organizations to take measures in order to maintain public order and security. It is also indisputable that the security of personal data should be observed in such cases.

Within this framework, in order for processing of personal data such as tracking the location and mobility of the individuals to be lawful, these activities need to be carried out within the framework of the fundamental principles governing the data protection law and this issue should be addressed in terms of our law.

In the Regulation on Processing of Personal Data and Protection of Privacy in the Electronic Communication Sector, location data are defined as "Specific data processed in an electronic communications network or by means of electronic communication service, indicating the geographic position of the device of a user of a publicly available electronic communications service", and it is clear that the location data that make natural persons identifiable are deemed as personal data under Personal Data Protection Law No.6698 (Law No.6698).

In cases where location data need to be used by relating to a natural person;

The provisions of Law does not apply in cases where personal data are processed within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations duly authorised and assigned by law to maintain national defence, national security, public security and order or economic security, pursuant to subparagraph (ç) of Article 28(1) of Law No.6698.

From this viewpoint, in order to eliminate the threat in situations where public order and public security are threatened by, such as, an epidemic disease, data processing activities to be carried out by competent public institutions and organizations in order to ensure isolation of people who have been diagnosed with the disease, to identify crowded areas by processing location data of the general population and to develop measures in these areas, are evaluated under the subparagraph (ç) of Article 28(1) of the Law.

In this context, there is no obstacle to the processing of location data by the competent institutions and organizations which fall under the scope of the mentioned article, in order to prevent the spread of the disease caused by COVID-19 that threatens public security and public order.

**The Board Decision No. 2019/10 of 24.01.2019 about Procedures and Principles of Personal Data
Breach Notification**

**The Board Decision No. 2019/10 of 24.01.2019 about Procedures and Principles of Personal Data
Breach Notification**

As known, pursuant to paragraph (1) of article 12 of the Personal Data Protection Law No. 6698 the data controller is obliged to take all necessary technical and organisational measures to ensure the appropriate level of security, so as to:

- a. Prevent unlawful processing of personal data,
- b. Prevent unlawful access to personal data,
- c. Ensure protection of personal data.

According to Article 12(5), in case the processed data are obtained by third parties by unlawful means, the data controller shall communicate the breach to the data subject (natural person concerned) and notify it to the Board within the shortest time. Where necessary, the Board may announce such breach at its official website or through in any other way it deems appropriate.

The purpose of the notification to the Board and to persons affected by the breach is to ensure that measures are taken to prevent or mitigate the adverse consequences of such violations. On the other hand, in respect of data breach notifications, European General Data Protection Regulation, which repeals Directive 95/46 / EC of the European Union which is the source of Law No. 6698, includes detailed arrangements contrary to the Directive. In order to ensure that there is no inconsistency between the decisions to be taken by the Board and that standardization can be achieved in practice; the Board adopted following decisions;

- The Board interpreted the provision of “the shortest time” in Article 12 (5) of the Law (In case the processed data are obtained by others by unlawful means, the data controller shall communicate the breach to the data subject and notify to the Board within the shortest time...) as 72 hours and within this scope the data controller shall notify the Board without delay and not later than 72 hours after having become aware of the breach. From the date following the identification of persons affected by such data breach, data subjects should be communicated about breach in the shortest reasonable period of time. If the contact address of the data subject can be reached,

notification should be made directly, or if it cannot be reached, notification should be made by appropriate methods such as the publication on the data controller's website,

- Where such notification cannot be achieved within 72 hours, the reasons for the delay should be attached to the notification to be made to the Board without undue further delay.
- The following "Personal Data Breach Notification Form" shall be used in the notification to the Board,
- In cases where it is not possible to provide the information in the form simultaneously, this information shall be provided gradually, without delay.
- The controller shall document all personal data breaches, including the facts relating to the personal data breach, its effects and the measures taken. That documentation shall be available for Board to examine.
- If the personal data held by the data processor is obtained by others by unlawful methods, the data processor shall notify the data controller without any delay.
- If data breach occurs in the presence of data controller established abroad, in case this breach affects data subject residing in Turkey and Data Subjects benefit from the products and services provided within Turkey, data controller shall notify the Board within the same principles,
- In case of a data breach, data controller shall prepare a data breach response plan to be reviewed periodically including issues such as to whom the report will be provided by the controller and determination of who has the responsibility regarding the notification to be made under The Law as well as the assessment of potential consequences of the data breach.

The following "Personal Data Breach Notification Form" shall be used in the notification to the Board.

For data breach notification the following link shall be used.

Respectfully announced to the public.

The Board Decision No. 2019/125 of 02/05/2019 about the form prepared to be used in the determination of the countries having adequate level of protection

The Board Decision No. 2019/125 of 02/05/2019 about the form prepared to be used in the determination of the countries having adequate level of protection

Decision Date : 02/05/2019

Decision Number : 2019/125

Subject Summary : The form prepared to be used in the determination of the countries having adequate level of protection

As is known to all, pursuant to Article 9 of the Personal Data Protection Law No. 6698 (the Law), personal data shall not be transferred abroad without explicit consent of the data subject. In the event that adequate protection is provided or when adequate protection is not provided, upon the existence of commitment for adequate protection in writing by the data controllers in Turkey and in the relevant foreign country and authorization of the Board personal data may be transferred abroad without explicit consent of the data subject. Moreover, the Article 9 contains the provisions that the countries with adequate protection are to be determined and announced by the Board and the issues are to be evaluated in the announcement of relevant countries.

In this context, pursuant to Article 9 of the Law, the relevant criteria adopted in the Board Decision No. 2019/125 of 02/05/2019 to be used in the determination of the countries having adequate level of protection can be accessed on the link below.

The criteria to be based on the determination of the countries having adequate level of protection...

CRITERIA FOR THE DETERMINATION OF COUNTRIES HAVING ADEQUATE LEVEL OF PROTECTION			
EXAMINED COUNTRY:			
RELEVANT ORGANIZATION OF EXAMINED COUNTRY:			
EVALUATION			
CRITERIA	AVAILABLE	NOT AVAILABLE	EXPLANATION
1. Reciprocity status			
2. Legislation of the relevant country and implementation of this legislation regarding the processing of personal data			
2.1. Personal data protection is a constitutional right			
2.2. The existence of a basic law on the personal data protection			
2.3. Effective date of the Basic Law			
2.4. Secondary regulations and compliance of these regulations with our legislation			
2.5. Basic concepts of personal data protection			
2.6. General Principles on the Personal Data Protection			
2.7. Compliance of the personal data processing conditions with the personal data processing conditions in the Law No. 6698			
2.8. Existence of specific processing conditions and additional security measures for the processing of sensitive personal data			
2.9. Existence of legal guarantees that personal data processing activities are carried out in accordance with the principle of transparency			
Obligation to take the necessary technical and organizational measures to provide the adequate level of security in order to prevent unlawful processing and access to personal data and to ensure the protection of personal data			

Technical measures			
Organizational measures			
2.11. Implementation status of administrative and/or penal sanctions against the data breach and other mechanisms to prevent data breach			
2.12. Rights of data subject			
2.13. The right to request of data subjects to the controller and the right to lodge complaint with to the data protection authority			
2.14. The right to compensation of data subjects whose rights on personal data have been violated according to the general provisions			
2.15. Implementation guidelines/publications as reference			
2.16. Exemptions to the implementation of the Law			
2.17. Data transfer system			
3. Existence of an independent data protection authority			
3.1. Structure			
3.2. Independence status			
3.3. Duties and powers			
3.4. Its authority to audit/investigate			
3.5. Whether there is a remedy to appeal against its decisions			
4. The status of being a party in the international agreements on the personal data protection and being a member of international organizations			
4.1. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No. 108			

4.2. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows No.181			
4.3. Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters(CETS 182)			
4.4. European Convention on Human Rights			
4.5. International Conference of Data Protection and Privacy Commissioners (ICDPPC)			
4.6. Global Privacy Enforcement Network (GPEN)			
5. Whether a member of global and regional organizations that Turkey is a member			
6. Trade volume with relevant country			
7. Other			

The Decision of Personal Data Protection Board No. 2018/88 of 19/07/2018 on “The Starting Dates of Obligation to Register with the Data Controller’s Registry”

The Decision of Personal Data Protection Board No. 2018/88 of 19/07/2018 on “The Starting Dates of Obligation to Register with the Data Controller’s Registry”

Decision Date : 19/07/2018

Decision No : 2018/88

Subject Summary : The starting dates of the obligation to register with Data Controllers’ Registry

By taking into consideration the provisions “Natural or legal persons who process personal data shall register with the Data Controllers’ Registry prior to the start of data processing. However, by taking into account the objective criteria set by the Board such as the nature and quantity of the data processed, that data processing is laid down in a law, or transferring the data to third parties, the Board may provide derogation from the obligation of registration with the Data Controllers’ Registry.” in the Article 16(2) and “Data controllers are obliged to register with the Data Controllers’ Registry within the time specified and announced by the Board.” in the Provisional Article 1(2) of the Personal Data Protection Law No. 6698;

The Board has adopted the following decisions unanimously:

- For natural and legal person data controllers whose number of employees is more than 50 or annual financial balance sheet is greater than 25 million Turkish Liras, the starting date of obligation to register with Data Controllers’ Registry is 01.10.2018 and the deadline for the registration of these data controllers is 30.06.2020[1] ,
- For data controllers which are natural and legal persons not established in Turkey, the starting date of obligation to register to Data Controllers’ Registry is 01.10.2018 and the deadline for the registration of these data controllers is 30.06.2020[2] ,
- For natural and legal person data controllers whose number of employees are fewer than 50 and annual turnover is less than 25 million Turkish Liras as well as their field of main activity is processing special categories of personal data, the starting data of obligation to register with the

Data Controllers' Registry is 01.01.2019 and the deadline for registration of these data controllers is 30.09.2020[3],

- For public institutions and organizations, the starting date of obligation to register with the Data Controllers' Registry is 01.04.2019 and the deadline for the registration of these data controllers is 31.12.2020[4],
- This Decision will be published on the Official Website of the Authority and in the Official Gazette.

THE DATE OF REGISTRATION WITH THE DATA CONTROLLERS' REGISTRY ANNOUNCED BY PERSONAL DATA PROTECTION BOARD ACCORDING TO THE PROVISIONAL ARTICLE 1* OF THE LAW NO. 6698			
Data Controllers	The starting date of obligation to register	The prescribed time to register	The deadline to register
Natural and legal person data controllers whose number of employees are more than 50 or annual turnover is more than 25 million Turkish Liras	01.10.2018	12 months	30.06.2020
Data controllers which are natural and legal person not established in Turkey	01.10.2018	12 months	30.06.2020
natural and legal person data controllers whose number of employees are less than 50 and annual turnover is less than 25 million Turkish Liras as well as their field of main activity is processing special categories of personal data,	01.01.2019	15 months	30.09.2020
Public Institutions and Organizations	01.04.2019	15 months	31.12.2020
<p>*Provisional Article 1-(2) Data controllers are obliged to register with the Data Controllers' Registry within the time specified and announced by the Board. 1 The deadline for registration of these data controllers have been updated as 30.06.2020 by the Board</p> <p>[1] The deadline for registration of these data controllers have been updated as 30.06.2020 by the Board Decision No. 2019/387 of 17/12/2019.</p> <p>[2] The deadline for registration of these data controllers have been updated as 30.09.2020 by the Board Decision No. 2019/387 of 17/12/2019.</p> <p>[3] The deadline for registration of these data controllers have been updated as 31.12.2020 by the Board Decision No. 2019/387 of 17/12/2019.</p>			

[1] The deadline for registration of these data controllers have been updated as 30.06.2020 by the Board Decision No. 2019/387 of 17/12/2019.

[2] The deadline for registration of these data controllers have been updated as 30.06.2020 by the Board Decision No. 2019/387 of 17/12/2019.

[3] The deadline for registration of these data controllers have been updated as 30.09.2020 by the Board Decision No. 2019/387 of 17/12/2019.

[4]The deadline for registration of these data controllers have been updated as 31.12.2020 by the Board Decision No. 2019/387 of 17/12/2019.

Fulfilment of Obligation to Inform

PUBLIC ANNOUNCEMENT ON FULFILMENT OF OBLIGATION TO INFORM

Within the framework of Law No. 6698 on the Protection of Personal Data, secondary legislation regarding the Law and decisions made by the Personal Data Protection Board, the data controllers have a number of obligations. One of these obligations is obligation to inform specified in the Article 10 of the Law.

As well as obligation to inform is a responsibility for the data controllers; it is also a right for the natural persons whose data are processed. Obligation to inform, which means that the data subject is informed regarding processed personal data, is an essential condition for the personal data processing to be performed in accordance with the law.

Fulfilment of obligation to inform is not an obligation on a request of data subject. In addition, the data controller shall fulfil the obligation to inform in each of the cases where the data subject's explicit consent or any other personal data processing conditions exist when processing personal data. Since the obligation to inform is an obligation that must be fulfilled in any case, regardless of both explicit consent and other personal data processing conditions listed in the Law.

As a result of the evaluation made on the information and documents conveyed to the Authority by the relevant data controllers upon the for notices and complaints made to our Authority or other documents that are foreseen to be examined and investigated by the Board;

It has been determined that there are deficiencies and violations of the legislation such as;

- That the informing is not done by the data controller during the obtaining personal data from the data subject, it is done afterwards or not at all,
- That the content of the informing does not cover the issues listed in the Article 10 of the Law No. 6698,
- That in the informing, the purpose of personal data processing is not limited, specific, explicit or legitimate to the processing activity, statements expressing that personal data may be processed for other purposes which are likely to come to the agenda in the future are used,
- That "Legal reason", which is one of the minimum elements of informing, and "purpose of processing" are used in the same sense or there is no place for legal reason,

- That understandable, clear and plain language is not used in the texts used for informing, information that are general, suitable for misunderstanding, incomplete, misleading data subjects and wrong are included,
- That in the informing process, the purpose of transfer and the group or groups of transmitters are not sufficiently covered,
- That the informing texts are “privacy policies” or “data processing policies”, which have the characteristics of general data processing documents for the data controller,
- That informing texts are not presented on a platform that can be easily accessed by the data subjects,
- That when a layered approach to inform is preferred, before the data subjects are directed to another channel for detailed information, in the first stage, basic information is not presented, appropriate ways and methods for accessing detailed information are not followed, data subjects are generally directed to privacy policies or data processing policies,
- That explicit consent and informing are presented together under the same title in the same text or platform,
- That the confirmation regarding that the informing has been made is requested and the service is not provided if the consent is not given.

Due to the mentioned deficiencies and violations of the legislation, the data controllers should pay particular attention to the following issues while fulfilling their obligation to inform in order not to face the sanctions specified in the Law:

- a) The proof of fulfilment of the obligation to inform belongs to the data controller.
- b) The obligation to inform should be fulfilled by the data controller or the persons authorized by the data controller during the obtaining personal data from the data subject.
- c) The informing to be made within the scope of the obligation to inform shall include “the identity of the controller and of his representative, if any, the purpose of data processing, to whom and for what purposes the processed data may be transferred, the method and legal reason of collection of personal data which are included in the Article 10 of the Law and the rights of data subject specified in the Article 11 of the Law”
- d) According to the Communiqué On Principles and Procedures To Be Followed in Fulfilment of the Obligation to Inform published in the Official Gazette dated 10.03.2018; in cases where personal data are not obtained directly from data subjects due to actual impossibility or inaccessibility of the data subject, the obligation to inform shall be fulfilled within a reasonable time following the obtainment

of the personal data or at the first instance of communication in case personal data are used to communicate with the data subject; and at the time of the first transfer of personal data at the late

e) The personal data to be disclosed during the fulfilment of the obligation to inform should be specific, clear, legitimate, and limited to the purposes for the processing activity. Statements expressing that personal data may be processed for other purposes which are likely to come to the agenda in the future should not be used.

f) Clear, plain language should be used in the texts when fulfilling the obligation to inform. In addition, general, ambiguous, incomplete, misleading and false information should not be included.

g) "Processing purpose" and "legal reason" are the separate elements that should be included in the information to be made while fulfilling the obligation to inform and it should be noted that with the statement "legal reason" of collecting data it is referred that the personal data are processed based on which processing conditions specified in the Articles 5 and 6 of the Law.

h) Privacy policies or data processing policies, which are not limited to the processing activity and which have the characteristics of general data processing documents for the data controller, should not be used as informing texts.

i) Attention should be paid to make the informing easily accessible and noticeable, and methods that would make it difficult for the data subjects to access the informing should not be used.

j) In cases where the transfer of personal data are transferred, the purpose of the transfer and the group of recipients to whom the transfer is made should also be included in the informing.

k) If a layered approach to inform is preferred, it should be ensured that the basic information (for example, the identity of the data controller and the purpose of the data processing) is presented in the first stage and that the directed text has limited content for the processing activity before the data subjects are directed to another channel for detailed information.

In this context, it is necessary to act in accordance with the Law No. 6698, Communiqué On Principles And Procedures To Be Followed In Fulfilment Of The Obligation To Inform, Board Decisions published on the website of the Authority and the Guide on Fulfilment of Obligation to Inform prepared by our Authority while fulfilling the obligation to inform.

Respectfully announced to the public.

TÜRK HUKUKUNDAKİ DİĞER DÜZENLEMELER

Bölüm İçeriği

- Kanunlar
- Tüzükler
- Yönetmelikler
- Tebliğler
- Cumhurbaşkanlığı Kararnameleri
- Genelgeler

KANUNLAR

Bölüm İçeriği

- 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu
- 7252 sayılı Dijital Mecralar Komisyonu Kurulması ile Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun
- 7223 sayılı Ürün Güvenliği ve Teknik Düzenlemeler Kanunu
- 7091 sayılı Olağanüstü Hal Kapsamında Alınması Gereken Tedbirler Hakkında Kanun Hükmünde Kararnamenin Kabul Edilmesine Dair Kanun
- 7075 sayılı Olağanüstü Hal İşlemleri İnceleme Komisyonu Kurulması Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun
- 7068 sayılı Genel Kolluk Disiplin Hükümleri Hakkında Kanun Hükmünde Kararnamenin Kabul Edilmesine Dair Kanun
- 6713 sayılı Kolluk Gözetim Komisyonu Kurulması Hakkında Kanun
- 6706 sayılı Cezai Konularda Uluslararası Adli İşbirliği Kanunu
- 6701 sayılı Türkiye İnsan Hakları ve Eşitlik Kurumu Kanunu
- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunu
- 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun
- 6475 sayılı Posta Hizmetleri Kanunu
- 6458 sayılı Yabancılar ve Uluslararası Koruma Kanunu
- 6362 sayılı Sermaye Piyasası Kanunu
- 6328 sayılı Kamu Denetçiliği Kurumu Kanunu
- 6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun
- 6114 sayılı Ölçme, Seçme ve Yerleştirme Merkezi Başkanlığının Teşkilat ve Görevleri Hakkında Kanun
- 6102 sayılı Türk Ticaret Kanunu
- 6100 sayılı Hukuk Muhakemeleri Kanunu
- 6098 sayılı Türk Borçlar Kanunu
- 5809 sayılı Elektronik Haberleşme Kanunu
- 5718 sayılı Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun
- 5684 sayılı Sigortacılık Kanunu

- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- 5624 sayılı Kan ve Kan Ürünleri Kanunu
- 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu
- 5502 sayılı Sosyal Güvenlik Kurumu Kanunu
- 5490 sayılı Nüfus Hizmetleri Kanunu
- 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu
- 5429 sayılı Türkiye İstatistik Kanunu
- 5411 sayılı Bankacılık Kanunu
- 5352 sayılı Adli Sicil Kanunu
- 5271 sayılı Ceza Muhakemesi Kanunu
- 5258 sayılı Aile Hekimliği Kanunu
- 5237 sayılı Türk Ceza Kanunu
- 5070 sayılı Elektronik İmza Kanunu
- 4982 sayılı Bilgi Edinme Hakkı Kanunu
- 4904 sayılı Türkiye İş Kurumu ile İlgili Bazı Düzenlemeler Hakkında Kanun
- 4857 sayılı İş Kanunu
- 4721 sayılı Türk Medeni Kanunu
- 4632 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanunu
- 3359 sayılı Sağlık Hizmetleri Temel Kanunu
- 2937 sayılı Devlet İstihbarat Hizmetleri Ve Milli İstihbarat Teşkilatı Kanunu
- 2920 sayılı Türk Sivil Havacılık Kanunu
- 2559 sayılı Polis Vazife ve Selâhiyet Kanunu
- 1774 sayılı Kimlik Bildirme Kanunu
- 1512 sayılı Noterlik Kanunu
- 1136 sayılı Avukatlık Kanunu
- 1211 sayılı Türkiye Cumhuriyet Merkez Bankası Kanunu
- 211 sayılı Türk Silahlı Kuvvetleri İç Hizmet Kanunu

7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu

Resmî Gazete Tarihi : 17.04.2021

Resmî Gazete Sayısı : 31457

GÜVENLİK SORUŞTURMASI VE ARŞİV ARAŞTIRMASI KANUNU

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç ve kapsam

MADDE 1- (1) Bu Kanun, güvenlik soruşturması ve arşiv araştırmasının yapılmasına ve elde edilecek verilerin kullanılmasına ilişkin temel ilkeleri, kimler hakkında yapılacağını, araştırma konusu edilecek bilgi ve belgelerin neler olduğunu, bu bilgilerin ne şekilde kullanılacağını, hangi mercilerin soruşturma ve araştırma yapacağını, Değerlendirme Komisyonunun oluşumu ve çalışma usul, esaslarını, veri güvenliği ile verilerin saklanma ve silinme sürelerini düzenlemektedir.

Tanımlar

MADDE 2- (1) Bu Kanunda geçen;

- a) Değerlendirme Komisyonu: Güvenlik soruşturması veya arşiv araştırması sonucunda elde edilen kişisel verilerin göreve atanma yönünden değerlendirildiği komisyonu,
 - b) Kurum ve kuruluş: Güvenlik soruşturması ve/veya arşiv araştırması yapılmasını talep eden kamu kurum ve kuruluşları ile milli güvenlik açısından stratejik önemi haiz birim, proje, tesis ve hizmetleri yerine getiren diğer kurum ve kuruluşu,
 - c) Üst kademe kamu yöneticisi: Atanmasına ilişkin usul ve esaslar Cumhurbaşkanlığı kararnamesi ile üst kademe kamu yöneticisi olarak belirlenenini,
- ifade eder.

İKİNCİ BÖLÜM

Güvenlik Soruşturması ve Arşiv Araştırması

Hakkında güvenlik soruşturması ve arşiv araştırması yapılacaklar

MADDE 3- (1) Arşiv araştırması, statüsü veya çalıştırma şekline bağlı olmaksızın ilk defa veya yeniden memuriyete yahut kamu görevine atanacaklar hakkında yapılır.

(2) Kurum ve kuruluşlarda, yetkili olmayan kişilerin bilgi sahibi olmaları hâlinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile Milli Savunma Bakanlığı, Genelkurmay Başkanlığı, jandarma, emniyet, sahil güvenlik ve istihbarat teşkilatlarında çalıştırılacak kamu personeli ile ceza infaz kurumları ve tutukevlerinde çalışacak personel, kamu kurum ve kuruluşlarında çalışacak öğretmenler, üst kademe kamu yöneticileri, özel kanunları uyarınca güvenlik soruşturması ve arşiv araştırmasına tabi tutulan kişiler ile milli güvenlik açısından stratejik önemi haiz birim, proje, tesis, hizmetlerde statüsü veya çalıştırma şekline bağlı olmaksızın istihdam edilenler hakkında güvenlik soruşturması ve arşiv araştırması birlikte yapılır.

Arşiv araştırması

MADDE 4- (1) Arşiv araştırması;

- a) Kişinin adli sicil kaydının,
- b) Kişinin kolluk kuvvetleri tarafından hâlen aranıp aranmadığının,
- c) Kişi hakkında herhangi bir tahdit olup olmadığının,
- ç) Kişi hakkında kesinleşmiş mahkeme kararları ve 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun 171 inci maddesinin beşinci ve 231 inci maddesinin onüçüncü fıkraları kapsamında alınan kararlar ile kişi hakkında devam eden veya sonuçlanmış olan soruşturma ya da kovuşturmalar kapsamındaki olguların,
- d) Hakkında kamu görevinden çıkarılma ya da kesinleşmiş memurluktan çıkarma cezası olup olmadığının,

mevcut kayıtlardan tespit edilmesidir.

Güvenlik soruşturması

MADDE 5- (1) Güvenlik soruşturması, arşiv araştırmasındaki hususlara ilave olarak kişinin;

- a) Görevin gerektirdiği niteliklerle ilgili kolluk kuvvetleri ve istihbarat ünitelerindeki olgusal verilerinin,
- b) Yabancı devlet kurumları ve yabancılarla ilişkisinin,

c) Terör örgütleri veya suç işlemek amacıyla kurulan örgütlerle eylem birliđi, irtibat ve iltisak içinde olup olmadığının,

mevcut kayıtlardan ve kişinin görevine yansıyacak hususların denetime elverişli olacak yöntemlerle yerinden araştırılmak suretiyle tespit edilmesidir.

Güvenlik soruşturması ve arşiv araştırmasını yapacak birimler

MADDE 6- (1) Güvenlik soruşturması ve arşiv araştırması, Milli İstihbarat Teşkilatı Başkanlığı, Emniyet Genel Müdürlüğü ve mahalli mülki idare amirlikleri tarafından yapılır.

(2) Güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimler, kendilerine iletilen taleple sınırlı olarak güvenlik soruşturması ve arşiv araştırması kapsamında bakanlıklar ile kamu kurum ve kuruluşları arşivlerinden ve elektronik bilgi işlem merkezlerinden gerekli bilgi ve belgeler ile bu Kanunun 4 üncü maddesinin birinci fıkrasının (ç) bendi kapsamındaki karar ve kayıtları almaya yetkilidir.

(3) Güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimlerde yetkilendirilmiş personel, hukuka aykırı olarak elektronik ortamda veya bilgisayar loglarında kişisel verilerle ilgili sorgulama yapamaz, log kayıtlarını değiştiremez veya silemez, bu şekilde elde edilen bilgileri paylaşamaz veya yayın yoluyla duyuramaz. Görevi geređi öğrendiđi veya edindiđi kişisel bilgi veya belgeleri yetkisiz kişilerle paylaşamaz ya da basın ve yayın kuruluşlarına veya diđer iletişim kanallarına veremez. Güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimler tarafından bu hususlara ilişkin gerekli tedbirler alınır.

Deđerlendirme Komisyonu

MADDE 7- (1) Yaptırılan güvenlik soruşturması ve arşiv araştırması sonucunda elde edilen verilerin deđerlendirilmesi amacıyla Deđerlendirme Komisyonu kurulur. Deđerlendirme Komisyonu; Cumhurbaşkanlığında İdari İşler Başkanının görevlendireceđi bir üst kademe yöneticisinin, Türkiye Büyük Millet Meclisi Başkanlığında genel sekreter yardımcısının, bakanlıklarda bakan yardımcısının, diđer kamu kurum ve kuruluşlarında en üst yöneticinin görevlendireceđi bir üst kademe yöneticisinin, üniversitelerde rektör yardımcısının, valiliklerde vali yardımcısının başkanlığında, teftiş/denetim, personel ve hukuk birimleri ile uygun görülecek diđer birimlerden birer üyenin katılımıyla başkan dahil en az beş kişiden ve tek sayıda olacak şekilde oluşturulur. Milli güvenlik açısından stratejik önemi haiz birim, proje, tesis ve hizmetlerde istihdam edilecekler hakkındaki deđerlendirme, ilgili bakanlık ya da kamu kurumları bünyesindeki Deđerlendirme Komisyonunca yapılır.

(2) Memuriyet veya kamu görevlerine uygunluğunun değerlendirilmesini sağlayacak yorum içermeyen olgusal veriler, güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimlerce ilgili kurum ve kuruluş bünyesinde kurulan Değerlendirme Komisyonuna iletilir.

(3) Değerlendirme Komisyonu kendisine iletilen verilere ilişkin nesnel ve gerekçeli değerlendirmelerini yazılı olarak atamaya yetkili amire sunar. Mahkemeler tarafından istenildiğinde bu bilgiler sunulur.

ÜÇÜNCÜ BÖLÜM

Kişisel Verilerin Korunması

Kişisel verilerin korunmasına ilişkin temel ilkeler

MADDE 8- (1) Güvenlik soruşturması ve arşiv araştırması kapsamında kişinin istihbari faaliyetlere konu olmayan kendisiyle ilgili kişisel verileri hakkında bilgilendirilmesi, bu verilere erişmesi, bunların düzeltilmesi ve silinmesi taleplerine ilişkin tedbirler alınır.

(2) Güvenlik soruşturması ve arşiv araştırmasına konu kişisel verilerin doğru ve güncel olması esastır. Bu veriler, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak kullanılır.

(3) Güvenlik soruşturması ve arşiv araştırması kapsamında yürütülen iş ve işlemlerde, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununun 4 üncü maddesinde belirtilen genel ilkelere aykırı hareket edilemez. Ancak millî savunma, millî güvenlik, kamu güvenliği, kamu düzeni ve ekonomik güvenlik ile ilgili istihbarat faaliyetleri kapsamında elde edilen bilgiler kişiye verilemez.

Kişisel veri güvenliği ve gizlilik

MADDE 9- (1) Bu Kanunda belirtilen güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimler ile değerlendirme komisyonları, veri güvenliğine ilişkin önlemleri alır.

(2) Güvenlik soruşturması ve arşiv araştırması işlemlerinin her evresinde gizliliğe uyulur. İlgili bilgi ve belgeler yasal olarak bilmesi gerekenlerden başkasına verilmez ve açıklanmaz.

(3) Bu Kanun kapsamında elde edilen kişisel veriler amacı dışında işlenemez ve aktarılamaz.

Kişisel verilerin silinmesi ve yok edilmesi

MADDE 10- (1) Güvenlik soruşturması ve arşiv araştırması sırasında elde edilen kişisel veriler, işleme amacının ortadan kalkması hâlinde veya her durumda iki yılın sonunda değerlendirme komisyonlarınca silinir ve yok edilir.

(2) Güvenlik soruşturması ve arşiv araştırmasını yapan birimlerdeki istihbari faaliyete konu olmayan ilgisine ait güvenlik soruşturması ve arşiv araştırmasına ait veriler iki yılın sonunda silinir ve yok edilir.

(3) Bu veriler, işleme karşı dava açılması hâlinde karar kesinleşmeden silinemez ve yok edilemez. Mahkemelerin bu konudaki talepleri, Değerlendirme Komisyonunun bünyesinde bulunduğu ilgili kurum ve kuruluş tarafından karşılanır.

DÖRDÜNCÜ BÖLÜM

Çeşitli Hükümler

Cezai hükümler

MADDE 11- (1) Güvenlik soruşturması ve arşiv araştırması yapılması ve değerlendirilmesinde görevli olanlar tarafından kişisel verilerle ilgili suç işlenmesi hâlinde, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde 6698 sayılı Kanunun 17 nci maddesi hükümleri uygulanır.

(2) Güvenlik soruşturması ve arşiv araştırması yapılması ve değerlendirilmesinde görevli olanlar tarafından kişisel verilerle ilgili kabahat işlenmesi hâlinde 6698 sayılı Kanunun 18 inci maddesi hükümleri uygulanır.

Yönetmelik

MADDE 12- (1) Devletin güvenliğini, ulusun varlığını ve bütünlüğünü iç ve dış menfaatlerinin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeler ile gizlilik dereceli kamu personeli ile meslek gruplarının tespiti, birim ve kısımların tanımlarının yapılması, güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak birimler ve değerlendirme komisyonlarının çalışma usul ve esasları ile uygulamaya ilişkin diğer hususlar Cumhurbaşkanınca yürürlüğe konulacak yönetmelik ile düzenlenir.

Değiştirilen ve yürürlükten kaldırılan hükümler

MADDE 13- (1) (24/2/1983 tarihli ve 2802 sayılı Hakimler ve Savcılar Kanunu ile ilgili olup yerine işlenmiştir.)

(2) (31/7/1970 tarihli ve 1325 sayılı Askeri Okullar, Askeri Öğrenciler, Askeri Fabrikalar ve Bazı Düzenlemeler Hakkında Kanun ile ilgili olup yerine işlenmiştir.)

(3) (9/6/1930 tarihli ve 1700 sayılı Dahiliye Memurları Kanunu ile ilgili olup yerine işlenmiştir.)

(4) (9/7/1982 tarihli ve 2692 sayılı Sahil Güvenlik Komutanlığı Kanunu ile ilgili olup yerine işlenmiştir.)

(5) (10/3/1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu ile ilgili olup yerine işlenmiştir.)

(6) (25/4/2001 tarihli ve 4652 sayılı Polis Yüksek Öğretim Kanunu ile ilgili olup yerine işlenmiştir.)

(7) (7/7/2010 tarihli ve 6004 sayılı Dışişleri Bakanlığı Personeline İlişkin Bazı Düzenlemeler Hakkında Kanun ile ilgili olup yerine işlenmiştir.)

(8) 26/10/1994 tarihli ve 4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun yürürlükten kaldırılmıştır.

Atıflar

MADDE 14- (1) Mevzuatta 4045 sayılı Kanuna yapılan atıflar bu Kanuna yapılmış sayılır.

Yürürlük

MADDE 15- (1) Bu Kanun yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 16- (1) Bu Kanun hükümlerini Cumhurbaşkanı yürütür.

**7252 sayılı Dijital Mecralar Komisyonu Kurulması ile Bazı Kanunlarda Değişiklik Yapılması
Hakkında Kanun**

Resmî Gazete Tarihi : 28.07.2020

Resmî Gazete Sayısı : 31199

**DİJİTAL MECRALAR KOMİSYONU KURULMASI İLE BAZI KANUNLARDA DEĞİŞİKLİK
YAPILMASI HAKKINDA KANUN**

Dijital Mecralar Komisyonu

MADDE 1 - (1) Kanunlara, bireylerin kişilik haklarına, özel hayatın gizliliğine ve diğer temel hak ve özgürlüklere aykırı yahut çocukların fiziksel ve psikolojik gelişimlerine zarar verici şekilde internet kullanımının önlenmesi amacıyla alınan tedbirler ile yapılan iş ve işlemler hakkında inceleme, görüşme, raporlama, tavsiye ve görüş bildirme işlemlerini yürütmek ve bu maddede belirtilen diğer görevleri yerine getirmek üzere, Türkiye Büyük Millet Meclisi bünyesinde Dijital Mecralar Komisyonu kurulmuştur.

(2) Komisyonun üye sayısı on yedidir. Üye dağılımı siyasi parti gruplarının parti grupları toplam sayısı içindeki yüzde oranlarına göre belirlenir. Komisyon, üye tamsayısının en az üçte biri ile toplanır ve toplantıya katılanların salt çoğunluğu ile karar verir.

(3) Komisyonun görevleri şunlardır:

a) Kendisine esas veya tali olarak havale edilen işleri görüşmek, Komisyon Başkanlığının talebi üzerine veya ihtisas komisyonlarınca talep edilmesi halinde; Türkiye Büyük Millet Meclisi Başkanlığına sunulan kanun teklifleri ile olağanüstü hal sırasında çıkarılan Cumhurbaşkanlığı kararnamelerini görev alanı yönünden inceleyerek görüş sunmak.

b) İnternet kullanımının kanunlara, bireylerin kişilik haklarına, özel hayatın gizliliğine ve diğer temel hak ve özgürlüklere aykırı yahut çocukların fiziksel ve psikolojik gelişimlerine zarar verici şekilde gerçekleşmesinin önlenmesi konularında görüş ve öneriler sunmak.

c) İnternet kullanımı yoluyla işlenen suçlarla etkin şekilde mücadele edilmesi konusunda görüş ve öneriler sunmak.

ç) (b) ve (c) bentlerinde belirtilen konularda uluslararası alanda kabul gören gelişmeleri izlemek, bu konular hakkında gerektiğinde yurt dışında incelemelerde bulunmak ve bu gelişmeler konusunda görüş ve öneriler sunmak.

d) İnternetin hukuka uygun kullanımı konusunda kamuoyunu bilgilendirici etkinlik ve projeler yapmak.

(4) Komisyonun yetkileri şunlardır:

a) Görevleri ile ilgili olarak kamu kurum ve kuruluşlarından, 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun kapsamında faaliyet gösteren içerik sağlayıcılar, erişim sağlayıcılar, yer sağlayıcılar ile yerli veya yabancı diğer gerçek ve tüzel kişilerden bilgi ve belge istemek ve ilgililerden bilgi almak.

b) Görev alanıyla ilgili faaliyet gösteren kamu kurum ve kuruluşları, üniversiteler, sivil toplum kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının çalışmalarından yararlanmak.

c) Gerekli gördüğünde uygun bulacağı uzmanları fikirlerini almak üzere çağırmak.

(5) Komisyon Ankara dışında da çalışabilir. Komisyon çalışmaları ile ilgili olarak, yurt içi ve yurt dışı görevlendirmelere ait giderler, Komisyon kararı ve Türkiye Büyük Millet Meclisi Başkanının onayı ile 10/2/1954 tarihli ve 6245 sayılı Harcırah Kanunu hükümlerine göre Türkiye Büyük Millet Meclisi bütçesinden karşılanır.

(6) Komisyonun çalışma usul ve esaslarına ilişkin olarak bu maddede hüküm bulunmayan hâllerde Türkiye Büyük Millet Meclisi İçtüzüğü hükümleri uygulanır.

(...)

MADDE 11 - (1) Bu Kanunun;

a) 4 üncü maddesi yayımı tarihini takip eden ayın başında,

b) 10 uncu maddesi 1/7/2020 tarihinden geçerli olmak üzere yayımı tarihinde,

c) Diğer maddeleri yayımı tarihinde,

yürürlüğe girer.

MADDE 12 - (1) Bu Kanunun;

a) 1 inci maddesini Türkiye Büyük Millet Meclisi Başkanı,

b) Diğer maddelerini Cumhurbaşkanı,

yürütür.

7223 sayılı Ürün Güvenliği ve Teknik Düzenlemeler Kanunu

Resmî Gazete Tarihi : 12.03.2020

Resmî Gazete Sayısı : 31066

ÜRÜN GÜVENLİĞİ VE TEKNİK DÜZENLEMELER KANUNU

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç

MADDE 1 - (1) Bu Kanunun amacı, ürünlerin güvenli ve ilgili teknik düzenlemelere uygun olmasını sağlamak; piyasa gözetimi ve denetiminin esasları ile yetkili kuruluşların görevlerini ve iktisadi işletmeciler ile uygunluk değerlendirme kuruluşlarının yükümlülüklerini belirlemektir.

Kapsam

MADDE 2 - (1) Bu Kanun, piyasaya arz edilmesi hedeflenen, arz edilen, piyasada bulundurulan veya hizmete sunulan tüm ürünleri kapsar.

(2) Avrupa Birliği üyesi ülkelere ihraç edilen veya ihraç edilmesi hedeflenen ürünler bu Kanun kapsamında piyasaya arz edilmiş sayılır.

(3) Bir ürüne ilişkin özel bir kanunun bulunması durumunda, bu Kanun hükümleri söz konusu ürüne, özel kanunda hüküm bulunmayan hallerde uygulanır.

(4) Avrupa Birliği üyesi ülkeler dışındaki ülkelere ihraç edilen veya ihraç edilmesi hedeflenen ürünler bu Kanunun kapsamı dışındadır. Ancak bu ürünlerin de güvenli olması, taşıma konusu olmaması ve ürüne ilişkin işaretleme, etiketleme ve belgelendirmenin alıcıyı yanıltmayacak şekilde yapılması zorunludur.

(...)

Gizlilik, ticari sırlar ve şeffaflık

MADDE 23 - (1) Yetkili kuruluş, bu Kanunu uygularken kişisel verilere dair, ticari sır niteliğindeki veya fikrî ve sınai mülkiyet hakkına ilişkin edindiği bilgilerin gizliliğini korumakla yükümlüdür.

Ancak, insan sađlıđı ve gvenliđinin gerektirdiđi hallerde bu bilgilerin aıklanması bu kapsamda sayılmaz.

(...)

**7091 sayılı Olağanüstü Hal Kapsamında Alınması Gereken Tedbirler Hakkında Kanun
Hükmünde Kararnamenin Kabul Edilmesine Dair Kanun**

Resmî Gazete Tarihi : 08.03.2018

Resmî Gazete Sayısı : 30354 (Mükerrer)

**OLAĞANÜSTÜ HAL KAPSAMINDA ALINMASI GEREKEN TEDBİRLER HAKKINDA
KANUN HÜKMÜNDE KARARNAMENİN KABUL EDİLMESİNE DAİR KANUN**

Amaç ve kapsam

MADDE 1- (1) Bu Kanun ile 20/7/2016 tarihli ve 2016/9064 sayılı Bakanlar Kurulu Kararıyla ülke genelinde ilan edilen olağanüstü hal kapsamında, darbe teşebbüsü ve terörle mücadele çerçevesinde gerekli bazı tedbirlerin alınması amaçlanmaktadır.

(...)

Kişisel verilerin paylaşımı

MADDE 3- (1) Olağanüstü halin devamı süresince; 22/7/2016 tarihli ve 667 sayılı Olağanüstü Hal Kapsamında Alınan Tedbirlere İlişkin Kanun Hükmünde Kararnamenin 3 üncü ve 4 üncü maddeleri uyarınca hakkında inceleme ve soruşturma yürütülen kişiler ile bunların eş ve çocuklarına ilişkin olarak yetkili kurul, komisyon ve diğer mercilerce ihtiyaç duyulan, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu uyarınca müşteri sırrı kapsamında kabul edilenler hariç, telekomünikasyon yoluyla iletişimin tespiti de dahil olmak üzere her türlü bilgi ve belge, kamu ve özel tüm kurum ve kuruluşlarca vakit geçirilmeksizin verilir.

(2) Kamu kurum ve kuruluşlarının personeline ve bunların eş ve çocuklarına ait olup Tasarruf Mevduatı Sigorta Fonuna devredilen ve faaliyet izni kaldırılan Asya Katılım Bankası A.Ş.'de veya bu Bankayla ilgili olarak Tasarruf Mevduatı Sigorta Fonunda, Bankacılık Düzenleme ve Denetleme Kurumunda ya da Malî Suçları Araştırma Kurulu Başkanlığında bulunan her türlü bilgi, bu personelin çalıştığı kurum ve kuruluşlarca talepte bulunulması durumunda gecikmeksizin verilir. Bu işlemlere ilişkin olarak 5411 sayılı Kanununun 73 üncü maddesinin birinci fıkrasında yer alan sınırlama uygulanmaz.

(...)

**7075 sayılı Olağanüstü Hal İşlemleri İnceleme Komisyonu Kurulması Hakkında Kanun
Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun**

Resmî Gazete Tarihi : 08.03.2018

Resmî Gazete Sayısı : 30354 (Mükerrer)

**OLAĞANÜSTÜ HAL İŞLEMLERİ İNCELEME KOMİSYONU KURULMASI HAKKINDA
KANUN HÜKMÜNDE KARARNAMENİN DEĞİŞTİRİLEREK KABUL EDİLMESİNE DAİR
KANUN**

Komisyonun Oluşumu

MADDE 1- (1) Anayasanın 120 nci maddesi kapsamında ilan edilen ve 21/7/2016 tarihli ve 1116 sayılı Türkiye Büyük Millet Meclisi Kararıyla onaylanan olağanüstü hal kapsamında, terör örgütlerine veya Milli Güvenlik Kurulunca Devletin milli güvenliğine karşı faaliyette bulunduğu karar verilen yapı, oluşum veya gruplara üyeliği, mensubiyeti, aidiyeti, iltisakı veya bunlarla irtibatı olduğu gerekçesiyle başka bir idari işlem tesis edilmeksizin doğrudan kanun hükmünde kararname hükümleri ile tesis edilen işlemlere ilişkin başvuruları değerlendirmek ve karara bağlamak üzere Olağanüstü Hal İşlemleri İnceleme Komisyonu kurulmuştur.

(2) Komisyon, yedi üyeden oluşur. Üyelerin üçü kamu görevlileri arasından Cumhurbaşkanı tarafından, bir üye Adalet Bakanlığının merkez teşkilatı ile bağlı ve ilgili kuruluşlarında çalışan hâkim ve savcılar arasından Adalet Bakanınca, bir üye mülki idare amirleri sınıfına mensup personel arasından İçişleri Bakanınca, birer üye Yargıtayda ve Danıştayda görev yapan tetkik hâkimleri arasından Hâkimler ve Savcılar Kurulu tarafından belirlenir. Komisyon, kendi üyeleri arasından yapacağı seçimle bir başkan ve bir başkanvekili seçer.

(3) Komisyonun toplantı ve karar yeter sayısı dördüttür. Oylamalarda çekimser oy kullanılamaz.

Gizlilik

MADDE 6- (1) Üyeler ve Komisyon çalışmalarında görevlendirilenler, görevlerini yerine getirmeleri sırasında edindikleri, kamuya, ilgililere ve üçüncü kişilere ait gizlilik taşıyan bilgileri, kişisel verileri, ticari sırları ve bunlara ait belgeleri, bu konuda kanunen yetkili kılınan mercilerden başkasına

açıklayamaz, kendilerinin veya üçüncü kişilerin yararına kullanamaz. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

(...)

İlave tedbirler için başvuru yolu

GEÇİCİ MADDE 4 - (Ek:11/11/2020-7256/41 md.)

(1) Bu Kanunun 2 nci maddesinde belirtilen işlemlere bağlı olarak olağanüstü hal kapsamında kabul edilen kanunlarda yer alan ilave tedbirlere karşı hakkında tedbir uygulanan kişi, kanuni temsilcisi ya da mirasçuları tarafından tedbiri uygulayan veya tedbirle ilgili olan kamu kurum ve kuruluşlarına bu maddenin yürürlüğe girdiği tarihten itibaren üç ay içinde başvurulur. Kamu kurum ve kuruluşları, başvuru üzerine yapacağı inceleme sonucuna göre en geç altı ay içinde başvurunun reddine veya tedbirin kaldırılmasına karar verir. 15/7/1950 tarihli ve 5682 sayılı Pasaport Kanununun ek 7 nci maddesi hükmü saklıdır.

(2) Başvuruların incelenmesi ve sonuçlandırılması için kamu kurum ve kuruluşları bünyesinde komisyon kurulabilir.

(3) Kamu kurum ve kuruluşları bu madde kapsamında yapılacak başvuruların sonuçlandırılması için her türlü bilgi ve belgeyi ilgililerden talep edebilir.

(4) Soruşturmanın gizliliğine ve Devlet sırlarına ilişkin ilgili mevzuat hükümleri saklı kalmak kaydıyla kurum ve kuruluşlar ile yargı mercileri, başvuru kapsamında ihtiyaç duyulan her türlü bilgi ve belgeyi gecikmeksizin başvuru yapılan kamu kurum ve kuruluşlarına göndermek veya yerinde incelenmesine imkân sağlamak zorundadır.

(5) Bu madde kapsamındaki çalışmalarda kamu kurum ve kuruluşlarınca görevlendirilenler, görevlerini yerine getirdikleri sırada edindikleri kamuya, ilgililere ve üçüncü kişilere ait gizlilik taşıyan bilgileri, kişisel verileri, ticari sırları ve bunlara ait belgeleri, bu konuda kanunen yetkili kılınan mercilerden başkasına açıklayamaz, kendilerinin veya üçüncü kişilerin yararına kullanamaz. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

(6) Bu madde ile olağanüstü hal kapsamında kabul edilen kanunlarda yer alan ilave tedbirlere karşı kamu kurum ve kuruluşlarına yapılan başvurular hakkında karar verenlerin görev ve fiillerine ilişkin hukuki, idari, mali ve cezai sorumlulukları hakkında 6755 sayılı Kanunun 37 nci maddesi uygulanır.

(7) Kamu kurum ve kuruluşlarının kararlarına karşı Hâkimler ve Savcılar Kurulunca belirlenecek Ankara idare mahkemelerinde iptal davası açılabilir.

(8) Bu madde uyarınca yetkili olmayan kamu kurum ve kuruluşuna yapılan başvurular yetkili olduğu değerlendirilen kamu kurum ve kuruluşuna gönderilir ve durum başvurana bildirilir.

(9) Bu maddenin uygulanmasına ilişkin ortaya çıkabilecek ihtilafları gidermeye Cumhurbaşkanlığı yetkilidir.

(...)

7068 sayılı Genel Kolluk Disiplin Hükümleri Hakkında Kanun Hükümünde Kararnamenin Kabul Edilmesine Dair Kanun

Resmî Gazete Tarihi : 08.03.2018

Resmî Gazete Sayısı : 30354 (Mükerrer)

**GENEL KOLLUK DİSİPLİN HÜKÜMLERİ HAKKINDA KANUN HÜKMÜNDE
KARARNAMENİN KABUL EDİLMESİNE DAİR KANUN**

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç

MADDE 1- (1) Bu Kanunun amacı; Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı personeline ilişkin disiplinsizlik ve cezaları, disiplin amirlerini ve kurullarını, disiplin soruşturma usulü ile diğer ilgili hususları düzenlemektir.

Kapsam

MADDE 2- (1) Bu Kanun;

a) Emniyet Genel Müdürlüğü teşkilatında çalışan her sınıftan memurları,

b) Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı teşkilatlarında görev yapan subay, astsubay, sözleşmeli subay, sözleşmeli astsubay, uzman jandarma, uzman erbaş, sözleşmeli erbaş ve sözleşmeli erler ile diğer sınıflardaki memurları,

kapsar.

(2) Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı emrine verilen yükümlü erbaş ve erler hakkında 31/1/2013 tarihli ve 6413 sayılı Türk Silahlı Kuvvetleri Disiplin Kanunu hükümleri uygulanır.

(...)

Disiplin cezası verilecek fiiller

MADDE 8- (1) Uyarma cezasını gerektiren fiiller şunlardır:

- a) Silahını, araç ve gerecini, giyim ve kuşamını temiz tutmamak, çalıştığı yerin temizliğine özen göstermemek.
- b) Yetkili makamlarca belirlenmiş tasarruf tedbirlerine riayet etmemek veya kullanımına sunulan kamu kaynaklarının kullanılmasında gösterilmesi gereken makul seviyedeki özeni göstermemek.
- c) İzinsiz veya kurumunca kabul edilebilir özrü olmaksızın belirli zamanda yapılması gereken faaliyetlere geç kalmak.
- ç) (Mülga:18/10/2018-7148/36 md.)
- d) Özürsüz veya izinsiz olarak mesaiye geç gelmek veya erken ayrılmak ya da günlük mesai saatlerine riayet etmemek.
- e) Nezaket kurallarına aykırı tavır ve davranışlarda bulunmak.
- f) Emrin icrası veya sonuçları ile katılım sağlanan toplantılarla ilgili olarak görevlendirme yapan amire bilgi vermemek.
- g) Usulüne uygun olarak kendisine verilmiş olan bir emir üzerine; emrin uygun olmadığı, yanlış verildiği, yapılamayacağı ve benzeri şekillerde amirini alenen eleştirmek veya amire karşı itirazda bulunmak (Amir tarafından karar verilene kadar astın fikrini savunması veya emrin kanunsuz olduğu hususundaki kanaatini belirtmek için amire yaptığı itiraz bu kapsamda disiplinsizlik teşkil etmez.).

(2) Kınama cezasını gerektiren fiiller şunlardır:

- a) Görev sırasında veya dışında, mevzuat veya talimatlarla yasaklanan davranışlarda bulunmak.
- b) Mevzuatta belirlenmiş usul ve kurallara riayet etmeden sözlü, yazılı veya elektronik olarak müracaat veya şikâyette bulunmak.
- c) Nöbeti teslimden sonra görev yerine özürsüz olarak geç dönmek.
- ç) Bildirimleri süresi içerisinde yerine ulaştırmamak.
- d) Mevzuat veya talimatlarla taşınmasına veya bulundurulmasına izin verilmiş olanlar dışında, mesleğin ciddiyeti ile bağdaşmayacak biçimde yüzük, bilezik, kolye, madalyon, rozet ve benzeri şeyleri takmak.
- e) Görev sırasında veya dışında kendisi ile aynı rütbede çalışanlara veya mesai arkadaşlarına karşı saygısız davranmak.

f) Mevzuat ve talimatlarla kendisine tevdi edilmiş görevlerin gerektirdiği sorumluluğu üstlenmekten imtina ettiğini gösterecek tavır ve davranışlarda bulunmak.

g) Amirleri, üstleri, aynı rütbedeki veya çalışma arkadaşları hakkında ve onların bulunmadığı ortamlarda, onların işlem, eylem ve kişilikleri hakkında kötüleyici veya konuştuğu kişilerde kötü intiba bırakacak tarzda olumsuz sözler söylemek.

ğ) Zati demirbaş tabanca veya geçici olarak verilen demirbaş tabancanın üzerinde orijinalliğini bozacak boya, kaplama, gravür veya ciddiyetle bağdaşmayacak şekil, desen, resim ve karakter gibi değişiklikler yapmak.

h) Mevzuata veya mesleki teamüllere aykırı hitaplarda bulunmak.

i) Bu fıkroda disiplinsizlik olarak saptanan eylem, işlem, tutum ve davranışlar dışında herhangi bir biçimde görevin takdir ve yerine getirilmesinde müsamaha ve savsaklama göstermek.

i) (Mülga:18/10/2018-7148/36 md.)

(3) Aylıktan kesme cezasını gerektiren fiiller şunlardır:

a) Üç günlüğe kadar aylıktan kesme cezasını gerektiren fiiller;

1) Mevzuat veya talimata aykırı olarak eksik kuşam ve teçhizatla göreve çıkmak.

2) Amir ve üstlerinin, görev ve mesleki konulara veya tutum ve davranışlarına ilişkin uyarılarına uymamak ya da bu uyarılara kayıtsız kalmak, amir ve üstleri tarafından sorulan soruları gereken süre içinde yanıtlamamak.

3) Özlük hakları ile ilgili veya başka bir kişisel menfaat temini için başkalarını aracı koyup öncelik ve ayrıcalık talep etmek.

4) İzinsiz veya kurumunca kabul edilebilir bir özrü olmaksızın yirmidört saate kadar göreve gelmemek.

5) Görev dışında amir veya üstlerine saygısız davranmak.

6) Nöbet görevine gelmemek veya nöbet ya da nokta görevinde mevzuatla ve/veya talimatlarla belirlenen kurallara aykırı hareket etmek.

7) Görevli bulunduğu sırada görev gereği olmaksızın veya amirin izni olmadan resmi kıyafet ile kahvehane, kiraathane, lokal, kulüp ve benzeri yerlerde oturmak.

8) Amirinden izin almaksızın görevli bulunduğu il sınırları dışına çıkmak.

9) Emrinde çalışanları veya Devletin araç ve gereçlerini idarece kabul edilebilir bir mazereti olmaksızın özel işlerinde kullanmak.

10) Kendisine verilmiş olan personel kimlik kartını kabul edilebilir bir neden olmaksızın kaybetmek.

11) Bazı isteklerini yerine getirmek, kişisel bir menfaat sağlamak, görev veya sorumluluktan kaçmak gibi amaçlarla hastalığını abartmak veya olmadığı halde bir rahatsızlığı varmış gibi göstererek günlük mesainin bir kısmına katılmamayı alışkanlık haline getirmek.

12) Herhangi bir yolu, yeri veya kişiyi arayıp soranlara cevap vermemek, baştan savmak.

13) Görevde kayıtsızlık göstermek, görevi savsaklamak veya geçerli bir özrü olmaksızın belirtilen sürede bitirmemek.

14) Haklı bir neden olmadan kişileri bekletmek.

15) Selamlama ile ilgili olarak belirlenmiş kurallara riayet etmemek.

16) Resmi protokol kurallarına aykırı tavır ve davranışlarda bulunmak.

17) (Ek:18/10/2018-7148/36 md.) Görevdeyken, yetkili makamlar tarafından izin verilen durumlar haricinde görev veya hizmetle ilgisi olmayan işlerle uğraşmak.

18) (Ek:18/10/2018-7148/36 md.) Kılık ve kıyafet ile ilgili olarak mevzuatta belirlenmiş kurallara uymamak.

b) Dört ila on günlüğe kadar aylıktan kesme cezasını gerektiren fiiller;

1) Kendisi ile aynı rütbede çalışanlara, astlarına veya mesai arkadaşlarına karşı onur kırıcı söz söylemek, davranışta bulunmak veya söz, yazı ya da eylemle hakaret etmek.

2) Resmi belge veya göreve ilişkin evrakı kaybetmek.

3) Önlem almamak veya tedbirli davranmamak yüzünden Devlet malı eşyanın hasar görmesine veya kaybolmasına neden olmak.(1)

4) İzinli olduğu zamanlarda resmi kıyafetle, izinli olmadığı zamanlarda görevli olmaksızın resmi veya sivil kıyafetle, personelin girmesine veya oturup eğlenmesine izin verilen yerler dışındaki kahvehane, lokal, kulüp veya benzeri yerlerde oyun oynamak.

5) İzinsiz veya kurumunca kabul edilebilir bir özrü olmaksızın yirmidört saatten fazla ve iki güne kadar (ikinci gün dahil) göreve gelmemek.

6) Mühür veya beratını kabul edilebilir bir neden olmaksızın kaybetmek.

7) Yüklümlü bulunduđu devir ve teslim işlemlerini tamamlamadan ya da devir ve teslim işleri tamamlanamadıđı takdirde ilgili mevzuatında belirtilen süre dolmadan görev yerinden ayrılmak.

8) Görevle ilgili resmi belge, araç ve gereçleri görevin sona ermesine ya da kurumca istenmesine rağmen geri vermemek.

9) İzin verilen haller dışında üniforma giymemek.

c) Onbir ila onbeş günlüğe kadar aylıktan kesme cezasını gerektiren fiiller;

1) İzensiz veya kurumunca kabul edilebilir bir özrü olmaksızın iki günden fazla ve üç güne kadar (üçüncü gün dahil) görevine gelmemek.

2) İzinli bulunduđu sürede, hizmet ve görevin gerektirdiđi durumlarda, görevine derhal dönmesi kendisine sözlü, yazılı ya da herhangi bir iletişim vasıtasıyla duyurulduđu halde, kabul edilebilir özrü bulunmaksızın görevine makul sürede dönmemek.

3) Amir ve üstlerine iletilmesi gereken olay, bilgi ve emirleri zamanında iletmemek.

4) Görev sırasında kişilere karşı onur kırıcı söz söylemek veya davranışta bulunmak.

5) Denetleme ve soruşturmaları uzatmak, denetleme raporları ve soruşturma raporlarını süresinde ilgili yerlere vermemek veya göndermemek ya da kabul edilebilir bir neden olmadan soruşturmayı eksik bırakmak.

(4) Kısa süreli durdurma cezasını gerektiren fiiller şunlardır:

a) Dört ay kısa süreli durdurma cezasını gerektiren fiiller;

1) Amir ve memurlara görevle ilgili olarak yalan söylemek.

2) Denetim görevini yerine getirmemek.

3) İzensiz ya da kurumunca kabul edilebilir özrü olmaksızın kesintisiz olarak üç günden fazla ve beş güne kadar (beşinci gün dahil) göreve gelmemek.

4) Amirlerini, üstlerini, aynı rütbedeki arkadaşlarını, astlarını veya diđer mesai arkadaşlarını haksız yere şikâyet etmek.

5) Astlarını, aynı rütbedeki arkadaşlarını ve diđer mesai arkadaşlarını dövme girişiminde bulunmak.

6) Toplu olarak sözlü veya yazılı şikâyette bulunmak.

7) Görev sırasında amir veya üstlerine saygısız davranmak.

8) Bu Kanunda ayrıca disiplinsizlik olarak tanımlanmamış olmak kaydıyla astları veya mesai arkadaşlarına yönelik olarak sürekli ve sistemli her türlü baskı ve taciz uygulamak.

b) Altı ay kısa süreli durdurma cezasını gerektiren fiiller;

1) Doğrudan veya aracı eliyle astlarından ya da iş sahiplerinden hediye veya borç almak.

2) Kabul edilebilir mücbir sebepler haricinde borçlanıp ödememeyi alışkanlık haline getirmek.

3) Görevde kullanılan telsiz haberleşme araçlarıyla görevle ilgili olmayan veya saygısızca konuşmalar yapmak ya da anlaşılmaz sesler çıkarmak.

4) Teslim aldığı her çeşit motorlu araç, makine, cihaz ve teçhizatta ağır kusur veya hizmetten ayrılabilen kişisel kusurla hasara sebep olmak.

5) Görev içinde veya dışında amir ya da üstlerinin eylem veya işlemlerini olumsuz yönde eleştirici nitelikte söz söylemek ya da yazı yazmak.

6) Hizmet dışında resmi sıfatının gerektirdiği saygınlığı ve güven duygusunu sarsacak eylem ve davranışlarda bulunmak.

7) Bir görevin kendisine tevdi edildiğini öğrendikten sonra mazeretler ileri sürmek suretiyle göreve başlamayı geciktirmek.

c) On ay kısa süreli durdurma cezasını gerektiren fiiller;

1) Amir ve üstlerine iletilmesi gereken olayları ve bunlarla ilgili bilgileri amirlerinden ve resmen istenmesi halinde görevli ve yetkili kuruluş ve kişilerden gizlemek.

2) Yetkili olmadığı halde basın, haber ajansları, radyo ve televizyon kurumları veya diğer iletişim kanalları vasıtasıyla kamuoyuna bilgi ya da demeç vermek.

3) Silahla dikkatsizlik, tedbirsizlik veya ihmal sonucu yaralamaya sebebiyet vermek, kendisini yaralamak ya da bu fiillerin başkaları tarafından işlenmesine neden olmak.(1)

4) Hizmet aracıyla ağır kusuru veya hizmetten ayrılabilen kişisel kusuruyla trafik kazası sonucu yaralamaya sebebiyet vermek.

5) (Ek:18/10/2018-7148/36 md.) Aynı rütbedeki meslektaşları ile diğer mesai arkadaşlarını tehdit etmek,

(5) Uzun süreli durdurma cezasını gerektiren fiiller şunlardır:

a) Oniki ay uzun süreli durdurma cezasını gerektiren fiiller;

1) Belirlenen durum ve sürelerde mal bildiriminde bulunmamak veya gerçeğe aykırı bildirimde bulunmak.

2) Görev sırasında kişilere veya herhangi bir nedenle kurum binalarına gelen ya da getirilenlere hakaret etmek.

b) Onaltı ay uzun süreli durdurma cezasını gerektiren fiiller;

1) Devlet malı motorlu araçları, muhabere araçlarını, silah veya mühimmatı ihmal nedeniyle kaybetmek.

2) Hizmet içinde resmi sıfatının gerektirdiği saygınlığı ve güven duygusunu sarsacak eylem ve davranışlarda bulunmak.

3) (Değişik:18/10/2018-7148/36 md.) Görev sırasında herhangi bir şekilde uyumak veya uyuklamak.

c) Yirmi ay uzun süreli durdurma cezasını gerektiren fiiller;

1) İzinsiz veya kurumca kabul edilebilir özrü olmaksızın kesintisiz olarak beş günden fazla ve dokuz güne kadar (dokuzuncu gün dahil) görevine gelmemek.

2) Muhafazası veya sevkiyle yükümlü bulunduğu şüpheli, sanık, tutuklu veya hükümlünün uyanık davranmamak ya da önlem almamak yüzünden kaçmasına neden olmak ya da yakalama görevini savsaklamak.

3) (Ek:18/10/2018-7148/36 md.) Kanunun verdiği yetkiye dayalı olmaksızın spor müsabakalarına dayalı sabit ihtimalli veya müşterek bahis veya şans oyunlarını oynamak.

ç) Yirmidört ay uzun süreli durdurma cezasını gerektiren fiiller;

1) Silahla dikkatsizlik, tedbirsizlik veya ihmal sonucu ölüme sebebiyet vermek ya da bu fiilin başkaları tarafından işlenmesine neden olmak.

2) Silahla yaralama suçunu kasten işlemek.(2)

3) Meskûn yerlerde, binalarda, herkesin dolaşp gezebileceği veya oturabileceği yerlerde silah atmak.

4) Amirin usulüne göre verdiği emri yerine getirmemek.

5) Amirin izni olmaksızın görev yerini terk etmek.

6) Kişinin iffetine yönelik söz söylemek, fiil veya harekette bulunmak.

7) Amir veya üste hakaret etmek.

8) Amir veya üstlerini söz, yazı, tutum veya davranışlarıyla küçümsemek.

9) Amir veya üstlerini dövmeye teşebbüs etmek.

10) Amir veya üstlerini sözlü veya fiili olarak tehdit etmek.

11) Göreve ilişkin her türlü yazılı kağıt, belge, mikrofilm aslı veya kopyalarını kasıtlı olarak yok etmek, ortadan kaldırmak ya da belge niteliği taşıyan bilgisayar programlarını, dosyalarını, verilerini hukuka aykırı olarak ele geçirmek, başkasına zarar vermek üzere kullanmak, tahrip etmek, değiştirmek, silmek, sistemin işlemesine engel olmak ya da yanlış biçimde işlemesini sağlamak.

12) Kriptolu telsiz cihazının ve her türlü kriptolu cihazın kaybını veya çalındığını, idarece kabul edilebilir bir mazereti olmaksızın ilgili birime derhal bildirmemek.

13) Hizmet aracıyla ağır kusuru veya hizmetten ayrılabilen kişisel kusuruyla trafik kazası sonucu ölüme sebebiyet vermek.

(6) Meslekten çıkarma cezasını gerektiren fiiller şunlardır:

a) Görevin yerine getirilmesinde dil, ırk, cinsiyet, siyasi düşünce, felsefi inanç, din ve mezhep ayrımı yapmak veya personel arasında bu yolda ayırım yapıcı tutum ve davranışlarda bulunmak.

b) Göreve çıkılmaması için propaganda yapmak, kışkırtmak, zorlamak, karar alınmasını sağlamak, alınan bu karara katılmak veya karar uyarınca göreve çıkmamak.

c) Amir ya da üstlerinin icraatına karşı çıkmak ve bu hareketi toplu hale dönüştürerek görev yapılmasını ya da göreve çıkılmasını engellemek, buna katılmak, katılmaya tahrik ya da teşvik etmek.

ç) Yetkisini veya nüfuzunu kendisine veya başkalarına çıkar sağlamak amacıyla ya da kin ve dostluk gibi nedenlerle kötüye kullanmak.

d) Hizmetle ilgili her türlü dosya, kayıt, resmi evrak veya belgeyi ya da örneklerini yetkisiz kişilere vermek, verilmesini emretmek, verilmesine göz yummak.

e) Gizli tutulması zorunlu olan ve görev ile ilgili bulunan bilgi ve belgeleri görevli veya yetkili olmayan kişilere açıklamak.

f) Muhafazası veya sevkiyle görevli olduğu şüpheli, sanık, tutuklu veya hükümlünün kaçmasına bilerek ve isteyerek imkân vermek.

g) Bilerek ve isteyerek suç kanıtlarını yok etmek veya bunların yok olmasına neden olmak, kanıtları silmek, gizlemek, değiştirmek, bozmak veya bu fiillere yardımcı olmak.

ğ) Devlet malı araç, gereç, hayvan, silah, mermi ve mühimmatı satmak veya mal edinmek, personel kimlik kartını, araç, gereç, hayvan, silah ve mühimmatı başkalarının kullanımına vermek.

- h) Kasıtlı olarak gerçek dışı rapor vermek veya tutanak düzenleyip imza etmek veya ettirmek.
- ı) Görev sırasında yardım isteyen güvenlik görevlilerine haklı bir neden yokken yardımdan kaçınmak veya bildiği ya da gördüğü bir suçun izlenmesi ve suçlunun yakalanması için gerekli girişimde bulunmamak.
- i) Mesleğin saygınlığını zedeleyecek şekilde uygunsuz yerlere gitmek.
- j) Görev mahallinde veya görevli bulunduğu sırada alkollü içki içmek veya içilmesine göz yummak.
- k) Göreve sarhoş veya alkollü içki içtiği belli olacak biçimde gelmek.
- l) Resmi kıyafetle umuma açık yerlerde alkollü içki içmek veya resmi kıyafetli olarak gizlenemeyecek derecede sarhoş görünmek.
- m) Uyuşturucu maddeleri yapmak veya kullanmak, bunların yapılmasına, kullanılmasına, saklanmasına, nakledilmesine, yakalanacağı sırada ortadan kaldırılmasına, satılmasına veya satın alınmasına aracı olmak, kullanılmasını kolaylaştırmak ya da özendirmek.
- n) Kumar oynamak veya oynatmak, kumar oynatanlarla ilişki kurmak.
- o) Kaçakçılık yapmak veya kaçakçılarla ilişki kurmak.
- ö) Geliri ile uygun sayılmayacak biçimde yaşadığı ve aşırı harcamada bulunduğu kanıtlanmış olmak ve bunun haklı kaynağını gösterememek.
- p) 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu ile öngörülen grev yasağı kapsamına giren eylemlerde bulunmak.
- r) Devlet memurları tarafından yapılamayacağı 657 sayılı Kanunda belirtilen kazanç getirici faaliyetlerde bulunmak.
- s) Siyasi partilerin yararına veya zararına çalışmak ya da siyasal eylemlerde bulunmak, görevli olmaksızın siyasal amaçla yapılacak açık veya kapalı yer toplantılarına ya da gösteri yürüyüşlerine katılmak.
- ş) İffetsizliği bilinen veya anlaşılmış olan bir kimse ile bilerek evlenmek ya da evlilik bağına devam ettirmek veya böyle bir kimseyi yanında bulundurmamak ya da nikahsız olarak devamlı surette yaşamakta ısrar etmek.
- t) Kanuna aykırı olarak sendikalara üye olmak, sendikaların veya üyesi bulunmadıkları derneklerin yapacakları bilimsel, kültürel ve teknik nitelik taşımayan açık veya kapalı yer toplantılarına ya da gösteri yürüyüşlerine görevli olmaksızın katılmak, açık yer toplantı ve gösteri yürüyüşlerine resmi

kıyafetli veya silahlı olarak katılmak ya da üyesi buldukları derneklerin tüzüklerinde belirtilen amaçları dışındaki çalışmalarını veya bu nitelikteki toplantı ya da gösteri yürüyüşlerini düzenlemek veya bunlara katılmak.

u) Görevde kullanılan telsiz, telefon haberleşmesini veya kurum içi iletişim sistemlerini kasıtlı olarak engellemek.

ü) Mesleğin onur ve saygınlığını zedeleyici veya amir ya da üstlerinin eylem ve işlemlerini olumsuz yönde eleştirici nitelikte tek başına veya topluca bildiri dağıtmak ya da basın, haber ajansları, radyo ve televizyon kurumları ve diğer iletişim kanalları vasıtasıyla kamuoyuna yönelik bilgi, yazı ve demeç vermek.

v) Amir ya da üste karşı itaatsizliğe, mukavemete ya da fiilen taarruza tahrik ya da teşvik etmek.

y) Menşei belli olmayan, bulundurulması ve taşınması yasak olan her çeşit silah, mühimmat ve benzerlerini bulundurmak.

z) Hukuka aykırı olarak kişiler arasındaki haberleşmenin gizliliğini ihlal etmek, kişiler arasındaki haberleşme içeriklerini ifşa etmek, kişiler arasındaki aleni olmayan konuşmaları taraflardan herhangi birinin rızası olmaksızın kaydetmek, kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri ifşa etmek, kişilerin özel hayatının gizliliğini ihlal etmek, kişilerin özel hayatına ilişkin görüntü veya sesleri ifşa etmek, kişisel verileri kaydetmek, kişisel verileri bir başkasına vermek, yaymak veya ele geçirmek, kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olduğu halde bu görevini kasıtlı olarak yerine getirmemek, gerçeğin meydana çıkmasını engellemek amacıyla suç delillerini yok etmek, silmek, gizlemek, değiştirmek veya bozmak, sayılan fiilleri emir vererek yaptırmak.

aa) Yetkili olmadığı halde hukuka aykırı olarak elektronik ortamda veya bilgisayar loglarında kişisel verilerle ilgili sorgulama yapmak, bu şekilde elde edilen bilgileri paylaşmak veya yayın yoluyla duyurmak, log kayıtlarını değiştirmek veya silmek.

bb) Görevi gereği öğrendiği veya edindiği kişisel bilgi veya belgeleri yetkisiz kişilerle paylaşmak ya da basın ve yayın kuruluşlarına veya diğer iletişim kanallarına vermek.

cc) Bir kimseyle gayri tabii mukarenette bulunmak yahut bu fiili kendisine rızasıyla yaptırmak.

çç) Görevine, sosyal ve aile yaşantısına zarar verecek derecede menfaatine, içkiye, kumara ve benzeri kötü alışkanlıklara düşkün olmak.

dd) Üstlerine, aynı rütbedeki meslektaşları ile diğer mesai arkadaşlarına fiili tecavüzde bulunmak.

ee) Görevde kullanılan telsiz haberleşme araçlarıyla amir ya da üstleri hakkında olumsuz yönde eleştirici nitelikte konuşmalar yapmak.

ff) Dernek kurmak ya da spor dernekleri dışındaki derneklere üye olmak.

gg) Vakıf kurmak veya Bakanlıkça belirlenmiş vakıflardan başka vakıfların organlarında görev almak.

hh) (Ek:18/10/2018-7148/36 md.) Fuhşa teşvik eden, bunun yolunu kolaylaştıran ya da fuhuş için aracılık eden veya yer temin eden kişilerle bilerek ilişki kurmak.

(7) (Değişik:17/1/2019-7161/64 md.) Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığında, terfileri 27/7/1967 tarihli ve 926 sayılı Türk Silâhlı Kuvvetleri Personel Kanunu, 28/5/1988 tarihli ve 3466 sayılı Uzman Jandarma Kanunu, 18/3/1986 tarihli ve 3269 sayılı Uzman Erbaş Kanunu ve 10/3/2011 tarihli ve 6191 sayılı Sözleşmeli Erbaş ve Er Kanunu hükümlerine tabi olan personelin;

a) Kısa süreli durdurma cezası verilmesini gerektiren hallerde brüt aylıklarının 1/5'i ila 1/4'ü,

b) Uzun süreli durdurma cezası verilmesini gerektiren hallerde brüt aylıklarının 1/3'ü ila 1/2'si,

kesilir.

(8) Yedinci fıkrada yer alan cezalar yetkili disiplin kurullarınca verilir.

(...)

6713 sayılı Kolluk Gözetim Komisyonu Kurulması Hakkında Kanun

Resmî Gazete Tarihi : 20.05.2016

Resmî Gazete Sayısı : 29717

KOLLUK GÖZETİM KOMİSYONU KURULMASI HAKKINDA KANUN

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç ve kapsam

MADDE 1- (1) Bu Kanunun amacı; kolluk şikâyet sisteminin daha etkili ve hızlı işlemlerini sağlamak, saydamlığını ve güvenilirliğini geliştirmek üzere, kolluk görevlilerinin işledikleri iddia edilen suçlardan veya disiplin cezasını gerektiren eylem, tutum veya davranışlarından dolayı idarî merciler tarafından yapılan ya da yapılması gereken iş ve işlemlerin merkezî bir sistemde kayıt altına alınması ve izlenmesi amacıyla Kolluk Gözetim Komisyonunun kurulması, Komisyonun görevleri, yetkileri ve çalışma yöntemi ile kolluk şikâyet sistemine yönelik diğer idarî tedbirlere ilişkin usul ve esasları belirlemektir.

(2) Bu Kanun; Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı teşkilâtında görevli kolluk personelinin işlediği iddia edilen suçlarla veya disiplin cezasını gerektiren eylem, tutum veya davranışlarıyla ilgili olarak idarî merciler tarafından yapılan ya da yapılması gereken iş ve işlemleri kapsar.

(3) Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı teşkilâtında görevli kolluk personelinin askerî görevlerinden doğan suçları, bu Kanunun kapsamı dışındadır.

(4) Bu Kanunun uygulanmasında;

a) 25/10/1963 tarihli ve 353 sayılı Askerî Mahkemeler Kuruluşu ve Yargılama Usulü Kanunu,

b) 16/6/1964 tarihli ve 477 sayılı Disiplin Mahkemeleri Kuruluşu, Yargılama Usulü ve Disiplin Suç ve Cezaları Hakkında Kanun,

hükümleri saklıdır.

Tanımlar

MADDE 2- (1) Bu Kanunun uygulanmasında;

a) Bağlı kuruluşlar: Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığını,

b) Bakan: İçişleri Bakanını,

c) Bakanlık: İçişleri Bakanlığını,

ç) Başkan: Kolluk Gözetim Komisyonu Başkanını,

d) İhbar: Kolluk görevlilerinin hukuka aykırı eylem, tutum veya davranışlarının, herhangi bir kişi tarafından yetkili mercilere bildirilmesini,

e) Kolluk: Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı teşkilâtında, emniyet ve asayiş ile kamu düzeninin korunmasını sağlamak için kanunların ve kanunlara dayanarak yetkili makamların verdiği görevleri yerine getiren görevlileri,

f) Kolluk şikâyet sistemi: Kolluk görevlilerinin işledikleri iddia edilen suçlardan veya disiplin cezasını gerektiren eylem, tutum veya davranışlarından dolayı idarî merciler tarafından yapılan iş ve işlemler ile uygulamaların bütünü,

g) Komisyon: Kolluk Gözetim Komisyonunu,

ğ) Kurul: İçişleri Bakanlığı Mülkiye Teftiş Kurulunu,

h) Kurul Başkanı: İçişleri Bakanlığı Mülkiye Teftiş Kurulu Başkanını,

ı) Merkezî kayıt sistemi: Kolluk Gözetim Komisyonu ile bağlı kuruluşlar, valilikler ve kaymakamlıklar arasında, kolluk görevlileri hakkında idarî mercilerce yürütülen ceza ve disiplin işlemleriyle ilgili olarak gerekli bilgilerin kaydedilmesi ve yapılan uygulamaların izlenmesi amacıyla oluşturulan veri tabanını,

i) Müsteşar: İçişleri Bakanlığı Müsteşarını,

j) Şikâyet: Kolluk görevlilerinin hukuka aykırı eylem, tutum veya davranışlarının, bunlardan zarar gören veya mağdur olanlar ya da bunların kanunî temsilcileri veya ikinci derece dâhil, ikinci dereceye kadar kan ve kayın hısımları tarafından, yetkili mercilere bildirilmesini,

ifade eder.

İKİNCİ BÖLÜM

Kuruluş, Görev ve Yetkiler

Kuruluş

MADDE 3- (1) Bu Kanunla verilen görevleri, kendi yetki ve sorumluluğu altında bağımsız olarak yerine getirmek üzere Kolluk Gözetim Komisyonu kurulmuştur. Komisyon, İçişleri Bakanlığı bünyesinde sürekli kurul olarak görev yapar.

(2) Komisyon; Müsteşarın başkanlığında, Türkiye İnsan Hakları ve Eşitlik Kurumu Başkanı, Kurul Başkanı, Bakanlık I. Hukuk Müşaviri, Adalet Bakanlığı Ceza İşleri Genel Müdürü, üniversitelerin ceza ve ceza usul hukuku ana bilim dallarında görevli öğretim üyeleri (...) (1) ile baro başkanı seçilme yeterliğine sahip serbest avukatlar arasından Cumhurbaşkanınca seçilecek birer üyeden oluşur.[1]

(3) Öğretim üyeleri ile serbest avukatlar arasından seçilecek üyelerin, seçilmelerinden önceki son beş yıl içinde herhangi bir siyasî partiyle üyelik veya başka türde bir görev ilişkilerinin bulunmaması şarttır.

(4) Komisyon üyeliklerine öğretim üyeleri ile serbest avukatlar arasından seçilecek üyelerin görev süresi dört yıldır. Süresi dolan üyeler, aynı usulle yeniden seçilebilir. Bu üyeler, üyelikleri süresince Komisyondaki görevlerinden alınamazlar. Ancak, üyeler, ciddi bir hastalık veya sakatlık nedeniyle iş göremez hâle gelmeleri veya görevlendirmeye ilişkin şartları kaybetmeleri ya da seçilmeleri sırasında bu şartları taşımadıklarının daha sonra tespit edilmesi hâlinde, görevlendirildikleri usule göre süreleri dolmadan görevlerinden alınır. Bu üyelerin Komisyondaki görevlerinden doğan suçlarından dolayı, özel kanunlarındaki hükümler uygulanır. Komisyonun bu üyeleri mazeretsiz olarak arka arkaya üç toplantıya veya bir yıl içinde toplam dört toplantıya katılmadıkları takdirde, Komisyon kararıyla üyelikleri sona erer. Bu fıkrada belirtilen nedenlerle veya başka herhangi bir nedenle boşalan üyelikler için ilgisine göre ikinci fıkrada belirtilen usule göre en geç bir ay içinde yeni görevlendirme yapılır. Bu şekilde görevlendirilen üyeler, yerine görevlendirildikleri üyenin görev süresini tamamlar.

(5) Komisyon, bu Kanunla verilen görev ve yetkileri, kendi sorumluluğu altında bağımsız olarak yerine getirir. Hiçbir organ, makam, merci veya kişi Komisyonun kararlarını etkilemek amacıyla emir ve talimat veremez, tavsiye veya telkinde bulunamaz.

Görev ve yetkiler

MADDE 4- (1) Komisyonun görev ve yetkileri aşağıda belirtilmiştir:

a) Kolluk şikâyet sisteminin işleyişine dair ilkeleri tespit ederek bunlarla ilgili olarak Bakanlığa önerilerde bulunmak, bu konudaki uygulamaları izlemek ve sistemin işleyişinde kamu kurum ve kuruluşları arasında koordinasyonu sağlamak.

- b) Kolluk görevlilerinin işledikleri iddia edilen suçlardan veya disiplin cezasını gerektiren eylem, tutum veya davranışlarından dolayı gerektiğinde yetkili merciler tarafından haklarında disiplin soruşturması yapılmasını istemek.
- c) Kolluk şikâyet sisteminin işleyişiyle ilgili konularda teftiş ve denetim yapılması için Bakanlığa önerilerde bulunmak, bu teftiş ve denetimler sonucunda düzenlenen raporları değerlendirmek, tespit edilen eksiklikler konusunda alınması gereken idarî tedbirleri belirleyerek Bakanlığa önermek ve bu raporlardan uygun gördüklerini kamuoyuna açıklamak.
- ç) Merkezî kayıt sisteminin etkili bir şekilde işlemesi ve geliştirilmesi için Bakanlığa önerilerde bulunmak ve bu sistemin işleyişini izlemek.
- d) Merkezî kayıt sisteminden elde edilecek veri ve bilgilere ilişkin istatistikler hazırlamak, veri tabanı oluşturmak, elde edilen veri ve bilgilerin analizini yapmak veya yaptırmak, strateji belirlenmesine ve uygulamaya ilişkin önerilerde bulunmak ve gerekli görülen hâllerde bu analizlerin sonuçlarını kamuoyuna duyurmak.
- e) Görev alanına giren konularda tespit, görüş ve öneriler içeren yıllık raporlar hazırlamak ve bu raporları her yıl mart ayında Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonu ile Cumhurbaşkanlığına göndermek ve kamuoyuna açıklamak.[2]
- f) Kolluk görevlilerinin çalışma koşullarının iyileştirilmesine yönelik araştırmalar yapmak veya yaptırmak, kolluk hizmetlerinin geliştirilmesi ve iyileştirilmesine yönelik olarak yapılan çalışmalarını izlemek, değerlendirmek ve bu konularda Bakanlığa önerilerde bulunmak.
- g) Kolluk etik ilkelerinin uygulanmasını izlemek; bu ilkelerin etkin bir şekilde uygulanması konusunda yetkili makamlara önerilerde bulunmak ve bu konuda kolluk teşkilâtı ve diğer ilgili kuruluşlarla iş birliği yapmak.
- ğ) Kolluk şikâyet sistemine kamuoyunun duyduğu güveni ölçmek ve halkın sisteme ilişkin görüş ve düşüncelerini değerlendirmek amacıyla en az iki yılda bir olmak üzere kamuoyu araştırmaları yapmak veya yaptırmak.
- h) Görev alanına giren konularda üniversiteler, kamu kurumu niteliğindeki meslek kuruluşları ve ilgili sivil toplum kuruluşları ile iletişim kurmak ve iş birliği yapmak.
- ı) Kolluğun hizmet içi eğitim programlarıyla ilgili olarak yetkili birimlere görüş bildirmek ve önerilerde bulunmak.
- i) Görev alanına giren konularla ilgili mevzuat düzenlemeleri hakkında görüş bildirmek.

(2) Kolluk görevlilerinin disiplin cezasını gerektiren eylem, tutum veya davranışlarıyla ilgili ihbar ve şikâyetlerin Komisyona intikal etmesi veya Komisyon tarafından resen öğrenilmesi üzerine Komisyon, Kurul Başkanlığından söz konusu ihbar veya şikâyetlerin öğrenildiği tarihten itibaren otuz gün içinde disiplin soruşturması açılmasını isteyebilir. Bu istem üzerine Kurul Başkanlığınca genel disiplin hükümlerine göre işlem yapılır.

(3) Daha önce disiplin amirlerince disiplin soruşturması yapılmasına gerek görülmemiş olan ihbar veya şikâyetler hakkında da ikinci fıkra hükümleri uygulanır.

(4) Birinci fıkranın (d) ve (e) bentleri uyarınca kamuoyuna yapılacak açıklamalarda, 9/10/2003 tarihli ve 4982 sayılı Bilgi Edinme Hakkı Kanununda yer alan sınırlamalar dikkate alınır.

Çalışma usul ve esasları

MADDE 5- (1) Komisyon, en az ayda bir defa olmak üzere, gerekli hâllerde toplanır. Toplantıları Başkan yönetir. Komisyon, Başkanın isteğiyle veya Başkan dışında en az üç üyenin birlikte talep etmesi hâlinde, Başkan tarafından olağanüstü toplantıya çağrılır. Başkanın izin, hastalık veya başka bir nedenle görevde bulunmadığı hâllerde Kurul Başkanı, Başkana vekâlet eder.

(2) Komisyon, en az beş üyenin hazır bulunması ile toplanır ve en az dört üyenin aynı yöndeki oyuyla karar alır. Kararlarda çekimser oy kullanılamaz.

(3) Toplantı gündemi Başkan tarafından belirlenerek toplantıdan en az üç gün önce üyelere bildirilir. Gündeme yeni madde eklenebilmesi için toplantıda üyelere birinin öneride bulunması ve önerilen maddenin Komisyon tarafından kabul edilmesi gerekir.

(4) İhtiyaç duyulması hâlinde, gündemdeki konularla ilgili olarak görüşlerinden yararlanılmak üzere kamu görevlileri, özel kuruluşların temsilcileri veya uzmanlar, Başkan tarafından Komisyon toplantılarına davet edilebilir. Ancak, Komisyon kararları, toplantıya dışarıdan katılanların yanında alınmaz.

(5) Komisyon kararları tutanakla tespit edilir ve karar tutanağı, toplantı esnasında veya en geç toplantıyı izleyen beş iş günü içinde, toplantıya katılan tüm üyeler tarafından imzalanır.

(6) Başkan ve üyeler; kendileri, eşleri, evlatlıkları ve üçüncü derece dâhil, üçüncü dereceye kadar kan ve ikinci derece dâhil, ikinci dereceye kadar kayın hısımlarıyla ilgili veya kişisel menfaat ilişkisi içinde oldukları konularda müzakere ve oylamaya katılamaz. Bu durum karar metninde ayrıca belirtilir.

(7) Aksi kararlaştırılmadıkça, Komisyon toplantılarındaki müzakereler gizlidir.

(8) Komisyon, gerekli gördüğü durumlarda kararlarını uygun vasıtalarla kamuoyuna duyurabilir. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu hükümleri saklıdır.

(9) Bakanlıklar ve diğer kamu kurum ve kuruluşları, kanunlardaki özel hükümler saklı kalmak kaydıyla, Komisyonun istediği bilgi ve belgeleri talebi hâlinde Komisyona vermek zorundadır.

(10) Komisyonun faaliyetleri ve diğer ihtiyaçları ile yolluk giderleri için, her yıl İçişleri Bakanlığı bütçesine gerekli ödenek konulur.

(11) Başkan ve üyeler ile bu Kanunla verilen görevleri yürüten personel, görevlerini yerine getirmeleri sırasında edindikleri gizli bilgileri, kişisel verileri, ticarî sırları ve bunlara ilişkin belgeleri, kanunlarla yetkili kılınan mercilerden başkasına açıklayamazlar ve kendilerinin veya üçüncü kişilerin yararına kullanamazlar. Bu yükümlülük, görevden ayrılmalarından sonra da devam eder.

ÜÇÜNCÜ BÖLÜM

Sekretarya, Kayıt İşleri ve Diğer İdarî İşlemler

Sekretarya

MADDE 6- (1) Komisyonun sekretarya hizmetleri, Kurul Başkanlığı tarafından yerine getirilir. Komisyonun sekretarya hizmetlerinin etkili şekilde yürütülmesini temin etmek üzere, Kurul bünyesinde şube müdürlükleri oluşturulur. Bu hizmetlerin sevk ve idaresinde Kurul Başkanına yardımcı olmak üzere, en az beş yıllık meslekî kıdeme sahip bir mülkiye başmüfettişi, Kurul Başkanının önerisi ve Başkanın teklifi üzerine Bakan onayı ile görevlendirilir.

(2) Sekretarya hizmetlerinin yürütülmesine ilişkin usul ve esaslar, Cumhurbaşkanınca yürürlüğe konulacak yönetmelikle düzenlenir.

Merkezî kayıt sistemi

MADDE 7- (1) Komisyon ile bağlı kuruluşlar, valilikler ve kaymakamlıklar arasında, kolluk görevlileri hakkında idarî mercilerce yürütülen ceza ve disiplin işlemleriyle ilgili olarak, dördüncü fıkrada belirtilen bilgilerin kaydedilmesi ve yapılan uygulamaların izlenmesi amacıyla, Bakanlıkça merkezî kayıt sistemi kurulur. Kolluk görevlileri hakkında Komisyona ve/veya diğer idarî mercilere yapılan her türlü ihbar ve şikâyet, merkezî kayıt sisteminden bir numara verilerek kayıt altına alınır ve bu numara ihbar veya şikâyette bulunan kişilere tebliğ edilir. İdarî merciler tarafından resen tespit edilen ve işlem yapılmasını gerektiren fiil ve hâller için de merkezî kayıt sisteminden bir numara verilir.

(2) İhbar ve şikâyetlerin soyut ve genel nitelikte olmaması, ilgili olduğu kişi veya olayların belirtilmesi, iddiaların ciddî bulgu ve belgelere dayanması, dilekçe sahibinin adı, soyadı ve imzası ile iş veya yerleşim yeri adresinin ve Türkiye Cumhuriyeti kimlik numarasının doğru olarak bildirilmesi zorunludur. Bu şartları taşımadığı, doğrudan veya yapılan araştırma sonucunda anlaşılan ihbar ve şikâyetlerle ilgili olarak, soruşturma izni vermeye yetkili mercilerce veya disiplin amirlerince, 2/12/1999 tarihli ve 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun ya da disiplin mevzuatına göre işlem yapılmaz ve bu durum ihbar veya şikâyette bulunan kişilere bildirilir. Ancak iddiaların sıhhatinin şüpheye mahal vermeyecek belgelerle ortaya konulmuş olması hâlinde adı, soyadı, imzası ile iş veya yerleşim yeri adresinin ve Türkiye Cumhuriyeti kimlik numarasının doğruluğu şartı aranmaz; işleme konulmayan ihbar ve şikâyetlerle ilgili bilgiler de merkezî kayıt sistemine işlenir. İhbar veya şikâyette bulunan kişilerin kimlik bilgileri gizli tutulur.

(3) Merkezî kayıt sistemine işlenen veriler, 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu uygulamasında kişisel veri sayılır.

(4) Merkezî kayıt sistemine, ihbar veya şikâyete konu olayın özeti ve yapılan işlemlerin yanı sıra, mevcut ise dilekçe sahibinin adı ve soyadı ile iş veya yerleşim yeri adres bilgileri ve Türkiye Cumhuriyeti kimlik numarası işlenir. Bu bilgilere ilaveten, ihbarcı veya şikâyetçinin isteğine bağlı olarak merkezî kayıt sistemine işlenecek kişisel bilgiler ile bu sistemin işleyişine ilişkin usul ve esaslar, Cumhurbaşkanınca yürürlüğe konulacak yönetmelikle düzenlenir.[4]

Ön inceleme ve disiplin soruşturması işlemleri

MADDE 8- (1) Ön inceleme ve disiplin soruşturması işlemleri aşağıdaki usule göre yürütülür:

a) Kolluk görevlilerinin suç işledikleri yönünde 7 nci maddenin ikinci fıkrasındaki şartlara uygun herhangi bir ihbar veya şikâyet alındığında ya da böyle bir durum doğrudan öğrenildiğinde, soruşturma izni vermeye yetkili mercilerce ve/veya disiplin amirlerince 4483 sayılı Kanun ve/veya kolluk görevlilerinin tâbi oldukları disiplin mevzuatı uyarınca gerekli işlemler yerine getirilir.

b) Kolluk görevlilerince işlendiği iddia edilen veya doğrudan öğrenilen; öldürme, kasten yaralama, işkence, zor kullanma yetkisine ilişkin sınırın aşılması ve suç işlemek amacıyla örgüt kurma suçları ile örgüt faaliyeti çerçevesinde işlenen suçlarla ilgili ön incelemelerin ve/veya disiplin soruşturmalarının mülkiye müfettişleri tarafından yapılması esastır. Olayın niteliğinin gerektirdiği hâllerde, ön incelemeyi ve/veya disiplin soruşturmasını yürüten mülkiye müfettişleriyle birlikte görev yapmak üzere bağlı kuruluşların müfettişleri de görevlendirilebilir. Söz konusu suçlarla ilgili ön incelemeler ve/veya disiplin soruşturmalarının valiliklerce veya kaymakamlıklarca yapılması

hâlinde, bu işlemler imkânlar ölçüsünde mülkî idare amirliği hizmetleri sınıfında bulunan görevliler tarafından yürütülür.

c) Ön inceleme ve/veya disiplin soruşturmasını icra etmek üzere mülkiye müfettişi görevlendirilmesi durumunda, diğer idarî mercilerce başlatılmış olan ön inceleme ve/veya disiplin soruşturmaları, mülkiye müfettişine devredilir.

ç) Cumhuriyet savcılarının doğrudan soruşturma yapabilmelerine ilişkin özel hükümler saklıdır.

(2) Kurul Başkanlığınca, bu madde ve 4 üncü madde hükümleri çerçevesinde verilen görevleri yürütmek üzere yeteri kadar mülkiye müfettişi tahsis edilir. (Değişik cümle: 6/12/2019-7196/89 md.) Bu müfettişlere mezkûr görevlerinin haricinde zorunluluk olmadıkça başka bir görev verilmez ve bunlar görev alanlarıyla ilgili konularda düzenli hizmet içi eğitime tabi tutulurlar. Bu müfettişlerin belirlenmesine ilişkin esaslar, görevlendirilme yöntemi ve hizmet içi eğitimleri ile benzeri hususlar, Cumhurbaşkanınca yürürlüğe konulacak yönetmelikle düzenlenir.[5]

(3) Cumhuriyet savcılarını, kolluk görevlileri hakkında görevlerinden doğan veya görevleri sırasında işledikleri suçlar ile kişisel suçları sebebiyle soruşturma başlatmaları hâlinde, durumu, personelin ilgisine göre, Bakanlığa, valiliğe veya kaymakamlığa en geç yedi iş günü içinde bildirir. Bakanlık, valilik ve kaymakamlıklar ile idarî soruşturmayı yürüten görevliler, soruşturmanın gizliliğine zarar verilmemesine yönelik gerekli tüm tedbirleri alır.

(4) Şikâyetçi ile ihbar veya şikâyet edilen kolluk görevlileri, yapılan disiplin soruşturmasının safahatı hakkında, ilgisine göre Bakanlık, valilik veya kaymakamlıklarca en az iki ayda bir bilgilendirilir.

DÖRDÜNCÜ BÖLÜM

Değiştirilen, Geçici ve Son Hükümler

MADDE 9- (14/2/1985 tarihli ve 3152 sayılı İçişleri Bakanlığı Teşkilat ve Görevleri Hakkında Kanun ile ilgili olup yerine işlenmiştir.)

MADDE 10- (4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu ile ilgili olup yerine işlenmiştir.)

MADDE 11- (1) Bu Kanuna ekli (1) sayılı listede yer alan kadrolar ihdas edilerek, 13/12/1983 tarihli ve 190 sayılı Genel Kadro ve Usulü Hakkında Kanun Hükmünde Kararnamenin eki (I) sayılı cetvelin İçişleri Bakanlığına ait bölümüne eklenmiştir.[6]

Geçiş hükümleri

GEÇİCİ MADDE 1- (1) Bu Kanunda çıkarılması öngörülen yönetmelikler, bu Kanunun yayımı tarihinden itibaren altı ay içinde çıkarılır.

(2) 8 inci maddenin birinci fıkrasının (b) bendi hükmü, anılan fıkranın yürürlüğe girdiği tarihten önce başlatılan ön inceleme ve/veya disiplin soruşturmaları hakkında uygulanmaz.

(3) Merkezî kayıt sisteminin altyapısının oluşturulmasına yönelik iş ve işlemler, bu Kanunun yayımı tarihinden itibaren başlatılır.

(4) Öğretim üyeleri ile serbest avukatlar arasından teklif edilecek adaylar, Adalet ve İçişleri bakanları tarafından bu Kanunun yayımı tarihinden itibaren bir ay içinde Başbakanlığa bildirilir. Komisyon, Bakanlar Kurulunca üye seçiminin Bakanlığa bildirimini izleyen bir ay içinde Başkanın belirleyeceği bir tarihte ilk toplantısını yapar.

Yürürlük

MADDE 12- (1) Bu Kanunun;

a) 7 nci maddesi yayımı tarihinden itibaren bir yıl sonra,

b) Diğer hükümleri yayımı tarihinde,

yürürlüğe girer.

Yürütme

MADDE 13- (1) Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

6706 sayılı Cezai Konularda Uluslararası Adli İşbirliği Kanunu

Resmî Gazete Tarihi : 05.05.2016

Resmî Gazete Sayısı : 29703

CEZAÎ KONULARDA ULUSLARARASI ADLÎ İŞ BİRLİĞİ KANUNU

BİRİNCİ BÖLÜM

Genel Hükümler

Amaç ve kapsam

MADDE 1- (1) Bu Kanunun amacı, cezaî konularda uluslararası adlî iş birliğinin usul ve esaslarını düzenlemektir.

(2) Bu Kanun, yabancı devletlerle cezaî konularda yapılacak adlî iş birliğini kapsar.

(3) Türkiye'nin taraf olduğu adlî iş birliğine ilişkin milletlerarası andlaşmalar ile diğer kanun hükümleri saklıdır.

Tanımlar

MADDE 2- (1) Bu Kanunun uygulanmasında;

a) Adlî merci: Mahkeme, hâkimlik ve savcılıklar ile kanunla istisnaî olarak ceza soruşturması yapma yetkisi verilen diğer makamları, devletlerin milletlerarası andlaşmalara yaptıkları beyanlarda belirttikleri mercileri,

b) Merkezî Makam: Adalet Bakanlığını,

c) Uluslararası adlî iş birliği: Cezaî konularda bir devletin adlî mercilerinin diğer bir devletin adlî mercileri adına yerine getirdiği işlemleri,

ifade eder.

Merkezî Makamın görev ve yetkileri

MADDE 3- (1) Merkezî Makamın görev ve yetkileri şunlardır:

a) Taraf olunan milletlerarası andlaşmalar veya mütakabiliyet ilkesi çerçevesinde, yabancı devletlerin adlı iş birliđi taleplerinin kabulü ile Türk adlı mercilerinin yapacağı iş birliđi taleplerinin uygunluđu konusunda karar vermek.

b) Uygulanacak adlı iş birliđinin türü ve izlenecek yöntem konusunda karar vermek.

c) Adlı iş birliđi kapsamında devletlerce talep edilen bilgi ve belgelerin kullanılmasına muvafakat vermek, bunların kullanılmasını sınırlandırmak, teminat veya şarta bağlamak.

(2) Yabancı devlet ile Türkiye arasında hukukî ve fiilî mütakabiliyet bulunmaması hâlinde, adlı iş birliđi talebinin yerine getirilmesi, talep eden devletin Türkiye'nin aynı konuya ilişkin adlı iş birliđi taleplerini karşılamayı garanti etmesi şartına bağlanabilir.

(3) Yabancı bir devletin adlı iş birliđi talebinin yerine getirilmesi, Merkezî Makam tarafından şarta veya teminata bağlanabilir.

(4) Merkezî Makam, yargı yetkisine giren hususlar hariç olmak üzere, devletlerce ileri sürülen şartları kabul edebilir veya istenen teminatı verebilir. Merkezî Makamca kabul edilen şartlar veya verilen teminatlar adlı mercileri bağlar.

(5) Adlı iş birliđi taleplerinin yerine getirilmesi nedeniyle tazminat ödenmesi durumunda, Merkezî Makam ödenen tazminatı ilgili devletten talep edebilir.

(6) Adlı iş birliđi talebine esas teşkil eden suçun ağırlığı ile talebin yerine getirilmesi için sarf edilecek emek, mesai ve masraf arasında açık orantısızlık bulunması veya bir devletin mutad olarak yerine getirmekten imtina ettiđi işlemlere ilişkin olması hâlinde, Merkezî Makam talebi geri çevirebilir.

(7) Merkezî Makam, bu Kanun kapsamında yabancı devletlerle yapacağı işlemlerde gerektiğinde ilgili kamu kurum ve kuruluşlarının görüşünü alabilir.

Adlı iş birliđi taleplerinin reddi

MADDE 4- (1) Yabancı devletlerin adlı iş birliđi talepleri;

a) Türkiye'nin egemenlik hakları, millî güvenliđi, kamu düzeni veya diđer temel çıkarlarının ihlal edilmesi,

b) Talebe konu fiilin sırf askerî suç, düşünce suçu, siyasî suç veya siyasî suçla bağlantılı bir suç olması,

c) Talebe konu kişinin ırkı, etnik kökeni, dini, vatandaşlığı, belli bir sosyal gruba mensubiyeti veya siyasî görüşleri nedeniyle bir soruşturma veya kovuşturmaya maruz bırakılacağına veya

cezalandırılacağına ya da işkence veya kötü muameleye maruz kalacağına dair inandırıcı nedenlerin bulunması,

ç) Talepte bulunan devlette savunma hakkına ilişkin temel güvencelerin bulunmaması,

hâllerinde reddedilebilir.

Usul hükümlerinin uygulanması

MADDE 5- (1) Adlî iş birliği talepleri yerine getirilirken, bu Kanunda ve diğer kanunlarda hüküm bulunmayan hâllerde, 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümleri uygulanır.

Bilgi ve belgelerin kullanılması

MADDE 6- (1) Adlî iş birliği kapsamında gelen bilgi ve belgeler, gönderen devlet izin vermedikçe, talebe konu olan soruşturma veya kovuşturma ya da infaz işlemleri dışında kullanılamaz.

(2) Aşağıdaki hâllerde izin şartı aranmaz:

a) Talebe konu suçun hukukî vasfının değişmesi.

b) Adlî iş birliği işleminden sonra ortaya çıkan yeni şüpheli veya sanıkların soruşturma ya da kovuşturmayaya dâhil edilmesi.

c) Talebe konu suçla ilgili bilgi ve belgelerin, bu suçla bağlantılı olan hukuk davalarında gerekli olması.

İKİNCİ BÖLÜM

Adlî Yardımlaşma

Türk adli mercilerinin talepleri

MADDE 7- (1) Adlî merciler, soruşturma veya kovuşturmanın sonuçlandırılması ya da verilen mahkûmiyet kararlarının yerine getirilmesi için ihtiyaç duyulan konularda adlî yardımlaşma talebinde bulunabilir. Bu durumda aşağıdaki hükümler uygulanır:

a) Gecikmesinde sakınca bulunan hâllerde adlî yardımlaşma talebinden önce delillerin korunması amacıyla geçici tedbirlerin alınması istenebilir.

b) Tebligata ilişkin adlî yardımlaşma taleplerinde, kısıtlayıcı veya zorlayıcı tedbir uygulanacağına ilişkin ihtarlar yer verilmez.

c) Adlî yardımlaşma talebine konu işlemin yerine getirilmesi sırasında hazır bulunma talebinde bulunulabilir.

ç) Adlî yardımlaşma talebi kapsamında ilgili devletin iç hukukuna uygun olarak yerine getirdiği işlemler, Türk hukuku bakımından da geçerli sayılır.

(2) Adlî mercilerce, yürütülen bir soruşturma veya kovuşturma kapsamında başka bir devletin ceza soruşturması başlatmasına neden olabilecek bilgilerin öğrenilmesi hâlinde, talep olmaksızın bu bilgiler, ilgili devlete gönderilmek üzere Merkezî Makama bildirilebilir.

Yabancı adlî mercilerin talepleri

MADDE 8- (1) Adlî yardımlaşma talepleri hakkında aşağıdaki hükümler uygulanır:

a) Talepler, Türk hukukuna uygun olarak yerine getirilir. Özel bir usulün talep edilmesi hâlinde, Türk hukukuna aykırı olmadığı takdirde, talep bu usule uygun olarak yerine getirilebilir.

b) Türk adlî mercileri, talepleri kısmen veya tamamen reddedebilir ya da gerek görülen hâllerde ek bilgi veya belge isteyebilir.

c) Gecikmesinde sakınca bulunan hâllerde, adlî yardımlaşma talebi gönderilmeden önce delillerin korunması amacıyla geçici tedbirler alınabilir. Geçici tedbirin alındığı tarihten itibaren kırk gün içinde adlî yardımlaşma talebinin Merkezî Makama ulaşmaması hâlinde tedbir, yetkili makam veya merciler tarafından derhâl kaldırılır.

ç) Arama veya elkoyma talebinde bulunulması hâlinde, talebin konusu olan suçun iadeye elverişli bir suç olması gerekir. Talep üzerine elkonulan malvarlığı değerleri ile taşınmaz, hak ve alacaklarla ilgili olarak Türk adlî mercileri yılda en az bir defa talep eden devletten tedbirin devamının istenip istenmediğine ilişkin bilgi ister.

d) Tebligata ilişkin adlî yardımlaşma talebinde kısıtlayıcı veya zorlayıcı tedbir uygulanacağına ilişkin ihtar bulunması hâlinde talep reddedilir.

e) Adlî yardımlaşma talebine konu işlemin yerine getirilmesi sırasında yabancı adlî merciler, Türk adlî mercileri önünde hazır bulunma talebinde bulunabilir. Talep, uygun görülmesi hâlinde yerine getirilir.

f) Kişi hakkında Türk mahkemelerince verilen mahkûmiyet veya beraat hükmü bulunması ya da suçun affa veya zamanaşımına uğramış olması hâlinde, aynı fiile ilişkin adlî yardımlaşma talepleri yerine getirilmeyebilir.

Görüntülü ve sesli iletişim tekniğiyle adlî yardımlaşma

MADDE 9- (1) Adli yardımlaşma talebinin yerine getirilmesinde görüntülü ve sesli iletişim tekniğinin kullanılması istenebilir. Bu işlemler, yerine getiren devletin yetkili makam veya mercilerinin yönetimi altında ve bu devletin hukuku uyarınca yürütülür.

(2) Türk adli mercileri tarafından adli yardımlaşma talebinin görüntülü ve sesli iletişim tekniği kullanılmak suretiyle yerine getirilmesinin istenmesi hâlinde, milletlerarası andlaşmalarda hüküm bulunması kaydıyla işlem, Türk adli mercilerinin yönetimi altında ve Türk hukuku uyarınca yürütülür.

(3) Yabancı devlet tarafından adli yardımlaşma talebinin görüntülü ve sesli iletişim tekniği kullanılmak suretiyle yerine getirilmesinin istenmesi hâlinde, milletlerarası andlaşmalarda hüküm bulunması kaydıyla işlem, talep eden devletin adli mercilerinin yönetimi altında ve bu devletin hukuku uyarınca yürütülür. Bu işlem sırasında Türk adli mercileri hazır bulunur ve Türk hukukunun temel ilkelerinin ihlal edilmemesi gözetilir.

ÜÇÜNCÜ BÖLÜM

İade

Türkiye'den yabancı devlete iade

MADDE 10- (1) Yabancı ülkede işlenen bir suç nedeniyle hakkında adli merciler tarafından ceza soruşturması veya kovuşturması başlatılan ya da mahkûmiyet kararı verilen bir yabancı, talep üzerine, soruşturma veya kovuşturmanın sonuçlandırılabilmesi ya da hükmedilen cezanın infazı amacıyla talep eden devlete iade edilebilir.

(2) Talep eden devlet hukuku ile Türk hukukuna göre, soruşturma veya kovuşturma aşamasında üst sınırı bir yıl veya daha fazla hürriyeti bağlayıcı cezayı gerektiren suçlardan dolayı iade talebi kabul edilebilir. Kesinleşmiş mahkûmiyet kararları bakımından iade talebinin kabul edilebilmesi için hükmolunan cezanın en az dört ay hürriyeti bağlayıcı ceza olması gerekir. İadesi istenen kişinin birden fazla suçu bulunması hâlinde, bunlardan bazılarının cezası belirtilen sürelerin altında olsa dahi birlikte iadeye konu edilebilir.

(3) Aynı kişi hakkında birden fazla devlet tarafından iade talebinde bulunulması hâlinde, suçların ağırlığı ve işlendiği yer, taleplerin geliş sırası, kişinin vatandaşlığı ve yeniden iade edilme ihtimali gibi şartlar dikkate alınarak, iade taleplerinden hangisinin öncelikli olarak işleme alınacağı Merkezî Makam tarafından belirlenir.

(4) İade hâlinde, kişi ancak iade kararına dayanak teşkil eden suçlardan dolayı yargılanabilir veya kişinin mahkûm olduğu ceza infaz edilebilir.

İadenin kabul edilemeyeceği hâller

MADDE 11- (1) Aşağıda sayılan hâllerde iade talebi kabul edilmez:

a) Uluslararası Ceza Divanına taraf olmanın gerektirdiği yükümlülükler hariç olmak üzere, iadesi talep edilen kişinin Türk vatandaşı olması.

b) İadesi talep edilen kişinin ırkı, etnik kökeni, dini, vatandaşlığı, belli bir sosyal gruba mensubiyeti veya siyasî görüşleri nedeniyle bir soruşturma veya kovuşturmaya maruz bırakılacağına veya cezalandırılacağına ya da işkence veya kötü muameleye maruz kalacağına dair kuvvetli şüphe sebeplerinin bulunması.

c) İade talebine esas teşkil eden fiilin;

1) Düşünce suçu, siyasî suç veya siyasî suçla bağlantılı bir suç niteliğinde olması,

2) Sırf askerî suç niteliğinde olması,

3) Türkiye Devletinin güvenliğine karşı, Türkiye Devletinin veya bir Türk vatandaşının ya da Türk kanunlarına göre kurulmuş bir tüzel kişinin zararına işlenmesi,

4) Türkiye'nin yargılama yetkisine giren bir suç olması,

5) Zamanaşımı veya affa uğramış olması.

ç) İadesi talep edilen kişi hakkında, talebe konu fiil nedeniyle daha önce Türkiye'de beraat veya mahkûmiyet kararı verilmiş olması.

d) İade talebinin, ölüm cezası veya insan onuru ile bağdaşmayan bir ceza gerektiren suçlara ilişkin olması.

(2) Birinci fıkranın (c) bendinin (1) numaralı alt bendi kapsamındaki iade talebinin dayanağını teşkil eden fiilin bütün unsurları, özellikle işleniş şekli, suçun işlenişinde kullanılan araçların veya ortaya çıkan sonuçların ağırlığı dikkate alınarak fiil siyasî suç olarak kabul edilmeyebilir. Soykırım ve insanlığa karşı suçlar, siyasî suç olarak kabul edilmez.

(3) Birinci fıkranın (d) bendinde, cezanın niteliğine ilişkin bir ret sebebinin varlığı hâlinde, talep eden devlet tarafından, öngörülen cezanın infaz edilmeyeceğine dair yeterli teminat verilmesi hâlinde, iade talebi kabul edilebilir.

(4) İadesi talep edilen kişinin, talep tarihinde on sekiz yaşını doldurmamış olması, uzun zamandan beri Türkiye’de bulunuyor olması veya evli bulunması gibi kişisel hâlleri nedeniyle, iadenin kişinin kendisini veya ailesini, fiilin ağırlığı ile orantısız şekilde mağdur edecek olması durumunda iade talebi kabul edilmeyebilir.

İade ve sınır dışı ilişkisi

MADDE 12- (1) Yabancı, iade sürecinde Merkezî Makamın görüşü alınmadan sınır dışı edilemez.

(2) Yabancı, Merkezî Makamın görüşü alınmadan, iade talebi reddedilen devlete sınır dışı edilemez.

Merkezî Makamın incelemesi

MADDE 13- (1) Merkezî Makam, iade taleplerini inceleyerek, lüzum görmesi hâlinde ek bilgi ve belge talebinde bulunabilir ve gerekli şartları taşımayan talepleri reddeder.

(2) Gerekli şartları taşıyan talepler, yetkili ağır ceza mahkemesi nezdindeki Cumhuriyet başsavcılığına gönderilir.

Geçici tutuklama

MADDE 14- (1) İade talebine konu olabilecek bir suçun işlendiğinin kabulü için kuvvetli şüphe bulunması hâlinde, iade talebinin Merkezî Makama ulaşmasından önce, Türkiye’nin taraf olduğu milletlerarası andlaşma hükümleri veya mütekabiliyet ilkesi çerçevesinde, ilgili devletin talebi ve Merkezî Makamın uygun bulması üzerine kişi geçici olarak tutuklanabilir.

(2) İade talebine konu olabilecek ve 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 12 nci maddesinin üçüncü fıkrasının (a) bendi kapsamına giren bir suç işlediği yönünde kuvvetli şüphe bulunan kişi, ilgili devletin talebi aranmaksızın geçici olarak tutuklanabilir.

(3) İlgili devletin geçici tutuklama talebi, Merkezî Makam tarafından iade amacıyla yakalanması ve Cumhuriyet başsavcılığına sevki için İçişleri Bakanlığına gönderilir. Yakalanan kişi, geçici tutuklama hususunda karar verilmek üzere en geç yirmi dört saat içinde sulh ceza hâkimi önüne çıkarılır. Sulh ceza hâkimi geçici tutuklanması talep edilen kişiye, rızaya dayalı iade imkânı ile bunun hukukî sonuçları hakkında bilgi verdikten sonra talep hakkında karar verir.

(4) Geçici tutuklama süresi ilgili milletlerarası andlaşma hükümlerine göre belirlenir. Mütekabiliyet ilkesi çerçevesinde kişi, en fazla kırk gün geçici tutuklu kalabilir.

(5) Geçici tutuklama yerine kişinin kaçmasına engel olacak şekilde Ceza Muhakemesi Kanununun 109 uncu maddesi uyarınca adlî kontrol kararı verilebilir.

(6) İlgili devlet tarafından dördüncü fıkrada belirtilen süre içinde iade evrakının gönderilmemesi hâlinde geçici tutuklama veya adlî kontrol kararı kaldırılır. Bu durum, iade talebinin alınmasından sonra iade amacıyla koruma tedbirleri uygulanmasına engel teşkil etmez.

Görev ve yetki

MADDE 15- (1) İade talebi hakkında karar vermeye, kişinin bulunduğu yer ağır ceza mahkemesi yetkilidir. Kişinin bulunduğu yer belli değilse, Ankara ağır ceza mahkemesi yetkilidir.

(2) Cumhuriyet başsavcılığı, iade talebine ilişkin karar vermek üzere ağır ceza mahkemesinden talepte bulunur.

İade amacıyla koruma tedbirlerinin uygulanması

MADDE 16- (1) Ağır ceza mahkemesi iade sürecinin her aşamasında iadesi talep edilen kişi hakkında Ceza Muhakemesi Kanunu hükümleri uyarınca koruma tedbirlerine karar verebilir.

(2) İade sürecinde kişinin tutuklanması durumunda teslimine kadar geçen süre içindeki tutukluluk durumu, ağır ceza mahkemesince en geç otuzar günlük sürelerle incelenir.

(3) Ağır ceza mahkemesinin iade talebinin kabulüne ilişkin kararının kesinleşmesinden itibaren bir yıl içinde 19 uncu maddeye göre iade kararı verilmemesi hâlinde kişi hakkındaki koruma tedbirleri kaldırılır.

(4) Toplam tutukluluk süresi, kişinin iade talebine konu suçtan dolayı alabileceği veya mahkûm olduğu cezanın infaz süresini geçemez.

Rızaya dayalı iade usulü

MADDE 17- (1) Kişi, iadeye rıza göstermesi hâlinde normal iade usulü uygulanmadan talep eden devlete iade edilebilir.

(2) Ağır ceza mahkemesince kişiye, Ceza Muhakemesi Kanununda belirtilen haklarıyla birlikte rızaya dayalı iadenin mahiyeti ve hukukî sonuçları anlatılır. Kişiye rızaya dayalı iade usulünü kabul edip etmediği sorulur.

(3) Mahkeme, kişinin rızaya dayalı iade usulünü kabul etmesi üzerine bu Kanun ve Türkiye'nin taraf olduğu milletlerarası andlaşma hükümlerine göre iade talebinin kabul edilebilir olup olmadığına karar verir. Bu karara karşı itiraz yoluna başvurulabilir. Kararın kesinleşmesi hâlinde iade evrakı Merkezî Makama gönderilir.

(4) Rızaya dayalı iade usulü uygulanarak verilen iade kararının yerine getirilmesi, Merkezî Makamın onayına bağlıdır.

İade yargılaması

MADDE 18- (1) Kişinin rızaya dayalı iade usulünü kabul etmemesi hâlinde mahkeme, iade şartlarını bu Kanun ve Türkiye'nin taraf olduğu milletlerarası andlaşma hükümlerine göre inceleyerek iade talebinin kabul edilebilir olup olmadığına karar verir.

(2) Talep eden devlet tarafından gönderilen belgelerin yeterli görülmemesi hâlinde mahkeme, uygun bir süre içinde ek bilgi ve belgelerin gönderilmesini isteyebilir.

(3) İade yargılamasında katılma talebinde bulunulamaz.

(4) Mahkemenin kararına karşı temyiz yoluna başvurulabilir. Yargıtay bu başvuruları üç ay içinde sonuçlandırır. Kararın kesinleşmesi hâlinde iade evrakı karar ile birlikte Merkezî Makama gönderilir.

İade kararı

MADDE 19- (1) Ağır ceza mahkemesince iade talebinin kabul edilebilir olduğuna karar verilmesi hâlinde, bu kararın yerine getirilmesi, Dışişleri ve İçişleri bakanlıklarının görüşü alınarak Adalet Bakanının teklifi ve Cumhurbaşkanı'nın onayına bağlıdır.[1]

(2) Merkezî Makam iade talebinin kabul veya ret edildiğini, talep eden devlete ve iadesi talep edilen kişiye bildirir.

Teslim

MADDE 20- (1) İadesine karar verilen kişinin teslim işlemleri, ilgili bakanlıklarla iş birliği hâlinde yürütülür.

(2) İadesine karar verilen kişinin, talep eden devlet makamları ile kararlaştırılan tarihte haklı bir neden olmaksızın teslim alınmaması hâlinde, bu tarihten itibaren otuz gün sonra mahkemece kişi hakkında verilen koruma tedbirleri kaldırılır.

(3) İadesine karar verilen kişi hakkında, başka bir suç nedeniyle Türkiye'de ceza soruşturması veya kovuşturması ya da infazı gerekli bir hapis cezası bulunması veya kişinin seyahat edebilecek durumda olmaması hâlinde, Merkezî Makam tarafından teslimin ertelenmesine karar verilebilir. Bu karar, kişiye ve talep eden devlete bildirilir.

(4) İade talebine konu suç bakımından ispat aracı olarak yararlı görülen veya suçun işlenmesiyle elde edilen ve kişi yakalandığında üzerinde ele geçen ya da daha sonra ortaya çıkan eşya, talep eden

devlete teslim edilebilir. İadesi talep edilen kişinin ölümü, kaçması veya benzer sebeplerle iade hakkında bir karar verilememesi hâlinde de eşyanın teslimi gerçekleştirilebilir.

(5) Türkiye’de yürütülmekte olan bir soruşturma veya kovuşturma bakımından zorunlu olduğu takdirde eşyanın teslimi ertelenebilir.

(6) İyiniyetli üçüncü kişilere ait eşyanın teslim talepleri yerine getirilmez.

Transit geçiş kararı

MADDE 21- (1) Türk hukuku açısından iade koşullarının bulunması hâlinde, bir devlet tarafından başka bir devlete iadesine karar verilen kişinin Türkiye’den transit geçişine izin verilebilir.

(2) Transit geçiş talebi, Merkezî Makam tarafından değerlendirilir ve verilen karar, talep eden devletin yetkili makamına bildirilir.

(3) Transit geçişin yirmi dört saatten fazla sürmesi ve bu nedenle kişinin hürriyetinin kısıtlanması ihtiyacının ortaya çıkması durumunda, sulh ceza hâkimince transit geçişin sağlanması amacıyla yedi günü geçmemek üzere geçici tutuklama kararı verilebilir.

(4) Transit geçiş talebinin reddini gerektiren nedenlerin ortaya çıkması veya kişinin transit geçiş sırasında resen soruşturma yapılmasını gerektirecek bir suç işlemesi hâlinde transit geçiş durdurulabilir.

(5) Bir devletten başka bir devlete gerçekleştirilecek hükümlü nakilleri ile ilgili olarak Türkiye üzerinden yapılacak transit geçişler hakkında da bu madde hükümleri uygulanır.

Türkiye’nin iade talepleri ve şartları

MADDE 22- (1) Soruşturma veya kovuşturmanın sonuçlandırılabilmesi ya da verilen mahkûmiyet kararlarının infazı amacıyla yabancı bir ülkede bulunan ve hakkında yakalama emri veya tutuklama kararı verilen kişinin Türkiye’ye iadesi, adlî merciler tarafından istenebilir.

(2) Üst sınırı bir yıl veya daha fazla hapis cezasını gerektiren bir suçtan dolayı kişinin iadesi talep edilebilir. Kesinleşmiş mahkûmiyet kararları bakımından iade talebinde bulunulabilmesi için hükmolunan hapis cezasının en az dört ay olması gerekir. İadesi istenen kişinin birden fazla suçta bulunması hâlinde, bunlardan bazılarının cezası belirtilen sürelerin altında olsa dahi birlikte iadeye konu edilebilir.

(3) Merkezî Makam tarafından uygun görülmesi hâlinde talep, yabancı devlete gönderilir. Ancak, aşağıdaki durumlarda Merkezî Makam iade talebini yabancı devlete göndermeden reddedebilir:

a) Talebin, iade için gerekli şartları taşımaması.

b) Ceza infaz kurumlarında geçirilecek süre dikkate alındığında, iade yoluna başvurulmasının kişi yararı ve kamu yararı arasında açık bir orantısızlığa sebep olması.

c) Türkiye'nin millî güvenliğinin veya uluslararası ilişkilerinin zarar görme ihtimalinin bulunması.

(4) Türkiye'ye iadesine karar verilen kişinin üçüncü ülkelerden transit geçişi ve teslim konusunda, uygun olduğu ölçüde 20 nci ve 21 inci maddelerde yer alan hükümler uygulanır.

DÖRDÜNCÜ BÖLÜM

Soruşturma veya Kovuşturmanın Devri

Soruşturmanın veya kovuşturmanın devri

MADDE 23- (1) Bu Kanun ve taraf olunan milletlerarası andlaşmalar çerçevesinde, işlenen suçlarla ilgili Türkiye'de yürütülen soruşturma veya kovuşturmalar yabancı devletlere devredilebilir; yabancı devletlerde işlenen suçlarla ilgili yürütülen soruşturma veya kovuşturmalar devralınabilir.

(2) Milletlerarası andlaşma bulunmaması hâlinde, mütekabiliyet ilkesi esas alınarak bu Kanun çerçevesinde soruşturma veya kovuşturmalar devredilebilir veya devralınabilir.

Soruşturmanın veya kovuşturmanın yabancı devlete devredilmesi

MADDE 24- (1) Üst sınırı bir yıl veya daha fazla hapis cezasını gerektiren suçlardan dolayı yürütülen soruşturma veya kovuşturmalar;

a) Şüpheli veya sanığın yabancı devletin vatandaşı olması nedeniyle Türkiye'de hazır bulundurulamaması veya adlî yardımlaşma yoluyla savunmasının alınamaması,

b) Türk vatandaşı olan şüpheli veya sanığın yabancı devlette mutat olarak bulunması veya delillerin bu devlette olması nedeniyle devrin, gerçeğin ortaya çıkarılmasına imkân vermesi,

hâllerinde devredilebilir.

(2) Soruşturma veya kovuşturmanın devri adlî merciler tarafından talep edilir. Merkezî Makamın olumlu görüşü üzerine talep, ilgili devlete gönderilir. Bu işlem, soruşturma veya kovuşturmanın yürütülmesine engel değildir. Devir talebine, soruşturma veya kovuşturma dosyasının bir sureti ve gerekli olduğunda tercümesi eklenir. Devir talebinin kabul edilmesi ve istem üzerine delil niteliğindeki eşyalar da gönderilir.

(3) Soruşturmanın devri talebinin kabul edilmesi üzerine, Ceza Muhakemesi Kanununun 171 inci maddesinde düzenlenen koşullara ve sonuçlarına bakılmaksızın kamu davasının açılmasının

ertelenmesine karar verilir. Şüpheli hakkında yabancı adlî merci tarafından dava açılması durumunda kovuşturmayaya yer olmadığına karar verilir. Dava açılmaması hâlinde, buna ilişkin kararın gerekçesi değerlendirilmek suretiyle soruşturmaya devam edilebilir.

(4) Kovuşturmanın devri talebinin kabul edilmesi üzerine durma kararı verilir. Sanık hakkında yabancı adlî merci tarafından mahkûmiyet kararı verilmesi durumunda düşme kararı verilir. Mahkûmiyet kararı dışında bir karar verilmesi durumunda, buna ilişkin kararın gerekçesi değerlendirilmek suretiyle kovuşturmayaya devam edilebilir.

(5) Yabancı devletin soruşturma veya kovuşturmanın devrinin kabulüne ilişkin karardan vazgeçtiğini bildirmesi veya devredilen soruşturma veya kovuşturmanın sağlıklı bir şekilde yürütülmediğinin Merkezî Makamca adlî mercie bildirilmesi hâlinde soruşturma veya kovuşturmanın yürütülmesine karar verilir.

(6) Gecikmesinde sakınca bulunan hâllerde soruşturma veya kovuşturmanın devri talebiyle birlikte veya öncesinde, talep edilen devlet makamlarından elkoyma ve tutuklama dâhil bütün geçici tedbirlerin alınması istenebilir.

Soruşturma veya kovuşturmanın devralınması

MADDE 25- (1) Yurt dışında işlenen ve Türk hukukuna göre zamanaşımına veya affa uğramamış, üst sınırı bir yıl veya daha fazla hapis cezasını gerektiren bir suç nedeniyle yabancı bir devlette yürütülen soruşturma veya kovuşturmalar devralınabilir. Ancak;

- a) Kişi, Türkiye’de mutad olarak bulunmuyorsa,
 - b) Kişi, Türk vatandaşı değilse,
 - c) Suç, talep eden devletin sınırları dışında işlenmişse,
 - ç) Devir talebine konu fiil nedeniyle kişi daha önce Türkiye’de yargılanmışsa,
- devir talebi kabul edilmez.

(2) Merkezî Makamın uygun görmesi üzerine soruşturmanın veya kovuşturmanın devrine ilişkin talep, yetkili Cumhuriyet başsavcılığına gönderilir. Cumhuriyet başsavcılığı soruşturma veya kovuşturmanın devrine konu olan suça ilişkin soruşturma başlatır ve sonucuna göre işlem yapar.

(3) Talepte bulunan yabancı devlet mevzuatına göre yapılmış soruşturma veya kovuşturma işlemleri ve elde edilen deliller Türk hukuku bakımından geçerli sayılır.

BEŞİNCİ BÖLÜM

İnfazın Devri

İnfazın devralınması

MADDE 26- (1) Yabancı devlet mahkemeleri tarafından verilen mahkûmiyet kararları aşağıdaki koşulların birlikte bulunması hâlinde Türkiye’de infaz edilebilir:

- a) Hükümlünün Türkiye’de bulunması.
- b) Mahkûmiyet kararının kesinleşmiş olması.
- c) Mahkûmiyet kararına konu fiilin Türk hukukuna göre suç teşkil etmesi ve zamanaşımına uğramamış olması.
- ç) Hürriyeti bağlayıcı cezalar için, merkezî makamlarca aksi kararlaştırılmadıkça talep tarihinde, hükümlünün ceza infaz kurumunda infazı gereken en az altı ay hürriyeti bağlayıcı cezasının bulunması.
- d) Aynı suçtan dolayı Türkiye’de soruşturma veya kovuşturma yapılmamış olması.

(2) İnfazın devri talebinde bulunulması hâlinde, yabancı devlet makamlarından;

- a) Mahkûmiyet kararının onaylı sureti,
 - b) Hükme esas alınan kanun maddelerinin metni,
 - c) İnfazı gereken bakiye cezayı gösteren belge,
 - ç) Talebin değerlendirilmesi için gerekli görülebilecek diğer bilgi ve belgeler,
 - d) Gerekli görüldüğü takdirde bu fıkrada belirtilen belgelerin tercümeleleri,
- talep edilir.

(3) Devir koşullarının bulunmadığının tespit edilmesi veya devrin Türkiye’nin millî güvenliği ile temel çıkarlarına uygun düşmeyeceğinin anlaşılması hâlinde, devir talebi Merkezî Makam tarafından reddedilir.

(4) İnfazın devrine ilişkin talep alınmadan önce mahkûmiyete konu suç, ceza miktarı ve şahsın kaçma şüphesi dikkate alınarak, yabancı devletin istemi ve Merkezî Makamın olumlu görüşü üzerine 14 üncü madde uyarınca koruma tedbirlerine karar verilebilir.

(5) İnfazın devrine ilişkin talep, Türk hukukuna göre uyarılama kararı verilmesi için Ankara ağır ceza mahkemesine gönderilir. Mahkemece on beş gün içinde, yabancı devlette verilen mahkûmiyet kararında sübutu kabul edilen fiile, Türk kanunlarına göre verilmesi gereken ceza tayin olunur. Bu

suretle belirlenen ceza, yabancı mahkeme kararında tayin edilmiş ceza süresini geçemez. Uyarlama kararına karşı itiraz kanun yoluna başvurulabilir. Ağır ceza mahkemesi koruma tedbirleri hakkında da karar vermeye yetkilidir.

(6) Uyarlama kararı, talep eden devlet makamlarına bildirilmek üzere Merkezî Makama gönderilir.

Türkiye’de infaz

MADDE 27- (1) Yabancı devletin infazı devretmesi üzerine durum, uyarlama kararını veren mahkemeye bildirilir. Mahkeme infaza başlanması için kararı Cumhuriyet başsavcılığına gönderir. Mahkeme ayrıca kararı Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğüne bildirir.

(2) Ağır ceza mahkemesince verilen mahkûmiyet kararı Türk kanunlarına göre infaz edilir.

(3) Mahkûmiyetin esasına taallûk eden talepler, hükmün esası hakkında karar veren devlet mahkemelerine yapılabilir, verilen kararlar ağır ceza mahkemesince yeniden uyarlanır.

(4) İnfaz sırasında, hükmün verildiği devlette veya Türkiye’de genel veya özel af kabul edilmesi ya da suç ve cezayı ortadan kaldıran veya hafifleten bir sebebin ortaya çıkması hâlinde hükümlünün hukukî durumu, uyarlama kararını veren ağır ceza mahkemesince karara bağlanır.

İnfazın devredilmesi

MADDE 28- (1) Aşağıdaki koşulların birlikte bulunması hâlinde, Cumhuriyet başsavcılığınca, Türk mahkemeleri tarafından verilen mahkûmiyet kararlarının yabancı devlette infaz edilmesi talep edilebilir:

a) İnfazın devredileceği devlette bulunan hükümlünün, bu devletin vatandaşı olması veya bu devlet ile güçlü sosyal bağlarının bulunması.

b) Mahkûmiyet kararının kesinleşmiş olması.

c) Mahkûmiyet kararına konu fiilin yabancı devlet hukukuna göre suç teşkil etmesi.

ç) Hapis cezaları için, merkezî makamlarca aksi kararlaştırılmadıkça talep tarihinde, hükümlünün ceza infaz kurumunda infazı gereken en az altı ay hapis cezasının bulunması.

d) Merkezî Makamın olumlu görüşünün bulunması.

(2) Cezaları denetimli serbestlik tedbiri uygulanarak infaz edilen hükümlülerin cezaları devredilebilir.

(3) İnfazın devri talebinde bulunulması infaz işlemlerinin yürütülmesine engel değildir.

(4) Devrin, ceza adaletinin amaçlarına hizmet etmeyeceğinin veya Türkiye'nin millî güvenliği ile temel çıkarlarına uygun düşmeyeceğinin anlaşılması hâlinde, devir talebi Merkezî Makam tarafından reddedilir.

(5) Yabancı devlet makamlarına;

a) Mahkûmiyet kararının onaylı sureti,

b) Hükme esas alınan kanun maddelerinin metni,

c) İnfazı gereken bakiye cezayı gösteren belge,

ç) Talebin değerlendirilmesi için gerekli görülebilecek diğer bilgi ve belgeler,

d) Gerekli görüldüğü takdirde bu fıkra da belirtilen belgelerin tercümele ri,

gönderilir.

(6) İnfazın devredilebilmesi için devrin yapılacağı devletten infazın nasıl yapılacağı nın bildirilmesi istenir. Gelen bilgilere göre devir talebi, Merkezî Makamın uygun görüşüyle Cumhuriyet başsavcılığınca geri alınabilir.

Yabancı devlette infazın sonuçları

MADDE 29- (1) Merkezî Makam, yabancı devletten infaz sırasında ortaya çıkacak özel durumlar ile infazın tamamlanması veya hükümlünün firarı gibi önemli bilgileri bildirmesini ister. Merkezî Makama ulaşan bilgiler, Cumhuriyet başsavcılığına bildirilir.

(2) Kararın tamamen infaz edilmesi veya infaz kabiliyetini kısmen veya tamamen kaybetmesi, Türk hukuku bakımından da aynı sonuçları doğurur.

(3) Yabancı devletin kararı infaz etmemesi veya edememesi hâlinde infaz işlemlerine Türkiye'de devam edilir.

ALTINCI BÖLÜM

Hükümlü Nakli

Türkiye'ye hükümlü nakli

MADDE 30- (1) Yabancı devlet mahkemeleri tarafından hakkında mahkûmiyet kararı verilen ve ceza infaz kurumunda bulunan hükümlü, aşağıdaki koşulların birlikte bulunması hâlinde cezanın infazı amacıyla Türkiye'ye nakledilebilir:

a) Hükümlünün Türk vatandaşı olması veya Türkiye ile güçlü sosyal bağlarının bulunması.

b) Hükümlünün veya kanunî temsilcisinin rıza göstermesi.

c) Mahkûmiyet kararının kesinleşmiş olması.

ç) Mahkûmiyet kararına konu fiilin Türk hukukuna göre suç teşkil etmesi.

d) Merkezî makamlarca aksi kararlaştırılmadıkça, talep tarihinde, hükümlünün ceza infaz kurumunda infazı gereken en az altı ay hapis cezasının bulunması.

(2) Hükümlü, kanunî temsilcisi veya yakını tarafından Türkiye'ye nakil talebinde bulunulması hâlinde, yabancı devlet makamlarından;

a) Mahkûmiyet kararının onaylı sureti,

b) Hükme esas alınan kanun maddelerinin metni,

c) Hükümlünün veya kanunî temsilcisinin nakle rıza gösterdiğine dair belge,

ç) İnfazı gereken cezayı gösteren belge,

d) Gerekli görüldüğü takdirde, hükümlünün sağlık durumunu gösteren tıbbî raporlar ile hastalığı varsa tedavisine ilişkin tavsiyeleri içeren belgeler,

e) Gerekli görüldüğü takdirde bu fıkrada belirtilen belgelerin tercümeleri,

talep edilir.

(3) Nakil koşullarının bulunmadığının, naklin, hükümlünün sosyal rehabilitasyonuna katkı sağlamayacağı, ceza adaletinin amaçlarına hizmet etmeyeceğinin veya Türkiye'nin millî güvenliği ile temel çıkarlarına uygun düşmeyeceğinin anlaşılması hâlinde, nakil talebi Merkezî Makam tarafından reddedilebilir.

(4) Hükümlülerin nakline Adalet Bakanı karar verir.

Türkiye'de infaz

MADDE 31- (1) Hükümlünün nakline karar verilmesi üzerine, ceza infaz kurumlarında kalacağı süre hükümlüye ve yabancı makamlara bildirilir. Yabancı devlet ile hükümlünün, nakli kabul etmesi üzerine, hükümlü Türkiye'ye getirilir. Hükümlü, nakil dosyası ile birlikte Cumhuriyet başsavcılığına teslim edilir. Cumhuriyet başsavcılığı, infazına başlanan karara ilişkin bilgileri Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğüne bildirir.

(2) Hükümlü hakkında verilen mahkûmiyet kararı Türk kanunlarına göre infaz edilir.

(3) Mahkûmiyetin esasına taallûk eden talepler, hükmün esası hakkında karar veren devlet mahkemelerine yapılabilir; verilen kararlar ikinci fıkra uyarınca infaz edilir.

(4) İnfaz sırasında, hükmün verildiği devlette veya Türkiye’de genel veya özel af kabul edilmesi ya da suç veya cezayı ortadan kaldıran veya hafifleten bir sebebin ortaya çıkması hâlinde hükümlünün hukukî durumu hakkında bulunduğu yer ağır ceza mahkemesince karar verilir.

Türkiye’den hükümlü nakli

MADDE 32- (1) Türk mahkemeleri tarafından hakkında mahkûmiyet kararı verilen ve ceza infaz kurumunda bulunan hükümlü, aşağıdaki koşulların birlikte bulunması hâlinde cezanın infazı amacıyla yabancı devlete nakledilebilir:

a) Hükümlünün nakledileceği devletin vatandaşı olması veya bu devlet ile güçlü sosyal bağlarının bulunması.

b) Hükümlünün veya kanunî temsilcisinin rıza göstermesi.

c) Mahkûmiyet kararının kesinleşmiş olması.

ç) Mahkûmiyet kararına konu fiilin nakli istenen devlet hukukuna göre suç teşkil etmesi.

d) Merkezî makamlarca aksi kararlaştırılmadıkça, talep tarihinde, hükümlünün ceza infaz kurumunda infazı gereken en az altı ay hapis cezasının bulunması.

e) Hükümlü hakkında başka bir suçtan dolayı, Türkiye’de bir soruşturma veya kovuşturma bulunmaması.

(2) Hükümlü, kanunî temsilcisi veya yakını tarafından Türkiye’den başka bir devlete nakil talebinde bulunulması hâlinde, bu devlet makamlarına;

a) Mahkûmiyet kararının onaylı sureti,

b) Hükme esas alınan kanun maddelerinin metni,

c) Hükümlünün veya kanunî temsilcisinin nakle rıza gösterdiğine dair belge,

ç) İnfazı gereken bakiye cezayı gösteren belge,

d) Gerekli görüldüğü takdirde, hükümlünün sağlık durumunu gösteren tıbbî raporlar ile hastalığı varsa tedavisine ilişkin tavsiyeleri içeren belgeler,

e) Gerekli görüldüğü takdirde bu fıkroda belirtilen belgelerin tercümeleleri,

gönderilir.

(3) Nakil koşullarının bulunmadığının, naklin, hükümlünün sosyal rehabilitasyonuna katkı sağlamayacağına, ceza adaletinin amaçlarına hizmet etmeyeceğinin veya Türkiye'nin millî güvenliği ile temel çıkarlarına uygun düşmeyeceğinin anlaşılması hâlinde, nakil talebi Merkezî Makam tarafından reddedilebilir.

(4) Hükümlünün hapis cezası ile birlikte adlî para cezasının bulunması hâlinde, nakle karar verilebilmesi için adlî para cezasının ödenmesi gerekir. Adlî para cezasının ödenmemesi hâlinde, ödenmeyen kısma karşılık gelen gün miktarı hapis cezasına çevrilir. Hükümlünün Türkiye'de infaz edilen cezası, öncelikle adlî para cezasından çevrilen hapis cezasına mahsup edilir. Hükümlünün ceza infaz kurumunda kaldığı süre adlî para cezasından çevrilen hapis cezasını karşılamadığı takdirde infazı gereken bakiye, hapis cezasına eklenir. Bulunan ceza miktarı yabancı devlete bildirilir ve kabul edilmesi hâlinde nakle karar verilebilir.

(5) Nakil talebinin kabul edilebilmesi için yargılama giderlerinin ödenmiş olması gerekir. Ancak, hükümlünün yargılama giderlerini ödeyebilecek durumda olmadığına anlaşılması hâlinde, yargılama giderleri ödenmeden de nakle karar verilebilir.

(6) Hükümlünün nakline karar verilebilmesi için naklin yapılacağı devletten hükümlünün ceza infaz kurumunda kalacağı süre ve infazın nasıl yapılacağına bildirilmesi istenir. Bu bilgi hükümlüye tebliğ edilir.

(7) Yabancı devletin muvafakat vermesi üzerine hükümlünün nakline Adalet Bakanı karar verir.

Yabancı devlette infazın sonuçları

MADDE 33- (1) Merkezî Makam yabancı devletten infaz sırasında ortaya çıkacak özel durumlar ile infazın tamamlanması ve hükümlünün firarına ilişkin bilgileri bildirmesini ister. Merkezî Makama ulaşan bilgiler, kararı veren mahkemeye bildirilir.

(2) Kararın yabancı devlet tarafından tamamen infaz edilmesi veya infaz kabiliyetini kısmen veya tamamen kaybetmesi, Türk hukuku bakımından da aynı sonuçları doğurur.

(3) Yabancı devletin kararı infaz edememesi hâlinde infaz işlemlerine Türkiye'de devam edilir.

YEDİNCİ BÖLÜM

Çeşitli ve Son Hükümler

Masraflar

MADDE 34- (1) Bu Kanun uyarınca yapılan adli iş birliği taleplerinin yerine getirilmesine ilişkin giderler, merkezî makamların aksine bir mutabakatı bulunmaması hâlinde, yerine getiren devlet tarafından karşılanır.

(2) Soruşturma veya kovuşturmanın sonuçlandırılması amacıyla iade talebinde bulunulması hâlinde, talebin yerine getirilmesi için yapılan masraflar, yargılama giderlerinden sayılır. Mahkûmiyet kararlarının infazı amacıyla iade talebinde bulunulması hâlinde, talebin yerine getirilmesi için yapılan masrafların, ödendiği tarihten tahsil edildiği tarihe kadar geçen süreye 21/7/1953 tarihli ve 6183 sayılı Amme Alacaklarının Tahsil Usulü Hakkında Kanununun 51 inci maddesinde belirtilen gecikme zammı oranında hesaplanacak faiz ile birlikte bir ay içinde ödenmesi gerektiği, iade talep eden Cumhuriyet başsavcılığı tarafından hükümlüye bildirilir. Bu süre içinde ödeme yapılmaması hâlinde, bu alacaklar Amme Alacaklarının Tahsil Usulü Hakkında Kanun hükümlerine göre takip ve tahsil edilmek üzere Cumhuriyet başsavcılığınca ilgili vergi dairesine bildirilir.

(3) Hükümlünün bulunduğu devletten Türkiye'ye nakli için gerekli masraflar, hükümlü tarafından karşılanır. Söz konusu masraflar, hükümlü veya onun adına herhangi bir kişi tarafından Adalet Bakanlığınca bu maksatla açılan bir hesaba yatırılır. Hükümlünün nakil masraflarını karşılayacak durumda olmadığı tespit edilmesi hâlinde, mahkûm olunan suçun niteliği, naklin kamusal yararı, kişinin bulunduğu devletteki cezaevi koşulları, infazı gereken bakiye cezanın süresi gibi hususlar göz önüne alınarak, nakil masrafları, Adalet Bakanlığı bütçesine konulan ödenekten karşılanabilir. Nakil masraflarından görevlilere ilişkin olanların hesabı, 10/2/1954 tarihli ve 6245 sayılı Harcırah Kanunu hükümlerine göre yapılır.

Yönetmelik

MADDE 35- (1) Bu Kanunun uygulanmasına ilişkin yönetmelikler Adalet Bakanlığı tarafından yürürlüğe konulur.

Yürürlükten kaldırılan mevzuat

MADDE 36- (1) Bu Kanunun yürürlüğe girdiği tarih itibarıyla;

a) 1/3/1977 tarihli ve 2080 sayılı Ceza Kovuşturmalarının Aktarılmasına Dair Avrupa Sözleşmesi'nin Onaylanması ve Uygulanması Hakkında Kanununun 3 üncü maddesi,

b) 1/3/1977 tarihli ve 2081 sayılı Ceza Yargılarının Milletlerarası Değeri Konusunda Avrupa Sözleşmesinin Onaylanması ve Uygulanması Hakkında Kanununun 4 üncü maddesinin birinci ve üçüncü fıkraları ile 5 inci maddesi,

c) 8/5/1984 tarihli ve 3002 sayılı Türk Vatandaşları Hakkında Yabancı Ülke Mahkemelerinden ve Yabancılar Hakkında Türk Mahkemelerinden Verilen Ceza Mahkumiyetlerinin İnfazına Dair Kanun,
ç) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 18 inci maddesi,
yürürlükten kaldırılmıştır.

Yürürlük

MADDE 37- (1) Bu Kanun yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 38- (1) Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

6701 sayılı Türkiye İnsan Hakları ve Eşitlik Kurumu Kanunu

Resmî Gazete Tarihi : 20.04.2016

Resmî Gazete Sayısı : 29690

TÜRKİYE İNSAN HAKLARI VE EŞİTLİK KURUMU KANUNU

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç ve kapsam

MADDE 1- (1) Bu Kanunun amacı; insan onurunu temel alarak insan haklarının korunması ve geliştirilmesi, kişilerin eşit muamele görme hakkının güvence altına alınması, hukuken tanınmış hak ve hürriyetlerden yararlanmada ayrımcılığın önlenmesi ile bu ilkeler doğrultusunda faaliyet göstermek, işkence ve kötü muameleyle etkin mücadele etmek ve bu konuda ulusal önleme mekanizması görevini yerine getirmek üzere Türkiye İnsan Hakları ve Eşitlik Kurumunun kurulması, teşkilat, görev ve yetkilerine ilişkin esasların düzenlenmesidir.

Tanımlar

MADDE 2- (1) Bu Kanunun uygulanmasında;

- a) Ayrı tutma: Kişilerin bu Kanunda sayılan temellerden biri veya birden fazlası nedeniyle, bir eylem veya eylemsizliğin sonucu olarak diğerlerinden ayrı tutulması durumunu,
- b) Ayrımcılık talimatı: Bir kişinin kendi nam veya hesabına eylem ve işlemlerde bulunmaya yetkili kıldığı kişilere veya bir kamu görevlisinin diğer kişilere verdiği ayrımcılık yapılmasına yönelik talimatı,
- c) Başkan: Türkiye İnsan Hakları ve Eşitlik Kurumu Başkanı,
- ç) Çoklu ayrımcılık: Ayrımcı uygulamanın birden fazla ayrımcılık temeli ile ilişkili olması durumunu,
- d) Doğrudan ayrımcılık: Bir gerçek veya tüzel kişinin, hukuken tanınmış hak ve hürriyetlerden karşılaştırılabilir durumdakilere kıyasla eşit şekilde yararlanmasını bu Kanunda sayılan ayrımcılık temellerine dayanılarak engelleyen veya zorlaştıran her türlü farklı muameleyi,

- e) Dolaylı ayrımcılık: Bir gerçek veya tüzel kişinin, görünüşte ayrımcı olmayan her türlü eylem, işlem ve uygulamalar sonucunda, bu Kanunda sayılan ayrımcılık temelleriyle bağlantılı olarak, hukuken tanınmış hak ve hürriyetlerden yararlanma bakımından nesnel olarak haklılaştırılmayan dezavantajlı bir konuma sokulmasını,
- f) Engelli: Fiziksel, zihinsel, ruhsal ve duyuşsal yetilerinde çeşitli düzeyde kayıplarından dolayı topluma diğer bireyler ile birlikte eşit şartlarda tam ve etkin katılımını kısıtlayan tutum ve çevre şartlarından etkilenen bireyi,
- g) İşyerinde yıldırma: Bu Kanunda sayılan ayrımcılık temellerine dayanılarak kişiyi işinden soğutmak, dışlamak, bıktırmak amacıyla kasıtlı olarak yapılan eylemleri,
- ğ) Kamu görevlisi: Kamu hizmetlerinin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli, süreli veya geçici olarak katılan kişiyi,
- h) Kurul: Türkiye İnsan Hakları ve Eşitlik Kurulunu,
- ı) Kurum: Türkiye İnsan Hakları ve Eşitlik Kurumunu,
- i) Makul düzenleme: Engellilerin hak ve özgürlüklerini tam ve diğer bireylerle eşit şekilde kullanmasını veya bunlardan yararlanmasını sağlamak üzere belirli bir durumda ihtiyaç duyulan, mali imkânlar nispetinde, ölçülü, gerekli ve uygun değişiklik ve tedbirleri,
- j) Taciz: Psikolojik ve cinsel türleri de dâhil olmak üzere bu Kanunda sayılan temellerden birisine dayanılarak, insan onurunun çiğnenmesi amacını taşıyan veya böyle bir sonucu doğuran yıldırıcı, onur kırıcı, aşağılayıcı veya utandırıcı her türlü davranışı,
- k) Ulusal önleme mekanizması: İşkenceye ve Diğer Zalimane, Gayriinsanî veya Küçültücü Muamele veya Cezaya Karşı Birleşmiş Milletler Sözleşmesine Ek İhtiyari Protokol hükümleri çerçevesinde kişilerin özgürlüklerinden yoksun bırakıldığı yerlere düzenli ziyaretler yapmak üzere oluşturulan sistemi,
- l) Uygulamalı iş deneyimi: Bir mesleğin gerektirdiği bilgi, beceri ve iş alışkanlıklarının eğitimle eş zamanlı ya da eğitim sonrası dönemde iş içerisinde geliştirilmesini,
- m) Varsayılan temele dayalı ayrımcılık: Bir gerçek veya tüzel kişinin, bu Kanunda sayılan ayrımcılık temellerinden birisiyle gerçekte ilgisi olmamasına rağmen, bu temellerden birisini taşıdığı sanılarak hukuken tanınmış hak ve hürriyetlerden yararlanma bakımından ayrımcı muameleyle maruz kalmasını,
- ifade eder.

İKİNCİ BÖLÜM

Ayrımcılıkla Mücadele

Eşitlik ilkesi ve ayrımcılık yasağı

MADDE 3- (1) Herkes, hukuken tanınmış hak ve hürriyetlerden yararlanmada eşittir.

(2) Bu Kanun kapsamında cinsiyet, ırk, renk, dil, din, inanç, mezhep, felsefi ve siyasi görüş, etnik köken, servet, doğum, medeni hâl, sağlık durumu, engellilik ve yaş temellerine dayalı ayrımcılık yasaktır.

(3) Ayrımcılık yasağının ihlali hâlinde, konuya ilişkin görev ve yetkisi bulunan kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları ihlalin sona erdirilmesi, sonuçlarının giderilmesi, tekrarlanmasının önlenmesi, adli ve idari yoldan takibinin sağlanması amacıyla gerekli tedbirleri almakla yükümlüdür.

(4) Ayrımcılık yasağı bakımından sorumluluk altında olan gerçek ve özel hukuk tüzel kişileri, yetki alanları içerisinde bulunan konular bakımından ayrımcılığın tespiti, ortadan kaldırılması ve eşitliğin sağlanması için gerekli tedbirleri almakla yükümlüdür.

Ayrımcılık türleri

MADDE 4- (1) Bu Kanun kapsamına giren ayrımcılık türleri şunlardır:

- a) Ayrı tutma.
- b) Ayrımcılık talimatı verme ve bu talimatları uygulama.
- c) Çoklu ayrımcılık.
- ç) Doğrudan ayrımcılık.
- d) Dolaylı ayrımcılık.
- e) İşyerinde yıldırma.
- f) Makul düzenleme yapmama.
- g) Taciz.
- ğ) Varsayılan temele dayalı ayrımcılık.

(2) Eşit muamele ilkesine uyulması veya ayrımcılığın önlenmesi amacıyla idari ya da adli süreçleri başlatan yahut bu süreçlere katılan kişiler ile bunların temsilcilerinin, bu nedenle maruz kaldıkları olumsuz muameleler de ayrımcılık teşkil eder.

Ayrımcılık yasağının kapsamı

MADDE 5- (1) Eğitim ve öğretim, yargı, kolluk, sağlık, ulaşım, iletişim, sosyal güvenlik, sosyal hizmetler, sosyal yardım, spor, konaklama, kültür, turizm ve benzeri hizmetleri sunan kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, gerçek kişiler ve özel hukuk tüzel kişileri, yürüttükleri faaliyetler bakımından bu hizmetlerden yararlanmakta olan veya yararlanmak üzere başvurmuş olan ya da bu hizmetler hakkında bilgi almak isteyen kişi aleyhine ayrımcılık yapamaz. Bu hüküm kamuya açık hizmetlerin sunulduğu alanlar ve binalara erişimi de kapsar.

(2) Birinci fıkrada belirtilen hizmetlerin planlanması, sunulması ve denetlenmesinden sorumlu olan kişi ve kurumlar, farklı engelli grupların ihtiyaçlarını dikkate almakla ve makul düzenlemelerin yapılmasını sağlamakla yükümlüdür.

(3) Kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, gerçek kişiler, özel hukuk tüzel kişileri ve bunlar tarafından yetkilendirilenler, taşınır ve taşınmazları kamuya açık bir şekilde sunarken bu malları edinmek veya kiralamak isteyenler ile bunlar hakkında bilgi almak isteyenler aleyhine, bunların kiralanması, kira akdinin şartlarının belirlenmesi, kira akdinin yenilenmesi veya sona erdirilmesi, satışı ve devri süreçlerinin hiçbirinde ayrımcılık yapamaz.

(4) Dernek, vakıf, sendika, siyasi parti ve meslek örgütlerine, ilgili mevzuatlarında veya tüzüklerinde belirtilen istisnalar dışında üye olma, organlarına seçilme, üyelik imkânlarından yararlanma, üyeliğin sonlandırılması ve bunların faaliyetlerine katılma ve yararlanma bakımından, hiç kimse aleyhine ayrımcılık yapılamaz.

İstihdam ve serbest meslek

MADDE 6- (1) İşveren veya işveren tarafından yetkilendirilmiş kişi; işverenin çalışanı veya bu amaçla başvuran kişi, uygulamalı iş deneyimi edinmek üzere bir işyerinde bulunan veya bu amaçla başvuran kişi ve herhangi bir sıfatla çalışmak ya da uygulamalı iş deneyimi edinmek üzere işyeri veya iş ile ilgili olarak bilgi edinmek isteyen kişi aleyhine, bilgilenme, başvuru, seçim kriterleri, işe alım şartları ile çalışma ve çalışmanın sona ermesi süreçleri dâhil olmak üzere, işle ilgili süreçlerin hiçbirinde ayrımcılık yapamaz.

(2) Birinci fıkra iş ilanı, işyeri, çalışma şartları, mesleki rehberlik, mesleki eğitim ve yeniden eğitimin tüm düzeylerine ve türlerine erişim, meslekte yükselme ve mesleki hiyerarşinin tüm düzeylerine erişim, hizmet içi eğitim, sosyal menfaatler ve benzeri hususları da kapsar.

(3) İşveren veya işveren tarafından yetkilendirilmiş kişi, istihdam başvurusunu gebelik, annelik ve çocuk bakımı gerekçeleriyle reddedemez.

(4) Serbest mesleğe kabul, ruhsat, kayıt, disiplin ve benzeri hususlar bakımından ayrımcılık yapılamaz.

(5) 22/5/2003 tarihli ve 4857 sayılı İş Kanunu kapsamına girmeyen her türlü iş ve iş görme sözleşmeleri de bu madde kapsamındadır.

(6) Kamu kurum ve kuruluşlarında istihdam bu madde hükümlerine tabidir.

Ayrımcılık iddiasının ileri sürülemeyeceği hâller

MADDE 7- (1) Bu Kanun kapsamında ayrımcılık iddiasının ileri sürülemeyeceği hâller ve istisnalar şunlardır:

a) İstihdam ve serbest meslek alanlarında, zorunlu mesleki gerekliliklerin varlığı hâlinde amaca uygun ve orantılı olan farklı muamele.

b) Sadece belli bir cinsiyetin istihdamını zorunlu kılan durumlar.

c) İşe kabul ve istihdam sürecinde, hizmetin zorunlulukları nedeniyle yaş sınırlarının belirlenmesi ve uygulanması, gereklilik ve amaçla orantılı olması şartıyla yaşa dayalı farklı muamele.

ç) Çocuk veya özel bir yerde tutulması gereken kişilere yönelik özel tedbirler ve koruma önlemleri.

d) Bir dine ait kurumda, din hizmeti veya o dine ilişkin eğitim ve öğretim vermek üzere sadece o dine mensup kişilerin istihdamı.

e) Dernek, vakıf, sendika, siyasi parti ve meslek örgütlerinin, ilgili mevzuatlarında veya tüzüklerinde yer alan amaç, ilke ve değerler temelinde üye olacak kişilerde belli şart ve nitelik aramaları.

f) Eşitsizlikleri ortadan kaldırmaya yönelik, gerekli, amaca uygun ve orantılı farklı muamele.

g) Vatandaş olmayanların ülkeye giriş ve ikametlerine ilişkin şartlarından ve hukuki statülerinden kaynaklanan farklı muamele.

ÜÇÜNCÜ BÖLÜM

Kuruluş, Teşkilat Yapısı ve Görevler

Türkiye İnsan Hakları ve Eşitlik Kurumu

MADDE 8- (1) (Değişik: 2/7/2018 - KHK/703/149 md.) Bu Kanunla ve diğer mevzuatla verilen görevleri yerine getirmek ve yetkileri kullanmak üzere, idari ve mali özerkliğe sahip, özel bütçeli ve kamu tüzel kişiliğini haiz, Cumhurbaşkanının görevlendireceği bakan ile ilişkili Türkiye İnsan Hakları ve Eşitlik Kurumu kurulmuştur. Cumhurbaşkanı bu teşkilatın yönetimi ile ilgili yetkilerini gerekli gördüğü hallerde bakan vasıtasıyla kullanabilir.

(2) Kurum, Kurul ve Başkanlıktan oluşur.

Kurumun görevleri

MADDE 9- (1) Kurumun görevleri şunlardır:

- a) İnsan haklarının korunmasına, geliştirilmesine, ayrımcılığın önlenmesine ve ihlallerin giderilmesine yönelik çalışmalar yapmak.
- b) İnsan hakları ve ayrımcılıkla mücadele konularında kitle iletişim araçlarını da kullanarak bilgilendirme ve eğitim yoluyla kamuoyunda duyarlılığı geliştirmek.
- c) Millî eğitim müfredatında bulunan insan hakları ve ayrımcılık yasağıyla ilgili bölümlerin hazırlanmasına katkıda bulunmak.
- ç) İnsan haklarının korunması, ayrımcılığın ortadan kaldırılması ve toplumdaki eşitlik anlayışının geliştirilmesine yönelik olarak üniversiteler ile ortaklaşa faaliyetlerde bulunmak, Yükseköğretim Kurulunun eşgüdümünde üniversitelerin insan hakları ve eşitlik ile ilgili bölümlerinin kurulmasına ve insan hakları ve eşitlik öğretimine dair müfredatın belirlenmesine katkıda bulunmak.
- d) Kamu kurum ve kuruluşlarının meslek öncesi ve meslek içi insan hakları ve eşitlik eğitimi programlarının esaslarının belirlenmesine ve bu programların yürütülmesine katkıda bulunmak.
- e) Görev alanıyla ilgili mevzuat çalışmalarını izlemek, değerlendirmek, bunlara ilişkin görüş ve önerilerini ilgili mercilere bildirmek.
- f) İnsan hakları ihlallerini resen incelemek, araştırmak, karara bağlamak ve sonuçlarını takip etmek.
- g) Ayrımcılık yasağı ihlallerini resen veya başvuru üzerine incelemek, araştırmak, karara bağlamak ve sonuçlarını takip etmek.
- ğ) Ayrımcılık yasağı ihlalleri nedeniyle mağdur olduğu iddiasıyla Kuruma başvuranlara mağduriyetlerinin giderilmesi için kullanabilecekleri idari ve hukuki süreçler konusunda yol göstermek ve başvurularını takip etmelerini sağlamak amacıyla yardımcı olmak.
- h) İşkence ve kötü muamele ile mücadele etmek ve bu konuda çalışmalar yapmak.
- ı) İşkenceye ve Diğer Zalimane, Gayriinsanî veya Küçültücü Muamele veya Cezaya Karşı Birleşmiş Milletler Sözleşmesine Ek İhtiyari Protokol hükümleri çerçevesinde ulusal önleme mekanizması olarak görev yapmak.
- i) Özgürlüğünden mahrum bırakılan ya da koruma altına alınan kişilerin ulusal önleme mekanizması kapsamındaki başvurularını incelemek, araştırmak, karara bağlamak ve sonuçlarını takip etmek.

j) Özgürlüğünden mahrum bırakılan ya da koruma altına alınan kişilerin buldukları yerlere haberli veya habersiz düzenli ziyaretler gerçekleştirmek, bu ziyaretlere ilişkin raporları ilgili kurum ve kuruluşlara iletme, Kurulca gerekli görülmesi durumunda kamuoyuna açıklamak, ceza infaz kurumları ve tutukevleri izleme kurulları, il ve ilçe insan hakları kurulları ile diğer kişi, kurum ve kuruluşların bu gibi yerlere gerçekleştirdikleri ziyaretlere ilişkin raporları incelemek ve değerlendirmek.

k) Cumhurbaşkanlığına, ve Türkiye Büyük Millet Meclisi Başkanlığına sunulmak üzere, insan haklarının korunması ve geliştirilmesi, işkence ve kötü muameleyle mücadele ve ayrımcılıkla mücadele alanlarında yıllık raporlar hazırlamak.

l) Kamuoyunu bilgilendirmek, düzenli yıllık raporlar dışında, gerek görüldüğünde görev alanına ilişkin özel raporlar yayımlamak.

m) İnsan hakları ve ayrımcılıkla mücadele alanındaki uluslararası gelişmeleri izlemek ve değerlendirmek, alanındaki uluslararası kuruluşlarla ilgili mevzuat dâhilinde işbirliği yapmak.

n) İnsan haklarının korunması ve ayrımcılıkla mücadele kapsamında faaliyet yürüten kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek kuruluşları ve üniversitelerle işbirliği yapmak.

o) Diğer kurumların ayrımcılığın önlenmesine yönelik faaliyetlerine destek vermek.

ö) Türkiye'nin taraf olduğu uluslararası insan hakları sözleşmelerinin uygulanmasını izlemek, bu sözleşmeler uyarınca kurulan inceleme, izleme ve denetleme mekanizmalarına Devletin sunmakla yükümlü olduğu raporların hazırlanması sürecinde, ilgili sivil toplum kuruluşlarından da yararlanmak suretiyle görüş bildirmek, bu raporların sunulacağı uluslararası toplantılara temsilci göndererek katılmak.

p) Kanunlarla verilen diğer görevleri yapmak.

(2) Kamu kurum ve kuruluşları ile görevliler, birinci fıkranın (j) bendi kapsamındaki ziyaretler sebebiyle gerekli yardım ve kolaylığı göstermek zorundadır.

(3) Kurum, görev ve yetkilerine ilişkin olarak Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonunu ve Kadın Erkek Fırsat Eşitliği Komisyonunu yılda en az bir defa bilgilendirir.

Kurul

MADDE 10- (1) Kurul, Kurumun karar organıdır. Kurul, bu Kanunla ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getirir ve kullanır. Görev

alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişi, Kurula emir ve talimat veremez, tavsiye ve telkinde bulunamaz.

(2) (Değişik: 2/7/2018 - KHK/703/149 md.) Kurul; biri Başkan, biri İkinci Başkan olmak üzere Cumhurbaşkanlığı tarafından atanan on bir üyeden oluşur.

(3) İkinci fıkraya göre Cumhurbaşkanlığına seçilen üyelerin görev süreleri dolmadan iki ay önce durum, Kurum tarafından uygun iletişim araçlarıyla kamuoyuna duyurulur. Başvurular ve aday bildirimleri Cumhurbaşkanlığına yapılır. İkinci fıkrada belirtilen usule göre yeni seçilen üyeler, yerlerine seçildikleri üyenin görev süresinin bitiminden itibaren göreve başlar.

(4) Kurula üye olabilmek için aşağıdaki şartlar aranır:

a) (Mülga: 2/7/2018 - KHK/703/149 md.)

b) 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanununun 48 inci maddesinin birinci fıkrasının (A) bendinin (1), (4), (5), (6) ve (7) numaralı alt bentlerinde belirtilen nitelikleri taşımak.

c) Herhangi bir siyasi partinin yönetim ve denetim organlarında görevli veya yetkili bulunmamak.

ç) En az dört yıllık lisans düzeyinde yükseköğrenim görmüş olmak.

d) (Mülga: 2/7/2018 - KHK/703/149 md.)

(5) (Mülga: 2/7/2018 - KHK/703/149 md.)

(6) (Mülga birinci ve ikinci cümleler: 2/7/2018 - KHK/703/149 md.) Üyeliklerde görev süresi dolmadan herhangi bir sebeple boşalma olması hâlinde, bir ay içinde aynı usulle yeni üye seçilir. Bu şekilde seçilen üye, yerine seçildiği üyenin kalan süresini tamamlar ve bunlardan iki yıl veya daha az süreyle görev yapanların bu görevleri seçilme dönemi olarak değerlendirilmez.

(7) (Mülga: 2/7/2018 - KHK/703/149 md.)

(8) Başkan, İkinci Başkan ve üyelerin süreleri dolmadan herhangi bir nedenle görevlerine son verilemez. Ancak üyenin;

a) Seçilmesi için gerekli şartları taşıyamaması ya da sonradan kaybetmesi,

b) Kurul kararlarını süresi içinde imzalamaması,

c) Kurul tarafından kabul edilebilir mazereti olmaksızın bir takvim yılı içinde toplam beş Kurul toplantısına katılmaması,

ç) Ağır hastalık veya engellilik nedeniyle iş göremeyeceğinin sağlık kurulu raporuyla belgelenmesi,

d) Görevi ile ilgili olarak işlediği suçlardan dolayı hakkında verilen mahkûmiyet kararının kesinleşmesi,

e) Geçici iş göremezlik hâlinin üç aydan fazla sürmesi,

f) 657 sayılı Kanununun 48 inci maddesinin birinci fıkrasının (A) bendinin (5) numaralı alt bendinde belirtilen suçlardan mahkûm edilip de cezasının infazına fiilen başlanması,

hâllerinin Kurul tarafından tespit edilmesi üzerine Cumhurbaşkanı veya görevlendireceği bakanın onayıyla üyeliğine son verilir.(2)

(9) Üyelerin Kurulda görev yaptıkları sürece önceki görevleri ile olan ilişkileri kesilir. Üyeler, özel bir kanuna dayanmadıkça, Kuruldaki görevlerinin dışında resmî veya özel hiçbir görev alamaz, dernek, vakıf, kooperatif ve benzeri yerlerde yöneticilik ve denetçilik yapamaz, ticaretle uğraşamaz, serbest meslek faaliyetinde bulunamaz, hakemlik ve bilirkişilik yapamaz. Ancak üyeler, asli görevlerini aksatmayacak şekilde bilimsel amaçlı yayın yapabilir, ders ve konferans verebilir ve bunlardan doğacak telif hakları ile ders ve konferans ücretlerini alabilir.

(10) Kamu görevlisi iken üyeliğe seçilenler, memuriyete giriş şartlarını kaybetmemeleri kaydıyla, görev sürelerinin sona ermesi veya görevden ayrılma isteğinde bulunmaları ve otuz gün içinde önceki kurum veya kuruluşlarına başvurmaları durumunda atamaya yetkili makam tarafından bir ay içinde mükteseplerine uygun bir kadroya atanır. Atama gerçekleşinceye kadar, bunların almakta oldukları her türlü ödemelerin Kurum tarafından yapılmasına devam olunur. Bunların Kurumda geçirdiği süreler, özlük ve diğer hakları açısından önceki kurum veya kuruluşlarında geçirilmiş sayılır. Bir kamu kurumunda çalışmayanlardan üyeliğe seçilip yukarıda belirtilen şekilde görevi sona erenlere herhangi bir görev veya işe başlayıncaya kadar, almakta oldukları her türlü ödemeler Kurum tarafından ödenmeye devam edilir ve bu şekilde üyeliği sona erenlere Kurum tarafından yapılacak ödeme üç ayı geçemez.

(11) Başkan ve üyeler, 19/4/1990 tarihli ve 3628 sayılı Mal Bildiriminde Bulunulması, Rüşvet ve Yolsuzluklarla Mücadele Kanununa tabidir.

(12) Seçilen üyeler ilk toplantının başında aşağıdaki şekilde yemin ederler:

“Görevimi tam bir tarafsızlık, dürüstlük, hakkaniyet ve adalet anlayışı içinde yerine getireceğime, namusum ve şerefim üzerine yemin ederim.”

(13) 2/12/1999 tarihli ve 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun uyarınca Başkan ve üyeler için soruşturma yapılması Cumhurbaşkanı veya görevlendireceği

bakanın iznine tabidir. Soruşturma izni verilmesi veya verilmemesine ilişkin kararlara karşı itirazlar Danıştay tarafından karara bağlanır.

(14) Başkan ve üyeler ile Kurum personeli, görevlerini yerine getirmeleri sırasında edindikleri, kamuya, ilgililere ve üçüncü kişilere ait gizlilik taşıyan bilgileri, kişisel verileri, Kurumla ilgili gizlilik taşıyan bilgileri, ticari sırları ve bunlara ait belgeleri, bu konuda kanunen yetkili kılınan mercilerden başkasına açıklayamaz, kendilerinin veya üçüncü kişilerin yararına kullanamaz. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

Kurulun görev ve yetkileri

MADDE 11- (1) Kurulun görev ve yetkileri şunlardır:

- a) Kurumla ve Kurumun görev alanıyla ilgili düzenlemeler yapılmasına yönelik kararlar almak.
- b) Ayrımcılık yasağı ihlallerine ilişkin başvurular ile insan hakları veya ayrımcılık yasağı ihlallerine ilişkin resen yapılan incelemeleri karara bağlamak, bu başvuru ve incelemelere ilişkin gerekli hâllerde uzlaşma sürecini sonuçlandırmak, ayrımcılık yasağı ihlallerine ilişkin bu Kanunda öngörülen idari yaptırımlara karar vermek.
- c) İnsan hakları ve ayrımcılık yasağı ihlallerine ilişkin yargı kararlarının uygulanmasına ilişkin sorunları izlemek ve değerlendirmek.
- ç) Özgürlüğünden mahrum bırakılan ya da koruma altına alınan kişilerin ulusal önleme mekanizması kapsamındaki başvurularını ve bu kapsamda resen yürütülen incelemeleri karara bağlamak.
- d) Görev alanıyla ilgili olarak yargı organlarına, kamu kurum ve kuruluşlarına ve ilgili kişilere talepleri hâlinde görüş bildirmek.
- e) Gerek gördüğünde Kurumun kendi alanında çalışan uluslararası kuruluşlara üye olmasına ve bu kuruluşlarla işbirliği yapmasına karar vermek.
- f) Kurum tarafından insan haklarının korunması, ayrımcılıkla mücadele ve ulusal önleme mekanizması görevleri kapsamında yapılan inceleme ve araştırmaları, hazırlanan raporları ve benzeri çalışmaları karara bağlamak.
- g) Kurumun stratejik planını karara bağlamak, amaç ve hedeflerini, hizmet kalite standartlarını ve performans ölçütlerini belirlemek.
- ğ) Kurumun stratejik planı ile amaç ve hedeflerine uygun olarak hazırlanan bütçe teklifini görüşmek ve karara bağlamak.

h) Kurumun faaliyet raporlarını karara bağlamak.

i) Taşınmaz alımı, satımı ve kiralanması konularındaki önerileri görüşüp karara bağlamak.

i) Kanunlarla verilen diğer görevleri yapmak.

Kurulun çalışma esasları

MADDE 12- (1) Kurul, Başkanın çağrısı üzerine toplanır. Toplantıları Başkan yönetir. Başkanın dışında en az beş üyenin birlikte talep etmesi hâlinde, Kurul, Başkan tarafından beş gün içinde toplanmak üzere derhâl toplantıya çağrılır.

(2) Toplantı gündemi Başkan tarafından hazırlanarak, toplantıdan en az üç gün önce Kurul üyelerine bildirilir. Gündeme yeni madde eklenebilmesi için toplantıda üyelere birinin öneride bulunması ve önerilen maddenin Kurul tarafından kabul edilmesi gerekir.

(3) Kurul, en az yedi üye ile toplanır ve en az altı üyenin aynı yöndeki oyuyla karar alır. Kararlarda çekimser oy kullanılamaz.

(4) Kurul, kendi üyeleri arasından, her bir çalışma alanı için üçer üyeli komisyonlar oluşturabilir.

(5) Kurul, başvuruları görüşmek ve sonuçlandırmak üzere Başkan hariç beş üyeli daireler oluşturabilir. Başkan, dairelerin doğal üyesidir.

(6) Kurul kararları tutanakla tespit edilir ve karar tutanağı toplantı esnasında veya en geç toplantıyı izleyen beş iş günü içinde toplantıya katılan tüm üyeler tarafından imzalanarak tekemmül ettirilir. Toplantı tarihinden itibaren en geç on beş iş günü içinde gerekçeler ve varsa karşı oy gerekçeleri yazılır. Gerekliğinde, Kurul tarafından bu süre uzatılabilir.

(7) Başkan ve üyeler; kendileri, aralarındaki evlilik bağı kalkmış olsa bile eşleri, evlatlıkları ve üçüncü derece dâhil üçüncü dereceye kadar kan ve ikinci derece dâhil ikinci dereceye kadar kayın hısımlarıyla ilgili veya kişisel menfaat ilişkisi içinde oldukları konularda toplantı ve oylamaya katılamaz. Bu durum karar metninde ayrıca belirtilir.

(8) Aksi kararlaştırılmadıkça Kurul toplantılarındaki müzakereler gizlidir.

(9) İhtiyaç duyulması hâlinde görüşlerinden yararlanılmak üzere ilgililer Kurul toplantısına davet edilebilir. Ancak, Kurul kararları toplantıya dışarıdan katılanların yanında alınamaz.

(10) Kurul kararları, tekemmül etmesinden itibaren en geç beş iş günü içinde ilgililere gönderilir. Kurul kararlarında, ilgili kişilerin bu kararlara karşı hangi hukuki yollara başvurabilecekleri süreleri ile birlikte belirtilir.

(11) Kurul, gerekli gördüğü durumlarda kararlarını, kişisel verilerin gizliliği ilkesine bağlı kalmak kaydıyla uygun vasıtalarla kamuoyuna duyurabilir.

(12) Kurul üyeleri ile Kurum personelinin uyacakları mesleki ve etik ilkeler, bu maddede belirtilen komisyonların ve dairelerin oluşumu, çalışma esasları ile Kurulun çalışma usul ve esasları ve diğer hususlar yönetmelikle düzenlenir.

Başkan

MADDE 13- (1) Başkan, Kurumun en üst amiri olup, Kurum hizmetlerini mevzuata, Kurumun amaç ve politikalarına, stratejik planına, performans ölçütlerine ve hizmet kalite standartlarına uygun olarak düzenler, yürütür ve hizmet birimleri arasında eşgüdümü sağlar. Başkan, Kurumun genel yönetim ve temsilinden sorumludur.

(2) Başkanın görev ve yetkileri şunlardır:

- a) Kurul toplantılarının gündemini, gün ve saatini belirlemek ve toplantıları yönetmek.
- b) Kurul kararlarının tebliğini ve Kurulca gerekli görülenlerin kamuoyuna duyurulmasını sağlamak.
- c) Hizmet birimi koordinatörlerini görevlendirmek ve diğer Kurum personelini atamak.
- ç) Hizmet birimlerinden gelen önerilere son şeklini vererek Kurula sunmak.
- d) Kurumun stratejik planını, performans ölçütlerini hazırlamak, amaç ve hedeflerini, hizmet kalite standartlarını, insan kaynakları ve çalışma politikalarını oluşturmak.
- e) Belirlenen stratejilere, yıllık amaç ve hedeflere uygun olarak Kurumun yıllık bütçesi ile mali tablolarını hazırlamak.
- f) Yıllık faaliyet raporlarını hazırlamak, yıllık amaç ve hedeflere, performans ölçütlerine göre faaliyetlerin değerlendirmesini yapmak ve bunları Kurula sunmak.
- g) Kurul ve hizmet birimlerinin uyumlu, verimli, disiplinli ve düzenli bir biçimde çalışması amacıyla eşgüdümü sağlamak.
- ğ) Kurumun yönetim ve işleyişine ilişkin diğer görevleri yerine getirmek.

(3) Başkanın yokluğunda İkinci Başkan, Başkana vekâlet eder.

Başkanlık

MADDE 14- (1) Başkanlık, Başkan Yardımcıları, hizmet birimleri ve çalışma gruplarından oluşur. Hizmet birimlerinin sayısı onu geçemez. Başkanlık, Kurul kararlarını uygulamakla ve diğer konularda Başkana ve Kurula yardımcı olmakla görevlidir.

(2) Kurul Başkanı, Kurumun da başkanıdır.

(3) Hizmet birimleri, Başkan tarafından belirlenen koordinatörlerin eşgüdümünde faaliyet gösterir.

(4) Kurum, görev alanına giren konularla ilgili olarak çalışmalarda bulunmak üzere kamu kurum ve kuruluşları, sivil toplum kuruluşları ve konuyla ilgili uzmanların katılımı ile altı ay süreli geçici komisyonlar oluşturabilir. Başkan, bu süreyi üç aya kadar uzatabilir. Gerekli görülmesi hâlinde Kurul, altı aylık süreyi iki katına kadar uzatabilir. Ayda ikiyi geçmemek kaydıyla komisyonların toplantılarına ilişkin giderler Kurum bütçesinden karşılanır.

(5) Gerek görülmesi hâlinde, Kurumun teklifi üzerine Cumhurbaşkanı kararıyla Kuruma bağlı bürolar kurulabilir.

(6) Hizmet birimleri ve büroların çalışma usul ve esasları, bu Kanunda belirtilen faaliyet alanı, görev ve yetkilerine uygun olarak Kurumun teklifi üzerine Cumhurbaşkanınca yürürlüğe konulan yönetmelikle belirlenir.

DÖRDÜNCÜ BÖLÜM

Personel Rejimi

Personele ve özlük haklarına ilişkin hükümler

MADDE 15- (1) Kurum personeli, bu Kanunla düzenlenen hususlar dışında 657 sayılı Kanuna tabidir. Hizmet birimi koordinatörü olarak görevlendirilenlerde bakanlık daire başkanı kadrolarına atanmak için aranan şartlar aranır ve bunlara kadrolarına bağlı olarak mali haklar kapsamında yapılan aylık net ödeme tutarının, bakanlık daire başkanına kadrosuna bağlı olarak yapılması öngörülen aylık net ödeme tutarından az olması hâlinde aradaki fark, herhangi bir vergi ve kesintiye tabi olmaksızın ödenir.

(2) Kurul Başkanına 27/6/1989 tarihli ve 375 sayılı Kanun Hükmünde Kararnameye ekli (II) sayılı cetvelin 3 üncü sırasında, Kurul üyelerine anılan cetvelin 4 üncü sırasında yer alan göstergeler üzerinden anılan Kanun Hükmünde Kararnamenin ek 10 uncu maddesinde öngörülen usul ve esaslar çerçevesinde ödeme yapılır. Söz konusu ödemelerden vergi ve diğer yasal kesintilere tabi olmayanlar bu fıkraya göre yapılacak ödemelerde de vergi ve diğer yasal kesintilere tabi tutulmaz. Başkan ve üyeler, 657 sayılı Kanun ve diğer ilgili mevzuat uyarınca Devlet memurlarının yararlandığı sosyal hak ve yardımlardan da aynı usul ve esaslar çerçevesinde yararlanır.

(3) Başkan ve üyeler ile Kurum personeli 31/5/2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 4 üncü maddesinin birinci fıkrasının (c) bendi hükümlerine tabidir.

Başkan ve üyeler ile başkan yardımcılarını emeklilik hakları bakımından sırasıyla Gelir İdaresi Başkanı, bakanlık genel müdürleri ve bakanlık genel müdür yardımcılarını ile denk kabul edilir. Bunlardan bu görevleri sırasında 5510 sayılı Kanunun geçici 4 üncü maddesi kapsamına girenlerin bu görevlerde geçen süreleri makam tazminatı ile temsil tazminatı ödenmesi gereken süre olarak değerlendirilir. 5510 sayılı Kanunun 4 üncü maddesinin birinci fıkrasının (c) bendi kapsamında sigortalı iken üyeliğe seçilenlerden bu görevleri sona erenler veya bu görevlerinden ayrılma isteğinde bulunanların bu görevlerde geçen hizmet süreleri kazanılmış hak aylık, derece ve kademelerinin tespitinde dikkate alınır. Kamu kurum ve kuruluşlarında 5510 sayılı Kanunun 4 üncü maddesinin birinci fıkrasının (a) bendi kapsamında sigortalı iken üyeliğe seçilenlerin, önceki kurum ve kuruluşları ile ilişkilerinin kesilmesi kendilerine kıdem tazminatı veya iş sonu tazminatı ödenmesini gerektirmez. Bu durumda olanların kıdem tazminatı veya iş sonu tazminatı ödenmesi gereken hizmet süreleri, üyelikte geçen hizmet süreleri ile birleştirilir ve emeklilik ikramiyesi ödenecek süre olarak değerlendirilir.

(4) Kurul tarafından, Kuruma ilişkin görevlerinde Başkana yardımcı olmak üzere, Kurumun görev alanları dikkate alınarak üç Başkan Yardımcısı atanır. Başkan Yardımcısı olarak atanacaklarda;

a) En az dört yıllık lisans düzeyinde yükseköğrenim görmüş olma,

b) Kamu hizmetinde en az on yıllık mesleki tecrübeye sahip olma,

c) 657 sayılı Kanunun 48 inci maddesinin birinci fıkrasının (A) bendinin (1), (4), (5), (6) ve (7) numaralı alt bentlerinde belirtilen nitelikleri taşıma,

şartları aranır. Başkan yardımcılarının görev süresi dört yıldır. Görevi sona eren başkan yardımcılarını yeniden atanabilir.

(5) Başkan, sınırlarını yazılı ve açık olarak belirlemek şartıyla Kurula ilişkin olmayan görev ve yetkilerinin bir bölümünü başkan yardımcılarını veya hizmet birimi koordinatörlerine devredebilir. Yetki devri, uygun araçlarla ilgililere duyurulur.

(6) Kurumda, 657 sayılı Kanun ve diğer mevzuat hükümlerine bağlı kalmaksızın, sözleşmeli personel istihdam edilebilir. Sözleşmeli olarak istihdam edilecek personel, 5510 sayılı Kanunun 4 üncü maddesinin birinci fıkrasının (a) bendi kapsamında sigortalı sayılır. Bu personelin atama usul ve esasları Kurumca belirlenir. Bunlara ödenecek ücretin net tutarı, birinci dereceli İnsan Hakları ve Eşitlik Uzmanına ödenen aylık ortalama net tutarı aşmamak üzere Başkan tarafından tespit edilir. Bu fıkra uyarınca çalıştırılacakların sayısı İnsan Hakları ve Eşitlik Uzmanı ve İnsan Hakları ve Eşitlik Uzman Yardımcısı toplam kadro sayısının yüzde on beşini geçemez. Bu fıkraya göre istihdam edilecek sözleşmeli personelin, yurt içindeki ve yurt dışındaki üniversitelerin en az dört yıllık eğitim

veren Kurumca belirlenecek bölümlerinden mezun olması ve en az yarısının Kurumca belirlenecek yabancı diller için Yabancı Dil Bilgisi Seviye Tespit Sınavından en az (C) düzeyinde puan alması veya buna denk kabul edilen ve uluslararası geçerliliği bulunan bir belgeye sahip olması gerekir. Kurumca belirlenecek yabancı dillerin konuşulduğu ülkelerde dört yıllık eğitim veren kurumlardan mezun olan kişilerden yabancı dil belgesi istenmez. Bu fıkrada belirtilen yabancı dil bilgisine ilişkin şartlar yabancı uyruklular için aranmaz.

(7) Merkezi yönetim kapsamındaki kamu idarelerinde, sosyal güvenlik kurumlarında, mahalli idarelerde, mahalli idarelere bağlı idarelerde, mahalli idare birliklerinde, döner sermayeli kuruluşlarda, kanunlarla kurulan fonlarda, kamu tüzel kişiliğini haiz kuruluşlarda, sermayesinin yüzde ellisinden fazlası kamuya ait kuruluşlarda, iktisadi devlet teşekkülleri ve kamu iktisadi kuruluşları ile bunlara bağlı ortaklıklar ve müesseselerde görevli memurlar ile diğer kamu görevlileri kurumlarının, hakimler ve savcılar ise kendilerinin muvafakati ile aylık, ödenek, her türlü zam ve tazminatlar ile diğer mali ve sosyal hak ve yardımları kurumlarınca ödenmek kaydıyla geçici olarak Kurumda görevlendirilebilir. Kurumun bu konudaki talepleri, ilgili kurum ve kuruluşlarca öncelikle sonuçlandırılır. Bu şekilde görevlendirilen personel, kurumlarından aylıklı izinli sayılır. Bu personelin izinli oldukları sürece memuriyetleri ile ilgileri ve özlük hakları devam ettiği gibi, bu süreler yükselme ve emekliliklerinde de hesaba katılır ve yükselmeleri başkaca bir işleme gerek duyulmadan süresinde yapılır. Hakim ve savcılar dâhil bu madde kapsamında görevlendirilenlerin Kurumda geçirdikleri süreler, kendi kurumlarında geçirilmiş sayılır. Görevlendirme süresi iki yılı geçemez. Ancak ihtiyaç hâlinde bu süre bir yıllık dönemler hâlinde uzatılabilir.

İnsan Hakları ve Eşitlik Uzmanı ve Uzman Yardımcıları

MADDE 16- (1) Kurumda, İnsan Hakları ve Eşitlik Uzmanı ve İnsan Hakları ve Eşitlik Uzman Yardımcısı istihdam edilebilir.

BEŞİNCİ BÖLÜM

Başvurular ve İnceleme Usulleri

Başvurular

MADDE 17- (1) Ayrımcılık yasağı ihlalden zarar gördüğü iddiasında bulunan her gerçek ve tüzel kişi Kuruma başvurabilir. Kuruma başvuru, illerde valilikler, ilçelerde kaymakamlıklar aracılığıyla da yapılabilir. Başvuru hakkının etkin bir şekilde kullanılmasına hiçbir surette engel olunamaz. Başvurulardan herhangi bir ücret alınmaz.

(2) İlgililer, Kuruma başvurmadan önce bu Kanuna aykırı olduğunu iddia ettikleri uygulamanın düzeltilmesini ilgili taraftan talep eder. Bu taleplerin reddedilmesi veya otuz gün içerisinde cevap verilmemesi hâlinde Kuruma başvuru yapılabilir. Ancak Kurum, telafisi güç veya imkânsız zararların doğması ihtimali bulunan hâllerde, bu şartı aramadan başvuruları kabul edebilir.

(3) Dava açma süresi içinde Kuruma yapılan başvurular işlemeye başlamış olan dava açma süresini durdurur.

(4) Yasama ve yargı yetkilerinin kullanılmasına ilişkin işlemler, Hâkimler ve Savcılar Yüksek Kurulu kararları ile Anayasanın yargı denetimi dışında bıraktığı işlemler başvurunun konusu olamaz.

(5) 4857 sayılı Kanunun 5 inci maddesi kapsamına giren ayrımcılık iddialarına ilişkin başvurular, 4857 sayılı Kanun ve ilgili mevzuatında belirlenen şikâyet usulleri izlendikten sonra herhangi bir yaptırım kararı alınmadığı hâllerde yapılabilir.

(6) İnsan hakları ve ayrımcılık yasağı ihlallerine ilişkin resen yapılan incelemeler için ihlal mağdurunun şahsen belirlenebilir olduğu durumlarda kendisinin veya kanuni temsilcisinin açık rızasının alınması şarttır. Ancak, çocuğun yüksek yararının gerektirdiği hâllerde kanuni temsilcisinin rızası aranmaz.

(7) Kuruma yapılacak başvurularda, vesayet ya da koruma altında olanlar ve çocuklar ile talepleri üzerine mağdur ya da mağdurların kimlik bilgileri gizli tutulur.

(8) 9 uncu maddenin birinci fıkrasının (i) bendi kapsamında yapılan başvurular hakkında da bu madde hükümleri uygulanır.

(9) İşleme konulmayacak başvurular ve gerekçeli kabul edilmezlik kararları ile başvuruya ilişkin diğer usul ve esaslar yönetmelikle düzenlenir.

İhlal incelemeleri

MADDE 18- (1) Kurum, başvuruları ve resen yaptığı incelemeleri başvuru ve resen inceleme kararı tarihinden itibaren en geç üç ay içinde sonuçlandırır. Bu süre, Başkan tarafından bir defaya mahsus olmak üzere en fazla üç ay uzatılabilir.

(2) Kurum, ihlal iddiasına muhatap olan taraftan yazılı görüşünü sunmasını ister. Yazılı görüş, istemin tebliğinden itibaren on beş gün içinde Kuruma ulaştırılır. Yazılı görüş, başvuran kişiye tebliğ edilerek, görüşünü tebliğden itibaren en geç on beş gün içinde Kuruma sunması istenir. Talep hâlinde Başkan bu süreleri bir defaya mahsus olmak üzere on beş gün uzatabilir. Taraflara talepleri hâlinde Kurul önünde ayrı ayrı sözlü açıklama yapma hakkı tanınabilir.

(3) Başkan, incelemenin özelliğine göre, görüşlerin alınmasından sonra, resen veya talep üzerine tarafları uzlaşmaya davet edebilir. Uzlaşma, insan hakları veya ayrımcılık yasağı ihlali olduğu iddia olunan uygulamaya son verilmesi veya mağdur açısından bu sonucu sağlayacak çözümleri içerebileceği gibi mağdura belli bir tazminatın ödenmesi biçiminde de olabilir. Uzlaşma en geç bir ay içinde sonuçlandırılır. Uzlaşma müzakereleri sırasında yapılan tespitler, alınan beyanlar veya açıklamalar, herhangi bir soruşturma ve kovuşturmada ya da davada delil olarak kullanılamaz.

(4) Uzlaşma yoluyla sonuçlandırılmayan başvurular ve incelemeler hakkında ilgili rapora ilişkin müzakkere yirmi gün içinde Kurula sunulur. Bunun üzerine Kurul, insan hakları veya ayrımcılık yasağı ihlali yapıp yapılmadığına ilişkin karar verir.

(5) Kurul, konusu suç teşkil eden insan hakları veya ayrımcılık yasağı ihlallerini tespit ettiği takdirde, bunlarla ilgili suç duyurusunda bulunur.

İnceleme yetkisi

MADDE 19- (1) Bu Kanunla ve diğer mevzuatla Kuruma verilen inceleme, araştırma, ziyaret ve rapor hazırlama görevleri ile diğer görevler, insan hakları ve eşitlik uzmanları, insan hakları ve eşitlik uzman yardımcıları ve Başkan tarafından görevlendirilen diğer Kurum personeli tarafından yerine getirilir.

(2) Birinci fıkrada sayılanlar, Başkanın yetkilendirmesi hâlinde, tüm kamu kurum ve kuruluşları ile diğer gerçek ve tüzel kişilerden ilgili bilgi ve belgeleri istemeye, incelemeye ve bunların örneklerini almaya, ilgililerden yazılı ve sözlü bilgi almaya, özgürlüğünden mahrum bırakılan ya da koruma altına alınan kişilerin buldukları yerleri ziyaret etmeye, buralarda inceleme yapmaya ve gerekli tutanakları düzenlemeye, kötü muameleye maruz kaldığı iddia edilen kişi ya da kişilerle görüşmeye yetkilidir. Kamu kurum ve kuruluşları ile diğer gerçek ve tüzel kişiler, Kurumun ziyaretlerini kolaylaştırmak ve taleplerini gecikmeksizin yerine getirmek zorundadırlar.

(3) Kurumun görev ve yetki alanına giren konularda yerinde inceleme ve araştırma yapmak üzere, Başkanın belirleyeceği Kurum personelinin başkanlığında, ilgili kurum ve kuruluşların temsilcilerinin ve diğer kişilerin katılımıyla heyet oluşturulabilir. Heyette görev alacak kamu kurum ve kuruluşları temsilcileri kendi kurum ve kuruluşlarınca, diğer kişiler ise Başkan tarafından belirlenir. Heyetler tarafından yapılan inceleme ve araştırmaların sonuçları Kurum tarafından bir rapor hâline getirilir. Heyetlerin giderleri Kurum bütçesinden karşılanır.

(4) Kurumun inceleme ve araştırma konusuyla ilgili olarak gerekçesini belirterek istediği bilgi ve belgelerin, bu talebin tebliğ edildiği tarihten itibaren otuz gün içinde verilmesi zorunludur.

Bilirkişi görevlendirilmesi ve tanık dinlenmesi

MADDE 20- (1) Kurumca inceleme ve araştırma yapılan ve ileri derecede teknik ve mali uzmanlık bilgisi gerektiren konularla ilgili olarak, Başkan ya da Kurul tarafından, ücreti Kurum bütçesinden ödenmek üzere bilirkişi görevlendirilebilir. Bilirkişi olarak görev yapacakların nitelikleri ve çalışma esasları yönetmelikle düzenlenir.

(2) 10/2/1954 tarihli ve 6245 sayılı Harcırah Kanunu hükümleri saklı kalmak üzere, Kurum dışından görevlendirilmek ve ayda beşi geçmemek kaydıyla her inceleme ve araştırma konusu için uhdesinde kamu görevi bulunan her bilirkişiye (1.000), uhdesinde kamu görevi bulunmayan her bilirkişiye (2.000) gösterge rakamının memur aylık katsayısıyla çarpımı sonucu bulunacak miktarı geçmemek üzere bilirkişi ücreti ödenir. Bu ödemeler, damga vergisi hariç herhangi bir vergi ve kesintiye tabi tutulmaz.

(3) İnceleme ve araştırma konusuyula ilgili olarak gerek görülmesi hâlinde Kurul ve inceleme ve araştırma yapmaya yetkili Kurum personeli, tanık veya ilgili kişileri dinleyebilir.

İspat yükü

MADDE 21- (1) Münhasıran ayrımcılık yasağının ihlali iddiasıyla Kuruma yapılan başvurularda, başvuranın iddiasının gerçekliğine ilişkin kuvvetli emarelerin ve karine oluşturan olguların varlığını ortaya koyması hâlinde, karşı tarafın ayrımcılık yasağını ve eşit muamele ilkesini ihlal etmediğini ispat etmesi gerekir.

İstişare komisyonu ve istişare toplantıları

MADDE 22- (1) Ayrımcılık yasağıyla ilgili konularda sorunları ve çözüm önerilerini tartışmak ve bu konularda bilgi ve görüş alışverişinde bulunmak amacıyla, kamu kurum ve kuruluşları, sivil toplum kuruluşları, sendikalar, sosyal ve mesleki kuruluşlar, yükseköğretim kurumları, basın ve yayın kuruluşları, araştırmacılar ve ilgili diğer kişi, kurum ve kuruluşların katılımıyla istişare komisyonu oluşturulur.

(2) Kurum, insan hakları sorunlarını tartışmak ve insan hakları konularında bilgi ve görüş alışverişinde bulunmak amacıyla, kamu kurum ve kuruluşları, sivil toplum kuruluşları, sendikalar, sosyal ve mesleki kuruluşlar, yükseköğretim kurumları, basın ve yayın kuruluşları, araştırmacılar ve ilgili diğer kişi, kurum ve kuruluşların katılımıyla merkezde ve illerde istişare toplantıları gerçekleştirir.

(3) Bu maddenin uygulanmasına ilişkin usul ve esaslar yönetmelikle belirlenir.

ALTINCI BÖLÜM

Çeşitli ve Son Hükümler

Kurumun gelirleri

MADDE 23- (1) Kurumun gelirleri şunlardır:

- a) Genel bütçeden yapılacak hazine yardımları.
- b) Kuruma ait taşınır ve taşınmazlardan elde edilen gelirler.
- c) Gelirlerinin değerlendirilmesinden elde edilen gelirler.
- ç) Diğer gelirler.

İstatistik

MADDE 24- (1) Kurul, ayrımcılıkla mücadele amacıyla hangi alanlarda resmî nitelikte istatistik toplanmasına ihtiyaç olduğuna Türkiye İstatistik Kurumu ve diğer ilgili kurum ve kuruluşlarla birlikte karar verir. Ayrımcılık belirtilerinin tüm boyutlarını ortaya koyabilmek için gerekli olan istatistiksel bilgilerin, verilere sürekli ve eksiksiz şekilde erişilmesini sağlayacak bir sistem içinde toplanmasından Resmî İstatistik Programı kapsamında Türkiye İstatistik Kurumu sorumludur.

İdari yaptırımlar

MADDE 25- (1) Ayrımcılık yasağının ihlali hâlinde, bu ihlalin etki ve sonuçlarının ağırlığı, failin ekonomik durumu ve çoklu ayrımcılığın ağırlaştırıcı etkisi dikkate alınarak ihlalden sorumlu olan kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, gerçek kişiler ve özel hukuk tüzel kişileri hakkında bin Türk lirasından on beş bin Türk lirasına kadar idari para cezası uygulanır.

(2) Birinci fıkrada belirtilen idari para cezasının kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları hakkında uygulanması hâlinde, ödenen idari para cezası, cezaya esas ayrımcı uygulamaya kusuruyla sebebiyet veren kamu kurum ve kuruluşlarında görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlara rücu edilir.

(3) 19 uncu maddede öngörülen yükümlülüklerle, uyarıya rağmen haklı bir neden olmaksızın belirtilen sürede uymayan birinci fıkra kapsamındaki kişi ve kuruluşlar hakkında beş yüz Türk lirasından iki bin Türk lirasına kadar idari para cezası uygulanır. Bu fıkrada düzenlenen idari para cezaları hakkında da ikinci fıkra hükmü uygulanır.

(4) Kurul, verdiği idari para cezasını bir defaya mahsus olmak üzere uyarı cezasına dönüştürebilir. Hakkında uyarı cezası verilen kişi veya kurumun ayrımcı fiilinin tekrarı hâlinde alacağı ceza yüzde elli oranında artırılır. Bu artış ceza üst sınırını aşamaz.

(5) Bu Kanuna göre verilen idari para cezaları tebliğinden itibaren bir ay içinde ödenir.

(6) Bu Kanunda hüküm bulunmayan hâllerde idari yaptırımlara ilişkin olarak 30/3/2005 tarihli ve 5326 sayılı Kabahatler Kanunu hükümleri uygulanır.

İnsan hakları ve ayrımcılıkla mücadele eğiticileri

MADDE 26- (1) İnsan hakları ve ayrımcılıkla mücadele eğitimi, Kurum personeli veya insan hakları ve ayrımcılıkla mücadele eğiticileri tarafından verilir. Eğiticilerin nitelikleri, çalışma usul ve esasları ile eğiticilere verilecek ücret Maliye Bakanlığının uygun görüşü alınarak yönetmelikle düzenlenir.

Yönetmelik

MADDE 27- (1) Bu Kanunun uygulanmasına ilişkin yönetmelikler Kurum tarafından yürürlüğe konulur.

Yürürlükten kaldırılan ve değiştirilen hükümler

MADDE 28- (1) 21/6/2012 tarihli ve 6332 sayılı Türkiye İnsan Hakları Kurumu Kanunu yürürlükten kaldırılmıştır. Diğer mevzuatta mülga Türkiye İnsan Hakları Kurumuna yapılmış olan atıflar Türkiye İnsan Hakları ve Eşitlik Kurumuna yapılmış sayılır.

(2) (14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu ile ilgili olup yerine işlenmiştir.)

(3) 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanunu ile ilgili olup yerine işlenmiştir.)

(4) Türkiye İnsan Hakları Kurumuna ait kadrolar iptal edilerek 13/12/1983 tarihli ve 190 sayılı Genel Kadro ve Usulü Hakkında Kanun Hükmünde Kararnamenin ilgili cetvellerinden çıkarılmış ve ekli (1) sayılı listede yer alan kadrolar ihdas edilerek anılan Kanun Hükmünde Kararnamenin eki (I) sayılı cetvele Türkiye İnsan Hakları ve Eşitlik Kurumu bölümü olarak eklenmiştir.

(5) (27/6/1989 tarihli ve 375 sayılı Kanun Hükmünde Kararname ile ilgili olup yerine işlenmiştir.)

Hak ve yetkiler ile personelin devri

GEÇİCİ MADDE 1- (1) Bakanlar Kurulunca ilk yapılacak seçimde seçilecek üyelere ilişkin başvurular ve aday bildirimleri Başbakanlığa yapılır. Başvurular ve aday bildirimlerine ilişkin hususlar Başbakanlık tarafından ilan edilir.

(2) Bu Kanun ile kurulan Türkiye İnsan Hakları ve Eşitlik Kurumu teşkilatlanıncaya kadar Kuruma verilen görev ve hizmetler mülga Türkiye İnsan Hakları Kurumunun mevcut personeli eliyle yürütölmeye devam edilir.

(3) Bu maddenin yürürlüğe girdiği tarihte mülga Türkiye İnsan Hakları Kurumuna ait her türlü taşınır, taşıt, araç, gereç ve malzeme, nakit ve benzeri değerler, her türlü borç ve alacaklar, yazılı ve elektronik ortamdaki her türlü kayıtlar ve diğer dokümanlar ile kadro ve pozisyonlarda bulunan personel, hiçbir işleme gerek kalmaksızın Türkiye İnsan Hakları ve Eşitlik Kurumuna devredilmiş sayılır.

(4) Mülga Türkiye İnsan Hakları Kurumu tarafından yapılmış olan sözleşmelere Türkiye İnsan Hakları ve Eşitlik Kurumu halef olur. Mülga Türkiye İnsan Hakları Kurumunun leh ve aleyhine açılmış davalar ile icra takiplerinde Türkiye İnsan Hakları ve Eşitlik Kurumu kendiliğinden taraf sıfatını kazanır.

(5) Mülga Türkiye İnsan Hakları Kurulu üyelerinin üyelikleri bu maddenin yürürlüğe girdiği tarihte sona erer. Mülga Türkiye İnsan Hakları Kurumu Başkanı ve İkinci Başkanı, bu Kanuna göre seçilen Türkiye İnsan Hakları ve Eşitlik Kurumu Başkanı göreve başlayıncaya kadar Türkiye İnsan Hakları ve Eşitlik Kurumu Başkanı ve İkinci Başkanı olarak görev yapar. Bunlar, bu Kanuna göre seçilen Türkiye İnsan Hakları ve Eşitlik Kurumu Başkanı göreve başladığında, atandıkları mevzuata göre kalan görev sürelerinin sonuna kadar görev yapmak üzere ekli (2) sayılı liste ile ihdas edilen Kurum Başkanlık Müşaviri kadrolarına hiçbir işleme gerek kalmaksızın atanmış sayılır ve Başkan tarafından belirlenen istişari görevleri yürütür. Bu fıkra ile ihdas edilen Kurum Başkanlık Müşaviri kadroları, bu kadroların herhangi bir sebeple boşalması ve her hâlde anılan kadrolara atanmış sayılan Başkan ve İkinci Başkanın atandıkları mevzuata göre kalan görev sürelerinin sona ermesi hâlinde hiçbir işleme gerek kalmaksızın iptal edilmiş sayılır. Bu fıkraya göre Kurum Başkanlık Müşaviri kadrolarına atanmış sayılanlara, fiilen görev yapma şartına bağlı ödemeler hariç mali ve sosyal haklar kapsamında bu maddenin yürürlüğe girdiği tarihten önce yürürlükte bulunan mevzuata göre yapılmakta olan ödemelere, kalan görev süreleri sonuna kadar devam edilir. Bunlar görev sürelerinin sonunda talepleri hâlinde, Kurumda veya önceki kurumlarında öğrenim durumları, hizmet yılı ve kazanılmış hak aylık derecelerine uygun bir kadroya en geç bir ay içinde atanır.

(6) Bu maddenin yürürlüğe girdiği tarihte İnsan Hakları Uzmanı ve İnsan Hakları Uzman Yardımcısı kadrolarında bulunanlar, İnsan Hakları ve Eşitlik Uzmanı ile İnsan Hakları ve Eşitlik Uzman Yardımcısı kadrolarına başka bir işleme gerek kalmaksızın hâlen buldukları kadro derecelerleriyle atanmış sayılır ve bunlardan 375 sayılı Kanun Hükmünde Kararnamenin geçici 12 nci maddesi

hükmünden yararlananların bu hakları söz konusu kadrolarda buldukları sürece devam eder. Bu fıkraya göre atananların İnsan Hakları Uzmanı kadrosunda geçirdiği süreler İnsan Hakları ve Eşitlik Uzmanı kadrosunda, İnsan Hakları Uzman Yardımcısı kadrosunda geçirdiği süreler ise İnsan Hakları ve Eşitlik Uzman Yardımcısı kadrosunda geçmiş sayılır.

(7) Mülga Türkiye İnsan Hakları Kurumu kadrolarında bulunan memurlardan yukarıdaki fıkralarda belirtilenler dışında kalanlar, Kurum için ihdas edilen aynı unvanlı kadrolara hâlen buldukları kadro dereceleriyle başka bir işleme gerek kalmaksızın atanmış sayılır.

(8) Bu madde uyarınca atanan veya atanmış sayılan personelin yeni kadrolarına atandıkları veya atanmış sayıldıkları tarih itibarıyla eski kadrolarına ilişkin en son ayda aldıkları sözleşme ücreti, aylık, ek gösterge, ikramiye (bir aya isabet eden net tutarı), her türlü zam ve tazminatları, makam tazminatı, temsil tazminatı, görev tazminatı, ek ödeme ve benzeri adlarla yapılan her türlü ödemelerin toplam net tutarının (Bu tutar sabit bir değer olarak esas alınır.); yeni atandıkları kadrolara ilişkin olarak yapılan sözleşme ücreti, aylık, ek gösterge, ikramiye (bir aya isabet eden net tutarı), her türlü zam ve tazminatları, makam tazminatı, temsil tazminatı, görev tazminatı, ek ödeme ve benzeri adlarla yapılan her türlü ödemelerin (ilgili mevzuatı uyarınca fiili çalışmaya bağlı fazla mesai ücreti hariç) toplam net tutarından fazla olması hâlinde aradaki fark tutarı, herhangi bir vergi ve kesintiye tabi tutulmaksızın fark kapanıncaya kadar ayrıca tazminat olarak ödenir. Atandıkları veya atanmış sayıldıkları kadro unvanlarında isteğe bağlı olarak herhangi bir değişiklik olanlarla, kendi istekleriyle başka kurumlara atananlara fark tazminatı ödenmesine son verilir.

(9) Bu maddenin yürürlüğe girdiği tarihe kadar mülga Türkiye İnsan Hakları Kurumunda geçen hizmetler, Türkiye İnsan Hakları ve Eşitlik Kurumunda geçmiş sayılır.

(10) Türkiye İnsan Hakları ve Eşitlik Kurumunun 2016 mali yılı harcamaları, 2016 Yılı Merkezi Yönetim Bütçe Kanununa istinaden Maliye Bakanlığınca yeni bir düzenleme yapılınca kadar, mülga Türkiye İnsan Hakları Kurumunun 2016 yılı bütçesinde yer alan ödeneklerinden karşılanır.

(11) Cumhurbaşkanlığı tarafından yeni bir düzenleme yapılınca kadar il ve ilçe insan hakları kurulları faaliyetine devam eder.

(12) En az dört yıllık lisans eğitimi veren yükseköğretim kurumlarını bitirerek mesleğe özel yarışma sınavı ile giren ve belirli süreli meslek içi eğitimden sonra özel bir yeterlik sınavı sonunda insan hakları alanında faaliyet gösteren kurumların merkez teşkilatı kadrolarına atanmış olanlar talepleri hâlinde kurumlarının, hakimler ve savcılar ise kendilerinin muvafakati ile, Kurumun görev alanına giren konularda doktora yapmış olan Devlet memurları ile öğretim elemanları ise başvurularını

hâlinde bu Kanunun yürürlüğe girdiği tarihten itibaren bir yıl içinde, bu Kanun kapsamında atanan Kurul tarafından belirlenecek usul ve esaslar dâhilinde İnsan Hakları ve Eşitlik Uzmanı olarak atanabilirler. Bu fıkra hükümlerine göre atanacak olanların sayısı, Kurumun kadro cetvellerindeki İnsan Hakları ve Eşitlik Uzmanı ve İnsan Hakları ve Eşitlik Uzman Yardımcısı kadro sayısının yüzde onunu geçemez.

(13) Bu Kanunun uygulanmasına ilişkin yönetmelikler Kurulun ilk toplantı tarihinden itibaren altı ay içerisinde yürürlüğe konulur. Ayrımcılık yasağı ihlali iddialarına ilişkin başvurular 17 nci maddenin dokuzuncu fıkrasında öngörülen yönetmeliğin yürürlüğe girdiği tarihten itibaren alınır.

Yürürlük

MADDE 29- (1) Bu Kanun yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 30- (1) Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunu

Resmî Gazete Tarihi : 5.11.2014

Resmî Gazete Sayısı : 29166

ELEKTRONİK TİCARETİN DÜZENLENMESİ HAKKINDA KANUN

Amaç ve kapsam

MADDE 1 - (1) Bu Kanunun amacı, elektronik ticarete ilişkin esas ve usulleri düzenlemektir.

(2) Bu Kanun, ticari iletişimi, hizmet sağlayıcı ve aracı hizmet sağlayıcıların sorumluluklarını, elektronik iletişim araçlarıyla yapılan sözleşmeler ile elektronik ticarete ilişkin bilgi verme yükümlülüklerini ve uygulanacak yaptırımları kapsar.

Tanımlar

MADDE 2 - (1) Bu Kanunun uygulanmasında;

- a) Elektronik ticaret: Fiziki olarak karşı karşıya gelmeksizin, elektronik ortamda gerçekleştirilen çevrim içi iktisadi ve ticari her türlü faaliyeti,
 - b) Ticari iletişim: Alan adları ve elektronik posta adresi dışında, mesleki veya ticari faaliyet kapsamında kazanç sağlamaya yönelik olarak elektronik ticarete ilişkin her türlü iletişimi,
 - c) Ticari elektronik ileti: Telefon, çağrı merkezleri, faks, otomatik arama makineleri, akıllı ses kaydedici sistemler, elektronik posta, kısa mesaj hizmeti gibi vasıtalar kullanılarak elektronik ortamda gerçekleştirilen ve ticari amaçlarla gönderilen veri, ses ve görüntü içerikli iletileri,
 - ç) Hizmet sağlayıcı: Elektronik ticaret faaliyetinde bulunan gerçek ya da tüzel kişileri,
 - d) Aracı hizmet sağlayıcı: Başkalarına ait iktisadi ve ticari faaliyetlerin yapılmasına elektronik ticaret ortamını sağlayan gerçek ve tüzel kişileri,
 - e) Bakanlık: Gümrük ve Ticaret Bakanlığını,
- ifade eder.

Bilgi verme yükümlülüğü

MADDE 3 - (1) Hizmet sağlayıcı, elektronik iletişim araçlarıyla bir sözleşmenin yapılmasından önce;

- a) Alıcıların kolayca ulaşabileceği şekilde ve güncel olarak tanıtıcı bilgilerini,
 - b) Sözleşmenin kurulabilmesi için izlenecek teknik adımlara ilişkin bilgileri,
 - c) Sözleşme metninin sözleşmenin kurulmasından sonra, hizmet sağlayıcı tarafından saklanıp saklanmayacağı ile bu sözleşmeye alıcının daha sonra erişiminin mümkün olup olmayacağı ve bu erişimin ne kadar süreyle sağlanacağına ilişkin bilgileri,
 - ç) Veri girişindeki hataların açık ve anlaşılır bir şekilde belirlenmesine ve düzeltilmesine ilişkin teknik araçlara ilişkin bilgileri,
 - d) Uygulanan gizlilik kuralları ve varsa alternatif uyumsuzluk çözüm mekanizmalarına ilişkin bilgileri,
- sunar.

(2) Hizmet sağlayıcı, varsa mensubu olduğu meslek odası ile meslekle ilgili davranış kurallarını ve bunlara elektronik olarak ne şekilde ulaşılabilirliğini belirtir.

(3) Tarafların tüketici olmadığı hâllerde taraflar, birinci ve ikinci fıkralardaki düzenlemelerin aksini kararlaştırabilirler.

(4) Hizmet sağlayıcı, sözleşme hükümlerinin ve genel işlem şartlarının alıcı tarafından saklanmasına imkan sağlar.

(5) Birinci ve ikinci fıkralar, münhasıran elektronik posta yoluyla veya benzeri bireysel iletişim araçlarıyla yapılan sözleşmelere uygulanmaz.

Sipariş

MADDE 4 - (1) Elektronik iletişim araçlarıyla verilen siparişlerde aşağıdaki esaslar geçerlidir:

- a) Hizmet sağlayıcı, siparişin onaylanması aşamasında ve ödeme bilgilerinin girilmesinden önce, ödeyeceği toplam bedel de dâhil olmak üzere, sözleşmenin şartlarının alıcı tarafından açıkça görülmesini sağlar.
- b) Hizmet sağlayıcı, alıcının siparişini aldığını gecikmeksizin elektronik iletişim araçlarıyla teyit eder.
- c) Sipariş ve siparişin alındığının teyidi, tarafların söz konusu beyanlara erişiminin mümkün olduğu anda gerçekleşmiş sayılır.

(2) Hizmet sağlayıcı, sipariş verilmeden önce alıcıya, veri giriş hatalarını belirleyebilmesi ve düzeltebilmesi için uygun, etkili ve erişilebilir teknik araçları sunar.

(3) Tarafların tüketici olmadığı hâllerde taraflar, birinci ve ikinci fıkralardaki düzenlemelerin aksini kararlaştırabilirler.

(4) Birinci fıkranın (a) ve (b) bentleri ile ikinci fıkra, münhasıran elektronik posta yoluyla veya benzeri bireysel iletişim araçlarıyla yapılan sözleşmelere uygulanmaz.

Ticari iletişime ilişkin esaslar

MADDE 5 - (1) Ticari iletişimde:

a) Ticari iletişimin ve bu iletişimin adına yapıldığı gerçek ya da tüzel kişinin açıkça belirlenebilir olmasını sağlayan bilgiler sunulmalıdır.

b) İndirim ve hediye gibi promosyonlar ile promosyon amaçlı yarışma veya oyunların bu niteliği açıkça belirlenebilmeli, bunlara katılımın ve bunlardan faydalanmanın şartlarına kolayca ulaşılabilmesi ve bu şartlar açık ve şüpheye yer bırakmayacak şekilde anlaşılır olmalıdır.

Ticari elektronik ileti gönderme şartı

MADDE 6 - (1) Ticari elektronik iletiler, alıcılara ancak önceden onayları alınmak kaydıyla gönderilebilir. Bu onay, yazılı olarak veya her türlü elektronik iletişim araçlarıyla alınabilir. Kendisiyle iletişime geçilmesi amacıyla alıcının iletişim bilgilerini vermesi hâlinde, temin edilen mal veya hizmetlere ilişkin değişiklik, kullanım ve bakıma yönelik ticari elektronik iletiler için ayrıca onay alınmaz.

(2) Esnaf ve tacirlere önceden onay alınmaksızın ticari elektronik iletiler gönderilebilir.

Ticari elektronik iletinin içeriği

MADDE 7 - (1) Ticari elektronik iletinin içeriği, alıcıdan alınan onaya uygun olmalıdır.

(2) İletide, hizmet sağlayıcının tanınmasını sağlayan bilgiler ile haberleşmenin türüne bağlı olarak telefon numarası, faks numarası, kısa mesaj numarası ve elektronik posta adresi gibi erişilebilir durumdaki iletişim bilgileri yer alır.

(3) İletide, haberleşmenin türüne bağlı olarak, iletinin konusu, amacı ve başkası adına yapılması hâlinde kimin adına yapıldığına ilişkin bilgilere de yer verilir.

Alıcının ticari elektronik iletiyi reddetme hakkı

MADDE 8 - (1) Alıcılar diledikleri zaman, hiçbir gerekçe belirtmeksizin ticari elektronik iletileri almayı reddedebilir.

(2) Hizmet sağlayıcı ret bildiriminin, elektronik iletişim araçlarıyla kolay ve ücretsiz olarak iletilmesini sağlamakla ve gönderdiği iletide buna ilişkin gerekli bilgileri sunmakla yükümlüdür.

(3) Talebin ulaşmasını müteakip hizmet sağlayıcı üç iş günü içinde alıcıya elektronik ileti göndermeyi durdurur.

Aracı hizmet sağlayıcıların yükümlülükleri

MADDE 9 - (1) Aracı hizmet sağlayıcılar, hizmet sundukları elektronik ortamı kullanan gerçek ve tüzel kişiler tarafından sağlanan içerikleri kontrol etmek, bu içerik ve içeriğe konu mal veya hizmetle ilgili hukuka aykırı bir faaliyetin ya da durumun söz konusu olup olmadığını araştırmakla yükümlü değildir.

(2) Bu Kanunun 3, 4, 5, 6, 7 ve 8 inci maddelerinde düzenlenen yükümlülüklerin aracı hizmet sağlayıcılarına uygulanmasına ilişkin usul ve esaslar yönetmelikle belirlenir.

Kişisel verilerin korunması

MADDE 10 - (1) Hizmet sağlayıcı ve aracı hizmet sağlayıcı:

a) Bu Kanun çerçevesinde yapmış olduğu işlemler nedeniyle elde ettiği kişisel verilerin saklanması ve güvenliğinden sorumludur.

b) Kişisel verileri ilgili kişinin onayı olmaksızın üçüncü kişilere iletmez ve başka amaçlarla kullanamaz.

Bakanlık yetkisi

MADDE 11 - (1) Bakanlık, bu Kanunun uygulanması ve elektronik ticaretin gelişimiyle ilgili her türlü tedbiri almaya ve denetimi yapmaya yetkilidir.

(2) Bakanlıkça görevlendirilen denetim elemanları, bu Kanun kapsamında Bakanlık yetkisine giren hususlarla ilgili olarak her türlü bilgi, belge ve defterleri istemeye, bunları incelemeye ve örneklerini almaya, ilgililerden yazılı ve sözlü bilgi almaya yetkili olup ilgililer istenilen bilgi, belge ve defterler ile elektronik kayıtlarını, bunların örneklerini noksansız ve gerçeğe uygun olarak vermek, yazılı ve sözlü bilgi taleplerini karşılamak ve her türlü yardım ve kolaylığı göstermekle yükümlüdür.

(3) (Ek:28/11/2017-7061/117 md.) Kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları ve diğer gerçek veya tüzel kişiler, elektronik ticaretin gelişiminin izlenebilmesi ve değerlendirilebilmesi amacıyla Bakanlık tarafından istenilen bilgileri Bakanlıkça oluşturulan sisteme bildirir.

(4) (Ek:28/11/2017-7061/117 md.) Bakanlık, ticari elektronik ileti onaylarının alınmasına ve reddetme hakkının kullanılmasına imkân tanıyan bir elektronik sistem kurmaya veya kurdurmaya yetkilidir. Bu Kanun çerçevesinde alınan onaylar Bakanlıkça belirlenen süre içinde sisteme aktarılır. Sisteme aktarılmayan onaylar geçersiz kabul edilir. Alıcılar, sisteme kaydedilen onayları Bakanlıkça belirlenen süre içinde kontrol eder. Bu sürenin bitiminden sonra gönderilen ticari elektronik iletiler onaylı kabul edilir. Alıcılar tarafından reddetme hakkı bu sistem üzerinden kullanılır. Sistemin kurulması, onayların sisteme aktarılması, saklanması, reddetme hakkının sistem üzerinden kullanılması ve sistemin işleyişine ilişkin diğer usul ve esaslar yönetmelikle belirlenir.

Cezai hükümler

MADDE 12 - (1) Bu Kanunun;

a) 3 üncü maddesindeki yükümlülüklerle, 4 üncü maddesinin birinci fıkrasının (a) bendindeki yükümlülüklerle, 6 ncı maddesinin birinci fıkrasına veya 7 nci maddesinin birinci fıkrasına aykırı hareket eden hizmet sağlayıcılara ve aracı hizmet sağlayıcılara bin Türk lirasından beş bin Türk lirasına kadar,

b) 4 üncü maddesinin birinci fıkrasının (b) bendindeki veya aynı maddenin ikinci fıkrasındaki, 5 inci maddesinin birinci fıkrasının (a) bendindeki veya 7 nci maddesinin ikinci ve üçüncü fıkralarındaki yükümlülüklerle aykırı hareket eden hizmet sağlayıcılara ve aracı hizmet sağlayıcılara bin Türk lirasından on bin Türk lirasına kadar,

c) 5 inci maddesinin birinci fıkrasının (b) bendindeki, 8 inci maddesinin ikinci ve üçüncü fıkralarındaki yükümlülüklerle aykırı hareket eden hizmet sağlayıcılara ve aracı hizmet sağlayıcılara iki bin Türk lirasından on beş bin Türk lirasına kadar,

ç) 11 inci maddesinin ikinci fıkrasına aykırı hareket edenlere iki bin Türk lirasından beş bin Türk lirasına kadar,

d) (Ek:28/11/2017-7061/118 md.) 11 inci maddesinin üçüncü fıkrasına aykırı hareket eden gerçek kişiler ile özel hukuk tüzel kişileri hakkında beş bin Türk lirasından yirmi bin Türk lirasına kadar,

idari para cezası verilir.

(2) Bir defada birden fazla kimseye 6 ncı maddenin birinci fıkrasına aykırı olarak ileti gönderilmesi hâlinde, birinci fıkranın (a) bendinde öngörülen idari para cezası on katına kadar artırılarak uygulanır.

(3) Bu maddede öngörülen idari para cezalarını verme yetkisi Bakanlığa aittir. Bu yetki, merkezde Bakanlığın ilgili genel müdürlüğüne, taşrada ise Bakanlığın il müdürlüklerine devredilebilir.

Yönetmelikler

MADDE 13 - (1) Bu Kanunun uygulanmasına ilişkin yönetmelikler; Adalet Bakanlığı, Maliye Bakanlığı, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ve Ekonomi Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumunun görüşleri alınarak Bakanlık tarafından hazırlanır.

Değiştirilen mevzuat

MADDE 14 - (1) (5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu ile ilgili olup yerine işlenmiştir.)

Onay alınarak oluşturulan veri tabanları

GEÇİCİ MADDE 1 - (1) Bu Kanunun yürürlüğe girdiği tarihten önce, ticari elektronik ileti gönderilmesi amacıyla onay alınarak oluşturulmuş olan veri tabanları hakkında 6 ncı maddenin birinci fıkrası uygulanmaz.

Yürürlük

MADDE 15 - (1) Bu Kanun 1/5/2015 tarihinde yürürlüğe girer.

Yürütme

MADDE 16 - (1) Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

**6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik
Para Kuruluşları Hakkında Kanun**

Resmî Gazete Tarihi : 27.06.2013

Resmî Gazete Sayısı : 28690

**ÖDEME VE MENKUL KIYMET MUTABAKAT SİSTEMLERİ, ÖDEME HİZMETLERİ VE
ELEKTRONİK PARA KURULUŞLARI HAKKINDA KANUN**

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç

MADDE 1 - (1) Bu Kanunun amacı, ödeme ve menkul kıymet mutabakat sistemlerine, ödeme hizmetlerine, ödeme kuruluşlarına ve elektronik para kuruluşlarına ilişkin usul ve esasları düzenlemektir.

Kapsam

MADDE 2 - (1) Bu Kanun, ödeme ve menkul kıymet mutabakat sistemlerini, ödeme hizmetlerini, ödeme kuruluşları ile elektronik para kuruluşlarını kapsar.

Tanımlar

MADDE 3 - (1) Bu Kanunun uygulanmasında;

(...)

ğ) Kişisel güvenlik bilgileri: Ödeme aracı ile işlem gerçekleştirirken kullanılacak şifre, son kullanma tarihi, güvenlik numarası gibi ödeme aracını ve ödeme aracı kullanıcısının kimliğini belirleyici bilgileri,

(...)

ifade eder.

(...)

Belge ve kayıtların saklanması ile kişisel bilgilerin korunması, değişikliklerin bildirilmesi

MADDE 23 - (1) (Değişik: 27/3/2015-6637/13 md.) Sistem işleticisi, ödeme kuruluşu ve elektronik para kuruluşu bu Kanunda yer alan hususlar ile ilgili belgeleri ve kayıtları en az on yıl süreyle güvenli ve istenildiği an erişime imkân sağlayacak şekilde yurt içinde saklar. Sistem işleticisinin faaliyetlerini yürütmede kullandığı bilgi sistemleri ve bunların yedekleri de yurt içinde tutulur. Ödeme kuruluşu ve elektronik para kuruluşunun faaliyetlerini yürütmede kullandıkları bilgi sistemlerine ilişkin usul ve esaslar Bankaca belirlenir.(2)

(2) Ödeme usulsüzlüklerini önlemek, araştırmak ve ortaya çıkarmak için gerekli durumlarda, sistem işleticisi ve ödeme hizmeti sağlayıcısı, kişisel bilgileri kişisel verilerin korunmasına ilişkin gerekli tedbirleri alarak kullanır.

(3) Banka tarafından istenen bilgi ve belgelerin geçerliliğini etkileyecek herhangi bir değişikliğin olması durumunda sistem işleticisi, ödeme kuruluşu ve elektronik para kuruluşu Bankayı bu konuda derhâl bilgilendirir.

6475 sayılı Posta Hizmetleri Kanunu

Resmî Gazete Tarihi : 23.05.2013

Resmî Gazete Sayısı : 28655

POSTA HİZMETLERİ KANUNU

BİRİNCİ KISIM

Genel Hükümler

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç

MADDE 1 - (1) Bu Kanunun amacı; ülke genelinde posta hizmetlerinin kaliteli, sürekli, tüm kullanıcılar için karşılanabilir bir ücretle, etkin, rekabete dayalı esaslar çerçevesinde sunulmasını sağlamak üzere posta sektörünün serbestleştirilerek mali açıdan güçlü, istikrarlı ve şeffaflığı sağlanmış bir sektör oluşturulması ve bu sektörde düzenleme ve denetimin gerçekleştirilmesi ve posta hizmetlerinin yürütülmesine ilişkin usul ve esasları düzenlemektir.

Kapsam

MADDE 2 - (1) Bu Kanun; posta gönderilerinin kabulü, toplanması, işlenmesi, sevki, dağıtımı ve teslimine ilişkin işlem ve hizmetlerin sunulması, yetkilendirme, tarife ilkeleri ve hizmet şartlarının tespit edilmesi, sektörde düzenleme ve denetimin gerçekleştirilmesi, bunlara ilişkin yaptırımların belirlenmesi ve posta hizmetlerinin yürütülmesine ilişkin usul ve esasları kapsar.

(...)

Posta hizmetlerinin gizliliği ve güvenliği

MADDE 7 - (1) Hizmet sağlayıcıları ile posta hizmetlerinde çalışanlar veya herhangi bir şekilde posta hizmetleri ile ilgili bilgiye sahip olanların, bu bilgileri ve posta hizmetleri ile ilgili ilişkileri açığa vurmaları, gönderileri açmaları, içlerinde ne olduğunu araştırmaları, üçüncü kişilere bilgi vermeleri veya herhangi birinin bunları yapmasına neden olmaları, gönderileri zapt veya yok etmeleri yasaktır.

(2) Hizmet sağlayıcıları, yürüttüğü hizmetlerle ilgili olarak gerekli güvenlik önlemlerini almakla yükümlüdür.

(3) Posta gönderileri, kanunla yetkili kılınan merciler dışındaki kişilerce alıkonulamaz, açılmaz ve içeriği araştırılmaz.

(...)

Hizmet sağlayıcılarının yükümlülükleri

MADDE 12 - (1) Hizmet sağlayıcılarının yükümlülükleri şunlardır:

a) Teşkilat birimlerini, mevzuatın öngördüğü defter ve kayıtlarını denetime hazır bulundurmak, Kurum tarafından talep edildiğinde denetime açmak ve Kurumun faaliyetlerini yerine getirebilmesi için ihtiyaç duyacağı her türlü bilgi ve belgeyi zamanında Kuruma vermek

b) Kişisel veri ve bilgilerin gizliliğinin korunması yükümlülüklerine uymak

c) Yetki belgesine konu her hizmet için ayrı hesap ve kayıt tutmak

ç) Sermaye şirketlerinin ortaklık yapılarında toplamda yüzde 10 veya daha fazla bir sermaye payı değişimi, halka açık şirketlerde ise doğrudan veya dolaylı yönetim hakimiyeti değişikliği, birleşmeleri veya herhangi bir tüzel kişinin katılımıyla genişlemesi, kontrolün değişmesi, satış, devir veya diğer düzenlemeler ile tüzel kişilik yapısında meydana gelen değişiklikler için Kurum onayı almak

d) Can ve mal güvenliğini tehdit eden veya tehlike arz eden her türlü faaliyetin oluşumunun engellenmesi için gerekli tedbirleri almak ve alınan tedbirleri Kuruma bildirmek

e) Bu Kanun hükümleri uyarınca posta sektöründe verimli, istikrarlı ve ekonomik bir sistem oluşturmak suretiyle posta gönderilerinin kabulü, toplanması, işlenmesi, sevki ve dağıtımını rekabet ortamına uygun olarak sağlamak

f) Çevreye zarar vermemek için gerekli tedbirleri almak

g) Millî güvenlik ile kamu düzeni gereklerine ve acil durum ihtiyaçlarına öncelik vermek

ğ) Mevzuatın ve Kurul kararlarının gereklerini yerine getirmek

(...)

Faaliyet konuları ve nitelikleri

MADDE 22 - (1) PTT; yurt içinde ve yurt dışında her türlü taşımacılık hizmetlerini de içerecek şekilde posta, koli, kargo ve lojistik hizmetleri, pul basımı ve satımı, denetlemeye ilişkin hükümleri saklı kalmak kaydıyla, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununa tabi olmaksızın, anılan Kanun

kapsamında belirtilen faaliyet konuları ile ilgili olarak bankalarla yapacağı sözleşmeler doğrultusunda bankalara destek hizmeti, parasal posta hizmeti, ödeme hizmeti sunma, adres bilgi kayıt sistemi ve elektronik sertifika hizmet sağlayıcılığı, elektronik ortam dâhil her türlü tebligat ve telgraf hizmetine ilişkin faaliyetler, 20/6/1984 tarihli ve 3028 sayılı Yabancı Resmî Belgelerin Tasdiki Mecburiyetinin Kaldırılması Sözleşmesinin Tasdikinın Uygun Olduğu Hakkında Kanunla uygun bulunan Sözleşme uyarınca yetkili birimler tarafından onay şerhi (apostille) verilmiş belgelerin, kişisel verilerin korunması kaydıyla, elektronik ortamda ilgililere ulaştırılması için aracılık işlemleri ile esas sözleşmesinde belirlenen diğer faaliyetleri yürütür.

(...)

6458 sayılı Yabancılar ve Uluslararası Koruma Kanunu

Resmî Gazete Tarihi : 11.04.2013

Resmî Gazete Sayısı : 28615

YABANCILAR VE ULUSLARARASI KORUMA KANUNU

BİRİNCİ KISIM

Amaç, Kapsam, Tanımlar ve Geri Gönderme Yasağı

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç (1)

MADDE 1 - (1) Bu Kanunun amacı; yabancıların Türkiye'ye girişleri, Türkiye'de kalışları ve Türkiye'den çıkışları ile Türkiye'den koruma talep eden yabancılara sağlanacak korumanın kapsamına ve uygulanmasına ilişkin usul ve esasları (...) (1) düzenlemektir. (1)

Kapsam

MADDE 2 - (1) Bu Kanun, yabancılarla ilgili iş ve işlemleri; sınırlarda, sınır kapılarında ya da Türkiye içinde yabancıların münferit koruma talepleri üzerine sağlanacak uluslararası korumayı, ayrılmaya zorlandıkları ülkeye geri dönemeyen ve kitlesel olarak Türkiye'ye gelen yabancılara acil olarak sağlanacak geçici korumayı (...) kapsar.

(2) Bu Kanunun uygulanmasında, Türkiye'nin taraf olduğu milletlerarası anlaşmalar ile özel kanunlardaki hükümler saklıdır.

(...)

Sınır dışı etmek üzere idari gözetim ve süresi

MADDE 57 - (1) 54 üncü madde kapsamındaki yabancılar, kolluk tarafından yakalanmaları hâlinde, haklarında karar verilmek üzere derhâl valiliğe bildirilir. Bu kişilerden, sınır dışı etme kararı alınması gerektiği değerlendirilenler hakkında, sınır dışı etme kararı valilik tarafından alınır. Değerlendirme ve karar süresi kırk sekiz saati geçemez.

(2) (Değişik:6/12/2019-7196/77 md.) Hakkında sınır dışı etme kararı alınanlardan; kaçma ve kaybolma riski bulunan, Türkiye'ye giriş veya çıkış kurallarını ihlal eden, sahte ya da asılsız belge kullanan, kabul edilebilir bir mazereti olmaksızın Türkiye'den çıkmaları için tanınan sürede çıkmayan, kamu düzeni, kamu güvenliği veya kamu sağlığı açısından tehdit oluşturanlar hakkında valilik tarafından idari gözetim kararı alınır ya da 57/A maddesi uyarınca idari gözetime alternatif yükümlülükler getirilir. Hakkında idari gözetim kararı alınan yabancılar, yakalamayı yapan kolluk birimince geri gönderme merkezlerine kırk sekiz saat içinde götürülür.

(3) Geri gönderme merkezlerindeki idari gözetim süresi altı ayı geçemez. Ancak bu süre, sınır dışı etme işlemlerinin yabancıнын iş birliği yapmaması veya ülkesiyle ilgili doğru bilgi ya da belgeleri vermemesi nedeniyle tamamlanamaması hâlinde, en fazla altı ay daha uzatılabilir.

(4) (Değişik:6/12/2019-7196/77 md.) İdari gözetimin devamında zaruret olup olmadığı, valilik tarafından her ay düzenli olarak değerlendirilir. Gerek görüldüğünde, otuz günlük süre beklenmez. İdari gözetimin devamında zaruret görülmeyen yabancılar için idari gözetim derhâl sonlandırılır. Bu yabancılar, 57/A maddesi uyarınca idari gözetime alternatif yükümlülükler getirilir.

(5) İdari gözetim kararı, idari gözetim süresinin uzatılması ve her ay düzenli olarak yapılan değerlendirmelerin sonuçları, gerekçesiyle birlikte yabancıya veya yasal temsilcisine ya da avukatına tebliğ edilir. Aynı zamanda, idari gözetim altına alınan kişi bir avukat tarafından temsil edilmiyorsa, kendisi veya yasal temsilcisi kararın sonucu, itiraz usulleri ve süreleri hakkında bilgilendirilir.

(6) İdari gözetim altına alınan kişi veya yasal temsilcisi ya da avukatı, idari gözetim kararına karşı sulh ceza hâkimine başvurabilir. Başvuru idari gözetimi durdurmaz. Dilekçenin idareye verilmesi hâlinde, dilekçe yetkili sulh ceza hâkimine derhâl ulaştırılır. Sulh ceza hâkimi incelemeyi beş gün içinde sonuçlandırır. Sulh ceza hâkiminin kararı kesindir. İdari gözetim altına alınan kişi veya yasal temsilcisi ya da avukatı, idari gözetim şartlarının ortadan kalktığı veya değiştiği iddiasıyla yeniden sulh ceza hâkimine başvurabilir.

(7) İdari gözetim işlemine karşı yargı yoluna başvuranlardan, avukatlık ücretlerini karşılama imkânı bulunmayanlara, talepleri hâlinde 19/3/1969 tarihli ve 1136 sayılı Avukatlık Kanunu hükümlerine göre avukatlık hizmeti sağlanır.

(8) (Ek:6/12/2019-7196/77 md.) İdari gözetim altına alınan yabancıların uyruklarının tespit edilmesi amacıyla elektronik ve iletişim cihazları incelenebilir. İnceleme sonucunda elde edilen veriler bu amaç dışında kullanılmaz.

(...)

Kayıt ve kontrol

MADDE 69 - (1) Uluslararası koruma başvuruları valiliklerce kaydedilir.

(2) Başvuru sahibi kayıt esnasında kimlik bilgilerini doğru olarak bildirmek ve varsa kimliğini ispatlayacak belge ve seyahat dokümanlarını yetkili makamlara teslim etmekle yükümlüdür. Bu yükümlülüğün yerine getirilmesini sağlamak amacıyla, başvuru sahibinin üzerinde ve eşyalarında kontrol yapılabilir.

(3) Kayıt esnasında başvuru sahibinin kimliğine ilişkin belge olmaması hâlinde, kimlik tespitinde kişisel verilerinin karşılaştırılmasından ve yapılan araştırmalardan elde edilen bilgiler kullanılır. Kimlik tespit araştırmaları sonucunda da kimliğine dair bilgi elde edilememesi hâlinde, başvuranın beyanı esas alınır.

(4) Kayıt esnasında; başvuru sahibinin menşe veya ikamet ülkesini terk etme sebepleri, ülkesini terktikten sonra başından geçen ve başvuru yapmasına neden olan olaylar, Türkiye'ye giriş şekli, kullandığı yol güzergâhları ve vasıta bilgileri, daha önceden başka bir ülkede uluslararası korumaya başvurmuş veya korumadan yararlanmışsa, bu başvuru veya korumaya ilişkin bilgi ve belgeleri alınır.

(5) Mülakat zamanı ve yeri kayıt esnasında bildirilir.

(6) Kamu sağlığını tehlikeye düşürebileceği değerlendirilen başvuru sahibi sağlık kontrolünden geçirilir.

(7) (Mülga:18/10/2018-7148/35 md.)

(...)

Başvurunun geri çekilmesi veya geri çekilmiş sayılması

MADDE 77 - (1) Başvuru sahibinin;

- a) Başvurusunu geri çektiğini yazılı olarak beyan etmesi,
- b) Mazeretsiz olarak mülakata üç defa üst üste gelmemesi,
- c) İdari gözetim altında bulunduğu yerden kaçması,
- ç) Mazeretsiz olarak; bildirim yükümlülüğünü üç defa üst üste yerine getirmemesi, belirlenen ikamet yerine gitmemesi veya ikamet yerini izinsiz terk etmesi,
- d) Kişisel verilerinin alınmasına karşı çıkması,
- e) Kayıt ve mülakattaki yükümlülüklerine uymaması,

hâllerinde başvurusu geri çekilmiş kabul edilerek değerlendirme durdurulur.

(...)

Gizlilik ilkesi ve kişisel dosyaya erişim

MADDE 94 - (1) Başvuru sahibinin ve uluslararası koruma statüsü sahibi kişinin tüm bilgi ve belgelerinde gizlilik esastır.

(2) Ancak, başvuru sahibi ve uluslararası koruma statüsü sahibi kişi ile yasal temsilcisi veya avukatı, başvuru sahibi ve uluslararası koruma statüsü sahibinin kişisel dosyasında yer alan belgeleri inceleyebilir, birer örneğini alabilir. Millî güvenlik ve kamu düzeninin korunması ile suç işlenmesinin önlenmesine ilişkin belgeler incelenemez ve verilemez.

(...)

Kişisel veriler

MADDE 99 - (1) Yabancılara, başvuru ve uluslararası koruma statüsü sahiplerine ait kişisel veriler, Genel Müdürlükçe veya valiliklerce ilgili mevzuata ve taraf olunan uluslararası anlaşmalara uygun olarak alınır, korunur, saklanır ve kullanılır.

6362 sayılı Sermaye Piyasası Kanunu

Resmî Gazete Tarihi : 30.12.2012

Resmî Gazete Sayısı : 28513

SERMAYE PİYASASI KANUNU

BİRİNCİ KISIM

Genel Hükümler

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç

MADDE 1 - (1) Bu Kanunun amacı; sermaye piyasasının güvenilir, şeffaf, etkin, istikrarlı, adil ve rekabetçi bir ortamda işleyişinin ve gelişmesinin sağlanması, yatırımcıların hak ve menfaatlerinin korunması için sermaye piyasasının düzenlenmesi ve denetlenmesidir.

Kapsam

MADDE 2 - (1) Sermaye piyasası araçları, bu araçların ihracı, ihraççılar, halka arz edenler, sermaye piyasası faaliyetleri, sermaye piyasası kurumları, borsalar ile sermaye piyasası araçlarının işlem gördüğü diğer teşkilatlanmış piyasalar, piyasa işleticileri, Türkiye Sermaye Piyasaları Birliği, Türkiye Değerleme Uzmanları Birliği, merkezî takas kuruluşları, merkezî saklama kuruluşları, Merkezî Kayıt Kuruluşu ve Sermaye Piyasası Kurulu bu Kanun hükümlerine tabidir. Halka açık olmayan anonim ortaklıkların halka arz edilmeyen pay ihraçları, bu Kanun kapsamı dışındadır.

(2) Bu Kanunda ve bu Kanuna dayanılarak yürürlüğe konulan ikincil mevzuatta hüküm bulunmayan ve diğer kanunlarda bu Kanunun uygulanmayacağı belirtilmiş hâllerde genel hükümler uygulanır.

(...)

ÜÇÜNCÜ KISIM

Sermaye Piyasası Kurumları ve Faaliyetleri

BİRİNCİ BÖLÜM

Genel Hükümler

Sermaye piyasası faaliyetleri

MADDE 34 - (1) Sermaye piyasası faaliyetleri, sermaye piyasası kurumlarının bu Kanun kapsamındaki faaliyetleri, bu Kanun kapsamına giren yatırım hizmetleri ve faaliyetleri ile bunlara ek olarak sunulan yan hizmetlerden oluşur.

Sermaye piyasası kurumları

MADDE 35 - (1) Bu Kanuna göre faaliyette bulunabilecek sermaye piyasası kurumları aşağıda gösterilmiştir:

- a) Yatırım kuruluşları
 - b) Kolektif yatırım kuruluşları
 - c) Sermaye piyasasında faaliyette bulunacak bağımsız denetim, değerlendirme ve derecelendirme kuruluşları
 - ç) Portföy yönetim şirketleri
 - d) İpotek finansmanı kuruluşları
 - e) Konut finansmanı ve varlık finansmanı fonları
 - f) Varlık kiralama şirketleri
 - g) Merkezî takas kuruluşları
 - ğ) Merkezî saklama kuruluşları
 - h) Veri depolama kuruluşları
 - ı) Kuruluş ve faaliyet esasları Kurulca belirlenen diğer sermaye piyasası kurumları
- (...)

Merkezî Kayıt Kuruluşu

MADDE 81 - (1) Merkezî Kayıt Kuruluşu, sermaye piyasası araçlarının kaydileştirilmesine ilişkin işlemleri gerçekleştirmek, kaydileştirilen bu araçları ve bunlara bağlı hakları, elektronik ortamda, üyeler ve hak sahipleri itibarıyla kayden izlemek, bu araçların merkezî saklamasını yapmak üzere kurulmuş, özel hukuk tüzel kişiliğini haiz anonim şirkettir.

(2) MKK'nın kuruluş, faaliyet, üyelik, çalışma ve denetim esasları, gelirleri ve kâr payı dağıtım esasları Kurul tarafından çıkarılacak bir yönetmelikle düzenlenir.

(3) MKK, birinci fıkrada yer alan görevlerin yanı sıra aşağıda sayılan faaliyetleri de yerine getirir:

a) 6102 sayılı Kanun ve ilgili diğer mevzuatta yer alan kurumsal yönetim ilkelerine şirketlerin uyumunu sağlamaya yönelik olarak şirketler ile ortaklarının ve yatırımcılarının iletişiminin sağlanabileceği elektronik bir platform oluşturmak

b) Sermaye piyasalarına ilişkin verilerin tek bir noktada toplanmasını sağlamaya yönelik elektronik bir veri bankası oluşturmak, Kurulun belirleyeceği ilkeler çerçevesinde verilerin kullanımını sağlamak

c) Kurul tarafından sermaye piyasası ve ilgili mevzuat çerçevesinde verilen diğer görevleri ve düzenlemelerin gerektirdiği işlemleri yapmak

ç) İlgili mevzuata göre yetkilendirilmek kaydıyla, lisanslı depolar tarafından düzenlenen ürün senetlerinin kaydileştirilmesine, bunların ve bunlara bağlı hakların elektronik ortamda kayden izlenmesine ilişkin işlemleri yürütmek ve bunlara ilişkin platform oluşturmak

(4) Kurul tarafından çıkarılan düzenlemeler çerçevesinde MKK, iş ve işlemleri ile ilgili olarak gerekli gördüğü hususlarda üyelerinden bilgi ve belge istemeye ve inceleme yapmaya yetkilidir. Üyeler, MKK'nın görev alanına giren hususlarda özel mevzuatında yer alan hükümlere dayanarak bilgi vermekten imtina edemezler.

(5) MKK ve üyeleri, kayıtların yanlış tutulmasından dolayı hak sahiplerinin uğrayacağı zararlardan kusurları oranında sorumludur.

(6) Kurul, MKK'nın gözetim ve denetim merciidir. Kurul, sermaye piyasası araçlarının kayden izlenmesi ile gerekli gördüğü diğer hususların yerine getirilmesini, her türlü bilgi ve belgenin yazılı ya da elektronik ortamda, talebi üzerine veya düzenli olarak gönderilmesini MKK ile bu kuruluşun üyelerinden isteyebilir.

(...)

Veri depolama kuruluşları

MADDE 87 - (1) Sistemik riskin gözetimi ve finansal istikrarın korunması amacıyla, Kurul, sermaye piyasasında gerçekleştirilen işlemlere ilişkin olarak, bu işlemleri gerçekleştirenlerden, bu işlemlere ilişkin bilgilerin, belirleyeceği şekil ve içerikte, doğrudan kendisine veya yetkilendireceği bir veri depolama kuruluşuna bildirilmesini isteyebilir. Bu madde kapsamında, bildirim yapmakla yükümlü olanlar, özel mevzuatındaki gizlilik ve sır saklama yükümlülüklerini ileri sürerek talep edilen bilgileri vermekten imtina edemez.

(2) Bildirim Kurul tarafından yetkilendirilen bir veri depolama kuruluşuna yapılması durumunda, ilgili veri depolama kuruluşunun yükümlülüğü, bilgilerin hangi şekil ve ortamda tutulacağı ile bu madde kapsamındaki görevlerine yönelik faaliyet usul ve esasları Kurulca yapılacak düzenleme ile belirlenir.

(3) Veri depolama kuruluşları nezdindeki bilgilerin kamu tüzel kişileri dâhil üçüncü kişiler ile paylaşımı Kurulun onayına tabidir. Bu fıkranın uygulanmasında kişisel verilerin kullanılmasına ilişkin mevzuata riayet edilir.

(4) Kurul, veri depolamada etkinliğin artırılması amacıyla, Türkiye’de finansal işlem gerçekleştiren gerçek ve tüzel kişilerin, Kurulca belirlenecek bir kurumdan tanımlayıcı bir kod veya numara almalarını zorunlu tutabilir. Bu fıkranın uygulanmasına ilişkin usul ve esaslar Kurulca düzenlenir.

(...)

6328 sayılı Kamu Denetçiliği Kurumu Kanunu

Resmî Gazete Tarihi : 29.06.2012

Resmî Gazete Sayısı : 28338

KAMU DENETÇİLİĞİ KURUMU KANUNU

BİRİNCİ BÖLÜM

Genel Hükümler

Amaç

MADDE 1 - (1) Bu Kanunun amacı; kamu hizmetlerinin işleyişinde bağımsız ve etkin bir şikâyet mekanizması oluşturmak suretiyle, idarenin her türlü eylem ve işlemleri ile tutum ve davranışlarını; insan haklarına dayalı adalet anlayışı içinde, hukuka ve hakkaniyete uygunluk yönlerinden incelemek, araştırmak ve önerilerde bulunmak üzere Kamu Denetçiliği Kurumunu oluşturmaktır.

Kapsam

MADDE 2 - (1) Bu Kanun; Kamu Denetçiliği Kurumunun kuruluş, görev ve çalışma usullerine ilişkin ilkeler ile Kamu Başdenetçisi ve kamu denetçilerinin niteliklerine, seçimlerine, özlük haklarına ve Kurum personelinin atanmaları ile özlük haklarına ilişkin hükümleri kapsar.

(...)

Bilgi ve belge istenmesi

MADDE 18 - (1) Kurumun inceleme ve araştırma konusu ile ilgili olarak istediği bilgi ve belgelerin, bu isteğin tebliğ edildiği tarihten itibaren otuz gün içinde verilmesi zorunludur. Bu süre içinde istenen bilgi ve belgeleri haklı bir neden olmaksızın vermeyenler hakkında Başdenetçi veya denetçinin başvurusu üzerine ilgili merci soruşturma açar.

(2) Devlet sırrı veya ticari sır niteliğindeki bilgi ve belgeler, yetkili mercilerin en üst makam veya kurulunca gerekçesi belirtilmek suretiyle verilmeyebilir. Ancak, Devlet sırrı niteliğindeki bilgi ve belgeler Başdenetçi veya görevlendireceği denetçi tarafından yerinde incelenebilir.

(...)

6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun

Resmî Gazete Tarihi : 14.04.2011

Resmî Gazete Sayısı : 27905

SPORDA ŞİDDET VE DÜZENSİZLİĞİN ÖNLENMESİNE DAİR KANUN

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç

MADDE 1 - (1) Bu Kanunun amacı; müsabaka öncesinde, esnasında veya sonrasında spor alanları ile bunların çevresinde, taraftarların sürekli veya geçici olarak gruplar halinde buldukları yerlerde veya müsabakanın yapılacağı yere gidiş ve geliş güzergâhlarında şiddet ve düzensizliğin önlenmesidir.

Kapsam

MADDE 2 - (1) Bu Kanun; müsabaka öncesinde, esnasında veya sonrasında, spor alanları ile bunların çevresinde, taraftarların sürekli veya geçici olarak gruplar halinde buldukları yerlerde veya müsabakanın yapılacağı yere gidiş ve geliş güzergâhlarında, takımların kamp yaptığı yerlerde uygulanacak güvenlik önlemlerini, şike, teşvik primi ve diğer yasak fiil ve davranışları, bunlara uygulanacak yaptırımları, spor kulüplerinin, spor kulübü yöneticilerinin, sporcularının ve diğer görevlilerinin, genel kolluk veya özel güvenlik görevlilerinin, hakemlerin, taraftarların, taraftar derneklerinin, taraftar temsilcilerinin, spor federasyonlarının, yazılı veya görsel ya da işitsel kitle iletişim kuruluşları ile mensuplarının ve diğer ilgili kişi ve kurumların spor müsabakalarında şiddet ve düzensizliğin önlenmesine ilişkin hususlardaki görev ve sorumluluklarını kapsar.

(...)

Müsabaka ve seyir alanlarının güvenlik ve düzenine ilişkin tedbirler

MADDE 5 - (1) Ev sahibi spor kulüpleri;

a) Müsabaka ve seyir alanlarında sağlık ve güvenliğe,

b) Müsabakanın yapılacağı yerde konuk takım seyircilerine bağımsız bir bölüm ayırmak ve taraftarlar arasında temas olmamasını sağlamaya yönelik olarak, ilgili spor federasyonları ve uluslararası spor federasyonları tarafından belirlenen önlemleri almakla yükümlüdür.

(2) Spor kulüpleri, müsabakanın güvenliğini sağlamak amacıyla il veya ilçe spor güvenlik kurullarının kendileriyle ilgili olarak aldığı kararları yerine getirmekle yükümlüdür.

(3) Birinci ve ikinci fıkralar kapsamındaki yükümlülüklerin yerine getirilmesi amacıyla özellikle;

a) Müsabaka ve seyir alanlarına, seyri engellemeyecek şekilde ve federasyonun bağlı olduğu uluslararası federasyonun talimatlarına uygun olarak seyirci ile müsabakanın yapıldığı yer arasına tel, duvar, bariyer ve benzeri fizikî engeller konulabilir.

b) Fizikî engeller, ilgili spor güvenlik biriminin görüşü alınarak, il veya ilçe spor güvenlik kurullarının kararı ile kaldırılabilir.

c) Seyir alanlarında, çocuklar ve engellilerin müsabakaları izleyebilmeleri için durumlarına uygun yerler tahsis edilir.

ç) (Değişik:4/7/2019-7182/3 md.) Seyir alanlarında seyircilerin oturma yerleri numaralandırılır. Bilet satışları koltuk numarasıyla ilişkilendirilerek yapılır. Seyircilerin ayakta seyredebileceği şekilde düzenlenmiş numaralı alanla ilişkilendirmek suretiyle de bilet satışı yapılabilir. Bu uygulamaya, ilgili federasyon ve İçişleri Bakanlığının görüşü alınarak Bakanlıkça karar verilir. Seyir alanlarına kapasitenin üzerinde veya biletsiz seyirci alınamaz.

(4) (Değişik cümle:4/7/2019-7182/3 md.) Futbol dalında en üst lig ile bir altındaki ligde seyir alanlarına girişi sağlayacak biletler, elektronik sistem üzerinden usul ve esasları Hazine ve Maliye Bakanlığınca belirlenen şekilde elektronik olarak oluşturulur. Bilet satın almak isteyen kişilerle ilgili olarak, üzerinde adı, soyadı, Türkiye Cumhuriyeti kimlik numarası ve fotoğrafı olan bir elektronik kart oluşturulur. Kişinin yabancı olması halinde kart üzerinde Türkiye Cumhuriyeti kimlik numarası yerine uyruğu olduğu devletin adı ile Türkiye'ye giriş yaptığı pasaportun seri numarası kaydedilir. Bilet satışları kişilere özgü elektronik kart üzerinden yapılabilir. Spor müsabakalarına, kişi ancak adına düzenlenen elektronik kart ile izleyici olarak girebilir. Spor müsabakasına izleyici olarak girecek kişilerin kontrolünü ev sahibi kulüp yapmakla yükümlüdür. Bu yükümlülük ev sahibi olmayan müsabakalarda, müsabakaya katılan her iki kulüp; milli müsabakalarda ise, ilgili federasyon tarafından yerine getirilir.

(5) Müsabaka ve seyir alanlarında; güvenliğin sağlanması ve bu Kanuna aykırı davranışların tespiti amacıyla, gerekli teknik donanımlar kurulur. Kameralar ve benzeri teknik donanımların yerleştirilecekleri yerler ve sayıları il veya ilçe spor güvenlik kurulları tarafından belirlenir.

(6) (Değişik:4/7/2019-7182/3 md.) Futbol dalında en üst lig ile bir altındaki ligde bulunan kulüpler, dördüncü ve beşinci fıkralardaki sistemle ilgili teknik donanımları kendi kullanımındaki müsabaka ve seyir alanlarında kurmakla yükümlüdür. Aynı yükümlülükler basketbol, voleybol ve hentbol dallarındaki en üst ligde bulunan kulüplerin kendi kullanımındaki müsabaka ve seyir alanları bakımından da geçerlidir; ancak bu spor dallarında dördüncü fıkrada öngörülen elektronik kart ve elektronik bilete ilişkin hükümlerin uygulanmasına ilgili federasyonun görüşü alınarak Bakanlık tarafından; en üst iki futbol ligi dışındaki liglerde ise Türkiye Futbol Federasyonu tarafından karar verilir.

(7) Futbolda en üst profesyonel lig ve bir altındaki ligde bulunan kulüplerin müsabakalarının yapıldığı müsabaka alanlarında; bu Kanunda sayılan diğer spor branşlarında ise uluslararası spor müsabakalarının yapıldığı müsabaka alanlarında ev sahibi ve misafir takım için ayrı ayrı olmak ve gerektiğinde kullanılmak üzere azami yirmi kişi kapasiteli en az iki tane bekletme odası ile genel kolluk görevlileri ile özel güvenlik görevlilerinin kullanımına açık tutulacak güvenlik kameraları ve anons sistemlerinin yönetildiği yeteri kadar kontrol odasının oluşturulması zorunludur. Kontrol odasında federasyon ve spor kulübü temsilcileri de bulunur. Kayıt altına alınan görüntü ve dokümanların birer örneği, müsabakanın sonunda ilgili spor güvenlik birimine, federasyona ve her iki kulüp temsilcisine verilir.(8) Dördüncü, beşinci ve yedinci fıkralarda belirtilen güvenlik sistemlerinin ve odalarının giderleri, en üst profesyonel futbol ligi ve bir altındaki ligdeki kulüplerin kendileri tarafından; basketbol, voleybol ve hentbol dalları için ise spor tesisinin kullanım hakkına sahip olan kulüp ya da kuruluş tarafından karşılanır.

(9) Müsabaka ve seyir alanlarında hangi güvenlik sistemi veya teknik donanımın uygulanacağı ilgili federasyonun bağlı olduğu uluslararası spor örgütlerinin düzenlemeleri çerçevesinde yönetmelikle belirlenir.

(10) Müsabaka ve seyir alanları ile çevresinde; bu alanlara sokulması yasak maddelere ve eşyalara, yasak olan davranışlara ve bu alanlarda elektronik takibin yapıldığına ilişkin uyarı levhalarına yer verilir. Bu yükümlülük ilgili müsabaka ve seyir alanı kullanımında olan spor kulübü tarafından yerine getirilir.

(11) Dördüncü fıkrada belirtilen elektronik kart uygulaması ile ilgili olarak;

a) Bilet organizasyonu ve seyircilerin müsabaka alanlarına giriş ve çıkışına ilişkin kontrol ve denetim yetkisi federasyonlara ait olup federasyonlar bu amaçla bünyelerinde merkezi kontrol sistemi oluşturur. Elektronik kart oluşturulmak amacıyla alınacak kişisel bilgiler federasyon bünyesinde oluşturulan merkezi veri tabanında tutulur. Bu veri tabanı Hazine ve Maliye Bakanlığı ve İçişleri Bakanlığı erişimine açıktır.

b) Elektronik kart ile elektronik kart kapsamında satışı gerçekleştirilecek biletlerin basım, satış ve dağıtımına ilişkin yerel uygulamalar kulüpler tarafından, sistem üzerinden merkezi satışları ise ilgili federasyonlar tarafından gerçekleştirilir. (Ek cümle:4/7/2019-7182/3 md.) Spor müsabakaları için ilgili federasyon, spor kulüpleri ve yetkili diğer kişiler tarafından uygun görülen yerler ve görevliler dışında, her ne suretle olursa olsun bilet satışı yapılamaz.c) (Ek cümleler:4/7/2019-7182/3 md.) İlgili federasyonlar elektronik kart almak amacıyla verilen bilgileri, bu Kanun kapsamındaki faaliyet alanıyla sınırlı olarak kulüpler adına paylaşabilir. Paylaşılan bilgiler 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununa aykırı olarak işlenemez ve kullanılamaz. (İptal cümle: Anayasa Mahkemesi'nin 12/11/2015 tarihli ve E.: 2014/196, K.: 2015/103 sayılı Kararı ile.) Merkezi pazarlama ve bilet satışından elde edilecek gelirler kulüplere ait olup federasyon ya da yetki verdiği üçüncü kişiler nezdinde oluşacak bu gelirler kamu kurum ve kuruluşlara ilişkin alacaklar ile kulüplerle bankalar arasında yapılan yeniden yapılandırma işlemleri kapsamındaki tüm banka alacakları hariç olmak üzere haczedilemez, devir ve temlik edilemez. Federasyonlar bu fıkra kapsamında belirtilen yetkilerini kısmen veya tamamen üçüncü kişilere devredebilir ve teknik hizmet satın alabilir.

(...)

**6114 sayılı Ölçme, Seçme ve Yerleştirme Merkezi Başkanlığının Teşkilat ve Görevleri Hakkında
Kanun**

Resmî Gazete Tarihi : 03.03.2011

Resmî Gazete Sayısı : 27863

ÖLÇME, SEÇME VE YERLEŞTİRME MERKEZİ HİZMETLERİ HAKKINDA KANUN

BİRİNCİ BÖLÜM

Amaç ve Tanımlar

Amaç

MADDE 1 - (1) Bu Kanunun amacı, Ölçme, Seçme ve Yerleştirme Merkezi Başkanlığı tarafından yapılacak her türlü sınav ve yerleştirmeler ve bu sınavlarda görev alanların yetki ve sorumluluklarına ilişkin usul ve esasları düzenlemektir.

(...)

Personel rejimi ve mali hükümler

MADDE 6 - (1) (Mülga: 2/7/2018-KHK-703/84 md.)

(2) Başkana, Yükseköğretim Kurulu Başkan Vekiline ödenen aylık ve sosyal yardımları; Başkan yardımcılara, Yükseköğretim Yürütme Kurulu üyelerine ödenen aylık ve sosyal yardımları geçmemek üzere, Cumhurbaşkanı tarafından tespit edilecek tutarda ödeme yapılır. (Değişik son cümle: 4/7/2012-6353/49 md.) Başkan ve Başkan yardımcıları tam zamanlı görev yapar ve görevleri süresince, lisansüstü eğitim faaliyetleri ve bu Kanun uyarınca kurulan şirket organlarında alınan görevler hariç, başka hiçbir kurum veya kuruluşta ücretli iş göremez. Bunlara, şirket organlarında aldıkları görevleri nedeniyle şirket kaynaklarından yapılabilecek aylık ödeme tutarı, 22/1/1990 tarihli ve 399 sayılı Kanun Hükmünde Kararnamenin 34 üncü maddesine göre kamu iktisadi teşebbüsleri yönetim kurulu başkan ve üyelerine ödenen miktarları geçemez.

(3) (Mülga: 2/7/2018-KHK-703/84 md.)

(4) (Mülga: 11/10/2011-KHK-666/1 md.)

(5) (Mülga: 2/7/2018-KHK-703/84 md.)

(6) (Mülga: 2/7/2018-KHK-703/84 md.)

(7) (Mülga: 2/7/2018-KHK-703/84 md.)

(8) (Mülga: 2/7/2018-KHK-703/84 md.)

(9) (Mülga birinci ila yedinci cümleler: 2/7/2018-KHK-703/84 md.) (...) (Ek cümleler: 2/12/2016-6764/68 md.) 8/4/1929 tarihli ve 1416 sayılı Ecnebi Memleketlere Gönderilecek Talebe Hakkında Kanun uyarınca Başkanlık adına mecburi hizmet karşılığı yurt dışına gönderilenlerden doktora öğrenimlerini başarıyla tamamladıktan sonra mecburi hizmet yükümlülüklerini ifa etmek üzere Başkanlığın ilgili kadrolarına atananlar, bu fıkra kapsamında belirlenen kadro sayısına bağlı kalmaksızın sözleşmeli yerli uzman olarak da istihdam edilebilir. Bu şekilde istihdam edilenler, bu görevleri süresince aylıksız izinli sayılırlar ve aylıksız izinli sayıldıkları kadro unvanları dikkate alınmak suretiyle 5510 sayılı Kanununun 4 üncü maddesinin birinci fıkrasının (c) bendine tabi olmaya devam ederler. Bu görevlerde geçen hizmet süreleri kazanılmış hak aylık derece ve kademelerinde değerlendirilir. Bunlara sözleşmeli personel olarak çalıştıkları süreler için iş sonu tazminatı ödenmez ve bu şekilde çalışılan süreler bunların emekli ikramiyelerinin hesabında dikkate alınır.

(10) Bu Kanunun yürütülmesinde görev alan kamu görevlileri ile hizmet satın alınması durumunda yüklenici özel hukuk tüzel kişilerinin ilgili personeli, göreve getirilmeden önce imzalayacakları bir gizlilik sözleşmesi ile görevlerini yerine getirmeleri sırasında edindikleri kamuya, ilgililere ve üçüncü kişilere ait gizlilik taşıyan bilgileri, kişisel verileri, Başkanlıkla ve Başkanlık tarafından yapılan sınavlarla ilgili gizlilik taşıyan bilgileri, ticari sırları ve bunlara ait belgeleri bu konuda kanunen yetkili kılınan mercilerden başkasına açıklayamaz, kendilerinin veya üçüncü kişilerin yararına kullanamaz. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

(11) (Mülga: 2/7/2018-KHK-703/84 md.)

(12) (Mülga: 2/7/2018-KHK-703/84 md.)

(13) (Değişik: 2/12/2016-6764/68 md.) Başkanlıkça yurtiçinde ve yurtdışında sınav soru havuzunda yer alacak soruların hazırlanmasında görevlendirilenlere ve cevapların değerlendirilmesinde katkısı olanlara soru ücreti; 2 nci maddenin birinci fıkrasının (h) bendi uyarınca oluşturulan koordinatörlüklerin koordinatörüne ve diğer personeline, bina sınav sorumluları ile bina yöneticilerine, salon başkanlarına, gözetmenlere, sınav güvenliğini sağlayan kolluk kuvvetlerine, kapalı dönem çalışanlara ve sınav sürecinde görev alan diğer personele sınav ücreti ödenir. Kadrolu veya sözleşmeli çalışan personele ayrıca soru ücreti ödenmez. Memuriyet mahalli dışına sınav görevi için görevlendirilenlerden sınav ücreti ödenenlere 10/2/1954 tarihli ve 6245 sayılı Harcırah Kanunu

hükümlerine göre sadece yol gideri ödenir. Sınav ve soru ücreti tutarına ilişkin usul ve esaslar; sınavın ve soruların özelliği, sınava katılanların sayısı, görev ve yetkileri, sınav yerinin özelliği ve çalışma süresi gibi hususlar değerlendirilmek suretiyle, Cumhurbaşkanı tarafından belirlenir. Bu fıkrada yer alan hükümler, yükseköğretim kurumlarının açık öğretim sınavları, kamu kurum ve kuruluşları ile özel hukuk tüzel kişilerinin talepleri üzerine yükseköğretim kurumlarınca yapılan sınavlar hakkında da uygulanır.(7)

(14) Ölçme, Seçme ve Yerleştirme Merkezi Başkanlığı tarafından yapılan merkezi sistem sınavlarında Millî Eğitim Bakanlığına bağlı okul ve kurum müdürlükleri ile koordinatörlüklerce, her bir başvuru kaydı için adaylardan alınacak başvuru, tercih, şifre verme gibi hizmet bedeli, okulların ve koordinatörlüklerin sınav hizmetlerine yönelik ihtiyaçlarında kullanılmak üzere koordinatörlük ile okul ve kurum müdürlüklerinin bağlı olduğu il veya ilçe millî eğitim müdürlükleri nezdinde açılan hesaba aktarılır. Başvuru, tercih, şifre verme gibi hizmet bedellerinin tahsiline ve söz konusu tutarların harcanmasına ilişkin usul ve esaslar Millî Eğitim Bakanlığı ve Ölçme, Seçme ve Yerleştirme Merkezi Başkanlığı arasında imzalanacak protokolle, koordinatörlüklere ilişkin usul ve esaslar Ölçme, Seçme ve Yerleştirme Merkezi Başkanlığınca Maliye Bakanlığının görüşü alınarak belirlenir. Bu harcamalar Sayıştay tarafından denetlenir. (Ek cümle: 2/12/2016-6764/68 md.) Millî Eğitim Bakanlığına bağlı okul ve kurum müdürlükleri ile sınav koordinatörlüklerinin bu fıkra kapsamındaki mal ve hizmet alımlarına ilişkin ödemeleri nedeniyle düzenledikleri kâğıtlar damga vergisinden istisnadır.

(15) Başkan, Başkan yardımcıları, Yönetim Kurulu üyeleri ile Başkanlık Müşaviri, Daire Başkanı, I. Hukuk Müşaviri, Basın ve Halkla İlişkiler Müşaviri, Hukuk Müşaviri, Ölçme, Seçme ve Yerleştirme Merkezi Uzmanı ve Ölçme, Seçme ve Yerleştirme Merkezi Uzman Yardımcısı ile Şube Müdürü olarak çalıştırılanlar, sekizinci ve dokuzuncu fıkralarda belirtilenler, Başkanlıktaki görevlerinin sona ermesinden itibaren iki yıl süreyle, Başkanlık tarafından yapılan sınavlara yönelik hazırlık kursları veya yayınlarla ilgili faaliyet gösteren gerçek kişiler ile özel hukuk hükümlerine tâbi tüzel kişilerde ya da bunların iştiraklerinde görev alamaz ya da bu tür işlere ortak olamaz ve bu tüzel kişilerden ya da iştiraklerden gelir sağlayacak ya da sağlayabilecek doğrudan ya da dolaylı ilişkiye giremez. Bunların eşleri, çocukları ile ikinci dereceye kadar kan ve kayın hısımları, bunların görevleri süresince, Başkanlık tarafından yapılan sınavlara yönelik hazırlık kursları veya yayınlarla ilgili faaliyet gösteren kamu kurum ve kuruluşları dışındaki tüzel kişiliklerde ya da bunların iştiraklerinde görev alamaz ya da bu tür işlere ortak olamaz ve bu tüzel kişilerden ya da iştiraklerden gelir sağlayacak ya da sağlayabilecek doğrudan ya da dolaylı ilişkiye giremez. (Ek cümle: 2/12/2016-

6764/68 md.) Soru hazırlama ve denetleme faaliyetlerine ilişkin birimlerde görev yapanlardan bu fıkra hükümlerine aykırı durumları tespit edilenler başka birimlerde görevlendirilir.

(16) (Mülga: 2/7/2018-KHK-703/84 md.)

(17) (Ek: 4/7/2012-6353/49 md.) Yurt dışı temsilcilikler bünyesinde sınav koordinatörlüğünün kurulacağı yerler ve süresi ile koordinatörlüklerin çalışma usul ve esasları, bu koordinatörlüklerde görevlendirilenlerin niteliği, görev süresi ve ödenecek ücretler, koordinatörlere yapılacak ödemeler dışında kalan diğer harcamaların neler olacağına ilişkin usul ve esaslar Cumhurbaşkanınca belirlenir.

(18) (Ek: 4/7/2012-6353/49 md.) Soru hazırlama, denetleme ve değerlendirme konularında ihtisaslaşmış yardımcı doçent, doçent ve profesör unvanlı öğretim üyeleri, üniversitelerinin muvafakati ile Başkanlığın soru hazırlama ve denetleme hizmetlerinde görevlendirilebilir. Bu şekilde görevlendirilenlerin sayısı onu geçemez. Görevlendirilenler, görev süresince kadrosunda bulunduğu üniversitede aylıksız izinli sayılırlar ve bunlara 6 ncı maddenin ikinci fıkrası uyarınca Başkan yardımcılara ödenen aylık ve sosyal yardımların yüzde doksanı tutarında ödeme yapılır. Görevleri süresince, kadrolarıyla ilgili özlük hakları devam eder ve bu süreler terfi ve emekliliklerinde hesaba katılır. Görevleri sona erenler, başka bir işleme gerek kalmaksızın üniversitedeki kadrosuna geri döner. Bu fıkra hükümlerine göre görevlendirilenlerin asli kadroları esas alınarak belirlenecek sigorta primi işveren payı veya 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun geçici 4 üncü maddesi kapsamına girenlerin emeklilik keseneği kurum karşılığı ve genel sağlık sigortası primleri Başkanlık tarafından karşılanır.

(19) (Ek: 12/7/2013-6495/53 md.) Yükseköğretim kurumlarının önlisans, lisans ve lisansüstü diploma programlarına kayıtlı öğrencilerden Başkanlıkça hizmetlerine ihtiyaç duyulanlar başvuru, tercih, sınav evrakının tanzimi ve benzeri sınav hizmetlerine yönelik geçici işlerde kısmî zamanlı olarak çalıştırılabilir. Bu şekilde çalıştırılan öğrenciler, bu çalışmalarından dolayı işçi olarak kabul edilmez. Kısmî zamanlı olarak çalıştırılan öğrencilere bir saatlik çalışma karşılığı ödenecek ücret, 22/5/2003 tarihli ve 4857 sayılı İş Kanunu gereğince on altı yaşından büyük işçiler için belirlenmiş olan günlük brüt asgarî ücreti geçemez. Kısmî zamanlı çalışma karşılığı ücret ödenmesi, Yüksek Öğrenim Kredi ve Yurtlar Kurumu tarafından verilmekte olan burs veya öğrenim kredisinin kesilmesi veya aynı Kuruma ait yurtlardan yararlanma hakkının kaldırılması sonucunu doğurmaz. Kısmî zamanlı olarak öğrenci çalıştırılmasına ilişkin haftalık çalışma süreleri ve yapılacak ücret ödemelerinin tutarı ile diğer usul ve esaslar Maliye Bakanlığının uygun görüşü alınarak Başkanlık tarafından belirlenir. Bunlar hakkında 31/5/2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 5 inci maddesinin birinci fıkrasının (b) bendi hükmü uygulanır ve prim ödeme yükümlüsü Ölçme, Seçme

ve Yerleřtirme Merkezi Bařkanlıđıdır. Hak sahibi olarak almıř oldukları gelir ve aylıkları bu alıřmalarından dolayı kesilmez.

(20) (Ek: 2/12/2016-6764/68 md.) Bařkanlık sınav, lme, deđerlendirme ve yerleřtirme hizmetleri ile sınırlı olmak zere đretim elemanlarına proje, arařtırma ve incelemeler yaptırabilir, bilimsel raporlar hazırlatabilir. Bu hizmetlerde grev alan đretim elemanlarına (40.000) gsterge rakamının ve bir ayda yapılacak toplam olarak (60.000) gsterge rakamının memur aylıklarına uygulanan aylık katsayısı ile arpımı sonucu elde edilecek tutarı gememek zere Bařkanlıka belirlenecek tutarda, diđer kanunlardaki dzenleme ve kısıtlamalara tabi olmaksızın dođrudan deme yapılır. Bu fıkra uyarınca yapılacak demelere iliřkin usul ve esaslar Maliye Bakanlıđının uygun grř alınıarak Ynetim Kurulu tarafından belirlenir.

(...)

Sınav gvenliđi

MADDE 9 - (1) Sınav soruları ile bunları hazırlamakla grevlendirilmiř olan kiřilerin kimlikleri gizli tutulur. (Deđerliřik ikinci cmle: 2/12/2016-6764/71 md.) Bařkanlık, gizlilik ve gvenliđin sađlanması iin sınav ncesinde, sınav sırasında ve sonrasında gerekli btn tedbirleri alır, ilgili tm kurumlarla iřbirliđi yapar, ilgili kamu kurum ve kuruluřları ile yapılacak protokoller erevesinde veri tabanlarında sınav ve yerleřtirmeler iin ihtiya duyulan kiřisel veri sorgulaması yapabilir. Soru havuzundaki sorular hibir kořul altında kısmen ya da tamamen nc řahıslara verilmez. Adli ve idari soruřturma ve kovuřturmalarda soru havuzuna eriřim iin Cumhurbaşkanı'nın izni gereklidir.

(2) Sorular ve cevapları, yapılan sınav sona erdikten sonra Ynetim Kurulu kararına istinaden zel eriřim usulleri ile adaylara aıklanabilir. (Mlga ikinci cmle: 12/7/2013-6495/53 md.) (...) (Ek cmleler: 2/12/2016-6764/71 md.) Ancak deneme soruları ve bu sorulara iliřkin bilgi ve belgeler sınav sonrasında hibir surette aıklanmaz ve paylařılmaz. Bu soruları sınav sonrasında yetkilendirilmiř grevliler dıřında herhangi bir yolla ezberlemek suretiyle de olsa elde ederek kaydeden, saklayan, aktaran ya da paylařanlar hakkında 10 uncu madde hkmleri uygulanır. Bireyselleřtirilmiř veya elektronik sınavlarda soruların aıklanıp aıklanmayacađı sınav aēřuru aēamasında adaylardan alınacak onaylar erevesinde yrtlr.

(3) Soruların hazırlanması da dhil olmak zere, sınav srecinin herhangi bir aēamasında grev alanlar, ilgili mevzuat erevesinde Ynetim Kurulu tarafından belirlenen kurallara titizlikle uymakla ykmldr. (Ek cmle: 2/12/2016-6764/71 md.) Bařkanlık sınavların her aēamasında ve sınav sonrası iřlemlerde her trl yazıřma, aıklama, grevlendirme ve bilgilendirme iřlemlerini, tebliđ hkmnde

olmak üzere sınav görevlilerinin kişisel bilgi ve şifreleri ile girebildikleri Başkanlıkça sağlanan güvenli elektronik ortamlarda yapabilir.

(4) Sınavlarda güvenliğin sağlanması amacıyla, soruların hazırlandığı, basıldığı, dağıtıldığı, muhafaza edildiği ve sınavların yapıldığı binalarda sınav öncesinde ve sınav esnasında sinyal karıştırıcı ve her türlü işaret, sembol, ses ve görüntünün ve elektrik sinyallerine dönüştürülebilen her türlü verinin herhangi bir iletim sistemi vasıtasıyla gönderilmesi veya alınması yoluyla yapılan iletişimin tespiti için gerekli teknik araç ve gereçler ve benzeri diğer cihazlar kullanılabilir.

(5) Sınav güvenliğinin sağlanması amacıyla, genel kolluk görevlileri ile bunların gözetiminde olmak üzere özel güvenlik görevlileri, herhangi bir emir veya karar olmasına bakılmaksızın, adayların ve sınavın yapıldığı binaya girme hakkına sahip olan diğer kişilerin üstünü ve eşyasını teknik cihazlarla, gerektiğinde el ile kontrol etmeye ve aramaya yetkilidir. (Ek cümle: 2/12/2016-6764/71 md.) Sınav sırasında veya sınavdan sonra incelenen tutanaklar, kamera ses ve görüntüleri, telefon kayıtları, ihbarlar veya başka yollarla bu Kanun ve sınav kurallarının düzenlendiği yönetmelik veya kılavuz esaslarına aykırılık teşkil eden davranışlarının tespit edilmesi hâlinde adayın sınavı geçersiz sayılır, bu sınav veya yerleştirmeye kendisine sağlanan haklar geri alınır. Adayların ve sınav görevlilerinin sınav binalarına giriş koşulları yönetmelikle düzenlenir.

(6) Görevli olması sebebiyle sınav süresince sınav yapılan bina ve salonlara girmek isteyenler, sorulmaksızın kimliklerini ibraz etmekle yükümlüdür. (Ek cümleler: 2/12/2016-6764/71 md.) Başkanlık, adaylar ve sınav görevlilerini kapsayacak şekilde biyometrik yöntemlerle kimlik doğrulaması yapabilir. Biyometrik doğrulamanın kullanılmadığı durumlarda; adayların ve sınav görevlilerinin sınav binalarına girişinde nüfus cüzdanı veya geçerlilik süresi dolmamış pasaport haricinde ilgili kanunlarında resmi kimlik belgesi hükmünde olsa bile başka bir kimlik belgesi geçerli kabul edilmez. Biyometrik yöntemlerle kimlik doğrulama uygulamaları için elde edilen veriler sınav hizmetlerinde kullanılmak üzere saklanabilir.

(7) (Ek: 2/12/2016-6764/71 md.) Başkanlık, sınav güvenliğinin sağlanması amacıyla sınav sırasında veya sonrasında kopya amaçlı kullanıldığı yolunda şüpheler üzerine ses ve kamera görüntü çözümleri ile yazı, imza, ifade ve sınav evrakında her türlü tespit, işleme, karşılaştırma, analiz ve inceleme yapabilir veya yaptırabilir, doğruluk analizi yapmak üzere gerekli cihazları kullanabilir, her türlü cihaz içeriğinin kopyasını alabilir.

(8) (Ek: 2/12/2016-6764/71 md.) Sınavlardan sonra incelenen sınav belgelerinde, elektronik kayıtlarda veya yapılan analizlerde olağandışı bulgulara rastlanması hâlinde adaylar, maliyeti Başkanlık tarafından karşılanmak üzere Yönetim Kurulu kararı ile eşdeğer sınava çağrılabilir. Adayın sınavının

geçerli sayılıp sayılmayacağına eşdeğer sınav sonuçlarına bakılarak Yönetim Kurulu tarafından karar verilir. Çağrıya rağmen eşdeğer sınava katılmayan adayın sınavı geçersiz sayılır.

Ceza hükümleri

MADDE 10 - (1) Başkanlık tarafından yapılan sınavlarla ilgili olarak, sınav sorularının hazırlanma sürecinden başlamak üzere, görevlendirilen kişiler, başka bir kamu kurumunda veya özel kuruluşta görevli olup olmadığına bakılmaksızın, bu Kanun hükümlerine göre ifa ettiği görev bakımından, kamu görevlisi sayılır.

(2) Bu Kanun hükümlerine göre gizli olan bilgileri, hukuka aykırı olarak elde eden veya elinde bulunduran kişi, fiili daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır. Bu bilgileri ifşa eden kişi, iki yıldan beş yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

(3) Başkanlık tarafından yapılan sınavlarda;

a) Ses veya görüntü nakleden cihaz kullanmak suretiyle kopya çeken veya bu suretle kopya çekilmesine aracılık eden,

b) Başka bir adayın yerine sınava giren veya kendi yerine bir başkasının sınava girmesine katkı sağlayan,

c) Bireysel veya toplu olarak kopya çeken veya Kopya çektirilmesine imkân sağlayan,

kişi; fiili daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.

(4) Sınav sonuçlarını adayın lehine veya aleyhine olacak şekilde değiştiren kişi, fiili daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, üç yıldan sekiz yıla kadar hapis cezası ile cezalandırılır.

(5) (Değişik birinci cümle: 2/12/2016-6764/72 md.) Sınavda kopya çektiği veya bu yönde fiiller işlediği tespit edilen adayın sınavı ile çok oturumlu sınavlarda oturumların herhangi birinde kopya çektiği veya bu yönde fiiller işlediği tespit edilen adayın bu oturumlardan oluşan sınavı iptal edilir. Bu aday ve başkasının yerine sınava giren kişi, sınavın yapıldığı tarihten itibaren iki yıl süreyle Başkanlık tarafından yapılan hiçbir sınava ve yerleştirmeye aday olarak başvuramaz ve giremez. Sınavı iptal edilenlerin, iptal kararı verilmeden önce, bu sınavdaki veya yasaklılık süresi içinde girmiş olduğu Başkanlıkça yapılan bir sınavdaki başarısına dayalı olarak bir kamu görevine atanmış veya sair bir hak iktisap etmiş olması hâlinde, ilgili kurum yetkilileri tarafından görevine derhal son verilir ve

kendisine sağlanan hak geri alınır. Bu fıkrada yer alan hükümler ikinci, üçüncü ve dördüncü fıkralarda yer alan fiilleri işleyen adaylar hakkında da uygulanır.

(6) Bu maddede tanımlanan suçların bir örgütün faaliyeti çerçevesinde işlenmesi halinde, verilecek cezalar yarı oranında artırılır. Bu suçların bir tüzel kişinin faaliyeti çerçevesinde işlenmesi hâlinde, tüzel kişi hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

(7) Gizlilik ihlali suretiyle soruların elde edilmiş olmasından yararlanarak kopya çektiği için kendisiyle ilgili sınavın iptaline karar verilen adayın, soruların kimler tarafından temin edildiği ve ne suretle eline geçtiği hususunda bilgi vermesi hâlinde, Yönetim Kurulu kararıyla, sınava giriş yasağının süresi kısaltılabileceği gibi yasak tamamen de kaldırılabilir.

(8) Bu Kanun hükümlerine göre kamu görevlisi sayılan kişiler hakkında, görevleriyle bağlantılı olarak işledikleri iddia edilen suçlardan dolayı, 2/12/1999 tarihli ve 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun hükümlerine göre, soruşturma izni kararı vermeye ÖSYM Yönetim Kurulu; Yönetim Kurulu Başkan ve üyeleri hakkında ise Yükseköğretim Genel Kurulu yetkilidir.

(9) (Ek: 2/12/2016-6764/72 md.) 9 uncu maddenin birinci fıkrasında yer alan görevlilerin kimlik bilgilerini, deneme sorularını veya sınavın devam ettiği süre içinde sınavlarda sorulan soruları aynen veya değiştirerek herhangi bir ortamda paylaşan, ifşa eden, her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma ileten, yayımlayan veya işleyenler hakkında beşbin Türk lirası idari para cezası uygulanır. Fiilin tekrürü hâlinde ceza her defasında bir kat artırımlı olarak uygulanır. İdari para cezası, 5/12/1951 tarihli ve 5846 sayılı Fikir ve Sanat Eserleri Kanunundan kaynaklanan yükümlülükleri ve bu Kanununun 10 uncu maddesindeki ceza hükümlerinin uygulanmasını ortadan kaldırmaz. İdari para cezalarına ilişkin karar Yönetim Kurulu tarafından verilir. İdari para cezalarına karşı açılacak davalarda yetkili mahkeme Başkanlık merkezinin bulunduğu yerdeki idare mahkemeleridir. Bu Kanuna göre verilen idari para cezaları tebliğinden itibaren bir ay içerisinde ödenir.

(...)

6102 sayılı Türk Ticaret Kanunu

Resmî Gazete Tarihi : 14.02.2011

Resmî Gazete Sayısı : 27846

TÜRK TİCARET KANUNU

BAŞLANGIÇ

A) Kanunun uygulama alanı

I - Ticari hükümler

MADDE 1- (1) Türk Ticaret Kanunu, 22/11/2001 tarihli ve 4721 sayılı Türk Medenî Kanununun ayrılmaz bir parçasıdır. Bu Kanundaki hükümlerle, bir ticari işletmeyi ilgilendiren işlem ve fiillere ilişkin diğer kanunlarda yazılı özel hükümler, ticari hükümlerdir.

(2) Mahkeme, hakkında ticari bir hüküm bulunmayan ticari işlerde, ticari örf ve âdete, bu da yoksa genel hükümlere göre karar verir.

(...)

İKİNCİ KISIM

Ticaret Sicili

A) Kuruluş

I - Genel olarak

MADDE 24- (1) (Değişik: 15/8/2017-KHK-694/162 md.; Aynen kabul: 1/2/2018-7078/157 md.) Gümrük ve Ticaret Bakanlığı tarafından il merkezindeki ticaret ve sanayi odaları ile ticaret odalarında faaliyet gösterecek şekilde ticaret sicili müdürlükleri kurulur. Bakanlık il merkezleri dışındaki odalarda ticaret sicili müdürlükleri kurabileceği gibi müdürlüklere bağlı şubeler de kurabilir.

(2) (Ek: 15/8/2017-KHK-694/162 md.; Aynen kabul: 1/2/2018-7078/157 md.) Ticaret sicili, Bakanlığın gözetim ve denetiminde ticaret sicili müdürlükleri ve şubeleri tarafından tutulur.

(3) Ticaret sicili kayıtlarının elektronik ortamda tutulmasına ilişkin usul ve esaslar Kanununun 26 ncı maddesine göre çıkarılacak yönetmelikte gösterilir. Bu kayıtlar ile tescil ve ilan edilmesi gereken

içeriklerin düzenli olarak depolandığı ve elektronik ortamda sunulabilen merkezi ortak veri tabanı, Gümrük ve Ticaret Bakanlığı ile Türkiye Odalar ve Borsalar Birliği nezdinde oluşturulur.

(4) Ticaret sicili müdürlüğünün kurulmasında aranacak şartlar ve odalar arasında sicil işlemleri ile ilgili olarak varlığı gerekli işbirliğinin sağlanmasına ilişkin esaslar, Gümrük ve Ticaret Bakanlığınca çıkarılacak bir tebliğle düzenlenir.

(5) (Ek: 26/6/2012-6335/3 md.) Ticaret sicili kayıt işlemlerinin elektronik ortamda yapılması için toplanması ve işlenmesi gerekli olan kişisel veriler, kişisel verilerin korunması ve bilgi güvenliğinin sağlanmasına ilişkin mevzuata uygun bir şekilde korunur.

(...)

DÖRDÜNCÜ KISIM

Haksız Rekabet

A) Genel olarak

I - Amaç ve ilke

MADDE 54- (1) Haksız rekabete ilişkin bu Kısım hükümlerinin amacı, bütün katılanların menfaatine, dürüst ve bozulmamış rekabetin sağlanmasıdır.

(2) Rakipler arasında veya tedarik edenlerle müşteriler arasındaki ilişkileri etkileyen aldatıcı veya dürüstlük kuralına diğer şekillerdeki aykırı davranışlar ile ticari uygulamalar haksız ve hukuka aykırıdır.

II - Dürüstlük kuralına aykırı davranışlar, ticari uygulamalar

MADDE 55- (1) Aşağıda sayılan hâller haksız rekabet hâllerinin başlıcalarıdır:

a) Dürüstlük kuralına aykırı reklamlar ve satış yöntemleri ile diğer hukuka aykırı davranışlar ve özellikle;

1. Başkalarını veya onların mallarını, iş ürünlerini, fiyatlarını, faaliyetlerini veya ticari işlerini yanlış, yanıltıcı veya gereksiz yere incitici açıklamalarla kötülemek,

2. Kendisi, ticari işletmesi, işletme işaretleri, malları, iş ürünleri, faaliyetleri, fiyatları, stokları, satış kampanyalarının biçimi ve iş ilişkileri hakkında gerçek dışı veya yanıltıcı açıklamalarda bulunmak veya aynı yollarla üçüncü kişiyi rekabette öne geçirmek,

3. Paye, diploma veya ödül almadığı hâlde bunlara sahipmişçesine hareket ederek müstesna yeteneğe malik bulunduğu zannını uyandırmaya çalışmak veya buna elverişli doğru olmayan meslek adları ve sembolleri kullanmak,

4. Başkasının malları, iş ürünleri, faaliyetleri veya işleri ile karıştırılmaya yol açan önlemler almak,

5. Kendisini, mallarını, iş ürünlerini, faaliyetlerini, fiyatlarını, gerçeğe aykırı, yanıltıcı, rakibini gereksiz yere kötüleyici veya gereksiz yere onun tanınmışlığından yararlanacak şekilde; başkaları, malları, iş ürünleri veya fiyatlarıyla karşılaştırmak ya da üçüncü kişiyi benzer yollardan öne geçirmek,

6. Seçilmiş bazı malları, iş ürünlerini veya faaliyetleri birden çok kere tedarik fiyatının altında satışa sunmak, bu sunumları reklamlarında özellikle vurgulamak ve bu şekilde müşterilerini, kendisinin veya rakiplerinin yeteneği hakkında yanıltmak; şu kadar ki, satış fiyatının, aynı çeşit malların, iş ürünlerinin veya faaliyetlerinin benzer hacimde alımında uygulanan tedarik fiyatının altında olması hâlinde yanıltmanın varlığı karine olarak kabul olunur; davalı, gerçek tedarik fiyatını ispatladığı takdirde bu fiyat değerlendirmeye esas olur,

7. Müşteriyi ek edimlerle sunumun gerçek değeri hakkında yanıltmak,

8. Müşterinin karar verme özgürlüğünü özellikle saldırgan satış yöntemleri ile sınırlamak,

9. Malların, iş ürünlerinin veya faaliyetlerin özelliklerini, miktarını, kullanım amaçlarını, yararlarını veya tehlikelerini gizlemek ve bu şekilde müşteriyi yanıltmak,

10. Taksitle satım sözleşmelerine veya buna benzer hukuki işlemlere ilişkin kamuya yapılan ilanlarda unvanını açıkça belirtmemek, peşin veya toplam satış fiyatını veya taksitle satımdan kaynaklanan ek maliyeti Türk Lirası ve yıllık oranlar üzerinden belirtmemek,

11. Tüketici kredilerine ilişkin kamuya yapılan ilanlarda unvanını açıkça belirtmemek veya kredilerin net tutarlarına, toplam giderlerine, efektif yıllık faizlerine ilişkin açık beyanlarda bulunmamak,

12. İşletmesine ilişkin faaliyetleri çerçevesinde, taksitle satım veya tüketici kredisi sözleşmeleri sunan veya akdeden ve bu bağlamda sözleşmenin konusu, fiyatı, ödeme şartları, sözleşme süresi, müşterinin cayma veya fesih hakkına veya kalan borcu vadeden önce ödeme hakkına ilişkin eksik veya yanlış bilgiler içeren sözleşme formülleri kullanmak.

b) Sözleşmeyi ihlale veya sona erdirmeye yöneltmek; özellikle;

1. Müşterilerle kendisinin bizzat sözleşme yapabilmesi için, onları başkalarıyla yapmış oldukları sözleşmelere aykırı davranmaya yöneltmek,

2. Üçüncü kişilerin işçilerine, vekillerine ve diğer yardımcı kişilerine, hak etmedikleri ve onları işlerinin ifasında yükümlülüklerine aykırı davranmaya yöneltebilecek yararlar sağlayarak veya önererek, kendisine veya başkalarına çıkar sağlamaya çalışmak,

3. İşçileri, vekilleri veya diğer yardımcı kişileri, işverenlerinin veya müvekkillerinin üretim ve iş sırlarını ifşa etmeye veya ele geçirmeye yöneltmek,

4. Onunla kendisinin bu tür bir sözleşme yapabilmesi için, taksitle satış, peşin satış veya tüketici kredisi sözleşmesi yapmış olan alıcının veya kredi alan kişinin, bu sözleşmeden caymasına veya peşin satış sözleşmesi yapmış olan alıcının bu sözleşmeyi feshetmesine yöneltmek.

c) Başkalarının iş ürünlerinden yetkisiz yararlanma; özellikle;

1. Kendisine emanet edilmiş teklif, hesap veya plan gibi bir iş ürününden yetkisiz yararlanmak,

2. Üçüncü kişilere ait teklif, hesap veya plan gibi bir iş ürününden, bunların kendisine yetkisiz olarak tevdi edilmiş veya sağlanmış olduğunun bilinmesi gerektiği hâlde, yararlanmak,

3. Kendisinin uygun bir katkısı olmaksızın başkasına ait pazarlanmaya hazır çalışma ürünlerini teknik çoğaltma yöntemleriyle devralıp onlardan yararlanmak.

d) Üretim ve iş sırlarını hukuka aykırı olarak ifşa etmek; özellikle, gizlice ve izinsiz olarak ele geçirdiği veya başkaca hukuka aykırı bir şekilde öğrendiği bilgileri ve üretenin iş sırlarını değerlendiren veya başkalarına bildiren dürüstlüğe aykırı davranmış olur.

e) İş şartlarına uymamak; özellikle kanun veya sözleşmeyle, rakiplere de yüklenmiş olan veya bir meslek dalında veya çevrede olağan olan iş şartlarına uymayanlar dürüstlüğe aykırı davranmış olur.

f) Dürüstlük kuralına aykırı işlem şartları kullanmak. Özellikle yanıltıcı bir şekilde diğer taraf aleyhine;

1. Doğrudan veya yorum yoluyla uygulanacak kanuni düzenlemeden önemli ölçüde ayrılan, veya

2. Sözleşmenin niteliğine önemli ölçüde aykırı haklar ve borçlar dağılımını öngören, önceden yazılmış genel işlem şartlarını kullananlar dürüstlüğe aykırı davranmış olur.

(...)

ÜÇÜNCÜ BÖLÜM

Çek

BİRİNCİ AYIRIM

Çeklerin Düzenlenmesi ve Şekli

A) Şekli

I - Unsurlar

MADDE 780- (1) Çek;

- a) Senet metninde “çek” kelimesini ve eğer senet Türkçe’den başka bir dille yazılmış ise o dilde “çek” karşılığı olarak kullanılan kelimeyi,
 - b) Kayıtsız ve şartsız belirli bir bedelin ödenmesi için havaleyi,
 - c) Ödeyecek kişinin, “muhatabın” ticaret unvanını,
 - d) Ödeme yerini,
 - e) Düzenlenme tarihini ve yerini,
 - f) Düzenleyenin imzasını,
 - g) (Ek: 15/7/2016-6728/70 md.) Banka tarafından verilen seri numarasını,
 - h) (Ek: 15/7/2016-6728/70 md.) Karekodu,
- içerir.

(2) (Ek fıkra : 15/7/2016-6728/70 md.) Çek alacaklıları, ellerinde bulunan çek ile çek hesabı sahibine ve bu çeki düzenleyenlere ilişkin verilere karekod aracılığıyla erişim sağlayabilir. Karekod ile;

- a) Çek hesabı sahibinin adı, soyadı veya ticaret unvanı,
- b) Çek hesabı sahibinin tacir olması hâlinde, ticaret siciline tescil edilen yetkililerinin adı, soyadı veya ticaret unvanı,
- c) Çek hesabı sahibinin, çek hesabı bulunan toplam banka sayısı,
- d) Çek hesabı sahibine ait bankalara ibraz edilmemiş çek adedi ve tutarı,
- e) Düzenlenerek bankalara teslim edilen çeklerin adedi ve tutarı,
- f) Son beş yıl içerisinde ibrazında ödenen çeklerin adedi ve tutarı,
- g) İbraz edilen ilk çekin ibraz tarihi,
- h) İbraz edilen son çekin ibraz tarihi,
- i) İbrazında ödenen son çekin ibraz tarihi,
- i) Son beş yılda “karşılıksızdır” işlemi gören ve halen ödenmemiş çeklerin adedi ve tutarları,
- j) Son beş yılda “karşılıksızdır” işlemi gören ve sonradan ödenen çeklerin adedi ve tutarı,

- k) Son beş yılda “karşılıksızdır” işlemi gören son çekin ibraz tarihi,
- l) Çek hesabı sahibi hakkında çek hesabı açma yasağı bulunup bulunmadığı, varsa yasaklama kararının tarihi,
- m) Her bir çek yaprağı ile ilgili olarak tedbir kaydı olup olmadığı,
- n) Çek hesabı sahibi tacirse, iflasına karar verilip verilmediği, iflasına karar verilmişse kararın tarihi, çek hesabı sahibi ya da cirantanın rızası aranmaksızın üçüncü kişilerin erişimine sunulur.

(3) (Ek fıkra : 15/7/2016-6728/70 md.) İkinci fıkrada belirtilen verilere ulaşılmasını sağlayacak karekod okutma ve bilgi paylaşım sistemi 5411 sayılı Kanunun ek 1 inci madde hükmü uyarınca kurulan Türkiye Bankalar Birliği Risk Merkezi tarafından oluşturulur. Risk Merkezi sistemdeki verileri, 5411 sayılı Kanunun ek 1 inci maddesinin on birinci fıkrası uyarınca bilgi alışverişini gerçekleştirdiği şirket ile paylaşmaya yetkilidir. Bu yetki kullanıldığı takdirde sistem bilgilerin paylaşıldığı şirket nezdinde kurulabilir.

(4) (Ek fıkra : 15/7/2016-6728/70 md.) Çekte yer alacak MERSİS numarası ile karekodun tanım ve içerikleri ile bu maddenin uygulanmasına ilişkin usul ve esaslar Gümrük ve Ticaret Bakanlığı ile Hazine Müsteşarlığının müştereken çıkaracağı tebliğle belirlenir.

II - Unsurların bulunmaması

MADDE 781- (1) 780 inci maddede gösterilen unsurlardan birini içermeyen bir senet, ikinci, üçüncü ve dördüncü fıkralarda yazılı hâller dışında çek sayılmaz. (1)

(2) Çekte açıklık yoksa, muhatabın ticaret unvanı yanında gösterilen yer ödeme yeri sayılır. Muhatabın ticaret unvanı yanında birden fazla yer gösterildiği takdirde, çek, ilk gösterilen yerde ödenir. Böyle bir açıklık ve başka bir kayıt da yoksa, çek muhatabın merkezinin bulunduğu yerde ödenir.

(3) Düzenlenme yeri gösterilmemiş olan çek, düzenleyenin adı yanında yazılı olan yerde düzenlenmiş sayılır.

(4) (Ek : 15/7/2016-6728/71 md.) Yabancı banka tarafından bastırılan çeklerde, 780 inci maddenin birinci fıkrasının (g) bendinde belirtilen banka tarafından verilen seri numarası ve/veya (h) bendinde belirtilen karekodun bulunmaması senedin çek olarak geçerliliğini etkilemez.

(...)

6100 sayılı Hukuk Muhakemeleri Kanunu

Resmî Gazete Tarihi : 04.02.2011

Resmî Gazete Sayısı : 27836

HUKUK MUHAKEMELERİ KANUNU

Kayıt ve yayın yasağı

MADDE 153- (1) Duruşma sırasında fotoğraf çekilemez ve hiçbir şekilde ses ve görüntü kaydı yapılamaz. Ancak, dava dosyasında saklı kalmak kaydıyla, yargılamanın zorunlu kıldığı hâllerde, mahkemece çekim yapılabilir ve kayıt alınabilir. Bu şekilde yapılan çekim ve kayıtlar ile kişilik haklarını ilgilendiren konuları içeren dava dosyası içindeki her türlü belge ve tutanak, mahkemenin ve ilgili kişilerin açık izni olmadıkça hiçbir yerde yayımlanamaz.

(2) Duruşma sırasında bu yasağa aykırı davranan kişi hakkında 151 inci madde hükmü uygulanır.

(3) Kayıt ve yayın yasağına aykırı davranan kişi hakkında, ayrıca Türk Ceza Kanununun 286 ncı maddesi hükümleri uygulanır.

(...)

İKİNCİ BÖLÜM

Belge ve Senet

Belge

MADDE 199- (1) Uyuşmazlık konusu vakıaları ispata elverişli yazılı veya basılı metin, senet, çizim, plan, kroki, fotoğraf, film, görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcıları bu Kanuna göre belgedir.

Senetle ispat zorunluluğu

MADDE 200- (1) Bir hakkın doğumu, düşürülmesi, devri, değiştirilmesi, yenilenmesi, ertelenmesi, ikrarı ve itfası amacıyla yapılan hukuki işlemlerin, yapıldıkları zamanki miktar veya değerleri ikibinbeşyüz Türk Lirasını geçtiği takdirde senetle ispat olunması gerekir. Bu hukuki işlemlerin miktar veya değeri ödeme veya borçtan kurtarma gibi bir nedenle ikibinbeşyüz Türk Lirasından aşağı düşse bile senetsiz ispat olunamaz.

(2) Bu madde uyarınca senetle ispatı gereken hususlarda birinci fıkradaki düzenleme hatırlatılarak karşı tarafın açık muvafakati hâlinde tanık dinlenebilir.

Senede karşı tanıkla ispat yasağı

MADDE 201- (1) Senede bağlı her çeşit iddiaya karşı ileri sürülen ve senedin hüküm ve kuvvetini ortadan kaldıracak veya azaltacak nitelikte bulunan hukuki işlemler ikibinbeşyüz Türk Lirasından az bir miktara ait olsa bile tanıkla ispat olunamaz.

Delil başlangıcı

MADDE 202- (1) Senetle ispat zorunluluğu bulunan hâllerde delil başlangıcı bulunursa tanık dinlenebilir.

(2) Delil başlangıcı, iddia konusu hukuki işlemin tamamen ispatına yeterli olmamakla birlikte, söz konusu hukuki işlemi muhtemel gösteren ve kendisine karşı ileri sürülen kimse veya temsilcisi tarafından verilmiş veya gönderilmiş belgedir.

Senetle ispat zorunluluğunun istisnaları

MADDE 203- (1) Aşağıdaki hâllerde tanık dinlenebilir:

- a) Altsoy ve üstsoy, kardeşler, eşler, kayınbaba, kaynana ile gelin ve damat arasındaki işlemler.
- b) İşin niteliğine ve tarafların durumlarına göre, senede bağlanmaması teamül olarak yerleşmiş bulunan hukuki işlemler.
- c) Yangın, deniz kazası, deprem gibi senet alınmasında imkânsızlık veya olağanüstü güçlük bulunan hâllerde yapılan işlemler.
- ç) Hukuki işlemlerde irade bozukluğu ile aşırı yararlanma iddiaları.
- d) Hukuki işlemlere ve senetlere karşı üçüncü kişilerin muvazaa iddiaları.
- e) Bir senedin sahibi elinde beklenmeyen bir olay veya zorlayıcı bir nedenle yahut usulüne göre teslim edilen bir memur elinde veya noterlikte herhangi bir şekilde kaybolduğu kanısını kuvvetlendirecek delil veya emarelerin bulunması hâli.

İlamların ve resmî senetlerin ispat gücü

MADDE 204- (1) İlamlar ile düzenleme şeklindeki noter senetleri, sahteliği ispat olunmadıkça kesin delil sayılırlar.

(2) İlgililerin beyanına dayanılarak noterlerin tasdik ettikleri senetlerle diğer yetkili memurların görevleri içinde usulüne uygun olarak düzenledikleri belgeler, aksi ispatlanıncaya kadar kesin delil sayılırlar.

(3) Mahkeme, yukarıdaki belgelerden biri hakkında şüphe uyandıran bir hâl görürse, ilgili daireden açıklama isteyebilir.

Adi senetlerin ispat gücü

MADDE 205- (1) Mahkeme huzurunda ikrar olunan veya mahkemece inkâr edenden sadır olduğu kabul edilen adi senetler, aksi ispat edilmedikçe kesin delil sayılırlar.

(2) Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler, senet hükmündedir.

(3) Hâkim, mahkemeye delil olarak sunulan elektronik imzalı belgenin, güvenli elektronik imza ile oluşturulmuş olup olmadığını resen inceler.

İmza atamayanların durumu

MADDE 206- (1) Okuma ve yazma bilmediği için imza atamayanların mühür veya bir alet ya da parmak izi kullanmak suretiyle yapacakları hukuki işlemleri içeren belgelerin senet niteliğini taşıyabilmesi, noterler tarafından düzenleme biçiminde oluşturulmasına bağlıdır.(1)

(2) (Ek:22/7/2020-7251/21 md.) Okuma ve yazma bildiği hâlde imza atamayanların mühür veya bir alet ya da parmak izi kullanmak suretiyle yapacakları hukuki işlemleri içeren belgelerin senet niteliğini taşıyabilmesi, noterler tarafından onaylanmasına veya düzenlenmesine bağlıdır.

(3) İmza atamayan kimselerin, cüzdanla iş yapmayı usul edinmiş kuruluşlarla olan işlemlerde kullanacakları mühür, kazınmış imza, işaret veya parmak izinin, işlemin başlangıcında hesap defterine veya cüzdanına basılmış olması veya önceden noterde bir örneği saklanmak üzere onanmış bulunması yeterli olup, her işlemde ayrıca onamaya bağlı değildir.

(4) Yukarıda belirtilen hükümler dairesinde noterlerce onaylanacak veya düzenlenecek olan senetler için ilgisinden harç, vergi ve değerli kâğıt bedeli alınmaz.

Senette çıkıntı, kazıntı ve silinti

MADDE 207- (1) Senetteki çıkıntı, kazıntı veya silinti ayrıca onanmamışsa, inkâr hâlinde göz önünde tutulmaz. Bu tür çıkıntı, kazıntı veya silinti mahkemece senedin geçerliliğine ve anlamına etkili olacak nitelikte görülürse, senet kısmen veya tamamen hükümsüz sayılabilir.

Yazı veya imza inkârı

MADDE 208- (1) Taraflardan biri, kendisi tarafından düzenlendiği iddia edilen bir belgedeki yazı veya imzayı inkâr etmek isterse, sahtelik iddiasında bulunmalıdır; aksi hâlde belge, aleyhine delil olarak kullanılır.

(2) Bir belgenin sahteliği iddia edildiğinde, belgenin mahkemeye verildiği tarih yazılıp mühürlenerek, saklanması için mahkemece gerekli tedbirler alınır.

(3) Bir belgenin sahteliğini iddia eden kimse, bunu aynı mahkemede ön sorun şeklinde ileri sürebileceği gibi, bu konuda ayrı bir dava da açabilir.

(4) Resmî bir senetteki yazı veya imzayı inkâr eden tarafın bu iddiası, ancak ilgili evraka resmiyet kazandıran kişiyi de taraf göstererek açacağı ayrı bir davada incelenip karara bağlanabilir. Asıl davaya bakan hâkim, gerekirse bu konuda imza veya yazıyı inkâr eden tarafa, dava açması için iki haftalık kesin bir süre verir.

Yazı veya imza inkârının sonucu

MADDE 209- (1) Adi bir senetteki yazı veya imza inkâr edildiğinde, bu konuda bir karar verilinceye kadar, o senet herhangi bir işleme esas alınamaz.

(2) Resmî senetlerdeki yazı veya imza inkâr edildiğinde, senetteki yazı veya imzanın sahteliği, ancak mahkeme kararıyla sabit olursa, bu senet herhangi bir işleme esas alınamaz.

(3) Senede dayanılarak verilmiş olan ihtiyati tedbir, o senet hakkındaki sahtelik iddiasından etkilenmez ve gerektiğinde senet sahibi haklarının korunması için yeni tedbirler talep edebilir.

Güvenli elektronik imzalı belgenin inkârı

MADDE 210- (1) Güvenli elektronik imzayla oluşturulmuş verinin inkârı hâlinde, hâkim tarafından veriyi inkâr eden taraf dinlendikten sonra bir kanaate varılamamışsa, bilirkişi incelemesine başvurulur.

Sahtelik incelemesi

MADDE 211- (1) Bir belgenin sahteliğinin iddia edilmesi durumunda, bu hususta karşı tarafın açıklamaları da dikkate alınarak, aşağıdaki sıra ile inceleme yapılarak öncelikle karar verilir:

a) Hâkim, yazı veya imzayı inkâr eden tarafı isticvap ettikten sonra bir kanaat edinmemişse, huzurda bu kişiye yazı yazdırıp imza attırmak suretiyle elde ettiği belge ve diğer delilleri değerlendirir. Hâkim, sahtelik konusunda başka bir incelemeye gerek duymadan karar verebilecek durumda ise gerekçesini açıkça belirtmek suretiyle, senedin sahteliği hakkında bir karar verir. İsticvap için mahkemeye davet edilen taraf, belirtilen günde hazır bulunmadığı takdirde, inkâr etmiş olduğu

belgedeki yazı veya imzayı ikrar etmiş sayılır; bu husus kendisine çıkartılacak davetiyede ayrıca ihtar edilir.

b) (a) bendi hükmüne göre yaptığı incelemeye rağmen, hâkimde sahtelik konusunda kesin bir kanaat oluşmamışsa, bilirkişi incelemesine karar verir. Bilirkişi incelemesinden önce, mevcutsa, o tarafa ait olan karşılaştırma yapmaya elverişli yazı ve imzalar, ilgili yerlerden getirilir. Bilirkişi, bu yazı ve imzalarla, o mahkemede elde edilen yazı ve imzaları esas alarak inceleme yapar. Bilirkişi, inceleme için gerekli görürse, kendi huzurunda tarafın yeniden yazı yazması veya imza atmasını mahkemeden talep edebilir.

Sahte senedin iptali

MADDE 212- (1) Bir senedin sahte olduğuna dair karar kesinleştikten sonra, senedin altına sahte olduğu yazılarak senet iptal olunur. Resmî senetlerde, senedin ilgili dairedeki aslı da bu yolla iptal edilir.

Haksız yere sahtelik iddiası

MADDE 213- (1) Sahtelik iddiası sonunda haksız çıkan taraf kötüniyetli ise bu sebeple ertelenen her bir duruşma için celse harcına ve talep hâlinde bu sebeple diğer tarafın uğradığı zararları tazmin etmeye mahkûm edilir.

(2) Resmî senetteki imza veya yazı inkâr edildiğinde, yukarıdaki harç miktarı iki katı olarak uygulanır.

(3) Bilirkişi incelemesi yapılmasına karar verilmesinden önce, tarafların sahteliğe ilişkin iddialarından vazgeçmeleri hâlinde, hâkim, tazminattan indirim yapabileceği gibi tazminata hükmetmeyebilir.

Sahtelik hakkında hukuk ve ceza mahkemesi kararlarının etkisi

MADDE 214- (1) Belgenin sahte olmadığına dair hukuk mahkemesince verilen karar kesinleştikten sonra, söz konusu belge hakkında ceza mahkemesinde de sahtelik iddiası dinlenmez.

(2) Ceza mahkemesince belgeyi düzenleyen hakkında ceza verilmesine yer olmadığı ya da beraat kararı verilmiş olması, hukuk mahkemesinin belgenin sahteliğini incelemesini engellemez.

Belgelerin halefler aleyhine kullanılması ve adi senetlerin üçüncü kişiler için hüküm ifade etmesi

MADDE 215- (1) Bir kimsenin aleyhine delil olarak kullanılacak belgeler, o kimsenin halefleri aleyhine de delil teşkil eder.

(2) (Ek:22/7/2020-7251/22 md.) Bir adi senet bakımından, kendisine ibraz olunduğu noter veya yetkili memur tarafından usulüne uygun olarak onaylanmış ise ibraz tarihi, resmi bir işleme konu olmuşsa işlem tarihi, imza edenlerden biri ölmüşse ölüm tarihi, imza edenlerden birinin imza etmesine fiilen imkân kalmamışsa bu imkânı ortadan kaldıran olayın meydana geldiği tarih üçüncü kişiler hakkında da hüküm ifade eder. Adi senette bahsedilen diğer senetlerin tarihleri, üçüncü kişiler hakkında ancak son senet tarihinin onaylanmış olduğunun kabul edildiği tarihte hüküm ifade eder.

Mahkemece belge aslının istenmesi ve geri verilmesi

MADDE 216- (1) Belgenin sadece örneğinin mahkemeye verildiği durumlarda, mahkeme kendiliğinden veya taraflardan birinin talebi üzerine belgenin aslının verilmesini de isteyebilir.

(2) Belgenin aslını elinde bulunduran taraf, üçüncü kişi veya resmî makamlar, istenmesi hâlinde bunu mahkemeye vermek zorundadır.

(3) Mahkeme, belge aslının verilmesi durumunda, belgenin saklanması için gerekli tedbirleri alır veya istendiğinde tekrar verilmek üzere belgeyi ibraz edene geri verebilir.

(4) Taraflardan biri elindeki belgenin aslını mahkemeye verirse, bu belgenin geri verilmesini talep edebilir. Bu takdirde hâkim, belgenin aslının verilip verilmeyeceğine karar verir. Geri verilmesine karar verildiğinde, aslına uygun olduğu mahkeme mührü ve yazı işleri müdürünün imzasıyla onanmış örneği dosyaya konur.

Belge aslının ibrazı usulü

MADDE 217- (1) Bir kişi veya kurumun elinde bulunup mahkemeye teslim edilmesi gereken belgenin aslı istendiğinde, kişi veya kurumun bulunduğu ya da belgenin teslim edileceği yerdeki asliye mahkemesi tarafından örneği onaylanarak aslı mahkemeye gönderilir yahut teslim edilir.

(2) Mahkemece onaylanmış belge örneği, aslı gibi hüküm ifade eder.

Belgenin yerinde incelenmesi

MADDE 218- (1) Mahkemeye getirilmesi zor veya sakıncalı olan belgeler, hâkim veya görevlendireceği bilirkişi tarafından yerinde incelenir ya da bu belgelerin mahkemeye sunulmuş örnekleri asıllarıyla karşılaştırılır. İnceleme sonunda bir tutanak düzenlenir ve gerekli görülürse uygun teknik araçlarla belgenin aslı kaydedilir.

(2) Mahkemenin bu yöndeki emrinin yerine getirilmesine haklı bir sebep olmaksızın engel olunması hâlinde hâkim tarafından, engel olan kişi hakkında sebep olduğu giderlere ve beşyüz Türk Lirasından

beşbin Türk Lirasına kadar disiplin para cezasına hükmolunur. Gerektiğinde zor kullanılmasına da karar verilebilir.

Tarafların belgeleri ibrazı zorunluluğu

MADDE 219- (1) Taraflar, kendilerinin veya karşı tarafın delil olarak dayandıkları ve ellerinde bulunan tüm belgeleri mahkemeye ibraz etmek zorundadırlar. Elektronik belgeler ise belgenin çıktısı alınarak ve talep edildiğinde incelemeye elverişli şekilde elektronik ortama kaydedilerek mahkemeye ibraz edilir.

(2) Ticari defterler gibi devamlı kullanılan belgelerin sadece ilgili kısımlarının onaylı örnekleri mahkemeye ibraz edilebilir.

Tarafın belgeyi ibraz etmemesi

MADDE 220- (1) İbrazı istenen belgenin, ileri sürülen hususun ispatı için zorunlu ve bu isteğin kanuna uygun olduğuna mahkemece kanaat getirildiği ve karşı taraf da bu belgenin elinde olduğunu ikrar ettiği veya ileri sürülen talep üzerine sükut ettiği yahut belgenin var olduğu resmî bir kayıtla anlaşıldığı veya başka bir belgede ikrar olunduğu takdirde, mahkeme bu belgenin ibrazı için kesin bir süre verir.

(2) Mahkemece, ibrazı istenen belgenin elinde bulunduğunu inkâr eden tarafa, böyle bir belgenin elinde bulunmadığına, özenle aradığı hâlde bulamadığına ve nerede olduğunu da bilmediğine ilişkin yemin teklif edilir.

(3) Belgeyi ibraz etmesine karar verilen taraf, kendisine verilen sürede belgeyi ibraz etmez ve aynı sürede, delilleriyle birlikte ibraz etmemesi hakkında kabul edilebilir bir mazeret göstermez ya da belgenin elinde bulunduğunu inkâr eder ve teklif edilen yemini kabul veya icra etmezse, mahkeme, duruma göre belgenin içeriği konusunda diğer tarafın beyanını kabul edebilir.

Üçüncü kişinin belgeyi ibraz etmemesi

MADDE 221- (1) Mahkeme, üçüncü kişi veya kurumun elinde bulunan bir belgenin taraflarca ileri sürülen hususun ispatı için zorunlu olduğuna karar verirse, bu belgenin ibrazını emreder.

(2) Belgeyi ibraz etmesine karar verilen herkes, elindeki belgeyi ibraz etmek; belgeyi ibraz edememesi hâlinde ise bunun sebebini delilleri ile birlikte açıklamak zorundadır. Mahkeme yapılan açıklamayı yeterli görmezse, bu kimseyi tanık olarak dinleyebilir.

(3) Belgeyi ibraz zorunda olanlar, tanıklıktan çekilmeye ilişkin hükümlere göre, belgeyi ibrazdan veya bu konudaki tanıklıktan çekinebilirler. Belgeyi ibraz veya bu konuda tanıklık yapmak zorunda olanlar hakkında, tanıklara ilişkin hükümler uygulanır.

Ticari defterlerin ibrazı ve delil olması

MADDE 222 - (1) Mahkeme, ticari davalarda tarafların ticari defterlerinin ibrazına kendiliğinden veya taraflardan birinin talebi üzerine karar verebilir.

(2) Ticari defterlerin, ticari davalarda delil olarak kabul edilebilmesi için, kanuna göre eksiksiz ve usulüne uygun olarak tutulmuş, açılış ve kapanış onayları yaptırılmış ve defter kayıtlarının birbirini doğrulamış olması şarttır.

(3) İkinci fıkrada belirtilen şartlara uygun olarak tutulan ticari defter kayıtlarının sahibi ve halefleri lehine delil olarak kabul edilebilmesi için, diğer tarafın aynı şartlara uygun olarak tutulmuş ticari defterlerindeki kayıtların bunlara aykırı olmaması veya diğer tarafın ticari defterlerini ibraz etmemesi yahut defter kayıtlarının aksinin senet veya diğer kesin delillerle ispatlanmamış olması gerekir. (Ek cümle:22/7/2020-7251/23 md.) Diğer tarafın ikinci fıkrada yazılan şartlara uygun olarak tutulan ticari defterlerinin, ilgili hususta hiçbir kayıt içermemesi hâlinde ticari defterler, sahibi lehine delil olarak kullanılamaz. Bu şartlara uygun olarak tutulan defterlerdeki sahibi lehine ve aleyhine olan kayıtlar birbirinden ayrılamaz.

(4) Açılış veya kapanış onayları bulunmayan ve içerdiği kayıtlar birbirini doğrulamayan ticari defter kayıtları, sahibi aleyhine delil olur.

(5) Taraflardan biri tacir olmasa dahi, tacir olan diğer tarafın ticari defterlerindeki kayıtları kabul edeceğini belirtir; ancak, karşı taraf defterlerini ibrazdan kaçınırsa, ibrazı talep eden taraf iddiasını ispat etmiş sayılır.

Yabancı dilde yazılmış belgeler

MADDE 223- (1) Yabancı dilde yazılmış belgeye dayanan taraf, tercümesini de mahkemeye sunmak zorundadır.

(2) Mahkeme kendiliğinden veya diğer tarafın talebi üzerine, belgenin resmî tercümesini de isteyebilir.

Yabancı resmî belgelerin yetkili makamlar tarafından onaylanması zorunluluğu

MADDE 224- (1) Yabancı devlet makamlarınca hazırlanan resmî belgelerin, Türkiye’de bu vasfı taşıması, belgenin verildiği devletin yetkili makamı veya ilgili Türk konsolosluk makamı tarafından onaylanmasına bağlıdır.

(2) Türkiye’nin taraf olduğu milletlerarası sözleşmelerin yabancı resmî belgelerin tasdiki ile ilgili hükümleri saklıdır.

(...)

Elektronik işlemler

MADDE 445- (1) Ulusal Yargı Ağı Bilişim Sistemi (UYAP), adalet hizmetlerinin elektronik ortamda yürütülmesi amacıyla oluşturulan bilişim sistemidir. Dava ve diğer yargılama işlemlerinin elektronik ortamda gerçekleştirildiği hâllerde UYAP kullanılarak veriler kaydedilir ve saklanır.

(2) Elektronik ortamda, güvenli elektronik imza kullanılarak dava açılabilir, harç ve avans ödenebilir, dava dosyaları incelenebilir. Bu Kanun kapsamında fizikî olarak hazırlanması öngörülen tutanak ve belgeler güvenli elektronik imzayla elektronik ortamda hazırlanabilir ve gönderilebilir. Güvenli elektronik imza ile oluşturulan tutanak ve belgeler ayrıca fizikî olarak gönderilmez, belge örneği aranmaz.

(3) Elektronik ortamdan fizikî örnek çıkartılması gereken hâllerde tutanak veya belgenin aslının aynı olduğu belirtilerek hâkim veya görevlendirdiği yazı işleri müdürü tarafından imzalanır ve mühürlenir.

(4) Elektronik ortamda yapılan işlemlerde süre gün sonunda biter.

(5) Mahkemelerde görülmekte olan dava, çekişmesiz yargı, geçici hukuki koruma ve diğer tüm işlemlerde UYAP’ın kullanılmasına dair usul ve esaslar yönetmelikle düzenlenir.

6098 sayılı Türk Borçlar Kanunu

Resmî Gazete Tarihi : 04.02.2011

Resmî Gazete Sayısı : 27836

TÜRK BORÇLAR KANUNU

3. Kişilik hakkının zedelenmesi

MADDE 58- Kişilik hakkının zedelenmesinden zarar gören, uğradığı manevi zarara karşılık manevi tazminat adı altında bir miktar para ödenmesini isteyebilir.

Hâkim, bu tazminatın ödenmesi yerine, diğer bir giderim biçimi kararlaştırabilir veya bu tazminata ekleyebilir; özellikle saldırıyı kınayan bir karar verebilir ve bu kararın yayımlanmasına hükmedebilir.

(...)

3. Kişisel verilerin kullanılmasında

MADDE 419- İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir.

Özel kanun hükümleri saklıdır.

5809 sayılı Elektronik Haberleşme Kanunu

Resmî Gazete Tarihi : 10.11.2008

Resmî Gazete Sayısı : 27050 (Mükerrer)

ELEKTRONİK HABERLEŞME KANUNU

BİRİNCİ KISIM

Genel Hükümler

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç

MADDE 1 - (1) Bu Kanunun amacı; elektronik haberleşme sektöründe düzenleme ve denetleme yoluyla etkin rekabetin tesisi, tüketici haklarının gözetilmesi, ülke genelinde hizmetlerin yaygınlaştırılması, kaynakların etkin ve verimli kullanılması, haberleşme alt yapı, şebeke ve hizmet alanında teknolojik gelişimin ve yeni yatırımların teşvik edilmesi ve bunlara ilişkin usul ve esasların belirlenmesidir.

Kapsam

MADDE 2 - (1) Elektronik haberleşme hizmetlerinin yürütülmesi ve elektronik haberleşme alt yapı ve şebekesinin tesisi ve işletilmesi ile her türlü elektronik haberleşme cihaz ve sistemlerinin imali, ithali, satışı, kurulması, işletilmesi, frekans dahil kıt kaynakların planlaması ve tahsisi ile bu konulara ilişkin düzenleme, yetkilendirme, denetleme ve uzlaştırma faaliyetlerinin yürütülmesi bu Kanuna tabidir.

(2) Millî güvenlik ve kamu düzeni ile olağanüstü hal, (...) seferberlik, savaş hallerinde ve doğal afet durumlarında elektronik haberleşme hizmetlerinin sağlanmasına ilişkin özel kanunların ve 16/7/1965 tarihli ve 697 sayılı Ulaştırma ve Haberleşme Hizmetlerinin Olağanüstü Hallerde ve Savaşta Ne Suretle Yürütüleceğine Dair Kanun, 9/4/1987 tarihli ve 3348 sayılı Ulaştırma Bakanlığının Teşkilat ve Görevleri Hakkında Kanun, 16/6/2005 tarihli ve 5369 sayılı Evrensel Hizmetin Sağlanması ve Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun, 3/7/2005 tarihli ve 5397 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan

Yayımların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun hükümleri saklıdır.

(3) Türk Silahlı Kuvvetleri, Jandarma Genel Komutanlığı ile Sahil Güvenlik Komutanlığı ve kuruluş kanunları ile Cumhurbaşkanlığı kararnamelerinde belirtilen görev sahaları ile ilgili konularda olmak üzere Dışişleri Bakanlığı, Telekomünikasyon İletişim Başkanlığı, Millî İstihbarat Teşkilatı Müsteşarlığı ve Emniyet Genel Müdürlüğünün elektronik haberleşme cihaz, sistem ve şebekeleri ile bedeli bu kurumlar tarafından ödenerek işletmeciler tarafından kurulan veya kurulacak elektronik haberleşme cihaz, sistem ve şebekeleri hakkında 36 ncı ve 39 uncu maddeler hariç, bu Kanun hükümleri uygulanmaz.

(...)

İlkeler

MADDE 4 - (1) Her türlü elektronik haberleşme cihaz, sistem ve şebekelerinin kurulması ve işletilmesine müsaade edilmesi, gerekli frekans, numara, uydu pozisyonu ve benzeri kaynak tahsislerinin yapılması ile bunların düzenlenmesi Devletin yetki ve sorumluluğu altındadır. İlgili merciler tarafından elektronik haberleşme hizmetinin sunulmasında ve bu hususta yapılacak düzenlemelerde aşağıdaki ilkeler göz önüne alınır:

- a) Serbest ve etkin rekabet ortamının sağlanması ve korunması.
- b) Tüketici hak ve menfaatlerinin gözetilmesi.
- c) Kalkınma planları ve üst politika metinleri ile Bakanlık tarafından belirlenen stratejilerin gözetilmesi.
- ç) Herkesin, makul bir ücret karşılığında elektronik haberleşme şebeke ve hizmetlerinden yararlanmasını sağlayacak uygulamaların teşvik edilmesi.
- d) Aksini gerektiren objektif nedenler bulunmadıkça veya toplumdaki ihtiyaç sahibi kesimlere özel, kapsamı açık ve sınırları belirlenmiş kolaylıklar sağlanması halleri dışında, eşit şartlardaki aboneler, kullanıcılar ve işletmeciler arasında ayırım gözetilmemesi ve hizmetlerin benzer konumdaki kişiler tarafından eşit şartlarla ulaşılabilir olması.
- e) Bu Kanunda aksi belirtilmedikçe ya da objektif nedenler aksini gerektirmedikçe, niteliksel ve niceliksel devamlılık, düzenlilik, güvenilirlik, verimlilik, açıklık, şeffaflık ve kaynakların verimli kullanılmasının gözetilmesi.
- f) Elektronik haberleşme sistemlerinin uluslararası normlara uygun olması.

- g) Teknolojik yeniliklerin uygulanması ile araştırma-geliştirme faaliyet ve yatırımlarının teşvik edilmesi.
- ğ) Hizmet kalitesi artırımının teşvik edilmesi.
- h) Millî güvenlik ile kamu düzeni gereklerine ve acil durum ihtiyaçlarına öncelik verilmesi.
- ı) Bu Kanunda, ilgili mevzuatta ve yetkilendirmelerde açıkça belirlenen durumlar haricinde, işletmecilerin, arabağlantı da dahil olmak üzere erişim ücretleri ile hat ve devre kiralalarını da kapsayacak biçimde, elektronik haberleşme hizmeti sunulması karşılığı alacakları ücretleri serbestçe belirlemesi.
- i) Elektronik haberleşme cihaz ve sistemlerinin kurulması, kullanılması ve işletilmesinde insan sağlığı, can ve mal güvenliği, çevre ve tüketicinin korunması açısından asgarî uluslararası normların dikkate alınması.
- j) Elektronik haberleşme hizmetlerinin sunulmasında ve bu hususlarda yapılacak düzenlemelerde tarafsızlığın sağlanması.
- k) Teknolojik yeniliklerin kullanılması da dahil olmak üzere engelli, yaşlı ve sosyal açıdan korunmaya muhtaç diğer kesimlerin özel ihtiyaçlarının dikkate alınması
- l) Bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi.

İKİNCİ BÖLÜM

Elektronik Haberleşme Sektöründe Yetkili

Merciler ve Görevleri

Bakanlığın görev ve yetkileri

MADDE 5 - (1) Bakanlığın elektronik haberleşme sektörüne ilişkin yetki ve görevleri şunlardır:

- a) Numaralandırma, internet alan adları, uydu pozisyonu, frekans tahsisi gibi kıt kaynaklara dayalı elektronik haberleşme hizmetlerine ilişkin strateji ve politikaları belirlemek.
- b) Elektronik haberleşme sektörünün; serbest rekabet ortamında gelişimini teşvik etmeye ve bilgi toplumuna dönüşümün desteklenmesini sağlamaya yönelik hedef, ilke ve politikaları belirlemek ve bu amaçla teşvik edici tedbirleri almak.
- c) Elektronik haberleşme alt yapı, şebeke ve hizmetlerinin; teknik, ekonomik ve sosyal ihtiyaçlara, kamu yararına ve millî güvenlik amaçlarına uygun olarak kurulması, geliştirilmesi ve birbirlerini tamamlayıcı şekilde yürütülmesini sağlamaya yönelik politikaları belirlemek.

- ç) Elektronik haberleşme cihazları sanayisinin gelişmesine ilişkin politikaların oluşumuna ve elektronik haberleşme cihazları bakımından yerli üretimi özendirici tedbirleri almaya yönelik politikaları belirlemeye katkıda bulunmak.
- d) Ülkemizin üyesi bulunduğu elektronik haberleşme sektörü ile ilgili uluslararası birlik ve kuruluşlar nezdinde 5/5/1969 tarihli ve 1173 sayılı Milletlerarası Münasebetlerin Yürütülmesi ve Koordinasyonu Hakkında Kanun hükümleri saklı kalmak üzere Devleti temsil etmek veya temsile yetkilendirmek, çalışmalara katılım ve kararların uygulanması konusunda koordinasyonu sağlamak.
- e) Elektronik haberleşme politikalarının tespiti ve uygulanması amacıyla gerekli araştırmaları yapmak ve yaptırmak.
- f) Elektronik haberleşmenin doğal afetler ve olağanüstü haller nedeniyle aksamamasını teminen gerekli tedbirleri almak ve koordinasyonu sağlamak. Haberleşmenin aksamaya riskine karşı önceden haberleşmenin kesintisiz bir biçimde sağlanmasına yönelik alternatif haberleşme alt yapısını kurmak, kurdurmak ve ihtiyaç durumunda söz konusu sistemi devreye sokmak.
- g) Olağanüstü hal ve savaşta elektronik haberleşme hizmetlerini, 16/7/1965 tarihli ve 697 sayılı Kanun hükümleri dahilinde planlamak, gerekli işleri yapmak ve yaptırmak.
- ğ) Elektronik haberleşme sistemlerinin yerli tasarım ve üretimini, bu amaçla sektöre ilişkin araştırma, geliştirme ve eğitim faaliyetlerini teknik ve maddi destek de dahil olmak üzere teşvik etmek ve Kurumun gelirlerinin % 20'sini aşmamak kaydıyla söz konusu faaliyetlere ilişkin olarak ayıracağı kaynağı belirlemek ve bu kaynağın kullanımına ilişkin gereken düzenlemeleri yaparak bu kaynağı kullandırmak.
- h) (Ek: 6/2/2014-6518/102 md.) Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek, eylem planlarını hazırlamak, (...) ilgili faaliyetlerin koordinasyonunu sağlamak, kritik altyapılar ile ait oldukları kurumları ve konumları belirlemek, gerekli müdahale merkezlerini kurmak, kurdurmak ve denetlemek, her türlü siber müdahale aracının ve millî çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapmak, yaptırmak ve bunları teşvik etmek ve siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek, siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlamak.(5)
- ı) (Ek: 27/3/2015-6639/31 md.) Ulusal kamu entegre veri merkezlerine yönelik politika, strateji ve hedefleri belirlemek, eylem planlarını hazırlamak, eylem planlarını izlemek, e-Devlet hizmetlerinde

kullanılan verilerin ve sistemlerin barındırıldığı veri merkezlerini kamu entegre veri merkezlerinde toplamak amacıyla verilerin transferi de dahil gerekli altyapıları kurmak, kurdurmak, işletmek, işletmek ve tüm bu faaliyetlere yönelik uygulama usul ve esaslarını belirlemek, kurulum, uygulama ve işletim süreçlerini planlamak, yürütmek ve koordine etmek.

Kurumun görev ve yetkileri

MADDE 6 - (1) Kurumun görev ve yetkileri şunlardır:

a) Elektronik haberleşme sektöründe; rekabeti tesis etmeye ve korumaya, rekabeti engelleyici, bozucu veya kısıtlayıcı uygulamaların giderilmesine yönelik düzenlemeleri yapmak, bu amaçla ilgili pazarlarda etkin piyasa gücüne sahip işletmecilere ve gerekli hallerde diğer işletmecilere yükümlülükler getirmek ve mevzuatın öngördüğü tedbirleri almak.

b) Bu Kanun ve bu Kanuna dayanılarak yapılan düzenlemelere aykırı olarak, elektronik haberleşme sektöründe ortaya çıkan rekabet ihlallerini denetlemek, yaptırım uygulamak, mevzuatın öngördüğü hallerde elektronik haberleşme sektöründe rekabet ihlallerine ilişkin konularda Rekabet Kurumundan görüş almak.

c) Abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak.

ç) İşletmeciler ile tüketicileri ilgilendiren Kurul kararlarını gerekçe ve süreçleri ile kamuoyuna açık tutmak.

d) Bu Kanun çerçevesinde gerektiğinde işletmeciler arasında uzlaştırma prosedürünü işletmek, uzlaşma sağlanamadığı takdirde ilgili taraflar arasında aksi kararlaştırılıncaya kadar geçerli olmak üzere gerekli tedbirleri almak.

e) Elektronik haberleşme sektöründeki gelişmeleri takip etmek, sektörün gelişimini teşvik etmek amacıyla gerekli araştırmaları yapmak veya yaptırmak ve bu konularda ilgili kurum ve kuruluşlarla işbirliği halinde çalışmak.

f) Bu Kanununun 5 inci maddesinin (a) bendini de göz önünde bulundurarak, elektronik haberleşme hizmetlerinin sunulması ve elektronik haberleşme şebeke ve altyapılarının tesis ve işletilmesi için gerekli olan frekans, uydu pozisyonu ve numaralandırma planlamasını ve tahsisini yapmak.

g) Elektronik haberleşme ile ilgili olarak Bakanlığın strateji ve politikalarını dikkate alarak, yetkilendirme, tarifeler, erişim, geçiş hakkı, numaralandırma, spektrum yönetimi, telsiz cihaz ve

sistemlerine kurma ve kullanma izni verilmesi, spektrumun izlenmesi ve denetimi, piyasa gözetimi ve denetimi de dahil gerekli düzenlemeler ile denetlemeleri yapmak.

ğ) Telsiz sistemlerinin belirlenen tekniklere ve usullere uygun olarak kurulmasının ve çalıştırılmasının kontrolünü yapmak, elektromanyetik girişimleri tespit etmek ve giderilmesini sağlamak.

h) İşletmecilerin ticari sırları ile kamuoyuna açıklanabilecek bilgilerinin kapsamını belirlemek, işletmecilerin ticari sırları ile yatırım ve iş planlarının gizliliğini korumak ve bunları adli makamların talepleri dışında muhafaza etmek.

ı) Elektronik haberleşmeyle ilgili olarak, işletmeciler, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden ihtiyaç duyacağı her türlü bilgi ve belgeyi almak ve gerekli kayıtları tutmak, Bakanlık tarafından elektronik haberleşme sektörüne yönelik strateji ve politikaların belirlenmesinde ihtiyaç duyulanları, talebi üzerine Bakanlığa iletmek.

i) Bu Kanunun 5 inci maddesinin birinci fıkrasının (ğ) bendi uyarınca Bakanlıkça yapılacak düzenlemeler çerçevesinde, elektronik haberleşme sektörüne ilişkin araştırma, geliştirme ve eğitim faaliyetlerine ilişkin olarak, mevcut Kurum gelirlerini göz önünde bulundurarak gelirlerinin % 20'sini aşmamak kaydıyla ayıracağı kaynağı Bakanlığa aktarmak. Bu aktarım, katma değer vergisi ve damga vergisi dahil her türlü vergi, resim, harç ve benzeri mali yükümlülüklerden istisnadır.

j) Kullanıcılara ve erişim kapsamında diğer işletmecilere uygulanacak tarifelere, sözleşme hükümlerine, teknik hususlara ve görev alanına giren diğer konulara ilişkin genel kriterler ile uygulama usul ve esaslarını belirlemek, tarifeleri onaylamak, tarifelerin denetlenmesine ilişkin düzenlemeleri yapmak.

k) İşletmeciler tarafından hazırlanan referans erişim tekliflerini onaylamak.

l) Yürütülecek elektronik haberleşme hizmetleri, şebeke ve/veya alt yapısı ile ilgili olarak yapılacak yetkilendirmelere ilişkin hüküm ve şartları belirlemek, uygulanmasını ve yetkilendirmeye uygunluğu denetlemek, bu hususta gereken iş ve işlemleri yürütmek ve mevzuatın öngördüğü tedbirleri almak.

m) Radyo ve televizyon yayıncılığına ilişkin ilgili kanununda belirtilen hükümler saklı kalmak kaydıyla, frekans planlama, tahsis ve tescil işlemlerini, güç ve yayın sürelerini de göz önünde tutarak uluslararası kuruluşlarla işbirliği de yapmak suretiyle yürütmek.

- n) Elektronik haberleşme sektöründe kullanılacak her çeşit sistem ve cihazların, uyumlaştırılmış ulusal standartlarını yayımlamak ve uygulanmasını sağlamak, teknik düzenlemelerini yapmak, piyasa denetimini yapmak ve/veya yaptırmak, bu amaçla laboratuvarlar kurup işletebilmek ve bu laboratuvarlarda verebileceği eğitim ve danışmanlık hizmetleri karşılığında alınacak ücretleri belirlemek.
- o) Elektronik haberleşme sektöründe tesis, ölçüm ve bakım-onarım yapacak kuruluşların yetkilendirmesini bu konuda görevli kuruluşlarla koordine etmek.
- ö) Elektronik haberleşme sektörüne yönelik pazar analizleri yapmak, ilgili pazarı ve ilgili pazarda etkin piyasa gücüne sahip işletmeci veya işletmecileri belirlemek.
- p) Elektronik haberleşme sektörü ile ilgili uluslararası birlik ve kuruluşların çalışmalarına katılmak, kararların uygulanmasını takip etmek ve gerekli koordinasyonu sağlamak.
- r) Bu Kanununun 46 ncı maddesinde belirtilen ücretlerle ilgili olarak terkin de dahil olmak üzere her türlü usul ve esasları belirlemek, Kurumun yıllık bütçesini, gelir-gider kesin hesabını, yıllık çalışma programını onamak, gerekirse bütçede hesaplar arasında aktarma yapmak veya gelir fazlasını mevzuat çerçevesinde genel bütçeye devretmek.
- s) Elektronik haberleşme sektöründe faaliyet gösterenlerin mevzuata uymasını denetlemek ve/veya denetlettirmek, konu ile ilgili usul ve esasları belirlemek, aykırılık halinde mevzuatın öngördüğü işlemleri yapmak ve yaptırımları uygulamak.
- ş) Elektronik haberleşme sektörüne yönelik olarak, millî güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirleri almak.
- t) Ara bağlantı ve ulusal dolaşım da dahil erişim ile ilgili uygulanacak usul ve esasları belirlemek ve mevzuatın öngördüğü düzenlemeleri yapmak, elektronik haberleşme sağlanması amacıyla imzalanan anlaşmaların rekabeti kısıtlayan, mevzuata ve/veya tüketici menfaatlerine aykırı hükümler içermemesi amacıyla mevzuatın öngördüğü tedbirleri almak.
- u) İlgili kanun hükümleri dahilinde, evrensel hizmetlere ilişkin hizmet kalitesi ve standartları da dahil olmak üzere, gerektiğinde her türlü elektronik haberleşme hizmetine yönelik hizmet kalitesi ve standartlarını belirlemek, denetlemek, denetlettirmek ve buna ilişkin usul ve esasları belirlemek.
- ü) Elektronik haberleşme sektöründe, bağımsız denetim faaliyetine ilişkin esasları, bağımsız denetleme faaliyetlerinde bulunacak kuruluşların kuruluş şartlarını, çalışma esaslarını ve çalıştıracağı personelin niteliklerini belirlemek.

v) (Ek: 6/2/2014-6518/103 md.) Siber güvenlik ve internet alan adları konularında Cumhurbaşkanı, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri Telekomünikasyon İletişim Başkanlığı veya diğer birimleri marifetiyle yerine getirmek.

y) Bu Kanunla verilen görevlere ilişkin yönetmelik, tebliğ ve diğer ikincil düzenlemeleri çıkarmak.

Rekabetin sağlanması

MADDE 7 - (1) Kurum, 7/12/1994 tarihli ve 4054 sayılı Rekabetin Korunması Hakkında Kanun hükümleri saklı kalmak kaydıyla, elektronik haberleşme sektöründe rekabete aykırı davranış ve uygulamaları re'sen veya şikâyet üzerine incelemeye, soruşturmaya ve rekabetin tesisine yönelik gerekli gördüğü tedbirleri almaya, görev alanına giren konularda bilgi ve belgelerin sağlanmasını talep etmeye yetkilidir.

(2) Rekabet Kurulu, elektronik haberleşme sektörüne ilişkin olarak yapacağı inceleme ve tetkiklerde, birleşme ve devralmalara ilişkin olarak vereceği kararlar da dahil olmak üzere elektronik haberleşme sektörüne ilişkin olarak vereceği tüm kararlarda, öncelikle Kurumun görüşünü ve Kurumun yapmış olduğu düzenleyici işlemleri dikkate alır.

(3) Kurum, yapacağı pazar analizleri sonucu ilgili pazarlarda etkin piyasa gücüne sahip işletmecileri belirleyebilir. Kurum, etkin rekabet ortamının sağlanması ve korunması amacıyla etkin piyasa gücüne sahip işletmecilere yükümlülükler getirebilir. Aynı ve/veya farklı pazarlarda etkin piyasa gücüne sahip olan işletmeciler arasında söz konusu yükümlülükler açısından farklılaştırma yapılabilir.

(...)

İşletmecilerin hak ve yükümlülükleri

MADDE 12 - (1) İşletmeci, Kurum düzenlemeleri ve yetkilendirmesinde öngörülen şartlara uygun olarak yetkilendirildiği kapsamdaki elektronik haberleşme hizmetini sunma hakkına sahiptir.

(2) Kurum, işletmecilere sektörün ihtiyaçları, uluslararası düzenlemeler, teknolojiye meydana gelen gelişmeler gibi hususları gözeterek aşağıdaki hususlar başta olmak üzere, mevzuat doğrultusunda yükümlülükler getirebilir:

a) İdari ücretler.

b) Hizmetlerin birbiriyle uyumlu çalışabilmesi ve şebekelerarası arabağlantının sağlanması.

c) Ulusal numaralandırma planındaki numaralardan son kullanıcılara erişimin sağlanması.

- ç) Ortak yerleşim ve tesis paylaşımı.
 - d) Kişisel veri ve gizliliğin korunması.
 - e) Tüketicinin korunması.
 - f) Kuruma bilgi ve belge verilmesi.
 - g) Kanunlarla yetkili kılınan ulusal kurumlarca yasal dinleme ve müdahalenin yapılmasına teknik olanak sağlanması.
 - ğ) Afet durumlarındaki haberleşmenin kesintisiz devam edebilmesi için gerekli tedbirlerin alınması.
 - h) Elektronik haberleşme şebekelerinden kaynaklanan elektromanyetik alanlara kamu sağlığını tehdit edecek şekilde maruz kalınmasının engellenmesi ile ilgili önlemlerin bu Kanun çerçevesinde alınması.
 - ı) Erişim yükümlülükleri.
 - i) Elektronik haberleşme şebekelerinin bütünlüğünün idame ettirilmesi.
 - j) İzinsiz erişime karşı şebeke güvenliğinin sağlanması.
 - k) Hizmet kalitesi de dahil olmak üzere standartlar ve spesifikasyonlara uyumluluk.
 - l) İlgili mevzuat uyarınca Kurum tarafından istenen hizmetleri yerine getirmek.
- (3) Kullanım hakkı verildiği durumlarda, yukarıdakilere ilaveten sektörün ihtiyaçları, uluslararası düzenlemeler, teknolojide meydana gelen gelişmeler gibi hususları gözetenek aşağıdaki hususlar başta olmak üzere, mevzuat doğrultusunda yükümlülükler getirilebilir:
- a) Frekans kullanım hakkının verildiği hizmet, şebeke ya da teknoloji türü ile numara kullanım hakkının verildiği hizmetin kapsamı.
 - b) Frekans ve numaraların etkin ve verimli kullanımı.
 - c) Elektromanyetik girişimin önlenmesi.
 - ç) Numara taşınabilirliği.
 - d) Rehber hizmeti.
 - e) Yetkilendirme süresi.
 - f) Hak ve yükümlülüklerin devri.
 - g) Kullanım hakkı ücretleri.

ğ) İhale sürecinde üstlenilen taahhütler.

h) Frekans ve numara kullanımları ile ilgili uluslararası anlaşmalar çerçevesindeki yükümlülüklere uyulması.

(4) İşletmecilerin hak ve yükümlülükleri ile ilgili usul ve esaslar Kurumca belirlenir.

(5) İşletmeciler, elektronik haberleşme sistemleri üzerinden millî güvenlikle ve 5397 ve 5651 sayılı kanunlar ve ilgili diğer kanunlarda getirilen düzenlemelerle ilgili taleplerin karşılanmasına yönelik teknik alt yapıyı, elektronik haberleşme sistemini hizmete sunmadan önce kurmakla yükümlüdür. Halen elektronik haberleşme hizmeti sunan işletmeciler de; söz konusu teknik alt yapıyı, Kurum tarafından belirlenecek süre içerisinde aynı şartlarla ve tüm harcamaları kendilerine ait olmak üzere kurmakla yükümlüdürler.

(...)

Kişisel verilerin işlenmesi ve gizliliğin korunması

MADDE 51 - (İptal: Anayasa Mahkemesi'nin 9/4/2014 tarihli ve E.: 2013/122 K.: 2014/74 sayılı Kararı ile.; Yeniden düzenleme: 27/3/2015-6639/32 md.)

(1) Kişisel verilerin işlenmesinde; hukuka ve dürüstlük kurallarına uygun olması, doğru ve gerektiğinde güncel olması, belirli, açık ve meşru amaçlar için işlenmesi, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ile işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi ilkelerine uyulur.

(2) Elektronik haberleşmenin ve ilgili trafik verisinin gizliliği esas olup, ilgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi yasaktır.

(3) Elektronik haberleşme şebekeleri, haberleşmenin sağlanması dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla işletmeciler tarafından ancak ilgili abonelerin/kullanıcıların verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve açık rızalarının alınması kaydıyla kullanılabilir.

(4) İşletmeciler şebekelerinin, abonelerine/kullanıcılarına ait kişisel verilerin ve sundukları hizmetlerin güvenliğini sağlamak amacıyla uygun teknik ve idari tedbirleri alır.

(5) Bu Kanunun 49 uncu maddesi kapsamında veya kamu yararının sağlanması amacıyla Kurum tarafından işletmecilere getirilen yükümlülüklerin yerine getirilebilmesi için kişisel veriler işlenebilir.

(6) Kişisel verilerin yurt dışına aktarılmasına ilişkin ilgili mevzuat hükümleri saklı kalmak kaydıyla, trafik ve konum verileri ancak ilgili kişilerin açık rızaları alınmak koşuluyla yurt dışına aktarılabilir.

(7) Trafik verileri; trafiğin yönetimi, arabağlantı, faturalama, usulsüzlük/dolandırıcılık tespitleri ve benzeri işlemleri gerçekleştirmek veya tüketici şikâyetleri ile arabağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü amacıyla sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla işlenir ve bu uzlaşmazlıkların çözüm süreci tamamlanıncaya kadar gizliliği ve bütünlüğü sağlanarak saklanır. Katma değerli elektronik haberleşme hizmetlerinin sunulması ya da elektronik haberleşme hizmetlerinin pazarlanması amacıyla ihtiyaç duyulan trafik verileri ile konum verileri anonim hâle getirilerek veya ilgili abonelerin/kullanıcıların açık rızalarının alınması ve sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla, belirtilen faaliyetlerin gerektirdiği ölçü ve sürede işlenebilir.

(8) İşletmeciler konum verilerinin işlenmesinde abonelere/kullanıcılara bu verilerin işlenmesini reddetme imkânı sağlar. İlgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde ancak acil yardım çağrıları ile 29/5/2009 tarihli ve 5902 sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanunda tanımlanan afet ve acil durum hâllerinde abonelerin/kullanıcıların açık rızası aranmaksızın konum verileri ve ilgili kişilerin kimlik bilgileri işletmeci tarafından yetkilendirilen kişilerle sınırlı olmak kaydıyla işlenebilir.

(9) Abone/kullanıcı şikâyetlerinin incelenmesi ve denetim faaliyetleri kapsamında trafik ve konum verileri ile kişisel veriler, belirtilen faaliyetlerle sınırlı olmak kaydıyla işlenebilir.

(10) Bu Kanun kapsamında sunulan hizmetlere ilişkin olarak;

a) Soruşturma, inceleme, denetleme veya uzlaşmazlığa konu olan kişisel veriler ilgili süreç tamamlanıncaya kadar,

b) Kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtları iki yıl,

c) Kişisel verilerin işlenmesine yönelik abonelerin/kullanıcıların rızalarını gösteren kayıtlar asgari olarak abonelik süresince, saklanır. Veri kategorileri ile haberleşmenin yapıldığı tarihten itibaren bir yıldan az ve iki yıldan fazla olmamak üzere verilerin saklanma süreleri yönetmelikle belirlenir.

(11) (Değişik:17/7/2019-7186/22 md.) Tahsilata ilişkin riskin yönetilmesi ve kötü niyetli kullanımların önlenmesi amacıyla abonelerin elektronik haberleşme hizmetlerine ve elektronik kimlik bilgisini haiz cihazlara yönelik tarafların kendi sistemlerinde oluşan fatura tutarı ve ödeme bilgileri ile sahtecilik, dolandırıcılık riski içeren şüpheli veya zarar doğurucu vakalara ve işlem hareketlerine ilişkin kayıtlar, işletmeciler ve Kurumun MCKS'si arasında paylaşılabilir veya işlenebilir.

(12) Bu Kanun kapsamında kişisel verilerin gizliliğinin, güvenliğinin ve amacı doğrultusunda kullanılmasının temininden işletmeciler sorumludur.

(13) Bu maddenin uygulanmasına ilişkin usul ve esaslar Kurum tarafından belirlenir.

(...)

İKİNCİ BÖLÜM

Kurumun Yetkisi ve İdari Yaptırımlar

Kurumun yetkisi ve idarî yaptırımlar

MADDE 60 - (1) Kurum; mevzuata, kullanım hakkı ve diğer yetkilendirme şartlarına uyulmasını izleme ve denetlemeye, aykırılık halinde işletmecilere bir önceki takvim yılındaki net satışlarının yüzde üçüne kadar idarî para cezası uygulamaya, millî güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi ve kanunlarla getirilen hükümlerin uygulanması amaçlarıyla gerekli tedbirleri almaya, gerektiğinde tesisleri tazminat karşılığında devralmaya, belirlediği süre içerisinde yetkilendirme ücretinin ödenmemesi ya da ağır kusur halinde verdiği yetkilendirmeyi iptal etmeye yetkilidir. Ancak, Kurum, ulusal çapta verilecek frekans bandı kullanımını ihtiva eden ve sınırlı sayıda işletmeci tarafından yürütülmesi gereken elektronik haberleşme hizmetlerine ilişkin yetkilendirmelerin iptalini gerektiren hallerde Bakanlığın görüşünü alır.

(2) Kurum, işletmecinin faaliyete yeni başlamış olması halinde, ihlalin niteliği, ihlal neticesinde herhangi bir ekonomik kazanç elde edilip edilmemesi, iyi niyet ve gönüllü bildirim gibi ölçütleri de dikkate alarak önceden belirleyeceği usul ve esaslar çerçevesinde bin liradan bir milyon liraya kadar idarî para cezası ile bu Kanunda belirtilen diğer idarî yaptırımları uygulamaya yetkilidir.

(3) Kurum, kamu hizmetinin gerekleri ve kamu düzeninin korunması amacıyla yönetmelikle önceden belirleyeceği hallerde, işletmecinin faaliyetinin geçici olarak durdurulmasına ya da ihlalin önlenmesi için işletmeciye somut tedbirler uygulama zorunluluğu getirmeye de yetkilidir.

(4) Elektronik haberleşme hizmeti sunan bir işletmeci ile abonelik sözleşmesi yapan gerçek ve tüzel kişiler faaliyetlerinin gereği olarak aldıkları hizmeti üçüncü kişilere ücretli veya ücretsiz verebilir. Aboneler yararlandıkları hizmeti ticaret amacıyla üçüncü kişilere sunamazlar. Aksine davrananların abonelik sözleşmeleri iptal edilir.

(5) Kurumun belirlediği usul ve esaslar çerçevesinde elektronik haberleşme tesisleri ile ilgili bildirimlerin yapılmaması veya güvenlik sertifikası alınmadan kurulması veya Kurum veya Kurum tarafından yetki verilen kuruluşlarca yapılacak ölçümler sonucu Kurum tarafından belirlenen

elektromanyetik alan şiddeti limit değere uygun bulunmaması hallerinde, bunların sahibine bu Kanuna ekli ücret tarifesinde belirlenen ruhsatname ücretinin elli katı idarî para cezası her bir cihaz için ayrı ayrı uygulanır. Bu Kanunun 46 ncı maddesinin ikinci fıkrasında telsiz ruhsatnamesi ve yıllık kullanım ücretinden muaf tutulanlar hakkında da bu madde hükümleri uygulanır. Bu fıkradaki idarî para cezaları Kurumun taşra teşkilatı tarafından da verilebilir.

(6) Bu Kanunun 53 üncü maddesinin birinci fıkrasına aykırılık hallerinde, 4703 sayılı Kanunun 12 nci maddesinde dağıtıcı, üretici ve onaylanmış kuruluşlar bakımından öngörülmüş bulunan idarî para cezaları bir katından dört katına kadar artırılarak uygulanır.

(7) Bu Kanunun 57 nci maddesinin birinci fıkrasına aykırı hareket edenlere, cihaz başına onbin liradan yirmibin liraya kadar; ikinci fıkrasına aykırı hareket edenlere onmilyon liraya kadar idarî para cezası verilir.

(8) Bu maddedeki idarî para cezaları Kurum tarafından verilir.

(9) (Ek: 28/11/2017-7061/99 md.) İşletmecinin tüketicilerden haksız olarak ücret tahsil ettiğinin tespiti hâlinde, idari yaptırım uygulama hakkı saklı kalmak kaydıyla, işletmeci bu tutarları tüketicilere iade etmekle yükümlüdür. İadeye ilişkin kararın Kurum tarafından işletmeciye tebliğ edildiği tarihten itibaren iki yıl içerisinde işletmecinin tüketiciye ulaşamaması veya Kurum tarafından haklı görülen herhangi bir nedenle işletmeci tarafından iadelerin gerçekleştirilememesi halinde, bu iade bedelleri evrensel hizmet gelirleri olarak genel bütçeye gelir kaydedilmek üzere Bakanlığın merkez muhasebe birimi hesabına yatırılır. Bu fıkranın uygulanmasına ilişkin usul ve esaslar Kurum tarafından belirlenir.

(10) (Ek: 15/8/2016-KHK-671/25 md.; Aynen kabul: 9/11/2016-6757/22 md.) Anayasanın 22 nci maddesinde sayılan sebeplerden biri veya birkaçına bağlı olarak, gecikmesinde sakınca bulunan hâllerde Cumhurbaşkanlığı, alınması gereken tedbirleri belirler ve uygulanmak üzere Kuruma bildirir. Kurum Başkanı, Cumhurbaşkanlığının gerekli gördüğü tedbirlere ilişkin kararını derhal işletmecilere, erişim sağlayıcılara, veri merkezlerine ve ilgili içerik ve yer sağlayıcılara bildirir. Bu kararın gereği, derhal ve kararın bildirilmesi anından itibaren en geç iki saat içinde yerine getirilir. Bu karar, yirmidört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim kararını kırksekiz saat içinde açıklar, aksi halde karar kendiliğinden kalkar.

(11) (Ek: 15/8/2016-KHK-671/25 md.; Aynen kabul: 9/11/2016-6757/22 md.) Kurum, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır.

(12) (Ek: 15/8/2016-KHK-671/25 md.; Aynen kabul: 9/11/2016-6757/22 md.) Kurum, görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilir ve değerlendirmesini yapabilir; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilir, bunlarla irtibat kurabilir ve bu kapsamda diğer gerekli önlemleri alabilir veya aldırabilir. Kurum, bu fıkrada belirtilen görevlerin ifasında bakanlıklar, kurum ve kuruluşlar ile işbirliği içerisinde çalışır. Bu kapsamda Kurum tarafından istenen her türlü bilgi ve belge talebi; ilgili bakanlık, kurum ve kuruluşlar tarafından gecikmeksizin yerine getirilir. Bu fıkraya göre bilgi ve belge talebinde bulunulması ve bu taleplerin yerine getirilmesine ilişkin usul ve esaslar ile diğer hususlar Cumhurbaşkanlığınca belirlenir.

(13) (Ek: 15/8/2016-KHK-671/25 md.; Aynen kabul: 9/11/2016-6757/22 md.) Gerçek kişiler ile özel hukuk tüzel kişileri, Kurumun bu maddedeki görevleri ile ilgili taleplerini, tabi oldukları mevzuat hükümlerini gerekçe göstermek suretiyle yerine getirmekten kaçınamazlar. İşletmeciler dışında Kurumun görevleri ile ilgili yükümlülüklerini yerine getirmeyenlere bu maddenin ikinci fıkrasındaki yaptırım uygulanır.

(14) (Ek: 28/11/2017-7061/99 md.) Eksik ödenen Kurum alacaklarının hesaplanmasında, işletmecilerce fazla ödendiği tespit edilen tutarlar, ödendikleri tarih esas alınarak mahsup edildikten sonra kalan tutar dikkate alınır. Bu takdirde mahsup suretiyle tahsil edilen Kurum alacağı, vadesinden sonra tahsil edilmişse tahsil tarihine kadar gecikme zammı uygulanır.

(15) Bu maddenin uygulanmasına ve bu Kanunda öngörülen yükümlülüklerin işletmeciler tarafından yerine getirilmemesi halinde uygulanacak idarî para cezalarına ilişkin hususlar Kurum tarafından çıkarılacak yönetmelikle düzenlenir.

5718 sayılı Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun

Resmî Gazete Tarihi : 12/12/2007

Resmî Gazete Sayısı : 26728

MİLLETLERARASI ÖZEL HUKUK VE USUL HUKUKU HAKKINDA KANUN

BİRİNCİ KISIM

Milletlerarası Özel Hukuk

BİRİNCİ BÖLÜM

Genel Hükümler

Kapsam

MADDE 1 - (1) Yabancılik unsuru taşıyan özel hukuka ilişkin işlem ve ilişkilerde uygulanacak hukuk, Türk mahkemelerinin milletlerarası yetkisi, yabancı kararların tanınması ve tenfizi bu Kanunla düzenlenmiştir.

(2) Türkiye Cumhuriyetinin taraf olduğu milletlerarası sözleşme hükümleri saklıdır.

(...)

Kişilik haklarının ihlâlinde sorumluluk

MADDE 35 - (1) Kişilik haklarının, basın, radyo, televizyon gibi medya yoluyla, internet veya diğer kitle iletişim araçları ile ihlâlinden doğan taleplere, zarar görenin seçimine göre;

a) Zarar veren, zararın bu ülkede meydana geleceğini bilecek durumda ise zarar görenin mutad meskeni hukuku,

b) Zarar verenin işyeri veya mutad meskeninin bulunduğu ülke hukuku veya

c) Zarar veren, zararın bu ülkede meydana geleceğini bilecek durumda ise zararın meydana geldiği ülke hukuku,

uygulanır.

(2) Kişilik haklarının ihlâlinde cevap hakkı, süreli yayınlarda, münhasıran baskının yapıldığı ya da programın yayınlandığı ülke hukukuna tâbidir.

(3) Maddenin birinci fıkrası, kişisel verilerin işlenmesi veya kişisel veriler hakkında bilgi alma hakkının sınırlandırılması yolu ile kişiliğin ihlâl edilmesinden doğan taleplere de uygulanır.

5684 sayılı Sigortacılık Kanunu

Resmî Gazete Tarihi : 14/6/2007

Resmî Gazete Sayısı : 26552

SİGORTACILIK KANUNU

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç ve kapsam

MADDE 1 - (1) Bu Kanunun amacı, ülkemiz sigortacılığının geliştirilmesini sağlamak, sigorta sözleşmesinde yer alan kişilerin hak ve menfaatlerini korumak ve sigortacılık sektörünün güvenli ve istikrarlı bir ortamda etkin bir şekilde çalışmasını temin etmek üzere bu Kanuna tâbi kişi ve kuruluşların, faaliyete başlama, teşkilât, yönetim, çalışma esas ve usûlleri ile faaliyetlerinin sona ermesi ve denetlenmesine ilişkin hususlar ve sigorta sözleşmesinden doğan uyuşmazlıkların çözümlenmesine yönelik olarak sigorta tahkim sistemi ile ilgili usûl ve esasları düzenlemektir.

(2) Türkiye’de faaliyet gösteren sigorta şirketleri, reasürans şirketleri, Türkiye Sigorta, Reasürans ve Emeklilik Şirketleri Birliği, araçlar, aktüerler ile sigorta eksperleri bu Kanun hükümlerine tâbidir.

(3) Sosyal güvenlik kurumları, Türkiye İhracat Kredi Bankası Anonim Şirketi ile bu Kanunun denetimle ilgili hükümleri hariç olmak üzere özel kanunlarına göre sigortacılık faaliyetinde bulunan diğer kuruluşlar bu Kanun kapsamında değildir.

(...)

BEŞİNCİ BÖLÜM

Aktüerler, Araçlar ve Sigorta Eksperleri

Aktüerler ve brokerler

MADDE 21 - (1) Sigorta şirketleri ile reasürans şirketleri, yeterli sayıda aktüerle çalışmak zorundadır. Müsteşarlık tarafından aktüerlerin kaydedildiği bir Aktüerler Sicili tutulur. Sicile kaydolunmadan aktüerlik yapılamaz. Aktüerlik unvanının kazanılması ile aktüerlerin görev ve yetkilerine ilişkin usûl ve esaslar yönetmelikle belirlenir.

(2) Brokerlik, Müsteşarlıktan alınan brokerlik ruhsatı ile yapılır. Müsteşarlık, ruhsat ile ilgili işlemlerin incelemeye ve onaya hazır hale getirilmesi hususunda ilgili sivil toplum ve meslek kuruluşlarına görev verebilir. Brokerlerin görev ve yetkilerine ilişkin usûl ve esaslar yönetmelikle belirlenir.

(3) Sigorta şirketlerinin, sigorta acentelerinin ve sigorta eksperlerinin ortakları, yönetim ve denetiminde bulunan kişiler ve bunlar adına imza atmaya yetkili olanlar ile meslekî faaliyette bulunan şirket çalışanları; brokerlik yapamaz, tüzel kişi brokerin yönetim ve denetim kurullarında görev alamaz, imzaya yetkili olarak çalışamaz, bunlara ortak olamaz ve bunlardan ücret karşılığı herhangi bir iş kabul edemez. Bu sınırlandırmalar söz konusu kimselerin eş ve velayeti altındaki çocukları için de geçerlidir.

(4) Sigorta brokerliği yapması yasaklananlar, brokerlik ile ilgili faaliyetlerde çalıştırılmaz ve her ne şekilde olursa olsun bu kişilerle brokerlik mesleğinin icrası için işbirliği yapılamaz.

(5) Sigorta brokerleri ve bunların yanlarında çalışanlar, işleri dolayısıyla öğrendikleri bilgi ve sırları ilgililerin izni olmaksızın açıklayamaz. Ancak, suç teşkil eden hallerin yetkili mercilere duyurulması zorunludur.

Sigorta eksperleri

MADDE 22 - (1) Sigorta eksperliği gerçek veya tüzel kişilerce yapılır.

(2) Sigorta eksperliği yapmak isteyen kişilerin;

a) Müsteşarlıktan sigorta eksperlik ruhsatı alması,

b) Levhaya yazılı olması,

gerekir.

(3) Yabancı sigorta eksperlerinin faaliyetlerine ilişkin usûl ve esasları belirlemeye Cumhurbaşkanı yetkilidir.(1)

(4) Sigorta eksperleri unvanı, sigorta eksperliği ruhsatnamesinin alınmasından sonra kazanılır. Sigorta eksperliği yapacaklar, ruhsatnamelerini aldıktan sonra Levhaya kayıt olmak için Türkiye Odalar ve Borsalar Birliğine başvurur. Müsteşarlık, ruhsatnameye ilişkin işlemlerin incelemeye ve onaya hazır hale getirilmesi hususunda ilgili sivil toplum ve meslek kuruluşlarına görev verebilir.

(5) Sigorta eksperinin kaydı;

a) Almış olduğu ruhsatların tümü iptal edilmişse,

b) Hakkında meslekten çıkarma kararı verilmişse,

c) Levhaya yazılmasından itibaren altı ay içinde mesleğini ifa etmezse,

ç) Sigorta eksperliğinden ayrılmışsa,

d) Tespit edilen kayıt ücretini süresi içinde yatırmamışsa veya aidatını üç yıl üst üste hiç ödemişse, Levhadan silinir.

(6) Levhadan silinme kararı verilmeden önce sigorta eksperinin yazılı savunması istenir. Ayrıca, Levhadan silinme kararının verilebilmesi için sigorta eksperinin savunmasının dinlenmesi veya dinlenmek üzere kendisine yapılan çağrıya uymamış olması gerekir. Levhadan silinme kararı gerekçeli olarak verilir.

(7) Levhadan silinmeyi gerektiren hallerinin sona erdiğini ispat eden sigorta eksperisi, Levhaya yeniden yazılma hakkını kazanır. Ancak, hakkında meslekten çıkarma kararı verilmiş olan kişinin bir daha Levhaya yazılması mümkün değildir. Levhaya yeniden yazılan sigorta eksperinden kayıt ücreti alınmaz.

(8) Levhaya yeniden yazılma talebinde bulunanlar, Levhaya yazılma şartlarının varlığının devam ettiğini ispatla zorunlu tutulabilir. Levhaya yeniden yazılma talebinin reddine ilişkin karar gerekçeli olarak verilir.

(9) Levhadan silinen veya Levhaya yeniden yazılma talebi reddolunan kişi, bu kararlara karşı onbeş iş günü içinde Müsteşarlığa yazılı itirazda bulunabilir. Yapılacak itiraz karşısında Müsteşarlık en geç onbeş iş günü içinde görüşünü bildirmek zorundadır. Bu karar kesindir.

(10) Gerçek kişi sigorta eksperleri, sigorta eksperliğini mutlak meslek halinde yapmak zorundadır. Gerçek kişi sigorta eksperleri, bu faaliyetlerine devam ettikleri sürede esnaf veya tacir sıfatıyla mesleğin niteliği ile bağdaşması mümkün olmayan başka bir işle uğraşamaz, sigorta acenteliği ve brokerlik faaliyetinde bulunamaz.

(11) Bir gerçek kişi sigorta eksperisi birden fazla büro açamaz.

(12) Tüzel kişi sigorta eksperleri münhasıran sigorta eksperliği konusunda faaliyet göstermek zorundadır. Tüzel kişi sigorta eksperisi ile iş yapılması durumunda, eksperlik işi tüzel kişiye verilir. Ancak, işi takip edecek olan sigorta eksperisine tüzel kişi tarafından yetki belgesi düzenlenir. Ekspertiz raporunda şirket kaşesi yanında gerçek kişi sigorta eksperinin de imzası yer alır. Tüzel kişi sigorta eksperleri nezdinde çalışan sigorta eksperleri, tüzel kişilerden bağımsız olarak iş kabul edemez, ücretli veya maaşlı bir görevde bulunamaz ve hiçbir şekilde bir başka tüzel kişi sigorta eksperinin nam ve hesabına çalışamaz.

(13) Sigorta eksperleri tarafsız olmak zorundadır. Sigorta eksperleri, taraflardan birisi ile arasında tarafsızlığını şüpheye düşürecek önemli nedenler veya taraflardan birisi ile 18/6/1927 tarihli ve 1086 sayılı Hukuk Usûlü Muhakemeleri Kanununun 245 inci maddesinin (1), (2) ve (3) numaralı bentlerinde yazılı derecelerde akrabalığı veya bir iş ortaklığı varsa, sigorta eksperliği görevini kabul edemez. Bu hüküm, tüzel kişi sigorta eksperlerinin yanında çalıştırdıkları sigorta eksperleri için de geçerlidir. Bu hükme aykırı olarak düzenlenen raporlar geçersizdir.

(14) Sigorta şirketlerinin, sigorta acentelerinin ve brokerlerin ortakları, yönetim ve denetiminde bulunan kişiler ve bunlar adına imza atmaya yetkili olanlar ile meslekî faaliyette bulunan şirket çalışanları sigorta eksperliği yapamaz; tüzel kişi sigorta eksperlerinin yönetim ve denetim kurullarında görev alamaz, imzaya yetkili olarak çalışamaz, bunlara ortak olamaz ve bunlardan ücret karşılığı herhangi bir iş kabul edemez. Bu sınırlandırmalar söz konusu kimselerin (...) (1) velayeti altındaki çocukları için de geçerlidir. (1)

(15) Sigorta eksperleri ve bunların yanlarında çalışanlar, işleri dolayısıyla öğrendikleri bilgi ve sırları ilgililerin izni olmaksızın açıklayamaz. Ancak, suç teşkil eden hallerin yetkili mercilere duyurulması zorunludur.

(16) Sigorta eksperliği yapması yasaklananlar, sigorta eksperliği ile ilgili faaliyetlerde çalıştırılmayacakları gibi bu kişilerle her ne şekilde olursa olsun sigorta eksperliği mesleğinin icrası için işbirliği yapılamaz.

(17) Maddî hasarla sonuçlanan trafik kazaları için yetkili sigorta eksperleri tarafından düzenlenmiş, örneği İçişleri Bakanlığınca tespit olunacak rapor, sigorta tazminatının ödenmesinde Karayolları Trafik Kanununun 99 uncu maddesindeki kaza ve zarara ilişkin tespit tutanağı hükmündedir. Eksperler tarafından düzenlenen raporlar delil niteliğindedir.

(18) (Mülga: 27/3/2015-6637/10 md.)

(19) (Değişik: 27/3/2015-6637/10 md.) Sigorta eksperinin, sigortacı veya sigorta ettiren ya da sigorta sözleşmesinden menfaat sağlayan kişiler tarafından atanması, eksperin iş kabulü, asgari ücret tarifesinin tespiti de dahil olmak üzere ekspertiz ücretinin belirlenmesi ile ilgili usul ve esaslar Birlik ve Sigorta Eksperleri İcra Komitesinin görüşleri alınarak yönetmelikle düzenlenir.

(20) (Değişik: 3/4/2013-6456/ 43 md.) Sigorta eksperliği yapacakların niteliklerine; sigorta eksperlerinin sınıflandırılmasına, branşlar itibarıyla görev ve yetki alanlarının belirlenmesine; ruhsat, Levhaya kayıt ve faaliyete ilişkin usul ve esaslar ile bu maddenin uygulanmasına ilişkin diğer hususlar yönetmelikle belirlenir.

(21) Sigorta eksperliđi kursları, sınavları ve stajı, yönetmelikle belirlenecek her bir eksperlik dalı için ayrı ayrı yapılır. Sigorta eksperlik kursu ve diđer eğitim faaliyetleri, 8/2/2007 tarihli ve 5580 sayılı Özel Öğretim Kurumları Kanununa tâbi değildir.

(22) Bu Kanuna göre yetkili olanlar dışında hiçbir kiři, sigorta eksperliđi faaliyetinde bulunamayacağı gibi ticaret unvanlarında veya herhangi bir belgede, sigorta eksperliđi iş ve işlemleriyle uğraştığı izlenimini yaratacak kelime ve işaretler kullanamaz.

Sigorta acenteleri

MADDE 23 - (1) Sigorta acenteliđi gerçek veya tüzel kişilerce yapılır. Sigorta acenteliđi yapmak isteyenlerin Türkiye Odalar ve Borsalar Birliğince tutulan Levhaya yazılı olması gerekir.

(2) Sigorta acenteliđi yapacakların niteliklerine ilişkin usûl ve esaslar yönetmelik ile belirlenir. Sigorta acenteliđi yapacaklar, Müsteşarlıktan bu nitelikleri taşıdıklarını gösteren bir belge olarak Levhaya kayıt olmak için Türkiye Odalar ve Borsalar Birliğine başvurur. Müsteşarlık, belge alınmasına ilişkin işlemlerin incelemeye ve onaya hazır hale getirilmesi için Türkiye Odalar ve Borsalar Birliğine görev verebilir. Türkiye Odalar ve Borsalar Birliği bu işlemlerin gerçekleştirilmesi için uygun gördüğü ilgili sivil toplum ve meslek kuruluşları ile işbirliği yapabilir.

(3) Bankalar ile özel kanunla kurulmuş ve kendisine sigorta acenteliđi yapma yetkisi tanınan kurumlar hakkında bu maddenin birinci fıkrasında yer alan Levhaya kayıt zorunluluđu ile Müsteşarlıktan belge almaya ilişkin ikinci fıkrası hükmü uygulanmaz.

(4) Aşağıdaki hallerde sigorta acentesinin kaydı;

a) Sigorta acenteliđi yapması için gerekli nitelikleri kaybetmişse,

b) Hakkında meslekten çıkarma kararı verilmişse,

c) Levhaya yazılmasını müteakip altı ay içinde faaliyete geçmezse,

ç) Sigorta acenteliđinden ayrılmışsa,

d) Ticaret veya ticaret ve sanayi odasındaki kaydı silinmişse,

e) Tespit edilen kayıt ücretini süresi içinde yatırmamışsa veya aidatını üç yıl üst üste hiç ödememişse, Levhadan silinir.

(5) Levhadan silinme kararı verilmeden önce sigorta acentesinin yazılı savunması istenir. Levhadan silinme kararının verilebilmesi için sigorta acentesinin savunmasının dinlenmesi veya savunması

dinlenmek üzere kendisine yapılan çağrıya uymamış olması gerekir. Levhadan silinme kararı gerekçeli olarak verilir.

(6) Levhadan silinmeyi gerektiren hallerinin sona erdiğini ispat eden sigorta acentesi, Levhaya yeniden yazılma hakkını kazanır. Ancak, hakkında meslekten çıkarma kararı verilmiş olan kişinin bir daha Levhaya yazılması mümkün değildir. Levhaya yeniden yazılan sigorta acentesinden kayıt ücreti alınmaz.

(7) Levhaya yeniden yazılma talebinde bulunanlar, Levhaya yazılma şartlarının varlığının devam ettiğini ispatla zorunlu tutulabilir. Levhaya yeniden yazılma talebinin reddine ilişkin karar gerekçeli olarak verilir.

(8) Levhadan silinen veya Levhaya yeniden yazılma talebi reddolunan kişi, bu kararlara karşı onbeş iş günü içinde Türkiye Odalar ve Borsalar Birliği Yönetim Kuruluna yazılı itirazda bulunabilir. Yapılacak itiraz karşısında Türkiye Odalar ve Borsalar Birliği Yönetim Kurulu en geç onbeş iş günü içinde görüşünü bildirmek zorundadır. Bu karar kesindir.

(9) 23/2/1995 tarihli ve 4077 sayılı Tüketicinin Korunması Hakkında Kanunun 4/A maddesinin üçüncü fıkrası hükmü sigorta acenteleri için sadece acentelik faaliyeti dolayısıyla sunulan hizmetlerde uygulanır. Sigorta şirketinin sağlayıcı olarak yaptığı ayıplı hizmetlerden sigorta acentesi sorumlu değildir.

(10) (Değişik: 3/4/2013-6456/ 44 md.) Bankalar ile özel kanunla kurulmuş ve kendisine sigorta acenteliği yapma yetkisi tanınan kurumlar hariç olmak üzere, sigorta acenteleri, bireysel emeklilik işlemleriyle ilgili aracılık ile Müsteşarlığın uygun göreceği sigortacılıkla bağlantılı diğer aracılık faaliyetleri dışında başka bir ticari faaliyette bulunamaz.

(11) Cumhurbaşkanı, yabancı sigorta acentelerinin Türkiye'deki faaliyetleri ile Türkiye'de faaliyet gösteren sigorta acentelerinin yabancı sigorta şirketleri adına Türkiye'deki aracılık hizmetlerine ilişkin düzenleme yapmaya yetkilidir.(1)

(12) Sigorta şirketlerinin, sigorta sözleşmeleri için brokerlik yapanların ve sigorta eksperlerinin yönetim ve denetiminde bulunan kişiler ile bunlar adına imza atmaya yetkili olanlar sigorta acentelerinin yönetim ve denetim kurullarında görev alamaz; imzaya yetkili olarak çalışamaz; bu şirketlere ortak olamaz ve bunlardan ücret karşılığı herhangi bir iş kabul edemez. Bu sınırlandırmalar söz konusu kimselerin eş ve velayeti altındaki çocukları için de geçerlidir. Ancak, sigorta şirketlerinin yönetiminde, denetiminde bulunan kişiler ile bunlar adına imza atmaya yetkili olanların eş ve

velayeti altındaki çocukları için sınırlandırma bu kişilerin faaliyette bulunduğu şirketin sigorta acenteliği içindir.

(13) Bu Kanuna göre yetkili olanlar dışında hiçbir gerçek veya tüzel kişi, sigorta acenteliği faaliyetinde bulunamayacağı gibi ticaret unvanlarında veya herhangi bir belgede, sigorta acenteliği iş ve işlemleriyle uğraştığı izlenimini yaratacak kelime ve işaretler kullanamaz.

(14) Sigorta acenteliği yapmaktan yasaklananlar, sigorta acenteliğiyle ilgili faaliyetlerde çalıştırılmayacakları gibi bu kişilerle her ne şekilde olursa olsun sigorta acenteliği mesleğinin icrası için işbirliği yapılamaz.

(15) Sigorta acentesi, acentelik sözleşmesinin sona ermesi halinde, sigorta ettirenlerle yaptığı veya kısa bir süre içinde yapacağı işlerle ilgili sözleşme ilişkisi devam etmiş olsaydı elde edeceği komisyona hak kazanır.

(16) Sözleşme ilişkisinin sona ermesinden sonra sigorta şirketi sigorta acentesinin portföyü sayesinde önemli menfaatler elde ediyor ve hakkaniyet gerektiriyorsa, sigorta acentesi, sigorta şirketinden tazminat talep edebilir. Ancak, sigorta acentesinin haklı bir nedene dayanmaksızın sözleşmeyi feshetmesi ya da kendi kusuruyla sözleşmenin feshine neden olması halinde tazminat hakkı düşer.

(17) Sigorta acenteleri ile bunların yanlarında çalışanlar, işleri dolayısıyla öğrendikleri bilgi ve sırları ilgililerin izni olmaksızın açıklayamaz. Ancak, suç teşkil eden hallerin yetkili mercilere duyurulması zorunludur.

(18) Türk Ticaret Kanununun acentelere ilişkin hükümleri sigorta acenteleri hakkında da uygulanır.

ALTINCI BÖLÜM

Meslek Örgütlenmeleri

Türkiye Sigorta, Reasürans ve Emeklilik Şirketleri Birliği

MADDE 24 - (Değişik: 13/6/2012-6327/54 md.)

(1) Sigorta şirketleri, reasürans şirketleri ve 4632 sayılı Kanuna göre kurulan emeklilik şirketleri merkezi İstanbul'da bulunan ve kamu kurumu niteliğinde bir meslek kuruluşu olan Türkiye Sigorta, Reasürans ve Emeklilik Şirketleri Birliğine giriş aidatını ödeyerek üye olmak zorundadır. Bu zorunluluk sigorta şirketleri ve reasürans şirketleri için sigortacılık ruhsatı, emeklilik şirketleri için emeklilik ruhsatı almalarından itibaren en geç bir ay içinde yerine getirilir. Ancak, Cumhurbaşkanı, üye olma zorunluluğunu kaldırmaya yetkilidir. Sigorta şirketleri, reasürans şirketleri ve emeklilik

şirketleri hakkında 18/5/2004 tarihli ve 5174 sayılı Türkiye Odalar ve Borsalar Birliği ile Odalar ve Borsalar Kanununun 9 uncu maddesinin yedinci fıkrası hükmü uygulanmaz.(2)

(2) Birlik nezdinde biri sigorta şirketleri ve reasürans şirketleri, diğeri emeklilik şirketleri için olmak üzere iki ayrı Levha tutulur ve Birliğe üyelik işlemlerini tamamlayan ilgili sigorta şirketi, reasürans şirketi ve emeklilik şirketi Birlik Yönetim Kurulu tarafından derhal ilgili olduğu Levhaya kaydedilir.

(3) Levhadan silinme aşağıda belirtilen hâllerde gerçekleşir:

a) Sigorta şirketi ve reasürans şirketi için;

- 1) Tüm branşlarda yeni sigorta ve reasürans sözleşmesi yapma yetkisinin kaldırılması,
- 2) Ruhsatın verildiği tarihten itibaren bir yıl içinde veya takip eden yıllarda Müsteşarlığın bilgisi haricinde, aralıksız olarak altı ay süre ile sigorta veya reasürans sözleşmesi akdetmemesi,
- 3) Kendisine yapılan tebligata rağmen süresi içinde giderlere katılma paylarını ve aidatlarını ödememesi,
- 4) Birlik üyeliğinin düşmesi.

b) Emeklilik şirketi için;

- 1) 4632 sayılı Kanunun 9 uncu maddesinin ikinci fıkrası kapsamında faaliyet ruhsatının geçersiz hâle gelmesi,
- 2) Yeni sözleşme akdetme yetkisinin kaldırılması,
- 3) 4632 sayılı Kanun uyarınca oluşturulan fonlarının tamamının başka bir şirkete devredilmesi,
- 4) 4632 sayılı Kanun uyarınca Bakan tarafından iflasının istenmesi,
- 5) Kendisine yapılan tebligata rağmen süresi içinde giderlere katılma paylarının ve aidatlarının ödenmemesi,
- 6) Birlik üyeliğinin düşmesi.

(4) Levhaya kayıtlı olmayan sigorta şirketi, reasürans şirketi ile emeklilik şirketi Genel Kurulda seçme ve seçilme hakkına sahip değildir. Levhadan silinmeyi gerektiren hâllerin sona erdiğini ispat eden sigorta şirketi, reasürans şirketi ile emeklilik şirketi, Levhaya yeniden yazılma hakkını kazanır ve bu şirketlerden giriş aidatı alınmaz.

(5) Birlik Yönetim Kurulu gerekli gördüğü hâllerde, nedenlerini de açıklamak suretiyle Levhaya yeniden yazılma talebinde bulunan sigorta şirketi, reasürans şirketi ile emeklilik şirketini Levhaya

yazılma şartlarının varlığının devam ettiğini ispatla zorunlu tutabilir. Levhaya yeniden yazılma talebinin reddine ilişkin karar gerekçeli olarak verilir.

(6) Levhadan silinen veya Levhaya yeniden yazılma talebi reddolunan sigorta şirketi, reasürans şirketi ile emeklilik şirketi, Yönetim Kurulunun silme veya ret kararına karşı onbeş iş günü içinde Müsteşarlığa yazılı itirazda bulunabilir. Yapılacak itiraz karşısında Müsteşarlık en geç onbeş iş günü içinde kararını bildirmek zorundadır. Müsteşarlığın bu konuda vereceği karar kesindir.

(7) Birlik üyeliğinin düşmesi aşağıda belirtilen hâllerde gerçekleşir:

a) Sigorta şirketi ile reasürans şirketi için;

1) Ruhsatlarının tümünün iptal edilmesi,

2) Hakkında iflas veya tasfiye kararı verilmiş olması ya da başka nedenlerle faaliyetinin sona ermesi.

b) Emeklilik şirketi için;

1) Emeklilik faaliyet ruhsatı ile sigorta ruhsatlarının geçersiz olması,

2) Hakkında iflas veya tasfiye kararı verilmiş olması ya da başka nedenlerle faaliyetinin sona ermesi.

(8) Birliğin amacı; mesleğin gelişmesini temin etmek, üyelerinin dayanışma, birlik ve mesleğin gerektirdiği vakar ve disiplin içinde çalışmalarını sağlamak ve haksız rekabeti önlemek üzere gerekli kararları almak ve uygulamaktır.

(9) Birliğin görev ve yetkileri şunlardır:

a) Mesleğin gelişmesini sağlayıcı önlemler almak, bu amaçla araştırma kuruluşları tesis etmek ve bu konudaki araştırma ve çalışmaları desteklemek.

b) Türkiye’de sigortacılığı ve bireysel emeklilik tasarruf ve yatırım sistemini temsil etmek ve tanıtmak için gerekli girişimlerde bulunmak, yurt içi ve yurt dışındaki ilgili kuruluşlara gerektiğinde üye olmak ve delege göndermek.

c) Gerektiğinde sigorta sözleşmelerine ilişkin rehber tarifeleri hazırlayarak sektörün hizmetine sunmak.

ç) Sigortacılık ve bireysel emeklilik tasarruf ve yatırım sistemi mevzuatı ile kendisine verilen görevleri yerine getirmek ve aldığı kararların ve önlemlerin uygulanmasını izlemek.

d) Uyulması zorunlu meslek kurallarını belirlemek, üyelerinin mesleğin gerektirdiği disiplin içinde ekonominin ihtiyaçlarına uygun olarak çalışmalarını sağlamak, üyeleri arasındaki haksız rekabeti önlemek amacıyla gerekli her türlü tedbiri almak ve uygulamak.

e) Sigortacılık ve bireysel emeklilik tasarruf ve yatırım sistemi konusunda eğitim vermek amacıyla ilgili kuruluş ve derneklerle işbirliği yapmak, seminerler ve konferanslar düzenlemek, kitap, dergi ve broşürler yayımlamak.

f) Sigorta ve bireysel emeklilik tasarruf ve yatırım sistemine ilişkin olarak gerekli sayı ve nitelikte inceleme ve araştırma komiteleri kurmak; görev, yetki ve çalışma şekillerini düzenlemek.

g) Üyelerinin yıllık faaliyet sonuçları hakkında her yıl raporlar hazırlamak ve bu raporları üyelerine ve ilgililere dağıtmak.

ğ) Sigortacılıkta tahkimin işleyişini düzenlemek ve sigorta hakemlerinin listesini tutmak.

(10) Birlik, ilgili olduğu meslekler konusundaki mevzuat ile almış olduğu karar ve önlemlerin uygulanmasını takip eder ve Müsteşarlıkça alınması talep edilen tedbirleri alır.

(11) Birlik, Müsteşarlığın uygun görüşü alınarak bu Kanun hükümleri çerçevesinde sigortacılık ve bireysel emeklilik tasarruf ve yatırım sistemi ile ilgili tüzel kişiliği haiz büro, şirket ve vakıf kurmaya ve kurulu şirketlere iştirak etmeye yetkilidir.

(12) Birlik organları; Genel Kurul, Birlik Başkanı, Yönetim Kurulu, Hayat Dışı Yönetim Komitesi, Hayat ve Emeklilik Yönetim Komitesi, Disiplin Kurulu ve Denetim Kuruludur. Yönetim Kurulu hariç olmak üzere, sigorta, reasürans ve emeklilik şirketleri, Genel Kurul dışında bu organlardan sadece birinde temsil edilir.

(13) Sigorta şirketleri, reasürans şirketleri ile emeklilik şirketleri Genel Kurulda, genel müdür veya genel müdürün bu amaçla vekalet verdiği, birinci derece imza yetkisine sahip bir yönetici tarafından temsil edilir. Müsteşarlık, Birlik Genel Kurulunda gözlemci bulundurabilir.

(14) Birlik Başkanı ile Hayat Dışı Yönetim Komitesi, Hayat ve Emeklilik Yönetim Komitesi, Disiplin Kurulu ve Denetim Kurulu üyeleri Genel Kurul tarafından iki yıllığına seçilir. Birlik Başkanı Yönetim Kurulunun da başkanıdır.

(15) Hayat Dışı Yönetim Komitesi, hayat dışı şirket temsilcileri tarafından, Hayat ve Emeklilik Yönetim Komitesi ise hayat ve emeklilik şirket temsilcileri tarafından seçilecek dokuz üyeden oluşur. Hayat Dışı Yönetim Komitesi ve Hayat ve Emeklilik Yönetim Komitesi üyeleri arasında yapılacak seçimle komite başkanları ve komiteyi Yönetim Kurulunda temsil edecek bir komite üyesi belirlenir.

(16) Hayat Dışı ve Hayat ve Emeklilik yönetim komitelerinin seçiminde, beş üye ilgili alandaki prim üretiminde ilk ona giren şirketler, üç üye yine ilgili alandaki ilk on dışında kalan şirketler ve bir üye ilgili alanda ağırlıklı olarak çalışan reasürans şirketleri arasında yapılan ve ilgili alanda faaliyet

gösteren tüm şirketlerin katıldığı seçimle belirlenir. Hayat veya emeklilik alanında ilk ona giren şirketler belirlenirken, seçim yılından bir önceki yıl sonu kapanmış prim ve katkı payı toplamı dikkate alınır. İlgili alanda ağırlıklı olarak çalışan reasürans şirketinin bulunmaması veya reasürans şirketlerinin ilgili komite üyeliğine aday olmaması halinde, reasürans şirketlerine tahsis edilen kontenjan ilk ona giren şirketler kontenjanına eklenmek suretiyle bu şirketlerin kontenjanı beşten altıya çıkarılır. Yukarıda belirtilen dağılımı sağlayacak sayıda gruplardan aday çıkmaması halinde, gruplar arasındaki dağılım Genel Kurulca kararlaştırılır.

(17) Birlik organlarında üye şirketler, genel müdür veya genel müdür niteliklerini haiz birinci derece imza yetkisine sahip bir yönetici seviyesinde temsil edilir. Yönetim Kurulu, Hayat Dışı Yönetim Komitesi, Hayat ve Emeklilik Yönetim Komitesi, Disiplin Kurulu ve Denetim Kurulu üyelikleri kişiye bağlı olmayıp, bahse konu organlarda şirketi temsil eden kişinin şirketiyle ilişkisinin kesilmesi hâllerinde, yerine aynı şirketi temsilen genel müdür veya genel müdür niteliklerini haiz birinci derece imza yetkisine sahip bir yönetici geçer. Birlik organlarında görev alan üye şirketlerin Levha kaydının silinmesi durumunda boşalan üyelik için usulüne göre seçim yapılır.

(18) Birlik Başkanının şirketiyle ilişkisinin kesilmesi halinde Birlik Başkanlığı düşer. İki ay içinde yapılan seçimle, görevi düşen Birlik Başkanının tamamlayamadığı süreyi tamamlamak üzere Birlik Başkanı seçilir.

(19) Yönetim Kurulu; Birlik Başkanı, Hayat Dışı Yönetim Komitesi ve Hayat ve Emeklilik Yönetim Komitesi başkanları ve ayrıca her iki komiteye seçilen birer komite üyesi olmak üzere beş kişiden oluşur. Birlik Başkanı Yönetim Kurulu Başkanı olup komite başkanları da yönetim kurulu başkan yardımcısıdır. Yönetim Kurulunda yer alan komite üyelerinden biri Yönetim Kurulunca muhasip üye olarak seçilir.

(20) Denetim Kurulu ile Disiplin Kurulu, üçer üyeden teşekkül eder. Denetim Kurulu ile Disiplin Kurulu ilk toplantısında birer başkan seçer.

(21) Sigorta şirketleri, reasürans şirketleri ile emeklilik şirketleri Birlik üyeliğine girişte Genel Kurul tarafından her yıl belirlenen miktarda giriş aidatı öder. Birliğin masraflarına iştirak payları; sigorta ve reasürans şirketleri için bir yıl zarfında Türkiye dahilinde elde ettikleri direkt prim gelirleri; emeklilik şirketleri için ise bir yıl zarfında Türkiye dahilinde elde ettikleri emeklilik katkı payı ile direkt prim gelirleri dikkate alınarak yönetmelikteki esaslar dairesinde hesap edilir ve paylaşılır. Aidatlar ve giderlere katılma payları yönetmelikte belirtilen süre içinde ödenmediği takdirde Birlik tarafından icra yoluyla tahsil olunur. Giderlere katılma paylarının ödenmesine dair kararlar 9/6/1932 tarihli ve 2004 sayılı İcra ve İflas Kanununun 68 inci maddesinde yazılı resmî belge niteliğindedir.

(22) Hayat, hayat dıřı, reasürans ve bireysel emeklilik tasarruf ve yatırım sistemi alanlarına ilişkin gelir ve giderler Birlik bütçesinde ayrı kalemlerde izlenir.

(23) Birliđin bu madde uyarınca aldıđı karar ve tedbirlere zamanında ve tam olarak uymayan üyeler hakkında Yönetim Kurulunca beřbin Türk Lirasından ellibin Türk Lirasına kadar idari para cezası uygulanır.

(24) Birliđin çalıřma esasları Birlikçe hazırlanan ve Müsteřarlıkça onaylanan yönetmelik ile belirlenir.

(25) Birliđin tüm faaliyetleri Müsteřarlık tarafından denetlenir.

Birlik organlarının seçim esasları ve yasaklar

MADDE 25 - (1) Birliđin organ seçimleri gizli oy ve açık tasnif ile yapılır ve organlarda her üyenin bir oy hakkı vardır.

(2) Seçim yapılacak Genel Kurul toplantısından en az onbeř gün önce Birlik seçimleri için üyelerin temsilcilerini belirleyen liste, toplantının gündemi, yeri, günü, saati ile çođunluk olmadıđı takdirde yapılacak ikinci toplantıya dair hususları belirten bir yazıyla birlikte üç nüsha olarak o yer ilçe seçim kurulu başkanı olan hâkime tevdi edilir. Seçim yapılacak yerde birden fazla ilçe seçim kurulu bulunması halinde, görevli hâkim, Yüksek Seçim Kurulunca belirlenir. (Deđişik son cümle: 13/6/2012-6327/55 md.) Toplantı tarihlerinin, gündemde yer alan diđer konular göz önünde bulundurularak görüşmelerin en fazla iki gün içinde sonuçlandırılacak şekilde düzenlenmesi zorunludur.

(3) Hâkim, gerektiğinde ilgili kayıt ve belgeleri de getirtip incelemek suretiyle varsa noksanları tamamlattırdıktan sonra seçime katılacak üyeleri belirleyen liste ile ikinci fıkrada belirtilen diđer hususları onaylar. Onaylanan liste ile toplantıya ait diđer hususlar Birliđin ilan yerlerinde asılmak suretiyle üç gün süre ile ilan edilir.

(4) İlan süresi içinde listeye yapılacak itirazlar hâkim tarafından incelenir ve en geç iki gün içinde karara bağlanır.

(5) Bu suretle kesinleşen listeler ile toplantıya ait diđer hususlar onaylanarak Birliğe gönderilir.

(6) Hâkim, aday olmayan üyeler arasından bir başkan ile iki üyeden oluşan bir seçim sandık kurulu atar. Aynı şekilde ayrıca üç yedek üye de hâkim tarafından belirlenir. Seçim sandık kurulu başkanının yokluđunda kurula en yařlı üye başkanlık eder.

(7) Seçim sandık kurulu, seçimlerin Kanunun öngördüđü esaslara göre yürütülmesi, yönetimi ve oyların tasnifi ile görevli olup, bu görevleri seçim ve tasnif işleri bitinceye kadar aralıksız olarak devam eder.

(8) Seçim süresinin sonunda seçim sonuçları tutanakla tespit edilip seçim sandık kurulu başkan ve üyeleri tarafından imzalanır. Birden fazla sandık bulunması halinde tutanaklar, hâkim tarafından birleştirilir. Tutanakların birer örneği seçim yerinde asılmak suretiyle geçici seçim sonuçları ilan edilir. Kullanılan oylar ve diğer belgeler tutanağın bir örneği ile birlikte üç ay süreyle saklanmak üzere ilçe seçim kurulu başkanlığına tevdi edilir.

(9) Seçimin devamı sırasında yapılan işlemler ile tutanakların düzenlenmesinden itibaren iki gün içinde seçim sonuçlarına yapılacak itirazlar, hâkim tarafından aynı gün incelenir ve kesin olarak karara bağlanır. İtiraz süresinin geçmesi ve itirazların karara bağlanmasından hemen sonra hâkim, yukarıdaki hükümlere göre kesin sonuçları ilan eder ve Birliğe bildirir.

(10) Listede adı yazılı olmayan üyeler oy kullanamaz. Oylar, oy verenin kimliğini Birlik veya resmî kuruluşça verilen belge ile ispat etmesinden ve listedeki isminin karşısındaki yerin imzalanmasından sonra kullanılır. Oylar, organlara göre birlikte veya ayrı ayrı düzenlenen oy pusulalarının, üzerinde ilçe seçim kurulu mühürü bulunan ve oy verme sırasında sandık kurulu başkanı tarafından verilecek zarfa konulması suretiyle kullanılır. Bunların dışındaki zarflara konulan oylar geçersiz sayılır. Seçimlerde kullanılacak araç ve gereçler ilçe seçim kurulundan sağlanır ve sandıkların konacağı yerler hâkim tarafından belirlenir.

(11) Hâkim, seçim sonuçlarını etkileyecek ölçüde bir usûlsüzlük veya kanuna aykırı uygulama sebebiyle seçimlerin iptaline karar verdiği takdirde, süresi bir aydan az ve iki aydan fazla olmamak üzere seçimin yenileneceği pazar gününü tespit ederek Birliğe bildirir. Belirlenen günde yalnızca seçim yapılır ve seçim işlemleri bu madde ile Kanunun öngördüğü diğer hükümlere uygun olarak yürütülür.

(12) İlçe seçim kurulu başkanına, hâkime ve seçim sandık kurulu başkanı ile üyelerine, 26/4/1961 tarihli ve 298 sayılı Seçimlerin Temel Hükümleri ve Seçmen Kütükleri Hakkında Kanunda belirtilen esaslara göre ücret ödenir. Bu ücret ve diğer seçim giderleri Birlik bütçesinden karşılanır.

(13) Seçimler sırasında sandık kurulu başkan ve üyelerine karşı işlenen suçlar kamu görevlilerine karşı işlenmiş gibi cezalandırılır.

(14) Birlik, kuruluş amaçları dışında faaliyette bulunamaz. Birlik organlarının seçimlerinde siyasi partiler aday gösteremez. Amaçları dışında faaliyet gösteren Birliğin sorumlu organlarının görevine, Bakanın veya Cumhuriyet savcısının istemi üzerine mahkeme kararıyla son verilir ve yerlerine yenileri seçtirilir.

(15) Görevlerine son verilen organların yerine en geç bir ay içinde yenileri seçilir. Yeni seçilenler eskilerin süresini tamamlar.

(16) Göreve son verme hükümleri Birlik Genel Kurulu hakkında uygulanmaz.

(17) Bakan veya Müsteşarlığın bu Kanun uyarınca Birlik organları tarafından yürütülen işlemler hakkında verdiği kararları, görevli organlar aynen yerine getirmekle yükümlüdür. Bu kararları kanunî bir sebep olmaksızın yerine getirmeyen veya eski kararda direnme niteliğinde yeni bir karar veren veya kanunun zorunlu kıldığı işlemleri uyarılmasına rağmen yerine getirmeyen Birlik organları hakkında da ondördüncü fıkra hükümleri uygulanır.

(18) Görevlerine son verilen organ üyelerinin ve tüzel kişi temsilcilerinin cezaî sorumlulukları saklıdır. Bu organların onyedinci fıkra gereğince görevlerine son verilmesine sebep olan tasarrufları hükümsüzdür.

(19) Millî güvenliğin, kamu düzeninin, suç işlenmesini veya suçun devamını önlemenin yahut yakalamanın gerektirdiği hallerde gecikmede sakınca varsa, Bakan, Birliği faaliyetten men edebilir. Bakanın kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim kararını kırksekiz saat içinde açıklar; aksi halde bu idarî karar kendiliğinden yürürlükten kalkar.

(20) Birlik yönetim ve denetiminde yer alanlar ile Birlik çalışanları, işleri dolayısıyla öğrendikleri bilgi ve sırları ilgililerin izni olmaksızın açıklayamaz. Ancak, suç teşkil eden hallerin yetkili mercilere duyurulması zorunludur.

(...)

YEDİNCİ BÖLÜM

Denetim ve Bilgi Verme

Denetim

MADDE 28 - (1) Türkiye’de faaliyet gösteren sigorta şirketleri, reasürans şirketleri, özel kanunlarına göre sigortacılık faaliyetinde bulunan kuruluşlar, sigorta ve reasürans aracıları, sigorta eksperlik faaliyetleri, aktüerler ve sigortacılık işlemi yapan veya sigortacılık alanında faaliyet gösteren diğer kişilerin her türlü sigortacılık işlemlerinin denetimi, Sigorta Denetleme Kurulu tarafından yapılır.

(2) Sigorta Denetleme Kurulu, bir başkan ile sigorta denetleme uzmanları, sigorta denetleme aktüerleri ile bunların yardımcılarında oluşur. Bu Kanun ve diğer kanunların sigortacılığa, sigortaya veya sigortacılık alanında faaliyet gösteren kişi ve kuruluşlara ilişkin hükümlerinin Müsteşarlığın bağlı olduğu Bakanlığa veya Müsteşarlığa verdiği teftiş, denetim, inceleme ve soruşturma görev ve

yetkileri sigorta denetleme uzmanları, sigorta denetleme aktüerleri ve bunların yardımcıları eliyle ifa edilir ve kullanılır.

(3) Sigorta şirketleri ile reasürans şirketlerinin faaliyetleri, varlıkları, iştirakleri, alacakları, özkaynakları ve borçları ile kâr ve zarar hesapları arasındaki ilgi ve dengelerin ve malî bünyelerini ve idarî yapılarını etkileyen diğer tüm unsurların, tahsil edilen primler ile birikimlerin değerlendirilmesi ve korunması ile aktüeryal ve finansal hesap ve dengelerin incelenmesi, tespit ve denetimi sigorta denetleme uzmanları, sigorta denetleme aktüerleri ile bunların yardımcıları tarafından yapılır.

(4) Sigorta denetleme uzmanları, sigorta denetleme aktüerleri ile bunların yardımcıları; sigorta şirketleri ve reasürans şirketleri ile bunların bağlı ortaklıkları, iştirakleri, şubeleri ile temsilciliklerinden, araçlar ve bankalar da dahil olmak üzere diğer kişilerden bu Kanun ve diğer kanunların sigortacılıkla ilgili hükümleri bakımından gerekli görecekları bilgileri istemeye ve bunların tüm defter, kayıt ve belgelerini incelemeye yetkilidir.

(5) Kamu kurum ve kuruluşları, Birlik ile diğer benzeri sivil toplum ve meslek kuruluşları, bu madde kapsamına giren konu ve işlemlerle sınırlı olmak üzere, Devletin güvenliği ve temel dış yararlarına karşı ağır sonuçlar doğuracak haller ile aile hayatının gizliliği ve savunma hakkına ilişkin hükümler saklı kalmak kaydıyla, özel kanunlardaki yasaklayıcı ve sınırlayıcı hükümler dikkate alınmaksızın gizli dahi olsa sigorta denetleme uzmanları, sigorta denetleme aktüerleri ve bunların yardımcıları tarafından istenecek görevleriyle ilgili her türlü bilgi ve belgeyi uygun süre ve ortamda vermeye, istenecek defter ve belgeleri ibraz etmeye ve incelemeye hazır bulundurmaya, bilgi işlem sistemini denetim amaçlarına uygun olarak açmaya ve verilerin güvenliğini sağlamaya mecburdur. Sigorta denetleme uzmanları, sigorta denetleme aktüerleri ve bunların yardımcıları bu madde kapsamındaki kuruluşların yönetim ve denetim kurullarının toplantı tutanakları ile bu kurullara verilen raporları istemeye, inceleme konusu olan işlemlerle ilgisi olan diğer kişi, kurum ve kuruluşlar nezdinde inceleme yapmaya yetkilidir.

(6) Sigorta denetleme uzmanları, sigorta denetleme aktüerleri ve bunların yardımcıları tarafından gerçekleştirilen denetim, inceleme ve soruşturmalar sırasında talep edilmesi halinde, incelemeye, denetime veya soruşturmaya tâbi kuruluşlar tarafından, iç kontrol sistemlerinde çalışanların yardımı da dahil olmak üzere her türlü destek sağlanır. (1)

(7) Bu Kanun hükümleri ile diğer kanunlarda yer alan hükümler çerçevesinde, bu Kanuna tâbi kuruluşların faaliyetlerinin, risk yapısının, varlıkları, alacakları, özkaynakları, borçları, yükümlülükleri ve taahhütleri, gelir ve gider hesapları arasındaki ilgi ve dengelerin ve malî bünyeyi

etkileyen diğerk tüm unsurların ve bu kuruluşlarca karşılaşılan risklerin gözetim faaliyetleri çerçevesinde tespiti, tahlili, izlenmesi ve ölçülmesi çıkartılacak yönetmeliğe göre Müsteşarlık tarafından yapılır.

(8) Müsteşarlık, bu Kanuna tâbi kuruluşlara ait bilgi ve belgeleri, bu kuruluşların konsolide ve konsolide olmayan bazda malî bünyeleri ve idarî yapılarının mevzuata uygunluğunu izlemek, analiz etmek, ilgili kuruluşlara ait rapor, tablo ve iç kontrol raporları ile Müsteşarlığın denetim ve gözetim sonuçlarını karşılaştırmak suretiyle değerlendirmek, elde edilen sonuçlara göre kuruluşların taşıdıkları risklerin türleri, büyüklüğü ve kuruluşları etkileme durumunu, risk yönetim sisteminin güvenilirliği ile denetim riskini dikkate almak suretiyle kuruluşlar hakkında gerekli görülen tüm tedbirlerin alınmasını ve sonuçlandırılmasını sağlamak, söz konusu kuruluşların bağlı ortaklıklarının, malî iştiraklerinin ve şubelerinin faaliyetlerini önemli ölçüde etkileyen veya etkileyebilecek uygulamaları takip etmek, gerekirse ilgililer nezdinde girişimde bulunmak konularında yetkilidir. (1)

(9) Bu Kanuna tâbi kişi ve kuruluşlar hesap ve kayıt düzenleriyle uyumlu olarak Müsteşarlıkça belirlenen formatlara uygun bir şekilde üretecekleri bilgi, belge, cetvel, rapor ve malî tabloları Müsteşarlıkça belirlenen iletişim kanallarını kullanmak suretiyle belirlenen süreler içinde Müsteşarlığa tevdi etmekle yükümlüdür. Kuruluşlar tarafından elektronik ortamda gönderilen bilgiler, iç kontrol sistemi kapsamında yönetim kurulunun sorumluluğundadır. (1)

Bilgi verme yükümlülüğü, uluslararası kuruluşlara üyelik ve işbirliği (2)

MADDE 29 - (1) Bu Kanuna tâbi kişiler ile sigortacılıkla ilgili her tür meslekî faaliyet icra edenler, sigorta şirketleri ile reasürans şirketlerinin iştirakleri, bankalar ve diğerk kişiler, özel kanunlardaki yasaklayıcı ve sınırlayıcı hükümler dikkate alınmaksızın gizli dahi olsa bu Kanunun uygulanması ile ilgili olarak Müsteşarlıkça istenen her türlü bilgi ve belgeyi vermekle yükümlüdür. Devletin güvenliği ve temel dış yararlarına karşı ağır sonuçlar doğuracak haller ile aile hayatının gizliliği ve savunma hakkına ilişkin hükümler saklıdır.

(2) Müttekabiliyet çerçevesinde ve bu Kanunun uygulanması ile ilgili olarak yabancı ülke kanunlarına göre denetime yetkili mercilerin, kendi ülkelerindeki sigortacılık sektöründe faaliyet gösteren kuruluşların bu Kanuna tâbi Türkiye'deki teşkilât veya ortaklıklarında denetim yapma ve bilgi isteme taleplerinin yerine getirilmesi Müsteşarlığın iznine tâbidir. Bu mercilerce istenen bilgiler, açıklanmaması kaydıyla Müsteşarlık tarafından verilebilir. Müsteşarlık, yabancı ülkelerin denetime yetkili mercileri ile yapacağı anlaşmalar çerçevesinde sigortacılıkla ilgili her türlü işbirliği ve bilgi alışverişinde bulunabilir.

(3) (Ek: 13/6/2012-6327/57 md.) Müsteşarlık, sigortacılıkla ilgili denetim ve düzenleme otoritelerinin katıldığı uluslararası mali, iktisadi ve mesleki kuruluşlara üye olabilir ve işbirliği ve bilgi paylaşımında bulunabilmeyi teminen uluslararası mesleki kuruluşlar ve yabancı ülkelerin yetkili mercileri ile mutabakat zaptı imzalayabilir. İmzalanan mutabakat zaptı Bakanın onayı ile yürürlüğe girer.

SEKİZİNCİ BÖLÜM

Tahkim

Sigortacılıkta tahkim

MADDE 30 - (1) Sigorta ettiren veya sigorta sözleşmesinden menfaat sağlayan kişiler ile riski üstlenen taraf arasında sigorta sözleşmesinden veya Hesaptan faydalanacak kişiler ile Hesap arasında doğan uyuşmazlıkların çözümü amacıyla Birlik nezdinde Sigorta Tahkim Komisyonu oluşturulur. Sigortacılık yapan kuruluşlardan, sigorta tahkim sistemine üye olmak isteyenler, durumu yazılı olarak Komisyona bildirmek zorundadır. Sigorta tahkim sistemine üye olan kuruluşlarla uyuşmazlığa düşen kişi, uyuşmazlık konusu sözleşmede özel bir hüküm olmasa bile tahkim usûlünden faydalanabilir. (Ek cümle : 3/4/2013-6456/45 md.) İlgili mevzuat ile zorunlu tutulan sigortalardan kaynaklanan bu fıkra kapsamındaki uyuşmazlıklar için ilgili kuruluş sigorta tahkim sistemine üye olmasa dahi hak sahipleri bu bölüm hükümlerine göre tahkim usulünden faydalanabilir. (Ek cümle : 3/4/2013-6456/45 md.) Sigorta tahkim sistemine üye olmayan kuruluşlar bakımından Sigorta Tahkim Komisyonu giderlerine katılım Hazine Müsteşarlığınca ayrıca belirlenir.

(1)

(2) Komisyon, bir Müsteşarlık temsilcisi, iki Birlik temsilcisi, bir tüketici derneği temsilcisi ile Müsteşarlıkça belirlenecek bir akademisyen hukukçu temsilcinin katılımı ile oluşur. Müsteşarlık temsilcisinin asgarî on yıl kamu hizmetinde çalışmış, sigortacılık alanında deneyim sahibi ve en az daire başkanı seviyesinde olması; Birlik temsilcilerinin de 4 üncü maddede genel müdür yardımcısı için öngörülen şartlara sahip olması gerekir. Tüketici derneği temsilcisi ise Türkiye çapında en fazla üyeye sahip tüketici derneğinin önereceği üç aday arasından Müsteşarlıkça seçilir. Komisyon kendi içinden bir Başkan seçer. Komisyonda kararlar üye tamsayısının salt çoğunluğu ile alınır. İki yıl için seçilen Komisyon Başkan ve üyelerine, kamu iktisadî teşebbüsleri yönetim kurulu başkan ve üyelerine ödenen aylık ücret ve diğer ödemeler tutarında ücret ödenir.

(3) Komisyon aşağıdaki görevleri yerine getirir:

a) Müdür ve müdür yardımcılarını atamak.

- b) Birlikçe ayrı bir hesapta izlenecek olan Komisyonun bütçesini hazırlayarak Birliğe sunmak.
- c) Tahkim sisteminin adil, tarafsız ve etkin bir biçimde işleyişini sağlamak için gerekli önlemleri almak.
- ç) Komisyonun faaliyet sonuçları hakkında yıllık rapor hazırlayarak Birliğe ve Müsteşarlığa göndermek.
- d) Bilgi işlem alt yapısını hazırlamak.
- e) Kanunlarla kendisine verilen diğer görevleri yapmak.

(4) Komisyon, gerekli görülen yerlerde büro açmaya yetkilidir. Büro müdürünün, Komisyon müdürü ile aynı nitelikleri taşıması zorunludur. Büro müdürüne verilecek görevler Komisyon tarafından belirlenir.

(5) Komisyona bağlı çalışmak üzere bir müdür ve iki müdür yardımcısı, raportörler ile yeterli sayıda personel görevlendirilir. Müdür ve müdür yardımcıları Komisyonca, raportörler ve diğer personel ise müdürün önerisiyle Komisyon tarafından atanır. Görevden alınma, göreve atanma ile aynı usûle tâbidir. Komisyon müdürünün;

- a) Malî güç dışında sigorta şirketi ve reasürans şirketi kurucularında aranan nitelikleri taşıması,
 - b) En az dört yıllık yüksek okul mezunu olması,
 - c) Sigorta hukukunda en az iki yıl veya sigortacılıkta en az beş yıl deneyimi olması,
- gerekir.

(6) Müdür yardımcılarının (c) bendi hariç olmak üzere beşinci fıkrada sayılan nitelikleri taşıması zorunludur. Ayrıca, müdür yardımcılarının en az birinde iki yıllık sigortacılık deneyimi aranır.

(7) Uyuşmazlıklar, hayat ve hayat dışı sigorta gruplarının sadece birinde görev yapacak olan sigorta hakemleri ve raportörler aracılığıyla çözülür.

(8) Sigorta hakemlerinin;

- a) Malî güç dışında sigorta şirketi ve reasürans şirketi kurucularında aranan nitelikleri taşıması,
- b) En az dört yıllık yüksek okul mezunu olması,
- c) Sigorta hukukunda en az beş yıl veya sigortacılıkta en az on yıl deneyimi olması,

gerekir. (Ek cümle: 13/6/2012-6327/58 md.) Müsteşarlık bu fıkra uyarınca aranacak deneyim ve bu deneyime esas teşkil eden bilginin tespitine ilişkin ölçütleri belirlemeye yetkilidir.

(9) Komisyon nezdinde çalışacak olan sigorta raportörleri, Komisyon müdüründe aranan niteliklere sahip olmak zorundadır.

(10) Sigorta hakemi olmak isteyenlerin gerekli nitelikleri taşıdıklarını belgelemek suretiyle Komisyona başvurması gerekir. Başvurusu uygun görülenler kabul için Müsteşarlığa bildirilir. Müsteşarlığın kabul etmesi halinde ilgilinin ismi, Komisyon tarafından tutulacak ve bir örneği Adalet Bakanlığına gönderilecek olan sigorta hakemliği listesine kaydolunur ve bu listede değişiklik olması halinde de değişiklikler altı aylık dönemler itibarıyla Adalet Bakanlığına ve Müsteşarlığa bildirilir.

(11) Sigorta hakeminin ismi;

a) Sigorta hakemliği yapmak için gereken nitelikleri kaybetmişse veya tarafsızlık ilkesine aykırı hareket ettiği tespit edilmişse sürekli olarak,

b) Kendisine ulaşan dosyaları bir yıl içinde en fazla üç kez zamanında sonuçlandırmamışsa bir yıl süreyle,

Listeden silinir.

(12) Tahkim sistemine üye olmak isteyenlerden katılma payı, uyuşmazlık çözümü için Komisyona başvuranlardan ise başvuru ücreti alınır. (Değişik ikinci ve üçüncü cümle: 3/4/2013-6456/45 md.) Beş bin Türk Lirasının altındaki uyuşmazlıklar hakkında verilen hakem kararları kesindir. Beş bin Türk Lirası ve daha üzerindeki uyuşmazlıklar hakkında verilen hakem kararlarına karşı kararın Komisyonca ilgiliye bildiriminden itibaren on gün içinde bir defaya mahsus olmak üzere Komisyon nezdinde itiraz edilebilir. (Ek cümle: 3/4/2013-6456/45 md.) İtiraz talebinde bulunmak için bu madde uyarınca belirlenen başvuru ücretinin Komisyona yatırılması şarttır. (Ek cümle: 3/4/2013-6456/45 md.) İtiraz üzerine hakem kararının icrası durur. (Ek cümle: 3/4/2013-6456/45 md.) İtiraz talebi münhasıran bu talepleri incelemek üzere Komisyon tarafından teşkil edilen hakem heyetlerince incelenir. (Ek cümle: 3/4/2013-6456/45 md.) İtiraz talebi hakkında işin heyete intikalinden itibaren iki ay içinde karar verilir. (Ek cümle: 3/4/2013-6456/45 md.) Beşbin Türk Lirası ve daha üzerindeki uyuşmazlıklar hakkında verilen hakem kararları bu madde uyarınca süresinde itiraz başvurusunda bulunulmaması hâlinde kesinleşir. (Ek cümle: 3/4/2013-6456/45 md.) Bu uyuşmazlıklar hakkında bu madde uyarınca yapılan itiraz üzerine verilen karar kesindir. (Ek cümle: 3/4/2013-6456/45 md.) Kırk bin Türk Lirasının üzerindeki uyuşmazlıklar hakkında itiraz üzerine verilen kararlar için temyize gidilebilir. (Değişik cümle: 13/6/2012-6327/58 md.) Ancak, tahkim süresinin sona ermesinden sonra karar verilmiş olması, talep edilmemiş bir şey hakkında karar verilmiş olması, hakemlerin yetkileri dahilinde olmayan konularda karar vermesi ve hakemlerin, tarafların iddiaları hakkında karar vermemesi durumlarında

her hâlikarda temyiz yolu açıktır. Temyize ilişkin usûl ve esaslar hakkında Hukuk Usûlü Muhakemeleri Kanunu uygulanır.

(13) Komisyona gidilebilmesi için, sigortacılık yapan kuruluşla uyuşmazlığa düşen kişinin, uyuşmazlığa konu teşkil eden olay ile ilgili olarak sigortacılık yapan kuruluşa gerekli başvuruları yapmış ve talebinin kısmen ya da tamamen olumsuz sonuçlandığını belgelemiş olması gerekir. Sigortacılık yapan kuruluşun, başvuru tarihinden itibaren onbeş iş günü içinde yazılı olarak cevap vermemesi de Komisyona başvuru için yeterlidir.

(14) Mahkemeye ve Tüketicinin Korunması Hakkında Kanun hükümleri uyarınca Tüketici Sorunları Hakem Heyetine intikal etmiş uyuşmazlıklar ile ilgili olarak Komisyona başvuru yapılamaz.

(15) Sigortacılık yapan kuruluşla uyuşmazlığa düşen kişinin Komisyona başvurusu, öncelikle raportörler tarafından incelenir. Raportörler en geç onbeş gün içinde incelemelerini tamamlamak zorundadır. Raportörler tarafından çözümlendirilemeyen başvurular sigorta hakemine iletilir. Uyuşmazlığa hangi sigorta hakeminin bakacağı, Komisyon tarafından sigorta hakemi listesinden seçilir. Komisyon, işin niteliğine bağlı olarak en az üç sigorta hakeminden oluşan bir heyet oluşturulmasına karar verebilir. Ancak, uyuşmazlık konusu miktarın onbeşbin Türk Lirası ve üzerinde olduğu durumlarda heyet teşekkülü zorunludur. Heyet kararını çoğunlukla verir. Hakemler, sadece kendilerine verilen evrak üzerinden karar verir. Seçilen sigorta hakemi mücbir nedenler ve umulmayan haller hariç olmak üzere görevi reddedemez. Bununla birlikte, taraflar, Hukuk Usûlü Muhakemeleri Kanununda yer alan hâkimi ret nedenlerine dayanarak hakemi reddedebilir. Ret talebi Komisyona, durumun öğrenildiği tarihten itibaren en geç beş iş günü içinde bir dilekçeyle yapılır. Ret talebi üzerine Komisyon müdürü, iki tarafın görüşlerini dinledikten sonra bu konuda en geç beş iş günü içinde karar verir.

(16) Hakemler, görevlendirildikleri tarihten itibaren en geç dört ay içinde karar vermeye mecburdur. Aksi halde, uyuşmazlık yetkili mahkemece halledilir. Ancak, bu süre tarafların açık ve yazılı muvafakatleriyle uzatılabilir. Hakem, kararını Komisyon müdürüne tevdi eder. (Değişik son cümle:22/7/2020-7251/56 md.) Komisyon Müdürünce karar en geç üç iş günü içinde taraflara bildirilir; ayrıca kararın aslı dosya ile birlikte Komisyonca saklanır.

(17) (Ek: 13/6/2012-6327/58 md.) Talebi kısmen ya da tamamen reddedilenler aleyhine hükmolunacak vekalet ücreti, Avukatlık Asgarî Ücret Tarifesinde belirlenen vekalet ücretinin beşte biridir. (1)

(18) Hakemlik ücreti, Komisyona başvuru ücreti ve üyeliğe katılma payı, Komisyonun görüşü alınarak Müsteşarlıkça belirlenir; hakem ücreti Komisyon tarafından ödenir.

(19) Sigorta hakemleri ve raportörler tarafsız olmak zorundadır. Sigorta şirketlerinin, reasürans şirketlerinin, sigortacılık yapan diğer kuruluşların, sigorta eksperlerinin, sigorta acentelerinin ve brokerlerin ortakları, yönetim ve denetiminde bulunan kişiler ve bunlar adına imza atmaya yetkili olanlar ile tüm bu kuruluşlarda meslekî faaliyette bulunanlar ve sigorta eksperleri, sigorta acenteleri ve brokerler sigorta hakemliği yapamaz. Bu sınırlandırmalar söz konusu kimselerin eş ve çocukları için de geçerlidir. Hukuk Usûlü Muhakemeleri Kanununun 28 inci maddesi sigorta hakemleri hakkında da uygulanır.

(20) Komisyonda görev alanlar, hakemler ve raportörler, işleri dolayısıyla öğrendikleri bilgi ve sırları ilgililerin izni olmaksızın açıklayamaz. Ancak, suç teşkil eden hallerin yetkili mercilere duyurulması zorunludur.

(21) Komisyonun yapısı ve görevleri ile Komisyon müdürü ve Komisyon müdür yardımcılarının nitelikleri, çalışma usûl ve esasları, raportörlerin, sigorta hakemlerinin çalışma usûl ve esasları, kararların ne şekilde düzenleneceği, Komisyona başvuru esasları, Liste tutulmasına ve bütçeye ilişkin esaslar ile katılım ücreti gibi hususlar yönetmelikle belirlenir.

(22) Müsteşarlık bu maddede yer alan maktu para miktarlarını, Türkiye İstatistik Kurumu tarafından açıklanan Üretici Fiyatları Endeksi artış oranını aşmamak suretiyle artırmaya yetkilidir.

(23) Bu Kanunda hüküm bulunmayan hallerde Hukuk Usûlü Muhakemeleri Kanununun hükümleri, sigortacılıktaki tahkim hakkında da kıyasen uygulanır.

(24) Hukuk Usûlü Muhakemeleri Kanunu çerçevesinde yapılacak tahkim için seçilecek hakemlerin de bu maddede sigorta hakemleri için aranılan nitelikleri taşıması gerekir.

(...)

Sır saklama yükümlülüğü

MADDE 31/A - (Ek: 13/6/2012-6327/60 md.)

(1) Bu Kanunun uygulanmasında ve uygulanmasının denetiminde görev alanlar, bu Kanuna tâbi kuruluşların görevlileri ve yetkilileri, bu Kanuna tâbi kişiler ile bunların yanında çalışanlar ve dışarıdan hizmet alımı yoluyla sigortacılık sektöründe iş görenler, sıfat ve görevleri dolayısıyla öğrendikleri bu Kanun kapsamında faaliyet gösteren kişi ve kuruluşlar ile bunların iştirakleri, kuruluşları ve sigorta sözleşmesi ile ilgili kişilere ait sırları bu konuda kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamaz, kendilerinin veya başkalarının yararlarına kullanamaz. Bu yükümlülük söz konusu sıfat ve görevlerin sona ermesinden sonra da devam eder.

(2) Ancak, gizlilik sözleşmesi yapılması ve sadece risk değerlendirmesi amacıyla kullanılmak üzere sigorta şirketi, reasürans şirketi ve emeklilik şirketlerinin kendi aralarında doğrudan doğruya ya da Sigorta Bilgi ve Gözetim Merkezi vasıtasıyla yapacakları her türlü bilgi ve belge alışverişi sırasında sigorta şirketi, reasürans şirketi ve emeklilik şirketlerine ya da sigorta sözleşmesi ile ilgili kişilere ait, yanlış sigorta uygulamaları dâhil, sır niteliğindeki bilgilerin öğrenilmesi ve paylaşımı sır saklama yükümlülüğü dışındadır.

Sigorta Bilgi ve Gözetim Merkezi

MADDE 31/B - (Ek: 13/6/2012-6327/61 md.)

(1) Türkiye Sigorta, Reasürans ve Emeklilik Şirketleri Birliği nezdinde, sigortalılar ve sigorta sözleşmesinden dolayı da olsa menfaat sağlayanlara ilişkin olarak, yanlış sigorta uygulamaları dâhil, risk değerlendirmesine esas bilgileri toplamak ve bu bilgilerin sigorta, reasürans ve sigortacılık faaliyetinde bulunan emeklilik şirketleri ile Müsteşarlıkça belirlenecek kişilerle paylaşılmasını sağlamak amacıyla Sigorta Bilgi ve Gözetim Merkezi kurulur.

(2) Bu maddenin birinci fıkrasında belirtilen şirketler, Sigorta Bilgi ve Gözetim Merkezine üye olmak zorundadır. Üye kuruluşlar, Sigorta Bilgi ve Gözetim Merkezince istenilen her türlü bilgiyi vermekle yükümlüdür.

(3) Sigorta Bilgi ve Gözetim Merkezi kuruluş amaçları doğrultusunda, özel hukuk tüzel kişileri ile kamu kurum ve kuruluşlarından, kamu kurumu niteliğinde meslek kuruluşları ve bunların üst kuruluşlarından, ilgili mevzuatla kurulmuş diğer bilgi merkezlerinden bilgi talep etmeye ve bunlarla Müsteşarlığın uygun görüşüne istinaden bilgi alışverişine yönelik sözleşmeler imzalamaya yetkilidir. Söz konusu kurum ve kuruluşlar Sigorta Bilgi ve Gözetim Merkezi tarafından talep edilen bilgileri vermekle yükümlüdür. Sigorta Bilgi ve Gözetim Merkezinde toplanan bilgilerin bilgi sahibinin kendisi veya onay vermesi durumunda bu madde uyarınca Sigorta Bilgi ve Gözetim Merkezi ile bilgi alışverişine ilişkin sözleşme yapan özel hukuk tüzel kişileri, kamu kurum ve kuruluşları ile kamu kurumu niteliğinde meslek kuruluşları ve bunların üst kuruluşlarıyla anılan sözleşmeler çerçevesinde paylaşılması bu Kanunun 31/A maddesinin ikinci fıkrası kapsamında değerlendirilir.

(4) Sigorta Bilgi ve Gözetim Merkezi kendi yönetimi tarafından temsil ve idare edilir. Sigorta Bilgi ve Gözetim Merkezi iş ve işlemlerinden kendi yönetimi yetkili ve sorumlu olup faaliyetleri için gereken giderler kendi bütçesinden karşılanır. Müsteşarlık, Sigorta Bilgi ve Gözetim Merkezini denetler. Sigorta Bilgi ve Gözetim Merkezi sigorta uygulamaları kapsamında, poliçe yazım ve hasar

süreçlerinin izlenmesi de dâhil olmak üzere Müsteşarlık tarafından talep edilen her türlü çalışmayı yapar ve bu amaçla gerekli alt yapıyı tesis eder.

(5) Sigorta Bilgi ve Gözetim Merkezinin bütün işlem ve kayıtları gizlidir. Sigorta Bilgi ve Gözetim Merkezi topladığı her türlü bilgiyi, Müsteşarlığa istenen biçim ve sürede vermekle yükümlüdür. Söz konusu bilgiler, sahibinin açık rızasının bulunması durumunda belirlediği kişiye belli bir ücret karşılığında verilir.

(6) Sigorta Bilgi ve Gözetim Merkezi nezdinde bulunan sır niteliğindeki bilgileri, bu konuda kanunen yetkili kılınan mercilerden başkalarına açıklayanlar, hukuka aykırı olarak kendisi ya da başkası yararına kullananlar, yayanlar, verenler, aktaranlar veya ele geçirenler hakkında 35 inci maddenin dokuzuncu ve onuncu fıkraları hükümleri uygulanır. Bu fıkrada tanımlanan suçların bir tüzel kişinin faaliyeti çerçevesinde işlenmesi halinde, ilgili tüzel kişi hakkında 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun tüzel kişilere özgü güvenlik tedbirlerine hükmolunur.

(7) Sigorta Bilgi ve Gözetim Merkezine üye şirketlerin Sigorta Bilgi ve Gözetim Merkezi giderlerine katılım payları anılan şirketlerin bir önceki yıl gerçekleştirdikleri prim üretiminin binde birini aşmamak üzere Müsteşarlıkça belirlenir. Müsteşarlık, bu oranın yüzde elli oranında azaltılmasına veya artırılmasına karar verebilir. (Ek cümle: 3/4/2013-6456/46 md.) Bu surette tespit edilen katılım paylarının Sigorta Bilgi ve Gözetim Merkezi giderlerini karşılayamaması durumunda bu madde uyarınca yayımlanacak yönetmelikte belirlenecek usul ve esaslar dâhilinde Birlik Yönetim Kurulunca üye şirketlerden ayrıca katılma payı talep edilebilir. Sigorta Bilgi ve Gözetim Merkezi giderlerine Müsteşarlığın belirleyeceği esaslar dahilinde Hesaptan katkı sağlanabilir.

(8) Sigorta Bilgi ve Gözetim Merkezinin kuruluşu, faaliyetleri, Sigorta Bilgi ve Gözetim Merkezinde toplanan bilgilerin kapsam, biçim ve içeriğine ve bunların paylaşılmasına, paylaşılacak bilgilerin kapsam ve içeriğine, ücretlendirilmesine ve üyelerce ödenecek katılım paylarının belirlenmesi, yükümlülüklerle uymayan üyeler hakkında yapılacak işlemler ve bu maddenin uygulanmasına ilişkin usul ve esaslar yönetmelikle belirlenir.

(...)

Adli cezalar

MADDE 35 - (1) Bu Kanuna göre ruhsat almadan risk üstlenmek suretiyle sigortacılık faaliyetinde bulunan veya ticaret unvanlarında ya da her türlü belgeleri yahut ilan ve reklamlarında veyahut kamuoyuna yaptıkları açıklamalarda bu Kanunda belirtilen kuruluşların adını kullanan, bu Kanunda düzenlenen faaliyetlerde buldukları izlenimini yaratacak söz ve işaretleri kullanan gerçek kişiler

ve tüzel kişilerin yetkilileri, üç yıldan beş yıla kadar hapis cezası ve altıyüz günden az olmamak üzere bin güne kadar adlî para cezası ile cezalandırılır.

(2) Bu Kanunun 3 üncü maddesinin dördüncü fıkrasına aykırı olarak Müsteşarlıktan izin alınmadan sigorta sözleşmesi yapan kooperatiflerin yetkilileri beşyüz günden az olmamak üzere bin güne kadar adlî para cezası ile cezalandırılır.

(3) Sigorta şirketleri ile reasürans şirketlerinin yönetim kurulu başkan ve üyeleri ile diğer mensupları, görevleri dolayısıyla kendilerine tevdi olunan veya muhafazaları, denetimleri ve sorumlulukları altında bulunan kuruluşa ait para veya sair varlıkları zimmetlerine geçirmeleri halinde, altı yıldan oniki yıla kadar hapis cezası ile cezalandırılır. Ayrıca, kuruluşun uğradığı zararı da tazmine mahkûm edilir.

(4) Üçüncü fıkrada gösterilen suç, kuruluşu aldatacak ve fiilin açığa çıkmamasını sağlayacak her türlü hileli faaliyette bulunmak suretiyle işlenmişse fail, oniki yıldan az olmamak üzere hapis cezası ve adlî para cezası ile cezalandırılır. Ancak, adlî para cezasının miktarı, meydana gelen zararın üç katından az olamaz. Zararın, kovuşturma yapılmadan önce tamamıyla ödenmesi halinde verilecek ceza üçte bir oranında indirilir.

(5) Bu Kanunda gösterilen yetkili mercilerin ve denetim görevlilerinin istedikleri bilgi ve belgeleri vermeyen ya da denetim görevlilerinin görevlerini yapmalarına engel olan gerçek kişilerle tüzel kişilerin yetkilileri, bir yıldan üç yıla kadar hapis cezası ve ikiyüz günden az olmamak üzere adlî para cezası ile cezalandırılır.

(6) Bu Kanunda gösterilen mercilere, denetim görevlilerine, mahkemelere ve diğer resmî dairelere yanıltıcı şekilde yanlış ya da gerçeğe aykırı bilgi veya belge veren gerçek kişiler ile tüzel kişilerin yetkilileri, bir yıldan üç yıla kadar hapis ve üçyüz günden az olmamak üzere adlî para cezası ile cezalandırılır.

(7) Bu Kanuna tâbi kuruluşların itibarını zedeleyebilecek ya da servetine zarar verebilecek bir hususa kasten sebep olan ya da bu yolda asılsız haberler yayanlar bir yıldan iki yıla kadar hapis cezası ve ikiyüz günden az olmamak üzere adlî para cezası ile cezalandırılır. Bu fiilin 9/6/2004 tarihli ve 5187 sayılı Basın Kanununda yazılı araçlarla ya da radyo, televizyon, video, internet, kablolu yayın veya elektronik bilgi iletişim araçları ve benzer yayın araçlarından biri ile işlenmesi halinde hapis cezası iki yıldan dört yıla kadar uygulanır. İsimleri belirtilmese dahi bu Kanuna tâbi kuruluşların güvenilirliği konusunda kamuoyunda tereddüte yol açarak bu kuruluşların malî bünyelerinin

olumsuz etkilenmesine neden olabilecek nitelikte asılsız haberleri yukarıda belirtilen araçlarla yayanlar dörtyüz günden az olmamak üzere bin güne kadar adlî para cezası ile cezalandırılır.

(8) Bu Kanunun uygulanmasında ve uygulanmasının denetiminde görev alanlar ile sigorta hakemleri ve raportörleri, sıfat veya görevleri dolayısıyla öğrendikleri, bu Kanun kapsamında faaliyet gösteren kişi ve kuruluşlar ile bunların iştirakleri, kuruluşları ve sigorta sözleşmesi ile ilgili kişilere ait sırları, görevlerinden ayrılmalarından sonra dahi, bu Kanuna ve özel kanunlarına göre yetkili olanlardan başkasına açıklamaları veya kendi yararına kullanmaları halinde iki yıldan dört yıla kadar hapis cezası ve üçyüz günden az olmamak üzere adlî para cezası ile cezalandırılır.

(9) Bu Kanuna tâbi kuruluşların görevlileri ve yetkilileri, bu maddenin sekizinci fıkrasında yazılı kişiler hariç olmak üzere bu Kanuna tâbi kişiler ile bunların yanında çalışanlar ve dışarıdan hizmet alımı yoluyla sigortacılık sektöründe iş görenler, sıfat ve görevleri dolayısıyla öğrendikleri bu Kanuna tâbi kuruluşlara veya sigorta sözleşmesi ile ilgili kişilere ait sırları bu konuda kanunen açıkça yetkili kılınan mercilerden başkasına açıklamaları halinde bir yıldan üç yıla kadar hapis cezası ve ikiyüz günden az olmamak üzere adlî para cezası ile cezalandırılır.

(10) Sekiz ve dokuzuncu fıkralarda yazılı kişilerin bu fıkralarda belirtilen türden sırları kendileri ya da başkalarına yarar sağlamak amacıyla açıklamaları halinde, bu kişiler üç yıldan beş yıla kadar hapis cezası ve adlî para cezası ile cezalandırılır. Ayrıca, fiilin önemine göre bu kişilerin görev yapmaları sürekli veya altı aydan bir yıla kadar geçici olarak yasaklanır.

(11) Gerçeğe aykırı malî tablo düzenleyenler ile bunları tasdik eden sigorta şirketi ve reasürans şirketi denetçileri adlî para cezası ile cezalandırılır. Ancak adlî para cezası, gerçeğe aykırılık tutarının yüzde birinden az olamaz.

(12) Bu Kanunun 9 uncu maddesinin birinci, ikinci ve dördüncü fıkralarında yazılan izinleri almayanlar üçyüz günden az olmamak üzere; altıncı fıkrasına göre belirlenen hisse sınırlamalarına uymayanlar dörtyüz günden az olmamak üzere; üçüncü fıkrasına aykırı olarak izin alınmadan yapılan hisse devirlerini pay defterine kaydettirenler ise dörtyüz günden az olmamak üzere bin güne kadar adlî para cezası ile cezalandırılır.

(13) Bu Kanunun 12 nci maddesinin ikinci fıkrasına aykırı olarak tarifeleri Müsteşarlığın onayı olmaksızın uygulayanlar beşyüz günden az olmamak üzere; Müsteşarlığın tespit ve ilan ettiği aracılık komisyonları dışında komisyon verenler üçyüz günden az olmamak üzere; bu komisyonları alanlar ise yüz günden az olmamak üzere adlî para cezası ile cezalandırılır.

(14) Bu Kanunun 13 üncü maddesinin birinci fıkrası hükmüne aykırı olarak sözleşme yapmaktan kaçınanlar beşyüz günden az olmamak üzere adli para cezası ile cezalandırılır.

(15) Bu Kanunun 15 inci maddesine aykırı şekilde Türkiye’de sigortalanabilir menfaatlerini Türkiye’de faaliyette bulunan sigorta şirketleri haricinde ve Türkiye dışında sigorta ettirenler adli para cezası ile cezalandırılır.

(16) Bu Kanunun 16 ncı maddesinin birinci fıkrasına aykırı olarak yeteri kadar karşılık ayırmayanlar ile iki ilâ yedinci fıkralarına aykırı olarak teknik karşılık ayıranlar ve sekizinci fıkrasına aykırı olarak reasürör payını belirleyenler; 17 nci maddesinin birinci ve ikinci fıkrasına aykırı olarak teminat, dördüncü fıkrasına aykırı olarak minimum garanti fonu tesis edenler ile beşinci fıkra uyarınca teminatlardan ödeme yapmayanlar adli para cezası ile cezalandırılır. (Değişik son cümle: 13/6/2012-6327/64 md.) Ancak, adli para cezasının miktarı, yerine getirilmeyen yükümlülüğün veya yükümlülük eksik olarak yerine getirilmiş ise eksik kalan miktarın yüzde ikisinden az, yüzde onikisinden fazla olamaz.

(17) Bu Kanunun 19 uncu maddesinin birinci fıkrasına aykırı davrananlar bin güne kadar; aykırılığın, iyiniyet kurallarını ihlâl edici şekilde aktifin değerini düşürmesi halinde bu işlemi yapanlar, ikibin güne kadar adli para cezası ile cezalandırılır. (Değişik son cümle: 13/6/2012-6327/64 md.) Ancak, adli para cezasının miktarı, aktifte gerçekleşen azalmanın yüzde beşinden az, yüzde yirmisinden fazla olamaz.

(18) Bu Kanunun 21 inci maddesinin üçüncü fıkrasına aykırı hareket eden brokerler üçyüz günden az olmamak üzere; sigorta brokerliği dışında sigorta acenteliği ve eksperlik yapanlar dörtüyük günden az olmamak üzere; dördüncü fıkrasına aykırı hareket edenler ikiyüz günden az olmamak üzere adli para cezası ile cezalandırılır.

(19) Bu Kanunun 22 nci maddesinin üçüncü fıkrası uyarınca belirlenecek esaslara aykırı hareket edenler üçyüz günden az olmamak üzere adli para cezası ile; onuncu fıkrasına aykırı olarak sigorta eksperliği dışında başka bir işle uğraşanlar yüz günden az olmamak üzere adli para cezası ile; onbirinci fıkrasına aykırı olarak birden fazla büro açanlar altmış günden az olmamak üzere adli para cezası ile; onikinci fıkrasına aykırı hareket eden gerçek kişi sigorta eksperleri ve tüzel kişi sigorta eksperlerinin yetkilileri yüz günden az olmamak üzere adli para cezası ile; onüçüncü fıkrasına aykırı olarak görev kabul eden sigorta eksperleri ile tüzel kişi sigorta eksperinin yanında çalışan sigorta eksperleri veya tarafsızlığı ihlâl eden sigorta eksperleri beşyüz günden az olmamak üzere adli para cezası ile; ondördüncü fıkrası hükmüne aykırı davrananlar üçyüz günden az olmamak üzere adli para cezası ile; onaltıncı fıkrasına aykırı hareket edenler ile bu fıkra gereğince sigorta eksperliği ile

ilgili faaliyetlerde çalışmaması gerektiği halde çalışanlar ikiyüz günden az olmamak üzere adli para cezası ile; yirmiikinci fıkrasına aykırı olarak sigorta eksperliği yetkilerini veya unvanlarını başka kişilere kullandıranlar ve söz konusu yetki ve unvanları kullananlar beşyüz günden az olmamak üzere adli para cezası ile; sigorta eksperliği yaptığı izlenimini uyandıranlar yüz günden az olmamak üzere adli para cezası ile cezalandırılır.

(20) Bu Kanunun 23 üncü maddesinin onuncu fıkrasına aykırı olarak ticarî faaliyette bulunanlar yüz günden az olmamak üzere adli para cezası ile; onikinci fıkrasına aykırı davrananlar üçyüz günden az olmamak üzere adli para cezası ile; onüçüncü fıkrasına aykırı olarak sigorta acenteliği yetkilerini veya unvanlarını başka kişilere kullandıranlar ve söz konusu yetki ve unvanları kullananlar beşyüz günden az olmamak üzere adli para cezası ile; sigorta acenteliği yaptığı izlenimini uyandıranlar yüz günden az olmamak üzere adli para cezası ile; ondördüncü fıkrasına aykırı hareket edenler ile bu fıkra gereğince sigorta acenteliğiyle ilgili faaliyetlerde çalışmaması gerektiği halde çalışanlar ikiyüz günden az olmamak üzere adli para cezası ile cezalandırılır.

(21) Sigorta acenteliği yapamayacaklarla, sigorta acenteliği sözleşmesi yapan sigorta şirketlerinin bu işten sorumlu yöneticileri beşyüz günden az olmamak üzere adli para cezası ile; prim tahsil etme veya sözleşme yapma yetkisi verilemeyeceklere bu yetkileri veren sigorta şirketlerinin bu işten sorumlu yöneticileri üçyüz günden az olmamak üzere adli para cezası ile; bu yetkileri kabul eden kişiler ikiyüz günden az olmamak üzere adli para cezası ile cezalandırılır.

(22) Hakkında meslekten çıkarma kararı verildiği halde bu Kanunun 26 ncı maddesinin altıncı fıkrasına aykırı olarak tüzel kişi sigorta eksperinde denetçi veya temsile ve ilzama yetkili olarak çalışanlar ve bu kişileri çalıştıranlar ile hakkında meslekten çıkarma kararı verildiği halde 27 nci maddenin altıncı fıkrasına aykırı olarak tüzel kişi sigorta acentesinde denetçi veya temsile ve ilzama yetkili olarak çalışanlar ve bu kişileri çalıştıranlar bir yıldan iki yıla kadar hapis cezası ve üçyüz günden az olmamak üzere adli para cezası ile cezalandırılır.

(23) Bu Kanuna aykırı olarak ruhsatı olmadan brokerlik ve sigorta eksperliği yapanlar; Müsteşarlıktan uygunluk belgesi olmadan sigorta acenteliği yapanlar ile Aktüerler Siciline kaydolmadan aktüerlik yapanlar bir yıldan üç yıla kadar hapis cezası ve dörtyüz günden az olmamak üzere adli para cezası ile cezalandırılır.

(24) Bu Kanunda öngörülen süre içinde Birliğe üye olmayan sigorta şirketleri ve reasürans şirketlerinin yetkilileri ile Levhaya kayıtlı olmadan sigorta eksperliği veya sigorta acenteliği faaliyetinde bulunanlar yüzelli günden az olmamak üzere adli para cezası ile cezalandırılır.

(25) Aktüer ve broker yetki veya unvanlarını başka kişilere kullandıranlar ve söz konusu yetki ve unvanları kullananlar beşyüz günden az olmamak üzere, bu işleri yaptığı izlenimini uyandıranlar yüz günden az olmamak üzere adlî para cezası ile cezalandırılır.

(26) Bu Kanunun 31 inci maddesinin ikinci fıkrasındaki izni almadan sigortacılıkla ilgili organizasyon oluşturanlar üçyüz günden az olmamak üzere adlî para cezası ile cezalandırılır.

(27) Bu Kanunun 32 nci maddesinin ikinci fıkrasına aykırı davrananlar ile üçüncü fıkrasına aykırı olarak iyiniyet kurallarını ihlâl edici şekilde sigorta tazminatı ödemesini geciktirenler üçyüz günden az olmamak üzere adlî para cezası ile cezalandırılır.

(...)

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

Resmî Gazete Tarihi : 23.05.2007

Resmî Gazete Sayısı : 26530

İNTERNET ORTAMINDA YAPILAN YAYINLARIN DÜZENLEN-MESİ VE BU YAYINLAR YOLUYLA İŞLENEN SUÇLARLA MÜCA-DELE EDİLMESİ HAKKINDA KANUN

Amaç ve kapsam

MADDE 1

(1) Bu Kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemektir.

Tanımlar

MADDE 2

(1) Bu Kanunun uygulamasında;

a) Bakanlık: Ulaştırma Bakanlığını,

b) (Mülga: 15/8/2016-KHK-671/20 md.; Aynen kabul: 9/11/2016-6757/17 md.)

c) (Değişik: 15/8/2016-KHK-671/20 md.; Aynen kabul: 9/11/2016-6757/17 md.) Başkan: Bilgi Teknolojileri ve İletişim Kurumu Başkanını,

ç) Bilgi: Verilerin anlam kazanmış biçimini,

d) Erişim: Bir internet ortamına bağlanarak kullanım olanağı kazanılmasını,

e) Erişim sağlayıcı: Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri,

f) İçerik sağlayıcı: İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri,

g) İnternet ortamı: Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortamı,

- ğ) İnternet ortamında yapılan yayın: İnternet ortamında yer alan ve içeriğine belirsiz sayıda kişilerin ulaşabileceği verileri,
- h) İzleme: İnternet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesini,
- ı) (Değişik: 15/8/2016-KHK-671/20 md.; Aynen kabul: 9/11/2016-6757/17 md.) Kurum: Bilgi Teknolojileri ve İletişim Kurumunu,
- i) Toplu kullanım sağlayıcı: Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayanı,
- j) (Değişik: 26/2/2014-6527/15 md.) Trafik bilgisi: Taraflara ilişkin IP adresi, (EK: 29/7/2020-7253/1. md.) port bilgisi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini,
- k) Veri: Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri,
- l) Yayın: İnternet ortamında yapılan yayını,
- m) Yer sağlayıcı: Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri,
- n) (Ek: 6/2/2014-6518/85 md.) Birlik: Erişim Sağlayıcıları Birliğini,
- o) (Ek: 6/2/2014-6518/85 md.) Erişimin engellenmesi: Alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi ve benzeri yöntemler kullanılarak erişimin engellenmesini,
- ö) (Ek: 6/2/2014-6518/85 md.) İçeriğin yayından çıkarılması: İçerik veya yer sağlayıcılar tarafından içeriğin sunuculardan veya barındırılan içerikten çıkarılmasını,
- p) (Ek: 6/2/2014-6518/85 md.) URL adresi: İlgili içeriğin internette bulunduğu tam internet adresini,
- r) (Ek: 6/2/2014-6518/85 md.) Uyarı yöntemi: İnternet ortamında yapılan yayın içeriği nedeniyle haklarının ihlal edildiğini iddia eden kişiler tarafından içeriğin yayından çıkarılması amacıyla öncelikle içerik sağlayıcısına, makul sürede sonuç alınamaması hâlinde yer sağlayıcısına iletişim adresleri üzerinden gerçekleştirilecek bildirim yöntemini,
- s) (EK: 29/7/2020-7253/1. md.) Sosyal ağ sağlayıcı: Sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses, konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşmalarına imkân sağlayan gerçek veya tüzel kişileri,
- ifade eder.

Bilgilendirme yükümlülüğü

MADDE 3

(1) İçerik, yer ve erişim sağlayıcıları, yönetmelikle belirlenen esas ve usûller çerçevesinde tanıtıcı bilgilerini kendilerine ait internet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlüdür.

(2) Yukarıdaki fıkrada belirtilen yükümlülüğü yerine getirmeyen içerik, yer veya erişim sağlayıcısına Başkan tarafından iki bin Türk lirasından elli bin Türk lirasına kadar idarî para cezası verilir.

(3) (Ek: 6/2/2014-6518/86 md.) Bu Kanun kapsamındaki faaliyetleri yurt içinden ya da yurt dışından yürütenlere, internet sayfalarındaki iletişim araçları, alan adı, IP adresi ve benzeri kaynaklarla elde edilen bilgiler üzerinden elektronik posta veya diğer iletişim araçları ile bildirim yapılabilir.

(4) (Ek: 26/2/2014-6527/16 md.; Değişik: 10/9/2014-6552/126 md.; İptal: Anayasa Mahkemesi'nin 2/10/2014 tarihli ve E.: 2014/149, K.: 2014/151 sayılı Kararı ile.)

(5) (EK: 29/7/2020-7253/2. md.) Bu Kanun kapsamında verilen idari para cezaları, muhatabın yurt dışında bulunması hâlinde Kurum tarafından doğrudan muhataba üçüncü fıkradaki usulle de bildirilebilir. Bu bildirim 11/2/1959 tarihli ve 7201 sayılı Tebligat Kanununa göre yapılan tebligat hükmündedir. Bu bildirim yapıldığı tarihi izleyen beşinci günün sonunda tebligat yapılmış sayılır.

İçerik sağlayıcının sorumluluğu

MADDE 4

(1) İçerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur.

(2) İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur.

(3) (Ek: 6/2/2014-6518/87 md.) (İptal: Anayasa Mahkemesinin 8/12/2015 tarihli ve E.: 2014/87, K.: 2015/112 sayılı Kararı ile.)

Yer sağlayıcının yükümlülükleri

MADDE 5

(1) Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir.

(2) (Değişik: 6/2/2014-6518/88 md.) Yer sağlayıcı, yer sağladığı hukuka aykırı içeriği bu Kanunun 8 inci ve 9 uncu maddelerine göre haberdar edilmesi hâlinde yayından çıkarmakla yükümlüdür.

(3) (Ek: 6/2/2014-6518/88 md.) Yer sağlayıcı, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür.

(4) (Ek: 6/2/2014-6518/88 md.) Yer sağlayıcılar, yönetmelikle belirlenecek usul ve esaslar çerçevesinde yaptıkları işin niteliğine göre sınıflandırılabilir ve hak ve yükümlülükleri itibarıyla farklılaştırılabilirler.

(5) (Ek: 6/2/2014-6518/88 md.) (İptal: Anayasa Mahkemesinin 8/12/2015 tarihli ve E.: 2014/87, K.: 2015/112 sayılı Kararı ile.)

(6) (Ek: 6/2/2014-6518/88 md.) Yer sağlayıcılık bildiriminde bulunmayan veya bu Kanundaki yükümlülüklerini yerine getirmeyen yer sağlayıcı hakkında Başkan tarafından (Değişik: 29/7/2020-7253/3. md.) yüz bin Türk lirasından bir milyon Türk lirasına kadar idari para cezası verilir.

Erişim sağlayıcının yükümlülükleri

MADDE 6

(1) Erişim sağlayıcı;

a) Herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, bu Kanun hükümlerine uygun olarak haberdar edilmesi halinde (...) erişimi engellemekle,

b) Sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla,

c) Faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma, içerik sağlayıcılarına ve müşterilerine bildirmek ve trafik bilgilerine ilişkin kayıtları yönetmelikte belirtilen esas ve usûllere uygun olarak Kuruma teslim etmekle,

ç) (Ek: 6/2/2014-6518/89 md.) Erişimi engelleme kararı verilen yayınlarla ilgili olarak alternatif erişim yollarını engelleyici tedbirleri almakla,

d) (Ek: 6/2/2014-6518/89 md.) (İptal: Anayasa Mahkemesinin 8/12/2015 tarihli ve E.: 2014/87, K.: 2015/112 sayılı Kararı ile.)

yükümlüdür.

(2) Erişim sağlayıcı, kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü değildir.

(3) Birinci fıkranın (b), (c), (ç) (...) bentlerinde yer alan yükümlülüklerden birini yerine getirmeyen erişim sağlayıcısına Başkan tarafından onbin Yeni Türk Lirasından ellibin Yeni Türk Lirasına kadar idarî para cezası verilir.

Erişim Sağlayıcıları Birliği

MADDE 6/A (Ek: 6/2/2014-6518/90 md.)

(1) Bu Kanunun 8 inci maddesi kapsamı dışındaki erişimin engellenmesi kararlarının uygulanmasını sağlamak üzere Erişim Sağlayıcıları Birliği kurulmuştur.

(2) Birlik özel hukuk tüzel kişiliğini haizdir. Birliğin merkezi Ankara'dır.

(3) Birliğin çalışma usul ve esasları Kurum tarafından onaylanacak Tüzükle belirlenir. Tüzük değişiklikleri de Kurumun onayına tabidir.

(4) Birlik, Tüzüğünün Kurum tarafından incelenerek uygun bulunmasını müteakip faaliyete başlar.

(5) Birlik, 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu kapsamında yetkilendirilen tüm internet servis sağlayıcıları ile internet erişim hizmeti veren diğer işletmecilerin katılımıyla oluşan ve koordinasyonu sağlayan bir kuruluştur.

(6) Bu Kanunun 8 inci maddesi kapsamı dışındaki erişimin engellenmesi kararları erişim sağlayıcılar tarafından yerine getirilir. Kararların uygulanması amacıyla gerekli her türlü donanım ve yazılım erişim sağlayıcıların kendileri tarafından sağlanır.

(7) Bu Kanunun 8 inci maddesi kapsamı dışındaki erişimin engellenmesi kararları gereği için Birliğe gönderilir. Bu kapsamda Birliğe yapılan tebligat erişim sağlayıcılara yapılmış sayılır.

(8) Birlik, kendisine gönderilen mevzuata uygun olmadığını düşündüğü kararlara itiraz edebilir.

(9) Birliğin gelirleri, üyeleri tarafından ödenecek ücretlerden oluşur. Alınacak ücretler, Birliğin giderlerini karşılayacak miktarda belirlenir. Bir üyenin ödeyeceği ücret, üyelerin tamamının net satış tutarı toplamı içindeki o üyenin net satışı oranında belirlenir. Üyelerin ödeme dönemleri, yeni katılan üyelerin ne zamandan itibaren ödemeye başlayacağı ve ödemelere ilişkin diğer hususlar Birlik Tüzüğünde belirlenir. Süresinde ödenmeyen ücretler Birlikçe kanuni faizi ile birlikte tahsil edilir.

(10) Birliğe üye olmayan internet servis sağlayıcıları faaliyette bulunamaz.

Toplu kullanım sağlayıcıların yükümlülükleri

MADDE 7

(1) Ticarî amaçla toplu kullanım sağlayıcılar, mahallî mülkî amirden izin belgesi almakla yükümlüdür. İzne ilişkin bilgiler otuz gün içinde mahallî mülkî amir tarafından Kuruma bildirilir. Bunların denetimi mahallî mülkî amirler tarafından yapılır. İzin belgesinin verilmesine ve denetime ilişkin esas ve usûller, yönetmelikle düzenlenir.

(2) (Değişik: 6/2/2014-6518/91 md.) Ticari amaçla olup olmadığına bakılmaksızın bütün internet toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimin engellenmesi ve kullanıma ilişkin erişim kayıtlarının tutulması hususlarında yönetmelikle belirlenen tedbirleri almakla yükümlüdür.

(3) (Değişik: 6/2/2014-6518/91 md.) Ticari amaçla toplu kullanım sağlayıcılar, ailenin ve çocukların korunması, suçun önlenmesi ve suçluların tespiti kapsamında usul ve esasları yönetmelikte belirlenen tedbirleri almakla yükümlüdür.

(4) (Ek: 6/2/2014-6518/91 md.) Bu maddede belirtilen yükümlülükleri ihlal eden ticari amaçla toplu kullanım sağlayıcılarına, ihlalin ağırlığına göre yönetmelikle belirlenecek usul ve esaslar çerçevesinde uyarma, bin Türk Lirasından on beş bin Türk Lirasına kadar idari para cezası verme veya üç güne kadar ticari faaliyetlerini durdurma müeyyidelerinden birine karar vermeye mahalli mülki amir yetkilidir.

İçeriğin çıkarılması ve erişimin engellenmesi kararları ile yerine getirilmesi

MADDE 8

(1) İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak (Değişik: 29/7/2020-7253/4. md.) içeriğin çıkarılmasına ve/veya erişimin engellenmesine karar verilir:

a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;

1) İntihara yönlendirme (madde 84),

2) Çocukların cinsel istismarı (madde 103, birinci fıkra),

3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),

4) Sağlık için tehlikeli madde temini (madde 194),

5) Müstehcenlik (madde 226),

6) Fuhuş (madde 227),

7) Kumar oynanması için yer ve imkân sağlama (madde 228),

suçları.

b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

c) (Ek:25/3/2020-7226/32 md.) 29/4/1959 tarihli ve 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanunda yer alan suçlar.

(2) (Değişik: 29/7/2020-7253/4. md.) İçeriğin çıkarılması ve/veya erişimin engellenmesi kararı, soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme tarafından verilir. Soruşturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da (Değişik: 29/7/2020-7253/4. md.) içeriğin çıkarılmasına ve/veya erişimin engellenmesine karar verilebilir. Bu durumda Cumhuriyet savcısı kararını yirmidört saat içinde hâkimin onayına sunar ve hâkim, kararını en geç yirmidört saat içinde verir. Bu süre içinde kararın onaylanmaması halinde tedbir, Cumhuriyet savcısı tarafından derhal kaldırılır. (Ek cümle: 6/2/2014-6518/92 md.) Erişimin engellenmesi kararı, amacı gerçekleştirecek nitelikte görülürse belirli bir süreyle sınırlı olarak da verilebilir. Koruma tedbiri olarak verilen (Değişik: 29/7/2020-7253/4. md.) içeriğin çıkarılmasına ve/veya erişimin engellenmesine ilişkin karara 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz edilebilir.

(3) Hâkim, mahkeme veya Cumhuriyet savcısı tarafından verilen (Değişik: 29/7/2020-7253/4. md.) içeriğin çıkarılması ve/veya erişimin engellenmesi kararının birer örneği, gereği yapılmak üzere Kuruma gönderilir.

(4) İçeriği birinci fıkrada belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsa bile, içeriği birinci fıkranın (a) bendinin (2) ve (5) ve (6) ve (7) numaralı alt bentlerinde ve (c) bendinde yazılı suçları oluşturan yayınlara ilişkin olarak (Değişik: 29/7/2020-7253/4. md.) içeriğin çıkarılması ve/veya erişimin engellenmesi kararı re'sen Başkan tarafından verilir. (Değişik cümle:29/7/2020-7253/4 md.) Bu karar, ilgili içerik ve yer sağlayıcılar ile erişim sağlayıcısına bildirilerek gereğinin yerine getirilmesi istenir.

(5) (Değişik: 29/7/2020-7253/4. md.) İçeriğin çıkarılması ve/veya erişimin engellenmesi kararının gereği, derhal ve en geç kararın bildirilmesi anından itibaren dört saat içinde yerine getirilir.

(6) Başkan tarafından verilen (Değişik: 29/7/2020-7253/4. md.) içeriğin çıkarılması ve/veya erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi halinde, Başkan tarafından, Cumhuriyet başsavcılığına suç duyurusunda bulunulur.

(7) Soruşturma sonucunda kovuşturmayaya yer olmadığı kararı verilmesi halinde, (Değişik: 29/7/2020-7253/4. md.) içeriğin çıkarılması ve/veya erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda Cumhuriyet savcısı, (Ek: 17-10-2019-7188/36 md.) hükümsüz kalan (Değişik: 29/7/2020-7253/4. md.) içeriğin çıkarılması ve/veya erişimin engellenmesi kararına konu internet adresini belirtmek suretiyle, kovuşturmayaya yer olmadığı kararının bir örneğini Kuruma gönderir.

(8) Kovuşturma evresinde beraat kararı verilmesi halinde, (Değişik: 29/7/2020-7253/4. md.) içeriğin çıkarılması ve/veya erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda (Ek: 17-10-2019-7188/36 md.) mahkemece hükümsüz kalan (Değişik: 29/7/2020-7253/4. md.) içeriğin çıkarılması ve/veya erişimin engellenmesi kararına konu internet adresini belirtmek suretiyle, beraat kararının bir örneği Kuruma gönderilir.

(9) Konusu birinci fıkrada sayılan suçları oluşturan içeriğin yayından çıkarılması halinde; erişimin engellenmesi kararı, soruşturma evresinde Cumhuriyet savcısı, kovuşturma evresinde mahkeme tarafından kaldırılır.

(10) Koruma tedbiri olarak verilen (Değişik: 29/7/2020-7253/4. md.) içeriğin çıkarılması ve/veya erişimin engellenmesi kararının gereğini yerine getirmeyen içerik, yer veya erişim sağlayıcılarının sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır.

(11) İdarî tedbir olarak verilen (Değişik: 29/7/2020-7253/4. md.) içeriğin çıkarılması ve/veya erişimin engellenmesi kararının yerine getirilmemesi halinde, Başkan tarafından ilgili (Değişik: 29/7/2020-7253/4. md.) içerik, yer ve erişim sağlayıcısına, onbin Yeni Türk Lirasından yüzbin Yeni Türk Lirasına kadar idarî para cezası verilir. İdarî para cezasının verildiği andan itibaren yirmidört saat içinde (EK: 29/7/2020-7253/4. md.) erişim sağlayıcı tarafından kararın yerine getirilmemesi halinde (...) Kurum tarafından yetkilendirmenin iptaline karar verilebilir.

(12) Bu Kanunda tanımlanan kabahatler dolayısıyla (...) Kurum tarafından verilen idarî para cezalarına ilişkin kararlara karşı, 6/1/1982 tarihli ve 2577 sayılı İdarî Yargılama Usulü Kanunu hükümlerine göre kanun yoluna başvurulabilir.

(13) (Ek: 5/11/2008-5809/67 md.) İşlemlerin yürütülmesi için Kuruma gönderilen hakim ve mahkeme kararlarına 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre Kurum tarafından itiraz edilebilir.

(14) (Ek: 12/7/2013-6495/47 md.) 14/3/2007 tarihli ve 5602 sayılı Şans Oyunları Hasılatından Alınan Vergi, Fon ve Payların Düzenlenmesi Hakkında Kanununun 3 üncü maddesinin birinci fıkrasının (ç)

bendinde tanımlanan kurum ve kuruluşlar, kendi görev alanına giren suçların internet ortamında işlendiğini tespit etmeleri hâlinde, bu yayınlarla ilgili olarak erişimin engellenmesi kararı alabilirler. Erişimin engellenmesi kararları uygulanmak üzere Kuruma gönderilir.

(15) (Ek: 26/2/2014-6527/17 md.) Bu maddeye göre soruşturma aşamasında verilen hâkim kararı ile 9 uncu ve 9/A maddesine göre verilen hâkim kararı birden fazla sulh ceza mahkemesi bulunan yerlerde Hâkimler ve Savcılar Yüksek Kurulu tarafından belirlenen sulh ceza mahkemeleri tarafından verilir.

(16) (Ek: 10/9/2014-6552/127 md.; İptal: Anayasa Mahkemesinin 2/10/2014 tarihli ve E.: 2014/149, K.: 2014/151 sayılı Kararı ile.)

(17) (Ek:17/10/2019-7188/36 md.) Bu maddenin ikinci, dördüncü ve ondördüncü fıkraları kapsamında verilen erişimin engellenmesi kararları, ihlalin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verilir. Ancak, teknik olarak ihlale ilişkin içeriğe erişimin engellenmesi yapılamadığı veya ilgili içeriğe erişimin engellenmesi yoluyla ihlalin önlenemediği durumlarda, internet sitesinin tümüne yönelik olarak erişimin engellenmesi kararı verilebilir.

Gecikmesinde sakınca bulunan hâllerde içeriğin çıkarılması ve/veya erişimin engellenmesi

MADDE 8/A- (Ek: 27/3/2015-6639/29 md.)

(1) Yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması sebeplerinden bir veya bir kaçına bağlı olarak hâkim veya gecikmesinde sakınca bulunan hâllerde, Cumhurbaşkanlığı veya millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması ile ilgili bakanlıkların talebi üzerine Başkan tarafından internet ortamında yer alan yayınlara ilgili olarak içeriğin çıkarılması ve/veya erişimin engellenmesi kararı verilebilir. Karar, Başkan tarafından derhâl erişim sağlayıcılara ve ilgili içerik ve yer sağlayıcılara bildirilir. İçerik çıkartılması ve/veya erişimin engellenmesi kararının gereği, derhâl ve en geç kararın bildirilmesi anından itibaren dört saat içinde yerine getirilir.

(2) Cumhurbaşkanlığı veya ilgili Bakanlıkların talebi üzerine Başkan tarafından verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararı, Başkan tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi hâlde, karar kendiliğinden kalkar.

(3) Bu madde kapsamında verilen erişimin engellenmesi kararları, ihlalin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verilir. Ancak,

teknik olarak ihlale ilişkin içeriğe erişimin engellenmesi yapılamadığı veya ilgili içeriğe erişimin engellenmesi yoluyla ihlalin önlenemediği durumlarda, internet sitesinin tümüne yönelik olarak erişimin engellenmesi kararı verilebilir.

(4) Bu madde kapsamındaki suçla konu internet içeriklerini oluşturan ve yayanlar hakkında Başkan tarafından, Cumhuriyet Başsavcılığına suç duyurusunda bulunulur. Bu suçların faillerine ulaşmak için gerekli olan bilgiler içerik, yer ve erişim sağlayıcılar tarafından hâkim kararı üzerine adli mercilere verilir. Bu bilgileri vermeyen içerik, yer ve erişim sağlayıcıların sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, üç bin günden on bin güne kadar adli para cezası ile cezalandırılır.

(5) Bu madde uyarınca verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararının gereğini yerine getirmeyen erişim sağlayıcılar ile ilgili içerik ve yer sağlayıcılara Başkan tarafından elli bin Türk lirasından beş yüz bin Türk lirasına kadar idari para cezası verilir.

İçeriğin yayından çıkarılması ve erişimin engellenmesi

MADDE 9- (Değişik: 6/2/2014-6518/93 md.)

(1) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak (Değişik: 29/7/2020-7253/5. md.) içeriğin çıkarılmasını ve/veya erişimin engellenmesini de isteyebilir.

(2) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişilerin talepleri, içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılır.

(3) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talepleri doğrultusunda hâkim bu maddede belirtilen kapsamda (Değişik: 29/7/2020-7253/5. md.) içeriğin çıkarılmasına ve/veya erişimin engellenmesine karar verebilir.

(4) Hâkim, bu madde kapsamında vereceği erişimin engellenmesi kararlarını esas olarak, yalnızca kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verir. Zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemez. Ancak, hâkim URL adresi belirtilerek içeriğe erişimin engellenmesi yöntemiyle ihlalin engellenemeyeceğine kanaat getirmesi hâlinde,

gerekçesini de belirtmek kaydıyla, internet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilir.

(5) Hâkimin bu madde kapsamında verdiği (Değişik: 29/7/2020-7253/5. md.) içeriğin çıkarılması ve/veya erişimin engellenmesi kararları doğrudan Birliğe gönderilir.

(6) Hâkim bu madde kapsamında yapılan başvuruyu en geç yirmi dört saat içinde duruşma yapmaksızın karara bağlar. Bu karara karşı 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir.

(7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

(8) (Değişik:29/7/2020-7253/5 md.) Birlik tarafından ilgili içerik ve yer sağlayıcılar ile erişim sağlayıcıya gönderilen (Değişik:29/7/2020-7253/5 md.) içeriğin çıkarılması ve/veya erişimin engellenmesi kararının gereği derhâl, en geç dört saat içinde ilgili içerik ve yer sağlayıcılar ile erişim sağlayıcı tarafından yerine getirilir.

(9) Bu madde kapsamında hâkimin verdiği içeriğin çıkarılması ve/veya erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının (...) başka internet adreslerinde de yayınlanması durumunda ilgili kişi tarafından Birliğe müracaat edilmesi hâlinde mevcut karar bu adresler için de uygulanır.

(10) (Ek:29/7/2020-7253/5 md.) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talep etmesi durumunda hâkim tarafından, başvuranın adının bu madde kapsamındaki karara konu internet adresleri ile ilişkilendirilmemesine karar verilebilir. Kararda, Birlik tarafından hangi arama motorlarına bildirim yapılacağı gösterilir.

(11) Sulh ceza hâkiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen (Değişik:29/7/2020-7253/5 md.) içerik, yer ve erişim sağlayıcıların sorumluları, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır.

Özel hayatın gizliliği nedeniyle içeriğe erişimin engellenmesi

MADDE 9/A (Ek: 6/2/2014-6518/94 md.)

(1) İnternet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, Kuruma doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilir.

(2) Yapılan bu istekte; hakkın ihlaline neden olan yayının tam adresi (URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilere yer verilir. Bu bilgilerde eksiklik olması hâlinde talep işleme konulmaz.

(3) Başkan, kendisine gelen bu talebi uygulanmak üzere derhâl Birliğe bildirir, erişim sağlayıcılar bu tedbir talebini derhâl, en geç dört saat içinde yerine getirir.

(4) Erişimin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanır.

(5) Erişimin engellenmesini talep eden kişiler, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebini talepte bulunduğu saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunar. Hâkim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklar ve doğrudan Kuruma gönderir; aksi hâlde, erişimin engellenmesi tedbiri kendiliğinden kalkar.

(6) Hâkim tarafından verilen bu karara karşı Başkan tarafından 5271 sayılı Kanun hükümlerine göre itiraz yoluna gidilebilir.

(7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

(8) Özel hayatın gizliliğinin ihlaline bağlı olarak gecikmesinde sakınca bulunan hâllerde doğrudan Başkanın emri üzerine erişimin engellenmesi Kurum tarafından yapılır. (Mülga cümle: 26/2/2014-6527/18 md.)

(9) (Ek: 26/2/2014-6527/18 md.) Bu maddenin sekizinci fıkrası kapsamında Başkan tarafından verilen erişimin engellenmesi kararı, (...) yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar.

İdarî yapı ve görevler

MADDE 10

(1) Kanunla verilen görevler, Kurum tarafından yerine getirilir.

(2) Bu Kanunla ekli listedeki kadrolar ihdas edilerek Kurumun hizmetlerinde kullanılmak üzere 5/4/1983 tarihli ve 2813 sayılı Telsiz Kanununa ekli (II) sayılı listeye eklenmiştir. (Mülga ikinci ve üçüncü cümle: 15/8/2016-KHK-671/21 md.; Aynen kabul: 9/11/2016-6757/18 md.)

(3) Kuruma Kanunla verilen görevlere ilişkin olarak yapılacak her türlü mal veya hizmet alımları, ceza ve ihalelerden yasaklama işleri hariç, 4/1/2002 tarihli ve 4734 sayılı Kamu İhale Kanunu ile 5/1/2002 tarihli ve 4735 sayılı Kamu İhale Sözleşmeleri Kanunu hükümlerine tâbi olmaksızın Kurum bütçesinden karşılanır.

(4) Kanunlarla verilen diğer yetki ve görevleri saklı kalmak kaydıyla, Kurumun bu Kanun kapsamındaki görev ve yetkileri şunlardır:

a) Bakanlık, kolluk kuvvetleri, ilgili kamu kurum ve kuruluşları ile içerik, yer ve erişim sağlayıcılar ve ilgili sivil toplum kuruluşları arasında koordinasyon oluşturarak internet ortamında yapılan ve bu Kanun kapsamına giren suçları oluşturan içeriğe sahip faaliyet ve yayınları önlemeye, internetin güvenli kullanımını sağlamaya, bilişim şuurunu geliştirmeye yönelik çalışmalar yapmak, bu amaçla, gerektiğinde, her türlü giderleri yönetmelikle belirlenecek esas ve usûller dahilinde Kurumca karşılanacak çalışma kurulları oluşturmak.

b) İnternet ortamında yapılan yayınların içeriklerini izleyerek, bu Kanun kapsamına giren suçların işlendiğinin tespiti halinde, bu yayınlara erişimin engellenmesine yönelik olarak bu Kanunda öngörülen gerekli tedbirleri almak.

c) İnternet ortamında yapılan yayınların içeriklerinin izlenmesinin hangi seviye, zaman ve şekilde yapılacağını belirlemek.

ç) Kurum tarafından işletmecilerin yetkilendirilmeleri ile mülkî idare amirlerince ticarî amaçlı toplu kullanım sağlayıcılara verilecek izin belgelerinde filtreleme ve bloke etmede kullanılacak sistemlere ve yapılacak düzenlemelere yönelik esas ve usûlleri belirlemek.

d) İnternet ortamındaki yayınların izlenmesi suretiyle bu Kanunun 8 inci maddesi ile 8/A maddesinde sayılan suçların işlenmesini önlemek için izleme ve bilgi ihbar merkezi dahil, gerekli her türlü teknik altyapıyı kurmak veya kurdurmak, bu altyapıyı işletmek veya işletilmesini sağlamak.

e) İnternet ortamında herkese açık çeşitli servislerde yapılacak filtreleme, perdeleme ve izleme esaslarına göre donanım üretilmesi veya yazılım yapılmasına ilişkin asgari kriterleri belirlemek.

f) Bilişim ve internet alanındaki uluslararası kurum ve kuruluşlarla işbirliği ve koordinasyonu sağlamak.

g) Bu Kanunun 8 inci maddesinin birinci fıkrasında sayılan suçların, internet ortamında işlenmesini konu alan her türlü temsili görüntü, yazı veya sesleri içeren ürünlerin tanıtımı, ülkeye sokulması, bulundurulması, kiraya verilmesi veya satışının önlenmesini teminen yetkili ve görevli kolluk

kuvvetleri ile soruşturma mercilerine, teknik imkânları dahilinde gereken her türlü yardımda bulunmak ve koordinasyonu sağlamak.

(5) (Değişik: 6/2/2014-6518/95 md.) Kurum; Bakanlık bünyesinde 26/9/2011 tarihli ve 655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname hükümleri uyarınca oluşturulan İnternet Geliştirme Kurulunca internetin yaygınlaştırılması, geliştirilmesi, yaygın ve güvenli kullanılması gibi konularda yapılacak öneriler ile ilgili gerekli her türlü tedbir veya kararları alır.

(6) (Ek: 6/2/2014-6518/95 md.) Kurum, ulusal siber güvenlik faaliyetleri kapsamında, siber saldırıların tespiti ve önlenmesi konusunda, içerik, yer, erişim sağlayıcılar ve ilgili diğer kurum ve kuruluşlarla koordinasyon sağlar, gerekli tedbirlerin alınması konusunda faaliyet yürütür ve ihtiyaç duyulan çalışmaları yapar.

(7) (Ek: 6/2/2014-6518/95 md.) Kurum kanunlarla kendisine verilen görevlerin ifası amacıyla araştırma ve geliştirme merkezleri kurabilir.

Yönetmelikler

MADDE 11

(1) Bu Kanunun uygulanmasına ilişkin esas ve usûller, Cumhurbaşkanı tarafından çıkarılacak yönetmeliklerle düzenlenir. Bu yönetmelikler, Kanunun yürürlüğe girdiği tarihten itibaren dört ay içinde çıkarılır.

(2) Yer veya erişim sağlayıcı olarak faaliyet icra etmek isteyen kişilere, telekomünikasyon yoluyla iletişim konusunda yetkilendirme belgesi olup olmadığına bakılmaksızın, yer, erişim ve toplu kullanım sağlayıcıların yükümlülüklerine ilişkin esas ve usûller, Kurum tarafından çıkarılacak yönetmelikle düzenlenir. Bu yönetmelik, Kanunun yürürlüğe girdiği tarihten itibaren beş ay içinde çıkarılır.

İlgili kanunlarda yapılan değişiklikler

MADDE 12

(1) (4/2/1924 tarihli ve 406 sayılı Telgraf ve Telefon Kanunu ile ilgili olup yerine işlenmiştir.)

(2) (4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Salahiyet Kanunu ile ilgili olup yerine işlenmiştir.)

(3) (5/4/1983 tarihli ve 2813 sayılı Telsiz Kanunu ile ilgili olup yerine işlenmiştir.)

(4) (1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu ile ilgili olup yerine işlenmiştir.)

EK MADDE 1 - (Ek: 5/11/2008-5809/67 md.)

(1) (Mülga: 15/8/2016-KHK-671/21 md.; Aynen kabul: 9/11/2016-6757/18 md.)

(2) (Mülga: 15/8/2016-KHK-671/21 md.; Aynen kabul: 9/11/2016-6757/18 md.)

(3) (Mülga: 15/8/2016-KHK-671/21 md.; Aynen kabul: 9/11/2016-6757/18 md.)

(4) (Mülga: 15/8/2016-KHK-671/21 md.; Aynen kabul: 9/11/2016-6757/18 md.)

(5) (Ek: 6/2/2014-6518/97 md.) 8/6/1984 tarihli ve 217 sayılı Devlet Personel Başkanlığı Kuruluş ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 2 nci maddesinde sayılan kamu kurum ve kuruluşlarında çalışanlar kurumlarının, hâkim ve savcılar ise kendilerinin muvafakati ile aylık, ödenek, her türlü zam ve tazminatlar ile diğer mali ve sosyal hak ve yardımları kurumlarınca ödenmek kaydıyla geçici olarak Kurum emrinde görevlendirilebilir. Bu kapsamda görevlendirilen personel sayısı Kurumun kadro sayısının yüzde yirmisini geçemez. Bu personel kurumlarından izinli sayılır. İzinli oldukları sürece memuriyetleri ile ilgili özlük hakları devam eder ve bu süreler terfi ve emekliliklerinde hesaba katılır. Terfileri başkaca bir işleme gerek kalmaksızın süresinde yapılır.

(6) (Ek: 6/2/2014-6518/97 md.; Mülga: 15/8/2016-KHK-671/21 md.; Aynen kabul: 9/11/2016-6757/18 md.)

(7) Bu Kanunla ekli (V) sayılı cetveldeki kadrolar ihdas edilerek Telekomünikasyon İletişim Başkanlığı hizmetlerinde kullanılmak üzere 5651 sayılı Kanuna ekli (I) sayılı listeye eklenmiştir.

EK MADDE 2 - (Ek: 6/2/2014-6518/99 md.)

Kuruma verilen görevlerin yürütülmesi için, 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu ile diğer kanunların sözleşmeli personel çalıştırılmasına dair hükümlerine bağlı kalınmaksızın özel bilgi ve ihtisas gerektiren konularda Kurumda sözleşmeli personel çalıştırılabilir. Bu suretle çalıştırılacakların unvanı, sayısı, süresi, ücretleri ve diğer hususlar Cumhurbaşkanınca yürürlüğe konulacak hizmet sözleşmesi esaslarına göre tespit edilir. Bunlara ödenecek ücret, 657 sayılı Kanunun 4 üncü maddesinin (B) bendine göre çalıştırılanlar için uygulanmakta olan sözleşme ücreti tavanının beş katını, çalıştırılabilecek toplam sözleşmeli personel sayısı ise ikiyüzelliye geçemez ve bu fıkrada belirtilen ücret dışında herhangi bir ödeme yapılamaz.

EK MADDE 3 - (Ek: 15/8/2016-KHK-671/22 md.; Aynen kabul: 9/11/2016-6757/19 md.)

(1) Telekomünikasyon İletişim Başkanlığı kapatılmıştır.

(2) Dięer mevzuatta Telekomünikasyon İletiřim Bařkanlıęına yapılan atıflar Bilgi Teknolojileri ve İletiřim Kurumuna, Telekomünikasyon İletiřim Bařkanına yapılan atıflar Bilgi Teknolojileri ve İletiřim Kurumu Bařkanına yapılmıř sayılır.

EK MADDE 4 - (Ek:29/7/2020-7253/6 md.)

(1) Türkiye'den gnlk eriřimi bir milyondan fazla olan yurt dıřı kaynaklı sosyal aę saęlayıcı; Kurum, Birlik, adli veya idari makamlarca gnderilecek tebligat, bildirim veya taleplerin gereęinin yerine getirilmesi ve kiřiler tarafından bu Kanun kapsamında yapılacak bařvuruların cevaplandırılması ve bu Kanun kapsamındaki dięer ykmllklerin yerine getirilmesini temin iin yetkili en az bir kiřiyi Türkiye'de temsilci olarak belirler ve bu kiřinin iletiřim bilgilerine kolayca grlebilecek ve doęrudan eriřilebilecek Őekilde internet sitesinde yer verir. Sosyal aę saęlayıcı bu kiřinin kimlik ve iletiřim bilgilerini Kuruma bildirmekle ykmldr. Temsilcinin gerek kiři olması hlinde Trk vatandařı olması zorunludur.

(2) Birinci fıkrada dzenlenen temsilci belirleme ve bildirme ykmllęn yerine getirmeyen sosyal aę saęlayıcıya, Kurum tarafından bildirimde bulunulur. Bildirimden itibaren otuz gn iinde bu ykmllęn yerine getirilmemesi hlinde sosyal aę saęlayıcıya Bařkan tarafından on milyon Trk lirası idari para cezası verilir. Verilen idari para cezasının teblięinden itibaren otuz gn iinde bu ykmllęn yerine getirilmemesi hlinde otuz milyon Trk lirası daha idari para cezası verilir. İkinici kez verilen idari para cezasının teblięinden itibaren otuz gn iinde bu ykmllęn yerine getirilmemesi hlinde Bařkan tarafından Türkiye'de mukim vergi mkellefi olan gerek ve tzel kiřilerin ilgili sosyal aę saęlayıcısına yeni reklam vermesi yasaklanır, bu kapsamda yeni szleřme kurulamaz ve buna iliřkin para transferi yapılamaz. Reklam yasaęı kararının verildięi tarihten itibaren  ay iinde bu ykmllęn yerine getirilmemesi hlinde Bařkan, sosyal aę saęlayıcının internet trafięi bant geniřlięinin yzde elli oranında daraltılması iin sulh ceza hkimlięine bařvurabilir. Bařvurunun kabulne iliřkin hkim kararının uygulanmasından itibaren otuz gn iinde sz konusu ykmllęn yerine getirilmemesi hlinde Bařkan, sosyal aę saęlayıcının internet trafięi bant geniřlięinin yzde doksan oranına kadar daraltılması iin sulh ceza hkimlięine bařvurabilir. Hkim ikinci bařvuru zerine vereceęi kararında, yzde elliden dřk olmamak kaydıyla, sunulan hizmetin nitelięini de dikkate alarak daha dřk bir oran belirleyebilir. Bu kararlara karřı Bařkan tarafından 5271 sayılı Kanun hkmlerine gre itiraz yoluna gidilebilir. Hkim tarafından verilen kararlar eriřim saęlayıcılara bildirilmek zere Kuruma gnderilir. Kararların gereęi, bildirimden itibaren derhl ve en ge drt saat iinde eriřim saęlayıcıları tarafından yerine getirilir. Temsilci belirleme ve bildirme ykmllęnn yerine getirilmesi hlinde; verilen idari

para cezalarının dördte biri tahsil edilir, reklam yasağı kaldırılır ve hâkim kararları kendiliğinden hükümsüz kalır. İnternet trafiği bant genişliğine yapılan müdahalenin sona erdirilmesi için erişim sağlayıcılara Kurum tarafından bildirim yapılır.

(3) Türkiye’den günlük erişimi bir milyondan fazla olan yurt içi veya yurt dışı kaynaklı sosyal ağ sağlayıcı, 9 uncu ve 9/A maddeleri kapsamındaki içeriklere yönelik olarak kişiler tarafından yapılacak başvurulara, başvurudan itibaren en geç kırk sekiz saat içinde olumlu ya da olumsuz cevap vermekle yükümlüdür. Olumsuz cevaplar gerekçeli olarak verilir.

(4) Türkiye’den günlük erişimi bir milyondan fazla olan yurt içi veya yurt dışı kaynaklı sosyal ağ sağlayıcı, kendisine bildirilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararlarının uygulanmasına ve üçüncü fıkra kapsamındaki başvurulara ilişkin istatistiksel ve kategorik bilgileri içeren Türkçe hazırlanmış raporları altı aylık dönemlerle Kuruma bildirir. Üçüncü fıkra kapsamındaki başvurulara ilişkin rapor, kişisel verilerden arındırılmak suretiyle sosyal ağ sağlayıcının kendi internet sitesinde de yayınlanır.

(5) Türkiye’den günlük erişimi bir milyondan fazla olan yurt içi veya yurt dışı kaynaklı sosyal ağ sağlayıcı, Türkiye’deki kullanıcıların verilerini Türkiye’de barındırma yönünde gerekli tedbirleri alır.

(6) Üçüncü fıkradaki yükümlülüğü yerine getirmeyen sosyal ağ sağlayıcıya beş milyon Türk lirası, dördüncü fıkradaki yükümlülüğü yerine getirmeyen sosyal ağ sağlayıcıya ise on milyon Türk lirası idari para cezası Başkan tarafından verilir.

(7) Türkiye’den günlük erişimi bir milyondan fazla olan yurt dışı kaynaklı sosyal ağ sağlayıcılar hakkında 8 inci ve 8/A maddeleri kapsamında verilecek olan idari para cezaları bir milyon Türk lirası olarak, 8 inci ve 9 uncu maddeleri kapsamında verilecek olan adli para cezaları ise elli bin gün olarak verilir. Söz konusu idari para cezasını gerektiren ihlallerin bir yıl içinde her bir tekrarında cezalar bir kat artırılarak uygulanır.

(8) Hukuka aykırılığı hâkim veya mahkeme kararı ile tespit edilen içeriğin sosyal ağ sağlayıcıya bildirilmesi durumunda, bildirime rağmen yirmi dört saat içinde içeriği çıkarmayan veya erişimi engellemeyen sosyal ağ sağlayıcı, doğan zararların tazmin edilmesinden sorumludur. Bu hukuki sorumluluğun işletilmesi için içerik sağlayıcının sorumluluğuna gidilmesi veya içerik sağlayıcıya dava açılması şartı aranmaz.

(9) Bu maddenin uygulanmasında sosyal ağ sağlayıcının yükümlülükleri, içerik veya yer sağlayıcısı olmasından doğan sorumluluk ve yükümlülüklerini ortadan kaldırmaz.

(10) Bu maddenin uygulanmasına ilişkin usul ve esaslar Kurum tarafından belirlenir.

GEÇİCİ MADDE 1 - (1) Başkanlığın kuruluştaki hizmet binasının yapımı, ceza ve ihalelerden yasaklama işleri hariç, Kamu İhale Kanunu ve Kamu İhale Sözleşmeleri Kanunu hükümlerine tâbi olmaksızın Kurum bütçesinden karşılanır.

(2) Halen faaliyet icra eden ticarî amaçla toplu kullanım sağlayıcılar, bu Kanunun yürürlüğe girdiği tarihten itibaren altı ay içinde 7 nci maddeye göre alınması gereken izin belgesini temin etmekle yükümlüdürler.

(3) Halen yer veya erişim sağlayıcı olarak faaliyet icra eden kişilere, Kurum tarafından, telekomünikasyon yoluyla iletişim konusunda yetkilendirme belgesi olup olmadığına bakılmaksızın, yer veya erişim sağlayıcı olarak faaliyet icra etmesi amacıyla bir yetkilendirme belgesi düzenlenir.

GEÇİCİ MADDE 2 - (Ek: 5/11/2008-5809/67 md.)

(1) Telekomünikasyon İletişim Başkanlığı kadrolarında bulunan personelden ek 1 inci maddede belirtilen öğrenim şartlarını haiz olanlar; kamuda üç yıllık hizmet süresini tamamlamaları, KPDS'den en az 60 veya uluslararası geçerliliği olan sınavlardan muadili puan almaları ve hazırlayacakları tezin kabul edilmesi halinde bu Kanunun yayımı tarihinden itibaren beş yıl içerisinde iletişim uzmanı kadrosuna atanabilirler. Bu personelden; diğer kamu kurum ve kuruluşlarında özel mevzuatları uyarınca yarışma sınavına tabi tutularak mesleğe alınan ve yeterlik sınavını vererek veya tezi başarılı bulunarak kariyer meslek kadrolarına atanmış olanlar yabancı dil şartını karşıladıklarında; yüksek lisans veya doktora öğrenimini tamamlamış olanlardan, hazırladıkları yüksek lisans veya doktora tezlerinin konularının Kurumun veya Başkanlığın görev alanı ile ilgili olduğunun yapılacak inceleme sonucu belirlenenlerden doktora öğrenimini tamamlamış olanlar doğrudan, yüksek lisans öğrenimini tamamlamış olanlar yabancı dil şartını karşıladıklarında, iletişim uzmanı olarak atanabilirler.

(2) Telekomünikasyon İletişim Başkanlığı personelinden dört yıllık fakülte mezunu olanlar, kamuda üç yıllık hizmet süresini tamamlamaları, çıkarılacak yönetmelikte öngörülen şartları taşımaları ve buna ilave olarak hazırlayacakları tezin kabul edilmesi veya tezli yüksek lisans veya doktora yapmaları halinde, bu Kanunun yayımı tarihinden beş yıl içinde öğrenim alanına göre teknik uzman veya idarî uzman kadrosuna atanabilirler.

GEÇİCİ MADDE 3 - (Ek: 6/2/2014-6518/100 md.)

(1) Birliğin kuruluşu bu Kanunun yayımı tarihinden itibaren üç ay içinde tamamlanır.

(2) (Değişik: 27/3/2015-6639/30 md.) Birlik, bu maddenin yürürlük tarihi itibarıyla aboneli bulunan mevcut internet servis sağlayıcıları ile erişim hizmeti veren işletmecilerin en az dörtte birinin katılımıyla imzalanan Birlik Tüzüğü'nün Kurum tarafından incelenerek uygun bulunmasını müteakip

faaliyete başlar. Birliğin kurulmasını müteakip en geç bir ay içinde hâlen üye olmayan internet servis sağlayıcıları ve erişim hizmeti veren işletmeciler üyeliklerini tamamlamak zorundadır.

(3) Belirtilen sürede Birliğin kuruluşunu tamamlayamaması hâlinde, Kurum tarafından internet servis sağlayıcılarına ve internet erişim hizmeti veren diğer işletmecilere bir önceki takvim yılındaki net satışlarının yüzde biri oranında idari para cezası uygulanır.

(4) Birliğin kurulmasını müteakip bir ay içinde üye olmayan internet servis sağlayıcılarına veya internet erişim hizmeti veren diğer işletmecilere, Kurum tarafından bir önceki takvim yılındaki net satışlarının yüzde biri oranında idari para cezası uygulanır.

GEÇİCİ MADDE 4 - (Ek: 15/8/2016-KHK-671/23 md.; Aynen kabul: 9/11/2016-6757/20 md.)

(1) Telekomünikasyon İletişim Başkanının görevi bu maddenin yürürlüğe girdiği tarihte sona erer ve hakkında 375 sayılı Kanun Hükmünde Kararnamenin ek 18 inci maddesi hükümleri uygulanır. Telekomünikasyon İletişim Başkanlığında görevli daire başkanlarının görevleri bu maddenin yürürlüğe girdiği tarihte sona erer. Bunlardan daha önce İletişim Uzmanı unvanını ihraz etmiş olanlar Bilgi Teknolojileri ve İletişim Kurumunda Bilişim Uzmanı kadrolarına atanmış sayılırlar.

(2) Telekomünikasyon İletişim Başkanlığında görevli olup terör örgütlerine veya Milli Güvenlik Kurulunca Devletin milli güvenliğine karşı faaliyette bulunduğu karar verilen yapı, oluşum veya gruplara üyeliği, mensubiyeti veya iltisakı yahut bunlarla irtibatı olmadığı değerlendirilen personelden İletişim Uzmanı ve İletişim Uzman Yardımcıları, Bilgi Teknolojileri ve İletişim Kurumunda bulunan Bilişim Uzmanı ve Bilişim Uzman Yardımcısı kadrolarına, diğer personel ise Bilgi Teknolojileri ve İletişim Kurumunda bulunan aynı unvanlı kadrolara başka bir işleme gerek kalmaksızın halen buldukları kadro derecesiyle atanmış sayılırlar. Bunların atanmış sayıldıkları tarih itibarıyla diğer kanunlardaki hükümlere bakılmaksızın ve başka bir işleme gerek kalmaksızın kadroları ihdas edilmiş ve ilgili mevzuatı uyarınca Kurum kadro cetvellerine eklenmiş sayılır. Bu şekilde atananların Uzman ve Uzman Yardımcılığında geçirdiği süreler atanmış sayıldıkları Kurum kadrolarında geçmiş sayılır.

GEÇİCİ MADDE 5 - (Ek:29/7/2020-7253/7 md.)

(1) Sosyal ağ sağlayıcılar, ek 4 üncü maddenin;

a) Üçüncü fıkrası kapsamındaki yükümlülüklerini yerine getirmek üzere bu maddenin yürürlük tarihinden itibaren üç ay içinde gerekli çalışmaları tamamlar.

b) Dördüncü fıkrası kapsamındaki yükümlülükleri uyarınca hazırlayacakları ilk raporlarını, 2021 yılı Haziran ayında Kuruma bildirir ve internet sitesinde yayınlar.

Yürürlük

MADDE 13- (1) Bu Kanunun;

a) 3 üncü ve 8 inci maddeleri, yayımı tarihinden altı ay sonra,

b) Diğer maddeleri yayımı tarihinde,

yürürlüğe girer.

Yürütme

MADDE 14- (1) Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

5624 sayılı Kan ve Kan Ürünleri Kanunu

Resmî Gazete Tarihi : 02.05.2007

Resmî Gazete Sayısı : 26510

KAN VE KAN ÜRÜNLERİ KANUNU

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç ve kapsam

MADDE 1 - (1) Bu Kanunun amacı; kan, kan bileşenleri ve ürünleri ile ilgili usûl ve esasları düzenlemektir.

(2) Bu Kanun; kan, kan bileşenleri ve ürünleri hizmetlerini yürüten kamu kurum ve kuruluşları ile bu alanda faaliyette bulunmak üzere Bakanlıkça izin verilmiş gerçek kişiler ile özel hukuk tüzel kişilerini kapsar.

(3) Kan kök hücresi uygulamaları bu Kanun kapsamı dışındadır.

Tanımlar

MADDE 2 - (1) Bu Kanunda geçen;

a) Aferez: Elde edilmek istenen kan bileşenlerinin özel bir cihaz kullanılarak ayrıştırılmasını,

b) Bakan: Sağlık Bakanını,

c) Bakanlık: Sağlık Bakanlığını,

ç) Bölge kan merkezi: Bakanlığın belirleyeceği bölgelerde kurulan, kendi bölgesindeki kan bağış ve transfüzyon merkezleri ile işbirliği içinde çalışan, sorumlu olduğu bölgenin kan ihtiyacını karşılayacak kapasitede olan, kan bankacılığı ile ilgili bütün iş ve işlemlerin yapılabilirdiği en kapsamlı birimi,

d) Hizmet birimi: Transfüzyon merkezi, kan bağış merkezi ve bölge kan merkezini,

e) Kan bağışçısı (donör): Tam kan veya bileşenlerini veren kişiyi,

f) Kan bağış (donasyon): Tam kan veya kan bileşenleri verme işlemini,

- g) Kan bağış merkezi: Bağışçıdan kan alan, işleyiş yönünden bölge kan merkezine bağılı olarak çalışan birimi,
- ğ) Kan bileşenleri: Doğrudan, aferez veya diğere yöntemlerle tam kandan elde edilen eritrosit, trombosit, granülosit suspansiyonları gibi hücresel kan bileşenleri ile plazmayı,
- h) Kan ürünleri: Kandan elde edilen kan bileşenleri ve plazma ürünlerini,
- ı) Plazma ürünleri: İnsan plazmasının işlenmesi suretiyle elde edilen tedavi maksatlı bütün ürünleri,
- i) Plazma ürünleri üretim tesisi: Taze donmuş plazmadan, tedavi amacıyla ihtiyaç duyulan proteinlerin ayrıştırılarak kullanılabilir hale getirildiğı millî ve milletlerarası standartlara uygun olarak üretim yapan tesisi,
- j) Tam kan: Kan bağışçısından transfüzyon için veya işlenerek yeni ürünler elde etmek üzere alınan ve uygun bir antikoagülan madde ile karıştırılmış ve hiçbir ayırım işlemine tâbi tutulmamış insan kanını,
- k) Transfüzyon: Sağıık sorunu sebebiyle ihtiyacı olan hastaya tam kan ya da kan bileşeni naklini,
- 1) Transfüzyon merkezi: Acil durumlar dışında kan bağışçısından kan alma yetkisi olmayan, temin edilen kanı veya bileşenini transfüzyon için çapraz karşılaştırma ve gerek duyulan diğere testleri yaparak hastalara kullanılması amacıyla hazırlayan birimi,
- ifade eder.

İKİNCİ BÖLÜM

Genel Esaslar, Kan ve Kan Ürünleri Kurulu

Genel esaslar

MADDE 3 - (1) Kan, kan bileşenleri ve ürünleri ile ilgili genel esaslar şunlardır:

- a) Bu Kanun kapsamındaki hizmetlerin planlanması, yürütülmesi ve denetlenmesi hususlarında, Bakanlık münhasıran yetkili ve sorumludur.
- b) Kan, kan bileşenleri ve ürünlerinin temininde karşılıksız ve gönüllü bağış esastır. Ancak malî karşılık anlamına gelmeyecek şekilde kan bağışçısını teşvik edici uygulamalar müstesnadır.
- c) Kan, kan bileşenleri ve ürünlerinin alınmasında ve verilmesinde bağışçı ve alıcının sağıığının tehlikeye düşürülmemesi, tıbbî risklere karşı korunması, transfüzyonun güvenle yapılması ve transfüzyon sonrası bağışçı ve alıcının izlenmesi şarttır. Alıcı ve vericide ortaya çıkabilecek komplikasyonların bildirilmesi zorunludur. Kan, kan bileşenleri ve ürünlerinin alınması, kaydı,

analizi, işlenmesi, depolanması, kullanılır hale getirilmesi, dağıtım ve kullanımını ilgilendiren kan bağıışı, kan bağıışçısı, hazırlayan kuruluş, kullanım yeri ve alıcı ile ilgili bütün verilerin yazılı veya elektronik ortamda kaydedilmesi ve otuz yıl süreyle saklanması zorunludur. Kan istek formu ve bağıışçı sorgulama formlarının asılları ile kan bağıışçısından alınan kan örneklerinin şahit numuneleri bir yıldan az olmamak üzere Bakanlıkça belirlenecek süreyle saklanır.

ç) Kan, kan bileşenleri ve ürünlerinin alınması veya transfüzyonu hekimin sorumluluğı ve denetimi altında yapılır.

d) Yurt içinde toplanan plazmanın ürün üretimi amacıyla yurt içinde ve yurt dışında değerlendirilmesi ancak Bakanlığın izni ile mümkündür. Ürün üretimi amacıyla yurtdışından plazma getirilmesi de Bakanlığın iznine tâbidir.

e) Hizmet birimi açan ve işletenlerin bu Kanun kapsamındaki faaliyetlerini ulusal ve uluslararası kalite güvence programları çerçevesinde yürütmeleri zorunludur.

f) Kan, kan bileşenleri ve ürünleri hizmetini yürütenler bağıışçıya ilişkin kişisel bilgileri korumak, üçüncü kişilere vermemek, basına açıklamamak ile yükümlüdürler. Bu bilgiler ancak Bakanlığa verilir.

g) Olağanüstü haller ile (...) [1] seferberlik ve savaş halinde lüzumlu olacak kan ve kan ürünleri ve bunlar için gerekli malzemenin temini ve ülke çapında stoklanmasını bölge kan merkezleri Bakanlığın planlaması çerçevesinde organize eder.(1)

Kan ve Kan Ürünleri Kurulu

MADDE 4 - (1) Bakanlığın; kan, kan bileşenleri ve ürünleri konusunda yapacağı çalışmalarda gerekebilecek bilimsel desteğı sağlamak üzere Bakanlık ilgili birim amiri başkanlığında kan, kan ürünleri ve kan bankacılığı konusunda yaptığı çalışmalarda alanında temayüz etmiş uzman hekimler veya bu konularda lisansüstü eğitim yapmış kişiler arasından Bakan tarafından seçilen yedi üyeden oluşan Kan ve Kan Ürünleri Kurulu oluşturulur.

(2) Kan ve Kan Ürünleri Kurulu üyelerinin görev süresi iki yıldır. Görev süresi sona eren üye tekrar seçilebilir.

ÜÇÜNCÜ BÖLÜM

Kan Temini ve Kullanımı Hizmet Birimleri

Hizmet birimleri, hizmet birimi açmaya yetkili kişiler

MADDE 5 - (1) Kanın temini ve kullanımı için transfüzyon merkezleri, kan bağışı merkezleri ve bölge kan merkezleri kurulur.

(2) Bu Kanun kapsamındaki hizmet birimlerinden;

a) Bölge kan merkezi ve kan bağışı merkezini; kamu kurum ve kuruluşları ile Türkiye Kızılay Derneği,

b) Transfüzyon merkezini; bu fıkranın (a) bendinde sayılanların yanı sıra, bünyesinde acil müdahale şartlarını taşıyan özel sağlık kuruluşlarında olmak kaydıyla gerçek kişiler ile özel hukuk tüzel kişileri,

c) Plazma ürünleri üretim tesisini; kamu kurum ve kuruluşları ile gerçek kişiler ve özel hukuk tüzel kişileri,

açıp, işletebilir.

DÖRDÜNCÜ BÖLÜM

Ruhsat, Denetim ve Cezaî Hükümler

Ruhsat alma zorunluluğu, denetim ve cezaî hükümler

MADDE 6 - (1) Bu Kanun kapsamında faaliyet gösterecek olan gerçek ve tüzel kişiler, faaliyetlerine başlamadan önce, Bakanlıktan veya Bakanlığın yetkilendirmesi halinde valiliklerden ruhsat almak ve ruhsata tâbi her faaliyet için ayrı ayrı hesap ve kayıt tutmak zorundadırlar. Gerçek ve tüzel kişiler, Bakanlık tarafından belirlenen ruhsat alma, ruhsat tadili, ruhsat sureti çıkartma ve yıllık ruhsat bedellerini Maliye Bakanlığınca belirlenecek muhasebe birimine ödemek zorundadırlar.

(2) Bakanlık, hizmet birimlerinin her türlü faaliyetini denetler veya denetlettirir. Ruhsat sahibi kişiler; tesislerini, yasal defter ve kayıtlarını Bakanlık denetimine hazır ve açık bulundurmak ve Bakanlığın ihtiyaç duyacağı her türlü bilgi ve belgeyi zamanında Bakanlığa vermek zorundadırlar.

(3) Ruhsat alınmış olması bu Kanun ve diğer mevzuatın gereklerinin yerine getirilmesi mecburiyetini ortadan kaldırmaz. Bu Kanun kapsamındaki hizmet birimleri, standartlar ve çalışma usûl ve esasları ile ilgili olarak Bakanlıkça sonradan yapılacak düzenlemelere de uymak zorundadırlar.

(4) Yapılan denetimler sonucunda tespit edilen eksikliklerin giderilmesi veya gerekli tedbirlerin alınması, işin mahiyetine göre süre verilerek veya derhal istenilir. Bakanlık, hizmetin gereği olarak giderilmesi lüzumlu eksikliklerin giderilmediği durumlarda gerekiyorsa masrafları ilgisinden alınmak kaydıyla gereken tedbirleri re'sen alır. Bu sürede eksikliğin giderilmesi Bakanlığın yaptırım uygulama yetkisini ortadan kaldırmaz.

(5) Ruhsat şartlarını faaliyetleri sırasında yitirmiş olanların ruhsatları Bakanlıkça geri alınır.

(6) (Değişik:15/11/2018-7151/30 md.) Ruhsat almadan faaliyet gösterenler valilikçe faaliyetten men edilir ve on bin Türk lirası idarî para cezası ile cezalandırılır. 3 üncü maddenin birinci fıkrasının (c) bendinde saklanması zorunlu tutulan belge ve örnekleri saklamadığı tespit edilenler ile mevcut ruhsatı kapsamı dışında faaliyet gösterenlere on bin Türk lirası idarî para cezası uygulanır; bu ihlallerin iki yıl içinde tekrarı hâlinde idarî para cezası bir kat artırılarak uygulanır; üçüncü tekrarında artırımlı idarî para cezası uygulanır ve on güne kadar faaliyeti durdurulur; dördüncü tekrarında ise faaliyetten men edilir.

(7) Yapılan denetimlerde;

a) İstenilen bilgileri zamanında vermeyenlere Bakanlıkça veya ilgili valilikçe bin Yeni Türk Lirası idarî para cezası uygulanır. Aynı fiilin tekrarı halinde beşbin Yeni Türk Lirası idarî para cezası verilir.

b) Uygun nitelikte personel çalıştırmadığı tespit edilenlere Bakanlıkça veya ilgili valilikçe beşbin Yeni Türk Lirası idarî para cezası uygulanır.

(8) Bu Kanun kapsamındaki hizmetlerde kişilerin hayatını ve sağlığını tehlikeye sokacak biçimde faaliyet gösterenler, derhal faaliyetten men edilerek bir yıldan beş yıla kadar hapis ve binbeşyüz güne kadar adlî para cezası ile cezalandırılır. Bu kişilere beş yıl süreyle ruhsat verilmez. Ayrıca teknik ve tıbbî şartları haiz olmadığı tespit edilen kan ve kan ürünlerinin müsaderesine hükmolunur.

(9) Ruhsatı geri alınan veya faaliyetten men edilen bölge kan merkezleri ile kan bağış merkezlerine ihtiyaç halinde el konularak Bakanlıkça gerekli tedbirler alınmak suretiyle işletilir.

(10) Kan yolu ile bulaşan bir hastalığı veya böyle bir hastalık taşıma riski olduğunu bilip, bu durumu saklayarak kan verenlere bir yıldan üç yıla kadar hapis ve beşyüz gün adlî para cezası verilir.

BEŞİNCİ BÖLÜM

Çeşitli Hükümler

Yönetmelik

MADDE 7 - (1) Bu Kanunda kurulması öngörülen transfüzyon merkezi, kan bağış merkezi ve bölge kan merkezlerinin kurulması, cihaz, malzeme ve personel standartlarının belirlenmesi, birbirleriyle olan ilişkileri ile çalışma usûl ve esaslarının tespiti, uygulayacakları kalite güvence programlarına dair usûl ve esaslar, ruhsat alınması ile bedelleri ve iptaline ilişkin usûl ve esaslar, plazma ürünleri üretim tesisinin kurulma ve işletilme esasları ile sair hususlar, Kan ve Kan Ürünleri Kurulunun çalışma usûl ve esasları Bakanlık tarafından çıkarılacak yönetmelikle belirlenir.

Yürürlükten kaldırılan hükümler

MADDE 8 - (1) 23/6/1983 tarihli ve 2857 sayılı Kan ve Kan Ürünleri Kanunu yürürlükten kaldırılmıştır.

Yönetmeliğin yürürlüğe konulması ve mevcut birimlerin ruhsatlandırılması

GEÇİCİ MADDE 1 - (1) Bu Kanunda öngörülen yönetmelik, altı ay içinde Bakanlıkça yürürlüğe konulur. Yönetmelik yürürlüğe girinceye kadar mevcut düzenlemelerin bu Kanuna aykırı olmayan hükümlerinin uygulanmasına devam olunur.

(2) Bu Kanunun yürürlüğe girdiği tarihe kadar faaliyet göstermekte olan A ve B tipi kan merkezleri ile kan istasyonları ve diğer hizmet birimleri, yönetmeliğin yürürlüğe girmesinden itibaren bir yıl içinde eksikliklerini gidererek faaliyet türlerine uygun şekilde ruhsat almak ve bu Kanuna uygunluklarını sağlamak zorundadırlar. Bu süre içinde Bakanlık izni olmadan bu Kanun kapsamında yeni bir birim açılmaz.

Yürürlük

MADDE 9 - (1) Bu Kanun yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 10 - (1) Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun

Resmî Gazete Tarihi : 18.10.2006

Resmî Gazete Sayısı : 26323

SUÇ GELİRLERİNİN AKLANMASININ ÖNLENMESİ HAKKINDA KANUN

BİRİNCİ BÖLÜM

Amaç ve Tanımlar

Amaç

MADDE 1 - (1) Bu Kanunun amacı, suç gelirlerinin aklanmasının önlenmesine ilişkin usûl ve esasları belirlemektir.

(...)

İKİNCİ BÖLÜM

Yükümlülükler ve Bilgi Değişimi

Müşterinin tanınması

MADDE 3 - (1) Yükümlüler, müşterinin tanınmasına ilişkin esaslar kapsamında; kendileri nezdinde yapılan veya aracılık ettikleri işlemlerde işlem yapılmadan önce, işlem yapanlar ile nam veya hesaplarına işlem yapılanların kimliklerini tespit etmek ve gerekli diğer tedbirleri almak zorundadır.

(2) Kimlik tespitine esas belge nevilerini belirlemeye Bakanlık yetkili olup, kimlik tespitini gerektiren işlem türleri, bunların parasal sınırları ile müşterinin tanınmasına ilişkin ve konuyla ilgili diğer usûl ve esaslar yönetmelikle belirlenir.

(...)

Devamlı bilgi verme

MADDE 6 - (1) Yükümlüler taraf oldukları veya aracılık ettikleri işlemlerden, Bakanlıkça belirlenecek tutarı aşanları Başkanlığa bildirmek zorundadırlar.

(2) Devamlı bilgi verme kapsamındaki işlem türleri, bilgilerin ne şekilde ve hangi sürelerde verileceği, kapsam dışında tutulacak yükümlüler ile uygulamaya ilişkin diğer usûl ve esaslar Bakanlıkça belirlenir.

(3) Bu Kanunun uygulanmasına ilişkin olarak, yükümlüler dışındaki kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki kurum ve kuruluşlardan da Başkanlığa devamlı bilgi vermeleri istenebilir. Kimlerin, hangi usûl ve esaslara göre devamlı bilgi vereceği yönetmelikle belirlenir.

Bilgi ve belge verme

MADDE 7 - (1) Kamu kurum ve kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği olmayan kuruluşlar, Başkanlık ve denetim elemanları tarafından istenilecek her türlü bilgi, belge ve bunlara ilişkin her türlü ortamdaki kayıtları, bu kayıtlara erişimi sağlamak veya okunabilir hale getirmek için gerekli tüm bilgi ve şifreleri tam ve doğru olarak vermek ve gerekli kolaylığı sağlamakla yükümlüdür.

(2) Yukarıdaki fıkraya göre talepte bulunulanlar savunma hakkına ilişkin hükümler saklı kalmak kaydıyla, özel kanunlarda yazılı hükümleri ileri sürerek bilgi ve belge vermekten kaçınamazlar.

Muhafaza ve ibraz

MADDE 8 - (1) Yükümlüler, bu Kanunla getirilen yükümlülüklerle ve işlemlerine ilişkin her türlü ortamdaki; belgeleri düzenleme tarihinden, defter ve kayıtları son kayıt tarihinden, kimlik tespitine ilişkin belgeleri ise son işlem tarihinden itibaren sekiz yıl süreyle muhafaza ve istenmesi halinde yetkililere ibraz etmekle yükümlüdür.

(...)

Sırrın ifşası

MADDE 22 - (1) Aşağıda yazılı kimseler görevlerinden ayrılışları dahi, görevleri dolayısıyla kişilerin ve bu kişilerle ilgili kimselerin şahıslarına, muamele ve hesap durumlarına, işlerine, işletmelerine, servetlerine ve mesleklerine ilişkin olarak öğrendikleri sırları ifşa edemezler ve kendilerinin veya üçüncü şahısların yararına kullanamazlar:

a) Koordinasyon Kurulu Başkan ve üyeleri, denetim elemanları ile Kurul personeli.

b) Bilgilerine ve ihtisaslarına başvuru alan kişiler.

c) Bu bilgileri görevleri dolayısıyla öğrenen diğer kamu görevlileri.

(2) Bu kişiler, öğrendikleri sırları ifşa etmeleri halinde, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır. Bu sırlar maddi menfaat karşılığında ifşa edildiğinde verilecek hapis cezası iki yıldan az olamaz.

(3) Bu Kanun uyarınca yabancı ülkelerdeki muadil kuruluşlara Başkanlıkça bilgi verilmesi sırrın ifşası sayılmaz.

5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu

Resmî Gazete Tarihi : 16.06.2006

Resmî Gazete Sayısı : 26200

SOSYAL SİGORTALAR VE GENEL SAĞLIK SİGORTASI KANUNU

BİRİNCİ KISIM

Amaç, Kapsam ve Tanımlar

Amaç

MADDE 1- Bu Kanunun amacı, sosyal sigortalar ile genel sağlık sigortası bakımından kişileri güvence altına almak; bu sigortalardan yararlanacak kişileri ve sağlanacak hakları, bu haklardan yararlanma şartları ile finansman ve karşılama yöntemlerini belirlemek; sosyal sigortaların ve genel sağlık sigortasının işleyişi ile ilgili usûl ve esasları düzenlemektir.

Kapsam

MADDE 2- Bu Kanun; sosyal sigortalar ile genel sağlık sigortasından yararlanacak kişileri, işverenleri, sağlık hizmeti sunucularını, bu Kanunun uygulanması bakımından gerçek kişiler ile her türlü kamu ve özel hukuk tüzel kişilerini ve tüzel kişiliği olmayan diğer kurum ve kuruluşları kapsar.

(...)

Sağlık hizmeti sunucularının kayıt ve bildirim zorunluluğu ve kontrol yetkisi

MADDE 78- Kurum ile sözleşmesi olan, tüm sağlık hizmeti sunucuları, sağlık hizmeti sunduğu tüm kişilere ait sözleşme hükümlerinde yer verilen bilgileri, belirlenen yöntemlere ve süreye uygun biçimde elektronik ortamda veya yazılı olarak Kuruma göndermek zorundadır. Bu bilgiler gönderilmeksizin talep edilen sağlık hizmeti bedelleri, bilgiler gönderilinceye kadar ödenmez.

Genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişinin sağlık bilgilerinin gizliliği esastır. (İptal ikinci cümle: Anayasa Mahkemesi'nin 25/12/2014 tarihli ve E.: 2014/74, K.: 2014/201 sayılı Kararı ile.) (Ek cümle: 17/4/2008-5754/66 md.; İptal cümle: Anayasa Mahkemesi'nin 25/12/2014 tarihli ve E.: 2014/74, K.: 2014/201 sayılı Kararı ile.)

Kurum, genel sađlık sigortası h k mlerinin uygulanmasıyla ilgili olarak iřverenler, sađlık hizmeti sunucuları ve diđer gerek ve t zel kiřiler nezdindeki defter, belge ve bilgileri inceleyebilir, ibrazını isteyebilir.

Kurum, bu Kanunda belirtilen g revleriyle ilgili olarak sađlık hizmeti sunucularının y r tt đ  hizmet ve iřlemleri kontrol yetkisine sahiptir. Kurum, bu yetkisini g revlendirdiđi personeli vasıtasıyla veya kamu kurumları ve  zel kurumlardan hizmet satın almak suretiyle kullanabilir.

5502 sayılı Sosyal Güvenlik Kurumu Kanunu

Resmî Gazete Tarihi : 20.05.2006

Resmî Gazete Sayısı : 26173

SOSYAL GÜVENLİK KURUMUNA İLİŞKİN BAZI DÜZENLEMELER HAKKINDA KANUN

Kurumun taşınmaz edinimi, taşınır ve taşınmaz mal varlıkları ile gayri maddi haklarının hukuki durumu

MADDE 35- Kurum, görevlendirildiği hizmetlerin gereği ve bağışlar dışında taşınmaz edinemez.

Kurumun malları, alacakları, banka hesapları 2004 sayılı İcra ve İflâs Kanunu ile 6183 sayılı Amme Alacaklarının Tahsil Usulü Hakkında Kanun bakımından Devlet malı hükmünde olup, alacakları imtiyazlı alacaklardır.

Kurumun taşınır ve taşınmazları, bankalardaki mevduatları dahil her türlü hak ve alacakları haczedilemez, hakkında 2004 sayılı İcra ve İflâs Kanununun haciz ve iflas hükümleri uygulanmaz.

Kurum her türlü dava ve icra işlemlerinde teminat yatırmak mükellefiyetinden muaftır.

(Ek fıkra: 10/9/2014-6552/37 md.) Kurumca, işverenlerin, sigortalıların, genel sağlık sigortalılarının, emeklilerin, bunların hak sahipleri ile dul ve yetimlerinin ve Kurumdan aylık alan diğer kişilerin bireysel veri ve hakları, bireysel veri ve haklarından oluşan toplu veri ve hakları ile işletmelerin ticari sırları satılamaz ve paylaşılamaz. Kurum bunların dışında sahip olduğu gayri maddi haklarını Yönetim Kurulunun onayı ile satabilir veya paylaşabilir. Bu fıkranın aksine davrananlar hakkında Türk Ceza Kanununun ilgili hükümleri uygulanır.

(Değişik altıncı fıkra: 4/4/2015-6645/43 md.) Kurum, bu Kanun ve diğer mevzuatla verilen görevleri yerine getirmek amacıyla işlediği kişisel veriler ile ticari sır niteliğinde olan verileri, veri sahibinin noter onaylı muvafakati veya e-Devlet uygulaması üzerinden kimlik teyidi ile verilen izni olmadan gerçek veya tüzel kişilerle paylaşamaz. Ancak, 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununun eki (I), (II), (III) ve (IV) sayılı cetvellerde yer alan kamu idareleri ile Türkiye Cumhuriyet Merkez Bankasının ilgili mevzuatında belirtilen görevleri yapabilmeleri için ihtiyaç duydukları sağlık verisi dışındaki kişisel veriler ile ticari sır niteliğindeki veriler paylaşılabilir. (Ek cümle:17/7/2019-7186/18 md.) Kurum, kişisel sağlık verilerini kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, verilen sağlık hizmetlerinin

uygunluğunun ve yerindeliliğinin takibi ve finansmanının planlanması amacıyla talebi hâlinde Sağlık Bakanlığı ile paylaşır. Kurum, bunların dışındaki gayri maddi hakları ile kimliği belirli veya belirlenebilir bir gerçek veya tüzel kişiyle ilişkilendirilemeyecek şekilde anonim hâle getirdiği verileri araştırma, planlama ve istatistik gibi amaçlar için kamu idareleri, Türkiye Cumhuriyet Merkez Bankası, bilimsel araştırma yapan kamu personeli, bilimsel dernekler, kamu kurumu niteliğindeki meslek kuruluşları veya üniversiteler ile ücretsiz olarak paylaşabilir. Anonim hâle getirilen verinin tüzel kişilere ait olması hâlinde bu fıkrada sayılanlar dışındaki gerçek veya tüzel kişilere tüzel kişinin noter onaylı muvafakati alınmak kaydıyla ücretli olarak verilebilir. Veri paylaşılan kamu idareleri ile gerçek ve tüzel kişiler, paylaşılan verinin gizliliğinden ve güvenliğinden sorumludur. Bu fıkranın aksine davrananlar hakkında, veri paylaşımı yapılanlar da dâhil olmak üzere 5237 sayılı Türk Ceza Kanunu ile diğer ilgili mevzuat hükümleri uygulanır.

Kurumun sahibi bulunduğu taşınmazların kira artış oranları, 213 sayılı Vergi Usul Kanunu uyarınca her yıl belirlenen yeniden değerlendirme oranından az olmamak üzere rayiç değerle belirlenir. (Ek cümle: 17/1/2012-6270/4 md.) Ancak ekonomik koşullar göz önünde bulundurularak kira bedellerini belirlemeye Yönetim Kurulu yetkilidir.

5490 sayılı Nüfus Hizmetleri Kanunu

Resmî Gazete Tarihi : 29.04.2006

Resmî Gazete Sayısı : 26153

NÜFUS HİZMETLERİ KANUNU

BİRİNCİ KISIM

Genel Hükümler

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç

MADDE 1- (1) Bu Kanunun amacı; kişinin doğumundan ölümüne kadar kişisel ve medenî durumuna, uyrukluğuna ve bunlarda meydana gelebilecek değişikliklere ait doğal ve hukukî olayların belirlenip saptanması, bu amaçla düzenlenmiş kütüklere yazılması, elektronik ortamda ulusal adres veri tabanının oluşturulması, nüfus kayıtları ile adres bilgilerinin ilişkilendirilmesini sağlamaktır.

Kapsam

MADDE 2- (1) Bu Kanun, Türk vatandaşları, doğumla Türk vatandaşı olup da çıkma izni almak suretiyle Türk vatandaşlığını kaybedenler ve bunların altsoyları ile Türkiye'de bulunan yabancıların nüfus hizmetlerinin düzenlenmesine, yürütülmesine ve geliştirilmesine ilişkin esas ve usûl hükümlerini kapsar.

Tanımlar

MADDE 3- (1) Bu Kanunda geçen;

- Adres: Herhangi bir toprak parçası veya binanın coğrafi konumu ve işlevi açısından tanımlanmasını,
- Adres beyan formu: Adreslerin bildiriminde kullanılan, şekli ve içeriği Bakanlıkça belirlenen formu,

- c) (Değişik: 19/10/2017-7039/1 md.) Adres bileşenleri: İl, ilçe, köy ve köy başlıları, mahalle, bulvar, cadde, sokak, bina, dış kapı numarası, iç kapı numarası, posta kodu gibi adres bilgisine ulaşmak için gerekli sözel ve mekânsal verileri,
- ç) (Mülga: 19/10/2017-7039/1 md.)
- d) Aile: Aynı soydan olup, bir aile sıra numarası altında kayıtlı olan kişiler ile onların eş ve çocuklarını,
- e) Aile kütüğü: Nüfus olaylarına ilişkin kayıtların kâğıt veya elektronik ortamda tutulduğu kütüğü,
- f) Aile sıra numarası: Ailelerin aile kütüğüne yazılış sırasına göre verilen numarayı,
- g) Bakanlık: İçişleri Bakanlığını,
- ğ) Dayanak belgesi: Aile kütüğüne işlenen nüfus olaylarının dayanağı olan form, tutanak, mahkeme kararı, noter senedi, doğum veya ölüm raporu gibi resmî belgeler ile bunların yedeklerini,
- h) (Değişik: 14/1/2016-6661/8 md.) Değerli kâğıtlar: Kimlik kartını, uluslararası aile cüzdanını ve mavi kartı,
- ı) Diğer adres: Yerleşim yeri adresi dışında kalan yerleri,
- i) Genel Müdürlük: Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünü,
- j) İl müdürlüğü: İl nüfus ve vatandaşlık müdürlüğünü,
- k) (Değişik: 19/10/2017-7039/1 md.) Kimlik Paylaşımı Sistemi: Merkezi veri tabanında tutulan kayıtların kurumlar ve kamu hizmeti sunan tüzel kişiler ile paylaşıldığı sistemi,
- l) Kurum: Genel Müdürlük dışındaki diğer kamu kurum ve kuruluşlarını,
- m) (Ek: 9/5/2012-6304/11 md.) Mavi Kart: Doğumla Türk vatandaşı olup da çıkma izni almak suretiyle Türk vatandaşlığını kaybedenler ve bunların 29/5/2009 tarihli ve 5901 sayılı Türk Vatandaşlığı Kanununun 28 inci maddesinde belirtilen altsoylarına verilen ve söz konusu maddede belirtilen haklardan faydalanabileceklerini gösteren resmi belgeyi,
- n) (Ek: 9/5/2012- 6304/11 md.) Mavi Kartlılar Kütüğü: Doğumla Türk vatandaşı olup da çıkma izni almak suretiyle Türk vatandaşlığını kaybedenler ve bunların altsoylarının kayıtlarının elektronik ortamda tutulduğu kütüğü,
- o) (Değişik: 19/10/2017-7039/1 md.) Merkezî veri tabanı: Genel Müdürlükçe elektronik ortamda tutulan verileri,
- ö) (Değişik: 19/10/2017-7039/1 md.) MERNİS: Merkezî Nüfus İdaresi Sistemini,

- p) Numaralama: Mahalle, semt, meydan, bulvar, cadde, sokak ve bina gibi adres bileşenlerine isim veya numara verilmesi işlemini,
- r) (Değişik: 14/1/2016-6661/8 md.) Kimlik kartı: Kişinin Türk vatandaşı olduğunu ve aile kütüğüne kayıtlı bulunduğunu gösteren Türkiye Cumhuriyeti kimlik kartını,
- s) Nüfus hizmetleri: Nüfus olaylarına ve kişinin nüfusa ve yerleşim yeri adresine ilişkin bilgilerinin toplanmasına, nüfus kütüklerine geçirilmesine, korunmasına ve gerektiğinde tasnif edilerek değerlendirilmesine dair iş ve işlemleri,
- ş) Nüfus kaydı: Aile kütüğüne işlenmiş kişisel bilgileri,
- t) Nüfus kayıt örneği: Aile kütüğüne işlenmiş kişisel bilgilerin özetlerini gösterir belgeyi,
- u) Nüfus kütüğü: Aile kütüğü, özel kütük ve yedeklerinden oluşan kayıtların tümünü,
- ü) Nüfus müdürlüğü: İlçe nüfus müdürlüğünü,
- v) Nüfus müdürü: İlçe nüfus müdürünü,
- y) Nüfus olayı: Doğum, ölüm, evlenme, boşanma, evlât edinme, tanıma, kayıt düzeltme, soybağının düzeltilmesi, gaiplik gibi kişisel durumlarda değişiklik meydana getiren olayı,
- z) Özel kütük: Doğum, evlenme, boşanma, ölüm, kayıt düzeltme ve diğer olaylar şeklinde tutulan ve ayrı ayrı tasnif edilen dayanak belgelerinin konulduğu dosyayı,
- aa) Ulusal adres veri tabanı: Adres bilgilerinin tutulduğu merkezî veri tabanını,
- bb) Uluslararası aile cüzdanı: Bir aileyi oluşturan eş ve çocukların kimlik bilgilerini kapsayan ve uyruğunu kanıtlayan çok dilli resmî belgeyi,
- cc) (Değişik: 19/10/2017-7039/1 md.) Vekâletname: Temsil yetkisini kapsayan noterden onaylı belgeyi,
- çç) (Değişik: 19/10/2017-7039/1 md.) Yabancılar kütüğü: Kimlik numarası verilen yabancıların kayıtlarının elektronik ortamda tutulduğu kütüğü,
- dd) Yapı belgeleri: Yapı Ruhsat Formu, Yapı Kullanma İzin Belgesi, yanan ve yıkılan yapılar formunu ve binalar cetvelini,
- ee) Yerleşim yeri adresi: Sürekli kalma niyetiyle oturulan yeri,
- ff) (Ek: 14/1/2016-6661/8 md.) Biyometrik veri: Elektronik sistemler aracılığı ile kimlik tespit ve kimlik doğrulama işlemlerinin gerçekleştirilmesini sağlamak amacıyla alınan parmak izi, damar izi ve el ayasından elde edilen kişiye özgü verileri,

gg) (Ek: 19/10/2017-7039/1 md.) Veri Paylaşımı Kurulu: Merkezî veri tabanında yer alan bilgilerin paylaşımına ilişkin talepleri değerlendirmek üzere oluşturulan kurulu,

ğğ) (Ek: 19/10/2017-7039/1 md.) Yetkili idare: Adres numaralama veya yapı belgeleri düzenleme yetki ve sorumluluğu verilen idareleri,

hh) (Ek:23/7/2020-7252/8 md.) Elektronik Kimlik Doğrulama Sistemi: Türkiye Cumhuriyeti kimlik kartının elektronik kimlik doğrulama işlemlerinde kullanılabilmesini sağlayan sistemi, ifade eder.

İKİNCİ KISIM

Nüfus Hizmetlerinin Yürütülmesi

BİRİNCİ BÖLÜM

Yetkililer ve Nüfus Kütükleri

Nüfus hizmetleri yetkilileri

MADDE 4- (1) Nüfus hizmetleri, Bakanlığın merkez ve taşra teşkilâtı ile dış temsilcilikler tarafından yürütülür.

Hukukî mahiyeti

MADDE 5- (1) Nüfus kütükleri; kişilerin kimliklerinin, yerleşim yeri adreslerinin, aile bağlarının, vatandaşlık durumlarının ve şahsî hallerinin belirlenmesi amacıyla ilçe ve aile esasına göre nüfus olaylarının tescil edildiği, daimî olarak saklanması gerekli resmî belgelerdir.

(2) Aile kütüğü ve özel kütüklerde tutulan kayıtlar ile yedekleri ve bunlardan çıkarılan kayıt örnekleri aynı hukukî değere sahiptir. Kayıtlar arasında farklılık olduğu takdirde, aksi sabit oluncaya kadar kayda esas olan dayanak belgesi geçerlidir.

(3) (Ek: 19/10/2017-7039/2 md.) Bakanlık, elektronik ortamda tutulan aile kütüklerinde kişiye ait tek bir kaydın tutulmasına, kişi ve olay kayıtlarının Türkiye Cumhuriyeti kimlik numarası ile ilişkilendirilmesine yetkilidir. Bu durumda diğer kanunların bu maddeye aykırı hükümleri uygulanmaz.

Nüfus kütüklerinin tutulması

MADDE 6- (1) Nüfus olayları, iletişim ağı kullanılarak nüfus müdürlüklerindeki aile kütüklerine ve merkezî veri tabanına tescil edilir.

(2) Bakanlık, doğal afet ve olağanüstü hallere karşı kesintisiz olarak hizmet verilmesini sağlamak amacıyla, merkezî veri tabanının yedeğinin farklı bir yerde tutulmasını sağlar.

(3) Kâğıt ortamındaki aile kütüklerinin her sayfasına cilt ve sayfa sıra numaraları konur. Kütüğün sonuna kaç sayfadan ibaret olduğu yazılır. Sayfa birleşim yerleri asliye hukuk mahkemesince mühürlenerek sonu onaylanır.

(4) Nüfus kütüklerinin tutulmasına ilişkin usûl ve esasları belirlemeye, mevzuat ve sistemdeki gelişmelere bağlı olarak değiştirmeye ve kâğıt ortamında tutulan aile kütüklerini uygulamadan kaldırmaya Bakanlık yetkilidir.

Aile kütüklerinde bulunması gereken kişisel bilgiler

MADDE 7- (1) Her mahalle veya köy için ayrı aile kütüğü tutulur. Aile kütüklerinde aşağıdaki bilgiler bulunur:

a) Türkiye Cumhuriyeti kimlik numarası.

b) Kayıtlı bulunduğu il, ilçe, köy veya mahalle adı ile cilt, aile ve birey sıra numarası.

c) Kişinin adı ve soyadı, cinsiyeti, baba ve ana adı ile soyadları, evli kadınların önceki soyadları.

ç) Doğum yeri ile gün, ay ve yıl olarak doğum tarihi ve kütüğe kayıt tarihi.

d) Evlenme, boşanma, soybağının kurulması veya reddi, ölüm, vatandaşlığın kazanılması veya kaybedilmesi gibi kişisel durumda meydana gelen değişiklik veya yetkili makamlarca yapılan düzeltmeler.

e) Dini.

f) Medenî hali.

g) Yerleşim yeri adresi.

ğ) Fotoğrafı.

h) (Ek: 14/1/2016-6661/9 md.) Biyometrik verisi.

ı) (Ek: 19/10/2017-7039/3 md.) Velayete ve vesayete ilişkin bilgileri.

(Değişik son cümle: 19/10/2017-7039/3 md.) (a), (g), (ğ), (h) ve (ı) bentlerinde belirtilen kayıtlar sadece elektronik ortamda tutulur.

(2) Türkiye'de aile kütüğü bulunmayan ve yabancı ülkelerde oturan vatandaşlar Bakanlığın göstereceği bir nüfus müdürlüğünde açılacak aile kütüğüne kaydedilir.

Yabancıların kayıtlarının tutulması

MADDE 8- (Başlığı ile Birlikte Değişik:18/10/2018-7148/32 md.)

(1) 4/4/2013 tarihli ve 6458 sayılı Yabancılar ve Uluslararası Koruma Kanunu kapsamındaki yabancılara kimlik numarası vermeye, bunları yabancılar kütüğüne kaydetmeye ve herhangi bir işlem sebebiyle Türkiye’de bir kamu kurumuna veya dış temsilciliklerimize müracaat eden yabancılara, talep etmeleri hâlinde yabancı kimlik numarası (YKN) vermeye Bakanlık yetkilidir. Diplomatik misyon mensupları bu hükmün kapsamı dışındadır.

(2) Yabancı kimlik numarasının geçerlilik süresi, başvuru esnasında ve sonrasında istenilecek belgeler ile diğer hususlar İçişleri Bakanlığınca çıkarılacak yönetmelikle belirlenir.

Mavi Kartlıların kayıtları

MADDE 8/A- (Ek: 9/5/2012-6304/12 md.)

(1) Doğumla Türk vatandaşı olup da çıkma izni almak suretiyle Türk vatandaşlığını kaybedenler ve bunların 5901 sayılı Kanununun 28 inci maddesinde belirtilen altsoyları, Genel Müdürlükçe elektronik ortamda tutulan Mavi Kartlılar Kütüğüne kaydedilir. Bu Kütüğe kaydedilenler, her türlü nüfus olaylarını yurt içinde nüfus müdürlüklerine, yurt dışında ise dış temsilciliklere beyan etmekle yükümlüdürler.

İKİNCİ BÖLÜM

Nüfus Kayıtlarının Özellikleri

Gizlilik

MADDE 9- (1) Nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Bunlar, yetkili ve sorumlu memurlar ile teftiş ve denetim yetkisi olanlar dışında kimse tarafından görülüp incelenemez. Mahkemeler bu hükmün dışındadır.

(2) Nüfus kayıtlarına bu bilgileri işleyen memurlar ve Kimlik Paylaşımı Sistemi kapsamında nüfus kayıtlarından faydalanan diğer görevliler de bu gizliliğe uymak zorundadırlar. Bu yükümlülük, kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam eder.

Resmî işlemlerde esas alınması

MADDE 10- (1) Kurumlarda kişiyle ilgili olarak yapılan işlemlerde nüfus kayıtları esas alınır. Kayıtlar arasında farklılık olması halinde nüfus kayıtlarında değişiklik yapılmaz, usûlüne göre diğer kayıtlar düzeltilir.

ÜÇÜNCÜ BÖLÜM

Nüfus Kütüklerinin Tutulmasına İlişkin Esaslar

Tescil mecburiyeti

MADDE 11- (1) Türkiye Cumhuriyeti vatandaşı olan her kişi yurt içinde nüfus müdürlüğüne, yurt dışında dış temsilciliğe müracaatla kendisini nüfus kütüklerine yazdırmaya ve kimlik kartı almaya mecburdur. Ergin olmayanların nüfus olaylarını yazdırıp kimlik kartlarını almaya veli, vasi veya kayyımları, bunların bulunmaması halinde, çocukları yanlarında bulunduranlar ile 24/5/1983 tarihli ve 2828 sayılı Sosyal Hizmetler ve Çocuk Esirgeme Kurumu Kanununun yetkili kıldığı kuruluş yetkilileri görevlidirler.

(2) Türk vatandaşlığını sonradan kazanmış olanlar da vatandaşlığı kazandıkları tarihten itibaren nüfus kütüğüne geçirilir.

Tescilde dayanak belgesi zorunluluğu

MADDE 12- (1) Nüfus kütüklerine düşülen kişisel durumla ilgili her kayıt ve açıklamanın bu Kanuna göre yetkili kılınmış görevlilerce, usûlüne ve örneğine uygun olarak düzenlenmiş belgelere dayandırılması zorunludur.

(2) Nüfus olaylarını tescil eden memurlar tarafından her işlem sonunda dayanak belgeleri aile kütüklerine işlendikten sonra imzalanır ve bir nüshası arşivlenmek üzere Genel Müdürlüğe gönderilecek olan ilgili özel kütüğe konulur.

Tescil

MADDE 13- (1) Yetkili kişi ve kuruluşlarca bildirilen nüfus olaylarına ilişkin belge ve tutanaklar bu Kanun hükümlerine göre tescil edilir. Bakanlık her türlü nüfus işlemlerinde elektronik imza kullanılmasına karar vermeye yetkilidir.

Kaydın kapatılması ve yeniden açılması

MADDE 14- (1) Nüfus kaydının kapatılması; ölüm, gaiplik, Türk vatandaşlığının kaybı, evlenme, boşanma, evlât edinilme, soybağının düzeltilmesi veya reddi gibi olaylar nedeniyle bir kaydın üzerinde işlem yapılamaz hale getirilmesidir.

(2) Kaydın kapatılmasına ilişkin sebep ortadan kalktığında veya kaydın yeniden açılmasını gerektirecek yeni bir sebep ortaya çıktığında kayıt yeniden açılır. Kaydın açılmasından sonra kişisel durumda meydana gelmiş olan olaylar kişinin kaydına işlenir.

ÜÇÜNCÜ KISIM

Nüfus Olayları

BİRİNCİ BÖLÜM

Doğum

Bildirim yükümlülüğü ve süresi

MADDE 15- (Değişik: 19/10/2017-7039/5 md.)

(1) Sağ olarak dünyaya gelen her çocuğun, doğumdan itibaren Türkiye’de otuz gün içinde nüfus müdürlüğüne, yurt dışında ise altmış gün içinde dış temsilciliğe bildirilmesi zorunludur. Doğum bildirimleri, doğumu gerçekleştiren sağlık kuruluşlarına da yapılabilir.

(2) Sağlık kuruluşları ve sağlık kuruluşları dışında sağlık personeli nezaretinde gerçekleşen doğumlar, ilgili sağlık birimince bulunulan yer nüfus müdürlüğüne beş iş günü içinde bildirilir. Bildirimde, doğumun sağlık kuruluşunda veya sağlık personeli nezaretinde olduğunu ispatlayan rapor veya resmi belge ve doğum tescil isteğini belirten form dilekçe yer alır.

(3) Sağlık personeli nezaretinde gerçekleşmeyen doğum bildirimini; gebelik sırasında anneyi takip eden tabip ya da sağlık mesleği mensubunca düzenlenecek rapor veya belge ile yapılır.

(4) Sağlık personelinin takibi dışında doğan çocukların doğum bildirimini nüfus müdürlüklerine sözlü beyanla yapılır. Her sözlü beyanda mülki idare amirinin emri ile aile hekimlerince beyanların doğruluğunun araştırılması zorunludur.

(5) Doğum bildirimini; veli, vasi, kayyım, bunların bulunmaması hâlinde çocuğun büyük ana, büyük baba veya ergin kardeşleri ya da çocuğu yanında bulunduranlar tarafından yapılır. Çocuğa konulan ad, üç adı geçmemek üzere ve kısaltma yapılmadan yazılır. Doğum ve gebelik raporu ile doğumun bildirilmesi ve doğum tutanağının düzenlenmesine ilişkin usul ve esaslar Sağlık Bakanlığının görüşü alınarak Bakanlıkça belirlenir.

(6) Yurt dışındaki doğum bildirimleri, yabancı makamlardan alınmış resmî belge veya raporun dış temsilciliğe verilmesi ile yapılır. Doğum bildiriminin dış temsilciliğe bizzat yapılamaması hâlinde, yabancı makamlardan alınmış resmî belge veya rapor ile çocuğa konulan adın belirtildiği dilekçe, ana ve babanın kimlik bilgilerini gösteren belgelerle birlikte dış temsilciliğe gönderilmesi suretiyle de yapılabilir.

(7) Ölü doğan çocuklar aile kütüğüne yazılmaz. Bir doğumda birden fazla çocuk doğması hâlinde bunlar, doğuş sırasıyla yazılır.

Süresi içinde bildirilmeyen doğumlar

MADDE 16- (1) Bu Kanununun 15 inci maddesinde belirtilen süreyi geçirdikten sonra bildirilen altı yaşını bitirmemiş olan çocukların doğum tarihinin tespitinde beyan esas alınır. Çocuk altı yaşını doldurmuş ise nüfus müdürlüğüne getirilerek resmî sağlık kuruluşunca yaşının tespit edilmesi sağlanır. Doğuma ait resmî belge ibraz edilmesi halinde, yaş tespitine gerek kalmaz.

Nüfus müdürlüklerinin yetkisi

MADDE 17- (1) Nüfus müdürlükleri; süresi içerisinde bildirilmemiş çocukların veya nüfusa tescil edilmemiş erginlerin varlığını haber aldıkları takdirde; erginlerin kendilerini, çocukların veli, vasi veya kayyımlarını, bunların bulunmaması halinde; büyük ana, büyük baba veya kardeşlerini ya da çocukları yanlarında bulunduranları veya muhtarları beyana davet etmeye yetkilidirler. İlgililer de bu davet üzerine otuz gün içinde nüfus müdürlüklerine başvurmak ve beyanda bulunmakla görevlidir.

(2) Verilen süre içerisinde bildirim yapılmaması halinde mülkî idare amirinin göreceği lüzum üzerine kolluk kuvvetlerince bunların zorla getirilmesi için gereken işlem yapılarak çocuğun aile kütüklerine tescili sağlanır.

Bildirimle yükümlü diğer görevliler

MADDE 18- (1) 2828 sayılı Kanununun yetkili kıldığı kuruluş yetkilileri, yetiştirme yurtları, bakım evleri ve benzeri yerlerin sorumluları ile kişiler; yanlarında çalıştırdıkları veya barındırdıkları çocuk veya erginlerin kimlik kartlarını kontrol etmek, aile kütüklerine kayıtlı olmayanların tescillerini sağlamak için nüfus müdürlüklerine beyanda bulunmak ve gerekli işlemleri yaptırmakla görevlidirler.

(2) Kolluk görevlileri; kimlik kontrolleri veya herhangi bir işlem nedeniyle kimliğini ispat edemeyenlerle, nüfusta kayıtlı olmadığını tespit ettikleri kişileri, haklarında gerekli işlemleri yaptıktan sonra düzenleyecekleri evrakı o yerdeki nüfus müdürlüğüne bildirmekle yükümlüdürler.

(3) Okul müdürleri; okula kayıt için başvuran çocuklardan nüfusa kayıtlı olmayanların beyana dayalı kimlikleri ile baba, ana, vasi veya kayyımlarının kimliklerini ve adreslerini o yerin nüfus müdürlüğüne bildirmekle görevlidirler.

(4) Kamu veya özel kurumlar iş verecekleri kişilerden kimlik kartı istemekle, nüfusta kayıtlı olmadıklarını anladıkları kişilerin beyana dayalı kimlik ve adreslerini nüfus müdürlüklerine bildirmekle yükümlüdürler.

Bulunmuş çocuklar ve zihinsel engelli kişiler

MADDE 19- (1) Yaşının küçüklüğü nedeniyle kendisini ifade edemeyen bulunmuş çocukların nüfus kütüklerine kaydedilmesi, kolluk görevlileri veya ilgili kurumların bu durumu belirten tutanaklarına veya ilgililerin beyanlarına dayanılarak buldukları yerin nüfus müdürlüğüne yapılır.

(2) Zihinsel engelli olup da bulunmuş onsekiz yaşından büyük kişileri, mahkemece tayin edilecek olan kayyımları bildirmekle yükümlüdür. Bildirimin tam teşekküllü devlet hastahanesinden alınacak sağlık kurulu raporu ile nüfus müdürlüğüne yapılması zorunludur.

(3) Bu kişiler hakkında düzenlenen tutanaklarda doğum tarihi, adı ve soyadı ile ana ve baba adı belirtilmemiş ise; nüfus müdürlüğüne ad ve soyad ile ana ve baba adı verilir. Doğum tarihi belirlenmemişse resmî sağlık kuruluşunca tespit edilmesi sağlanır.

Türk vatandaşlığını kazananlar

MADDE 20- (1) Kanun gereğince Türk vatandaşlığını kazananlar yetkili makam veya kurulların kararı üzerine düzenlenecek formlara uygun olarak aile kütüğüne tescil edilirler.

Yabancıların nüfus olayları

MADDE 21- (Mülga: 19/10/2017-7039/27 md.)

İKİNCİ BÖLÜM

Evlenme

Evlendirme yetkisi

MADDE 22- (1) Bakanlık, evlendirme işlemlerinin nüfus ve vatandaşlık hizmetlerinin bütünlüğü içerisinde yürütülmesi için gereken her türlü tedbiri alır ve uygular.

(2) Evlendirme memuru; belediye bulunan yerlerde belediye başkanı veya bu işle görevlendireceği memur, köylerde muhtardır. Bakanlık, il nüfus ve vatandaşlık müdürlüklerine, nüfus müdürlüklerine ve dış temsilciliklere, il ve ilçe müftülüklerine evlendirme memurluğu yetkisi ve görevi verebilir. Eşlerden birinin yabancı olması halinde evlendirmeye, (...) belediye evlendirme memurlukları ile nüfus müdürleri yetkilidir.

Evlenmenin bildirilmesi ve tescili

MADDE 23- (1) 22 nci madde uyarınca evlendirme işlemi yapanlar; evlenmenin yapıldığı tarihten itibaren on gün içinde düzenlenecek evlenme bildirimini nüfus müdürlüğüne göndermekle, nüfus müdürlüğü de tescil etmekle yükümlüdür.

(2) Evlenen kadının kaydı kocasının hanesine taşınır. Kocasını ölen kadın yeniden evlenmedikçe ölen kocasının aile kütüğünde kalır. Ancak dilerse babasının kütüğüne dönebilir.

(3) Dış temsilciliklerce yapılan evlenmeler, evlenmenin yapıldığı tarihten itibaren otuz gün içinde nüfus müdürlüklerine bildirilir.

(4) Mülga 743 sayılı Türk Kanunu Medenisinin yürürlüğe girdiği 4/10/1926 tarihinden önce eski hükümlere göre yapıp da halen nüfus kütüklerine tescil edilmemiş olan evlenmeler ilgililerin mahkemen karar almaları suretiyle aile kütüğüne tescil edilir.

Yurt dışında yapılan evlendirmeler

MADDE 24- (1) Yurt dışında yabancı yetkili makamlar önünde Türk vatandaşlarının yaptığı evlenmeler, 22/11/2001 tarihli ve 4721 sayılı Türk Medenî Kanunu hükümlerine uygun olmak ve butlanla batıl olmayı gerektiren bir sebep bulunmamak kaydıyla geçerlidir. Bu evliliklerin koca, kocanın yabancı olması halinde kadın tarafından en geç otuz gün içerisinde evlenmeyi yapan yabancı makamdan alınmış belgenin o yerdeki dış temsilciliğe verilmesi veya dış temsilciliğe gönderilmesi suretiyle yapılır. Beyanı alan dış temsilcilik evlenme bildirimini usûlüne göre düzenleyerek nüfus müdürlüklerine göndermekle yükümlüdür.

(2) O yerde dış temsilcilik bulunmadığı veya dış temsilciliğe bildirimde bulunulmadığı takdirde, evlenme bildirimi; yabancı makamlardan alınan evlenme belgesinin Türkçeye çevrilip usûlüne göre onaylanmış ve Dışişleri Bakanlığınca tasdik edilmiş olması şartıyla yurt içinde nüfus müdürlüğüne verilmek suretiyle de yapılabilir. Bu belgeye dayanılarak düzenlenecek evlenme bildirimi ile kütüğe tescil işlemi yapılır.

Evlenmekle Türk vatandaşlığını kazananların tescili

MADDE 25- (1) Evlenmekle Türk vatandaşlığını kazanan kadın, kocasının hanesine tescil edilir. Bu şekilde aile kütüklerine tescil edilen kadının ölüm dışında evliliğinin sona ermesi halinde kaydı, kayıtlı bulunduğu kütüğün sonuna taşınır.

(2) Evlenmekle Türk vatandaşlığını kazanan erkek karısının evlenmekle kaydının taşındığı haneye tescil edilir. Evliliğin ölüm dışında sona ermesi halinde kadının kaydı evlenmeden önce kayıtlı bulunduğu haneye taşınır, erkeğin kaydı ise kayıtlı bulunduğu hanede kalır.

ÜÇÜNCÜ BÖLÜM

Boşanma ve Evliliğin İptali

Kadının bekleme süresinin başlangıcı

MADDE 26- (1) Kadının bekleme süresi, mahkeme kararının kesinleştiği tarihten itibaren hüküm ifade eder.

Boşanma veya evliliğin iptali kararlarında bulunması gerekli hususlar

MADDE 27- (1) Boşanma veya evliliğin iptaline ilişkin kararlarda aşağıdaki bilgilere yer verilmesi zorunludur:

- a) Tarafların Türkiye Cumhuriyeti kimlik numarası, adı, soyadı, doğum yeri ve tarihi, baba ve ana adları ile kadının evlenmeden önceki soyadı ve aile kütüğünde kayıtlı olduğu yer bilgileri.
- b) Evlilik içinde doğmuş çocuklar ve bunların kimlik bilgileri.
- c) Karara ait usûl mevzuatının öngördüğü diğer esas ve usûle ait hükümler.

Yabancı ülke adlî veya idarî makamlarınca verilen boşanma kararlarının nüfus kütüğüne tescili

MADDE 27/A - (Ek: 17/4/2017-KHK-690/4 md.; Aynen kabul: 1/2/2018-7077/3 md.)

(1) Yabancı ülke adlî veya idarî makamlarınca boşanmaya, evliliğin butlanına, iptaline veya mevcut olup olmadığının tespitine ilişkin olarak verilen kararlar; bizzat veya vekilleri aracılığıyla tarafların birlikte veya taraflardan birinin ölmüş ya da yabancı olması halinde Türk vatandaşı olan diğer taraf veya vekilinin tek başına başvurması, verildiği devlet kanunlarına göre konusunda yetkili adlî veya idarî makam tarafından verilmiş ve usulen kesinleşmiş olması ve Türk kamu düzenine açıkça aykırı bulunmaması şartlarıyla nüfus kütüğüne tescil edilir.

(2) Nüfus kütüğüne yapılacak tescil işlemleri, yurt dışında kararın verildiği ülkedeki dış temsilcilikler, yurt içinde ise Bakanlık tarafından belirlenen nüfus müdürlükleri tarafından yapılır.

(3) Bu maddede sayılan şartlar yerine getirilmediği gerekçesiyle tescil talebi reddedilen kararların Türkiye’de tanınması, 27/11/2007 tarihli ve 5718 sayılı Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun uyarınca yapılır.

(4) Bu maddenin uygulanmasına ilişkin usul ve esaslar Bakanlık tarafından yönetmelikle belirlenir.

DÖRDÜNCÜ BÖLÜM

Tanıma ve Evlât Edinme

Tanıma ve babalığa hüküm

MADDE 28- (1) Tanıma; babanın yazılı başvurusu üzerine mahkemede yapılmışsa mahkeme tarafından, notere başvurusu üzerine düzenlenen senetle yapılmışsa noter tarafından tanımanın yapıldığı tarihten itibaren on gün içinde nüfus müdürlüğüne bildirilir.

(2) Tanınanın babanın vasiyetnamesindeki beyanla yapılması durumunda nüfus müdürlüğüne bildirim, vasiyetnameyi açan hâkim tarafından yapılır.

(3) Nüfus memuruna yapılan tanıma beyanı ise doğrudan aile kütüklerine tescil edilir.

(4) (Değişik: 19/10/2017-7039/7 md.) Tanınan veya babalığa hüküm kararı ile soybağı kurulan çocuklar babalarının hanesine baba adı ve soyadı ile nakledilir.

(5) Yurt dışında yapılan tanıma işlemlerine ait bildirimler dış temsilciliklere veya Türkçeye tercüme edilip, onaylanmış olmak kaydıyla yurt içinde nüfus müdürlüklerine yapılabilir.

Evlât edinme işlemi

MADDE 29- (1) Evlât edinme kararı mahkeme tarafından on gün içinde o yerin nüfus müdürlüğüne bildirilir. Evlât edinme olayı aile kütüklerine tescil edilir ve evlât edinilenin kaydı evlât edinenin aile kütüğüne taşınır.

Yurt dışında yapılan evlât edinme işlemleri

MADDE 30- (1) Yurt dışında yabancı yetkili makamlar önünde yapılan evlât edinme işlemleri aslı şartlar bakımından Türk mevzuatına uygun olmak şartıyla Türkiye'de de geçerlidir.

(2) Evlât edinme olaylarına ilişkin yabancı adlî veya idarî makamlarca verilen ve o ülkenin hukukuna göre kesinleşmiş olan veya kesin hüküm gibi sonuç doğuran karar ve belgelerin Türkiye'de icra olunabilmesi, yetkili Türk mahkemesi tarafından tenfiz veya tanıma kararı verilmesine bağlıdır.

BEŞİNCİ BÖLÜM

Ölüm ve Gaiplik

Bildirim süresi ve yükümlü olanlar

MADDE 31- (1) Ölüm olayını;

a) Şehir ve kasabalarda 24/4/1930 tarihli ve 1593 sayılı Umumi Hıfzıssıhha Kanunu gereğince defin ruhsatı vermeye yetkili olanlar,

b) Köylerde, varsa resmî tabip veya sağlık kuruluşu yetkilileri, yoksa köy muhtarları,

c) Hastane ve bakım evi gibi sağlık kurumlarında kurum amirlikleri,

ç) Askeri birliklerde tabipler veya iç hizmet mevzuatına göre kıta komutanlıklarınca görevlendirilmiş olanlar ve askerlik şubeleri,

d) Doğal afetlerde mülkî idare amirlerince görevlendirilecek memurlar,

e) Adli olaylarda ve kazalarda ilgili Cumhuriyet savcılıkları,

olayın meydana geldiği tarihten itibaren, dış temsilcilikler ise olaydan haberdar oldukları tarihten itibaren on gün içerisinde Genel Müdürlüğe ya da nüfus müdürlüğüne bildirmekle yükümlüdürler.

(2) Kanunî süre geçtikten sonra nüfus müdürlüklerine gelen ölümlere ait tutanaklar resmî sağlık kurumları kayıtlarına veya diğer resmî belgelere dayanılarak düzenlenmiş ise nüfus müdürlüklerince kabul edilip işleme alınır.

(3) Yurt içinde meydana gelen ölümlerde, ölüm nerede meydana gelmişse o yerin nüfus müdürlüğüne, ölüm yerinin tespit edilememesi halinde ceset nerede bulunmuşsa o yerin, ölüm bir taşıt içinde olmuşsa bu taşıttan çıkarıldığı yerin nüfus müdürlüğüne bildirilir.

(4) Ölenin kaydı yok ise yapılacak soruşturma sonunda Türk vatandaşlığı ve ailesi tespit edildiği takdirde doğum tutanağı düzenlenerek aile kütüğüne önce doğum, sonra ölüm olayı işlenir.

Ölüm karinesi

MADDE 32- (1) Bir kimse ölümüne kesin gözle bakılmayı gerektiren durumlar içinde kaybolursa, cesedi bulunamamış olsa bile müracaat edilen yerin mülkî idare amirinin emri ile ölüm tutanağı düzenlenerek ölüm olayı işlenir.

(2) Bu madde uyarınca işlem yapılabilmesi için ölüm karinesi bulunan kişinin alt veya üst soyundan bir kişinin ya da kardeşlerinin, bunlar yoksa mirasçılarının dilekçe ile başvurarak olayı belgelendirmeleri ya da yetkili makamların durumu resmî bir yazı ile nüfus müdürlüğüne bildirmeleri gereklidir.

(3) Dilekçeye ekli belgeler ve gerektiğinde nüfus müdürlüğüne yaptırılacak soruşturma olayın doğruluğunu ve öldüğü iddia edilen kişinin de olayın meydana geldiği sırada orada bulunduğunu kanıtlamaya yeterli görülürse mülkî idare amirinin emri ile ölüm kaydı düşülür.

Ölü olduğu halde aile kütüklerinde sağ görünenler

MADDE 33- (1) Ölmüş olduğu halde aile kütüklerinde sağ görülenlere ait ölüm tutanakları, ölüm olayını gösterir belge ile başvurulması halinde nüfus müdürlüklerince düzenlenir ve gerekli işlem yapılır. Herhangi bir belge ibraz edilememesi durumunda ölüm beyanının doğruluğu nüfus müdürlüklerince tahkik ettirildikten sonra düzenlenecek ölüm tutanağı, mülkî idare amirinin emri ile işleme konulur.

(2) (Ek: 19/10/2017-7039/8 md.) Merkezî veri tabanında yer alan kayıtlara göre uzun süre işlem görmeyen ve yaşı itibarıyla ölü olması muhtemel kişiler Genel Müdürlükçe tespit edilir. Tespit edilen

kayıtların araştırılması mülkî idare amirinin emriyle kolluk kuvvetlerine yaptırılır. Araştırma sonucu ölü oldukları tespit edilenlerin ölümleri tescil edilir.

Gaiplik işlemi

MADDE 34- (1) Gaiplik kararları mahkemelerce on gün içinde o yerin nüfus müdürlüğüne bildirilir ve nüfus memurlarınca aile kütüklerine tescil edilir.

DÖRDÜNCÜ KISIM

Kayıt Düzeltmeleri

BİRİNCİ BÖLÜM

Nüfus Kaydının Düzeltilmesine İlişkin Esaslar

Kayıt düzeltilmesi

MADDE 35- (1) Kesinleşmiş mahkeme hükmü olmadıkça nüfus kütüklerinin hiçbir kaydı düzeltilemez ve kayıtların anlamını ve taşıdığı bilgileri değiştirecek şerhler konulamaz. Ancak olayların aile kütüklerine tescili esnasında yapılan maddî hatalar nüfus müdürlüğüne dayanak belgesine uygun olarak düzeltilir.

(2) Aile kütüklerindeki din bilgisine ilişkin talepler, kişinin yazılı beyanına uygun olarak tescil edilir, değiştirilir, boş bırakılır veya silinir.

Nüfus davaları

MADDE 36- (1) Mahkeme kararı ile yapılan kayıt düzeltmelerinde aşağıdaki usûllere uyulur:

a) Nüfus kayıtlarına ilişkin düzeltme davaları, düzeltmeyi isteyen şahıslar ile ilgili resmî dairenin göstereceği lüzum üzerine Cumhuriyet savcılar tarafından yerleşim yeri adresinin bulunduğu yerdeki görevli asliye hukuk mahkemesinde açılır. Kayıt düzeltme davaları (..) nüfus müdürü veya görevlendireceği nüfus memuru huzuru ile görülür ve karara bağlanır.

b) (Değişik: 19/10/2017-7039/9 md.) Haklı sebeplerin bulunması hâlinde aynı konuya ilişkin düzeltme yapılması hâkimden istenebilir. Ad değişikliği hâlinde, nüfus müdürlüğü bu kişinin çocuklarının baba veya ana adına ilişkin kaydı, soyadı değişikliğinde ise eşin ve ergin olmayan çocukların soyadını da düzeltir.

c) Tespit davaları, kaydın iptali veya düzeltilmesi için açılacak davalara karine teşkil eder.

(2) Kişilerin başkasına ait kaydı kullandıklarına ilişkin başvurular Bakanlıkça incelenip sonuçlandırılır.

Nüfus müdürlüklerinin yetkisi

MADDE 37- (1) Genel Müdürlük ve nüfus müdürlükleri, mahkemece verilen kararlar hakkında her türlü kanun yoluna başvurmaya yetkilidir.

(2) Genel Müdürlük ve nüfus müdürlükleri kanunî harç ve her türlü mahkeme masraflarından muaftır.

İKİNCİ BÖLÜM

Maddî Hatalar ve Nüfus Kaydının İptali

Maddî hatalar

MADDE 38- (1) Bu Kanunun 7 nci maddesinde sayılan aile kütüklerine tescil edilmesi gereken bilgilerden; dayanak belgesinde bulunduğu halde nüfus kütüklerine hatalı veya eksik olarak tescil edilen ya da hiç yazılmayan bilgiler veya mükerrer kayıtlar maddî hata kapsamında değerlendirilir. Bu tür maddî hatalar Genel Müdürlükçe ya da nüfus müdürlükleri tarafından düzeltilir veya tamamlanır.

Tarihlerde düzeltme ve tamamlama yetkisi

MADDE 39- (1) Genel Müdürlük, nüfus kayıtlarına göre vatandaşların hicrî veya rumî tarihle yazılmış nüfus olaylarının tarihlerini miladî yıla çevirerek aile kütüklerine geçirmeye, doğum tarihlerinin ay ve günü belli olmayanların da eksikliklerini tamamlamaya yetkilidir.

(2) Doğum tarihlerinde doğum yılı yazılıp, doğum ayı ve günü yazılmamış olanların yaşlarının hesaplanmasında doğduğu yılın Temmuz ayının birinci günü, ayı yazılıp da günü belli olmayanlar için de o ayın birinci günü başlangıç olarak alınır.

Nüfus kaydının iptali

MADDE 40- (1) Usûlüne göre düzenlenmemiş bir belgeye dayanılarak tesis edilmiş nüfus kayıtları Genel Müdürlüğün ya da nüfus müdürlüklerinin göstereceği lüzum üzerine mahkemece verilecek kararla iptal edilir. Nüfus kütüğüne düşülmüş olan şerh ve açıklamaların iptal edilmesi de aynı usûle tâbidir.

BEŞİNCİ KISIM

Kimlik Kartı, Uluslararası Aile Cüzdanı ve Mavi Kart

Düzenlenmesi ve dağıtılması

MADDE 41- (Değişik: 14/1/2016-6661/12 md.)

- (1) Kimlik kartında yer alacak bilgiler ile kartın tasarımı, temini, basımı, dağıtım ve teslim yöntemi ile üretim ve kişiselleştirilmesinde kullanılacak sistem ile elektronik kimlik doğrulama sistemini belirlemeye Bakanlık yetkilidir.
- (2) Kimlik kartında yer alacak biyometrik verinin türü, niteliği ve alınma yaşı Bakanlıkça belirlenir.
- (3) Biyometrik verisi alınacak kişilerin şahsen müracaatı esastır. Biyometrik verisi alınmayacak çocukların kimlik kartı müracaatı veli veya vasileri ile 15 inci ve 17 nci maddelerde yer alan bildirim yükümlülüğü bulunan kişiler tarafından yapılır.
- (4) Merkezî veri tabanında tutulan biyometrik veriler kimlik doğrulama işlemleri dışında kullanılamaz.
- (5) Kişi, müracaat sırasında yazılı muvafakatı ile kimlik kartını teslim alacak kişiyi belirleyebilir.
- (6) Kimlik kartı talebinde bulunan kişi ile nüfus kütüklerinde kayıtlı kişinin aynı kişi olup olmadığı hususunda tereddüte düşülmesi hâlinde mülkî idare amirinin emri ile kolluk kuvvetlerine araştırma yaptırılır.
- (7) Kimlik kartının kaybı veya değiştirilmesi nedeniyle yapılacak müracaatlarda, yenisi verilinceye kadar geçerli olmak üzere, usul ve esasları Bakanlıkça belirlenen geçici bir belge verilebilir.
- (8) Kimlik kartına bu Kanunda öngörülenler dışında kayıt ve işaret konulamaz. Kimlik kartı hiçbir kişi veya kurum tarafından alıkonulamaz.
- (9) Evlenme işlemi tamamlandıktan sonra, çiftlere uluslararası aile cüzdanı verilir.
- (10) Uluslararası aile cüzdanı ve mavi kart Bakanlıkça belirlenen tasarım ve sayıda Maliye Bakanlığınca bastırılır. Aile cüzdanları ve mavi kartlar Maliye Bakanlığınca yurt içinde nüfus müdürlüklerine ve evlendirme memurluklarına verilmek üzere maliye yetkililerine, yurt dışında ise dış temsilciliklere verilmek üzere Dışişleri Bakanlığına gönderilir. Uluslararası aile cüzdanları ve mavi kartların en fazla üç bin adedi, bedeli sonradan ödenmek üzere, müteakiben üç bin adetlik partiler hâlinde peşin para karşılığında nüfus müdürlüğüne verilir.
- (11) Kimlik kartı, uluslararası aile cüzdanı ve mavi kart bedeli müracaat sırasında tahsil edilir. Doğum bildiriminin kanuni süresi içinde yapılması hâlinde ve 2828 sayılı Kanun kapsamında düzenlenecek kimlik kartlarından değerli kâğıt bedeli alınmaz.
- (12) Hatalı yazım nedeniyle iade edilen uluslararası aile cüzdanları ve mavi kartlar değerli kâğıt bedelinden düşülür. Hatalı üretim ya da yazım nedeniyle kimlik kartlarının değiştirilmesi hâlinde kimlik kartı bedeli alınmaz.

(13) Genel M¼d¼rl¼k, n¼fus m¼d¼rl¼kleri ile dıř temsilcilikler, kimlik kartı, uluslararası aile c¼zdanı ve mavi kart bedeli aısından 2/6/1934 tarihli ve 2489 sayılı Kefalet Kanunu h¼k¼mlerine tabi deęildir.

(14) Kimlik kartı bedellerinin Hazine veznelerine yatırılmasına iliřkin usul ve esaslar Bakanlık ve Maliye Bakanlıęınca m¼řtereken belirlenir.

(15) (Ek:23/7/2020-7252/8 md.) Elektronik Kimlik Doęrulama Sisteminin uygulanmasında; 24/3/2016 tarihli ve 6698 sayılı Kiřisel Verilerin Korunması Kanunu h¼k¼mlerine g¼re ve kiřinin aık rızası alınarak iřlem yapılır.

Talep belgesi

MADDE 42- (Deęiřik: 14/1/2016-6661/13 md.)

(1) Kimlik kartı ve uluslararası aile c¼zdanlarının verilebilmesi iin řekli ve kapsamı Bakanlıka belirlenen ve bastırılan talep belgeleri kullanılır. Doęum tutanaklarına dayanılarak kimlik kartı d¼zenlemesinde talep belgesi aranmaz.

(2) Talep belgelerini uygulamaya koymaya veya uygulamadan kaldırmaya ve bunların saklama s¼relerini belirlemeye Bakanlık yetkilidir.

ALTINCI KISIM

N¼fus Kayıtlarındaki Bilgilerin Verilmesi

N¼fus kayıt ¼rneęi verilmesi

MADDE 43- (1) Kiřinin aile k¼t¼ę¼ndeki kaydının ıkarılması ve aslına uygunluęunun n¼fus m¼d¼rl¼ę¼nce onanması ile elde edilen n¼fus kayıt ¼rneklere, aksi ispat edilene kadar geerlidir. N¼fus kayıt ¼rneęi, istenme nedeni ve hangi amala kullanılacaęının belirtildięi yazılı istek olmadan verilemez. Ancak kiřinin kimlięini kanıtlayan resm¼ bir belge ile řahsen bařvurması halinde yazılı m¼racaat aranmaz. N¼fus kayıt ¼rneklere, bunları istemeye yetkili olanlar tarafından aıka ve gerekeli olarak istenmedięi takdirde, kimlik bilgileri dıřında kiřisel bilgilere yer verilmez. Bu belgeler ¼zerinde silinti ve kazıntı yapılamaz.

(2) D¼zenlendikleri tarihten itibaren y¼zseksen g¼n iinde kullanılmayan n¼fus kayıt ¼rneklere geerlilięini kaybeder. N¼fus kayıt ¼rneęinin kullanılacaęı alanlara g¼re Bakanlık bu s¼reyi otuz g¼ne kadar kısaltmaya yetkilidir.

N¼fus kayıt ¼rneęini almaya yetkili olanlar

MADDE 44- (1) N¼fus kayıt ¼rneklere;

- a) Bakanlık,
 - b) Dış temsilcilikler,
 - c) Asker alma işlemleri için Milli Savunma Bakanlığı,
 - ç) Adlî makamlar,
 - d) Adlî işlemlerle sınırlı olmak üzere kolluk kuruluşları,
 - e) Evlenme işlemleri için evlendirme işlemi yapmaya yetkili olanlar,
 - f) Ölüm işlemleri için resmî sağlık kuruluşları,
 - g) Kaydın sahipleri veya bunların eşleri ile veli, vasi, alt ve üst soyları ya da bu kişilere ait vekâletnameyi ibraz edenler,
- nüfus müdürlüklerinden doğrudan almaya yetkilidirler.

(2) Birinci fıkrada sayılanlar dışında kalan kurumlar ve tüzel kişiler, yazılı olarak başvurmak ve istem nedenini açıkça belirtmek suretiyle Bakanlık veya mülkî idare amirinin emri ile nüfus kayıt örneğini alabilirler. Bakanlık bu madde hükümlerini işletmek üzere Kimlik Paylaşımı Sistemi kurar.

(3) Yerleşim yeri adresi ve diğer adres bilgilerinin verilmesi kişinin rızasına bağlıdır.

(4) Birinci fıkranın (g) bendinde sayılan kişiler dışında kalan üçüncü şahıslar medenî hal bilgisi dışında bir kişinin nüfus kaydına ilişkin örnek veya bilgi alamazlar.

(5) (Ek: 19/10/2017-7039/10 md.) Kişiler; kendileri ve alt ya da üst soylarına ait nüfus kayıt örneklerini, kendileri ve ergin olmayan çocuklarının ise yerleşim yeri belgelerini, güvenli kimlik doğrulama araçlarını kullanarak e-Devlet kapısı üzerinden sorgulayabilir, sonucu fiziki veya elektronik ortamda merciine verebilirler. E-Devlet kapısı üzerinden alınan belgeler, nüfus müdürlüklerinden alınmış diğer belgelerle aynı hukuki değere sahiptir.

Kimlik Paylaşımı Sisteminin kullanılması

MADDE 45- (Değişik: 19/10/2017-7039/11 md.)

(1) Bakanlık, merkezî veri tabanında tutulan verileri bu Kanunda belirtilen usul ve esaslar çerçevesinde kurumlarla; kimlik verilerini, kamu hizmeti sunan tüzel kişilikler, 3/6/2007 tarihli ve 5684 sayılı Sigortacılık Kanunu çerçevesinde faaliyette bulunan sigorta ve emeklilik şirketleri, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu çerçevesinde faaliyette bulunan bankalar, Risk Merkezi ve 5411 sayılı Kanununun 73 üncü maddesinin son fıkrası uyarınca bilgi paylaşımı amacıyla kurulmuş şirketler, 21/11/2012 tarihli ve 6361 sayılı Finansal Kiralama, Faktoring ve Finansman

Şirketleri Kanunu kapsamındaki finansal kiralama şirketleri, finansman şirketleri ile tasarruf finansman şirketleri, 6/12/2012 tarihli ve 6362 sayılı Sermaye Piyasası Kanunu kapsamındaki aracı kurumlar ve portföy yönetim şirketleri, 20/6/2013 tarihli ve 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun kapsamındaki ödeme hizmeti sağlayıcıları; yerleşim yeri ve diğer adres bilgilerini ise Bakanlıkça belirlenen adrese dayalı kamu hizmeti sunan kuruluşlar, 5684 sayılı Kanun çerçevesinde faaliyette bulunan sigorta ve emeklilik şirketleri, 5411 sayılı Kanun çerçevesinde faaliyette bulunan bankalar, Risk Merkezi ve 5411 sayılı Kanununun 73 üncü maddesinin son fıkrası uyarınca bilgi paylaşımı amacıyla kurulmuş şirketler, 6361 sayılı Finansal Kiralama, Faktoring ve Finansman Şirketleri Kanunu kapsamındaki finansal kiralama şirketleri, finansman şirketleri ve tasarruf finansman şirketleri, 6362 sayılı Kanun kapsamındaki aracı kurumlar ve portföy yönetim şirketleri, 6493 sayılı Kanun kapsamındaki ödeme hizmeti sağlayıcıları ile paylaşabilir.

(2) Veri paylaşımından yararlanacakları belirlemeye, paylaşımın kapsamına ve hangi yöntemle yapılacağına karar vermek üzere Genel Müdürlük bünyesinde Veri Paylaşımı Kurulu oluşturulur. Veri Paylaşımı Kurulunun çalışma usul ve esasları Bakanlıkça çıkarılan yönetmelikle belirlenir.

(3) Birinci fıkrada belirtilenler kendi iş ve işlemlerine esas olmak üzere sadece ilgili kişilerin bilgilerini alabilirler ve aldıkları bilgileri tanımlanmış hizmetlerin yerine getirilmesi dışında başka hiçbir amaçla kullanamaz; ilgilisi veya 44 üncü maddede belirtilenler dışında kimseye veremez. Sistemin bütün aşamalarında görev yapan yetkililer de bu kurallara uymakla yükümlüdür. Bu yükümlülük, kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam eder. (Ek cümle:18/6/2020-7247/8 md.) Birinci fıkrada belirtilenler, Kimlik Paylaşımı Sistemi kullanıcılarının, sistemi bu madde hükümlerine uygun kullanmalarına yönelik gerekli her türlü idari ve teknik tedbirleri almak, takip etmek ve idari ve teknik tedbirlere ilişkin raporları talep edildiğinde Bakanlığa bildirmekle yükümlüdür. Bu fıkra hükümlerine aykırı davranışlar hakkında 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu hükümlerine göre işlem yapılır.

(4) Birinci fıkrada belirtilenler Kimlik Paylaşımı Sisteminden alabilecekleri verileri çevrimdışı olarak talep edemezler. Ancak kamusal hizmetin planlanması ve yürütülmesinde zorunlu bir ihtiyaç olduğunun tespit edilmesi, kullanım amacı ve yasal dayanağının belirtilmesi hâlinde ihtiyaç ile orantılı olarak veri talepleri asgari düzeyde çevrimdışı karşılanabilir.

(5) Genel Müdürlük, kişisel verilerin hukuka aykırı olarak işlenmesini, erişilmesini önlemek ve muhafazasını sağlamak amacıyla uygun güvenlik tedbirlerini alır ve veri talebinde bulunan kurum ve kamu hizmeti sunan tüzel kişilerin de bu tedbirleri almasını takip eder ve denetler.

(6) Genel Müdürlükten alınan bilgilerin iş ve işlemlerde kullanılmasının hukukî sonuçları bilgiyi alan kurum ve tüzel kişiliğin sorumluluğundadır.

(7) Kimlik Paylaşımı Sistemi üzerinden nüfus kayıt örneği, yerleşim yeri belgesi ve kimlik kartı örneğine erişebilen kurum ve tüzel kişiler bu belgeleri ilgisinden ve nüfus müdürlüğünden talep etmeksizin Kimlik Paylaşımı Sisteminden temin ederler.

(8) Bu Kanun ile kurulan veri tabanlarının istatistik amaçlı kullanımında 10/11/2005 tarihli ve 5429 sayılı Türkiye İstatistik Kanunu hükümleri uygulanır.

YEDİNCİ KISIM

Türkiye Cumhuriyeti Kimlik Numarası

Kimlik numarası

MADDE 46- (1) Kimlik numarası, Türkiye Cumhuriyeti vatandaşlarının nüfus kayıtları arasında bağ kurmak, kişilerin kaydına ulaşmak ve kamu kuruluşlarında tutulan kayıtlar arasında ilişki sağlamak amacını taşıyan bir numara sistemidir. Türkiye Cumhuriyeti kimlik numarası kişiye bir defa verilir ve değiştirilemez.

(2) (Mülga: 19/10/2017-7039/27 md.)

Kullanımı

MADDE 47- (1) Kişiler adına düzenlenecek olan her türlü form, beyanname, kimlik kartı, vergi kimlik kartı, sürücü belgesi, pasaport gibi bütün tanıtıcı belgelerde Türkiye Cumhuriyeti kimlik numarasına yer verilir.

(2) Türkiye Cumhuriyeti kimlik numarası kurumlar ile diğer gerçek ve tüzel kişilerin her türlü işlem ve kayıtlarında esas alınır.

(3) Kimlik numarasının uygulanmasında ortaya çıkan sorunlar ile tereddüt edilen hususlarda Genel Müdürlüğün görüşü alınır.

SEKİZİNCİ KISIM

Adres Kayıt Sistemi

Adres bilgilerinin tutulması ve adres standardı

MADDE 48- (1) Yerleşim yeri adresi ve diğer adreslere ait bilgilerin tutulmasına ilişkin politikanın oluşturulması, geliştirilmesi, yaygınlaştırılması, idarî birimlere göre genel uygulamaya geçiş tarihlerinin tespit edilmesi, ulusal adres veri tabanı ile MERNİS veri tabanının ilişkilendirilmesi ve

adres bilgilerinin paylaşılmasına ilişkin işlemler Bakanlıkça yürütülür. Bakanlığın nüfus kütüklerindeki adres kayıtlarını tamamlamak maksadıyla işbirliği talebi kurumlarca karşılanır.

(2) Adres standardı, Mahallî İdareler Genel Müdürlüğünün takip ve sorumluluğunda; Genel Müdürlük, Türkiye İstatistik Kurumu, Türk Standartları Enstitüsü ve ilgili diğer kuruluşlarca ortaklaşa belirlenir. Mahallî İdareler Genel Müdürlüğü tespit edilen standardın yetkili idareye bildirilmesinden sorumludur. Kurumlar ile gerçek ve tüzel kişiler adres ile ilgili iş ve işlemlerinde adres standardına uymak zorundadır.

(3) Bakanlık, adrese ilişkin her türlü bilgiyi kurumlardan istemeye yetkilidir. Kurumlar söz konusu isteğe yirmi gün içinde cevap vermekle yükümlüdür.

(4) (Değişik: 19/10/2017-7039/12 md.) Faydalanılan kamu hizmetleriyle sınırlı olmak üzere adrese dayalı olarak yürütülen iş ve işlemlerde diğer adres, yerleşim yeri adresi ile aynı hukuki değere sahiptir. Kurumlar yürütecekleri iş ve işlemlerde yerleşim yeri adresi gibi diğer adres bilgilerini de esas alır.”

(5) (Ek: 19/10/2017-7039/12 md.) 11/2/1959 tarihli ve 7201 sayılı Tebligat Kanunu hükümleri saklıdır.

Adres bilgisi ve güncellenmesi

MADDE 49- (1) İl özel idaresi ve belediyeler sorumluluk alanlarındaki adres bileşenlerini adres standardına uygun olarak tanımlayıp bunlara değiştirilemeyecek sabit tanıtım numarası vererek mahallindeki bütün adresleri kapsayacak şekilde adres bilgilerini oluşturmakla yükümlüdür. Herhangi bir sebeple sabit tanıtım numarası dışında adres bileşenlerinde yapılan değişiklikler de il özel idaresi ve belediyelerce takip edilerek ulusal adres veri tabanına işlenir.

(2) Ulusal adres veri tabanı Genel Müdürlükte tutulur. Genel Müdürlük, ulusal adres veri tabanındaki yerleşim yeri adresi bilgilerini nüfus kütüklerindeki kişi kayıtları ile ilişkilendirerek elektronik ortamda, yedekleme sistemleri ile birlikte güncel olarak tutar.

(3) (Mülga: 9/5/2012-6304/13 md.; Yeniden düzenleme: 2/1/2017 - KHK-680/80 md.; Aynen kabul: 1/2/2018-7072/78 md.) Yerleşim yeri adresi yurt dışında olan Türk vatandaşlarının adres kayıtları, yaşadıkları ülkede kullanılan adres verilerine veya o ülke ve bağlı olduğu temsilcilik bilgisine göre tutulur.

Bildirim yükümlülüğü ve süresi (1)

MADDE 50- (Değişik: 19/10/2017-7039/13 md.)

- (1) Adres bildiriminde kişilerin yazılı beyanı esas alınır. Bildirim şahsen veya güvenli elektronik imza ile yapılır.
- (2) Adres bildirimi, nüfus müdürlüklerine veya dış temsilciliklere yapılır. Hizmet alımı ile ilgili başvuru sırasında, Bakanlıkça belirlenen adrese dayalı hizmet sunan kuruluşlara da adres değişikliğine ilişkin beyanda bulunulabilir.
- (3) Adres bildiriminin, yirmi işgünü içinde yapılması zorunludur.
- (4) Yerleşim yeri ve diğer adresi aynı olan ailenin ergin fertleri birbirlerinin yerine adres beyanında bulunabilirler. Vekâletname ibraz edenler de kişilerin adresleri ile ilgili bildirimde bulunabilirler.
- (5) Çocukların ve kısıtlıların adresleri veli, vasi, kayyım, bunların bulunmaması hâlinde, çocuğun büyük ana, büyük baba, ergin olan kardeşleri veya çocuğu yanında bulunduranlar tarafından bildirilir.
- (6) Huzurevi, yetiştirme yurdu, cezaevi, öğrenci yurdu gibi yerlerde kalanların adres bildirimleri ilgili kurum yetkililerince, bildirim yapamayacak durumda olan kimsesizlerin ise muhtarlar tarafından yapılır.
- (7) Beyanda şüphe duyulması hâlinde kişinin beyanını teyit eden bilgi ve belgeler istenebilir.
- (8) Yetkili idareler adres oluşumuna dayanak teşkil eden yapı belgelerini, belgelerin oluşturulması ile eş zamanlı olarak ulusal adres veri tabanına işlemekle yükümlüdür.

Adrese dayalı hizmet sunan kuruluşların yükümlülüğü (2)

MADDE 51- (Değişik: 19/10/2017-7039/14 md.)

- (1) Kuruluşlarca, adres değişikliği beyan formları elektronik ortamda Genel Müdürlüğe veya kâğıt ortamında en geç on işgünü içinde kuruluşun bulunduğu yerin nüfus müdürlüğüne gönderilir.

Adres bilgilerinin kullanımı

MADDE 52- (1) Bakanlık, talepleri halinde kurumlara, usûl ve esasları Bakanlıkça tespit edilmek üzere adres bilgilerini elektronik ortamda Kimlik Paylaşımı Sistemi çerçevesinde verebilir.

- (2) Teknik altyapısını tamamlamış olan muhtarlıklar sorumluluk alanlarındaki yerleşim yeri adres bilgilerinin güncelliğini takip etmek amacıyla Kimlik Paylaşımı Sistemine erişebilirler.

- (3) Kurumlar, yürütecekleri iş ve işlemlerde Genel Müdürlükte tutulan adres bilgilerini esas alırlar.

(4) Adrese ilişkin bilgi ve belgeler nüfus müdürlüklerinden, Kimlik Paylaşımı Sistemine bağlanarak bu sistemdeki kayıtlara uygun belge üretebilen muhtarlıklardan temin edilebilir. Bu şekilde üretilen belgelerin güvenliği Bakanlığın tespit ettiği usûl ve esaslara göre sağlanır.

(5) Nüfus sayımında veya tespitinde, aile ve hayatî istatistiklerin oluşturulmasında ve bu bilgileri esas alan kanunların uygulanmasında MERNİS nüfus bilgileri kullanılır.

Koordinasyon ve işbirliği

MADDE 53- (1) Genel Müdürlük, ulusal adres veri tabanının etkin, süratli ve güncel bir şekilde oluşturulmasını sağlamak ve devam ettirmek için kurumlar arası koordinasyonla sorumludur. Kurumlar, adrese ve adres bileşenlerine ilişkin ellerindeki bilgileri Genel Müdürlükle ve ilgili kurumlarla paylaşmakla yükümlüdür.

DOKUZUNCU KISIM

Ortak Hükümler

Tescil görevi ve süre

MADDE 54- (1) Nüfus olaylarını tescil etmekle görevli memurlar, nüfus müdürlüğünde düzenlenen ve aile kütüklerine tescil edilmesi gereken dayanak belgelerini işlem anında, diğer makamlarca düzenlenen dayanak belgelerini ise nüfus müdürlüğüne intikal ettiği tarihten itibaren yedi gün içinde aile kütüklerine tescil etmekle ve bir örneğini Genel Müdürlüğe göndermekle yükümlüdürler.

Mahkeme yazı işleri müdürlerinin görevleri

MADDE 55- (1) Mahkeme yazı işleri müdürleri, aile kütükleri üzerinde tescil yapılmasını gerektirecek bütün karar ve işlemleri, kesinleştirme işlemi veya düzenleme tarihinden itibaren on gün içerisinde o yerin nüfus müdürlüğüne bildirmekle görevlidirler.

Sağlık kuruluşlarının görevleri

MADDE 56- (Mülga: 19/10/2017-7039/27 md.)

Vekiller

MADDE 57- (Değişik: 19/10/2017-7039/17 md.)

(1) Nüfus idarelerindeki işlemlere esas olmak üzere üçüncü kişilerin beyanda bulunabilmeleri ancak vekâletname ibrazı ile mümkündür.

Yazım dışı kalanlar

MADDE 58- (1) Nüfus yazımlarında kayıt dışı kalanlar Türkiye'de buldukları yerin nüfus müdürlüğüne, yurt dışında ise en yakın dış temsilciliğe Türk vatandaşı olduklarını gösterir resmî belgeler ile müracaat ederler. Yapılacak inceleme sonucunda tescillerine engel bir halin bulunmaması halinde, nüfus müdürlüklerince aile kütüklerine tescil edilirler.

(2) (Ek: 19/10/2017-7039/18 md.) Nüfus yazımlarından önce ölenler aile kütüklerine tescil edilmez. Ancak, yersel yazımdan önce ölen kişiye ait kimlik ile ölüme ilişkin belge ibrazı hâlinde kişinin kanunî mirasçılarının kaydına açıklama yapılır.

Tutanakların imzalanması

MADDE 59- (1) Nüfus müdürlüklerine yapılan bildirimler üzerine düzenlenen dayanak belgeleri, nüfus müdürlüğüne imzalanarak onaylanır. Dayanak belgelerinin ilgilinin kendisi veya veli, vasi ya da vekâletname ibraz edenler tarafından imzalanması gereklidir. Okuma yazması olmayanların parmak izi alınır.

Beyanda şüphe

MADDE 60- (1) Nüfus olayları ve adres ile ilgili beyanlarda şüpheye düşülmesi halinde mülkî idare amirinin emri ile kolluk makamları tarafından gerekli soruşturma ve incelemeler yapılarak nüfus müdürlüğüne bildirilir.

Sürelerin hesaplanması

MADDE 61- (1) Bu Kanunda belirtilen sürelerin hesaplanmasında olayın meydana geldiği tarihi izleyen gün başlangıç olarak alınır. Süreler; tayin edilen müddetin son günü, son gün resmî tatile rastlarsa tatili izleyen ilk iş günü çalışma saatinin bitiminde sona erer.

Atık veya eski aile kütükleri

MADDE 62- (1) İşlemden kaldırılmış olan atık veya eski aile kütükleri üzerinde herhangi bir işlem yapılamaz, kayıt düşülemez.

(2) (Değişik: 19/10/2017-7039/21 md.) Atık defter kayıtlarına dayanılarak idarece düzeltme yapılamaz. Bu defterlerden çıkartılan kayıtlara "Kişinin kimliği ve aile bağlarının mahkemelerce tespit edilmesi amacı dışında herhangi bir hukukî işleme esas alınamaz." açıklaması yapılır.

(3) (Değişik: 19/10/2017-7039/21 md.) Nüfus olaylarına ait dayanak belgelerinin bulunamaması hâlinde kişinin adı, soyadı, baba adı, ana adı, doğum tarihi veya doğum yerine ilişkin maddi hataların düzeltilmesi ya da eksikliklerin tamamlanması, işlemde kaldırılmış eski aile kütüklerine istinaden

yapılır. Bu defterlerden çıkartılan kayıtlara ise “İşbu kayıtlar güncel kayıtların yerine esas alınamaz.” açıklaması yapılır.

Askerlik çağına girenlerin listesi

MADDE 63- (Değişik: 19/10/2017-7039/22 md.)

(1) Aile kütüklerinde kayıtlı olanlardan askerlik çağına giren erkek nüfusun listesi Millî Savunma Bakanlığınca Kimlik Paylaşımı Sistemi üzerinden alınır.

Formların düzenlenmesi

MADDE 64- (1) Bu Kanunun uygulanmasında kullanılacak olan form ve belgeleri hazırlamaya ve gerekli düzenlemeleri yapmaya Bakanlık yetkilidir. Elektronik ortamda tutulan yerleşim yeri adresinin bildirimine ilişkin beyan formları taranarak elektronik ortama aktarıldıktan sonra imha edilir.

ONUNCU KISIM

Çeşitli Hükümler

Katılma payı

MADDE 65- (Değişik: 25/6/2009-5917/39 md.)

(1) (Değişik: 19/10/2017-7039/23 md.) Kimlik Paylaşımı Sisteminde yer alan bilgilerin genel yönetim kapsamındaki kamu idareleri dışındaki kamu kurum ve kuruluşları ve tüzel kişilerle paylaşılması karşılığında sorgu veya dönen kayıt başına katılma payı alınır. Katılma payının miktarı, Kimlik Paylaşımı Sisteminden sunulan servisin niteliği dikkate alınarak 3 kuruştan az olmamak üzere Bakanlık ve Maliye Bakanlığınca müştereken mekânsal ve metinsel veriler için ayrı ayrı belirlenir. Bu miktarlar her yıl, bir önceki yıla ilişkin olarak 4/1/1961 tarihli ve 213 sayılı Vergi Usul Kanununun mükerrer 298 inci maddesi hükümleri uyarınca tespit ve ilan edilen yeniden değerlendirme oranında artırılır. Sorgu ve dönen kayıt sayısının belirlenmesinde Bakanlık kayıtları esas alınır.

(2) Katılma payları, takvim yılının üçer aylık dönemleri itibarıyla her bir dönemde yapılan sorgulamalar üzerinden hesaplanır. Hesaplanan katılma payları, dönemi takip eden ayın 15 inci günü akşamına kadar sorgulama yapan kurumlara bildirilir ve bildirim yapıldığı ayın sonuna kadar Bakanlık merkez muhasebe birimine ödenir.

(3) Süresinde ödeme yapmayanların sistemle bağlantısı kesilir. Süresinde ödenmeyen katılma payları 6183 sayılı Amme Alacaklarının Tahsil Usulü Hakkında Kanun hükümlerine göre vergi dairelerince takip ve tahsil edilir. Katılma payları genel bütçeye gelir kaydedilir.

(4) Köy ve mahalle muhtarlıkları katılma payından muaftır.

(5) Bu maddenin uygulamasına ilişkin usul ve esaslar Bakanlık ile Maliye Bakanlığınca müştereken belirlenir.

Fazla çalışma ücreti

MADDE 66- (Mülga: 11/10/2011-KHK-666/1 md.)

ONBİRİNCİ KISIM

Ceza Hükümleri

Gerçek dışı beyan

MADDE 67- (1) Gerçeğe aykırı yerleşim yeri veya cüzdan talep belgesi veren köy veya mahalle muhtarları ile herhangi bir işlem sebebiyle nüfus müdürlüğüne gerçek dışı beyanda bulunanlar ve bunlara tanıklık edenler altı aydan dört yıla kadar hapis cezası ile cezalandırılır.

(2) Adrese ilişkin yükümlülükleri yerine getirmeyen ve yasalara aykırı hareket eden kamu görevlileri 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun kamu idaresinin güvenilirliğine ve işleyişine karşı suçlara ilişkin hükümlerine göre cezalandırılır.

İdarî para cezaları

MADDE 68- (1) Bu Kanuna göre;

a) Nüfus olaylarını bildirmekle görevli olup, bu görevlerini bu Kanunda belirtilen süreler içinde yerine getirmeyen kamu görevlilerine, fiil başka bir suç oluştursa bile, nüfus memurunun teklifi üzerine o yerin ilçe nüfus müdürünün kararı ile 25 YTL idarî para cezası verilir.

b) (Mülga: 19/10/2017-7039/24 md.)

c) (Değişik: 14/1/2016-6661/14 md.) Adres değişikliğini bildirme yükümlülüğünü süresi içinde yerine getirmeyenlere 50 Türk lirası, gerçeğe aykırı beyanda bulunanlara 1000 Türk lirası idarî para cezası, yurt içinde mülkî idare amirlerince, yurt dışında ise dış temsilciliklerce verilir.

(2) Yurt dışında verilen idarî para cezaları, işlem sırasında mahallî para karşılığı verildiği ülkede konsolosluk hasılatının tahsil edildiği para birimi üzerinden tahsil edilir.

(3) Bu Kanuna göre;

a) (Mülga: 14/1/2016-6661/14 md.)

b) (Mülga: 14/1/2016-6661/14 md.)

c) (Mülga: 14/1/2016-6661/14 md.)

d) (Değişik: 19/10/2017-7039/24 md.) Bu Kanununun 15 inci maddesinde belirtilen sağlık personeline ve 31 inci maddesinde belirtilen Cumhuriyet savcılıklarına,

bu maddede belirtilen idarî para cezaları uygulanmaz.

ONİKİNCİ KISIM

Çeşitli Hükümler

Yönetmelik

MADDE 69- (1) Bu Kanunun uygulanmasına ilişkin yönetmelikler Cumhurbaşkanınca yürürlüğe konulur.

(2) Adres ve numaralamaya ilişkin yönetmelik ise doksan gün içerisinde Bakanlık, Türkiye İstatistik Kurumu ve Türk Standartları Enstitüsü Kurumu tarafından müştereken hazırlanarak yürürlüğe konulur.

Kadrolar

MADDE 70- (1) Bu Kanuna ekli (1) sayılı listede yer alan kadrolar bu Kanun kapsamındaki hizmetlerde kullanılmak üzere ihdas edilerek 190 sayılı Genel Kadro ve Usulü Hakkında Kanun Hükmünde Kararnamenin eki (I) sayılı cetvelin İçişleri Bakanlığı bölümüne eklenmiştir.

Kaldırılan hükümler

MADDE 71- (1) 5/5/1972 tarihli ve 1587 sayılı Nüfus Kanunu, 24/2/1972 tarihli ve 1543 sayılı Genel Nüfus Yazımı Kanunu ve 5/7/1939 tarihli ve 3686 sayılı Evlenme Kâğıtları ve Bunların Nüfus Kütüklerine Tescilleri Hakkında Kanun, 26/6/1973 tarihli ve 1774 sayılı Kimlik Bildirme Kanununun 5 inci maddesi, 6 ncı maddesinin (a) ve (d) bentleri, 8 inci maddesi, 16 ncı maddesi ve 17 nci maddesinde yer alan "8" ibaresi ile 10/4/1927 tarihli ve 1003 sayılı Binaların Numaralanması ve Sokaklara İsim Verilmesi Hakkında Kanun yürürlükten kaldırılmıştır.

Diğer kanunların değiştirilen hükümleri

MADDE 72- (1) 1774 sayılı Kanununun 6 ncı maddesinin (c) bendinden sonra gelmek üzere "tarafından örneğine uygun kimlik belgesi doldurularak üç gün içinde genel kolluk örgütüne verilmesi zorunludur." ibaresi eklenmiş ve aynı maddenin ikinci fıkrasında yer alan "olanlar ile (d) bendinde belirtilen yerlerde kalanların" ibaresi "olanların" şeklinde değiştirilmiştir.

Diğer kanunlara eklenen hükümler

MADDE 73- (1) (14/2/1985 tarihli ve 3152 sayılı İçişleri Bakanlığı Teşkilat ve Görevleri Hakkında Kanun ile ilgili olup yerine işlenmiştir.)

Atıflar

EK MADDE 1- (Ek: 14/1/2016-6661/15 md.)

(1) Diğer mevzuatta “nüfus cüzdanı”, “hüviyet cüzdanı”, “nüfus hüviyet cüzdanı”, “hüviyet varakası”, “nüfus kâğıdı” ibarelerine yapılan atıflar “Türkiye Cumhuriyeti kimlik kartı”na yapılmış sayılır.

Tescil yetkisi ve görevlendirme

EK MADDE 2- (Ek: 19/10/2017-7039/25 md.)

(1) Bakanlık, nüfus olayları ve adrese ilişkin dayanak belgesi düzenleyen kurumlara veya dış temsilciliklere bu belgeleri elektronik ortamda gönderme ya da tescil yetkisi verebilir. Dayanak belgelerinin tescil yetkisi verilen kurumlarda muhafaza edilmesine karar vermeye Bakanlık yetkilidir.

(2) Dışişleri Bakanlığının talebi hâlinde, büyükelçiliklerin konsolosluk şubeleri ile başkonsolosluklarda nüfus ve vatandaşlık işlemlerini gerçekleştirmek amacıyla nüfus personeli görevlendirilebilir. Söz konusu memurların yurt dışındaki görev ve sorumlulukları ile görev süreleri Bakanlık ve Dışişleri Bakanlığınca müştereken belirlenir.

Soyadı değişikliği

EK MADDE 3- (Ek: 19/10/2017-7039/25 md.)

(1) Yazılı talepte bulunmak kaydıyla;

a) Boşandığı eşinin soyadını kullanmasına izin verilen kadının evlenmeden önceki soyadını,

b) Eşinin soyadı ile birlikte önceki soyadını taşıyan kadının sadece eşinin soyadını,

kullanmak istemesi hâlinde, nüfus müdürlüğünce gerekli işlem yapılır.

Ölüm olayının tespiti

EK MADDE 4- (Ek: 19/10/2017-7039/25 md.)

(1) Ölüm olayları, nüfus müdürlüğünce kurum ve noterlere kâğıt ortamında bildirilmez. Kurum ve noterler ölüm olaylarının tespitini elektronik ortamda yapar. Mücbir sebeplerle ölüm olaylarına ilişkin bilgilerin elektronik ortamda gönderilememesi hâllerinde kâğıt ortamında gönderilebilir.

(2) 18/1/1972 tarihli ve 1512 sayılı Noterlik Kanununun 69 uncu maddesinin ve 213 sayılı Kanunun 150 nci maddesinin bu Kanuna aykırı hükümleri uygulanmaz.

ONÜÇÜNCÜ KISIM

Geçici Hükümler

GEÇİCİ MADDE 1- (1) Kurumlar ve tüzel kişiler bu Kanunun yayımı tarihinden itibaren iki yıl içinde mevzuatlarını bu Kanun hükümlerine uygun hale getirerek işlemlerinde kimlik numarasını kullanmak zorundadırlar.

GEÇİCİ MADDE 2- (1) Bu Kanunun yayımı tarihinden itibaren adres bilgilerinin kaydedilmesine ilişkin uygulamaya hazırlık olarak sırasıyla aşağıdaki iş ve işlemler yapılır:

a) Ulusal adres veri tabanının altyapı çalışmaları Türkiye İstatistik Kurumu Başkanlığı bünyesinde yapılarak veri tabanı kurulur ve bu maddede öngörülen iş ve işlemlerin tamamlanmasından sonra Genel Müdürlüğe devredilir.

b) Mahallî İdareler Genel Müdürlüğü, adres ve numaralamaya ilişkin yönetmeliğe uygun olarak il özel idareleri ve belediyelerin numaralama ve levhalama çalışmalarını takip eder.

c) Adres çalışmaları ile eş zamanlı olarak il özel idareleri ve belediyeler ile Genel Müdürlük, ulusal adres veri tabanlarının teknik altyapısını oluşturur. Ulaştırma Bakanlığı tarafından ülke genelinde il özel idareleri ve belediyeler ile ulusal adres veri tabanı arasında on-line işleyecek bir ağ altyapısı oluşturulur. Her yerleşim biriminin ulusal adres veri tabanına ulaşabileceği bir merkezî bilgisayar programı Türkiye İstatistik Kurumu Başkanlığınca hazırlanır. Gerekli şifreleme ve kullanıcı eğitimi verilerek il özel idareleri ve belediyelerin kullanımına açılır.

ç) Adres standardının belirlendiği tarihten itibaren en geç üçyüzaltmış gün içerisinde il özel idare ve belediyeler tarafından yerleşim birimlerinin adres bileşenleri standartlara uygun hale getirilerek numaralama işlemi tamamlanır ve merkezî olarak kurulan ulusal adres veri tabanına (c) bendinde bahsedilen program aracılığı ile işlenir.

d) İl özel idareleri ve belediyelerce gerçekleştirilen numaralama ve levhalama çalışmalarının uygunluğunun yerinde tespit edilmesi amacıyla Türkiye İstatistik Kurumu Başkanlığı ve Mahallî İdareler Genel Müdürlüğü tarafından numaralama işlemi tamamlandıktan sonra doksan gün içerisinde alan kontrolü yapılır. Kontrol sonuçları ulusal adres veri tabanına işlenir.

e) Ulusal adres veri tabanındaki yerleşim yeri adreslerinin nüfus kütüklerindeki kişi kayıtları ile ilişkilendirilmesi ve Türkiye Cumhuriyeti kimlik numarasına bağlı kişisel yerleşim yeri adresi

kayıtlarının tutulabilmesi için, numaralaması tamamlanan yerleşim yerlerinden başlamak ve bu Kanunun yürürlüğe girdiği tarihten itibaren en geç altıyüzotuz gün içerisinde tamamlanmak üzere Türkiye İstatistik Kurumu Başkanlığı tarafından alan uygulaması yapılır. Uygulama esnasında ulusal adres veri tabanına dayalı olarak alanda tespit edilen yerleşim yeri adres bilgileri, MERNİS kayıtları ile Türkiye Cumhuriyeti kimlik numarası esasına göre elektronik ortamda eşleştirilir. Alan taraması sırasında Türkiye'de yerleşim yeri adresi tespit edilen yabancılar ile ilgili ayrı bir veri tabanı oluşturulur.

f) Elde edilen kayıtlar, mahalle ve köy muhtarlıklarında altmış gün süreyle askıya çıkartılır. Askı süresince, itirazlar üzerine yapılacak inceleme sonucunda Türkiye İstatistik Kurumu Başkanlığı tarafından temin edilen bilgilere göre kayıtlarda gerekli düzeltmeler yapılır. Bu çalışma ile kayıtların kesinleşmesi sonucunda alan uygulamasında kullanılan formlar 28/9/1988 tarihli ve 3473 sayılı Muhafazasına Lüzum Kalmayan Evrak ve Malzemenin Yok Edilmesi Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabulü Hakkında Kanun hükümlerine göre mahallî kurulların kararı ile yerinde imha edilir.

(2) İşlemler sırasında kullanılacak formlar Genel Müdürlük ile işbirliği halinde Türkiye İstatistik Kurumu Başkanlığı tarafından hazırlanır. Türkiye İstatistik Kurumu Başkanlığı tarafından formlara istatistik amaçlı olarak eklenen sorulara ilişkin kayıtlar Türkiye İstatistik Kanunu hükümleri çerçevesinde değerlendirilir.

(3) Türkiye İstatistik Kurumu Başkanlığının bu madde kapsamında yapacağı alan çalışması, 5429 sayılı Kanunun sayım ve araştırmalarla ilgili hükümleri çerçevesinde yürütülür. Bu maddede belirtilen iş ve işlemlerin yapılması için ilgili kurumlar mal ve hizmet satın alabilir. Bu madde kapsamında yaptırılacak işler hakkında, ceza ve ihalelerden yasaklama hükümleri hariç 4/1/2002 tarihli ve 4734 sayılı Kamu İhale Kanunu ile 5018 sayılı Kanun hükümleri uygulanmaz. Bu kapsamda yapılacak mal ve hizmet alımlarının usûl ve esasları, saydamlık, rekabet, eşit muamele, güvenilirlik, kamuoyu denetimi, ihtiyaçların uygun şartlarla ve zamanında karşılanması ve kaynakların verimli kullanılmasını sağlayacak ilkeler doğrultusunda hizmetin gereklerine göre Bakanlar Kurulunca belirlenir.

(4) Bu maddenin birinci fıkrasının (a) bendinin uygulanmasına ilişkin usûl ve esaslar yönetmelikle belirlenir.

GEÇİCİ MADDE 3- (1) Bu Kanunun geçici 2 nci maddesinin uygulama süresi içinde nüfus olaylarını nüfus mevzuatında öngörülen süreyi geçirdikten sonra bildirenler ile nüfus ve aile cüzdanını kaybedenlere bu Kanunun 68 inci maddesi hükmü uygulanmaz.

GEÇİCİ MADDE 4- (1) Bu Kanunda öngörülen süre içerisinde ulusal adres veri tabanına bağlanamayan il özel idareleri ve belediyeler, mahallî adres bilgilerini tespit edip güncelliğini takip ederler ve ulusal adres veri tabanına işlenmek üzere elektronik ortamda ilçe nüfus müdürlüklerine gönderirler.

GEÇİCİ MADDE 5- (1) Bu Kanun yürürlüğe girinceye kadar tanıma beyanı veya babalığa hüküm kararı sonucu ana hanesine tescil edilen çocukların baba hanelerine nakline ana ve babanın birinin, çocuk ergin ise kendisinin müracaatı aranır.

GEÇİCİ MADDE 6- (Ek: 14/1/2016-6661/16 md.)

(1) Nüfus cüzdanlarının düzenlenmesi ve dağıtılması 31/12/2016 tarihine kadar aşağıdaki usul ve esaslara göre yapılır:

a) Nüfus cüzdanları, Bakanlıkça tespit edilen şekil, ebat ve örneğe uygun olarak Maliye Bakanlığınca bastırılır ve nüfus müdürlüklerinin ihtiyaçlarını karşılamak üzere muhasebe yetkililerine, dış temsilciliklerin ihtiyaçlarını karşılamak üzere Dışişleri Bakanlığına gönderilir.

b) Muhasebe yetkilisince nüfus müdürlüklerinin ihtiyacı göz önünde tutularak, kadın ve erkek nüfus cüzdanlarının her biri için en fazla üçer bin adedi, bedeli sonradan ödenmek üzere, müteakiben üçer bin adetlik partiler hâlinde peşin para karşılığında verilir. Doğum bildirimlerinin kanuni süresi içinde yapılması hâlinde düzenlenecek nüfus cüzdanlarından değerli kâğıt bedeli alınmaz. Hatalı yazım nedeniyle iade edilen nüfus cüzdanları değerli kâğıt bedelinden düşülür.

c) Nüfus cüzdanı, yurt içinde ilçe nüfus müdürlüklerince ve yurt dışında dış temsilciliklerce kişilerin kendilerine, ergin olmayanların veli, vasi veya resmî vekillik belgesi ibraz edenler ile bu Kanunun 17 nci maddesinde belirtilen, beyanla yükümlü kişilere Bakanlıkça tespit edilecek usûller çerçevesinde verilir.

ç) Genel Müdürlük ile başkonsolosluklar, nüfus cüzdanı bedeli açısından 2489 sayılı Kanun hükümlerine tabi değildir.

Katılma payı

GEÇİCİ MADDE 7- (Ek: 19/10/2017-7039/26 md.)

(1) 65 inci maddenin birinci fıkrası uyarınca katılma payı Bakanlık ve Maliye Bakanlığınca müştereken belirleninceye kadar 65 inci maddenin bu maddeyi ihdas eden Kanunla değiştirilmeden önceki hükümlerinin uygulanmasına devam olunur.

Ad ve soyadı düzeltilmesi

GEÇİCİ MADDE 8- (Ek: 19/10/2017-7039/26 md.)

(1) Kişinin iki yıl içerisinde yerleşim yerinin bulunduğu nüfus müdürlüğüne yazılı olarak başvurması kaydıyla; 21/6/1934 tarihli ve 2525 sayılı Soyadı Kanununun 3 üncü maddesine aykırı soyadları ile yazım ve imla hatası veya düzeltme işareti kullanılmamasından kaynaklanan anlam değişiklikleri bulunan ad ve soyadları, mahkeme kararı aranmaksızın, il veya ilçe idare kurulunun vereceği kararla bir defaya mahsus olmak üzere değiştirilebilir. İl ve ilçe idare kurullarının vereceği karar kesindir. Soyadı değiştirilen erkek ise kendisi ile birlikte varsa karısının ve müracaat tarihinde ergin olmayan çocuklarının da soyadları düzeltilir. Soyadı değiştirilen kadın ise kendisi ile birlikte ergin olmayan evlilik dışı çocukları varsa onların da soyadları düzeltilir.

Göçmenlerin doğum yeri ve tarihinin düzeltilmesi

GEÇİCİ MADDE 9- (Ek: 19/10/2017-7039/26 md.)

(1) Göçmen olarak Türk vatandaşlığına alınanlardan doğum yeri ve tarihi hatalı olan kişilerin kayıtları, bu maddenin yürürlüğe girdiği tarihten itibaren beş yıl içinde usulüne göre onaylanmış doğum belgeleri ile müracaatları hâlinde, nüfus müdürlüğüne düzeltilir.

Evlat edinilen çocuğun ana ve baba adı

GEÇİCİ MADDE 10- (Ek: 19/10/2017-7039/26 md.)

(1) Bu maddenin yürürlüğe girdiği tarihten önce birlikte veya tek başına evlat edinilen çocuk veya erginlerin bu maddenin yürürlüğünü izleyen beş yıl içinde nüfus müdürlüklerine başvurmaları hâlinde nüfus kaydında ana ve/veya baba adı ya da soyadı olarak evlat edinilenlerin ad ve soyadları yazılır.

(2) Bu maddenin yürürlüğe girdiği tarihte ergin ve mümeyyiz olan evlat edinilenlerin de muvafakatleri aranır.

GEÇİCİ MADDE 11- (Ek:6/12/2019-7196/61 md.)

(1) Kişinin üç yıl içerisinde yerleşim yerinin bulunduğu nüfus müdürlüğüne yazılı olarak başvurması kaydıyla; 21/6/1934 tarihli ve 2525 sayılı Soyadı Kanununun 3 üncü maddesine aykırı soyadları ile yazım ve imla hatası veya düzeltme işareti kullanılmamasından kaynaklanan anlam değişiklikleri bulunan, genel ahlaka uygun olmayan, toplum tarafından gülünç karşılandığı değerlendirilen ad ve soyadları, mahkeme kararı aranmaksızın, il veya ilçe idare kurulunun vereceği kararla bir defaya mahsus olmak üzere değiştirilebilir. İl ve ilçe idare kurullarının vereceği karar kesindir. Soyadı değiştirilen erkek ise kendisi ile birlikte varsa karısının ve müracaat tarihinde ergin olmayan

çocuklarının da soyadları düzeltilir. Soyadı deęiştirilen kadın ise kendisi ile birlikte ergin olmayan evlilik dıőı çocukları varsa onların da soyadları düzeltilir. Bu maddede belirlenen sürenin bir katına kadar uzatılmasında Cumhurbaşkanı yetkilidir.

Yürürlük

MADDE 74- (1) Bu Kanun yayımı tarihinde yürürlüęe girer.

Yürütme

MADDE 75- (1) Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

5464 sayılı Banka Kartları ve Kredi Kartları Kanunu

Resmî Gazete Tarihi : 01.03.2006

Resmî Gazete Sayısı : 26095

BANKA KARTLARI VE KREDİ KARTLARI KANUNU

Amaç

MADDE 1 - Bu Kanunun amacı; banka kartları ve kredi kartlarının çıkarılmasına ve kullanımına ilişkin usûl ve esasları düzenlemek suretiyle kartlı ödemeler sisteminin etkin çalışmasını sağlamaktır.

Kapsam

MADDE 2 - Kartlı sistem kuran, kart çıkaran, üye işyeri anlaşması yapan kuruluşlar ile üye işyerleri ve kart hamilleri bu Kanun hükümlerine tâbidir.

Kendi işyerleri ile sınırlı olmak üzere, mal veya hizmetlerin vadeli satışı ile alıcının borç alacak durumunun izlenmesi amacıyla kart çıkaran veya sistem oluşturan veya herhangi bir kredilendirme işlemi yapılmaksızın veya hesaba bağlı olmaksızın önceden belirlenen bir tutarla sınırlı olmak üzere kart düzenleyen gerçek veya tüzel kişiler bu Kanun hükümlerine tâbi değildir.

(...)

ÜÇÜNCÜ BÖLÜM

Kart Çıkaran Kuruluşların Yükümlülükleri

Kart çıkarma ve buna ilişkin yükümlülükler

MADDE 8 - Kart çıkaran kuruluşlar, talepte bulunmayan veya sözleşme imzalamayan kişiler adına hiçbir şekil ve surette kart veremezler. Bu kuruluşlarca genel müdürlük veya şube haricinde kredi kartı talebi toplanabilecek yerler Kurumun uygun görüşü alınarak Türkiye Bankalar Birliği ve Türkiye Katılım Bankaları Birliği tarafından müştereken belirlenir. Asgarî tutarın son ödeme tarihini takip eden üç ay içinde ödenmemesi durumunda kart çıkaran kuruluşça kart hamiline yapılacak bildirimden itibaren bir aylık süre içerisinde bu tutarın ödenmemesi ya da banka kartı ile kredi kartı kullanımından dolayı adli cezaların uygulanması halinde, ilgili kart çıkaran kuruluşça kart hamiline verilen kredi kartları iptal edilir ve borcun tamamı ödeninceye kadar yeni kredi kartı düzenlenemez.

Kart çıkaran kuruluşlar, kartların düzenli ve güvenli kullanımı ile bildirim, talep, şikâyet ve itirazlara ilişkin gerekli tedbirleri almaya yönelik sistemi kurmak ve kesintisiz olarak açık tutmakla yükümlüdür.

Kart çıkaran kuruluşlar, kartın verilmesi anında kart hamilini yeteri derecede bilgilendirmek ve talep edilmesi halinde, gerçekleştirilmiş işlemlere ait kayıtları otuz günü geçmemek üzere işlemin mahiyetine uygun bir süre zarfında sağlamakla yükümlüdür. Yurt dışı işlemlerinde bu süre altmış gün olarak uygulanır.

Kart çıkaran kuruluşlar, kartların kullanılması bir kod numarası, şifre ya da kimliği belirleyici başka bir yöntemin kullanılmasını gerektiriyorsa, bu tür bilgilerin gizli kalması amacıyla gerekli önlemleri almak ve harcama ve alacak belgesinin müşteri nüshası üzerinde ve yazışmalarda kart numarasının açıkça yer almasını engellemekle yükümlüdür.

Kart çıkaran kuruluşlar, banka kartı ve kredi kartlarının asıl kart hamiline teslim edilmesini sağlayacak önlemleri almak, reşit olmayan ek kart hamilleri adına düzenlenen banka ve kredi kartlarının asıl kart hamillerine teslimini sağlamakla yükümlüdür.

(...)

Bilgilerin saklanması

MADDE 23 - Üye işyerleri, kartın kullanımı sonucunda kart ve kart hamili ile ilgili edindikleri bilgileri, kanunla yetkili kılınan kişi, kurum ve kuruluşlar hariç olmak üzere kart hamilinin yazılı rızasını almadan başkasına açıklayamaz, saklayamaz ve kopyalayamaz. Üye işyerleri, kart bilgilerini üye işyeri anlaşması yaptığı kuruluş dışındaki şahıs veya kuruluşlarla paylaşamaz, satamaz, satın alamaz ve takas edemez. Üye işyeri anlaşması yapan kuruluşlar, bu fıkranın uygulanmasını gözetmekle yükümlüdür.

Kart çıkaran kuruluşlar, edindikleri kişisel bilgileri gizli tutmak, kendi hizmetlerinin pazarlanması dışında başka amaçlarla kullanmamak ve kanunla yetkili kılınan kişi, kurum ve kuruluşlar dışında kalanların bu bilgilere ulaşmasını engellemek amacıyla gereken önlemleri almakla yükümlüdür.

(...)

Sırların saklanması

MADDE 31 - Kurul üyeleri ile Kurum personeli, görevleri sırasında öğrendikleri bu Kanun kapsamındaki kuruluşlara, kart hamillerine ve kefillere ait sırları kanunen açıkça yetkili olanlardan başkasına açıklayamaz ve kendi yararlarına kullanamazlar.

Kartlı sistem kuran, kart çıkaran, üye işyeri anlaşması yapan kuruluşlar, 29 uncu maddede yer alan kuruluşlar ile üye işyerleri, bunların ortakları, yönetim kurulu üyeleri, mensupları, bunlar adına hareket eden kişiler ile görevlileri, sıfat ve görevleri dolayısıyla öğrendikleri sırları kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamazlar. Kart çıkaran kuruluşların destek hizmeti aldığı kuruluş ve çalışanları hakkında da bu hüküm uygulanır.

(...)

Bilgi güvenliği yükümlülüğüne aykırı davranılması

MADDE 39 - Bu Kanununun 8 inci maddesinin beşinci fıkrası ve 23 üncü maddesi hükümlerine kasten aykırı hareket eden kuruluşlar, üye işyerleri ve üye işyeri anlaşması yapan kuruluşların işlerini fiilen yöneten görevlileri ve işlemi yapan kişiler, bir yıldan üç yıla kadar hapis ve bin güne kadar adli para cezası ile cezalandırılırlar.

Kartların kullanılması için zorunlu olup gizli kalması gereken kod numarası, kart numarası, şifre ya da kimliği belirleyici başka bir yöntemin dikkatsizlik veya tedbirsizlik veya meslekte yetersizlik veya emir ve kurallara aykırılık nedeniyle açığa çıkmasına neden olan kart çıkaran kuruluşlar, üye işyerleri ve üye işyeri anlaşması yapan kuruluşların işlerini fiilen yöneten görevli ve ilgili mensupları bin güne kadar adli para cezası ile cezalandırılırlar.

Bu Kanununun 31 inci maddesine aykırı davranışlar hakkında bir yıldan üç yıla kadar hapis ve bin güne kadar adli para cezası uygulanır.

(...)

5429 sayılı Türkiye İstatistik Kanunu

Resmî Gazete Tarihi : 18.11.2005

Resmî Gazete Sayısı : 25997

TÜRKİYE İSTATİSTİK KANUNU

BİRİNCİ KISIM

Genel Hükümler

Amaç

Madde 1- Bu Kanunun amacı; resmî istatistiklerin üretimine ve organizasyonuna ilişkin temel ilkeleri ve standartları belirlemek; ülkenin ihtiyaç duyduğu alanlarda veri ve bilgilerin derlenmesini, değerlendirilmesini, gerekli istatistiklerin üretilmesini, yayımlanmasını, dağıtımını ve Resmî İstatistik Programında istatistik sürecine dâhil kurum ve kuruluşlar arasında koordinasyonu sağlamaktır.

Tanımlar

Madde 2- Bu Kanunun uygulanmasında;

- a) Kurum: Türkiye İstatistik Kurumunu (TÜİK),
- b) Konsey: İstatistik Konseyini,
- c) Başkanlık: Türkiye İstatistik Kurumu Başkanlığını,
- d) Başkan: Türkiye İstatistik Kurumu Başkanını,
- e) Kurum ve kuruluşlar: Cumhurbaşkanlığı ve bakanlıklar ile bunların bağlı, ilgili ve ilişkili kuruluşlarını, mahallî idareler ve bunların bağlı ve ilgili kuruluşları ile birlik ve şirketlerini, Türkiye Cumhuriyet Merkez Bankası, İstanbul Menkul Kıymetler Borsası ve üniversiteler de dâhil olmak üzere, tüzel kişiliği haiz enstitü, teşebbüs, teşekkül, birlik, döner sermaye, fon ve sair adlarla kurulmuş olan diğer kurum ve kuruluşlar ile kamu kurumu niteliğindeki meslek kuruluşlarını, (2)
- f) Program: Resmî İstatistik Programını,

- g) Resmî istatistik: Türkiye İstatistik Kurumu veya Programda yer alan konularda istatistik üretecek kurum ve kuruluşlar tarafından derlenen verilerin, kitle özelliklerini ortaya koymak amacıyla işlenmesi ile elde edilen bilgiyi,
- h) İstatistikî birim: Yapılan sayım veya örnekleme çalışmalarına konu olan, hakkında veri toplanacak gerçek ve tüzel kişiler ile kurum ve kuruluşları,
- i) Kitle: Sayım veya örnekleme konu olan istatistikî birim veya alt birimlerin tamamını,
- j) Sayım: Kitle özelliklerini ortaya koymak üzere ilgili tüm istatistikî birimlerden veri derlenmesini,
- k) Örnekleme: Kitleyi oluşturan istatistikî birimler arasından kitleyi temsil etmek üzere belli sayıda birimin seçilmesi işlemi,
- l) Ulusal kayıt sistemi: Kurum ve kuruluşların idarî işlemlerini yürütmek amacıyla kayıt altına aldıkları bilgilerin standartlaştırılarak tanımlanmış tek bir numara vasıtasıyla ulusal düzeyde ilgili diğer kurum ve kuruluşların kayıtları ile konuşabilirliğinin sağlandığı veri tabanı sistemini,
- m) Alan çalışması: İstatistik çalışmalarıyla ilgili her türlü veriyi derlemek üzere istatistikî birim ile görüşülmesi, bilgilerin anket formuna aktarılması ve bu formların Başkanlığa teslimine kadar geçen sürede yapılan çalışmaları,
- n) Veri: Anket veya idarî kayıtlar yoluyla elde edilen nicel ve/veya nitel istatistikî bilgileri,
- o) Bireysel veri: Hakkında bilgi toplanan istatistikî birimlerin, özellikleri ile birlikte tanımlandığı veriyi,
- p) Doğrudan tanınma: Bir istatistikî birimin kimliğinin adı, adresi veya resmen verilmiş ve genel olarak bilinen bir kimlik numarası ile ortaya çıkarılmasını,
- r) Dolaylı tanınma: Bir istatistikî birimin kimliğinin, doğrudan tanımlamada yer almayan diğer özelliklerinden faydalanılarak ortaya çıkarılmasını,
- s) Gizli veri: İstatistik birimin doğrudan veya dolaylı bir şekilde özellikleri ile birlikte tanınabilmesine ve bu şekilde bireysel bilgilerin açığa çıkarılmasına imkân sağlayan bireysel veya tablo hâlinde saklı tutulan veriyi,
- t) İstatistik amaçlı kullanım: İstatistik birimlerden toplanan verilerin sadece istatistikî tabloların oluşturulması ve istatistikî analizlerin yapılması için kullanımını,
- u) Dağıtım: Kullanılan şekil ve araçlara bakılmaksızın, istatistikî bilgilerin kullanıcılara sunulmasını, ifade eder.

(...)

Gizli veriler

Madde 13- Gizli verilere yalnızca resmî istatistik üretiminde görev alanlar, görevlerini yerine getirebilmek için ihtiyaç duydukları ölçüde erişebilirler.

Bireysel verinin toplulaştırılması ile oluşturulan veri tablosunun herhangi bir hücresindeki istatistikî birim sayısının üçten az olması veya birim sayısı üç ve daha fazla olduğu hâlde bir veya iki istatistikî birimin hakim durumda olması hâlinde ilgili hücredeki veri gizli kabul edilir.

Resmî istatistiklerin üretilmesi için toplanan, işlenen ve saklanan verilerden gizli olanları, idarî, adlî ve askerî hiçbir organ, makam, merci veya kişiye verilemez, istatistik amacı dışında kullanılamaz ve ispat aracı olamaz. Bu bilgileri derleyen ve değerlendiren memurlar ve diğer görevliler de bu yasağa uymak zorundadır. Bu yükümlülük, görevlilerin görevlerinden ayrılmalarından sonra da devam eder.

Resmî istatistik üreten kurum ve kuruluşların yetkilileri tarafından, gizli verilerin hukuka aykırı erişimine, açıklanmasına veya kullanımına karşı her türlü önlem alınır.

Herkese açık kaynaklardan elde edilen veri veya bilgiler gizli kabul edilmez.

İstatistikî birimin, kendisine ait gizli verilerin açıklanmasına yazılı onay vermesi hâlinde, veri gizliliği ortadan kalkar.

Gizli veriler, ancak doğrudan veya dolaylı tanımlamaya yol açmayacak şekilde diğer bilgilerle birleştirilerek yayımlanabilir.

(Ek fıkra: 25/11/2008-5813/2 md.) Dış ticaret istatistiklerinde dolaylı tanınma ile gizlilik kapsamına giren veriler için bu gizlilik hükümleri, istatistikî birimin kendisine ait verinin gizlenmesini talep eden yazılı başvurusu halinde uygulanır.

Veri gizliliği ve güvenliğine ilişkin usûl ve esaslar, ulusal ve uluslararası ilkeler doğrultusunda, ilgili kurum ve kuruluşların görüşleri alınarak çıkarılacak yönetmelikle düzenlenir.

Bireysel verilerin kullanımı

Madde 14- Bireysel veriler, istatistikî birimlerin doğrudan veya dolaylı olarak tanınmasına yol açacak bölümleri gizlendikten sonra, münferit birimlere atıfta bulunmayan bilimsel amaçlı araştırmalarda kullanılması kaydı ve Başkanlığın yazılı izniyle verilebilir. Bireysel verileri kullanma hakkı elde edenler, bu verileri üçüncü şahıslara veremezler.

İstatistikî birimlerin hakları

Madde 15- Resmî istatistiklerin üretimi için veri veya bilgi talep edilen istatistikî birimler, sayımın veya araştırmanın amacı, kapsamı, istatistikî verinin gizliliğinin sağlanması için alınan önlemler ve hakları ile ilgili konularda 4982 sayılı Bilgi Edinme Hakkı Kanunu çerçevesinde, bilgi edinme, kendilerine ait gizli verinin izinsiz açıklanması durumunda da maddi ve manevi her türlü zararının tazmin edilmesini isteme hakkına sahiptir.

Kendilerine ait gizli verilerin açıklanması nedeniyle açılan davalarda Başkanlık veya diğer kurum ve kuruluşlar aleyhine tazminata hükmedilmesi durumunda, bu hususta kusuru olan memur ve diğer görevlilere genel hükümlere göre rücu edilir.

(...)

5411 sayılı Bankacılık Kanunu

Resmî Gazete Tarihi : 01.11.2005

Resmî Gazete Sayısı : 25983 (Mük.)

BANKACILIK KANUNU

BİRİNCİ KISIM

Genel Hükümler

Amaç

Madde 1 - Bu Kanunun amacı, finansal piyasalarda güven ve istikrarın sağlanmasına, kredi sisteminin etkin bir şekilde çalışmasına, tasarruf sahiplerinin hak ve menfaatlerinin korunmasına ilişkin usûl ve esasları düzenlemektir.

Kapsam

Madde 2 - Türkiye'de kurulu mevduat bankaları, katılım bankaları, kalkınma ve yatırım bankaları, yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubeleri, finansal holding şirketleri, Türkiye Bankalar Birliği, Türkiye Katılım Bankaları Birliği, Bankacılık Düzenleme ve Denetleme Kurumu, Tasarruf Mevduatı Sigorta Fonu ve bunların faaliyetleri bu Kanun hükümlerine tâbidir.

Özel kanunlarla kurulmuş olan bankalar hakkında da kanunlarında yer alan hükümler saklı kalmak kaydıyla bu Kanun hükümleri uygulanır.

Bu Kanunda hüküm bulunmayan hallerde genel hükümler tatbik olunur.

(...)

Belgelerin saklanması

Madde 42 - Alınan yazılar ve faaliyetler ile ilgili belgelerin asılları veya bunun mümkün olmadığı hâllerde sıhhatlerinden şüpheye mahal vermeyecek kopyaları ve yazılan yazıların makine ile alınmış, tarih ve numara sırası verilerek düzenlenecek suretleri, usûlleri çerçevesinde ilgili banka nezdinde on yıl süreyle saklanır. Bu belgelerin mikrofilm, mikrofiş şeklinde veya elektronik, manyetik veya benzeri ortamlarda saklanmaları mümkündür. Bu maddenin uygulanmasına ilişkin usûl ve esaslar Kurulca belirlenir.

(...)

YEDİNCİ KISIM

Kanunî Yükümlülükler

Sırların saklanması

Madde 73 - Kurul başkan ve üyeleri ile Kurum personeli, Fon Kurulu başkan ve üyeleri ile Fon personeli görevleri sırasında öğrendikleri bankalara ve bunların bağlı ortaklık, iştirak, birlikte kontrol edilen ortaklıkları ve müşterilerine ait sırları bu Kanuna ve özel kanunlarına göre yetkili olanlardan başkasına açıklayamaz ve kendilerinin veya başkalarının yararlarına kullanamazlar. Kurumun dışarıdan destek hizmeti aldığı kişi ve kuruluşlar ile bunların çalışanları da bu hükme tâbidir. Bu yükümlülük görevden ayrıldıktan sonra da devam eder.

Bu Kanun hükümleri uyarınca Kurumun, yurt dışındaki muadili denetim mercileri ile düzenleyeceği mutabakat zabıtları çerçevesinde vereceği bilgi ve belgeler birinci fıkradaki sır kapsamında değildir. Kurul düzenleyeceği mutabakat zabıtları veya zabıtlar dışında elde edeceği sırların korunmasını sağlamakla görevlidir. Kurumun elde edeceği sır niteliğindeki bilgi ve belgeler, kuruluş ve faaliyet izni verilmesinde, faaliyetlerin denetiminde, düzenlemelere uyulup uyulmadığının izlenmesinde ve Kurul kararlarına karşı açılacak idarî davaların görülmesinde kullanılabilir. (Değişik dördüncü cümle: 13/2/2011-6111/146 md.) Kurumun bu fıkra kapsamında elde edeceği sır niteliğindeki bilgi ve belgeler, ceza soruşturması ve kovuşturması kapsamında savcılıklar ile ceza mahkemeleri, görevden ayrılmış olsalar dahi, görevleriyle bağlantılı olarak işledikleri iddia edilen suçlardan dolayı başlatılan soruşturma ve kovuşturmalar ile bağlantılı olarak talepte bulunacak Kurul Başkanı ve üyeleri ile Kurum personeli dışında hiçbir kişi, kurum ve kuruluşa verilemez. Mahkeme kararına bağlanmış sır kapsamına giren bilgilerin verilmesinden Kurum sorumlu tutulamaz.

(Değişik üçüncü fıkra: 13/2/2011-6111/146 md.) Sıfat ve görevleri dolayısıyla bankalara veya müşterilerine ait sırları öğrenenler, söz konusu sırları bu konuda kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamazlar. Bu yükümlülük görevden ayrıldıktan sonra da devam eder.

(Ek cümleler:20/2/2020-7222/10 md.) Bankacılık faaliyetlerine özgü olarak bankalarla müşteri ilişkisi kurulduktan sonra oluşan gerçek ve tüzel kişilere ait veriler, müşteri sırrı hâline gelir. Diğer kanunların emredici hükümleri saklı kalmak kaydıyla, müşteri sırrı niteliğindeki bilgiler, bu maddede belirtilen sır saklama yükümlülüğünden istisna tutulan hâller haricinde, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca müşterinin açık rızası alınsa dahi, müşteriden gelen bir talep ya da talimat olmaksızın yurt içindeki ve yurt dışındaki üçüncü kişilerle

paylaşamaz ve bunlara aktarılamaz. Kurul ekonomik güvenliğe ilişkin yapacağı değerlendirme neticesinde, müşteri sırrı ya da banka sırrı niteliğinde olan her türlü verinin, yurt dışındaki üçüncü kişilerle paylaşılmasını ya da bunlara aktarılmasını yasaklamaya, ayrıca bankaların faaliyetlerini yürütmede kullandıkları bilgi sistemleri ve bunların yedeklerinin yurt içinde bulundurulması hususunda karar almaya yetkilidir. Bu maddede belirtilen sır saklama yükümlülüğünden istisna tutulan hâllerde yapılacak paylaşımlar da dâhil olmak üzere, müşteri sırrı ve banka sırrı niteliğindeki bilgiler, sadece belirtilen amaçlarla sınırlı olmak ve ölçülülük ilkesine uygun olarak bu amaçların gerektirdiği kadar veriyi içermek kaydıyla paylaşılabilir. 22/4/1926 tarihli ve 818 sayılı Borçlar Kanunu, 13/6/1952 tarihli ve 5953 sayılı Basın Mesleğinde Çalışanlarla Çalıştıranlar Arasındaki Münasebetlerin Tanzimi Hakkında Kanun, 20/4/1967 tarihli ve 854 sayılı Deniz İş Kanunu ile 22/5/2003 tarihli ve 4857 sayılı İş Kanunu kapsamında çalıştırılan işçi, gemi adamı ve gazetecinin ücret, prim, ikramiye ve bu nitelikte her çeşit istihkak ödemelerinin özel olarak açılan banka hesabına yapılması halinde, bu hesaplara ilişkin bilgi ve belgelerin Çalışma ve Sosyal Güvenlik Bakanlığı, Maliye Bakanlığı ve Hazine Müsteşarlığı ile bunlara bağlı ve ilgili kurum ve kuruluşlara verilmesi ile 31/5/2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 8 inci ve 100 üncü maddelerinin uygulanması ile genel sağlık sigortalılığında gelir testinin yapılmasına ilişkin bilgi ve belgelerin Sosyal Güvenlik Kurumuna ve il veya ilçe sosyal yardımlaşma ve dayanışma vakıflarınca yapılan sosyal yardım hak sahiplerinin tespiti ile gelir testi işlemlerinin yürütülmesi amacıyla Aile ve Sosyal Politikalar Bakanlığı Sosyal Yardımlar Genel Müdürlüğüne verilmesi sırrın ifşası sayılmaz. Bu bilgi ve belgelerin verilmesine ilişkin usûl ve esaslar Çalışma ve Sosyal Güvenlik Bakanlığı, Maliye Bakanlığı, Hazine Müsteşarlığının bağlı olduğu Bakanlık ile Kurulca belirlenir.

(Değişik dördüncü fıkra: 13/2/2011-6111/146 md.) Kurumun gözetim ve denetimine tabi kuruluşların, bunların ortaklarına, bağlı ortaklık, iştirak, birlikte kontrol edilen ortaklıklarının faaliyetlerine veya müşterilerine ilişkin yabancı ülke kanunlarına göre denetime yetkili ve Kurum muadili mercilerin taleplerinin Kurumca karşılanması, gizlilik sözleşmesi yapılması ve sadece belirtilen amaçlar ile sınırlı kılınması koşuluyla bankaların ve finansal kuruluşların, kendi aralarında doğrudan doğruya ya da risk merkezi veya en az beş banka ya da finansal kuruluş tarafından kurulacak şirketler vasıtasıyla yapacakları her türlü bilgi ve belge alışverişinin yanı sıra doğrudan veya dolaylı pay sahipliği yoluyla sermayelerinin yüzde onunu ve daha fazlasını temsil eden paylarının satışı amacıyla muhtemel alıcıların yapacakları değerlendirme çalışmalarında ya da sermayelerinin yüzde on veya daha fazlasına sahip olan yurt içinde veya yurt dışında yerleşik kredi kuruluşu ile finansal kuruluşlar da dâhil ana ortaklıkların konsolide finansal tablo hazırlama çalışmalarında, risk yönetimi ve iç denetim uygulamalarında veya kredileri de dâhil varlıklarının ya da bunlara dayalı menkul kıymetlerin satışı

amacıyla yapılacak deęerleme alıřmalarında ya da deęerleme, derecelendirme veya destek hizmeti alınması ile baęımsız denetim faaliyetlerinde ve gerekli tedbirlerin alınması kaydıyla hizmet alımlarına ynelik iřlemlerde kullanılmak zere bilgi ve belge taleplerinin karřılanması sırasında banka ya da mřteri sırrı nitelięindeki bilgilerin ęrenilmesi sır saklama ykmllę dıřındadır.

(Ek fıkra:20/2/2020-7222/10 md.) Sır nitelięindeki bilgilerin, nc ve drdnc fıkralar uyarınca yapılacak paylařım ve aktarımlarına iliřkin kapsam, Őekil, usul ve esasları belirlemeye veya bunlara iliřkin sınırlamalar getirmeye Kurul yetkilidir.

(...)

Yerinde denetim ve gzetim

Madde 95 - Bu Kanun hkmleri ile bu Kanun kapsamındaki kuruluřlar hakkında dięer kanunlarda yer alan hkmlerin uygulanmasının ve bu kuruluřların her trl iřlemlerinin gzetimi ve yerinde denetimi ve bu Kanun kapsamındaki kuruluřların konsolide ve konsolide olmayan bazda risk yapısı, i kontrol, risk ynetimi ve i denetim sistemleri ile varlıkları, alacakları, zkaynakları, borları, kr ve zarar hesapları, ykmllkleri ve taahhtleri arasındaki ilgi ve dengelerin ve mal bnyeyi etkileyen dięer tm unsurların ve bu kuruluřların kurumsal ynetim ilkelerine uyum seviyesinin gzetimi, tahlili ve lm Kurum tarafından yapılır.

Kurum, baęımsız denetim kuruluřlarınca yapılan yıllık finansal raporların yapısı, uygunluęu ve gvenilirlięinin deęerlendirilmesini de yerine getirir.

Bu Kanuna tab kuruluřlar tarafından, Kurulca belirlenen usl ve esaslar erevesinde konsolide ve konsolide olmayan bazda istenilen her trl bilgi, belge, cetvel, rapor ve finansal tabloların, hesap ve kayıt dzenleriyle uyumlu olarak, zamanında ve doęru Őekilde Kuruma tevdi edilmesi Őarttır.

Sz konusu kuruluřlarda denetim yapma yetkisi bulunanlar tarafından dzenlenen rapor ve mtalaların bir suretinin anılan kuruluřlarca Kuruma gnderilmesi zorunludur.

Kurum, incelemelerini Bařkanın onayından gemiř alıřma programları ile Bařkan tarafından yapılacak grevlendirmeler erevesinde gerekleřtirir.

Bařkan, yapılacak yerinde denetimde, Kurumun meslek personelini oluřturan bankalar yeminli murakıp ve yardımcıları, bankacılık uzmanı ve yardımcıları, biliřim uzmanı ve yardımcıları, hukuk uzmanı ve yardımcıları arasından uygun greceęi bir denetim ekibini grevlendirir. Kurumun yerinde denetim yapmaya yetkili meslek personeli İstanbul'da Asliye Ticaret Mahkemesinde (1)

yemin etmedikçe yerinde denetim yapamazlar. Yerinde denetim yapan Kurumun meslek personeli denetim konularıyla ilişkili olarak bu maddede belirtilen tüm yetkileri haizdir.

Başkan, gerekli gördüğünde ve özellik arz eden konularda bağımsız denetim kuruluşlarını ilgili konu hakkında inceleme yapılması için görevlendirme yetkisini haizdir. Bağımsız denetim yapan kuruluşun denetçisi denetim konularıyla ilişkili olmak kaydıyla bu maddede belirtilen ilgili yetkileri haiz olduğu gibi, bu Kanun kapsamındaki sırların saklanması yükümlülüklerine de tâbidir.

Kurum, bankalardan, bunların bağlı ortaklıklarından, nitelikli paya sahip oldukları ortaklıklardan, birlikte kontrol ettikleri ortaklıklardan, şubeleri ile temsilciliklerinden, destek hizmeti kuruluşlarından ve diğer gerçek ve tüzel kişilerden bu Kanun hükümleri ile ilgili görecekları bütün bilgileri gizli dahi olsa istemeye, bunların vergiyle ilgili kayıtları dahil olmak üzere tüm defter, kayıt ve belgelerini incelemeye yetkili olup, bilgi istenenler de istenilen bilgileri vermekle, defter, kayıt ve belgeleri incelemeye hazır bulundurmamakla, tüm bilgi işlem sistemini denetim amaçlarına uygun olarak Kurumun yerinde denetim yapan meslek personeline açmakla, verilerin güvenliğini sağlamakla ve muhafaza etmek zorunda oldukları her türlü defter, belge ve karneler ile vermek zorunda buldukları bilgilere ilişkin mikrofiş, mikrofilm, manyetik teyp, disket ve benzeri ortamlardaki kayıtlarını ve bu kayıtlara erişim veya kayıtları okunabilir hale getirmek için gerekli tüm sistem ve şifrelerini inceleme için ibraz etmek ve işletmekle yükümlüdür.

Kamu kurum ve kuruluşları, Merkez Bankası ve benzeri kuruluşlar ile Risk Merkezi görevleriyle ilgili olarak istenecek her türlü bilgi ve belgeyi gizli de olsa Kurumun yerinde denetim yapan meslek personeline geciktirilmeksizin verirler. Kurul, ilgili taraflarla bu husustaki detayları belirleyen mutabakat zaptı düzenleyebilir.

Kurum tarafından gerçekleştirilen denetimler sırasında talep edilmesi hâlinde, bankalar tarafından iç kontrol, risk yönetimi ve iç denetim sistemlerinde çalışanların görevlendirilmesi dâhil olmak üzere her türlü destek sağlanır.

Diğer kanunlar uyarınca Kurumun meslek personelinin bu Kanun kapsamındaki görevleri dışında görevlendirilmeleri, bu maddede sayılan görevleri öncelikli olmak kaydıyla Başkan tarafından yapılır.

Kurum; bu Kanunun, Kurumun görev, yetki ve sorumluluklarına ilişkin hükümlerinde zikredilen ve 20.2.1930 tarihli ve 1567 sayılı Türk Parasının Kıymetini Koruma Hakkında Kanun hükümlerine aykırı hareket eden kuruluşlar ve ilgilileri hakkında, adı geçen Kanunun ek 1 inci maddesindeki

yetkilere sahip olduđu gibi tüm bankaların kuruluş kanunu hükümleri ile diđer kanunların bankalarla ilgili hükümlerinin uygulanmasını denetlemeye de yetkilidir.

Bankalarda yerinde denetim yapan kişiler, bu Kanunda belirtilen düzenlemeler dışında diđer kanunlara aykırılıkları tespit ettikleri takdirde bu tespitleri ilgili mercilere derhal bildirmek zorundadırlar.

Denetim ve gözetime ilişkin usûl ve esaslar Kurulca düzenlenecek yönetmelikle belirlenir.

(...)

Bilgi ve belge isteme

Madde 96 - Bu Kanununun 93 üncü maddesinin birinci fıkrasının (a) bendinde belirtilen kuruluşlar ile ortakları, bunların bađlı ortaklıkları, nitelikli paya sahip olduđu ortaklıkları, birlikte kontrol ettiđi ortaklıkları, şubeleri ile temsilcilikleri, bađımsız denetim, deđerleme ve destek hizmeti kuruluşları gizli dahi olsa bu Kanunun uygulanması ile ilgili olarak her türlü bilgi ve belgeyi Kurumun talebi üzerine Kuruma tevdi etmekle yükümlüdür.

Kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler, Devletin güvenliđi ve temel dış yararlarına karşı ağır sonuçlar doğuracak hâller ile meslek sırrı, aile hayatının gizliliđi ve savunma hakkına ilişkin hükümler saklı kalmak kaydıyla özel kanunlardaki yasaklayıcı ve sınırlayıcı hükümler dikkate alınmaksızın gizli dahi olsa Kurum tarafından bu Kanun kapsamında verilen görevler ile sınırlı olmak üzere istenecek her türlü bilgi ve belgeyi uygun süre ve ortamda, sürekli veya münferit olarak vermeye, istenecek defter ve belgeleri ibraz etmeye ve incelemeye hazır bulundurmaya, tüm bilgi işlem sistemini denetim amaçlarına uygun olarak ilgili personele açmaya, verilerin güvenliđini sağlamaya ve muhafaza etmek zorunda oldukları her türlü defter, belge ve karneler ile vermek zorunda buldukları bilgilere ilişkin mikrofiş, mikrofilm, manyetik teyp, disket ve benzeri ortamlardaki kayıtlarını ve bu kayıtlara erişim veya kayıtları okunabilir hale getirmek için gerekli tüm sistem ve şifreleri incelemek için ibraz etmeye ve işletmeye mecburdurlar.

Bu madde kapsamında ilgili kişi, kurum ve kuruluşlar Kurumun belirleyeceđi süre içerisinde söz konusu talebe cevap vermek ve gereken kolaylıđı göstermekle yükümlüdürler.

(...)

Kurumlararası işbirliđi

Madde 98 - Para, kredi ve bankacılık politikalarının yürütülmesiyle ilgili konularda Kurum, Hazine Müsteşarlığı, Devlet Plânlama Teşkilatı Müsteşarlığı, Tasarruf Mevduatı Sigorta Fonu ve Merkez Bankası karşılıklı mütalâa ve bilgi teatisinde bulunurlar.

Kurum, Fon ve Merkez Bankası bu Kanunda belirtilen görevleri yerine getirmek amacıyla veri tabanlarında yer alan ve birlikte üzerinde uzlaşılan bilgileri gizlilik hükümleri çerçevesinde paylaşırlar.

Yabancı ülke kanunlarına göre denetime yetkili ve Kurum muadili mercilerin, kendi ülkelerindeki finansal piyasalarda faaliyet gösteren kuruluşların Türkiye'deki şube veya ortaklıklarında denetim yapma ve bilgi talepleri ile bankaların yurt dışındaki şube veya ortaklıklarının konsolidasyon kapsamında yer alan bilgilerine ilişkin taleplerinin, karşılıklılık ilkesi de dikkate alınarak yerine getirilmesi Kurulun iznine tâbidir.

Kurum ayrıca, politikaların ve düzenlemelerin uyumlaştırılmasına yönelik olarak, gerekli gördüğü hâllerde yabancı ülkelerde denetim yapma ve eğitim ile personel değişimi imkânı sağlamak üzere Kurum muadili merciler ile düzenleyeceği ikili mutabakat zabıtları çerçevesinde veya başka yollarla finansal kuruluşlarla ve finansal piyasalarla ilgili her türlü işbirliği ve bilgi alışverişinde bulunmaya yetkilidir. Kurum, bu mutabakat zabıtlarının usûl ve esasları hakkında kamuoyunu bilgilendirir.

Kurum, yurt dışında şube veya ortaklığı bulunan bir bankanın faaliyet iznini kaldırdığı veya Fona devrettiği takdirde, ilgili ülkenin muadil merciine durumu ivedilikle bildirir.

Yurt içi ve yurt dışı yetkili mercilerle denetime, bilgi paylaşımına ve diğer hususlara dair yapılacak işbirliğine ilişkin usûl ve esaslar ilgili tarafların görüşü alınmak suretiyle Kurulca belirlenir.

(...)

Sistemi engelleme, bozma, verileri yok etme veya değiştirme

Madde 157 - Bu Kanuna tâbi kuruluşlar, 5237 sayılı Türk Ceza Kanununun 244 üncü maddesinde tanımlanan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu açısından banka veya kredi kurumu olarak kabul edilir.

İtibarın zedelenmesi

Madde 158 - Bu Kanunun 74 üncü maddesine aykırı davrananlar bir yıldan üç yıla kadar hapis ve bin günden ikibin güne kadar adlî para cezası ile cezalandırılır.

Yukarıdaki fıkrada yazılı fiil neticesinde özel veya kamusal bir zarar doğarsa verilecek ceza altıda bir oranında artırılarak hükmolünür.

Sırların açıklanması

Madde 159 - Bu Kanunun 73 üncü maddesinin birinci ve üçüncü fıkralarında belirtilen yükümlülüğe uymayanlar için bir yıldan üç yıla kadar hapis ve bin günden ikibin güne kadar adli para cezası hükümlenir. Banka ve müşterilere ait sırları açıklayan üçüncü kişiler hakkında da aynı cezalar uygulanır.

Yukarıdaki fıkrada belirtilen kimseler sırları kendileri ya da başkaları için yarar sağlamak amacıyla açıklamış olursa verilecek cezalar altıda bir oranında artırılır. Ayrıca, fiilin önemine göre sorumluların bu Kanun kapsamına giren kuruluşlarda görev yapmaları, iki yıldan aşağı olmamak üzere geçici veya sürekli olarak yasaklanır.

(...)

Risk Merkezi

Ek Madde 1 - (Ek: 13/2/2011-6111/149 md.)

Türkiye Bankalar Birliği nezdinde, kredi kuruluşları ile Kurulca uygun görülecek finansal kuruluşların müşterilerinin risk bilgilerini toplamak ve söz konusu bilgileri bu kuruluşlar ile gerçek veya tüzel kişilerin kendileriyle ya da onay vermeleri koşuluyla gerçek kişiler ve özel hukuk tüzel kişileri ile de paylaşılmasını sağlamak üzere Risk Merkezi kurulmuştur.(1)

Kredi kuruluşları ile Kurulca uygun görülecek finansal kuruluşlar, Risk Merkezine üye olmak zorundadır. Üye kuruluşlar, Risk Merkezince istenilen, müşterileri ile ilgili her türlü bilgiyi vermekle yükümlüdür. Risk Merkezi, bu yükümlülüğe uymayanlara bilgi akışını durdurmaya yetkilidir.

Risk Merkezi, Kurumun ve Merkez Bankasının personeli arasından belirleyeceği birer üye dâhil olmak üzere dokuz üyeden oluşan bir yönetim tarafından idare edilir. Risk Merkezi yönetimini oluşturan üyeler üç yıllık dönem için görev yapmak üzere seçilir. Risk Merkezi yönetimi, Risk Merkezinin kuruluş amaçları doğrultusunda özel hukuk tüzel kişileri ile kamu kurum ve kuruluşlarından, kamu kurumu niteliğinde meslek kuruluşları ve bunların üst kuruluşlarından bilgi talep etmeye ve bunlarla Kurulun uygun görüşüne istinaden bilgi alış-verişine yönelik sözleşmeler imzalamaya yetkilidir. Özel hukuk tüzel kişileri ile kamu kurum ve kuruluşları, kamu kurumu niteliğinde meslek kuruluşları ve bunların üst kuruluşları Risk Merkezi yönetimi tarafından talep edilen bilgileri vermekle yükümlüdürler. Kredi kuruluşları ile Kurulca uygun görülecek finansal kuruluşların müşterilerinin onay vermesi koşuluyla, Risk Merkezi ile bilgi alış-verişi sözleşmesi imzalayan özel hukuk tüzel kişileri ile kamu kurum ve kuruluşlarına kamu kurumu niteliğinde

meslek kuruluşları ve bunların üst kuruluşlarına verilecek, müşterilerin bu kuruluşlar nezdindeki risk bilgileri Kanunun 73 üncü maddesinin dördüncü fıkrası kapsamında değerlendirilir.

Risk Merkezinin kuruluşuna, faaliyetine ve çalışmasına, Risk Merkezi yönetiminin oluşumuna, toplanmasına ve karar almasına, Risk Merkezine verilen bilgilerin kapsam, biçim ve içeriğine ve bunların paylaşılmasına, paylaşılacak bilgilerin kapsam ve içeriğine, ücretlendirilmesine ve üyelerce ödenecek aidatların belirlenmesine ilişkin usul ve esaslar, Türkiye Katılım Bankaları Birliği ve Kurul tarafından belirlenen finansal kuruluşların üye oldukları meslek örgütlerinin görüşü ile Kurulun ve Merkez Bankasının uygun görüşü alınarak Türkiye Bankalar Birliğince belirlenir ve Resmi Gazetede yayımlanır.

Süresinde üyeler tarafından ödenmeyen aidatlar ve komisyonlar Türkiye Bankalar Birliğince kanuni yollara başvurulur tahsil edilir.

Kurum, gerektiğinde Risk Merkezini denetler, denetime ilişkin usul ve esaslar Kurum tarafından belirlenir.

Risk Merkezi, topladığı her türlü bilgiyi, Kurum ve Merkez Bankasına istenen biçim ve sürede vermekle yükümlüdür. Ayrıca, gerçek ya da tüzel kişilerin gerekçesini belirterek risk bilgilerinin kendilerine verilmesi için yazılı talepte bulunmaları ya da kredi kuruluşları ile Kurulca uygun görülecek finansal kuruluşlar dışındaki bir gerçek kişi veya özel hukuk tüzel kişisine bu nitelikteki bilgilerin verilmesi için onay verdiklerinin ispat edilmesi halinde bahse konu bilgiler de talepte bulunan tarafça karşılanacak belli bir ücret karşılığında verilir.(1)

Risk Merkezinin bütün işlem ve kayıtları gizlidir. Sır sahibinin bilgilerinin açıklanması konusunda açık rızasının bulunması durumunda belirlediği kişiye risk bilgileri verilir. Kişinin rızasına dayanan bilgilerin verilmesine ilişkin usul ve esaslar, Kurulun ve Merkez Bankasının uygun görüşü, Türkiye Katılım Bankaları Birliğinin ve Kurulun belirleyeceği kurum ve kuruluşların görüşü alınarak Türkiye Bankalar Birliğince belirlenir ve Resmi Gazetede yayımlanır.

Risk Merkezi nezdinde bulunan sır niteliğindeki bilgileri, bu konuda kanunen yetkili kılınan mercilerden başkalarına açıklayanlar, hukuka aykırı olarak kendisi ya da başkası yararına kullananlar, yayanlar, verenler, aktaranlar veya ele geçirenler hakkında 159 uncu madde hükümleri uygulanır. Bu fıkra tanımlanan suçların bir tüzel kişinin faaliyeti çerçevesinde işlenmesi halinde, ilgili tüzel kişi hakkında Türk Ceza Kanununun tüzel kişilere özgü güvenlik tedbirlerine hükmolunur.

Risk Merkezi, nezdindeki her türlü bilgi alış-verişini 73 üncü maddenin dördüncü fıkrası uyarınca en az beş banka tarafından kurulmuş şirketler aracılığı ile ve bu şirketlerle yapılacak sözleşmeler çerçevesinde de gerçekleştirebilir.

5352 sayılı Adli Sicil Kanunu

Resmî Gazete Tarihi : 01.06.2005

Resmî Gazete Sayısı : 25832

ADLİ SİCİL KANUNU

Amaç ve kapsam

Madde 1- (1) Bu Kanun, kesinleşmiş ceza ve güvenlik tedbirlerine mahkûmiyete ilişkin bilgilerin otomatik işleme tâbi bir sistem kullanılarak toplanmasına, sınıflandırılmasına, değerlendirilmesine, muhafaza edilmesine ve gerektiğinde en seri ve sağlıklı biçimde ilgililere bildirilmesine dair usul ve esasları belirler.

Adli sicil kayıtlarının tutulması

Madde 2- (1) Hakkında Türk mahkemeleri veya yabancı ülke mahkemeleri tarafından kesinleşmiş ve Türk Hukukuna göre tanınan mahkûmiyet kararı bulunan Türk vatandaşları ile Türkiye'de suç işlemiş olan yabancıların kayıtları da dahil tüm adli sicil bilgileri; mahallinde bilgisayar ortamına aktarılmasını takiben, Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğündeki Merkezî Adli Sicilde tutulur.

Merkezî ve mahalli adli sicillerin görevleri

Madde 3- (1) Merkezî Adli Sicil, adli sicil kayıtlarının güncelleştirilmesi, düzenlenmesi, düzeltilmesi ve mahalli adli sicillere ulaştırılması ile görevlidir.

(2) Mahalli adli sicil, bulunduğu yer ile gerektiğinde diğer yerlere ait adli sicil bilgilerinin bilgisayara girilmesi, bu bilgilerin merkezî adli sicile aktarılması ile merkezî adli sicilden bilgilerin alınıp ilgili şahıs ve kurumlara iletilmesi ile görevlidir.

Adli sicile kaydedilecek bilgiler

Madde 4- (1) Türk mahkemeleri tarafından vatandaş veya yabancı hakkında verilmiş ve kesinleşmiş mahkûmiyet hükümleri adli sicile kaydedilir. Bu bağlamda;

a) Hapis cezaları ile ilgili olarak;

1. Hapis cezasına mahkûmiyet kararı,

2. Koşullu salıverilme kararı,
3. Koşullu salıverilmede denetim süresinin uzatılmasına ilişkin karar,
4. Koşullu salıverilme kararının geri alınmasına dair karar,
5. Hapis cezasının infazının tamamlandığı hususu,

b) Hapis cezasının ertelenmesi halinde;

1. Denetim süresi,
2. Denetim süresinin yükümlülüklerle uygun veya iyi halli olarak geçirilmesi dolayısıyla cezanın infaz edilmiş sayıldığı hususu,
3. Ertelenen hapis cezasının infaz kurumunda çektirilmesine ilişkin karar,

c) Adlî para cezası ile ilgili olarak;

1. Adlî para cezasına ilişkin mahkûmiyet hükmü,
2. Adlî para cezasının ödenmek suretiyle infaz edildiği hususu,
3. Adlî para cezasının tazyik hapsi suretiyle kısmen veya tamamen infaz edildiği hususu,
4. Adlî para cezasının tazyik hapsinden sonra kalan kısmının ödenmek suretiyle infaz edildiği hususu,

d) Kısa süreli hapis cezasına seçenek yaptırıma mahkûmiyet halinde;

1. Kısa süreli hapis cezasına seçenek yaptırım olarak, adlî para cezasına mahkûmiyet veya güvenlik tedbiri uygulanması hükmü,
2. (Değişik: 26/2/2008-5739/7 md.) Kısa süreli hapis cezasına seçenek yaptırım olarak hükmedilen güvenlik tedbirinin gereklerinin yerine getirilmemesi dolayısıyla hapis cezasının infazına ilişkin karar,
3. Kısa süreli hapis cezasına seçenek yaptırım olarak hükmedilen güvenlik tedbirinin değiştirilmesine ilişkin karar,

e) Belli hakları kullanmaktan yoksun bırakılma ile ilgili olarak;

1. Kasten işlenen bir suç nedeniyle hapis cezasına mahkûmiyetin kanunî sonucu olarak yoksun kalınan haklara cezanın ertelenmesi dolayısıyla getirilen istisnaya ilişkin karar,

2. Mahkûmiyet hükmüyle bağlantılı olarak verilen, belli bir hak ve yetkinin kullanılmasının veya belli bir meslek veya sanatın icrasının yasaklanmasına ya da sürücü belgesinin geri alınmasına ilişkin karar,

f) Türk vatandaşı hakkında yabancı mahkemeden verilmiş ve kesinleşmiş olan mahkûmiyet kararının Türk hukuku bakımından doğurduğu hak yoksunluklarına ilişkin olarak Cumhuriyet savcısının istemi üzerine mahkemece verilen karar,

g) Ceza mahkûmiyetini bütün sonuçlarıyla ortadan kaldıran şikayetten vazgeçme veya etkin pişmanlık dolayısıyla verilen karar,

h) Ceza zamanaşımının dolduğunun tespitine ilişkin karar,

i) Genel veya özel affa ilişkin kanun; özel affa ilişkin Cumhurbaşkanlığı kararı,

j) Askerî Ceza Kanununa göre verilmiş mahkûmiyet kararlarındaki ferî cezalar,

k) (Ek: 24/11/2016-6763/39 md.) Akıl hastalığı nedeniyle hükmedilen güvenlik tedbirlerine ilişkin kararlar,

Adlî sicile kaydedilir.

(2) Kanun yararına bozma veya yargılamanın yenilenmesi sonucunda verilen mahkûmiyet hükmü ya da eski hükümde değişiklik yapan tüm hüküm ve kararlar açısından da birinci fıkra hükümleri uygulanır.

(3) Kanun gereği olarak gerçek kimliği saklı tutulan kişilerin adlî sicil ve arşiv kayıtlarına ilişkin usul ve esaslar yönetmelikle düzenlenir.

Adlî sicile kaydedilmeyecek bilgiler

Madde 5- (1) Türk mahkemeleri tarafından verilmiş olsa bile;

a) Disiplin suçlarına ve sırf askerî suçlara ilişkin mahkûmiyet hükümleri,

b) Disiplin veya tazyik hapsine ilişkin kararlar,

c) İdarî para cezasına ilişkin kararlar,

Adlî sicile kaydedilmez.

Diğer bilgilerin kaydı

Madde 6- (1) Kamu davasının açılmasının ertelenmesine ve hükmün açıklanmasının geri bırakılmasına ilişkin kararlar, ancak bir soruşturma veya kovuşturmayla bağlantılı olarak mahkeme, hâkim veya Cumhuriyet Başsavcılığı tarafından istenmesi halinde verilmek üzere kaydedilir.

(2) (Ek: 2/7/2012-6352/103 md.) Karşılıksız yararlanma suçunda etkin pişmanlıktan yararlanması dolayısıyla şüpheli, sanık veya hükümlü hakkında verilen kararlar adlî sicilde bunlara mahsus bir sisteme kaydedilir. Onbeş yıl süreyle muhafaza edilen bu kayıtlar, ancak bir soruşturma veya kovuşturmayla bağlantılı olarak Cumhuriyet savcısı veya mahkeme tarafından istenmesi halinde verilebilir.

Adlî sicil bilgileri verilebilecek olanlar

Madde 7- (1) Adlî sicil bilgileri, kullanılış amacı belirtilmek suretiyle;

- a) İlgili kişiye veya vekâletnamede açıkça belirtilmek koşuluyla vekiline,
 - b) Kamu kurum ve kuruluşlarına, kamu kurumu niteliğindeki meslek kuruluşlarına,
- Verilebilir.

(2) Yabancı devletler tarafından istenilen adlî sicil bilgileri mütekabiliyet esasına göre verilir.

Adlî sicil bilgilerini verebilecek merciler

Madde 8- (1) Adlî sicil bilgileri; mahalli adlî sicillerde Cumhuriyet başsavcılıklarınca, (...) kaymakamlıklarca yurt dışında elçilik ve konsolosluklarca, merkezî adlî sicilde ise Adalet Bakanlığı Adlî Sicil ve İstatistik Genel Müdürlüğünce verilir.

Adlî sicil bilgilerinin silinmesi

Madde 9- (1) Adlî sicildeki bilgiler;

- a) Cezanın veya güvenlik tedbirinin infazının tamamlanması,
- b) Ceza mahkûmiyetini bütün sonuçlarıyla ortadan kaldıran şikayetten vazgeçme veya etkin pişmanlık,
- c) Ceza zamanaşımının dolması,
- d) Genel af,

Halinde Adlî Sicil ve İstatistik Genel Müdürlüğünce silinerek, arşiv kaydına alınır.

(2) Adlî sicil bilgileri, ilgilinin ölümü üzerine tamamen silinir.

(3) Türk vatandaşları hakkında yabancı mahkemelerce verilmiş olup 4 üncü maddenin birinci fıkrasının (f) bendine göre adlî sicile kaydedilen hürriyeti bağlayıcı cezaya mahkûmiyet hükümleri, kesinleştiği tarihten itibaren mahkûmiyet kararında belirtilen sürenin geçmesiyle, Adlî Sicil ve İstatistik Genel Müdürlüğüne adlî sicil kayıtlarından çıkartılarak arşiv kaydına alınır. Adlî para cezasına mahkûmiyet hükümleri ile cezanın ertelenmesine ilişkin hükümler, adlî sicil kaydına alınmadan doğrudan arşive kaydedilir.

Arşiv bilgilerinin istenmesi

Madde 10- (1) Arşiv bilgileri;

- a) Kullanılış amacı belirtilmek suretiyle, kişinin kendisi veya vekâletnamede açıkça belirtilmiş olmak koşuluyla vekili,
- b) Bir soruşturma veya kovuşturma kapsamında Cumhuriyet başsavcılıkları, hâkim veya mahkemeler,
- c) Yetkili seçim kurulları,
- d) Özel kanunlarda gösterilen hallerde ilgili kamu kurum ve kuruluşları,

Tarafından istenebilir.

(2) Kanunda açıkça belirtilmediği takdirde, kişi hakkında alınacak bir karar veya yapılacak bir işlemle ilgili olarak, bir yakınının adlî sicil ve arşiv kayıtları istenemez ve bu bilgiler, kişiyi herhangi bir haktan yoksun bırakmak için dayanak olarak kullanılamaz.

(3) Onsekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebilir.

Adlî sicil ve arşiv bilgilerinin gizliliği

Madde 11- (1) Adlî sicil ve arşiv bilgileri gizlidir. Bu bilgiler, görevlilerce açıklanamaz ve bu Kanun hükümlerine göre verilen kişi, kurum ve kuruluşlarca veriliş amacı dışında kullanılamaz.

Adlî sicil ve arşiv bilgilerinin silinmesi

Madde 12- (1) (Değişik: 5/4/2012-6290/2 md.) Arşiv bilgileri;

- a) İlgilinin ölümü üzerine,
- b) Anayasanın 76 ncı maddesi ile Türk Ceza Kanunu dışındaki kanunlarda bir hak yoksunluğuna neden olan mahkûmiyetler bakımından kaydın arşive alınma koşullarının oluştuğu tarihten itibaren;

1. Yasaklanmış hakların geri verilmesi kararı alınması koşuluyla onbeş yıl geçmesiyle,
2. Yasaklanmış hakların geri verilmesi kararı alınması koşulu aranmaksızın otuz yıl geçmesiyle,
- c) Diğer mahkûmiyetler bakımından kaydın arşive alınma koşullarının oluştuğu tarihten itibaren beş yıl geçmesiyle,

tamamen silinir.

(2) Fiilin kanunla suç olmaktan çıkarılması halinde, bu suçtan mahkûmiyete ilişkin adlî sicil ve arşiv kayıtları, talep aranmaksızın tamamen silinir.

(3) Kanun yararına bozma veya yargılamanın yenilenmesi sonucunda verilen beraat veya ceza verilmesine yer olmadığı kararının kesinleşmesi halinde, önceki mahkûmiyet kararına ilişkin adlî sicil ve arşiv kaydı tamamen silinir.

(4) (Ek: 24/11/2016-6763/40 md.) Akıl hastalığı nedeniyle hükmedilen güvenlik tedbirlerine ilişkin kayıtlar, infazının tamamlanmasıyla tamamen silinir.

Adlî sicil ve arşiv kayıtlarında sorgulama yetkisi verilmesi

Madde 13- (1) Bir suça ilişkin soruşturma ve kovuşturma kapsamında adlî sicil ve arşiv kayıtlarında;

a) Mahkeme, hâkim ve Cumhuriyet Başsavcılığı doğrudan doğruya,

b) Kolluk ve diğer kamu kurum ve kuruluşları Adalet Bakanının onayı ile,

Sorgulama yapabilirler.

(2) (Ek: 4/7/2012-6353/32 md.) Kamu kurum ve kuruluşları, mevzuatın adli sicil ve arşiv kaydı alınmasını öngördüğü hallerde, Adalet Bakanlığının belirleyeceği usul ve esaslar çerçevesinde ilgili kişiler hakkında adli sicil ve arşiv kayıtlarında sorgulama yapabilirler. Gerçek kişiler de kendileriyle ilgili adli sicil ve arşiv kayıtlarını, Adalet Bakanlığının belirleyeceği usul ve esaslar çerçevesinde ve güvenli kimlik doğrulama araçlarını kullanarak sorgulayabilir, sonucu fiziki veya elektronik ortamda merciine verebilirler.

Yasaklanmış hakların geri verilmesi

Madde 13/A - (Ek: 6/12/2006-5560/38 md.)

(1) 5237 sayılı Türk Ceza Kanunu dışındaki kanunların belli bir suçtan dolayı veya belli bir cezaya mahkûmiyete bağladığı hak yoksunluklarının giderilebilmesi için, yasaklanmış hakların geri verilmesi yoluna gidilebilir. Bunun için; Türk Ceza Kanununun 53 üncü maddesinin beşinci ve altıncı fıkraları saklı kalmak kaydıyla,

a) Mahkûm olunan cezanın infazının tamamlandığı tarihten itibaren üç yıllık bir sürenin geçmiş olması,

b) Kişinin bu süre zarfında yeni bir suç işlememiş olması ve hayatını iyi halli olarak sürdürdüğü hususunda mahkemede bir kanaat oluşması,

gerekir.

(2) Mahkûm olunan cezanın infazına genel af veya etkin pişmanlık dışında başka bir hukukî nedenle son verilmiş olması halinde, yasaklanmış hakların geri verilmesi yoluna gidilebilmesi için, hükmün kesinleştiği tarihten itibaren beş yıl geçmesi gerekir. Ancak, bu süre kişinin mahkûm olduğu hapis cezasına üç yıl eklenmek suretiyle bulunacak süreden az olamaz.

(3) Yasaklanmış hakların geri verilmesi için, hükümlünün veya vekilinin talebi üzerine, hükmü veren mahkemenin veya hükümlünün ikametgâhının bulunduğu yerdeki aynı derecedeki mahkemenin karar vermesi gerekir.

(4) Mahkeme bu husustaki kararını, dosya üzerinde inceleme yaparak ya da Cumhuriyet savcısını ve hükümlüyü dinlemek suretiyle verebilir.

(5) Yasaklanmış hakların geri verilmesi talebi üzerine mahkemenin verdiği karara karşı, hükümle ilgili olarak Ceza Muhakemesi Kanununda öngörülen kanun yoluna başvurulabilir.

(6) Yasaklanmış hakların geri verilmesine ilişkin karar, kesinleşmesi halinde, adlî sicil arşivine kaydedilir.

(7) Yasaklanmış hakların geri verilmesi yoluna başvurulması nedeniyle oluşan bütün masraflar hükümlü tarafından karşılanır.

Komisyon

Madde 14- (1) Adlî sicil ve arşiv kayıtlarının silinmesiyle ilgili kararları almak ve kanunla verilen diğer görevleri yerine getirmek üzere, Adlî Sicil ve İstatistik Genel Müdürlüğünün teklifi ve Bakan onayı ile üç hâkimden oluşan bir komisyon kurulur.

Yönetmelik

Madde 15- (1) Bu Kanunun uygulama usul ve esasları, yürürlüğe girdiği tarihten itibaren altı ay içinde Adalet Bakanlığınca çıkartılacak yönetmelikte belirlenir.

Merkezî ve mahalli adlî sicildeki atamalar

Madde 16- (1) Merkezî ve mahalli adlî sicildeki şube müdürü, mühendis, çözümleyici, programcı, istatistik uzmanı, tercüman, şef, bilgisayar işletmeni ile veri hazırlama ve kontrol işletmenleri Adalet Bakanlığınca atanırlar; gerektiğinde sözleşmeli olarak da çalıştırılabilirler.

Malî hükümler

Madde 17- (Mülga: 4/7/2012-6353/33 md.)

Yürürlükten kaldırılan hükümler

Madde 18- (1) Bu Kanunun yürürlüğe girdiği tarih itibarıyla 22.11.1990 tarihli ve 3682 sayılı Adlî Sicil Kanunu yürürlükten kaldırılmıştır.

Geçici Madde 1- (1) Bu Kanunda öngörülen adlî sicil sistemi ile mevcut kayıtların bu Kanuna uyarlanması bu Kanunun yürürlüğe girdiği tarihten itibaren beş yıl içinde tamamlanır.

Geçici Madde 2- (1) Bu Kanunun yürürlüğe girdiği tarihte, Adalet Bakanlığı Adlî Sicil ve İstatistik Genel Müdürlüğünce toplanmış olsun veya olmasın, suç tarihi itibarıyla bu Kanunun yürürlük tarihinden önceki kayıtlar hakkında, 3682 sayılı Kanuna göre süre yönünden silinme koşulu oluşmaları halinde, diğer kayıtlar için bu Kanun hükümlerine göre işlem yapılır. (Mülga ikinci cümle: 5/4/2012-6290/3 md.)

(2) (Değişik: 5/4/2012-6290/3 md.) Bu Kanunun yayımı tarihinde, Anayasanın 76 ncı maddesi ile bazı özel kanunlarda yer alan ve bir hak yoksunluğuna neden olan mahkûmiyetler bakımından, arşive alınan veya şartları oluştuğu halde ya da henüz şartları oluşmadığı için arşive alınmayan kayıtlar hakkında 12 nci maddenin birinci fıkrası hükmü uygulanır.

(3) (Ek: 5/4/2012-6290/3 md.) İkinci fıkrada sayılanlar dışında, birinci fıkra gereğince işlem yapılarak arşive alınan kayıtlar 3682 sayılı Kanunun 8 inci maddesinde öngörülen sürelerin dolduğu veya ertelenmiş olan mahkûmiyetin esasen vaki olmamış sayıldığı hallerde bu tarih esas alınarak Adli Sicil ve İstatistik Genel Müdürlüğünce silinir.

Yürürlük

Madde 19- (1) Bu Kanun 1 Haziran 2005 tarihinde yürürlüğe girer.

Yürütme

Madde 20- (1) Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

5271 sayılı Ceza Muhakemesi Kanunu

Resmî Gazete Tarihi : 17/12/2004

Resmî Gazete Sayısı : 25673

CEZA MUHAKEMESİ KANUNU

BİRİNCİ KİTAP

Genel Hükümler

BİRİNCİ KISIM

Kapsam, Tanımlar, Görev ve Yetki

BİRİNCİ BÖLÜM

Kapsam ve Tanımlar

Kanunun kapsamı

Madde 1 - (1) Bu Kanun, ceza muhakemesinin nasıl yapılacağı hususundaki kurallar ile bu sürece katılan kişilerin hak, yetki ve yükümlülüklerini düzenler.

(...)

Elektronik işlemler

Madde 38/A - (Ek: 2/7/2012-6352/95 md.)

(1) Her türlü ceza muhakemesi işlemlerinde Ulusal Yargı Ağı Bilişim Sistemi (UYAP) kullanılır. Bu işlemlere ilişkin her türlü veri, bilgi, belge ve karar, UYAP vasıtasıyla işlenir, kaydedilir ve saklanır.

(2) Kanunlarda gösterilen istisnalar hariç olmak üzere, dosyalar güvenli elektronik imza kullanılarak UYAP'tan incelenebilir ve her türlü ceza muhakemesi işlemi yapılabilir.

(3) Bu Kanun kapsamında fiziki olarak hazırlanması öngörülen her türlü belge ve karar elektronik ortamda düzenlenebilir, işlenebilir, saklanabilir ve güvenli elektronik imza ile imzalanabilir.

(4) Güvenli elektronik imza ile imzalanan belge ve kararlar diğer kişi veya kurumlara elektronik ortamda gönderilir. Güvenli elektronik imza ile imzalanarak gönderilen belge veya kararlar, gerekmedikçe fiziki olarak ayrıca düzenlenmez ve ilgili kurum ve kişilere gönderilmez.

- (5) Elektronik imzalı belgenin elle atılan imzalı belgeyle çelişmesi halinde UYAP'ta kayıtlı olan güvenli elektronik imzalı belge geçerli kabul edilir.
- (6) Güvenli elektronik imza ile imzalanan belge ve kararlarda, mühürleme işlemi ile kanunlarda birden fazla nüshanın düzenlenmesini öngören hükümler uygulanmaz.
- (7) Zorunlu nedenlerle fiziki olarak düzenlenmiş belge veya kararlar, yetkili kişilerce taranarak UYAP'a aktarılır ve gerektiğinde ilgili birimlere elektronik ortamda gönderilir.
- (8) Elektronik ortamdan fiziki örnek çıkartılması gereken hallerde tutanak veya belgenin aslının aynı olduğu belirtilerek hâkim, Cumhuriyet savcısı veya görevlendirilen yetkili kişi tarafından imzalanır ve mühürlenir.
- (9) Elektronik ortamda yapılan işlemlerde süre gün sonunda biter.
- (10) Yargı birimlerinin ihtiyaç duyduğu nüfus, tapu, adlî sicil kaydı gibi dış bilişim sistemlerinden UYAP vasıtasıyla temin edilen bilgi, belge ve kayıtlar, zorunlu olmadıkça ayrıca fiziki olarak istenilmez. UYAP'tan dış bilişim sistemlerine gönderilen bilgi ve belgeler ayrıca zorunlu olmadıkça fiziki ortamda gönderilmez.
- (11) Ceza muhakemesi işlemlerinin UYAP'ta yapılmasına dair usul ve esaslar, Adalet Bakanlığı tarafından çıkarılacak yönetmelikle düzenlenir.
- (...)

Şüpheli veya sanığın beden muayenesi ve vücudundan örnek alınması

Madde 75 - (Değişik: 25/5/2005 - 5353/2 md.)

- (1) Bir suçla ilişkin delil elde etmek için şüpheli veya sanık üzerinde iç beden muayenesi yapılabilmesine ya da vücuttan kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak gibi örnekler alınabilmesine; Cumhuriyet savcısı veya mağdurun istemiyle ya da re'sen hâkim veya mahkeme, gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından karar verilebilir. Cumhuriyet savcısının kararı, yirmidört saat içinde hâkim veya mahkemenin onayına sunulur. Hâkim veya mahkeme, yirmidört saat içinde kararını verir. Onaylanmayan kararlar hükümsüz kalır ve elde edilen deliller kullanılamaz.
- (2) İç beden muayenesi yapılabilmesi veya vücuttan kan veya benzeri biyolojik örnekler alınabilmesi için müdahalenin, kişinin sağlığına zarar verme tehlikesinin bulunmaması gerekir.
- (3) İç beden muayenesi veya vücuttan kan veya benzeri biyolojik örnekler alınması, ancak tabip veya sağlık mesleği mensubu diğer bir kişi tarafından yapılabilir.

- (4) Cinsel organlar veya anüs bölgesinde yapılan muayene de iç beden muayenesi sayılır.
- (5) Üst sınırı iki yıldan daha az hapis cezasını gerektiren suçlarda, kişi üzerinde iç beden muayenesi yapılamaz; kişiden kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak gibi örnekler alınmaz.
- (6) Bu madde gereğince alınacak hâkim veya mahkeme kararlarına itiraz edilebilir.
- (7) Özel kanunlardaki alkol muayenesine ve kan örneği alınmasına ilişkin hükümler saklıdır.
- (...)

Genetik inceleme sonuçlarının gizliliği

Madde 80 - (Değişik: 25/5/2005 - 5353/4 md.)

- (1) 75, 76 ve 78 inci madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez.
- (2) Bu bilgiler, kovuşturmayaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde Cumhuriyet savcısının huzurunda derhâl yok edilir ve bu husus dosyasında muhafaza edilmek üzere tutanağa geçirilir.

Fizik kimliğin tespiti

Madde 81 - (Değişik: 25/5/2005 - 5353/5 md.)

- (1) Üst sınırı iki yıl veya daha fazla hapis cezasını gerektiren bir suçtan dolayı şüpheli veya sanığın, kimliğinin tespiti için gerekli olması halinde, Cumhuriyet savcısının emriyle fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup tespitini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri kayda alınarak, soruşturma ve kovuşturma işlemlerine ilişkin dosyaya konulur.
- (2) Kovuşturmayaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde söz konusu kayıtlar Cumhuriyet savcısının huzurunda derhâl yok edilir ve bu husus tutanağa geçirilir.

(...)

DÖRDÜNCÜ BÖLÜM

Arama ve Elkoyma

Şüpheli veya sanıkla ilgili arama

Madde 116 - (1) Yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa; şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerler aranabilir.

Diğer kişilerle ilgili arama

Madde 117 - (1) Şüphelinin veya sanığın yakalanabilmesi veya suç delillerinin elde edilebilmesi amacıyla, diğer bir kişinin de üstü, eşyası, konutu, işyeri veya ona ait diğer yerler aranabilir.

(2) Bu hâllerde aramanın yapılması, aranılan kişinin veya suçun delillerinin belirtilen yerlerde bulunduğu kabul edilebilmesine olanak sağlayan olayların varlığına bağlıdır.

(3) Bu sınırlama, şüphelinin veya sanığın bulunduğu yerler ile, izlendiği sırada girdiği yerler hakkında geçerli değildir.

Gece yapılacak arama

Madde 118 - (1) Konutta, işyerinde veya diğer kapalı yerlerde gece vaktinde arama yapılamaz.

(2) Suçüstü veya gecikmesinde sakınca bulunan hâller ile yakalanmış veya gözaltına alınmış olup da firar eden kişi veya tutuklu veya hükümlünün tekrar yakalanması amacıyla yapılan aramalarda, birinci fıkra hükmü uygulanmaz.

Arama kararı

Madde 119 - (1) (Değişik : 25/5/2005 - 5353/15 md.) Hâkim kararı üzerine veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının, Cumhuriyet savcısına ulaşamadığı hallerde ise kolluk amirinin yazılı emri ile kolluk görevlileri arama yapabilirler. Ancak, konutta, işyerinde ve kamuya açık olmayan kapalı alanlarda arama, hâkim kararı veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının yazılı emri ile yapılabilir. Kolluk amirinin yazılı emri ile yapılan arama sonuçları Cumhuriyet Başsavcılığına derhal bildirilir.

(2) Arama karar veya emrinde;

a) Aramanın nedenini oluşturan fiil,

b) Aranılacak kişi, aramanın yapılacağı konut veya diğer yerin adresi ya da eşya,

c) Karar veya emrin geçerli olacağı zaman süresi,

Açıkça gösterilir.

(3) Arama tutanağına işlemi yapanların açık kimlikleri yazılır. (Mülga ikinci cümle: 25/5/2005 - 5353/15 md.)

(4) Cumhuriyet savcısı hazır olmaksızın konut, işyeri veya diğer kapalı yerlerde arama yapabilmek için o yer ihtiyar heyetinden veya komşulardan iki kişi bulundurulur.

(5) (Değişik: 25/7/2018-7145/14 md.) Askerî mahallerde yapılacak arama, Cumhuriyet savcısının nezaretinde askerî makamların katılımıyla adlî kolluk görevlileri tarafından yerine getirilir. Gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının yazılı emriyle de askerî makamların katılımıyla adlî kolluk görevlileri tarafından arama yapılabilir.

Aramada hazır bulunabilecekler

Madde 120 - (1) Aranacak yerlerin sahibi veya eşyanın zilyedi aramada hazır bulunabilir; kendisi bulunmazsa temsilcisi veya ayırt etme gücüne sahip hısımlarından biri veya kendisiyle birlikte oturmakta olan bir kişi veya komşusu hazır bulundurulur.

(2) 117 nci maddenin birinci fıkrasında gösterilen hâllerde zilyet ve bulunmazsa yerine çağrılacak kişiye, aramaya başlamadan önce aramanın amacı hakkında bilgi verilir.

(3) Kişinin avukatının aramada hazır bulunmasına engel olunamaz.

Arama sonunda verilecek belge

Madde 121 - (1) Aramanın sonunda hakkında arama işlemi uygulanan kimseye istemi üzerine aramanın 116 ve 117 nci maddelere göre yapıldığını ve 116 ncı maddede gösterilen durumda soruşturma veya kovuşturma konusu fiilin niteliğini belirten bir belge ve istemi üzerine elkonulan veya koruma altına alınan eşyanın listesini içeren bir defter ve eğer şüpheyi haklı kılan bir şey elde edilmemiş ise bunu belirten bir belge verilir.

(2) Birinci fıkrada belirtilen belgelerde, hakkında arama işlemi uygulanan kimsenin, elkonulan eşyanın mülkiyetine ilişkin görüş ve iddialarına da yer verilir.

(3) Koruma altına alınan veya elkonulan eşyanın tam bir defteri yapılır ve bu eşya resmî mühürle mühürlenir veya bir işaret konulur.

Belge veya kâğıtları inceleme yetkisi

Madde 122 - (1) Hakkında arama işlemi uygulanan kimsenin belge veya kâğıtlarını inceleme yetkisi, Cumhuriyet savcısı ve hâkime aittir.

(2) Belge ve kâğıtların zilyedi veya temsilcisi kendi mührünü de koyabilir veya imzasını atabilir. İleride mührün kaldırılmasına ve kâğıtların incelenmesine karar verildiğinde bu işlemin yapılmasında hazır bulunmak üzere, zilyedi veya temsilcisi ya da müdafii veya vekili çağrılır; çağrıya uyulmadığında gerekli işlem yapılır.

(3) İnceleme sonucu soruşturma veya kovuşturma konusu suça ilişkin olmadığı anlaşılan belge veya kâğıtlar ilgisine geri verilir.

Eşya veya kazancın muhafaza altına alınması ve bunlara elkonulması

Madde 123 - (1) İspat aracı olarak yararlı görülen ya da eşya veya kazanç müsaderesinin konusunu oluşturan malvarlığı değerleri, muhafaza altına alınır.

(2) Yanında bulunduran kişinin rızasıyla teslim etmediği bu tür eşyaya elkonulabilir.

(3) (Ek:27/12/2020-7262/19 md.) Muhafaza altına alınan veya elkonulan eşya ya da malvarlığı değerlerinin kıymeti tespit edilir.

İstenen eşyayı vermeyenler hakkında yapılacak işlem

Madde 124 - (1) 123 üncü maddede yazılı eşya veya diğer malvarlığı değerlerini yanında bulunduran kişi, istem üzerine bu şeyi göstermek ve teslim etmekle yükümlüdür.

(2) Kaçınma hâlinde bu şeyin zilyedi hakkında 60 ıncı maddede yer alan disiplin hapsine ilişkin hükümler uygulanır. Ancak, şüpheli veya sanık ya da tanıklıktan çekinebilecekler hakkında bu hüküm uygulanmaz.

İçeriği Devlet sırrı niteliğindeki belgelerin mahkemece incelenmesi

Madde 125 - (1) Bir suç olgusuna ilişkin bilgileri içeren belgeler, Devlet sırrı olarak mahkemeye karşı gizli tutulamaz.

(2) Devlet sırrı niteliğindeki bilgileri içeren belgeler, ancak mahkeme hâkimi veya heyeti tarafından incelenebilir. Bu belgelerde yer alan ve sadece yüklenen suçu açıklığa kavuşturabilecek nitelikte olan bilgiler, hâkim veya mahkeme başkanı tarafından tutanağa kaydettirilir.

(3) Bu madde hükmü, hapis cezasının alt sınırı beş yıl veya daha fazla olan suçlarla ilgili olarak uygulanır.

Elkonulamayacak mektuplar, belgeler

Madde 126 - (1) Şüpheli veya sanık ile 45 ve 46 ncı maddelere göre tanıklıktan çekinebilecek kimseler arasındaki mektuplara ve belgelere; bu kimselerin nezdinde bulundukça elkonulamaz.

Elkoyma kararını verme yetkisi

Madde 127 - (1) (Değişik: 25/5/2005 - 5353/16 md.) Hâkim kararı üzerine veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının, Cumhuriyet savcısına ulaşamadığı hallerde ise kolluk amirinin yazılı emri ile kolluk görevlileri, elkoyma işlemini gerçekleştirebilir.

(2) Kolluk görevlisinin açık kimliği, elkoyma işlemine ilişkin tutanağa geçirilir.

(3) (Değişik: 25/5/2005 - 5353/16 md.) Hâkim kararı olmaksızın yapılan elkoyma işlemi, yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını elkoymadan itibaren kırksekiz saat içinde açıklar; aksi hâlde elkoyma kendiliğinden kalkar.

(4) Zilyedliğinde bulunan eşya veya diğer malvarlığı değerlerine elkonulan kimse, hâkimden her zaman bu konuda bir karar verilmesini isteyebilir.

(5) Elkoyma işlemi, suçtan zarar gören mağdura gecikmeksizin bildirilir.

(6) (Değişik: 25/7/2018-7145/15 md.) Askerî mahallerde yapılacak elkoyma işlemi, Cumhuriyet savcısının nezaretinde askerî makamların katılımıyla adli kolluk görevlileri tarafından yerine getirilir. Gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının yazılı emriyle de askerî makamların katılımıyla adli kolluk görevlileri tarafından elkoyma işlemi yapılabilir.

Taşınmazlara, hak ve alacaklara elkoyma

Madde 128 - (1) Soruşturma veya kovuşturma konusu suçun işlendiğine ve bu suçlardan elde edildiğine dair somut delillere dayanan kuvvetli şüphe sebebi bulunan hallerde, şüpheli veya sanığa ait;

a) Taşınmazlara,

b) Kara, deniz veya hava ulaşım araçlarına,

c) Banka veya diğer malî kurumlardaki her türlü hesaba,

d) Gerçek veya tüzel kişiler nezdindeki her türlü hak ve alacaklara,

e) Kıymetli evraka,

f) Ortağı bulunduğu şirketteki ortaklık paylarına,

g) Kiralık kasa mevcutlarına,

h) Diğer malvarlığı değerlerine,

Elkonulabilir. Somut olarak belirlenen Bu taşınmaz, hak, alacak ve diğer malvarlığı değerlerinin şüpheli veya sanıktan başka bir kişinin zilyetliğinde bulunması halinde dahi, elkoyma işlemi yapılabilir. (Ek cümle: 21/2/2014 - 6526/10 md.) Bu madde kapsamında elkoyma kararı alınabilmesi için ilgisine göre Bankacılık Düzenleme ve Denetleme Kurumu, Sermaye Piyasası Kurulu, Mali Suçları Araştırma Kurulu, Hazine Müsteşarlığı ve Kamu Gözetimi, Muhasebe ve Denetim

Standartları Kurumundan, suçtan elde edilen değere ilişkin rapor alınır. Bu rapor en geç üç ay içinde hazırlanır. Özel sebepler zorunlu kıldığında bu süre talep üzerine iki ay daha uzatılabilir.

(2) Birinci fıkra hükmü;

a) Türk Ceza Kanununda tanımlanan;

1. Soykırım ve insanlığa karşı suçlar (madde 76, 77, 78),
 2. Göçmen kaçakçılığı ve insan ticareti (madde 79, 80) ile organ veya doku ticareti (madde 91),
 3. Hırsızlık (madde 141, 142),
 4. Yağma (madde 148, 149),
 5. Güveni kötüye kullanma (madde 155),
 6. Dolandırıcılık (madde 157, 158),
 7. Hileli iflas (madde 161),
 8. Uyuşturucu veya uyarıcı madde imal ve ticareti (madde 188),
 9. Parada sahtecilik (madde 197),
 10. (Mülga: 21/2/2014 - 6526/10 md.; Yeniden düzenleme: 24/11/2016-6763/25 md.) Suç işlemek amacıyla örgüt kurma (madde 220, fıkra üç),
 11. İhaleye fesat karıştırma (madde 235),
 12. Edimin ifasına fesat karıştırma (madde 236),
 13. (Ek: 24/11/2016-6763/25 md.) Tefecilik (madde 241),
 14. Zimmet (madde 247),
 15. İrtikap (madde 250)
 16. Rüşvet (madde 252),
 17. Devletin Güvenliğine Karşı Suçlar (madde 302, 303, 304, 305, 306, 307, 308),
 18. (Değişik: 2/12/2014-6572/41 md.) Anayasal Düzene ve Bu Düzenin İşleyişine Karşı Suçlar (madde 309, 311, 312, 313, 314, 315, 316),
 19. Devlet Sırlarına Karşı Suçlar ve Casusluk (madde 328, 329, 330, 331, 333, 334, 335, 336, 337) suçları.
- b) Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanunda tanımlanan silah kaçakçılığı (madde 12) suçları,

- c) Bankalar Kanununun 22 nci maddesinin (3) ve (4) numaralı fıkralarında tanımlanan zimmet suçu,
d) Kaçakçılıkla Mücadele Kanununda tanımlanan ve hapis cezasını gerektiren suçlar,
e) Kültür ve Tabiat Varlıklarını Koruma Kanununun 68 ve 74 üncü maddelerinde tanımlanan suçlar,
Hakkında uygulanır.

(3) Taşınmaza elkonulması kararı, tapu kütüğüne şerh verilmek suretiyle icra edilir.

(4) Kara, deniz ve hava ulaşım araçları hakkında verilen elkoyma kararı, bu araçların kayıtlı bulunduğu sicile şerh verilmek suretiyle icra olunur.

(5) Banka veya diğer malî kurumlardaki her türlü hesaba elkonulması kararı, teknik iletişim araçlarıyla ilgili banka veya malî kuruma derhâl bildirilerek icra olunur. Söz konusu karar, ilgili banka veya malî kuruma ayrıca tebliğ edilir. Elkoyma kararı alındıktan sonra, hesaplar üzerinde yapılan bu kararı etkisiz kılmaya yönelik işlemler geçersizdir.

(6) Şirketteki ortaklık paylarına elkoyma kararı, ilgili şirket yönetimine ve şirketin kayıtlı bulunduğu ticaret sicili müdürlüğüne teknik iletişim araçlarıyla derhâl bildirilerek icra olunur. Söz konusu karar, ilgili şirkete ve ticaret sicili müdürlüğüne ayrıca tebliğ edilir.

(7) Hak ve alacaklara elkoyma kararı, ilgili gerçek veya tüzel kişiye teknik iletişim araçlarıyla derhâl bildirilerek icra olunur. Söz konusu karar, ilgili gerçek veya tüzel kişiye ayrıca tebliğ edilir.

(8) Bu madde hükmüne göre alınan elkoyma kararının gereklerine aykırı hareket edilmesi halinde, Türk Ceza Kanununun "Muhafaza görevini kötüye kullanma" başlıklı 289 uncu maddesi hükümleri uygulanır.

(9) (Değişik: 24/11/2016-6763/25 md.) Bu madde hükümlerine göre elkoymaya ve onuncu fıkra uyarınca kayyım atanmasına ancak hâkim karar verebilir.

(10) (Ek: 15/8/2016-KHK-674/13 md.; Aynen kabul: 10/11/2016-6758/13 md.) Bu madde uyarınca elkonulan taşınmaz, hak ve alacakların idaresi gerektiğinde bu malvarlığı değerlerinin yönetimi amacıyla kayyım atanabilir. Bu durumda 133 üncü madde hükümleri kıyasen uygulanır.

Postada elkoyma

Madde 129 - (1) Suçun delillerini oluşturduğundan şüphe edilen ve gerçeğin ortaya çıkarılması için soruşturma ve kovuşturmada adliyenin eli altında olması zorunlu sayılıp, posta hizmeti veren her türlü resmî veya özel kuruluşta bulunan gönderilere, hâkimin veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının kararı ile elkonulabilir.

(2) Hâkim kararının veya Cumhuriyet savcısının emrinin kendilerine bildirilmesi üzerine elkoyma işlemini yerine getiren kolluk memurları, birinci fıkrada belirtilen gönderilerin içinde bulunduğu zarfları veya paketleri açamazlar. Elkonulan gönderiler, ilgili posta görevlilerinin huzuru ile mühür altına alınıp derhâl elkoyma kararını veya emrini veren hâkim veya Cumhuriyet savcısına teslim edilir.

(3) (Ek:20/11/2017-KHK-696/94 md.; Aynen kabul: 1/2/2018-7079/89 md.) (1) Elkoyma kararı veya emrinin aşağıda sayılan suçlarla ilgili olarak verilmesi halinde gönderilerin bulunduğu zarf veya paketler Cumhuriyet savcısının talimatıyla kolluk memurları tarafından açılabilir.

a) 5237 sayılı Türk Ceza Kanununda yer alan;

1. Tehlikeli maddelerin izinsiz olarak bulundurulması veya el değiştirmesi (madde 174),

2. Uyuşturucu veya uyarıcı madde imal ve ticareti (madde 188),

suçları.

b) 10/7/1953 tarihli ve 6136 sayılı Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanununun 12 nci ve 13 üncü maddelerinde tanımlanan suçlar.

c) 21/7/1983 tarihli ve 2863 sayılı Kültür ve Tabiat Varlıklarını Koruma Kanununun 67 nci ve 68 inci maddelerinde tanımlanan suçlar.

(4) Soruşturma ve kovuşturmanın amacına zarar vermek olasılığı bulunmadıkça, alınmış tedbirler ilgililere bildirilir.

(5) Açılmamasına veya açılıp da içeriği bakımından adliyenin eli altında tutulmasına gerek bulunmadığına karar verilen gönderiler, hemen ilgililerine teslim olunur.

Avukat bürolarında arama, elkoyma ve postada elkoyma

Madde 130 - (1) Avukat büroları ancak mahkeme kararı ile ve kararda belirtilen olayla ilgili olarak Cumhuriyet savcısının denetiminde aranabilir. Baro başkanı veya onu temsil eden bir avukat aramada hazır bulundurulur.

(2) Arama sonucu elkonulmasına karar verilen şeyler bakımından bürosunda arama yapılan avukat, baro başkanı veya onu temsil eden avukat, bunların avukat ile müvekkili arasındaki meslekî ilişkiye ait olduğunu öne sürerek karşı koyduğunda, bu şey ayrı bir zarf veya paket içerisine konularak hazır bulunanlarca mühürlenir ve bu konuda gerekli kararı vermesi, soruşturma evresinde sulh ceza hâkiminden, kovuşturma evresinde hâkim veya mahkemeden istenir. Yetkili hâkim elkonulan şeyin avukatla müvekkili arasındaki meslekî ilişkiye ait olduğunu saptadığında, elkonulan şey derhâl

avukata iade edilir ve yapılan işlemi belirten tutanaklar ortadan kaldırılır. Bu fıkrada öngörülen kararlar, yirmidört saat içinde verilir.

(3) Postada elkoyma durumunda bürosunda arama yapılan avukat veya baro başkanı veya onu temsil eden avukatın karşı koyması üzerine ikinci fıkrada belirtilen usuller uygulanır.

Elkonulan eşyanın iadesi

Madde 131 - (1) Şüpheliye, sanığa veya üçüncü kişilere ait elkonulmuş eşyanın, soruşturma ve kovuşturma bakımından muhafazasına gerek kalmaması veya müsadereye tabi tutulmayacağına anlaşılması halinde, re'sen veya istem üzerine geri verilmesine Cumhuriyet savcısı, hâkim veya mahkeme tarafından karar verilir. İstem reddi kararlarına itiraz edilebilir.

(2) 128 inci madde hükümlerine göre elkonulan eşya veya diğer malvarlığı değerleri, suçtan zarar gören mağdura ait olması ve bunlara delil olarak artık ihtiyaç bulunmaması halinde, sahibine iade edilir.

Elkonulan eşyanın muhafazası veya elden çıkarılması

Madde 132 - (1) Elkonulan eşya, zarara uğraması veya değerinde esaslı ölçüde kayıp meydana gelme tehlikesinin varlığı halinde, hükmün kesinleşmesinden önce elden çıkarılabilir.

(2) Elden çıkarma kararı, soruşturma evresinde hâkim, kovuşturma evresinde mahkeme tarafından verilir.

(3) Karar verilmeden önce eşyanın sahibi olan şüpheli, sanık veya ilgili diğer kişiler dinlenir; elden çıkarma kararı, kendilerine bildirilir.

(4) Elkonulan eşyanın değerinin muhafazası ve zarar görmemesi için gerekli tedbirler alınır.

(5) Elkonulan eşya, soruşturma evresinde Cumhuriyet Başsavcılığı, kovuşturma evresinde mahkeme tarafından, bakım ve gözetimiyle ilgili tedbirleri almak ve istendiğinde derhâl iade edilmek koşuluyla, muhafaza edilmek üzere, şüpheliye, sanığa veya diğer bir kişiye teslim edilebilir. Bu bırakma, teminat gösterilmesi koşuluna da bağlanabilir.

(6) Elkonulan eşya, delil olarak saklanmasına gerek kalmaması halinde, rayiç değerinin derhâl ödenmesi karşılığında, ilgiliye teslim edilebilir. Bu durumda müsadere kararının konusunu, ödenen rayiç değer oluşturur.

Şirket yönetimi için kayyım tayini

Madde 133 - (1) Suçun bir şirketin faaliyeti çerçevesinde işlenmekte olduğu hususunda kuvvetli şüphe sebeplerinin varlığı ve maddi gerçeğin ortaya çıkarılabilmesi için gerekli olması halinde; soruşturma ve kovuşturma sürecinde, hâkim veya mahkeme, şirket işlerinin yürütülmesiyle ilgili olarak kayyım atayabilir. Atama kararında, yönetim organının karar ve işlemlerinin geçerliliğinin kayyımın onayına bağlı kılındığı veya yönetim organının yetkilerinin ya da yönetim organının yetkileri ile birlikte ortaklık payları veya menkul kıymetler idare yetkilerinin tümüyle kayyıma verildiği açıkça belirtilir. Kayyım tayinine ilişkin karar, ticaret sicili gazetesinde ve diğer uygun vasıtalarla ilan olunur.

(2) Hâkim veya mahkemenin kayyım hakkında takdir etmiş bulunduğu ücret, şirket bütçesinden karşılanır. Ancak, soruşturma veya kovuşturma konusu suçtan dolayı kovuşturmaya yer olmadığı veya beraat kararının verilmesi halinde; ücret olarak şirket bütçesinden ödenen paranın tamamı, kanunî faiziyle birlikte Devlet Hazinesinden karşılanır.

(3) İlgililer, atanan kayyımın işlemlerine karşı, görevli mahkemeye 22.11.2001 tarihli ve 4721 sayılı Türk Medeni Kanunu ve 29.6.1956 tarihli ve 6762 sayılı Türk Ticaret Kanunu hükümlerine göre başvurabilirler.

(4) Bu madde hükümleri ancak aşağıda sayılan suçlarla ilgili olarak uygulanabilir.

a) Türk Ceza Kanununda yer alan,

1. Göçmen kaçakçılığı ve insan ticareti (madde 79, 80),
2. Uyuşturucu veya uyarıcı madde imal ve ticareti (madde 188),
3. Parada sahtecilik (madde 197),
4. Fuhuş (madde 227),
5. Kumar oynanması için yer ve imkân sağlama (madde 228),
6. Zimmet (madde 247),
7. Suçtan kaynaklanan malvarlığı değerlerini aklama (madde 282),
8. Silahlı örgüt (madde 314) veya bu örgütlere silah sağlama (madde 315),
9. Devlet Sırlarına Karşı Suçlar ve Casusluk (madde 328, 329, 330, 331, 333, 334, 335, 336, 337),

Suçları,

b) Ateşli Silahlar ve Bıçaklar İle Diğer Aletler Hakkında Kanunda tanımlanan silah kaçakçılığı (madde 12) suçları,

- c) Bankalar Kanununun 22 nci maddesinin (3) ve (4) numaralı fıkralarında tanımlanan zimmet suçu,
- d) Kaçakçılıkla Mücadele Kanununda tanımlanan ve hapis cezasını gerektiren suçlar,
- e) Kültür ve Tabiat Varlıklarını Koruma Kanununun 68 ve 74 üncü maddelerinde tanımlanan suçlar.

(5) (Ek: 1/7/2016-6723/32 md.) Bu madde uyarınca atanan kayyımların görevleriyle ilgili iş ve işlemlerinden dolayı tazminat davaları, 142 ila 144 üncü maddeler uyarınca Devlet aleyhine açılır. Devlet, ödediği tazminattan dolayı görevinin gereklerine aykırı hareket etmek suretiyle görevini kötüye kullanan kayyımlara bir yıl içinde rücu eder.

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma

Madde 134 - (1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine (...) (2) karar verilir. (Ek üç cümle: 25/7/2018-7145/16 md.) Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hâkim onayına sunulur. Hâkim kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edilir.

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşamaması ya da işlemin uzun sürecek olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

(4) Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır.

(...)

BEŞİNCİ BÖLÜM

Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi

İletişimin tespiti, dinlenmesi ve kayda alınması

Madde 135 - (1) (Değişik: 21/2/2014-6526/12 md.) Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi (...) (3) dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir. Cumhuriyet savcısı kararını derhâl hâkimin onayına sunar ve hâkim, kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde tedbir Cumhuriyet savcısı tarafından derhâl kaldırılır. (Mülga son iki cümle: 24/11/2016-6763/26 md.)

(2) (Ek: 21/2/2014-6526/12 md.) Talepte bulunulurken hakkında bu madde uyarınca tedbir kararı verilecek hattın veya iletişim aracının sahibini ve biliniyorsa kullanıcıyı gösterir belge veya rapor eklenir.

(3) Şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle arasındaki iletişimi kayda alınamaz. Kayda alma gerçekleşikten sonra bu durumun anlaşılması hâlinde, alınan kayıtlar derhâl yok edilir.

(4) Birinci fıkra hükmüne göre verilen kararda, yüklenen suçun türü, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, telefon numarası veya iletişim bağlantısını tespiti imkân veren kodu, tedbirin türü, kapsamı ve süresi belirtilir. Tedbir kararı en çok iki ay için verilebilir; bu süre, bir ay daha uzatılabilir. (Ek cümle: 25/5/2005 - 5353/17 md.) Ancak, örgütün faaliyeti çerçevesinde işlenen suçlarla ilgili olarak gerekli görülmesi halinde, hâkim yukarıdaki sürelerle ek olarak her defasında bir aydan fazla olmamak ve toplam üç ayı geçmemek üzere uzatılmasına karar verebilir.

(5) Şüpheli veya sanığın yakalanabilmesi için, (...) (1) mobil telefonun yeri, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının kararına istinaden tespit edilebilir. Bu hususa ilişkin olarak verilen kararda, (...) (1) mobil telefon numarası ve tespit işleminin süresi belirtilir. Tespit işlemi en çok iki ay için yapılabilir; bu süre, bir ay daha uzatılabilir.

(6) (Ek: 2/12/2014-6572/42 md.) Şüpheli ve sanığın telekomünikasyon yoluyla iletişiminin tespiti, soruşturma aşamasında hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı, kovuşturma aşamasında mahkeme kararına istinaden yapılır. Kararda, yüklenen suçun türü, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, telefon numarası veya iletişim bağlantısını tespiti imkân veren kodu ve tedbirin süresi belirtilir. (Ek cümleler: 24/11/2016-6763/26

md.) Cumhuriyet savcısı kararını yirmi dört saat içinde hâkimin onayına sunar ve hâkim, kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde kayıtlar derhâl imha edilir.

(7) Bu madde hükümlerine göre alınan karar ve yapılan işlemler, tedbir süresince gizli tutulur.

(8) Bu madde kapsamında dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesine ilişkin hükümler ancak aşağıda sayılan suçlarla ilgili olarak uygulanabilir:

a) Türk Ceza Kanununda yer alan;

1. Göçmen kaçakçılığı ve insan ticareti (madde 79, 80) ile organ veya doku ticareti (madde 91),

2. Kasten öldürme (madde 81, 82, 83),

3. İşkence (madde 94, 95),

4. Cinsel saldırı (birinci fıkra hariç, madde 102),

5. Çocukların cinsel istismarı (madde 103),

6. (Ek: 21/2/2014 - 6526/12 md.) Nitelikli hırsızlık (madde 142) ve yağma (madde 148, 149) ile nitelikli dolandırıcılık (madde 158),

7. Uyuşturucu veya uyarıcı madde imal ve ticareti (madde 188),

8. Parada sahtecilik (madde 197),

9. (Mülga: 21/2/2014 - 6526/12 md.; Yeniden düzenleme: 24/11/2016-6763/26 md.) Suç işlemek amacıyla örgüt kurma (madde 220, fıkra üç),

10. (Ek: 25/5/2005 - 5353/17 md.) Fuhuş (madde 227),

11. İhaleye fesat karıştırma (madde 235),

12. (Ek: 24/11/2016-6763/26 md.) Tefecilik (madde 241),

13. Rüşvet (madde 252),

14. Suçtan kaynaklanan malvarlığı değerlerini aklama (madde 282),

15. (Değişik: 2/12/2014-6572/42 md.) Devletin birliğini ve ülke bütünlüğünü bozmak (madde 302),

16. (Ek: 2/12/2014-6572/42 md.) Anayasal Düzene ve Bu Düzenin İşleyişine Karşı Suçlar (madde 309, 311, 312, 313, 314, 315, 316),

17. Devlet Sırlarına Karşı Suçlar ve Casusluk (madde 328, 329, 330, 331, 333, 334, 335, 336, 337) suçları.

b) Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanunda tanımlanan silah kaçakçılığı (madde 12) suçları.

c) (Ek: 25/5/2005 - 5353/17 md.) Bankalar Kanununun 22 nci maddesinin (3) ve (4) numaralı fıkralarında tanımlanan zimmet suçu,

d) Kaçakçılıkla Mücadele Kanununda tanımlanan ve hapis cezasını gerektiren suçlar.

e) Kültür ve Tabiat Varlıklarını Koruma Kanununun 68 ve 74 üncü maddelerinde tanımlanan suçlar.

(9) Bu maddede belirlenen esas ve usuller dışında hiç kimse, bir başkasının telekomünikasyon yoluyla iletişimini dinleyemez ve kayda alamaz.

(...)

Kararların yerine getirilmesi, iletişim içeriklerinin yok edilmesi

Madde 137 - (1) 135 inci maddeye göre verilecek karar gereğince Cumhuriyet savcısı veya görevlendireceği adli kolluk görevlisi, telekomünikasyon hizmeti veren kurum ve kuruluşların yetkililerinden iletişimin tespiti, dinlenmesi veya kayda alınması işlemlerinin yapılmasını ve bu amaçla cihazların yerleştirilmesini yazılı olarak istediğinde, bu istem derhâl yerine getirilir; yerine getirilmemesi hâlinde zor kullanılabilir. İşlemin başladığı ve bitirildiği tarih ve saat ile işlemi yapanın kimliği bir tutanakla saptanır.

(2) 135 inci maddeye göre verilen karar gereğince tutulan kayıtlar, Cumhuriyet Savcılığınca görevlendirilen kişiler tarafından çözümlenerek metin hâline getirilir. Yabancı dildeki kayıtlar, tercüman aracılığı ile Türkçe'ye çevrilir.

(3) 135 inci maddeye göre verilen kararın uygulanması sırasında şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da aynı maddenin birinci fıkrasına göre hâkim onayının alınamaması halinde, bunun uygulanmasına Cumhuriyet savcısı tarafından derhâl son verilir. Bu durumda, yapılan tespit veya dinlemeye ilişkin kayıtlar Cumhuriyet savcısının denetimi altında en geç on gün içinde yok edilerek, durum bir tutanakla tespit edilir. (Ek cümle:8/7/2021-7331/18 md.) Beraat kararı verilmesi durumunda da tespit veya dinlemeye ilişkin kayıtlar, hâkim denetimi altında aynı usulle yok edilir.

(4) Tespit ve dinlemeye ilişkin kayıtların yok edilmesi halinde soruşturma veya kovuşturma evresinin bitiminden itibaren, en geç onbeş gün içinde, Cumhuriyet başsavcılığı veya mahkeme, tedbirin nedeni, kapsamı, süresi ve sonucu hakkında ilgisine yazılı olarak bilgi verir.

Tesadüfen elde edilen deliller

Madde 138 - (1) Arama veya elkoyma koruma tedbirlerinin uygulanması sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ancak, diğer bir suçun işlendiği şüphesini uyandırabilecek bir delil elde edilirse; bu delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhâl bildirilir.

(...)

Duruşmada anlatılması zorunlu belge ve tutanaklar

Madde 209 - (1) Naip veya istinabe yoluyla sorgusu yapılan sanığa ait sorgu tutanakları, naip veya istinabe yoluyla dinlenen tanığın ifade tutanakları ile muayene ve keşif tutanakları gibi delil olarak kullanılacak belgeler ve diğer yazılar, adlî sicil özetleri ve sanığın kişisel ve ekonomik durumuna ilişkin bilgilerin yer aldığı belgeler, duruşmada anlatılır. (1)

(2) Sanığa veya mağdura ait kişisel verilerin yer aldığı belgelerin, açıkça istemeleri halinde, kapalı oturumda anlatılmasına mahkemece karar verilebilir.

(...)

Bilgi isteme

Madde 332 - (1) Suçların soruşturma ve kovuşturması sırasında Cumhuriyet savcısı, hâkim veya mahkeme tarafından yazılı olarak istenilen bilgilere on gün içinde cevap verilmesi zorunludur. Eğer bu süre içinde istenen bilgilerin verilmesi imkânsız ise, sebebi ve en geç hangi tarihte cevap verilebileceği aynı süre içinde bildirilir.

(2) Bilgi istenen yazıda yukarıdaki fıkra hükmü ile buna aykırı hareket etmenin Türk Ceza Kanununun 257 nci maddesine aykırılık oluşturabileceği yazılır. Bu durumda haklarında kamu davasının açılması, izin veya karar alınmasına bağlı bulunan kişiler hakkında, yasama dokunulmazlığı saklı kalmak üzere, doğrudan soruşturma yapılır.

5258 sayılı Aile Hekimliği Kanunu

Resmî Gazete Tarihi :

Resmî Gazete Sayısı :

AİLE HEKİMLİĞİ KANUNU

Amaç ve kapsam

Madde 1- Bu Kanunun amacı; Sağlık Bakanlığının (...) belirleyeceği illerde, birinci basamak sağlık hizmetlerinin geliştirilmesi, birey ihtiyaçları doğrultusunda koruyucu sağlık hizmetlerine ağırlık verilmesi, kişisel sağlık kayıtlarının tutulması ve bu hizmetlere eşit erişimin sağlanması amacıyla aile hekimliği hizmetlerinin yürütülebilmesini teminen görevlendirilecek veya çalıştırılacak sağlık personelinin statüsü ve malî hakları ile hizmetin esaslarını düzenlemektir.

(...)

Hizmetin esasları

Madde 5- (Değişik fıkra:15/11/2018-7151/27 md.) Aile hekimliği uygulaması kapsamında kişilerin aile hekimine kaydı yapılır. Sağlık Bakanlığınca belirlenen süre sonunda kişiler aile hekimlerini değiştirebilirler veya sağlık hizmet planlamasına uygun olarak Sağlık Bakanlığı kişilerin aile hekimini değiştirebilir. Her bir aile hekimi için kayıtlı kişi sayısı; coğrafi şartlar, sağlık hizmet planlaması gibi kriterler esas alınarak Hazine ve Maliye Bakanlığının görüşü alınarak Sağlık Bakanlığınca belirlenir.

Aile hekimliği hizmetleri ücretsizdir; acil haller hariç, haftada kırk saatten az olmamak kaydı ile Bakanlıkça belirlenen kıstaslar çerçevesinde ilgili aile hekiminin talebi ve o yerin sağlık idaresince onaylanan çalışma saatleri içinde yerine getirilir. (Ek cümle: 10/9/2014-6552/117 md.) Türkiye Halk Sağlığı Kurumunca belirlenen aile sağlığı merkezlerinde çalışma saatleri dışında, aile hekimleri ve aile sağlığı çalışanları ile gerektiğinde Sağlık Bakanlığı ve bağlı kuruluşları personeline nöbet görevi verilebilir. Aile hekimliği uygulamasına geçilen yerlerde acil haller ve mücbir sebepler dışında, kişi hangi sosyal güvenlik kuruluşuna tâbi olursa olsun, aile hekiminin sevki olmaksızın sağlık kurum ve kuruluşlarına müracaat edenlerden katkı payı alınır. Alınacak katkı payı tutarı Sağlık, Maliye ve Çalışma ve Sosyal Güvenlik bakanlıklarınca müştereken belirlenir. Aile hekimliği uygulamasına geçilen yerlerde, diğer kanunların aile hekimliği hizmetleri kapsamındaki hizmetlerin sunumu ile sevk ve müracaata ilişkin hükümleri uygulanmaz. (Ek cümle:11/10/2011-KHK-663/58 md.) Aile

hekimliđi hizmetleri dıřında kalan birinci basamak sađlık hizmetleri toplum sađlığı merkezleri tarafından verilir ve bu merkezlerin organizasyonu, kadroları, görevleri ile alıřma usul ve esasları Trkiye Halk Sađlığı Kurumunca belirlenir. Yabancılar hakkında ilgili mevzuat hkmleri uygulanır.

Aile hekimlerinin řahs kayıtları ilgili il ve ile sađlık idare birimlerinde tutulur. Aile hekimlerinin kullandığı basılı veya elektronik ortamda tutulan kayıtlar, kiřilerin sađlık dosyaları ile raporlar, sevk belgesi ve reete gibi belgeler resm kayıt ve evrak niteliğindedir. Bu kayıt ve belgeler, hekimin ayrılması veya kiřinin hekim deđiřtirmesi halinde eksiksiz olarak devredilir. İlgili mevzuatta birinci basamak sađlık kuruluřları ve resm tabiplerce dzenlenmesi ngrlen her trl rapor, sevk evrakı, reete ve sair belgeler, aile hekimliđi uygulamasına geilen yerlerde aile hekimleri tarafından dzenlenir.

5237 sayılı Türk Ceza Kanunu

Resmî Gazete Tarihi : 12.10.2004

Resmî Gazete Sayısı : 25611

TÜRK CEZA KANUNU

BİRİNCİ KİTAP

Genel Hükümler

BİRİNCİ KISIM

Temel İlkeler, Tanımlar ve Uygulama Alanı

BİRİNCİ BÖLÜM

Temel İlkeler ve Tanımlar

Ceza Kanununun amacı

Madde 1- (1) Ceza Kanununun amacı; kişi hak ve özgürlüklerini, kamu düzen ve güvenliğini, hukuk devletini, kamu sağlığını ve çevreyi, toplum barışını korumak, suç işlenmesini önlemektir. Kanunda, bu amacın gerçekleştirilmesi için ceza sorumluluğunun temel esasları ile suçlar, ceza ve güvenlik tedbirlerinin türleri düzenlenmiştir.

(...)

Tüzel kişiler hakkında güvenlik tedbirleri

Madde 60- (1) Bir kamu kurumunun verdiği izne dayalı olarak faaliyette bulunan özel hukuk tüzel kişinin organ veya temsilcilerinin iştirakiyle ve bu iznin verdiği yetkinin kötüye kullanılması suretiyle tüzel kişi yararına işlenen kasıtlı suçlardan mahkûmiyet halinde, iznin iptaline karar verilir.

(2) Müsadere hükümleri, yararına işlenen suçlarda özel hukuk tüzel kişileri hakkında da uygulanır.

(3) Yukarıdaki fıkralar hükümlerinin uygulanmasının işlenen fiile nazaran daha ağır sonuçlar ortaya çıkarabileceği durumlarda, hakim bu tedbirlere hükmetmeyebilir.

(4) Bu madde hükümleri kanunun ayrıca belirttiği hallerde uygulanır.

(...)

DOKUZUNCU BÖLÜM

Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar

Haberleşmenin gizliliğini ihlal

Madde 132- (1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır

(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.(1)

(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. (Ek cümle: 2/7/2012-6352/79 md.) İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.

(4) (Mülga: 2/7/2012-6352/79 md.)

Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması

Madde 133- (1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.

(3) (Değişik: 2/7/2012-6352/80 md.) Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adlî para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.

Özel hayatın gizliliğini ihlal

Madde 134- (1) Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.

(2) (Değişik: 2/7/2012-6352/81 md.) Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.

Kişisel verilerin kaydedilmesi

Madde 135- (1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.

(2) Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır.

Verileri hukuka aykırı olarak verme veya ele geçirme

Madde 136- (1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.

(2) (Ek:17/10/2019-7188/17 md.) Suçun konusunun, Ceza Muhakemesi Kanununun 236 ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır.

Nitelikli haller

Madde 137- (1) Yukarıdaki maddelerde tanımlanan suçların;

a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,

b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle,

İşlenmesi halinde, verilecek ceza yarı oranında artırılır.

Verileri yok etmeme

Madde 138- (1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.

(2) (Ek: 21/2/2014-6526/5 md.) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.

Şikayet

Madde 139- (1) Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması şikayete bağlıdır.

Tüzel kişiler hakkında güvenlik tedbiri uygulanması

Madde 140- (1) Yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

(...)

ONUNCU BÖLÜM

Bilişim Alanında Suçlar

Bilişim sistemine girme

Madde 243- (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

(4) (Ek: 24/3/2016-6698/30 md.) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.

Sistemi engelleme, bozma, verileri yok etme veya değiştirme

Madde 244- (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur.

Banka veya kredi kartlarının kötüye kullanılması

Madde 245 - (Değişik: 29/6/2005 - 5377/27 md.)

(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

(2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adli para cezası ile cezalandırılır.

(3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

(4) Birinci fıkrada yer alan suçun;

a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,

b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,

c) Aynı konutta beraber yaşayan kardeşlerden birinin,

Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

(5) (Ek: 6/12/2006 - 5560/11 md.) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır.

Yasak cihaz veya programlar

Madde 245/A- (Ek: 24/3/2016-6698/30 md.)

(1) Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden,

nakleden, depolayan, kabul eden, satan, satıřa arz eden, satın alan, başkalarına veren veya bulunduran kiři, bir yıldan üç yıla kadar hapis ve beřbin güne kadar adli para cezası ile cezalandırılır.

Tüzel kişiler hakkında güvenlik tedbiri uygulanması

Madde 246- (1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

5070 sayılı Elektronik İmza Kanunu

Resmî Gazete Tarihi : 23.01.2004

Resmî Gazete Sayısı : 25355

ELEKTRONİK İMZA KANUNU

BİRİNCİ KISIM

Amaç, Kapsam ve Tanımlar

Amaç

Madde 1- Bu Kanunun amacı, elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları düzenlemektir.

Kapsam

Madde 2- Bu Kanun, elektronik imzanın hukukî yapısını, elektronik sertifika hizmet sağlayıcılarının faaliyetlerini ve her alanda elektronik imzanın kullanımına ilişkin işlemleri kapsar.

(...)

Bilgilerin korunması

Madde 12- Elektronik sertifika hizmet sağlayıcısı;

a) Elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez,

b) Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz,

c) Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletmez ve başka amaçlarla kullanamaz.

(...)

İmza oluşturma verilerinin izinsiz kullanımı

Madde 16- (Değişik: 23/1/2008 - 5728/525 md.)

Elektronik imza oluřturma amacı ile ilgili kiřinin rızası dıřında; imza oluřturma verisi veya imza oluřturma aracını elde eden, veren, kopyalayan ve bu araları yeniden oluřturanlar ile izinsiz elde edilen imza oluřturma aralarını kullanarak izinsiz elektronik imza oluřturanlar bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlı para cezasıyla cezalandırılırlar.

Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet saėlayıcısı alıřanları tarafından iřlenirse bu cezalar yarısına kadar artırılır.

Elektronik sertifikalarda sahtekârlık

Madde 17- (Deėiřik: 23/1/2008 - 5728/526 md.)

Tamamen veya kısmen sahte elektronik sertifika oluřturanlar veya geerli olarak oluřturulan elektronik sertifikaları taklit veya tahrif edenler ile bu elektronik sertifikaları bilerek kullananlar, iki yıldan beř yıla kadar hapis ve yüz günden az olmamak üzere adlı para cezasıyla cezalandırılır.

Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet saėlayıcısı alıřanları tarafından iřlenirse bu cezalar yarısına kadar artırılır.

4982 sayılı Bilgi Edinme Hakkı Kanunu

Resmî Gazete Tarihi : 24.10.2003

Resmî Gazete Sayısı : 25269

BİLGİ EDİNME HAKKI KANUNU

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç

Madde 1- Bu Kanunun amacı; demokratik ve şeffaf yönetimin gereği olan eşitlik, tarafsızlık ve açıklık ilkelerine uygun olarak kişilerin bilgi edinme hakkını kullanmalarına ilişkin esas ve usulleri düzenlemektir.

Kapsam

Madde 2- Bu Kanun; kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının faaliyetlerinde uygulanır.

1.11.1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun hükümleri saklıdır.

(Ek fıkra: 12/7/2013-6495/33 md.; İptal fıkra: Anayasa Mahkemesi'nin 4/12/2014 tarihli ve E.:2013/114, K.:2014/184 sayılı Kararı ile.)

Tanımlar

Madde 3- Bu Kanunda geçen;

- Kurum ve kuruluş: Bu Kanunun 2 nci maddesinde geçen ve kapsama dahil olan bilgi edinme başvurusu yapılacak bütün makam ve mercileri,
- Başvuru sahibi: Bu Kanun kapsamında bilgi edinme hakkını kullanarak kurum ve kuruluşlara başvuran gerçek ve tüzel kişileri,
- Bilgi: Kurum ve kuruluşların sahip oldukları kayıtlarda yer alan bu Kanun kapsamındaki her türlü veriyi,
- Belge: Kurum ve kuruluşların sahip oldukları bu Kanun kapsamındaki yazılı, basılı veya çoğaltılmış dosya, evrak, kitap, dergi, broşür, etüt, mektup, program, talimat, kroki, plân, film,

fotoğraf, teyp ve video kaseti, harita, elektronik ortamda kaydedilen her türlü bilgi, haber ve veri taşıyıcılarını,

e) Bilgi veya belgeye erişim: İstenen bilgi veya belgenin niteliğine göre, kurum ve kuruluşlarca, başvuru sahibine söz konusu bilgi veya belgenin bir kopyasının verilmesini, kopya verilmesinin mümkün olmadığı hâllerde, başvuru sahibinin bilgi veya belgenin aslını inceleyerek not almasına veya içeriğini görmesine veya işitmesine izin verilmesini,

f) Kurul: Bilgi Edinme Değerlendirme Kurulunu,

İfade eder.

İKİNCİ BÖLÜM

Bilgi Edinme Hakkı ve Bilgi Verme Yükümlülüğü

Bilgi edinme hakkı

Madde 4- Herkes bilgi edinme hakkına sahiptir.

Türkiye'de ikamet eden yabancılar ile Türkiye'de faaliyette bulunan yabancı tüzel kişiler, isteyecekleri bilgi kendileriyle veya faaliyet alanlarıyla ilgili olmak kaydıyla ve karşılıklılık ilkesi çerçevesinde, bu Kanun hükümlerinden yararlanırlar.

Türkiye'nin taraf olduğu uluslararası sözleşmelerden doğan hak ve yükümlülükleri saklıdır.

Bilgi verme yükümlülüğü

Madde 5- Kurum ve kuruluşlar, bu Kanunda yer alan istisnalar dışındaki her türlü bilgi veya belgeyi başvuranların yararlanmasına sunmak ve bilgi edinme başvurularını etkin, süratli ve doğru sonuçlandırmak üzere, gerekli idarî ve teknik tedbirleri almakla yükümlüdürler.

Bu Kanun yürürlüğe girdiği tarihten itibaren diğer kanunların bu Kanuna aykırı hükümleri uygulanmaz.

ÜÇÜNCÜ BÖLÜM

Bilgi Edinme Başvurusu

Başvuru usulü

Madde 6- Bilgi edinme başvurusu, başvuru sahibinin adı ve soyadı, imzası, oturma yeri veya iş adresini, başvuru sahibi tüzel kişi ise tüzel kişinin unvanı ve adresi ile yetkili kişinin imzasını ve yetki belgesini içeren dilekçe ile istenen bilgi veya belgenin bulunduğu kurum veya kuruluşa yapılır. Bu başvuru, kişinin kimliğinin ve imzasının veya yazının kimden neşet ettiğinin tespitine yarayacak

başka bilgilerin yasal olarak belirlenebilir olması kaydıyla elektronik ortamda veya diğer iletişim araçlarıyla da yapılabilir.

Dilekçede, istenen bilgi veya belgeler açıkça belirtilir.

İstenecek bilgi veya belgenin niteliği

Madde 7- Bilgi edinme başvurusu, başvuru kurum ve kuruluşların ellerinde bulunan veya görevleri gereği bulunması gereken bilgi veya belgelere ilişkin olmalıdır.

Kurum ve kuruluşlar, ayrı veya özel bir çalışma, araştırma, inceleme ya da analiz neticesinde oluşturulabilecek türden bir bilgi veya belge için yapılacak başvurulara olumsuz cevap verebilirler.

İstenen bilgi veya belge, başvuru kurum ve kuruluşta başka bir yerde bulunuyorsa, başvuru dilekçesi bu kurum ve kuruluşa gönderilir ve durum ilgiliye yazılı olarak bildirilir.

Yayımlanmış veya kamuya açıklanmış bilgi veya belgeler

Madde 8- Kurum ve kuruluşlarca yayımlanmış veya yayın, broşür, ilân ve benzeri yollarla kamuya açıklanmış bilgi veya belgeler, bilgi edinme başvurularına konu olamaz. Ancak, yayımlanmış veya kamuya açıklanmış bilgi veya belgelerin ne şekilde, ne zaman ve nerede yayımlandığı veya açıklandığı başvurana bildirilir.

Gizli bilgileri ayırarak bilgi veya belge verme

Madde 9- İstenen bilgi veya belgelerde, gizlilik dereceli veya açıklanması yasaklanan bilgiler ile açıklanabilir nitelikte olanlar birlikte bulunuyor ve bunlar birbirlerinden ayrılabilirse, söz konusu bilgi veya belge, gizlilik dereceli veya açıklanması yasaklanan bilgiler çıkarıldıktan sonra başvuranın bilgisine sunulur. Ayırma gerekçesi başvurana yazılı olarak bildirilir.

Bilgi veya belgeye erişim

Madde 10- Kurum ve kuruluşlar, başvuru sahibine istenen belgenin onaylı bir kopyasını verirler.

Bilgi veya belgenin niteliği gereği kopyasının verilmesinin mümkün olmadığı veya kopya çıkarılmasının aslına zarar vereceği hâllerde, kurum ve kuruluşlar ilgilinin;

- a) Yazılı veya basılı belgeler için, söz konusu belgenin aslını incelemesi ve not alabilmesini,
- b) Ses kaydı şeklindeki bilgi veya belgelerde bunları dinleyebilmesini,
- c) Görüntü kaydı şeklindeki bilgi veya belgelerde bunları izleyebilmesini,

Sağlarlar.

Bilgi veya belgenin yukarıda belirtilenlerden farklı bir şekilde elde edilmesi mümkün ise, belgeye zarar vermemek koşuluyla bu olanak sağlanır.

Başvurunun yapıldığı kurum ve kuruluş, erişimine olanak sağladığı bilgi veya belgeler için başvuru sahibinden erişimin gerektirdiği maliyet tutarı kadar bir ücreti bütçeye gelir kaydedilmek üzere tahsil edebilir.

Bilgi veya belgeye erişim süreleri

Madde 11- Kurum ve kuruluşlar, başvuru üzerine istenen bilgi veya belgeye erişimi onbeş iş günü içinde sağlarlar. Ancak istenen bilgi veya belgenin, başvurulmuş kurum ve kuruluş içindeki başka bir birimden sağlanması; başvuru ile ilgili olarak bir başka kurum ve kuruluşun görüşünün alınmasının gerekmesi veya başvuru içeriğinin birden fazla kurum ve kuruluşu ilgilendirmesi durumlarında bilgi veya belgeye erişim otuz iş günü içinde sağlanır. Bu durumda, sürenin uzatılması ve bunun gerekçesi başvuru sahibine yazılı olarak ve onbeş iş günlük sürenin bitiminden önce bildirilir.

10 uncu maddede belirtilen bilgi veya belgelere erişim için gereken maliyet tutarının idare tarafından başvuru sahibine bildirilmesiyle onbeş iş günlük süre kesilir. Başvuru sahibi onbeş iş günü içinde ücreti ödemezse talebinden vazgeçmiş sayılır.

Başvuruların cevaplandırılması

Madde 12- Kurum ve kuruluşlar, bilgi edinme başvurularıyla ilgili cevaplarını yazılı olarak veya elektronik ortamda başvuru sahibine bildirirler. Başvurunun reddedilmesi hâlinde bu kararın gerekçesi ve buna karşı başvuru yolları belirtilir.

İtiraz usulü

Madde 13- Bilgi edinme istemi (...) reddedilen başvuru sahibi, yargı yoluna başvurmadan önce kararın tebliğinden itibaren onbeş gün içinde Kurula itiraz edebilir. Kurul, bu konudaki kararını otuz iş günü içinde verir. Kurum ve kuruluşlar, Kurulun istediği her türlü bilgi veya belgeyi onbeş iş günü içinde vermekle yükümlüdürler.

Kurula itiraz, başvuru sahibinin idarî yargıya başvurma süresini durdurur.

Bilgi Edinme Değerlendirme Kurulu

Madde 14- Bilgi edinme başvurusuyla ilgili yapılacak itirazlar üzerine, (...) verilen kararları incelemek ve kurum ve kuruluşlar için bilgi edinme hakkının kullanılmasına ilişkin olarak kararlar vermek üzere; Bilgi Edinme Değerlendirme Kurulu oluşturulmuştur.

Kurul; birer üyesi Yargıtay ve Danıştay genel kurullarının kendi kurumları içinden önerecekleri ikişer aday, birer üyesi ceza hukuku, idare hukuku ve anayasa hukuku alanlarında profesör veya doçent unvanına sahip kişiler, bir üyesi Türkiye Barolar Birliğinin baro başkanı seçilme yeterliliğine sahip kişiler içinden göstereceği iki aday, iki üyesi en az genel müdür düzeyinde görev yapmakta olanlar ve bir üyesi de Adalet Bakanının önerisi üzerine bu Bakanlıkta idarî görevlerde çalışan hâkimler arasından Cumhurbaşkanınca seçilecek dokuz üyeden oluşur. (1)

Kurul üyeliğine önerilen adayların muvafakatlari aranır.

Kurul Başkanı, kurul üyelerince kendi aralarından seçilir.

Kurul, en az ayda bir defa veya ihtiyaç duyulduğu her zaman Başkanın çağrısı üzerine toplanır.

Kurul üyelerinin görev süreleri dört yıldır. Görev süresi sona erenler yeniden seçilebilirler. Görev süresi dolmadan görevinden ayrılan üyenin yerine aynı usule göre seçilen üye, yerine seçildiği üyenin görev süresini tamamlar. Yeni seçilen Kurul göreve başlayıncaya kadar önceki Kurul görevine devam eder.

Kurul üyelerine 10.2.1954 tarihli ve 6245 sayılı Harcırah Kanunu hükümleri saklı kalmak kaydıyla fiilen görev yaptıkları her gün için (3000) gösterge rakamının memur aylık katsayısı ile çarpımı sonucu bulunacak miktarda huzur hakkı ödenir. Bu ödemelerde damga vergisi hariç herhangi bir kesinti yapılmaz. (Ek cümle: 17/11/2005-5432/2 md.) Bir ayda fiilen görev yapılan gün sayısının dördü aşması halinde, aşan günler için huzur hakkı ödenmez.(2)

Kurul, belirleyeceği konularda komisyonlar ve çalışma grupları kurabilir; ayrıca gerekli gördüğü takdirde, ilgili bakanlık ile diğer kurum ve kuruluşların ve sivil toplum örgütlerinin temsilcilerini bilgi almak üzere toplantılarına katılmaya davet edebilir.

Kurulun sekretarya hizmetleri Adalet Bakanlığı tarafından yerine getirilir.

Kurulun görev ve çalışmalarına ilişkin esas ve usuller Cumhurbaşkanlığınca hazırlanarak yürürlüğe konulacak bir yönetmelikle düzenlenir.

DÖRDÜNCÜ BÖLÜM

Bilgi Edinme Hakkının Sınırları

Yargı denetimi dışında kalan işlemler

Madde 15- Yargı denetimi dışında kalan idarî işlemlerden kişinin çalışma hayatını ve mesleki onurunu etkileyecek nitelikte olanlar, bu Kanun kapsamına dahildir. Bu şekilde sağlanan bilgi edinme hakkı işlemin yargı denetimine açılması sonucunu doğurmaz.

Devlet sırrına ilişkin bilgi veya belgeler

Madde 16- Açıklanması hâlinde Devletin emniyetine, dış ilişkilerine, millî savunmasına ve millî güvenliğine açıkça zarar verecek ve niteliği itibarıyla Devlet sırrı olan gizlilik dereceli bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır.

Ülkenin ekonomik çıkarlarına ilişkin bilgi veya belgeler

Madde 17- Açıklanması ya da zamanından önce açıklanması hâlinde, ülkenin ekonomik çıkarlarına zarar verecek veya haksız rekabet ve kazanç sebep olacak bilgi veya belgeler, bu Kanun kapsamı dışındadır.

İstihbarata ilişkin bilgi veya belgeler

Madde 18- Sivil ve askerî istihbarat birimlerinin görev ve faaliyetlerine ilişkin bilgi veya belgeler, bu Kanun kapsamı dışındadır.

Ancak, bu bilgi ve belgeler kişilerin çalışma hayatını ve meslek onurunu etkileyecek nitelikte ise, istihbarata ilişkin bilgi ve belgeler bilgi edinme hakkı kapsamı içindedir.

İdarî soruşturmaya ilişkin bilgi veya belgeler

Madde 19- Kurum ve kuruluşların yetkili birimlerince yürütülen idarî soruşturmalarla ilgili olup, açıklanması veya zamanından önce açıklanması hâlinde;

- a) Kişilerin özel hayatına açıkça haksız müdahale sonucunu doğuracak,
- b) Kişilerin veya soruşturmayı yürüten görevlilerin hayatını ya da güvenliğini tehlikeye sokacak,
- c) Soruşturmanın güvenliğini tehlikeye düşürecek,
- d) Gizli kalması gereken bilgi kaynağının açığa çıkmasına neden olacak veya soruşturma ile ilgili benzeri bilgi ve bilgi kaynaklarının temin edilmesini güçleştirecek,

Bilgi veya belgeler, bu Kanun kapsamı dışındadır.

Adlî soruşturma ve kovuşturmaya ilişkin bilgi veya belgeler

Madde 20- Açıklanması veya zamanından önce açıklanması hâlinde;

- a) Suç işlenmesine yol açacak,
- b) Suçların önlenmesi ve soruşturulması ya da suçluların kanunî yollarla yakalanıp kovuşturulmasını tehlikeye düşürecek,
- c) Yargılama görevinin gereğince yerine getirilmesini engelleyecek,

d) Hakkında dava açılmış bir kişinin adil yargılanma hakkını ihlâl edecek,

Nitelikteki bilgi veya belgeler, bu Kanun kapsamı dışındadır.

4.4.1929 tarihli ve 1412 sayılı Ceza Muhakemeleri Usulü Kanunu, 18.6.1927 tarihli ve 1086 sayılı Hukuk Usulü Muhakemeleri Kanunu, 6.1.1982 tarihli ve 2577 sayılı İdari Yargılama Usulü Kanunu ve diğer özel kanun hükümleri saklıdır.

Özel hayatın gizliliği

Madde 21- Kişinin izin verdiği hâller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, meslekî ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır.

Kamu yararının gerektirdiği hâllerde, kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir.

Haberleşmenin gizliliği

Madde 22- Haberleşmenin gizliliği esasını ihlâl edecek bilgi veya belgeler, bu Kanun kapsamı dışındadır.

Ticarî sır

Madde 23- Kanunlarda ticarî sır olarak nitelenen bilgi veya belgeler ile, kurum ve kuruluşlar tarafından gerçek veya tüzel kişilerden gizli kalması kaydıyla sağlanan ticarî ve malî bilgiler, bu Kanun kapsamı dışındadır.

Fikir ve sanat eserleri

Madde 24- Fikir ve sanat eserlerine ilişkin olarak yapılacak bilgi edinme başvuruları hakkında ilgili kanun hükümleri uygulanır.

Kurum içi düzenlemeler

Madde 25- Kurum ve kuruluşların, kamuoyunu ilgilendirmeyen ve sadece kendi personeli ile kurum içi uygulamalarına ilişkin düzenlemeler hakkındaki bilgi veya belgeler, bilgi edinme hakkının kapsamı dışındadır. Ancak, söz konusu düzenlemeden etkilenen kurum çalışanlarının bilgi edinme hakları saklıdır.

Kurum içi görüş, bilgi notu ve tavsiyeler

Madde 26- Kurum ve kuruluşların faaliyetlerini yürütmek üzere, elde ettikleri görüş, bilgi notu, teklif ve tavsiye niteliğindeki bilgi veya belgeler, kurum ve kuruluş tarafından aksi kararlaştırılmadıkça bilgi edinme hakkı kapsamındadır.

Bilimsel, kültürel, istatistik, teknik, tıbbî, malî, hukukî ve benzeri uzmanlık alanlarında yasal olarak görüş verme yükümlülüğü bulunan kişi, birim ya da kurumların görüşleri, kurum ve kuruluşların alacakları kararlara esas teşkil etmesi kaydıyla bilgi edinme istemlerine açıktır.

Tavsiye ve mütalaa talepleri

Madde 27- Tavsiye ve mütalaa talepleri bu Kanun kapsamı dışındadır.

Gizliliği kaldırılan bilgi veya belgelerMadde 28- Gizliliği kaldırılmış olan bilgi veya belgeler, bu Kanunda belirtilen diğer istisnalar kapsamına girmiyor ise, bilgi edinme başvurularına açık hâle gelir.

BEŞİNCİ BÖLÜM

Çeşitli ve Son Hükümler

Ceza hükümleri

Madde 29- Bu Kanunun uygulanmasında ihmâli, kusuru veya kastı bulunan memurlar ve diğer kamu görevlileri hakkında, işledikleri fiillerin genel hükümler çerçevesinde ceza kovuşturması gerektirmesi hususu saklı kalmak kaydıyla, tâbi oldukları mevzuatta yer alan disiplin cezaları uygulanır.

Bu Kanunla erişilen bilgi ve belgeler ticarî amaçla çoğaltılamaz ve kullanılamaz.

Rapor düzenlenmesi

Madde 30- Kurum ve kuruluşlar, bir önceki yıla ait olmak üzere;

- a) Kendilerine yapılan bilgi edinme başvurularının sayısını,
- b) Olumlu cevaplanarak bilgi veya belgelere erişim sağlanan başvuru sayısını,
- c) Reddedilen başvuru sayısı ve bunların dağılımını gösterir istatistik bilgileri,
- d) Gizli ya da sır niteliğindeki bilgiler çıkarılarak ya da bu nitelikteki bilgiler ayrılarak bilgi veya belgelere erişim sağlanan başvuru sayısını,
- e) Başvurunun reddedilmesi üzerine itiraz edilen başvuru sayısı ile bunların sonuçlarını,

Gösterir bir rapor hazırlayarak, bu raporları her yıl Şubat ayının sonuna kadar Bilgi Edinme Değerlendirme Kuruluna gönderirler. Bağlı, ilgili ve ilişkili kamu kurum ve kuruluşları raporlarını bağlı, ilgili ya da ilişkili oldukları bakanlık vasıtasıyla iletirler. Kurul, hazırlayacağı genel raporu, söz

konusu kurum ve kuruluşların raporları ile birlikte her yıl Nisan ayının sonuna kadar Türkiye Büyük Millet Meclisine gönderir. Bu raporlar takip eden iki ay içinde Türkiye Büyük Millet Meclisi Başkanlığınca kamuoyuna açıklanır.

Yönetmelik

Madde 31- Bu Kanunun uygulanması ile ilgili esas ve usullerin belirlenmesine ilişkin yönetmelik, Kanunun yayımını takip eden altı ay içinde Cumhurbaşkanlığı tarafından hazırlanarak (...) (1) yürürlüğe konulur.

Yürürlük

Madde 32- Bu Kanun yayımı tarihinden itibaren altı ay sonra yürürlüğe girer.

Yürütme

Madde 33- Bu Kanun hükümlerini Cumhurbaşkanı yürütür.

4904 sayılı Türkiye İş Kurumu ile İlgili Bazı Düzenlemeler Hakkında Kanun

Resmî Gazete Tarihi : 05.07.2003

Resmî Gazete Sayısı : 25159

TÜRKİYE İŞ KURUMU İLE İLGİLİ BAZI DÜZENLEMELER HAKKINDA KANUN

BİRİNCİ KISIM

Türkiye İş Kurumunun Kuruluş ve Görevleri

BİRİNCİ BÖLÜM

Amaç, Kapsam, Tanımlar ve Kurumun Görevleri

Amaç ve kapsam

Madde 1 - (Mülga birinci fıkra: 2/7/2018 - KHK-703/74 md.)

Genel bütçeye dahil dairelerle katma bütçeli idarelerde, bunlara bağlı döner sermayeli kuruluşlarda, kanunla kurulan fonlarda, özel kanunla veya Cumhurbaşkanlığı kararnamesiyle kurulan kamu kurum ve kuruluşlarında, kefalet sandıklarında, sosyal güvenlik kuruluşlarında, genel ve katma bütçelerin transfer tertiplerinden yardım alan kuruluşlarda, kamu iktisadi teşebbüsleri ve bunların bağlı ortaklıklarında, il özel idareleri ve belediyelerle bunların kurdukları birlik ve müesseselerde ve diğer kamu kurum ve kuruluşlarında aylık ve ücret alan ve işçi statüsünde çalışmayan memur, sözleşmeli personel, geçici personel ve diğer kamu görevlilerinin istihdamı hakkında bu Kanun hükümleri uygulanmaz.

(Mülga üçüncü fıkra: 2/7/2018 - KHK-703/74 md.)

(Mülga birinci cümle: 2/7/2018 - KHK-703/74 md.) (...) Kurumun malları, alacakları, banka hesapları 9.6.1932 tarihli ve 2004 sayılı İcra ve İflas Kanunu ile 1.3.1926 tarihli ve 765 sayılı Türk Ceza Kanunu bakımından Devlet malı hükmünde olup haczedilemez, alacakları da Devlet alacağı derecesinde imtiyazlıdır. Kurum malları hakkında İcra ve İflas Kanununun iflase ilişkin hükümleri uygulanmaz.

(Mülga dördüncü cümle: 2/7/2018 - KHK-703/74 md.)

(...)

Bilgi verme ve gizlilik

Madde 21 - (Deęişik: 23/1/2008-5728/504 md.)

Kurum tarafından, kamu ve özel kesim işyerlerinden iş ve işgücü konularında bilgi istenildiğinde, belirtilen süre içinde bilgi verilmesi zorunludur.

İşverenlerden toplanan bilgiler, Kurum hizmetlerinden başka amaçla kullanılamaz.

İkinci fıkraya aykırı davrananlar hakkında Türk Ceza Kanununun 136 ncı maddesi hükümleri uygulanır.

4857 sayılı İş Kanunu

Resmî Gazete Tarihi : 10.06.2003

Resmî Gazete Sayısı : 25134

İŞ KANUNU

BİRİNCİ BÖLÜM

Genel Hükümler

Amaç ve kapsam

Madde 1 - Bu Kanunun amacı işverenler ile bir iş sözleşmesine dayanarak çalıştırılan işçilerin çalışma şartları ve çalışma ortamına ilişkin hak ve sorumluluklarını düzenlemektir.

Bu Kanun, 4 üncü Maddedeki istisnalar dışında kalan bütün işyerlerine, bu işyerlerinin işverenleri ile işveren vekillerine ve işçilerine faaliyet konularına bakılmaksızın uygulanır.

İşyerleri, işverenler, işveren vekilleri ve işçiler, 3 üncü maddedeki bildirim gününe bakılmaksızın bu Kanun hükümleri ile bağlı olurlar.

(...)

İşçi özlük dosyası

Madde 75 - İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır.

İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür.

(...)

Yetkili memurların ödevi

Madde 93 - İş hayatını izleme, denetleme ve teftiş yetkisi olan iş müfettişleri görevlerini yaparlarken işin normal gidişini ve işyerinin işlemlerini, inceledikleri konunun niteliğine göre mümkün olduğu kadar aksatmamak, durdurmamak ve güçleştirmemekle ve resmi işlemlerin yürütülüp

sonuçlandırılması için, açıklanması gerekmedikçe, işverenin ve işyerinin meslek sırları ve şartları, ekonomik ve ticari hal ve durumları hakkında gördükleri ve öğrendikleri hususları tamamen gizli tutmak ve kendileri tarafından bilgileri ve ifadeleri alınan yahut kendilerine başvuran veya ihbarda bulunan işçilerin ve başka kişilerin isimlerini ve kimliklerini açıklamamakla yükümlüdürler.

4721 sayılı Türk Medeni Kanunu

Resmî Gazete Tarihi : 08.12.2001

Resmî Gazete Sayısı : 24607

TÜRK MEDENİ KANUNU

B. Kişiliğin korunması

I. Vazgeçme ve aşırı sınırlamaya karşı

Madde 23- Kimse, hak ve fiil ehliyetlerinden kısmen de olsa vazgeçemez.

Kimse özgürlüklerinden vazgeçemez veya onları hukuka ya da ahlâka aykırı olarak sınırlayamaz.

Yazılı rıza üzerine insan kökenli biyolojik maddelerin alınması, aşılması ve nakli mümkündür. Ancak, biyolojik Madde verme borcu altına girmiş olandan edimini yerine getirmesi istenemez; maddî ve manevî tazminat isteminde bulunulamaz.

II. Saldırıya karşı

1. İlke

Madde 24- Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir.

Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.

2. Davalar

Madde 25- Davacı, hâkimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir.

Davacı bunlarla birlikte, düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabilir.

Davacının, maddî ve manevî tazminat istemleri ile hukuka aykırı saldırı dolayısıyla elde edilmiş olan kazancın vekâletsiz iş görme hükümlerine göre kendisine verilmesine ilişkin istemde bulunma hakkı saklıdır.

Manevî tazminat istemi, karşı tarafça kabul edilmiş olmadıkça devredilemez; mirasbırakan tarafından ileri sürülmüş olmadıkça mirasçılara geçmez.

Davacı, kişilik haklarının korunması için kendi yerleşim yeri veya davalının yerleşim yeri mahkemesinde dava açabilir.

III. Ad üzerindeki hak

1. Adın korunması

Madde 26- Adının kullanılması çekişmeli olan kişi, hakkının tespitini dava edebilir.

Adı haksız olarak kullanılan kişi buna son verilmesini; haksız kullanan kusurlu ise ayrıca maddî zararının giderilmesini ve uğradığı haksızlığın niteliği gerektiriyorsa manevî tazminat ödenmesini isteyebilir.

2. Adın değiştirilmesi

Madde 27- Adın değiştirilmesi, ancak haklı sebeplere dayanılarak hâkimden istenebilir.

Adın değiştirildiği nüfus siciline kayıt ve ilân olunur.

Ad değişmekle kişisel durum değişmez.

Adın değiştirilmesinden zarar gören kimse, bunu öğrendiği günden başlayarak bir yıl içinde değiştirme kararının kaldırılmasını dava edebilir.

C. Kişiliğin başlangıcı ve sonu

I. Doğum ve ölüm

Madde 28- Kişilik, çocuğun sağ olarak tamamıyla doğduğu anda başlar ve ölümle sona erer.

Çocuk hak ehliyetini, sağ doğmak koşuluyla, ana rahmine düştüğü andan başlayarak elde eder.

II. Sağ olmanın ve ölümün ispatı

1. İspat yükü

Madde 29- Bir hakkın kullanılması için bir kimsenin sağ veya ölü olduğunu veya belirli bir zamanda ya da başka bir kimsenin ölümünde sağ bulunduğunu ileri süren kimse, iddiasını ispat etmek zorundadır.

Birden fazla kişiden hangisinin önce veya sonra öldüğü ispat edilemezse, hepsi aynı anda ölmüş sayılır.

2. İspat araçları

a. Genel olarak

Madde 30- Doğum ve ölüm, nüfus sicilindeki kayıtlarla ispat olunur.

Nüfus sicilinde bir kayıt yoksa veya bulunan kaydın doğru olmadığı anlaşılırsa, gerçek durum her türlü kanıtla ispat edilebilir.

b. Ölüm karinesi

Madde 31- Bir kimse, ölümüne kesin gözle bakılmayı gerektiren durumlar içinde kaybolursa, cesedi bulunamamış olsa bile gerçekten ölmüş sayılır.

III. Gaiplik kararı

1. Genel olarak

Madde 32- Ölüm tehlikesi içinde kaybolan veya kendisinden uzun zamandan beri haber alınamayan bir kimsenin ölümü hakkında kuvvetli olasılık varsa, hakları bu ölüme bağlı olanların başvurusu üzerine mahkeme bu kişinin gaipliğine karar verebilir.

Yetkili mahkeme, kişinin Türkiye'deki son yerleşim yeri; eğer Türkiye'de hiç yerleşmemişse nüfus sicilinde kayıtlı olduğu yer; böyle bir kayıt da yoksa anasının veya babasının kayıtlı bulunduğu yer mahkemesidir.

2. Yargılama usulü

Madde 33- Gaiplik kararının istenebilmesi için, ölüm tehlikesinin üzerinden en az bir yıl veya son haber tarihinin üzerinden en az beş yıl geçmiş olması gerekir.

Mahkeme, gaipliğine karar verilecek kişi hakkında bilgisi bulunan kimseleri, belirli bir sürede bilgi vermeleri için usulüne göre yapılan ilânla çağırır.

Bu süre, ilk ilânın yapıldığı günden başlayarak en az altı aydır.

3. İstem düşmesi

Madde 34- Gaipliğine karar verilecek kişi, ilân süresi dolmadan ortaya çıkar veya kendisinden haber alınır ya da öldüğü tarih tespit edilirse gaiplik istemi düşer.

4. Hükmü

Madde 35- İlândan sonuç alınamazsa, mahkeme gaipliğe karar verir ve ölüme bağlı haklar, aynen gaibin ölümü ispatlanmış gibi kullanılır.

Gaiplik kararı ölüm tehlikesinin gerçekleştiği veya son haberin alındığı günden başlayarak hüküm doğurur.

İKİNCİ BÖLÜM

KİŞİSEL DURUM SİCİLİ

A. Genel olarak

I. Sicil

Madde 36- Kişisel durum, bu amaçla tutulan resmî sicille belirlenir.

Bu sicilin tutulmasına ve zorunlu bildirimlerin yapılmasına ilişkin esaslar, ilgili kanunda gösterilir.

II. Görevliler

Madde 37- Kişisel durum sicili, Devletçe atanan memurlar tarafından tutulur. Sicil kayıtlarını tutmak ve örnek vermek bu memurların görevidir.

Yabancı memleketlerdeki Türkiye temsilcilerine, Cumhurbaşkanlığının onayı ile nüfus memurluğu yetkisi verilebilir. (1)

III. Sorumluluk

Madde 38- Kişisel durum sicilinin tutulmasından doğan zararlar, kusurlu memura rücu edilmek kaydıyla, Devletçe tazmin edilir.

Tazminat ve rücu davaları, kişisel durum sicilinin tutulduğu yer mahkemesinde açılır.

IV. Düzeltme

1. Genel olarak

Madde 39- Mahkeme kararı olmadıkça, kişisel durum sicilinin hiçbir kaydında düzeltme yapılamaz.

2. Cinsiyet değişikliğinde

Madde 40- Cinsiyetini değiştirmek isteyen kimse, şahsen başvuruda bulunarak mahkemece cinsiyet değişikliğine izin verilmesini isteyebilir. Ancak, iznin verilebilmesi için, istem sahibinin onsekiz yaşını doldurmuş bulunması ve evli olmaması; ayrıca transeksüel yapıda olup, cinsiyet değişikliğinin ruh sağlığı açısından zorunluluğunu (...) bir eğitim ve araştırma hastanesinden alınacak resmî sağlık kurulu raporuyla belgelemesi şarttır.

Verilen izne bađlı olarak ama ve tıbbî ynemlere uygun bir cinsiyet deđiřtirme ameliyatı gerekleřtirildiđinin resmî sađlık kurulu raporuyla dođrulanması hâlinde, mahkemece nfus sicilinde gerekli dzeltmenin yapılmasına karar verilir.

B. Dođum ktđ

I. Bildirme

Madde 41- Dođumlara iliřkin bildirimler ve kimliđi bilinmeyen bulunmuř ocuklar hakkındaki iřlemler ilgili kanun hkmlerine gre yapılır.

II. Dođum ktđnde deđiřiklikler

Madde 42- Kiřisel durumdaki deđiřiklikler, zellikle evlilik dıřı bir ocuđun tanınması veya hâkimin babalıđa karar vermesi, soybađının dzeltilmesi, evlâat edinme ya da bulunmuř bir ocuđun soybađının belli olması, ilgili kanun hkmlerine gre ktđe iřlenir.

C. lm ktđ

I. lmn bildirilmesi

Madde 43- lmlere iliřkin bildirimler ilgili kanun hkmlerine gre yapılır.

II. Cesedi bulunamayan kiři

Madde 44- Bir kimse, lmne kesin gzle bakılmayı gerektiren durumlar iinde ortadan kaybolursa cesedi bulunamamıř olsa bile, o yerin en byk mlk amirinin emriyle ktđe lm kaydı dřrlr.

Bununla birlikte her ilgili, bu kiřinin lm veya sađ olduđunun mahkemece tespitini dava edebilir.

III. Gaiplik kararı

Madde 45- Gaiplik kararı, hâkimin bildirmesi zerine, lm ktđne kaydolunur.

IV. Deđiřikliklerin ktđe geirilmesi

Madde 46- Tescile esas olan bir bildirim dođru olmadıđının tespit edilmesi veya kime ait olduđu bilinmeyen cesedin kimliđinin belli olması ya da gaiplik kararının kaldırılması sebepleriyle zorunlu olan deđiřiklikler, ilgilinin ktkteki kaydının dřnceler stnuna yazılarak yapılır.

4632 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanunu

Resmî Gazete Tarihi : 07.04.2001

Resmî Gazete Sayısı : 24366

BİREYSEL EMEKLİLİK TASARRUF VE YATIRIM SİSTEMİ KANUNU

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç ve kapsam

Madde 1 - Bu Kanunun amacı, kamu sosyal güvenlik sisteminin tamamlayıcısı olarak, bireylerin emekliliğe yönelik tasarruflarının yatırıma yönlendirilmesi ile emeklilik döneminde ek bir gelir sağlanarak refah düzeylerinin yükseltilmesi, ekonomiye uzun vadeli kaynak yaratarak istihdamın artırılması ve ekonomik kalkınmaya katkıda bulunulmasını teminen, gönüllü katılıma dayalı ve belirlenmiş katkı esasına göre oluşturulan bireysel emeklilik sisteminin düzenlenmesi ve denetlenmesidir.

Bu Kanunun kapsamı, emeklilik şirketlerinin kuruluş, çalışma, yönetim ve denetimine, kişilerin sisteme katılma, ayrılma ve emeklilik koşullarına, emeklilik yatırım fonlarının kuruluşuna, katkıların bu fonlarda toplanmasına ve değerlendirilmesine, aracılık hizmetlerine, kamuya açıklanacak bilgilerin kapsamına ve bireysel emeklilikle ilgili diğer hususlara ilişkin esas ve usulleri düzenlemektir.

Bu Kanunda hüküm bulunmayan hallerde sermaye piyasası ve sigortacılık mevzuatının ilgili hükümleri ve genel hükümler uygulanır.

(...)

Çalışanların otomatik olarak bir emeklilik planına dâhil edilmesi

Ek Madde 2- (Ek: 10/8/2016-6740/1 md.)

(Değişik birinci cümle: 18/1/2017-6770/18 md.) Türk vatandaşı veya 29/5/2009 tarihli ve 5901 sayılı Türk Vatandaşlığı Kanununun 28 inci maddesi kapsamında olup kırk beş yaşını doldurmamış olanlardan; 31/5/2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 4 üncü maddesinin birinci fıkrasının (a) ve (c) bentlerine göre çalışmaya başlayanlar ile 17/7/1964 tarihli

ve 506 sayılı Sosyal Sigortalar Kanununun geçici 20 nci maddesi kapsamında kurulmuş olan sandıkların iştirakçisi olarak çalışmaya başlayanlar, işverenin bu Kanun hükümlerine göre düzenlediği bir emeklilik sözleşmesiyle emeklilik planına dâhil edilir. İşveren, çalışanını ancak otomatik katılım için emeklilik planı düzenleme konusunda Müsteşarlıkça uygun görülen şirketlerden birinin sunacağı emeklilik planına dâhil edebilir. Cumhurbaşkanı, bu madde uyarınca emeklilik planına dâhil edilecek işyerleri ile çalışanları ve bu kapsamdaki uygulama esaslarını belirlemeye yetkilidir.

Çalışan katkı payı, çalışanın 5510 sayılı Kanunun 80 inci maddesi çerçevesinde belirlenen prime esas kazancının yüzde üçüne karşılık gelen tutardır. (Ek cümle: 18/1/2017-6770/18 md.) 506 sayılı Kanunun geçici 20 nci maddesi kapsamında kurulmuş olan sandıkların iştirakçisi olan çalışanlar için bu çalışanların bağlı bulunduğu sandığa, katılım payı, kesenek veya diğer adlar altında ödediği tutarların hesaplanmasına esas kazancının yüzde üçüne karşılık gelen tutardır. Bu oranı iki katına kadar artırmaya, yüzde bire kadar azaltmaya veya katkı payına maktu limit getirmeye Cumhurbaşkanı yetkilidir. Bu tutar, en geç çalışanın ücretinin ödeme gününü takip eden iş günü, bu Kanun hükümleri uyarınca işveren tarafından şirkete aktarılır. İşveren bu madde uyarınca katkı payını zamanında şirkete aktarmaz veya geç aktarırsa çalışanın 5 inci maddedeki hesaplama yöntemi uyarınca varsa birikiminde oluşan parasal kaybindan sorumludur. Çalışan, otomatik katılıma ilişkin emeklilik sözleşmesinde belirlenen tutardan daha yüksek bir tutarda kesinti yapılmasını işverenden talep edebilir.

Çalışan, emeklilik planına dâhil olduğunun kendisine bildirildiği tarihi müteakip iki ay içinde sözleşmeden cayabilir. (Ek cümle: 21/3/2018-7103/45 md.) Bu süreyi üç katına kadar artırmaya Cumhurbaşkanı yetkilidir. Cayma hâlinde, ödenen katkı payları, varsa hesabında bulunan yatırım gelirleri ile birlikte on iş günü içinde çalışana iade edilir. Şirket, cayma süresince ödenen katkı paylarının değer kaybetmemesini sağlayacak şekilde fon yönetiminden sorumludur. Cayma hakkını kullanmayan çalışan Müsteşarlıkça belirlenen hâllerde katkı payı ödemesine ara verilmesini talep edebilir.

(Mülga dördüncü fıkra: 21/3/2018-7103/45 md.)

Çalışan adına bireysel emeklilik hesabına ödenen katkı payları üzerinden ek 1 inci maddedeki usul ve esaslara göre bu madde uyarınca ayrıca Devlet katkısı sağlanır. Çalışanın bu madde kapsamında cayma hakkını kullanmaması hâlinde, sisteme girişte bir defaya mahsus olmak üzere, ek 1 inci maddedeki Devlet katkısı hak etme ve ödeme koşuluna tabi olmak kaydıyla, bin Türk lirası tutarında ilave Devlet katkısı sağlanır. Cumhurbaşkanı, bu tutarı yarısına kadar artırmaya veya yarısına kadar

azaltmaya yetkilidir. Emeklilik hakkının kullanılması hâlinde, hesabında bulunan birikimi en az on yıllık, yıllık gelir sigortası sözleşmesi kapsamında almayı tercih eden çalışana, birikiminin yüzde beşi karşılığı ek Devlet katkısı ödemesi yapılır. Bu madde hükmüne göre çalışan katkı payının takip ve tahsil sorumluluğu şirkete aittir. Müsteşarlık takip ve tahsil sorumluluğunun bu amaçla yetkilendirilecek bir kuruluşça yerine getirilmesine karar verebilir. Bankalar, Sosyal Güvenlik Kurumu, 506 sayılı Kanunun geçici 20 nci maddesi kapsamındaki sandıklar ile bunların ilgili buldukları kuruluşlar ve ilgili diğer kamu kurumları, çalışan katkı payının takip ve tahsili ile Devlet katkısının hesaplanması için ihtiyaç duyulan verileri, Müsteşarlıkça belirlenen usul ve esaslara göre emeklilik gözetim merkezi ile bu maddeye göre takip ve tahsil sorumluluğu ile yetkilendirilecek kuruluşça aktarır. Emeklilik gözetim merkezi ile bu maddeye göre yetkilendirilecek kuruluş, söz konusu verileri şirketler ile paylaşabilir. Bu verilerden kişisel nitelikte olanlar, veri sahibinin açık rızasının alınmasına gerek olmaksızın ilgili kuruluşlar arasında paylaşılabilir ve veri paylaşımı, kişisel verilerin korunmasına ilişkin mevzuat hükümlerine aykırılık teşkil etmez.

Bu madde kapsamında sunulan emeklilik planları kapsamında şirketlerce 7 nci madde uyarınca fon işletim gideri kesintisi dışında başka bir kesinti yapılamaz. Çalışan katkı payı, işverenin taraf olduğu 9/6/1932 tarihli ve 2004 sayılı İcra ve İflas Kanunu kapsamındaki haciz ve iflas yoluyla takip bakımından işçi alacağı niteliğinde imtiyazlı bir alacaktır. İşverenler bu madde kapsamındaki yükümlülükleri bakımından Çalışma ve Sosyal Güvenlik Bakanlığı tarafından denetlenir. İşverenin bu madde kapsamındaki yükümlülüklerine ve bu madde uyarınca yürürlüğe konulan düzenlemelere uymaması hâlinde, her bir ihlal için Çalışma ve Sosyal Güvenlik Bakanlığınca yüz Türk lirası idari para cezası uygulanır.

(Değişik yedinci fıkra: 21/3/2018-7103/45 md.) Bakan, belirleyeceği esaslar dâhilinde, bu Kanun kapsamında sağlanan Devlet katkısının, ilgililerin hesaben takip edebilmesini sağlayacak şekilde taahhüt olarak hesaplanmasına, taahhüt olarak hesaplanan bu tutarların nemalandırılmasına ve ek 1 inci maddede belirtilen hak kazanma koşulları dikkate alınarak nemalarıyla birlikte ödenmesine karar vermeye; bu Kanun kapsamında sağlanan Devlet katkısının nemalandırılmasına, bin Türk lirası tutarındaki ilave Devlet katkısının yıllar itibarıyla yeniden değerlemesine ve ek devlet katkısının azami limiti ile iade edilmesine ilişkin usul ve esasları belirlemeye yetkilidir. Bu Kanun uyarınca yapılacak bildirimler, Müsteşarlığın belirleyeceği usul ve esaslar çerçevesinde güvenli elektronik iletişim araçları ile de yapılabilir.

Çalışanın işvereni aracılığıyla bir emeklilik planına dâhil olması, işveren tarafından şirket ve plan belirlenmesinde göz önünde bulundurulacak kriterler, katkı paylarının yatırıma yönlendirileceği

fonlar, işverenin şirket ile yapacağı sözleşme, cayma hakkı, çalışanın işyerinin değişmesi hâlinde işverenin çalışanı bir emeklilik planına dâhil etmesi, işyeri değişikliğinde birikimin aktarılması, çalışma ilişkisi sona eren çalışanın talebi üzerine ilgili emeklilik planına ödeme yapması, ara verme, sistemden ayrılma, Devlet katkısının ödenmesi ve bu maddenin uygulanmasına ilişkin diğer usul ve esaslar Müsteşarlık tarafından belirlenir.

3359 sayılı Sağlık Hizmetleri Temel Kanunu

Resmî Gazete Tarihi : 15.05.1987

Resmî Gazete Sayısı : 19461

SAĞLIK HİZMETLERİ TEMEL KANUNU

Amaç

Madde 1 - Bu Kanunun amacı; sağlık hizmetleriyle ilgili temel esasları düzenlemektir.

Kapsam

Madde 2 - Bu Kanun, Milli Savunma Bakanlığı hariç, bütün kamu kurum ve kuruluşları ile özel hukuk tüzelkişilerini ve gerçek kişileri kapsar.

Temel Esaslar

Madde 3 - Sağlık hizmetleriyle ilgili temel esaslar şunlardır:

- a) Sağlık kurum ve kuruluşları yurt sathında eşit, kaliteli ve verimli hizmet sunacak şekilde Sağlık ve Sosyal Yardım Bakanlığınca, diğer ilgili bakanlıkların da görüşü alınarak planlanır, koordine edilir, mali yönden desteklenir ve geliştirilir.
- b) Koruyucu sağlık hizmetlerine öncelik verilmek suretiyle kamu ve özel bütün sağlık kurum ve kuruluşlarının kurulması ve işletilmesinde kaynak israfı ve atıl kapasiteye yol açılmaksızın gerektiğinde hizmet satın alınarak kaliteli hizmet arzı ve verimliliği esas alınır. Sağlık ve Sosyal Yardım Bakanlığı ilgili Bakanlığın muvafakatını alarak, kamu ve özel bütün sağlık kurum ve kuruluşlarına koruyucu sağlık hizmeti görevi verir ve bu kurum ve kuruluşların bütün sağlık hizmetlerini denetler.
- c) Bütün sağlık kurum ve kuruluşları ile sağlık personelinin ülke sathında dengeli dağılımı ve yaygınlaştırılması esastır.Sağlık kurum ve kuruluşlarının kurulması ve işletilmesi bu esas içerisinde Sağlık ve Sosyal Yardım Bakanlığınca düzenlenir. Bu düzenleme ilgili Bakanlığın görüşü alınarak yapılır. Gerek görüldüğünde özel sağlık kuruluşlarının her türlü ücret tarifeleri sağlık ve Sosyal Yardım Bakanlığınca onaylanır.Kamu kurum ve kuruluşlarına ait sağlık kuruluşları veya sağlık işletmelerinde verilen her türlü hizmetin fiyatları Sağlık ve Sosyal Yardım Bakanlığınca tespit ve ilan edilir.

d) (Mülga: 31/5/2006-5510/106 md.)

e) Tesis edilecek eğitim, denetim, değerlendirme ve oto kontrol sistemi ile sağlık kuruluşlarının tespit edilen standart ve esaslar içinde hizmet vermesi sağlanır.

f) (Değişik: 24/3/2016-6698/30 md.) Herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi maksadıyla, Sağlık Bakanlığı ve bağlı kuruluşlarınca gerekli kayıt ve bildirim sistemi kurulur. Bu sistem, e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabilir. Bu amaçla, Sağlık Bakanlığınca, bağlı kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemi kurulabilir.

g) Sağlık ve Sosyal Yardım Bakanlığı; sağlık ve yardımcı sağlık personelinin yurt düzeyinde dengeli dağılımını sağlamak üzere istihdam planlaması yapar, ülke ihtiyacına uygun nitelikli sağlık personeli yetiştirilmesi amacıyla hizmet öncesi eğitim programları için Yükseköğretim Kurulu ile koordinasyonu sağlar. Serbest ya da kamu kuruluşlarında mesleklerini icra eden sağlık ve yardımcı sağlık personeline hizmetiçi eğitim yaptırır. Bunu sağlamak amacıyla üniversitelerin, kamu kurumu niteliğindeki meslek kuruluşları ile kamu kurum ve kuruluşlarının imkanlarından da yararlanır. Hizmetiçi eğitim programını ne şekilde ve hangi sürelerle yapılacağı Sağlık ve Sosyal Yardım Bakanlığınca çıkartılacak yönetmelikte tespit edilir.

h) (İptal: Ana.Mah.19.4.1988 tarih ve E. 1987/16, K. 1988/8 sayılı kararıyla.)

i) Sağlık hizmetlerinin yurt çapında istenilen seviyeye ulaştırılması amacıyla; bakanlıklar seviyesinden en uçtaki hizmet birimine kadar kamu ve özel sağlık kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları arasında koordinasyon ve işbirliği yapılır. Sağlık kurum ve kuruluşları coğrafik ve fonksiyonel hizmet alanları, verecekleri hizmetler, yönetim, hizmet ilişki ve bağlantıları gibi konularda tespit edilen esaslara uymak ve verilen görevleri yapmakla yükümlüdürler. Çağdaş tıbbi bilgi ve teknolojinin ülkeye getirilmesi ve teşviki sağlanır.

j) Vatandaşların hastalıklardan korunma, sağlıklı çevre, beslenme, ana çocuk sağlığı ve aile planlaması ve benzeri konularda eğitilmeleri ve takipleri bütün kamu kuruluşlarının sorumluluğu, kamu kurumu niteliğindeki meslek kuruluşları, özel ve gönüllü kuruluşların işbirliği içerisinde gerçekleştirilir.

k) Koruyucu, teşhis, tedavi ve rehabilite edici hizmetlerde kullanılan ilaç, aşı, serum ve benzeri biyolojik maddelerin üretiminin ve kalitesinin teşvik ve temini esas olup, her türlü müstahzar, terkip, madde, malzeme, farmakope mamülleri, kozmetikler ve bunların üretiminde kullanılan ham ve yardımcı maddelerin ithal, ihraç, üretim, dağıtım ve tüketiminin, amaç dışı kullanılmak suretiyle fizik

ve psişik bağımlılık yapan veya yapma ihtimali bulunan madde, ilaç, aşı, serum ve benzeri biyolojik maddeler ile diđer terkiplerin kontroluna, murakabesine ve bunların yurt içinde ve yurt dışında ücret karşılıđı kalite kontrollerini yaptırmaya, özel mevzuata göre ruhsatlandırma, izin ve fiyat verme işlerini yürütmeye Sağlık ve Sosyal Yardım Bakanlığı yetkilidir.

Özel mevzuatına göre izin veya ruhsat alınmamış ilaç ve terkiplerin üretimi, ithali, satışı ile ruhsat veya izin alınmış dahi olsa ilaç ve terkiplerin bilimsel araştırma amacıyla Sağlık ve Sosyal Yardım Bakanlığı ve ilgili kişinin rızası olmadan insan üzerinde kullanımı yasaktır.

l) (Ek: 30/5/1997 - KHK - 572/24 md.) Engelli çocuk doğumlarının önlenmesi için, gebelik öncesi ve gebelik döneminde tıbbi ve eğitsel çalışmalar yapılır. Yeni doğan bebeklerin metabolizma hastalıkları için gerekli olan testlerden geçirilerek risk taşıyanların belirlenmesine ilişkin tedbirler alınır. (1)

m) (Ek: 1/7/2005-5378/34 md.) Rehabilite edici tıbbi hizmetlerde kullanılan yardımcı araç ve gereçleri üretmek amacıyla, kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler tarafından kurulacak kuruluşların açılış iznini vermeye Sağlık Bakanlığı yetkilidir. Bu kurum ve kuruluşların açılış izninin verilmesine, üretim ve personel standardına, işleyiş ve denetimi ile daha önce açılmış olan kurum ve kuruluşların durumlarına ilişkin esaslar Sağlık Bakanlığınca çıkarılacak yönetmelikle düzenlenir.

2937 sayılı Devlet İstihbarat Hizmetleri Ve Milli İstihbarat Teşkilatı Kanunu

Resmî Gazete Tarihi : 03.11.1983

Resmî Gazete Sayısı : 18210

DEVLET İSTİHBARAT HİZMETLERİ VE MİLLİ İSTİHBARAT TEŞKİLATI KANUNU

BİRİNCİ KISIM

Genel Hükümler, Kuruluş ve Görevler

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç

Madde 1 - Bu Kanunun amacı; Devlet İstihbaratının istihsalı ve kullanılması ile Milli İstihbarat Teşkilatının kuruluş, görev ve faaliyetlerine ait esas ve usulleri düzenlemektir.

Tanımlar

Madde 2 - Bu Kanunda geçen deyimlerden;

- a) MİT: İstihbarat Teşkilatının kısaltılmış adı,
- b) MİT mensubu: Bu Kanun veya bu Kanuna göre çıkarılmış yönetmelikler de yazılı görevleri yerine getirmekle görevlendirilmiş MİT personeli ile diğer görevlileri,
- c) MİT personeli;
 1. MİT'in kadrosuna dahil memurları,
 2. Türk Silahlı Kuvvetleri kadrolarında olup MİT'de görevlendirilenleri,
 3. MİT'de çalıştırılan sözleşmeli personeli,
- ç) (Ek: 2/7/2018-KHK-703/152 md.) Teşkilat Başkanı: MİT Başkanı,

İfade eder.

İKİNCİ BÖLÜM

Kuruluş, Görev, Yetki ve Sorumluluk

Kuruluş

Madde 3 - Cumhurbaşkanına bağlı MİT kurulmuştur.

MİT; Başkan, Başkan yardımcıları, başkanlıklar, daireler ve şubeler ile diğer teşkilat birimlerinden oluşur.

MİT, Başkan tarafından idare edilir.

Milli İstihbarat Teşkilatının (...) teşkilatı ihtiyaca göre yönetmelikle düzenlenir.

Milli İstihbarat Teşkilatının görevleri

Madde 4 - Milli İstihbarat Teşkilatının görevleri şunlardır;

a) Türkiye Cumhuriyetinin ülkesi ve milleti ile bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, Anayasal düzenine ve milli gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkında milli güvenlik istihbaratını Devlet çapında oluşturmak ve bu istihbaratı Cumhurbaşkanı (...), Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile gerekli kuruluşlara ulaştırmak.

b) Devletin milli güvenlik siyasetiyle ilgili planların hazırlanması ve yürütülmesinde; Cumhurbaşkanı (...), Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile ilgili bakanlıkların istihbarat istek ve ihtiyaçlarını karşılamak.

c) Kamu kurum ve kuruluşlarının istihbarat faaliyetlerinin yönlendirilmesi için Cumhurbaşkanı (...) (2)ve Milli Güvenlik Kuruluna tekliflerde bulunmak.

d) Kamu kurum ve kuruluşlarının istihbarat ve istihbarata karşı koyma faaliyetlerine teknik konularda müşavirlik yapmak ve koordinasyonun sağlanmasında yardımcı olmak.

e) Genelkurmay Başkanlığınca Silahlı Kuvvetler için lüzum görülecek haber ve istihbaratı, yapılacak protokole göre Genelkurmay Başkanlığına ulaştırmak.

f) Milli Güvenlik Kurulunda belirlenecek diğer görevleri yapmak.

g) İstihbarata karşı koymak.

h) (Ek: 17/4/2014-6532/1 md.) Dış güvenlik, terörle mücadele ve millî güvenliğe ilişkin konularda Cumhurbaşkanınca (...) verilen görevleri yerine getirmek.

i) (Ek: 17/4/2014-6532/1 md.) Dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini

kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak.

j) (Ek: 17/4/2014-6532/1 md.) İstihbarat kapasitesini, niteliğini ve etkinliğini artırmak amacıyla çağdaş istihbarat usul ve yöntemlerini araştırmak, teknolojik gelişmeleri takip etmek ve uygun görülenleri temin etmek.

(Değişik birinci cümle: 17/4/2014-6532/1 md.) Millî İstihbarat Teşkilatına bu görevler dışında görev verilemez. Milli İstihbarat Teşkilatı birimlerinin görev, yetki ve sorumlulukları Cumhurbaşkanınca onaylanacak bir yönetmelikte belirtilir.

Bakanlıklar ve diğer kamu kurum ve kuruluşlarının görev ve yükümlülükleri

Madde 5 - Bakanlıklar ve diğer kamu kurum ve kuruluşlarının Devlet istihbaratına ilişkin görevleri şunlardır:

a) Kendi konularında;

1. Görevlerinin gerektirdiği istihbaratı oluşturmak,
2. MİT tarafından istenecek haber ve istihbaratı elde etmek,
3. İstihbarata karşı koymak.

b) Elde ettikleri milli güvenliğe ilişkin haber ve istihbaratı anında MİT'e ulaştırmak.

MİT mensuplarına hizmetlerinin yerine getirilmesi sırasında bakanlıklar ile diğer kamu kurum ve kuruluşları gereken her türlü yardım ve kolaylığı göstermekle yükümlüdürler.

(Değişik üçüncü fıkra: 15/8/2017-KHK-694/62 md.; Aynen kabul: 1/2/2018-7078/58 md.) Bakanlıklar ile diğer kamu kurum ve kuruluşlarının yukarıda belirtilen görev ve yükümlülüklerinin yerine getirilmesiyle ilgili koordinasyonu sağlamak ve istihbarat çalışmalarının yönetilmesinde temel görüşleri oluşturmak ve uygulamayı belirlemek üzere, Cumhurbaşkanının başkanlığında Milli İstihbarat Koordinasyon Kurulu (MİKK) kurulmuştur. Kurulun sekretarya hizmetleri MİT (...) tarafından yürütülür. (1)

(Mülga dördüncü fıkra: 15/8/2017-KHK-694/62 md.; Aynen kabul:1/2/2018-7078/58 md.)

(Mülga beşinci fıkra: 15/8/2017-KHK-694/62 md.; Aynen kabul: 1/2/2018-7078/58 md.)

(Değişik altıncı fıkra: 15/8/2017-KHK-694/62 md.; Aynen kabul: 1/2/2018-7078/58 md.) Milli İstihbarat Koordinasyon Kurulunun üyeleri, ayrıntılı görev ve yetkileri ile çalışma usul ve esasları yönetmelikle düzenlenir.

Yetkiler

Madde 6 - (Değişik birinci fıkra: 17/4/2014-6532/3 md.) Millî İstihbarat Teşkilatı bu Kanun kapsamındaki görevlerini yerine getirirken aşağıdaki yetkileri kullanır:

- a) Yerli ve yabancı her türlü kurum ve kuruluş, tüm örgüt veya oluşumlar ve kişilerle doğrudan ilişki kurabilir, uygun koordinasyon yöntemlerini uygulayabilir.
- b) Kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu kapsamındaki kurum ve kuruluşlar ile diğer tüzel kişiler ve tüzel kişiliği bulunmayan kuruluşlardan bilgi, belge, veri ve kayıtları alabilir, bunlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim alt yapısından yararlanabilir ve bunlarla irtibat kurabilir. Bu kapsamda talepte bulunulanlar, kendi mevzuatlarındaki hükümleri gerekçe göstermek suretiyle talebin yerine getirilmesinden kaçınamazlar.
- c) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun İkinci Kitap Dördüncü Kısım Dört, Beş, Altı ve Yedinci bölümlerinde yer alan suçlara (318, 319, 324, 325 ve 332 nci maddeleri hariç olmak üzere) ilişkin soruşturma ve kovuşturmalarda ifade tutanaklarına, her türlü bilgi ve belgeye erişebilir, bunlardan örnek alabilir.
- d) Görevlerini yerine getirirken gizli çalışma usul, prensip ve tekniklerini kullanabilir.
- e) İstihbari faaliyetler için görevlendirilenlerin kimliklerini değiştirebilir, kimliğin gizlenmesi için her türlü önlemi alabilir, tüzel kişilikler kurabilir. Kimliğin oluşturulması veya tüzel kişiliğin kurulması ve devam ettirilmesi için zorunlu olması durumunda gerekli belge, kayıt ve dokümanlar ile araç ve gereçler hazırlayabilir, değiştirebilir ve kullanabilir.
- f) Yabancıların ülkeye giriş ve çıkış ile vize, ikamet, çalışma izni ve sınır dışı edilmesi gibi konularda, ilgili kurum ve kuruluşlardan talepte bulunabilir.
- g) Telekomünikasyon kanallarından geçen dış istihbarat, millî savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplayabilir.
- h) Yabancı unsurların ülkenin ve vatandaşların iletişim güvenliğini tehdit eden faaliyetlerinin engellenmesine yönelik çalışmalar yapabilir, ilgili kurum ve kuruluşlardan talepte bulunabilir.
- i) MİT'te görev alan veya alacak kişilerin güvenilirliklerini ve uygunluklarını belirlemek için yalan makinası uygulaması dâhil test teknik ve yöntemlerini kullanabilir.

j) MİT mensupları görevlerini yerine getirirken ceza ve infaz kurumlarındaki tutuklu ve hükümlülerle önceden bilgi vermek suretiyle görüşebilir, görüşmeler yaptırabilir, görevinin gereği terör örgütleri dâhil olmak üzere millî güvenliği tehdit eden bütün yapılarla irtibat kurabilir.

(Ek fıkra: 3/7/2005 - 5397/3 md.) Bu Kanunun 4 üncü maddesinde sayılan görevlerin yerine getirilmesi amacıyla Anayasanın 2 nci maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde Devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, Devlet sırrının ifşasının tespiti ve terörist faaliyetlerin önlenmesine ilişkin olarak, hâkim kararı veya gecikmesinde sakınca bulunan hallerde Teşkilat Başkanı veya yardımcısının yazılı emriyle telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir. Gecikmesinde sakınca bulunan hallerde verilen yazılı emir, yirmidört saat içinde yetkili ve görevli hâkimin onayına sunulur. Hâkim, kararını en geç yirmidört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde tedbir derhal kaldırılır. Bu halde dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir. Bu işlemler, MİT tarafından kurulan merkez veya 4.7.1934 tarihli ve 2559 sayılı Polis Vazife ve Selahiyet Kanununun ek 7 nci maddesinin onuncu fıkrası hükmüne göre kurulan merkez tarafından yürütülür. (Değişik son cümle: 4/5/2007-5651/12 md.) 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun 135 inci maddesinin altıncı fıkrasının (a) bendinin (14) numaralı alt bendi kapsamında yapılacak dinlemeler de bu merkezler üzerinden yapılır.

(Ek fıkra: 3/7/2005 - 5397/3 md.; Değişik üçüncü fıkra: 17/4/2014-6532/3 md.) Yetkili ve görevli hâkim, Ankara ağır ceza mahkemesinin üyesidir.

(Ek fıkra: 3/7/2005 - 5397/3 md.) Kararda ve yazılı emirde, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, kullandığı telefon numaraları veya iletişim bağlantısını tespiti imkân veren kodundan belirlenebilenler ile tedbirin türü, kapsamı ve süresi ile tedbire başvurulmasını gerektiren nedenler belirtilir. Kararlar, en fazla üç ay için verilebilir; bu süre aynı usûlle üçer ayı geçmeyecek şekilde en fazla üç defa uzatılabilir. Ancak, casusluk faaliyetlerinin tespiti ve terör örgütünün faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi halinde, hâkim üç aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebilir.

(Ek fıkra: 3/7/2005 - 5397/3 md.) Uygulanan tedbirin sona ermesi halinde, dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir.

(Ek fıkra: 3/7/2005 - 5397/3 md.) Bu madde hükümlerine göre yürütülen faaliyetler çerçevesinde elde edilen kayıtlar, bu Kanunda belirtilen amaçlar dışında kullanılamaz. Elde edilen bilgi ve kayıtların saklanması ve korunmasında gizlilik ilkesi geçerlidir. (Mülga son cümle: 17/4/2014-6532/3 md.)

(Ek fıkra: 3/7/2005 - 5397/3 md.) Hâkim kararları ve yazılı emirler, MİT Müsteşarlığı görevlilerince yerine getirilir. İşlemin başladığı ve bitirildiği tarih ve saat ile işlemi yapanın kimliği bir tutanakla saptanır.

(Ek fıkra: 3/7/2005 - 5397/3 md.) Bu maddede yer alan faaliyetlerin denetimi, sıralı kurum amirleri ve Devlet Denetleme Kurulu (...) (2) tarafından yapılır. (2) (3)

(Ek fıkra: 3/7/2005 - 5397/3 md.) Bu maddede belirlenen usûl ve esaslara aykırı dinlemeler hukuken geçerli sayılmaz ve bu şekilde dinleme yapanlar hakkında 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu hükümlerine göre işlem yapılır.

(Ek fıkra: 3/7/2005 - 5397/3 md.; Değişik onuncu fıkra: 2/7/2018-KHK-703/152 md.) Bu maddenin uygulanmasına ilişkin esas ve usuller Cumhurbaşkanınca çıkarılan yönetmelikle düzenlenir.

(Ek fıkra: 17/4/2014-6532/3 md.) Önleyici istihbarat elde etmek ve analiz yapabilmek amacıyla yukarıdaki hükümlere ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın; Teşkilat Başkanı veya yardımcısının onayıyla yurt dışında veya yabancılar tarafından gerçekleştirilen iletişim ile ankesörlü telefonlarla gerçekleştirilen iletişim ve MİT mensuplarının, MİT'te görev almış olanların veya görev almak üzere başvuruların iletişimi tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir. (1)

(Ek fıkra: 17/4/2014-6532/3 md.) Bu Kanundaki görevlerin ifası ve yetkilerin kullanılmasına ilişkin usul ve esaslar yönetmelikle düzenlenir.

Bu Kanunda yazılı görevlerin yerine getirilmesi sırasında genel zabıtaya tanınmış olan hak ve yetkilerin, MİT mensuplarından kimlere tanınacağı, yönetmelikte belirtilir.

Sorumluluk

Madde 7 - Teşkilat Başkanı 4 üncü maddede belirtilen görevlerin yerine getirilmesinden Cumhurbaşkanına karşı sorumlu olup, Cumhurbaşkanının dışında herhangi bir kişi veya makama karşı sorumlu tutulamaz.

ÜÇÜNCÜ BÖLÜM

Olağanüstü Hal, (...) Seferberlik veya Savaş Hali

Madde 8 - Olağanüstü haller ile (...) seferberlik veya savaş halinin ilanında, Milli İstihbarat Teşkilatının bakanlıklar, Türk Silahlı Kuvvetleri ve diğer kamu kurum ve kuruluşlarıyla münasebetleri, Milli Güvenlik Kurulunun mütalaası alındıktan sonra Cumhurbaşkanı tarafından onaylanan yönetmelikle düzenlenir.

Bu hallerde MİT için gerekli görülecek ilave personel, her türlü teknik araç ve gereçler, akaryakıt, silah, savaş gereci, donatım ve giyecek, bina ve tesisler gibi ihtiyaçlar Milli Savunma, İçişleri ve ilgili bakanlık, kamu kurum ve kuruluşlarıyla MİT arasında önceden hazırlanacak planlarla belli edilir.

Seferberlik veya savaş halinin ilanında silah altına alınan MİT mensupları, MİT emrine tertip edilir.

İKİNCİ KISIM

Kadro, Personel ve Mali Hükümler

BİRİNCİ BÖLÜM

Kadro ve Personel İşleri

Kadro

Madde 9 - Milli İstihbarat Teşkilatının fiili kadrosu, her yıl tarafından tespit olunur ve Cumhurbaşkanı tarafından onaylanır.

Memur ve sözleşmeli personel

Madde 10 - MİT kadrolarında istihdam edilen memurlar, bu Kanunda belirtilen özel hükümler dışında, 657 sayılı Devlet Memurları Kanunu hükümlerine tabidir.

MİT'de istihdam edilen sözleşmeli personelin istihdam şekli, sözleşme esasları, alacakları ücretlerin taban ve tavanı ile sağlık işlerine ait esaslar, 657 sayılı Devlet Memurları Kanununun 4 üncü maddesindeki sözleşmeli personel istihdamına ilişkin şartlar aranmaksızın, yönetmelikle düzenlenir.

MİT'de sözleşmeli olarak çalıştırılan emekli personele ödenecek ücretler kendilerine sosyal güvenlik kuruluşlarınca bağlanmış olan emekli aylığının ve benzeri ödemelerin kesilmesini gerektirmez.

Askeri ve diğer personel

Madde 11 - (Değişik: 15/8/2017-KHK-694/67 md.; Aynen kabul: 1/2/2018-7078/63 md.)

Milli İstihbarat Teşkilatında görevlendirilecek subay, astsubay, sivil memur, uzman erbaş, erbaş ve erlerin sınıf, rütbe, unvan ve miktarları her yıl ihtiyaca göre ilgili kurumlar ve MİT tarafından müştereken tespit edilir. Bu kapsamda görevlendirilecek subay, astsubay, sivil memur, uzman erbaş, erbaş ve erler ilgisine göre İçişleri Bakanlığı, Milli Savunma Bakanlığı veya Genelkurmay

Başkanlığınca teklif edilir; bunların görevlendirilmesine ise MİT tarafından karar verilir. Bunların teşkilat içinde görevlendirilmeleri, bölge değiştirmeleri, ihtisas ve ihtiyaca göre MİT tarafından yapılır.

Milli İstihbarat Teşkilatında görevlendirileceklere ilişkin olarak 27/7/1967 tarihli ve 926 sayılı Türk Silâhlı Kuvvetleri Personel Kanunu ve diğer mevzuatta öngörülen izin, onay ve benzeri şartlar aranmaz.

Milli İstihbarat Teşkilatında görevlendirilen personelin her türlü istihkakları ilgili mevzuat hükümlerine göre bağlı buldukları kurum bütçesinden ödenir. Ancak, emsali MİT personeline (kadro karşılık gösterilmek suretiyle sözleşmeli çalışanlar dahil) net ödenen tüm istihkaklar toplamının, bunların tabi oldukları kanunlar gereğince aldıkları bütün ödemelerin net tutarından fazla olması halinde aradaki fark bu personele MİT bütçesinden tazminat olarak ve net ödenir. Bunların MİT'teki emsal kadro ve görev unvanlarını belirlemeye Teşkilat Başkanı yetkilidir.

Personele ilişkin özel hüküm

Madde 12 - MİT personelinin görev, yetki ve sorumlulukları genel hükümlere ilave olarak nitelikleri, atama ve hizmet süreleri, yer değiştirme esasları ile teşkilata alınma usul ve şartları ve teşkilatla ilişkilerinin kesilmesi gibi hususlar yönetmelikle düzenlenir.

(Ek fıkra: 15/8/2017-KHK-694/68 md.;Aynen kabul: 1/2/2018-7078/64 md.) MİT personelinin kimliğinin gizlenmesi esastır. Bu personele ilişkin özlük ve sosyal güvenlik haklarının tespitinde MİT (...) (1) kayıtları esas alınır. Buna ilişkin usul ve esaslar Sosyal Güvenlik Kurumu ile MİT (...) (1) tarafından müştereken hazırlanan ve Cumhurbaşkanı tarafından onaylanan yönetmelikle belirlenir.

Atama işlemleri

Madde 13 - (Mülga birinci fıkra: 2/7/2018-KHK-703/152 md.)

(Mülga ikinci fıkra: 2/7/2018-KHK-703/152 md.)

(Mülga üçüncü fıkra: 2/7/2018-KHK-703/152 md.)

(Değişik dördüncü fıkra: 2/7/2018-KHK-703/152 md.) MİT kadrolarına yapılacak atamalar Resmi Gazete'de yayımlanmaz ve gizli tutulur.

İstifa

Madde 14 - (Değişik: 20/11/2017-KHK-696/51 md.; Aynen kabul: 1/2/2018-7079/46 md.)

MİT fiili kadrosuna atanan personel teşkilata yazılı olarak müracaat etmek suretiyle istifa edebilir. MİT personeli hakkında 657 sayılı Kanunun çekilmiş sayılma ile ilgili hükümleri uygulanmaz. İstifa müracaatında bulunan personel hakkında; uhdesinde bulunan bilgi, belge ve kayıtlar, yürüttüğü faaliyetler, takip ettiği iş ve işlemler ile kullanımında bulunan kaynak ve diğer hususlara ilişkin olarak teşkilat tarafından bir rapor oluşturulur ve bu rapor sonucuna göre işlem yapılır.

MİT'te göreve başladıkları tarihten itibaren beş yıl geçmeden istifa edenler görevle ilişkilerinin kesildiği tarihten itibaren beş yıl geçmedikçe Devlet memurluğuna alınamazlar.

657 sayılı Kanunun 97 nci maddesinin birinci fıkrasının (D) bendi hükümleri saklıdır.

Zorunlu giderler

Madde 15 - MİT mensuplarına görevlerinin zorunlu kıldığı giderleri karşılamak üzere yönetmelikte belirlenecek miktar ve esaslara göre ödeme yapılır.

Bu harcamalar hakkında 1050 sayılı Muhasebei Umumiye Kanununun 77 nci maddesi hükmü uygulanır.

Hizmet tazminatı

Madde 16 - (Mülga : 13/7/1993 - KHK - 486/27 md.)

Madalya

Madde 16/A – (Ek: 17/4/2014-6532/4 md.)

Yurt içinde veya yurt dışında olağanüstü gayret ve fedakârlıkla yaptığı çalışmalar sonucunda; ülkenin ve milletin bölünmez bütünlüğünün korunmasında, Devletin yücelmesinde, millî menfaatlere katkıda ve hizmette üstün başarı ve yararlılık gösteren MİT personeline madalya verilebilir.

Birinci fıkra uyarınca verilecek madalyaların ebat, biçim ve özellikleri, kimlere ve nasıl verileceği ile bunların kaydına, muhafazasına ve taşınmasına ilişkin usul ve esaslar yönetmelikle düzenlenir.

Nakdi tazminat

Madde 17 - MİT mensuplarından:

a) Görevleri sırasında veya görevleri sona ermiş olsa bile MİT mensubu olmaları nedeniyle maruz kalacakları saldırı sonucu yaralanan, engelli hâle gelen veya ölenler hakkında 3/11/1980 tarih ve 2330 sayılı Nakdi Tazminat ve Aylık Bağlanması Hakkında Kanun hükümleri uygulanır.

b) Görevleri nedeniyle yaralanan veya hastalananlardan maluliyete uğrayanlara veya ölenlerin dul ve yetimlerine yoksa muhtaç ana ve babasına yoksa bakmakla yükümlü olduğu kardeşlerine genel hükümlere ilave olarak ayrıca tazminat verilir. Bu tazminatın miktarı birinci derecedeki Devlet memurunun maaşının brüt tutarının on katını geçemez.

c) Bu tazminatların birinden yararlanan diğerinden yararlanamaz.

Tazminatın verilmesine ait usul ve esaslar yönetmelikte gösterilir.

Sağlık İşleri

Madde 18 - (Mülga : 31/5/2006-5510/106 md.)

Başka kuruma nakil

Madde 19 - (Değişik: 15/8/2017-KHK-694/70 md.; Aynen kabul: 1/2/2018-7078/66 md.)

MİT fiili kadrosuna dahil personelden teşkilatın özelliği ve hizmetin gerekli kıldığı şart ve vasıflar gözönüne alınarak teşkilata intibak edemedikleri üstlerince tescil edilenler, Teşkilat Başkanının teklifi ve Cumhurbaşkanının uygun görmesi üzerine, genel hükümlere göre başka bir kurum veya kuruluşa naklen atanmak üzere Devlet Personel Başkanlığına bildirilir. Devlet Personel Başkanlığının yedi gün içinde atama teklifini yapmasını müteakip, ilgili kurum veya kuruluş tarafından on gün içinde atama işlemleri tamamlanarak ilgili personelin MİT ile ilişkisi kesilir.

İKİNCİ BÖLÜM

Mali Hükümler

Bütçe

Madde 20 - Milli İstihbarat Teşkilatının giderlerini karşılamak amacıyla her yıl Cumhurbaşkanlığı bütçesi içerisinde özel bir tertibe yeteri kadar ödenek konulur.

MİT (...) için konulan ödeneğin mali yıl içerisinde hizmete kafi gelmemesi halinde ihtiyaç duyulan ödenek Maliye Bakanlığınca öncelikle karşılanır.

MİT'e tahsis edilen ödeneklerin ita amiri Teşkilat Başkanıdır.

Teşkilat Başkanı bu yetkisini yazılı olarak devredebilir.

MİT (...) için Cumhurbaşkanlığı bütçesine konulan ödenekler, Yasama Organının ilgili komisyonunda gizli bir oturumda görüşülerek karara bağlanır.

MİT (...) bütçesinin hazırlanması ile harcama esas ve usulleri yönetmelikle belirlenir.

Gizli hizmet giderleri

Madde 21 - Teşkilat Başkanı gizli hizmet giderlerinin hizmetin gereklerine göre harcanmasından Cumhurbaşkanına karşı sorumludur.

Bütçe uygulaması

Madde 22 - MİT'in harcamaları, 1050 sayılı Muhasebe Umumiye Kanunu ile 2886 sayılı Devlet İhale Kanunu ve bunların ek ve değişikliklerine tabi değildir.

Bu konularda takip edilecek usul ve esaslar yönetmelikle tespit edilir.

Döviz tahsisi ve muafiyetler

Madde 23 - MİT tarafından yurt dışından sağlanacak her türlü silah, araç, gereç ve malzeme için acil ve zorunlu hallerde normal ithal kotası dışında öncelikle döviz tahsisi yapılır. Bu silah, araç, gereç ve malzemeler her ne yolla sağlanırsa sağlansın gümrük ve her türlü vergi, resim ve harçlardan muaftır.

Taşıt alımı

Madde 24 - MİT (...) 237 sayılı Taşıt Kanununun 4, 5 ve 6 ncı maddelerine tabi değildir. (3)

Aynı Kanunun 10 uncu maddesi uyarınca gerek yurt içinden ve gerekse yurt dışından alınacak araçların cins ve miktarı ile nereden alınacağı Cumhurbaşkanının onayı ile tespit edilir. (4)

Silah taşıma

Madde 25 - (Değişik: 17/4/2014-6532/5 md.)

MİT mensupları ile emeklileri, demirbaş silahları ve zatî silahlarını MİT (...) kayıtlarına geçirilmek ve MİT tarafından verilen belgelere işlenmek kaydıyla, meskûn mahaller dâhil her yerde taşıyabilirler.

Bu suretle düzenlenen belgeler taşıma izni belgesi yerine geçer.

ÜÇÜNCÜ KISIM

Çeşitli Hükümler

Soruşturma izni ve yargılama

Madde 26 - (Değişik: 17/2/2012-6278/1 md.)

MİT mensuplarının veya belirli bir görevi ifa etmek üzere kamu görevlileri arasından Cumhurbaşkanı (...) tarafından görevlendirilenlerin; görevlerini yerine getirirken, görevin niteliğinden doğan veya görevin ifası sırasında işledikleri iddia olunan suçlardan dolayı ya da 5271 sayılı Kanunun 250 nci

maddesinin birinci fıkrasına göre kurulan ağır ceza mahkemelerinin görev alanına giren suçları işledikleri iddiasıyla haklarında soruşturma yapılması Cumhurbaşkanının iznine bağlıdır.

(Ek fıkra: 17/4/2014-6532/6 md.) Cumhuriyet savcıları, MİT görev ve faaliyetleri ile mensuplarına ilişkin herhangi bir ihbar veya şikâyet aldıklarında veya böyle bir durumu öğrendiklerinde MİT'e bildirirler. MİT'in, konunun görev ve faaliyetlerine ilişkin olduğunu belirtmesi veya belgelendirmesi hâlinde adli yönden başkaca bir işlem yapılmaz ve herhangi bir koruma tedbiri uygulanmaz. Ancak birinci fıkra hükümlerine göre işlem yapılabilir.

(Ek fıkra: 17/4/2014-6532/6 md.) İsimsiz, imzasız, adresiz yahut takma adla yapıldığı anlaşılan ya da belli bir olayı ve nedeni içermeyen, delilleri ve dayanakları gösterilmeyen ihbar ve şikâyetler, Cumhuriyet savcılarınca işleme konulmaz.

(Ek fıkra: 17/4/2014-6532/6 md.; Değişik dördüncü fıkra: 15/8/2017-KHK-694/74 md.; Aynen kabul: 1/2/2018-7078/70 md.) Teşkilat Başkanı hakkında soruşturma yapılması Cumhurbaşkanının iznine bağlıdır. Soruşturma izni verilmesi veya verilmemesi kararlarına karşı on gün içinde Danıştay Birinci Dairesine itiraz edilebilir. İtirazlar öncelikle incelenir ve en geç üç ay içinde karara bağlanır. Verilen kararlar kesindir. İzin verilmesi üzerine soruşturma Yargıtay Cumhuriyet Başsavcısı tarafından yapılır. Hakim kararı gerektiren işlemlere dair Yargıtay Cumhuriyet Başsavcılığının talepleri ile kovuşturmayaya yer olmadığına dair kararlara yapılan itirazlar hakkında, soruşturma konusu suçların en ağırına bakmakla görevli Yargıtay ceza dairesini numara itibarıyla izleyen ceza dairesi başkanı tarafından karar verilir. Suçun son numaralı ceza dairesinin görevine girmesi halinde talebi inceleme yetkisi Birinci Ceza Dairesi Başkanına aittir. Hakim kararı gerektiren işlemlerde Başkanın verdiği kararlara karşı yapılan itirazı numara itibarıyla izleyen ceza dairesi başkanı inceler. Son numaralı daire başkanının kararı Birinci Ceza Dairesi Başkanı tarafından incelenir. İddianame hazırlanması halinde kovuşturma Yargıtay ilgili ceza dairesince yapılır.

(Ek fıkra: 17/4/2014-6532/6 md.) Aynı konuya ilişkin yeni ve somut bir delil ortaya çıkmadan yeniden soruşturma yapılamaz.

(Ek fıkra: 17/4/2014-6532/6 md.) MİT mensupları ile istihbarat hizmetlerine yardımları tevsik edilenler ve bunların eş, çocuk, ana, baba ve kardeşleri Teşkilat Başkanının onayıyla 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanununda yer alan koruma tedbirlerinden yararlandırılabilir.

(Ek fıkra: 17/4/2014-6532/6 md.) MİT mensuplarının görevlerini yerine getirirken, görevin niteliği gereği veya görevin ifası sebebiyle diğer kişilere vermiş oldukları zararlar idare tarafından tazmin

edilir. Tazmin, zararın göreve ilişkin bir husustan doğması ve ilgili personelin kasit veya ağır kusurunun bulunmaması hâlinde rücu işlemine konu edilmez.

(Ek fıkra: 17/4/2014-6532/6 md.; İptal fıkra: Anayasa Mahkemesi'nin 30/12/2015 tarihli ve E.: 2014/122, K.: 2015/123 sayılı Kararı ile.)

(Ek fıkra: 15/8/2017-KHK-694/74 md.; Aynen kabul: 1/2/2018-7078/70 md.) Türk vatandaşları hariç olmak üzere tutuklu veya hükümlü bulunanlar; ırkı, etnik kökeni, dini, vatandaşlığı nedeniyle cezalandırılmayacağı, onur kırıcı ceza veya muameleye tabi tutulmayacağı ya da işkence ve kötü muameleye maruz kalmayacağına ilişkin güvenceler bulunması kaydıyla, milli güvenliğin veya ülke menfaatlerinin gerektirdiği hallerde Dışişleri Bakanının talebi üzerine Adalet Bakanının teklifi ve Cumhurbaşkanının onayı ile başka bir ülkeye iade edilebilir veya başka bir ülkede tutuklu ya da hükümlü bulunanlar ile takas edilebilir.

Cezai hükümler

Madde 27 - (Değişik: 17/4/2014-6532/7 md.)

Millî İstihbarat Teşkilatının görev ve faaliyetlerine ilişkin bilgi ve belgeleri, yetkisiz olarak alan, temin eden, çalan, sahte olarak üreten, bunlar üzerinde sahtecilik yapan ve bunları yok eden kişiye dört yıldan on yıla kadar hapis cezası verilir.

MİT mensupları ve ailelerinin kimliklerini, makam, görev ve faaliyetlerini herhangi bir yolla ifşa edenler ile MİT mensuplarının kimliklerini sahte olarak düzenleyen veya değiştiren ya da bu sahte belgeleri kullananlara üç yıldan yedi yıla kadar hapis cezası verilir.

Birinci ve ikinci fıkra kapsamındaki bilgi ve belgelerin; radyo, televizyon, internet, sosyal medya, gazete, dergi, kitap ve diğer tüm medya araçları ile her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim araçları vasıtasıyla yayımlanması, yayılması veya açıklanması hâlinde; 9/6/2004 tarihli ve 5187 sayılı Basın Kanununun 11 inci maddesi ile 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 4 üncü ve 6 ncı maddeleri hükümlerine göre sorumlulukları belirlenenler ile bunları yayanlar hakkında üç yıldan dokuz yıla kadar hapis cezası verilir.

Bu Kanun kapsamındaki görev ve yetkilerin kullanılmasını engelleyenlere üç yıldan beş yıla kadar, ihmal veya suistimal suretiyle önleyenlerle yükümlülüklerini yerine getirmeyenlere iki yıldan dört yıla kadar hapis cezası verilir.

Söz konusu fiillerin MİT mensuplarınca işlenmesi hâlinde verilecek ceza üçte biri oranına kadar artırılır.

(Ek fıkra: 20/11/2017-KHK-696/52 md.; Aynen kabul: 1/2/2018-7079/47 md.) İstifa işlemleri tamamlanmadan görev yerini terk eden, görev yerinden veya görevi icabı bulunmak zorunda olduğu yerden izinsiz veya mazeretsiz olarak kesintisiz on gün süreyle ayrılan MİT personeli, yürütülecek idari soruşturma sonucuna göre Devlet memurluğundan çıkarılır. Bu kişilere iki yıldan dört yıla kadar hapis cezası verilir.

Taleplerin karşılanması

Madde 28 - (Değişik: 17/4/2014-6532/8 md.)

Bu Kanunda MİT'e verilen görev ve yetkiler çerçevesinde yapılan her türlü talep öncelikli olarak yerine getirilir, bu talepleri yerine getirenlerin hukuki ve cezai sorumluluğu doğmaz.

Bu Kanun ile diğer kanunlarda aynı konuyu düzenleyen farklı hükümler bulunması hâlinde bu Kanun hükümleri uygulanır.

Tanıklık

Madde 29 - (Değişik: 15/8/2017-KHK-694/76 md.; Aynen kabul: 1/2/2018-7078/72 md.)

Devletin çıkarlarının veya görevin gizliliğinin zorunlu kıldığı hâllerde MİT mensuplarının ve MİT'te görev yapmış olanların tanıklığı Teşkilat Başkanının, Teşkilat Başkanının tanıklığı ise Cumhurbaşkanının iznine bağlıdır.

İstisna

Madde 30 - Milli İstihbarat Teşkilatı merkez ve taşra kuruluşları ve personeli, Bakanlıkların Kuruluş ve Görev Esasları Hakkındaki Kanunun kapsamı dışındadır.

Milli İstihbarat Teşkilatında çalışan tabiplere Bazı Sağlık Personelinin Devlet Hizmeti Yükümlülüğüne Dair 21/8/1981 tarih ve 2514 sayılı Kanun hükümleri uygulanmaz. Ancak bunlardan pratisyen tabiplerin 4 yıl, uzman tabiplerin 4 yıl süre ile MİT'de sürekli çalışmaları şarttır.

(Ek fıkra: 17/4/2014-6532/10 md.) Kamu kurum ve kuruluşları ile diğer kurum ve kuruluşlar, bu Kanunda yazılı görevlerin yerine getirilmesi sırasında ihtiyaç duyulan hâllerde, kullanımlarında bulunan her türlü malzeme, ekipman, teçhizat ve cihazı, diğer kanunların bu konudaki düzenlemelerine bakılmaksızın MİT'e geçici olarak tahsis edebilir veya bedelsiz devredebilirler.

(Ek fıkra: 25/7/2018-7145/10 md.) MİT'in tarafı olduğu hukuk uyuşmazlıklarında, dava şartı olarak öngörülen arabuluculuk dâhil, arabuluculuk usulü uygulanmaz.

(Ek fıkra: 25/7/2018-7145/10 md.) MİT, 9/10/2003 tarihli ve 4982 sayılı Bilgi Edinme Hakkı Kanunu kapsamı dışındadır.

Fiili hizmet zammı

Madde 31 - MİT fiili kadrosuna dahil olup, halen çalışan memurların teşkilatta geçen hizmet sürelerine, görevlerine intisap tarihinden başlamak üzere, 5434 sayılı Kanunun 32 nci maddesine göre yılda üç aylık fiili hizmet zammı eklenir.

Yönetmelikler

Madde 32 - Bu Kanunun muhtelif maddelerinde çıkarılması öngörülen yönetmelikler, Cumhurbaşkanı tarafından onaylanmak suretiyle yürürlüğe konulur. Bu yönetmelikler Resmi Gazete'de yayımlanmaz.

Yürürlükten kaldırma

Madde 33 - 644 sayılı Milli İstihbarat Teşkilatı Kanunu ile ek ve değişiklikleri yürürlükten kaldırılmıştır.

Ek Madde 1 – (Ek: 17/4/2014-6532/11 md.)

Millî İstihbarat Teşkilatı uhdesindeki istihbari nitelikteki bilgi, belge, veri ve kayıtlar ile yapılan analizler, Türk Ceza Kanununun İkinci Kitap Dördüncü Kısım Yedinci Bölümünde yer alan suçlar hariç olmak üzere, adli mercilerce istenemez.

6 ncı maddenin birinci fıkrasının (e) bendine göre kimlikleri değiştirilenler, MİT'in görev ve faaliyetlerine yardımcı olanlar veya istihbarat hizmetlerinde istifade edilenler, kamu görevlisi olup olmadıklarına bakılmaksızın; görev, faaliyet ve yardımları sebebiyle sorumlu tutulamaz.

Teşkilat uhdesindeki bilgi ve belgelerin gizlilik derecelerinin ve sürelerinin tespit edilmesine, birim ve kısımlara ayrılmasına, kullanıma veya paylaşımına açılmasına ve bunların akademik çalışmalar ile her türlü yayın ve edebî eserde kullanılmasına Teşkilat Başkanı tarafından oluşturulacak bir Komisyonca karar verilir.

Ek Madde 2 – (Ek: 17/4/2014-6532/12 md.)

Bu maddede belirtilen görevleri yerine getirmek üzere, Türkiye Büyük Millet Meclisi bünyesinde Güvenlik ve İstihbarat Komisyonu kurulmuştur.

MİT tarafından yürütülen Devlet istihbarat hizmetleri ile Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Mali Suçları Araştırma Kurulu Başkanlığı tarafından görevleri gereği yürütülen güvenlik faaliyetlerine ve istihbari nitelikteki faaliyetlere ilişkin olarak İçişleri Bakanlığı, Maliye Bakanlığı ve MİT tarafından hazırlanacak yıllık raporlar Cumhurbaşkanlığına gönderilir. Cumhurbaşkanlığınca bu raporlar üzerine hazırlanacak yıllık rapor mart ayı içinde Güvenlik ve İstihbarat Komisyonuna sunulur. Komisyon, incelemelerini ve görüşmelerini raporun kendisine intikalinden itibaren doksan gün içinde tamamlar ve hazırlayacağı raporu bu süre içinde Türkiye Büyük Millet Meclisi Başkanlığına sunar.

Komisyonun üye sayısı on yedidir. Üye dağılımı siyasi parti gruplarının parti grupları toplam sayısı içindeki yüzde oranlarına göre yapılır.

Komisyonun görevleri şunlardır:

- a) Millî güvenliğe ilişkin konularda görüş ve öneriler sunmak
- b) Güvenlik ve istihbarat konularında uluslararası alanda kabul gören gelişmeleri izlemek
- c) Kendi faaliyetlerine ilişkin rapor hazırlamak
- d) Güvenlik ve istihbarat hizmetleri sırasında elde edilen kişisel verilerin güvenliğini ve bireyin hak ve özgürlüklerini koruyucu öneriler geliştirmek

Komisyon görüşmeleri kapalı oturumla yapılır. Kapalı oturumda Komisyon üyeleri, ilgili bakanlar, görevli hükümet temsilcileri ve Komisyonda görev yapan yasama uzmanları ile stenograflardan başkası bulunamaz.

Komisyon çalışmalarına ilişkin bilgi ve belgelerin saklanması ve korunmasında gizlilik esastır. Komisyon görüşmelerine katılanlar ile bu görüşmelere herhangi bir suretle vâkıf olanlar, Komisyon çalışmaları ve görüşülen konular hakkında hiçbir açıklama yapamaz ve bunları sır olarak saklamakla yükümlüdür.

Komisyon tarafından hazırlanan raporları ve bunların eklerini taşıyan, çoğaltan, teslim alanlar da dâhil olmak üzere tüm görevliler, bu raporların ve eklerinin korunması için gereken dikkat ve özeni göstermek zorundadır.

İlgili kurumlar ve Cumhurbaşkanlığınca hazırlanacak rapordaki, Komisyon raporlarında ve bunların ekleri ile Komisyon tutanaklarında, Devlet sırrı niteliğindeki bilgi ve belgelere yer verilmez.

Komisyonun çalışma usul ve esaslarına ilişkin olarak bu maddede hüküm bulunmayan hâllerde Türkiye Büyük Millet Meclisi İçtüzüğü hükümleri uygulanır.

İlgili kurumlar ve Cumhurbaşkanlığınca hazırlanacak raporların hazırlanmasına ve kapsamına ilişkin usul ve esaslar (...) yönetmelikle belirlenir.

Geçici Madde 1 - Bu Kanun yürürlüğe girdiği tarihte Milli İstihbarat Teşkilatının kuruluşu yeniden düzenlenir. Bu kuruluşa uygun şekilde yeniden kadrolar alınır.

Bu kadroların alınması ve atamaların yapılması tarihine kadar geçecek süre zarfında eski kadrolar yürürlükte kalır ve bu kadrolara istinaden ödemelere devam edilir.

Kanunun yürürlüğe girdiği tarihte Milli İstihbarat Hizmetleri Sınıfı personelinin memuriyet statülerinin gerçekleşmesi için alınmış bulunan her türlü onay bir defaya mahsus olmak üzere bu durumdaki personel için geçerli sayılır.

Geçici Madde 2 - Milli İstihbarat Teşkilatı personelinin, geçmiş yıllar için 31 inci maddeye göre fiili hizmet sürelerine eklenecek fiili hizmet zamları, ilave edilecek müddet hangi yıl için hesaplanmışsa o yılın emekli keseneği ve kurum karşılıkları ile aylık tutarına göre, kurumca tahakkuk ettirilir.

Geçici Madde 3 - Bu Kanunda öngörülen yönetmelikler yürürlüğe konuluncaya kadar 644 sayılı Kanun uyarınca çıkarılmış olan talimatların bu Kanuna aykırı olmayan hükümlerinin uygulanmasına devam olunur.

Geçici Madde 4 - (Ek: 17/2/2012-6278/2 md.)

Bu Kanunun yürürlüğe girdiği tarih itibarıyla hâlen devam eden soruşturma ve kovuşturmalar hakkında da 26 ncı madde hükümleri uygulanır.

Geçici Madde 5- (Ek: 15/8/2017-KHK-694/78 md.; Aynen kabul:1/2/2018-7078/74 md.)

Bu maddenin yürürlüğe girdiği tarihten önce;

a) 32 nci madde, 657 sayılı Kanunun 80 inci maddesi, 3238 sayılı Kanunun 10 uncu maddesinin ikinci fıkrası ile 6136 sayılı Kanunun ek 6 ncı maddesi uyarınca Başbakan onayı ile yürürlüğe konulan yönetmeliklerin,

b) Başbakan tarafından 657 sayılı Kanunun 43 üncü maddesi uyarınca belirlenen ek gösterge rakamları, 152 nci maddesi uyarınca belirlenen zam ve tazminatlar ve ek 29 uncu maddesi uyarınca belirlenen kadro karşılığı sözleşmeli personel çalıştırılmasına ilişkin usul ve esasların, yeni bir düzenleme yapıncaya kadar uygulanmasına devam olunur.

Diğer mevzuatta Milli İstihbarat Teşkilatı Müsteşarlığı ile ilgili olarak Başbakana yapılmış olan atflar Cumhurbaşkanına yapılmış sayılır.

Geçici Madde 6- (Ek: 2/7/2018-KHK-703/152 md.)

Bu maddenin yayımlandığı tarihte Milli İstihbarat Teşkilatı Müsteşarı ve Müsteşar Yardımcılarının kadro unvanı Milli İstihbarat Teşkilatı Başkanı ve Başkan Yardımcısı şeklinde değiştirilmiştir. Halen anılan kadrolarda bulunanlar başka bir işleme gerek kalmaksızın Milli İstihbarat Teşkilatı Başkanı ve Başkan Yardımcısı kadrolarına atanmış sayılır.

Milli İstihbarat Teşkilatı Başkanı ve Başkan Yardımcısına, sırasıyla Milli İstihbarat Teşkilatı Müsteşarı ve Müsteşar Yardımcısı için ilgili mevzuat hükümlerinde kadrosuna bağlı olarak öngörülmüş mali ve sosyal hak ve yardımlar kapsamındaki ödemeler aynı usul ve esaslar çerçevesinde yapılır. Bu ödemelerden vergi ve diğer kesintilere tabi olmayanlar bu maddeye göre de vergi ve diğer kesintilere tabi olmaz. Bunlar, emeklilik hakları bakımından da sırasıyla Milli İstihbarat Teşkilatı Müsteşarı ve Müsteşar Yardımcısına denk kabul edilir.

Diğer mevzuatta Milli İstihbarat Teşkilatı Müsteşarına ve Müsteşar Yardımcılarına yapılan atıflar Milli İstihbarat Teşkilatı Başkanına ve Başkan Yardımcılarına yapılmış sayılır.

Geçici Madde 7- (Ek: 2/7/2018-KHK-703/152 md.)

Diğer mevzuatta Milli İstihbarat Teşkilatı Müsteşarlığına veya MİT Müsteşarlığına yapılmış atıflar Milli İstihbarat Teşkilatına, MİT Müsteşarına yapılmış atıflar Milli İstihbarat Teşkilatı Başkanına yapılmış sayılır.

Yürürlük

Madde 34 - Bu Kanun 1 Ocak 1984 tarihinde yürürlüğe girer.

Yürütme

Madde 35 - Bu Kanunun hükümlerini Bakanlar Kurulu yürütür.

1/11/1983 TARİHLİ VE 2937 SAYILI ANA KANUNA İŞLENEMEYEN HÜKÜMLER:

1)3/7/2005 tarihli ve 5397 sayılı Kanunun geçici maddesi:

Geçici Madde -2559 sayılı Kanunun ek 7 nci maddesinde düzenlenen merkez, en geç altı ay içinde kurulur. Merkez kuruluncaya kadar 2559 sayılı Kanunun ek 7 nci maddesi, 2803 sayılı Kanunun ek 5 inci maddesi ve 2937 sayılı Kanunun 6 ncı maddesi hükümleri uyarınca verilen iletişimin dinlenmesi, tespiti, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasına dair karar veya yazılı emirler,

telekomünikasyon hizmeti veren kurum ve kuruluşlar tarafından derhal yerine getirilir; ilgili istihbarat kurumlarının mevcut sistemlerinin kullanılmasına devam olunur.

2920 sayılı Türk Sivil Havacılık Kanunu

Resmî Gazete Tarihi : 19.10.1983

Resmî Gazete Sayısı : 18196

TÜRK SİVİL HAVACILIK KANUNU

BİRİNCİ KISIM

Amaç, Kapsam ve Tanımlar

Amaç

Madde 1 - Bu Kanunun amacı; devamlı ve hızlı bir gelişme gösteren,ileri teknolojinin uygulandığı, sürat ve emniyet faktörlerinin büyük önem taşıdığı sivil havacılık sahasındaki faaliyetlerin ulusal çıkarlarımız ve uluslararası ilişkilerimize uygun bir şekilde düzenlenmesini sağlamaktır.

Kapsam

Madde 2 - Bu Kanun,kamu kurum ve kuruluşları ile gerçek ve özel hukuk tüzelkişilerinin havacılık sahasındaki faaliyetlerini kapsar.

Devlet hava araçları, açık hüküm bulunmayan hallerde bu Kanunun kapsamı dışındadır.

(...)

Milli Sivil Havacılık Güvenlik Kurulu ve havacılık güvenliği

Madde 40 - (Değişik: 28/11/2017-7061/39 md.)

Tüm sivil havacılık faaliyetleri ile sivil havacılık tesis ve eklentilerinin yasadışı eylemlere karşı korunması amacıyla uluslararası uygulamalara uygun olarak gereken mevzuatı hazırlamak, denetlemek, uygun eğitimlerin alınmasını sağlamak ve ülkemizi uluslararası kuruluşlar nezdinde temsile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı yetkilidir. Bakanlık, bu görevini öncelikle İçişleri Bakanlığı olmak üzere diğer kurum ve kuruluşlar ile koordineli şekilde yürütür.

(Mülga ikinci fıkra: 2/7/2018-KHK-703/189 md.)

Sivil havacılık alanında faaliyet gösteren tüm kurum ve kuruluşlar, şahıslar ve yolcuların uyması gereken güvenlik tedbirleri ile yasaklanan hususlar, 5/6/1945 tarihli ve 4749 sayılı Kanunla uygun bulunan Şikago Sözleşmesinin 17 numaralı eki ile uluslararası uygulamalara ve önlemlere uygun

olarak Milli Sivil Havacılık Güvenlik Kurulu tarafından hazırlanan ve İçişleri Bakanlığı ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından müştereken çıkarılan yönetmelikle düzenlenir. Acil durumlarda alınması gereken ilave tedbirler, İçişleri Bakanlığı temsilcisinin başkanlığında, Gümrük ve Ticaret Bakanlığı, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı temsilcileri, Sivil Havacılık Genel Müdürü ve Devlet Hava Meydanları İşletmesi Genel Müdüründen oluşan Güvenlik Komisyonu tarafından alınır.

Havaalanlarında, ulusal ve uluslararası mevzuata göre güvenliğin sağlanması, havacılık güvenliğine yönelik kurum ve kuruluşlar arasında işbirliği ve koordinasyonun tesis edilmesi, kurum ve kuruluşların havacılık güvenliğine yönelik çalışmalarının denetlenmesi, denetim sonuçlarının takibi ve icrası, havaalanı güvenlik programının oluşturulması ve icrası 10/6/1949 tarihli ve 5442 sayılı İl İdaresi Kanunu uyarınca görevlendirilen mülki idare amiri tarafından yerine getirilir. Havaalanı mülki idare amirlerinin havaalanlarındaki havacılık güvenliğine ilişkin görev, yetki ve sorumlulukları İçişleri Bakanlığının uygun görüşü üzerine Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından çıkarılan yönetmelikte düzenlenir.

Havayolu ile seyahat edecek kişilerin bilgileri kişilerin seyahatini kolaylaştırmak veya güvenlik ve risk değerlendirmesi yapmak amacıyla 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu çerçevesinde toplanabilir, kaydedilebilir, işlenebilir, paylaşılabilir, havacılık güvenliği ve emniyetini sağlamak üzere değerlendirilerek gereken tedbirler alınabilir. Bu kapsamda, talep halinde yolcu bilgileri havayolu işletmeleri veya kurumlar tarafından üçüncü ülkelerle İçişleri Bakanlığının uygun görüşü ile paylaşılabilir. İçişleri Bakanlığı değerlendirme esnasında ilgili tüm kurum ve kuruluşlar ile koordine sağlar ve mütekabiliyet çerçevesinde karar verir.

Türk tescilli sivil hava araçlarında özel eğitimli silahlı güvenlik görevlileri bulundurulabilir. Türkiye'ye uçuşu olan yabancı tescilli sivil hava araçlarında silahlı güvenlik görevlisi bulundurulmasına izin verilmesine, mütekabiliyet ilkesi saklı kalmak kaydıyla İçişleri Bakanlığı yetkilidir. Silahlı güvenlik görevlisinin görev, yetki ve sorumlulukları İçişleri Bakanlığı tarafından çıkarılan yönetmelikle düzenlenir.

2559 sayılı Polis Vazife ve Selâhiyet Kanunu

Resmî Gazete Tarihi : 14.07.1934

Resmî Gazete Sayısı : 2751

POLİS VAZİFE VE SALÂHİYET KANUNU

Madde 1 - Polis, asayiş amme, şahıs, tasarruf emniyetini ve mesken masuniyetini korur. Halkın ırz, can ve malını muhafaza ve ammenin istirahatini temin eder.

Yardım isteyenlerle yardıma muhtaç olan çocuk, alil ve acizlere muavenet eder. Kanun, Cumhurbaşkanlığı karnameleri ve ilgili mevzuatın kendisine verdiği vazifeleri yapar.

(...)

Parmak izi ve fotoğrafların kayda alınması

Madde 5- (Değişik: 2/6/2007-5681/2 md.)

Polis;

- a) Gönüllü,
- b) Her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunan,
- c) Başta polis olmak üzere, genel veya özel kolluk görevlisi ya da özel güvenlik görevlisi olarak istihdam edilen,
- ç) Türk vatandaşlığına başvuruda bulunan,
- d) Sığınma talebinde bulunan veya gerekli görülmesi halinde, ülkeye giriş yapan sair yabancı,
- e) Gözaltına alınan,

kişilerin parmak izini alır.

Birinci fıkraya göre alınan parmak izi, ait olduğu kişinin kimlik bilgileri ile birlikte, ne zaman ve kim tarafından alındığı belirtilmek suretiyle, bu amaca özgü sisteme kaydedilerek saklanır. Ancak, parmak izinin hangi sebeple alındığı sisteme kaydedilmez.

Olay yerinden elde edilen ve kime ait olduğu henüz tespit edilemeyen parmak izleri, kime ait olduğu tespit edilinceye kadar, ilgili soruşturma dosya numarası ile birlikte sisteme kaydedilir.

5271 sayılı Ceza Muhakemesi Kanununun 81 inci maddesi ile 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanunun 21 inci maddesi hükümlerine göre alınan parmak izleri de bu sisteme kaydedilir.

(a) bendi hariç birinci fıkra ile dördüncü fıkra kapsamına giren kişilerin ayrıca fotoğrafları alınarak, ikinci fıkrada belirlenen esaslara uygun olarak parmak izi ile birlikte sisteme kaydedilir.

Bu sistemde yer alan bilgiler, kimlik tespiti, suçun önlenmesi veya yürütülmekte olan soruşturma ve kovuşturma kapsamında maddî gerçeğin ortaya çıkarılması amacıyla mahkeme, hâkim, Cumhuriyet savcısı ve kolluk tarafından kullanılabilir.

Kolluk birimleri, kimlik tespiti yapmak ya da olay yerinden alınan parmak izini karşılaştırmak amacıyla doğrudan bu sistemle bağlantı kurabilir.

Sistemde kayıtlı bilgilerin hangi kamu görevlisi tarafından ve ne amaçla kullanıldığının denetlenebilmesine imkân tanıyan bir güvenlik sistemi kurulur.

Sistemde yer alan kayıtlar gizlidir; altıncı ve yedinci fıkralarda belirlenen amaçlar dışında kullanılamaz.

Sisteme kayıtlı olan parmak izi ve fotoğraflar, kişinin ölümünden itibaren on yıl ve her halde kayıt tarihinden itibaren seksen yıl geçtikten sonra sistemden silinir.

Parmak izi ile fotoğrafların sistemde kaydedilmesi ve saklanması ile bu kayıtlardan yararlanmaya ilişkin diğer esas ve usûller, İçişleri Bakanlığı tarafından Adalet Bakanlığının görüşü alınarak çıkarılacak yönetmelikle düzenlenir.

(...)

Adli görev ve yetkiler

Ek Madde 6 - (Ek: 16/6/1985 - 3233/7 md.; Değişik: 2/6/2007-5681/5 md.)

Polis, bu maddede yazılı görevlerinin yanında, Ceza Muhakemesi Kanunu ve diğer mevzuatta yazılı soruşturma işlemlerine ilişkin görevleri de yerine getirir.

Polis, bir suça ilişkin olarak kendisine yapılan sözlü ihbar ve şikâyetleri ve görevi sırasında öğrendiği suça ilişkin bilgileri yazılı hale getirir.

Edinilen bilgi veya alınan ihbar veya şikâyet üzerine veya kendiliğinden bir suçla karşılaşan polis, olay yerinde kişilerin ve toplumun sağlığına, vücut bütünlüğüne veya malvarlığına zarar gelmemesi ve suçun delillerinin kaybolmaması ya da bozulmaması için derhal gerekli tedbirleri alır.

Bir suç işlendiği veya işlenmekte olduğu bilgisini edinen polis, olay yerinin korunması, delillerin tespiti, kaybolmaması ya da bozulmaması için acele tedbirleri aldıktan sonra el koyduğu olayları, yakalanan kişiler ile uygulanan tedbirleri derhal Cumhuriyet savcısına bildirir ve Cumhuriyet savcısının emri doğrultusunda işin aydınlatılması için gerekli soruşturma işlemlerini yapar.

Yapılacak araştırma sonunda edinilen bilginin bir kabahate ilişkin olduğu hallerde, konu araştırılarak gerekli yasal işlem yapılır veya yapılması sağlanır.

Olay yerinde görevine ait işlemlere başlayan polis, bunların yapılmasına engel olan veya yetkisi içinde aldığı tedbirlere aykırı davranan kişileri, işlemler sonuçlanıncaya kadar ve gerektiğinde zor kullanarak bundan men eder.

Polis, suçun delillerini tespit etmek amacıyla, Cumhuriyet savcısının emriyle olay yerinde gerekli inceleme ve teknik araştırmaları yapar, delilleri tespit eder, muhafaza altına alır ve incelenmek üzere ilgili yerlere gönderir.

Olay yeri dışında kalan ve o suça ilişkin delil elde edilebileceği yönünde kuvvetli şüphe sebebi bulunan konut, işyeri ve kamuya açık olmayan kapalı alanlarda yapılacak işlemler için Ceza Muhakemesi Kanununun arama ve elkoymaya ilişkin hükümleri uygulanır.

Polis, olaydaki failin, gözaltına alınan şüpheli ile aynı kişi olup olmadığının belirlenmesi bakımından zorunlu olması halinde, Cumhuriyet savcısının talimatıyla teşhis yaptırabilir.

Tanıklıktan çekinebilecek olanlar, teşhiste bulunmaya zorlanamaz.

İşleme başlanmadan önce, teşhiste bulunacak kişinin faili tarif eden beyanları tutanağa bağlanır.

Teşhis işlemine tâbi tutulan kişilerin birden fazla ve aynı cinsten olması, aralarında yaş, boy, ağırlık, giyinme gibi görünüşe ilişkin hususlarda benzerlik bulunması gerekir. Teşhis için gerekli olması halinde, şüphelinin görünüşü ile ilgili gerekli değişiklikler yapılabilir. Teşhis işlemine tâbi tutulan kişilerin her birinde, teşhis sırasında bir numara bulundurulur.

Teşhiste bulunan kişi ile teşhis işlemine tâbi tutulan kişilerin birbirini görmemesi gerekir.

Teşhis işlemi en az iki kez tekrarlanır ve teşhiste bulunması istenen kişiye, şüphelinin teşhis edilecek kişiler arasında yer almıyor olabileceği hatırlatılır.

Teşhis işlemine tâbi tutulan kişilerin, bu işlem sırasında birlikte fotoğrafları çekilerek veya görüntüleri kayda alınarak, soruşturma dosyasına konur.

Şüphelinin fotoğrafı üzerinden de teşhis yaptırılabilir. Ancak tek bir fotoğraf veya aynı kişinin farklı fotoğrafları üzerinden teşhis yaptırılamaz. Değişik kişilerin fotoğraflarının aynı büyüklük ve özellikte olmaları gerekir.

Teşhis işlemi tutanağa bağlanır. (Ek fıkra: 2/1/2017-KHK-680/27 md.; Aynen kabul: 1/2/2018-7072/26 md.) (İptal onsekizinci fıkra:Anayasa Mahkemesinin 19/2/2020 tarihli ve E.:2018/91 K.:2020/10 sayılı kararı ile)

1774 sayılı Kimlik Bildirme Kanunu

Resmî Gazete Tarihi : 11.07.1973

Resmî Gazete Sayısı : 14591

KİMLİK BİLDİRME KANUNU

Madde 1 - Bu Kanunda sayılan, özel veya resmi, her türlü konaklama, dinlenme bakım ve tedavi tesisleri ve işyerleri ile konutlarda geçici veya sürekli olarak kalanlar, oturanlar, çalışanlar ve ayrılanlar ile araç kiralayan gerçek ve tüzel kişilerin kimliklerinin tespiti ve bildirilmesi bu Kanunun hükümlerine göre yapılır. (1)

Askeri konaklama, dinlenme ve kamp tesisleri ile ordu evleri bu Kanunun kapsamı dışındadır.

Madde 2 - Otel, motel, han, pansiyon, bekar odaları, günübirlik kiralanan evler, kamp, kamping, tatil köyü ve benzeri her türlü, özel veya resmi konaklama yerleri ile özel sağlık müesseseleri, dinlenme ve huzur evleri, dini ve hayır kurumlarının sosyal tesislerinin sorumlu işleticileri, bu yerlerde ücretli veya ücretsiz, gündüz veya gece, yatacak yer gösterdikleri yerli veya yabancı herkesin kimlik ve geliş-ayrılış kayıtlarını, örneğine ve usulüne uygun şekilde günü gününe tutmak, genel kolluk örgütlerinin her an incelemelerine hazır bulundurmak, Devlet İstatistik Enstitüsüne, talebi halinde vermek zorundadırlar. (2)

Madde 3 - İkinci maddede sayılan tesislerin sorumlu işleticilerinin kimlikleri, tesis açılmadan evvel müessesenin sahibi veya kanuni temsilcisi tarafından örneğine uygun şekilde, en yakın kolluk örgütüne bildirilir.

Sorumlu işleticinin değişmesi halinde keyfiyetin 24 saat içinde ve yukarıdaki fıkrada gösterilen şekilde bildirilmesi zorunludur.

İşleticiler, kendilerine bu konuda verilen görev ve yükümlülükleri, kendi sorumlulukları altında yöneticilerine devredebilirler.

Bu durumda işletici ve yönetici müştereken sorumlu olurlar.

Kamu kuruluşlarına ait tesislerin amir ve müdürleri işletici gibi sorumludurlar.

Madde 4 - İkinci maddedeki tesislerin sorumlu işleticileri, müesseselerinde sürekli veya geçici olarak çalıştırdıkları kimseleri ve bunların ayrılışlarını, örneğine uygun kimlik bildirme belgesi doldurarak, 24 saat içinde bağlı oldukları en yakın kolluk örgütüne bildirirler.

Kolluk örgütüne bildirilerek çalıştırılanlara, sorumlu işletici tarafından doldurulup onaylanan, örneğine uygun bir kimlik kartı verilir.Kolluk görevlilerince her istenildiğinde bu kimlik kartının gösterilmesi zorunludur.

Madde 5 - (Mülga: 25/4/2006 - 5490/71 md.)

Madde 6 - Şehir, kasaba ve köy sınırları içindeki;

a) (Mülga: 25/4/2006 - 5490/71 md.)

b) Bu Kanunun ikinci maddesinde sayılanlar dışında kalan her çeşit ticaret ve sanat amacı güden iş yerlerinde çalışanlar ve buralarda her türlü barındırmalar için iş yerlerinin sorumlu işleticisi;

c) Öğrenci yurtları ve benzeri yerlerde çalışanlar ile bu yerlerde kalmakta olan öğrenciler için o yerin sorumlu işleticisi;

(Ek ibare: 25/4/2006 - 5490/72 md.) tarafından örneğine uygun kimlik belgesi doldurularak üç gün içinde genel kolluk örgütüne verilmesi zorunludur.

d) (Mülga: 25/4/2006 - 5490/71 md.)

Konutun değiştirilmesi veya (b) ve (c) bentlerinde sayılan konut, iş yeri ve yurtlarda çalışmakta veya barınmakta olanların ayrılmaları halinde de, yukarıdaki şekil ve süre içinde bildirim belgesi gereklidir. (1)

(Değişik: 29/8/1996 - 4178/8 md.) Kimlik bildirimleri, mahalli kolluk örgütüne verilmeden evvel mahalle veya köy muhtarına onaylatılır.

(Ek fıkra:25/3/2020-7226/5 md.) Bu bildirimler sorumlu işleticiler tarafından, yukarıda belirtilen süre içerisinde genel kolluk kuvvetlerine elektronik ortamda da yapılabilir. Bildirimlerin elektronik ortamda yapılması durumunda üçüncü fıkra hükmü uygulanmaz. Bu fıkra kapsamında elektronik ortamda yapılan bildirimler, genel kolluk tarafından köy ve mahalle muhtarları ile paylaşılır.

Madde 7 - Geçici yer değiştirmelerde;

a) Konutlarda 30 günden fazla kalacak misafir için aile reisi;

b) Yaylak ve kışlak gibi yerlere mevsimlik olarak göçenler için de aile reisi tarafından, örneğine uygun bildirim,

Üç gün içinde kolluk örgütüne verilir.

(Ek fıkra: 28/11/2017-7061/36 md.) Mevsimlik tarım işçisi olarak sürekli ikametinin dışında bir başka ilde çalışmak amacıyla geçici olarak yer değiştirenlerin kimlik bildirimleri, bu kişilerin yaşadıkları geçici yerleşim alanlarında doğrudan kolluk kuvvetlerince alınır ve bu bildirimler Çalışma ve Sosyal Güvenlik Bakanlığı ile elektronik ortamda paylaşılır.

Madde 8 - (Mülga: 25/4/2006 - 5490/71 md.)

Madde 9 - Bu Kanun hükümlerine göre kimlik bildirme belgesini yetkili idareye vermekle yükümlü tutulanlar, kimliğini nüfus hüviyet cüzdanı ve diğer resmi geçerli belgelerle ispat edemeyen kimseleri tesislerinde barındıramaz, konut ve işyerlerinde çalıştıramaz.

Madde 10 - Kahvehane, oyun salonu, kulüp, lokal ve benzeri yerlerde ve bu Kanunun kapsamına giren diğer yatsız iş yerlerinde, özel kanunları müsaade ettiği takdirde, ancak sahipleri ve çalıştırdıkları kimseler yatabilir, başkaları kalamazlar.

İskele, istasyon, hava meydanı terminal, garaj, benzin istasyonu ve benzeri kara, deniz ve hava ulaşım merkezleri ile fuar, panayır, sergi ve pazar kurulması gibi zorunluluk olan zaman ve yerlerde, sabahçı kahvesi ve benzeri diğer tesislere, bağlı olduğu kolluk kuvvetinin görüşü alınmak şartıyla belediye veya il özel idaresi tarafından geçici veya, sürekli olarak izin verilebilir. Buralarda kalanlar için bildirim yapılmaz.

Madde 11 - Kat mülkiyetine tabi taşınmaz mal yöneticileri ve kapıcıları, binalarında bildirim dışı kimselerin oturup oturmadığını, çalışıp çalışmadığını, garaj, kömürlük, boş daire gibi bölümlere saklanmalar, sığınmalar, bazı eşya veya maddeleri gizlemeler olup olmadığını kontrol etmekle yükümlüdürler.

Bütün kat sahipleri ve kiracıları ile binada çalışanlar bu konularda yöneticiye yardımcı olmak ve gereken bilgileri vermek zorundadırlar.

Yönetici ve kapıcıların, bu Kanuna aykırılıkları ve diğer şüpheli gördükleri hususları, bağlı oldukları genel kolluk örgütüne bildirmeleri gereklidir.

Madde 12 - Bu Kanunun bildirimlerle ilgili maddelerinin uygulama biçimi, söz konusu kimlik bildirme belge, defter ve kartlarının şekli, muhtevası, verilmesi, alınması, Adalet, İçişleri, Turizm ve Tanıtma ve Devlet İstatistik Enstitüsü işlerine bakan Devlet Bakanlıklarınca müştereken hazırlanacak bir yönetmelikle gösterilir.

Madde 13 - (Mülga: 29/8/1996 - 4178/9 md.)

Madde 14 - Bu Kanuna göre verilecek belgeler ve yapılacak her türlü bildirimler, her çeşit vergi, resim ve harçtan muaftır. Mahkeme kararı olmadıkça, yetkili resmi örgütler dışında, hiç kimsenin bunlardan yararlanmasına müsaade edilemez.

Madde 15 - (Değişik: 23/1/2008-5728/363 md.) (1)

(...) (1) 3 ve 4 üncü maddelerdeki yükümlülüklerden her birine aykırı hareket edenlere ikiyüzelli Türk Lirası idarî para cezası verilir.

Madde 16 - (Mülga: 25/4/2006 - 5490/71 md.)

Madde 17 - (Değişik: 23/1/2008-5728/364 md.)

6, 7, 9, 10 ve 11 inci maddelerdeki hükümlere aykırı hareket edenlere yirmi Türk Lirası; kimlik bildirme belgesinde gerçeğe uymayan bilgi verenlere yüz Türk Lirası idarî para cezası verilir.

Madde 18 - (Değişik: 23/1/2008-5728/365 md.)

Bu Kanunda belirtilen idarî para cezaları, mahallî mülkî amir tarafından verilir.

Madde 19 - 10/6/1930 tarihli ve 1704 sayılı Otel Pansiyon, Ticarethane vesair Umumi Müesseselerde Oturan ve Çalışanların Hüviyet Varakası Vermeleri Mecburiyetine dair Kanun ile bu Kanunun bazı maddelerini tadil ve tashih icrasına ve bir madde ilavesine dair 14/1/1933 tarih ve 2099 sayılı Kanun yürürlükten kaldırılmıştır.

Ek Madde 1 - (Ek: 29/8/1996 - 4178/10 md.)

Bu Kanunun uygulanması sırasında genel kolluk kuvvetlerine ait karakollara, il merkezlerinden de sorgulanabilen bilgisayar terminalleri konulur. Bunun için gerekli giderler İçişleri Bakanlığı bütçesine konulacak ödenekten karşılanır.

(Değişik ikinci fıkra: 31/10/2016-KHK-678/4 md.; Aynen kabul: 1/2/2018-7071/4 md.) Bu Kanunun 2 nci maddesinde sayılan özel veya resmi her türlü konaklama tesisleri tüm kayıtlarını bilgisayarda günü gününe tutmak, genel kolluk kuvvetlerinin bilgisayar terminallerine bağlanarak mevcut bilgi, belge ve kayıtları genel kolluk kuvvetlerine anlık olarak bildirmek zorundadırlar.

(Ek fıkra: 31/10/2016-KHK-678/4 md.; Aynen kabul: 1/2/2018-7071/4 md.) İkinci fıkrada belirtilen genel kolluk kuvvetlerinin terminallerine bağlanmayanlara onbin Türk Lirası, anlık veri göndermeyen veya gerçeğe aykırı kayıt tutanlara beşbin Türk Lirası idari para cezası, mülki idare amirlerince verilir. Bu fiillerin tekrarı halinde işletme ruhsatları iptal edilir. Bu maddeye göre verilen idari para cezaları tebliğinden itibaren bir ay içinde ödenir.

(Ek fıkra: 31/10/2016-KHK-678/4 md.; Aynen kabul: 1/2/2018-7071/4 md.) Bu Kanunun 2 nci maddesinde sayılan özel veya resmi her türlü konaklama tesisleri, ikinci fıkrada belirtilen genel kolluk kuvvetlerinin terminallerine bağlanmak için gerekli işlemleri bu maddenin yürürlüğe girdiği tarihten itibaren iki ay içinde tamamlar.

(Ek fıkra: 31/10/2016-KHK-678/4 md.; Aynen kabul: 1/2/2018-7071/4 md.) Bu maddenin uygulanması ile görevi gereği bu verileri kullanan kamu personelinin denetimine ilişkin usul ve esaslar İçişleri Bakanlığı tarafından belirlenir.

Ek Madde 2 - (Ek: 15/5/2008-5763/12 md.)

Bu Kanunun 4 üncü ve 6 ncı maddeleri gereğince verilen sürekli veya geçici olarak çalışanlara ait kimlik bilgileri, genel kolluk kuvvetlerince ilgili Sosyal Güvenlik Kurumu Başkanlığı il müdürlükleri veya merkez müdürlüklerine bildirilir.

Ek Madde 3 - (Ek: 27/3/2015-6638/19 md.)

Araç kiralama şirketlerinin sorumlu işleticileri ve yöneticileri, kiralanan araç bilgileri ile aracı kiralayanların kimlik bilgileri ve kira sözleşmesi kayıtlarını usulüne uygun şekilde günü gününe tutmak ve bu kapsamda mevcut bilgi, belge ve kayıtları genel kolluk kuvvetlerinin her an incelemelerine hazır bulundurmak zorundadırlar. Ancak araç kiralayanın kamu kurum veya kuruluşu olması hâlinde sadece kamu kurum veya kuruluşuyla yapılan sözleşme ile araç bilgileri sisteme kaydedilir.

Araç kiralama esnasında gerçeğe aykırı kimlik kullananlar ile birinci fıkra kapsamında elde edilen bilgi ve kayıtları, hukuka aykırı olarak kullanan, bir başkasına veren, yayan veya ele geçiren kişi, 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu hükümlerine göre cezalandırılır.

Birinci fıkrada belirtilen yükümlülüklerle aykırı hareket edenlere beş bin Türk Lirası, gerçeğe aykırı kayıt tutan veya bilgi verenlere on bin Türk Lirası idari para cezası, mülki idare amirlerince verilir. Bu Kanuna göre verilen idari para cezaları tebliğinden itibaren 1 ay içinde ödenir. İşlenen bir suçun gizlenmesi amacıyla bilgilerin yok edilmesi hâlinde işletme ruhsatı iptal edilir. Bu fıkraya göre idari yaptırımların uygulanması ceza soruşturması ve kovuşturması yapılmasına engel değildir.

Bu maddenin uygulanması ile görevi gereği bu verileri kullanan kamu personelinin denetimine ilişkin esas ve usuller İçişleri Bakanlığı tarafından belirlenir.

Geçici Madde 1 - Bu Kanunun yayım tarihi ile 12 nci madde gereğince hazırlanacak yönetmeliğin yürürlüğe giriş tarihi arasında geçecek süre içinde 1704 ve 2099 sayılı Kanunların uygulanmasına devam olunur.

Geçici Madde 2 - Bu Kanunun yayımı tarihinden sonra 12 nci maddedeki yönetmelik çıkıncaya kadar 5 inci madde ve 6 ncı maddenin (a), (c), (d) bentlerini gerekli görülen yerlerde uygulamaya İçişleri Bakanı yetkilidir. **Geçici Madde 3** - Bu Kanunun 12 nci maddesinde belirtilen yönetmelik, bu Kanunun yürürlüğe girdiği tarihten itibaren altı ay içinde çıkarılır.

Geçici Madde 4 - (Ek: 27/3/2015-6638/20 md.)

Bu maddenin yürürlüğe girdiği tarihten itibaren altı ay içinde araç kiralama şirketleri tüm kayıtlarını bilgisayarda tutmak ve bilgisayar terminallerini genel kolluk kuvvetlerinin ek 1 inci maddeye göre kurulan bilgisayar terminallerine bağlamak zorundadırlar. Bu şartı yerine getirmeyen işletmelere mülki idare amirlerince on bin Türk Lirası idari para cezası verilir. Bu fiilin tekrarı hâlinde işletme ruhsatları iptal edilir.

Madde 20 - Bu Kanunun 6 ve 7 nci maddeleri, 6 ncı maddenin (b) bendi hariç, 12 nci maddeye dayanılarak çıkarılacak yönetmeliğin yürürlük tarihinde, diğer maddeleri bu Kanunun yayımı tarihinde yürürlüğe girer.

Madde 21 - Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

1512 sayılı Noterlik Kanunu

Resmî Gazete Tarihi : 05.02.1972

Resmî Gazete Sayısı : 14090

NOTERLİK KANUNU

BİRİNCİ KISIM

Genel Hükümler

Noterlik Mesleği:

Madde 1 - Noterlik bir kamu hizmetidir. Noterler, hukuki güvenliği sağlamak ve anlaşmazlıkları önlemek için işlemleri belgelendirir ve kanunlarla verilen başka görevleri yaparlar.

(...)

Elektronik işlemler:

Madde 198/A- (Ek: 2/12/2014-6572/6 md.)

Bu Kanunda öngörülen işlemler, elektronik ortamda güvenli elektronik imza kullanılarak da yapılabilir. Ancak, düzenleme şeklinde yapılması zorunlu tutulan işlemler ile irade beyanlarının alınmasına ilişkin işlemlerde güvenli elektronik imza kullanılabilmesi için ilgililerin noter huzurunda olmaları gerekir.

Elektronik ortamda güvenli elektronik imza kullanılarak noter huzurunda veya huzurda olmadan yapılabilecek noterlik işlemleri ile 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununda tanımlanan zaman damgası kullanılmasının zorunlu olduğu noterlik işlemleri yönetmelikle düzenlenir. Belirlenen bu noterlik işlemlerine ilişkin tüm bilgi ve belgeler güvenli elektronik imzayla elektronik ortamda işlenebilir, saklanabilir ve gerektiğinde ilgili diğer kişi veya kurumlara elektronik ortamda gönderilebilir. Ayrıca 61 inci maddede düzenlenen tespit işleri güvenli elektronik imza ile elektronik ortamda da yapılabileceği gibi aynı usulle elektronik ortamdaki durum, görüntü, işlem veya benzeri her türlü verinin tespiti de yapılabilir.

Noterler tarafından yapılan tüm işlemlere dair bilgi ve belgeler Türkiye Noterler Birliğinin Bilişim Sisteminde kaydedilir ve saklanır. Güvenli elektronik imza ile imzalanmış belgelerde kanunlarda belirtilen mühürleme işlemi uygulanmaz ve ayrıca suret aranmaz. Güvenli elektronik imza ile

oluřturulan belge, talep edilmedikçe ayrıca fiziki olarak dzenlenmez. Elektronik ortamdan fiziki örnek ıkartılması gereken hâllerde belgenin aslının aynı olduđu belirtilerek noterlike imzalanır ve mhrlenir. Gvenli elektronik imza ile imzalanmıř belgenin elle atılan imzalı suretiyle eliřmesi hâlinde noterlerin kullandığı biliřim sisteminde kayıtlı olan gvenli elektronik imzalı belge esas alınır.

Noterlik iřlemlerinin elektronik ortamda yapılması sırasında iřlenen kiřisel verilerin korunması ve bilgi gvenliđinin sađlanması iin gerekli tedbirler alınır.

Elektronik ortamda yapılacak noterlik iřlemlerine iliřkin cretler, 112 nci maddeye gre dzenlenecek tarifede gsterilir.

İkinci fıkraya uyarınca elektronik ortamda yapılabilecek bir noterlik iřleminin bir belgeye dayanması hâlinde; belge sureti, taraflar, vekilleri veya temsilcileri tarafından gvenli elektronik imza ile imzalanarak elektronik ortamda notere gnderilebilir. Ancak belge aslının fiziki olarak ibrazının zorunlu olduđu hâllerde elektronik ortamda yapılan bařvuru sonrasında belge aslı ynetmelikte belirlenen sre iinde notere ibraz edilir. Birlik, noter odaları ve noterlik personeli ile noterlere dađıtılacak nitelikli elektronik sertifikalar, Trkiye Noterler Birliđi tarafından temin edilerek dađıtılır.

Noterlik iřlemlerinin elektronik ortamda yapılmasına, saklanmasına ve paylařılmasına iliřkin usul ve esaslar ynetmelikte dzenlenir.

Yabancı memleketlerde, noterlik iřlemlerinin elektronik ortamda yapılması iin sađlanması gerekli olan teknik ve idari řartlara dair usul ve esaslar ynetmelikte dzenlenir.

Bu madde kapsamında hazırlanacak ynetmelik, Dıřiřleri Bakanlıđı, Trkiye Noterler Birliđi ve Bilgi Teknolojileri ve İletiliřim Kurumunun grřleri alınarak Adalet Bakanlıđı tarafından ıkarılır.

1136 sayılı Avukatlık Kanunu

Resmî Gazete Tarihi : 07.04.1969

Resmî Gazete Sayısı : 13168

AVUKATLIK KANUNU

BİRİNCİ KISIM

Avukatlık ve Avukat

Avukatlığın mahiyeti:

Madde 1 - Avukatlık, kamu hizmeti ve serbest bir meslektir.

(Değişik ikinci fıkra: 2/5/2001 - 4667/1 md.) Avukat, yargının kurucu unsurlarından olan bağımsız savunmayı serbestçe temsil eder.

(...)

Avukatın dosya saklaması ve hapis hakkı:

Madde 39 - Avukat, kendisine tevdi olunan evrakı, vekaletin sona ermesinden itibaren üç yıl süre ile saklamakla yükümlüdür. Şu kadar ki, evrakın geri alınması müvekkile yazı ile bildirilmiş olduğu hallerde saklama yükümlülüğü, bildirme tarihinden itibaren üç ayın sonunda sona erer.

Avukat, ücreti ve yapmış olduğu giderleri kendisine ödenmedikçe, elinde bulunan evrakı geri vermekle yükümlü değildir.

1211 sayılı Türkiye Cumhuriyet Merkez Bankası Kanunu

Resmî Gazete Tarihi : 26.01.1970

Resmî Gazete Sayısı : 13409

TÜRKİYE CUMHURİYET MERKEZ BANKASI KANUNU

Bilgi isteme yetkisi, bankaların bilançoları ve raporları:

Madde 43 – (Değişik: 25/4/2001 - 4651/9 md.)

Türkiye’de faaliyette bulunan bütün bankalar, özel finans kurumları ve Bankaca uygun görülecek diğer mali kurumlar, yıllık bilançoları ile kâr ve zarar hesaplarını, idare meclisi ve denetçi raporları ile birlikte, genel kurullarının toplantı tarihinden; bağımsız denetim kuruluşlarınca hazırlanacak denetim raporlarını ise düzenlenme tarihinden itibaren en geç bir ay içinde Bankaya vermekle yükümlüdürler.

Banka, bu Kanun ve mevzuat ile kendisine verilen görevleri yerine getirebilmek amacıyla birinci fıkrada belirtilen kurum ve kuruluşlardan her türlü bilgi ve belgeyi, belirleyeceği usul ve esaslar çerçevesinde istemeye yetkilidir. Birinci fıkrada belirtilen kurum ve kuruluşlar, kendilerinden istenen bilgileri Bankanın belirteceği süre içinde vermeye mecburdurlar. Banka, gerektiğinde kendisine verilmesi gereken bilgileri doğru ve zamanında vermeyen birinci fıkrada belirtilen kurum ve kuruluşların bu Kanunun verdiği yetkilere konu olan işlemlerini sınırlayabilir veya durdurabilir.

Banka, kendi yetki ve görev alanına giren hususlarla ilgili olarak birinci fıkrada belirtilen kurum ve kuruluşları düzenleme ve denetleme ile görevli kurum ve kuruluşlardan bilgi isteyebilir. Banka, gerektiğinde birinci fıkrada belirtilen kurum ve kuruluşlar hakkındaki görüşlerini ve tespitlerini Cumhurbaşkanlığı ile Bankacılık Düzenleme ve Denetleme Kurumuna ve bu kurum ve kuruluşları düzenleme ve denetleme yetkisine sahip olan diğer kurum ve kuruluşlara bildirebilir. (1)

Banka, istatistiki bilgilerin toplanmasında, kamu kurum ve kuruluşları, Hazine Müsteşarlığı, Devlet İstatistik Enstitüsü, diğer ülkelerin istatistiki bilgi toplamaya yetkili makamları ve uluslararası kuruluşlarla işbirliği yapabilir. Banka, finansal sistemle ilgili tüm istatistiki bilgiler ile ekonomideki ve ödemeler dengesindeki gelişmelerin izlenmesinde gerekli görülecek diğer istatistiki bilgileri bankalar, diğer mali kurumlar ile kişilerden doğrudan isteme ve toplama yetkisine sahiptir.

Kendilerinden bilgi istenilenler, bu bilgileri Bankanın belirleyeceği usul ve esaslara göre doğru olarak vermekle yükümlüdürler. Banka bu bilgilerin doğru olup olmadığını ilgililer nezdinde araştırmaya ve denetlemeye, ek bilgi ve belge istemeye yetkilidir.

Banka, gerekli gördüğü istatistiki bilgileri yayımlayabilir. Ancak banka toplanan istatistiki bilgilerden kişisel ve özel nitelikte olanları yayımlayamaz, açıklayamaz. Bankacılık Düzenleme ve Denetleme Kurumu dışında resmi veya özel herhangi bir makama veremez. Bu bilgiler istatistiki amaçlar dışında ve ispat aracı olarak kullanılamaz.

Gerçek ve tüzel kişilerden bilgi isteme yetkisi:

Madde 44- (Mülga:13/2/2011-6111/160 md.; Yeniden düzenleme: 28/11/2017-7061/33 md.)

Banka, gerçek ve tüzel kişilerin döviz pozisyonunu etkileyen işlemlerini izlemek amacıyla belirleyeceği gerçek ve tüzel kişilerden her türlü bilgi ve belgeyi istemeye yetkilidir. İstenilecek bilgi ve belgelerin kapsamı, toplanma ve izlenme yöntemi, doğruluğunun denetimi, paylaşımı, destek hizmeti temini de dâhil olmak üzere usul ve esaslar Bankaca belirlenir.

Bu maddenin uygulanmasında destek hizmeti kuruluşu çalışanları hakkında da bu Kanunun 35 inci maddesi ve 68 inci maddesinin (II) numaralı fıkrasının (a) bendi hükümleri tatbik olunur.

211 sayılı Türk Silahlı Kuvvetleri İç Hizmet Kanunu

Resmî Gazete Tarihi : 09.01.1961

Resmî Gazete Sayısı : 10702

TÜRK SİLAHLI KUVVETLERİ İÇ HİZMET KANUNU

Kimlik kartları, özlük dosyaları, kişisel veriler ve posta gönderileri

Madde 34/A - (Ek: 11/2/2014-6519/8 md.)

Askerî kimlik kartı; kişinin, Türk Silahlı Kuvvetleri personeli olduğunu ve kimliğini gösteren resmî belgedir. Türk Silahlı Kuvvetleri mensupları, yönetmelikle belirlenen istisnalar saklı kalmak kaydıyla askerî kimlik kartlarını resmî ve sivil olarak üzerlerinde bulundururlar.

Türk Silahlı Kuvvetleri personelinin temin, yetiştirme, istihdam, emeklilik, ayırma, atama, yer değiştirme, görevlendirme, seferberlik ve özlük hakları gibi işlemleri ve askerî hizmetlerin yürütülmesine ilişkin kişisel verileri personel bilgi sistemlerinde ve özlük dosyalarında muhafaza edilir.

Uzman erbaşlar hariç erbaş ve erler ile askerî öğrenciler tarafından gönderilen ve kendilerine gelen posta gönderileri ilgilinin amirince denetlenebilir.

TÜZÜKLER

Bölüm İçeriği

- Tıbbi Deontoloji Nizamnamesi
- Özel Hastaneler Tüzüğü

Tıbbi Deontoloji Nizamnamesi

Resmî Gazete Tarihi : 19.02.1960

Resmî Gazete Sayısı : 10436

TIBBİ DEONTOLOJİ NİZAMNAMESİ

Madde 1 - Tabip ve diř tabiplerinin, deontoloji bakımından riayetle mükellef oldukları kaide ve esaslar bu Nizamnamede gösterilmiştir.

6023 sayılı Türk Tabipleri Birlięi Kanununun 7 nci maddesi mucibince tabip odalarına kayıtlı bulunan tabip ve diřtabipleri, bu Nizamname hükümlerine tabidirler.

(...)

Madde 4 - Tabip ve diř tabibi, meslek ve sanatının icrası vesilesiyle muttali olduęu sırları, kanuni mecburiyet olmadıkça, ifşa edemez.

Tıbbi toplantılarda takdim edilen veya yayınlarda bahis konusu olan vakalarda, hastanın hüviyeti açıklanamaz.

Özel Hastaneler Tüzüğü

Resmî Gazete Tarihi : 10.01.1983

Resmî Gazete Sayısı : 17924

ÖZEL HASTANELER TÜZÜĞÜ

BİRİNCİ BÖLÜM

Kapsam, Kabul Edilecek Hastalar, Özel Hastane

Binalarının Nitelikleri

Kapsam:

Madde 1 - Özel hastanelere kabul edilecek hastalar, hastanelerin türleri,binalarının nitelikleri, personel kadroları, bulundurulması zorunlu ilaç, araç ve gereçler ve özel hastanelerin iç hizmetlerine ilişkin esaslar bu tüzükte gösterilmiştir.

(...)

Hasta dosyaları ve iç hizmet yönergesi:

Madde 29 - Özel hastanelerde yatan hastaların kimliğini, doğum yerini, ad- resini, yattığı ve çıktığı tarihi, hastalığının tanısını ve çıkıştaki durumunu yazmak için bir protokol defteri ile derece kağıdı, tabelası, filmleri, labora-tuvar raporları vb. hastanın izlenmesi ile ilgili belgeleri içeren bir dosya tutulur.

Protokol defterinin ilgili yerleri ile dosyadaki belgeler, giriş ve çıkışta geciktirilmeden doldurulur.

Gerçek kişilere ait hastanelerde sorumlu müdürler, yönetim kurulu bulunanların bu kurulla birlikte sorumlu müdürleritarafından hususi hastaneler kanunu ve bu tüzük esaslarına göre bir iç hizmet yönergesi düzenlenir.

Bu yönergede hastaların kabul koşul ve yöntemleri, sınıfına göre hastalardan alınacak ücret ve ne zaman alınacağı, hasta emanet ve eşyasının saklanması, hasta ziyaret saatleri, sınıflarına göre hasta odalarının nitelikleri hastanın özel durumunun gerekleri dışında verilecek yemeklerin nitelik ve niceliği, yemek zamanları, ölüm halinde yapılacak dezenfeksiyon, tabiplerin nöbet görevleri, hemşirelerin, hastabakıcıların ve diğer hizmetlilerin görevleri, polikliniği olan hastanelerin bu hizmetlerinin yapılış biçimi ile iç hizmetlere ilişkin diğer hususların gösterilmesi zorunludur.

Sanatoryumlarla kürevleri için düzenlenecek yönergelerde, yukarıda sayılan hususlardan başka dinlenme zamanları ve kuruluşun özelliğine göre yapılacak tedavi yöntemi ile disiplinine ilişkin hususlar da yazılır.

YÖNETMELİKLER

Bölüm İçeriği

- Türkiye Cumhuriyeti Kimlik Kartı Yönetmeliği
- Türkiye Cumhuriyeti Kimlik Kartı Elektronik Kimlik Doğrulama Sistemi Yönetmeliği
- Kimlik Paylaşımı Sistemi Yönetmeliği
- Veri Paylaşımı Kurulu Yönetmeliği
- Kimlik Bildirme Kanununun Uygulanması ile İlgili Yönetmelik
- E-Devlet Hizmetlerinin Yürütülmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik
- Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik
- Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik
- Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında Yönetmelik
- Hasta Hakları Yönetmeliği
- Özel Hastaneler Yönetmeliği
- Kan ve Kan Ürünleri Yönetmeliği
- Bulaşıcı Hastalıklar Sürveyans ve Kontrol Esasları Yönetmeliği
- Uluslararası Sağlık Turizmi ve Turistin Sağlığı Hakkında Yönetmelik
- Tıbbi Cihaz Yönetmeliği
- Tıbbi Cihaz Klinik Araştırmaları Yönetmeliği
- Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmelik
- 6713 Sayılı Kolluk Gözetim Komisyonu Kurulması Hakkında Kanunun Uygulanmasına Dair Yönetmelik
- Hukuk Muhakemelerinde Ses ve Görüntü Nakledilmesi Yoluyla Duruşma İcrası Hakkında Yönetmelik
- Yolcu Gemilerinin Emniyetine ve Gemilerdeki Yolcuların Kayıt Altına Alınmasına İlişkin Yönetmelik
- Eczacılar ve Eczaneler Hakkında Yönetmelik
- Genel Sağlık Sigortası Kapsamında Gelir Tespiti, Tescil ve İzleme Sürecine İlişkin Usul ve Esaslar Hakkında Yönetmelik
- Bireysel Emeklilik Sistemi Hakkında Yönetmelik

- 112 Acil Çağrı Merkezleri Kuruluş, Görev ve Çalışma Yönetmeliği
- Afet ve Acil Durum Müdahale Hizmetleri Yönetmeliği
- Bilgi Teknolojileri ve İletişim Kurumu İdari Yapıtlar Yönetmeliği
- Bilgi Teknolojileri ve İletişim Kurumu Posta Sektöründe İdari Yapıtlar Yönetmeliği
- Bilgi Teknolojileri ve İletişim Kurumu Teşkilât Yönetmeliği
- Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik
- Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği
- İnternet Alan Adları Yönetmeliği
- Sosyal Yardım Verilerinin Kaydedilmesine ve Paylaşılmasına İlişkin Yönetmelik
- Mesafeli Sözleşmeler Yönetmeliği
- Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik
- Elektronik Ticarete Hizmet Sağlayıcı ve Aracı Hizmet Sağlayıcılar Hakkında Yönetmelik
- Özel İstihdam Büroları Yönetmeliği
- Ticaret Sicili Yönetmeliği
- Veri Depolama Kuruluşunun Faaliyet, Çalışma ve Denetim Esasları Hakkında Yönetmelik
- Yenilenmiş Ürünlerin Satışı Hakkında Yönetmelik
- Elektrikli Skuter Yönetmeliği
- Yabancı Plakalı Araçlara Verilen Trafik İdari Para Cezalarının Tahsiline İlişkin Yönetmelik
- Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanunun Uygulanmasına İlişkin Yönetmelik
- Nüfus Hizmetleri Uygulama Yönetmeliği
- Genel Ürün Güvenliği Yönetmeliği
- Tapu ve Kadastro Verilerinin İşlenmesi ve Elektronik Ortamda Yapılacak İşlemler Hakkında Yönetmelik
- Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik
- Vakıflar Yönetmeliği
- Türkiyede Oturan Yabancıların Nüfus Kayıtlarının Tutulması Hakkında Yönetmelik
- Güvenlik Soruşturması ve Arşiv Araştırması Yapılmasına Dair Yönetmelik
- Sigortacılık Verilerinin Toplanması, Saklanması ve Paylaşılmasına Dair Yönetmelik
- Sağlık Bilgi Sistemleri Hakkında Yönetmelik

Türkiye Cumhuriyeti Kimlik Kartı Yönetmeliđi

Resmî Gazete Tarihi : 03.12.2019

Resmî Gazete Sayısı : 30967

TÜRKİYE CUMHURİYETİ KİMLİK KARTI YÖNETMELİĐİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliđin amacı; Türkiye Cumhuriyeti kimlik kartı ile ilgili yapılacak iş ve işlemlere ilişkin usul ve esasların belirlenmesidir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, Türkiye Cumhuriyeti kimlik kartının tasarımı, temini veya üretimi, başvurusu, kişiselleştirmesi, dağıtımını, teslimi, iptali, imhası, kimlik doğrulama yöntemi, biyometrik verilerin alınması ve işlenmesine ilişkin usul ve esasları kapsamaktadır.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 25/4/2006 tarihli ve 5490 sayılı Nüfus Hizmetleri Kanununun 41 inci maddesi ile 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete'de yayımlanan 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinin 258 inci maddesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Yönetmeliđin uygulanmasında;

- a) Bakanlık: İçişleri Bakanlığını,
- b) Başvuru makamı: Yurt içinde nüfus müdürlüklerini, yurt dışında dış temsilcilikleri,
- c) Biyometrik fotoğraf: Uluslararası Sivil Havacılık Teşkilatının (ICAO) 9303 sayılı Makede Okunabilir Seyahat Belgeleri (MRTD) dokümanı ve eklerine uygun olarak, standartları Genel Müdürlük tarafından belirlenen yüz biyometrisinin tespit edilebildiđi fotoğrafı,

- c) Biyometrik veri: Elektronik sistemler aracılığı ile kimlik tespiti ve kimlik doğrulama işlemlerinin gerçekleştirilmesini sağlamak amacıyla alınan kişiye özgü verileri,
- d) Çağrı merkezi: Genel Müdürlük bünyesindeki etkileşim merkezini,
- e) Dağıtım birimi: Kimlik kartı dağıtımında yetkili posta yükümlüsünü,
- f) Dış temsilcilik: Başkonsolosluk, konsolosluk, muavin konsolosluk, konsolosluk ajanlığı ve büyükelçilik konsolosluk şubelerini,
- g) Elektronik imza: Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi,
- ğ) Elektronik sertifika: Kimlik kartında yer alan ve kimlik doğrulama amacıyla kullanılan sertifikaları,
- h) Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) : Elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerini,
- ı) Genel Müdürlük: Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünü,
- i) Gezici kayıt terminali: Kimlik kartı başvurularının alınabilmesine olanak sağlayan ve başvuru işlemleri için gerekli yazılım ve donanımı içeren taşınabilir cihazı,
- j) İmha tutanağı: İmha edilecek kimlik kartının kime ait olduğu, seri numarası, imha edilme nedeni gibi bilgileri içeren ve yılı itibarıyla tarih ve sayı sırasına göre tutulan kayıtları,
- k) İptal tutanağı: İptal edilecek kimlik kartının kime ait olduğu, seri numarası, iptal edilme nedeni gibi bilgileri içeren ve yılı itibarıyla tarih ve sayı sırasına göre tutulan kayıtları,
- l) Kanun: Nüfus Hizmetleri Kanununu,
- m) Kart erişim cihazı (KEC): Biyometrik veri ve PIN ile kimlik doğrulaması ve PIN değişikliği yapılabilen cihazı,
- n) Kimlik belgesi: Nüfus cüzdanı, kimlik kartı, uluslararası aile cüzdanı, sürücü belgesi, pasaport, geçici kimlik belgesi ve kurumların kendi mevzuatlarında kimlik yerine geçen belgeyi,
- o) Kimlik kartı: Türkiye Cumhuriyeti vatandaşlarının kimliğini ispata yarayan Türkiye Cumhuriyeti kimlik kartını,
- ö) KİOSK: PIN değiştirme, PIN blokesi kaldırma, kişisel mesaj değiştirme ve kart kontrolü gibi işlemlerin yapıldığı cihazı,

- p) Kişiselleştirilmemiş kimlik kartı: Kişinin kimliğine ilişkin bilgiler ile biyometrik veri ve elektronik sertifikaların bulunmadığı ham kartı,
- r) Kişiselleştirilmiş kimlik kartı: Kişinin kimliğine ilişkin bilgiler ile biyometrik veri ve elektronik sertifikaların yer aldığı kartı,
- s) Kart yayıncı kart erişim cihazı (KYKEC): PIN, PUK, kişisel mesaj değiştirme, kart kontrolü, kart iptali ve kişinin kimliğini doğrulama işlemi gibi işlemleri gerçekleştirmek için başvuru makamınca kullanılan cihazı,
- ş) Merkezi veri tabanı: Genel Müdürlük tarafından elektronik ortamda tutulan verileri,
- t) MERNİS: Merkezî Nüfus İdaresi Sistemini,
- u) MRZ: Optik karakter okuma yöntemlerini kullanarak makine okuması için biçimlendirilmiş, zorunlu ve isteğe bağlı verileri kapsayan, kimlik kartı üzerinde yer alan sabit boyutlu alanı,
- ü) Nüfus müdürlüğü: İl nüfus ve vatandaşlık müdürlükleri ile ilçe nüfus müdürlüklerini,
- v) PIN: Kimlik kartı sahibi ile kartın eşleştirilmesine olanak sağlayan sayısal veriyi,
- y) PIN zarfı: Kişiyeye özel PIN, PUK ve kişisel mesaj bilgilerinin bulunduğu kapalı zarfı,
- z) PUK: PIN bloke edildiğinde blokeyi kaldırmak için kullanılan sayısal veriyi,
- aa) Resmî vekil: Vekâletname ile başkası adına işlem yapmakla yetkilendirilen kimseyi,
- bb) Seyahat belgesi: Uluslararası seyahatlerde kullanılması amacıyla makina tarafından okunabilir verileri içeren resmi belgeyi,
- cc) Talep belgesi: Kimlik kartı düzenlenmesine dayanak teşkil eden ve başvuruya ilişkin bilgileri kapsayan standart belgeyi,
- çç) Vekâletname: Temsil yetkisini kapsayan noterden onaylı belgeyi,
- dd) Yonga: Kimlik bilgileri, biyometrik veriler ve elektronik sertifikalar gibi bilgilerin elektronik olarak tutulduğu, kimlik kartında yer alan elektronik devreyi ifade eder.

İKİNCİ BÖLÜM

Temel Esaslar

Görev ve yükümlülük

MADDE 5 - (1) Kimlik kartının özelliklerini, tasarımını, güvenlik öğelerini, temini ve kişiselleştirilmesinde kullanılacak yöntemler ile kimlik kartında yer alacak bilgileri belirlemeye ve değiştirmeye Bakanlık yetkilidir.

(2) Kimlik kartının kişiselleştirilmesinde kullanılacak tüm elektronik sertifika ve anahtarlar Bakanlık tarafından yetkilendirilmiş Elektronik Sertifika Hizmet Sağlayıcısı tarafından temin edilir.

(3) Elektronik Sertifika Hizmet Sağlayıcısı, elektronik sertifika ve anahtarların teknik güvenliğinden sorumludur.

(4) Kimlik kartı işlemlerinde kullanılacak form ve belgeler ile bunların şekli ve içeriğiyle; kartın üretimi, dağıtımı, teslim yöntemi Genel Müdürlük tarafından belirlenir.

Kimlik kartının özellikleri ve kullanım alanı

MADDE 6 - (1) Kimlik kartı seri numarası bir harf, iki rakam ve bir harf, beş rakamdan oluşur.

(2) Kimlik kartında; kişi bilgileri, fotoğraf, imza, yonga, MRZ ve barkod alanları, biyometrik veri, elektronik sertifikalar ile güvenlik öğeleri bulunur.

(3) Kimlik kartının üzerindeki alan adları Türkçe ve İngilizce olmak üzere iki dilde yazılır.

(4) Kimlik kartının son geçerlilik tarihi kartın üzerinde yer alır.

(5) Kimlik kartı; kimlik tespiti ve kimlik doğrulama amacıyla kullanılır.

(6) Kimlik kartı, elektronik imza sertifikası yüklenmesi halinde elektronik imza işlemlerinde kullanılabilir.

(7) Kimlik kartı seyahat belgesi olarak kullanılabilir. Bu amaçla kullanımında ilgili ülkelerle yapılacak uluslararası anlaşma hükümleri uygulanır.

Bedel

MADDE 7 - (1) Kimlik kartının satış bedeli, 21/2/1963 tarihli ve 210 sayılı Değerli Kâğıtlar Kanununa göre Hazine ve Maliye Bakanlığınca belirlenir. Kimlik kartı satış bedelinin belirlenmesinde başvuru tarihi esas alınır.

(2) Kanuni süresi içinde yapılan doğum bildirimini ve 24/5/1983 tarihli ve 2828 sayılı Sosyal Hizmetler Kanunu ile 3/7/2005 tarihli ve 5395 sayılı Çocuk Koruma Kanunu uyarınca ilgili kuruluş yetkililerince yapılan bildirimler nedeniyle düzenlenen kimlik kartlarından değerli kâğıt bedeli alınmaz.

(3) Hatalı üretim, üretimden kaynaklanan yazım ve yonga arızası tespit edilen kartlar ile kimlik kartı sahiplerinin nüfus kayıtlarındaki maddi hataların idare tarafından düzeltilmesi sonucunda düzenlenecek kartlar, bedel alınmadan yenilenir.

ÜÇÜNCÜ BÖLÜM

Başvuru, Kişiselleştirme ve Teslim İşlemleri

Başvuru şekli ve nedenleri

MADDE 8 - (1) Türkiye Cumhuriyeti vatandaşı olan herkes kimlik kartı almak zorundadır. Kimlik kartı; doğum, değiştirme, kayıp, yeniden kayıt ve vatandaşlığın kazanılması nedenleriyle düzenlenir.

(2) Kimlik kartı başvuruları yurt içinde Genel Müdürlük web portalı üzerinden ya da çağrı merkezinden alınacak randevu ile veya randevusuz olarak nüfus müdürlüklerine, yurt dışında ise dış temsilciliklere yapılır.

(3) Kimlik kartı başvurusu, kimlik belgesi ve son altı ay içerisinde çekilmiş bir adet biyometrik fotoğraf ile yapılır. Kimlik belgesini ibraz edemeyen veya ibraz ettiği kimlik belgesinde fotoğrafı bulunmayan kişiler hakkında 12 nci maddenin ikinci fıkrasına göre işlem yapılır.

(4) Türk vatandaşlığının kazanılması nedeniyle kimlik kartı düzenlenmesinde kişinin bir adet biyometrik fotoğrafı, kimliğini ispatlayan pasaport benzeri bir belge veya vatandaşlığı kazandığını gösterir resmi bir belge istenir.

(5) On beş yaşını tamamlamış olanların şahsen başvurmaları esastır. On beş yaşını tamamlamayanların başvuruları ise veli, vasi, kayyum, bunların bulunmaması halinde, çocuğun büyük ana, büyük baba, ergin kardeşleri, çocuğu yanında bulunduranlar ya da vekâletname ibraz eden resmî vekil tarafından yapılır.

(6) Kimlik kartı başvurularında alınacak biyometrik veri, biyometrik fotoğraf ve imzaya ilişkin usul ve esaslar Bakanlık tarafından belirlenir.

(7) İlk defa kimlik kartı başvurusunda bulunan kişinin varsa nüfus cüzdanı geçersiz hale getirilir.

(8) Kimlik kartında kan grubu bilgisinin yer almasının talep edilmesi halinde kan grubu alanı sağlık birimlerinden alınmış belgeye göre düzenlenir. Daha sonraki başvurularda ise belge istenmez.

(9) Kimlik kartı başvurusu sırasında, gerekli bilgilendirmelerin yapılabilmesi için bulunması halinde başvuru sahibinin beyan ettiği iletişim numarası ve e-posta adresi de kayıt altına alınır.

(10) Kişi adına birden fazla kimlik kartı düzenlenemez.

Biyometrik fotoğraf

MADDE 9 - (1) Kimlik kartı başvurusunda kullanılacak biyometrik fotoğraflarda yüz tamamen görünür şekilde ön cepheden çekilmiş, gözler açık konumda; alın, yüz ve çene açık olmalı ve renkli cam ya da güneş gözlüğü kullanılmaz. Başvurularda kullanılacak biyometrik fotoğrafa ilişkin diğer standartlar Genel Müdürlük tarafından belirlenir.

(2) Kimlik kartı başvurusunda kullanılacak biyometrik fotoğraf taranarak sisteme kaydedildikten sonra başvuru sahibine iade edilir. Fotokopi, bilgisayarda çoğaltılan veya biyometrik olmayan fotoğraflar kabul edilmez.

(3) Yüz biyometrisinin tespit edilmesine engel olacak herhangi bir sağlık sorunu bulunması halinde bu durum başvuru makamınca kayıt altına alınır.

Koruma altında bulunan çocuklar

MADDE 10 - (1) 2828 sayılı Kanun ile 5395 sayılı Kanun kapsamında koruma altında bulunan on beş yaşını tamamlamayan çocuklara ait kimlik kartı başvurusu; veli veya vasiye ulaşılamaması veya ulaşılmamasının sakıncalı olması halinde ilgili kuruluş yetkililerince yapılır.

Kısıtlıların başvuruları

MADDE 11 - (1) Bir yıl veya daha uzun süreli özgürlüğü bağlayıcı bir cezaya mahkûm olanların başvuruları veli veya vasinin nezaretinde alınır.

(2) Akıl hastalığı veya zayıflığı nedeniyle kısıtlananların başvuruları veli, vasi veya kayyum tarafından yapılır. Bu kişilerden imza alınmaz. Standartlara uygun biyometrik fotoğraf veya biyometrik verilerin alınamaması halinde bu durum başvuru makamınca kayıt altına alınarak başvuru işlemi tamamlanır.

(3) Savurganlık, alkol veya uyuşturucu madde bağımlılığı, kötü yaşam tarzı, kötü yönetim nedeniyle kısıtlananların başvuruları veli, vasi veya kayyum nezaretinde alınır.

(4) Yaşlılığı, engelliliği, deneyimsizliği veya ağır hastalığı sebebiyle işlerini gerektiği gibi yönetememesi nedeniyle kısıtlananların başvuruları veli, vasi veya kayyum nezaretinde alınır. Standartlara uygun biyometrik fotoğraf veya biyometrik verilerinin alınamaması halinde bu durum başvuru makamınca kayıt altına alınarak başvuru işlemi tamamlanır.

İnceleme

MADDE 12 - (1) Kimlik kartı başvurusunda bulunan kişinin kimlik ve adres bilgileri kontrol edilir. Yerleşim yeri adres bilgisinin olmaması veya bu bilgilerde değişiklik olması durumunda usulüne uygun olarak adres beyan işlemi tamamlandıktan sonra kimlik kartı başvurusu alınır.

(2) Kimlik belgesi ibraz edemeyen veya ibraz ettiği kimlik belgesinde fotoğrafı bulunmayan kişilerin başvurularında kimlik kartı düzenlenmesinde aşağıda belirtildiği şekilde işlem yapılır:

a) On beş yaşını tamamlayan kişinin MERNİS'te kayıtlı aynı kişi olup olmadığı hususunda tereddüde düşülmesi durumunda ana, baba, büyük ana, büyük baba, eş, varsa ergin kardeş veya ergin çocuklarının veya vasinin beyanı başvuru makamlarınca yeterli sayılır.

b) 2828 sayılı Kanun ile 5395 sayılı Kanun kapsamında koruma altındakiler ile cezaevi, bakımevi, huzurevi gibi kurumlar bünyesinde bulunan on beş yaşını tamamlamış kişilerin sistemde kayıtlı kişi olup olmadığı konusunda tereddüde düşülmesi halinde ilgili kurumlar tarafından düzenlenecek fotoğraflı resmî belge ile başvuruları alınır.

c) (a) ve (b) bentleri kapsamında alınan başvurularda sistem üzerinden beyanın doğruluğu kontrol edilir ve başvuru belgesinde "Başvuran Kişinin İmzası" alanında kayıt altına alınır.

ç) Nüfus müdürlüğüne yapılan inceleme sonucunda başvuran kişinin, kaydın sahibi olup olmadığı hususunda tereddüt oluşması halinde, Kimlik Tespit Formu düzenlenerek mülkî idare amirinin emri ile kolluk kuvvetlerince soruşturma yaptırılır. Soruşturmanın olumlu sonuçlanması durumunda kişinin başvurusu ile ilgili işlem tamamlanır.

d) Dış temsilciliklere yapılan başvurularda başvuran kişinin, kaydın sahibi olup olmadığı hususunda tereddüt oluşması halinde ise Kimlik Tespit Formu düzenlenerek başvuru sahibinin ana, baba, ergin kardeş, eş ve ergin çocuklarının; bunların bulunmaması halinde ise başvuru sahibinin belirlediği Türkiye'de tanıklığına başvurulacak kişi/kişilerin yerleşim yeri adreslerinin bulunduğu nüfus müdürlüklerine gönderilir. İlgili nüfus müdürlükleri tarafından mülkî idare amirinin emri ile kolluk kuvvetlerince soruşturma yaptırılarak sonucundan başvurunun yapıldığı dış temsilciliğe bilgi verilir. Soruşturmanın olumlu sonuçlanması hâlinde kişinin başvurusu alınır.

e) Soruşturma sonucunda kişinin iddia ettiği kaydın sahibi olduğunun tespit edilememesi hâlinde; varsa ana veya babasından, ana veya babasının ölmüş olması hâlinde ise varsa kardeşlerinden; anası, babası veya kardeşi olduğuna dair tıbbi rapor veya Türk mahkemelerinden alınmış tespit kararı ibraz edilmedikçe kimlik kartı başvurusu alınmaz.

Biyometrik verilerin alınması, karşılaştırılması ve kaydedilmesi

MADDE 13 - (1) Biyometrik verilerin alınmasına, işlenmesine ve karşılaştırılmasına ilişkin usul ve esaslar Bakanlık tarafından belirlenir. Kimlik kartı başvurusunda Bakanlıkça belirlenen usul ve esaslara göre işlem yapılır.

(2) Kimlik kartı başvurusunda bulunan kişinin daha önce alınmış olan biyometrik verisinin doğrulanması halinde tekrar biyometrik verisi alınmaz.

(3) Kişilerden biyometrik veri alınmasına engel teşkil eden bir durumun bulunması veya belgelendirilmesi halinde biyometrik veri alma işlemi yapılmaz ve bu husus kayıt altına alınır.

(4) Kompozit doku veya el nakli yapıldığı tespit edilen kişilerin ya da bağışçının daha önceden biyometrik veri kaydının olması hâlinde doku nakli operasyonundan sonra nakil yapılan kişilerin biyometrik verileri alınarak merkezi veri tabanındaki kayıtları güncellenir ve açıklama yapılır.

Geçici kimlik belgesi

MADDE 14 - (1) Kimlik kartı başvurusunda bulunan kişiye, kimlik kartı teslim edilinceye kadar geçerli olan ve kimliğini ispata yarayan geçici kimlik belgesi düzenlenir. Geçici kimlik belgesinin şeklini ve geçerlilik süresini belirlemeye Genel Müdürlük yetkilidir.

(2) Geçici kimlik belgesi ile işlem yapacaklar tarafından belgenin geçerliliği ve doğruluğu Kimlik Paylaşımı Sistemi, e-Devlet veya Bakanlığın belirleyeceği sistem üzerinden kontrol edilebilir.

Afet durumunda kimlik kartı alınması

MADDE 15 - (1) Afet nedeniyle genel hayata etkili olacak derecede zarar gören yerlerde kimlik kartı kullanılamaz hale gelen veya kaybolan vatandaşların başvuruları, mülki idare amirinin vereceği karar üzerine Genel Müdürlüğün koordinesi ile alınır.

(2) Afet nedeniyle kimlik kartı talebinde bulunan kişinin merkezi veri tabanında fotoğrafı ile biyometrik verisinin bulunması hâlinde güncel fotoğraf şartı aranmaksızın başvurusu alınır.

(3) Afet nedeniyle herhangi bir yerleşim yerinde bulunan kişinin kimlik kartı talebinde, kendisini tanıyan veya misafir edenlerin tanıklığı ile başvuru alınır. Talep belgesine, iki tanığın imzası alınır.

Gezici kayıt terminali

MADDE 16 - (1) Kimlik kartı başvurusu için nüfus müdürlüğüne gelemeyeceğini belgelendiren kişilerin başvurularında, iş hacmi ve personel durumu göz önüne alınarak mülki idare amirinin onayı ile Gezici Kayıt Terminali kullanılabilir.

Kişiselleştirme

MADDE 17 - (1) Kimlik kartının kişiselleştirilmesinde kullanılacak sistemi belirlemeye Bakanlık yetkilidir.

(2) Başvuru sahibinin kimlik bilgileri, biyometrik verisi, fotoğrafı, ıslak imzası, kart seri numarası ve elektronik sertifikaları ile talep edilmesi halinde din bilgisi ve kan grubu, belirlenen veri yapısına uygun olarak yazılmak suretiyle kart kişiselleştirilir.

(3) Kişiselleştirme aşamasından sonra kimlik kartı değerli kâğıt olarak kabul edilir.

(4) Kişiselleştirilmemiş ve kişiselleştirilmiş kimlik kartlarının kontrollerinin yapılmasına ilişkin usul ve esaslar Genel Müdürlük tarafından belirlenir.

(5) Kalite kontrolü veya kişiselleştirme sırasında hatalı olduğu tespit edilen kimlik kartları belirlenen usul ve esaslar çerçevesinde imha edilir.

Kimlik kartı teslim işlemleri

MADDE 18 - (1) On beş yaşını tamamlayan kişilerin kimlik kartları kendilerine veya başvuru sırasında belirlediği kişiye teslim edilir. Bu durumda talepte bulunan ile kimlik kartını teslim alacak kişi arasında soy bağı bulunması şartı aranmaz.

(2) İlgilisine veya başvurusu sırasında belirlediği kişiye teslim edilemeyen kartlar ilgilinin başvurusu sırasında belirttiği nüfus müdürlüğüne teslim edilir.

(3) Kısıtlı olanların kimlik kartları veli, vasi veya kayyum ya da bunların belirlediği kişiye teslim edilir.

(4) On beş yaşını tamamlamamış çocukların kimlik kartları; ana, baba ya da vasileri, bunların bulunmaması hâlinde büyük ana, büyük baba veya ergin kardeşleri ya da çocukları yanlarında bulunduranlar veya vekâletname ibraz eden resmî vekili ile veli ya da vasi tarafından belirlenen kişiye teslim edilir.

(5) 2828 sayılı Kanun ile 5395 sayılı Kanun kapsamında adına başvuru yapılan kişinin kimlik kartı, kuruluş yetkilisine teslim edilir.

(6) Dış temsilciliklerce alınan başvurularda Genel Müdürlük tarafından kişiselleştirilen kimlik kartları dış temsilcilikler yoluyla başvuru sahibine teslim edilmek üzere Dışişleri Bakanlığına gönderilir.

(7) Kimlik kartı teslim edildikten sonra kart aktif hale getirilir.

Kimlik kartı sahibinin yükümlülükleri

MADDE 19 - (1) Kimlik kartı sahibi;

- a) Başvuru sırasında kendisine teslim edilen PIN zarfını ve içerisindeki bilgileri muhafaza etmekle ve bu bilgileri paylaşmamakla,
 - b) Teslim aldığı kartı kontrol edip, kart ile yongasında maddi hata bulunduğunu tespit etmesi halinde iade etmekle,
 - c) Kartın yenilenmesini gerektiren bir durum olması halinde yurt içinde nüfus müdürlüklerine, yurt dışında ise en yakın dış temsilciliğe başvurarak yeniletmekle,
 - ç) Kartı kaybetmesi halinde durumu yurt içinde çağrı merkezine veya nüfus müdürlüklerine, yurt dışında ise en yakın dış temsilciliğe bildirmekle,
- yükümlüdür.

Kimlik kartı şifre işlemleri

MADDE 20 - (1) Başvuru makamlarında bulunan KYKEC veya KİOSK cihazlarından PIN ve kişisel mesaj bilgisi değiştirilebilir.

(2) Başvuru makamları dışında kullanılacak KEC'ler ile de PIN değiştirilebilir, değiştirilecek PIN'lere ilişkin işlem bilgileri Genel Müdürlüğün belirleyeceği sisteme aktarılır.

(3) PIN zarfı, PIN, PUK ve kişisel mesaj bilgisi verilmesi ile diğer şifre işlemlerine ilişkin yöntemi belirlemeye Genel Müdürlük yetkilidir.

(4) Açılmış veya tahrifata uğramış PIN zarfları işleme alınmaz ve başvuru makamlarınca yerinde kayıt altına alınarak imha edilir.

PIN ve biyometrik bloke kaldırma işlemi

MADDE 21 - (1) Bloke kaldırma işlemleri kişi doğrulandıktan sonra KYKEC aracılığı ile; PUK bilinmesi halinde ise PIN blokesi kaldırma işlemi KEC aracılığı ile yapılır.

(2) Kimlik kartı sahipleri tarafından KİOSK'larda PIN değiştirme, PIN bloke kaldırma, kişisel mesaj değiştirme ve kart kontrolü işlemleri gerçekleştirilebilir.

(3) Kimlik kartı sahipleri tarafından PUK bilinmemesi veya biyometrik veri ile PIN blokesi kaldırılamaması durumunda yeni bir PIN zarfı kişiye verilir ve sonrasında yeni PUK ve PIN bilgisi KYKEC aracılığı ile yongaya yazılır.

(4) Biyometrik hata sayacı eşik değeri Genel Müdürlük tarafından belirlenir. Karttaki biyometrik hata sayacı sıfırlanıp biyometri blokesi başvuru makamlarınca kaldırılır.

(5) Bloke kaldırma işlemleri başvuru makamınca MERNİS'e kaydedilir.

Yeniden kimlik kartı başvurusu

MADDE 22 - (1) Yeniden kimlik kartı başvurusunda merkezi veri tabanındaki fotoğrafın son altı ay içerisinde yapılmış bir başvuruya ait olmaması halinde, ilgiliden son altı ay içinde çekilmiş bir adet biyometrik fotoğraf istenir ve kimlik belgesi aranmaksızın biyometrik doğrulaması yapılarak kimlik kartı başvurusu alınır.

(2) Yeniden kimlik kartı taleplerinde kimlik belgesi ibraz edilememesi ve biyometrik doğrulama da yapılamaması halinde öncelikle merkezi veri tabanında bulunan fotoğraf, imza ve kişi bilgileri üzerinden doğrulama yapılır. Doğrulama yapılamaması ve kişinin kimliğinde tereddüde düşülmesi halinde kimliğin tespiti için 12 nci maddede belirtilen usul ve esaslara göre işlem yapılır.

Gerçeğe aykırı beyan ve tahrifat

MADDE 23 - (1) Kimlik kartları ve geçici kimlik belgesi üzerinde veya içinde silinti, kazıntı, düzeltme yapılamaz.

(2) Kimlik Paylaşımı Sisteminden faydalanan kurumlar, kimlik kartının örneğini almaksızın, geçerliliğini Kimlik Paylaşımı Sistemi üzerinden teyit eder.

(3) Kimlik kartı başvurusunda gerçek dışı beyanda bulunulduğunun veya kimlik kartında tahrifat yapıldığının başvuru makamınca tespit edilmesi hâlinde durum Cumhuriyet Savcılığına bildirilir.

Kimlik kartının iptali

MADDE 24 - (1) Kimlik kartı;

- a) Yonganın okunamaması,
 - b) Yonga içinde yer alan verilerden herhangi birinde eksiklik olması,
 - c) Yongadan kaynaklanan bir nedenle kimlik kartının kullanılamaması,
 - ç) Kartın kullanılamayacak derecede tahribata uğraması,
 - d) Kartın geçerlilik süresinin sona ermesi,
 - e) Kartın süresi içerisinde teslim alınmaması,
 - f) Kartın değiştirilmesi,
 - g) Kartın kaybolduğunun ya da çalındığının bildirilmesi,
 - ğ) Genel Müdürlük tarafından belirlenecek benzer hallerde,
- başvuru makamınca iptal edilir.

- (2) İptal edilen kimlik kartları Genel Müdürlük tarafından belirlenen usul ve esaslara göre imha edilir.
- (3) Fiziki olarak imha edilecek kimlik kartlarının seri numaraları, iptal nedenleri ve kart durum bilgileri, imha tutanağına ve merkezi veri tabanına kaydedilir.
- (4) Genel Müdürlük tarafından belirlenen başvuru makamlarınca imha edilecek olan kimlik kartlarına ilişkin bilgiler imha tutanağına aktarılır ve merkezi veri tabanına kaydedilir. İmha tutanağı dosyasında muhafaza edilir.

Kimlik kartının imhası

MADDE 25 - (1) Kimlik kartının değiştirilmesinde mevcut kimlik kartı geri alınır. Kurumlarda unutulmuş veya kişiler tarafından bulunan nüfus cüzdanları ve kimlik kartları o yerin nüfus müdürlüğüne gönderilir. İlgilinin adresinin tespit edilmesi ve kişinin yeni bir kimlik kartı almamış olması halinde bulunmuş olan nüfus cüzdanı veya kimlik kartı nüfus müdürlüğüne ait olduğu kişiye teslim edilir, aksi takdirde ilgili mevzuatına göre iptal ve imha edilir.

(2) Dağıtım birimince ilgisine teslim edilemeyen kimlik kartları, başvuru sırasında bildirilen nüfus müdürlüğüne teslim edilir. Bu kartlar teslim alan nüfus müdürlüğüne kayıt altına alınır. Genel Müdürlük tarafından belirlenen süre içerisinde başvuru makamından teslim alınmayan kimlik kartlarının elektronik sertifikası geçersiz hale getirilir. Geçersiz hale getirilen kimlik kartları Genel Müdürlük tarafından belirlenen başvuru makamlarınca imha edilir.

(3) Dışişleri Bakanlığı tarafından kişiye teslim edilmek üzere dış temsilciliklere gönderilen kimlik kartlarının belirlenen süre içerisinde teslim alınmaması halinde Genel Müdürlük tarafından elektronik sertifikası geçersiz hale getirilir. Bu kartlar Dışişleri Bakanlığı veya belirleyeceği dış temsilciliklerce fiziki olarak imha edilir.

(4) Türk vatandaşlığının kaybı, çıkma, kaybettirme ya da vatandaşlığa alınmanın iptali ile ölüm, gaiplik veya ölüm karinesi gibi hallerde kimlik kartı geri alınarak kimlik kartının elektronik sertifikası geçersiz hale getirilir ve imha edilir.

(5) Kimlik kartlarının zarflanması, teslimatı, geçersiz hale getirilmesi ve imhası ile nüfus cüzdanlarının geçersiz hale getirilmesi ve imhasına ilişkin usul ve esaslar Genel Müdürlük tarafından belirlenir.

DÖRDÜNCÜ BÖLÜM

Çeşitli ve Son Hükümler

Hüküm bulunmayan haller

MADDE 26 - (1) Bu Yönetmelikte hüküm bulunmayan hallerde 25/4/2006 tarihli ve 5490 sayılı Nüfus Hizmetleri Kanunu, 29/5/2009 tarihli ve 5901 sayılı Türk Vatandaşlığı Kanunu, 29/9/2006 tarihli ve 2006/11081 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan Nüfus Hizmetleri Kanununun Uygulanmasına İlişkin Yönetmelik ile 11/2/2010 tarihli ve 2010/139 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan Türk Vatandaşlığı Kanununun Uygulanmasına İlişkin Yönetmelik hükümlerine göre işlem yapılır.

Yürürlük

MADDE 27 - (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 28 - (1) Bu Yönetmelik hükümlerini İçişleri Bakanı yürütür.

Türkiye Cumhuriyeti Kimlik Kartı Elektronik Kimlik Doğrulama Sistemi Yönetmeliđi

Resmî Gazete Tarihi : 22.10.2020

Resmî Gazete Sayısı : 31282

TÜRKİYE CUMHURİYETİ KİMLİK KARTI ELEKTRONİK KİMLİK DOĞRULAMA SİSTEMİ YÖNETMELİĐİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak, Tanımlar ve Kısaltmalar

Amaç

MADDE 1 - (1) Bu Yönetmeliđin amacı, Türkiye Cumhuriyeti kimlik kartı ile gerçekleştirilen elektronik kimlik doğrulama sistemi ile ilgili usul ve esasları belirlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, Türkiye Cumhuriyeti kimlik kartı ile gerçekleştirilen elektronik kimlik doğrulama sistemi uygulamasında yapılacak iş ve işlemlere ilişkin usul ve esasları kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 25/4/2006 tarihli ve 5490 sayılı Nüfus Hizmetleri Kanununun 41 inci maddesi ile 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete’de yayımlanan 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinin 258 inci maddesi hükümlerine dayanılarak hazırlanmıştır.

Tanımlar ve kısaltmalar

MADDE 4 - (1) Bu Yönetmeliđin uygulanmasında;

- a) Akıllı kart okuyucu: Kimlik doğrulama sürecinde kimlik kartının elektronik olarak kullanılmasını sağlayan terminali,
- b) Bakan: İçişleri Bakanını,
- c) Bakanlık: İçişleri Bakanlığını,
- ç) Beyaz Liste: Kimlik doğrulama işlemi yapması onaylanmış Kart Erişim Cihazı listesini,

- d) Biyometrik veri: Elektronik sistemler aracılığı ile kimlik doğrulama işlemlerinin gerçekleştirilmesini sağlamak amacıyla kullanılan kişiye özgü veriyi,
- e) EKDS Değerlendirme Komisyonu: EKDS'nin kullanılması için gerekli inceleme, değerlendirme ve izin işlemlerini gerçekleştirmek üzere Bakan onayı ile oluşturulan komisyonu,
- f) Elektronik Kimlik Doğrulama Sistemi (EKDS): Türkiye Cumhuriyeti kimlik kartının elektronik kimlik doğrulama işlemlerinde kullanılabilmesini sağlayan sistemi,
- g) EKDS standardı: Türk Standartları Enstitüsü (TSE) tarafından EKDS ile ilgili belirlenen standartları,
- ğ) ESHS: Elektronik sertifika hizmet sağlayıcısını,
- h) Genel Müdür: Nüfus ve Vatandaşlık İşleri Genel Müdürünü,
- ı) Genel Müdürlük: Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünü,
- i) Güvenli Erişim Modülü (GEM) Akıllı Kartı: Kart erişim cihazı üzerindeki kriptografik işlemlerin gerçekleştirilmesi için kullanılan güvenli modülü,
- j) Güvenli iletişim sertifikası: KEC ve rol sunucusu arasında güvenli hat kurmak için gerekli olan sertifikayı,
- k) Hizmet alan: KDHS'den EKDS hizmeti alan kurum, kuruluş ve kişileri,
- l) Hizmet veren: EKDS kullanarak hizmet sunan kamu veya özel hukuk tüzel kişileri ile EKDS hizmetinden faydalanarak hizmet veren bir kamu veya özel hukuk tüzel kişiliğinde elektronik kimlik doğrulama işleminin gerçekleştirilmesinde rol alan yetkili personeli,
- m) HSM: Donanımsal güvenlik modülünü,
- n) Kart Erişim Cihazı (KEC): Vatandaşın kimliğini doğrulama işlevi için kullanılan terminali,
- o) KEC standardı: Elektronik kimlik kartları için güvenli kart erişim cihazları ile ilgili TSE tarafından belirlenen standartları,
- ö) KEC üreticisi: KEC standardına göre KEC üretimi yapan kamu veya özel hukuk tüzel kişilerini,
- p) Kimlik doğrulama: Kimlik kartını ibraz eden kişinin kimlik doğrulama sertifikası, PIN, biyometrik veri, dijital fotoğraf veya kartın fiziksel güvenlik öğeleri kullanılarak doğrulanmasını ve geçerlenmesini,
- r) Kimlik doğrulama başarımlar onayı: Kimlik doğrulama sunucusu tarafından kimlik doğrulama bildirimini doğrulanması sonrasında oluşturulan ve hizmet alanın sistemlerine gönderilen imzalı veri nesnesini,

- s) Kimlik Doğrulama Bildirimi (KDB): KEC'in GEM Akıllı Kart aracılığı ile elektronik kimlik doğrulama için kimlik kartı ile etkileşim halinde yapmış olduğu kriptografik ve biyometrik işlemlerin sonucunu gösteren elektronik bildirimini,
- ş) Kimlik Doğrulama Hizmet Sağlayıcı (KDHS): EKDS standartlarına uygun olarak elektronik kimlik doğrulama ve kimlik doğrulamanın arşivlenmesine ilişkin hizmeti sağlayan kamu veya özel hukuk tüzel kişilerini,
- t) Kimlik Doğrulama Politikası (KDP): KEC tarafından kimlik doğrulama işleminde kullanılacak yöntem ve parametreleri içeren sayısal veriyi,
- u) Kimlik Doğrulama Politika Sunucusu (KDPS): EKDS'de Kimlik Doğrulama Politikası üretmek ve yayımlamak için kullanılan sunucuyu,
- ü) Kimlik doğrulama sertifikası: Kimlik doğrulaması amacıyla kullanılan sertifikayı,
- v) Kimlik Doğrulama Sunucusu (KDS): EKDS'de kimlik doğrulama bildirimlerini doğrulayan ve kimlik doğrulama başarımlarını dönen ve sonucu kaydeden sunucuyu,
- y) Kimlik kartı: Türkiye Cumhuriyeti kimlik kartını,
- z) Kimlik kartındaki veriler: 5490 sayılı Nüfus Hizmetleri Kanununun 41 inci maddesi hükümlerine göre Bakanlık tarafından belirlenen bilgileri,
- aa) MRZ: Makine tarafından okunabilen bölgeyi,
- bb) Ortak kriterler: Uluslararası Standartlar Organizasyonunun Uluslararası Bilgi Teknolojileri Güvenlik Değerlendirme Standardı olarak kabul ettiği ISO 15408 güvenlik standardını,
- cc) PIN: Kimlik sahibi ile kartın eşleştirilmesine olanak sağlayan sayısal veriyi,
- çç) PUK: PIN bloke edildiğinde, blokeyi kaldırmak için kullanılan sayısal veriyi,
- dd) Rol: Kimlik kartındaki alanlara erişmek isteyen taraflara tanımlanan erişim yetkisini,
- ee) Rol doğrulama: Kimlik kartındaki rol yetkisi gerektiren alanlara erişmek isteyen uygulamaların yetkisini kontrol etmekte kullanılan yöntemi,
- ff) Rol sertifikası: Rol doğrulamada kullanılan yetki sertifikasını,
- gg) Rol sunucusu: Rol doğrulamada kullanılan ve kimlik kartındaki alanlara erişen sunucuyu,
- ğğ) Taahhütname: KDHS'nin sorumluluk alanıyla ilgili EKDS kapsamında bulunan verilerin güvenliğinin ve idamesinin sağlanmasına ilişkin yeterli korumayı taahhüt ettiği idari ve teknik tedbirleri kapsayan belgeyi,

hh) Uygunluk belgesi: EKDS veya KEC standardına uygun ürün olduğuna dair TSE tarafından verilen belgeyi,

ıı) Yazılım yayıncı sertifikası: KEC yazılım paketlerini imzalamak için kullanılan sertifikayı, ifade eder.

İKİNCİ BÖLÜM

Temel Esaslar

Kimlik kartının kullanım alanları

MADDE 5 - (1) Kimlik kartında; kişi bilgileri, fotoğraf, imza, yonga, MRZ ve barkod alanları, biyometrik veri, elektronik sertifikalar ile güvenlik öğeleri bulunur.

(2) Kimlik kartı, kimlik doğrulama amacıyla kullanılır.

(3) Kimlik kartının elektronik imza aracı olarak kullanılmasında 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu hükümleri uygulanır.

(4) Kimlik kartının temassız yongasındaki bilgiler ikili antlaşma yapılan ülkelerde seyahat belgesi olarak kullanılabilir.

Yetki ve sorumluluk

MADDE 6 - (1) EKDS ile ilgili inceleme, değerlendirme ve izin işlemlerini gerçekleştirmek üzere Bakan onayı ile Genel Müdürün başkanlığında EKDS Değerlendirme Komisyonu oluşturulur. Genel Müdürlük inceleme, değerlendirme ve izin işlemleri için EKDS yönetim altyapısını kurar.

(2) Görevli ESHS, Bakan onayı ile belirlenerek Genel Müdürlüğün resmi internet sitesinden duyurulur.

(3) Görevlendirilen ESHS'nin sağlayacağı tüm anahtar ve sertifikaların başvuru, temin, dağıtım, teslim ve iptal işlemlerine ilişkin yöntemi belirlemeye Genel Müdürlük yetkilidir.

(4) Genel Müdürlük, hizmet alan, KDHS ve KEC üreticilerinden EKDS'ye ilişkin her türlü bilgi ve belgeyi istemeye yetkilidir.

(5) Görevlendirilen ESHS, görevlendirildiği alanla sınırlı olmak üzere yazılım yayıncı, KDS, KDPS, güvenli iletişim, rol sertifikalarının ve GEM akıllı kartının üretiminden, tesliminden ve bunların teslim edilene kadar güvenliğinin sağlanmasından sorumludur.

(6) Görevlendirilen ESHS tarafından EKDS ile ilgili sunulan hizmetlerden alınacak bedellerin üst sınırı Bakan onayı ile belirlenir.

(7) EKDS üzerinden yapılan kimlik doęrulama iř ve iřlemlerine iliřkin hukuki sonuęlar; KEC üreticisi, KDHS ve hizmet alanın sorumluluęundadır.

(8) Genel Müdürlük, EKDS hizmetine iliřkin yaptıęı ęalıřmalarla ilgili yıllık durum raporu hazırlar ve internet sayfasından yayınlar.

ÜÇÜNCÜ BÖLÜM

Başvuru ve Deęerlendirme Süreci

KDHS genel řartları

MADDE 7 - (1) KDHS olabilmek için kamu veya özel hukuk tüzel kiřilerinin ařaęıdaki asgari řartları tařımaları zorunludur:

- a) TS EN ISO/IEC 27001 Bilgi Güvenlięi Yönetim Sistemi sertifikası sahibi olmak.
- b) TSE tarafından EKDS ile ilgili yayımlanan standartlara uygunluęunu belgelemek.
- c) KDHS'nin sorumluluk alanıyla ilgili EKDS'nin güvenlięi ve idamesine dair alınacak idari ve teknik tedbirleri kapsayan taahhünameyi imzalamak.

KDHS başvuru süreci

MADDE 8 - (1) Kamu veya özel hukuk tüzel kiřileri, KDHS olma talebini ięeren başvurusunu Genel Müdürlüęün resmi internet sitesinde yayımlanan yöntem ile Genel Müdürlüęe yapar.

(2) Başvurular en geę 3 (üç) ay içinde EKDS Deęerlendirme Komisyonu tarafından sonuęlandırılarak Bakan onayına sunulur. Kararlar, Genel Müdürlük tarafından başvuru sahibine bildirilir.

(3) EKDS Deęerlendirme Komisyonu tarafından, başvuru řartlarında eksiklik bulunması halinde bu eksikliklerin giderilmesi için başvuruda bulunanlara 1 (bir) ayı geęmemek üzere süre verilir. EKDS Deęerlendirme Komisyonu eksikliklerin giderilmesinden itibaren en geę 2 (iki) ay içinde başvuruyu sonuęlandırır.

(4) Onay verilen KDHS'ler, Genel Müdürlüęün internet sitesi üzerinden kamuoyuna duyurulur.

(5) EKDS Deęerlendirme Komisyonu tarafından yapılan inceleme sonucunda başvuru řartlarının yerine getirilmedięinin tespit edilmesi halinde uygun görülmeyen başvuru gerekęeli olarak başvuru sahibine bildirilir.

(6) Bildirilen eksikliklerin giderilmesi halinde, başvuru sahibi, bu maddede belirtilen řekilde yeniden başvurusunu geręekleřtirebilir.

KDHS sürecindeki deęiřiklikler

MADDE 9 - (1) KDHS, faaliyete geçtikten sonra, yapmış olduğu başvuru şartlarında herhangi bir değişiklik meydana gelmesi halinde, bu değişiklikleri en geç 20 (yirmi) gün içinde Genel Müdürlüğe bildirir ve taahhütname bu değişikliklere uygun olarak yenilenir. Meydana gelen değişikliğin bildirilmediğinin tespit edilmesi halinde 26 ncı maddenin birinci fıkrasının (b) bendine göre işlem yapılır.

(2) Bu Yönetmelikte, EKDS ile ilgili standartlarda veya taahhütnamede yapılan değişikliklere KDHS'nin ne kadar sürede uyum sağlayacağını belirlemeye Genel Müdürlük yetkilidir. KDHS'nin değişikliklere uyum sağlayamaması durumunda, KDHS faaliyet izni Bakan onayı ile iptal edilir.

KDPS, rol ve güvenli iletişim sertifikaları başvuru süreci

MADDE 10 - (1) KDHS, hizmet alan adına, TSE tarafından yayımlanan KDPS ve rol sunucusuna ilişkin EKDS standardını sağlamak şartıyla, KDPS ile rol ve güvenli iletişim sertifikaları talep etmek üzere, Genel Müdürlüğün resmi internet sitesinde yayımlanan yöntem ile Genel Müdürlüğe başvuru yapar.

(2) Kamu kurum ve kuruluşları, rol ve güvenli iletişim sertifikası başvurularını Genel Müdürlüğün belirleyeceği yönteme uygun olarak doğrudan yapabilir.

(3) Genel Müdürlük, EKDS Değerlendirme Komisyonunun kararı ve Bakan onayı neticesinde, talebi uygun görülenleri yetkilendirmek üzere ESHS'ye ve başvuru sahibine bildirir.

GEM akıllı kartı ve yazılım yayıncı sertifikası başvuru süreci

MADDE 11 - (1) KEC üreticileri, GEM akıllı kartı talepleri için aşağıdaki belgelerle birlikte Genel Müdürlüğe başvuru yapar:

- a) KEC standardı uygunluk belgesi,
- b) Ortak kriterler uygunluk belgesi,
- c) Kullanılacak KEC yazılımı sürümü,
- ç) Talep edilen GEM akıllı kartı miktarı.

(2) KEC üreticileri, GEM akıllı kartı talebini içeren başvurularını Genel Müdürlüğün resmi internet sitesinde yayımlanan yöntem ile Genel Müdürlüğe yapar.

(3) Başvurular en geç 3 (üç) ay içinde EKDS Değerlendirme Komisyonu tarafından sonuçlandırılarak Bakan onayına sunulur. Genel Müdürlük, başvurusu onaylananların GEM akıllı kartı ve yazılım yayıncı sertifikası taleplerini ESHS'ye ve başvuru sahibine bildirir.

(4) GEM akıllı kartı ve yazılım yayıncı sertifikası talepleri uygun görülen KEC üreticilerine ilişkin detaylar Genel Müdürlüğün resmi internet sitesi üzerinden kamuoyuna duyurulur.

(5) EKDS Değerlendirme Komisyonu tarafından yapılan incelemede, başvuru şartlarının yerine getirilmediğinin tespit edilmesi halinde uygun görülmeyen başvurunun sonucu gerekçeli olarak başvuru sahibine bildirilir.

(6) Başvuru sahibi, bildirilen eksiklikleri gidermesi halinde bu maddede belirtilen şekilde başvurusunu yeniden gerçekleştirebilir.

DÖRDÜNCÜ BÖLÜM

Sertifikasyon Süreci

KDS sertifikası oluşturulması süreci

MADDE 12 - (1) EKDS'yi işletmek isteyen KDHS, Genel Müdürlüğün resmi internet sitesinde yayımlanan yöntem ile KDS sertifikası talebini Genel Müdürlüğe iletir ve talep EKDS Değerlendirme Komisyonu tarafından sonuçlandırılarak Bakan onayına sunulur.

(2) Genel Müdürlük, onaylanan KDS sertifikası taleplerini ESHS'ye en geç 7 (yedi) iş günü içerisinde bildirir.

(3) Görevli ESHS, Genel Müdürlük tarafından geçerlilik süresi belirlenen KDS sertifikasını oluşturur ve en geç 7 (yedi) iş günü içerisinde teslim eder.

(4) ESHS, üretilen KDS sertifikasını kamuya açık bir dizinde yayımlar ve dizin hizmetinin kesintisiz olarak verilmesini sağlar.

(5) Görevli ESHS, KDS sertifikası başvurusundan sonra sertifikayı oluşturur ve KDHS'nin HSM'sine yükler.

KDPS, rol ve güvenli iletişim sertifikalarının oluşturulması

MADDE 13 - (1) Genel Müdürlük, uygun görülen, KDPS, rol ve güvenli iletişim sertifikası taleplerini ESHS'ye bildirir.

(2) Görevli ESHS, KDPS ve rol sertifikasını üretir ve başvuru sahibine en geç 30 (otuz) gün içinde teslim eder.

(3) Rol sertifikasının özel anahtarı HSM'de saklanır.

(4) Güvenli iletişim sertifikası, görevli ESHS tarafından rol sertifikası ile birlikte teslim edilir.

GEM akıllı kartının oluşturulması

MADDE 14 - (1) KEC üreticisi, onay verilen miktardaki GEM akıllı kartını, ESHS ile yapacağı GEM akıllı kart sözleşmesi ile beraber görevli ESHS'den talep eder.

(2) GEM akıllı kartları, sözleşmenin imzalanmasından sonra sözleşmede belirtildiği şekilde kullanıma kapalı ve aktifleştirilmemiş halde, başvuru tarihinden itibaren en geç 30 (otuz) gün içerisinde yazılım yayıncı sertifikası ile birlikte KEC üreticisine teslim edilir.

GEM akıllı kartının kullanıma açılması

MADDE 15 - (1) KDHS, hizmet alanın KEC ile eşleşmiş GEM akıllı kartlarının kullanıma açılmasına ilişkin başvuruyu, Genel Müdürlüğün resmi internet sitesinde yayımlanan yöntem ile Genel Müdürlüğe yapar.

(2) Genel Müdürlük, GEM akıllı kartlarının kullanıma açılması talebini herhangi bir idari ve teknik engelin bulunmaması halinde görevli ESHS'ye en geç 7 (yedi) iş günü içerisinde bildirir.

(3) Görevli ESHS, kendisine bildirilen GEM akıllı kartlarındaki sertifikaları en geç 7 (yedi) iş günü içerisinde kullanıma açarak Genel Müdürlüğe ve KDHS'ye bildirir.

Sertifika iptal süreci

MADDE 16 - (1) EKDS'de üretilen bütün sertifikaların iptalleri görevlendirilmiş ESHS tarafından aşağıdaki gerekçelerle yapılabilir:

- a) Genel Müdürlüğün talebi,
- b) Sertifika sahiplerinin talebi,
- c) Sertifikanın ilişkili olduğu özel anahtarın yüklendiği ortamın kaybolması veya çalınması,
- ç) Sertifikanın ilişkili olduğu özel anahtarın güvensiz veya kullanılmaz hale gelmesi,
- d) KEC üreticisinin GEM akıllı kartlarının içerisindeki sertifikaların iptal edilmesini talep etmesi.

(2) Rol sertifikaları ve güvenli iletişim sertifikalarının geçerlilik süresi sona erdiğinde yenilenmesi durdurulur. İptal talebi yapılan rol sertifikaları ve güvenli iletişim sertifikalarının talep yapıldığı andan itibaren kullanılmamasının sağlanması KDHS ve sertifika sahibi kurumun sorumluluğundadır.

(3) Sertifika iptal talepleri, görevli ESHS tarafından belirlenen yöntemle doğrudan ESHS'ye yapılır.

(4) Görevli ESHS kendisine iletilen sertifika iptal taleplerine derhal müdahale eder, bildirim ve iptal işleminin sonucunu Genel Müdürlüğe en geç 2 (iki) iş günü içerisinde raporlar. İptal işleminin gerçekleştirilmemesi durumunda ortaya çıkabilecek sorumluluk görevli ESHS'ye aittir.

(5) Görevli ESHS, sertifikalara ilişkin iptal durum kaydını herhangi bir kimlik doğrulamasına gerek olmaksızın ücretsiz ve kesintisiz olarak kamu erişimine açık tutar.

(6) İptal edilen sertifikalara ilişkin iptal sebepleri, olası riskler ve alınacak önlemlere ilişkin kamuoyu duyuruları görevli ESHS tarafından yapılır.

BEŞİNCİ BÖLÜM

Yükümlülükler

ESHS'nin yükümlülükleri

MADDE 17 - (1) Yetkili ESHS, EKDS'ye ilişkin iş ve işlemlerini, Genel Müdürlüğün kuracağı yönetim altyapısı üzerinden Genel Müdürlüğe bildirir.

(2) Yetkili ESHS, EKDS'ye ilişkin sunduğu hizmetlerin sürekli ve kesintisiz sağlanması için gerekli önlemleri alır.

(3) Yetkili ESHS, Bakanlığın izni dışında EKDS'ye ilişkin iş ve işlemlerin hiçbirini yürütmez.

KDHS'nin yükümlülükleri

MADDE 18 - (1) KDHS, kurduğu altyapı sistemindeki beyaz listeyi Genel Müdürlük ile paylaşır.

(2) KDHS verdiği hizmeti, Genel Müdürlük ile paylaştığı beyaz liste ile sınırlamakla yükümlüdür.

(3) KDHS, beyaz liste dışında tesis edilmeye çalışılan işlemleri engellemeye ve yaptığı tespiti Genel Müdürlüğe bildirmekle yükümlüdür.

(4) KDHS, EKDS ile ilgili verdiği hizmette kullandığı donanım ve yazılımların EKDS standartlarına uygunluğuna ve bunların güvenliğine ilişkin gerekli tedbirleri almakla yükümlüdür.

(5) KDHS, imzalanan ve güncellenen taahhütname hükümlerine uymakla yükümlüdür.

Hizmet alanın yükümlülükleri

MADDE 19 - (1) Hizmet alan, yeni temin ettiği veya operasyonel sebeplerden dolayı;

a) Çalıştığı KEC üreticilerinden,

b) Temin ettiği KEC'lerin seri numaralarından,

c) KEC'ler ile ilişkilendirilmiş GEM akıllı kart seri numaralarından,

ç) Çalıştığı KDHS'lerden,

herhangi birinde veya tamamında deęişiklik olması durumunda; söz konusu hususları, anlaşma sağladığı veya deęişiklięin olduęu tarihten itibaren en geç 20 (yirmi) gün içerisinde Genel Müdürlüğe ileilmek üzere KDHS'ye bildirmekle yükümlüdür.

ALTINCI BÖLÜM

Teknik Hususlar, Güvenlik ve Denetim

KDHS verileri

MADDE 20 - (1) KDHS, EKDS'ye ilişkin imza oluşturma ve doğrulama verileri ile sertifikasını Türkiye Cumhuriyeti sınırları dışına çıkaramaz.

(2) KDHS'ye ait imza oluşturma ve doğrulama verilerinin geçerlilik süresi 10 (on) yılı aşamaz.

Elektronik kimlik doğrulama sisteminde verilerin güvenliği

MADDE 21 - (1) Kimlik kartındaki veriler kimlik doğrulama amacı dışında kullanılamaz.

(2) Hizmet alan ve KDHS, kimlik kartındaki verilerin hukuka aykırı olarak işlenmesi ile söz konusu verilere hukuka aykırı olarak erişilmesini önlemek ve muhafazasını sağlamak amacıyla, uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri alır. Özel nitelikli kişisel veriler için ayrıca, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununun 6 ncı maddesinin dördüncü fıkrası uyarınca Kişisel Verileri Koruma Kurulu tarafından belirlenen yeterli önlemler alınır.

(3) Biyometrik veriler ile kimlik kartlarına ait PIN veya PUK bilgileri toplanamaz, saklanamaz ve paylaşamaz.

(4) EKDS Deęerlendirme Komisyonunun belirledięi yetkiler dâhilinde hizmet alanlar, 5490 ve 6698 sayılı Kanunlarda belirtilen usul ve esaslara uymakla ve hizmet verdięi ilgili birimlerin de bu esaslar dâhilinde işlem yaptığını takip etmekle yükümlüdür.

(5) ESHS tarafından verilen anahtar, sertifika ve yetkiler Bakanlığın izni olmadan devredilemez.

Elektronik kimlik doğrulama sistemi sunucularına erişim ve güvenlik

MADDE 22 - (1) KDHS yetkili personeli ve EKDS'de kullanılacak yazılım, EKDS standardında belirlenen esaslara göre EKDS sunucularına erişir.

(2) EKDS sunucularına ve çevre birimlerine karşı yetkisiz erişimlerin engellenmesi amacıyla KDHS tarafından geri izleme ve güvenlik sistemi kurulur.

(3) EKDS ile ilgili güvenliğe ilişkin olarak 6698 sayılı Kanun ve ilgili mevzuata uygun gerekli her türlü teknik ve idari tedbirler alınır.

(4) EKDS ile ilgili güvenliğe ilişkin diğer usul ve esaslar Genel Müdürlük tarafından belirlenir.

KDS'den kimlik doğrulama başarımlarının alınmadan hizmetin verilmesi

MADDE 23 - (1) Kimlik doğrulama işlemi için KDS'den kimlik doğrulama başarımlarının alınmadan hizmet verilmesinin sorumluluğu hizmet alanına aittir.

Geri izleme

MADDE 24 - (1) EKDS'ye ilişkin kayıtlar, KDHS tarafından EKDS standartlarına uygun şekilde geri izleme bilgisi olarak 8 (sekiz) yıl süreyle saklanır.

Denetim

MADDE 25 - (1) EKDS'nin mevzuata, ilgili standartlara ve taahhünameye uygun olarak işletilip işletilmediği Genel Müdürlükçe denetlenir.

(2) Genel Müdürlük yapacağı denetimlerde kamu kurum ve kuruluşlar ile özel hukuk tüzel kişilerinden faydalanabilir veya hizmet alabilir.

(3) Denetim sırasında, denetim yapmaya yetkili görevliler, EKDS ile ilgili her türlü belge ve kayıtları isteyebilir; EKDS ile ilgili fiziki alanlara girebilir.

(4) Denetim sonucuna göre mevzuata aykırı faaliyet gösterdiği tespit edilenler hakkında, 5490 ve 6698 sayılı Kanunlar ile 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun ilgili madde hükümlerine göre işlem yapılır.

YEDİNCİ BÖLÜM

Faaliyetin Sona Ermesi

Denetim sonucunda KDHS'nin faaliyetine son verilmesi

MADDE 26 - (1) Denetim sonucunda;

a) Genel Müdürlük tarafından faaliyetinin devamına engel teşkil edecek bir durumun tespit edilmesi halinde KDHS'nin faaliyetlerine 1 (bir) ayı geçmemek üzere belirlenecek süre içerisinde son verileceği hizmet alanlarla paylaşılır ve sürenin sonunda KDHS'nin faaliyetine Bakan onayı ile son verilir.

b) KDHS'nin gerekli şartları yerine getirmediğinin tespit edilmesi halinde, eksikliğin giderilmesi için KDHS'ye 3 (üç) aya kadar süre verilebilir. KDHS'nin, verilmiş olan sürenin sonunda eksikliği giderememesi halinde KDHS'nin faaliyetlerine 1 (bir) ayı geçmemek üzere belirlenecek süre

içerisinde son verileceği hizmet alanlarla paylaşılır ve sürenin sonunda KDHS'nin faaliyetine Bakan onayı ile son verilir.

(2) Hizmet alan, KDHS'nin faaliyeti sonlanmadan önce başka bir KDHS ile kimlik doğrulama hizmeti almak üzere anlaşır.

(3) Hizmet alan, faaliyetine son verilen KDHS'de saklanan, KDB verilerinin anlaştığı KDHS'ye devrinden eski KDHS ile birlikte müteselsilen sorumludur.

(4) Genel Müdürlük, mücbir sebeplerin ortaya çıkması halinde bu maddede belirtilen süreleri uzatabilir.

(5) Faaliyetine son verilen KDHS, hizmet alanların tamamının devir işlemlerini tamamlamasını müteakip kimlik doğrulama hizmetine son verir.

(6) Faaliyetine son verilen KDHS, devir işlemlerinden sonra KDB verileri ve EKDS ile ilgili imza oluşturma verisi ile yedeklerini imha eder ve bu durumu kayıt altına alarak Genel Müdürlüğe bildirir.

(7) Kimlik doğrulama hizmetinin devredilebileceği herhangi bir KDHS'nin bulunamaması durumunda kimlik doğrulama faaliyetine son verilen KDHS'nin oluşturduğu KDB verilerini teslim alacak merciyi belirlemeye Genel Müdürlük yetkilidir. KDB verilerini teslim alan merci, KDB verilerini bu Yönetmelikte belirtildiği süre kadar saklamak ve veriyi sakladığı süre içerisinde adli ve idari taleplere cevap vermekle yükümlüdür.

KDHS'nin kendi faaliyetine son vermesi halinde yapılacak işlemler

MADDE 27 - (1) KDHS, faaliyetine son vereceği tarihten en az 3 (üç) ay önce durumu Genel Müdürlüğe bildirir.

(2) KDHS ve Genel Müdürlük, KDHS'nin faaliyetine son vereceğini internet sayfasında yayımlar.

(3) KDHS; faaliyetine son verme tarihine kadar hizmetlerine devam eder. Genel Müdürlük alacağı karar doğrultusunda 1 (bir) ayı geçmemek üzere süreyi uzatabilir.

(4) Hizmet alan, KDHS'nin faaliyeti sonlanmadan önce başka bir KDHS ile kimlik doğrulama hizmeti devri konusunda anlaşır.

(5) Genel Müdürlük, taraflar arasında anlaşma sağlanması halinde, faaliyetine son verilen KDHS'de bulunan KDB verilerinin devredilmesine karar verir.

(6) Hizmet alan, faaliyetine son veren KDHS'de saklanan, KDB verilerinin anlaştığı KDHS'ye devrinden eski KDHS ile birlikte müteselsilen sorumludur.

(7) KDHS, devir işlemlerinin tamamlanmasını müteakip kimlik doğrulama hizmetine son verir.

(8) Faaliyetine son veren KDHS, devir işlemlerinden sonra KDB verisini ve EKDS ile ilgili imza oluşturma verisi ile yedeklerini imha eder ve bu durumu kayıt altına alarak Genel Müdürlüğe bildirir.

(9) Kimlik doğrulama hizmetinin devredilebileceği herhangi bir KDHS'nin bulunamaması durumunda kimlik doğrulama faaliyetine son veren KDHS'nin oluşturduğu KDB verilerini teslim alacak merciyi belirlemeye Genel Müdürlük yetkilidir. KDB verilerini teslim alan merci, KDB verilerini bu Yönetmelikte belirtildiği süre kadar saklamak ve veriyi sakladığı süre içerisinde adli ve idari taleplere cevap vermekle yükümlüdür.

Hizmet alanın KDHS değişikliği yapması

MADDE 28 - (1) Hizmet alan, hizmet almakta olduğu KDHS'yi değiştirebilir.

(2) Hizmet alan, hizmet almına son verdiği KDHS'de saklanan KDB verilerinin, anlaştığı KDHS'ye devrinden eski KDHS ile birlikte müteselsilen sorumludur.

(3) KDB verilerini devir alan KDHS, KDB verilerini bu Yönetmelikte belirtildiği süre kadar saklamak ve veriyi sakladığı süre içerisinde adli ve idari taleplere cevap vermekle yükümlüdür.

Hizmet alanın faaliyetine son vermesi

MADDE 29 - (1) Hizmet alanın, faaliyetine son vermesi halinde; hizmet aldığı KDHS, KDB verilerini bu Yönetmelikte belirtildiği süre kadar saklamak ve veriyi sakladığı süre içerisinde adli ve idari taleplere cevap vermekle yükümlüdür.

SEKİZİNCİ BÖLÜM

Kimlik Doğrulama Yöntemleri

Kimlik doğrulama yöntemleri

MADDE 30 - (1) Kimlik doğrulama işlemleri aşağıdaki yöntemlerden biri kullanılarak gerçekleştirilir:

a) Fiziksel kimlik doğrulama: Kart gövdesi üzerinde bulunan görsel güvenlik özellikleri ve kimlik bilgileri kullanılarak yapılan doğrulama yöntemidir.

b) Kimlik doğrulama sertifikası ile kimlik doğrulama: Kimlik doğrulama sertifikasının Genel Müdürlük tarafından verildiğinin ve geçerliliğinin akıllı kart okuyucu kullanılarak kontrol edilmesi yöntemidir.

c) KEC kullanılarak kimlik doğrulama sertifikası ile kimlik doğrulama: Kimlik doğrulama sertifikasının ve temaslı yonganın Genel Müdürlük tarafından verildiğinin ve geçerliliğinin KEC kullanılarak kontrol edilmesi yöntemidir.

ç) KEC kullanılarak kimlik doğrulama sertifikası ve fotoğraf ile kimlik doğrulama: Kimlik doğrulama sertifikasının ve temaslı yonganın Genel Müdürlük tarafından verildiğinin ve geçerliliğinin KEC kullanılarak kontrol edilmesi ve vatandaşın kimlik kartından okunan fotoğrafının hizmet veren tarafından doğrulanması yöntemidir.

d) KEC kullanılarak kimlik doğrulama sertifikası ve biyometrik veri ile kimlik doğrulama: Kimlik doğrulama sertifikasının ve temaslı yonganın Genel Müdürlük tarafından verildiğinin ve geçerliliğinin, KEC kullanılarak kontrol edilmesi ve vatandaşın biyometrik verisinin KEC kullanılarak doğrulanması yöntemidir.

e) KEC kullanılarak kimlik doğrulama sertifikası, fotoğraf ve biyometrik veri ile kimlik doğrulama: Kimlik doğrulama sertifikasının ve temaslı yonganın Genel Müdürlük tarafından verildiğinin ve geçerliliğinin KEC kullanılarak kontrol edilmesi, vatandaşın biyometrik verisinin KEC kullanılarak doğrulanması ve vatandaşın kimlik kartından okunan fotoğrafının hizmet veren tarafından doğrulanması yöntemidir.

f) Kimlik doğrulama sertifikası ve PIN ile kimlik doğrulama: Kimlik doğrulama sertifikasının Genel Müdürlük tarafından verildiğinin ve geçerliliğinin Akıllı Kart Okuyucu kullanılarak kontrol edilmesi ve kimlik doğrulama PIN'inin akıllı kart okuyucu kullanılarak doğrulanması yöntemidir.

g) KEC kullanılarak kimlik doğrulama sertifikası ve PIN ile kimlik doğrulama: Kimlik doğrulama sertifikasının ve temaslı yonganın Genel Müdürlük tarafından verildiğinin ve geçerliliğinin KEC kullanılarak kontrol edilmesi ve kimlik doğrulama PIN'inin KEC kullanılarak doğrulanması yöntemidir.

ğ) KEC kullanılarak kimlik doğrulama sertifikası, PIN ve fotoğraf ile kimlik doğrulama: Kimlik doğrulama sertifikasının ve temaslı yonganın Genel Müdürlük tarafından verildiğinin ve geçerliliğinin KEC kullanılarak kontrol edilmesi, kimlik doğrulama PIN'inin KEC kullanılarak doğrulanması ve vatandaşın kimlik kartından okunan fotoğrafının hizmet veren tarafından doğrulanması yöntemidir.

h) KEC kullanılarak kimlik doğrulama sertifikası, PIN ve biyometrik veri ile kimlik doğrulama: Kimlik doğrulama sertifikasının ve temaslı yonganın Genel Müdürlük tarafından verildiğinin ve

geçerliliğinin KEC kullanılarak kontrol edilmesi, kimlik doğrulama PIN'inin ve vatandaşın biyometrik verisinin KEC kullanılarak doğrulanması yöntemidir.

1) KEC kullanılarak kimlik doğrulama sertifikası, PIN, fotoğraf ve biyometrik veri ile kimlik doğrulama: Kimlik doğrulama sertifikasının ve temaslı yonganın Genel Müdürlük tarafından verildiğinin ve geçerliliğinin KEC kullanılarak kontrol edilmesi, kimlik doğrulama PIN'inin ve vatandaşın biyometrik verisinin KEC kullanılarak doğrulanması ve vatandaşın kimlik kartından okunan fotoğrafının hizmet veren tarafından doğrulanması yöntemidir.

(2) Kimlik doğrulama yöntemlerinden hangisinin veya hangilerinin kullanılacağı, hizmet alan kurumun tabi olduğu mevzuat hükümlerine ve hizmetin niteliğine uygun olarak hizmet alan tarafından belirlenir.

(3) Genel Müdürlük tarafından belirlenecek diğer yöntemler standart olarak tanımlandıktan sonra, kimlik tespit ve doğrulama yöntemi olarak kullanılabilir.

DOKUZUNCU BÖLÜM

Çeşitli ve Son Hükümler

Faaliyet raporu

MADDE 31 - (1) KDHS, her yıl Mart ayı sonuna kadar Genel Müdürlüğe bir önceki yıla ilişkin rapor verir. Rapor aşağıdaki asgari unsurları içerir:

- a) Yıl içinde sunulan hizmetin detaylarını,
- b) Varsa kendisine devredilen KDB verilerini,
- c) Genel Müdürlük tarafından istenecek diğer bilgi ve belgeleri.

(2) Genel Müdürlük tarafından talep edilmesi durumunda, görevlendirilen ESHS, EKDS'nin kullanımına yönelik rapor hazırlamakla sorumludur.

Tereddütlerin giderilmesi

MADDE 32 - (1) Bu Yönetmeliğin uygulanması sırasında doğabilecek tereddütleri ve uygulamaya ilişkin aksaklıkları gidermeye Bakanlık yetkilidir.

Yürürlük

MADDE 33 - (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 34 - (1) Bu Yönetmelik hükümlerini İçişleri Bakanı yürütür.

Kimlik Paylaşımı Sistemi Yönetmeliđi

Resmî Gazete Tarihi : 21.08.2020

Resmî Gazete Sayısı : 31220

KİMLİK PAYLAŞIMI SİSTEMİ YÖNETMELİĐİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1- (1) Bu Yönetmeliđin amacı; İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü merkezi veri tabanında yer alan verilerin, alıcı kurumlarla çevrimiçi paylaşımına ilişkin usul ve esasları düzenlemektir. (1)

Kapsam

MADDE 2- (1) Bu Yönetmelik, merkezi veri tabanındaki verilerin; alıcı kurumlarla paylaşımı, paylaşımına ilişkin başvuru, taahhütnamenin imza, iptal ve fesih süreçleri, yetkilendirilme, paylaşılan verilerin gizliliğinin ve güvenliğinin sağlanması, kurumların iş ve işlemlerine ilişkin bilgilerin takibi ve kullanıcıların eğitimine ilişkin usul ve esasları kapsar.

Dayanak

MADDE 3- (1) Bu Yönetmelik, 25/4/2006 tarihli ve 5490 sayılı Nüfus Hizmetleri Kanunu ile 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi hükümlerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4- (1) Bu Yönetmelikte geçen;

- Alıcı kurum: Kimlik Paylaşımı Sisteminden faydalanan Genel Müdürlük dışındaki kurum ve kamu hizmeti sunan tüzel kişilikleri,
- Alt kullanıcı: Alıcı kurumun, uygulamalar üzerinden web servis yolu ile Kimlik Paylaşımı Sisteminden faydalanması için yetkilendirdiği kişileri,
- Bakanlık: İçişleri Bakanlığını,

- c) Genel Mdrlk: Nfus ve Vatandaşlık İşleri Genel Mdrlğn,
- d) IP adresi: İnternet ya da diğr paket anahtarlamalı ağlara baėlı cihazların, ağ zerinden birbirleri ile veri alışverişı yapmak iin kullandıkları adresi,
- e) İdari kullanıcı: Alıcı kurum adına Kimlik Paylaşımı Sistemi ile ilgili iş ve işlemleri yrtmeye ve imzaya yetkili kurum temsilcisini,
- f) Kanun: 25/4/2006 tarihli ve 5490 sayılı Nfus Hizmetleri Kanununu,
- g) Kimlik numarası: Genel Mdrlk merkezi veri tabanında tutulan kimlik numaralarını,
- ğ) Kimlik Paylaşımı Sistemi: Merkezi veri tabanında tutulan verilerin alıcı kurumlar ile paylaşıldığı sistemi,
- h) Kişisel veri: Kimliği belirli veya belirlenebilir gerek kişiye ilişkin her trl bilgiyi,
- ı) Kullanıcı: Alıcı kurumca tanımlanan idari kullanıcıyı, teknik kullanıcıları, servis kullanıcılarını ve alt kullanıcıları,
- i) Kurul: Merkezi veri tabanında yer alan verilerin paylaşımına ilişkin talepleri deėerlendirmek zere oluřturulan Veri Paylaşımı Kurulunu,
- j) Kurum: Genel Mdrlk dıřındaki diğr kamu kurum ve kuruluřlarını,
- k) Merkezi veri tabanı: Genel Mdrlke elektronik ortamda tutulan verileri,
- l) Nfus mdrlğ: İl nfus ve vatandaşlık mdrlğ ile ile nfus mdrlğn,
- m) Portal: Bu Ynetmelikle yetkileri tanımlanmış olan alıcı kurum kullanıcılarının iş ve işlemlerini takip ettiėi elektronik ortamı,
- n) Servis kullanıcı: Alıcı kurum adına Kimlik Paylaşımı Sistemi aracılıėıyla sunulan web servis hizmetlerinin eklenti yolu ile kullanılabilmesi iin merkezi veri tabanında oluřturulan sanal kullanıcıyı,
- o) Taahhtname: Alıcı kurumların imzaladıėı ve paylaşılan verilerin gvenliėini saėlamaya ynelik olmayı taahht ettiėi idari ve teknik tedbirleri ieren belgeyi,
- ) Teknik kullanıcı: İdari kullanıcı tarafından Kimlik Paylaşımı Sisteminden faydalanması iin merkezi veri tabanına tanımlanmış kişileri,
- ifade eder.

İKİNCİ BLM

Paylaşım Esasları

Verilerin paylaşımına ilişkin esaslar

MADDE 5- (1) Merkezi veri tabanında tutulan veriler, Kanun ile 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununda ve bu Kanunların ikincil düzenlemelerinde belirtilen usul ve esaslar çerçevesinde alıcı kurumlar ile paylaşılır. Paylaşılacak veriler, alıcı kurumun veri işleme amacı ve yasal dayanağı göz önüne alınarak belirlenir.

(2) Kimlik Paylaşımı Sisteminden, mücbir sebepler dışında güvenli ve kesintisiz bir şekilde hizmet sunulması esastır.

(3) Genel Müdürlük, alıcı kurumlar tarafından tanımlanmış kullanıcılar haricinde Kimlik Paylaşımı Sistemine yetkisiz erişimin engellenmesi için gerekli tedbirleri alır.

(4) Alıcı kurumlar, kendi iş ve işlemlerine esas olmak üzere sadece ilgili kişilerin bilgilerini alabilirler ve aldıkları bilgileri tanımlanmış hizmetlerin yerine getirilmesi dışında başka hiçbir amaçla kullanamaz. Alıcı kurumlar, yaptıkları iş ve işlemleri Kimlik Paylaşımı Sisteminden elde ettikleri güncel verilerle gerçekleştirir.

(5) Kimlik Paylaşımı Sistemi yoluyla merkezi veri tabanından elde edilen veriler, aksi ispat oluncaya kadar geçerlidir.

(6) Kimlik Paylaşımı Sistemi üzerinden erişilebilen bilgi ve belgeler, alıcı kurumlar tarafından ilgisinden veya nüfus müdürlüğünden talep edilemez. Kimlik Paylaşımı Sistemi vasıtasıyla üretilen belgeler, nüfus müdürlüklerinden alınmış belgelerle aynı hukuki değere sahiptir.

(7) Alıcı kurumun, kendi iş ve işlemlerinde kullanmak üzere Kimlik Paylaşımı Sistemi üzerinden ürettiği belgeler, gerekli görülmesi halinde alıcı kurumun görevlisi tarafından onaylanır.

(8) Alıcı kurumlar, Kimlik Paylaşımı Sisteminden yaptıkları sorgulamalara ilişkin kullanım bilgilerini takip ve kontrol eder.

Başvuru ve taahhütname süreci

MADDE 6- (1) Kimlik Paylaşımı Sisteminden yararlanmak isteyen alıcı kurumlar, Genel Müdürlüğe yazılı olarak veya elektronik ortamda talepte bulunur.

(2) Başvuruda, talep edilen bilgilerin kullanılma gerekçesinin açık, net ve somut olması, alıcı kurumun bilgileri almasına esas olan yasal dayanağın belirtilmesi ve Genel Müdürlük tarafından talep edilen belgelerin gönderilmesi zorunludur.

(3) Yapılan başvurular Kurul tarafından değerlendirilir. Kurulca uygun görülmeyen alıcı kurumların başvurusu gerekçesi belirtilerek reddedilir.

(4) Başvurusu Kurulda uygun görülen kurumların Genel Müdürlükçe belirlenen uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü idari ve teknik tedbirleri aldığını yazılı olarak beyan etmesi zorunludur. Beyan edilen idari ve teknik tedbirlerin devamlılığı ve güncelliğinden alıcı kurum sorumludur.

(5) Genel Müdürlükçe belirlenen güvenlik unsurlarını sağlamayan alıcı kurumlar, bu hususun bildirildiği tarihten itibaren altmış gün içinde eksiklikleri tamamlamak zorundadır. Aksi halde alıcı kurumun başvurusu reddedilir.

(6) Başvurusu uygun görülen alıcı kurum tarafından taahhütname imzalanır. Genel Müdürlüğün uygun ve gerekli gördüğü hallerde taahhütname hükümlerinde değişikliğe gidilebilir ve bu durumda taahhütname yenilenir.

(7) Taahhütnamede aşağıda belirtilen hususlara yer verilir:

- a) Verilere hangi amaçla erişileceği.
- b) Erişimin hukuki sebebi.
- c) Verilere erişim şekli ve süresi.
- ç) Yetki ve görevler.
- d) Hukuki sorumluluk.
- e) Alınması gereken idari ve teknik tedbirler.
- f) Diğer hususlar.

(8) Genel Müdürlük, merkezi veri tabanında tutulan verileri, bu Yönetmelikte belirlenen usul ve esaslara göre hazırlanmış taahhütnamenin alıcı kurum tarafından imzalanmasından sonra Kimlik Paylaşımı Sistemi ile paylaşımına açabilir.

Kimlik Paylaşımı Sisteminde tanımlama ve yetkilendirme

MADDE 7- (1) Genel Müdürlük alıcı kurumların, sabit IP adresi ve uygun görülecek güvenlik yöntemleri ile bağlantı kurarak internet üzerinden Kimlik Paylaşımı Sistemine erişimini sağlar.

(2) Alıcı Kurum, Kimlik Paylaşımı Sistemi bağlantısını taahhütnamede belirlenen amaçlar doğrultusunda taşra teşkilatına, şubelerine ve alt kuruluşlarına da sağlayabilir. Kamu kurum ve kuruluşları, yurt dışı teşkilatlarına da bu hizmeti sağlayabilir.

(3) Alıcı kurumların taşra teşkilatları, şubeleri, alt kuruluşları veya yurt dışı teşkilatları ile ayrıca taahhütname yapılmaz.

(4) Alıcı kurum, kendi teşkilat yapısı dışındaki kurum, kuruluş ve kişileri Kimlik Paylaşımı Sistemi sorgulama hizmetinden faydalandıramaz.

(5) Alıcı kurum, alt kullanıcıların yetkilerini belirlemek ve tanımlamakla yükümlüdür. Alıcı kurum, tanımladığı kullanıcı bilgilerini Genel Müdürlüğün belirleyeceği yöntem ile Genel Müdürlüğe bildirir.

(6) Genel Müdürlük, alıcı kurumların idari ve teknik kullanıcılarının kontrol edilmesini, taahhütname ile sağlanan yetkilendirme çerçevesinde bilgi almasını ve tanımlanan kullanıcılara ait tüm güncel bilgilerin merkezi veri tabanında tutulmasını sağlamakla yükümlüdür.

Kimlik Paylaşımı Sisteminin kullanılması

MADDE 8- (1) Alıcı kurumların Kimlik Paylaşımı Sistemi yoluyla yapabilecekleri sorgulama yöntemleri, sorgu sayısı limitleri ve alabilecekleri veriler, Kurul tarafından belirlenir. Alıcı kurumlar, tanımlanan yetkilerine ilişkin veri ve dokümanlara Genel Müdürlüğün sunduğu portal üzerinden erişim sağlar.

(2) Kimlik Paylaşımı Sistemi, alıcı kurumların web sayfaları ile ulaşabilecekleri etkileşimli sorgulamalar ve kendi yazılım uygulamaları içerisine ekleyecekleri eklentiler ile sorgulama yapmalarına olanak verecek web servislerinden oluşur.

(3) Alıcı kurumun almaya yetkili olduğu veri, sorgu sonucu gönderilir. Alıcı kurumun mevcut yetkilerine ek olarak yetki talep etmesi durumunda, talep ettiği yetkinin kullanma gerekçesi ve yasal dayanağının belirtilmesi zorunludur. Talep edilen ek yetkinin verilip verilmeyeceğine dair değerlendirme Kurul tarafından yapılır.

Kimlik Paylaşımı Sistemi yoluyla erişilecek bilgilerin gizliliği

MADDE 9- (1) Kimlik Paylaşımı Sisteminin kullanılmasında, mevzuatta yer alan özel hayatın gizliliği ve kişisel verilerin korunmasına ilişkin hükümler esas alınır.

(2) Alıcı kurumlar, aldıkları verileri taahhütnamede belirtilen esaslar doğrultusunda ve mevzuatta belirlenen görev ve sorumluluklarının yerine getirilmesi dışında herhangi bir amaçla kullanamaz.

(3) Alıcı kurumlar, aldıkları verilerin gizliliğini sağlar ve bu verilerin hukuka aykırı olarak işlenmesi ile erişilmesini önlemek ve muhafazasını sağlamak amacıyla her türlü idari ve teknik tedbirleri alır.

Özel nitelikli kişisel veriler için ise 6698 sayılı Kanununun 6 ncı maddesinin dördüncü fıkrası uyarınca Kişisel Verileri Koruma Kurulu tarafından belirlenen önlemler alınır.

(4) Kimlik Paylaşımı Sistemi yoluyla elde edilen verilerin kullanılmasının hukuki sorumluluğu, alıcı kurumlara aittir. Kimlik Paylaşımı Sisteminin bütün aşamalarında görev yapan yetkililer, taahhütnamede belirtilen esaslara uymakla yükümlüdür. Bu yükümlülük, kişilerin görevlerinden ayrılmalarından sonra da devam eder.

(5) Kimlik Paylaşımı Sisteminden elde edilen verilerin ilgili mevzuat ve taahhütnamede yer alan hükümlere aykırı olarak kullanılması, alıcı kurumun sistem yazılımlarından kaynaklanan hatalı sorgulamalar ve güvenlik açıkları gibi sebeplerle verilerin yetkisiz kişilerce elde edilmesi ve kullanılmasından doğan her türlü hukuki, mali ve cezai sorumluluk alıcı kuruma aittir.

(6) Alıcı kurumlar, Kanunda ve 6698 sayılı Kanunda belirtilen usul ve esaslara uymakla ve bu esaslar dahilinde kullanıcıların yaptığı işlemleri takip etmekle yükümlüdür.

Geri izleme bilgilerinin oluşturulması

MADDE 10- (1) Genel Müdürlük, alıcı kurumun Kimlik Paylaşımı Sisteminden yaptığı her türlü işlemin tarihi, saati ve web servis adına ilişkin kayıtları, kullanıcı veya servis, idari ve teknik kullanıcı düzeyinde geri izleme bilgisi olarak tutar.

(2) Alıcı kurumlar, Kimlik Paylaşımı Sisteminden yapılan her türlü işlemin tarihi, saati, web servis adına ilişkin kayıtları, kullanıcı düzeyinde geri izleme bilgisi olarak tutar.

(3) Genel Müdürlük ve alıcı kurumlar geri izleme bilgisini, sorgulanan kişi ve sorgu sonucundan etkilenen diğer kişilerin de kimlik numaralarını içerecek şekilde tutar.

(4) Genel Müdürlük ile alıcı kurumun geri izleme bilgilerinde tutarsızlık olması halinde Genel Müdürlük kayıtları esas alınır.

(5) Genel Müdürlük ve alıcı kurum, değiştirilmesini engelleyerek ve yetkisiz erişime karşı koruyarak, geri izleme bilgilerini sekiz yıl süre ile saklar. Bu süre sonunda geri izleme bilgileri, 28/10/2017 tarihli ve 30224 sayılı Resmî Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik hükümleri kapsamında silinir veya yok edilir.

ÜÇÜNCÜ BÖLÜM

Takip, Denetim ve Değerlendirme

Alıcı kurum işlemlerinin takibi

MADDE 11- (1) Genel Müdürlük, kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek ile muhafazasını sağlamak amacıyla her türlü idari ve teknik güvenlik tedbirlerini alır ve alıcı kurumların da bu tedbirleri almasını takip eder ve denetler.

(2) Genel Müdürlük, alıcı kurumların iş ve işlemlerine ilişkin tüm bilgileri takip eder ve değerlendirir.

(3) Kimlik Paylaşımı Sisteminden faydalanmak isteyen alıcı kurumlar başvuru aşamasında, faydalanan kurumlar ise her takvim yılı sonunda, Kanunun 45 inci maddesinin beşinci fıkrası kapsamında Genel Müdürlükçe talep edilen idari ve teknik güvenlik tedbirlerini sağladığını gösterir güvenlik taahhütnamesini Genel Müdürlüğe gönderir.

Denetim

MADDE 12- (1) Kimlik Paylaşımı Sisteminin kullanan alıcı kurumlar;

a) Mevzuatla kendisine denetim yetkisi ve görevi verilmiş kurum ve kuruluşlar,

b) Genel Müdürlük veya yetkilendireceği kurum,

aracılığıyla denetlenir.

(2) Denetleme sırasında, alıcı kurum tarafından her türlü bilgi, belge, kayıt ve veri taleplerinin karşılanması ve sistemin incelemeye açılması zorunludur.

(3) Denetleme sonucuna göre usulsüzlük tespiti halinde, Kanun, 6698 sayılı Kanun ve 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun ilgili maddelerine göre işlem yapılır.

Taahhütmenin askıya alınması ve iptali

MADDE 13- (1) Alıcı kurumlar; isim, unvan, idari kullanıcı ve adres değişikliğini en geç on beş gün içerisinde Genel Müdürlüğe bildirmekle yükümlüdür. Bu yükümlülüğü yerine getirmediği tespit edilen alıcı kurumların Kimlik Paylaşımı Sisteminden faydalanması geçici olarak askıya alınır. Bu yükümlülüğün yerine getirilmesini müteakip Kimlik Paylaşımı Sistemi kullanıma açılır.

(2) Alıcı kurumun yapısının değişerek birleşmesi veya ayrılması halinde üç ay içerisinde yeni taahhütname imzalanır. Yeni taahhütname imzalanana kadar bu alıcı kurumlar, Kimlik Paylaşımı Sisteminden faydalanmaya devam eder. Belirtilen süre sonunda alıcı kurumca taahhütname imzalanmadığı takdirde bu sürenin uzatılmasına veya erişimin kapatılmasına karar vermeye Kurul yetkilidir.

(3) Alıcı kurum tarafından taahhüt edilen idari ve teknik güvenlik tedbirlerinin yerine getirilmediğinin Genel Müdürlükçe tespit edilmesi halinde Kimlik Paylaşımı Sistemi kullanıma kapatılır ve taahhütname tek taraflı olarak iptal edilebilir.

(4) Kişisel verilerin hukuka aykırı olarak işlenmesinin tespit edilmesi halinde 6698 sayılı Kanunun ilgili hükümlerine göre işlem yapılır.

(5) Kimlik Paylaşımı Sisteminden alınan verilerin doğrudan veya dolaylı olarak gizliliğinin ve güvenliğinin tehlikeye düştüğünün tespit edilmesi halinde alıcı kurumun Kimlik Paylaşımı Sistemine erişim yetkisi askıya alınır. Alıcı kurumun her türlü idari ve teknik tedbirleri alması ve bu tedbirlerin Genel Müdürlükçe uygun görülmesi halinde Kimlik Paylaşımı Sistemine yeniden erişimi sağlanır.

(6) Kamu hizmeti sunan tüzel kişiliğin bu niteliğini kaybetmesi halinde Kimlik Paylaşımı Sistemi taahhütnameyi Genel Müdürlükçe tek taraflı olarak iptal edilir.

DÖRDÜNCÜ BÖLÜM

Çeşitli ve Son Hükümler

Eğitim

MADDE 14- (1) Kimlik Paylaşımı Sistemi ile ilgili eğitim, Genel Müdürlükçe sağlanacak bir portal üzerinden yapılır.

Katılma payı

MADDE 15- (1) Kanunun 65 inci maddesi kapsamında alınacak hizmetler ücrete tabidir.

(2) Ücretlendirmenin usul ve esasları, Bakanlık ile Hazine ve Maliye Bakanlığınca müştereken belirlenir.

Düzenleme yetkisi

MADDE 16- (1) Bu Yönetmeliğin uygulanması sırasında doğacak tereddütleri ve uygulamaya ilişkin aksaklıkları gidermeye, ilke ve standartları belirlemeye, uygulama birliğini sağlayacak gerekli düzenlemeleri yapmaya, bu hususta her türlü bilgi ve belgeyi istemeye ve bu Yönetmelikte yer almayan konularda ilgili mevzuat hükümleri çerçevesinde düzenleme yapmaya Bakanlık yetkilidir.

Yürürlükten kaldırılan yönetmelik

MADDE 17- (1) 16/11/2006 tarihli ve 2006/11249 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan Kimlik Paylaşımı Sistemi Yönetmeliği yürürlükten kaldırılmıştır.

Taahhütnamelerin uyumlu hale getirilmesi

GEÇİCİ MADDE 1- (1) Bu Yönetmeliğin yürürlüğe girdiği tarihten önce imzalanmış bulunan mevcut taahhütnameler, bir yıl içerisinde bu Yönetmelik hükümlerine uygun olarak yenilenir.

Kullanıcı bilgilerinin bildirim ve güncellenmesi

GEÇİCİ MADDE 2- (1) Alıcı kurumlar mevcut kullanıcı bilgilerini, Genel Müdürlüğün belirleyeceği yöntemler ile bir yıl içerisinde Genel Müdürlüğe bildirmek ve güncellemek zorundadır.

Yürürlük

MADDE 18- (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 19- (1) Bu Yönetmelik hükümlerini Cumhurbaşkanı yürütür.

Veri Paylaşımı Kurulu Yönetmeliği

Resmî Gazete Tarihi : 08.08.2020

Resmî Gazete Sayısı : 31207

VERİ PAYLAŞIMI KURULU YÖNETMELİĞİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı; Genel Müdürlük merkezi veri tabanında tutulan kayıtlardan yararlanacak Genel Müdürlük birimlerini, kurumları, kamu hizmeti sunan tüzel kişilikleri ve adrese dayalı kamu hizmeti sunan kuruluşları tespit etmek, çevrimiçi ve çevrimdışı paylaşımın kapsamı, yöntemi ve güvenliğine ilişkin genel usul ve esasları saptamak ve Genel Müdürlük bünyesinde oluşturulan Veri Paylaşımı Kurulunun çalışma usul ve esaslarını belirlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, Genel Müdürlük birimlerinin, kurumların ve kamu hizmeti sunan tüzel kişiliklerin Genel Müdürlük merkezi veri tabanındaki verilerden çevrimiçi veya çevrimdışı yolla yararlanmaları, paylaşımın kapsamı ve yöntemine ilişkin genel usul ve esaslar ile Veri Paylaşımı Kurulunun çalışma usul ve esaslarını kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 25/4/2006 tarihli ve 5490 sayılı Nüfus Hizmetleri Kanununun 45 inci maddesi ile 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete’de yayımlanan 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinin 258 inci maddesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Yönetmelikte geçen;

a) Alıcı kurum: Kimlik Paylaşımı Sisteminden faydalanan Genel Müdürlük dışındaki kurum ve kamu hizmeti sunan tüzel kişilikleri,

- b) Bakanlık: İçişleri Bakanlığını,
- c) Çevrimdışı veri paylaşımı: Merkezi veri tabanında tutulan kayıtların veri tabanından sorgulanarak harici depolama araçları ve Genel Müdürlükçe belirlenen yöntemler ile paylaşımını,
- ç) Çevrimiçi veri paylaşımı: Kimlik Paylaşımı Sistemi servisleri ile yapılan veri paylaşımını,
- d) Diğer kişiler: Çevrimdışı veri paylaşımı yapılacak alıcı kurum dışında kalan kurum ve tüzel kişilikleri,
- e) Genel Müdür: Nüfus ve Vatandaşlık İşleri Genel Müdürünü,
- f) Genel Müdürlük: Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünü,
- g) İdari kullanıcı: Alıcı kurum adına Kimlik Paylaşımı Sistemi ile ilgili iş ve işlemleri yürütmeye ve imzaya yetkili kurum temsilcisini,
- ğ) Kanun: 25/4/2006 tarihli ve 5490 sayılı Nüfus Hizmetleri Kanununu,
- h) Kimlik Paylaşımı Sistemi (KPS): Merkezi veri tabanında tutulan verilerin alıcı kurumlar ile paylaşıldığı sistemi,
- ı) Kişisel veri: Kimliği belirli veya belirlenebilir bir gerçek kişiye ilişkin her türlü bilgiyi,
- i) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olarak ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,
- j) KPS servisi: Merkezi veri tabanındaki verilerin KPS aracılığı ile paylaşılmasını sağlayan web servisini,
- k) Kurul: Veri Paylaşımı Kurulunu,
- l) Kurum: Genel Müdürlük dışındaki diğer kamu kurum ve kuruluşlarını,
- m) Kurum bilgi formatı: Kişi bilgileri ile Türkiye Cumhuriyeti kimlik numarası eşleştirme taleplerinin karşılanmasına yönelik olarak kullanılan, veri deseni ve veri giriş kurallarını içeren ve Genel Müdürlükçe belirlenen formattaki elektronik tabloyu,
- n) Merkezi veri tabanı: Genel Müdürlükçe elektronik ortamda tutulan verileri,
- o) Özel nitelikli kişisel veri: 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununun 6 ncı maddesinin birinci fıkrasında sayılan verileri,

- ö) Servis çıktı parametresi: KPS servisini oluşturan veri elemanlarının her birini,
- p) Servis çıktı yetkisi: Farklı servis parametrelerinin birleşiminden oluşan veri grubunu,
- r) Taahhütname: Alıcı kurumlar ile diğer kişilerin imzaladığı ve elde ettikleri verilerin güvenliğini sağlamaya yönelik almayı taahhüt ettiği idari ve teknik tedbirleri içeren belgeyi,
- s) UAVT: Ulusal Adres Veri Tabanını,
- ifade eder.

İKİNCİ BÖLÜM

Veri Paylaşımı Kurulunun Oluşumu ve Görevleri

Kurulun oluşumu, toplanması ve karar alınması

MADDE 5 - (1) Merkezi veri tabanında yer alan bilgilerin paylaşımına ilişkin talepleri değerlendirerek veri paylaşımından yararlanacakları belirlemek, paylaşımın kapsamı ve hangi yöntemle yapılacağına karar vermek üzere Genel Müdürlük bünyesinde Bakanlık onayı ile Veri Paylaşımı Kurulu oluşturulur.

(2) Kurul, Bakanlık tarafından belirlenen başkan dahil beş üyeden oluşur.

(3) Kurul, her ayın ilk iş günü olağan olarak toplanır. Kurul Başkanının talebi halinde ise olağanüstü toplanır.

(4) Toplantıların gündemi, yeri ve saati Kurul Başkanı tarafından belirlenir. Toplantıda görüşülecek konular ve gündeme ilişkin bilgi ve belgeler Kurul üyelerine en az bir gün önce yazılı veya elektronik olarak iletilir.

(5) Kurul gündemine, toplantı sırasında üyelerden herhangi birinin teklifi üzerine madde eklenebilir.

(6) Kurul en az üç üyenin katılımıyla toplanır. Kurul kararları oy çokluğu ile alınır. Oylarda eşitlik olması halinde Kurul Başkanının bulunduğu taraf çoğunluk sayılır.

(7) Karara muhalif olanlar, şerh koymak suretiyle kararı imzalarlar. Muhalif görüş gerekçesi bir sonraki Kurul toplantısına kadar karar dosyasına eklenmek üzere sekreteryaya teslim edilir.

(8) Kurul kararları, toplantıya katılan tüm üyeler tarafından imzalanır. İmzaların tamamlanması ve Genel Müdür onayına müteakiben karar yürürlüğe girer.

(9) Toplantılarda alınan kararlar her yıl birden başlanarak yılsonuna kadar numaralandırılır.

(10) Gerekli görülen hallerde Kurul Başkanının onayı ile toplantıya üyeler haricinde de oy hakkı olmaksızın katılım sağlanabilir.

(11) Kurulun sekretarya işlemleri, Genel Müdürlük Bilgi İşlem Daire Başkanlığınca yürütülür.

Kurulun görevleri

MADDE 6 - (1) Kurulun görevleri şunlardır:

- a) Çevrimiçi veya çevrimdışı veri paylaşım taleplerini karara bağlamak.
- b) Alıcı kurumlarla, hangi verilerin çevrimiçi olarak paylaşılacağına karar vermek.
- c) Çevrimiçi ek servis, servis çıktı yetkisi ve servis çıktı parametresi taleplerini değerlendirerek karar vermek.
- ç) Benzer konulardaki, çevrimiçi veya çevrimdışı veri paylaşımına ilişkin ilke kararları almak.
- d) Veri paylaşımının kapsamını belirlemek ve hangi yöntemle yapılacağına karar vermek.
- e) Genel Müdürlüğün web sayfası üzerinde doğrulama amaçlı olarak, hangi servislerin yer alacağına ve bu servislerin girdi ve çıktı parametrelerine karar vermek.
- f) Taahhütnamenin iptali, feshi veya veri paylaşımının askıya alınmasına yönelik karar almak.

Sekretaryanın görevleri

MADDE 7 - (1) Kurulun çalışmasına yardımcı olmak üzere sekretarya aşağıdaki görevleri yerine getirir:

- a) Kurulun toplantı gündemini hazırlamak.
- b) Kurul toplantılarının düzenlenmesine ilişkin yazışmaları yapmak.
- c) Kurul toplantılarının tutanaklarını tutmak.
- ç) Kurulun raportörlüğünü yürütmek.
- d) Kurul tarafından alınan kararların ve ilke kararlarının uygulanması için gerekli yazışmaları yapmak.
- e) Kurul kararlarının muhafazasını sağlamak.

ÜÇÜNCÜ BÖLÜM

Veri Paylaşım Yöntemleri ve Taleplerin Değerlendirilmesi

Veri paylaşım yöntemleri

MADDE 8 - (1) Merkezi veri tabanında tutulan veriler Kanunda ve 6698 sayılı Kanunda belirtilen usul ve esaslar çerçevesinde, Kurul tarafından uygun görülen paylaşım yöntemi ile alıcı kurum veya diğer kişiler ile paylaşılabilir.

Taleplerin değerlendirilmesi

MADDE 9 - (1) KPS'den faydalanmak için yapılan tüm talepler Kurul tarafından değerlendirilir.

Taleplerin değerlendirilmesinde uyulacak esaslar

MADDE 10 - (1) KPS üzerinden veri paylaşılacak alıcı kurumları, bu kurumların kullanımına açılacak KPS servisleri ile servis parametrelerini belirlemeye Kurul yetkilidir. Başvuruların değerlendirilmesinde aşağıdaki kriterler esas alınarak başvurular kabul edilir veya reddedilir:

- a) Kendi mevzuatında merkezi veri tabanındaki verileri sorgulama veya doğrulamaya ilişkin görev ve sorumluluğunun bulunması.
- b) Kamu hizmeti sunan tüzel kişiliklerin, faaliyetlerini kamu kurum veya kuruluşlarının denetimi altında sürdürmeleri.
- c) KPS üzerinden veri paylaşımının kamusal ve toplumsal yarar bakımından gereklilik arz etmesi.
- ç) İş ve işlemlerin vatandaşların toplumsal ihtiyaçlarını karşılamak için yapılması, hizmetlerin genel olması ve süreklilik göstermesi.

(2) Kurul gerektiğinde, KPS'den faydalanma talebinde bulunan kamu hizmeti sunan tüzel kişilikler için ilgili kamu kurum veya kuruluşlarından görüş isteyebilir.

(3) Alıcı kurumlara açılacak servis, servis çıktı parametresi ve çıktı yetkisi Kurulca uygun görülen düzeyde karşılanır.

(4) KPS'den faydalanan alıcı kurumların taşra teşkilatı, şubeleri veya alt kuruluşları tarafından yapılan talepler, bünyesinde bulunduğu alıcı kurum tarafından karşılanmak üzere Kurula sunulmaksızın reddedilir.

Çevrimiçi veri paylaşımı kuralları

MADDE 11 - (1) Alıcı kurumlarla internet veya web servisleri vasıtasıyla çevrimiçi veri paylaşımından önce taahhütname imzalanması zorunludur.

(2) Alıcı kurumların ek servis taleplerinin resmi yazı ile yapılması zorunludur.

(3) KPS servis talepleri karşılanırken;

- a) Alıcı kurumun tabi olduğu mevzuat çerçevesinde talep ettiği veriyi alma ve işleme konusunda yetkili ve sorumlu olup olmadığı,
- b) Bilgi paylaşımının kişiler ve toplum için oluşturacağı kamusal ve toplumsal yarar bakımından gereklilik arz edip etmediği,
- c) Talep edilen verilerin, belirtilen amaç ve yasal dayanak ile orantılı olup olmadığı,
- hususlarında; ihtiyaç ve yetki analizi kriterleri kapsamında Kurul tarafından değerlendirme yapılır. Değerlendirme sonucunda alıcı kurumların uygun görülen ek servis talepleri, servis çıktı yetkisi veya servis çıktı parametreleri Kurulca uygun görülen düzeyde karşılanır.

Çevrimdışı taleplerin değerlendirilmesine ilişkin esaslar

MADDE 12 - (1) Alıcı kurumlar, KPS'den alabilecekleri verileri çevrimdışı talep edemezler. Ancak,

- a) Çevrimdışı toplu veri taleplerini resmi yazı ile yapmaları,
- b) Talep yazılarında veriyi kullanma gerekçesi ile yasal dayanağını belirtmeleri,
- c) Kamusal hizmetin planlanması ve yürütülmesinde zorunlu bir ihtiyaç olması,
- ç) Kamusal ve toplumsal yarar bakımından gereklilik arz etmesi,

durumlarının birlikte gerçekleşmesi halinde, belirtilen amaç ve yasal dayanak ile orantılı olarak veri talepleri asgari düzeyde karşılanabilir.

(2) Birinci fıkranın (a) ve (b) bentlerine uygun olmayan talepler Kurul gündemine alınmaz. Bu durumda, talebin ileildiği daire başkanlığınca; kullanma gerekçesi ile yasal dayanağının bildirilmesi gerektiği yönünde alıcı kurumlara veya diğer kişilere yazılı olarak bildirim yapılır.

(3) UAVT'ye ait toplu veriler, alıcı kurumlarla ve diğer kişilerle elektronik ortamda paylaşılır.

(4) Alıcı kurumlarla ve diğer kişilerle çevrimdışı veri paylaşımından önce taahhütname imzalanması zorunludur.

DÖRDÜNCÜ BÖLÜM

Verilerin Hazırlanması, Teslimi ve İmhası

Verilerin hazırlanması

MADDE 13 - (1) Kurul gündemine alınarak karara bağlanan talepler, Genel Müdürlükçe geliştirilen uygulamalar ve tanımlanmış yetkiler doğrultusunda ilgili daire başkanlıkları tarafından karşılanır.

Uygulamalar üzerinden temin edilmesi mümkün olmayan talepler ise Genel Müdürlük Bilgi İşlem Daire Başkanlığı tarafından karşılanır.

(2) Genel Müdürlük Bilgi İşlem Daire Başkanlığı, Kurul kararları çerçevesinde süreklilik arz eden toplu veri taleplerinin web servisler veya uygulama seviyesinde karşılanmasına yönelik gerekli tedbirleri alır.

(3) Diğer kişilerden gelen toplu eşleştirme taleplerinde yer alan veriler, veri tabanı kullanım performansını arttırmak ve daha etkin veriye ulaşabilmek amacıyla; Genel Müdürlük tarafından belirlenecek veri desenine göre oluşturulmuş kurum bilgi formatına uygun şekilde elektronik ortamda gönderilir. Genel Müdürlük gerektiğinde kurum bilgi formatında yer alan veri deseninde değişiklik yapabilir.

(4) Kurul tarafından olumlu olarak değerlendirilen, kişi bilgileri ile kimlik numarası eşleştirme taleplerinin, kâğıt ortamında olması veya belirtilen formata uygun olmaması durumunda, bu verilerin kurum bilgi formatına uygun şekilde Genel Müdürlüğe yeniden gönderilmesi talep edilir.

(5) Kurul tarafından kabul edilen talepler, veri tabanının verimliliğini ve performansını düşürmeyecek şekilde on iş günü içerisinde hazırlanır. Bu süre talep edilen verinin niteliğine bağlı olarak uzatılabilir.

(6) Çevrimdışı gönderilecek kişisel veriler; Genel Müdürlükçe belirlenen yöntem ve şifreleme tekniği ile iletilir.

Verilerin teslimi ve imhası

MADDE 14 - (1) Kişisel verilerin elektronik ortamda toplu olarak gönderilmesi veya tesliminde gizli evraka ilişkin usul ve esaslar uygulanır.

(2) Elektronik ortamda gönderilen veya teslim edilen kişisel veriler, işlenmesini gerektiren sebeplerin ortadan kalkması sonrasında, 28/10/2017 tarihli ve 30224 sayılı Resmî Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik hükümleri kapsamında alıcı kurum ve diğer kişiler tarafından silinir veya yok edilir.

BEŞİNCİ BÖLÜM

İstisnalar ve Alıcı Kurumlar ile Diğer Kişilerin Yükümlülükleri

İstisnalar

MADDE 15 - (1) Yüksek Mahkemeler, Sayıştay, Yüksek Seçim Kurulu, Mahkemeler, Savcılıklar ve 2/12/1999 tarihli ve 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında

Kanuna göre görevlendirilen ön incelemeçiler tarafından yürütülen; dava, soruşturma ve incelemelere ilişkin veri talepleri Kurula sunulmaksızın karşılanır.

(2) Görev ve yetkilerine uygun olmak ve görev onay yazılarının gönderilmesi şartıyla, 10/12/2003 tarihli ve 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu kapsamındaki kamu kurum ve kuruluşlarınca yürütülen soruşturma, inceleme, denetim ve teftişlerle ilgili veri talepleri Kurula sunulmaksızın karşılanır.

(3) 6698 sayılı Kanununun 28 inci maddesinin birinci fıkrasının (ç) bendi kapsamında talep edilen veriler Kurula sunulmaksızın karşılanabilir.

(4) Bu maddede yer alan çevrimdışı veri taleplerinde, 12 nci madde hükümleri uygulanmaz.

Alıcı kurumlar ve diğer kişilerin yükümlülükleri

MADDE 16 - (1) Alıcı kurumlar ve diğer kişiler çevrimiçi veya çevrimdışı olarak Genel Müdürlükten elde ettikleri verilerin; yetkisiz kişilerin eline geçmesinden veya yetkisiz kullanımından doğan her türlü hukuki ve cezai yaptırımdan ve mali zararın tazmininden sorumludur.

(2) Alıcı kurum ve diğer kişiler;

a) Kendi iş ve işlemlerine esas olmak üzere sadece ilgili kişilerin bilgilerini alabilirler ve aldıkları bilgileri mevzuatında sayılan görev ve sorumluluklarının yerine getirilmesinin dışında başka hiçbir amaçla kullanamazlar.

b) Elde ettikleri verileri üçüncü şahıslarla paylaşamaz ve yayınlamayamazlar.

c) Elde edilen verilerin hukuka aykırı olarak işlenmesi ile erişilmesini önlemek ve muhafazasını sağlamak amacıyla her türlü idari ve teknik tedbirleri alır. Özel nitelikli kişisel veriler için ise 6698 sayılı Kanununun 6 ncı maddesinin dördüncü fıkrası uyarınca Kişisel Verileri Koruma Kurulu tarafından belirlenen önlemler alınır.

(3) Edinilen verilerin iş ve işlemlerde kullanılmasının hukuki sonuçları, veriyi alan alıcı kurumun ve diğer kişilerin sorumluluğundadır.

(4) Edinilen veriler, ilgili mevzuatta yer alan özel hayatın gizliliğine ve kişisel verilerin korunması hükümlerine uygun olarak kullanılır.

(5) Elde edilen verilere erişim sağlayan tüm yetkililer bu maddede sayılan kurallara uymakla yükümlüdürler. Bu yükümlülük ilgililerin görevden ayrılmalarından sonra da devam eder.

(6) Kişisel verilerin korunması ile ilgili hükümleri ihlal edenler ile gizli verileri değiştiren veya bütünlüğünü bozanlar hakkında; 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu ve 6698 sayılı Kanunun ilgili hükümleri uygulanır.

ALTINCI BÖLÜM

Çeşitli ve Son Hükümler

Gizliliğin korunması

MADDE 17 - (1) Toplantılarda görüşülen ve gizlilik derecesi bulunan gündem maddelerinin korunması ve saklanması kapsamında; toplantıya katılım sağlayanlar, çalışmalar sırasında edindikleri sırları kanunen yetkili kılınan mercilerden başkasına açıklayamaz ve kendi yararlarına kullanamazlar. Kurul Başkanı ve üyeleri ile toplantılara katılan tüm kişiler bu gizlilik ilkesine uymakla yükümlüdür. Bu yükümlülük ilgili personelin görevinden ayrılmasından sonra da devam eder.

Düzenleme yetkisi

MADDE 18 - (1) Bu Yönetmeliğin uygulanması sırasında doğacak tereddütleri ve uygulamaya ilişkin aksaklıkları gidermeye, ilke ve standartları belirlemeye, uygulama birliğini sağlayacak gerekli düzenlemeleri yapmaya, bu hususta her türlü bilgi ve belgeyi istemeye ve bu Yönetmelikte yer almayan konularda ilgili mevzuat hükümleri çerçevesinde karar vermeye Bakanlık yetkilidir.

Yürürlük

MADDE 19 - (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 20 - (1) Bu Yönetmelik hükümlerini İçişleri Bakanı yürütür.

Kimlik Bildirme Kanununun Uygulanması ile İlgili Yönetmelik

Resmî Gazete Tarihi : 13.07.1974

Resmî Gazete Sayısı : 14944

KİMLİK BİLDİRME KANUNUNUN UYGULANMASI İLE İLGİLİ YÖNETMELİK

BÖLÜM I :

Genel Esaslar

Konu

Madde 1 - Bu Yönetmelik; 26/06/1973 tarihli ve 1774 sayılı Kimlik Bildirme Kanununun 12. maddesi gereğince, anılan kanunun bildirimlerle ilgili maddelerinin uygulanma kurallarının, belge, kart ve defterlerin biçim ve kapsamı alınıp, verilip ve saklanma yöntemlerinin belirli ve standart kayıtlara bağlanması amacı ile hazırlanmıştır.

Kapsam

Madde 2 - Özel veya resmi her türlü konaklama, dinlenme, bakım ve tedavi tesislerinin, ticaret ve sanat amacı güden bütün iş yerlerinin ve öğrenci yurtlarının sorumlu işleticileri ile bu gibi yerlerde çalışanlar ve barınanlar; resmi dairelerin yetkili amirleri; konutlarda sürekli veya geçici olarak kalanlar, çalışanlar veya konutlarını değiştirenler, bu Yönetmelik hükümlerine tabidir.

Tanımlamalar

Madde 3 - (Değişik:RG-17/6/2022-31869)

Bu Yönetmelikte geçen;

- Aile reisi: Eşlerden biri, eşlerin yerleşim yerinin ayrı olması halinde ayrı ayrı eşleri ya da aynı konutu paylaşan aile fertlerinden yaşça en büyük olanı,
- En yakın yetkili genel kolluk örgütü: Tesis, iş yeri veya konutun bulunduğu yerin sürekli olarak genel güvenliğini sağlayan polis veya jandarma karakollarını,
- Günübirlik kiralanan ev: Konut olarak kullanılmak ya da konut olarak kullanılmak üzere kiraya verilmek yerine fiilen işyeri gibi işletilmek suretiyle, otel, motel, pansiyon, kamping, apart otel ve

benzeri gibi temel veya yardımcı konaklama işletmesi ya da sosyal tesis statüsünde bulunmamakla beraber, saatlik, günlük, haftalık ve benzeri kısa süreli konaklama hizmeti sunulan, Ulusal Adres Veri Tabanında hizmetten faydalananlara ait kayıtlarda adresi yer almayan veya hizmetten faydalananlara ait herhangi bir abonelik kaydı bulunmayan yerleri,

ç) Sorumlu işletici: Bu Yönetmeliğin 6 ncı maddesinde sayılan tesislerle, her türlü ticaret ve sanat amacı güden iş yerlerini ve öğrenci yurtlarını sürekli veya geçici, sözleşmeli veya sözleşmesiz, ücretli veya ücretsiz olarak çalıştırmak ve yönetmek üzere, özel kuruluşlar için sahibi, kanuni temsilcisi veya kiracısı, resmi kuruluşlar için en büyük amir tarafından iş verilen veya atanan kişiyi veya bu kişi tayin edilmediği takdirde o yerin sahip, kanuni temsilci veya kiracısını,

d) Ticaret ve sanat amacı güden iş yeri: Her türlü ticarethane, tüccar yazıhanesi, ocak veya şantiye, fabrika ve imalathane ve atölye, depo, antrepo, ardiye, mağaza ve dükkan, banka ve banker dairesi, ikraz ve istikraz müessesesi, imtiyazlı ve imtiyazsız anonim, kooperatif, limited, komandit ve kolektif şirket gibi çalışma konusu mal veya para ticareti olan, dolayısı ile belirli yerinde para veya mal bulunduran veya hizmet arz eden ve amacı doğrultusunda maddi iş yapan özel veya kamu kuruluşlarını,

e) Yetkili amir: Kanuni yöntemine göre örgütü tarafından atanan ve resmi bina ve eklentilerinin korunması ile görevli ve sorumlu kişiyi,

ifade eder.

Süreler

Madde 4 - Bu Yönetmelikte sözü edilen:

a) 24 saat deyimi; işe başlamanın veya ayrılmanın vuku bulduğu saatten itibaren geçen 24 saatlik,

b) Üç gün deyimi; işe başlama veya geliş veya ayrılmanın vuku bulduğu saatten itibaren işlemeye başlayan 72 saatlik,

süreyi kapsar.

Kayıtlama

Madde 5 - Bu Yönetmelik hükümlerine göre kimlik bildirme belgelerini en yakın yetkili genel kolluk örgütüne vermekle yükümlü tutulanlar, kimliğini nüfus hüviyet cüzdanı veya diğer resmi geçerli belgelerle ispat edemeyen kimseleri, tesislerinde barındıramaz, konut ve iş yerinde çalıştıramaz.

BÖLÜM II :

Yükümlülükler

KISIM I :

İşyerleri Sorumlu İşleticilerinin ve Bu Yerlerde Çalışanların ve Barınanların Bildirilmesi

A - Sorumlu İşleticiler

İşe Başlama-Yükümlü

Madde 6 - Otel, motel, han, pansiyon, bekar odaları, (Ek ibare:RG-17/6/2022-31869) günübirlik kiralanan evler, kamp, kamping, tatil köyü, her türlü özel veya resmi konaklama yerleri (yatılı okulların pansiyonları, yetiştirme yurtları ve köy odaları dahil) ile özel sağlık müesseseleri, dinlenme ve huzur evleri ve dini ve hayır kurumlarının sosyal tesislerinde (Değişik ibare:RG-17/6/2022-31869) her an ulaşılacak bir sorumlu işletici bulunur.

Sorumlu işleticinin kimliği, o tesis açılmadan önce, sahip veya kanuni temsilci veya kiracısı tarafından iki örnek İŞLETİCİ KİMLİK BİLDİRME BELGESİ (form: 1) ne yazılır ve bu belgeler en yakın yetkili genel kolluk örgütüne verilir.

İşleticinin Değişmesi

Madde 7 - Sorumlu işleticinin değişmesi halinde, tesisin sahip, kanuni temsilci veya kiracısı tarafından, 24 saat içinde, yeni işleticiye ait kimlik bildirme belgesi, ayrılan işleticinin adı ve ayrılış tarihi de yazılarak yukarıdaki maddede belirtilen yöntemle göre en yakın yetkili genel kolluk örgütüne verilir.

B - Çalışanlar

Yükümlü

Madde 8 - Yönetmeliğin:

- a) 6. maddesi kapsamına giren tesislerle,
- b) 6. madde kapsamı dışındaki her çeşit ticaret ve sanat amacı güden iş yerlerinin sorumlu işleticileri tarafından; buralarda sürekli veya geçici olarak çalıştırılanların kimlikleri, iki örnek ÇALIŞANLARA AİT KİMLİK BİLDİRME BELGESİ (Form: 2) ne yazılır ve (a) bendi kapsamında olanların belgesi 24 saat, (b) bendi kapsamında olanların belgesi üç gün içinde en yakın yetkili genel kolluk örgütüne verilir.

Maddenin (b) bendindeki yerler köylerde ise belgeler anılan örgütle verilmeden önce muhtara onaylatılır.

(Ek fıkra:RG-17/6/2022-31869) Bu bildirimler sorumlu işleticiler tarafından, yukarıda belirtilen süre içerisinde genel kolluk kuvvetlerinin bilgisayar terminallerine bağlanılarak elektronik ortamda da yapılabilir. Bildirimlerin elektronik ortamda yapılması durumunda muhtar onayı aranmaz.

(Ek fıkra:RG-17/6/2022-31869) Köy ve mahalle muhtarları sorumluluk bölgelerinde bulunan işyerleri tarafından elektronik ortamda yapılan bildirimleri talepleri halinde genel kolluk birimlerinden temin eder.

(Ek fıkra:RG-17/6/2022-31869) Elektronik ortamda bildirimde bulunmak isteyen iş yerlerinin sahibi veya kanuni temsilcisi veya kiracısı tarafından sorumlu işleticilerinin kimlikleri örneğine uygun şekilde en yakın kolluk birimine bildirilir. Sorumlu işleticinin değişmesi halinde değişikliğin yirmi dört saat içerisinde aynı şekilde bildirilmesi zorunludur.

(Ek fıkra:RG-17/6/2022-31869) İşleticiler, kendilerine bu konuda verilen görev ve yükümlülükleri, kendi sorumlulukları altında yöneticilerine devredebilirler. Bu durumda işletici ve yönetici müştereken sorumlu olurlar.

Kimlik Kartı

Madde 9 - Yönetmeliğin 6. maddesinde yazılı tesislerde çalıştıklarından ötürü haklarında çalışanlara ait kimlik bildirme belgesi düzenlenenler adına sorumlu işletici tarafından; bu belgenin örgüte verildiği tarihten itibaren en geç üç gün içinde KONAKLAMA TESİSİ PERSONELİNE AİT KİMLİK KARTI (Form: 3) doldurulur ve kendilerine verilir.

Ayrılmak için başvuran kişinin kimlik kartının geri alınması zorunludur.

Kimlik kartları, ilgili konaklama tesisi tarafından örneğine ve boyutlarına uygun biçimde sağlanır.

C - Barınanlar

Yükümlü

Madde 10 - Yönetmeliğin 8. maddesine göre haklarında çalışanlara ait kimlik bildirme belgesi düzenlenen kişi aynı zamanda o iş yerinde barınıyorsa, bu belgenin ilgili hanesi işaretlenir.

İş yerlerinde çalışmadan, her ne suretle olursa olsun barınmalarına müsaade edilen kişilerin kimliği o yerin sorumlu işleticisi tarafından iki örnek BARINANLARA AİT KİMLİK BİLDİRME BELGESİ (Form: 4) ne yazılır ve bu belgeler üç gün içinde en yakın yetkili genel kolluk örgütüne verilir.

Bu iş yerleri köylerde ise belgeler anılan örgüte verilmeden önce muhtara onaylatılır.

(Ek fıkra:RG-17/6/2022-31869) Bildirimlerin elektronik ortamda yapılması halinde yukarıda yer alan hükümler uygulanmaz.

KISIM II :

Konutlarda Çalışanların ve Oturanların Bildirilmesi

A - Çalışanlar

Ortak hizmetlerde çalışanlar-Yükümlü

Madde 11 - (Mülga:RG-17/6/2022-31869)

Konut hizmetlerinde çalışanlar-Yükümlü

Madde 12 - (Mülga:RG-17/6/2022-31869)

Yükümlü

Madde 13 - (Mülga:RG-17/6/2022-31869)

Örnek verilmesi

Madde 14 - Kat mülkiyetine tabi taşınmaz mallarda oturmakta olan aile reisleri veya kişiler, düzenleyecekleri çalışanlara ait kimlik bildirme ve konutta kalanlara ait kimlik bildirme belgelerinin birer örneğini sorumlu yöneticiye verirler.

Misafirler - Yükümlü

Madde 15 - (Değişik madde:RG-25/1/1998-23241)

Şehir, kasaba ve köy sınırları içindeki konutlara misafir olarak gelen ve 30 günden fazla bir süre için kalacak kişilerin kimlikleri, bu konutlarda oturmakta olan ailelerin reisleri veya aralarında aile bağı olmaksızın kalan veya yalnız yaşayan kişiler tarafından form 6'daki Misafirlere Ait Kimlik Bildirme Belgesine yazılır ve iki nüsha olarak düzenlenen bu belgeler üç gün içinde en yakın yetkili genel kolluk örgütüne verilir.

Göçenler - Yükümlü

Madde 16 - (Değişik madde:RG-25/1/1998-23241)

Şehir, kasaba ve köy sınırları içindeki konutlarda otururken mevsimlik olarak yaylak ve kışlak gibi yerlere göçen veya yaylak ve kışlaklar arasında yer değiştiren aile veya kişilerin kimlikleri, aile reisleri ve kişiler tarafından form 6'daki Konutta Kalanlara Ait Kimlik Bildirme Belgesine yazılır ve iki nüsha olarak düzenlenecek bu belgeler üç gün içinde en yakın yetkili genel kolluk örgütüne verilir.

KISIM III :

Diğer Yerlerde Çalışanların ve Barınanların Bildirilmesi

Öğrenci yurtlarında bulunanlar-Yükümlü

Madde 17 - Öğrenci yurtları ve benzeri yerlerin sorumlu işleticileri tarafından ; buralarda:

a) Çalıştırılanların kimlikleri iki örnek ÇALIŞANLARA AİT KİMLİK BİLDİRME BELGESİ (Form.2) ne,

b) Kalan öğrencilerin veya diğer kişilerin kimlikleri iki örnek BARINANLARA AİT KİMLİK BİLDİRME BELGESİ (Form 4) ne,

yazılır ve bu belgeler üç gün içinde en yakın yetkili genel kolluk örgütüne verilir.

Köylerde düzenlenen belgeler, anılan örgüte verilmeden önce muhtara onaylatılır.

(Ek fıkra:RG-17/6/2022-31869) Bu bildirimler sorumlu işleticiler tarafından, yukarıda belirtilen süre içerisinde genel kolluk kuvvetlerinin bilgisayar terminallerine bağlanılarak elektronik ortamda da yapılabilir. Bildirimlerin elektronik ortamda yapılması durumunda muhtar onayı aranmaz.

(Ek fıkra:RG-17/6/2022-31869) Köy ve mahalle muhtarları sorumluluk bölgelerinde bulunan işyerleri tarafından elektronik ortamda yapılan bildirimleri talepleri halinde genel kolluk birimlerinden temin eder.

(Ek fıkra:RG-17/6/2022-31869) Elektronik ortamda bildirimde bulunmak isteyen iş yerlerinin sahibi veya kanuni temsilcisi veya kiracısı tarafından sorumlu işleticilerinin kimlikleri örneğine uygun şekilde en yakın kolluk birimine bildirilir. Sorumlu işleticinin değişmesi halinde değişikliğin yirmi dört saat içerisinde aynı şekilde bildirilmesi zorunludur.

(Ek fıkra:RG-17/6/2022-31869) İşleticiler, kendilerine bu konuda verilen görev ve yükümlülükleri, kendi sorumlulukları altında yöneticilerine devredebilirler. Bu durumda işletici ve yönetici müştereken sorumlu olurlar.

Resmi binalarda barınanlar-Yükümlü

Madde 18 - (Mülga:RG-17/6/2022-31869)

Özel durumu olan sabahçı kahveleri

Madde 19 - İskele, istasyon, hava meydanı, terminal, garaj, benzin istasyon ve benzeri kara, deniz hava ulaşım merkezleri ile fuar, panayır, sergi ve pazar kurulması gibi zorunluluk olan zaman ve yerlerdeki sabahçı kahvesi ve diğer benzeri tesislerin, o yerin bağlı bulunduğu kolluk örgütü ile

belediye veya köy idaresinin olumlu görüşü alındıktan sonra mahallin en büyük mülkiye amiri tarafından geçici veya sürekli olarak açık tutulması ve buralarda kişilerin kalması için verilen izin belgesinin, tesislerin görünür bir yerine asılması zorunludur. Buralarda kalanlar için bildirim yapılmaz.

KISIM IV :

Belgelerin Verilmesi ve Örneklerinin Saklanması

Sorumlu işleticinin işe başlaması ve ayrılması

Madde 20 - İşletici kimlik bildirme belgesi:

- a) İlk sorumlu işletici için doldurulduğunda önceki sorumlu işleticiye ait haneler boş bırakılarak,
- b) Ayrılanı izleyen sorumlu işleticiler için doldurulduğunda önceki sorumlu, işleticiye ait bilgiler her halde yazılarak, kolluk örgütüne verilir.

Örgütteki görevli, önceki sorumlu işletici yoksa hemen, varsa ona ait kimlik bildirme belgesinin bulup isim karşılaştırması yaptıktan sonra yeni belgenin alınış hanelerini bizzat doldurarak imzalar, birinci örneği saklar, öteki örneği yükümlüye geri verir ve önceki sorumlu işleticiye ait belgeyi imha eder.

Belge örnekleri ayrılış ve başlayış tarihleri birbirini izlemek kaydı ile tesisin çalıştığı süre boyunca yükümlüler tarafından tesiste saklanır.

İşe başlaması veya Öteki kişilerin gelişi

Madde 21 - İşletici kimlik bildirme belgesi dışındaki bütün belgelerin tabloları her iki örnekte doldurup imzalandıktan sonra ve zımbalı kısmın örneklerdeki ayrılış tarihi ve imza haneleri boş bırakılarak kolluk örgütüne verilir.

Örgütteki görevli, aldığı belge örneklerinin benzerliğini saptadıktan sonra, belgenin alınış hanelerini bizzat doldurarak imzalar, birinci örneği saklar, öteki örneği yükümlüye geri verir.

Öteki kişilerin ayrılması veya konutun değiştirilmesi

Madde 22 - Adına belge düzenlenmiş olan çalışan veya barınan kişinin o yerden ilişiğinin kesilerek ayrılması veya konutun değiştirilmesi halinde yükümlü, belgelerin verilmesindeki sürelerle uymak kaydı ile; kendisindeki örnekten ayırdığı zımbalı kısma ayrılış tarihini yazıp imzalayarak kolluk örgütüne verir.

Örgütteki görevli zımbalı kısmın ilgili olduğu belge örneğini bulup karşılaştırır, bunun altındaki zımbalı kısmı ayırarak, ayrılış tarihini de yazdıktan sonra imzalar ve yükümlüye verir, ondan aldığı zımbalı kısmı kendisindeki belge örneği ile birlikte imha eder.

Yükümlü, kendisinde kalan belge örneğini kolluk örgütünden aldığı zımbalı kısım ile birlikte üç yıl süre ile saklar.

Konutta kalanlara ait kimlik bildirme belgesinin örneği ile kolluk örgütünden alınan zımbalı kısmın saklanması zorunlu değildir.

Hakkında belge verilmiş bulunan misafirlerin ayrılışı kolluk örgütüne bildirilmez.

KISIM V :

Konaklama Tesislerindeki Geçici Oturmaların Saptanması

Yükümlü

Madde 23 - (Değişik:RG-21/01/1975-15125) Yönetmeliğin 6.maddesinde sayılan yerlerin sorumlu işleticileri tarafından; buralarda ücretli veya ücretsiz, gündüz veya gece yatacak yer gösterilen yerli veya yabancı herkesin kimliği ile geliş ve ayrılış tarihleri, KONAKLAMA YERİ KAYIT DEFTERİ (Form:7) ne günü gününe geçirilir.

Bu yerlerde kalacak kişilerin, kendilerine verilecek kopyalı bir örnek KONAKLAMA BELGESİ (form:8) ni doldurarak imzalamaları ve sorumlu işleticiye vermeleri şarttır.

Konaklama belgesindeki bilgiler, kişinin kimliğini belirten geçerli resmi belge ile karşılaştırıldıktan sonra, konaklama yeri kayıt defterine aktarılır.

Konaklama yeri kayıt defteri ve konaklama belgesinin sağlanması ve saklanması

Madde 24 - Konaklama yeri kayıt defteri ve konaklama belgesi, örneğine ve boyutlarına göre ilgili konaklama tesisi tarafından sağlanır.

Defter yıllık olarak tutulur, kapağına tesis adı ve yılı yazılır. Kullanılmağa başlanılmadan önce, sonu en yakın yetkili genel kolluk örgütüne sahife sayısı belirtilerek onaylatılır.

Defter yüz sahifeden aşağı olamaz. Yılı içinde birden fazla defter kullanılması halinde bunların kapağına birbirini izleyen sıra numarası verilir. Şu kadar ki, gelen konuk sayısını az olduğu tesislerde tek defter kullanılması ile yetinilebilir. Bu halde, yeni yılın kayıtlarına boş bir sahife bırakıldıktan sonra başlanır.

Yılın ilk gününde bir önceki yıldan kayıtları devam eden kimlikleri, o gün gelenlerden önce yeni deftere veya sahifeye bütünü ile aktarılır.

Bir yıla ait konaklama belgeleri, düzenlendiği yılı izleyen takvim yılından başlayarak bir yıl; konaklama yeri kayıt defterleri, dolduğu yılı izleyen takvim yılından başlayarak beş yıl süre ile, sorumlu işleticinin sorumluluğu altında tesiste saklanır.

Saklama süreleri içinde sorumlu işleticisi değişen tesisin belgeleri ve defterleri yeni sorumlu işleticiye; kesin olarak kapanan tesisin belgeleri ve defterleri en yakın yetkili genel kolluk örgütüne hemen verilir. Bu halde, saklama görevi, geri kalan süreler için yeni sorumlu işletici veya örgüt tarafından yerine getirilir.

Belge ve defterden yararlanma olanağı

Madde 25 - Yetkili resmi örgütler dışında, mahkeme kararı olmadıkça, hiç kimsenin konaklama belgelerinden ve konaklama yeri kayıt defterlerinden yararlanmasına müsaade edilemez.

BÖLÜM III :

Uygulamada Yapılacak Çalışmalar ve İşlemler

Belgelerin saklanma yeri ve yöntemi

Madde 26 - Belgeler, verildiği en yakın genel kolluk örgütünde, karakol bölge krokisi ve binalar cetveli esas alınarak; önce mahalle ve semt (varsa bölge) sonra cadde ve sokak ve bina numarası üzerinden sınıflandırılmış ve üstünde bu bilgiler bulunan gözlerde kilit altında saklanır.

Aynı binada bulunan yükümlülerce birden fazla türden belge verilmesi halinde her belge türü form sıra numarasına göre; misafirlere ait kimlik bildirme belgesi, onu düzenleyen tarafından verilmiş konutta kalanlara ait kimlik bildirme belgesine bağlanarak saklanır.

Karakol amirleri, yukarıdaki yöntem esas olmak kaydı ile belgeleri daha kolay izlenmesini sağlayacak öteki yolları uygulayabilirler.

Yetkili resmi örgütler dışında, mahkeme kararı olmadıkça, hiç kimsenin belgelerden yararlanmasına müsaade edilemez.

Görevliler

Madde 27 - Belgeleri teslim alınması ve ayrılması, sıralanması ve saklanması görevin aynı personele gördürülmesi esastır.

Yapıların izlenmesi

Madde 28 - Her karakol üç ayda bir kez ve gerektiğinde sürekli olarak, bölgesini tarar ve bölge krokisinde veya binalar cetvelinde yer almayan yeni veya yıkılan yapıları ve her türlü ilave ve değişiklikleri saptar, bunları kroki veya cetveline işler veya düşümünü sağlar.

Belediyeler, mahallin en büyük mülki amirince istenilmesi halinde düzenledikleri nümerotaj cetvelinin birer örneğini vermekle yükümlüdürler.

Belgelerin sağlanma yeri

Madde 29 - (Değişik:RG-6/12/1996-22839) Valiliklerce, İlin yıllık belge ihtiyacına göre, bu Yönetmelikte sözü edilen belgelerin özel kuruluşlarca basılarak ilgililerin taleplerine sunulması için gerekli tedbirler alınır.

Özel kuruluşlarca basılan söz konusu belgeler muhtarlıklar ile herkesin kolaylıkla ulaşabileceği diğer yerlerde arza sunulur ve ilgililerce bedeli mukabili temin edilen bu belgeler doldurularak yetkili mercilere teslim edilir.

İçişleri Bakanlığının yetkisi

Madde 30 - (Değişik:RG-17/6/2022-31869)

İçişleri Bakanlığı bu Yönetmeliğin verilmesini öngördüğü belgelerin örnek sayısında değişiklik yapmaya yetkilidir.

Madde 31 - (Mülga madde:RG-25/01/1998-23241)

İstatistik bilgi istenmesi

Madde 32 - Devlet İstatistik Enstitüsü; Yönetmeliğin 6.maddesinde yazılı tesislerin sayılarını, unvan ve adreslerini, türlerini sınıflarını, oda ve yatak sayılarını belirten listeleri Valiliklerden sağlar. Bu tesislerin tamamı veya bir kısmından, öngöreceği yonteme ve formlara göre, belli süreler içinde istatistik bilgiler istemeye yetkilidir.

Dağıtım-Görevlendirilecek kişiler

Madde 33 - Belgelerin boş olarak dağıtımı ve doldurulmuş olarak geri alınması konusunda, genel kolluk örgütleri, köy ve mahalle muhtarlarını görevlendirebilirler.

Ek Madde 1 - (Değişik:RG-17/6/2022-31869)

1774 sayılı Kanunun 2 nci maddesinde sayılan özel veya resmi her türlü konaklama tesisleri ve işletmeler tüm kayıtlarını bilgisayarda günü gününe tutmak, genel kolluk kuvvetlerinin bilgisayar

terminallerine bağlanarak mevcut bilgi, belge ve kayıtları genel kolluk kuvvetlerine anlık olarak bildirmek zorundadırlar.

Bildirilen kayıtlar genel kolluk kuvvetlerine ait sistemde beş yıl süre ile muhafaza edilir. Bu süreyi dolduran kayıtlar kaydedilen sistemden otomatik olarak silinir.

Bu veriler üzerinden yapılan tüm işlemler kayıt altına alınır.

Ek Madde 2 - (Ek:RG-10/6/2015-29382) Araç kiralama şirketlerinin sorumlu işleticileri ve yöneticileri, kiralanan araç bilgileri ile aracı kiralayanların kimlik bilgileri ve kira sözleşmesi kayıtlarını usulüne uygun şekilde günü gününe tutmak ve bu kapsamda mevcut bilgi, belge ve kayıtları genel kolluk kuvvetlerinin her an incelemelerine hazır bulundurmak zorundadırlar. Ancak araç kiralayanın kamu kurum veya kuruluşu olması halinde sadece kamu kurum veya kuruluşuyla yapılan sözleşme ile araç bilgileri sisteme kaydedilir.

Birinci fıkrada belirtilen veriler 5 yıl süreyle muhafaza edilir. Sistemdeki kayıtlar 5 yıl sonunda sistemden otomatik olarak silinir. (Ek cümle:RG-17/6/2022-31869) Bu veriler üzerinden yapılan tüm işlemler kayıt altına alınır.

Ek Madde 3 - (Ek:RG-10/6/2015-29382) Bu Yönetmeliğe tabi gerçek kişiler ile özel hukuk tüzel kişilerinin; defter tutma, bilgi, belge ve kayıtları arşivleme yükümlülükleri ile bunları muhafaza etme sürelerine ilişkin olarak 213 sayılı Vergi Usul Kanunu, 6102 sayılı Türk Ticaret Kanunu ve diğer mevzuatta yer alan hükümler saklıdır.

Ek Madde 4- (Ek:RG-17/6/2022-31869)

Bu Yönetmeliğin uygulanmasında, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununun ilgili hükümleri kapsamında verilerin uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirler alınır.

Geçici Madde 1 - (Ek:RG-10/6/2015-29382)

Araç kiralama şirketleri tüm kayıtlarını İçişleri Bakanlığının tespit edeceği bir bilgisayar programında tutmak ve bilgisayar terminallerini genel kolluk kuvvetlerinin 1774 sayılı Kanunun ek 1 inci maddesine göre kurulan bilgisayar terminallerine bağlamak zorundadırlar. 4/10/2015 tarihine kadar bu şartı yerine getirmeyen işletmelere mülki idare amirlerince on bin Türk lirası para cezası verilir. Bu fiilin tekrarı halinde işletme ruhsatları iptal edilir.

Yürürlük tarihi

Madde 34 - Bu Yönetmelik yayımı tarihinden altı ay sonra yürürlüğe girer.

Yürütme yetkisi

Madde 35 - Bu Yönetmelik hükümlerini Adalet, İçişleri, Turizm ve Tanıtma ve Devlet İstatistik Enstitüsü işlerine Bakan Devlet Bakanları yürütür.

FORMLAR VE AÇIKLAMALAR

- 1 - (Form: 1) İşletici kimlik bildirme belgesi (Madde 6) (Değişik:RG-17/6/2022-31869)
- 2 - (Form : 2) Çalışanlara ait kimlik bildirme belgesi (Madde 8, 11, 12, 17/a) (Değişik:RG-17/6/2022-31869)
- 3 - (Form: 3) Konaklama tesisleri personeline ait kimlik kartı Açıklamasız. (Madde 9)
- 4 - (Form: 4) Barınanlara ait kimlik bildirme belgesi (Madde 10, 17/b, 18)
- 5 - (Form : 5) Konutta kalanlara ait kimlik bildirme belgesi (Madde 13, 16) (Mülga:RG-17/6/2022-31869)
- 6 - (Form: 6) Misafirlere ait kimlik bildirme belgesi (Madde 15)
- 7 - (Form : 7) Konaklama yeri kayıt defteri (Madde 23, Z4)
- 8 - (Form: 8) Konaklama belgesi (Madde 23, 24)

E-Devlet Hizmetlerinin Yürütülmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik

Resmî Gazete Tarihi : 03.09.2016

Resmî Gazete Sayısı : 29820

E-DEVLET HİZMETLERİNİN YÜRÜTÜLMESİNE İLİŞKİN USUL VE ESASLAR HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı; bilgi toplumu politika, hedef ve stratejileri çerçevesinde, e-Devlet hizmetlerinin kapsamı ve yürütülmesine ilişkin usul ve esasları belirlemek, bu hizmetlere ilişkin eylem planları yapmak, koordinasyon ve izleme faaliyetlerini yürütmektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanunu eki (I), (II), (III) ve (IV) sayılı cetvellerde yer alan genel yönetim kapsamındaki Bakanlıklar, Bakanlıklara bağlı, ilgili ve ilişkili kamu idarelerini, üniversiteleri ve sosyal güvenlik kurumları ile mahalli idareler kapsamında görev, yetki ve sorumlulukları 3/7/2005 tarihli ve 5393 sayılı Belediye Kanunu, 10/7/2004 tarihli ve 5216 sayılı Büyükşehir Belediyesi Kanunu ve 22/2/2005 tarihli ve 5302 sayılı İl Özel İdaresi Kanunu ile belirlenmiş kamu tüzel kişiliği olan belediyeler ve il özel idarelerini ve bunların kurdukları kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları ve bunların üst kuruluşlarını, hissesinin yüzde elliden fazlası kamuya ait olan şirketler ve özel kanunlarla kurulan diğer kuruluşları kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 26/9/2011 tarihli ve 655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 2 nci maddesinin birinci fıkrasının (f) bendi ve 13 üncü maddesinin birinci fıkrasının (ç) bendi hükümlerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Yönetmelikte yer alan;

- a) (Değişik:RG-15/1/2019-30656 Mükerrer) Bakanlık: Ulaştırma ve Altyapı Bakanlığını,
- b) Birlikte Çalışabilirlik Esasları Rehberi: 28/2/2009 tarihli ve 27155 sayılı Resmî Gazete’de yayımlanan 2009/4 sayılı Başbakanlık Genelgesinde belirtilen rehberi,
- c) e-Devlet hizmeti: Hizmet süreçlerinin vatandaş odaklı olarak yeniden yapılandırılmasını da içerecek şekilde, kurumlar arası veri paylaşımı esasına dayalı olarak yürütülmesi için kurumlar tarafından, hızlı, güvenli, etkili, verimli, şeffaf ve hesap verebilir, temel hak ve özgürlüklere riayet edilerek ve mahremiyet gözetilecek şekilde elektronik ortama aktarılan her bir kamu hizmetini,
- ç) e-Devlet Kapısı: e-Devlet hizmetlerinin son kullanıcıya farklı erişim kanallarından tek noktadan bütünleşik olarak sunulduğu ortak elektronik platformu,
- d) e-Devlet Kapısı İşletmecisi: 24/3/2006 tarihli ve 2006/10316 sayılı Bakanlar Kurulu Kararı ve 10/8/2006 tarihli ve 2006/22 sayılı Başbakanlık Genelgesi ile e-Devlet Kapısının kurulması ve işletilmesiyle yetkilendirilmiş, 4/2/1924 tarihli ve 406 sayılı Telgraf ve Telefon Kanununun Ek 33 üncü maddesi ile kurulan Türksat Uydu Haberleşme Kablo TV ve İşletme Anonim Şirketini,
- e) e-Devlet projeleri: Kamu hizmetlerinin bilgi ve iletişim teknolojileri kullanılarak e-Devlet hizmetlerine dönüştürülmesi amacıyla yürütülen projeleri,
- f) Güvenli Elektronik İmza: 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununun 4 üncü maddesinde tanımlanan elektronik imzayı,
- g) KAYSİS: Devlet teşkilatında yer alan kurum ve kuruluşların organizasyon yapıları, yapı içerisindeki birimlerin sundukları hizmetler, süreç entegrasyonları, kullanılan belgeler ve resmi yazışmalar ile bunlara ilişkin yasal dayanaklar gibi kamu yönetimine ilişkin temel verilerin tespit edilerek sadeleştirme ve standartlaştırma çalışmalarının yapıldığı ve elektronik ortamda tanımlandığı, (Değişik ibare:RG-15/1/2019-30656 Mükerrer) Cumhurbaşkanlığı tarafından yürütülen Elektronik Kamu Bilgi Yönetim Sistemini,
- ğ) Kimlik doğrulama işlemi: e-Devlet hizmetleri kullanımı için kullanıcıların e-Devlet Şifresi, Güvenli Elektronik İmza veya Elektronik TC Kimlik Kartı gibi yollarla kimliklerinin doğrulanmasını,
- h) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
- ı) Kullanıcı: e-Devlet hizmetlerinden yararlanan gerçek veya tüzel kişiyi,
- i) Olgunluk seviyesi yüksek e-Devlet hizmeti: Sağladığı toplam maliyet ve zaman tasarrufu ile bürokratik süreçlerde önemli sadeleşme sağlayan, ileri teknoloji gerektiren işlemlerin sunulabildiği,

servis bazlı entegrasyonun kurum içinde tamamen sağlandığı ve kurum dışı entegrasyonu mevcut bulunan e-Devlet hizmetini,

j) Siber güvenlik: Bilgi ve iletişim teknolojileri vasıtasıyla sağlanan hizmet, işlem ve veri ile bunların sunumunda yer alan sistemlerin gizlilik, bütünlük ve erişilebilirlik açısından güvenliğini,

k) Veri tabanı: Kamu hizmetlerinin sunulmasına esas teşkil eden kamu kurum ve kuruluşlarına ait verilerin bulunduğu elektronik sistemleri,

l) Veri yetkilisi: Kamu hizmetlerinin sunulmasına esas teşkil eden veri tabanlarının kurulmasından, yönetilmesinden, verilerin bu veri tabanlarına kaydedilmesinden, güvenliğinden, işlenmesinden ve paylaşılmasından sorumlu olan gerçek veya tüzel kişiyi,

ifade eder.

İKİNCİ BÖLÜM

E-Devlet Hizmetlerinin Sunulması

İlkeler

MADDE 5 - (1) Bu Yönetmelik kapsamındaki kamu kurum ve kuruluşları e-Devlet projelerinin hayata geçirilmesi ve e-Devlet hizmetlerinin sunumuna ilişkin faaliyetlerini aşağıdaki ilkeler dâhilinde yürütür;

a) Kullanıcı odaklı ve erişilebilir olması,

b) Zaman ve maliyet tasarrufu sağlanması,

c) Siber güvenliğin sağlanması,

ç) Kesintisiz ve kaliteli hizmet sağlanması,

d) Bilgi ve iletişim teknolojilerinin kullanımının yaygınlaştırılması,

e) e-Devlet altyapısının oluşturulması, kurumlar arası bilgi paylaşımının ve birlikte çalışabilirliğin sağlanması amacıyla Birlikte Çalışabilirlik Esasları Rehberine riayet edilmesi,

f) Kişisel verilerin korunması ve mahremiyet prensibinin de dikkate alınarak, temel hak ve özgürlüklere riayet edilmesi,

g) Bilişim sistemlerinin güvenliğine yönelik ulusal ve uluslararası standartlara uyulması,

ğ) Elektronik ortamda kamu kurum ve kuruluşlarının paylaşımına açık olan verilerin ayrıca kişilerden talep edilmemesi, yalnızca sunulan hizmetin gerektirdiği verilerin istenmesi,

- h) Kullanıcı ihtiyaçlarına uygun olarak, mobil cihazlar da dâhil olmak üzere güncel teknolojinin gerektirdiği mümkün olan bütün elektronik erişim ortamlarından hizmet sunulabilmesinin sağlanması,
- i) Kamu kurum ve kuruluşlarınca oluşturulan ve işlenen elektronik ortamdaki verilerin, kaynakların verimliliğinin sağlanması ve mükerrerliğin önlenmesi ilkeleri çerçevesinde katma değerli hizmetler yaratmak üzere mer'î mevzuattan kaynaklanan istisnalar saklı kalmak kaydıyla paylaşılması,
- i) Gereksinimlerin karşılanmasında yerli ürün ve hizmet kullanımının teşvik edilmesi,
- j) Açık standarda dayalı ürün/hizmetlerin tercih edilmesi, mükerrer ve birbiriyle örtüşen yatırımlardan kaçınılması,
- k) Proje ve uygulamalarda, herhangi bir teknoloji tercihini öne çıkartmayan ve teknolojik bağımlılık yaratmayan çözümlerin benimsenmesi,
- l) Ödeme gerektiren hizmetlere ilişkin tahsilatların elektronik ortamdan alınabilmesi.

Bakanlığın görev ve sorumlulukları

MADDE 6 - (1) e-Devlet hizmetlerinin kapsamı ve yürütülmesinde Bakanlığın görev ve sorumlulukları şunlardır:

- a) Bilgi toplumu politika, hedef ve stratejileri çerçevesinde; e-Devlet hizmetlerinin kapsamı ve yürütülmesine ilişkin usul ve esasları belirler.
- b) Kamu kurum ve kuruluşları ile yapacağı müşterek çalışmalar neticesinde e-Devlet hizmetlerinin kapsamı ve yürütülmesine ilişkin ilke, politika ve stratejileri oluşturup, e-Devlet Strateji ve Eylem Planını hazırlar.
- c) e-Devlet hizmetleri kapsamında koordinasyon ve izleme faaliyetlerini yürütür. Kullanıcı Odaklı e-Devlet Hizmet Sunumu Rehberi, Birlikte Çalışabilirlik Esasları Rehberi, Kamu İnternet Siteleri Rehberi gibi rehber, kılavuz ve referans dokümanların oluşturulması ve/veya güncellenmesine ilişkin çalışmalar yapar.
- ç) e-Devlet alanında oluşturulan strateji ve eylem planı ile rehber, kılavuz ve benzeri çalışmalara uyumun sağlanması ve mükerrer yatırımların önlenmesi amacıyla, kamu kurum ve kuruluşlarınca yatırım programına alınması teklif edilen e-Devlet projeleri hakkında görüş verir.
- d) Bakanlık, mer'î mevzuattan kaynaklanan istisnalar saklı kalmak kaydıyla, kamu kurum ve kuruluşları ile gerçek veya tüzel kişilerden e-Devlet hizmetleri ile ilgili gerekli gördüğü bilgileri talep eder.

- e) Kamu kurum ve kuruluşlarının sunduğu ve/veya sunacağı elektronik ortamdaki hizmetlerin tespit edilmesine yönelik çalışmalar yapar.
- f) Kurumlar arası işbirliğini desteklemek ve doğrudan bir kamu kurumu tarafından yerine getirilemeyecek nitelikteki ortak proje ve uygulamaların hayata geçirilmesini kurumlar arası koordinasyonu sağlar.
- g) Bakanlık, KAYSİS'te kurum ve kuruluşlar tarafından tanımlanan hizmetler, hizmetler arasındaki bağlantıları gösteren süreç entegrasyonları, süreçlerdeki belgeler, hizmetlerin tamamlanma süreleri, yıllık işlem sayıları ve bunlara ilişkin yasal dayanaklar gibi verileri de kullanarak e-Devlet çalışmalarının yürütülmesinde kurum ve kuruluşlarıyla işbirliği yapar.
- ğ) Kurumlardan alınacak bilgiler doğrultusunda hangi hizmetlerin elektronik ortamda e-Devlet Kapısı üzerinden sunulması gerektiği ve bunun için hangi faaliyetlerin yürütüleceği hususunda ilgili kurum ve kuruluşlarla işbirliği yapar.
- h) Kamu kurum ve kuruluşlarının internet siteleri üzerinden sunduğu ve sunacağı uygulamaların e-Devlet Kapısına entegrasyonu için işbirliği yapar.
- ı) e-Devlet hizmetleri kapsamında, ulusal siber güvenliğin ve kişisel verilerin korunması konusunda farkındalık sağlamak ve bilişim sistemlerinde gerekli önlemlerin alınması için kamu kurum ve kuruluşlarıyla işbirliği yapar.
- i) e-Dönüşüm ve e-Devlet istatistiklerini hazırlayan uluslararası kuruluşların veri taleplerini değerlendirir.
- j) Bakanlık, kamu kurumları, üniversiteler ve sivil toplum kuruluşları ve özel sektör ile işbirliği halinde eğitim programları, ulusal ve uluslararası etkinlikler düzenleyebilir.

Kamu kurum ve kuruluşlarının görev ve sorumlulukları

MADDE 7 - (1) e-Devlet hizmetlerinin kapsamı ve yürütülmesinde kamu kurum ve kuruluşlarının görev ve sorumlulukları şunlardır:

- a) Kamu kurum ve kuruluşları, yürüttükleri e-Devlet projeleri veya sundukları e-Devlet hizmetleri kapsamında üretmiş oldukları verilerin elektronik ortama taşınmasından, doğruluğundan, güncelliğinden, veri bütünlüğü ve güvenliğinin sağlanmasından ve saklanmasından sorumludur.
- b) Kamu kurum ve kuruluşları, ulusal stratejiler ve planlar ile mevcut kurumsal stratejik planlarıyla uyumlu, kurumun e-Devlet hizmetleri sunumu amacıyla yapacakları yatırım, teknoloji tercihleri,

kurumsal kapasite, tasarruf planları, fayda-maliyet, iş planı gibi unsurları kapsayacak bilişim stratejilerini hazırlar.

c) Kamu kurum ve kuruluşları, e-Devlet projeleri ile e-Devlet hizmetlerinin planlanması, geliştirilmesi, sunumu, yürütülmesi konularında Bakanlık ile gerekli koordinasyon ve işbirliğini sağlamak amacıyla kurum içi e-dönüşüm yönetim yapısını kurar.

ç) Mer'î mevzuattan kaynaklanan istisnalar saklı kalmak kaydıyla, e-Devlet hizmetlerinin yürütülmesi kapsamında ilgili veriler, kamu kurum ve kuruluşları arasında yapılan protokoller çerçevesinde elektronik ortamda paylaşılır ve ilgili kullanıcılara sunulur.

d) Kamu kurum ve kuruluşları, e-Devlet hizmetlerini kullanım kolaylığı ve kullanıcı memnuniyetini sağlayacak şekilde; ulusal ve uluslararası standartlara uygun olarak, işlevsel, güvenli, talebe cevap verebilir ve kesintisiz şekilde sunar.

e) Kamu kurum ve kuruluşları e-Devlet hizmetlerinin izlenip ölçülmesi amacıyla kullanıcılardan gelecek talep, öneri ve şikâyetlerin değerlendirilmesine yönelik mekanizmalar oluşturur.

f) Kamu kurum ve kuruluşları, resmi internet sayfaları üzerinden sundukları e-Devlet hizmetlerinde vatandaşların memnuniyet dereceleri ve nedenlerinin izlenmesi amacıyla KAYSİS'te yer alan Kamu Memnuniyet Anketi uygulamasını (Değişik ibare:RG-15/1/2019-30656 Mükerrer) Cumhurbaşkanlığı tarafından sunulacak servisleri kullanarak kendi uygulamalarına entegre eder.

g) Kamu kurum ve kuruluşları kendilerine ait bilgi sistemleri üzerinde siber güvenlik önlemlerini alır, kullanıma ilişkin erişim kayıtlarını tutar ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlar.

ğ) e-Devlet Kapısı üzerinden verilecek her bir hizmette, gerekli olan veri ya da uygulama entegrasyonu için, veri veya uygulama sahibi kurumlar, e-Devlet Kapısı İşletmecisi ile Bakanlık adına bir veri paylaşım protokolü imzalar.

h) Kamu kurum ve kuruluşları e-Devlet uygulamalarının internet üzerinden sunumunda yetkisiz erişimi engelleyecek önlemleri alır.

ı) Kamu kurum ve kuruluşları, e-Devlet hizmetlerinin sunumunda mobil teknolojilerden ve sosyal medya imkânlarından etkin biçimde yararlanır.

i) Kamu kurum ve kuruluşları sundukları ve/veya sunacakları hizmetler içerisinde geniş kitlelere hitap eden ve olgunluk seviyesi yüksek olan e-Devlet hizmetlerini yalnızca e-Devlet Kapısı üzerinden

sunulacak şekilde projelendirip takvime bağlar ve projenin tamamlanmasına müteakip e-Devlet Kapısına entegrasyonunu sağlamak için gerekli çalışmaları başlatır.

j) Kamu kurum ve kuruluşları KAYSİS'te yer alan Kamu Bilişim Sistemleri Envanterinde bilgi sistemlerine ilişkin envanter kayıtlarını oluşturur ve sürekli güncel tutar.

k) Kamu kurum ve kuruluşları geliştirecekleri e-Devlet projelerinde e-Devlet Kapısı İşletmecisi tarafından hazırlanacak Web Servis Standartları Kılavuzunun son sürümünü esas alır.

l) Kamu kurum ve kuruluşları sundukları hizmetler veya diğer işlemleri kapsamında gerçek veya tüzel kişileri doğrudan etkileyebilecek durumlar için e-Devlet Kapısı üzerinden resmi tebligat kabul edilmeyecek bildirimlerin yapılmasını sağlayacak alt yapının geliştirilmesine yönelik hazırlık çalışmalarını yapar.

m) Kamu kurum ve kuruluşları herhangi bir felaket anında sistemlerin kesintiye uğramaması için gerekli tedbirleri alır.

n) Kamu kurum ve kuruluşları, e-Devlet Kapısı üzerinden kredi kartı, banka kartı, havale, EFT, mobil ödeme gibi yöntemlerle de alacaklarının tahsilatını yapabilecekleri alt yapıyı kurar.

E-Devlet Kapısı İşletmecisinin görev ve sorumlulukları

MADDE 8 - (1) e-Devlet hizmetlerinin kapsamı ve yürütülmesinde e-Devlet Kapısı İşletmecisinin görev ve sorumlulukları şunlardır:

a) e-Devlet Kapısı İşletmecisi, bireysel ve kurumsal tüm kullanıcıların kamu hizmetlerine elektronik ortamdan güvenli ve etkin bir şekilde erişebilecekleri, e-Devlet hizmetlerinin sunumunda tek adres olabilecek özelliklere sahip ortak bir platform kurar ve işletir.

b) e-Devlet hizmetlerinin e-Devlet Kapısından sunumunu, kullanım kolaylığı ve kullanıcı memnuniyetini sağlayacak şekilde, işlevsel, güvenli ve kesintisiz şekilde yapar.

c) e-Devlet Kapısı üzerinden verilecek her bir hizmette, gerekli olan veri ya da uygulama entegrasyonu için, veri yetkilisi kurumlar ile işbirliği yapar.

ç) e-Devlet hizmetlerinin oluşturulması, sunulması, yürütülmesi ve geliştirilmesine ilişkin, kullanıcıdan ve e-Devlet hizmetini sağlayan kamu kurum ve kuruluşlarından görüş, öneri ya da geri bildirim alarak, varsa önerilerini Bakanlığa sunar.

d) e-Devlet Kapısı üzerinden sunulan kamu hizmetlerinin engelli kişiler tarafından da erişilebilir olması için gerekli çalışmaları yapar.

- e) e-Devlet Kapısı üzerinden verilecek her bir hizmette, gerekli olan veri ya da uygulama entegrasyonu için, e-Devlet Kapısı İşletmecisi veri yetkilisi ile bir veri paylaşım protokolü imzalar.
- f) e-Devlet Kapısı İşletmecisi, kamu kurum ve kuruluşlarının e-Devlet hizmetlerinin e-Devlet Kapısına entegrasyonu, e-Devlet Kapısının işletilmesi, kapı ile ilgili geliştirme, iletişim altyapısı, tanıtım, güvenlik, donanım, yazılım, erişim imkânlarının yaygınlaştırılması gibi e-Devlet Kapısı hizmetlerinin gerektirdiği faaliyetlerin yürütülmesinden görevli ve sorumludur.
- g) Kullanıcıların e-Devlet süreçlerine etkin katılımını sağlayacak, hizmet sunumu ve kalitesine ilişkin görüşlerini doğrudan iletebilecekleri ve aynı zamanda kullanıcı memnuniyetini ölçen uygulamalar geliştirir.
- ğ) Hizmet Entegrasyonunda Web Servis Standartları Kılavuzunu hazırlar ve güncel tutar.

ÜÇÜNCÜ BÖLÜM

E-Devlet Hizmetlerinin İzleme ve Değerlendirilmesi

İzleme ve raporlama faaliyetleri

MADDE 9 - (1) e-Devlet proje ve faaliyetlerinin mali ve fiziki gerçekleştirmelerini, performanslarını, risklerini, sorun ve ihtiyaçlarını zamanında tespit etmek ve gerekli tedbirleri almak amacıyla Bakanlık tarafından izleme faaliyetleri yapılır.

- a) Bakanlık, izleme faaliyetlerinde gerekli bilgi ve iletişim altyapısını oluşturarak bilgiye erişimi kolaylaştırmak, şeffaflığı ve hızlı bilgi akışını sağlamak ve gerekli önlemlerin en kısa zamanda alınmasını temin etmek üzere; belirli zaman aralıkları ile güncel verileri toplayarak kullanıcıların sorunlarını ve ihtiyaçlarını tespit etmek, risklerini analiz etmek amacıyla internet tabanlı izleme bilgi sisteminin geliştirilmesi, kurulması ve işletilmesinde ilgili kurum ve kuruluşlarla gerekli işbirliğini sağlar.
- b) Bakanlık, izleme bilgi sistemini de kullanarak gerekli risk analizlerini sürekli yapar, izleme ve denetim faaliyetlerini bu analizlere göre yönetir, yönlendirir ve gerekli tedbirleri alır.
- c) Bakanlık, uygulanan proje ve faaliyetlerin performans göstergelerini kullanarak başarısını ölçer, uygulanan programların kısa, orta ve uzun vadede sonuçlarını ve etkilerini analiz ederek, bunlardan gelecekte yapılacak planlama ve programlama çalışmalarında yararlanır.
- ç) Kamu kurum ve kuruluşları yürüttükleri projelerde kaydedilen ilerlemelere ilişkin altışar aylık ilerleme raporlarını Bakanlığa sunar ve Bakanlıkça geliştirilecek internet tabanlı izleme bilgi sistemini yürüttükleri projeler hakkında günceller.

d) Raporların teknik bölümü; proje faaliyetleri, proje yönetimi, ortakların katılımı, paydaşlarla ilişkiler, görünürlük, performans göstergelerindeki ilerlemeler ve projenin genel değerlendirilmesini ihtiva eder.

e) Kamu kurum ve kuruluşları yürüttükleri e-Devlet projesinin tamamlanmasını müteakip dört ay içerisinde Bakanlığa nihai gerçekleşme raporunu sunar.

Etki analizi

MADDE 10 - (1) Bakanlık izlediği proje ve faaliyetlerin doğurduğu etki ve sonuçlarını en geç yılda bir analiz eder ve Bakanlığın kurumsal internet sayfasında yayınlar.

DÖRDÜNCÜ BÖLÜM

Geçici ve Son Hükümler

E-Devlet hizmetlerinde geçiş dönemi

GEÇİCİ MADDE 1 - (1) Kamu kurum ve kuruluşları sundukları ve/veya sunacakları e-Devlet hizmetlerinden kullanıcıların istifade edebilmesi amacıyla gerekli olan kimlik doğrulama işlemini, bu Yönetmeliğin yayımı tarihinden itibaren en geç 12 ay içerisinde sadece e-Devlet Kapısı üzerinden yapar.

(2) Kamu kurum ve kuruluşları kendi sistemleri üzerinden sundukları geniş kitlelere hitap eden ve uygunluk seviyesi yüksek olan e-Devlet hizmetlerini, bu Yönetmeliğin yayımı tarihinden itibaren en geç 24 ay içerisinde e-Devlet Kapısı üzerinden sunar.

(3) e-Devlet Kapısı İşletmecisi, e-Devlet Kapısı üzerinde yer alan kimlik paylaşımının mobil cihazlarda kullanılabilmesi için gerekli alt yapıyı geliştirerek bu Yönetmeliğin yayımı tarihinden itibaren 18 ay içerisinde kurum ve kuruluşların kullanımına sunar.

(4) e-Devlet Kapısı İşletmecisi, kullanıcıların SMS, e-posta, Mobil Push, Web mesaj yollarından herhangi biri ile bilgilendirilmelerini sağlamak amacı ile bilgilendirme altyapısını kurarak bu Yönetmeliğin yayımı tarihinden itibaren 18 ay içerisinde kurum ve kuruluşların kullanımına sunar.

(5) e-Devlet İşletmecisi, vatandaş ve şirketlerin kamu hizmetlerine ilişkin her türlü ödemelerini e-Devlet kapısı aracılığıyla yapabilecekleri bir sistemi bu Yönetmeliğin yayımı tarihinden itibaren 18 ay içerisinde geliştirerek kullanıma sunar.

Yürürlük

MADDE 11 - (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 12 - (Değişik:RG-15/1/2019-30656 Mükerrer)

(1) Bu Yönetmelik hükümlerini Ulaştırma ve Altyapı Bakanı yürütür.

Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik

Resmî Gazete Tarihi : 11.07.2015

Resmî Gazete Sayısı : 29413

NOTERLİK İŞLEMLERİNİN ELEKTRONİK ORTAMDA YAPILMASI HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı, noterlik işlemlerinin elektronik ortamda yapılmasına, saklanmasına, paylaşılmasına ilişkin usûl ve esasları düzenlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, elektronik ortamda güvenli elektronik imza ile noter huzurunda veya huzurda olmadan yapılabilecek noterlik işlemleri ile 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununda tanımlanan zaman damgası kullanılmasının zorunlu olduğu noterlik işlemlerinin belirlenmesi, belirlenen bu işlemlerin elektronik ortamda yapılması, işlenmesi, saklanması, ilgili ve diğer kişi veya kurumlara elektronik ortamda gönderilmesi, Noterlik Kanununun 61 inci maddesinde düzenlenen tespit işleri ile elektronik ortamdaki durum, görüntü, işlem veya benzeri her türlü verinin tespiti işleri, elektronik ortamdan fizikî örnek çıkarılması, yabancı memleketlerde noterlik işlemlerinin elektronik ortamda yapılması için gerekli olan teknik ve idarî şartlara ilişkin usûl ve esasları kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 18/1/1972 tarihli ve 1512 sayılı Noterlik Kanununun 198/A maddesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Yönetmelikte geçen;

- a) Arşiv: Noterlikte yapılan işlemlere ilişkin bilgi ve belgelerin 18/9/1990 tarihli ve 20639 sayılı Resmî Gazete’de yayımlanan Noterlik Daireleri Arşiv Hizmetleri Hakkında Yönetmelik hükümlerine uygun olarak TNBBS’de saklanması,
- b) Bakanlık: Adalet Bakanlığını,
- c) Birlik: Türkiye Noterler Birliğini,
- ç) Donanım: Üzerindeki verinin elektronik ortamda tespitine imkân veren cihazları,
- d) Güvenli elektronik imza: 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununun 4 üncü maddesinde tanımlanan elektronik imzayı,
- e) İlgili: Kanunun 72 nci maddesinde belirtilen belgelendirme talebinde bulunan kişiyi,
- f) İz bilgisi (Log kaydı): TNBBS üzerinden yapılan tüm işlemlerin elektronik ortamda tutulan kaydını,
- g) Kanun: 18/1/1972 tarihli ve 1512 sayılı Noterlik Kanununu,
- ğ) KEP: 25/8/2011 tarihli ve 28036 sayılı Resmî Gazete’de yayımlanan Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 4 üncü maddesinde tanımlanan kayıtlı elektronik posta sistemini,
- h) Nitelikli elektronik sertifika: 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununun 9 uncu maddesinde sayılan nitelikleri haiz elektronik sertifikayı,
- ı) SMS: Kısa mesaj servisini,
- i) TNBBS: Türkiye Noterler Birliği Bilişim Sistemini,
- j) Zaman damgası: 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununun 3 üncü maddesinde tanımlanan zaman damgasını,
- ifade eder.

İKİNCİ BÖLÜM

Elektronik Ortamda Yapılacak Noterlik İşlemleri

Noterlik işlemlerinin elektronik ortamda yapılması ve güvenli elektronik imza ile zaman damgasının kullanılması

MADDE 5 - (1) Kanunda öngörülen işlemler, elektronik ortamda güvenli elektronik imza ile de yapılabilir. Şu kadar ki, kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler

ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez. Güvenli elektronik imza ile yapılan tüm noterlik işlemlerinde zaman damgası kullanılır.

(2) Düzenleme şeklinde yapılması gereken işlemler ile irade beyanlarının alınmasına ilişkin işlemlerin noter huzurunda yapılması gerekir. İlgililer huzurda olmadan güvenli elektronik imzalarını kullanarak TNBBS'ye girerek işlem hazırlıklarını başlatabilir, ancak işlem noter huzurunda tamamlanır. Bu işlemler sırasında işleme katılanlar ve noter, güvenli elektronik imzalarını TNBBS sistemi üzerinde kullanırlar.

(3) Düzenleme şeklinde olmayan veya irade beyanının noter huzurunda alınması gerekmeyen işlemler TNBBS üzerinden güvenli elektronik imza ile başlatılıp, bu şekilde tamamlanabilir. Belgenin düzenlenmesi de dâhil tüm aşamalar elektronik ortamda yapılır. İşlem, noterlik ücretleri, vergi, harç ve diğer giderlerin tahsil edilmesi ile tamamlanır.

(4) Yukarıdaki fıkralar uyarınca yapılacak noterlik işleminin bir belgeye dayanması hâlinde; belge sureti, taraflar, vekilleri veya temsilcileri tarafından güvenli elektronik imza ile imzalanarak elektronik ortamda notere gönderilebilir. Gönderilen belgenin aslının ibrazının zorunlu olduğu hâller ile söz konusu belgenin TNBBS üzerinden doğrulanamaması hâlinde belge aslının fizikî olarak başvurudan sonraki üç iş günü içerisinde ve her halükârda işlem tamamlanmadan ibrazı zorunludur. Belgenin doğrulanamaması hâlinde süre, duruma ilişkin bildirim ilgiliye noter tarafından SMS, KEP ya da TNBBS sistemi vasıtasıyla bildirim gününden başlar. Anılan sürelerin sonunda belgenin ibraz edilmemesi hâlinde başvuru iptal edilir.

(5) Noterlik Kanununun 61 inci maddesindeki tespit işlemleri ilgilinin talep etmesi hâlinde elektronik ortamda güvenli elektronik imza ile de yapılabilir.

(6) Elektronik ortamdaki bir verinin tespiti işleminde;

a) Bir donanımdaki veya internet ortamındaki verinin tespiti işlemi ile o verinin belirli bir anda ya da zaman aralığında o anki veya zaman aralığındaki hâlinin değişmez olarak belirlenmesi, tekrar edilebilir hâlde tutulması ve saklanması anlaşılır.

b) Tespit edilecek veri bir donanımda ise tespit, malikin ya da zilyedin rızasıyla noterlikte veya mahallinde yapılabilir.

c) Tespit edilecek veri internet ortamında ise tespit işlemi TNBBS kullanılarak yapılır.

ç) Elektronik ortamda yapılan tespit işlemine ilişkin tutanak noterlik mevzuatı çerçevesinde noterliğin çalışma saatlerinde düzenlenir.

Güvenli elektronik imza ile noter huzurunda olmadan yapılabilecek işlemler

MADDE 6 - (1) Aşağıdaki işlemler TNBBS üzerinde güvenli elektronik imza ile ilgililer noter huzurunda olmadan yapılabilir.

- a) Çevirme işlemleri,
- b) Tescil işlemleri,
- c) Tespit işlemleri,
- ç) Örnek verme işlemleri,
- d) Defter onayları,
- e) İmza onaysız ihtarname ve ihbarname.

Güvenli elektronik imza ile noter huzurunda yapılabilecek işlemler

MADDE 7 - (1) Bu Yönetmeliğin 6 ncı maddesinde sayılanlar dışındaki işlemlerin güvenli elektronik imza ile yapılabilmesi ya da 5 inci maddenin ikinci fıkrası uyarınca başlatılan bir işlemin sonuçlanması ilgililerin noter huzurunda bulunması şartına bağlıdır.

ÜÇÜNCÜ BÖLÜM

Elektronik Ortamda Yapılan Noterlik İşlemlerinin Güvenli Elektronik İmza ile İşlenmesi, Kaydedilmesi, Saklanması ve Paylaşılması

Elektronik işlemler için kurulacak ve işletilecek sistem

MADDE 8 - (1) Birlik, elektronik ortamda güvenli elektronik imza ile işlem yapılmasına imkân sağlayacak altyapıyı kurar ve işletir. Bu altyapının güvenli olarak kurulması ve işletilmesi için gerekli tüm tedbirleri alır.

(2) Bu Yönetmelik kapsamında diğer kurum ve kuruluşlarla yapılacak bilgi ve belge paylaşımlarında kullanım ve erişim standartları ile diğer gerekli şartlar Birlik tarafından belirlenir.

(3) TNBBS üzerinden elektronik ortamdan başvurunun başlatılması sırasında işlemin sistem tarafından herhangi bir notere yönlendirilmemesi için kişiye öncelikle istediği noteri seçme imkânı, seçtiği bir noter yok ise en yakın noterleri bulma imkânı sağlanır.

(4) İşlemlerin elektronik ortamda yürütülmesini sağlayacak yönergeleri Birlik hazırlar, bu yönergeler Birliğin resmî internet sitesinde yayımlanır.

(5) Sistem tarafından tutulacak iz bilgilerinin kapsamı Birlik tarafından belirlenir.

İşlemlerin elektronik ortamda kaydedilmesi ve saklanması

MADDE 9 - (1) İşleme katılanların tamamının güvenli elektronik imzası ile elektronik ortamda yapılan bir işlem için talep edilmedikçe fizikî olarak belge düzenlenmez ve bu işleme ilişkin olarak elektronik ortam dışında bir saklama yapılmaz. Bu kayıtlar iş sürekliliği ve bilgi güvenliğine ilişkin uluslararası kabul görmüş standartlara uygun olarak, yedekli ve güvenli bir şekilde saklanır.

(2) Birinci fıkra kapsamında kalmayan diğer noterlik işlemlerinde ise işleme ait belgenin imzaya açılan son hâli noter tarafından güvenli elektronik imza ile imzalanarak TNBBS'ye kaydedilir. Belgenin ilgililerce imzalı hâli ise Noterlik Daireleri Arşiv Hizmetleri Hakkında Yönetmelik hükümlerine göre saklanır.

İşlemlerin elektronik ortamda paylaşılması

MADDE 10 - (1) (Danıştay Sekizinci Dairesinin 30/9/2021 tarihli ve E.:2016/3785; K.:2021/4266 sayılı kararı ile iptal fıkra; İşleme katılanların tamamının güvenli elektronik imzası ile yapılan işlemlere ilişkin bilgi ve belgeler gerektiğinde noterler ile diğer kişi ve kurumlarla paylaşılabilir.)

(2) (Değişik:RG-11/11/2021-31656) TNBBS'ye kaydedilen işlemlere ilişkin bilgiler gerektiğinde noterler ile ilgili diğer kişi ve kurumlarla paylaşılabilir.

(3) Birlik, noterlik işlemlerinin elektronik ortamda yapılması sırasında kişisel verilerin korunması ve bilgi güvenliğinin sağlanması için gerekli tedbirleri alır.

(4) (Danıştay Sekizinci Dairesinin 30/9/2021 tarihli ve E.:2016/3785; K.:2021/4266 sayılı kararı ile iptal fıkra; Noterlik işlemlerine ilişkin bilgi ve belgenin paylaşılmasının sağlanması için Bakanlığın görüşü alınarak Birlik tarafından ilgili kurum ve kuruluşlar ile protokol imzalanır. Paylaşımına ilişkin ücretler protokolda düzenlenir.)

(5) Paylaşımına ilişkin iz bilgileri güvenliği, gizliliği ve bütünlüğü sağlanarak TNBBS'de tutulur. Saklanacak iz bilgisi içeriği Birlik tarafından belirlenir.

İlgilinin talebiyle belgenin elektronik ortamda gönderilmesi veya paylaşılması

MADDE 11 - (1) İlgilisi tarafından bir belgenin üçüncü kişi ile elektronik ortamda paylaşılmasının istenmesi durumunda belge, gerekli ücretlerin ödenmesi koşuluyla;

a) Üçüncü kişinin KEP adresine gönderilmesi,

b) Üçüncü kişinin Birlik tarafından bilgi ve belge paylaşımı için protokol imzalanan bir kurum veya kuruluş olması durumunda ilgili protokol hükümleri çerçevesinde belgeye erişim sağlanması,

c) İlgiliye erişim kodu verilmesi hâlinde bu kod ile TNBBS üzerinden erişiminin sağlanması, yöntemlerinden biri veya birkaçı ile paylaşılır.

(2) Belgeye birinci fıkranın (c) bendinde belirlenen erişim kodu ile talep edilen üçüncü kişi yerine başka bir kişinin erişmesinden noter veya Birlik sorumlu tutulamaz.

(3) Birlik, kendi kuracağı sistem gereği ilgili kurumdan bilgi veya belge paylaşımı için, protokol imzalanmasını isteme, paylaşım alt yapısını belirleme hak ve yetkisine sahiptir. İlgili kurum veya kuruluş bu gerekleri karşılamadan bilgi ve belgenin elektronik ortamda paylaşılmasını talep edemez.

Yabancı memleketlerde noterlik işlemlerinin elektronik ortamda yapılması ve Dışişleri Bakanlığı ile bilgi ve belge paylaşımı

MADDE 12 - (1) Yabancı memleketlerde noterlik işlemleri bu Yönetmelikte gösterilen usullere göre elektronik ortamda güvenli elektronik imza ile de yapılabilir, işlenebilir, saklanabilir, paylaşılabilir ve gönderilebilir.

(2) Yabancı memleketlerde noterlik işlemlerinin elektronik ortamda yapılması için sağlanması gerekli olan teknik ve idarî şartlara dair usul ve esaslar Birlik ve Dışişleri Bakanlığı arasında yapılacak protokol ile belirlenir.

(3) Bu Yönetmeliğin 5 inci maddesinin dördüncü fıkrasında yer alan süre ve bildirim usûlü Dışişleri Bakanlığınca belirlenir ve Dışişleri Bakanlığı Konsolosluk resmî internet sitesinde ilân edilir.

DÖRDÜNCÜ BÖLÜM

Ortak Hükümler

Elektronik ortamda ödeme

MADDE 13 - (1) Elektronik ortamda yapılacak işlemlerden kaynaklanan noterlik işlem ücretleriyle, vergi, resim, harç ve değerli kâğıt bedellerine ve diğer giderlere ilişkin ödemelerin elektronik ortamda yapılmasına ilişkin alt yapı Birlik tarafından sağlanır.

Elektronik arşiv

MADDE 14 - (1) Bu Yönetmelik gereğince elektronik ortamda yapılan işlemlere ilişkin bilgi ve belgeler Noterlik Daireleri Arşiv Hizmetleri Hakkında Yönetmelik hükümlerine, iş sürekliliği ve bilgi güvenliğine ilişkin uluslararası kabul görmüş standartlara uygun olarak, yedekli ve güvenli bir şekilde TNBBS'de saklanır. Belgelerin saklama süreleri de aynı Yönetmelik hükümlerine göre belge grupları esas alınarak belirlenir.

Elektronik belgeden fizikî örnek çıkarılması

MADDE 15 - (1) Bu Yönetmelik hükümlerine göre işleme katılanların tamamının güvenli elektronik imzası ile imzalanan bir belgenin fizikî örneğinin çıkartılması gerektiği hâllerde belgenin aslının aynı olduğu belirtilerek noter tarafından imzalanır, mühürlenir ve ilgisine verilir.

Noterlik elektronik işlemler ücret tarifesi

MADDE 16 - (1) Bu Yönetmelik kapsamında yapılacak noterlik işlemlerinden ne kadar ücret alınacağı Kanunun 112 nci maddesi uyarınca Bakanlıkça hazırlanan tarifede gösterilir.

Noterlik Kanunu Yönetmeliğinin uygulanacağı hâller

MADDE 17 - (1) Bu Yönetmelikte hüküm bulunmayan hâllerde, 13/7/1976 tarihli ve 15645 sayılı Resmî Gazete’de yayımlanan Noterlik Kanunu Yönetmeliğinin hükümleri uygulanır.

BEŞİNCİ BÖLÜM

Çeşitli ve Son Hükümler

Geçiş hükümleri

GEÇİCİ MADDE 1 - (1) Yabancı memleketlerde, noterlik işlemlerinin elektronik ortamda güvenli elektronik imza ile yapılmasına ilişkin Birlik ile Dışişleri Bakanlığı arasında yapılacak protokolde belirtilecek tarihe kadar noterlik işlemleri bu Yönetmelik uygulanmadan yapılmaya devam edilir. Gerekli altyapının sağlanamadığı dış temsilciliklerde işlemler bu Yönetmelik uygulanmadan yapılır.

Yürürlük

MADDE 18 - (1) Bu Yönetmelik 1/3/2016 tarihinde yürürlüğe girer.

Yürütme

MADDE 19 - (1) Bu Yönetmelik hükümlerini Adalet Bakanı yürütür.

Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik

Resmî Gazete Tarihi : 15.03.2020

Resmî Gazete Sayısı : 31069

BANKALARIN BİLGİ SİSTEMLERİ VE ELEKTRONİK BANKACILIK HİZMETLERİ HAKKINDA YÖNETMELİK

BİRİNCİ KISIM

Başlangıç Hükümleri

Amaç ve kapsam

MADDE 1 - (1) Bu Yönetmeliğin amacı, bankaların faaliyetlerinin ifasında kullandıkları bilgi sistemlerinin yönetimi ile elektronik bankacılık hizmetlerinin sunulmasında ve bunlara ilişkin risklerin yönetiminde esas alınacak asgari usul ve esaslar ile tesis edilmesi gereken bilgi sistemleri kontrollerini düzenlemektir.

Dayanak

MADDE 2 - (1) Bu Yönetmelik, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununun 93 üncü maddesi uyarınca düzenlenmiştir.

Tanımlar ve kısaltmalar

MADDE 3 - (1) Bu Yönetmelikte yer alan;

- a) Açık bankacılık servisleri: Müşterilerin ya da müşteriler adına hareket eden tarafların API, web servis, dosya transfer protokolü gibi yöntemlerle bankanın sunduğu finansal servislere uzaktan erişerek bankacılık işlemlerini gerçekleştirebildikleri veya gerçekleştirilmesi için bankaya talimat verebildikleri elektronik dağıtım kanalını,
- b) Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,
- c) API: Bir yazılımın başka bir yazılımda tanımlanmış işlevleri kullanabilmesi için oluşturulmuş uygulama programlama arayüzünü,

- c) ATM: Otomatik para çekme işleminin yanı sıra diğer bankacılık işlemlerinin tamamının veya bir bölümünün gerçekleştirilmesine imkân veren elektronik işlem cihazlarını,
- d) Banka: Kanunun 3 üncü maddesinde tanımlanan bankaları,
- e) Bilgi sistemleri (BS): Bilginin toplanması, işlenmesi, saklanması, dağıtımı ve kullanımına yönelik insan kaynağı, operasyonel faaliyetler ve süreçler ile bunlarla etkileşim içinde bulunan bilgi teknolojilerini,
- f) Bilgi sistemleri süreklilik planı: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan bilgi sistemleri süreklilik planını,
- g) Bilgi sistemleri yönetimi: Bankaca gerçekleştirilen faaliyetlerin ve verilen hizmetlerin etkin, güvenilir ve kesintisiz bir şekilde yürütülmesine; mevzuattan kaynaklanan yükümlülüklerin yerine getirilmesine; muhasebe ve finansal raporlama sisteminden sağlanan bilgilerin bütünlüğünün, tutarlılığının, güvenilirliğinin, zamanında elde edilebilirliğinin ve gereken durumlarda gizliliğinin sağlanması amacıyla uygun bilgi sistemleri ortamının tesis edilmesine; bilgi sistemleri kaynaklarının verimli olarak kullanılmasına; bilgi sistemlerinin kullanılmasından kaynaklanan risklerin kontrolünün ve izlenmesinin sağlanmasına; bu amaçla gerekli sistemsel ve yönetsel önlemlerin alınmasına ilişkin faaliyetleri,
- ğ) Bilgi teknolojileri (BT): Herhangi bir biçimdeki verinin, girişinin yapılması, saklanması, işlenmesi, iletilmesi ve çıktılarının alınması için kullanılan donanım, yazılım, iletişim altyapısı ve ilgili diğer teknolojileri,
- h) Bilgi varlığı: Bankacılık faaliyetlerinin yürütülmesinde kullanılan veriler ile bu verilerin taşındığı, saklandığı, iletildiği veya işlendiği sistem, yazılım, ağ cihazları, BT donanımları, iş süreçleri gibi Banka için değeri olan varlığı,
- ı) Birincil merkez: Birincil sistemlerin tesis edildiği yapıyı,
- i) Birincil sistemler: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan birincil sistemleri,
- j) Biyometrik kimlik doğrulama bileşeni: Kimlik doğrulama işlemlerinin gerçekleştirilmesini sağlamak amacıyla kullanılan bir kişiye özgü ölçülebilir biyolojik veya davranışsal karakteristiği,
- k) Dış hizmet: 5/11/2011 tarihli ve 28106 sayılı Resmî Gazete’de yayımlanan Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik kapsamındaki destek hizmetleri de dâhil olmak üzere bankaların bilgi sistemlerine ilişkin dışarıdan temin ettikleri, bankacılık verilerinin gizliliği,

bütünlüğü ve erişilebilirliği ile bankacılık hizmetlerinin sürekliliğini etkileme potansiyeli olan, bankacılık verilerine erişimi bulunan ya da bu verilerin paylaşıldığı hizmet alımlarını,

l) Elektronik bankacılık hizmetleri: İnternet bankacılığı, mobil bankacılık, telefon bankacılığı, açık bankacılık servisleri ile ATM ve kiosk cihazları gibi müşterilerin, uzaktan bankacılık işlemlerini gerçekleştirebildikleri veya gerçekleştirilmesi için bankaya talimat verebildikleri her türlü elektronik dağıtım kanalını,

m) Elektronik imza: 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununda tanımlanan elektronik imzayı,

n) Güvenlik duvarı: Farklı güvenlik seviyelerine sahip ağlar veya ağa bağlı cihazlar arasındaki trafik akış kontrolünü sağlayan donanım ya da yazılımları,

o) Hassas veri: Kimlik doğrulamada kullanılan veriler başta olmak üzere; müşteriye ait olan, çeşitli sebeplerle bankaca muhafaza edilen ve üçüncü kişilerce ele geçirilmesi halinde, bu kişilerin müşteri olan kişilerle ayırt edilebilme mekanizmalarının zarar göreceği ve dolandırıcılık ya da müşteriler adına sahte işlem yapılmasına imkân verebilecek nitelikteki verileri,

ö) İkincil merkez: İkincil sistemlerin kullanıma hazır olacak şekilde tesis edildiği ve birincil sistemlerde herhangi bir kesinti yaşanması durumunda personelin çalışmasına imkân tanıyacak ve birincil merkez ile aynı riskleri taşımayacak şekilde oluşturulmuş yapıyı,

p) İkincil sistemler: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan ikincil sistemleri,

r) İnternet bankacılığı: Bankaların kendi ticaret unvanı, işletme adı ya da herhangi başka bir ad altındaki bir web sayfası üzerinden sundukları hizmetlere müşterilerin, kullandıkları cihaz ya da platformdan bağımsız olarak, internet yoluyla ulaşabildiği ve kendilerine ait finansal veya kişisel verileri görüntüleyebildiği, değiştirebildiği ya da finansal sorumluluk yaratacak işlemler gerçekleştirebildiği elektronik dağıtım kanallarını,

s) İSEDES Yönetmeliği: 11/7/2014 tarihli ve 29057 sayılı Resmî Gazete’de yayımlanan Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmeliği,

ş) İş etki analizi: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan iş etki analizini,

t) Kanun: 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununu,

u) Kesinti: Bir bankanın faaliyetlerindeki sürekliliğin, planlı geçişler haricinde sekteye uğramasını,

ü) Kimlik doğrulama: Bildirilen bir kimliğin gerçekten bildiren şahsa ait olduğuna dair güvence sağlayan mekanizmayı,

- v) Kişisel veri: 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununda tanımlanan kişisel veriyi,
- y) Kontrol: Banka içerisinde BT süreçlerinde gerçekleştirilen ve iş hedeflerinin gerçekleştirilmesi, istenmeyen olayların engellenmesi, belirlenmesi ve düzeltilmesi ile ilgili olarak yeterli derecede güvenceyi oluşturma amacı güden politikalar, prosedürler, uygulamalar ve organizasyonel yapıların tamamını,
- z) Kullanıcı: Banka personeli, dış hizmet sağlayıcı çalışanı veya banka müşterisi gibi bankanın bilgi sistemleri üzerinde işlem gerçekleştirmek üzere kendilerine hesap tanımlanmış olan her türlü kullanıcıyı,
- aa) Kurum: Bankacılık Düzenleme ve Denetleme Kurumunu,
- bb) Kurumsal SOME: 11/11/2013 tarihli ve 28818 sayılı Resmî Gazete'de yayımlanan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğin 5 inci maddesinde ifade edilen Kurumsal SOME'yi,
- cc) Kurul: Bankacılık Düzenleme ve Denetleme Kurulunu,
- çç) Mobil bankacılık: Akıllı telefon veya tablet gibi mobil bir cihaz üzerinde yüklü, bankaya ait mobil uygulama üzerinden müşterilerin bankacılık işlemlerini gerçekleştirebildikleri özelleşmiş internet bankacılığı dağıtım kanalını,
- dd) Oturum: Veri aktarımı, sunuşu veya gerçekleştirilecek finansal işlemler için taraflar arasında kurulan mantıksal bağı,
- ee) Parola: Kimlik doğrulamada kullanılan, gizli harf, rakam ve/veya özel işaretlerden oluşan karakter dizisini,
- ff) Risk limitleri: İSEDES Yönetmeliğinin 38 inci maddesinde açıklanan risk limitlerini,
- gg) Sektörel SOME: Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğin 7 nci maddesinde ifade edilen Kurum bünyesinde teşkil edilmiş Sektörel SOME'yi,
- ğğ) Sızma testi: Sistemin güvenlik açıklarını istismar edilmeden önce tespit etmek ve düzeltmek amacıyla gerçekleştirilen güvenlik testlerini,
- hh) Siber olay: Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğin 3 üncü maddesinde tanımlanan siber olayı,

- ıı) Siber olaya müdahale: Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğin 3 üncü maddesinde tanımlanan siber olaya müdahaleyi,
- ii) SMS OTP: Elektronik haberleşme işletmecilerinin sunduğu kısa mesaj servisi aracılığıyla iletilen tek kullanımlık parolayı,
- jj) Tek kullanımlık parola: Kimlik doğrulamada sadece bir kez kullanılmak üzere rastgele oluşturulan harf ve/veya rakamlar dizisini,
- kk) Uçtan uca güvenli iletişim: İletişime konu veriye sadece alıcısının erişebilmesi amacıyla, verinin gönderen tarafından sadece alıcının çözebileceği şekilde şifrelenerek iletilmesini,
- ll) Üst düzey yönetim: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan üst düzey yönetimi,
- mm) Üst yönetim: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan üst yönetimi,
- nn) Varlık muhafızı: Varlık sahibinin tanımladığı güvenlik gereksinimlerine uygun olarak, bir bilgi varlığının saklanması, taşınması, işlenmesi veya iletilmesi esnasında korunmasından sorumlu olan kişiyi,
- oo) Varlık sahibi: Bilgi varlıklarına yönelik güvenlik gereksinimlerini belirleyerek varlık muhafızlarına ileten ve bu gereksinimlere uygun güvenlik kontrollerinin varlık muhafızları tarafından uygulandığını gözeterek bilgi varlığının idamesi ve erişilebilirliğinden sorumlu olan kişiyi,
- öö) Yama: Programlarda tespit edilen güvenlik açıkları veya programın içeriğindeki hatalı bir fonksiyonu düzeltme amaçlı hazırlanan program eklentisini,
- ifade eder.

İKİNCİ KISIM

Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi

BİRİNCİ BÖLÜM

Bilgi Sistemleri Yönetişimi

Yönetim gözetimi, roller ve sorumluluklar

MADDE 4 - (1) Banka yönetim kurulu, bilgi sistemlerinin yönetimini kurumsal yönetim uygulamalarının bir parçası olarak ele almakla, bilgi sistemlerinin doğru yönetimi için gerekli finansman ve insan kaynağını tahsis etmekle, bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliğini sağlamak amacıyla bilgi sistemleri üzerinde etkin kontrollerin tesis edilmesini

sağlamakla ve gelişen yeni teknolojileri de göz önünde bulundurarak bilgi sistemlerinin kullanımından kaynaklanan risklerin yönetilmesi için etkin bir gözetim yürütmekle sorumludur. Bu amaçla, yönetim kurulu tarafından onaylanmış bir BS strateji planı, BS Strateji Komitesi ve BS Yönlendirme Komitesi oluşturulur. Banka yönetim kurulu bankanın ölçeği, bilgi sistemlerine bağımlılığı, personel sayısı ve bilgi sistemleri konusunda alınan dış hizmetler gibi kriterleri esas alarak strateji ve yönlendirme komitelerini birleştirebilir. Bu komitelerin görev tanımları ve çalışma esasları yönetim kurulu tarafından onaylanır.

(2) BS Strateji Komitesi, yönetim kurulu adına, BS strateji planı doğrultusunda BS yatırımlarının uygun bir şekilde kullanılıp kullanılmadığının ve bankanın iş hedefleri ile BS hedeflerinin birbiriyle uyumluluğunun gözetimini yürütmekle; bu hususlarda yönetim kuruluna doğrudan ve düzenli olarak raporlama yapmakla; BS strateji planını yılda en az bir defa olmak üzere gözden geçirerek gerekli olduğu durumlarda revize ederek yönetim kurulu onayına sunmakla ve BS Yönlendirme Komitesinin faaliyetlerini gözetmekle sorumludur.

(3) BS Strateji Komitesinde en az bir yönetim kurulu üyesinin bulunması ve bilgi sistemlerinden sorumlu üst düzey yönetici ile bankanın ilgili iş birimlerinden üst düzey yöneticilerin bu komiteye üye olması esastır. BS Strateji Komitesi, BS strateji planının düzgün bir şekilde uygulanıp uygulanmadığını gözden geçirmek ve önemli BS yatırım kararlarını değerlendirmek üzere yılda en az iki defa bir araya gelir ve yılda en az bir defa yönetim kuruluna rapor sunar.

(4) BS stratejisinin yönetim kurulu onayı doğrultusunda uygulanmasında, BS Strateji Komitesine ve üst düzey yönetime yardımcı olmak amacıyla bir BS Yönlendirme Komitesi oluşturulur. BS Yönlendirme Komitesi, BS yatırımlarının ve projelerinin öncelik sırasını belirlemek, devam eden BS projelerinin durumunu takip etmek, projeler arasındaki kaynak çatışmalarını çözüme kavuşturmak, BS mimarisi ve BS projelerinin mevzuata uyumluluğunu sağlamak üzere gerekli yönlendirmeleri yapmak ve BS servislerine ilişkin hizmet seviyelerini izlemekten sorumludur. BS Yönlendirme Komitesinde BS, insan kaynakları, bankanın ilgili iş birimlerinden temsilcilerin ve banka organizasyonunda bulunması durumunda uyum ve hukuk ile ilgili birim ya da pozisyonlardan temsilcilerin bulunması esastır. BS Yönlendirme Komitesi, yılda en az iki defa bir araya gelir ve yılda en az bir defa BS Strateji Komitesine rapor sunar.

(5) BS organizasyonu ve bilgi sistemlerinin kapsamlılık düzeyinin, bankanın büyüklüğü ve faaliyetlerinin karmaşıklığı ile orantılı olması ve BS organizasyon şemasının da bu doğrultuda oluşturulması esastır. BS organizasyon şeması kapsamındaki birimlerin görev ve sorumlulukları ile bu birimlerdeki personelin görev tanımları açık bir şekilde yazılı hale getirilir, yönetim kurulu ya da

yönetim kurulunun bu yönde yetkisini devrettiği üst düzey yöneticilerce onaylanır, bu görev tanımlarının uygunluğu düzenli olarak gözden geçirilir.

(6) BS personelinin kendilerine atanan görev ve sorumluluklar hakkında farkındalığa sahip olması ve kendilerine ait görev ve sorumluluklarda değişiklik yapılması halinde bu değişikliklerden haberdar olmaları sağlanır.

Bilgi sistemleri politika, prosedür ve süreç dokümanları

MADDE 5 - (1) Banka, bilgi sistemlerinin kullanımından kaynaklanan riskleri yönetmek ve bilgi varlıklarını korumak amacıyla uygulanması gereken usul ve esaslar ile tesis edilmesi gereken kontrolleri tarif eden BS politika, prosedür ve süreç dokümanlarını oluşturur.

(2) Dokümanların gizlilik derecesi ve banka çalışanlarının görev ve sorumluluklarının uygunluğu nispetinde dokümanlara erişim imkânı verilir. Dokümantasyonda asgari olarak doküman kodu ve dokümanın gizlilik derecesine yer verilir.

(3) BS politikaları yönetim kurulu tarafından, BS prosedürleri ve süreç dokümanları ise yönetim kurulu ya da yönetim kurulunun bu yönde yetkisini devrettiği yöneticilerce onaylanır.

(4) BS politika, prosedür ve süreç dokümanlarının gerekleri, bankanın organizasyonel ve yönetsel yapıları içerisinde fiili olarak işleyecek şekilde yerleştirilir, bunların işlerliğine ilişkin gözetim ve takip gerçekleştirilir. Politika ve prosedürlerin işletilmesinden sorumlu birimler ve görev tanımları ile süreç dokümanlarının işletilmesinden sorumlu süreç sahipleri ilgili politika, prosedür ve süreç dokümanları içinde belirtilir.

(5) BS politika, prosedür ve süreç dokümanları yılda en az bir defa gözden geçirilir ve gerekli güncellemeler yapılır. Dokümanlarda meydana gelen değişiklikleri takip edebilmek adına, dokümanın önceki versiyonu ile asgari olarak dokümanı onaylayan, revizyon tarihi ve gözden geçirme tarihi bilgileri kayıt altına alınır.

İKİNCİ BÖLÜM

Bilgi Sistemleri Risklerinin Yönetilmesi

Bilgi varlıkları envanteri ve sınıflandırılması

MADDE 6 - (1) Banka, bilgi varlıklarının güvenlik gereksinimlerine uygun kontroller tesis etmek için bu varlıkları sınıflandırarak detaylı bir varlık envanteri hazırlar. Hazırlanacak varlık envanterinde her bir bilgi varlığı için;

a) Varlığın ne olduğunu açıkça belirtecek tanımına,

b) Banka için görece değerine,

c) Bulunduğu konuma,

ç) Varlığın güvenlik sınıfına ve bu sınıfın belirlenmesini sağlayan gizlilik, bütünlük, erişilebilirlik gibi değerlerine,

d) Varlığın sahibine,

e) Varlığın muhafızına,

yer verilir.

(2) Bilgi varlıklarının değeri ele alınırken bu varlıkların ilişkili olduğu iş hedefleri ve iş süreçleri ile bunların bağlı olduğu diğer iş hedefleri ve iş süreçleri dikkate alınır.

(3) Bilgi varlıklarının bir parçası olan veriler için oluşturulacak veri envanterine birinci fıkrada belirtilen detaylara ilave olarak kişisel veri olup olmadığı bilgisi dâhil edilir.

(4) Varlık sahipleri ile birlikte çalışılmak suretiyle, her bir varlığın tanımlı ve onaylı bir güvenlik sınıfına ve erişim kısıtlamasına sahip olması sağlanır. Güvenlik sınıfları ve erişim kısıtlamaları iki yıldan uzun olmayacak periyotlarla düzenli olarak gözden geçirilir.

(5) Bilgi varlıklarının, nasıl sınıflandırılacağına yönelik olarak Bilgi Güvenliği Komitesi tarafından onaylı bir varlık sınıflandırma kılavuzu hazırlanır. Varlıkların güvenlik sınıfı belirlenirken gizlilik derecesi, bütünlük gereksinimi, erişilebilirlik gereksinimi, saklama süresi ve asgari yedekleme sıklığı gibi kriterler göz önünde bulundurulur.

(6) Verilerin güvenlik sınıfı asgari olarak bu verilerin gizlilik derecesi, bütünlük gereksinimi, erişilebilirlik gereksinimi ve hassas veri, kişisel veri ya da sır kapsamındaki veri olup olmadığı gibi kriterler göz önünde bulundurularak belirlenir.

Bilgi sistemleri risk yönetim süreci

MADDE 7 - (1) Banka, bankacılık faaliyetlerinde bilgi teknolojilerini kullanıyor olmasından kaynaklanan riskleri analiz etmek, azaltmak, takip etmek ve raporlamak üzere bir BS risk yönetim süreci tesis eder.

(2) BS risk analizi kapsamında aşağıdaki faaliyetler yerine getirilir:

a) 6 ncı maddenin birinci fıkrası kapsamında oluşturulan varlık envanterindeki bilgi varlıklarına ilişkin tehdit ve güvenlik açıklarının tespit edilmesi suretiyle risklerin belirlenmesi,

b) Tespit edilen tehditlere ve güvenlik açıklarına göre bilgi varlıklarının riske maruz kalma olasılıklarının belirlenmesi,

c) Risklerin gerçekleşmesi durumunda ilişkili bilgi varlığının gizliliği, bütünlüğü, erişilebilirliği gibi kriterlerine olan etkilerin belirlenmesi suretiyle ilgili bilgi varlığına yönelik etki hesaplaması yapılması,

ç) Bilgi varlıklarını tehdit eden risklerin belirlenen olasılık ve etki değerlerine göre risk derecelendirmesinin yapılması,

d) Risk analizinde gerçekleştirilen çalışmaların bütünü temsil eden özet risk değerlendirme raporunun hazırlanarak üst yönetime sunulması.

(3) Risk analizi sonuçlarına göre tespit edilen her bir BS riskine ilişkin, bu risklerin ilişkili olduğu bilgi varlıklarının değerine ve bankanın risk limitlerine uygun olacak şekilde risklere ilişkin aksiyonlar belirlenir. Risk aksiyonlarının belirlenmesi aşamasında, riskin ilgili olduğu iş biriminin temsilcileriyle beraber risk analizi sonucunda, riskin azaltılması, riskten kaçınma, riskin kabulü ve riskin transferi gibi yöntemlerle nasıl ele alınacağına karar verilir.

(4) Her bir risk için belirlenen aksiyonlar risk aksiyon planına dönüştürülür. Alınacak aksiyonlar için yapılacak kaynak aktarımında ve aksiyonların tamamlanma tarihlerinin önceliklendirilmesinde, risk analizi aşamasında belirlenen risk dereceleri dikkate alınır. Aksiyon planının uygulanması sonucunda kalacak artık riskler için de alınacak aksiyonlar planlanır ve aksiyon planı güncellenir.

(5) Riskin kabul edilebilmesi için bilgi sistemlerinden sorumlu üst düzey yöneticinin onayının bulunması, riskin BS stratejisine ve mevzuata aykırılık teşkil etmemesi şarttır. Kabul edilecek riskin aynı zamanda bir iş süreci veya iş uygulamasıyla ilgili olması durumunda ilgili iş biriminin üst düzey yöneticisinin de riskin kabul edildiğine ilişkin onayının bulunması gerekir. Sonradan telafi edici yeni kontrol tekniklerinin ya da yeni güvenlik çözümlerinin ortaya çıkmış olması veya riskin eskiye nazaran artıp artmadığı yönünde koşulların değişmiş olması ihtimaline karşı, önceden kabul edilmiş olan riskler periyodik olarak gözden geçirilir.

(6) Risk analizleri sonucu hazırlanan güncel risk değerlendirme raporu ve güncel risk aksiyon planı birleştirilerek bankanın BS risk envanteri oluşturulur. Banka, yılda en az bir defa olmak üzere veya bilgi sistemlerinde meydana gelecek önemli değişikliklerden önce risk analizlerini tekrarlar. Tekrarlanan risk analizi sonuçlarına göre risk aksiyon planı ve BS risk envanterinin güncellenmesi sağlanır. Banka bünyesinde gerçekleştirilen BS iç kontrol ve iç denetim çalışmalarının sonuçlarının veya tespit edilen bulguların risk envanterine girdi teşkil etmesi sağlanır.

(7) Bankanın kurumsal risk yönetimi sürecinin, BS risklerini de kapsamı esastır. BS risklerinin bankacılık faaliyetlerinden kaynaklanan diđer risklerin de bir arpanı olabileceđi dikkate alınarak banka genelinde, bilgi sistemlerinden kaynaklanan riskleri de ierecek Őekilde, bütünlüŐik bir risk yönetim metodolojisi uygulanır. BS risk yönetim süreci ıktılarından elde edilen verilerin bankanın bütünlüŐik risk yönetim erevesinin bir parası haline gelmesi sađlanır. Bilgi sistemlerinden kaynaklanan riskler ele alınırken geliŐen yeni teknolojilerin getireceđi riskler ayrıca deđerlendirilir. BS risk envanteri kapsamında riskler takip edilerek yönetim kuruluna ve üst düzey yönetime yılda en az bir defa raporlanır.

ÜÜNCÜ BÖLÜM

Bilgi Güvenliđi Yönetimi

Bilgi güvenliđi organizasyonu, roller ve sorumluluklar

MADDE 8 - (1) Banka bünyesinde bilgi güvenliđinin sađlanmasında nihai sorumluluk yönetim kuruluna aittir. Yönetim kurulu, bilgi sistemlerine iliŐkin güvenlik önlemlerinin uygun düzeye getirilmesi hususunda gerekli kararlılıđı göstermekle ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynađı tahsis etmekle yükümlüdür. Bu sorumluluk kapsamında yönetim kurulu, banka genelinde uygulanmasını gözetmekle yükümlü olduđu bir bilgi güvenliđi yönetim sistemi tesis eder. Bilgi güvenliđi yönetim sisteminin ulusal veya uluslararası standartları ya da en iyi uygulamaları referans alması ve aŐađıdaki faaliyetleri iermesi esastır:

- a) Bilgi varlıklarına yönelik olarak düzenli bir Őekilde tehdit ve risk deđerlendirme alıŐmalarının yapılması,
- b) Bilgi varlıklarının sınıflandırılarak varlık sahipliklerinin belirlenmesi ve varlık sınıflarına uygun güvenlik önlemlerinin alınması,
- c) Bilgi güvenliđi ihlaline iliŐkin olayların izlenmesi ve raporlanması,
- ) Banka genelinde verilen bankacılık hizmetlerinde, görevler ayrılıđı prensibi ile tutarlı etkin bir kimlik dođrulama ve erişim yönetimi tesis edilmesinin sađlanması,
- d) Bilgi güvenliđinin sađlanmasına iliŐkin kontrollerin ve tesis edilen yapıların test edilmesi ve test sonuçlarının takip edilerek raporlanması,
- e) Bilgi varlıklarına yönelik güncel güvenlik açıklarının takip edilmesi ve gerekli aksiyonların alınmasının sađlanması,

f) Üst yönetim de dâhil olmak üzere banka çalışanları, dış hizmet sağlayıcılar ve müşteriler gibi bankanın bilgi güvenliğini ilgilendiren paydaşlara yönelik, bilgi güvenliği farkındalığını artıracak çalışmaların yapılması,

g) İş sürekliliği yönetimi kapsamında bilgi güvenliğini ilgilendiren hususların da yer almasının sağlanması,

ğ) Dış hizmet alımlarının yönetimi kapsamında bilgi güvenliğini ilgilendiren hususların da yer almasının sağlanması.

(2) Bilgi güvenliği yönetim sisteminin banka genelinde nasıl uygulanacağı bilgi güvenliği politikası, prosedürleri ve süreç dokümanları ile düzenlenir. Bankanın bilgi güvenliği politikası yönetim kurulu tarafından onaylanır ve banka genelinde çalışanlara ulaştırılması sağlanır. Bu kapsamda bilgi sistemlerine ilişkin kabul edilebilir kullanım standartları belirlenir.

(3) Bilgi güvenliği politikasının oluşturulması ve uygulanması faaliyetleri yönetim kurulu adına Bilgi Güvenliği Komitesi tarafından gerçekleştirilir. Bilgi Güvenliği Komitesine, belirlenen bir yönetim kurulu üyesi veya genel müdür başkanlık eder ve komitenin koordinasyonunu bilgi güvenliği sorumlusu yerine getirir. Bilgi Güvenliği Komitesi toplantılarına bilgi sistemlerinden sorumlu üst düzey yöneticinin, bankanın ilgili iş birimlerinden üst düzey yöneticilerin, insan kaynakları, risk yönetimi birimlerinden ve banka organizasyonunda bulunması durumunda uyum ve hukuk ile ilgili birim ya da pozisyonlardan temsilcilerin de katılması esastır. Bilgi Güvenliği Komitesinin görev tanımları ve çalışma esasları, yönetim kurulu tarafından onaylı olacak şekilde yazılı hale getirilir, yılda en az iki defa toplanması ve yılda en az bir defa yönetim kuruluna rapor sunması sağlanır.

(4) Bilgi güvenliği politikası, prosedürleri ve süreç dokümanları yılda en az bir defa gözden geçirilir. Önemli güvenlik olayları, yeni güvenlik açıkları ya da teknik altyapıdaki önemli değişikliklerden sonra da bunların ayrıca gözden geçirilmesi sağlanır.

(5) Banka bünyesinde, bilgi sistemlerinden sorumlu üst düzey yönetici ve ona bağlı birimlerden meydana gelen BS fonksiyonundan ayrı ve bağımsız olacak şekilde bir BS güvenlik fonksiyonu oluşturulur. BS güvenlik fonksiyonunun doğrudan yönetim kuruluna veya genel müdüre bağlı olması esastır. Bankanın BS güvenlik fonksiyonu, bilgi güvenliği sorumlusu tarafından yönetilir.

(6) Bilgi güvenliği sorumlusu aşağıdaki görevleri yerine getirir:

a) Bilgi güvenliği politikası, prosedürleri ve süreç dokümanlarının oluşturulması, bunların güncellenmesi ve onaya sunulması,

- b) Bilgi güvenliği bakış açısıyla, bilgi varlıklarının sınıflandırılması ve bilgi varlıklarına yönelik gizlilik, bütünlük, erişilebilirlik kriterleri bakımından BS risk yönetimi çalışmalarına aktif katkı sunulması ve yardımcı olunması,
- c) İlgili birimlerle uyum içinde, iş gereksinimleri ve iş hedefleriyle uyumlu banka genelinde bilgi güvenliğinin tesis edilmesi,
- ç) Bilgi güvenliği ile ilgili mevzuat hükümlerine, standartlara, politika, prosedür ve süreç dokümanlarına uyumun takip edilmesi,
- d) Bilgi güvenliği faaliyetlerinin ve testlerinin yürütülmesinin sağlanması ve bunların takip edilmesi,
- e) Önemli projeler ve değişiklikler için bilgi güvenliği gereksinimlerinin belirlenmesi çalışmalarına katkıda bulunulması,
- f) Bankanın bilgi güvenliğini ilgilendiren paydaşlara yönelik bilgi güvenliği farkındalık programının yürütülmesi.

Veri gizliliği

MADDE 9 - (1) Banka, bankacılık faaliyetlerinin yürütülmesinde kullanılan verilerin taşındığı, iletildiği, işlendiği, saklandığı ve yedek olarak tutulduğu ortamlarda gizliliğini sağlayacak önlemleri alır. Verilerin tutulduğu ortamın kâğıt veya elektronik ortam olmasından bağımsız olarak alınacak önlemlerin, gizliliği sağlanmaya çalışılan verilerin gizlilik derecesine uygun olması ve gerekli yerlerde ek kontrollerin tesis edilmesi esastır. Veri barındıran medya ya da cihazların kullanımdan kaldırılması durumunda, içerdikleri verilerin gizlilik derecesine uygun olarak güvenli bir şekilde imha edilmesi sağlanır.

(2) Veri gizliliğini sağlamada kullanılacak şifreleme teknikleri için güncel durum itibarıyla güvenilirliğini yitirmemiş ve günün teknolojisine uygun algoritmalar kullanılır. Kullanılacak şifreleme anahtarları, ilgili algoritmalar için anahtarın geçerli olacağı ve kullanılabilceği zaman zarfında kırılmayacak şekilde uzun seçilir ve ilgili veri ya da operasyonun kritiklik seviyesine göre bu anahtarların geçerlilik süresi belirlenir. Geçerlilik süresi dolan ya da güvenilirliğini yitirdiği tespit edilen şifreleme anahtarlarının kullanımı derhal engellenir. Şifreleme anahtarlarının yaşam döngüsü boyunca güvenliğinin sağlanması, güvenli bir şekilde oluşturulması, müşteri ve personel kullanımına sunulması ve saklanması esastır.

(3) Hassas verilerin farklı güvenlik seviyesine sahip ortamlar arasında iletiminde uçtan uca güvenli iletişimin kullanılması ve bu verilerin şifrelenmiş bir şekilde saklanması esastır. Bankanın personeline

tahsis ettiği hassas veya sır kapsamındaki veri içeren masaüstü, dizüstü ve mobil cihazların içeriğinin şifrenmesi sağlanır ve ağa bağlı sunucu cihazlar üzerinde açık metin halinde hassas verilerin bulunup bulunmadığını belirlemek için sunucu makineleri taranır.

Verilerin paylaşılması

MADDE 10 - (1) Banka, müşterinin kendisinden gelen ve yazılı şekilde ya da kalıcı veri saklayıcısı yoluyla kanıtlanabilir nitelikte olan bir müşteri talebi olmaksızın, faaliyetlerinin ifası sırasında ve her türlü dış hizmet alımlarında bilgi sistemleri aracılığıyla edindiği, sakladığı veya işlediği müşteri sırrı niteliğindeki bilgileri, Kanunda yer alan istisnai haller haricinde yurtiçindeki ve yurtdışındaki üçüncü kişilerle paylaşamaz ve bunlara aktaramaz.

(2) Müşterinin, bilgilerini paylaşmaya dair açık rıza göstermesi verilecek hizmet için bir ön şart haline getirilemez.

Kimlik ve erişim yönetimi

MADDE 11 - (1) Banka, bilgi varlıklarına olan erişimlerin, görevler ayrılığı prensibine göre belirlenmiş ve kullanıcıların sorumluluğu gereği kendileri için tanımlanan erişim kontrolleri uyarınca, ilişkili bilgi varlığının güvenlik sınıfına uygun bir kimlik doğrulama yöntemiyle gerçekleştirilmesini sağlamakla yükümlüdür. Banka, süreçler ve sistemler üzerinde kullanıcılarına sağlayacağı yetkilerin, kullanıcılara görev ve sorumluluklarına uygun roller ve/veya profiller aracılığı ile temin edilmesini sağlar ve kullanıcıların görev tanımlarına uygun uygulama ve sistemler üzerindeki rolleri dokümante eder.

(2) Bilgi sistemleri üzerindeki kullanıcılara uygulanacak kimlik doğrulama mekanizması, kullanıcıların bilgi sistemlerine dâhil olmalarından, işlemlerini tamamlayıp sistemden ayrılmalarına kadar geçecek süreci kapsayacak şekilde tesis edilir ve kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek önlemler alınır.

(3) Banka, bilgi sistemleri üzerindeki kullanıcılara ait kimlik doğrulama bilgilerinin güvenliğine yönelik; kimlik doğrulama bilgilerinin veritabanlarında şifreli olarak veya matematiksel olarak geriye dönüştürülmesi mümkün olmayan yöntemlerle muhafaza edilmesi, kimlik doğrulama amacıyla aktarılırken şifrenmesi, yetkisiz erişimlere veya görevler ayrılığı prensibine aykırı olarak kontrolsüz bir şekilde gerçekleştirilecek değişikliklere karşı korunması, bu veritabanları üzerinde gerçekleştirilen işlemlere ilişkin yeterli iz kayıtlarının tutulması ve bu iz kayıtlarının güvenliğinin sağlanması gibi önlemler alır.

(4) Kullanıcılara uygulanacak kimlik doğrulama mekanizmasının aşağıdaki fonksiyonları yerine getirmesi sağlanır:

- a) Başarısız kimlik doğrulama teşebbüslerinin belirli bir sayıyı aşması halinde ilgili kullanıcının erişimini engellemesi,
- b) Başarısız kimlik doğrulama teşebbüsleri sonrasında, bu teşebbüsü gerçekleştiren kişiye, hatalı girilen kullanıcı adı bilgisi veya parola ile ilgili, böyle bir kullanıcı adının sistemde olmadığı veya parolanın hatalı girildiği bilgisini vermemesi,
- c) Hiçbir işlem yapılmayan hareketsiz oturumlar için oturumu belirli bir süre sonra sonlandırması veya kilitlemesi,
- ç) Birden fazla kullanıcının aynı kullanıcı hesabını kullanabilmesi ya da bir kullanıcının aynı anda farklı oturumlar açabilmesi konusunda bilgi güvenliği sorumlusunun onay verdiği durumlar hariç olmak üzere, aynı kullanıcı için aynı anda birden fazla oturum açılmaya çalışılması durumunda buna izin vermemesi ve kullanıcıya uyarı vermesi.

(5) Kullanıcılara uygulanacak erişim kontrolleri ve atanacak yetkilerin belirlenmesinde görevler ayrılığı prensibi esas alınır. Süreçler ve sistemler, kritik bir işlemin tek bir kişi tarafından başlatılması, onaylanması ve tamamlanmasına imkân vermeyecek şekilde tasarlanır ve işletilir. Banka, görevler ayrılığı prensibinin uygulanmasına yönelik bankacılık ve BS süreçlerinde uygulanacak erişim kontrollerini ve atanacak yetkileri net olarak belirler ve dokümente eder. Erişim yetkilerinin talep edilmesi, yetkilendirilmesi ve yönetilmesi görevlerinin birbirinden ayrılması sağlanır. Görevlerin tam manasıyla ve uygun şekilde ayrıştırılmasının mümkün olmadığı durumlarda, bu durumdan kaynaklanabilecek hata ve suistimalleri önlemeye yönelik risk azaltıcı veya telafi edici ilave kontroller tesis edilir.

(6) Kullanıcılar, geçerli bir iş ihtiyacının mevcut olduğu ve erişimin gerekli olduğu süre zarfında, bilgi varlıklarına erişebilmeleri için yetkilendirilir. Bilgi varlıklarına erişim yetkisi olan kullanıcılar, ilgili bilgi varlığı sahibi tarafından yılda en az bir defa gözden geçirilir. Kullanıcıların görev ve sorumlulukları göz önünde bulundurularak sadece bu görevleri yerine getirmelerine yetecek ve sadece bilmeleri gereken verilere erişmelerini sağlayacak kadar yetkiye sahip olmaları sağlanır.

(7) Ayrıcalıklı yetkilere sahip kullanıcı ve uygulama hesapları ile ilgili asgari olarak aşağıdaki tedbirlerin alınması sağlanır:

- a) Kimlik doğrulamayla birlikte ek güvenlik kontrollerinin uygulanması,

- b) Ayrıcalıklı yetkilerin yalnızca gerekli olan kullanıcılara atanması ve sadece gerekli olan durumlarda bu tür hesapların kullanılması,
- c) Bu tür hesaplar ile gerçekleştirilen işlemleri takip edecek şekilde iz kayıtlarının tutulması ve bunların düzenli olarak gözden geçirilmesi,
- ç) Hesap oluşturulması veya silinmesi gibi işlemler için iz kaydı tutulması ve uyarı üretilmesi,
- d) Yapılan başarısız giriş denemeleri için iz kaydı tutulması ve uyarı üretilmesi,
- e) Hesapların ortaklaşa kullanılmasının engellenmesi veya bu hesapları kullanan gerçek kişilere sorumluluk atayacak tekniklerin kullanılması,
- f) Parolaların güvenli ortamlarda saklanması ve bu parolaların belirli periyotlarda değiştirilmesini sağlayacak konfigürasyonların yapılması,
- g) Parolaların tahmin edilmesi zor ve günün teknolojisine uygun uzunluk ve zorlukta olacak şekilde sıklıkla değiştirilmesi,
- ğ) Sistemsel sebeplerle uygulama hesaplarına yönelik iz kayıtlarının oluşturulamaması veya takip edilememesi durumunda bu hesapların son kullanıcı tarafından kullanımının engellenmesi.
- (8) Acil durumlara özgü yetkilendirmeler geçici olarak yapılır ve bu yetkilendirme süresince gerçekleştirilecek işlemlerin takibine imkân verecek iz kayıtlarının tutulması sağlanır.
- (9) Personelin işten ayrılması ve görev değişikliği gibi insan kaynaklarında yaşanan değişiklikler sonrasında, gecikmeksizin ilgili kullanıcı hesaplarının silinmesi, askıya alınması, kullanıcıya atanmış yetkilerin geri alınması ya da değiştirilmesi gibi işlemler yerine getirilir. İnsan kaynakları değişikliklerine dayanan yetkilendirme işlemleri otomatik olarak gerçekleştirilmiyorsa, manuel değişiklik gerçekleştirme sürecinde görevler ayrılığı prensibi uygulanır ve değişikliği gerçekleştirmeye yetkili personelin faaliyetlerine ilişkin iz kayıtları ile insan kaynaklarındaki değişikliklerin uyumlu olup olmadığı düzenli olarak gözden geçirilir.
- (10) Bilgi sistemleri üzerindeki kullanıcılar için benzersiz kullanıcı tanımlama kodları belirlenir ve zorunlu olmadığı müddetçe ortak veya ön tanımlı kullanıcı hesapları kullanılmaz. Ortak veya ön tanımlı kullanıcı hesaplarının kullanımının zorunlu olduğu durumlarda ise bu kullanıcı hesapları ile işlemi yapan kişiye sorumluluk atamaya yönelik ilave kontroller tesis edilir.
- (11) Kullanıcı parolalarının yönetiminde asgari olarak aşağıdaki tedbirlerin alınması sağlanır:
- a) Sistem tarafından geçici olarak verilen parolaların kullanıcı tarafından sisteme ilk girişte değiştirilmesinin sağlanması,

- b) Kullanıcıların, parolalarını belirlerken tahmin edilmesi zor, günün teknolojisine uygun uzunlukta ve zorlukta parola seçimine zorlanması,
- c) Kullanıcıların, düzenli aralıklarla ve sistem güvenliği ile ilgili bir kuşku oluşması halinde parolalarını değiştirmeye zorlanması,
- ç) Kullanıcıların eski parolalarının hatırlanması suretiyle geriye dönük olarak belirli sayıda eski parolanın kullanılmasının engellenmesi.

(12) Banka, kullanıcı hesaplarına yönelik olarak kilitli hesaplar, devre dışı bırakılmış hesaplar, parola geçerlilik süresini aşan hesaplar ve parola son kullanma süresi hiçbir zaman dolmayacak şekilde ayarlanmış hesaplar için otomatik olarak rapor üreten yöntemler kullanır ve bu raporları gerekli önlemleri alması için ilgili sistem yöneticisine iletir.

(13) Zorunlu bir iş gereksinimi olmadıkça ve bilgi güvenliği sorumlusu tarafından onaylanmadıkça banka personelinin ya da dış hizmet sağlayıcıların yerel yönetici haklarına sahip olması engellenir.

(14) Banka, her kullanıcının normal günlük kullanım ve erişim süresini belirleyerek tipik hesap kullanım profilleri oluşturur. Bu kullanım profilleri, olağandışı saatlerde giriş yapmış, normal giriş sürelerini aşmış ya da genel olarak çalıştığı bilgisayar dışındaki bir bilgisayardan işlem gerçekleştirmiş olan kullanıcıların raporlanarak olağandışı durumların tespit edilmesinde veya uzun süredir hiç bir aktivite göstermeyen pasif hesapların tespit edilip bu tür hesaplar için gerekli bir iş ihtiyacı kalmamış ise bunların kullanımının engellenmesinde kullanılır.

Bütünlük kontrolleri

MADDE 12 - (1) Banka, bilgi sistemleri üzerinden gerçekleşen işlemlerin, kayıtların ve verilerin bütünlüğünün sağlanmasına yönelik gerekli tedbirleri alarak bunların doğruluğunu, tamlığını ve güvenilirliğini temin eder. Bütünlüğü sağlamaya yönelik tedbirler verinin iletimi, işlenmesi ve saklanması aşamalarının tamamını kapsayacak şekilde tesis edilir. Dış hizmet sağlayıcılar nezdinde gerçekleşen işlemler için de aynı yaklaşım gösterilir.

(2) Bilgi sistemlerine ilişkin işlemlerin doğruluğu ve güvenilirliği asgari olarak, yapılmak istenen işleme ait anahtar öneme sahip bilgilerin işlemin başlangıcından tamamlanışına kadar doğruluğunu yitirmemesini ve yapılmak istenen işlemin kendinden beklenen sonucu yerine getirmesini; tamlığı ise asgari olarak bütün işlemlerin hata üretmeden gerçekleşmesini ve mükerrer olmamasını gerektirir.

İz kayıtlarının oluşturulması ve takibi

MADDE 13 - (1) Banka, bilgi sistemlerinin ve faaliyetlerinin boyutu ve karmaşıklığıyla orantılı olacak şekilde bilgi sistemleri dâhilinde gerçekleşen işlem ve olaylara ilişkin etkin bir iz kayıt mekanizması tesis eder. İz kayıtları, işlemin doğasına uygun detay ve içerikte, asgari olarak aşağıdaki bilgileri barındırır:

- a) Kaydı oluşturan sistem,
- b) Kaydın oluşturulduğu tarih, saat ve zaman dilimi bilgisi,
- c) Kaydı oluşturan işlem ya da olayla birlikte, gerçekleştirilen değişikliğin ne olduğunu gösteren bilgi,
- ç) Kaydın ilişkili olduğu tekil kullanıcıyı veya sistemi gösteren bilgi.

(2) Tesis edilecek iz kayıt mekanizmasının, yaşanan bilgi güvenliği olaylarının sonradan incelenmesine ve bunlar hakkında güvenilir delillerin elde edilmesine imkân tanıyacak nitelikte olması sağlanır.

(3) Bilgi sistemleri dâhilinde gerçekleşen ve bankacılık faaliyetlerine ait kayıtlarda değişikliğe sebep olan işlemler ile hassas ya da sır kapsamındaki verilere erişilmesine veya bunların sorgulanmasına, görüntülenmesine, kopyalanmasına, değiştirilmesine yönelik işlemler ve kritik bilgi varlıklarına yönelik erişim yetkilerinin verilmesine, değiştirilmesine ve geri alınmasına yönelik aktiviteler ile bu varlıklara yönelik yetkisiz erişim teşebbüslerine ilişkin iz kayıtları asgari beş yıl boyunca banka nezdinde saklanır.

(4) Bankanın, web servisleri, API ya da benzeri metotlarla diğer kurum veya kuruluşlar nezdinde tutulan verilere ilişkin yaptığı sorgulamalar ve bu sorgulamaları hangi amaçla yaptığına ilişkin iz kayıtları beş yıl boyunca banka nezdinde saklanır ve bu tür sorgulamalara ilişkin iz kayıtları en geç aylık periyotlarla raporlanarak yetkisiz ya da amaç dışı sorgulama yapıp yapılmadığına dair inceleme yapılır ve bu incelemeden elde edilen sonuçların gerekleri yerine getirilir.

(5) İz kayıtları güvenilir ortamlarda yedeklenir ve ihtiyaç duyulması halinde makul bir sürede bu yedeklerden geri dönüş sağlanarak inceleme yapılmasına imkân verecek şekilde banka nezdinde saklanır.

(6) İz kayıtlarının bütünlüğünün bozulmasının önlenmesine ve herhangi bir bozulma durumunda bunun tespit edilebilmesine ilişkin teknikler kullanılır. İz kayıtlarına, bilmesi gerektiği kadar prensibine uygun olarak sadece erişim yetkisi verilen kişilerin ulaşabilmesi ve kayıt sisteminin her türlü yetkisiz değişiklik ve müdahalelere karşı korunması sağlanır. Kullanıcıların kendi faaliyetlerine

ilişkin iz kayıtlarına müdahalesi engellenir ve iz kayıt sisteminin durdurulmasını önlemeye veya durdurulması halinde bu durumu tespit etmeye yönelik teknikler kullanılır.

(7) Banka, iz kayıt sisteminin önceden belirlenmiş ve belirli periyotlarla güncellenen senaryolar çerçevesinde düzenli olarak gözden geçirilmesine, takip edilmesine ve olağan dışı durumlar ile riskli işlemlerin raporlanmasına ilişkin süreçleri tesis eder. Olağan dışı durumlar ile riskli işlemlere yönelik rapor üretilmesi ve rapor sonuçlarının banka denetim birimlerince takip edilmesi sağlanır.

(8) Banka, dış hizmet sağlayıcıları tarafından tutulan iz kayıtlarının kendi standartlarına uygunluğunu ve bu iz kayıtlarının kendisi tarafından erişilebilir olmasını temin eder.

Ağ güvenliği

MADDE 14 - (1) Banka, gerek kendi kurumsal ağı gerek dış ağlardan gelebilecek tehditler için gerekli ağ güvenlik kontrol sistemlerini tesis eder. Güvenlik önlemlerinin tesis edilmesinde, bir güvenlik katmanının aşılması halinde diğer güvenlik katmanının devreye girdiği katmanlı güvenlik mimarisi esas alınır.

(2) Banka, dış ağı ve iç ağı arasındaki trafiği kontrol altında tutmak için gerektiği şekilde konfigürasyonu yapılmış ve sürekli gözetim altında tutulan güvenlik duvarı çözümleri ile saldırıları tespit edebilecek ve önleyebilecek günün teknolojisine uygun sistemler kullanır.

(3) İç ağdan gelebilecek tehditlerin etkisini azaltmak ve banka iç ağının farklı güvenlik hassasiyetine sahip alt bölümlerini birbirinden ayırarak kontrollü geçişi temin etmek üzere banka iç ağındaki her bir servise ilişkin trafiğin yalnızca kendisi için gerekli olan ağ segmentlerine ulaşmasını sağlayacak şekilde banka iç ağı alt bölümlere ayrılır. Farklı ağ segmentleri arasındaki veri trafiğinin güvenliği sağlanır. İç ağa sadece yetkilendirilmiş cihazların bağlanabilmesi sağlanır.

(4) Hassas veya sır kapsamındaki verilere sahip sistemlerin özel iç ağda bulunması ve hiçbir şekilde doğrudan internetten erişilemiyor olması sağlanır. Özel iç ağdaki sistemlerle yalnızca vekil uygulamalar veya güvenlik duvarı cihazları üzerinden iletişim kurulur.

(5) Ağ üzerinde kimlik ve erişim yönetimine yönelik kurulan etki alanı yönetimi sunucuları gibi yapıların bankaya özgü oluşturulmuş olması ve banka dışındaki başka bir etki alanı ya da benzerinin parçası olmaması esastır.

(6) Kritik ağ segmentlerine yapılan bağlantılar düzenli olarak tespit edilerek bu bağlantıların her biri için gereksinim değerlendirmesi yapılır ve gereksiz bağlantıların sonlandırılması sağlanır.

(7) Bilgi güvenliği sorumlusu tarafından onaylanmadıkça banka personeli ya da dış hizmet sağlayıcıları tarafından banka içi uygulama ve sistemlere, banka dışından uzaktan erişim gerçekleştirilmez. Uzaktan erişimin gerçekleştiği hallerde ise çok bileşenli kimlik doğrulamaya dayanan güvenli bağlantı yöntemleri uygulanır, erişimlere ilişkin iz kayıtları tutulur, bağlantının süresi ve bağlantının yapılabileceği cihazlar kısıtlanır ve kullanıcı belli aralıklarla kimliğini tekrar doğrulamaya zorlanır.

(8) İnternet üzerinden veya banka dış ağından görünür olan sunucu ve sistemler, görünür olmalarını gerektirecek geçerli bir iş ihtiyacı olup olmadığının tespit edilmesi amacıyla düzenli olarak kontrol edilir ve eğer gerekli değilse bu sunucu ve sistemlerin banka iç ağına taşınması ve iç ağ IP adreslerine sahip olması sağlanır.

(9) Banka, iç ağından dış ağa akan trafik içeriğini kontrol eder. Yapılacak içerik kontrolünün, zararlı IP adreslerine olan trafik akışını ve hassas veriler ile sır kapsamındaki verilerin sızdırılmasını engelleyecek nitelikte olması ve oturum bilgilerini kayıt altına alarak olağan dışı uzun süreli oturumları tespit edecek ve bunlar için uyarı üretebilecek yetenekte olması sağlanır.

(10) Bankadan gönderilen e-postalar için e-posta sunucularında gönderici kimliğini doğrulayıcı teknikler kullanılır.

Güvenlik konfigürasyonu yönetimi

MADDE 15 - (1) Banka; masaüstü, dizüstü, mobil cihazlar ve sunucuları üzerindeki işletim sistemi, veritabanları ve uygulamalar ile güvenlik duvarları, yönlendirici ve anahtarlama cihazları gibi ağ cihazları için sıkılaştırılmış ve test edilmiş güvenli standart konfigürasyon bilgilerini oluşturur. Bu standart konfigürasyon bilgileri, standart konfigürasyondan sapmalar veya standart konfigürasyondaki güncellemeler değişiklik yönetiminin bir parçası olarak kayıt altına alınır ve onay mekanizmasına tabi tutulur. Güvenli standart konfigürasyon dışında kalacak her türlü değişiklik isteği için bu değişikliği gerektiren iş gereksinimi ve bu iş gereksinimine ihtiyaç duyan iş sorumlusunun kim olduğu ve gereksinim süresi gibi bilgiler de kayıt altına alınır.

(2) Birinci fıkradaki kontrollere ek olarak, banka kullanmakta olduğu veya ihtiyaç duyabileceği uygulamalar için bir beyaz liste uygular. Böylelikle yalnızca ihtiyaç duyulan uygulamaların sistemlerde yüklü olması ve bu beyaz liste dışındaki herhangi bir uygulamanın sistemlere yüklenmesinin veya çalıştırılmasının engellenmesi sağlanır. Banka aynı zamanda, sistemleri üzerinde beyaz listede yer almayan herhangi bir uygulamanın yüklü olup olmadığına yönelik düzenli olarak tarama gerçekleştirir. Beyaz listedeki uygulamaların çalıştırılabilir dosyalarının veya bunların

kullandığı kütüphane dosyalarının zararlı yazılımlar yoluyla değiştirilip değiştirilmediği, dosya bütünlük kontrol araçları kullanılarak kontrol edilir.

(3) Banka; masaüstü, dizüstü, mobil cihazlar ve sunucular üzerindeki işletim sistemleri için bu işletim sistemlerinin tipi, versiyon numarası, yama seviyesi ve üzerinde yüklü olan veritabanları ve uygulamaların listesini gösterecek şekilde bir yazılım envanteri tutar. Kullanılacak yazılım envanterinin aynı zamanda donanım envanteri ile de entegre olması ve tek bir noktadan hangi donanım üzerinde hangi yazılımların olduğu bilgisinin takip edilebilir olması sağlanır.

(4) Bankanın masaüstü ve dizüstü makineleri ile sunucuları, bu makinelere taşınabilir bir medya veya harici cihaz takıldığında otomatik olarak içeriği oynatmayacak şekilde yapılandırılır ve zararlı yazılım engelleme araçları bu tür cihazlar takıldığında otomatik olarak bu cihazları tarayacak şekilde ayarlanır. Bunun yanında bu tür harici cihazların makinelere bağlanacağı bağlantı arayüzlerinin ön tanımlı olarak kullanıma kapatılarak bu tür cihazların kullanımının yalnızca iş gereksinimi olan kullanıcılarla sınırlı tutulması ve harici cihazları kullanma denemesi yapılan durumların da takip edilmesi sağlanır.

(5) Ağa bağlı her bir sistem üzerindeki portların, protokol ve servislerin sadece gerekliliği onaylanmış iş ihtiyaçlarına istinaden açık ve çalışıyor olması sağlanır. Bu doğrultuda, güvenli bir baz konfigürasyonu temel alınarak önemli sunucu ve sistemler için düzenli olarak port taraması gerçekleştirilir ve güvenli baz konfigürasyonda bulunmadığı halde açık durumda olan portların kapatılması sağlanır.

Güvenlik açıkları ve yama yönetimi

MADDE 16 - (1) Bankacılık faaliyetlerini kesintiye uğratacak veya önemli ölçüde olumsuz etkileyecek durumların ortaya çıkma olasılığını azaltmak için sistem, yazılım ve cihazlardaki güvenlik açıklarını hızlı ve etkin bir şekilde ele alacak bir güvenlik açıkları ve yama yönetimi süreci tesis edilir. Güvenlik açıkları ve yama yönetimi süreci kapsamında gerçekleştirilen faaliyetler değişiklik yönetiminin bir parçası olarak kayıt altına alınır ve onay mekanizmasına tabi tutulur. Bu süreç kapsamında aşağıdaki faaliyetler yerine getirilir:

- a) Uygulanacak yamaların güvenilir bir kaynaktan gelmesini sağlayacak ve bunu doğrulayacak teknikler kullanılması,
- b) Banka tarafından kullanılan sistem, yazılım ve cihazlarda yer alan güvenlik açıklarının ve bu açıklara yönelik yamaların tespit edilmesi,
- c) Tespit edilen yamaları uygulamanın ya da uygulamamanın etkisinin değerlendirilmesi,

- ç) Uygulanacak yamaların uygulama öncesi test edilmesi,
- d) Yamaların nasıl uygulanacağına ilişkin metotların tanımlanması,
- e) Uygulanan ya da uygulanmamasına karar verilen yamalarla ilgili olarak bilgi güvenliği sorumlusuna düzenli rapor verilmesi,
- f) Yamaların yanlış uygulanması ya da uygulanması sırasında sorun çıkması halinde sorunun ne şekilde çözüme kavuşturulacağına dair metotların tanımlanması,
- g) Uygulanamayan yamaların gidermeye çalıştığı güvenlik açıklarına ilişkin riskleri azaltmaya yönelik telafi edici kontrollerin tesis edilmesi.

(2) Sağlayıcı veya üretici desteği biten sistem, yazılım ve cihazlar artık güncellenemediğinde, bunlar için yüklenebilen en son güncellemelerin günün şartlarına göre artık güvenli olmaması ve telafi edici kontroller ile de makul seviyede bir güvenlik sağlanamaması halinde sistem, yazılım ve cihazlar kullanımdan kaldırılır.

(3) Banka, ağa bağlı olan sistem ve cihazlarına yönelik olarak otomatik güvenlik açığı tarama araçları kullanır. Tespit edilen her bir güvenlik açığıyla ilgili olarak bilgi güvenliği sorumlusuna ve açığın tespit edildiği sistemden sorumlu sistem yöneticisine en kritik güvenlik açıklarını öncelikli olarak listeleyecek şekilde raporlama yapılır.

(4) Banka, masaüstü ve dizüstü makineleri ile sunucularını, sürekli bir şekilde izleyerek üzerindeki zararlı yazılımları tespit etmekle yükümlüdür.

(5) Banka, e-posta sunucusuna gelen ve giden e-postaları tarayarak zararlı yazılım barındıran ya da bankanın iş ihtiyaçları doğrultusunda gereksiz olan eklentiler içeren e-postaları engelleyecek çözümler kullanır.

Fiziksel güvenlik kontrolleri

MADDE 17 - (1) Kritik bilgi sistemleri, uygun güvenlik engelleri ve giriş kontrollerine sahip veri merkezleri, sistem odaları, ağ ekipman odaları gibi güvenli alanlarda barındırılır. Bu alanlara erişim, sadece erişim yetkisine sahip olması gereken personelle sınırlandırılır, erişim yetkileri düzenli olarak gözden geçirilir ve güncellenir.

(2) Banka, veri merkezlerinin yerlerini seçerken doğal riskleri ve çevresel tehditleri göz önünde bulundurur. Binaların, barındırdıkları bilgi işlem tesislerinin varlığını açık edecek işaretler ve bilgiler bulundurmaması sağlanır.

(3) Banka, veri merkezlerinin çalışmasını olumsuz etkileyebilecek elektrik kesintisi, yangın, duman, sıcaklık, su, toz ve nem gibi çevresel koşulları izleyecek sistem ve sensörler kullanır, bunların bakımlarını düzenli olarak yapar.

(4) Birinci fıkra kapsamında yetkilendirilen personel dışında kalan herhangi bir banka personeli, ziyaretçi, dış hizmet sağlayıcı ya da yüklenici firma personelinin veri merkezlerine ve kritik bilgi sistemlerine erişimleri onay mekanizmasına tabi tutulur, veri merkezindeki çalışmalarını boyunca faaliyetleri yakından izlenir ve mutlaka kendilerine refakat edilir. Veri merkezlerine ve sistem odalarına yapılan erişim talepleri ve onayları ile bu erişimler kapsamında gerçekleştirilen işlemler ve giriş çıkışlar için iz kaydı tutulur. Bu alanlar için kör nokta barındırmayacak ve en az bir yıl süreyle kayıt saklayacak şekilde kamera kayıt sistemleri kullanılır. Kamera kayıt sistemleri tarafından kaydedilen görüntülerin farklı bir konumda yedeklenmesi sağlanır.

Siber olay yönetimi, sızma testi ve siber istihbarat paylaşımı

MADDE 18 - (1) Banka, siber olaylardan sonra bankacılık faaliyetlerini en az etkileyecek şekilde ve mümkün olan en kısa sürede BS hizmetlerini normal işleyişine döndürmek üzere gerçekleşen siber olayların ele alınmasına ve takibine yönelik siber olay yönetimi ve siber olaylara müdahale süreci oluşturur. Yeterli teknik ve operasyonel becerilere sahip bir Kurumsal SOME kurulması, bu Kurumsal SOME'ye ilişkin güncel iletişim bilgilerinin Kuruma iletilmesi ve siber olayların Kuruma ve ilgili yönetim birimlerine raporlanması sağlanır.

(2) Kurumsal SOME siber olay öncesinde, bilgi işlem varlıkları üzerinde rutin sızma testi çalışması yapmak veya yaptırmakla, kayıt yönetimi sistemi arayüzünden rutin olarak iz kayıtlarını takip etmekle, iz kayıtları arasında anlamlı sonuçlar doğurabilecek korelasyonları kontrol etmekle; siber olay esnasında ise, BS fonksiyonunun yapacağı müdahaleyi yönetmekle ve BS fonksiyonunda görevli ilgili personeli koordine etmekle sorumludur.

(3) Siber olayların önem derecelerine uygun olacak şekilde ele alınmasını sağlamak üzere, siber olayların önemlilik sınıflandırmasına yönelik kriterler yazılı hale getirilir ve gerçekleşen her bir siber olayın bu kriterlere göre belirlenen önem düzeyiyle orantılı olan bir zaman zarfında ele alınması ve çözüme kavuşturulmasına yönelik prosedürler ile müdahale planları oluşturulur. Oluşturulan müdahale planlarında öngörülen senaryolar için, faaliyetlerin güvenilir bir şekilde sürdürülmesini sağlayan hızlı, etkili ve düzenli bir tepki süreci tesis edilir. Müdahale planlarının işlerliği yılda en az bir kez test edilir ve test sonuçları üst yönetime raporlanır.

(4) Müdahale planları kapsamında, bilgi sistemlerine ilişkin olayın kaynağını hızlı bir şekilde bulma, yetkili birimlere ulaşma, olayın potansiyel boyutunu, etkisini, hasarı ve etkilenen müşterileri tespit etme ve olayı çözüme kavuşturma süreçleri ele alınır.

(5) Banka, yaşanan bir siber olayın büyüyerek bir krize dönüşmesi, verilerin sızması ya da ifşası ile sonuçlanması, Bilgi Sistemleri Süreklilik Planının ya da ikincil merkezin devreye alınması gibi hallerde derhal Sektörel SOME'yi bilgilendirir. Hassas verilerin ya da kişisel verilerin sızmasına ya da ifşasına yol açan bir siber olayın yaşanması halinde banka tarafından yapılacak değerlendirme sonrasında müşterilerin bilgilendirilmesi sağlanır.

(6) Banka, BS hizmetlerinde ciddi kesintilere veya bozulmalara yol açan önemli siber olaylar için bir kök neden ve etki analizi yapmak ve benzer olayların tekrarını önlemek için iyileştirici önlemleri almakla ve yapılan çalışmaları Sektörel SOME'ye bildirmekle yükümlüdür.

(7) Banka, bilgi sistemleri aracılığıyla sunduğu hizmetlerin tasarımı, geliştirilmesi, uygulanması veya yürütülmesinde görevi bulunmayan bağımsız ekiplere yılda en az bir defa sızma testi yaptırır.

(8) Banka, Kurumun belirleyeceği usul ve esaslar çerçevesinde, tespit ettiği ya da haber aldığı yeni siber tehditler, zararlı yazılımlar, siber olaylar ya da bankacılık sektöründe ortaya çıkan yeni dolandırıcılık yöntemleri hakkında bilgilendirmeleri yapmakla ve dolandırıcılıkla mücadelede erken müdahaleyi sağlamak amacıyla 7/24 irtibat kurulabilecek bir irtibat görevlisi atamakla yükümlüdür.

Bilgi güvenliği farkındalığını artırma

MADDE 19 - (1) Banka genelinde bilgi güvenliği farkındalık seviyesini artırmak için kapsamlı bir bilgi güvenliği farkındalığı eğitim programı oluşturulur. Eğitim programı, bilgi güvenliği politikaları ve standartları ile birlikte, bilgi güvenliği ve verilerin korunması konusundaki bireysel sorumlulukların neler olabileceği ve bilgi varlıklarını korumak için alınması gereken önlemler hakkında bilgi içerir. Bu eğitimler yoluyla bankanın BT kaynaklarına ve sistemlerine erişimi olan herkesin bu kaynakların kullanımı ile ilgili mevzuat ve yönergeler hakkında bilgi sahibi olması sağlanır.

(2) Bilgi güvenliği farkındalığı eğitim programı Bilgi Güvenliği Komitesi tarafından onaylanır ve programın içeriği yılda en az bir defa yeni teknolojiler ve ortaya çıkan yeni riskler dikkate alınarak gözden geçirilir ve güncellenir. Bankanın BT kaynaklarına ve sistemlerine erişimi olan yeni ve mevcut personelin ve ilgili olduğu alanlar doğrultusunda BT kaynaklarına ve sistemlerine erişimi olan dış hizmet sağlayıcıların bu eğitimlerden geçmesi veya eğitimi aldıklarını belgelendirmeleri ve eğitim programı güncellendikçe ilgili kişilerin güncellenen kısımlarla ilgili tekrar eğitim alması sağlanır.

(3) Banka, bilgi güvenliği farkındalığını artırmak üzere eğitim programının haricinde kurum içi bültenler hazırlar, varsa banka iç portalında bilgi güvenliği ile ilgili bir bölüm oluşturur, çalışanlarına periyodik olarak bilgi güvenliğiyle ilgili hatırlatma mesajları gönderir, çalışanlara yönelik düzenli olarak bilgi güvenliği farkındalığını ölçecek anketler yapar.

(4) Banka bu madde kapsamındaki farkındalık artırıcı çalışmaların etkinliğini doğrulamak ve geliştirilmesi gereken eksiklikleri tespit etmek amacıyla gerekli çalışmaları yapar. Güncel saldırı yöntemlerini dikkate alarak gerekli sosyal mühendislik senaryoları üzerinden çalışanlara yönelik periyodik testler gerçekleştirir ve bu testlerden geçemeyen çalışanlara yönelik ilave hedefli eğitimler verilmesini sağlar.

DÖRDÜNCÜ BÖLÜM

Sistem Geliştirme ve Değişiklik Yönetimi

Bilgi mimarisinin tanımlanması

MADDE 20 - (1) Banka, bilgi sistemleri yoluyla işlenecek ve saklanacak verilerin bütünlüğünü ve tutarlılığını sağlayacak, veri tekrarını en aza indirecek bir kurumsal bilgi mimarisi modelini esas alır.

(2) Banka, bilgi mimarisi modelinin bir parçası olarak veri söz dizimi kurallarını belirler ve bu söz dizimi kuralları doğrultusunda verilerin uyması gereken standart yapıları tarif eden veri sözlüğünü oluşturarak yazılım geliştirme ve veritabanları yönetimi süreçlerinde bu veri sözlüğünün kullanılmasını sağlar. 6 ncı madde kapsamında oluşturulan veri envanteri ile bilgi mimarisi modelinin entegre olması sağlanır.

(3) Bilgi mimarisi modeli, veri söz dizimi kuralları ve veri sözlüğünün merkezi olarak takibi ve yönetilmesi için ilgili sorumluluklar atanır, uygulamalarda veya veritabanlarında meydana gelecek mimariyi etkileyen değişiklikler için sorumluların onayı alınır ve değişikliklerin bilgi mimarisi modeline yansıtılarak güncellenmesi sağlanır.

Proje yönetimi

MADDE 21 - (1) Banka, yürüteceği BS projelerinin doğru önceliklendirilmesini ve koordinasyonunu sağlamak ve bu projeler yoluyla edinilecek ya da geliştirilecek bilgi sistemlerinin, zamanında ve gerekli işlevsellik düzeyine sahip olacak şekilde teslim edilmesini sağlamak üzere bir proje yönetim süreci uygular. Proje yönetim süreci, projelerin büyüklüklerine, karmaşıklıklarına ve riskliliklerine göre uygun bir yönetim yapısı tesis edilmesini sağlar.

(2) Hangi kapsamdaki işlerin proje olarak sınıflandırılacağına ve bunların önceliklendirilmesine ilişkin somut kriterler tanımlanır ve bu kriterler çerçevesinde proje talepleri ele alınarak projelerin işletilmesi ve gözetimi gerçekleştirilir.

(3) Süreç, asgari olarak proje gereksinimlerinin belirlenmesi, rol ve sorumlulukların belirlenmesi, zaman ve kaynak planlamasının yapılması, proje kapsamında gerçekleştirilecek faaliyet detaylarının tanımlanması, proje aşamalarının ve çıktılarının tanımlanması, anahtar bağımlılıkların belirlenmesi, kalite temin, risk değerlendirmesi ve onay adımlarını içerir.

(4) Proje gereksinimlerinin belirlenmesi adımı, gereksinimlere detaylı olarak yer verilen bir analiz dokümanı hazırlanır. Bu analiz dokümanında, proje yaşam döngüsü boyunca yasal gereksinimler, kimlik doğrulama, yetkilendirme, erişim kontrolleri, onay mekanizmaları, şifreleme, iz kaydı gibi güvenlik ve gizlilik gereksinimleri, beklenen kullanım yoğunluğu ve kullanıcı sayısı gibi performans gereksinimleri ile hizmet seviyeleri ve yedekleme düzeni gibi erişilebilirlik gereksinimlerinin neler olabileceği belirlenir.

(5) Banka, BS projeleri için proje planı hazırlar ve proje planlarında, projenin her aşamasında gerçekleştirilecek çıktılar ve ulaşılması gereken kilometre taşları açıkça belirtilir. Proje planlarında belirtilen kilometre taşlarına ulaşılmasını ve teslimin zamanında gerçekleştirilmesini sağlamak ve proje risklerini yönetmek üzere, banka proje ilerleyişini takip eder ve gerektiğinde BS Yönlendirme Komitesine, projelerin gidişatı ve karşılaşılan sorunlara ilişkin bilgilendirme yapılmasını sağlar.

Sistem geliştirme, taşıma ve kurulum

MADDE 22 - (1) Banka, yazılım geliştirme sürecinde görevler ayrılığı prensibine uygun olarak geliştirme, test ve üretim ortamlarının birbirinden ayrı tutulmasını sağlar. Sistem ve uygulamaların geliştirilme süreci, kaynak kodlarının tek bir kişi tarafından hazırlanıp derlenerek geliştirme, test ve üretim ortamları arasında taşınmasına imkân vermeyecek şekilde görevler ayrılığı prensibine uygun olarak işletilir.

(2) Yalnızca geçerli bir iş ihtiyacı ve zorunluluk halinde ve sadece onay mekanizmasından geçmek suretiyle, yazılım geliştirmeden sorumlu personelin üretim ortamına erişimine izin verilebilir. Böyle durumlarda dahi personelin üretim ortamında gerçekleştirdiği işlemler takip edilir ve kayıt altına alınır. Banka üretim ortamına erişimde kullanılan yöntemleri kayıt altına alarak yazılı hale getirir ve üst düzey yöneticilerce onaylanmasını sağlar.

(3) Bankanın yazılım geliştirme sürecinde bulunan aşamalar ve bu aşamalara ilişkin geçiş koşulları, dokümantasyon gereksinimleri, kodlama standartları ve iş birimleri ile diğer paydaşların hangi

aşamalarda sürece dâhil olacağı ve onaylarının alınacağı yazılı olarak belirlenir. Yazılım geliştirme süreci kapsamında, dış hizmet alımları da dâhil olmak üzere bankanın yazılım geliştirme yaşam döngüsüne, mevzuat gereksinimleri ile banka içi politikalara uyumu sağlanır.

(4) Yazılım kalitesini artırmak ve güvenlik açıklarını en aza indirmek amacıyla bilgi güvenliği, yazılım geliştirme yaşam döngüsünde dikkatle ele alınır. Yazılım geliştirme veya tedarik sürecinin başından itibaren, iş gereksinimlerinin ve yazılımdan beklenen fonksiyonel gereksinimlerin neler olduğunun belirlenmesinin yanında, yetkilendirme ve erişim, kimlik doğrulama, veri bütünlüğü, iz kayıtları, istisnai durum yönetimi gibi güvenlikle ilgili gereksinimlerin neler olduğu da belirlenir ve bankanın güvenlik standartlarına, politikalarına ve mevzuat gerekliliklerine ilişkin uyum durumu kontrol edilir.

(5) Banka içinde geliştirilen veya dışarıdan tedarik edilen internete açık uygulamalar, kurulumları yapılmadan önce ve bu uygulamalarda yapılan güncellemeler sonrası düzenli olarak yinelenen bir temelde, güvenlik açıkları bakımından taranır.

(6) Alınan hizmetin kritikliği, riskliliği ve tedarikçinin iş dışı kalması olasılığı dikkate alınarak yazılımı dış bir firma tarafından geliştirilen ve kaynak kodu tedarik edilemeyen uygulamalar için üçüncü tarafların da katılımıyla bir yazılım saklama sözleşmesi yapılır. Ürün güncellemelerinin ve program düzeltmelerinin de saklama sözleşmesi kapsamında yer alması sağlanır.

(7) Banka, yazılım geliştirme personelinin, kullandıkları yazılım geliştirme ortamları özelinde güvenli kod geliştirme eğitimlerini almasını sağlar.

(8) Bankanın yazılım geliştirme sürecinde yapılan yeni veri tanımları ya da veri tanımlarında yapılan değişikliklerin bilgi mimarisi ile veri sözlüğü açısından tutarlılığı değerlendirilerek gerekli güncellemelerin yapılması sağlanır.

(9) Yazılım kodlarının geliştirme, test ve üretim ortamları arasında taşınması esnasında bunların içine yetkilendirilmemiş ya da zararlı kod parçalarının eklenmesini engellemek üzere versiyonlama ve sürüm kontrollerine dayanan bütünlük kontrolleri gerçekleştirilir. Üretim ortamına aktarım sırasında ilgili kullanıcı ya da uygulama sahiplerinin onayları alınır.

(10) Test ortamının işletim sistemi, veritabanı yönetim sistemi, entegre olunan uygulamalar ve sistemler itibarıyla üretim ortamını temsil etmesi ve test verilerinin sayı ve nitelikçe üretim ortamında gerçekleşen operasyonu temsil etmesi ve müşterilere ait üretim ortamı verilerinden arındırılması sağlanır.

Uygulama kontrolleri

MADDE 23 - (1) Bankada geliştirilen ya da dışarıdan tedarik edilen uygulamalar, ilgili oldukları bankacılık faaliyetlerini ve iş süreçlerini banka içi politikalara ve mevzuat gereksinimlerine uygun olarak yürütmek ve bu uygulamalara girilen, bu uygulamalar tarafından değiştirilen, işlenen veya üretilen verilerin doğruluğunu, tamlığını, güvenilirliğini sağlamak üzere sistemsal veya manuel kontroller barındırır. Bu kontroller, uygulamaya girdi teşkil edecek verilerin tanımlanması; türü, tipi, formatı ve büyüklüğünün kontrol edilmesi; kaynağının doğrulanması; uygulamanın işlediği verilerin bütünlük ve güvenilirliğinin sağlanması; verilere erişimin görevler ayrılığı prensibine uygun olarak yetkilendirilmesi; gerekli olduğu durumlarda girişçi-onaycı yapısının tesis edilmesi; uygulamanın çıktısı olan verilerin gizliliğinin, bütünlüğünün, mutabakatının ve sadece gerekli taraflara dağıtımının sağlanması gibi fonksiyonları yerine getirir. Banka, uygulama kontrollerinin mümkün mertebe sistemsal kontroller olmasına ve manuel yordamlarla yürütülmemesine dikkat eder, uygulamaların kurulumundan önce banka içi politikalara ve mevzuat gereksinimlerine uyduklarından emin olmak için barındırdıkları kontrolleri test eder ve test sonuçlarını kayıt altına alır.

Değişiklik yönetimi

MADDE 24 - (1) Banka, meydana gelen değişiklikler sebebiyle gerçekleşebilecek hata ve sorunların sayısını ve etkisini en aza indiren, değişikliklerin etkili, hızlı ve kontrollü bir şekilde gerçekleştirilmesini ve değişiklikler sırasında yapılan işlemlerin değişiklik sonrasında da denetlenebilir olmasını sağlayacak etkin bir değişiklik yönetimi süreci tesis eder. Ağ altyapısı, donanım, işletim sistemleri, yazılım gibi bilgi sistemleri öğeleri ile sistem, servis, uygulama konfigürasyonu ve parametrelerinde yapılacak her türlü değişikliğin değişiklik yönetimi süreci çerçevesinde başlatılması, değişiklik talebinin geçerli bir iş ihtiyacına dayalı olması ve görevler ayrılığı prensibine uygun olarak yetkilendirilmesi, test edilmesi, gerçekleştirilmesi, kaydedilmesi ve dokümantasyonu sağlanır. Değişikliklerin, kimlik doğrulaması uygun tekniklerle gerçekleştirilmiş yetkili kullanıcılar tarafından yapılması, bunlar için yeterli iz kaydı tutulması ve tutulan iz kayıtlarının düzenli olarak gözden geçirilmesi esastır.

(2) Banka, bilgi sistemi yazılım bileşenlerinin ana versiyonunun kaydını tutar ve bilgi sistemi bileşenlerinde meydana gelen değişiklikleri, meydana geldiği sırayla ve değişimin gerçekleştiği tarihle birlikte kaydeder.

(3) Değişiklik yönetimi süreci, asgari olarak talep yönetimi, risk değerlendirmesi, yetkili merci onayı, yapılan değişikliğin uygulanması, test edilmesi ve doğrulanması adımlarını içerir. Bu kapsamda;

- a) Değişiklik taleplerinin kayıt altına alınması, sadece yetkili kişilerden gelen değişiklik taleplerinin kabul edilmesi, bunlara ilişkin bir risk ve etki analizi yapılması, gelen taleplerin sınıflandırılması ve önceliklendirilmesi sağlanır.
- b) Değişikliklerin bir güvenlik zafiyetine neden olmadığından emin olmak için, kaynak kod incelemesi de dâhil olmak üzere mümkün olduğunca yüksek güvence veren inceleme faaliyetleri gerçekleştirilir.
- c) Değişiklikler uygun test planları doğrultusunda test edilir ve değiştirilen modüllerin üretim ortamına aktarılmasından önce kullanıcıların ve ilgili birimlerin onayları alınır.
- ç) Değişiklikler ile bağlantılı riskleri en aza indirmek için değişiklik yönetim süreci risk değerlendirmesine bağlı olarak değişiklikten önce, değişiklikten etkilenecek sistem veya uygulamaların yedekleri alınır, üretim ortamına aktarım sırasında veya sonrasında bir sorunla karşılaşıldığında sistem ya da uygulamaların eski bir versiyonuna dönebilmek için bir geri alma planı oluşturulur.
- d) Değişiklikler gerçekleştirildikten sonra, operasyonel prosedürler, konfigürasyon bilgileri, uygulama dokümantasyonu, yardım ekranı ve eğitim materyalleri gibi ilgili sistem ve kullanıcı dokümanları ve prosedürlerinde de değişiklikleri yansıtacak gerekli güncellemeler yapılır.
- (4) Acil durum değişiklikleri kapsamında değişiklik yönetim süreci içerisinde tanımlanan istisnalar dolayısıyla sürecin normal işleyişinde yer aldığı halde alınamayan onaylar ya da oluşturulamayan belge ve kayıtların, değişiklik sonrasında mümkün olan en kısa sürede tamamlanması sağlanır.

BEŞİNCİ BÖLÜM

Bilgi Sistemleri Sürekliliği ve Erişilebilirlik Yönetimi

Birincil ve ikincil sistemler

MADDE 25 - (1) Bankaların birincil ve ikincil sistemlerini yurt içinde bulundurmaları zorunludur.

(2) Birincil sistemlerin kaçınıcı yedeği olduğuna bakılmaksızın birincil sistemlerin her türlü yedeği ikincil sistemler olarak kabul edilir ve birinci fıkra hükmüne tabidir.

(3) Bankacılık faaliyetlerinin yürütülmesi veya Kanun ve mevzuatta tanımlanan sorumlulukların yerine getirilmesi amacını taşımayan banka içi mesajlaşma sistemleri, piyasa izleme platformları gibi sistemler birincil sistemler kapsamında değildir. Bankanın kullanmakta olduğu herhangi bir sistem ya da uygulamanın birincil sistemler kapsamına girmemesi için sistem veya uygulama üzerinden

herhangi bir iş sürecinin yürütülmemesi, hassas veri ya da sır kapsamına girebilecek verilerin işlenmemesi, iletilmemesi ve saklanmaması gereklidir.

(4) İşlemlerin doğası gereği yurt dışı ile etkileşimin gerekli olduğu ödeme veya mesajlaşma sistemleri gibi bankacılık işlemleri hariç olmak üzere, bankanın yurt dışında kurulu bir sistemden herhangi bir onay sürecine tabi olmaksızın bankacılık işlemlerini gerçekleştirebilmesi ve yurt dışı iletişim ağlarıyla bağlantılarının kesildiği durumlarda dahi yurt içinde kurulu bulunan birincil ve ikincil sistemleri aracılığıyla ülke içerisinde bankacılık faaliyetlerini sunmaya devam edebilmesi esastır.

(5) Birincil veya ikincil sistemler kapsamında olan bir faaliyet için dış hizmet ya da bulut bilişim hizmeti alınması halinde, dış hizmet sağlayıcının sunduğu hizmete ilişkin faaliyetleri yürütmede kullandığı bilgi sistemleri ve bunların yedekleri de birincil ve ikincil sistemler kapsamında ele alınır ve yurt içinde bulundurulur.

BT operasyon yönetimi

MADDE 26 - (1) Banka, BS servislerinin tanımlanmış hizmet seviyelerine uygun olarak sunulmasını sağlamak üzere BT altyapısının günlük yönetim ve bakımını yerine getiren bir BT operasyon yönetimi fonksiyonu işletir. BS strateji planındaki hedefler ve iş gereksinimleriyle uyumlu olacak şekilde iş birimlerinin de katılımı ve onayıyla bu servislere ilişkin hizmet seviyeleri tanımlanır.

(2) Banka, BT operasyonel olaylarına derhal müdahale etmek, teknoloji ile ilgili sorunlarda kullanıcılara destek sağlamak, araştırılması ve çözümü için sorunları ilgili BT birimlerine aktarmak, rapor edilen sorunların düzeltilmesine kadar olayların kaydını tutmak, analiz etmek ve takip etmek üzere bir yardım masası fonksiyonu ve problem yönetim sistemi tesis eder.

(3) Banka, bilgi sistemlerinin performansının sürekli olarak izlenmesini ve beklenmedik durumların zamanında raporlanmasını sağlamak için bir performans izleme süreci uygular. Performans izleme süreci, sistem performansını etkilemeden önce sorunların tanımlanmasını ve düzeltilmesini sağlayacak bir erken uyarı fonksiyonu içerir, planlanan iş hedefleri doğrultusunda kapasite planı için ihtiyaç duyulan bilgileri sağlar ve iş yükü tahminlerinin hazırlanmasına yardımcı olur.

(4) Banka, BS strateji planında belirtilen mevcut ve gelecekteki iş gereksinimlerini, tanımlanan hizmet seviyelerine ve iş yükü tahminlerine uygun olarak karşılayabilecek BT kapasitesinin mevcut olmasını sağlamak üzere kapasite yönetimi ve planlaması yapar. Banka, kapasite planının sürekli bir şekilde bakımını ve güncellenmesini sağlar ve BS servislerinin performansını, mutabık kalınan hizmet seviyelerindeki performans hedeflerini karşılayacak veya aşacak şekilde yönetir, kapasite ile ilgili olayların ve problemlerin teşhisi ve çözümünü sağlar.

(5) Banka, ay sonu, resmi tatil sonrası, maaş ödemesi yapılan günler gibi müşterilerin yoğun olarak işlem yaptığı günlerde tekrar eden sistem performansı azalması, kapasitenin yetmemesi, teknik arızalarla karşılaşılması gibi sorunların belirli bir desen takip ettiğini tespit edecek yöntemler kullanmakla ve bu sorunların kök nedenlerini tespit ederek çözüme kavuşturulmasını sağlamakla yükümlüdür.

Erişilebilirlik yönetimi ve yedekleme

MADDE 27 - (1) Banka, herhangi bir donanım veya yazılım bileşeninin beklendiği gibi çalışmadığı durumlarda, sistemin veya bankacılık faaliyetlerinin önemli bir bölümünün çalışamaz hale gelmesini önlemek adına kritik donanım ve sistemler için yedekli çalışma ya da hazırda bekleme düzenleri kurmakla yükümlüdür. Hangi donanım ve sistemlerin kritik olduğu belirlenirken, 28 inci maddede belirtilen BS servisleri ve bunların bağlı olduğu hizmet seviyeleri ile 6 ncı maddede belirtilen bilgi varlıklarının erişilebilirlik gereksinimleri dikkate alınır.

(2) Banka, verilerin erişilebilirliğini sağlamak adına 6 ncı maddede belirtilen her bir verinin erişilebilirlik gereksinimlerine uygun yedekleme düzenini tesis etmekle yükümlüdür. Sistemin alınan yedeğinden geri yüklenebilmesi için, işletim sistemi, uygulama yazılımı ve veriler gibi sistemin çalışmasını sağlayan bileşenler yedekleme prosedürüne dâhil edilir. Yedeklemenin düzgün bir şekilde çalıştığından emin olmak için, geri yükleme işlemleri gerçekleştirilerek yedekleme ortamındaki veriler düzenli olarak test edilir. Yedeklerin taşınırken, uygun şifreleme teknikleri ve fiziksel güvenlik kontrolleri yoluyla korunması sağlanır.

(3) Banka, ağ ve iletişim altyapısından kaynaklanabilecek kesintilere karşı uygun alternatif iletişim kanalları oluşturmakla yükümlüdür.

(4) Banka, hangi sistem, sunucu ve veri yedeklerinin, hangi sıklıkta ve hangi yöntemlerle alındığını ve bu yedeklerin hangi ortam ve konumlarda tutulduğunu, güncel durumu yansıtacak şekilde kayıt altına almakla yükümlüdür.

(5) Banka, soruşturma veya kovuşturma yürüten adli merciler ile Kurumdan gelen veri taleplerini alır almaz bu verilerin bir kopyasını alarak yedeklemekle ya da talep yerine getirilene kadar aslını saklamakla yükümlüdür. Banka verileri, talepte bulunan mercilerin kolaylıkla inceleyebileceği bilinen formatlara dönüştürerek tevdi etmekle veya talepte bulunan mercilere bu verilerle birlikte verilerin incelenmesini mümkün kılan uygulama ve araçları temin etmekle yükümlüdür. Banka, bu fıkra kapsamında kendisine iletilen veri taleplerini geç işleme almasından dolayı mevzuattaki veri saklama sürelerinin geçmiş olduğunu ve bu sebepten verilerin erişilemez olduğunu ileri süremez.

Banka bu fıkra kapsamında kendisinden talep edilen verilere ilişkin almış olduğu kopyaları veya ilave yedekleri en az iki yıl süreyle saklar.

Bilgi sistemleri sürekliliğinin sağlanması

MADDE 28 - (1) Bankacılık faaliyetlerini yürütmeye kullanılan BS servislerinin sürekliliğini sağlamak üzere iş sürekliliği yönetiminin ve planının bir parçası olan BS süreklilik yönetimi süreci ve Yönetim Kurulu onaylı bir BS süreklilik planı hazırlanır, BS süreklilik yönetimi süreci sorumlusu atanır ve BS Süreklilik Komitesi tesis edilir. BS Süreklilik Komitesi, bankanın insan kaynakları, ilgili iş birimleri, BS güvenlik fonksiyonu, ilgili BS birimlerinin temsilcileri ve organizasyonda bulunması durumunda uyum ve hukuk ile ilgili birim ya da pozisyonların temsilcilerinden oluşur ve BS süreklilik yönetimi süreci sorumlusu bu komiteye başkanlık eder. BS Süreklilik Komitesi meydana gelen olaylarla ilgili bütün faktörleri göz önünde bulundurarak kriz durumu olduğunu ilan etmekle, BS planın devreye alınmasına karar vermekle ve diğer kurtarma, süreklilik ve müdahale ekipleriyle koordinasyonu sağlamakla yükümlüdür.

(2) BS süreklilik yönetimi sürecinin ulusal veya uluslararası standartları ya da en iyi uygulamaları referans alması esastır. Bu süreç kapsamında banka BS süreklilik planıyla ilgili olarak aşağıdaki faaliyetleri yerine getirir:

- a) İş etki analizi, risk değerlendirmesi, risk yönetimi, izleme ve test faaliyetlerini içeren bir bilgi sistemleri süreklilik yönetim süreci tesis etmek,
- b) İş birimlerinin de katılımıyla gerçekleştirilen iş etki analizi ve önceliklendirilen iş hedefleri çerçevesinde planı geliştirmek ve kurtarma için gerekli olan işlemleri belirlemek,
- c) Planın uygulanabilir olmasını ve bakımını sağlamak,
- ç) Planın müdahale planları, kapasite planı gibi diğer planlarla ve mevzuat gereksinimleriyle uyumlu olmasını sağlamak,
- d) Yılda en az bir defa, denetimler ve risk analiz çalışmaları sonucu tespit edilen bulgular ve testlerden öğrenilen derslere göre veya iş süreçlerini ya da BS sürekliliğini etkileyen değişikliklerden sonra planın gözden geçirilerek güncellenmesini sağlamak,
- e) Yaşanan acil durum ve felaketlerden kaynaklanan yasal konuları ele almak ve halkla ilişkiler ve basın ile olan iletişimi yürütmek,
- f) İlgili ekiplere ve çalışanlara plan kapsamında eğitim verilmesini ve farkındalığın artırılmasını sağlamak.

(3) Planın hazırlanması sürecinde, bilgi varlıklarının ve tutulan verilerin önem düzeyi değerlendirilerek iş etki analizi çerçevesinde her bir BS servisi için kabul edilebilir kesinti süreleri ile kabul edilebilir veri kayıpları belirlenir ve belirlenen bu limitler doğrultusunda servislerin tekrar erişime açılabilmesine imkân tanıyacak kurtarma prosedürleri geliştirilir. Banka, felaket durumunun sona ermesi sonrasında ikincil merkezden birincil merkeze geri dönüşün sağlanmasına yönelik prosedürleri hazırlar.

(4) Plan kapsamında ikincil merkez tesis edilir. Veri ve sistem yedeklerinin ikincil merkezde kullanıma hazır bulundurulması sağlanır. İkincil merkezin coğrafi olarak, deprem, yangın, patlama, sel, su baskını, heyelan, elektrik ve iletişim hattı kesintisi gibi sebeplerden kaynaklanacak zararlar açısından birincil merkez ile aynı risklere maruz olmaması esastır.

(5) Planın yürütülmesinden sorumlu kritik kişiler ile plan kapsamında sorumluluğu bulunan personel, her yıl sorumlulukları ile orantılı bir detay ve içerikte BS sürekliliği eğitimine tabi tutulur ve plan kapsamındaki görev ve sorumlulukları hakkında bilgilendirilir.

(6) Birincil sistemlerin tamamen devre dışı kaldığı felaket senaryolarında dahi bankanın en geç yirmi dört saat içerisinde faaliyetlerini yeniden sürdürebiliyor olması esastır. Planın etkinliğini ve güncelliğini temin etmek üzere yılda en az bir defa gerçek bir felaket senaryosunu sağlamaya ve ikincil merkez üzerinden faaliyetleri sürdürmeye yönelik testler yapılır. Testlere varsa dış hizmet sağlayıcılar da dâhil edilir, test sonuçları üst yönetime raporlanır ve bu sonuçlara göre plan güncellenir. Bu fıkranın uygulanmasına ilişkin ilave usul ve esasları belirlemeye Kurum yetkilidir.

(7) Planın yürütülmesinden sorumlu kritik kişiler ile plan kapsamında sorumluluğu bulunan personelin ve dış hizmet sağlayıcıların iletişim bilgilerinin geçerliliği ve bu kişilerin göreve hazır olarak ulaşılabilir olduğu, iletişim zinciri testleri ile yılda en az iki defa test edilir. İletişim bilgileri ile planın ve ilgili kurtarma veya geri dönüş prosedürlerinin güncel kopyalarının, yalnızca bilmesi gereken kişilerin erişebileceği şekilde sürekli olarak erişime açık tutulması ve gereken konumlarda kopyalarının bulundurulması sağlanır.

(8) Banka, birincil merkezdeki sistem, sunucu, ağ cihazı ve diğer BT bileşenlerinde yapılan güncellemelerin, yama yüklemelerinin ve konfigürasyon değişikliklerinin ikincil merkezdeki yedeklerinde de aynı şekilde uygulanmasını sağlar, ikincil merkeze kopyalanan veri ve sistem yedeklerinin birincil merkez ile aynı olduğunu garanti edecek bütünlük kontrollerini gerçekleştirir.

(9) Banka, ikincil merkez kapsamına aldığı BS servisleri, sunucu, sistem, uygulama ve verilerin listesi ile ikincil merkez kapsamına almadığı BS servisleri, sunucu, sistem, uygulama ve verilerin listesini güncel durumu yansıtacak şekilde belgelendirir.

(10) Birincil veya ikincil merkez için dış hizmet alınması ya da başka kuruluşlarla paylaşılan bir veri merkezinde barındırılması halinde, veri merkezlerinin bulunduğu konumda veya bölgesel olarak yaşanacak gerçek bir felaket anında birincil ve ikincil merkezdeki çalışma ortamının ve dış hizmet sağlayıcıların bankaya ayıracağı kaynağın, bankanın iş sürekliliğini sağlamayı garanti edecek nitelikte olması esastır.

ALTINCI BÖLÜM

Dış Hizmet Alımı

Dış hizmet alımı sürecinin yönetimi

MADDE 29 - (1) Banka üst yönetimi, dış hizmet olarak alınacak hizmetlerin banka açısından doğuracağı risklerin yeterli düzeyde değerlendirilmesi, yönetilmesi ve dış hizmet sağlayıcı ile ilişkilerin etkin bir şekilde yürütülebilmesine olanak sağlayan yeterli bir gözetim mekanizması tesis eder. Dış hizmet alımı kapsamında;

- a) Alınacak dış hizmetin doğuracağı risklerin tüm yönleriyle değerlendirilmesi,
- b) Dış hizmet sağlayıcının seçiminde gerekli özenin gösterilmesi,
- c) Hizmet alınan dış hizmet sağlayıcılar ile bunların hizmet alanları, iletişim bilgileri ve hizmetlerin sonlanma tarihlerinin yazılı hale getirilmesi,
- ç) Dış hizmet alımına konu edilen hizmetlerin erişilebilirliğinin, performansının, kalitesinin, taahhüt edilen hizmet seviyelerine uyulup uyulmadığının, bu hizmetler kapsamında gerçekleşen güvenlik ihlali olaylarının, dış hizmet sağlayıcının gizlilik, bütünlük ve erişilebilirlik ile ilgili güvenlik kontrollerinin, operasyonel ve finansal durumunun yükümlülüklerini yerine getirmeye uygun olup olmadığının ve sözleşme şartlarına uygunluğunun düzenli aralıklarla takip edilmesi,
- d) Dış hizmet alımı kapsamındaki sistem ve süreçlerin bankanın kendi risk yönetimi, güvenlik ve müşteri mahremiyeti politikalarına uygun olması,
- e) Dış hizmet alımı kapsamında banka verilerinin dış hizmet sağlayıcıya aktarılmasının gerekli olduğu durumlarda, dış hizmet sağlayıcının güvenlik konusundaki prensip ve uygulamalarının en az bankanın uyguladığı düzeyde olması için gerekli tedbirlerin alınması,

f) Dış hizmet alımı kapsamındaki faaliyetlerin banka bünyesinde gerçekleştirilmesi durumunda hangi denetimlere tabi tutulması öngörüülüyorsa, herhangi bir kapsam daraltılmasına gidilmeden dış hizmet sağlayıcının da aynı denetimlere tabi tutulması,

g) Dış hizmet alımına ilişkin hususların banka iş süreklilik planı göz önünde bulundurularak düzenlenmesi ve gerekli önlemlerin alınması,

ğ) Dış hizmet alımının, planlananın dışında sonlanması veya kesintiye uğraması durumlarına ilişkin risklerin yönetilmesine uygun bir çıkış stratejisinin belirlenmesi,

h) Alınan dış hizmetin alt yüklenicilere devrinin bankanın izin vermesi halinde mümkün olması, sağlanır.

(2) Dış hizmet alımına ilişkin koşul, kapsam ve her türlü diğer tanımlama yazılı sözleşmeye bağlanır. Sözleşme, asgari olarak aşağıdaki hususları içerir:

a) Hizmet seviyelerine ilişkin tanımlamalar,

b) Hizmetin sonlanma koşulları,

c) Bankanın iş sürekliliğinin sektöre uğramasını engellemek üzere dış hizmet sağlayıcının alması gereken önlemlere ilişkin hükümler,

ç) Bankanın güvenlik politikası dâhilinde hassasiyet arz eden konulara ilişkin gereklilikler ve gerek hizmet sırasında gerek hizmetin sonlanması halinde dış hizmet sağlayıcının banka ve müşterileri hakkında öğrendiği bilgiler hususunda gizliliğe riayet etmesini sağlayacak hükümler,

d) Dış hizmet sağlayıcı bünyesinde gerçekleşen güvenlik ihlali veya veri sızıntısı gibi olayların derhal bankaya bildirilmesini sağlayacak hükümler,

e) Sözleşmeye konu ürün ve hizmetlerin sahipliği ve fikri mülkiyet haklarına ilişkin hükümler,

f) Sözleşmede dış hizmet sağlayıcı için yükümlülük teşkil eden hükümlerin, alt yüklenici kuruluşlar ile yapılacak olan sözleşmelerde de bağlayıcı maddeler olarak yer almasını sağlayacak hükümler,

g) Dış hizmet alımının, planlananın dışında sonlanmasından veya kesintiye uğramasından kaynaklanacak risklerin yönetilmesine ilişkin hükümler,

ğ) Alınan hizmetin sonlanması halinde, banka ve müşteri verilerinin uygun bir şekilde bankaya teslim edilmesini ve imha edilmesini sağlayacak hükümler,

h) Bankanın tabi olduğu mevzuat hükümlerinin alınan hizmet çerçevesinde dış hizmet sağlayıcılar için de uygulanmasını sağlayacak hükümler,

1) Dış hizmet sağlayıcıların, gerçekleştirdikleri faaliyetlere ilişkin olarak Kurumca talep edilen her tür bilgi ve belgeyi zamanında ve doğru olarak vermekle ve bunlara ilişkin her türlü elektronik, manyetik ve benzeri ortamlardaki kayıtları ve bu kayıtlara erişim ve kayıtları okunabilir hale getirmek için gerekli sistem ve şifreleri incelemeye hazır bulundurmakla ve işletmekle yükümlü olduğuna ilişkin hükümler,

i) Banka ile bağımsız denetçisinin, dış hizmet alınan konuyla ilgili olarak dış hizmet sağlayıcıdan her türlü bilgi ve belgeyi talep etme yetkisinin bulunduğuna ilişkin hükümler.

(3) Banka, ikinci fıkrada belirtilen sözleşmede bulunması gereken yükümlülükleri uygulama imkânının bulunmadığı standart sözleşmeler çerçevesinde yürütülen dış hizmet modelleri ile kritik servis ve hizmetleri edinemez ve kritik iş akışlarını bu tür dış hizmet modelleri yoluyla yürütemez.

(4) Banka, sunmakta olduğu bankacılık hizmetlerine yönelik reklam hizmeti almak istediği arama motoru, sosyal medya platformu gibi sağlayıcıların banka adına verilen sahte reklamları engellemeye yönelik tedbirleri alıp almadığını kontrol eder ve uygun tedbirleri almayan sağlayıcılardan reklam hizmeti alamaz. Banka, reklam hizmeti aldığı arama motoru, sosyal medya platformları gibi sağlayıcılarla yapacağı sözleşmelerde, sahte reklam yayımlanması durumunda, müşteriyi korumak adına, olaya özel gerekli bilgiyi alabileceğine dair hükümleri ekletmek zorundadır. Bankanın bu kapsamda reklam hizmeti almak üzere anlaştığı aracı firmalar ile yapılan sözleşmeler için de bu fıkra hükümleri geçerlidir.

(5) Banka, güvenlik politikasının tanımladığı ilkeler doğrultusunda, dış hizmet alımından kaynaklanan riskleri kontrol altında tutmak üzere gerekli organizasyonel değişiklikleri yapar, idari prosedürleri tanımlar ve dış hizmet sağlayıcıyla ilişkileri yürütecek, yeterli bilgi ve tecrübeye sahip bir sorumlu atar.

(6) Dış hizmet sağlayıcıya verilen erişim hakkı tipleri özel olarak değerlendirilir. Fiziksel veya mantıksal olabilecek bu erişimler için risk değerlendirmesi yapılır, risk değerlendirmesi sonucuna göre ilave kontroller tesis edilir. Risk değerlendirmesi yapılırken ihtiyaç duyulan erişim tipi, erişilen verinin değeri, dış hizmet sağlayıcı tarafından yürütülmekte olan kontroller ve bu erişimin banka bilgilerinin güvenliği üzerindeki etkileri dikkate alınır.

(7) Banka, dış hizmet alımlarında kendisine ve kullanıcılarına ait gizli bilgilerin güvenliğinin sağlanması için gerekli tedbirleri almakla yükümlüdür. Dış hizmet sağlayıcılara verilecek sisteme erişim, veriye erişim veya veriyi görme yetkisi, işin gerektirdiği bilgiyi kapsayacak şekilde

sınırlandırılır. Dış hizmet sağlayıcı tarafından kuruluşa ve kullanıcılarına ait gizli bilgilerin korunmasına yönelik tedbirlerin alınmasını sağlamak bankanın sorumluluğundadır.

(8) Bu Yönetmelik kapsamında belirtilen BS iç kontrol ve iç denetim faaliyetleri dış hizmet alımına konu edilemez ve bankanın kendi personeli tarafından yerine getirilir.

(9) Bankanın bilgi sistemlerinin bir bütün olarak veya kısmen dış hizmet alımına konu edilebilmesi;

a) Bankacılık mevzuatının gerektirdiği bankacılık faaliyet ve yükümlülükleri bakımından bankanın bilgi sistemleri üzerinde yönetim, içerik tasarımı, erişim, kontrol, denetim, güncelleme, bilgi/rapor alma gibi konularla alakalı hususlarda herhangi bir sınırlama olmaksızın karar alma gücünün ve hâkim rolün bankada bulunması,

b) Dış hizmet alımına konu edilen bilgi sistemleri ile ilgili yönetsel tüm detaylara bankanın vâkıf olması,

c) Bankanın veritabanlarına ve verilerine erişim yetkilerinin, kritik bilgi olsun veya olmasın mutlaka bankanın kendi vereceği izinler doğrultusunda gerçekleştirilmesini sağlayacak bir yetkilendirme mekanizması tesis edilmesi ve bankanın kullanmakta olduğu uygulamaların tamamının yetkilendirmesini ve iz kayıtlarının gözden geçirilmesi gibi iç kontrol faaliyetlerini bizzat bankanın kendisinin yapması,

ç) Yazılıma ilişkin fikri mülkiyet hakları saklı olmak üzere, alınan dış hizmet kapsamında oluşan hesap, kayıt ve işlemlere ait her türlü bilgi ve belgenin mülkiyetinin bankaya ait olması,

şartıyla mümkündür.

(10) Kritik bilgi sistemleri ve güvenlik kapsamında alınacak ürün ve hizmetlerin Türkiye'de üretilmesi veya üreticilerinin ar-ge merkezlerinin Türkiye'de bulunması için azami özen gösterilir ve dış hizmet alımında önemli bir kriter olarak değerlendirilir. Bu tür sağlayıcıların ve üreticilerin Türkiye'de müdahale ekiplerinin bulunması şarttır. Kurum, bankaların kullanacağı güvenlik ürünleri ve diğer BT unsurları hakkında ilave şartlar belirlemeye yetkilidir.

(11) Banka, bir dış hizmet olarak bulut bilişim hizmetlerini kullanabilir. Birincil veya ikincil sistemler için bulut hizmeti tek bir bankaya tahsis edilmiş donanım ve yazılım kaynakları üzerinden özel bulut hizmet modeliyle alınabilir. Bunun yanında, sadece Kurum denetimine tabi kuruluşlara tahsis edilmiş donanım ve yazılım kaynaklarının fiziksel olarak paylaşıldığı ancak mantıksal olarak her bankaya özgü ayrı kaynağın atandığı topluluk bulutu hizmet modeliyle dış hizmet alınması Kurul

iznine tabidir. Kurul, gerekli gördüğü hallerde topluluk bulutu hizmeti kapsamına dâhil olabilecek kuruluşları değiştirmeye yetkilidir.

YEDİNCİ BÖLÜM

Bilgi Sistemleri İç Kontrol ve İç Denetim Faaliyetleri

Bilgi sistemleri iç kontrol faaliyetleri

MADDE 30 - (1) Banka ve bankanın dış hizmet sağlayıcıları nezdindeki BS yönetimine ilişkin faaliyetler, bu faaliyetleri destekleyen süreçler ve tesis edilen BS kontrollerinin mevzuata ve banka içi politika, prosedür ve standartlara uyumlu olduğunu kontrol etmek üzere BS iç kontrol fonksiyonu oluşturulur, BS iç kontrol sorumlusu atanır ve BS iç kontrol faaliyetleri bu kişinin sorumluluğunda yürütülür. BS iç kontrol fonksiyonu ilave olarak aşağıdaki faaliyetleri de yerine getirir:

- a) Kontroller sonucunda belirlenen eksikliklerin giderilmesi ve aksiyon alınması amacıyla ilgili birimlere ve üst yönetime bildirimde bulunulması,
- b) Kontroller sonucunda gerekli olduğu anlaşılan süreçsel veya sistemsel iyileştirme önerilerinin ilgili birimlere ve üst yönetime bildirilmesi,
- c) Talep halinde bankanın ürünlerinde ve süreçlerinde planlanan değişiklikler, yenilikler veya banka içi politika, prosedür ve süreç dokümanları hakkında görüş oluşturulması,
- ç) Görev alanına giren kritik süreçlerle ilgili proje ve çalışma gruplarına, kurul ve komitelere katılım sağlanması ve ilgili toplantılarda riski en aza indirmeye yönelik öneriler getirilmesi,
- d) BT yönetimi ve dış hizmet alımından kaynaklı risklerin takibinin sağlanmasına yönelik üst yönetim, denetim komitesi ve iç kontrol birimi yöneticisine periyodik olarak raporlama yapılması,
- e) Bir sonraki yıl yapılacak planlı incelemeleri gösterecek şekilde her yıl BS iç kontrol inceleme planları oluşturulması ve bunların banka denetim komitesinin onayından geçirilmesi.

(2) BS iç kontrol sorumlusunun BS iç kontrol, BS denetimi, BS yönetimi ve kontrollerinin tesisi veya bilgi güvenliği alanlarının herhangi birinde ya da birkaçında toplamda en az beş yıllık mesleki tecrübesinin bulunması şarttır. BS iç kontrol fonksiyonunda görev alacak personelin de, ilgili alanlarda öğrenim durumları itibarıyla veya aldıkları sertifikalarla kanıtlanabilir asgari bilgi ve beceriye sahip olmaları zorunludur.

(3) BS iç kontrol faaliyetleri kapsamında yapılan periyodik kontroller kayıt altına alınır ve yapılan kontrollere ilişkin çalışma kanıtları en az üç yıl banka nezdinde saklanır.

Bilgi sistemleri iç denetim faaliyetleri

MADDE 31 - (1) Banka ve bankanın dış hizmet sağlayıcıları nezdindeki BS yönetimine ilişkin faaliyetler, bu faaliyetleri destekleyen süreçler ve tesis edilen BS kontrollerinin mevzuata ve banka içi politika, prosedür ve standartlara uyumlu olduğu ve bilgi sistemlerine ilişkin iç kontrol ve risk yönetimi faaliyetlerinin etkinliği ve yeterliliği hususunda yönetim kuruluna güvence sağlamak üzere BS iç denetim fonksiyonu oluşturulur, BS iç denetim sorumlusu atanır ve BS iç denetim faaliyetleri bu kişinin sorumluluğunda yürütülür.

(2) BS iç denetim sorumlusunun BS iç kontrol, BS denetimi, BS yönetimi ve kontrollerinin tesisi veya bilgi güvenliği alanlarının herhangi birinde ya da birkaçında toplamda en az beş yıllık mesleki tecrübesinin bulunması şarttır. BS iç denetim fonksiyonunda görev alacak personelin de, ilgili alanlarda öğrenim durumları itibarıyla veya aldıkları sertifikalarla kanıtlanabilir asgari bilgi ve beceriye sahip olmaları zorunludur.

(3) BS iç denetimlerinin kapsamının kritik BS servisleri, süreçleri ve kritik varlıkları içerecek ve bunlara ilişkin güvence verecek derinlikte ve detayda olması esastır. Yıllık olarak denetlenebilir BS alanlarından oluşan bir BS denetim planı oluşturularak banka denetim komitesinin onayından geçirilir.

(4) Bankanın BS iç denetimlerinin sıklığı ve denetim döngülerinin; BS servislerinin, süreçlerinin ve varlıklarının kritikliği ve riski ile orantılı olması sağlanır. Bu Yönetmelikte yer alan hükümlerin tamamının banka tarafından yerine getirildiği konusunda güvence vermek üzere yapılacak BS iç denetimleri için denetim döngüsü iki yılı aşmayacak şekilde belirlenir.

(5) BS iç denetim fonksiyonu tarafından gerçekleştirilecek BS denetimleri için denetim rehberleri ve kontrol listeleri hazırlanarak yazılı hale getirilir ve günün teknolojisine uygun olacak şekilde düzenli olarak gözden geçirilerek güncellenir. Yapılan denetimlere ilişkin çalışma kanıtları en az üç yıl banka nezdinde saklanır.

Bulguların takibi ve güvence sağlanması

MADDE 32 - (1) Banka denetim komitesi, BS iç kontrol, BS iç denetim ve diğer BS denetim çalışmaları sonucu tespit edilen bulguların ele alınması konusuna yeterli zaman ayırır, bu çalışmalar sonucu tespit edilen kritik konuları bizzat gözden geçirir ve gerekli önlemlerin alınması konusunda üst yönetime rehberlik eder. Banka denetim komitesi üyelerinin kompozisyonu, BS iç kontrol ve BS iç denetim raporlarını ve bulgularını uygun bir şekilde değerlendirebilecek mesleki tecrübeye veya bilgi birikimine sahip olacak şekilde oluşturulur.

(2) Banka, BS iç kontrol, BS iç denetim ve diğer BS denetim çalışmaları sonucu tespit edilen bulguların aksiyon planına bağlanarak takip edilmesini sağlar. Bulguların kapatılmasına yönelik olarak aksiyon planında hedef tamamlanma tarihi atanamayan, aşılma, aşma süresi bir seneden fazla uzatılan veya iptal edilen bulgular denetim komitesine düzenli olarak raporlanır ve bu bulgular denetim komitesinde kritik konular olarak ele alınır.

(3) BS iç kontrol ve iç denetim fonksiyonu, tespit ettiği bulguların giderilmesine yönelik olarak denetlenen ilgili birim tarafından alınabilecek önlemler ve aksiyonlara yönelik önerilerde bulunur ya da denetlenen ilgili birimin bu yönde almayı planladığı aksiyonlar konusunda mutabık kalır. Öneri ve aksiyonların uygulamasının tamamlanması neticesinde kapatılabilir duruma gelen bulgulara ilişkin nihai karar, bulgunun sahibi olan BS iç kontrol ya da BS iç denetim fonksiyonu tarafından incelenmesi neticesinde verilir.

(4) BS iç kontrol ve iç denetim fonksiyonları tarafından gerçekleştirilen çalışmalar sonucunda, bankanın BS kontrollerinin incelenmesi ve bağımsız denetim kuruluşları tarafından gerçekleştirilen çalışmalardan bağımsız olarak bu kontroller hakkında bütün önemli kontrol eksikliklerini ortaya koymak üzere bir değerlendirme yapılması ve bu kapsamda;

a) Bankanın BS kontrollerinde, İSEDES Yönetmeliğinin "İç Kontrol Sistemi" başlıklı İkinci Kısım ile bu Yönetmelikte belirtilen usul ve esaslar açısından etkinlik, yeterlilik veya uyumluluğa engel teşkil edecek herhangi bir önemli kontrol eksikliğinin bulunmadığı,

b) Finansal tablolarda önemli yanlış beyana sebep olan veya başta finansal veriler olmak üzere banka açısından hassasiyet arz eden verilerin bütünlüğü, tutarlılığı, güvenilirliği, gereken durumlarda gizliliği ve faaliyetlerin sürekliliğini önemli ölçüde etkileyen bir durumun ya da yöneticiler ile iç kontrol sisteminde kritik görevleri bulunan diğer görevlilerin dâhil olduğu bir suistimalin ya da yolsuzluğun bulunmadığı,

c) Tespit edilen bulgular arasında (a) ve (b) bentleri kapsamına giren hususlar varsa, bunların hepsinin banka denetim komitesine ve yönetim kuruluna raporlandığı,

hususlarında güvence sağlanması esastır.

Personelin eğitilmesi ve kaynak tahsisi

MADDE 33 - (1) BS iç kontrol ve BS iç denetim faaliyetlerinin etkin bir biçimde yerine getirilmesini sağlamak üzere, yeterli nitelik ve sayıda personel istihdam edilmesi ve banka tarafından yeterli kaynağın tahsis edilmesi esastır. BS iç kontrol ve iç denetim fonksiyonlarında görev alacak personelin, yılda en az yirmi saat, üç yılda en az yüz yirmi saat olmak üzere BS iç kontrol, BS denetimi, BS

yönetişimi ve kontrollerinin tesisi veya bilgi güvenliği alanlarında eğitim almaları, konferans ve seminerlere katılımları sağlanır.

(2) BS iç kontrol ve BS iç denetim faaliyetlerinin karşılıklı iş birliği ve bilgilendirmeye dayalı olarak koordineli bir şekilde yürütülmesi, önemlilik arz eden sistem, süreç ve alanların zamanında ve öncelikli olarak değerlendirilmesini sağlayacak şekilde iç kontrol ve iç denetim faaliyetlerinin planlanması ve bu faaliyetler için gerekli kaynakların sağlanması esastır.

ÜÇÜNCÜ KISIM

Elektronik Bankacılık Hizmetleri

BİRİNCİ BÖLÜM

Ortak Hükümler

Kimlik doğrulama ve işlem güvenliği

MADDE 34 - (1) Bu Yönetmelikte aksi belirtilmedikçe, müşteri bilgilerinin görüntülenmesi gibi finansal sonuç doğurmayan işlemler de dâhil olmak üzere elektronik bankacılık hizmetleri için bankaların müşterilerine birbirinden bağımsız en az iki bileşenden oluşan bir kimlik doğrulama mekanizması uygulaması ve bu bileşenlerin kimlik doğrulama sürecinde kullanılmaları esnasında barındırdıkları kimlik doğrulama verilerinin gizliliğini sağlayacak önlemleri alması esastır. Bu iki bileşen; müşterinin “bildiği”, “sahip olduğu” veya “biyometrik bir karakteristiği olan” unsur sınıflarından farklı ikisine ait olmak üzere seçilir. Bileşenlerin bağımsız olması, bir bileşenin ele geçirilmesinin diğer bileşenin güvenliğini tehlikeye atmamasını ifade eder. Müşterinin sahip olduğu bileşenin müşteriye özgü olması ve taklit edilememesi esastır.

(2) Kimlik doğrulamada T.C. Kimlik Kartının kart PIN'i veya biyometrik veri ile birlikte kullanılması veya elektronik imzanın kullanılması hallerinde birinci fıkranın gerekleri yerine getirilmiş sayılır.

(3) Kurum, elektronik bankacılık dağıtım kanalları üzerinden gerçekleştirilebilen işlemler bazında, birinci fıkranın uygulanmasına ilişkin istisna veya ilave güvenlik önlemleri tanımlamaya veya ilave usul ve esaslar belirlemeye yetkilidir. Birinci fıkraya uygun olmayacak şekilde iki bileşenli kimlik doğrulama kullanılmaksızın gerçekleştirilen her türlü işlem için, gerçekleştirilen işlemlerin müşteri tarafından yapıldığını ispat etme yükümlülüğü bankaya aittir.

(4) Kullanıcılara uygulanacak kimlik doğrulama mekanizmasında kullanılacak bileşenlerin üretim aşamalarından başlayarak kullanıcıya ulaştırılmasına kadar geçen sürecin tamamı boyunca güvenliği sağlanır.

(5) Kimlik doğrulamada kullanılacak şifreleme anahtarları; bu anahtarların ele geçirilme ihtimallerini en aza indiren, gizliliğini sağlayan, değiştirilmesini ve bozulmasını önleyen yöntemler barındıracak şekilde müşteri kullanımına sunulur.

(6) Kullanıcılara uygulanacak kimlik doğrulama mekanizmasının, başarısız kimlik doğrulama teşebbüsleri hakkında ilgili kullanıcıya sisteme ilk girdiği anda bilgi vermesi sağlanır. Başarısız teşebbüslerin belirli bir sayıyı aşması halinde müşterinin erişimi için ilave güvenlik önlemleri alınır, başarısız kimlik doğrulama teşebbüslerinin devam etmesi halinde ise ilgili kullanıcının erişimi engellenir.

(7) Banka, mobil bankacılık uygulamasını yükleyerek aktifleştirmiş olan müşterilerine, oturum açma ya da oturumun devamında herhangi bir işlemin doğrulanması için hiçbir şekilde SMS ile OTP ya da doğrulama kodu gönderemez ve bunu bir kimlik doğrulama unsuru olarak kullanamaz. Mobil bankacılık uygulamasının ilk kurulumu, aktifleştirilmesi, yeniden aktifleştirilmesi aşamalarında ya da uygulamanın kullanılamaz olması durumunda SMS ile OTP ya da doğrulama kodu gönderilmesi bu fıkra hükmüne aykırılık teşkil etmez.

(8) Banka, SIM kart değişikliği gerçekleştirmiş veya numara taşıma yoluyla elektronik haberleşme işletmecisini değiştirmiş müşterilerini Türkiye’de yerleşik mobil haberleşme işletmeleriyle gerekli entegrasyonu sağlayarak SMS OTP göndermeden önce belirler ve ilgili müşterilere, değişiklikler teyit edilmediği müddetçe, değişikliğin yapıldığı tarihten itibaren 90 gün boyunca elektronik bankacılık hizmetleri sunulurken SIM karta dayalı unsur kimlik doğrulama unsuru olarak kullanılamaz. Değişiklikler teyit edilirken iki bileşenli kimlik doğrulama kullanılmaksızın gerçekleştirilen her türlü işlem için, gerçekleştirilen işlemlerin müşteri tarafından yapıldığını ispat etme yükümlülüğü bankaya aittir.

(9) Müşterilere kimlik ya da işlem doğrulama amacıyla kullanılacak tek kullanımlık parolaların, tahmin edilmesi zor olacak şekilde yeterli uzunlukta, rastgele, değişken ve eşsiz olarak üretilmesi ve belirli bir süre için geçerli olması sağlanır.

(10) Müşterinin kimliğini tespit etmeye yarayan ve resmi kimlik belgesi yerine geçen belgeler üzerinde yer alan bilgiler ile anne kızlık soyadı, elektronik bankacılık hizmetlerinin sunulması esnasında hiçbir aşamada kimlik doğrulama amacıyla kullanılamaz. Bankanın kimlik doğrulamada müşterinin bildiği unsur olarak bir güvenlik sorusu kullanmak istemesi durumunda, bu güvenlik sorusunun resmi kimlik belgesi yerine geçen belgeler üzerinde yer alan bilgilerden birine ilişkin olmaması ve cevabının müşterinin kendisi tarafından belirleniyor olması gerekir.

(11) Bir kimlik doğrulama bileşeninin bir müşteri ile ilk defa ilişkilendirilmesi uzaktan gerçekleştirilecekse, ilişkilendirme güvenli yöntemlerle ve birinci fıkraya uygun olarak en az iki bileşenli kimlik doğrulama gerçekleştirilerek yapılır. 23/2/2006 tarihli ve 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu kapsamındaki kartlar ve 20/6/2013 tarihli ve 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun kapsamındaki ödeme aracına ait PIN, ilgili elektronik bankacılık dağıtım kanalının aktifleştirilmesinden ve ilk parolanın alınmasından sonra kartın sahip olunan unsur olarak kullanıldığı işlemler hariç olmak üzere birinci fıkrada belirtilen "müşterinin bildiği" kimlik doğrulama unsuru olarak kullanılamaz. Elektronik bankacılık dağıtım kanalının aktifleştirilmesinden ve ilk parolanın alınmasından sonra parolanın unutulmasından veya yanlış girilmesinden dolayı sıfırlanması gereken hallerde, yeni parolanın uzaktan belirlenmesi için birinci fıkraya uygun olarak en az iki bileşenli kimlik doğrulama gerçekleştirilmesi şartıyla yukarıda belirtilen PIN bilgisi müşterinin bildiği unsur olarak kullanılabilir.

(12) Banka elektronik bankacılık dağıtım kanallarından gerçekleştirilebilecek işlemler için müşterilerine, varsayılan ve müşteri tarafından güncellenebilecek erişim kısıtlamaları, günlük işlem limitleri, güvenli alıcılar listesi gibi ilave güvenlik önlemleri sunar. Güvenlik önlemlerinin tanımlanması, güncellenmesi veya değiştirilmesinin birinci fıkraya uygun olan bir kimlik doğrulama sonrasında gerçekleştirilmesi esastır. Banka kendi risk değerlendirmesi çerçevesinde güvenlik önlemlerinde yapılacak değişiklikler için birinci fıkraya ilave güvenlik önlemleri belirleyebilir.

(13) Elektronik bankacılık dağıtım kanallarından sunulmakta olan herhangi bir işlemin tersinin gerçekleştirilmesi mümkün ve orijinal işleme göre eşit ya da daha az riskliyse, banka orijinal işlemin tersi olan bu işlemlerin de aynı elektronik dağıtım kanalından gerçekleştirilmesini sağlar.

(14) Bankanın elektronik bankacılık hizmetlerinde kullanmak üzere müşterilerine sunduğu her türlü yazılım ya da mobil uygulamanın kaynağının, ilgili banka olduğunun doğrulanabiliyor olması sağlanır. Banka bu yazılım ya da mobil uygulamaların, müşteri güvenliğini tehlikeye sokacak herhangi bir kod içermemesini sağlamakla, güvenlik açıklarını giderecek gerekli yamaları ve güncellemeleri müşteri kullanımına sunmakla yükümlüdür.

(15) Banka, akıllı telefonlar gibi birden fazla kimlik doğrulama bileşeninin bankaya iletilmesinde kullanılan mobil cihazlar üzerindeki bankacılık uygulamalarının kullandığı hassas verilerin, aynı mobil cihaz üzerindeki diğer uygulamalar ve çalışmakta olan işlemler tarafından erişilemez olmasını sağlayacak önlemler alır. Banka, söz konusu mobil cihazların kaybolması ya da çalınması halinde bunlar üzerindeki hassas verilerin yetkisiz kişilerce erişilemez olmasını sağlamak ve mobil cihazların

ele geçirilmesi, güvenilirliğinin bozulması, işletim sistemi yazılımının kırılması veya değiştirilmesi gibi hallerden kaynaklanacak risklerin azaltılması amacıyla günün teknolojisine uygun kontroller tesis etmekle yükümlüdür.

İnkâr edilemezlik ve sorumluluk atama

MADDE 35 - (1) Banka, sunmakta olduğu elektronik bankacılık hizmetleri kapsamında gerçekleştirilen işlemlerde hem banka hem de müşteri için inkâr edilemezliği ve sorumluluk atamayı mümkün kılacak teknikler kullanır. Kullanılan tekniğin oluşturduğu iz kayıtlarının güvenilir delillerin elde edilmesini sağlayacak ve sorumluluk atayacak nitelikte olması sağlanır.

İşlemlerin takibi

MADDE 36 - (1) Banka, elektronik bankacılık hizmetleri kapsamında gerçekleşen olağan dışı, sahtekârlık amaçlı veya dolandırıcılık riski bulunan işlemleri tespit etmeye ve bunları önlemeye yönelik işlem takip mekanizmaları kurar. İşlem takip mekanizması kapsamında uygun olan durumlarda asgari olarak aşağıdaki risk unsurları takip edilir:

- a) Finansal sonuç doğuran işlemlere yönelik bilinen dolandırıcılık yöntemleri,
- b) Gerçekleştirilen her bir bankacılık işleminin tutarı ve bu tutarlara göre müşterinin konum bilgisi de kullanılarak normal dışı bir ödeme, fon transferi ya da davranış deseni gösterip göstermediği,
- c) Kaybolmuş, çalınmış ya da yetkisiz kişilerce ele geçirilmiş kimlik doğrulama unsurlarının listesi,
- ç) Her bir kimlik doğrulama oturumuna yönelik olarak zararlı yazılımların bulaşmış olabileceğini gösteren belirtiler.

(2) Banka, riskli işlemleri filtreleyerek değerlendirir ve bu filtrelere takılan müşterileri daha yakından takip eder. Riskli işlemlerin gerçekleştirildiğinin tespit edilmesi halinde banka, telefon ya da kısa mesaj gibi uygun yöntemlerle müşterilerin en kısa sürede uyarılmasını sağlar.

Müşterilerin bilgilendirilmesi

MADDE 37 - (1) Banka tarafından sunulan elektronik bankacılık hizmetlerinden yararlanacak müşteriler; hizmetlere ilişkin şartlar, riskler ve istisnâ durumlarla ilgili olarak açık bir şekilde bilgilendirilir. Bankanın elektronik bankacılık hizmetlerine ilişkin risklerin etkisini azaltmaya yönelik benimsediği güvenlik prensipleri ve bu risklerden korunmak için kullanılması gereken yöntemler müşterinin dikkatine sunulur. Bu Yönetmelik kapsamında belirtilen müşterilerin bilgilendirilmesine yönelik her türlü bilgi ve açıklama, bankanın gerek kendi internet sitesinde gerek internet bankacılığı hizmetini verdiği internet sitesinde, müşteri erişimine daima açık tutulur ve erişilen bu sitelerin

bankaya ait olduğunu gösterecek teknikler kullanılır. Bilgi ve açıklamaların açık ve anlaşılır olması sağlanır, verildiği internet sitesinde dikkat çekici bir yere yerleştirilir ve ilgili elektronik bankacılık hizmetinden yararlanmaya başlamadan önce müşterilerin en az bir kere okumasını garanti edecek şekilde yönlendirmeler ve sistemselsel kısıtlamalar uygulanır. Hizmetlerden yararlanmaya başladıktan sonra müşterilerin dikkatine sunulması gereken önemli güvenlik uyarıları ve duyurular için de müşterilerin bu uyarı ve duyuruları okumasını sağlayacak teknikler kullanılır.

(2) Birinci fıkra kapsamında, banka kendi internet sitesinde veya internet bankacılığı hizmetini verdiği internet sitesinde;

a) Bankanın kimliği, ticaret unvanı, genel müdürlük adresi, kanuni statüsü, bankanın denetiminden sorumlu olan Bankacılık Düzenleme ve Denetleme Kurumuna ilişkin iletişim bilgilerine,

b) Elektronik bankacılık hizmetlerinin kullanımının taşıdığı riskler, bu risklerden korunmak için müşterilerin kullanması gereken yöntemler, müşteri farkındalığını artıracak yönlendirici güvenlik kılavuzları ile bu hizmetlerden yararlanacak müşterilerin sorumluluk ve haklarına,

c) Bankanın sunduğu elektronik bankacılık hizmetlerine, bu hizmetlerin ve bu hizmetler dâhilinde gerçekleştirilebilecek bankacılık işlemlerinin erişime açık olduğu gün ve saatlere ve hizmetlere ilişkin diğer koşullara,

ç) Elektronik bankacılık hizmetlerinde iki saatten daha uzun süreli bir kesinti öngörülen planlı bakım ve değişikliklerde müşterilerin önceden bilgilendirilmesini sağlayacak duyurulara,

d) Verilen hizmetlerle ilgili olarak müşterilerin herhangi bir sorunla ya da dolandırıcılık vakasıyla karşılaşması durumunda neler yapması gerektiğine ilişkin yönlendirici bilgilere,

yer verilir.

(3) Elektronik bankacılık hizmetlerinden dolayı müşterilerin yaşayabileceği sorunları ve şikâyetlerini iletebileceği ve takip edebileceği mekanizmalar oluşturulur. Oluşturulacak şikâyet birimleri veya çağrı merkezlerinde müşteriye karşılayacak menülerde ilgili elektronik bankacılık hizmetine ilişkin yaşanan dolandırıcılık vakalarının iletilmesi işleminin ana menüde ve ilk sıralarda müşterinin dikkatine sunulması ve bankaya ulaştırılan bildirimlerin en kısa sürede giderilmesine yönelik gerekli çalışmaların yapılması sağlanır.

(4) Banka tarafından sunulan elektronik bankacılık hizmetlerinde, müşterilerin yanlış işlem yapma ihtimalini en aza indirecek kontrollerin bulunması, müşterilerin başlattıkları işlemlere ilişkin ödemekle yükümlü oldukları her türlü tutar, komisyon ve ücret bilgilerinin işlem anında açıkça

müşteri bilgisine sunulması ve müşterinin bunları onaylaması halinde işlemlerin gerçekleştirilmesi temin edilir.

(5) Banka, müşteri talebi olmadan internet bankacılığı ve mobil bankacılık hizmetini ilgili müşterinin kullanımına açamaz. Müşteri, herhangi bir elektronik bankacılık hizmetine erişimini kapatmışsa veya kapattırmışsa, müşterinin yeni bir talebi olmadan ilgili hizmet kullanıma açamaz.

(6) Banka, yapacağı pazarlama faaliyetleri, reklâmlar veya yayınlarda, müşterilerine sunmakta olduğu herhangi bir elektronik bankacılık hizmetinin mutlak manada güvenli olduğu veya bu hizmetlerde hiçbir güvenlik riskinin bulunmadığı izlenimini ve bilgisini verecek ifadeler kullanmaktan kaçınır.

(7) Bankanın sunduğu elektronik bankacılık hizmetleri için bu Yönetmelik kapsamında yapılması gereken bilgilendirmelerin, hizmetin verildiği platformdan ya da müşterinin hizmeti alırken kullandığı cihazdan kaynaklanan nedenlerle bilgilendirme olanakları açısından yetersiz kalması durumunda, müşterinin bilgilendirmelere farklı kanallar üzerinden ulaşması için gerekli yönlendirmeler yapılır.

(8) Bankanın elektronik ortamda müşterilerine ileteceği hassas veri veya sır niteliğinde veri içeren her türlü ekstre, dekont, hesap özeti gibi bilgilerin elektronik bankacılık hizmeti sunulan kanallar üzerinden gönderilmesi esastır. Banka, bu gibi bilgilerin sunulmasında elektronik dağıtım kanallarının kullanılması için müşterilerine gerekli yönlendirmeleri yapmakla yükümlüdür.

İKİNCİ BÖLÜM

İnternet Bankacılığı

İnternet bankacılığında kimlik doğrulama ve işlem güvenliği

MADDE 38 - (1) İnternet bankacılığı dağıtım kanalında 34 üncü maddenin birinci fıkrasına göre gerçekleştirilecek kimlik doğrulama işleminin çevrimdışı olarak lokalde değil banka nezdinde çevrimiçi gerçekleşmesi ve müşterinin bildiği unsurun, mobil bankacılık uygulaması ya da internet tarayıcısı tarafından hatırlanarak veya bu unsurun başka lokal kimlik doğrulama yöntemlerine bağlanarak otomatik olarak gönderilmemesi gerekir. Müşterinin bildiği unsurun müşteri tarafından girilmesi zorunlu tutulur ve 34 üncü maddenin ikinci fıkrası hükmü saklı kalmak kaydıyla bu unsur lokalde değil banka nezdinde çevrimiçi doğrulanır.

(2) İnternet bankacılığı dağıtım kanalında kimlik doğrulama işlemi gerçekleştirilirken, müşteri tarafından ilk kimlik doğrulama bileşeni girildikten veya bankaya gönderildikten sonra ve internet

bankacılığı oturumu açılmadan önce, müşteri tarafından 34 üncü maddenin birinci fıkrasına göre iki bileşenli bir kimlik doğrulama ile önceden belirlenmiş olan bir karşılama mesajının veya resminin, müşteriye gösterilmesi sağlanır.

(3) İnternet bankacılığı dağıtım kanalında 34 üncü maddenin birinci fıkrasına göre gerçekleştirilecek kimlik doğrulama işlemi için müşteriye atanmış bir şifreleme gizli anahtarı ile imzalanacak şekilde tek kullanımlık bir doğrulama kodu üretilir. Doğrulama kodu aracılığıyla 34 üncü maddenin birinci fıkrasında belirtilen kimlik doğrulama unsurlarından hiçbiri hakkında bilgi edinilememesi, bilinen bir doğrulama kodu ile geçerli başka doğrulama kodlarının türetilmemesi, doğrulama kodlarının taklit edilememesi sağlanır. Finansal sonuç doğuran işlemler için doğrulama kodlarının, işlemi gerçekleştirirken müşterinin onayladığı tutar ve alıcı bilgisine göre spesifik olması, tutar veya fonun aktarılacağı alıcı bilgisindeki herhangi bir değişiklik halinde bu bilgilere göre oluşturulmuş ilgili doğrulama kodunun da geçersiz hale gelmesi temin edilir. Kurumsal internet bankacılığı müşterileri için yığın halinde birden fazla alıcı için toplu işlem gerçekleştirilmesine izin verilen fon transferi gibi işlemlerde, üretilen doğrulama kodunun ilgili yığın işlem toplam tutarı ve alıcılar için spesifik olması gerekir. Müşteriye atanmış bir şifreleme gizli anahtarı ile doğrulama kodunun imzalanmasının mümkün olmadığı hallerde, 34 üncü maddenin yedinci fıkrası saklı kalmak kaydıyla, SMS yoluyla müşteriye doğrulama kodu iletilebilir.

(4) İnternet bankacılığında müşterinin gerçekleştirdiği finansal sonuç doğuran işlemler için doğrulama kodunun oluşturulması, iletilmesi ve kullanılması da dâhil olmak üzere doğrulama sürecinin her aşamasında, tutar ve alıcı bilgisi gibi müşteriye gösterilen ve onayına sunulan bilgilerin gizliliğini, güvenilirliğini ve bütünlüğünü sağlamaya yönelik ve internet bankacılığı oturumu esnasındaki veri iletişiminin yetkisiz kişilere yönlendirilmesi riskine karşı gerekli önlemlerin alınması sağlanır.

(5) Doğrulama kodunun üretilmesinde hata meydana gelmesi ya da üretilmemesi halinde, kimlik doğrulama teşebbüsünde bulunan kişi tarafından hatanın hangi kimlik doğrulama unsurundan kaynaklandığının anlaşılmasını sağlayacak önlemler alınır.

ÜÇÜNCÜ BÖLÜM

Mobil Bankacılık

Mobil bankacılıkta kimlik doğrulama ve işlem güvenliği

MADDE 39 - (1) Mobil bankacılık uygulamasına tanımlanan uygulama PIN'inin müşteriye özgü bir şifreleme anahtarına erişmek üzere kullanılması ve bu şifreleme anahtarı yoluyla müşteriyle iltisap

eşsiz bir bilginin banka nezdinde çevrimiçi olarak doğrulanması halinde, 34 üncü maddenin birinci fıkrasında belirtilen iki bileşenli kimlik doğrulama yerine getirilmiş kabul edilir. Benzer şekilde, müşteriye ait bir biyometrik kimlik doğrulama bileşeninin mobil bankacılık uygulamasında kullanılarak müşteriye özgü bir şifreleme anahtarına erişilmesi suretiyle bu şifreleme anahtarı yoluyla müşteriyle ilintili eşsiz bir bilginin banka nezdinde çevrimiçi olarak doğrulanması halinde, 34 üncü maddenin birinci fıkrasında belirtilen iki bileşenli kimlik doğrulama yerine getirilmiş kabul edilir.

(2) Mobil bankacılık uygulaması kontrolünde olmayıp cihaz üreticisi kontrolünde olan parola, PIN ya da biyometrik veriler, 34 üncü maddenin birinci fıkrasında belirtilen müşterinin bildiği ya da biyometrik karakteristiği olan unsurlar olarak kullanılamaz.

(3) Mobil bankacılık uygulamasının yüklü olduğu cihazın ve/veya mobil bankacılık uygulamasının müşteriye bağlanmış olan, müşterinin sahip olduğu bir kimlik doğrulama unsuru olarak kullanılması şartıyla, müşterinin yalnızca mobil bankacılık uygulaması aracılığıyla müşteri ve hesap bilgilerini görüntülemek istemesi ya da daha önce tanımlanmış güvenli alıcılar listesine para transfer etmek veya ödeme yapmak istemesi halinde ilave bir kimlik doğrulama unsuruna gerek kalmadan tek bileşen ile yapılacak kimlik doğrulama 34 üncü maddenin birinci fıkrasına aykırılık olarak kabul edilmez. Müşterinin bu fıkrada belirtilen müşteri ve hesap bilgilerini görüntülemek üzere ilk defa oturum açması halinde ya da 34 üncü maddenin birinci fıkrasına göre iki bileşenle kimlik doğrulama gerçekleştirerek açtığı son oturumun üzerinden 90 günden daha fazla bir süre geçmiş olması halinde, iki bileşenli kimlik doğrulamaya tabi tutulması esastır.

DÖRDÜNCÜ BÖLÜM

Telefon Bankacılığı

Telefon bankacılığında kimlik doğrulama, işlem güvenliği ve hizmet kalitesi

MADDE 40 - (1) Müşteri 34 üncü maddenin birinci fıkrasına uygun olarak bir kimlik doğrulama gerçekleştirmediği müddetçe, telefon bankacılığında hizmet vermek üzere müşteriye karşılayan görevlinin müşteriye ilişkin bilgileri görememesi veya müşteriye ilişkin işlem menüsünün aktif olmaması sağlanır. Müşterinin kendi hesapları arasındaki finansal işlemler ile finansal olmayan işlemlerin gerçekleştirilmesi için uygulanacak kimlik doğrulamada PIN bilgisi müşterinin bildiği unsur olarak kullanılabilir. Kayıp, çalıntı ve dolandırıcılık gibi riskli işlem bildirim durumunda, görevliye bağlanan müşterilerin kimlik doğrulaması yapılmaksızın görevlinin bilmesi gerektiği kadar müşteri bilgisine erişebilmesi sağlanır ve gerekli güvenlik önlemleri alınır. Telefon bağlantısı

olmaksızın ya da bağlantının sonlanması halinde kayıp, çalıntı ve dolandırıcılık gibi riskli işlem bildirimini haricinde müşteriye ilişkin herhangi bir işlem gerçekleştirilemez.

(2) Müşterinin telefon bankacılığı kanalıyla, elektronik bankacılık dağıtım kanallarının herhangi birinde kullandığı kimlik doğrulama veya telefon bilgilerinde değişiklik gerçekleştirmek istemesi halinde bu değişikliğin görevli dahli ve erişimi olmadan otomatik sistemler üzerinden gerçekleştirilmesi sağlanır.

(3) Telefon bankacılığı hizmetlerinin verilmesi sırasında kimlik doğrulama gerçekleştirilirken, müşterinin bildiği kimlik doğrulama unsurları ile tek kullanımlık parola veya işlem doğrulama kodu gibi bileşenlerin, görevli dahli ve erişimi olmadan otomatik sistemler üzerinden girişinin yapılması sağlanır.

(4) Müşterinin bankada kayıtlı olan telefon numarasından aranması gerektiği durumlarda, arama gerçekleştirilmeden önce telefonun başka bir numaraya yönlendirilmemiş olduğuna ilişkin kontroller işletilir.

(5) Telefon bankacılığı hizmetlerinin verilmesi sırasında müşterinin gerçekleştirdiği işlemlere ilişkin alınan ses kayıtları için bu Yönetmelikte iz kayıtları hususunda belirtilen hükümler uygulanır. Alınan ses kayıtlarının güvenilir delillerin elde edilmesini sağlayacak ve sorumluluk atayacak nitelikte ve kalitede olması esastır.

(6) Banka, telefon bankacılığı hizmetlerinin müşterilere sunulmasında görev alan müşteri temsilcileri ve çağrı merkezi görevlileri gibi çalışanlara sosyal mühendislik saldırıları ve bilinen diğer dolandırıcılık yöntemleri konusunda periyodik eğitimler aldirmek ve bu çalışanların güvenlik farkındalıklarını artırıcı çalışmalar yapmakla yükümlüdür.

(7) Banka telefon bankacılığı hizmet kalitesini sağlamak adına asgari olarak aşağıdaki kriterleri yerine getirir:

a) Sesli yanıt sisteminin ana ve alt menülerinin, reklamlar, duyurular ve bilgilendirmeler dâhil, anons sürelerinin altmışar saniyeyi geçmemesi sağlanır.

b) Ses ile yönlendirme sisteminde müşterinin işlemini söylemeye başlaması için anonsu müteakip iki defa on saniye süre verilmesi, akabinde işlemini yapamayan müşterinin ana menüye aktarılması sağlanır.

c) Ana menüde veya alt menülerde çağrı merkezi görevlisi veya müşteri temsilcisine bağlanma seçeneği sunulur.

ç) Çağrı karşılama hedefinin tutturulması için çağrı merkezi görevlisi veya müşteri temsilcisinin müşteri ile görüşme süresinin sınırlandırılması gibi bir uygulamaya yer verilmemesi sağlanır.

BEŞİNCİ BÖLÜM

Açık Bankacılık Servisleri

Açık bankacılık servislerinde kimlik doğrulama ve işlem güvenliği

MADDE 41 - (1) Açık bankacılık servislerinin kullanılması sırasında, müşteri veya müşteri adına hareket eden taraf ile banka arasındaki iletişimin uçtan uca güvenli iletişim şeklinde olması, banka tarafından telafi edici ilave kontroller uygulanması ve müşterinin bağlantı kurabileceği kaynaklara ilişkin ilave kısıtlamalar getirilmesi şartıyla tek bileşen ile yapılacak kimlik doğrulama 34 üncü maddenin birinci fıkrasına aykırılık olarak kabul edilmez.

(2) Açık bankacılık servisleri aracılığıyla sunulabilecek hizmetler ve bu hizmetlere ilişkin usul ve esasları belirlemeye Kurul yetkilidir.

ALTINCI BÖLÜM

ATM Bankacılığı

ATM'lerde kimlik doğrulama ve işlem güvenliği

MADDE 42 - (1) Banka, ATM cihazları üzerinde kart kopyalama veya dolandırıcılığını önlemek için bilinen suç aygıtlarına ve tekniklerine karşı gerekli önlemleri almakla yükümlüdür. Banka asgari olarak aşağıdaki önlemleri alır:

a) Sahte önyüz, sahte klavye, kart sıkıştırma aparatları, kart kopyalama aparatları, nakit sıkıştırma aparatları, mobil kamera gibi kart okuyucu içerisine, para giriş ve çıkış noktalarına veya ATM'nin diğer birimlerine monte edilebilecek yabancı cihazların ATM'ye takılmasını ve mevcut ATM ekipmanlarının ATM'den çıkarılmasını zorlaştıran teknikler ile önleyici veya tespit edici kontroller kullanılır.

b) Yapılacak risk analizleri sonucunda belirlenen periyotlarda ATM cihazları yabancı cisimlerin mevcudiyetine karşı fiziksel olarak kontrol edilir. Kart kopyalama ve kart dolandırıcılığına yönelik cihazların monte edilme ihtimalinin yüksek olduğu tespit edilen ATM'ler için ilgili kontrol periyotları sıklaştırılır.

(2) ATM üzerine herhangi bir kart kopyalama ve dolandırıcılık amaçlı cismin monte edildiğinin veya ATM cihazının kurcalandığının tespit edilmesi, kart kopyalama ve dolandırıcılığı önlemeye yönelik çözümlerin alarm üretmesi veya bu çözümlerin çalışmadığının algılanması durumlarında; ATM'nin

güvenlik amacıyla merkezden devre dışı bırakılabilmesi ve fiziksel olarak kontrol edilmeden ya da kamera görüntüleri incelenerek herhangi bir problemin bulunmadığı hususunda güvence sağlanmadan tekrar hizmete açılmaması temin edilir.

(3) ATM cihazları üzerinde ön tanımlı olarak gelen her türlü parola, ATM cihazının bu ön tanımlı parolalarını bilen kötü niyetli kişiler tarafından yönetilmesini engellemek amacıyla, kolaylıkla tahmin edilemeyecek şekilde değiştirilir.

(4) ATM cihazları üzerine, zararlı içerikli programların kötü niyetli kişilerce yüklenmesini ve yetkisiz erişimi engelleyecek gerekli tedbirler alınır, uygulamaların ve uygulamalara ilişkin kritik servis ve verilerin bütünlüğü periyodik olarak doğrulanır. ATM'ler üzerine güvenlik açıklarını gidermek amacıyla otomatik olarak veya düzenli periyotlar ile gerekli güncellemeler ve yamalar yüklenir. ATM'ler üzerinde çalışan işletim sisteminin gerekli olan en az yetki ve ayrıcalıklara sahip olarak çalışacak şekilde ayarlanmış, gerekli güncellemeleri ve yamaları yüklenerek sıkılaştırılmış, stabil ve günün teknolojisine göre güvenli bir işletim sistemi olması sağlanır. Banka, ATM'lerde, kaynağını ve bütünlüğünü onaylayamadığı uygulama ve kodların çalışmasını engelleyecek önlemleri alır.

(5) ATM'lere yetkisiz kişilerin herhangi bir şekilde başka bir elektronik cihaz bağlamasına imkân verecek bütün giriş noktaları erişime kapatılır ve ATM cihazı ile banka arasındaki ağ bağlantısına yetkisiz olarak diğer cihazların bağlanmasını engelleyecek ilave güvenlik tedbirleri uygulanır.

(6) ATM cihazları üzerinden gerçekleştirilen işlemler için kullanılan iletişim ağının veri güvenliğini, gizliliğini ve bütünlüğünü sağlayacak özellikte olması sağlanır. ATM üzerinde saklanan, iletilen, işlenen her türlü verinin gizliliği ve bütünlüğü uygun yöntemlerle korunur. PIN bilgisi, parmak izi bilgisi, kart bilgisi gibi kimlik doğrulamaya ilişkin kritik bilgilerin sayısallaştırılarak sisteme girildiği aşamadan itibaren gizliliği ve bütünlüğü sağlanır.

(7) Banka, ATM cihazlarının güvenli kullanımı hususunda müşterilerinde farkındalık oluşturan çalışmalarda bulunur.

(8) Banka şubesinde gerçekleştirildiği takdirde yasal kimlik ibrazı zorunlu tutulan işlemlerin ATM'ler üzerinden yapılmak istenmesi durumunda 34 üncü maddenin birinci fıkrasına uygun olarak kimlik doğrulama uygulanır.

(9) Banka, ATM cihazlarının bulunduğu yerlere müşterinin klavye hareketlerini göremeyecek uygun bir açıyla güvenlik kamerası yerleştirir. Güvenlik kamerası kayıtları en az altı ay süreyle saklanır. Kamera kayıtlarındaki görüntünün delil niteliği teşkil etmesi ve görüntü kalitesinin ATM'deki müşterinin ve yakın çevresindekilerin eşkâllerinin belirlenmesini sağlayabilecek nitelikte olması

esastır. Kameraların saatlerinin güncel, doğru olması ve ATM'de gerçekleştirilen işlem referans numarası, dekont numarası gibi parametrelerin zaman bilgisi ile uyumlu olması sağlanır. Kameranın herhangi bir sebeple görüntü kalitesinin düşmesi, görüntü alımının durması, lensinin dış bir etkenle kapatılması veya devre dışı kalması durumunu tespit edip gerekli aksiyonların alınmasını sağlayacak bir yapı kurulur.

(10) Görüntüleme alanı bakımından ATM'yi de kapsayan ve dokuzuncu fıkrada yer alan koşulları karşılayan bir güvenlik kamerası altyapısının varlığı durumunda ATM'ye özel ayrıca bir güvenlik kamerası kurulmasına gerek yoktur. Kamu güvenlik ve istihbarat kurumlarının faaliyet bölgesinde bulunan ATM'ler için güvenlik kamerası kurulma şartı, ilgili kamu güvenlik ve istihbarat kurumlarından izin alınabilmesi koşuluyla yerine getirilir.

DÖRDÜNCÜ KISIM

Çeşitli ve Son Hükümler

BİRİNCİ BÖLÜM

Çeşitli Hükümler

Uzaktan kimlik tespiti ve üçüncü tarafa güven

MADDE 43 - (1) Banka, 11/10/2006 tarihli ve 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun ve alt düzenlemelerinde yer alan yükümlülükler saklı kalmak kaydıyla, müşterinin veya müşteri adına hareket eden kişinin kimliğini tespit etmek amacıyla, uzaktan kimlik tespiti yöntemleri kullanabilir ya da hâlihazırda müşteri veya müşteri adına hareket eden kişi için daha önce kimlik tespitinde bulunmuş başka bir bankadan açık bankacılık servisleri aracılığıyla hizmet alabilir. Bu fıkranın uygulanmasına ilişkin usul ve esasları belirlemeye Kurul yetkilidir.

Mesleki tecrübeye ilişkin alanlar ve süreler

MADDE 44 - (1) 2/1/2014 tarihli ve 2014/5885 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan Bankacılık Düzenleme ve Denetleme Kurumu Teşkilat Yönetmeliğine göre Kurum tarafından ilgili kuruluşlarda BS yerinde denetimlerini yapmakla görevli daire başkanlığı bünyesinde görev alan Kurum meslek personeli, bu Yönetmelikte geçen mesleki tecrübeye ilişkin alanlarda çalışmış kabul edilir ve meslek personelinin ilgili daire başkanlığı bünyesinde çalıştığı süreler, bu Yönetmelikte geçen mesleki tecrübeye ilişkin alanlarda çalışılmış süreler olarak kabul edilir.

İstisna hükmü

MADDE 45 - (1) Bu Yönetmelik kapsamında kurulacak komiteler, birimler ve sorumlular konusunda, bankaların ölçeđi, bilgi sistemlerine bađımlılıđı, personel sayısı, alınan dıř hizmetler gibi kriterler esas alınarak istisna tanımlamaya Kurum yetkilidir.

İKİNCİ BÖLÜM

Son Hükümler

Yürürlük

MADDE 46 - (Deđişik:RG-20/6/2020-31161)

(1) Bu Yönetmeliđin 13 üncü maddesi, 29 uncu maddesi, 34 üncü maddesinin on üçüncü fıkrası ile on beşinci fıkrası, 37 nci maddesinin sekizinci fıkrası, 40 ıncı maddesi ve 42 nci maddesi 1/7/2020 tarihinde, diđer hükümleri ise 1/1/2021 tarihinde yürürlüđe girer.

Yürütme

MADDE 47 - (1) Bu Yönetmelik hükümlerini Bankacılık Düzenleme ve Denetleme Kurumu Başkanı yürütür.

**Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında
Yönetmelik**

Resmî Gazete Tarihi : 01.12.2021

Resmî Gazete Sayısı : 31676

**ÖDEME HİZMETLERİ VE ELEKTRONİK PARA İHRACI İLE ÖDEME HİZMETİ
SAĞLAYICILARI HAKKINDA YÖNETMELİK**

BİRİNCİ KISIM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç ve kapsam

MADDE 1 - (1) Bu Yönetmeliğin amacı, ödeme kuruluşları ve elektronik para kuruluşlarının yetkilendirilmesi ve faaliyetleri ile ödeme hizmeti sağlayıcılarına, ödeme hizmetlerinin sunulmasına ve elektronik para ihracına ilişkin usul ve esasları düzenlemektir.

Dayanak

MADDE 2 - (1) Bu Yönetmelik, 20/6/2013 tarihli ve 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanununun 12 nci, 14 üncü, 14/A, 18 inci, 19 uncu, 20 nci, 21 inci, 22 nci, 23 üncü, 24 üncü, 25 inci ve 26 ncı maddelerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 3 - (1) Bu Yönetmelikte yer alan;

- a) Açık rıza: 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununun 3 üncü maddesinin birinci fıkrasının (a) bendinde tanımlanan açık rızayı,
- b) Alıcı: Ödeme işlemine konu fonun ulaşması istenen gerçek veya tüzel kişiyi,
- c) Anonim ön ödemeli araç: Herhangi bir şekilde ödeme hesabına bağlı olmayan ve kimlik tespiti veya doğrulaması yapılmamış, önceden ödeme ya da yükleme yapılması suretiyle kullanılabilir hale gelen, tekrar yükleme yapılma imkanı bulunan veya bulunmayan şekilde ihraç edilebilen ve yüklenen bakiye kadar kullanıma izin verilen ön ödemeli aracı,

- ç) Banka: Türkiye Cumhuriyet Merkez Bankası Anonim Şirketini,
- d) Banka Ödeme Sistemleri: Banka tarafından işletilen ödeme sistemlerini,
- e) Başlangıç sermayesi: Ödenmiş sermaye, hisse senedi ihraç primleri, yedek akçeler, geçmiş yıllar kârı ve dönem net kârı toplamından varsa net dönem zararı ve geçmiş yıllar zararının düşülmesi suretiyle hesaplanan tutarı,
- f) Birlik: Türkiye Ödeme ve Elektronik Para Kuruluşları Birliğini,
- g) Çerçeve sözleşme: Ödeme hizmeti sağlayıcısı ile müşteri arasında tekil veya süreklilik arz eden ödeme işlemlerinin yürütülmesine ve mümkün olan durumlarda ödeme hesabının açılmasına ilişkin usul ve esasları belirleyen sözleşmeyi,
- ğ) Doğrudan borçlandırma: Gönderenin kendi ödeme hizmeti sağlayıcısına, alıcıya veya alıcının ödeme hizmeti sağlayıcısına verdiği onaya dayanılarak, ödeme işleminin alıcı tarafından başlatıldığı ve gönderenin ödeme hesabının borçlandırıldığı ödeme hizmetini,
- h) Elektronik haberleşme hizmeti: 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun 3 üncü maddesinin birinci fıkrasının (j) bendinde tanımlanan hizmetleri,
- ı) Elektronik haberleşme işletmecisi: 5809 sayılı Kanunun 3 üncü maddesinin birinci fıkrasının (z) bendinde tanımlanan şirketi,
- i) Elektronik para: Elektronik para ihraç eden kuruluş tarafından kabul edilen fon karşılığı ihraç edilen, elektronik olarak saklanan, Kanunda tanımlanan ödeme işlemlerini gerçekleştirmek için kullanılan ve elektronik para ihraç eden kuruluş dışındaki gerçek ve tüzel kişiler tarafından da ödeme aracı olarak kabul edilen parasal değeri,
- j) Elektronik para ihraç eden kuruluş: Elektronik para kuruluşlarını, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu kapsamındaki bankaları ve Posta ve Telgraf Teşkilatı Anonim Şirketini,
- k) Elektronik para kuruluşu: Kanun kapsamında elektronik para ihraç etme yetkisi verilen tüzel kişiyi,
- l) Fatura ödemesi: Elektrik, iletişim, su, doğalgaz gibi ihtiyaçların karşılanmasına yönelik sunulan hizmetlerin karşılığı olarak yapılan ödemeler ile Bankaca uygun görülen diğer ödemeleri,
- m) Fon: Banknot, madeni para, kaydî para veya elektronik parayı,
- n) Fona çevirme: Elektronik paranın kullanılması veya geri ödenmesi sonucunda banknot, madeni para, kaydî para veya başka bir kuruluş tarafından ihraç edilmiş elektronik paraya çevrilmesini,

- o) Gönderen: Kendi ödeme hesabından veya ödeme hesabı bulunmaksızın ödeme emri veren gerçek veya tüzel kişiyi,
- ö) Hassas müşteri verisi: Ödeme emrinin verilmesinde veya müşterinin kimliğinin doğrulanmasında kullanılan ve üçüncü kişilerce ele geçirilmesi veya değiştirilmesi halinde dolandırıcılık ya da müşteri adına sahte işlem yapılmasına imkân verebilecek kişisel veriler ile müşteri güvenlik bilgilerini,
- p) Güven Damgası: 6/6/2017 tarihli ve 30088 sayılı Resmî Gazete’de yayımlanan Elektronik Ticarete Güven Damgası Hakkında Tebliğde öngörülen asgari güvenlik ve hizmet kalitesi standartlarına uyan hizmet sağlayıcı ve aracı hizmet sağlayıcıya verilen elektronik işareti,
- r) Hesap bilgisi hizmeti: Kanununun 12 nci maddesinin birinci fıkrasının (g) bendinde tanımlanan hizmeti,
- s) İcraî görev: Doğrudan gelir getirici faaliyetlerin icrasına yönelik görevleri,
- ş) İşyeri: Ödeme hizmeti sağlayıcısı ile yaptığı sözleşme çerçevesinde, ödeme hizmeti kapsamına giren bir ödeme yöntemi ile mal ve hizmet satmayı kabul eden gerçek veya tüzel kişiyi,
- t) Kalıcı veri saklayıcısı: Müşterinin gönderdiği veya müşteriye gönderilen bilgiyi, bu bilginin amacına uygun olarak makul bir süre incelemesine elverecek şekilde kaydedilmesini ve değiştirilmeden kopyalanmasını sağlayan ve bu bilgiye aynen ulaşılmasına imkân veren kısa mesaj, elektronik posta, internet, CD, DVD, hafıza kartı ve benzeri her türlü araç veya ortamı,
- u) Kanun: 20/6/2013 tarihli ve 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanunu,
- ü) Kart tabanlı ödeme aracı: Gönderenin, kart tabanlı bir ödeme işlemini başlatmasını sağlamak için gerekli ödeme uygulamalarını içeren ve ödeme aracı olarak kullanılan kart, cep telefonu, bilgisayar gibi teknolojik cihazı,
- v) Kart tabanlı ödeme işlemi: Ödeme işleminin kart, bilişim veya elektronik haberleşme cihazı veya yazılım aracılığıyla gerçekleştirilmesi için 23/2/2006 tarihli ve 5464 sayılı Banka Kartları ve Kredi Kartları Kanununda tanımlanan kartlı sistem kuruluşlarının altyapıları ve iş kurallarına göre sunulan ve bunun sonucunda bir banka kartı, kredi kartı veya ön ödemeli araç işlemi gerçekleşen hizmetleri,
- y) Katma değerli hizmetler: Kanun uyarınca ödeme hizmeti kapsamına girmeyen ancak ticari borç ve alacak yönetimi, muhasebeleştirme, faturalama, ürün, stok ve tedarik yönetimi gibi tüzel kişilerin ve tacirlerin idari ve operasyonel süreçlerini kolaylaştıran, güvenli kılan veya etkinliğini artıran hizmetleri,

z) Kimlik tanımlayıcı: Ödeme hizmeti sağlayıcısı tarafından kimliğinin belirlenmesi ve diğer kullanıcılardan ayırt edilmesi amacıyla müşteriye özgülenen sayı, harf veya sembollerden oluşan kombinasyonu,

aa) Kişisel veri: 6698 sayılı Kanununun 3 üncü maddesinin birinci fıkrasının (d) bendinde tanımlanan kişisel veriyi,

bb) Kontrol: Bir tüzel kişinin; sermayesinin, asgari yüzde ellibirine sahip olma şartı aranmaksızın, çoğunluğuna doğrudan veya dolaylı olarak sahip olunması veya bu çoğunluğa sahip olunmamakla birlikte imtiyazlı hisselerin elde bulundurulması veya diğer hissedarlarla yapılan anlaşmalara istinaden oy hakkının çoğunluğu üzerinde tasarrufta bulunulması suretiyle veya herhangi bir suretle yönetim kurulu üyelerinin karara esas çoğunluğunu atayabilme ya da görevden alma gücünün elde bulundurulmasını,

cc) Kuruluş: Ödeme kuruluşları ve elektronik para kuruluşlarını,

çç) Müşteri: Ödeme hizmeti kullanıcısı ile elektronik para kullanıcısını,

dd) Müşteri güvenlik bilgileri: Kimlik doğrulama işleminin yapılması amacıyla ödeme hizmeti sağlayıcısı tarafından müşterisine verilen veya müşteri tarafından belirlenerek ödeme hizmeti sağlayıcısı ile mutabık kalınan özelleştirilmiş bilgiyi,

ee) Nitelikli pay sahibi: Kuruluşların sermayesinin veya oy haklarının doğrudan veya dolaylı olarak yüzde on veya daha fazlasını teşkil eden paylar ile bu oranın altında olsa dahi yönetim kurullarına üye belirleme imtiyazı veren paylara sahip gerçek veya tüzel kişiyi,

ff) Ödeme aracı: Ödeme hizmeti sağlayıcısı ile müşterisi arasında belirlenen ve müşteri tarafından ödeme emrini vermek için kullanılan kart, cep telefonu, şifre ve benzeri kişiye özel aracı,

gg) Ödeme aracının ihracı: Ödeme hizmeti sağlayıcısı tarafından, ödeme işlemlerini başlatmak ve işlemek için gönderene ödeme aracı sağlanmasına ilişkin ödeme hizmetini,

ğğ) Ödeme aracının kabulü: Ödeme aracı kullanılarak ilgili ödeme işleminin gerçekleşmesi için ödeme hizmeti sağlayıcısı tarafından işyerine fon transferi yapılmasıyla sonuçlanacak şekilde sunulan ve işyeri ile anlaşılmasını da içeren hizmetleri,

hh) Ödeme emri: Müşteri tarafından ödeme işleminin gerçekleşmesi amacıyla ödeme hizmeti sağlayıcısına verilen talimatı,

ıı) Ödeme emri başlatma hizmeti: Kanununun 12 nci maddesinin birinci fıkrasının (f) bendinde tanımlanan hizmeti,

- ii) Ödeme hesabı: Müşteri adına açılan ve ödeme işleminin yürütülmesinde kullanılan hesabı,
- jj) Ödeme hesabının bulunduğu kuruluş: Nezdinde ödeme hesabı bulunan ödeme hizmeti sağlayıcısını,
- kk) Ödeme hizmeti: Kanunun 12 nci maddesi çerçevesinde ödeme hizmeti olarak kabul edilen hizmetleri,
- ll) Ödeme hizmeti kullanıcısı: Gönderen, alıcı veya her ikisi sıfatıyla belirli bir ödeme hizmetinden faydalanan gerçek veya tüzel kişiyi,
- mm) Ödeme hizmeti sağlayıcısı: 5411 sayılı Kanun kapsamındaki bankaları, elektronik para kuruluşlarını, ödeme kuruluşlarını ve Posta ve Telgraf Teşkilatı Anonim Şirketini,
- nn) Ödeme işlemi: Gönderen veya alıcının talimatı üzerine gerçekleştirilen fon yatırma, aktarma veya çekme faaliyetini,
- oo) Ödeme kuruluşu: Ödeme hizmeti sağlamak ve gerçekleştirmek için Kanun kapsamında yetkilendirilmiş tüzel kişiyi,
- öö) Ön ödemeli araç: Müşterinin ödemelerde kullanılabilecek fonu ödeme aracını ihraç eden ödeme hizmeti sağlayıcısına harcama yapmadan önce ödediği ve ödenene eşdeğer tutarda fonun ödeme hizmetlerinde kullanılmasına imkân veren fizikî veya fizikî varlığı bulunmayan ödeme aracını,
- pp) Referans döviz kuru: Ödeme hizmeti sağlayıcısı tarafından uygulanan veya kamuya açık bir kaynaktan alınan ve yabancı para ile yapılan işlemlerde kullanılan döviz kurunu,
- rr) Rekabete duyarlı veri: Ücret, komisyon, faiz gibi fiyat ile ilişkilendirilebilir her türlü niceliksel veriyi,
- ss) Şube: Kuruluşun bağımlı bir parçasını oluşturan ve faaliyetlerinin tamamını veya bir kısmını kendi başına yapan tüzel kişiyi,
- şş) Tedavüldeki elektronik para tutarı: Elektronik para kuruluşu, şubeleri, temsilcileri, insansız hizmet noktaları veya elektronik para kuruluşu adına hareket eden üçüncü taraf bir hizmet sağlayıcısı tarafından alınan fonlar karşılığı elektronik para kuruluşu tarafından ihraç edilen ve ihraç edildiği günü izleyen iş günü, tam iş günlerinde saat 15.00; yarım iş günlerinde saat 11.00 itibarıyla fona çevrilmeyen elektronik paraların toplam tutarını,
- tt) Temsilci: Kuruluş adına ve hesabına hareket eden gerçek veya tüzel kişiyi,

uu) Tüketici: 7/11/2013 tarihli ve 6502 sayılı Tüketicinin Korunması Hakkında Kanununun 3 üncü maddesinin birinci fıkrasının (k) bendinde tanımlanan kişiyi,

üü) Uzaktan iletişim aracı: Mektup, katalog, telefon, faks, elektronik posta mesajı, internet, kısa mesaj hizmetleri gibi fiziksel olarak karşı karşıya gelinmeksizin sözleşme kurulmasına imkân veren her türlü araç veya ortamı,

vv) Üst yönetim: Kuruluşun yönetim kurulu üyeleri, genel müdür ve genel müdür yardımcıları, iç kontrol ve risk yönetimi birimlerinin yöneticileri ile başka unvanlarla istihdam edilseler dahi, danışmanlık birimleri dışındaki birimlerin, yetki ve görevleri itibarıyla genel müdür yardımcısına denk veya daha üst konumlarda görev yapan yöneticilerini,

yy) Yaygın mağaza ağı: Türkiye genelinde belirli bir marka adı altında perakende satış gerçekleştiren tüzel kişileri,

ifade eder.

(...)

Dış hizmet alımı

MADDE 21 - (1) Bu Yönetmelikte aksine bir hüküm bulunmadığı sürece, kuruluş ödeme hizmeti sunma ve elektronik para ihraç etme faaliyetini dış hizmet alımına konu edemez.

(2) Kuruluş, Kanun, bu Yönetmelik ve ilgili alt düzenlemelerdeki yükümlülüklerle uyulması ve kapsamının yazılı sözleşme ile belirlenmesi kaydıyla ödeme hizmeti sunumu ve elektronik para ihracı dışında kalan faaliyetleri ile ödeme hizmeti sunumu ve elektronik para ihracı faaliyetleri ile ilgili olan bilgi sistemleri, pazarlama, reklam, kurumsal kaynak yönetimi, muhasebe, çağrı merkezi, kuruluşun idari işlerinin takibi faaliyetlerini dış hizmet alımına konu edebilir. Dış hizmet alımı, üst yönetimin 6102 sayılı Kanun, bu Yönetmelik ve kuruluşun iç düzenlemeleri ile belirlenen yetkilerinin devri sonucunu doğuracak şekilde gerçekleştirilemez. Banka, bu fıkrada belirlenmiş olan konulara ilişkin dış hizmet alımlarının sınırları ile gerektiğinde kuruluşların dış hizmet alımına konu edebilecekleri diğer konuları belirlemeye yetkilidir.

(3) Kuruluş dış hizmet alımı esnasında; dış hizmet sağlayıcı kuruluşun seçiminde gerekli özeni göstermekle, dış hizmet sağlayıcı kuruluşun yükümlülüklerini sözleşme ile netleştirmekle ve dışarıdan hizmet alımının doğuracağı ilave riskleri göz önünde bulundurarak bu riskleri etkin bir şekilde yönetmekle yükümlüdür.

(4) Faaliyet izni verilmesine esas şartların kaybedilmesi veya deęişmesi sonucunu doğuracak şekilde dış hizmet alımı yapılamaz. Alınacak dış hizmet, kuruluşun yasal yükümlülüklerini yerine getirmesini, ilgili düzenlemelere uymasını ve etkin biçimde denetlenmesini engelleyici nitelikte olamaz. Dış hizmet alımına konu edilen bir faaliyete ilişkin, ilgili mevzuatta kuruluşa yükümlülükler getirilmesi halinde, bu yükümlülüklerin dış hizmet sağlayıcı tarafından yerine getirilmesinin sağlanacağına taraflar arasında imzalanacak sözleşme ile taahhüt edilmesi zorunludur. Bu durum, kuruluşun sorumluluğunu ortadan kaldırmaz. Kuruluş, dış hizmete konu edilen faaliyetler bakımından dış hizmet sağlayıcının işlemlerinden de sorumludur. Dış hizmet alımı, Kanun kapsamındaki faaliyetlerin ödeme hizmeti sağlayıcısı olmayan bir şirket tarafından sunulması sonucunu veya izlenimini yaratacak şekilde gerçekleştirilemez.

(5) Dış hizmet alımları ve dış hizmet alınan firmalar kuruluş tarafından Bankaca belirlenecek usul ve esaslara göre Bankaya raporlanır.

(6) Kuruluş, dış hizmet alımında kendisine ve müşterilerine ait hassas müşteri verileri başta olmak üzere sırların ve kişisel verilerin korunması için gerekli tedbirleri alır.

(7) Dış hizmet sağlayıcının yurt dışında kurulu olması durumunda, faaliyet gösterdiği ülke mevzuatı ve uygulamalarında, Bankanın ihtiyaç duyduğu bilgi ve belgeleri zamanında, eksiksiz ve doğru edinmesine ve dış hizmet sağlayıcıdan alınan hizmetle ilgili denetim yapmasına ilişkin herhangi bir yasal engel bulunmaması zorunludur.

(8) Dış hizmet alımı, kuruluşun tüm hesap ve kayıtları ile her türlü işlemlerine ilişkin bilgilerin denetime hazır şekilde saklanması yükümlülüğünü ortadan kaldırmaz.

(9) Dış hizmet alımı, kuruluşun iç kontrol ve risk yönetimi sistemlerinin etkinliği ile Bankanın izleme ve denetim kabiliyetini azaltacak şekilde gerçekleştirilemez.

(10) Dış hizmet alımı, kuruluşun müşterilerine karşı sorumluluğunu ortadan kaldırmaz.

(11) Banka, bu maddede yer alan hükümlere uyulmaması, dış hizmet almasının kuruluşun faaliyetlerini olumsuz etkilediği kanaatine varılması veya dış hizmet sağlayıcının, Bankanın Kanun kapsamındaki denetim faaliyetlerini engellemesi durumunda kuruluşun dış hizmet alımını durdurmasını istemeye yetkilidir.

(12) Yemek, ulaşım ve temizlik gibi konularda alınan hizmetler ile kuruluşun mülkiyetine veya kullanma hakkına sahip olduğu bu Yönetmelik kapsamındaki faaliyetlerin sunumunda doğrudan kullanılmayan her türlü teknik ekipman ve demirbaşın temini, bakım ve onarımı ile eğitim hizmetleri, avukatlık hizmetleri ile hukuk danışmanlığı, danışmanlık faaliyetleri, başka şirket bünyesinde

istihdam edilmekle birlikte kuruluřta geici veya srekli olarak, yemek, ulařım, fiziki gvenlik ve temizlik gibi hizmetlerde alıřtırılacak personele ynelik olan dıř hizmet alımları iin bu madde hkmleri uygulanmaz.

(...)

Verilerin korunması

MADDE 62 - (1) deme hizmeti saėlayıcısı, deme hizmeti faaliyetinin gerekleřtirilmesi ile ilgili verilere yasalarca kendisine verilen yetki ve sorumluluklar kapsamında yalnızca ilgili mřteriyi aıka bilgilendirmek Őartı ile eriřebilir, bu verileri kullanabilir ve saklayabilir. deme hizmeti faaliyetinin gerekleřtirilmesi ile doėrudan ilgili olmayan sebeplerle bu verilere eriřilmesi, verilerin kullanılması ve saklanması yalnızca mřterinin onayı ile mmkndr. deme hizmeti faaliyetinin gerekleřtirilmesi ile doėrudan ilgili olmayan sebeplerle eriřilen veriler ierisinde kiřisel veriler olması durumunda mřterinin aık rızasının alınması gerekir.

(2) 4 nc maddenin birinci fıkrasının (f) veya (g) bentlerinde belirtilen deme hizmetlerini sunan kuruluřlar tarafından, bu hizmetler kapsamında temin edilmiř verilerin, tzel kiřilerin ve tacirlerin idari ve operasyonel srelerine iliřkin olarak sunmakta oldukları katma deėerli hizmetler iin kullanılması, mřterinin onayının alınmıř olması kaydıyla, 60 ıncı ve 61 inci maddelerde yer alan hkmlere aykırılık olarak deėerlendirilmez.

(3) deme hizmeti saėlayıcıları tarafından ihra edilmiř deme aralarına iliřkin hassas mřteri verilerinin yurt iinde bulunan iřyerleri nezdinde veya sorumluluėunda saklanması durumunda, bu verilerin yurt iinde tutulması ve saklanması zorunludur.

(4) 4 nc maddenin birinci fıkrasının (f) veya (g) bentlerinde belirtilen deme hizmetlerini sunan deme hizmeti saėlayıcıları tarafından, bu hizmetler kapsamında temin edilmiř veriler, deme hizmeti saėlayıcısı mřterinin onayını alsa dahi, mřteriden gelen bir talep ya da talimat olmaksızın yurt iindeki ve yurt dıřındaki nc kiřilerle paylařılamaz ve bunlara aktarılamaz.

(5) Kanun kapsamına giren iřlemler ile ilgili olarak kiřisel verilerin iřlenmesi faaliyetlerinde, 6698 sayılı Kanun ile 6698 sayılı Kanun uyarınca yapılan dzenlemelerde yer alan hkmler ncelikli olarak uygulanır ve bu hkmler kapsamında belirlenmiř olan usul ve esaslara uyulması zorunludur.

Hasta Hakları Yönetmeliđi

Resmî Gazete Tarihi : 01.08.1998

Resmî Gazete Sayısı : 23420

HASTA HAKLARI YÖNETMELİĐİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak, Tanımlar ve İlkeler

Amaç

Madde 1- Bu Yönetmelik; temel insan haklarının sađlık hizmetleri sahasındaki yansımaları olan ve başta Türkiye Cumhuriyeti Anayasası'nda, diđer mevzuatta ve milletlerarası hukuki metinlerde kabul edilen "hasta hakları"nın somut olarak göstermek ve sađlık hizmeti verilen bütün kurum ve kuruluşlarda ve sađlık kurum ve kuruluşları dışında sađlık hizmeti verilen hallerde, insan haysiyetine yakışır şekilde herkesin "hasta hakları"ndan faydalanabilmesine, hak ihlallerinden korunabilmesine ve gerektiğinde hukuki korunma yollarını fiilen kullanabilmesine dair usul ve esasları düzenlemek amacı ile hazırlanmıştır.

Kapsam

Madde 2- Bu Yönetmelik; sađlık hizmeti verilen resmi ve özel bütün kurum ve kuruluşları, bu kurum ve kuruluşlarda veya bunların dışında hizmete katılan her kademedeki ve unvandaki ilgilileri ve hizmetten faydalanma hakkını haiz olan bütün fertleri kapsar.

Dayanak

MADDE 3 - (Başlığı ile birlikte deđişik:RG-16/1/2019-30657) Bu Yönetmelik; 7/5/1987 tarihli ve 3359 sayılı Sađlık Hizmetleri Temel Kanununa ve 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete'de yayımlanan 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinin 355 inci ve 508 inci maddelerine dayanılarak hazırlanmıştır.

(...)

DÖRDÜNCÜ BÖLÜM

Hasta Haklarının Korunması

Mahremiyete Saygı Gösterilmesi

Madde 21- Hastanın, mahremiyetine saygı gösterilmesi esastır. Hasta mahremiyetinin korunmasını açıkça talep de edebilir. Her türlü tıbbi müdahale, hastanın mahremiyetine saygı gösterilmek suretiyle icra edilir.

Mahremiyete saygı gösterilmesi ve bunu istemek hakkı;

- a) Hastanın, sağlık durumu ile ilgili tıbbi değerlendirmelerin gizlilik içerisinde yürütülmesini,
- b) Muayenenin, teşhisin, tedavinin ve hasta ile doğrudan teması gerektiren diğer işlemlerin makul bir gizlilik ortamında gerçekleştirilmesini,
- c) Tıbben sakınca olmayan hallerde yanında bir yakınının bulunmasına izin verilmesini,
- d) Tedavisi ile doğrudan ilgili olmayan kimselerin, tıbbi müdahale sırasında bulunmamasını,
- e) Hastalığın mahiyeti gerektirmedikçe hastanın şahsi ve ailevi hayatına müdahale edilmemesini,
- f) Sağlık harcamalarının kaynağının gizli tutulmasını, kapsar.

Ölüm olayı, mahremiyetin bozulması hakkını vermez.

Eğitim verilen sağlık kurum ve kuruluşlarında, hastanın tedavisi ile doğrudan ilgili olmayanların tıbbi müdahale sırasında bulunması gerekli ise; önceden veya tedavi sırasında bunun için hastanın ayrıca rızası alınır.

(...)

Bilgilerin Gizli Tutulması

Madde 23- Sağlık hizmetinin verilmesi sebebiyle edinilen bilgiler, kanun ile müsaade edilen haller dışında, hiçbir şekilde açıklanamaz.

Kişinin rızasına dayansa bile, kişilik haklarından bütünüyle vazgeçilmesi, bu hakların başkalarına devri veya aşırı şekilde sınırlandırılması neticesini doğuran hallerde bilginin açıklanması, bunları açıklayanın hukuki sorumluluğunu kaldırmaz.

Hukuki ve ahlaki yönden geçerli ve haklı bir sebebe dayanmaksızın hastaya zarar verme ihtimali bulunan bilginin ifşa edilmesi, personelin ve diğer kimselerin hukuki ve cezai sorumluluğunu da gerektirir.

Araştırma ve eğitim amacı ile yapılan faaliyetlerde de hastanın kimlik bilgileri, rızası olmaksızın açıklanamaz.

Özel Hastaneler Yönetmeliđi

Resmî Gazete Tarihi : 27.03.2002

Resmî Gazete Sayısı : 24708

ÖZEL HASTANELER YÖNETMELİĐİ

BİRİNCİ KISIM

Genel Hükümler

BİRİNCİ BÖLÜM

Amaç, Kapsam, Hukukî Dayanak ve Tanımlar

Amaç

Madde 1- Bu Yönetmeliđin amacı; etkin, verimli ve kaliteli sađlık hizmeti sunulmasını sađlamak üzere, bütün özel hastanelerin tesis, hizmet ve personel standartlarının tespit edilmesine, (Deđişik ibare:RG-21/10/2006-26326) sınıflandırılmasına, sınıflarının deđiştirilmesine, amaca uygun olarak teşkilatlandırılmasına ve bunların açılmalarına, faaliyetlerine, kapanmalarına ve denetlenmelerine ilişkin usûl ve esasları düzenlemektir.

Kapsam

Madde 2- (Deđişik birinci fıkra:RG-14/01/2004-25346) Bu Yönetmelik; Devlete, il özel idarelerine, belediyelere, üniversitelere ve diđer kamu tüzelkişilerine ait hastaneler hariç olmak üzere; gerçek kişiler ve özel hukuk tüzelkişilerine ait hastaneleri kapsar.

Bu Yönetmeliđe tâbi olmayan yataklı tedavi kurumlarının açılma, tesis, hizmet, personel ve kapanma durumları ile diđer durum deđişikliklerinin ilgili kamu tüzel kişilerince Sađlık Bakanlıđına bildirilmesi ve ilgili diđer mevzuatın öngördüđu bilgi ve belgelerin Bakanlıđa verilmesi zorunludur.

Dayanak

MADDE 3 - (Deđişik:RG-25/8/2016-29812)

Bu Yönetmelik; 7/5/1987 tarihli ve 3359 sayılı Sađlık Hizmetleri Temel Kanununun 3 üncü maddesi ile 9 uncu maddesinin birinci fıkrasının (c) bendi ve Ek 11 inci maddesi ile (Deđişik ibare:RG-31/5/2019-30790) 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete’de yayımlanan 1 sayılı

Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinin 355 inci maddesinin birinci fıkrasının (a) ve (c) bentleri ile 508 inci maddesine dayanılarak hazırlanmıştır.

(...)

ALTINCI BÖLÜM

Tıbbî Kayıt ve Arşiv, Faturalandırma ve Hastaya Verilecek Belgeler

Tıbbî kayıt

Madde 48- Özel hastanelerin acil servis, poliklinik, klinik, röntgen, laboratuvar ve ameliyathane gibi tıbbî hizmet ünitelerinde, sayfa ve sıra numarası verilmiş ve her sayfası müdürlükçe mühürlenmiş protokol defterlerinin tutulması zorunludur.

Özel hastanelere başvuran her hasta için hasta dosyası düzenlenir. Hasta dosyasına hastanın tedavisiyle ilgili bütün müşahadeler ve yapılan muayene, tahlil ve tetkik sonuçları ile tedavi ve günlük değişiklikler yazılır.

(Değişik fıkra:RG-22/3/2017-30015) Hasta dosyası içerisinde, asgarî olarak aşağıdaki belgelerin bulunması şarttır:

- a) Hasta kabul kâğıdı,
- b) Tıbbî müşahade ve muayene kâğıdı,
- c) Hasta tabelası,
- ç) Hemşire gözlem kâğıdı,
- d) Röntgen ve laboratuvar istek kâğıdı ve tetkik raporları,
- e) Ameliyat kâğıdı,
- f) Hastanın muayene istek formu,
- g) Çıkış özeti,
- ğ) Uygulanacak tedavinin kabul edildiğine dair olan ve 1/8/1998 tarihli ve 23420 sayılı Resmî Gazete’de yayımlanan Hasta Hakları Yönetmeliğinin ilgili maddesi uyarınca alınmış rızayı gösteren muvafakat formu.

Tıbbî arşiv ve Bakanlığa yapılacak bildirimler

Madde 49- Özel hastanelerde, muayene, teşhis ve tedavi amacıyla başvuran hasta, yaralı, acil ve adli vakalar ile ilgili olarak yapılan tıbbî ve idarî işlemlere ilişkin kayıtların, düzenlenen ve kullanılan belgelerin toplanması ve bunların müteakip başvurular ile denetim ve adlî mercilerce her istenildiğinde hazır bulundurulması amacıyla tasnif ve muhafazaya uygun bir merkezî tıbbî arşiv kurulması zorunludur. (Ek cümle:RG-22/3/2017-30015) Merkezi tıbbî arşivin hastane bünyesinde bulunması zorunlu değildir.

İlgili diğer mevzuat hükümleri saklı kalmak kaydıyla, özel hastanede tutulan hasta dosyaları, en az yirmi yıl süre ile saklanır.

Faaliyeti sona eren özel hastanelerin arşiv belgeleri, bir tutanağa bağlanarak müdürlüğe teslim edilir.

(Değişik dördüncü fıkra:RG-31/5/2019-30790) Özel hastaneler tarafından kayıt altına alınan kişisel sağlık verileri, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ikincil düzenlemelere uygun bir şekilde Bakanlıkça belirlenen usul ve esaslar çerçevesinde merkezi sağlık veri sistemine aktarılır ve işlenir. Bakanlık tarafından kurulan kayıt ve bildirim sistemine ve Bakanlıkça yapılacak diğer iş ve işlemlere esas olmak üzere, istenilen bilgi ve belgelerin Bakanlığa gönderilmesi zorunludur.

(Ek fıkra:RG-23/9/2010-27708) Özel hastaneler, kliniklerinde takip ettikleri gebeler, yenidoğan ve bebeklerin izlenmesi ve kontrolü için Bakanlıkça istenilen kayıt ve bildirimleri istenilen formatta ve sürelerde Bakanlıkça belirlenen birime bildirir.

(Ek fıkra:RG-23/9/2010-27708) (Değişik:RG-1/7/2014-29047) Hasta mahremiyeti dikkate alınmak kaydıyla, ortak kullanım alanları kamera kayıt sistemi ile kayıt altına alınır ve kamera görüntüleri en az iki ay süre ile saklanır.

Kayıtların bilgisayar ortamında tutulması

Madde 50- (Değişik:RG-21/10/2006-26326)

Özel hastanelerde, bu Yönetmelikte belirtilmiş her türlü kayıt işlemi, bilgisayar ortamında ve/veya ihtiyaca göre yazılı kayıt sistemi ile tutulabilir. Bu amaçla, bilgisayar çıktılarının sistem dahilinde ilk numaradan başlayarak numaralandırılması ve mesul müdür tarafından onaylanması zorunludur.

Bilgisayar ortamındaki kayıtların, denetim veya başkaca resmî amaçla istenildiğinde, bilgisayar ekranında izlenen belgeyle daha önceki çıktıların tutarlılık göstermesi zorunludur.

Bu kayıtların bilgisayar ortamında saklanması, değiştirilmesinin ve silinmesinin önlenmesi, gizliliğin ihlal edilmemesi amacıyla fizikî, manyetik veya elektronik müdahalelere ve olası suistimallere karşı gerekli idarî ve teknik tedbirlerin alınmasından ve periyodik olarak

denetlenmesinden mesul müdür sorumludur. Mevcut yedekleme sisteminden günlük, haftalık, aylık ve yıllık olmak üzere veriler yedeklenir.

Adli vakalara ve adli raporlara ait kayıtların gizliliği ve güvenliği açısından vakayı takip eden tabip dışında vaka hakkında veri girişi yapılamaması yada adli raporu tanzim eden tabibin onayından sonra kendisi dahil hiç kimsenin rapor ile ilgili değişiklik yapamaması için gerekli düzenlemeler yapılır. Adli vaka kayıtlarına mesul müdür veya yetkilendirdiği kişiler erişebilir. Ancak, yetkililerin rapor üzerinde hiçbir şekilde değişiklik yapmasına izin verilmez. Adli kayıt veya raporların resmi olarak istenmesi halinde yeni çıktı alınarak suret olduğu belirtilmek kaydıyla tasdiklenebilir. Bu raporlar ile ilgili sorumluluk mesul müdüre ve hastane sahibine aittir.

Güvenli dijital hasta kaydına geçilmeyen hastanelerde bilgisayar ortamında kayıt tutulması, yazılı kayıt sisteminin gereklerini ortadan kaldırmaz. (Ek cümle:RG-27/5/2012-28305) 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu hükümlerine uygun elektronik imza ile imzalanmış tıbbi kayıtlar, resmi kayıt olarak kabul edilir ve ilgili mevzuata göre yedekleme ve arşivlemesi yapılır.

Hastane faturalarının düzenlenmesi

Madde 51- (Değişik birinci fıkra:RG-21/3/2014-28948) Özel hastanelerde ayakta veya yatarak tedavi edilen bütün hastalar için ilgili mevzuatına göre satış fişi veya fatura düzenlenmesi zorunludur. Satış fişi veya fatura ekinde hastaya sunulan sağlık hizmetinin ayrıntılı dökümünü ve birim fiyatlarını gösteren belge düzenlenir.

(Mülga ikinci fıkra:RG-13/04/2003-25078)

Özel hastanelerde kullanılan ilaç ve tıbbî malzemeler ile ayrıca verilen içecek, gazete, kitap, telefon konuşması ve benzeri ihtiyaçlar için alınacak ücret, piyasa rayiç bedellerinin üzerinde olamaz.

Hastalara verilecek belgeler

Madde 52- Özel hastaneler, hastalar tarafından istenildiğinde, aşağıda belirtilen belgeleri ücretsiz olarak vermek zorundadırlar:

- a) Özel hastanede kullanılıp bedeli hastadan alınan ilaç ve sarf malzemesinin tür ve miktarlarını gösteren liste,
- b) (Değişik:RG-22/3/2017-30015) Adli vakalara ilişkin olanların asılları verilmemek kaydıyla, özel hastanede veya dışarıda yapılan ve bedeli hasta tarafından ödenen her türlü tetkik, tahlil ve görüntüleme sonuçları,
- c) Dışarıdan satın alınan ilaç ve malzemenin reçeteleri,

d) Hastaların klinik ve laboratuvar bulguları, hastalığın teşhisi, seyri, yapılan incelemeler ile tedavi ve sonucuna ilişkin tedaviyi yapan tabip tarafından düzenlenecek çıkış özeti.

Kan ve Kan Ürünleri Yönetmeliđi

Resmî Gazete Tarihi :

Resmî Gazete Sayısı :

KAN VE KAN ÜRÜNLERİ YÖNETMELİĐİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliđin amacı, transfüzyon merkezi, kan bađışı merkezi ve bölge kan merkezlerinin kurulması, cihaz, malzeme ve personel standartlarının belirlenmesi, birbirleriyle olan ilişkileri ile çalışma usûl ve esaslarının tespiti, uygulayacakları kalite güvence programlarına dair usûl ve esaslar, ruhsat alınması ile bedelleri ve iptaline ilişkin usûl ve esaslar ile Kan ve Kan Ürünleri Kurulunun çalışma usûl ve esaslarını belirlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, kan ve kan bileşenleri ile ilgili faaliyetlerde bulunan bütün kamu kurum ve kuruluşlarını, gerçek ve özel hukuk tüzel kişilerini kapsar.

(2) Bu Yönetmeliđin uygulanmasında 9/1/2007 tarihli ve 26398 sayılı Resmî Gazete’de yayımlanan Tıbbi Cihaz Yönetmeliđi ile 9/1/2007 tarihli ve 26398 sayılı Resmî Gazete’de yayımlanan Vücut Dışında Kullanılan Tıbbi Tanı Cihazları Yönetmeliđi hükümleri saklıdır.

(3) İnsan kanı ve plazmasından endüstriyel yöntemlerle kamu ya da özel kurumlar tarafından elde edilen ve özellikle albumin, immünoglobulin ve koagülasyon faktörleri gibi ürünleri içeren kan bileşenlerine dayalı tıbbi ürünler, kan, kök hücreleri bu Yönetmeliđin kapsamı dışındadır.

Dayanak

MADDE 3 - (1) Bu Yönetmelik 11/4/2007 tarihli ve 5624 sayılı Kan ve Kan Ürünleri Kanununun 7 nci maddesi ile 13/12/1983 tarihli ve 181 sayılı Sağlık Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 43 üncü maddesine dayanılarak hazırlanmıştır.

(...)

İKİNCİ BÖLÜM

Genel Esaslar, Kan ve Kan Ürünleri Kurulu

Gönüllülük esası

MADDE 5 - (1) Kan ve kan bileşenleri ve ürünlerinin temininde karşılıksız, gönüllü ve düzenli bağış esastır. Ancak malî karşılık anlamına gelmeyecek şekilde kan bağışçısını teşvik edici uygulamalar müstesnadır.

(2) Hizmet birimleri kendi yetki ve sorumluluklarında olmak şartı ile; karşılıksız, gönüllü ve düzenli bağışı teşvik etmek amacıyla, kamu yararına hizmette bulunan kurumlarla işbirliği içinde ve Bakanlık bilgilendirerek çeşitli kampanyalar ve eğitim toplantıları düzenleyebilir. Ancak bu faaliyetler kesinlikle ticari amaç ve muhteva içeremez.

Görev ve sorumluluklar

MADDE 6 - (1) Kan ve kan ürünleri ile ilgili hizmetlerin planlanması, yürütülmesinin izlenmesi, hizmet birimlerinin açılması ve denetlenmesi hususlarında Bakanlık yetkili ve sorumludur.

(2) Yurt içinde toplanan plazmanın ürün üretimi amacıyla yurt içinde ve yurt dışında değerlendirilmesi veya ürün üretimi amacıyla yurt dışından plazma getirilmesi için gerekli izin Bakanlıkça verilir.

(3) Bakanlık, kan ve kan ürünleri konusunda yapacağı çalışmalarda gerekli bilimsel desteği sağlamak üzere Kan ve Kan Ürünleri Kurulunu oluşturur.

(4) Bakanlık gerektiğinde bilimsel ve danışman nitelikli komisyonlar oluşturur. Komisyonlar, kendi çalışma usul ve esaslarını belirler.

(5) Kan ve kan bileşenlerinin bağışçıdan temininden alıcıya verilmesine kadar bağışçı ve alıcının sağlığının tehlikeye düşürülmemesi, tıbbî risklere karşı korunması, transfüzyonun güvenle yapılması, transfüzyon sonrası bağışçı ve alıcının izlenmesi ilgili hizmet biriminin görevidir.

(6) Kan ve kan bileşenlerinin alınması, test edilmesi, işlenmesi, depolanması, kullanılır hale getirilmesi, kullanıma sunulması, dağıtılması ve transfüzyon uygulamalarının geri bildirimini izlenmesi, ilgili hizmet biriminin sorumluluğundadır.

(7) Hizmet birimlerinin rehberde belirlenen faaliyetleri yazılı veya elektronik ortamda kaydedilir ve 15 yıl saklanır. Bağışçıların temel test sonuçları elektronik ortamda 30 yıl saklanır. Saklanması zorunlu kayıt içerikleri EK-6'da belirtilen şekilde düzenlenir. Bağışçı şahit numuneleri 1 yıldan az olmamak şartıyla rehberde belirlenen şekilde ve sürede saklanır.

(8) Hizmet birimleri, bağışçı kişisel bilgilerini korumak, üçüncü kişilere vermemek, basına açıklamamak ile yükümlüdür. Her hizmet biriminin veri güvenliği ile ilişkili usul ve esasları bulunur ve bilgilerin korunma ve/veya açıklanması bu usul ve esaslara uygun olarak yapılır.

(9) Hizmet birimleri bağışçı bilgilendirilmesinden sorumludur.

(10) Kan, kan bileşenleri ve ürünlerinin bağışçıdan alınması ve alıcıya transfüzyonu hekim sorumluluğu ve denetimi altında yapılır.

(11) Hizmet birimleri faaliyetlerini kalite yönetim sistemi çerçevesinde yürütür.

(12) BKM'ler olağanüstü haller ile sıkıyönetim, seferberlik ve savaş halinde gerekebilecek kan ve kan ürünleri ile bunlar için gerekli malzemenin temini ve ülke çapında stoklanmasını Bakanlığın planlaması çerçevesinde organize eder.

(...)

Dokümantasyon

MADDE 16 - (1) Hizmet biriminin yürüttüğü tüm faaliyetleri kapsayan spesifikasyonlar, prosedürler ve kayıtları kapsayan dokümanlar oluşturulur ve güncellenir.

(2) Kayıtlar el yazısı ile okunaklı olarak veya mikrofilm ya da bilgisayar ortamında tutulur.

(3) Belgeler üzerinde yalnızca yetkili kişi değişiklik yapar. Değişiklik durumunda tarih ve imza atılır, gözden geçirilir, derhal uygulamaya konur.

(4) Tüm dokümanlar denetimler sırasında hazır bulundurulur.

İstenmeyen ciddi etki ve olayların bildirim

MADDE 17 - (1) Hizmet birimleri, kan ve kan bileşenlerinin kalite ve güvenliğine bağlı olabilecek transfüzyon öncesinde, sırasında veya sonrasında gözlenen istenmeyen ciddi etkilerin ve olayların kayıtlarını tutar ve Bakanlığa bildirir. Bildirim, rehberde yer alan "İstenmeyen ciddi etki ve olayların bildirim"ne göre yapılır.

(...)

KAN BAĞIŞÇISINDAN ALINMASI VE

BAĞIŞÇIYA VERİLMESİ GEREKEN BİLGİLER

(BÖLÜM A)

Kan ve kan bileşenleri bağışçı yapacak muhtemel vericilere sağlanacak bilgiler

1. Kanın esas yapısı, kan bağıışı işlemi, tam kandan elde edilen bileşenler ve aferez bağıışların hastalara sağladığı önemli faydalar hakkında kamuoyu tarafından anlaşılabilir eksiksiz eğitim materyalleri sağlanır.

2. Hem allojenik hem de otolog bağıışlarda vericilerin muayenesi sağlık ve tıbbi geçmişe, bağıışların test edilmesine ihtiyaç duyulmasının nedenleri açıklanır ve rızanın önemi belirtilir.

Allojenik bağıışlar için kişisel red, geçici ve kalıcı red ve alıcı için bir risk olması halinde kişilerin neden kan ve kan bileşenleri bağıışlamaması gerektiğinin nedenleri açıklanır.

Otolog bağıışlar için red olasılığı ve otolog kan ve kan bileşenlerinin vericisi ya da alıcısı olarak kişinin sağlığı için risk oluşturması halinde bağıış işleminin gerçekleşmemesinin nedenleri açıklanır.

3. Kişisel verilerin korunmasına ilişkin bilgi: Vericinin kimliği, vericinin sağlığı ile ilgili bilgiler ve gerçekleştirilen testlerin sonuçları izinsiz ifşa edilemez.

4. Kişilerin kendi sağlıklarına zarar verebilecek bağıışlarda bulunmamalarını gerektiren nedenler belirtilir.

5. Hem allojenik hem otolog bağıışlarda uygulanan işlemlerin yapısı ve bunlara bağılı riskler ile ilgili spesifik bilgiler verilir. Otolog bağıışlar için otolog kan ve kan bileşenlerinin amaçlanan transfüzyon gerekleri için yeterli gelmeme olasılığı belirtilir.

6. Vericiler için, gerçekleşecek bir işlemde önce fikirlerini değıştirme seçeneklerine ilişkin bilgi ya da bağıış sürecinin herhangi bir anında, herhangi bir usulsüzlük, utanç ya da rahatsızlık olmaksızın geri çekilme ya da kişisel-red imkanına ilişkin bilgi verilir.

7. Hizmet birimleri, vericinin önceki bağıışının, transfüzyon için herhangi bir nedenle uygun olmaması durumunda, konuya ilişkin neden bilgi vermesinin gerektiğinin önemi hakkında vericiyi bilgilendirir.

8. Test sonuçlarının vericinin sağlığında özel bir anormalliğı göstermesi halinde hizmet biriminin bağıışçıyı uygun bir mekanizma ile bilgilendirme sorumluluğuna ilişkin bilgi verilir.

9. Kullanılmamış otolog kan ve kan bileşenlerinin neden atıldığı ve diğere hastalara transfüzyon edilmediğı ile ilgili bilgi verilir.

10. HIV, HBV, HCV virüslerinin ya da kanla geçebilecek diğere mikrobiyolojik ajanların markerlarının tespit edildiğı, test sonuçlarının vericinin reddedilmesine neden olduğı ve alınan ünitenin yok edilmesi ile sonuçlanacağına dair bilgi verilir.

11. Vericilerin her zaman soru sorma fırsatının olduğuna dair bilgi verilir.

Bulaşıcı Hastalıklar Sürveyans ve Kontrol Esasları Yönetmeliği

Resmî Gazete Tarihi : 30.05.2007

Resmî Gazete Sayısı : 26537

BULAŞICI HASTALIKLAR SÜRVEYANS VE KONTROL ESASLARI YÖNETMELİĞİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak, Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmelik;

- a) Bulaşıcı hastalıkların önlenmesi ve kontrolünün sağlanması için; bildirim esas bulaşıcı hastalıklar listesinin belirlenmesi, olay ve vaka tanımlarının yapılması, iletişim ağı yapısı ile ihbar ve bildirim sisteminin oluşturulması,
- b) Bulaşıcı hastalıkların epidemiyolojik sürveyansı için her türlü uygun teknik araç kullanılarak sürveyans ile ilgili bilgilerin toplanmasında görevli yerel sağlık otoriteleri, ilgili diğer Bakanlıklar, özel ve kamuya ait kurum ve kuruluşlar ile Sağlık Bakanlığı arasında iletişimin sağlanması ve toplanan sürveyans verilerinin ulusal ve uluslararası düzeyde paylaşılması için gerekli yöntemlerin belirlenmesi,
- c) (Değişik:RG-4/5/2019-30764) Bulaşıcı hastalık açısından erken uyarı ve cevap sisteminde yer alan olaylar ile uyarı düzeylerinin tanımlanması,
- ç) Hastalıklara özgü genel veya özel sürveyans ve kontrol mekanizmalarının veya programlarının geliştirilmesi,
- d) Salgınların saptanması ve kontrolü için gerekli olan müdahale yöntemlerinin belirlenmesi, amacıyla hazırlanmıştır.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, bütün kamu kurum ve kuruluşları ile özel hukuk tüzel kişilerini ve gerçek kişileri kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik 24/4/1930 tarih ve 1593 sayılı Umumi Hıfzıssıhha Kanununun 3 üncü, 57 nci ve 64 üncü maddelerine, (Değişik ibare:RG-4/5/2019-30764) 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete’de yayımlanan 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinin 361 inci maddesinin birinci fıkrasının (c) bendine ve 508 inci maddesine, 7/5/1987 tarih ve 3359 sayılı Sağlık Hizmetleri Temel Kanununun 3 üncü maddesinin (b) ve (f) bentlerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (Değişik:RG-4/5/2019-30764)

(1) Bu Yönetmeliğin uygulanmasında;

a) Bakanlık: Sağlık Bakanlığını,

b) Bildirim sistemi: Bu fıkranın (d), (e), (f), (g), (ğ), (h) ve (ı) bentlerinde belirtilen aktivitelerin gerçekleştirilmesine yönelik gerekli bilginin paylaşılması için oluşturulan sistemi,

c) Bulaşıcı hastalık: Enfekte olmuş bir kişi ile doğrudan temas yoluyla veya bir vektör, hayvan, ürün veya çevreye maruz kalma gibi dolaylı yollardan veya bulaşıcı madde ile kirlenmiş olan sıvı alışverişi yolu ile insandan insana bulaşan, bir mikroorganizma veya onun toksik ürünlerine bağlı olarak ortaya çıkan hastalığı,

ç) Bildirimi zorunlu bulaşıcı hastalık: Ek-I’de yer alan bildirim zorunlu bulaşıcı hastalıkları,

d) Bulaşıcı hastalıkların önlenmesi ve kontrolü: Bulaşıcı hastalıkların yayılmasını önlemek ve durdurmak amacıyla epidemiyolojik araştırmalar da dâhil olmak üzere alınan önlemlerin tümünü,

e) Erken uyarı ve cevap sistemi (EUCS): Biyolojik, çevresel, kimyasal, radyolojik ve nükleer etkenler ile kaynağı bilinmeyen ve salgın yapma potansiyeli taşıyan durum ve olaylarla ilgili, zamanında veri ve bilgi toplayan, analiz eden, entegre sürveyans ile yerel, bölgesel, ulusal ve uluslararası düzeydeki ani gelişen halk sağlığı tehditlerinin yayılmasını önleme ve kontrol etmeyi içeren faaliyetleri,

f) Göstergelye dayalı sürveyans: Hastalıklarla ilgili önceden belirlenmiş verilerin rutin bir şekilde toplandığı, analiz edildiği, yorumlandığı ve geri bildirimini yapıldığı sürveyans yöntemini,

g) Olaya dayalı sürveyans: Hastalık kümelenmeleri, açıklanamayan ölümler gibi halk sağlığı olaylarının erken tespiti, bildirim, doğrulanması, değerlendirilmesi ve raporlanması amacıyla akut halk sağlığı olayları ile ilgili verilerin hızlı bir şekilde toplanması, analiz edilmesi, yorumlanması ve geri bildirimini yapıldığı sürveyans yöntemini,

- ğ) Salgın: Belirli bir alanda, belirli bir grup insan arasında, belirli bir süre boyunca beklenenden daha fazla vaka görülmesi veya salgın potansiyeli olan ve epidemiyolojik olarak bağlantılı iki veya daha fazla vaka ya da yeni görülen/elimine edilmiş veya eradike edilmiş hastalığa ait tek bir vakanın görülmesini,
- h) Sendromik sürveyans: Belirli bir hastalığa özgü olmayan tanı veya semptomlardan oluşan sağlık ile ilgili verilerin toplandığı, analiz edildiği, yorumlandığı ve geri bildirimini yapıldığı sürveyans yöntemini,
- ı) Sürveyans: Herhangi bir hastalık, durum veya olay ile ilgili olarak uygun koruyucu ve karşı önlemlerin önerilmesi, alınması ve uygulanması amacıyla, verilerin, sürekli ve sistematik bir şekilde toplanması, analiz edilmesi, yorumlanması ve ilgili taraflarla paylaşılmasını,
- i) Topluluk ağı: Bulaşıcı hastalıkların sürveyansı ve kontrolü ağı olarak adlandırılan ve Avrupa Parlamentosu ve Konseyinin 22 Ekim 2013 tarihli ve 1082/2013/EU kararında bahsi geçen faaliyetlerin gerçekleştirilmesine yönelik gerekli bilginin paylaşılması için oluşturulan sistemi,
- j) Vaka: Sürveyans amaçları veya salgın için yapılmış bir vaka tanımı ile uyumlu bir hastalığa ya da sağlık sorununa sahip kişiyi,
- k) Vaka tanımı: Belli bir hastalığın bildirim, sürveyansı veya salgın araştırma amaçları için bir bireyin "vaka" olarak tanımlanabilmesinde bir arada bulunması gereken tanısal kriterler setini,
- l) Vaka sınıflaması: Kriterlerin destekleme derecesine göre "vaka" olma olasılığının derecelendirilmesini,
- m) Şüpheli vaka: Genellikle laboratuvar kriterleri ya da epidemiyolojik kriterler olmadan klinik tanımlamaya uyan vakayı,
- n) Olası vaka: Genellikle klinik tanımlamaya uyan, epidemiyolojik bağlantılı veya bazı hastalıklarda destekleyici laboratuvar kriterleri de kullanılan vakayı,
- o) Kesin vaka: Genellikle klinik tanımlamaya uyan, epidemiyolojik bağlantılı ve/veya doğrulayıcı laboratuvar kriterlerini karşılayan, yüksek düzeyde seçici olan hastalığa spesifik vakayı,
- ö) Klinik tanımlama: Klinik kriterlerden birisi ve/veya birkaçının tek başına ya da birlikte verilmesi ile hastalığın tarif edilmesini,
- p) Klinik kriter: Vakayı açıklamak için kullanılan klinik ölçütleri,
- r) Laboratuvar kriteri: Bir vakanın kesin tanısının konması için gereken bir ya da birden fazla laboratuvar yöntemini,

s) Epidemiyolojik kriter: Epidemiyolojik bağlantının kurulabildiği durumlarda hastalıkla ilgili olarak kullanılan ve hastalığın bazı epidemiyolojik özelliklerini açıklamak için kullanılan kriterleri,

ş) Epidemiyolojik bağlantı: Hastalık için bilinen inkübasyon dönemi içinde, her hastalık için değişebilmekle birlikte; insandan insana bulaş, hayvandan insana bulaş, ortak bir kaynağa maruziyetle bulaş, kontamine olmuş gıda ya da içme suyu ile bulaş, çevresel bir etkene maruziyet ile bulaş ve laboratuvar maruziyeti ile bulaş yollarından birisi veya birkaçının bulunmasını,

t) Yerel sağlık birimi: Bakanlığın taşra teşkilatını,

ifade eder.

İKİNCİ BÖLÜM

Bulaşıcı Hastalıkların Sürveyansı ve Kontrolünün Genel Esasları, İl Bulaşıcı

Hastalık Danışma Komisyonu ve Ulusal Odak Noktası(2)

Bulaşıcı hastalıkların sürveyansı ve kontrolünün genel esasları

MADDE 5 - (Başlığı ile Birlikte Değişik:RG-4/5/2019-30764)

(1) İhbar ve bildirimlerin düzenlenmesi, takip edilmesi ve gerektiğinde bildirim zorunlu bulaşıcı hastalık tanısı alan vakalar için sürveyans çalışmalarını yürütmek üzere 100 veya daha fazla yatak kapasitesine sahip tüm yataklı tedavi kurumlarında hekim sorumluluğunda sürveyans birimi oluşturulur. Daha az yatak kapasitesine sahip yataklı tedavi kurum ve kuruluşlarında bu işlemler sürveyans sorumluları tarafından yürütülür.

(2) Tüm gerçek ve tüzel kişiler bulaşıcı hastalıkların sürveyansı ve kontrolü çalışmalarında görevli personele gerekli destek ve kolaylığı sağlamak zorundadır.

İl bulaşıcı hastalık danışma komisyonu

MADDE 6 - (Başlığı ile Birlikte Değişik:RG-4/5/2019-30764)

(1) İlde görülen bulaşıcı hastalıkları izlemek, bu konuda yürütülen çalışmaları değerlendirmek, gerekli durumlarda yapılacak müdahalelere yönelik önerilerde bulunmak ve koordinasyonu sağlamak üzere il sağlık müdürlüklerinde İl Bulaşıcı Hastalık Danışma Komisyonu oluşturulur.

(2) İl Bulaşıcı Hastalık Danışma Komisyonunun teşkili ile çalışma usul ve esasları Bakanlık tarafından belirlenir.

Laboratuvar hizmetleri alanında görev yapacak komisyon

MADDE 7 - (Mülga:RG-4/5/2019-30764)

Ulusal odak noktası

MADDE 8 - (Başlığı ile Birlikte Değişik:RG-4/5/2019-30764)

(1) Uluslararası Sağlık Tüzüğü kapsamında uluslararası önemi haiz halk sağlığı acil durumlarında ülke adına Dünya Sağlık Örgütü ve diğer üye ülkelerin ulusal odak noktaları ile haberleşmek üzere Bakanlıkça ulusal odak noktası belirlenir.

ÜÇÜNCÜ BÖLÜM

Bildirim Usul ve Esaslarının Belirlenmesi

Bilgi akış sisteminin çalışma esasları

MADDE 9 - (Değişik:RG-4/5/2019-30764)

(1) Bildirime esas bulaşıcı hastalıklar ile diğer bulaşıcı hastalıklarla veya halk sağlığı tehdidi oluşturabilecek durumlar ile ilişkili göstergelere dayalı sürveyans, olaya dayalı sürveyans ve sendromik sürveyansa dair bilgi akış sistemi Bakanlık tarafından belirlenir.

Bildirim sorumluları

MADDE 10 - (1) Bildirim sistemi kapsamında bir bulaşıcı hastalığın ihbarı ve bildiriminden, Bakanlığın belirlediği usul ve esaslar çerçevesinde sağlık hizmeti veren bütün kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler sorumludur.

(2) Bu kişi ve kuruluşlar;

a) (Değişik:RG-4/5/2019-30764) Bildirime esas bulaşıcı hastalıklar ile sürveyans sistemleri kapsamında yer alan diğer bulaşıcı hastalıklar ve olayları, bunlar için uygulanan kontrol önlemlerine dair bilgilerle birlikte bulaşıcı hastalık vakalarının görülmesi veya yeniden ortaya çıkışı ile ilgili bilgileri,

b) (Değişik:RG-4/5/2019-30764) Bir salgının gelişmekte olduğunu düşündüren her türlü uyarı ve/veya bilgiyi,

c) Beklenmedik bir epidemiyi veya kaynağı ya da etkeni bilinmeyen yeni bir bulaşıcı hastalık ile ilgili bilgileri,

ç) Komşu ülkelerde görülen bulaşıcı hastalıkları,

d) Özellikle olağanüstü durumlarda olmak üzere, bulaşıcı hastalıkların kontrolü ve önlenmesine yönelik olarak yapılmış çalışmalara ilişkin bilgi ve belgeleri,

e) Uygulanan tüm mücadele önlemleri de dahil olmak üzere, bulaşıcı hastalıkların önlenmesi ve kontrolü için Bakanlığa çalışmaların koordinasyonunda yardımcı olacak ilgili görüşleri,

derhal yerel sađlık birimine bildirmekle ykmldr.

(3) Yerel sađlık birimi 2'nci fıkrada bahsi geen bilgileri Bakanlıđa iletmekle ykmldr.

KiŐisel verilerin iŐlenmesi

MADDE 11 - (1) Epidemiyolojik srveyans ve bildirim sistemi ile elde edilen bilgilerden kiŐisel verilerin iŐlenmesi sırasında kiŐinin dokunulmazlıđı, maddi ve manevi varlıđı ile temel hak ve zgrlkleri korunur. (DeđiŐik cmle:RG-4/5/2019-30764) KiŐisel veriler, 24/3/2016 tarihli ve 6698 sayılı KiŐisel Verilerin Korunması Kanunu ve diđer mevzuata uygun olarak korunur.

Diđer gerek ve tzel kiŐilerle iŐbirliđi

MADDE 12 - (1) Bakanlık, hayvan sađlıđına, gıda gvenliđine ve evre sađlıđına iliŐkin unsurların bulaŐıcı hastalıklar zerine etkilerini gz nne alarak, ilgili btn kamu kurum ve kuruluŐları, gerek ve tzel kiŐilerle gerekli iŐbirliđini yapar.

zel sađlık sorunları

MADDE 13 - (1) Bakanlık bulaŐıcı hastalıkların kontrol kapsamında nazokomiyal enfeksiyonlar ve antimikrobiyal diren gibi zel sađlık sorunlarına zg epidemiyolojik srveyans ve bildirim sistemi oluŐturur.

Tanı ve referans laboratuvarları

MADDE 14 - (1) Bakanlık, bildirime esas bulaŐıcı hastalıkların tanısı, srveyansı ve kontrol kapsamında mikrobiyolojik tanı ve referans laboratuvarlarının alıŐma usul ve esaslarını belirler.

Yerel sađlık birimlerinin alıŐma usul ve esasları

MADDE 15 - (1) Bakanlık, bildirime esas bulaŐıcı hastalıkların srveyansı ve kontrol kapsamında il dzeyinde grev yapan tm birimlerin alıŐma usul ve esaslarını belirler.

zel srveyans ve kontrol programları

MADDE 16 - (1) Bakanlık, bildirime esas bulaŐıcı hastalıklar listesinde yer alan hastalıklar iin gerektiđinde zel srveyans ve kontrol programları oluŐturur ve yrtr; bu amala yerel odak noktalarını ve alıŐma sistemlerini belirler.

(2) Bakanlık, uluslararası dzeyde hastalıđa zg srveyans ađlarına katılır ve gerekli iletiŐimi sađlamak zere ulusal odak noktalarını tespit eder.

(3) Bakanlık, gerekli gördüğü takdirde, bildirim esas bulaşıcı hastalıklar listesi haricinde diğer hastalıklara özgü genel veya özel sürveyans ve kontrol programları oluşturabilir ve yürütebilir. Bu amaçla yerel odak noktalarını ve çalışma sistemlerini belirleyebilir.

Verilerin değerlendirilmesi

MADDE 17 - (1) (Değişik:RG-4/5/2019-30764) Bakanlık, bulaşıcı hastalıkların sürveyansı kapsamında gelen bilgileri değerlendirir.

(2) Bulaşıcı hastalıkların sürveyansı ile ilgili çalışmaları yürüten birimlerden Bakanlıkça belirlenmiş odak noktaları (Değişik ibare:RG-4/5/2019-30764) erken uyarı ve cevap sistemi de dahil olmak üzere uluslararası kuruluşlar ve toplulukların ağları ile iletişimi sağlar.

(3) Bu iletişim her bir kuruluş veya ağ tarafından belirlenmiş prosedüre göre yürütülür.

Bildirim sistemi kapsamındaki hastalıklar

MADDE 18 - (1) Bildirim sistemi kapsamında yer alan hastalıkların listesi bu Yönetmeliğin ekinde yer alan (EK-I)'de, seçim ölçütleri (EK-II)'de, vaka tanımları ise (EK-III)'te belirtilmiştir.

DÖRDÜNCÜ BÖLÜM

Erken Uyarı ve Cevap Sistemi

Erken uyarı ve cevap sistemi oluşturulması

MADDE 19 - (1) Bakanlık ulusal düzeyde bulaşıcı hastalıklarla mücadele ve bunların kontrolüne yönelik olarak bir (Değişik ibare:RG-4/5/2019-30764) erken uyarı ve cevap sistemi oluşturur.

Erken uyarı ve cevap sistemi kapsamındaki olay ve durumlar

MADDE 20 - (Başlığı ile Birlikte Değişik:RG-4/5/2019-30764)

(1) Halk sağlığı riski taşıyan ve EUCS kapsamında tespit edilen, değerlendirilen ve gerektiği durumda müdahale edilen ve paydaşlara bildirilmesi gereken olay ve durumlar şunlardır:

- a) Yayılma potansiyeli olan, önemli hastalık yüküne veya ölümlere yol açabilecek kümelenme, salgın hastalık veya sağlıkla ilgili olaylar,
- b) Yeni veya yeniden ortaya çıkan/çıkma olasılığı bulunan hastalık veya durumlar,
- c) Ani olarak meydana gelen ve kısa sürede çok sayıda kişiyi etkileme olasılığı bulunan durumlar,
- ç) Kişi, yer, zaman analizlerinde sıra dışı aktivite artışının görüldüğü durumlar,
- d) Beklenenden fazla ölümlerin tespit edildiği durumlar,

- e) Henüz insanda hastalık oluşturmamış ancak maruz kalmaya bağlı olarak hastalık yapma potansiyeli olan olaylar,
- f) Olası sağlık etkileri bulunabilecek kitlesel insan hareketleri,
- g) Halk sağlığını etkileme potansiyeli olan doğal afetler, beklenmedik hava olayları,
- ğ) Kamuoyunu meşgul eden ve halk sağlığı riski olan diğer sağlık olayları,
- h) Uluslararası önemi haiz halk sağlığı acil durumları.

Erken uyarı düzeyi 0 ve erken uyarı düzeyi 1

MADDE 21 - (Başlığı ile Birlikte Değişik:RG-4/5/2019-30764)

(1) 20 nci maddede yer alan olaylardan herhangi birinin bulunmadığı durum "Erken Uyarı Düzeyi 0" olarak tanımlanır.

(2) 20 nci maddede yer alan olaylardan herhangi birinin görülme olasılığının bulunması durumunda "Erken Uyarı Düzeyi 1" olarak tanımlanır ve Bakanlıkça belirlenen usule göre bilgi paylaşımını gerektirir.

Erken uyarı düzeyi 2

MADDE 22 - (Değişik:RG-4/5/2019-30764)

(1) 20 nci maddede yer alan olaylardan herhangi birinin kanıta dayalı veri/bilgiye göre meydana gelme, toplumu etkileme riskinin yüksek olasılık olduğu durum "Erken Uyarı Düzeyi 2" olarak tanımlanır ve potansiyel tehdit olarak adlandırılır.

Erken uyarı düzeyi 3

MADDE 23 - (Değişik:RG-4/5/2019-30764)

(1) 20 nci maddede yer alan olaylardan herhangi birinin ani gelişen halk sağlığı tehdidi ile sonuçlanması durumunda "Erken Uyarı Düzeyi 3" olarak tanımlanır ve kesin tehdit olarak adlandırılır.

Kamuoyuna bilgi verilmesi

MADDE 24 - (1) 20 nci maddedeki tarif edilen bir olay geliştiğinde ilgili meslek gruplarına ve kamuoyuna olay ve alınacak önlemler hakkında yerel sağlık otoritesi veya Bakanlık tarafından bilgi verilir. Ayrıca halk sağlığı tehdidi ortadan kalktığında bu durum ilgili taraflara gecikme olmaksızın bildirilir.

Erken uyarı düzeylerine göre alınacak önlemler

MADDE 25 - (Başlığı ile Birlikte Değişik:RG-4/5/2019-30764)

(1) Ulusal düzeyde erken uyarı düzeyi ve uluslararası yayılma riski taşıyan tehditler Bakanlıkça belirlenir ve uluslararası kuruluşlarla bilgi paylaşılır.

(2) Bakanlık erken uyarı ve cevap sistemi kapsamında her bir erken uyarı düzeyinde alınacak önlemler ve sistemin işleyişine ilişkin düzenlemeleri yapar.

BEŞİNCİ BÖLÜM

Salgınların Araştırılması ve Kontrolü

Salgınların araştırılması ve kontrolü

MADDE 26 - (1) Bakanlık, salgınların araştırılması ve kontrolü ile ilgili gerekli düzenlemeleri yapar.

Diğer gerçek ve tüzel kişilerle işbirliği

MADDE 27 - (1) Salgınların hayvan sağlığı, gıda güvenliği ve çevre sağlığı ile ilişkisi göz önünde bulundurularak, Bakanlık ve yerel sağlık birimi, ilgili tüm kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerle gerekli işbirliğini yapar.

Salgın raporu hazırlanması

MADDE 28 - (1) Bakanlık ve yerel sağlık birimi incelenen bütün salgınların raporlarını hazırlar ve Bakanlığın belirlediği kurallara göre ilgili yerlere gönderir.

ALTINCI BÖLÜM

Çeşitli ve Son Hükümler

Eğitim

MADDE 29 - (1) Bakanlık, bulaşıcı hastalıkların epidemiyolojik sürveyansı, bildirim sisteminin işletilmesi, (Değişik ibare:RG-4/5/2019-30764) erken uyarı ve cevap sisteminin oluşturulması ve kullanılması, salgınların araştırılması ve kontrolünde görevlendirilmek üzere, Bakanlık merkezinde ve her ilde, saha epidemiyolojisi, laboratuvar uygulamaları ve bulaşıcı hastalıkların kontrolü konularında personeli eğitir ve bu eğitimlerin sürekliliğini sağlar.

(2) Bakanlık, bu amaçlara özgü ulusal ve uluslararası kuruluşlar ve toplulukların iletişim ağları ile işbirliği yaparak bir eğitim müfredatı geliştirilmesi için gerekli düzenlemeleri yapar, uygular ve değerlendirir.

(3) Bakanlık, merkezde ve illerde saha epidemiyolojisi, laboratuvar uygulamaları ve bulaşıcı hastalıkların kontrolü konularında eğitilmiş personelin atama ve nakillerinde eğitim aldıkları alanda görev yapmaları için gerekli tedbirleri alır.

Yayın hazırlama ve dağıtma

MADDE 30 - (1) Bakanlık, bu Yönetmelik kapsamındaki faaliyetler ve sonuçları ile ilgili süreli yayınların ve bültenlerin hazırlanması, ulusal veya uluslararası düzeyde yayımlanması için gerekli tedbirleri almak zorundadır.

Cezai hükümler

MADDE 30/A - (Ek:RG-4/5/2019-30764)

(1) Bu Yönetmelik hükümlerine aykırı hareket edenler hakkında 1593 sayılı Umumi Hıfzıssıhha Kanununun 282 nci maddesi ile 3359 sayılı Sağlık Hizmetleri Temel Kanununun Ek 11 inci maddesine göre işlem yapılır.

Yürürlük

MADDE 31 - (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 32 - (1) Bu Yönetmelik hükümlerini Sağlık Bakanı yürütür.

Uluslararası Sağlık Turizmi ve Turistin Sağlığı Hakkında Yönetmelik

Resmî Gazete Tarihi : 13.07.2017

Resmî Gazete Sayısı : 30123

ULUSLARARASI SAĞLIK TURİZMİ VE TURİSTİN SAĞLIĞI HAKKINDA YÖNETMELİK BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı, uluslararası sağlık turizmi ve turistin sağlığı kapsamında uluslararası düzeyde sunulan sağlık hizmetlerinin asgari hizmet sunum standartlarının belirlenmesi, uluslararası sağlık turizmi hizmetlerinde faaliyet yürütecek sağlık kuruluşları ile aracı kuruluşların yetkilendirilmesi ve bu faaliyetlerin denetlenmesine ilişkin usul ve esasları düzenlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, 31/5/2006 tarihli ve 5510 Sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu ve milletlerarası ikili mütekabiliyet anlaşmaları kapsamına girmeyen, ancak; yurtdışından sağlık hizmeti almak amacıyla ülkemize gelenler ile turist olarak ülkemizde bulunduğu sırada sağlık hizmeti ihtiyacı ortaya çıkan kişiler ve bu kişilere sağlık hizmeti sunan kamu, üniversite ve özel sağlık kurum ve kuruluşları ile aracı kuruluşları kapsar.

(2) Aşağıdaki durumlar bu yönetmelik kapsamında yer almaz:

a) Savaş, afet, açlık ve benzeri olağanüstü durumlarda, Bakanlar Kurulunca, Başbakanlık veya ilgili Bakanlığın talimatıyla belirlenen ülkelerden, Türkiye’de buldukları sürede sağlık hizmeti alan veya bu ülkelerden sivil toplum kuruluşları tarafından tedavi amacıyla getirilerek tedavi bedeli ödenen yabancı hasta ve yaralılar.

b) Bakanlığımız veya Türk İşbirliği ve Koordinasyon Ajansı (TİKA) veya Başbakanlık Yurtdışı Türkler ve Akraba Topluluklar Başkanlığı tarafından uygun görülen sivil toplum kuruluşları tarafından Balkanlardan ve Türk Cumhuriyetlerinden ülkemize tedavi amaçlı getirilen hastalar.

c) Türk İşbirliği ve Koordinasyon Ajansı Başkanlığı (TİKA) tarafından getirilen hastalar.

ç) Türkiye Cumhuriyeti'nin imzalamış olduğu uluslararası anlaşma uyarınca Sosyal Güvenlik Sözleşmeleri kapsamında sağlık yardımı alma hakkı olan ülke vatandaşları ile Türkiye Cumhuriyeti vatandaşlarını ve ülkemize sağlık alanında milletlerarası ikili işbirliği anlaşması kapsamında tedavi için gelenler.

d) Ülkemize eğitim, öğretim, kurs için gelen kişiler ve bunların eğitimleri süresince bakmakla yükümlü oldukları yakınları.

e) Geçici korunanlar, mülteciler, sığınma başvurusu sahibi ve iltica başvurusu sahibi statüsünde olanlar, sığınmacılar, vatansızlar, insan ticareti mağdurları.

f) 29/5/2009 tarihli ve 5901 sayılı Türk Vatandaşlığı Kanununun 28 inci ve 44 üncü maddesi kapsamında bulunanlar.

g) Türk soylu olduğuna dair belge ibraz eden Türk soylu yabancılar.

ğ) Adli vaka kapsamında kolluk kuvvetlerince getirilerek acil sağlık hizmeti alan yabancılar.

(3) İkinci fıkrada yer alan kişiler, kendi isteği ile uluslararası sağlık turizmi kapsamında ücret ödemeyi taahhüt etmesi durumunda bu Yönetmelik kapsamında uluslararası sağlık turizmi hizmeti alabilir.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 7/5/1987 tarihli ve 3359 sayılı Sağlık Hizmetleri Temel Kanununun 9 uncu maddesinin (c) bendine ve Ek 11 inci maddesine, 11/10/2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 8 inci maddesinin birinci fıkrasının (a) ve (i) bentlerine ve 40 inci maddesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Yönetmelikte geçen;

a) Bakanlık: Sağlık Bakanlığını,

b) Genel Müdürlük: Sağlık Hizmetleri Genel Müdürlüğünü,

c) Müdürlük: İl /İlçe Sağlık Müdürlüklerini,

ç) SATURK: 2015/3 sayılı Başbakanlık Genelgesi ile oluşturulan Sağlık Turizmi Koordinasyon Kurulunu,

d) Uluslararası sağlık turizmi: Sağlık amaçlı yurtdışından ülkemize geçici bir süreliğine gelen, Türkiye Cumhuriyeti vatandaşı olmayan veya Türkiye Cumhuriyeti vatandaşı olmakla birlikte

yurtdışında ikamet eden gerçek kişilerin aldıkları her türlü sağlık hizmeti ile bunlarla ilgili destek hizmetlerini,

e) Turistin sağlığı: Ülkemizde herhangi bir nedenle geçici süreli olarak bulunan yabancıların, ülkemizde buldukları sırada ani gelişen hastalıklarda ve acil durumlarda sağlık hizmeti almasını,

f) Uluslararası sağlık turisti: Uluslararası sağlık turizmi ve turistin sağlığı kapsamında sağlık hizmeti alan hastayı,

g) Uluslararası sağlık turizmi aracı kuruluşu: Bakanlıkça, uluslararası sağlık turisti ile beraberindeki refakatçi ve diğer yakınlarına konaklama, ulaşım ve transfer hizmetlerinin sağlanması faaliyetlerini yürütmek üzere yetkilendirilen, 14/9/1972 tarihli ve 1618 sayılı Seyahat Acentaları ve Seyahat Acentaları Birliği Kanunu uyarınca işletme belgesi alan A grubu seyahat acentalarını,

ğ) Uluslararası sağlık turizmi sağlık tesisi: Sağlık tesisi ruhsatına sahip olan ve Bakanlıkça uluslararası sağlık turizmi yetki belgesi verilen kamu, üniversite ve özel sağlık kurum ve kuruluşunu,

h) Yabancı: Türkiye Cumhuriyeti Devleti ile vatandaşlık bağı bulunmayan kişiyi,

ı) Yetki belgesi: Uluslararası sağlık turizmi yetki belgesini,

ifade eder.

İKİNCİ BÖLÜM

Uluslararası Sağlık Turizmi

Genel esaslar

MADDE 5 - (1) Uluslararası sağlık turizmi kapsamında faaliyette bulunabilmek için; sağlık tesisinin ve aracı kuruluşun uluslararası sağlık turizmi yetki belgesi alması zorunludur. Yetki belgesi almayanların uluslararası sağlık turizmi faaliyetleri Bakanlıkça durdurulur.

(2) Uluslararası sağlık turizmi sağlık tesisinde bu Yönetmelikteki kriterlere uygun olarak teşhis, tedavi ve rehabilite edici sağlık hizmetleri ile geleneksel ve tamamlayıcı tıp uygulamaları sunulabilir.

(3) Uluslararası sağlık turizmi sağlık tesisi, kendisine doğrudan başvuran uluslararası sağlık turistini kabul edebilir. Ancak aracı kuruluş faaliyetlerine ihtiyaç duyulması halinde, Bakanlıkça yetki verilen uluslararası sağlık turizmi aracı kuruluşu ile protokol yapılması zorunludur. İmzalanan protokolün bir örneği Müdürlük aracılığıyla Genel Müdürlüğe gönderilir.

(4) Uluslararası sağlık turistinin yatışından taburcu edilinceye kadar sağlık tesisinde alacağı sağlık hizmetinin yanında ihtiyaç duyacağı diğer hizmetleri sunmak da uluslararası sağlık turizmi sağlık

tesisinin sorumluluğundadır. Bu hizmetlerin sunumu için, uluslararası sağlık turizmi aracı kuruluşu ile sözleşme yapabileceği gibi diğer kurum ve kuruluşlarla da sözleşme yapabilir.

(5) Uluslararası sağlık turizmi sağlık tesisi tarafından, bu Yönetmelik kapsamında sağlık hizmeti verilen kişilerin Bakanlıkça oluşturulan web tabanlı sisteme kaydedilmesi zorunludur.

(6) Uluslararası sağlık turizmi sağlık tesisi tarafından kayıt altına alınan kişisel sağlık verileri, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununa uygun bir şekilde işlenir ve Bakanlıkça belirlenen usul ve esaslara uygun bir şekilde merkezi sağlık veri sistemine aktarılır.

(7) Uluslararası sağlık turizmi sağlık tesisi ve uluslararası sağlık turizmi aracı kuruluşu, Bakanlıkça istenilen bilgi ve belgeleri göndermekle yükümlüdür.

Uluslararası sağlık turizmi birimi

MADDE 6 - (1) Uluslararası sağlık turizmi sağlık tesisinde, uluslararası sağlık turistinin kabul, kayıt, teşhis, tedavi, faturalandırma, taburculuk, tercümanlık ve aracı kuruluşlarla ilgili iş ve işlemlerin koordinasyonu ile görevli uluslararası sağlık turizmi birimi oluşturulur.

(2) Uluslararası sağlık turizmi biriminde bir tabip/uzman tabip uluslararası sağlık turizmi birimi sorumlusu olarak görevlendirilir ve Müdürlüğe bildirilir.(1) Uluslararası sağlık turisti potansiyeline göre, uluslararası sağlık turizmi birimi sorumlu yardımcısı olarak bir sağlık meslek mensubu görevlendirilebilir. Uluslararası sağlık turizmi sorumlusu ve uluslararası sağlık turizmi birimi sorumlu yardımcısı olarak görevlendirileceklerin aşağıdaki nitelikleri taşıması şarttır:

a) Türkiye’de sanatını yapmaya mezun olmak.

b) Bu maddenin dördüncü fıkrasında belirtilen yeterlilikte yabancı dil bilgisine sahip olmak.

c) Türkiye’de iki yılı kamu ya da özel sağlık kuruluşlarında olmak üzere, en az beş yıl meslek icrası yaptığını gösteren belge veya belgelere sahip olmak.

(3) Uluslararası sağlık turizmi biriminde, sorumlu dâhil yabancı dil bilen en az 2 personel istihdam edilir. Yabancı dilin birisinin İngilizce olması zorunludur.

(4) Yabancı dil yeterliliği için aşağıdaki belgelerden en az birine sahip olmak gerekir.

a) İngilizce veya hizmet sunulacak uluslararası sağlık turisti dilinden Yükseköğretim Kurulu tarafından yapılan ya da yaptırılan sınavda veya Ölçme, Seçme ve Yerleştirme Merkezi Başkanlığı tarafından yapılan Yabancı Dil Bilgisi Seviye Tespit Sınavında yüz üzerinden en az altmış beş puan almış olmak ya da ÖSYM tarafından bu puana denk kabul edilen uluslararası geçerliliği bulunan bir belgeye sahip olmak.

b) İngilizceden veya hizmet sunulacak uluslararası sağlık turistinin dilinden Avrupa Dil Portfolyosunda yer alan B2 dil düzeyini gösterir belgeye sahip olmak.

c) Çifte vatandaşlık kimliği olanların Türkçe dilinden Avrupa Dil Portfolyosunda yer alan B2 dil düzeyini gösterir belgeye sahip olması.

ç) Lisans düzeyinde mütercim ve tercümanlık bölümünden mezun olduğuna dair belgeye sahip olmak.

(5) Uluslararası sağlık turizmi biriminde, turistin sağlığı kapsamında bulunan kişiler ile milletlerarası sosyal güvenlik sözleşmesi ve sağlık alanında milletlerarası ikili işbirliği anlaşmaları gereği sağlık hizmeti almak için ülkemize gelen kişilere, yönlendirme ve rehberlik hizmetleri de sunulur.

Yetkinlik kriterleri

MADDE 7 - (1) Uluslararası sağlık turizmi alanında Bakanlıkça Uluslararası Sağlık Turizmi Yetki Belgesi verilebilmesi için:

a) Sağlık tesisinin, EK-1'de yer alan Uluslararası Sağlık Turizmi Sağlık Tesisi Yetkinlik Kriterlerinde belirtilen kriterleri taşıması zorunludur.

b) Aracı kuruluşun, EK-2'de yer alan Uluslararası Sağlık Turizmi Aracı Kuruluşu Yetkinlik Kriterlerinde belirtilen kriterleri taşıması zorunludur.

Yetki belgesi

MADDE 8 - (1) Yetki belgesi alabilmek için, sağlık tesisi/aracı kuruluş tarafından, hizmet verdiği faaliyet alanıyla ilgili EK-3'te yer alan yetki belgesi başvuru formu doldurulur, aynı ekte belirtilen başvuru evrakları forma eklenir ve bunlarla Müdürlüğe başvuru yapılır.

(2) Müdürlük tarafından, bu Yönetmeliğin ekindeki yetkinlik kriterlerini taşıyıp taşımadığı dosya üzerinde incelenir. İnceleme sonucunda başvuru evraklarında eksiklik veya kriterlere uygunsuzluk tespit edilmesi hâlinde, yedi iş günü içerisinde sağlık tesisine/aracı kuruluşa bildirilir.

(3) Başvuru evraklarında eksiklik veya kriterlere uygunsuzluk bulunmadığı anlaşılan sağlık tesisi/aracı kuruluş, Müdürlükçe oluşturulan inceleme ekibi tarafından yerinde incelenir. Yerinde inceleme neticesinde yetkinlik kriterleri bakımından uygunluğuna karar verilen başvurular onbeş iş günü içerisinde Bakanlığa gönderilir. Bakanlıkça da uygun görülmesi halinde, sağlık tesisine EK-4/A'da yer alan ve aracı kuruluşa EK-4/B'de yer alan Uluslararası Sağlık Turizmi Yetki Belgesi düzenlenir.

ÜÇÜNCÜ BÖLÜM

Turistin Saęlıęı

Turistin saęlıęı kapsamındaki hizmetler

MADDE 9 - (1) Ülkemizde toplantı, kongre, ticari veya turizm amaçlı süreli olarak kalan yabancılar, ülkemizde buldukları sırada gelişen hastalıklarında ve acil durumlarında kamu, üniversite veya özel saęlık kuruluşlarında sunulan saęlık hizmetlerinden yararlanabilir.

(2) Acil saęlık hizmetleri ve acil hasta nakilleri ücreti karşılıęı sunulur. Ancak, yurtdışında yaşayan ve hiçbir sosyal güvencesi olmayan Türkiye Cumhuriyeti vatandaşlarına 112 acil saęlık hizmetleri ücretsiz sunulur. Kamu tarafından verilen ambulans hizmeti ile acil hasta naklinden elde edilen gelir, hastaya ilk müdahale eden müdürlük döner sermayesine yatırılır.

(3) Acil saęlık hizmeti almak için saęlık tesisine başvuru yapan yabancı hastaların kabul edilmesi ve gerekli tıbbi müdahalenin kayıtsız-şartsız ve gecikmeksizin yapılması zorunludur. Hizmet bedelinin tahsiliyle ilgili işlemler, acil müdahale ve bakım saęlandıktan sonra yapılır.

(4) Trafik kazaları sonucunda verilecek saęlık hizmetlerinin bedeli, Türk vatandaşları ve yabancı uyruklu kişilerin uyruęuna ve sosyal güvencesinin olup olmadığına bakılmaksızın ilgili kanun gereęi Sosyal Güvenlik Kurumundan tahsil edilir. Trafik kazalarında, kişinin bizzat kendisinden tedavi bedeli talep edilemez. Ancak trafik kazası nedeniyle acil saęlık hizmeti alan kişinin, isteęe baęlı ilave seyahat sigortası var ise bu sigortaya fatura edilerek poliçe kapsamında ödeme tahsil edilir.

DÖRDÜNCÜ BÖLÜM

Fiyatlandırma ve Fatura İşlemleri ile Bilgilendirme ve Tanıtım

Fiyatlandırma

MADDE 10 - (1) Bu Yönetmelik kapsamında sunulacak uluslararası saęlık turizmi kapsamında verilen saęlık hizmetinin bedeli, SATURK'un görüşü alınarak Bakanlıkça belirlenir.

(2) Uluslararası saęlık turizmi saęlık tesisleri, Bakanlıkça belirlenen saęlık turizmi fiyat tarifesinde belirlenen usul ve esaslara uymakla yükümlüdür.

Fatura düzenlenmesi ve verilecek belgeler

MADDE 11 - (1) Uluslararası saęlık turizmi saęlık tesisleri tarafından, saęlık turizmi kapsamında hizmet alanlar için ilgili mevzuatna göre satış fişi veya fatura düzenlenmesi zorunludur. Satış fişi veya fatura ekinde hastaya sunulan saęlık hizmetinin ayrıntılı dökümünü ve birim fiyatlarını gösteren belge düzenlenir. Ayrıca, hizmet alan kişiler tarafından istenildiğinde, aşağıda belirtilen belgelerin de ücretsiz olarak verilmesi zorunludur:

a) Uluslararası sađlık turizmi tesisi tarafından;

1) Uluslararası sađlık turizmi sađlık tesisinde kullanılıp bedeli hastadan alınan ila ve sarf malzemesinin tr ve miktarlarını gsteren liste.

2) Adli vakalara iliřkin olanların asılları verilmemek kaydıyla, sađlık tesisinde veya dıřarıda yapılan ve bedeli hasta tarafından denen laboratuvar tetkik ve tahlil sonuları ile rntgen filmleri.

3) Dıřarıdan satın alınan ila ve malzemenin reeteleri.

b) Uluslararası sađlık turizmi aracı kuruluđu tarafından;

1) Uluslararası sađlık turisti ile beraberindeki refakati ve diđer yakınlarına sunulan konaklama, ulařım ve transfer, tercmanlık ve danıřmanlık gibi hizmetler iin talep edilen cretlerin ayrıntılı dkm.

Bilgilendirme ve tanıtım

MADDE 12 - (1) Uluslararası sađlık turizmi ile ilgili olarak bu Ynetmelik erevesinde yetki verilmemiř sađlık tesisi ve aracı kuruluřlar tarafından bilgilendirme ve tanıtım yapılamaz.

(2) Uluslararası sađlık turizmi kapsamındaki tanıtım faaliyetlerinin ařađıda belirtildiđi řekilde yrtlmesi zorunludur:

a) Trkiye sınırları ierisinde talep oluřturacak řekilde ve Trke dilinde tanıtım yapılamaz. Tanıtımlar, tanıtım yapılacak lkelerin dilleri ve/veya İngilizce dilinde yapılabilir.

b) Uluslararası sađlık turizmi sađlık tesisi ile uluslararası sađlık turizmi aracı kuruluřları tarafından internet sitelerinde, sađlık turizmi kapsamında sunulacak hizmetlere iliřkin bilgiler ve detaylı ulařım bilgileri son gncelleme tarihi belirtilerek yayınlanır.

c) Tanıtımlarda, yetkili olunmayan, sađlık tesisinin ruhsat ve faaliyet izin belgesinde kayıtlı olmayan sađlık hizmetleri hakkında bilgilere, mesleki ve etik kurallara aykırı, yanıř, yanıltıcı ve yurtiindeki vatandaşlar iin talep oluřturmaya ynelik bilgilere yer verilemez.

) İnternet sitesi ile diđer tanıtım ara ve gerelerinde sađlık ile ilgili bilgilendirmeler, alanında bilgi ve tecrbeye sahip hukuken yetkili sađlık meslek mensupları tarafından yapılır.

d) Tanıtımlarda; tedavi gren hastaların hikyelerine, hasta mahremiyeti gzetilmek, hasta haklarına uygun olmak ve bu konuda hasta onamının alındıđını belgelendirmek kaydıyla yer verilebilir.

e) Yrrlkteki mevzuata gre lkemizde uygulanması yasaklanmış veya uygulanmasına izin verilmemiř olan tıbbi iřlem ve uygulamalara tanıtımlarda yer verilemez.

BEŞİNCİ BÖLÜM

Çeşitli ve Son Hükümler

Eğitim

MADDE 13 - (1) Uluslararası sağlık turizmi alanında gerçekleştirilecek sertifikasyon ve meslek edindirme eğitimleri Bakanlık ve Yükseköğretim Kurulu ile yapılan işbirliği çerçevesinde yürütülür.

Denetim

MADDE 14 - (1) Uluslararası sağlık turizmi sağlık tesisi ile uluslararası sağlık turizmi aracı kuruluşu, şikâyet veya soruşturma hariç olmak üzere, bu Yönetmeliğe uygunluk bakımından, Müdürlük tarafından, yılda en az bir defa denetlenir. Denetimlerde bu Yönetmeliğin genel hükümlerinin yanında, Yönetmelik ekinde yer alan yetkinlik kriterleri ve müeyyide formu kullanılır.

(2) Uluslararası sağlık turizmi ve turistlerin sağlığı uygulaması sırasında oluşabilecek anlaşmazlıklar ile ilgili şikâyetlerin değerlendirilmesi için gerekli kayıt ve bildirim sistemi Bakanlık tarafından kurulur. Şikâyet usulü ile ilgili olarak yabancılar, uluslararası sağlık turizmi sağlık tesisi tarafından sağlık hizmet sunumu öncesinde bilgilendirilir.

(3) Bu Yönetmelikte belirtilen usul ve esaslara uymadığı için sağlık turizmi faaliyeti durdurulan sağlık tesisi ve aracı kuruluşu, Bakanlıkça Ekonomi Bakanlığına bildirilir.

Müeyyideler

MADDE 15 - (1) Bu Yönetmelikte belirtilen usul ve esaslara uymayanlar hakkında, EK-5' te ve EK-6' da yer alan idarî müeyyideler ile ilgili diğer mevzuat hükümleri uygulanır.

Mevcut uluslararası sağlık turizmi faaliyeti yürütenlerin durumu

GEÇİCİ MADDE 1 - (1) Bu Yönetmeliğin yürürlüğe girdiği tarihten önce uluslararası sağlık turizmi faaliyeti yürüten sağlık tesisi ve aracı kuruluşlar, yürürlük tarihinden itibaren 1 (bir) yıl içinde bu Yönetmelikteki yetkinlik kriterlerine uygunluk sağlayarak Bakanlıktan yetki belgesi almak zorundadır. Sürenin sonunda Uluslararası Sağlık Turizmi Yetki Belgesi almamış olanların bu Yönetmelik kapsamındaki faaliyetleri durdurulur.

Yürürlük

MADDE 16 - (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 17 - (1) Bu Yönetmelik hükümlerini Sağlık Bakanı yürütür.

Tıbbi Cihaz Yönetmeliği

Resmî Gazete Tarihi : 02.06.2021

Resmî Gazete Sayısı : 31499 Mükerrer

TIBBİ CİHAZ YÖNETMELİĞİ

BİRİNCİ KISIM

Amaç, Kapsam, Dayanak, Tanımlar ve Ürünlerin Mevzuat Durumu

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç ve kapsam

MADDE 1 - (1) Bu Yönetmeliğin amacı; hastalar, kullanıcılar ve diğer kişiler için sağlığın yüksek seviyede korunmasını esas alarak, tıbbi cihazlar için yüksek kalite ve güvenilirlik standartları belirleyerek, insan kullanımına yönelik tıbbi cihazların ve bunların aksesuarlarının piyasaya arz edilmesi, piyasada bulundurulması veya hizmete sunulmasıyla ilgili usul ve esasları belirlemektir. Bu Yönetmelik ayrıca, tıbbi cihazlara ve aksesuarlarına ilişkin yürütülen klinik araştırmalara da uygulanarak klinik araştırmalardan elde edilen verilerin güvenilir ve sağlam olmasını ve klinik araştırmaya katılan gönüllülerin güvenliğinin korunmasını sağlamayı da amaçlar.

(2) Bu Yönetmeliğin amacı doğrultusunda tıbbi cihazlar, tıbbi cihaz aksesuarları ve bu Yönetmeliğin uygulandığı Ek XVI'da listelenen ürünler, bundan sonra "cihaz" olarak adlandırılır.

(3) Bu Yönetmelik;

a) İn vitro tanı cihazları haricindeki tüm tıbbi cihazlara,

b) 9 uncu madde uyarınca kabul edilen ortak spesifikasyonların uygulanma tarihinden itibaren, özellikle benzer teknolojiyi esas alan tıbbi amaçlı benzer cihazlar için mevcut uyumlaştırılmış standartları ve en son teknolojik gelişmeleri dikkate almak suretiyle, Ek XVI'da listelenen tıbbi amaçlı olmayan ürün gruplarına ve bu ürün grupları ile ilgili klinik araştırmalara,

c) Cansız veya cansız hale getirilmiş hayvan kaynaklı dokular veya hücreler ya da bunların türevleri kullanılarak imal edilen cihazlara,

ç) Cansız veya cansız hale getirilmiş insan kaynaklı dokuların veya hücrelerin türevleri kullanılarak imal edilen cihazlara

uygulanır.

(4) Bu Yönetmelik;

a) tarihli ve sayılı Resmî Gazete’de yayımlanan İn Vitro Tanı Amaçlı Tıbbi Cihaz Yönetmeliği kapsamında yer alan in vitro tanı cihazlarına,

b) 19/1/2005 tarihli ve 25705 sayılı Resmî Gazete’de yayımlanan Beşeri Tıbbi Ürünler Ruhsatlandırma Yönetmeliğinin 4 üncü maddesinin birinci fıkrasının (c) bendinde tanımlandığı şekilde tıbbi ürünlere,

c) Beşeri Tıbbi Ürünler Ruhsatlandırma Yönetmeliği kapsamındaki ileri tedavi tıbbi ürünlere,

ç) İnsan kanına, kan ürünlerine, insan kaynaklı plazma veya kan hücrelerine ya da altıncı fıkrada atıfta bulunulan cihazlar hariç olmak üzere piyasaya arz edildiğinde ya da hizmete sunulduğunda bu gibi kan ürünlerini, plazma veya hücreleri ihtiva eden cihazlara,

d) 23/5/2005 tarihli ve 25823 sayılı Resmî Gazete’de yayımlanan Kozmetik Yönetmeliği kapsamındaki ürünlere,

e) Cansız veya cansız hale getirilmiş hayvan kaynaklı dokular veya hücreler ya da bunların türevleri kullanılarak imal edilen cihazlar hariç olmak üzere, hayvan kaynaklı transplantlara, dokulara veya hücrelere ya da bunların türevlerine veyahut bunları içeren ya da bunlardan oluşan ürünlere,

f) Cansız veya cansız hale getirilmiş insan kaynaklı dokuların veya hücrelerin türevleri kullanılarak imal edilen cihazlar hariç olmak üzere, 27/10/2010 tarihli ve 27742 sayılı İnsan Doku ve Hücreleri ile Bunlarla İlgili Merkezlerin Kalite ve Güvenliği Hakkında Yönetmelik kapsamında yer alan insan kaynaklı transplantlara, dokulara veya hücrelere ya da bunların türevlerine veyahut bunları içeren ya da bunlardan oluşan ürünlere,

g) (ç), (e) ve (f) bentlerinde atıfta bulunulan ürünlerden farklı olarak, ürünün kullanım amacını gerçekleştirmek veya desteklemek amacıyla, yaşayan mikro organizmalar, bakteriler, mantarlar veya virüsler dâhil canlı biyolojik materyal ya da canlı organizmalar içeren veya bunlardan oluşan ürünlere,

ğ) 11/6/2010 tarihli 5996 sayılı Veteriner Hizmetleri, Bitki Sağlığı, Gıda ve Yem Kanunu kapsamında yer alan gıdalara,

uygulanmaz.

(5) Piyasaya arz edildiğinde ya da hizmete sunulduğunda İn Vitro Tanı Amaçlı Tıbbi Cihaz Yönetmeliğinin 3 üncü maddesinin (ü) bendinde tanımlanan bir in vitro tanı cihazını bütünleşik parça olarak ihtiva eden bir cihaz, bu Yönetmelik hükümlerine tabi olur. Cihazın in vitro tanı cihazı olan parçası için İn Vitro Tanı Amaçlı Tıbbi Cihaz Yönetmeliği hükümleri uygulanır.

(6) Bir ürünün; Beşeri Tıbbi Ürünler Ruhsatlandırma Yönetmeliği ya da bu Yönetmelik kapsamında yer alıp almadığına karar verilirken, özellikle ürünün asli etki mekanizması dikkate alınır. Piyasaya arz edildiğinde veya hizmete sunulduğunda, Beşeri Tıbbi Ürünler Ruhsatlandırma Yönetmeliğinin 4 üncü maddesinin birinci fıkrasının (I) bendinde tanımlanan insan kanı veya insan plazmasından elde edilen bir tıbbi ürün de dâhil olmak üzere, ayrı olarak kullanıldığında aynı Yönetmeliğin 4 üncü maddesinin birinci fıkrasının (c) bendinde tanımlandığı şekilde bir tıbbi ürün olarak kabul edilen ve cihazın işlevine yardımcı olan bir maddeyi bütünleşik bir parça olarak ihtiva eden cihazlar bu Yönetmelik hükümlerine tabidir. Ancak bu madde, cihazın işlevine yardımcı olmayıp asli etki gösteriyor ise, bu bütünleşik ürün Beşeri Tıbbi Ürünler Ruhsatlandırma Yönetmeliğine tabi olur. Bu durumda, bu Yönetmeliğin Ek I'inde belirtilen ilgili genel güvenilirlik ve performans gereklilikleri, söz konusu cihaz parçasının güvenilirlik ve performansına yönelik uygulanır.

(7) Beşeri Tıbbi Ürünler Ruhsatlandırma Yönetmeliğinin tıbbi ürün ile ilgili hükümlerine hâle gelmeksizin, aynı Yönetmeliğin 4 üncü maddesinin birinci fıkrasının (c) bendinde tanımlanan bir tıbbi ürünü tatbik etme amaçlı bir cihaz bu Yönetmeliğe tabi olur. Ancak, bir tıbbi ürünü tatbik etme amaçlı cihaz ve tıbbi ürün, yalnızca belirtilen kombinasyonda kullanımı amaçlanan ve tekrar kullanılmayan bütünleşik tek bir ürün oluşturacak şekilde piyasaya arz ediliyor ise, bu bütünleşik tek ürün Beşeri Tıbbi Ürünler Ruhsatlandırma Yönetmeliğine tabi olur. Bu durumda, bu Yönetmeliğin Ek I'inde belirtilen ilgili genel güvenilirlik ve performans gereklilikleri, bütünleşik tek ürünün cihaz parçasının güvenilirlik ve performansına yönelik uygulanır.

(8) Piyasaya arz edildiğinde veya hizmete sunulduğunda, cihazın fonksiyonuna yardımcı olmak üzere cansız insan kaynaklı dokuları veya hücreleri ya da bunların türevlerini bütünleşik bir parça olarak ihtiva eden cihazlar bu Yönetmelik hükümlerine tabidir. Bu durumda, bağışlama, tedarik etme, test etme, işleme, koruma, depolama ve dağıtım ile ilgili mevzuat hükümleri de uygulanır. Ancak bu dokular veya hücreler ya da bunların türevleri, cihazın işlevine yardımcı olmayıp asli etki gösteriyorsa ve bu ürün Beşeri Tıbbi Ürünler Ruhsatlandırma Yönetmeliği kapsamında yer alan ileri tedavi tıbbi ürün değil ise, bağışlama, tedarik etme, test etme, işleme, koruma, depolama ve dağıtım ile ilgili mevzuata tabi olur. Bu durumda, bu Yönetmeliğin Ek I'inde belirtilen ilgili genel güvenilirlik

ve performans gereklilikleri, söz konusu cihaz parçasının güvenilirlik ve performansına yönelik uygulanır.

(9) Bu Yönetmelik kapsamında uygunluk değerlendirmesine tabi tutulan cihazlar için 2/10/2016 tarihli ve 29845 sayılı Resmî Gazete’de yayımlanan Elektromanyetik Uyumluluk Yönetmeliği (2014/30/AB) hükümleri aranmaz.

(10) Bu Yönetmeliğe tabi olup ayrıca 3/3/2009 tarihli ve 27158 sayılı Resmî Gazete’de yayımlanan Makina Emniyeti Yönetmeliği (2006/42/AT)’nin 4 üncü maddesinin birinci fıkrasının (ğ) bendi çerçevesinde makina olarak tanımlanan cihazlar, söz konusu Yönetmelik kapsamında ilgili tehlikelerin mevcut olduğu durumlarda, bu Yönetmeliğin Ek I’inin II. Bölümünde belirtilen genel güvenilirlik ve performans gerekliliklerinden daha spesifik olduğu ölçüde, Makina Emniyeti Yönetmeliği (2006/42/AT)’nin Ek I’inde belirtilen temel sağlık ve güvenlik gerekliliklerini de karşılar.

(11) Bu Yönetmelik, radyasyon güvenliği ve tıbbi ışınlamalara ilişkin mevzuatın uygulamasını etkilemez.

(12) Bu Yönetmelik, ikinci el satışlar gibi, tıbbi cihazların hâlihazırda hizmete sunulmuş olmasının ardından el değiştirmesi suretiyle piyasada bulundurulması ile ilgili kuralları kapsamaz.

(13) Bu Yönetmelik, kamu kurum ve kuruluşlarının, bu Yönetmelik kapsamında olmayan konulara ilişkin olarak, herhangi bir spesifik cihaz tipinin kullanımının kısıtlanmasına ilişkin hakkını etkilemez.

(14) Bu Yönetmelik, belirli cihazların yalnızca bir tıbbi reçeteyle temin edilebilmesi gerekliliği, belirli cihazları sadece belirli sağlık profesyonellerinin veya sağlık kuruluşlarının hazırlayabilmesi veya kullanabilmesi gerekliliği ya da belirli cihazların kullanımına spesifik profesyonel danışmanın eşlik etmesi gerekliliği gibi sağlık hizmetlerinin ve tıbbi bakımın organizasyonuna, sunumuna veya finansmanına ilişkin mevzuatın uygulanmasını etkilemez.

Dayanak

MADDE 2 - (1) Bu Yönetmelik; 5/3/2020 tarihli ve 7223 sayılı Ürün Güvenliği ve Teknik Düzenlemeler Kanununun 4 üncü maddesi ile 15/7/2018 tarihli ve 30479 sayılı Resmî Gazete’de yayımlanan 4 sayılı Bakanlıklara Bağlı, İlgili, İlişkili Kurum ve Kuruluşlar ile Diğer Kurum ve Kuruluşların Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinin 508 ve 796 ncı maddelerine dayanılarak hazırlanmıştır.

(...)

ÜÇÜNCÜ BÖLÜM

Tıbbi Cihazlara İlişkin Avrupa Veri Tabanı, Ulusal Ürün Takip Sistemi

Tıbbi cihazlara ilişkin Avrupa veri tabanı (EUDAMED)

MADDE 33 - (1) Komisyon tarafından aşağıda ifade edilen amaçlar doğrultusunda kurulup yönetilen ve tıbbi cihazlara ilişkin Avrupa veri tabanı olarak tanımlanan EUDAMED'e ilgili taraflarca veri girişi yapılır:

- a) Piyasaya arz edilen cihazlar, onaylanmış kuruluşlar tarafından düzenlenen ilgili sertifikalar ve ilgili iktisadi işletmeciler hakkında kamunun yeterince bilgilendirilmesine imkân sağlamak.
- b) Piyasada cihazların tekil tanımlanmasına imkân sağlamak ve onların izlenebilirliğini kolaylaştırmak.
- c) Kamunun, klinik araştırmalar hakkında yeterince bilgilendirilmesine ve klinik araştırmaların destekleyicilerininin 62 ila 79 uncu maddelerde ve 80 inci maddede belirtilen yükümlülükler ile Komisyonca kabul edilen tasarruflar kapsamındaki yükümlülüklere uymalarına imkân sağlamak.
- ç) İmalatçıların 85 ila 88 inci maddelerde veya Komisyonca kabul edilen tasarruflarda belirtilen bilgi yükümlülüklerine uymalarına imkân sağlamak.
- d) Yetkili otoritelerin ve Komisyonun bu Yönetmelikle ilgili görevlerini iyi bilgilendirilmiş bir temelde yürütmelerine imkân sağlamak ve aralarındaki iş birliğini güçlendirmek.

(2) EUDAMED aşağıdaki elektronik sistemleri içerir:

- a) 29 uncu maddenin dördüncü fıkrasında atıfta bulunulan, cihazların kaydına ilişkin elektronik sistem.
- b) 28 inci maddede atıfta bulunulan UDI veri tabanı.
- c) 30 uncu maddede atıfta bulunulan, iktisadi işletmecilerin kaydına ilişkin elektronik sistem.
- ç) 57 nci maddede atıfta bulunulan, onaylanmış kuruluşlara ve sertifikalara ilişkin elektronik sistem.
- d) 73 üncü maddede atıfta bulunulan, klinik araştırmalara ilişkin elektronik sistem.
- e) 89 uncu maddede atıfta bulunulan, vijilans ve piyasaya arz sonrası gözetime ilişkin elektronik sistem.
- f) 97 nci maddede atıfta bulunulan, piyasa gözetimi ve denetimine ilişkin elektronik sistem.

(3) Veriler; Türkiye ve AB üyesi ülkeler, onaylanmış kuruluşlar, iktisadi işletmeciler ve sponsorlar tarafından ikinci fıkrada atıfta bulunulan elektronik sistemlerle ilgili hükümlerde belirtildiği şekilde EUDAMED'e girilir.

(4) EUDAMED tarafından derlenen ve işlenen tüm bilgiler, yetkili otoriteler ve Komisyon için erişilebilir olur. Bilgiler; onaylanmış kuruluşlar, iktisadi işletmeciler, sponsorlar ve kamu için ikinci fıkrada atıfta bulunulan elektronik sistemler hakkındaki hükümlerde belirtilen ölçüde erişilebilir olur.

(5) EUDAMED, bu Yönetmelik uyarınca bilgileri toplamak ve işlemek üzere sadece ikinci fıkrada atıfta bulunulan elektronik sistemler için gerektiği ölçüde kişisel veri içerir. Kişisel veriler, veri sahiplerinin tanımlanmasına izin veren bir formda, 10 uncu maddenin sekizinci fıkrasında atıfta bulunulan süreleri aşmayacak şekilde tutulur.

(6) Veri sahiplerinin bilgiye erişim, düzeltme ve itiraz haklarını etkili şekilde kullanabilmeleri ve kendileriyle ilgili verilere erişim hakkı ile yanlış veya eksik verilerin düzeltilmesini ve silinmesini sağlama hakkını etkili şekilde kullanabilmeleri temin edilir. Bunu sağlamak amacıyla doğru olmayan ve yasalara aykırı bir şekilde işlenen veriler ivedilikle Komisyon'a bildirilir.

Ulusal ürün takip sistemi

MADDE 34 - (1) Bu Yönetmelikte belirtilen EUDAMED'le ilgili yükümlülükler hâle gelmeksizin yurt içinde yerleşik iktisadi işletmeciler, onaylanmış kuruluşlar, sağlık kuruluşları, sağlık profesyonelleri ve ilgili diğer kişiler; tıbbi cihazlara ilişkin ulusal ürün takip sistemi (ÜTS) ile ilgili yükümlülüklerini yerine getirir.

(2) ÜTS ile ilgili söz konusu yükümlülükler Kurum tarafından yayımlanan düzenlemeler ile belirlenir.

(...)

BİRİNCİ BÖLÜM

Klinik Değerlendirme ve Klinik Araştırmalar

Klinik değerlendirme

MADDE 61 - (1) Cihazın normal kullanım koşulları altında, Ek I'de belirtilen ilgili genel güvenlik ve performans gerekliliklerine uygunluğunun doğrulanması ile Ek I'in 1 ve 8 numaralı maddelerinde atıfta bulunulan istenmeyen yan etkilerin ve fayda/risk oranının kabul edilebilirliğinin değerlendirilmesi, gerektiği hallerde Ek III'te atıfta bulunulan ilgili veriler de dâhil olmak üzere yeterli klinik kanıt sağlayan klinik verilere dayanır. İmalatçı, genel güvenlik ve performans gerekliliklerine uygunluğu göstermek için gerekli klinik kanıt seviyesini belirler ve gerekçelendirir. Bu klinik kanıt seviyesi, cihazın karakteristikleri ve kullanım amacı bakımından uygun olur. Bu

amaçla imalatçılar, bu madde ve Ek XIV Kısım A uyarınca bir klinik değerlendirme planlar, yürütür ve dokümante eder.

(2) Tüm sınıf III cihazlar ve 54 üncü maddenin birinci fıkrasının (b) bendinde atıfta bulunulan sınıf IIb cihazlar için; imalatçı, klinik değerlendirmesinden ve/veya araştırmasından önce, amaçladığı Klinik Geliştirme Stratejisini ve klinik araştırmaya yönelik önerileri, incelemesi amacıyla bilimsel, teknik ve klinik görüş ve tavsiyelerde bulunmak üzere Komisyonca teşkil edilen uzman heyetine danışabilir. İmalatçı, uzman heyeti tarafından verilen görüşleri dikkate alır. Bu değerlendirmeler, on birinci fıkrada atıfta bulunulan klinik değerlendirme raporunda dokümante edilir. İmalatçı, gelecekteki bir uygunluk değerlendirme prosedürüyle ilgili olarak uzman heyeti tarafından verilen görüşlerle ilgili herhangi bir hak iddia edemez.

(3) Klinik değerlendirme; aşağıdakileri esas alacak şekilde tanımlanmış ve metodolojik açıdan geçerli bir prosedürü izler:

a) Ek XIV'ün 3 numaralı maddesi uyarınca, kullanım amacı açısından klinik değerlendirmeye konu olan cihazın, verilerin ait olduğu cihaza eşdeğer olduğunun gösterilmesini ve verilerin ilgili genel güvenilirlik ve performans gerekliliklerine uygunluğu göstermesi kaydıyla cihazın güvenliliği, performansı, tasarım karakteristikleri ve kullanım amacıyla ilgili hâlihazırda mevcut ilgili bilimsel literatürün kritik değerlendirmesini.

b) Araştırmaların, 62 ila 79 uncu maddeler, Komisyonca kabul edilen tasarruflar ve Ek XV kapsamında gerçekleştirilip gerçekleştirilmediğini gereken ölçüde dikkate alarak mevcut tüm klinik araştırmaların sonuçlarının kritik bir değerlendirmesini.

c) Varsa hâlihazırda mevcut olan alternatif tedavi seçeneklerinin göz önünde bulundurulmasını.

(4) Bu Yönetmelik uyarınca;

a) İmplant edilebilir cihazlar ve sınıf III cihazlar için aşağıdaki tüm koşullar sağlanmadıkça klinik araştırma yapılması gereklidir:

1) Cihaz, aynı imalatçı tarafından hâlihazırda piyasaya arz edilmiş bir cihazın modifikasyonları yoluyla tasarlanmışsa.

2) Modifiye edilmiş cihazın piyasaya arz edilmiş cihaza eşdeğer olduğu Ek XIV'ün 3 numaralı maddesi uyarınca imalatçı tarafından gösterilmiş ve bu gösterim onaylanmış kuruluş tarafından uygun bulunmuşsa.

3) Piyasaya arz edilmiş cihazın klinik değerlendirmesi, modifiye edilmiş cihazın ilgili güvenilirlik ve performans gerekliliklerine uygunluğunu göstermek için yeterliyse.

b) Bu fıkra uyarınca klinik araştırma yapılmasının gerekmediği durumda onaylanmış kuruluş; piyasaya arz sonrası klinik takip planının uygun olduğunu ve cihazın güvenilirliğini ve performansını göstermeye yönelik piyasaya arz sonrası çalışmaları içerdiğini teyit eder.

c) Altıncı fıkrada atıfta bulunulan durumlarda da klinik araştırmaların yapılması zorunlu değildir.

(5) Cihazının, hâlihazırda piyasaya arz edilmiş ve kendisi tarafından imal edilmeyen bir cihaza eşdeğer olduğunu gösteren bir imalatçı da dördüncü fıkrada gerekenlere ilave olarak;

a) İki imalatçı arasında, ikinci cihazın imalatçısının devamlılık arz eden bir biçimde teknik dokümantasyona tam erişimine açıkça imkân tanıyan geçerli bir sözleşmenin olması,

b) Orijinal klinik değerlendirmenin, bu Yönetmeliğin gerekliliklerine uygun olarak gerçekleştirilmiş olması,

şartıyla, klinik araştırma yapmamak için dördüncü fıkrayı dayanak olarak kullanabilir. Bu durumda imalatçı onaylanmış kuruluşa bunlarla ilgili açık kanıt sunar.

(6) Dördüncü fıkra uyarınca klinik araştırma yapma gerekliliği, aşağıda belirtilen implante edilebilir cihazlara ve sınıf III cihazlara uygulanmaz:

a) 110 uncu madde ile yürürlükten kaldırılan Tıbbi Cihaz Yönetmeliği ve Vücuda Yerleştirilebilir Aktif Tıbbi Cihazlar Yönetmeliği uyarınca mevzuata uygun şekilde piyasaya arz edilmiş ya da hizmete sunulmuş olan ve klinik değerlendirmesi;

1) Yeterli klinik veriye dayanan,

2) Mevcutsa bu tür cihazın klinik değerlendirmesine yönelik ilgili ürüne özgü ortak spesifikasyonlara uygun olan,

implante edilebilir cihazlara ve sınıf III cihazlara.

b) Klinik değerlendirmesi yeterli klinik veriye dayanan ve mevcutsa ilgili ürüne özgü ortak spesifikasyonlara uygun olan süturlara, zımba tellerine, dental dolgulara, dental braketlere, diş kronlarına, vidalara, kamalara, plaklara, tellere, pinlere, kliplere ve konnektörlere.

(7) Altıncı fıkraya istinaden dördüncü fıkranın uygulanmadığı durumlar, imalatçı tarafından klinik değerlendirme raporunda, onaylanmış kuruluş tarafından ise klinik değerlendirmenin değerlendirilmesi raporunda gerekçelendirilir.

(8) Ek XVI'da listelenen ve tıbbi bir kullanım amacı olmayan ürünler söz konusu olduğunda, bu Kısım ile Ek XIV ve Ek XV uyarınca bir klinik fayda gösterme gerekliliği, cihazın performansını göstermek için bir gereklilik olarak kabul edilir. Bu ürünlerin klinik değerlendirmeleri; piyasaya arz sonrası gözetimden, piyasaya arz sonrası klinik takipten ve gerektiği hallerde spesifik klinik araştırmadan elde edilen veriler dâhil olmak üzere güvenilirliğe ilişkin ilgili verilere dayanır. Benzer bir tıbbi cihazdan elde edilen mevcut klinik verilerin esas alındığı durumlar usulünce gerekçelendirilmez ise bu ürünler için klinik araştırma yapılması gerekir.

(9) Dördüncü fıkraya hâle gelmeksizin; genel güvenilirlik ve performans gerekliliklerine uygunluğun klinik verilere dayanan gösteriminin uygun bulunmadığı durumda, bu gibi istisnai duruma yönelik yeterli gerekçe;

a) İmalatçının risk yönetimi sonuçlarına,

b) Cihaz ile insan vücudu arasındaki etkileşimin ayrıntılarının, amaçlanan klinik performansın ve imalatçının iddialarının değerlendirilmesine,

dayalı olarak verilir. Bu gibi durumda imalatçı, genel güvenilirlik ve performans gerekliliklerine uygunluğun, bench testi, performans değerlendirmeleri ve klinik öncesi değerlendirme dâhil olmak üzere yalnızca klinik olmayan test yöntemlerinin sonuçlarına dayanarak gösterilmesinin yeterli olacağını düşünmesinin nedenini, Ek II'de atıfta bulunulan teknik dokümantasyonda usulüne uygun olarak ispat eder.

(10) Klinik değerlendirme ve dokümantasyonu, Ek XIV Kısım B uyarınca imalatçının piyasaya arz sonrası klinik takip planının ve 82 nci maddede atıfta bulunulan piyasaya arz sonrası gözetim planının uygulanmasından elde edilen klinik verilerle, ilgili cihazın yaşam döngüsü boyunca güncellenir. Sınıf III cihazlar ve implante edilebilir cihazlar için piyasaya arz sonrası klinik takip değerlendirme raporu ve uygulanabildiği hallerde 32 nci maddede atıfta bulunulan güvenilirlik ve klinik performans özeti, bu verilerle asgari yılda 1 kez güncellenir.

(11) Klinik değerlendirme, değerlendirme sonuçları ve değerlendirmeden elde edilen klinik kanıtlar, Ek XIV'ün 4 numaralı maddesinde atıfta bulunulduğu üzere bir klinik değerlendirme raporunda dokümente edilir. Bu rapor, ısmarlama imal edilen cihazlar hariç olmak üzere, ilgili cihaza ilişkin Ek II'de atıfta bulunulan teknik dokümantasyonun bir bölümünü oluşturur.

Cihazların uygunluğunu göstermek için yürütülen klinik araştırmalarla ilgili genel gereklilikler

MADDE 62 - (1) Klinik araştırmaların uygunluk değerlendirme amaçlarına yönelik klinik değerlendirmenin bir parçası olarak yürütülmesi durumunda klinik araştırmalar, bu madde ve 63 ila

79 uncu madde hükümleri, Komisyonca kabul edilen tasarruflar ve Ek XV uyarınca, aşağıdaki amaçlardan biri veya daha fazlası için tasarlanır, yetkilendirilir, yürütülür, kaydedilir ve raporlanır:

a) Normal kullanım koşulları altında, bir cihazın 3 üncü maddenin birinci fıkrasının (eee) bendinde listelenen spesifik amaçların biri veya daha fazlası için uygun olacak şekilde tasarlandığını, imal edildiğini, ambalajlandığını ve imalatçısı tarafından belirtildiği şekilde amaçlanan performansa ulaştığını saptamak ve doğrulamak.

b) İmalatçısı tarafından belirtildiği şekilde bir cihazın klinik faydalarını saptamak ve doğrulamak.

c) Cihazın klinik güvenliliğini saptamak ve doğrulamak, cihazın normal kullanım şartları altında istenmeyen yan etkilerini belirlemek ve bunların cihazın sağlayacağı faydalar ile karşılaştırıldığında kabul edilebilir riskler oluşturup oluşturmadığını değerlendirmek.

(2) Bir klinik araştırmanın sponsorunun yurt içinde yerleşik olmaması durumunda sponsor, yurt içinde yerleşik gerçek veya tüzel bir kişinin, kendisinin yasal temsilcisi olmasını sağlar. Bu yasal temsilci, bu Yönetmelik uyarınca sponsorun yükümlülüklerine uygunluğun sağlanmasından sorumlu olur ve bu Yönetmelikte sponsorla yapılması öngörülen bütün iletişimlerin muhatabı olur. Bu yasal temsilci ile yapılan her türlü iletişim, sponsorla yapılan iletişim olarak kabul edilir.

(3) Klinik araştırmalar;

a) İnsan Gönüllüleri Üzerinde Yapılan Tıbbi Araştırmalarda Etik İlkeler Üzerine Dünya Tıp Birliği Helsinki Bildirgesinin ve ilgili alandaki uluslararası standartların en güncel sürümü ile aynı doğrultuda olur.

b) Bir klinik araştırmaya iştirak eden gönüllülerin haklarının, güvenliğinin, onurunun ve refahının korunacağı ve diğer tüm çıkarlardan üstün geleceği, elde edilen klinik verilerin bilimsel olarak geçerli, güvenilir ve sağlam olacağı bir şekilde tasarlanır ve yürütülür.

c) Bilimsel ve etik incelemeye tabi olur. Etik inceleme, Kurum onayı ile kurularak Kurum web sayfasında yayımlanan listede yer alan bir etik kurul tarafından gerçekleştirilir. Kurum, klinik araştırma izin başvurusu incelemesine yönelik etik kurul prosedürlerinin, bu Yönetmeliğe uygun olmasını sağlar. Etik incelemede, meslekten olmayan en az bir kişi görev alır.

(4) Birinci fıkrada atıfta bulunulduğu şekliyle bir klinik araştırma, yalnızca aşağıdaki koşulların tamamı karşılandığında yürütülebilir:

a) Kurum tarafından bu Yönetmelik uyarınca klinik araştırmaya izin verilmiş olması.

- b) İlgili mevzuat uyarınca oluşturulan bir etik kurulun, klinik arařtırmaya iliřkin olarak ilgili mevzuat kapsamında olumsuz bir grř vermemesi.
- c) İkinci fıkra uyarınca sponsorun veya yasal temsilcisinin yurt iinde yerleřik olması.
- ) 64 ila 68 inci maddeler uyarınca etkilenebilir poplasyonların ve gnlllerin uygun bir řekilde korunması.
- d) Gnlller veya kamu saęlıęı iin beklenen faydaların, ngrlebilir riskleri ve dezavantajları makul kılması ve bu kořula uygunluęun srekli olarak izlenmesi.
- e) Gnllnin veya bilgilendirilmiř gnll olurunun gnllnin veremedięi durumda yasal vasisinin, 63 nc madde uyarınca bilgilendirilmiř gnll olurunun vermesi.
- f) Gnllye veya bilgilendirilmiř gnll olurunun gnllnin veremedięi durumda yasal vasisine, ihtiya halinde ilave bilgiler verebilecek bir kiřinin iletiřim bilgilerinin saęlanması.
- g) Gnlllerin fiziksel ve zihinsel btnlk, gizlilik ve 24/3/2016 tarihli ve 6698 sayılı Kiřisel Verilerin Korunması Kanunu uyarınca gnllyle ilgili verilerin korunmasına dair haklarının gvenceye alınması.
- ę) Klinik arařtırmanın, gnlller iin acı, rahatsızlık, korku ve dięer ngrlebilir riskleri mmkn olduęu kadar az ierecek řekilde tasarlanmıř olması ve hem risk eřięinin hem de distres seviyesinin klinik arařtırma planında zellikle tanımlanması ve srekli olarak izlenmesi.
- h) Gnlllere sunulan tıbbi bakımın, klinik arařtırma kořulları altında ilgili hasta bakımını saęlamak iin Tababet ve řuabatı San'atlarının Tarzı İcrasına Dair Kanun uyarınca yetkilendirilmiř; uygun nitelikli bir tıp doktorunun veya uygun olduęu hallerde nitelikli bir diř hekiminin ya da dięer bir kiřinin sorumluluęunda olması.
- ı) Klinik arařtırmaya iřtirak etmesi iin, gnll veya gerektięi hallerde gnllnin yasal vasisi zerinde, mali nitelikte olanlar da dhil olmak zere nfuzun ktye kullanılmaması.
- i) Sz konusu arařtırma amalı cihazın/cihazların, klinik arařtırmanın kapsadıęı hususlardan ayrı olarak Ek I'de belirtilen uygulanabilir genel gvenlilik ve performans gerekliliklerine uyması ve gnlllerin saęlıęını ve gvenlięini korumak iin bu hususlarla ilgili (en son teknolojik geliřmeleri gz nnde bulundurarak, iř gvenlięi ve kaza nleme alanındaki hkmlerle birlikte uygulanabildięi hallerde teknik ve biyolojik gvenlik testini ve klinik ncesi deęerlendirmeyi ieren) btn tedbirlerin alınmıř olması.
- j) Ek XV'in gerekliliklerinin yerine getirilmesi.

(5) Gönüllü veya gönüllünün bilgilendirilmiş gönüllü oluru veremediği durumlarda yasal vasisi, herhangi bir zarar ortaya çıkmadan ve herhangi bir gerekçe sunmadan, bilgilendirilmiş gönüllü oluru iptal ederek herhangi bir zamanda klinik araştırmadan geri çekilebilir. Kişisel Verilerin Korunması Kanunu ve kişisel verilerin korunması ile ilgili diğer mevzuatlara hâlihazırda hâli gelmeksizin, bilgilendirilmiş gönüllü olurunun geri çekilmesi, hâlihazırda yürütülen faaliyetleri ve geri çekilmesinden önce bilgilendirilmiş gönüllü oluru dayalı olarak elde edilen verilerin kullanımını etkilemez.

(6) Araştırmacı; hasta bakımında gerekli bilimsel bilgi ve deneyime sahip olması sebebiyle araştırmacı rolü için nitelikli olduğu Kurum tarafından kabul edilen bir mesleği icra eden kişidir. Bir klinik araştırmanın yürütülmesine dâhil olan diğer personel, görevlerini gerçekleştirmek için ilgili tıbbi alanda ve klinik araştırma metodolojisinde öğrenim, eğitim veya tecrübe yoluyla uygun bir şekilde kalifiye olur.

(7) Klinik araştırma, ilgili mevzuata hâli gelmeksizin cihazın kullanılmasının amaçlandığı tesislere benzer ve klinik araştırma için uygun olan tesislerde yürütülür.

(8) Klinik araştırma başvurusunun Türkiye’de yerleşik bir sponsor ya da ikinci fıkra uyarınca atanan yasal temsilci tarafından hem Türkiye’ye hem de AB üyesi ülkelere sunulması halinde, 70 inci maddede Kuruma yapılan atıflar aynı zamanda ilgili AB üyesi ülkenin/ülkelerin yetkili otoritesine yapılmış sayılır ve bu Yönetmeliğin ilgili hükümleri uygulanır.

Bilgilendirilmiş gönüllü oluru

MADDE 63 - (1) Bilgilendirilmiş gönüllü oluru; ikinci fıkra uyarınca usulüne uygun şekilde bilgilendirilmesinden sonra, gönüllü veya gönüllünün bilgilendirilmiş gönüllü oluru veremediği durumlarda yasal vasisi ile ikinci fıkranın (c) bendinde atıfta bulunulan görüşmeyi gerçekleştiren kişi tarafından yazılır, tarih atılır ve imzalanır. Gönüllünün yazamadığı hallerde gönüllü oluru, en azından bir tarafsız tanığın mevcudiyetinde uygun alternatif yollar vasıtasıyla verilebilir ve kaydedilebilir. Bu durumda tanık, bilgilendirilmiş gönüllü oluru dokümanını tarih atarak imzalar. Gönüllüye veya gönüllünün bilgilendirilmiş gönüllü oluru veremediği durumlarda yasal vasisine, uygun olduğunda bilgilendirilmiş gönüllü olurunun verilmiş olduğu dokümanın veya kaydın bir sureti sağlanır. Bilgilendirilmiş gönüllü oluru dokümanına edilir. Gönüllüye veya onun yasal vasisine, klinik araştırmaya iştirak etmeye yönelik kararını düşünmesi için yeterli zaman verilir.

(2) Bilgilendirilmiş gönüllü oluru almak amacıyla, gönüllüye veya gönüllünün bilgilendirilmiş gönüllü oluru veremediği durumlarda onun yasal vasisine verilen bilgiler;

a) Gönüllünün veya yasal vasisinin;

1) Klinik araştırmanın niteliğini, amaçlarını, faydalarını, olası sonuçlarını, risklerini ve dezavantajlarını,

2) Gönüllünün korunmasıyla ilgili hakları ve güvenceleri, özellikle gönüllünün araştırmaya iştirak etmeyi reddetme hakkını ve herhangi bir zarar ortaya çıkmadan ve herhangi bir gerekçe sunmadan herhangi bir zamanda klinik araştırmadan geri çekilme hakkını,

3) Klinik araştırmada gönüllüden beklenen iştirak süresi dâhil olmak üzere klinik araştırmaların hangi koşullar altında yürütüleceğini,

4) Gönüllünün klinik araştırmaya iştirakının sonlanması halinde, takip tedbirleri dâhil olmak üzere olası tedavi alternatiflerini,

anlamasını sağlar.

b) Gönüllü veya yasal vasisi için kapsamlı, özlü, açık, konuyla ilgili ve anlaşılabilir şekilde olur.

c) Araştırma ekibinin ilgili mevzuat kapsamında uygun nitelikte olan bir üyesi ile yapılan bir ön görüşmede sağlanır.

ç) 69 uncu maddede atıfta bulunulan uygulanabilir zarar tazminatı sistemi hakkındaki bilgileri içerir.

d) 70 inci maddenin birinci fıkrasında atıfta bulunulduğu şekliyle, klinik araştırmanın Türkiye ve AB genelindeki benzersiz tek bir kimlik numarasını ve bu maddenin altıncı fıkrası uyarınca klinik araştırma sonuçlarına erişilebilirlik hakkındaki bilgileri içerir.

(3) İkinci fıkrada atıfta bulunulan bilgiler, yazılı olarak hazırlanır ve gönüllü veya gönüllünün bilgilendirilmiş gönüllü olurlarını veremediği durumlarda yasal vasisi için elde edilebilir olur.

(4) İkinci fıkranın (c) bendinde atıfta bulunulan görüşmede, bilgileri vermek için kullanılan yöntemlerle birlikte spesifik hasta popülasyonlarının ve bireysel gönüllülerin bilgi ihtiyaçlarına özellikle dikkat edilir.

(5) İkinci fıkranın (c) bendinde atıfta bulunulan görüşmede, gönüllünün verilen bilgileri anladığı doğrulanır.

(6) Gönüllü, klinik araştırma raporunun ve hedeflenen kullanıcı için anlaşılabilir şekilde sunulan bir özetin, klinik araştırmanın sonuçlarına bakılmaksızın 73 üncü maddede atıfta bulunulan klinik araştırmalara yönelik elektronik sistemde 77 nci maddenin beşinci fıkrası uyarınca erişilebilir olacağı

hakkında bilgilendirilir. İlgili rapor ve özet kullanılabilir hale geldiğinde, mümkün olduğu ölçüde gönüllüye bildirilir.

(7) Bu Yönetmelik, yasal vasisi tarafından verilen bilgilendirilmiş gönüllü olmasına ilave olarak görüş oluşturma ve kendisine verilen bilgileri değerlendirme kabiliyeti olan bir çocuğun, bir klinik araştırmaya iştirak etmesi için ayrıca onay vermesini gerektiren ilgili mevzuata hâlel getirmez.

Kısıtlılara yönelik klinik araştırmalar

MADDE 64 - (1) Kısıtlılıklarından önce bilgilendirilmiş gönüllü olmasını vermemiş veya vermeyi reddetmemiş olan kısıtlılar söz konusu olduğunda, 62 nci maddenin dördüncü fıkrasında belirtilen koşullara ilave olarak, yalnızca aşağıdaki koşulların tamamının karşılanması durumunda bir klinik araştırma yürütülebilir:

- a) Yasal vasilerinden bilgilendirilmiş gönüllü olmasının alınmış olması.
- b) Kısıtlıların 63 üncü maddenin ikinci fıkrasında atıfta bulunulan bilgileri, anlama kapasiteleri bakımından yeterli olacak şekilde almış olmaları.
- c) Klinik araştırmaya iştirak etmeyi reddetmek ya da herhangi bir zamanda klinik araştırmadan geri çekilmek için görüş oluşturma ve 63 üncü maddenin ikinci fıkrasında atıfta bulunulan bilgileri değerlendirme kabiliyeti olan bir kısıtlının sarîh isteğine araştırmacı tarafından uygun davranılması.
- ç) Klinik araştırmaya iştirakle doğrudan ilişkili giderlere ve kazanç kayıplarına yönelik tazminat haricinde, hiçbir özendirici teşvikin ya da maddî mükâfatın gönüllülere veya yasal vasilerine verilmemesi.
- d) Kısıtlılar bakımından klinik araştırmanın zorunlu olması ve bilgilendirilmiş gönüllü oluru verebilecek kişilere yönelik klinik araştırmalardan veya diğer araştırma yöntemlerinden karşılaştırılabilir geçerliliğe ilişkin verilerin elde edilememesi.
- e) Klinik araştırmanın, gönüllünün muzdarip olduğu bir tıbbî durumla doğrudan ilişkili olması.
- f) Klinik araştırmaya iştirak etmenin kısıtlı için içerdiği risklerden ve yüklerden daha ağır basan doğrudan bir fayda oluşturacağı beklentisine yönelik bilimsel dayanakların bulunması.

(2) Gönüllü, bilgilendirilmiş gönüllü oluru prosedürüne mümkün olduğunca iştirak eder.

Çocuklara yönelik klinik araştırmalar

MADDE 65 - (1) Çocuklara yönelik bir klinik araştırma, 62 nci maddenin dördüncü fıkrasında belirtilen koşullara ilave olarak, yalnızca aşağıdaki koşulların tamamının karşılanması durumunda yürütülebilir:

- a) Yasal vasilerinden bilgilendirilmiş gönüllü olurunun alınmış olması.
- b) Çocukların, 63 üncü maddenin ikinci fıkrasında atıfta bulunulan bilgileri, yaşlarına ve zihinsel olgunluklarına uygun olacak şekilde ve çocuklarla çalışma konusunda eğitilmiş veya deneyimli olan araştırmacılardan ya da araştırma ekibi üyelerinden almış olmaları.
- c) Klinik araştırmaya iştirak etmeyi reddetmek ya da herhangi bir zamanda klinik araştırmadan geri çekilmek için görüş oluşturma ve 63 üncü maddenin ikinci fıkrasında atıfta bulunulan bilgileri değerlendirme kabiliyeti olan bir çocuğun sarih isteğine araştırmacı tarafından uygun davranılması.
- ç) Klinik araştırmaya iştirakle doğrudan ilişkili giderlere ve kazanç kayıplarına yönelik tazminat haricinde, hiçbir özendirici teşvikin ya da maddi mükâfatın gönüllülere veya yasal vasilerine verilmemesi.
- d) Klinik araştırmanın, yalnızca çocuklarda meydana gelen bir tıbbi duruma yönelik tedavileri araştırmak için amaçlanması ya da bilgilendirilmiş gönüllü oluru verebilecek kişilere yönelik klinik araştırmalarda elde edilen verileri veya diğer araştırma yöntemleriyle elde edilen verileri geçerli kılmak için klinik araştırmanın çocuklar üzerinde yapılmasının şart olması.
- e) Klinik araştırmanın, ilgili çocuğun muzdarip olduğu bir tıbbi durumla doğrudan ilişkili olması ya da yalnızca çocuklar üzerinde yürütülebilecek bir yapıda olması.
- f) Klinik araştırmaya iştirakin çocuk için içerdiği risklerden ve yüklerden daha ağır basan doğrudan bir fayda oluşturacağı beklentisine yönelik bilimsel dayanakların bulunması.
- g) Çocuğun, yaşına ve zihinsel olgunluğuna uygun bir şekilde, bilgilendirilmiş gönüllü oluru prosedürüne iştirak etmesi.
- ğ) Çocuğun bir klinik araştırma sırasında ilgili mevzuatta tanımlandığı şekilde bilgilendirilmiş gönüllü oluru vermek için hukuki ehliyet yaşına ulaşması durumunda, klinik araştırmaya iştirak etmeye devam etmesinden önce kendisinden açık bilgilendirilmiş gönüllü olurunun alınması.

Gebe veya emziren kadınlara yönelik klinik araştırmalar

MADDE 66 - (1) Gebe veya emziren kadınlara yönelik bir klinik araştırma, 62 nci maddenin dördüncü fıkrasında belirtilen koşullara ilave olarak, yalnızca aşağıdaki koşulların tamamının karşılanması durumunda yürütülebilir:

- a) Klinik araştırmanın, ilgili gebe veya emziren kadın ya da embriyosu, fetüsü veya doğumdan sonra çocuğu için içerdiği risklerden ve yüklerden daha ağır basan doğrudan bir fayda oluşturma potansiyelinin olması.
- b) Araştırmanın emziren kadınlar üzerinde yürütülmesi durumunda, çocuğun sağlığı üzerinde herhangi bir advers etkiden kaçınmaya özellikle dikkat edilmesi.
- c) Klinik araştırmaya iştirakle doğrudan ilişkili giderlere ve kazanç kayıplarına yönelik tazminat haricinde, gönüllülere özendirici bir teşvikin ya da maddi mükâfatın verilmemesi.

İlave tedbirler

MADDE 67 - (1) Zorunlu askerlik hizmeti gerçekleştiren kişiler, özgürlüğünden mahrum olan kişiler, bir adli karar nedeniyle klinik araştırmalarda yer alamayan kişiler veya bakım evlerindeki kişiler ile ilgili ilave tedbirler alınabilir veya sürdürülebilir.

Acil durumlarda klinik araştırmalar

MADDE 68 - (1) 62 nci maddenin dördüncü fıkrasının (e) bendine, 64 üncü maddenin birinci fıkrasının (a) ve (b) bentlerine ve 65 inci maddenin birinci fıkrasının (a) ve (b) bentlerine istisna olarak, gönüllüyü klinik araştırmaya dâhil etme kararının, bu klinik araştırmaya yönelik klinik araştırma planına uygun olarak gönüllüye ilk müdahale anında alınması söz konusu olduğunda aşağıdaki koşulların tamamının karşılanması şartıyla, bir klinik araştırmaya iştirak etmek için bilgilendirilmiş gönüllü oluru bu karardan sonra alınabilir ve klinik araştırmaya ilişkin bilgiler bu karardan sonra verilebilir:

- a) Gönüllünün, hayatı tehdit eden ani tıbbi koşullardan veya diğer ciddi koşullardan kaynaklı sağlık durumundaki aciliyet nedeniyle, bilgilendirilmiş gönüllü oluru önceden sağlayamaması ve klinik araştırmaya ilişkin önceden bilgi alamaması.
- b) Gönüllünün klinik araştırmaya iştirakinin; gönüllünün ızdırabını azaltacak ve/veya sağlığını geliştirecek, sağlıkla ilgili ölçülebilir bir iyileştirmeye ya da sağlık durumunun teşhisiyle sonuçlanacak şekilde, gönüllü için doğrudan klinik olarak ilgili bir fayda oluşturma potansiyeline sahip olacağı beklentisine yönelik bilimsel dayanakların bulunması.
- c) Gönüllünün yasal vasisine tüm bilgileri önceden sağlamanın ve ondan bilgilendirilmiş gönüllü oluru önceden almanın terapötik pencere içinde mümkün olmaması.
- ç) Araştırmacının, klinik araştırmaya iştirake yönelik gönüllü tarafından önceden ifade edilen herhangi bir itirazdan haberdar olmadığını garanti etmesi.

d) Klinik araştırmanın; gönüllünün kendisinden veya yasal vasisinden bilgilendirilmiş gönüllü oluru önceden almanın ve ona önceden bilgi vermenin, terapötik pencere içinde mümkün olmayan tıbbi durumuyla doğrudan ilişkili olması ve klinik araştırmanın sadece acil durumlarda yürütülebilecek bir yapıda olması.

e) Klinik araştırmanın gönüllünün standart tedavisine kıyasla gönüllü için asgari düzeyde risk oluşturması ve gönüllüye asgari düzeyde yük getirmesi.

(2) Birinci fıkra uyarınca bir müdahaleyi takiben, gönüllünün klinik araştırmaya iştirakinin devam etmesi için 63 üncü madde uyarınca bilgilendirilmiş gönüllü oluru aranır ve klinik araştırmaya yönelik bilgiler aşağıdaki gerekliliklere uygun olarak verilir:

a) Kısıtlılarla ve çocuklarla ilgili olarak bilgilendirilmiş gönüllü oluru, araştırmacı tarafından yasal vasisinden gecikmeksizin istenir ve 63 üncü maddenin ikinci fıkrasında atıfta bulunulan bilgiler mümkün olan en kısa sürede gönüllüye ve yasal vasisine verilir.

b) Diğer gönüllülerle ilgili olarak bilgilendirilmiş gönüllü oluru, araştırmacı tarafından hangisinden daha çabuk alınabilir ise gönüllüden veya yasal vasisinden gecikmeksizin istenir ve 63 üncü maddenin ikinci fıkrasında atıfta bulunulan bilgiler, uygulanabilir olduğu üzere gönüllüye veya yasal vasisine mümkün olan en kısa sürede verilir. Bu bendin amaçları doğrultusunda bilgilendirilmiş gönüllü olurunun yasal vasiden alınmış olması durumunda bilgilendirilmiş gönüllü oluru, klinik araştırmaya iştirakin devam etmesi için bilgilendirilmiş gönüllü oluru verme yetisine sahip olduğu an gönüllüden alınır.

(3) Gönüllü veya gerektiği hallerde yasal vasisi gönüllü oluru vermezse, söz konusu kişi klinik araştırmadan elde edilen verilerin kullanımına itiraz etme hakkı konusunda bilgilendirilir.

Zarar tazminatı

MADDE 69 - (1) Yurt içinde yürütülen bir klinik araştırmaya iştirakten dolayı bir gönüllünün maruz kaldığı zararlara yönelik tazminat sistemlerinin, sigorta biçiminde, güvence biçiminde veya amacı bakımından denk olan ve riskin yapısına ve boyutuna uygun benzer bir anlaşma biçiminde yürürlükte olması sağlanır.

(2) Sponsor ve araştırmacı, birinci fıkrada atıfta bulunulan sistemi uygun biçimde kullanır.

Klinik araştırma başvurusu

MADDE 70 - (1) Bir klinik araştırmanın sponsoru, Kuruma Ek XV'in II. Bölümünde atıfta bulunulan dokümantasyonla birlikte bir başvuru yapar. Başvuru, klinik araştırma ile ilgili her türlü iletişimde

kullanılmak üzere Türkiye ve AB genelinde benzersiz tek bir kimlik numarası oluşturan ve 73 üncü maddede atıfta bulunulan elektronik sistem aracılığıyla yapılır. Kurum, başvuruyu aldıktan sonra 10 gün içerisinde, klinik araştırmanın bu Yönetmeliğin kapsamına girip girmediğini ve başvuru dosyasının Ek XV'in II. Bölümü uyarınca tam olup olmadığını sponsora bildirir.

(2) Sponsor, Ek XV'in II. Bölümünde atıfta bulunulan dokümantasyona ilişkin meydana gelen herhangi bir değişiklikten itibaren 1 hafta içerisinde, 73 üncü maddede atıfta bulunulan elektronik sistemdeki ilgili verileri günceller ve dokümantasyondaki bu değişikliğin açıkça fark edilebilir olmasını sağlar. Kurum, bu elektronik sistem vasıtasıyla güncelleme hakkında bilgilendirilir.

(3) Bu Yönetmelik uyarınca;

a) Kurum, başvuru yapılan klinik araştırmanın bu Yönetmelik kapsamına girmediğini veya başvuru dosyasının tam olmadığını tespit ettiğinde, bunu sponsora bildirir ve sponsorun 73 üncü maddede atıfta bulunulan elektronik sistem vasıtasıyla açıklama yapması ya da başvuruyu tamamlaması için en fazla 10 günlük süre verir. Kurum, uygun olduğu hallerde, bu süreyi en fazla 20 günlük ek süreyle uzatabilir.

b) Sponsorun (a) bendinde atıfta bulunulan süre sınırı içerisinde açıklama yapmaması veya başvuruyu tamamlamaması durumunda, başvuru geçersiz sayılır. Sponsor, başvurunun bu Yönetmelik kapsamına girdiğini ve/veya tamamlandığını düşünse dahi Kurum bu görüşte değilse başvuru reddedilmiş sayılır. Sponsor, Kurumca oluşturulan itiraz prosedürü kapsamında bu karara itirazda bulunabilir.

c) Kurum, açıklamaların veya talep edilen ilave bilgilerin alınmasından itibaren 5 gün içerisinde, klinik araştırmanın bu Yönetmelik kapsamına girip girmediğini ve başvurunun tamamlanıp tamamlanmadığını sponsora bildirir.

(4) Kurum ayrıca, birinci ve üçüncü fıkralarda atıfta bulunulan sürelerin her birini beşer gün daha uzatabilir.

(5) Bu Kısımın amaçları doğrultusunda, sponsorun birinci veya üçüncü fıkralar uyarınca bilgilendirildiği tarih, başvurunun geçerlilik tarihi olur. Sponsorun bilgilendirilmediği durumda, geçerlilik tarihi sırasıyla birinci, üçüncü ve dördüncü fıkralarda atıfta bulunulan sürelerin son günü olur.

(6) Kurum, başvurunun değerlendirildiği süre boyunca, sponsordan ilave bilgiler talep edebilir. Yedinci fıkranın (b) bendinde belirtilen sürenin bitişi, ilk talep tarihinden itibaren ilave bilgilerin alınmış olduğu zamana kadar dondurulur.

(7) Sponsor;

a) Araştırma amaçlı sınıf I cihazlar ya da invaziv olmayan sınıf IIa ve sınıf IIb cihazlar söz konusu olduğunda beşinci fıkra uyarınca başvurunun geçerlilik tarihinden sonra ivedilikle ve etik kurulun klinik araştırmaya ilişkin olarak ilgili mevzuat kapsamında olumsuz bir görüş vermemesi şartıyla,

b) (a) bendinde atıfta bulunulanlar haricindeki araştırma amaçlı cihazlar söz konusu olduğunda, Kurum klinik araştırma iznini sponsora bildirir bildirmez ve etik kurulun klinik araştırmaya ilişkin olarak ilgili mevzuat kapsamında olumsuz bir görüş vermemesi şartıyla,

araştırmaya başlayabilir. Kurum beşinci fıkarda atıfta bulunulan geçerlilik tarihinden itibaren 45 gün içerisinde izni sponsora bildirir. Kurum, uzmanlara danışmak amacıyla, bu süreyi 20 gün daha uzatabilir.

Klinik araştırma başvurusunun değerlendirilmesi

MADDE 71 - (1) Kurum; başvuruyu geçerli kılan ve değerlendiren veya başvuru hakkında karar veren kişilerin çıkar çatışmasının olmamasını, bu kişilerin sponsordan, ilgili araştırmacılardan, klinik araştırmayı finanse eden gerçek veya tüzel kişilerden ve ilaveten diğer usulsüz etkilerden bağımsız olmalarını sağlar.

(2) Kurum; değerlendirmenin, gerekli niteliğe ve deneyime kolektif olarak sahip olan uygun sayıda kişi tarafından birlikte yapılmasını sağlar.

(3) Kurum; klinik araştırmanın, risk minimizasyonu sonrasında gönüllüler veya üçüncü kişiler için kalan potansiyel risklerin, beklenen klinik faydalarla karşılaştırıldığında, gerekçelendirilecek bir şekilde tasarlanıp tasarlanmadığını değerlendirir. Kurum, uygulanabilir ortak spesifikasyonları veya uyumlaştırılmış standartları göz önünde tutarken, özellikle;

a) Araştırma amaçlı cihazın/cihazların klinik araştırmanın kapsadığı hususlardan ayrı olarak uygulanabilir genel güvenilirlik ve performans gerekliliklerine uygunluğunun gösterilmesini ve bu hususlarla ilgili gönüllülerin sağlığını ve güvenliğini korumak için bütün tedbirlerin alınmış olup olmadığını inceler. Bu inceleme, gerektiğinde teknik ve biyolojik güvenlik testlerinin ve klinik öncesi değerlendirmenin kanıtlarını kapsar.

b) Sponsor tarafından kullanılan risk minimizasyon çözümlerinin uyumlaştırılmış standartlarda tanımlanıp tanımlanmadığını ve sponsorun uyumlaştırılmış standartları kullanmadığı durumlarda, risk minimizasyon çözümlerinin uyumlaştırılmış standartların sağladığına denk bir koruma seviyesi sağlayıp sağlamadığını inceler.

c) Araştırma amaçlı cihazın güvenli kurulumu, hizmete sunumu ve bakımı için planlanan tedbirlerin yeterli olup olmadığını inceler.

ç) İstatistiki yaklaşımlar, araştırmanın tasarımı ve örneklem büyüklüğü, karşılaştırma cihazı ve sonlanım noktaları da dâhil olmak üzere metodolojik hususlar dikkate alınarak klinik araştırmadan elde edilen verilerin güvenilirliğini ve tutarlılığını inceler.

d) Ek XV'in gerekliliklerinin karşılanıp karşılanmadığını inceler.

e) Steril kullanıma yönelik cihazlar söz konusu olduğunda, imalatçının sterilizasyon prosedürlerinin validasyon kanıtlarını veya araştırma tesisince yürütülmesi gereken yenileme ve sterilizasyon prosedürlerine ilişkin bilgileri inceler.

f) Hayvan veya insan kaynaklı bileşenlerin ya da Beşeri Tıbbi Ürünler Ruhsatlandırma Yönetmeliği uyarınca tıbbi ürünler olarak kabul edilebilen maddelerin güvenliliğinin, kalitesinin ve yararlılığının gösterilmesini inceler.

(4) Kurum; aşağıdaki durumlarda klinik araştırma için izin vermez ve Kurumca oluşturulan itiraz prosedürü kapsamında bu karara itirazda bulunulabilir:

a) 70 inci maddenin birinci fıkrası uyarınca sunulan başvuru dosyasının tamamlanmamış kalması.

b) Cihazın veya sunulan dokümanların, özellikle araştırma planının ve araştırmacı broşürünün güncel bilimsel bilgiyle uyumlu olmaması ve klinik araştırmanın özellikle, gönüllüler veya hastalar üzerinde cihazın güvenliliği, performans özellikleri veya faydalarına ilişkin kanıtlar sağlamak için uygun olmaması.

c) 62 nci maddenin gerekliliklerinin karşılanmaması.

ç) Üçüncü fıkra kapsamındaki herhangi bir değerlendirmenin olumsuz olması.

Klinik araştırmanın yürütülmesi

MADDE 72 - (1) Sponsor ve araştırmacı; klinik araştırmanın, onaylanan klinik araştırma planına uygun olarak yürütülmesini sağlar.

(2) Sponsor, gönüllülerin haklarının, güvenliğinin ve refahının korunduğunu, raporlanan verilerin güvenilir ve tutarlı olduğunu ve klinik araştırmanın yürütülmesinin bu Yönetmeliğin gerekliliklerine uygun olduğunu doğrulamak için, yürütülen klinik araştırmanın yeterli düzeyde izlenmesini sağlar. İzlemenin içeriği ve yapısı, aşağıdakiler de dâhil olmak üzere, klinik araştırmanın bütün özelliklerini göz önünde bulunduran bir değerlendirmeye dayanarak sponsor tarafından belirlenir:

a) Klinik araştırmanın amacı ve metodolojisi.

b) Müdahalenin normal klinik uygulamadan sapma derecesi.

(3) Klinik araştırmaya ilişkin tüm bilgiler; kişisel verilerin korunmasına ilişkin mevzuat uyarınca kayıtların gizliliğinin ve gönüllülerin kişisel verilerinin korunmasına hanel gelmeksizin uygulanabilir olduğunda söz konusu bilgilerin doğru olarak raporlanabileceği, yorumlanabileceği ve doğrulanabileceği bir şekilde sponsor veya araştırmacı tarafından kaydedilir, işlenir, kullanılır ve saklanır.

(4) İşlenen bilgileri ve kişisel verileri, özellikle işlemenin bir ağ üzerinden iletimi içerdiği durumlarda, yetkisiz olarak veya yasa dışı bir şekilde erişime, ifşaya, yaymaya ve değiştirmeye karşı veya imhaya ya da kazara kaybetmeye karşı korumak için uygun teknik ve idari tedbirler uygulanır. İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, bu durum dolayısıyla ilgisine ve Kişisel Verileri Koruma Kuruluna mümkün olan en kısa sürede bildirilir.

(5) Kurum, klinik araştırmaların bu Yönetmeliğin gereklilikleri ve onaylanan araştırma planı uyarınca yürütüldüğünü kontrol etmek için araştırma tesis/tesislerini uygun bir seviyede denetler.

(6) Sponsor, acil durumlarda, araştırmada kullanılan cihazların derhal tespit edilmesini ve gerektiğinde derhal geri çağırılmasını mümkün kılan bir prosedür oluşturur.

Klinik araştırmalara yönelik elektronik sistem

MADDE 73 - (1) Komisyon tarafından klinik araştırmalara ilişkin aşağıdaki amaçlara yönelik kurulan, yönetilen ve sürdürülen elektronik sistem,

a) 70 inci maddenin birinci fıkrasında atıfta bulunulan, klinik araştırmaya özgü tek kimlik numaralarını oluşturmaya yönelik,

b) 70 inci, 74 üncü, 75 inci ve 78 inci maddelerde atıfta bulunulan klinik araştırmalar için bütün başvuruların veya bildirimlerin sunulması ile diğer bütün verilerin sunulması için bir giriş noktası olarak kullanılmasına veya bu bağlamda verilerin işlenmesine yönelik,

c) 70 inci ve 76 ncı maddelerde atıfta bulunulan bilgi alışverişi dâhil olmak üzere, Türkiye ve AB üyesi ülkeler arasında ve bu ülkelerle Komisyon arasında klinik araştırmalarla ilgili bilgilerin alışverişine yönelik,

ç) 77 nci maddenin beşinci fıkrasının gerektirdiği şekilde klinik araştırma raporu ve bunun özeti dâhil olmak üzere, sponsor tarafından 77 nci madde uyarınca sağlanacak bilgilere yönelik,

d) 79 uncu maddede atıfta bulunulan ciddi advers olaylara, cihaz kusurlarına ve ilgili güncellemelere ilişkin raporlamaya yönelik,

hususları içerir.

(2) Birinci fıkranın (c) bendinde atıfta bulunulan bilgiler yalnızca Türkiye, AB üyesi ülkeler ve Komisyonun erişimine açık olur. Birinci fıkranın diğer bentlerinde atıfta bulunulan bilgiler, bu bilgilerin tamamı veya bir kısmı için bilgilerin gizliliği aşağıdaki dayanaklardan herhangi birisi ile gerekçelendirilmedikçe kamuya açık olur:

a) İlgili mevzuat uyarınca kişisel verilerin korunması.

b) Kamu yararı bakımından açıklanması gerekmedikçe, bilhassa cihazın uygunluk değerlendirme durumunu göz önünde bulundurma yoluyla araştırmacı broşüründekiler başta olmak üzere ticari gizli bilgilerin korunması.

c) İlgili AB üyesi ülke/ülkeler ve/veya Türkiye tarafından klinik araştırmanın yürütülmesinin etkin gözetimi.

(3) Gönüllülerin hiçbir kişisel verisi kamuya açık olmaz.

CE işareti taşıyan cihazlarla ilgili klinik araştırmalar

MADDE 74 - (1) Bir klinik araştırmanın 20 nci maddenin birinci fıkrası uyarınca hâlihazırda CE işareti taşıyan bir cihazı kullanım amacı kapsamı dâhilinde daha ileri seviyede değerlendirmek (piyasaya arz sonrası klinik takip araştırması) için yürütülmesi durumunda ve bu araştırmanın, gönüllülerin cihazın normal kullanım şartları altında gerçekleştirilenlere ilave olarak invaziv veya külfetli prosedürlere tabi tutulmasını içermesi durumunda; sponsor, piyasaya arz sonrası klinik takip araştırmasının başlangıcından en az 30 gün önce 73 üncü maddede atıfta bulunulan elektronik sistem vasıtasıyla Kurumu bilgilendirir. Sponsor, Ek XV'in II. Bölümünde atıfta bulunulan dokümantasyonu, bildirim bir parçası olarak sunar. 62 nci maddenin dördüncü fıkrasının (b) ile (i) ve (j) bentleri, 75 inci madde, 76 ncı madde, 77 nci madde, 79 uncu maddenin beşinci ve altıncı fıkrası ve Ek XV'in ilgili hükümleri piyasaya arz sonrası klinik takip araştırmalarına uygulanır.

(2) 20 nci maddenin birinci fıkrası uyarınca hâlihazırda CE işareti taşıyan bir cihazı kullanım amacının kapsamı dışında değerlendirmek üzere bir klinik araştırmanın yürütüleceği durumlarda 62 ila 79 uncu maddeler ve Komisyonca kabul edilen tasarruflar uygulanır.

Klinik araştırmalardaki önemli değişiklikler

MADDE 75 - (1) Sponsor; bir klinik arařtırmada, gönüllülerin güvenliđi, sađlıđı veya hakları üzerinde ya da arařtırmadan elde edilen klinik verilerin tutarlılıđı veya güvenilirliđi üzerinde önemli bir etkiye sahip olması muhtemel deđiřiklikler yapmayı amaçlarsa, bu deđiřikliklerin nedenlerini ve mahiyetini, 73 üncü maddede atıfta bulunulan elektronik sistem vasıtasıyla 1 hafta içerisinde Kuruma bildirir. Sponsor, Ek XV'in II. Bölümünde atıfta bulunulan ilgili dokümantasyonun güncel versiyonunu bildirim bir parçası olarak sunar. İlgili dokümanlardaki deđiřiklikler açık bir şekilde fark edilebilir olur.

(2) Kurum, klinik arařtırmadaki önemli deđiřiklikleri 71 inci maddede belirtilen prosedür uyarınca deđerlendirir.

(3) Sponsor;

a) Kurumun; 71 inci maddenin dördüncü fıkrasında atıfta bulunulan durumlara veya kamu sađlıđı, gönüllü ve kullanıcı güvenliđi veya sađlıđı ile kamu politikası deđerlendirmelerine dayanan reddini sponsora bildirmiş olması veya

b) İlgili etik kurulun; klinik arařtırmada yapılan önemli deđiřikliđe ilişkin olarak, olumsuz bir görüş vermiş olması,

dışında birinci fıkrada atıfta bulunulan deđiřiklikleri, söz konusu fıkrada atıfta bulunulan bildirimden itibaren en erken 38 gün sonra uygulayabilir.

(4) Kurum, uzmanlara danışmak amacıyla, üçüncü fıkrada atıfta bulunulan süreyi 7 gün daha uzatabilir.

Düzeltilici tedbirler ve bilgi alışveriři

MADDE 76 - (1) Kurum; bu Yönetmelikte belirtilen gerekliliklerin karşılanmadığını düşünmesi için gerekçesi olması durumunda, aşağıdaki tedbirlerden en az birini alabilir:

a) Klinik arařtırma iznini iptal etmek.

b) Klinik arařtırmayı askıya almak veya sonlandırmak.

c) Sponsordan klinik arařtırmanın herhangi bir hususunu deđerştirmesini talep etmek.

(2) Kurum, acil eylem gerektiren durumlar haricinde, birinci fıkrada atıfta bulunulan tedbirlerden herhangi birini almadan önce, sponsora veya arařtırmacıya veya her ikisine birden görüşlerini sorar. Bu görüş, 7 gün içerisinde verilir.

(3) Kurum; bu maddenin birinci fıkrasında atıfta bulunulan tedbirlerden birini aldığı veya bir klinik araştırmayı reddettiği durumda ya da güvenlik gerekçeleriyle bir klinik araştırmanın erken sonlandırılmasının sponsor tarafından kendisine bildirildiği durumda, ilgili kararı ve bunun gerekçelerini 73 üncü maddede atıfta bulunulan elektronik sistem vasıtasıyla AB üyesi ülkelere ve Komisyon'a bildirir.

(4) Bir başvurunun Kurumun kararından önce sponsor tarafından geri çekilmesi durumunda, bu bilgi 73 üncü maddede atıfta bulunulan elektronik sistem vasıtasıyla AB üyesi ülkelere ve Komisyon'a sunulur.

Bir klinik araştırma sona erdiğinde, geçici olarak durdurulduğunda veya erken sonlandırıldığında sponsordan gelen bilgiler

MADDE 77 - (1) Sponsor, bir klinik araştırmayı geçici olarak durdurursa veya erken sonlandırırsa; gerekçesini belirtmek suretiyle bu durumu, 73 üncü maddede atıfta bulunulan elektronik sistem vasıtasıyla 15 gün içerisinde Kuruma bildirir. Sponsor, güvenlik gerekçeleriyle klinik araştırmayı geçici olarak durdurması veya erken sonlandırması halinde, bu durumu 24 saat içerisinde Kuruma bildirir.

(2) Klinik araştırma planında aksi belirtilmedikçe, klinik araştırmanın bitiş tarihi ile son gönüllünün son ziyaret zamanı denk sayılır.

(3) Sponsor; Kuruma, klinik araştırmanın sona erdiğini bildirir. Bu bildirim, Türkiye'deki klinik araştırmanın sona ermesinden itibaren 15 gün içerisinde yapılır.

(4) Klinik araştırmanın Türkiye ve bir veya daha fazla AB üyesi ülke/ülkelerde yürütüldüğü durumda; sponsor, klinik araştırmanın tüm ülkelerde sona erdiğini klinik araştırmanın yürütüldüğü bütün ülkelere bildirir. Bu bildirim, klinik araştırmanın tüm ülkelerde sona ermesinden itibaren 15 gün içerisinde yapılır.

(5) Sponsor, klinik araştırmanın çıktılarına bakmaksızın, klinik araştırmanın sona ermesinden itibaren 1 yıl içerisinde veya erken sonlandırmadan ya da geçici olarak durdurmadan itibaren 3 ay içerisinde, Ek XV'in I. Bölümünün 2.8 numaralı maddesi ve III. Bölümünün 7 numaralı maddesinde atıfta bulunulduğu üzere bir klinik araştırma raporunu, Kuruma sunar. Klinik araştırma raporuna, hedeflenen kullanıcının kolaylıkla anlayabileceği bir şekilde sunulan bir özet eşlik eder. Söz konusu rapor ve özet, 73 üncü maddede atıfta bulunulan elektronik sistem vasıtasıyla sponsor tarafından sunulur. Bilimsel gerekçeler nedeniyle, klinik araştırma raporunun araştırmanın sona ermesinden itibaren 1 yıl içerisinde sunulmadığı durumda, söz konusu rapor mümkün olan en kısa sürede

sunulur. Bu gibi durumda, Ek XV'in II. Bölümünün 3 numaralı maddesinde atıfta bulunulan klinik araştırma planı, gerekçeyle birlikte klinik araştırma sonuçlarının ne zaman mevcut olacağını belirtir.

(6) Beşinci fıkrada atıfta bulunulan özet ve klinik araştırma raporu, 73 üncü maddede atıfta bulunulan elektronik sistem vasıtasıyla en geç, 29 uncu madde uyarınca cihaz kaydedildiğinde ve piyasaya arz edilmeden önce kamuya açık hale gelir. Erken sonlandırma veya geçici durdurma durumlarında, özet ve rapor, sunulduktan sonra ivedilikle kamuya açık hale gelir. Özet ve raporun beşinci fıkra uyarınca elektronik sisteme girilmiş olmasından itibaren 1 yıl içerisinde 29 uncu madde uyarınca cihaz kaydedilmezse, özet ve rapor kamuya açık hale gelir.

Klinik arařtırmalara yönelik koordineli deęerlendirme prosedürü

MADDE 78 - (1) Türkiye ve AB üyesi ülkelerin dâhil olduęu birden fazla ülkede yürütülecek olan bir klinik arařtırmanın sponsoru, 70 inci maddenin amaçları doęrultusunda, 73 üncü maddede atıfta bulunulan elektronik sistem vasıtasıyla klinik arařtırmanın yürütüleceęi tüm ülkelere elektronik ortamda iletilecek tek bir bařvuru yapabilir.

(2) Sponsor, birinci fıkrada atıfta bulunulan tek bařvuruda ilgili ülkelerden birini koordinatör ülke olarak faaliyet göstermesi için önerir. İlgili ülkeler, bařvurunun sunulmasından itibaren 6 gün içerisinde, içlerinden birisinin koordinatör ülke rolünü üstlenmesi konusunda anlaşır. İlgili ülkeler koordinatör ülke konusunda anlaşamazlarsa, sponsor tarafından önerilen koordinatör ülke bu rolü üstlenir.

(3) İkinci fıkrada atıfta bulunulan koordinatör ülkenin Türkiye olması durumunda Kurumun yönlendirmesi altında, ilgili ülkeler bařvurunun deęerlendirmesini, özellikle Ek XV'in II. Bölümünde atıfta bulunulan dokümantasyonun deęerlendirmesini koordine ederler. Ancak Ek XV'in II. Bölümünün 1.13, 3.1.3, 4.2, 4.3 ve 4.4 numaralı maddelerinde atıfta bulunulan dokümantasyonun tam olup olmadıęı, ilgili her ülke tarafından 70 inci maddenin bir ila beşinci fıkraları uyarınca ayrı ayrı deęerlendirilir.

(4) Kurum, koordinatör ülke olması durumunda, üçüncü fıkranın ikinci cümlesinde atıfta bulunulanlar haricindeki dokümantasyon ile ilgili olarak;

a) Tek bařvurunun alınmasından itibaren 6 gün içerisinde, koordinatör ülke olduęunu sponsora bildirir (bildirim tarihi).

b) Bařvurunun doęrulanması amacıyla, bildirim tarihinden itibaren 7 gün içerisinde ilgili bir ülke tarafından sunulan deęerlendirmeleri dikkate alır.

c) Bildirim tarihinden itibaren 10 gün içerisinde, klinik araştırmanın bu Yönetmelik kapsamına girip girmediğini ve başvurunun tam olup olmadığını değerlendirerek sponsoru bu doğrultuda bilgilendirir. 70 inci maddenin birinci fıkrası ve üç ila beşinci fıkraları, bu değerlendirme ile ilişkili olarak Kurum tarafından uygulanır.

ç) Değerlendirmesinin sonuçlarını, kabul tarihinden itibaren 26 gün içerisinde ilgili ülkelere iletilecek olan bir taslak değerlendirme raporu şeklinde oluşturur. Kabul tarihinden itibaren 38 güne kadar, taslak değerlendirme raporu ve esas başvuru hakkında ilgili AB üyesi ülkelere gelen yorumlar ve öneriler Kurumca dikkate alınır. Kurum kabul tarihinden itibaren 45 gün içerisinde sponsora ve diğer ilgili ülkelere iletilecek olan nihai değerlendirme raporunu neticelendirmesinde bu yorumları ve önerileri dikkate alır.

(5) Üçüncü fıkranın ikinci cümlesinde atıfta bulunulan dokümantasyonun değerlendirilmesi hususunda, Kurum da dâhil olmak üzere ilgili her ülke tek seferliğine spondordan ilave bilgiler talep edebilir. Sponsor, talep edilen ilave bilgileri, talebin alınmasından sonra 12 günü aşmayan ve ilgili ülke tarafından belirlenen süre içerisinde sunar. Dördüncü fıkranın (ç) bendinde belirtilen en son sürenin bitişi, talep tarihinden itibaren ilave bilgilerin alındığı zamana kadar dondurulur.

(6) Kurum, koordinatör ülke olması durumunda, sınıf IIB ve sınıf III cihazlar için uzmanlara danışmak amacıyla dördüncü fıkrada atıfta bulunulan süreleri 50 gün daha uzatabilir.

(7) Koordineli değerlendirme prosedürü uyarınca;

a) Koordinatör ülkenin koordineli değerlendirme alanıyla ilgili kararının, klinik araştırmanın yürütülmesinin kabul edilebilir olduğu veya spesifik koşullara uygun olması şartıyla kabul edilebilir olduğu durumda, bu karar ilgili tüm ülkelerin kararı olarak kabul edilir.

b) (a) bendine bakılmaksızın, ilgili bir ülke, koordinatör ülkenin koordineli değerlendirme alanıyla ilgili kararına yalnızca;

1) Klinik araştırmaya iştirakin, bir gönüllünün ilgili ülkedeki standart klinik uygulamada alacağından daha alt düzeyde tedavi almasına yol açabileceğini değerlendirdiği,

2) Ulusal mevzuat ihlali veya

3) Dördüncü fıkranın (ç) bendi kapsamında gönüllü güvenliğine ve sunulan veri güvenilirliğine ve tutarlılığına dair değerlendirmeler,

gerekçeleriyle katılmayabilir.

c) İlgili ülkelerden birinin (b) bendine dayanarak karara katılmaması durumunda, bu ülke, ihtilaf durumunu ayrıntılı bir gerekçeyle birlikte 73 üncü maddede atıfta bulunulan elektronik sistem vasıtasıyla Komisyon'a, ilgili diğer tüm ülkelere ve sponsora iletir.

(8) Koordinatör ülkenin koordineli değerlendirme alanıyla ilgili kararı, klinik araştırmanın kabul edilebilir olmadığı yönündeyse, bu karar ilgili tüm ülkelerin kararı olarak kabul edilir.

(9) Kurum, aşağıdaki durumlarda bir klinik araştırma için izin vermeyi reddeder ve Kurumca oluşturulan itiraz prosedürü kapsamında bu karara itirazda bulunulabilir:

a) Yedinci fıkranın (b) bendinde atıfta bulunulan gerekçelerden herhangi birine göre koordinatör ülkenin kararına katılmazsa.

b) Ek XV'in II. Bölümünün 1.13, 3.1.3, 4.2, 4.3 ve 4.4 numaralı maddelerinde ele alınan hususlara uyulmadığını usulünce gerekçelendirilmiş esaslarla ortaya çıkarırsa.

c) Bir etik kurulun bu klinik araştırmaya ilişkin olumsuz bir görüş vermesi durumunda.

(10) İlgili her ülke, 73 üncü maddede atıfta bulunulan elektronik sistem vasıtasıyla klinik araştırma için izin verilip verilmediğini, koşullu olarak izin verilip verilmediğini ya da iznin reddedilmiş olup olmadığını sponsora bildirir. Bildirim, nihai değerlendirme raporunun koordinatör ülke tarafından dördüncü fıkranın (ç) bendi uyarınca iletiminden itibaren 5 gün içerisinde tek bir karar yoluyla yapılır. Bir klinik araştırmaya koşullu olarak izin verilmesi, ancak bu koşullar izin verme sırasında yerine getirilemeyecekse mümkün olur.

(11) 75 inci maddede atıfta bulunulduğu üzere önemli değişiklikler, 73 üncü maddede atıfta bulunulan elektronik sistem vasıtasıyla ilgili ülkelere bildirilir. İlgili her ülke tarafından ayrı ayrı değerlendirilen Ek XV'in II. Bölümünün 1.13, 3.1.3, 4.2, 4.3 ve 4.4 numaralı maddelerine ilişkin önemli değişiklikler hariç olmak üzere, yedinci fıkranın (b) bendinde atıfta bulunulan ihtilaflara yönelik dayanakların varlığına ilişkin her bir değerlendirme, koordinatör ülkenin yönlendirmesi altında yürütülür.

Klinik araştırmalar sırasında meydana gelen advers olayların kaydedilmesi ve raporlanması

MADDE 79 - (1) Sponsor, aşağıdakilerin hepsini tam olarak kaydeder:

a) Klinik araştırma planında bu klinik araştırmanın sonuçlarının değerlendirilmesi için kritik olarak tanımlanan herhangi bir advers olay türünü.

b) Herhangi bir ciddi advers olayı.

c) Uygun faaliyet yapılmadığında, müdahale gerçekleşmediğinde veya şartlar daha olumsuz olduğunda ciddi bir advers olaya yol açabilecek herhangi bir cihaz kusurunu.

ç) (a) ile (c) bentlerinde atıfta bulunulan herhangi bir olayla ilgili yeni bulguları.

(2) Bu Yönetmelik uyarınca;

a) Sponsor, Kuruma 73 üncü maddede atıfta bulunulan elektronik sistem vasıtasıyla aşağıdakilerin hepsini gecikmeksizin raporlar:

1) Araştırma amaçlı cihazla, karşılaştırma cihazıyla veya araştırma prosedürüyle nedensel bir ilişkiye sahip olan veya bu tür nedensel ilişkinin ihtimal dâhilinde kurulabildiği herhangi bir ciddi advers olayı.

2) Uygun faaliyet yapılmadığında, müdahale gerçekleşmediğinde veya şartlar daha olumsuz olduğunda ciddi bir advers olaya yol açabilecek herhangi bir cihaz kusurunu.

3) (1) ve (2) numaralı alt bentlerde atıfta bulunulan herhangi bir olayla ilgili yeni bulguları.

b) Raporlama süresi için, olayın şiddeti dikkate alınır. Zamanında raporlamayı mümkün kılmak için gerekli olduğu durumda sponsor tam bir rapordan önce tamamlanmamış bir başlangıç raporu sunabilir.

c) Kurumun talebi üzerine, sponsor birinci fıkrada atıfta bulunulan tüm bilgileri temin eder.

(3) Sponsor, 73 üncü maddede atıfta bulunulan elektronik sistem vasıtasıyla bu Yönetmelik kapsamındaki bir klinik araştırmayla aynı klinik araştırma planı altında Türkiye ve AB üyesi ülkeler dışındaki ülkelerde yürütülen bir klinik araştırma sırasında meydana gelen, ikinci fıkrada atıfta bulunulan herhangi bir olayı da Kuruma raporlar.

(4) Koordineli değerlendirme prosedürü uyarınca;

a) Sponsorun 78 inci maddede atıfta bulunulan tek başvuruyu kullandığı bir klinik araştırma söz konusu olduğunda, sponsor, 73 üncü maddede atıfta bulunulan elektronik sistem vasıtasıyla, ikinci fıkrada atıfta bulunulduğu üzere her bir olayı raporlar. Bu rapor alındıktan sonra, klinik araştırmanın yürütüldüğü tüm ülkelere elektronik olarak iletilir.

b) İlgili ülkeler; 78 inci maddenin ikinci fıkrasında atıfta bulunulan koordinatör ülkenin yönlendirmesi altında, bir klinik araştırmada değişiklik yapıp yapılmayacağına, klinik araştırmanın askıya alınıp alınmayacağına veya sonlandırılıp sonlandırılmayacağına ya da bu klinik araştırmaya yönelik izin iptal edilip edilmeyeceğine karar vermek için, ciddi advers olaylar ve cihaz kusurları hakkındaki değerlendirmelerini koordine ederler.

c) Kurum, kamu sađlıđının ve hasta gvenliđinin korunmasını sađlamak amacıyla, bu Ynetmelik uyarınca kendi deđerlendirmelerini yapar ve gerektiđinde ilave tedbirler alır. Koordinatr lke ve Komisyon, bu tr deđerlendirmelerin sonucu ve bu tr tedbirlerin alınması hakkında daima bilgilendirilir.

(5) 74 nc maddenin birinci fıkrasında atıfta bulunulan piyasaya arz sonrası klinik takip arařtırmaları durumunda, bu madde yerine 85 ila 88 inci maddelerde ve Komisyonca kabul edilen tasarruflarda belirtilen vijilansa iliřkin hkmler uygulanır.

(6) Beřinci fıkraya bakılmaksızın, ciddi advers olay ile olaydan nceki arařtırma prosedr arasında nedensel bir iliřkinin kurulmuř olması durumunda bu madde uygulanır.

Diđer klinik arařtırmalarla ilgili gereklilikler

Madde 80 - (1) 62 nci maddenin birinci fıkrasında listelenen amaçların herhangi biri uyarınca gerçekleřtirilmeyen klinik arařtırmalar, 62 nci maddenin ikinci ve çnc fıkrasının, 62 nci maddenin drdnc fıkrasının (b), (c), (ç), (e), (g) ve (i) bentlerinin ve 62 nci maddenin altıncı fıkrasının hkmlerine uyar.

(2) Kurum; gnlllerin haklarını, gvenliđini, onurunu, refahını ve 62 nci maddenin birinci fıkrasında listelenen amaçlar haricinde yrtlen klinik arařtırmaların bilimsel ve etik btnlđn korumak iin ihtiyaları dođrultusunda bu tr arařtırmalara iliřkin ilave gereklilikler belirler.

(...)

DOKUZUNCU KISIM

Gizlilik, Verilerin Korunması, Finansman ve Cezalar

BİRİNCİ BLM

Gizlilik, Verilerin Korunması, Finansman ve Cezalar

Gizlilik

MADDE 103 - (1) Bu Ynetmelikte aksi belirtilmediđi srece ve gizliliđe iliřkin mevcut hkmlere ve uygulamalara halel gelmeksizin, bu Ynetmeliđin uygulanmasında yer alan tm taraflar;

a) 104 nc madde uyarınca kiřisel verileri korumak,

b) Kamu yararı bakımından aıklanması gerekmedike, fikri mlkiyet hakları dhil olmak zere, bir gerek veya tzel kiřinin ticari gizli bilgilerini ve mesleki sırlarını korumak,

c) Özellikle incelemeler, arařtırmalar veya denetimlerle ilgili amalar dođrultusunda bu Yönetmeliđin etkili uygulanmasını sađlamak,

iin görevlerini yerine getirirken elde edilen bilgilerin ve verilerin gizliliđine riayet eder.

(2) Birinci fıkraya habel gelmeksizin, yetkili otoritelerin ya da Komisyonun Kurumla gizlilik temelinde paylařtıđı bilgiler, bilginin kaynađı olan otoritenin onayı alınmadan aıklanmaz.

(3) Birinci ve ikinci fıkralar, Kurumun ve onaylanmış kuruluşların bilgi paylaşımı ve uyarıların duyurulması ile ilgili hak ve yükümlölüklerini ve ilgili kişilerin adli süreçte bilgi sunma yükümlölüklerini etkilemez.

Kişisel verilerin korunması

MADDE 104 - (1) Bu Yönetmelik uyarınca kişisel verilerin işlenmesinde Kişisel Verilerin Korunması Kanunu ve kişisel verilerin korunması ile ilgili diđer mevzuat uygulanır.

Ücretlendirme

MADDE 105 - (1) Kurum; ücret düzeylerini şeffaf bir şekilde ve maliyeti karşılama ilkeleri çerçevesinde belirleyerek, bu Yönetmelik kapsamındaki faaliyetlerine yönelik ücretlendirme uygulayabilir.

(2) Kurum; ücretlerin yapısının ve düzeyinin yayımlanmasından en az 3 ay önce, Komisyonu ve AB üyesi ülkeleri bilgilendirir. Ücretlerin yapısı ve düzeyi, talep üzerine kamuya aık hale getirilir.

(...)

Tıbbi Cihaz Klinik Arařtırmaları Yönetmeliđi

Resmî Gazete Tarihi : 08.07.2022

Resmî Gazete Sayısı : 31890

Türkiye İlaç ve Tıbbi Cihaz Kurumundan:

TIBBİ CİHAZ KLİNİK ARAŐTIRMALARI YÖNETMELİĐİ

BİRİNCİ BÖLÜM

Başlangıç Hükümleri

Amaç

MADDE 1- (1) Bu Yönetmeliđin amacı, taraf olunan uluslararası anlaşmalar ile Avrupa Birliđi standartları ve iyi klinik uygulamaları çerçevesinde piyasaya arz sonrası çalışmalarını ve tıbbi cihaz klinik arařtırmaları ile bu arařtırmalara katılan gönüllülerin haklarının korunmasına dair usûl ve esasları düzenlemektir.

Kapsam

MADDE 2- (1) Bu Yönetmelik, piyasaya arz sonrası çalışmalar ile tıbbi cihaz klinik arařtırmalarını, arařtırma yapılabilecek yerleri ve bu arařtırmaları gerçekleřtirecek gerçek veya tüzel kişileri kapsar.

(2) Retrospektif çalışmalar ve in vitro tanı amaçlı tıbbi cihazlar ile yapılan performans deđerlendirme çalışmalarını bu Yönetmeliđin kapsamı dışındadır.

Dayanak

MADDE 3- (1) Bu Yönetmelik; 7/5/1987 tarihli ve 3359 sayılı Sağlık Hizmetleri Temel Kanunununun Ek-10 uncu maddesi ile 4 sayılı Bakanlıklara Bađlı, İlgili, İliřkili Kurum ve Kuruluşlar ile Diđer Kurum ve Kuruluşların Teřkilatı Hakkında Cumhurbaşkanlıđı Kararnamesinin 508 inci ve 796 ncı maddelerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4- (1) Bu Yönetmelikte geçen;

- a) Çok merkezli klinik araştırma: Tek bir protokole göre birden fazla merkezde yürütülen, bu sebeple birden fazla sorumlu araştırmacının bulunduğu klinik araştırmayı,
- b) Denetim: Klinik araştırma yapılan yerlerin, sponsor, varsa yasal temsilci ve sözleşmeli araştırma kuruluşuna ait merkezlerin, araştırmaya ait belgeler ve kayıtların, kalite güvencesi düzenlemelerinin ve araştırma ile ilgili olan etik kurullar dâhil diğer kurum, kurul ve kuruluşların bu Yönetmeliğe ve ilgili diğer mevzuata uygunluğu açısından Kurum tarafından incelenmesi faaliyetlerini,
- c) EUDAMED işlevsellik tarihi: 2/6/2021 tarihli ve 31499 mükerrer sayılı Resmî Gazete’de yayımlanan Tıbbi Cihaz Yönetmeliğinin 33 üncü maddesi uyarınca Komisyonca kurulan tıbbi cihazlara ilişkin Avrupa veri tabanı olan EUDAMED’in Avrupa Birliği Resmî Gazetesinde tamamen işlevsel olduğu ve fonksiyonel spesifikasyonlarını karşıladığına dair bildirim yayımlandığı tarihten 6 ay sonraki tarihi,
- ç) İdari sorumlu: Çok merkezli bir araştırmada, uzmanlık veya doktora eğitimini tamamlamış olup, araştırmanın yürütülmesinden idari olarak sorumlu olan hekim veya diş hekimini,
- d) İyi klinik uygulamaları: Araştırmaların uluslararası bilimsel ve etik standartlarda yapılmasını sağlamak amacıyla araştırmanın tasarlanması, yürütülmesi, izlenmesi, bütçelendirilmesi, değerlendirilmesi ve raporlanması, gönüllünün tüm haklarının ve vücut bütünlüğünün korunması, araştırma verilerinin güvenilirliğinin sağlanması, gizliliğinin muhafaza edilmesi gibi konular hakkındaki düzenlemeleri kapsayan ve araştırmaya iştirak eden taraflarca uyulması gereken kuralları,
- e) İzleyici (Monitör): Araştırmanın, klinik araştırma planı, iyi klinik uygulamaları ilkeleri ve mevzuat gerekliliklerine uygun olarak yapıldığını izlemek için araştırma merkezinden bağımsız olarak sponsor tarafından atanan kişiyi,
- f) Koordinatör: Çok merkezli bir klinik araştırmada merkezlerin araştırmacıları ile etik kurul, sponsor, mevcutsa yasal temsilci ve gerekirse bunlar ile Kurum arasındaki koordinasyonun sağlanmasından sorumlu kişiyi,
- g) Piyasaya arz sonrası çalışma: Tıbbi Cihaz Yönetmeliğine uygun olarak üzerine CE işareti iliştirilerek piyasaya arz edilmiş cihazların imalatçısı tarafından belirlenmiş kullanım amaçlarına uygun olarak kullanılması kaydıyla cihazın performans veya güvenlik verilerinin toplanmasına yönelik gönüllüler üzerinde yapılan çalışmaları,
- ğ) Retrospektif çalışma: Geriye yönelik verilerin toplandığı çalışmaları,

h) Sözleşmeli araştırma kuruluşu: Sponsorun klinik araştırma ile ilgili görev ve yetkilerinin tümünü veya bir kısmını yazılı bir sözleşmeyle devrettiği, iyi klinik uygulamaları ilkelerine uygun çalışan bağımsız kuruluşu,

ı) Tıbbi Cihaz Yönetmeliği: 2/6/2021 tarihli ve 31499 mükerrer sayılı Resmî Gazete’de yayımlanan Tıbbi Cihaz Yönetmeliğini,

ifade eder.

(2) Tıbbi Cihaz Yönetmeliğinin 3 üncü maddesinde yer alan tanımlar bu Yönetmelik için de geçerlidir.

İKİNCİ BÖLÜM

Araştırmanın Genel Esasları

Klinik araştırmalar ile ilgili genel esaslar

MADDE 5- (1) Klinik araştırmalar ile ilgili olarak Tıbbi Cihaz Yönetmeliğinin 62 ila 80 inci madde hükümleri geçerlidir. Bu maddelere ilişkin Tıbbi Cihaz Yönetmeliğinin 111 inci maddesindeki yürürlük tarihleri doğrultusunda hareket edilir. Tıbbi Cihaz Yönetmeliğinin ilgili maddeleri ile birlikte aşağıdaki hükümler uygulanır.

(2) Tıbbi Cihaz Yönetmeliğinin 62 nci maddesinin üçüncü fıkrasının (a) bendinde belirtilen uluslararası standartlara uygun olarak;

a) Araştırma cihazının, öncelikle insan dışı deney ortamında veya yeterli sayıda deney hayvanı üzerinde araştırılmış olması şarttır.

b) İnsan dışı deney ortamında veya hayvanlar üzerinde yapılan deneyler sonucunda ulaşılan bilimsel verilerin, araştırma ile varılmak istenen hedefe ulaşmak açısından cihazın/cihazların klinik araştırmalarının yürütülebilmesi için yeterli kanıt sağlaması gerekmektedir.

c) Gönüllüye ait germ hücrelerinin genetik yapısını bozmaya yönelik hiçbir araştırma yapılamaz.

(3) Tıbbi Cihaz Yönetmeliğinin 62 nci maddesinin üçüncü fıkrasının (c) bendinde belirtilen bilimsel ve etik inceleme için 13/4/2013 tarihli ve 28617 sayılı Resmî Gazete’de yayımlanan İlaç ve Biyolojik Ürünlerin Klinik Araştırmaları Hakkında Yönetmelikte yapısı, çalışma usûl ve esasları belirtilen ve Kurumdan onay almış Klinik Araştırma Etik Kurulları yetkilidir. Klinik Araştırma Etik Kurulları, görev ve yetkileri ölçüsünde piyasaya arz sonrası çalışmaları ile tıbbi cihaz klinik araştırmalarının incelenmesi, izlenmesi ve takibi konusunda sorumludur.

(4) Tıbbi Cihaz Yönetmeliğinin 62 nci maddesinin dördüncü fıkrasının (1) bendi uyarınca gönüllülerin araştırmaya iştiraki veya iştirakin devamının sağlanmasına yönelik olarak gönüllü veya yasal vasisi için herhangi bir ikna edici teşvikte veya mâli teklifte bulunulamaz. Ancak gönüllülerin araştırmaya iştiraki ile ortaya çıkacak masraflar ile sağlıklı gönüllülerin çalışma günü kaybından doğan gelirden yoksunluk araştırma bütçesinde belirtilir ve bu bütçeden karşılanabilir.

(5) Tıbbi Cihaz Yönetmeliğinin 62 nci maddesinin altıncı fıkrası uyarınca araştırmalar, sorumlu araştırmacının başkanlığında, araştırmanın niteliğine uygun araştırmacılardan oluşan bir ekiple yürütülür. Araştırma ekibi içerisinde araştırma konusu ile ilgili dalda uzmanlık veya doktora eğitimini tamamlamış bir hekim veya dış hekimi sorumlu araştırmacı olarak belirlenir.

(6) Tıbbi Cihaz Yönetmeliğinin 62 nci maddesinin yedinci fıkrası uyarınca araştırmalar; üzerinde araştırma yapılacak kimselerin emniyetini sağlamaya ve araştırmanın sağlıklı bir şekilde yürütülebilmesine, takibine ve gereğinde acil müdahale yapılabilmesine elverişli ve araştırmanın vasfına uygun personel, teçhizat ve laboratuvar imkânlarına sahip olan; üniversite sağlık uygulama ve araştırma merkezleri, üniversitelere bağlı onaylanmış araştırma geliştirme merkezleri ve Sağlık Bakanlığı eğitim ve araştırma hastanelerinde tercihen klinik araştırma yapmak üzere tasarlanmış yerlerde yapılabilir. Bu merkezler ve hastanelerde yapılan klinik araştırmalara, gereğinde bu merkezlerin ve hastanelerin koordinatörlüğünde veya idari sorumluluğunda olmak kaydı ile belirtilen nitelikleri haiz sağlık kurum ve kuruluşları da dâhil edilebilir. İyi klinik uygulamaları esas alınarak klinik araştırma yapılacak yerler asgari olarak;

a) Araştırmanın niteliğine göre gerekli ve yeterli personel ile ekipmana,

b) Araştırma amaçlı cihazın niteliğine göre ürünün saklanması ve dağıtılması için gerekli yer ve imkânlar,

c) Acil müdahale gerekebilecek durumlar da dâhil olmak üzere gönüllü için uygun bakım hizmeti verecek imkân ve donanıma,

ç) Gönüllünün gerektiğinde daha ileri bir sağlık kurum veya kuruluşuna nakledilebilmesini mümkün kılacak yeterli imkân ve donanıma,

d) Araştırmanın tamamlanmasından sonra klinik araştırmaya ve gönüllülere ait bilgi ve belgeleri muhafaza edebilecek yeterli imkân ve donanıma,

sahip olmak zorundadır.

(7) Tıbbi Cihaz Yönetmeliğinin 63 üncü maddesi uyarınca gönüllünün bilgilendirilmiş gönüllü olurlarını veremediği durumlarda yürürlükteki mevzuat uyarınca gönüllünün arařtırmaya katılımı konusunda onay vermeye yetkili kiři, yetkili vasi olarak kabul edilir.

(8) Tıbbi Cihaz Yönetmeliğinin 63 üncü maddesinin ikinci fıkrasının (c) bendi uyarınca bilgilendirilmiş gönüllü olurlarına iliřkin ön görüřme sorumlu arařtırmacı veya arařtırma ekibinde yer alan ve sorumlu arařtırmacı tarafından yetkilendirilmiş olan bir hekim veya diř hekim tarafından yapılır.

(9) Tıbbi Cihaz Yönetmeliğinin 69 uncu maddesi uyarınca gönüllülerin klinik arařtırmadan doęabilecek zararlara karřı güvence altına alınması amacıyla CE iřareti taşıyan ve tıbbi cihazın imalatçısı tarafından belirtilen kullanım amacı doęrultusunda yapılan tıbbi cihaz klinik arařtırmalarında etik kurulun fayda-risk oranına göre uygun görmesi řartı ile sigorta aranmaz, ancak diđer tüm tıbbi cihaz klinik arařtırmalarında gönüllülere sigorta yapılması řarttır. Arařtırmanın bařlatılmasından önce nihai sigortanın sunulması řartıyla etik kurul ve Kuruma yapılacak bařvurularda teklif sigorta sunulabilir.

(10) Çok merkezli arařtırmalarda sponsor tarafından sorumlu arařtırmacılar arasından bir koordinatör seçilir. Çok uluslu ve çok merkezli arařtırmalarda ise sponsor tarafından ülke koordinatörü olarak Türkiye'deki sorumlu arařtırmacılar arasından bir koordinatör seçilir. Koordinatörün bulunduęu arařtırma merkezi koordinatör merkez olarak kabul edilir. Koordinatörün, altıncı fıkrada belirtilen koordinatör olabilecek merkezlerin sorumlu arařtırmacıları arasından seçilmesi gerekmektedir.

Etkilenebilir popülasyonlarda klinik arařtırmalar

MADDE 6- (1) Etkilenebilir popülasyonlarda klinik arařtırmalar ile ilgili olarak Tıbbi Cihaz Yönetmeliğinin 64 ila 68 inci madde hükümleri ile birlikte bu maddede yer alan hükümleri uygulanır.

(2) Tıbbi Cihaz Yönetmeliğinin 63 üncü maddesinin yedinci fıkrası uyarınca çocukların arařtırmalara iřtirak etmeleri için çocuk rızasını açıklama yetisine sahip ise kendi rızasının yanı sıra ana ve babasının veya vesayet altında ise vasisinin Yönetmeliğinin 63 üncü maddesine uygun řeklide yazılı olarak oluru alınır.

(3) Tıbbi Cihaz Yönetmeliğinin 64 üncü maddesinde belirtilen kısıtlılara yönelik arařtırmalarda; etik kurul, arařtırmayla ilgili klinik, etik, psikolojik ve sosyal problemler konusunda, arařtırma konusu ile ilgili alanda uzmanlıęı almıř bir hekim tarafından bilgilendirilir ve protokol bu yönde deęerlendirilir.

(4) Tıbbi Cihaz Yönetmeliğinin 65 inci maddesinde belirtilen çocuklara yönelik arařtırmalarda; etik kurul, arařtırmayla ilgili klinik, etik, psikolojik ve sosyal problemler konusunda çocuk saėlıėı ve hastalıkları uzmanı bir hekim tarafından bilgilendirilir ve protokol bu yönde deėerlendirilir. Çocuk saėlıėı ve hastalıkları uzmanı bir hekimin arařtırmanın çocuklar üzerinde yapılması hususunda müspet görüşü olmadan etik kurul bu arařtırmaya onay veremez.

(5) Tıbbi Cihaz Yönetmeliğinin 66 ncı maddesinde belirtilen gebe veya emziren kadınlara yönelik arařtırmalarda; etik kurul, gebe veya emziren kadın ya da embriyo, fetüs veya doğan çocuk saėlıėı yönünden, klinik, etik, psikolojik ve sosyal problemler konusunda arařtırma konusu ile ilgili alanda uzmanlıėı almıř bir hekim tarafından bilgilendirilir ve protokol bu yönde deėerlendirilir.

(6) Tıbbi Cihaz Yönetmeliğinin 67 nci maddesinde belirtilen ilave tedbirler, belirli bir hiyerarřik yapının içerisinde yer alan veya ekonomik, sosyal ve tıbbi gerekçeleri nedeni ile kendini koruyabilme özelliğinin henüz gelişmediėi, azaldıėı veya tamamen ortadan kalktıėı özerkliği sınırlı veya azalmıř kişiler için de uygulanabilir.

(7) Tıbbi Cihaz Yönetmeliğinin 68 inci maddesinde belirtilen acil durumlarda arařtırmalarda; etik kurul, arařtırmayla ilgili klinik, etik, psikolojik ve sosyal problemler konusunda, arařtırma konusu ile ilgili alanda uzmanlıėı almıř bir hekim tarafından bilgilendirilir ve protokol bu yönde deėerlendirilir.

(8) Arařtırma konusunun doğrudan bilinci kapalı kişileri ilgilendiren ya da bilinci kapalı kişilerde incelenebilir bir durum olması hâlinde veya bilinci kapalı kişilerin hastalığıyla ilgili mevcut tedavi seçeneklerinin tamamen tüketildiėi durumlarda, arařtırma bilinci kapalı kişilerin saėlıėı açısından öngörülebilir bir risk taşıyor ve arařtırmanın bilinci kapalı kişilere doğrudan bir fayda saėlayacaėı hususunda genel tıbbi bir kanaat bulunuyorsa 5 inci madde ve Tıbbi Cihaz Yönetmeliğinin 62 nci maddesinin dördüncü fıkrasında belirtilen hususlar ile birlikte ařaėıda belirtilenler çerçevesinde bilinci kapalı kişiler üzerinde arařtırma yapılmasına izin verilebilir:

a) Arařtırmanın bilinci kapalı kişiler üzerinde bilinen herhangi bir riskinin olmadığı hususunda genel tıbbi bir kanaatin bulunması gerekir.

b) Bilinci kapalı kişilerin varsa yasal vasileri Tıbbi Cihaz Yönetmeliğinin 63 üncü maddesi uyarınca bilgilendirilir ve yazılı olurları alınır.

c) Bilinci kapalı kişiler, kendisine verilen bilgi hakkında deėerlendirme yaparak bu konuda kanaate varabilme kapasitesine sahip hale gelirlerse, arařtırmaya iřtirak etmeyi reddetmeleri veya arařtırmanın herhangi bir safhasında arařtırmadan çekilmek istemeleri durumlarında arařtırmadan derhal çıkarılır.

ç) Etik kurul, arařtırmayla ilgili klinik, etik, psikolojik ve sosyal problemler konusunda, arařtırma konusu ile ilgili alanda uzmanlıđını almıř bir hekim tarafından bilgilendirilir ve protokol bu yönde deđerlendirilir.

d) Bilinci kapalı kiřilerin yasal vasilerine ulařılamaması nedeniyle yazılı olurlarının alınamaması durumlarında, birinci fıkra hükümleriyle beraber ařađıdaki řartların varlıđı hâlinde, sorumlu arařtırmacı veya hekim olan bir arařtırmacının sorumluluđunda, bilinci kapalı kiřiler arařtırmaya dâhil edilebilir:

1) Önerilen arařtırma protokolü veya diđer belgelerin, söz konusu arařtırmadaki etik hususları yeterince karřılayıp karřılamadıklarını etik kurulun önceden deđerlendirmiş olması,

2) Kardiyak arrest, kafa travması, santral sinir sistemi enfeksiyonları, beyin içi kanamaları gibi ani geliřip hekimin hemen müdahale etmesi gereken ve mevcut tedavi seeneklerinin tamamen tüketildiđi durumlarda, bilinci kapalı kiřilere arařtırmanın dođrudan bir fayda sađlayacađına yönelik genel tıbbi bir kanaatin bulunması.

ÜÇÜNCÜ BÖLÜM

Arařtırmaların Bařlatılması ve Yürütülmesi

Klinik arařtırma bařvurusu

MADDE 7- (1) EUDAMED işlevsellik tarihine kadar klinik arařtırma bařvuruları ile ilgili olarak ařađıdaki hükümler uygulanır:

a) Klinik arařtırmanın sponsoru, Tıbbi Cihaz Yönetmeliđinin Ek XV'inin II. Bölümünde atıfta bulunulan dokümantasyonla birlikte Kurumun elektronik bařvuru sistemi aracılıđıyla bařvuruda bulunur.

b) Bařvurunun usûlüne uygun olarak yapılması, bařvuruda bulunması gereken bilgi ve belgelerde eksiklik bulunmaması hâlinde bařvurunun Kurum tarafından incelenerek yirmi iş günü içerisinde sonuçlandırılması esastır.

c) Klinik arařtırmalar Kurumun izni olmadan bařlatılamaz.

(2) EUDAMED işlevsellik tarihinden itibaren Tıbbi Cihaz Yönetmeliđinin 70 inci maddesi uygulanır.

Klinik arařtırma bařvurusunun deđerlendirilmesi

MADDE 8- (1) Kurum, klinik arařtırma bařvurularını Tıbbi Cihaz Yönetmeliđinin 71 inci maddesinde belirlenen hususlar dođrultusunda deđerlendirir. İlgili maddenin dördüncü fıkrasının (a) bendinde

başvurunun tamlığına yapılmış atıf bu Yönetmeliğin 7 nci maddesinin birinci fıkrasının (a) ve (b) bentlerine de yapılmış sayılır.

(2) Çok merkezli klinik araştırmalarda tek etik kurul kararının bulunması yeterlidir. Kuruma yapılacak başvurularda etik kurul kararı başvurunun bir parçası olarak sunulur.

(3) Kuruma başvuru yapılırken, ilgili araştırma için aynı etik kuruldaki onay alınmış olsa bile önceki olumsuz etik kurul kararları başvuru esnasında Kuruma sunulur.

Klinik araştırmanın yürütülmesi

MADDE 9- (1) Klinik araştırmanın yürütülmesine ilişkin Tıbbi Cihaz Yönetmeliğinin 72 nci maddesindeki hükümler geçerlidir.

(2) Araştırmaya katılan gönüllülerin kimliğinin gizli kalması amacıyla sorumlu araştırmacı veya diğer araştırmacılar tarafından herhangi bir advers olay veya araştırmayla ilgili veri rapor edilirken gönüllünün adı ve tanımlayıcı bilgileri yerine her bir gönüllüye verilen gönüllü kodu kullanılır.

(3) Gönüllülerin kişisel verileri hiçbir şekilde kamuya açık hale getirilemez.

Piyasaya arz sonrası çalışmalar

MADDE 10- (1) EUDAMED işlevsellik tarihine kadar piyasa arz sonrası çalışmalar için;

a) Tıbbi Cihaz Yönetmeliğinin 62 ila 69 uncu maddeleri ile bu Yönetmeliğin 5 inci maddenin üçüncü ila onuncu fıkraları,

b) 6 ncı madde, 7 nci maddenin birinci fıkrası, 8 inci ve 9 uncu maddeler, 11 inci maddenin birinci fıkrası, 12 nci maddenin birinci fıkrası, 13 üncü maddenin birinci fıkrası ile 14 üncü maddenin birinci ve ikinci fıkrası,

hükümleri geçerlidir.

(2) EUDAMED işlevsellik tarihinden itibaren Tıbbi Cihaz Yönetmeliğinin 74 üncü maddesi uygulanır.

Klinik araştırmalardaki önemli değişiklikler

MADDE 11- (1) EUDAMED işlevsellik tarihine kadar bir klinik araştırmada, gönüllülerin güvenliği, sağlığı veya hakları üzerinde ya da araştırmadan elde edilen klinik verilerin tutarlılığı veya güvenilirliği üzerinde önemli bir etkiye sahip olması muhtemel değişiklikler (önemli değişiklikler) için;

a) Klinik araştırmanın sponsoru, yapılmak istenen değişikliklerin mahiyeti ve nedenleri ile birlikte Kurumun elektronik başvuru sistemi aracılığıyla başvuruda bulunur. Tıbbi Cihaz Yönetmeliğinin Ek

XV'inin II. Bölümünde atıfta bulunulan dokümantasyonun güncel halleri bu başvurunun bir parçası olarak sunulur. İlgili dokümanlardaki değişiklikler açık bir şekilde fark edilebilir olmalıdır.

b) Başvurunun usulüne uygun olarak yapılması, başvuruda bulunması gereken bilgi ve belgelerde eksiklik bulunmaması hâlinde başvurunun Kurum tarafından incelenerek otuz iş günü içerisinde sonuçlandırılması esastır.

c) Kurum önemli değişiklik başvurularını bu Yönetmeliğin 8 inci maddesinde belirlenen hususlar doğrultusunda değerlendirir.

ç) Önemli değişiklikler Kurumun izni olmadan uygulanamaz.

(2) EUDAMED işlevsellik tarihinden itibaren Tıbbi Cihaz Yönetmeliğinin 75 inci maddesi uygulanır.

Düzeltilici tedbirler

MADDE 12- (1) EUDAMED işlevsellik tarihine kadar araştırmalarda alınacak düzeltilici tedbirler için Tıbbi Cihaz Yönetmeliğinin 76 ncı maddesinin birinci ve ikinci fıkraları uygulanır.

(2) EUDAMED işlevsellik tarihinden itibaren Tıbbi Cihaz Yönetmeliğinin 76 ncı maddesi uygulanır.

Bir klinik araştırma sona erdiğinde, geçici olarak durdurulduğunda veya erken sonlandırıldığında sponsordan gelen bilgiler

MADDE 13- (1) EUDAMED işlevsellik tarihine kadar bir klinik araştırmanın sona ermesi, geçici olarak durdurulması ve erken sonlandırılması durumunda; Kurumun elektronik başvuru sisteminin kullanılması kaydıyla Tıbbi Cihaz Yönetmeliğinin 77 nci maddesinin birinci, ikinci, üçüncü ve beşinci fıkraları uygulanır.

(2) EUDAMED işlevsellik tarihinden itibaren Tıbbi Cihaz Yönetmeliğinin 77 nci maddesi uygulanır.

Klinik araştırmalar sırasında meydana gelen advers olayların kaydedilmesi ve raporlanması

MADDE 14- (1) EUDAMED işlevsellik tarihine kadar klinik araştırmalar sırasında meydana gelen advers olayların kaydedilmesi ve raporlanması için; Kurumun elektronik başvuru sisteminin kullanılması kaydıyla Tıbbi Cihaz Yönetmeliğinin 79 uncu maddesinin bir ila üçüncü fıkraları uygulanır.

(2) EUDAMED işlevsellik tarihine kadar piyasaya arz sonrası çalışmalar için; birinci fıkra yerine piyasa arz edilmiş cihazlar için ilgili mevzuatta belirlenen vijilansa ilişkin hükümler uygulanır.

(3) EUDAMED işlevsellik tarihinden itibaren Tıbbi Cihaz Yönetmeliğinin 79 uncu maddesi uygulanır.

DÖRDÜNCÜ BÖLÜM

Sponsorun ve Arařtırmacıların Sorumlulukları

Sponsor ve sorumlu arařtırmacının arařtırma amaçlı cihaza iliřkin sorumlulukları

MADDE 15- (1) Tıbbi Cihaz Yönetmeliğinde sponsorun ve arařtırmacıların arařtırma amaçlı cihaza iliřkin yükümlülükleri ile ilgili belirtilen hükümler yanında;

a) Arařtırma amaçlı cihazın, imalatı ya da ithalatından sonra ürünün özelliklerine uygun olarak depolanması, dağıtımı ve arařtırma merkezine teslimi, eğer gerekiyorsa kurulumu ve bakım, onarım kalibrasyon işlemleri ile arařtırma merkezinde bu koşulların devam ettirilmesi, kullanılmamış ürünlerin arařtırma merkezinden toplanarak iadesinin sağlanması veya uygun şekilde imhası ve bütün bu sürece ait kayıtların tutulması sponsorun yükümlülüğü altındadır.

b) Arařtırma amaçlı cihazın teslim alınması, muhafazası, yazılı istek veya arařtırma protokolüne uygun dağıtımı, stok kontrolü, artan kısmına yapılacak işlemler ve kayıtlarının tutulması arařtırmanın yapıldığı her bir merkezdeki sorumlu arařtırmacının yükümlülüğü altındadır.

c) Hâlihazırda CE işareti taşımayan cihazların klinik arařtırma amaçlı kullanılabilmesi için imalatçısı ya da yetkili temsilcisi tarafından Tıbbi Cihaz Yönetmeliğinin Ek I'inin III. Bölümünün 23.2 numaralı maddesine uygun bilgilerin arařtırma başvurularının bir parçası olarak sponsor aracılığıyla etik kurula ve Kuruma sunulması zorunludur.

ç) Hâlihazırda CE işareti taşımayan klinik arařtırma amaçlı cihazların ilgili arařtırmalarda kullanılması amacıyla ülkeye getirilebilmesi için sponsor tarafından Kurumdan izin alınır.

d) Sponsor, Tıbbi Cihaz Yönetmeliği Ek I'inin III. Bölümünün 23 numaralı maddesinde belirtilen bilgilerin cihazın beraberinde bulunmasını sağlar. Etiket üzerindeki detaylar; silinemez, kolayca okunabilir ve hedeflenen kullanıcı veya gönüllüler için açık bir şekilde anlaşılabilir olur.

e) Arařtırmanın güvenlik gerekçeleriyle geçici olarak durdurulması halinde, arařtırma merkezlerinde kalan arařtırma amaçlı cihazların tamamı, sponsor tarafından dağıtım yerlerinden derhal geri çekilir ve durum 15 gün içerisinde belgeleriyle birlikte ve bir rapor hâlinde sponsor tarafından Kurumun elektronik başvuru sistemi aracılığıyla Kuruma bildirilir. Arařtırma amaçlı cihazın geri çekilmesi ve geri çekilen ürünlerle ilgili yapılacak işlemler ve alınacak tedbirler Kuruma bildirilen raporda ayrıntılı olarak belirtilir.

Önemli olmayan deęişiklikler ve bildirimler

MADDE 16- (1) Tıbbi Cihaz Yönetmeliğinde sponsorun ve arařtırmacıların deęişiklik ve bildirim yükümlülükleri ile ilgili belirtilen hükümlerin yanında;

a) Sorumlu arařtırmacı, bařka kurumlardan uygun niteliklere haiz arařtırmacıları arařtırma ekibine dâhil edebilir. Bu arařtırmacıların görevlendirilmesine iliřkin bařvuru (b) bendinde belirtilen usul ile yapılır.

b) Arařtırmanın yürütülmesi sırasında, Kuruma sunulması gereken önemli olmayan deęiřiklikler ile bařvurularına iliřkin usûl ve esasları Kurum tarafından belirlenir. Kurum bu deęiřiklik bařvurularını, otuz iř günü ierisinde deęerlendirir.

c) Arařtırmaya ait ilerleme raporu yılda en az bir kere olmak üzere Kuruma bildirilir. Etik kurul ve Kurum gerekli gördüęü durumlarda veya kısa süreli arařtırmalarda daha kısa sürede de rapor talep edebilir.

) Bu fıkrada belirtilen Kuruma yapılacak deęiřiklik bařvuruları ve bildirimler sponsor tarafından Kurumun elektronik bařvuru sistemi aracılıęıyla yapılır.

(2) Deęiřikliklerin ve bildirimlerin etik kurula ve Kuruma düzenli olarak iletilmesinden sponsor sorumludur.

Görev devri ve paylařımı

MADDE 17- (1) Sponsor, yazılı sözleşme yapılmak kaydıyla kendi görevlerinin bir kısmını bilimsel esaslara ve iyi klinik uygulamalarına uygun şekilde alıřan sözleşmeli arařtırma kuruluşuna devredebilir. Görevlerin sözleşmeli arařtırma kuruluşuna devredilmesi, sponsorun devredilen hususlara dair muhtemel hukukî ve cezaî sorumluluęunu ortadan kaldırmaz. Sponsor ve sözleşmeli arařtırma kuruluşu, sözleşme konusu iřlerin ve iřlemlerin sonuçlarından birlikte sorumludurlar.

(2) Bu Yönetmelikte sponsora yapılan atıflar, geerli olan durumlarda Tıbbi Cihaz Yönetmelięinin 62 nci maddesinin ikinci fıkrası uyarınca sponsorun yasal temsilcisine veya görevleri ölçüsünde sözleşmeli arařtırma kuruluşuna da yapılmıř kabul edilir.

(3) Birinci fıkrada belirtilen yazılı sözleşmeler ile sponsor ve yasal temsilcisi arasında yapılan yazılı sözleşme arařtırma bařvurularının bir parası olarak etik kurul ve Kuruma sunulur.

(4) Kuruma yapılacak tüm bařvuru ve bildirimlerin yapılmasından;

a) Türkiye’de yerleřik olan sponsorlar için; sponsorun kendisi veya Türkiye’de yerleřik olan ve görev devri yapılmıř sözleşmeli arařtırma kuruluşu,

b) Türkiye’de yerleřik olmayan sponsorlar için; Tıbbi Cihaz Yönetmelięinin 62 nci maddesinin ikinci fıkrası uyarınca sponsorun yasal temsilcisi veya Türkiye’de yerleřik olan ve görev devri yapılmıř sözleşmeli arařtırma kuruluşu,

yetkili ve sorumludur.

Acil güvenlik tedbirleri

MADDE 18- (1) Sponsor veya arařtırmacılar, arařtırmanın yürütülmesi sırasında veya arařtırma amaçlı cihazın geliştirilmesiyle ilgili gönüllü güvenliğini etkileyebilecek yeni bir durumun ortaya çıkması hâlinde, bu tehlikelere karşı gönüllüleri koruyacak gerekli acil güvenlik tedbirlerini derhal alır. Sponsor, bu yeni durum ve alınan tedbirler hakkındaki bilgileri yedi gün içerisinde Kurumun elektronik başvuru sistemi aracılığıyla Kuruma bildirir.

Sorumluluk

MADDE 19- (1) Klinik arařtırmanın her türlü mali sorumluluđu sponsor ve mevcutsa yasal temsilcisi, görev devri yapılan sözleşmeli arařtırma kuruluşları ile arařtırma ekibine aittir.

(2) Arařtırmada kullanılan her türlü arařtırma ürününün, bu ürünlerin kullanılmasına mahsus her türlü malzeme ile muayene, tetkik, tahlil ve tedavilerin bedeli için gönüllüden herhangi bir ücret talep edilemez.

(3) Arařtırmalar kişisel verilerin gizliliğine riayet edilmesi kaydıyla kamuya açık bir veri tabanına kaydedilir.

BEŐİNCİ BÖLÜM

Çeřitli ve Son Hükümler

Klinik Arařtırmalar Danıřma Kurulu ve danıřma komisyonları

MADDE 20- (1) İlaç ve Biyolojik Ürünlerin Klinik Arařtırmaları Hakkında Yönetmelikte belirtilen ve Kurum nezdinde teşkil olunan Klinik Arařtırmalar Danıřma Kurulu, Kurumun talebi durumunda, bu Yönetmelik hükümlerine tabi tüm arařtırmalarda etik kurullarla ilgili Őikâyetleri ve arařtırmalarla ilgili olarak etik kurullarca veya arařtırmanın taraflarınca Kuruma iletilen ve uzmanlık görüşü gerektiren hususlarda görüş bildirir.

(2) Kurum, arařtırmaların incelenmesi ve deđerlendirilmesi sırasında ve yetkilerini kullanırken Tıbbi Cihaz Yönetmeliğinin 108 inci maddesi uyarınca Kurum bünyesinde teşkil edilen danıřma komisyonlarından görüş alabilir.

Klinik Arařtırma Etik Kurulları

MADDE 21- (1) Etik kurullar, piyasaya arz sonrası çalışmalar ile tıbbi cihaz klinik arařtırmalarını, bu Yönetmelik hükümleri ile birlikte İlaç ve Biyolojik Ürünlerin Klinik Arařtırmaları Hakkında

Yönetmeliğinin 28 inci maddesinde belirtilen hususlar ile iyi klinik uygulamaları doğrultusunda değerlendirir, izler ve takip eder.

(2) Etik kurullar bu Yönetmelik kapsamındaki araştırmaları İlaç ve Biyolojik Ürünlerin Klinik Araştırmaları Hakkında Yönetmeliğinde belirlenen inceleme süreleri içerisinde değerlendirir. Etik kurulun inceleme süreci içerisinde ek bilgi ve açıklamalara ihtiyaç duyulması hâlinde, gerekli olan tüm istekler tek bir seferde başvuru sahibine iletilir. İstenilen bilgi ve belgeler etik kurula sunuluncaya kadar inceleme süreci durdurulur.

(3) Tıbbi Cihaz Yönetmeliğinin Ek XV'inin III. Bölümünün 4 numaralı maddesi uyarınca sponsor tarafından atanacak monitörün yetkinliği ile araştırma merkezinden bağımsız olması hususlarının incelenmesi araştırmayı değerlendiren etik kurul tarafından yapılır.

(4) Bu Yönetmeliğin aşağıdaki maddelerinde belirtilen başvuruların Kuruma başvuru yapılmadan önce etik kurula sunulması gerekmektedir. Bu başvurulara ilişkin etik kurul kararları, Kuruma yapılacak başvurular ile birlikte Kuruma sunulur:

- a) 7 nci maddede belirtilen klinik araştırma başvurusu,
- b) 11 inci maddede belirtilen önemli değişiklik başvuruları.

(5) Bu Yönetmeliğin aşağıda belirtilen başvuru ve bildirimlerin Kurum ile birlikte etik kurula paralel olarak sunulması gerekmektedir. Kurum değerlendirme sürecinde bu başvuru ve bildirimlere ilişkin etik kurul kararını talep edebilir:

- a) 13 üncü maddede belirtilen klinik araştırmanın sona ermesi, geçici olarak durdurulması ve erken sonlandırılmasına ilişkin bildirimler,
- b) 14 üncü maddede belirtilen advers olay bildirimleri,
- c) 15 inci maddenin birinci fıkrasının (e) bendinde belirtilen araştırma amaçlı cihazların geri çekilmesine ilişkin bildirim,
- ç) 16 ncı maddenin birinci fıkrasının (b) bendinde belirtilen önemli olmayan değişiklik başvuruları,
- d) 16 ncı maddenin birinci fıkrasının (c) bendinde belirtilen ilerleme raporu bildirimleri,
- e) 18 inci maddenin birinci fıkrasında belirtilen acil güvenlik tedbirleri.

Denetim

MADDE 22- (1) Kurum; yurt içinde veya yurt dışında yürütülen araştırmaları, araştırmacıları, araştırmaların yapıldığı yerleri, sponsorları, yasal temsilcileri ve sözleşmeli araştırma kuruluşlarını,

arařtırma amaçlı cihazların imal edildiđi yerleri, arařtırma ile ilgili analizlerin yapıldıđı laboratuvarları, etik kurulları ve arařtırma kapsamındaki diđer tüm tarafları bu Yönetmelik ve ilgili diđer mevzuat hükümlerine uygunluđu yönünden, önceden haber vererek veya haber vermeden denetleyebilir.

Aykırı davranıřlar hakkında uygulanacak hükümler ve cezalar

MADDE 23- (1) Bu Yönetmelikte belirtilen hükümlere aykırı davranan ve faaliyette bulunanlar hakkında fiillerinin niteliđine göre 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu ve ilgili diđer mevzuat hükümleri uygulanır.

Hüküm bulunmayan haller

MADDE 24- (1) Bu Yönetmelikte hüküm bulunmayan hallerde Tıbbi Cihaz Yönetmeliđi ve arařtırmaya iřtirak eden gönüllülerin hakları ile ilgili olarak 1/8/1998 tarihli ve 23420 sayılı Resmî Gazete'de yayımlanan Hasta Hakları Yönetmeliđinde belirtilen hükümler ile diđer ilgili mevzuat hükümleri uygulanır.

Yürürlükten kaldırılan yönetmelik

MADDE 25- (1) 6/9/2014 tarihli ve 29111 sayılı Resmî Gazete'de yayımlanan Tıbbi Cihaz Klinik Arařtırmaları Yönetmeliđi yürürlükten kaldırılmıřtır.

Yürürlük

MADDE 26- (1) Bu Yönetmelik yayımı tarihinde yürürlüđe girer.

Yürütme

MADDE 27- (1) Bu Yönetmelik hükümlerini Türkiye İlaç ve Tıbbi Cihaz Kurumu Bařkanı yürütür.

**Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti
Hakkında Yönetmelik**

Resmî Gazete Tarihi : 01.06.2005

Resmî Gazete Sayısı : 25832

**CEZA MUHAKEMESİNDE BEDEN MUAYENESİ, GENETİK İNCELEMELER VE FİZİK
KİMLİĞİN TESPİTİ HAKKINDA YÖNETMELİK**

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç ve kapsam

Madde 1 - Bu Yönetmelik; bir suça ilişkin iz, eser, emare ve delillerin elde edilmesi; ayrıca, maddî gerçeğin ortaya çıkartılması bakımından şüpheli, sanık, mağdur ve diğer kişilerin beden muayenelerinin yapılması, tıbbî incelemelerde bulunmak üzere vücuttan, kan veya benzeri biyolojik örneklerle, saç, tükürük, tırnak gibi örneklerin alınması, moleküler genetik incelemeler ile şüpheli ve sanığın kimliğinin teşhisi için gerekli fizikî özelliklerin tespitine ilişkin usul ve esasları düzenlemektir.

Dayanak

Madde 2 - Bu Yönetmelik, 04/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun 82 nci maddesine dayanılarak hazırlanmıştır.

Tanımlar

Madde 3 - Bu Yönetmelikte geçen;

Şüpheli: Soruşturma evresinde suç şüphesi altında bulunan kişiyi,

Sanık: Kovuşturmanın başlamasından itibaren hükmün kesinleşmesine kadar suç şüphesi altında bulunan kişiyi,

Mağdur: Suçtan veya haksız eylemden zarar gören kişiyi,

Soruşturma: Ceza Muhakemesi Kanununa göre yetkili mercilerce suç şüphesinin öğrenilmesinden iddianamenin kabulüne kadar geçen evreyi,

Kovuşturma: İddianamenin kabulü ile başlayıp hükmün kesinleşmesine kadar geçen evreyi,

Gecikmesinde sakınca bulunan hâl: Derhâl işlem yapılmadığı takdirde suçun iz, eser, emare ve delillerinin kaybolması veya şüphelinin kaçması veya kimliğinin saptanamaması ihtimalinin ortaya çıkması hâlini,

Sağlık mesleği mensubu: Tabip, dış tabibi, eczacı, ebe, hemşire ve sağlık hizmeti veren diğer kişileri,

Bedenin tıbbî muayenesi: Tabip tarafından tıbbî yöntemler kullanılarak yapılan değerlendirmeleri,

Dış beden muayenesi: Vücudun dış yüzeyi ile kulak, burun ve ağız bölgelerinin gözle ve elle yapılan yüzeysel tıbbî incelemesini,

İç beden muayenesi: Kafa, göğüs ve karın boşlukları ile cilt altı dokularının incelenmesini,

Beden parçası: Bir bedenın tamamlayıcı unsuru olan baş, gövde, kol, el, bacak, ayak gibi uzuv ve iç organları,

Müdahale: Tabip veya diğer sağlık personeli tarafından tanı, tedavi, rehabilitasyon veya önlem amacıyla yapılan muayene, tedavi veya diğer tıbbî işlemleri,

Cerrahî müdahale: Tıbbî aletler yardımıyla vücutta yapılan tanı ya da tedaviye yönelik operasyonları,

Örnek: Bir suça ilişkin delil elde etmek amacıyla, inceleme yapmak üzere ilgililerden alınan biyolojik ve diğer materyali,

Moleküler genetik inceleme: Gereken tür ve miktardaki biyolojik materyali kullanarak, kişiyi diğer kişilerden ayıran ve kalıtım kurallarına uygun olarak aktarılan hastalık dışındaki özelliklerinin moleküler düzeyde araştırılmasını

ifade eder.

İKİNCİ BÖLÜM

Beden Muayenesi ve Vücuttan Örnek Alınması

Şüpheli veya sanığın iç beden muayenesi

Madde 4 - Bir suça ilişkin delil elde etmek için, şüpheli veya sanık üzerinde iç beden muayenesi yapılabilmesine Cumhuriyet savcısı veya mağdurun istemiyle ya da re•fsen hâkim veya mahkeme, gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından karar verilebilir. Cumhuriyet savcısının kararı, yirmidört saat içinde hâkim veya mahkeme onayına sunulur. Hâkim veya mahkeme, yirmidört saat içinde kararını verir. Onaylanmayan kararlar hükümsüz kalır ve elde edilen deliller kullanılamaz.

Şüpheli veya sanığın iç beden muayenesi ancak tabip tarafından yapılır.

Muayenenin yapılabilmesi için; müdahalenin, kişinin sağlığına açıkça ve öngörülebilir zarar verme tehlikesinin bulunmaması gerekir.

Cinsel organlar veya anüs bölgesinde yapılan muayene de iç beden muayenesi sayılır.

Üst sınırı iki yıldan daha az hapis cezasını gerektiren suçlarda kişi üzerinde iç beden muayenesi yapılamaz.

Şüpheli veya sanığın dış beden muayenesi

Madde 5 - Bir suçla ilişkin delil elde etmek için, şüpheli veya sanık üzerinde dış beden muayenesi Cumhuriyet savcısı ile, emrindeki adli kolluk görevlileri veya kovuşturma makamlarının talebiyle yapılabilir.

Şüpheli veya sanığın dış beden muayenesi ancak tabip tarafından yapılır.

Muayenenin yapılabilmesi için; müdahalenin, kişinin sağlığına açıkça ve öngörülebilir zarar verme tehlikesinin bulunmaması gerekir.

Girişimsel olmayan tıbbî görüntüleme yöntemleri de bedeninin dış muayenesi sayılır. Bu tür incelemeler tabip tarafından veya tabip gözetiminde sağlık mesleği mensubu diğer bir kişi tarafından yapılabilir.

Şüpheli veya sanığın vücudundan örnek alınması

Madde 6 - Bir suçla ilişkin delil elde etmek için, şüpheli veya sanığın vücudundan kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak, gibi örnekler alınabilmesine, Cumhuriyet savcısı veya mağdurun istemiyle ya da re•fsen hâkim veya mahkeme, gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından karar verilebilir. Cumhuriyet savcısının kararı, yirmidört saat içinde hâkim veya mahkeme onayına sunulur. Hâkim veya mahkeme, yirmidört saat içinde kararını verir. Onaylanmayan kararlar hükümsüz kalır ve elde edilen deliller kullanılamaz. Bu örnekler Cumhuriyet savcısının huzurunda ve uygun göreceği usullerle derhâl yok edilerek bu husus tutanağa geçirilir.

Bu müdahaleler ancak tabip tarafından veya tabip gözetiminde sağlık mesleği mensubu diğer bir kişi tarafından yapılabilir.

Vücuttan örnekler alınabilmesi için; müdahalenin, kişinin sağlığına açıkça ve öngörülebilir zarar verme tehlikesinin bulunmaması gerekir.

Tıbbî müdahaleler, hekimlik sanatının ve tıp biliminin kabul ettiği yöntem ve araçlarla yapılır.

Üst sınırı iki yıldan daha az hapis cezasını gerektiren suçlarda; kişiden kan, saç, tükürük, tırnak gibi örnekler alınmaz.

Özel kanunlardaki alkol muayenesine ve kan örneği alınmasına ilişkin hükümler saklıdır.

Diğer kişilerin beden muayenesi

Madde 7 - Bir suçla ilişkin delil elde etmek amacıyla, mağdurun ve diğer kişilerin vücudu üzerinde dış veya iç beden muayenesi yapılabilmesine sağlığını açıkça ve öngörülebilir şekilde tehlikeye düşürmemek ve cerrahî bir müdahalede bulunmamak koşuluyla; Cumhuriyet savcısının istemiyle ya da re•fsen hâkim veya mahkemece, gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından karar verilebilir. Cumhuriyet savcısının kararı, yirmidört saat içinde hâkim veya mahkemenin onayına sunulur. Hâkim veya mahkeme, yirmidört saat içinde kararını verir. Onaylanmayan kararlar hükümsüz kalır ve elde edilen deliller kullanılamaz.

Mağdurun ve diğer kişilerin beden muayenesi ancak tabip tarafından yapılır.

Diğer kişilerin vücudundan örnek alınması

Madde 8 - Bir suçla ilişkin delil elde etmek amacıyla, mağdurun ve diğer kişilerin vücudundan kan, veya benzeri biyolojik örneklerle saç, tükürük, tırnak gibi örnekler alınabilmesine, sağlığını açıkça ve öngörülebilir şekilde tehlikeye düşürmemek ve cerrahî bir müdahalede bulunmamak koşuluyla; Cumhuriyet savcısının istemiyle ya da re•fsen hâkim veya mahkeme, gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından karar verilebilir. Cumhuriyet savcısının kararı yirmidört saat içinde hâkim veya mahkemenin onayına sunulur. Hâkim veya mahkeme yirmidört saat içinde kararını verir. Onaylanmayan kararlar hükümsüz kalır ve elde edilen deliller kullanılamaz.

Bu müdahaleler ancak tabip tarafından veya tabip gözetiminde sağlık mesleği mensubu diğer bir kişi tarafından yapılabilir.

Tıbbî müdahaleler, hekimlik sanatının ve tıp biliminin kabul ettiği yöntem ve araçlarla yapılır.

Soy bağının araştırılması

Madde 9 - Çocuğun soy bağının araştırılmasına gerek duyulması hâlinde, bu araştırmanın yapılabilmesi için, bu Yönetmeliğin 7 ve 8 nci maddeleri hükümlerine göre karar alınması gereklidir.

Tanıklıktan çekinme sebeplerinin varlığı

Madde 10 - Tanıklıktan çekinme sebepleri ile muayeneden veya vücuttan örnek alınmasından kaçınılabilir.

Tanıklıktan çekinme sebeplerinin belirlenmesi hususunda Ceza Muhakemesi Kanununun ilgili hükümleri uygulanır.

Çocuk ve akıl hastasının çekinmesi konusunda kanunî temsilcisi karar verir. Çocuk veya akıl hastasının, tanıklığın hukukî anlam ve sonuçlarını algılayabilecek durumda olması hâlinde, görüşü de alınır.

Kanunî temsilci de şüpheli veya sanık ise bu konuda hâkim tarafından karar verilir. Ancak, bu hâlde elde edilen deliller davanın ileri aşamalarında şüpheli veya sanık olmayan kanunî temsilcinin izni olmadıkça kullanılamaz.

Kadının muayenesi

Madde 11 - Kadının muayenesi, istemi hâlinde ve olanaklar elverdiğinde bir kadın tabip tarafından yapılır.

Muayene edilecek kadının talebine rağmen bir kadın tabibin bulunmasına olanakların elvermediği durumlarda; muayene sırasında tabip ile birlikte bir başka kadın sağlık mesleği personelinin bulundurulmasına özen gösterilir.

ÜÇÜNCÜ BÖLÜM

Moleküler Genetik İncelemelerin Yapılması

Moleküler genetik incelemeler

Madde 12 - Bu Yönetmelikte öngörülen işlemlerle elde edilen örnekler üzerinde, soy bağının veya elde edilen bulgunun şüpheli veya sanığa ya da mağdura ait olup olmadığının tespiti için zorunlu olması hâlinde moleküler genetik incelemeler yapılabilir. Alınan örnekler üzerinde bu amaçlar dışında tespitler yapılmasına yönelik incelemeler yasaktır.

Birinci fıkra uyarınca yapılabilen incelemeler, bulunan ve kime ait olduğu belli olmayan beden parçaları üzerinde de yapılabilir. Birinci fıkranın ikinci cümlesi, bu hâlde de uygulanır.

Bilirkişi incelemesi

Madde 13 - Bu Yönetmeliğin 12 inci maddesi hükümleri uyarınca moleküler genetik incelemeler yapılmasına sadece hâkim karar verebilir. Kararda inceleme ile görevlendirilen bilirkişi de gösterilir.

Bilirkişi gerçek ya da tüzel kişi olabilir.

Yapılacak incelemeler için resmen atanan veya bilirkişilikle yükümlü olan ya da soruşturma veya kovuşturmayı yürüten makama mensup olmayan veya bu makamın soruşturma veya kovuşturmayı

yürüten dairesinden teşkilât yapısı itibarıyla ve objektif olarak ayrı bir birimine mensup olan görevliler, bilirkişi olarak görevlendirilebilirler. Bu kişiler, teknik ve teşkilât bakımından uygun tedbirlerle yasak moleküler genetik incelemelerin yapılmasını ve yetkisiz üçüncü kişilerin bilgi edinmesini önlemekle yükümlüdürler. İncelenecek bulgu, bilirkişiye ilgilinin adı ve soyadı, adresi, doğum tarihi bildirilmeksizin verilir.

Bilirkişiye gönderilen örneklerle ilgili olarak; hâkimlikler, mahkemeler ve Cumhuriyet başsavcılıkları gizliliği sağlamak ve karışıklığa yer vermemek için gerekli her türlü tedbiri alırlar. Bu amaçla güvenli ve gizli bir kayıt sistemi belirlenir. Bu kayıt sisteminde bedeninden örnek alınan kişinin adı, soyadı, adresi ve doğum tarihine karşılık gelmek üzere bir kod sistemi uygulanır.

Üçüncü fıkranın uygulanması açısından, teşkilât yapısı itibarıyla üniversiteler, Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Adli Tıp Kurumu objektif olarak ayrı birimler sayılırlar.

Moleküler genetik inceleme sonuçlarının gizliliği

Madde 14 - Bu Yönetmelik hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez.

Bu bilgiler, kovuşturmayla yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde Cumhuriyet savcısının huzurunda ve uygun göreceği usullerle yok edilir ve bu husus dosyasında muhafaza edilmek üzere tutanağa geçirilir. Olay yerinden elde edilen diğer delillere ilişkin hükümler saklıdır.

Bilirkişi tarafından yapılan analizler sonucu elde edilen bulgular ilgili makama gönderilir; bulgular üzerinden moleküler genetik analizler için izole edilen DNA örnekleri bilirkişi tarafından rapor hazırlandıktan sonra imha edilir ve bu husus raporda açıkça belirtilir.

Moleküler genetik incelemelerin özel kalıtsal karakterler hakkındaki açıklamayı içermediği bilinen kromozom bölgesi ile sınırlı kalmasına özen gösterilir.

DÖRDÜNCÜ BÖLÜM

Fizik Kimliğin Tespitinde Uyulacak Esaslar

Fizik kimliğin tespiti

Madde 15 - Üst sınırı iki yıl veya daha fazla hapis cezasını gerektiren bir suçtan dolayı şüpheli veya sanığın, kimliğinin tespiti için gerekli olması hâlinde, Cumhuriyet savcısının emriyle, fotoğrafı, iris görüntüsü, beden ölçüleri, diş izi, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini

kolaylaştıracak eşkâl bilgileri, kulak, dudak gibi organların bıraktığı kimlik tespitine yarayabilecek vücut izleri ile sesi ve görüntüleri, fizik kimliğin tespitinde kullanılan diğer teknik yöntemler ile kayda alınarak, soruşturma ve kovuşturma işlemlerine ilişkin dosyaya konulur.

Fizik kimliğin tespitinde, öncelikli olarak elin iç yüzeyindeki derinin özel kıvrımlı şekilleri olan parmak ve avuç içi izleri, fotoğrafı ve eşkâl bilgileri kullanılır. Bu işlemler olay yeri inceleme ve kimlik tespit konusunda özel eğitim almış uzman kolluk mensubu tarafından yapılır.

Fizik kimliğin tespiti açısından, kişinin ağzındaki dişlerin incelenmesi ve diş izlerinin alınması diş tabibi tarafından yapılır.

Soruşturma veya kovuşturma aşamasında da hâkim veya mahkeme kararıyla fizik kimliğinin tespitine ilişkin işlemler yaptırılabilir.

Verilerin imhası

Madde 16 - Kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde bu Yönetmeliğin 15 inci maddesi hükümleri uyarınca elde edilen veriler, Cumhuriyet savcısının huzurunda ve uygun göreceği usullerle derhâl yok edilir ve bu husus tutanağa geçirilir.

Verilerin korunması

Madde 17 - Mahkûmiyet kararı verilmesi hâlinde bu Yönetmeliğin 15 inci maddesinin birinci ve ikinci fıkraları uyarınca elde edilen veriler kolluk tarafından, üçüncü fıkrasında belirtilen diş izleri ise bu işlemi yapan sağlık kuruluşu tarafından arşivlenir.

BEŞİNCİ BÖLÜM

Çeşitli ve Son Hükümler

İlgilinin rızası

Madde 18 - Mevzuatta aranan tüm koşulların gerçekleşmiş olmasına ve şüpheli sanık veya diğer kişilerin bu konuda aydınlatılmış olmalarına rağmen muayene yapılmasına ya da örnek alınmasına rıza vermemeleri hâlinde, kararın infazı için ilgilinin muayenesini veya vücudundan örnek alınmasını sağlamak üzere ilgili Cumhuriyet başsavcılığınca gerekli önlemler alınır.

Mağdurun rızasının varlığı hâlinde bu işlemlerin yapılabilmesi için Yönetmeliğin 7 nci ve 8 inci maddeleri uyarınca karar alınmasına gerek yoktur.

Bir suçun aydınlatılmasını sağlamak amacıyla, şüpheli, sanık ve diğer kişilerin kendiliğinden başvurarak rıza göstermeleri hâlinde, soruşturma evresinde Cumhuriyet savcısının istemi, kovuşturma aşamasında ise hâkim veya mahkeme kararıyla tıbbî muayeneleri yapılabilir ya da vücutlarından örnek alınabilir.

Tedavi amaçlı müdahaleler

Madde 19 - Sağlık mevzuatı ve taraf olunan uluslararası sözleşmeler uyarınca tabip tarafından yapılması gereken tedavi amaçlı tıbbî muayene ve müdahaleler için Cumhuriyet savcısı ya da hâkim kararı aranmaz.

Raporların düzenlenmesi

Madde 20 - Tabip raporları üç nüsha hâlinde düzenlenir. Raporu düzenleyen sağlık kuruluşunca iki nüshası kapalı ve mühürlü zarf içerisinde ilgili Cumhuriyet başsavcılığına, hâkimliğe veya mahkemeye en seri şekilde iletilir. Raporun bir nüshası raporu düzenleyen sağlık kuruluşunda kalır.

Güvenlik önlemleri

Madde 21 - Muayene edilmesi veya vücudundan örnek alınması amacıyla sevk edilen kişi dışında başka bir kişinin muayene edilmemesi ya da vücudundan örnek alınmaması için Cumhuriyet başsavcılıklarınca gerekli önlemler alınır.

Tabip veya diğer sağlık mesleği mensuplarınca, sevk edilen kişinin kimliği konusunda şüpheye düşülmesi hâlinde durum derhâl Cumhuriyet başsavcılığına bildirilir.

Alınan, muhafaza edilen, nakledilen ve incelenen örneklerin değiştirilmemesi ve dış koşullardan etkilenip bozulmaması için Cumhuriyet başsavcılığı, kolluk, sağlık kuruluşu ve bilirkişi tarafından gerekli tedbirlere başvurulur.

Verilerle ilgili işlemler

Madde 22 - Cumhuriyet başsavcılıklarınca yapılan iş bölümlerinde, bu Yönetmelik kapsamında elde edilen verilerin imha edilmesi ve diğer işlemlerin yürütülmesi amacıyla yeterli sayıda Cumhuriyet savcısı görevlendirilir.

Kovuşturma sonunda verilen beraat ve mahkûmiyet kararları, bu Yönetmelik hükümlerince öngörülen işlemlerin yerine getirilmesi için mahkemece ilgili Cumhuriyet başsavcılığına gönderilir.

Diğer işlemler

Madde 23 - Kişinin vücut yüzeyinde bulunan atış artığı gibi biyolojik olmayan örnekler, elbiseleri ve diğer eşyaları üzerinde bulunan örnekler ile vücut yüzeyinden başkasına ait olduğu açıkça belli olan kıl, tüy, lif gibi örnekler olay yeri inceleme uzmanları tarafından alınabilir.

İtiraz

Madde 24 - Bu Yönetmeliğin 4, 5, 6, 7, 8, 9 ve 10 uncu maddeleri gereğince alınacak hâkim veya mahkeme kararlarına itiraz edilebilir.

İtiraz hâlinde Ceza Muhakemesi Kanununun ilgili hükümleri uygulanır.

Yürürlük

Madde 25 - Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

Madde 26 - Bu Yönetmelik hükümlerini Adalet Bakanı yürütür.

6713 Sayılı Kolluk Gözetim Komisyonu Kurulması Hakkında Kanunun Uygulanmasına Dair

Yönetmelik

Resmî Gazete Tarihi : 07.08.2019

Resmî Gazete Sayısı : 30855

6713 SAYILI KOLLUK GÖZETİM KOMİSYONU KURULMASI HAKKINDA KANUNUN UYGULANMASINA DAİR YÖNETMELİK

BİRİNCİ KISIM

Genel Hükümler

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç ve kapsam

MADDE 1- (1) Bu Yönetmeliğin amacı; kolluk şikâyet sisteminin daha etkili ve hızlı işlemlerini sağlamak, saydamlığını ve güvenilirliğini geliştirmek üzere kolluk görevlilerinin işledikleri iddia edilen suçlardan veya disiplin cezasını gerektiren eylem, tutum veya davranışlarından dolayı idari merciler tarafından yapılan ya da yapılması gereken iş ve işlemler ile kolluk görevlileri hakkındaki memnuniyet bildirimlerinin merkezi bir sistemde kayıt altına alınması ve izlenmesi amacıyla kurulan Komisyonun sekretarya hizmetlerinin yürütülmesi ve merkezi kayıt sisteminin işleyişi, Kanunun 4 üncü ve 8 inci maddelerinde verilen görevleri yürütmek üzere Kurul Başkanlığınca tahsis edilecek müfettişlerin belirlenmesi, görevlendirilme yöntemi ve hizmet içi eğitimleri ile ilgili usul ve esasları belirlemektir.

(2) Bu Yönetmelik; Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı teşkilâtında görevli kolluk personelinin işlediği iddia edilen suçlarla veya disiplin cezasını gerektiren eylem, tutum veya davranışlarıyla ilgili olarak idari merciler tarafından yapılan ya da yapılması gereken iş ve işlemleri kapsar.

Dayanak

MADDE 2- (1) Bu Yönetmelik, 3/5/2016 tarihli ve 6713 sayılı Kolluk Gözetim Komisyonu Kurulması Hakkında Kanuna dayanılarak hazırlanmıştır.

Tanımlar

MADDE 3- (1) Bu Yönetmelikte geçen;

- a) Araştırma: İhbar ve şikâyetlerin soyut ve genel nitelikte olup olmadığı, ilgili olduğu kişi veya olayların belirtilip belirtilmediği, iddiaların ciddî bulgu ve belgelere dayanıp dayanmadığı, dilekçe sahibinin adı, soyadı ve imzası ile iş veya yerleşim yeri adresinin ve Türkiye Cumhuriyeti vatandaşı ise Türkiye Cumhuriyeti kimlik numarasının, yabancı uyruklu ise varsa pasaport numarası ve yabancı kimlik numarası veya diğer tanıtıcı bilgilerin doğru olarak bildirilip bildirilmediği; dilekçe sahibinin adı, soyadı, imzası ile iş veya yerleşim yeri adresinin ve Türkiye Cumhuriyeti kimlik numarası belirtilmediği veya bunların doğru olmadığı hallerde iddiaların sıhhatinin şüpheye mahal vermeyecek belgelerle ortaya konulup konulmadığı hususlarını tespit etmek amacıyla yapılan çalışmaları,
- b) Bağlı kuruluşlar: Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığını,
- c) Bağlı kuruluşların en üst amiri: İlgisine göre Emniyet Genel Müdürünü, Jandarma Genel Komutanını ve Sahil Güvenlik Komutanını,
- ç) Bakan: İçişleri Bakanını,
- d) Bakan Yardımcısı: Kolluk Gözetim Komisyonu Başkanlığı görevi uhdesine verilen Bakan Yardımcısını,
- e) Bakanlık: İçişleri Bakanlığını,
- f) Başkan: Kolluk Gözetim Komisyonu Başkanını,
- g) Denetim: Kolluk şikâyet sisteminin işleyişi ile ilgili olarak mülki makamlar ve kolluk kuruluşlarınca yapılan iş ve işlemlerin kalitesini, verimini ve etkinliğini, hukuka uygunluğunu tespit etmek, sistemin işleyişinde hizmet standartlarının iyileştirilmesini sağlamak, bu kapsamda amirleri işbaşında değerlendirmek amacıyla haberli veya habersiz olarak yapılan faaliyetleri,
- ğ) Disiplin soruşturması: Kolluk görevlilerinin disiplin hukukundan doğan sorumluluklarının saptanması amacıyla disiplin amirleri tarafından yapılan veya yaptırılan araştırma ve inceleme faaliyetini,
- h) Elektronik imza: Herhangi bir elektronik veriye eklenen ve bu veri ile mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan bir elektronik veriyi,

- i) Hukuka aykırı eylem: Kolluk görevlilerinin; Anayasa ve kanunlar ile yönetmelik, tebliğ, genelge ve diğer düzenleyici metinlerle belirlenmiş kurallara ya da amirlerince usulünce verilmiş yazılı ve sözlü emirlere aykırı olan ve ceza, disiplin ve/veya tazmin hukuku bakımından sorumluk gerektiren icrai veya ihmali eylemleri,
- i) İhbar: Kolluk görevlilerinin hukuka aykırı eylem, tutum veya davranışlarının, herhangi bir kişi tarafından yetkili mercilere bildirilmesini,
- j) İhbarcı: İhbar yapan gerçek ve tüzel kişileri,
- k) İnceleme ve araştırma: Kolluk şikâyet sisteminin işleyişine dair ilke ve hizmet standartlarının tespit edilmesi, kolluk şikâyet sistemi ile merkezi kayıt sisteminin etkin bir şekilde işlemesi ve geliştirilmesi, kolluk görevlilerinin çalışma koşullarının iyileştirilmesi, kolluk hizmetlerinin geliştirilmesi ve iyileştirilmesi, kolluk etik ilkelerinin etkin bir şekilde uygulanması, kolluk şikâyet sistemine kamuoyunun duyduğu güvenin ölçülmesini ve halkın sisteme ilişkin görüş ve düşüncelerinin değerlendirilmesi, kolluğun hizmet içi eğitim programlarıyla ilgili önerilerde bulunulması, görev alanına giren konularla ilgili mevzuat düzenlemeleri konularında Komisyonun görüşmelerine esas olmak üzere yapılan çalışmaları,
- l) Kanun: 3/5/2016 tarihli ve 6713 sayılı Kolluk Gözetim Komisyonu Kurulması Hakkında Kanunu,
- m) Katalog suçlar: 6713 sayılı Kanununun 8 inci maddesinde belirtilen kolluk görevlilerince işlendiği iddia edilen veya doğrudan öğrenilen; öldürme, kasten yaralama, işkence, zor kullanma yetkisine ilişkin sınırın aşılması ve suç işlemek amacıyla örgüt kurma suçları ile örgüt faaliyeti çerçevesinde işlenen suçları,
- n) Kolluk: Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı teşkilâtında, emniyet ve asayiş ile kamu düzeninin korunmasını sağlamak için kanunların ve kanunlara dayanarak yetkili makamların verdiği görevleri yerine getiren personel ve görevlileri,
- o) Kolluk şikâyet sistemi: Kolluk görevlilerinin işledikleri iddia edilen suçlardan veya disiplin cezasını gerektiren eylem, tutum veya davranışlarından dolayı idari merciler tarafından yapılan iş ve işlemler ile uygulamaların bütünü,
- ö) Komisyon: Kolluk Gözetim Komisyonunu,
- p) Kurul: İçişleri Bakanlığı Mülkiye Teftiş Kurulunu,

- r) Kurul Başkan Yardımcısı: Komisyonun sekretarya hizmetlerinin sevk ve idaresinde Kurul Başkanına yardımcı olmak üzere Kurul Başkanının önerisi ve Başkanın teklifi üzerine Bakan onayı ile görevlendirilen en az beş yıllık mesleki kıdeme sahip mülkiye başmüfettişini,
- s) Kurul Başkanı: İçişleri Bakanlığı Mülkiye Teftiş Kurulu Başkanını,
- ş) Memnuniyet bildirim: Kişilerin kolluk görevlilerinin hizmet ve faaliyetleri ile tutum ve davranışlarına ilişkin beğeni ve takdirlerini beyan etmelerini,
- t) Merkezi kayıt sistemi: Kolluk Gözetim Komisyonu ile bağlı kuruluşlar, valilikler ve kaymakamlıklar arasında, kolluk görevlileri hakkında idari mercilerce yürütülen ceza ve disiplin işlemleriyle ilgili olarak gerekli bilgilerin elektronik ortamda kaydedilmesi ve yapılan uygulamaların izlenmesi amacıyla oluşturulan veri tabanını,
- u) Muhakkik: Araştırma, ön inceleme, disiplin soruşturması, inceleme ve soruşturma yapmakla görevlendirilen, mülki idare amiri hizmetleri sınıfı ve/veya soruşturma yapılan kolluk görevlisinin ilgisine göre emniyet hizmetleri, jandarma hizmetleri ve sahil güvenlik hizmetleri sınıfından üstü konumunda olan denetim elemanı haricindeki görevlilerini,
- ü) Müfettiş: Mülkiye başmüfettişi ve mülkiye müfettişini,
- v) Müfettişler grubu: Kanunun 4 üncü ve 8 inci maddeleri hükümleri çerçevesinde verilecek görevleri yürütmek üzere, en az üç yıl mesleki kıdeme sahip mülkiye müfettişleri arasından, Kurul Başkanının önerisi ve Bakanın onayı ile belirlenen müfettişler grubunu,
- y) Mülki idare amirlikleri: Valilik ve kaymakamlıkları,
- z) Ön inceleme: 2/12/1999 tarihli ve 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun gereğince, kolluk görevlilerinin aynı Kanun kapsamındaki suçlar bakımından sorumluluklarının saptanmasına yönelik olarak; soruşturma izni vermeye yetkili merci, mülkiye müfettişi veya bağlı kuruluşların müfettişleri, mülki idare amirliği hizmetleri sınıfındaki görevliler ya da kolluk görevlilerinin diğer üstleri tarafından 4483 sayılı Kanun ve 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununa göre yapılan işlemleri,
- aa) Sekretarya: Kolluk Gözetim Komisyonu sekretaryasını,
- bb) Soruşturma: 19/4/1990 tarihli ve 3628 sayılı Mal Bildiriminde Bulunulması, Rüşvet ve Yolsuzluklarla Mücadele Kanununun 19 uncu maddesinin ikinci fıkrası uyarınca kolluk görevlilerinin aynı Kanun kapsamındaki suçlar bakımından sorumluluklarının saptanmasına yönelik olarak müfettiş ve muhakkiklerce yapılan işlem ve faaliyetleri,

cc) Şikâyet: Kolluk görevlilerinin hukuka aykırı eylem, tutum veya davranışlarının, bunlardan zarar gören veya mağdur olanlar ya da bunların avukatı ya da kanunî temsilcileri veya ikinci derece dâhil, ikinci dereceye kadar kan ve kayın hısımları tarafından, yetkili mercilere bildirilmesini,

çç) Şikâyetçi: Şikâyet başvurusu yapan gerçek ve tüzel kişileri veya bunların kanuni temsilci ya da vekillerini,

dd) Teftiş: Komisyonun önerisi üzerine Bakanın onayıyla; kayıt ve belgeler üzerinde yapılan kolluk şikâyet sisteminin işleyişiyle ilgili konularda mülki makamlar ve kolluk kuruluşlarınca yapılan iş ve işlemlerin, hukuka ve usule uygun olup olmadığının tespit edilmesi ile bu konularla ilgili faaliyetlerin daha etkili, verimli ve ekonomik olarak yürütülmesine yönelik çalışmaları,

ee) Taşra teşkilatı: Bağlı kuruluşların, doğrudan merkeze bağlı olanlar hariç olmak üzere, il, ilçe ve bölge teşkilatlarını,

ifade eder.

İKİNCİ BÖLÜM

Genel Esaslar

Temel ilkeler

MADDE 4- (1) Kolluk şikâyet sistemine ilişkin olarak yürütülen bütün iş ve işlemler uzmanlaşma, şeffaflık, hesap verebilirlik, zamanlılık, katılımcılık ile bağımsızlık ve tarafsızlık ilkelerine uygun olarak yerine getirilir.

(2) Bu ilkeler aşağıdaki esasları içerir:

a) Uzmanlaşma ilkesi: Kolluk görevlileri hakkındaki ön inceleme/disiplin soruşturmalarının uzmanlaşmış personel tarafından yerine getirilmesi, bunu teminen ilgili personelin düzenli olarak hizmet içi eğitime tabi tutulmasıdır.

b) Şeffaflık ilkesi: Soruşturmanın güvenliğine hanel getirilmemesi şartı ile kolluk görevlileri hakkında ihbar ve şikâyetlere ilişkin yürütülen idari soruşturmaların safahatı hakkında tarafların düzenli olarak bilgilendirilmesidir.

c) Hesap verebilirlik ilkesi: Kolluğun eylemlerinden, ihmallerinden ve verdiği emirlerden şahsen sorumlu ve sıralı amirleri ile Türkiye Büyük Millet Meclisine karşı daima hesap verebilir olmasıdır.

ç) Zamanlılık ilkesi: İhbar ve şikâyetlere ilişkin yürütülen işlemlerin geciktirilmeksizin, süresi içerisinde yerine getirilmesidir.

d) Katılımcılık ilkesi: Kolluk şikâyet sistemine kamuoyunun duyduğu güveni ölçmek ve halkın sisteme ilişkin görüş ve düşüncelerinden faydalanmak amacıyla konu ile ilgili sivil toplum kuruluşları ile iş birliği içerisinde bulunulmasıdır.

e) Bağımsızlık ve tarafsızlık ilkesi: Komisyonun görevlerini kendi yetki ve sorumluluğu altında bağımsız ve tarafsız olarak yerine getirmesi; kolluk şikâyetlerine ilişkin olarak araştırma, soruşturma veya ön inceleme yapmakla görevlendirilen müfettişler grubunda yer alan müfettişler ile bu amaçla görevlendirilen diğer personelin, görevlerini adil, yansız ve bağımsız şekilde icra etmesidir.

İKİNCİ KISIM

Komisyon, Sekreteryâ ve Müfettişler Grubu

BİRİNCİ BÖLÜM

Komisyon

Komisyonun kuruluşu ve hukuki yapısı

MADDE 5- (1) Komisyon, Bakanlık bünyesinde sürekli kurul olarak teşekkül ettirilmiştir.

(2) Komisyon, Kanunla ve ilgili diğer mevzuatla kendisine verilen görev ve yetkilerini kendi sorumluluğu altında bağımsız olarak yerine getirir ve kullanır.

(3) Hiçbir organ, makam, merci veya kişi Komisyon kararlarını etkilemek amacıyla emir ve talimat veremez, tavsiye ve telkinde bulunamaz.

Komisyonun teşekkülü

MADDE 6- (1) Komisyon, Kanun kapsamındaki konularda her türlü kararı almak ve uygulamak üzere; Bakan Yardımcısının başkanlığında, Türkiye İnsan Hakları ve Eşitlik Kurumu Başkanı, Kurul Başkanı, Bakanlık Hukuk Hizmetleri Genel Müdürü, Adalet Bakanlığı Ceza İşleri Genel Müdürü, üniversitelerin ceza ve ceza usul hukuku ana bilim dallarında görevli öğretim üyeleri ile baro başkanı seçilme yeterliğine sahip serbest avukatlar arasından Cumhurbaşkanınca seçilecek birer üyeden oluşur.

(2) Öğretim üyeleri ile serbest avukatlar arasından seçilecek üyelerin, seçilmelerinden önceki son beş yıl içinde herhangi bir siyasî partiyle üyelik veya başka türde bir görev ilişkilerinin bulunmaması şarttır.

(3) Süresi dolan üyeler, aynı usulle yeniden seçilebilir.

(4) Başkanın izin, hastalık veya başka bir nedenle görevde bulunmadığı hâllerde Kurul Başkanı, Başkana vekâlet eder.

(5) Seçimle gelen üyeler dışındaki Komisyon üyelerinin izin, hastalık veya başka bir nedenle görevde bulunmadığı ya da Kanunun 3 üncü maddesinin ikinci fıkrasında belirtilen unvandaki kadroların boş olması durumunda, bu görevlere vekâlet eden kişiler üyelik görevini yerine getirir.

Komisyon üyelerinin teminatları

MADDE 7- (1) Komisyon üyeliklerine öğretim üyeleri ile serbest avukatlar arasından seçilecek üyelerin görev süresi dört yıl olup bu üyelerin görevlerine Kanunda belirtilen haller dışında son verilemez.

(2) Üyelerin, ciddi bir hastalık veya sakatlık nedeniyle iş göremez hâle gelmeleri veya görevlendirmeye ilişkin şartları kaybetmeleri ya da seçilmeleri sırasında bu şartları taşımadıklarının daha sonra tespit edilmesi hâlinde, görevlendirildikleri usule göre süreleri dolmadan görevlerinden alınır. Sıhhi yetersizlik durumlarının sağlık kurulu raporu ile belgelendirilmesi şarttır.

(3) Bu maddede belirtilen nedenlerle veya başka herhangi bir neden ile boşalan üyelikler için ilgisine göre 6 ncı maddede belirtilen usule göre en geç bir ay içinde yeni görevlendirme yapılır. Bu şekilde görevlendirilen üyeler, yerine görevlendirildikleri üyenin görev süresini tamamlar.

(4) Seçimle gelen üyelerin Komisyondaki görevlerinden doğan suçlarından dolayı, özel kanunlarındaki hükümler uygulanır.

Başkanın görevleri

MADDE 8- (1) Başkanın görev ve yetkileri şunlardır:

- a) Komisyonun uyumlu, verimli ve düzenli biçimde çalışmasını sağlamak.
- b) Komisyon toplantılarının gündemini belirlemek, Komisyonu toplantıya çağırarak ve toplantılara başkanlık etmek.
- c) Kurul Başkanının önerisi üzerine Kurul Başkanına yardımcı olmak üzere en az beş yıllık meslekî kıdeme sahip bir mülkiye başmüfettişini teklif etmek.
- ç) Komisyon kararlarının uygulanmasını takip etmek.
- d) Kanun ve ilgili mevzuattan doğan diğer görevleri yapmak.

Kurul Başkanının görevleri

MADDE 9- (1) Kurul Başkanının görev ve yetkileri şunlardır:

- a) Komisyonun sekretarya hizmetlerini sevk ve idare etmek, bu hizmetlerin uyumlu, verimli ve düzenli biçimde yürütülmesini sağlamak.
- b) Komisyon Başkanına, Kurul Başkan Yardımcısı olarak görevlendirilecek mülkiye başmüfettişini önermek.
- c) Kanununun 4 üncü ve 8 inci maddeleri hükümleri çerçevesinde verilen görevleri yürütmek üzere tahsis edilecek mülkiye müfettişlerini önermek.
- ç) Komisyon kararlarının yerine getirilmesini sağlamak.
- d) Kanunla Kurul Başkanlığına verilen diğer görevleri yerine getirmek.

Kurul Başkan Yardımcısının görevleri

MADDE 10- (1) Kurul Başkan Yardımcısının görevleri şunlardır:

- a) Komisyonun sekretarya hizmetlerinin sevk ve idare edilmesinde, Kurul Başkanlığına havale edilen Komisyon kararlarının yerine getirilmesinde, Kurul Başkanlığına verilen görevlerin yerine getirilmesinde, Kurul Başkanına yardımcı olmak.
- b) Müfettişler tarafından hazırlanan raporlarda, kanun, yönetmelik ve diğer düzenleyici işlemlere aykırılıklar, yanlışlıklar ve eksiklikler varsa, eksiklikleri tamamlamak, yanlışlıkları düzeltmek.
- c) Raporların mercilerine gönderilmesine ilişkin işlemleri yürütmek.
- ç) Teftiş ve denetim programlarının hazırlanmasında Kurul Başkanı tarafından verilecek talimatları yerine getirmek.

(2) Kurul Başkan Yardımcısına zorunluluk olmadıkça teftiş, denetleme, inceleme ve soruşturma görevleri verilmez.

(3) Kurul Başkan Yardımcısı, Kurulun diğer Başkan Yardımcılarıyla aynı hak ve yetkileri haizdir.

İKİNCİ BÖLÜM

Komisyonun Görev ve Yetki Alanı

Komisyonun görev ve yetkileri

MADDE 11- (1) Komisyonun görev ve yetkileri aşağıda belirtilmiştir:

- a) Kolluk şikâyet sisteminin işleyişine dair ilkeleri tespit ederek bunlarla ilgili olarak Bakanlığa önerilerde bulunmak, bu konudaki uygulamaları izlemek ve sistemin işleyişinde kamu kurum ve kuruluşları arasında koordinasyonu sağlamak.

- b) Kolluk görevlilerinin işledikleri iddia edilen suçlardan veya disiplin cezasını gerektiren eylem, tutum veya davranışlarından dolayı gerektiğinde yetkili merciler tarafından haklarında disiplin soruşturması yapılmasını istemek.
- c) Kolluk şikâyet sisteminin işleyişiyle ilgili konularda teftiş ve denetim yapılması için Bakanlığa önerilerde bulunmak, bu teftiş ve denetimler sonucunda düzenlenen raporları değerlendirmek, tespit edilen eksiklikler konusunda alınması gereken idari tedbirleri belirleyerek Bakanlığa önermek ve bu raporlardan uygun gördüklerini kamuoyuna açıklamak.
- ç) Merkezi kayıt sisteminin etkili bir şekilde işlemesi ve geliştirilmesi için Bakanlığa önerilerde bulunmak ve bu sistemin işleyişini izlemek.
- d) Merkezi kayıt sisteminden elde edilecek veri ve bilgilere ilişkin istatistikler hazırlamak, veri tabanı oluşturmak, elde edilen veri ve bilgilerin analizini yapmak veya yaptırmak, strateji belirlenmesine ve uygulamaya ilişkin önerilerde bulunmak ve gerekli görülen hâllerde bu analizlerin sonuçlarını kamuoyuna duyurmak.
- e) Görev alanına giren konularda tespit, görüş ve öneriler içeren yıllık raporlar hazırlamak ve bu raporları her yıl mart ayında Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonu ile Cumhurbaşkanlığına göndermek ve kamuoyuna açıklamak.
- f) Kolluk görevlilerinin çalışma koşullarının iyileştirilmesine yönelik araştırmalar yapmak veya yaptırmak, kolluk hizmetlerinin geliştirilmesi ve iyileştirilmesine yönelik olarak yapılan çalışmalarını izlemek, değerlendirmek ve bu konularda Bakanlığa önerilerde bulunmak.
- g) Kolluk etik ilkelerinin uygulanmasını izlemek; bu ilkelerin etkin bir şekilde uygulanması konusunda yetkili makamlara önerilerde bulunmak ve bu konuda kolluk teşkilâtı ve ilgili diğer kuruluşlarla iş birliği yapmak.
- ğ) Kolluk şikâyet sistemine kamuoyunun duyduğu güveni ölçmek ve halkın sisteme ilişkin görüş ve düşüncelerini değerlendirmek amacıyla en az iki yılda bir olmak üzere kamuoyu araştırmaları yapmak veya yaptırmak.
- h) Görev alanına giren konularda üniversiteler, kamu kurumu niteliğindeki meslek kuruluşları ve ilgili sivil toplum kuruluşları ile iletişim kurmak ve iş birliği yapmak.
- ı) Kolluğun hizmet içi eğitim programlarıyla ilgili olarak yetkili birimlere görüş bildirmek ve önerilerde bulunmak.
- i) Görev alanına giren konularla ilgili mevzuat düzenlemeleri hakkında görüş bildirmek.

İlke ve standartların tespit edilmesi ve koordinasyon görevi

MADDE 12- (1) Komisyon, Kurul Başkanlığı, mülki idare amirlikleri, bağlı kuruluşlar tarafından yürütülen kolluk şikâyet sisteminin işleyişine ilişkin hizmetler arasında, yeknesaklığın sağlanması ve sistemin etkili çalışmasını temin etmek amacıyla;

- a) Kolluk şikâyet sisteminin işleyişine ilişkin ilke kararları alır.
- b) Teftiş ve denetim standartları belirler.
- c) Teftiş ve denetim rehberleri hazırlar.
- ç) Araştırma, ön inceleme, disiplin soruşturması ve soruşturmaların usul işlemlerinde uygulama birliği ve standardizasyon sağlanmasına yönelik esasları belirler.
- d) Müfettiş ve muhakkikler tarafından düzenlenecek rapor ve diğer belgelerin biçim ve standartlarının belirlenmesine yönelik çalışmalar yapar.
- e) Görev alanına giren konularda yönetmelik, yönerge ve diğer düzenleyici işlem taslakları hazırlar.

(2) Birinci fıkra hükümleri çerçevesinde, Komisyonun almış olduğu kararlar Bakanlık Makamına sunulur.

(3) Komisyon kolluk şikâyet sisteminin işleyişine ilişkin olarak kamu kurum ve kuruluşları arasında koordinasyonu sağlamakla görevli ve yetkilidir. Kamu kurum ve kuruluşları koordinasyonu gerektiren hallerde Komisyonu bilgilendirir. Komisyon, koordinasyonu gerektiren hususlarla ilgili olarak, yılda en az bir defa, ilgili kamu kurum ve kuruluş temsilcilerinin katılımı ile toplantı düzenler. Toplantılara Adalet Bakanlığı, Dışişleri Bakanlığı, Tarım ve Orman Bakanlığı, Ticaret Bakanlığı, Kamu Denetçiliği Kurumu, bağlı kuruluşlar, Polis Akademisi, Jandarma ve Sahil Güvenlik Akademisi temsilcileri ile uygun görülen diğer kamu kurum ve kuruluşları çağrılır. Toplantılar ilgili kamu kurum ve kuruluşun üst yöneticileri veya yardımcılarının katılımı ile gerçekleştirilir.

Komisyonun disiplin soruşturması istemi ve suç duyurusu

MADDE 13- (1) Kolluk görevlilerinin disiplin cezasını gerektiren eylem, tutum veya davranışlarıyla ilgili ihbar ve şikâyetlerin Komisyona intikal etmesi veya Komisyon tarafından resen öğrenilmesi üzerine Komisyon, Kurul Başkanlığından söz konusu ihbar ve şikâyetlerin öğrenildiği tarihten itibaren 30 gün içinde disiplin soruşturması açılmasını isteyebilir. 30 günlük süre, ihbar ve şikâyetin Komisyonda görüşülmeye başlandığı tarihten itibaren işlemeye başlar. Bu istemlerden katalog suçlara ilişkin disiplin soruşturmalarının mülkiye müfettişleri tarafından yapılması esas olup olayın niteliğinin gerektirdiği hâllerde, disiplin soruşturmasını yürüten mülkiye müfettişleriyle birlikte

görev yapmak üzere bağlı kuruluşların müfettişleri de görevlendirilebilir. Katalog suçlarla ilgili disiplin soruşturmalarının valiliklerce veya kaymakamlıklarca yapılması hâlinde, bu işlemler imkânlar ölçüsünde mülkî idare amirliği hizmetleri sınıfında bulunan görevliler tarafından yürütülür. Diğer istemler yönünden genel hükümlere göre işlemler yürütülür.

(2) Komisyonun disiplin soruşturması açılması istemlerine ilişkin olarak, disiplin amiri tarafından önceden soruşturma açıldığı durumlarda, başlanmış olan soruşturmaya devam edilir. Disiplin soruşturması sonucunda yapılan işlemin neticesinden Komisyona bilgi verilir.

(3) Komisyon, daha önce disiplin amirlerince disiplin soruşturması yapılmasına gerek görülmemiş olan ihbar ve şikâyetler hakkında disiplin soruşturması yapılmasını Kurul Başkanlığından isteyebilir. Bu durumda, süre hariç, birinci fıkraya göre işlem yapılır. Daha önce disiplin amirlerince disiplin soruşturması yapılmasına gerek görülmemiş olan ihbar ve şikâyetler hakkında, müfettiş veya bağlı kuruluş müfettişi, disiplin soruşturmasına gerek görmeyen disiplin amirine göre üst disiplin amiri veya en üst disiplin amiri tarafından bizzat ya da görevlendirecekleri müfettiş veya muhakkik eliyle disiplin soruşturması yapılır.

(4) Birinci ve üçüncü fıkra hükümleri çerçevesinde yürütülen disiplin soruşturmaları, zaman aşımı süreleri de dikkate alınarak, en geç üç ay içerisinde sonuçlandırılır. Üç aylık süre disiplin soruşturması emrinin müfettiş veya muhakkik tarafından alındığı tarihte başlar. Maddi veya hukuki sebeplerle bu süre disiplin soruşturması onayını veren amirin uygun bulmasıyla uzatılabilir. Bu sürenin aşılması halinde, gecikmenin gerekçesi Komisyona bildirilir. Yetkili disiplin amir veya kurulları tarafından verilen kararlar gerekçeleri ile birlikte en geç yedi iş günü içerisinde Komisyon sekreterliğine bildirilir.

(5) Komisyon, bir suç işlendiğini ihbar, şikâyet, bilgi, belge veya bulgulara dayanarak öğrendiğinde durumu Kurul Başkanlığına bildirir. Kurul Başkanlığı, tabi olduğu usuller dairesinde, 4483 sayılı Kanun kapsamındaki suçlarla ilgili olarak bu Kanun kapsamında işlem yapılmasını, genel hükümlere tabi suçlar hakkında ise yetkili Cumhuriyet savcılığına geciktirilmeksizin suç duyurusunda bulunulmasını sağlar. 4483 sayılı Kanun kapsamında yetkili merciler tarafından yapılan işlemin sonucundan Kurul Başkanlığına yedi iş günü içerisinde bilgi verilir. Katalog suçlarla ilgili hükümler saklıdır.

Komisyonun teftiş ve denetim istemi

MADDE 14- (1) Komisyon, kolluk şikâyet sisteminin işleyişiyle ilgili konularda teftiş ve denetim yapılması için Kurul Başkanlığı ve bağlı kuruluşların teftiş ve denetim birimlerinden istemde

bulunabilir. Bu isteme ilişkin Kurul Başkanlığı ve bağlı kuruluşların teftiş ve denetim birimlerinin tabi oldukları usule göre işlem yapılır.

Teftiş

MADDE 15- (1) Teftiş, rehberlik anlayışına dayalı olarak aşağıda belirtilen amaçlarla yapılır:

- a) Kolluk şikâyet sisteminin süreç ve sonuçlarını mevzuata, önceden belirlenmiş standartlara, amaç ve hedeflere, performans ölçütlerine ve kalite standartlarına göre tarafsız olarak analiz etmek, karşılaştırmak, ölçmek ve değerlendirmek.
- b) İhbar ve şikâyetlere ilişkin olarak yapılan iş ve işlemleri geçmişe dönük olarak hukuka uygunluk açısından incelemek ve mevzuattan sapmalar varsa, bunları ve meydana geliş nedenlerini ortaya çıkartmak, bu sapmaların düzeltilmesine yönelik tavsiyelerde bulunmak, tespit edilen hukuka aykırılıklara ilişkin hakkında yasal işlem yapılması gerektiği değerlendirilen kamu görevlileri hakkında işlem yapılması amacıyla teklifte bulunmak.
- c) Kolluk hakkındaki ihbar ve şikâyetlere ilişkin izlenen süreçlerde hataların önlenmesine yardımcı olmak, şikâyet sisteminin gelişmesine, yönetim ve kontrol sistemlerinin geçerli, güvenilir ve tutarlı hale gelmesine rehberlik etmek.
- ç) Kolluk şikâyet sisteminde mevzuatın doğru uygulanmasına katkı sağlayacak bilgi ve tecrübe aktarımında bulunmak.

Denetim

MADDE 16- (1) Denetim, kolluk hakkındaki ihbar ve şikâyetlere ilişkin izlenen süreçlerin geliştirilmesini, yönetim ve kontrol sistemlerinin geçerli, güvenilir ve tutarlı hale getirilmesini hedefleyen bir rehberlik anlayışına dayalı olarak, aşağıda belirtilen amaçlarla yapılır:

- a) Kolluk şikâyet sisteminin etkinliğini tespit etmek, hizmet standartlarının iyileştirilmesini sağlamak, kırtasiyeciliğe yol açan uygulamaları belirlemek.
- b) Kolluk şikâyet sistemine ilişkin kolluk amirlerini işbaşında değerlendirmek, bilgi, beceri ve performanslarını ölçmek, hiyerarşik ilişkilerdeki aksaklıkları tespit etmek, personelin moral, motivasyon ve uyumunu araştırmak,
- c) Hukuka uygunluğu tespit etmek.

(2) Müfettişler denetimleri sırasında:

a) Kolluk şikâyet sistemini olağan işleyişi içinde izler ve değerlendirir, bu işleyişe ilişkin aksaklıkları belirler.

b) Gerekirse personele görevleriyle ilgili uygulama yaptırır.

c) Mülâkat ve diğer denetim tekniklerinden yararlanır.

(3) Denetim, haberli veya habersiz olarak yapılabilir.

Komisyonun inceleme ve araştırma istemi

MADDE 17- (1) Komisyon, kendisine Kanunla verilen görevlerle ilgili konularda inceleme ve araştırma yapılmasını Kurul Başkanlığı veya bağlı kuruluşlardan isteyebilir.

(2) Bu isteme ilişkin olarak Kurul Başkanlığı ve bağlı kuruluşların teftiş ve denetim birimlerinin tabi oldukları usule göre işlem yapılır.

(3) İnceleme ve araştırma görevlerine ilişkin süre, görevin kapsamı ve niteliği dikkate alınarak görev emrinde belirtilir.

Raporlar üzerine yapılacak işlemler

MADDE 18- (1) Bu Yönetmelik hükümleri kapsamında mülkiye müfettişleri ve bağlı kuruluşların teftiş ve denetim elemanları tarafından yapılan teftiş, denetim, inceleme ve araştırma görevleri sonucunda düzenlenen raporların bir örneği, yetkili mercilere sunulup Bakanlıkça havale onayı alınmasını müteakip yedi iş günü içerisinde değerlendirilmek üzere Komisyon Başkanlığına gönderilir.

(2) Komisyonun bu raporlar üzerine alınması gereken idari tedbirlere ilişkin önerileri, gerektiğinde bağlı kuruluşların ve/veya mülki idare amirliklerinin görüşleri alındıktan sonra Bakanlık Makamına sunulur. Komisyon önerilerine ilişkin Bakanlık Makamınca nihai olarak karar verilir. Bakanlıkça verilen kararlar yetkili birimler tarafından ivedilikle yerine getirilir. Bakanlık merkez birimleri ve bağlı kuruluşları ile valiler ve kaymakamlar, Bakanlıkça verilen kararların gereklerinin yerine getirilmesinden sorumlu olup yapılan işlemlerin sonucundan Başkanlığa bilgi verilir.

(3) İlgili kurum ve kuruluşlar tarafından, raporlar ve bunlarla ilgili olarak verilen emir ve yazılar özel bir dosyada saklanır. Bunların saklanmasından, devir ve tesliminden, kurum ve kuruluşun amirleri ve ilgili memurları birlikte sorumludur.

(4) Komisyon kesinleşmiş inceleme ve araştırma ile teftiş ve denetim raporlarından uygun gördüklerini, kamuoyuna açıklayabilir. Bu raporlar Komisyonun internet sitesinde yayımlanabileceği gibi sair yollarla da kamuoyu ile paylaşılabilir.

(5) Her yıl ocak ayında önceki yıl içerisinde Kanun kapsamında mülkiye müfettişleri tarafından düzenlenen araştırma, ön inceleme ve disiplin soruşturma raporları, ihbar ve şikâyete sebep olan konu ve uygulamaların tespiti ve ortadan kaldırılmasına yönelik gereken tedbir ve öneriler geliştirilmesi amacıyla Kurul tarafından mülkiye müfettişlerine incelettirilebilir. Bu inceleme sonucunda düzenlenecek raporlar hakkında birinci ve ikinci fıkra hükümleri doğrultusunda işlem yapılır.

Komisyonun yerinde inceleme yapması

MADDE 19- (1) Komisyon, görev alanıyla ilgili konularda, ihtiyaç duyması halinde; topluca veya görevlendireceği üye ya da üyeler vasıtasıyla, yerinde ziyaret, inceleme ve araştırma yapabilir, özel hükümler saklı kalmak kaydı ile ilgililerden yazılı ve sözlü bilgi alabilir.

(2) Yerinde yapılan inceleme ve araştırmalar sırasında özel hükümler saklı kalmak kaydı ile ilgili kamu kurum ve kuruluşları gereken her türlü yardım ve kolaylığı göstermek, iş birliği içerisinde bulunmak zorundadır.

(3) Yerinde yapılan inceleme ve araştırma sonuçları ilk Komisyon toplantısında görüşülür.

Kolluğun hizmet içi eğitim programlarına görüş bildirme

MADDE 20- (1) Kolluk görevlilerinin yıllık genel hizmet içi eğitim programları belirlenirken Komisyonun görüşü alınır.

(2) Kolluk teşkilatları tarafından kolluğun hizmet içi eğitim programlarına ilişkin olarak Komisyonun görüş ve önerileri doğrultusunda, geçen yıl içerisinde yapılan çalışmalar hakkında, her yıl ocak ayının 15'ine kadar Komisyona bilgi verilir.

(3) Komisyon, resen kolluk amir ve personelinin hizmet içi eğitim programlarına ilişkin görüş ve önerilerde de bulunabilir.

(4) Komisyon her eğitim döneminin başlangıcında Polis Akademisi, Jandarma ve Sahil Güvenlik Akademisi eğitim programlarının hazırlanmasında dikkate alınmak üzere görüş bildirebilir.

Kolluk etik ilkelerinin uygulanmasının izlenmesi ve iş birliği

MADDE 21- (1) Kolluk etik ilkelerinin belirlenmesinde ve değiştirilmesinde Komisyonun görüşü alınır.

(2) Komisyon, kolluk etik ilkelerinin uygulanmasına ilişkin olarak kolluk birimlerine önerilerde bulunabilir.

(3) Kolluk teşkilatları tarafından her yıl ocak ayının 20'sine kadar bir önceki yıl kolluk etik ilkelerinin uygulanması konusunda yapılan eğitim, faaliyet, ceza ve disiplin işlemleri bir rapor halinde Komisyona sunulur.

Kolluk hizmetlerinin geliştirilmesi ve iyileştirilmesi konusunda izleme ve görüş bildirme

MADDE 22- (1) Kolluk teşkilatları tarafından her yıl şubat ayının 20'sine kadar bir önceki yıl kolluk hizmetlerinin geliştirilmesi ve iyileştirilmesi konusunda yapılan çalışmalar bir rapor halinde Komisyona sunulur.

(2) Komisyon, kolluk hizmetlerinin iyileştirilmesi ve geliştirilmesine yönelik görüş ve tavsiyelerini uygun gördüğü zamanlarda değerlendirmek üzere Bakanlığa sunar.

(3) Görüş ve önerilerden Bakanlık Makamınca uygun görülenler gereğinin yapılması amacıyla ilgisine göre Bakanlık merkez, bağlı kurum ve kuruluşları ile mülki idare amirliklerine bildirilir.

Kolluk görevlilerinin çalışma koşulları konusunda araştırma

MADDE 23- (1) Komisyon, kolluk görevlilerinin çalışma koşullarının iyileştirilmesine yönelik araştırmalar yapar veya bu konuda araştırma yapılmasını Kurul Başkanlığından, bağlı kuruluşlardan ve mülki idare amirliklerinden isteyebilir. Bu araştırmalar hizmet alımı yolu ile de yaptırılabilir.

(2) Araştırmaların, katılımcı bir anlayışla hazırlanmasına özen gösterilir. Bu amaçla çalıştay, seminer veya konferans düzenlenebilir.

(3) Araştırma sonuçları Komisyonda görüşülür ve alınan tavsiye kararları Bakanlık Makamına sunulur.

Mevzuat düzenlemeleri konusunda görüş bildirme

MADDE 24- (1) Komisyon, görev alanına giren konularda, Bakanlık merkez ve bağlı kuruluşları ile ilgili diğer kamu kurum ve kuruluşları tarafından yapılan mevzuat düzenleme ve değişiklikleri için görüş bildirebilir.

(2) Komisyon, mevzuat düzenleme ve değişikliklerine ilişkin görüşünü oluştururken Kurul Başkanlığı ile bağlı kuruluşlardan konu hakkında inceleme ve araştırma yapılmasını isteyebilir.

(3) Bu isteme ilişkin olarak Kurul Başkanlığı ve bağlı kuruluşların teftiş ve denetim birimlerinin tabi oldukları usule göre işlem yapılır. Hazırlanan inceleme ve araştırma raporlarının bir örneği Komisyonda görüşülmek üzere Başkanlığa gönderilir.

İhbar ve şikâyet istatistik ve analizleri

MADDE 25- (1) İhbar ve şikâyet başvurularına ilişkin istatistikler ve bu verilere ilişkin analizler yıllık olarak hazırlanır ve faaliyet yılını takip eden yılın şubat ayı içerisinde Bakana sunulur, ayrıca gerekli görülen diğer kurum ve kuruluşlara gönderilir.

(2) Gerekli görülen hâllerde istatistikler ve bunlara ilişkin analiz sonuçları Komisyonun internet sitesi veya sair yollarla kamuoyuna duyurulur.

(3) Farklı zaman aralıkları esas alınarak da istatistik ve bunlara ilişkin analizler yayınlanabilir.

(4) Kolluk teşkilatlarının hizmet içi eğitim programlarının hazırlanması sırasında, istatistikler ve bunlara dayalı düzenlenen analizler dikkate alınır.

Yıllık rapor

MADDE 26- (1) Komisyon, görev alanına giren konularda yürüttüğü faaliyetler ile tespit, görüş ve önerilerini içeren yıllık rapor hazırlar. Bu rapor, Komisyonda görüşülerek mart ayında Bakan tarafından Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonu ile Cumhurbaşkanlığına gönderilir.

(2) Yıllık rapor Komisyonun internet sitesinde yayımlanmak suretiyle veya başka yöntemlerle kamuoyuna duyurulur.

(3) Komisyonca gerek görülen konularda özel rapor da hazırlanabilir.

Kamuoyunun bilgilendirilmesi

MADDE 27- (1) Komisyon tarafından kolluk şikâyet sistemi konusunda tanıtıcı ve yol gösterici bilgileri içeren rehber, kitapçık, kamu spotu hazırlanması ve benzeri yazılı ve görsel yöntemler kullanılarak kamuoyu bilgilendirilir.

(2) Kamuoyunun sağlıklı, doğru ve yeterli şekilde bilgilendirilmesi amacıyla Komisyon, görev alanı ile ilgili konularda basın ve yayın organları ile iletişim içinde bulunur.

(3) Komisyon yılın ilk toplantısında, yıl içerisinde kamuoyunun bilgilendirilmesi, aydınlatılması ve bilinçlendirilmesi konularında yapılması planlanan faaliyetleri içeren iletişim planını görüşerek kabul eder. Plan, Komisyon tarafından kabul edilmesinin ardından Bakanlık Makamına sunulur.

(4) Komisyon yılın ilk toplantısında, önceki yıla ait iletişim planı kapsamında yapılan çalışmalara ilişkin hazırlanan raporu görüşür.

Sivil toplum kuruluşları ile diğer kurum ve kuruluşlarla ilişkiler

MADDE 28- (1) Komisyon, katılımcı yönetim anlayışının bir gereği olarak görev alanına giren konularda bilgi ve görüş alışverişinde bulunmak amacıyla, kamu kurum ve kuruluşları, sivil toplum kuruluşları, sendikalar, sosyal ve mesleki kuruluşlar, yükseköğretim kurumları, basın-yayın kuruluşları, araştırmacılar ve ilgili diğer kişi, kurum ve kuruluşlarla iletişim içinde bulunur. Bu amaçla toplantı, kongre, konferans, şura, seminer, çalıştay, panel ve benzeri faaliyetler icra eder.

(2) Sivil toplum kuruluşları ile diğer kurum ve kuruluşlarla bu kapsamda yapılan istişare ve faaliyetlere ilişkin sonuçlar Komisyonda görüşülür ve alınan tavsiye kararları Bakanlık Makamına sunulur.

Kamuoyu araştırmaları yapma

MADDE 29- (1) Komisyon, kolluk şikâyet sistemine kamuoyunun duyduğu güveni ölçmek ve halkın sisteme ilişkin görüş ve düşüncelerini değerlendirmek amacıyla en az iki yılda bir olmak üzere Kurul Başkanlığı Koordinesinde Bakanlık ilgili merkez birimleri, bağlı kuruluşlar ve mülki idare amirlikleri vasıtasıyla kamuoyu araştırması yapar veya hizmet alımı yoluyla yaptırabilir.

(2) Kamuoyu araştırmaları bütün veya belirli paydaşlara yönelik olarak yerine getirilebilir.

(3) Kamuoyu araştırma sonuçları, Komisyonda görüşülür, gerektiğinde Komisyonun internet sitesinde yayınlanır.

Kolluk Gözetim Komisyonu amblemi

MADDE 30- (1) Komisyonun yayımlarında, basılı kâğıtlarında, Komisyon tarafından kabul edilen ve ancak bu yolla değiştirilebilecek olan amblem kullanılır.

ÜÇÜNCÜ BÖLÜM

Komisyonun Çalışma Usul ve Esasları

Gündem ve toplantılar

MADDE 31- (1) Komisyon, en az ayda bir defa olmak üzere, gerekli hâllerde toplanır. Toplantıları Başkan yönetir. Başkanın izin, hastalık veya başka bir nedenle görevde bulunmadığı hâllerde Kurul Başkanı, Başkana vekâlet eder. Komisyon, Başkanın isteğiyle veya Başkan dışında en az üç üyenin birlikte talep etmesi hâlinde, Başkan tarafından olağanüstü toplantıya çağrılır.

(2) Toplantı gündemi Başkan tarafından belirlenerek toplantıdan en az üç gün önce üyelere yazılı veya elektronik ortamda bildirilir. Gündeme yeni madde eklenebilmesi için toplantıda üyelere birinin öneride bulunması ve önerilen maddenin Komisyon tarafından kabul edilmesi gerekir.

(3) Gündem maddelerine geçmeden önce Başkan tarafından Komisyonun faaliyetleri hakkında Komisyona bilgi verilir.

(4) Toplantıda Komisyon üyelerinin verdikleri önerilerin aynen benimsenmesi halinde önerge karar kapsamına dâhil edilir ve verilen önerge ilgili dosyasında muhafaza edilir.

(5) Bir toplantıda gündem maddelerinin görüşülmesi süre nedeniyle bitirilemezse; görüşülemeyen maddeler herhangi bir işleme gerek kalmaksızın bir sonraki toplantı gündemine taşınır.

(6) Toplantılar esas itibarıyla Bakanlıkça belirlenecek Komisyon merkezinde yapılır. Komisyonca kararlaştırılması halinde merkez dışındaki yerlerde de toplantı yapılabilir.

Toplantıya katılım

MADDE 32- (1) Üyelerin, izin, rapor ve görevlendirme dışında mazeretlerinin olması durumunda, mazeretlerini yazılı olarak Başkanlığa bildirmeleri gerekir. Acil durumlarda yazılı bildirim sonradan yapılmak kaydıyla diğer iletişim vasıtaları aracılığıyla durum Başkanlığa bildirilir.

(2) Komisyonun seçimle gelen üyeleri mazeretsiz olarak arka arkaya üç toplantıya veya bir yıl içinde toplam dört toplantıya katılmadıkları takdirde, Komisyon kararıyla üyeliklerine son verilir. Bu fıkrada belirtilen nedenlerle boşalan üyelikler için en geç bir ay içinde yeni görevlendirme yapılır. Bu şekilde görevlendirilen üyeler, yerine görevlendirildikleri üyenin görev süresini tamamlar.

Toplantı ve karar yeter sayısı

MADDE 33- (1) Komisyon, en az beş üyenin hazır bulunması ile toplanır ve en az dört üyenin aynı yöndeki oyuyla karar alır.

(2) Kararlarda çekimser oy kullanılamaz.

(3) Toplantılara katılmayan Başkan ve üyeler, yazılı olarak oy kullanamazlar, oyunu kullanmak üzere üyelerden birine ya da Başkana vekâlet veremezler.

Görüşmelerde usul

MADDE 34- (1) Kararlar müzakere yapılarak alınır. Konular gündemdeki sırasına göre görüşülür. Başkan, bir maddenin görüşülmesinde söz isteyenlere bir sıra dâhilinde söz verir. Konu üzerinde görüşmeler tamamlandıktan sonra gündem maddesi oya sunulur. Başkan oyunu en son kullanır.

(2) Başkan ve üyeler; kendileri, eşleri, evlatlıkları ve üçüncü derece dâhil, üçüncü dereceye kadar kan ve ikinci derece dâhil, ikinci dereceye kadar kayın hısımlarıyla ilgili veya kişisel menfaat ilişkisi içinde oldukları konularda müzakere ve oylamaya katılamaz. Bu durum karar metninde ayrıca belirtilir.

(3) Kararlar, kabul veya ret için el kaldırmak suretiyle işaretle oylanır.

Tutanak ve kararlar

MADDE 35- (1) Toplantılarda alınan kararlar, toplantı sırasında tutanağa geçirilerek, tutanağın her sayfası katılan Başkan ve üyelerce toplantı esnasında veya en geç toplantıyı izleyen beş iş günü içinde, toplantıya katılan tüm üyeler tarafından imzalanır.

(2) Kurul, gündem veya gündem dışı konularla ilgili olan konuşmaların sesli veya görüntülü olarak kayda alınmasını ya da yazılı olarak tutanağa geçirilmesini önceden bir ilke kararına bağlayabilir ya da bu husus toplantı sırasında da kararlaştırılabilir.

(3) Kararlar birbirini takip edecek şekilde numaralandırılır ve karara ilişkin ekler, tutanağa karardaki sıraya göre eklenir.

(4) Çoğunluk kararına katılmayan üye en geç iki gün içinde karşı oy gerekçesini yazılı olarak Komisyona bildirir.

(5) Komisyon kararları, imzalanmasını müteakip Bakanlık Makamına bilgi amaçlı olarak iki iş günü içerisinde sunulur.

Karar defteri

MADDE 36- (1) Kararlara ilişkin tutanakların aslı ve varsa karşı görüş yazıları Komisyon Başkanı tarafından onaylanmış birbirini izleyen sayfa numaralı bir deftere, metnin sağlığından hiçbir şekilde şüpheyi gerektirmeyecek bir biçimde tarih ve numara sırasıyla yapıştırılır ve mühürler karar defterine de taşacak şekilde, dört köşesinden Komisyon mührüyle mühürlenir. Komisyon defteri Komisyon sekretaryasında saklanır. Defterler elektronik ortamda da tutulabilir.

Gizlilik ve toplantılara katılabilecek olanlar

MADDE 37- (1) Komisyon tarafından aksi kararlaştırılmadıkça, toplantılardaki müzakereler gizlidir.

(2) İhtiyaç duyulması hâlinde, gündemdeki konularla ilgili olarak görüşlerinden yararlanılmak üzere kamu görevlileri, kamu ve özel hukuk tüzel kişilerinin temsilcileri veya uzmanlar, Başkan tarafından Komisyon toplantılarına davet edilebilir. Ancak Komisyon kararları, toplantıya dışarıdan katılanların yanında alınamaz.

(3) Başkan ve üyeler ile Kanunla verilen görevleri yürüten personel, görevlerini yerine getirmeleri sırasında edindikleri gizli bilgileri, kişisel verileri, ticarî sırları ve bunlara ilişkin belgeleri, kanunlarla yetkili kılınan mercilerden başkasına açıklayamazlar ve kendilerinin veya üçüncü kişilerin yararına kullanamazlar. Bu yükümlülük, görevden ayrılmalarından sonra da devam eder.

Kararların açıklanması ve yayınlanması

MADDE 38- (1) Komisyon, gerekli gördüğü durumlarda kararlarını uygun vasıtalarla kamuoyuna duyurabilir.

(2) Komisyon tarafından duyurulmasına karar verilen Komisyon kararları, alındığı tarihten itibaren yedi iş günü içerisinde Komisyonun internet sayfasında yayınlanır veya sair yollarla ilan edilir.

Komisyonun bilgi istemi

MADDE 39- (1) Komisyon kendisine verilen görevlerin yerine getirilmesi sırasında, Bakanlıklar ve diğer kamu kurum ve kuruluşları ile doğrudan yazışabilir, bilgi ve belge isteyebilir.

(2) Bakanlıklar ve diğer kamu kurum ve kuruluşları, kanunlardaki özel hükümler saklı kalmak kaydıyla, Komisyonun istediği bilgi ve belgeleri, talebi hâlinde en geç on beş gün içinde Komisyona vermek zorundadır.

(3) Bilgi ve belge talepleri, ancak yazılı olarak ilgili kanun hükmünün açıkça belirtilmesi şartı ile gerekçeli olarak yerine getirilmeyebilir.

(4) Komisyon, Bakanlıklar ve diğer kamu kurum ve kuruluşlarının, istenen bilgi ya da belgeyi sunmaktan kaçındığı ya da bir delili gizlediği kanaatine varırsa, bu durumda sorumlular hakkında gerekli adli ve idari işlemlerin yapılmasını teminen gerekli bildirimlerde bulunur.

DÖRDÜNCÜ BÖLÜM

Komisyon Sekreteryası

Komisyon sekreteryası

MADDE 40- (1) Komisyonun sekreteryaya hizmetleri, Kurul Başkanlığı tarafından yerine getirilir. Komisyonun sekreteryaya hizmetleri Kurul bünyesinde oluşturulan şube müdürlükleri tarafından yürütülür.

Şube müdürlükleri

MADDE 41- (1) Kurul Başkanlığı bünyesinde aşağıdaki şube müdürlükleri oluşturulur:

- a) Soruşturma ve Denetim Hizmetleri Şube Müdürlüğü,
- b) Merkezi Kayıt Araştırma İletişim ve Analiz Hizmetleri Şube Müdürlüğü,
- c) Yönetim Hizmetleri Şube Müdürlüğü.

(2) Şube müdürlüklerinde, müdürlüklerin görevlerinin gerektirdiği niteliklerde ve yeteri kadar personel görev yapar.

(3) Şube müdürlükleri Kurul Başkanı ve onun adına Kurul Başkan Yardımcısının sevk ve idaresi altında görevlerini yerine getirir.

Soruşturma ve Denetim Hizmetleri Şube Müdürlüğünün görevleri

MADDE 42- (1) Soruşturma ve Denetim Hizmetleri Şube Müdürlüğünün görevleri şunlardır:

- a) Katalog suçlarla ilgili araştırma, ön inceleme, inceleme ve disiplin soruşturmalarıyla ilgili iş ve işlemleri yürütmek.
- b) Komisyonun disiplin soruşturması yapılmasına yönelik almış olduğu kararlara ilişkin işlemleri yürütmek.
- c) Komisyona doğrudan gelen şikâyet ve ihbar dilekçeleri, ilgili birimler tarafından Komisyona gönderilen ihbar ve şikâyetler ile Komisyonca resen gündeme alınan konulara ilişkin işlemleri yürütmek.
- ç) Komisyonca disiplin soruşturması yapılması istenen hallerde genel hükümlere göre gerekli işlemleri yürütmek.
- d) Komisyonun teftiş ve denetim görevleri ile ilgili işlemlerini yürütmek.
- e) Komisyonun gündemini hazırlamak, kararlarını kayda almak.
- f) Görev alanına giren konulardaki kararların, işlemlerin, emir ve talimatların uygulanmasını izlemek.
- g) Başkan ile Kurul Başkanı tarafından verilen diğer görevleri yapmak.

Merkezi Kayıt, Araştırma, İletişim ve Analiz Hizmetleri Şube Müdürlüğünün görevleri

MADDE 43- (1) Merkezi Kayıt, Araştırma, İletişim ve Analiz Hizmetleri Şube Müdürlüğünün görevleri şunlardır:

- a) Merkezi kayıt sisteminin işlemlerini sağlamaya yönelik işlemleri yürütmek.
- b) Merkezi kayıt sisteminin işleyişini izlemek.
- c) Merkezi kayıt sisteminden elde edilecek veri ve bilgilere ilişkin istatistikler hazırlanması, elde edilen veri ve bilgilerin analizinin yapılması veya yaptırılması, strateji belirlenmesine ve uygulamaya ilişkin önerilerde bulunulması ve gerekli görülen hâllerde bu analizlerin sonuçlarının kamuoyuna duyurulması işlemlerini yürütmek.

- ç) Merkezi kayıt sisteminin güvenliğinin sağlanması ve sistemde tutulan kişisel verilerin korunmasına yönelik işlemleri yürütmek.
- d) Kolluk şikâyet sisteminin işleyişine dair ilke ve standartlar tespit edilmesi, bu konudaki uygulamaların izlenmesi ve gelişmelerin araştırılmasına ilişkin işlemleri yürütmek.
- e) Kolluk şikâyet sisteminin işleyişinde kamu kurum ve kuruluşları arasında koordinasyonun sağlanmasına yönelik işlemleri yürütmek.
- f) Kolluk görevlilerinin çalışma koşullarının iyileştirilmesine yönelik araştırmalar yapılması veya yaptırılmasına ilişkin işlemleri yürütmek.
- g) Kolluk şikâyet sistemi ile kolluk hizmetlerinin geliştirilmesi ve iyileştirilmesine yönelik çalışmalarının izlenmesi ve değerlendirmesi ile ilgili işlemleri yürütmek.
- ğ) Kolluk etik ilkelerinin uygulanmasının izlenmesi; bu ilkelerin etkin bir şekilde uygulanması konusunda yetkili makamlara önerilerde bulunulması ve bu konuda kolluk teşkilâtı ve diğer ilgili kuruluşlarla iş birliği yapılması konusundaki işlemleri yürütmek.
- h) Komisyonun görev alanına giren konulardaki tespit, görüş ve önerileri içeren yıllık raporların hazırlanması ve bu raporların her yıl mart ayında Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonu ile Cumhurbaşkanlığına gönderilmesi ve kamuoyuna açıklanmasına ilişkin işlemleri yürütmek.
- ı) Kamuoyu araştırmalarına ilişkin işlemleri yürütmek.
- i) Komisyonun görev alanına giren konularda üniversiteler, kamu kurumu niteliğindeki meslek kuruluşları ve ilgili sivil toplum kuruluşları ile iletişim kurulması ve iş birliği yapılmasına ilişkin işlemleri yürütmek.
- j) Komisyonun, Kanunun uygulanmasına ilişkin mevzuat hazırlanması ve gerektiğinde mevzuatta değişiklik yapılmasına ilişkin işlemleri yürütmek.
- k) Komisyona intikal eden, ülkeler, uluslararası ve bölgesel kuruluşlar ile Avrupa Birliği karar alma mekanizmaları ile ilgili yazışmaları yürütmek.
- l) Kolluğun hizmet içi eğitim programlarıyla ilgili olarak yetkili birimlere görüş bildirilmesi ve önerilerde bulunulması işlemlerini yürütmek.
- m) Komisyonun görev alanına giren konularda ilgili mevzuat düzenlemeleri hakkında görüş bildirmesine ilişkin işlemleri yürütmek.

- n) Basın ve halkla ilişkiler faaliyetlerini yürütmek.
- o) Soru önermelerinin cevaplanmasına ilişkin işlemleri yürütmek.

Yönetim Hizmetleri Şube Müdürlüğünün görevleri

MADDE 44- (1) Yönetim Hizmetleri Şube Müdürlüğünün görevleri şunlardır:

- a) Komisyon üyeleri ile ilgili iş ve işlemleri yürütmek.
- b) Komisyonun faaliyetleri ve diğer ihtiyaçları ile yolluk giderleri için her yıl İçişleri Bakanlığı bütçesine ödenek konulmasına ilişkin teklifleri hazırlamak.
- c) Komisyonda görev yapan personelin özlük ve disiplin işleri ile sağlık ve sosyal hizmet faaliyetlerini yürütmek.
- ç) Komisyonun kullanımında bulunan taşınır ve taşınmazlara ilişkin iş ve işlemleri yürütmek.
- d) Başkanlığın, Komisyonun görev alanı ile ilgili sekretarya hizmetlerinin yürütülmesi, günlük, haftalık ve aylık programlarının hazırlanması ve takibi gibi sekretarya hizmetlerini yerine getirmek.
- e) Komisyon Başkan ve üyeleri ile personelin yurt içi ve yurt dışı geçici görev yolluk bildirimleri ve eklerinin yürürlükteki mevzuata uygunluğunu kontrol etmek, bildirimlerin tahakkuk evraklarını düzenleyerek, gerçekleştirme görevlisi ile harcama yetkilisine sunmak, ilgili birimlere ulaştırılmasını sağlamak.
- f) e-icisleri kapsamında uygulamaya alınan modülün kullanımı konusundaki işlemleri yürütmek.
- g) Komisyonun insan gücü planlaması ve personel politikası ile ilgili çalışmaları yapmak, personel sisteminin geliştirilmesi için teklifte bulunmak, Komisyonda görev yapan personelin hizmet içi eğitim planını hazırlamak ve uygulamak.
- ğ) Komisyonun arşiv hizmetlerini yürütmek.
- h) Genel evrak faaliyetlerini düzenlemek ve yürütmek.
- ı) Komisyon faaliyetleri ile ilgili olarak Bakanlıklar ve diğer kamu kurum ve kuruluşlarından bilgi ve belge talep edilmesi ve bunların takibinin sağlanması ile ilgili işlemleri yerine getirmek.
- i) Müfettişlerin hizmet içi eğitimlerine ilişkin işlemleri yürütmek.
- j) Komisyon kararlarına yönelik Bakanlık aleyhine açılan idari davalara ilişkin dava dilekçelerine karşı yapılacak savunma ve mahkeme ara kararının yerine getirilebilmesi açısından Bakanlığın ilgili birimi tarafından ihtiyaç duyulan bilgi ve belgeler hazırlamak.

k) M nhasıran dięer Őube m d rl klerinin g rev alanına girmeyen protokol iŐleri, eŐitli temas ve ziyaretler, g nl k programlar ve benzeri sosyal faaliyetleri, gerektięi takdirde ilgili dięer Őube m d rl kleri ile iŐ birlięi yapmak suretiyle yerine getirmek.

l) Komisyonun internet sayfasının hazırlanması ve sayfada gerekli g ncelleŐtirmelerin yapılmasına iliŐkin iŐlemleri y r tmek.

Őube m d rl klerinin ortak alıŐma esasları

MADDE 45- (1) Őube m d rl kleri aŐaęıda belirtilen alıŐma esasları dairesinde g revlerini yerine getirir:

a) Sekreteryada g revli Őube m d r  ve dięer personel Kurul BaŐkanı ve Kurul BaŐkan Yardımcısının vereceęi b ro iŐlerini yapar ve bu iŐleri dolayısıyla Kurul BaŐkanına ve Kurul BaŐkan Yardımcısına karŐı sorumludur.

b) Komisyonun g ndemi, BaŐkanının emir ve talimatları doęrultusunda, SoruŐturma ve Denetim Hizmetleri Őube M d rl ę  tarafından hazırlanır ve kayda alınır. G ndeme iliŐkin konular, ilgili Őube m d rl ę  tarafından g ndemi hazırlamakla g revli Őube m d rl ę ne s resi ierisinde bildirilir.

c) Komisyon kararlarının takibinden, kararın ilgili olduęu Őube m d rl ę  sorumludur.

) 9/10/2003 tarihli ve 4982 sayılı Bilgi Edinme Hakkı Kanunu ile dięer mevzuat h k mleri erevesindeki bilgi talepleri, talebin ilgili olduęu Őube m d rl ę  tarafından yerine getirilir.

d) BaŐkan tarafından mevzuat h k mleri erevesinde verilen dięer g revler, BaŐkanın takdir edeceęi ilgili Őube m d rl klerincede yerine getirilir.

e) Komisyon kararları ile ilgili olarak uygulamada oluŐan teredd tlerin giderilmesine dair verilecek idari g r Őlere iliŐkin iŐlemler, ilgili Őube m d rl ę  tarafından yerine getirilir.

Őube m d rlerinin g rev ve yetkileri

MADDE 46- (1) Őube m d rlerinin g rev ve yetkileri Őunlardır:

a) Őube m d rl ę n n iŐ ve iŐlemlerini y r tmek ve denetlemek, etkin, verimli ve mevzuata uygun olarak alıŐmasını saęlamak.

b) Yapacaęı iŐ b l m ne g re birimindeki personelin yetki ve sorumluluklarını tespit etmek ve alıŐma prensiplerini belirlemek.

c) İŐ ve iŐlemlerde birimler arası koordinasyonu saęlamak.

- ç) Gizli evrak ve yazışmaların güvenliğini sağlamak için gerekli tedbirleri almak.
- d) Personelin performans değerlendirmesini yapmak, izin işlemlerini yürütmek.
- e) Dairenin hizmet birimlerine tahsis edilen demirbaş, araç ve gereçlerin ilgililerine tevdiini yaparak, denetimlerini yapmak.
- f) Görev alanına giren iş ve işlemler ile amirlerince verilen diğer talimatları yerine getirmek.

BEŞİNCİ BÖLÜM

Müfettişler Grubu

Müfettişler grubu

MADDE 47- (1) Kurul Başkanlığınca, Kanunun 4 üncü ve 8 inci maddeleri hükümleri çerçevesinde verilecek görevleri yürütmek üzere yeteri kadar mülkiye müfettişi tahsis edilir.

(2) Bu amaçla görevlendirilecek mülkiye müfettişleri en az üç yıl mesleki kıdeme sahip mülkiye müfettişleri arasından, hizmet gerekleri ve ihtiyaç durumu dikkate alınarak, Kurul Başkanlığınca belirlenir.

(3) Müfettişlerin belirlenmesinde; başarı belgeleri, ödül, tecziye ve yabancı dil bilgisi, hizmet içi eğitim konuları, yurt dışı inceleme-araştırma konuları, varsa yüksek lisans ve diğer akademik çalışmaları, benzer konularda yapmış oldukları mesleki çalışmaları ve müfettişlik görevi sırasında yapmış olduğu çalışmaları dikkate alınır.

(4) Hizmet gerekleri veya mazeret nedeniyle müfettişler bu amaçla oluşturulan çalışma gruplarından aynı usul ve esaslar dairesinde ayrılabilirler.

(5) Görevlendirilen müfettişler mazeret belirmek şartı ile gruptan ayrılmak isteminde bulunabilirler. Mazeretleri Kurul Başkanlığınca uygun görülenler aynı usulle gruptan ayrılırlar.

Müfettişlerin görevleri

MADDE 48- (1) Kanun kapsamında tahsis edilen mülkiye müfettişlerinin görev ve yetkileri aşağıda belirtilmiştir:

- a) Kolluk görevlilerince işlendiği iddia edilen veya doğrudan öğrenilen; öldürme, kasten yaralama, işkence, zor kullanma yetkisine ilişkin sınırın aşılması ve suç işlemek amacıyla örgüt kurma suçları ile örgüt faaliyeti çerçevesinde işlenen suçlarla ilgili ön inceleme ve/veya disiplin soruşturmalarını yapmak.
- b) Komisyonun talebi üzerine Bakanın onayı ile disiplin soruşturması yapmak.

- c) Kolluk şikâyet sisteminin işleyişiyle ilgili konularda teftiş ve denetim yapmak.
- ç) Komisyona Kanunla verilen görevler ile ilgili konularda inceleme ve araştırma yapmak.
- d) Kurul Başkanlığı tarafından Kanun ve bu Yönetmelik kapsamında verilecek diğer görevleri yerine getirmek.

(2) Bu mülkiye müfettişlerine bu görevlerin haricinde başka bir görev verilmez ve bunlar görev alanlarıyla ilgili konularda düzenli hizmet içi eğitime tabi tutulurlar.

Müfettişlerin tarafsızlığı ve bağımsızlığı

MADDE 49- (1) Müfettişler, Bakanlık Makamının emri ve onayı üzerine Kurul Başkanından aldıkları emirle görev yaparlar.

(2) Görevin yürütülmesinde hiçbir makam veya merci, müfettişlere telkin ve tavsiyede bulunamaz; belirli bir kanaatin belirtilmesi ya da değiştirilmesi için baskı yapamaz.

(3) Müfettişlerin görevlerini adil, etkin, nitelikli ve verimli bir biçimde yürütmeleri açısından Kurul Başkanlığı tarafından gerekli tedbirler alınır.

(4) İşlerin süresinde ve amacına uygun olarak tamamlanması Kurul Başkanlığının gözetim ve takibine tabidir.

Müfettiş görevlendirme kriterleri

MADDE 50- (1) Kurul Başkanlığı tarafından müfettişler arasında görevler adil ve dengeli bir şekilde dağıtılır.

(2) Kanun kapsamında görevlendirilecek müfettişler arasında iş dağılımında; Kurulun ve müfettişlerin iş yükleri, görevlerin ağırlığı ve azami tamamlanma süreleri dikkate alınır.

(3) Başlanmış bir işle ilgili görevlendirmenin devrinin söz konusu olduğu durumlarda, bulunulan aşama itibariyle görev kapsamında elde edilmiş olan belgeler dizi pusulası ekinde Kurul Başkanlığına sunulur. Görevin devrine ilişkin işlemler Kurul Başkanlığı tarafından gerçekleştirilir.

Müfettişlerin çekinebilecekleri hâller

MADDE 51- (1) Müfettişler görevini tarafsız ve nesnel bir şekilde yürütmesini engelleyecek potansiyel veya gerçek çıkar çatışması sebebiyle görevinden çekinme talebini Kurul Başkanlığına bildirir. Başvuru üzerine ileri sürülen sebepler incelenerek müfettişin göreve devam edip etmeyeceğine, görevin aciliyetine göre Kurul Başkanlığınca karar verilir. Bu süre bir haftayı geçemez.

(2) Kurul Başkanlığınca müfettişin görevini tarafsız ve nesnel bir şekilde yürütmesini engelleyecek potansiyel veya gerçek çıkar çatışmasının resen tespit edilmesi hâlinde de görev müfettişten alınır.

Müfettişlerin yükümlülükleri

MADDE 52- (1) Kanun kapsamında görevlendirilen müfettişler görevleri nedeniyle öğrendiği tüm bilgi ve belgelerin güvenliğinin sağlanması hususunda gereken özeni göstermekle yükümlüdür.

(2) Müfettişler, araştırma, ön inceleme, disiplin soruşturması ve soruşturma görevlerini, suçsuzluk karinesini zedelemeyecek şekilde yürütmekle yükümlüdür.

(3) Müfettişler, her soruşturmanın kendine özgü koşullarını dikkate alarak, gecikmeye mahal vermeyecek şekilde tamamlamakla yükümlüdür.

(4) Müfettişler görevlerini, 14/9/2010 tarihli ve 27699 sayılı Resmî Gazete’de yayımlanan Denetim Görevlilerinin Uyacakları Meslekî Etik Davranış İlkeleri Hakkında Yönetmelik hükümlerine uygun olarak yerine getirir.

Müfettişe yardım yükümlülüğü

MADDE 53- (1) Müfettişler, görevleri ile ilgili olarak gerekli gördükleri bilgileri, defter, evrak ve belgeleri; ilgili birim ve kuruluşlardan istemek ve görmek, bunların onaylı örneklerini, gerektiğinde asıllarını almak, ihtiyaç duyulduğunda diğer kamu kurum ve kuruluşlarıyla gerçek ve tüzel kişilerden bilgi ve belge istemek yetkisine sahiptirler. İlgililer müfettişlerin bu isteklerini geciktirmeden yerine getirmek ve sorularını cevaplamakla yükümlüdürler. Asılları alınan belgelerin, müfettişlerin mühür ve imzasıyla tasdik edilmiş örnekleri, dosyasında saklanmak üzere, alındığı yere verilir.

(2) Müfettişlerin görevlerini yerine getirmeleri sırasında bağlı kuruluşlar ile diğer kamu kurum ve kuruluşları gereken her türlü yardım ve kolaylığı göstermekle yükümlüdür. İlgili birim ve kuruluşların yöneticileri, hizmetin gereği gibi yürütülebilmesi için müfettişlere, görevleri süresince uygun bir yer sağlamak, personel ve araç taleplerini karşılamak ve diğer önlemleri almak zorundadır.

(3) Müfettişler yürüttükleri görevleri ile ilgili olarak, birimin ilgili personelinin yıllık izinleri, hastalık ve benzeri zorunlu nedenler dışında, müfettişlerin istemi üzerine, görevin sonuna kadar ertelenebilir. İznini kullanmaya başlamış olan görevli kesin zorunluluk bulunmadıkça geri çağrılmaz.

(4) Müfettişlerin teknik inceleme yapılması talepleri bağlı kuruluşların kriminal laboratuvar müdürlükleri ve diğer ilgili birimleri tarafından öncelikle ve ivedilikle, bedelsiz olarak yerine getirilir.

Müfettişlerin hizmet içi eğitimleri

MADDE 54- (1) Müfettişler görev alanlarıyla ilgili konularda düzenli olarak hizmet içi eğitime tabi tutulur.

(2) Hizmet içi eğitimde müfettişlerin;

- a) Mevzuatta meydana gelen değişikliklerin uygulamaya yansıtılması ve uygulama birliğinin sağlanması,
 - b) Meslekî bilgi, beceri, birikim ve yeterlilik düzeyini artırmak suretiyle meslekî ve kişisel gelişimine katkı sağlanması,
 - c) İnsan haklarına ve hukuka uygun, adil ve hızlı bir soruşturma, ön inceleme, araştırma yapabilme becerisinin geliştirilmesi,
 - ç) Sosyal, kültürel ve teknolojik değişim ve gelişmeleri yakından takip ederek doğru ve hızlı algılama, anlama ve duruma uygun düşünce üretme becerilerinin geliştirilmesi,
 - d) Evrensel hukuk anlayışının içselleştirilmesine katkı sağlanması,
 - e) Meslek etiği bilincinin geliştirilmesi,
 - f) Zamanı verimli şekilde kullanabilme ve karşılaşılabilecek hukuki problemleri kavrama ve doğru çözüm üretebilme becerilerinin geliştirilmesi,
 - g) Kolluk hukuku ve insan hakları alanındaki uluslararası temel belgeler ve ulusal ve uluslararası yargı içtihatları çerçevesinde meslekî yetkinliğin geliştirilmesi,
 - ğ) Yazışma, rapor yazma, inceleme ve araştırma teknikleri konularında gerekli bilgi ve yeteneğin kazandırılması,
 - h) Yurt içi veya yurt dışında görevleriyle ilgili konferans, seminer ve benzeri programlara katılım sağlanarak deneyim kazandırılması,
 - ı) Bilgisayar ve teknoloji kullanım becerilerinin geliştirilmesi,
 - i) Yabancı dil bilgisinin geliştirilmesi,
- esasları gözetilir.

(3) Bu madde hükümleri bağlı kuruluşlar müfettişleri hakkında da uygulanabilir.

Yıllık eğitim planının hazırlanması

MADDE 55- (1) Müfettişlerin yıllık eğitim planı, Kurul Başkanlığı tarafından ihtiyaç duyulan diğer kurum, kuruluş veya kurulların görüş ve önerileri alınarak, her yıl ocak ayı içerisinde Yıllık Eğitim

Planı Taslağı hazırlanır. Taslağın hazırlanmasında mevzuatta, Bakanlığın stratejik planları ile eylem planlarında belirtilen eğitim konularına öncelik verilir.

(2) Yıllık Eğitim Planı Taslağında aşağıdaki hususlar belirtilir:

a) Kongre, konferans, şura, sempozyum, seminer, çalıştay, panel gibi bilimsel ve kültürel toplantı türlerinden hangi yöntemle yapılacağı.

b) Konusu, amaç ve hedefleri.

c) Katılımcı sayısı.

ç) Yapılacağı yer, tarih ve süresi.

(3) Gerekğinde Kurul Başkanlığı tarafından mülakat, anket veya diğer ölçme ve değerlendirme araçları kullanılmak suretiyle eğitime yönelik ihtiyaç analizleri yapılır.

(4) Hizmet içi eğitim programlarından Bakanlık tarafından uygun görüldüğü takdirde Kanun kapsamında görevlendirilmeyen mülkiye müfettişleri de yararlandırılabilir.

(5) Müfettişler grubunda yeni görevlendirilen müfettişler öncelikle hizmet içi eğitime alınır.

Yıllık eğitim planının uygulanması

MADDE 56- (1) Kurul Başkanlığı tarafından hazırlanan Yıllık Eğitim Planı Taslağı, Komisyonun şubat ayı toplantısında görüşülerek karara bağlanır. Karara bağlanan yıllık eğitim planı Kurul Başkanlığına gönderilir. Kurul Başkanlığı, yıllık eğitim planını uygular, programların etkin ve verimli bir şekilde uygulanması için gerekli tedbirleri alır.

(2) Kurul Başkanlığınca kabule değer özürleri olmadıkça hizmet içi eğitim faaliyetlerine katılmak zorunludur.

(3) Eğitim programları, eğitimin konusu ve amacına göre gerektiğinde ilgili kurum, kuruluş ve sivil toplum kuruluşları ile iş birliği yapılarak düzenlenebilir.

(4) Hizmet içi eğitimlerde; mülki idare amirleri, hâkimler ve savcılar, yükseköğretim kurumlarında görev yapan öğretim elemanları, kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarına mensup uzmanlar, avukatlar, yabancı ülkelerden gelen akademisyenler ve uzmanlar, özel eğitim ve danışmanlık kurumlarında çalışan uzmanlardan tabi oldukları mevzuat çerçevesinde yararlanılabilir.

(5) Hizmet içi eğitim görevlilerinin tespitinde, yıllık eğitim planı doğrultusunda oluşturulan programlarda yer verilen konu başlıkları ve içerikleri kapsamında mesleki ya da akademik çalışmaları bulunan ve konusunda uzman kişilerin seçimine öncelik verilir.

Yayımlar

MADDE 57- (1) Müfettişlere, Avrupa İnsan Hakları Mahkemesi ve yüksek mahkeme içtihatları, sıklıkla karşılaşılan ihlal iddiaları ile diğer pratik bilgiler içeren mesleki konularda kitap, bülten, dergi, broşür, CD, DVD ve benzeri gereçler dağıtılabılır.

(2) Kongre, konferans, sempozyum, seminer, çalıştay, panel gibi programlarda sunulan tebliğ veya çalışma raporları yayın hâline getirilebilir.

Yurt dışına gönderilme

MADDE 58- (1) Müfettişler, Kanunun 4 üncü ve 8 inci maddelerinde belirtilen görev alanıyla ilgili konularda inceleme ve araştırma yapmak ve mesleki bilgilerini arttırmak üzere, bir çalışma programı dahilinde, diğer mülkiye müfettişlerinin tabi olduğu usul ve esaslar dairesinde bir yılı geçmemek üzere yurt dışına gönderilir.

ÜÇÜNCÜ KISIM

İhbar ve Şikâyet, Memnuniyet Bildirimleri ve Merkezi Kayıt Sistemi

BİRİNCİ BÖLÜM

İhbar ve Şikâyet, Memnuniyet Bildirimi

İhbar ve şikâyet hakkı, memnuniyet bildirimi

MADDE 59- (1) Herkes;

a) Hak arama hürriyeti kapsamında kolluk görevlileri hakkında ihbar ve şikâyette bulunabilir.

b) Kolluk görevlilerinin hizmet ve faaliyetleri ile tutum ve davranışlarından memnuniyetini bildirebilir.

(2) Kanunî temsilci veya vekil aracılığıyla yapılan şikâyetlerde buna dair kanıtlayıcı bir belgenin sunulması zorunludur. Şikâyet başvurusunun kanunî temsilci veya vekil tarafından yapılması durumunda kanunî temsilci veya vekilin; adı, soyadı ve imzası, Türkiye Cumhuriyeti vatandaşları için vatandaşlık kimlik numarası, yabancı uyruklular için, uyruğu ve varsa yabancı kimlik numarası ve pasaport numarası, tebligata esas yerleşim yeri veya iş adresi, varsa bildirim esas elektronik posta adresi, telefon ve faks numarası, şikâyet başvurusunda yer alır.

İhbar ve şikâyet başvurularında bulunması gereken hususlar

MADDE 60- (1) İhbar ve şikâyet başvurularında, başvuru sahibinin adı, soyadı ve iş veya yerleşim yeri adresi, Türkiye Cumhuriyeti vatandaşları için Türkiye Cumhuriyeti kimlik numarası, yabancı uyruklu ise varsa pasaport numarası ve yabancı kimlik numarası, iddia konusu olayın meydana geldiği yer, zaman, biliniyorsa ilgili olduğu kişi veya kişiler belirtilir.

(2) Dilekçelerin ıslak imzalı olması esastır. İhbar ve şikâyetler güvenli elektronik imza kullanılmak suretiyle de yapılabilir. Başvurunun elektronik posta yoluyla yapılması halinde ise, ihbar ve şikâyet başvurusunda Kanunun 7 nci maddesinin ikinci fıkrasında belirtilen koşulların bulunması gerekir. Bu başvurularda imza şartı aranmaz.

(3) İhbarcı veya şikâyetçinin isteğine bağlı olarak, birinci fıkrada belirtilen hususlar dışında, bu Yönetmelikte belirtilen kişisel verilerine başvuru dilekçesinde yer verilir.

(4) Başvurucu tüzel kişi ise unvanı, adresi ve temsil yetkisini haiz kişinin kimlik bilgileri, varsa telefon numaraları ve elektronik posta adresi başvuru dilekçesinde belirtilir.

(5) Türkiye Cumhuriyeti vatandaşı olmayanlar uyruğu oldukları ülkeyi, var ise pasaport veya yabancı kimlik numarasını, herhangi bir ülke vatandaşı olmayanlar ise bu durumlarını belirtir.

(6) Varsa, ihbar ve şikâyet başvurusundaki iddiasını destekleyecek nitelikte video kaydı, fotoğraf, karar, haber ve yazışma örnekleri, sosyal medya yazışmaları ve benzeri belgeler dilekçeye eklenir.

(7) İhbar ve şikâyetçinin medeni haklarını kullanma ehliyetinden mahrum olduğunun anlaşılması hâlinde bu durum tespit altına alınır. Vesayet altına alınmamış olmakla birlikte akıl hastalığına düçar olduğunun anlaşılması durumunda, varsa raporun evraka eklenmesi ve 22/11/2001 tarihli ve 4721 sayılı Türk Medeni Kanununun "Akıl hastalığı veya akıl zayıflığı" kenar başlıklı 405 inci maddesine göre işlem yapılması için konu yetkili vesayet makamına bildirilir.

(8) İddiaların sıhhatinin şüpheye mahal vermeyecek belgelerle ortaya konulmuş olması hâlinde ihbar ve şikâyet ad, soyad, imza ile iş veya yerleşim yeri adresi, Türkiye Cumhuriyeti vatandaşları için Türkiye Cumhuriyeti kimlik numarası, yabancı uyruklular için pasaport ve yabancı kimlik numarasının belirtilmesi şartı aranmaz.

İhbar ve şikâyetin ve memnuniyet bildiriminin yapılacağı idari merciler ve ihbar ve şikâyet yöntemleri

MADDE 61- (1) İhbar ve şikâyetler ya da memnuniyet bildirimleri, mülki makamlara, kolluk birimlerine, bağlı kuruluşlara elden, yazılı dilekçe veya sözlü olarak doğrudan yapılabileceği gibi

telefon, mektup, faks veya elektronik posta yolu ile de yapılabilir. İhbar ve şikâyet başvurusu ya da memnuniyet bildirimini Komisyonun internet sitesinde örneği yer alan başvuru formunun elektronik ortamda veya çıktısının alınarak doldurulması suretiyle de yapılabilir.

(2) Yapılan sözlü ihbar ve şikâyetlerde öncelikle şikâyetçi veya ihbarcının kimlik bilgisi tespit edilerek, ifadesi tutanağa geçirilir. Muhbir ve müştekinin ihbar ve şikâyete esas konu, biliniyorsa kişi veya kişiler açıkça belirtilir, varsa deliller tutanağa ek yapılır. Başvurunun tutanağa geçirilmek koşuluyla sözlü yapılması durumunda başvuranın imzası ve adresi de tutanağa alınır. Telefonla yapılan başvurularda 59 uncu ve 60 ıncı maddelerde belirtilen ihbar ve şikâyette bulunması gereken unsurlar, ihbar ve şikâyeti alan personel tarafından derhal tutanağa bağlanır. Bu tutanağın ihbarcı ve şikâyetçi tarafından imzalanması şartı aranmaz.

(3) İhbar ve şikâyetin ya da memnuniyet bildiriminin yetkili olmayan bir idari makama yapılması durumunda, başvuru yetkili idari makama gönderilir ve ayrıca başvuru sahibine de bilgi verilir.

(4) Engelli bireylerin başvurularını kolaylaştırmak için gerekli tedbirler alınır.

(5) Kolluk personeli hakkındaki Cumhurbaşkanlığı İletişim Merkezi (CİMER) ile diğer kurumsal başvuru kanalları kullanılarak yapılan ihbar ve şikâyetler ya da memnuniyet bildirimleri hakkında da bu Yönetmelik hükümleri uygulanır.

İhbar ve şikâyet hakkının kötüye kullanılması

MADDE 62- (1) Kolluk personeli hakkındaki ihbar ve şikâyetin, garaz veya mücerret hakaret için, uydurma bir suç isnadı suretiyle yapıldığının araştırma, ön inceleme sonucunda veya soruşturma ve yargılamanın tabi olduğu kanuni işlem sonucunda bu isnadın sabit olmadığına anlaşılması halinde merkezde bu memurun en üst amiri, illerde valiler tarafından isnatta bulunanlar hakkında kamu davasının açılması Cumhuriyet savcılığında talep edilir.

(2) Kolluk personelinin birinci fıkrada belirtilen durumlarda kamu davası açılması için Cumhuriyet başsavcılığına başvurma ve haksız isnatta bulunanlar hakkında genel hükümlere göre tazminat davası açma hakları saklıdır.

İKİNCİ BÖLÜM

İhbar ve Şikâyet Dilekçeleri Üzerine Yapılacak İşlemler

Araştırma

MADDE 63- (1) Suç iddiası içeren herhangi bir ihbar ve şikâyet, taşrada görevli personel için mülki idare amirliklerince, bağlı kuruluşların merkez teşkilatlarında görevli personel için ilgili personel

birimlerince, evvela, 59 uncu ve 60 ıncı maddelerde belirtilen unsurları taşıyıp taşımadığı yönüyle incelenir. Zamanaşımına uğrama ihtimali bulunan ihbar ve şikâyetlere öncelik verilir. Kimlik bilgileri hiç bulunmayan ya da yanlış olan ihbar ve şikâyetler ile kimliğin tespit edilemediği durumlarda (telefon, mektup, e-posta gibi) iddiaların somut verileri içerip içermediği değerlendirilir. İhbar ve şikâyetin içeriğinden Kanunda belirtilen unsurları taşıyıp taşımadığı hususu doğrudan veya olağan idari usullerle anlaşılıyor ise bir araştırma yaptırılır.

(2) Araştırma, mülki idare amirliği hizmetleri sınıfında bulunan görevliler ve/veya kolluk görevlisinin üstü konumundaki kamu görevlileri eliyle yaptırılır.

(3) Araştırma görevi verilenler, bu görevi tebellüğ ettikleri tarihten itibaren zamanaşımı süresi göz önünde bulundurulmak kaydıyla en geç kırk beş gün içerisinde araştırmayı tamamlayarak düzenleyecekleri raporu kendilerini görevlendiren mercie vermek veya soruşturma onayı talep etmekle yükümlüdürler. Maddi veya hukuki sebeplerle kırk beş gün içerisinde tamamlanması mümkün olmayan araştırma görevleri için gerekçesi belirtilmek suretiyle araştırma görevini veren merciden ek süre istenebilir.

(4) Kanununun 2 nci maddesinin birinci fıkrasının (d) ve (j) bentlerindeki tanıma göre ihbar ve şikâyet niteliği taşımadığı mahiyetinden açıkça anlaşılın dilekçeler hakkında 1/11/1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun hükümleri çerçevesinde işlem yapılır.

(5) Komisyon sekreteryasına doğrudan yapılan ihbar ve şikâyetler hakkında birinci fıkraya göre işlem yapılabileceği gibi, Kurul Başkanlığınca da işlem yapılabilir.

İşleme konulmama

MADDE 64- (1) İhbar veya şikâyet dilekçesi ile konuya ilişkin belge ve kayıtlar üzerinde doğrudan veya yapılan araştırma sonucunda;

a) İhbar veya şikâyetlerin soyut ve genel nitelikte olması, ihbar ve şikâyetlerde kişi veya olay belirtilmemesi, iddiaların ciddî bulgu ve belgelere dayanmaması, ihbar ve şikâyet dilekçesinde dilekçe sahibinin doğru ad, soyad ve imzası ile iş veya ikametgâh adresinin bulunmaması durumunda, ihbar ve şikâyet 4483 sayılı Kanununun 3 üncü maddesinde belirtilen soruşturma izni vermeye yetkili mercilerce işleme konulmaz.

b) Yalnızca disiplin suçu iddiası niteliğinde olan ve 59 uncu ve 60 ıncı maddelerde belirtilen şartları taşımadığı anlaşılın ihbar ve şikâyetler ise başvurunun intikal ettiği disiplin amirince, araştırma yapılmış ise araştırma emrini veren disiplin amirince işleme konulmaz. Bu bendin tatbikinde disiplin amiri olarak; ilde vali, ilçede kaymakam, bağlı kuruluşların merkez teşkilatlarında, Cumhurbaşkanı

kararı veya Cumhurbaşkanı onayı ile atananlar için İçişleri Bakanı, diğerleri için ilgisine göre Jandarma Genel Komutanı, Emniyet Genel Müdürü veya Sahil Güvenlik Komutanı anlaşılır.

(2) Araştırma sonucunda ihbar ve şikâyetlerdeki iddiaların sıhhatinin şüpheye mahal vermeyecek belgelerle ortaya konulmuş olması hâlinde adı, soyadı, imzası ile iş veya yerleşim yeri adresinin ve Türkiye Cumhuriyeti kimlik numarasının, yabancı uyruklular için pasaport ve yabancı kimlik numarasının doğruluğu şartı aranmaz. Bu nitelikteki ihbar ve şikâyet hakkında, işleme konulmama kararı verilmez, genel hükümlere göre işlem yapılır.

Kapsam dışı ihbar ve şikâyetler ile ilgili işlemler

MADDE 65- (1) Bakanlık, Komisyon, bağlı kuruluşların merkez birimleri ile mülki idare amirliklerince;

- a) Kamu kurum ve kuruluşlarından talep mahiyeti taşıyan ve idari bir işlem veya eylemle çözümlenebilecek vasıfta olan,
 - b) Kamu kurum ve kuruluşlarının ifa ettikleri hizmetlerde, tesis ettikleri idari işlemlere ilişkin olup ihtilaf halinde idari yargıda dava konusu edilebilecek nitelikte olan,
 - c) İdare ile gerçek ya da tüzel kişiler arasında özel hukuk ilişkilerinden kaynaklanan ve taraflarca adli yargı mercilerinde dava konusu edilebilecek hukuki uyuşmazlıklara ilişkin bulunan,
 - ç) İdarenin veya personelin hukuki sorumluluğunu gerektirebilecek nitelikte bulunan,
- ihbar veya şikâyetlerin, ilgili mevzuat çerçevesinde sonuçlandırılması sağlanır.

(2) İhbar ve şikâyet birinci fıkradaki nitelikte olup, konunun Bakanlık, Komisyon, bağlı kuruluşlar ve mülki idare amirliklerinin görev, yetki ve sorumluluk alanında bulunması halinde; yargı mercilerinin görevine giren konularla ilgili olanlar hariç, gerekli karar ve tedbirler alınır ve yapılan işlem hakkında başvuru sahibine bilgi verilir. İstemin yerine getirilmesi maddi ve/veya hukuki sebeplerle mümkün değilse durum başvuru sahibine gerekçesiyle bildirilir. Bu fıkra kapsamındaki başvurular en geç otuz gün içinde sonuçlandırılır. Bu süre içinde sonuçlandırılmayan başvurularla ilgili işlemin safahatı hakkında dilekçe sahiplerine bilgi verilir. İşlem safahatının duyurulması halinde alınan sonuç ayrıca bildirilir.

(3) 26/9/2011 tarihli ve 659 sayılı Genel Bütçe Kapsamındaki Kamu İdareleri ve Özel Bütçeli İdarelerde Hukuk Hizmetlerinin Yürütülmesine İlişkin Kanun Hükmünde Kararname kapsamında hukuki uyuşmazlıklara konu ihbar ve şikâyetlerle ilgili olarak bu Kanun Hükmünde Kararname hükümleri uygulanır.

Katalog suçlara ilişkin soruşturma usulü

MADDE 66- (1) Kolluk görevlilerince işlendiği ihbar veya şikâyet edilen ya da mülki idare amirlikleri tarafından doğrudan veya yapılan araştırma sonucunda öğrenilen eylemin; öldürme, kasten yaralama, işkence, zor kullanma yetkisine ilişkin sınırın aşılması ve suç işlemek amacıyla örgüt kurma suçları ile örgüt faaliyeti çerçevesinde işlenen suçlardan olduğu kanaatine varılmış ise;

a) Genel hükümlere göre soruşturulması gereken nitelikte olanlar, yetkili Cumhuriyet savcılığına, ayrıca disiplin mevzuatına göre işlem yapılmak üzere de Kurul Başkanlığına gönderilir.

b) Kanunun temel amacı dikkate alınarak ve gerekçesi ortaya konulmak kaydıyla, katalog suçlara yönelik işlemler valilik ve kaymakamlıklarca da yürütülebilir. Bu kapsamda yürütülen ön inceleme ve/veya disiplin soruşturmalarında, esas olarak, mülki idare amirliği hizmetleri sınıfında bulunanlar görevlendirilir. İmkânların elvermemesi nedeniyle mülki idare amirliği hizmetleri sınıfında olmayan personelin görevlendirilmesi durumunda bu uygulamanın gerekçesi görevlendirme onayında belirtilir ve ayrıca bu husus Komisyon Başkanlığına bildirilir. Olayın niteliği gereği ihtiyaç duyulması durumunda, mülki idare amiri ile birlikte kolluk personeli de görevlendirilebilir.

c) Ön inceleme ve/veya disiplin soruşturmalarını yürütmek üzere mülki idare amirliği hizmetleri sınıfından olmayan muhakkik görevlendirildiği takdirde hakkında ön inceleme ve/veya disiplin soruşturması yapılan kolluk görevlisinin, ilgisine göre emniyet hizmetleri, jandarma hizmetleri ve sahil güvenlik hizmetleri sınıfından, üstü konumunda olanlar görevlendirilir.

(2) İhbar ve şikâyetlerin doğrudan Bakanlığa veya bağlı kuruluşlara intikal etmesi veya Bakanlıkça, Komisyonca, bağlı kuruluşlarca ya da müfettiş veya bağlı kuruluşların müfettişlerince resen tespit edilmesi hallerinde; doğrudan veya yapılan araştırma sonucunda; Kanunun 8 inci maddesinin birinci fıkrasının (b) bendinde belirtilen katalog suçlardan olduğu anlaşılanlar;

a) Genel hükümlere göre soruşturulması gereken nitelikte olanlar, yetkili Cumhuriyet savcılığına, ayrıca disiplin mevzuatına göre işlem yapılmak üzere de Kurul Başkanlığına gönderilir.

b) Kurul Başkanlığınca yapılan değerlendirme sonucunda mahallinde veya bağlı kuruluşlarca sonuçlandırılması uygun görülen ihbar ve şikâyetler taşra teşkilatlarında görevli personel için ilgili mülki idare amirliklerine, bağlı kuruluşların merkez teşkilatında görevli personel için bağlı kuruluşların merkez teşkilatlarına gönderilir; Kurulca sonuçlandırılması uygun görülenler için ise Kurul mevzuatına göre gerekli işlemler icra edilir.

c) Ön inceleme ve/veya disiplin soruşturmasını icra etmek üzere müfettiş görevlendirilmesi durumunda, diğer idari mercilerce başlatılmış ve henüz yetkili disiplin amir veya kurullarınca

sonuçlandırılmamış olan ön inceleme ve/veya disiplin soruşturmaları, dizi pusulasına bağlı olarak mülkiye müfettişine devredilir.

ç) Ön incelemeler ve/veya disiplin soruşturmalarının bağlı kuruluşların merkez teşkilatına yaptırılması durumunda; bu işlemler bağlı kuruluşların teftiş ve denetim birimleri tarafından yerine getirilir.

d) Olayın niteliği gereği ihtiyaç duyulması durumunda, mülkiye müfettişiyle birlikte bağlı kuruluşların müfettişleri de görevlendirilebilir.

Katalog suçlara ilişkin değerlendirme kriterleri

MADDE 67- (1) Katalog suçlara ilişkin araştırma, ön inceleme ve/veya disiplin soruşturmalarının, Kanun kapsamında oluşturulan müfettişler grubunda görev yapan mülkiye müfettişleri tarafından yerine getirilmesi esastır.

(2) Birinci fıkrada belirtilen katalog suçlarla ilgili araştırma, ön inceleme ve/veya disiplin soruşturmalarının; mülkiye müfettişleri, bağlı kuruluş müfettişleri, mülki idare amirlikleri veya muhakkikler tarafından yerine getirilmesine ilişkin değerlendirmelerde;

a) T.C. Anayasası ile Avrupa İnsan Hakları Sözleşmesinde tanımlanan temel hak ve hürriyetlerin ihlali,

b) İsnat konusu eyleme ilişkin delillerin toplanmasındaki engeller,

c) İşin karmaşıklık derecesi,

ç) Hukuki meselenin çözümündeki güçlük,

d) Müşteki veya mağdur, tanık ve/veya isnada maruz görevli sayısı,

e) İsnat konusu eylemin kamuoyunda yarattığı etki,

f) Olayın niteliği gereği ülke genelini ilgilendirmesi,

g) Meydana gelen zarar veya tehlikenin ağırlığı,

ğ) Kolluk personelin kast veya taksire dayalı kusurunun ağırlığı,

ve benzeri kriterler göz önünde bulundurularak, bu niteliklerde olduğu değerlendirilen katalog suçların araştırma, ön inceleme ve/veya disiplin soruşturmaları mülkiye müfettişleri tarafından yerine getirilir.

(3) Katalog suçlarla ilgili olarak; bağlı kuruluşların en üst amirleri ve bunların yardımcıları, başkanlar ve daire başkanları, jandarma veya sahil güvenlik bölge komutanları, il emniyet müdürleri, il

jandarma komutanları hakkındaki araştırma, ön inceleme ve/veya disiplin soruşturmaları mülkiye müfettişlerince yürütülür.

(4) İkinci ve üçüncü fıkra kapsamında görevlendirilen mülkiye müfettişleri ile birlikte görev yapmak üzere bağlı kuruluş müfettişleri de görevlendirilebilir.

ÜÇÜNCÜ BÖLÜM

Merkezi Kayıt Sistemi

Amaç ve temel ilkeler

MADDE 68- (1) Bakanlık tarafından Komisyon ile bağlı kuruluşlar ve mülki idare amirlikleri arasında, kolluk görevlileri hakkında idari mercilerce yürütülen ceza ve disiplin işlemleri ya da memnuniyet bildirimleri ile ilgili olarak gerekli bilgilerin elektronik ortamda kaydedilmesi ve yapılan uygulamaların izlenmesi amacıyla merkezi kayıt sistemi oluşturulur.

(2) Kolluk görevlileri hakkında Komisyona ve/veya diğer idari mercilere yapılan her türlü ihbar ve şikâyet ile idari merciler tarafından resen tespit edilen ve işlem yapılmasını gerektiren fiil ve hâller merkezi kayıt sistemine kaydedilerek, sistemden bir kayıt numarası verilir. Bu numara, ihbar ve şikâyetin başlangıcından buna ilişkin yapılan işlemlerinin sonuna kadar sürecin takip edildiği, yapılan işlemlerin aşamalarının tutulduğu kayıt numarasıdır.

(3) Cumhuriyet savcılarının kolluk görevlileri hakkında görevlerinden doğan veya görevleri sırasında işledikleri suçlar ile kişisel suçları sebebiyle başlattıkları soruşturmalarla ilgili olarak Kanunun 8 inci maddesinin üçüncü fıkrası hükmü kapsamında mülki idare amirlikleri ile Bakanlığa yapmış oldukları bildirimler merkezi kayıt sistemine kaydedilir.

(4) İşleme konulmama kararı verilen ihbar ve şikâyetlerle ilgili bilgiler de merkezi kayıt sistemine kaydedilir.

(5) Merkezi kayıt sistemine sağlıklı kayıt yapılması, aynı ihbar ve şikâyet konusu ile ilgili olarak birden fazla kayıt yapılmaması amacıyla sistem ve yetkili kullanıcı tarafından gerekli tedbirler alınır. Mükerrer kayıt yapıldığının sonradan anlaşılması halinde kayıtlar eşleştirilerek sistemde gerekli düzeltmeler yapılır. Merkezi kayıt sisteminden numara verilmesi sırasında, daha önce aynı kişi tarafından aynı konuda yapılan başvuru ile ilgili olarak bir kayıt numarası verildiğinin tespiti halinde, işlemler önceki kayıt numarası üzerinden yürütülür.

(6) Merkezi kayıt sisteminin alt yapısı Bakanlık Bilgi İşlem Daire Başkanlığının sorumluluğunda bağlı kuruluşların bilgi işleminden sorumlu birimleri ile müştereken hazırlanır. Bu sistem kapsamında Bilgi

İşlem Dairesi Başkanlığının ihtiyaç duyduğu verileri, kurumlar web servis yolu ile elektronik ortamda paylaşmak ile yükümlüdürler.

(7) Merkezi kayıt sistemindeki verilerin, mevzuat çerçevesinde bağlı kuruluşlar ve diğer kamu kuruluşları ile paylaşılmasına ilişkin esaslar Komisyonun görüşü alınarak Bakanlıkça belirlenir. Bu suretle paylaşılan veriler başka amaçla kullanılamaz.

(8) Merkezi kayıt sistemi ile Ulusal Yargı Ağı Bilişim Sistemi (UYAP) arasında, gerek duyulduğu durumda, Bakanlık ve Adalet Bakanlığı arasında müştereken belirlenecek esaslar çerçevesinde bilgi paylaşımında bulunulabilir.

Kayıt altına alınacak bilgiler

MADDE 69- (1) Merkezi kayıt sisteminde aşağıdaki veriler kayıt altına alınır:

a) Başvuru sahibi ile ilgili olarak;

- 1) Adı ve soyadı,
- 2) İş veya yerleşim yeri adres bilgileri,
- 3) Türkiye Cumhuriyeti vatandaşı ise Türkiye Cumhuriyeti kimlik numarası,
- 4) Yabancı ise uyruğu, varsa pasaport numarası ve yabancı kimlik numarası,
- 5) Yaşı.

b) İhbar ve şikâyete konu kolluk personel ile ilgili olarak;

- 1) Adı ve soyadı,
- 2) Olay tarihinde çalıştığı birim,
- 3) Olay tarihindeki yaşı,
- 4) Eğitim durumu,
- 5) Türkiye Cumhuriyeti kimlik numarası,
- 6) Hizmet yılı.

c) İhbar veya şikâyete konu olaya ilişkin olarak;

- 1) Olayın tarih ve saati,
- 2) Olay yeri,
- 3) Olayın özeti,

- 4) Olaya ilişkin yaralama veya ölüm olup olmadığı,
 - 5) Olaya ilişkin maddi bir kayıp olup olmadığı,
 - 6) İsnat edilen suç,
 - 7) Olay ile ilgili olarak daha önce herhangi bir adli veya idari mercie başvurulup başvurulmadığı.
- ç) Olay hakkında yürütülen işlemlerin safahatına ilişkin olarak;
- 1) Araştırmaya ilişkin işleme konulmama kararı özeti, var ise bu kararla ilgili idari yargı kararı özeti,
 - 2) Disiplin soruşturması kararı özeti, var ise bu kararla ilgili idari yargı kararı özeti,
 - 3) Ön inceleme sonucunda verilen karar özeti, var ise bu kararla ilgili idari yargı kararı özeti,
 - 4) Ceza soruşturması ve kovuşturmasına ilişkin karar özetleri,
 - 5) Var ise tazmin, görevden uzaklaştırma, görev yeri değişikliği ve benzeri diğer idari işlemlerin özeti ve var ise bunlara ilişkin idari ve adli yargı kararının özeti ile bu nedenle yapılan işlemin özeti.
- (2) İsteğine bağlı olarak, başvuru sahibine ait aşağıdaki veriler merkezi kayıt sistemine kaydedilir:
- a) Meslek,
 - b) Elektronik posta adresi,
 - c) Diğer iletişim bilgileri,
 - ç) Öğrenim durumu,
 - d) Diğer kişisel veriler.
- (3) İhbar ve şikâyetlere ilişkin olarak kullanılacak örnek şikâyet/ihbar formu, memnuniyet bildirim formu ile diğer ihtiyaç duyulacak form ve sair standart belgeler yönerge ile düzenlenir.

Sorumluluk

MADDE 70- (1) Merkezi kayıt sisteminin teknik altyapısının işleyişinden Bakanlığın Bilgi İşlem Dairesi Başkanlığı, idari işleyişinden ise Kurul Başkanlığı sorumludur.

(2) Merkezi kayıt sistemine ilişkin iş ve işlemler; Bakanlık düzeyinde Komisyon sekreteryası, valiliklerde il idare kurulu müdürlükleri, kaymakamlıklarda ilçe yazı işleri müdürlükleri, bağlı kuruluşların merkez teşkilatlarında ise personel işlerinden sorumlu birimler tarafından yürütülür.

(3) Merkezi kayıt sisteminin mevzuata uygun olarak yürütülmesinden illerde vali, ilçelerde kaymakam, bağlı kuruluşlarda ise kuruluşun en üst amiri sorumludur.

(4) Merkezi kayıt sisteminde kayıt altına alınmadığı anlaşılan ihbar, şikâyet ve benzeri durumun tespiti halinde, sorumlular hakkında gerekli yasal işlemler ivedilikle yerine getirilir.

Merkezi kayıt sisteminin işleyişi

MADDE 71- (1) İhbar ve şikâyetlerin, mülki idare amirliklerine, bağlı kuruluşlara veya Komisyon sekreteryasına elden verildiği veya posta ya da elektronik posta yoluyla gönderildiği durumlarda, 70 inci maddenin ikinci fıkrasında belirtilen birimler tarafından başvuru, merkezi kayıt sistemine kaydedilir ve sistemden bir merkezi kayıt numarası verilir.

(2) Bu merciler tarafından resen tespit edilen ve işlem yapılmasını gerektiren fiil ve hâllerde de birinci fıkra hükmü uygulanır.

(3) İhbar ve şikâyetlerin yetkili olmayan mülki idare amirlikleri ile diğer idari mercilere yapıldığı durumlarda, bu merciler ihbar ve şikâyeti iki iş günü içinde, ilgisine göre, mahalli mülki idare amirliğine veya bağlı kuruluşların personel birimine varsa ekleri ile birlikte gönderir. Bildirim üzerine bu birimler tarafından birinci fıkraya göre işlem yapılır.

(4) Kolluk personeli hakkında Cumhurbaşkanlığı İletişim Merkezi (CİMER) ile diğer kurumsal başvuru kanallarına yapılan ihbar ve şikâyetler de bu Yönetmelikte düzenlenen usul ve esaslar dairesinde merkezi kayıt sistemine kaydedilir.

(5) Kanun kapsamında, Cumhuriyet savcılar tarafından kolluk görevlilerinin görevlerinden doğan veya görevleri sırasında işledikleri suçlar ile kişisel suçları sebebiyle başlatılan soruşturmalarla ilgili olarak, personelin ilgisine göre, Bakanlığa, valiliğe veya kaymakamlığa yapmış oldukları bildirimler, yetkili idari merciler tarafından merkezi kayıt sistemine kaydedilir.

Merkezi kayıt numarasının bildirimi

MADDE 72- (1) Merkezi kayıt numarası, mülki idare amirliklerine, bağlı kuruluşlara veya Komisyon sekreteryasına elden yapılan başvurularda, başvuruyu kabul eden görevlinin adı, soyadı ve unvanı ile başvurunun yapıldığı tarih ve saati de gösteren alındı belgesi ile başvuru sahibine bildirilir. Telefon, posta veya elektronik posta yolu ile ihbar ve şikâyetlerin yetkili olmayan mülki idare amirlikleri ile diğer idari mercilere yapılması dolayısıyla bu birimler tarafından gönderilen başvurulara ilişkin olarak ise, merkezi kayıt numarası telefonla yapılanlarda tutanağın düzenlendiği, posta veya elektronik posta yolu ile yapılanlarda ise başvurunun idareye intikal ettiği tarihten itibaren en geç üç iş günü içerisinde başvuru sahibinin belirtmiş olduğu tebligat adresine, elektronik posta yolu yapılan başvurularda, aksine bir adres belirtilmemiş ise gelen elektronik posta adresine gönderilir.

(2) İhbar ve şikâyetlerin yetkili olmayan mülki idare amirlikleri ile diğer idari mercilere yapıldığı durumlarda, bu birimler tarafından, başvurulara ilişkin genel evrak kayıt numarası verilir ve bu numara başvuran kişiye bildirilir. Bu bildirimle ilişkin işlemler birinci fıkrada belirtilen usuller dairesinde yerine getirilir.

Yetkilendirme

MADDE 73- (1) Komisyon tarafından belirlenen esaslar dahilinde merkezde Kurul Başkanı, bağlı kuruluşların merkez teşkilatında bağlı kuruluşların en üst amiri, illerde vali, ilçelerde kaymakam tarafından merkezi kayıt sistemine kayıt iş ve işlemlerinden sorumlu personel belirlenerek yetkilendirilir. Yetkilendirilmemiş personelin merkezi kayıt sistemine giriş veya veri kaydı yapması yasaktır.

(2) Yetkilendirilmiş personel tarafından merkezi kayıt sisteminde oluşturulan kayıtların merkezde Kurul Başkanı veya Kurul Başkan Yardımcısı, ilçelerde kaymakam, illerde vali veya görevlendireceği vali yardımcısı, bağlı kuruluşların merkez teşkilatında ise personel işlerinden sorumlu birim amirine elektronik ortamda havalesi zorunludur. Havale üzerine söz konusu merciler tarafından bu Yönetmeliğin ilgili hükümleri çerçevesinde işlem yapılır.

(3) Görev ve hizmeti ile sınırlı olmak kaydıyla aşağıda belirtilenler merkezi kayıt sisteminde sorgulama yapma yetkisine sahiptir:

a) Komisyon Başkanı.

b) Kurul Başkanı.

c) Kurul Başkan Yardımcısı.

ç) Bağlı kuruluşların merkez teşkilatında personel işlerinden sorumlu birim amiri.

d) İllerde vali, görevlendireceği vali yardımcısı.

e) İlçelerde kaymakam.

f) Yetkilendirilmiş büro personeli.

(4) Mülki idare amirliklerindeki bürolarda görevlendirilecek ve merkezi kayıt sistemine kayıt ve sorgulama yapma yetkisi verilecek personel hakkında, 14/2/2000 tarihli ve 2000/284 sayılı Bakanlar Kurulu Kararıyla yürürlüğe konulan Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği hükümlerine göre güvenlik soruşturması yapılır. Güvenlik soruşturması sonuçlanmadan yetkilendirme işlemi yapılamaz.

Verilerin gizliliğinin korunması

MADDE 74- (1) İhbar veya şikâyette bulunan kişilerin kimlik bilgileri gizli tutulur. İhbar ve şikâyet başvurusunun gizli kalmasına yönelik her türlü tedbir; müfettişler, muhakkikler ve diğer idari makam ve merciler tarafından alınır.

(2) Merkezi kayıt sisteminde elektronik belgelerin kayıt altına alınması, kullanılması ve arşivlenmesi konularında E-Dönüşüm ve e-Devlet uygulamalarına ilişkin esas ve usuller uygulanır.

(3) Merkezi kayıt sistemine ilişkin elektronik log kayıtları, en az altı ayda bir olmak üzere; Komisyon merkezinde kurulu sisteme ilişkin olarak Komisyon Başkanı, bağlı kuruluşların merkez teşkilatlarında kurulu bulunan sisteme ilişkin olarak kuruluşun en üst amiri, il genelinde kurulu bulunan sisteme ilişkin olarak ise il valisi tarafından, oluşturulacak en az üç kişiden müteşekkil bir heyet tarafından denetlenir.

(4) Gizlilik, savunma hakkı ile hak arama hürriyetinin kullanılmasını engelleyecek şekilde uygulanamaz.

Valilik ve kaymakamlık kolluk şikâyet büroları

MADDE 75- (1) Kolluk şikâyetlerine ilişkin iş ve işlemleri yürütmek üzere illerde, il idare kurulu müdürlüğü, ilçelerde ise yazı işleri müdürlüğü bünyesinde kolluk şikâyet büroları oluşturulur. Bu birimler, mülki idare amirlikleri tarafından görevlendirilecek yeteri kadar personelden oluşur. Bu birimlerde kolluk personeli görevlendirilemez. İhbar ve şikâyetlere ilişkin olarak iş ve işlemlerin yürütülmesi ve takibi bu birim tarafından yerine getirilir.

(2) Kolluk şikâyet büroları aşağıdaki görevleri yürütmekle görevlidir:

- a) İhbar ve şikâyetlerin merkezi kayıt sistemine kaydını yapmak.
- b) Kanun kapsamında Komisyon ile ilgili yazışmaları yürütmek.
- c) İhbar ve şikâyetlerle ilgili yazışmaların kaydı, takibi, ilgili birimlere sevk edilmesi ve diğer işlemleri yapmak.

(3) Bu birimlerde görevlendirilen personel ilgili mevzuat hükümleri ve merkezi kayıt sisteminin işleyişi ile ilgili olarak valilik tarafından her yıl şubat ayı içerisinde hizmet içi eğitime tabi tutulur.

Kolluk teşkilatları şikâyet birimleri

MADDE 76- (1) Bağlı kuruluşların merkez ve taşra teşkilatlarında, kolluk şikâyetleri ile ilgili birimler oluşturulur.

(2) Bu birimler bağı kuruluşların merkez teşkilatlarında personel işlerinden sorumlu birim bünyesinde, taşra teşkilatlarında ise Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı için il ve ilçe düzeyinde, Sahil Güvenlik Komutanlığı için ise Bölge ve Grup Komutanlığı düzeyinde kurulur.

(3) Bu birimler kolluk hakkındaki şikâyetlere ilişkin iş ve işlemleri yerine getirmek, kolluk etik ilkelerinin uygulanmasına ilişkin işlemleri yürütmekle görevlidirler.

(4) Bu birim, kolluk personeli hakkındaki şikâyetlerin önlenmesine ilişkin olarak risk analizleri yaparak, alınması gerekli gördükleri tedbirler konusunda yetkili mercilere yılda en az bir defa olmak üzere rapor sunmakla mükelleftir.

(5) Bu birimlerde görevlendirilen kolluk personeli kolluk şikâyetlerine ilişkin olarak her yıl ocak ayı içerisinde ve ihtiyaç duyulan diğer zamanlarda düzenli olarak hizmet içi eğitime tabi tutulur.

(6) Bu birimlerde görev yapan personelin göreviyle ilgili herhangi adli veya idari bir ceza almamış olması zorunludur.

(7) Bu birimler görevlerini doğrudan birimin en üst amirine bağı olarak yerine getirir.

(8) Bu birimlerde görev yapan personele, büronun görevleri dışında, nöbet ve benzeri başka görev verilmez.

DÖRDÜNCÜ KISIM

Bilgilendirme ile Çeşitli ve Son Hükümler

BİRİNCİ BÖLÜM

Disiplin Soruşturmalarında Bilgilendirme

Bilgilendirme yapmakla görevli merciler

MADDE 77- (1) Şikâyetçi ile ihbar ve şikâyet edilen kolluk görevlileri, disiplin soruşturmasının safahatı hakkında, ilgisine göre Bakanlık, mülki idare amirlikleri ve bağı kuruluşların merkez teşkilatları tarafından en az iki ayda bir bilgilendirilir.

(2) Disiplin soruşturmalarına ilişkin bildirimlerin sekreteryaya hizmetleri aşağıdaki birimler tarafından yerine getirilir:

a) İllerde il idare kurulu müdürlükleri.

b) İlçelerde ilçe yazı işleri müdürlükleri.

c) Mülkiye müfettişleri tarafından yapılan disiplin soruşturmalarında Kurul Başkanlığı.

ç) Bağlı kuruluşların merkez teşkilatlarında görevli kolluk personeli hakkında olup disiplin soruşturması yine bu birimler tarafından yerine getirilen şikâyetlere ilişkin bağlı kuruluş merkez teşkilatının personel işlerinden sorumlu birimi.

Disiplin soruşturmasının safahatı hakkında bilgilendirme süreci

MADDE 78- (1) Bildirimlere esas olmak üzere, iki aylık sürenin dolmasından en geç beş iş günü önce, disiplin soruşturması yapan görevli veya görevliler tarafından, disiplin soruşturması onayını veren mercie, soruşturmalarının safahatı hakkında bilgi verilir.

(2) Kanun kapsamında yapılacak bilgilendirmeler, soruşturmanın safahatını tam olarak ortaya koyacak nitelikte açık ve anlaşılabilir ifadelerle yapılır.

(3) Bilgilendirmelere ilişkin yazıların bir örneği disiplin soruşturması işlem dosyasında denetime esas olmak üzere muhafaza edilir.

(4) Bildirimlere ilişkin gerekli hassasiyeti göstermeyen personel hakkında yetkili merciler tarafından yasal işlemler ivedilikle yerine getirilir.

(5) Disiplin soruşturmasının tamamlanmasını müteakip disiplin soruşturması sonucunda verilen karar şikâyetçiye ayrıca bildirilir.

Araştırma sonucu hakkında bilgilendirme

MADDE 79- (1) Bu Kanun hükümleri kapsamında yürütülen araştırma görevinin sonucu hakkında şikâyetçi ile ihbar ve şikâyet edilen kolluk görevlilerine bilgi verilir.

(2) Bu kapsamda yapılacak bildirimler, araştırmanın yetkili makam tarafından sonuçlandırılmasını müteakip, izleyen en geç onbeş gün içerisinde yerine getirilir.

İKİNCİ BÖLÜM

Cumhuriyet Savcılıkları Tarafından Bilgilendirme

Cumhuriyet savcılıkları tarafından bilgilendirme yükümlülüğü

MADDE 80- (1) Cumhuriyet savcılıkları kolluk görevlileri hakkında görevlerinden doğan veya görevleri sırasında işledikleri suçlar ile kişisel suçları sebebiyle soruşturma başlattıkları takdirde durumu personelin ilgisine göre Bakanlığa veya mülki idare amirliklerine en geç yedi iş günü içinde bildirir. Bildirimlerde kolluk personeli hakkındaki soruşturma konusu açık bir şekilde belirtilir.

(2) Bildirimde bulunulan yetkili idari merciler tarafından gerek görülen idari tedbirler alınır ve disiplin soruşturması başlatılır.

(3) Kolluk görevlileri hakkındaki araştırma, disiplin soruşturması, ön inceleme ve soruşturmalarda görevli müfettiş veya muhakkiklerin talep etmeleri hâlinde, Cumhuriyet savcılıkları tarafından ceza soruşturmasının amacını tehlikeye düşürmemek ve gizlilik ilkesine sadık kalınmak kaydıyla, başka yolla temini mümkün olmayan delillerin birer örneği dizi pusulasına bağlanarak gönderilir. Soruşturma dosyasıyla ilgili 5271 sayılı Kanununun 153 üncü maddesine göre kısıtlama kararı bulunduğu takdirde, Cumhuriyet savcılığınca bu kararın bir örneği de diğer belgelerle birlikte müfettiş veya muhakkiklere verilir. Müfettiş ve muhakkikler ile diğer idari makam, merci ve kurullar kısıtlama kararının ihlalini önlemek için gerekli tedbirleri almakla yükümlüdürler.

(4) Cumhuriyet savcılıkları tarafından kolluk personeli hakkında, görevden doğan veya görevi sırasında işledikleri suçlarla kişisel suçları sebebiyle yapılan soruşturma sonunda düzenlenen kovuşturmayaya yer olmadığı kararları, iddianame ile ilgili mahkemelerce verilen karar suretleri ilgisine göre Bakanlık, bağlı kuruluş merkez teşkilatı ve mülki idare amirliklerine gönderilir.

ÜÇÜNCÜ BÖLÜM

Çeşitli ve Son Hükümler

Müfettişlerin çalışma usul ve esasları

MADDE 81- (1) Mülkiye müfettişleri ile bağlı kuruluş müfettişlerinin çalışma usul ve esasları, yetkileri, düzenleyecekleri raporların türleri, şekilleri, tevdi edecekleri merciler, takibi ve raporlamaya ilişkin diğer hususlar; Kanun ve bu Yönetmelik hükümleri saklı kalmak kaydıyla kendi özel mevzuatlarına tabidir.

(2) Mülkiye müfettişleri ve bağlı kuruluş müfettişlerinin birlikte görev yapmaları hâlinde mülkiye müfettişlerinin tabi olduğu usul ve esaslar uygulanır.

Saklı hükümler

MADDE 82- (1) Kanun ve bu Yönetmeliğin uygulanmasına ilişkin olarak 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile 4982 sayılı Kanundaki sınırlamalar saklıdır.

Bütçe ve mali hükümler

MADDE 83- (1) Komisyonun faaliyetleri ve diğer ihtiyaçları ile yurt içi ve yurt dışı görevlendirmelere ilişkin yolluk giderleri için her yıl Kurul bütçesine gerekli ödenek konulur.

(2) Komisyon başkan ve üyeleri ile bu Kanun kapsamında yapılan faaliyetlere ilişkin olarak görevlendirilenlere 10/2/1954 tarihli ve 6245 sayılı Harcırah Kanunu kapsamında yolluk ödenir.

Yazışmalar

MADDE 84- (1) Komisyon ile baęlı kuruluşların tařra teřkilatları arasındaki her türlü yazıřma mülki idare amirlikleri aracılıęı ile yapılır.

Dięer ÷lke ve uluslararası kuruluşların muadil kuruluşları ile iliřkiler

MADDE 85- (1) Komisyon, kolluk řikâyetlerine iliřkin olarak oluşturulmuş dięer ÷lke kurum ve kuruluşları, uluslararası kuruluşların ilgili birimleriyle Dıřıřleri Bakanlıęı koordinasyonunda iletiřim ve iř birlięi ierisinde bulunur.

Denetim

MADDE 86- (1) Kolluk hakkındaki ihbar ve řikâyetler üzerine yapılan iřlemler ile merkezi kayıt sisteminin iřleyiřine iliřkin iř ve iřlemler, sıralı kurum amirleri, mülki idare amirleri, baęlı kuruluşların teftiř ve denetim elemanları ile Kurul Bařkanlıęı tarafından yılda en az bir defa denetlenir.

(2) Kurul Bařkanlıęı ile baęlı kuruluşların teftiř ve denetim birimlerinin olaęan teftiř programlarının yürüt÷lmesi sırasında, kolluk hakkındaki ihbar ve řikâyetlere iliřkin yapılan iř ve iřlemler öncelikle teftiř edilir.

(3) Birinci ve ikinci fıkrada kapsamında kolluk řikâyetlerine iliřkin yapılan denetimler sonucunda düzenlenen raporların bir örneęi, yetkili mercilere sunulmalarını takiben en ge yedi iř günü ierisinde Komisyon sekreteryasına gönderilir.

Düzenleyici iřlemler

MADDE 87- (1) Bakanlık, gerek gör÷len hallerde bu Yönetmelięin uygulanmasını saęlamak amacıyla düzenleyici iřlemleri ıkarmakla görevli ve yetkilidir.

Hüküm bulunmayan haller

MADDE 88- (1) Bu Yönetmelikte hüküm bulunmayan hallerde Kanun ve ilgili dięer mevzuat hükümlerine göre iřlem yapılır.

Yetki

MADDE 89- (1) Bu Yönetmelięin uygulanmasından doęabilecek tereddütleri gidermeye ve yönergeler ile dięer usul ve esasları belirlemeye Bakan yetkilidir.

Yürürlük

MADDE 90- (1) Bu Yönetmelik yayımı tarihinde yürürlüęe girer.

Yürütme

MADDE 91- (1) Bu Yönetmelik hükümlerini Cumhurbaşkanı yürütür.

Hukuk Muhakemelerinde Ses ve Görüntü Nakledilmesi Yoluyla Duruşma İcrası Hakkında Yönetmelik

Resmî Gazete Tarihi : 30.06.2021

Resmî Gazete Sayısı : 31527

HUKUK MUHADEMELERİNDE SES VE GÖRÜNTÜ NAKLEDİLMESİ YOLUYLA DURUŞMA İCRASI HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak, Tanımlar, İlkeler ve Standartlar

Amaç ve kapsam

MADDE 1 - (1) Bu Yönetmeliğin amacı, hukuk yargılamalarında aynı anda ses ve görüntü nakledilmesi yoluyla buldukları yerden, tarafın veya vekilinin duruşmaya katılmalarına ve usul işlemleri yapabilmelerine; tanığın, bilirkişinin, uzmanın ve diğer ilgililerin dinlenilmelerine ilişkin usul ve esasları düzenlemektir.

(2) Bu Yönetmelik, hukuk yargılamalarında aynı anda ses ve görüntü nakledilmesi yoluyla duruşma ve usul işlemleri yapılmasına ilişkin hususları kapsar.

Dayanak

MADDE 2 - (1) Bu Yönetmelik, 12/1/2011 tarihli ve 6100 sayılı Hukuk Muhakemeleri Kanununun 149 uncu maddesinin beşinci fıkrasına dayanılarak hazırlanmıştır.

Tanımlar

MADDE 3 - (1) Bu Yönetmelikte geçen;

a) Bakanlık: Adalet Bakanlığını,

b) e-Duruşma: Hukuk yargılamalarında aynı anda ses ve görüntü nakledilmesi yoluyla buldukları yerden, tarafın veya vekilinin duruşmaya katılmalarını ve usul işlemleri yapabilmelerini; tanığın, bilirkişinin, uzmanın ve diğer ilgililerin dinlenilmelerini,

c) e-Duruşma Sistemi: Aynı anda ses ve görüntü nakledilmesi yoluyla duruşma işlemlerini yürütmek amacıyla Bakanlık tarafından Ulusal Yargı Ağı Bilişim Sistemine entegre olarak kurulan ve güvenliği sağlanan sistemi,

ç) Kanun: 12/1/2011 tarihli ve 6100 sayılı Hukuk Muhakemeleri Kanununu,

d) Merkezi Kayıt Sistemi: Mahkemece yargılamanın zorunlu kıldığı hâllerde e-Duruşmanın kaydedilip belirli süre ile saklandığı sistemi,

e) UYAP: Ulusal Yargı Ağı Bilişim Sistemini,

ifade eder.

İlkeler

MADDE 4 - (1) Bu Yönetmeliğin uygulanmasında hukuk yargılamasına hâkim olan tasarruf, taraflarca getirilme, taleple bağıllık, aleniyet ve usul ekonomisi ilkeleri, dürüst davranma ve doğruyu söyleme yükümlülüğü, hukuki dinlenilme hakkı, Türk Hukukunun resen uygulanması, hâkimin davayı aydınlatma ödevi ile yargılamanın sevk ve idaresine ilişkin ilkelerin yanı sıra aşağıdaki ilkeler göz önüne alınır:

a) Bilgi güvenliğinin sağlanması.

b) Kişisel verilerin korunması.

c) Hizmet kalitesinin sağlanması.

ç) Ulusal ve uluslararası standartların sağlanması.

e-Duruşma Sisteminin standartları

MADDE 5 - (1) e-Duruşmada görüntü ile ses aynı anda güvenli bir şekilde nakledilir.

(2) Görüntü, ilgilinin yüz ifadelerini, vücut hareketlerini, tavır ve davranışlarını gözlemlemeye; ses, ilgilinin duygularını anlamaya, söylediklerini anlaşılır ve net şekilde dinlemeye imkân verecek nitelikte olur.

(3) e-Duruşma sırasında, bilgi, belge ve deliller UYAP üzerinden anında iletilebilir.

İKİNCİ BÖLÜM

e-Duruşma, Talep ve Değerlendirilmesi

e-Duruşma

MADDE 6 - (1) Hukuk yargılamalarında aynı anda ses ve görüntü nakledilmesi yoluyla, taraf veya vekili bu Yönetmelikte belirlenen yerden duruşmaya katılabilir ve usul işlemleri yapabilir; tanık, bilirkişi, uzman ve diğer ilgililer dinlenilebilir.

Talep üzerine e-Duruşma

MADDE 7 - (1) Taraflardan birinin talebi üzerine; mahkeme, talep eden tarafın veya vekilinin, bu Yönetmelikte belirlenen yerden duruşmaya e-Duruşma Sistemi yoluyla katılmalarına ve usul işlemleri yapabilmelerine karar verebilir.

(2) Taraflardan birinin talebi üzerine; mahkeme tanığın, bilirkişinin veya uzmanın bu Yönetmelikte belirlenen yerden e-Duruşma Sistemi yoluyla dinlenilmesine karar verebilir.

e-Duruşma talep ve usulü

MADDE 8 - (1) Taraflardan biri veya vekili, duruşmaya e-Duruşma Sistemi yoluyla katılmayı, usul işlemleri yapmayı ya da tanığın, bilirkişinin veya uzmanın e-Duruşma Sistemi yoluyla dinlenilmesini gerekçesiyle birlikte mahkemeden talep edebilir.

(2) e-Duruşma, UYAP mobil uygulamaları, avukat veya vatandaş portalı üzerinden duruşma gününden en az iki iş günü önce mahkemesinden talep edilir.

e-Duruşma talebinin değerlendirilmesi

MADDE 9 - (1) e-Duruşma talebi hakkında hâkim, duruşma gününden en az bir iş günü önce kabul veya ret hususunda karar verir. Bu karar kesindir.

(2) Aşağıdaki sebeplerden birinin bulunması durumunda e-Duruşma talebi gerekçesi gösterilmek suretiyle reddedilebilir:

a) Talebin süresinde yapılmaması.

b) Talebin hakkın kötüye kullanılması veya yargılamayı sürüncemede bırakma amacı taşıması.

c) e-Duruşma yapılmasını zorlaştıran hukuki, fiilî veya teknik engellerin bulunması.

(3) Hastalığı, yaşlılığı veya engelliliği sebebiyle mahkemeye bizzat gelmesi durumunda zorluk yaşaması muhtemel olan taraf, tanık, bilirkişi, uzman ve diğer ilgililerin talepleri hâlinde öncelikle e-Duruşma Sistemi yoluyla dinlenilmelerine karar verilir.

(4) e-Duruşma talebinin kabulüne veya reddine ilişkin karar, UYAP üzerinden veya diğer usullerle talepte bulunana bildirilir.

Resen e-Duruşma

MADDE 10 - (1) Mahkeme; tanığın, bilirkişinin veya uzmanın e-Duruşma Sistemi yoluyla dinlenilmesine resen karar verebilir.

(2) Mahkeme; tarafların üzerinde serbestçe tasarruf edemeyecekleri dava ve işlerde ilgililerin, e-Duruşma Sistemi yoluyla dinlenilmesine resen karar verebilir.

(3) İsticvap olunacak veya yemin edecek taraf, mahkemenin bulunduğu il dışında oturuyor ve mahkemeye bizzat gelemiyor ise öncelikle e-Duruşma Sistemi yoluyla isticvap olunur veya yemin ettirilir.

(4) Mahkemece, e-Duruşma Sistemi yoluyla dinlenilmesine karar verilen kişiye gönderilecek meşruhatlı davetiyeye ayrıca e-Duruşmaya ne şekilde katılacağı da yazılır.

ÜÇÜNCÜ BÖLÜM

e-Duruşmaya Katılma, e-Duruşmanın İcrası, Düzeni ve Kayıt

e-Duruşmaya katılımın sağlanabileceği yer

MADDE 11 - (1) e-Duruşma talep eden taraf vekili, avukatlık bürosundan, baro tarafından bu amaç için belirlenen bölümden, adliyede bu amaca tahsis edilen yerden veya beşinci fıkradaki şartları taşıyan başkaca uygun bir yerden duruşmaya katılabilir.

(2) e-Duruşma talep eden veya e-Duruşma Sistemi yoluyla isticvap olunacak ya da yemin edecek taraf ile mahkemece e-Duruşma Sistemi yoluyla dinlenilmesine karar verilen tanık, bilirkişi, uzman ve diğer ilgililer buldukları yerdeki adliye veya ceza infaz kurumlarında bu amaca tahsis edilen yerden duruşmaya katılabilir.

(3) İsticvap olunacak veya yemin edecek olan hariç, taraf, vekili ile birlikte birinci fıkrada belirtilen yerlerden duruşmaya katılabilir.

(4) Hastalığı, yaşlılığı veya engelliliği sebebiyle; e-Duruşma Sistemi yoluyla duruşmaya katılmasına ve usul işlemleri yapabilmesine karar verilen taraf ile e-Duruşma Sistemi yoluyla dinlenilmesine karar verilen tanık, bilirkişi, uzman veya diğer ilgililer buldukları mesken ya da kurumdan duruşmaya katılabilir.

(5) e-Duruşmaya katılımın sağlanacağı yerin, her türlü etki ve yönlendirmeden uzak, ilgilinin yüz ifadelerini, vücut hareketlerini, tavır ve davranışlarını gözlemlemeye, duygularını anlamaya ve söylediklerini net bir şekilde dinlemeye imkân sağlayacak nitelikte olması gerekir.

e-Duruşmaya katılacakların kimlik tespiti

MADDE 12 - (1) e-Duruřmaya katılan taraf vekilinin kimlik tespiti; güvenli elektronik imza veya mobil imza ile UYAP kayıtları ve benzeri yöntemler kullanılarak mahkemece yapılır.

(2) Mahkemece e-Duruřmaya katılmasına karar verilen taraf, tanık, bilirkiři, uzman ve diđer ilgililerin kimlik tespiti; buldukları yerdeki adliye veya ceza infaz kurumunda e-Duruřma için tahsis edilen yerde görevlendirilecek yazı iřleri müdürü, zabıt kâtabi veya ceza infaz kurumu görevlisi tarafından yapılır ve bu hususta bir tutanak düzenlenir.

(3) Vekili ile birlikte 11 inci maddenin birinci fıkrasında belirtilen yerlerden e-Duruřmaya katılan tarafın kimlik tespiti, UYAP kayıtları incelenerek veya benzeri yöntemler kullanılarak mahkemece yapılır.

(4) Hastalığı, yaşlılığı veya engelliliğı sebebiyle bulunduğı mesken veya kurumdan e-Duruřmaya katılan taraf, tanık, bilirkiři, uzman ve diđer ilgililerin kimlik tespiti, güvenli elektronik imza veya mobil imza kullanılarak yapılır.

e-Duruřma icrası

MADDE 13 - (1) e-Duruřma, mahkeme huzurunda yapılan duruřma ile aynı hukuki sonuçları doğurur.

(2) Birden fazla vekil ile takip edilen dosyalarda e-Duruřmaya, ancak talepte bulunan ve talebi kabul edilen vekiller katılabilir.

(3) e-Duruřma Sistemi yoluyla beyanda bulunan tarafın, vekilin ve diđer ilgililerin sözlü açıklamaları, Kanunun 154 üncü maddesinde belirtilen usul ve esaslara göre zabıt kâtabi aracılığıyla tutanağı yazdırılır.

(4) e-Duruřma Sistemi yoluyla duruřmaya katılan taraf veya vekilince davaya son veren feragat, kabul ve sulhe ilişkin beyanda bulunulması hâlinde, mahkemece yeni bir duruřma günü tayin edilir ve tayin edilen günde feragat, kabul ve sulhe ilişkin bu iřlem mahkeme huzurunda yenilenerek, duruřma tutanağı beyanda bulunan tarafından imza edilirse geçerli hâle gelir.

(5) e-Duruřma Sistemi yoluyla beyanda bulunan tarafın, vekilin veya ilgililerin imzasının alınması gereken diđer durumlarda, mahkemece düzenlenen ve güvenli elektronik imza ile imzalanan duruřma tutanağı, e-Duruřmanın yapıldığı adliyeye elektronik ortamda gönderilir. e-Duruřmaya tahsis edilen yerde görevlendirilen yazı iřleri müdürü veya zabıt kâtabi elektronik ortamda gelen duruřma tutanağının ilgili kısmına beyanda bulunanın imzasını alır ve evrakı tarayarak sistem

üzerinden mahkemesine geri gönderir. Ayrıca el yazısıyla imzalanmış tutanak aslı da dosyasına, masrafı talep edenin yatırmış olduğu avanstaki karşılanarak posta yoluyla gönderilir.

(6) e-Duruşma Sistemi yoluyla beyanda bulunan tarafın, vekilin veya ilgililerin imzası, UYAP'a entegre olmuş güvenli elektronik imza ile alınabilir.

(7) e-Duruşmaya katılan taraf veya vekili ile dinlenen bilirkişi, uzman ve diğer ilgililer, UYAP üzerinden belge iletebilir.

(8) e-Duruşma esnasında ses ve görüntü naklinin aynı anda sağlanamaması veya yaşanan kesintinin beyanların anlaşılmasını güçleştirmesi durumunda e-Duruşma yeniden açılır. Söz konusu aksaklığın devam etmesi hâlinde gerekçesi belirtilerek e-Duruşma sonlandırılır ve bu husus tutanağa geçirilir.

(9) Taraf veya vekilin kusuru olmaksızın teknik sebeplerden dolayı e-Duruşmanın yapılamaması hâlinde, ilgili taraf veya vekil yönünden Kanunun 150 nci maddesinin birinci fıkrası uygulanmaz.

(10) e-Duruşma öncesinde veya e-Duruşma sırasında ortaya çıkan teknik sorunlar ve bu sorunların kaynağı, istem hâlinde Bakanlık tarafından mahkemeye bildirilir.

e-Duruşma düzeni

MADDE 14 - (1) e-Duruşma düzeni, mahkeme huzurunda yapılan duruşma düzeniyle aynı usul ve esaslara tabidir.

(2) e-Duruşma sırasında fotoğraf çekilemez ve hiçbir şekilde ses ve görüntü kaydı yapılamaz. Ancak, yargılamanın zorunlu kıldığı hâllerde, mahkemece kayıt yapılabilir. Kayıt ve yayın yasağına aykırı davranan kişi hakkında 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 286 nci maddesi hükümleri uygulanır.

Kayıt alınması ve saklanması

MADDE 15 - (1) Mahkeme, yargılamanın zorunlu kıldığı hâllerde, gerekçesini belirterek e-Duruşmanın kayıt altına alınmasına karar verebilir.

(2) e-Duruşma Sistemi ile elde edilen kayıtlar, mahkemece e-Duruşmanın yönetildiği bilgisayarda veya veri depolayabilen ağıta aktararak dosyasında saklanmak üzere Merkezi Kayıt Sisteminde iki hafta süre ile muhafaza edilir. Süre sonunda Merkezi Kayıt Sistemindeki bu veriler geri döndürülemeyecek şekilde silinir.

(3) Bu şekilde alınan kayıtlar mahkemenin ve ilgili kişilerin açık izni olmadıkça hiçbir yerde yayımlanamaz.

DÖRDÜNCÜ BÖLÜM

Çeşitli ve Son Hükümler

e-Duruşma Sisteminin kurulması ve idamesi

MADDE 16 - (1) Bakanlık, e-Duruşma Sistemini kurar, geliştirir, sistemin güvenliğini, bakım ve idamesini sağlar.

(2) e-Duruşma Sisteminin etkin, verimli ve güvenli bir şekilde yürütülmesi için kullanılacak sistemler ve cihazlar hakkındaki teknik kriterlere ilişkin usul ve esaslar Bakanlık tarafından belirlenir.

(3) Bakanlık, önceden bildirim yapmak koşuluyla, e-Duruşma Sisteminin idamesi, güncellenmesi ve bakımına ilişkin işlemleri yerine getirmek için süreli veya süresiz kesinti yapabilir.

(4) Bakanlık, e-Duruşma Sisteminin kurulması, idamesi ve geliştirilmesinde kamu veya özel kurum ya da kuruluşlarla iş birliği yapabilir.

e-Duruşmaya katılanın yükümlülükleri

MADDE 17 - (1) e-Duruşmaya katılanın yükümlülükleri şunlardır:

- a) Bakanlık tarafından belirlenen teknik kriterleri sağlamak.
- b) Bulunduğu yerin e-Duruşma Sistemi ile dinlenilmeye elverişli ve güvenli olmasını sağlamak.
- c) Mahkemece belirlenen gün ve saatte, e-Duruşmaya katılacağı yer ve e-Duruşma Sisteminde hazır bulunmak.

Geçiş hükmü

GEÇİCİ MADDE 1 - (1) Bu Yönetmelikte düzenlenen ve elektronik ortamda yapılması gerekmekte birlikte henüz UYAP'ta bulunmayan işlemlere ilişkin hükümler, gerekli yazılım çalışması tamamlandıktan sonra uygulanır.

Yürürlük

MADDE 18 - (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 19 - (1) Bu Yönetmelik hükümlerini Adalet Bakanı yürütür.

**Yolcu Gemilerinin Emniyetine ve Gemilerdeki Yolcuların Kayıt Altına Alınmasına İlişkin
Yönetmelik**

Resmî Gazete Tarihi : 12.12.2007

Resmî Gazete Sayısı : 26728

**YOLCU GEMİLERİNİN EMNİYETİNE VE GEMİLERDEKİ YOLCULARIN KAYIT ALTINA
ALINMASINA İLİŞKİN YÖNETMELİK**

Amaç

MADDE 1 - (1) Bu Yönetmelik; kabotaj hatlarında çalışan yeni ve mevcut yolcu gemileri ile yüksek hızlı yolcu gemilerinde; can ve mal emniyetini sağlamak, bu gemilerin tabi olduğu kuralları uluslararası sefer yapan yolcu gemilerinin kuralları ile uyumlaştırmak, yolcu gemilerindeki yolcular ile mürettebatın güvenliğine ve kurtarılmalarına ilişkin imkânları geliştirmek, oluşabilecek kazalarda arama ve kurtarma faaliyetlerinin ve kazanın olumsuz sonuçlarıyla mücadelenin daha etkin bir şekilde yapılmasını sağlamak amacıyla hazırlanmıştır.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, liman sınırlarını aşmak suretiyle kabotaj seferi yapan;

- a) Yeni yolcu gemilerini,
 - b) Boyları 24 metre ve daha büyük olan mevcut yolcu gemilerini,
 - c) Yüksek hızlı yolcu gemilerini,
- kapsar.

(2) Aşağıda belirtilen gemiler bu Yönetmelik kapsamı dışındadır.

- a) Yolcu gemileri;
 - 1) Silahlı kuvvetlere ait gemiler ile asker taşımaya tahsisli gemiler,
 - 2) Makine ile yürütülmeyen gemiler,
 - 3) Çelik veya eşdeğeri dışındaki malzemelerden yapılan ve Yüksek Hızlı Tekneler (Resolution MSC.36(63)) veya Dinamik Destekli Tekneler (Resolution A.373(X)) ile ilgili standartların kapsamına girmeyen gemiler,

4) İlkel yöntemlerle inşa edilen ahşap tekneler,

5) 1965 yılından önce dizayn edilen ve orijinal malzemesiyle inşa edilmiş olan; orijinal veya kopya tarihî gemiler,

6) Teknik özellikleri gereği veya isteğe bağlı olarak tekneyi sevk ve idare edenden başka mürettebatı bulunmayan ve ticari amaçla onikiye kadar (oniki dâhil) yolcu taşıyabilen gezi tekneleri,

(b) Yüksek hızlı gemiler;

1) Silahlı kuvvetlere ait gemiler ile asker taşımaya tahsisli gemiler,

2) Teknik özellikleri gereği veya isteğe bağlı olarak tekneyi sevk ve idare edenden başka mürettebatı bulunmayan ve ticari amaçla onikiye kadar (oniki dâhil) yolcu taşıyabilen yüksek hızlı gezi gemileri.

(3) Bu Yönetmeliğin üçüncü bölümü aşağıdaki belirtilenler dışındaki denizde çalışan tüm yolcu gemilerini kapsar.

a) Silahlı kuvvetlere ait gemiler ile asker taşımaya tahsisli gemiler,

b) Teknik özellikleri gereği veya isteğe bağlı olarak tekneyi sevk ve idare edenden başka mürettebatı bulunmayan ve ticari amaçla onikiye kadar (oniki dâhil) yolcu taşıyabilen gezi tekneleri.

Dayanak

MADDE 3 - (1) Bu Yönetmelik;

a) 10/8/1993 tarihli ve 491 sayılı Denizcilik Müsteşarlığının Kuruluş ve Görevleri Hakkında Kanun Hükmündeki Kararnamenin 2 nci maddesinin (c) bendi ile 10/6/1946 tarihli ve 4922 sayılı Denizde Can ve Mal Koruma Hakkında Kanun hükümlerine dayanılarak,

b) İlgili uluslararası sözleşmeler ve kurallar paralelinde,

hazırlanmıştır.

(...)

ÜÇÜNCÜ BÖLÜM

Yolcu Gemilerinde Seyahat Eden Kişilerin Kaydedilmesi

Zorunluluk

MADDE 16 - (1) Herhangi bir yerdeki Türk yolcu gemileri ile Türk limanlarından veya Türk limanlarına kabotaj seferleri veya uluslararası seferler yapan diğer yolcu gemilerinde bulunan kişilerin sayılması ve bildirilmesi zorunludur.

(2) Bir Türk limanından kalkacak her yolcu gemisindeki kişiler, yolcu gemisi hareket etmeden önce sayılır ve gemideki kişilerin sayısı, yolcu gemisinin kaptanına ve şirketin yolcu kayıt görevlisine veya aynı işlevi gören kara esaslı şirket sistemine bildirilir.

Yolcu kayıtları

MADDE 17 - (1) Bir Türk limanından kalkarak, kalkış noktasından itibaren 20 milden fazla mesafeye sefer yapacak her yolcu gemisinde bulunan kişilere ilişkin aşağıdaki bilgiler kaydedilir.

a) Gemideki kişilerin soyadları,

b) Bu kişilerin isimleri,

c) Cinsiyetleri,

ç) Her kişinin ait olduğu yaş kategorilerinin (yetişkin, çocuk veya bebek) veya yaşlarının ya da doğum yıllarının kayıtları,

d) Uyrukları,

e) Yolcuların kendi istekleri olması hâlinde, acil durumlarda özel ilgi veya yardım gerekliliği hakkında bilgiler.

(2) Bu bilgiler hareketten önce toplanır ve yolcu gemisinin hareketinden en fazla otuz dakika sonra şirketin yolcu kayıt görevlisine veya aynı işlevi gören kara esaslı şirket sistemine bildirilir.

(3) İdare, birinci fıkrada belirtilen 20 millik eşiği azaltmaya yetkilidir.

Bilgilerin sağlanması

MADDE 18 - (1) Üçüncü bir ülkede bulunan bir limandan kalkarak Türkiye içinde veya herhangi bir Avrupa Birliği üyesi ülke içinde yer alan bir limana giden bir yolcu gemisinin işleticisi, 16 ncı ve 17 nci maddede belirtilen hükümlere uygunluğun sağlanmasından ve belirtilen bilgilerin, gerektiği takdirde, arama ve kurtarma faaliyetleri ve kazanın olumsuz sonuçları ile mücadele amacıyla belirlenmiş otoriteye verilmek üzere toplanmasından ve muhafaza edilmesinden sorumludur.

(2) Türkiye dışında bulunan bir limandan kalkarak bir Türk limanına gelen bir Türk gemisine, ilgili SOLAS-1974 Sözleşmesi hükümleri çerçevesinde İdarenin yolcu bilgilerine ait bir muafiyet veya istisna vermesi hâlinde, bu muafiyet ve istisnalar sadece bu Yönetmeliğin 21 inci maddesinde belirtilen muafiyetler veya istisnalar çerçevesinde yapılabilir.

Gemi kaptanının sorumluluğu

MADDE 19 - (1) Bir yolcu gemisinin bir Türk limanından kalkışından önce gemi kaptanı, gemideki yolcu sayısının geminin taşımasına izin verilen yolcu sayısından fazla olmamasını ve yolcuların uygun stabilite kriterlerine uygun olarak taşınmasını sağlar.

Yolcu bilgilerinin kaydedilmesi

MADDE 20 - (1) Bir yolcu gemisinin işletim sorumluluğunu üzerine alan her şirket;

a) Yolcu bilgilerinin kaydedilmesiyle ilgili olarak 22 nci maddeye uygun bir kayıt sistemi kurmak zorundadır.

b) Acil bir durum oluştuğunda veya bir kazanın sonuçları ile mücadelede, bu bilgilerin muhafazasından ve iletilmesinden sorumlu bir yolcu kayıt görevlisi belirlemiş olmalıdır.

(2) Şirket; bu Yönetmelikte istenilen bilgilerin, acil bir durumda veya bir kazanın sonuçları ile mücadelede arama ve kurtarma amacıyla, belirlenmiş otoriteye iletmeye devamlı olarak hazır olmasını sağlamalıdır.

(3) 17 nci maddeye göre toplanan kişisel veriler, bu Yönetmeliğin amacı için gerekenden fazla saklanmamalıdır.

(4) Şirket; sefer sırasında meydana gelebilecek acil durumlarda kendisi için özel ilgi veya yardım gerekliliğini bildirmiş bulunan kişilerle ilgili bilgilerin doğru olarak kaydedilmesini ve yolcu gemisinin hareketinden önce gemi kaptanına bildirilmesini sağlar.

İstisna ve muafiyetler

MADDE 21 - (1) İdare, sadece korumalı deniz alanlarında olmak üzere;

a) Uğranılan limanlar arasındaki mesafe bir saatten daha kısa olan düzenli seferlerde çalışan yolcu gemilerini, 16 nci maddede belirtilen sorumluluktan muaf tutabilir.

b) Ara uğraklar olmaksızın, iki liman arasında veya bir limandan kalkarak aynı limana gelmek üzere sefer yapan yolcu gemilerini, 17 nci maddede belirtilen sorumluluktan muaf tutabilir.

(2) İdare, kara esaslı seyir yardım hizmetlerinin ve güvenilir hava tahminlerinin sağlanması ve uygun ve yeterli arama ve kurtarma imkânlarının birlikte mevcut olması koşuluyla; bu Yönetmeliğin uygulanmasında zorluklar bulunduğunu değerlendirdiği hâllerde; iki metreyi aşan belirgin dalga yüksekliğinin yıllık olasılığının %10'dan daha az olduğu kabotaj hatlarında ve alanlardaki düzenli seferlerde;

a) Seferin, kalkış noktasından itibaren yaklaşık olarak otuz mili aşmaması hâlinde veya,

b) Servisin temel amacının fiziksel nedenlerle birbirinden uzakta bulunan yerleşim yerleri arasında mutlak bağlantı sağlamaya yönelik olduğu hâllerde, 17 nci maddede belirtilen bilgilerle ilgili sorumluluktan kısmen veya tamamen istisna getirebilir.

(3) İdare, muafiyet tanınması veya istisna getirilmesine dair kararını, talep hâlinde gerekçeleri ile birlikte ilgili kuruluşlara bildirir.

(4) İdare, bu Yönetmelik hükümleri çerçevesinde; Türk limanlarından sefer yapan ve SOLAS-1974 Sözleşmesine taraf olan ve SOLAS-1974 Sözleşmesinin ilgili hükümlerine göre bu muafiyetlerin uygulanmasına uygun olmayan herhangi bir yolcu gemisine muafiyet veya istisna sağlayamaz.

Kayıt sistemi

MADDE 22 - (1) Şirketler tarafından oluşturulan kayıt sistemi İdare tarafından onaylanır. İdare, oluşturulan kayıt sisteminin doğru olarak uygulanması hususunda, Türkiye dâhilinde program dışı denetimler yapabilir. Şirketler, bu Yönetmelikte istenilen bilgileri talep edildiğinde ilgili ülkenin belirlenmiş otoritesine bildirmek zorundadır.

(2) Şirketler tarafından oluşturulacak kayıt sistemleri aşağıdaki fonksiyonel gerekleri sağlamış olmalıdır.

a) Okunabilirlik: Gerekli veriler kolayca okunabilecek düzende olmalıdır.

b) Hazır Bulunma: Gerekli veriler, ilgili belirlenmiş otoritelere sunulmak üzere hazır bulundurulmalıdır.

c) Kolaylık: Sistem, gemiye binen ve/veya gemiden inen yolcular için aşırı gecikmeye neden olmayacak şekilde tasarlanmalıdır.

ç) Güvenlik: Veriler, kazara veya yasa dışı olarak imhalar veya kayıplara ve yetkisiz değiştirmelere, ifşaata veya ulaşımlara karşı uygun şekilde korunmalıdır.

d) Benzerlik: Sistemler, aynı veya benzer hatlarda benzer olarak belirlenmeli, farklı şekilde belirlenmesinden kaçınılmalıdır.

(...)

Eczacılar ve Eczaneler Hakkında Yönetmelik

Resmî Gazete Tarihi : 12.04.2014

Resmî Gazete Sayısı : 28970

ECZACILAR VE ECZANELER HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı; eczacıların görev, yetki ve sorumluluklarının belirlenmesi, eczanelerin açılması, işletilmesi, nakli, devri ve kapanması ile eczanelerin özellikleri ve eczacılık hizmetlerinin yürütülmesine dâir usûl ve esasları düzenlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, 18/12/1953 tarihli ve 6197 sayılı Eczacılar ve Eczaneler Hakkında Kanuna göre açılmış ve açılacak eczaneler ile eczacılık hizmetlerini ve eczacıları kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 6197 sayılı Kanunun 5 inci, 20 nci ve geçici 4 üncü maddesi ile 11/10/2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 40 ıncı maddesine dayanılarak hazırlanmıştır.

(...)

YEDİNCİ BÖLÜM

Eczanelerin Denetimi ve Kapatılması

Eczane defter ve kayıtları

MADDE 45 - (1) Eczanede satışı yapılan tüm ilaçlar elektronik ortamda kaydedilir. Bu kayıtlar denetimlerde istenilmesi hâlinde sunulmak üzere saklanır.

(2) Eczanelerde teftiş defteri, personel defteri ve stajyer defteri tutulur. Defterler eczacıların bağlı oldukları eczacı odalarından temin edilir ve eczacı odalarına tasdik ettirilir.

Genel Sağlık Sigortası Kapsamında Gelir Tespiti, Tescil ve İzleme Sürecine İlişkin Usul ve Esaslar Hakkında Yönetmelik

Resmî Gazete Tarihi : 28.12.2011

Resmî Gazete Sayısı : 28156

GENEL SAĞLIK SİĞORTASI KAPSAMINDA GELİR TESPİTİ, TESCİL VE İZLEME SÜRECİNE İLİŞKİN USUL VE ESASLAR HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç ve kapsam

MADDE 1 - (1) Bu Yönetmeliğin amacı, 31/5/2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 60 ıncı maddesinin birinci fıkrasının (c) bendinin (1) numaralı alt bendi ile (g) bendi kapsamındaki genel sağlık sigortası yükümlülerinin gelir tespitinin yapılması ve tesciline ilişkin usûl ve esasları düzenlemektir.

Dayanak

MADDE 2 - (1) Bu Yönetmelik, 5510 sayılı Kanun ile 3/6/2011 tarihli ve 633 sayılı Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 11 inci maddesine dayanılarak hazırlanmıştır.

(...)

DÖRDÜNCÜ BÖLÜM

Vakıf Mütevelli Heyeti, Gelir Tespitine Esas Veriler,

Verilerin Değerlendirilmesi

(...)

Gelir tespitine esas veriler

MADDE 14 - (1) Gelir tespitinde, aile bireylerinin harcamaları, taşınır ve taşınmazları ile bunlardan doğan hakları da dikkate alınarak aile içinde kişi başına düşen gelirin aylık tutarı tespit edilir.

(2) Gelir tespit yönteminde, BSYHP üzerinden puanlama formülü esasına göre belirlenecek hane geliri ve kişi başına düşen gelir kullanılır. Puanlama formülünde kullanılacak haneye ilişkin veriler, BSYHP'den ve hane ziyaretinden elde edilen bilgilerden oluşur.

(3) Aile içinde kişi başına düşen gelirin aylık tutarının tespitinde, puanlama formülünün gelir, harcama ve servet verileri dikkate alınarak geliştirilen gelir tespit ölçütleri kullanılır. Puanlama formülünde ekonomik ve sosyal şartların değişmesi nedeniyle Bakanlık ve SGK'nın önerisi ve Sosyal Yardımlaşma ve Dayanışmayı Teşvik Fon Kurulu'nun kararı ile güncellemeler yapılabilir.

(4) Gelir tespiti yöntemi olarak kullanılacak olan puanlama sisteminde ayrıca aşağıdaki unsurlar dikkate alınır:

- a) Kişilere ait taşınır ve taşınmazlar ile bunlardan doğan haklar.
- b) Bankaların muvafakati alınmak suretiyle SGK tarafından Bakanlığa sağlanacak olan aile bireylerinin bankalardaki tüm hesaplarına ilişkin bilgiler.
- c) Sürekli olarak alınan nakdî sosyal yardımlar.

(5) Bakanlık veya SGK tarafından aile bireylerine ilişkin, aile içinde kişi başına düşen geliri etkileyecek diğer unsurların belirlenmesi hâlinde, bu unsurlara göre vakıf personeli tarafından yapılacak tespitler sonucu elde edilen bilgiler de kişilerin gelir tespitinde dikkate alınır.

Verilerin değerlendirilmesi

MADDE 15 - (1) Gelir tespitinde aile bireyleri için 14 üncü maddedeki esaslara göre tespit edilen verilerin değerlendirilmesi 3294 sayılı Kanuna göre il ve ilçelerde yer alan heyetler tarafından yapılır. Gelir tespiti iş ve işlemleri, kişinin gelir tespiti başvurusundan itibaren en geç bir ay içinde tamamlanır.

(2) Gelir tespitinde 14 üncü maddedeki verileri de esas alan puanlama sistemi kullanılır.

(3) Heyet tarafından yapılan değerlendirme sonucu verilen karar ve aileye ilişkin bilgiler, kişi bazlı olarak veri paylaşımını sağlayan elektronik sistem üzerinden SGK'ya bildirilir.

(4) Heyet tarafından verilen gelir tespiti kararları ile kararlara esas veriler ve bunların değerlendirilmesine ilişkin bilgi ve belgeler, gelir tespiti yapılan her bir ailenin vakıfta bulunan hane dosyasında muhafaza edilir.

(5) Gelir tespiti sonucu elde edilen ailenin ortalama aylık geliri, gelir tespitine esas alınan aile bireyi sayısına bölünerek aile içindeki kişi başına düşen gelir tespit edilir.

(...)

ALTINCI BÖLÜM

Çeşitli Hükümler

Verilerin korunması ve sorumluluk

MADDE 19 - (1) Gelir tespitine esas olmak üzere elde edilen veriler ve yaptırılan incelemelere ait raporlar ile gelir tespitine yapılan itiraza ve karara bağlanmasına ilişkin bilgi ve belgeler vakıf tarafından muhafaza edilir.

(2) SGK'nın denetim ve kontrolle görevli memurlarınca yürütülen inceleme ve soruşturmalar dolayısıyla ya da yargı organlarınca ve Bakanlık tarafından talep edilmeleri dışında, gelir tespitine esas olmak üzere elde edilen kişisel veriler ve incelemelere ait raporlar üçüncü kişilere verilemez.

(3) Gelir tespitine esas veri sorgulamaları ile itirazların sonuçlandırılması, bunlara ilişkin yazışmalar ve diğer işlemler Bakanlık, SGK ve vakıf tarafından belirlenen personel tarafından yapılır.

(4) Gelir tespitine esas veriler ve yaptırılan incelemelere ait raporlar ile gelir tespitine itiraza ve karara bağlanmasına ilişkin bilgi ve belgelerin muhafazasından ilgili personel ile bunların bağlı bulunduğu yetkililer sorumludur.

(...)

Bireysel Emeklilik Sistemi Hakkında Yönetmelik

Resmî Gazete Tarihi : 09.11.2012

Resmî Gazete Sayısı : 28462

BİREYSEL EMEKLİLİK SİSTEMİ HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç ve kapsam

MADDE 1 - (1) Bu Yönetmeliğin amacı, kişilerin bireysel emeklilik sistemine girmesine, emeklilik sözleşmesinin düzenlenmesinden sona ermesine kadar geçen süreçte emeklilik sözleşmesine taraf olanların hak ve yükümlülüklerine ve bireysel emeklilik sisteminin işleyişine ilişkin esas ve usulleri düzenlemektir.

Dayanak

MADDE 2 - (1) Bu Yönetmelik 28/3/2001 tarihli ve 4632 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanununa dayanılarak hazırlanmıştır.

(...)

Emeklilik sözleşmesinin asgari içeriği

MADDE 22/D - (1) Bu bölüm kapsamındaki emeklilik sözleşmesinde tarafların hak ve yükümlülükleri yer alır, bu bölümün uygulanmasına esas olmak üzere ücret ödeme günü ve mutabakat süreci belirlenir, ilgililere yapılacak iade ve ödeme esasları, çalışana ait güncel verilerin tutulması ve ilgililere yapılacak bildirimlerin usulü belirlenir. Bu sözleşme ile şirket seçimi ve katkı payının işveren tarafından şirkete aktarılması hariç bu bölüm kapsamındaki yükümlülüklerin şirketlerce yerine getirilmesi kararlaştırılabilir.

(...)

112 Acil Çağrı Merkezleri Kuruluş, Görev ve Çalışma Yönetmeliği

Resmî Gazete Tarihi : 16.05.2014

Resmî Gazete Sayısı : 29002

112 ACİL ÇAĞRI MERKEZLERİ KURULUŞ, GÖREV VE ÇALIŞMA YÖNETMELİĞİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı, büyükşehir belediyesi bulunan illerde valiliğe bağlı olarak kurulan yatırım izleme ve koordinasyon başkanlığı bünyesinde, diğer illerde ise valilikler bünyesinde kurulan acil çağrı merkezlerinin işleyişine dair usul ve esasları düzenlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik; acil çağrı merkezlerinin kuruluş, görev ve çalışmalarına ilişkin usul ve esasları, personelin ve ilgili kurumların görev, yetki ve sorumlulukları ile acil çağrı hizmeti kapsamında yararlanılan her türlü donanımın temin ve kullanımında uyulacak hususları kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 14/2/1985 tarihli ve 3152 sayılı İçişleri Bakanlığı Teşkilat ve Görevleri Hakkında Kanununun 28 inci ve 33 üncü maddeleri ile 10/6/1949 tarihli ve 5442 sayılı İl İdaresi Kanununa dayanılarak hazırlanmıştır.

(...)

Kalite, koordinasyon ve değerlendirme bürosunun görevleri

MADDE 11 - (1) Kalite koordinasyon ve değerlendirme bürosunun görevleri şunlardır:

- Birden fazla kurumu ilgilendiren önemli olayları takip ederek varsa koordinasyonda meydana gelen aksaklıkları ve nedenlerini tespit ederek raporlamak,
- Haberleşme sistemi ve yazılım ile ilgili eksiklik ve aksaklıkları belirleyerek müdürlüğe bildirmek,

- c) Çağrı merkezi ile ilgili basında çıkan haberleri takip etmek, çağrı merkezi müdürünü bilgilendirmek, istenildiği takdirde kamuoyunu aydınlatmak üzere ilgili kurumlar ile koordineli olarak basın bildirisi hazırlayarak müdürlüğe sunmak,
- ç) Sistemin çalışmasıyla ilgili istatistikleri takip etmek, ilgili birimlerin istatistik çalışmalarına yardımcı olmak,
- d) Çağrı merkezinin işleyişiyle ilgili bilgi notları ve brifingleri hazırlayarak müdürlüğe sunmak,
- e) Eğitim amaçlı kullanılacak ses kayıtlarını kişisel verilerin gizliliği ve korunmasına dair mevzuat hükümlerine uygun olarak belirlemek,
- f) İdari veya adli soruşturmaya konu olan vakalarla ilgili sesli ve yazılı kayıtların örneklerini yetkili idari veya adli mercilere teslim etmek üzere çıkartmak,
- g) Çağrı alma teknolojisindeki yenilikler ve çağrı merkezinde kullanılacak yeni teknolojiler konusunda çalışmalar yapmak ve müdürlüğü bilgilendirmek,
- ğ) Kalite yönetim sistemi dokümanlarının kayıtlarını tutmak, ilgili birimlerin kalite standartlarını oluşturma çalışmalarına yardımcı olmak,
- h) Öneri ve şikâyetleri takip etmek ve bu konuda gerekli çalışmaları yapmak,
- ı) Düzenlenecek olan hizmet içi eğitim, seminer ve sosyal faaliyetlere ilişkin iş ve işlemleri yapmak,
- i) Çağrı merkezi müdürü tarafından verilen benzeri diğer iş ve işlemleri yapmak.

(...)

BEŞİNCİ BÖLÜM

Veri Paylaşımı Güvenliği ve Yaptırımlar

Veri paylaşımı ve güvenliği

MADDE 22 - (1) Çağrı merkezlerinde bulunan her türlü kişisel bilgi veya belgenin gizliliği esastır. Çağrı merkezi görevlileri görevleri nedeniyle elde ettikleri bu bilgi veya belgeleri, çağrı merkezi işlemleri dışında ilgili kişinin izni olmadan veya kanunlarla yetkilendirilen ve görevlendirilen merciler ile görevleri ile ilgili olarak muttali olanlar dışında hiçbir kişi ya da kurumla paylaşamazlar.

(2) Çağrı merkezinde hizmet veren kurumların kendi alanlarına ilişkin istatistiki verilere esas ses ve veri kayıtları hizmet gerekleri, hizmetin kalite ve etkinliğini artırmak, personelin performans değerlendirmesini yapabilmek üzere elektronik ortamda ilgili kurumlarla paylaşılabilir. Kişisel verilerin ve özel hayatın gizliliği dikkate alınarak, verilerin güvenliği ilgili birimlerce sağlanır.

(3) Çaęrı merkezine yapılan aramalara iliřkin yazılı ve sesli kayıtlar, vaka adli soruřturmaya konu olduęunda, Cumhuriyet Bařsavcılıęı veya yetkili mahkemesince istenilmesi halinde ve idari soruřturmalarda görevli mufettiřlere veya muhakkiklere verilir. Dięer soruřturmalarda soruřturmayı aan kurumun en st amirinin yazılı talebi zerine verilebilir.

Yaptırımlar

MADDE 23 - (1) Grřme kayıtlarını izinsiz alan, aıklayan veya bařka kiři, kurum ve kuruluřlara yetkili makamın bilgisi, izni dıřında verenler; grevlerle ilgili izinsiz aıklama yapanlar, bilgi ve belgelerin yetkisiz kiřilerin eline gemesinde ihmali, kusuru ve kastı bulunanlar; yerine getirmekle ykml olduęu grevlerini aksatan veya yerine getirmeyenler hakkında gerekli adli ve idari iřlemler derhal bařlatılır.

(2) Çaęrı Merkezini asılsız ihbarda bulunmak suretiyle meřgul ettikleri tespit edilen kiřilere 30/3/2005 tarihli ve 5326 sayılı Kabahatler Kanununa gre il valileri tarafından 250 Trk Lirası idari para cezası verilir. Tekerrr hlinde bu ceza iki katı olarak uygulanır.

(...)

Afet ve Acil Durum Müdahale Hizmetleri Yönetmeliđi

Resmî Gazete Tarihi : 24.02.2022

Resmî Gazete Sayısı : 31760

AFET VE ACİL DURUM MÜDAHALE HİZMETLERİ YÖNETMELİĐİ

BİRİNCİ BÖLÜM

Genel Hükümler

Amaç

MADDE 1- (1) Bu Yönetmeliđin amacı; afet ve acil durumlara müdahalede ihtiyaç duyulacak kapasiteyi ulusal ve yerel düzeyde planlamak, bu kapasitenin olay bölgesine hızlı ve etkin bir şekilde ulaştırılmasını ve kullanılmasını sağlamak, müdahale hizmetlerini ve bu hizmetlerin koordinasyonundan sorumlu ana ve destek çözüm ortaklarının ve yerel düzeyde sorumlu birimlerin, görev ve sorumlulukları ile planlama esaslarını belirlemektir.

Kapsam

MADDE 2- (1) Bu Yönetmelik, afet ve acil durumlarda müdahale hizmetlerini yürütecek bakanlıklar, kamu kurum ve kuruluşları, valilikler, kaymakamlıklar, özel ve özerk kuruluşlar, sivil toplum kuruluşları ile gerçek ve tüzel kişileri, bunların görev ve sorumlulukları ile bunlar arasındaki işbirliđi, koordinasyon ve karşılıklı yardımlaşmaya dair iş ve işlemleri kapsar.

Dayanak

MADDE 3- (1) Bu Yönetmelik, 15/5/1959 tarihli ve 7269 sayılı Umumi Hayata Müessir Âfetler Dolayısıyla Alınacak Tedbirlerle Yapılacak Yardımlara Dair Kanun ve 29/5/2009 tarihli ve 5902 sayılı Afet ve Acil Durum Yönetimi Başkanlıđı ile İlgili Bazı Düzenlemeler Hakkında Kanun hükümleri ile 4 sayılı Bakanlıklara Bağlı, İlgili, İlişkili Kurum ve Kuruluşlar ile Diđer Kurum ve Kuruluşların Teşkilatı Hakkında Cumhurbaşkanlıđı Kararnamesinin 30 ila 54 üncü maddelerine dayanılarak hazırlanmıştır.

(...)

Gizlilik esasları

MADDE 32- (1) Hazırlanacak afet müdahale planları ile bu planlarda yer alacak envanterlerin ve kişisel verilerin paylaşılmasında ilgili mevzuatında öngörülen gizlilik esaslarına riayet edilir.

(...)

Bilgi Teknolojileri ve İletişim Kurumu İdari Yaptırımlar Yönetmeliği

Resmî Gazete Tarihi : 15.02.2014

Resmî Gazete Sayısı : 28914

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU İDARİ YAPTIRIMLAR YÖNETMELİĞİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı, Kurum tarafından uygulanacak idari para cezaları ile diğer yaptırım ve tedbirlere ilişkin usul ve esasları düzenlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik; 4/2/1924 tarihli ve 406 sayılı Telgraf ve Telefon Kanunu, 29/6/2001 tarihli ve 4703 sayılı Ürünlere İlişkin Teknik Mevzuatın Hazırlanması ve Uygulanmasına Dair Kanun, 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu, 4/7/1934 tarihli ve 2559 sayılı Kanunun ek 7 nci maddesi, 10/3/1983 tarihli ve 2803 sayılı Kanunun Ek 5 inci maddesi, 1/11/1983 tarihli ve 2937 sayılı Kanunun 6 ncı maddesi, 4/12/2004 tarihli ve 5271 sayılı Kanunun 135, 136, 137 ve 138 inci maddeleri ile 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu, 13/1/2011 tarihli ve 6102 sayılı Türk Ticaret Kanunu ve Kurum düzenlemeleri de dahil olmak üzere, ilgili mevzuatta yer alan yükümlülüklerin yerine getirilmemesi ve ilgili mevzuata aykırılık halinde uygulanacak yaptırımlara ve bunların uygulanmasına ilişkin usul ve esasları kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 5/11/2008 tarihli ve 5809 sayılı Kanunun 9 uncu, 60 ıncı ve 61 inci maddeleri, 4703 sayılı Kanunun 12 nci maddesi, 5070 sayılı Kanunun 18 inci maddesi ile 5651 sayılı Kanunun 3 üncü, 4 üncü, 5 inci, (Değişik ibare:RG-29/9/2018-30550) 6 ncı, 8 inci ve 10 uncu maddelerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Yönetmelikte geçen;

- a) Bakanlık: Ulaştırma, Denizcilik ve Haberleşme Bakanlığını,
 - b) Bir önceki takvim yılı: İhlalin vukû bulduğu tarihten bir önceki takvim yılını, ihlalin vukû bulduğu tarihin tam olarak tespit edilemediği veya ihlalin devam ettiği durumlarda idari para cezasının uygulanacağı yıldan bir önceki takvim yılını, ihlalin yıllara yaygın olması durumunda ihlalin sona erdiği takvim yılından bir önceki takvim yılını,
 - c) Brüt satışlar: İşletmecinin faaliyetleri çerçevesinde satılan mal ya da hizmetler karşılığında alınan veya tahakkuk ettirilen toplam değerleri kapsayan ve gelir tablosunda "60. Brüt Satışlar" hesabında kaydedilen tutarları,
 - ç) İdari yaptırım: İdari para cezaları ile diğer yaptırım ve tedbirleri,
 - d) İlgili mevzuat: Kurumun görev alanına ilişkin kanun, kanun hükmünde kararname, tüzük, yönetmelik, Bakanlar Kurulu kararı, eki kararlar, tebliğ, Kurul kararları, diğer düzenleyici işlemler, görev sözleşmeleri, imtiyaz sözleşmeleri ve diğer yetkilendirme belgelerini,
 - e) İşletmeci: Yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirketi,
 - f) Kurul: Bilgi Teknolojileri ve İletişim Kurulunu,
 - g) Kurum: Bilgi Teknolojileri ve İletişim Kurumunu,
 - ğ) Net satışlar: Brüt satışlardan, satış indirimlerinin düşülmesi sonucu kalan tutarı,
 - h) Satış indirimleri: Net satış hâsılatına ulaşabilmek için brüt satışlardan indirilmesi gereken satıştan iadeler, satış iskontoları ve diğer indirimleri,
- ifade eder.

(2) Bu Yönetmelikte geçen ve birinci fıkrada yer almayan tanımlar için ilgili mevzuatta yer alan tanım ve kısaltmalar geçerlidir.

İKİNCİ BÖLÜM

İdari Para Cezaları

Yetkilendirmeye ilişkin ihlaller

MADDE 5 - (1) Aşağıda belirtilen hallerde işletmecinin bir önceki takvim yılındaki net satışlarının aşağıda belirtilen oranına kadar idari para cezası uygulanır:

a) İşletmecinin;

1) İmtiyaz sözleşmesi kapsamında kurduğu elektronik haberleşme şebekesi ve tesislerini sözleşme süresinin sonuna kadar iyi, güncel ve çalışır durumda bulundurma yükümlülüğünü yerine getirmemesi,

2) Acil durumlara ve/veya acil yardım çağrı hizmetlerine ilişkin yükümlülüklerini yerine getirmemesi,

3) Yetkilendirmesi kapsamı dışına çıkararak hizmet vermesi veya şebeke ve altyapı kurması ve/veya işletmesi,

4) (Ek:RG-25/5/2019-30784) Yetkilendirme devri, hisse devri veya birleşme veya devralmaya ilişkin yükümlülüklerini yerine getirmemesi,

5) (Ek:RG-25/5/2019-30784) Acentelik ve diğer iş modellerine ilişkin yükümlüklerini yerine getirmemesi,

halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır.

b) İşletmecinin;

1) Şebekesine ilişkin donanım ve yazılım gibi yatırımlarına yönelik olarak yetkilendirmesinde ve/veya ilgili mevzuatta yer alan yükümlülüklerle uymaması,

2) "All Risk" sigortası yaptırma konusundaki yükümlülüklerini yerine getirmemesi,

3) Kapsama alanına ilişkin yükümlülüklerini yerine getirmemesi,

halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde ikisine (%2) kadar idari para cezası uygulanır.

c) İşletmecinin;

1) Rehber ve bilinmeyen numaralar konusundaki yükümlülüklerini yerine getirmemesi,

2) Tüm çalışanlarının mevzuata uygun davranışta bulunması için gerekli olan önlemi almaması ve işin düzenli yürümesini sağlamaması,

3) (Mülga:RG-25/5/2019-30784)

halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde birine (%1) kadar idari para cezası uygulanır.

(2) İşletmecinin birinci fıkrada sayılan fiiller dışında yetkilendirmeye ilişkin ilgili mevzuatı ihlal etmesi halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır.

(3) (Ek:RG-25/5/2019-30784) Bu madde kapsamındaki ihlallerin ilgili mevzuat çerçevesinde ağır kusur oluşturduğunun Kurul tarafından tespiti halinde, işletmecinin yetkilendirmesi fesh/iptal edilir. Bu madde gereği yapılacak fesihlerde, 5809 sayılı Kanununun 60 ıncı maddesinin birinci fıkrası uyarınca Bakanlık görüşü alınması gereken durumlarda Bakanlık görüşü alınır.

Numaralandırmaya ilişkin ihlaller

MADDE 6 - (1) Aşağıda belirtilen hallerde işletmecinin bir önceki takvim yılındaki net satışlarının aşağıda belirtilen oranına kadar idari para cezası uygulanır.

a) İşletmecinin numaralandırma düzenlemeleri çerçevesinde kendisine tahsis edilen numaralar dışında diğer numara kaynaklarından numara kullanması halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde ikisine (%2) kadar idari para cezası uygulanır.

b) İşletmecinin;

1) Ulusal numaralandırma planı kapsamında şebekelerinde gerekli düzenlemeleri yapmaması,

2) Ulusal numaralandırma planında veya kendisine tahsisli numaralarda yapılan değişikliklere ilişkin olarak 27/6/2009 tarihli ve 27271 sayılı Resmî Gazete’de yayımlanan Numaralandırma Yönetmeliği ile diğer ilgili mevzuatta belirtilen yükümlülükleri yerine getirmemesi,

halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde birine (%1) kadar idari para cezası uygulanır.

c) İşletmecinin;

1) Kendisine tahsis edilen veya kullanım izni verilen numaraları, Kurumun izni olmadan bir başkasına kullandırması veya devretmesi,

2) Hizmet türüne göre numara gruplarına yönelik ilgili mevzuatta yer alan düzenlemelere uymaması,

3) Kendisine tahsis edilen numaraları, ulusal numaralandırma planında bulunan diğer numaralarla karışıklığa neden olacak şekilde kullanması,

4) (Mülga:RG-29/9/2018-30550)

halinde işletmecinin bir önceki takvim yılındaki net satışlarının binde beşine (% 0,5) kadar idari para cezası uygulanır.

(2) Kurum gerekli görmesi halinde; idarî para cezalarına ek olarak, Numaralandırma Yönetmeliğinde ve diğer ilgili mevzuatta yer alan tahsisli numaraların geri alınmasına ilişkin hükümleri de uygulayabilir.

(3) (Değişik:RG-29/9/2018-30550) İşletmecinin CLI'a ilişkin ilgili mevzuat hükümlerini ihlal etmesi halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır. İhlalin ilgili mevzuat çerçevesinde ağır kusur oluşturduğunun Kurul tarafından tespiti halinde ise işletmecinin yetkilendirmesi fesh/iptal edilir.

(4) (Ek:RG-29/9/2018-30550) İşletmecinin birinci, ikinci ve üçüncü fıkralarda sayılan fiiller dışında numaralandırmaya ilişkin ilgili mevzuatı ihlal etmesi halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır.

Numara taşınabilirliğine ilişkin ihlaller

MADDE 7 - (1) Aşağıda belirtilen hallerde işletmecinin bir önceki takvim yılındaki net satışlarının aşağıda belirtilen oranına kadar idari para cezası uygulanır:

a) İşletmecinin;

1) Verici konumda iken, numara taşınması konusunda alıcı işletmeciden gelen talebi yerine getirmemesi ve/veya Kurum düzenlemelerine aykırı bir şekilde reddetmesi,

2) Abonenin numara taşıma talebi olmadan, aboneye ait kimlik bilgileri alınmadan veya eksik alınarak taşıma sürecinin başlatılması,

halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde birine (%1) kadar idari para cezası uygulanır.

b) İşletmecinin;

1) Numaranın taşınacağı tarih ve saati numara taşınabilirliğine ilişkin Kurum düzenlemelerine uygun şekilde ilgili taraflara bildirmemesi,

2) Numara taşınabilirliğine yönelik tarife şeffaflığına ilişkin yükümlülüklerini yerine getirmemesi,

3) Numara taşıma işlemi sırasında elde ettiği bilgileri, ilgili abonenin numara taşıma konusundaki talebini geri alması ya da erteleme amacıyla kullanması,

4) Abonenin numara taşıma iptal talebini numara taşınabilirliğine ilişkin Kurum düzenlemelerine uygun olarak yerine getirmemesi,

5) Numara taşınabilirliğinde uygulanacak ücretlere ilişkin Kurum düzenlemelerine uymaması,

- 6) Taşıma sürecinde numara taşınabilirliğine ilişkin Kurum düzenlemelerinde belirtilen sürelere uymaması,
- 7) Taşınmış bir numaranın iadesine ilişkin Kurum düzenlemelerine uymaması,
- 8) Taşınmış numaralara ilişkin çağrı yönlendirme yükümlülüğünü yerine getirmemesi,
- 9) Alıcı konumda iken, kendisine tahsisli olmayan taşınmış bir numaraya ilişkin olarak devir işlemi gerçekleştirilmesi,

halinde işletmecinin bir önceki takvim yılındaki net satışlarının binde beşine (%0,5) kadar idari para cezası uygulanır.

(2) İşletmecinin birinci fıkrada sayılan fiiller dışında numara taşınabilirliğine ilişkin ilgili mevzuatı ihlal etmesi halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır.

Frekans kullanımına ilişkin ihlaller

MADDE 8 - (1) Aşağıda belirtilen hallerde işletmecinin bir önceki takvim yılındaki net satışlarının aşağıda belirtilen oranına kadar idari para cezası uygulanır:

a) İşletmecinin kendisine tahsisli frekanslar dışında frekans kullanması halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde ikisine (%2) kadar idari para cezası uygulanır.

b) İşletmecinin;

- 1) Frekans değişikliği, iptali gibi konulara ilişkin olarak Kurum tarafından istenilen iş ve işlemleri süresi içinde yerine getirmemesi,
- 2) Tahsis edilmiş frekansları Kurumun izni olmaksızın bir başkasına kullandırması veya devretmesi,
- 3) Kendisine tahsis edilen frekansları tahsis amacına uygun olarak kullanmaması,
- 4) Enterferansı önlemeye ilişkin yükümlülüklerini ihlal etmesi,

halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde birine (%1) kadar idari para cezası uygulanır.

(2) İşletmecinin birinci fıkrada sayılan fiiller dışında frekans kullanımına ilişkin ilgili mevzuatı ihlal etmesi halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır.

Tahakkuka esas bildirimlere ilişkin ihlaller

MADDE 9 - (1) Tahakkuka esas bildirimlerin Kuruma süresi içinde ve eksiksiz olarak yapılmaması veya yanlış bildirimde bulunulması durumunda işletmecinin bir önceki takvim yılındaki net satışlarının yüzde birine (%1) kadar idari para cezası uygulanır.

(2) Tahakkuka esas bildirimlerin yanıltıcı olması durumunda işletmecinin bir önceki takvim yılındaki net satışlarının yüzde ikisine (%2) kadar idari para cezası uygulanır.

Erişim ve ara bağlantıya ilişkin ihlaller

MADDE 10 - (1) Aşağıda belirtilen hallerde ilgili mevzuat çerçevesinde yükümlü işletmecinin bir önceki takvim yılındaki net satışlarının aşağıda belirtilen oranına kadar idari para cezası uygulanır:

a) İşletmecinin;

- 1) Erişim sağlamaya ilişkin yükümlülüklerini,
- 2) Arabağlantı sağlamaya ilişkin yükümlülüklerini,
- 3) Ayırıştırma sağlamaya ilişkin yükümlülüklerini,
- 4) Hesap ayrımı ve maliyet muhasebesine ilişkin yükümlülüklerini,
- 5) Ortak yerleşime ilişkin yükümlülüklerini,
- 6) Tesis paylaşımına ilişkin yükümlülüklerini,
- 7) Taşıyıcı seçimine ilişkin yükümlülüklerini,
- 8) Uzlaştırma prosedürü kapsamında geçici ücret dâhil Kurum tarafından belirlenen hüküm, koşul ve ücretlere uymaması veya söz konusu hüküm, koşul ve ücretlerin uygulanmasına ilişkin yükümlülüklerini,

9) Referans erişim tekliflerine ve şeffaflığa ilişkin yükümlülüklerini,

yerine getirmemesi veya haklı bir neden olmaksızın geciktirmesi halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde ikisine (%2) kadar idari para cezası uygulanır.

b) İşletmecinin;

- 1) Kendisinden erişim veya arabağlantı hizmeti talep eden işletmecileri talep etmedikleri bir hizmeti almak zorunda bırakması,
- 2) İşletmeciler arasında ayırım gözetmeme yükümlülüğünü ihlal etmesi,
- 3) Erişim tarifelerini 8/9/2009 tarihli ve 27343 sayılı Resmî Gazete’de yayımlanan Erişim ve Arabağlantı Yönetmeliği hükümlerine aykırı olarak uygulaması,

halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde birine (%1) kadar idari para cezası uygulanır.

(2) Aşağıda belirtilen hallerde işletmecinin bir önceki takvim yılındaki net satışlarının aşağıda belirtilen oranına kadar idari para cezası uygulanır:

a) İşletmecinin, erişim sağlanması kapsamındaki bilgilerin gizliliğine ilişkin yükümlülüklerini ihlal etmesi halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde birine (%1) kadar idari para cezası uygulanır.

b) İşletmecinin, erişim sözleşmelerinin Kuruma sunulması veya mevzuata aykırı hükümlerinin düzeltilmesi veya sözleşmelerin aleniyetine ilişkin yükümlülüklerini yerine getirmemesi halinde bir önceki takvim yılındaki net satışlarının binde beşine (%0,5) kadar idari para cezası uygulanır.

(3) İşletmecinin birinci ve ikinci fıkralarda sayılan fiiller dışında erişim ve ara bağlantıya ilişkin ilgili mevzuatı ihlal etmesi halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır.

Son kullanıcı tarifelerine ilişkin ihlaller

MADDE 11 - (1) Aşağıda belirtilen hallerde işletmecinin bir önceki takvim yılındaki net satışlarının aşağıda belirtilen oranına kadar idari para cezası uygulanır:

a) İşletmecinin;

1) Kurumun tarifeleri ve bu tarifelerin kapsam, süre ve koşullarını izleme ve inceleme sürecinde ve/veya sonucunda öngördüğü tarifenin veya tarifeye ilişkin genel hükümlerin düzeltilmesinin sağlanması, tarifenin uygulanmasının geçici olarak durdurulması veya tarifenin yürürlükten kaldırılması şeklindeki tedbirleri uygulamadığının tespit edilmesi,

2) Tarifelerin aşırı fiyatları içerecek şekilde uygulanması, rekabetin kısıtlanmasını hedefleyen fiyat indirimlerini ihtiva etmesi, haklı olmayan nedenlerle tüketiciler arasında ayırım yapılmasına yol açması ve bir hizmetin maliyetinin diğer bir hizmetin ücretiyle desteklenmesi suretiyle çapraz sübvansiyona neden olması gibi ihlallerinin tespit edilmesi,

halinde bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır.

b) İşletmecinin;

1) İlgili mevzuat kapsamında tarifeleri bildirim usulüne tabi olan herhangi bir elektronik haberleşme hizmetini bildirim yapmadan sunduğunun veya uygulanan tarifede Kuruma bildirimde bulunmaksızın değişiklik yaptığının tespit edilmesi,

2) Tarifelerine yönelik olarak Kurum tarafından belirlenen alt ve/veya üst sınıra uymadığının tespit edilmesi,

3) Tarifeleri maliyet esaslı yöntem veya tavan fiyat yöntemi çerçevesinde onaya tabi olan herhangi bir elektronik haberleşme hizmetini, onaylanmamış tarife ile sunduğunun tespit edilmesi,

4) Yetkilendirmesinde, görev veya imtiyaz sözleşmelerinde yer alan tarifelere ilişkin hükümlere uymaması,

halinde bir önceki takvim yılındaki net satışlarının yüzde ikisine (%2) kadar idari para cezası uygulanır.

c) İşletmecinin;

1) İlgili mevzuat kapsamında tarifelerin kamuoyuna duyurulmasına dair yükümlülüklerine ve/veya buna ilişkin Kurumca belirlenen süreye riayet etmediğinin tespit edilmesi,

2) İlgili mevzuatta öngörülen zorunlu tarife teklifini Kuruma onay için sunmaması veya onaylandıktan sonra gerekçesiz bir şekilde yürürlüğe koymaması,

halinde bir önceki takvim yılındaki net satışlarının yüzde birine (%1) kadar idari para cezası uygulanır.

(2) İşletmecinin, tarifelerinin kamuoyuna duyurulması veya uygulanması aşamasında tarifelerinin adında değişiklik yapmadan önce Kurumu bilgilendirmediğinin tespit edilmesi halinde bir önceki takvim yılındaki net satışlarının binde beşine (%0,5) kadar idari para cezası uygulanır.

(3) İşletmecinin birinci ve ikinci fıkralarda sayılan fiiller dışında tarifelere ilişkin ilgili mevzuatı ihlal etmesi halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır.

Tüketici haklarına ilişkin ihlaller

MADDE 12 - (1) Aşağıda belirtilen hallerde işletmecinin bir önceki takvim yılındaki net satışlarının belirtilen oranına kadar idari para cezası uygulanır:

a) İşletmecinin;

1) Tüketicilere yaptığı bilgilendirmelerin yanlış ya da yanıltıcı olması,

- 2) Doğru faturalama yapmaya ilişkin ilgili mevzuatta yer alan yükümlülüğünü yerine getirmemesi,
 - 3) Hizmetin kısıtlanması ve durdurulmasına ilişkin yükümlülüklerini yerine getirmemesi,
 - 4) Şeffaflığın sağlanması ve bilgilendirmeye ilişkin yükümlülüklerini yerine getirmemesi,
 - 5) Tarife/kampanyalar dâhilinde taahhüt ettiği edimleri yerine getirmemesi,
 - 6) Tüketici şikâyetleri çözüm mekanizmasına ilişkin yükümlülüklerini yerine getirmemesi,
 - 7) Abonelik sözleşmelerinin kuruluşuna, uygulanmasına, feshine, değişikliğine, incelenmesi ve onayına yönelik yükümlülükler ile abonelik sözleşmelerine ilişkin ilgili mevzuatta belirtilen diğer yükümlülükleri yerine getirmemesi,
 - 8) Abonelik sözleşmesi ve/veya aboneye ait kimliğini ispata yarar herhangi bir belgenin bulunmaması ve/veya muhafaza edilmesi gibi hususlardaki yükümlülüklerini ihlal etmesi,
 - 9) Abonelik kayıtlarının eksik tutulması veya açık hatlara ilişkin ilgili mevzuata uymaması,
 - 10) Tüketici mağduriyetinin giderilmesine yönelik yükümlülüklerini yerine getirmemesi,
 - 11) Tarife değişikliklerini abonelere duyurma yükümlülüğünü yerine getirmemesi,
- halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde ikisine (%2) kadar idari para cezası uygulanır.

b) İşletmecinin;

- 1) Fatura gönderme yükümlülüğü, faturalarda bulunması gereken hususlar ile ayrıntılı fatura sağlamaya ilişkin yükümlülüklerini yerine getirmemesi,
 - 2) Engelli abonelere ilişkin yükümlülüklerini yerine getirmemesi,
 - 3) Tüketici haklarına ilişkin ilgili mevzuatta düzenlenen kapsamda işletmeci değişikliğiyle ilgili yükümlülüklerini yerine getirmemesi,
 - 4) İnternetin güvenli kullanımına ilişkin yükümlülüklerini yerine getirmemesi,
 - 5) (Değişik ibare:RG-29/9/2018-30550) Tüketicinin aldatılması veya yanıltılmasının amaçlanması halleri dışında katma değerli elektronik haberleşme hizmetlerine ilişkin yükümlülükleri yerine getirmemesi,
- halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde birine (%1) kadar idari para cezası uygulanır.

(2) (Değişik:RG-29/9/2018-30550) Katma değerli elektronik haberleşme hizmetlerinde tüketicinin aldatılması veya yanıtılmasının amaçlandığının tespit edilmesi halinde, işletmecinin bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır. İhlalin ilgili mevzuat çerçevesinde ağır kusur oluşturduğunun Kurul tarafından tespiti halinde ise işletmecinin yetkilendirmesi fesh/iptal edilir.

(3) (Ek:RG-29/9/2018-30550) İşletmecinin birinci ve ikinci fıkralarda sayılan fiiller dışında tüketici haklarına ilişkin ilgili mevzuatı ihlal etmesi halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır.

Kişisel verilerin korunmasına ilişkin ihlaller

MADDE 13 - (1) Aşağıda belirtilen hallerde işletmecinin bir önceki takvim yılındaki net satışlarının aşağıda belirtilen oranına kadar idari para cezası uygulanır:

a) İşletmecinin;

1) Kişisel verilere sadece yetkili kişiler tarafından erişilebilmesini ve kişisel verilerin tutulduğu sistemlerin ve kişisel verilere erişim sağlamak için kullanılan uygulamaların güvenliğini sağlama yükümlülüğünü yerine getirmemesi,

2) İlgili mevzuat gereği abonelere/kullanıcılara ait işlenen ve saklanan trafik verilerinin öngörülen sürede tutma veya silme yükümlülüğünü yerine getirmemesi,

3) Trafik verisinin ve konum verisinin işlenmesine ilişkin yükümlülüklerini yerine getirmemesi,

4) Asgari istem dışı, yetki dışı ya da yasa dışı olarak; kişisel verilerin tahrip edilmesi, kaybolması, değiştirilmesi, depolanması veya başka bir ortama kaydedilmesi, işlenmesi, ifşa edilmesi ve söz konusu verilere erişilmesine karşı kişisel verilerin korunmasına ilişkin yükümlülüklerini yerine getirmemesi,

5) Kişisel verilere ve ilişkili diğer sistemlere sağlanan tüm erişimlere ve erişim yetkisi olan personelin yaptığı işlemlere dair detaylı işlem kayıtlarını ilgili mevzuatta belirlenen süre boyunca tutma yükümlülüğünü yerine getirmemesi,

6) Kişisel verilerin işlenmesi ve gizliliğine ilişkin ilgili mevzuatta düzenlenen diğer yükümlülükleri ihlal etmesi,

halinde bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır.

Milli güvenlik, kamu düzeni ve gizliliğin ihlali

MADDE 14 - (1) İşletmecinin, haberleşmenin gizliliğine, milli güvenlik ve kamu düzenine aykırı davranışta bulunması, işletmeci ve çalışanların yasaların öngördüğü istisnalar dışında haberleşmeyi engellemesi, gizliliğini ihlal etmesi, başkalarına bildirmesi ve açıklaması, yasalarla belirlenen hallerde istenilen bilgilerin Kanunla yetkili kılınan kişi ve kuruluşlara verilmesi ve elde edilmesinin engellenmesi hallerinde, işletmecinin bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır.

(2) Milli güvenlik ve kamu düzeni ihlali oluşması halinde ayrıca 31 ve 32 nci maddeler de uygulanır. 31 ve 32 nci maddeler gereğince yaptırım uygulanması, idari para cezası uygulamasını engellemez.

(3) İşletmecinin elektronik haberleşme alt yapısına mahkeme kararı veya ilgili mevzuat uyarınca Kurum, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı veya diğer yetkili merciler tarafından alınmış bir karar olmadıkça, elektronik haberleşmenin aksamasına neden olacak biçimde müdahalelerde bulunması halinde işletmecinin bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır.

Hizmet kalitesine ilişkin yükümlülüklerin ihlali

MADDE 15 - (1) Aşağıda belirtilen hallerde, işletmecinin bir önceki takvim yılındaki net satışlarının yüzde ikisine (%2) kadar idari para cezası uygulanır:

a) İşletmecinin ilgili mevzuat çerçevesinde vereceği hizmetlere ilişkin yükümlülüklerini mücbir sebep halleri veya Kurul tarafından kabul edilen haklı nedenler olmaksızın ilgili mevzuattaki koşullara uygun bir şekilde, kesintisiz olarak yerine getirmemesi.

b) İşletmecinin uluslararası standartlara ve/veya hizmet kalitesine ilişkin ilgili mevzuata uymaması, ilgili mevzuat ile diğer yükümlülükleri ihlal etmesi.

Rekabet ihlalleri

MADDE 16 - (1) Rekabetin tesisi, korunması, rekabetin engellenmesi, bozulması veya kısıtlayıcı uygulamaların giderilmesine yönelik ilgili mevzuatın ihlal edilmesi veya rekabete aykırı uygulamaların tespit edilmesi halinde işletmeciye bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır.

Kısa mesaj hizmetlerinde Türkçe karakter kullanımına ilişkin ihlal

MADDE 17 - (1) İşletmecinin kısa mesaj hizmetlerinde Türkçe karakter kullanımına dair mevzuata uymaması durumunda işletmeciye, bir önceki takvim yılındaki net satışlarının binde beşine (% 0,5) kadar idari para cezası uygulanır.

Anten tesislerinin tasarımı, kurulması ve paylaşımına ilişkin ihlal

MADDE 18 - (1) Hücresel sistem anten tesislerinin tasarımı, kurulması ve paylaşımına ilişkin yükümlülüklerini yerine getirmemesi durumunda işletmeciye bir önceki takvim yılındaki net satışlarının yüzde birine (%1) kadar idari para cezası uygulanır ve yükümlülüğünü yerine getirmesi için otuz iş gününe kadar süre verilir.

(2) İşletmecinin verilen süreye rağmen yükümlülüğünü yerine getirmemesi durumunda söz konusu anten tesisinin faaliyetleri yükümlülük yerine getirilene kadar durdurulabilir.

Şebeke ve bilgi güvenliği ile siber güvenliğe ilişkin ihlaller (3)

MADDE 19 - (1) İşletmecinin, şebeke güvenliği de dahil olmak üzere elektronik haberleşme güvenliğine ilişkin mevzuata uymaması halinde bir önceki takvim yılındaki net satışlarının yüzde birine (%1) kadar idari para cezası uygulanır.

(2) (Ek:RG-29/9/2018-30550) Ulusal siber güvenlik faaliyetleri ile siber saldırılara karşı korunma ve caydırıcılığın sağlanmasına yönelik Kurumun görevleri kapsamında belirleyeceği yükümlülükleri yerine getirmeyen veya aldiracağı tedbirleri uygulamayan gerçek kişiler ile işletmeciler dışındaki özel hukuk tüzel kişilerine bin liradan bir milyon liraya kadar idarî para cezası uygulanır. Kurum ihlal konusuna ilişkin olarak gerçek veya tüzel kişiden yazılı açıklamalarını 15 günden 30 güne kadar belirlenebilecek süre içerisinde göndermesini ister. Süresinde gönderilmeyen yazılı açıklama dikkate alınmaz.

Arayüz teknik özelliklerinin yayımlanmasına ilişkin ihlal

MADDE 20 - (1) İşletmecinin, arayüz teknik özelliklerinin yayımlanmasına ilişkin mevzuata uymaması halinde işletmeciye bir önceki takvim yılındaki net satışlarının yüzde birine (%1) kadar idari para cezası uygulanır.

Kayıtlı elektronik posta hizmetine ilişkin ihlaller

MADDE 21 - (1) Kayıtlı elektronik posta sisteminin idarî, teknik ve hukukî gereklilikleri ile işleyişinde güvenli ürün ve sistemleri kullanmaması, hizmeti güvenilir bir biçimde yürütmemesi, hizmetlerini belirlenen kalitede sunulabilmesini teminen gerekli idarî ve teknik imkân ve kabiliyetlere sahip olmaması, bu sistemlerde kişisel verilerin korunması ve bilgi güvenliğinin sağlanmasına ilişkin belirlenen kurallara aykırı davranması veya Kurum tarafından ilgili mevzuat ile belirlenen diğer yükümlülüklerle uymaması, kayıtlı elektronik posta sisteminin işleyişinin tüm aşamalarında kayıt altına alınması gerekli olan verileri gerektiği şekilde kaydetmemesi hallerinde kayıtlı elektronik posta

hizmet sağlayıcısına bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır.

İnternet alan adlarına ilişkin ihlaller

MADDE 22 - (1) Kayıt kuruluşunun veya uyuşmazlık çözüm hizmet sağlayıcısının internet alan adlarına ilişkin mevzuata uymaması halinde kayıt kuruluşuna veya uyuşmazlık çözüm hizmet sağlayıcısına bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır.

Bilgi ve/veya belgelerin süresinde verilmemesi

MADDE 23 - (1) Kurum tarafından talep edilen her türlü bilgi ve/veya belge ile ilgili mevzuat gereği verilmesi gereken bilgi ve/veya belgelerin Kuruma süresi içinde verilmemesi halinde 44 üncü maddede yer alan ölçütler dikkate alınarak işletmeci uyarılır veya işletmeciye bir önceki takvim yılındaki net satışlarının yüzbinde üçü (%0,003) oranında idari para cezası uygulanır.

(2) Söz konusu bilgi ve/veya belgenin tekrar istenmesine rağmen süresi içinde verilmemesi halinde 44 üncü maddedeki ölçütler dikkate alınarak, işletmecinin bir önceki takvim yılındaki net satışlarının yüzbinde üçününün (%0,003) iki katından az olmamak üzere yüzde birine (%1) kadar idari para cezası uygulanır.

Yanlış bilgi ve/veya belge verilmesi

MADDE 24 - (1) Kurum tarafından talep edilen her türlü bilgi ve/veya belge ile ilgili mevzuat kapsamında verilmesi gereken bilgi ve/veya belgelerin yanlış olması halinde 44 üncü maddede yer alan ölçütler dikkate alınarak işletmeci uyarılır veya işletmeciye bir önceki takvim yılındaki net satışlarının yüzbinde ikisi (%0,002) oranında idari para cezası uygulanır.

(2) Yanlış olan bilgi ve/veya belgelerin tekrar istenmesine rağmen tamamlanmaması halinde 44 üncü maddedeki ölçütler dikkate alınarak, işletmecinin bir önceki takvim yılındaki net satışlarının yüzbinde ikisininin (%0,002) iki katından az olmamak üzere yüzde birine (%1) kadar idari para cezası uygulanır.

Eksik bilgi ve/veya belge verilmesi

MADDE 25 - (1) Kurum tarafından talep edilen her türlü bilgi ve/veya belge ile ilgili mevzuat kapsamında verilmesi gereken bilgi ve/veya belgelerin eksik olması durumunda, 44 üncü maddede yer alan ölçütler dikkate alınarak işletmeci uyarılır veya işletmeciye bir önceki takvim yılındaki net satışlarının yüzbinde ikisi (%0,002) oranında idari para cezası uygulanır.

(2) Eksik olan bilgi ve/veya belgelerin tekrar istenmesine rağmen tamamlanmaması halinde 44 üncü maddedeki ölçütler dikkate alınarak, işletmecinin bir önceki takvim yılındaki net satışlarının yüzbinde ikisinin (%0,002) iki katından az olmamak üzere yüzde birine (%1) kadar idari para cezası uygulanır.

Yanıtıcı bilgi ve/veya belge verilmesi

MADDE 26 - (1) Kurum tarafından talep edilen her türlü bilgi ve/veya belge ile ilgili mevzuat kapsamında verilmesi gereken bilgi ve/veya belgelerin yanıtıcı olması halinde işletmeciye bir önceki takvim yılındaki net satışlarının yüzde ikisine (%2) kadar idari para cezası uygulanır.

Denetime ilişkin ihlaller

MADDE 27 - (1) Denetime ilişkin mevzuat kapsamında getirilen yükümlülüklerin ihlal edilmesi halinde İşletmeciye bir önceki takvim yılına ait net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır. Ayrıca, bu kişilerin kayıtlı elektronik posta hizmet sağlayıcısı, ölçüm yetki belgesine sahip kuruluş, denetim yapma yetki belgesine sahip şirket veya deneme iznine sahip kuruluş olması durumunda Kurum tarafından kendilerine verilen yetki, ruhsat gibi her türlü izin iptal edilebilir.

Teknik uyumluluk

MADDE 28 - (1) Aşağıda belirtilen hallerde işletmeciye cihaz başına on bin Türk Lirasından yirmi bin Türk Lirasına kadar idari para cezası uygulanır:

- a) Kayıp, kaçak veya çalıntı cihazlara elektronik haberleşme hizmeti verilmesi.
- b) Mobil Cihaz Kayıt Sisteminde kayıtlı iken elektronik kimlik bilgisi kopyalanmış gerçek cihazları sadece eşleştirme yapılan abone numaraları ile kullanılmak üzere kullanıma açılmasına ilişkin yükümlülüğe uyulmaması.

(2) İşletmeci tarafından birinci fıkrada belirtilen yasal olmayan cihazların haberleşme şebekelerine bağlanılmalarını önlemek üzere Mobil Cihaz Kayıt Tabanı sistemlerini Kurumdaki Mobil Cihaz Kayıt Sistemi ile uyumlu olarak çalışır hâle getirme, bununla ilgili teknik alt yapı ve sisteminin güvenliği ve güvenilirliğini sağlama ve aksamaksızın işletme yükümlülüklerinin ihlali halinde işletmeciye on milyon Türk Lirasına kadar idari para cezası uygulanır.

Kamu güvenlik ve istihbarat kurumları

MADDE 29 - (Değişik:RG:30/12/2014-29221) (1) (2)

(1) Kamu güvenlik ve istihbarat kurumları ile Telekomünikasyon İletişim Başkanlığının, özel yasaları ile kendilerine verilmiş bulunan görevleri yerine getirmelerine imkan sağlayacak tedbirleri almaya

yönelik olarak; ilgili mevzuat uyarınca teknik altyapıyı, Kurum tarafından belirlenecek süre ve şartlar içerisinde ve tüm harcamaları kendilerine ait olmak üzere kurmasına ve bu alandaki güncellemeleri Kurum tarafından verilen süre içerisinde yapmasına ilişkin yükümlülükleri yerine getirmemesi durumları ağır kusur sayılarak işletmecinin ilgili yetkilendirmesi fesh/iptal edilir.

(2) Telekomünikasyon İletişim Başkanlığınca bir işletmecinin teknik altyapıyı kurmadığına veya süresinde gerekli güncellemeleri yapmadığına ilişkin bildirimının yapılmasına rağmen, bu işletmeciye erişim hizmeti veren işletmecinin verdiği hizmete derhal son vermemesi halinde ihlalin niteliğine göre işletmecinin bir önceki takvim yılındaki net satışlarının yüzde üçüne (% 3) kadar idari para cezası verilebilir veya işletmecinin ilgili yetkilendirmesi fesh/iptal edilebilir.

İletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesine ilişkin ihlaller

MADDE 30 - (1) (Değişik:RG-30/12/2014-29221) İşletmecinin, iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesine yönelik olarak Telekomünikasyon İletişim Başkanlığına verilmiş olan görevlerin yerine getirilmesine imkân sağlayacak kanun ve diğer düzenlemelerle getirilen yükümlülüklere uymaması halinde ihlalin niteliğine göre işletmecinin bir önceki takvim yılındaki net satışlarının yüzde üçüne (% 3) kadar idari para cezası verilebilir veya işletmecinin ilgili yetkilendirmesi fesh/iptal edilebilir.

ÜÇÜNCÜ BÖLÜM

Diğer Yaptırım ve Tedbirler

Millî güvenliğe aykırılık

MADDE 31 - (1) Milli güvenliğe aykırı işletmecilik yapıldığının yetkili makamlarca tespiti ve Kuruma bildirim halinde bu durum ağır kusur sayılarak işletmecinin yetkilendirmesi fesh/iptal edilir.

(2) Milli güvenliğe aykırı davranışın işletmecinin çalışanlarından kaynaklandığının yine yetkili makamlarca tespiti ve Kuruma bildirim halinde işletmeciye ihlalin sonlandırılması ve gerekli tedbirlerin alınması hususunda uyarıda bulunulur. Uyarıya rağmen aykırı davranışın sürdürüldüğünün yetkili makamlarca tespiti halinde bu durum yine ağır kusur sayılarak işletmecinin faaliyetinin geçici olarak durdurulmasına karar verilir veya işletmecinin yetkilendirmesi fesh/iptal edilir.

(3) Bu madde hükümlerinin uygulanmasında 14 üncü madde hükümleri saklıdır.

(4) Bu madde gereği yapılacak fesihlerde, 5809 sayılı Kanununun 60 ıncı maddesinin birinci fıkrası uyarınca Bakanlık görüşü alınması gereken durumlarda Bakanlık görüşü alınır.

Kamu düzeninin ihlali

MADDE 32 - (1) İşletmeci ve çalışanları, haberleşmenin engellenmemesi veya haberleşmenin gizliliğine veya içeriğine dokunulmaması gibi anayasal temel hak ve hürriyetlere ve kamu düzenine ilişkin ilkelere aykırı davranışta bulunamaz. İşletmeci bu kapsamda gerekli tedbirleri almakla yükümlüdür. Kamu düzenine aykırı fiillerde aşağıdaki yaptırımlar uygulanır:

a) İşletmeci veya çalışanları tarafından bu maddede belirtilen yükümlülüklerin ihlalinin tespiti halinde işletmeciye ihlalin sonlandırılması ve gerekli tedbirlerin alınması hususu yazılı olarak bildirilir. Kurul tarafından ihlalin ağır kusur teşkil ettiğine karar verilmesi halinde işletmecinin faaliyetinin geçici olarak durdurulmasına veya işletmecinin yetkilendirmesinin fesh/iptaline karar verilir.

b) (a) bendindeki ihlalin işletmeci ve çalışanları tarafından resmi görevleri dolayısıyla kamu görevlilerine karşı işlenmiş olduğunun mahkemelerce tespiti halinde işletmecinin yetkilendirmesi fesh/iptal edilir.

c) İşletmeci tarafından kamu düzeninin ihlal edildiğinin Kurum ya da yetkili makamlarca tespiti halinde, işletmeciye derhal ihlalin sonlandırılması ve gerekli tedbirlerin alınması hususu yazılı olarak bildirilir. Kurul tarafından ihlalin ağır kusur teşkil ettiğine karar verilmesi halinde işletmecinin yetkilendirmesi fesh/iptal edilir.

(2) Bu madde hükümlerinin uygulanmasında 14 üncü madde hükümleri saklıdır.

(3) Bu madde gereği yapılacak fesihlerde, 5809 sayılı Kanununun 60 ıncı maddesinin birinci fıkrası uyarınca Bakanlık görüşü alınması gereken durumlarda Bakanlık görüşü alınır.

Kamu hizmetinin gereği gibi yürütülmemesi

MADDE 33 - (1) İlgili mevzuat gereği kamu hizmetinin gereği gibi yürütülmemesi halinde idari para cezasına ilişkin hükümler saklı kalmak üzere, işletmeci önce kamu hizmetinin gereği gibi yürütülmesi ve gerekli tedbirlerin alınması için uyarılır. İhlalin devamı ve kamu hizmetinin gereği gibi yürütülmemesinin ilgili mevzuat çerçevesinde ağır kusur oluşturduğunun Kurul tarafından tespiti halinde işletmecinin yetkilendirmesi fesh/iptal edilir. Bu madde gereği yapılacak fesihlerde, 5809 sayılı Kanununun 60 ıncı maddesinin birinci fıkrası uyarınca Bakanlık görüşü alınması gereken durumlarda Bakanlık görüşü alınır.

Savaş, seferberlik ve olağanüstü hal

MADDE 34 - (1) Kurum, savaş, genel seferberlik ve benzeri durumlarda, kamu güvenliği ve ulusal savunma için yetkili makamlarca talep edilmesi halinde, sınırlı veya sınırsız bir süreyle işletmecinin işletme faaliyetlerinin tamamını veya bir kısmını askıya alabilir ve doğrudan doğruya şebekeyi işletebilir, millî güvenlik ve kamu düzeni gerekleri nedeniyle işletmeciye tahsis edilen kaynakların bir kısmını geri alabilir. Bu durumda geçecek süre, yetkilendirme süresine eklenir ve bu dönemde elde edilen gelir işletmeciye ait olur.

(2) Söz konusu hallerde Kurumca bu hususlara ilişkin olarak yapılmış bulunan düzenleme ve alınmış olan kararlara işletmeci tarafından uyulmaması ağır kusur sayılarak işletmecinin yetkilendirmesi fesh/iptal edilir.

(3) İkinci fıkra gereği yapılacak fesihlerde, 5809 sayılı Kanununun 60 ıncı maddesinin birinci fıkrası uyarınca Bakanlık görüşü alınması gereken durumlarda Bakanlık görüşü alınır.

Yeniden yetkilendirilmeme

MADDE 35 - (1) (Değişik:RG-30/12/2014-29221) Teknik altyapının kurulması ve iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesine ilişkin ihlaller, milli güvenlik, kamu düzeninin ihlali, haberleşmenin engellenmesi ve gizliliğine dokunulması, kamu hizmetinin gereği gibi yürütülmemesi sebepleri ile yetkilendirmesi fesh/iptal edilen şirketler ile söz konusu şirket hisselerinden en az yüzde beşine (%5) sahip ortaklar, yönetim kurulu üyeleri ile tüzel kişiliği idareye yetkili kişiler tarafından kurulmuş şirketler yeniden yetkilendirilmez.

(2) (Değişik:RG-25/5/2019-30784) Birinci fıkrada sayılan durumlar dışında yetkilendirmesi bu Yönetmelik hükümleri kapsamında fesh/iptal edilen şirketler ile söz konusu şirket hisselerinin en az yüzde onuna (%10) sahip ortaklar, yönetim kurulu üyeleri ile tüzel kişiliği idareye yetkili kişiler tarafından kurulmuş şirketler fesh/iptal edilen yetkilendirme konusunda üç yıl süreyle yeniden yetkilendirilmez. Bu sürenin sonunda yeniden yetkilendirme için ilgili mevzuat hükümlerinin yanı sıra fesih/iptal sebebinin ortadan kalkması şartı da aranır.

(3) (Mülga:RG-25/5/2019-30784)

Elektronik haberleşme tesislerine ilişkin yükümlülüklerin ihlali

MADDE 36 - (1) Elektronik haberleşme tesislerine ilişkin ilgili mevzuatın ihlali halinde sabit elektronik haberleşme cihazının faaliyeti uygun şartlar sağlanıncaya kadar Kurum tarafından durdurulur.

(2) Kurumun belirlediği usul ve esaslar çerçevesinde elektronik haberleşme tesisleri ile ilgili bildirimlerin yapılmaması veya güvenlik sertifikası alınmadan kurulması veya montajına başlanması veya izinsiz revizyon yapılması veya Kurum ya da Kurum tarafından yetki verilen kuruluşlarca yapılacak ölçümler sonucu Kurum tarafından belirlenen elektromanyetik alan şiddeti limit değere uygun bulunmaması veya konuya ilişkin diğer düzenleme hükümlerinin ihlali hallerinde, bunların sahibine her bir cihaz için ayrı ayrı olmak üzere ruhsatname ücretinin elli katı idarî para cezası uygulanır.

(3) Tekrar istenmesine rağmen Kurum tarafından talep edilen her türlü bilgi ve belge ile ilgili mevzuat gereği verilmesi gereken bilgi veya belgelerin süresi içerisinde tam ve eksiksiz olarak verilmemesi durumunda, Ölçüm Yetki Belgeli Kuruluşun Ölçüm Yetki Belgesi iptal edilir. Ölçüm Yetki Belgeli Kuruluşun yanlış ve yanıltıcı bilgi vermesi halinde Ölçüm Yetki Belgesi doğrudan iptal edilir.

DÖRDÜNCÜ BÖLÜM

Ortak Hükümler

İşletmecinin faaliyete yeni başlamış olması

MADDE 37 - (1) Kurum tarafından bu Yönetmelik kapsamında idari yaptırım uygulanması öngörülen işletmecinin faaliyete yeni başlamış olması halinde, 44 üncü madde hükümleri dikkate alınarak bin Türk Lirasından bir milyon Türk Lirasına kadar idari para cezası uygulanır.

(2) Birinci fıkrada belirtilen durumlarda ilgili mevzuatta belirtilen diğer idari yaptırımlar saklıdır.

Somut tedbirlerin uygulanması

MADDE 38 - (1) Bu Yönetmeliğe göre belirtilen ihlallerin tespiti halinde, bu Yönetmelikte belirtilen yaptırımların yanı sıra, ihlalin niteliğine göre Kurul tarafından somut tedbirlerin uygulanmasına karar verilebilir.

Ödeme ve kesinleşme

MADDE 39 - (1) Bu Yönetmeliğe göre verilen idari para cezaları tebliğ tarihinden itibaren otuz gün içerisinde Kurum hesaplarına ödenir. Bu süre içerisinde ödenmeyen idarî para cezaları, Kurumun bildiri üzerine ilgili vergi dairesince 6183 sayılı Amme Alacaklarının Tahsil Usulü Hakkında Kanun hükümlerine göre tahsil olunur.

(2) Tahsil olan idarî para cezalarının tamamı Kurum hesaplarına aktarılır.

(3) İdari para cezasının tebliğini müteakip otuz gün içerisinde defaten ödenmesi halinde idari para cezasının ¼'ü oranında indirim yapılır.

(4) Kuruma idari para cezasının tebliğinden itibaren otuz gün içerisinde para cezasının biri peşin olmak üzere dört eşit taksitte ödenmesi başvurusunda bulunulabilir. Kişinin borcunu taksitlendirme isteğinde bulunması halinde, idarî para cezasının, ilk taksitin peşin ödenmesi koşuluyla, bir yıl içinde ve devam eden aylarda dört eşit taksit halinde ödenmesine Kurul başkanı tarafından karar verilir. Taksitlerin zamanında ve tam olarak ödenmemesi halinde, idarî para cezasının kalan kısmının tamamı tahsil edilir.

(5) Kurum tarafından uygulanan idari para cezalarının tahsilinde kesinleşme şartı aranmaz.

(6) 6183 sayılı Kanununun 106 ncı maddesinin birinci fıkrası çerçevesinde uygulanan idari para cezalarının tahsil zamanaşımı süresi beklenilmeksizin Kurum tarafından terkinine karar verilebilir.

İdari para cezalarının arttırılması

MADDE 40 - (1) 5070 sayılı Kanun, 4703 sayılı Kanun, 5651 sayılı Kanun ve ilgili mevzuat kapsamında Kurum tarafından uygulanacak idari para cezaları 5326 sayılı Kabahatler Kanununda belirlenen esaslar çerçevesinde arttırılarak uygulanır.

İçtima

MADDE 41 - (1) Bir fiil ile birden fazla yükümlülüğün ihlal edilmesi halinde bu ihlaller için sadece idarî para cezası öngörülmüşse, en ağır idarî para cezası verilir. Bu ihlaller ile ilgili olarak ilgili mevzuatta idarî para cezasından başka idarî yaptırımlar da öngörülmüş ise, bu yaptırımların her biri de ayrıca uygulanır.

(2) Aynı ihlalin birden fazla işlenmesi halinde her bir ihlale ilişkin olarak ayrı ayrı idari para cezası verilir. Kesintisiz fiille işlenebilen ihlallerde idari yaptırım kararı verilinceye kadar bu ihlaller tek fiil sayılır.

İdari yaptırımların uygulanması

MADDE 42 - (1) İşletmecinin ihlal sonucunda elde ettiği gelir veya sebep olduğu zarar bu Yönetmelikte o ihlal için belirlenen üst sınırdan daha yüksek ise 44 üncü madde hükümleri gözetilerek uygulanacak idari para cezası işletmecinin bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar arttırılabilir.

(2) Bu Yönetmelikte yer alan idari yaptırımların uygulanması ilgili mevzuatta düzenlenen yükümlülüklerin yerine getirilmesini engellemez.

Tekerrür

MADDE 43 - (1) İdari para cezası uygulanmış bir işletmeci tarafından, üç yıl içinde aynı yükümlülüğün ihlal edilmesi durumunda söz konusu ihlal için, 23 üncü, 24 üncü ve 25 inci maddeler saklı kalmak kaydıyla, uygulanacak idari para cezası işletmecinin bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar arttırılabilir.

(2) (Ek:RG-30/12/2014-29221) 30 uncu madde kapsamında idari para cezası uygulanmış bir işletmecinin üç yıl içinde aynı yükümlülüğü ihlal etmesi durumunda yetkilendirmesi fesh/iptal edilir.

Yaptırım ölçütleri

MADDE 44 - (1) Bu Yönetmelikteki cezaların belirlenmesinde ağırlaştırıcı veya hafifletici sebep olarak aşağıda sayılan unsurlar göz önünde bulundurulur.

- a) Zararın varlığı,
- b) Haksız ekonomik kazancın varlığı,
- c) Tekerrürün varlığı,
- ç) Aynı madde ihlaline ilişkin olarak işletmeciye son beş yılda uygulanan idari yaptırımlar,
- d) İyi niyetin varlığı.

Yetki

MADDE 45 - (Değişik:RG-25/5/2019-30784)

(1) Bu Yönetmelikteki idari para cezaları ve idari tedbirleri uygulamaya bu maddenin ikinci fıkraya hükmü hariç olmak üzere Kurul yetkilidir. Kurul bu yetkinin bir bölümünü çerçevesini belirleyerek Kurul Başkanına devredebilir.

(2) 5651 sayılı Kanun kapsamında uygulanacak idari yaptırımlar ile bu Yönetmeliğin 23 üncü maddesinin birinci fıkrası, 24 üncü maddesinin birinci fıkrası ile 25 inci maddesinin birinci fıkrasında yer alan idari yaptırımları uygulamaya Kurul Başkanı; 18 inci ve 36 ncı maddelerde belirtilen idari yaptırımları uygulamaya Bölge Müdürleri yetkilidir.

(3) Denetim mevzuatı kapsamında yürütülen idari süreçlerde Kurul ve Kurul Başkanının idari yaptırım uygulamaya yetkili olduğu ihlallerin birlikte bulunması halinde, bu kapsamdaki idari yaptırımların tamamı doğrudan Kurul tarafından uygulanabilir.

Uyarı

MADDE 46 - (1) Bu Yönetmelik kapsamında meydana gelen ihlaller için, bu Yönetmeliğin 44 üncü maddesinde yer alan hususlar dikkate alınmak ve 23 üncü, 24 üncü, 25 inci, 31 inci ve 33 üncü

maddeler saklı kalmak kaydıyla idari yaptırım uygulanmadan önce, bu Yönetmeliğin aynı maddesi kapsamında olmak üzere işletmeci Kurul tarafından bir defaya mahsus uyarılabilir.

(2) Uyarı yapılırken tekerrür süresi dikkate alınır. Tekerrüre esas sürenin dolması halinde aynı madde kapsamında tekrar uyarıda bulunulabilir.

Zaman bakımından uygulama

MADDE 46/A - (Ek:RG-25/5/2019-30784)

(1) Bu Yönetmelik hükümlerinin zaman bakımından uygulanması ile ilgili olarak 5326 sayılı Kabahatler Kanununun ilgili hükümleri kıyasen uygulanır.

(2) Ancak ihlalin yıllara yaygın olması durumunda ihlalin tespit edildiği yıl içinde yürürlükte bulunan Yönetmelik hükümlerine göre idari yaptırım uygulanır.

BEŞİNCİ BÖLÜM

Çeşitli ve Son Hükümler

Hüküm bulunmayan haller

MADDE 47 - (1) İlgili mevzuat ihlallerine ilişkin bu Yönetmelikte hüküm bulunmayan hallerde Kurul tarafından, bu Yönetmelikte yer alan genel hükümler çerçevesinde idari yaptırım kararları alınır.

Atıflar

MADDE 48 - (1) İlgili mevzuatta 49 uncu madde ile yürürlükten kaldırılan Telekomünikasyon Kurumu Tarafından İşletmecilere Uygulanacak İdari Para Cezaları İle Diğer Müeyyide ve Tedbirler Hakkında Yönetmeliğe yapılan atıflar, Erişim ve Ara bağlantı Yönetmeliğinin Müeyyideler başlıklı 21 inci maddesine yapılan atıflar, 12/11/2009 tarihli ve 27404 sayılı Resmî Gazete’de yayımlanan Tarife Yönetmeliğinin Müeyyideler başlıklı 16 ncı maddesine yapılan atıflar ve 21/4/2011 tarihli ve 27912 sayılı Resmî Gazete’de yayımlanan Elektronik Haberleşme Cihazlarından Kaynaklanan Elektromanyetik Alan Şiddetinin Uluslararası Standartlara Göre Maruziyet Limit Değerlerinin Belirlenmesi, Kontrolü ve Denetimi Hakkında Yönetmeliğin İdarî yaptırımlar başlıklı 23 üncü maddesine yapılan atıflar bu Yönetmeliğe yapılmış sayılır.

Yürürlükten kaldırılan yönetmelik

MADDE 49 - (1) 5/9/2004 tarihli ve 25574 sayılı Resmî Gazete’de yayımlanan Telekomünikasyon Kurumu Tarafından İşletmecilere Uygulanacak İdari Para Cezaları ile Diğer Müeyyide ve Tedbirler Hakkında Yönetmelik yürürlükten kaldırılmıştır.

Yürürlük

MADDE 50 - (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 51 - (1) Bu Yönetmelik hükümlerini Bilgi Teknolojileri ve İletişim Kurulu Başkanı yürütür.

Bilgi Teknolojileri ve İletişim Kurumu Posta Sektöründe İdari Yaptırımlar Yönetmeliği

Resmî Gazete Tarihi : 03.06.2014

Resmî Gazete Sayısı : 29019

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU POSTA SEKTÖRÜNDE İDARİ YAPTIRIMLAR YÖNETMELİĞİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak, Tanımlar ve Kısaltmalar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı, Kurum tarafından posta sektöründe uygulanacak idari yaptırımlara ve bunların uygulanmasına ilişkin usul ve esasları düzenlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik 9/5/2013 tarihli ve 6475 sayılı Posta Hizmetleri Kanunu ve Kurum düzenlemeleri de dâhil olmak üzere, posta sektörüne ilişkin ilgili mevzuatta yer alan yükümlülüklerin yerine getirilmemesi veya ilgili mevzuata aykırılık halinde uygulanacak idari para cezaları ile diğer yaptırım ve tedbirlere ve bunların uygulanmasına ilişkin usul ve esasları kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 9/5/2013 tarihli ve 6475 sayılı Posta Hizmetleri Kanununa dayanılarak hazırlanmıştır.

(...)

Kullanıcı menfaatlerine ilişkin ihlaller

MADDE 9 - (1) Aşağıda belirtilen hallerde ilgili hizmet sağlayıcısına bir önceki takvim yılındaki net satışlarının yüzde ikisine (%2) kadar idari para cezası uygulanır:

- a) Hizmet sağlayıcısının, kullanıcılara yaptığı bilgilendirmelerin yanlış olması.
- b) Hizmet sağlayıcısının, hizmetin kısıtlanmasına veya durdurulmasına ilişkin yükümlülüklerini yerine getirmemesi.

c) Hizmet sağlayıcısının, şeffaflığın sağlanması ve bilgilendirmeye ilişkin yükümlülüklerini yerine getirmemesi.

ç) Hizmet sağlayıcısının, kullanıcı mağduriyetinin giderilmesine yönelik yükümlülüklerini yerine getirmemesi.

d) Hizmet sağlayıcısının, kullanıcı şikâyetleri çözüm mekanizmasına ilişkin yükümlülüklerini yerine getirmemesi.

(2) Hizmet sağlayıcısının, hizmet sunumunu ispatlayan belge düzenlemesine ilişkin yükümlülüklerini yerine getirmemesi halinde söz konusu hizmet sağlayıcısına bir önceki takvim yılındaki net satışlarının yüzde birine (%1) kadar idari para cezası uygulanır.

(3) Evrensel posta hizmet yükümlüsü veya evrensel posta hizmet sağlayıcısının evrensel posta hizmetini belirlenen ulusal veya uluslararası standartlara uygun olarak yürütmemesi halinde söz konusu hizmet sağlayıcısına bir önceki takvim yılındaki net satışlarının yüzde birine (%1) kadar idari para cezası uygulanır.

Kişisel veri ve bilgilerin korunmasına ilişkin ihlaller

MADDE 10 - (1) Hizmet sağlayıcısının, kişisel veri ve bilgilerin gizliliğinin korunmasına ilişkin yükümlülüklerini ihlal etmesi halinde ilgili hizmet sağlayıcısına bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır.

Hizmet kalitesine ilişkin yükümlülüklerin ihlali

MADDE 11 - (1) Hizmet sağlayıcısının, hizmet kalitesine ilişkin yükümlülüklerini mücbir sebep halleri veya Kurul tarafından kabul edilen haklı nedenler olmaksızın ihlal etmesi halinde söz konusu hizmet sağlayıcısına bir önceki takvim yılındaki net satışlarının yüzde ikisine (%2) kadar idari para cezası uygulanır.

Rekabet ihlalleri

MADDE 12 - (1) Hizmet sağlayıcısının, rekabetin tesisi ve korunmasına yönelik ilgili mevzuatı veya getirilen yükümlülükleri ihlal etmesi ya da rekabeti engellemeye, bozmaya yahut kısıtlamaya yönelik rekabete aykırı uygulamalarının tespiti halinde söz konusu hizmet sağlayıcısına bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır.

Bilgi ve/veya belgelerin süresinde verilmemesi

MADDE 13 - (1) Kurum tarafından talep edilen her türlü bilgi ve/veya belge ile ilgili mevzuat gereği verilmesi gereken bilgi ve/veya belgelerin hizmet sağlayıcısı tarafından süresi içinde verilmemesi

halinde 27 nci maddede yer alan ölçütler dikkate alınarak ilgili hizmet sağlayıcısı uyarılır veya ilgili hizmet sağlayıcısına bir önceki takvim yılındaki net satışlarının yüz binde üçü (%0,003) oranında idari para cezası uygulanır.

(2) Söz konusu bilgi ve/veya belgenin tekrar istenmesine rağmen süresi içinde verilmemesi halinde 27 nci maddedeki ölçütler dikkate alınarak, ilgili hizmet sağlayıcısının bir önceki takvim yılındaki net satışlarının yüz binde üçünün (%0,003) iki katından az olmamak üzere yüzde birine (%1) kadar idari para cezası uygulanır.

Yanlış bilgi ve/veya belge verilmesi

MADDE 14 - (1) Kurum tarafından talep edilen her türlü bilgi ve/veya belge ile ilgili mevzuat kapsamında verilmesi gereken bilgi ve/veya belgelerin hizmet sağlayıcısı tarafından yanlış olarak verilmesi halinde 27 nci maddede yer alan ölçütler dikkate alınarak ilgili hizmet sağlayıcısı uyarılır veya ilgili hizmet sağlayıcısına bir önceki takvim yılındaki net satışlarının yüz binde ikisi (%0,002) oranında idari para cezası uygulanır.

(2) Söz konusu bilgi ve/veya belgelerin tekrar istenmesine rağmen ilgili hizmet sağlayıcısı tarafından yine yanlış olarak verilmesi halinde 27 nci maddedeki ölçütler dikkate alınarak, ilgili hizmet sağlayıcısının bir önceki takvim yılındaki net satışlarının yüz binde ikisinin (%0,002) iki katından az olmamak üzere yüzde birine (%1) kadar idari para cezası uygulanır.

Eksik bilgi ve/veya belge verilmesi

MADDE 15 - (1) Kurum tarafından talep edilen her türlü bilgi ve/veya belge ile ilgili mevzuat kapsamında verilmesi gereken bilgi ve/veya belgelerin hizmet sağlayıcısı tarafından eksik olarak verilmesi durumunda, 27 nci maddede yer alan ölçütler dikkate alınarak ilgili hizmet sağlayıcısı uyarılır veya ilgili hizmet sağlayıcısına bir önceki takvim yılındaki net satışlarının yüz binde ikisi (%0,002) oranında idari para cezası uygulanır.

(2) Eksik olan bilgi ve/veya belgelerin tekrar istenmesine rağmen ilgili hizmet sağlayıcısı tarafından tamamlanmaması halinde 27 nci maddedeki ölçütler dikkate alınarak, hizmet sağlayıcısının bir önceki takvim yılındaki net satışlarının yüz binde ikisinin (%0,002) iki katından az olmamak üzere yüzde birine (%1) kadar idari para cezası uygulanır.

Denetime ilişkin ihlaller

MADDE 16 - (1) Hizmet saęlayıcısının denetime ilişkin mevzuat kapsamında getirilen yükümlölükleri ihlal etmesi halinde söz konusu hizmet saęlayıcısına bir önceki takvim yılına ait net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanır.

(...)

Bilgi Teknolojileri ve İletişim Kurumu Teşkilât Yönetmeliği

Resmî Gazete Tarihi : 08.06.2011

Resmî Gazete Sayısı : 27958

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU TEŞKİLÂT YÖNETMELİĞİ

BİRİNCİ BÖLÜM

Genel Hükümler

Amaç ve kapsam

MADDE 1- (1) Bu Yönetmelik; Bilgi Teknolojileri ve İletişim Kurumunun teşkilât yapısını, çalışma usûl ve esaslarını, hizmet birimlerinin görevlerini yetkilerini ve sorumluluklarını belirlemek amacıyla hazırlanmıştır.

Dayanak

MADDE 2- (1) Bu Yönetmelik 5/4/1983 tarihli ve 2813 sayılı Bilgi Teknolojileri ve İletişim Kurumunun Kuruluşuna İlişkin Kanunun 5 inci maddesi ile 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununa dayanılarak hazırlanmıştır.

Tanımlar

MADDE 3- (1) Bu Yönetmelikte geçen;

- a) Bakanlık: Ulaştırma Bakanlığını,
 - b) Başkan: Bilgi Teknolojileri ve İletişim Kurulu Başkanını
 - c) Kurul: Bilgi Teknolojileri ve İletişim Kurulunu,
 - ç) Kurum: Bilgi Teknolojileri ve İletişim Kurumunu,
 - d) Sektör: Elektronik haberleşme sektörünü,
 - e) Üye: Bilgi Teknolojileri ve İletişim Kurulu üyelerini,
- ifade eder.

(...)

Tüketici Hakları Dairesi Başkanlığı

MADDE 23- (1) Tüketici Hakları Dairesi Başkanlığının görevleri şunlardır:

- a) Abone, kullanıcı, tüketici ve son kullanıcıların haklarının korunmasına ilişkin düzenlemeleri yapmak ve gerekli tedbirleri almak.
- b) Abonelik sözleşmelerine ilişkin düzenlemeler yapmak, abonelik sözleşmelerini incelemek ve değiştirilmesi gerekli görülen hususları işletmeciye bildirmek.
- c) Kişisel verilerin işlenmesine ve gizliliğinin korunmasına ilişkin gerekli tedbirleri almak ve düzenlemeler yapmak.
- ç) Tüketici ve son kullanıcılara sunulan elektronik haberleşme hizmetlerinin hizmet kalitesine yönelik düzenlemeler yapmak.
- d) Özürlü, yaşlı ve sosyal açıdan korunmaya muhtaç kesimlerin özel ihtiyaçlarının dikkate alınmasına yönelik çalışmalar ve düzenlemeler yapmak.
- e) Tüketici ihtiyaçlarının belirlenmesi ve menfaatlerinin korunması için gerekli çalışmaları ve düzenlemeleri yapmak.
- f) Tüketici şikâyetleri çözüm mekanizmasına ilişkin usûl ve esasları belirlemek.
- g) Tüketicilerin bilgilendirilmesi, bilinçlendirilmesi ve tüketici davranışlarına ilişkin gerekli araştırmaları yapmak veya yaptırmak, öneriler geliştirmek.
- ğ) Evrensel hizmete ilişkin olarak Bakanlıkla, tüketiciler konusunda ise Sanayi ve Ticaret Bakanlığı ile ilişkileri yürütmek.
- h) Başkan tarafından verilecek diğer görevleri yapmak.

**Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına
İlişkin Yönetmelik**

Resmî Gazete Tarihi : 04.12.2020

Resmî Gazete Sayısı : 31324

**ELEKTRONİK HABERLEŞME SEKTÖRÜNDE KİŞİSEL VERİLERİN İŞLENMESİ VE
GİZLİLİĞİN KORUNMASINA İLİŞKİN YÖNETMELİK**

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı, özel hayatın gizliliği ile kişi temel hak ve özgürlüklerinin korunmasını teminen elektronik haberleşme sektöründe kişisel verilerin işlenmesi ve gizliliğin korunmasına yönelik usul ve esasları belirlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin tüzel kişi abonelikleri dâhil elektronik haberleşme hizmeti sunulması kapsamında elde ettikleri veriler bakımından uyacakları usul ve esasları kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun 4, 6, 12, 49, 51 ve 60 ıncı maddelerine dayanılarak hazırlanmıştır.

Tanımlar ve kısaltmalar

MADDE 4 - (1) Bu Yönetmelikte geçen;

- a) Abone: Bir işletmeci ile elektronik haberleşme hizmetinin sunumuna yönelik olarak yapılan bir sözleşmeye taraf olan gerçek ya da tüzel kişiyi,
- b) Acil yardım çağrıları: Ulusal ve uluslararası düzenlemelerde kabul görmüş yangın, sağlık, doğal afetler ve güvenlik gibi acil durumlarla ilgili olarak itfaiye, polis, jandarma, sağlık ve benzeri kuruluşlara yardım talebiyle yapılan çağrıları,

- c) Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,
- ç) İşlem kaydı: Kişisel verilere ve ilişkili diğer sistemlere erişen kişiler tarafından yapılan işlemin, işlemin gerçekleştiği tarihten sonra tanımlanabilmesini teminen tutulan ve asgari olarak işlem, işlemin detayı, işlemi yapan kişi, işlemin yapıldığı tarih ve zaman ile işlemi yapan kişinin bağlandığı nokta bilgilerini içeren elektronik kayıtları,
- d) İşletmeci: Yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirketi,
- e) Kanun: 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununu,
- f) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
- g) Kişisel veri ihlali: Yasa dışı, yetki dışı ya da istem dışı olarak; kişisel verilerin tahrip edilmesine, silinmesine, kaybolmasına, iletilmesine, değiştirilmesine, depolanmasına veya başka bir ortama kaydedilmesine, işlenmesine, ifşa edilmesine ve söz konusu verilere erişilmesine neden olan güvenlik ihlalini,
- ğ) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,
- h) Konum verisi: Kamuya açık elektronik haberleşme hizmeti kullanıcısına ait bir cihazın coğrafi konumunu belirleyen ve elektronik haberleşme şebekesinde veya elektronik haberleşme hizmeti aracılığıyla işlenen belirli veriyi,
- ı) Kullanıcı: Aboneliği olup olmamasına bakılmaksızın elektronik haberleşme hizmetlerinden yararlanan gerçek veya tüzel kişiyi,
- i) Kurul: Bilgi Teknolojileri ve İletişim Kurulunu,
- j) Kurum: Bilgi Teknolojileri ve İletişim Kurumunu,
- k) Trafik verisi: Bir elektronik haberleşme şebekesinde haberleşmenin iletimi veya bu haberleşmenin faturalandırılması amacıyla işlenen her türlü veriyi,
- l) Veri: Kişisel veri, trafik verisi veya konum verisini,
- ifade eder.

(2) Bu Yönetmelikte geçen ancak birinci fıkrada tanımlanmayan kavramlar ve kısaltmalar için ilgili mevzuatta yer alan tanımlar geçerlidir.

İKİNCİ BÖLÜM

İlkeler ve Uygulama Esasları

İlkeler

MADDE 5 - (1) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

- a) Hukuka ve dürüstlük kurallarına uygun olarak işlenmesi.
- b) Doğru ve gerektiğinde güncel olması.
- c) Belirli, açık ve meşru amaçlar için işlenmesi.
- ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması.
- d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi.

(2) Milli güvenlik gerekçesiyle trafik ve konum verilerinin yurt dışına çıkarılmaması esastır.

Güvenlik

MADDE 6 - (1) İşletmeciler abonelerine/kullanıcılarına ait kişisel verilerin ve sundukları hizmetlerin güvenliğini sağlamak amacıyla Kanuna, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununa, ulusal ve uluslararası standartlara uygun olarak gerekli her türlü teknik ve idari tedbirleri alır. Bu güvenlik tedbirleri, teknolojik imkânlar göz önünde bulundurularak muhtemel riske uygun düzeyde alınır.

(2) Birinci fıkrada belirtilen tedbirler asgari olarak;

- a) 5 inci maddede yer alan ilkeler çerçevesinde kişisel verilerin işlenmesine ilişkin güvenlik politikalarını belirlemeyi,
- b) İstem dışı, yetki dışı ya da mevzuata aykırı olarak; kişisel verilerin tahrip edilmesi, kaybolması, değiştirilmesi, depolanması veya başka bir ortama kaydedilmesi, işlenmesi, ifşa edilmesi ve söz konusu verilere erişilmesi gibi ihlallere karşı kişisel verilerin korunmasını,
- c) Kişisel verilere sadece yetkili kişiler tarafından erişilebilmesini ve kişisel verilerin saklandığı sistemler ile kişisel verilere erişim sağlamak için kullanılan uygulamaların güvenliğini sağlanmasını, içerir.

(3) Kurum, gerekli gördüğü hâllerde alınan güvenlik tedbirlerine ilişkin işletmecilerden, bilgi ve belge isteyebilir, ayrıca idari yaptırım uygulama hakkı saklı kalmak kaydıyla söz konusu güvenlik tedbirlerinde değişiklik talep edebilir.

(4) İşletmeciler, kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtlarını iki yıl saklamakla yükümlüdür.

(5) İşletmeciler, yetkilendirdikleri taraflarca bu Yönetmelik hükümlerinin ihlal edilmesi de dâhil olmak üzere, sundukları hizmetler kapsamında elde ettikleri verilerin gizliliğinin, güvenliğinin, bütünlüğünün, erişilebilirliğinin ve amacı doğrultusunda kullanılmasının temininden sorumludur.

Riskin ve kişisel veri ihlalinin bildirilmesi

MADDE 7 - (1) İşletmeciler, şebekelerinin ve sundukları hizmetlerin güvenliğini tehdit eden belirli bir risk olması durumunda;

a) Bu risk hakkında,

b) Bu riskin işletmeci tarafından alınan tedbirlerin dışında kalması hâlinde, söz konusu riskin kapsamı ve giderilme yöntemleri hakkında,

ilgili aboneleri/kullanıcıları en kısa sürede bilgilendirir.

(2) İşletmeciler, kişisel veri ihlali olması durumunda 6698 sayılı Kanun ve ilgili mevzuata uygun yöntemlerle Kuruma, Kişisel Verileri Koruma Kurumuna ve ilgili abonelere/kullanıcılara en kısa sürede bildirimde bulunur.

Açık rıza alma şartları

MADDE 8 - (1) İşletmeciler, aboneden/kullanıcıdan açık rıza alınmasını gerektiren durumlarda aşağıdaki şartları yerine getirir:

a) Açık rıza beyanı belirli bir konuya ilişkin olarak ilgili işlem öncesinde alınır. Belirli bir konu ile sınırlandırılmayan ve ilgili işlemle sınırlı olmayan genel nitelikteki rızalar geçersiz kabul edilir.

b) Açık rıza beyanı özgür iradeyle açıklanmış olmalıdır. Abonelik tesis edilmesi ve temel elektronik haberleşme hizmetleri veya cihazların sunulması, abonenin/kullanıcının verilerinin işlenmesine yönelik açık rıza verme ön şartına bağlanamaz. Hediye dakika, SMS ve veri gibi ek fayda sağlanması karşılığında aboneden/kullanıcıdan açık rıza talep edilebilir.

c) Abone/kullanıcı, açık rıza beyanının alınması öncesinde; işlenecek kişisel veri türü ile trafik ve konum verisi türleri, kapsamı, işleme amacı ve süresi hakkında işletmeciler tarafından açık ve

anlaşılır bir şekilde bilgilendirilir. Bu bilgilendirmenin yazılı yapılması halinde yazılar en az on iki punto ile hazırlanır.

ç) İşletmecinin gerekli bilgilendirmeyi yapması sonrasında abonenin/kullanıcının “evet/onay/kabul” şeklindeki irade beyanı yazılı veya elektronik ortamda alınır. Söz konusu irade beyanı rıza alınan duruma özgü olmalıdır. Bu irade beyanı, bir sözleşmenin veya hizmetin kabulü ya da pazarlama amaçlı haberleşmelere onay verilmesi ve benzeri hukuki işlemlere yönelik irade beyanları ile birleştirilemez.

d) İşletmeciler, abonelerin/kullanıcıların açık rızalarını gösteren kayıtları, ilgili mevzuat hükümlerinde yer alan süreler saklı kalmak kaydıyla, asgari abonelik süresince saklamakla yükümlüdür.

e) Trafik ve konum verilerinin üçüncü taraflara aktarımının söz konusu olduğu durumlar için;

1) Aktarılabacak verinin kapsamı,

2) Aktarılabacak tarafın adı ve açık adresi,

3) Aktarma amacı ve süresi,

4) Üçüncü tarafın yurt dışında olması halinde verinin aktarılabacağı ülkenin adı,

şeklindeki bilgiler verilerek ayrıca açık rıza alınır. Bu bilgilerde değişiklik olması halinde tekrar açık rıza alınır.

f) İşletmeciler, trafik ve konum verilerinin açık rıza alınarak üçüncü taraflara aktarımının söz konusu olduğu durumlarda, bu verilerin sadece açık rıza bilgilendirmesinde belirtilen üçüncü taraflarca ve belirtilen amaçla işlenmesini temin etmekle yükümlüdür.

Trafik ve konum verilerine ilişkin aydınlatma yükümlülüğü

MADDE 9 - (1) 6698 sayılı Kanununun 10 uncu maddesi hükümleri saklı kalmak üzere, trafik ve konum verilerinin işlenebildiği hallerde işletmeciler, işlenebilecek trafik veya konum verisi türleri, işleme amacı ve süresi hakkında abonelere/kullanıcılara bilgi vermekle yükümlüdür.

ÜÇÜNCÜ BÖLÜM

Sağlanan İmkânlar

Numaranın gizlenmesi

MADDE 10 - (1) İşletmeci, arayan numaranın görünmesine imkân sağladığı durumlarda;

a) Arayan kullanıcıya basit bir yöntemle ve ücretsiz olarak numarasını gizleme imkânı sağlamakla,

b) Aranan aboneye basit bir yöntemle ve ücretsiz olarak, gelen aramalarda arayan numaranın gösterilmesini engelleme imkânı sağlamakla,

c) Arayan kişinin numarasını gizlemesi hâlinde, ancak aranan abonenin/kullanıcının gizli arama alma yönündeki iradesini daha önceden işletmeciye beyan etmiş olması durumunda çağrıyı sonlandırmakla,

yükümlüdür.

(2) İşletmeci, yönlendirilmiş aramalar gibi bağlanılan numaranın görünmesine imkân sağladığı durumlarda, bağlanılan aboneye basit bir yöntemle ve ücretsiz olarak, bağlanılan numaranın arayan kullanıcıya gösterilmesini engelleme imkânı sağlamakla yükümlüdür.

(3) İşletmeci, birinci ve ikinci fıkralarda belirtilen imkânlar hakkında abonelerini/kullanıcılarını kısa mesaj, internet veya benzeri araçlarla bilgilendirmekle yükümlüdür.

(4) Arayan numaranın gizlenmesi imkânı, acil yardım çağrıları için geçerli değildir.

Otomatik çağrı yönlendirme

MADDE 11 - (1) İşletmeci, aboneye/kullanıcıya kendisine üçüncü kişilerden gelen otomatik yönlendirmeleri ücretsiz ve basit yöntemlerle durdurma imkânı tanır.

(2) İşletmeciler tarafından başka bir numaraya veya otomatik mesaj sistemine yapılan yönlendirmelerin ücretli olması hâlinde, abonenin/kullanıcının onayı alınır.

Ayrıntılı faturalarda gizlilik

MADDE 12 - (1) İşletmeciler, abonelerin talep etmeleri hâlinde kullanım detayında veya ayrıntılı faturada yer alan telefon numaralarının bazı rakamlarının gizlenmesini sağlar.

Abonenin/kullanıcının diğer hakları

MADDE 13 - (1) İşletmeciler, abonelerin/kullanıcıların verilerinin işlenmesine yönelik olarak, kısa mesaj, çağrı merkezi, internet ve benzeri yöntemlerle vermiş oldukları açık rızayı aynı yöntem ya da daha basit bir yöntem ile her zaman ücretsiz olarak geri almalarına imkân sağlar. Bu imkâna ilişkin bilgilendirme de açık rıza alınması sırasında yapılır.

(2) İşletmeciler tarafından her yılın üçüncü çeyreği içinde, mobil numara bilgisi bulunan abonelere/kullanıcılara asgari kısa mesajla, diğerlerine e-posta veya arama yöntemlerinden biri ile olmak üzere, daha önce alınan açık rızaları kapsamında verilerinin işlendiğine dair bilgilendirme

yapılır. Aksi durumda daha önce verilen açık rızalar kapsamındaki veri işleme faaliyeti bilgilendirme yapıncaya kadar durdurulur.

(3) İşletmeciler tarafından bu Yönetmelik kapsamında engelli tarifelerinden yararlanan abonelere/kullanıcılara yapılacak bilgilendirmeler, işitsel ve/veya görsel yöntemler kullanılarak Kurum düzenlemelerine uygun şekilde gerçekleştirilir.

(4) Aboneliğin sonlanması halinde, sona erme tarihi itibarıyla, abonenin aksi talebi olmaması halinde daha önce verilen tüm açık rızalar geri alınmış sayılır.

(5) Bu Yönetmelik kapsamındaki abonelere/kullanıcılara yapılacak tüm bilgilendirmeler, ücretsiz olarak gerçekleştirilir.

(6) Bu Yönetmelik kapsamındaki bilgilendirmeler, açık rıza, abone/kullanıcı talebi ve onayına ilişkin ispat sorumluluğu işletmeciye aittir.

(7) Açık rızanın geri alınması durumunda işletmeci açık rızaya dayalı olarak yapılan veri işleme faaliyetlerini derhal durdurur.

DÖRDÜNCÜ BÖLÜM

Çeşitli ve Son Hükümler

İdari para cezaları ve diğer yaptırımlar

MADDE 14 - (1) İşletmecilerin bu Yönetmelik ile belirlenen yükümlülükleri yerine getirmemeleri hâlinde 15/2/2014 tarihli ve 28914 sayılı Resmî Gazete’de yayımlanan Bilgi Teknolojileri ve İletişim Kurumu İdari Yaptırımlar Yönetmeliği hükümleri uygulanır.

Kurumun yetkisi

MADDE 15 - (1) Bu Yönetmeliğin uygulanması sırasında doğacak tereddütleri ve uygulamaya ilişkin aksaklıkları gidermeye ve uygulamayı yönlendirmeye, ilke ve standartları belirlemeye ve uygulama birliğini sağlamaya Kurum yetkilidir.

Yürürlükten kaldırılan yönetmelik

MADDE 16 - (1) 24/7/2012 tarihli ve 28363 sayılı Resmî Gazete’de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik yürürlükten kaldırılmıştır.

Atıflar

MADDE 17 - (1) Mevzuatta 24/7/2012 tarihli ve 28363 sayılı Resmî Gazete’de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmeliğe yapılan atıflar bu Yönetmeliğe yapılmış sayılır.

Mevcut rızaların durumu

GEÇİCİ MADDE 1 - (1) Bu Yönetmeliğin yürürlüğe girdiği tarihten önce hukuka uygun olarak alınmış rızalar geçerli sayılır.

(2) Bu Yönetmeliğin yürürlüğe girdiği tarihten önce rızaları alınarak verileri işlenen tarafların abonelikleri sona ermesine rağmen açık rızaları olmaksızın verilerinin işlenmeye devam etmesi durumunda bu işlem, ilgili mevzuatta yer alan yükümlülükler saklı kalmak kaydıyla, bu Yönetmeliğin yürürlüğe girdiği tarihi takip eden bir ay içinde durdurulur.

Yürürlük

MADDE 18 - (1) Bu Yönetmelik yayımı tarihinden altı ay sonra yürürlüğe girer.

Yürütme

MADDE 19 - (1) Bu Yönetmelik hükümlerini Bilgi Teknolojileri ve İletişim Kurulu Başkanı yürütür.

Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği

Resmî Gazete Tarihi : 28.10.2017

Resmî Gazete Sayısı : 30224

ELEKTRONİK HABERLEŞME SEKTÖRÜNE İLİŞKİN TÜKETİCİ HAKLARI YÖNETMELİĞİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı, elektronik haberleşme sektöründe tüketici hak ve menfaatlerini korumaya yönelik usul ve esasları belirlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, elektronik haberleşme sektöründe tüketici hakları ile işletmeci yükümlülüklerini kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununa dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Yönetmelikte geçen;

- a) Abone: Bir işletmeci ile elektronik haberleşme hizmetinin sunumuna yönelik olarak yapılan bir sözleşmeye taraf olan gerçek ya da tüzel kişiyi,
- b) Abonelik sözleşmesi: İşletmeci ile abone arasında akdedilen ve işletmecinin bir bedel karşılığında dönemsel ya da sürekli olarak bir hizmeti yerine getirmeyi veya mal teminini üstlendiği ya da her ikisini birden kapsayan sözleşmeyi,
- c) Elektronik haberleşme: Elektriksel işaretlere dönüştürülebilen her türlü işaret, sembol, ses, görüntü ve verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesini, gönderilmesini ve alınmasını,

- ç) Elektronik haberleşme hizmeti: Elektronik haberleşme tanımına giren faaliyetlerin bir kısmının veya tamamının hizmet olarak sunulmasını,
- d) İşletmeci: Yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirketi,
- e) Kampanya: İşletmeci tarafından sunulmakta olan elektronik haberleşme hizmetlerinin, ilave edimler dâhil özel şartlarla ve belirli bir süre için sunulmasını,
- f) Kişisel veri: Belirli veya kimliği belirlenebilir gerçek veya tüzel kişilere ilişkin bütün bilgileri,
- g) Kurul: Bilgi Teknolojileri ve İletişim Kurulunu,
- ğ) Kurum: Bilgi Teknolojileri ve İletişim Kurumunu,
- h) Tüketici: Elektronik haberleşme hizmetini ticari veya mesleki olmayan amaçlarla kullanan veya talep eden gerçek veya tüzel kişiyi,
- ifade eder.

(2) Bu Yönetmelikte geçen ancak bu maddenin birinci fıkrasında tanımlanmayan kavramlar için ilgili mevzuatta yer alan tanımlar geçerlidir.

İKİNCİ BÖLÜM

Başlıca Haklar ve Yükümlülükler

Tüketici hakları

MADDE 5 - (1) Elektronik haberleşme hizmetlerinden yararlanan tüketiciler asgarî olarak aşağıda sıralanan haklara sahiptir:

- a) Benzer konumdaki tüketicilerin hizmetlere eşit şartlarda erişebilme ve ayırım gözetmeyen adil ücretlerle hizmetlerden yararlanma hakkı,
- b) Tüketicilerin elektronik haberleşme hizmetine abone olurken bu hizmeti sağlayan işletmeciyile sözleşme yapma hakkı,
- c) Abonelerin kişisel verilerinin kamuya açık rehberlerde yer alıp almamasını talep etme hakkı,
- ç) Rehber ayırım gözetilmeksizin kaydolma ve rehber hizmetinden ücretli ve/veya ücretsiz yararlanma hakkı,
- d) Acil arama hizmetleri hakkında bilgilendirilme ve bu hizmetlere ücretsiz erişebilme hakkı,
- e) Abonelerin ayrıntılı fatura talep edebilme hakkı,

- f) İşletmecinin sunacağı elektronik haberleşme hizmetinin kapsamı hakkında bilgi alabilme hakkı,
- g) Abonelere sunulan hizmet için uygulanacak tarifeler/kampanyalar konusunda açık, detaylı ve güncel bilgilere erişebilme hakkı ile tarifelerdeki/kampanyalardaki değişiklikler yürürlüğe girmeden önce bilgilendirilme hakkı,
- ğ) Abonelerin katma değerli elektronik haberleşme hizmetleri de dâhil olmak üzere kısa mesaj, müşteri hizmetleri, internet ve benzeri yöntemlerle katıldıkları tarife, kampanya ve benzeri kapsamda sunulan tüm hizmetlerden başvurduğu yöntem ya da basit bir yöntem ile vazgeçme hakkı,
- h) Arızaların giderilmesinde, sağlık, yangın, afet, güvenlik ve benzeri acil durum ve güvenlikle ilgili kurum ve kuruluşlar ile ilgili mevzuat hükümleri saklı kalmak kaydıyla, benzer konumdaki tüketiciler arasında ayırım gözetmeme temelinde bir uygulamayı talep etme hakkı,
- ı) Uluslararası standartlar ile Kurumun belirleyeceği standartlara uygun kalitede hizmetten yararlanma hakkı.

Şeffaflık ve bilgilendirme

MADDE 6 - (1) İşletmeciler, sundukları elektronik haberleşme hizmetlerine erişim ve bu hizmetlerin kullanımı ile ilgili olarak asgari aşağıdaki bilgiler olmak üzere, özellikle hizmetler arasında seçim yapılırken ve abonelik sözleşmesi kurulurken tüketicilerin karar vermelerinde etkili olabilecek hususlar ile dürüstlük kuralı gereğince bilgilendirilmelerinin gerekli olduğu her durumda talep olmaksızın tüketicileri bilgilendirmekle ve bu bilgilere kolayca ulaşılabilmesini sağlamakla yükümlüdür:

- a) İşletmecinin adı, unvanı ve adresi,
- b) Sunulacak hizmete ilişkin olarak; hizmetin tanımı ve kapsamı, hizmete erişim ve hizmetin kullanımı konusunda genel hüküm ve şartlar, hizmet için uygulanacak tarifeler ve varsa abonelik paketleri, tarifelerin içerdiği vergi türleri ile bu vergilerin tarifeler hesaplanırken tarifelere yansıtılma oranı, doğru tüketici algısının oluşması amacıyla tarifelerin yalnızca tüm vergiler dahil değeri, abonelik tesisi dolayısıyla alınacak diğer ücretler, tarife ücreti ile birlikte telsiz kullanım ücreti yansıtılacağına dair abonenin doğru değerlendirme yapabileceği açıklıkta bilgi,
- c) Taahhütnamelere ilişkin şartlar, sunulan bakım/onarım hizmetlerine ilişkin genel bilgi ve standart sözleşme şartları ile geri ödeme şartları ve/veya işletmecinin kusurundan kaynaklanan nedenlerle sözleşmede belirtilen hizmet kalite seviyesinin sağlanamaması halinde zararın giderilmesine ilişkin bilgi,

ç) Tüketici şikâyetlerinin çözüm usul ve süreçlerine ilişkin bilgi.

(2) İşletmeci, Kurum düzenlemelerine uygun internet sitesi kurmak veya mevcut internet sitesini bu düzenlemelere uygun hale getirmekle yükümlüdür. İşletmeciler internet sitelerinden şikâyet başvurularının iletilebilmesini ve tüketicinin tam ve gereği gibi bilgilendirilmesini sağlar. İnternet sitelerinde tarife, kampanya ve diğer ücretler ile arıza giderilmesine ilişkin genel hususlar ve fesih gibi hizmet sunum koşulları başta olmak üzere gerekli bilgilere yer verilir.

(3) Bu Yönetmelik kapsamında abonelere yapılacak bilgilendirme yöntemlerinde Kurum tarafından gerekli görülmesi halinde değişiklik yapılabilir.

ÜÇÜNCÜ BÖLÜM

Abonelik Sözleşmesinin Şekli, İçeriği ve Uygulanması

Abonelik sözleşmelerinin kuruluşu ve içeriği

MADDE 7 - (1) İşletmecinin dönemsel ya da sürekli olarak bir hizmeti yerine getirmeyi veya mal teminini üstlendiği durumlarda tarafların birbirine uygun karşılıklı rızası ile abonelik sözleşmesi yapılır. Abonelik sözleşmeleri, elle atılan imza ve güvenli elektronik imza ile yapılabilir. Sözleşmenin kuruluşu ve uygulanması sürecine ilişkin tüm tedbirlerin alınmasına yönelik sorumluluk işletmecide olmak şartıyla Kurum tarafından belirlenecek usuller ile elektronik ortamda abonelik sözleşmesi akdedilebilir. Kurum abonelik sözleşmeleri ile ilgili işletmecilere ilave yükümlülükler getirebilir.

(2) İşletmeciler, abonelik sözleşmelerinde asgari aşağıdaki bilgilerin yer almasını sağlamakla yükümlüdür:

a) Sözleşmenin konusu,

b) Sözleşmenin yapıldığı yer ve tarih,

c) Sözleşme taraflarının isim, unvan ve açık adresleri ile hizmet numarası gibi aboneliği tanımlayıcı bilgi,

ç) Tarafların yükümlülükleri,

d) Sözleşmenin süresi, feshi ve yenilenmesine ilişkin şartlar,

e) Sunulacak hizmetlerin tanımı, hizmet kalitesi seviyeleri ve ilk bağlantının gerçekleştirileceği süre,

f) Sunulacak bakım/onarım hizmetlerine ilişkin genel bilgi,

g) Uygulanacak tarifelerin içeriği ve tarifelerdeki değişiklikler hakkında güncel bilgilerin hangi yollardan öğrenilebileceği,

ğ) İşletmecinin kusurundan kaynaklanan nedenlerle sözleşmede belirtilen hizmet kalitesi seviyesinin sağlanamaması halinde zararın giderilmesi ve/veya geri ödemeye ilişkin prosedür,

h) Abonenin fatura bedelini süresi içerisinde ödememesi durumunda; hizmet sunumunun ne şekilde ve asgari olarak ne kadar süre içerisinde durdurulabileceğine/kısıtlanabileceğine ilişkin bilgi ile hukuki sonuçlara (temerrüt, yasal takip ve benzeri) ilişkin bilgi,

ı) Abone tarafından sözleşme tarihinde tercih olunan tarife ve abonelik paketi,

i) Abone ile işletmeci arasında uzlaşmazlık çıkması halinde yargı yolu da dâhil olmak üzere uygulanacak çözüm prosedürü,

j) Abonenin hizmetten yararlanabilmesi için gerekli olan teknik ekipman, cihaz ve donanıma ilişkin bilgi,

k) Hizmetten yararlanılması sırasında oluşabilecek güvenliği tehdit eden durumlara karşı işletmeci ve abone tarafından alınacak ya da alınması gereken tedbirler,

l) Onaylanması gereken abonelik sözleşmelerinin Kurum tarafından onaylandığı tarih,

m) Cihaz temini içeren hizmetlerde işletmecinin de cihazın ayıbından sorumlu olduğuna ilişkin bilgi,

n) Tüketiciden güvence, depozito veya teminat adı altında bir ücret alınması söz konusu ise bu ücretin tutarı ve aboneliğin sona ermesi durumunda tüketiciye ne kadar süre içerisinde ve ne şekilde iade edileceğine ilişkin bilgi,

o) Sözleşmenin feshedilmesi halinde, modem, telefon, uydu alıcısı ve benzeri cihazların işletmeciye iadesi öngörülüyorsa iade sürecine ve cihazın arızalanması halinde izlenecek sürece ilişkin bilgi.

(3) Abonelik sözleşmelerinin en az on iki punto ile hazırlanması, aboneye yükümlülük getiren hususların açık, sade ve anlaşılabilir şekilde siyah koyu harflerle belirtilmesi ve tip abonelik sözleşmelerinin kolay erişilebilir bir şekilde işletmecilerin internet sitelerinde yayınlanması zorunludur.

(4) İşletmeci bu Yönetmeliğe uygun şekilde düzenlenmiş abonelik sözleşmesinin eksiksiz tanzim edilmesiyle yükümlüdür.

(5) İşletmeci, abonelik sözleşmelerinin güvenli elektronik imza ile kurulması halinde kimlik belgesi örneğini temin etmekle yükümlüdür.

(6) Abonelik sözleşmelerinin elle atılan imza ile kurulması halinde, işletmeci abonelik sözleşmesinin yanında;

- a) Bireysel aboneliklerde T.C. Kimlik Numarası ile kimlik belgesinin,
- b) Kurumsal aboneliklerde yetkili kişinin T.C. Kimlik Numarası ve kimlik belgesi ile temsile yetkili olduğuna dair belge ile imza sirkülerinin,
- c) Yabancı uyrukluların aboneliklerinde geçerlilik tarihi uygun pasaport, uluslararası geçerliliği olan muadili belge veya ulusal geçerliliği olan kimlik muadili belgenin,

birer örneğini almakla yükümlüdür. Abonelik tesisi için gerekli kimlik belgesi veya muadili belgelerin aslının ibrazı istenir. İşletmeci tarafından bu belgelerin örneği asılları üzerinden ve yalnızca uygun elektronik ortama aktarılarak alınır.

(7) İşletmeciler, abonelik sözleşmelerini ve sözleşmenin tesisi için gerekli bilgi ve belgeleri kuruluş şekline uygun olarak muhafaza etmekle yükümlüdür.

(8) Abonenin hattının kullanıma açılabilmesi için, abonelik sözleşmesinin tesisine ilişkin belgelerin tam olduğu ve söz konusu belgelerdeki bilgilerin doğruluğu işletmeci tarafından kontrol edilerek gerekli teyit işlemi İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü Kimlik Paylaşımı Sisteminden yapılır.

(9) Akdedilen abonelik sözleşmelerinin bir nüshası, abone tarafından aksi belirtilmedikçe sözleşmenin kuruluş şekline göre kâğıt üzerinde veya uygun elektronik ortamda aboneye verilir.

(10) Abonelik sözleşmesi yapılırken rehber hizmetleri için, aboneden bu rehberlerde kişisel verilerinin yer alıp almayacağına ilişkin tercihleri alınır.

(11) İşletmeciler görme engelli olan tüketicilerin talep etmesi halinde abonelik sözleşmelerini ve faturalarını asgari olarak Braille alfabesi ya da sesli olarak dinleterek ücretsiz sunarlar.

(...)

İnternet Alan Adları Yönetmeliđi

Resmî Gazete Tarihi : 07.11.2010

Resmî Gazete Sayısı : 27752

İNTERNET ALAN ADLARI YÖNETMELİĐİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak, Tanımlar ve İlkeler

Amaç ve kapsam

MADDE 1 - (1) Bu Yönetmeliđin amacı; “.tr” uzantılı İnternet alan adları yönetimine ilişkin usul ve esasları düzenlemektir.

Dayanak

MADDE 2 - (1) Bu Yönetmelik, 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun 5 inci, 34 üncü ve 35 inci maddelerine dayanılarak hazırlanmıştır.

(...)

ÜÇÜNCÜ BÖLÜM

Kurumun Görevleri ve Yetkileri

Kurumun görevleri

MADDE 14 - (1) Kurumun görevleri aşağıda yer almaktadır;

- a) TRABİS'i kurmak ve işletmek veya belirlediđi usul ve esaslar çerçevesinde TRABİS'in üçüncü bir tarafça kurulması ve işletilmesini sağlamak,
- b) UÇHS'leri ve KK'ları belirlemek ve bunların iletişim bilgilerini İnternet sitesinde yayımlamak,
- c) Alan adı tahsis ve yenilemesine ilişkin ücretler ile uyumsuzluk çözüm mekanizmasının işletilmesi ile ilgili işlemlere ilişkin ücretleri belirlemek ve gerektiğinde deđişiklik yapmak,
- ç) Tahsise açılacak veya kullanımına son verilecek alt alan adlarını belirlemek,
- d) Belgeli tahsis edilen alt alanların tahsisinde istenecek belgeleri belirlemek,

- e) Bu Yönetmelikte belirtilen veya Kurul tarafından belirlenen hallerle sınırlı olmak kaydıyla KK niteliğinde faaliyet yürütmek,
- f) (Değişik:RG-20/4/2021-31460) Alan adı ihtilaflarına ilişkin kendisine iletilen mahkeme kararlarını, UÇHS'nin kendisine ilettiği ihtilafa konu olan alan adları ile hakem veya hakem heyeti kararlarını İnternet sitesinde, kişisel verilerin korunması amacıyla gerekli önlemleri de alarak güncel olarak bulundurmak,
- g) Kendisine iletilen talep ve şikâyetleri değerlendirmek ve mevzuat çerçevesinde gerekli tedbirleri almak,
- ğ) Her yıl Nisan ayı sonuna kadar bir önceki yıla ait faaliyet raporunu hazırlayarak Kurumun internet sitesinden ve gerekli olduğu hallerde diğer uygun araçlarla kamuoyuna duyurmak,
- h) ICANN, RIPE NCC, CENTR gibi kuruluşlar nezdinde gerekli çalışmaları yürütmek.
- (...)

Sosyal Yardım Verilerinin Kaydedilmesine ve Paylaşılmasına İlişkin Yönetmelik

Resmî Gazete Tarihi : 13.09.2014

Resmî Gazete Sayısı : 29118

SOSYAL YARDIM VERİLERİNİN KAYDEDİLMESİNE VE PAYLAŞILMASINA İLİŞKİN YÖNETMELİK

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı;

a) (Değişik:RG-6/7/2019-30823) Aile, Çalışma ve Sosyal Hizmetler Bakanlığı Sosyal Yardımlar Genel Müdürlüğüne, Sosyal Yardımlaşma ve Dayanışma Vakıfları ile işbirliği içinde yürütülen sosyal yardım faaliyetlerine ilişkin verilerin kişinin ya da kurumun mahremiyeti, maddi ve manevi varlığı ile temel hak ve özgürlüklerini koruyarak kaydedilmesine,

b) Sosyal yardım faaliyeti yürüten diğer kamu kurum ve kuruluşları ile mahalli idareler ve Türkiye Kızılay Derneği tarafından yürütülen sosyal yardım faaliyetlerine ilişkin verilerin karşılıklı olarak paylaşılmasına,

c) Bilimsel çalışmalarda söz konusu verilerin anonimleştirilerek kullanılmasına,

ç) Veri güvenliğinin sağlanmasına,

ilişkin usul ve esasların düzenlenmesidir.

Kapsam

MADDE 2 - (Değişik:RG-6/7/2019-30823)

(1) Bu Yönetmelik; sosyal yardıma başvuran kişi ve hanelere ilişkin verilerin toplanması, kaydedilmesi, Aile, Çalışma ve Sosyal Hizmetler Bakanlığınca diğer kamu kurum ve kuruluşları ve karşılıklılık ilkesine göre mahalli idareler ve Türkiye Kızılay Derneği ile toplanan verilerin paylaşılması ve yoksullukla mücadele ve sosyal yardım alanındaki bilimsel çalışmalara anonimleştirilmiş veri sağlanmasına ilişkin düzenlemeleri kapsar.

Dayanak

MADDE 3 - (Değişik:RG-6/7/2019-30823)

(1) Bu Yönetmelik, 3/6/2011 tarihli ve 633 sayılı Sosyal Hizmetler Alanında Bazı Düzenlemeler Hakkında Kanun Hükmünde Kararnamenin 33 üncü maddesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Yönetmelikte geçen;

a) Aktif dosya: İşlem zamanı itibarıyla durumu aşağıdaki tanımlardan en az birine uygun olan hanelere ait dosyaları;

1) Düzenli yardım programlarından faydalanan en az bir kişi bulunan haneler.

2) SYDV'ler tarafından yapılan genel sağlık sigortası gelir testine göre gelir durumu kişi başına brüt asgari ücretten az olan (G0 veya G1) en az bir kişi bulunan haneler.

3) Son bir yıl içinde en az bir defa süreli yardım alan en az bir kişi bulunan haneler.

4) Şartlı sosyal yardımlar kapsamında izleme, takip süreci devam eden haneler.

b) Açık rıza: İlgili kişilerin sosyal yardım kapsamındaki kişisel verilerinin işlenmesine, paylaşılmasına ve kullanılmasına özgür iradesiyle verdiği ispatlanabilir yazılı kabul beyanı,

c) Alıcı: Paylaşım açılacak verilerden, yapılacak protokol/sözleşme çerçevesinde yararlanan kamu kurum ve kuruluşlarını, mahalli idareleri ve Türkiye Kızılay Derneği ile veri paylaşımı yapılması Kurul tarafından uygun bulunacak gerçek ve tüzel kişileri,

ç) Anonimleştirilmiş veri: Kişisel verilerin, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde düzenlenmiş halini,

d) (Değişik:RG-6/7/2019-30823) Bakanlık: Aile Çalışma ve Sosyal Hizmetler Bakanlığını,

e) (Değişik:RG-6/7/2019-30823) Bakan: Aile, Çalışma ve Sosyal Hizmetler Bakanını,

f) Bütünleşik sistem: Bütünleşik Sosyal Yardım Bilgi Sistemini,

g) Düzenli yardım: Hane veya kişiye hak sahipliği kriterlerini kaybedinceye kadar ve başka bir başvuru yapma şartı aranmaksızın düzenli olarak, belirli periyotlarda yapılan sosyal yardımları,

ğ) GO: Bakanlık tarafından belirlenen usul esaslar çerçevesinde yapılan gelir tespitinde hesaplanan hane içinde kişi başına düşen brüt asgari ücretin üçte birinden az tutardaki gelir seviyesini,

h) G1: Bakanlık tarafından belirlenen usul esaslar çerçevesinde yapılan gelir tespitinde hesaplanan hane içinde kişi başına düşen brüt asgari ücretin üçte birinden fazla ancak asgari brüt ücretten az tutardaki gelir seviyesini,

ı) Genel Müdür: Sosyal Yardımlar Genel Müdürünü,

i) Genel Müdürlük: Sosyal Yardımlar Genel Müdürlüğünü,

j) Hane: Aralarında akrabalık bağı bulunsun ya da bulunmasın adres kayıt sistemindeki kayıtlara göre aynı konutta ya da aynı konutun bir bölümünde yaşayan bir kişiyi veya birden fazla kişiden oluşan topluluğu,

k) Hısım: 4721 sayılı Türk Medeni Kanununun 17 nci maddesinde tanımlanan kan hısımlığı,

l) İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,

m) Karşılıklılık ilkesi: Mahalli idareler ve Türkiye Kızılay Derneği ile veri paylaşımında geçerli olan ve sadece protokol yapılan kurumların bu Yönetmelik kapsamında belirlenen verileri karşılıklı olarak paylaşacağını belirten ilkeyi,

n) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin sosyal yardım sürecinde elde edilen bütün bilgileri,

o) Kurul: Bakanlık bünyesinde oluşturulan Veri Paylaşımı Kurulunu,

ö) Sosyal inceleme: Sosyal yardım başvurusu yapan kişilerin muhtaçlığının tespiti ve başvuru sırasında verilen bilgilerin teyidinin yapılabilmesi için ilgili kurumların görevlendirdiği personel tarafından yapılan hane ziyaretini ve çevre araştırmasını,

p) Sosyal yardım: İhtiyaç sahibi hanelere ve kişilere; muhtaçlıkları nedeniyle tek taraflı karşılıksız olarak ve/veya kamu hizmetlerine katılım, geri ödeme gibi bir edimi yerine getirme şartına/şartlarına dayalı olarak yapılan aynı ve nakdi yardımları,

r) Süreli yardım: Hane veya kişiye düzenli olmaksızın başvurusu sonucunda yapılan tek seferlik yardımları,

s) SYDV: 3294 sayılı Kanun kapsamında kurulan sosyal yardımlaşma ve dayanışma vakıflarını,

ş) Veri: Sosyal yardım sürecinde elde edilen kişilere ait nicel ve/veya nitel bilgileri,

ifade eder.

Genel ilkeler

MADDE 5 - (1) Kişisel verilerin; toplanmasında, kaydedilmesinde ve paylaşılmasında aşağıdaki ilkelere uyulması zorunludur;

- a) Hukuka ve dürüstlük kurallarına uygun olmak,
- b) Doğruluk ilkesine bağlı olmak,
- c) Verileri belirli, açık ve meşru amaçlar için işlemek,
- ç) Toplandıkları veya işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmak,
- d) Elde edilmesi mümkün olmayan veriler hariç olmak üzere verileri eksiksiz ve doğru işlemek,
- e) Verileri güncel tutmak,
- f) Başvuranın ve hane halkının psikolojik açıdan zarar görmemesi ve sosyal çevresinde rencide edilmemesi için azami özen göstermek.

(2) Mahalli idareler ve Türkiye Kızılay Derneği ile karşılıklılık ilkesine göre yapılacak veri paylaşımları bu Yönetmelik kapsamındadır. Türkiye Kızılay Derneği doğrudan; mahalli idareler ise doğrudan veya Türkiye Belediyeler Birliği, İçişleri Bakanlığı Mahalli İdareler Genel Müdürlüğü aracılığıyla Genel Müdürlük ile yapacakları protokol kapsamında, bu Yönetmelikte yer alan usullere uygun olarak veri paylaşımı gerçekleştirebilirler. Karşılıklılık ilkesine uygun protokol yapılmadan bu Yönetmeliğin veri paylaşımına ilişkin hükümleri uygulanmaz ve veri paylaşımı gerçekleştirilmez. Protokol imzalayan mahalli idareler ve Türkiye Kızılay Derneği ile yapılacak veri paylaşımlarında bu Yönetmeliğin ikinci bölüm hükümleri, 7 nci maddenin birinci fıkrasının (c) bendi hariç olmak üzere, uygulanmaz.

İKİNCİ BÖLÜM

Kişisel Verilerin Toplanması, Kaydedilmesi ve Güncellenmesi

Kişisel verilerin toplanması

MADDE 6 - (1) Sosyal yardım başvurularında hanede yaşayan kişilere ve hanenin refahına ilişkin olarak Genel Müdürlük tarafından belirlenerek Bakanlık web sayfasında yayınlanan bilgiler toplanır. Yardım programının özelliğine göre başvuru sırasında belirtilmek üzere ek bilgiler talep edilebilir.

(2) Kişilerin ırkı, etnik kökeni, siyasî düşüncesi, felsefî inancı, dini, mezhebi veya diğer inançları, özel nitelikli kişisel veriler olup bunların özel olarak toplanması veya veri toplama esnasında amaçlanmadığı halde elde edilmesi durumunda hukuka aykırı olarak işlenmesi, herhangi bir kişiyle veya kurumla paylaşılması yasaktır.

(3) Kişisel veriler aşağıda sayılan durumlar hariç olmak üzere ilgili kişilerin açık rızası olmaksızın toplanamaz ve işlenemez;

a) Kanunlarda ve yönetmeliklerde açıkça öngörülmesi,

b) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

(4) İlgili kişilerin rızası, başvuru sırasında Başvuru Formunun imzalatılması suretiyle alınır. Başvuru Formu Genel Müdürlük tarafından hazırlanarak Bakanlık web sayfasında yayınlanır.

(5) Hanenin muhtaçlığı nedeniyle yapılan sosyal yardımlarda adres kayıt sistemine göre hanede yaşayanların ve hane refahını paylaşan ve/veya etkileyen hısımların verileri bu maddenin 4 üncü fıkrasında belirtilen yöntemle toplanır.

(6) Sosyal yardıma başvuran kişiye ve hanesine ilişkin bilgiler;

a) Başvuru esnasında gerekli formların kişinin beyanı ile doldurulması yoluyla,

b) Protokoller çerçevesinde kamu kurum ve kuruluşlarının veri tabanları ile Mahalli İdarelerin ve Türkiye Kızılay Derneğinin veri tabanlarından elektronik ortamda yapılacak sorgulamalar yoluyla,

c) Kişinin sosyal yardım için başvurduğu kurumun görevlendirdiği personel tarafından kişinin hanesinde yapılacak sosyal inceleme yoluyla,

toplanır.

(7) Kişisel verilerin elde edilmesi sırasında görevli personel, başvuran kişiye veya sosyal inceleme sırasında görüşme yapılan kişiye;

a) Kendisinin kimliği,

b) Verilerin hangi amaçla işleneceği,

c) İşlenen verilerin kimlere ve hangi amaçla aktarılabilmesi,

ç) Veri toplamanın yöntemi ve hukukî sebebi,

konusunda bilgi vermekle yükümlüdür.

Kişisel verilerin kaydedilmesi

MADDE 7 - (1) Veriler aşağıdaki sürelerde veri tabanına kaydedilir ve paylaşımına hazır hale getirilir.

a) SYDV'ler sosyal yardım işlemlerini başvurudan itibaren bütünleşik sistem üzerinden, eşzamanlı olarak yürütür. Genel Müdürlük SYDV'lerin kaydettiği verilerin, eşzamanlı olarak paylaşımına hazır hale getirilmesini sağlar.

b) Genel Müdürlük haricinde sosyal yardım faaliyeti yürüten diğer kamu kurum ve kuruluşları yardım yapılmasına onay veren belgelerin oluşturulması ile eşzamanlı olarak verilerin kaydedilmesini ve paylaşımına hazır hale getirilmesini sağlar.

c) Mahalli idareler ve Türkiye Kızılay Derneği karar tarihinden itibaren eşzamanlı olarak verilerin kaydedilmesini ve paylaşımına hazır hale getirilmesini sağlar.

(2) Veri tabanına başvuruyu yapan kişi ve hanesine ilişkin;

a) Kimlik bilgileri,

b) Başvurulan yardım türü ve tutarı,

c) Başvurulan yardım programının düzenli yardım veya süreli yardım şeklindeki niteliği,

ç) Yardım hak sahipliğine ilişkin kararın sonucu ve tarihi,

d) Yardım teslim tarihi ve aynı veya nakdi teslim yöntemi,

e) Yardımın feshedilmesi, durdurulması veya sonlandırılması durumlarında karar tarihi ve nedeni,

f) Sosyal incelemede ve kişilerin beyanlarından elde edilen bilgiler,

g) Sosyal yardım sistemindeki değişiklikler ve ortaya çıkacak bilgi ihtiyaçları çerçevesinde Kurul tarafından belirlenecek diğer bilgiler,

kaydedilir.

Kişisel verilerin güncellenmesi

MADDE 8 - (1) SYDV'ler, veri tabanlarından elektronik ortamda yapılacak sorgulamaları, her bir başvurunun karar ve inceleme işlemlerinde yenilerler. Ayrıca, aktif dosyası bulunan hanelerin sosyal incelemeleri en az yılda bir defa yenilenir.

(2) SYDV'de dosyası bulunan haneler, başvuruları esnasında altıncı maddenin altıncı fıkrasının (a) bendinde belirtilen şekilde verdikleri beyanlarındaki değişen bilgileri güncellerler.

Verilerin doğruluğuna ilişkin sorumluluk

MADDE 9 - (1) Kişisel verilerin toplanması, kaydedilmesi ve güncellenmesi esnasında hanenin gerçek durumunu ortaya koyacak işlemlerin yapılmaması ya da hanenin beyanının ve tespit edilen hususların gerçeğe uygun şekilde kayıt altına alınmaması nedeniyle kamu kaynağının hak etmeyen kişilere aktarılması sonucu oluşacak kamu zararından veya oluşabilecek kişi mağduriyetlerinden, işlemi yapması gerektiği halde yapmayan veya hatalı kaydı yapan personel sorumludur.

ÜÇÜNCÜ BÖLÜM

Veri Paylaşım Esasları

Gizli veriye ilişkin hükümler

MADDE 10 - (1) Genel Müdürlük ilgili birimlerine yapılan tüm veri talepleri kapsamında;

a) 9/10/2003 tarihli ve 4982 sayılı Bilgi Edinme Hakkı Kanununda açıkça belirtildiği üzere, açıklanması hâlinde Devletin emniyetine, dış ilişkilerine, millî savunmasına ve millî güvenliğine açıkça zarar verecek ve niteliği itibarıyla Devlet sırrı olan gizlilik dereceli bilgiler,

b) Kişilerin doğrudan veya dolaylı bir şekilde sahip olduğu özellikleri ile tanınabilmesine ve bu şekilde bireysel bilgilerin açığa çıkarılması ile söz konusu kişilerin itibarını zedeleyebilecek, maddi hasara uğratabilecek veya yasal yaptırımlara maruz bırakabilecek TC kimlik numarası ile kimliği teşkil eden her türlü bilgiler (ad, soyad, anne adı, baba adı, nüfus cüzdanı seri no, cilt no ve benzeri), gizli veri niteliğinde değerlendirilir.

(2) İlgili mevzuat hükümleri nedeniyle bilgileri resmi kayıtlarda gizli tutulan kişilerin bilgileri gizli veri niteliğindedir.

Kişisel ve ticari sır niteliğindeki verilerin korunması

MADDE 11 - (1) Veri tabanında yer alan kişisel bilgilerin gizliliği esastır.

(2) Verilerin paylaşımında; Anayasa, uluslararası sözleşmeler ve ulusal mevzuatta yer alan özel hayatın gizliliğine ve ticari sır niteliğindeki verilerin korunmasına ilişkin hükümler esas alınır.

Veri paylaşım prosedürü

MADDE 12 - (1) Bakanlık ile kamu kurum ve kuruluşları arasındaki veri paylaşımı ve bilimsel çalışmalar için veri paylaşımı aşağıdaki hususlar çerçevesinde sürekli veri paylaşımı veya tek seferlik veri paylaşımı şeklinde yürütülür.

a) Sürekli veri paylaşımı/web servis talepleri karşılanırken kamu kurum/kuruluşlarının verileri alabilmesi için protokol veya sözleşme imzalamaları zorunludur.

b) Tek seferlik veri talepleri karşılanırken Kurul tarafından uygun görülen talepler Genel Müdürlüğe iletilir. Söz konusu taleplerde gizli veri istenmesi durumunda, kişi, kamu kurum/kuruluşlarının verileri alabilmesi için protokol veya sözleşme imzalamaları zorunludur.

c) Tek seferlik veri taleplerinde alıcı tarafın verileri teslim alabilmesi için kullanım amacını, süresini içeren gizlilik taahhüt belgesi imzalaması ve Genel Müdürlüğe vermesi zorunludur. Kurul verilerin

kullanım süresini talep edilen süreye bağlı kalınmaksızın belirleyebilir. Veriler beyan edilen amaç ve belirlenen süre dışında kullanılamaz.

ç) Yükseköğretim kurumları tarafından bünyelerinde yürütülen bilimsel araştırmalarda, yüksek lisans ve doktora tezi çalışmalarında kullanılmak üzere tek seferlik veri talebi yapılabilir. Yükseköğretim kurumu ve bilimsel araştırmayı, tez çalışmasını yürüten kişi, alıcının yükümlülükleri bakımından müteselsilen sorumludur. Söz konusu kişi tarafından, ilgili yükseköğrenim kurumunun çalışmayı ve talep edilen verileri açıklayıcı talep yazısının teslim edilmesi zorunludur. Ancak bu talepler gizli veri niteliğinde olan verilere yönelik olamaz.

d) Bu fıkranın (ç) bendi kapsamında alınan verilerin kullanıldığı bilimsel araştırma, tez ve benzeri çalışmaların bir örneği alıcı tarafından basılı ve elektronik ortamda çalışmanın niteliğine göre Genel Müdürlük tarafından belirlenen formatta, çalışmanın tamamlanma tarihinden itibaren bir ay içinde Genel Müdürlüğe teslim edilir. Bu çalışmaların yayımlanması durumunda; verilerin Genel Müdürlükten temin edildiği ancak çalışmayı yürüten kişi ve/veya kurum ve kuruluşların sorumluluğunda olduğu belirtilir.

e) Protokol/sözleşme metni, Bakanlık adına Genel Müdür veya Genel Müdürlük Araştırma Geliştirme ve Tanıtım Dairesinin bağlı olduğu genel müdür yardımcısı tarafından imzalanır. Islak imzalı nüshalardan birisi veri talep eden kurumda, diğer imzalı nüsha ise Genel Müdürlükte muhafaza edilir.

f) Protokol/sözleşmelerin süresini belirlemeye, yenilenip yenilenmemesine karar vermeye ve protokol/sözleşmeleri feshetmeye Genel Müdürlük yetkilidir.

(2) Bakanlık ile mahalli idareler arasındaki veri paylaşımı sürekli veri paylaşımı yöntemiyle, protokol veya sözleşme imzalanması suretiyle yapılır. Veri paylaşımı aşağıdaki hususlar çerçevesinde yürütülür:

a) Mahalli idareler ile yapılan veri paylaşımı karşılıklılık ilkesi çerçevesinde gerçekleştirilir. Yapılan protokolde paylaşılacak verilere açıkça yer verilir.

b) Bakanlık, mahalli idareler ile doğrudan protokol yapabileceği gibi mahalli idareler adına Türkiye Belediyeler Birliği veya İçişleri Bakanlığı Mahalli İdareler Genel Müdürlüğü ile de protokol yapabilir.

(3) Bakanlık ile Türkiye Kızılay Derneği arasındaki karşılıklılık ilkesine göre veri paylaşımı, sürekli veri paylaşımı yöntemiyle, protokol veya sözleşme imzalanması suretiyle yapılır. Tek seferlik veri talepleri bu maddenin birinci fıkrasının (b) ve (c) bentleri kapsamında yapılır.

(4) Bakanlık; mahalli idarelerin ve Türkiye Kızılay Derneğinin, karşılıklılık ilkesine uygun şekilde veri paylaşımı yapmadığını, protokol veya sözleşmelerde belirtilen şartlara uymadığını, veri paylaşımı yapabilme yeterliliğini teknik yönden kaybettiğini tespit etmesi halinde veri paylaşımını Kurul kararıyla durdurur.

Verilerin iletildiği kişi, kurum/kuruluşlara düşen görevler

MADDE 13 - (1) Alıcının yükümlülükleri;

a) Alıcı, veri talebine uygun olarak yaptığı çalışmaların, gizli verilerin açıklanmasına imkân vermeyecek şekilde yürütülmesini sağlar. Verilerin istenilen amaç dışında kullanılmaması için her türlü önlemi alır ve verinin incelenip değerlendirilmesi aşamasında, gizli verinin bulunduğu ortama yetkisiz kimselerin fiziksel veya elektronik yollarla erişiminin engellenmesi için gerek duyulan güvenlik sistemini kurar veya gerekli tedbirleri alır.

b) Genel Müdürlük tarafından görüntülenmesi sağlanan veya elektronik ya da benzeri usullerle gönderilen veriler, kişisel verilerin gizliliği ilkesine bağlı kalmak şartıyla ilgili mevzuat, uluslararası anlaşmalar ve kamu hizmetinin gerektirdiği yükümlülöklere göre kullanılır. Paylaşılan verilerin yetkisi olmayan kişi, kurum ve kuruluşların eline geçmemesi için gerekli tüm tedbirler alınır.

c) Veri güvenliğinin sağlanması konusunda her türlü sorumluluk süre ile sınırlandırılmaksızın veri talebinde bulunan kişi, kurum/kuruluşlara aittir.

ç) Alıcı, paylaşılan verileri üçüncü şahısların kullanımına sunamaz ve yayımlayamaz.

d) Her türlü sorumluluk alıcıya ait olmak üzere, kamu kurum ve kuruluşlarının kanunun emredici hükmünden kaynaklanan bir görevi ifa etmesi durumunda bu fıkranın (ç) bendi hükmü uygulanmaz.

(2) Uygulanacak müeyyideler:

a) Verilerin kötüye kullanılmasından doğacak her türlü hukuki, mali ve cezai sonuçlardan alıcı sorumludur. Bu kapsamda verilerin kullanılmasında ve paylaşımında Anayasa, uluslararası sözleşmeler ve ulusal mevzuatta yer alan özel ve ticari hayatın gizliliğine ilişkin hükümler uygulanır.

b) Gizli verilerin korunması ile ilgili hükümleri ihlal eden kişiler Türk Ceza Kanununun Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar Bölümünün ilgili maddelerince suç işlemiş sayılır.

c) Kurum tarafından kendilerine erişim yetkisi verilen kişilerden, gizli verileri değiştiren veya bütünlüğünü bozanlar Türk Ceza Kanununun Bilişim Alanında Suçlar Bölümünün ilgili maddelerince suç işlemiş sayılır.

İstisnai durumlar

MADDE 14 - (1) Aşağıda belirtilenlerin veri talebinde bulunması halinde 12 nci madde hükümleri uygulanmaz.

- a) Bakanlığın denetim ve kontrol ile görevlendirdiği personel,
- b) Yasal görev ve yetkilerine uygun olmak ve soruşturma, inceleme ve denetim konusu ile sınırlı olmak şartıyla kamu kurum ve kuruluşlarının denetim birimleri tarafından yapılacak soruşturma, inceleme ve denetimlerle ilgili görevlendirilen personel,
- c) Bakanlığın politikalarıyla ilgili olarak iş ve işlemleri yürüten veya bununla ilgili çalışma yapan Bakanlık personeli,
- ç) Görülmekte olan bir dava veya yürütülen bir soruşturmaya istinaden savcılıklar, mahkemeler ve Sayıştay Başkanlığı.

(2) Bu maddenin birinci fıkrasının (b) bendinde belirtilen kişilerin görevli oldukları kamu kurum ve kuruluşları ile Bakanlık arasında, bu Yönetmeliğin 12 nci maddesinin birinci fıkrasında düzenlenen sürekli veri paylaşımı yöntemi ile veri paylaşımı yapılıyorsa, söz konusu kişiler için bu madde kapsamında istisnai durum hükümleri uygulanmaz.

(3) Bakanlık tarafından, sosyal yardım politikalarının geliştirilmesi amacıyla yapılan ve yaptırılan araştırma geliştirme çalışmalarında bu Yönetmelik kapsamındaki veriler ve oluşturulan istatistikler kullanılabilir.

(4) Diğer Bakanlıklar tarafından, sosyal politikaların geliştirilmesi amacıyla yapılan çalışmalarda bu Yönetmelik kapsamındaki verilerden oluşturulan istatistikler kullanılabilir.

Tek seferlik veri taleplerinin yönetimi

MADDE 15 - (1) Veriler istenmeden önce, bu veri taleplerinin amaçlarının belli olması, talep yazısında açık ve net bir şekilde belirtilmesi, sonraki kullanımların da bu amaçlarla sınırlı tutulacağı ve varsa yasal dayanağının belirtilmesi zorunludur.

(2) Veri taleplerinde izlenecek yöntem;

- a) İlgili her tür talep resmi yazı ile yapılır.
- b) Verinin doğru üretilebilmesi için veriler talep edilmeden önce ilgili birim ile ön görüşme yapılır. Gerekli fizibilite çalışması yapılmaksızın iletilen taleplerdeki geri dönüşlerde ve aynı talebe dair değişikliklerde ikinci bir resmi yazı olmadan cevap verilmez.
- c) Bakanlık tarafından kamuoyu ile paylaşılan istatistikler ayrıca talep edilemez.

ç) Ayrı veya özel bir çalışma, araştırma, inceleme ya da analiz neticesinde oluşturulabilecek türden veriler için yapılacak başvurulara olumsuz cevap verilebilir.

DÖRDÜNCÜ BÖLÜM

Verilerin Güvenliği ve İletilmesi

Verilerin güvenliği

MADDE 16 - (1) Bakanlık, veri tabanında tutulan verilerin güvenliğinin sağlanması amacıyla, Bakanlıkta uygulanan bilgi güvenliği standartları ve bilgi güvenliği politikalarının hazırlanmasını, uygulamaya konulmasını, güncellenmesini ve denetlenmesini sağlamakla yükümlüdür. Bu kapsamda;

a) Kaynak veri tabanına, veri ambarına erişimler gerçek kişi (ad, soyad) kullanıcı adı ve şifreleri kullanılarak güvenlik politikaları çerçevesinde yapılacaktır.

b) Bakanlık kaynak sistemlerinde sadece test edilmiş ve onaylanmış Bakanlık uygulamaları aracılığı ile toplanan veriler esastır. Hata sonucu veya farklı nedenlerle verilerde değiştirme, silme, ekleme ihtiyacı oluşursa, bu işlemler Bakanlık tarafından yetkilendirilmiş kişiler ile tutanak altına alınarak yapılacaktır.

c) Bakanlık yedekleme politikaları çerçevesinde mutata bir şekilde kaynak verilerinin yedekleme işlemi Bilgi İşlem Daire Başkanlığı sistem personeli tarafından yapılacaktır.

ç) Bakanlık tarafından veriye erişim yetkisi verilmiş personelin ayrılması veya görev yerinin değişmesi durumunda personelin veri tabanına erişim yetkisi iptal edilir. Personelin üzerinde çalıştığı veri ile ilgili sorumluluğu kurumdan ayrıldıktan sonra da devam eder.

d) Bakanlık tarafından yetki verilen kamu kurum ve kuruluşları ile mahalli idareler ve Türkiye Kızılay Derneği personelinin kurumlarından ayrılması veya görev yeri değişikliği durumunda ilgili kurum tarafından Bakanlığa aynı işgünü içerisinde bilgi verilir, yetki değişimi veya iptali sağlanır.

Verilerin iletilmesi

MADDE 17 - (1) Elektronik Belge Yönetim Sistemi (EBYS) ortamında veri iletme: Bakanlık içi veri talepleri karşılanırken hazırlanan veriler EBYS üzerinden ilgili birimlere iletilir.

(2) Elektronik posta ile veri iletme: Veriler elektronik ortamda iletilirken sadece 'gov.tr' uzantılı e-posta adreslerine gönderilir ve veri ulaştıktan sonra bilgi verilmesi istenir.

(3) Posta ile veri iletme: Posta ile iletilecek veriler şifrelenerek CD, DVD ve benzeri ile kapalı bir zarf içerisinde taahhütlü ya da iadeli taahhütlü gönderilir.

(4) Telefonla veri iletme: Telefonla hiçbir veri iletmez.

(5) Protokol/sözleşme imzalanan alıcı ile veri paylaşımının gerçekleştirilmesinde kurumsal elektronik alt yapı vasıtasıyla web servis, VPN, XML ve benzeri uygulamalar kullanılabilir.

(6) Elden teslim alma yoluyla veri iletme: Veriler şifrelenerek CD, DVD vb. ile kapalı bir zarf içerisinde ve tutanak karşılığı alıcıya teslim edilir.

(7) Kurul tarafından kabul edilen tek seferlik veri taleplerine ilişkin veri paylaşımı: Kurul tarafından belirlenecek veri iletme yöntemi kullanılarak, kurulun karar tarihinden itibaren iki ay içinde teslim edilir. Talep edilen verinin kapsamı nedeniyle işlemlerin iki aydan uzun sürmesi durumunda bu süre Kurul tarafından talebin kabul tarihinden itibaren altı aya kadar uzatılabilir.

BEŞİNCİ BÖLÜM

Veri Paylaşımı Kurulunun Oluşumu ve Görevleri

Kurulun oluşumu

MADDE 18 - (1) (Değişik:RG-6/7/2019-30823) Kurul; Genel Müdürlükten sorumlu Bakan Yardımcısı başkanlığında, Genel Müdür ve Genel Müdürlük Araştırma Geliştirme ve Tanıtım Dairesinin bağlı olduğu genel müdür yardımcısı, Genel Müdürlük Araştırma Geliştirme ve Tanıtım Daire Başkanı, bir hukuk müşaviri, bir başdenetçi veya denetçi ve Genel Müdür tarafından görevlendirilecek bir üyeden oluşur.

(2) Kurul, üç ayda bir, asgarî dört üye ile toplanır. Kararlar toplantıya katılan üyelerin çoğunluğu ile alınır. Oylarda eşitlik olması halinde, Kurul Başkanının bulunduğu taraf çoğunluk sayılır. Gerekli görülen hallerde başkanın talebi üzerine Kurul olağanüstü toplantıya çağrılabilir.

(3) Kurulun sekretarya işlemleri Genel Müdürlük Araştırma Geliştirme ve Tanıtım Daire Başkanlığınca yürütülür.

Kurulun görevleri

MADDE 19 - (1) Kurulun görevleri şunlardır:

- a) Sürekli veri paylaşım taleplerini karara bağlamak.
- b) Tek seferlik veri taleplerini karara bağlamak.
- c) Veri paylaşımının hangi yolla yapılacağına karar vermek.

ç) Paylaşılan verilerin kullanım sürelerini belirlemek.

ALTINCI BÖLÜM

Son Hükümler

Yürürlük

MADDE 20 - (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 21 - (Değişik:RG-6/7/2019-30823)

(1) Bu Yönetmelik hükümlerini Aile, Çalışma ve Sosyal Hizmetler Bakanı yürütür.

Mesafeli Sözleşmeler Yönetmeliği

Resmî Gazete Tarihi : 27.11.2014

Resmî Gazete Sayısı : 29188

MESAFELİ SÖZLEŞMELER YÖNETMELİĞİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı, mesafeli sözleşmelere ilişkin uygulama usul ve esaslarını düzenlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, mesafeli sözleşmelere uygulanır.

(2) Bu Yönetmelik hükümleri;

- a) Finansal hizmetler,
- b) Otomatik makineler aracılığıyla yapılan satışlar,
- c) Halka açık telefon vasıtasıyla telekomünikasyon operatörleriyle bu telefonun kullanımı,
- ç) Bahis, çekiliş, piyango ve benzeri şans oyunlarına ilişkin hizmetler,
- d) Taşınmaz malların veya bu mallara ilişkin hakların oluşumu, devri veya kazanımı,
- e) Konut kiralama,
- f) Paket turlar,
- g) Devre mülk, devre tatil, uzun süreli tatil hizmeti ve bunların yeniden satımı veya değişimi,
- ğ) Yiyecek ve içecekler gibi günlük tüketim maddelerinin, satıcının düzenli teslimatları çerçevesinde tüketicinin meskenine veya işyerine götürülmesi,
- h) 5 inci maddenin birinci fıkrasının (a), (b) ve (d) bentlerindeki bilgi verme yükümlülüğü ile 18 inci ve 19 uncu maddelerde yer alan yükümlülükler saklı kalmak koşuluyla yolcu taşıma hizmetleri,
- ı) Malların montaj, bakım ve onarımı,

i) Bakımevi hizmetleri, çocuk, yaşlı ya da hasta bakımı gibi ailelerin ve kişilerin desteklenmesine yönelik sosyal hizmetler

ile ilgili sözleşmelere uygulanmaz.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 7/11/2013 tarihli ve 6502 sayılı Tüketicinin Korunması Hakkında Kanununun 48 inci ve 84 üncü maddelerine dayanılarak hazırlanmıştır.

(...)

Bilgilerin saklanması ve ispat yükümlülüğü

MADDE 20 - (1) Satıcı veya sağlayıcı, bu Yönetmelik kapsamında düzenlenen cayma hakkı, bilgilendirme, teslimat ve diğer hususlardaki yükümlülüklerine dair her bir işleme ilişkin bilgi ve belgeyi üç yıl boyunca saklamak zorundadır.

(2) Oluşturdukları sistem çerçevesinde, uzaktan iletişim araçlarını kullanmak veya kullandırmak suretiyle satıcı veya sağlayıcı adına mesafeli sözleşme kurulmasına aracılık edenler, bu Yönetmelikte yer alan hususlardan dolayı satıcı veya sağlayıcı ile yapılan işlemlere ilişkin kayıtları üç yıl boyunca tutmak ve istenilmesi halinde bu bilgileri ilgili kurum, kuruluş ve tüketicilere vermekle yükümlüdür. (Ek cümle:RG-9/2/2019-30681) Ancak abonelik sözleşmesinin kamu hizmetlerinin tek noktadan sunulduğu ortak kamu elektronik platformu üzerinden kurulması halinde, kayıtların tutulması ve bilgilerin sunulmasına ilişkin yükümlülük satıcı veya sağlayıcıya aittir.

(3) Satıcı veya sağlayıcı elektronik ortamda tüketiciye teslim edilen gayrimaddi malların veya ifa edilen hizmetlerin ayıpsız olduğunu ispatla yükümlüdür.

(...)

Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik

Resmî Gazete Tarihi : 15.07.2015

Resmî Gazete Sayısı : 29417

TİCARİ İLETİŞİM VE TİCARİ ELEKTRONİK İLETİLER HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı, elektronik iletişim araçlarıyla yapılan ticari iletişime dair bilgi verme yükümlülüklerine ve ticari elektronik iletilerde uyulması gereken hususlara ilişkin usul ve esasları düzenlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, gerçek ve tüzel kişilerin mal ve hizmetlerini tanıtmak, pazarlamak ya da işletmesini tanıtmak veya bunları başkaları adına yapmak amacıyla elektronik iletişim araçlarıyla yapılan her türlü ticari iletişimi kapsar.

(2) Bu Yönetmelik hükümleri;

a) 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu kapsamındaki işletmecilerin abone ve kullanıcılarına; münhasıran kendi mal ve hizmetlerini tanıtmak, pazarlamak ya da işletmesini tanıtmak amacıyla gönderdiği ticari elektronik iletilere,

b) Vakıf üniversitelerinin (Değişik ibare:RG-4/1/2020-30998) ve diğer özel eğitim ve öğretim kurumlarının öğrencilerine ve bunların velilerine gönderdiği iletilere,

c) Kamu kurumu niteliğindeki meslek kuruluşları ile kamuya yararlı dernekler ve vergi muafiyeti sağlanan vakıfların, kendilerine ait ticari işletmelerin faaliyetleriyle ilgili olarak üyelerine gönderdiği iletilere,

ç) 15/2/2011 tarihli ve 6112 sayılı Radyo ve Televizyonların Kuruluş ve Yayın Hizmetleri Hakkında Kanun hükümlerine göre radyo ve televizyon yayıncılığı yapan kuruluşlarca, kamuoyunu bilgilendirmek ve eğitmek amacıyla yapılan yayın hizmetlerine ilişkin bilgilendirme iletilerine,

d) Devlet, mahalli idareler ve diğerk kamu tüzeli kişilerinin kamuoyunu bilgilendirmek amacıyla gönderdikleri iletilere,
uygulanmaz.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 23/10/2014 tarihli ve 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanuna dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (Değişik:RG-4/1/2020-30998)

(1) Bu Yönetmelikte geçen;

- a) Alıcı: Tüketiciyi ya da meslekî veya diğerk amaçlarla hareket eden gerçek veya tüzeli kişiyi,
- b) Aracı hizmet sağlayıcı: Başkalarına ait iktisadî ve ticari faaliyetlerin yapılmasına elektronik ticaret ortamını sağlayan gerçek ve tüzeli kişileri,
- c) Bakanlık: Ticaret Bakanlığını,
- ç) Bayi işletme: Sözleşmeye dayalı olarak bir işletmenin mal ve hizmetlerinin satışına aracılık eden ve kendi adına bağımsız çalışan işletmeyi,
- d) Elektronik iletişim adresi: Elektronik posta ve telefon numarası gibi elektronik ortamda münhasıran iletişim kurmayı sağlayan adresi,
- e) Elektronik iletişim araçları: İnternet ve diğerk iletişim ağları üzerinden iletilerin gönderilmesine, alınmasına veya saklanmasına imkân sağlayan bilgisayar, telefon, faks, otomatik arama makineleri gibi her türlü cihazı,
- f) Elektronik ortam: Verilerin sayısallaştırılarak işlenmesi, saklanması ve iletilmesinin sağlandığı ortamı,
- g) Elektronik ticaret: Fizikî olarak karşı karşıya gelmeksizin, elektronik ortamda gerçekleştirilen çevrim içi iktisadi ve ticari her türlü faaliyeti,
- ğ) Hizmet sağlayıcı: Elektronik ticaret faaliyetinde bulunan gerçek ya da tüzeli kişileri,
- h) İl müdürlüğü: Ticaret il müdürlüğünü,
- ı) İl müdürü: Ticaret il müdürünü,
- i) İş günü: Ulusal bayram ile genel ve hafta sonu tatil günleri hariç diğerk günleri,

- j) İYS Numarası: İYS'ye kayıt olan tüm hizmet sağlayıcı ve markalarına ayrı ayrı atanan tekil numarayı,
- k) Kanun: 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunu,
- l) Kuruluş: Bakanlıkça ticari elektronik ileti yönetim sistemini kurmakla yetkilendirilen kuruluşu,
- m) MERSİS: Merkezi Sicil Kayıt Sistemini,
- n) Özel yetkili işletme: Sözleşmeye dayalı olarak bir işletmenin, yönetim ve organizasyon ile dağıtım veya pazarlama teknolojileri gibi konularda bilgi ve desteğini almak suretiyle bu işletmenin mal veya hizmetinin satışı üzerindeki imtiyaz hakkını bedel, bölge ve süre gibi belirli şartlar ve sınırlamalar dâhilinde kullanan bağımsız ticari işletmeyi,
- o) Ticari elektronik ileti: Telefon, çağrı merkezleri, faks, otomatik arama makineleri, akıllı ses kaydedici sistemler, elektronik posta, kısa mesaj hizmeti gibi vasıtalar kullanılarak elektronik ortamda gerçekleştirilen ve ticari amaçlarla gönderilen veri, ses ve görüntü içerikli iletileri,
- ö) Ticari elektronik ileti yönetim sistemi (İYS): Ticari elektronik ileti onayı alınmasına, reddetme hakkının kullanılmasına ve şikâyet süreçlerinin yönetilmesine imkân tanıyan sistemi,
- p) Ticari iletişim: Alan adları ve elektronik posta adresi dışında, meslekî veya ticari faaliyet kapsamında kazanç sağlamaya yönelik olarak elektronik ticarete ilişkin her türlü iletişimi,
- r) URL adresi: İlgili içeriğin internet gibi bir ağ üzerinde bulunduğu tam adresi,
- ifade eder.

(...)

Kişisel verilerin korunması

MADDE 12 - (1) Hizmet sağlayıcı ve aracı hizmet sağlayıcı (Ek ibare:RG-4/1/2020-30998) ile Kuruluş, bu Yönetmelik çerçevesinde yapmış olduğu işlemler ve sunduğu hizmetler nedeniyle elde ettiği verilerin, ilgili mevzuat hükümleri saklı kalmak kaydıyla muhafazasından ve hukuka aykırı olarak bunlara erişilmesini ve işlenmesini önlemek amacıyla gerekli tedbirlerin alınmasından sorumludur.

(...)

Elektronik Ticarete Hizmet Sağlayıcı ve Aracı Hizmet Sağlayıcılar Hakkında Yönetmelik

Resmî Gazete Tarihi : 26.08.2015

Resmî Gazete Sayısı : 29457

ELEKTRONİK TİCARETTE HİZMET SAĞLAYICI VE ARACI HİZMET SAĞLAYICILAR HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı, hizmet sağlayıcı ve aracı hizmet sağlayıcıların elektronik ticaret işlemlerinin yapıldığı ağ üzerinde bulundurmalarıyla yükümlü oldukları genel bilgiler ile sözleşme öncesinde ve sipariş sürecinde alıcılara sunmaları gereken bilgilere ve elektronik ticaret ile ilgili diğer uygulamalara ilişkin usul ve esasları düzenlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, hizmet sağlayıcı ve aracı hizmet sağlayıcıların ağ üzerinde mal veya hizmet satışına ilişkin sözleşme ve siparişlerdeki bilgi verme yükümlülükleri ile elektronik ticaretle ilgili diğer tedbirleri kapsar.

(2) Bu Yönetmelik hükümleri, münhasıran elektronik posta, telefon araması, kısa mesaj veya elektronik ortamda doğrudan iletişime imkân veren benzeri bireysel iletişim araçlarıyla yapılan sözleşmelere uygulanmaz.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 23/10/2014 tarihli ve 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanuna dayanılarak hazırlanmıştır.

(...)

İşlem rehberi

MADDE 7 - (1) Aracı hizmet sağlayıcı ve kendine ait elektronik ortamda satış yapan hizmet sağlayıcı tarafından, elektronik ticaret işlemlerinin gerçekleştirildiği ağ üzerinden doğrudan ulaşılabilecek şekilde ana sayfada “işlem rehberi” başlığı altında aşağıdaki bilgiler güncel olarak bulundurulur:

a) Sözleşmenin kurulabilmesi için mal ve hizmetin seçilmesi, teslimat ve ödeme bilgilerinin girilmesi ile siparişin onaylanması gibi gerekli aşamaları gösterir şekilde teknik adımlar.

b) Elektronik ticarete ilişkin sözleşmenin, elektronik ortamda saklanıp saklanmayacağı ile bu sözleşmeye alıcının daha sonra aynı ortamda erişiminin mümkün olup olmayacağı ve bu erişimin ne kadar süreyle sağlanacağına ilişkin bilgi.

c) Alıcının siparişi vermeden önce veri girişindeki hatalarını açık ve anlaşılır bir şekilde belirleyebilmesi ve düzeltebilmesi amacıyla özet sipariş formu ile geri al ve değiştir gibi teknik araçların sunulacağına ilişkin bilgi.

ç) Elektronik ticaret işlemleri nedeniyle elde ettiği kişisel verilere ilişkin gizlilik kuralları.

d) Alıcıyla arasında uyuşmazlık çıkması halinde varsa alternatif uyuşmazlık çözüm mekanizmaları.

(2) Alternatif uyuşmazlık çözüm mekanizmaları, tarafların diğer hukuki çözüm yollarına başvurma hakkına engel teşkil etmez.

(...)

Kişisel verilerin korunması

MADDE 10 - (1) Hizmet sağlayıcı ve aracı hizmet sağlayıcı, bu Yönetmelik çerçevesinde yaptığı işlemler ve sunduğu hizmetler nedeniyle elde ettiği kişisel verilerin, 23/2/2006 tarihli ve 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu ve diğer ilgili mevzuat hükümleri saklı kalmak kaydıyla muhafazasından ve hukuka aykırı olarak bunlara erişilmesini ve işlenmesini önlemek amacıyla gerekli tedbirlerin alınmasından sorumludur.

(2) Kişisel veriler, ilgili kişinin açık irade beyanını içerecek şekilde önceden alınan onayı olmaksızın üçüncü kişilerle paylaşılamaz, işlenemez ve başka amaçlarla kullanılamaz.

İspat yükümlülüğü ve elektronik kayıtların saklanma süresi

MADDE 11 - (1) Şikâyet konusu işlemlerde ispat yükümlülüğü, hizmet sağlayıcı ve/veya aracı hizmet sağlayıcıya aittir.

(2) Hizmet sağlayıcı ve/veya aracı hizmet sağlayıcı, elektronik ticaret işlemlerine ilişkin elektronik kayıtları işlem tarihinden itibaren üç yıl süreyle saklar ve talep halinde bu kayıtları Bakanlığa sunar.

(3) (Ek:RG-15/2/2019-30687) Abonelik sözleşmesinin kamu hizmetlerinin tek noktadan sunulduğu ortak kamu elektronik platformu üzerinden kurulması halinde ispat yükümlülüğü ve elektronik ticaret işlemlerine ilişkin elektronik kayıtların saklanması ve talep olması halinde bu kayıtların Bakanlığa sunulmasında yükümlülük hizmet sağlayıcıya aittir.

(...)

Özel İstihdam Büroları Yönetmeliği

Resmî Gazete Tarihi : 11.10.2016

Resmî Gazete Sayısı : 29854

ÖZEL İSTİHDAM BÜROLARI YÖNETMELİĞİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç ve kapsam

MADDE 1 - (1) Bu Yönetmeliğin amacı; özel istihdam bürolarının kurulması ve faaliyetleri ile incelenmesine, kontrolüne, denetim ve teftişine ilişkin usul ve esasların belirlenmesidir.

Dayanak

MADDE 2 - (1) Bu Yönetmelik, 22/5/2003 tarihli ve 4857 sayılı İş Kanununun 7 nci maddesi, 25/6/2003 tarihli ve 4904 sayılı Türkiye İş Kurumu Kanununun 17 nci 18 inci ve 19 uncu maddeleri ile 32 nci maddesinin birinci fıkrasının (i) bendine dayanılarak hazırlanmıştır.

(...)

YEDİNCİ BÖLÜM

Özel İstihdam Bürolarının Bilgi Toplaması, Veri Kaydı ve Gizlilik

Bilgi toplama ve kullanma

MADDE 24 - (1) Özel istihdam büroları, iş arayanlara ve işverenlere ilişkin bilgileri sadece iş ve işçi bulma faaliyeti için toplayabilir, işleme tabi tutabilir veya bunlardan yararlanabilir.

(2) 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ve 4904 sayılı Kanunun 19 uncu maddesi hükümleri çerçevesinde; özel istihdam bürosu, iş ve işçi bulmaya aracılık için derlediği verileri bu amaçlar dışında kullanamaz.

Kuruma bilgi, belge verme ve saklama zorunluluğu

MADDE 25 - (1) Özel istihdam büroları; faaliyet süresi içinde unvan, faaliyet alanı, yetkili kişi, nitelikli personel, işyeri adresi, posta adresi, internet sayfası ve elektronik posta adresi değişikliklerini on gün içinde izin başvurusunu yaptıkları il müdürlüklerine veya hizmet merkezlerine bildirmek,

uygulamanın takibi için gerekli olan diğer bilgi ve belgeleri de talep edilmesi halinde Kuruma ibraz etmek zorundadır.

(2) Özel istihdam büroları, yıl içerisinde yaptıkları iş ve işçi bulmaya ilişkin aracılık faaliyeti, işgücü piyasası ile istihdam ve insan kaynaklarına yönelik hizmetleri, düzenledikleri mesleki eğitim ve yetki verilmesi hâlinde kurdukları geçici iş ilişkisi ile ilgili bilgilerini kayıt altına alır ve bu bilgileri Kurum internet sayfası üzerinden sisteme kaydeder. Bu verileri içeren üçer aylık dönemlere ait raporlarını ise yine Kurum internet sayfası üzerinden Ocak, Nisan, Temmuz ve Ekim aylarının yirminci günü sonuna kadar Kuruma gönderir.

(3) Üçer aylık dönemsel raporların Kurumca incelenmesi ve değerlendirilmesi sonucunda eksikliklerin tespit edilmesi hâlinde, raporun bir sureti eksikliklerin tamamlanması için özel istihdam bürosuna gönderilir. Belirtilen süre içerisinde eksikliklerin giderilmemesi hâlinde raporun bir sureti gereği yapılmak üzere ilgili mercilere gönderilir.

(4) Özel istihdam büroları, düzenleme tarihini izleyen takvim yılı başından itibaren;

a) 22 nci maddenin ikinci fıkrasında belirtilen ücret alınabilecek mesleklerle ilgili yazılı sözleşmeleri,

b) İş arayanlara ait kimlik, eğitim ve meslek bilgilerini,

c) Geçici iş ilişkisi kapsamında; geçici iş sözleşmesi imzaladıkları işçilere ait kimlik, eğitim, meslek bilgileri ile geçici işçi çalıştıran işverene ait bilgileri,

ç) Geçici işçi sağlama sözleşmesi ile geçici iş sözleşmelerini,

d) İşe yerleştirilen kişilere ait kimlik, eğitim ve meslek bilgilerini,

e) İşverenlerden alınan açık işlere ait eğitim, meslek ve iletişim bilgilerini,

f) Kurumca onaylanan yurt dışı iş sözleşmelerini,

g) Yetkili kişi dışında imza atabilecek kişilerle ilgili olarak düzenlenen belgeleri,

beş yıl süreyle saklamak ve Kurumun talebi halinde ibraz etmek zorundadır.

Gizlilik

MADDE 26 - (1) Özel istihdam bürolarından alınan bilgilerin Kurumca kullanımında, bu bilgilerin hizmete özel olduğu hususu dikkate alınır ve bu bilgiler Kurum hizmetlerinden başka amaçla kullanılamaz.

(...)

Ticaret Sicili Yönetmeliđi

Resmî Gazete Tarihi : 27.01.2013

Resmî Gazete Sayısı : 28541

TİCARET SİCİLİ YÖNETMELİĐİ

BİRİNCİ KISIM

Genel Hükümler

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1- (1) Bu Yönetmeliđin amacı, ticaret sicili kayıtlarının tam ve sağlıklı tutulmasını ve emredici hukuk kuralları çerçevesinde kayıtların aleniyetinin ve üçüncü kişiler dahil tarafların hukuki güvenliğinin teminat altına alınmasını sağlamaktır.

Kapsam

MADDE 2- (1) Bu Yönetmelik; ticaret sicili müdürlüklerinin kurulmasına ve işleyişine, sicil defterlerinin tutulmasına, ticaret sicili kayıtlarının elektronik ortamda tutulmasına, tescil zorunluluğunun yerine getirilmesine, ticaret sicili müdürlüklerinin kararlarına karşı itiraz yollarına, ticaret sicili müdür ve müdür yardımcıları ile diđer personelde aranacak niteliklere ve disiplin işlerine ilişkin usul ve esaslar ile ticaret siciline ilişkin diđer hususları kapsar.

Dayanak

MADDE 3- (1) Bu Yönetmelik 13/1/2011 tarihli ve 6102 sayılı Türk Ticaret Kanununun 26 ncı maddesine dayanılarak hazırlanmıştır.

(...)

Sicil kayıtlarına erişim hakkı

MADDE 15- (1) Herkes, sicilin içeriğini ve müdürlükte saklanan tüm senet ve belgeleri inceleyebilir. Bu inceleme elektronik ortamda ve/veya müdürlükte yapılabilir.

(2) Defterler ve belgeler, sicil dairesinin bulunduđu kısımdan dıřarıya ıkarılamaz. Bunların incelenmesinde mdr, kiřisel verilerin korunmasına iliřkin hkmler erevesinde gerekli tedbirleri almak zorundadır. İnceleme esnasında mdrn vereceđi talimatlara uyulması zorunludur. Aksi takdirde mdr defter ve belgeleri derhal kaldırabilir.

(3) Elektronik ortamda yapılacak olan incelemelerde de kiřisel verilerin korunmasını ve bilgi gvenliđini sađlayacak tedbirler alınır.

(...)

Veri Depolama Kuruluşunun Faaliyet, Çalışma ve Denetim Esasları Hakkında Yönetmelik

Resmî Gazete Tarihi : 19.09.2018

Resmî Gazete Sayısı : 30540

VERİ DEPOLAMA KURULUŞUNUN FAALİYET, ÇALIŞMA VE DENETİM ESASLARI HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak, Tanımlar ve Kısaltmalar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı, 6/12/2012 tarihli ve 6362 sayılı Sermaye Piyasası Kanununun 87 nci maddesi çerçevesinde yetkilendirilen veri depolama kuruluşunun yükümlülüklerine, veri depolama kuruluşuna raporlanacak bilgilerin hangi şekil ve ortamda tutulacağı ile bu kuruluşun Kanun uyarınca yerine getireceği görevlerine yönelik faaliyet usul ve esaslarını belirlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, 6362 sayılı Kanunun 87 nci maddesi çerçevesinde veri depolama kuruluşunun yükümlülüklerini, faaliyet, üyelik, çalışma ve denetim esaslarını kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 6/12/2012 tarihli ve 6362 sayılı Sermaye Piyasası Kanununun 87 nci maddesine dayanılarak hazırlanmıştır.

Tanımlar ve kısaltmalar

MADDE 4 - (1) Bu Yönetmelikte geçen;

- a) Kanun: 6362 sayılı Sermaye Piyasası Kanununu,
- b) Kurul: Sermaye Piyasası Kurulunu,
- c) Merkezi karşı taraf/MKT: Sermaye piyasalarında işlem gören sözleşmelerde alıcıya karşı satıcı, satıcıya karşı da alıcı rolünü üstlenen kuruluşu,
- ç) Veri depolama faaliyeti: Kanunda ve bu Yönetmelikte öngörülen şekilde verileri toplama ve merkezi olarak tutma faaliyetini,

- d) Veri depolama kuruluđu/VDK: Kanununun 87 nci maddesi uyarınca Kurulca yetkilendirilen ve veri depolama faaliyetini yrten kuruluđu,
- e) Yan hizmetler: Veri depolama faaliyeti ile bađlantılı olan iřlem onayı, iřlem eřleřtirme, kredi sicil servisi, portfy teyidi, portfy sıkıřtırma ve diđer hizmetleri,
- f) Yatırım kuruluđu: Aracı kurumlar ile yatırım hizmeti ve faaliyetinde bulunmak zere kuruluđu ve faaliyet esasları Kurulca belirlenen diđer sermaye piyasası kurumlarını ve bankaları,
- g) Ynetici: Sermaye Piyasası Kurulu tarafından VDK olarak yetkilendirilmiř kuruluđuun ynetim kurulu başkan ve yeleri, genel mdr ve yardımcıları ile birim mdrlerini,
- ifade eder.

İKİNCİ BLM

Faaliyet Őartları

Veri Depolama Kuruluđuunun kuruluđu ve faaliyet Őartları

MADDE 5 - (1)Veri Depolama Kuruluđularına kuruluđu izni verilebilmesi iin VDK'ların;

- a) Anonim Őirket Őeklinde kurulmaları,
- b) Paylarının tamamının nama yazılı olması,
- c) Paylarının nakit karřılıđı ıkarılması,
- ) Sermayelerinin Kurulca belirlenen miktardan az olmaması ve tamamının denmiř olması,
- d) Kurucularının ve tzel kiři kurucular zerinde dođrudan veya dolaylı olarak nemli etkiye sahip olan ortaklarının Kanununun 44 nc maddesinde yer alan Őartları tařımaları,
- e) Esas szleřmelerinin Kanun ve ilgili dzenlemelerde yer alan hkmlere uygun olması,
- f) Ortaklık yapısının aık ve Őeffaf olması,
- řarttır.

(2) Kamu tzel kiřileri hari tzel kiři kurucuların ve tzel kiři kurucular zerinde dođrudan veya dolaylı olarak nemli etkiye sahip tzel kiři ortaklarının son 3 yıla ait bađımsız denetimden gemiř finansal tablolarını sunmaları gereklidir. Yabancı kurucu ve ortaklar iin uygun olduđu lde, Trk uyruklu gerek ve tzel kiřiler iin aranan Őartların mevcut olduđunu tevsik edici ve buldukları lkenin yetkili makamlarınca onanmiř bilgi ve belgelerin noterce tasdikli evirilerinin veya geerliliđi kanun veya uluslararası szleřmelerle kabul edilen Őekilde hazırlanarak sunulması zorunludur.

(3) Kurul tarafından yetkilendirilen VDK'nın bu faaliyette bulunabilmesi için;

- a) Esas sözleşmesinin Kanun ve bu Yönetmelikte yer alan hükümlere uygun hale getirilmiş olması,
 - b) Kuruluşun varsa diğer faaliyetlerinden bağımsız, münhasıran veri depolama ve raporlama faaliyetini yürütecek şekilde organizasyon yapısının kurulmuş, sorumluluklarının açıkça belirlenmiş, iç kontrol, iç denetim ve gözetim ile risk yönetimi sistemlerinin oluşturularak işlerliğinin sağlanmış olması,
 - c) VDK hizmetlerinin etkin, güvenilir ve kesintisiz bir şekilde yerine getirilmesi amacıyla gerekli bilgi işlem sistemlerinin ve teknolojik altyapının kurulmuş olması, bilgilerin tutarlılığının, güvenilirliğinin, bütünlüğünün ve zamanında elde edilebilirliğinin sağlanması amacıyla gerekli sistemsel ve yönetsel önlemlerin alınmış ve prosedürlerin oluşturulmuş olması,
- şarttır.

(4) Kurul, bu maddede belirtilen şartların yanında ilave şartlar öngörebilir.

(5) VDK, bu Yönetmelikle belirlenen faaliyet şartlarından herhangi birini kaybetmesi halinde, durumun ortaya çıktığı gün itibarıyla Kurula bildirimde bulunur.

(6) VDK'nın sunacağı veri depolama faaliyeti ile bağlantılı olan yan hizmetlere Kurulca izin verilebilmesi için yan hizmetlerin veri depolama faaliyetinden operasyonel olarak ayrılmış olması şarttır.

(7) VDK'nın yurt dışında yetkilendirilerek veri depolama faaliyetinde bulunması için Kuruldan izin alması zorunludur.

(8) Kurulca verilen faaliyet izninin iptalinde Kanununun 41 inci maddesi hükmü uygulanır.

(9) Kurulca Kanun uyarınca merkezi saklama kuruluşu ya da merkezi takas kuruluşu olarak yetkilendirilmiş bir kuruluş bu maddede öngörülen koşulların tevsiki gerekmeksizin VDK olarak yetkilendirilebilir. Bu halde, yetkilendirilmiş kuruluşun 13/1/2011 tarihli ve 6102 sayılı Türk Ticaret Kanunu uyarınca oluşturulmuş organları dışında VDK için ayrıca organ oluşturulmaz; ilgili kuruluşun organları VDK'nın organları yerine geçer. Yetkilendirilmiş kuruluşlarca VDK faaliyetlerinin diğer faaliyetlerden operasyonel olarak ayrılmış olması gerekir. Yetkilendirilmiş kuruluşlarca Kurulun düzenlemeleri uyarınca bilgi sistemlerine ve mali konulara ilişkin olarak yapılan denetimler 21 inci maddenin ikinci ve üçüncü fıkralarında sayılan denetimler kapsamında değerlendirilir.

(10) VDK'ların esas sözleşme değişikliklerinde Kurulun uygun görüşü alınır.

(11) Doğrudan veya dolaylı olarak; yüzde beşi aşan pay devirleri veya ortaklık yapısında yüzde beş ve üzeri değişiklik yaratan pay devirleri ile pay devri söz konusu olmasa dahi doğrudan veya dolaylı kontrol devri sonucunu doğuran her türlü işlem Kurulun iznine tâbidir. İmtiyazlı payların devri her halükarda Kurul iznine tabidir. Pay devirlerinde, payları devralacak gerçek ve tüzel kişiler ile tüzel kişilerin önemli etkiye sahip ortaklarının da 7 nci maddede sayılan şartları taşımaları zorunludur. Kurulun uygun görüş vermediği esas sözleşme değişiklikleri ile izin vermediği pay devirleri veya kontrol devri sonucunu doğuran işlemler hükümsüzdür. Bu hükme aykırı pay devirleri ortaklık pay defterine kaydolmaz ve bu şekilde yapılan kayıtlar hüküm ifade etmez. Yüzde beşi aşmayan pay devirleri, devrin gerçekleşmesinden itibaren en geç 15 iş günü içerisinde Kurula bildirilir.

ÜÇÜNCÜ BÖLÜM

Görev, Yetki ile Faaliyet İlke ve Esasları

VDK'nın görev ve yetkileri

MADDE 6 - (1) VDK'nın görev ve yetkileri şunlardır:

- a) Kanununun 87 nci maddesi çerçevesinde, Kurulca belirlenen işlemlere ilişkin kendisine raporlanan verileri Türkiye sınırları içerisinde olmak üzere elektronik ortamda kaydetmek ve saklamak,
- b) Üyelerce yapılan raporlamaların üyeler itibarıyla tutarlılığını izlemek, tutarsızlık ve düzenlemelere aykırılığın tespiti halinde üyeler nezdinde gerekli düzeltmelerin yapılmasını istemek ve mutabakat sağlanamadığı durumlarda Kurula bilgi vermek, sistemin güvenli çalışmasını sağlayacak önlemler almak ve uygulamak,
- c) Yönetmelikteki VDK verilerinin paylaşılmasına ilişkin esaslar çerçevesinde verilerin analiz edilmesine imkân sağlayacak gerekli araçları geliştirmek,
- ç) Kayıtların mevzuatta öngörülen çerçevede gizliliğini sağlamak,
- d) Yönetmelikte belirlenen esaslar çerçevesinde verileri kamuya açıklamak,
- e) Veri taleplerini Yönetmelikte belirlenen esaslar çerçevesinde karşılamak,
- f) Kurul tarafından verilen diğer görevleri ve düzenlemelerin gerektirdiği işlemleri yapmak.

Faaliyet ilke ve esasları

MADDE 7 - (1) VDK'nın faaliyetleri sırasında aşağıda yer alan ilkelere uyması zorunludur:

- a) Üyelerin VDK nezdindeki işlemlerini güven ve istikrar içerisinde gerçekleştirmesini sağlayacak gerekli altyapı, donanım ve organizasyonel yapının tesis edilmesini teminen ilgili düzenlemeleri yapmak,
- b) Üyelerinin, VDK'nın iş ve işlemleriyle ilgili yapacağı düzenlemelere uyumu konusunda gerekli önlemleri almak,
- c) Kendisine bildirilen verileri 10 yıl süreyle saklamak,
- ç) Uluslararası düzenlemeleri ve uygulamaları takip etmek, verdiği hizmetlerin uluslararası uygulamalara uyum sağlaması için önerilerini Kurula sunmak,
- d) Kendisi, üyeleri ve Kurul arasında, talep edilen çerçevede düzenli bilgi akışını sağlamak,
- e) İşlettiği elektronik ortamın güven ve istikrar içinde yürütülmesini sağlayacak yeterli organizasyona sahip olmak,
- f) Faaliyetlerinde ve hizmetlerinin ücretlendirmesinde adil davranmak,
- g) İş ve işlemlerini Kurul ve menfaat sahipleri ile işbirliği ve koordinasyon içinde yürütmek,
- ğ) Veri depolama hizmetlerine ilişkin ücretleri, verdiği hizmetlere ilişkin düzenlemeleri ve prosedürlerini düzenli olarak internet sitesi aracılığıyla kamuya açıklamak.

Teşkilat ve personel

MADDE 8 - (1) Kanun ve bu Yönetmelikle VDK'ya verilmiş görevlerin yerine getirilmesi ve yetkilerin kullanılmasına ilişkin olarak, veri depolama biriminin organizasyonu, görev tanımları, yetki ve sorumlulukları, bu yetki ve sorumlulukların devri ile görevlilerin çalışma usul ve esasları ile bunların alacakları ücretlere ilişkin usuller VDK yönetim kurulunca belirlenir.

Sır saklama yükümlülüğü

MADDE 9 - (1) VDK yöneticileri ve tüm personeli, raporlanan verilerin gizliliğine uymak ve sırları bu Yönetmelikte belirlenen haller dışında açıklamamakla, kendilerinin veya üçüncü kişilerin yarar veya zararına kullanmamakla yükümlüdürler. Bu yükümlülük ilgililerin VDK'daki görevlerinden ayrılmalarından sonra da devam eder.

Yasaklar

MADDE 10 - (1) (Değişik:RG-15/10/2020-31275) VDK yöneticileri ve personeli ile bunların eşleri ve velayeti altındaki çocukları, VDK'ya bildirilen işlemlerin ilgili olduğu piyasalarda ikinci fıkra hükümleri hariç olmak üzere alım satım işlemi yapamazlar ve pozisyon alamazlar.

(2) (Değişik:RG-15/10/2020-31275) VDK yöneticileri ve tüm personeli; göreve başlamadan önce maliki oldukları, VDK'ya bildirilen işlemlerin ilgili olduğu piyasalarda gerçekleştirdikleri alım satım işlemleri nedeniyle sahip oldukları, TCMB, Hazine ve Maliye Bakanlığı ve 28/3/2002 tarihli ve 4749 sayılı Kamu Finansmanı ve Borç Yönetiminin Düzenlenmesi Hakkında Kanun çerçevesinde kurulan varlık kiralama şirketleri tarafından ihraç edilen araçlar ile yatırım fonu ve emeklilik fon payları dışındaki kıymetleri ve pozisyonları görev sürelerinin başlamasından itibaren otuz gün içinde satmak veya devretmek suretiyle elden çıkarmak zorundadır.

(3) Bu madde hükmüne aykırı hareket eden VDK yönetim kurulu üyelerinin tespiti halinde VDK Genel Kurulu en geç otuz gün içerisinde ilgili yönetim kurulu üyesinin görevden alınması gündemiyle Kurulca olağanüstü toplantıya çağrılır. VDK'nın diğer yönetici ve personeli ise bu madde hükmüne aykırılığın tespit edildiği tarihten itibaren görevlerinden istifa etmiş sayılır.

DÖRDÜNCÜ BÖLÜM

Üyelik Esasları

Üyeler

MADDE 11 - (1) İşlem tarafı tüzel kişiler, işlemlere aracılık eden yatırım kuruluşları, merkezi karşı taraf hizmeti veren kuruluşlar, işlemlerin taraflarına raporlama hizmeti sağlayan kuruluşlar ve Kurulca uygun görülen diğer kuruluşlar VDK'ya üye olurlar.

Üyelik türleri

MADDE 12 - (1) Genel VDK üyeleri, kendilerinin taraf oldukları veya aracılık ettikleri işlemlerin yanı sıra bu işlemlerden bağımsız olarak üçüncü taraflar adına da raporlama hizmeti sağlamaya yetkili kuruluşlardır. Merkezi karşı taraf hizmeti veren kuruluş da genel VDK üyesidir.

(2) Doğrudan VDK üyeleri, taraf oldukları işlemlere veya aracılık ettikleri işlemlere ilişkin raporlama yükümlülüklerini kendileri adına ve/veya aracılık edilen işlemin tarafı müşterileri adına yerine getiren kuruluşlardır.

(3) Üyelik türü değişikliklerine ilişkin usul ve esaslar VDK yönetim kurulunca belirlenir.

Üyelik şartları ve üyeliğe kabul

MADDE 13 - (1) Üyelerin, üyeliğe kabulü için;

a) Raporlama faaliyetlerini yerine getirebilecek ve VDK tarafından asgari nitelikleri belirlenmiş teknik donanım ve güvenlik sistemine sahip olmaları,

- b) Raporlama işlemlerinin yapılmasını ve izlenmesini yürütecek yeterli sayıda ve nitelikte personeli istihdam etmiş olmaları,
 - c) Üyeliğe giriş aidatını yatırmaları,
 - ç) Tüzel Kişi Kimlik Kodu almış olmaları,
 - d) VDK yönetim kurulu tarafından belirlenen diğer şartları taşımaları,
- şarttır.

(2) Gerekli şartların taşındığının VDK tarafından tespit edilmesi halinde başvuruda bulunan kuruluşlar yönetim kurulu kararı ile üyeliğe kabul edilir. Başvuruya ilişkin VDK tarafından alınan karar ilgiliye yazılı olarak bildirilir. Üyelik ilişkisi sözleşme ile kurulur. Üyelik sözleşmesi ile taraflar uygulama prosedürlerini de benimser.

(3) Merkezi takas hizmeti veren kuruluşlar birinci fıkrada belirtilen üyeliğe giriş aidatından muaftır.

Üyeliğin geçici durdurulması veya iptali

MADDE 14 - (1) Üyeliğin geçici durdurulması veya iptaline ilişkin usul ve esaslar VDK yönetim kurulunca belirlenir.

Üyelerin sorumluluğu ve faaliyet esasları

MADDE 15 - (1) VDK üyeleri; VDK nezdinde gerçekleştirmiş oldukları işlemlerin tümünden ve bu kapsamda çalışanlarının görevleri çerçevesinde yaptıkları işlerden sorumludur. VDK üyeleri ile müşterileri arasında yapılacak sözleşmelere konulacak hükümlerle üyelerin sorumlulukları kaldırılamaz ve sınırlandırılmaz.

(2) VDK üyeleri ilgili mevzuatta yer alan ilke ve kurallar ile aşağıda sayılan hususlara uymak zorundadır:

- a) VDK tarafından belirlenen prosedürlere, ilke ve kurallara uygun hareket etmek,
- b) Raporlamaları gerçeğe uygun ve işlem taraflarının mutabakatı doğrultusunda yapmak,
- c) İyi niyet ve dürüstlük ilkelerine uygun davranmak,
- ç) Raporlanan bilgilerin gizliliğini ve güvenliğini sağlamak,
- d) Raporlanan bilgileri on yıl boyunca saklamak,
- e) Üyelik şartlarında her türlü değişikliği VDK'ya bildirmek.

BEŞİNCİ BÖLÜM

Veri Depolama Kuruluşu Nezdindeki Verilerin Paylaşılması

Gizlilik

MADDE 16 - (1) VDK kayıtları gizlidir. Ancak, bu Yönetmelikte belirlenen esaslara uygun olarak bilgi verilmesi gizliliğin ihlali sayılmaz.

(2) VDK nezdindeki bilgilerin kamu tüzel kişileri dâhil üçüncü kişiler ile paylaşımında 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununa ve ilgili diğer mevzuata riayet edilir.

Veri depolama kuruluşları nezdindeki verilere doğrudan erişim

MADDE 17 - (1) Kurul, VDK'lar nezdindeki tüm bilgilere erişim hakkına sahiptir.

(2) Aşağıdaki kuruluşlar mevzuattan kaynaklanan görev, yetki ve sorumlulukları çerçevesinde ihtiyaç duyabilecekleri VDK nezdindeki bilgilere erişim hakkına sahiptir:

- a) Türkiye Cumhuriyeti Hazine ve Maliye Bakanlığı,
- b) Bankacılık Düzenleme ve Denetleme Kurumu,
- c) Türkiye Cumhuriyet Merkez Bankası,
- ç) Tasarruf Mevduatı Sigorta Fonu,
- d) Yatırımcı Tazmin Merkezi,
- e) Kurulca uygun görülecek diğer kamu kurumları.

(3) VDK kapsamındaki bilgilere erişim yetkisine sahip kuruluşlarla oluşturulacak elektronik sistemler ve diğer erişim yöntemlerine ilişkin usul ve esaslar, VDK yönetim kurulu tarafından belirlenir. Bilgi paylaşımından önce bu kurumlar ile VDK arasında protokol imzalanır.

Bildirim yapan tarafların verilere erişimi

MADDE 18 - (1) VDK'ya raporlanan işlemlerin tarafları ile MKT ya da işlemin taraflarına raporlama hizmeti sağlayan yatırım kuruluşları, VDK verilerine yalnızca taraf oldukları ve/veya raporladıkları işlemlerle sınırlı olmak üzere erişim hakkına sahiptir.

Diğer veri talepleri

MADDE 19 - (1) 18 inci maddede sayılan doğrudan erişim yetkisi bulunan kurumlar dışındaki kanun veya kanunla açıkça yetki verilmiş mevzuat hükmü ile yetkili kılınmış kişilerin veri talepleri VDK tarafından karşılanır.

(2) İstatistiki amaçlı veri talepleri, işlemleri gerçekleştiren ve/veya aracılık eden yatırım kuruluşları ve yararlanıcı bazında olmamak koşulu ile kişisel verilerin korunması hakkında mevzuat hükümleri çerçevesinde gecikmeli olarak karşılanabilir.

(3) Yabancı ülke otoritelerinin VDK nezdindeki verilerin paylaşılmasına ilişkin taleplerinin VDK tarafından karşılanması Kurul onayına tabidir. Kurul, söz konusu talepleri;

a) İki ülke arasında verilerin paylaşılmasına ilişkin olarak karşılıklılık esasına dayanan ikili veya çok taraflı işbirliği anlaşması ya da ilgili otoriteler arasında mutabakat zaptı bulunması,

b) Paylaşılan verilerin kullanılmasına ilişkin olarak bu Yönetmelikteki gizlilik ilkelerine eş değer hükümlerin ilgili ülke mevzuatında bulunması,

hususlarını da dikkate alarak sonuçlandırır.

ALTINCI BÖLÜM

Mali Hükümler

Gelirler, ücret ve komisyonlar

MADDE 20 - (1) VDK'nın veri depolama hizmetleri kapsamında uyguladığı ücret ve komisyonlar ile bunların tahsil zaman ve şekilleri VDK yönetim kurulu tarafından belirlenerek Kurul onayına sunulur.

(2) Mevzuat uyarınca üyeler tarafından ilgili VDK'dan alınması zorunlu olmayan ve VDK'nın kendi uhdesinde üyelere sunulan diğer hizmetleri ile ilgili ücretler ise VDK yönetim kurulunca belirlenir.

(3) Merkezi takas hizmeti veren kuruluşlar birinci fıkrada belirtilen ücret ve komisyonlardan muaftır.

YEDİNCİ BÖLÜM

Diğer Hükümler

VDK'nın denetimi

MADDE 21 - (1) Kurul, Kanun kapsamındaki faaliyetleri ile ilgili olarak VDK'nın düzenleme, gözetim ve denetim merciidir. Kurul gerekli gördüğü durumlarda VDK nezdinde, Kanun kapsamındaki faaliyetleri ile ilgili olarak her türlü inceleme ve denetim yapmaya yetkilidir.

(2) VDK'nın bilgi sistemleri, Kurulun bilgi sistemleri denetimine ilişkin düzenlemeleri uyarınca denetime tabidir.

(3) VDK'nın malî denetimi Kurulca ilân edilen listede yer alan bağımsız denetim kuruluşlarınca yapılır. Bağımsız denetim neticesinde hazırlanan rapor eşzamanlı olarak VDK'ya ve Kurula

gönderilir. Kurul gerek gördüğünde belirlediği hususlarla ilgili bağımsız denetim yapılmasını talep edebilir.

VDK'ların dışarıdan hizmet alımı

MADDE 22 - (1) VDK'ların teknolojik altyapısıyla ilgili olarak dışarıdan hizmet alması durumunda;

- a) Hem VDK'nın hem hizmet sağlayan kuruluşun gizlilik prosedürlerini uygulaması,
 - b) VDK ve hizmet sağlayıcı kuruluş arasında bir "Gizlilik Sözleşmesi" imzalanması,
 - c) İş akışının belirlenmesi, bilgi güvenliğine ilişkin gerekli tedbirlerin alınması ve dışarıdan hizmet alımına ilişkin prosedürlerin oluşturulması,
- şarttır.

(2) Kanununun 87 nci maddesi kapsamında kendisine raporlanan verileri bir dış hizmet olarak bulut bilişim hizmetlerini kullanmak suretiyle saklayamaz.

Disiplin hükümleri

MADDE 23 - (1) Düzen ve dürüstlüğü bozan, işlere hile karıştıran, işlerin açık, düzenli ve dürüst yürütülmesine, mevzuata ve kararlara aykırı hareket eden üyeler VDK tarafından Kurula bildirilir. Kurulca gerekli işlemler yerine getirilir.

Uygulama esasları

MADDE 24 - (1) Bu Yönetmelikte yer almayan ya da açıklık bulunmayan konularda, genel hükümleri ve veri depolama hizmetine ilişkin uluslararası prensip ve düzenlemeleri göz önünde bulundurarak karar vermeye ve uygulamayı yönlendirmeye Kurul yetkilidir.

Yürürlük

MADDE 25 - (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 26 - (1) Bu Yönetmelik hükümlerini Sermaye Piyasası Kurulu yürütür.

Yenilenmiş Ürünlerin Satışı Hakkında Yönetmelik

Resmî Gazete Tarihi : 22.08.2020

Resmî Gazete Sayısı : 31221

YENİLENMİŞ ÜRÜNLERİN SATIŞI HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı, Ek-1’de yer alan kullanılmış malların yenilenecek tekrar satışa sunulmasına ilişkin uygulama usul ve esaslarını düzenlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, Ek-1’de yer alan kullanılmış malların yenilenmesi, sertifikalandırılması ve tekrar satışa sunulmasına ilişkin faaliyetleri kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 7/11/2013 tarihli ve 6502 sayılı Tüketicinin Korunması Hakkında Kanununun 12 nci, 57 nci ve 84 üncü maddelerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Yönetmelikte geçen;

- a) Bakanlık: Ticaret Bakanlığını,
- b) Genel Müdürlük: Tüketicinin Korunması ve Piyasa Gözetimi Genel Müdürlüğünü,
- c) İş günü: Ulusal, resmî ve dinî bayram günleri ile yılbaşı, 1 Mayıs, 15 Temmuz ve Pazar günleri dışındaki çalışma günlerini,
- ç) İthalatçı: Kamu tüzel kişileri de dâhil olmak üzere mal veya hizmetleri ya da bu malların hammaddelerini yahut ara mallarını ticari veya mesleki amaçlarla ithal ederek satım, kira, finansal kiralama veya benzeri bir yolla piyasaya süren gerçek veya tüzel kişiyi,

- d) Kalıcı veri saklayıcısı: Tüketicinin gönderdiği veya kendisine gönderilen bilgiyi, bu bilginin amacına uygun olarak makul bir süre incelemesine elverecek şekilde kaydedilmesini ve değiştirilmeden kopyalanmasını sağlayan ve bu bilgiye aynen ulaşılmasına imkân veren kısa mesaj, elektronik posta, internet, disk, CD, DVD, hafıza kartı ve benzeri her türlü araç veya ortamı,
- e) Kanun: Tüketicinin Korunması Hakkında Kanunu,
- f) Kullanılmış mal: Alışverişe konu olan taşınır eşyalardan Ek-1’de yer alan ikinci el malları,
- g) Tüketici: Ticari veya mesleki olmayan amaçlarla hareket eden gerçek veya tüzel kişiyi,
- ğ) Üretici: Kamu tüzel kişileri de dâhil olmak üzere tüketiciye sunulmuş olan mal ya da bu malların hammaddelerini yahut ara mallarını üretenler ile mal üzerine markasını, unvanını veya herhangi bir ayırt edici işaretini koyarak kendisini üretici olarak gösteren gerçek veya tüzel kişiyi,
- h) Yenileme merkezi: Kullanılmış malın yenilenmesi, sertifikalandırılması ve bu Yönetmelikte belirtilen diğer işlemleri yürütmek üzere kurulan, Bakanlık veya Türk Standardları Enstitüsünün belirlediği standartları taşıyan ve Bakanlıktan aldığı yenileme yetki belgesine dayanarak faaliyet gösteren tüzel kişiyi,
- ı) Yenileme yetki belgesi: Yenileme merkezi faaliyetiyle iştigal edilebilmesi için ticari işletmeler adına Bakanlık tarafından düzenlenen belgeyi,
- i) Yenilenmiş ürün: Yenileme merkezi tarafından yapılan yenileme ve sertifikalandırma işleminden sonra satışa sunulan kullanılmış malı,
- j) Yetkili alıcı: Kullanılmış malı yenilenmesi amacıyla (Mülga ibare:RG-2/9/2021-31586) yenileme merkezi adına alan ve yenileme merkezi tarafından yetkilendirilmiş gerçek veya tüzel kişiyi,
- k) Yetkili satıcı: Kamu tüzel kişileri de dâhil olmak üzere ticari veya mesleki amaçlarla tüketiciye yenilenmiş ürün sunan ya da yenilenmiş ürün sunanın adına veya hesabına hareket eden ve yenileme merkezi tarafından yetkilendirilmiş gerçek veya tüzel kişiyi,
- ifade eder.

İKİNCİ BÖLÜM

Yenileme Faaliyetlerine İlişkin Usul ve Esaslar

Genel esaslar

MADDE 5 - (1) Kullanılmış mallar, yenileme merkezleri tarafından, Bakanlıkça belirlenen düzenleme veya Türk Standardları Enstitüsünün belirlediği standartlara uygun şekilde yenilenebilir. Yenilenen

kullanılmış mallar, sertifikalandırıldıktan ve ambalajlandıktan sonra yenilenmiş ürün olarak tekrar satışa sunulabilir.

(2) Kullanılmış mal yetkili alıcı tarafından tüketiciden alınarak yenileme merkezine iletilmek suretiyle veya yenileme merkezi tarafından tüketiciden doğrudan alınarak yenilenebilir.

(3) (Değişik:RG-2/9/2021-31586) Elektronik kimlik bilgisi bulunan kullanılmış malların yenilenebilmesi için en az bir yıl öncesine ilişkin data, ses ya da kısa mesaj kullanım trafiğinin bulunması zorunludur.

(4) Yenilenmiş ürünün ambalajında, etiketinde, reklam ve ilanlarında tüketicinin kolaylıkla algılayabileceği bir şekilde, “yenilenmiş ürün” ibaresine ve yenileme merkezinin bilgisine yer verilerek satışa sunulması zorunludur. Yenileme işlemi yapılırken yenilenen tüm parçaların üretici ya da üreticinin yetki verdiği ithalatçı onaylı parçalar olması halinde, “üretici onaylı parçalar kullanılarak yenilenmiş ürün” ibaresine de yer verilir.

(5) Yenilenmiş ürünün 14 üncü maddede düzenlenen yenilenmiş ürün garantisi ile satışa sunulması zorunludur. Yenilenmiş ürün garantisi taahhüdünün hazırlanması sorumluluğu yenileme merkezine, tüketiciye verilmesi ve teslim edildiğinin ispat yükü ise yetkili satıcıya aittir. Yenilenmiş ürün garantisi yazılı olarak veya kalıcı veri saklayıcısıyla verilebilir. Yenilenmiş ürün garantisinden ve garanti süresince verilecek bakım, onarım ve montaj gibi satış sonrası hizmetlerden yetkili satıcı ve yenileme merkezi müteselsilen sorumludur.

(6) Kullanılmış malın üreticisi veya ithalatçısı tarafından veya yenileme merkezi tarafından üreticisinin veya ithalatçısının yenileme işlemine ilişkin muvafakati alınarak yenilenmesi hallerinde üreticinin veya ithalatçının sağladığı garantiler geçerliliğini korur.

(7) Yenilenmiş ürünün Türkçe tanıtma ve kullanma kılavuzuyla satışa sunulması zorunludur. Türkçe tanıtma ve kullanma kılavuzunun hazırlanması sorumluluğu yenileme merkezine, tüketiciye verilmesi ve teslim edildiğinin ispat yükü ise yetkili satıcıya aittir. Türkçe tanıtma ve kullanma kılavuzu yazılı olarak veya kalıcı veri saklayıcısıyla verilebilir.

(8) Yetkili alıcı ve yetkili satıcı, ayrı ayrı yetki almak şartıyla, birden fazla yenileme merkezine hizmet verebilir. Yetkili alıcı ve yetkili satıcının bu Yönetmelik kapsamındaki iş ve işlemleri yenileme merkezinin kendilerine verdiği yetki ile sınırlıdır.

(9) (Ek:RG-2/9/2021-31586) Yenileme yetki belgesi bulunmayanlar veya bu belgeye sahip firmalara bağlı yetkili alıcı ve yetkili satıcı vasfını taşımayanlar tarafından yenilenmiş ürün algısı oluşturacak şekilde reklam ve ticari uygulama yapılamaz.

Yenileme merkezlerinin kuruluşu

MADDE 6 - (1) Kullanılmış malların bu Yönetmelikte belirlenen esaslara göre yenilenmesi, sertifikalandırılması ve tekrar satışa sunulması amacıyla, Bakanlıkça belirlenen düzenleme veya Türk Standardları Enstitüsünün belirlediği standartlara uygun şekilde faaliyet göstermek üzere yenileme merkezleri kurulur.

Başvuru ve izin

MADDE 7 - (1) Yenileme merkezlerinin Bakanlıkça onaylı yenileme yetki belgesi alması zorunludur.

(2) Yenileme yetki belgesi verilmesine ilişkin hususlar Bakanlığın internet sayfasında ilan edilir.

(3) Bakanlığa yapılan başvurular üzerine, Genel Müdürlük tarafından bu Yönetmeliğe uygunluk açısından gerekli incelemeler yapılarak yeterli görülenlere yenileme yetki belgesi verilir.

(4) Yenileme yetki belgesi her bir yenileme merkezi için ayrı ayrı düzenlenir ve bu yetki belgesi başkasına devredilemez.

(5) Genel Müdürlük, başvuruları değerlendirirken gerek duyması halinde tüketicilerin sağlık ve güvenliği ile ekonomik çıkarlarını korumak amacıyla, başvuruda bulunan yenileme merkezi ile ilgili olarak diğer kurum ve kuruluşlardan görüş alabilir ve inceleme yaptırabilir.

Yenileme yetki belgesi verilmesinde aranan şartlar

MADDE 8 - (1) Yenileme yetki belgesinin alınabilmesi için;

a) Bakanlıkça veya Türk Standardları Enstitüsü tarafından belirlenen düzenleme veya standartlarda yer alan özelliklere uygun olarak alınmış hizmet yeri yeterlilik belgesine sahip olunması,

b) Ticaret odasına kayıtlı olunması,

c) Kurumlar vergisi mükellefi olunması,

ç) Ticaret şirketlerinin temsile yetkili kişilerinin;

1) On sekiz yaşını doldurmuş olması,

2) İflas etmemiş veya iflas etmiş olsa bile itibarının yerine gelmiş olması,

3) Kasten işlenen bir suçtan dolayı beş yıldan fazla hapis cezasına mahkûm edilmemiş veya devletin güvenliğine, anayasal düzene ve bu düzenin işleyişine, milli savunmaya ve devlet sırlarına karşı suçlar; casusluk, zimmet, irtikâp, rüşvet, hırsızlık, dolandırıcılık, sahtecilik, güveni kötüye kullanma, hileli iflas, ihaleye fesat karıştırma, edimin ifasına fesat karıştırma, suçtan kaynaklanan malvarlığı değerlerini aklama, terörizmin finansmanı, kaçakçılık, vergi kaçakçılığı veya haksız mal edinme,

işkence, cinsel saldırı ve çocukların cinsel istismarı, cinsel taciz, kişiyi hürriyetinden yoksun kılma, fuhuş, kumar oynanması için yer ve imkân sağlama, bilişim suçları ile özel hayata veya hayatın gizli alanına karşı işlenmiş suçlardan hüküm giymemiş veya ticaret ve sanat icrasından hükmen yasaklanmamış olması,

d) On milyon Türk Lirasından az olmamak üzere ödenmiş sermayeye sahip olunması,

e) Bakanlık tarafından ilan edilecek diğer hususların sağlanması,
gereklidir.

Yenileme yetki belgesinin geçerlilik süresi ve diğer işlemler

MADDE 9 - (1) Yenileme yetki belgesinin geçerlilik süresi beş yıldır. Belgenin geçerlilik süresi dolmadan yenilenmesi zorunludur.

(2) Yenileme merkezinin unvan, adres ve diğer iletişim bilgileri ile ortaklık yapısında değişiklik olması durumunda bu değişiklikler otuz gün içinde Bakanlığa bildirilir.

Yenileme yetki belgesinin iptali

MADDE 10 - (1) Bu Yönetmeliğe aykırı uygulamaların tespiti ve bununla ilgili olarak Genel Müdürlüğün yazılı uyarısına rağmen verilen süre içinde aykırılığın düzeltilmemesi, belge verilmesinde aranan şartların kaybedilmesi veya yenileme merkezinin başvurusu üzerine yenileme yetki belgesi iptal edilir. Belgesi iptal edilen yenileme merkezine bir yıl süreyle belge verilmez.

(2) Geçerlilik süresi sona ermesine rağmen belgesini yenilemeyen veya belgesi iptal edilen yenileme merkezi faaliyetlerine devam edemez.

ÜÇÜNCÜ BÖLÜM

Sorumluluğa İlişkin Usul ve Esaslar

Yetkili alıcının sorumlulukları

MADDE 11 - (1) Yetkili alıcı, elektronik kimlik bilgisi bulunan kullanılmış mallar için Dijital Türkiye Portalı (e-Devlet) üzerinden malın "Beyaz Liste"de olup olmadığını kontrol eder. (Ek ibare:RG-2/9/2021-31586) Varsa Garanti belgesi, fatura veya fatura yerine geçen perakende satış fişi, ödeme kaydedici cihaz fişi, gider pusulası ve benzeri belgelerin kontrolünü yapar ve bu kontrole ilişkin işlem kayıtlarını saklar.

(2) (Değişik:RG-2/9/2021-31586) Yetkili alıcı, elektronik kimlik bilgisi bulunan kullanılmış malların en az bir yıl öncesine ilişkin data, ses ya da kısa mesaj kullanım trafiği bulunduğunu Bilgi Teknolojileri ve İletişim Kurumu kayıtlarından kontrol eder.

(3) Kullanılmış malın kişisel veri bulundurma özelliğinin bulunması halinde; yetkili alıcı tüketiciden, malın içinde bulunan verilerin yenileme merkezi tarafından herhangi bir veri işleme yapılmadan yok edileceğine ve bir daha bu verilere ulaşılamayacağına dair onayını ve malın yetkili alıcıya teslim tarihinden önceki her türlü hukuki, idari ve cezai sorumluluğun tüketicinin kendisine ait olduğuna dair beyanını alır. Bu beyanın bir örneği tüketiciciye yazılı olarak veya kalıcı veri saklayıcısı ile verilir. Beyanın bir örneğinin tüketiciciye verildiğinin ispat yükü yetkili alıcıya aittir.

(4) (Değişik:RG-2/9/2021-31586) Yetkili alıcı, kullanılmış malın değerlendirme işlemini malın kendisine teslim edildiği veya ulaştığı tarihi takip eden üç işgünü içinde sonuçlandırır ve bu süre içinde tüketicinin bu değerlemeyi kabul ettiğine ilişkin onayını yazılı olarak veya kalıcı veri saklayıcısıyla alır.

(5) (Değişik:RG-2/9/2021-31586) Yetkili alıcı, tüketicinin onayı alındığında tüketiciciye ödemeyi yapar veya yapılmasını sağlar. Ödeme süresi, tüketiciciye önceden bildirilmesi ve onayının alınması koşuluyla üç işgününe kadar uzatılabilir. Bu ödeme miktarı, tüketicinin yeni bir mal satın aldığı durumda, yeni malın fiyatından indirilebilir.

Yenileme merkezinin sorumlulukları

MADDE 12 - (1) Yenileme merkezi, kendisine ulaşan kullanılmış malı, Bakanlığın veya Türk Standardları Enstitüsünün belirlediği düzenleme veya standartlara uygun şekilde yenileyerek satışa hazır hale getirir.

(2) Yenileme merkezi, kullanılmış malı yenileme işlemini yaparken;

a) Onarım veya parça değişikliği gerekiyorsa bu onarım ve değişikliğin yapılmasını,

b) Önceki kullanıcıya ait kişisel veriler dâhil tüm bilgilerin yok edilmesini,

c) Fabrika ayarlarına getirilmesini,

ç) Performansının ve tüm fonksiyonlarının gerektiği gibi çalıştığının test edilmesini,

sağlar.

(3) Yenileme merkezi, 11 inci maddenin birinci ve ikinci fıkralarında düzenlenen hükümlerde yer alan yükümlülüklerin yerine getirilip getirilmediğinin kontrolünü sağlar ve 11 inci maddenin birinci fıkrasında belirtilen şartları taşımayan kullanılmış mallara yenileme işlemi yapamaz.

- (4) (Değişik:RG-2/9/2021-31586) Yenileme merkezi, elektronik kimlik bilgisi bulunan kullanılmış malların en az bir yıl öncesine ilişkin data, ses ya da kısa mesaj kullanım trafiği bulunduğunu Bilgi Teknolojileri ve İletişim Kurumu kayıtlarından kontrol eder. Bu şartları sağlamayan kullanılmış mallara yenileme işlemi yapamaz.
- (5) Yenileme merkezi yenileme işlemini yaparken kullanılmış malın elektronik kimlik bilgisini değiştiremez.
- (6) (Değişik:RG-2/9/2021-31586) Yenileme merkezi yenilediği kullanılmış malın sertifikalandırma işlemini, Türk Standardları Enstitüsü tarafından numaralandırılmış hologramlı sertifika formunu kullanarak ve ticari unvanı, iletişim bilgileri, yenileme yetki belgesi ve yenileme işlemine ilişkin bilgileri içeren karekod ile güvenliğini sağlayacak şekilde yapar ve bu sertifikanın yenilenmiş ürünle birlikte yazılı olarak veya kalıcı veri saklayıcısıyla verilmesini sağlar.
- (7) Yenileme merkezinin kullanılmış malı tüketiciden doğrudan alarak yetkili alıcı sıfatı taşıması halinde 11 inci madde hükümlerine uyması zorunludur.
- (8) Yenileme merkezinin yenilenmiş ürünü tüketicie doğrudan satarak yetkili satıcı sıfatını taşıması halinde 13 üncü madde hükümlerine uyması zorunludur.
- (9) Yenileme merkezi, yapılan yenileme işlemi nedeniyle yenilenmiş ürünün bir kişiye veya bir mala zarar vermesi halinde zararın tazmininden sorumludur.
- (10) Yenileme merkezinin herhangi bir şekilde ticari faaliyetinin sona ermesi, yetki belgesinin yenilenmemesi veya iptal edilmesi halinde, yenilenmiş ürün garantisi süresince bakım ve onarım hizmetlerinin sunulmasından yetkili satıcı ve yenileme merkezi müteselsilen sorumludur.
- (11) (Ek:RG-2/9/2021-31586) Yenileme merkezi, ilgili standartta belirlenen yenileme işlemini kendisi yapabileceği gibi ihtiyaç duyulması halinde yenileme yetki belgesi almış diğer yenileme merkezlerinden de hizmet alabilir.
- (12) (Ek:RG-2/9/2021-31586) Yenileme merkezi, sekizinci maddedeki sermaye şartı dışında Yönetmelikteki diğer şartları sağlayan kendisine bağlı şubeler oluşturabilir. Bu şubeler için ayrıca yenileme yetki belgesi alınması zorunludur.
- (13) (Ek:RG-2/9/2021-31586) Yenileme merkezi, yenileme faaliyetlerine ilişkin Bakanlıkça belirlenecek bilgi ve belgeleri Bakanlığa bildirmek zorundadır.

Yetkili satıcının sorumlulukları

MADDE 13 - (1) Tüketici ödeme yükümlülüğü altına girmeden önce, yenilenmiş ürüne ilişkin yapılan işlemler, değiştirilen parçalar ve garantiyle ilgili hususlar hakkında bilgilendirilir. Bu bilgilendirmenin yapıldığına ilişkin ispat yükü satıcıya aittir.

(2) Yetkili satıcı, yenilenmiş ürüne ilişkin reklam ve ilanlarında yer alan ifadelerle bağlıdır.

(3) Yetkili satıcı, satışa sunulan yenilenmiş ürünün Türkçe tanıtma ve kullanma kılavuzuyla tüketiciye verilmesini sağlamak zorundadır. Tanıtma ve kullanma kılavuzu yazılı olarak veya kalıcı veri saklayıcısıyla verilebilir.

(4) Yetkili satıcı, satışa sunulan yenilenmiş ürün için 14 üncü maddede belirtilen yenilenmiş ürün garantisini sağlamak zorundadır. Yenilenmiş ürün garantisi yazılı olarak veya kalıcı veri saklayıcısıyla verilebilir.

(5) Yetkili satıcı ve ilgili yenileme merkezi, ayrı tüzel kişiliklere sahip olsalar dahi, yenilenmiş ürüne ilişkin tüketicinin yasal haklarından müteselsilen sorumludur.

(6) Yetkili satıcının herhangi bir şekilde ticari faaliyetinin sona ermesi halinde, yenilenmiş ürün garantisi süresince bakım ve onarım hizmetlerinin sunulmasından yetkili satıcı ve yenileme merkezi müteselsilen sorumludur.

Yenilenmiş ürün garantisi ve satış sonrası hizmetler

MADDE 14 - (1) Yenileme merkezi tüketicinin yasal hakları saklı kalmak kaydıyla yenilenmiş ürünle ilgili değişim, onarım, bakım, bedel iadesi, bedel indirimi ve benzeri hususlarda taahhütlerini içeren yenilenmiş ürün garantisi vermek zorundadır. Taahhüt veren yenilenmiş ürüne ilişkin reklam ve ilanlarında yer alan ifadelerle de bağlıdır.

(2) Yenilenmiş ürün garantisi, yenilenmiş ürünün tüketiciye teslim tarihinden itibaren başlar ve asgari bir yıldır.

(3) Yenilenmiş ürün garantisi taahhüdünde; tüketicinin yasal haklarının saklı olduğu bilgisi ile garantiden faydalanma koşulları, garanti süresi, garanti verenin unvanı ve iletişim bilgileri yer almak zorundadır. Bu taahhüdün tüketiciye yazılı olarak veya kalıcı veri saklayıcısı ile verilmesi sorumluluğu yetkili satıcıya aittir.

(4) Yenilenmiş ürün garantisi süresince, taahhüt edilen hakların kullanılması nedeniyle; nakliye, posta, kargo veya servis elemanlarının ulaşım gideri dahil olmak üzere tüketiciden herhangi bir masraf talep edilemez.

(5) Yenilenmiş ürün garantisi süresi içinde ücretsiz onarım veya ayıpsız yenilenmiş misli ile değişim haklarından birinin seçilmesi durumunda, bu talebin yenileme merkezine veya yetkili satıcıya yöneltilmesinden itibaren azami yirmi iş günü içinde yerine getirilmesi zorunludur. Bu süre, ürünün yetkili satıcıya ya da yenileme merkezine teslim edilmesiyle başlar.

(6) Tüketicinin bedel iadesi veya bedel indirimi hakkını seçtiği durumlarda, ödemiş olduğu bedelin tümü veya yapılan indirim tutarı derhâl tüketiciye iade edilir.

(7) Yenilenmiş ürünün tamirinin tamamlandığı tarih tüketiciye telefon, faks, e-posta, iadeli taahhütlü mektup ve benzeri bir yolla bildirilir. Uyuşmazlık halinde bildirimle ilişkin ispat yükü yetkili satıcıya ve yenileme merkezine aittir.

(8) Yenilenmiş ürünün, yenileme merkezi tarafından hazırlanan tanıtma ve kullanma kılavuzunda yer alan hususlara aykırı kullanılması nedeniyle ortaya çıkan arızalarda, tüketici yenilenmiş ürün garantisi taahhüdünden faydalanamaz.

(9) Yetkili satıcı ya da yenileme merkezi tarafından, kargo ile gönderilen arızalı yenilenmiş ürünler hariç olmak üzere, kendilerine teslim edilen veya kendileri tarafından teslim alınan arızalı yenilenmiş ürünler ile ilgili olarak ürünün teslim alındığına dair aşağıdaki bilgileri içeren teslim fişinin düzenlenmesi ve tüketiciye verilmesi zorunludur:

- a) Teslim edenin adı, soyadı ve imzası.
- b) Teslim alanın adı, soyadı ve imzası.
- c) Tüketicinin yenilenmiş ürüne ilişkin şikâyet ve talepleri.
- ç) Yenilenmiş ürünün cinsi, markası ve modeli.
- d) Teslim tarihi.

(10) Yetkili satıcı ya da yenileme merkezi tarafından, onarım hakkını kullanan tüketicilere teslim edilen yenilenmiş ürünlerle ilgili olarak aşağıdaki bilgileri içeren servis fişinin tekemmül ettirilmesi ve tüketicilere verilmesi zorunludur:

- a) Yenileme merkezinin unvanı, adresi ve iletişim bilgileri.
- b) Tüketicilere teslim tarihi.
- c) Arızasına ve yapılan işlemlere ilişkin bilgi.
- ç) Yenilenmiş ürün garantisi kapsamı dışında ise ücreti.
- d) Yenileme merkezi yetkilisinin imzası.

e) Kargo ile teslim alınanlar haricinde, tüketicinin adı, soyadı, adresi ve telefonu ile imzası.

(11) Teslim fişi ve servis fişi kalıcı veri saklayıcısıyla da tüketiciye verilebilir. Bu durumda, bu belgelerin tüketiciye verildiğine ilişkin onayının alınması zorunludur. Tüketicinin onayının alındığının ispat yükü yetkili satıcı ve yenileme merkezine aittir.

DÖRDÜNCÜ BÖLÜM

Çeşitli ve Son Hükümler

Bilgi ve belgelerin saklanması

MADDE 15 - (1) Bu Yönetmelikte düzenlenmesi öngörülen her bir işleme ilişkin bilgi ve belgelerin beş yıl boyunca saklanması zorunludur.

Kişisel verilerin korunması

MADDE 16 - (1) Bu Yönetmelik kapsamında yürütülen kişisel veri işleme faaliyetlerinde 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile bu Kanuna dayanılarak çıkarılan ikincil mevzuatta yer alan usul ve esaslara uyulması zorunludur.

Bilgilendirme yükümlülüğü

MADDE 17 - (Ek:RG-2/9/2021-31586)

(1) Ek-1'de yer alan ve yenileme işlemi yapılmadan ikinci el ticarete konu olan kullanılmış malların, tüketicinin kolaylıkla görebileceği ve okuyabileceği şekilde, malın mevcut durumunu ve varsa yapılan işlemleri gösteren bilgilendirme etiketi ile satılması zorunludur.

Yürürlük

MADDE 18 - (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 19 - (1) Bu Yönetmelik hükümlerini Ticaret Bakanı yürütür.

Elektrikli Skuter Yönetmeliđi

Resmî Gazete Tarihi : 14.04.2021

Resmî Gazete Sayısı : 31454

Ulaştırma ve Altyapı, Çevre ve Şehircilik ile İçişleri Bakanlıklarından:

ELEKTRİKLİ SKUTER YÖNETMELİĐİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliđin amacı;

a) Paylaşımli elektrikli skuter (e-skuter) işletmeciliđi faaliyetlerini ÷lke ekonomisinin gerektirdiđi şekilde düzenlemek, bu faaliyetlerde düzeni ve güvenliđi sağlamak, ulaşımın çevre üzerindeki egzoz emisyon ve karbon salınımı gibi olumsuz etkilerini azaltarak çevresel deđerleri korumak, hareketliliđi artırarak kısa mesafeli seyahatlerde şahsi araç kullanımı yerine paylaşımli e-skuter kullanımının yaygınlaştırılması ile paylaşımli e-skuterlerin diđer ulaşım türleri ile entegre, sürdürülebilir bir ulaşım sistemi içerisinde gelişimini sağlamak üzere bu faaliyetlere ilişkin pazara giriş şartlarını ve hizmet üretenler ile hizmetten yararlananların hak, yükümlölük ve sorumluluklarını,

b) Elektrikli skuter ve kullanımına ilişkin 13/10/1983 tarihli ve 2918 sayılı Karayolları Trafik Kanununda sayılan hususlar dışında kalan diđer hususları,

belirlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, karayolunda kullanılacak e-skuterler, paylaşımli e-skuter işletmeciliđi faaliyeti yapanlar ile bu faaliyetlerden yararlananlar ve bu faaliyetlerde kullanılan her türlü e-skuterleri kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik; 13/10/1983 tarihli ve 2918 sayılı Karayolları Trafik Kanununun 66 ncı maddesi, 26/5/1981 tarihli ve 2464 sayılı Belediye Gelirleri Kanunu, 10/7/2004 tarihli ve 5216 sayılı

Büyükşehir Belediyesi Kanunu, 3/7/2005 tarihli ve 5393 sayılı Belediye Kanunu, 26/9/2011 tarihli ve 655 sayılı Ulaştırma ve Altyapı Alanına İlişkin Bazı Düzenlemeler Hakkında Kanun Hükmünde Kararname ve 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete’de yayımlanan 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Yönetmelikte geçen;

- a) Bakanlık: İlgisine göre, Çevre ve Şehircilik Bakanlığını, İçişleri Bakanlığını ya da Ulaştırma ve Altyapı Bakanlığını,
- b) e-Devlet (www.turkiye.gov.tr): e-Devlet hizmetlerinin son kullanıcıya farklı erişim kanallarından tek noktadan bütünleşik olarak sunulduğu ortak elektronik platformu,
- c) Elektrikli skuter (e-skuter): Hızı en fazla 25 km/saate ulaşan, tekerlekli, fren mekanizmasına sahip, ayak tahtası ve tutamağı olabilen, dikey bir direksiyon mekanizması içerebilen ve ayakta kullanılan elektrikli taşıtı,
- ç) Elektronik tebligat sistemi: 655 sayılı Kanun Hükmünde Kararnameye ve bu Yönetmeliğe göre düzenlenen idari para cezalarının, 4/1/1961 tarihli ve 213 sayılı Vergi Usul Kanununun 107/A maddesi hükümlerine göre Gelir İdaresi Başkanlığı tarafından kurulan teknik altyapı üzerinden muhatapların elektronik adreslerine tebliğ edilmek üzere tebliğ evrakının gönderildiği ve elektronik ortamda delillendirilerek tesliminin sağlandığı sistemi,
- d) İdare: Ulaştırma ve Altyapı Bakanlığını,
- e) Kararname: 26/9/2011 tarihli ve 655 sayılı Ulaştırma ve Altyapı Alanına İlişkin Bazı Düzenlemeler Hakkında Kanun Hükmünde Kararnameyi,
- f) Kısa unvan: Yetki belgesi sahibinin, Türk Patent ve Marka Kurumu tarafından tescil edilmiş markasını veya ticaret sicilinde tescil edilmiş, varsa işletme adını,
- g) Paylaşımlı e-skuter: Kullanıcılara kısa süreli e-skuter kiralama imkanı veren elektronik sistemin kullanıldığı hizmetleri,
- ğ) Paylaşımlı e-skuter izni (e-skuter izni): Bu Yönetmelik kapsamında yetki belgesi almış olan gerçek veya tüzel kişilerin faaliyetlerinde kullanacakları e-skuterler için aldıkları izni,
- h) UKOME: Büyükşehir belediyesi ulaşım koordinasyon merkezlerini,

1) Ulaştırma Otomasyon Sistemi (U-Net): Bu Yönetmeliğe göre faaliyet gösteren gerçek ve tüzel kişilerin, faaliyetlerine ilişkin belirlenen verilerin İdare tarafından tutulduğu, gerektiğinde ilgili kamu kurum ve kuruluşlarıyla veri paylaşımına açık olduğu/olabileceği sistemi,

i) Yetki belgesi: Bu Yönetmelik kapsamında paylaşımlı e-skuter işletmeciliği faaliyetinde bulunmak isteyen gerçek veya tüzel kişilere faaliyet izni veren ve İdare tarafından düzenlenen belgeyi, ifade eder.

İKİNCİ BÖLÜM

Genel Hususlar

E-skuter kullanımına ilişkin genel hususlar

MADDE 5 - (1) E-skuter sürücülerinin uyacakları kurallar aşağıda gösterilmiştir:

a) E-skuterin;

- 1) Ayrı bisiklet yolu veya bisiklet şeridi varsa taşıt yolunda sürülmesi,
- 2) Otoyol, şehirler arası karayolları ve azami hız sınırı 50 km/s üzerinde olan karayollarında sürülmesi,
- 3) İki den fazlasının taşıt yolunun bir şeridinde yan yana sürülmesi,
- 4) Yaya yollarında sürülmesi,
- 5) Başka bir araca bağlanarak, asılıp tutunarak sürülmesi,
- 6) İzin alınarak yapılan gösteriler dışında, akrobatik hareketler yapılarak sürülmesi,
- 7) Manevra için işaret verme halleri dışında tek elle sürülmesi,
- 8) Kamu nizamını bozacak, özel mülkiyeti ihlal edecek ve yayalar, engelliler veya hareket kısıtlılığı olan kişilerin güvenli ve bağımsız hareketlerini, araç ve yaya trafiğini engelleyecek şekilde park edilmesi,

b) E-skuterde;

- 1) Diğer araçlar izlenirken, geçilirken, manevra yapılırken; karayolunu kullananların hareketini zorlaştırıcı, tehlike doğurucu davranışlarda bulunulması,
- 2) Sürücü dışında başka kişilerin taşınması,
- 3) Sırtta taşınabilen kişisel eşya harici yük ve yolcu taşınması,

yasaktır.

(2) Kullanılacak e-skuterin; gece diğer araç sürücüleri ve yayalar tarafından rahat bir şekilde fark edilmelerini sağlamak üzere; önde beyaz ışık verecek ve en az 20 metre öne aydınlatabilecek şekilde bir adet far, arkada, kırmızı renkte ışık veren bir lamba ve kırmızı reflektör ile 30 metreden duyulabilecek ses çıkarabilen zil, korna veya benzeri ses aleti ile teçhiz edilmiş olması zorunludur.

(3) E-skuter kullananlar 2918 sayılı Kanunda ve ilgili diğer mevzuatta belirtilen kurallara uymakla yükümlüdürler.

Paylaşımlı e-skuter işletmeciliğine ilişkin genel hususlar

MADDE 6 - (1) Bu Yönetmelik kapsamında yürütülecek paylaşımlı e-skuter işletmeciliği faaliyetleri, ekonomik, güvenli, çevreye olumsuz etkisi en az, fert, toplum ve çevre sağlığı ile bunların güvenliğini, engelli erişilebilirliğini ve trafik güvenliğini olumsuz yönde etkilemeyecek ve kamu yararını gözeterek tarzda serbest rekabet ortamında gerçekleştirilir.

(2) Bu Yönetmeliğe göre yürütülecek paylaşımlı e-skuter işletmeciliği faaliyetlerinin, ilgili diğer mevzuata uygun olarak gerçekleştirilmesi esastır.

(3) Paylaşımlı e-skuter işletmeciliği faaliyeti, sadece yetki belgesi ve paylaşımlı e-skuter izni alan gerçek veya tüzel kişiler tarafından yapılır.

(4) Bu Yönetmeliğe göre düzenlenecek yetki belgeleri ile verilecek e-skuter izinleri, satılamaz ve devredilemez.

(5) Yetki belgesi alanlar, verdikleri hizmetlerden ayırım yapmaksızın, haksız rekabete imkan vermeyecek şekilde, herkesin yararlanmasını ve hizmetin sürekliliğini sağlamak zorundadırlar.

(6) Bu Yönetmelik kapsamında yürütülecek paylaşımlı e-skuter işletmeciliği faaliyetlerinin yerine getirilmesi üçüncü şahıslar tarafından engellenemez.

(7) İdare, paylaşımlı e-skuter kullanım ücreti ile ilgili taban ve/veya tavan ücret tarifesi uygulaması getirebilir.

ÜÇÜNCÜ BÖLÜM

Yetki Belgesi ve E-Skuter İzni Almanın Genel ve Özel Şartları

Yetki belgesi almanın veya yenilemenin genel şartları ile faaliyetin geçici durdurulması

MADDE 7 - (1) Yetki belgesi almak veya yenilemek için;

a) Gerçek kişilerin Türkiye Cumhuriyeti tabiiyetinde olmaları,

- b) Tüzel kişilerin Türkiye Cumhuriyeti kanunlarına göre kurulmuş ve ticaret siciline tescil edilmiş olmaları,
 - c) Faal vergi mükellefi olmaları,
 - ç) Merkezi adreslerinin bulunduğu yerdeki ticaret odası veya ticaret ve sanayi odası veya esnaf ve sanatkarlar odasından birine kayıtlı olmaları,
 - d) Elektronik tebligat sistemine üye olmaları,
 - e) 8 inci maddede belirtilen özel şartları sağlamaları,
 - f) 24 üncü maddenin birinci fıkrasında belirtilen ücreti ödemiş olmaları,
- şarttır.

(2) Bu Yönetmelik kapsamında faaliyet gösterecek yabancı gerçek ve tüzel kişilere, 5/6/2003 tarihli ve 4875 sayılı Doğrudan Yabancı Yatırımlar Kanunu hükümleri ile bu Yönetmeliğin belirlediği şartları yerine getirmeleri halinde yetki belgesi verilir.

(3) Birinci fıkranın (c), (ç), (d) veya (e) bendinde belirlenen yetki belgesi alma şartlarından herhangi birinin kaybedilmesi ve kaybedilen şartın veya şartların, kaybedildiği tarihten itibaren doksan gün içerisinde giderilmemesi veya tamamlanmaması halinde, yetki belgesi verilenin bu Yönetmelik kapsamındaki faaliyeti geçici olarak durdurulur. Bu şekilde faaliyeti geçici olarak durdurulanlara, kaybedilen şartı/şartları sağlaması/tamamlaması halinde faaliyetine yeniden izin verilir.

Yetki belgesi almanın veya yenilemenin özel şartları

MADDE 8 - (1) Yetki belgesi için başvuranların;

- a) 500.000 Türk Lirası sermayeye veya işletme sermayesine sahip olması,
 - b) Standartları İdare tarafından belirlenen ve yapılacak faaliyete uygun bir internet sitesi ile mobil uygulama/uygulamalara sahip olması,
 - c) Gerçekleştirecekleri faaliyetlere ilişkin verilerin tutulacağı veri tabanının saklanacağı sunucuların Türkiye Cumhuriyeti sınırları içerisinde barındırılması ve İdarenin erişimine açık olması,
 - ç) Seri/plaka/id numaralarını U-Net'e kaydetmek koşulu ile kendilerine ait en az 250 adet e-skutere sahip olması,
 - d) Güncel hali esas olmak üzere TS EN ISO 9001, TS EN ISO 14001, TS ISO/IEC 27001, ISO 45001 kalite belgelerine sahip olması,
- şarttır.

(2) Kamu kurum ve kuruluşları ile iştiraklerinden bu maddede belirtilen sermaye şartı aranmaz.

Yetki belgesi verilmesi ve verilen yetki belgesinin iptali

MADDE 9 - (1) Yetki belgesi almak veya yenilemek isteyen gerçek ve tüzel kişiler, 7 nci ve 8 inci maddelerde belirtilen şartların sağlandığını gösteren belgelerle İdareye başvurur.

(2) Yetki belgesi verilirken, verilen izne; iznin veriliş tarihi, geçerlilik süresi, numarası ile belge sahibinin ticaret unvanı, varsa kısa unvanı, adresi, ticaret odası/esnaf odası sicil numarası, bağlı bulunduğu vergi dairesinin adı ve vergi kimlik numarası (gerçek kişilerde T.C. kimlik numarası) ve benzeri bilgiler yazılır.

(3) Her bir gerçek veya tüzel kişiye sadece bir yetki belgesi verilir.

(4) Adi ortaklıklara yetki belgesi verilmez.

(5) İdare tarafından verilecek yetki belgeleri e-Devlet üzerinden düzenlenir.

(6) İdarece, sunulan belgelerin gerçeğe aykırı olduklarının tespiti halinde, gerçek veya tüzel kişilerin yetki belgesi iptal edilir ve faaliyetleri durdurulur.

Paylaşımli e-skuter izni verecek merciler

MADDE 10 - (1) Bu Yönetmelik kapsamında yetki belgesi almış olan gerçek veya tüzel kişilerin, paylaşımli e-skuter faaliyetlerinde kullanacakları e-skuterler için;

a) Büyükşehir belediyesi kurulu bulunan illerde UKOME'den,

b) Büyükşehir belediyesi bulunmayan illerde il trafik komisyonundan,

c) (a) ve (b) bentlerinde belirtilen mercilerin görevli ve yetkili olmadığı ve özel kanunlar ile belirlenmiş alanlarda, kendilerine yetki verilmiş ilgili kurum ve işletmelerden,

izin almaları ve 24 üncü maddenin ikinci fıkrasındaki harcı ödemeleri zorunludur.

Paylaşımli e-skuter izni verilmesine ilişkin esaslar

MADDE 11 - (1) Paylaşımli e-skuter izni verilmesinde, özellikle toplu taşıma hatları ile entegrasyon, arz/talep dengesi ve haksız rekabete ya da piyasada tekelleşmeye mahal verilmemesi hususları esas alınır.

(2) Büyükşehirlerde izin verilecek her bir ilçedeki nüfusun, büyükşehir olmayan yerlerde belediye nüfusunun en fazla 200'de biri kadar olacak şekilde e-skuter izni verilebilir.

(3) Nüfusun mevsimsel veya dönemsel değişiminin kullanım talebini artırması ile kapasite kullanım durumu ve benzeri gerekçelerle ikinci fıkra ile belirlenen sayı %50'ye kadar artırılabilir.

(4) Nüfusu 20.000'in altında olan belediyelerde ikinci fıkra ile belirlenen e-skuter izni sayısı 3 katına kadar artırılabilir.

(5) Her bir yetki belgesi sahibine, ikinci fıkrada belirlenen e-skuter sayısının beşte birini aşmamak kaydıyla e-skuter izni verilir.

(6) Özel kanunlar ile korunan ve yetkili kurum/işletme uhdesindeki alanlarda (havalimanları, üniversite kampüsleri, hastaneler, milli parklar ve benzeri) verilebilecek e-skuter izin sayısı için bu maddede belirtilen sınırlamalar uygulanmaz.

Paylaşımli e-skuter izni verilmesi

MADDE 12 - (1) 11 inci maddedeki esaslar çerçevesinde UKOME ve il trafik komisyonlarınca, sorumluluk sahalarında verilecek e-skuter sayıları, her bir yetki belgesi sahibinin başvuruda bulunabileceği azami e-skuter izni sayısı, e-skuterlerin kullanılmayacağı alanlar, başvuru süreci ve talep edilebilecek diğer şartlara ilişkin karar alınır ve alınan bu karar son başvuru tarihinden en az 10 gün önce ilgili kurumların internet sayfasında duyurulur.

(2) Başvurular büyükşehir belediyesi kurulu bulunan illerde UKOME, büyükşehir belediyesi kurulu bulunmayan yerlerde il trafik komisyonu başkanlığına yapılır. Başvurular her bir belediye için ayrı ayrı değerlendirilir, 60 gün içinde karar alınarak sonuçlandırılır ve duyurulur. Yapılan değerlendirme sonucunda; talep edilen e-skuter izni sayısının, verilebilecek e-skuter izin sayısının;

a) Üstünde olduğu durumlarda, yetki belgesi sahibi başvuru arasında talep ettikleri sayılar ile orantılı olarak eşit şekilde e-skuter izni verilir.

b) Altında olduğu durumlarda, e-skuter izni düzenlenmesini müteakip 6 ay içerisinde ilgisine göre UKOME veya il trafik komisyonlarınca varsa ilave talepler alınır. E-skuter izni alan yetki belgesi sahipleri haricinde yeni talep olmaması durumunda, 11 inci maddenin beşinci fıkrasındaki kısıta bakılmaksızın izin alan yetki belgesi sahiplerinin ilave e-skuter izni talepleri (a) bendinde belirtilen usule göre karşılanır.

(3) Bu maddeye göre alınacak kararlarda;

a) Her bir yetki belgesi sahibi için verilecek e-skuter izni sayısı ile hangi ilçe veya belediyede faaliyet gösterileceğinin,

b) E-skuter izni verilen gerçek veya tüzel kişiliğın yazılı olduğu listenin,

c) İzin verilen e-skuterlerin varsa kullanılmayacağı yasaklı bölgelerin,
ç) E-skuterler için, 25 km/saati aşmamak kaydıyla bölgelere göre belirlenen azami hız sınırının,
belirtilmesi zorunludur.

(4) Özel kanunlar ile korunan ve yetkili kurum/işletme uhdesindeki alanlarda (havalimanları, üniversite kampüsleri, hastaneler, milli parklar ve benzeri) verilebilecek e-skuter izni sayısının tespiti, başvuru süreci ve ilan ile yetki belgesi sahiplerine e-skuter izni verilmesine ilişkin iş ve işlemler, ilgili kurumlar/işletmeler tarafından yürütülür.

(5) Bu maddeye göre alınan kararlar; olumlu ise üçüncü fıkrada belirtilen bilgiler ile birlikte 7 iş günü içerisinde U-Net'e, olumsuz ise 15 iş günü içerisinde gerekçesiyle birlikte yazılı olarak İdareye bildirilir.

(6) UKOME/il trafik komisyonları tarafından verilen paylaşımlı e-skuter izin sayısının, verilebilecek azami sayıya ulaşmadığı durumlarda, her 6 ayda bir yeniden değerlendirme yapılarak e-skuter izni talepleri bu maddeye göre değerlendirilir.

(7) E-skuter izni verilen yetki belgesi sahipleri, bu maddeye göre e-skuter izninin düzenlendiği tarihten itibaren en geç 45 gün içerisinde e-skuterlerini sahada bulundurmamak zorundadır.

Yetki belgesi ve e-skuter izin süresi ile yenilenmesi

MADDE 13 - (1) Bu Yönetmelik kapsamında verilen ve yenilenen yetki belgelerinin süresi 5 yıldır. Ancak süresi bitmeden yenilenen yetki belgeleri için, yetki belgesinde kalan süre, yenilenen belgenin geçerlilik süresine ilave edilir.

(2) 12 nci maddeye göre verilecek e-skuter izin süresi, e-skuter izninin verildiği karar tarihinden itibaren 2 yıldır. Ancak 2 yılın sonunda yeni başvuru olmaması durumunda ve 24 üncü maddenin ikinci fıkrasında belirlenen harcın ödenmesi kaydıyla, bu fıkra ile belirlenmiş süre başka bir işleme gerek kalmaksızın izni veren merci tarafından 1 yıl daha uzatılabilir.

(3) Mevsimsel veya dönemsel nüfus değişikliklerinin olduğu yerlerde ilgili merciler tarafından 2 yıldan daha kısa süreyi kapsayan e-skuter izni verilebilir.

DÖRDÜNCÜ BÖLÜM

Bölünme, Birleşme, Tür Değişikliği ve Hizmet Sözleşmesi

Bölünme, birleşme ve tür değişikliği

MADDE 14 - (1) Tüzel kişiliklerin, bölünmeleri, birleşmeleri ve tür değiştirmeleri halinde aşağıdaki kurallar uygulanır:

a) Yetki belgesi verilmiş bir tüzel kişiliğin 13/1/2011 tarihli ve 6102 sayılı Türk Ticaret Kanununa uygun olarak bölünmesi halinde; tüzel kişiliğe verilmiş yetki belgesi, yeni ortaya çıkan tüzel kişiliklerden sadece birine verilebilir. Bunun için, bölünme sonucunda ortaya çıkan tüzel kişiliklerin, yetki belgesinin verileceği tüzel kişilik lehine noter onaylı muvafakatname vermeleri şarttır. Bu bentle ilgili İdare tarafından ayrıca düzenleme yapılabilir.

b) Yetki belgesi verilmiş veya verilmemiş bir tüzel kişiliğin 6102 sayılı Kanuna uygun olarak aktif ve pasifiyle bir başka yetki belgesi sahibi tüzel kişiyle birleşmesi halinde; bu birleşmeye göre birleşilen tüzel kişilik adına yetki belgesi yeniden verilir.

c) Yetki belgesi verilmiş bir tüzel kişiliğin 6102 sayılı Kanuna uygun olarak tür değiştirmesi halinde; yetki belgesi, yeni ortaya çıkan tüzel kişiliğe verilir.

(2) Bu maddeye göre yapılan/yapılacak işlemler için;

a) Bu Yönetmelikle belirlenmiş tüm şartların sağlanmış olması,

b) Bu Yönetmeliğe göre yetki belgesinin faaliyetinin durdurulmamış olması,
şarttır.

(3) Bu maddeye göre verilecek yetki belgeleri kapsamında daha önce izin alınmış e-skuterler için 24 üncü maddenin ikinci fıkrasına göre ayrıca harç alınmaz.

Hizmet sözleşmesi

MADDE 15 - (1) Bu Yönetmelik kapsamındaki faaliyetlerle ilgili yetki belgesi sahipleri ile hizmetten yararlananlar arasında sözleşme yapılması zorunludur.

(2) Yapılacak sözleşmenin elektronik olarak yapılması ve onaylanması mümkündür.

(3) Bu madde kapsamında yapılacak sözleşmede, yetki belgesi sahibinin adı/unvanı, yetki belgesi numarası, adresi, vergi kimlik numarası (gerçek kişilerde T.C. kimlik numarası), hizmetten yararlanan tarafın adı, soyadı, cinsiyeti, Türk vatandaşı ise T.C. kimlik numarası, Türk vatandaşı değilse uyruğu, pasaport numarası veya varsa yabancı kimlik numarası ile hizmetten yararlanma bedelinin bulunması şarttır.

BEŞİNCİ BÖLÜM

Sorumluluk, Yükümlülük ve Haklar

Yetki belgesi verilenlerin yükümlülükleri

MADDE 16 - (1) Yetki belgesi sahipleri, sadece izin aldıkları belediye/bölge sınırları içerisinde faaliyette bulunabilirler. E-skuterlerin izin alınmayan bir belediye/bölge sınırları içerisinde kullanılması durumunda, söz konusu e-skuterlerin 48 saat içerisinde izin alınan belediye/bölge sınırları içerisine getirilmesi zorunludur.

(2) Yetki belgesi sahipleri, yapacakları faaliyetlerle ilgili olarak, e-skuterlerin seri/plaka/id numaraları ve konum bilgileri ile 15 inci maddenin üçüncü fıkrasında belirtilen bilgileri, verilen hizmetin bitişine kadar U-Net'e işlemek/iletmek zorundadırlar.

(3) Yetki belgesi sahipleri, firmalarında meydana gelen unvan, adres ve sermaye şartını kaybedecek şekilde sermaye azaltışlarını, değişikliğin meydana geldiği tarihten itibaren doksan takvim günü içinde İdareye elektronik olarak bildirmekle yükümlüdürler.

(4) Yetki belgesi sahipleri, 24/4/1930 tarihli ve 1593 sayılı Umumi Hıfzıssıhha Kanununda ön görülen tedbirler, kaideler ve yasaklamalara uygun olarak faaliyette bulunmaktan sorumludurlar. Bu fıkraya aykırılığın tespiti halinde, bu durum ilgili mercilere iletilir.

(5) Yetki belgesi sahipleri, çevreyi ve insan sağlığını koruma, çevre kirliliğini önleme amacıyla yürürlüğe konulan mevzuat hükümlerini bilmek ve faaliyetlerini bunlara uygun olarak yürütmekten sorumludurlar.

(6) Yetki belgesi sahiplerinin, hizmet alanlara ait bilgilerin gizliliği ve güvenliğine ilişkin; her türlü bilgiyi açığa vurmaları, üçüncü kişilere bilgi vermeleri veya herhangi birinin bunları yapmasına neden olmaları yasaktır. Bu fıkraya aykırılığın tespiti halinde, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu hükümleri çerçevesinde ilgili mercilere bilgilendirme yapılır.

(7) Yetki belgesi sahipleri, hizmetten yararlananlara hizmetleriyle ilgili çevrimiçi (mobil/internet) eğitim vermek ve bu eğitimin tamamlanıp tamamlanmadığını kontrol etmekle yükümlüdürler.

(8) Yetki belgesi sahipleri, e-skuterin kullanımı sırasında kask, dizlik, reflektörlü ceket gibi koruyucu ve görünürlüğü artırıcı ekipmanların giyilmesi konusunda hizmetten yararlananları bilgilendirmekle yükümlüdürler.

(9) Yetki belgesi sahipleri, 15 yaşını bitirmemiş olanlara hizmet veremez.

(10) Yetki belgesi sahipleri, UKOME/il veya ilçe trafik komisyonu tarafından belirlenen hız sınırları çerçevesinde e-skuterlerini kullanırlar. Girilmesi yasak bölgeler ve hız limitleri için coğrafi çitleme uygulanır ve coğrafi çitleme verileri U-Net üzerinden İdare ile paylaşılır.

(11) Yetki belgesi sahipleri, faaliyet gösterdikleri il için aldıkları toplam e-skuter izin sayısını aşmamak kaydıyla, faaliyet gösterdikleri ilçede/bölgede izni aldıkları toplam e-skuter sayısının %70'inden az (Kasım-Şubat döneminde %40 olarak uygulanır) %130'undan fazla e-skuter bulunduramazlar. Bu uygulamada e-skuter sayısı kontrolü için 00:00-23:59 saatleri esas alınarak bir tam günlük izleme yapılır.

(12) Yetki belgesi sahipleri, kullanıcılarına 7 gün 24 saat esasına göre hizmet verebilecek kapasitede bir çağrı merkezi veya aynı amaçla hizmet edecek mobil uygulama bulundurmakla yükümlüdürler.

(13) Yetki belgesi sahipleri, kamu nizamını bozacak, özel mülkiyeti ihlal edecek ve yayalar, engelliler ve hareket kısıtlılığı olan kişilerin güvenli ve bağımsız hareketlerini, araç ve yaya trafiğini engelleyecek şekilde park edilen e-skuterlerini iki saat içerisinde toplamakla yükümlüdürler.

(14) Yetki belgesi sahipleri, hizmet verecekleri e-skuterlerin en az % 30'u için, e-skuterlerin Sanayi ve Teknoloji Bakanlığı tarafından yayımlanacak tebliğ ile belirlenecek yerlilik esaslarına uygunluğunu gösteren TSE Uygunluk Belgesi almakla yükümlüdürler.

(15) Yetki belgesi sahipleri, unvan veya varsa kısa unvanlarını ve seri, plaka veya id numaralarından birini izni aldıkları e-skuterlerin en az bir yerine görülebilecek şekilde yazdırmak zorundadırlar.

(16) Yetki belgesi sahipleri, e-skuterlerle ilgili hizmetten yararlananların yapmış oldukları trafik kural ihlallerinin 2918 sayılı Kanun kapsamında işlem yapılacağını kullanıcılara bildirmekle yükümlüdürler.

(17) Yetki belgesi sahipleri, kullanacakları e-skuterleri 5 inci maddenin ikinci fıkrasına uygun olarak teçhiz etmek zorundadırlar.

(18) Yetki belgesi sahipleri, faaliyetleriyle ilgili olarak İdarece yayımlanan düzenleyici işlemlere uymakla yükümlüdürler.

Hizmetten yararlananların hakları

MADDE 17 - (1) Bu Yönetmelik kapsamındaki paylaşımlı e-skuter hizmetinden yararlananların, 7/11/2013 tarihli ve 6502 sayılı Tüketicinin Korunması Hakkında Kanun hükümlerinden doğan hakları saklıdır.

(2) Yetki belgesi verilenler, hizmetten yararlananlara kusursuz hizmet vermek zorundadırlar. Kusursuz hizmet, hizmetten yararlananların hakkıdır.

ALTINCI BÖLÜM

İstatistik ve Bilgi Paylaşımı

İstatistik

MADDE 18 - (1) İdare tarafından, bu Yönetmelik kapsamındaki faaliyetlerin genel seyrinin tespiti ve politika oluşturulması bakımından bu faaliyetlere ilişkin güvenilir verilere dayalı istatistikler oluşturulur.

(2) İdare oluşturduğu istatistikleri gerektiğinde yayımlar.

Bilgi paylaşımı

MADDE 19 - (1) Bu Yönetmelik kapsamındaki faaliyetler, bu faaliyetleri yürüten gerçek ve tüzel kişiler ile kullanılan e-skutere ait İdare tarafından elektronik ortamda tutulan verilerin ilgili kamu idareleriyle; ilgili kamu idarelerince elektronik ortamda tutulan verilerin de ihtiyaç halinde İdare ile paylaşımı esastır.

(2) Talep edilmesi halinde; birinci fıkraya göre İdare tarafından elektronik ortamda tutulan veriler, tâbi olduğu usul ve esaslar ilgili Bakanlıklarca yayımlanan yönetmeliklerle belirlenen ve ilgili kamu idarelerinin denetimine tabi kuruluşlarla; bu kuruluşlarca elektronik ortamda tutulan veriler de İdare ile paylaşılır.

(3) Elektronik ortamda paylaşılan verilerin gizliliğinin korunmasından veriyi alan taraf sorumludur. Bilgi paylaşımına ilişkin usul ve esaslar yapılacak protokollerle belirlenir.

YEDİNCİ BÖLÜM

Denetim ve Tutanaklar

Denetim

MADDE 20 - (1) Yetki belgesi verilenlerin bu Yönetmelik kapsamında yer alan faaliyetleri İdarenin denetimine tâbidir.

(2) İdare yapacağı denetimleri; doğrudan yapabileceği gibi, Kararnamenin 28 inci maddesinin birinci fıkrasının verdiği yetkiye dayanarak bu Yönetmeliğin 21 inci maddesinde belirtilen personel eliyle de yapabilir.

(3) İdare ve yetkili diğer kurum ve kuruluşlar, denetim faaliyetleri sırasında iş birliği içerisinde ve koordineli olarak görev yapar.

(4) Yetki belgesi sahiplerinin, denetim yapmakla görevli/yetkili olanlar tarafından istenilen belgeleri vermesi zorunludur.

(5) Bu Yönetmeliğe göre yapılacak denetimlere ilişkin usul ve esaslar ayrıca belirlenir.

(6) Denetimle ilgili diđer mevzuat hükümleri saklıdır.

Denetimle görevli ve yetkili kuruluşlar

MADDE 21 - (1) Paylaşımli e-skuter işletmeciliđi faaliyeti yapanlar ile bu faaliyetlerden yararlananlar ve bu faaliyetlerde kullanılan her türlü e-skuterlerle ilgili olarak, İdare ile belediye denetim birimleri, bu Yönetmeliđin kendilerine yüklediđi görev ve yetkileri doğrudan yerine getirir ve kullanırlar.

(2) Denetimle görevli ve yetkili kılınanlar, Kararname ile bu Yönetmelik esaslarına göre denetim görevlerini yerine getirmek ve denetimler sırasında tespit ettikleri kusurlar için tutanak düzenlemekle yükümlüdürler.

(3) E-skuterlerin 2918 sayılı Kanun kapsamına giren alanlarda mevzuatta belirtilen kurallara, şartlara, hak ve yükümlülöklere uygun olarak kullanımı hususundaki denetimler Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı kolluk personeline yerine getirilir.

İdari yaptırımlar

MADDE 22 - (1) Bu Yönetmelik hükümlerinin ihlali durumunda, Kararnamenin 28 inci maddesinin birinci fıkrasına göre aşıđıdaki idari para cezaları uygulanır. Buna göre;

a) 6 ncı maddenin üçüncü fıkrasına, 10 uncu maddenin birinci fıkrasına veya 16 ncı maddenin on dördüncü fıkrasına aykırı davrananlara on bin Türk Lirası (10.000 TL),

b) 6 ncı maddenin birinci, ikinci, beşinci veya altıncı fıkralarına, 15 inci maddenin birinci fıkrasına, 16 ncı maddenin birinci, ikinci, üçüncü, yedinci, sekizinci, dokuzuncu, onuncu, on üçüncü, on beşinci, on altıncı, on yedinci veya on sekizinci fıkralarına aykırı davrananlara bin Türk Lirası (1.000 TL),

c) 16 ncı maddenin on birinci fıkrasına aykırı davrananlara, ilk aykırılıkta bin Türk Lirası (1.000 TL), ikinci aykırılıkta on bin Türk Lirası (10.000 TL), üçüncü aykırılıkta elli bin Türk Lirası (50.000 TL),

ç) 16 ncı maddenin on ikinci fıkrasına aykırı davrananlara beş bin Türk Lirası (5.000 TL),

idari para cezası uygulanır. Ayrıca, bu fıkranın (c) bendine göre üçüncü aykırılık nedeniyle idari para cezası verilenlerin yetki belgesi kapsamındaki faaliyetleri 6 ay süreyle geçici olarak durdurulur.

(2) Bu Yönetmelikte belirtilen kusurları işleyenler hakkında, 21 inci maddede belirtilen görevliler tarafından idari para cezası düzenlenir.

(3) Birden fazla kusurun bir arada işlenmesi halinde her kabahat için ayrı idari para cezası karar tutanağı düzenlenir.

(4) E-skuter ile ihlallerde bulunulması halinde, her bir e-skuter için ayrı ayrı idari para cezası uygulanır.

(5) İdari para cezalarına ilişkin diğer hususlarda ilgili mevzuat hükümleri esas alınır.

(6) Bu maddeye göre düzenlenecek tutanaklar, elektronik olarak da düzenlenebilir. Elektronik olarak düzenlenecek tutanıklara ilişkin hususlar, İdare tarafından düzenlenir.

Geçici durdurma ve iptal

MADDE 23 - (1) Bu Yönetmeliğe göre yapılacak geçici durdurma ve iptal işlemleri, geçici durdurma işleminin ilgili yetki belgesi sahibine bildirim tarihini takip eden otuzuncu günde yürürlüğe girer. Bu durum, işlem tesis edilen yetki belgesi kapsamında e-skuter izni veren mercie bildirilir.

SEKİZİNCİ BÖLÜM

Ücretler ve Yeniden Değerleme Oranı

Ücretler

MADDE 24 - (1) İdare tarafından verilecek yetki belgesi için 10.000 TL ücret alınır. Bu ücret, İdarenin döner sermaye işletmesinin ilgili hesaplarına yatırılır.

(2) Bu Yönetmelik kapsamında yetki belgesi almış firmalardan faaliyetlerinde kullanacakları e-skuterler için işgal harcı 2464 sayılı Kanununun 56 ncı maddesinde belirtildiği şekilde, ilgili belediyeye ödenir. Yetki belgesi almış firmalardan bu fıkrada belirtilen harçların konusunu oluşturan hususlarda ayrıca ücret alınmaz.

(3) Yetki belgesi için ödenmiş olan ücretler iade edilmez.

Yeniden değerlendirme oranı

MADDE 25 - (1) 24 üncü maddenin birinci fıkrası ile belirlenen ücretler her yıl, bir önceki yıla ilişkin olarak 213 sayılı Kanun uyarınca tespit ve ilan edilen yeniden değerlendirme oranında, takvim yılı başından geçerli olmak üzere artırılarak uygulanır. Bu Yönetmelik kapsamındaki idari para cezaları ise 30/3/2005 tarihli ve 5326 sayılı Kabahatler Kanununun 17 nci maddesinin yedinci fıkrası hükümlerine göre yeniden değerlemeye tabi tutulur.

DOKUZUNCU BÖLÜM

Çeşitli ve Son Hükümler

Alt düzenleyici işlemler

MADDE 26 - (1) Bu Yönetmelik hükümlerinin uygulanması amacıyla alt düzenleyici işlemler yapılabilir.

Sürelerin başlangıcı, bitişi ve nüfus sayıları

MADDE 27 - (1) Bu Yönetmeliğe göre düzenlenen belgelerde belirtilen geçerlilik tarihleri hariç diğer süreler, işlem tarihini izleyen günden itibaren işlemeye başlar. Tatil günleri sürelere dahildir. Sürenin son gününün tatil gününe rastlaması halinde, süre tatil gününü izleyen ilk iş günü mesai bitimine kadar uzar.

(2) Bu Yönetmelikte belirtilen ve belli bir süre içinde tekrarı halinde idari yaptırım gerektiren fiiller için söz konusu sürenin belirlenmesinde başlangıç tarihi olarak ilk fiilin işlendiği tarih esas alınır.

(3) Bu Yönetmelikle belirlenen nüfus sayılarında, Türkiye İstatistik Kurumu tarafından yayımlanan yıl sonu nüfus sayıları esas alınır.

Bildirim

MADDE 28 - (1) Bu Yönetmeliğe göre idari para cezaları, geçici durdurma ve iptallere ilişkin bildirimler, 11/2/1959 tarihli ve 7201 sayılı Tebligat Kanununa ve ilgili diğer mevzuat hükümlerine göre yapılır.

Paylaşımlı e-skuter izni

GEÇİCİ MADDE 1 - (1) Bu Yönetmeliğin yürürlüğe girdiği tarihten itibaren 60 gün içerisinde 12 nci maddenin birinci fıkrası gereği ilgili kurumların karar alması zorunludur.

Yerlilik oranı

GEÇİCİ MADDE 2 - (1) 16 ncı maddenin on dördüncü fıkrası, 31/12/2024 tarihine kadar uygulanmaz.

Kalite belgesi zorunluluğu

GEÇİCİ MADDE 3 - (1) 1/1/2022 tarihinden önce yapılan yetki belgesi başvurularında, 8 inci maddenin birinci fıkrasının (d) bendinde belirtilen belgelere ilişkin başvuru yapılmış olması ve başvuruya ilişkin belgelerin sunulması kaydıyla söz konusu belgelerin ibraz edilmesi zorunlu değildir.

Muafiyet

GEÇİCİ MADDE 4 - (1) Özel kanunlar ile korunan ve yetkili kurum/işletme uhdesindeki alanlar hariç olmak üzere, bu Yönetmeliğin yürürlüğe girdiği tarihten önce paylaşılımlı e-skuter işletmeciliği yapan

gerçek veya tüzel kişiler, 31/7/2021 tarihine kadar bu Yönetmelik hükümlerinden muaftır. Ancak bu Yönetmelik kapsamında e-skuter izinleri düzenlenen ilçeler/bölgeler için muafiyetler iptal edilir.

Yürürlük

MADDE 29 - (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 30 - (1) Bu Yönetmelik hükümlerini Ulaştırma ve Altyapı, Çevre ve Şehircilik ile İçişleri Bakanları birlikte yürütür.

Yabancı Plakalı Araçlara Verilen Trafik İdari Para Cezalarının Tahsiline İlişkin Yönetmelik

Resmî Gazete Tarihi : 13.02.2018

Resmî Gazete Sayısı : 30331

YABANCI PLAKALI ARAÇLARA VERİLEN TRAFİK İDARİ PARA CEZALARININ TAHSİLİNE İLİŞKİN YÖNETMELİK

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç ve kapsam

MADDE 1 - (1) Bu Yönetmeliğin amacı, sürücüsünün Türk vatandaşı olup olmadığına bakılmaksızın yabancı plakalı araçlara ve Türk plakalı araç kullanan yabancı sürücülere verilen trafik idari para cezalarının tahsiline ilişkin usul ve esasları belirlemektir.

Dayanak

MADDE 2 - (1) Bu Yönetmelik, 13/10/1983 tarihli ve 2918 sayılı Karayolları Trafik Kanununun 115 inci maddesinin sekizinci fıkrasına dayanılarak hazırlanmıştır.

(...)

İKİNCİ BÖLÜM

Genel Hükümler

Trafik idari para cezası

MADDE 4 - (1) Sürücüsünün Türk vatandaşı olup olmadığına bakılmaksızın yabancı plakalı araçlarla 2918 sayılı Kanunda belirtilen hükümlere aykırı hareket edilmesi halinde yetkili personel tarafından, ceza tutanağı düzenlenerek trafik idari para cezası verilir.

(2) Yabancı plakalı araçlarla ilgili olarak 2918 sayılı Kanunun 116 ncı maddesi kapsamında verilen trafik cezaları 30/3/2005 tarihli ve 5326 sayılı Kabahatler Kanununun 26 ncı maddesine göre tebliğ edilir.

(3) Yabancı plakalı araçların;

a) Sürücülerine,

b) 2918 sayılı Kanununun 116 ncı maddesinde sayılan durumlarda araçların tescil plakasına,

düzenlenen ceza tutanaklarına ilişkin bilgiler anında elektronik ortama aktarılır. Emniyet Genel Müdürlüğü ile Gelir İdaresi Başkanlığı bu tutanakların elektronik ortamda sorgulanmasına imkân sağlar.

(4) Emniyet Genel Müdürlüğü trafik idari para cezasına ilişkin tutanakların bilgilerini anlık olarak kesinleşme şartı aranılmadan Gelir İdaresi Başkanlığına aktarır. Aktarılacak olan bilgiler protokolle belirlenir.

(5) Gelir İdaresi Başkanlığına aktarılan bilgiler, alacak kaydı oluşturulmaksızın trafik idari para cezalarının tahsilinde veri olarak kullanılır.

(6) 2918 sayılı Kanununun 116 ncı maddesi kapsamında düzenlenen trafik idari yaptırım kararlarının 5326 sayılı Kanununun 20 nci maddesinin ikinci fıkrasının son cümlesinde yer alan süre içerisinde tebliğ edildiğine ilişkin bilginin Gelir İdaresi Başkanlığına bildirilmemesi halinde, bu trafik cezalarına ilişkin veriler Gelir İdaresi Başkanlığınca Emniyet Genel Müdürlüğüne bildirilerek tahsilat amaçlı olarak tutulan sistem kayıtlarından çıkarılır.

(7) Yabancı plakalı araçlara kesilen trafik cezalarından ilgisine tebliğ edilmiş ve kesinleşmiş olanlar 21/7/1953 tarihli ve 6183 sayılı Amme Alacaklarının Tahsil Usulü Hakkında Kanun kapsamında ilgili vergi dairesince takip edilmek üzere Gelir İdaresi Başkanlığına aktarılır. Bu cezaların takip edilebilmesi için 5326 sayılı Kanununun 25 inci maddesi uyarınca tutanakta yer alması gereken bilgilerin bulunması şarttır.

(...)

Veri paylaşımı

MADDE 6 - (1) Yabancı plakalı araçlara ilişkin Gümrük ve Ticaret Bakanlığında yer alan bilgiler, trafik idari para cezası verilecek olan aracın tespiti amacıyla ilgili kurumlar ile paylaşılır. Paylaşılacak olan bilgiler protokol ile belirlenir.

(2) Muhasebe birimlerince yapılacak olan “yabancı plakalı araçlara ait trafik idari para cezaları” tahsilatları, Gelir İdaresi Başkanlığının veri tabanı üzerinden yapılacak sorgulamalar üzerine gerçekleştirilir.

(3) Yabancı plakalı araçların trafik idari para cezalarına ilişkin veriler elektronik ortamda Maliye Bakanlığı ile Gümrük ve Ticaret Bakanlığı arasında paylaşılır.

(4) Yabancı plakalı araçlarla ilgili olarak kesilen trafik idari para cezalarına karşılık gümrük kapılarında muhasebe birimlerince veya bu birimlere bağlı muhasebe yetkilisi mutemetlerince yapılan tahsilatlar, Muhasebat Genel Müdürlüğünce anında Gelir İdaresi Başkanlığına bildirilir.

(...)

Sistem kayıtlarından çıkarma

GEÇİCİ MADDE 1 - (1) Bu Yönetmeliğin yayımı tarihinden önce yabancı plakalı araçlara uygulanan trafik idari yaptırım karar tutanaklarına ilişkin veriler elektronik ortamda, alacak kaydı oluşturulmaksızın ve trafik idari para cezalarının tahsilinde veri olarak kullanmak üzere, Gelir İdaresi Başkanlığına aktarılır. Bu cezalardan 31/12/2018 tarihi bitimine kadar tahsil edilemeyen ve cezaı veren Kurum tarafından tebliğ edilemeyen trafik cezalarına ilişkin veriler Gelir İdaresi Başkanlığınca Emniyet Genel Müdürlüğüne bildirilerek tahsilat amaçlı olarak tutulan sistem kayıtlarından çıkarılır.

Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanunun Uygulanmasına İlişkin Yönetmelik

Resmî Gazete Tarihi : 22.12.2012

Resmî Gazete Sayısı : 28505

SPORDA ŞİDDET VE DÜZENSİZLİĞİN ÖNLENMESİNE DAİR KANUNUN UYGULANMASINA İLİŞKİN YÖNETMELİK

BİRİNCİ BÖLÜM

Genel Hükümler

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı, 31/3/2011 tarihli ve 6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanunun uygulanmasına ilişkin usul ve esasları düzenlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik; müsabaka öncesinde, esnasında veya sonrasında, spor alanları ile bunların çevresinde, taraftarların sürekli veya geçici olarak gruplar halinde buldukları yerlerde veya müsabakanın yapılacağı yere gidiş ve geliş güzergâhlarında, takımların kamp yaptığı yerlerde uygulanacak güvenlik önlemlerini; il ve ilçe spor güvenlik kurullarının, spor dallarının bağlı bulunduğu federasyonların, spor kulüplerinin, Spor Genel Müdürlüğünün, genel kolluk ve özel güvenlik görevlilerinin, taraftar derneklerinin, taraftardan sorumlu kulüp temsilcilerinin, hakemlerin, basın ve yayın kuruluşları ve diğer ilgili kişi ve kurumların ve müsabaka amirlerinin görev, yetki ve sorumluluklarını; saha içi ve dışında alınacak güvenlik önlemlerini; biletlerin basılması ve satışa sunulmasını, müsabaka alanlarının düzenlenmesini, spor alanlarına giriş ve çıkışlar ile uygulanacak güvenlik sistemlerini, sağlık teşkilatı ve belediyelerin alacağı önlemler ile 6222 sayılı Kanunda öngörülen diğer hususlara ilişkin usul ve esasları kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 31/3/2011 tarihli ve 6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanunun 24 üncü maddesine dayanılarak hazırlanmıştır.

Federasyonların görev, yetki ve sorumlulukları

(...)

MADDE 11 - (1) Federasyonların görev, yetki ve sorumlulukları şunlardır:

a) Milli müsabakalarda, spor müsabakasına seyirci olarak girecek kişilerin kontrolünü yaptırmak, haklarında seyirden yasaklanma tedbiri bulunanların spor alanlarına girişlerini engellemek ve tespit edilenleri genel kolluk kuvvetlerine bildirmek.

b) Elektronik kartlı bilet sistemine geçilen müsabakalarda;

1) Bilet organizasyonu ve seyircilerin müsabaka alanlarına giriş ve çıkışına ilişkin kontrol ve denetimi gerçekleştirmek ve bu amaçla bünyesinde merkezi kontrol sistemi oluşturmak ve kurulacak sistemi kulüplerin hizmetine sunmak.

2) Elektronik kart oluşturmak amacıyla alınacak kişisel bilgileri merkezi veri tabanında tutmak ve bu veri tabanını Maliye Bakanlığı ve İçişleri Bakanlığının erişimine açık tutmak ve veri tabanları arasındaki erişimi sağlamak.

(...)

Biletlerin basılması ve satışa sunulması

MADDE 21 - (1) Biletler, teknik olarak her türlü sahtecilik suçunu önleyecek tedbirler dikkate alınarak, kişinin adı ve soyadı, Türkiye Cumhuriyeti kimlik numarası, koltuk numarası, müsabaka tarihi ve saati, takımların isimleri, tesisin adı ve tribün sırasını içerecek şekilde ait olduğu seyir alanına göre farklı renklerde basılır.

(2) Elektronik kart uygulamasına geçilen spor alanlarında, müsabakada görevli genel kolluk görevlileri haricinde, spor alanlarına giren diğer görevliler elektronik kart ile giriş yaparlar.

(3) Elektronik kart uygulaması ile ilgili olarak aşağıda yer alan usul ve esaslara uyulur:

a) Elektronik kart üzerinde kişilerin adı, soyadı, Türkiye Cumhuriyeti kimlik numarası ve fotoğrafının bulunması zorunludur. (Danıştay Onuncu Dairesinin 30/5/2019 tarihli ve E.:2014/2995; K.:2019/4586 sayılı kararı ile iptal ikinci cümle; Danıştay İDDK'nın 30/11/2020 tarihli E.:2020/131, K.:2020/2779 sayılı Onama kararı ile mezkûr karar kesinleşmiştir.) Bilet organizasyonu ve seyircilerin müsabaka alanlarına giriş ve çıkışına ilişkin kontrol ve denetim yetkisi federasyonlara aittir. Federasyonlar bu amaçla bünyelerinde merkezi kontrol sistemi oluşturur. Elektronik kart oluşturulmak amacıyla alınacak kişisel bilgiler federasyon bünyesinde oluşturulan merkezi veri tabanında tutulur. Bu veri tabanı İçişleri Bakanlığı ve Maliye Bakanlığının erişimine açıktır.

b) Elektronik kart basımı ile bu kart üzerinden satışı gerçekleştirilecek biletlerin satış ve dağıtımına ilişkin yerel uygulamalar kulüpler tarafından, sistem üzerinden merkezi satışları ise ilgili federasyonlar tarafından gerçekleştirilir.

c) Kulüpler, kişisel bilgilerin kullanılmasına ilişkin olarak seyircilerden elektronik ortamda veya yazılı muvafakatlerini alırlar. Muvafakatin içeriğinde kişisel bilgiler ile bağlı bulunan federasyon ve kulüplere ilişkin bilgilerin bulunmasının yanı sıra bu bilgilerin Kanunda belirtilen görev ve yetkilerini yerine getirmesi amacıyla, (Danıştay Onuncu Dairesinin 30/5/2019 tarihli ve E.:2014/2995; K.:2019/4586 sayılı kararı ile iptal ibare; Danıştay İDDK'nın 30/11/2020 tarihli E.:2020/131, K.:2020/2779 sayılı Onama kararı ile mezkûr karar kesinleşmiştir.) kullanılabilmesi ve saklanabileceği hususları yer alır.

ç) (Danıştay Onuncu Dairesinin 30/5/2019 tarihli ve E.:2014/2995; K.:2019/4586 sayılı kararı ile iptal birinci cümle; Danıştay İDDK'nın 30/11/2020 tarihli E.:2020/131, K.:2020/2779 sayılı Onama kararı ile mezkûr karar kesinleşmiştir.) Merkezi pazarlama ve bilet satışından elde edilecek gelirler kulüplere aittir. Federasyon ya da yetki verdiği üçüncü kişiler nezdinde oluşacak bu gelirler kamu kurum ve kuruluşlarına ilişkin alacaklar hariç olmak üzere haczedilemez, devir ve temlik edilemez. Federasyonlar bu fıkra kapsamında belirtilen yetkilerini kısmen veya tamamen üçüncü kişilere devredebilir.

d) Elektronik kart ve merkezi elektronik bilet uygulamasına geçilmiş olan en üst ve bir alt futbol liglerinde fiziksel bilet basım zorunluluğu yoktur.

(4) İlgili federasyon veya kulüp tarafından belirlenen yerler ve görevliler dışında bilet satışı yapılamaz.

(5) Müsabakanın yapılacağı spor alanına tesis kapasitesinin üzerinde seyirci alınmaz ve biletsiz seyirci kabul edilemez.

(6) Spor alanlarında bilet satış noktalarında düzenin sağlanması için özel güvenlik personeli bulundurulur.

(7) En üst ve bir alt futbol liglerinde elektronik kart ve merkezi elektronik bilet uygulamasına geçilinceye kadar ve diğer profesyonel ligler ile Kanunda adı geçen spor dallarının en üst liglerinde, usulüne uygun olarak düzenlenmiş bilet olmaksızın spor alanlarına girilmesi Kanunun 15 inci maddesi kapsamında değerlendirilir.

(...)

Nüfus Hizmetleri Uygulama Yönetmeliđi

Resmî Gazete Tarihi : 09.05.2020

Resmî Gazete Sayısı : 31122

NÜFUS HİZMETLERİ UYGULAMA YÖNETMELİĐİ

BİRİNCİ KISIM

Genel Esaslar

Amaç

MADDE 1- (1) Bu Yönetmeliđin amacı; kişinin doğumundan ölümüne kadar kişisel ve medenî durumuna, uyrukluđuna ve bunlarda meydana gelen deđişikliklere ait doğal ve hukuki olayların belirlenmesinin, bu amaçla düzenlenmiş kütüklere yazılmasının, dış temsilciliklerce ve yetkili kurumlarca nüfus olaylarına ait dayanak belgelerini oluşturan bilgilerin merkezi veri tabanına elektronik ortamda gönderilmesinin veya tescilinin, hizmetlerin yürütülmesinde izlenecek yöntemlerin tespit edilmesinin ve uygulamada birliđin sağlanmasıdır.

Kapsam

MADDE 2- (1) Bu Yönetmelik; nüfus hizmetlerinin yürütülmesine, nüfus kütüklerinin kâğıt ve elektronik ortamda tutulmasına, dış temsilcilikler ve yetkili kurumlarca nüfus olaylarına ait dayanak belgelerini oluşturan bilgilerin merkezi veri tabanına elektronik ortamda gönderilmesi veya tesciline, uluslararası aile cüzdanları ve mavi kartlara ait form ve tutanakların düzenlenmesine, devir ve teslimine ve bu hizmetleri yürüten kamu görevlilerinin denetlenmesine ilişkin usul ve esasları kapsar.

Dayanak

MADDE 3- (1) Bu Yönetmelik, 22/11/2001 tarihli ve 4721 sayılı Türk Medenî Kanunu, 25/4/2006 tarihli ve 5490 sayılı Nüfus Hizmetleri Kanunu ve 29/5/2009 tarihli ve 5901 sayılı Türk Vatandaşlıđı Kanunu hükümleri ile 1 sayılı Cumhurbaşkanlıđı Teşkilatı Hakkında Cumhurbaşkanlıđı Kararnamesinin 258 ve 537 nci maddelerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4- (1) Bu Yönetmelikte geçen;

- a) Aile: Aynı soydan olup, bir aile sıra numarası altında kayıtlı olan kişiler ile onların eş ve çocuklarını,
- b) Aile kütüğü: Nüfus olaylarına ilişkin kayıtların kâğıt veya elektronik ortamda tutulduğu kütüğü,
- c) Aile sıra numarası: Ailelerin aile kütüğüne yazılış sırasına göre verilen numarayı,
- ç) Atık kütük: 1904 yılı öncesinde yapılan nüfus yazımı esas alınarak oluşturulan aile kütüklerini,
- d) Bakanlık: İçişleri Bakanlığını,
- e) Bekârlık hanesi: Kişinin evlenmeden önce nüfusa kayıtlı olduğu haneyi,
- f) Bekârlık soyadı: Kişinin evlenmeden önce taşıdığı soyadını,
- g) Çocuk: On sekiz yaşını tamamlamamış olan kişiyi,
- ğ) Çok vatandaşlık: Kişinin Türk vatandaşlığının yanı sıra bir ya da birden fazla vatandaşlığa sahip olmasını,
- h) Dayanak belgesi: Aile kütüğüne işlenen nüfus olaylarının dayanağı olan form, tutanak, mahkeme kararı, noter senedi, doğum veya ölüm raporu gibi resmî belgeler ile bunların yedeklerini,
- ı) Değerli kâğıtlar: Kimlik kartı, uluslararası aile cüzdanı ve mavi kartı,
- i) Dış temsilcilik: Türkiye Cumhuriyetinin yabancı ülkelerde bulunan büyükelçilik, başkonsolosluk ve konsolosluklarını,
- j) e-Başvuru: Elektronik ortamda e-Devlet kapısı üzerinden ya da elektronik imza ile yapılan başvuruyu,
- k) Elektronik imza: Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi,
- l) Ergin: 4721 sayılı Türk Medenî Kanununa göre ergin olan kişiyi,
- m) Eski aile kütüğü: 1904 yılı sonrasında kullanılan ve yenileme nedeniyle işleminden kaldırılmış olan aile kütüklerini,
- n) Genel Müdür: Nüfus ve Vatandaşlık İşleri Genel Müdürünü,
- o) Genel Müdürlük: Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünü,
- ö) Gün sonu listesi: Her nüfus müdürlüğünün gün sonunda yetkili olduğu aile kütükleri üzerinde; kendileri ile diğer ilçe nüfus müdürlükleri ve yetki verilen kurumlar tarafından yapılan tescil işlemlerini gösteren listeyi,
- p) İdarî birim: Kişilerin kayıtlı buldukları aile kütüklerinin ait olduğu mahalle veya köyü,

- r) İl müdürlüğü: İl nüfus ve vatandaşlık müdürlüğünü,
- s) Kamu görevlisi: Kamusal hizmetlerin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli, süreli veya geçici olarak katılan kişiyi,
- ş) Kanun: 25/4/2006 tarihli ve 5490 sayılı Nüfus Hizmetleri Kanununu,
- t) Kayıt: Aile kütüğüne işlenmiş kişisel durum olaylarına ilişkin bilgilerin ayrı ayrı her birini,
- u) Kayyım: Belirli işleri görmek veya malvarlığını yönetmek için atanan kişiyi,
- ü) Kimlik numarası: Türkiye Cumhuriyeti vatandaşlarının nüfus kayıtları arasında bağ kurmak, kişilerin kaydına ulaşmak ve kamu kuruluşlarında tutulan kayıtlar arasında ilişki sağlamak amacıyla taşıyan numara sistemini,
- v) Kimlik paylaşımı sistemi: Merkezi veri tabanında tutulan kayıtların kurumlar ve kamu hizmeti sunan tüzel kişiler ile paylaşıldığı sistemi,
- y) Kurum: Genel Müdürlük dışındaki diğer kamu kurum ve kuruluşlarını,
- z) Mavi kart: Doğumla Türk vatandaşı olup da çıkma izni almak suretiyle Türk vatandaşlığını kaybedenler ve bunların 5901 sayılı Kanununun 28 inci maddesinde belirtilen altsoylarına verilen ve söz konusu maddede belirtilen haklardan faydalanabileceklerini gösteren resmî belgeyi,
- aa) Merkezî veri tabanı: Genel Müdürlükçe elektronik ortamda tutulan verileri,
- bb) MERNİS: Merkezî Nüfus İdaresi Sistemini,
- cc) Mülkî idare amiri: İlde valiyi, ilçede kaymakamı,
- çç) Nüfus hizmetleri: Nüfus olaylarına ve kişinin nüfusa ve yerleşim yeri adresine ilişkin bilgilerinin toplanmasına, nüfus kütüklerine geçirilmesine, korunmasına ve gerektiğinde tasnif edilerek değerlendirilmesine dair iş ve işlemleri,
- dd) Nüfus kaydı: Aile kütüğüne işlenmiş kişisel bilgileri,
- ee) Nüfus kayıt örneği: Aile kütüğüne işlenmiş kişisel bilgilerin özetlerini gösterir belgeyi,
- ff) Nüfus kütüğü: Aile kütüğü, özel kütük ve yedeklerinden oluşan kayıtların tümünü,
- gg) Nüfus müdürü: İlçe nüfus müdürünü,
- ğğ) Nüfus müdürlüğü: İlçe nüfus müdürlüğünü,
- hh) Nüfus olayı: Doğum, ölüm, evlenme, boşanma, evlât edinme, tanıma, kayıt düzeltme, soybağının düzeltilmesi, gaiplik gibi kişisel durumlarda değişiklik meydana getiren olayı,

- ıı) Özel kütük: Doğum, evlenme, boşanma, ölüm, kayıt düzeltme ve diğer olaylar şeklinde tutulan ve ayrı ayrı tasnif edilen dayanak belgelerinin konulduğu dosyayı,
- ii) Resmî vekil: Vekâletname ile başkası adına işlem tesis etmekle yetkilendirilen kimseyi,
- jj) Saklı nüfus: On sekiz yaşını tamamlayıncaya kadar herhangi bir nedenle aile kütüklerine kayıt edilmemiş olan ve yabancı bir devletle vatandaşlık bağı bulunmayan kişiyi,
- kk) Sağlık kuruluşu: Üniversitelerin sağlık eğitim birimleri ve benzerleri dahil kamu ve tüm özel sağlık kurum ve kuruluşlarını,
- ll) Sistem: MERNİS dışındaki elektronik ortamda tescil ve diğer işlemler için kullanılan sistemleri,
- mm) Uluslararası aile cüzdanı: Bir aileyi oluşturan eş ve çocukların kimlik bilgilerini kapsayan ve uyruğunu kanıtlayan çok dilli resmî belgeyi,
- nn) Vasi: Vesayet altındaki küçüğün veya kısıtlının kişiliği ve malvarlığı ile ilgili bütün menfaatlerini korumak ve hukuki işlemlerde onu temsil etmekle yükümlü kişiyi,
- oo) Vekâletname: Temsil yetkisini kapsayan noterden onaylı belgeyi,
- öö) Veri giriş formu: Nüfus olaylarına ilişkin bilgilerin elektronik ortamda tutulması ve istatistikî bilgilerin elde edilmesi amacıyla MERNİS'e göre hazırlanan formları,
- pp) Vukuat defteri: 1 Eylül 1974 tarihinden önce nüfus olaylarına ilişkin form ve belgelerin tarih sırasına göre kaydedildiği defteri,
- rr) Yabancı: Türkiye Cumhuriyeti Devleti ile vatandaşlık bağı bulunmayan kişiyi,
- ss) Yetkili kurum: Nüfus hizmetlerine ilişkin dayanak bilgilerinin elektronik ortamda merkezi veri tabanına gönderilmesine ve tesciline ilişkin yetki verilen kurumlar ile Bakanlıkça yetki verilmiş diğer kuruluşları,
- ifade eder.

İKİNCİ KISIM

Görev, Yetki ve Sorumluluk

Görev

MADDE 5- (1) Genel Müdürlük; nüfus hizmetlerini düzenlemek, yürütmek, takip etmek, denetlemek ve değerlendirmek, nüfus olaylarının aile kütüklerine tescili esnasında yapılan hatalı veya eksik kayıtları dayanak belgesine göre düzeltmek, değiştirmek, birleştirmek, tamamlamak, mükerrer kayıtları silmek, usulüne göre düzenlenmemiş kayıtlara ilişkin gerekli işlemleri yapmak ve diğer

işlemleri tesis etmek, nüfus hizmetleri ile ilgili olarak kurumlar ve diğer yetkili kuruluşlar arasında koordinasyonu sağlamakla görevlidir.

Yetki

MADDE 6- (1) Genel Müdürlük; nüfus hizmetlerinin yürütülmesi, soybağının kurulması, maddi hataların düzeltilmesi, aile kayıtlarının birleştirilmesi, mükerrer kayıtların birbirine göre tamamlanması ve diğerlerinin silinmesi, kayıtların taşınması, açılması/kapatılması, tamamlanması, nüfus olaylarının aile kütüklerine tescili esnasında yapılan hatalı veya eksik kayıtların dayanak belgesine uygun olarak düzeltilmesi ve usulüne göre tesis edilmemiş kayıtlara ilişkin gerekli işlemlerin yapılması ile saklı nüfus ve aile kütüklerine yapılacak tescil işlemlerine ilişkin usul ve esasların belirlenmesi hususlarında yetkilidir.

Sorumluluk

MADDE 7- (1) Genel Müdürlük, nüfus hizmetlerinin; Anayasaya, kanunlara, Cumhurbaşkanlığı kararnamelerine uygun olarak ve Cumhurbaşkanlığı genel hizmet politikaları doğrultusunda, günün değişen şartlarına göre vatandaş odaklı, etkin, verimli bir şekilde yürütülmesinden ve geliştirilmesinden sorumludur.

ÜÇÜNCÜ KISIM

Nüfus Kütüklerine İlişkin Esaslar

BİRİNCİ BÖLÜM

Özel Kütükler

Özel kütüklerin tutulmasına ilişkin esaslar

MADDE 8- (1) Özel kütükler; doğum, ölüm, evlenme, boşanma, kayıt düzeltme ve diğer kişisel durum değişikliklerine ait dayanak belgelerinin ayrı ayrı tutulduğu kütüklerdir. Özel kütükler; tescilin gerçekleştiği yer nüfus müdürlüğü, dış temsilcilikler ve tescil yetkisi verilen kurumlar tarafından nüfus olayının tesciline dayanak olan belgelerin tarih ve sayı sırasına göre bir araya getirilip yıllar itibarıyla dosyalanmasından oluşur. Bu kütüklerin bir örneği, nüfus olayını tescil eden nüfus müdürlüğünde, dış temsilciliklerde ve tescil yetkisi verilen kurumlarda, bir örneği de Genel Müdürlükte muhafaza edilir.

(2) Nüfus müdürlükleri, dış temsilcilikler ve tescil yetkisi verilen kurumlarca nüfus olaylarının tescil işlemleri sırasında düzenlenen veri giriş formu, ilgili dayanak belgeleri ve ekleri özel kütüğünde muhafaza edilir.

(3) Nüfus olaylarına ait dayanak belgeleri aile kütüklerine tescil edildikten sonra düzenlenen veri giriş formlarının ıslak veya elektronik ortamda onaylanan bir örneği arşivlenmek üzere Genel Müdürlüğe gönderilecek olan özel kütüğe konulur.

(4) Yıl sonunda arşivlenmek üzere Genel Müdürlüğe gönderilecek olan özel kütüklere nüfus olaylarına ait ekler konulmaz. Özel kütüklerin, dış temsilcilikler tarafından gönderilmesine ilişkin usul ve esaslar Dışişleri Bakanlığının görüşü alınarak Genel Müdürlük tarafından belirlenir.

İKİNCİ BÖLÜM

Aile Kütüklerinin Tutulmasına İlişkin Esaslar

Aile esası

MADDE 9- (1) Aynı aileye mensup kişiler bir aile kütük sıra numarası altında kaydedilirler.

(2) Ailenin çocukları, erkeklerin eş ve çocukları ile kadınların evlilik dışı dünyaya gelmiş çocukları, aynı aile sıra numarası altında yazılırlar.

(3) Aile bireylerinden birinin sonradan soyadını değiştirmesi bu haneden çıkarılmasını gerektirmez.

Kapalı kayıtlar üzerinde işlem yapılması

MADDE 10- (1) Kanunun 14 üncü maddesi gereğince kapatılan kayıtlara, kaydın kapatılma tarihinden önce gerçekleşmiş olan nüfus olaylarının tescilinde Genel Müdürlük yetkilidir. Bu yetki valiliklere, kaymakamlıklara ve dış temsilciliklere devredilebilir.

Nüfus kütüklerinin incelenmesi

MADDE 11- (1) Nüfus kütükleri, teftiş ve denetim yetkisi olanlar dışında hiç kimse tarafından görülüp incelenemez ve incelenmek üzere il müdürlüğü, nüfus müdürlüğü, dış temsilcilik ve yetkili kurum dışına çıkarılamaz. Mahkemeler bu hükmün dışındadır.

(2) Mahkemeler tarafından istenmesi halinde, aile kütüğü ve/veya dayanak belgeleri mahkemece görevlendirilen kişiye bir tutanakla teslim edilir. Mahkemece gerekli inceleme yapıldıktan sonra aile kütüğü ve/veya dayanak belgeleri en kısa sürede iade edilir.

(3) Özel kütükten teslim edilen belgelerin asılları iade edilinceye kadar belgelerin bir örneği ve mahkeme talep yazısı ait olduğu özel kütükte muhafaza edilir.

DÖRDÜNCÜ KISIM

Nüfus Olaylarına İlişkin İşlemler

BİRİNCİ BÖLÜM

Soybağına İlişkin Esaslar

Soybağı

MADDE 12- (1) Soybağı; çocuğun soyadının, vatandaşlığının ve aile kütüklerinde yazılacağı yerin belirlenmesinde esas alınır.

(2) Türk Medenî Kanununun 282 nci maddesine göre soybağı; çocuk ile ana arasında doğumla, çocuk ile baba arasında ana ile evlilik, tanıma veya hâkim hükmüyle kurulur. Soybağı ayrıca evlât edinme yoluyla da kurulur.

(3) Soybağının kurulmasına yönelik tescil işlemlerine dair usul ve esaslar Genel Müdürlük tarafından belirlenir.

İKİNCİ BÖLÜM

Doğum

Bildirim süresi

MADDE 13- (1) Sağ olarak doğan çocuğun doğum bildirimini, yurt içinde doğumun gerçekleştiği tarihten itibaren otuz gün içinde, doğumun olduğu yer veya herhangi bir nüfus müdürlüğüne yapılır.

(2) Sağlık kuruluşunda gerçekleşen doğumlara ilişkin bildirimler, doğumu takip eden beş iş günü içinde ve sağlık kuruluşundan ayrılmadan doğumun gerçekleştiği sağlık kuruluşuna da yapılabilir.

(3) Yurt dışında sağ olarak doğan çocuğun doğum bildiriminin, altmış gün içinde dış temsilciliğe yapılması esastır. Ancak doğuma ilişkin bildirim yapılmamış olması halinde yurt içinde herhangi bir nüfus müdürlüğüne de yapılır.

Bildirim yükümlülüğü

MADDE 14- (1) Bildirim; ana, baba, vasi veya kayyım, bunların bulunmaması halinde çocuğun büyük ana, büyük baba veya ergin kardeşleri ya da çocuğu yanında bulunduranlar tarafından, doğumu gösteren resmî belgeye veya sözlü beyana dayalı olarak yapılır.

(2) Evlilik dışında dünyaya gelen çocukların bildirimini ise ana; ananın küçük, kısıtlı, ölmüş veya velayetin kendisinden alınmış olması durumlarında çocuk için atanacak vasi ya da kayyım tarafından veya velayetin babaya verilmesi durumunda baba tarafından yapılır.

(3) Resmî vekiller, çocuğa verilecek adın da belirtildiği vekâletnameyi ibraz etmek suretiyle müvekkilleri adına bildirimde bulunabilirler.

Bildirim şekli ve tescili

MADDE 15- (1) Doğuma ilişkin bildirimler, doğumun gerçekleştiği sağlık kuruluşuna veya resmî belge ile nüfus müdürlüklerine yapılır. Doğum olayı bildirim yapıldığı sağlık kuruluşunca veya nüfus müdürlüğünce usulüne uygun olarak tescil edilir.

(2) Yurt dışında doğuma ilişkin bildirim, resmî belge ile dış temsilciliklere yapılır.

(3) Sağlık personelinin takibi dışında doğan çocukların doğum bildirimini, nüfus müdürlüklerine sözlü beyanla yapılır.

(4) Sözlü beyanla yapılan doğum bildirimlerinde, mülkî idare amirinin talimatı ile il sağlık müdürlüğünce beyanın doğruluğunun araştırılması zorunludur.

a) Araştırma sonucu sözlü doğum bildiriminin doğruluğunun anlaşılması halinde doğum olayı aile kütüğüne tescil edilir.

b) Sözlü doğum bildiriminin araştırma sonucunda doğrulanamaması durumunda, ana ile çocuk arasında; anasının ölü, gaip veya kayıp olması ya da bulunamaması halinde çocuk ile baba arasında soy bağı bulunduğu dair tıbbî rapora göre doğum olayı aile kütüğüne tescil edilir.

ÜÇÜNCÜ BÖLÜM

Yurt Dışındaki Doğumlar

Yurt dışındaki doğumların yurt içinde bildirim ve tescili

MADDE 16- (1) Yurt dışında gerçekleşen doğum olaylarının, herhangi bir nedenle dış temsilciliklere bildirilememesi halinde, doğum belgesinin aslı ile birlikte Türkçe'ye tercüme edilmiş noter tasdikli bir örneği, yurt içinde bulunulan yer nüfus müdürlüğüne verilmek suretiyle bildirim yapılır ve doğum olayı aile kütüklerine tescil edilir.

(2) Doğum belgesinin aynı zamanda kimlik belgesi olarak kullanıldığı beyan edilmesi halinde, aslı ilgisine verilerek Türkçe'ye tercüme edilmiş onaylı bir örneği doğum özel kütüğünde muhafaza edilir.

DÖRDÜNCÜ BÖLÜM

Saklı Nüfus

Başvuru makamı ve işlemler

MADDE 17- (1) On sekiz yaşını tamamlayıncaya kadar herhangi bir nedenle aile kütüklerine kaydedilmemiş olan ve yabancı bir devletle vatandaşlık bağı bulunmayan kişiler; ana veya baba,

bunların ölmüş olması halinde, varsa kardeşleri ile hısımlığını gösterir tıbbî rapor ibraz etmeleri durumunda aile kütüklerine tescil edilerek Türk vatandaşlığını kazanır.

(2) Saklı nüfus oldukları iddiasıyla aile kütüklerine tescil için başvuru makamı illerde valilikler, ilçelerde kaymakamlıklardır.

(3) Saklı nüfusun tespitine ve tesciline ilişkin usul ve esaslar Genel Müdürlük tarafından belirlenir.

BEŞİNCİ BÖLÜM

Nüfus Yazımında Kayıt Dışı Kalanlar

Başvuru makamı

MADDE 18- (1) Nüfus yazımlarında kayıt dışı kalanlar, Türkiye’de buldukları yer nüfus müdürlüğüne veya Genel Müdürlüğe, yurt dışında ise en yakın dış temsilciliğe başvururlar.

Aranacak belgeler

MADDE 19- (1) Nüfus yazımında kayıt dışı kaldıkları iddiasıyla aile kütüklerine tescilini isteyenler, nüfus yazımı tarihinden önce aile kütüklerinde kayıtlı olduklarını ispata yarayacak aşağıdaki belgelerden en az birini ibraz etmekle yükümlüdür:

- a) Nüfus cüzdanı/kimlik kartı veya uluslararası aile cüzdanı.
- b) Türkiye Cumhuriyeti pasaportu.
- c) Askerlik terhis belgesi.
- ç) Yaş, ad ve soybağı gibi kişi hallerine ilişkin olarak verilmiş kesinleşmiş mahkeme kararı.
- d) Genel Müdürlük tarafından verilmiş vatandaşlık kararı.
- e) Nüfus müdürlüklerinden alınmış onaylı nüfus kayıt örneği.
- f) Nüfusa kayıtlı olduğu yer bilgilerini içeren diploma, tasdikname veya benzeri belgeler ile çalışılan kurumlarca verilmiş onaylı kimlik belgeleri.

Aile kütüğüne tescile ilişkin esaslar

MADDE 20- (1) Kayıt dışı kaldığından bahisle müracaat makamlarına başvuran kişi için kayıt dışı kalmış olanların aile kütüklerine geçirilmesine ilişkin “Yazım Dışı/Yersel Nüfus Yazımı Formu” doldurulur. Bildirim formuna 19 uncu maddede sayılan belgelerden ibraz edilenler eklenir ve nüfus yazımından önce kayıtlı olduğu yer nüfus müdürlüğüne gönderilir.

(2) Kişinin nüfus yazımından önce kayıtlı olduğu yer nüfus müdürlüğünce, ibraz edilen belge/belgeler ile Genel Müdürlükten temin edilecek eski kütüklerdeki kaydı incelenir. Mülkî idare amirinin talimatı ile yapılacak inceleme ve araştırma sonucunda, başvuran kişinin nüfus yazımından önce aile kütüklerinde kayıtlı olduğu anlaşılır ise mülkî idare amirinin onayı ile ilgili kişi, ailesinin kaydı varsa aynı aile sıra numarası altında ailesinin yanına, ailesinin kaydı yoksa yeni bir aile sıra numarası altında aile kütüğüne tescil edilir.

BEŞİNCİ KISIM

Çok Vatandaşlığa Sahip Olanlara Ait Nüfus Olaylarının Aile Kütüklerine Tescil Edilmesi

Çok vatandaşlığa sahip olan kişilerin nüfus olaylarının tescili

MADDE 21- (1) Çok vatandaşlığa sahip olan kişilerin, vatandaşlığını taşıdıkları diğer devlet kimliği ile yapmış oldukları kişisel durum değişikliklerinin aile kütüklerine tescil edilebilmesi için;

a) İlgili kişinin veya vekilinin yazılı olarak talepte bulunması, ilgili kişinin ölü olması halinde ise nüfus olayının tescilinde hukuki yararı bulunduğunu belgelendiren kanunî mirasçılarının yazılı olarak talepte bulunması,

b) Tescili istenen olayın Türk hukukuna uygun olarak gerçekleşmesi,

c) Kişinin nüfus kaydında çok vatandaşlığa sahip olduğuna dair açıklama bulunması, zorunludur.

ALTINCI KISIM

Evlenme

Bildirim süresi

MADDE 22- (1) Dış temsilciliklerce ve yetki verilen evlendirme memurluklarınca evlenme bildirimının düzenlenmesine ilişkin bilgiler, on gün içerisinde elektronik ortamda merkezi veri tabanına gönderilir veya tescil edilir.

(2) Yurt içinde evlendirme yetkisi ve görevi verilmiş olanlarca, evlenme bildirimlerinin elektronik ortamda gönderilememesi veya tescil edilememesi halinde evlenmenin yapıldığı tarihten başlayarak on gün içinde düzenlenecek evlenme bildiriminin iki örneği o yerin nüfus müdürlüğüne gönderilir.

(3) Dış temsilciliklerce yapılan evlenmelere ilişkin evlenme bildirimlerinin elektronik ortamda tescil edilememesi halinde düzenlenecek evlenme bildiriminin iki örneği otuz gün içinde, Türk vatandaşı olan kişinin kayıtlı bulunduğu nüfus müdürlüğüne gönderilir.

Kanunî bekleme süresi

MADDE 23- (1) Kadın için üç yüz günlük bekleme süresi, boşanma veya evliliğin iptali kararının kesinleştiği tarihten, kocası ölen kadının bekleme süresi ise kocasının ölüm tarihinden itibaren hüküm ifade eder.

(2) Yabancı kadının milli hukukunda bekleme süresi öngörülüyorsa evlendirme memurluklarınca bu süre göz önüne alınmaz.

Evlenen kadının soyadı

MADDE 24- (1) Evlenen kadın, kocasının soyadını alır. Kocasının soyadı ile birlikte önceki soyadını da kullanmak isteyen kadın, bu isteğini evlenme sırasında yazılı olarak evlendirme memurundan, evlenmeden sonra ise yazılı olarak veya e-başvuru ile nüfus müdürlüğünden talep edebilir.

(2) Eşinin soyadı ile birlikte önceki soyadını da kullanan kadın, sadece eşinin soyadını kullanmak istediğini yazılı olarak veya e-başvuru ile talep ettiği takdirde nüfus müdürlüğünce gerekli işlem yapılır. Bu talepler herhangi bir sayısal sınırlamaya tâbi değildir.

(3) Evlenmeden önce iki soyadı taşıyan kadın, bu soyadlarından sadece birinden yararlanabilir.

Yabancı makamlar önünde yapılan evlenmelerde bildirim yükümlülüğü ve tescili

MADDE 25- (1) Evlenme bildirimiminin, yabancı makamlardan alınmış belgeye göre dış temsilciliklere yapılması halinde dış temsilciliklerce iki örnek evlenme bildirimini düzenlenir ve evlenme olayı sistem üzerinden tescil edilir.

(2) Yurt dışında gerçekleşen evlenmenin herhangi bir nedenle dış temsilciliklere bildirilememesi halinde, evlenme bildirimini; yabancı makamlardan alınan usulüne göre onaylanmış evlenme belgesinin aslı ile birlikte Türkçe'ye tercüme edilmiş noter tasdikli birer örneği yurt içinde bulunan yer nüfus müdürlüğüne verilmek suretiyle yapılır.

(3) Yabancı devlet makamlarınca düzenlenen evlenme belgesinin aynı zamanda kimlik belgesi olarak kullanıldığının beyan edilmesi halinde, aslı ilgisine verilerek onaylı bir örneği evlenme özel kütüğünde muhafaza edilir.

(4) Evlenmenin tescili sırasında veya sonrasında, evlenme belgesinde, yabancı uyruklu kadının veya erkeğin kimlik bilgilerinin eksik olduğunun veya çeviriden kaynaklanan maddi hataların bulunduğu tespit edildiğinde, kişilerin uyruğunda bulunduğu devletin yetkili makamlarınca verilmiş ve usulüne göre onaylanmış belgenin aslı ile Türkçe'ye tercüme edilmiş noter tasdikli bir

örneğin ibrazı durumunda Genel Müdürlük tarafından eksik olan bilgiler tamamlanır veya maddi hatalar düzeltilir. Genel Müdürlük bu yetkisini devredebilir.

Cumhuriyet başsavcılığına bildirilecek evlenmeler

MADDE 26- (1) Nüfus müdürlüğüne gönderilen evlenme bildirimleri üzerinde yapılan inceleme sonucunda; evlenmenin kanunen yetkili kılınmış memurlarca yapılmadığının anlaşılması, aile kütüklerindeki kayıtlara göre karı veya kocadan birinin başkasıyla evli olduğunun tespit edilmesi veya karı ve koca arasında Türk Medenî Kanununun 129 uncu maddesinde belirtildiği şekilde evlenmeye mani derecede kan ya da kayın hısımlığının bulunması hallerinde, evlenme aile kütüğüne tescil edilerek bu durum Cumhuriyet başsavcılığına bildirilir.

(2) Eşlerden birinin sürekli bir sebeple ayırt etme gücünden yoksun olduğunun ya da evlenmeye engel olacak derecede akıl hastalığının bulunduğu ihbar edilmesi ve belgelendirilmesi halinde, evlenme aile kütüklerine tescil edilerek bu durum Cumhuriyet başsavcılığına bildirilir.

YEDİNCİ KISIM

Boşanma ve Boşanmanın İptali

Boşanma tarihi

MADDE 27- (1) Boşanma tarihi, boşanma kararının kesinleştiği tarihtir. Yabancı ülke adlî veya idarî makamlarınca verilen boşanma kararlarına yönelik Türk mahkemelerince tanıma/tenfiz kararı verilmesi ya da Kanunun 27/A maddesine göre yetkili kurumlar tarafından aile kütüklerine tesciline karar verilmiş olması halinde, yabancı ülke adlî veya idarî makamlarınca verilen kararın kesinleşme tarihi, boşanma tarihi olarak aile kütüklerine tescil edilir.

Boşanan kadının soyadı ve hanesi

MADDE 28- (1) Boşanan kadının koca hanesindeki kaydı kapatılarak, bu evlenmeden önce kayıtlı bulunduğu hanedeki nüfus kaydı açılır.

(2) Dul olarak evlenen kadının boşanması sırasında bekârlık soyadını taşımasına mahkemece izin verilmiş ise kadın, bekârlık soyadını alarak bekârlık hanesindeki nüfus kaydı açılır.

(3) Hâkim, boşanan kadının kocasının soyadını kullanmasına izin vermiş ise kadın, bu evlenmeden önce kayıtlı bulunduğu haneye, izin verilen koca soyadı ile döner ve nüfus kaydı açılır.

(4) Dul olarak evlenen ve boşanarak önceki hanesine dönen kadın, yazılı olarak veya e-başvuru ile talep etmesi halinde kapanmış olan nüfus kaydı açılarak bekârlık hanesine bekârlık soyadı ile döner.

(5) Boşandıđı eşinin soyadını kullanmasına izin verilen kadın, evlenmeden önceki soyadıyla eşinin soyadını birlikte kullanmak istediđini yazılı olarak veya e-başvuru ile talep etmesi halinde nüfus müdürlüğüne gerekli işlem yapılır.

(6) Boşandıđı eşinin soyadını kullanmasına izin verilen kadın, evlenmeden önceki soyadını kullanmak istediđini yazılı olarak veya e-başvuru ile talep etmesi halinde nüfus müdürlüğüne gerekli işlem yapılır.

(7) Kocasını ile birlikte Türk vatandaşlığını kazanan ya da Türk vatandaşı ile evlenmesi nedeniyle Türk vatandaşlığını kazanıp kocasının kütüğüne kocasının soyadı ile tescil edilen kadın boşandıđı takdirde; bulunduğu yere ait aile kütüğünün son aile sıra numarasından sonra yeni bir aile sıra numarası altında, boşanma kararında belirtilen soyadıyla tescil edilir. Boşanma kararında soyadı belirtilmemiş ya da boşanma kararı yabancı yetkili mahkemeler tarafından verilmiş ve Türkiye'de tanınmış veya tenfiz kararına bağlanmış ya da Kanununun 27/A maddesine göre aile kütüklerine tesciline karar verilmiş ise kadın, evlenmeden önceki soyadı ile tescil edilir. Ancak evlenmeden önceki soyadının tespit edilememesi ve boşanan kadının başvurusu sağlanamadığı takdirde bulunduğu yer mülkî idare amirince soyadı verilir.

Boşanmanın iptali kararları

MADDE 29- (1) Boşanmanın iptaline ilişkin verilen kararlar, ilgililerin kayıtlarına tescil edilir ve kayıtları boşanmadan önceki haline getirilir.

SEKİZİNCİ KISIM

Kayıt Düzeltme

BİRİNCİ BÖLÜM

Kayıt Düzeltme Davalarında Yetki ve Temsil

Dava açma yetkisi

MADDE 30- (1) Nüfus kayıtlarına ilişkin düzeltme davaları, düzeltmeyi isteyen şahıslar ile ilgili resmî kurumun göstereceđi lüzum üzerine Cumhuriyet savcılarını tarafından yerleşim yeri adresinin bulunduğu yerdeki görevli asliye hukuk mahkemesinde açılır.

(2) Haklı sebeplerin bulunması halinde aynı konuya ilişkin nüfus kaydında düzeltme yapılması hâkimden istenebilir.

(3) Tespit davaları, kaydın iptali veya düzeltilmesi için açılacak davalara karine teşkil eder.

(4) Babalık veya babalığın tespiti davası adı altında açılan davalar sonucunda alınan kararlar, hukuki niteliği itibari ile değerlendirilmesinin ardından aile kütüklerine tescil edilir.

Nüfus müdürlüklerinin mahkemede temsili

MADDE 31- (1) Kayıt düzeltme davalarında veya ceza mahkemelerinde görülmekte olan davaların yaş düzeltme aşamasında nüfus müdürü veya görevlendireceği memur, nüfus müdürlüğünü temsilen taraf olarak bulunur. Kayıt düzeltme davaları nüfus müdürü veya görevlendireceği memur huzurunda görülür ve karara bağlanır.

(2) Nüfus müdürü veya görevlendirilen nüfus temsilcisi, düzeltme isteğinin mevzuata uygun olup olmadığını mahkemeye yazılı olarak bildirmekle veya duruşma sırasında tutanağa geçirilmek üzere beyanda bulunmakla yükümlüdür.

(3) Kayıt düzeltme davalarında gerekli görülmesi halinde valilik tarafından nüfus müdürlüğünü temsilen avukat görevlendirilebilir.

Dava takip dosyası

MADDE 32- (1) Nüfus müdürlüklerinin taraf olarak bulunduğu her dava için davaya katılan nüfus müdürü veya nüfus temsilcisi tarafından davanın safahatına ilişkin bir dava takip dosyası tutulur. Kesinleşen kararlara ait dava takip dosyaları işlemde kaldırılır.

İKİNCİ BÖLÜM

Mahkemelerce Verilen Kayıt Düzeltme Kararlarının Tesciline İlişkin Esaslar

Yanlılıkla kesinleşen mahkeme kararları

MADDE 33- (1) Sehven kesinleşme şerhi verilen kararlara dayanılarak tescil edilen nüfus olaylarının, sonradan kesinleşmediğinin ilgili mahkemece yazı veya ara karar ile bildirilmesi halinde, idarece geri alma işlemi yapılarak kayıtlar eski haline getirilir.

Mahkemelerce verilen kayıt düzeltme kararlarının tesciline ilişkin esaslar

MADDE 34- (1) Kayıt düzeltme kararlarının aile kütüklerine tesciline ilişkin esaslar aşağıda belirtilmiştir:

a) Soyadının düzeltilmesine karar verilen erkek ise kendisinin, varsa karısının ve karar tarihinde ergin olmayan çocuklarının soyadları düzeltilir. Soyadının düzeltilmesine karar verilen kadın ise kendisinin ve varsa karar tarihinde ergin olmayan evlilik dışı doğmuş çocuklarının soyadları düzeltilir.

b) Adının düzeltilmesine karar verilen kişinin çocukları var ise mahkeme kararında bu işleme ilişkin herhangi bir hüküm aranmaksızın çocukların kaydındaki ana veya baba adları da düzeltilir. Baba veya ana adının düzeltilmesinden önce yer değiştirme, evlenme, evlât edinme gibi nedenlerle bu haneden gitmiş olan ergin çocukların açık kayıtlarında da gerekli düzeltme işlemi yapılır.

c) Doğum tarihinin düzeltilmesine ilişkin mahkeme kararında, sadece yılın düzeltilmesine karar verilmesi halinde doğum tarihi, aile kütüğündeki ay ve gün değiştirilmeksizin düzeltilen doğum yılı ile tescil edilir.

ç) Kapalı nüfus kayıtlarına yönelik kaydın kapatılma tarihinden sonra mahkemeler tarafından verilen kesinleşmiş kayıt düzeltme kararları aile kütüklerine tescil edilir. 12/1/2011 tarihli ve 6100 sayılı Hukuk Muhakemeleri Kanununun 363 üncü maddesi gereğince Cumhuriyet başsavcılığına bildirilir.

DOKUZUNCU KISIM

Ölüm

BİRİNCİ BÖLÜM

Ölüm Bildirimi

Ölüm bildirimi ve tescili

MADDE 35- (1) Yurt içinde meydana gelen ölüm olayları kurumlar ve yetkililer tarafından nüfus müdürlüğüne on gün içinde bildirilir.

(2) Ölüm bildiriminin düzenlenmesine ilişkin bilgiler, Sağlık Bakanlığı veya dış temsilcilikler tarafından on gün içerisinde elektronik ortamda merkezi veri tabanına gönderilir veya tescil edilir.

Yurt dışındaki ölümler

MADDE 36- (1) Yurt dışında buldukları sırada ölen Türk vatandaşlarının ölüm olayı, ilgili yerel makamlardan alınan belgenin dış temsilciliğe verilmesi suretiyle bildirilir. Ölüm bildirim formuna dayanak belgesine ilişkin açıklama yapılır ve dış temsilciliklerce sistem üzerinden tescil işlemi gerçekleştirilir.

(2) Dış temsilciliklerce tescil işleminin sistem üzerinden yapılamaması durumunda; iki örnek ölüm bildirim formu düzenlenir ve ölenin nüfus cüzdanı/kimlik kartı eklenerek ölüm olayının tescil edilmesi için ölüm belgesinin dış temsilciliğe intikal ettirildiği tarihten itibaren on gün içerisinde kişinin aile kütüğünde kayıtlı olduğu yer nüfus müdürlüğüne gönderilir.

Ölü olduğu halde aile kütüğünde sağ görünenler

MADDE 37- (1) Ölmüş olduğu halde aile kütüklerinde sağ görünenlerin ölüm olayını gösterir belge ile başvurulması halinde nüfus müdürlüklerince gerekli işlem yapılır.

(2) Ölüm olayını gösterir herhangi bir belge ibraz edilememesi durumunda ya da aile kütükleri üzerinde yapılan inceleme sonucunda; nüfus cüzdanı/kimlik kartı aldığına ilişkin bir bilgi olmayan, adres kaydı bulunmayan, uzun süredir işlem görmediği anlaşılan ve yaşı itibarıyla ölü olması muhtemel kişilerin ölü olup olmadıkları araştırılır. Araştırma sonucu ölü oldukları tespit edilenlerin ölüm olayı mülkî idare amirinin onayı ile tescil edilir.

(3) Ölü olduğu değerlendirilen fakat aile kütüğünde sağ görünenler hakkında yapılan araştırma sonucu ölüm tarihi ve yeri tespit edilemeyenlerin ve fiilen idarece araştırma imkânı kalmadığı tespit edilen kayıtların, işlem yapılamaz hale getirilmesinde Genel Müdürlük yetkilidir.

Nüfusta kayıtlı olmayanların ölümü

MADDE 38- (1) Aile kütüğünde kaydı bulunmayan kişinin ölümüne ilişkin resmî/özel sağlık kurumları veya kamu kurum ve kuruluşlarının kayıtlarına dayanılarak düzenlenen ölüm bildirim formlarında yer alan bilgilere göre ölen kişinin önce doğum olayı, sonra da ölüm olayı aile kütüğüne tescil edilir.

(2) Nüfusta kayıtlı olmayanların ölüm olaylarının tesciline ilişkin usul ve esaslar Genel Müdürlük tarafından belirlenir.

İKİNCİ BÖLÜM

Ölüm Karinesi ve Gaiplik

Ölüm karinesi

MADDE 39- (1) Bir kimse, ölümüne kesin gözle bakmayı gerektiren durumlar içinde ortadan kaybolursa, cesedi bulunamamış olsa bile kişinin alt veya üst soyundan bir kişinin ya da kardeşlerinin, bunlar yoksa mirasçılarının yazılı başvurusu üzerine olaya ilişkin resmî belgelerin ibraz edilmesi ya da yetkili makamların durumu resmî yazı ile nüfus müdürlüğüne bildirmeleri halinde mülkî idare amirinin onayı ile aile kütüğüne ölüm olayı tescil edilir.

Gaiplik

MADDE 40- (1) Ölüm tehlikesi içinde kaybolan veya kendisinden uzun zamandan beri haber alınamayan bir kimsenin ölümü hakkında kuvvetli olasılık varsa, hakları bu ölüme bağlı olanların başvurusu üzerine mahkeme bu kişinin gaipliğine karar verebilir.

(2) Mahkeme tarafından verilen gaiplik kararı ilgili kişinin kaydına tescil edilir. Gaiplik, ölümün hukuki sonuçlarını doğurur.

(3) Gaipliğine karar verilen kişinin eşi, mahkemece evliliğin feshine karar verilmedikçe yeniden evlenemez.

ONUNCU KISIM

Diğer Kişisel Durum Kütüğüne İlişkin İşlemler

BİRİNCİ BÖLÜM

Maddi Hata ve Tamamlama

Maddi hata

MADDE 41- (1) Aile kütüklerine tescil edilmesi gereken bilgilerden; dayanak belgesinde bulunduğu halde nüfus kütüklerine hatalı veya eksik olarak tescil edilen ya da hiç yazılmayan bilgiler veya mükerrer kayıtlar maddi hata kapsamında değerlendirilir. Bu tür maddi hatalar Genel Müdürlük ya da dayanak belgesinin bulunduğu nüfus müdürlükleri tarafından düzeltilir.

(2) Dayanak belgelerindeki bilgilerin aile kütüklerine işlenmesi sırasında yapılmış bir maddi hata söz konusu değil ise aile kütüğünün herhangi bir kaydında düzeltme veya değişiklik, mahkeme kararı ile yapılır.

(3) Genel Müdürlük tarafından gerekli görülmesi halinde, dış temsilciliklere kendi yaptıkları iş ve işlemlerle sınırlı olarak maddi hataları düzeltme yetkisi verilebilir.

Tamamlama

MADDE 42- (1) Tamamlama; aile kütüklerine eksik olarak tescil edilen ya da hiç yazılmayan kişisel duruma ilişkin bilgilerin, Genel Müdürlük veya nüfus müdürlüğünce dayanak belgesine uygun şekilde tescil edilmesine ilişkin işlemdir.

Geri alma işlemi

MADDE 43- (1) Geri alma işlemi; nüfus olaylarının veya mahkeme kararlarının ilgili kişi yerine başka kişi üzerine tescil edilmesi, henüz kesinleşmemiş mahkeme kararlarının veya gerçekleşmemiş bir evliliğin aile kütüklerine sehven tescil edilmesi nedeniyle, hatalı yapılan idarî işlemin alınan idarî bir karar ile hükümsüz hale getirilmesidir. Bu olaylar dışında kalan işlemlerde geri alma işlemi yapılamaz.

(2) Geri alma işlemi tescili gerçekleştiren nüfus müdürlüğünce yapılır.

(3) Nüfus müdürlüklerince herhangi bir nedenle geri alma işlemi yapılamaması halinde bu işlem Genel Müdürlük tarafından yapılır.

(4) Genel Müdürlük tarafından yetki verilmesi halinde, geri alma işlemi tescili gerçekleştiren dış temsilciliklerce yapılabilir.

İKİNCİ BÖLÜM

Nüfus Kaydının İptali

Dayanak belgesi olmadan tescil edilen kaydın iptali

MADDE 44- (1) Aile kütüklerine tescil edilen bir kaydın, hukuken geçerli bir belgeye dayalı olmadan tescil edildiği hususunda şüpheye düşülmesi halinde; doğum, yer değiştirme ve diğer kişisel durum değişiklikleri özel kütükleri, doğum, yer değiştirme veya diğer vukuat defterleri incelenerek ilgilinin başka bir haneden naklen gelip gelmediği, doğum, yeniden kayıt ya da yersel yazım suretiyle tescil edilip edilmediği araştırılır. Araştırma sonucunda;

a) İlgilinin doğum, yeniden kayıt veya yersel yazım nedeniyle tescil edildiği ya da başka bir haneden naklen geldiğinin anlaşılması halinde, önceki kaydı ile bağ kurularak kimlik numaraları eşleştirilir. İdarece kayıt düzeltme veya tamamlamaya ilişkin form düzenlenerek, kayıtlara gerekli açıklamalar yapılır.

b) Nüfus kaydının veya nüfus olayının usulüne göre düzenlenmiş bir belgeye dayanılarak tescil edilmediğinin tespit edilmesi halinde, kaydın iptali için durum Cumhuriyet başsavcılığına bildirilir. Dava sonuçlanıncaya kadar Genel Müdürlük tarafından nüfus kaydı işlem yapılamaz hale getirilir.

Mükerrer kaydın iptali

MADDE 45- (1) Mükerrer kayıt; aynı ya da farklı dayanak belgeleri ile kişinin aile kütüklerine birden fazla kaydının yapılmış olmasıdır.

(2) Mükerrer olarak yapılan kayıtların iptal edilmesine; Genel Müdürlük, nüfus müdürlükleri veya mahkemeler yetkilidir.

(3) Nüfus müdürlükleri tarafından mükerrer kayıt iptallerinde kayıt sahibinin ve yakınlarının ifadelerine başvurulur. Kayıtların tesciline esas dayanak belgeleri ve ifadeler doğrultusunda kayıtların aynı kişiye ait olduğunun tespit edilmesi halinde, mükerrer kayıt üzerindeki nüfus olayları kişinin işlem gören kaydına taşındıktan sonra mükerrer olan diğer kayıt mülkî idare amirinin onayı ile iptal edilir.

ON BİRİNCİ KISIM

Tescil Edilmiş Nüfus Olaylarının İptal Edilmesi Halinde Usul

Evliliğin feshi veya iptal edilmesi

MADDE 46- (1) Evliliğin feshi veya iptali, mahkeme kararı ile evliliğin sona erdirilmesidir.

(2) Evliliğin feshi veya iptali tarihi, kararın kesinleştiği tarihtir. Yabancı mahkemeler tarafından verilen evliliğin feshi veya iptali kararlarının Türk mahkemelerince tanıma veya tenfiz kararı verilmesi ya da Kanununun 27/A maddesine göre yetkili kurumlar tarafından aile kütüklerine tesciline karar verilmiş olması halinde, yabancı ülke adli veya idarî makamlarınca verilen kararın kesinleşme tarihi, evliliğin feshi veya iptali tarihi olarak kabul edilir.

(3) Evliliği fesh veya iptal edilen kadının, koca hanesindeki kaydı kapatılıp önceki soyadı verilerek bu evlenmeden önce kayıtlı bulunduğu hanedeki nüfus kaydı açılır.

ON İKİNCİ KISIM

Uluslararası Aile Cüzdanı ve Mavi Kart

Değerli kâğıt türleri

MADDE 47- (1) Uluslararası aile cüzdanı ve mavi kart 21/02/1963 tarihli ve 210 sayılı Değerli Kâğıtlar Kanununa ekli değerli kâğıtlar tablosunda yer almaktadır.

Uluslararası Aile Cüzdanı basımı ve dağıtımı

MADDE 48- (1) Uluslararası aile cüzdanlarının şekil, ebat ve içeriğinde yer alacak bilgileri belirlemeye Bakanlık yetkilidir.

(2) Uluslararası aile cüzdanlarının düzenlenmesine ilişkin usul ve esaslar Genel Müdürlük tarafından belirlenir.

(3) Uluslararası aile cüzdanları Bakanlıkça tespit edilen şekil, ebat ve örneğine uygun olarak Hazine ve Maliye Bakanlığınca bastırılır ve nüfus müdürlüklerinin ihtiyaçlarını karşılamak üzere muhasebe yetkililerine, dış temsilciliklerin ihtiyaçlarını karşılamak üzere de Dışişleri Bakanlığına gönderilir.

Mavi kart düzenlenmesi

MADDE 49- (1) Mavi kart, doğumla Türk vatandaşı olup da çıkma izni almak suretiyle Türk vatandaşlığını kaybedenlere ve bunların Türk Vatandaşlığı Kanununun 28 inci maddesinde belirtilen alt soylarına nüfus müdürlükleri tarafından düzenlenir.

ON ÜÇÜNCÜ KISIM

Nüfus Kayıtları

Nüfus kayıt örneği verilmesi

MADDE 50- (1) Gerçek kişiler, Genel Müdürlük tarafından belirlenen usul ve esaslar çerçevesinde ve güvenli kimlik doğrulama araçlarını kullanarak e-Devlet kapısı üzerinden kendileri ve alt ve üst soyları ile ilgili nüfus kayıt örneklerini sorgulayabilir. Elde edilen belgeler ilgili kurum, kuruluşlar veya tüzel kişilere verilebilir. e-Devlet kapısı üzerinden alınan belgeler, nüfus müdürlüklerinden alınmış resmî belgeler ile aynı hukuki değere sahiptir.

(2) Kişi, kurum ve kuruluşların nüfus kayıt örneği taleplerinde aşağıdaki hususlar göz önünde bulundurulur:

a) Nüfus kayıt örneklerinde, kimlik bilgileri dışında kişisel bilgilere ve nüfus olaylarına ilişkin açıklamalara yer verilmez. Ancak bunları istemeye yetkili olanlar tarafından, istenme nedeni açıkça belirtilerek talep edilmesi halinde nüfus kayıt örneklerinde kişisel bilgilere ve nüfus olaylarına ilişkin açıklamalara da yer verilebilir.

b) Türk Medenî Kanununun 314 üncü maddesi gereğince mahkeme kararı olmadıkça ya da evlâtlık istemedikçe nüfus kayıt örneklerinde evlât edinme ile ilgili açıklamalara yer verilmez.

(3) Kimlik Paylaşımı Sistemi üzerinden nüfus kayıt örneğine erişebilen kurum ve tüzel kişiler bu belgeleri ilgisinden veya nüfus müdürlüğünden talep etmeksizin Kimlik Paylaşımı Sisteminden temin ederler ya da e-Devlet kapısı üzerinden temin edilen nüfus kayıt örnekleri ile işlem yaparlar.

(4) Mahkemeler tarafından istenen nüfus kayıt örneklerinde, aile kütüğünün düşünceler alanındaki açıklamaların tamamına yer verilir.

Yabancı ülkelerde kullanılacak kayıt örnekleri

MADDE 51- (1) Milletlerarası Ahval-i Şahsiye Komisyonuna üye ve ilgili sözleşmelerine taraf devlet makamlarına ibraz edilecek doğum, ölüm, evlenme, evlenme ehliyet belgesi ve nüfus kayıt örneği gibi bu amaçla bastırılmış veya elektronik ortamda hazırlanmış çok dilli belgelerde, imza ve mühür taşıması şartı ile herhangi bir tasdik aranmaz.

(2) Doğum, ölüm, evlenme, evlenme ehliyet belgesi ve nüfus kayıt örneği gibi belgeler, La Haye Devletler Özel Hukuk Konferansına üye ve 5/10/1961 tarihli Yabancı Resmî Belgelerin Tasdiki Mecburiyetinin Kaldırılması Sözleşmesine taraf devlet makamlarına verilecek ise tasdik şerhi (Apostille) işlemi ilgili kişilerce yaptırılır.

(3) Kişilerin yabancı ülke makamlarına vermek üzere talep ettiği nüfus kayıt örneklerinde, kimlik bilgileri dışında kişisel bilgilere ve nüfus olaylarına ilişkin açıklamalara kişinin talebi olmaksızın yer verilmez.

Bilgi ve belge istenmesi

MADDE 52- (1) Türkiye'nin taraf olduğu uluslararası sözleşme hükümleri saklı kalmak üzere, yabancı devlet makamları veya temsilcilikleri; karşılıklılık ilkesi çerçevesinde, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununun 9 uncu maddesi gereğince ve kullanım amacı belirtilmek suretiyle Dışişleri Bakanlığı kanalı ile nüfus olayları ve nüfus kayıtları hakkında bilgi ve belge isteyebilirler.

(2) Uluslararası niteliği bulunmayan ve nüfus kayıtlarındaki bilgilerin tümünü veya bir kısmını ya da aile kütüklerine tescil edilen kayıtların dayanağını teşkil eden belgelerin örneklerinin, yabancı makamlara verilmek üzere ilgili kişi tarafından yazılı olarak talep edilmesi ve mülkî idare amirinin uygun görmesi halinde usulüne göre tasdik edildikten sonra ilgisine verilir.

ON DÖRDÜNCÜ KISIM

Diğer İşlemler

Tescil yetkisi ve görevlendirme

MADDE 53- (1) Bakanlık, dış temsilciliklere veya nüfus olaylarına ilişkin dayanak belgesi düzenleyen kurumlara, bu belgeleri elektronik ortamda gönderme ya da tescil yetkisi verebilir.

(2) Dış temsilcilikler ve yetki verilen kurumlarca, elektronik ortamda gönderilecek veya MERNİS'e doğrudan tescil edilecek nüfus olaylarına ilişkin bilgileri belirlemeye Genel Müdürlük yetkilidir.

(3) Nüfus olaylarına ilişkin bilgileri merkezi veri tabanına, gönderme veya tescili talebinde bulunan kurumlar ile Genel Müdürlük arasında protokol yapılır. Bu protokol; nüfus olaylarına ilişkin bilgileri merkezi veri tabanına gönderme, tescil, sorumluluk, gizlilik, güvenlik, muhafaza, bilgilere erişim, bilgilerin paylaşımı ve süreler ile diğer hususları kapsar.

(4) Nüfus olaylarını aile kütüklerine tescil etmekle görevli olan ve Kanuna aykırı hareket eden kamu görevlileri hakkında 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun kamu idaresinin güvenilirliğine ve işleyişine ile kamu güvenine karşı suçlara ilişkin hükümlerine göre işlem yapılır.

Tescil görevi ve süre

MADDE 54- (1) Nüfus olaylarını tescil etmekle görevli olanlar, nüfus müdürlüğünde düzenlenen ve aile kütüklerine tescil edilmesi gereken dayanak belgelerini işlem anında, diğer makamlarca

düzenlenen dayanak belgelerini ise nüfus müdürlüğüne intikal ettiği tarihten itibaren üç iş günü içinde aile kütüklerine tescil etmekle yükümlüdürler.

Elektronik sistemin kullanılmasına ilişkin esaslar

MADDE 55- (1) Elektronik ortamda merkezi veri tabanına bilgi gönderecek veya tescil edecek dış temsilcilikler, yetkili kurumlar ve Bakanlık tarafından yetkilendirilen kuruluşlar, sistemi kullanabilmek için Genel Müdürlük tarafından belirlenmiş kullanıcı adı ve parola gibi güvenlik kodları ile Elektronik Sertifika Hizmet Sağlayıcısı tarafından düzenlenmiş olan ve tescili gerçekleştirecek personele ait nitelikli elektronik sertifika kullanırlar.

(2) Sistemi kullanmak isteyen kurum ve yetkili kuruluşlara ait kimlik doğrulama bilgileri kontrol edildikten sonra şifrelenmiş güvenli veri iletişimi üzerinden hizmet verilir. Dış temsilcilik, kurumlar ve yetkili kuruluşlar güvenli ağ bağlantısını Genel Müdürlük tarafından belirlenen usul ve esaslar doğrultusunda taşra teşkilatlarına ve bu hizmeti kullanacak diğer birimlerine de sağlayabilirler.

(3) Dış temsilcilikler, kurum ve yetkili kuruluşlar elektronik ortamda merkezi veri tabanında yaptıkları işlemlerle ilgili kesintisiz ve sürekli veri girişini sağlamak amacıyla Genel Müdürlük ile birlikte gerekli tedbirleri almakla ve kişisel verilerin hukuka aykırı olarak işlenmesini, erişilmesini önlemek ve muhafazası için uygun güvenlik tedbirlerini sağlamakla yükümlüdür.

Mahkeme kararları

MADDE 56- (1) Mahkemeler tarafından verilen kararların aile kütüklerine tesciline dayanak olan bilgiler, mahkeme yazı işleri müdürlükleri tarafından Kanunda öngörülen on günlük süre içerisinde elektronik ortamda merkezi veri tabanına gönderilir veya tescil edilir.

(2) Mahkemeler tarafından verilen kararların elektronik ortamda gönderilememesi veya tescil edilememesi halinde, mahkeme yazı işleri müdürlükleri tarafından kararın kesinleştirme işlem tarihini takip eden on gün içerisinde mahkeme kararları nüfus müdürlüklerine gönderilir. Nüfus müdürlüklerine gönderilen kesinleşmiş kararlar aile kütüklerine tescil edilir.

Vasiyetname ve ölüme bağlı tasarruflar

MADDE 57- (1) Vasiyetname ve ölüme bağlı tasarrufların aile kütüklerine tesciline dayanak olan bilgiler, noterler tarafından Kanunda öngörülen süre içerisinde elektronik ortamda merkezi veri tabanına gönderilir veya tescil edilir.

ON BEŞİNCİ KISIM

Ortak Hükümler

Gün sonu listeleri

MADDE 58- (1) Gün sonu listelerinde yer alan nüfus olaylarının, günlük olarak kâğıt ortamında tutulan aile kütüklerine tescil edilmesi zorunludur.

(2) Kişilerin aile kütüğünün olduğu yer nüfus müdürlüğü tarafından; gün sonu listesinde yer alan nüfus olayları, elektronik ortamda tescil eden nüfus müdürlüğü, dış temsilcilik, kurum ve yetkili kuruluş kodu ve tescil numarası verilerek, kâğıt ortamındaki aile kütüğüne tescil edilir.

(3) Gün sonu listesinde yer alan dış temsilcilikler, kurumlar ve yetkili kuruluşlarca elektronik ortamda merkezi veri tabanına tescil edilen nüfus olaylarına ait Cumhuriyet başsavcılıkları, mahkemeler, diğer kurum ve kişilerle yapılması gereken yazışmalar ilgili nüfus müdürlüğüne yapılır.

Yabancı makamlarca verilmiş olan resmî belgelerin işleme alınması

MADDE 59- (1) Yetkili makamların imza ve mührünü taşıması şartıyla tarafı bulunduğumuz uluslararası antlaşmalar çerçevesinde düzenlenen belgelerin asılları kabul edilerek işleme alınır. Bu belgeler ayrıca bir tasdik işlemine tâbi tutulmaz.

a) Milletlerarası Ahval-i Şahsiye Komisyonunca hazırlanarak uygulamaya konulan sözleşmeler gereğince düzenlenen ve belirli bir formüle sahip kişi hallerine ilişkin çok dilli belgeler herhangi bir tasdik işlemine tâbi tutulmadan doğrudan işleme alınır.

b) La Haye Devletler Özel Hukuk Konferansınca hazırlanan Yabancı Resmî Belgelerin Tasdiki Mecburiyetinin Kaldırılması Sözleşmesine taraf olan devletlerin yetkili makamlarınca verilmiş belgeler, belgenin aslına eklenecek tasdik şerhi (Apostille) ve noter tarafından onaylanmış Türkçe tercümesi ile birlikte işleme alınır.

(2) Yabancı ülke makamlarına göre farklılık arz eden, belirli bir formüle tâbi olmayan ve ispat niteliği taşıyan resmî belgelerin asılları, usulüne uygun bir şekilde tasdik edilmiş ve noter tarafından onaylanmış Türkçe tercümesi ile birlikte işleme alınır.

(3) Fahri konsolosluklarca düzenlenen belgelere dayanılarak işlem tesis edilmez.

Yabancı devlet makamlarınca verilmiş kararlar

MADDE 60- (1) 27/11/2007 tarihli ve 5718 sayılı Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun hükümleri gereğince, yabancı devlet mahkemelerince verilen ve ilgili devletin kanunlarına göre kesinleşmiş bulunan kararların işleme konulabilmesi için yetkili Türk mahkemesi tarafından

tanınması veya tenfiz edilmesi zorunludur. Türkiye Cumhuriyetinin taraf olduđu uluslararası sözleşmelerin bu konudaki hükümleri saklıdır.

(2) Kanunun 27/A maddesi gereğince, 7/2/2018 tarihli ve 30325 sayılı Resmî Gazete’de yayımlanarak yürürlüğe giren Yabancı Ülke Adli veya İdarî Makamlarınca Verilen Kararların Nüfus Kütüğüne Tescili Hakkında Yönetmelikle belirlenen usul ve esaslar doğrultusunda; yabancı ülke adli veya idarî makamlarınca boşanmaya, evliliğin butlanına, iptaline veya mevcut olup olmadığının tespitine ilişkin olarak verilen kararlar aile kütüğüne tescil edilir.

Sürelerin hesaplanması

MADDE 61- (1) Kanunda belirtilen sürelerin hesaplanmasında olayın meydana geldiği tarihi izleyen gün başlangıç olarak alınır. Süreler; tayin edilen müddetin son günü, son gün resmî tatile rastlarsa tatili izleyen ilk iş günü çalışma saatinin bitiminde sona erer.

Vekilin yetkisi

MADDE 62- (1) Vekiller, vekâletname ibraz etmek suretiyle, il/ilçe nüfus müdürlüklerinde müvekkillerine ait işleri bizzat takip etmeye, dayanak belgelerini imzalamaya ve nüfus kayıt örneğini almaya yetkilidirler.

(2) Doğum, tanıma, din ve soyadı seçimi gibi ilgisi tarafından bizzat bildirimde bulunulmasını gerektiren olaylarda, bu hakkın kullanılmasına ilişkin hususları içerir vekâletname ibraz edilmesi zorunludur.

Nüfus olaylarına ilişkin dayanak belgelerinin imzalanması

MADDE 63- (1) Nüfus müdürlüklerine, dış temsilciliklere ve yetki verilen kurumlara yapılan bildirimler üzerine düzenlenen dayanak belgeleri, ıslak veya elektronik imza ile imzalanır.

(2) Nüfus olaylarına ait dayanak belgelerinin hangi hallerde bildirimde bulunan tarafından imzalanacağı Genel Müdürlükçe belirlenir.

Dayanak belgelerinin çoğaltılması ve dayanak belgesine ekli belgeler

MADDE 64- (1) Kişisel durum olaylarının aile kütüklerine tescili sırasında tutanak, karar veya belgelerin gereken sayıdan az olduğu ve temini mümkün olmadığı takdirde, işlemi yapan nüfus müdürlüğü tarafından belgenin örneği ya da sistemden alınan çıktısı veya vukuatından çıkartılacak aslına uygun okunaklı örneği düzenlenir ve onaylandıktan sonra işleme alınır.

(2) Kişisel durum siciline tescil edilecek bir kaydın dayanak belgesi niteliğindeki tutanak, karar ve belgelerin fotokopileri veya faks cihazı ile gönderilen örnekleri kabul edilip işleme konulamaz. Nüfus

müdürlüklerinin kendi aralarında yapacakları elektronik iletişim veya faks cihazı ile yazışmaları bu kapsam dışındadır.

ON ALTINCI KISIM

Devir ve Teslim

Devir ve teslim zorunluluğu ve süre

MADDE 65- (1) Başka bir yere atanma veya Devlet memurluğundan çekilme, emeklilik gibi nedenlerle kesin olarak görevinden ayrılan personel, yerine görevlendirilen personele on beş günü aşmamak koşuluyla devir ve teslim yapmakla yükümlüdür.

(2) Nüfus müdürlükleri tarafından devir ve teslim, tutanak düzenlenerek yapılır. Tutanaklar devralan ve devreden tarafından imzalanır ve yetkili tarafından onaylanır.

Devir ve teslimin yapılamaması

MADDE 66- (1) Memurun devir ve teslim yapmasına imkân vermeyecek durumda işten ayrılması halinde, Genel Müdürlük merkez kuruluşunda yetkili amir, taşra kuruluşunda ise mülkî idare amiri tarafından tayin edilecek bir kurul marifetiyle bu Yönetmeliğin ilgili maddelerine göre devir ve teslim işlemi yapılır.

Devir ve teslimin konusu

MADDE 67- (1) Devir ve teslim ile yükümlü bulunan memurların devir ve teslim işlerinin kapsamına giren hususlar şunlardır:

- a) Nüfus kütükleri.
- b) İşlemden kaldırılmış atik ve eski aile kütükleri, vukuat defterleri ile tescile esas olan belgeleri.
- c) Zimmetindeki demirbaşlar, resmî mühür, soğuk damga ve beratları.
- ç) Mavi kart ve uluslararası aile cüzdanları, bunların satış bedelleri ile kayıt ve satışına ilişkin elektronik ortamdan alınan defterlerin örnekleri.
- d) Resmî posta pulları.
- e) Teftiş ve denetleme dosyası.
- f) Memurlara ait özlük dosyaları.

Devir ve teslimde usul

MADDE 68- (1) Devir ve teslim, örneğine uygun üç örnek devir ve teslim tutanağının düzenlenmesi suretiyle yapılır. Tutanaklar devralan ve devreden tarafından imzalanır. Genel Müdürlük merkez kuruluşunda devir ve teslim memurlar arasında yapılmışsa şube müdürü, şube müdürleri arasında yapılmışsa daire başkanı, daire başkanları arasında yapılmışsa genel müdür yardımcısı, genel müdür yardımcısı arasında yapılmışsa Genel Müdür tarafından onaylanır.

(2) Genel Müdürlük taşra kuruluşunda ise devir ve teslim memurlar arasında yapılmışsa nüfus müdürü, nüfus müdürleri arasında yapılmışsa ilçelerde kaymakam, merkez ilçe nüfus müdürlüklerinde il nüfus ve vatandaşlık müdürü, il nüfus ve vatandaşlık müdürleri arasında yapılmışsa vali yardımcısı tarafından onaylanır.

Nüfus kütüklerinin devir ve tesliminde uygulanacak esaslar

MADDE 69- (1) Kâğıt ortamındaki nüfus kütükleri devir ve teslim edilirken;

- a) Usulüne uygun olarak onaylanıp onaylanmadığı ve sayfa numaralarının verilip verilmediği,
- b) Eksik sayfa olup olmadığı,
- c) Kütüklerde silinti veya kazıntı bulunup bulunmadığı,
- ç) Kütüklerin düzgün tutulup tutulmadığı, dağınık ve yırtık olup olmadıkları,
- d) Aile kütüklerinin güncel olarak tutulup tutulmadığı,

tespit edilir.

Denetim yetkisi

MADDE 70- (1) Genel Müdürlük taşra kuruluşlarını; vali, Genel Müdür, genel müdür yardımcısı, daire başkanı, mülkiye müfettişleri ve ayrıca ilçe nüfus müdürlüklerini kaymakam ve il nüfus ve vatandaşlık müdürü denetlemeye yetkilidir.

(2) İl nüfus ve vatandaşlık müdürleri ve nüfus müdürleri dairelerindeki personeli ve çalışmalarını Genel Müdürlük tarafından belirlenen usul ve esaslara göre denetim ve gözetim altında bulundurarak gereken tedbirleri alırlar.

ON YEDİNCİ KISIM

Çeşitli ve Son Hükümler

Formların tasarımı

MADDE 71- (1) Bakanlık, görev alanına giren konularda uygulamada kullanılacak olan form, belge ve tutanakları hazırlamaya ve gerekli düzenlemeleri yapmaya yetkilidir.

İdarî para cezası kararları

MADDE 72- (1) İdarî para cezalarına ilişkin kararlar, her takvim yılı için tarih ve sıra sayılarına göre saklanır.

Hüküm bulunmayan haller

MADDE 73- (1) Bu Yönetmelikte hüküm bulunmayan hallerde ilgili diğer mevzuat hükümleri uygulanır.

Uygulama talimatları

MADDE 74- (1) Bu Yönetmeliğin uygulanmasına ilişkin talimatlar, Genel Müdürlük tarafından belirlenir.

Yürürlükten kaldırılan mevzuat

MADDE 75- (1) 29/9/2006 tarihli ve 2006/11081 sayılı Bakanlar Kurulu Kararıyla yürürlüğe konulan Nüfus Hizmetleri Kanununun Uygulanmasına İlişkin Yönetmelik yürürlükten kaldırılmıştır.

Yürürlük

MADDE 76- (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 77- (1) Bu Yönetmelik hükümlerini Cumhurbaşkanı yürütür.

Genel Ürün Güvenliği Yönetmeliği

Resmî Gazete Tarihi : 11.03.2021

Resmî Gazete Sayısı : 31420

GENEL ÜRÜN GÜVENLİĞİ YÖNETMELİĞİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı; piyasaya arz edilen, piyasada bulundurulmuş veya tedarik edilen ve tüketicinin kullanımına hazır edilen, tüketici için amaçlanan veya tüketici için amaçlanmamış olsa dahi makul ölçüde öngörülebilir koşullarda tüketici tarafından kullanılacak ürünlerin güvenli olmasının sağlanması ve bu alanda yetkili kuruluşların görevleri ile üreticilerin ve dağıtıcıların yükümlülüklerinin belirlenmesidir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik, ürünlere ilişkin bir teknik düzenlemenin bulunmadığı veya teknik düzenleme bulunsada dahi insan sağlığı ve güvenliğine ilişkin hükümler içermediği veya belirli risklere yahut risk kategorilerine ilişkin hükümler içermediği durumlarda uygulanır.

(2) Bu Yönetmelik; piyasaya arz edilen, piyasada bulundurulmuş veya tedarik edilen ve tüketicinin kullanımına hazır edilen, tüketici için amaçlanan veya tüketici için amaçlanmamış olsa dahi makul ölçüde öngörülebilir koşullarda tüketici tarafından kullanılacak olan yeni, kullanılmış veya ıslah edilmiş tüm ürünlere uygulanır.

(3) Bu Yönetmelik, elektronik satışlar ve diğer uzaktan iletişim araçları vasıtasıyla gerçekleşen satışlar dahil, satış tekniğine bakılmaksızın tüm ürünlere uygulanır.

(4) Bu Yönetmelik, bir hizmet esnasında tüketicilere sunulan ürünlere uygulanır. Tüketicilere hizmet sunanlar tarafından kullanılan veya işletilen ekipmanları kapsamaz.

(5) Bu Yönetmelik, antika ürün veya kullanımından önce tamir veya ıslah edilmesi gereken ürün olarak tedarik edilen kullanılmış ürünlere, tedarikçinin tedarik ettiği kişiye bu konuda açıkça bilgi vermesi koşuluyla uygulanmaz.

Dayanak

MADDE 3 - (1) Bu Yönetmelik, 5/3/2020 tarihli ve 7223 sayılı Ürün Güvenliği ve Teknik Düzenlemeler Kanununun 24 üncü maddesi ve 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete’de yayımlanan 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinin 455 inci maddesine dayanılarak hazırlanmıştır.

(...)

Gizlilik, ticari sırlar ve şeffaflık

MADDE 10 - (1) Yetkili kuruluş, tüketicilerin üründen kaynaklanan risklere ilişkin bilgi sahibi olmaları amacıyla, bu Yönetmelik kapsamında yer alan tehlikeli ve ciddi risk arz eden ürünlere ilişkin olarak ürünü ve riski tanımlayan bilgiler ile üreticiler, dağıtıcılar veya kendisi tarafından alınan önlemleri kendi internet sitesinde veya gerekli gördüğü diğer uygun yöntemlerle ilan eder.

(2) Yetkili kuruluş, bu Yönetmelik hükümlerini uygularken kişisel verilere dair, ticari sır niteliğindeki veya fikrî ve sınai mülkiyet hakkına ilişkin edindiği bilgilerin gizliliğini korumakla yükümlüdür. Ancak, insan sağlığı ve güvenliğinin gerektirdiği hallerde bu bilgilerin açıklanması bu kapsamda sayılmaz.

(...)

Tapu ve Kadastro Verilerinin İşlenmesi ve Elektronik Ortamda Yapılacak İşlemler Hakkında Yönetmelik

Resmî Gazete Tarihi : 08.06.2022

Resmî Gazete Sayısı : 31860

Çevre, Şehircilik ve İklim Değişikliği Bakanlığı (Tapu ve Kadastro Genel Müdürlüğü)'ndan:

TAPU VE KADASTRO VERİLERİNİN İŞLENMESİ VE ELEKTRONİK ORTAMDA YAPILACAK İŞLEMLER HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM

Başlangıç Hükümleri

Amaç

MADDE 1- (1) Bu Yönetmeliğin amacı; Tapu ve Kadastro Genel Müdürlüğü merkezi veri tabanında yer alan verilerin işlenmesine ve elektronik ortamda yapılacak işlemlere ilişkin usul ve esasları belirlemektir.

Kapsam

MADDE 2- (1) Bu Yönetmelik, Tapu ve Kadastro Genel Müdürlüğü merkezi veri tabanında yer alan verilerin çevrimiçi olarak işlenmesine ve elektronik ortamda yapılacak işlemlere ilişkin usul ve esasları kapsar.

Dayanak

MADDE 3- (1) Bu Yönetmelik, 22/11/2001 tarihli ve 4721 sayılı Türk Medeni Kanununun 1020 nci maddesi, 4 sayılı Bakanlıklara Bağlı, İlgili, İlişkili Kurum ve Kuruluşlar ile Diğer Kurum ve Kuruluşların Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinin 480 inci maddesinin birinci fıkrasının (ğ) bendi, 487 nci maddesinin altıncı fıkrası, 488 inci maddesinin birinci ve beşinci fıkraları ile 22/7/2013 tarihli ve 2013/5150 sayılı Bakanlar Kurulu Kararıyla yürürlüğe konulan Tapu Sicili Tüzüğü'nün 14 üncü ve 15 inci maddelerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4- (1) Bu Yönetmelikte geçen;

- a) Açık tapu/kadastro verisi: Açık veri haline getirilen tapu ve kadastro verisini,
- b) Açık veri: Ücretsiz olarak veya hazırlanma maliyetini geçmeyecek şekilde internet üzerinden herkesin erişimine sunulan, üzerinde herhangi bir fikri mülkiyet hakkı bulunmayan ve herhangi bir amaçla serbestçe kullanılabilen, makineler tarafından okunabilen ve böylelikle diğer veriler ve sistemlerle birlikte çalışabilen anonim hale getirilmiş veriyi,
- c) Alıcı: TAKPAS'tan faydalanan kişi veya kurumları,
- ç) Alt kullanıcı: Alıcının, uygulamalar üzerinden TAKPAS'tan faydalanması için yetkilendirdiği kişileri,
- d) Anonim hale getirme: Tapu ve kadastro verilerinin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir kişiyle ilişkilendirilemeyecek hâle getirilmesini,
- e) Belirteç bilgisi: Alıcının, TAKPAS ile yaptıkları sorgulamaya ait kendi sistemleri/işlemleri ile ilişkisini gösterir işlem sistem numarası, işlem evrak numarası gibi bilgileri,
- f) Elektronik kabul beyanı: Protokol imzalananlar dışında kalan kişilerin, TAKPAS arayüzleri üzerinden veriye ulaşmaları için elektronik ortamda bilgisine sunulan metni kabulüne ilişkin beyanını,
- g) Elektronik ortamda yapılacak işlemler: 4 sayılı Cumhurbaşkanlığı Kararnamesinin 488 inci maddesinin beşinci fıkrası uyarınca, Genel Müdürlük tarafından belirlenen ve tapu müdürlüklerince tescili sağlanan işlemlerden, yargı mercileri ile yetkili kurum ve kuruluşların taleplerine istinaden ilgili mercilerce doğrudan elektronik ortamda tescil, terkin veya tadil edilebilecek işlemleri,
- ğ) Eşsiz belirteç: Alıcının onaylanmış toplu veri taleplerinde ihtiyaç duyulan verinin TAKPAS'ta tanımlanan servisler aracılığı ile alınmasını sağlayan, onaylanan her toplu veri talebi için Genel Müdürlükçe eşsiz olarak oluşturulan, sorgulamanın yapılabileceği gün içi zaman aralığını da içerir, TAKPAS arayüzleri üzerinden üretilen erişim süresi tanımlı yetki anahtarını,
- h) Genel Müdürlük: Tapu ve Kadastro Genel Müdürlüğünü,
- ı) İlgili kişi: Türk Medeni Kanununun 1020 nci maddesi kapsamında merkezi veri tabanındaki tapu ve kadastro verisine ulaşma hakkına sahip ilgisini inanılır kılan kişiyi,
- i) Kimliksizleştirme: Tapu ve kadastro verilerinin; kimliği belirli veya belirlenebilir kişiyle ilişkilendirilememesi için teknik ve idari tedbirlerin alınması şartıyla ve farklı bir ortamda muhafaza

edilen diğerk verilerle bir araya getirilmeksizin kimliğı belirli veya belirlenebilir kiřiyle iliřkilendirilemeyecek řekilde iřlenmesini,

j) Kiři: Kurumlar dıřında kalan geręek ve tuzel kiřileri,

k) Kiřisel veri: Kimliğı belirli veya belirlenebilir geręek kiřiye iliřkin her turlu bilgiyi,

l) Kiřisel verilerin iřlenmesi: Kiřisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değıřtirilmesi, yeniden duzenlenmesi, aęıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi tapu ve kadastro verileri uzerinde geręekleřtirilen her turlu iřlemi,

m) Kurum: Elektronik Kamu Bilgi Yonetim Sisteminde (KAYSİS) yer alan kamu kurum ve kuruluřlarını,

n) Maskeleye: Tapu ve kadastro verilerinin belirli alanlarının, kimliğı belirli veya belirlenebilir bir kiřiyle iliřkilendirilemeyecek řekilde silinmesi, uřtlerinin cizilmesi, boyanması ve yıldızlanması gibi iřlemleri,

o) Merkezi veri tabanı: Genel Muđurluęe elektronik ortamda tutulan verileri,

ö) Muvafakatname: Kamu kurumu nitelięindeki meslek kuruluřları ile tařınmaza iliřkin konularda faaliyet gořteren geręek ve tuzel kiřilerden, tařınmaz maliki ve hak sahiplerinin talep edilen iřlemleri ile ilgili olarak TAKPAS'tan sorgulanma ve her turlu belgenin edinilmesine rıza ve taahhut ięerir beyanın gořterildięi bir orneęi Ek-3'te yer alan belgeyi,

p) Protokol: Tapu ve kadastro verilerini talep eden kurumlar, kendi iřleriyle sınırlı olmak uzerine kamu kurumu nitelięindeki meslek kuruluřları ve tařınmaza iliřkin konularda faaliyet gořteren tuzel kiřiler ile 24/3/2016 tarihli ve 6698 sayılı Kiřisel Verilerin Korunması Kanunu ve anılan Kanun kapsamında cıkarılan duzenlemelere uygun řekilde hazırlanarak imzalanan TAKPAS'a eriřim protokolunu,

r) Taahhutname: Bu Yonetmelik huęuimleri cergevesinde kendileriyle protokol yapılan alıcının imzaladıęı ve paylařılan verilerin guvenlięini saęlamaya yonelik olarak almayı taahhut ettikleri idari ve teknik tedbirleri ięeren ve bir orneęi Ek-3'un ekinde yer alan belgeyi,

s) TAKBİS: Tapu ve Kadastro Bilgi Sistemini,

ř) Tapu ve Kadastro Paylařım Sistemi (TAKPAS): Merkezi veri tabanında tutulan verilerin kurumlarla ve kiřilerle paylařılmasına imkân saęlayan servis, Web Tapu veya Genel Muđurluęe belirlenen dięer arayuzlerden oluřan sistemi,

t) Taşınmazı tanımlayıcı bilgiler: Kimliksizleştirilmiş taşınmazın; bulunduğu il, ilçe, mahalle/köy, mevkii, ada/parsel numarası, niteliği, yüzölçümü, kat irtifakı veya kat mülkiyeti durumu, varsa blok ve bağımsız bölüm numarasına ilişkin bilgileri,

u) Veri: Genel Müdürlük tarafından üretilen veya arşivlenen her türlü bilgi ve belgeyi,

ü) Web-Tapu sistemi: Elektronik ortamda taşınmazların yönetilebildiği, sisteme entegre edilen tapu, kadastro ve haritacılık işlemleri ile Osmanlıca ve eski kayıt belge işlemleri için başvuru yapılabilen, işlemler için gerekli olan bilgi ve belgelerin gönderilebilmesine olanak sağlayan, belge doğrulaması yapılabilen ve bu konularda üçüncü kişilere yetki verilebilen e-Devlet sistemine entegre olan ve Genel Müdürlüğün merkezi veri tabanı verilerine erişimi sağlayan TAKPAS arayüzünü,

ifade eder.

İKİNCİ BÖLÜM

Tapu ve Kadaastro Verileri, Erişim Usul ve Esasları

Tapu ve kadaastro verileri

MADDE 5- (1) TAKPAS'taki veriler; taşınmazın gerçek ve tüzel kişiyle ilişkilendirilmesi ve üzerindeki hakların gösterilmesine ilişkin bilgileri içerir.

(2) TAKBİS üzerindeki kayıtlar, her bir birim için, sicillerin elektronik ortamda tutulmaya başlandığı tarihte aktif olan ve bu tarihten sonra oluşan bilgileri içerir.

(3) TAKBİS öncesi pasif kayıtlara yönelik talepler, kişi ve kurumlar tarafından, taşınmazın kaydına ulaşılmasını sağlayacak tanımlayıcı bilgileri belirtilerek tapu sicilinin tutulduğu ve dayanak belgelerin arşivlendiği ilgili birimlere yapılır. 30/4/2011 tarihli ve 27920 sayılı Resmî Gazete'de yayımlanan Tapu Müdürlüklerince Yetki Alanı Dışında Kayıtlı Bulunan Taşınmazlarla İlgili Tapu İşlemlerinin Yapılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik hükümleri saklıdır.

Veri erişimine ilişkin genel esaslar

MADDE 6- (1) Alıcı tarafından veri talebi oluşturulması ve sorgulama yapılabilmesi için Genel Müdürlük ile protokol yapılması veya elektronik kabul beyanı zorunludur.

(2) Zorunlu haller veya protokolda belirtilen özel haller dışında güvenli ve kesintisiz bir hizmet sunulması esastır.

(3) Genel Müdürlük tarafından merkezi veri tabanında tutulan veriler, Türk Medeni Kanununda, 6698 sayılı Kanunda, 4 sayılı Cumhurbaşkanlığı Kararnamesi ile ilgili kanunlarda, Tapu Sicili

Tüzüğünde ve anılan mevzuat uyarınca çıkarılan düzenlemelerde belirtilen usul ve esaslar çerçevesinde alıcı ile yalnızca çevrimiçi olarak paylaşılır. Paylaşılacak veriler, alıcının veri kullanım amacı ve yasal dayanağı göz önünde bulundurularak belirlenir.

(4) Alıcı, Genel Müdürlük ile imzalanan protokol uyarınca işleme konu kişilerin bilgilerini alabilir. Söz konusu kişilerin verilerini, kullanım amacı tanımlanmış faaliyetin yerine getirilmesi dışında başka hiçbir amaçla kullanamaz.

(5) Kadastro verileri için arşiv onaylı olması kaydıyla Genel Müdürlük merkezi veri tabanından elde edilen veriler aksi ispatlanıncaya kadar geçerlidir.

(6) Genel Müdürlük, veri erişim talebi kapsamında elde edilen bilginin yetkisiz kişilerin eline geçmesi hâlinde kime ait olduğunun tespit edilmesini zorlaştıracak şekilde gerekli gördüğü bilgiler üzerinde kısmî kimliksizleştirme veya maskeleyme tedbirlerini uygular.

(7) Alıcı tarafından alınan verilerin çıktılarında alıcı adı, varsa alt kullanıcı adı, tarih ve saat bilgisi yer alır.

(8) Alıcı, aldığı verilerin gizliliğini sağlamakla yükümlüdürler. Bu verilerin hukuka aykırı olarak işlenmesi ve erişilmesini önlemek ve muhafazasını sağlamak amacıyla her türlü idari ve teknik tedbirleri alırlar. Tapu ve kadastro verilerinin yurt dışına aktarılmasında 6698 sayılı Kanunun 9 uncu maddesindeki sınırlandırmalar ve kurallara uyulur. Özel nitelikli kişisel veriler için ise ayrıca anılan Kanunun 6 ncı maddesinin dördüncü fıkrası uyarınca Kişisel Verileri Koruma Kurulu tarafından belirlenen önlemler alınır.

(9) TAKPAS'ın işletilmesinde, paylaşılmasında ve kullanılmasında; Türkiye Cumhuriyeti Anayasası, uluslararası sözleşmeler ve diğer mevzuatta yer alan; Devlet sırrına, kişisel verilerin korunmasına, özel hayatın ve soruşturmanın gizliliğine, mahkemelerce verilen gizlilik kararlarına, gizli tanıklığa, 27/12/2007 tarihli ve 5726 sayılı Tanık Koruma Kanunu ile 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu kapsamında alınan tedbir kararlarına ilişkin hükümler esas alınır.

(10) Taşınmazı tanımlayıcı bilgilere ve taşınmaza yönelik hak ve kısıtlamalara herkes tarafından herhangi bir kısıtlama olmaksızın ulaşılabilir. 4721 sayılı Türk Medeni Kanununun 1020 nci maddesi kapsamında taşınmaz üzerinde hak sahibine yönelik hak ve kısıtlamalar sadece ilgisini inanılır kılanlar tarafından öğrenilebilir.

TAKPAS verilerine erişim ve erişim hakkı

MADDE 7- (1) TAKPAS hizmetleri; kurumlar ve kişilerin, arayüzler ile ulaşabilecekleri etkileşimli sorgulamalar ve kendi yazılım uygulamaları içerisinde ekleyecekleri bölümler ile sorgulama ve elektronik ortamda tapu işlemleri yapmalarına olanak verecek internet servislerinden oluşur. Sorgulamalarda, sorgu kriterine göre sorgu sonucu olarak TAKPAS'ta bulunan, kurum ve kişilerin almaya yetkili olduğu bilgiler paylaşılır. Kurumlar ve kişilerle yetkisi dâhilinde olmayan bilgilerin paylaşılması engellenir.

(2) Mahkemeler, Cumhuriyet savcılıkları, icra ve iflas müdürlükleri ile kamu kurum ve kuruluşlarının görevleriyle ilgili taşınmaz verilerine erişimi protokol düzenlenerek belirlenebilir.

(3) Kamu kurumu niteliğindeki meslek kuruluşları ile taşınmaza ilişkin konularda faaliyet gösteren tüzel kişiler kendi işleriyle sınırlı olmak üzere, düzenlenecek protokol kapsamında gerekli verilere erişebilirler.

(4) Taşınmaz malikleri ile taşınmaz üzerinde hak sahibi olanlar, taşınmazları hakkında elektronik kabul beyanı ile ilgili verilere erişebilirler.

(5) Tapu sicilinin açıklığı ilkesi gereğince, taşınmazın tanımlayıcı bilgileri ile taşınmaza yönelik hak ve kısıtlamalar herkes tarafından elektronik kabul beyanı ile sorgulanabilir.

Elektronik ortamda işlem tesisi

MADDE 8- (1) Tapu siciline yönelik her türlü tescil, şerh, beyan, terkin taleplerinde; TAKPAS'tan erişilen taşınmaz ada, parsel ve varsa bağımsız bölüm bilgilerinin yanında, gerçek kişilerde T.C. kimlik numarası/yabancı kimlik numarası, ad, soyad, baba adı gibi kimlik bilgileri; tüzel kişilerde ise MERSİS numarası/vergi numarası ile tüzel kişi tanımlayıcı bilgisinin de protokol yapılan kurumlarca taşınmazın bulunduğu tapu müdürlüğüne sunulması gereklidir. Aksi halde söz konusu talepler reddedilir.

(2) Elektronik ortamda yapılan işlemlerde, gerekli kontroller internet servisleri tarafından yapılarak işlemin yevmiye numarası TAKBİS tarafından üretilir. İşlemin türüne göre elektronik ortamda tescil veya terkin işlemi TAKBİS tarafından yapılır. İşlemin hatalı olarak yapıldığının fark edilmesi durumunda tapu müdürlüğüne resen tesis veya terkine yönelik gerekli düzeltme işlemi yapılarak başvuru sahibine bilgi verilir.

(3) Elektronik ortamda yapılan işlemlere ilişkin fiziki belge üretilmez. İşlemin sonuç yazıları servisleri kullanılarak işlemin tarafınca sorgulanmak sureti ile elde edilir. Elektronik ortamda yapılan işlem sonucunda, işlemin tarafı dışındaki diğer kurumlara mevzuatı uyarınca bildirimde bulunulması gereken hallerde, işlemin tarafı olmayan kurum tarafından internet servisleri kullanılarak gerekli

sorgulama yapılır. Genel Müdürlükçe işlemin tarafı olan Kurum ile mevzuatı uyarınca bildirim yapılması gereken işlemin tarafı olmayan kurumlara ayrıca bildirimde bulunulmaz.

TAKPAS'a tanımlama ve yetkilendirme

MADDE 9- (1) Genel Müdürlük ile protokol yapmış olan alıcı, protokol ile belirlenen internet servislerini, metotları ve sunulan verilerin kullanılması için gerekli yazılım ve donanımı sağlamakla yükümlüdür.

(2) TAKPAS'a erişmek isteyen alıcıya ait güvenlik kodları kontrol edildikten sonra, hizmet alanların güvenlik duvarları ile sistem güvenlik duvarları arasında özel şifrelenmiş güvenli ağ bağlantısı kurularak iki bağlantı noktası arasında hizmet verilir.

(3) Genel Müdürlük; alıcının, sabit IP adresi ve uygun görülecek güvenlik yöntemleri ile bağlantı kurarak TAKPAS'a erişimini sağlar.

(4) Alıcı, TAKPAS bağlantısını protokol ve güvenlik taahhütnamesinde belirlenen amaçlar ve kurallar doğrultusunda taşra teşkilatlarına, şubelerine ve alt kuruluşlarına da sağlayabilir. Kamu kurum ve kuruluşları, bu bağlantıyı yurt dışı teşkilatlarına da sağlayabilir.

(5) Alıcının taşra teşkilatları, şubeleri, alt kuruluşları veya yurt dışı teşkilatları ile ayrıca protokol yapılmaz.

(6) Alıcı, kendi teşkilat yapısı dışındaki kurum, kuruluş ve kişileri TAKPAS'tan faydalandıramaz.

(7) Alıcı, Genel Müdürlükçe kullanıma açılan arayüzlerde, alt kullanıcılarının yetkilerini belirlemek ve tanımlamakla yükümlüdür. Alıcı, tanımladığı kullanıcı bilgilerini Genel Müdürlüğün belirleyeceği yöntem ile Genel Müdürlüğe bildirir.

(8) Alıcı, Genel Müdürlükçe kullanıma açılan internet servislerde, alt kullanıcılarının yetkilerini belirlemek ve tanımlamakla yükümlüdür. Alıcı, tanımladığı kullanıcı bilgilerini Genel Müdürlükçe talep edilmesi halinde bildirir.

(9) Genel Müdürlük, kullanıma açtığı arayüzlerde, alıcının alt kullanıcılarının kontrol edilmesini, protokol ve güvenlik taahhütnamesi ile sağlanan yetkilendirme çerçevesinde bilgi almasını ve tanımlanan kullanıcılara ait tüm güncel bilgilerin sistemde tutulmasını sağlamakla yükümlüdür.

Başvuru ve protokol süreci, güvenlik taahhütnamesi

MADDE 10- (1) TAKPAS'tan yararlanmak isteyen alıcı, Genel Müdürlüğe yazılı olarak veya elektronik ortamda talepte bulunur.

(2) Başvuruda, talep edilen verilerin kullanılma amacının açık, net ve somut olması, alıcının verileri almasına esas olan yasal dayanağın belirtilmesi ve Genel Müdürlük tarafından talep edilen bu Yönetmeliğin ekinde yer alan belgelerin ve güvenlik taahhünamesinin gönderilmesi zorunludur. Yasal dayanağın belirtilmemesi halinde herhangi bir işlem yapılmaksızın talep reddedilir.

(3) Yapılan başvurular Veri Paylaşımı Alt Komisyonu tarafından incelenir, en geç bir ay içerisinde anılan komisyonun görüşü ile birlikte Veri Paylaşımı Üst Komisyonuna sunulur. Uygun görülmeyen alıcı başvurusu gerekçesi belirtilerek Veri Paylaşımı Üst Komisyonunca reddedilir.

(4) Başvurusu Üst Komisyonda uygun görülen alıcının Genel Müdürlükçe belirlenen uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü idari ve teknik tedbirleri sağladığını gösterir güvenlik taahhünamesini sunması zorunludur. Ayrıca alıcı her takvim yılı sonunda, Genel Müdürlükçe talep edilen idari ve teknik güvenlik tedbirlerinin sağlandığını gösterir güvenlik taahhünamesini Genel Müdürlüğe gönderir.

(5) Genel Müdürlükçe belirlenen güvenlik unsurlarını sağlamayan alıcı, bu hususun bildirildiği tarihten itibaren altmış gün içinde eksiklikleri tamamlamak zorundadır. Aksi halde alıcının başvurusu reddedilir.

(6) Başvurusu uygun görülenlerle protokol imzalanır.

(7) Protokollerde aşağıda belirtilen hususlara yer verilir:

a) Verinin niteliği ve sınırı, kullanıcı başına günlük sorgulama sayısı sınırı.

b) Verilere erişim şekli, süresi, kontrol ve güvenliği.

c) Protokolün süresi.

ç) Kişisel verilerin muhafaza edilme süresi.

d) Veriye erişecek kullanıcıların bilgileri.

e) Verilere hangi amaçla erişileceği ve hukuki gerekçesi.

f) Tarafların yetki ve görevleri ile hukuki sorumlulukları.

g) Alınması gereken idari ve teknik tedbirler.

ğ) Eğitim.

h) Ücretlendirme.

ı) Diğer hususlar.

ÜÇÜNCÜ BÖLÜM

Veriye Erişim Kuralları, Toplu Veriye Erişim, Diğer Verilere Erişim

Alıcının veriye erişimi

MADDE 11- (1) Genel Müdürlükçe protokol yapılan alıcı, gerçek kişilerde T.C. kimlik numarası/yabancı kimlik numarası, tüzel kişilerde ise vergi kimlik numarası/MERSİS numarası ile sorgulama yapabilir. Bununla birlikte mevzuattan kaynaklanan görevlerini yerine getirmek amacı ile taşınmaz tanımlayıcı bilgileri ile tekil taşınmaz ve mülkiyet sorgulaması yapması gereken kurumların talepleri Genel Müdürlük Veri Paylaşımı Üst Komisyonunca karara bağlanır.

(2) Alıcı, yaptığı sorgulamalar için, Genel Müdürlüğe sorgu yapılan kişinin kendilerinde tabi olduğu işleme ait belirteç bilgisini sorguya ekler. Alıcı, sorgu içerisinde verilen bu belirteç bilgisi ile kendilerinde başlatılan işlemin Genel Müdürlükçe kontrol edilebileceği, işleme taraf kişileri gösterir bir servis hazırlayıp çevrimiçi olarak Genel Müdürlüğün kullanımına açar. İşlem bağlantılı yapılmayan sorgulamalar için ise belirteç yerine Genel Müdürlükçe yapılacak olan denetimlerde işlem ve sorgu kontrolünün yapılabilmesini temin edecek şekilde açıklama girilmesi zorunludur.

(3) Alıcı, yalnızca talep esnasında belirtilen amaç ve hukuki gerekçeyle sınırlı olarak taşınmaz bilgilerine erişebilir. Mevzuattan kaynaklanan görevlerini yerine getirmesi amacı ile toplu veriye ihtiyacı olduğu Genel Müdürlük Veri Paylaşımı Üst Komisyonunca karara bağlanmış olan kurumların münferit toplu veri talepleri Genel Müdürlük ilgili birimince veri talebinin dayanağı kontrol edilerek değerlendirilir. Toplu veri talebinin içeriği Ek-1'de yer alan işlem bazlı toplu veri talep listesine göre belirlenir. Dayanak ile uyumlu talepler ilgili birimce karşılanır. Ek-1 listede yer alan kişisel veri içermeyen istatistiki veri talepleri ile anılan listede yer almayan toplu veri taleplerinde Genel Müdürlük Veri Paylaşımı Üst Komisyonundan ayrıca onay alınır.

(4) Toplu veri alımı için;

a) Genel Müdürlük ile protokol yapan alıcı, TAKPAS arayüzleri üzerinden elektronik imzalı belge ile toplu veri talebini oluşturur. Talebin onaylanmasını müteakip, talep edilen bilgilerin sorgulanabileceği eşsiz belirteç alıcının kullanımına sunulur.

b) Alıcı, TAKPAS arayüzleri üzerinden (a) bendi uyarınca aldığı eşsiz belirteç bilgisini kendi sistemine girerek Genel Müdürlüğün hazırladığı internet servisler vasıtası ile onaylanan verilere erişebilir.

Genel Müdürlük personelinin veriye erişimi

MADDE 12- (1) Genel Müdürlük kullanıcılarının tanımlanması, yetkilendirilmesi ve izlenmesi Genel Müdürlükçe yapılır.

(2) Genel Müdürlükçe yetkilendirilen personel her yıl 6698 sayılı Kanun kapsamında eğitime tabi tutulur.

Türkiye Barolar Birliği üzerinden avukatların veriye erişimi

MADDE 13- (1) Avukatlar, görevleri ile ilişkili olarak TAKPAS arayüzleri veya internet servisleri üzerinden Türkiye Barolar Birliğinin alt kullanıcısı sıfatıyla taşınmaz bilgisini sorgulayabilir. Bu kapsamda avukat, ilgisini ortaya koyan ulaşmak istediği verinin dayanağı yazılı belgeyi (çek, senet, alacak belgesi, kira kontratı, icra takip yazısı ve benzeri) sisteme taratıp belgenin tarih ve/veya sayısını eklemek ve elektronik kabul beyanını e-imza ile onaylamak suretiyle ilgilinin sadece taşınmazının (pasif kayıt bilgisi dâhil) olup olmadığı bilgisine sistemden ulaşabilir. Bununla birlikte ilgisini ortaya koyan vekaletname taratılmak suretiyle yapılacak sorgulamalarda, hangi kişinin malvarlığının hangi amaçla sorgulandığına dair bilginin sisteme girilmesi ve elektronik kabul beyanının e-imza ile onaylanması suretiyle avukatın talebine bağlı olarak taşınmazın (pasif kayıt bilgisi dahil) bilgisine veya kayıt örneğine ulaşılmasına ve örnek alınmasına imkan verilir.

Türkiye Değerleme Uzmanları Birliği üzerinden değerlendirme uzmanlarının veriye erişimi

MADDE 14- (1) Değerleme uzmanları görevleri ile ilişkili olarak TAKPAS arayüzleri üzerinden Türkiye Değerleme Uzmanları Birliğinin alt kullanıcı sıfatıyla taşınmaz sahibinin TAKPAS arayüzleri üzerinden vereceği yetki veya onay ile aşağıda belirtilen şekilde taşınmaz bilgisini sorgulayabilirler:

a) Taşınmaz sahibinin yetki vermesi ile veriye erişim: Değerleme yapılacak olan taşınmazın sahibi, TAKPAS arayüzlerini kullanarak değerlemeye konu olacak taşınmazı üzerinde yapılacak olan taşınmaz değerlendirme işlemi için yetki tanımlar. Bu kapsamda değerlendirme uzmanları kendilerinden talep edilen değerlendirme faaliyeti ile ilgili olarak malikin T.C. kimlik numarası/yabancı kimlik numarası, tüzel kişilerde ise vergi kimlik numarası/MERSİS numarası ile TAKPAS arayüzünden talep oluşturur. Değerleme uzmanlarınca, yetki tanımlanmış taşınmaz için yapılan değerlendirme talebinde taşınmaz sahibinden ikinci bir onay aranmaz. TAKPAS arayüzleri üzerinden yapılan yetki tanımı, ilgilisi tarafından iptal edilene kadar geçerlidir.

b) Taşınmaz sahibinin onay vermesi ile veriye erişim: Değerleme uzmanları kendilerinden talep edilen değerlendirme faaliyeti ile ilgili olarak malikin T.C. kimlik numarası/yabancı kimlik numarası, tüzel kişilerde ise vergi kimlik numarası/MERSİS numarası ile TAKPAS arayüzünden talep oluşturur. Sorgulama yapılabilmesi için taşınmaz malikinin, TAKPAS arayüzüne telefon numarasını tanımlamış

ve deęerleme uzmanının talebi sonrası kendisine sistemden gönderilen kısa mesaj üzerine arayüze girerek deęerleme uzmanının veriye ulaşımını onaylamış olması gerekir. Bu işlem çağrı merkezi üzerinden de yürütülebilir. Talebin taşınmaz malikince onaylanmasını müteakip deęerleme uzmanının taşınmaz bilgilerine ulaşımına izin verilir.

(2) Banka/finans kurumlarının deęerleme uzmanları üzerinden yapmış oldukları taşınmaz deęerleme taleplerinde Türk Medeni Kanununun 1020 nci maddesinde öngörülen ilginin var olduğu kabul edildiğinden, TAKPAS servisi veya arayüzleri üzerinden verilen deęerleme onaylarında ayrıca taşınmaz sahibinin onayı aranmaz. Talepte birinci fıkrada belirtilen usullerle yetki veya onay işleminin gerçekleştirilememesine ilişkin olarak Genel Müdürlükçe yapılacak denetimlerde işlem ve sorgu kontrolünün yapılabilmesini temin edecek ve ilgisini ortaya koyacak şekilde açıklama girilmesi zorunludur.

(3) TAKPAS arayüzleri üzerinden yetki veya onay vermesi mümkün olmayan taşınmaz sahiplerinin taşınmazlarına yönelik deęerleme taleplerine yönelik deęerleme onayı Genel Müdürlükçe verilir. TAKPAS arayüzleri üzerinden yetki veya onay vermesi mümkün olmayan taşınmaz sahiplerini belirlemeye Genel Müdürlük yetkilidir.

Harita verilerine erişim

MADDE 15- (1) Harita verileri, 29/12/2014 tarihli ve 2014/7155 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan Bakanlıklararası Harita İşlerini Koordinasyon ve Planlama Kurulu Yönetmeliği ile 5/7/1994 tarihli ve 94/5856 sayılı Bakanlar Kurulu Kararıyla yürürlüğe konulan Harita ve Harita Bilgilerini Temin ve Kullanma Yönetmeliği esaslarına göre TAKPAS üzerinden paylaşılabilir.

Kadastral verilere erişim

MADDE 16- (1) Kimliksizleştirilen taşınmaz tanımlayıcı bilgiler, yer kontrol noktaları ve detay koordinatlar TAKPAS üzerinden protokol düzenlenen alıcı ile paylaşılabilir.

Tapu tahrir defterlerine erişim

MADDE 17- (1) Tapu tahrir defterlerine ait kayıtlar elektronik ortamda TAKPAS üzerinden protokol düzenlenen alıcı ile paylaşılabilir.

Yabancı uyruklu kişiler ve yabancı sermayeli şirketlerin verilerine erişim

MADDE 18- (1) Yabancı uyruklu kişilerin ve yabancı sermayeli şirketlerin verilerinin paylaşılmasında bu Yönetmelikte belirlenen usul ve esaslar geçerlidir. Yabancı uyruklu kişilere ilişkin sorgulama kriterleri protokollerde ayrıca belirlenebilir.

Veriye diđer eriřim hallerine iliřkin usul ve esaslar

MADDE 19- (1) Protokol yapılmayan kiři ve kurumlar TAKPAS internet servislerinden yararlanamaz. Bu kiři ve kurumlar tapu ve kadastro verilerine y6nelik sorgulama taleplerini tařınmaz kaydının bulunduđu tapu veya kadastro m6d6rl6klerine yazılı olarak iletirler. Taleplerin, y6r6rl6kteki mevzuat kapsamında uygun olduđu deđerlendirildiđinde bilgi ve belge 6rnekleri verilir.

(2) Tapu M6d6rl6klerincede Yetki Alanı Dıřında Kayıtlı Bulunan Tařınmazlarla İlgili Tapu İřlemlerinin Yapılmasına İliřkin Usul ve Esaslar Hakkında Y6netmelik kapsamında yetki alanı dıřındaki tapu iřlemleri hari6 olmak 6zere tapu siciline y6nelik tescil, řerh, beyan, terkin ve TAKPAS'ta yer almayan veri talepleri ile uyumsuz kayıt iddialarına iliřkin taleplerin asli sicillerinin bulunduđu tapu m6d6rl6klerine yapılması gerekir. S6z konusu taleplerde tařınmazın tanımlayıcı bilgilerinin bildirilmesi zorunludur. Bunun dıřındaki talepler karřılanmaz.

(3) Tařınmaz malikleri ve tařınmaz 6zerinde hak sahibi olanlar ile 4721 sayılı Kanunun 1020 nci maddesi uyarınca ilgisini inanılır kılanlar; kayıtların tutulduđu ilgili birimlerden yazılı olarak talepte bulunmaları halinde bilgi ve belge 6rneklerini edinebilir.

(4) TAKPAS'tan herhangi bir nedenle uzun s6reli olarak veri alınamaması halinde de birinci fıkra h6k6mleri uygulanır.

(5) Bu madde kapsamında verilerin dok6man olarak paylařılması da bu Y6netmeliđin 38 inci maddesi h6k6mlerine tabidir.

(6) İlgililerince sorgulama sonucunu g6sterir belge/tapu kayıt 6rneđinin istenilmesi durumunda ise 2/7/1964 tarihli ve 492 sayılı Har6lar Kanunu geređince kayıt ve belge 6rneđi verilmesine iliřkin har6 tahsil edilir.

(7) Tapu kadastro verileri, 6evrimdıřı olarak tařınabilir bellek, CD, DVD ve benzeri ortamlarda paylařılamaz. Protokol yapılmıř alıcı ve alt kullanıcılarının da 6evrimdıřı veri talepleri karřılanmaz.

(8) Kanunlardaki 6zel h6k6mler ile afet ve benzeri durumlara iliřkin zorunlu haller saklıdır.

D6RD6NC6 B6L6M

Kiřisel Verilerin Gizlenmesi, Tapu ve Kadastro Verisinin D6zeltilmesi, Tapu ve Kadastro Verisinin İmha Edilmesi

Kiřisel verilerin gizlenmesi

MADDE 20- (1) Hakkında gizlilik kararı verilen kişilere ait verilerin gizlenmesi için yargı makamları tarafından gönderilen müzekkerenin gereği Genel Müdürlük tarafından yerine getirilir. Gizlilik kararlarının sadece görevi gereği bilmesi gereken kişiler tarafından bilinmesini sağlamak üzere gerekli her türlü teknik ve idari tedbir alınır.

Tapu ve kadastro verisinin düzeltilmesi

MADDE 21- (1) Tapu ve kadastro verisinin paylaşımında, paylaşılan taraflarca veride herhangi bir hata bulunduğu bildirilmesi halinde, bu husus ilgili tapu ve kadastro müdürlüklerine bildirilir ve varsa hatanın mevzuat dâhilinde ivedilikle giderilmesi sağlanır.

Tapu ve kadastro verisinin imha edilmesi

MADDE 22- (1) Tapu ve kadastro verisinin, kullanım amacının sona ermesini takiben imhası, alıcının sorumluluğundadır.

BEŞİNCİ BÖLÜM

Veri Güvenliği

Veri güvenliğine ilişkin yükümlülükler

MADDE 23- (1) 6698 sayılı Kanununun 12 nci maddesinde yer alan veri güvenliğine ilişkin yükümlülüklerle riayet edilir. Teknik ve idari tedbirlerin alınmasında, Kişisel Verileri Koruma Kurumu tarafından hazırlanan Kişisel Veri Güvenliği Rehberi esas alınır.

(2) Genel Müdürlük, kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek ile muhafazasını sağlamak amacıyla her türlü idari ve teknik güvenlik tedbirlerini alır ve kurum ve kişi kullanıcılarının da bu tedbirleri almasını takip eder ve denetler.

(3) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde veri sorumlusu tarafından ilgisine ve Kişisel Verileri Koruma Kuruluna yapılacak bildirimde 6698 sayılı Kanun hükümleri ile Kişisel Verileri Koruma Kurulunun bu hususa ilişkin düzenleyici işlemleri esas alınır.

Bilgi güvenliği

MADDE 24- (1) Genel Müdürlük merkez birimleri ve taşra teşkilatında yürütülen bilgi güvenliği süreçleri, Genel Müdürlük tarafından hazırlanan yönerge ile belirlenir.

Yedekleme

MADDE 25- (1) Sistemde oluşabilecek veri kayıplarının önlenmesi için, Genel Müdürlüğün belirleyeceği aralıklarla verilerin yedeklenmesi sağlanır.

Donanım güvenliği

MADDE 26- (1) Sistemin bulunacağı yerdeki donanımın sahip olması gereken güvenlik ihtiyaçlarının tespit edilmesi, sistem odasına veya sistem konsollarına erişimde yetkisiz erişimin engellenmesi ve iş sürekliliğinin sağlanması hususunda Genel Müdürlükçe gerekli tedbirler alınır.

Yeterli önlemler

MADDE 27- (1) Özel nitelikli kişisel verilerin işlenmesinde ayrıca, 6698 sayılı Kanununun 6 ncı maddesinin dördüncü fıkrası kapsamında Kişisel Verileri Koruma Kurulu tarafından yapılan düzenlemelerde yer alan önlemlere riayet edilir.

ALTINCI BÖLÜM

İzleme, Denetim, İhlal ve Yaptırımlar

Alıcının işlemlerinin izlenmesi

MADDE 28- (1) Alıcı, 6698 sayılı Kanunda belirtilen usul ve esaslara uymakla ve bu esaslar dâhilinde alt kullanıcıların yaptığı işlemleri izlemekle yükümlüdür.

(2) Genel Müdürlük, alıcının iş ve işlemlerine ilişkin tüm bilgileri izler ve değerlendirir.

Geri izleme bilgilerinin oluşturulması

MADDE 29- (1) Genel Müdürlük, alıcının TAKPAS'tan yaptığı her türlü işlemin tarihi, saati ve internet servis adına ilişkin kayıtları geri izleme bilgisi olarak tutar.

(2) Alıcı, TAKPAS'tan yapılan her türlü işlemin tarihi, saati, internet servis adına ilişkin kayıtları alt kullanıcı düzeyinde geri izleme bilgisi olarak tutar.

(3) Genel Müdürlük ve alıcı geri izleme bilgisini, sorgulanan kişi ve sorgu sonucundan etkilenen diğer kişilerin de kimlik numarasını içerecek şekilde tutar. Bu bilgiler, sadece mahkeme veya savcılık taleplerinin yerine getirilmesi için gönderilir.

(4) Genel Müdürlük ile alıcının geri izleme bilgilerinde tutarsızlık olması halinde Genel Müdürlük kayıtları esas alınır.

(5) Genel Müdürlük ve alıcı, değiştirilmesini engelleyerek ve yetkisiz erişime karşı koruyarak, geri izleme bilgilerini sekiz yıl süre ile saklar. Bu süre sonunda geri izleme bilgileri, 28/10/2017 tarihli ve

30224 sayılı Resmî Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik hükümleri kapsamında silinir veya yok edilir.

Denetim

MADDE 30- (1) Genel Müdürlükle protokol yapan alıcı, gerekli görüldüğünde mevzuatla kendisine denetim yetkisi ve görevi verilmiş kurum ve kuruluşlar ile Genel Müdürlük veya Genel Müdürlükçe yetkilendirilen kuruluşlar tarafından denetlenir.

(2) Denetleme sırasında, alıcı tarafından her türlü bilgi, belge, kayıt ve veri taleplerinin karşılanması ve sistemin incelemeye açılması zorunludur.

(3) Denetleme sonucuna göre usulsüzlük tespiti halinde, 6698 sayılı Kanun kapsamında gerekli işlemler yapılır ve 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu uyarınca gerekli işlemler başlatılır.

Veri paylaşımı ilkelerinin ihlali ve hukuki sorumluluk

MADDE 31- (1) Alıcı, kişisel veri ihlali olması durumunda 6698 sayılı Kanun ve ilgili mevzuata uygun yöntemlerle gecikmeksizin ve en kısa sürede Kişisel Veri Koruma Kuruluna, Genel Müdürlüğe ve kişisel verisi ihlal edilen kişiye bildirimde bulunur.

(2) Erişilen ve paylaşılan veriler; Genel Müdürlüğün yazılı izni olmadıkça, tarafların kendi görev ve faaliyet alanı kapsamında gerçekleştirecekleri işlemler haricinde başka kurum, kuruluş ve diğer kişilere kullanılamaz ve yayınlanamaz.

(3) TAKPAS’taki verilere erişimde kısıtlama yapmaya Genel Müdürlük yetkilidir. Verilere erişim hakkının kötüye kullanılması halinde, özel kanun hükümleri saklı kalmak üzere, sisteme erişim derhal durdurulur.

(4) Protokol hükümleri yerine getirilmediği takdirde alıcının TAKPAS’tan faydalanması geçici olarak askıya alınır. Alıcının her türlü idari ve teknik tedbirleri alması ve bu tedbirlerin Genel Müdürlükçe uygun görülmesi halinde TAKPAS’a yeniden erişimi sağlanır. Alıcı tarafından taahhüt edilen idari ve teknik güvenlik tedbirlerinin yerine getirilemediğinin Genel Müdürlükçe tespit edilmesi halinde TAKPAS kullanıma kapatılır ve protokol tek taraflı olarak feshedilir.

(5) TAKPAS’tan elde edilen verilerin ilgili mevzuat, protokol veya elektronik kabul beyanında yer alan hükümlere aykırı olarak kullanılması, hizmetten yararlanan kişi ve kurumların kendi sistem yazılımlarından kaynaklanan hatalı sorgulamaları ve güvenlik açıkları gibi sebeplerle verilerin yetkisiz kişilerce elde edilmesi ve kullanılmasından doğan her türlü hukuki, idari, mali ve cezai

sorumluluk hizmetten yararlanan kişi ve kurumlara, alt kullanıcılarına ve/veya veriyi kullananlara aittir. TAKPAS'ın her aşamasında yer alan yetkili ve görevliler protokolde belirtilen esaslara uymakla yükümlüdürler. Bu yükümlülük, kişilerin görevlerinden ayrılmalarından sonra da devam eder.

Yaptırım

MADDE 32- (1) Kişisel verilerin korunması hususu ile ilgili hükümlere aykırı hareket edenler hakkında kabahatler bakımından, 6698 sayılı Kanununun 18 inci maddesi hükümlerinin uygulanmasını teminen durum Kurula bildirilir.

(2) Kurum tarafından kendilerine erişim yetkisi verilen kişilerden, kişisel verileri değiştiren veya bütünlüğünü bozanlar hakkında 5237 sayılı Kanunun ilgili maddeleri uyarınca suç duyurusunda bulunulur.

(3) Bu Yönetmelik gereklerini yerine getirmeyen kamu görevlileri için bağlı oldukları disiplin amirliğine bildirim yapılır ve varsa yetkileri iptal edilir.

YEDİNCİ BÖLÜM

Veri Paylaşım Komisyonları

Veri Paylaşımı Üst Komisyonunun oluşumu, toplanması ve karar alınması

MADDE 33- (1) Merkezi veri tabanında yer alan bilgilerin paylaşımına ilişkin talepleri değerlendirerek veri paylaşımından yararlanacakları belirlemek, paylaşımın kapsamı ve hangi yöntemle yapılacağına karar vermek üzere Genel Müdürlük bünyesinde Veri Paylaşımı Üst Komisyonu oluşturulur.

(2) Veri Paylaşımı Üst Komisyonu; Genel Müdürün veya Bilgi Teknolojileri Dairesi Başkanlığının bağlı olduğu genel müdür yardımcısının başkanlığında, Teftiş Kurulu Başkanı, I. Hukuk Müşaviri, Strateji Geliştirme Daire Başkanı, Arşiv Dairesi Başkanı, Bilgi Teknolojileri Dairesi Başkanı, Tapu Dairesi Başkanı, Kadastro Dairesi Başkanı, Yabancı İşler Dairesi Başkanı, Harita Dairesi Başkanı ile Döner Sermaye İşletme Müdüründen oluşur. Komisyon, doğrudan Genel Müdüre bağlıdır.

(3) Komisyon; Ocak, Nisan, Temmuz ve Ekim aylarının ilk işgünü mutad olarak toplanır. Bunun haricinde de, başkanın talebi ve çağrısı üzerine Komisyon toplanabilir.

(4) Toplantıların gündemi, yeri ve saati Komisyon Başkanı tarafından belirlenir. Toplantıda görüşülecek konular ve gündeme ilişkin bilgi ve belgeler Komisyon üyelerine en az bir gün önce yazılı veya elektronik olarak iletilir.

(5) Komisyon gündemine, toplantı sırasında üyelerden herhangi birinin teklifi üzerine madde eklenebilir.

(6) Komisyon en az yedi üyenin katılımıyla toplanır. Komisyon kararları oy çokluğu ile alınır. Oylarda eşitlik olması halinde Komisyon Başkanının bulunduğu taraf çoğunluk sayılır.

(7) Karara muhalif olanlar, şerh koymak suretiyle kararı imzalarlar. Muhalif görüş gerekçesi bir sonraki Komisyon toplantısına kadar karar dosyasına eklenmek üzere sekreteryaya teslim edilir.

(8) Komisyon kararları, toplantıya katılan tüm üyeler tarafından imzalanır. İmzaların tamamlanması ve Genel Müdür onayını müteakiben karar yürürlüğe girer.

(9) Toplantılarda alınan kararlar her yıl birden başlanarak yıl sonuna kadar numaralandırılır.

(10) Gerekli görülen hallerde Komisyon Başkanının onayı ile toplantıya üyeler haricinde de oy hakkı olmaksızın katılım sağlanabilir.

(11) Komisyonun görevlerinin yerine getirilmesinde kendisine yardımcı olmak üzere Veri Paylaşımı Alt Komisyonu oluşturulur. Her iki komisyonun sekreteryaya işlemleri, Strateji Geliştirme Daire Başkanlığınca yürütülür.

Veri Paylaşımı Üst Komisyonunun görevleri

MADDE 34- (1) Veri Paylaşımı Üst Komisyonunun görevleri şunlardır:

- a) Veri paylaşım taleplerini karara bağlamak.
- b) Alıcıyla, hangi verilerin paylaşılacağına karar vermek.
- c) Toplu veri paylaşımı yapılabilecek kurumlara karar vermek.
- ç) Benzer konulardaki veri paylaşımına ilişkin ilke kararları almak.
- d) Veri paylaşımının kapsamını belirlemek ve hangi yöntemle yapılacağına karar vermek.
- e) Protokol iptali, feshi veya veri paylaşımının askıya alınmasına yönelik karar almak.
- f) Protokol konusu ücretlendirmede çıkan ihtilafların çözümünde karar vermek.

Veri Paylaşımı Alt Komisyonunun oluşumu, toplanması ve karar alınması

MADDE 35- (1) Veri Paylaşımı Alt Komisyonu, Strateji Geliştirme Daire Başkanlığının koordinasyonu ve görevlendireceği (2) iki üyeden, yine aynı başkanlıkça belirlenecek, birisinin başkanlığında; Tapu Dairesi Başkanlığından (1) bir, Kadastro Dairesi Başkanlığından (1) bir, Hukuk Müşavirliğinden (1) bir, Harita Dairesi Başkanlığından (1) bir, Arşiv Dairesi Başkanlığından (1) bir,

Yabancı İşler Dairesi Başkanlığından (1) bir, Bilgi Teknolojileri Dairesi Başkanlığından (1) bir ve Döner Sermaye İşletmesi Müdürlüğünden (1) bir üyenin görevlendirilmesi ile toplam 10 asıl üyeden oluşur. Ayrıca, Veri Paylaşımı Alt Komisyonunda temsil edilen her başkanlıkça aynı sayıda yedek üye görevlendirilir. Strateji Geliştirme Daire Başkanlığına görevlendirilecek üyelerden birinin Mali Hizmetler Uzmanı kadrosunda görevli olması zorunludur. Mali Hizmetler Uzmanı için belirlenecek yedek üyenin de aynı kadroda olması gerekir.

(2) Diğer başkanlıklar ilgisi halinde Veri Paylaşımı Alt Komisyonu başkanının daveti üzerine komisyonda temsil edilir.

(3) Veri Paylaşımı Alt Komisyonu, Başkanının uygun göreceği zamanlarda en az altı üye ile toplanır. Kararlar toplantıya katılan üyelerin çoğunluğu ile alınır. Veri Paylaşımı Alt Komisyonu Başkanının yazılı daveti üzerine komisyonda temsil edilen Başkanlıkların da oy hakkı vardır.

(4) Koordinasyon birimleri tarafından tüm alt detayları ile hazırlanan taleplerin gündeme alınıp alınmayacağına dair hazırlanan konu başlıklarını, gündeme alınması için Komisyon Başkanlığına sunmak ve toplantı tarihi ve yeri ile ilgili süreçleri takip etmek görevi Komisyon Sekreteryasına aittir.

Veri Paylaşımı Alt Komisyonunun görevleri

MADDE 36- (1) Veri Paylaşımı Alt Komisyonunun görevleri şunlardır:

- a) Veri paylaşım talepleri için Veri Paylaşımı Üst Komisyona görüş bildirmek.
- b) Protokol ve güvenlik taahhütnamesi metinlerini ve eklerini düzenlemek ve hazırlamak, gerektiğinde madde eklemek ya da çıkarmak suretiyle Veri Paylaşımı Üst Komisyonunun onayına sunmak.
- c) Veri Paylaşımı Üst Komisyonunun talep ettiği konularda rapor hazırlamak, gerektiğinde sunum yapmak.
- ç) Komisyon sekreteryasınca gündeme alınan konular hakkında görüş bildirmek.

SEKİZİNCİ BÖLÜM

Çeşitli ve Son Hükümler

Eğitim

MADDE 37- (1) Alt kullanıcılara, ihtiyaç duyulması halinde veri paylaşımına yönelik kullanılan uygulamalar ile ilgili eğitim Genel Müdürlük tarafından verilir.

Ücretlendirme

MADDE 38- (1) Bu Yönetmelik kapsamında alınacak hizmetler 8/1/2002 tarihli ve 4736 sayılı Kamu Kurum ve Kuruluşlarının Ürettikleri Mal ve Hizmet Tarifeleri ile Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun uyarınca döner sermaye hizmet bedeline tabidir.

(2) Döner sermaye hizmet bedeli, Genel Müdürlük döner sermaye tarife cetveli kapsamında belirlenir.

(3) Bu Yönetmelik kapsamında alınacak hizmetlerin karşılığında ödenecek döner sermaye hizmet bedelinin ödeme usul ve esasları protokol ile belirlenir.

(4) Kanunlardaki özel hükümler saklıdır.

Düzenleme yetkisi

MADDE 39- (1) Bu Yönetmeliğin uygulanması sırasında doğacak tereddütleri ve uygulamaya ilişkin aksaklıkları gidermeye, ilke ve standartları belirlemeye, uygulama birliğini sağlayacak gerekli düzenlemeleri yapmaya ve bu Yönetmelikte yer almayan konularda ilgili mevzuat hükümleri çerçevesinde düzenleme yapmaya Genel Müdürlük yetkilidir.

(2) 4721 sayılı Kanun, 6698 sayılı Kanun ve ilgili diğer mevzuat hükümleri uyarınca; mevzuatta yapılan düzenlemeler ve hizmet gereği duyulacak ihtiyaçlar çerçevesinde TAKPAS üzerinden paylaşılacak verileri belirlemeye Genel Müdürlük yetkilidir. TAKPAS'ın kullanılması için alıcıyla bu Yönetmeliğin Ek-2'sinde yer alan Tip Protokol yapılır.

Tapu sicil ve TAKPAS uyumlaştırılması

MADDE 40- (1) Elektronik sicile geçilen işlemler haricinde veri paylaşımı sicil tutma faaliyeti olarak değerlendirilmez. TAKPAS'taki bilgiler ile sicildeki bilgiler arasında ihtilaf olması halinde tapu sicil bilgileri esastır.

Yürürlükten kaldırılan yönetmelik

MADDE 41- (1) 7/3/2015 tarihli ve 29288 sayılı Resmî Gazete'de yayımlanan Tapu ve Kadastro Verilerinin Paylaşımı Hakkında Yönetmelik yürürlükten kaldırılmıştır.

Protokollerin uyumlaştırılması

GEÇİCİ MADDE 1- (1) Mevcut protokollerin bu Yönetmeliğe aykırı hükümlerinin olması halinde bu Yönetmelik hükümleri geçerli olup mevcut protokoller bu Yönetmeliğin yayımı tarihinden itibaren 1 (bir) yıl içerisinde bu Yönetmeliğe uygun hale getirilir.

Yürürlük

MADDE 42- (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 43- (1) Bu Yönetmelik hükümlerini Tapu ve Kadastro Genel Müdürlüğünün bağlı olduğu Bakan yürütür.

Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik

Resmî Gazete Tarihi : 01.04.2021

Resmî Gazete Sayısı : 31441

**BANKALARCA KULLANILACAK UZAKTAN KİMLİK TESPİTİ YÖNTEMLERİNE VE
ELEKTRONİK ORTAMDA SÖZLEŞME İLİŞKİSİNİN KURULMASINA İLİŞKİN
YÖNETMELİK**

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç ve kapsam

MADDE 1 - (1) Bu Yönetmeliğin amacı, bankalar tarafından yeni müşteri kazanımında kullanılacak uzaktan kimlik tespiti yöntemlerine ve müşteri kimliğinin tespit edilmesini müteakip sunulacak bankacılık hizmetlerine yönelik olarak mesafeli olsun olmasın bir bilişim veya elektronik haberleşme cihazı üzerinden yazılı şeklin yerine geçecek şekilde ya da mesafeli olarak sözleşme ilişkisinin kurulmasına yönelik usul ve esasları düzenlemektir.

(2) Uzaktan kimlik tespiti yöntemi, 11/10/2006 tarihli ve 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun ile 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ve bu Kanunlarla ilgili mevzuatta yer alan yükümlülükler saklı kalmak kaydıyla uygulanır.

Dayanak

MADDE 2 - (1) Bu Yönetmelik, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununun 76 ncı maddesinin ikinci fıkrası ile 93 üncü maddesine dayanılarak düzenlenmiştir.

Tanımlar ve kısaltmalar

MADDE 3 - (1) Bu Yönetmelikte yer alan;

- a) Açık rıza: Kişisel Verilerin Korunması Kanununda tanımlanan açık rızayı,
- b) Banka: Bankacılık Kanununun 3 üncü maddesinde tanımlanan bankaları,
- c) Beyaz ışık: Gün ışığı gibi görünürde renksiz olan ışığı,

- ç) BSEBY: 15/3/2020 tarihli ve 31069 sayılı Resmî Gazete’de yayımlanan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmeliği,
- d) Güvenlik öğeleri: Kimlik belgesinde yer alan giyoş, gökkuşağı baskı, optik deęişken mürekkep, gizli görüntü, hologram ve mikro yazıyı,
- e) Kimlik belgesi: 3/12/2019 tarihli ve 30967 sayılı Resmî Gazete’de yayımlanan Türkiye Cumhuriyeti Kimlik Kartı Yönetmeliğinde tanımlanan kimlik kartını,
- f) Kimlik Paylaşımı Sistemi: 20/8/2020 tarihli ve 2837 sayılı Cumhurbaşkanu Kararıyla yürürlüğe konulan Kimlik Paylaşımı Sistemi Yönetmeliğinde tanımlanan Kimlik Paylaşımı Sistemini,
- g) Kişi: Uzaktan kimlik tespiti yapılacak gerçek kişiyi veya gerçek kişi taciri,
- ğ) Kurul: Bankacılık Düzenleme ve Denetleme Kurulunu,
- h) MRZ: Optik karakter okuma yöntemlerini kullanarak makine okuması için biçimlendirilmiş, zorunlu ve isteğe baęlı verileri kapsayan, kimlik belgesi üzerinde yer alan sabit boyutlu alanı,
- ı) Müşteri temsilcisi: Kişinin uzaktan kimlik tespitini yapacak banka personelini,
- i) SMS OTP: BSEBY’de tanımlanan SMS OTP’yi,
- j) Yakın alan iletişimi: Elektronik cihazların güvenilir, temassız işlem yapabilmesini ve sayısal içeriğe ve/veya elektronik cihazlara erişimini mümkün kılan, veri okuma ve yazmakta kullanılan kısa menzilli kablosuz teknolojiyi,

ifade eder.

İKİNCİ BÖLÜM

Uzaktan Kimlik Tespiti Sürecine İlişkin Şartlar

Süreç başlatılmadan önce uyulması gereken genel ilkeler

MADDE 4 - (1) Uzaktan kimlik tespiti, müşteri temsilcisi ile kişinin; fiziksel olarak aynı ortamda bulunmasına gerek olmadan, çevrim içi olarak görüntülü görüşmesi ve birbiriyle iletişim kurması ile yapılır.

(2) Uzaktan kimlik tespiti yöntemi bu Yönetmelikte belirtilen şartlar dâhilinde uygulanır. Uygulanacak yöntem, yüz yüze yapılan kimlik tespiti yöntemine benzer ve asgari seviyede risk ihtiva edecek şekilde tasarlanır.

(3) Uzaktan kimlik tespitinde kullanılacak görüntülü görüşme yönteminde olası teknolojik, operasyonel ve benzeri riskler dikkate alınarak yeterli seviyede güvenlik önlemleri alınır.

(4) Uzaktan kimlik tespiti işlemi, kritik bir işlem olarak değerlendirilir ve işlemin bilgi teknolojileri veya müşteri temsilcisi tarafından tek başına başlatılması, onaylanması ve tamamlanmasına imkân vermeyecek şekilde tasarlanır ve işletilir. Sürecin kişi tarafından başlatılması, bilgi teknolojileri tarafından uygulanan kontroller ile devam ettirilmesi ve müşteri temsilcisi tarafından yapılacak onaylama ve ek kontroller ile tamamlanması sağlanır. Müşteri temsilcisi tarafından yapılan kontrollerde işlemin riskli bulunması halinde işlem ikinci bir onaya gönderilir veya sonlandırılır.

(5) Uzaktan kimlik tespitine ilişkin kullanılacak süreçler ve sistemler, BSEBY'nin 29 uncu maddesinin onuncu fıkrası kapsamında kritik bilgi sistemleri olarak değerlendirilir.

(6) Kimlik tespiti sırasında kullanılacak belgelere, bu belgelerde var olan doğrulanabilir özelliklere ve doğrulamanın yapılması sırasında kullanılacak kriterlere ilişkin detaylı dokümanlar oluşturulur.

(7) Bankanın belirlediği uzaktan kimlik tespiti sürecinin uygulanmasından önce, süreç dokümanları oluşturulur ve sürecin etkinliği test edilerek sonuçları yazılı hale getirilir. Test sonuçlarının başarılı bulunmaması durumunda süreçte gerekli güncellemeler yapılır ve sürecin etkinliği ve yeterliliği sağlanmadıkça süreç uygulanmaz.

(8) Uzaktan kimlik tespiti süreci yılda en az iki defa gözden geçirilir. Güvenlik ihlallerinin tespit edilmesi veya gerçekleşmesi, ilgili mevzuatta değişiklik yapılması, bankanın muhtemel dolandırıcılık veya sahtecilik teşkil edebilecek eylemlerden haberdar olması ve kullanılan uzaktan kimlik tespiti yöntemine ilişkin zayıflıkların ortaya çıkması gibi durumlarda teknolojik gelişmeler ve uygulamada kazanılan deneyimler dikkate alınarak sürecin ayrıca gözden geçirilmesi sağlanır ve gerekli güncellemeler yapılır.

Uzaktan kimlik tespitini yapacak müşteri temsilcisi ve çalışma ortamı

MADDE 5 - (1) Uzaktan kimlik tespitinin görüntülü görüşme aşaması, bu konuda eğitim almış müşteri temsilcisi tarafından gerçekleştirilir.

(2) Müşteri temsilcisinin, kimlik tespitinde kullanılacak belgelerin özelliklerini ve bu belgeler için uygulanan geçerli doğrulama yöntemlerini öğrenmesi ve dolandırıcılık veya sahtecilik teşkil edebilecek eylemlere, bu Yönetmelikte ve ilgili diğer mevzuatta yer alan yükümlülüklerle ilişkin bilgi sahibi olması sağlanır.

(3) Müşteri temsilcisinin, uzaktan kimlik tespiti sürecine ilişkin yılda en az bir defa ve her bir güncelleme sonrasında kişisel verilerin korunması mevzuatı da dâhil olmak üzere eğitim alması sağlanır.

(4) Müşteri temsilcisinin, kişinin banka müşterisi olma veya bankacılık hizmetlerinden yararlanma isteğini kendi iradesiyle bankadan talep ettiğine dair karar verebilmesi konusunda eğitim alması sağlanır.

(5) Uzaktan kimlik tespiti sürecinde müşteri temsilcisinin, yaşanabilecek güvenlik zafiyetlerinin ya da suistimallerin engellenmesine yönelik gerekli tedbirlerin alındığı, erişimi sınırlandırılmış ayrı alanlarda çalışması sağlanır.

(6) Kişiye güven vermesi açısından müşteri temsilcisinin banka adına çalıştığını yansıtacak şekilde uygun bir ortam oluşturulması veya yöntemler kullanılması sağlanır.

(7) Engelli kişilere hizmet verebilmek amacıyla en az bir müşteri temsilcisine gerekli eğitimlerin verilmesi sağlanır.

Sürecin başlatılması ile uyulması gereken genel ilkeler

MADDE 6 - (1) Uzaktan kimlik tespiti sürecinde görüntülü görüşme başlamadan önce kişinin başvurusu uzaktan kimlik tespiti sürecinin işletildiği banka uygulaması üzerinden elektronik ortamda doldurulan bir form ile alınır, alınan veriler kullanılarak kişi hakkında risk değerlendirmesi gerçekleştirilir. Risk değerlendirmesi sonucunda gerekiyorsa görüntülü görüşme başlatılmadan süreç sonlandırılır.

(2) Bu Yönetmelik kapsamında uygulanacak uzaktan kimlik tespiti sürecinde, kişinin uzaktan kimlik tespitinin yapılması amacıyla özel nitelikli kişisel verilerden sadece biyometrik verisi kullanılabilir ve kişinin buna dair açık rızası elektronik ortamda kayıt altına alınır.

(3) Müşteri temsilcisine uzaktan kimlik tespiti işlemleri atanırken belirli bir kişinin belirli bir müşteri temsilcisine atanması gibi önceden tahmin edilebilir durumlardan kaynaklı suistimal olasılığını azaltmak için gerekli mekanizmalar tesis edilir.

(4) Kişi ile yapılacak görüntülü görüşmeden önce müşteri temsilcisinin soracağı asgari sorular belirlenir ve sorulan soruların sırası ve/veya türü değişkenlik arz eder.

(5) Uzaktan kimlik tespitinin görüntülü görüşme aşaması gerçek zamanlı ve kesintisiz şekilde yapılır. Müşteri temsilcisi ile kişi arasındaki görsel-ışitsel iletişimin bütünlüğünün ve gizliliğinin yeterli seviyede olması sağlanır. Bu amaçla, yapılan görüntülü görüşme uçtan uca güvenli iletişim ile gerçekleştirilir.

(6) Gerçekleşen iletişimin görüntü ve ses kalitesinin, bu Yönetmelikte yer alan hükümler ve kontroller çerçevesinde şüpheye yer bırakmayacak ve kimlik tespitinde herhangi bir kısıtlamaya imkân

vermeyecek şekilde tüm görüşme esnasında yeterli seviyede olması sağlanır. Görüntü kalitesi, sunulan belgeyi beyaz ışık altında görsel olarak doğrulayabilmeye ve sunulan belgenin yıpranmamış ya da tahrif edilmemiş olduğunu kontrol edebilmeye yönelik güvenlik öğelerinin incelenmesine olanak tanır.

(7) Uzaktan kimlik tespiti sürecinde kişiye yalnızca yapılan kimlik tespiti işlemi için geçerli, merkezi olarak üretilen SMS OTP iletilir. İletilen SMS OTP'nin kişi tarafından çevrim içi olarak uygulama ara yüzü üzerinden geri gönderilmesi sağlanır. Sistemde bu SMS OTP'nin başarılı şekilde onaylanması durumunda kişinin cep telefonu numarası doğrulanmış olur.

Kullanılabilecek kimlik belgesi ve doğrulanması

MADDE 7 - (1) Uzaktan kimlik tespiti sürecinde beyaz ışık altında görsel olarak ayırt edilebilen güvenlik öğelerine, fotoğraf ve imzaya sahip olan kimlik belgesi kullanılır.

(2) Yakın alan iletişimi kullanılarak kimlik belgesinin yongası üzerinde yer alan kimlik bilgilerinin doğrulanması, kimlik belgesinden kişinin kimliğinin tespit edilmesi için gereken eşleşmenin sağlandığı anlamına gelir. Söz konusu doğrulama;

a) Kullanılan kimlik belgesinin, belgeyi çıkaran yetkili makam tarafından verildiği ve belgenin temassız yongası üzerindeki bilgilerin değiştirilmediği,

b) Kimlik belgesinin temassız yongası üzerindeki anahtarların kopyalanarak oluşturulmadığı, kontrol edilerek yapılır.

(3) Yakın alan iletişimi kullanılarak ikinci fıkrada geçen doğrulamanın herhangi bir nedenle yapılamaması halinde kimlik belgesinin sahip olduğu birinci fıkrada ifade edilen görsel güvenlik unsurlarından en az dört adedinin şekil ve içerik bakımından doğrulanması sağlanır. Sadece görsel güvenlik unsurlarının doğrulanması hallerinde banka ilave olarak kişi ile sürekli iş ilişkisi tesisi öncesinde ilk finansal hareketin, müşterinin tanınmasına ilişkin esasların uygulandığı bir başka bankadaki kişinin kendi hesabından yapılmasını zorunlu tutar.

(4) Görsel kimlik tespiti esnasında kişinin, kimlik belgesini kameranın önünde yatay veya dikey olarak eğmesi ve müşteri temsilcisinin vereceği talimata göre ilave hareketler yapması sağlanır. Bu amaçla kişiden, kimlik belgesinin güvenlikle ilgili kısımlarından sistem tarafından değişken ve rastgele şekilde belirlenen kısımlarına parmağını koyması istenir.

(5) Müşteri temsilcisi, görüntülü görüşme sürecinde kişiyi ve kişi tarafından sunulan kimlik belgesinin ön ve arka yüzü ile birlikte belgenin üzerindeki bilgileri gösteren fotoğraflar ve/veya ekran görüntüleri oluşturur.

(6) Müşteri temsilcisi, kişinin hareketlerinden alınan, kesilen ve büyütülen tekil görselleri kullanarak, beyaz ışık altında görsel olarak ayırt edilebilen tüm güvenlik öğeleri ile birlikte kimlik belgesinin doğru açıyla tam olarak kapsandığından ve kimlik belgesinin üzerindeki kısımlar arasındaki geçiş noktalarında tahrifatı ve sahteliği gösteren hiçbir yapaylık bulunmadığından emin olur.

(7) Sunulan kimlik belgesinde bulunan veri ve bilgilerin geçerliliği ve gerçekliğine ilişkin doğrulama, uzaktan kimlik tespiti sürecinin bir parçası olarak gerçekleştirilir. Bu kapsamda asgari olarak;

a) Kimlik belgesinde bulunması gereken karakterlerin yazı tipi, düzeni, sayısı, büyüklüğü, aralığı ve tipografisi gibi belgeyi çıkaran yetkili makamca tanımlanan özelliklere sahip olduğu,

b) Kimlik belgesinin zarar görmemiş, tahrif edilmemiş, değiştirilmemiş ve özellikle üzerine sonradan fotoğraf yapıştırılmamış olduğu,

c) Kimlik belgesi geçerlilik süresinin söz konusu kimlik belgesinin sahip olduğu standartlara aykırı olmadığı,

ç) Kimlik belgesinin MRZ' sinde yer alan bilgiler ile kimlik belgesine ait bilgilerin uyduğu,

d) Kişiyi ilişkin kimlik belgesinde yer alan bilgilerin banka tarafından bilinen, Kimlik Paylaşımı Sisteminden alınan ve varsa kimlik tespiti yapmak amacıyla bankanın erişimine açık olan diğer bilgiler ile eşleştiği,

e) Kimlik belgesinde yer alan seri numarasının görüntülü görüşme sırasında kimlik belgesi üzerinden kişiye okutulması suretiyle seri numarası,

doğrulanır.

Kimliği tespit edilecek kişinin doğrulanması

MADDE 8 - (1) Uzaktan kimlik tespitinin görüntülü görüşme aşamasında kişinin canlılığını tespit edici yöntemler kullanılır. Banka sahte yüz teknolojisine dair riskleri önlemeye yönelik ilave tedbirler alır.

(2) Uzaktan kimlik tespiti sürecinde kişinin yüzü ile kimlik belgesinden yakın alan iletişimi kullanılarak alınabilmesi halinde temassız yongadaki fotoğrafın, alınamaması halinde ise kimlik belgesi üzerinde yer alan fotoğrafın biyometrik karşılaştırması yapılır.

(3) Müşteri temsilcisi, kullanılan kimlik belgesindeki fotoğrafın ve kişisel bilgilerin kişi ile uyduğundan emin olur.

(4) Müşteri temsilcisi, kimlik tespiti sürecinde kişi ile kuracağı diyalog ve yapacağı gözlemler neticesinde kimlik belgesindeki bilgilerin, görüşme esnasında kişi tarafından sağlanan bilgilerin ve belirtilen niyetin inandırıcı ve yeterli olduğuna kanaat getirir. Bu kapsamda kimlik avına, sosyal mühendisliğe, başka bir tarafın zorlamasıyla baskı altında gerçekleşen hareketlere ve benzeri dolandırıcılık yöntemlerine ilişkin riskler göz önünde bulundurulur.

(5) Uzaktan kimlik tespitinin görüntülü görüşme aşamasının sonunda kişinin verilecek bankacılık hizmetleri hakkında bilgilendirilmesi ve banka müşterisi olacağını kabul ettiğine ilişkin sözlü onay alınması ile süreç tamamlanmış olur.

Görüntülü görüşmede sürecin sonlandırılması

MADDE 9 - (1) Zayıf ışık koşulları, düşük görüntü kalitesi ya da iletimi ve benzeri durumlar nedeniyle bu Yönetmelikte belirtildiği şekilde görsel doğrulama yapılmasının ve/veya kişi ile sözlü iletişim kurmanın mümkün olmadığı hallerde uzaktan kimlik tespitinin görüntülü görüşme aşaması sonlandırılır. Süreçte başkaca bir tutarsızlık veya belirsizlik bulunması durumunda da bu hüküm uygulanır.

(2) Uzaktan kimlik tespitinin görüntülü görüşme aşamasında kişi tarafından sunulan belgenin geçerliliği hususunda ya da dolandırıcılık veya sahtecilik teşkil edebilecek eylemlerden şüphe edilmesi durumunda, uzaktan kimlik tespiti süreci sonlandırılır.

Verilerin kaydedilmesi ve saklanması

MADDE 10 - (1) Uzaktan kimlik tespiti sürecinin tamamı, sürecin tüm adımlarını içerecek ve denetlenebilir olmasını sağlayacak şekilde kayıt altına alınır ve saklanır. Bilgi ve belge saklama gerekliliklerine ilişkin ilgili mevzuat hükümleri saklıdır.

Uzaktan kimlik tespitinde sorumluluk

MADDE 11 - (1) Uzaktan kimlik tespiti için kullanılan çözümlerin kişiyi yanlış tespit riskini en aza indirecek şekilde kullanılmasını sağlamak bankanın sorumluluğundadır. Banka uzaktan kimlik tespiti ile kimlik tespiti yaptığı kişileri farklı bir risk profilinde izler. Bu kişilerce yapılan işlemin türüne ve tutarına bağlı olarak ilave güvenlik ve kontrol yöntemleri uygulanır. Kişilere ya da üçüncü bir tarafa yükümlülük doğuran işlemlerde itiraz halinde ispat yükümlülüğü bankadadır.

(2) Bu Yönetmelikte yer alan şartlar dâhilinde uzaktan kimlik tespitinin yapılması halinde BSEBY'nin kimlik doğrulamaya ilişkin 34 üncü maddesinin birinci fıkrasının gerekleri yerine getirilmiş sayılır.

(3) Bankanın BSEBY'de ve bu Yönetmelikte yer alan hükümlere uyum durumunun, şikâyetler ile sahtecilik veya dolandırıcılık teşkil edebilecek eylemlerin değerlendirilmesi neticesinde ve gerekli görülen diğer hallerde uzaktan kimlik tespiti kullanımını kısıtlamaya veya durdurmaya Kurul yetkilidir.

ÜÇÜNCÜ BÖLÜM

Elektronik Ortamda Sözleşme İlişkisinin Kurulması

Kimlik tespitini müteakip sözleşme ilişkisinin kurulması

MADDE 12 - (1) Bu Yönetmelikte yer alan şartlar dâhilinde uzaktan kimlik tespitinin yapılmasını ya da şubeler aracılığıyla müşteri kimliğinin yüz yüze tespit edilmesini müteakiben, BSEBY'de düzenlenen internet bankacılığı ya da mobil bankacılık dağıtım kanallarından herhangi biri kullanıma açık olan müşterilerce gerçekleştirilmek istenen işlemlere yönelik sözleşme ilişkisinin mesafeli olarak kurulması durumunda, müşterinin sözleşmeyi kuran irade beyanının BSEBY'nin 34 üncü maddesinin birinci fıkrasına uygun olarak gerçekleştirilmiş bir kimlik doğrulama sonrasında söz konusu dağıtım kanalları üzerinden alınması şarttır.

(2) Bu Yönetmelikte yer alan şartlar dâhilinde uzaktan kimlik tespitinin yapılmasını ya da şubeler aracılığıyla müşteri kimliğinin yüz yüze tespit edilmesini müteakiben, mesafeli olsun olmasın, müşterilerce gerçekleştirilmek istenen işlemlere yönelik olarak bir bilişim veya haberleşme cihazı üzerinden yazılı şeklin yerine geçecek nitelikte bir sözleşme ilişkisi kurulabilmesi için;

a) Söz konusu sözleşmenin bütün şartlarının, müşterinin okuyabileceği şekilde internet bankacılığı ya da mobil bankacılık dağıtım kanalları üzerinden müşteriye iletilmesi,

b) (a) bendine göre müşteriye iletilen sözleşme ve bu sözleşme ile birlikte müşterinin sözleşmeyi kuran irade beyanının, BSEBY'nin 38 inci maddesinin üçüncü fıkrası ile 39 uncu maddesinin birinci fıkrasında belirtilen müşteriye özgü şifreleme gizli anahtarı ile imzalanarak bankaya iletilmesi,

c) (a) bendine göre iletilen sözleşmede müşteriye sözleşme içeriği olarak hangi bilgiler gösterilmiş ise

(b) bendine göre müşteri tarafından yalnızca o bilgilerin imzalanmasının sağlanması,

şarttır.

(3) Müşteriye sunulacak bankacılık hizmetlerine yönelik olarak banka ile müşteri arasındaki ilişkileri düzenleyen ve resmi şekle veya özel bir merasime tabi olmayan her türlü sözleşmenin;

a) İkinci fıkraya uygun olarak elektronik ortamda kurulması ya da

b) Müşterinin sözleşmeyi kuran irade beyanının uzaktan kimlik tespitinin görüntülü görüşme aşamasında kimlik tespitini müteakip alınması suretiyle mesafeli olarak kurulması,

hallerinde, bu sözleşmeler için yazılı şekil şartı gerçekleşmiş sayılır.

DÖRDÜNCÜ BÖLÜM

Son Hükümler

Yürürlük

MADDE 13 - (1) Bu Yönetmelik 1/5/2021 tarihinde yürürlüğe girer.

Yürütme

MADDE 14 - (1) Bu Yönetmelik hükümlerini Bankacılık Düzenleme ve Denetleme Kurumu Başkanı yürütür.

Vakıflar Yönetmeliđi

Resmî Gazete Tarihi : 27.09.2008

Resmî Gazete Sayısı : 27010

VAKIFLAR YÖNETMELİĐİ

BİRİNCİ KISIM

Genel Hükümler

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç ve kapsam

MADDE 1 - (Deđişik:RG-10/11/2013-28817)

(1) Bu Yönetmelik; yeni vakıfların kuruluşu, vakıfların yönetimi, faaliyetleri, denetimlerine ilişkin usûl ve esaslar ile Vakıflar Meclisi, Rehberlik ve Teftiş Başkanlığı, Vakıf Uzmanlığı ve Uzman Yardımcılığı, Hukuk Müşavirliği ve Avukatlık ile ilgili görev, yetki ve sorumlulukların düzenlenmesi amacıyla hazırlanmıştır.

Dayanak

MADDE 2 - (Deđişik:RG-10/11/2013-28817)

(1) Bu Yönetmelik 20/2/2008 tarihli ve 5737 sayılı Vakıflar Kanunu, 657 sayılı Devlet Memurları Kanununun Ek 41 inci maddesi ve 18/3/2002 tarihli ve 2002/3975 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan Kamu Görevlerine İlk Defa Atanacaklar İçin Yapılacak Sınavlar Hakkında Genel Yönetmeliđin Ek 6 ncı maddesine dayanılarak hazırlanmıştır.

(...)

Yoklama

MADDE 70 -(Deđişik:RG-30/9/2021-31614)

(1) Genel Müdürlük ve Bölge Müdürlükleri; aşevi ve kuru gıda yardımı başvurularını değerlendirirken ve yardım alanların kontrollerini sağlarken, yardım alanların ve aile bireylerinin beyan ettiđi bilgilerin doğruluđunu kontrol eder, söz konusu kontrollerde başvuru yapanlar, yardım

alanlar ve aile bireylerinin kişisel verilerini 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuatı kapsamında işleyebilir ve gerçeğe aykırı bir durum tespit edilmesi halinde başvuru veya yardımları iptal eder.

(2) Aşevi veya kuru gıda yardımı hizmetinden yararlanma süresi aralıksız 5 yıl ile sınırlıdır.

(...)

Verilerin işlenmesi ve takip

MADDE 79 - (Başlığı ile Birlikte Değişik:RG-30/9/2021-31614)

(1) Genel Müdürlük ve Bölge Müdürlükleri; muhtaç aylığı başvurularını değerlendirirken ve aylık alanların kontrollerini sağlarken, aylık alanların ve aile bireylerinin beyan ettiği bilgilerin doğruluğunu kontrol eder, söz konusu kontrollerde başvuru yapanlar, aylık alanlar ve aile bireylerinin kişisel verilerini 6698 sayılı Kanun ve ilgili mevzuatı kapsamında işleyebilir ve gerçeğe aykırı bir durum tespit edilmesi halinde başvuru veya aylık ödemesini iptal eder.

(2) Aylık alanlar banka hesaplarından aylıkları çektiklerini gösteren hesap ekstrelerini her yıl Kasım ayında Bölge Müdürlüğü'ne ulaştırırlar. Aylıkların aralıksız üç ay çekilmediği görülenlerin aylıkları kesilebilir.

(...)

DÖRDÜNCÜ BÖLÜM

Eğitim Yardımı

Eğitim yardımı

MADDE 82 - (Değişik:RG-12/9/2020-31242)

(1) Vakfiyelerde yer alan hayır şartlarının yerine getirilmesi amacıyla, ailelerinin maddi durumu yeterli olmayan, Millî Eğitim Bakanlığına bağlı resmi okullarda örgün eğitim gören öğrencilere eğitim yardımı yapılabilir.

(2) Aynı aileden sadece bir öğrenciye eğitim yardımı verilir.

(3) Genel Müdürlükten muhtaç aylığı alanlar, kamu kurum ve kuruluşlarınca bakım altına alınan, eğitim desteği ya da burs alan öğrenciler ile özel okulda okuyan öğrencilere eğitim yardımı yapılmaz.

(4) Eğitim yardımı verilecek öğrenci sayısı ve illere göre dağılımı, miktarı, yıllık artış oranı, ödeme zamanları ve bursun verilmesine ilişkin diğer hususlar Genel Müdürlükçe belirlenir.

(5) Bu Yönetmelikte eğitim yardımları ile ilgili hüküm bulunmayan hususlarda, karar almaya Genel Müdürlük yetkilidir.

Başvuru

MADDE 83 - (Değişik:RG-12/9/2020-31242)

(1) Başvurular EK-15'te yer alan formun doldurulması suretiyle yapılır.

(2) Eğitim yardımından faydalanmak isteyen öğrenciler her eğitim yılının başında Genel Müdürlükçe belirlenen tarihler arasında başvuru yaparlar. Başvuru şekli ve zamanı Genel Müdürlüğün internet sitesi üzerinden başvuru başlama tarihinden en az onbeş gün önce duyurulur.

(3) Genel Müdürlük tarafından belirlenen başvuru tarihleri arasında başvuru beyanı değiştirilebilir. Başvuru süresi sonunda başvuru beyanında değişiklik yapılamaz.

İstenen belgeler

MADDE 84 - (Değişik:RG-12/9/2020-31242)

(1) Eğitim yardımından faydalanmak isteyen öğrencilerden, başvuru sırasında herhangi bir belge istenmez; ancak gerekmesi halinde başvuru değerlendirme işlemleri sırasında başvuru beyanını kanıtlayıcı belge talebinde bulunulabilir. Talep edilen belgeyi zamanında göndermeyen öğrencinin başvurusu iptal edilir.

(2) Başvuru yapıldıktan sonra öğrenciye bakmakla yükümlü kişiler tarafından burs başvurusunun iptal edilmesi talebinin Genel Müdürlüğe yazılı olarak bildirilmesi halinde burs başvurusu iptal edilir.

Başvuruların değerlendirilmesi

MADDE 85 - (Değişik:RG-12/9/2020-31242)

(1) Eğitim yardımı başvurusunda bulunan öğrencilerin başvuruları EK-16'da yer alan değerlendirme cetveline göre puanlanır ve her başvuru ili için ayrı ayrı sıralanır.

(2) Birinci fıkrada oluşan sıralamada; başvuru puanı eşit olan öğrencilerden sınıfı küçük olan öğrenciler, yine eşitlik olması halinde yaşı küçük olan öğrenciler, yine eşitlik olması halinde okuyan kardeş sayısı fazla olan öğrenciler, yine eşitlik olması halinde ise başvuru zamanı önce olan öğrenciler sıralamada önde yer alır.

(3) Burs başvurusunda bulunan öğrenci, başvuru süreleri içerisinde başvuru beyanını değiştirmiş ise puanı eşit olan başvuruların sıralanmasında dikkate alınan başvuru zamanı başvurusunu en son değiştirdiği zaman olarak alınır.

(4) Başvuru değerlendirmeleri illerdeki açık kadrolar nispetinde birinci, ikinci ve üçüncü fıkralarda belirtilen sıralamaya göre yapılır.

(5) Başvuru değerlendirme işlemi sonrasında her ile ait açık kadro sayısı kadar asıl ve yedek öğrenci listeleri oluşturulur. Asıl listede boşalma olduğu takdirde yedek listedeki sıraya göre eğitim yardımı verilir. Asıl ve yedek listeler, içinde bulunulan eğitim yılı için geçerlidir.

(6) Genel Müdürlük ve Bölge Müdürlükleri; eğitim yardımı başvurularını değerlendirirken başvuru sahibi öğrencilerin ve aile bireylerinin beyan ettiği bilgilerin doğruluğunu kontrol eder, söz konusu kontrollerde başvuru yapan öğrenci ve aile bireylerinin kişisel verilerini 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında işleyebilir ve gerçeğe aykırı bir durum tespit edilmesi halinde eğitim yardımı başvurusunu iptal eder.

(7) Başvuru sonuçları Genel Müdürlüğün internet sitesi üzerinden açıklanır ve en az bir ay süre ile sorgulanabilir.

(8) Eğitim yardımı almaya hak kazanamayan öğrenciler, sonuçların Genel Müdürlüğün internet sitesi üzerinden duyurulduğu tarihten itibaren onbeş gün içerisinde başvuru sonuçlarının incelenmesini isteyebilirler.

Eğitim yardımı verilme süresi

MADDE 86 - (Değişik:RG-12/9/2020-31242)

(1) Eğitim yardımı almaya hak kazanan öğrenciye, öğrencilik halinin devamı ve eğitim yardımı almasına engel bir durumun olmaması koşuluyla ilkokul birinci sınıftan başlayarak yükseköğrenim eğitimine kadar eğitim yardımı verilir. Öğrencinin başka bir ilde bulunan okula naklini yaptırması halinde eğitim yardımı aynı Bölge Müdürlüğünce ödenmeye devam edilir.

Öğrencinin takibi ve eğitim yardımının kesilmesi

MADDE 87 - (Başlığı ile Birlikte Değişik:RG-12/9/2020-31242)

(1) Bölge Müdürlükleri, eğitim yardımı alan öğrencinin öğrencilik halinin devam edip etmediğini her yıl tespit eder.

(2) Öğrenciliğin sona ermesi veya sınıf tekrarı olması halinde eğitim yardımı kesilir. Ancak, sağlık sebebiyle öğrenim süresinin uzadığına ilişkin rapor ibrazı halinde eğitim yardımı devam eder.

- (3) Örgün eğitim görmediği tespit edilen öğrencilerin eğitim yardımı kesilir.
- (4) Millî Eğitim Bakanlığına bağlı özel okullara kayıt yaptıran öğrencilerin eğitim yardımı kesilir.
- (5) Eğitim yardımı almaktan vazgeçen öğrencilerin eğitim yardımı kesilir.
- (6) Genel Müdürlük ve Bölge Müdürlükleri; eğitim yardımı alan öğrencilerin bu Yönetmelik kapsamında eğitim yardımının devamı için gerekli kontrolleri yapar, söz konusu kontrollerde eğitim yardımı alan öğrencilerin ve aile bireylerinin kişisel verilerini 6698 sayılı Kanun kapsamında işleyebilir ve eğitim yardımı almaya engel bir durum tespit edilmesi halinde eğitim yardımını keser.
- (7) Bursun kesilmesine ilişkin itirazlar Bölge Müdürlüğünün burs kesme işleminin bildirim tarihinden sonra onbeş gün içerisinde öncelikle ilgili Bölge Müdürlüğüne yapılır. Bölge Müdürlüğüne yapılan itirazdan bir sonuç alınamaz ise burs kesme işleminin bildirim tarihinden sonraki otuz gün içerisinde yazılı ya da elektronik ortamda Genel Müdürlüğe itirazda bulunulabilir.
- (8) Eğitim yardımı alan öğrenciye bakmakla yükümlü kişiler, öğrencinin burs almaya devam ettiği süre içerisinde iletişim bilgilerinde, eğitim kurumu ve eğitim durumundaki değişiklikler ile diğer kamu kurumlarından sonradan almaya hak kazandığı bursları bir ay içerisinde ilgili Bölge Müdürlüğüne bildirmekle yükümlüdürler.
- (9) Eğitim yardımı alan öğrenciye bakmakla yükümlü kişiler, öğrencinin burs almaya devam ettiği süre içerisinde Genel Müdürlük veya ilgili Bölge Müdürlüğü tarafından istenen bilgi ve belgeleri zamanında ve eksiksiz olarak tamamlamakla yükümlüdürler.

Başarı desteği

MADDE 88 - (Başlığı ile Birlikte Değişik:RG-12/9/2020-31242)

- (1) Bu Yönetmelik uyarınca eğitim yardımı almakta olan öğrencilerden bir önceki eğitim yılının her iki döneminde takdir belgesi alanlara bu Yönetmelik hükümleri doğrultusunda bir eğitim yılında verilen toplam eğitim yardımı miktarını geçmeyecek şekilde Genel Müdürlük tarafından bütçe imkanları doğrultusunda belirlenen tutarda başarı desteği verilebilir.
- (2) Bu Yönetmelik uyarınca eğitim yardımı almakta olan öğrencilerden dört eğitim yılının her döneminde üst üste takdir belgesi alanlara bu Yönetmelik hükümleri doğrultusunda bir eğitim yılında verilen toplam eğitim yardımı miktarının iki katını geçmeyecek şekilde miktarı Genel Müdürlük tarafından bütçe imkanları doğrultusunda belirlenen tutarda başarı desteği verilebilir.
- (3) Bu Yönetmelik kapsamında ilk kez eğitim yardımı almaya hak kazanan öğrencilere başarı desteği verilmez.

(...)

Sözlü sınav süreci, değerlendirilmesi ve sonuçların tutanağa bağlanması

MADDE 139 - (1) Sözlü sınavlar, yazılı sınav gruplarına giren konularda yapılır. Ayrıca bu sınavlarda adayların temsil ve ifade kabiliyeti, tavır ve davranışları gibi kişisel nitelikleri göz önünde bulundurulur.

(2) Sözlü sınavda grupların tümü için adaylara sınav kurulu üyelerinin her biri tarafından 100 tam puan üzerinden not verilir. Verilen bu notların ortalaması sözlü sınav puanını teşkil eder. Sözlü sınavda başarılı sayılmak için sözlü sınav puanının en az 65 olması şarttır.

(3) Sınav kurulu yazılı ve sözlü sınav sonuçlarını ayrı ayrı bir tutanağa bağlar.

Türkiyede Oturan Yabancıların Nüfus Kayıtlarının Tutulması Hakkında Yönetmelik

Resmî Gazete Tarihi : 20.10.2006

Resmî Gazete Sayısı : 26325

TÜRKİYEDE OTURAN YABANCILARIN NÜFUS KAYITLARININ TUTULMASI HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1- (1) Bu Yönetmeliğin amacı; Türkiye’de herhangi bir amaçla en az altı ay süreli yabancılara mahsus ikamet tezkeresi alan yabancıların kimlik bilgilerinin ve beyan edecekleri nüfus olaylarının yabancılar kütüğünde tutulmasına ilişkin esas ve usulleri düzenlemektir.

Kapsam

MADDE 2- (1) Bu Yönetmelik, Türkiye’de herhangi bir amaçla en az altı ay süreli ikamet eden yabancıların kayıtlarının tutulmasına ilişkin yabancılar kütüğünün ve bu kütüğe yazılacak bilgilere dayanak olan belgelerden meydana gelen özel kütüklerin oluşturulmasına ve düzenlenmesine ilişkin hükümleri kapsar.

Dayanak

MADDE 3- (1) Bu Yönetmelik, 25/4/2006 tarihli ve 5490 sayılı Nüfus Hizmetleri Kanununun 8 inci ve 69 uncu maddelerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4- (1) Bu Yönetmelikte geçen;

- a) Aile : Aynı soydan olup, bir aile sıra numarası altında kayıtlı olan kişiler ile onların eş ve çocuklarını,
- b) Bakanlık: İçişleri Bakanlığını,
- c) Genel Müdürlük: Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünü,

- ç) İkamet tezkeresi:15/7/1950 tarihli 5683 sayılı Yabancıların Türkiye’de İkamet ve Seyahatleri Hakkında Kanun uyarınca Türkiye’de ikametleri uygun görülen yabancılara verilen izin belgesini,
- d) Merkezi veri tabanı: Genel Müdürlükte elektronik ortamda tutulan aile kütüğü kayıtlarını,
- e) Nüfus müdürlüğü: İlçe nüfus müdürlüğünü,
- f) Nüfus olayı : Doğum, ölüm, evlenme, boşanma, evlat edinme, tanıma, kayıt düzeltme, soybağının düzeltilmesi, gaiplik gibi kişisel durumda değişiklik meydana getiren olayı,
- g) Yabancı: 11/2/1964 tarihli ve 403 sayılı Türk Vatandaşlığı Kanununa göre Türk vatandaşı sayılmayan kişiyi,
- ğ) Yabancılar kütüğü: Türkiye’de herhangi bir amaçla en az altı ay süreli Yabancılara Ait İkamet Tezkeresi verilen yabancıların kayıtlarının tutulduğu kütüğü,
- h) Yabancılar veri giriş formu: Yabancıların nüfus olaylarının kütüğe işlenmesine dayanak olan belgeyi,
- ifade eder.

İKİNCİ BÖLÜM

Kayıtların Tutulmasına İlişkin Esaslar

Yabancılara kimlik numarası verilmesi

MADDE 5- (1) Yabancılar kütüğünde kayıtlı bulunan kişilerin kaydına ulaşmak, nüfus kayıtları arasında bağ kurmak, kamu kuruluşlarında yabancılarla ilgili olarak tutulan kayıtları ilişkilendirmek ve kimlik numaralarının zorunlu tutulduğu diğer işlemlerde karşılaşılabilecekleri sıkıntıları gidermek amacıyla yabancılar kimlik numarası verilir.

(2) Yabancı kişiler adına düzenlenecek ikamet tezkeresi ve bu Yönetmelikte kullanılacak formlarda yabancılar kimlik numarasına yer verilir.

(3) Yabancılar kimlik numarası, kurumlar ile diğer gerçek ve tüzel kişilerin her türlü işlem ve kayıtlarında esas alınır.

Yerleşim yeri esası

MADDE 6 - (1) Yabancıların nüfus olaylarına ilişkin işlemler, yerleşim yerinin bulunduğu nüfus müdürlüğünde yürütülür.

Aile esası

MADDE 7- (1) Bir ailenin çocukları, erkek çocuklarının eş ve çocukları ile kız çocuklarının evlilik dışı dünyaya gelmiş çocukları yabancılar kimlik numarası ile birbirleriyle ilişkilendirilir.

Nüfus kayıtlarının kapatılması ve yeniden açılması

MADDE 8 - (1) Yabancılar kütüğünde kayıtlı kişilerin ölmeleri, gaipliklerine karar verilmesi ya da Türkiye'den ayrılmaları halinde nüfus kayıtları kapatılır.

(2) Kaydın kapatılmasına ilişkin sebep ortadan kalktığında veya kaydın yeniden açılmasını gerektirecek yeni bir sebep ortaya çıktığında kayıt yeniden açılır.

Nüfus olaylarının bildirim yükümlülüğü

MADDE 9- (1) Nüfus kayıtları tutulan yabancılar kendileri ile ilgili nüfus olaylarını, yerleşim yeri adreslerini ve bunlardaki değişiklikleri, yerleşim yeri nüfus müdürlüğüne bildirmekle yükümlüdürler. Nüfus müdürlüklerince gerekli işlemler yapılarak, bu değişiklikler yabancılar kütüğüne işlenir.

Nüfus olaylarının bildiriminde kullanılacak belgeler

MADDE 10 - (1) Yabancılar kütüğünde kayıtlı olanların kişisel durumlarına ilişkin olarak kişi veya ilgili kurumlarca nüfus müdürlüğüne intikal ettirilen doğum, ölüm, evlenme, boşanma, evliliğin iptali, evliliğin feshi, gaiplik, tanıma, mahkeme kararıyla babalığa hüküm ve evlat edinme olaylarına ilişkin belgeler nüfus müdürlüğüne kabul edilerek, ilgili veri giriş formu kullanılmak suretiyle kayıtlarına işlenir.

Yabancılar kütüğünde bulunması gereken bilgiler ve ilk bildirim

MADDE 11 - (1) Yabancılar kütüğü; aile bireylerinin kimlik numarası, cinsiyeti, adı, soyadı, baba ve analarının ad ve soyadları ile uyruğu, sağ olup olmadıkları, doğum yeri ve tarihi, medeni hali, diğer kişisel durum değişiklikleri ile adresini kapsar.

(2) Yabancılara ait kimlik bilgileri Emniyet Genel Müdürlüğüne elektronik ortamda Genel Müdürlüğe bildirilir. Gönderilen bilgiler merkezi veri tabanında tutulur.

Veri giriş formu

MADDE 12- (1) Yabancıların kayıtları ilçe esasına göre ve veri giriş formuna zincirleme sıra numarası verilmek suretiyle tutulur. Zincirleme sıra numarasının birden fazla yılı kapsayacak şekilde kullanılmasına ve yabancılar veri giriş formunun iki örnek tutulmasına karar vermeye Bakanlık yetkilidir.

Soybağına ilişkin esaslar

MADDE 13- (1) Yabancılar kütüğünde kayıtlı ana ile Türk vatandaşı babadan evlilik dışında doğan çocuk, yabancılar kütüğüne annenin bildireceği baba adı ile yazılır. Çocuk ile anası arasında yabancı kimlik numaraları ile bağ kurulur. Ana ve babanın evlenmesi veya baba tarafından tanınması ya da mahkeme kararıyla babalığa hükmedilmesi halinde; çocuğun yabancılar kütüğündeki kaydı kapatılır. Çocuğun kaydı babasının kayıtlı bulunduğu haneye nüfus mevzuatı uyarınca tescil edilerek Türkiye Cumhuriyeti kimlik numarası verilir. Çocuğun kapatılan kaydı ile baba hanesindeki kaydı arasında bağ kurulur.

(2) Türk anadan evlilik dışı doğan, anasının aile kütüğüne ananın kızlık soyadı ve beyan ettiği baba adıyla kayıtlı olan çocuğun anasının, yabancılar kütüğünde kayıtlı baba ile evlenmesi veya çocuğun baba tarafından tanınması ya da mahkeme kararıyla babalığına hükmedilmesi halinde; olay nüfus mevzuatı hükümlerine göre çocuğun kaydına işlenir. Yabancılar kütüğünde kayıtlı bulunan babanın kaydına da yabancılar veri giriş formu ile olay işlendikten sonra baba ile çocuk arasında bağ kurulur.

(3) Yabancılar kütüğünde çocuğu ile birlikte kayıtlı bulunan ananın, yabancılar kütüğünde kayıtlı bulunan baba ile evlenmesi veya çocuğun baba tarafından tanınması ya da mahkeme kararıyla babalığa hükmedilmesi halinde; olay ilgililerin kayıtlarına yabancılar veri giriş formu ile işlenerek, yabancılar kimlik numaraları vasıtası ile aralarında gerekli bağlar kurulur. Çocuğun baba adının veya soyadının düzeltilmesi gerekiyor ise gerekli düzeltme yapılır.

(4) Yabancılar kütüğünde kayıtlı ana veya babanın, yabancılar kütüğünde kayıtlı olmayan yabancı ile evlenmesi veya yabancılar kütüğünde kayıtlı bulunan çocuğunun yabancılar kütüğünde kayıtlı bulunmayan yabancı tarafından tanınması ya da mahkeme kararıyla babalığa hükmedilmesi halinde, olay ilgililerin kayıtlarına yabancılar veri giriş formu ile işlenerek, gerekli açıklama yapılır.

ÜÇÜNCÜ BÖLÜM

Nüfus Olaylarının Yabancılar Kütüğüne İşlenmesi

Doğum

MADDE 14- (1) Yabancılar kütüğünde kayıtlı bulunan kişinin doğum bildiriminde bulunması halinde, çocuğunun kaydı yabancılar veri giriş formu ile kütüğe işlenir. Çocuk ile doğum bildiriminde bulunan ana veya baba arasında yabancılar kimlik numarası vasıtası ile bağ kurulur.

(2) Doğum bildirimlerinde veri giriş formu bildirimde bulunana imza ettirilir. Diğer nüfus olaylarında o olayın meydana geldiğini gösterir belgelerin asılları veya noter tasdikli Türkçe'ye

çevrilmiş örnekleri veri giriş formuna eklenir. Yabancılar veri giriş formu, düzenleyen memur tarafından imza edilip, nüfus müdürünce onaylandıktan sonra özel kütüğe takılır.

Evlenme

MADDE 15- (1) Evlenme ile ilgili belgenin nüfus müdürlüğüne intikal etmesi halinde;

a) Her iki kişi de yabancılar kütüğünde kayıtlı ise evlenme, yabancılar veri giriş formu ile kayıtlarına işlenerek, yabancılar kimlik numaraları ile kayıtlar arasında eş bağı kurulur.

b) Eşlerden biri Türk aile kütüklerinde kayıtlı ise evlenme, Türk olan kişinin kaydına nüfus mevzuatına göre işlenir. Yabancılar kütüğünde kaydı tutulan diğer kişinin evlenmesi yabancılar veri giriş formu ile işlenerek, evlenmiş olduğu Türk vatandaşının Türkiye Cumhuriyeti kimlik numarası belirtilmek suretiyle eş bağı kurulur.

c) Eşlerden biri yabancılar kütüğünde kayıtlı değil ise evlenme, yabancılar kütüğünde kayıtlı bulunan kişinin kaydına yabancılar veri giriş formu ile işlenerek, evlendiği kişinin uyruk ve kimlik bilgileri açıklama alanına yazılır.

Boşanma

MADDE 16- (1) Boşanma kararlarının nüfus müdürlüğüne intikal etmesi halinde;

a) Her iki kişi de yabancılar kütüğünde kayıtlı ise boşanma, yabancılar veri giriş formu ile kayıtlarına işlenir.

b) Eşlerden biri yabancılar kütüğünde, diğeri Türk aile kütüklerinde kayıtlı ise, Türk olan kişinin kaydına nüfus mevzuatına göre, yabancılar kütüğünde kaydı tutulan kişinin kaydına da yabancılar veri giriş formu ile boşanma işlenir.

c) Eşlerden biri yabancılar kütüğünde kayıtlı değil ise, yabancılar kütüğünde kayıtlı bulunan kişinin kaydına yabancılar veri giriş formu ile boşanma işlenir.

Evliliğin feshi veya iptali

MADDE 17- (1) Evliliğin feshine veya iptaline ilişkin kararların nüfus müdürlüğüne intikal etmesi halinde, 16 ncı maddeye göre işlem yapılır.

Evlat edinme

MADDE 18- (1) Yabancılar kütüğünde kayıtlı olan kişilerin evlat edinmeleri veya evlat edinilmeleri halinde aşağıdaki işlemler yapılır.

a) Yabancılar kütüğünde kayıtlı bulunan kişi veya karı koca tarafından yabancılar kütüğünde kayıtlı bulunan çocuğun evlat edinilmesi halinde; evlat edinme olayı ilgililerin kayıtlarına yabancılar veri giriş formu ile işlenir ve yabancı kimlik numaraları vasıtasıyla aralarında gerekli bağlar kurulur.

b) Yabancılar kütüğünde kayıtlı bulunan kişi veya karı koca tarafından yabancılar kütüğünde kayıtlı olmayan yabancı bir çocuğun evlat edinilmesi halinde; evlat edinme olayı yabancılar kütüğünde kayıtlı bulunan kişilerin kayıtlarına yabancılar veri giriş formu ile işlenir ve kayıtlarına gerekli açıklama yapılır.

c) Yabancılar kütüğünde kayıtlı bulunan kişi veya karı koca tarafından Türk vatandaşı olan çocuğun evlat edinilmesi halinde; evlat edinme olayı yabancılar kütüğünde kayıtlı bulunan kişilerin kayıtlarına yabancılar veri giriş formu ile işlenir. Evlat edinen yabancılar kütüğünde kayıtlı kişiler ile Türk vatandaşı çocuk arasında bağ kurulur. Türk vatandaşı çocuğun kaydına da nüfus mevzuatı uyarınca evlat edinme olayı işlenerek, evlat edinenler ile arasında bağ kurulur.

ç) Türk vatandaşı kişi veya karı koca tarafından yabancılar kütüğünde kayıtlı bulunan çocuğun evlat edinilmesi halinde; evlat edinme olayı evlat edinen Türk vatandaşı kişilerin kaydına nüfus mevzuatına göre, yabancılar kütüğünde kayıtlı bulunan çocuğun kaydına da yabancılar veri giriş formu ile işlenir ve ilgililerin kayıtları arasında gerekli bağ kurulur.

d) Yabancılar kütüğünde kayıtlı bulunan çocuğun, yabancılar kütüğünde kayıtlı olmayan yabancı kişi veya karı koca tarafından evlat edinilmesi halinde; evlat edinme olayı çocuğun kaydına yabancılar veri giriş formu ile işlenerek gerekli açıklama yapılır.

Ölüm

MADDE 19- (1) Ölüme ilişkin belgenin nüfus müdürlüğüne intikal etmesi halinde; yabancılar veri giriş formu ile ölüm olayı kişinin kaydına işlenir.

(2) Ölen kişi evli ve eşi de yabancılar kütüğünde kayıtlı ise sağ olan eşin medeni hali, yabancılar veri giriş formu ile düzeltilir.

(3) Ölen kişinin eşi Türk vatandaşı ise sağ olan eşin medeni hali, nüfus mevzuatındaki hükümlere göre düzeltilir.

Gaiplik

MADDE 20- (1) Gaiplik kararlarının nüfus müdürlüğüne intikal etmesi halinde 19 uncu maddeye göre işlem yapılır.

Maddi hataların düzeltilmesi

MADDE 21- (1) Yabancılar veri giriş formunun düzenlenmesine esas olan dayanak belgesi ile veri giriş formu arasındaki farklılık, işlemin dayanağı olan belgeye göre düzeltilir.

(2) Kütüğe kayıtlı kişilerin kimlik bilgilerinin ilgili kişi veya emniyet makamlarınca yanlış olduğunun bildirilmesi halinde, yanlış olan kimlik bilgileri nüfus mevzuatının öngördüğü usule göre yabancılar veri giriş formu ile düzeltilir ve yabancının ikamet ettiği il emniyet müdürlüğüne de bilgi verilir.

Adres

MADDE 22- (1) Yabancılar, yerleşim yeri adreslerine ilişkin değişiklikleri yirmi iş günü içinde nüfus müdürlüğüne bildirirler. Yabancılar kütüğünde kayıtlı bulunan kişinin adres değişikliği yabancı veri giriş formu ile güncellenir.

DÖRDÜNCÜ BÖLÜM

Kayıt Örneği ve Bilgi Verilmesi

Kayıt örneklerinin verilmesi ve geçerlilik süresi

MADDE 23- (1) İlgilisi ya da kurum veya kuruluşlarca istendiğinde ilgili kişiye veya talep eden kurum veya kuruluşa yabancılar kütüğünden çıkartılacak yabancılar kayıt örneği onaylanarak verilir.

(2) Yabancılara ait nüfus kayıt örneklerinin üst tarafına kişinin Türk vatandaşı olmadığı ve uyruğu, açıklamalar bölümüne de kayıt örneğinin ne amaçla kullanılacağı açıkça yazılır. Bu kayıt örnekleri altı ay içinde kullanılmadığı takdirde geçerliliğini kaybeder.

Yabancılar kütüğünden kayıt örneği ve bilgi isteyebilecekler

MADDE 24- (1) Yabancılar nüfus kayıt örneği aşağıdaki kişi ve kurumlara istendiğinde verilir:

- a) Bakanlıklara,
- b) Dış temsilciliklere,
- c) Nüfus müdürlüklerine,
- ç) Adli mercilere,
- d) Adli ve idari işlem nedeniyle kolluk makamlarına,
- e) Kaydın sahipleri, eşleri, veli, vasi, alt ve üst soyları veya resmi vekillerine,
- f) Yabancının çalıştığı veya çalışmak istediği kurum ve kuruluşlara.

(2) Yabancılar nüfus kayıt örneği yazılı olarak istenir. Yazıda kayıt örneğinin istenmesinin nedeni ve hangi amaçla kullanılacağı belirtilir.

(3) Yazılı bir isteğe dayanmaksızın kayıt örneği çıkartılıp verilemez. Yabancıların kimliklerini kanıtlayan belgelerle başvurmaları halinde yazılı müracaatları aranmaz.

Olay formu alınması

MADDE 25- (1) Yabancılar veri giriş formu ile yabancıların kayıtlarına işlenen nüfus olayları hakkında bilgi almaya yetkili olan kişi veya kurumlara istenildiğinde; doğum, ölüm, evlenme formu veya bu formlar, çok dilli bildirim formu şeklinde verilir.

(2) Türkiye'nin taraf olduğu uluslararası sözleşmeler uyarınca doğum, evlenme ve ölüm olayı çok dilli bildirim ile yabancıların doğum yeri nüfus idaresine gönderilir.

BEŞİNCİ BÖLÜM

Çeşitli ve Son Hükümler

Koordinasyon

MADDE 26- (1) Genel Müdürlük, yabancılar kütüğünün oluşturulmasını ve güncel bir şekilde tutulmasını sağlamak için Emniyet Genel Müdürlüğü ile koordinasyonu sağlamakla, Emniyet Genel Müdürlüğü de yabancıların uyruk ve kimliklerine ilişkin bilgileri Genel Müdürlükle paylaşmakla yükümlüdür.

Belge, form ve tutanakların kayıt edilmesi

MADDE 27- (1) Yabancılar kütüğünde kayıtlı olanların kişisel durumlarına ilişkin olarak nüfus müdürlüklerine intikal eden her türlü form, tutanak, yazı, evrak ve belgeler nüfus müdürlüklerinde bilgi işlem ortamında tutulan evrak kayıt defterine kayıt edilir.

Yürürlük

MADDE 28 - (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 29 - (1) Bu Yönetmelik hükümlerini Bakanlar Kurulu yürütür.

Güvenlik Soruşturması ve Arşiv Araştırması Yapılmasına Dair Yönetmelik

Resmî Gazete Tarihi : 03.06.2022

Resmî Gazete Sayısı : 31855

GÜVENLİK SORUŞTURMASI VE ARŞİV ARAŞTIRMASI YAPILMASINA DAİR YÖNETMELİK

BİRİNCİ BÖLÜM

Başlangıç Hükümleri

Amaç

MADDE 1- (1) Bu Yönetmeliğin amacı, yetkili olmayan kişilerin bilgi sahibi olmaları halinde Devletin güvenliğinin, iç ve dış menfaatlerinin, ulusal varlığın ve bütünlüğün zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeler ile gizlilik dereceli birim ve kısımların tespitine, güvenlik soruşturması ve arşiv araştırması yapılmasına ve değerlendirme komisyonlarının çalışmalarına ilişkin usul ve esasları belirlemektir.

Kapsam

MADDE 2- (1) Bu Yönetmelik, haklarında güvenlik soruşturması ve/veya arşiv araştırması yapılacak kişileri, talep eden kurum ve kuruluşları ve yapacak birimleri kapsar.

Dayanak

MADDE 3- (1) Bu Yönetmelik 7/4/2021 tarihli ve 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanununun 12 nci maddesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4- (1) Bu Yönetmelikte geçen;

- a) Bilmesi gereken: Gizlilik dereceli bilgi ve belgeleri ancak görevinden dolayı öğrenen, onu inceleyen, uygulayan ve korumaktan sorumlu bulunanları,
- b) Değerlendirme Komisyonu: Güvenlik soruşturması veya arşiv araştırması sonucunda elde edilen kişisel verilerin göreve atanma yönünden değerlendirildiği komisyonu,

- c) İstihbari faaliyet: İlgili kişi hakkında istihbarat üniteleri tarafından çeşitli kaynak ve araçlardan derlenen haber ve bilgilerin işlenmesi suretiyle veri elde etme faaliyeti,
- ç) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
- d) Kurum ve kuruluş: Güvenlik soruşturması ve/veya arşiv araştırması yapılmasını talep eden kamu kurum ve kuruluşları ile milli güvenlik açısından stratejik önemi haiz birim, proje, tesis ve hizmetleri yerine getiren diğer kurum ve kuruluşu,
- e) Olgusal veri: Yürütülecek görevin gerektirdiği niteliklerle ilgisi bulunan, yorum içermeyen, somut veya gözlemlenebilir ya da doğrulanabilir vâkıalara dayanan veriyi,
- f) Üst kademe kamu yöneticisi: 3 sayılı Üst Kademe Kamu Yöneticileri ile Kamu Kurum ve Kuruluşlarında Atama Usûllerine Dair Cumhurbaşkanlığı Kararnamesi ile üst kademe kamu yöneticisi olarak belirlenen kişiyi,
- ifade eder.

İKİNCİ BÖLÜM

Gizlilik Dereceli Bilgi ve Belgeler ile Birim ve Kısımlar

Gizlilik dereceli bilgi ve belgeler

MADDE 5- (1) Gizlilik dereceleri ile gizlilik dereceli belgelerin sınıflandırılması, oluşturulması, kullanım yerleri, muhteviyatı, güncelliği ve diğer hususlarda 25/4/2022 tarihli ve 5529 sayılı Cumhurbaşkanlığı Kararı ile yürürlüğe konulan Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik hükümleri uygulanır.

Gizlilik dereceli birim ve kısımlar

MADDE 6- (1) Gizlilik dereceli birim ve kısımlar, kamu kurum ve kuruluşlarında Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik hükümlerine göre “çok gizli” ve “gizli” gizlilik dereceli bilgi ve belgeleri oluşturan ve saklayan birim ve kısımlardır.

(2) Kamu kurum ve kuruluşları, gizlilik dereceli birim ve kısımları birinci fıkra gereğince belirler. Ancak tüm kamu kurum ve kuruluşlarının; teftiş ve denetim birimleri, personel birimleri, bilgi işlem birimleri ve özel kalem müdürlükleri gizlilik dereceli birimlerden sayılır.

(3) Kamu kurum ve kuruluşları tarafından ikinci fıkra gereğince belirlenen gizlilik dereceli birim ve kısımlar Cumhurbaşkanlığına bildirilir. Ancak bu bildirim il özel idareleri ve il özel idarelerinin üyesi olduğu mahalli idare birlikleri ile köylere hizmet götürme birlikleri için İçişleri Bakanlığına,

belediyeler ve bağılı kuruluşları ile belediyelerin üyesi olduğu mahalli idare birlikleri için Çevre, Şehircilik ve İklim Değişikliği Bakanlığına yapılır. İlgili bakanlık tarafından yapılan inceleme neticesinde birinci fıkraya uygun olduğu tespit edilen bildirimler Cumhurbaşkanlığına iletilir.

(4) Cumhurbaşkanlığına bildirilen birim ve kısımların birinci fıkra kapsamında olup olmadığı değerlendirildikten sonra uygun görülenler Cumhurbaşkanlığınca İçişleri Bakanlığı, Milli İstihbarat Teşkilatı Başkanlığı ve Emniyet Genel Müdürlüğüne gönderilir.

ÜÇÜNCÜ BÖLÜM

Güvenlik Soruşturması ve Arşiv Araştırmasının Usul ve Esasları

Arşiv araştırması

MADDE 7- (1) Arşiv araştırması;

- a) Kişinin adli sicil kaydının,
 - b) Kişinin kolluk kuvvetleri tarafından halen aranıp aranmadığının,
 - c) Kişi hakkında herhangi bir tahdit olup olmadığının,
 - ç) Kişi hakkında kesinleşmiş mahkeme kararları ve 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun 171 inci maddesinin beşinci ve 231 inci maddesinin on üçüncü fıkraları kapsamında alınan kararlar ile kişi hakkında devam eden veya sonuçlanmış olan soruşturma ya da kovuşturmalar kapsamındaki olguların,
 - d) Hakkında kamu görevinden çıkarılma ya da kesinleşmiş memurluktan çıkarma cezası olup olmadığının,
- mevcut kayıtlardan tespit edilmesidir.

Güvenlik soruşturması

MADDE 8- (1) Güvenlik soruşturması, arşiv araştırmasındaki hususlara ilave olarak kişinin;

- a) Görevin gerektirdiği niteliklerle ilgili kolluk kuvvetleri ve istihbarat ünitelerindeki olgusal verilerinin,
- b) Yabancı devlet kurumları ve yabancılarla ilişkisinin,
- c) Terör örgütleri veya suç işlemek amacıyla kurulan örgütlerle eylem birliği, irtibat ve iltisak içinde olup olmadığının,

mevcut kayıtlardan ve kişinin görevine yansiyacak hususların denetime elverişli olacak yöntemlerle yerinden araştırılmak suretiyle tespit edilmesidir.

Hakkında güvenlik soruşturması ve arşiv araştırması yapılacaktır

MADDE 9- (1) Statüsü veya çalışma şekline bağlı olmaksızın ilk defa veya yeniden memuriyete yahut kamu görevine atanacaklar hakkında arşiv araştırması yapılır.

(2) Aşağıda belirtilenler hakkında güvenlik soruşturması ve arşiv araştırması birlikte yapılır:

- a) Kamu kurum ve kuruluşlarının gizlilik dereceli birim ve kısımlarında çalıştırılacak kamu personeli.
- b) Milli Savunma Bakanlığı teşkilatında çalıştırılacak kamu personeli.
- c) Genelkurmay Başkanlığında çalıştırılacak kamu personeli.
- ç) Emniyet Genel Müdürlüğünde çalıştırılacak kamu personeli.
- d) Jandarma Genel Komutanlığında çalıştırılacak kamu personeli.
- e) Sahil Güvenlik Komutanlığında çalıştırılacak kamu personeli.
- f) Milli İstihbarat Teşkilatı Başkanlığında çalıştırılacak kamu personeli.
- g) Ceza infaz kurumları ve tutukevlerinde çalışacak personel.
- ğ) Kamu kurum ve kuruluşlarında çalışacak öğretmenler.
- h) Üst kademe kamu yöneticileri.
- ı) Özel kanunları gereğince güvenlik soruşturması ve arşiv araştırmasına tabi tutulan kişiler.
- i) Milli güvenlik açısından stratejik önemi haiz birim, proje, tesis ve hizmetlerde statüsü veya çalışma şekline bağlı olmaksızın istihdam edilenler.

Güvenlik soruşturması ve arşiv araştırmasını yapacak birimler

MADDE 10- (1) Güvenlik soruşturması ve arşiv araştırması;

- a) Milli İstihbarat Teşkilatı Başkanlığı,
 - b) Emniyet Genel Müdürlüğü,
 - c) Mahalli mülki idare amirlikleri,
- tarafından yapılır.

(2) Güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimler, kendilerine iletilen taleple sınırlı olarak güvenlik soruşturması ve arşiv araştırması kapsamında bakanlıklar ile kamu kurum ve

kuruluşlarının arşivlerinden ve elektronik bilgi işlem merkezlerinden gerekli bilgi ve belgeler ile 7315 sayılı Kanununun 4 üncü maddesinin birinci fıkrasının (ç) bendi kapsamındaki karar ve kayıtları almaya yetkilidir.

(3) Güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimlerde yetkilendirilmiş personel;

a) Hukuka aykırı olarak elektronik ortamda veya bilgisayar kayıtlarında ve loglarında kişisel verilerle ilgili sorgulama yapamaz.

b) Log kayıtlarını değiştiremez veya silemez.

c) Elde edilen bilgileri paylaşamaz veya yayın yoluyla duyuramaz.

ç) Görevi gereği öğrendiği veya edindiği kişisel bilgi veya belgeleri, yetkisiz kişilerle paylaşamaz ya da basın ve yayın kuruluşlarına veya diğer iletişim kanallarına veremez.

(4) Güvenlik soruşturması ve/veya arşiv araştırması yapmakla görevli birimler tarafından, üçüncü fıkrada belirtilen hususlara ilişkin gerekli tedbirler alınır.

Güvenlik soruşturması ve arşiv araştırmasında izlenecek yöntem

MADDE 11- (1) Cumhurbaşkanlığının arşiv araştırması ve/veya güvenlik soruşturması talepleri, Milli İstihbarat Teşkilatı Başkanlığınca ve/veya Emniyet Genel Müdürlüğünce karşılanır.

(2) Kurum ve kuruluşların talebi üzerine yapılacak arşiv araştırması, Emniyet Genel Müdürlüğü ve/veya mahalli mülki idare amirliklerince gerçekleştirilir.

(3) Dördüncü fıkra hükmü saklı kalmak kaydıyla;

a) Milli Savunma Bakanlığında uzman erbaş, sözleşmeli er/erbaş ve işçi olarak çalıştırılacak personele,

b) Emniyet Genel Müdürlüğünde çalıştırılacak kamu personeline,

c) Jandarma Genel Komutanlığında çalıştırılacak kamu personeline,

ç) Sahil Güvenlik Komutanlığında çalıştırılacak kamu personeline,

d) Ceza infaz kurumları ve tutukevlerinde çalıştırılacaklara,

e) Kamu kurum ve kuruluşlarında çalıştırılacak öğretmenlere,

f) Kurum ve kuruluşların gizlilik dereceli birimlerinde görev yapacaklara,

ilişkin güvenlik soruşturması ile dördüncü fıkrada yer almayan diğer güvenlik soruşturmaları, doğrudan yapılacak talep üzerine Emniyet Genel Müdürlüğü ve/veya mahalli mülki idare

amirliklerince gerçekleştirilir. İllerden gelen güvenlik soruşturması ve arşiv araştırması talepleri valilikler tarafından yerine getirilir.

(4) Aşağıda belirtilen kişiler hakkındaki güvenlik soruşturması talepleri Cumhurbaşkanlığına iletilir ve bunlar hakkındaki güvenlik soruşturması Milli İstihbarat Teşkilatı Başkanlığı ve/veya Emniyet Genel Müdürlüğüne yaptırılır:

a) Kurum ve kuruluşların gizlilik dereceli birim ve kısımlarında görev yapacaklardan; merkez teşkilatındaki şube müdürü, dengi ve üstü birim amirleri ile 14/7/1965 tarihli ve 657 sayılı Kanununun 36 ncı maddesinin "Ortak Hükümler" bölümünün (A) fıkrasının (11) numaralı bendi ile ek 41 inci maddesinde sayılanlar ve mesleğe özel yarışma sınavına tabi tutulmak suretiyle alınanlar.

b) İhtisas alanlarına da yer verilmek suretiyle Milli Savunma Bakanlığı ve Genelkurmay Başkanlığında çalıştırılacak kamu personeli.

c) Üst kademe kamu yöneticileri.

ç) 24/2/1983 tarihli ve 2802 sayılı Hâkimler ve Savcılar Kanunu kapsamında hâkim ve savcı adaylığına atanacaklar ile hâkimlik ve savcılık mesleğine kabul edilecekler.

d) 9/6/1930 tarihli ve 1700 sayılı Dahiliye Memurları Kanunu kapsamında kaymakam adaylığına atanacaklar.

e) 7/7/2010 tarihli ve 6004 sayılı Dışişleri Bakanlığı Personeline İlişkin Bazı Düzenlemeler Hakkında Kanun kapsamında aday meslek memurluğu ile aday konsolosluk ve ihtisas memurluğuna atanacaklar ile doğrudan yurtdışı teşkilatında istihdam edilecekler.

f) Milli güvenlik açısından stratejik önemi haiz birim, proje, tesis, hizmetlerde statüsü veya çalışma şekline bağlı olmaksızın istihdam edilecekler.

g) 29/6/2004 tarihli ve 5202 sayılı Savunma Sanayii Güvenliği Kanunu kapsamındakiler.

(5) Arşiv araştırması taleplerine, ilgili kişinin; adı, soyadı ve kimlik numarası bilgilerini içeren liste elektronik ortamda eklenir.

(6) Güvenlik soruşturması taleplerine, ilgili kişinin; adı, soyadı, kimlik numarası, güncel adresi, iletişim bilgileri, mezun olduğu okul, son çalıştığı işyeri ve unvan bilgilerini içeren liste elektronik ortamda eklenir.

(7) Güvenlik soruşturması ve arşiv araştırması yapılması taleplerinin ilgili kuruma ulaşmasından itibaren;

a) Arşiv araştırması sonuçları en geç 30 iş günü,

b) Güvenlik soruşturması sonuçları en geç 60 iş günü,

içinde talep eden kuruma bildirilir. Soruşturma ve araştırma sonucunu içeren bilgi ve belgeler, ilgilinin işlemini yapan kurum dosyasında asgari "gizli" gizlilik derecesinde aidiyet konusuna göre fiziki ve/veya elektronik ortamda muhafaza edilir. Ancak bu bilgi ve belgelerden istihbari faaliyetlere konu olanlar elektronik ortamda muhafaza edilemez.

(8) Dördüncü fıkranın (f) bendinde belirtilenlerin güvenlik soruşturması ve arşiv araştırması yapılmasına ilişkin taleplerde, ilgili veya bağlı bulunulan bakanlık veya kamu kurum ve kuruluşu tarafından bu birim, proje, tesis veya hizmetin milli güvenlik açısından taşıdığı stratejik önem gerekçelendirilerek belirtilir.

(9) 6 ncı maddenin üçüncü fıkrası ve bu maddenin sekizinci fıkrası gereğince bildirimde bulunmayan kamu kurum ve kuruluşlarının güvenlik soruşturması ve arşiv araştırması talepleri güvenlik soruşturması ve arşiv araştırmasını yapacak birimlerce yerine getirilmez.

Değerlendirme Komisyonu

MADDE 12- (1) Yaptırılan güvenlik soruşturması ve arşiv araştırması sonucunda elde edilen verilerin değerlendirilmesi amacıyla Değerlendirme Komisyonu kurulur. Değerlendirme Komisyonu; Cumhurbaşkanlığında İdari İşler Başkanının görevlendireceği bir üst kademe yöneticisinin, Türkiye Büyük Millet Meclisi Başkanlığında genel sekreter yardımcısının, bakanlıklarda bakan yardımcısının, diğer kamu kurum ve kuruluşlarında en üst yöneticinin görevlendireceği bir üst kademe yöneticisinin, üniversitelerde rektör yardımcısının, valiliklerde vali yardımcısının başkanlığında, teftiş/denetim, personel ve hukuk birimleri ile uygun görülecek diğer birimlerden birer üyenin katılımıyla başkan dahil en az beş kişiden ve tek sayıda olacak şekilde oluşturulur. Milli güvenlik açısından stratejik önemi haiz birim, proje, tesis ve hizmetlerde istihdam edilecekler hakkındaki değerlendirme, ilgili bakanlık ya da kamu kurumları bünyesindeki Değerlendirme Komisyonunca yapılır.

(2) Memuriyet veya kamu görevlerine uygunluğunun değerlendirilmesini sağlayacak yorum içermeyen olgusal veriler, güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimlerce ilgili kamu kurum ve kuruluşunun bünyesinde kurulan Değerlendirme Komisyonuna iletilir.

(3) Güvenlik soruşturması kapsamında elde edilen verilerden somut olarak gözlemlenemeyen veya doğruluğu denetlenemeyenler ya da iftira olduğu yahut kin ve düşmanlık gibi saiklerle verildiği açık olan bilgi ve beyanlar Değerlendirme Komisyonuna iletilmez ve bu bilgi ve beyanlar komisyonca

dikkate alınmaz. Değerlendirme Komisyonu gerekli görmesi halinde kendisine iletilen bilgiler hakkında bilginin kaynağını açıklamaksızın ilgili kişiden açıklama yapmasını isteyebilir.

(4) Değerlendirme Komisyonu, yaptırılan güvenlik soruşturması ve arşiv araştırması sonucunda elde edilen verileri analiz ederek ilgili kişinin memuriyete ya da kamu görevine atanıp atanmaması veya gizlilik dereceli birim ve kısımlarda yahut milli güvenlik açısından stratejik önemi haiz birim, proje, tesis ve hizmetlerde çalışıp çalışmaması gibi hususlarda nesnel ve gerekçeli değerlendirmelerini yazılı olarak atamaya yetkili amire sunar. Mahkemeler tarafından istenildiğinde bu bilgiler sunulur.

(5) Değerlendirme Komisyonu üye tam sayısı ile toplanır, kararlarını oy çokluğuyla alır.

(6) Değerlendirme Komisyonunun sekretarya hizmetleri, bünyesinde bulunduğu ilgili kamu kurum ve kuruluşunun personel işlemlerini yürüten birimlerce yapılır.

DÖRDÜNCÜ BÖLÜM

Kişisel Verilerin Korunması

Kişisel verilerin korunmasına ilişkin temel ilkeler

MADDE 13- (1) Güvenlik soruşturması ve arşiv araştırması kapsamında kişinin istihbari faaliyetlere konu olmayan kendisiyle ilgili kişisel verileri hakkında bilgilendirilmesi, bu verilere erişmesi, bunların düzeltilmesi ve silinmesi taleplerine ilişkin tedbirler alınır.

(2) Güvenlik soruşturması ve arşiv araştırmasına konu kişisel verilerin doğru ve güncel olması esastır. Bu veriler, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak kullanılır.

(3) Güvenlik soruşturması ve arşiv araştırması kapsamında yürütülen iş ve işlemlerde, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununun 4 üncü maddesinde belirtilen genel ilkelere aykırı hareket edilemez. Ancak milli savunma, milli güvenlik, kamu güvenliği, kamu düzeni ve ekonomik güvenlik ile ilgili istihbarat faaliyetleri kapsamında elde edilen bilgiler kişiye verilemez.

Kişisel veri güvenliği ve gizlilik

MADDE 14- (1) Güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimler ile Değerlendirme Komisyonları, veri güvenliğine ilişkin önlemleri alır.

(2) Güvenlik soruşturması ve arşiv araştırması işlemlerinin her evresinde gizliliğe uyulur. İlgili bilgi ve belgeler yasal olarak bilmesi gerekenlerden başkasına verilmez ve açıklanmaz. Arşiv araştırmasındaki hususlar hariç olmak üzere güvenlik soruşturması kapsamında elde edilen tüm verilere ilişkin bilgi ve belgeler ile Değerlendirme Komisyonu kararlarına yönelik işlemler, Gizlilik

Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelikte “gizli” gizlilik dereceli belgeler için belirtilen hükümlere göre yürütülür.

(3) Bu Yönetmelik kapsamında elde edilen kişisel veriler, amacı dışında işlenemez ve aktarılamaz.

Kişisel verilerin silinmesi ve yok edilmesi

MADDE 15- (1) Güvenlik soruşturması ve arşiv araştırması sırasında elde edilen kişisel veriler, işleme amacının ortadan kalkması halinde veya her durumda iki yılın sonunda Değerlendirme Komisyonlarınca silinir ve yok edilir.

(2) Güvenlik soruşturması ve arşiv araştırmasını yapan birimlerdeki istihbari faaliyete konu olmayan ilgisine ait güvenlik soruşturması ve arşiv araştırmasına ait veriler, iki yılın sonunda silinir ve yok edilir.

(3) Bu veriler, işleme karşı dava açılması halinde karar kesinleşmeden silinemez ve yok edilemez. Mahkemelerin bu konudaki talepleri, Değerlendirme Komisyonunun bünyesinde bulunduğu ilgili kamu kurum ve kuruluşu tarafından karşılanır. Mahkemenin olası taleplerinin karşılanabilmesinde ihtiyaç duyulabilecek ilgili evrakın saklanabilmesi için bu durum güvenlik soruşturması ve arşiv araştırması yapan birime ilgili kamu kurum ve kuruluşu tarafından bildirilir. Dava sonucunda verilen karar kesinleştiğinde ise ilgili güvenlik soruşturması ve arşiv araştırmasını yapan birime kişisel verilerin silinmesi ve evrakın imha edilebilmesi için ayrıca ilgili kamu kurum ve kuruluşu tarafından bildirimde bulunulur.

BEŞİNCİ BÖLÜM

Çeşitli ve Son Hükümler

Yürürlükten kaldırılan yönetmelik

MADDE 16- (1) 14/2/2000 tarihli ve 2000/284 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği yürürlükten kaldırılmıştır.

(2) Mevzuatta, birinci fıkra ile yürürlükten kaldırılan Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliğine yapılan atıflar bu Yönetmeliğe yapılmış sayılır.

Gizlilik dereceli birim ve kısımların bildirilmesi ile devam eden işlemler

GEÇİCİ MADDE 1- (1) Kamu kurum ve kuruluşları tarafından 6 ncı madde gereğince belirlenen gizlilik dereceli birim ve kısımlar, bu Yönetmeliğin yürürlüğe girdiği tarihten itibaren 60 gün içerisinde Cumhurbaşkanlığına bildirilir.

(2) Birinci fıkraya gereğince bildirim yapılmaya kadar talep edilecek güvenlik soruşturması ve arşiv arařtırmaları ile bu Yönetmeliğın yürürlüğe girdiđi tarihten önce başlatılan güvenlik soruşturması ve arşiv arařtırması işlemleri, 16 ncı maddenin birinci fıkrası ile yürürlükten kaldırılan yönetmeliğın 7315 sayılı Kanuna aykırı olmayan hükümlerine göre sonuçlandırılır.

Yürürlük

MADDE 17- (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 18- (1) Bu Yönetmelik hükümlerini Cumhurbaşkanı yürütür.

Sigortacılık Verilerinin Toplanması, Saklanması ve Paylaşılmasına Dair Yönetmelik

Resmî Gazete Tarihi : 18.10.2022

Resmî Gazete Sayısı : 31987

Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurumundan:

SİGORTACILIK VERİLERİNİN TOPLANMASI, SAKLANMASI VE PAYLAŞILMASINA DAİR YÖNETMELİK

BİRİNCİ BÖLÜM

Başlangıç Hükümleri

Amaç ve kapsam

MADDE 1- (1) Bu Yönetmelik; özel hukuk tüzel kişileri, kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları ve bunların üst kuruluşları ile bilgi merkezlerinden sigortacılık verilerinin elde edilmesi, saklanması, kullanılması gibi sigortacılık verileri üzerinde gerçekleştirilen her türlü işleme; bu verilerin sigorta, reasürans ve sigortacılık faaliyetinde bulunan emeklilik şirketleri ile Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurumunca belirlenecek diğer kişi ve kuruluşlarla paylaşılmasına dair usul ve esasları düzenlemektedir.

Dayanak

MADDE 2- (1) Bu Yönetmelik, 3/6/2007 tarihli ve 5684 sayılı Sigortacılık Kanununun 31/A ve 31/B maddelerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 3- (1) Bu Yönetmelikte geçen;

- a) Eksper: 3/6/2007 tarihli ve 5684 sayılı Sigortacılık Kanunu kapsamında faaliyet gösteren sigorta eksperini,
- b) Kanun: 3/6/2007 tarihli ve 5684 sayılı Sigortacılık Kanununu,
- c) Kurum: Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurumunu,
- ç) Merkez: Sigorta Bilgi ve Gözetim Merkezini,

d) Özellikli kuruluşlar: Türkiye Sigorta, Reasürans ve Emeklilik Şirketleri Birliği ve nezdindeki alt kuruluşları, Emeklilik Gözetim Merkezi, Doğal Afet Sigortaları Kurumu, Tarım Sigortaları Havuzu ile sigortacılık ve özel emeklilik alanında faaliyet gösteren kurum ve kuruluşları,

e) Üye kuruluşlar: Merkezin veri paylaşımında bulunduğu ilgisine göre sigorta, reasürans ve emeklilik şirketlerini,

f) Yetkili kullanıcı: Genel veri tabanında yer alan verilere sınırlı şekilde erişim yetkisi tanınan, ilgisine göre üye kuruluş ve özellikli kuruluş yetkilileri, sigorta acenteleri, sigorta ve reasürans brokerleri, sigorta eksperleri ile diğer kişi ve kuruluşları,

ifade eder.

İKİNCİ BÖLÜM

Sigortacılık Verilerinin Toplanması

Sigortacılık verisi

MADDE 4- (1) Sigorta sözleşmelerine, sigorta sözleşmesine taraf olan sigorta ettiren ve sigorta şirketlerine, sigorta sözleşmesinden doğrudan veya dolaylı menfaat sağlayan sigortalı, lehtar ve diğer üçüncü kişilere ilişkin veriler ile yanlış sigorta uygulamaları dahil olmak üzere risk değerlendirmesine esas tüm veriler, sigortacılık verisidir.

Genel veri tabanı

MADDE 5- (1) Sigortacılık verileri, özel hukuk tüzel kişileri ile kamu kurum ve kuruluşlarından, kamu kurumu niteliğindeki meslek kuruluşları ve bunların üst kuruluşlarından, ilgili mevzuatla kurulmuş diğer bilgi merkezlerinden Merkez tarafından toplanarak genel veri tabanında tutulur. Söz konusu kurum ve kuruluşlar, Merkez tarafından talep edilen verileri Kanunun 31/B maddesi uyarınca vermekle yükümlüdür. Özel kanunlarında açıkça yer almadıkça bu kapsamdaki veri paylaşımı için Merkezden ücret talep edilemez.

(2) Genel veri tabanı, birinci fıkrada sayılan kurum ve kuruluşlardan toplanan tüm üretim, hasar, yanlış sigorta uygulamaları verileri ile Merkez nezdinde tutulan diğer tüm verileri içerir.

(3) Sigorta, reasürans ve sigortacılık faaliyetinde bulunan emeklilik şirketleri, Merkeze üye olmak ve genel veri tabanını güncel tutmakla yükümlüdür.

(4) Genel veri tabanında yer alan sigortacılık verileri, yetkili kullanıcılar tarafından Merkez sistemlerine iletilir.

(5) Hayat grubu ve hayat dışı grubu sigortalar aktüerya raporları ile eksperler tarafından düzenlenen ekspertiz raporları, genel veri tabanında tutulur.

Üretim verileri

MADDE 6- (1) Üye kuruluşlar; tüm sigortalara ilişkin poliçe üretimlerini, Merkezden alınan referans numarası ile gerçekleştirmek ve poliçelerde bu numaralara yer vermekle yükümlüdür.

(2) Üye kuruluşlar, sigorta sözleşmelerine ilişkin üretim verilerini eş zamanlı olarak Merkeze iletmekle yükümlüdür.

Hasar verileri

MADDE 7- (1) Üye kuruluşlar, eksper görevlendirmeyecek olsalar dahi kendilerine iletilen tüm ihbarlar için Merkezden alınan referans numarası ile dosya açmakla yükümlüdür.

(2) Üye kuruluşlar, güncel muallâk tazminat verilerini gün sonuna kadar, diğer hasar verilerini eş zamanlı olarak Merkeze iletmek ve gerekmesi halinde güncellemekle yükümlüdür. Yargı mercilerinde verilen kararlar doğrultusunda hasar verilerinin değişmesi halinde genel veri tabanında gerekli güncellemeler üye kuruluş tarafından yapılır.

(3) Eksperler, raporlarını Kurumca belirlenecek usul ve esaslar çerçevesinde Merkez sistemlerine aktarmak, üye kuruluşlar ise ihbardan ödemenin sonuçlanmasına kadar hasara ilişkin bilgi ve belgeleri eksiksiz olarak Merkeze iletmekle yükümlüdür.

Yanlış sigorta uygulamaları verileri

MADDE 8- (1) Üye kuruluşlar, özellikli kuruluşlar ile diğer kaynaklardan elde edilen yanlış sigorta uygulamaları verileri, Merkez tarafından oluşturulan veri tabanında tutulur.

(2) Merkez, yanlış sigorta uygulamalarına ilişkin sistemde, veri girişi, değiştirilmesi ve kaldırılmasına dair süreçlerin yürütülmesini, tanımlanmasını ve kontrol noktalarının oluşturulmasını sağlar.

Tahkim sistemi verileri

MADDE 9- (1) Kanununun 30 uncu maddesi çerçevesinde oluşturulan tahkim sistemi ile sigortacılık verilerinin paylaşılmasına ve tahkim verilerinin genel veri tabanına dahil edilmesine ilişkin usul ve esaslar, Kurum tarafından belirlenir.

ÜÇÜNCÜ BÖLÜM

Sigortacılık Verilerinin Paylaşımı

Genel veri paylaşım kuralları

MADDE 10- (1) Sigortacılık verileri, Kanununun 31/B maddesi çerçevesinde Merkez tarafından üye kuruluşlarla paylaşılır.

(2) Üye kuruluşlar dışındaki kurum, kuruluş ve veri merkezleri ile veri paylaşımları, Kurumun onayına istinaden Merkez tarafından imzalanan protokoller aracılığıyla gerçekleştirilir. Bu protokoller kapsamında veri paylaşımı, ilgili platformlar veya kısa mesaj, mobil uygulama, çağrı merkezi gibi iletişim kanalları yoluyla sağlanabilir. Kamu yararının söz konusu olması şartıyla Kurumca belirlenecek usul ve esaslar çerçevesinde Merkez, veri paylaşımını belirli bir ücret karşılığında yapabilir.

(3) Merkez, elde ettiği verileri, başka verilerle eşleştirilerek dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde anonim hale getirerek yayımlayabilir.

Yanlış sigorta uygulamalarına ilişkin verilerin paylaşımı

MADDE 11- (1) Yanlış sigorta uygulamalarına ilişkin veriler, üye kuruluşların, özelliği kuruluşların ve Kurum tarafından belirlenen ilgili diğer kişi ve kuruluşların erişimine açılır.

(2) Özel mevzuatında açıkça yer almadıkça yanlış sigorta uygulamalarına ilişkin veriler, birinci fıkrada sayılanlar dışındaki kişilerle paylaşılabilir.

Sigorta eksperleri ile veri paylaşımı

MADDE 12- (1) Hasar dosyası için eksper atanması ve atamanın Merkeze iletilmesini müteakip eksper, ilgili maddi varlıkların ve tarafların geçmiş poliçe ve hasar verilerine erişebilir. Kesin ekspertiz raporunun Merkez sistemlerine kaydedilmesi ile eksperin ilgili verilere erişim yetkisi, raporda değişiklik yapılması veya ek rapor tanzimi hariç olmak üzere sona erer.

(2) Eksper, tanzim ettiği ekspertiz raporlarına genel veri tabanından erişebilir.

(3) Merkez, görevlendirildikleri dosyalar ve görev süreleri ile sınırlı olarak motorlu araç sigortalarına ilişkin tazminat hesaplamalarında kullanılmak üzere uyuşmazlığa dahil olan motorlu araçların ve tarafların geçmiş poliçe ve hasar verilerini Sigorta Tahkim Komisyonu hakemleri tarafından görevlendirilen eksper bilirkişilerin erişimine açar.

Yetkili kullanıcılar ile veri paylaşımı

MADDE 13- (1) Genel veri tabanında yer alan verilere erişim tanınacak yetkili kullanıcılar ve münhasıran çalışma konuları ile ilgili olmak üzere erişebilecekleri verilerin içeriği, Kurumun onayına istinaden Merkez tarafından belirlenir.

(2) Eriřim kurallarını ihlal eden yetkili kullanıcıların sisteme erişimleri, Merkez Yönetim Komitesi kararına istinaden Kurumun onayıyla sınırlandırılır. İhlalin süreklilik göstermesi halinde ise ilgililerin sisteme erişim yetkileri, Merkez Yönetim Komitesi kararına istinaden Kurumun onayıyla kaldırılır. Yetkili kullanıcıların sisteme erişim yetkilerinin sınırlandırılması veya kaldırılması halinde bu durum, Merkez tarafından ilgili kurum ve kuruluşlara bildirilir.

(3) Merkez, durumun aciliyetine ve önemine istinaden yetkili kullanıcıların sisteme erişim yetkilerini derhal askıya almaya yetkilidir. Askıya alma işlemini müteakip beş iş günü içinde ikinci fıkra hükümleri yerine getirilir.

(4) İkinci ve üçüncü fıkralar kapsamında erişim yetkisi sınırlandırılan, kaldırılan veya askıya alınan yetkili kullanıcının eksper ya da bilirkiři olması halinde ilgili süre zarfında kendisine Merkez sistemleri üzerinden görevlendirme yapılmaz.

Diğer kişiler ile veri paylaşımı

MADDE 14- (1) Merkez, sigorta sözleşmeleri ile ilgili poliçe ve hasar verilerinden Kurumca uygun görülenleri, gerekli kimlik doğrulamasının sağlanması ya da hak sahipliğinin ispatlanması şartıyla ilgili diğer kişilerin erişimine sunar.

(2) Genel veri tabanında yer alan verilere ilişkin diğer talepler, kullanım amacı bildirilmek şartıyla Merkez Yönetim Komitesi tarafından karara bağlanır. Bu verilerin içeriği Kurum tarafından belirlenir.

(3) Bu madde kapsamında paylaşılacak veriler için ücret belirlenmesine veya bunların ücretsiz olarak sağlanmasına Merkez Yönetim Komitesi tarafından karar verilir. Münhasıran çalışma konuları ile ilgili olmak üzere 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununa ekli cetvellerde yer alan kamu kurum ve kuruluşlarına bu madde kapsamında sağlanan hizmet ücrete tabi değildir.

DÖRDÜNCÜ BÖLÜM

Sigortacılık Verilerinin Kullanılması

Temel amaçlar

MADDE 15- (1) Sigortacılık verileri, aşağıdaki amaçlar doğrultusunda kullanılır:

a) Sigortacılık sektöründe kamu gözetimi, denetimi ve ekonomik güvenliğin sağlanmasına ve sağlık hizmetleri finansmanının planlanmasına katkıda bulunmak.

b) Sigorta uygulamalarını takip etmek, sigorta branşlarında uygulama birliğini sağlamak.

- c) Zorunlu sigortaların takibini yapmak.
- ç) Yanlış sigorta uygulamalarının önlenmesine katkıda bulunmak.
- d) Sigortalılık oranlarının artırılmasına yönelik çalışmalar yapmak.
- e) Sigortacılık sektörüne ilişkin güvenilir istatistikler üretilmesini sağlamak.
- f) Sigorta puanını hesaplamak.

Merkezin veri kullanımı

MADDE 16- (1) Genel veri tabanında yer alan veriler, Merkez tarafından aşağıdaki amaçlar doğrultusunda kullanılır:

- a) Üye kuruluşlardan gelen güncel üretim, hasar ve tazminat verilerini genel veri tabanında yer alan veriler ile ilişkilendirmek.
- b) Zorunlu sigortaların takibi ve tespiti amacıyla ilgili kurum ve kuruluşlarla iş birliği yapmak.
- c) Motorlu araç işletenlere ve sürücülere ilişkin verileri almak, bunları genel veri tabanında yer alan veriler ile ilişkilendirmek, ilgili mevzuat kapsamında kamu kurum ve kuruluşları ile paylaşmak, kaza tespit tutanaklarına ilişkin bilgilerin tutulduğu bir veri tabanı oluşturmak.
- ç) Türkiye Cumhuriyeti sınırlarından giriş yapan yabancı plakalı araçlar ve Türkiye Cumhuriyeti sınırlarından çıkış yapan Türkiye’de kayıtlı motorlu araçların üçüncü şahıs mali sorumluluk sigortası sözleşmelerine ilişkin verileri tutmak.
- d) Üye kuruluşların sağlık ve hastalık branşlarında tanzim ettikleri ve yürürlükte olan poliçeleri için yapacakları risk değerlendirme süreçlerinde ekonomik güvenliğin sağlanmasının ve sağlık hizmetleri finansmanının planlanmasının sağlıklı şekilde yürütülebilmesini teminen sigortalıya ait geçmiş poliçe verilerini üye kuruluşlarla paylaşmak.
- e) Üye kuruluşların karşılıklı rücu alacaklarına yönelik mahsuplaşma platformu kurmak.

Sigorta puanı

MADDE 17- (1) Yanlış sigorta uygulamaları dahil risk değerlendirmesine esas sigortacılık verileri ile diğer kaynaklardan elde edilen veriler doğrultusunda sigorta puanı hesaplaması Merkez tarafından yapılır.

(2) Sigorta puanının hesaplanması, saklanması, değiştirilmesi, kullanılacağı sigorta branşları ve diğer kurum ve kuruluşlarla paylaşımı ile risk değerlendirmesinde kullanılmasına ilişkin usul ve esaslar Kurum tarafından belirlenir.

BEŞİNCİ BÖLÜM

Merkezin Sigortacılık Verilerine İlişkin Faaliyetleri

Veri olgunluğu ölçümü

MADDE 18- (1) Merkez, üye kuruluşlardan temin ettiği verilerin doğru, eksiksiz, tutarlı ve zamanında iletilmesini ve bu verilerin kalitesinin artırılmasını teminen veri olgunluğunun ölçümü için puanlama metotları geliştirir, verinin bu metotlara uyumluluğunu tespit ederek puanlar ve bunları Kuruma raporlar. Bu raporlara istinaden Kurum, Merkez sistemlerine erişim ve verilerden yararlanma yetkilerinin sürekli kaldırılması dahil her türlü tedbiri uygulayabilir.

Raporlama

MADDE 19- (1) Merkez, Kurum tarafından belirlenen metot ve biçimde üye kuruluşlara, özellikle kuruluşlara ve yetkili kullanıcılara ilişkin raporlar hazırlar ve bunları güvenli ortamlar üzerinden Kuruma iletir; rapordarda mevzuata aykırı olduğu tespit edilen uygulamaları da Kuruma bildirir.

(2) Merkez, ticari sırların ve kişisel verilerin korunması hakkının ihlal edilmemesi kaydıyla, üye kuruluşların ve özellikle kuruluşların talebi üzerine özel bilgi raporları üretebilir; bu raporları eş zamanlı olarak Kurumun da erişimine açar.

(3) Merkez, görev ve faaliyetleri kapsamında elde ettiği verileri, anonim hale getirerek raporlar, hazırlar ve bunları yayımlar.

(4) Merkez, Kurum tarafından iletilen veri ve raporlama taleplerini öncelikli olarak sonuçlandırır.

Bilgilendirme

MADDE 20- (1) Merkez, kamunun, üye kuruluşların, özellikle kuruluşların, yetkili kullanıcıların, sigortalıların ve diğer hak sahiplerinin bilgilendirilmesine yönelik çalışmalar yapar.

(2) Merkez, ilgili kişi, kurum ve kuruluşlar ile doğrudan veya dolaylı iletişim kurarak anket, inceleme, araştırma ve benzeri çalışmalar yapabilir; yaptığı istatistikî çalışmaların sonuçları hakkında kamuyu bilgilendirir.

Teknik altyapı uygunluğunun sınanması

MADDE 21- (1) Merkez, üye kuruluşların teknik altyapılarının yeterliliğini, gözetim ve denetime uygunluğunu sına ve değerlendirme işlemlerini yürütür; veri paylaşımında aksama olmaması için üye kuruluşların teknik altyapı eksikliklerinin giderilmesine yönelik gerekli uyarılarda bulunur; süreklilik arz eden aksaklıkları Kuruma bildirir.

Diğer faaliyetler

MADDE 22- (1) Kurum tarafından Merkezin görev ve yetki alanı çerçevesinde talep edilen her türlü uygulama ve çalışma, ayrıca bir işleme gerek olmaksızın münhasıran Merkez tarafından yerine getirilir.

ALTINCI BÖLÜM

Sorumluluk ve Bilgi Verme Yükümlülüğü

Sorumluluk

MADDE 23- (1) Üye kuruluşlar, özellikli kuruluşlar ile yetkili kullanıcılar, Merkezle sağlıklı veri paylaşımı gerçekleştirilmesi için gereken altyapıyı oluşturmak, Merkez tarafından sistemseller değişikliklerin yapılması durumunda bu değişikliklere uyum sağlamak ve talep edilen her türlü bilgi ve belgeyi gecikmeksizin sunmakla yükümlüdür.

(2) Üye kuruluşlar, özellikli kuruluşlar ile yetkili kullanıcılar, Merkeze verileri doğru, eksiksiz, tutarlı ve zamanında aktarmakla yükümlüdür. Üye kuruluşlar, özellikli kuruluşlar ile yetkili kullanıcıların bu madde kapsamındaki yükümlülüklerini yerine getirmemesinden veya aktarılan verilerin üçüncü şahıslar ile paylaşılmasından kaynaklanan bir zararın doğması sebebiyle Merkez tarafından tazminat ödenmesi halinde Merkez, ilgililere rücu edebilir.

(3) Genel veri tabanında yer alan ve paylaşılan veriler için veri sahibinin açık rızası veya onayı aranan hallerde veri sahibinden açık rıza veya onayın alınmasından ve aydınlatma yükümlülüğünün yerine getirilmesinden veri alışverişi yapan muhatap üye kuruluş, özellikli kuruluş ve yetkili kullanıcı ile veri sahibinin muhatabı diğer kurum ve kuruluşlar sorumludur. Yanlış sigorta uygulamalarına taraf kişi ve kuruluşlara ait verilerin genel veri tabanına kaydedilmesi ve ilgili mevzuat çerçevesinde kurum ve kuruluşlarla bu verilerin paylaşılmasında veri sahibinin açık rızası veya onayı aranmaz.

(4) Merkez, veri sistemlerinde yaşanan sistemseller hata ya da aksaklıklardan ve kayıtlı verilerin güvenliğinden sorumludur. Sistemseller hata veya aksaklıkların yaşanması durumunda Merkez, sorunun derhal giderilmesini ve ilgisine göre üye kuruluşların, özellikli kuruluşların veya yetkili kullanıcıların en geç bir iş günü içinde konuya ilişkin olarak bilgilendirilmesini sağlamakla yükümlüdür.

Bilgi verme yükümlülüğü

MADDE 24- (1) Üye kuruluşlar ile özelliikli kuruluşlar, Merkez tarafından istenen ve genel veri tabanının işleyişi için gerekli olan tüm bilgileri, doğru, eksiksiz ve tutarlı olarak Merkeze iletmekle yükümlüdür. Kurum, gerek görmesi halinde verilerin şekli ve içeriğine ilişkin sınırlamalar getirebilir.

(2) Üye kuruluşlar, zamanında aktarılmayan ve eksik veya hatalı olarak aktarıldığı Merkez tarafından tespit edilen verileri, Merkezin bildirimine üzerine gecikmeksizin düzeltmek ve en geç bir iş günü içinde düzeltme yapılan verileri Merkeze iletmek zorundadır. Süresi içinde verileri düzeltmeyen üye kuruluşların ve özelliikli kuruluşların Merkez sistemlerine erişim yetkisi, Kurumca belirlenen usul ve esaslar çerçevesinde üç iş gününe kadar kaldırılır. Bu sürenin sonunda veri düzeltilmemişse erişim yetkisi kaldırma işlemi, düzeltme yapılana kadar tekrarlanır.

(3) Bu madde kapsamında bilgi verme yükümlülüğünün yerine getirilmemesi, 7/8/2007 tarihli ve 26606 sayılı Resmî Gazete’de yayımlanan Sigorta ve Reasürans ile Emeklilik Şirketlerinin Mali Bünyelerine İlişkin Yönetmeliğin 11 inci maddesinin birinci fıkrasının (i) bendi kapsamında değerlendirilir.

Gizlilik

MADDE 25- (1) Bu Yönetmelik kapsamında veri paylaşımına dahil olan tüm kurum ve kuruluşların unvanına bakılmaksızın ilgili tüm çalışanları, görevleri dolayısıyla haiz oldukları sigortacılık verilerine ilişkin bilgi ve belgeleri gerek görevleri süresince gerekse görevleri sona erdikten sonra hiçbir şekilde kullanamaz; üçüncü şahıslarla paylaşamaz ve yayımlayamaz. Merkez tarafından bu madde kapsamında olup uhdesinde kamu görevi bulunmayan kişilerden Kurumun uygun göreceği bir gizlilik taahhünamesi alınır.

(2) Birinci fıkradaki hükümler, anılan kurum ve kuruluşlar adına bilişim, donanım, ağ hizmetleri, çağrı merkezi ve doğrudan satış gibi hizmetleri sağlayan kuruluşları da kapsar.

(3) Bu maddeyi ihlal eden kişiler hakkında, Kanunun 31/B maddesinin altıncı fıkrası uygulanır.

YEDİNCİ BÖLÜM

Sigortacılık Verilerine İlişkin Talepler

Bilgi edinme talebi

MADDE 26- (1) Veri sahipleri, yanlış sigorta uygulamalarına ilişkin veriler dışında kalan ve genel veri tabanında yer alan kendilerine ait veriler hakkında Merkezdten bilgi isteyebilir. Merkez, bilgi edinme taleplerini onbeş gün içinde karşılar; bu sürenin yeterli olmaması durumunda süre bir

defalığına onbeş gün uzatılır. Merkez, veri sahibinin başvurusundan itibaren en geç otuz gün içerisinde bilgi edinme talebini yanıtlamak zorundadır.

(2) Merkez, bilgi edinme taleplerinde kimlik doğrulaması yapabilir veya hak sahipliğini ya da yetkiyi gösterir bilgi ve belgeleri isteyebilir.

Verilerin değiştirilmesi talebi

MADDE 27- (1) Genel veri tabanında yer alan verilerin eksik veya yanlış olduğu iddiasıyla veri sahibi tarafından Merkeze başvurulması halinde Merkez, başvuruyu inceleyerek gerekmesi halinde veri sahiplerinin taleplerinin on günlük kesin süre içinde ilgili üye kuruluşa iletilmesine karar verir. Başvurunun ilgili kuruluşa iletilmesi halinde bu kuruluş, kendisine iletilen talebi on günlük kesin süre içinde inceler; incelemenin akabinde talebin kabulüne karar vererek verileri düzeltip Merkeze düzeltme işlemini bildirir veya talebin reddine karar vererek gerekçeli açıklamasıyla birlikte ret kararını Merkeze iletir. Merkez, ilgili kuruluşun kararının kendisine iletilmesinden veya on günlük kesin sürenin sona ermesinden sonra on günlük kesin süre içinde veri sahibine başvurusunun sonucu hakkında bilgi verir. Talebin kabulü halinde Merkez, verilerin düzeltilip düzeltilmediğini kontrol ederek 24 üncü maddenin ikinci fıkrası kapsamında gerekli işlemleri yürütür.

(2) Merkez, birinci fıkrada düzenlenen sürelerle uymayan üye kuruluşları, aylık olarak Kuruma raporlar. Bu raporlara istinaden Kurum, Merkez sistemlerine erişim ve verilerden yararlanma yetkilerinin kaldırılması dahil her türlü tedbiri uygulayabilir.

(3) Yanlış sigorta uygulamaları verilerine ilişkin talep ve itirazlarda bu madde uygulanmaz; anılan talep ve itirazlar, ilgili mevzuat çerçevesinde sonuçlandırılır.

SEKİZİNCİ BÖLÜM

Çeşitli ve Son Hükümler

Kişisel verilerin korunması

MADDE 28- (1) Bu Yönetmelik kapsamında yürütülen kişisel veri işleme faaliyetlerinde, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile bu Kanuna dayanılarak yürürlüğe konulan mevzuatta yer alan usul ve esaslara uyulması zorunludur.

Geçiş takvimi

GEÇİCİ MADDE 1- (1) Merkez, Kurumun uygun görüşü üzerine 6 ncı maddenin birinci fıkrasının ve 7 nci maddenin birinci fıkrasının uygulamaya koyulmasına ilişkin olarak dokuz ayı geçmemek

üzere; 6 ncı maddenin ikinci fıkrasının ve 7 nci maddenin ikinci fıkrasının uygulamaya koyulmasına ilişkin olarak bir yılı geçmemek üzere branş ya da üye kuruluş bazında geçiş takvimi yayımlar.

(2) Gerek görülmesi halinde 6 ncı maddenin ikinci fıkrasının ve 7 nci maddenin ikinci fıkrasının uygulamaya koyulmasına ilişkin olarak yayımlanacak geçiş takvimi, Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurulu kararına istinaden en fazla bir yıl uzatılabilir.

Yürürlük

MADDE 29- (1) Bu Yönetmelik 18/10/2022 tarihinde yürürlüğe girer.

Yürütme

MADDE 30- (1) Bu Yönetmelik hükümlerini Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurumu Başkanı yürütür.

Sađlık Bilgi Sistemleri Hakkında Yönetmelik

Resmî Gazete Tarihi : 25.08.2022

Resmî Gazete Sayısı : 31934

Sađlık Bakanlıđından:

SADLIK BILGI YONETIM SISTEMLERİ HAKKINDA YONETMELİK

BİRİNCİ BÖLÜM

Başlangıç Hükümleri

Amaç

MADDE 1- (1) Bu Yönetmeliđin amacı; sađlık bilgi yönetim sistemi hizmeti sađlayıcılarının uyacakları kurallara, sađlık bilgi yönetim sistemlerinin alım süreçlerine, standartlarına ve tescil işlemlerinin belirlenmesine ilişkin usul ve esasları düzenlemektir.

Kapsam

MADDE 2- (1) Bu Yönetmelik; sađlık bilgi yönetim sistemi hizmeti sađlayıcıları ile bu hizmetten yararlanan sađlık bilgi yönetim sistemi hizmet alıcılarının uymaları gereken kurallara ilişkin hükümleri kapsar.

Dayanak

MADDE 3- (1) Bu Yönetmelik; 7/5/1987 tarihli ve 3359 sayılı Sađlık Hizmetleri Temel Kanununun 3 üncü maddesinin birinci fıkrasının (f) bendi ile 1 sayılı Cumhurbaşkanlıđı Teşkilatı Hakkında Cumhurbaşkanlıđı Kararnamesinin 358 inci maddesinin birinci fıkrasının (ç) bendine dayanılarak hazırlanmıştır.

Tanımlar ve kısaltmalar

MADDE 4- (1) Bu Yönetmelikte geçen;

a) AHBS: Aile Hekimliđi Bilgi Sistemini,

b) Bakanlık: Sađlık Bakanlıđını,

- c) Cihaz: Sağlık hizmeti sunucularında kullanılan, sağlık hizmeti üretmek ya da sağlık hizmeti üretmeye yardımcı olmak amacı ile veri oluşturma, ölçme, denetleme, görüntüleme, dönüştürme amacı ile çalıştırılan her türlü aygıtı veya sistemi,
- ç) CMMI: Yetenek Olgunluk Model Entegrasyonunu (Capability Maturity Model Integration),
- d) DICOM: Tıbbi görüntüleme cihazlarından alınan iki ve üç boyutlu bilimsel verilerin depolanması, görüntülenmesi ve analizinde kullanılmak maksadıyla geliştirilmiş olan dijital veri formatını (Digital Imaging and Communications in Medicine),
- e) Entegrasyon: Herhangi bir SBYS ya da cihazın, yüksek kalitede ve etkinlikte sağlık hizmeti üretebilmek için, diğer SBYS ya da cihazlarla ihtiyacı karşılayacak yeterlilikte karşılıklı veri alışverişi yapılması işini,
- f) Elektronik sertifika: İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı,
- g) Entegre edilebilir cihaz: Entegrasyon sağlamak için gerekli her türlü yazılımı üzerinde barındıran, entegrasyon dokümanı olan, gerektiğinde cihaz hizmeti sağlayıcısı tarafından entegrasyon hizmet veya desteğinin sağlanabildiği her türlü cihazı,
- ğ) Genel Müdürlük: Sağlık Bilgi Sistemleri Genel Müdürlüğünü,
- h) Görüntü: VTYS terminolojisinde VIEW olarak da bilinen, gerektiğinde birden çok VTYS tablosunu kendi aralarındaki ilişkileri kullanarak birleştirebilen, genellikle başkaları tarafından verinin daha anlamlı şekilde görülebilmesini sağlayan VTYS nesnesini,
- ı) İdare: SBYS hizmetini alan kamu kurumları ile kamu sağlık tesisi yönetimlerini,
- i) KTS: Kayıt Tescil Sistemini,
- j) KTS Yetki Belgesi: SBYS hizmeti sağlayıcısının KTS'de kayıtlı olduğunu ve aktif listede yer aldığını doğrulayan belgeyi,
- k) PACS: Görüntü Arşivleme ve İletişim Sistemlerini (Picture Archiving and Communication Systems),
- l) Sağlık hizmeti sunucusu: Sağlık hizmetini sunan veya üreten gerçek kişiler ile kamu hukuku ve özel hukuk tüzel kişilerini,

- m) SAMİLOG: SBYS veri tabanında bulunan kayıtlarla ilgili yapılan değişikliklerin olay ve iz kayıtlarını tutmak amacı ile Genel Müdürlük tarafından hazırlanarak internet sitesinde yayımlanan Sağlıkta Minimum Loglama Standardını,
- n) SBYS: Sağlık hizmeti sunucuları tarafından klinik, idari ya da yönetsel amaçlarla kullanılan, gerektiğinde diğer bilgi yönetim sistemleri ile veri alışverişi yapabilen ve Sağlık Bilgi Yönetim Sistemleri olarak adlandırılan yazılımları,
- o) SBYS hizmeti alıcısı: SBYS hizmetini alan idareleri ve sağlık hizmeti sunucularını,
- ö) SBYS hizmeti sağlayıcısı: SBYS hizmeti sunmak üzere Kayıt Tescil Sisteminde kayıt edilerek yetkilendirilmiş olan gerçek veya tüzel kişiyi,
- p) SBYS yetkilisi: SBYS hizmeti sağlayıcısının imzaya yetkili temsilcisini,
- r) SPICE: Yazılım süreç geliştirme yetenek düzeyini (Software Process Improvement and Capability Determination),
- s) TSE: Türk Standardları Enstitüsünü,
- ş) ÜTS: Ürün Takip Sistemini,
- t) VEM: Sağlık hizmeti sunucularının yerel veri tabanlarında tutmuş oldukları verilere ait tablo ve alanların ulusal standartlara uyumunu sağlamak, veri kayıplarını asgari düzeyde tutmak, adaptasyonu hızlandırarak vatandaşların geçmiş verilerine erişimini kolaylaştırmak ve sürecin kesintisiz ilerlemesini temin etmek amacı ile Genel Müdürlük tarafından geliştirilen ve SBYS hizmeti alıcılarının SBYS değişiklikleri ile diğer veri aktarımı süreçlerinde kullanılan Minimum Veri Modelini,
- u) VEM Görüntüsü: SBYS hizmeti sağlayıcısı tarafından VEM'e uygun olarak hazırlanan ve güncellenen, SBYS'nin minimum içeriğini tanımlayan Minimum Veri Modeli görüntüsünü (view),
- ü) Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,
- v) VTYS: İlişkisel Veri Tabanı Yönetim Sistemini (RDBMS-Relational Database Management System),
- y) Zaman damgası: Bir elektronik verinin üretildiği, değiştirildiği, gönderildiği, alındığı veya kaydedildiği zamanın tespit edilmesi amacıyla elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt,

ifade eder.

İKİNCİ BÖLÜM

Genel Kurallar ve Kayıt Tescil Sistemi

Genel kurallar

MADDE 5- (1) SBYS hizmeti sağlayıcıları, aşağıdaki kurallara uymak zorundadır:

- a) SBYS'nin; Bakanlık tarafından belirlenen veri tanımlarına, iş kurallarına, yayımlanan yazılım sürüm notlarına, yayımlanan sağlık bilişim standartlarına ve veri gönderimi servislerine uyumlu olmasını sağlamak.
- b) Sağlık hizmeti sunucularında faaliyet gösterebilmek için KTS'de kayıtlı olmak.
- c) Veri gönderimi servislerini SBYS hizmeti sağlayıcısına ait olmayan donanımlardan kaynaklanan arızalar dışında kesintisiz çalıştırmak; verilerin olduğu anda doğru bir şekilde gönderilmesi ile gönderilen verilerin tam ve doğru olmasını sağlamak için teknik gereklilikleri yerine getirmek.
- ç) SBYS hizmeti alımı ve değişikliği süreçlerinde, SBYS hizmeti alıcısı tarafından belirlenen zaman aralığındaki VEM görüntülerinin herhangi bir gerekçe ile başka bir sisteme aktarılmak üzere istenmesi durumunda ilgili görüntüleri SBYS hizmeti alıcısına teslim etmek.
- d) SBYS hizmet süresinin sonunda sistemin kapatılmasını takiben yedekleri eksiksiz olarak almak ve güncel VEM sürümü görüntüleri ile birlikte SBYS hizmeti alıcısına teslim etmek.
- e) İdarenin uygun ortamı sağlaması hâlinde SBYS'yi, sözleşmenin sona erdiği tarihten itibaren iki ay süre ile tüm raporlama özellikleri çalışır durumda ve herhangi bir değişiklik yapılmasına izin vermeyecek şekilde açık tutmak.
- f) Genel Müdürlük tarafından yapılan veya yapılmasına onay verilen tüm projelerden Genel Müdürlükçe gerekli görülenlere tam entegre olmak.
- g) Genel Müdürlük tarafından yayımlanan diğer politika, kılavuz ve kurallara uymak.

Sisteme kayıt ve aktif liste

MADDE 6- (1) SBYS hizmeti sağlayıcılarının kayıt süreçleri, Genel Müdürlük tarafından geliştirilen Kayıt Tescil Sistemi üzerinden yürütülür. KTS'ye kayıt için gerekli olan belgeler Genel Müdürlüğün internet sitesinde yayımlanır.

(2) KTS'ye kayıt için gerekli olan belgeler Genel Müdürlüğe resmî yazı ile iletilir, kayıtlı elektronik posta (KEP) ile Bakanlığa gönderilir ya da e-Devlet üzerinden KTS'ye yüklenir.

(3) KTS'ye kayıt olacak SBYS hizmeti sağlayıcılarından ayrıca aşağıdaki belgeler istenir:

a) TS ISO/IEC 17021 standardı kapsamında Türk Akreditasyon Kurumundan (TÜRKAK) akredite edilmiş kurum ve kuruluşlardan alınmış TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi belgesi.

b) TS ISO/IEC 17065 akreditasyonuna sahip olup SPICE baş tetkikçisi bulunan kurum ve kuruluşlardan alınmış TS ISO/IEC 15504 en az ikinci seviyede SPICE belgesi veya CMMI baş tetkikçisi olan kurum ve kuruluşlar ile şirketlerden alınmış en az üçüncü seviyede CMMI belgesi (TS ISO/IEC 15504 en az ikinci seviyede SPICE belgesine, TSE tarafından eşdeğer bir belge yayımlanması durumunda TSE tarafından yayımlanan eşdeğer belge SPICE belgesi yerine kabul edilir. Eşdeğer belgenin yayımlanma tarihinden sonra başvurusu yapılan ve temin edilen SPICE belgeleri kabul edilmez.).

c) ÜTS kaydı gerektiren SBYS yazılımlarını üreten SBYS hizmeti sağlayıcılarından (b) bendinde belirtilen belge yerine ÜTS kaydına ilişkin belge istenir. Ancak SBYS hizmet sağlayıcısının ÜTS kaydı gerektirmeyen SBYS yazılımı da üretmesi halinde (b) bendinde belirtilen belge de istenir.

(4) Belgelerini eksiksiz teslim eden SBYS hizmeti sağlayıcılarının SBYS'leri, Genel Müdürlük veya yetkilendirdiği bir kuruluş tarafından denetlenir ve denetimden başarıyla geçenler KTS'ye kaydedilir. SBYS hizmeti sağlayıcılarına, gizlilik sözleşmesi imzalandıktan sonra gerçek ortamda veri gönderebilmeleri için yazılım erişim kodu teslim edilir. Yazılım erişim kodunun muhafazasından SBYS yetkilisi sorumludur.

(5) KTS'ye kayıtlı SBYS hizmeti sağlayıcıları; SBYS'lerini, sürümlerini ve mimarilerini KTS portalı üzerinden günceller. Kaydedilen bilgi ve belgelerde herhangi bir değişiklik olması halinde bu değişiklikler en geç on iş günü içerisinde KTS'ye işlenir.

(6) Kayıt ve denetim süreçleri başarı ile tamamlanan SBYS hizmeti sağlayıcıları aktif listeye alınarak Genel Müdürlüğün internet sitesinde ilan edilir.

(7) Genel Müdürlük, oluşan ihtiyaçlar doğrultusunda yeni SBYS türlerinin de KTS'ye tescil edilmesine karar verebilir. Yeni SBYS türünün KTS'ye tescil edilmesini müteakip ilgili SBYS hizmeti sağlayıcılarının KTS'ye kayıt olmaları ve üçüncü fıkrada istenilen belgeleri ibraz etmeleri için bir yıl süre verilir.

Pasif liste

MADDE 7- (1) Aktif listede yer alan SBYS hizmeti sağlayıcıları denetlenir. Denetim sonucunda herhangi bir eksikliğin tespit edilmesi halinde SBYS hizmeti sağlayıcısı uyarılır ve bu eksikliklerin belirlenen süre içerisinde giderilmesi istenir. Belirlenen süre içerisinde ilgili eksiklikleri gidermeyen SBYS hizmeti sağlayıcısı pasif listeye alınır.

(2) Pasif listeye alınan SBYS hizmeti sağlayıcısı aktif listeye geçene kadar KTS yetki belgesi alamaz.

Sistemden silinme

MADDE 8- (1) Pasif listeye alınmasını takip eden üç ay içinde aktif listeye geçemeyen SBYS hizmeti sağlayıcısı ile son bir yıl içerisinde üç defa pasif listeye alınan SBYS hizmeti sağlayıcısı KTS'den silinir.

(2) Gerçeğe aykırı bilgi ve belge sunan, veri gönderimlerine veya standartlara uyum konusunda yanıltıcı işlem yapan ya da yazılım erişim kodunu üçüncü kişilerle haksız fayda sağlamak amacıyla paylaştığı tespit edilen SBYS hizmeti sağlayıcısı, herhangi bir uyarıya gerek kalmaksızın KTS'den silinir ve KTS'ye yeniden kaydedilmek için yaptığı başvuru bir yıl süreyle kabul edilmez.

(3) 16 ncı ve 17 nci maddelerde yer alan hükümlere aykırılığın tespiti hâlinde ilgili SBYS hizmeti sağlayıcısı KTS'den silinir.

(4) KTS'den silinme tarihinden itibaren SBYS hizmeti sağlayıcısının yazılım erişim kodu en geç üç ay içerisinde kullanıma kapatılır. İlgili sağlık tesisinin resmî olarak talebi halinde yeni SBYS hizmeti alım süreci de göz önünde bulundurularak bu süre altı aya kadar Bakanlıkça uzatılabilir. Ancak SBYS hizmet sağlayıcısı KTS'de aktif listeye geçinceye kadar yeni bir sağlık hizmeti sunucusunda hizmet veremez.

(5) KTS'den silinen SBYS hizmeti sağlayıcısının KTS'ye yeniden kaydına ilişkin işlemler, 6 ncı maddede öngörülen hükümlere uygun olarak yürütülür.

(6) SBYS hizmeti sağlayıcısının KTS'de pasif listeye alınması veya KTS'den silinmesi hâlinde faaliyet göstermekte olduğu sağlık hizmeti sunucularının bağlı bulunduğu il sağlık müdürlüklerine Genel Müdürlük tarafından bildirim yapılır.

KTS yetki belgesi

MADDE 9- (1) Aktif listede yer alan SBYS hizmeti sağlayıcısının isteği üzerine KTS yetki belgesi düzenlenir. Üzerinde geçerlilik süresi bulunmayan veya doğrulanabilir nitelikte olmayan KTS yetki belgesi geçersiz sayılır.

(2) SBYS hizmeti sağlayıcısı olmayıp, herhangi bir SBYS hizmeti sağlayıcısının izni ile SBYS'yi ticari faaliyetlerine konu eden gerçek ve tüzel kişilere KTS yetki belgesi verilmez.

ÜÇÜNCÜ BÖLÜM

SBYS Hizmeti Alımı ve Kamu Hastaneleri Bilişim Süreçleri

SBYS hizmeti alımı süreçleri

MADDE 10- (1) İdare, SBYS hizmeti alımı süreçlerini Genel Müdürlük tarafından internet sitesinde yayımlanan Sağlık Bilgi Yönetim Sistemi Alım Kılavuzuna göre yürütür. İdareler, bu kılavuz ile çelişmeyen hükümleri şartnamelere veya yöntem beyanı dokümanına ekleyebilir.

(2) İdare tarafından SBYS hizmeti alımı süreçlerinde kullanılacak teknik şartnameler veya teknik dokümanlar, Genel Müdürlükçe Sağlık Bilgi Yönetim Sistemi Alım Kılavuzuna göre oluşturulan Alım Kılavuzu Sihirbazı üzerinden hazırlanır. İdare, Alım Kılavuzunda yer alan hükümler ile çelişmeyen isteklerine özel hükümler başlığı altında yer verir.

(3) İdare, 4734 sayılı Kanununun 38 inci maddesinin dördüncü fıkrası kapsamında SBYS hizmeti sağlayıcısından KTS yetki belgesini ibraz etmesini ister. İdare; 4/3/2009 tarihli ve 27159 mükerrer sayılı Resmî Gazete’de yayımlanan Hizmet Alımı İhaleleri Uygulama Yönetmeliğinin Ek-2’sinde yer alan Açık İhale Usulü ile İhale Edilen Hizmet Alımlarında Uygulanacak Tıp İdari Şartnamenin 7.1 maddesinin (h) bendi uyarınca düzenlenecek idari şartnamenin 7.1 maddesinin (h) bendinde, KTS yetki belgesini ister. Birden fazla SBYS hizmeti alımlarında iş, meri mevzuat hükümleri kapsamında kısmi teklife açılabilir. SBYS hizmeti sağlayıcısı alt yüklenicilerle de teklif sunabilir ancak SBYS hizmeti sağlayıcısı olan alt yüklenicilerin her birinin KTS’de kayıtlı olması ve KTS yetki belgesi sunması zorunludur.

(4) SBYS hizmeti alımı süreçlerinde alımı yapılacak her SBYS için ayrı KTS yetki belgesi istenir. SBYS hizmeti alımı süreçlerinde alımı yapılacak olan SBYS’lerden herhangi birini alt yüklenicinin sağlayacak olması hâlinde, alt yüklenici tarafından temin edilecek olan SBYS için de KTS yetki belgesi istenir.

(5) SBYS hizmeti alıcısı, SBYS hizmeti sağlayıcısı tarafından sunulan KTS yetki belgesinin geçerliliğini kontrol eder.

(6) Kit karşılığı laboratuvar cihazı alımı veya rapor okuma hizmeti alımı gibi ana hizmetin SBYS olmadığı ancak hizmetin unsurunun bir parçasının SBYS hizmeti olduğu durumlarda ana yükleniciden KTS yetki belgesi istenmez. Ancak hizmete ait sözleşme işlemleri esnasında ilgili SBYS hizmeti sağlayıcısına ait KTS yetki belgesi SBYS hizmeti alıcısına sunulur. KTS’ye kayıtlı olmayan SBYS hizmeti sağlayıcıları bu hizmetler için alt yüklenici olarak çalıştırılmaz veya bunlar tarafından geliştirilen yazılımlar bu hizmetlerde kullanılamaz.

(7) Veri Tabanı Yönetim Sistemi (VTYS) için açık kaynak kodlu VTYS tercih edilebilir, bu konuda sorumluluk tamamen SBYS hizmeti sağlayıcısına aittir.

(8) VTYS’nin açık kaynak kodlu olması durumunda lisans ile ilgili ibareler dikkate alınmaz.

(9) SBYS hizmeti sağlayıcısı tarafından temin edilen SBYS yazılımının çalışabildiği VTYS altyapısının İdarenin sahip olduğu VTYS'den farklı bir VTYS olması durumunda gereken VTYS lisansları SBYS hizmeti sağlayıcısı tarafından temin edilir.

(10) VTYS için gerekecek diğer her türlü lisans sözleşme süresince SBYS hizmeti sağlayıcısı tarafından İdare adına lisanslandırılmalı ve her türlü lisans İdarenin kendi şartnamelerinde belirtilen süreler içerisinde İdareye teslim edilmelidir.

(11) VTYS'nin performansından SBYS hizmeti sağlayıcısı sorumludur.

Kamu hastaneleri bilişim süreçleri

MADDE 11- (1) Kamu hastanelerinde, birimlerin talepleri doğrultusunda SBYS'lerde yapılacak iyileştirme, güncelleme ve ek geliştirmelerin tıbbi, idari ve teknik açılardan değerlendirilmesi için hastanelerde, yazılım geliştirme süreçlerini SBYS hizmeti sağlayıcısı ile birlikte yönetmek üzere Talep Değerlendirme Komisyonu oluşturulur.

(2) Talep Değerlendirme Komisyonunda; gelen talepleri tıbbi açıdan değerlendirmek üzere başhekim veya yardımcısı, idari açıdan değerlendirmek üzere hastane müdürü veya yardımcısı, bakım hizmetleri müdürü veya yardımcısı, bilgi işlem sorumlusu ile İdare tarafından belirlenen diğer çalışanlar yer alır. Komisyona ilgili SBYS hizmeti sağlayıcısından da katılım sağlanır ve geliştirme süreçleri birlikte değerlendirilir. İhtiyaç olması hâlinde bu komisyonlara, hastanenin bağlı bulunduğu il sağlık müdürlüğü bünyesindeki teknik personelden görevlendirme yapılır. Tüm ili kapsayan SBYS hizmeti alımlarında Talep Değerlendirme Komisyonu ilgili il sağlık müdürlüğünün bünyesinde kurulabilir.

(3) Talep Değerlendirme Komisyonu; İdarenin belirleyeceği tarihlerde toplanarak SBYS hizmeti sağlayıcısına iletilecek talepleri değerlendirir. Komisyon, teknik şartnamede yer alan ve modüller kapsamında kalmak kaydıyla yapılmasına karar verilen talepleri önemine göre sıralar, taleplerin yerine getirilmesi için ortak ve makul bir süre belirleyerek SBYS hizmeti sağlayıcısına iletir. Komisyondan geçmeyen talepler SBYS hizmeti sağlayıcısına gönderilemez ve SBYS hizmeti sağlayıcısı yükümlülük altına sokulamaz.

(4) İdare, bilgi işlem ile ilgili temel konular hakkında bilgi sahibi olan bir personeli bilgi işlem sorumlusu olarak görevlendirir. Bilgi işlem sorumlusu, görev yaptığı yerde sağlık bilgi sistemlerine ilişkin tüm süreçleri takip eder, gerekli iş ve işlemleri yerine getirir. Bilgi işlem sorumlusu olarak görevlendirilen personel mümkün olduğu kadar başka birimlerde çalıştırılmaz. Bilgi işlem

sorumlusunun görevleri, hizmet kıstasları, birimin fiziki şartları ve genel işleyişi Genel Müdürlük tarafından belirlenir.

(5) İdare, mevcut donanım ve yerel ağ cihazlarının kesintisiz çalıştırılabilmesi için gerekli olan bakım, onarım ve teknik destek hizmetleri ile ek donanımı temin eder.

(6) İdare, kendisine verilen son yedek üzerinde veri kurtarma testi yapmasını SBYS hizmeti sağlayıcısından ister ve gerekli kontrolleri sağlar.

DÖRDÜNCÜ BÖLÜM

Standartlar ve Entegrasyon, Görüntüleme, Veri Modeli, Verinin Teslimi ve Aktarımı,

Veri Yedekleme ve Arşivleme

Standartlar ve entegrasyon

MADDE 12- (1) Genel Müdürlük tarafından kullanımına karar verilen bilişim standartları ve veri gönderiminde dikkat edilecek hususlar Genel Müdürlüğün internet sitesinde yayımlanır ve gerektiğinde güncellenir.

(2) SBYS'ler, sağlık hizmeti sunucularının entegrasyona uygun cihazlarına, sistemlerine ve Bakanlıkça geliştirilen diğer sistemlere uyum sağlar.

(3) İdare, SBYS hizmeti alımı dokümanlarında veya sözleşmelerinde entegre edilecek sistem ve cihazların listesini tanımlar. Hizmet alımına ilişkin dokümanlarda veya sözleşmelerde önceden tanımlanmayan sistem ve cihazlar hariç olmak üzere Bakanlıkça geliştirilen sistemlere entegrasyon için İdareden bedel talep edilemez. Kamu özel iş birliği modeli ile işletilen hastanelerde faaliyet gösteren SBYS hizmeti sağlayıcıları, sözleşmede aksi belirtilmedikçe İdareden sistem ve cihaz entegrasyonları için ücret talep edemez.

(4) Entegrasyon yapılacak sistemler ile cihazlara ait puantaj tablosu Genel Müdürlüğün internet sitesinde yayımlanır ve her altı ayda bir güncellenir. Sistem ve cihaz entegrasyon ücreti, puantaj tablosunda belirtilen puan ile katsayının çarpımı sonucunda bulunan tutarı geçemez.

(5) Cihaz entegrasyon katsayısı Genel Müdürlükçe belirlenir ve Genel Müdürlüğün internet sitesinde yayımlanır.

(6) Entegrasyonlar sağlık hizmeti sunumunu aksatmayacak şekilde yapılır. Sağlık hizmeti sunumunu aksatacak olmasına rağmen yapılması zorunluluk arz eden değişiklik ve entegrasyon işleri ise SBYS hizmeti alıcısının bilgisi ve yönetiminde gerçekleştirilir.

(7) SBYS hizmeti sağlayıcılarının sağlık hizmeti sunucularına ait cihazlara ve Bakanlığın veri merkezlerine erişiminin ne şekilde olacağına dair kurallar Genel Müdürlük tarafından belirlenir.

(8) Entegre edilecek cihaz veya sistemlere ait entegrasyon dokümanları İdare tarafından SBYS hizmeti sağlayıcısına teslim edilir. Entegrasyon dokümanları teslim edilmeyen ve entegrasyon kabiliyeti bulunmayan cihaz veya sistemlerin entegrasyonu SBYS hizmeti sağlayıcısından talep edilmez.

Görüntüleme

MADDE 13- (1) Doğru hastaya doğru çekimin yapılabilmesi amacıyla PACS sistemlerinde DICOM çalışma listesi kullanılır ve tıbbi görüntü ile bu görüntüye ait istem bilgilerinin eşleştirilmesi sağlanır. SBYS hizmeti alıcısı, bu sistem kullanılmadan yapılacak hasta girişlerinin önüne geçmek amacıyla gerekli tedbirleri alır.

(2) Radyoloji ve patoloji raporlarının hekim tarafından onaylandıktan sonra değiştirilmesi gerekirse bu değişiklikler yeni bir ek rapor ile sisteme kaydedilir. Onaylanmış raporlar üzerinde değişikliğe izin verilmeyecek şekilde gerekli düzenlemeler yapılır.

(3) PACS sistemi kullanan sağlık hizmeti sunucularının Teletıp Sistemine entegre olmaları sağlanır. Entegrasyon takvimi ve ayrıntılı entegrasyon dokümanları Genel Müdürlük tarafından yayımlanır.

Veri modeli, verinin teslimi ve aktarımı

MADDE 14- (1) VEM görüntüsünün oluşturulmasında, Genel Müdürlükçe yayımlanan güncel VEM Kılavuzu esas alınır. VEM görüntüleri, sağlık hizmeti sunucusunun yerel veri tabanında bulunan ve VEM Standardının içerisinde yer alan tüm verileri içerecek şekilde oluşturulur. Oluşturulan VEM görüntülerinin kayıt sayısı ile sağlık hizmeti sunucusunun yerel veri tabanında VEM görüntüsü ile ilişkili tablo veya tablolarda bulunan kayıt sayısı tutarlı olmalıdır.

(2) SBYS hizmeti sağlayıcısı tarafından oluşturulan VEM görüntüleri, Genel Müdürlükçe hazırlanan VEM Doküman ve Veri Tabanı Analiz Programı ile denetlenir.

(3) Sağlık hizmeti sunucusuna özgü olup VEM içerisinde bulunmayan veriler için SBYS hizmeti alıcıları, ilgili veri tabanı sorgularını bir önceki SBYS hizmeti sağlayıcısına hazırlatır ve yeni başlayacak SBYS hizmeti sağlayıcısına teslim eder. Veri tabanı sorgusu ve sonucu olmayan veya VEM içerisinde bulunmayan verilerin aktarılması yeni SBYS hizmeti sağlayıcısından istenmez.

(4) Bir önceki SBYS hizmeti sağlayıcısı, verilerin tamamını orijinal veri tabanı formatında VEM'e uygun görüntüleri de içerecek şekilde kolay ve sorunsuz okunabilir bir medya ortamında üç kopya halinde SBYS hizmeti alıcısına teslim eder. Teslim sırasında düzenlenecek olan tutanakta; varsa

DVD/CD numarası, HDD seri numarası gibi ilgili medya ortamını tanımlayan işaretler, dosyaların boyutu ve oluşturulma tarihi, her bir tablodaki kayıt sayılarını gösteren bir doküman, dosyaları teslim eden SBYS yetkilisi ile teslim alan SBYS hizmeti alıcısı yetkilisinin bilgileri yer alır.

(5) SBYS hizmeti alıcısı, geçmiş yıllarda kullanılan SBYS'lerde bulunan ve bu SBYS'leri ayrı ayrı açarak ulaşabildiği verilerin tamamının SBYS'ye aktarımını, mevcut SBYS hizmet sağlayıcısından teknik destek alarak yapar. Bunun için gerekli olan veri tabanı yönetim sistemi erişim bilgileri, VEM görüntüsünü de içerecek şekilde SBYS hizmeti alıcısı tarafından temin edilir.

(6) PACS sistemlerinde oluşan görüntüler orijinal DICOM formatı veya kayıpsız JPEG formatında SBYS hizmeti alıcısına teslim edilir veya onun göstereceği ortamlara yüklenir. Önceki SBYS hizmeti sağlayıcısının sıkıştırma formatı kullanmış olması hâlinde; görüntüleri açmak için gerekli olan üçüncü parti yazılım bileşenleri, bu bileşenlerin veri aktarımı için öngörülen sürenin sonuna kadar gerekli olan lisansları ve bunların nasıl kullanılacağına dair dokümanlar, SBYS hizmeti alıcısına teslim edilir.

(7) İdare, sistemlerindeki geçmiş yıllara ait verilerin VEM görüntülerini elde edememesi hâlinde, verilerin VEM görüntüsü biçimine dönüştürülmesi için herhangi bir SBYS hizmeti sağlayıcısından hizmet alımı yapabilir. Bu hizmet alımı kapsamında idare tarafından VEM görüntüsü için ödenecek hizmet bedeli, mevcut SBYS hizmeti sağlayıcısına ödenen aylık SBYS hizmeti bedelinin veya demirbaşa kayıtlı yazılımlar için ödenen aylık bakım destek bedelinin yüzde yirmisini geçemez. Bu bedelin hesaplanmasında personel ve donanım maliyetleri dâhil edilmez.

(8) Veri aktarımı ile veri modelinin oluşturulmasında SBYS'lerin yetkinliğini test etmek için Genel Müdürlük tarafından internet sitesinde duyurulan tarihlerde Veri Aktarımı Teknik Yetkinlik Testi yapılır. Bu teste katılarak VEM'e göre kendi veri modelini oluşturan ve teslim edilen örnek veriler için başarılı bir şekilde aktarım sağlayan SBYS hizmeti sağlayıcılarına bir yıl süre ile geçerli Veri Aktarımı Teknik Yetkinlik Belgesi verilir. Bu belgeyi almaya hak kazanan SBYS hizmeti sağlayıcıları, hizmet alımı süreçlerinde veri aktarımı ve teslimiyle ilgili olarak yazılımları için kendilerinden demonstrasyon istenilmesi durumunda demonstrasyonun bu bölümünden başarıyla geçmiş sayılır. Veri Aktarımı Teknik Yetkinlik Belgesine sahip SBYS hizmeti sağlayıcılarına ait SBYS'lerin işlevselliğine yönelik demonstrasyon çalışmaları, örnek veri formatları veya SBYS hizmeti sağlayıcısı tarafından oluşturulmuş örnek veri yapısı üzerinden yapılır.

(9) Karar Destek Sistemleri gibi sistemlerde analiz amaçlı veri sorgulamaları VEM üzerinden yapılabilir. Buna istinaden VEM görüntüleri içerisinde yer almayan ancak eklenmesi istenilen veriler gerekçeleriyle birlikte Genel Müdürlüğe iletilir, gerekli ve yeterli bulunması halinde Genel

Müdürlükçe bir sonraki VEM sürümüne eklenir. İdare, SBYS hizmeti sağlayıcılarından bu amaçla herhangi bir web servis veya farklı bir ortama veri gönderimi talebinde bulunmaz.

(10) SBYS hizmeti sağlayıcısından VEM dışında herhangi bir görüntü oluşturması istenmez ancak gerekli durumlarda güvenlik, gizlilik ve performans gibi hususlar gözetilmek suretiyle ihtiyaç duyulması halinde SBYS hizmeti sağlayıcısı tarafından SBYS hizmeti alıcısına VEM üzerinden sadece verileri okuma yetkisi verilir. Eksikliği saptanan veriler için yeni VEM görüntüsü istekleri ise Genel Müdürlüğe iletilir.

(11) Sağlık hizmeti sunucusunda faaliyet göstermekte olan SBYS hizmeti sağlayıcısının herhangi bir sebeple değişmesi durumunda veri aktarımı için analiz verisi SBYS hizmeti alıcısı tarafından yeni SBYS hizmeti sağlayıcısına teslim edilir ve VEM standardına göre veri aktarımının yapılması sağlanır. Aktarılan verilere görüntüleyici ya da benzeri araçlardan değil veri tabanından bütünlüğü bozmadan doğrudan SBYS uygulaması üzerinden ulaşılabilmelidir. VEM'e uygun olarak hazırlanan verilerin aktarımında, Genel Müdürlükçe belirlenerek her VEM sürümünde yayımlanan sürelerle riayet edilir. Hastanın geçmiş sağlık verisine ihtiyaç duyulması durumunda yeni SBYS hizmeti sağlayıcısı, ilgili kayıtlara en kısa süre içerisinde erişir ve gerekli aktarımı en kısa sürede sağlar.

(12) AHBS hizmeti alımı ve değişiklik süreçlerinde önceki AHBS hizmeti sağlayıcısı, aile hekiminin kullanımı ve hizmetin sürekliliği için VEM görüntülerini içeren veri tabanı yedeğini oluşturmakla yükümlüdür. İlgili veri tabanı yedeği, taşınabilir ortamda imza karşılığında aile hekimine teslim edilir.

(13) Aile hekiminin herhangi bir gerekçe ile görevden ayrılması veya yer değiştirmesi durumunda önceki aile hekimi tarafından VEM görüntülerini içeren veri tabanı yedeği AHBS vasıtası ile alınır ve taşınabilir ortamda imza karşılığında il veya ilçe sağlık müdürlüğüne teslim edilir. Bu sürecin sonunda aile hekimi, kendi bilgisayarında hastalara ilişkin bulunan tüm verileri güvenli bir şekilde yok eder.

(14) VEM'de yapılacak sürüm değişikliklerine Genel Müdürlüğün internet sitesinden erişim sağlanır. SBYS hizmeti sağlayıcısı, VEM yeni sürümünün yayımlanarak duyurulmasından itibaren en geç iki ay içerisinde sisteminde gerekli güncellemeleri yapar.

(15) SBYS hizmeti sağlayıcısı tarafından Bakanlığın ve Sosyal Güvenlik Kurumunun merkezi sistemlerine veri gönderimi yapılırken, SBYS hizmeti sağlayıcısına verilen yazılım erişim kodu kontrolü ve SBYS hizmeti sağlayıcısı ile sağlık hizmeti sunucusu eşleştirme kontrolü yapılır.

(16) SBYS hizmeti alıcısına ait yedeklerin ve/veya güncel VEM sürümüne uygun görüntülerin aktarılması için Bakanlık tarafından altyapı hazırlanması durumunda yedekler ve/veya VEM görüntüleri Bakanlığa aktarılır.

Veri yedekleme ve arşivleme

MADDE 15- (1) SBYS hizmeti sağlayıcısı, SBYS'ye ait veri tabanı yedeklerini düzenli olarak alır ve bu yedekleri; SBYS hizmeti alıcısının ortamlarına veya Bakanlığın belirlediği ortamlara ya da her ikisine kaydeder. Bu yedekler içerisinde VEM'e uygun oluşturulan görüntüler de yer alır. SBYS hizmeti alıcısı, yedeklerin düzenli olarak alındığını kontrol eder. AHBS yazılımları için veri tabanı yedeği, Bakanlık tarafından herhangi bir barındırma hizmeti sunulana kadar AHBS yazılımı aracılığı ile aile hekimi tarafından günlük olarak alınır ve veri güvenliği yine aile hekimi tarafından sağlanır.

(2) Yedeklenen verilerin orijinal verileri yansıtması ve başarılı bir şekilde yedeklenip yedeklenmediğinden emin olunması için SBYS hizmeti sağlayıcısı tarafından en az altı ayda bir defa geri dönüş testi yapılır ve test sonuçları tutanak ile kayıt altına alınır. Tutanakta SBYS hizmeti alıcısının temsilcisine ait imza da bulunur. Geri dönüş testi için gerekli olan donanım ve lisans maliyeti SBYS hizmeti alıcısı tarafından karşılanır. AHBS için geri dönüş testleri, Genel Müdürlük tarafından da yapılabilir.

(3) Alınan yedeklerin bir kopyası, uygun ortamın sağlanması durumunda ilgili SBYS hizmeti alıcısının belirlediği farklı bir fiziksel lokasyona aktarılır.

BEŞİNCİ BÖLÜM

Gizlilik, İz Kayıtları, Denetim ve Yaptırım

Gizlilik

MADDE 16- (1) Sağlık hizmeti sunumu kapsamında işlenen kişisel veriler bakımından SBYS hizmeti sağlayıcısı veri işleyen sıfatını haiz olup, kişisel veri koruma mevzuatında öngörülen ilgili yükümlülükleri yerine getirir.

(2) Sağlık hizmeti sunumu ve ilgili süreçler kapsamında elde edilen veriler; sağlık hizmeti sunucularının veri kayıt ortamları, Bakanlığın merkezi sağlık veri sistemleri veya Genel Müdürlüğün onayladığı diğer veri kayıt ortamları haricinde hiçbir yere kaydedilemez ve aktarılamaz.

(3) Kişisel sağlık verilerinin muhafaza edileceği veri ortamları, talep üzerine Genel Müdürlük tarafından kurulan bir komisyon marifeti ile uzaktan ya da yerinde denetlenir ve onaylanır. Veriler yalnızca yurt içinde ve güvenli bir şekilde muhafaza edilir.

(4) Ülke dışında hizmet veren sağlık kuruluşlarında ise hizmet verilen yerdeki düzenlemeler çerçevesinde işlem tesis edilir.

(5) Kişisel veriler, ancak SBYS hizmeti alıcısı tarafından anonim hale getirilebilir. SBYS hizmeti alıcısı veya Bakanlığın izni olmaksızın kişisel veriler, SBYS hizmeti sağlayıcısı tarafından anonim hale getirilemez. Kişisel verilerin, SBYS hizmeti sağlayıcısı tarafından anonim hale getirilerek farklı amaçlarla işlendiğinin tespiti halinde başta 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ve 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu olmak üzere ilgili mevzuat hükümleri çerçevesinde işlem tesis edilir.

Olay ve iz kayıtları

MADDE 17- (1) SBYS hizmeti sağlayıcısı, herhangi bir bilgi güvenliği ihlal olayı oluştuğunda geriye dönük inceleme yapılmasını sağlamak üzere SBYS'lerde, SBYS verilerinin saklandığı veri tabanı ortamlarında ve SBYS'lerin sözleşme kapsamında sunulan hizmetlere ilişkin sorumluluk alanında bulunan yazılım ve donanım bileşenlerinde üretilen olay ve iz kayıtlarını saklamak üzere gerekli tedbirleri alır. SBYS hizmeti alıcısı, SAMİLOG kayıtlarını en az beş yıl, diğer kayıtları ise en az iki yıl süre ile kendi sunucularında saklar. AHBS'lerin SAMİLOG kayıtları ise AHBS üzerinden değiştirilemez şekilde veri tabanında saklanır.

(2) Olay ve iz kayıtları asgari olarak aşağıdaki hususları içerir:

a) SAMİLOG gereği oluşturulan kayıtları.

b) Veri tabanı seviyesindeki kullanıcılar tarafından yapılan veri ekleme, veri silme, veri güncelleme ve veri tabanı nesnelere üzerinde yapılan tüm değişiklikleri.

(3) SBYS hizmeti alıcısı tarafından sistemde kullanılan yazılım ve donanımların imkân ve kabiliyetleri doğrultusunda daha kapsamlı olay ve iz kaydı tutulmasının talep edilmesi halinde, bu maksatla ihtiyaç duyulan kaynaklar SBYS hizmeti alıcısı tarafından sağlanır.

(4) Olay ve iz kaydı üreten tüm sistemler, sistem genelinde tutarlı bir zaman bilgisi oluşturulması amacıyla SBYS hizmeti alıcısı tarafından sağlanacak bir zaman sunucusu aracılığı ile senkronize edilir.

(5) Olay ve iz kayıtları; yetkisiz erişim, silinme ve değiştirmeye karşı korunur. Üretilen olay ve iz kayıtları, Türkiye'de yerleşik nitelikli elektronik sertifika hizmet sağlayıcıları tarafından veya Genel Müdürlük tarafından sunulan nitelikli zaman damgası ile imzalanmak suretiyle saklanır.

Denetim

MADDE 18- (1) Bakanlık, mevzuat hükümleri kapsamında resen veya şikâyet üzerine SBYS hizmeti sağlayıcısını denetleyebilir ya da denetletebilir. Yapılacak olan denetim, SBYS hizmeti sağlayıcısının sorumluluğu ile verdiği hizmetin kapsamı dışına çıkamaz.

(2) Bakanlık veya il sağlık müdürlükleri bünyesinde izleme denetleme ekipleri kurulabilir veya denetim faaliyetleri için görevlendirmeler yapılabilir.

(3) Uzaktan ya da yerinde yapılacak SBYS denetimlerinde aşağıdaki konular hakkında denetleme yapılır:

a) SBYS'nin varlığı ve tekilliği.

b) Genel Müdürlük tarafından belirlenen iş akışlarına ve iş kurallarına uyumu.

c) Bakanlık merkezi veri sistemlerine entegrasyon ile veri gönderimi.

ç) Genel Müdürlük tarafından belirlenen standartlara uyumu.

d) Güncel VEM sürümüne uyumu ve veri aktarım kabiliyeti.

e) SBYS hizmeti sağlayıcısının KTS'ye kayıt durumu.

f) Kişisel verilerin korunması mevzuatı ile bilgi güvenliği düzenlemelerine uyumu.

(4) Bakanlık gerekli gördüğü durumlarda SBYS'ler için güvenlik ve sızma testlerini yapar veya yaptırır.

Yaptırım

MADDE 19- (1) SBYS hizmeti alıcısı; KTS'den silinen veya pasif listeye alınan SBYS hizmeti sağlayıcısına, aralarında imzalanan sözleşme hükümleri çerçevesinde yaptırım uygular.

(2) SBYS hizmeti sağlayıcısı veya alıcısı tarafından yasal düzenlemelerin ihlâli halinde ilgili mevzuat hükümleri çerçevesinde gerekli işlemler tesis edilir.

ALTINCI BÖLÜM

Yetkinlik Puanı

Yetkinlik puanı

MADDE 20- (1) SBYS hizmeti sağlayıcısı, sağlık hizmeti sunumunun daha kaliteli, kesintisiz ve sağlıklı yürütülmesi amacı ile değerlendirilir.

(2) SBYS hizmeti sağlayıcısının Genel Yetkinlik Puanı, Genel Müdürlüğün internet sayfasında yayımlanır. Genel Yetkinlik Puanının hesaplanmasında aşağıdaki kurallar geçerlidir:

a) SBYS hizmeti sağlayıcısına ait Genel Yetkinlik Puanı hesaplanırken, Personel Kapasite Puanı ve Teknik Değerlendirme Puanı olmak üzere iki ölçüt dikkate alınır.

b) Genel Yetkinlik Puanı; Personel Kapasite Puanı ve Teknik Değerlendirme Puanının Genel Müdürlükçe belirlenen ağırlıklı ortalaması alınarak bulunur.

(3) SBYS hizmeti sağlayıcısının personel yetkinliklerini gösteren Personel Kapasite Skorlama Ölçeği Genel Müdürlüğün internet sitesinde yayımlanır ve Personel Kapasite Puanı bu Ölçeğe göre hesaplanır.

(4) SBYS hizmeti sağlayıcısı, Genel Müdürlük tarafından belirlenen kriterlere uygunluğunun tespiti amacı ile her bir SBYS için ayrı ayrı teknik değerlendirmeye tâbi tutulur ve yapılan değerlendirme sonucunda Teknik Değerlendirme Puanı verilir. Teknik Değerlendirme Puanının hesaplanmasında aşağıdaki kurallar esas alınır:

a) SBYS hizmeti sağlayıcısının çalıştığı en az üç farklı sağlık hizmeti sunucusunda her yıl en az bir kez teknik değerlendirme yapılır. SBYS hizmeti sağlayıcısının üçten daha az sağlık hizmeti sunucusunda faaliyet göstermesi hâlinde teknik değerlendirme yalnızca ilgili sağlık hizmeti sunucularında yapılır.

b) Teknik değerlendirme, ilgili SBYS hizmeti sağlayıcısının faaliyet gösterdiği farklı illerdeki sağlık hizmeti sunucularında yapılır. Yalnızca tek bir ilde faaliyet gösteren SBYS hizmeti sağlayıcısının değerlendirmesi o ilde yapılır.

c) Teknik değerlendirmenin yapılacağı sağlık hizmeti sunucuları, SBYS hizmeti sağlayıcısının en az altı aydır faaliyet gösterdiği sağlık hizmeti sunucuları arasından seçilir.

ç) Teknik değerlendirmeler, Genel Müdürlük personeli tarafından yapılabileceği gibi Genel Müdürlüğün görevlendirmesi ile illerde bilişim alanında görev yapan personel tarafından da yapılabilir. Teknik değerlendirmeler, değerlendirme yapılacak olan sağlık hizmeti sunucusunun bulunduğu ilde görev yapan personel tarafından yapılamaz.

d) Teknik değerlendirme kriterleri, sağlık hizmeti sunucularında yapılacak yıllık denetimler başlamadan en az bir ay önce Genel Müdürlük tarafından internet sitesinde yayımlanır ve gerektiği durumlarda güncellenir.

(5) Açık kaynak kodlu veya lisans gerektirmeyen veri tabanı kullanan SBYS hizmeti sağlayıcılarının Genel Yetkinlik Puanı %5 oranında artırılır.

(6) Açık kaynak kodlu veya lisans gerektirmeyen işletim sistemi kullanan SBYS hizmeti sağlayıcılarının Genel Yetkinlik Puanı %5 oranında artırılır.

YEDİNCİ BÖLÜM

Çeşitli ve Son Hükümler

Anlaşmazlıkların halli

MADDE 21- (1) Veri aktarımlarında yaşanan anlaşmazlıklar, ilgili SBYS hizmeti alıcısının hakemliğinde eski ve yeni SBYS hizmeti sağlayıcısı bir araya getirilerek çözümlenir. Anlaşmazlığın tarafları, anlaşmazlığın çözümü için SBYS hizmeti alıcısı tarafından belirlenen sürelerle riayet eder. Çözüm sağlanamaması durumunda sözleşmeler ve ilgili mevzuat uyarınca gerekli süreçler işletilir.

(2) Bu Yönetmeliğin uygulanması sırasında doğacak tereddütleri ve uygulamaya ilişkin aksaklıkları gidermeye ve uygulamayı yönlendirmeye, ilke ve standartları belirlemeye ve uygulama birliğini sağlayacak gerekli düzenlemeleri yapmaya, bu hususta gerekli her türlü bilgi ve belgeyi istemeye, bu Yönetmelikte yer almayan konularda ilgili mevzuat hükümleri çerçevesinde karar vermeye Genel Müdürlük yetkilidir.

Geçiş hükmü

GEÇİCİ MADDE 1- (1) Alım Kılavuzu Sihirbazı Genel Müdürlükçe oluşturularak kullanıma açılana kadar, SBYS hizmeti alımı süreçleri kapsamında hazırlanan şartname ve dokümanlar, ilgili mevzuat hükümleri uyarınca herhangi bir yazılım desteği olmaksızın hazırlanır.

Yürürlük

MADDE 22- (1) Bu Yönetmeliğin;

- a) 17 nci maddesi yayımı tarihinden 12 ay sonra,
 - b) 20 nci maddesi yayımı tarihinden 20 ay sonra,
 - c) Diğer hükümleri ise yayımı tarihinde,
- yürürlüğe girer.

Yürütme

MADDE 23- (1) Bu Yönetmelik hükümlerini Sağlık Bakanı yürütür.

TEBLİŐLER

Bölüm İeriđi

- Vergi Usul Kanunu Genel Tebliđi (Sıra No: 538)
- İnternet Alan Adları Tebliđi
- Elektronik Ticarete Güven Damgası Hakkında Tebliđ
- Kamu İ Kontrol Standartları Tebliđi
- Bilgi Sistemleri Yönetimi Tebliđi
- Yapı Kooperatiflerine Ait Bilgilerin Elektronik Ortamda Kaydına Dair Tebliđ

Vergi Usul Kanunu Genel Tebliği (Sıra No: 538)

Resmî Gazete Tarihi : 31.05.2022

Resmî Gazete Sayısı : 31852

Hazine ve Maliye Bakanlığı (Gelir İdaresi Başkanlığı)'ndan:

VERGİ USUL KANUNU GENEL TEBLİĞİ

(SIRA NO: 538)

Amaç ve kapsam

MADDE 1- (1) Vergiye uyum düzeyinin ve kayıt dışı ekonomi ile mücadelede etkinliğin artırılmasına hizmet etmek amacıyla vergi kanunları çerçevesinde vergiye tabi olay ve bu olaya ilişkin işlemlerin kavranabilmesi büyük önemi haizdir.

(2) Bu kapsamda, internet ortamında yayımlanan ilanlara yönelik bazı bilgilerin alınmasına ilişkin usul ve esasların belirlenmesi bu Tebliğin amaç ve kapsamını oluşturmaktadır.

Yasal düzenlemeler

MADDE 2- (1) 4/1/1961 tarihli ve 213 sayılı Vergi Usul Kanununun;

a) 149 uncu maddesinde, "Kamu idare ve müesseseleri (Kamu hizmeti ifa eden kurum ve kuruluşlar dahil) ile gerçek ve tüzelkişiler vergilendirmeye ilişkin olaylarla ilgili olarak Maliye ve Gümrük Bakanlığı ve vergi dairesince kendilerinden yazı ile istenecek bilgileri belli fasılalarla ve devamlı olarak yazı ile vermeye mecburdurlar.",

b) Mükerrer 257 nci maddesinin birinci fıkrasında, "Maliye Bakanlığı;

....

4. Bu Kanunun 149 uncu maddesine göre devamlı bilgi vermek zorunda olanlardan istenilen bilgiler ile beyanname, bildirim, yazı, dilekçe, tutanak, rapor ve diğer belgelerin, şifre, elektronik imza veya diğer güvenlik araçları kullanılmak suretiyle internet de dâhil olmak üzere her türlü elektronik bilgi iletişim araç ve ortamında verilmesine, beyanname, bildirim, yazı, dilekçe, tutanak, rapor ve diğer belgelerin yetki verilmiş gerçek veya tüzel kişiler aracı kılınarak gönderilmesi hususlarında izin vermeye, standart belirlemeye veya zorunluluk getirmeye, beyanname, bildirim, yazı, dilekçe, tutanak, rapor ve diğer belgeler ile bilgilerin aktarımında uyulacak format ve standartlar ile

uygulamaya ilişkin usul ve esasları tespit etmeye, bu zorunluluk veya standartları beyanname, bildirim, yazı, dilekçe, tutanak, rapor ve diğer belgeler veya bilgi ve işlem çeşitleri, mükellef grupları ve faaliyet konuları itibarıyla ayrı ayrı uygulatmaya ya da belirlemeye,

....

7. Elektronik ticarete vergi güvenliğini sağlamak amacıyla elektronik ortamda ticari faaliyette bulunan gerçek ya da tüzel kişi hizmet sağlayıcılara ve/veya başkalarına ait iktisadi ve ticari faaliyetlerin yapılmasına elektronik ticaret ortamını sağlayan gerçek ve tüzel kişi aracı hizmet sağlayıcılara ticari faaliyetlerine ilişkin bildirim verme yükümlülüğü getirmeye, bildirim içeriği, format, standart, verilme süresi ve yöntemini belirlemeye, bunlarda değişiklik yapmaya, bildirim verme yükümlülüğünü iş hacmi, sektör, mükellef grupları, alış-satış tutarı, alım satım konu mal ve hizmet türleri itibarıyla belirlemeye, başkalarına ait iktisadi ve ticari faaliyetlerin yapılmasına ilişkin bildirim konu bilgilerin aracı hizmet sağlayıcıları tarafından alınması zorunluluğunu getirmeye, bu bent kapsamındaki bilgi ve bildirimlerin elektronik ortamda muhafaza ve ibraz edilmesi yükümlülüğü getirmeye ve uygulamaya ilişkin diğer usul ve esasları belirlemeye,

....

Yetkilidir. ...”

hükümleri yer almaktadır.

Tanımlar ve kısaltmalar

MADDE 3- (1) Bu Tebliğ uygulamasında;

- a) Aracı hizmet sağlayıcı: 23/10/2014 tarihli ve 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunda tanımlanan başkalarına ait iktisadi ve ticari faaliyetlerin yapılmasına elektronik ticaret ortamını sağlayan gerçek ya da tüzel kişiyi,
- b) Banka: 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununa göre faaliyette bulunan bankaları,
- c) Başkanlık: Gelir İdaresi Başkanlığını,
- ç) BTRANS: Gelir İdaresi Başkanlığı Bilgi Transfer Sistemini,
- d) İlan veren: İnternet ortamında kendisine ve/veya üçüncü kişilere yönelik her türlü ilanı veren gerçek ve tüzel kişiyi,

- e) Ödeme hizmeti: 5411 sayılı Kanuna göre faaliyette bulunan bankalar aracılığıyla yapılan ödemeler ile 20/6/2013 tarihli ve 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanununun 12 nci maddesinde belirtilen hizmetleri,
- f) Ödeme kuruluşu: 6493 sayılı Kanun kapsamında yetkilendirilmiş tüzel kişiyi,
- g) Sosyal ağ sağlayıcı: 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanununun 2 nci maddesinde tanımlanan sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses, konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşımlarına imkân sağlayan gerçek veya tüzel kişileri,
- ğ) Taşınır: 22/11/2001 tarihli ve 4721 sayılı Türk Medeni Kanununun 762 nci maddesi uyarınca mülkiyete konu olabilen eşyaları,
- h) Taşınmaz: 4721 sayılı Kanununun 704 üncü maddesinde sayılan arazi, tapu kütüğünde ayrı sayfaya kaydedilen bağımsız ve sürekli haklar ile kat mülkiyeti kütüğüne kayıtlı bağımsız bölümleri,
- ı) TCKN: Türkiye Cumhuriyeti kimlik numarasını,
- i) VKN: Vergi kimlik numarasını,
- j) Yer sağlayıcı: 5651 sayılı Kanununun 2 nci maddesinde tanımlanan ve hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri,
- k) YKN: Yabancı kimlik numarasını,
- ifade eder.

Sürekli bilgi verme zorunluluğu getirilenler ve bildirilecek bilgiler

MADDE 4- (1) Taşınır ve taşınmazlar ile mal ve hizmetlerin alınması, satılması veya kiralanmasının temin edilmesine yönelik olarak verilen ilanların yayımlanmasına aracılık eden aracı hizmet sağlayıcıları, sosyal ağ sağlayıcıları ile yer sağlayıcılar takvim yılının birer aylık süreleri içerisinde gerçekleştirmiş oldukları söz konusu işlemlere ilişkin olarak;

- a) Verilen hizmetin sağlandığı internet adres veya adreslerini,
- b) Hizmet verilen gerçek ya da tüzel kişilere ait ad soyad/unvan, TCKN/YKN/VKN bilgileri ile işyeri adres bilgilerini,

c) Hizmet verilenler adına gerçekleştirilen taşınır, taşınmaz, mal ve hizmet satış/kiralama işlemlerine ilişkin her bir tahsilat veya satış işlemi tutarı ve tarihi ile tahsil edilen tutarların aracılık hizmeti verilenlere ödenmesine ilişkin banka hesap bilgilerini,

ç) Başkanlık tarafından belirlenecek diğer bilgileri,

elektronik ortamda bu Tebliğin 5 inci maddesinde açıklanan yöntemle Başkanlık sistemlerine bildirmek zorundadır.

(2) Birinci fıkrada sayılanların, ödemelere ilişkin olarak satıcının/kiralayanın ticari temsilcisi olması sebebiyle ödemeye aracılık etmesi veya ödeme hizmetini bir dış hizmet olarak banka veya ödeme kuruluşundan alması bilgi verme yükümlülüğünü etkilemeyecektir.

(3) Aracı hizmet sağlayıcıları, sosyal ağ sağlayıcıları ile yer sağlayıcılar üzerinden ilan verenler, verdikleri ilanlara yönelik olarak söz konusu sağlayıcıların bu madde kapsamında Başkanlığa bildirmek zorunda olduğu bilgileri bunlara vermek zorundadırlar. Verilen ilanın konusu olan taşınır, taşınmaz, mal veya hizmetlerin mülkiyetinin ilan veren dışındaki bir gerçek veya tüzel kişiye ait olması durumunda, mülkiyet sahibine ilişkin bilgilerin de aracı hizmet sağlayıcıları, sosyal ağ sağlayıcıları ile yer sağlayıcılara bildirilmesi zorunludur.

(4) Aracı hizmet sağlayıcıları, sosyal ağ sağlayıcıları ile yer sağlayıcılar kendilerine üçüncü fıkra kapsamında bildirimde bulunmayan ilan verenlere ilişkin bilgileri bu Tebliğin 5 inci maddesinde belirtilen yöntemle Başkanlığa bildirecektir.

Verilecek bilgilere ilişkin format ve bilgi verme dönemi

MADDE 5- (1) Bu Tebliğin 4 üncü maddesi kapsamında sürekli bilgi verme yükümlülüğü getirilenlerin bildirmesi gereken bilgilere ilişkin veri format ve standardı Başkanlık tarafından BTRANS aracılığıyla duyurulacak ve bilgiler bu Sistem üzerinden Başkanlığa bildirilecektir.

(2) Bu Tebliğ kapsamında bildirilmesi zorunlu olan bilgiler Başkanlığa aylık olarak bildirilecektir. Bir aya ait bilgilerin, takip eden ayın son günü saat 23.59'a kadar bildirilmesi zorunludur.

(3) Başkanlık, bildirilmesi zorunlu olan bilgilerin kapsam ve içeriğinin belirlenmesinde yetkili olup, bunlar ile bunlara ilişkin veri format ve standardında yapılacak değişiklikler BTRANS aracılığıyla duyurulacaktır.

Sorumluluk ve ceza uygulaması

MADDE 6- (1) İlan verenler, aracı hizmet sağlayıcıları, sosyal ağ sağlayıcıları ile yer sağlayıcıların bu Tebliğ kapsamında bildirmek zorunda oldukları bilgileri bunlara temin etmek zorunda olduğu gibi bu bilgilerin doğruluğundan da sorumludurlar.

(2) Aracı hizmet sağlayıcıları, sosyal ağ sağlayıcıları ile yer sağlayıcılar ilan verenlerin bu Tebliğ gereğince temin etmeleri gereken bilgilerin kendilerine bildirilebilmesi için gerekli olan koşulları yerine getirmek zorundadır.

(3) Aracı hizmet sağlayıcıları, sosyal ağ sağlayıcıları ile yer sağlayıcılar BTRANS aracılığıyla bildirdikleri bilgilerin doğruluğundan sorumlu oldukları gibi bu bilgileri Başkanlığın belirlemiş olduğu format, standart ve bildirim yöntemine uygun olarak bildirmek zorundadırlar.

(4) Başkanlıkça belirlenen format, standart ve bildirim yöntemi haricinde bildirilen bilgiler kabul edilmeyecek ve bildirim yapılmamış sayılacaktır.

(5) Bilgi verme zorunluluğu getirilenler, Başkanlık sistemine bildirmekle yükümlü oldukları bilgileri 213 sayılı Kanununun defter, kayıt ve belgeler için öngördüğü muhafaza süreleri içerisinde elektronik ortamda saklamak ve istenildiğinde elektronik araçlar ve ortamlar vasıtası ile ibraz etmekle yükümlüdürler.

(6) Bu Tebliğde yapılan düzenlemeler kapsamında bildirilmesi gereken bilgileri bildirmeyen, eksik veya yanıltıcı bildirimde bulunanlar ile bu Tebliğle getirilen zorunluluklara uymayanlar hakkında 213 sayılı Kanununun ilgili ceza hükümleri tatbik olunur.

Diğer hususlar

MADDE 7- (1) Aracı hizmet sağlayıcıları, sosyal ağ sağlayıcıları ile yer sağlayıcıların ilk kez bildirim yapılacak tarihten önce BTRANS'ın kullanımına ilişkin başvurularını tamamlamaları gerekmektedir.

(2) Aracı hizmet sağlayıcıları, sosyal ağ sağlayıcıları ile yer sağlayıcılar tarafından, bu Tebliğ ile bildirilmesi zorunlu olan bilgilere yayımlanacak ilanlarda yer verilmesi zorunlu olmayıp, zorunluluk bu bilgilerin Başkanlığa bildirilmesine yöneliktir.

(3) Başkanlık, bu Tebliğde yer alan süreleri uzatmaya, bilgi verme dönemini bildirilecek bilgiler ve/veya mükellef grupları itibarıyla birlikte veya ayrı ayrı belirlemeye ve uygulamaya ilişkin usul ve esasları tespit etmeye yetkilidir.

İlk bildirim yapılması

GEÇİCİ MADDE 1- (1) Bu Tebliğ kapsamında sürekli bilgi verme yükümlülüğü getirilenler, ilk bildirimlerini ilk kez 2022 Haziran ayında verilen ilanlara ilişkin olarak 1/8/2022 tarihine (31/7/2022

tarixinin hafta sonuna isabet etmesi nedeniyle) kadar Başkanlığa yapmak zorundadır. Bu Tebliğ kapsamında sürekli bilgi verme yükümlülüğü getirilenlerin, söz konusu ilanların bu Tebliğin 4 üncü ve 5 inci maddelerince bildirilmesi zorunlu olan bilgileri içerecek şekilde alınması için gerekli olan teknik çalışmaları en kısa sürede tamamlamaları gerekmektedir. Bahse konu ilanların mezkûr maddeler gereğince bu fıkra kapsamında bildirim konusu edilebilmesi için ilan verenler tarafından ilanlara ilişkin ilave bilgi verilmesinin gerekmesi halinde bu durum ilan verenlere uygun yöntemlerle duyurulacak ve bu duyuruya rağmen bildirilmesi zorunlu olan bilgilerini tamamlamayanlar Başkanlığa bildirilecektir. 2022 Temmuz ve sonraki aylara ilişkin bildirimler bu Tebliğin 5 inci maddesinde yapılan açıklamalar uyarınca yapılacaktır.

(2) Bu Tebliğ kapsamında sürekli bilgi verme yükümlülüğü getirilenlerin bu Tebliğin yayımlandığı tarih itibarıyla yayında olan ilanlar ile bu Tebliğin yayımlandığı tarihten 31/5/2022 tarihine kadar (bu tarih dâhil) ilk kez verilen ilanlara (bunlardan bu Tebliğin yayımlandığı tarihten 31/5/2022 tarihine kadar yayından kaldırılanlar ile 2022 Haziran ayında yayını devam eden veya yayından kaldırılanlar dâhil) ilişkin bildirim 31/8/2022 tarihine kadar yapmaları gerekmektedir. Bu bildirim yapılabilmesi için ilan verenler tarafından ilanlara ilişkin ilave bilgi verilmesinin gerekmesi halinde bu durum ilan verenlere uygun yöntemlerle duyurulacak ve bu duyuruya rağmen bildirilmesi zorunlu olan bilgilerini tamamlamayanlar Başkanlığa bildirilecektir.

Yürürlük

MADDE 8- (1) Bu Tebliğ yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 9- (1) Bu Tebliğ hükümlerini Hazine ve Maliye Bakanı yürütür.

İnternet Alan Adları Tebliği

Resmî Gazete Tarihi : 21.08.2013

Resmî Gazete Sayısı : 28742

İNTERNET ALAN ADLARI TEBLİĞİ

BİRİNCİ BÖLÜM

Genel Hükümler

Amaç ve kapsam

MADDE 1 - (1) Bu Tebliğin amacı, 7/11/2010 tarihli ve 27752 sayılı Resmî Gazete’de yayımlanan İnternet Alan Adları Yönetmeliği kapsamında kayıt kuruluşlarının belirlenmesine, faaliyet göstermelerine ve “.tr” uzantılı internet alan adlarının yaşam çevrimine ilişkin usul ve esasları düzenlemektir.

Dayanak

MADDE 2 - (1) Bu Tebliğ, İnternet Alan Adları Yönetmeliğinin 14 üncü, 15 inci, 16 ncı ve 17 nci maddelerine dayanılarak hazırlanmıştır.

Diğer yükümlülükler

MADDE 13 - (1) KK;

a) İAAS'nin İAA'ya sahip olmak için gerekli şartları kaybetmesi, İAAS'nin verdiği bilgilerin tam ve/veya doğru olmadığının tespit edilmesi, İAAS'nin ilgili mevzuatı ihlal ettiğine ilişkin bilgi olması, İAA'nın tahsisinin iptaline yönelik mahkeme veya UÇHS kararı bulunması hallerinde TRABİS'e durum hakkında derhal bilgi vermekle,

b) İAA'ya ilişkin bir adli süreç veya uyuşmazlık çözüm süreci başlatıldığı yönünde bir bilgi aldığında TRABİS'e durum hakkında derhal bilgi vermekle,

c) İAA ile ilgili işlemler dolayısıyla elde ettiği bilgi ve belgeleri ilgili mevzuat hükümleri dışında üçüncü taraflarla paylaşmamakla ve İAA işlemlerinin gereğini yerine getirmek dışında hiçbir amaç için kullanmamakla,

ç) Kurumun talep ettiği tüm bilgi ve belgeleri Kuruma derhal sunmakla,

- d) Uyuşmazlık çözümü mekanizmasında KK'nın yapması gereken tüm yükümlülükleri titizlikle ve ivedilikle yerine getirmekle,
- e) Kötü niyetli İAA tahsisine karşı tedbir almakla,
- f) Transfer işlemleri için gereken süreci İAAS'nin kolaylıkla tamamlamasını sağlamakla,
- g) Faaliyete geçmek için Kuruma yapmış olduğu başvuruda sunduğu bilgi ve belgelerde herhangi bir değişiklik meydana gelmesi halinde, bu değişiklikleri (Değişik ibare:RG-17/10/2020-31277) on (10) işgünü içinde Kuruma bildirmekle,
- ğ) Her yıl Mart ayı sonuna kadar bir önceki yıla ait faaliyet raporunu Kuruma sunmakla,
- h) Devletin İAA strateji ve politikalarına uyum sağlamakla,
- ı) (Değişik:RG-17/10/2020-31277) Kişisel verilerin korunmasına ilişkin mevzuat ile ilgili diğer mevzuata uymakla,
- i) (Ek:RG-17/10/2020-31277) TRABİS'e entegre olan sistemlerini ve yedeklerini Türkiye Cumhuriyeti sınırları içinde bulundurmamakla,
- j) (Ek:RG-17/10/2020-31277) Bir önceki yıla ait ve internet alan adı işlemlerine ilişkin net satış tutarlarını içeren vergi dairesi, imza atmaya yetkili serbest muhasebeci mali müşavir veya yeminli mali müşavir onaylı gelir tablolarını, her yılın Mayıs ayı sonuna kadar Kuruma göndermekle, yükümlüdür.

DÖRDÜNCÜ BÖLÜM

İnternet Alan Adı Yaşam Çevrimi

İnternet alan adı başvurusu

MADDE 14 - (1) İAA başvuruları KK internet sayfasında yer alan elektronik başvuru formunun başvuru sahibi tarafından doldurulması suretiyle yapılır.

(2) KK, elektronik başvuru formunun başvuru sahibinden alınması sırasında;

a) Başvuru sahibinin;

1) KK'ya tam ve doğru bilgiler vereceğini, bu bilgilerde meydana gelebilecek değişiklikleri derhal KK'ya bildireceğini,

2) Üçüncü kişilerin haklarını ihlal etmeyeceğini,

3) İAA'yı hukuka aykırı bir şekilde kullanmayacağını,

- 4) İAA'ya ilişkin bir alternatif uyuşmazlık çözüm sürecinin başlaması durumunda buna katılacağını,
- 5) KK'lar arası zorunlu transfer hallerinde bilgilendirilmesini müteakip gereken işlemleri yapacağını,
- 6) Yönetmelikte ve ilgili mevzuatta geçen iptal hallerinde İAA'nın iptal edileceğini,
- 7) İptal veya feragat durumunda bu işlemlerin İAAS lehine bir hak doğurmayacağını,
- 8) Başvuru esnasında bildirdiği e-posta adresine yapılan bildirimlerin kendisine yapıldığını,
- 9) Türkiye Cumhuriyeti mevzuatına uyacağını,

kabul, beyan ve taahhüt etmesini sağlar.

b) (Değişik:RG-17/10/2020-31277) Başvuru sahibine; 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuatı çerçevesinde gerekli bilgilendirmeleri yapmakla yükümlüdür.

c) (Değişik:RG-17/10/2020-31277) Başvuru sahibi gerçek kişi ise, başvuru sırasında aşağıdaki bilgileri alır:

- 1) Ad, soyad,
- 2) Telefon,
- 3) Adres,
- 4) T.C. kimlik numarası veya yabancı kimlik numarası,
- 5) E-posta adresi,
- 6) Varsa faks,
- 7) Varsa internet sitesi adı,
- 8) İdari, teknik ve ödeme sorumlularının adı ve e-posta adresleri,
- 9) Kurum tarafından uygun görülen diğer bilgi ve belgeler.

ç) (Ek:RG-17/10/2020-31277) Başvuru sahibi tüzel kişi ise başvuru sırasında aşağıdaki bilgileri alır:

- 1) Unvan veya kuruluş adı,
- 2) Telefon,
- 3) Adres,
- 4) Vergi kimlik numarası,
- 5) E-posta adresi,

- 6) Varsa faks,
- 7) Varsa internet sitesi adı,
- 8) İdari, teknik ve ödeme sorumlularının adı ve e-posta adresleri,
- 9) Kurum tarafından uygun görülen diğer bilgi ve belgeler.

(3) KK, aldığı İAA başvurularını derhal TRABİS'e iletir.

(4) TRABİS gerekli görmesi halinde kontroller yapabilir ve başvuruyu reddedebilir. KK, başvuru sahibini başvurusunun ret gerekçesi konusunda derhal bilgilendirir.

(5) TRABİS tarafından onaylanan başvuru sonrasında İAA kaydı veri tabanına girilir ve İAAS KK tarafından derhal bilgilendirilir.

(6) KK, İAA tahsisi yaparken başvuru sahibini İAA tahsisi dışında başka bir hizmeti almak zorunda bırakmaz.

(7) Belgeli tahsis gerektiren başvurularda uygulanacak usul ve esaslar Kurul tarafından belirlenir.
(Mülga cümle:RG-17/10/2020-31277) (...) (Mülga cümle:RG-17/10/2020-31277) (...)

(8) (Mülga:RG-17/10/2020-31277)

(9) (Mülga:RG-17/10/2020-31277)

(10) Başvuru sırasında İAA yazımında yapılan maddi hatalar İAA'nın tahsisine kadar düzeltilebilir. Başvuru süreci sonunda TRABİS'e iletilen ve tahsisi yapılan İAA için maddi hata düzeltilmesi yapılmaz.

TRABİS'e gönderilecek veriler

MADDE 15 - (1) KK başvuruların mevzuata uygun olduğunu kontrol ettikten sonra TRABİS'e iletir.
(Değişik cümle:RG-17/10/2020-31277) KK başvuru sırasında aldığı bilgileri ve Kurum tarafından istenebilecek diğer bilgi ve elektronik belgeleri TRABİS'e gönderir. Bu bilgi ve belgelerde değişiklik olması halinde KK bunların güncel hallerini derhal TRABİS'e iletir.

(...)

Rehber

MADDE 19 - (Değişik:RG-17/10/2020-31277)

(1) Rehberlik hizmeti TRABİS vasıtasıyla Kurum tarafından verilir.

(2) Rehberde asgari aşağıdaki bilgilere yer verilir:

- a) Tahsisli İAA,
- b) Birincil ve ikincil ad sunucuların isimleri,
- c) İlgili KK bilgileri,
- ç) İAA'nın tahsis edildiği tarih,
- d) İAA'nın tahsis süresinin bitiş tarihi,
- e) İAAS'nin, adı, adresi ve e-posta adresi,
- f) Rehber bilgisinin güncellenme tarihi.

(3) KK, gerçek kişi İAAS'nin kişisel verilerinin rehberde paylaşımına ilişkin açık rızasını alır. Gerçek kişi İAAS'nin açık rızasının bulunmaması halinde ikinci fıkranın (e) bendinde yer alan bilgiler rehberde yayımlanmaz. KK, rehberdeki e-posta adresi alanında yayımlanmak üzere anonimleştirilmiş bir e-posta adresi belirleyerek İAAS'ye ve TRABİS'e bildirir. Bu adrese gelen e-postalar KK tarafından İAAS'ye ait e-posta adresine iletilir.

(4) Gerçek kişi olmayan İAAS'nin açık rızası aranmaksızın ikinci fıkradaki tüm bilgiler rehberde yayımlanır.

(...)

Elektronik Ticarete Güven Damgası Hakkında Tebliğ

Resmî Gazete Tarihi : 06.06.2017

Resmî Gazete Sayısı : 30088

ELEKTRONİK TİCARETTE GÜVEN DAMGASI HAKKINDA TEBLİĞ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak, Tanımlar ve Kısaltmalar

Amaç

MADDE 1 - (1) Bu Tebliğin amacı, elektronik ticarete güven damgasına ilişkin usul ve esasları belirlemektir.

Kapsam

MADDE 2 - (1) Bu Tebliğ, güven damgası almak isteyen ve Elektronik Ticarete Hizmet Sağlayıcı ve Aracı Hizmet Sağlayıcılar Hakkında Yönetmelik kapsamında bulunan aracı hizmet sağlayıcı ve kendine ait elektronik ticaret ortamında faaliyet gösteren hizmet sağlayıcının uyması gereken güvenlik ve hizmet kalitesi standartlarını; güven damgası sağlayıcının faaliyetleri ve yükümlülükleri ile güven damgasının verilmesi, askıya alınması ve iptaline ilişkin usul ve esasları kapsar.

(2) 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununa ve 20/6/2013 tarihli ve 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanuna göre faaliyet izni almış kuruluşlar bu Tebliğ kapsamı dışındadır.

Dayanak

MADDE 3 - (1) Bu Tebliğ, (Değişik ibare:RG-13/8/2020-31212) 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete'de yayımlanan 1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinin 446 ncı maddesi, 23/10/2014 tarihli ve 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunun 11 inci maddesi ile 26/8/2015 tarihli ve 29457 sayılı Resmî Gazete'de yayımlanan Elektronik Ticarete Hizmet Sağlayıcı ve Aracı Hizmet Sağlayıcılar Hakkında Yönetmeliğin 16 ncı maddesine dayanılarak hazırlanmıştır.

(...)

İKİNCİ BÖLÜM

Güven Damgasının Tahsisi, Askıya Alınması ve İptali

Güven damgası alma şartları

MADDE 5 - (1) Güven damgası almak isteyen hizmet sağlayıcı ve aracı hizmet sağlayıcı asgari olarak aşağıdaki standartlara uyar:

- a) (Değişik:RG-25/2/2021-31406) Kişisel veri ve ödeme bilgisi içeren her türlü işlemin internet sitesi, mobil site ve uygulamada EV SSL veya SSL ile gerçekleştirilmesini sağlar.
- b) Güven damgası başvurusunda bulunmadan en fazla üç ay önce ve her takvim yılı içinde en az bir defa, Türk Standardları Enstitüsü tarafından onaylı A veya B sınıfı sızma testi firmalarına sızma testi yaptırarak gerekli önlemleri alır ve bu önlemleri aldığına ilişkin doğrulama testi yaptırır.
- c) (Değişik:RG-13/8/2020-31212) 23/2/2006 tarihli ve 5464 sayılı Banka Kartları ve Kredi Kartları Kanununa, 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna, 20/6/2013 tarihli ve 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanuna, 7/11/2013 tarihli ve 6502 sayılı Tüketicinin Korunması Hakkında Kanuna, 23/10/2014 tarihli ve 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanuna, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununa ve bu kanunların ikincil düzenlemelerine, 14/1/2015 tarihli ve 6585 sayılı Perakende Ticaretin Düzenlenmesi Hakkında Kanunun ek 1 inci maddesi ve bu maddeye dayanılarak hazırlanan ikincil düzenlemeler ile elektronik ticaret ortamında satışı yasak olan ya da şarta bağlanan ürünlere ilişkin düzenleme ve idari kararlara uygun süreçler tasarlar.
- ç) Elektronik ticaret ortamında çocukların fiziksel, zihinsel, ahlaki, psikolojik ve toplumsal gelişim özelliklerini olumsuz yönde etkileyebilecek içeriğe yönelik tedbirleri alır.
- d) Elektronik ticarete konu malın stok bilgisi, içeriği, malzemesi, ölçüleri gibi özelliklerine, kullanımına ve varsa garantisine, teknik desteğine ve bunların kim tarafından sağlanacağına ilişkin detaylar ile gerçek boyutlarının anlaşılmasını mümkün kılan görselleri, tedarik, kargo ve teslimat süresi gibi hususları, sipariş alıcıya teslim edilinceye kadar siparişin durumu hakkında gerekli bilgileri ve kargo takip imkânını sunar ya da sunulmasına olanak sağlar.
- e) Elektronik ticarete konu hizmetin kim tarafından sağlanacağı, kapsamı ve süresi gibi bilgileri sunar ya da sunulmasına olanak sağlar.
- f) Bu fıkranın (d) ve (e) bentlerine ilişkin taahhütlerine uygun hareket eder.

g) Alıcının siparişi hakkında bilgi alabilmesi, talep ve şikâyetlerini internet tabanlı iletişim yöntemlerinden en az biri ve telefon aracılığıyla iletebilmesi için müşteri hizmetleriyle iletişim imkânı sunar. Talep ve şikâyetlerin etkin bir şekilde yönetilmesini, sonuçlandırılmasını ve konuya ilişkin alıcının bilgilendirilmesini sağlar.

(2) Güven damgası almak isteyen hizmet sağlayıcı ve aracı hizmet sağlayıcının gerçek kişi olması halinde kendisinin ve yetkili temsilcisinin, tüzel kişi olması halinde ise yöneticilerinin ve yetkili temsilcilerinin 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 53 üncü maddesinde belirtilen süreler geçmiş olsa bile; kasten işlenen bir suçtan dolayı bir yıl veya daha fazla süreyle hapis cezasına ya da affa uğramış olsa bile devletin güvenliğine karşı suçlar, Anayasal düzene ve bu düzenin işleyişine karşı suçlar, zimmet, irtikâp, rüşvet, hırsızlık, dolandırıcılık, sahtecilik, güveni kötüye kullanma, hileli iflas, ihaleye fesat karıştırma, edimin ifasına fesat karıştırma, suçtan kaynaklanan malvarlığı değerlerini aklama, kaçakçılık veya bilişim suçlarından mahkûm olmaması gerekir.

(3) Güven damgası almak isteyen hizmet sağlayıcı ve aracı hizmet sağlayıcı iflas etmiş ise itibarın iadesinin sağlanmış olması gerekir.

(...)

Kamu İç Kontrol Standartları Tebliği

Resmî Gazete Tarihi : 26.12.2007

Resmî Gazete Sayısı : 26738

KAMU İÇ KONTROL STANDARTLARI TEBLİĞİ

Bilindiği üzere, 10/12/2003 tarihli ve 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanununun Beşinci Kısımında "iç kontrol sistemi" düzenlenmiştir. Bu kısımda, iç kontrol sistemine ilişkin olarak; iç kontrolün tanımı ve amacı, kontrolün yapısı ve işleyişi, ön mali kontrol, mali hizmetler birimi, muhasebe hizmeti ve muhasebe yetkilisinin yetki ve sorumlulukları, muhasebe yetkilisinin nitelikleri ve atanması, iç denetim, iç denetçinin görevleri, iç denetçilerin nitelikleri ve atanması, iç denetim koordinasyon kurulu, iç denetim koordinasyon kurulunun görevleri hususlarına yer verilmiştir.

5018 sayılı Kanunun 55 inci maddesinde iç kontrol, "idarenin amaçlarına, belirlenmiş politikalara ve mevzuata uygun olarak faaliyetlerin etkili, ekonomik ve verimli bir şekilde yürütülmesini, varlık ve kaynakların korunmasını, muhasebe kayıtlarının doğru ve tam olarak tutulmasını, malî bilgi ve yönetim bilgisinin zamanında ve güvenilir olarak üretilmesini sağlamak üzere idare tarafından oluşturulan organizasyon, yöntem ve süreçle iç denetimi kapsayan malî ve diğer kontroller bütünü" olarak tanımlanmıştır.

Kanunun 56 ncı maddesinde iç kontrolün amaçları;

- Kamu gelir, gider, varlık ve yükümlülüklerinin etkili, ekonomik ve verimli bir şekilde yönetilmesini,
- Kamu idarelerinin kanunlara ve diğer düzenlemelere uygun olarak faaliyet göstermesini,
- Her türlü malî karar ve işlemlerde usulsüzlük ve yolsuzluğun önlenmesini,
- Karar oluşturmak ve izlemek için düzenli, zamanında ve güvenilir rapor ve bilgi edinilmesini,
- Varlıkların kötüye kullanılması ve israfını önlemek ve kayıplara karşı korunmasını, sağlamak olarak belirlenmiştir.

Kanunun 57 nci maddesinde ise kamu idarelerinin malî yönetim ve kontrol sistemlerinin harcama birimleri, muhasebe ve malî hizmetler ile ön malî kontrol ve iç denetimden oluştuğu belirtilmiş, yeterli ve etkili bir kontrol sisteminin oluşturulabilmesi için;

- Mesleki deęerlere ve dürüst yönetim anlayışına sahip olunması,
- Malî yetki ve sorumlulukların bilgili ve yeterli yöneticilerle personele verilmesi,
- Belirlenmiş standartlara uyulmasının sağlanması,
- Mevzuata aykırı faaliyetlerin önlenmesi,
- Kapsamlı bir yönetim anlayışı ile uygun bir çalışma ortamının ve saydamlığın sağlanması,

bakımından ilgili idarelerin üst yöneticileri ile diğer yöneticileri tarafından görev, yetki ve sorumluluklar göz önünde bulundurulmak suretiyle gerekli önlemlerin alınması öngörülmüştür.

Kanunun 11 inci maddesinde, üst yöneticilerin, mali yönetim ve kontrol sisteminin işleyişinin gözetilmesi, izlenmesi ve Kanunda belirtilen görev ve sorumlulukların yerine getirilmesinden sorumlu oldukları ve bu sorumluluğun gereklerini harcama yetkilileri, mali hizmetler birimi ve iç denetçiler aracılığıyla yerine getirecekleri hükme bağlanmıştır.

Buna göre üst yöneticilere, iç kontrol sisteminin kurulması ve gözetilmesi, iç kontrol sisteminin bir gereği olarak yazılı prosedür ve talimatların oluşturulması gibi her türlü düzenlemelerin yapılması, harcama yetkililerine ise görev ve yetki alanları çerçevesinde, idari ve malî karar ve işlemlere ilişkin olarak iç kontrolün işleyişini sağlama sorumluluğu verilmiş bulunmaktadır.

Kanunun 60, 61, 63 ve 64 üncü maddelerinde, mali hizmetler birimleri, muhasebe yetkilileri ve iç denetçilerin iç kontrol alanındaki görev ve sorumluluklarına yer verilmiştir. Buna göre; mali hizmetler birimleri, idarenin iç kontrol sisteminin kurulması, standartlarının uygulanması ve geliştirilmesi konularında çalışmalar yapmak ve ön mali kontrol faaliyetini yürütmekten, muhasebe yetkilileri, ödeme emri belgesi ve eklerinin kontrolünden, muhasebe işlemlerinin belirlenmiş standartlara ve usulüne uygun olarak kaydedilmesinden, raporlanmasından, muhafazasından ve denetime hazır halde bulundurulmasından, iç denetçiler ise idarelerin iç kontrol sistemlerinin denetlenmesinden ve geliştirilmesi yönünde önerilerde bulunulmasından sorumludurlar.

Kanunun 55 inci maddesinin ikinci fıkrasında, "Görev ve yetkileri çerçevesinde, mali yönetim ve iç kontrol süreçlerine ilişkin standart ve yöntemler Maliye Bakanlığınca, iç denetime ilişkin standart ve yöntemler ise İç Denetim Koordinasyon Kurulu tarafından belirlenir, geliştirilir ve uyumlaştırılır. Bunlar ayrıca sistemlerin koordinasyonunu sağlar ve kamu idarelerine rehberlik hizmeti verir" hükmü yer almaktadır. Buna göre, İç Denetim Koordinasyon Kurulunun 20.11.2006 tarihli ve (12) sayılı kararı ile Kamu İç Denetim Standartları belirlenmiş bulunmaktadır. Kamu İç Kontrol

Standartları ise COSO modeli, INTOSAI Kamu Sektörü İç Kontrol Standartları Rehberi ve Avrupa Birliği İç Kontrol Standartları çerçevesinde Maliye Bakanlığı tarafından belirlenmiştir.

Bilindiği üzere, 31.12.2005 tarihli ve 26040 (3. mükerrer) sayılı Resmî Gazete’de yayımlanan İç Kontrol ve Ön Mali Kontrole İlişkin Usul ve Esasların "İç kontrol standartları" başlıklı 5 inci maddesinde, iç kontrol standartlarının, merkezi uyumlaştırma görevi çerçevesinde Maliye Bakanlığı tarafından belirlenip yayımlanacağı, kamu idarelerinin malî ve malî olmayan tüm işlemlerinde bu standartlara uymakla ve gereğini yerine getirmekle yükümlü bulunduğu, Kanuna ve iç kontrol standartlarına aykırı olmamak koşuluyla, idarelerce, görev alanları çerçevesinde her türlü yöntem, süreç ve özellikli işlemlere ilişkin standartlar belirlenebileceği belirtilmiştir.

Bu çerçevede, kamu idareleri tarafından görev alanları çerçevesinde her türlü yöntem, süreç ve özellikli işlemlere ilişkin olarak belirlenebilecek ayrıntılı standartlar, 5018 sayılı Kanuna, ilgili diğer mevzuata ve Kamu İç Kontrol Standartlarına uygun olmak ve idareye münhasır spesifik süreçlere ilişkin olmak zorundadır. İdarelerce gerek görülmesi halinde hazırlanabilecek İdare Ayrıntılı İç Kontrol Standartları, idarelerin yasal ve idari yapıları ile personel ve mali durumları gibi her bir idarenin kendine özgü koşulları dikkate alınarak katılımcı yöntemlerle belirlenecek ve üst yönetici onayını izleyen 10 işgünü içinde Maliye Bakanlığına gönderilecektir.

Kamu idarelerinin, iç kontrol sistemlerinin Kamu İç Kontrol Standartlarına uyumunu sağlamak üzere; yapılması gereken çalışmaların belirlenmesi, bu çalışmalar için eylem planı oluşturulması, gerekli prosedürler ve ilgili düzenlemelerin hazırlanması çalışmalarını yürütmeleri ve bu çalışmaları en geç 31.12.2008 tarihine kadar tamamlamaları gerekmektedir. Söz konusu çalışmaların etkili bir şekilde ve zamanında yürütülmesini sağlamak üzere, idarelerin üst yöneticileri tarafından gerekli önlemler alınacaktır.

Diğer taraftan, 26.5.2006 tarihli ve 26179 sayılı Resmî Gazete’de yayımlanan Kamu İdarelerinde Stratejik Planlamaya İlişkin Usul ve Esaslar Hakkında Yönetmelikle belirlenen geçiş takvimi uyarınca, 2008 ve sonraki yıllarda stratejik plan ve performans programı hazırlayacak idareler, hazırlık çalışmalarında bunlara ilişkin standartları da dikkate alacaklardır. Stratejik plan ve performans programı hazırlamayacak kamu idareleri ise bu plan ve programların hazırlanması dışında kalan hususlara uyum sağlayacaklardır.

Tebliğ olunur.

KAMU İÇ KONTROL STANDARTLARI

Kamu İç Kontrol Standartları, idarelerin, iç kontrol sistemlerinin oluşturulmasında, izlenmesinde ve değerlendirilmesinde dikkate alınmaları gereken temel yönetim kurallarını göstermekte ve tüm kamu idarelerinde tutarlı, kapsamlı ve standart bir kontrol sisteminin kurulmasını ve uygulanmasını amaçlamaktadır.

Kamu İç Kontrol Standartları, uluslararası standartlar ve iyi uygulama örnekleri çerçevesinde, iç kontrolün; kontrol ortamı, risk değerlendirmesi, kontrol faaliyetleri, bilgi ve iletişim ile izleme bileşenleri esas alınarak, tüm kamu idarelerinde uygulanabilir düzeyde olmasını sağlamak üzere genel nitelikte düzenlenmiştir.

1. KONTROL ORTAMI STANDARTLARI

Kontrol ortamı, iç kontrolün diğer unsurlarına temel teşkil eden genel bir çerçeve olup, kişisel ve mesleki dürüstlük, yönetim ve personelin etik değerleri, iç kontrole yönelik destekleyici tutum, mesleki yeterlilik, organizasyonel yapı, insan kaynakları politikaları ve uygulamaları ile yönetim felsefesi ve iş yapma tarzına ilişkin hususları kapsar.

Standart: 1. Etik Değerler ve Dürüstlük

Personel davranışlarını belirleyen kuralların personel tarafından bilinmesi sağlanmalıdır.

Bu standart için gerekli genel şartlar:

1.1. İç kontrol sistemi ve işleyişi yönetici ve personel tarafından sahiplenilmeli ve desteklenmelidir.

1.2. İdarenin yöneticileri iç kontrol sisteminin uygulanmasında personele örnek olmalıdırlar.

1.3. Etik kurallar bilinmeli ve tüm faaliyetlerde bu kurallara uyulmalıdır.

1.4. Faaliyetlerde dürüstlük, saydamlık ve hesap verebilirlik sağlanmalıdır.

1.5. İdarenin personeline ve hizmet verilenlere adil ve eşit davranılmalıdır.

1.6. İdarenin faaliyetlerine ilişkin tüm bilgi ve belgeler doğru, tam ve güvenilir olmalıdır.

Standart: 2. Misyon, organizasyon yapısı ve görevler

İdarelerin misyonu ile birimlerin ve personelin görev tanımları yazılı olarak belirlenmeli, personele duyurulmalı ve idarede uygun bir organizasyon yapısı oluşturulmalıdır.

Bu standart için gerekli genel şartlar:

- 2.1. İdarenin misyonu yazılı olarak belirlenmeli, duyurulmalı ve personel tarafından benimsenmesi sağlanmalıdır.
- 2.2. Misyonun gerçekleştirilmesini sağlamak üzere idare birimleri ve alt birimlerince yürütülecek görevler yazılı olarak tanımlanmalı ve duyurulmalıdır.
- 2.3. İdare birimlerinde personelin görevlerini ve bu görevlere ilişkin yetki ve sorumluluklarını kapsayan görev dağılım çizelgesi oluşturulmalı ve personele bildirilmelidir.
- 2.4. İdarenin ve birimlerinin teşkilat şeması olmalı ve buna bağlı olarak fonksiyonel görev dağılımı belirlenmelidir.
- 2.5. İdarenin ve birimlerinin organizasyon yapısı, temel yetki ve sorumluluk dağılımı, hesap verebilirlik ve uygun raporlama ilişkisini gösterecek şekilde olmalıdır.
- 2.6. İdarenin yöneticileri, faaliyetlerin yürütülmesinde hassas görevlere ilişkin prosedürleri belirlemeli ve personele duyurmalıdır.
- 2.7. Her düzeydeki yöneticiler verilen görevlerin sonucunu izlemeye yönelik mekanizmalar oluşturmalıdır.

Standart: 3. Personelin yeterliliği ve performansı

İdareler, personelin yeterliliği ve görevleri arasındaki uyumu sağlamalı, performansın değerlendirilmesi ve geliştirilmesine yönelik önlemler almalıdır.

Bu standart için gerekli genel şartlar:

- 3.1. İnsan kaynakları yönetimi, idarenin amaç ve hedeflerinin gerçekleşmesini sağlamaya yönelik olmalıdır.
- 3.2. İdarenin yönetici ve personeli görevlerini etkin ve etkili bir şekilde yürütebilecek bilgi, deneyim ve yeteneğe sahip olmalıdır.
- 3.3. Mesleki yeterliliğe önem verilmeli ve her görev için en uygun personel seçilmelidir.
- 3.4. Personelin işe alınması ile görevinde ilerleme ve yükselmesinde liyakat ilkesine uyulmalı ve bireysel performansı göz önünde bulundurulmalıdır.
- 3.5. Her görev için gerekli eğitim ihtiyacı belirlenmeli, bu ihtiyacı giderecek eğitim faaliyetleri her yıl planlanarak yürütülmeli ve gerektiğinde güncellenmelidir.
- 3.6. Personelin yeterliliği ve performansı bağlı olduğu yöneticisi tarafından en az yılda bir kez değerlendirilmeli ve değerlendirme sonuçları personel ile görüşülmelidir.

3.7. Performans deęerlendirmesine gre performansı yetersiz bulunan personelin performansını geliřtirmeye ynelik nlemler alınmalı, yksek performans gsteren personel iin dllendirme mekanizmaları geliřtirilmelidir.

3.8. Personel istihdamı, yer deęiřtirme, st grevlere atanma, eęitim, performans deęerlendirmesi, zlk hakları gibi insan kaynakları ynetimine iliřkin nemli hususlar yazılı olarak belirlenmiř olmalı ve personele duyurulmalıdır.

Standart: 4. Yetki Devri

İdarelerde yetkiler ve yetki devrinin sınırları aıka belirlenmeli ve yazılı olarak bildirilmelidir. Devredilen yetkinin nemi ve riski dikkate alınarak yetki devri yapılmalıdır.

Bu standart iin gerekli genel řartlar:

4.1. İř akıř srelerindeki imza ve onay mercileri belirlenmeli ve personele duyurulmalıdır.

4.2. Yetki devirleri, st ynetici tarafından belirlenen esaslar erevesinde devredilen yetkinin sınırlarını gsterecek řekilde yazılı olarak belirlenmeli ve ilgililere bildirilmelidir.

4.3. Yetki devri, devredilen yetkinin nemi ile uyumlu olmalıdır.

4.4. Yetki devredilen personel grevin gerektirdięi bilgi, deneyim ve yeteneęe sahip olmalıdır.

4.5. Yetki devredilen personel, yetkinin kullanımına iliřkin olarak belli dnemlerde yetki devredene bilgi vermeli, yetki devreden ise bu bilgiyi aramalıdır.

2. RİSK DEęERLENDİRME STANDARTLARI

Risk deęerlendirme, idarenin hedeflerinin gerekleřmesini engelleyecek risklerin tanımlanması, analiz edilmesi ve gerekli nlemlerin belirlenmesi srecidir.

Standart: 5. Planlama ve Programlama

İdareler, faaliyetlerini, ama, hedef ve gstergelerini ve bunları gerekleřtirmek iin ihtiya duydukları kaynakları ieren plan ve programlarını oluřturmalı ve duyurmalı, faaliyetlerinin plan ve programlara uygunluęunu saęlamalıdır.

Bu standart iin gerekli genel řartlar:

5.1. İdareler, misyon ve vizyonlarını oluřturmak, stratejik amalar ve llebilir hedefler saptamak, performanslarını lmek, izlemek ve deęerlendirmek amacıyla katılımcı yntemlerle stratejik plan hazırlamalıdır.

5.2. İdareler, yürütecekleri program, faaliyet ve projeleri ile bunların kaynak ihtiyacını, performans hedef ve göstergelerini içeren performans programı hazırlamalıdır.

5.3. İdareler, bütçelerini stratejik planlarına ve performans programlarına uygun olarak hazırlamalıdır.

5.4. Yöneticiler, faaliyetlerin ilgili mevzuat, stratejik plan ve performans programıyla belirlenen amaç ve hedeflere uygunluğunu sağlamalıdır.

5.5. Yöneticiler, görev alanları çerçevesinde idarenin hedeflerine uygun özel hedefler belirlemeli ve personeline duyurmalıdır.

5.6. İdarenin ve birimlerinin hedefleri, spesifik, ölçülebilir, ulaşılabilir, ilgili ve süreli olmalıdır.

Standart: 6. Risklerin belirlenmesi ve değerlendirilmesi

İdareler, sistemli bir şekilde analizler yaparak amaç ve hedeflerinin gerçekleşmesini engelleyebilecek iç ve dış riskleri tanımlayarak değerlendirmeli ve alınacak önlemleri belirlemelidir.

Bu standart için gerekli genel şartlar:

6.1. İdareler, her yıl sistemli bir şekilde amaç ve hedeflerine yönelik riskleri belirlemelidir.

6.2. Risklerin gerçekleşme olasılığı ve muhtemel etkileri yılda en az bir kez analiz edilmelidir.

6.3. Risklere karşı alınacak önlemler belirlenerek eylem planları oluşturulmalıdır.

3. KONTROL FAALİYETLERİ STANDARTLARI

Kontrol faaliyetleri, idarenin hedeflerinin gerçekleştirilmesini sağlamak ve belirlenen riskleri yönetmek amacıyla oluşturulan politika ve prosedürlerdir.

Standart: 7. Kontrol stratejileri ve yöntemleri

İdareler, hedeflerine ulaşmayı amaçlayan ve riskleri karşılamaya uygun kontrol strateji ve yöntemlerini belirlemeli ve uygulamalıdır.

Bu standart için gerekli genel şartlar:

7.1. Her bir faaliyet ve riskleri için uygun kontrol strateji ve yöntemleri (düzenli gözden geçirme, örnekleme yoluyla kontrol, karşılaştırma, onaylama, raporlama, koordinasyon, doğrulama, analiz etme, yetkilendirme, gözetim, inceleme, izleme v.b.) belirlenmeli ve uygulanmalıdır.

7.2. Kontroller, gerekli hallerde, işlem öncesi kontrol, süreç kontrolü ve işlem sonrası kontrolleri de kapsamalıdır.

7.3. Kontrol faaliyetleri, varlıkların dönemsel kontrolünü ve güvenliğini sağlanmasını kapsamalıdır.

7.4. Belirlenen kontrol yönteminin maliyeti beklenen faydayı aşmamalıdır.

Standart: 8. Prosedürlerin belirlenmesi ve belgelendirilmesi

İdareler, faaliyetleri ile mali karar ve işlemleri için gerekli yazılı prosedürleri ve bu alanlara ilişkin düzenlemeleri hazırlamalı, güncellemeli ve ilgili personelin erişimine sunmalıdır.

Bu standart için gerekli genel şartlar:

8.1. İdareler, faaliyetleri ile mali karar ve işlemleri hakkında yazılı prosedürler belirlemelidir.

8.2. Prosedürler ve ilgili dokümanlar, faaliyet veya mali karar ve işlemin başlaması, uygulanması ve sonuçlandırılması aşamalarını kapsamalıdır.

8.3. Prosedürler ve ilgili dokümanlar, güncel, kapsamlı, mevzuata uygun ve ilgili personel tarafından anlaşılabilir ve ulaşılabilir olmalıdır.

Standart: 9. Görevler ayrılığı

Hata, eksiklik, yanlışlık, usulsüzlük ve yolsuzluk risklerini azaltmak için faaliyetler ile mali karar ve işlemlerin onaylanması, uygulanması, kaydedilmesi ve kontrol edilmesi görevleri personel arasında paylaştırılmalıdır.

Bu standart için gerekli genel şartlar:

9.1. Her faaliyet veya mali karar ve işlemin onaylanması, uygulanması, kaydedilmesi ve kontrolü görevleri farklı kişilere verilmelidir.

9.2. Personel sayısının yetersizliği nedeniyle görevler ayrılığı ilkesinin tam olarak uygulanamadığı idarelerin yöneticileri risklerin farkında olmalı ve gerekli önlemleri almalıdır.

Standart: 10. Hiyerarşik kontroller

Yöneticiler, iş ve işlemlerin prosedürlere uygunluğunu sistemli bir şekilde kontrol etmelidir.

Bu standart için gerekli genel şartlar:

10.1. Yöneticiler, prosedürlerin etkili ve sürekli bir şekilde uygulanması için gerekli kontrolleri yapmalıdır.

10.2. Yöneticiler, personelin iş ve işlemlerini izlemeli ve onaylamalı, hata ve usulsüzlüklerin giderilmesi için gerekli talimatları vermelidir.

Standart: 11. Faaliyetlerin sürekliliği

İdareler, faaliyetlerin sürekliliğini sağlamaya yönelik gerekli önlemleri almalıdır.

Bu standart için gerekli genel şartlar:

11.1. Personel yetersizliği, geçici veya sürekli olarak görevden ayrılma, yeni bilgi sistemlerine geçiş, yöntem veya mevzuat değişiklikleri ile olağanüstü durumlar gibi faaliyetlerin sürekliliğini etkileyen nedenlere karşı gerekli önlemler alınmalıdır.

11.2. Gerekli hallerde usulüne uygun olarak vekil personel görevlendirilmelidir.

11.3. Görevinden ayrılan personelin, iş veya işlemlerinin durumunu ve gerekli belgeleri de içeren bir rapor hazırlaması ve bu raporu görevlendirilen personele vermesi yönetici tarafından sağlanmalıdır.

Standart: 12. Bilgi sistemleri kontrolleri

İdareler, bilgi sistemlerinin sürekliliğini ve güvenilirliğini sağlamak için gerekli kontrol mekanizmaları geliştirmelidir.

Bu standart için gerekli genel şartlar:

12.1. Bilgi sistemlerinin sürekliliğini ve güvenilirliğini sağlayacak kontroller yazılı olarak belirlenmeli ve uygulanmalıdır.

12.2. Bilgi sistemine veri ve bilgi girişi ile bunlara erişim konusunda yetkilendirmeler yapılmalı, hata ve usulsüzlüklerin önlenmesi, tespit edilmesi ve düzeltilmesini sağlayacak mekanizmalar oluşturulmalıdır.

12.3. İdareler bilişim yönetişimini sağlayacak mekanizmalar geliştirmelidir.

4. BİLGİ VE İLETİŞİM STANDARTLARI

Bilgi ve iletişim, gerekli bilginin ihtiyaç duyan kişi, personel ve yöneticiye belirli bir formatta ve ilgililerin iç kontrol ve diğer sorumluluklarını yerine getirmelerine imkan verecek bir zaman dilimi içinde iletilmesini sağlayacak bilgi, iletişim ve kayıt sistemini kapsar.

Standart: 13. Bilgi ve iletişim

İdareler, birimlerinin ve çalışanlarının performansının izlenebilmesi, karar alma süreçlerinin sağlıklı bir şekilde işleyebilmesi ve hizmet sunumunda etkinlik ve memnuniyetin sağlanması amacıyla uygun bir bilgi ve iletişim sistemine sahip olmalıdır.

Bu standart için gerekli genel şartlar:

13.1. İdarelerde, yatay ve dikey iç iletişim ile dış iletişimi kapsayan etkili ve sürekli bir bilgi ve iletişim sistemi olmalıdır.

13.2. Yöneticiler ve personel, görevlerini yerine getirebilmeleri için gerekli ve yeterli bilgiye zamanında ulaşabilmelidir.

13.3. Bilgiler doğru, güvenilir, tam, kullanışlı ve anlaşılabilir olmalıdır.

13.4. Yöneticiler ve ilgili personel, performans programı ve bütçenin uygulanması ile kaynak kullanımına ilişkin diğer bilgilere zamanında erişebilmelidir.

13.5. Yönetim bilgi sistemi, yönetimin ihtiyaç duyduğu gerekli bilgileri ve raporları üretebilecek ve analiz yapma imkanı sunacak şekilde tasarlanmalıdır.

13.6. Yöneticiler, idarenin misyon, vizyon ve amaçları çerçevesinde beklentilerini görev ve sorumlulukları kapsamında personele bildirmelidir.

13.7. İdarenin yatay ve dikey iletişim sistemi personelin değerlendirme, öneri ve sorunlarını iletebilmelerini sağlamalıdır.

Standart: 14. Raporlama

İdarenin amaç, hedef, gösterge ve faaliyetleri ile sonuçları, saydamlık ve hesap verebilirlik ilkeleri doğrultusunda raporlanmalıdır.

Bu standart için gerekli genel şartlar:

14.1. İdareler, her yıl, amaçları, hedefleri, stratejileri, varlıkları, yükümlülükleri ve performans programlarını kamuoyuna açıklamalıdır.

14.2. İdareler, bütçelerinin ilk altı aylık uygulama sonuçları, ikinci altı aya ilişkin beklentiler ve hedefler ile faaliyetlerini kamuoyuna açıklamalıdır.

14.3. Faaliyet sonuçları ve değerlendirmeler idare faaliyet raporunda gösterilmeli ve duyurulmalıdır.

14.4. Faaliyetlerin gözetimi amacıyla idare içinde yatay ve dikey raporlama ağı yazılı olarak belirlenmeli, birim ve personel, görevleri ve faaliyetleriyle ilgili hazırlanması gereken raporlar hakkında bilgilendirilmelidir.

Standart: 15. Kayıt ve dosyalama sistemi

İdareler, gelen ve giden her türlü evrak dahil iş ve işlemlerin kaydedildiği, sınıflandırıldığı ve dosyalandığı kapsamlı ve güncel bir sisteme sahip olmalıdır.

Bu standart için gerekli genel şartlar:

15.1. Kayıt ve dosyalama sistemi, elektronik ortamdakiler dahil, gelen ve giden evrak ile idare içi haberleşmeyi kapsamalıdır.

15.2. Kayıt ve dosyalama sistemi kapsamlı ve güncel olmalı, yönetici ve personel tarafından ulaşılabilir ve izlenebilir olmalıdır.

15.3. Kayıt ve dosyalama sistemi, kişisel verilerin güvenliğini ve korunmasını sağlamalıdır.

15.4. Kayıt ve dosyalama sistemi belirlenmiş standartlara uygun olmalıdır.

15.5. Gelen ve giden evrak zamanında kaydedilmeli, standartlara uygun bir şekilde sınıflandırılmalı ve arşiv sistemine uygun olarak muhafaza edilmelidir.

15.6. İdarenin iş ve işlemlerinin kaydı, sınıflandırılması, korunması ve erişimini de kapsayan, belirlenmiş standartlara uygun arşiv ve dokümantasyon sistemi oluşturulmalıdır.

Standart: 16. Hata, usulsüzlük ve yolsuzlukların bildirilmesi

İdareler, hata, usulsüzlük ve yolsuzlukların belirlenen bir düzen içinde bildirilmesini sağlayacak yöntemler oluşturmalıdır.

Bu standart için gerekli genel şartlar:

16.1. Hata, usulsüzlük ve yolsuzlukların bildirim yöntemleri belirlenmeli ve duyurulmalıdır.

16.2. Yöneticiler, bildirilen hata, usulsüzlük ve yolsuzluklar hakkında yeterli incelemeyi yapmalıdır.

16.3. Hata, usulsüzlük ve yolsuzlukları bildiren personele haksız ve ayırıcı bir muamele yapılmamalıdır.

5. İZLEME STANDARTLARI

İzleme, iç kontrol sisteminin kalitesini değerlendirmek üzere yürütülen tüm izleme faaliyetlerini kapsar.

Standart: 17. İç kontrolün değerlendirilmesi

İdareler iç kontrol sistemini yılda en az bir kez değerlendirmelidir.

Bu standart için gerekli genel şartlar:

17.1. İç kontrol sistemi, sürekli izleme veya özel bir değerlendirme yapma veya bu iki yöntem birlikte kullanılarak değerlendirilmelidir.

17.2. İç kontrolün eksik yönleri ile uygun olmayan kontrol yöntemlerinin belirlenmesi, bildirilmesi ve gerekli önlemlerin alınması konusunda süreç ve yöntem belirlenmelidir.

17.3. İç kontrolün değerlendirilmesine idarenin birimlerinin katılımı sağlanmalıdır.

17.4. İç kontrolün değerlendirilmesinde, yöneticilerin görüşleri, kişi ve/veya idarelerin talep ve şikâyetleri ile iç ve dış denetim sonucunda düzenlenen raporlar dikkate alınmalıdır.

17.5. İç kontrolün değerlendirilmesi sonucunda alınması gereken önlemler belirlenmeli ve bir eylem planı çerçevesinde uygulanmalıdır.

Standart: 18. İç denetim

İdareler fonksiyonel olarak bağımsız bir iç denetim faaliyetini sağlamalıdır.

Bu standart için gerekli genel şartlar:

18.1. İç denetim faaliyeti İç Denetim Koordinasyon Kurulu tarafından belirlenen standartlara uygun bir şekilde yürütülmelidir.

18.2. İç denetim sonucunda idare tarafından alınması gerekli görülen önlemleri içeren eylem planı hazırlanmalı, uygulanmalı ve izlenmelidir.

Bilgi Sistemleri Yönetimi Tebliği

Resmî Gazete Tarihi : 05.01.2018

Resmî Gazete Sayısı : 30292

BİLGİ SİSTEMLERİ YÖNETİMİ TEBLİĞİ

(VII-128.9)

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Tebliğin amacı, 2 nci maddede sayılan Kurum, Kuruluş ve Ortaklıkların bilgi sistemlerinin yönetimine ilişkin usul ve esasları belirlemektir.

Kapsam

MADDE 2 - (1) Aşağıdaki Kurum, Kuruluş ve Ortaklıklar, bu Tebliğ hükümlerine uymakla yükümlüdürler:

- a) Borsa İstanbul A.Ş.,
- b) Borsalar ve piyasa işleticileri ile teşkilatlanmış diğer pazar yerleri,
- c) Emeklilik yatırım fonları,
- ç) İstanbul Takas ve Saklama Bankası A.Ş.,
- d) Merkezi Kayıt Kuruluşu A.Ş.,
- e) Portföy saklayıcısı kuruluşlar,
- f) Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş.,
- g) Sermaye piyasası kurumları,
- ğ) Halka açık ortaklıklar,
- h) Türkiye Sermaye Piyasaları Birliği,
- ı) Türkiye Değerleme Uzmanları Birliği.

(2) Birinci fıkrada sayılan Kurum, Kuruluş ve Ortaklıklardan, 6/12/2012 tarihli ve 6362 sayılı Sermaye Piyasası Kanununun 136 ncı maddesi uyarınca banka ve sigorta şirketleri ile 21/11/2012 tarihli ve 6361 sayılı Finansal Kiralama, Faktoring ve Finansman Şirketleri Kanunu uyarınca finansal kiralama, faktoring ve finansman şirketlerinin bilgi sistemlerinin, kendi özel mevzuatlarında belirlenen ilkeler çerçevesinde yönetilmesi, bu Tebliğde öngörülen yükümlülüklerin yerine getirilmesi hükmündedir.

Dayanak

MADDE 3 - (1) Bu Tebliğ, 6362 sayılı Kanunun 128 inci maddesinin birinci fıkrasının (h) bendine dayanılarak hazırlanmıştır.

(...)

Müşteri bilgilerinin gizliliği

MADDE 19 - (1) Kurum, Kuruluş ve Ortaklıklar bilgi sistemleri aracılığıyla edindiği veya sakladığı müşteri bilgilerinin gizliliğini sağlamaya yönelik kontrolleri tesis eder ve bunların gerektirdiği önlemleri alır.

(2) Kurum, Kuruluş ve Ortaklıklar personelin kişisel verilerin korunması ve işlenmesine uygun davranışlarını temin etmelerine yönelik gerekli tedbirleri alırlar. Bu maddede yer almayan durumlarda 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu uygulanır.

(...)

Yapı Kooperatiflerine Ait Bilgilerin Elektronik Ortamda Kaydına Dair Tebliğ

Resmî Gazete Tarihi : 17.11.2016

Resmî Gazete Sayısı : 29891

YAPI KOOPERATİFLERİNE AİT BİLGİLERİN ELEKTRONİK ORTAMDA KAYDINA DAİR TEBLİĞ

Amaç ve kapsam

MADDE 1 - (1) Bu Tebliğin amacı; yapı kooperatiflerine ait bilgilerin elektronik ortama aktarılması ile ortaklarının elektronik ortamda kaydedilmesi ve izlenmesine ilişkin usul ve esasları düzenlemektir.

(2) Bu Tebliğ her türlü hak, yetki ve görevleri Çevre ve Şehircilik Bakanlığınca yürütülmekte olan konut, toplu işyeri ve küçük sanayi sitesi yapı kooperatifleri ile bunların üst kuruluşları ile ilgili hükümleri kapsar.

Dayanak

MADDE 2 - (1) Bu Tebliğ; 29/6/2011 tarihli ve 644 sayılı Çevre ve Şehircilik Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 12 nci maddesinin birinci fıkrasının (1) bendine dayanılarak hazırlanmıştır.

Elektronik kayıt

MADDE 3 - (1) Çevre ve Şehircilik Bakanlığınca, yürürlükteki mevzuata göre yayınlanması uygun görülen yapı kooperatiflerine ait bilgilerin elektronik ortamda kayıt altına alındığı Yapı Kooperatifleri Bilgi Sistemi (e-kooperatif) kurulur.

(2) Yapı Kooperatifleri Bilgi Sistemi e-Devlet Kapısından ilgililerin erişimine sunulur.

Sorumluluk

MADDE 4 - (1) Kooperatiflerin yönetim kurulu; ortaklarının kimlik bilgilerini (adı, soyadı ve T.C. kimlik numarası) ve kooperatifin üzerine kayıtlı taşınmaz bulunması halinde taşınmaza ilişkin tapu bilgilerini, kooperatiflerin defter ve belgelerine uygun olarak güncel şekilde sisteme aktarmakla yükümlüdür. Veri girilmesi ile girilen bilgilerin doğruluğu ve güncelliğine dair her türlü sorumluluk kooperatif yönetim kuruluna aittir.

Kişisel verilerin korunması

MADDE 5 - (1) Bu Tebliğ kapsamında elektronik ortamda kaydedilen verilerin korunması 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu hükümlerine göre sağlanır.

Yürürlük

MADDE 6 - (1) Bu Tebliğ yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 7 - (1) Bu Tebliğ hükümlerini Çevre ve Şehircilik Bakanı yürütür.

CUMHURBAŐKANLIĐI KARARNAMELERİ

Bölüm İeriĐi

- 1 sayılı CumhurbaşkanlıĐı TeŐkilatı Hakkında CumhurbaşkanlıĐı Kararnamesi
- 49 sayılı CoĐrafi Bilgi Sistemleri Hakkında CumhurbaşkanlıĐı Kararnamesi

1 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi

Resmî Gazete Tarihi : 10.07.2018

Resmî Gazete Sayısı : 30474

CUMHURBAŞKANLIĞI TEŞKİLATI HAKKINDA CUMHURBAŞKANLIĞI KARARNAMESİ

BİRİNCİ KISIM

CUMHURBAŞKANLIĞI MAKAMI

Cumhurbaşkanı

MADDE 1- (1) Cumhurbaşkanı Devletin başıdır. Yürütme yetkisi Cumhurbaşkanına aittir.

(2) Cumhurbaşkanı, Devlet başkanı sıfatıyla Türkiye Cumhuriyetini ve Türk Milletinin birliğini temsil eder; Anayasanın uygulanmasını, Devlet organlarının düzenli ve uyumlu çalışmasını temin eder.

(3) Cumhurbaşkanı, yetkilerinden bir kısmını gerektiğinde sınırlarını yazılı olarak belirterek astlarına devredebilir. Ancak devrettiği yetkiyi, gerek gördüğünde kendisi de doğrudan kullanabilir.

(...)

Bilgi toplama ve sır saklama yükümlülüğü

MADDE 36 - (1) Kurullar, görevleri ile ilgili olarak gerekli olan bilgileri bütün kamu kurum ve kuruluşlarından istemeye yetkilidir. Kendilerinden bilgi istenen bütün kamu kurum ve kuruluşları bu bilgileri vermekle yükümlüdürler.

(2) Bu şekilde elde edilen bilgilerden ticari sır niteliğinde olanların gizliliğine uyulur.

(3) Kurulların başkan ve üyeleri ile personeli, görevlerini yerine getirmeleri sırasında edindikleri, kamuya, ilgililere ve üçüncü kişilere ait gizlilik taşıyan bilgileri, kişisel verileri, gizlilik taşıyan bilgileri, ticari sırları ve bunlara ait belgeleri, bu konuda mevzuat gereği yetkili kılınan mercilerden başkasına açıklayamaz, kendilerinin veya üçüncü kişilerin yararına kullanamaz. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

(...)

Risk Analizi Genel Müdürlüğü

MADDE 222- (Başlığı ile Birlikte Yeniden Düzenleme:RG-18/4/2020-31103-CK-60/4 md.)

(1) Risk Analizi Genel Müdürlüğünün görev ve yetkileri şunlardır:

- a) Vergi kayıp ve kaçığı ile kayıt dışı ekonomik faaliyetleri araştırmak, bunların önlenmesine yönelik risk analiz ve değerlendirme çalışmalarını gerçekleştirmek,
- b) Vergi kayıp ve kaçığı ile kayıt dışı ekonomik faaliyetlerin önlenmesi amacıyla ilgili kamu kurum ve kuruluşlarıyla koordinasyonu sağlamak,
- c) Risk analizi ve değerlendirme çalışmalarını, belirlenen plan ve programlar dâhilinde tanımlanan risk senaryoları, veri modellemeleri ve elektronik ortamdaki dâhil olmak üzere ilgili mevzuatına göre temin edilen her türlü bilgi, belge ve bunlara ilişkin her türlü ortamdaki kayıtlar üzerinden çeşitli analiz araçlarını kullanmak suretiyle gerçekleştirmek,
- ç) Risk analizi ve değerlendirme çalışmalarına ait sonuçları raporlara bağlayarak gerekli önlemlerin alınmasını teminen bu raporları ilgili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarına iletmek ve bu kurumlarca alınan önlemlerin sonuçlarını takip etmek, analiz etmek ve gerek görüldüğünde ilgili kurumlar ile paylaşmak,
- d) Risk analizi ve değerlendirme çalışmaları için kanunları veya faaliyet konuları gereğince ekonomik olaylara ilişkin kayıt tutan ilgili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının bilgi işlem sistemlerine Bakanlık ve ilgili Bakanlığın veya kamu kurumu niteliğindeki meslek kuruluşlarının yetkili organlarının Kişisel Verilerin Korunması Kanunu ve ilgili diğer mevzuat hükümlerine uygun olarak birlikte belirleyeceği usul ve esaslar dâhilinde erişim sistemi kurmak, bu kurumlarla birlikte gerekli çalışmaları yürütmek,
- e) Bakan tarafından verilen diğer görevleri yapmak.

(...)

Mükellef Hakları Kurulu

MADDE 238/A- (Ek:RG-18/4/2020-31103-CK-60/8 md.)

(1) Mükellef haklarının korunmasına yönelik temel ilke ve kuralları belirlemek, bu ilke ve kuralların benimsenmesi ve uygulanmasını sağlamak, mükellef haklarına yönelik başvuruları değerlendirmek ve Bakanlığa önerilerde bulunmak üzere Mükellef Hakları Kurulu kurulur.

(2) Mükellef Hakları Kurulunun oluşumu, üyelerin seçimi, görevlendirilmesi ve görev süreleri ile çalışma usul ve esasları yönetmelikle düzenlenir.

(3) Kurul, görevleri ile ilgili olarak gerekli olan bilgileri bütün kamu kurum ve kuruluşlarından istemeye yetkilidir. Kendilerinden bilgi istenen bütün kamu kurum ve kuruluşları bu bilgileri

vermekle yükümlüdürler. Bu şekilde elde edilen bilgilerden vergi mahremiyeti kapsamında olanların gizliliğine uyulur. Kurulun Başkan ve üyeleri ile Kurulda görevlendirilen personel, görevlerini yerine getirmeleri sırasında edindikleri, kamuya, ilgililere ve üçüncü kişilere ait gizlilik taşıyan bilgileri, kişisel verileri, ticari sırları ve bunlara ait belgeleri, bu konuda mevzuat gereği yetkili kılınan mercilerden başkasına açıklayamaz, kendilerinin veya üçüncü kişilerin yararına kullanamaz. Bu yükümlülük görevden ayrılımlarından sonra da devam eder.

(4) Mükellef Hakları Kurulu Başkan ve üyelerine bu görevleri sebebiyle, ayda dört toplantıyı geçmemek üzere her toplantı günü için 375 sayılı Kanun Hükmünde Kararnamenin ek 29 uncu maddesi uyarınca (3.000) gösterge rakamının memur aylık katsayısı ile çarpımı sonucu bulunacak tutarda Bakanlık bütçesinden huzur hakkı ödenir.

(...)

Mükellef Hakları Kurulu

MADDE 238/A- (Ek:RG-18/4/2020-31103-CK-60/8 md.)

(1) Mükellef haklarının korunmasına yönelik temel ilke ve kuralları belirlemek, bu ilke ve kuralların benimsenmesi ve uygulanmasını sağlamak, mükellef haklarına yönelik başvuruları değerlendirmek ve Bakanlığa önerilerde bulunmak üzere Mükellef Hakları Kurulu kurulur.

(2) Mükellef Hakları Kurulunun oluşumu, üyelerin seçimi, görevlendirilmesi ve görev süreleri ile çalışma usul ve esasları yönetmelikle düzenlenir.

(3) Kurul, görevleri ile ilgili olarak gerekli olan bilgileri bütün kamu kurum ve kuruluşlarından istemeye yetkilidir. Kendilerinden bilgi istenen bütün kamu kurum ve kuruluşları bu bilgileri vermekle yükümlüdürler. Bu şekilde elde edilen bilgilerden vergi mahremiyeti kapsamında olanların gizliliğine uyulur. Kurulun Başkan ve üyeleri ile Kurulda görevlendirilen personel, görevlerini yerine getirmeleri sırasında edindikleri, kamuya, ilgililere ve üçüncü kişilere ait gizlilik taşıyan bilgileri, kişisel verileri, ticari sırları ve bunlara ait belgeleri, bu konuda mevzuat gereği yetkili kılınan mercilerden başkasına açıklayamaz, kendilerinin veya üçüncü kişilerin yararına kullanamaz. Bu yükümlülük görevden ayrılımlarından sonra da devam eder.

(4) Mükellef Hakları Kurulu Başkan ve üyelerine bu görevleri sebebiyle, ayda dört toplantıyı geçmemek üzere her toplantı günü için 375 sayılı Kanun Hükmünde Kararnamenin ek 29 uncu maddesi uyarınca (3.000) gösterge rakamının memur aylık katsayısı ile çarpımı sonucu bulunacak tutarda Bakanlık bütçesinden huzur hakkı ödenir.

(...)

Bilgi toplama, işleme ve paylaşma yetkisi

MADDE 378 - (1) Sağlık hizmeti almak üzere, kamu veya özel sağlık kuruluşları ile sağlık mesleği mensuplarına müracaat edenlerin, sağlık hizmetinin gereği olarak vermek zorunda oldukları veya kendilerine verilen hizmete ilişkin kişisel verileri işlenebilir.

2) Sağlık hizmetinin verilmesi, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve maliyetlerin hesaplanması amacıyla Bakanlık, birinci fıkra kapsamında elde edilen verileri alarak işleyebilir. Bu veriler, Kişisel Verilerin Korunması Kanununda öngörülen şartlar dışında aktarılamaz.

(3) Bakanlık, ikinci fıkra gereğince toplanan ve işlenen kişisel verilere, ilgili kişilerin kendilerinin veya yetki verdikleri üçüncü kişilerin erişimlerini sağlayacak bir sistem kurar.

(4) Üçüncü fıkraya göre kurulan sistemlerin güvenliği ve güvenilirliği ile ilgili standartlar Kişisel Verileri Koruma Kurulunun belirlediği ilkelere uygun olarak Bakanlıkça belirlenir. Bakanlık, ilgili mevzuat uyarınca elde edilen kişisel sağlık verilerinin güvenliğinin sağlanması için gerekli tedbirleri alır. Bu amaçla, sistemde kayıtlı bilgilerin hangi görevli tarafından ne amaçla kullanıldığının denetlenmesine imkân tanıyan bir güvenlik sistemi kurar.

(5) Sağlık personeli istihdam eden kamu kurum ve kuruluşları ile özel hukuk tüzel kişileri ve gerçek kişiler, istihdam ettiği personeli ve personel hareketlerini Bakanlığa bildirmekle yükümlüdür.

(6) Kişisel sağlık verilerinin işlenmesi, güvenliği ve bu maddenin uygulanması ile ilgili diğer hususlar Bakanlıkça yürürlüğe konulan yönetmelikle düzenlenir.

(...)

49 sayılı Coğrafi Bilgi Sistemleri Hakkında Cumhurbaşkanlığı Kararnamesi

Resmî Gazete Tarihi : 07.11.2019

Resmî Gazete Sayısı : 30941

COĞRAFI BİLGİ SİSTEMLERİ HAKKINDA CUMHURBAŞKANLIĞI KARARNAMESİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Tanımlar ve İlkeler

Amaç

MADDE 1- (1) Bu Cumhurbaşkanlığı Kararnamesinin amacı coğrafi bilgi sistemleri ile Ulusal Coğrafi Bilgi Sistemi ve altyapısına ilişkin; kamu kurum ve kuruluşları arasında koordinasyonun sağlanması, hedef ve stratejilerin oluşturulması, coğrafi veri temaları içinde yer alan coğrafi veri ve bilginin üretilmesi ve güncelliğinin sağlanması, yönetilmesi, kullanılması, erişimi, güvenliğinin sağlanması, paylaşılması ve dağıtımına yönelik usul, esas ve standartlar ile bu Cumhurbaşkanlığı Kararnamesi kapsamında oluşturulan kurulların, kamu kurum ve kuruluşlarının, gerçek ve tüzel kişilerin görev, yetki ve sorumluluklarının belirlenmesidir.

Kapsam

MADDE 2- (1) Bu Cumhurbaşkanlığı Kararnamesi, 1 inci maddede belirtilen amaçlarla sınırlı olmak üzere, kamu kurum ve kuruluşları ile gerçek ve tüzel kişileri ve bunların faaliyetlerini kapsar.

(2) Ulusal Coğrafi Veri Sorumluluk Matrisinde yer almayan coğrafi veriler bu Cumhurbaşkanlığı Kararnamesinin kapsamı dışındadır.

(...)

İlkeler

MADDE 4- (1) Coğrafi bilgi sistemleri hizmet ve uygulamalarına ilişkin tüm faaliyetlerde;

- Kamu kaynaklarının etkin ve verimli kullanılması için coğrafi verinin toplanmasında, üretilmesinde, depolanmasında ve paylaşımında mükerrerliğin önlenmesi,
- Coğrafi verinin toplanmasında, üretilmesinde, depolanmasında, paylaşımında, kullanımında ve sunumunda ulusal standartlara uyulması,

- c) Coğrafi verinin ve veri bilgisinin doğru ve kaliteli üretmesinin, güncelliğinin, güvenliğinin, sürekliliğinin ve paylaşılmasının sağlanması,
- ç) Ulusal güvenliğe, kişisel verilerin korunmasına, fikri, sınai ve ticari haklara ilişkin mevzuat hükümleri ile milletlerarası andlaşma hükümleri saklı kalmak kaydıyla her türlü coğrafi verinin erişilebilir, paylaşılabilir ve kullanılabilir olması,
- d) Birlikte çalışabilirliğin ve katılımcılığın sağlanması,
- e) Ülke düzeyinde nitelikli insan kaynağı ve kapasitesinin geliştirilmesi,
- f) Araştırma, geliştirme ve yenilik faaliyetlerinin teşvik edilmesi,
- g) Standartların belirlenmesinde kamu kurum ve kuruluşlarının ihtiyaçlarının dikkate alınması, ilkeleri gözetilir.
- (...)

MUHTELİF DÜZENLEMELER

Bölüm İçeriği

- BTK - 27.12.2016 tarihli Posta Gönderilerine İlişkin Güvenlik Tedbirlerine Yönelik Usul ve Esaslar

BTK - 27.12.2016 tarihli Posta Gnderilerine İliŐkin Gvenlik Tedbirlerine Ynelik Usul ve Esaslar

BİLGİ TEKNOLOJİLERİ VE İLETİŐİM KURULU KARARI

Karar Tarihi: 27.12.2016

Karar No: 2016/DK-YED/517

Gndem Konusu: Posta Gnderilerine İliŐkin Gvenlik Tedbirlerine Ynelik Usul ve Esaslar

KARAR: Yetkilendirme Dairesi BaŐkanlıđının hazırladıđı tahrir ve ekleri incelenmiŐtir.

23.05.2013 tarihli ve 6475 sayılı Posta Hizmetleri Kanununun 4, 7, 12 ve 19'uncu maddeleri, 03.06.2014 tarihli ve 29019 sayılı Resmi Gazete'de yayımlanarak yrrlđe giren Posta Sektrne İliŐkin Yetkilendirme Ynetmeliđin 16'ncı maddesi, 03.06.2014 tarihli ve 29019 sayılı Resmi Gazete'de yayımlanarak yrrlđe giren Posta Hizmetlerinin Sunulmasına İliŐkin Ynetmeliđin 15, 17, 18 ve 21'inci maddeleri ile ilgili diđer mevzuata istinaden;

Ek'te yer alan "Posta Gnderilerine İliŐkin Gvenlik Tedbirlerine Ynelik Usul ve Esaslar"ın onaylanması hususuna karar verilmiŐtir.

POSTA GÖNDERİLERİNE İLİŞKİN GÜVENLİK TEDBİRLERİNE YÖNELİK USUL VE ESASLAR

Amaç ve kapsam

MADDE 1 - (1) Bu Usul ve Esaslar, 6475 sayılı Posta Hizmetleri Kanunu çerçevesinde faaliyet gösteren posta hizmet sağlayıcılarının kabul ettiği ve/veya alıcısına teslim ettiği posta gönderilerine ilişkin güvenlik tedbirlerinin belirlenmesine yönelik usul ve esasları kapsar.

Hukuki dayanak

MADDE 2 - (1) Bu Usul ve Esaslar, 23/05/2013 tarihli ve 6475 sayılı Posta Hizmetleri Kanununun 4, 7, 12 ve 19 uncu maddeleri, 03/06/2014 tarihli ve 29019 sayılı Resmi Gazete’de yayımlanarak yürürlüğe giren Posta Sektörüne İlişkin Yetkilendirme Yönetmeliğinin 16 ncı maddesi, 03/06/2014 tarihli ve 29019 sayılı Resmi Gazete’de yayımlanarak yürürlüğe giren Posta Hizmetlerinin Sunulmasına İlişkin Yönetmeliğin 15, 17, 18 ve 21 inci maddelerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 3 - (1) Bu Usul ve Esaslarda geçen kavramlar için ilgili mevzuatta yer alan tanımlar geçerlidir.

Posta gönderilerinin kabulü ve teslimi aşamasında yapılacak işlemler

MADDE 4 – (1) Hizmet sağlayıcılar tarafından, haberleşme gönderileri hariç, posta gönderilerinin kabulü aşamasında; asgari olarak;

(a) Gönderici ve/veya alıcının gerçek kişi olması halinde;

1. Göndericinin adı-soyadı, TC Kimlik numarası (yabancı uyruklular için pasaport numarası, uluslararası geçerliliği olan muadili belgenin numarası veya TC yetkili mercilerince verilmiş kimliği tespiti yarayan belge numarası), açık adres bilgisi, telefon numarası bilgileri,
2. Gönderinin, üzerinde gönderici olarak belirtilen kişiden farklı bir kişi tarafından hizmet sağlayıcısına teslim edilmesi durumunda; bu fıkranın (a) bendinin (1) numaralı alt bendinde belirtilen bilgilere ilaveten, gönderiyi teslim eden kişinin adı-soyadı, TC Kimlik numarası (yabancı uyruklular için pasaport numarası, uluslararası geçerliliği olan muadili belgenin numarası veya TC yetkili mercilerince verilmiş kimliği tespiti yarayan belge numarası), açık adres bilgisi, telefon numarası bilgileri,
3. Alıcının adı-soyadı ve açık adres bilgisi,

4. Gönderiye ilişkin olarak gönderinin cinsi, gönderinin birden fazla bağımsız materyal içermesi halinde her biri için cins bilgileri,

5. Kabul sırasında göndericinin kimlik ve gönderinin içeriğinin kontrolü işlemlerini gerçekleştiren hizmet sağlayıcısı şirket personelinin adı, soyadı, TC kimlik numarası bilgileri,

kayıt altına alınır, gerektiğinde ilgili mercilere sunulmak üzere gizliliği sağlanarak en az iki yıl süreyle saklanır.

(b) Gönderici ve/veya alıcının tüzel kişi olması halinde;

1. Gönderici tüzel kişiliğin tam unvanı, vergi kimlik numarası veya MERSİS numarası, açık adres bilgisi, telefon numarası bilgileri, tüzel kişinin gönderisini göndermeye yetkili gerçek kişinin bu fıkranın (a) bendinin (1) numaralı alt bendinde belirtilen bilgileri,

2. Alıcıya ilişkin olarak alıcının adı-soyadı ve/veya alıcının tüzel kişi olması halinde unvanı ile açık adres bilgisi,

3. Gönderiye ilişkin olarak gönderinin cinsi, gönderinin birden fazla bağımsız materyal içermesi halinde her biri için cins bilgileri,

4. Kabul sırasında kimlik ve gönderinin içeriğinin kontrolü işlemlerini gerçekleştiren hizmet sağlayıcısının personelinin adı, soyadı, TC kimlik numarası bilgileri kayıt altına alınır ve gerektiğinde ilgili mercilere sunulmak üzere gizliliği sağlanarak en az iki yıl süreyle saklanır. Ancak, hizmet sağlayıcı ile bir sözleşme kapsamında fatura ya da irsaliye ile taşıttırılan gönderiler için işbu bendin (3) numaralı alt bendinde yer alan bilgiler kayıt altına alınmayabilir.

(2) Hizmet sağlayıcılar tarafından, posta gönderilerinin alıcıya teslimi aşamasında; asgari olarak; teslim alanın, adı-soyadı, TC kimlik numarası (yabancı uyruklular için pasaport numarası, uluslararası geçerliliği olan muadili belgenin numarası veya TC yetkili mercilerince verilmiş kimliği tespiti yarayan belge numarası) kayıt altına alınır ve gerektiğinde ilgili mercilere sunmak üzere gizliliği sağlanarak en az iki yıl süreyle saklanır. Alıcının kimlik bilgilerini vermek istememesi durumunda gönderi teslim edilmez, göndericisine iade edilir.

(3) Hizmet sağlayıcıya gönderileri teslim edenin kimlik bilgilerinin doğruluğu, Türk uyruklular için TC kimlik kartı veya TC nüfus cüzdanı, TC sürücü belgesi veya pasaport ibraz ettirilerek, yabancı uyruklular için pasaport, uluslararası geçerliliği olan muadili belge veya TC yetkili mercilerince verilmiş kimliği tespiti yarayan belge ibraz ettirilerek teyit edilir.

(4) Haberleşme gönderileri ile hizmet sağlayıcı ile bir sözleşme kapsamında fatura ya da irsaliye ile taşıttırılan gönderiler hariç diğer gönderiler, özel hayatın gizliliğine de dikkat edilerek gönderici huzurunda kontrol edilerek kabul edilir. Ancak, haberleşme gönderileri ile hizmet sağlayıcı ile bir sözleşme kapsamında fatura ya da irsaliye ile taşıttırılan gönderilerden; içerisinde yasak madde bulunduğundan şüphelenilen veya posta kolisi veya kargosu niteliğindeki kapalı gönderiler özel hayatın gizliliğine de dikkat edilerek göndericiye açılarak kapsamı kontrol edildikten sonra kabul edilir. Göndericinin, gönderinin kabulü aşamasında gerekli olan kimlik bilgileri ve iletişim bilgilerini vermek istememesi veya kapsam kontrolüne razı olmaması durumunda gönderiler kabul edilmez.

(5) Haberleşme gönderileri hariç diğer gönderilerde, gönderi sayısının 10'dan az olması halinde en az yarısı, 10 ila 100 arasında olması halinde asgari 6 olmak üzere gönderi sayısının en az %10'u ve 100'den fazla olması halinde asgari 10 olmak üzere gönderi sayısının en az %5'i hizmet sağlayıcı tarafından rastgele seçilerek gönderici huzurunda kontrol edilir. Hizmet sağlayıcısının seçilen paketleri kontrol eden personelinin ad-soyad ve kimlik bilgileri ile kontrol edilen paketlere ilişkin bilgiler kayıt altına alınır ve gerektiğinde ilgili mercilere sunulmak üzere gizliliği sağlanarak en az iki yıl süreyle saklanır. Göndericinin söz konusu kontrole razı olmaması halinde gönderi kabul edilmez. Ancak, hizmet sağlayıcı ile bir sözleşme kapsamında fatura ya da irsaliye ile taşıttırılan gönderiler için işbu fıkranın birinci cümlesinde yer alan hüküm uygulanmayabilir.

Kullanıcıların hizmet sağlayıcıları hakkında bilgi sahibi olması

MADDE 5 – (1) Posta hizmetinde kullanılan işyerlerinde, araçlarda ve kıyafetlerde, gönderinin kabulü ve alıcıya teslimi aşamasında ilgili hizmet sağlayıcının kurumsal amblem/logo, marka ismi gibi ayırt edici işaretinin ve/veya ilgili personelin personel kimlik kartının görünür bir şekilde bulunması zorunludur.

(2) Gönderinin kabulü ve alıcıya teslimi aşamasında, hizmet sağlayıcının başka bir hizmet sağlayıcının gönderilerini kabul veya alıcıya teslim hizmeti vermesi durumunda, gönderileri kabul veya alıcıya teslim eden hizmet sağlayıcının kurumsal amblem/logo marka ismi gibi ayırt edici işaretinin ve/veya ilgili personelin personel kimlik kartının görünür bir şekilde bulunması zorunludur.

(3) Hizmet sağlayıcısı, acentelerinin de hizmet sağlayıcılarına ait kurumsal amblem/logo marka ismi gibi ayırt edici işaretini ve/veya ilgili personelin personel kimlik kartını görünür bir şekilde bulundurmasından sorumludur.

Posta gönderilerinin görüntüleme cihazları ile kontrolü

MADDE 6 – (1) Kabulden sonra, hizmet sağlayıcıları tarafından posta gönderileri içerisinde yasak madde bulunduğundan şüphelenilmesi durumunda, en yakın resmi güvenlik birimi görevlileri huzurunda şüpheli gönderi kontrol ettirilebilir. Hizmet sağlayıcının görüntüleme cihazı varsa, söz konusu gönderi resmi güvenlik birimi görevlileri huzurunda görüntüleme cihazları ile kontrol edilir. Gönderilmesi yasak maddelerin tespit edilmesi halinde ilgili mevzuata göre işlem yapılır.

(2) Hizmet sağlayıcılarının posta gönderilerini kabul merkezlerinde kamera sistemi kurularak kayıtlar, gerektiğinde ilgili mercilere sunulmak üzere en az bir (1) ay süreyle saklanır.

Hizmet sağlayıcılar tarafından Kuruma bilgi gönderilmesi ile ilgili hükümler

MADDE 7 – (1) Hizmet sağlayıcıları, posta gönderilerine ilişkin olarak iş bu Usul ve Esasların 4 üncü maddesinin birinci ve ikinci fıkraları ile 5 inci maddesinde yer alan bilgi ve belgeleri, Kurum tarafından belirlenecek usul, esas ve standartlarda eksiksiz ve zamanında tüm harcamaları kendilerine ait olmak üzere elektronik ortamda kuruma teslim etmekle yükümlüdür.

(2) Hizmet sağlayıcıları, masrafları kendilerine ait olmak üzere her türlü sistemin işletilmesinden, bakımından, söz konusu sistemlerin çalışır vaziyette tutulması için gerekli donanım, yazılım, bakım, onarım, teknik destek gibi gerekli tedbiri almakla ve bunları etkileyen donanım, yazılım, altyapı ve şebekeye ilişkin değişiklikleri Kurum onayını alarak yapmakla yükümlüdürler.

Cezai hükümler

MADDE 8 – (1) Bu Usul ve Esaslarda yer alan hükümlere uyulmaması halinde Bilgi Teknolojileri ve İletişim Kurumu Posta Hizmetlerinde İdari Yaptırım Yönetmeliği ve ilgili diğer mevzuat hükümleri uyarınca işlem yapılır.

Yürürlük

MADDE 9 - (1) Bu Usul ve Esaslar'ın 6 ncı ve 7 nci maddelerinde yer alan hükümler bu Usul ve Esasların Bilgi Teknolojileri ve İletişim Kurulu tarafından onaylandığı tarihten 6 ay sonra, diğer hükümleri onaylandığı tarihten 3 ay sonra yürürlüğe girer.

Yürütme

MADDE 10 - (1) Bu Usul ve Esasların hükümlerini Bilgi Teknolojileri ve İletişim Kurulu Başkanı yürütür.

ANAYASA MAHKEMESİ NORM DENETİMİ KARARLARI

Bölüm İçeriği

- 6698 sayılı Kişisel Verilerin Korunması Kanunu Kararı (E. 2016/125)
- 715 sayılı Kanun - MİT Kanunu Kararı (E. 2018/137)
- 5188 sayılı Özel Güvenlik Hizmetlerine Dair Kanun Kararı (E. 2021/42)
- 1 numaralı CBK Kararı (MASAK) (E. 2019/96)
- 7068 sayılı Genel Kolluk Disiplin Hükümleri Hakkında Kanun Hükmünde Kararnamenin Kabul Edilmesine Dair Kanun Kararı (E. 2020/77)
- 77 numaralı CBK Kararı (E. 2021/88)
- 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu Kararı (E. 2021/43)
- 6791 sayılı Kanun Kararı (E. 2020/41)
- 4045 sayılı Kanun Kararı (E. 2020/24)
- 4045 sayılı Kanun Kararı (E. 2018/163)
- 14 numaralı CBK Kararı (E. 2018/134)
- 13 numaralı CBK Kararı (E. 2018/133)
- 2559 sayılı Polis Vazife ve Salahiyet Kanunu Kararı (E. 2018/91)
- 657 sayılı Kanun Kararı (E. 2018/73)
- 5490 sayılı Nüfus Hizmetleri Kanunu Kararı (2017/180)
- 5809 sayılı Elektronik Haberleşme Kanunu Kararı (Madde 60) (E. 2017/16)
- 4632 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanunu Kararı (E. 2016/179)
- 5809 sayılı Elektronik Haberleşme Kanunu Kararı (Revize-Madde 51) (E. 2015/61)
- 5237 sayılı Türk Ceza Kanunu Kararı (E. 2015/32)
- 6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun Kararı (E. 2014/196)
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu Kararı (E. 2014/180)
- 5651 sayılı Kanun (Trafik Bilgisi) Kararı (E. 2014/149)
- 6532 sayılı Kanun - MİT Kanunu Kararı (E. 2014/122)
- 5651 sayılı Kanun (TİB Yetkileri) Kararı (E. 2014/87)
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu (Madde 78) Kararı (E. 2014/74)
- 663 Sayılı KHK Kararı (E. 2013/114)
- 5809 sayılı Elektronik Haberleşme Kanunu (Madde 51) Kararı (E. 2013/122)
- 6475 sayılı Posta Hizmetleri Kanunu (E. 2013/84)

- 2004 sayılı İcra ve İflas Kanunu Kararı (E. 2012/100)
- 663 sayılı Kanun Kararı (E. 2011/150)
- 5952 sayılı Kanun Kararı (E. 2010/40)
- 5429 sayılı Türkiye İstatistik Kanunu (2010/12)
- 5237 sayılı Türk Ceza Kanun (245. Madde) Kararı (E. 2006/123)

ANAYASA MAHKEMESİ KARARI

Esas Sayısı : 2016/125

Karar Sayısı : 2017/143

Karar Tarihi : 28.9.2017

RG Tarih/Sayı: 23.1.2018 - 30310

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri Engin ALTAY, Levent GÖK, Özgür ÖZEL ile birlikte 124 milletvekili

İPTAL DAVASININ KONUSU: 24.3.2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun;

A. 4. maddesinin (2) numaralı fıkrasının (d) bendinde yer alan "...veya işlendikleri amaç için gerekli olan..." ibaresinin,

B. 5. maddesinin (2) numaralı fıkrasının (c), (ç), (e) ve (f) bentlerinin,

C. 6. maddesinin;

1. (1) numaralı fıkrasında yer alan "...mezhebi,..." ve "...kılık ve kıyafeti..." ibarelerinin,

2. (3) numaralı fıkrasının,

D. 7. maddesinin (2) numaralı fıkrasının,

E. 8. maddesinin (3) numaralı fıkrasının,

F. 9. maddesinin (6) numaralı fıkrasının,

G. 13. maddesinin (2) numaralı fıkrasının ikinci cümlesinin,

H. 15. maddesinin (3) numaralı fıkrasında yer alan "Devlet sırrı niteliğindeki bilgi ve belgeler hariç..." ibaresinin,

I. 16. maddesinin (2) numaralı fıkrasının ikinci cümlesinin,

İ. 24. maddesinin (3) numaralı fıkrasının (b) bendinde yer alan "...Kurulca gerekli görülenlerin..." ibaresinin,

J. 28. maddesinin (1) numaralı fıkrasının (a) ve (ç) bentlerinin,

K. 30. maddesinin (7) numaralı fıkrası ile değiştirilen 11.10.2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 47. maddesinin,

Anayasa'nın 2., 5., 10., 13., 17., 20., 24., 25., 41., 56. ve 90. maddelerine aykırılığı ileri sürülerek iptallerine ve yürürlüklerinin durdurulmasına karar verilmesi talebidir.

I. İPTALİ İSTENEN KANUN HÜKÜMLERİ

İptali istenen kuralların yer aldığı 6698 sayılı Kanun'un;

1. 4. maddesi şöyledir:

"Genel ilkeler

MADDE 4- (1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.

(2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

- a) Hukuka ve dürüstlük kurallarına uygun olma.
- b) Doğru ve gerektiğinde güncel olma.
- c) Belirli, açık ve meşru amaçlar için işlenme.
- ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
- d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme."

2. 5. maddesi şöyledir:

"Kişisel verilerin işlenme şartları

MADDE 5- (1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

- a) Kanunlarda açıkça öngörülmesi.
- b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

- c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.”

3. 6. maddesi şöyledir:

“Özel nitelikli kişisel verilerin işleme şartları

MADDE 6- (1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebiveya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.”

4. 7. maddesi şöyledir:

“Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi

MADDE 7- (1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.

(2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır.

(3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir.”

5. 8. maddesi şöyledir:

“Kişisel verilerin aktarılması

MADDE 8- (1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz.

(2) Kişisel veriler;

a) 5 inci maddenin ikinci fıkrasında,

b) Yeterli önlemler alınmak kaydıyla, 6 ncı maddenin üçüncü fıkrasında, belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir.

(3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.”

6. 9. maddesi şöyledir:

“Kişisel verilerin yurt dışına aktarılması

MADDE 9- (1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz.

(2) Kişisel veriler, 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede;

a) Yeterli korumanın bulunması,

b) Yeterli korumanın bulunmaması durumunda Türkiye’deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması, kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir.

(3) Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir.

(4) Kurul yabancı ülkede yeterli koruma bulunup bulunmadığına ve ikinci fıkranın (b) bendi uyarınca izin verilip verilmeyeceğine;

a) Türkiye’nin taraf olduğu uluslararası sözleşmeleri,

b) Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu,

c) Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işleme amaç ve süresini,

ç) Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını,

d) Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri, değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir.

(5) Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir.

(6) Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır."

7. 13. maddesi şöyledir:

"Veri sorumlusuna başvuru

MADDE 13- (1) İlgili kişi, bu Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir.

(2) Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak, işlemin ayrıca bir maliyeti gerektirmesi hâlinde, Kurulca belirlenen tarifedeki ücret alınabilir.

(3) Veri sorumlusu talebi kabul eder veya gerekçesini açıklayarak reddeder ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. Başvuruda yer alan talebin kabul edilmesi hâlinde veri sorumlusunca gereği yerine getirilir. Başvurunun veri sorumlusunun hatasından kaynaklanması hâlinde alınan ücret ilgiliye iade edilir."

8. 15. maddesi şöyledir:

"Şikâyet üzerine veya resen incelemenin usul ve esasları

MADDE 15- (1) Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapar.

(2) 1/11/1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesinde belirtilen şartları taşımayan ihbar veya şikâyetler incelemeye alınmaz.

(3) Devlet sırrı niteliğindeki bilgi ve belgeler hariç; veri sorumlusu, Kurulun, inceleme konusuyla ilgili istemiş olduğu bilgi ve belgeleri on beş gün içinde göndermek ve gerektiğinde yerinde inceleme yapılmasına imkân sağlamak zorundadır.

(4) Şikâyet üzerine Kurul, talebi inceleyerek ilgililere bir cevap verir. Şikâyet tarihinden itibaren altmış gün içinde cevap verilmezse talep reddedilmiş sayılır.

(5) Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması hâlinde Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ eder. Bu karar, tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilir.

(6) Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin yaygın olduğunun tespit edilmesi hâlinde Kurul, bu konuda ilke kararı alır ve bu kararı yayımlar. Kurul, ilke kararı almadan önce ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşlerini de alabilir.

(7) Kurul, telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması hâlinde, veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulmasına karar verebilir.”

9. 16. maddesi şöyledir:

“Veri Sorumluları Sicili

MADDE 16- (1) Kurulun gözetiminde, Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili tutulur.

(2) Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir.

(3) Veri Sorumluları Siciline kayıt başvurusu aşağıdaki hususları içeren bir bildirimle yapılır:

- a) Veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri.
- b) Kişisel verilerin hangi amaçla işleneceği.
- c) Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar.
- ç) Kişisel verilerin aktarılabilceği alıcı veya alıcı grupları.
- d) Yabancı ülkelere aktarımı öngörülen kişisel veriler.
- e) Kişisel veri güvenliğine ilişkin alınan tedbirler.
- f) Kişisel verilerin işlendikleri amaç için gerekli olan azami süre.

(4) Üçüncü fıkra uyarınca verilen bilgilerde meydana gelen değişiklikler derhâl Başkanlığa bildirilir.

(5) Veri Sorumluları Siciline ilişkin diğer usul ve esaslar yönetmelikle düzenlenir.”

10. 24. maddesi şöyledir:

“Başkan

MADDE 24- (1) Başkan, Kurul ve Kurumun başkanı sıfatıyla Kurumun en üst amiri olup Kurum hizmetlerini mevzuata, Kurumun amaç ve politikalarına, stratejik planına, performans ölçütlerine ve hizmet kalite standartlarına uygun olarak düzenler, yürütür ve hizmet birimleri arasında koordinasyonu sağlar.

(2) Başkan, Kurumun genel yönetim ve temsilinden sorumludur. Bu sorumluluk, Kurum çalışmalarının düzenlenmesi, yürütülmesi, denetlenmesi, değerlendirilmesi ve gerektiğinde kamuoyuna duyurulması görev ve yetkilerini kapsar.

(3) Başkanın görevleri şunlardır:

a) Kurul toplantılarını idare etmek.

b) Kurul kararlarının tebliğini ve Kurulca gerekli görülenlerin kamuoyuna duyurulmasını sağlamak ve uygulanmalarını izlemek.

c) Başkan Yardımcısını, daire başkanlarını ve Kurum personelini atamak.

ç) Hizmet birimlerinden gelen önerilere son şeklini vererek Kurula sunmak.

d) Stratejik planın uygulanmasını sağlamak, hizmet kalite standartları doğrultusunda insan kaynakları ve çalışma politikalarını oluşturmak.

e) Belirlenen stratejilere, yıllık amaç ve hedeflere uygun olarak Kurumun yıllık bütçesi ile mali tablolarını hazırlamak.

f) Kurul ve hizmet birimlerinin uyumlu, verimli, disiplinli ve düzenli bir biçimde çalışması amacıyla koordinasyonu sağlamak.

g) Kurumun diğer kuruluşlarla ilişkilerini yürütmek.

ğ) Kurum Başkanı adına imzaya yetkili personelin görev ve yetki alanını belirlemek.

h) Kurumun yönetim ve işleyişine ilişkin diğer görevleri yerine getirmek.

(4) Kurum Başkanının yokluğunda İkinci Başkan, Başkana vekalet eder.”

11. 28. maddesi şöyledir:

“İstisnalar

MADDE 28- (1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:

- a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklerle uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi.
- b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.
- c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.
- ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.
- d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

(2) Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri aşağıdaki hâllerde uygulanmaz:

- a) Kişisel veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.
- b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.
- c) Kişisel veri işleminin kanunun verdiği yetkiye dayanarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.
- ç) Kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.”

12. 30. maddesi şöyledir:

“Değiştirilen ve eklenen hükümler

MADDE 30- (1) (10/12/2003 tarihli ve 5018 sayılı Kanun ile ilgili olup yerine işlenmiştir.)

(2) ila (5) - (26/9/2004 tarihli ve 5237 sayılı Kanun ile ilgili olup yerine işlenmiştir.)

(6) (7/5/1987 tarihli ve 3359 sayılı Sağlık Hizmetleri Temel Kanunu ile ilgili olup yerine işlenmiştir.)

(7) 11/10/2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 47 nci maddesi aşağıdaki şekilde değiştirilmiştir.

'MADDE 47- (1) Sağlık hizmeti almak üzere, kamu veya özel sağlık kuruluşları ile sağlık mesleği mensuplarına müracaat edenlerin, sağlık hizmetinin gereği olarak vermek zorunda oldukları veya kendilerine verilen hizmete ilişkin kişisel verileri işlenebilir.

(2) Sağlık hizmetinin verilmesi, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve maliyetlerin hesaplanması amacıyla Bakanlık, birinci fıkra kapsamında elde edilen verileri alarak işleyebilir. Bu veriler, Kişisel Verilerin Korunması Kanununda öngörülen şartlar dışında aktarılamaz.

(3) Bakanlık, ikinci fıkra gereğince toplanan ve işlenen kişisel verilere, ilgili kişilerin kendilerinin veya yetki verdikleri üçüncü kişilerin erişimlerini sağlayacak bir sistem kurar.

(4) Üçüncü fıkraya göre kurulan sistemlerin güvenliği ve güvenilirliği ile ilgili standartlar Kişisel Verileri Koruma Kurulunun belirlediği ilkelere uygun olarak Bakanlıkça belirlenir. Bakanlık, bu Kanun uyarınca elde edilen kişisel sağlık verilerinin güvenliğinin sağlanması için gerekli tedbirleri alır. Bu amaçla, sistemde kayıtlı bilgilerin hangi görevli tarafından ne amaçla kullanıldığının denetlenmesine imkân tanıyan bir güvenlik sistemi kurar.

(5) Sağlık personeli istihdam eden kamu kurum ve kuruluşları ile özel hukuk tüzel kişileri ve gerçek kişiler, istihdam ettiği personeli ve personel hareketlerini Bakanlığa bildirmekle yükümlüdür.

(6) Kişisel sağlık verilerinin işlenmesi, güvenliği ve bu maddenin uygulanması ile ilgili diğer hususlar Bakanlıkça yürürlüğe konulan yönetmelikle düzenlenir.'''

II. İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Zühtü ARSLAN, Burhan ÜSTÜN, Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ, Alparslan ALTAN, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Erdal TERCAN, Muammer TOPAL, M. Emin KUZ, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA ve Rıdvan GÜLEÇ'in katılımlarıyla 22.6.2016 tarihinde yapılan ilk inceleme toplantısında dosyada eksiklik bulunmadığından işin esasının incelenmesine, yürürlüğü durdurma talebinin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

III. ESASIN İNCELENMESİ

2. Dava dilekçesi ve ekleri, Raportör Berrak YILMAZ tarafından hazırlanan işin esasına ilişkin rapor, dava konusu kanun hükümleri, dayanılan ve ilgili görülen Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A. Kanun'un 4. Maddesinin (2) Numaralı Fıkrasının (d) Bendinde Yer Alan "...veya işlendikleri amaç için gerekli olan..." İbaresinin İncelenmesi

1. İptal Talebinin Gerekçesi

3. Dava dilekçesinde özetle, dava konusu kuralın yer aldığı maddenin esas itibarıyla kişisel verilerin işlenmesindeki güvenceleri düzenlediği, bu güvencelerden en önemlisinin kişisel verilerin muhafaza süresi olduğu, işlendiği amaç için gerekli olan süre şeklindeki dava konusu kuralın ise belirsiz, subjektif, geniş ve yorumlayana göre değişebilecek nitelikte olduğundan kişisel verileri işleyen gerçek veya tüzel kişilerin ne kadar süre ile kişisel verileri muhafaza edebileceğinin belirli olmadığı, kişilerin hukuk güvenliğini tehdit ettiği ve Avrupa Konseyi tarafından hazırlanarak 1981 tarihinde imzaya açılan 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşme'de (108 sayılı Sözleşme) yer alan esaslarla uyumlu olmadığı belirtilerek kuralın Anayasa'nın 2. ve 90. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

4. 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 43. maddesi uyarınca kural, ilgisi nedeniyle Anayasa'nın 20. maddesi yönünden de incelenmiştir.

5. Dava konusu kuralın yer aldığı fıkrada, kişisel verilerin işlenmesinde uyulması zorunlu ilkeler düzenlenmektedir. Fıkranın (d) bendinde bu ilkelerden biri olarak kişisel verilerin mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi öngörülmektedir. Fıkrada yer alan "...veya işlendikleri amaç için gerekli olan ..." ibaresi dava konusu kuralı oluşturmaktadır.

6. Anayasa'nın 2. maddesinde belirtilen hukuk devleti; eylem ve işlemleri hukuka uygun, insan haklarına saygılı, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adaletli bir hukuk düzeni kurup bunu geliştirerek sürdüren, Anayasa'ya aykırı durum ve tutumlardan kaçınan, Anayasa ve hukukun üstün kurallarıyla kendini bağlı sayan, yargı denetimine açık olan devlettir.

7. Hukuk devletinin temel ilkelerinden biri de "belirlilik"tir. Bu ilkeye göre yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olması, ayrıca kamu otoritelerinin keyfî uygulamalarına karşı koruyucu önlem içermesi gereklidir. Belirlilik ilkesi, hukuksal güvenlikle bağlantılı olup bu ilke gereği birey

hangi somut eylem ve olguya hangi hukuksal yaptırımın veya sonucun bağlandığını, bunların hangi müdahale yetkisini doğurduğunu bilmelidir. Birey ancak bu durumda kendisine düşen yükümlülükleri öngörebilir ve davranışlarını belirler. Hukuk güvenliği; normların öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar.

8. Anayasa'nın 20. maddesinin birinci fıkrasında, "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz." denilerek özel hayatın gizliliği hakkı güvence altına alınmıştır. Maddenin üçüncü fıkrasında ise herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı ifade edilmiştir. Maddede ayrıca kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir.

9. 6698 sayılı Kanun'un 3. maddesine göre kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Anayasa Mahkemesinin kararlarında da belirtildiği üzere "... Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler" kişisel veri olarak kabul edilmektedir (E. 2013/122, K. 2014/74, 9.4.2014; E. 2014/149, K. 2014/151, 2.10.2014; E. 2013/84, K. 2014/183, 4.12.2014; E. 2014/74, K. 2014/201, 25.12.2014; E. 2014/180, K. 2015/30, 19.3.2015; E. 2015/32, K. 2015/102, 12.11.2015).

10. Kişisel veri kavramı tarafı olduğumuz Avrupa İnsan Hakları Sözleşmesi'nde (AİHS) açık bir şekilde düzenlenmemekle birlikte, AİHS'nin uygulanmasına ilişkin Avrupa İnsan Hakları Mahkemesi (AİHM) kararlarında 108 sayılı Sözleşme'ye atıfta bulunulmakta ve bu verilerin özel yaşamın gizliliğinin bir parçası olduğu kabul edilmektedir. AİHM kararlarında kişilere ait "görüntü", "fotoğraf", "parmak izi", "DNA profili", "hücre örnekleri", "ev adresi" ve "yaş, doğum tarihi ve fiziksel özellikler" kişisel veri kapsamında değerlendirilmektedir (Peck/Birleşik Krallık, B. No: 44647/98, 28.01.2003; Sciacca/İtalya, B. No: 50774/99, 11.01.2005; S. ve Marper/Birleşik Krallık(Büyük Daire), B. No: 30562/04, 30566/04, 04.12.2008; Alkaya/Türkiye, B. No: 42811/06, 09.10.2012; K.U./Finlandiya, B. No: 2872/02, 02.12.2008).

11. Kişisel verilerin korunmasında hâkim olan temel ilkeler dava konusu kuralın da yer aldığı 6698 sayılı Kanun'un 4. maddesinde belirtilmiştir. Maddede, kişisel verilerin işlenmesinde uyulması zorunlu bu ilkeler; hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayılmıştır.

12. 108 sayılı Sözleşme'nin verilerin niteliğini düzenleyen 5. maddesinin (e) bendinde de otomatik işleme konu olan kişisel verilerin "Kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkân veren bir biçimde" saklanacağı belirtilmiştir.

13. AİHM kararlarında da kişisel verilerin gerekenden uzun süre tutulması ihlal nedeni olarak kabul edilmiştir. Mahkeme şüphelilerin parmak izi, DNA profili ve hücre örneklerinin ulusal bir veri tabanına aktarılmasına ilişkin başvuruda, kayıt altına alınabilir herhangi bir suç dolayısıyla bir kişinin parmak izi ve DNA örneklerinin belirsiz bir süre saklanmasına izin veren uygulamayı AİHS'nin 8. maddesine aykırı bulmuştur (S. ve Marper/Birleşik Krallık ((Büyük Daire), B. No: 30562/04, 30566/04, 04.12.2008).

14. Dava konusu kuralın yer aldığı madde gerekçesinde, kişisel verilerin ancak ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesinin zorunlu olduğu, buna göre veri sorumlularının ilgili mevzuatta verilerin saklanması için öngörülen bir süre varsa bu süreye uyacağı yoksa verileri ancak işlendikleri amaç için gerekli olan süre kadar muhafaza edebileceği, bir verinin daha fazla saklanması için geçerli bir sebep olmaması durumunda o verinin silineceği veya anonim hâle getirileceği, gelecekte kullanma ihtimalinin varlığına dayanarak veri saklanamayacağı, veri sorumlularının Kanun'un 16. maddesi uyarınca Veri Sorumluları Siciline kayıt için başvuru yaparken kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi bildirmek zorunda oldukları ifade edilmektedir.

15. Kişisel verilerin işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi ilkesi kişisel verilerin korunmasının en önemli ilkelerinden biridir. Zira kişisel verilerin korunması hakkı, herhangi bir kişinin kendisiyle ilgili olarak toplanan kişisel verilerin toplanma amacına ulaşıldıktan sonra bilgisi dışında muhafaza edilmeyeceği veya başka bir amaç için kullanılmayacağı güvencesine sahip olması hâlinde söz konusu olabilir. Kişinin kişisel verilerinin hayatı boyunca bir yerlerde kayıtlı tutulacağını ve başka bir amaçla kullanılabileceğini düşünmesi kişisel verilerin korunması hakkını zedeler. Bu bağlamda dava konusu kuralla kanun koyucunun, ilgili mevzuatta kişisel verilerin

saklanması için bir süre öngörülmemesi durumunda bu verilerin ancak işlendikleri amaç için gerekli olan süre kadar muhafaza edilebilmesi suretiyle kişisel verilerin süresiz bir şekilde muhafaza edilmesi ihtimalini ortadan kaldırmaya yönelik bir düzenleme yapmayı ve kanunda muhafaza süresi belirtilmeyen kişisel verilerle ilgili olarak kişilere güvence sağlamayı amaçladığı anlaşılmaktadır.

16. Çok geniş bir kavramı ifade eden kişisel veriler çok farklı amaçlarla ve farklı şekillerde işlenebileceğinden kanun koyucu tarafından her bir kişisel veri için önceden muhafaza edilme süresi öngörülmesi mümkün olmayabilir. Diğer taraftan 6698 sayılı Kanun'un bireylere veri sorumlusuna başvuru hakkının düzenlendiği 11. maddesine göre veri sahipleri her zaman kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme hakkına sahip olduğu gibi kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesini düzenleyen 7. maddesine göre öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme hakkına da sahiptir.

17. Ayrıca 6698 sayılı Kanun'un 16. maddesine göre Kişisel Verileri Koruma Kurulu gözetiminde Başkanlık tarafından kamuya açık olarak tutulan Veri Sorumluları Sicili'ne kişisel verileri işleyen gerçek ve tüzel kişiler tarafından veri işlenmeye başlanmadan önce bulunulması gereken kayıt başvurusunda yapılan bildirimde kişisel verilerin işlendikleri amaç için gerekli olan azami sürenin de belirtilmesi gerekir. Kanun'un anılan hükümleri ve 108 sayılı Sözleşme'nin 5. maddesinin (e) bendindeki süreye yönelik düzenleme dikkate alındığında, muhafaza süresi mevzuatta öngörülmemeyen kişisel verilerle ilgili olarak kişilere güvence sağlamaya yönelik dava konusu kuralın belirsiz ve subjektif bir niteliğe sahip olduğu söylenemez. Dolayısıyla kuralda kişisel verilerin korunmasıyla ilgili uluslararası hukukta da temel ilkelerden biri olarak kabul edilen verilerin amacın gerektirdiğinden daha uzun süre tutulmama ilkesine aykırı bir yön bulunmamaktadır.

18. Açıklanan nedenlerle kural Anayasa'nın 2. ve 20. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

19. Kuralın Anayasa'nın 90. maddesiyle ilgisi görülmemiştir.

B. Kanun'un 5. Maddesinin (2) Numaralı Fıkrasının (c), (ç), (e) ve (f) Bentlerinin İncelenmesi

1. İptal Taleplerinin Gerekçesi

20. Dava dilekçesinde özetle, dava konusu kuralların yer aldığı maddede kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği kuralının istisnalarının düzenlendiği, istisnaların sınırları belirlenmiş bir şekilde tadadi olarak sayılması gerektiği ancak dava konusu kurallarla istisnaların esas düzenleme hâline gelerek Kanun'un uygulanmasında açık rızanın aranmasına gerek

duyulmasının neredeyse imkânsız hâle getirildiği, kişisel verilerin korunmasına ilişkin anayasal güvencenin yaşama geçirilebilmesi için bu hakkı ilgilendiren yasal düzenlemelerin açık, anlaşılabilir ve kişilerin söz konusu haklarını kullanabilmelerine elverişli olması gerektiği ancak dava konusu kuralların kapsam ve sınırlarının belirsiz olduğu, özellikle “meşru menfaat” kavramının kapsamının belli olmadığı, temel hak ve özgürlüklere ilişkin sınırlamanın Anayasa’ya uygun olabilmesi için temel hakların sınırlandırılmasına ilişkin ilkelere aykırı olmaması ve bu bağlamda kamu yararı ile özel hayatın gizliliği hakkı arasında adil bir denge kurması gerektiği, dava konusu kuralların ise bireylerin özel yaşamına doğrudan bir müdahale niteliğinde olduğu, kişisel verilerin korunması hakkını ölçüsüzce sınırladığı ve hakkın özüne zarar verdiği, kanun koyucunun takdir yetkisini adalet, hakkaniyet ve kamu yararı ölçütlerini göz önünde tutarak kullanması gerektiği, kuralların kamu yararı amacı taşımadığı belirtilerek Anayasa’nın 2., 13., 20. ve 90. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa’ya Aykırılık Sorunu

21. Dava konusu kuralların yer aldığı maddede kişisel verilerin işleme şartları düzenlenmiştir. Maddenin birinci fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği hükme bağlanmış, ikinci fıkrasında ise ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hâller belirtilmiştir. Bunlar (2) numaralı fıkranın (a) bendinde, kanunlarda açıkça öngörülmesi; (b) bendinde, fiilî imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması; (c) bendinde, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; (ç) bendinde, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; (d) bendinde, ilgili kişinin kendisi tarafından alenileştirilmiş olması; (e) bendinde, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması ve (f) bendinde, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şeklinde belirlenmiştir. Dava konusu kurallar Kanun’un 5. maddesinin (2) numaralı fıkrasının (c), (ç), (e) ve (f) bentleridir.

22. Anayasa’nın 2. maddesindeki hukuk devleti ilkesinin gereği olarak kanunlar kamu yararı amacını gerçekleştirmek üzere çıkarılmalıdır. Anayasa Mahkemesi’nin kimi kararlarında kamu yararı kavramından ne anlaşılması gerektiği ortaya konulmuştur. Buna göre kamu yararı kavramı genel bir ifadeyle bireysel, özel çıkarılardan ayrı ve bunlara üstün olan toplumsal yararı ifade etmektedir. Bu bağlamda kanun koyucu, sosyal yaşamı düzenlemek için kamu yararı amacıyla kimi kurallar

koyabilir. Kamu yararı düşüncesi olmaksızın yalnız özel çıkarlar için veya yalnız belli kişilerin yararına olarak kanun hükmü konulamaz. Böyle bir durumun açık bir biçimde ve kesin olarak saptanması hâlinde söz konusu kanun hükmü Anayasa'nın 2. maddesine aykırı düşer. Açıklanan ayırık hâl dışında bir kanun hükmünün ülke gereksinimlerine uygun olup olmadığı, hangi araç ve yöntemlerle kamu yararının sağlanabileceği bir siyasi tercih sorunu olarak kanun koyucunun takdirinde olduğundan bu kapsamda kamu yararı değerlendirmesi yapmak anayasa yargısıyla bağdaşmaz.

23. Anayasa'nın 20. maddesinin birinci fıkrasında özel hayatın gizliliği hakkı güvence altına alınmıştır. Ancak aynı maddenin ikinci fıkrasında millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biriyle özel hayatın gizliliğinin sınırlanmasına olanak tanınmıştır. Anayasa Mahkemesi kararlarında da vurgulandığı üzere özel sınırlama nedeni öngörülmemiş özgürlüklerin de o özgürlüğün doğasından kaynaklanan sınırlarının bulunduğu, ayrıca Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebileceği kabul edilmektedir.

24. Anayasa'nın 20. maddesinin üçüncü fıkrasında ise "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmü yer almaktadır.

25. 108 sayılı Sözleşme'nin 9. maddesinde de devlet güvenliği, kamu güvenliği, devletin ekonomik menfaatlerinin korunması ve suçlarla mücadele edilmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması ile verilerin istatistiki veya bilimsel amaçlarla kullanılması durumlarında kişisel verilerin korunmasına sınırlamalar getirilebileceği belirtilmektedir.

26. Ancak bu sınırlama yapılırken temel hak ve özgürlüklerin sınırlandırılması rejimini belirleyen Anayasa'nın 13. maddesine de uyulması gerekmektedir. Anayasa'nın 13. Maddesinde "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz." denilmektedir. Anayasa'nın 13. maddesi uyarınca özel hayatın gizliliği ve kişisel verilerin korunması hakları, yalnızca kanunla ve demokratik bir toplumda gerekli olduğu ölçüde sınırlanabilir. Ayrıca

getirilen bu sınırlamalar hakkın özüne dokunamayacağı gibi Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamaz.

27. Temel hak ve özgürlükler özlerine dokunulmaksızın yalnızca Anayasa'da öngörülen sebeplerle ve ancak kanunla sınırlanabilir. Dokunulamayacak "öz", her temel hak ve özgürlük açısından farklılık göstermekle birlikte kanunla getirilen sınırlamanın hakkın özüne dokunmadığının kabulü için temel hakların kullanılmasını ciddi surette güçleştirip amacına ulaşmasına engel olmaması ve etkisini ortadan kaldırıcı bir nitelik taşımaması gerekir.

28. Temel hak ve özgürlüklerin özlerine dokunulmaksızın yapılan sınırlamaların ise demokratik toplum düzeninin gerekleri ile ölçülülük ilkesine aykırı olamayacağı belirtilmiştir. Öze dokunma yasağını ihlal etmeyen müdahaleler yönünden gözetilmesi öngörülen "demokratik toplum düzeninin gerekleri" kavramı, öncelikle ilgili hak yönünden getirilen sınırlamaların zorunlu ve istisnai tedbir niteliğinde olmalarını gerektirmektedir. "Demokratik toplum düzeninin gerekleri"nden olma, bir sınırlamanın demokratik bir toplumda zorlayıcı bir toplumsal ihtiyacın karşılanması amacına yönelik olmasını ifade etmektedir.

29. Anayasa'nın 13. maddesinde ifade edilen "ölçülülük ilkesi", temel hak ve özgürlüklerin sınırlandırılmasına ilişkin başvurularda dikkate alınması gereken bir diğer ilkedir. Demokratik toplum düzeninin gerekleri ve ölçülülük ilkeleri, iki ayrı kriter olarak düzenlenmiş olmakla birlikte bu iki kriter arasında sıkı bir ilişki vardır. Temel hak ve özgürlüklere yönelik herhangi bir sınırlamanın başvurulabilecek en son çare ya da alınabilecek en son önlem olarak temel haklara en az müdahaleye olanak veren ölçülü bir sınırlama niteliğinde olup olmadığının incelenmesi gerekir.

30. Demokratik toplum kişilerin temel hak ve özgürlüklerinin en geniş şekilde güvence altına alındığı bir düzeni gerektirir. Demokrasilerde devlete düşen görev temel hak ve özgürlükleri korumak ve geliştirmek, bunların etkili şekilde kullanılmasını sağlayacak tedbirleri almaktır. Bu kapsamda devlet, özellikle temel hak ve özgürlükleri ortadan kaldıracak veya bunlara ölçüsüz müdahale teşkil edecek tutumlardan kaçınmalı ve başkalarından gelebilecek tehditlere karşı bireyleri korumalıdır.

31. Özel hayatın gizliliği ve kişisel verilerin korunması hakkı, temel hak ve özgürlükler arasında önemli bir yer alır. Özel hayatın gizliliğinin korunması, bu hayatın başkalarının gözleri önüne serilmemesi demektir. Kişinin özel hayatının, yalnız kendisi veya kendisinin bilmesini istediği kişiler tarafından bilinmesini isteme hakkı, kişinin temel haklarından biridir ve bu niteliği nedeniyle insan haklarına ilişkin beyanname ve sözleşmelerde yer almış; demokratik ülkelerin mevzuatında açıkça belirlenen istisnalar dışında devlete, topluma ve diğer kişilere karşı korunmuştur. Kişisel verilerin korunması hakkı ise özel hayatın gizliliği hakkının özel bir biçimi

olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvencenin yaşama geçirilebilmesi için bu hakkı ilgilendiren yasal düzenlemelerin açık, anlaşılabilir ve kişilerin söz konusu haklarını kullanabilmelerine elverişli olması gerekir. Ancak böyle bir düzenleme ile kişilerin özel hayatlarını ilgilendiren veri ve bilgilerin resmî makamların keyfî müdahalelerine karşı korunması mümkün olabilir.

32. 6698 sayılı Kanun'un 5. maddesinde kişisel verilerin işleme şartları düzenlenmiştir. Buna göre kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. Maddenin dava konusu kuralın yer aldığı (2) numaralı fıkrasında belirtilen şartlardan birinin varlığı hâlinde ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür.

33. 6698 sayılı Kanun'un 3. maddesinde açık rıza "belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza" şeklinde tanımlanmıştır. Madde gerekçesinde açık rızanın 95/46/EC sayılı Avrupa Birliği Veri Koruma Direktifi (95/46/EC sayılı Direktif) dikkate alınarak tanımlandığı ifade edildikten sonra açık rızanın ilgili kişinin kendisiyle ilgili veri işlenmesine özgürce, konuyla ilgili yeterli bilgi sahibi olarak tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı şeklinde anlaşılması gerektiği ifade edilmiştir.

34. 95/46/EC sayılı Direktif'in 2. maddesinin (h) bendine göre "veri öznesinin rızası", "kendisine dair kişisel verilerin işlenmesi için veri öznesinin kabulüne işaret eden, özgürce ve bilgilendirilme yapıldıktan sonra alınan rızayı" ifade etmektedir. Avrupa Birliği tarafından 95/46/EC sayılı Direktif'in yerini almak üzere 2016 yılında kabul edilen ve 2018 yılında yürürlüğe girecek olan 2016/679 sayılı Genel Veri Koruma Yönetmeliği'nin 4. maddesinin (11) numaralı bendinde de veri sahibinin rızası "veri sahibinin bir beyan yoluyla ya da açık bir onay eylemiyle kendisine ait kişisel verilerin işlenmesine onay verdiğini gösteren özgür bir şekilde verilmiş spesifik, bilinçli ve açık gösterge" şeklinde tanımlanmaktadır.

35. 95/46/EC sayılı Direktif'in 7. maddesinin devamında açık rıza kuralının istisnaları düzenlenmiştir. Buna göre kişisel verilerin işlenmesi, bir sözleşme yapmadan önce veri öznesinin talebi üzerine önlem almak için ya da veri öznesinin taraf olduğu bir sözleşmenin yerine getirilmesi için gerekliyse veya işleme denetleyicinin konusu olan bir yasal yükümlülüğe uyum için gerekirse veya işleme, veri öznesinin hayati menfaatlerini korumak için gerekliyse veya işleme, verilerin açıklandığı üçüncü bir şahıs veya denetleyiciye yetki veren kamu makamının uygulamasında veya kamu menfaatine yapılan bir görevin yerine getirilmesi için gerekliyse veya işleme, bu tür menfaatlerin 1. maddenin (1) numaralı fıkrası kapsamında koruma gerektiren veri öznesinin temel hak ve özgürlükleriyle ilgili

menfaatleri çiğnemesi haricinde verilerin açıklandığı üçüncü şahıs veya şahıslar tarafından ya da denetleyici tarafından takip edilen meşru menfaatlerin amaçları için gerekliyse veri öznesinin açık rızası aranmayabilecektir.

36. Dava konusu kurallarla, ilgili kişinin açık rızası olmasa dahi kişisel verilerin işlenebileceği hâllerden bir kısmı düzenlenmektedir. Buna göre ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hâller “bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması”; “veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması”; “Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması” ile “ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması” şeklinde öngörülmüştür.

37. Dava konusu kuralların yer aldığı madde gerekçesinde, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenebileceği hâller örnekler verilmek suretiyle detaylı olarak açıklanmıştır.

38. Fıkranın (c) bendiyle ilgili olarak madde gerekçesinde bir sözleşmenin kurulması veya ifasıyla ilgili olarak kişisel veri işlenebileceği, örneğin yapılan bir sözleşme gereği paranın ödenmesi için alacaklı tarafın hesap numarasının alınabileceği, bir bankayla kredi sözleşmesi yapılması sırasında bankanın o kişiye ait maaş bordrosunu, tapu kayıtlarını, icra borcu olmadığına dair belgeyi edinmesinin bu kapsamda değerlendirileceği belirtilmiştir.

39. Fıkranın (ç) bendiyle ilgili olarak madde gerekçesinde veri sorumlusunun, hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olan verileri, ilgili kişinin rızası olmasa dahi işleyebileceği, örneğin bir şirketin çalışanına maaş ödeyebilmesi için banka hesap numarası, evli olup olmadığı, bakmakla yükümlü olduğu kişiler, eşinin çalışıp çalışmadığı, sosyal sigorta numarası gibi verileri işlenmesinin bu bendin verdiği yetkiye istinaden olacağı ifade edilmiştir.

40. Fıkranın (e) bendiyle ilgili olarak madde gerekçesinde bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması durumunda kişisel verilerin işlenebileceği, bu bağlamda bir şirketin kendi çalışanı tarafından açılan bir davada ispat için bazı verileri kullanmasının veya kısıtlı bir kişinin haklarının korunması amacıyla vasinin veya kayyımın, kısıtlının mali bilgilerini tutmasının hukuka uygun sayılacağı belirtilmiştir.

41. Fıkranın (f) bendiyle ilgili olarak madde gerekçesinde ise ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması durumunda da açık rıza şartı aranmaksızın kişisel verilerin işlenebileceği, örneğin bir şirket

sahibinin çalışanlarının temel hak ve özgürlüklerine zarar vermemek kaydıyla onların terfileri, maaş zamları yahut sosyal haklarının düzenlenmesinde ya da işletmenin yeniden yapılandırılması sürecinde görev ve rol dağıtımında esas alınmak üzere çalışanların kişisel verilerini işleyebileceği, burada işletmenin yeniden yapılandırılması ya da ehliyetli ve liyakatli çalışanların terfi almalarının veri sorumlusu statüsündeki şirket sahibinin “meşru menfaati” cümlesinden olduğu, kişisel verilerin korunmasına ilişkin temel ilkelere uyulması ve veri sorumlusu ile ilgili kişinin menfaat dengesinin gözetilmesi gerektiği açıklanmıştır.

42. Dava konusu kuralların, kişisel verilerin korunmasına yönelik bir sınırlandırma getirdiği açıktır. Dava konusu kurallarla ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu bir kısım hâller düzenlenmek suretiyle kişisel verilerin korunması hakkına müdahalede bulunulmuş ise de açık rıza olmaksızın işlenebilecek kişisel veriler, ilgilinin her türlü kişisel verisi olmayıp dava konusu kurallarda açıkça düzenlenen şartlardan birinin gerçekleşmesi durumu ile sınırlıdır. Bu bağlamda açık rıza kavramına getirilen istisnaların esas düzenleme hâline getirildiği veya açık rızaya gerek duyulmasını imkânsız hâle getirdiği söylenemez. Ayrıca dava konusu kuralların, kişisel verilerin işlenmesini, bir işlemin yapılması, bir hakkın tesisi, kullanılması veya korunması veya veri sorumlusunun meşru menfaatleri için gerekli veya zorunlu olması durumlarıyla sınırlı tuttuğu dikkate alındığında getirilen sınırlamaların kişisel verilerin korunması hakkının kullanılmasını son derece zorlaştıran veya onu kullanılamaz duruma düşüren kayıtlara bağlamadığı da açıktır. Bir başka deyişle dava konusu kurallar, maddede belirtilen konularda gereklilik veya zorunluluk hâllerinde ortaya çıkacak bir ihtiyacın karşılanmasını sağlamaya yönelik olup hakkın özüne dokunmamaktadır. Bu nedenle değerlendirilmesi gereken hususlar söz konusu sınırlamanın demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine uygun olup olmadığıdır.

43. Kanun koyucunun kurallarla zorunlu ve gerekli olan hâllerle sınırlı olarak belirtilen konularda ilgili kişinin açık rızası olmaksızın kişisel verilerinin işlenebilmesine olanak sağlamak suretiyle toplumsal yaşamda belirtilen konularda ortaya çıkabilecek gecikme, aksaklık veya düzensizlikler ile hak ve menfaat kayıplarının engellenmesini sağlamayı amaçladığı anlaşılmaktadır. Kurallarla söz konusu verileri işleme yetkisinin amacı ve faaliyet alanı belirlenmiş ve bu şekilde kamu yararı ile özel hayatın gizliliği ve kişisel verilerin korunması hakları arasında adil bir denge kurulmuştur. Ayrıca kurallarla belirtilen konularda söz konusu kişisel verilerin işlenmesi durumunda ise 6698 sayılı Kanun’dan kaynaklanan kişisel verilerin işlenmesine ilişkin tüm ilke, yükümlülük ve sorumluluklara ilişkin düzenlemeler geçerliliğini korumaktadır. Bu durumda kişisel verilerin işlenmesinde 6698 sayılı Kanun’da yer alan kişisel verilerin korunmasıyla ilgili olarak kişisel verilerin işlenmesinde

uyulması zorunlu kurallar, kişisel verilerin işleme şartları, veri sorumlusunun aydınlatma yükümlülüğü, veri güvenliğine ilişkin yükümlülükler ile veri sorumlusuna başvuru ve Kurula şikâyete ilişkin hükümler uygulanacaktır.

44. Öte yandan 6698 sayılı Kanun'un 17. maddesinde kişisel verilere ilişkin suçlar bakımından 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140. maddeleri hükümlerinin uygulanacağı ve Kanun'un 7. maddesi hükmüne aykırı olarak kişisel verileri silmeyen veya anonim hâle getirmeyenlerin 5237 sayılı Kanun'un 138. maddesine göre cezalandırılacağı hükme bağlanmıştır. 5237 sayılı Kanun'un 136. maddesi uyarınca da kişisel verileri hukuka aykırı olarak başkasına vermek, yaymak veya ele geçirmek suç olarak düzenlenmiştir. Dolayısıyla dava konusu kural kapsamında elde edilecek bilgilerin amacı dışında kullanılmasını önleyecek ve kişilerin özel hayatına dair bilgilerin ve kişisel verilerin ifşa edilmesini önleyecek yasal güvencenin sağlandığı görülmektedir.

45. Bu bağlamda Kanun'da sınırlama aracının sınırlama amacına uygun ve orantılı şekilde kullanılmasını sağlayacak yasal güvencelere yer verildiği ve yeterli korumanın sağlandığı da dikkate alındığında dava konusu kurallarla getirilen sınırlamaların özel hayatın gizliliği ve kişisel verilerin korunması hakkının özünü zedelediği gibi amaç ile araç arasında makul denge kurduğu da açıktır. Dolayısıyla anılan kurallar, demokratik toplum düzeninin gereklerine aykırılık teşkil etmediği gibi özel hayatın gizliliği ve kişisel verilerin korunması hakkına ölçsüz bir müdahale de teşkil etmemektedir.

46. Anayasa'nın 20. maddesi, kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvenceyi kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği şeklinde belirtmiştir. Dolayısıyla bu hakkı ilgilendiren yasal düzenlemelerin çerçevesi çizilmiş; açık, anlaşılabilir, kişilerin söz konusu haklarını kullanabilmelerine elverişli ve özel hayatlarını ilgilendiren veri, bilgi ve belgelerin resmî makamların keyfî müdahalelerine karşı korunmasını mümkün hâle getirmesi gerekmektedir. Bu bağlamda dava konusu kurallar madde gerekçeleriyle birlikte değerlendirildiğinde ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu hâllerin kapsam, amaç ve sınırlarının Kanun'da açıkça yer alması karşısında kuralların belirsiz olduğu söylenemez.

47. Ayrıca dava dilekçesinde "meşru menfaat" kavramının belirsiz olduğu ifade edilmiştir. Ancak bu kavramın çalışanların temel hak ve özgürlüklerine zarar vermemek kaydıyla gerekçede ifade edilen temel ilkelere uyulması ve veri sorumlusu ile ilgili kişinin menfaat dengesinin gözetilmesi

çerçevesinde değerlendirilmesi gereken bir kavram olarak anlaşılması gerektiği dikkate alındığında belirsiz olduğu söylenemez.

48. Açıklanan nedenlerle kurallar Anayasa'nın 2., 13. ve 20. maddelerine aykırı değildir. İptal taleplerinin reddi gerekir.

49. Kuralların Anayasa'nın 90. maddesiyle ilgisi görülmemiştir.

C. Kanun'un 6. Maddesinin (1) Numaralı Fıkrasında Yer Alan "...mezhebi...", "...kılık ve kıyafeti,..." İbareleri ile (3) Numaralı Fıkrasının İncelenmesi

1. "...mezhebi..." ve "...kılık ve kıyafeti,..." İbarelerinin İncelenmesi

a. İptal Taleplerinin Gerekçesi

50. Dava dilekçesinde özetle, dava konusu "mezhebi" ile "kılık ve kıyafeti" ibarelerinin, Anayasa Mahkemesi kararları, 108 sayılı Sözleşme, Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) tarafından yayımlanan Kişisel Verilerin Korunması Rehber İlkeler ile 95/46/EC sayılı Direktif'te tanımlanan kişisel veri kavramlarıyla uyumlu olmadığı, uluslararası insan hakları hukuku ile bağdaşmayacak nitelikte olduğu, mezhep, kılık ve kıyafete ilişkin verilerin toplanmasının Her Türlü Irk Ayrımcılığının Tasfiye Edilmesine Dair Uluslararası Sözleşme'de sağlanan güvencelere aykırı olduğu, kanun koyucunun takdir yetkisinin aşıldığı ve yerleşik fişleme tarihi tartışmalarının olduğu ülkemizde bireyler bakımından güvence değil risk oluşturduğu, toplumsal cinsiyet ayrımcılığına neden olacak nitelikte olduğundan eşitlik ilkesine aykırılık teşkil ettiği, kişinin sahip olduğu din ve vicdan özgürlüğü ile düşünce ve ifade özgürlüğünü ihlal ettiği belirtilerek dava konusu ibarelerin Anayasa'nın 2., 10., 20., 24., 25. ve 90. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

51. Dava konusu ibarelerin yer aldığı fıkrada özel nitelikli kişisel veriler düzenlenmiştir. Fıkrada kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerin özel nitelikli kişisel veri olduğu belirtilmektedir. Fıkrada yer alan "...mezhebi..." ve "...kılık ve kıyafeti..." ibareleri dava konusu kuralları oluşturmaktadır.

52. Anayasa'nın 2. maddesinde hukuk devleti ilkesi, 20. maddesinde ise kişisel verilerin korunması hakkı düzenlenmiştir.

53. Dava konusu kuralla, kişilerin mezhebine, kılık ve kıyafetine ilişkin verileri özel nitelikli kişisel veriler olarak kabul edilmektedir. Mezhep bir dinin görüş, yorum ve anlayış farklılıkları sebebiyle ortaya çıkan kollarından her biri; kılık ve kıyafet ise bir kimsenin giyinişi, dış görünüşü, üst başı, giysisi şeklinde ifade edilmektedir.

54. 6698 sayılı Kanun'un 6. maddesinin (2) numaralı fıkrası gereğince özel nitelikli kişisel verilerin kural olarak ilgilinin açık rızası olmaksızın işlenmesi yasaktır. Bu kuralın istisnaları ise maddenin (3) numaralı fıkrasında düzenlenmiştir. Maddenin (4) numaralı fıkrasına göre ise özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kişisel Verileri Koruma Kurulu tarafından belirlenen yeterli önlemlerin alınması şarttır.

55. Dava konusu kuralların yer aldığı maddenin gerekçesinde bazı kişisel verilerin başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olmasına veya ayrımcılığa maruz kalmasına neden olabileceğinden bu tür verilerin özel nitelikli (hassas) veri olarak kabul edildiği ifade edilmiştir. Bu bağlamda kişilerin dinî görüş, yorum ve anlayış farklılıklarını ortaya koyan verileri ile dinî inancıyla bağlantılı kılık ve kıyafetine ilişkin verilerin özel nitelikli kişisel veriler olduğu kuşkusuzdur.

56. Nitekim 108 sayılı Sözleşme'nin 6. maddesi ile 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Yönetmeliği'nin 9. maddesinde "dini veya diğer inançları ortaya koyan kişisel nitelikteki veriler" özel veri kategorileri arasında belirtilmiştir.

57. Kanun koyucunun dava konusu kurallarla, kişilerin mezhebi ile kılık ve kıyafetiyle ilgili verileri daha özel bir korumaya tabi olması gereken verilerden kabul etmek suretiyle bu tür verileri diğer verilerden ayırdığı ve işlenmesini daha özel koşullara bağladığı anlaşılmaktadır. Dolayısıyla dava konusu kuralların amacının bu verilerin toplanmasına yasal dayanak sağlamak değil kişisel veri olduğunda şüphe olmayan bu verileri özel koruma altına almaya yönelik olduğu açıktır. Bu bağlamda kişilerin mezhebi ve kılık ve kıyafetiyle ilgili verileri daha özel bir koruma altına almak kanun koyucunun takdir yetkisi kapsamında olup kuralların Anayasa'ya aykırı bir yönü bulunmamaktadır.

58. Öte yandan kişilerin ayrımcılığa uğramasına neden olabilecek alanlarda bilgilerin toplanmasının, farklı grupların özel ihtiyaçlarının tespit edilmesi ve ayrımcılıkla mücadelede oluşan boşluk ve eksikliklerin tespit edilmesi ve giderilmesi bakımından önemli olduğu da bir gerçektir. Bu kapsamda hak sahiplerine yönelik politika ve hizmet geliştirmek için bazı verilerin toplanması gerekli olabilir. Bu durumlarda mezhep ve kılık kıyafet ile ilgili verilerin işlenmesine olanak sağlayacak kanunların amaç, kapsam ve sınırlarının Anayasa'da güvence altına alınan din ve vicdan özgürlüğü, düşünce ve ifade özgürlüğü ve kişisel verilerin korunmasına ilişkin hükümlerde düzenlenen hakların özüne

dokunmaması gerekir. Bu husus ise özellikle kanun koyucunun kişilerin mezhebi ve kılık ve kıyafet ile ilgili verilerin işlenmesine kişilerin açık rızası olmaksızın imkân verdiği yasal düzenlemeler yapılırken göz önüne alınmalıdır. Bu bağlamda her ne kadar dava dilekçesinde dava konusu kuralların söz konusu özgürlükleri ihlal ettiği ifade edilmişse de kanun koyucunun salt kişilerin mezhebi ve kılık ve kıyafeti ile ilgili kişisel verileri özel nitelikli kişisel veri kabul etmek suretiyle daha özel bir koruma altına almayı amaçladığı dikkate alındığında dava konusu kuralın bu hak veya özgürlükleri ve dolayısıyla Anayasa'yı ihlal ettiği söylenemez.

59. Açıklanan nedenlerle kural Anayasa'nın 2. ve 20. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

60. Serdar ÖZGÜLDÜR, Serruh KALELİ ile Osman Alifeyyaz PAKSÜT bu görüşe katılmamışlardır.

61. Kuralın Anayasa'nın 10., 24., 25. ve 90. maddeleriyle ilgisi görülmemiştir.

2. (3) Numaralı Fıkranın İncelenmesi

a. İptal Talebinin Gerekçesi

62. Dava dilekçesinde özetle, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla kişilerin cinsel hayatlarına ve sağlığına ilişkin verilerin açık rıza olmaksızın işlenebilmesinin kabul edilemez olduğu, özellikle cinsel hayatın bireyin özel yaşamının en mahrem yönünü oluşturduğu, kişilerin cinsel hayatlarına ve sağlığına ilişkin verilerin toplanmasında hiçbir ayırt edici ölçütün bulunmadığı, kuralın kişilerin sağlık hakkına erişimden çeşitli endişelerle kaçınmalarına neden olabileceği ve bu durumun aynı zamanda kişilerin yaşam hakkına, maddi ve manevi varlıklarını geliştirmesine de müdahale anlamına geldiği, sağlıkla ilgili kişisel verilerin neredeyse hiçbir sınırlamaya tabi tutulmadan toplanması, işlenmesi ve aktarılmasının insan haklarına saygılı bir devlet olma yükümlülüğü ile bağdaşmadığı, yeterli tedbirlerin niteliğine ve kapsamına yer vermeyerek etkin korumanın sağlanmadığı ve belirsizliğe neden olduğu, demokratik bir toplumda kişilerin özel hayatının gizliliği hakkını bütünüyle ortadan kaldıracak bir müdahale niteliğinde olan kuralın kişilerin sağlıkları ile ilgili bilgilerin korunmasına yönelik uluslararası normlara aykırı olduğu, verileri işleyecek yetkili kurum ve kuruluşlar ibaresinin geniş bir kapsama sahip olduğu belirtilerek kuralın Anayasa'nın 2., 10., 17., 20., 24., 25., 56. ve 90. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

63. 6216 sayılı Kanun'un 43. maddesi uyarınca kural ilgisi nedeniyle Anayasa'nın 5. ve 13. maddeleri yönünden de incelenmiştir.

64. Dava konusu kuralın yer aldığı maddede özel nitelikli kişisel veriler sayılarak bu verilerin ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğu belirtilmiştir. Dava konusu kural ise birinci fıkrada sayılan cinsel hayat ve sağlık dışındaki kişisel verilerin kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebileceği, cinsel hayata ve sağlığa ilişkin kişisel verilerin ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği öngörülmektedir.

65. Anayasa'nın 2. maddesinde belirtilen sosyal hukuk devleti; insan hak ve hürriyetlerine saygı gösteren, kişilerin huzur, refah ve mutluluk içinde yaşamalarını güvence altına alan, kişi ile toplum arasında denge kuran, güçsüzleri güçlüler karşısında koruyarak sosyal adaleti gerçekleştiren, bu bağlamda sağlık hizmetlerinden bireylerin yeteri kadar yararlanmasını sağlayan devlettir. Devlet, herkesin sağlık hizmetlerinden yararlanması için gerekli tedbirleri almalı; kişilerin sağlık hizmetlerinden yararlanmasını sağlamalıdır. Devletin bu alandaki görevlerini yerine getirirken uygulayacağı sınırlamalar, Anayasa'nın 13. maddesinin öngördüğü üzere Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olmamalıdır.

66. Anayasa'nın 17. maddesinde "Herkes, yaşama, maddî ve manevî varlığını koruma ve geliştirme hakkına sahiptir." denilmektedir. Kişinin yaşama hakkı ile maddi ve manevi varlığını koruma hakkı; birbirleriyle sıkı bağlantıları olan, devredilmez ve vazgeçilmez haklarından biridir.

67. Anayasa'nın 56. maddesinin birinci fıkrasında herkesin sağlıklı ve dengeli bir çevrede yaşam hakkına sahip olduğu hüküm altına alınmış, üçüncü fıkrasında ise devlete herkesin hayatını, beden ve ruh sağlığı içinde sürdürmesini sağlamak amacıyla sağlık kuruluşlarını tek elden planlayıp hizmet vermesini düzenlemek ödevi verilmiştir. Sağlık hakkı, insanların sağlıklarının korunması, hastalandıklarında iyileşmeleri, tıbbi bakım görebilmeleri ve tedavi edilebilmeleri için devletin sağladığı her türlü imkândan yararlanma hakkıdır. Sağlık hakkı, insanların doğuştan kazandıkları vazgeçilemez ve devredilemez haklardan biridir. Yine devlet, kişilerin yaşam hakkını güvence altına almakla yükümlüdür. Aynı maddede "Herkes, yaşama, maddî ve manevî varlığını koruma ve geliştirme hakkına sahiptir." denilmektedir.

68. Anayasa'nın 5. maddesi de insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamayı devletin temel amaç ve görevleri arasında saymıştır. Devlet, kişilerin sağlık hakkından tam anlamıyla yararlanabilmeleri ve sağlıklı bir yaşam sürdürebilmeleri amacıyla yasal, idari, mali,

yargısal ve diğere önlemleri almak zorundadır. Bu nedenle Anayasa, kişiler için bir hak olan sağlık hizmetinin yerine getirilmesinde sosyal hukuk devleti olmanın gereğı olarak devlete pozitif yükümlülük getirmektedir.

69. Anayasa, sosyal hukuk devleti olmanın gereğı olarak sağlık hizmetlerinin sunumunda yüklediğı pozitif yükümlülük kapsamında devleti, bu haklardan yararlanmayı artıracak önlemleri almakla mükellef kılmıştır. Bu nedenle Anayasa'nın 17. ve 56. maddelerinde öngörülen kişilerin yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkı ile sağlık hakkından yararlanma konusunda en geniş ölçekli uygulamaların gerçekleştirilmesi gerekir. Zira sağlık hizmeti doğrudan yaşama hakkı ile ilgili olması nedeniyle diğere kamu hizmetlerinden farklı olup bu hizmetin temel hedefi olan insan sağlığı ve yaşamı, mahiyeti itibarıyla ertelenemez ve ikame edilemez bir özelliğe sahiptir. Kişiler için bir hak olan bu hizmetten yararlanmayı kolaylaştırıcı düzenlemeler yapılması ve bu hizmetin daha iyi bir şekilde gerçekleştirilmesi için gerekli tedbirlerin alınması devletin Anayasa'dan kaynaklanan bir ödevidir. Dolayısıyla Anayasa'da devlete verilen görevlerin gereğı olarak kişilerin sağlıklı bir şekilde yaşam sürdürmeleri için genel sağlığın korunması amacıyla düzenlenen dava konusu kurallar demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır.

70. Anayasa'nın 20. maddesinin birinci fıkrasında "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz." denilerek özel hayatın gizliliğı güvence altına alınmıştır. Maddenin üçüncü fıkrasında ise herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı ifade edilmiştir. Maddede ayrıca kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceğı ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceğı belirtilmiştir. Kişisel verilerin korunması hakkı, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Ancak bu hak sınırsız olmayıp düzenlendiğı maddede özel sınırlama nedeni öngörülmemiş özgürlüklerin de o özgürlüğün doğasından kaynaklanan bazı sınırlarının bulunduğu, ayrıca Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile Devlete yüklenen ödevlerin özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebileceğı kabul edilmektedir.

71. Ancak bu sınırlama yapılırken temel hak ve özgürlüklerin sınırlandırılması rejimini belirleyen Anayasa'nın 13. maddesine de uyulması gerekmektedir. Anayasa'nın 13. maddesi uyarınca, temel hak ve özgürlüklere yapılacak müdahaleler, demokratik toplum düzeninin gereklerine ve ölçülülük

ilkesine aykırı olamaz. Ölçülülük ilkesi, yasal sınırlamanın öngörülen amaç için zorunlu ve amaca ulaşmaya elverişli olmasını, ayrıca amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder.

72. 108 sayılı Sözleşme'nin 9. maddesinde de bazı durumlarda kişisel verilerin korunmasına sınırlamalar getirilebilmesi öngörülmüştür. Ayrıca 95/46/EC sayılı Direktif'in 8. maddesinin (1) numaralı fıkrasında beş kategoride yer alan özel nitelikli kişisel verilerin işlenmesi kural olarak yasaklanmış ancak maddenin (2) numaralı fıkrasında bunun istisnaları düzenlenerek veri işlemenin önleyici hekimlik, tıbbi teşhis, tıbbi yardım veya bakım veya sağlık hizmetlerinin idarî olarak yürütülmesi için gerekli olması ve bu verilerin ya sağlık personeli veya sağlık personeli gibi sır saklamaya tabi kişiler tarafından işlenmesinin mümkün olduğu ifade edilmiştir. Maddede ayrıca bu istisnaların yanında üye devletlerin uygun önlemleri almak koşuluyla kamu yararı için başka bazı istisnalar da belirleyebileceği belirtilmiştir.

73. Dava konusu kuralın ilk cümlesinde, cinsel hayat ve sağlık dışındaki özel nitelikli kişisel verilerin kanunlarda öngörülen hâllerde kişilerin açık rızası olmaksızın da işlenebileceği belirtilmiştir. Bunlar ise kanun koyucunun takdir yetkisi kapsamında Kanun'un 6. maddesinin (1) numaralı fıkrasında kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri olarak ifade edilmiştir. Anayasa'nın 20. maddesinde de belirtildiği üzere kişisel veriler ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir. Dolayısıyla kişisel verilerin işlenmesine kanunda açıkça imkân tanınan durumlarda kişinin açık rızasına ayrıca ihtiyaç bulunmamaktadır. Bu yönüyle kural Anayasa hükmünün tekrarı niteliğinde olup söz konusu kişisel verilerin, ilgilinin açık rızası olmaksızın işlenebileceği halleri doğrudan düzenlememekte, "kanunlarda öngörülen hâllere" atıfta bulunmaktadır. Kişisel verilerin ilgili kişilerin açık rızası olmaksızın işlenebileceği halleri düzenleyen kanunların iptalleri talebiyle Anayasa Mahkemesine başvurulması durumunda ise söz konusu düzenlemelerin Anayasa'ya aykırı olup olmadıklarının inceleneceği ve bu kapsamda Anayasa'nın 13. maddesi hükmünün de gözetileceği tabiidir. Bu nedenle, Anayasanın 20. maddesinde yer alan düzenlemeye uygun olarak kişisel verilerin "kanunlarda öngörülen hâllerde" ilgili kişinin açık rızasının aranmaksızın işlenebileceğinin belirtildiği kuralda Anayasa'ya aykırılık bulunmamaktadır.

74. Dava konusu kuralın ikinci cümlesinde ise sağlık ve cinsel hayata ilişkin kişisel verilerin kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla sır saklama yükümlülüğü

altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği belirtilmektedir. Dava konusu kuralla kişisel verilerin korunması hakkı, Anayasa'nın 17. ve 56. maddelerinden kaynaklanan sebeplerle ve maddede sayma yöntemiyle belirtilen amaçlarla sınırlandırıldığı anlaşılmaktadır.

75. Cinsel hayata ve sağlığa ilişkin kişisel verilerin işlenmesi bakımından kural ilgilinin açık rızasının bulunmasıdır. Dava konusu kuralla bu kişisel verilerin ilgilinin açık rızası olmaksızın işlenebileceği hâller belirtilmek suretiyle bu kurala istisna getirilmiştir. Özel nitelikli kişisel veri olduğunda kuşku olmayan sağlık ve cinsel hayata ilişkin verilerin söz konusu durumlarda ilgilinin açık rızası aranmaksızın işlenebileceğini düzenleyen kuralla özel hayatın gizliliği ve kişisel verilerin korunması haklarına bir müdahale söz konusu ise de kuralla kişisel verilerin işlenmesinin amaç bakımından sınırlandırıldığı dikkate alındığında, getirilen sınırlamanın mezkûr hakların kullanılmasını son derece zorlaştıran veya onu kullanılamaz duruma düşüren kayıtlara bağlandığı söylenemeyeceğinden hakkın özüne dokunmadığı açıktır. Bu nedenle değerlendirilmesi gereken husus, bu müdahalenin demokratik toplum düzeninin gerekleri ile ölçülülük ilkesine uygun olup olmadığıdır.

76. Kanun koyucunun dava konusu kuralla, halk sağlığının korunması ve geliştirilmesi, hastalık risklerinin azaltılması ve önlenmesi suretiyle kamu sağlığının korunmasını; sağlık hizmetleri ile bu hizmetlerin finansmanının planlanması ve yönetimi suretiyle teşhis, tedavi ve rehabilite edici sağlık hizmetlerinin yürütülmesi, eğitim ve araştırma faaliyetlerinin geliştirilmesi, insan gücü ve maddi kaynaklarda tasarruf sağlanması ve verimin artırılmasını amaçladığı anlaşılmaktadır. Dolayısıyla Anayasa'da devlete verilen görevlerin gereği olarak kişilerin sağlıklı bir şekilde yaşam sürdürmeleri için genel sağlığın korunması amacıyla düzenlenen dava konusu kural demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır.

77. Öte yandan ilgilinin kişisel verilerinin açık rızası olmaksızın kamu yararı amacıyla işlenebileceği hâllerin kapsam, amaç ve sınırların kanunda açıkça yer alması ve maddenin (4) numaralı fıkrasında belirtildiği gibi özel nitelikli kişisel verilerin işlenmesinde ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınacağı dikkate alındığında dava konusu kuralın belirsiz olduğu da söylenemez.

78. Ayrıca dava konusu kuralda belirtilen sebeplerle kişisel verilerin işlenmesi ancak sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından yapılabilecektir. Sır saklama yükümlülüğü altında olan kişiler ise avukat, hekim veya mali müşavir gibi kendi kanunlarında görevleri dolayısıyla edindikleri bilgileri zamanla sınırlı olmaksızın açığa vurmaları yasak olan ve bu yasağın ihlali hâlinde hukuki ve cezai sorumluluğu olan kişilerdir.

79. 6698 sayılı Kanun'da kişisel verilerin işlenmesinde uyulması zorunlu ilke ve kurallar, kişisel verilerin işlenme şartları, veri sorumlusunun aydınlatma yükümlülüğü, veri güvenliğine ilişkin yükümlülükler ile veri sorumlusuna başvuru ve Kurula şikâyete ilişkin ayrıntılı düzenlemeler yapılmıştır. Kanun'un 17. maddesinde ise kişisel verilere ilişkin suçlar bakımından 5237 sayılı Kanun'un 135 ila 140. maddeleri hükümlerinin uygulanacağı ve Kanun'un 7. maddesi hükmüne aykırı olarak kişisel verileri silmeyen veya anonim hâle getirmeyenlerin 5237 sayılı Kanun'un 138. maddesine göre cezalandırılacağı hükme bağlanmıştır. 5237 sayılı Kanun'un 136. maddesi uyarınca da kişisel verileri hukuka aykırı olarak başkasına vermek, yaymak veya ele geçirmek suç olarak düzenlenmiştir.

80. 6698 sayılı Kanun, 5237 sayılı Kanun ve ilgili diğer kanunlarda yer alan düzenlemeler birlikte değerlendirildiğinde dava konusu kural kapsamında işlenecek verilerin amacı dışında kullanılmasını ve kişilerin özel hayatına dair bilgilerin ve kişisel verilerin ifşa edilmesini önleyecek yasal güvencenin sağlandığı görülmektedir. Bu bağlamda dava konusu kuralda kişisel verilerin korunması hakkına sınırlama yapılırken Kanun'da sınırlama aracının sınırlama amacına uygun ve orantılı şekilde kullanılmasını sağlayacak yasal güvencelere de yer verildiği, böylece hem özel hayatın gizliliği ve kişisel verilerin korunması haklarının özünün zedelenmesinin önlenmesi hem de bu haklar ile toplum sağlığının korunmasına yönelik önlemler arasındaki makul dengenin kurulduğu görülmektedir. Dolayısıyla dava konusu kuralla kişisel verilerin korunmasını isteme hakkının özüne dokunan ya da bu hakkı ölçüsüz şekilde sınırlandıran bir husus bulunmadığı gibi kuralın demokratik toplum düzeninin gereklerine aykırılık teşkil ettiği de söylenemez.

81. Açıklanan nedenlerle kurallar 2., 5., 13., 17., 20. ve 56. maddelerine aykırı değildir. İptal taleplerinin reddi gerekir.

82. Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ ile Osman Alifeyyaz PAKSÜT bu görüşe katılmamışlardır.

83. Kuralların Anayasa'nın 10., 24., 25. ve 90. maddeleriyle ilgisi görülmemiştir.

D. Kanun'un 7. Maddesinin (2) Numaralı Fıkrasının İncelenmesi

1. İptal Talebinin Gerekçesi

84. Dava dilekçesinde özetle, 6698 sayılı Kanun'un kişisel veriler alanına ilişkin genel kanun niteliğinde olduğu, kişisel verilerinin silinmesi, yok edilmesi veya anonim hâle gelmesi hakkında bu Kanun hükümlerinin esas alınması gerektiği, bu hususlara ilişkin diğer kanunlarda yer alan hükümleri saklı tutan dava konusu kuralın çok geniş kapsamlı olduğu, bireylerin hangi kişisel

verilerinin hangi kanunda hangi düzenleme ile silineceği veya ne kadar sürede silineceğini bilemeyeceği, kişisel verilerin yok edilme ve anonim hâle getirilmesi şartlarının belirsiz olduğu, kamu yararı ve ölçülülük ilkesinin gözetilmediği belirtilerek kuralın Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

85. Dava konusu kuralın yer aldığı maddede kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi düzenlenmiştir. Maddede, Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silineceği, yok edileceği veya anonim hâle getirileceği hükme bağlanmaktadır. Dava konusu kuralda ise kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu belirtilmektedir.

86. Hukuk devleti ilkesinin gereği olarak kanunlar kamu yararı amacını gerçekleştirmek üzere çıkarılmalıdır. Anayasa Mahkemesi kararlarında ifade edildiği gibi kamu yararı düşüncesi olmaksızın yalnız özel çıkarlar için veya yalnız belli kişilerin yararına olarak kanun hükmü konulamaz. Böyle bir durumun açık bir biçimde ve kesin olarak saptanması hâlinde söz konusu kanun hükmü Anayasa'nın 2. maddesine aykırı düşer. Açıklanan ayırık hâl dışında bir kanun hükmünün ülke gereksinimlerine uygun olup olmadığı ve hangi araç ve yöntemlerle kamu yararının sağlanabileceği bir siyasi tercih sorunu olarak kanun koyucunun takdirinde olduğundan bu kapsamda kamu yararı değerlendirmesi yapmak anayasa yargısıyla bağdaşmaz.

87. Kanun koyucu, takdir yetkisi içerisindeki düzenlemeleri yaparken hukuk devleti ilkesinin bir gereği olan ölçülülük ilkesiyle de bağlıdır. Bu ilke ise "elverişlilik", "gereklilik" ve "orantılılık" olmak üzere üç alt ilkeden oluşmaktadır. "Elverişlilik" getirilen kuralın ulaşılmak istenen amaç için elverişli olmasını, "gereklilik" getirilen kuralın ulaşılmak istenen amaç bakımından gerekli olmasını, "orantılılık" ise getirilen kural ile ulaşılmak istenen amaç arasında olması gereken ölçüyü ifade etmektedir. Bir kuralda öngörülen düzenleme ile ulaşılmak istenen amaç arasında da "ölçülülük ilkesi" gereğince makul bir dengenin bulunması zorunludur.

88. Dava konusu kuralla maddenin gerekçesinde de ifade edildiği gibi kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda hüküm bulunması hâlinde bunların öncelikle uygulanması amaçlanmaktadır.

89. Genel kanun niteliğindeki 6698 sayılı Kanun'da kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin her durumun öngörülmesi ve düzenlenmesi mümkün olmayacağı gibi daha sonra ortaya çıkabilecek özel durumlara ilişkin hususların özel kanunlarda daha detaylı düzenlenmesi de gerekebilir. Bu durumda aynı konuyla ilgili olarak genel kanunda ve özel kanunda hüküm bulunması hâlinde özel kanun hükmü uygulanacağından kuralın belirsiz olduğu söylenemez. Ayrıca dava konusu kuralın bazı özel durumlara ilişkin hususların daha ayrıntılı şekilde düzenlenmesini sağlamaya yönelik kamu yararı amacıyla düzenlendiği açıktır. Dava konusu kuralın ulaşılmak istenen amaç için elverişli ve gerekli olduğu, amaç ve araç arasında makul ve uygun bir ilişki kurduğu ve orantılı olduğu anlaşıldığından kuralda ölçülülük ilkesine aykırı bir yön de bulunmamaktadır.

90. Öte yandan özel hayatın gizliliği ve kişisel verilerin korunmasını isteme hakkı Anayasa'nın 20. maddesinde güvence altına alınmıştır. Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin kanun koyucu tarafından özel kanunlarda yapılacak diğer düzenlemelerin de kişisel verilerin korunmasını düzenleyen Anayasa'nın 20. maddesine aykırı olmaması gerektiği hususunda şüphe yoktur. Bu bağlamda diğer kanunlarda yer alacak hükümlerin bireylerin kişisel verilerinin ne kadar sürede ve ne şekilde silineceği, bu verilerin yok edilme ve anonim hâle getirilmesi şartlarını ölçülülük ve belirlilik ilkesi çerçevesinde kamu yararını gözeterek düzenlenmesi gerektiği açıktır. Dolayısıyla Anayasa'nın 20. maddesinde düzenlenen ilke ve esaslara aykırı olmayacak şekilde kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanun hükümlerini saklı tutan dava konusu kuralın Anayasa'ya aykırı bir yönü bulunmamaktadır.

91. Açıklanan nedenlerle kural Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

E. Kanun'un 8. Maddesinin (3) Numaralı Fıkrasının İncelenmesi

1. İptal Talebinin Gerekçesi

92. Dava dilekçesinde özetle 6698 sayılı Kanun'un kişisel veriler alanına ilişkin genel kanun niteliğinde olduğu, kişisel verilerin aktarılması hakkında bu Kanun hükümlerinin esas olması gerektiği, dolayısıyla bu hususa ilişkin diğer kanunlarda yer alan hükümleri saklı tutan dava konusu kuralın, bireylerin hangi kişisel verilerinin hangi kanundaki hangi düzenleme ile aktarıldığını bilmesini imkânsız kıldığı ve bireyler bakımından belirsizlik yarattığı, kamu yararı ve ölçülülük ilkesini gözetmediği belirtilerek kuralın Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

93. Dava konusu kuralın yer aldığı maddede kişisel verilerin aktarılması düzenlenmiştir. Buna göre kişisel veriler, kural olarak ilgili kişinin açık rızası olmaksızın aktarılamaz. Ancak kişisel verilerin 5. maddenin ikinci fıkrasında ve yeterli önlemler alınmak kaydıyla 6. maddenin üçüncü fıkrasında belirtilen şartlardan birinin bulunması hâlinde ilgili kişinin açık rızası aranmaksızın aktarılması mümkündür. Dava konusu kuralla ise kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu belirtilmektedir.

94. Kanun'un 7. maddesinin (2) numaralı fıkrasının incelendiği bölümde kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümlerin saklı olması hakkında kuralın Anayasa'ya uygunluk denetimi kapsamında belirtilen gerekçeler dava konusu kural bakımından da geçerli bulunduğundan aynı gerekçelerle dava konusu kural da Anayasa'nın 2. maddesine aykırı değildir.

95. Açıklanan nedenle kural Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

F. Kanun'un 9. Maddesinin (6) Numaralı Fıkrasının İncelenmesi

1. İptal Talebinin Gerekçesi

96. Dava dilekçesinde özetle 6698 sayılı Kanun'un kişisel veriler alanına ilişkin genel kanun niteliğinde olduğu, kişisel verilerin yurt dışına aktarılması hakkında bu Kanun hükümlerinin esas olması gerektiği, dolayısıyla bu hususa ilişkin diğer kanunlarda yer alan hükümleri saklı tutan dava konusu kuralın bireylerin hangi kişisel verilerinin hangi kanundaki hangi düzenleme ile yurt dışına aktarıldığını bilmesini imkânsız kıldığı ve bireyler bakımından belirsizlik yarattığı, kamu yararı ve ölçülülük ilkesini gözetmediği belirtilerek kuralın Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

97. Dava konusu kuralın yer aldığı maddede kişisel verilerin yurt dışına aktarılması düzenlenmiştir. Buna göre kişisel veriler, kural olarak ilgili kişinin açık rızası olmaksızın aktarılamaz. Ancak kişisel verilerin 5. maddenin ikinci fıkrası ile 6. maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede yeterli korumanın bulunması hâlinde, yeterli korumanın bulunmaması durumunda ise Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılmasının mümkün olduğu hükme bağlanmakta, dava konusu kuralla ise kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu belirtilmektedir.

98. Kanun'un 7. maddesinin (2) numaralı fıkrasının incelendiği bölümde kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümlerin saklı olması hakkında kuralın Anayasa'ya uygunluk denetimi kapsamında belirtilen gerekçeler dava konusu kural bakımından da geçerli bulunduğundan aynı gerekçelerle dava konusu kural da Anayasa'nın 2. maddesine aykırı değildir.

99. Açıklanan nedenle kural Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

G. Kanun'un 13. Maddesinin (2) Numaralı Fıkrasının İkinci Cümlesinin İncelenmesi

1. İptal Talebinin Gerekçesi

100. Dava dilekçesinde özetle, hakkında işlenen verilerinin ne olduğunu öğrenebilmesi için kişiden ücret talep edilmesinin, bireyin temel haklarından olan özel hayatın gizliliği hakkından etkin olarak yararlanmasını engellediği, bu hakkı sosyal hukuk devleti ve adalet ilkeleriyle bağdaşmayacak surette sınırlandırdığı, sınırlandırmanın hakkın özüne dokunduğu ve demokratik toplum düzeninin gereklerine aykırı olduğu, yürütmenin şekillendirdiği Kurul tarafından ücretin belirlenmesinin hukuki güvenlik ve belirlilik ilkelerine ve 108 sayılı Sözleşme'deki güvencelere aykırı olduğu belirtilerek kuralın Anayasa'nın 2., 5., 13., 20. ve 90. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

101. Dava konusu kuralın yer aldığı maddede veri sorumlusuna başvuru usulü belirlenmiştir. Buna göre ilgili kişi, 6698 sayılı Kanun'un uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir. Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Dava konusu kuralla ise işlemin ayrıca bir maliyeti gerektirmesi hâlinde Kurulca belirlenen tarifedeki ücretinalınabileceği öngörülmektedir.

102. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Ancak bu hak sınırsız olmayıp Anayasa Mahkemesi kararlarında, özel sınırlama nedeni öngörülmemiş özgürlüklerin de o özgürlüğün doğasından kaynaklanan bazı sınırları bulunduğu, ayrıca Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebileceği de kabul edilmektedir.

103. Ancak bu sınırlama yapılırken temel hak ve özgürlüklerin sınırlandırılması rejimini belirleyen Anayasa'nın 13. maddesine de uyulması gerekmektedir. Anayasa'nın 13. maddesi uyarınca, temel

hak ve özgürlüklerin özlerine dokunulmaksızın yapılacak sınırlamalar, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamaz. Ölçülülük ilkesi, yasal sınırlamanın öngörülen amaç için zorunlu ve amaca ulaşmaya elverişli olmasını, ayrıca amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder.

104. Dava konusu kuralla 6698 sayılı Kanun'un uygulanmasıyla ilgili taleplerini veri sorumlusuna ileten ilgili kişiden, yapılacak işlemin ayrıca bir maliyeti gerektirmesi hâlinde Kurulca belirlenen tarifedeki ücretin alınabileceği öngörülmek suretiyle kişisel veriler erişim hakkına bir sınırlandırma getirildiği açıktır. Kuralla kişilerin kendileri ile ilgili kişisel verilere erişme hakkına müdahalede bulunmuş ise de kişisel verilere erişimin bir maliyet gerektirmesi hâlinde söz konusu ücretin alınabileceği dikkate alındığında getirilen sınırlamanın Anayasa'nın 20. maddesinde düzenlenen kişisel verilerin korunması hakkının kullanılmasını son derece zorlaştıran veya onu kullanılamaz duruma düşüren kayıtlara bağlandığı söylenemeyeceğinden hakkın özüne dokunmadığı açıktır. Bu nedenle değerlendirilmesi gereken bu müdahalenin demokratik toplum düzeninin gerekleri ile ölçülülük ilkesine uygun olup olmadığıdır.

105. 6698 sayılı Kanun kapsamında veri sorumlusu; kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade etmektedir. Kanun'un 11. maddesinde ilgili kişinin hakları düzenlenmiştir. Buna göre herkes veri sorumlusuna başvurarak kendisiyle ilgili kişisel veri işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, 7. maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, 11. maddenin (d) ve (e) bentleri uyarınca yapılan kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini, silinmesini veya yok edilmesi işlemlerini kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme ve kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme haklarına sahiptir.

106. Dava konusu kuralda, ilgili kişinin 6698 sayılı Kanun'dan kaynaklanan hakları çerçevesinde başvurduğu veri sorumlusu tarafından talebinin yerine getirilmesinin ayrıca bir maliyet gerektirmesi hâlinde bu maliyetin Kurulca belirlenen tarifeye göre talepte bulunan ilgili tarafından karşılanabileceği öngörülmektedir.

107. Kanun koyucunun kuralla, takdir yetkisi kapsamında ilgililerin isteğine bağı olarak veri sorumluları tarafından ifa edilecek hizmetlerin ayrıca maliyet gerektirmesi hâlinde bu maliyetin ilgililer tarafından alınabilmesini sağlamayı amaçladığı anlaşılmaktadır. Zira veri sorumlusunun Kanun'da öngörülen ilgili kişinin hakları çerçevesinde yerine getireceği bazı işlemlerin maliyetinin olabileceği, bu hâlde ise söz konusu maliyet karşılanmadan ilgilinin taleplerini yerine getirebilmesinin mümkün olmayacağı açıktır. Veri sorumlusunun verdiği hizmetin ayrıca bir maliyet gerektirmesi hâlinde bu maliyetten sorumlu tutulması beklenemeyeceği gibi Kanun'un 13. maddesinde belirtildiği üzere ancak başvurunun veri sorumlusunun hatasından kaynaklanması hâlinde alınan ücret ilgiliye iade edilecektir. Diğer yandan 108 sayılı Sözleşme de bu tür masrafların alınmasına imkân tanımaktadır.

108. Öte yandan işlemin ayrıca bir maliyeti gerektirmesi hâlinde söz konusu ücretin belirsiz olduğu da söylenemez. Zira Kurul tarafından belirlenecek ücretin miktarı yapılan işlemin maliyeti kadardır. Bir işlemin maliyetinin belirlenebilir, ölçülebilir bir değer olması nedeniyle objektif bir kriter olması karşısında söz konusu ücretin Kurul tarafından belirlenecek tarifeye göre alınmasında hukuki güvenlik ve belirlilik ilkelerine aykırı bir yön bulunmamaktadır.

109. Dolayısıyla dava konusu kuralla sınırlama yapılırken Kanun'da sınırlama aracının sınırlama amacına uygun ve orantılı olduğu ve sınırlamayla kişisel verilerin korunması hakkı arasında hakkaniyete uygun bir denge kurulduğundan kuralların makul, ölçülü olduğu ve demokratik toplum düzeninin gereklerine aykırılık teşkil etmediği de açıktır.

110. Açıklanan nedenlerle kural Anayasa'nın 2., 5., 13. ve 20. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

111. Kuralın Anayasa'nın 90. maddesiyle ilgisi görülmemiştir.

H. Kanun'un 15. Maddesinin (3) Numaralı Fıkrasında Yer Alan "Devlet sırrı niteliğindeki bilgi ve belgeler hariç..." İbaresinin İncelenmesi

1. İptal Talebinin Gerekçesi

112. Dava dilekçesinde özetle, kişisel verilerin korunmasına dair normların kişiyi ve kişisel verileri korumak için oluşturulması gerektiği, devlet sırrı niteliğindeki bilgi ve belgelerin veri sorumlusu tarafından Kişisel Verileri Koruma Kuruluna (Kurul) gönderilmesine veya gerektiğinde yerinde inceleme yapılmasına istisna getiren dava konusu kuralın belirli ve ölçülü olmadığı, idarenin keyfi uygulamalarına sebep verecek nitelikte olduğu, kişinin kendisiyle ilgili kişisel veriler hakkında

bilgilendirilmesine engel olduğundan kişinin özel hayatının gizliliğine doğrudan müdahalede bulunduğu belirtilerek kuralın Anayasa'nın 2., 13. ve 20. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

113. Dava konusu kuralın yer aldığı maddede Kurul tarafından şikâyet üzerine veya resen incelemenin usul ve esasları düzenlenmektedir. Maddenin (3) numaralı fıkrasında; devlet sırrı niteliğindeki bilgi ve belgeler hariç veri sorumlusunun, Kurulun inceleme konusuyla ilgili istemiş olduğu bilgi ve belgeleri on beş gün içinde göndermek ve gerektiğinde yerinde inceleme yapılmasına imkân sağlamak zorunda olduğu hüküm altına alınmıştır. Fıkroda yer alan "Devlet sırrı niteliğindeki bilgi ve belgeler hariç..." ibaresi dava konusu kuralı oluşturmaktadır.

114. Kişisel verilerin korunması hakkı sınırsız olmayıp Anayasa Mahkemesi kararlarında, özel sınırlama nedeni öngörülmemiş özgürlüklerin de o özgürlüğün doğasından kaynaklanan bazı sınırları bulunduğu, ayrıca Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebileceği de kabul edilmektedir. Dolayısıyla kişisel verilerin korunması hakkının Anayasa'da Devlete bir görev olarak yüklenen millî güvenliğin ve kamu düzeninin sağlanması ile suç işlenmesinin önlenmesi amaçlarıyla sınırlandırılması mümkündür.

115. Nitekim 108 sayılı Sözleşme'nin 9. maddesinde de devlet güvenliği, kamu güvenliği, devletin ekonomik menfaatlerinin korunması ve suçlarla mücadele edilmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması ile verilerin istatistiki veya bilimsel amaçlarla kullanılması durumlarında kişisel verilerin korunmasına sınırlamalar getirilebileceği öngörülmüştür.

116. Ancak bu sınırlama yapılırken temel hak ve özgürlüklerin sınırlandırılması rejimini belirleyen Anayasa'nın 13. maddesine de uyulması gerekmektedir. Anayasa'nın 13. maddesi uyarınca özel hayatın gizliliği ve kişisel verilerin korunması hakkı, yalnızca kanunla ve Anayasa'da öngörülen sebeplere bağlı olarak sınırlanabilir. Ayrıca getirilen bu sınırlamalar hakkın özüne dokunamayacağı gibi Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamaz.

117. 6698 sayılı Kanun'un 13. maddesinde ilgili kişinin veri sorumlusuna başvuru hakkı düzenlenmiş; 14. maddesinde ise söz konusu başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya başvuruya süresinde cevap verilmemesi hâllerinde ilgili kişinin Kurula şikâyette bulunabileceği hüküm altına alınmıştır. Kanun'un 15. maddesine göre ise Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapar.

118. 5271 sayılı Ceza Muhakemesi Kanunu'nun 47. maddesinin (1) numaralı fıkrasında yer alan "Açıklanması, Devletin dış ilişkilerine, milli savunmasına ve milli güvenliğine zarar verebilecek; anayasal düzeni ve dış ilişkilerinde tehlike yaratabilecek nitelikteki bilgiler, Devlet sırrı sayılır." hükmü dikkate alındığında dava konusu kuralda yer alan "Devlet sırrı niteliğindeki bilgi ve belgeler" ibaresinin devletin iç ve dış güvenliği ile millî savunmasını sağlamaya ve anayasal düzenini korumaya yönelik bilgi ve belgeleri ifade ettiği anlaşılmaktadır. Bu bağlamda söz konusu ibarenin belirsiz bir kavram olduğu söylenemez.

119. Kurulun inceleme konusuyla ilgili veri sorumlusundan isteyebileceği bilgi ve belgeler arasında özel hayatın gizliliği kapsamında kalacak kişisel verilerin bulunduğu devlet sırrı niteliğindeki bilgi ve belgeler de bulunabilir. Dava konusu kural söz konusu bilgi ve belgelerin Kurula gönderilmesi veya incelenmesi imkânını ortadan kaldırdığından Kurul tarafından bu bilgi ve belgeler üzerinde ihlal iddiasıyla ilgili inceleme yapılamayacaktır. Bu durum ise Kurulda incelenmekte olan ihlal iddiasıyla ilgili olan kişilerin kendileriyle ilgili kişisel verilere ulaşmasını bir anlamda kısıtlayacağından kurulla özel hayatın gizliliği ve kişisel verilerin korunması haklarına sınırlama getirildiği açıktır. Ancak bu sınırlamanın; devletin dış ilişkilerine, millî savunmasına, millî güvenliğine, anayasal düzeni ve dış ilişkilerinde tehlike yaratabilecek veya zarar verebilecek nitelikteki bilgi ve belgelerin açıklanmasının önlenmesini sağlamak amacıyla yapıldığı dikkate alındığında demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kaldığı kuşkusuzdur.

120. Öte yandan devlet sırrı kavramı altında her türlü kişisel verinin gizli tutulması söz konusu değildir. Zira ceza yargılamasında 5271 sayılı Kanun'un 47. maddesinin (1) numaralı fıkrasındaki "Bir suç olgusuna ilişkin bilgiler, Devlet sırrı olarak mahkemeye karşı gizli tutulamaz." hükmü ile (2) numaralı fıkrasındaki "Tanıklık konusu bilgilerin Devlet sırrı niteliğini taşıması halinde; tanık, sadece mahkeme hâkimi veya heyeti tarafından zâbit kâtabi dahi olmaksızın dinlenir. Hâkim veya mahkeme başkanı, daha sonra, bu tanık açıklamalarından, sadece yüklenen suçu açıklığa kavuşturabilecek nitelikte olan bilgileri tutanağa kaydettirir." hükmü gereğince bir suç olgusuna ilişkin bilgiler devlet sırrı olarak mahkemeye karşı gizli tutulamayacağı gibi tanıklık konusu bilgilerin devlet sırrı niteliği taşıması hâlinde bunların mahkeme hâkimi veya heyeti tarafından dinlenme imkânı da bulunmaktadır.

121. Öte yandan dava konusu kurulla sadece Kurulun inceleme konusuyla ilgili gönderilmesini isteyebileceği veya inceleyebileceği bilgi ve belgelere istisna getirilmiş olup bu istisna dışında kişisel verilerle ilgili olarak 6698 sayılı Kanun'da yer alan kişisel verilerin işlenmesinde uyulması zorunlu

ilke ve kurallar, kişisel verilerin işleme şartları ve veri güvenliğine ilişkin yükümlülükler ile kişisel verilere ilişkin suçlar bakımından 5237 sayılı Kanun'un 135 ila 140. maddeleri hükümlerinin uygulanacağına ilişkin hükümler geçerliliğini korumaktadır.

122. 6698 sayılı Kanun, 5237 sayılı Kanun ve diğer kanunlarda yer alan bu düzenlemeler birlikte değerlendirildiğinde kişilerin özel hayatına dair bilgilerin ve kişisel verilerin korunması hakkında yeterli yasal güvencenin sağlandığı anlaşılmaktadır. Bu bağlamda bir devlet sırrı niteliğindeki bilgi ve belgelerin ifşa edilmesini önlemeye yönelik dava konusu kuralın ulaşılmak istenen amaç için elverişli ve gerekli olduğu, amaç ve araç arasında makul ve uygun bir ilişki kurduğu ve öngörülen amaçla kişisel verilerin korunması hakkına yapılan sınırlamanın orantılı olduğu açıktır. Dolayısıyla dava konusu kuralla kişisel verilerin korunması hakkına sınırlama yapılırken, Kanun'da sınırlama aracının sınırlama amacına uygun ve orantılı şekilde kullanılmasını sağlayacak yasal güvencelere yer verildiği, böylece hem özel hayatın gizliliği ve kişisel verilerin korunması haklarının özünün zedelenmesinin önlendiği hem de bu haklar ile ülkede millî güvenliğin sağlanmasına yönelik önlemler arasındaki makul dengenin kurulduğu anlaşıldığından dava konusu kuralın özel hayatın gizliliği ve kişisel verilerin korunması haklarının özünü zedelediğinden söz edilemeyeceği gibi demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı düştüğü de söylenemez.

123. Açıklanan nedenlerle kural Anayasa'nın 2., 13. ve 20. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

I. Kanun'un 16. Maddesinin (2) Numaralı Fıkrasının İkinci Cümlesinin İncelenmesi

1. İptal Talebinin Gerekçesi

124. Dava dilekçesinde özetle, Veri Sorumluları Sicilinin kişisel verilerin kimler ve hangi kuruluşlar tarafından işlendiğini gösteren bir liste olduğu, bu listeye kayıt zorunluluğuna getirilecek istisnanın kişisel verileri işlenen kişiyi korumasız hâle getireceği, bu durumun kişinin maddi ve manevi varlığına doğrudan, ölçüsüz bir müdahale olduğu, hukuk devleti ilkesi ile bağdaşmadığı ve istisnanın uluslararası sözleşmelere aykırı olduğu belirtilerek kuralın Anayasa'nın 2. ve 90. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

125. Dava konusu kuralın yer aldığı maddede Kurulun gözetiminde, Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili tutulacağı ve kişisel verileri işleyen gerçek ve tüzel kişilerin veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorunda olduğu hüküm altına alınmıştır. Dava konusu kuralla ise işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan

kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebileceği öngörülmektedir.

126. Anayasanın 2. maddesinde yer alan hukuk devleti ilkesi gereğince kanun koyucu düzenlemeler yaparken ölçülülük ilkesiyle bağlıdır. Bu ilke ise “elverişlilik”, “gereklilik” ve “orantılılık” olmak üzere üç alt ilkeden oluşmaktadır. “Elverişlilik”, başvuru önlemin ulaşılmak istenen amaç için elverişli olmasını, “gereklilik” başvuru önlemin ulaşılmak istenen amaç bakımından gerekli olmasını, “orantılılık” ise başvuru önlem ve ulaşılmak istenen amaç arasında olması gereken ölçüyü ifade etmektedir. Bir kuralda öngörülen düzenleme ile ulaşılmak istenen amaç arasında da “ölçülülük ilkesi” gereğince makul bir dengenin bulunması zorunludur.

127. 95/46/EC sayılı Direktif de ulusal veri koruma otoritelerine sicillere bildirim yapılması yükümlülüğünü kaldırma veya basitleştirme imkânı tanımaktadır.

128. Dava konusu kuralın yer aldığı 16. maddeye göre kişisel verileri işleyen gerçek ve tüzel kişiler veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorunda olup kayıt başvurusunda maddede belirtilen hususları içeren bildirimde bulunurlar. Bu bildirim; veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgilerini, kişisel verilerin hangi amaçla işleneceğini, veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamaları, kişisel verilerin aktarılabilirliği alıcı veya alıcı grupları, yabancı ülkelere aktarımı öngörülen kişisel verileri, kişisel veri güvenliğine ilişkin alınan tedbirler ve kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi içerir. Bu bilgilerde meydana gelen değişiklikler derhâl Başkanlığa bildirilir. Veri Sorumluları Siciline ilişkin diğer usul ve esaslar yönetmelikle düzenlenir.

129. Veri Sorumluları Siciline kaydolmak zorunda olan gerçek ve tüzel kişiler birbirinden farklı büyüklük ve ölçekte olabileceği gibi bunlar tarafından işlenen verilerle ilgili olarak nitelik, sayı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılması gibi farklı yoğunluk ve önem derecesine sahip durumlar da olabilir. Kanun koyucunun dava konusu kuralla, söz konusu farklılıkları dikkate alarak kişisel verileri işleyen gerçek ve tüzel kişilerin tümünün Veri Sorumluları Siciline kaydolmasına gerek görmediği ve bazılarını Kurul tarafından belirlenecek objektif kriterler göz önüne alınmak suretiyle yine Kurul tarafından verilecek kararlarla kayıt zorunluluğundan istisna tutmayı amaçladığı anlaşılmaktadır. Bu bağlamda kanun koyucunun takdir yetkisi kapsamında düzenlediği dava konusu kuralın amaç ve araç arasında makul ve uygun bir ilişki kurduğu ve orantılı olduğu anlaşıldığından ölçülülük ilkesine aykırı bir yönü bulunmamaktadır.

130. Öte yandan dava konusu kuralla sadece Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilmiş olup veri sorumlularının veri güvenliğine ilişkin olarak Kanun'da öngörülen yükümlülüklerle istisna getirilmemiştir. Zira Kanun'un 12. maddesinde veri sorumlusunun veri güvenliğine ilişkin yükümlülükleri belirlenmiştir. Buna göre veri sorumlusu kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde 12. maddenin birinci fıkrasında belirtilen tedbirlerin alınması hususunda bu kişilerle müştereken sorumlu olup kendi kurum veya kuruluşunda bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır. Ayrıca veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük, veri işleyen kişilerin görevden ayrılmalarından sonra da devam eder. Bu bağlamda veri sorumlularının yükümlülükleri bakımından bunların Sicile kayıtlı olup olmamalarının bir önemi bulunmamakta olup dava konusu kural, ilgili kişinin haklarını korumak üzere oluşturulan icrai mekanizma ve özel tedbirleri ortadan kaldıran veya zedeleyen bir düzenleme şeklinde değerlendirilemez. Dolayısıyla kuralla ulaşılmak istenen amaç arasında makul bir denge kurulduğundan ve veri sorumlularının yükümlülükleri de ortadan kaldırılmadığından kuralın Anayasa'ya aykırı bir yönü bulunmamaktadır.

131. Açıklanan nedenlerle kural Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

132. Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ ile Osman Alifeyyaz PAKSÜT bu görüşe katılmamışlardır.

133. Kuralın Anayasa'nın 90. maddesiyle ilgisi görülmemiştir.

İ. Kanun'un 24. Maddesinin (3) Numaralı Fıkrasının (b) Bendinde Yer Alan "Kurulca gerekli görülenlerin..." İbaresinin İncelenmesi

1. İptal Talebinin Gerekçesi

134. Dava dilekçesinde özetle, Kurulun gerek görmemesi hâlinde kararlarının yayımlanmamasına olanak sağlayan kuralın başvuru kişi ve kamuoyu bakımından belirsizlik yarattığı, Kurula yapılan başvurular arasında ayırım yapıldığı, bu ayırma dair objektif kriterlerin belirlenmediği belirtilerek kuralın Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

135. Dava konusu kuralın yer aldığı maddenin (3) numaralı fıkrasında Başkanın görevleri sayılmıştır. Bu görevlerden biri de fıkranın (b) bendinde “Kurul kararlarının tebliğini ve Kurulca gerekli görülenlerin kamuoyuna duyurulmasını sağlamak ve uygulanmalarını izlemek” şeklinde belirlenmiştir. Fıkroda yer alan “Kurulca gerekli görülenlerin” ibaresi, dava konusu kuralı oluşturmaktadır.

136. Anayasa'nın 2. maddesinde yer alan hukuk devletinin önemli bir unsuru olan belirlilik ilkesi bireylerin hukuk kurallarını önceden bilmeleri, davranış ve tutumlarını bu kurallara göre güvenle düzene sokabilmelerini gerektirmekte olup hukuk kurallarının belirliliğinin sağlanması yalnızca kanunla düzenleme yapılması anlamına gelmemektedir. Belirlilik ilkesi, yalnızca yasal belirliliği değil daha geniş anlamda hukuki belirliliği de ifade etmektedir. Yasal dayanağının bulunması ve erişilebilir, bilinebilir ve öngörülebilir olması gibi gereklilikleri karşılaması koşuluyla mahkeme içtihatları ve yürütmenin düzenleyici işlemleri ile de hukuki belirlilik sağlanabilir. Hukuki belirlilik ilkesinde asıl olan, bir hukuk normunun uygulanmasıyla ortaya çıkacak sonuçların o hukuk düzeninde öngörülebilir olmasıdır.

137. Dava konusu kuralda, Kişisel Verileri Koruma Kurulu tarafından verilen kararlardan Kurulca gerekli görülenlerin Başkan tarafından kamuoyuna duyurulması öngörülmektedir. Dolayısıyla Kurul tarafından gerekli görülmeyen kararlar kamuoyuna duyurulmayacaktır.

138. 6698 sayılı Kanun'un Kurulun çalışma esaslarının düzenlendiği 23. maddesinde Kurulun toplantı günlerini ve gündemini Başkanın belirleyeceği, Başkanın gereken hâllerde Kurulu olağanüstü toplantıya çağırabileceği, Kurul toplantılarındaki görüşmelerin gizli olduğu, Kurulda görüşülen işlerin tutanağa bağlanacağı ve Kurulun gerekli gördüğü kararları kamuoyuna duyuracağı, Kurulun çalışma usul ve esasları ile kararların yazımı ve diğer hususların yönetmelikle düzenleneceği hüküm altına alınmıştır. Bu bağlamda Kurulca kamuoyuna duyurulacak kararların söz konusu yönetmelikteki usul ve esaslara göre yapılacak çalışma çerçevesinde belirleneceği dikkate alındığında kuralın belirsiz olduğundan söz edilemez.

139. Öte yandan dava dilekçesinde Kurula yapılan başvurular arasında ayırım yapıldığı ve bu ayırma dair objektif kriterlerin belirlenmediği ifade edilmişse de kurulla, verdiği kararların hangilerinin kamuoyuna duyurulacağını belirleme konusunda Kurula yetki verildiği anlaşılmaktadır. Zira Kanun'un 22. maddesinde Kurulun görev ve yetkileri düzenlenmekte olup bu görev ve yetkilerin bir kısmının idari işleyiş ve yönetime ilişkin olması karşısında Kurulca verilen tüm kararların kamuoyuna duyurulmasında kamu yararı olduğu söylenemez. Bu bağlamda kuralın kanun

koyucunun takdir yetkisi kapsamında olduğunda kuşku yoktur. Dolayısıyla kuralda hukuk devleti ilkesine aykırı bir yön bulunmamaktadır.

140. Açıklanan nedenlerle kural Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

J. Kanun'un 28. Maddesinin (1) Numaralı Fıkrasının (a) ve (ç) Bentlerinin İncelenmesi

1. (a) Bendinin İncelenmesi

a. İptal Talebinin Gerekçesi

141. Dava dilekçesinde özetle, sadece aynı konutta yaşamayan bir başkasının kişisel alanına müdahale edilebileceği anlamına gelmediği, özel yaşamın sadece aile yaşamı veya konut mahremiyeti olmadığı, kişisel özerkliğin özel yaşama saygı kapsamındaki güvencelerin yorumlanmasında önemli bir ilke olduğu, aynı konutta yaşayan bireyler kapsamında eşler, eşlerin üstsoyu, evlilik birliği içinde veya dışında doğan veya evlat edinilen yahut koruyucu aile olarak bakımı üstlenilen çocukların da olabileceği, özel yaşamın gizliliği konusunda özellikle çocuklar ve korunmasız bireylerin etkili bir şekilde korunma hakkına sahip olduğu, velayet ilişkisinin çocuğun varlığını, onurunu, maddi ve manevi bütünlüğünü ortadan kaldıran bir hukuki müessese olmadığı, çocukların kişisel verilerinin işlenmesi öncesinde yaşları ve gelişim durumlarına göre uygun kapsam ve yöntemlerle bilgilendirilmeleri ve açık rızalarının alınmasının gerektiği belirtilerek kuralın Anayasa'nın 2., 13., 20., 41. ve 90. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

142. Dava konusu kuralın yer aldığı maddede 6698 sayılı Kanun hükümlerinin uygulanmayacağı hâller hüküm altına alınmıştır. Dava konusu kuralla kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülükler uymak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi hâlinde 6698 sayılı Kanun hükümlerinin uygulanmayacağı hüküm altına alınmaktadır.

143. Anayasa'nın 20. maddesinin birinci fıkrasının birinci cümlesinde "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir." denilmek suretiyle özel hayat ve aile hayatına saygı gösterilmesini isteme hakkı güvence altına alınmıştır.

144. Anayasa'nın 41. maddesinde "Aile, Türk toplumunun temelidir ve eşler arasında eşitliğe dayanır. Devlet, ailenin huzur ve refahı ile özellikle ananın ve çocukların korunması ve aile planlamasının öğretimi ile uygulanmasını sağlamak için gerekli tedbirleri alır, teşkilâtı kurar. Her

çocuk, korunma ve bakımdan yararlanma, yüksek yararına açıkça aykırı olmadıkça, ana ve babasıyla kişisel ve doğrudan ilişki kurma ve sürdürme hakkına sahiptir. Devlet, her türlü istismara ve şiddete karşı çocukları koruyucu tedbirleri alır.” denilmektedir.

145. Anayasa'nın 41. maddesinde aile Türk toplumunun temeli olarak tanımlanmış, ailenin birey ve toplum hayatındaki önemine işaret edilmiş ve devlete ailenin korunması için gerekli düzenlemeleri yapması ve teşkilatı kurması konusunda ödevler yüklenmiştir. Böylece aile kurumuna anayasal koruma sağlanmıştır. Bu düzenlemeyle eşler ve çocuklardan oluşan ailenin birlik ve bütünlüğünün korunması amaçlanmaktadır. 41. maddeye 7.5.2010 tarihli ve 5982 sayılı Kanun'la eklenen dördüncü fıkrada da devletin her türlü istismara ve şiddete karşı çocukları koruyucu tedbirleri alacağı belirtilmiştir. Bu düzenlemeyle “Ailenin korunması” şeklindeki madde başlığı “Ailenin korunması ve çocuk hakları” şeklinde değiştirilip maddeye çocukların korunması konusu da eklenerek çocukların temel hakları vurgulanmış ve devletin çocukları koruyucu tedbirleri alacağı belirtilmiştir.

146. Dava konusu kuralla kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülükler uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi hâlinde 6698 sayılı Kanun'da yer alan kişisel verilerin korunmasına ilişkin hükümlerin uygulanmayacağı düzenlenmiştir. Söz konusu düzenleme ile bir kişinin gerek kendi gerekse aynı konutta birlikte oturduğu aile fertlerine ilişkin kişisel verileri işlenmesinin, söz konusu birlikte yaşamının doğal ve zorunlu bir sonucu olduğu anlaşılmaktadır. Ayrıca dava konusu kuralın söz konusu hakların kullanılmasını son derece zorlaştıran veya onu kullanılamaz duruma düşüren kayıtlara bağlandığı da söylenemeyeceğinden hakkın özüne dokunmadığı açıktır. Bu nedenle değerlendirilmesi gereken husus bu müdahalenin demokratik toplum düzeninin gerekleri ile ölçülülük ilkesine uygun olup olmadığıdır.

147. Dava konusu kuralla, kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında kişisel verilerin işlenmesi hâlinde 6698 sayılı Kanun hükümlerinin uygulanmayacağı hüküm altına alınmıştır. 4721 sayılı Türk Medeni Kanunu'na göre eşler ve çocuklardan oluşan aile fertlerinin, kendileriyle veya diğer aile fertleriyle ilgili olarak 4721 sayılı Kanun'da veya diğer kanunlarda belirtilen faaliyet ve yükümlülükleri olabileceği gibi günlük hayatın akışı içinde gerçekleştirilecek faaliyetleri de olabilir. Bu faaliyet ve yükümlülüklerin yerine getirilmesi ise söz konusu aile fertleriyle ilgili bazı kişisel verilerin işlenmesini gerektirebilir. Kanun koyucunun kuralla takdir yetkisi kapsamında gerçek kişilerin kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili söz konusu faaliyet ve yükümlülüklerin sıklık ve yoğunluk derecesini de dikkate alarak bunlarla ilgili veri işleme prosedürünü kolaylaştırmayı amaçladığı anlaşılmaktadır. Aynı

konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında tanınan dava konusu istisnanın başta çocuklar olmak üzere aile fertlerinin özerk varlığını, onurunu, maddi ve manevi bütünlüğünü ortadan kaldırmayı amaçlayan ya da bu amaca matuf bir hukuki müessese olmadığı aksine Anayasa'nın 41. maddesi ve başta 4721 sayılı Kanun olmak üzere diğer kanunlardan kaynaklanan aile fertleriyle ilgili hukuki faaliyet ve yükümlüklerin tam ve zamanında yerine getirilebilmesi suretiyle ailenin ve özellikle çocukların korunmasını sağlamaya yönelik olduğu açıktır.

148. Öte yandan anne ve babaların, çocukları üzerinde velayet hakkını yerine getirirken 4721 sayılı Kanun'dan kaynaklanan yükümlülüklere uygun hareket etme zorunluluğu bulunmaktadır. 4721 sayılı Kanun'da çocukların korunması ve yetiştirilmesine ilişkin söz konusu yükümlülükler aykırı hareketlerin hukuki sonuçlarına ilişkin hükümlere yer verildiği gibi 5395 sayılı Çocuk Koruma Kanunu'nda yer alan ilkeler uyarınca çocuğun haklarının korunması konusunda da ayrıntılı düzenlemeler hüküm altına alınmıştır. Bu bağlamda kuralla sınırlama yapılırken ilgili kanunlarda sınırlama aracının sınırlama amacına uygun ve orantılı şekilde kullanılmasını sağlayacak yasal güvencelere yer verildiği de görülmektedir. Dolayısıyla kuralla ulaşılmak istenen amaç arasında makul bir denge kurulduğu de dikkate alındığında kuralın demokratik toplum düzeninin gerekleri ve ölçülülük ilkesine aykırı bir yönü bulunduğu söylenemez.

149. Açıklanan nedenlerle kural Anayasa'nın 2., 13., 20. ve 41. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

150. Kuralın Anayasa'nın 90. maddesiyle ilgisi görülmemiştir.

2. (ç) Bendinin İncelenmesi

a. İptal Talebinin Gerekçesi

151. Dava dilekçesinde özetle, önleyici, koruyucu ve istihbari faaliyetlerin geniş ve belirsiz bir kavram olarak idarenin keyfî uygulamalarına yol açabilecek nitelikte olduğu, bu istisnalar kapsamına giren konularda kamu kurumlarının hangi hâllerde veri toplayacağı ve işleyeceğinin sayılması ve sınırlandırılması gerektiği, kuralın kişilerin özel yaşamlarının gizliliği hakkının özüne dokunduğu, hakkın kullanımını olanaksız hâle getirdiği, belirlilik ilkesine aykırı olduğu, sınırları belirsiz şekilde bireylerin özel yaşamlarının gizliliğine doğrudan bir müdahale niteliğinde olduğu belirtilerek kuralın Anayasa'nın 2., 13., 20. ve 90. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

152. Dava konusu kuralda 6698 sayılı Kanun hükümlerinin uygulanmayacağı hâllerden biri olarak kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik

güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi sayılmaktadır.

153. Kişisel verilerin korunması hakkı sınırsız olmayıp Anayasa Mahkemesi kararlarında, özel sınırlama nedeni öngörülmemiş özgürlüklerin de o özgürlüğün doğasından kaynaklanan bazı sınırları bulunduğu, ayrıca Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebileceği de kabul edilmektedir. Dolayısıyla kişisel verilerin korunması hakkının Anayasa'da Devlete bir görev olarak yüklenen millî güvenliğin ve kamu düzeninin sağlanması ile suç işlenmesinin önlenmesi amaçlarıyla sınırlandırılması mümkündür.

154. Ancak bu sınırlama yapılırken temel hak ve özgürlüklerin sınırlandırılması rejimini belirleyen Anayasa'nın 13. maddesine de uyulması gerekmektedir. Anayasa'nın 13. maddesi uyarınca özel hayatın gizliliği ve kişisel verilerin korunması hakkı, yalnızca kanunla ve demokratik bir toplumda gerekli olduğu ölçüde sınırlanabilir. Ayrıca getirilen bu sınırlamalar hakkın özüne dokunamayacağı gibi Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamaz.

155. Nitekim 108 sayılı Sözleşme'nin 9. maddesinde de devlet güvenliği, kamu güvenliği, devletin ekonomik menfaatlerinin korunması ve suçlarla mücadele edilmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması ile verilerin istatistiki veya bilimsel amaçlarla kullanılması durumlarında kişisel verilerin korunmasına sınırlamalar getirilebileceği belirtilmiştir. AİHM de işe alınırken gizli bir polis dosyasında yer alan daha önceki sendikal faaliyetlerine ilişkin verilerin saklanması ve kullanılması hakkında yapılan bir başvuruda demokratik bir toplumda istihbarat servislerinin varlığının ve verilerin saklanması yasalara uygun olabileceğini, meşru menfaat başka bir deyişle suç işlenmesinin önlenmesi ya da ulusal güvenliğin korunması amaçlarını gözetmesi koşuluyla vatandaşların menfaatlerinin önüne geçebileceğini belirterek söz konusu müdahaleyi demokratik bir toplumda ulusal güvenlik gibi devlete geniş bir takdir yetkisi tanıyan bir konuda ağır basan sosyal ihtiyacı da göz önüne alarak AİHS'ne aykırı görmemiştir (Leander/İsveç, B. No: 9248/81, 23.3.1987).

156. Kuralın yer aldığı madde gerekçesinde kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesinin istisna olarak düzenlendiği; buna göre Millî İstihbarat Teşkilatı ile diğer istihbarat birimlerinin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik faaliyetler kapsamında işlediği verilerin Kanun

kapsamı dışında tutulduğu; aynı şekilde suç gelirlerinin aklanması, terörizmin finansmanının önlenmesi ve mali suçların araştırılması konusunda yetkili birim tarafından yürütülen faaliyetler kapsamında işlenen verilerin de bu istisna kapsamında olduğu, bu konulardaki yetkili birimin millî savunmayı, millî güvenliği kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik olmak üzere mali araştırma yapmak, mali istihbarat elde etmek ve üretmek, veri toplamak, şüpheli işlem bildirimleri ve diğer bildirimleri almak, analiz etmek, değerlendirmek, inceleme yapmak ve ilgili kurumlarla paylaşmak suretiyle işlediği verilerin de 6698 sayılı Kanun kapsamı dışında tutulduğu ifade edilmektedir.

157. Kuralla millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak görev ve yetki verilmiş olan kamu kurum ve kuruluşları tarafından yürütülecek önleyici, koruyucu ve istihbari faaliyetler kapsamında kişisel verilerin işlenmesinde 6698 sayılı Kanun hükümlerinin uygulanmayacağı hüküm altına alınmaktadır. İşlenecek bu bilgiler arasında özel hayatın gizliliği kapsamında kalacak bilgiler ve kişisel veriler de bulunabileceğinden kuralla özel hayatın gizliliği ve kişisel verilerin korunması haklarına sınırlama getirildiği açıktır. Ancak bu sınırlama, Anayasa'da devlete verilen görevlerin gereği olarak millî güvenliğin, kamu düzeninin ve suç işlenmesinin önlenmesini sağlamak amacıyla yapıldığından demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır.

158. Kuralda yer alan "önleyici, koruyucu ve istihbari faaliyetler", "millî savunma", "millî güvenlik", "kamu güvenliği", "kamu düzeni", "ekonomik güvenlik" ibarelerinin soyut ve genel kavramlar olması kuralın belirsiz olduğu anlamına gelmemekte, bu durum kanun yapma tekniğinin doğasından kaynaklanmaktadır. Zira yasa kurallarının genel ve soyut olması; somut olayın özelliğine göre değişebilecek tüm çözümleri kuralın bünyesinde barındırma, bir başka ifadeyle kuralın amaca uygun sonuca ulaştıracak herhangi bir çözümü dışlamasını önleme ihtiyacından kaynaklanmaktadır.

159. Öte yandan 2559 sayılı Polis Vazife ve Salahiyet Kanunu, 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu gibi ilgili kuruluş kanunlarında görev ve yetki verilmiş polis teşkilatı ve MİT gibi veya 4208 sayılı Kanun'la kurulan, görev ve yetkileri 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun ile yeniden belirlenen Malî Suçları Araştırma Kurulu (MASAK) gibi kamu kurum ve kuruluşlarının dava konusu kuralda yer alan millî güvenliği, kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilen kamu kurum ve kuruluşları olduğu açıktır. Bu kanunlarda, söz konusu kamu kurum ve kuruluşlarının görev ve yetkileri ayrıntılı şekilde düzenlenmiş ve bu düzenlemelerde söz konusu görevlerin Türkiye Cumhuriyeti'nin ülkesi ve milleti ile bütünlüğüne, varlığına, bağımsızlığına,

güvenliğine, Anayasal düzenine ve millî gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkında millî güvenlik istihbaratını oluşturmak veya suç gelirlerinin aklanmasının önlenmesini sağlamaya yönelik olduğu belirtilerek bu kamu kurum ve kuruluşları tarafından yürütülecek önleyici, koruyucu ve istihbari faaliyetler de düzenlenmiştir. Bu bağlamda dava konusu kuralla düzenlenen “önleyici, koruyucu ve istihbari” faaliyetlerin ilgili kuruluş kanunlarında veya diğer kanunlarda kapsam, sınır ve içeriklerinin ayrıntılı şekilde düzenlenmesi karşısında söz konusu faaliyetlerin kapsamının belirsiz olduğu söylenemez.

160. Ayrıca söz konusu kurum ve kuruluşların yetki ve sorumlulukları ile bunlara aykırı davranılması hâlinde öngörülen cezai yaptırımlar ilgili kanunlarda ayrıntılı şekilde düzenlendiği gibi 5237 sayılı Kanun’un 136. maddesi uyarınca da kişisel verileri hukuka aykırı olarak başkasına vermek, yaymak veya ele geçirmek suç olarak düzenlenmiştir. Dolayısıyla dava konusu kural kapsamında elde edilecek bilgilerin amacı dışında kullanılmasını önleyecek ve kişilerin özel hayatına dair bilgilerin ve kişisel verilerin ifşa edilmesini önleyecek yasal güvencenin sağlandığı görülmektedir. Bu bağlamda ilgili kanunlarda sınırlama aracının sınırlama amacına uygun ve orantılı şekilde kullanılmasını sağlayacak yasal güvencelere yer verildiği ve yeterli korumanın da sağlandığı dikkate alındığından dava konusu kurallarla kişisel verilerin korunması hakkına getirilen sınırlamaların özel hayatın gizliliği ve kişisel verilerin korunması hakkının özünü zedelediği gibi bu haklar ile ülkede millî güvenliğin sağlanmasına yönelik önlemler arasındaki makul dengenin kurulduğu görülmektedir. Dolayısıyla dava konusu kuralla özel hayatın gizliliği ve kişisel verilerin korunması haklarına getirilen sınırlamanın söz konusu hakların özünü zedelediğinden söz edilemeyeceği gibi demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı düştüğü de söylenemez.

161. Açıklanan nedenlerle kural Anayasa’nın 2., 13. ve 20. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

162. Kuralın Anayasa’nın 90. maddesiyle ilgisi görülmemiştir.

K. Kanun’un 30. Maddesinin (7) Numaralı Fıkrası ile Değiştirilen 663 Sayılı Kanun Hükmünde Kararname’nin 47. Maddesinin İncelenmesi

1. İptal Talebinin Gerekçesi

163. Dava dilekçesinde özetle, dava konusu kuralların kişilerin sağlık hizmeti almaktan imtina etmesine neden olabileceğinden sağlık hakkına ve yaşam hakkına bir müdahale niteliğinde olduğu, kişilerin sağlıklı ilgili bilgilerinin kamu yararı bulunan bazı durumlar dışında devletten dahi gizli tutulmasını isteme hakkı bulunduğu ancak kuralla geniş şekilde sayılan amaçların kamu sağlığını

korumayı aşacak nitelikte olduğu, sağlık hizmetlerinin planlanması ve maliyetlerin hesaplanması amacının yerine getirebilmesi için bireylerin her türlü verisinin işlenmesine ihtiyaç bulunmadığı, Sağlık Bakanlığının topladığı her türlü kişisel veriyi üçüncü kişilere aktarması hususunun sadece 6698 sayılı Kanun'daki düzenlemelere tabi olduğu ancak Kanun'daki düzenlemelerin kişilerin açık rızasının alınmasına gerek duyulmayacak şekilde ve kapsamı geniş tutulan istisnalar şeklinde düzenlendiğinden her türlü kişisel verinin üçüncü kişilere aktarılabilmesi, kurulacak sistemin üçüncü kişilere kişisel verilere erişim imkânı yarattığı, bu durumun özellikle kadın üzerinde toplumsal baskı yaratacağı, töre ve namus cinayetlerine zemin hazırlayacağı, oluşturulacak merkezî sisteme kimler tarafından erişilebileceğinin belirsiz olduğu, yetkili kılınacak sağlık personeli bakımından sınırlama yapılmadığı, kişinin doktorunun bu verilere erişmesi hedeflenmiş olsa da kurulan merkezî sistemin bu amacı ve kastı aştığı, merkezî sistemin güvenliği ve güvenilirliği ile ilgili standartların Kişisel Verileri Koruma Kurulunun belirlediği ilkelere uygun olarak Sağlık Bakanlığınca belirlenmesi ile Sağlık Bakanlığı'nun kişisel sağlık verilerinin güvenliğinin sağlanması için gerekli tedbirleri almasına ilişkin düzenlemesinin belirsiz olduğu, Kurulun çoğunluğunun yürütme tarafından oluşturulan bir yapı olduğu, belirlenecek ilkelerin yürütmenin çoğunlukta olduğu bu yapı tarafından belirlenmesinin keyfiliğe yol açabileceği, kuralların uluslararası sözleşmelere aykırı olduğu, yönetmelikle düzenleneceği öngörülen kişisel sağlık verilerinin işlenmesi, güvenliği ve kapsamı belirli olmayan ilgili diğer hususların neler olduğunun kanun ile belirlenmesinin zorunlu olduğu belirtilerek kuralın Anayasa'nın 2., 13., 17., 20., 56. ve 90. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

164. 6216 sayılı Kanun'un 43. maddesi uyarınca, kural ilgisi nedeniyle Anayasa'nın 5. ve 7. maddeleri yönünden de incelenmiştir.

165. Dava konusu kuralların yer aldığı 663 sayılı Kanun Hükmünde Kararname (KHK) Sağlık Bakanlığı ve bağlı kuruluşlarının teşkilat, görev, yetki ve sorumluluklarını düzenlemektedir. KHK'nın 2. maddesine göre Bakanlığın görevi; herkesin bedenî, zihnî ve sosyal bakımdan tam bir iyilik hâli içinde hayatını sürdürmesini sağlamaktır. Bu kapsamda Bakanlık halk sağlığının korunması ve geliştirilmesi, hastalık risklerinin azaltılması ve önlenmesi, teşhis, tedavi ve rehabilite edici sağlık hizmetlerinin yürütülmesi, uluslararası önemi haiz halk sağlığı risklerinin ülkeye girmesinin önlenmesi, sağlık eğitimi ve araştırma faaliyetlerinin geliştirilmesi, sağlık hizmetlerinde kullanılan ilaçlar, özel ürünler, ulusal ve uluslararası kontrole tabi maddeler, ilaç üretiminde kullanılan etken ve yardımcı maddeler, kozmetikler ve tıbbi cihazların güvenli ve kaliteli bir şekilde

piyasada bulunması, halka ulaştırılması ve fiyatlarının belirlenmesi, insan gücünde ve maddi kaynaklarda tasarruf sağlamak ve verimi artırmak, sağlık personelinin ülke sathında dengeli dağılımını sağlamak ve bütün paydaşlar arasında iş birliğini gerçekleştirmek suretiyle yurt sathında eşit, kaliteli ve verimli hizmet sunumunun sağlanması, kamu ve özel hukuk tüzel kişileri ile gerçek kişiler tarafından açılacak sağlık kuruluşlarının ülke sathında planlanması ve yaygınlaştırılması ile ilgili olarak sağlık sistemini yönetir ve politikaları belirler.

166. Bakanlık, bu amaçları gerçekleştirmek üzere strateji ve hedefleri belirler; planlama, düzenleme ve koordinasyon, uluslararası ve sektörler arası iş birliği, rehberlik, izleme, değerlendirme, teşvik, yönlendirme ve denetleme yapar, müeyyide uygular, acil durum ve afet hâllerinde sağlık hizmetlerini planlar ve yürütür, bölgesel farklılıkları gidermeye ve herkesin sağlık hizmetine erişimini sağlamaya yönelik tedbirler alır, ilgili kurum ve kuruluşların insan sağlığını doğrudan ve dolaylı olarak etkileyen faktörler ve sosyal belirleyicilerle ilgili uygulamalarına ve düzenlemelerine yön verir, bunu teminen gerekli bildirimleri yapar, görüş bildirir ve müeyyide uygular, görevin ve hizmetin gerektirdiği her türlü tedbiri alır.

167. Dava konusu kuralların yer aldığı 663 sayılı KHK'nın 47. maddesinde sağlık hizmetine ilişkin kişisel veriler hakkında bilgi toplama, işleme ve paylaşma yetkisi düzenlenmiştir. Maddenin (1) numaralı fıkrasında sağlık hizmeti almak üzere kamu veya özel sağlık kuruluşları ile sağlık mesleği mensuplarına müracaat edenlerin, sağlık hizmetinin gereği olarak vermek zorunda oldukları veya kendilerine verilen hizmete ilişkin kişisel verilerin işlenebileceği, (2) numaralı fıkrasında ise sağlık hizmetinin verilmesi, kamu sağlığının korunması; koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve maliyetlerin hesaplanması amacıyla Bakanlığın bu fıkra kapsamında elde edilen verileri alarak işleyebileceği ve bu verilerin, Kişisel Verilerin Korunması Kanununda öngörülen şartlar dışında aktarılamayacağı öngörülmektedir.

168. Anayasa'nın 20. maddesinde belirtildiği üzere kişisel veriler ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir. 6698 sayılı Kanun'un 6. maddesinin (2) numaralı fıkrasına göre özel nitelikli kişisel verilerden olan kişilerin sağlığı ile ilgili verilerin kural olarak ilgilinin açık rızası olmaksızın işlenmesi yasaktır. Maddenin (3) numaralı fıkrasına göre özel nitelikli kişisel veriler kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir, cinsel hayata ve sağlığa ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar

tarafından ilgilinin açık rızası aranmaksızın işlenebilir. Kanun koyucunun dava konusu kurallarla kişisel verilerin korunması hakkında genel kanun niteliğinde olan 6698 sayılı Kanun'da belirtilen hükümleri Sağlık Bakanlığı ve bağlı kuruluşlarının teşkilat, görev, yetki ve sorumluluklarını düzenleyen özel kanun niteliğindeki 663 sayılı KHK'da da benzer şekilde düzenlemek suretiyle uygulamada ortaya çıkabilecek sıkıntıları önlemeyi amaçladığı anlaşılmaktadır.

169. Diğer taraftan 108 sayılı Sözleşme'nin 9. maddesinde, maddede belirtilen bazı hâllerde kişisel verilerin korunmasına sınırlamalar getirilebileceği belirtilmiştir. 95/46/EC sayılı Direktif'in 8. maddesinin (2) numaralı fıkrasında da veri işlemenin önleyici hekimlik, tıbbi teşhis, tıbbi yardım veya bakım ya da sağlık hizmetlerinin idari olarak yürütülmesi için gerekli olması ve bu verilerin ya sağlık personeli veya sağlık personeli gibi sır saklama yükümlülüğüne tabi kişiler tarafından işlenmesi mümkün kılınmıştır. Maddede ayrıca üye devletlerin uygun önlemleri almak koşuluyla kamu yararı için başka istisnalar da belirleyebileceği belirtilmiştir.

170. Dava konusu kurallarla özel hayatın gizliliği ve kişisel verilerin korunması haklarına sınırlama getirildiği şüphesizdir. Kurallarla her ne kadar söz konusu haklara müdahalede bulunulmuş ise de kuralların sadece sağlık hizmeti almak üzere müracaat edenlerin sağlık hizmetlerinin gereği olarak vermek zorunda oldukları veya kendilerine verilen hizmete ilişkin kişisel verilerin işlenebilmesini düzenlediği dikkate alındığında dava konusu kurallarla getirilen sınırlamanın söz konusu hakların kullanılmasını son derece zorlaştıran veya onu kullanılamaz duruma düşüren kayıtlara bağlandığı söylenemeyeceğinden hakkın özüne dokunmadığı açıktır. Bu nedenle değerlendirilmesi gereken husus bu müdahalenin demokratik toplum düzeninin gerekleri ile ölçülülük ilkesine uygun olup olmadığıdır.

171. Sağlık hizmetlerinin yerine getirilebilmesi, hasta takip sisteminin iyi bir şekilde işleyebilmesi ve hastaların sağlık hizmetlerinden en iyi şekilde yararlanabilmesi için söz konusu verilerin kamu veya özel sağlık kuruluşları ile sağlık mesleği mensupları tarafından işlenmesi gerektiği açıktır. Ayrıca söz konusu verilerin Bakanlık tarafından işlenmesinin Bakanlığın 663 sayılı KHK'da belirtilen sağlık hizmetleriyle ilgili strateji ve hedefleri belirlemek, planlama, düzenleme ve koordinasyon yapmak, acil durum ve afet hâllerinde sağlık hizmetlerini planlamak ve yürütmek, bölgesel farklılıkları gidermeye ve herkesin sağlık hizmetine erişimini sağlamaya yönelik tedbirler almak, ilgili kurum ve kuruluşların insan sağlığını doğrudan ve dolaylı olarak etkileyen faktörler ve sosyal belirleyicilerle ilgili uygulamalarına ve düzenlemelerine yön vererek bunu temin için gerekli bildirimleri yapmak, görüş bildirmek ve müeyyide uygulamak gibi görev, yetki ve sorumluluklarını yerine getirmesi bakımından da gerekli olduğunda kuşku yoktur.

172. Anayasa'nın 5. maddesi insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamayı devletin temel amaç ve görevleri arasında saymıştır. Devlet, kişilerin sağlık hakkından tam anlamıyla yararlanabilmeleri ve sağlıklı bir yaşam sürdürebilmeleri amacıyla yasal, idari, mali, yargısal ve diğer önlemleri almak zorundadır. Ayrıca Anayasa, sosyal hukuk devleti olmanın gereği olarak sağlık hizmetlerinin sunumunda yüklediği pozitif yükümlülük kapsamında devleti bu haklardan yararlanmayı artıracak önlemleri almakla mükellef kılmıştır. Bu nedenle Anayasa'nın 17. ve 56. maddelerinde öngörülen kişilerin yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkı ile sağlık hakkından yararlanma konusunda en geniş ölçekli uygulamaların gerçekleştirilmesi gerekir. Kişiler için bir hak olan sağlık hizmetinden yararlanmayı kolaylaştırıcı düzenlemeler yapılması ve bu hizmetin daha iyi bir şekilde gerçekleştirilmesi için gerekli tedbirlerin alınması devletin Anayasa'dan kaynaklanan bir ödevidir. Dolayısıyla Anayasa'da devlete verilen görevlerin gereği olarak kişilerin sağlıklı bir şekilde yaşam sürdürmeleri için genel sağlığın korunması amacıyla düzenlenen dava konusu kurallar demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır.

173. Öte yandan 6698 sayılı Kanun'un 2. maddesine göre Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır. Dolayısıyla dava konusu kurallar kapsamında sağlık verilerinin işlenmesi bakımından 6698 sayılı Kanun'da yer alan tüm ilke ve kurallar ile güvencelere uyulması zorunlu olup Kanun'da yer alan kişisel verilerin işleme şartlarına, aktarılmasına, veri sorumlusunun aydınlatma yükümlülüğüne, veri güvenliğine ilişkin kurallar uygulanacaktır. Aksi hâlde Kanun'un 17. maddesinde yer alan kişisel verilere ilişkin suçlar bakımından 5237 sayılı Kanun'un 135 ila 140. maddeleri hükümleri uygulanacak ve Kanun'un 7. maddesi hükmüne aykırı olarak kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanun'un 138. maddesine göre cezalandırılacaktır. Kişisel verileri hukuka aykırı olarak başkasına verme, yayma veya ele geçirme suçu ise 5237 sayılı Kanun'un 136. maddesi uyarınca cezalandırılacaktır. Bu bağlamda dava konusu kurallar kapsamında işlenecek verilerin amacı dışında kullanılmasını ve kişilerin özel hayatına dair bilgilerin ve kişisel verilerin ifşa edilmesini önleyecek yasal güvencelerin sağlandığı görülmektedir. Dava konusu kurallarda kişisel verilerin korunması hakkına sınırlama getirilirken Kanun'da sınırlama aracının sınırlama amacına uygun ve orantılı şekilde kullanılmasını sağlayacak yasal güvencelere de yer verildiği, böylece hem özel hayatın gizliliği ve kişisel verilerin korunması haklarının özünün zedelenmesinin önlendiği, hem de bu haklar ile ülkede genel sağlığın sağlanmasına yönelik önlemler arasındaki makul dengenin kurulduğu görülmektedir.

174. Dolayısıyla dava konusu (1) ve (2) numaralı fıkralarda kişisel verilerin korunmasını isteme hakkının özüne dokunan ya da bu hakkı ölçsüz şekilde sınırlandıran bir husus bulunmamaktadır. Kurallarla söz konusu verileri işleme yetkisinin amacı ve faaliyet alanı belirlenmiş ve bu şekilde kamu yararı ile özel hayatın gizliliği ve kişisel verilerin korunması hakları arasında adil bir denge kurulmuştur. Bu nedenle dava konusu kurallarda öngörülen sağlık verilerinin işlenmesi yetkisinin ölçülülük ilkesine aykırı bir yönü bulunmamaktadır.

175. Maddenin (3) numaralı fıkrasında Bakanlığın ikinci fıkra gereğince toplanan ve işlenen kişisel verilere, ilgili kişilerin kendilerinin veya yetki verdikleri üçüncü kişilerin erişimlerini sağlayacak bir sistem kuracağı; (4) numaralı fıkrasında, üçüncü fıkraya göre kurulan sistemlerin güvenliği ve güvenilirliği ile ilgili standartların Kişisel Verileri Koruma Kurulunun belirlediği ilkelere uygun olarak Bakanlıkça belirleneceği, Bakanlığın bu Kanun uyarınca elde edilen kişisel sağlık verilerinin güvenliğinin sağlanması için gerekli tedbirleri alacağı, bu amaçla sistemde kayıtlı bilgilerin hangi görevli tarafından ne amaçla kullanıldığının denetlenmesine imkân tanıyan bir güvenlik sistemi kuracağı; (5) numaralı fıkrasında ise sağlık personeli istihdam eden kamu kurum ve kuruluşları ile özel hukuk tüzel kişileri ve gerçek kişilerin istihdam ettiği personeli ve personel hareketlerini Bakanlığa bildirmekle yükümlü olduğu hüküm altına alınmıştır.

176. Dava konusu kurallarla kanun koyucunun KHK'nın 47. maddesinin (1) ve (2) numaralı fıkraları gereğince toplanan ve işlenen kişisel verilere, ilgili kişilerin kendilerinin veya yetki verdikleri üçüncü kişilerin erişimlerini sağlayacak bir sistemin kurulması ile kurulacak bu sistemin güvenliği ve güvenilirliğinin sağlanmasına yönelik ilke ve tedbirlerin belirlenmesi suretiyle özel nitelikli kişisel veri kategorisindeki sağlık verilerini daha özel olarak koruma altına almayı amaçladığı anlaşılmaktadır. Kanun koyucunun, kamu yararı amacıyla sağlığa ilişkin kişisel verilerin korunmasının önemini dikkate alarak bu verilerin güvenliğinin sağlanmasına yönelik olarak düzenlediği anlaşılan dava konusu kuralların Anayasa'ya aykırı bir yönü bulunmamaktadır.

177. AİHM'nin kararlarında da kişisel sağlık verilerine izinsiz erişilmesine karşı etkin ve somut bir korumanın önemi vurgulanarak kamu kurumları ve devletin bu verilerin gizliliğini güvence altına alabilmek için kişisel verileri koruyacak kuralları yürürlüğe koyma ve gerekli güvenceleri sağlama yükümlülüğü altında olduğu ifade edilmiş ve kişisel sağlık verilerini saklamakta başarısız olunması veya bu bilgilere erişime engel olacak güvenli ve sağlam bir sistem kurulamamasının AİHS'nin ihlali olarak değerlendirildiği görülmektedir. (I/Finlandiya, B.No: 20511/03, 17.07.2008).

178. Maddenin (6) numaralı fıkrasında kişisel sağlık verilerinin işlenmesi, güvenliği ve maddenin uygulanması ile ilgili diğer hususların Bakanlıkça yürürlüğe konulan yönetmelikle düzenleneceği belirtilmektedir.

179. Anayasa'nın 7. maddesinde yasama yetkisinin Türk Milleti adına Türkiye Büyük Millet Meclisine ait olduğu ve bu yetkinin devredilemeyeceği öngörülmüştür. Anayasa'da kanun ile düzenlenmesi öngörülen konularda yürütme organına genel ve sınırları belirsiz bir düzenleme yetkisinin verilmesi mümkün değildir. Anayasa'nın 20. maddesinde kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği öngörülmüştür.

180. Kanunla düzenleme ilkesi, düzenlenen alanda temel ilkelerin kanunla konulmasını ve çerçevenin kanunla çizilmesini ifade etmektedir. Gelişen koşul ve durumlara göre sık sık değişik önlemler alma, bunları kaldırma ve süratli biçimde hareket etme zorunluluğunun bulunduğu alanlarda yasama organının temel kuralları saptadıktan sonra uzmanlık ve idare tekniğine ilişkin hususları yürütmeye bırakması, yasama yetkisinin devri olarak yorumlanamayacağı gibi yürütme organının yasama organı tarafından çerçevesi çizilmiş alanda ve değişen koşullara uyum sağlayabilecek esnekliğe sahip kriterlere uygun olarak genel nitelikte hukuksal tasarruflarda bulunması, kanunla düzenleme ilkesine aykırılık oluşturmaz ve yasama yetkisinin devri olarak yorumlanamaz.

181. Maddenin (1), (2), (3), (4) ve (5) numaralı fıkralarında sağlık hizmetinin gereği olarak verilmesi zorunlu kişisel verilerin işlenmesi ve güvenliğine ilişkin genel çerçevenin belirlendiği; hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir olduğu ve kamu otoritelerinin keyfî uygulamalarına karşı koruyucu önlem içerdiği açıktır. Dolayısıyla kanun koyucunun temel esasları ve ilkeleri belirleyip sınırları çizdikten sonra bazı teknik konuların düzenlenmesini idareye bıraktığı dava konusu kuralın belirsiz olduğu söylenemeyeceği gibi yasama yetkisinin devredilmezliği ilkesine aykırı bir yönü de bulunmamaktadır.

182. Açıklanan nedenlerle kural Anayasa'nın 2., 5., 7., 13., 17., 20. ve 56. maddesine aykırı değildir. İptal talebinin reddi gerekir.

183. Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ ile Osman Alifeyyaz PAKSÜT bu görüşe katılmamışlardır.

184. Kuralın Anayasa'nın 90. maddesiyle ilgisi görülmemiştir.

IV. YÜRÜRLÜĞÜN DURDURULMASI TALEBİ

185. Dava dilekçesinde özetle iptali istenen kuralların Anayasa'ya açıkça aykırı olduğu ve yürürlüklerinin durdurulmaması hâlinde hukuk devleti yönünden giderilmesi olanaksız durum ve zararların ortaya çıkacağı belirtilerek kuralların yürürlüklerinin durdurulmasına karar verilmesi gerektiği ileri sürülmüştür.

24.03.2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun;

A. 4. maddesinin (2) numaralı fıkrasının (d) bendinde yer alan "...veya işlendikleri amaç için gerekli olan..." ibaresine,

B. 5. maddesinin (2) numaralı fıkrasının (c), (ç), (e) ve (f) bentlerine,

C. 6. maddesinin;

1. (1) numaralı fıkrasında yer alan "...mezhebi,..." ve "...kılık ve kıyafeti..." ibarelerine,

2. (3) numaralı fıkrasına,

D. 7. maddesinin (2) numaralı fıkrasına,

E. 8. maddesinin (3) numaralı fıkrasına,

F. 9. maddesinin (6) numaralı fıkrasına,

G. 13. maddesinin (2) numaralı fıkrasının ikinci cümlesine,

H. 15. maddesinin (3) numaralı fıkrasında yer alan "Devlet sırrı niteliğindeki bilgi ve belgeler hariç..." ibaresine,

I. 16. maddesinin (2) numaralı fıkrasının ikinci cümlesine,

J. 24. maddesinin (3) numaralı fıkrasının (b) bendinde yer alan "...Kurulca gerekli görülenlerin..." ibaresine,

K. 28. maddesinin (1) numaralı fıkrasının (a) ve (ç) bentlerine,

L. 30. maddesinin (7) numaralı fıkrası ile değiştirilen 11.10.2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 47. maddesine yönelik iptal talepleri, 28.9.2017 tarihli, E.2016/125, K.2017/143 sayılı kararla reddedildiğinden, bu madde, fıkra, bent, cümle ve ibarelere ilişkin yürürlüğün durdurulması taleplerinin REDDİNE, 28.9.2017 tarihinde OYBİRLİĞİYLE karar verilmiştir.

V. HÜKÜM

24.03.2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun;

- A.** 4. maddesinin (2) numaralı fıkrasının (d) bendinde yer alan "...veya işlendikleri amaç için gerekli olan..." ibaresinin, Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,
- B.** 5. maddesinin (2) numaralı fıkrasının (c), (ç), (e) ve (f) bentlerinin Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE OYBİRLİĞİYLE,
- C.** 6. maddesinin;
1. (1) numaralı fıkrasında yer alan "...mezhebi,..." ve "...kılık ve kıyafeti..." ibarelerinin Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, Serdar ÖZGÜLDÜR, Serruh KALELİ ile Osman Alifeyyaz PAKSÜT'ün karşıoyları ve OYÇOKLUĞUYLA,
2. (3) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ ile Osman Alifeyyaz PAKSÜT'ün karşıoyları ve OYÇOKLUĞUYLA,
- D.** 7. maddesinin (2) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,
- E.** 8. maddesinin (3) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,
- F.** 9. maddesinin (6) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,
- G.** 13. maddesinin (2) numaralı fıkrasının ikinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,
- H.** 15. maddesinin (3) numaralı fıkrasında yer alan "Devlet sırrı niteliğindeki bilgi ve belgeler hariç..." ibaresinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,
- I.** 16. maddesinin (2) numaralı fıkrasının ikinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ ile Osman Alifeyyaz PAKSÜT'ün karşıoyları ve OYÇOKLUĞUYLA,
- J.** 24. maddesinin (3) numaralı fıkrasının (b) bendinde yer alan "...Kurulca gerekli görülenlerin..." ibaresinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, OYBİRLİĞİYLE,
- K.** 28. maddesinin (1) numaralı fıkrasının (a) ve (ç) bentlerinin Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE OYBİRLİĞİYLE,

L. 30. maddesinin (7) numaralı fıkrası ile deđiřtirilen 11.10.2011 tarihli ve 663 sayılı Sađlık Bakanlıđı ve Bađlı Kuruluřlarının Teřkilat ve Gevleri Hakkında Kanun Hukmunde Kararname'nin 47. maddesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Engin YILDIRIM, Serdar ZGULDUR, Serruh KALELİ ile Osman Alifeyyaz PAKSUT'un karřıoyları ve OYOKLUĐUYLA, 28.9.2017 tarihinde karar verildi.

Başkan - Zuhtu ARSLAN

Başkanvekili - Burhan STUN

Başkanvekili - Engin YILDIRIM

ye: Serdar ZGULDUR; Serruh KALELİ; Osman Alifeyyaz PAKSUT; Recep KOMURCU; Hicabi DURSUN; Celal Mumtaz AKINCI; Muammer TOPAL; M. Emin KUZ; Hasan Tahsin GOKCAN; Kadir ZKAYA; Rıdvan GULEE; Recai AKYEL; Yusuf řevki HAKYEMEZ

KARřIOY GORUSU

A. 6698 Sayılı Kiřisel Verilerin Korunması Kanunu'nun 6. Maddesinin uncu Fıkrası Yonunden

1. Dava konusu kural, cinsel hayata ve sađlıđa iliřkin kiřisel verilerin ancak kamu sađlıđının korunması, koruyucu hekimlik, tıbbi teřhis, tedavi ve bakım hizmetlerinin yurutulmesi, sađlık hizmetleri ile finansmanının planlanması ve yonetimi amacıyla sır saklama yukumluluđu altında bulunan kiřiler veya yetkili kurum ve kuruluřlar tarafından ilgilinin aık rızası aranmaksızın iřlenebileceđini duzenlemektedir.

2. Devletin kamu sađlıđının korunması, koruyucu hekimlik, tıbbi teřhis, tedavi ve bakım hizmetlerinin yurutulmesi amalarıyla bazı verilere ihtiya duyması ve bunun iin ilgili kiřilerin aık rızasını aramaması bir an iin kabul edilebilir olsa bile aynı řeyi sađlık hizmetleri ile finansmanının planlanması ve yonetimi amaları dođrultusunda kiřilerin sađlık ve cinsel hayatlarına iliřkin hassas kiřisel verilerin aık rıza olmadan iřlenmesi iin soyleyemeyiz.

3. Cinsel hayata ve sađlıđa iliřkin zel nitelikli hassas veriler kiřinin zel hayatına ait en mahrem bilgileri de ierdiđinden bunların ancak aık rıza ile iřlenmesi gerekmektedir. Kiřiler, bu tur bilgilerin kendi rızaları dıřında kaydedilmesinden, toplanması, aktarılması ve iřlenmesinden endiře duyarak bazı temel hak ve hurriyetlerini kullanmaktan kaınabilecekleri gibi sađlık hizmeti almakta tereddut yařayabilirler.

4. Anayasa'nın 20. maddesinin birinci fıkrasında "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz." denilerek özel hayatın gizliliği güvence altına alınmıştır. Maddenin üçüncü fıkrasında ise herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı hükme bağlanarak kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir.

5. Cinsel hayata ve sağlığa ilişkin özel nitelikli hassas kişisel verilerin işlenmesinde temel ilke ilgilinin açık rızasının bulunmasıdır. İptali istenen kuralla bu kişisel verilerin ilgilinin açık rızası olmaksızın işlenebileceği hâller belirtilmek suretiyle yukarıda ifade edilen temel ilkeye istisna getirilmiştir. Özel nitelikli hassas kişisel veri olduğundan en küçük şüphe duyulmayan sağlık ve cinsel hayata ilişkin verilerin belirtilen hallerde ilgilinin açık rızası olmadan işlenebileceğini düzenleyen kuralla özel hayatın gizliliği ve kişisel verilerin korunması haklarına bir müdahalede bulunulmaktadır.

6. Bu müdahale söz konusu hakların kullanılmasını son derece zorlaştırmadığı veya onları kullanılamaz hale getirmediğinden hakkın özüne dokunmamakla beraber, müdahalenin demokratik toplum düzeninin gerekleri ile ölçülülük ilkesine uygun olup olmadığının değerlendirilmesi gerekmektedir.

7. Anayasa'nın 13. maddesinde, temel hak ve özgürlüklerin özlerine dokunulmaksızın ölçülülük ilkesine uygun şekilde, yasayla sınırlandırılabilmesi belirtilmektedir. Ölçülülük ilkesi sınırlamada başvurulan aracın sınırlama amacını gerçekleştirmeye elverişli olmasını; bu aracın sınırlama amacı açısından gerekli olmasını ve araçla amacın ölçüsüz bir oran içinde bulunmamasını ifade eder. Burada kısıtlama için kullanılan araçla amaç arasında hak ve özgürlüğü en az sınırlayacak dengeli bir orantı aranmaktadır.

8. Elverişlilik ölçütüne göre bir yasal düzenlemenin sınırlama amacı bakımından elverişli sayılması için bu düzenlemenin arzulan amaca katkı yapması gerekmektedir. İncelediğimiz kural bu niteliği kısmen taşımaktadır. Gereklik ise bir temel hakkı en az sınırlayan aracın seçilmesini gerektirmekle birlikte dava konusu kuralın, hakkı en az sınırlayan yumuşak bir araç olduğunu söylemek mümkün değildir. Çünkü söz konusu kural, çok geniş ve adeta sınırsız bir çerçeveyi kapsayarak bireyin neredeyse her türlü özel nitelikli hassas sağlığa ve cinsel hayata ilişkin kişisel verisinin toplanması, aktarılması ve işlenmesini kapsamı dâhilinde görmektedir.

9. Kuralın, Anayasa'nın amir hükümleri gereğince genel sağlığın korunması amacına dönük olarak kamu yararı taşıdığı açıktır ancak kuralın özel hayatın gizliliği ve kişisel verilerin korunması hakları ile toplum sağlığının korunmasına yönelik önlemler arasındaki makul bir denge kurmayarak, birincisini ikincisine feda ettiğini ifade etmek mümkündür.

10. Özel hayatın gizliliği ve bu kapsamda özel nitelikli hassas kişisel verilerin korunması konusu her şeyden önce insan onuruna saygı ve kişilik haklarına dayanmaktadır. Bu hak, kişinin saygınlığını ve kişiliğini serbestçe geliştirmesini mümkün kılan şeref ve haysiyet, özel yaşam ve sağlık gibi kişisel değerler üzerindeki çıkarlarını belirterek, bireye kişiliğini dilediği şekilde, serbestçe geliştirebileceği, kendisi ve sevdikleriyle bir arada olabileceği özerk bir yaşam alanına sahip olma şansı vermektedir. Bu alanda birey, maddi ve manevi kişiliğini geliştirmek ve başkaları tarafından bilinmesini istemediği hususların güvence altına alınmasını istemek hakkına sahiptir.

11. Kişisel verilerin toplanması ve işlenmesi sırasında bireyin bu veriler üzerindeki hakkı, onun devlet veya üçüncü kişiler tarafından sıradan bir veri nesnesine indirgenmesini önlemek amacını taşımaktadır. Sağlık ve cinsel hayatla ilgili özel nitelikli hassas kişisel verilerin ilgili kişinin açık rızası olmadan toplanması, işlenmesi ve aktarılması, kişinin basit bir veri nesnesi olarak değerlendirilmesine yol açtığından insan haysiyetini zedelemektedir. Bireyin, ahlaki ve toplumsal kişiliğinin gelişiminde ve diğer insanlarla olan ilişkilerini düzenlemede önemli bir kavram olan mahremiyetin ihlali insan haysiyetinin ve kişiliğinin ihlali anlamına gelmektedir.

12. Hassas kişisel verilerin korunması kişinin maddi ve manevi varlığını geliştirmesine imkân tanıyarak, bireyin hayatını kendi özgür iradesiyle düzenlemesine katkı sağlamaktadır. Bireyin özel nitelikli hassas kişisel verileri üzerindeki hakkı yeteri kadar korunmazsa, kişiliğini serbestçe geliştirmesi zora gireceğinden, özgür iradeleriyle yaşamlarını biçimlendiren bireylerden oluşan demokratik bir toplum düzeninin ortaya çıkması ve korunması da güçleşecektir.

13. Anayasa'nın 20. maddesinde kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmekle beraber dava konusu kural sağlık ve cinsel hayatla ilgili özel nitelikli hassas kişisel verilerle ilgili olduğundan bunların toplanması, aktarılması ve işlenmesinde ilgili kişinin açık rızasının aranmaması demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırılık taşımaktadır. "Kanunda öngörülen haller" ibaresi her türlü kişisel verinin rıza olmadan işlenmesine imkân tanıyan açık bir çek olarak yorumlanmamalıdır.

14. Sonuç olarak kuralın Anayasa'nın 20. ve 13. maddelerine aykırı olduğu gerekçesiyle karara muhalif kalınmıştır.

B. Kanun'un 16. Maddesinin İkinci Fıkrasının İkinci Cümlesi Yönünden

1. İptali istenen kuralın yer aldığı maddede Kurulun gözetiminde, Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili tutulacağı ve kişisel verileri işleyen gerçek ve tüzel kişilerin veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorunda olduğu hüküm altına alınmıştır. Dava konusu kural ise işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebileceğini öngörmektedir.

2. Kişisel verileri işleyen gerçek ve tüzel kişiler veri işlemeye başlamadan önce Veri Sorumluları Siciline Kaydolmak Zorundadır. Bu sicil kişisel verilerin kimler ve hangi kuruluşlar tarafından işlendiğini gösteren bir listedir. Getirilen istisna sayesinde kuruluş kanunu ile kendisine kişisel verileri toplama yetkisi verilen kurumlar kişisel verileri toplarken kanunda düzenlendiği gerekçesiyle kişinin açık rızasını aramadan da bu işlemlerini yapabilecektir.

3. Birey kişisel verisinin kim tarafından işlendiğini görmek için veri sorumluları siciline bakmak istediğinde kanundan kaynaklanan istisnai düzenlemeden yararlanılması durumunda bunu öğrenemeyeceği gibi listede yer almayan veri sorumlusunun kişisel verileri üçüncü kişilere aktarıp, aktarmadığını da bilemeyecektir.

4. Kuralla getirilen istisna kişisel verileri işlenen kişiyi korumasız hâle getirdiğinden hukuk devleti ilkesi ile bağdaşmamaktadır. Bu nedenle Anayasa'nın 2. maddesine aykırılık taşıdığı düşüncesindeyim.

C. Kanun'un 30. Maddesinin (7) Numaralı Fıkrası ile Değiştirilen 663 Sayılı Kanun Hükmünde Kararname'nin 47. Maddesinin Birinci, İkinci ve Üçüncü Fıkraları Yönünden

Dava konusu kuralın birinci, ikinci ve üçüncü fıkralarının yukarıda (A) başlığı altında yazılan gerekçelerle Anayasa'ya aykırı olduğu kanaatine varılmıştır.

Başkanvekili - Engin YILDIRIM

KARŞI OY GEREKÇESİ

I. 24.3.2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Özel nitelikli kişisel verilerin işleme şartları" başlıklı 6 ncı maddesinin, iptal istemine konu (1) numaralı fıkrasında yer alan "...mezhebi..." ve "...kılık ve kıyafeti..." ibarelerinin, fıkrada yer alan diğer unsurlarla birlikte

“özel nitelikli (hassas) veri” olarak kabul edildiği, gerek madde metninden, gerek madde gerekçesinden anlaşılmaktadır. Kanun’un 6 ncı maddesinin (1) ve (2) numaralı fıkra metinlerinden, kişilerin “mezhebi” ve “kılık ve kıyafeti” nin, kendilerinin açık rızası olmaksızın işlenemeyeceği gibi bir anlam çıkıyorsa da, maddenin yine iptal istemine konu (3) numaralı fıkrasında sayılan birçok durumda bu kurala istisna getirilmiş ve “Kanunlarda öngörülen hallerde” kişilerin “mezhebi” ile “kılık ve kıyafetinin” de işlenebileceği hükme bağlanmıştır. Her ne sebep ve gerekçeye dayanırsa dayansın, kişilerin “mezhebi” ile “kılık ve kıyafeti” gibi hassas verilerin bir şekilde işlenmesine (kaydedilmesi, başka kurum ve birimlerle paylaşılması, kategorize edilmesi vb.) imkân tanıyan yasal düzenlemenin Anayasa’nın 2., 20., 24. ve 25. maddeleri ile bağdaştırılmasına imkân yoktur. Toplumun hassas bir yönü olan işaret edilen hususların (verilerin) değil işlenmesi, kaydının tutulması dahi Anayasaya açık aykırılıkla malüldür. Ülkemizin yakın tarihine bakıldığında da, vahim toplumsal çatışmaların çıkmasına neden olan bir konunun “kişisel veri” olarak kabulü ve geniş istisnalar tanınarak işlenmesine imkân tanınmasının hukuk devleti kavramı ile de bağdaşır bir yönü bulunmamaktadır.

Avrupa Konseyi’nin 108 sayılı “Kişisel Nitelikli Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme”sinin, (1) numaralı fıkrasında “Dini veya felsefi inançları” özel veri kabul edilmiş; ancak metinde “mezhep” kavramına yer verilmemiş; istisnaları düzenleyen (2) numaralı fıkrasında da, bu özel verilerin işlenebileceği haller arasında, iptal istemine konu (3) numaralı fıkradaki gibi geniş bir takdir yetkisi tanınmamıştır. Dolayısıyla, kuralın Avrupa Birliği ilkeleri ile uyumlu olduğundan da söz edilemez.

6 ncı maddenin iptal istemine konu (3) numaralı fıkrasında, yukarıda açıklandığı gibi hem “mezhep” ile “kılık ve kıyafet” gibi kişisel verilerin rahatça işlenmesine yol açacak istisna hükümlerine yer verilmiş, hem de “sağlık ve cinsel hayata ilişkin kişisel verilerin” bir çok halde (hemen hemen sağlık birimlerinin uygun göreceği her durumda) ilgili kişinin açık rızası aranmaksızın işlenebileceği ifade edilmiştir. Sağlık Bakanlığı ve bağlı kuruluşlarına, görevlerini yürütebilmeleri için gerekli olan bilgileri toplama, işleme, paylaşma yetkisi veren kuralın (663 sayılı KHK’nin 47. maddesinin 1, 2 ve 3 numaralı fıkralarının) iptali istemi ile açılan davada Anayasa Mahkemesi 4.12.2014 tarih ve E.2013/114, K.2014/184 sayılı kararında, şu gerekçeyle kurulların iptaline karar vermiştir: “...663 sayılı KHK’nin 47. maddesinin dava konusu (1) numaralı fıkrasıyla Bakanlık ve bağlı kuruluşlarına, mevzuatla kendilerine verilen görevleri, e-devlet uygulamalarına uygun olarak daha etkin ve daha hızlı biçimde yerine getirebilmeleri amacıyla bütün kamu ve özel sağlık kurum ve kuruluşlarından; sağlık hizmeti alanların, hizmetin gereği olarak ilgili sağlık kurum ve kuruluşuna vermek zorunda

oldukları kişisel bilgileri ve bu kimselere verilen hizmete ilişkin bilgileri her türlü vasıta ile toplama, işleme ve paylaşma yetkisi verilmektedir. Verilen yetkiyle özel hayatın ve kişisel verilerin korunması haklarına bir sınırlama getirildiği açık olup, bu sınırlama, demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır... Ancak kuralda söz konusu kişisel bilgilerin 'her türlü vasıta ile' toplanmasına, işlenmesine ve paylaşılmasına izin verilmesi, sınırlamayı, öngörülme amacının ötesinde kişisel bilgilerin gizliliğinin keyfi şekilde ihlâl edilmesi sonucunu doğurabilecek bir araca dönüştürmektedir. Bu ise sınırlama aracıyla sınırlama amacı arasında bulunması gereken makul dengeyi bozmakta, özel hayatın ve kişisel verilerin korunmasını isteme haklarına kuralda belirtilen sınırlama amacı dışında ölçüsüz bir şekilde müdahale edilebilmesine imkân tanımaktadır... 47. maddenin dava konusu (2) numaralı fıkrasında da (1) numaralı fıkrada belirtilen yöntemlerle toplanan ve işlenen verilerin, ilgili üçüncü kişiler ile kamu kurum ve kuruluşlarıyla paylaşılması öngörüldüğünden, yukarıda belirtilen aynı gerekçelerle bu düzenleme de ölçülülük ilkesini ihlâl etmektedir... 47. maddenin dava konusu (3) numaralı fıkrasında ise Bakanlık ve bağlı kuruluşlarının, mevzuatla kendilerine verilen görevleri yerine getirebilmek için gereken bilgileri, kamu ve özel ilgili bütün kişi ve kuruluşlardan istemeye yetkili olduğu ve ilgili kişi ve kuruluşların istenilen bilgileri vermekle yükümlü oldukları düzenlenmektedir. Bakanlık ve bağlı kuruluşlarına verilen görevler çok geniş bir alanı kapsamakta olup, bu görevlerin tamamının kişilerin özel hayatlarına müdahale edilmesini gerektirecek bir toplumsal zorunluluğu bünyesinde barındırdığı söylenemez. Dolayısıyla dava konusu kuralla sadece demokratik toplum düzeni yönünden zorunlu olan sınırlamalara değil, özel hayatın ve kişisel verilerin korunması haklarına yapılabilecek her türlü sınırlamaya izin verilmesi, bir başka ifadeyle, kuralda anılan haklara sınırlama getirilirken sınırlama aracının sınırlama amacına uygun ve orantılı olarak kullanılmasını temin edecek güvencelere yer verilmemesi ölçülülük ilkesine aykırı düşmektedir. Açıklanan nedenlerle dava konusu kurallar Anayasa'nın 2., 13. ve 20. maddelerine aykırıdır. İptali gerekir..." İptal istemine konu (3) numaralı fıkranın incelenmesinde, "Sağlık ve cinsel hayata ilişkin kişisel veriler" in, maddede sayılan pek çok halde, "sır saklama yükümlülüğü altında bulunan kişiler" veya "yetkili kurum ve kuruluşlar" tarafından, ilgilinin açık rızası aranmaksızın işlenebileceği hüküm altına alınmaktadır. Kural, bu haliyle, Anayasa Mahkemesinin yukarıda işaret edilen iptal kararına açıkça aykırı düştüğü gibi, kişi hakkında sağlık bilgilerine sahip olup, bunu kayıtla yükümlü olan ilgili hekim ve sağlık kuruluşu dışında merkezi bir kayıt tutma (işleme) ve bunu başka kişi veya birimlerle paylaşma gibi istisnalar (imtiyazlar) getirmesi itibarıyla Anayasa'nın 2., 13. ve 20. maddelerine aykırılıkla malûldür. Keza, kişilerin cinsel hayatına ilişkin durum ve tercihlerinin işlenmesi imkânı tanınması aynı nedenlerle Anayasa'ya aykırıdır.

II. 6698 sayılı Kanun'un "Veri sorumluları sicili" başlıklı 16 ncı maddesinin iptal istemine konu (2) numaralı fıkrasıyla, (1) numaralı fıkrada öngörülen kamuya açık "Veri sorunluları sicili" ne tüm kişisel veri işleyen gerçek ve tüzel kişilerin kaydedilmesi zorunluluğuna istisnalar getirilmekte ve işlenen kişisel verilerin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebileceği belirtilmektedir. Kişisel verileri kaydedip işleyen kimi görevliler yönünden getirilen bu istisna, ilgili görevlileri koruyacak ancak hakkındaki veriler işlenen kişileri tamamen korumasız duruma getirecek, haksız ve sübjektif nedenlerle veri işlendiği iddiasıyla yasal yolların kullanılması halinde dava edilecek bir muhatap bile bulunamayacaktır. Kişisel verilerin işlenmesi gibi çok önemli bir idari fonksiyonu ifade eden kişiler yönünden getirilen ve imtiyaz mahiyetindeki bu kuralın hukuk devleti ilkesi ile bağdaştırılabilmesi imkânı bulunmamaktadır. Dolayısıyla kural Anayasa'nın 2. maddesine aykırıdır.

III. 6698 sayılı Kanun'un 30. maddesinin (7) numaralı fıkrası ile değiştirilen 11.10. 2011 tarih ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 47. maddesi de, "Karşioy Gerekeçesi"nin (I) no'lu başlığındaki gerekçelerle Anayasa'nın, 13. ve 20. maddesine aykırı düşmektedir.

Yukarıdaki açıklanan nedenlerle, anılan kuralların iptaline karar verilmesi gerektiği kanaatine ulaştığımızdan, aksi yöndeki çoğunluk kararına katılmıyoruz.

Üye -Serdar ÖZGÜLDÜR

Üye - Serruh KALELİ

KARŞIOY YAZISI

I. GİRİŞ

1. 24.3.2016 tarihli ve 6698 sayılı Kişisel verilerin Korunması Kanunu'nun,

- 6. maddesinin (1) numaralı fıkrasında yer alan "...mezhebi..." ve "...kılık ve kıyafeti..." ibarelerinin,

- (3) numaralı fıkrasının,

- 16. maddesinin (2) numaralı fıkrasının ikinci cümlesinin,

- 30. maddesinin (7) numaralı fıkrası ile değiştirilen 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 47. maddesinin,

Anayasa'ya aykırı olmadıklarına dair çoğunluk görüşüne katılmamaktayım. Karşıoy gerekçelerim aşağıda maruzdur.

II. GENEL AÇIKLAMALAR

2. Anayasa'ya aykırılık iddiasıyla iptali istenen kuralların incelenmesi, öncelikle bahse konu kural veya kuralların anlam ve kapsamının tesbitini gerektirir. Bir kuralın, içinde yer aldığı yasanın veya diğer yasaların ilgili maddeleriyle birlikte uygulandığında Anayasa'ya aykırı sonuçlara yol açmadığının değerlendirilmesi yapılmadan, iptal talebine konu edilen kuralın Anayasa'ya uygunluğu konusunda hükme ulaşılamaz. Bir sözcük, ibare veya cümlenin, veya bir rakamın atıf yaptığı veya kapsamı itibariyle sirayet ettiği diğer kuralların, anlam ve işlerlik kazandığı veya kazandırdığı diğer kurullarla birlikte değerlendirilmesi Anayasa'ya aykırılık sonucunu ortaya koyabileceği gibi, ilk bakışta Anayasa'ya aykırı olduğu izlenimi veren bir kuralın da birlikte uygulanacağı, aynı yasadaki veya başka yasalardaki farklı hükümler nedeniyle, Anayasa'ya aykırı olmadığı sonucuna da varılabilir.

3. İnceleme konusu 6698 sayılı Kişisel Verilerin Korunması Kanunu, büyük ölçüde Avrupa Birliği mevzuatından iktibas edilmek suretiyle, sistematik bir yaklaşım içerisinde düzenlenmiştir. Kanunda amaç, kapsam ve tanımlar; kişisel verilerin işlenmesi ilkeleri ve işlenmesi şartları; haklar ve yükümlülükler; başvuru, şikayet ve veri sorumluları sicili; suçlar ve kabahatler ve nihayet, Kişisel Verileri Koruma Kurulu düzenlenmiştir. Yasadaki hükümlerin pek çoğu diğerlerine işlerlik ve anlam kazandıran veya diğerlerine istisna getiren hükümler olup, iptal istemine konu kurullar özellikle böyledir.

4. Bu nedenle, iptal istemlerine konu olan kurullar yönünden bir denetim yapabilmek için Kanunun iptal istemine konu olmayan ilgili kurullarının ve koşullarının 6698 sayılı bu Kanun'daki güvenceleri etkisiz kılıp kılmayacağı yönünden değerlendirme yapılmalıdır. Aksi halde kişisel verilerin korunması için somut ve etkili görünen düzenlemelerin içi boşaltılmış olacak, kanundaki genel ilkeler birer temenni, kurulan yeni kurullar da bürokratik ve hantal yapılardan ibaret kalabilecektir.

5. Kanunlar kamu yararı amacıyla çıkarıldığında ve ancak bir kanunun kamu yararını gerçekleştirmeye elverişli olup olmadığının denetiminin, Anayasa Mahkemesinin yetkisi dışında olduğunda kuşku yoktur. Diğer bir ifadeyle, kamu yararını gerçekleştirmeye elverişli olmayan bir kanun da yasa koyucunun takdir yetkisi içinde kalmak ve Anayasaya aykırı olmamak koşuluyla, iptal edilemeyecektir. Ancak Anayasa'nın 20. maddesinin son fıkrasında Devlete, kişisel verilerin korunmasını kanunla düzenleme yönünde bir yükümlülük getirildiğinden, bu doğrultuda yasa ile yapılacak düzenlemelerin Anayasal gerekleri karşılayıp karşılamadığının denetimi, Anayasa

Mahkemesinin yetkisi dahilindedir. Bu nedenle kişisel verilerin kaydının demokratik bir toplumda zorunlu ve ölçülü olup olmadığına, ayrıca verilerin korunması için öngörülen düzenlemelerin yeterli olup olmadığına da bakılması gerekir.

6. Anayasa'nın 20. maddesinin son fıkrası şöyledir:

"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir".

Buna göre, özel hayatın gizliliğinin korunmasını isteme hakkı kapsamında bir hak olan kişisel verilerin korunması hakkı, bir temel hak olması nedeniyle, kanunla bir müdahale söz konusu olduğunda Anayasa'nın 2. maddesindeki hukuk devleti ve 13. maddesindeki temel hak ve hürriyetlerin sınırlanması konusundaki ölçütlere tabidir. Anayasa'da "...kanunda öngörülen hallerde veya..."denilmiş olmasına bakılarak, meşru bir amaç taşımadıkça ve demokratik bir toplumda zorunlu ve ölçülü olmadıkça her türlü kişisel verinin işlenmesine yol açan kanuni düzenlemeler yapılamayacağı açıktır.

7. Öte yandan, kişisel verilerin korunmasında Anayasa'nın Eşitlik İlkesini düzenleyen 10. maddesi, Din ve Vicdan Hürriyetini düzenleyen 24. ile Düşünce ve Kanaat Hürriyetini düzenleyen 25. maddeleri, aşağıda açıklanacağı üzere konu ile doğrudan ilgilidir. Ancak 10. maddenin ve mezhep ibaresi dışında 24. maddenin ilgisiz görülmesi, kanaatimce bazı özel nitelikli veriler yönünden ciddi sakıncalara yol açacak bir sonuca varılmasına neden olmuştur.

III. İPTALİ İSTENEN KURALLARIN İNCELENMESİ

Altıncı Maddenin (1) Numaralı Fıkrasındaki "...mezhebi" İbaresinin İncelenmesi

8. (1) numaralı fıkrayla, kişilerin mezhepleri ile kılık ve kıyafetleri, "özel nitelikli kişisel veri" olarak sınıflandırılmaktadır. Özel nitelikli kişisel verinin yasada ayrı bir tanımı yer almamakla birlikte, maddenin (2) numaralı fıkrasındaki "Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır" hükmünden, özel nitelikli bir kişisel verinin, açık rıza olmaksızın işlenemeyecek veri olarak belirlendiği anlaşılmaktadır. Açık rıza ise Kanun'un 3. maddesinin (1) numaralı fıkrasına göre "Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rızayı" ifade eder.

9. Mezhepler, gerek İslam aleminde gerek ülkemizde, inkar edilemeyecek bir realitedir. Mezhepler konusu aynı zamanda son derece hassas olup, mezhep farklılıklarının körüklenmesinin toplumlar için yıkıcı sonuçlara yol açabildiği, tarihte ve bölgemizin yakın tarihinde görülmüş ve görülmektedir. Bu nedenle kişilerin mezheplerine ilişkin verilerin alenileşmesinden ve yaygınlaştırılmasından ve özellikle kamusal veri tabanlarına işlenmesinden kaçınılarak, Anayasa'nın değiştirilemeyecek hükümlerinde esasları ve nitelikleri belirlenen Türkiye Cumhuriyeti devletinin özgür ve eşit vatandaşlarının din, vicdan ve inanç alanında bırakılmalıdır.

Anayasa'nın 10. maddesinde "Kanun önünde eşitlik" ilkesi düzenlenmiştir. Buna göre "Herkes dil, ırk, renk, cinsiyet, siyasi düşünce, felsefi inanç, din, mezhep ve benzeri sebeplerle ayırım gözetilmeksizin kanun önünde eşittir". Bu ilkeyle kişiler arasındaki eşitlik güvence altına alınmakta, aynı zamanda hem kişilere hem de Devlete ayırımcılık yasağı getirilmektedir.

Anayasa'nın 24. maddesinin birinci fıkrasında herkesin vicdan, dini inanç ve kanaat hürriyetine sahip olduğu; maddenin üçüncü fıkrasında da kimsenin ibadete, dini ayin ve törenlere katılmaya, dini inanç ve kanaatlerini açıklamaya zorlanamayacağı, dini inanç ve kanaatlerinden dolayı kınanamayacağı ve suçlanamayacağı belirtilmiştir.

10. Çoğunluk gerekçesinde iptali istenen kuralın, her ne kadar kişinin mezhebinin özel nitelikli veri sayılmasını ve böylece bu verinin ancak kişinin açık rızasıyla işlenebileceğini öngörmek suretiyle daha üst bir koruma sağladığı ve bu suretle toplanacak verilerin kişilerin ayırımcılığa uğramasına neden olabilecek alanlarda ihtiyaçların belirlenmesi, boşluk ve eksikliklerin giderilmesi gibi konularda önemli olacağı belirtilmekteyse de, somutluk taşımayan, farazi ihtiyaçların, temel bir hakka yani kişisel mezhep bilgilerine yapılacak somut bir müdahale bakımından Anayasa'nın 13. maddesinde güvence altına alınan "demokratik bir toplumda zorunlu olmak" ve "ölçülülük" ilkelerini karşıladığından söz edilemez. Zira çoğunluk gerekçesinde belirtilen türden ihtiyaçlar için kişisel verilerin kaydedilmesi zorunlu olmayıp, verilerin anonim olarak işlenmesiyle de aynı sonuçlar elde edilebilecektir. Mezhebin, kişinin açık rızası aranmaksızın veri olarak işlenebilmesi meşru bir amaca dayanmalıdır. İnanç alanında kalan ve ancak kişinin kendisinin bilebileceği mezhep, esas itibarıyla ancak kişinin açık rızasının varlığı halinde kaydedilebilecek bir veridir. Kişinin mezhebi ve dini inançları, o mezhebin ibadet yerleri veya mezhebi tören ve ritüeller gibi, kamusal alana sirayet eden konularda dahi, ilgilinin açık rızası olmadan kaydedilemez. Zira kişinin sadece bir mezhebin ibadet yerlerine gitmesi veya törenlerine katılması dahi kişinin mezhebinin kendi rızası hilafına kaydedilmesi için yeterli değildir. Anayasa'nın 24. maddesi buna engeldir. Bu nedenle, mutlak ayırımcılık yasağı bulunan ve Devleti ilgilendirebilecek yönleri çok sınırlı olan bir konuda, kanunla

genel bir ifadeyle mezhep verilerinin işlenebileceğinin öngörülmesinin Anayasa'ya uygun olmadığı açıktır.

11. 6698 sayılı Kanun'un 6. maddesinin (3) numaralı fıkrasında yapılan düzenleme ile, görünüşte özel veri sayılarak daha yüksek bir koruma sağlanan mezhep verileri, kişinin açık rızası aranmaksızın işlenemeyecek veriler arasından çıkartılmıştır. Maddenin (3) numaralı fıkrasının birinci cümlesinde "Birinci fıkrada sayılan ... kişisel veriler, kanunlarda öngörülen hallerde, ilgili kişinin açık rızası aranmaksızın işlenebilir" denilmiş olup, mezhep de birinci fıkrada sayılan bu kişisel veriler arasında yer almaktadır. Tabir caizse aynı madde içindeki düzenlemelerle bir elle verilen diğer elle geri alınmakta, "mezhep" verisinin korunmasına yönelik en önemli güvence yani "açık rıza" esas ortadan kaldırılmaktadır.

12. Mezhep verilerinin yine de özel nitelikli veri sayılması nedeniyle Kanunda öngörülen düzenlemeler kapsamında uygulanabilecek daha üst bir korumadan yararlanabileceği, bu nedenle yasadaki düzenlemenin bütünüyle anlamsız olmadığı şeklindeki gerekçelere katılmak mümkün değildir. Zira, Maddenin (4) numaralı fıkrasında özel nitelikli veriler için Kurulca (Kişisel Verileri Koruma Kurulu) belirleneceği öngörülen önlemlerin yeterli olmadığı görülmektedir.

6698 sayılı Kanun'un 22. maddesinin (1) numaralı fıkrasının (ç) bendinde Kurula, "Özel nitelikli kişisel verilerin işlenmesi için aranan yeterli önlemleri belirlemek" görev ve yetkisi verilmiştir. Yeterli önlemlerin neler olabileceği hakkında kanunla ilke ve esaslar belirlenmeden, çerçevesi çizilmeden idareye ucu açık, belirsiz, etkili olup olmayacağı şüpheli bir yetkinin verilmiş olması, Anayasa'nın öngördüğü anlamda kanunla düzenleme sayılamayacağından, yeterli kanuni güvenceleri de içermeden kişisel verilere müdahale imkanı veren iptal istemine konu düzenlemenin Anayasa'nın 20. maddesine uygun olmadığı açıktır.

13. Sonuç olarak eşitlik ilkesi ve ayrımcılık yasağı gereği, ilgilinin açık rızası olmadıkça her hangi bir eylem, işlem veya uygulamaya konu yapılamayacak olan mezhep bilgisinin işlenmesinin, Anayasa'nın 13. maddesindeki esaslara aykırı olarak kanunla öngörülemeyeceği açıktır. Bu nedenle kural, Anayasa'nın 2. maddesindeki hukuk devletine, 3. maddesindeki millet bütünlüğüne ve ayrıca 10. ve 24. maddelerine aykırıdır.

"...kılık ve kıyafeti..." İbaresinin İncelenmesi

14. Kılık ve kıyafet, kişinin inançları gereği benimsediği belirli bir giyim tarzı olabileceği gibi, her hangi bir siyasi veya felsefi anlam taşımaksızın, sırf kişinin özel yaşamı kapsamındaki bir tercihten ibaret de olabilir. Ayrıca, kişi, kılık ve kıyafetini her zaman serbestçe değiştirebilmek hakkına da

sahiptir. Kılık ve kıyafetin tercihindeki nedenler tamamen kişinin iç alemine ait olup, Anayasa'nın 24. ve 25. maddelerinde güvence altına alınan hürriyetlerle yakın ilgisi bulunan bu bilgilerin işlenmesinde ancak çok açık zorunluluk bulunmalı ve bahse konu özgürlüğe yapılacak müdahale ölçülü olmalıdır.

15. Kılık ve kıyafetin, kişinin açıkça görülebilen bir özelliği olması, bu verinin işlenmesi için kişinin rızasının bulunduğu anlamına gelmemektedir. Esasen 6698 sayılı Kanun'un 3. maddesinin (1) numaralı fıkrasının (a) bendinde "açık rıza"nın, belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rızayı ifade ettiği belirtilmektedir. Bu nedenle, iptali istenen kuralla kılık ve kıyafetin, özel nitelikli yani açık rıza olmadıkça işlenemeyecek veri kapsamına alan bir düzenleme konusu yapılmış olması, bu temel hak ve özgürlük yönünden ek bir güvence getirmemiştir.

16. Öte yandan, "...mezhebi..." ibaresi ile ilgili olarak Anayasa'nın 2., 3., 10., 13., 20., 24. ve 25. maddeleri bağlamında yukarıda belirtilen Anayasa'ya aykırılık gerekçeleri, "...kılık ve kıyafeti..." yönünden de aynen geçerlidir.

Altıncı Maddenin (3) Numaralı Fıkrasının Birinci Cümlesi

17. Bahse konu birinci cümle şöyledir:

"Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebilir".

Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki veriler ise şunlardır:

"Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, ... ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri..."

18. Buna göre, daha önce incelenen mezhep ve kılık kıyafet hariç tutulursa, kişinin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, diğer inançları, dernek, vakıf ya da sendika üyeliği, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri, biyometrik ve genetik verileri kişinin açık rızası olmaksızın işlenebilecektir.

Verilerden bir kısmı esasen işlenmesinde zorunluluk bulunan, kişinin özel yaşamının yanı sıra kamusal alanı da ilgilendiren verilerdir. Bunlar; dernek, vakıf ya da sendika üyeliği, ceza mahkumiyeti ve güvenlik tedbirleridir. Bu nedenle bu veriler ayrı bir kategori halinde değerlendirilebilir. Kuşkusuz, bu tür verilere ilişkin işlemlerde de yine Anayasa'nın 13. maddesi esasları gözetilmek zorundadır.

Diğer taraftan, kişinin ırkı, etnik kökeni, dini, siyasi düşüncesi ve diğer inançları somut olarak tesbit edilemeyecek verilerdir. Din, siyasi ve diğer inançlar ise tamamen kişinin iç alemine ilişkin ve yine kişinin serbest iradesiyle her zaman değişebilecek verilerdir. Bu nedenle bunların, kişinin açık rızası dışında diğer kişiler veya devlet tarafından işlenmesi, tahmin, yakıştırma ve yaftalamadan öteye gidemez. Bu veriler mahiyetleri icabı, açık rıza dışında işlenebilecek veriler değildir.

Mezhep ve kılık-kıyafet konusunda daha önce belirtilen Anayasaya aykırılık gerekçeleri, ırk, etnik köken, dini ve diğer inançlar, siyasi ve felsefi düşünceler yönünden de aynen geçerlidir.

20. Fıkranın iptali istenen birinci cümlesinin yaptığı atıfla, -Anayasa'ya aykırı olarak- açık rıza aranmaksızın işlenebilir veri haline getirilen konuların tahdidi olarak sayıldıkları anlaşılmaktadır. Halbuki bunlar arasında birinci fıkrada sayılmayan ancak, kişinin rızası dışında işlenmesi halinde kişinin maddi ve manevi mağduriyetine neden olabilecek, daha pek çok veri kategorisi saymak mümkündür (kişinin merakları, hobileri, yeme içme ve tüketim alışkanlıkları, hoşlandığı ve hoşlanmadığı kişi ve konular ve bunun gibi sayılamayacak kadar çok, özel hayat kapsamındaki veriler). İptali istenen kuralla, bunlara ilişkin tüm veriler de açık rıza aranmaksızın kanunla işlenebilecek veriler haline getirilmektedir.

21. Özetle, 6. maddenin (1) numaralı fıkrasıyla bazı kişisel veriler özel nitelikli yani kişinin açık rızası olmaksızın işlenemeyecek veri olarak düzenlenir ve böylece üst düzey bir korumaya kavuşturulur gözükmektedir, aynı maddenin (3) numaralı fıkrasının birinci cümlesi ile bu kapsamdan çıkartılmakta; diğer her türlü kişisel veriler ise açık rıza şartı aranmaksızın kanunla işlenebilir veri haline getirilmektedir. Bu şekilde kanundaki düzenlemelerle, Anayasa'nın 20. maddesinde öngörülen ve Anayasanın diğer hükümleri ile birlikte değerlendirilmesi gereken "kanunla düzenleme" ile "açık rıza" koşullarından "kanunla düzenlemeye mutlak üstünlük verilip, "açık rıza" şartının etkisiz hale getirdiği, Anayasa'da üstün kamu yararı ile kişi hak ve özgürlükleri arasında kurulması gereken makul ve adil dengenin bozulduğu anlaşılmaktadır.

Bu nedenle iptali istenen kurallar Anayasa'nın 2., 10., 20., 24. ve 25. maddelerine aykırıdır.

Altıncı Maddenin (3) Numaralı Fıkrasının İkinci Cümlesinin ve 30. Maddenin (7) Numaralı Fıkrası ile Değiştirilen 663 Sayılı KHK'nin 47. Maddesinin İncelenmesi

22. Bahse konu (3) numaralı fıkranın ikinci cümlesinde, "Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama

yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir” denilmektedir.

663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 47. maddesinin (1) numaralı fıkrasında sağlık hizmeti almak üzere kamu veya özel sağlık kuruluşları veya sağlık mesleği mensuplarına müracaat edenlerin, sağlık hizmetinin gereği olarak vermek zorunda oldukları veya hizmete ilişkin kişisel verilerin işlenebileceği, (2) numaralı fıkrasında sağlık hizmetinin verilmesi, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetlerinin planlanması ve maliyetinin hesaplanması amacıyla Sağlık Bakanlığının birinci fıkra kapsamında elde edilen verileri alarak işleyebileceği, (3) numaralı fıkrasında Bakanlığın bu verilere ilgili kişilerin erişimini sağlayacak bir sistem kuracağı, (4) numaralı fıkrasında üçüncü fıkraya göre kurulan bu sistemlerin güvenliği ve güvenilirliği ile ilgili standartların Kişisel Verileri Koruma Kurulu'nun belirlediği ilkelere uygun olarak Bakanlıkça belirleneceği, Bakanlığın verilerin güvenliğinin sağlanması amacıyla sisteme kayıtlı bilgilerin hangi görevli tarafından ne amaçla kullanıldığının denetlenmesine imkan tanıyan bir güvenlik sistemi kuracağı, (5) numaralı fıkrasında sağlık kurum ve kuruluşları ile özel kişilerin istihdam ettikleri personeli ve personel hareketlerini Bakanlığa bildirmekle yükümlü olduğu, (6) numaralı fıkrasında ise sağlık verilerinin işlenmesi ve güvenliği ile ilgili hususların Bakanlıkça yürürlüğe konulacak yönetmelikle düzenleneceği belirtilmiştir.

23. Buna göre, 6698 sayılı Kanun'un 6. maddesinin (3) numaralı fıkrasının ikinci cümlesinde sağlık ve cinsel hayata ilişkin verilerin ilgililerin açık rızası aranmaksızın işlenmesinin hangi amaçlarla gerçekleştirilebileceği düzenlenmiş, 30. maddesi ile düzenlenen 663 sayılı KHK'nin 47. maddesinde ise verilerin alınması ve güvenliği ile ilgili olarak Sağlık Bakanlığının görev ve yetkileri belirlenmiştir. Başka bir deyişle, sağlık ve cinsel hayata ait veriler sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenemeyecek olmakla birlikte, verilerin korunması için gerekli düzenlemeleri yapmak ve birtakım önlemler almakla sadece Sağlık Bakanlığı görevlidir.

24. Bu durumda, kapsamı belli olmayan “yetkili kurum ve kuruluşlar” tanımı altında gerek idarenin farklı birimlerine gerek yetkilendirilebilecek diğer özel kurum ve kuruluşlara, ilginin açık rızası aranmaksızın cinsel hayata ait verileri işleme yetkisi verilebileceği, ancak bunların Sağlık Bakanlığına bağlı olmamaları nedeniyle Sağlık Bakanlığının verileri koruma yükümlülüğü kapsamında alacağı önlemleri uygulamak zorunda olup olmayacakları konusunda belirsizlik bulunduğu anlaşılmaktadır.

25. Kurallar birlikte değerlendirildiğinde; bir kısım meşru amaçlar belirtilmek ve verilerin korunmasına ilişkin güvenceler getirilmek suretiyle kamusal üstün yararlar ve kişi hak ve hürriyetlerinin sınırlandırılması arasında makul bir denge kurulmaya çalışılmış ise de kuralların bunu sağlayamadığı, bu nedenle iptali istenen hükümlerin Anayasanın 20. maddesine aykırı oldukları anlaşılmaktadır.

Anayasa Mahkemesinin 4.12.2014 tarihli ve Esas:2013/114, Karar:2014/184 sayılı kararında kişisel verilerle ilgili bazı kuralların iptaline karar verilirken, Sağlık Bakanlığı ve bağlı kuruluşlarına verilen görevlerin çok geniş bir alanı kapsadığı, ilgili kurullarla öngörülen veri toplama görevlerinin toplumsal bir zorunluluğu bünyesinde barındırdığının söylenemeyeceği belirtilmiştir. Anayasa Mahkemesi ayrıca bahse konu düzenlemelerde öngörülen güvenceleri de yeterli bulmamıştır. Bu kere incelenen kurullarda da aynı durumun devam ettiği anlaşılmaktadır. Nitekim, "... kamu sağlığının korunması, koruyucu hekimlik, ... sağlık hizmetleri ile finansmanının planlanması ve yönetimi ..." gibi görevlerin sağlık ve özellikle cinsel hayata ilişkin kişisel verilerin işlenmesini zorunlu kıldığından ve bu verileri korumak amacıyla getirilen düzenlemelerin açık, net ve etkili olduğundan söz edilemez.

26. Sonuç olarak, iptali istenen kurullar, kişinin sağlık ve özel hayatın en mahrem alanı olan cinsel hayatına ait verilerinin işlenmesi ve korunması konusunda yeterli yasal dayanakları ortaya koymayan, kamu yararı ile kişi hak ve hürriyetleri arasında Anayasal ölçütlere göre kurulması gereken adil ve makul dengeyi kişi aleyhine bozan, Anayasa'nın 20. maddesinde güvence altına alınan temel haklara yapılmış ölçüsüz bir müdahaledir.

Onaltıncı Maddenin (2) Numaralı Fıkrasının İkinci Cümlesi

27. İptal istemine konu cümle şu şekildedir:

"Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir."

Veri Sorumlusu, 6698 sayılı Kanun'un 3. maddesinin (1) numaralı fıkrasının (1) bendinde "Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder" şeklinde tanımlanmıştır. Kanun'un 10. maddesine göre veri sorumlusunun, kişisel verilerin elde edilmesi sırasında ilgili kişileri ayrıntılı biçimde aydınlatması gerekmekte, yine Kanun'un 12. maddesine göre veri güvenliğine ilişkin yükümlülükleri ve sorumlulukları bulunmaktadır. Kanun'un 13. maddesinde, kişilerin, veri sorumlusuna, kanuni yükümlülük ve sorumluluklarıyla ilgili taleplerini iletebilecekleri, talebin

yerine getirilmemesi halinde Kurula şikayette bulunabilecekleri belirtilmiş ve bunun yöntemleri ile süreleri düzenlenmiştir.

Veri Sorumluları Sicili, Kanun'un 16. maddesinin (1) numaralı fıkrasına göre, Kurulun gözetiminde "kamuya açık olarak" tutulacaktır.

28. İptal isteminin reddine ilişkin çoğunluk gerekçesinde veri sorumlularının yükümlülükleri bakımından bunların sicile kayıtlı olup olmadıklarının bir önemi bulunmadığı ifade edilmiş ise de bu görüşe katılmak mümkün değildir. Zira kişilerin veri sorumlularına kolayca ulaşmaları, verilerin korunması bakımından en önemli güvencelerden biri olup, Kurulun kendi takdirine göre bazı veri sorumlularına sicil muafiyeti getirmesi, Kanun'da kişiler lehine tanınan hakların birçoğunun kullanılmasını güçleştirecek, veri gizliliğinin ihlali halinde sorumluların takibini engelleyecek, veri güvenliğine ilişkin kurulan sistemlerin ve kanuni güvencelerin etkisizleşmesine yol açabilecektir.

29. Bugünkü teknolojik gelişmeler doğrultusunda maliye, vergi, sigorta, bankacılık gibi işlemlerde en küçük veriler dahi kolayca işlenebilir ve binlerce terabayt hacminde veriler muhafaza edilebilirken, veri sorumlularının tam bir sicilinin tutulamayışı için her hangi bir nesnel güçlük ve haklı neden söz konusu olamaz. Bu nedenle sırf gerek bulunmadığı düşüncesiyle bazı veri sorumlularının sicilden muaf tutulmasının, Anayasa'nın 20. maddesinde yer alan kişisel verilerin korunmasını isteme hakkının "bilgilendirilme, bu verilere erişme, bunların düzeltilmesini ve silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme" unsurları yönünden ağır biçimde zedelenmesine yol açan, ölçsüz bir düzenleme olduğu, dolayısıyla Anayasa'ya aykırı olduğu açıktır.

Yukarıda belirtilen nedenlerle çoğunluk görüşlerine katılmamaktayım.

Üye - Osman Alifeyyaz PAKSÜT

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2020/67

Karar Sayısı: 2022/139

Karar Tarihi: 9/11/2022

R.G. Tarih - Sayı: 30/3/2023 - 32148

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri Engin ALTAY, Özgür ÖZEL ve Engin ÖZKOÇ ile birlikte 134 milletvekili

İPTAL DAVASININ KONUSU: 16/6/2020 tarihli ve 7246 sayılı Rekabetin Korunması Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun'un;

A. 3. maddesiyle 7/12/1994 tarihli ve 4054 sayılı Rekabetin Korunması Hakkında Kanun'un 9. maddesinin değiştirilen birinci fıkrasının birinci cümlesinin "...ve teşebbüslerin belirli faaliyetlerini yahut ortaklık paylarını ya da mal varlıklarını devretmeleri şeklindeki yapısal tedbirleri..." bölümünün,

B. 4. maddesiyle 4054 sayılı Kanun'un 15. maddesinin birinci fıkrasının değiştirilen (a) bendinde yer alan "...bunların kopyalarını ve fiziki örneklerini alabilir," ibaresinin,

C. 6. maddesiyle 4054 sayılı Kanun'un 34. maddesine eklenen üçüncü fıkranın,

Ç. 12. maddesiyle 4054 sayılı Kanun'a eklenen geçici 6. maddenin birinci fıkrasının;

1. Birinci cümlesinin "...Kurum danışmanı, Başkan danışmanı, idari koordinatör, müdür, araştırma uzmanı, basın danışmanı, sistem çözümleyici, veri iletişim uzmanı, programcı, idari hizmet yetkilisi ve idari hizmet uzmanı kadrolarında bulunanlar araştırmacı kadrolarına;..." bölümünün,

2. Dördüncü cümlesinin,

Anayasa'nın 2., 7., 13., 20., 35., 36., 48., 90., 123., 128., 153. ve 167. maddelerine aykırılığı ileri sürülerek iptaline ve yürürlüklerinin durdurulmasına karar verilmesi talebidir.

I. İPTALİ İSTENEN KANUN HÜKÜMLERİ

Kanun'un iptali talep edilen kuralların da yer aldığı;

1. 3. maddesiyle 4054 sayılı Kanun'un birinci fıkrası değiştirilen 9. maddesi şöyledir:

“İhlale Son Verme

Madde 9- (Değişik birinci fıkra:16/6/2020-7246/3 md.) Kurul; ihbar, şikâyet ya da Bakanlığın talebi üzerine veya resen bu Kanunun 4 üncü, 6 ncı veya 7 nci maddelerinin ihlal edildiğini tespit ederse, ilgili teşebbüs veya teşebbüs birliklerine rekabetin tesisi için yerine getirilmesi ya da kaçınılması gereken davranışları ve teşebbüslerin belirli faaliyetlerini yahut ortaklık paylarını ya da mal varlıklarını devretmeleri şeklindeki yapısal tedbirleri nihai kararında bildirir. Davranışsal ve yapısal tedbirler, ihlale orantılı ve ihlalin etkili biçimde sona erdirilmesi için gerekli olmalıdır. Yapısal tedbirlere ancak daha önce getirilen davranışsal tedbirlerin sonuç vermediği hallerde başvurulur. Davranışsal tedbirlerin sonuç vermediğinin nihai kararla tespit edilmesi halinde ilgili teşebbüs veya teşebbüs birliklerine yapısal tedbire uyması için en az 6 ay süre verilir.

Meşru bir menfaati olan gerçek ve tüzelkişiler şikayette bulunabilir.

Kurul, birinci fıkraya göre bir karar almadan önce ilgili teşebbüs veya teşebbüs birliklerine ihlale ne şekilde son vereceklerine ilişkin görüşlerini yazılı olarak bildirir.

Kurul, nihai karara kadar ciddi ve telafi olunamayacak zararların ortaya çıkma ihtimalinin bulunduğu durumlarda, ihlalden önceki durumu koruyucu nitelikte ve nihai kararın kapsamını aşmayacak şekilde geçici tedbirler alabilir.”

2. 4. maddesiyle 4054 sayılı Kanun’un birinci fıkrasının (a) bendi değiştirilen 15. maddesi şöyledir:

“Yerinde İnceleme

Madde 15- Kurul, bu Kanunun kendisine verdiği görevleri yerine getirirken gerekli gördüğü hallerde, teşebbüs ve teşebbüs birliklerinde incelemelerde bulunabilir. Bu amaçla teşebbüslerin veya teşebbüs birliklerinin:

a) (Değişik:16/6/2020-7246/4 md.) Defterlerini, fiziki ve elektronik ortam ile bilişim sistemlerinde tutulan her türlü verilerini ve belgelerini inceleyebilir, bunların kopyalarını ve fiziki örneklerini alabilir,

b) Belirli konularda yazılı veya sözlü açıklama isteyebilir,

c) Teşebbüslerin her türlü mal varlığına ilişkin mahallinde incelemeler yapabilir.

İnceleme, Kurul emrinde çalışan uzmanlar tarafından yapılır. Uzmanlar incelemeye giderken yanlarında incelemenin konusunu, amacını ve yanlış bilgi verilmesi halinde idari para cezası uygulanacağını gösteren bir yetki belgesi bulundurlar.

(Ek fıkra: 1/8/2003-4971/25 md.) İlgililer istenen bilgi, belge, defter ve sair vasıtaların suretlerini vermekle yükümlüdür. Yerinde incelemenin engellenmesi veya engellenme olasılığının bulunması durumunda sulh ceza hakimi kararı ile yerinde inceleme yapılır.”

3. 6. maddesiyle 4054 sayılı Kanun’un üçüncü fıkranın eklendiği 34. maddesi şöyledir:

“Kurum Personelinin Statüsü

Madde 34 – (Değişik cümle:16/6/2020-7246/6 md.) Kurum hizmetlerinin gerektirdiği asli ve sürekli görevleri yürüten personelin kadroları ekli (I) sayılı Cetvelde gösterilmiştir. Kurum emrinde yeteri kadar uzman meslek personeli ile kariyer dışı ihtisas personeli çalıştırılabilir.

Kurum personeli ücret ve mali haklar dışında 657 sayılı Devlet Memurları Kanununa tabidir. (İptal ikinci ve üçüncü cümleler: Anayasa Mahkemesinin 6/6/2013 tarihli ve E.: 2013/47, K.: 2013/72 sayılı Kararı ile.) (...)

(Ek fıkra:16/6/2020-7246/6 md.) Ekli (I) sayılı Cetveldeki toplam kadro sayısını geçmemek ve mevcut kadro unvanları veya 10/7/2018 tarihli ve 2 sayılı Genel Kadro ve Usulü Hakkında Cumhurbaşkanlığı Kararnamesi eki cetvellerde yer alan kadro unvanları ile sınırlı olmak kaydıyla hizmet sınıfı, kadro, unvan ve derecelerin değiştirilmesi ile bu kadroların kullanılmasına ilişkin usul ve esasları belirlemeye Kurul yetkilidir.

Geçicilik veya belli bir ihtisas gerektiren nitelikteki hizmetler Başkanlıkça tespit olunur. Bu işlerde çalışacak personel hakkında vekalet veya istisna akdi hükümleri uygulanır. Bu fıkraya göre istihdam edileceklerden sosyal güvenlik kuruluşlarından almakta oldukları aylıkları kesilmez.

Yabancı uzmanlar da Başkanlığın hazırlayıp Kurulun onayı ile yürürlüğe konacak yönetmelik esaslarına göre istihdam edilebilir.”

4. 12. maddesiyle 4054 sayılı Kanun’a eklenen geçici 6. maddenin birinci fıkrası şöyledir:

“Bu maddenin yürürlüğe girdiği tarihte Kurumda inceleme uzmanı kadrosunda bulunanlar rekabet uzmanı kadrolarına ve kıdemli koordinatör ile mesleki koordinatör kadrosunda bulunanlar rekabet başuzmanı kadrolarına; Kurum danışmanı, Başkan danışmanı, idari koordinatör, müdür, araştırma uzmanı, basın danışmanı, sistem çözümleyici, veri iletişim uzmanı, programcı, idari hizmet yetkilisi ve idari hizmet uzmanı kadrolarında bulunanlar araştırmacı kadrolarına; garaj şefi kadrosunda bulunanlar şoför kadrosuna başkaca bir işleme gerek kalmaksızın kadro dereceleriyle atanmış sayılır. Bu şekilde atananların eski kadrolarına bağlı olarak en son ayda fiilî çalışmaya bağlı ödemeler hariç mali haklar kapsamında yapılan her türlü ödemeler toplamı net tutarının (bu tutar sabit bir değer

olarak esas alınır), atandıkları yeni kadrolarına bağılı olarak fiilî çalışmaya bağılı ödemeler hariç mali haklar kapsamında yapılan her türlü ödemeler toplamı net tutarından fazla olması halinde aradaki fark tutarı, herhangi bir vergi ve kesintiye tabi tutulmaksızın fark kapanıncaya kadar ayrıca tazminat olarak ödenir. Atandıkları kadro unvanında isteğe bağılı olarak herhangi bir deęişiklik olanlarla kendi istekleriyle başka kurumlara atanana fark tazminatı ödenmesine son verilir. Araştırmacı kadrosuna atanana Kurumca ihtiyaç duyulan işlerde görevlendirilir.”

II. İLK İNCELEME

1. Anayasa Mahkemesi İctüzüğü hükümleri uyarınca Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Serdar ÖZGÜLDÜR, Burhan ÜSTÜN, Engin YILDIRIM, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĞLU, Selahaddin MENTEŞ ve Basri BAĞCI'nın katılmalarıyla 10/9/2020 tarihinde yapılan ilk inceleme toplantısında dosyada eksiklik bulunmadığından işin esasının incelenmesine, yürürlüğü durdurma talebinin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

III. ESASIN İNCELENMESİ

2. Dava dilekçesi ve ekleri, Raportör Alparslan KOÇAK tarafından hazırlanan işin esasına ilişkin rapor, dava konusu kanun hükümleri, dayanılan Anayasa kuralları ve bunların gerekçeleri ile dięer yasama belgeleri okunup incelendikten sonra gereęi görüşülüp düşünöldü:

A. Genel Açıklama

3. Serbest piyasa ekonomisinin benimsendięi toplumlarda her teşebbüs, kârını en üst düzeye çıkarmak için elindeki kıt üretim faktörlerini hangi mal veya hizmet üretiminde kullanacağına ve mal veya hizmetleri ne miktarda üretilip dięer ürünlerden hangi yöntemlerle farklılaştırarak hangi fiyata satacağına karar vermektedir. Bu kararların alınma sürecinde tüm teşebbüslerin özgür ve birbirleriyle yarış hâlinde, bir başka deyişle rekabet içinde olmaları gerekir. Nitekim rekabet; piyasaya sürülen malların miktarının artmasına, fiyatların düşmesine, malların kalitesinin yükselmesine ve bu suretle toplumun daha geniş kesiminin daha çok, daha ucuz ve kaliteli mal edinmesine imkân sağlar. Dolayısıyla rekabet tüketicilerin yararınadır.

4. Teşebbüsler kârlarını en üst düzeye çıkarma amacı çerçevesinde teknolojik gelişme ve taşıma maliyetlerindeki deęişikliklerin eşlik ettięi küreselleşme nedeniyle piyasalarda güçlü konuma gelme, çevre ya da istihdam duyarlılığı nedeniyle oluşan mevzuat deęişikliklerine uyum sağlama, yeni bir ürün ya da coęrafi pazara girme, iflas etme risklerinden kurtulma gibi nedenlerle rekabeti sınırlayıcı

anlaşmalara, birbirleriyle uyumlu davranışlara, pazardaki egemenliklerini kötüye kullanma yoluna, birleşme veya devralmaya başvurabilmektedirler. Söz konusu uygulama ve işlemlerin üretilen ürün miktarı ve çeşidinin artması, fiyatların düşmesi, pazarlamanın etkinleşmesi, araştırma ve geliştirmeye daha fazla kaynak aktarılması, dağıtım ve personel verimliliğinin, uluslararası piyasalardaki rekabet gücünün ve tüketicinin refahının artması gibi olumlu sonuçları olabilir. Ancak bu durum, etkin rakiplerin sayılarının azalması, pazara girişin engellenmesi, üretim ve pazarlamada yenileşme güdüsünün azalması, tüketici tercihlerindeki seçeneklerin azalması, fiyatların artması gibi olumsuz sonuçlar da doğurabilir.

5. Bu kapsamda mal ve hizmet piyasalarındaki rekabeti engelleyici, bozucu veya kısıtlayıcı anlaşma, karar ve uygulamaları ve piyasaya hâkim olan teşebbüslerin bu hâkimiyetlerini kötüye kullanmalarını önlemek, bunun için gerekli düzenleme ve denetlemeleri yaparak rekabetin korunmasını sağlamak amacıyla 4054 sayılı Kanun kabul edilmiştir.

6. Anılan Kanun'un "Tanımlar" başlıklı 3. maddesinde teşebbüs (işletme), 13/1/2011 tarihli ve 6102 sayılı Türk Ticaret Kanunu'nun 11. maddesi ile diğer mevzuatta yer alan tanımlardan daha geniş şekilde ve Avrupa Birliği Komisyonunun yorumuyla uyumlu olarak "Piyasada mal veya hizmet üreten, pazarlayan, satan gerçek ve tüzelkişilerle, bağımsız karar verebilen ve ekonomik bakımdan bir bütün teşkil eden birimler..." biçiminde tanımlamıştır. Bir başka deyişle tek gerçek kişi tarafından işletilenden büyük ölçekli sanayi şirketlerine kadar ticari ve ekonomik faaliyetlerde bulunan bütün ekonomik varlıklar 4054 sayılı Kanun uygulamasında teşebbüs olarak kabul edilmiştir.

7. Anılan Kanun'un 3. maddesinde ise teşebbüs birlikleri "Teşebbüslerin belirli amaçlara ulaşmak için oluşturduğu tüzelkişiliği haiz ya da tüzelkişiliği olmayan her türlü birlikler..." şeklinde tanımlanmıştır. Söz konusu tanım uyarınca kanunla veya iradi olarak kurulmaları, özel hukuk veya kamu hukuku tüzel kişisi olmaları ya da tüzel kişiliklerinin bulunup bulunmadığı önem taşımaksızın katılan teşebbüslerin kararlarına uyduğu tüm birlikler teşebbüs birlikleri olarak kabul edilmiştir.

B. Kanun'un 3. Maddesiyle 4054 Sayılı Kanun'un 9. Maddesinin Değiştirilen Birinci Fıkrasının Birinci Cümlesinin "...ve teşebbüslerin belirli faaliyetlerini yahut ortaklık paylarını ya da mal varlıklarını devretmeleri şeklindeki yapısal tedbirleri..." Bölümünün İncelenmesi

1. Anlam ve Kapsam

8. 4054 sayılı Kanun'un 4. maddesiyle teşebbüslerin aralarında gizli veya açık anlaşma yapmak suretiyle oluşturdukları birliklerinin kararlarıyla ya da birlikte davranarak piyasada rekabeti sınırlamaları, 6. maddesiyle teşebbüslerin ülkenin bütününde ya da bir bölümünde bir mal veya

hizmet piyasasındaki hâkim durumunu tek başına yahut başkalarıyla yapacağı anlaşmalarla ya da birlikte davranarak kötüye kullanmasıyla rekabeti kısıtlaması yasaklanmıştır. Anılan Kanun'un 7. maddesiyle de ülkenin bütününde ya da bir kısmında herhangi bir mal veya hizmet piyasasındaki etkin rekabetin önemli ölçüde azaltılması, hâkim durum yaratılması ya da mevcut hâkim durumun güçlendirilmesi sonucunu doğuracak şekilde teşebbüslerin birleşmeleri veya herhangi bir teşebbüsün ya da kişinin diğer bir teşebbüsün mal varlığını yahut ortaklık paylarının tümünü veya bir kısmını ya da kendisine yönetimde hak sahibi olma yetkisi veren araçları, miras yoluyla iktisap durumu hariç olmak üzere, devralması yasaklanmış ve teşebbüslerin belirli bir ölçek ve etkide birleşme ve devralmaları Rekabet Kurulunun (Kurul) iznine tabi tutulmuştur.

9. Kanun'da, anılan maddelerdeki yasaklara uyulmaması hâlinde uygulanacak yaptırımlar düzenlenmiş ve bu konuda araştırma, soruşturma ve yaptırımlara karar verme yetkisi Kurula verilmiştir. Kurul kararlarına karşı ise idare mahkemelerine başvurma imkânı tanınmıştır.

10. Söz konusu idari yaptırımların uygulanması ilgili mal veya hizmet piyasasındaki rekabetin yeniden tesisini mümkün kılmayabilir. Bu takdirde idari yaptırımların uygulanması yerine ihlale konu işlem ve eylemlerin rekabeti kısıtlayıcı etkilerini ortadan kaldırmaya yönelik tedbirlerin alınmasına karar verilebilir.

11. Bu bağlamda "İhlale Son Verme" başlıklı 9. maddenin birinci cümlesinde Kurula ihbar, şikâyet ya da Ticaret Bakanlığının talebi üzerine veya resen 4., 6. veya 7. maddelerin ihlal edildiğini tespit etmesi hâlinde bu ihlallere neden olan anlaşma, davranış, karar, birleşme, devralma gibi tüm işlem ve eylemlere yönelik rekabeti kısıtlayıcı duruma son verecek tedbirleri alma görev ve yetkisi tanınmıştır. Bu tedbirler ilgili teşebbüslere belirli davranışlarda bulunma zorunluluğu getiren veya rekabete aykırı belirli davranışlarda bulunmaktan alıkoyan davranışsal tedbirler olabileceği gibi piyasanın yapısının değiştirilmesi amacıyla teşebbüslerin belirli faaliyetlerinin yahut ortaklık paylarının ya da mal varlıklarının devredilmesi şeklindeki yapısal tedbirler de olabilir. Anılan cümlenin "...ve teşebbüslerin belirli faaliyetlerini yahut ortaklık paylarını ya da mal varlıklarını devretmeleri şeklindeki yapısal tedbirleri..." bölümü dava konusu kuralı oluşturmaktadır.

12. Davranışsal tedbirler; rakip teşebbüslerin belirli bir imkâna erişiminin sağlanması, teşebbüsler arası bilgi paylaşımının tasarlanmış güvenlik duvarlarıyla engellenmesi, ayrımcı olmayacak şekilde davranmayı öngören hükümlerin veya fiyat kontrollerinin getirilmesi, rakip teşebbüslere altyapıya, şebekeye, patentlere, üretim yöntemlerine (know-how) veya fikrî haklar gibi teknolojilere ve zorunlu girdilere erişim hakkının tanınması, müşteri ya da rakiplerle iş yapılmasına mâni olan sözleşmelerin imzalanmasının engellenmesi veya yasaklanması, belirli tip sözleşmelere kısıtlama getirilmesi,

teşebbüs çalışanlarının rekabet etme yasağının uygulanmasının engellenmesi ve piyasaya girişlerin teşvik edilmesi gibi çeşitli şekillerde olabilmektedir.

13. Davranışsal tedbirler teşebbüslerin davranışlarına, varlıklarını nasıl kullanacaklarına, pazarda rekabet etmelerine veya diğer teşebbüslerle yapacakları sözleşmelere yönelik yükümlülükler içerir. Ancak herhangi bir rekabet yasağı ihlalinin sona erdirilmesi için davranışsal tedbirler her zaman yeterli olmayabilir.

14. Rekabeti kısıtlayıcı ihlalin sona erdirilmesi konusunda davranışsal tedbirlerin sonuç vermediği durumlarda dava konusu kuralla teşebbüslerin belirli faaliyetlerini yahut ortaklık paylarını ya da mal varlıklarını devretmeleri şeklindeki yapısal tedbirlere başvurulabileceği öngörülmüştür. Ancak yine 9. maddenin birinci fıkrası uyarınca davranışsal tedbirler öncelikle uygulanacak ve davranışsal tedbirlerin sonuç vermediği hâllerde yapısal tedbirlere başvurulacaktır. Davranışsal ve yapısal tedbirler, ihlalle orantılı ve ihlalin etkili biçimde sona erdirilmesi için gerekli olmalıdır.

15. Uygulanacak yapısal tedbirler kapsamındaki devirlerin 11/1/2011 tarihli ve 6098 sayılı Türk Borçlar Kanunu ile 6102 sayılı Kanun'da yer alan işletme ve pay devrine ilişkin hükümlere göre yapılacağı açıktır. Anılan hükümler çerçevesinde devrin konusunu hangi unsurların oluşturacağına dair ilgili teşebbüslerin taahhüt ve öneride bulunması mümkün olmakla birlikte bu hususlar Kurul tarafından belirlenecek olup devirlerin uygulanması için altı aydan az olmamak üzere süre verileceği öngörülmüştür. Söz konusu süre içinde devre konu unsurların ilgili sicillere tescil ve ilanları, borç ve alacaklardan sorumluluk, lisans ve izinlerin yenilenmesi gibi devir işlemlerinin seyri ile gerçekleştirilen devrin yeterliliği ve karara uygunluğu Kurulun takdirindedir. Kurulun bu kapsamda almış olduğu tedbirlerin ihlalle orantılı ve gerekli olup olmadığına yönelik itirazlar ise idari yargının denetimine tabidir.

16. Kurulca belirlenen yapısal tedbirlere uyulmaması hâlinde ise hukuken geçersiz sayma, zarara uğrayanlar lehine tazminat, idari para cezası, birleşme ve devralmaya izin vermeme gibi Kanun'da sayılan diğer yaptırımlara hükmedilebilecektir.

2. İptal Talebinin Gerekçesi

17. Dava dilekçesinde özetle; dava konusu kuralın yargı kararı olmaksızın mal varlığının devri sonucunu doğurduğu, mülkiyet ve teşebbüs özgürlüğünün sınırlanmasına neden olduğu, bu yöndeki kararın yargı kararıyla iptal edilmesi hâlinde dahi devir dolayısıyla teşebbüslerin ağır ve telafisi imkânsız zararlara uğramasının kaçınılmaz olduğu, 4054 sayılı Kanun'un 7. maddesi kapsamındaki devir ve birleşmelerin gerçekleşmesi hâlinde yapılacak hususların 10. ve 11. maddelerde

düzenlendiği, rekabet yasağı ihlalini düzenleyen 4. ve 6. maddelere aykırılıkların özünde davranışsal fiiller olduğu, kuralla bunlar için yapısal tedbirlerin öngörüldüğü, hâlbuki davranışsal fiillere ilişkin yaptırımın 57. ve 58. maddelerde zarara uğrayan kişilerin zararlarının tazmini olarak belirlendiği, bu tür ihlaller için anılan yaptırımların yeterli olduğu, kuralla öngörülen hak sınırlamalarının orantılı olmadığı belirtilerek kuralın Anayasa'nın 2., 13., 35., 48., 90. ve 167. maddelerine aykırı olduğu ileri sürülmüştür.

3. Anayasa'ya Aykırılık Sorunu

18. Anayasa'nın 35. maddesinde "Herkes, mülkiyet ve miras haklarına sahiptir./Bu haklar, ancak kamu yararı amacıyla, kanunla sınırlanabilir./Mülkiyet hakkının kullanılması toplum yararına aykırı olamaz." denilmektedir. Anayasa'nın anılan maddesiyle güvenceye bağlanan mülkiyet hakkı, ekonomik değer ifade eden ve parayla değerlendirilebilen her türlü mal varlığı hakkını kapsamaktadır. Teşebbüslerin fiziki varlıklarının, faaliyet alanlarının, ortaklık payları ya da fikrî haklar dâhil olmak üzere mal varlıklarının da mülkiyet hakkının kapsamında olduğu hususunda tereddüt bulunmamaktadır.

19. Mülkiyet hakkı, kişiye başkasının hakkına zarar vermemek ve kanunların öngördüğü sınırlamalara uymak koşuluyla sahibi olduğu şeyi dilediği gibi kullanma, onun semerelerinden yararlanma ve ondan tasarruf etme imkânı veren bir haktır. Bu bağlamda malikin mülkünü kullanma, onun semerelerinden yararlanma ve mülkü üzerinde tasarruf etme yetkilerinden herhangi birinin sınırlanması veya mülkünden yoksun bırakılması mülkiyet hakkına müdahale teşkil eder.

20. Anayasa'nın "Çalışma ve sözleşme hürriyeti" başlıklı 48. maddesi ise şöyledir: "Herkes, dilediği alanda çalışma ve sözleşme hürriyetlerine sahiptir. Özel teşebbüsler kurmak serbesttir./Devlet, özel teşebbüslerin millî ekonominin gereklerine ve sosyal amaçlara uygun yürümesini, güvenlik ve kararlılık içinde çalışmasını sağlayacak tedbirleri alır."

21. Anayasa'nın anılan maddesinde özel teşebbüsler kurmanın serbest olduğu belirtilmiş ancak devlete özel teşebbüslerin millî ekonominin gereklerine ve sosyal amaçlara uygun yürümesini sağlayacak tedbirleri alma görevi verilmiştir. Bu husus madde gerekçesinde "Devlet, kamu yararı olan hallerde ve millî ekonominin gerekleri ve sosyal amaçlarla özel teşebbüs özgürlüğüne sınırlamalar getirebilir..." şeklinde ifade edilmiştir.

22. Anayasa'nın anılan maddesiyle güvence altına alınan teşebbüs özgürlüğü, gelir ve kâr elde etmek amacıyla kişi ve teşebbüslerin piyasalarda ticari faaliyette bulunma, mal ve hizmet üreterek satın alma ya da satma, sözleşme yapma, teşebbüs kurma ve yönetme özgürlüğünü kapsamaktadır.

23. Anlaşma, uyumlu davranış, karar alma, hâkim durumun kötüye kullanılması ya da birleşme veya devralma suretiyle belirli bir mal ya da hizmet piyasasında doğrudan veya dolaylı olarak rekabetin engellenmesi, bozulması ya da kısıtlanması nedeniyle ilgili teşebbüslerin belirli faaliyetlerinin, ortaklık paylarının veya fikrî haklar dâhil olmak üzere mal varlıklarının bir kısmının üçüncü teşebbüslere devredilmesini öngören kural bir yandan mülkiyet hakkını, diğer yandan bu devirlerin teşebbüslerin ticari stratejileri üzerinde doğrudan etkili olması nedeniyle teşebbüs özgürlüğünü sınırlamaktadır.

24. Anayasa'nın 13. maddesinde "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz." denilmektedir. Buna göre temel hak ve özgürlüklere sınırlama getiren düzenlemelerin kanunla yapılması, Anayasa'da öngörülen sınırlama sebebine uygun ve ölçülü olması gerekir.

25. Bu kapsamda mülkiyet hakkını ve teşebbüs özgürlüğünü sınırlamaya yönelik bir kanuni düzenlemenin şeklen var olması yeterli olmayıp yasal kuralların keyfiliğe izin vermeyecek şekilde belirli, ulaşılabilir ve öngörülebilir nitelikte olması gerekir.

26. Esasen temel hak ve özgürlükleri sınırlayan kanunun bu niteliklere sahip olması Anayasa'nın 2. maddesinde güvenceye alınan hukuk devleti ilkesinin de bir gereğidir. Hukuk devletinde kanuni düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi gerekir. Kanunda bulunması gereken bu nitelikler hukuki güvenliğin sağlanması bakımından da zorunludur. Zira bu ilke hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar (AYM, E.2015/41, K.2017/98, 4/5/2017, §§ 153, 154). Dolayısıyla Anayasa'nın 13. maddesinde sınırlama ölçütü olarak belirtilen kanunilik, Anayasa'nın 2. maddesinde güvenceye alınan hukuk devleti ilkesi ışığında yorumlanmalıdır.

27. Kuralda hangi yapısal tedbirlerin alınabileceği herhangi bir tereddüde yer vermeyecek biçimde açık ve net olarak düzenlenmiştir. Ayrıca bu yapısal tedbirlerin hangi ihlallerin varlığı hâlinde, hangi oranda ve hangi aşamada karara bağlanabileceği ve uygulanması için en az ne kadar süre tanınması gerektiği hususları da kuralın yer aldığı fıkrada belirtilmiştir. Dolayısıyla kuralın belirli, ulaşılabilir ve öngörülebilir nitelikte olduğu ve bu yönüyle kanunilik şartını taşıdığı anlaşılmaktadır.

28. Anayasa'nın 35. maddesinde mülkiyet hakkının kamu yararı amacıyla sınırlanabileceği öngörülmüştür. Anayasa'nın 48. maddesinde ise teşebbüs özgürlüğü için herhangi bir sınırlama nedeni öngörülmemiş olmakla birlikte özel sınırlama nedeni öngörülmemiş hakların da o hakkın doğasından kaynaklanan bazı sınırlarının bulunduğu kabul edilmektedir. Ayrıca Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevler, özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebilir (AYM, E.2018/99, K.2021/14, 3/3/2021, § 24).

29. Mal ve hizmet üretiminde verimliliğin artırılması, kaynak dağılımında etkinliğin sağlanması ve teknolojiye yararlanmanın azami düzeye çıkarılabilmesi bakımından rekabetin esas olduğu bir serbest piyasa modelinin varlığı zorunludur. Rekabetin hüküm sürdüğü bir ortam, üretilen ve tüketicilere sunulan mal ve hizmetlerin belirli bir kalitede olmasını ve fiyatının makul düzeylerde kalmasını sağladığından aynı zamanda tüketicinin korunmasına da hizmet etmektedir. Ayrıca rekabet, ekonomik gücün tek bir elde toplanmasını önleyip topluma yayarak iktisadi güce sahip olanların siyasi hayata da egemen olmasını engellediğinden demokratik sistemin işlevsellik kazanabilmesi için gerekli bir nitelik taşımaktadır. Anayasa'nın 167. maddesinin gerekçesinde, tekeller ve tekel benzeri gruplaşmaları hem tüketim hem de hizmet sektöründe önlemenin sağlıklı bir toplum ve demokrasi için vazgeçilmez olduğu ifade edilerek bu gerçeğe işaret edilmektedir (AYM, E.2013/50, K.2015/38, 1/4/2015).

30. Kuralla rekabeti kısıtlayıcı her türlü anlaşma, birlik kararı, uyumlu davranış, hâkim durumu kötüye kullanma, birleşme veya devralma söz konusu olduğunda bozulan rekabetin yeniden tesisi için ilgili teşebbüslerin davranışlarına, varlıklarını nasıl kullanacaklarına, pazarda rekabet etmelerine veya diğer teşebbüslerle yapacakları sözleşmelere yönelik yükümlülüklerden oluşan davranışsal tedbirlerin sonuç vermediği durumlarda teşebbüslerin belirli faaliyetlerini yahut ortaklık paylarını ya da mal varlıklarını devretmeleri şeklindeki yapısal tedbirlere başvurulması öngörülmektedir. Kuralın Anayasa'nın 48. maddesinin ikinci fıkrası ve 167. maddesiyle devlete yüklenen özel teşebbüslerin güvenli ve serbest piyasa içinde çalışmasını sağlama, piyasalarda fiilî şekilde veya anlaşmayla doğacak tekel ve kartelleşmeyi engelleme yükümlülüğü kapsamında piyasada rekabete aykırı davranış ya da işlemle zarar gören rekabet sürecinin kalıcı ve etkili bir şekilde düzeltilmesi suretiyle serbest piyasa ekonomisinin, rekabetçi ortamın, ekonomik aktörlerin davranışlarının oluşturduğu tehditlerden korunmasını amaçladığı anlaşılmaktadır. Bu itibarla kamu yararını gerçekleştirmeye yönelik kuralın anayasal bağlamda meşru bir amacının bulunduğu görülmektedir.

31. Öte yandan Anayasa'nın 13. maddesi uyarınca sınırlamanın ölçülü olup olmadığının da değerlendirilmesi gerekir. Anayasa'nın anılan maddesinde güvence altına alınan ölçülülük ilkesi

elverişlilik, gereklilik ve orantılılık olmak üzere üç alt ilkedен oluşmaktadır. Elverişlilik öngörülen sınırlamanın ulaşılmaк istenen amacı gerçekleştirmeye elverişli olmasını, gereklilik ulaşılmaк istenen amaç bakımından sınırlamanın zorunlu olmasını, diğеr bir ifadeyle aynı amaca daha hafif bir sınırlama ile ulaşılmasının mümkün olmamasını, orantılılık ise hakka getirilen sınırlama ile ulaşılmaк istenen amaç arasında makul bir dengenin gözetilmesi gerekliliğini ifade etmektedir.

32. Teşebbüslerin aralarındaki gizli veya açık anlaşmalarla, oluşturdukları birliklerinin kararlarıyla ya da birlikte gerçekleştirdikleri davranışlarla, piyasadaki hâkim durumlarını tek başına yahut başkalarıyla yapacağı anlaşmalar ya da birlikte davranışlarla kötüye kullanması, birleşme veya devralmalar suretiyle piyasadaki etkin rekabetin kısıtlanması durumlarında ilgili teşebbüslerin devam eden faaliyetlerinin, mal varlıklarının veya ortaklık paylarının tamamının ya da bir kısmının elden çıkarılması suretiyle piyasayı yeniden yapılandırma ve piyasadaki hâkim yoğunlaşmayı engelleme imkânı sağladığından kuralın zarar gören rekabet sürecinin etkin bir biçimde yeniden tesisi amacını gerçekleştirmeye elverişli olmadığı söylenemez.

33. Davranış, anlaşma ve işlemlerin rekabeti sınırlayıcı ve rekabetçi yapıyı önemli ölçüde bozucu etkisi söz konusu olduğunda anılan eylem ve işlemler yasaklanmakta ve söz konusu yasağa uyulmaması durumunda çeşitli yaptırımlara başvurulmaktadır. Herhangi bir yaptırım uygulanmaksızın rekabet üzerindeki olumsuz etkilerin giderilmesi mümkün ise öncelikle teşebbüslere belirli bir şekilde davranma ya da davranmama yükümlülüğü yükleyen tedbirlere hükmedilmektedir.

34. Ancak piyasadaki rekabetçi yapıda oluşan zararların giderilmesi her zaman davranışsal tedbirlerle mümkün olmaz. Nitekim ilgili teşebbüslere belirli davranışlarda bulunma zorunluluğu getiren veya teşebbüsleri rekabet karşıtı davranışlarda bulunmaktan alıkoyan davranışsal tedbirler, tarafların gelecekteki davranışlarını ele aldığından izlenme ve piyasa şartlarındaki değişime göre güncellenme gerektirir. Ayrıca davranışsal tedbirler etkin tasarım gerektirdiği gibi rekabet otoritelerinin sektörel düzeyde düzenleyici otoriteye dönüşmesine ve piyasanın gerekli gelişim, büyüme ve rekabetçi ortamın tesisine olumsuz etki de yapabilir. Öte yandan davranışsal tedbirlerin ilgili teşebbüsler yönünden yapısal çözümden daha külfetli olacağı durumlarda teşebbüsler söz konusu tedbirlere uymamayı tercih edebilmektedir. Dolayısıyla kalıcı ve daha etkili olan yapısal tedbirlerin söz konusu durumlarda uygulanmasının gerekli olmadığı savunulamaz.

35. Kuralla getirilen yapısal tedbirler bir elkoyma ya da cebri icra niteliğinde olmayıp bu yapısal tedbirlerin gereği bizzat Kurulca değil ilgili teşebbüsler tarafından yerine getirilecektir. Kanun'un 9. maddesinde yapısal tedbirlerin ihlalle orantılı ve gerekli olması gerektiği gibi yapısal tedbirlere ancak

daha önce getirilen davranışsal tedbirlerin sonuç vermediği hâllerde başvurulabileceği öngörülmüştür. Söz konusu yapısal tedbir Kurul kararı ile bağlayıcı kılındıktan sonra ilgili teşebbüslere tedbirlere uyması için en az altı ay süre verilmekte ve uyulmaması hâlinde tedbirin resen ve cebri icra yoluyla infazı mümkün olmayıp Kanun'da sayılan diğer yaptırım ve cezalara hükmedilmektedir. Üstelik söz konusu süreçlerde ilgili teşebbüslerin savunma, dosyadan örnek alma ve diğer hakları Kanun'un 43. ila 47. maddelerinde ayrıntılı olarak düzenlenmiş ve Kurulun bu yöndeki kararları idari yargı denetimine tabi tutulmuştur. Dolayısıyla kuralın orantısız bir müdahaleye neden olmadığı ve anılan haklara ölçsüz bir sınırlama getirmediği sonucuna ulaşılmıştır.

36. Açıklanan nedenlerle kural, Anayasa'nın 13., 35. ve 48. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

Kuralın Anayasa'nın 2. ve 167. maddelerine de aykırı olduğu ileri sürülmüş ise de bu bağlamda belirtilen hususların Anayasa'nın 13., 35. ve 48. maddeleri yönünden yapılan değerlendirmeler kapsamında ele alınmış olması nedeniyle Anayasa'nın 2. ve 167. maddeleri yönünden ayrıca bir inceleme yapılmasına gerek görülmemiştir.

Kuralın Anayasa'nın 90. maddesiyle ilgisi görülmemiştir.

C. Kanun'un 4. Maddesiyle 4054 Sayılı Kanun'un 15. Maddesinin Birinci Fıkrasının Değiştirilen (a) Bendinde Yer Alan "...bunların kopyalarını ve fiziki örneklerini alabilir," İbaresinin İncelenmesi

1. İptal Talebinin Gerekçesi

37. Dava dilekçesinde özetle; dava konusu kuralla hiçbir sınırlama olmaksızın teşebbüslerin her türlü belgesinin kopyalanmasının ve örneğinin alınmasının mümkün kılındığı, bu işlem sırasında ilgili teşebbüs temsilcisinin hazır bulunmasına ilişkin bir şarta yer verilmediği gibi teşebbüslerin ticari sır ve müşteri çevresine ilişkin verilere erişim yetkisi tanıyan kuralın kişisel verilerin elde edilmesi ve işlenmesi konusunda herhangi bir güvence de içermediği, bu durumun hukuki belirlilik ilkesiyle de bağdaşmadığı ve orantılı olmadığı belirtilerek kuralın Anayasa'nın 2., 13., 20., 35. ve 90. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

38. Anayasa'nın 20. maddesinin birinci fıkrasında herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş; üçüncü fıkrasında da "Herkes, kendisiyle ilgili kişisel verilerin

korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.” denilerek kişisel verilerin korunması, özel hayatın gizliliğinin korunması kapsamında güvenceye kavuşturulmuştur.

39. Kişisel verilerin korunmasını isteme hakkı, kişinin insan onurunun korunması ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Bilişim teknolojilerindeki gelişmeler sonucunda geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi, daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezî olarak bir araya getirilebilmesi, verilerin veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle veriden yeni veriler üretme kapasitesinin artması, verilere erişim ve veri transferinin kolaylaşması, kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde özel sektör unsurlarınca oluşturulan risklerin daha yaygın ve önemli boyutlara ulaşması, terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır.

40. Öte yandan Anayasa'nın anılan maddesinde kişisel verilerin kişi bakımından korunma alanının gerçek kişiler ya da tüzel kişileri veya her ikisini içine alıp almadığı konusunda bir açıklık bulunmamaktadır. Maddenin gerekçesinde de buna ilişkin bir değerlendirme yoktur. Her ne kadar Anayasa'nın anılan maddesinde daha ziyade gerçek kişilerin özel hayatı ve bu bağlamda gerçek kişilere ilişkin kişisel verilerin korunma altında tutulduğu ileri sürülebilir ise de madde metninde kişisel verilerle ilgili olarak “Herkes,...” ibaresinin kullanıldığı gözetildiğinde tüzel kişilere ilişkin verilerin de madde kapsamında değerlendirilmesi gerektiği açıktır.

41. Nitekim Anayasa'nın 148. maddesinin üçüncü fıkrasında Anayasa'da güvence altına alınmış temel hak ve özgürlüklerinden Avrupa İnsan Hakları Sözleşmesi kapsamındaki herhangi birinin kamu gücü tarafından ihlal edildiğini iddia eden herkese Anayasa Mahkemesine bireysel başvuru yapma imkânı tanınmıştır. Buna göre medeni haklara sahip gerçek kişilerin yanı sıra tüzel kişilerin de bireysel başvuru yönünden dava ehliyetine sahip oldukları açıktır.

42. Esasen her ne kadar 20/2/1995 tarihli ve 95/46/EC sayılı Avrupa Veri Koruması Direktifi'nde yer alan tanım, tüzel kişilere ilişkin verileri dışlamakta ve kişisel veri kapsamına yalnızca gerçek kişilere ilişkin bilgilerin gireceğini kabul etmekte ise de gerek elektronik haberleşme sektöründe kişisel

bilgilerin işlenmesi ve gizliliğinin korunması hakkındaki 12/7/2002 tarihli ve 2002/58/EC sayılı Avrupa Parlamentosu ve Konsey Direktifi'nde, yalnızca elektronik haberleşme sektörüne ilişkin olarak hem gerçek kişilerin hem de tüzel kişilerin veri sahibi kabul edileceğinin ifade edilmesi gerekse son yıllarda kabul edilen bazı ülke kanunlarında tüzel kişilerin de kişisel verilerin koruma alanına dâhil edilmesi bir bütün olarak gözetildiğinde uluslararası gelişmelerin kişisel verilerin korunması kapsamında tüzel kişilerin de yer alması gerektiği yönünde olduğu görülmektedir (AYM, E.2013/84, K.2014/183, 4/12/2014).

43. Dava konusu kural, Kurulun 4054 sayılı Kanun kapsamındaki görevlerini yerine getirirken gerekli gördüğü hâllerde teşebbüslerin veya teşebbüs birliklerinin defterlerinin, fiziki ve elektronik ortam ile bilişim sistemlerinde tutulan her türlü verilerinin ve belgelerinin kopyalarını, fiziki örneklerini alabileceğini öngörmek suretiyle kişisel verilerin korunmasını isteme hakkını sınırlamaktadır.

44. Temel hak ve özgürlüklerin sınırlandırılması rejimini düzenleyen Anayasa'nın 13. maddesinde hak ve özgürlüklerin ancak kanunla sınırlandırabileceği temel bir ilke olarak benimsenmiştir. Bunun yanında Anayasa'nın 20. maddesinin üçüncü fıkrasının üçüncü cümlesinde kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği belirtilmiş, anılan fıkranın dördüncü cümlesinde ise kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hüküm altına alınmıştır.

45. Kuralda Kurula tanınan yetkinin konusu, kapsamı ve sınırları ile kullanılacak hâllerin açık ve net olarak belirlendiği gözetildiğinde kuralın belirli, ulaşılabilir ve öngörülebilir nitelikte olduğu ve bu yönüyle kanunilik şartını taşıdığı anlaşılmaktadır.

46. Kuralın Anayasa'nın 48. maddesinin ikinci fıkrası ve 167. maddesiyle devlete yüklenen özel teşebbüslerin güvenli ve serbest piyasa içinde çalışmasını sağlama ve piyasalarda fiilî şekilde veya anlaşmayla doğacak tekel ve kartelleşmeyi önleme yükümlülüğü kapsamında piyasada rekabete aykırı davranış ya da işlemlerin tespit edilmesi amacıyla delil niteliğindeki defter, belge, kayıt ve verilerin kopyalarının ve fiziki örneklerinin alınmasını öngördüğü gözetildiğinde kuralın anayasal anlamda meşru bir amacının bulunduğu anlaşılmaktadır.

47. Öte yandan devletin rekabet ortamının korunması suretiyle piyasaların sağlıklı ve düzenli şekilde işlenmesini sağlamak için rekabet ihlallerinin tespit edilebilmesi amacıyla getirilen sınırlamanın zorunlu bir toplumsal ihtiyaçtan kaynaklanmadığı söylenemeyeceğinden kuralın demokratik toplum düzeninin gerekleriyle bağdaşmayan bir yönü de bulunmamaktadır.

48. Kuralla Kurulun görevlerini yerine getirirken gerekli gördüğü hâllerde teşebbüslerin veya teşebbüs birliklerinin bilgi, defter, belge ve verilerinin kopyalarını ve fiziki örneklerini alabileceğinin öngörülmesinin rekabete aykırı davranış ya da işlemlerin tespit edilmesini kolaylaştıracağı gözetildiğinde kuralın özel teşebbüslerin güvenli ve serbest piyasa içinde çalışmasını sağlama ve piyasalarda fiilî şekilde veya anlaşmayla doğacak tekel ve kartelleşmeyi engelleme amacına ulaşma bakımından elverişli bir sınırlama olmadığı söylenemez.

49. İletişim, veri depolama, üretim ve pazarlama gibi alanlardaki teknolojik gelişim ve dönüşüm gözetildiğinde rekabet ihlallerinin teşebbüslerin iç yapıları ve piyasa gücü gibi veriler üzerinde uzman incelemesi yapılmaksızın ortaya çıkarılması mümkün değildir. Bu durum teşebbüsler bünyesinde bulunan defter, kayıt, belge ve elektronik verilerin elde edilmesini ve değiştirilemeyecek ya da ortadan kaldırılamayacak şekilde saklanmasını gerektirmektedir. Dolayısıyla kuralla öngörülen sınırlamanın anılan amaca ulaşma bakımından gerekli olma kriterinin sağlandığı değerlendirilmiştir.

50. Teşebbüsler ister gerçek ister tüzel kişi olsun ticari faaliyetin gereği olarak haberleşme, veri ve kayıt tutma zorunluluğunun yanı sıra ticaret, sosyal güvenlik ve vergi mevzuatı gereği işlem ve eylemlerini belgelendirmek, bir kısım kayıt tutmak, mali varlıklarını ve buna ilişkin işlemlerini muhasebeleştirmek zorundadır. Bu zorunluluk teşebbüslerin kendi hak ve menfaatlerinin belirlenmesi ve korunması ile söz konusu mevzuat uyarınca ortakları, çalışanları, müşterileri ve kamu kurumlarına karşı sorumluluklarının yerine getirilmesi açısından güven ve belirlilik sağlamaktadır. Çoğu zaman anılan kayıt ve veriler dışında rekabet ihlallerinin ortaya çıkarılması açısından elde edilebilecek gerçeğe uygun, delil zinciri korunmuş başkaca delil bulma imkânı mevcut olmayabilmektedir. Bu kapsamda inceleme sırasında elde edilen defterler, fiziki ve elektronik ortam ile bilişim sistemlerinde bulunan her türlü veri ve belgelerin kopyalarının ve fiziki örneklerinin alınabilmesi gerekeceği açıktır.

51. Söz konusu işlem 4054 sayılı Kanun'un 15. maddesinin ikinci fıkrası uyarınca Kurul emrinde çalışan uzmanlar eliyle ve incelemenin konusu ile amacını gösteren bir yetki belgesi ibrazı suretiyle yapılacaktır. Yine anılan maddenin üçüncü fıkrasına göre yerinde incelemenin engellenmesi veya engelleme olasılığının doğması hâlinde yerinde inceleme ancak sulh ceza hâkiminin kararı ile mümkün olup Kurulun kendiliğinden zor kullanma yetkisi bulunmamaktadır.

52. Öte yandan anılan Kanun'un 44. maddesinde haklarında soruşturma başladığı bildirilen tarafların sözlü savunma hakkını kullanma taleplerine kadar Rekabet Kurumu (Kurum) bünyesinde kendileri ile ilgili düzenlenmiş her türlü evrakın ve mümkünse elde edilmiş olan her türlü delilin bir örneğinin

kendilerine verilmesini talep edebilecekleri ve Kurulun tarafları bilgilendirmediği ve taraflara savunma hakkı vermediği konuları kararlarına dayanak yapamayacağı öngörülmüştür.

53. Ayrıca 25. maddede Kurul üyeleri ile personelinin Kanun'un uygulanması sırasında öğrendikleri teşebbüs ve teşebbüs birliklerinin ticari sırlarını görevlerinden ayrılmış olsalar bile ifşa edemeyecekleri, kendilerinin veya başkalarının menfaatine kullanamayacakları hükme bağlanmıştır.

54. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Kapsam" başlıklı 2. maddesinde bu Kanun hükümlerinin, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanacağı, 3. maddesinin (1) bendinde veri sorumlusunun kişisel verilerin işleme amaçlarını ve araçlarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade ettiği hükme bağlanmıştır.

55. Anılan Kanun'un "Kabahatler" başlıklı 18. maddesinin (3) numaralı fıkrasında da anılan Kanun kapsamında yer alan kabahatlerin kamu kurum ve kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılacağı ve sonucunun Kurula bildirileceği belirtilmiş; geçici 1. maddesinin (5) numaralı fıkrasında ise Kanun'un yayımı tarihinden itibaren bir yıl içinde, kamu kurum ve kuruluşlarında Kanun'un uygulanmasıyla ilgili koordinasyonu sağlamak üzere üst düzey bir yöneticinin belirlenerek Kişisel Verileri Koruma Kurumu Başkanlığına bildirileceği öngörülmüştür.

56. Bu kapsamda Kurulun gerçek kişi de olabilecek teşebbüslerin defterlerinin, fiziki ve elektronik ortam ile bilişim sistemlerinde tutulan her türlü verilerinin ve belgelerinin kopyalarını ve fiziki örneklerini alabileceği gözetildiğinde 6698 sayılı Kanun'da yer alan yükümlülüklerle tabi olduğu anlaşılmaktadır.

57. Anılan Kanun'un 6. maddesinde ise özel nitelikli kişisel verilerin işlenmesi daha katı şartlara bağlanmıştır. Bu düzenlemeye göre sağlığa ve cinsel hayata ilişkin kişisel veriler dışındaki özel nitelikli veriler kişinin açık rızasının varlığı hâlinde işlenebilecektir. İtiraz konusu kural, piyasada rekabete aykırı davranış ya da işlemlerin tespit edilmesi amacıyla delil niteliğindeki defter, belge, kayıt ve verilerin kopyalarının ve fiziki örneklerinin alınmasını öngörmekte olup özel nitelikli kişisel veri kapsamında kalan verilerin kaydedilmesini ve bu verilerin kullanılmasını içermemektedir.

58. 6698 sayılı Kanun'un 7. maddesinde kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi, 8. ve 9. maddelerinde bu verilerin aktarılması, 10. maddesinde veri sorumlusunun aydınlatma yükümlülüğü, 11. maddesinde ilgili kişinin hakları, 12. maddesinde veri güvenliğinin sağlanması, 13. maddesinde veri sorumlusuna başvuru, 14. maddesinde Kişisel Verilerin Korunması Kuruluna şikâyet, 16. maddesinde veri sorumluları sicili, 17. ve 18. maddelerinde ise kişisel verilere ilişkin suçlar ve kabahatler düzenlenmiştir. Dolayısıyla piyasada rekabete aykırı davranış ya da işlemlerin tespit edilmesi amacıyla delil niteliğindeki defter, belge, kayıt ve verilerin kopyalarının ve fiziki örneklerinin alınmasını öngörmekte olan kural 6698 sayılı Kanun hükümleri kişisel verilerin korunmasına ilişkin olarak bilgilendirme hakkı, erişim hakkı, verilerin amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkı, verilerin güvenliğinin sağlanması gibi gerekli güvenceleri karşılamaktadır.

59. Bu itibarla yasal güvencelerin sağlandığı, teşebbüs ve teşebbüs birliklerine aşırı külfet yüklenmediği gözetildiğinde kuralın orantısız bir müdahaleye neden olmadığı ve kişisel verilerin korunmasını isteme hakkına ölçüsüz bir sınırlama getirmediği sonucuna ulaşılmıştır.

60. Açıklanan nedenlerle kural, Anayasa'nın 13. ve 20. maddelerine aykırı değildir.

Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, Yusuf Şevki HAKYEMEZ ve Selahaddin MENTEŞ bu görüşe katılmamışlardır.

Kuralın Anayasa'nın 2. maddesine de aykırı olduğu ileri sürülmüş ise de bu bağlamda belirtilen hususların Anayasa'nın 13. ve 20. maddeleri yönünden yapılan değerlendirmeler kapsamında ele alınmış olması nedeniyle Anayasa'nın 2. maddesi yönünden ayrıca bir inceleme yapılmasına gerek görülmemiştir.

Kuralın Anayasa'nın 35. ve 90. maddeleriyle ilgisi görülmemiştir.

Ç. Kanun'un 6. Maddesiyle 4054 Sayılı Kanun'un 34. Maddesine Eklenen Üçüncü Fıkranın İncelenmesi

1. Anlam ve Kapsam

61. Dava konusu kuralla Kurulun, 4054 sayılı Kanun'a ekli (I) sayılı Cetvel'deki toplam kadro sayısını geçmemek ve mevcut kadro unvanları veya 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete'de yayımlanan (2) numaralı Genel Kadro ve Usulü Hakkında Cumhurbaşkanlığı Kararnamesi (CBK) eki cetvellerde yer alan kadro unvanları ile sınırlı olmak kaydıyla hizmet sınıfı, kadro, unvan ve derecelerinin değiştirilmesi ile bu kadroların kullanılmasına ilişkin usul ve esasları belirlemeye yetkili olduğu öngörülmüştür.

62. Kural uyarınca Kurul kendisine tahsis edilmiş kadroların hizmet sınıfını, kadro adedini, unvanını ve derecelerini değiştirebilecek ve bu kadroların kullanılmasına ilişkin usul ve esasları belirleyebilecektir. Kurul anılan yetkiyi kullanırken Kanun'a ekli (I) sayılı Cetvel'deki toplam kadro sayısını geçemeyecek olup unvan değişikliği hâlinde ise yeni belirlenen kadro unvanları anılan cetvelde veya (2) numaralı CBK'nın eki cetvellerde yer alan kadro unvanlarından biri olacaktır. Başka bir deyişle söz konusu cetvellerde yer almayan yeni bir unvanın ihdası mümkün değildir.

2. İptal Talebinin Gerekçesi

63. Dava dilekçesinde özetle; Kurumun tüm personelinin kadro unvan ve derecelerini ve sayılarını Kurulun takdirine bırakan önceki düzenlemenin Anayasa Mahkemesi tarafından iptal edildiği, dava konusu kuralla iptal edilen düzenlemenin yeniden ihdas edildiği, memurların ve diğer kamu görevlilerinin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülükleri, aylık ve ödenekleri ve diğer özlük işlerinin kanunla düzenlenmesi gerektiği, kuralın yasama yetkisinin devri niteliğinde olup idarenin kanuniliği ilkesine aykırı olduğu, bu durumun Anayasa Mahkemesi kararlarının bağlayıcılığıyla da bağdaşmadığı belirtilerek kuralın Anayasa'nın 7., 123., 128. ve 153. maddelerine aykırı olduğu ileri sürülmüştür.

3. Anayasa'ya Aykırılık Sorunu

64. Anayasa'nın 7. maddesinde "Yasama yetkisi Türk Milleti adına Türkiye Büyük Millet Meclisindedir. Bu yetki devredilemez." denilmektedir. Yasama yetkisinin Türkiye Büyük Millet Meclisine ait olması ve bu yetkinin devredilememesi, kuvvetler ayrılığı ilkesinin bir gereğidir. Bu hükme yer veren Anayasa'nın 7. maddesinin gerekçesinde yasama yetkisinin parlamentoya ait olması "demokrasi rejimini benimseyen siyasi rejimlerde kaçınılmaz bir durum" olarak nitelendirilmiştir. Ayrıca, gerekçede "Millet adına kanun koyma yetkisini yasama meclisi yerine getirir. Bu yetki devredilemez. Ancak, Anayasanın 99 ve 129 uncu maddeleri hükümleri saklıdır." denilmek suretiyle bu ilkenin anlamı ve istisnaları belirtilmiştir. Madde gerekçesinden de anlaşılacağı üzere yasama yetkisinin devredilemezliği, esasen kanun koyma yetkisinin Türkiye Büyük Millet Meclisi dışında başka bir organca kullanılamaması anlamına gelmektedir. Anayasa'nın 7. maddesi ile yasaklanan kanun yapma yetkisinin devredilmesidir (AYM, E.2011/42, K.2013/60, 9/5/2013).

65. Türevsel nitelikteki düzenleyici işlemler bakımından yürütmenin düzenleme yetkisi sınırlı, tamamlayıcı ve bağımlıdır. Bu nedenle temel ilkeleri belirlenmeksizin ve çerçevesi çizilmeksizin yürütme organına düzenleme yetkisi veren bir kanun kuralı ile sınırsız, belirsiz, geniş bir alanın yürütmenin düzenlemesine bırakılması, Anayasa'nın belirtilen maddesine aykırılık oluşturur. Bununla birlikte yasama organının temel ilkeleri ve çerçeveyi kanunla belirlendikten sonra uzmanlık

ve idare tekniğine ilişkin hususları yürütmeye bırakması, yasama yetkisinin devri olarak yorumlanamaz (AYM, E.2011/42, K.2013/60, 9/5/2013; E.2019/36, K.2021/15, 4/3/2021, § 57).

66. Anayasa'nın 123. maddesinin birinci fıkrasında ise "İdare, kuruluş ve görevleriyle bir bütündür ve kanunla düzenlenir." hükmü yer almaktadır. Bu maddede yer alan düzenleme, idarenin kanuniliği ilkesini güvence altına almaktadır. İdarenin kanuniliği ilkesi, idarenin ve organlarının görev ve yetkilerinin hiçbir duraksamaya yer vermeyecek şekilde, açık bir biçimde kanunla düzenlenmesini gerekli kılar.

67. Anılan ilke, idarenin hizmet birimleri ile bu birimlerin kadro ve görev unvanlarının ve görevlerinin kanunla düzenlenmesini de içerir. Kadrolar, bir kamu hizmetinin teşkilatlanmasının ön koşuludur. 4054 sayılı Kanun'un 21. maddesi uyarınca Kurumun Kurul, Başkanlık ve hizmet birimlerinden oluştuğu, 32. maddesinde de hizmet birimlerinin daire başkanlıkları şeklinde teşkilatlanmış ana hizmet birimleri, danışma birimleri ve yardımcı hizmet birimlerinden meydana geldiği belirtilmiştir. Bu itibarla anılan anayasal ilkeler ile Kurumun önemli organlarından olan hizmet birimlerinin neler olduğunun ve bunların görev ve sorumluluklarının kanunla belirlenmediği gözetildiğinde hizmet sınıfı, kadro, unvan ve derecelerin değiştirilmesi ile bu kadroların kullanılmasına ilişkin usul ve esasları belirleme yetkisinin kuralla idareye bırakılmasının yasama yetkisinin devredilmezliği ve idarenin kanuniliği ilkeleriyle bağdaşmadığı görülmektedir.

68. Öte yandan Anayasa'nın 128. maddesinde; devletin kamu iktisadi teşebbüsleri ve diğer kamu tüzel kişilerinin genel idare esaslarına göre yürütmekle yükümlü oldukları kamu hizmetlerinin gerektirdiği asli ve sürekli görevlerinin memurlar ve diğer kamu görevlileri eliyle görüleceği, memurların ve diğer kamu görevlilerinin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülükleri, aylık ve ödenekleri ile diğer özlük işlerinin kanunla düzenleneceği hükme bağlanmıştır (AYM, E.2016/133, K.2017/155, 15/11/2017, § 91).

69. Kadrolara ilişkin hizmet sınıfı ücret tespiti, personel alma, yükselme gibi personel işlemlerine rasyonel bir temel sağlayan genel gruplandırmayı; kadro unvanı personelin yerine getireceği görevlerini, yetkilerini, haklarını ve yükümlülüklerini, aylık ve ödenekleri ile diğer özlük haklarını ifade etmektedir. Kadro derecesi ile personelin özellikle aylık ve ödenekleri ve diğer özlük hakları bakımından sıkı bir bağ bulunmaktadır. Kadro ile birlikte ana hizmet, danışma ve yardımcı hizmet birimlerinde istihdam edilecek personelin niteliklerinin kanunla belirlenmesi Anayasa'nın 128. maddesinin gereğidir (AYM, E.2002/35, K.2007/95, 12/12/2007).

70. Anılan Kanun'un 34. maddesi uyarınca Kurum hizmetlerinin gerektirdiği asli ve sürekli görevler, idari hizmet sözleşmesi ile sözleşmeli olarak istihdam edilen personel eliyle yürütülmekte ve Kurum

personeli ücret ve mali haklar dışında 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu'na tabi bulunmaktadır. Anayasa Mahkemesinin yerleşik içtihatları uyarınca devlet, kamu iktisadi teşebbüsleri ve diğer kamu tüzel kişileri bünyesinde genel idare esaslarına göre yürütülen asli ve sürekli görevleri yerine getiren sözleşmeli personel, Anayasa'nın 128. maddesinde belirtilen diğer kamu görevlileri kapsamında kalmaktadır. Dolayısıyla bir kamu tüzel kişisi olan Kurumda genel idare esaslarına göre yürütülen asli ve sürekli görevleri yerine getiren kurum personelinin statüsünün ve özlük haklarının Anayasa'nın anılan maddesi uyarınca kanunla düzenlenmesi gerektiği açıktır.

71. Kurulla ekli cetveller uyarınca Kuruma tahsis edilen toplam kadro sayısı ve değiştirilmek suretiyle kararlaştırılabilecek kadro unvanları sınırlandırılmıştır. Ancak Kurula kamu görevlisi olan Kurum personelinin mali haklarının içerik ve sınırlarını belirleyen hizmet sınıfı, kadro, unvan ve derecelerin tümünü değiştirme yetkisi verilmiştir. Dolayısıyla anılan konulara ilişkin olarak temel ilkelerin belirlendiği de söylenemeyeceği gözetildiğinde söz konusu yetkinin idarenin bir unsuru olan Kurula bırakılması, yasama yetkisinin devri sonucunu doğurmakta ve kamu görevlilerinin statülerinin kanunla düzenlenmesi yolundaki anayasal ilkeye aykırılık oluşturmaktadır.

72. Açıklanan nedenlerle kural, Anayasa'nın 7., 123. ve 128. maddelerine aykırıdır. İptali gerekir.

Kuralın Anayasa'nın 153. maddesiyle ilgisi görülmemiştir.

D. Kanun'un 12. Maddesiyle 4054 Sayılı Kanun'a Eklenen Geçici 6. Maddenin Birinci Fıkrasının Birinci Cümlesinin "...Kurum danışmanı, Başkan danışmanı, idari koordinatör, müdür, araştırma uzmanı, basın danışmanı, sistem çözümleyici, veri iletişim uzmanı, programcı, idari hizmet yetkilisi ve idari hizmet uzmanı kadrolarında bulunanlar araştırmacı kadrolarına;..." Bölümü ile Dördüncü Cümlesinin İncelenmesi

1. Birinci Cümleinin "...Kurum danışmanı, Başkan danışmanı, idari koordinatör, müdür, araştırma uzmanı, basın danışmanı, sistem çözümleyici, veri iletişim uzmanı, programcı, idari hizmet yetkilisi ve idari hizmet uzmanı kadrolarında bulunanlar araştırmacı kadrolarına;..." Bölümü

a. İptal Talebinin Gerekçesi

73. Dava dilekçesinde özetle; dava konusu kurulla araştırmacı adı altında torba bir kadronun oluşturulduğu, Kurum danışmanından programcıya kadar uzmanlık alanları ve eğitim düzeyleri birbirinden çok farklı olan kişilerin tamamının araştırmacı kadrosuna atandığı, kişilerin kazanılmış hakları korunsun da maaş ve ödenekleri eşitlenene kadar maaş ve ödenek artışının yapılmayacak olması nedeniyle uzun dönemde maaş kaybına uğrayacakları, emeklilik haklarının ne olacağı ile ilgili bir düzenlemeye yer verilmediği, bu durumun kadroların kanunla düzenlenmesi ilkesiyle

bağdaşmadığı ve kadrosu değiştirilen kişilerin dava açmasına engel olunduğu belirtilerek kuralın Anayasa'nın 2., 36. ve 48. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

74. 4054 sayılı Kanun'un geçici 16. maddesinin birinci cümlesinde bu maddenin yürürlüğe girdiği tarihte Kurumda inceleme uzmanı kadrosunda bulunanların rekabet uzmanı kadrolarına ve kıdemli koordinatör ile mesleki koordinatör kadrosunda bulunanların rekabet başuzmanı kadrolarına; Kurum danışmanı, başkan danışmanı, idari koordinatör, müdür, araştırma uzmanı, basın danışmanı, sistem çözümleyici, veri iletişim uzmanı, programcı, idari hizmet yetkilisi ve idari hizmet uzmanı kadrolarında bulunanların araştırmacı kadrolarına; garaj şefi kadrosunda bulunanların şoför kadrosuna başkaca bir işleme gerek kalmaksızın kadro dereceleriyle atanmış sayılacağı öngörülmüştür. Anılan cümlenin "...Kurum danışmanı, Başkan danışmanı, idari koordinatör, müdür, araştırma uzmanı, basın danışmanı, sistem çözümleyici, veri iletişim uzmanı, programcı, idari hizmet yetkilisi ve idari hizmet uzmanı kadrolarında bulunanlar araştırmacı kadrolarına;..." bölümü dava konusu kuralı oluşturmaktadır.

75. Anayasa'nın 2. maddesinde belirtilen hukuk devleti eylem ve işlemleri hukuka uygun, insan haklarına saygılı, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adil bir hukuk düzeni kurup bunu geliştirerek sürdüren, hukuki güvenliği sağlayan, Anayasa'ya aykırı durum ve tutumlardan kaçınan, hukuk kurallarıyla kendini bağlı sayan ve yargı denetimine açık olan devlettir.

76. Anayasa Mahkemesinin kamu görevlilerinin kanunla görevden alınmalarına ve başka görevlere atanmalarına ilişkin düzenlemeler yönünden daha önce ifade ettiği gibi;

"Kamu personeli olarak görev yapan kişilerin buldukları görevlerden alınmalarını gerektiren haklı bir neden olmadıkça görevlerine son verilememesi, hukuki güvenlik ilkesinin bir gereğidir. Kamu personelinin buldukları görevden alınma ve başka bir göreve atanmalarının, haklarında bu yönde idari işlem tesis edilmesi ile gerçekleşmesi kural olmakla birlikte, hukuki ve fiili zorunluluk hallerinde bu hususlarda yasal düzenlemeler yapılabileceği de kabul edilmektedir. Söz konusu zorunluluklar nedeniyle getirilen ve ilgililerin kazanılmış haklarını ihlal etmeyen düzenlemeler, hukuki güvenlik ilkesine aykırılık oluşturmaz.

Kanun koyucu Anayasa'ya uygun olmak kaydıyla, kamu hizmetinin yürütülmesine ilişkin koşulları belirleyerek kadro düzenlemesi yapabilir. Kamu hizmetinin gerekleri yönünden ve kamu yararı amacıyla yeni kadrolar ihdas edebileceği gibi, mevcut bazı kadroları da kaldırabilir. Ayrıca, kamu

idareleri ile kamu görevlileri arasındaki ilişkiler, kural tasarruflarla düzenlendiğinden, kamu görevlilerinin statülerine ilişkin yeni kurallar koyabilir ya da var olan kuralları değiştirebilir.

Kamu kurum ve kuruluşlarının yeniden yapılandırılmaları kapsamında, teşkilat yapısı değiştirilen kurum ve kuruluşların bazı kadrolarında görev yapan kamu görevlilerinin görevlerinin sona erdirilerek başka kadrolara atanmalarının öngörülmesi, söz konusu hukuki ve fiilî zorunluluklar nedeniyle getirilen yasal düzenlemelerin bir örneğini oluşturmakta ve hak arama özgürlüğünün ihlaline yol açmamaktadır.

Bu durumda, ilgililerin başka kadrolara atanmalarının sebep unsuru, ilgili kurumun ya da kuruluşun yeniden teşkilatlandırılması olup yürürlükte bulunan kanunlara dayanılarak ve kamu görevlisinin öznel durumu dikkate alınarak idarece tesis edilen naklen atama işlemlerinden tamamen farklıdır. Söz konusu hukuki ve fiilî zorunluluklar nedeniyle kazanılmış haklar korunarak başka kadrolara atama yapılması, kanun koyucunun takdir alanı içindedir.” (AYM, E.2014/57, K.2014/81, 10/4/2014).

77. Kurala göre geçici 16. maddenin yürürlüğe girdiği tarihte Kurumda Kurum danışmanı, başkan danışmanı, idari koordinatör, müdür, araştırma uzmanı, basın danışmanı, sistem çözümleyici, veri iletişim uzmanı, programcı, idari hizmet yetkilisi ve idari hizmet uzmanı kadrolarında bulunanlar araştırmacı kadrolarına başkaca bir işleme gerek kalmaksızın kadro dereceleriyle atanmış sayılır.

78. 7246 sayılı Kanun’la Kurumun teşkilat yapısında herhangi bir değişikliğe gidilmemiştir. Anılan Kanun’la Kurula piyasalardaki teşebbüs ve teşebbüs birliklerinin anlaşma, davranış, karar, birleşme, devralma gibi işlem ve eylemleri nedeniyle 4054 sayılı Kanun’da sayılan yasakların ihlali sonucu oluşan rekabeti kısıtlayıcı durumlara ceza ve yaptırımlar dışında davranışsal ve yapısal tedbirlerle son vermeye yönelik bir kısım görev ve yetki verilmiştir. Ancak söz konusu görev ve yetkiler Kurumun teşkilat yapısında yer alan bazı kadrolarda bulunanların görevlerinin sona ermesiyle araştırmacı kadrosuna atanmalarını gerektiren hukuki ve fiilî zorunluluk olarak değerlendirilemez.

79. Bu itibarla Kurumda belirtilen kadrolarda görev yapan kişilerin araştırmacı kadrolarına atanmalarını öngören kural hukuki güvenlik ilkesiyle bağdaşmamaktadır.

80. Açıklanan nedenlerle kural, Anayasa’nın 2. maddesine aykırıdır. İptali gerekir.

Kadir ÖZKAYA, Rıdvan GÜLEÇ, Recai AKYEL, Yıldız SEFERİNOĞLU, Basri BAĞCI, İrfan FİDAN ve Muhterem İNCE bu görüşe katılmamışlardır.

Kural, Anayasa’nın 2. maddesine aykırı görülerek iptal edildiğinden ayrıca Anayasa’nın 36. maddesi yönünden incelenmemiştir.

Kuralın Anayasa'nın 48. maddesiyle ilgisi görülmemiştir.

2. Dördüncü Cümle

81. 4054 sayılı Kanun'un geçici 6. maddesinin birinci fıkrasının birinci cümlesinin "...Kurum danışmanı, Başkan danışmanı, idari koordinatör, müdür, araştırma uzmanı, basın danışmanı, sistem çözümleyici, veri iletişim uzmanı, programcı, idari hizmet yetkilisi ve idari hizmet uzmanı kadrolarında bulunanlar araştırmacı kadrolarına;..." bölümünün iptali nedeniyle anılan fıkranın dördüncü cümlesinin uygulanma imkânı kalmamıştır. Bu nedenle söz konusu cümle 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 43. maddesinin (4) numaralı fıkrası kapsamında değerlendirilmiş ve bu kural yönünden Anayasa'ya uygunluk denetiminin yapılmasına gerek görülmemiştir.

IV. İPTALİN DİĞER KURALLARA ETKİSİ

82. 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrasında kanunun, Cumhurbaşkanlığı kararnamesinin veya Türkiye Büyük Millet Meclisi İçtüzüğü'nün belirli kurallarının iptali diğer bazı hükümlerinin veya tamamının uygulanmaması sonucunu doğuruyorsa bunların da Anayasa Mahkemesince iptaline karar verilebileceği öngörülmektedir.

83. 4054 sayılı Kanun'un geçici 6. maddesinin birinci fıkrasının birinci cümlesinin "...Kurum danışmanı, Başkan danışmanı, idari koordinatör, müdür, araştırma uzmanı, basın danışmanı, sistem çözümleyici, veri iletişim uzmanı, programcı, idari hizmet yetkilisi ve idari hizmet uzmanı kadrolarında bulunanlar araştırmacı kadrolarına;..." bölümünün iptali nedeniyle uygulanma imkânı kalmayan anılan fıkranın dördüncü cümlesinin 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrası gereğince iptali gerekir.

V. YÜRÜRLÜĞÜN DURDURULMASI TALEBİ

84. Dava dilekçesinde özetle; dava konusu kuralların uygulanmaları hâlinde telafisi güç veya imkânsız zararların doğabileceği belirtilerek yürürlüklerinin durdurulmasına karar verilmesi talep edilmiştir.

16/6/2020 tarihli ve 7246 sayılı Rekabetin Korunması Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun'un;

A. 1. 6. maddesiyle 7/12/1994 tarihli ve 4054 sayılı Rekabetin Korunması Hakkında Kanun'un 34. maddesine eklenen üçüncü fıkraya,

2. 12. maddesiyle 4054 sayılı Kanun'a eklenen geçici 6. maddenin birinci fıkrasının;

a. Birinci cümlesinin “...Kurum danışmanı, Başkan danışmanı, idari koordinatör, müdür, araştırma uzmanı, basın danışmanı, sistem çözümleyici, veri iletişim uzmanı, programcı, idari hizmet yetkilisi ve idari hizmet uzmanı kadrolarında bulunanlar araştırmacı kadrolarına;...” bölümüne,

b. Dördüncü cümlesine,

yönelik yürürlüğün durdurulması taleplerinin, koşulları oluşmadığından REDDİNE,

B. 1. 3. maddesiyle 4054 sayılı Kanun’un 9. maddesinin değiştirilen birinci fıkrasının birinci cümlesinin “...ve teşebbüslerin belirli faaliyetlerini yahut ortaklık paylarını ya da mal varlıklarını devretmeleri şeklindeki yapısal tedbirleri...” bölümüne,

2. 4. maddesiyle 4054 sayılı Kanun’un 15. maddesinin birinci fıkrasının değiştirilen (a) bendinde yer alan “...bunların kopyalarını ve fiziki örneklerini alabilir,” ibaresine,

yönelik iptal talepleri, 9/11/2022 tarihli, E.2020/67, K.2022/139 sayılı kararlar reddedildiğinden bu bölüme ve ibareye ilişkin yürürlüğün durdurulması taleplerinin REDDİNE,

9/11/2022 tarihinde OYBİRLİĞİYLE karar verilmiştir.

VI. HÜKÜM

16/6/2020 tarihli ve 7246 sayılı Rekabetin Korunması Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun’un;

A. 3. maddesiyle 7/12/1994 tarihli ve 4054 sayılı Rekabetin Korunması Hakkında Kanun’un 9. maddesinin değiştirilen birinci fıkrasının birinci cümlesinin “...ve teşebbüslerin belirli faaliyetlerini yahut ortaklık paylarını ya da mal varlıklarını devretmeleri şeklindeki yapısal tedbirleri...” bölümünün Anayasa’ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

B. 4. maddesiyle 4054 sayılı Kanun’un 15. maddesinin birinci fıkrasının değiştirilen (a) bendinde yer alan “...bunların kopyalarını ve fiziki örneklerini alabilir,” ibaresinin Anayasa’ya aykırı olmadığına ve iptal talebinin REDDİNE, Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, Yusuf Şevki HAKYEMEZ ile Selahaddin MENTEŞ’in karşıoyları ve OYÇOKLUĞUYLA,

C. 6. maddesiyle 4054 sayılı Kanun’un 34. maddesine eklenen üçüncü fıkranın Anayasa’ya aykırı olduğuna ve İPTALİNE OYBİRLİĞİYLE,

Ç. 12. maddesiyle 4054 sayılı Kanun’a eklenen geçici 6. maddenin birinci fıkrasının;

1. Birinci cümlesinin “...Kurum danışmanı, Başkan danışmanı, idari koordinatör, müdür, araştırma uzmanı, basın danışmanı, sistem çözümleyici, veri iletişim uzmanı, programcı, idari hizmet yetkilisi

ve idari hizmet uzmanı kadrolarında bulunanlar arařtırmacı kadrolarına;...” bölümünün Anayasa’ya aykırı olduđuna ve İPTALİNE, Kadir ÖZKAYA, Rıdvan GÜLEÇ, Recai AKYEL, Yıldız SEFERİNOĐLU, Basri BAĐCI, İrfan FİDAN ile Muhterem İNCE’nin karşıoyları ve OYÇOKLUĐUYLA,

2. Dördüncü cümlesinin 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun’un 43. maddesinin (4) numaralı fıkrası geređince İPTALİNE OYBİRLİĐİYLE,

9/11/2022 tarihinde karar verildi.

Başkan

Zühtü ARSLAN

Başkanvekili

Hasan Tahsin GÖKCAN

Başkanvekili

Kadir ÖZKAYA

Üye

Engin YILDIRIM, Muammer TOPAL, M. Emin KUZ, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĐLU, Selahaddin MENTEŞ, Basri BAĐCI, İrfan FİDAN, Kenan YAŞAR, Muhterem İNCE

KARŞIOY GEREKÇESİ

1. Mahkememiz çođunluđu, 7246 sayılı Kanun’un 4. maddesiyle 4054 sayılı Rekabetin Korunması Hakkında Kanun’un (Kanun) 15. maddesinin birinci fıkrasının deđiřtirilen (a) bendinde yer alan “... bunların kopyalarını ve fiziki örneklerini alabilir.” ibaresinin Anayasa’ya aykırı olmadığına karar vermiřtir.

2. Kanun’un “Yerinde İnceleme” kenar bařlıklı 15. maddesinin birinci fıkrasında Rekabet Kurulunun, gerekli gördüđu hallerde teřebbüs ve teřebbüs birliklerinde incelemelerde bulunabilme, bu amaçla teřebbüslerin veya teřebbüs birliklerinin (a) defterlerini, fiziki ve elektronik ortam ile biliřim sistemlerinde tutulan her türlü verilerini ve belgelerini inceleyebilme, bunların kopyalarını ve fiziki örneklerini alabilme, (b) belirli konularda yazılı veya sözlü açıklama isteyebilme ve (c) teřebbüslerin

her türlü mal varlığına ilişkin mahallinde inceleme yapabilme yetkilerine sahip olduğu belirtilmektedir. Dava konusu kural, Kurul tarafından işyerlerinde yapılan incelemelerde teşebbüslere veya teşebbüs birliklerine ait defterlerin, her türlü verilerin ve belgelerin kopyalarının ve fiziki örneklerinin alınabileceğini öngörmektedir.

3. Kural, Anayasa'nın 20. maddesinde güvence altına alınan kişisel verilerin korunmasını isteme hakkına ve 21. maddesinde korunan konut dokunulmazlığı hakkına yönelik müdahale teşkil etmektedir. Kuşkusuz bu haklar mutlak değildir. Anayasa'nın 13. maddesi uyarınca temel hak ve özgürlükler, özlerine dokunulmaksızın, bir sınırlama sebebinin (meşru amacın) bulunması halinde kanunla sınırlanabilir. Ancak bu sınırlamanın Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmaması gerekmektedir.

4. Anayasa, bu genel güvencelerin yanında, temel hak ve özgürlükleri düzenleyen maddelerde özel ve ilave güvenceye de yer vermiştir. Bu kapsamda Anayasa'nın 20. maddesinde usulüne uygun hâkim kararı olmadıkça kimsenin üstünün, özel kağıtlarının ve eşyalarının aranmayacağı ve bunlara el konulamayacağı belirtilmiştir. Aynı şekilde Anayasa'nın 21. maddesi de usulüne uygun hâkim kararı olmadıkça kimsenin konutuna girilemeyeceğini, arama yapılamayacağını ve buradaki eşyalara el konulamayacağını güvenceye almaktadır. Her iki madde de gecikmesinde sakınca bulunan hâllerde kanunla yetkili kılınmış merciin yazılı emriyle bu işlemlerin yapılabilmesine imkân tanımakta, ancak bu kararın yirmi dört saat içinde görevli hâkimin onayına sunulmasını, hâkim kırk sekiz saat içinde kararını açıklamadığında el koymanın kendiliğinden kalkmasını öngörmektedir.

5. Kural kapsamında, Kurul uzmanlarınca kopyaları ve fiziki örnekleri alınabilen defterler, veriler ve belgelerin kişisel veriler içerdiği, bu anlamda düzenlemenin kişisel verilerin korunmasını isteme hakkına bir sınırlandırma niteliğinde olduğu açıktır. Bu sınırlamanın Anayasa'ya uygun olabilmesi için, öncelikle belli nitelikleri haiz bir kanuna dayanması gerekmektedir.

6. Bu anlamda kanunilik aynı zamanda hukuk devletinin vazgeçilmez unsurlarından biridir. Anayasa Mahkemesi kararlarında vurgulandığı üzere hukuk devletinde, kanuni düzenlemelerin "hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfî uygulamalarına karşı koruyucu önlem içermesi gerekir" (AYM, E.2015/41, K.2017/98, 4/5/2017, § 153).

7. Dava konusu kural, defterler ve belgeler dışında, gerçek kişi de olabilen teşebbüs veya teşebbüs birliklerinin fiziki ve elektronik ortam ile bilişim sistemlerinde tutulan her türlü verilerinin alınabileceğini belirtmektedir. Bu haliyle kural, Kurul yetkilileri tarafından ticari sırlar dahil tüm verilerin işlenmesine imkân tanımaktadır. Buna karşılık, alınan verilerin nasıl ve ne kadar süreyle

kaydedileceğine, belli bir süreden sonra silinip silinmeyeceğine, fiziki örneklerin iade edilip edilmeyeceğine ve benzeri hususlara ilişkin herhangi bir düzenlemeye veya atfa yer verilmiş değildir.

8. Bununla birlikte, çoğunluk kararında olduğu gibi, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda yer alan güvencelerin dava konusu kural uyarınca elde edilen verilerin işlenmesi bakımından da geçerli olduğu ileri sürülebilir (§§ 54-59). Bir an için bu görüşün doğru olduğu kabul edilse bile, iptali istenen kuralla "her türlü veriler" in alınabileceği öngörüldüğünden bu veriler arasında kişilerin rızalarına rağmen işlenebilmesi ancak "kanunlarda öngörülen hâllerde" mümkün olan özel nitelikli kişisel veriler de bulunabilecektir. Ne kural ne de kuralın içinde yer aldığı Kanun, idare tarafından alınabilecek veriler arasında özel nitelikli verilerin bulunmamasını temine yönelik herhangi bir tedbire yer vermiştir.

9. Dolayısıyla kişisel verilerin korunmasını isteme hakkına sınırlama getiren dava konusu kuralın keyfiliğe izin vermeyecek şekilde belirli ve öngörülebilir nitelikte olmadığı, bu nedenle de kanunilik şartını sağlamadığı açıktır. Açıklanan gerekçelerle kural Anayasa'nın 20. maddesine aykırıdır.

10. Diğer yandan Avrupa İnsan Hakları Mahkemesi (AİHM) ve Anayasa Mahkemesi kararlarında konut dokunulmazlığı hakkı -bazı istisnalarla birlikte- işyerlerini de kapsayacak şekilde geniş yorumlanmaktadır. Bu bağlamda, bir kişinin mesleğini sürdürdüğü bürosu, özel bir kişinin işlettiği şirketin faaliyetlerinin yürütüldüğü kayıtlı merkezi, tüzel kişilerin kayıtlı merkezleri, şubeleri ve diğer işyerleri "konut" kapsamında görülebilmektedir (Petri Sallinen/Finlandiya, B. No: 50882/99, 27/12/2005, § 70 ; Günay Dağ ve diğerleri [GK], B.No: 2013/1631, 17/12/2015, § 133).

11. Buna göre Anayasa'nın 21. maddesinde konut dokunulmazlığı için öngörülen hâkim kararı güvencesi, teşebbüslerin yönetim işlerinin yürütüldüğü merkez, şube ve tesisleri için de geçerlidir. Dava konusu kural böyle bir güvenceyi içermemektedir. Kurul uzmanlarının hâkim kararı olmaksızın işyerlerinde inceledikleri defterlerin, verilerin ve belgelerin kopyalarını ve fiziki örneklerini alabilme yetkisine sahip olduğunu belirten kural, konut dokunulmazlığı hakkını da ihlal etmektedir.

12. Kuralla verilen yetkinin Anayasa'nın 21. maddesi kapsamında gecikmesinde sakınca bulunan hallere münhasır olduğu da söylenemez. Zira kuralda ve kuralın içinde bulunduğu Kanun'da yerinde incelemenin gecikmesinde sakınca bulunan hallerle sınırlı olarak Kurul'un verdiği yazılı emirle yapılacağına dair herhangi bir düzenleme bulunmamaktadır.

13. Kaldı ki, bir an için böyle yorumlansa bile, Kurul'un yazılı inceleme kararının yirmi dört saat içinde görevli hâkimin onayına sunulmasını zorunlu kılan bir hüküm de yoktur. Kanun'un 15.

maddesinin üçüncü fıkrası uyarınca, hâkim kararıyla inceleme ancak “yerinde incelemenin engellenmesi veya engellenme olasılığının bulunması durumunda” yapılabilmektedir. Dolayısıyla, hâkim kararı olmadan incelenen defter, veri ve belgelerin alınabilmesine izin veren kuralın Anayasa’nın 21. maddesinin sözüne aykırı olduğu açıktır.

14. Açıklanan gerekçelerle, kuralın Anayasa’nın 13., 20. ve 21. maddelerine aykırı olduğunu düşündüğümden çoğunluğun aksi yöndeki kararına katılmıyorum.

Başkan

Zühtü ARSLAN

KARŞIOY GEREKÇESİ

1. 7246 sayılı Rekabetin Korunması Hakkında Kanunda Değişiklik Yapılması Hakkında Kanunun 4. maddesiyle, 4054 sayılı Kanunun 15. maddesinin değiştirilen birinci fıkrasının a bendinde yer alan “bunların kopyalarını ve fiziki örneklerini alabilir” ibaresi

2. Kural ile Rekabet Kuruluna 15. maddede verilen yetki kapsamında görevlerini yerine getirirken gerekli gördüğü hallerde teşebbüs ve teşebbüs birliklerinde incelemelerde bulunabileceği ve defterlerini, fiziki ve elektronik ortam ile bilişim sistemlerinde tutulan her türlü verilerini ve belgelerini inceleyebileceği gibi bunların kopyalarını ve fiziki örneklerini alabileceği düzenlenmektedir.

3. Öncelikle kanunların düzenlenmesinde belirliliğin sağlanması, keyfiliğe karşı güvencelerin yer alması zorunludur. AYM’nin kararlarında ifade ettiği gibi; “...hukuk devletinde, kanuni düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfî uygulamalarına karşı koruyucu önlem içermesi gerekir. Kanunda bulunması gereken bu nitelikler hukuki güvenliğin sağlanması bakımından da zorunludur. Zira bu ilke, hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar” (AYM, E.2015/41, K.2017/98, 4/5/2017, par. 153, 154). Kanunilik ilkesi ayrıca Anayasa’nın 13. maddesinde de temel hakların yalnızca kanunla sınırlanabileceği belirtilerek güvence altına alınmıştır. Anayasa’nın 13. maddesinde sınırlama ölçütü olarak belirtilen kanunilik, Anayasa’nın 2.

maddesinde güvenceye bağlanan hukuk devleti ilkesi ışığında yorumlanmalıdır (AYM E. 2020/53 – K. 2021/55, 14/7/2021).

4. İkinci olarak kural ile incelemeye tabi kurumların ticari verileri, sırları veya ticari ilişkiler veya müşteri ilişkileri dolayısıyla kişisel verilerin kopyalarının ve fiziki örneklerinin alınması yetkisi verilmektedir. Bu durumda verilen yetkinin keyfi kullanımına ilişkin güvencelerin varlığı daha da önem kazanmaktadır. Diğer taraftan kuralın kişisel verilerle ilgili boyutu yönünden konunun Anayasa'nın 20/3. maddesi açısından incelenmesi gerekir.

5. Anayasa'nın 20. maddesinin birinci fıkrasında herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş; üçüncü fıkrasında da "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." denilerek kişisel verilerin korunması özel hayatın gizliliğinin korunması kapsamında güvenceye kavuşturulmuştur.

6. Anayasa'nın 20. maddesinin üçüncü fıkrasında düzenlenen kişisel verilerin korunmasını isteme hakkı, insan onurunun korunması ve bireyin kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. İncelenen kuralda denetime konu edilecek kişisel veri niteliğindeki bilgi ve belgelerin ne şekilde kullanılacağına, bu bilgilerin ne suretle ve ne kadar süre ile saklanacağına, ilgililerin söz konusu bilgilere itiraz etme imkânının olup olmadığına, bilgilerin bir müddet sonra silinip silinmeyeceğine, silinecekse bu sırada izlenecek usulün ne olduğuna, yetkinin kötüye kullanımını önlemeye yönelik nasıl bir denetim yapılacağına ilişkin herhangi bir düzenlemeye yer verilmemiştir. Bu nedenlerle de kural Anayasa'nın 13, 20. maddesine aykırılık nedeniyle iptal edilmelidir.

Başkanvekili

Hasan Tahsin GÖKCAN

KARŞI OY GEREKÇESİ

1. Mahkememiz çoğulunca 16.6.2020 tarihli ve 7246 sayılı Rekabetin Korunması Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun'un 12. maddesiyle 4054 sayılı Kanun'a eklenen geçici 6. maddenin birinci fıkrasının birinci cümlesinde yer alan "Kurum danışmanı, Başkan danışmanı, idari koordinatör, müdür, araştırma uzmanı, basın danışmanı, sistem çözümleyici, veri iletişim uzmanı, programcı, idari hizmet yetkilisi ve idari hizmet uzmanı kadrolarında bulunanlar araştırmacı kadrolarına;" ibaresinin iptaline karar verilmiş bulunmaktadır.

2. Aşağıda açıklanan gerekçelerle iptal sonucuna tarafımızca iştirak edilmesi mümkün olmamıştır.

3. 4054 sayılı Kanun'un, iptali istenilen ibareleri de içeren geçici 6. maddesinin birinci fıkrasında, "Bu maddenin yürürlüğe girdiği tarihte Kurumda inceleme uzmanı kadrosunda bulunanlar rekabet uzmanı kadrolarına ve kıdemli koordinatör ile mesleki koordinatör kadrosunda bulunanlar rekabet başuzmanı kadrolarına; Kurum danışmanı, Başkan danışmanı, idari koordinatör, müdür, araştırma uzmanı, basın danışmanı, sistem çözümleyici, veri iletişim uzmanı, programcı, idari hizmet yetkilisi ve idari hizmet uzmanı kadrolarında bulunanlar araştırmacı kadrolarına; garaj şefi kadrosunda bulunanlar şoför kadrosuna başkaca bir işleme gerek kalmaksızın kadro dereceleriyle atanmış sayılır. Bu şekilde atananların eski kadrolarına bağlı olarak en son ayda fiilî çalışmaya bağlı ödemeler hariç mali haklar kapsamında yapılan her türlü ödemeler toplamı net tutarının (bu tutar sabit bir değer olarak esas alınır), atandıkları yeni kadrolarına bağlı olarak fiilî çalışmaya bağlı ödemeler hariç mali haklar kapsamında yapılan her türlü ödemeler toplamı net tutarından fazla olması halinde aradaki fark tutarı, herhangi bir vergi ve kesintiye tabi tutulmaksızın fark kapanıncaya kadar ayrıca tazminat olarak ödenir. Atandıkları kadro unvanında isteğe bağlı olarak herhangi bir değişiklik olanlarla kendi istekleriyle başka kurumlara atananlara fark tazminatı ödenmesine son verilir. Araştırmacı kadrosuna atananlar Kurumca ihtiyaç duyulan işlerde görevlendirilir." hükmü yer almaktadır.

4. Kanaatimizce dava konusu kuralın Anayasal denetim bağlamında iki yönü bulunmaktadır. Bunlardan ilki, kamu personeli olarak görev yapan kişilerin buldukları görevlerden alınıp başka bir göreve atanmalarının ilkece idari işlemlerle yapılarak onlara bu işlemleri ilgili idari yargı yerlerinde denetlettirme hakkı tanınması gerekirken, kadroların kanunla düzenlenmesi suretiyle kadrosu değiştirilen kişilerin dava açma haklarına engel olunması nedeniyle kuralın anayasaya aykırı olup olmadığı hususu; diğeri de kuralın kişilerin kazanılmış haklarına ölçsüz bir müdahalede bulunup bulunmadığıdır.

5. Anayasa'nın 36. maddesinin birinci fıkrasında, "Herkes meşru vasıta ve yollardan yararlanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir" denilerek yargı organlarına davacı ve davalı olarak başvurabilme ve bunun doğal

sonucu olarak da iddia, savunma ve adil yargılanma hakkı güvence altına alınmıştır. Anayasa'nın 125. maddesinde ise "İdarenin her türlü eylem ve işlemlerine karşı yargı yolu açıktır." denilmektedir.

6. Her iki maddeyle güvence altına alınan dava yoluyla hak arama özgürlüğü, kendisi bir temel hak niteliği taşımasının ötesinde diğer temel hak ve özgürlüklerden gereken şekilde yararlanılmasını ve bunların korunmasını sağlayan en etkili güvencelerden biridir. Kişilere yargı mercileri önünde dava hakkı tanınması adil bir yargılamanın ön koşulunu oluşturur.

7. Kamu personeli olarak görev yapan kişilerin buldukları görevlerden alınmalarını gerektiren haklı bir neden olmadıkça görevlerine son verilememesi, hukukî güvenlik ilkesinin bir gereğidir. Ayrıca kural olarak, kamu personelinin buldukları görevden alınmalarının ve başka bir göreve atanmalarının, haklarında bu yönde bir idari işlem tesis edilmesi yoluyla gerçekleşmesi gerekir. Bununla birlikte, hukukî ve fiilî zorunluluk hallerinde bu hususlarda yasal düzenlemeler yapılabileceği Anayasa Mahkemesi'nce de kabul edilmektedir.

8. Öte yandan bir kamu kurumunun ve buna bağlı olarak bu kurumun gördüğü kamu hizmetinin niteliğinin değiştirilmesine, kaldırılıp kaldırılmayacağına veya bir kamu hizmetinin hangi kamu kurum veya kuruluşunca yerine getirileceğine karar verme yetkisi yasa koyucuya aittir. Yasa koyucu Anayasa'ya uygun olmak kaydıyla, kamu hizmetinin yürütülmesine ilişkin koşulları belirleyerek kadro düzenlemesi yapabilir. Kamu hizmetinin gerekleri yönünden ve kamu yararı amacıyla yeni kadrolar ihdas edebileceği gibi, mevcut bazı kadroları da kaldırabilir. Ayrıca, kamu idareleri ile kamu görevlileri arasındaki ilişkiler, kural tasarruflarla düzenlendiğinden, kamu görevlilerinin statülerine ilişkin yeni kurallar koyabilir ya da var olan kuralları değiştirebilir. (AYM, E.2008/105, K.2010/123, 30/12/2010).

9. Kamu kurum ve kuruluşlarının yeniden yapılandırılmaları kapsamında ortaya çıkan hukukî ve fiilî zorunluluklar nedeniyle getirilen yasal düzenlemelerle teşkilat yapısı değiştirilen kurum ve kuruluşların bazı kadrolarında görev yapan kamu görevlilerinin görevlerinin sona erdirilerek başka kadrolara atanmalarının öngörülmesi durumlarında, ilgililerin başka kadrolara atanmalarının sebep unsurunu, ilgili kurumun ya da kuruluşun yeniden teşkilatlandırılması durumu oluşturur. Bu haller, yürürlükte bulunan kanunlara dayanılarak ve kamu görevlisinin öznel durumu dikkate alınarak idarece tesis edilen naklen atama işlemlerinden farklıdır ve belirtildiği üzere söz konusu hukukî ve fiilî zorunluluklar nedeniyle kazanılmış haklar korunarak başka kadrolara atama yapılması, kanun koyucunun takdir yetkisi kapsamındadır. (AYM, E.2017/160, K.2017/178, 28/12/2017, § 14 - 15)

10. 7246 sayılı Kanunla piyasalardaki teşebbüs ve teşebbüs birliklerinin anlaşma, davranış, karar, birleşme, devralma gibi işlem ve eylemleri nedeniyle Kanun'da sayılan yasakların ihlali sonucu

oluşan rekabeti kısıtlayıcı durumlara ceza ve yaptırımlar dışında davranışsal ve yapısal tedbirlerle son vermeye ilişkin Rekabet Kuruluna yeni görev ve yetkiler verilmiştir. Rekabet Kurumunun kadro yapısının da (taahhüt ve uzlaşma müesseseleri getirilmesi gibi) verilen bu görev ve yetkiler nedeniyle değiştirildiği anlaşılmaktadır. Yeni düzenlemelerle her bir rekabet ihlali iddiası için ayrı ayrı piyasa, sektör ve teşebbüs, finansal, yönetsel veya sair hususlar gibi hususlar yönünden araştırma ve değerlendirme yapılması gerekeceği anlaşılmaktadır. Söz konusu araştırma ve değerlendirmelerin ardından teşebbüslerin davranışlarına, varlıklarını nasıl kullanacaklarına, pazarda rekabet etmelerine veya diğer teşebbüslerle yapacakları sözleşmelere yönelik yükümlülükler içerir nitelikte davranışsal tedbirlere karar verilecektir. Davranışsal tedbirlerin izlenmesi gerekliliği nedeniyle izleme süreçlerine ilişkin tasarım, planlama ve yeniden değerlendirme gerekecektir. Davranışsal tedbirlerin rekabeti kısıtlayıcı ihlalin sona erdirilmesi konusunda sonuç vermediği belirlendiğinde bu defa ilgili teşebbüslerin belirli faaliyetlerini yahut ortaklık paylarını ya da mal varlıklarını devretmeleri şeklindeki yapısal tedbirlerin araştırılması, uygun tedbirin karara bağlanması ve yerine getirilmesinin takibi gerekecektir. Tüm bu süreçlerde ilgili teşebbüslerin uzlaşma ve taahhütleri de söz konusu olabilecektir. Böylesine karmaşık, teknik, yoğun ve uzun süreçlerin sıhhatli takip ve yönetimi ile bilgi akışının sağlanmasının buna uygun kadro değişim ve dönüşümü gerektireceği ortadadır.

11. Bu nedenle bazı kadrolarda görev yapan kamu görevlilerinin görevlerinin sona erdirilerek araştırmacı kadrolarına atanmış sayılmalarının öngörülmesi, yeniden yapılanma sonucu kadro unvan ve derecelerinin değişmesi sonucu ortaya çıkmıştır. İptali istenilen kural, bu hukuki ve fiili imkânsızlığın bir sonucu olup, eski görevlerine atanma imkânı bulunmayan kişilerin söz konusu kuralda olduğu gibi durumlarına uygun başka kadrolara atanmasına imkân sağlayan geçiş hükümlerinin getirilmesi yasa koyucu açısından bir mecburiyet halini almaktadır. Meydana gelebilecek bu değişiklik, daha önce kural tasarrufların doğurmuş olduğu objektif ve genel hukuki durumlara da uygulanabilecektir.

12. Yukarıda yapılan açıklamalar gözetildiğinde, bazı görevlerde bulunan kişiler hakkında yasayla düzenleme yapılmış olmasının Anayasa'nın 36 ve 125. maddelerine aykırılık oluşturmadığı, araştırmacı kadrolarına atanmış sayılanların bu düzenleme aleyhine yargı mercilerine başvurma olanaklarının bulunmamasının hak arama hürriyetinin ihlali olarak değerlendirilemeyeceği sonucuna varılmaktadır.

13. Kazanılmış haklar hususuna gelince:

Anayasa'nın 2. maddesinde belirtilen hukuk devleti ve bu bağlamda hukuki güvenlik ilkesi gereğince, hukuki veya fiili bir zorunluluk olması haline bağlı dahi olsa kamu görevlilerinin

buldukları görevden alınıp başka görevlere atanmaları konusunda bir kanuni düzenleme yapılırken onların bu kapsamdaki kazanılmış haklarının ihlal edilmemesi gerekir.

14. İptali istenilen kural içinde yer aldığı maddenin dava konusu edilmeyen diğer kurallarıyla birlikte değerlendirildiğinde kuralın, kişilerin bulunduğu statülerden doğan, tahakkuk etmiş ve kendileri yönünden kesinleşmiş ve kişisel alacak niteliğine dönüşmüş haklarını ihlal edici nitelikte bir düzenleme olmadığı anlaşılmaktadır. Dolayısıyla kuralla, kazanılmış hakları ihlal edici bir müdahale de söz konusu değildir.

15. Kaldı ki bu kişilerin yeni atandıkları kadrodaki kadrolarına bağlı fiili çalışmaya bağlı yapılan ödemeler hariç mali haklar kapsamında yapılan her türlü ödemeler toplamı net tutarının, eski kadrolarına bağlı olarak en son ayda fiili çalışmaya bağlı olarak yapılan ödemeler hariç mali haklar kapsamında yapılan her türlü ödemeler net tutarından daha düşük olması halinde aradaki fark kapanıncaya kadar fark tazminatı olarak ödenmesi öngörülmektedir.

16. Bu bağlamda ayrıca belirtmek gerekir ki ilgililerin şahsa bağlı hakları kapsamında öngörülen parasal haklarının belli bir süre ile sınırlandırılması hukuki güvenlik ilkesinin ihlali anlamına gelmez.

17. Bu nedenle maddede sayılan görevlerde bulunanların görevlerine son verilerek aynı dereceli araştırmacı unvanlı kadrolara atanmalarını öngören kuralın kazanılmış hakları ihlal ettiği de söylenemez.

18. Açıklanan nedenlerle kural Anayasa'nın 2. ve 36. maddelerine aykırı değildir, iptal talebinin reddi gerekir. Dolayısıyla çoğunluk görüşü doğrultusunda oluşan iptal kararına katılmıyoruz.

Başkanvekili

Kadir ÖZKAYA

Üye Rıdvan GÜLEÇ, Recai AKYEL, Yıldız SEFERİNOĞLU, Basri BAĞCI, İrfan FİDAN, Muhterem İNCE

KARŞIOY GEREKÇESİ

1. Dava konusunu ilgili Kanun'un "...bunların kopyalarını ve fiziki örneklerini alabilir" bölümü oluşturmaktadır. Kural, Kurumun 4154 sayılı Kanun kapsamındaki görevlerini yerine getirirken gerekli gördüğü hallerde teşebbüslerin veya teşebbüs birliklerinin defterlerinin, fiziki ve elektronik ortam ile bilişim sistemlerinde tutulan her türlü veri ve belgelerinin kopyalarını ve fiziki örneklerini alabileceğini düzenlemektedir.

2. Anayasa'nın 20. maddesinin birinci fıkrasında özel hayata saygı hakkı güvence altına alınırken, üçüncü fıkrasında da kişisel verilerin korunmasını isteme hakkı güvenceye bağlanmıştır. Bu fıkralarda hak sahibi "herkes" olarak belirlendiğinden hem gerçek hem de tüzel kişileri kapsamaktadır. Teşebbüs kavramı da tüzel kişiler yanında gerçek kişileri de içermektedir.

3. Anayasa'nın 20. maddesinin üçüncü fıkrası kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsamaktadır. Bununla birlikte kural, demokratik toplum düzeni bakımından gerekli ve ölçülülük açısından da elverişli ve gerekli olmakla beraber orantılı olmayan bir müdahaleye neden olmaktadır çünkü teşebbüse veya teşebbüs birliklerine ait kişisel verilerin elde edilmesi, işlenmesi, ne kadar süreyle muhafaza edileceği, veri sahibi hakkında otomatik sonuç doğurma ve usule ilişkin güvenceler yönlerinden herhangi bir güvence öngörmemektedir.

4. İptali talep edilen kural 4154 sayılı Kanun'un "Yerinde inceleme" başlıklı 15. maddesinde yer almaktadır. Yerinde inceleme, Kurum yetkililerinin teşebbüslerin veya teşebbüs birliklerinin işyerlerine giderek mahallinde inceleme yapmasıdır. Bu çerçevede Kurum yetkilileri teşebbüslerin veya teşebbüs birliklerinin defterlerinin, fiziki ve elektronik ortam ile bilişim sistemlerinde tutulan her türlü veri ve belgelerinin kopyalarını ve fiziki örneklerini inceleyebilir ve alabilirler. Yerinde inceleme teşebbüs ya da teşebbüs birliklerinin işyerlerinde yapılmaktadır. Bu işyerleri Anayasa'nın 21. maddesi çerçevesinde "konut" kavramı içinde değerlendirilebilir.

5. Nitekim Avrupa İnsan Hakları Mahkemesi (AİHM) özel hayata saygı hakkının kapsamında bulunan konuta saygı kavramını iş yerlerini de kapsayacak şekilde genişletmiş; bu bağlamda bir kişinin mesleğini sürdürdüğü bürosunun, özel bir kişinin işlettiği şirketin faaliyetlerinin yürütüldüğü kayıtlı merkezin, tüzel kişilerin kayıtlı merkezlerinin, şubelerinin ve diğer iş yerlerinin bu kapsamda olduğunu ifade etmiştir. Bununla birlikte bütünüyle işe özgülenmiş yerlerin "konut" kavramı kapsamında olmadığını da AİHM vurgulamıştır (Niemietsz/Almanya, B. No:13710/88, 16/12/1992 §30; Soci t  Colas Est c./Fransa, B. No. 37971/97, 16 Nisan 2002, §§ 40-42; Petri Sallinen ve diğ erleri/Finlandiya, B. No: 50882/99, 27/12/2005, § 70).

6. AİHM, Soci t  Colas Est kararında konuta saygı hakkının öznesinin gerçek kişiler olabileceği gibi tüzel kişiler de olabileceğini kabul ederek Avrupa İnsan Hakları S zleşmesi'nin 8. maddesinin bir şirketin genel merkezi, şubesi veya iş yerine saygı gösterilmesi hakkını içerir bir şekilde yorumlanmasının zamanının geldiğini belirterek ilgili başvuruda m fettişlerin, başvuruculara ait yerlere, arama izni olmadan girmelerinin 'konuta' tecav z teşkil ettiğine karar vermiştir.

7. Mahkememiz içtihadında da işyerleri “konut” kavramı içinde kabul edilmektedir ancak tamamıyla işe özgülenmiş kısımlar bunun dışında tutulmaktadır (Mehmet Taşdemir, B. No: 2013/3436, 18/5/2016, § 55).

8. Anayasa'nın 21.maddesinin birinci fıkrasının ikinci cümlesinde millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin konutuna girilemez, arama yapılamaz ve buradaki eşyaya el konulamaz hükmü yer almaktadır. Fıkranın devamında etkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulacağı ve hâkimin, kararını el koymadan itibaren kırk sekiz saat içinde açıklayacağı; aksi halde, el koymanın kendiliğinden kalkacağı düzenlemesi bulunmaktadır.

9. Önümüzdeki kural teşebbüs veya teşebbüs birliklerinin işyerlerinin sadece işe özgülenmemiş kısımlarındaki bilgisayar ve diğer araç ve eşyalarından belge teminine imkân tanıdığından konut dokunulmazlığı hakkına müdahale etmektedir. Konut dokunulmazlığı konut sahibinin rızası dışında konuta girilmemesi anlamına gelmektedir. Konut sahibinin rızası varsa veya rızanın bulunduğu meşru olarak kabul edilirse konut dokunulmazlığı açısından sorun ortaya çıkmaz. Bununla birlikte bu konutu (işyerine) teşebbüs sahiplerinin rekabet uzmanlarının girmelerine açıkça karşı çıkmamaları rızaları olduğu anlamına gelmez. Çünkü 4154 sayılı Kanun'un 15. maddesine göre teşebbüs sahibi yerinde incelemeye rıza göstermek zorundadır. Aksi takdirde para cezası ile karşı karşıya gelecektir.

10. Kanun'un 15. maddesi Kurum uzmanlarının yerinde inceleme yapmak için hâkim kararı olmadan teşebbüslerin veya teşebbüs birliklerinin işyerlerinin salt işe özgülenmemiş kısımlarına yani “konutlarına” girerek defterlerine, fiziki ve elektronik ortam ile bilişim sistemlerinde tutulan her türlü veri ve belgelerinin kopyalarına ve fiziki örneklerini alabilmelerine izin vermektedir. Kurum uzmanlarının yerinde inceleme yapması gecikmesinde sakınca bulunan hallerde meşru olsa bile bunun 24 saat içinde görevli hâkim onayına sunulmasının zorunlu olmaması Anayasa'nın 21. maddesindeki güvencelere aykırılık taşımaktadır.

11. Kuralın, özel hayata saygı hakkına ve konut dokunulmazlığına ölçülü olmayan bir müdahaleye fırsat vermesi Anayasa'nın 13. 20. ve 21. maddeleriyle bağdaşmamaktadır. Bu nedenle çoğunluk kararına katılmıyorum.

Üye

KARŞIOY GEREKÇESİ

1. Mahkememiz çoğunluğunun 16/6/2020 tarihli ve 7246 sayılı Rekabetin Korunması Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun'un 4. maddesiyle 4054 sayılı Kanun'un 15. maddesinin birinci fıkrasının değiştirilen (a) bendinde yer alan "...bunların kopyalarını ve fiziki örneklerini alabilir" ibaresinin Anayasa'ya aykırı olmadığına ve iptal talebinin reddine ilişkin kararına katılmamaktayım.

2. Bahse konu maddede "Yerinde inceleme" başlığı altında Rekabet Kurulunun Kanun'un kendisine verdiği görevleri yerine getirirken gerekli gördüğü hallerde teşebbüs ve teşebbüs birliklerinin defterlerini, fiziki ve elektronik ortam ile bilişim sistemlerinde tutulan her türlü verilerini ve belgelerini inceleme yetkisi kullanması öngörülmüş olup iptali talep edilen ibareyle Kurula bu amaçla fiziki ve elektronik ortam ile bilişim sistemlerinde tutulan her türlü veri ve belgenin kopyalarını ve fiili örneklerini alabilme yetkisi verilmiştir.

3. Öncelikle kuraldaki fiziki ve elektronik ortam ile bilişim sistemlerinde tutulan her türlü veri ve belgenin kopyaları ve fiziki örneklerinin Anayasa'nın 20. maddesi kapsamına giren kişisel veri niteliğinde olduğunun tespit edilmesi gerekir. Anayasanın 20. maddesinin (3) numaralı fıkrasında herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğuna işaret edildikten sonra kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenlenmesi gerektiği ifade edilmiştir.

4. Dava konusu Kanun'da iptali gerektiği kanaatinde olduğum ibarede her türlü veri ve belgenin kopyalarını ve fiili örneklerini alabilme yetkisi düzenlenmiş olmasına rağmen Kanun'da elde edilecek bu kopya ve fiziki örneklerin nasıl kullanılacağı, nerede işleneceği ve saklanacağı konusunda Anayasa'nın 20. maddesinin (3) numaralı fıkrasında aranan koşulları karşılayacak güvencelere yer verilmediği görülmektedir.

5. Dolayısıyla bu bağlamda Kanun'la teşebbüs ve teşebbüs birliklerinin kişisel verilerine yapılan müdahalenin kanunilik bağlamında Anayasa'nın 13. maddesinde aranan niteliklere sahip olmadığı anlaşıldığından dava konusu "bunların kopyalarını ve fiziki örneklerini alabilir" şeklindeki ibarenin Anayasa'nın 13. ve 20. maddelerine aykırılık gerekçesiyle iptali gerektiği kanaatiyle çoğunluğun aksi yöndeki kararına katılmamaktayım.

Üye

KARŞI OY GEREKÇESİ

16/6/2020 tarih 7246 sayılı kanunun 4. Maddesiyle 4054 sayılı kanunun 1. Fıkrasının a bendi ile değiştirilen (a) "... bunların kopyalarını ve fiziki örneklerini alabilirler," ibaresinin Anayasa'ya aykırı olmadığına sayın çoğunlukça karar verilmiştir. Aşağıda belirttiğim gerekçelerle sayın çoğunluğun görüşüne katılmadım.

Dava konusu kural ile 4054 sayılı kanun kapsamındaki görevlilerin görevlerini yerine getirirken gerekli gördüğü hallerde teşebbüslerin veya teşebbüs birliklerinin defterlerinin fiziki ve elektronik ortam ile bilişim sistemlerinde tutulan her türlü verilerinin ve belgelerinin kopyalarını ve fiziki örneklerini alabileceğini düzenlemektedir.

Dava konusu kuralın tekabül ettiği anayasal hakların neler olduğunu belirlenmesi gerekir.

Kural ile yerinde incelemenin belirtilen teşebbüsleri her türlü malvarlığına ilişkin mahallinde incelemeler yapmasına izin vermektedir. Bu nedenle incelemelerin iş yerinde yapılması halinde iş yerinin konut kapsamında kalıp kalmadığı belirlenmelidir. AHİM sözleşmesinin 8. Maddesi kapsamında konut kavramının şirketlerin, yönetim ofislerinin, şubeleri ve iş yerlerini de kapsadığı belirtilmektedir.

4054 sayılı kanunun 15. Maddesinde belirtilen yetkiler incelemenin teşebbüsün bütünüyle işe özgülenmiş tesislerinden ziyade yönetim işlerini yürüttüğü merkez, şube ve tesislerinde yapılan faaliyet alanını kapsadığı anlaşılmaktadır.

Somut kural kapsamındaki belge ve verilerin konutta yapılan arama sonucu elde edildiği gözetildiğinde kuralın konut dokunulmazlığı yönünden incelenmesi gerekir.

Anayasa'nın 21. Maddesinin birinci fıkrasının ikinci cümlesinde, usulüne göre verilmiş hakim kararı olmadıkça kimsenin konutuna girilemeyeceği, arama yapılamayacağı, buradaki eşyaya el konulamayacağı belirtilmiştir.

Aynı fıkra da gecikmesinde sakınca bulunan hallerde ise doğrudan hakim kararı yerine kanunla yetkili kılınmış mercii yazılı emrinin yeterli görülebileceği düzenlenmiştir. Ancak bu emrin 24 saat içinde görevli hakim onayına sunulma zorunluluğu getirilmiştir. Yine el koyma kararın 48 saat içinde açıklanması yükümlülüğü getirilmiş, aksi takdirde el koymanın kendiliğinden kalkacağı düzenlenmiştir.

İptale konu 4054 sayılı kanunun 15. Maddesi incelendiğinde rekabet uzmanlarının yerinde inceleme yapabilmesinin kural olarak hakim kararına bağı kılınmadığı görölmektedir. Yerinde yapılan incelemeler çoğunlukla müteşebbisin bütünüyle işe özgülenmiş tesislerinde yapılmayıp Anayasanın 21. Maddesinde korunan konut kapsamında değerlendirilen merkez, şube ve tesislerinde yapılabilecektir. Kural bu haliyle hakim kararı olmadan konut sayılan alanlara girebilme yetkisi tanımaktadır. Kural ile hakim kararının engellenmesi ya da engellenme ihtimalinin varlığı Anayasanın 21. Maddesinde düzenlenen konut dokunulmazlığı hakkını ihlal eder niteliktedir.

Anayasanın 21. Maddesinde düzenlenen konut dokunulmazlığı hakkının güvenceler kapsamında güvenceler içermediği için bu kuralın Anayasanın 21. Maddesi uyarınca iptali gerekmektedir.

Yukarıda belirttiğim gerekçelerle sayın çoğunluğun görüşüne katılmadım.

Üye

Selahaddin MENTEŞ

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2018/137

Karar Sayısı: 2022/86

Karar Tarihi: 30/6/2022

R.G.Tarih-Sayı: 12/1/2023-32071

İPTAL DAVALARINI AÇANLAR:

1. Türkiye Büyük Millet Meclisi üyeleri Engin ALTAY, Özgür ÖZEL, Engin ÖZKOÇ ile birlikte 138 milletvekili (E.2018/137)
2. Türkiye Büyük Millet Meclisi üyeleri Engin ALTAY, Özgür ÖZEL, Engin ÖZKOÇ ile birlikte 132 milletvekili (E.2021/106)

İPTAL DAVALARININ KONUSU:

A. 25/7/2018 tarihli ve 7145 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un;

1. 1. maddesiyle 10/6/1949 tarihli ve 5442 sayılı İl İdaresi Kanunu'nun 11. maddesinin (C) fıkrasına eklenen ikinci paragrafın,

2. 2. maddesiyle 4/1/1961 tarihli ve 211 sayılı Türk Silahlı Kuvvetleri İç Hizmet Kanunu'na eklenen;

a. 56/A maddesinin birinci fıkrasının "...veya bu sebeplere bağılı olarak gecikmesinde sakınca bulunan hâllerde askerî birlik komutanının veya askerî kurum amirinin ya da hukuk hizmetleri başkanı veya birim amirinin yazılı emri..." bölümünün,

b. 56/B maddesinin birinci fıkrasının ikinci cümlesinde yer alan "...gerektiğinde el ile..." ibaresi ile üçüncü ve dördüncü cümlelerinin,

3. 5. maddesiyle 9/7/1982 tarihli ve 2692 sayılı Sahil Güvenlik Komutanlığı Kanunu'na eklenen ek 7. maddenin birinci fıkrasında yer alan "...veya bu sebeplere bağılı olarak gecikmesinde sakınca bulunan hâllerde birlik komutanının veya kurum amirinin yazılı emri..." ibaresinin,

4. 6. maddesiyle 10/3/1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'na eklenen 15/A maddesinin birinci fıkrasında yer alan "...veya bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hâllerde birlik komutanının veya kurum amirinin yazılı emri..." ibaresinin,
5. 8. maddesiyle 6/10/1983 tarihli ve 2911 sayılı Toplantı ve Gösteri Yürüyüşleri Kanunu'nun 6. maddesinin ikinci fıkrasının birinci cümlesine eklenen "...vatandaşların günlük yaşamını aşırı ve katlanılamaz derecede zorlaştırmayacak..." ibaresinin,
6. 9. maddesiyle 2911 sayılı Kanun'un 7. maddesinin değiştirilen ikinci fıkrasının,
7. 10. maddesiyle 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu'nun 30. maddesine eklenen dördüncü ve beşinci fıkraların,
8. 11. maddesiyle 4/11/1983 tarihli ve 2941 sayılı Seferberlik ve Savaş Hali Kanunu'nun 17. maddesinin birinci fıkrasında yer alan "1402 sayılı Sıkıyönetim Kanununun 15 inci maddesinde yazılı suçları işleyenler" ibaresinin "26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 109, 124, 148, 149, 170 ila 172, 179, 185 ila 188, 190, 202, 213 ila 217, 220, 223, 240, 299 ila 339 uncu maddelerinde belirtilen suçları işleyenler" şeklinde değiştirilmesi ile anılan maddeye eklenen ikinci, üçüncü ve dördüncü fıkraların,
9. 12. maddesiyle 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu'na eklenen ek 4. maddenin birinci fıkrasının birinci cümlesinin "...ile Milli Güvenlik Kurulunca Devletin millî güvenliğine karşı faaliyette bulunduğu karar verilen yapı, oluşum veya gruplara üyeliği, mensubiyeti ve iltisakı yahut bunlarla irtibatı nedeniyle kamu görevinden çıkarılanların..." ve "...bu silahların mülkiyetinin kamuya geçirilmesine karar verilir ve 10/7/1953 tarihli ve 6136 sayılı Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanunun ek 8 inci maddesine göre ilgili idarelerce işlem tesis edilir..." bölümlerinin,
10. 13. maddesiyle 3713 sayılı Kanun'a eklenen geçici 19. maddenin,
11. 16. maddesiyle 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu'nun 134. maddesinin;
- a. (1) numaralı fıkrasının birinci cümlesinde yer alan "...Cumhuriyet savcısının istemi üzerine..." ibaresinin "hakim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından..." şeklinde değiştiren ibarede bulunan "...veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı..." ibaresinin,
- b. (1) numaralı fıkrasına eklenen ikinci, üçüncü ve dördüncü cümlelerin,
- c. (2) numaralı fıkrasının birinci cümlesine eklenen "ya da işlemin uzun sürecek olması" ibaresinin,

12. 21. maddesiyle 18/10/2016 tarihli ve 6749 sayılı Olağanüstü Hal Kapsamında Alınan Tedbirlere İlişkin Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun'un 4. maddesinin (2) numaralı fıkrasına eklenen üçüncü cümlelerin,

13. 22. maddesiyle 1/2/2018 tarihli ve 7075 sayılı Olağanüstü Hal İşlemleri İnceleme Komisyonu Kurulması Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun'un 10. maddesinin değiştirilen (1) numaralı fıkrasının;

a. Üçüncü cümlesinin,

b. Dördüncü cümlesinin "...Ankara, İstanbul, İzmir illeri dışında ve 2006 yılından sonra kurulan yükseköğretim kurumlarına öncelik verilmek kaydıyla, Yükseköğretim Kurulu Başkanlığı tarafından kamu görevinden çıkarıldığı yükseköğretim kurumu haricinde tespit edilecek yükseköğretim kurumlarından birine..." bölümünün,

c. Dokuzuncu ve on üçüncü cümlelerinin,

14. 23. maddesiyle 7075 sayılı Kanun'a eklenen 10/A maddesinin,

15. 24. maddesiyle 7075 sayılı Kanun'a eklenen geçici 3. maddenin (3) numaralı fıkrasının ikinci cümlesinin,

16. 26. maddesiyle 27/6/1989 tarihli ve 375 sayılı Kanun Hükmünde Kararname'ye eklenen geçici 35. maddenin,

17. Geçici 1. maddesinin,

B. 18/7/2021 tarihli ve 7333 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un;

1. 11. maddesiyle 3713 sayılı Kanun'un geçici 19. maddesinde yer alan "...üç yıl..." ibaresinin "...dört yıl..." şeklinde değiştirilmesinin,

2. 20. maddesiyle 7145 sayılı Kanun'un geçici 1. maddesinin (1) numaralı fıkrasında yer alan "...üç yıl..." ibaresinin "...altı yıl..." şeklinde değiştirilmesinin,

3. 23. maddesiyle 375 sayılı Kanun Hükmünde Kararname'nin geçici 35. maddesinin (A), (B), (C), (Ç), (D) ve (G) fıkralarında yer alan "...üç yıl..." ibarelerinin "...dört yıl..." şeklinde değiştirilmesinin,

Anayasa'nın Başlangıç kısmı, 2., 6., 9., 10., 13., 15., 17., 19., 20., 22., 23., 34., 35., 36., 38., 40., 48., 49., 70., 74., 118., 119., 125., 128., 129., 138., 142. ve 153. maddelerine aykırılığı ileri sürülerek iptallerine ve yürürlüklerinin durdurulmasına karar verilmesi talepleridir.

I. İPTALİ İSTENEN KANUN HÜKÜMLERİ

A. 7145 sayılı Kanun'un iptali talep edilen kuralların da yer aldığı;

(...)

7.10. maddesiyle 2937 sayılı Kanun'un 30. maddesine eklenen dördüncü ve beşinci fıkraları şöyledir:

“(Ek fıkra: 25/7/2018-7145/10 md.) MİT'in tarafı olduğu hukuk uyuşmazlıklarında, dava şartı olarak öngörülen arabuluculuk dâhil, arabuluculuk usulü uygulanmaz.

(Ek fıkra: 25/7/2018-7145/10 md.) MİT, 9/10/2003 tarihli ve 4982 sayılı Bilgi Edinme Hakkı Kanunu kapsamı dışındadır.”

(...)

II. İLK İNCELEME

A. E.2018/137 Sayılı Başvuru Yönünden

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Zühtü ARSLAN, Burhan ÜSTÜN, Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Rıdvan GÜLEÇ, Recai AKYEL ve Yusuf Şevki HAKYEMEZ'in katılımlarıyla 17/10/2018 tarihinde yapılan ilk inceleme toplantısında dosyada eksiklik bulunmadığından işin esasının incelenmesine, yürürlüğü durdurma talebinin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

B. E.2021/106 Sayılı Başvuru Yönünden

2. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Engin YILDIRIM, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĞLU, Selahaddin MENTEŞ, Basri BAĞCI ve İrfan FİDAN'ın katılımlarıyla 13/10/2021 tarihinde yapılan ilk inceleme toplantısında dosyada eksiklik bulunmadığından işin esasının incelenmesine, yürürlüğü durdurma talebinin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

III. BİRLEŞTİRME KARARI

3. 18/7/2021 tarihli ve 7333 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un;

A. 11. maddesiyle 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu'nun geçici 19. maddesinde yer alan "...üç yıl..." ibaresinin "...dört yıl..." şeklinde değiştirilmesinin,

B. 20. maddesiyle 25/7/2018 tarihli ve 7145 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un geçici 1. maddesinin (1) numaralı fıkrasında yer alan "...üç yıl..." ibaresinin "...altı yıl..." şeklinde değiştirilmesinin,

C. 23. maddesiyle 27/6/1989 tarihli ve 375 sayılı KHK'nın geçici 35. maddesinin (A), (B), (C), (Ç), (D) ve (G) fıkralarında yer alan "...üç yıl..." ibarelerinin "...dört yıl..." şeklinde değiştirilmesinin,

iptallerine ve yürürlüklerinin durdurulması talebiyle açılan davaya ilişkin E.2021/106 sayılı davanın, aralarındaki hukuki irtibat nedeniyle E.2018/137 sayılı dava ile BİRLEŞTİRİLMESİNE, esas incelemenin E.2018/137 sayılı dosya üzerinden yürütülmesine, 13/10/2021 tarihinde OYBİRLİĞİYLE karar verilmiştir.

IV. ESASIN İNCELENMESİ

4. Dava dilekçesi ve ekleri, Raportör Yakup MACİT tarafından hazırlanan işin esasına ilişkin rapor, dava konusu kanun hükümleri, dayanılan ve ilgili görülen Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

(...)

F. Kanun'un 10. Maddesiyle 2937 Sayılı Kanun'un 30. Maddesine Eklenen Dördüncü ve Beşinci Fıkraların İncelenmesi

1. Dördüncü Fıkra

a. Anlam ve Kapsam

147. 2937 sayılı Kanun'un 30. maddesinin dava konusu dördüncü fıkrasında, Millî İstihbarat Teşkilatı'nın (MİT) tarafı olduğu hukuk uyuşmazlıklarında, dava şartı olarak öngörülen arabuluculuk dâhil, arabuluculuk usulünün uygulanmayacağı düzenlenmiştir.

148. 7/6/2012 tarihli ve 6325 sayılı Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu'nun 2. maddesinin (b) bendinde arabuluculuk, sistematik teknikler uygulayarak görüşmek ve müzakerelerde bulunmak amacıyla tarafları bir araya getiren, onların birbirini anlamalarını ve bu suretle çözümlerini kendilerinin üretmesini sağlamak için aralarında iletişim sürecinin kurulmasını gerçekleştiren, tarafların çözüm üretmediklerinin ortaya çıkması hâlinde çözüm önerisi de getirebilen, uzmanlık eğitimi almış olan tarafsız ve bağımsız bir üçüncü kişinin katılımıyla ve ihtiyari olarak yürütülen uyuşmazlık çözüm yöntemi olarak tanımlanmıştır.

149. Anılan Kanun'un 1. maddesinin (2) numaralı fıkrasına göre bir uyuşmazlığın arabuluculuk uygulamasına konu olabilmesi için özel hukuka ilişkin olması ve tarafların üzerinde serbestçe tasarruf edebilecekleri iş ve işlemlerden kaynaklanması gerekmektedir.

150. Kanun'un 3. maddesinin (1) numaralı fıkrasında da dava şartı olarak arabuluculuğun düzenlendiği Kanun'un 18/A maddesi istisna olmak üzere tarafların, arabulucuya başvurmak, arabuluculuk sürecini devam ettirmek, sonuçlandırmak, bundan vazgeçmek konularında serbest oldukları hükme bağlanmıştır.

151. Bu yönüyle Türk hukukunda kural olarak ihtiyari arabuluculuk sistemi benimsenmiştir. Ancak bazı dava türlerinde dava açılmadan önce arabulucuya başvurulması zorunluluğu getirilmek suretiyle arabuluculuk dava şartı olarak öngörülmüştür.

b. İptal Talebinin Gerekçesi

152. Dava dilekçesinde özetle; dava konusu kuralda ihtiyari ya da zorunlu olarak bütün kişi ve kurumlar için öngörülen arabuluculuk usulünün MİT bakımından uygulanmamasının eşitlik ilkesiyle bağdaşmadığı, Anayasa Mahkemesinin yerleşik içtihadına göre aynı durumda olanlar arasında farklı uygulama getiren kuralın Anayasa'ya uygun olduğunun ileri sürebilmesi için farklı muameleyi meşrulaştıran haklı bir nedenin varlığının ortaya konulması gerektiği, MİT'in tarafı olduğu hukuki uyuşmazlıklarda, özellikle de arabuluculuğun dava şartı olarak öngörüldüğü iş uyuşmazlıklarında arabuluculuğa başvurulmasının yasaklanmasını meşru kılacak objektif bir nedenin bulunmadığı, MİT'in bazı işlem ve ilişkilerinin devlet sırrı niteliği taşımasının arabuluculuğa başvurulması imkân veya zorunluluğunu ortadan kaldıran bir neden olarak görülemeyeceği, nitekim arabulucuların da sır saklama yükümlülüğü altında olduğu belirtilerek kuralın Anayasa'nın 2., 10., 17., 36., 70., 74. ve 125. maddelerine aykırı olduğu ileri sürülmüştür.

c. Anayasaya Aykırılık Sorunu

153. Anayasa'nın 10. maddesinde "Herkes, dil, ırk, renk, cinsiyet, siyasî düşünce, felsefî inanç, din, mezhep ve benzeri sebeplerle ayırım gözetilmeksizin kanun önünde eşittir./ Kadınlar ve erkekler eşit haklara sahiptir. Devlet, bu eşitliğin yaşama geçmesini sağlamakla yükümlüdür. Bu maksatla alınacak tedbirler eşitlik ilkesine aykırı olarak yorumlanamaz./ Çocuklar, yaşlılar, özürllüleri, harp ve vazife şehitlerinin dul ve yetimleri ile malul ve gaziler için alınacak tedbirler eşitlik ilkesine aykırı sayılmaz./ Hiçbir kişiye, aileye, zümreye veya sınıfa imtiyaz tanınamaz./ Devlet organları ve idare makamları bütün işlemlerinde kanun önünde eşitlik ilkesine uygun olarak hareket etmek zorundadırlar." denilmek suretiyle kanun önünde eşitlik ilkesine yer verilmiştir.

154. Anayasa'nın anılan maddesinde belirtilen kanun önünde eşitlik ilkesi hukuksal durumları aynı olanlar için söz konusudur. Bu ilke ile eylemler değil hukuksal eşitlik öngörülmüştür. Eşitlik ilkesinin amacı aynı durumda bulunan kişilerin kanunlar karşısında aynı işleme bağlı tutulmalarını sağlamak, ayırım yapılmasını ve ayrıcalık tanınmasını önlemektir. Bu ilkeyle, aynı durumda bulunan kimi kişi ve topluluklara ayrı kurallar uygulanarak kanun karşısında eşitliğin ihlali yasaklanmıştır. Kanun önünde eşitlik, herkesin her yönden aynı kurallara bağlı tutulacağı anlamına gelmez. Durumlarındaki özellikler, kimi kişiler ya da topluluklar için değişik kuralları ve uygulamaları gerektirebilir. Aynı hukuksal durumlar aynı, ayrı hukuksal durumlar farklı kurallara bağlı tutulursa Anayasa'da öngörülen eşitlik ilkesi zedelenmez (AYM, E.2019/13, K.2021/31, 29/04/2021, § 94).

155. MİT'in tarafı olduğu hukuk uyuşmazlıklarında zorunlu ve ihtiyari arabuluculuk hükümlerinin uygulanmaması bağlamında eşitlik ilkesi yönünden yapılacak anayasallık denetiminde öncelikle Anayasa'nın 10. maddesi çerçevesinde aynı ya da benzer durumda bulunan kişilere farklı uygulamanın mevcut olup olmadığı belirlenmelidir. Yapılacak bu belirlemenin ardından farklı uygulamanın nesnel ve makul bir temele dayanıp dayanmadığı ve ölçülü olup olmadığı hususları incelenmelidir.

156. Özel hukuk hükümleri kapsamında sözleşmeden kaynaklanan haklarının kullanımı, şartları ve sınırları ile ilgili olarak MİT'le sözleşme yapan gerçek ve tüzel kişilerle kamu görevi veya belirli kamu hizmetlerini yapmak üzere kurulan devletin başka bir kurumuyla özel hukuk ilişkisine giren kişilerin benzer hukuki konumda oldukları açıktır.

157. Dava konusu kuralla tarafların özel hukuktan kaynaklanan ve devletin diğer kurumlarının taraf olduğu bir uyuşmazlıkta gerçek ve tüzel kişiler arabuluculuk kurumundan yararlanmaya devam ederken MİT'le arasında özel hukuk uyuşmazlığı bulunan kişiler ise söz konusu müesseseden ve bunun getireceği faydalardan mahrum kalacaklardır. Bu yönüyle kuralla MİT ile arasında özel hukuk uyuşmazlığı bulunan ve arabuluculuk kurumuna başvurmak isteyen kişiler aleyhine farklı bir uygulama getirilmiştir.

158. Eşitlik ilkesinin gereği olarak karşılaştırma yapılmaya müsait olacak şekilde benzer durumda olanlar arasından bir kısmı lehine getirilen farklı düzenlemenin bir ayrıcalık niteliğinde olmaması için nesnel ve makul bir temele dayanması ve ölçülü olması gerekir. Bu konuda yapılacak değerlendirmede arabuluculuk kurumuna başvurmak isteyen kişilerle arasında özel hukuk uyuşmazlığı bulunan MİT'in diğer devlet kurumları karşısındaki konumuna değinmek gerekir.

159. 2937 sayılı Kanun'un 4. maddesinde, Türkiye Cumhuriyeti'nin ülkesi ve milleti ile bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, anayasal düzenine ve millî gücünü meydana getiren bütün

unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkında millî güvenlik istihbaratını devlet çapında oluşturmak MİT'in temel görevleri arasında sayılmıştır. Anılan Kanun'un 6. maddesinde MİT'in görevlerini yerine getirirken gizli çalışma usul, prensip ve tekniklerini kullanabileceği, 12. maddesinde de MİT personelinin kimliğinin gizlenmesinin esas olduğu belirtilmiştir.

160. Söz konusu hükümlere göre MİT'in ülke güvenliğini sağlamak üzere dış ve iç tehditlere karşı faaliyetlerini gizlilik prensibi çerçevesinde yürüttüğü söz konusu faaliyetlerin niteliği dikkate alındığında MİT'in teşkilat yapısının diğer devlet kurumlarından farklı özellikler taşıdığı anlaşılmaktadır. Kuralın "Düzenlemeyle, MİT personelinin kimliğinin gizli tutulmasının zorunluluğu dikkate alınarak Milli İstihbarat Teşkilatının tarafı olduğu özel hukuk uyuşmazlıklarında, dava şartı olarak öngörülen arabuluculuk dahil olmak üzere, arabuluculuk usulünün uygulanmaması amaçlanmaktadır. Böylelikle, MİT'in taraf olduğu özel hukuk uyuşmazlıklarında, arabuluculuğun dava şartı olarak öngörüldüğü 7036 sayılı İş Mahkemeleri Kanunu dahil, mevzuatta yer alan arabuluculuğa ilişkin tüm hükümlerin uygulanmayacağı hüküm altına alınmaktadır." şeklindeki gerekçesinde de belirtildiği üzere MİT personelinin kimliğinin gizli tutularak güvenliğinin sağlanması suretiyle istihbarat hizmetlerinin sağlıklı bir şekilde yürütülmesinin amaçlandığı anlaşılmaktadır. Bu açıdan kuralla yapılan ayırımın nesnel ve makul bir temelden yoksun olduğu söylenemez.

161. Kural kapsamında getirilen farklı uygulamanın aynı zamanda ölçülülük ilkesine uygun olması gerekir. Ölçülülük ilkesi, amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder. Diğer bir ifadeyle bu ilke, farklı uygulamanın öngörülen objektif amaç ile orantılı olmasını gerektirmektedir.

162. Hukuk sistemi ile toplumsal ihtiyaçlar arasındaki bağlantının bir sonucu olarak uyuşmazlıkların çözümünü kolaylaştırmak, adalet yapısının işleyişini hızlandırmak amacıyla devletler birtakım tercihlerde bulunabilir. Dolayısıyla hak arama özgürlüğünün en önemli araçlarından biri olan uyuşmazlığın mahkeme önünde dava konusu yapılmadan önce çözüme kavuşturulması, bu tercihten ortaya çıkmaktadır. Hukuk devletinde kanun koyucunun anayasal ilkelere bağlı kalmak şartıyla özel hukuk uyuşmazlıklarında alternatif uyuşmazlık çözüm yolu öngörüp öngörmemek veya hangi davalara söz konusu kurumların uygulanacağını, bunların şartlarını, kişi veya kurum yönünden kapsam ve sınırlarını belirlemede takdir yetkisi bulunmaktadır. Hukuk uyuşmazlıklarında alternatif uyuşmazlık çözüm yolu olarak öngörülen arabuluculuk da kanun koyucunun anılan takdir yetkisi kapsamında ihdas edilmiş bir kurumdur.

163. Dolayısıyla hukuk uyuşmazlıklarında asıl olan dava yoluyla uyuşmazlığın çözüme kavuşturulması olduğuna göre gizlilik ilkesinin sağlanması amacıyla MİT'in taraf olduğu uyuşmazlıklarda arabuluculuk hükümlerinin uygulanmamasını öngören kuralın getirdiği farklı uygulamanın söz konusu amaca ulaşma bakımından orantılı olmadığı söylenemez. Dolayısıyla ölçülülüğü aşan nitelikte farklı bir uygulama getirmeyen kuralın eşitlik ilkesini ihlal eden bir yönü bulunmamaktadır.

164. Açıklanan nedenlerle kural, Anayasa'nın 10. maddesine aykırı değildir. İptal talebinin reddi gerekir.

Kuralın Anayasa'nın 2. maddesine de aykırı olduğu ileri sürülmüş ise de bu bağlamda belirtilen hususların Anayasa'nın 10. maddesi yönünden yapılan değerlendirmeler kapsamında ele alınmış olması nedeniyle Anayasa'nın 2. maddesi yönünden ayrıca bir inceleme yapılmasına gerek görülmemiştir.

Kuralın Anayasa'nın 17., 36., 70., 74. ve 125. maddeleriyle ilgisi görülmemiştir.

2. Beşinci Fıkra

a. İptal Talebinin Gerekçesi

165. Dava dilekçesinde özetle; 9/10/2003 tarihli ve 4982 sayılı Bilgi Edinme Kanunu hükümlerinin, bilgi edinme hakkı kapsamı dışında tutulan durumlarda dahi kişilerin çalışma hayatını ve meslek onurunu etkileyecek durumlarda istihbarata ilişkin bilgi ve belgelere bireylerin erişmesine imkân tanıdığı, kuralın MİT tarafından toplanan ve kişilerin haysiyetini, itibarını, çalışma hayatını ilgilendiren her türlü bilgiyi anılan Kanun'un kapsamı dışına çıkardığı, Kanun'un 5. maddesinin ikinci fıkrasında yer alan "Bu Kanun yürürlüğe girdiği tarihten itibaren diğer kanunların bu Kanuna aykırı hükümleri uygulanmaz" hükmüyle kuralın açıkça çeliştiği, bu durumun hukuk güvenliği ilkesiyle bağdaşmadığı, istihbarat birimlerinin elindeki bilgiye dayalı olarak kişiler hakkında tesis edilen işlemlerin hangi nedenden kaynaklandığının öğrenilmesinin yanlış ise bunun düzeltilmesine imkân tanınmasının hukuk devleti ilkesinin bir gereği olduğu belirtilerek kuralın Anayasa'nın 2., 10., 17., 36., 70., 74. ve 125. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasaya Aykırılık Sorunu

166. 6216 sayılı Kanun'un 43. maddesi uyarınca kural, ilgisi nedeniyle Anayasa'nın 20. maddesi yönünden de incelenmiştir.

167. 2937 sayılı Kanun'un 30. maddesinin dava konusu beşinci fıkrasında MİT'in 4982 sayılı Kanun kapsamı dışında olduğu düzenlenmiştir.

168. Anayasa'nın 74. maddesinin dördüncü fıkrasında " Herkes, bilgi edinme ve kamu denetçisine başvurma hakkına sahiptir." denilmek suretiyle bilgi edinme hakkı anayasal güvenceye kavuşturulmuştur. Bilgi edinme hakkı, yönetilenlerin yönetenleri denetleyebilmesinin, dolayısıyla hukukun üstünlüğünün sağlanabilmesinin önemli bir aracı olarak işlev görmektedir. Bilgi edinme hakkı, devletin demokratik niteliğinin geliştirilmesi ve bireyin temel hak ve özgürlüklerinin korunması hususlarında önemli bir rol oynadığından demokratik hukuk devletinde vazgeçilmez bir hak niteliğine sahip bulunmaktadır (AYM, E.2013/114, K.2014/184, 4/12/2014, § 37).

169. Anılan maddenin yedinci fıkrasında ise "Bu maddede sayılan hakların kullanılma biçimi kanunla düzenlenir." denilmek suretiyle bu hakka ilişkin kuralın norm alanını belirleme yetkisi kanun koyucunun takdirine bırakılmıştır.

170. Kuralla MİT'in 4982 sayılı Kanun kapsamı dışına çıkarılması suretiyle bilgi edinme hakkına yönelik bir sınırlama öngörülmektedir.

171. Anayasa'nın 20. maddesinin üçüncü fıkrasında "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir" denilerek kişisel verilerin korunması özel hayatın gizliliğinin korunması hakkı kapsamında güvenceye kavuşturulmuştur.

172. Anayasa Mahkemesinin yerleşik kararlarında belirtildiği üzere "...adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler..." kişisel veri olarak kabul edilmektedir (AYM, E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2014/74, K.2014/201, 25/12/2014; E.2014/180, K.2015/30, 19/3/2015; E.2015/32, K.2015/102, 12/11/2015).

173. Kişisel verilerin korunmasını isteme hakkı, insan onurunun korunması ve bireyin kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır (AYM, E.2020/24, K. 2021/39, 3/6/2021, § 42).

174. Kural kapsamında erişim yasağı getirilen bilgi ve belgelerin bir kısmının kişisel veri niteliğinde olması mümkündür. Bu açıdan MİT tarafından düzenlenen, bireylerin özel hayatı, iş ve sosyal yaşamıyla ilgili belge ve bilgilere erişme, bunların düzeltilmesi ve silinmesini talep etme imkânının ortadan kaldırılması suretiyle kişisel verilerin korunmasını isteme hakkına da sınırlama getirilmektedir.

175. Kuralda öngörülen istisnanın kapsam ve sınırlarının açıkça belirlendiği gözetildiğinde kuralla bilgi edinme ve kişisel verilerin korunmasını isteme haklarına getirilen sınırlamanın kanuni bir temele dayandığı açıktır.

176. Anayasa'da bilgi edinme ve kişisel verilerin korunmasını isteme haklarına yönelik herhangi bir sınırlama nedeni öngörülmemiş olmakla birlikte özel sınırlama nedeni belirtilmemiş hakların da o hakkın doğasından kaynaklanan bazı sınırlarının bulunduğu kabul edilmektedir. Öte yandan Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevler, özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebilir (AYM, E.2018/99, K.2021/14, 3/3/2021, § 24).

177. MİT bünyesindeki mevcut bilgi ve belgelere 4982 sayılı Kanun kapsamında erişme imkânını ortadan kaldıran kuralın ülke güvenliğine ilişkin istihbarat faaliyetlerinin zafiyete uğratılmaması gerekçesiyle getirildiği, böylelikle millî güvenliğin korunmasına yönelik meşru bir amaç taşıdığı anlaşılmaktadır.

178. Kuralla bilgi edinme ve kişisel verilerin korunmasını isteme hakkına getirilen sınırlamanın demokratik toplum düzeninin gereklerine uygun ve ölçülü olması gerekir.

179. Kuralla getirilen sınırlamanın ülke güvenliğine ilişkin istihbarat faaliyetlerinin zafiyete uğratılmaması böylelikle millî güvenliğin korunması amacına ulaşma bakımından elverişli olmadığı söylenemez. Ancak sınırlama aynı zamanda meşru amaç yönünden gerekli ve orantılı olmalıdır.

180. Şeffaf ve açık yönetim anlayışının egemen olduğu demokratik toplumlarda hukuk devleti ilkesinin bir gereği olarak kamu gücünü elinde bulunduran idarenin tesis ettiği işlemlere karşı oluşturulan denetim mekanizmalarından birisi de idarenin işlem ve eylemlerine esas alınan ve erişilebilir nitelikte olmayan bilgi, belgeler ile kişisel verilere bireylerin ulaşmasına imkân tanınmasıdır. Böylelikle idarenin keyfî uygulamalarının önüne geçilmesi sağlanabilir.

181. Bu bağlamda kanun koyucunun bireylerce söz konusu bilgi ve belgelere ulaşılmasından elde edilecek fayda ile bunların gizli tutulması hâlinde oluşacak kamu yararı arasında bir denge kurması gerekmektedir. Bilgi ve belge erişimine yönelik sınırlamalar ancak bu dengenin sağlanmasıyla birlikte ölçülü olarak kabul edilebilir.

182. Gizlilik ilkesi doğrultusunda yurt içi ve dışında devletin varlığına ve ülke bütünlüğüne yönelik tehlikelere karşı faaliyet yürüten ve millî güvenlik istihbaratını ulusal düzeyde oluşturmakla görevli bir kurum olan MİT'in güvenlik alanında önemli bir işleve sahip olduğu açıktır.

183. 4982 sayılı Kanun'un 4. maddesinde, herkesin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının faaliyetleri ile ilgili bilgi edinme hakkına sahip olduğu belirtilmiş, 5. maddesinin birinci fıkrasında, kurum ve kuruluşların, bu Kanunda yer alan istisnalar dışındaki her türlü bilgi veya belgeyi başvuranların yararlanmasına sunmak ve bilgi edinme başvurularını etkin, süratli ve doğru sonuçlandırmak üzere gerekli idari ve teknik tedbirleri almakla yükümlü oldukları ifade edilmiştir.

184. Anılan Kanun'un 15 ila 28. maddelerinde bilgi edinme hakkını sınırlandıran durumlar düzenlenmiştir. Kanun'un 16. maddesinde açıklanması hâlinde devletin emniyetine, dış ilişkilerine, millî savunmasına ve millî güvenliğine açıkça zarar verecek ve niteliği itibarıyla devlet sırrı olan gizlilik dereceli bilgi veya belgelerin, 18. maddesinde sivil ve askerî istihbarat birimlerinin görev ve faaliyetlerine ilişkin bilgi veya belgelerin bilgi edinme hakkı kapsamı dışında olduğu belirtilmiştir. 18. maddenin ikinci fıkrasında ise istihbarata ilişkin bilgi ve belgelerin kişilerin çalışma hayatını ve meslek onurunu etkileyecek nitelikte olması hâlinde bunların bilgi edinme hakkı kapsamı içinde olduğu hükme bağlanmıştır.

185. Kanun'un 5. maddesinin ikinci fıkrasında da, Kanun'un yürürlüğe girdiği tarihten itibaren diğer kanunların bu Kanun'a aykırı hükümlerinin uygulanmayacağı belirtilmiştir.

186. Anılan hükümlere göre MİT'in görev ve faaliyetleri kapsamında elde ettiği veya hazırladığı ve doğası itibarıyla gizli olan, istihbarat niteliğindeki bilgi ve belgelerin bireylerin erişimine açılması mümkün değildir. İstihbarata ilişkin bilgi ve belgelere ise yalnızca kişilerin çalışma hayatını ve meslek onurunu etkileyecek nitelikte olması hâlinde bu kişiler hakkında tesis edilen işleme yönelik olarak söz konusu işlemi tesis eden kurumdan talep edilmek üzere ulaşılması mümkündür. Bunun yanında MİT bünyesinde, açıklandığında devletin emniyetine, dış ilişkilerine, millî savunmasına ve millî güvenliğine açıkça zarar verecek gizli veya istihbari nitelikte olmayan bilgi ve belgelerin 4982 sayılı Kanun kapsamında bireylerin erişimine açık olduğu anlaşılmaktadır.

187. Kuralla MİT'in herhangi bir istisna öngörülmeden Bilgi Edinme Kanunu kapsamı dışına çıkarılmasınının 4982 sayılı Kanun çerçevesinde istihbarat faaliyeti dışında kalan veya bu faaliyet içinde olmakla birlikte kişilerin çalışma hayatını ve meslek onurunu etkileyen bilgi ve belgelere bireylerin ulaşamaması sonucu doğmaktadır.

188. Bu açıdan MİT'in istihbarat niteliğinde olmayan ya da bu kapsamda olsa dahi kişilerin çalışma hayatı ve meslek onuru gibi belirli konularda ve yalnızca işlem tesis eden kurumdan talep edilebilmek üzere bilgi ve belgelere erişimini sağlayan 4982 sayılı Kanun kapsamından çıkarılması suretiyle MİT bünyesindeki bilgilere ulaşılmasına kategorik olarak yasak getirilmesi, kişilerin Anayasa'da güvence altına alınan bilgi edinme hakkını kullanma imkânını tamamen ortadan kaldırmaktadır. Böylelikle kuralla bilgi edinme ve kişisel verilerin korunması hakkına getirilen sınırlamada kişilerin söz konusu haklardan kaynaklanan yarar ile kamusal yarar arasındaki dengenin kişiler aleyhine bozulduğu anlaşılmaktadır. Dolayısıyla millî güvenlik, kamu düzeni ve kamu güvenliğinin tesis edilmesi ve korunması amaçlarına ulaşma bakımından bilgi edinme ve kişisel verilerin korunması hakkına getirilen sınırlamanın zorunlu toplumsal ihtiyacı karşılamaya yönelik olmadığı gibi söz konusu meşru amaç yönünden ölçülü olduğu da söylenemez.

189. Açıklanan nedenlerle kural, Anayasa'nın 13., 20. ve 74. maddelerine aykırıdır. İptali gerekir.

Kadir ÖZKAYA, Muammer TOPAL, Rıdvan GÜLEÇ, Basri BAĞCI ve İrfan FİDAN bu görüşe katılmamışlardır.

Kural, Anayasa'nın 13., 20. ve 74. maddelerine aykırı görülerek iptal edildiğinden ayrıca Anayasa'nın 2. maddesi yönünden incelenmemiştir.

Kuralın Anayasa'nın 10., 17., 36., 70. ve 125. maddeleri ile bir ilgisi görülmemiştir.

(...)

VI. YÜRÜRLÜĞÜN DURDURULMASI TALEBİ

1031. Dava dilekçesinde özetle, dava konusu kuralların bu hâliyle uygulanmasınının telafisi güç veya imkânsız zararların doğmasına sebebiyet vereceği belirtilerek kuralların yürürlüklerinin durdurulmasına karar verilmesi talep edilmiştir.

A. 25/7/2018 tarihli ve 7145 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un;

1. 2. maddesiyle 4/1/1961 tarihli ve 211 sayılı Türk Silahlı Kuvvetleri İç Hizmet Kanunu'na eklenen;

- a. 56/A maddesinin birinci fıkrasının "...veya bu sebeplere bađlı olarak gecikmesinde sakınca bulunan hâllerde askerî birlik komutanının veya askerî kurum amirinin ya da hukuk hizmetleri başkanı veya birim amirinin yazılı emri..." bölümüne,
- b. 56/B maddesinin birinci fıkrasının;
- i. İkinci cümlesinde yer alan "...gerektiğinde el ile..." ibaresine,
- ii. İkinci cümlede yer alan "...aracı,..." ibaresi yönünden üçüncü ve dördüncü cümlelerine,
2. 5. maddesiyle 9/7/1982 tarihli ve 2692 sayılı Sahil Güvenlik Komutanlığı Kanunu'na eklenen ek 7. maddenin birinci fıkrasında yer alan "...veya bu sebeplere bađlı olarak gecikmesinde sakınca bulunan hâllerde birlik komutanının veya kurum amirinin yazılı emri..." ibaresine,
3. 6. maddesiyle 10/3/1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'na eklenen 15/A maddesinin birinci fıkrasında yer alan "...veya bu sebeplere bađlı olarak gecikmesinde sakınca bulunan hâllerde birlik komutanının veya kurum amirinin yazılı emri..." ibaresine,
4. 9. maddesiyle 6/10/1983 tarihli ve 2911 sayılı Toplantı ve Gösteri Yürüyüşleri Kanunu'nun 7. maddesinin deđiştirilen ikinci fıkrasına,
5. 10. maddesiyle 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu'nun 30. maddesine eklenen beşinci fıkraya,
6. 11. maddesiyle 4/11/1983 tarihli ve 2941 sayılı Seferberlik ve Savaş Hali Kanunu'nun ibare deđişikliği yapılan ve fıkra eklenen 17. maddesine,
7. 12. maddesiyle 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu'na eklenen ek 4. maddenin birinci fıkrasının birinci cümlesinin;
- a. "...ile Milli Güvenlik Kurulunca Devletin millî güvenliğine karşı faaliyette bulunduđuna karar verilen yapı, oluşum veya gruplara üyeliđi, mensubiyeti ve iltisakı yahut bunlarla irtibatı nedeniyle kamu görevinden çıkarılanların..." bölümünde yer alan "...Milli Güvenlik Kurulunca..." ve "...üyeliđi, mensubiyeti ve..." ibarelerine,
- b. "...bu silahların mülkiyetinin kamuya geçirilmesine karar verilir ve 10/7/1953 tarihli ve 6136 sayılı Ateşli Silahlar ve Bıçaklar ile Diđer Aletler Hakkında Kanunun ek 8 inci maddesine göre ilgili idarelerce işlem tesis edilir." bölümüne,
8. 13. maddesiyle 3713 sayılı Kanun'a eklenen geçici 19. maddenin (c) bendine,

9. 21. maddesiyle 18/10/2016 tarihli ve 6749 sayılı Olağanüstü Hal Kapsamında Alınan Tedbirlere İlişkin Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun'un 4. maddesinin (2) numaralı fıkrasına eklenen üçüncü cümleye,

10. 22. maddesiyle 1/2/2018 tarihli ve 7075 sayılı Olağanüstü Hal İşlemleri İnceleme Komisyonu Kurulması Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun'un 10. maddesinin değiştirilen (1) numaralı fıkrasının;

a. Dördüncü cümlesinin "...Ankara, İstanbul, İzmir illeri dışında ve 2006 yılından sonra kurulan yükseköğretim kurumlarına öncelik verilmek kaydıyla, Yükseköğretim Kurulu Başkanlığı tarafından kamu görevinden çıkarıldığı yükseköğretim kurumu haricinde tespit edilecek yükseköğretim kurumlarından birine..." bölümüne,

b. Dokuzuncu cümlesinde yer alan "...ile mali hakları..." ibaresine,

c. On üçüncü cümlesine,

11. 23. maddesiyle 7075 sayılı Kanun'a eklenen 10/A maddesine,

12. 26. maddesiyle 27/6/1989 tarihli ve 375 sayılı Kanun Hükmünde Kararname'ye eklenen geçici 35. maddenin;

a. (A) fıkrasının birinci paragrafının;

i. Birinci cümlesinde yer alan "...Millî Güvenlik Kurulunca..." ve "...üyeliği, mensubiyeti veya..." ibarelerine,

ii. İkinci ve üçüncü cümlelerine,

iii. Beşinci cümlesinde yer alan "Görevden uzaklaştırılanlar veya..." ibaresine,

b. (B) fıkrasının;

i. Birinci paragrafında yer alan "...Millî Güvenlik Kurulunca..." ve "...üyeliği, mensubiyeti veya..." ibarelerine,

ii. Dördüncü paragrafının;

(1) Birinci Cümlesinde yer alan "...Millî Güvenlik Kurulunca..." ve "...üyeliği, mensubiyeti veya..." ibarelerine,

(2) Üçüncü ve dördüncü cümlelerine,

c. (C) fıkrasının "...üç yıl..." ibaresi dışında kalan kısmına,

ç. (Ç) fıkrasının;

i. Birinci paragrafının "...üç yıl..." ibaresi dışında kalan kısmına,

ii. İkinci paragrafının "...üç yıl..." ibaresi dışında kalan kısmına,

d. (D) fıkrasının "...üç yıl..." ibaresi dışında kalan kısmına,

e. (E) fıkrasında yer alan "...ve (D)..." ibaresine,

f. (F) fıkrasına,

g. (G) fıkrasının

i. Birinci;

(1) Paragrafında yer alan "...Milli Güvenlik Kurulunca..." ve "...üyeliği, mensubiyeti veya..." ibarelerine,

(2) Paragrafının (a) bendine,

ii. İkinci paragrafına,

13. Geçici 1. maddesinin (2) numaralı fıkrasına,

B. 18/7/2021 tarihli ve 7333 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un 23. maddesiyle 375 sayılı KHK'nın geçici 35. maddesinin (C), (Ç) ve (D) fıkralarında yer alan "...üç yıl..." ibarelerinin "...dört yıl..." şeklinde değiştirilmesine,

yönelik yürürlüğün durdurulması taleplerinin koşulları oluşmadığından REDDİNE,

C. 7145 sayılı Kanun'un;

1. 1. maddesiyle 10/6/1949 tarihli ve 5442 sayılı İl İdaresi Kanunu'nun 11. maddesinin (C) fıkrasına eklenen ikinci paragrafa,

2. 2. maddesiyle 211 sayılı Kanun'a eklenen 56/B maddesinin birinci fıkrasının ikinci cümlesinde yer alan "...üstleri,..." ve "...eşyaları..." ibareleri yönünden üçüncü ve dördüncü cümlelerine,

3. 8. maddesiyle 2911 sayılı Kanun'un 6. maddesinin ikinci fıkrasının birinci cümlesine eklenen "..., vatandaşların günlük yaşamını aşırı ve katlanılamaz derecede zorlaştırmayacak..." ibaresine,

4. 10. maddesiyle 2937 sayılı Kanun'un 30. maddesine eklenen dördüncü fıkraya,

5. 12. maddesiyle 3713 sayılı Kanun'a eklenen ek 4. maddenin birinci fıkrasının birinci cümlesinin "...ile Milli Güvenlik Kurulunca Devletin millî güvenliğine karşı faaliyette bulunduğu karar verilen yapı, oluşum veya gruplara üyeliği, mensubiyeti ve iltisakı yahut bunlarla irtibatı nedeniyle

kamu görevinden çıkarılanların...” bölümünde yer alan “...Millî Güvenlik Kurulunca...” ve “...üyeliği, mensubiyeti ve...” ibarelerinin dışında kalan kısmına,

6. 13. maddesiyle 3713 sayılı Kanun’a eklenen geçici 19. maddenin;

a. (a) ve (b) bentlerine,

b. (a), (b) ve (c) bentleri dışında kalan kısmına,

7. 16. maddesiyle 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu’nun 134. maddesinin;

a. (1) numaralı fıkranın birinci cümlesinin “...Cumhuriyet savcısının istemi üzerine...” ibaresinin “...hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından...” şeklinde değiştirilmesinde yer alan “...veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı...” ibaresine,

b. (1) numaralı fıkrasına eklenen ikinci, üçüncü ve dördüncü cümlelerine,

c. (2) numaralı fıkrasının birinci cümlesine eklenen “...ya da işlemin uzun sürecek olması...” ibaresine,

8. 22. maddesiyle 7075 sayılı Kanun’un 10. maddesinin değiştirilen (1) numaralı fıkrasının dokuzuncu cümlesinin “...ile mali hakları...” ibaresi dışında kalan kısmına,

9. 24. maddesiyle 7075 sayılı Kanun’a eklenen geçici 3. maddenin (3) numaralı fıkrasının ikinci cümlesine,

10. 26. maddesiyle 375 sayılı KHK’ya eklenen geçici 35. maddenin;

a. (A) fıkrasının;

i. Birinci paragrafının;

(1) Birinci cümlesinin “...üç yıl...”, “...Millî Güvenlik Kurulunca...” ve “...üyeliği, mensubiyeti veya...” ibareleri dışında kalan kısmına,

(2) Dördüncü cümlesine,

(3) Beşinci cümlesinin “Görevden uzaklaştırılanlar veya...” ibaresi dışında kalan kısmına,

ii. İkinci paragrafının birinci ve ikinci cümlelerine,

b. (B) fıkrasının;

i. Birinci paragrafının “...üç yıl...”, “...Millî Güvenlik Kurulunca...” ve “...üyeliği, mensubiyeti veya...” ibareleri dışında kalan kısmına,

ii. İkinci ve üçüncü paragraflarına,

iii. Dördüncü paragrafının;

(1) Birinci cümlesinin "...Millî Güvenlik Kurulunca..." ve "...üyeliği, mensubiyeti veya..." ibarelerinin dışında kalan kısmına,

(2) İkinci cümlesine,

c. (E) fıkrasının "...ve (D)..." ibaresi dışında kalan kısmına,

ç. (G) fıkrasının;

i. Birinci paragrafının "...üç yıl...", "...Millî Güvenlik Kurulunca..." ve "...üyeliği, mensubiyeti veya..." ibareleri ile (a) bendi dışında kalan kısmına,

ii. Üçüncü paragrafına,

11. Geçici 1. maddesinin;

a. (1) numaralı fıkrasının "...üç yıl..." ibaresi dışında kalan kısmına,

b. (3) numaralı fıkrasına,

Ç. 7333 sayılı Kanun'un;

1. 11. maddesiyle 3713 sayılı Kanun'un geçici 19. maddesinde yer alan "...üç yıl..." ibaresinin "...dört yıl..." şeklinde değiştirilmesine,

2. 20. maddesiyle 7145 sayılı Kanun'un geçici 1. maddesinin (1) numaralı fıkrasında yer alan "...üç yıl..." ibaresinin "...altı yıl..." şeklinde değiştirilmesine,

3. 23. maddesiyle 375 sayılı KHK'nın geçici 35. maddesinin (A), (B) ve (G) fıkralarında yer alan "...üç yıl..." ibarelerinin "...dört yıl..." şeklinde değiştirilmesine,

yönelik iptal talepleri 30/6/2022 tarihli ve E.2018/137, K.2022/86 sayılı kararlarla reddedildiğinden bu fıkralara, paragraflara, bentlere, kısımlara, bölümlere, cümlelere, ve ibarelere ilişkin yürürlüğün durdurulması taleplerinin REDDİNE,

D. 7145 sayılı Kanun'un;

1. 13. maddesiyle 3713 sayılı Kanun'a eklenen geçici 19. maddenin bentlerini bağlayan hükmünde yer alan "...üç yıl..." ibaresine,

2. 22. maddesiyle 7075 sayılı Kanun'un 10. maddesinin değiştirilen (1) numaralı fıkrasının üçüncü cümlesine,

3. 26. maddesiyle 375 sayılı KHK'ya eklenen geçici 35. maddenin;

a. (A) fıkrasının birinci paragrafının birinci cümlesinde yer alan "...üç yıl..." ibaresine,

b. (B) fıkrasının birinci paragrafında yer alan "...üç yıl..." ibaresine,

c. (C) fıkrasının birinci cümlesinde yer alan "...üç yıl..." ibaresine,

ç. (Ç) fıkrasının;

i. Birinci paragrafında yer alan "...üç yıl..." ibaresine,

ii. İkinci paragrafında yer alan "...üç yıl..." ibaresine,

d. (D) fıkrasının birinci cümlesinde yer alan "...üç yıl..." ibaresine,

e. (G) fıkrasının birinci paragrafında yer alan "...üç yıl..." ibaresine,

4. Geçici 1. maddesinin (1) numaralı fıkrasında yer alan "...üç yıl..." ibaresine,

yönelik iptal talepleri hakkında 30/6/2022 tarihli ve E.2018/137, K.2022/86 sayılı kararlar ile karar verilmesine yer olmadığına karar verildiğinden bu ibarelere ve cümleye ilişkin yürürlüğün durdurulması talepleri hakkında KARAR VERİLMESİNE YER OLMADIĞINA,

30/6/2022 tarihinde OYBİRLİĞİYLE karar verilmiştir.

VII. HÜKÜM

A. 25/7/2018 tarihli ve 7145 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un;

1. 1. maddesiyle 10/6/1949 tarihli ve 5442 sayılı İl İdaresi Kanunu'nun 11. maddesinin (C) fıkrasına eklenen ikinci paragrafın;

a. "...belirli yerlere girişi ve çıkışı kamu düzeni ya da kamu güvenliğini bozabileceği şüphesi bulunan kişiler için sınırlayabilir; belli yerlerde veya saatlerde kişilerin dolaşmalarını, toplanmalarını, araçların seyirlerini düzenleyebilir veya kısıtlayabilir ve..." bölümünün Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ, Yusuf Şevki HAKYEMEZ ve Kenan YAŞAR'ın karşıoyları ve OYÇOKLUĞUYLA,

b. Kalan kısmının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

2. 2. maddesiyle 4/1/1961 tarihli ve 211 sayılı Türk Silahlı Kuvvetleri İç Hizmet Kanunu'na eklenen;

a. 56/A maddesinin birinci fıkrasının "...veya bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hâllerde askerî birlik komutanının veya askerî kurum amirinin ya da hukuk hizmetleri

başkanı veya birim amirinin yazılı emri..." bölümünün Anayasa'ya aykırı olduğuna ve İPTALİNE Muammer TOPAL, Basri BAĞCI ve İrfan FİDAN'ın karşıoyları ve OYÇOKLUĞUYLA,

b. 56/B maddesinin birinci fıkrasının;

i. İkinci cümlesinde yer alan "...gerektiğinde el ile..." ibaresinin Anayasa'ya aykırı olduğuna ve İPTALİNE OYBİRLİĞİYLE,

ii. Üçüncü ve dördüncü cümlelerinin;

(1) İkinci cümlede yer alan "...aracı,..." ibaresi yönünden Anayasa'ya aykırı olduklarına ve İPTALLERİNE OYBİRLİĞİYLE,

(2) İkinci cümlede yer alan "...üstleri,..." ve "...eşyaları..." ibareleri yönünden Anayasa'ya aykırı olmadıklarına ve iptalleri talebinin REDDİNE OYBİRLİĞİYLE,

3. 5. maddesiyle 9/7/1982 tarihli ve 2692 sayılı Sahil Güvenlik Komutanlığı Kanunu'na eklenen ek 7. maddenin birinci fıkrasında yer alan "...veya bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hâllerde birlik komutanının veya kurum amirinin yazılı emri..." ibaresinin Anayasa'ya aykırı olduğuna ve İPTALİNE Muammer TOPAL, Basri BAĞCI ve İrfan FİDAN'ın karşıoyları ve OYÇOKLUĞUYLA,

4. 6. maddesiyle 10/3/1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'na eklenen 15/A maddesinin birinci fıkrasında yer alan "...veya bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hâllerde birlik komutanının veya kurum amirinin yazılı emri..." ibaresinin Anayasa'ya aykırı olduğuna ve İPTALİNE Muammer TOPAL, Basri BAĞCI ve İrfan FİDAN'ın karşıoyları ve OYÇOKLUĞUYLA,

5. 8. maddesiyle 6/10/1983 tarihli ve 2911 sayılı Toplantı ve Gösteri Yürüyüşleri Kanunu'nun 6. maddesinin ikinci fıkrasının birinci cümlesine eklenen "..., vatandaşların günlük yaşamını aşırı ve katlanılamaz derecede zorlaştırmayacak..." ibaresinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

6. 9. maddesiyle 2911 sayılı Kanun'un 7. maddesinin değiştirilen ikinci fıkrasının Anayasa'ya aykırı olduğuna ve İPTALİNE OYBİRLİĞİYLE,

7. 10. maddesiyle 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu'nun 30. maddesine eklenen;

a. Dördüncü fıkranın Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

b. Beşinci fıkranın Anayasa'ya aykırı olduğuna ve İPTALİNE Kadir ÖZKAYA, Muammer TOPAL, Rıdvan GÜLEÇ, Basri BAĞCI ve İrfan FİDAN'ın karşıoyları ve OYÇOKLUĞUYLA,

8. 11. maddesiyle 4/11/1983 tarihli ve 2941 sayılı Seferberlik ve Savaş Hali Kanunu'nun;

a. 17. maddesinin birinci fıkrasında yer alan "...1402 sayılı Sıkıyönetim Kanununun 15 inci maddesinde yazılı suçları işleyenler..." ibaresinin "...26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 109, 124, 148, 149, 170 ila 172, 179, 185 ila 188, 190, 202, 213 ila 217, 220, 223, 240, 299 ila 339 uncu maddelerinde belirtilen suçları işleyenler..." şeklinde değiştirilmesinin ve anılan maddeye eklenen ikinci, üçüncü ve dördüncü fıkraların Anayasa'ya aykırı olduklarına ve İPTALLERİNE OYBİRLİĞİYLE,

b. 17. maddesinin birinci fıkrasının kalan kısmının 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 43. maddesinin (4) numaralı fıkrası gereğince İPTALİNE OYBİRLİĞİYLE,

9. 12. maddesiyle 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu'na eklenen ek 4. maddenin birinci fıkrasının birinci cümlesinin;

a. "...ile Milli Güvenlik Kurulunca Devletin millî güvenliğine karşı faaliyette bulunduğu karar verilen yapı, oluşum veya gruplara üyeliği, mensubiyeti ve iltisakı yahut bunlarla irtibatı nedeniyle kamu görevinden çıkarılanların...";

i. Bölümünde yer alan "...Milli Güvenlik Kurulunca..." ve "...üyeliği, mensubiyeti ve..." ibarelerinin Anayasa'ya aykırı olduklarına ve İPTALLERİNE OYBİRLİĞİYLE,

ii. Bölümünün kalan kısmının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

b. "...bu silahların mülkiyetinin kamuya geçirilmesine karar verilir ve 10/7/1953 tarihli ve 6136 sayılı Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanunun ek 8 inci maddesine göre ilgili idarelerce işlem tesis edilir." bölümünün Anayasa'ya aykırı olduğuna ve İPTALİNE OYBİRLİĞİYLE,

10. 13. maddesiyle 3713 sayılı Kanun'a eklenen geçici 19. maddenin;

a. Bentlerini bağlayan hükmünde yer alan "...üç yıl..." ibaresine ilişkin iptal talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA OYBİRLİĞİYLE,

b. (a) bendinin;

i. Birinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

ii. İkinci, üçüncü ve dördüncü cümlelerinin Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ, Yusuf Şevki HAKYEMEZ ve Kenan YAŞAR'ın karşıoyları ve OYÇOKLUĞUYLA,

c. (b) bendinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

ç. (c) bendinin Anayasa'ya aykırı olduğuna ve İPTALİNE OYBİRLİĞİYLE,

d. Kalan kısmının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

11. 16. maddesiyle 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu'nun 134. maddesinin;

a. (1) numaralı fıkranın birinci cümlesinin "...Cumhuriyet savcısının istemi üzerine..." İbaresinin "...hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından..." şeklinde değiştirilmesinde yer alan "...veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı..." ibaresinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

b. (1) numaralı fıkrasına eklenen ikinci, üçüncü ve dördüncü cümlelerin Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE OYBİRLİĞİYLE,

c. (2) numaralı fıkrasının birinci cümlesine eklenen "...ya da işlemin uzun sürecek olması..." ibaresinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

12. 21. maddesiyle 18/10/2016 tarihli ve 6749 sayılı Olağanüstü Hal Kapsamında Alınan Tedbirlere İlişkin Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun'un 4. maddesinin (2) numaralı fıkrasına eklenen üçüncü cümlelerin Anayasa'ya aykırı olduğuna ve İPTALİNE Kadir ÖZKAYA, Muammer TOPAL, Rıdvan GÜLEÇ, Recai AKYEL, Basri BAĞCI, İrfan FİDAN'ın karşıoyları ve OYÇOKLUĞUYLA,

13. 22. maddesiyle 1/2/2018 tarihli ve 7075 sayılı Olağanüstü Hal İşlemleri İnceleme Komisyonu Kurulması Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun'un 10. maddesinin değiştirilen (1) numaralı fıkrasının;

a. Üçüncü cümlesine ilişkin iptal talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA OYBİRLİĞİYLE,

b. Dördüncü cümlesinin "...Ankara, İstanbul, İzmir illeri dışında ve 2006 yılından sonra kurulan yükseköğretim kurumlarına öncelik verilmek kaydıyla, Yükseköğretim Kurulu Başkanlığı tarafından kamu görevinden çıkarıldığı yükseköğretim kurumu haricinde tespit edilecek yükseköğretim kurumlarından birine..." bölümünün Anayasa'ya aykırı olduğuna ve İPTALİNE OYBİRLİĞİYLE,

c. Dokuzuncu;

i. Cümlesinde yer alan "...ile mali hakları..." ibaresinin Anayasa'ya aykırı olduğuna ve İPTALİNE OYBİRLİĞİYLE,

ii. Cümlesinin kalan kısmının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

ç. On üçüncü cümlesinin Anayasa'ya aykırı olduğuna ve İPTALİNE Basri BAĞCI ve İrfan FİDAN'ın karşıoyları ve OYÇOKLUĞUYLA,

14. 23. maddesiyle 7075 sayılı Kanun'a eklenen 10/A maddesinin;

a. (1) numaralı fıkrası ile (2) numaralı fıkrasının birinci cümlesinin Anayasa'ya aykırı olduklarına ve İPTALLERİNE OYBİRLİĞİYLE,

b. Kalan kısmının 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrası gereğince İPTALİNE OYBİRLİĞİYLE,

15. 24. maddesiyle 7075 sayılı Kanun'a eklenen geçici 3. maddenin (3) numaralı fıkrasının ikinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

16. 26. maddesiyle 27/6/1989 tarihli ve 375 sayılı Kanun Hükmünde Kararname'ye eklenen geçici 35. maddenin;

a. (A) fıkrasının;

i. Birinci paragrafının;

(1) Birinci;

(a) Cümlesinde yer alan "...üç yıl..." ibaresine ilişkin iptal talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA OYBİRLİĞİYLE,

(b) Cümlesinde yer alan "...Millî Güvenlik Kurulunca..." ve "...üyeliği, mensubiyeti veya..." ibarelerinin Anayasa'ya aykırı olduklarına ve İPTALLERİNE OYBİRLİĞİYLE,

(c) Cümlesinin kalan kısmının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ, Yusuf Şevki HAKYEMEZ 'in karşıoyları ve OYÇOKLUĞUYLA,

(2) İkinci ve üçüncü;

(a) Cümlelerinde yer alan "...Resmî Gazetede yayımlanır..." ibarelerinin Anayasa'ya aykırı olduklarına ve İPTALLERİNE OYBİRLİĞİYLE,

(b) Cümlelerin kalan kısımlarınının 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrası gereğince İPTALLERİNE OYBİRLİĞİYLE,

(3) Dördüncü cümlesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ, Yusuf Şevki HAKYEMEZ 'in karşıoyları ve OYÇOKLUĞUYLA,

(4) Beşinci;

(a) Cümlesinde yer alan "Görevden uzaklaştırılanlar veya..." ibaresinin Anayasa'ya aykırı olduğuna ve İPTALİNE OYBİRLİĞİYLE,

(b) Cümlesinin kalan kısmınının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ, Yusuf Şevki HAKYEMEZ 'in karşıoyları ve OYÇOKLUĞUYLA,

ii. İkinci paragrafının;

(1) Birinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ, Yusuf Şevki HAKYEMEZ 'in karşıoyları ve OYÇOKLUĞUYLA,

(2) İkinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ, Yusuf Şevki HAKYEMEZ 'in karşıoyları ve OYÇOKLUĞUYLA,

b. (B) fıkrasının;

i. Birinci;

(1) Paragrafında yer alan "...üç yıl..." ibaresine ilişkin iptal talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA OYBİRLİĞİYLE,

(2) Paragrafında yer alan "...Millî Güvenlik Kurulunca..." ve "...üyeliği, mensubiyeti veya..." ibarelerinin Anayasa'ya aykırı olduklarına ve İPTALLERİNE OYBİRLİĞİYLE,

(3) Paragrafının kalan kısmınının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ, Yusuf Şevki HAKYEMEZ 'in karşıoyları ve OYÇOKLUĞUYLA,

ii. İkinci paragrafının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ, Yusuf Şevki HAKYEMEZ 'in karşıoyları ve OYÇOKLUĞUYLA,

iii. Üçüncü paragrafının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ, Yusuf Şevki HAKYEMEZ 'in karşıoyları ve OYÇOKLUĞUYLA,

iv. Dördüncü paragrafının;

(1) Birinci;

(a) Cümlesinde yer alan "...Millî Güvenlik Kurulunca..." ve "...üyeliği, mensubiyeti veya..." ibarelerinin Anayasa'ya aykırı olduklarına ve İPTALLERİNE OYBİRLİĞİYLE,

(b) Cümlesinin kalan kısmının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ, Yusuf Şevki HAKYEMEZ 'in karşıoyları ve OYÇOKLUĞUYLA,

(2) İkinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ, Yusuf Şevki HAKYEMEZ 'in karşıoyları ve OYÇOKLUĞUYLA,

(3) Üçüncü cümlesinin Anayasa'ya aykırı olduğuna ve İPTALİNE Basri BAĞCI ve İrfan FİDAN'ın karşıoyları ve OYÇOKLUĞUYLA,

(4) Dördüncü cümlesinin Anayasa'ya aykırı olduğuna ve İPTALİNE OYBİRLİĞİYLE,

c. (C) fıkrasının;

i. Birinci cümlesinde yer alan "...üç yıl..." ibaresine ilişkin iptal talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA OYBİRLİĞİYLE,

ii. Kalan kısmının Anayasa'ya aykırı olduğuna ve İPTALİNE OYBİRLİĞİYLE,

ç. (Ç) fıkrasının;

i. Birinci;

(1) Paragrafında yer alan "...üç yıl..." ibaresine ilişkin iptal talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA OYBİRLİĞİYLE,

(2) Paragrafının "Bu maddenin yürürlüğe girdiği tarihten itibaren...süreyle; terör örgütlerine veya Millî Güvenlik Kurulunca Devletin millî güvenliğine karşı faaliyette bulunduğu karar verilen yapı,

oluşum veya gruplara üyeliği, mensubiyeti veya iltisakı yahut bunlarla irtibatı nedeniyle hakkında inceleme ve soruşturma yürütülen kişiler ile bunların eş ve çocuklarına ilişkin olarak yetkili kurul, komisyon ve diğer mercilerce ihtiyaç duyulan, ... telekomünikasyon yoluyla iletişimin tespiti de dâhil olmak üzere her türlü bilgi ve belge, kamu ve özel tüm kurum ve kuruluşlarca vakit geçirilmeksizin verilir." bölümünün Anayasa'ya aykırı olduğuna ve İPTALİNE OYBİRLİĞİYLE,

(3) Paragrafının kalan kısmının 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrası gereğince İPTALİNE OYBİRLİĞİYLE,

ii. İkinci;

(1) Paragrafında yer alan "...üç yıl..." ibaresine ilişkin iptal talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA OYBİRLİĞİYLE,

(2) Paragrafının kalan kısmının Anayasa'ya aykırı olduğuna ve İPTALİNE OYBİRLİĞİYLE,

d. (D) fıkrasının;

i. Birinci;

(1) Cümlesinde yer alan "...üç yıl..." ibaresine ilişkin iptal talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA OYBİRLİĞİYLE,

(2) Cümlesinin kalan kısmının Anayasa'ya aykırı olduğuna ve İPTALİNE OYBİRLİĞİYLE,

ii. Kalan kısmının 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrası gereğince İPTALİNE OYBİRLİĞİYLE,

e. (E);

i. Fıkrasında yer alan "...ve (D)..." ibaresinin 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrası gereğince İPTALİNE OYBİRLİĞİYLE,

ii. Fıkrasının kalan kısmının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ, Yusuf Şevki HAKYEMEZ 'in karşıoyları ve OYÇOKLUĞUYLA,

f. (F);

i. Fıkrasında yer alan "...ve (D)..." ibaresinin 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrası gereğince İPTALİNE OYBİRLİĞİYLE,

ii. Fıkrasının kalan kısmının Anayasa'ya aykırı olduğuna İPTALİNE OYBİRLİĞİYLE,

g. (G) fıkrasının;

i. Birinci;

(1) Paragrafında yer alan "...üç yıl..." ibaresine ilişkin iptal talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA OYBİRLİĞİYLE,

(2) Paragrafında yer alan "...Milli Güvenlik Kurulunca..." ve "...üyeliği, mensubiyeti veya..." ibarelerinin Anayasa'ya aykırı olduklarına ve İPTALLERİNE OYBİRLİĞİYLE,

(3) Paragrafının (a) bendinin Anayasa'ya aykırı olduğuna ve İPTALİNE Kadir ÖZKAYA, Muammer TOPAL, Basri BAĞCI ve İrfan FİDAN'ın karşıoyları ve OYÇOKLUĞUYLA,

(4) Paragrafının kalan kısmının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ, Yusuf Şevki HAKYEMEZ 'in karşıoyları ve OYÇOKLUĞUYLA,

ii. İkinci paragrafının Anayasa'ya aykırı olduğuna İPTALİNE OYBİRLİĞİYLE,

iii. Üçüncü paragrafının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ, Yusuf Şevki HAKYEMEZ 'in karşıoyları ve OYÇOKLUĞUYLA,

17. Geçici 1. maddesinin;

a. (1) numaralı;

i. Fıkrasında yer alan "...üç yıl..." ibaresine ilişkin iptal talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA OYBİRLİĞİYLE,

ii. Fıkrasının kalan kısmının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

b. (2) numaralı fıkrasının Anayasa'ya aykırı olduğuna ve İPTALİNE OYBİRLİĞİYLE,

c. (3) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ, Yusuf Şevki HAKYEMEZ 'in karşıoyları ve OYÇOKLUĞUYLA,

B. 18/7/2021 tarihli ve 7333 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un;

1. 11. maddesiyle 3713 sayılı Kanun'un geçici 19. maddesinde yer alan "...üç yıl..." ibaresinin "...dört yıl..." şeklinde değiştirilmesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

2. 20. maddesiyle 7145 sayılı Kanun'un geici 1. maddesinin (1) numaralı fıkrasında yer alan "... yıl..." ibaresinin "...altı yıl..." eklinde deęiřtirilmesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİęİYLE,

3. 23. maddesiyle 375 sayılı KHK'nın geici 35. maddesinin;

a. (A), (B) ve (G) fıkralarında yer alan "... yıl..." ibarelerinin "...dört yıl..." eklinde deęiřtirilmesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ, Yusuf Şevki HAKYEMEZ 'in karşıoyları ve OYÇOKLUĞUYLA,

b. (C), () ve (D) fıkralarında yer alan "... yıl..." ibarelerinin "...dört yıl..." eklinde deęiřtirilmesinin Anayasa'ya aykırı olduklarına ve İPTALLERİNE OYBİRLİęİYLE,

30/6/2022 tarihinde karar verildi.

Başkan

Zühtü ARSLAN

Başkanvekili

Hasan Tahsin GÖKCAN

Başkanvekili

Kadir ÖZKAYA

Üye

Engin YILDIRIM

Üye

Muammer TOPAL

Üye

M. Emin KUZ

Üye

Rıdvan GÜLEÇ

Üye

Recai AKYEL

Üye

Yusuf Şevki HAKYEMEZ

Üye

Selahaddin MENTEŞ

Üye

Basri BAĞCI

Üye

İrfan FİDAN

Üye

Kenan YAŞAR

(...)

Karşı Oy

25/07/2018 tarih ve 7145 sayılı Kanunun; 10. maddesiyle 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nun 30. maddesine eklenen Beşinci Fıkra.

1. Bu düzenleme ile Milli İstihbarat Teşkilatı 4982 sayılı Bilgi Edinme Hakkı Kanunu kapsamı dışına çıkartılmaktadır.

2. Kurumun milli güvenlik alanında görev ifa ettiği nazara alındığında, sahip olduğu bilgilerin çeşitli sınıflandırmalara tabi tutularak kişilerle paylaşılması kurumun fonksiyonuna uygun düşmemektedir.

3. Avrupa İnsan Hakları Mahkemesi kararında istihbari nitelikteki bilgilerin, kişilerin şahsi durumunu etkileyecek nitelikte olsa dahi, şahıslarla paylaşılması noktasında devlete bir yükümlülük getirmemektedir.

4. Bu nedenle anılan hükmün iptali yönündeki çoğunluk fikrine iştirak edilmemiştir.

Başkanvekili

Kadir ÖZKAYA

Üye

Muammer TOPAL

Üye

Rıdvan GÜLEÇ

Üye

Basri BAĞCI

Üye

İrfan FİDAN

(...)

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2021/42

Karar Sayısı: 2022/45

Karar Tarihi: 21/4/2022

R.G. Tarih - Sayı: 30/6/2022 - 31882

İTİRAZ YOLUNA BAŞVURAN: Danıştay Onikinci Dairesi

İTİRAZIN KONUSU: 10/6/2004 tarihli ve 5188 sayılı Özel Güvenlik Hizmetlerine Dair Kanun'un 10. maddesine 1/2/2018 tarihli ve 7072 sayılı Kanun'un 67. maddesiyle eklenen (h) bendinin Anayasa'nın 13., 20. ve 128. maddelerine aykırılığı ileri sürülerek iptaline karar verilmesi talebidir.

OLAY: Hakkında yapılan güvenlik soruşturmasının olumlu bulunmadığı gerekçesiyle sürekli işçi kadrosuna geçirilmemesine ilişkin işleminin iptali talebiyle açılan davada itiraz konusu kuralın Anayasa'ya aykırı olduğu kanısına varan Mahkeme, iptali için başvurmuştur.

I. İPTALİ İSTENEN KANUN HÜKMÜ

Kanun'un itiraz konusu kuralın da yer aldığı 10. maddesi şöyledir:

“Özel güvenlik görevlilerinde aranacak şartlar

Madde 10- Özel güvenlik görevlilerinde aşağıdaki şartlar aranır:

- a) Türkiye Cumhuriyeti vatandaşı olmak.
- b) (Değişik: 21/4/2005 - 5335/23 md.) Silahsız olarak görev yapacaklar için en az sekiz yıllık ilköğretim veya ortaokul; silahlı olarak görev yapacaklar için en az lise veya dengi okul mezunu olmak.
- c) 18 yaşını doldurmuş olmak.
- d) (Değişik: 2/1/2017 - KHK-680/69 md.; Aynen kabul: 1/2/2018-7072/67 md.) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 53 üncü maddesinde belirtilen süreler geçmiş veya hükmün açıklanmasının geri bırakılmasına karar verilmiş olsa bile;
 - 1) Kasten işlenen bir suçtan dolayı bir yıl veya daha fazla süreyle hapis cezasına mahkûm olmamak.
 - 2) Affa uğramış olsa bile Devletin güvenliğine, Anayasal düzene ve bu düzenin işleyişine, özel hayata ve hayatın gizli alanına ve cinsel dokunulmazlığa karşı suçlar ile uyuşturucu veya uyarıcı madde

suçları, zimmet, irtikâp, rüşvet, hırsızlık, dolandırıcılık, sahtecilik, güveni kötüye kullanma, hileli iflas, ihaleye fesat karıştırma, edimin ifasına fesat karıştırma, suçtan kaynaklanan malvarlığı değerlerini aklama, kaçakçılık ve fuhuş suçlarından mahkûm olmamak.

3) Anayasal düzene ve bu düzenin işleyişine, özel hayata ve hayatın gizli alanına, cinsel dokunulmazlığa karşı suçlar ile uyuşturucu veya uyarıcı madde suçlarından dolayı hakkında devam etmekte olan bir soruşturma veya kovuşturma bulunmamak.

e) (Mülga: 23/1/2008 - 5728/578 md.)

f) Görevin yapılmasına engel olabilecek vücut ve akıl hastalığı ile engelli bulunmamak.

g) 14 üncü maddede belirtilen özel güvenlik temel eğitimini başarıyla tamamlamış olmak.

h) (Ek: 2/1/2017-KHK-680/69 md.; Aynen kabul: 1/2/2018-7072/67 md.) Güvenlik soruşturması olumlu olmak.”

II. İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Engin YILDIRIM, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĞLU, Selahaddin MENTEŞ, Basri BAĞCI ve İrfan FİDAN'ın katılımlarıyla 29/4/2021 tarihinde yapılan ilk inceleme toplantısında dosyada eksiklik bulunmadığından işin esasının incelenmesine OYBİRLİĞİYLE karar verilmiştir.

III. ESASIN İNCELENMESİ

2. Başvuru kararı ve ekleri, Raportör Aydın AYGÜN tarafından hazırlanan işin esasına ilişkin rapor, itiraz konusu kanun hükmü, dayanılan Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A. Sınırlama Sorunu

3. Anayasa'nın 152. ile 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 40. maddelerine göre bir davaya bakmakta olan mahkeme, bu dava sebebiyle uygulanacak bir kanunun veya Cumhurbaşkanlığı kararnamesinin hükümlerini Anayasa'ya aykırı görmesi hâlinde veya taraflardan birinin ileri sürdüğü aykırılık iddiasının ciddi olduğu kanısına varması durumunda bu hükümlerin iptalleri için Anayasa Mahkemesine başvurmaya yetkilidir. Ancak anılan maddeler uyarınca bir mahkemenin Anayasa Mahkemesine başvurabilmesi için elinde yöntemince açılmış ve mahkemenin görevine giren bir davanın bulunması, iptali talep edilen kuralın da o davada uygulanacak olması gerekir. Uygulanacak kural ise bakılmakta

olan davanın deęişik evrelerinde ortaya çıkan sorunların çözümünde veya davayı sonuçlandırmada olumlu ya da olumsuz yönde etki yapacak nitelikte bulunan kurallardır.

4. Başvuru kararında 5188 sayılı Kanun'un 10. maddesinin (h) bendinin iptali talep edilmiştir. İtiraz konusu kural özel güvenlik görevlisi olabilmek için güvenlik soruşturmasının olumlu sonuçlanmış olması şartını öngörmektedir.

5. Kuralın öngördüğü güvenlik soruşturması faaliyetleri, 17/4/2021 tarihine kadar 26/10/1994 tarihli ve 4045 sayılı Kanun hükümlerine göre yürütülmekte iken anılan Kanun'un söz konusu tarihte 7/4/2021 tarihli ve 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu'yla yürürlükten kaldırılması üzerine anılan faaliyetler 17/4/2021 tarihinden itibaren 7315 sayılı Kanun hükümlerine göre yürütülmeye devam edilmiştir. Bu itibarla kural hem mülga 4045 sayılı Kanun hem de 7315 sayılı Kanun uyarınca gerçekleştirilen güvenlik soruşturması faaliyetleri bakımından geçerli, ortak kural niteliğindedir.

6. Bakılmakta olan davanın konusunu ise mülga 4045 sayılı Kanun hükümleri çerçevesinde gerçekleştirilen güvenlik soruşturması faaliyeti oluşturmaktadır. Bu nedenle kurala ilişkin esas incelemenin "mülga 26/10/1994 tarihli ve 4045 sayılı Kanun uyarınca yapılan güvenlik soruşturması" yönünden yapılması gerekir.

B. İtirazın Gerekçesi

7. Başvuru kararında özetle; itiraz konusu kuralın özel güvenlik görevlisi olabilmek için güvenlik soruşturmasının olumlu sonuçlanması şartını aradığı, ancak güvenlik soruşturmasını düzenleyen kanunun yalnızca hangi kamu görevlileri bakımından güvenlik soruşturması yapılacağını belirttiği, güvenlik soruşturmasıyla ilgili diğer hususları yönetmeliğe bıraktığı, güvenlik soruşturmasına konu bilgi ve belgelerin neler olduğu, bu bilgi ve belgelerin ne şekilde kullanılacağı, hangi mercilerin soruşturmayı yapacağı hususunda herhangi bir düzenlemeye yer verilmediği, güvenlik soruşturması sonucunda özel güvenlik görevlisi olarak alınmada esas alınacak kişisel veri niteliğindeki bilgilerin alınmasına, kullanılmasına ve işlenmesine yönelik güvence ve temel ilkelerin kanunla belirlenmediği belirtilerek kuralın Anayasa'nın 13., 20. ve 128. maddelerine aykırı olduğu ileri sürülmüştür.

C. Anayasa'ya Aykırılık Sorunu

8. İtiraz konusu kuralla özel güvenlik görevlisi olabilmek için güvenlik soruşturmasının olumlu olması şartı öngörülmüş olup kural "mülga 26/10/1994 tarihli ve 4045 sayılı Kanun uyarınca yapılan güvenlik soruşturması" yönünden incelenmiştir.

9. Anayasa'nın 20. maddesinin birinci fıkrasında herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş; üçüncü fıkrasında da "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." denilerek kişisel verilerin korunması özel hayatın gizliliğinin korunması kapsamında güvenceye kavuşturulmuştur.

10. Kişisel verilerin korunmasını isteme hakkı, insan onurunun korunması ve bireyin kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır.

11. Anayasa Mahkemesinin yerleşik kararlarında belirtildiği üzere "...adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler..." kişisel veri olarak kabul edilmektedir (AYM, E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2014/74, K.2014/201, 25/12/2014; E.2014/180, K.2015/30, 19/3/2015; E.2015/32, K.2015/102, 12/11/2015).

12. Bu bağlamda güvenlik soruşturmasıyla elde edilen veriler kişisel veri niteliğindedir. İtiraz konusu kural, güvenlik soruşturması yapmakla görevli birimler tarafından güvenlik soruşturması kapsamında kişilerin kişisel veri niteliğindeki özel hayatı, iş ve sosyal yaşamıyla ilgili bilgilerinin alınmasına ve bu kayıtların kullanılmasına imkân tanınması nedeniyle kişisel verilerin korunmasını isteme hakkına sınırlama getirmektedir.

13. Anayasa'nın 20. maddesi uyarınca kişisel veriler ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir. Anayasa'nın 13. maddesinde de "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz." hükmüne yer verilerek temel hak ve özgürlüklerin ancak kanunla sınırlanabileceği ifade edilmiştir. Anayasa'nın 13. ve 20. maddeleri uyarınca kişisel verilerin korunmasını isteme hakkını sınırlamaya yönelik kanuni bir

düzenlemenin şeklen var olması yeterli olmayıp yasal kuralların keyfiliğe izin vermeyecek şekilde belirli, ulaşılabilir ve öngörülebilir düzenlemeler niteliğinde olması gerekir.

14. Esasen temel hakları sınırlayan kanunun bu niteliklere sahip olması, Anayasa'nın 2. maddesinde güvenceye bağlanan hukuk devleti ilkesinin de bir gereğidir. Hukuk devletinde, kanuni düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi gerekir. Kanunda bulunması gereken bu nitelikler hukuki güvenliğin sağlanması bakımından da zorunludur. Zira bu ilke hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar (AYM, E.2015/41, K.2017/98, 4/5/2017, §§ 153, 154). Dolayısıyla Anayasa'nın 13. ve 20. maddelerinde sınırlama ölçütü olarak belirtilen kanunilik, Anayasa'nın 2. maddesinde güvenceye bağlanan hukuk devleti ilkesi ışığında yorumlanmalıdır.

15. 5188 sayılı Kanun'un 1. maddesinde anılan Kanun'un amacının, kamu güvenliğini tamamlayıcı nitelikteki özel güvenlik hizmetlerinin yerine getirilmesine ilişkin esas ve usulleri belirlemek olduğu ifade edilmiştir.

16. Kanun'un 7. ve 8. maddelerinde ise özel güvenlik görevlilerinin yetkileri ayrıntılı olarak düzenlenmiştir. Buna göre özel güvenlik görevlileri, koruma ve güvenliğini sağladıkları alanlara girmek isteyenleri duyarlı kapıdan geçirme, bu kişilerin üstlerini arama, 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu'nun 90. ve 168. maddelerine göre yakalama, görev alanında haklarında yakalama emri veya mahkûmiyet kararı bulunan kişileri yakalama ve arama, yangın, deprem gibi tabii afet durumlarında ve imdat istenmesi hâlinde görev alanındaki işyeri ve konutlara girme, genel kolluk kuvvetlerine derhal bildirmek şartıyla, aramalar sırasında suç teşkil eden veya delil olabilecek ya da suç teşkil etmemekle birlikte tehlike doğurabilecek eşyayı emanete alma, zor kullanma, silah taşıma ve bulundurma gibi yetkilere sahiptir.

17. Anılan yetkiler gözetildiğinde özel güvenlik görevlileri bakımından güvenlik soruşturması yapılması yönünde düzenlemeler getirilmesi kanun koyucunun takdir yetkisindedir. Ancak bu alanda düzenleme öngören kuralların kamu makamlarına hangi şartlarda ve hangi sınırlar içinde tedbirler uygulama ve özel hayata saygı gösterilmesini isteme hakkına yönelik müdahalelerde bulunma yetkisi verildiğini yeterince açık olarak göstermesi ve muhtemel kötüye kullanmalara karşı yeterli güvenceleri sağlaması gerekir.

18. Anayasa Mahkemesi 24/7/2019 tarihli ve E.2018/73, K.2019/65 sayılı, 19/2/2020 tarihli ve E.2018/91, K.2020/10 sayılı, 19/2/2020 tarihli ve E.2018/163, K.2020/13 sayılı, 3/6/2021 tarihli ve E.2020/24, K.2021/39 sayılı ile 16/12/2021 tarihli ve E.2020/41, K.2021/91 sayılı kararlarında güvenlik soruşturması ve arşiv araştırması yapılmasını öngören kuralları incelemiştir. Bu kararlarda Anayasa ve kanunlara sadık kalarak faaliyette bulunma yükümlülükleri olan memurların ve kamu görevlilerinin kamu görevlerine atanmalarında birtakım şartların aranmasının doğal olduğu, bu kapsamda kamu görevine atanmadan önce kişilerin güvenlik soruşturmasının ve arşiv araştırmasının yapılmasını öngören kuralların kanun koyucunun takdir yetkisinde bulunduğu belirtilmiştir. Bununla birlikte anılan kararlarda güvenlik soruşturması ve arşiv araştırmasının yapılmasına ve elde edilecek verilerin kullanılmasına ilişkin temel ilkelerin kanunda düzenlenmesi gerektiği ifade edilmiştir (bkz. sırasıyla §§ 170, 171; §§ 132, 134; §§ 15, 17; §§ 47, 49; §§ 17, 19).

19. Kuralla güvenlik soruşturmasının olumlu olması özel güvenlik görevlilerinde bulunması gereken şart olarak düzenlenmesine karşın 17/4/2021 tarihinden önceki süreç yönünden kanunda güvenlik soruşturmasına konu edilecek bilgi ve belgelerin ne şekilde kullanılacağına, hangi mercilerin soruşturmayı yapacağına, bu bilgilerin ne suretle ve ne kadar süre ile saklanacağına, ilgililerin söz konusu bilgilere itiraz etme imkânının olup olmadığına, bilgilerin bir müddet sonra silinip silinmeyeceğine, silinecekse bu sırada izlenecek usulün ne olduğuna, yetkinin kötüye kullanımını önlemeye yönelik nasıl bir denetim yapılacağına ilişkin herhangi bir düzenlemeye yer verilmemiştir. Diğer bir ifadeyle güvenlik soruşturmasının yapılmasına, elde edilecek verilerin kullanılmasına ilişkin temel ilkeler belirlenmeksizin kuralla sadece güvenlik soruşturmasının olumlu olması özel güvenlik görevlisi olmada aranacak şartlar arasında sayılmıştır.

20. Güvenlik soruşturması sonucunda kişisel veri niteliğindeki bilgilerin alınmasına, kullanılmasına, işlenmesine yönelik güvenceler ve temel ilkeler kanunla belirlenmeksizin bunların alınmasına ve kullanılmasına izin verilmesi Anayasa'nın 13. ve 20. maddeleriyle bağdaşmamaktadır (benzer yöndeki kararlar için bkz. AYM, E.2018/73, K.2019/65, 24/7/2019, §§ 171, 172; E.2018/91, K.2020/10, 19/2/2020, §§ 133, 134; E.2018/163, K.2020/13, 19/2/2020, §§ 16, 17; E.2020/24, K.2021/39, 3/6/2021, §§ 48, 49; E.2020/41, K.2021/91, 16/12/2021 § 18, 19; Fatih Saraman [GK], B. No: 2014/7256, §§ 89, 90; Turgut Duman, B. No: 2014/15365, § 88).

21. Açıklanan nedenlerle kural Anayasa'nın 13. ve 20. maddelerine aykırıdır. İptali gerekir.

Kuralın Anayasa'nın 128. maddesiyle ilgisi görülmemiştir.

IV. HÜKÜM

10/6/2004 tarihli ve 5188 sayılı Özel Güvenlik Hizmetlerine Dair Kanun'un 10. maddesine 1/2/2018 tarihli ve 7072 sayılı Kanun'un 67. maddesiyle eklenen (h) bendinin;

A. Esasına ilişkin incelemenin "mülga 26/10/1994 tarihli ve 4045 sayılı Kanun uyarınca yapılan güvenlik soruşturması" yönünden yapılmasına,

B. "mülga 26/10/1994 tarihli ve 4045 sayılı Kanun uyarınca yapılan güvenlik soruşturması" yönünden Anayasa'ya aykırı olduğuna ve İPTALİNE,

21/4/2022 tarihinde OYBİRLİĞİYLE karar verildi.

Başkan

Zühtü ARSLAN

Başkanvekili - Hasan Tahsin GÖKCAN, Kadir ÖZKAYA

Üye - Engin YILDIRIM, Hicabi DURSUN, Muammer TOPAL, M. Emin KUZ, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĞLU, Selahaddin MENTEŞ, Basri BAĞCI, İrfan FİDAN, Kenan YAŞAR

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2019/96

Karar Sayısı: 2022/17

Karar Tarihi: 24/2/2022

R.G. Tarih-Sayısı: 26/5/2022-31847

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri Engin ALTAY, Özgür ÖZEL, Engin ÖZKOÇ ile birlikte 129 milletvekili

İPTAL DAVASININ KONUSU: 6/8/2019 tarihli ve (43) numaralı Bazı Cumhurbaşkanlığı Kararnamelerinde Değişiklik Yapılması Hakkında Cumhurbaşkanlığı Kararnamesi'nin;

A. 1. maddesiyle 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete'de yayımlanan (1) numaralı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin 217. maddesinin (1) numaralı fıkrasının (ğ) bendine [17/4/2020 tarihli ve (60) numaralı CBK'nın 1. maddesiyle 217. maddede yapılan değişiklikten sonra (h) bendi] eklenen "...ve Hazinesin Cumhurbaşkanlığı kararı ile yurtçindeki ya da yurtdışındaki şirketlere iştirak etmesini sağlamak," ibaresinin,

B. 14. maddesiyle (1) numaralı Cumhurbaşkanlığı Kararnamesi'ne eklenen 227/B maddesinin (4) numaralı fıkrasının "...hazine ve maliye başmüfettişleri, müfettişleri ve müfettiş yardımcılarının görev, yetki ve sorumlulukları ile..." bölümünün,

C. 17. maddesiyle (1) numaralı Cumhurbaşkanlığı Kararnamesi'nin değiştirilen 231. maddesinin (1) numaralı fıkrasının (m) bendinin,

Ç. Geçici 1. maddesinin,

Anayasa'nın 2., 5., 8., 20., 35., 47., 104. ve 128. maddelerine aykırılığı ileri sürülerek iptallerine ve yürürlüklerinin durdurulmasına karar verilmesi talebidir.

I. İPTALİ İSTENEN CUMHURBAŞKANLIĞI KARARNAMESİ KURALLARI İLE İLGİLİ GÖRÜLEN MEVZUAT

A. İptali İstenen Cumhurbaşkanlığı Kararnamesi Kuralları

Cumhurbaşkanlığı Kararnamesi'nin (CBK);

1. 1. maddesiyle (1) numaralı CBK'nın 217. maddesinin (1) numaralı fıkrasının ibare eklenen (ğ) bendi [17/4/2020 tarihli ve (60) numaralı CBK'nın 1. maddesiyle 217. maddede yapılan değişiklikten sonra (h) bendi] şöyledir:

“(1) Hazine ve Maliye Bakanlığının görev ve yetkileri şunlardır:

...

h) Hazine işlemleri, kamu finansmanı, kamu sermayeli kuruluş ve işletmeler ve devlet iştirakleri, ikili ve çok taraflı dış ekonomik ilişkiler, uluslararası ve bölgesel ekonomik ve mali kuruluşlarla ilişkiler, yabancı ülke ve kuruluşlardan borç ve hibe alınması ve verilmesi ile ilgili işlemleri yapmak ve Hazinenin Cumhurbaşkanı kararı ile yurtiçindeki ya da yurtdışındaki şirketlere iştirak etmesini sağlamak,”

2. 14. maddesiyle (1) numaralı CBK'ya eklenen 227/B maddesi şöyledir:

“Teftiş Başkanlığı

MADDE 227/B- (Ek:RG-7/8/2019-30855-CK-43/14 md.)

(1) (Ek cümle:RG-18/4/2020-31103-CK-60/5 md.) Teftiş Başkanlığı, Başkan, Başkan Yardımcıları ile Hazine ve Maliye Müfettişleri (Hazine ve Maliye Başmüfettişi, Hazine ve Maliye Müfettişi, Hazine ve Maliye Müfettiş Yardımcısı)'nden oluşur. Teftiş Başkanlığı Bakanın emri veya onayı ile Bakan adına aşağıdaki görev ve yetkileri kullanır:

a) Bakanlık merkez, taşra ve yurtdışı teşkilatları ile bağlı, ilgili ve ilişkili kuruluşlarının her türlü faaliyet ve işlemleriyle ilgili olarak inceleme, denetim ve soruşturma işlerini yürütmek ve bu işlerle ilgili gerekli önlemleri almak veya aldırarak,

b) İlgili mevzuatın Bakanlığa tanındığı inceleme, denetim ve soruşturma yetkisini Bakanlığın diğer hizmet birimlerinin görev alanına girmediği durumlarda kullanmak,

c) İç denetim birimi ve Bakanlığın diğer birimleri tarafından Teftiş Başkanlığına bildirilen konularda gerekli inceleme, denetim ve soruşturma faaliyetlerini yürütmek,

ç) Bakan tarafından verilen diğer görevleri yapmak.

(2) Başkanlıkta 375 sayılı Kanun Hükmünde Kararnamenin ek 24 üncü maddesi uyarınca hazine ve maliye müfettişi ve hazine ve maliye müfettiş yardımcısı istihdam edilebilir.

(3) (Değişik:RG-18/4/2020-31103-CK-60/5 md.) Mali ve sosyal hak ve yardımlar ile diğer özlük hakları bakımından 375 sayılı Kanun Hükmünde Kararnamenin ek 30 uncu maddesi uyarınca Teftiş Başkanı,

Bakanlık Rehberlik ve Teftiş Başkanına; Teftiş Başkan Yardımcısı, Vergi Denetim Kurulu Başkan Yardımcısına denktir.

(4) Teftiş Başkanlığının çalışma usul ve esasları, hazine ve maliye başmüfettişleri, müfettişleri ve müfettiş yardımcılarının görev, yetki ve sorumlulukları ile diğer hususlar Bakanlıkça çıkarılan yönetmelikle belirlenir.”

3. 17. maddesiyle (1) numaralı CBK'nın değiştirilen 231. maddesinin (1) numaralı fıkrası şöyledir;

“(1) Malî Suçları Araştırma Kurulu Başkanlığı doğrudan Bakana bağlı olup görev ve yetkileri şunlardır:

a) Suç gelirlerinin aklanması ve terörizmin finansmanının önlenmesi amacıyla plan, program, politika, strateji hazırlama ve geliştirme süreçlerine katkıda bulunmak, kurum ve kuruluşlar arasında ulusal düzeyde risk değerlendirme çalışmaları da dâhil olmak üzere koordinasyonu sağlamak,

b) Faaliyet alanıyla ilgili mevzuat çalışmaları yapmak,

c) Suç gelirlerinin aklanmasının, terörizmin finansmanının ve ekonomik güvenliğe yönelik risklerin ortaya çıkarılması ve önlenmesi kapsamında gelişmeleri izlemek, önlemler geliştirmek, analiz, araştırma ve inceleme yapmak,

ç) Suç gelirlerinin aklanması ve terörizmin finansmanının önlenmesi kapsamında veri toplamak, şüpheli işlem bildirimlerini almak, analiz etmek ve bunları kaydetmek, istihbarat üretmek, gerekli görüldüğünde üretilen istihbarat ve analiz sonuçları hakkında ilgili birimleri bilgilendirmek,

d) 11/10/2006 tarihli ve 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun, ilgili mevzuat ve bu Cumhurbaşkanlığı Kararnamesi kapsamına giren hususlar ile ilgili olarak analiz, araştırma ve inceleme yapmak veya yaptırmak,

e) Aklama veya terörizmin finansmanı suçunun işlendiğine dair ciddi şüphelerin mevcut olması durumunda konuyu ilgili Cumhuriyet savcılığına intikal ettirmek,

f) Yapılan analiz, araştırma ve inceleme sonucunda aklama ve terörizmin finansmanı suçunun işlendiği hususunda olguların varlığının tespiti halinde, 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre gerekli işlemler yapılmak üzere Cumhuriyet başsavcılığına suç duyurusunda bulunmak,

g) Aklama ve terörizmin finansmanı suçlarına ilişkin olarak Cumhuriyet savcısı, hâkim veya mahkeme tarafından intikal ettirilen konuları analiz etmek ve incelemek,

- ğ) Analiz, araştırma ve inceleme sürecinde gerekli hallerde kolluk ve diğer birimlerden kendi görev alanlarında inceleme ve araştırma yapılması talebinde bulunmak,
- h) Suç gelirlerinin aklanması ve terörizmin finansmanının önlenmesi amacıyla istihbarat ve kolluk birimleri ile işbirliği yapmak ve bilgi alışverişinde bulunmak,
- ı) Suç gelirlerinin aklanması ve terörizmin finansmanının önlenmesi kapsamında risk kategorileri belirlemek ve gerekli hallerde yükümlüleri bilgilendirmek,
- i) 5549 sayılı Kanun ve ilgili mevzuat kapsamında yükümlülük denetimi yapmak veya yapılmasını sağlamak,
- j) Yabancı ülke kanunlarına göre yükümlülük denetimine yetkili mercilerin, merkezi yurtdışında bulunan yükümlülerinin Türkiye'deki birimleri nezdinde yükümlülük denetimi yapmasına ve bu kapsamdaki bilgi taleplerinin cevaplandırılmasına karşılıklılık ilkesi de dikkate alınarak izin vermek,
- k) Gerekli hallerde merkezi Türkiye'de bulunan yükümlülerin yurtdışındaki birimleri nezdinde yükümlülük denetimi yapmak ve bilgi talep etmek,
- l) Görev alanına giren konularda uluslararası ilişkileri yürütmek, yabancı ülkelerdeki muadil kurumlarla görüş ve bilgi alışverişinde bulunmak, bu amaçla uluslararası anlaşma niteliğinde olmayan mutabakat muhtırası imzalamak,
- m) Kamu kurum ve kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği olmayan kuruluşlardan her türlü bilgi ve belgeyi istemek,
- n) Bilgi ve ihtisasına ihtiyaç duyulması halinde, diğer kamu kurum ve kuruluşlarında çalışanların Başkanlık bünyesinde geçici olarak görevlendirilmelerini talep etmek,
- o) Kamuoyu duyarlılığını ve desteğini artırmaya yönelik çalışmalar yapmak,
- ö) Bakan tarafından verilen diğer görevleri yapmak."

4. Geçici 1. maddesi [17/4/2020 tarihli ve (60) numaralı CBK'nın 21. maddesiyle değiştirilmeden önce] şöyledir:

"GEÇİCİ MADDE 1- Bu maddenin yürürlüğe girdiği tarihte Hazine ve Maliye Bakanlığında vergi başmüfettişi, vergi müfettişi ve yeterlik sınavında başarı göstermiş olmak kaydıyla vergi müfettiş yardımcısı kadrolarında bulunanlardan uygun görülenler, bu maddenin yürürlüğe girdiği tarihten itibaren üç ay içerisinde durumlarına uygun hazine ve maliye başmüfettişi, hazine ve maliye müfettişi ya da hazine ve maliye müfettiş yardımcısı kadrolarına doğrudan Hazine ve Maliye Bakanınca

atanabilirler. Bu şekilde atanacakların sayısı hazine ve maliye müfettişi kadro sayısının yüzde ellisini geçemez. Bunların önceki kadrolarında geçirdikleri süreler atandıkları kadrolarda geçmiş sayılır.”

B. İlgili Görülen Mevzuat

1. (1) numaralı CBK'nın 224. maddesinin ilgili bölümü şöyledir:

“Kamu Sermayeli Kuruluş ve İşletmeler Genel Müdürlüğü

MADDE 224- (1) Kamu Sermayeli Kuruluş ve İşletmeler Genel Müdürlüğünün görev ve yetkileri şunlardır:

a) (Değişik:RG-7/8/2019-30855-CK-43/8 md.) Kamu iktisadi teşebbüsleri ve Hazinesinin iştirak ettiği şirketler ile ilgili olarak hazine pay sahipliğinin gerektirdiği her türlü işlemi yapmak,

...”

2. 27/6/1989 tarihli ve 375 sayılı 657 Sayılı Devlet Memurları Kanunu, 926 Sayılı Türk Silahlı Kuvvetleri Personel Kanunu, 2802 Sayılı Hakimler ve Savcılar Kanunu, 2914 Sayılı Yükseköğretim Personel Kanunu, 5434 Sayılı T.C. Emekli Sandığı Kanunu ile Diğer Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması, Devlet Memurları ve Diğer Kamu Görevlilerine Memuriyet Taban Aylığı ve Kıdem Aylığı ile Ek Tazminat Ödenmesi Hakkında Kanun Hükmünde Kararname'nin (KHK) ek 24. maddesinin ilgili bölümü şöyledir:

“Müfettiş, denetmen, denetçi, kontrolör, aktüer istihdamı

Ek Madde 24- (Ek: 2/7/2018 - KHK-703/178 md.)

Bakanlıklar ile diğer kamu kurum ve kuruluşlarının teşkilatlanmasına ilişkin Cumhurbaşkanlığı kararnamelerinde öngörülmesi kaydıyla bakanlık, kurum ya da birim düzeyinde müfettiş, denetmen, denetçi, kontrolör, aktüer ile müfettiş yardımcısı, denetmen yardımcısı, denetçi yardımcısı, aktüer yardımcısı ve stajyer kontrolör istihdam edilebilir.

Bu madde kapsamında merkez teşkilatına ait kadro veya pozisyonlarda istihdam edilecekler hakkında, 657 sayılı Devlet Memurları Kanununun ek 41 inci maddesinin ikinci, üçüncü ve dördüncü fıkraları ile yabancı dil şartı hariç olmak üzere beşinci fıkrasında yer alan hükümler kıyasen uygulanır.

Bu madde kapsamında taşra teşkilatına ait kadro veya pozisyonlarda istihdam edilecekler hakkında, 657 sayılı Devlet Memurları Kanununun ek 41 inci maddesinin ikinci, üçüncü ve dördüncü fıkraları ile yabancı dil ve tez şartı hariç olmak ve yeterlik sınavı yazılı ve sözlü aşamalardan oluşmak üzere beşinci fıkrasında yer alan hükümler kıyasen uygulanır.

...

Bu madde kapsamında istihdam edilen yardımcı veya stajyerlerden verilen ilave süre içerisinde tezlerini sunmayan veya ikinci defa hazırladıkları tezleri de kabul edilmeyenler, ikinci sınavda da başarı gösteremeyen veya sınav hakkını kullanmayanlar, yardımcı veya stajyer unvanını kaybederler ve kurumlarında durumlarına uygun kadro veya pozisyonlara atanırlar.

..."

3. 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu'nun ek 41. maddesinin ikinci, üçüncü, dördüncü ve beşinci fıkraları şöyledir:

"Uzman yardımcılığına atanabilmek için; 48 inci maddede sayılan şartlara ek olarak, yapılacak yarışma sınavında başarılı olma ve (...) en az dört yıllık lisans eğitimi veren hukuk, siyasal bilgiler, iktisat, işletme, iktisadi ve idari bilimler fakültelerinden veya bu bakanlıklar ve kurumlarca yürütülen kurumsal hizmet gerekleri çerçevesinde en az dört yıllık lisans eğitimi veren ve yönetmelikle belirlenen yükseköğretim kurumlarından ya da bunlara denkliği Yükseköğretim Kurulu tarafından kabul edilen yurtiçindeki veya yurtdışındaki öğretim kurumlarından mezun olma şartı aranır.

Uzman yardımcıları mesleğe özel yarışma sınavı ile alınır. Uzman yardımcılığı giriş sınavı merkezi sınav sonuçlarına göre; yazılı ve sözlü sınav veya yalnızca sözlü sınavdan oluşur. Öğrenim dalları itibarıyla belirlenecek uzman yardımcılığı kadrolarına giriş sınavı için, eleme sınavı sonucunda aranacak puan türleri, taban puanları ve sınavda alınan başarı derecelerine göre çağrılacak aday sayısı tespit edilerek, giriş sınavı duyurusuyla ilan edilir. Ancak, giriş sınavına çağrılacak aday sayısı, atama yapılacak kadro sayısının yirmi katından, yalnızca sözlü sınav yapılması hâlinde sözlü sınava çağrılacak aday sayısı giriş sınavı duyurusunda belirtilen kadronun dört katından fazla olamaz. Yazılı sınav, kurumun görev alanına göre yönetmelikle belirlenen konulardan yapılır. Yazılı sınav sonucunda yetmiş puandan az olmamak üzere, en yüksek puandan başlanarak giriş sınavı duyurusunda belirtilen kadronun dört katına kadar aday sözlü sınava çağrılır. Sözlü sınav, adayların;

- a) Sınav konularına ilişkin bilgi düzeyi,
- b) Bir konuyu kavrayıp özetleme, ifade yeteneği ve muhakeme gücü,
- c) Liyakati, temsil kabiliyeti, davranış ve tepkilerinin mesleğe uygunluğu,
- d) Özgüveni, ikna kabiliyeti ve inandırıcılığı,
- e) Genel yetenek ve genel kültürü,
- f) Bilimsel ve teknolojik gelişmelere açıklığı,

yönlerinden değerlendirilerek, ayrı ayrı puan verilmek suretiyle gerçekleştirilir.

Adaylar, komisyon tarafından üçüncü fıkranın (a) bendi için elli puan, (b) ile (f) bentlerinde yazılı özelliklerin her biri için onar puan üzerinden değerlendirilir ve verilen puanlar ayrı ayrı tutanağa geçirilir. Bunun dışında sözlü sınav ile ilgili herhangi bir kayıt sistemi kullanılmaz. Sınav komisyonu, kurum içinden veya dışından yönetmelikle belirlenen kişilerden oluşur. Sözlü sınavda başarılı sayılmak için, komisyon başkan ve üyelerinin yüz tam puan üzerinden verdikleri puanların aritmetik ortalamasının en az yetmiş olması şarttır. Başarı puanı en yüksek olan adaydan başlanmak suretiyle giriş sınavı duyurusunda belirtilen uzman yardımcısı kadro sayısı kadar asıl adayın isimleri ilan edilir. Yapılan sınavlarda başarılı olmak şartıyla, giriş sınavı duyurusunda belirtilen uzman yardımcısı kadro sayısının yarısını geçmemek üzere komisyon tarafından belirlenen sayıda yedek adayın isimlerini kapsayan bir liste belirlenerek ilan edilir.

Uzman yardımcılığına atananlar, en az üç yıl çalışmak ve istihdam edildikleri birimlerce belirlenecek konularda hazırlayacakları uzmanlık tezi, oluşturulacak tez jürisi tarafından kabul edilmek kaydıyla, yapılacak yeterlik sınavına girmeye hak kazanırlar. Süresi içinde tezlerini sunmayan veya tezleri kabul edilmeyenlere tezlerini sunmaları veya yeni bir tez hazırlamaları için altı ayı aşmamak üzere ilave süre verilir. Yeterlik sınavında başarılı olanların uzman kadrolarına atanabilmeleri, Kamu Personeli Yabancı Dil Bilgisi Seviye Tespit Sınavından asgari (C), Dışişleri Uzmanlığı için asgari (B) düzeyinde veya dil yeterliği bakımından bunlara denkliği kabul edilen ve uluslararası geçerliliği bulunan başka bir belgeye yeterlik sınavından itibaren en geç iki yıl içinde sahip olma şartına bağlıdır. Sınavda başarılı olamayanlar veya sınava girmeye hak kazandığı hâlde geçerli mazereti olmaksızın sınav hakkını kullanmayanlara, bir yıl içinde ikinci kez sınav hakkı verilir. Verilen ilave süre içinde tezlerini sunmayan veya ikinci defa hazırladıkları tezleri de kabul edilmeyenler, ikinci sınavda da başarı gösteremeyen veya sınav hakkını kullanmayanlar ile süresi içinde yabancı dil yeterliliği şartını yerine getirmeyenler, uzman yardımcısı unvanını kaybederler ve kurumlarında durumlarına uygun memur unvanlı kadrolara atanırlar.”

II. İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Zühtü ARSLAN, Engin YILDIRIM, Hasan Tahsin GÖKCAN, Serdar ÖZGÜLDÜR, Recep KÖMÜRCÜ, Burhan ÜSTÜN, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Kadir ÖZKAYA, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĞLU ve Selahaddin MENTEŞ'in katılımlarıyla 16/10/2019 tarihinde yapılan ilk inceleme toplantısında dosyada eksiklik bulunmadığından işin

esasının incelenmesine, yürürlüğü durdurma talebinin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

III. ESASIN İNCELENMESİ

2. Dava dilekçesi ve ekleri, Raportör Fatma KARAMAN ODABAŞI tarafından hazırlanan işin esasına ilişkin rapor, dava konusu CBK kuralları ve ilgili görülen mevzuat, dayanan ve ilgili görülen Anayasa kuralları ile bunların gerekçeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A. Cumhurbaşkanlığı Kararnamelerinin Anayasal Çerçevesi ve Yargısal Denetimi

3. 21/1/2017 tarihli ve 6771 sayılı Türkiye Cumhuriyeti Anayasasında Değişiklik Yapılmasına Dair Kanun ile Anayasa'nın bazı maddelerinde değişiklik yapılmıştır. Yapılan değişikliklerle yeni bir hükümet sistemine geçilmiş ve buna bağlı olarak Cumhurbaşkanı'nın görev ve yetkileri yeniden düzenlenmiştir. Anayasa'nın 8. maddesinde, yürütme yetkisi ve görevinin Cumhurbaşkanı ve Bakanlar Kuruluna ait olduğu ifade edilmekte iken maddede yapılan değişiklikle Bakanlar Kurulu kaldırılarak yürütme yetkisi ve görevi tek başına Cumhurbaşkanı'na verilmiştir. Anayasa'da Bakanlar Kuruluna verilen görev ve yetkilere ilişkin maddelerde de aynı doğrultuda değişiklik yapılarak daha önce Bakanlar Kuruluna ait olan görev ve yetkilerin Cumhurbaşkanı tarafından yerine getirilmesi öngörülmüştür.

4. Yeni hükümet sisteminin en önemli özelliklerinden biri Cumhurbaşkanı'na "Cumhurbaşkanlığı Kararnamesi" adı altında düzenleme yapma yetkisinin tanınmasıdır. CBK'ların en belirgin özelliği ise Cumhurbaşkanı'na belirli konularda ilk elden düzenleme yapma yetkisinin verilmiş olmasıdır. Yürütmenin diğer düzenleyici işlemlerinden farklı olarak Cumhurbaşkanı Anayasa'da belirlenen yetki çerçevesinde herhangi bir kanuna dayanmadan ya da yasama organının onayı olmadan CBK'lar yoluyla düzenleme yapabilecektir.

5. Anayasa'nın 104. maddesinin on yedinci fıkrasının birinci cümlesinde Cumhurbaşkanı'nın yürütme yetkisine ilişkin konularda CBK çıkarabileceği hüküm altına alınmıştır. Düzenlemeyle yürütme yetkisine ilişkin olmak kaydıyla CBK çıkarma konusunda Cumhurbaşkanı'na genel bir yetki verilmiştir. Maddenin gerekçesinde, yeni hükümet sistemi gözetilerek Cumhurbaşkanı'nın genel siyasetin yürütülmesinde yürütme yetkisi ile ilgili olarak ihtiyaç duyduğu konularda CBK çıkarabilmesine imkân tanımak amacıyla ilk elden düzenleme yapma yetkisinin tanındığı ifade edilmiştir.

6. Cumhurbaşkanı'na yürütme yetkisine ilişkin konularda CBK çıkarma yetkisinin genel olarak verilmesinin yanı sıra Anayasa'nın diğer bazı maddelerinde belirtilen kimi konuların CBK ile

düzenleneceği ayrıca ifade edilmiştir. Bu kapsamda Anayasa'nın 104. maddesinin dokuzuncu fıkrasında üst kademe kamu yöneticilerinin atanmalarına ilişkin usul ve esasların; 106. maddesinin on birinci fıkrasında bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulmasının; 108. maddesinin dördüncü fıkrasında Devlet Denetleme Kurulunun işleyişi, üyelerinin görev süresi ve diğer özlük işlerinin; 118. maddesinin altıncı fıkrasında Millî Güvenlik Kurulu Genel Sekreterliğinin teşkilatı ve görevlerinin CBK'larla düzenleneceği hüküm altına alınmıştır. Anayasa'nın 123. maddesinin üçüncü fıkrasında ise kamu tüzel kişiliğinin kanunla veya CBK ile kurulacağı belirtilmiştir.

7. Anayasa'nın 148. maddesinde CBK'ların şekil ve esas bakımdan Anayasa'ya uygunluğunun denetlenmesi öngörülmüş, yargısal denetim görev ve yetkisi de Anayasa Mahkemesine verilmiştir.

8. Anayasa'da Cumhurbaşkanı'na CBK çıkarma yetkisi verilmekle birlikte bu yetki sınırsız değildir. Kanunlardan farklı olarak Anayasa'da CBK'yla düzenlenecek konular sınırlandırılmıştır. Konu bakımından yetki yönünden getirilen bu sınırlamalar Anayasa'nın 104. maddesinin on yedinci fıkrasının ilk dört cümlesinde düzenlenmiştir.

9. Anılan fıkranın birinci cümlesinde Cumhurbaşkanı'nın yürütme yetkisine ilişkin konularda CBK çıkarabileceği ifade edilmiştir. Buna göre yürütme yetkisine ilişkin konular dışında CBK ile düzenleme yapılması mümkün değildir.

10. Fıkranın ikinci cümlesinde "Anayasa'nın ikinci kısmının birinci ve ikinci bölümlerinde yer alan temel haklar, kişi hakları ve ödevleriyle dördüncü bölümde yer alan siyasi haklar ve ödevlerin" CBK'yla düzenlenemeyeceği belirtilmiştir. Bu hüküm uyarınca belirtilen alanlarda CBK ile düzenleme yapılamaz.

11. Fıkranın üçüncü cümlesinde de Anayasa'da münhasıran kanunla düzenlenmesi öngörülen konularda CBK çıkarılmayacağı hüküm altına alınmıştır. Ancak Anayasa'da hangi konuların münhasıran kanunla düzenleneceğine ilişkin özel bir hüküm bulunmamaktadır. Bununla birlikte Anayasa Mahkemesinin yerleşik içtihadında anayasa koyucunun kanunla düzenlenmesini öngördüğü konuların bu kapsamda görülmesi gerektiği kabul edilmektedir (AYM, E.2016/150, K.2017/179, 28/12/2017, § 57; E.2016/180, K.2018/4, 18/1/2018, § 17; E.2017/51, K.2017/163, 29/11/2017, § 13; E.2016/139, K.2016/188, 14/12/2016, § 9; E.2013/47, K.2013/72, 6/6/2013). Buna göre Anayasa'da kanunla düzenleneceği belirtilen alanlarda Cumhurbaşkanı'nın CBK çıkarma yetkisi bulunmamaktadır.

12. Fıkranın dördüncü cümlesinde ise kanunda açıkça düzenlenen konularda CBK çıkarılamayacağı ifade edilmiştir. Anılan hükme göre Cumhurbaşkanı'nın yürütme yetkisine ilişkin konularda CBK çıkarılması için CBK'yla düzenlenecek konunun kanunlarda açıkça düzenlenmemiş olması gerekir.

13. CBK'ların yukarıda belirtilen konu bakımından yetki kurallarına uygun olarak çıkarılması gerekmektedir. Aksi takdirde içeriği Anayasa'ya aykırılık oluşturmasa bile bu düzenlemelerin Anayasa'ya uygunluğundan söz edilemez. Dolayısıyla CBK'ların yargısal denetiminde öncelikle Anayasa'nın 104. maddesinin on yedinci fıkrasında belirtilen konu bakımından yetki kurallarına uygunluğunun ele alınması gerekir. Anılan fıkra yönünden herhangi bir aykırılık tespit edilmemesi durumunda ise bu defa CBK'ların içerik yönünden Anayasa'ya uygunluk denetimi yapılmalıdır.

B. CBK'nın 1. Maddesiyle (1) Numaralı CBK'nın 217. Maddesinin (1) Numaralı Fıkrasının (ğ) Bendine [17/4/2020 Tarihli ve (60) Numaralı CBK'nın 1. Maddesiyle 217. Maddede Yapılan Değişiklikten Sonra (h) Bendi] Eklenen "...ve Hazinesinin Cumhurbaşkanı kararı ile yurtiçindeki ya da yurtdışındaki şirketlere iştirak etmesini sağlamak," İbaresinin İncelenmesi

1. Genel Açıklama

14. Anayasa'nın 47. maddesinin birinci fıkrasında kamu hizmeti niteliği taşıyan özel teşebbüslerin, kamu yararının zorunlu kıldığı hâllerde devletleştirilebileceği düzenlenmiş; ikinci fıkrasında ise devletleştirmenin gerçek karşılığı üzerinden yapılacağı, gerçek karşılığın hesaplanma tarzı ve usullerinin kanunla düzenleneceği belirtilmiştir.

15. Bu kapsamda kamu yararının zorunlu kıldığı hâllerde, kamu hizmeti niteliği taşıyan özel teşebbüslerin devletleştirilmesi esasları, devletleştirme karşılığının hesaplanma tarz ve usulleri ve bunlarla ilgili uyuşmazlıkların çözüm yolları 20/11/1984 tarihli ve 3082 sayılı Kamu Yararının Zorunlu Kıldığı Hallerde, Kamu Hizmeti Niteliği Taşıyan Özel Teşebbüslerin Devletleştirilebilmesi Usul ve Esasları Hakkında Kanun'da düzenlenmiştir.

16. Anılan Kanun'un 2. maddesinde devletleştirmenin şartları düzenlenerek özel teşebbüsün yaptığı hizmet veya üretimin ülke çapında kamu ihtiyacına hitap etmesi; kontrol, rekabet, ikame veya başka yollardan sağlama imkânının bulunmaması ve yavaşlatılması veya durdurulması durumunda kamunun büyük zarar görmesi şartlarının birlikte gerçekleşmesi hâlinde özel teşebbüsün devletleştirilmesinin mümkün olabileceği ifade edilmiştir. Buna göre her türlü özel teşebbüsün devletleştirilmesi mümkün olmayıp devletleştirmenin özel teşebbüsün yaptığı hizmet ve üretimin bir kısım özellik ve nitelikleri ile doğrudan bağlantılı bulunduğu anlaşılmaktadır.

17. Kanun'un 3. maddesinde özel teşebbüsün gördüğü kamu hizmetinin niteliğine göre kamu hizmeti niteliği taşıyan özel teşebbüslerin kamu yararının zorunlu kıldığı hâllerde devletleştirilmesinin kanunla düzenleneceği belirtilmiştir.

18. Kamusal bir müdahale niteliği taşıyan devletleştirme, tek taraflı olarak ve kamu gücü kullanılarak gerçek karşılığı ödenmek suretiyle özel teşebbüsün kamuya geçirilmesi şeklinde gerçekleştirilmektedir. Devletleştirmeye hak sahipleri veya özel teşebbüsü temsil eden organların rızası ve iradesinden bağımsız olarak teşebbüs üzerindeki tasarruf yetkileri sonlandırılmaktadır.

2. Anlam ve Kapsam

19. (1) numaralı CBK'nın 217. maddesinde Hazine ve Maliye Bakanlığının (Bakanlık) görev ve yetkileri düzenlenmiştir. Maddenin (1) numaralı fıkrasının (h) bendinde; Hazine işlemleri, kamu finansmanı, kamu sermayeli kuruluş ve işletmeler ve devlet iştirakleri, ikili ve çok taraflı dış ekonomik ilişkiler, uluslararası ve bölgesel ekonomik ve mali kuruluşlarla ilişkiler, yabancı ülke ve kuruluşlardan borç ve hibe alınması ve verilmesi ile ilgili işlemleri yapmak ve Hazinesin Cumhurbaşkanlığı kararı ile yurt içindeki ya da yurt dışındaki şirketlere iştirak etmesini sağlamak, Bakanlığın görevleri arasında sayılmıştır. Dava konusu kural bentte yer alan "...ve Hazinesin Cumhurbaşkanlığı kararı ile yurtiçindeki ya da yurtdışındaki şirketlere iştirak etmesini sağlamak," ibaresidir.

20. Kuralda geçen iştirak kavramı ortaklık, ortak olma, paydaşlık, katılma, katılım anlamlarına gelmektedir.

21. Anılan CBK'nın 224. maddesinde Bakanlığın hizmet birimlerinden olan Kamu Sermayeli Kuruluş ve İşletmeler Genel Müdürlüğü'nün görev ve yetkileri düzenlenmektedir. Maddenin (1) numaralı fıkrasının (a) bendinde kamu iktisadi teşebbüsleri ile ilgili olarak Hazine pay sahipliğinin gerektirdiği her türlü işlemi yapmak Genel Müdürlüğü'nün görev ve yetkileri arasında sayılmakta iken dava konusu ibarenin eklenmesiyle anılan bendin de Kamu İktisadi Teşebbüsleri (KİT) ve Hazinesin iştirak ettiği şirketler ile ilgili olarak Hazine pay sahipliğinin gerektirdiği her türlü işlemi yapmak şeklinde değiştirildiği görülmektedir. Buna göre Hazinesin yurt içindeki ve yurt dışındaki şirketlere iştirakinin şirkette pay sahipliği şeklinde olacağı anlaşılmaktadır.

22. 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 39. maddesinin (4) numaralı fıkrasında "İptal davalarında Mahkemece esasın incelenmesine karar verilmesi hâlinde, dava dilekçesi ile ekleri Türkiye Büyük Millet Meclisi Başkanlığı, Cumhurbaşkanlığı ile iptal davası açmaya yetkili siyasi parti gruplarına gönderilir. Bu

makamlar, iptal davasıyla ilgili yazılı görüşlerini değerlendirilmek üzere Mahkemeye bildirebilirler.” denilmektedir. CBK’lar gerekçeleri olmaksızın yayımlanmaktadırlar. Bu nedenle CBK kurallarının getiriliş amacının tespiti bakımından 6216 sayılı Kanun’un anılan hükmüne istinaden Cumhurbaşkanlığınca dosyaya sunulan görüş yazıları önem arz etmektedir.

23. Cumhurbaşkanlığından gelen ve dava konusu kuralın düzenlenme sebebinin açıklandığı görüş yazısında özetle, 8/6/1984 tarihli ve 233 sayılı Kamu İktisadi Teşebbüsleri Hakkında KHK’nın 27. maddesinde teşebbüs veya bağlı ortaklığın bir anonim şirkete iştirakinin düzenlendiği, kuralla teşebbüs veya bağlı ortaklıkların aracılığı olmadan da iştirak edilecek şirketlerde Hazinenin dolaylı pay sahipliği yerine doğrudan pay sahipliğine de imkân sağlanmasının amaçlandığı ifade edilmiştir.

24. 233 sayılı KHK’nın 2. maddesinde iştirakin, iktisadi devlet teşekküllerinin, kamu iktisadi kuruluşlarının veya bağlı ortaklıklarının, sermayelerinin en az yüzde on beşine, en çok yüzde ellisine sahip buldukları anonim şirketler oldukları açıklanmıştır. KHK’nın 27. maddesinde iştiraklerin teşkili ve nitelikleri düzenlenmiş; 28. maddesinde ise iştiraklerin yönetimine ilişkin esaslara yer verilerek teşebbüs veya bağlı ortaklıkların iştirak ettikleri anonim şirketlerde 13/1/2011 tarihli ve 6102 sayılı Türk Ticaret Kanunu gereğince ortakların haiz oldukları bütün haklara sahip buldukları belirtilmiştir.

25. Dava konusu kuralla Bakanlığa verilen görev ve yetkinin kapsamı genel itibarıyla şirketlere iştirak edilmesini sağlamak olarak ifade edilmiş, şirket türlerine göre herhangi bir sınırlama yapılmamıştır. 6102 sayılı Kanun’da şirket kavramı ticaret şirketlerini ifade edecek şekilde kullanılmakta olup Kanun’un 124. maddesinde ticaret şirketlerinin kollektif, komandit, anonim, limited ve kooperatif şirketlerinden ibaret olduğu belirtilmiş; kollektif ve komandit şirketlerin şahıs, anonim, limited ve sermayesi paylara bölünmüş komandit şirketlerin ise sermaye şirketleri sayıldıkları ifade edilmiştir.

26. 6102 sayılı Kanun’un 211. maddesinde kollektif şirket, ticari bir işletmeyi bir ticaret unvanı altında işletmek amacıyla gerçek kişiler arasında kurulan ve ortaklarından hiçbirinin sorumluluğu şirket alacaklılarına karşı sınırlandırılmamış olan şirket olarak tanımlanmış; 304. maddesinde ise komandit şirket, ticari bir işletmeyi bir ticaret unvanı altında işletmek amacıyla kurulan şirket alacaklılarına karşı ortaklardan bir veya birkaçının sorumluluğu sınırlandırılmamış ve diğer ortak veya ortakların sorumluluğu belirli bir sermaye ile sınırlandırılmış olan şirket olarak ifade edilmiştir. Maddede ayrıca sorumluluğu sınırlı olmayan ve ancak gerçek kişi olabilecek olan ortaklara komandite, sorumluluğu sınırlı olan ve gerçek kişi veya tüzel kişi olabilecek olan ortaklara ise komanditer ortak denileceği belirtilmiştir. Kanun’un 564. maddesinde sermayesi paylara bölünmüş komandit şirketin, sermayesi paylara bölünen ve ortaklardan bir veya birkaçı şirket alacaklılarına karşı bir kollektif şirket ortağı

gibi sınırsız, diğerleri bir anonim şirket pay sahibi gibi sınırlı sorumlu olan şirket olduğu ifade edilmiştir. Buna göre kollektif şirket ortakları ve komandit şirket ile sermayesi paylara bölünmüş komandit şirketteki komandite ortakların ancak gerçek kişiler olabilecekleri anlaşılmaktadır.

27. Öte yandan 6102 sayılı Kanun'un 329. maddesinde anonim şirket, sermayesi belirli ve paylara bölünmüş olan, borçlarından dolayı yalnız mal varlığıyla sorumlu bulunan şirket olarak tanımlanmış; pay sahiplerinin yalnızca taahhüt etmiş oldukları sermaye payları ile şirkete karşı sorumlu oldukları ifade edilmiştir. Kanun'un 573. maddesinde ise limited şirket, bir veya daha çok gerçek veya tüzel kişi tarafından bir ticaret unvanı altında kurulan, esas sermayesi belirli olup esas sermaye paylarının toplamından oluşan, ortaklarının şirket borçlarından sorumlu olmayıp sadece taahhüt ettikleri esas sermaye paylarını ödemekle ve şirket sözleşmesinde öngörülen ek ödeme ve yan edim yükümlülüklerini yerine getirmekle yükümlü oldukları şirket türü olarak tanımlanmıştır. Bu kapsamda anonim şirket ve limited şirket ortaklarının gerçek veya tüzel kişi olabilmeleri mümkün bulunmaktadır.

28. 6102 sayılı Kanun'un "Kavramlar" başlıklı 135. maddesinde ticaret şirketlerinin birleşmelerine, bölünmelerine ve tür değiştirmelerine uygulanacak maddeler bakımından "ortak" ibaresinin yalnızca anonim şirketler yönünden pay sahiplerini, limited şirketler ve şahıs şirketleri ile kooperatifler yönünden ortakları; "ortaklık payı" ibaresinin ise şahıs şirketlerindeki ortaklık payını, anonim şirketteki payı, limited şirketteki esas sermaye payını, sermayesi paylara bölünmüş komandit şirketteki ortaklık payını ifade ettiği belirtilmiştir. Buna göre terminolojik olarak ilk bakışta yalnızca anonim şirketlerde ortaklık payının pay, ortağın da pay sahibi olarak ifade edildiği; diğer şirketlerde ise ortak, ortaklık payı ve esas sermaye payı kavramlarının kullanıldığı söylenebilir ise de Kanun'un komandit şirketlere, sermayesi paylara bölünmüş komandit şirketlere ve limited şirketlere ilişkin çeşitli hükümlerinde pay ibaresine de yer verildiği açıktır.

29. Anılan hususlar birlikte değerlendirildiğinde kural kapsamında Hazinesinin iştirak edeceği şirketlerin anonim şirketlerle sınırlandırılmadığı, kollektif şirket ortağı ve komandit şirket ile sermayesi paylara bölünmüş komandit şirketteki komandite ortak dışında 6102 sayılı Kanun'da belirtilen şirket türlerine iştirakin mümkün olabileceği anlaşılmaktadır. Öte yandan 233 sayılı KHK'da iktisadi devlet teşekküllerinin, kamu iktisadi kuruluşlarının veya bağlı ortaklıklarının iştirakteki pay sahipliğinin şirket sermayesinin %15 ile %50'si arasında olacağı özel olarak açıklanmış ise de dava konusu kuralda Hazinesinin şirket sermayesine katılım payına ilişkin bir sınırlamaya yer verilmemiştir.

30. Kural; Bakanlıđı, Hazinesinin Cumhurbaşkanlıđı kararı ile yurt dışındaki şirketlere de iştirak etmesini sağlamak hususunda görevli ve yetkili kılmaktadır. Buna göre yurt dışındaki şirketlerin de yerleşik oldukları ülke hukuklarına uygun olarak ticari mevzuata uyumlu şekilde kurulmuş, ticari anlamda iştirak edilmesi ve iştirak suretiyle pay sahibi olunması mümkün kuruluşlar olacaktır.

3. İptal Talebinin Gerekçesi

31. Dava dilekçesinde özetle; Anayasa'nın 47. maddesinde devletleştirmeye ilişkin ilkelere yer verilerek konunun 3082 sayılı Kanun'la düzenlendiđi, bu nedenle Hazinesinin özel şirketlere iştirak etmesine imkân tanıyan kuralın kanunda açıkça düzenlenen konulara ilişkin olduđu, özel mülkiyete konu şirket paylarının kamuya geçirilmesinin mülkiyet hakkına müdahale niteliğinde bulunduđu, Anayasa'nın 35. maddesi uyarınca özel mülkiyetin ancak kanunla sınırlanabileceđi, mülkiyet hakkına ilişkin hususların CBK ile düzenlenemeyeceđi, yasamanın yetkisindeki konularda CBK ile düzenleme yapılamayacağı, kuralla herhangi bir sınır ve koşul öngörülmezsizin Cumhurbaşkanlıđı kararı ile uygun görülecek yurt içindeki ve yurt dışındaki özel mülkiyete konu herhangi bir şirketin ortaklık paylarının devralınması yoluyla devletleştirilmesine imkân tanınmasının Anayasa'nın 47. maddesine aykırı olduđu, 3082 sayılı Kanun'un 3. maddesinde devletleştirmenin kanunla düzenlenmesi gerektiğinin belirtilmiş olmasına rağmen kuralın Cumhurbaşkanı kararı ile devletleştirmeyi mümkün kıldıđı, devletin temel amaç ve görevleriyle bağdaşmayan ve şirketlere iştirak edilmesine ilişkin temel ilkelere yer vermeyen kuralda belirlilik ve öngörülebilirlik bulunmadığı belirtilerek kuralın Anayasa'nın 2., 5., 8., 35., 47. ve 104. maddelerine aykırı olduđu ileri sürülmüştür.

4. Anayasa'ya Aykırılık Sorunu

a. Kuralın Konu Bakımından Yetki Yönünden İncelenmesi

32. Dava dilekçesinde konu bakımından yetki yönünden kuralın Anayasa'nın 2., 5., 8., 35. ve 47. maddelerine de aykırı olduđu ileri sürülmüş ise de CBK'ya ilişkin konu bakımından yetki kuralları Anayasa'nın 104. maddesinin on yedinci fıkrasında düzenlendiğinden bu husustaki inceleme anılan fıkra kapsamında yapılacaktır.

33. Yürütme organının kararı ile Hazinesinin şirketlere iştirakinin iktisadi alanda bir faaliyetin gerçekleştirilmesi niteliğinde olduđu açık olup yürütmenin bir unsuru olan Bakanlıđı bu faaliyetin yürütülmesiyle bağlantılı olarak görevli ve yetkili kılan kuralın yürütme yetkisine ilişkin bir konuyu düzenlemediđi söylenemez.

34. Kural, Anayasa'nın CBK ile düzenlenmesi yasaklanan "İkinci Kısım" "Birinci Bölüm" ve "İkinci Bölüm"ünde yer alan temel haklar, kişi hakları ve ödevleriyle "Dördüncü Bölüm"ünde yer alan siyasi haklar ve ödevler ile ilgili herhangi bir düzenleme içermemektedir.

35. Anayasa'nın 104. maddesinin on yedinci fıkrasının üçüncü cümlesi uyarınca CBK'lar bakımından aranan bir diğer husus, CBK kuralının Anayasa'da münhasıran kanunla düzenlenmesi gereken konulara ilişkin olmaması gereğidir. Anayasa koyucunun bir konunun kanunla düzenlenmesini özel olarak öngörmesi bu alanın münhasıran kanunla düzenlenmesini istediği anlamına gelir. Bu kapsamda Anayasa bir konunun kanunla düzenleneceğini öngörmüşse bu konuda CBK çıkarılamaz. Bununla birlikte Anayasa'da CBK'larla düzenleneceği özel olarak öngörülen konulara ilişkin Anayasa hükümlerinin açıkça izin verdiği hususlarda CBK'larla düzenleme yapılabilir.

36. Anayasa'nın 123. maddesinin birinci fıkrasında idarenin kuruluş ve görevleriyle bir bütün olduğu ve kanunla düzenleneceği belirtilmiş; 106. maddesinin on birinci fıkrasında ise bakanlıkların kurulmasının, kaldırılmasının, görev ve yetkilerinin, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulmasının CBK ile düzenleneceği hükme bağlanmıştır. Dolayısıyla anılan fıkra kapsamındaki konular Anayasa'nın CBK ile düzenlenmesini ayrıca ve özel olarak öngördüğü konulardır. Bu kapsamda Bakanlığın görev ve yetkilerinden birini düzenleyen kural, Anayasa'nın 106. maddesinin on birinci fıkrasında CBK ile düzenlenmesi özel olarak öngörülen konulardan biri olan bakanlıkların görev ve yetkilerine ilişkin bulunmaktadır.

37. Öte yandan Anayasa'nın 47. maddesinin birinci ve ikinci fıkralarında devletleştirme düzenlenmiş bu bağlamda 3082 sayılı Kanun kapsamında yer alan özel teşebbüslerin devletleştirilmesi esas ve usullerine ilişkin çeşitli hükümlere Genel Açıklama bölümünde yer verilmiştir (bkz. §§ 14-18). Devletleştirme bir devlet müdahalesi iken iştirak özel hukuk hükümleri kapsamında, sözleşme ilişkisi çerçevesinde şirkete katılmayı ifade etmektedir. Buna göre kuralda belirtilen Hazinesinin yurt içindeki ve yurt dışındaki şirketlere iştirakine ilişkin faaliyetin devletleştirmeye ilişkin bir düzenleme niteliğinde olduğu söylenemez.

38. İştirakte, iştirak edilecek şirketin kamu hizmeti niteliği taşıması ve iştiraki kamu yararının zorunlu kılması şartları özel olarak aranmadığı gibi iştirakin şirket üzerinde tam bir hâkimiyet yaratacak şekilde tüm şirket paylarına sahip olunması şeklinde gerçekleştirilmesi zorunluluğu da bulunmamaktadır. İştirak, çoğu zaman ekonomik güç ve dengeler, piyasa gerekleri, finansman çeşitliliği gibi birtakım sebeplerle taraf iradelerine uygun olarak gerçekleştirilen sözleşme ilişkisi bağlamında şirkette pay sahibi olunması suretiyle şirkete katılımı ifade etmektedir.

39. Bu itibarla Anayasa'nın 106. maddesinin on birinci fıkrası uyarınca CBK ile düzenlenmesi mümkün olan, devletleştirme ile ilgili bulunmayan ve özel hukuk hükümleri kapsamında ekonomik ve iktisadi bir faaliyetin gerçekleştirilmesine ilişkin olduğu anlaşılan kural Anayasa'da münhasıran kanunla düzenlenmesi öngörülen konulardan değildir.

40. Anayasa'nın 104. maddesinin on yedinci fıkrasının dördüncü cümlesinde "Kanunda açıkça düzenlenen konularda Cumhurbaşkanlığı kararnamesi çıkarılamaz." denilmiştir. Buna göre CBK'ların anılan Anayasa hükmü yönünden yapılacak denetiminde öncelikle karşılaştırmaya esas olabilecek daha önce kabul edilmiş bir kanun hükmünün bulunup bulunmadığının tespit edilmesi gerekir. Sonrasında ise -böyle bir kanun hükmü varsa- incelenen CBK kuralının kanunun açıkça düzenlediği konuya ilişkin olup olmadığı belirlenmelidir. Bu değerlendirme yapılırken önce ilgili kanunun CBK ile düzenlenen alanda hüküm ifade edip etmediğinin belirlenmesi, ardından da kanundaki düzenlemenin açık olup olmadığının tespit edilmesi gerekir.

41. Ekonomi politikalarının tespitine yardımcı olmak ve bu politikalar çerçevesinde hazine işlemleri, kamu finansmanı, kamu iktisadi teşebbüsleri ve devlet iştirakleri gibi çeşitli konularda düzenleme ve işlem yapmak amacıyla Hazine Müsteşarlığının kurulmasına, teşkilat, görev ve yetkilerine ilişkin esasları düzenleyen 9/12/1994 tarihli ve 4059 sayılı Hazine Müsteşarlığının Teşkilat ve Görevleri Hakkında Kanun'un başlığı 2/7/2018 tarihli ve 703 sayılı Anayasada Yapılan Değişikliklere Uyum Sağlanması Amacıyla Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında KHK'nın 16. maddesiyle "Finansal İstikrar İle Bazı Düzenlemeler Hakkında Kanun" olarak değiştirilmiş; müsteşarlığın ve ana hizmet birimlerinin görev ve yetkilerini düzenleyen hükümler yürürlükten kaldırılmıştır. Benzer şekilde 13/12/1983 tarihli ve 178 sayılı Maliye Bakanlığının Teşkilat ve Görevleri Hakkında KHK, 703 sayılı KHK'nın 13. maddesiyle yürürlükten kaldırılmıştır. Bunların dışında Bakanlığın görev ve yetkilerine ilişkin olarak kuralın kapsamına giren konuda kanunla yapılan herhangi bir düzenlemeye rastlanmamıştır.

42. Öte yandan iktisadi devlet teşekküllerinin, kamu iktisadi kuruluşlarının veya bağlı ortaklıkların anonim şirketlere iştiraki hususunda 233 sayılı KHK kapsamındaki düzenlemelere Anlam ve Kapsam bölümünde yer verilmiş olup (bkz. § 24) kural, 233 sayılı KHK kapsamında kalan bir konuya da ilişkin bulunmamaktadır.

43. Buna göre Hazinesinin Cumhurbaşkanı kararı ile yurt içindeki ve yurt dışındaki şirketlere iştirak etmesini sağlamaya yönelik Bakanlığa ilk kez görev ve yetki veren kuralın kanunda açıkça düzenlenen konulara ilişkin olmadığı anlaşılmaktadır.

44. Açıklanan nedenlerle kural, Anayasa'nın 104. maddesinin on yedinci fıkrasına aykırı değildir. İptal talebinin reddi gerekir.

b. Kuralın İçerik Yönünden İncelenmesi

45. Anayasa'nın 2. maddesinde belirtilen hukuk devleti; eylem ve işlemleri hukuka uygun, insan haklarına saygılı, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adil bir hukuk düzeni kurup bunu geliştirerek sürdüren, hukuki güvenliği sağlayan, Anayasa'ya aykırı durum ve tutumlardan kaçınan, hukuk kurallarıyla kendini bağlı sayan ve yargı denetimine açık olan devlettir.

46. Hukuk devletinin temel unsurlarından biri belirlilik ilkesidir. Anayasa Mahkemesinin yerleşik kararlarına göre anılan ilke, yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olmasını gerektirmektedir. Belirlilik ilkesi hukuksal güvenlikle bağlantılı olup bireyin kanundan belirli bir kesinlik içinde hangi somut eylem ve olguya hangi hukuksal yaptırımın veya sonucun bağlandığını, bunların idareye hangi müdahale yetkisini verdiğini bilmesini zorunlu kılmaktadır.

47. Anayasa Mahkemesi birçok kararında belirlilik ilkesinin yalnızca yasal belirliliği değil daha geniş anlamda hukuki belirliliği ifade ettiğini, yasal düzenlemeye dayanarak erişilebilir, bilinebilir ve öngörülebilir olma gibi niteliklere ilişkin gereklilikleri karşılama koşuluyla mahkeme içtihatları ve yürütmenin düzenleyici işlemleri ile de hukuki belirliliğin sağlanabileceğini, asıl olanın muhtemel muhataplarının mevcut şartlar altında belirli bir işlemin ne tür sonuçlar doğurabileceğini öngörmelerini mümkün kılacak bir normun varlığı olduğunu vurgulamıştır. Anılan ilkenin yürütmenin asli düzenleyici işlemi niteliğinde olan CBK'lar bakımından da geçerli olduğunda şüphe bulunmamaktadır.

48. Kuralın anlam ve kapsam bölümünde de ifade edildiği üzere özel hukuk hükümleri bağlamında şirkete iştirak, ortaklık şeklinde şirketlerde pay sahibi olunması suretiyle gerçekleşmektedir. Kural kapsamında Hazinesin şirketlere iştiraki 233 sayılı KHK'daki düzenlemelerden farklılık arz etmekte olup iştirak anonim şirketlerle sınırlandırılmadığı gibi pay sahipliğinin oranına ilişkin de herhangi bir sınırlama bulunmamaktadır. Yurt dışında Hazinesin iştirak edebileceği şirketlerin ise yerleşik oldukları ülke hukuklarına uygun, ticari mevzuatla uyumlu şekilde kurulmuş şirket statüsündeki kuruluşlar olacakları, iştirakin yine ticari mevzuata uyumlu şekilde, şirkette pay sahibi olunması suretiyle gerçekleşeceği belirtilmiştir (bkz. §§ 19-30).

49. Hazinesin şirketlere iştiraki özel hukuk hükümlerine uygun olarak gerçekleştirilecek olup tarafların hak ve yükümlülükleri ile sorumlulukları başta olmak üzere iştirakin kapsam ve

mahiyetine ilişkin meselelerin kural olarak genel kanun niteliğindeki 6102 sayılı Kanun'a, mahiyetine uygun düştüğü ölçüde 6/12/2012 tarihli ve 6362 sayılı Sermaye Piyasası Kanunu, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu gibi özel kanunlardaki düzenlemelere, yabancılik unsuru taşıyan iştirak ilişkilerinde ise milletlerarası özel hukuk kuralları çerçevesinde ilgili ülke mevzuatlarına tabi olacağı açıktır.

50. Öte yandan kuralda Hazinesin şirketlere iştirak etmesi suretiyle gerçekleştirilecek iktisadi faaliyet kapsamında alınacak karar ve gerçekleştirilecek işlemlerin yürütme organının hangi unsurlarınca gerçekleştirileceği de açık, anlaşılır ve uygulanabilir bir şekilde belirtilmiş olup kuralda bu yönden de belirsizlik bulunmamaktadır.

51. Açıklanan nedenlerle kural Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ ve Yusuf Şevki HAKYEMEZ bu görüşe katılmamışlardır.

C. CBK'nın 14. Maddesiyle (1) Numaralı CBK'ya Eklenen 227/B Maddesinin (4) Numaralı Fıkrasının "...hazine ve maliye başmüfettişleri, müfettişleri ve müfettiş yardımcılarının görev, yetki ve sorumlulukları ile..." Bölümünün İncelenmesi

1. Genel Açıklama

52. (1) numaralı CBK'nın 227/B maddesinde Hazine ve Maliye Bakanlığının hizmet birimlerinden olan Teftiş Başkanlığı (Başkanlık) düzenlenmiştir. Maddenin (1) numaralı fıkrasında Teftiş Başkanlığının başkan, başkan yardımcısı ile hazine ve maliye müfettişlerinden (hazine ve maliye başmüfettişi, hazine ve maliye müfettişi, hazine ve maliye müfettiş yardımcısı) oluştuğu belirtilmiştir. Maddenin (2) numaralı fıkrasında ise Başkanlıkta 375 sayılı KHK'nın ek 24. maddesi uyarınca hazine ve maliye müfettişi ile hazine ve maliye müfettiş yardımcısı istihdam edilebileceği ifade edilmiştir.

53. 375 sayılı KHK'nın "Müfettiş, denetmen, denetçi, kontrolör, aktüer istihdamı" başlıklı ek 24. maddesinin birinci fıkrasında bakanlıklar ile diğer kamu kurum ve kuruluşlarının teşkilatlanmasına ilişkin CBK'larda öngörülmesi kaydıyla bakanlık, kurum ya da birim düzeyinde müfettiş, denetmen, denetçi, kontrolör, aktüer ile müfettiş yardımcısı, denetmen yardımcısı, denetçi yardımcısı, aktüer yardımcısı ve stajyer kontrolör istihdam edilebileceği düzenlenmiştir. Maddenin ikinci fıkrasında merkez teşkilatına ait kadro veya pozisyonlarda istihdam edilecekler hakkında 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu'nun ek 41. maddesinin ikinci, üçüncü ve dördüncü fıkraları ile yabancı dil şartı hariç olmak üzere beşinci fıkrasında yer alan hükümlerin kıyasen uygulanacağı belirtilmiş; üçüncü fıkrasında ise taşra teşkilatına ait kadro veya pozisyonlarda istihdam edilecekler

hakkında 657 sayılı Kanun'un ek 41. maddesinin ikinci, üçüncü ve dördüncü fıkraları ile yabancı dil ve tez şartı hariç olmak ve yeterlik sınavı yazılı ve sözlü aşamalardan oluşmak üzere beşinci fıkrasında yer alan hükümlerin kıyasen uygulanacağı ifade edilmiştir. Maddenin beşinci fıkrasında istihdam edilen yardımcı veya stajyerlerden verilen ilave süre içerisinde tezlerini sunmayan veya ikinci defa hazırladıkları tezleri de kabul edilmeyenlerin, ikinci sınavda da başarı gösteremeyen veya sınav hakkını kullanmayanların, yardımcı veya stajyer unvanını kaybedenlerin kurumlarında durumlarına uygun kadro veya pozisyonlara atanacakları öngörülmüştür.

54. 375 sayılı KHK'nın ek 24. maddesinin ikinci ve üçüncü fıkralarında kıyasen uygulanacağı belirtilen 657 sayılı Kanun'un "Uzman istihdamı" başlıklı ek 41. maddesinin ikinci, üçüncü, dördüncü ve beşinci fıkralarında uzman yardımcılığı kadrolarına giriş ve atanabilmek için 657 sayılı Kanun'un 48. maddesinde düzenlenen devlet memurluğuna atanacaklarda aranacak genel ve özel şartlara ek olarak yapılacak yarışma sınavına, sahip olunması gereken lisans eğitime, yarışma sınavının yazılı ve/veya sözlü olarak gerçekleştirilmesine, uzman yardımcılarının uzman kadrolarına atanabilmeleri için uzman yardımcısı olarak çalışılması gereken süreye, hazırlanacak uzmanlık tezine, yeterlilik sınavına, yabancı dil yeterlilik şartlarına ilişkin usul ve esaslar düzenlenmiştir. Bu bağlamda hazine ve maliye müfettişliği kadrolarına atanma ve mesleğe giriş, hazine ve maliye müfettiş yardımcılığına atanma suretiyle gerçekleşecektir.

2. İptal Talebinin Gerekçesi

55. Dava dilekçesinde özetle; hazine ve maliye başmüfettişleri, müfettişleri ve müfettiş yardımcılarının görev, yetki ve sorumluluklarının Anayasa'nın 128. maddesi kapsamında kanunla düzenlenmesi gerektiği, münhasıran kanunla düzenlenmesi gereken konularda CBK çıkarılmayacağı, kuralla yasamanın yetkisindeki bir alanda düzenleme yapıldığı, konuya ilişkin genel ilkeler ve çerçeve çizilmeksizin yönetmelikle düzenleme yapılmasına imkân tanınmasının hukuki belirlilik ilkesine aykırı olduğu, idareye geniş ve sınırsız bir yetki verildiği belirtilerek kuralın Anayasa'nın 2., 8., 104. ve 128. maddelerine aykırı olduğu ileri sürülmüştür.

3. Anayasa'ya Aykırılık Sorunu

56. Dava dilekçesinde konu bakımından yetki yönünden kuralın Anayasa'nın 2., 8. ve 128. maddelerine de aykırı olduğu ileri sürülmüş ise de CBK'ya ilişkin konu bakımından yetki kuralları Anayasa'nın 104. maddesinin on yedinci fıkrasında düzenlendiğinden bu husustaki inceleme anılan fıkra kapsamında yapılacaktır.

57. (1) numaralı CBK'nın 227/B maddesinin (4) numaralı fıkrasında Başkanlığın çalışma usul ve esaslarının, hazine ve maliye başmüfettişleri, müfettişleri ve müfettiş yardımcılarının görev, yetki ve sorumlulukları ile diğer hususların Hazine ve Maliye Bakanlığınca çıkarılan yönetmelikle belirleneceği öngörülmüştür. Dava konusu kural anılan fıkra da yer alan "...hazine ve maliye başmüfettişleri, müfettişleri ve müfettiş yardımcılarının görev, yetki ve sorumlulukları ile..." ibaresidir.

58. Anayasa'nın 128. maddesinde Devletin, kamu iktisadi teşebbüsleri ve diğer kamu tüzelkişilerinin genel idare esaslarına göre yürütmekle yükümlü oldukları kamu hizmetlerinin gerektirdiği asli ve sürekli görevlerin, memurlar ve diğer kamu görevlileri eliyle görüleceği ifade edilmiş; memurların ve diğer kamu görevlilerinin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülükleri, aylık ve ödenekleri ile diğer özlük işlerinin kanunla düzenleneceği belirtilmiştir.

59. Başkanlığın görev ve yetkileri CBK'nın 227/B maddesinin (1) numaralı fıkrasında genel itibarıyla Maliye ve Hazine Bakanlığı teşkilatları ile bağlı, ilgili ve ilişkili kuruluşlarının bünyesinde gerçekleştirilen faaliyet ve işlemlerin incelemesi, denetlenmesi ve soruşturulmasına ilişkin iş, işlem ve faaliyetleri yürütmek olarak belirlenmiştir. Kamu hizmeti niteliği taşıyan anılan görevlerin yerine getirilebilmesi bağlamında Başkanlıkta kadrolu olarak istihdam edilen hazine ve maliye başmüfettişleri, müfettişleri ve müfettiş yardımcılarının Anayasa'nın 128. maddesi anlamında memur veya diğer kamu görevlisi sıfatına sahip bulduklarında tereddüt bulunmamaktadır.

60. Anayasa'nın 128. maddesine göre memurlar ve diğer kamu görevlilerinin görev ve yetkileri, hakları ve yükümlülüklerinin kanunla düzenlenmesi gerekmekte olup kuralla hazine ve maliye başmüfettişleri, müfettişler ve müfettiş yardımcılarının görev, yetki ve sorumluluklarına yönelik bir düzenleme öngörülmektedir.

61. Bu itibarla Anayasa'nın 128. maddesi uyarınca münhasıran kanunla düzenlenmesi gereken bir konuda düzenleme yapan kuralın Anayasa'nın 104. maddesinin on yedinci fıkrasının üçüncü cümlesine aykırı olduğu anlaşılmaktadır.

62. Açıklanan nedenlerle kural Anayasa'nın 104. maddesinin on yedinci fıkrasının üçüncü cümlesine aykırıdır. İptali gerekir.

Kadir ÖZKAYA, Muammer TOPAL, Recai AKYEL, Yıldız SEFERİNOĞLU, Basri BAĞCI ve İrfan FİDAN bu görüşe katılmamışlardır.

Kural Anayasa'nın 104. maddesinin on yedinci fıkrasının üçüncü cümlesine aykırı görülerek iptal edildiğinden ayrıca aynı fıkranın birinci, ikinci ve dördüncü cümleleri yönünden incelenmemiştir.

Kural konu bakımından yetki yönünden Anayasa'nın 104. maddesinin on yedinci fıkrasının üçüncü cümlesine aykırı görülerek iptal edildiğinden içerik yönünden incelenmemiştir.

Ç. CBK'nın 17. Maddesiyle (1) Numaralı CBK'nın Değiştirilen 231. Maddesinin (1) Numaralı Fıkrasının (m) Bendinin İncelenmesi

1. Genel Açıklama

63. Kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esaslar bu konuda kabul edilmiş genel kanun niteliğindeki 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda düzenlenmiş, bazı kanunlarda da kişisel verilerle ilgili hükümlere yer verilerek konuya ilişkin kanuni güvencenin sağlanması amaçlanmıştır.

64. 6698 sayılı Kanun'un uygulanması bakımından genel olarak Kanun'a tabi bulunan kişiler, kurum veya kuruluşlar tek tek belirtilmek suretiyle herhangi bir istisna öngörülmemiş ise de Kanun'un 28. maddesinde kişisel verinin işlenmesindeki amaç ve kapsam yönünden birtakım istisnalara yer verilerek bazı hâllerde 6698 sayılı Kanun'un uygulanmayacağı düzenlenmiştir. Anılan maddenin (1) numaralı fıkrasının (ç) bendinde kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi hâlinde 6698 sayılı Kanun hükümlerinin uygulanmayacağı ifade edilmiştir. Kurala ilişkin olarak madde gerekçesinde ise suç gelirlerinin aklanması, terörizmin finansmanının önlenmesi ve mali suçların araştırılması konusunda yetkili birim tarafından yürütülen faaliyetler kapsamında işlenen verilerin de istisna kapsamında yer aldığı, bu konulardaki yetkili birimin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik olmak üzere mali araştırma yapmak, mali istihbarat elde etmek ve üretmek, veri toplamak, şüpheli işlem bildirimleri ve diğer bildirimleri almak, analiz etmek, değerlendirmek, inceleme yapmak ve ilgili kurumlarla paylaşmak suretiyle işlediği verilerin de kapsam dışında tutulduğu ifade edilmiştir.

65. Suç gelirlerinin aklanmasının önlenmesine ilişkin usul ve esasları belirlemek amacıyla 11/10/2006 tarihli ve 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun kabul edilmiş; Kanun'un 2. maddesinin (d) bendinde Kanun'da geçen yükümlü kavramının bankacılık, sigortacılık, bireysel emeklilik, sermaye piyasaları, ödünç para verme ve diğer finansal hizmetler ile posta ve taşımacılık, talih ve bahis oyunları alanında faaliyet gösterenleri, döviz, taşınmaz, değerli taş ve maden, mücevher, nakil vasıtası, iş makinesi, tarihî eser, sanat eseri ve antika ticareti ile iştiğal edenler veya bu faaliyetlere aracılık edenler ile noterler, spor kulüpleri, savunma hakkı bakımından diğer

kanun hükümlerine aykırı olmamak ve 19/3/1969 tarihli ve 1136 sayılı Avukatlık Kanunu'nun 35. maddesinin birinci fıkrası ile alternatif uyuşmazlık çözüm yolları kapsamında ifa edilen mesleki çalışmalar nedeniyle edinilen bilgiler hariç olmak üzere taşınmaz alım satımı, sınırlı ayni hak kurulması ve kaldırılması, şirket, vakıf ve dernek kurulması, birleştirilmesi ile bunların idaresi, devredilmesi ve tasfiyesi işlerine ilişkin finansal işlemlerin gerçekleştirilmesi, banka, menkul kıymet ve her türlü hesaplar ile bu hesaplarda yer alan varlıkların idaresi işleriyle sınırlı olmak üzere serbest avukatlar ve Cumhurbaşkanınca belirlenen diğer alanlarda faaliyet gösterenleri ifade ettiği açıklanmıştır.

66. Kanun'un şüpheli işlem bildirim yükümlülüğünü düzenleyen 4. maddesinin (1) numaralı fıkrasında yükümlüler nezdinde veya bunlar aracılığıyla yapılan veya yapılmaya teşebbüs edilen işlemlere konu mal varlığının yasa dışı yollardan elde edildiğine veya yasa dışı amaçlarla kullanıldığına dair herhangi bir bilgi, şüphe veya şüpheyi gerektirecek bir hususun bulunması hâlinde bu işlemlerin yükümlüler tarafından Mali Suçları Araştırma Kurulu Başkanlığına (MASAK) bildirilmesinin zorunlu olduğu belirtilmiştir.

67. Kanun'un, yükümlülerce MASAK'a devamlı bilgi verme zorunluluğunu düzenleyen 6. maddesinin (1) numaralı fıkrasında da, yükümlülerin taraf oldukları veya aracılık ettikleri işlemlerden, Hazine ve Maliye Bakanlığınca belirlenecek tutarı aşanları MASAK'a bildirmek zorunda oldukları belirtilmiş; (3) numaralı fıkrasında ise Kanun'un uygulanmasına ilişkin olarak yükümlüler dışındaki kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki kurum ve kuruluşlardan da MASAK'a devamlı bilgi vermelerinin istenebileceği açıklanmıştır. Kurala ilişkin madde gerekçesinde suç gelirlerinin aklanmasıyla mücadele kapsamındaki değerlendirmelerde ve uygulamaya ilişkin stratejilerin belirlenmesinde yararlanılacak verilerin elde edilmesi amacıyla yükümlülerin taraf oldukları veya aracılık ettikleri belli bir tutarı aşan işlemleri belirlenecek usul ve esaslar dâhilinde MASAK'a bildirmelerinin öngörüldüğü vurgulanmıştır.

68. Kanun'un 7. maddesinde kamu kurum ve kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği olmayan kuruluşların bilgi ve belge verme yükümlülüğü düzenlenmiştir. Maddenin (1) numaralı fıkrasında söz konusu kişi, kurum ve kuruluşların MASAK ve denetim elemanları tarafından istenilecek her türlü bilgi, belge ve bunlara ilişkin her türlü ortamdaki kayıtları, bu kayıtlara erişimi sağlamak veya okunabilir hâle getirmek için gerekli tüm bilgi ve şifreleri tam ve doğru olarak vermek ve gerekli kolaylığı sağlamakla yükümlü oldukları belirtilmiştir.

69. Ayrıca Kanun'un 9. maddesinde suç gelirlerinin aklanmasıyla mücadele kapsamında hızlı hareket edilebilmesinin ve uygun sürede veriye ulaşılabilmesinin sağlanabilmesi amacıyla, Türkiye

Cumhuriyet Merkez Bankası hariç olmak üzere kamu sermayeli bankalar ile kamu iktisadî teşebbüsleri dışında, kanunları veya faaliyet konuları gereğince ekonomik olaylara, servet unsurlarına, vergi mükellefiyetlerine, nüfus bilgilerine ve yasa dışı faaliyetlere ilişkin kayıt tutan kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki kurum ve kuruluşların bilgi işlem sistemlerine Bakanlık ve ilgili Bakanlığın veya kamu kurumu niteliğindeki kurum ve kuruluşların yetkili organlarının birlikte belirleyeceği usul ve esaslar dahilinde MASAK tarafından erişim sistemi kurulabileceği ifade edilmiştir.

2. İptal Talebinin Gerekçesi

70. Dava dilekçesinde özetle; kuralla MASAK'a kişisel verileri de içine alan geniş bir alanda bilgi toplama yetkisi verildiği, kişisel verilerin toplanması, işlenmesi ve verilerle ilgili diğer işlemlerin çerçevesinin ayrıntılı bir şekilde kanunla çizilmesi gerektiği, belirtilen hususlar gözetilmeksizin MASAK'ın bilgi ve belge istemeye yetkili kılınmasının hukuk devleti ve öngörülebilirlik ilkelerine aykırı olduğu, Anayasa'nın 20. maddesi kapsamında kalan kişisel verilerle ilgili meselelerin CBK ile düzenlenemeyeceği belirtilerek kuralın Anayasa'nın 2., 20. ve 104. maddelerine aykırı olduğu ileri sürülmüştür.

3. Anayasa'ya Aykırılık Sorunu

71. Dava dilekçesinde konu bakımından yetki yönünden kuralın Anayasa'nın 2. ve 20. maddelerine de aykırı olduğu ileri sürülmüş ise de CBK'ya ilişkin konu bakımından yetki kuralları Anayasa'nın 104. maddesinin on yedinci fıkrasında düzenlendiğinden bu husustaki inceleme anılan fıkra kapsamında yapılacaktır.

72. (1) numaralı CBK'nın dava konusu kuralın da yer aldığı 231. maddesinde Hazine ve Maliye Bakanlığının hizmet birimlerinden olan MASAK'ın görev ve yetkileri ile çalışma usul ve esasları düzenlenmiştir. Dava konusu kuralda MASAK'ın, kamu kurum ve kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği olmayan kuruluşlardan her türlü bilgi ve belgeyi istemek hususunda görevli ve yetkili olduğu hüküm altına alınmıştır.

73. Anayasa'nın 104. maddesinin on yedinci fıkrasının ikinci cümlesinde CBK ile düzenlenemeyecek konular Anayasa'nın İkinci Kısım Birinci ve İkinci Bölümlerinde yer alan temel haklar, kişi hakları ve ödevleriyle Dördüncü Bölüm'de yer alan siyasi haklar ve ödevler olarak belirtilmiştir.

74. Kişisel verilerin korunması hakkı Anayasa'nın 20. maddesi kapsamında anayasal güvenceye bağlanmıştır. Anılan maddenin üçüncü fıkrasında herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu ifade edilmiş; kişisel verilerin, ancak kanunda öngörülen

hâllerde veya kişinin açık rızasıyla işlenebileceği, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir. Buna göre Anayasa'nın anılan maddesinde düzenlenen ve "Kişinin Hakları ve Ödevleri" başlıklı "İkinci Bölüm"ünde yer alan kişisel verilerin korunması hakkına ilişkin olarak CBK ile düzenleme yapılması mümkün değildir.

75. CBK'nın 231. maddesinin (1) numaralı fıkrası kapsamında MASAK'ın suç gelirlerinin aklanmasının ve terörizmin finansmanının önlenmesi ile ekonomik güvenlikle ilgili olarak plan, program, politika, strateji hazırlama ve geliştirme süreçlerine katkıda bulunma, kurum ve kuruluşlar arasında koordinasyon ve iş birliği sağlama, mevzuat çalışmaları yapma, gelişmeleri izleme, önlemler geliştirme, analiz, araştırma ve inceleme yapma, yaptırma, yükümlülere bilgilendirme, veri toplama, suç şüphesi bulunması hâlinde konuyu ilgili Cumhuriyet savcılığına taşıma, suç duyurusunda bulunma, şüpheli işlem bildirimleri alma ve bunları analiz etme, kaydetme, istihbarat üretme, ilgili birimleri bilgilendirme, 5549 sayılı Kanun ve ilgili mevzuat kapsamında yükümlülük denetimi ve buna ilişkin iş ve işlemleri yapma, görev alanına giren konularda uluslararası ilişkileri yürütme, yabancı ülkelerdeki muadil kurumlarla görüş ve bilgi alışverişinde bulunma, kamuoyu duyarlılığını ve desteğini artırmaya yönelik çalışmalar yapma gibi hususlarda görevli ve yetkili kılındığı anlaşılmaktadır.

76. Anılan görev ve yetkiler ile Genel Açıklama bölümünde yer verilen (bkz. §§ 65-69) 5549 sayılı Kanun kapsamındaki düzenlemeler dikkate alındığında MASAK'ın görev ve yetkilerinin önemli ölçüde veri işlenmesi ile buna ilişkin iş ve işlemlerden oluştuğu anlaşılmaktadır.

77. Anayasa Mahkemesi daha önce CBK ile kurulan Cumhurbaşkanlığı İletişim Başkanlığı ile Strateji ve Bütçe Başkanlığının görevleriyle ilgili olarak gerekli gördükleri bilgileri isteyebilmelerine ilişkin kuralların Anayasa'ya aykırı olmadığına karar vermiştir. Mahkemenin, 3/3/2021 tarihli E.2018/134, K.2021/13 ve 13/10/2021 tarihli ve E.2018/133, K.2021/70 sayılı kararlarında öncelikle adı geçen Başkanlıkların görev ve yetkileri ortaya konulmuş; gerekli görülen bilgilerin istenebilmesinin CBK ile belirlenen görev ve yetkilerin yerine getirilebilmesinin doğal ve zorunlu bir sonucu olduğu ifade edilmiştir. Kuralların idarenin teşkilatlanması bağlamında bilgi ve belge istemeyi düzenlediği, yeni hükümet sistemine uygun kurumsal yapı ve işleyişin düzenlenmesinden hareketle getirilen kuralların kişisel verilere ilişkin düzenleme getirmeyi amaçlamadığı, kişisel verilere ilişkin her türlü işlemin 6698 sayılı Kanun ve kişisel verilere ilişkin diğer kanuni düzenlemelerde yer alan hükümlere uygun olarak gerçekleştirileceğinin açık olduğu ortaya konulmuştur.

78. Dava konusu kuralda ise yukarıda anılan kararlara konu olan düzenlemelerden farklı olarak MASAK'a her türlü bilgi ve belgeyi isteme yetkisi verildiği görülmektedir. Bu yönüyle kuralın

yalnızca teşkilatlanma ile kurumsal yapı ve işleyişin düzenlenmesinden ibaret olduğu söylenemez. Veri toplamak görev ve yetkisi MASAK'ın görev ve yetkileri arasında açıkça sayılmış olup suç gelirlerinin aklanması, terörizmin finansmanının önlenmesi ile mali suçların araştırılması gibi konularda yürütülen faaliyetler kapsamında istenecek bilgi ve belgelerin doğrudan kişisel verilere ilişkin bulunduğu açıktır.

79. Bu itibarla kural kişisel verilere ilişkin bir düzenleme niteliğinde olup CBK ile düzenlenemeyecek yasak alan içinde kalmaktadır.

80. Açıklanan nedenlerle kural, Anayasa'nın 104. maddesinin on yedinci fıkrasının ikinci cümlesine aykırıdır. İptali gerekir.

Zühtü ARSLAN, Engin YILDIRIM, M. Emin KUZ ile Yusuf Şevki HAKYEMEZ bu görüşe farklı gerekçeyle katılmışlardır.

Kural Anayasa'nın 104. maddesinin on yedinci fıkrasının ikinci cümlesine aykırı görülerek iptal edildiğinden ayrıca anılan fıkranın birinci, üçüncü ve dördüncü cümleleri yönünden incelenmemiştir.

Kural konu bakımından yetki yönünden Anayasa'nın 104. maddesinin on yedinci fıkrasının ikinci cümlesine aykırı görülerek iptal edildiğinden içerik yönünden incelenmemiştir.

D. CBK'nın Geçici 1. Maddesinin İncelenmesi

81. CBK'nın dava konusu geçici 1. maddesinin birinci fıkrasının birinci cümlesinin "Bu maddenin yürürlüğe girdiği tarihte Hazine ve Maliye Bakanlığında vergi başmüfettişi, vergi müfettişi ve yeterlik sınavında başarı göstermiş olmak kaydıyla vergi müfettiş yardımcısı kadrolarında bulunanlardan uygun görülenler, bu maddenin yürürlüğe girdiği tarihten itibaren üç ay içerisinde" bölümü 17/4/2020 tarihli ve (60) numaralı CBK'nın 21. maddesiyle "Hazine ve Maliye Bakanlığında vergi başmüfettişi, vergi müfettişi ve yeterlik sınavında başarı göstermiş olmak kaydıyla vergi müfettiş yardımcısı kadrolarında bulunanlardan uygun görülenler, vergi başmüfettişi ve vergi müfettişi unvanını ihraz etmiş olanlardan Hazine ve Maliye Bakanlığının merkez, bağlı, ilgili ve ilişkili kuruluşlarının kadrolarında bulunanlardan uygun görülenler, hazine kontrolörü kadrolarında bulunanlardan uygun görülenler ve 2/11/2011 tarihinden önce Hazine ve Maliye Bakanlığında mesleğe stajyer kontrolör olarak başlayıp yeterlik sınavında başarı göstermiş olanlardan bu maddenin yürürlüğe girdiği tarihte Hazine ve Maliye Bakanlığı ile bağlı, ilgili ve ilişkili kuruluşlarının kadrolarında bulunanlardan uygun görülenler 31/12/2020 tarihine kadar (bu tarih dahil)..." şeklinde; fıkranın ikinci cümlesinde yer alan "hazine ve maliye müfettişi" ibaresi "hazine ve maliye başmüfettişi, hazine ve maliye müfettişi ya da hazine ve maliye müfettiş yardımcısı"

şeklinde değiştirilmiş ve fıkraya “Bu şekilde atananların, önceki kurumlarında ihraz ettikleri yeterlikleri Hazine ve Maliye Bakanlığı Teftiş Başkanlığında ihraz edilmiş sayılır.” şeklindeki cümle eklenmiştir.

82. Açıklanan nedenle konusu kalmayan kurala ilişkin iptal talebi hakkında karar verilmesine yer olmadığına karar vermek gerekir.

IV. İPTAL KARARININ YÜRÜRLÜĞE GİRECEĞİ GÜN SORUNU

83. Anayasa'nın 153. maddesinin üçüncü fıkrasında “Kanun, Cumhurbaşkanlığı kararnamesi veya Türkiye Büyük Millet Meclisi İçtüzüğü ya da bunların hükümleri, iptal kararlarının Resmî Gazetede yayımlandığı tarihte yürürlükten kalkar. Gereken hallerde Anayasa Mahkemesi iptal hükmünün yürürlüğe gireceği tarihi ayrıca kararlaştırabilir. Bu tarih, kararın Resmî Gazetede yayımlandığı günden başlayarak bir yılı geçemez.” denilmekte; 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 66. maddesinin (3) numaralı fıkrasında da bu kural tekrarlanarak Mahkemenin gerekli gördüğü hâllerde Resmî Gazete'de yayımlandığı günden başlayarak iptal kararının yürürlüğe gireceği tarihi bir yılı geçmemek üzere ayrıca kararlaştırabileceği belirtilmektedir.

84. (43) numaralı CBK'nın 14. maddesiyle (1) numaralı CBK'ya eklenen 227/B maddesinin (4) numaralı fıkrasının “...hazine ve maliye başmüfettişleri, müfettişleri ve müfettiş yardımcılarının görev, yetki ve sorumlulukları ile...” bölümünün ve aynı CBK'nın 17. maddesiyle (1) numaralı CBK'nın değiştirilen 231. maddesinin (1) numaralı fıkrasının (m) bendinin iptal edilmesi nedeniyle doğacak hukuksal boşluk kamu yararını ihlal edecek nitelikte görüldüğünden Anayasa'nın 153. maddesinin üçüncü fıkrasıyla 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince bu bölüme ve bende ilişkin iptal hükmünün kararın Resmî Gazete'de yayımlanmasından başlayarak dokuz ay sonra yürürlüğe girmesi uygun görülmüştür.

V. YÜRÜRLÜĞÜN DURDURULMASI TALEBİ

85. Dava dilekçesinde özetle, dava konusu kuralların uygulanması hâlinde telafisi güç veya imkânsız zararlar doğabileceği belirtilerek yürürlüklerinin durdurulmasına karar verilmesi talep edilmiştir.

6/8/2019 tarihli ve (43) numaralı Bazı Cumhurbaşkanlığı Kararnamelerinde Değişiklik Yapılması Hakkında Cumhurbaşkanlığı Kararnamesi'nin ;

A. 1. 14. maddesiyle 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete'de yayımlanan (1) numaralı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'ne eklenen 227/B maddesinin

(4) numaralı fıkrasının "...hazine ve maliye başmüfettişleri, müfettişleri ve müfettiş yardımcılarının görev, yetki ve sorumlulukları ile..." bölümüne,

2. 17. maddesiyle (1) numaralı Cumhurbaşkanlığı Kararnamesi'nin değiştirilen 231. maddesinin (1) numaralı fıkrasının (m) bendine,

yönelik iptal hükümlerinin yürürlüğe girmelerinin ertelenmeleri nedeniyle bu bölüme ve bende ilişkin yürürlüğün durdurulması taleplerinin REDDİNE,

B. 1. maddesiyle (1) numaralı Cumhurbaşkanlığı Kararnamesi'nin 217. maddesinin (1) numaralı fıkrasının (ğ) bendine [17/4/2020 tarihli ve (60) numaralı CBK'nın 1. maddesiyle 217. maddede yapılan değişiklikten sonra (h) bendi] eklenen "...ve Hazinesinin Cumhurbaşkanlığı Kararnamesi ile yurtiçindeki ya da yurtdışındaki şirketlere iştirak etmesini sağlamak," ibaresine yönelik iptal talebi 24/2/2022 tarihli ve E.2019/96, K.2022/17 sayılı kararla reddedildiğinden bu ibareye ilişkin yürürlüğün durdurulması talebinin REDDİNE,

C. Geçici 1. maddesine ilişkin iptal talebi hakkında 24/2/2022 tarihli ve E.2019/96, K.2022/17 sayılı kararla karar verilmesine yer olmadığına karar verildiğinden bu maddeye ilişkin yürürlüğün durdurulması talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA,

24/2/2022 tarihinde OYBİRLİĞİYLE karar verilmiştir.

VI. SONUÇ

6/8/2019 tarihli ve (43) numaralı Bazı Cumhurbaşkanlığı Kararnamelerinde Değişiklik Yapılması Hakkında Cumhurbaşkanlığı Kararnamesi'nin;

A. 1. maddesiyle 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete'de yayımlanan (1) numaralı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin 217. maddesinin (1) numaralı fıkrasının (ğ) bendine [17/4/2020 tarihli ve (60) numaralı CBK'nın 1. maddesiyle 217. maddede yapılan değişiklikten sonra (h) bendi] eklenen "...ve Hazinesinin Cumhurbaşkanlığı Kararnamesi ile yurtiçindeki ya da yurtdışındaki şirketlere iştirak etmesini sağlamak," ibaresinin,

1. Konu bakımından yetki yönünden Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

2. İçeriği itibarıyla Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ ile Yusuf Şevki HAKYEMEZ'in karşıoyları ve OYÇOKLUĞUYLA,

B. 14. maddesiyle (1) numaralı Cumhurbaşkanlığı Kararnamesi'ne eklenen 227/B maddesinin (4) numaralı fıkrasının "...hazine ve maliye başmüfettişleri, müfettişleri ve müfettiş yardımcılarının görev, yetki ve sorumlulukları ile..." bölümünün konu bakımından yetki yönünden Anayasa'ya aykırı olduğuna ve İPTALİNE, Kadir ÖZKAYA, Muammer TOPAL, Recai AKYEL, Yıldız SEFERİNOĞLU, Basri BAĞCI ile İrfan FİDAN'ın karşıoyları ve OYÇOKLUĞUYLA, iptal hükmünün Anayasa'nın 153. maddesinin üçüncü fıkrası ile 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAŞLAYARAK DOKUZ AY SONRA YÜRÜRLÜĞE GİRMESİNE OYBİRLİĞİYLE,

C. 17. maddesiyle (1) numaralı Cumhurbaşkanlığı Kararnamesi'nin değiştirilen 231. maddesinin (1) numaralı fıkrasının (m) bendinin konu bakımından yetki yönünden Anayasa'ya aykırı olduğuna ve İPTALİNE, iptal hükmünün Anayasa'nın 153. maddesinin üçüncü fıkrası ile 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAŞLAYARAK DOKUZ AY SONRA YÜRÜRLÜĞE GİRMESİNE OYBİRLİĞİYLE,

Ç. Geçici 1. maddesine ilişkin iptal talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA OYBİRLİĞİYLE,

24/2/2022 tarihinde karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili - Hasan Tahsin GÖKCAN

Başkanvekili - Kadir ÖZKAYA

Üye: Engin YILDIRIM, Hicabi DURSUN, Muammer TOPAL, M. Emin KUZ, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĞLU, Basri BAĞCI, İrfan FİDAN, Kenan YAŞAR

FARKLI GEREKÇE VE KARŞIOY GEREKÇESİ

1. 6/8/2019 tarihli ve (43) numaralı Bazı Cumhurbaşkanlığı Kararnamelerinde Değişiklik Yapılması Hakkında Cumhurbaşkanlığı Kararnamesi'nin (CBK) 1. maddesiyle (1) numaralı CBK'nın 217. maddesinin (1) numaralı fıkrasının (ğ) bendine (bilahare (h) bendi) eklenen "... ve Hazinesinin Cumhurbaşkanı kararı ile yurtiçindeki ya da yurtdışındaki şirketlere iştirak etmesini sağlamak," ibaresinin Anayasa'ya aykırı olmadığına; 17. maddesiyle (1) numaralı CBK'nın değiştirilen 231. maddesinin (1) numaralı fıkrasının (m) bendinin ise iptaline karar verilmiştir. Aşağıda açıklanan

nedenlerle iptal sonucuna farklı gerekçeyle katılmakla birlikte, çoğunluğun red kararına içerik yönünden katılma imkânı olmamıştır.

I. FARKLI GEREKÇE

2. (43) numaralı CBK'nın 17. maddesiyle (1) numaralı CBK'nın değiştirilen 231. maddesinin (1) numaralı fıkrasının (m) bendi oybirliğiyle iptal edilmiştir. İptali istenen kuralda "Kamu kurum ve kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği olmayan kuruluşlardan her türlü bilgi ve belgeyi istemek" Hazine ve Maliye Bakanına bağlı Mali Suçları Araştırma Kurulu Başkanlığının (MASAK) görev ve yetkileri arasında sayılmıştır.

3. Mahkememiz çoğunluğu, kuralın daha önce Anayasa'ya aykırı olmadığına karar verilen Cumhurbaşkanlığı İletişim Başkanlığı ile Strateji ve Bütçe Başkanlığının görevleriyle ilgili olarak gerekli gördükleri bilgileri isteyebileceklerine dair CBK hükümlerinden farklı olduğunu, bu kurumlarca bilgi talebinin CBK'nın belirlediği görev ve yetkilerin yerine getirilebilmesinin doğal ve zorunlu sonucu olduğunu, halbuki görev ve yetkileri önemli ölçüde veri işlenmesi ile buna ilişkin iş ve işlemlerden oluşan MASAK'a her türlü bilgi ve belgeyi isteme yetkisi veren kuralın doğrudan kişisel verilere ilişkin olduğunu, bu sebeple CBK ile düzenlenemeyecek yasak alan kapsamında kaldığını belirtmiştir (§§ 77-79).

4. Dava konusu kuralın, Anayasa'nın 104. maddesinin on yedinci fıkrasının CBK ile temel hak ve özgürlüklerin düzenlenemeyeceğini öngören ikinci cümlesine aykırı olduğu sonucuna katılmakla birlikte, kuralın iptal gerekçesine katılmak mümkün değildir. Anayasa Mahkemesi, Cumhurbaşkanlığı İletişim Başkanlığı ile Strateji ve Bütçe Başkanlığının "görevleri ile ilgili olarak gerekli gördüğü bilgileri bütün kamu kurum ve kuruluşlarından ve diğer gerçek ve tüzel kişilerden doğrudan istemeye yetkili" olduklarını belirten CBK kurallarını "kişisel verilere ilişkin düzenleme içermeyen ve kişisel verilerle ilgili bulunmayan" hükümler olarak değerlendirmek suretiyle kuralların Anayasa'ya aykırı olmadığına karar vermiştir (AYM, E.2018/134, K.2021/13, 3/3/2021, § 23; AYM, E.2018/133, K.2021/70, 13/10/2021, § 45).

5. Bu kararlardaki karşıoy gerekçelerinde de belirttiğimiz üzere, söz konusu kurumların görev alanlarının genişliği dikkate alındığında istenen veriler arasında kişisel verilerin bulunmaması mümkün değildir. Zira kişisel veri sadece kişinin adı ve soyadı, doğum yeri ve tarihi gibi kimlik bilgilerini değil, telefon numarası, motorlu taşıt plakası, pasaport numarası, özgeçmiş bilgileri, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, etkileşimde bulunulan kişiler, grup üyelikleri ve aile bağları gibi kişiyi belirlenebilir kılan tüm bilgileri kapsamaktadır (AYM, E.2017/180, K.2018/109, 6/12/2018, § 54; AYM, E.2018/73, K.2019/65, 24/7/2019, § 168).

6. Diğer yandan bir CBK hükmünün Anayasa'nın 104. maddesinin on yedinci fıkrasının ikinci cümlesi çerçevesinde yasak alanda düzenleme içerip içermediğini belirlerken kurumun görev alanının ağırlıklı olarak kişisel verilerin toplanmasına veya işlenmesine ilişkin olması gerekmemektedir. Esasen böyle bir kriteri kabul etmek, görevi ağırlıklı olarak veri toplanmasına ve işlenmesine yönelik olan birkaç kamu kurumu dışında tüm kurum ve kuruluşların görevleriyle ilgili her türlü bilgiyi herkesten isteme yetkisine CBK ile sahip kılınabileceği anlamına gelecektir. Bunun da CBK'lara ilişkin yasak alan sınırlamasını işlevsiz hale getireceği açıktır.

7. Halbuki Anayasa'nın 104. maddesinin on yedinci fıkrasının ikinci cümlesi uyarınca temel haklar, kişi hakları ve siyasi haklar CBK ile düzenlenemez. Anayasa'nın 20. maddesinde güvence altına alınan kişisel verilerin korunmasını isteme hakkı, Anayasa'da CBK ile düzenlenemeyeceği öngörülen "yasak alan" kapsamında kalan temel haklar arasındadır. Buradaki düzenleme yasağı, sınırlandırmayı da içine alan ancak onunla sınırlı olmayan ve sınırlama mahiyetinde olmasa da anılan hak ve özgürlüklere yönelik olan her türlü düzenlemeyi içermektedir.

8. Sonuç olarak, dava konusu CBK hükmü ile daha önce Anayasa'ya uygun bulunan CBK hükümleri arasında anayasallık denetimi bakımından hiçbir fark bulunmamaktadır. Bu sebeple iptal kararına kuralın, tıpkı daha öncekiler gibi, kişisel verilerin korunması hakkına ilişkin bir düzenleme mahiyetinde olduğu gerekçesiyle ve yukarıda zikredilen karşıoylarda belirtilen nedenlerle katılıyorum.

II. KARŞIOY GEREKÇESİ

9. (43) numaralı CBK'nın 1. maddesiyle (1) numaralı CBK'nın 217. maddesinin (1) numaralı fıkrasının (ğ) bendine (bilahare (h) bendi) eklenen "... ve Hazinesin Cumhurbaşkanın kararı ile yurtiçindeki ya da yurtdışındaki şirketlere iştirak etmesini sağlamak," ibaresinin Anayasa'ya aykırı olmadığına ve iptal talebinin reddine karar verilmiştir.

10. İptali istenen ibarenin eklendiği madde Hazine ve Maliye Bakanlığının görev ve yetkilerini düzenlemektedir. Buna göre Cumhurbaşkanın kararıyla yurtiçindeki ya da yurtdışındaki şirketlere Hazinesin iştirak etmesini sağlamak da bu Bakanlığın görev ve yetkileri arasına dahil edilmiştir.

11. Kuşkusuz, Hazine ve Maliye Bakanlığına Cumhurbaşkanın kararıyla Hazinesin yurtiçi ve yurtdışı şirketlere iştirak etmesini sağlama görev ve yetkisinin verilmesi, bir ülkede uygulanan ekonomi politikasıyla doğrudan ilgilidir ve bu anlamda CBK koyucunun takdir yetkisi içindedir. Bunun yerindeliği anayasallık denetiminin konusu olamaz. Bununla birlikte Bakanlığa verilen görev ve

yetkinin konu ve içerik yönlerinden Anayasa'ya uygun olup olmadığını denetlemek Anayasa Mahkemesinin görevidir.

12. Hazine ve Maliye Bakanlığının görev ve yetkilerinin CBK ile düzenlenmesi mümkündür. Nitekim Anayasa'nın 106. maddesinin on birinci fıkrası uyarınca "Bakanlıkların ... görev ve yetkileri ...Cumhurbaşkanlığı kararnamesiyle düzenlenir". Kuralın CBK'ların konu yönünden taşıması gereken diğer şartları da haiz olduğu konusunda çoğunlukla hemfikirim. Ancak CBK hükmünün içerik yönünden de Anayasa'ya aykırı olmadığı görüşüne katılmak mümkün değildir.

13. Anayasa'nın 2. maddesinde güvence altına alınan ve bir anlamda devletin diğer tüm niteliklerini de belirleyen hukuk devleti ilkesi, toplumsal hayatı düzenleyen kuralların açık, belirli ve öngörülebilir olmasını gerektirmektedir. Bu durum demokratik hukuk devletinin olmazsa olmaz şartlarından biridir.

14. Anayasa Mahkemesinin kararlarında sıklıkla vurgulandığı üzere hukuk devletinin temel unsurlarından olan hukuki belirlilik ilkesi uyarınca kanuni düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfî uygulamalarına karşı koruyucu önlem içermesi gerekir. Kanunda bulunması gereken bu nitelikler hukuki güvenliğin sağlanması bakımından da zorunludur. Zira bu ilke hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar (AYM, E.2015/41, K.2017/98, 4/5/2017, §§ 153, 154; AYM, E. 2020/15, K. 2020/78, 24/12/2020, § 10; İ.K. [GK], B.No: 2019/20904, 15/4/2021, § 47).

15. Hukuki belirlilik ve güvenlik ilkelerinin yürütmenin ilk elden düzenleyici işlemi olan CBK'lar bakımında da geçerli olduğu izahtan varestedir. Bu anlamda CBK ile düzenlenebilecek bir konuda Cumhurbaşkanı tarafından usulüne uygun, şekil şartlarını taşıyan bir Cumhurbaşkanlığı kararnamesinin çıkarılması yeterli değildir. CBK hükümlerinin keyfi uygulamalara izin vermeyecek şekilde açık, belirli ve herkes için öngörülebilir nitelikte olması zorunludur.

16. Diğer yandan konuya ilişkin her ayrıntının mutlaka CBK'da düzenlenmesi gerekmez. Kanun koyucunun bazı durumlarda yaptığı gibi, CBK koyucu da düzenlediği konuya ilişkin genel çerçeveyi, temel kural, ilke, esas ve şartları belirledikten sonra idare tekniği ve uzmanlığa dair diğer hususların düzenlenmesini alt idari işlemlere bırakabilir. Bu şartları taşımayan bir CBK hükmü konu bakımından Anayasa'ya uygun olsa bile içerik yönünden Anayasa'ya aykırı olacaktır.

17. Dava konusu CBK hükmü tam da böyle bir kuraldır. Zira kural sadece Hazine ve Maliye Bakanlığının, Hazinesinin yurtiçi ve yurtdışı şirketlere Cumhurbaşkanı kararı ile iştirak etmesini sağlama görev ve yetkisine sahip olduğunu belirtmekte, bunun dışında söz konusu iştirakin usul ve esaslarına dair herhangi bir düzenlemeye yer vermemektedir. Başka bir ifadeyle, kural Cumhurbaşkanının hangi durumlarda, hangi kriter ve şartlara uyarak Hazinesinin yurtiçindeki ve yurtdışındaki şirketlere iştirak etmesine karar vereceğine ilişkin herhangi bir açıklık ve belirlilik taşımamaktadır. Kural iştirak edilecek şirketlerin türü, mali durumu ve faaliyet yürüttüğü alanlar gibi konularda herhangi bir sınırlama getirmediği gibi, söz konusu iştirakin bilhassa yurtdışındaki şirketler yönünden hangi hukuka tabi olacağına dair bir düzenleme ya da herhangi bir kanuna atıf da içermemektedir. Dahası CBK'nın başka maddelerinde veya diğer herhangi bir kanunda da doğrudan konuya ilişkin düzenleme yer almamaktadır. Kısacası, dava konusu kural iştirak öncesi ve sonrasına ilişkin usul ve esasları düzenlemediğinden belirlilik ilkesine aykırılık teşkil etmektedir.

18. Anılan belirsizliklerin "Cumhurbaşkanı kararıyla" veya Bakanlığın düzenlemeleriyle giderilebileceği söylenebilir. Nitekim (1) numaralı CBK'nın "Ortak Hükümler" başlıklı bölümünde yer alan 508. madde uyarınca "Bakanlık görev, yetki ve sorumluluk alanına giren konularda idari düzenlemeler yapabilir". Bu anlamda her ne kadar dava konusu kuralda açıkça ifade edilmemiş olsa da iştirake ilişkin usul ve esasların CBK dışında idari düzenleyici işlemlerle düzenlenmesinin öngörüldüğü kabul edilebilir.

19. Ancak bu yorum da kuralı Anayasa'ya uygun hale getirmeyecektir. Yukarıda ifade edildiği gibi, hukuk devletinde kanunilik ilkesi genel ilke ve esasların mutlaka kanunda/CBK'da düzenlenmesini gerektirmektedir. Bu yapılmadan konunun idarenin (diğer) düzenleyici işlemlerine bırakılması kanunlar bakımından yasama yetkisinin devri, kararnameler bakımından da CBK çıkarma yetkisinin devri sonucunu doğurabilir.

20. İkincisinde devreden ve devredilenin aynı organ (Cumhurbaşkanı) olması da bu durumu değiştirmemektedir. Zira Cumhurbaşkanlığı kararnameleriyle Cumhurbaşkanı kararlarının farklı hukuki rejimlere tabi olduğu, dolayısıyla CBK ile düzenlenebilecek bir konunun doğrudan Cumhurbaşkanı kararıyla düzenlenemeyeceği açıktır. Bu bağlamda Anayasa'nın 106. maddesinin son fıkrasının açık hükmü karşısında bakanlıkların görev ve yetkilerinin CBK yerine Cumhurbaşkanlığı kararı veya diğer düzenleyici işlemlerle belirlenmesi mümkün değildir.

21. Daha önemlisi CBK yetkisinin devri, diğer sakıncalarının yanında, yargısal denetimin mahiyetini ve mercilerini değiştirebilecektir. Nitekim CBK'ların konu ve içerik bakımından anayasallık denetimi Anayasa Mahkemesince yapılırken, Cumhurbaşkanlığı kararlarının veya bakanlıkların idari

işlemlerinin denetimi idari yargı düzeninde gerçekleşmektedir. Bu sebeple CBK ile düzenlenmesi gereken bir konunun Cumhurbaşkanı kararıyla veya diğer düzenleyici işlemlerle düzenlenmesi durumunda, normalde anayasa yargısı kapsamında denetlenmesi gereken söz konusu normun idari yargı düzenine taşınması mümkün olacaktır.

22. Bunun yanında CBK ile düzenlenmesi gereken bir konunun genel çerçevesi, temel ilke ve esasları belirlenmeden Cumhurbaşkanı kararına, Cumhurbaşkanı veya bakanlıklar tarafından çıkarılacak yönetmeliklere bırakılması, bu işlemlerin CBK'ya uygunluk denetimini de işlevsiz kılacaktır. Bu noktada can alıcı soru şudur: CBK yetkisinin devredildiği durumlarda idari yargı anılan kararların/düzenlemelerin CBK'ya uygunluk denetimini nasıl yapacaktır? CBK'nın hiçbir esas, kriter ve ilke belirlemeden bir görevin alanını belirleme yetkisini idareye bırakması halinde söz konusu idari işlemlerin yargısal denetiminin etkili bir şekilde yapılması mümkün değildir.

23. Sonuç olarak dava konusu kural hiçbir çerçeve çizmeden, temel ilke, esas ve şartları belirlemeden Hazinesin Cumhurbaşkanı kararıyla yurtiçindeki ve dışındaki şirketlere iştirakine imkân sağladığı, bu konudaki düzenlemeyi (zımnen de olsa) diğer düzenleyici işlemlere bıraktığı için Anayasa'ya aykırılık teşkil etmektedir.

24. Açıklanan gerekçelerle, kuralın içerik yönünden Anayasa'nın 2. maddesine ve 106. maddesinin on birinci fıkrasına aykırı olduğunu ve iptal edilmesi gerektiğini düşündüğümden çoğunluğun red yönündeki kararına katılmıyorum.

Başkan

Zühtü ARSLAN

KARŞIOY GEREKÇESİ

İncelemeye konu "... ve Hazinesin Cumhurbaşkanı kararı ile yurtiçindeki ya da yurtdışındaki şirketlere iştirak etmesini sağlamak" ibaresinin iptal isteminin reddine yönelik çoğunluk kararına aşağıda belirtilen nedenlerle katılamadım.

Kuralda belirtilen iştirak kavramı ile iç hukuka veya yurt dışındaki ilgili hukuk düzeninin kurallarına göre kurulmuş herhangi tür ve nitelikteki bir ticari şirkete ortak olunması kastedilmektedir. Bakanlığa verilen görev ve yetkinin kapsamı bakımından bir sınırlama yapılmadığından, bütün ticaret şirketlerine iştirakin kastedildiği anlaşılmaktadır. Öte yandan incelenen kuralda idari mercie iştirak yetkisi verilmekle birlikte, şirket iştirakinin hangi konular veya faaliyet alanlarıyla ilgili olacağı, hangi

amaçlarla ve hangi sınırlar içerisinde iştirak yetkisi verildiği hususlarında hiçbir belirlemenin de yapılmadığı görülmektedir. Diğer taraftan bu sınırsız yetki, iştirak edilen şirketin borçları dolayısıyla pay sahiplerinin sorumlulukları bakımından da sorunlara neden olma riski taşımaktadır. İştirak edilen şirketin borçlarına karşı iştirak eden şirketin tüm malvarlığıyla mı yoksa payıyla sınırlı olarak mı sorumlu olacağı belirsizdir. Yurt içindeki şirketler yönünden bu belirsizliğin Ticaret Kanunu ve ilgili mevzuat yönünden giderileceği söylenebilir. Buna karşın yurt dışındaki şirketler yönünden aynı şey söylenemeyecektir. İştirak edilen şirketin tabi olduğu hukuk düzeni ve şirket hukukuna bağlı olarak sözü edilen sınırsız sorumluluk halinin gerçekleşmesi de olasıdır. Dolayısıyla verilen yetkinin kapsamı ve çerçevesini ihata etmeyen, belirlemeyen düzenlemenin Cumhurbaşkanlığı kararnamelerinin yürütme yetkisine ilişkin konularda çıkarılabileceğine ilişkin Anayasanın 104. maddesinin 17. fıkrasının 1. cümlesine aykırı olması nedeniyle iptal edilmesi gerektiği düşüncesindeyim.

Başkanvekili

Hasan Tahsin GÖKCAN

Karşı Oy

6/8/2019 tarih ve (43) numaralı Cumhurbaşkanlığı Kararnamesi'nin 14. maddesiyle (1) numaralı Cumhurbaşkanlığı Kararnamesi'ne eklenen 227/B maddesinin 4. fıkrasının "...hazine ve maliye başmüfettişleri, müfettişleri ve müfettiş yardımcılarının görev, yetki ve sorumlulukları ile ..." ibaresinin incelenmesinde, çoğunluk tarafından düzenlemenin Anayasa'nın 128. maddesi uyarınca münhasıran kanunla düzenlenmesi gereken bir konuda Cumhurbaşkanlığı Kararnamesi (CBK) ile düzenleme yapıldığı, bu düzenlemenin Anayasa'nın 104/1. maddesinin onyedinci fıkrasının üçüncü cümlesine aykırı olduğundan bahisle iptal kararı verilmiştir.

Anayasa'nın 106/son maddesi "Bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulması Cumhurbaşkanlığı kararnamesiyle düzenlenir." demek suretiyle bakanlıkların kurulması yanında görev ve yetkilerinin belirlenmesinde de CBK ile düzenleme yapılmasına imkân tanımaktadır.

İptal talebine konu edilen düzenleme Anayasa'nın 106/son maddesinin verdiği yetki çerçevesinde Hazine ve Maliye Bakanlığı'nın kuruluş ve teşkilatını düzenlemektedir. Bu kapsamda söz konusu Bakanlığın Teftiş Kurulu'nun Bakanlık teşkilatının bir parçası olduğunda tereddüt bulunmamaktadır.

Anayasa Mahkemesi, kadro düzenlemelerine ilişkin (2) nolu CBK.nın iptalinin talep edildiği 2018/119 esas sayılı dosyada verilen 11/06/2020 gün ve 2020/25 sayılı kararında, kadroların teşkilatın ayrılmaz bir parçası olduğu ve buna ilişkin düzenlemelerin de yürütme yetkisi kapsamında olup CBK ile yapılabileceğine hükmetmiştir (19. Prg.).

Bu bağlamda bakanlık dahilinde yer alacak birimlerin neler olduğunun belirlenmesi de teşkilat kurma işleminin doğal bir parçasını oluşturmaktadır.

Anayasa'nın 106/son maddesinde yer alan düzenleme sadece bakanlık teşkilatlarının kurulmasını değil aynı zamanda bakanlıkların görev ve yetkilerinin düzenlenmesine de olanak sağlamaktadır.

Anayasa'nın 123. maddesinin üçüncü fıkrasında kamu tüzel kişiliğinin kanunla veya CBK ile kurulacağı hükme bağlanmıştır. Anayasa Mahkemesinin 12/6/2020 tarihli ve E.2019/105, K.2020/30 sayılı kararında da belirtildiği üzere anılan fıkrada yer alan "...kurulur." ibaresinin CBK ile kurulan bir kamu tüzel kişiliğinin CBK ile düzenlenmesini de içerdiği anlaşılmaktadır (45. Prg.).

Bu noktada bir teşkilatı kurmaya yetkili olan iradenin aynı zamanda düzenlemeye de yetkili olduğunun kabulü gerekmektedir.

Aksinin kabulü, teşkilatın CBK ile kurulmasına rağmen teşkilat içerisindeki birimlerin görev ve yetkilerinin kanunla düzenlenmesi gibi ikili bir gerekliliğin ortaya çıkması ve buna bağlı olarak belirsizlik oluşturulması gibi hukuk devletinde kabulü mümkün olmayan bir tabloya neden olma sonucunu da doğuracaktır.

Anılan bu gerekçelerle çoğunluğun hükmün iptal yönündeki görüşüne iştirak edilmemiştir.

Başkanvekili - Kadir ÖZKAYA

Üye: Muammer TOPAL, Recai AKYEL, Yıldız SEFERİNOĞLU, Basri BAĞCI, İrfan FİDAN

KARŞIOY GEREKÇESİ

1. Dava konusu kural, Hazinesinin Cumhurbaşkanı kararı ile yurt içindeki ya da yurt dışındaki şirketlere iştirak etmesinin sağlanmasını düzenlemektedir. (43) numaralı Cumhurbaşkanlığı Kararnamesi (CBK) içinde yer alan kural konu bakımından yetki yönünden Anayasaya uygundur. İçerik açısından ise hukuk devleti ve yürütmenin yetkileri yönünden Anayasaya aykırılık taşımaktadır.

2. Anayasa'nın 2. maddesinde yer alan hukuk devletinin temel ilkelerinden biri belirliliktir. Mahkememizin yerleşik içtihadına göre belirlilik ilkesinin kapsamında yasal düzenlemelerin hem

kişiler hem de idare yönünden herhangi bir tereddüde ve şüpheye yer vermeyecek şekilde açık, net, anlaşılır, nesnel ve uygulanabilir olması ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu tedbirler içermesi de gereklidir. Bu ilke yürütmenin asli düzenleyici işlemi özelliğine sahip bulunan CBK'lar için de geçerlidir.

3. Hazinesin Cumhurbaşkanını kararı ile yurt içindeki ya da yurt dışındaki şirketlere iştirakinin hangi ölçütler çerçevesinde gerçekleştirileceğine dair dava konusu kuralda bir açıklama bulunmamaktadır. Kural, Cumhurbaşkanına kararı ile Hazinesin herhangi sınırlamaya veya nesnel ölçütlere tabi olmadan yurt içi ya da yurt dışındaki şirketlere iştirak etmesine olanak tanımaktadır. Bu çerçevede mesela hangi şirketlere, hangi amaçlarla iştirak edileceği, bu şirketlerin mali durumlarının, bilançolarının dikkate alınıp, alınmayacağı, faaliyet gösterdikleri sektörler bakımından kamu yararı yönünden bir değerlendirme yapıp yapılmayacağı ve benzeri hususlarda tam bir belirsizlik bulunmaktadır.

4. Kuralla sadece yurt içi değil, yurt dışındaki şirketlere de iştirak imkânı getirilmektedir. Bu düzenleme de ciddi belirsizlikler içermektedir. Örneğin, hangi kanun hükümlerinin geçerli olacağı, yabancı ülke hukukunun mu, ulusal mevzuatın mı, uluslararası tahkim hukukunun mu uygulanacağı, Hazinesin sorumluluğunun ne boyutlarda olacağı ve benzeri konularda bir açıklık bulunmamaktadır.

5. Dava konusu kuralla kapsam ve sınırları belirlenmeden, çerçevesi çizilmeden bir yetkinin Cumhurbaşkanına verilmesi Anayasa'nın 2. ve 8. maddelerine aykırı düşmektedir.

FARKLI GEREKÇE

(43) Numaralı CBK'da, Mali Suçlar Araştırma Kurulu Başkanlığına (MASAK) kamu kurum ve kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği olmayan kuruluşlardan her türlü bilgi ve belgeyi isteme yetkisi verilmiştir. Mahkememizin bu konudaki iptal kararına E.2018/134, K.2021/13, 03/03/2021 sayılı karardaki karşıoy yazımda belirttiği gerekçelerle katılıyorum. Kaldı ki bahse konu karardaki kural "...gerekli gördüğü bilgiler"le ilgiliyken, mevcut davadaki kural "her türlü bilgi ve belgeyi" kapsadığından kişisel veriler bakımından Anayasa'nın 2., 13. ve 20. maddelerine aykırıdır.

Üye

Engin YILDIRIM

KARŞIOY GEREKÇESİ VE FARKLI GEREKÇE

(1) numaralı Cumhurbaşkanlığı Kararnamesinin (CBK) 217. maddesinin (1) numaralı fıkrasının değişik (h) bendindeki "...ve Hazinesin Cumhurbaşkanını kararı ile yurtiçindeki ya da yurtdışındaki şirketlere iştirak etmesini sağlamak," ibaresinin Anayasaya aykırı olmadığına ve iptal talebinin reddine; 231. maddesinin (1) numaralı fıkrasının (m) bendinin ise Anayasaya aykırı olduğuna ve iptaline karar verilmiştir.

1. Red kararının gerekçesinde; belirlilik ilkesinin yalnızca yasal belirliliği değil, daha geniş anlamda hukukî belirliliği ifade ettiği, mahkeme içtihatları ve yürütmenin düzenleyici işlemleri ile de hukukî belirliliğin sağlanabileceği, asıl olanın muhtemel muhataplarının mevcut şartlar altında belirli bir işlemin ne tür sonuçlar doğurabileceğini öngörmelerini mümkün kılacak bir normun varlığı olduğu, incelenen hükme göre Hazinesin şirketlere iştirakinin özel hukuk hükümlerine uygun olarak gerçekleştirileceği, iştirakin kapsam ve mahiyetine ilişkin meselelerin kural olarak 6102 sayılı Türk Ticaret Kanunu ile şirketlerin tâbi olduğu özel kanunların hükümlerine, yurtdışındaki şirketlere ilişkin olarak ise ilgili ülkelerin hukukuna tâbi olacağı, Hazinesin şirketlere iştirak etmesi suretiyle gerçekleştirilecek iktisadî faaliyet sebebiyle gerekli işlemlerin yürütme organının hangi unsuruna yapılacağına da açık, anlaşılır ve uygulanabilir bir şekilde belirlenmesi sebebiyle dava konusu kuralda bu yönden de belirsizlik olmadığı, dolayısıyla hukuk devleti ilkesine aykırılık oluşturan bir yönünün bulunmadığı ifade edilerek red sonucuna ulaşılmıştır.

Dava konusu kural Hazine ve Maliye Bakanlığının görev ve yetkilerine ilişkin bir düzenleme öngördüğünden, Anayasanın 106. maddesinin son fıkrasına göre CBK ile düzenlenebilecek konular arasındadır. Yine, kuralın konu bakımından Anayasaya aykırı olmadığına ilişkin gerekçede ifade edildiği gibi, aynı konuda açık bir kanunî düzenleme de bulunmamaktadır. Dolayısıyla Hazinesin yurtiçindeki veya yurtdışındaki şirketlere doğrudan ortak olması, ilk defa bu CBK ile öngörülmektedir.

Bu itibarla, içerik yönünden yapılan incelemede, kuralın belirlilik ilkesine uygun olup olmadığı değerlendirilirken konu yönünden yapılan bu tespitlerin gözardı edilmemesi gerekir.

Önceki kararlarımızda ve red gerekçesinde belirtildiği üzere, belirlilik ilkesi yalnızca kanunî belirliliği değil, daha geniş anlamda hukukî belirliliği de ifade etmekte ve kanunî bir düzenlemeye dayanarak erişilebilir, bilinebilir ve öngörülebilir olma gibi nitelikleri taşıması şartıyla mahkeme içtihatları ve yürütmenin düzenleyici işlemleri ile hukukî belirlilik sağlanabilmektedir. Anayasaya uygunluk denetiminde kanunlar bakımından kabul edilen ve CBK'lar için de geçerli olduğunda şüphe bulunmayan bu ilkeye uygun bir düzenleme yapıp yapılmadığının belirlenmesinde esas olan ise,

muhtemel muhataplarının -yani düzenleyici işlemin dayanağını oluşturan hükme dayanarak düzenleyici işlemi tesis edecek idarenin, bu düzenlemeden etkilenen kişilerin ve düzenleyici işlemlerin yargısal denetimini yapacak mahkemelerin- mevcut şartlar altında belirli bir işlemin ne tür sonuçlar doğurabileceğini öngörmelerini mümkün kılacak ve onlara yol gösterecek nitelikte bir normun varlığıdır.

Başka bir anlatımla, hukukî belirlilik ilkesine uygun bir düzenlemeden söz edilebilmesi için, öncelikle mahkeme içtihatları ile yürütmenin düzenleyici işlemlerinin dayanacağı kanun ve CBK hükümlerinin belirlilik ilkesine uygun olması zorunludur.

Bilindiği gibi, Anayasanın 2. maddesinde öngörülen hukuk devletinin temel unsurlarından biri olan belirlilik ilkesi, kanunî düzenlemelerin hem kişiler hem de idare yönünden herhangi bir tereddüte ve şüpheye yer bırakmayacak şekilde açık, net, anlaşılır, nesnel ve sınırlarının belirli olmasını, ayrıca keyfiliğe yol açmayacak bir içeriğinin bulunmasını gerektirmekte; hukukî güvenlik ilkesiyle bağlantılı olarak da normların öngörülebilir olmasını ve kanunda (veya CBK'da) belirli bir kesinlik içinde hangi somut olgulara hangi sonuçların bağlandığının görülebilmesini zorunlu kılmaktadır. Bu ilke yasama organının, CBK'lar yönünden ise Cumhurbaşkanının takdir yetkisini hukuk devleti ilkesine uygun şekilde, anayasal sınırlar içinde kullanıp kullanmadığının belirlenmesi bakımından da önem taşımaktadır (geniş açıklama için bkz. 3/6/2021 tarihli ve E.2020/9, K.2021/37 sayılı karara ilişkin karşıoy gerekçem).

Bu ilke uyarınca kanun ve CBK hükümleri, yukarıda belirtildiği gibi ilgililerin bir işlem veya fiilin belirli şartlarda ne tür sonuçlar doğurabileceğini makul bir düzeyde öngörmelerini mümkün kılacak ve kamu otoritelerinin keyfî uygulamalarına imkân tanımayacak şekilde düzenlenmeli ve idareye verilen takdir yetkisinin kapsamı ve uygulama usulü açık olarak belirlenmelidir.

Yukarıda belirtilen karşıoy gerekçemde de ifade edildiği üzere, kanunî düzenlemelerde veya CBK hükümlerinde, mezkûr ilkelere ilişkin şartların aranması, bu ilkelere uygun bir düzenleme yapılmadığı takdirde bunlara dayanılarak mutlaka keyfî ikincil düzenlemeler yapılacağı anlamına gelmediği gibi kanun veya CBK hükmündeki belirsizlik hukukî güvenlik ilkesiyle bağdaşmayan sonuçlar da doğurmayabilir. Ancak Anayasanın 2. maddesinde öngörülen hukuk devleti ilkesinin gereği olan bu ilkeler, Anayasaya uygunluk denetiminde, uygulamadan ve kanunun veya CBK'nın verdiği yetkiye dayanılarak yapılan düzenleyici idarî işlemlerden bağımsız olarak, sadece kanun ve CBK hükmü üzerinden değerlendirilir ve bu değerlendirmeye göre mezkûr düzenleyici işlemlerin dayanacağı, muhataplarınca öngörülebilir bir normun bulunup bulunmadığı tespit edilir.

Diğer taraftan, kanunla veya CBK ile düzenleme, konuya ilişkin bütün ayrıntılara kanunda veya CBK'da yer verilmesini gerektirmemekte; ancak bu düzenlemelerin belli bir ölçüde soyutluk içermesi kaçınılmaz olsa da, yapılan düzenlemede bir konudan sadece kavramsal veya kurumsal olarak bahsedilmesi belirlilik ilkesi bakımından yeterli bulunmamaktadır.

Hazinenin yurtiçindeki veya yurtdışındaki şirketlere doğrudan iştirak etmesi daha önce mümkün değilken, ilgili hükme dava konusu ibare eklenerek Hazine ve Maliye Bakanlığının görev ve yetkileri arasına bunu sağlamak da dahil edilmiş; ayrıca, dava konusu edilmemekle birlikte aynı yönde bir hükme Bakanlığın ilgili Genel Müdürlüğünün görev ve yetkileri arasında da yer verilmiştir.

Çoğunluğun red gerekçesinde de, kuralda geçen iştirak kavramının ortaklık, paydaşlık, katılma anlamına geldiği, Hazinenin yurtiçindeki veya yurtdışındaki şirketlere iştirakinin şirkette pay sahipliği şeklinde olacağı, dava konusu kuralın 233 sayılı KHK'nın 27. maddesindeki KİT'ler ve bağlı ortaklıklarının anonim şirketlere iştirakine ilişkin düzenlemeye benzer şekilde, ancak şirket türlerine ve Hazinenin ortaklık oranına göre bir sınırlama öngörülmeden, teşebbüs ve bağlı ortaklıklarının aracılığı da olmadan, iştirak edilecek şirketlerde Hazinenin dolaylı pay sahipliği yerine doğrudan pay sahipliğine imkân sağlanması amacıyla getirildiği belirtilmiştir.

Hazinenin, teşebbüsler ile bağlı ortaklıkların iştirak edebilecekleri şirketlerin türleri ile iştirakte sahip olabilecekleri hisse oranları da dahil olmak üzere 233 sayılı KHK'da öngörülen sınırlamalara tâbi olmadan şirketlere doğrudan iştirak edebilmesini sağlamak şeklinde ifade edilen bu düzenleme amacı bile -tek başına- anılan hükümlerle yapılan düzenlemenin belirlilik ilkesine uygun olmadığını ortaya koymaktadır.

Yukarıda belirtildiği gibi, Hazinenin 233 sayılı KHK'daki ve ilgili diğer kanunlardaki sınırlamalara bağlı olmadan şirketlere doğrudan iştirak edebilmesi öngörülürken (ve düzenlemenin amacı da kararın gerekçesinde bu şekilde açıklanırken), dava konusu ibarede veya bu ibarenin eklendiği bentte ya da fıkrada yahut CBK'nın başka hükümlerinde ve diğer kanunlarda bu konuya ilişkin hiçbir esas belirlenmemiş, başka mevzuatta yer alan esaslara da atıf yapılmamıştır.

Düzenlemenin söz konusu amacı da dikkate alındığında, 233 sayılı KHK hükümlerinin bu konuda uygulanması mümkün olmadığı gibi -anılan KHK'dakine benzer şekilde- mesela ortak olunacak şirketlerin türü, bunların sermayelerinde Hazinenin sahip olacağı hisse oranı, Hazine hisselerinin korunması için uygulanacak ilkeler ve bu şirketlerde Hazinenin temsili konularında bir kural öngörülmemiş veya herhangi bir kanun hükmünün uygulanacağı da belirtilmemiştir. Aynı sebeple söz konusu iştirak sebebiyle Hazinenin ortaya çıkacak sorumluluğunun kapsamı ve niteliği de belirsiz hâle gelmiştir.

Dava konusu hükme dayanarak Hazinesinin şirketlere iştirak etmesi kamu kaynaklarından bu şirketlere sermaye aktarılmasını, dolayısıyla kamu kaynaklarının kullanılmasını gerektirdiğinden, yukarıda belirtilen hususların belirlenmesi; özellikle kamu menfaatinin korunabilmesi bakımından bu şirketlerdeki kamu payının izlenmesi ve iştirak edilecek şirketlerin faaliyetlerinin değil ama bu hisselerin kullanılmasının denetlenmesi anayasal önem taşımaktadır.

Çoğunluğun red gerekçesinde kuralın anlam ve kapsamı belirlenirken, 6102 sayılı Türk Ticaret Kanununun (TTK) şirketlerle ilgili hükümleri aktararak, incelenen kural kapsamında mesela Hazinesinin iştirak edeceği şirketlerin anonim şirketlerle sınırlandırılmadığı, kollektif şirketler ile komandit şirketlerdeki sınırsız sorumlu gerçek kişi ortaklar dışında komandit şirketleri de kapsayacak şekilde anılan Kanunda belirtilen şirket türlerine iştirakin mümkün olabileceği belirtilmiştir. İncelenen kurala göre Hazinesinin iştirak edebileceği şirketlerin anonim şirketlerle sınırlı olmadığı yönündeki tespit isabetli olmakla birlikte, bu şirketleri 6102 sayılı Kanunda düzenlenen şirketlerle sınırlayan değerlendirmelere katılmak da mümkün değildir. İncelenen kuralın açık lâfzı Hazinesinin, iki veya daha fazla gerçek veya tüzel kişinin oluşturduğu adî şirketlere 6098 sayılı Türk Borçlar Kanununun 632. maddesine göre iştirak etmesine de imkân verecek genişliktedir.

Yine red gerekçesinde, “iştirakin kapsam ve mahiyetine ilişkin meselelerin kural olarak genel kanun niteliğindeki 6102 sayılı Kanuna ...tâbi olacağı açıktır” denilmekte ise de, 233 sayılı KHK’da olduğu gibi CBK’ya konulabilecek “genel hükümlere tâbi olmak kaydıyla” şeklinde bir hüküm olmadan yapılan bu tespit dava konusu kuralın lâfzı ile de, yukarıda aktarılan getiriliş amacıyla da bağdaşmamaktadır.

Kaldı ki TTK hükümlerine tâbi olacağı açık olan, incelenen hükme dayanılarak Hazinesinin iştirak edeceği, anılan Kanunda düzenlenen şirketlerdir. Bu hükme dayanılarak adî şirketlere de iştirak edilmesi mümkündür ve bu şirketler Türk Borçlar Kanununa tâbidir.

Buna karşılık, iştirakin kapsam ve mahiyeti konusunda; başka bir ifadeyle, Hazinesinin bu şirketlere iştirak etmesinin usul ve esasları, şartları, ortaklıktaki kamu payının izlenmesi, korunması ve kullanılmasının denetlenmesi gibi konularda anılan kanunların hükümlerinde de, bu düzenlemede de belirsizlik bulunmaktadır.

Başka bir ifadeyle, dava konusu kuralla iştirak edilmesine imkân sağlanan yurtiçindeki şirketlerin genel hükümlere; yurtdışındaki şirketlerin de kendi ulusal mevzuatına göre özel hukuk rejimine tâbi olacağı ve bu kurallara uygun olarak faaliyette bulunmaları gerektiği hususunda tereddüt bulunmamakla birlikte -yukarıda belirtildiği üzere- Hazine ve Maliye Bakanlığının Hazinesinin bu şirketlere iştirak etmesini sağlama yetkisini hangi şartlarla kullanacağı ve iştirak edilen şirketteki

Hazine hisselerinin nasıl korunacağı konusunda, yani iştirak edilen şirketin değil, Hazinesinin tâbi olacağı usul ve esaslar yönünden açık, net, anlaşılır ve öngörülebilir bir düzenleme bulunmadığı görülmektedir. İştirakin Cumhurbaşkanı kararı ile yapılmasını öngören CBK hükmünde, hukukî belirliliğin temel şartı olan bu niteliklerde bir dayanak oluşturacak kriterler öngörülmediği gibi buna ilişkin usul ve esasların Cumhurbaşkanı kararı ile belirleneceğine ilişkin genel bir ifadeye de yer verilmemiştir.

Mahkememizin birçok kararında, hiçbir usul ve esas öngörülmeden konunun alt düzenleyici işlemlerle düzenleneceğini belirten genel nitelikli yetkilendirme hükümlerinin bile yasama yetkisinin devredilmezliği ilkesi yanında belirlilik ilkesine aykırı bulunduğu dikkate alındığında böyle bir hükme de yer verilmeden idarenin diğer düzenleyici işlemleri ile hukukî belirliliğin sağlanabileceğinin kabul edilmesi belirlilik ilkesine ilişkin içtihadımızla çelişmektedir.

Diğer taraftan, (1) numaralı CBK'nın 224. maddesinin, ilgili birimin görev ve yetkilerinin düzenlendiği (1) numaralı fıkrasının (a) bendinin de değiştirilerek kamu iktisadî teşebbüsleri yanında "Hazinesinin iştirak ettiği şirketler ile ilgili olarak" Genel Müdürlüğe Hazine pay sahipliğinin gerektirdiği her türlü işlemi yapma görev ve yetkisinin verildiği, buna göre iştirak edilen şirketlerle ilgili olarak her türlü işlemin yapılabileceği savunulabilirse de, sadece ilgili birimin görev ve yetkilerini belirleyen böyle bir hükmün, kanunda veya CBK'da -233 sayılı KHK'da olduğu gibi mesela iştirak edilen şirketin türü, bunların sermayelerinde Hazinesinin sahip olabileceği hisse oranı, iştirak edilen şirketin yönetiminde Hazine payının kaç üye ile temsil edileceği veya Hazine hisselerinin korunması için neler yapılacağı konularında usul ve esaslar belirlenmeden gerekli belirliliği sağladığı söylenemez.

Kısaca, incelenen kuralda veya CBK'nın başka hükümlerinde yahut diğer kanunlarda konunun temel esasları herhangi bir tereddüte yer vermeyecek şekilde ve belli bir kesinlik içinde açık, net, anlaşılır ve nesnel olarak düzenlenmeden idareye çok geniş ve ölçsüz bir takdir alanı bırakılmıştır. Bu nedenle düzenleme, yorum ve değerlendirme farklılıklarına bağlı olarak keyfî uygulamalara yol açabilecek, başka bir ifadeyle belirlilik ve öngörülebilirlik ilkelerine aykırılık oluşturacak niteliktedir.

Diğer taraftan, belirlilik ilkesi, yargısal denetimde gözönünde bulundurulacak kriterlerin de belirlenmiş olmasını gerektirdiğinden bu ilkeye uyulmadan yapılan kanunî düzenlemeler, idareye esnek davranabileceği bir alan sağlamasına karşılık belirlilik ilkesinin temel amaçlarından birini oluşturan yargısal denetimi imkânsız hâle getirir ve aslında bunlara dayanılarak yapılacak idarî tasarruflar üzerinde idarî yargı mercilerince etkin bir yargısal denetim gerçekleştirilmesini, böylece hukukî belirliliği sağlayacak mahkeme içtihatlarının oluşmasını da engeller.

İncelenen kuralla Hazinesinin şirketlere iştirak etmesi konusunda ilkeleri, sınırları ve şartları belirlenmemiş genişlikte bir takdir yetkisi tanındığı dikkate alındığında, söz konusu yargı denetiminin etkili bir şekilde yapılması da, hukukî belirliliği sağlayabilecek mahkeme içtihatlarının ortaya çıkması da mümkün değildir.

Bu sebeplerle, dava konusu ibarenin Anayasanın 2. maddesine aykırı olduğu ve iptal edilmesi gerektiği düşüncesiyle çoğunluğun red kararına karşıyım.

2. Çoğunluğun, CBK'nın 231. maddesinin (1) numaralı fıkrasının (m) bendinin iptaline ilişkin gerekçesinde ise; Mahkememizin daha önceki iki kararına konu olan düzenlemelerden farklı olarak dava konusu kuralda, idareye görevleriyle ilgili olma şartı aranmadan her türlü bilgi ve belgeyi isteme yetkisinin verildiği, bu yönüyle kuralın yalnızca teşkilatlanma ile kurumsal yapı ve işleyişin düzenlenmesinden ibaret olduğunun söylenemeyeceği ve bazı faaliyetler kapsamında istenecek bilgi ve belgelerin doğrudan kişisel verilere ilişkin bulunduğu açık olduğu belirtilerek CBK ile düzenlenemeyecek yasak alan içinde bir düzenleme öngören kuralın Anayasanın 104. maddesinin onyedinci fıkrasının ikinci cümlesine aykırı olduğu sonucuna varılmıştır.

Kararda da belirtildiği üzere Mahkememiz, İletişim Başkanlığı ile Strateji ve Bütçe Başkanlığının görevleriyle ilgili olarak gerekli gördükleri bilgileri isteyebilmelerine ilişkin CBK kurallarının, CBK ile belirlenen görevlerin yerine getirilmesinin doğal ve zorunlu bir sonucu olduğu, anılan kuralların idarenin teşkilatlanması kapsamında bilgi ve belge istemeyi düzenlediği, kişisel verilere ilişkin her türlü işlemin 6698 sayılı Kanuna ve konuyla ilgili diğer kanunî düzenlemelere uygun olarak gerçekleştirileceğinin açık olduğu ve kişisel verilere ilişkin düzenleme içermediği, kişisel verilerle de ilgili bulunmadığı gerekçesiyle Anayasaya aykırı olmadığına karar vermiştir (3/3/2021 tarihli ve E.2018/134, K.2021/13 sayılı; 13/10/2021 tarihli ve E.2018/133, K.2021/70 sayılı kararlar).

Anılan kararlara konu olan kuralların da Anayasaya aykırı olduğu düşüncesiyle yazdığım karşıoy gerekçelerimde belirtildiği üzere, çoğunluğun red gerekçesinde yapılan bu değerlendirmelere katılmak mümkün değildir.

Anayasanın 104. maddesinin onyedinci fıkrasının ikinci cümlesinde CBK'lar bakımından belirlenen yasak alanın Anayasanın İkinci Kısmının "Kişinin Hakları ve Ödevleri" başlıklı İkinci Bölümünde yer alan 20. maddesindeki hakla ilgili -sınırlama getirmeyen- düzenlemeleri de kapsadığı ve incelenen bu kural gibi mezkûr kararların konusu olan kuralların da kişisel verilerle ilgili düzenlemeler içermesi sebebiyle, konu yönünden Anayasanın 104. maddesinin onyedinci fıkrasının ikinci cümlesindeki düzenleme yasağı kapsamında kaldığı açıktır.

Anayasanın 106. maddesinin son fıkrasında bakanlıkların kuruluş, görev ve yetkileriyle ilgili olarak öngörülen CBK ile düzenleme yetkisi, 104. maddenin onyedinci fıkrasının ikinci cümlesindeki yasak alanın bakanlıklarla ilgili CBK'lar için geçerli olmadığı şeklinde yorumlanamaz.

Aksinin kabulü, Anayasanın İkinci Kısımının Birinci ve İkinci Bölümlerinde yer alan bütün temel haklar, kişi hakları ve ödevleriyle Dördüncü Bölümündeki siyasî haklar ve ödevlerin bakanlıkların görev ve yetkilerine ilişkin CBK'larla düzenlenebileceği şeklinde bir yoruma götürür ki böyle bir yorumun Anayasanın 104. maddesinin onyedinci fıkrasının ikinci cümlesiyle getirilen yasak alanı ve temel haklarla ilgili güvenceyi tamamen anlamsız hâle getireceği tartışmasızdır.

Bu sebeplerle, bakanlıklar ile diğer kamu kurum ve kuruluşlarının görevlerinin yerine getirilebilmesinin doğal ve zorunlu bir sonucu olarak kişisel verilerin toplanmasına imkân veren düzenlemelerin CBK ile yapılabileceğine ilişkin çoğunluk gerekçesine katılmamakla birlikte, iptal sonucuna bu düşüncelerle ve Mahkememizin yukarıda belirtilen iki kararına ilişkin karşıoy gerekçelerimde yapılan açıklamalar çerçevesinde farklı gerekçeyle katılıyorum.

Üye

M. Emin KUZ

KARŞIOY GEREKÇESİ ve FARKLI GEREKÇE

1. Anayasa Mahkemesi çoğunluğunun 6/8/2019 tarihli ve (43) numaralı Bazı Cumhurbaşkanlığı Kararnamelerinde Değişiklik Yapılması Hakkında Cumhurbaşkanlığı Kararnamesi'nin 1. maddesiyle 10/7/2018 tarihli ve 30474 sayılı Resmi Gazete'de yayımlanan (1) numaralı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin 217. maddesinin (1) numaralı fıkrasının (ğ) bendine [17/4/2020 tarihli ve (60) numaralı CBK'nın 1. maddesiyle 217. maddede yapılan değişiklikten sonra (h) bendi] eklenen "...ve Hazinesinin Cumhurbaşkanlığı kararı ile yurtiçindeki ya da yurtdışındaki şirketlere iştirak etmesini sağlamak" ibaresindeki "ya da yurtdışındaki" ifadesinin içeriği itibariyle Anayasa'ya aykırı olmadığından iptal isteminin reddine ilişkin kararına katılmamaktayım.

2. Öte yandan aynı Cumhurbaşkanlığı Kararnamesinin 17. maddesiyle (1) numaralı Cumhurbaşkanlığı Kararnamesi'nin değiştirilen 231. maddesinin (1) numaralı fıkrasının (m) bendinin konu bakımından yetki yönüyle Anayasa'ya aykırı olduğunu ilişkin kanaate ise farklı gerekçe ile katılmamaktayım.

3. Bu konulara ilişkin gerekçelerim şu şekildedir:

4. İptali talep edilen "...ve Hazinesinin Cumhurbaşkanı kararı ile yurtiçindeki ya da yurtdışındaki şirketlere iştirak etmesini sağlamak" ibaresi 6/8/2019 tarihli ve (43) numaralı Bazı Cumhurbaşkanlığı Kararnamelerinde Değişiklik Yapılması Hakkında Cumhurbaşkanlığı Kararnamesi'nin 1. maddesiyle Hazine ve Maliye Bakanlığının görev ve yetkileri arasına eklenmiştir. Mahkememiz çoğunluğu dava konusu ibarenin içerik yönüyle Anayasa'ya aykırı olmadığına karar vermiş ise de kanaatimizce ibaredeki "yurtdışındaki şirketlere iştirak etmesini sağlamak" şeklindeki kısım Anayasa'ya aykırıdır. Bu nedenle de dava konusu ibaredeki "ya da yurtdışındaki" kısmının iptali gerekmektedir.

5. Dava konusu ibareyle Hazine ve Maliye Bakanlığının görev ve yetkileri arasına Hazinesinin Cumhurbaşkanı kararı ile yurtiçindeki ya da yurtdışındaki şirketlere iştirak etmesini sağlamak eklenmiş ise de bu kuralda özellikle Hazinesinin yurtdışındaki ticari şirketlere hangi şartlar dahilinde katılacağı hususunda bir belirleme mevcut değildir.

6. Elbette ki küreselleşen dünyada Türkiye Cumhuriyeti Devletinin Hazine aracılığı ile aynı zamanda yurtdışındaki şirketlere iştirak edebilmesi mümkün olmalıdır. Hatta bu biçimdeki etkinlikler ülke menfaati açısından fevkalade gerekli de görülebilir. Ancak dava konusu kuralda denetlenen hususun bununla bir ilgisi olmadığını öncelikle ifade etmek gerekir.

7. Dava konusu kuralın içerik yönüyle Anayasa'ya uygunluk denetiminde asıl sorunlu nokta Hazinesinin yurtdışındaki şirketlere iştirak etmesi noktasında belirlenmiş bir hukuki çerçeve olmamasından kaynaklanmaktadır. Zira ne dava konusu Cumhurbaşkanlığı Kararnamesinde ne de diğer Cumhurbaşkanlığı kararnameleri ve kanunlarda Hazinesinin yurtdışındaki şirketlere hangi şartlar dahilinde katılabileceğine dair bir çerçeve belirlenmiş ve bu konuya ilişkin usul ve esaslara yer verilmiştir.

8. Nitekim Anayasa Mahkemesinin belirlediği şu standart bu bağlamda dava konusu ibarenin Anayasa'ya uygunluk denetiminde fevkalade önem arz etmektedir:

"Anayasa'nın 2. maddesinde, Türkiye Cumhuriyeti, bir hukuk devleti olarak nitelendirilmiştir. Hukuk devletinin temel unsurlarından biri de 'belirlilik' ilkesidir. Bu ilkeye göre, yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi gerekir" (E.2015/41, K.2017/98, 04/05/2017, Ş 153).

9. Hazinesinin yurtiçindeki şirketlere katılması konusunda ticaret hukuku ile ilgili yasal mevzuatta konuya ilişkin çerçeve ve katılmanın usul ve esasları belirlenmiş durumdadır. Bu yönü ile şirketlere

iştirak durumunda ortaklıktan kaynaklanan sorumluluk başta olmak üzere pek çok konu 6102 sayılı Türk Ticaret Kanunu başta olmak üzere bu konu ile ilgili kanunlarda belirlenmiştir. Dolayısıyla dava konusu ibaredeki yurtiçindeki şirketlere iştirak konusunda bir belirsizlik veya yasal çerçevenin çizilmemesi gibi bir durumdan bahsedilemeyeceği söylenebilir.

10. Ancak aynı tespiti yurtdışındaki şirketlere iştirak etme boyutu ile yapabilmek mümkün değildir. Zira yurtdışındaki şirketlere iştirak etme durumunda gerek dava konusu Cumhurbaşkanlığı Kararnamesinde ve gerekse diğer Cumhurbaşkanlığı kararnameleri ve kanunlarda bir düzenleme bulunmamaktadır. Bu konularla ilgili kuralların bulunmaması Hazinesin yurtdışındaki şirketlere iştirak etmesi durumunda bunlarla ilgili ortaya çıkabilecek yetki, sorumluluk ve benzeri oldukça önemli konularda belirsizliği ortaya çıkarmaktadır. Bu belirsizliğin Hazinesin katılımının sağlanması, yurtdışındaki şirketlerdeki katılımdan kaynaklı sorumluluğu ve benzeri konular bağlamında uygulamada önemli sorunlara sebebiyet vermesi de mümkündür.

11. Dolayısıyla ve Hazinesin Cumhurbaşkanı kararı ile yurtdışındaki şirketlere iştirak etmesini sağlamak şeklindeki bir faaliyetin hangi usul ve esaslar dahilinde yapılabileceği, bu faaliyetin temel hukuki çerçevesi, kapsam ve sınırları ana hatları ile belirlenmiş olmadığından iptali talep edilen ibarenin “ya da yurtdışındaki” kısmının Anayasa’nın 2. maddesine aykırı olduğu açıktır.

12. Yukarıda sıralanan gerekçelerle Hazinesin yurtdışındaki şirketlere iştirak etmesine imkan sağlayan Cumhurbaşkanlığı Kararnamesindeki “ya da yurtdışındaki” ibaresi belirlilik koşulunu sağlamadığından içerik yönüyle Anayasa’nın 2. maddesine aykırı olup iptali gerektiği kanaatinde olduğumdan çoğunluğun aksi yöndeki kararına katılmamaktayım.

13. Öte yandan, aynı Cumhurbaşkanlığı Kararnamesi’nin 17. maddesiyle (1) numaralı Cumhurbaşkanlığı Kararnamesi’nin değiştirilen 231. maddesinin (1) numaralı fıkrasının (m) bendinde MASAK Başkanlığına “Kamu kurum ve kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği olmayan kuruluşlardan her türlü bilgi ve belgeyi istemek” yetkisi de verilmiştir. Mahkememiz çoğunluğu kuraldaki MASAK’ın görev ve yetkileri arasında açıkça sayılmış olanlar arasında sadece veri toplamak görev ve yetkisi bağlamında suç gelirlerinin aklanması, terörizmin finansmanının önlenmesi ile mali suçların araştırılması gibi konularda yürütülen faaliyetler kapsamında istenecek bilgi ve belgelerin doğrudan kişisel verilere ilişkin bulunduğu (§ 78) gerekçesiyle iptal sonucuna ulaşılmıştır.

14. Oysa kanaatimizce dava konusu kuraldaki kamu kurum ve kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği olmayan kuruluşlardan istenecek her türlü bilgi ve belge kişisel verilerle ilgili olabileceği gerekçesiyle Anayasa’nın 20. maddesi kapsamına girebileceğinden buradaki durum çoğunluk

gerekçesinde zikredilen Mahkememizin 3/3/2021 tarihli E.2018/134, K.2021/13 ve 13/10/2021 tarihli ve E.2018/133, K.2021/70 sayılı kararlarındaki dava konusu olan “gerekli gördüğü bilgileri” ibaresindeki bilgi ve belgelerden farklı değildir. Dolayısıyla Anayasa'nın 104. maddesinin on yedinci fıkrasının ikinci cümlesi dikkate alındığında bu konuların Cumhurbaşkanlığı Kararnamesi ile düzenlenmesi mümkün olmadığından çoğunluğun iptal kararına bu farklı gerekçe ile katılmaktayım.

Üye

Yusuf Şevki HAKYEMEZ

**Anayasa Mahkemesi - 7068 sayılı Genel Kolluk Disiplin Hükümleri Hakkında Kanun
Hükmünde Kararnamenin Kabul Edilmesine Dair Kanun Kararı (E. 2020/77)**

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2020/77

Karar Sayısı: 2021/93

Karar Tarihi: 16/12/2021

R.G.Tarih-Sayısı: 22/3/2022-31786

İTİRAZ YOLUNA BAŞVURAN: Mardin 2. İdare Mahkemesi

İTİRAZIN KONUSU: 31/1/2018 tarihli ve 7068 sayılı Genel Kolluk Disiplin Hükümleri Hakkında Kanun Hükmünde Kararnamenin Kabul Edilmesine Dair Kanun'un 8. maddesinin (6) numaralı fıkrasının (aa) bendinde yer alan "...sorgulama yapmak..." ibaresinin Anayasa'nın 2. maddesine aykırılığı ileri sürülerek iptaline karar verilmesi talebidir.

OLAY: Davacı hakkında, yetkili olmadığı hâlde elektronik ortamda kişisel verilerle ilgili sorgulama yaptığı gerekçesiyle verilen meslekten çıkarma cezasının iptali talebiyle açılan davada itiraz konusu kuralın Anayasa'ya aykırı olduğu kanısına varan Mahkeme, iptali için başvurmuştur.

I. İPTALİ İSTENEN KANUN HÜKMÜ

Kanun'un 8. maddesinin itiraz konusu kuralın da yer aldığı (6) numaralı fıkrası şöyledir:

"(6) Meslekten çıkarma cezasını gerektiren fiiller şunlardır:

- a) Görevin yerine getirilmesinde dil, ırk, cinsiyet, siyasi düşünce, felsefi inanç, din ve mezhep ayrımı yapmak veya personel arasında bu yolda ayırım yapıcı tutum ve davranışlarda bulunmak.
- b) Göreve çıkılmaması için propaganda yapmak, kışkırtmak, zorlamak, karar alınmasını sağlamak, alınan bu karara katılmak veya karar uyarınca göreve çıkmamak.
- c) Amir ya da üstlerinin icraatına karşı çıkmak ve bu hareketi toplu hale dönüştürerek görev yapılmasını ya da göreve çıkılmasını engellemek, buna katılmak, katılmaya tahrik ya da teşvik etmek.
- ç) Yetkisini veya nüfuzunu kendisine veya başkalarına çıkar sağlamak amacıyla ya da kin ve dostluk gibi nedenlerle kötüye kullanmak.

- d) Hizmetle ilgili her türlü dosya, kayıt, resmi evrak veya belgeyi ya da örneklerini yetkisiz kişilere vermek, verilmesini emretmek, verilmesine göz yummak.
- e) Gizli tutulması zorunlu olan ve görev ile ilgili bulunan bilgi ve belgeleri görevli veya yetkili olmayan kişilere açıklamak.
- f) Muhafazası veya sevkiyle görevli olduğu şüpheli, sanık, tutuklu veya hükümlünün kaçmasına bilerek ve isteyerek imkân vermek.
- g) Bilerek ve isteyerek suç kanıtlarını yok etmek veya bunların yok olmasına neden olmak, kanıtları silmek, gizlemek, değiştirmek, bozmak veya bu fiillere yardımcı olmak.
- ğ) Devlet malı araç, gereç, hayvan, silah, mermi ve mühimmatı satmak veya mal edinmek, personel kimlik kartını, araç, gereç, hayvan, silah ve mühimmatı başkalarının kullanımına vermek.
- h) Kasıtlı olarak gerçek dışı rapor vermek veya tutanak düzenleyip imza etmek veya ettirmek.
- ı) Görev sırasında yardım isteyen güvenlik görevlilerine haklı bir neden yokken yardımdan kaçınmak veya bildiği ya da gördüğü bir suçun izlenmesi ve suçlunun yakalanması için gerekli girişimde bulunmamak.
- i) Mesleğin saygınlığını zedeleyecek şekilde uygunsuz yerlere gitmek.
- j) Görev mahallinde veya görevli bulunduğu sırada alkollü içki içmek veya içilmesine göz yummak.
- k) Göreve sarhoş veya alkollü içki içtiği belli olacak biçimde gelmek.
- l) Resmi kıyafetle umuma açık yerlerde alkollü içki içmek veya resmi kıyafetli olarak gizlenemeyecek derecede sarhoş görünmek.
- m) Uyuşturucu maddeleri yapmak veya kullanmak, bunların yapılmasına, kullanılmasına, saklanmasına, nakledilmesine, yakalanacağı sırada ortadan kaldırılmasına, satılmasına veya satın alınmasına aracı olmak, kullanılmasını kolaylaştırmak ya da özendirmek.
- n) Kumar oynamak veya oynatmak, kumar oynatanlarla ilişki kurmak.
- o) Kaçakçılık yapmak veya kaçakçılarla ilişki kurmak.
- ö) Geliri ile uygun sayılmayacak biçimde yaşadığı ve aşırı harcamada bulunduğu kanıtlanmış olmak ve bunun haklı kaynağını gösterememek.
- p) 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu ile öngörülen grev yasağı kapsamına giren eylemlerde bulunmak.

- r) Devlet memurları tarafından yapılamayacağı 657 sayılı Kanunda belirtilen kazanç getirici faaliyetlerde bulunmak.
- s) Siyasi partilerin yararına veya zararına çalışmak ya da siyasal eylemlerde bulunmak, görevli olmaksızın siyasal amaçla yapılacak açık veya kapalı yer toplantılarına ya da gösteri yürüyüşlerine katılmak.
- ş) İffetsizliği bilinen veya anlaşılmış olan bir kimse ile bilerek evlenmek ya da evlilik bağını devam ettirmek veya böyle bir kimseyi yanında bulundurmamak ya da nikahsız olarak devamlı surette yaşamakta ısrar etmek.
- t) Kanuna aykırı olarak sendikalara üye olmak, sendikaların veya üyesi bulunmadıkları derneklerin yapacakları bilimsel, kültürel ve teknik nitelik taşımayan açık veya kapalı yer toplantılarına ya da gösteri yürüyüşlerine görevli olmaksızın katılmak, açık yer toplantı ve gösteri yürüyüşlerine resmi kıyafetli veya silahlı olarak katılmak ya da üyesi buldukları derneklerin tüzüklerinde belirtilen amaçları dışındaki çalışmalarını veya bu nitelikteki toplantı ya da gösteri yürüyüşlerini düzenlemek veya bunlara katılmak.
- u) Görevde kullanılan telsiz, telefon haberleşmesini veya kurum içi iletişim sistemlerini kasıtlı olarak engellemek.
- ü) Mesleğin onur ve saygınlığını zedeleyici veya amir ya da üstlerinin eylem ve işlemlerini olumsuz yönde eleştirici nitelikte tek başına veya topluca bildiri dağıtmak ya da basın, haber ajansları, radyo ve televizyon kurumları ve diğer iletişim kanalları vasıtasıyla kamuoyuna yönelik bilgi, yazı ve demeç vermek.
- v) Amir ya da üste karşı itaatsizliğe, mukavemete ya da fiilen taarruza tahrik ya da teşvik etmek.
- y) Menşei belli olmayan, bulundurulması ve taşınması yasak olan her çeşit silah, mühimmat ve benzerlerini bulundurmamak.
- z) Hukuka aykırı olarak kişiler arasındaki haberleşmenin gizliliğini ihlal etmek, kişiler arasındaki haberleşme içeriklerini ifşa etmek, kişiler arasındaki aleni olmayan konuşmaları taraflardan herhangi birinin rızası olmaksızın kaydetmek, kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri ifşa etmek, kişilerin özel hayatının gizliliğini ihlal etmek, kişilerin özel hayatına ilişkin görüntü veya sesleri ifşa etmek, kişisel verileri kaydetmek, kişisel verileri bir başkasına vermek, yaymak veya ele geçirmek, kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olduğu halde bu görevini kasıtlı olarak yerine

getirmemek, gerçeğin meydana çıkmasını engellemek amacıyla suç delillerini yok etmek, silmek, gizlemek, değiştirmek veya bozmak, sayılan fiilleri emir vererek yaptırmak.

aa) Yetkili olmadığı halde hukuka aykırı olarak elektronik ortamda veya bilgisayar loglarında kişisel verilerle ilgili sorgulama yapmak, bu şekilde elde edilen bilgileri paylaşmak veya yayın yoluyla duyurmak, log kayıtlarını değiştirmek veya silmek.

bb) Görevi gereği öğrendiği veya edindiği kişisel bilgi veya belgeleri yetkisiz kişilerle paylaşmak ya da basın ve yayın kuruluşlarına veya diğer iletişim kanallarına vermek.

cc) Bir kimseyle gayri tabii mukarenette bulunmak yahut bu fiili kendisine rızasıyla yaptırmak.

çç) Görevine, sosyal ve aile yaşantısına zarar verecek derecede menfaatine, içkiye, kumara ve benzeri kötü alışkanlıklara düşkün olmak.

dd) Üstlerine, aynı rütbedeki meslektaşları ile diğer mesai arkadaşlarına fiili tecavüzde bulunmak.

ee) Görevde kullanılan telsiz haberleşme araçlarıyla amir ya da üstleri hakkında olumsuz yönde eleştirici nitelikte konuşmalar yapmak.

ff) Dernek kurmak ya da spor dernekleri dışındaki derneklere üye olmak.

gg) Vakıf kurmak veya Bakanlıkça belirlenmiş vakıflardan başka vakıfların organlarında görev almak.

hh) (Ek:18/10/2018-7148/36 md.) Fuhşa teşvik eden, bunun yolunu kolaylaştıran ya da fuhuş için aracılık eden veya yer temin eden kişilerle bilerek ilişki kurmak.”

II. İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Serdar ÖZGÜLDÜR, Burhan ÜSTÜN, Engin YILDIRIM, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĞLU, Selahaddin MENTEŞ ve Basri BAĞCI'nın katılımlarıyla 15/10/2020 tarihinde yapılan ilk inceleme toplantısında dosyada eksiklik bulunmadığından işin esasının incelenmesine OYBİRLİĞİYLE karar verilmiştir.

III. ESASIN İNCELENMESİ

2. Başvuru kararı ve ekleri, Raportör Gülbin AYNUR tarafından hazırlanan işin esasına ilişkin rapor, itiraz konusu kanun hükmü, dayanan ve ilgili görülen Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A. Anlam ve Kapsam

3. 7068 sayılı Kanun Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı personeline ilişkin disiplinsizlik hâlleri ile cezalarını, disiplin amirlerini ve kurullarını, disiplin soruşturma usulünü ve ilgili diğer hususları düzenlemektedir. Anılan Kanun'un 2. maddesine göre; Emniyet Genel Müdürlüğü teşkilatında çalışan her sınıftan memurlar, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı teşkilatlarında görev yapan subay, astsubay, sözleşmeli subay, sözleşmeli astsubay, uzman jandarma, uzman erbaş, sözleşmeli erbaş ve sözleşmeli erler ile diğer sınıflardaki memurlar Kanun'un kapsamında yer almaktadır.

4. Kanun'un 7. maddesinin (1) numaralı fıkrasında fiilin niteliğine göre personele verilebilecek disiplin cezaları; uyarma, kınama, aylıktan kesme, kısa süreli durdurma, uzun süreli durdurma, meslekten çıkarma ve devlet memurluğundan çıkarma cezası olarak belirlenmiştir. Anılan fıkranın (e) bendinde meslekten çıkarma personelin emniyet, jandarma ve sahil güvenlik teşkilatlarında bir daha çalıştırılmamak üzere meslekten çıkarılması şeklinde tanımlanmış; (f) bendinde ise devlet memurluğundan çıkarmanın personelin bir daha devlet memurluğuna atanmamak üzere memurluktan çıkarılması olduğu belirtilmiştir. Dolayısıyla meslekten çıkarma cezasının verilmesi hâlinde emniyet, jandarma ve sahil güvenlik teşkilatlarında görev yapan personelin bir daha bu kolluk teşkilatlarında çalışabilmesi mümkün olmayıp aksi belirtilmedikçe diğer kamu kurumlarında çalışabilmesi söz konusu olabilmektedir.

5. Kanun'un 8. maddesinin meslekten çıkarma cezasını gerektiren fiillerin düzenlendiği (6) numaralı fıkrasının (aa) bendinde "Yetkili olmadığı halde hukuka aykırı olarak elektronik ortamda veya bilgisayar loglarında kişisel verilerle ilgili sorgulama yapmak, bu şekilde elde edilen bilgileri paylaşmak veya yayın yoluyla duyurmak, log kayıtlarını değiştirmek veya silmek" meslekten çıkarma cezasını gerektiren fiiller arasında sayılmış olup anılan bentte yer alan "...sorgulama yapmak,..." ibaresi itiraz konusu kuralı oluşturmaktadır. Buna göre yetkili olmadığı hâlde hukuka aykırı şekilde elektronik ortamda veya bilgisayar loglarında kişisel verilerle ilgili sorgulama yapan genel kolluk personeli meslekten çıkarma cezası ile cezalandırılacaktır.

6. Kişisel veri, kimliği belirli veya belirlenebilir kişiye ilişkin her türlü bilgiyi ifade etmekte olup Anayasa Mahkemesinin yerleşik kararlarında belirtildiği üzere "...adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan

tüm veriler...” kişisel veri olarak kabul edilmektedir (AYM, E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2014/74, K.2014/201, 25/12/2014; E.2014/180, K.2015/30, 19/3/2015; E.2015/32, K.2015/102, 12/11/2015).

7. Kurala göre kişisel verilerle ilgili olarak elektronik ortamda veya bilgisayar loglarında sorgulama yapılması fiilinin disiplin suçu teşkil edebilmesi için bir personelin, sistem üzerinde sorgulama yapma yetkisine sahip kılınmadığı hâlde hukuka aykırı olarak bu sorgulamayı gerçekleştirmiş olması gerekmektedir. Dolayısıyla kuralda yer alan “Yetkili olmadığı halde hukuka aykırı olarak...” ifadesi ile kastedilen hususun bir personelin görevinin kapsamı ve niteliği gereği haiz olduğu yetkiler uyarınca elektronik ortamda veya bilgisayar loglarında erişim imkânı bulunmayan kişisel verilere hukuka aykırı yol ve yöntemler kullanarak erişim sağlaması olduğu anlaşılmaktadır.

8. Yürüttüğü görevin niteliği gereği haiz olduğu yetkiler kapsamında bir personele elektronik ortamda ya da bilgisayar loglarında bu tür bilgilere hukuk düzeninin onayladığı bir yöntemle erişebilme imkânının sağlanmış olması personelin o bilgileri sorgulama konusunda yetkili kılındığı anlamına gelmektedir. Bu itibarla böyle bir durumda yetkili olmama hâlinde söz edilemeyeceğinden haiz olunan sorgulama yetkisinin hizmetin gerekleri ve amacı dışında kullanılması suretiyle gerçekleştirilen fiiller kuralın kapsamında yer almamaktadır.

B. İtirazın Gerekçesi

9. Başvuru kararında özetle; yetkisiz olarak kişiler hakkında sistem üzerinden sorgulama yapılması eyleminin disiplin cezasını gerektirdiğinde şüphe bulunmadığı, ancak kişisel verilerin sadece görüntülenmesi fiilinin bu verileri yayma, ilan etme gibi fiillerle aynı ağırlıkta görülerek meslekten çıkarma cezasıyla cezalandırılmasının hukuk devletinin gereği olan ölçülülük ilkesiyle bağdaşmadığı, disiplin suçu olarak görülen fiil ile karşılığı olarak belirlenen disiplin cezası arasında adil bir dengenin kurulmadığı belirtilerek kuralın Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüştür.

C. Anayasa'ya Aykırılık Sorunu

10. 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 43. maddesi uyarınca kural, ilgisi nedeniyle Anayasa'nın 13. ve 70. maddeleri yönünden incelenmiştir.

11. İtiraz konusu kuralın yer aldığı 7068 sayılı Kanun, olağanüstü hâl kapsamında çıkarılan 2/1/2017 tarihli ve 682 sayılı Genel Kolluk Disiplin Hükümleri Hakkında Kanun Hükmünde Kararname'nin Türkiye Büyük Millet Meclisi tarafından onaylanması sonucu yürürlüğe girmiştir. Bununla birlikte

kural olağanüstü hâl süresiyle sınırlı bir düzenleme öngörmediğinden kurala ilişkin incelemenin Anayasa'nın olağan dönem kuralları yönünden öngördüğü denetim rejimine göre yapılması gerekir.

12. Anayasa'nın 70. maddesinin birinci fıkrasında "Her Türk, kamu hizmetlerine girme hakkına sahiptir." denilmek suretiyle kamu hizmetlerine girme hakkı güvence altına alınmıştır.

13. Anılan hak sadece kamu hizmetlerine girmeyi değil kamu hizmetlerinde bulunmayı/kalmayı da güvence altına almaktadır (AYM, E. 2021/104, K. 2021/87, 11/11/2021). Dolayısıyla kişinin kamu hizmetinden çıkarılması sonucunu doğuran düzenlemeler Anayasa'nın 70. maddesi kapsamındadır.

14. İtiraz konusu kuralla yetkili olmadığı hâlde hukuka aykırı şekilde elektronik ortamda veya bilgisayar loglarında kişisel verilerle ilgili sorgulama yapan genel kolluk personelinin meslekten çıkarılmasına imkân tanınmak suretiyle kamu hizmetlerine girme hakkına bir sınırlama getirilmektedir.

15. Anayasa'nın 13. maddesinde "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz." denilmektedir.

16. Buna göre kamu hizmetlerine girme hakkına sınırlama getirilirken temel hak ve özgürlüklerin sınırlanması rejimini düzenleyen Anayasa'nın 13. maddesinin gözönünde bulundurulması gerekmektedir. Anayasa'nın söz konusu maddesi uyarınca kamu hizmetlerine girme hakkına getirilen sınırlamalar kanunla yapılmalı, Anayasa'da öngörülen sınırlama sebeplerine ve ölçülülük ilkesine uygun olmalıdır.

17. Bu kapsamda kamu hizmetlerine girme hakkını sınırlamaya yönelik bir kanuni düzenlemenin şeklen var olması yeterli olmayıp yasal kuralların keyfiliğe izin vermeyecek şekilde belirli, ulaşılabilir ve öngörülebilir düzenlemeler niteliğinde olması gerekir.

18. Esasen temel hak ve özgürlükleri sınırlayan kanunun bu niteliklere sahip olması Anayasa'nın 2. maddesinde güvenceye alınan hukuk devleti ilkesinin de bir gereğidir. Hukuk devletinde kanuni düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi gerekir. Kanunda bulunması gereken bu nitelikler hukuki güvenliğin sağlanması bakımından da zorunludur. Zira bu ilke hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar

(AYM, E.2015/41, K.2017/98, 4/5/2017, §§ 153, 154). Dolayısıyla Anayasa'nın 13. maddesinde sınırlama ölçütü olarak belirtilen kanunilik, Anayasa'nın 2. maddesinde güvenceye alınan hukuk devleti ilkesi ışığında yorumlanmalıdır.

19. Kuralda; genel kolluk personelinin meslekten çıkarılmasını gerektiren, başka bir ifadeyle kamu hizmetinden ilişkisinin kesilmesi sonucunu doğuran disiplin suçunun konusunu teşkil eden fiilin kapsamı, niteliği ve ne şekilde işlenebileceğinin herhangi bir tereddüde yer vermeyecek biçimde açık ve net olarak düzenlendiği gözetildiğinde kamu hizmetlerine girme hakkına sınırlama getiren kuralın belirli, ulaşılabilir ve öngörülebilir nitelikte olduğu ve bu yönüyle kanunilik şartını taşıdığı anlaşılmaktadır.

20. Kuralın Anayasa'nın 13. maddesine uygunluğu denetlenirken sınırlamayı haklı kılan sebebin, başka bir ifadeyle söz konusu düzenlemenin meşru amacının bulunup bulunmadığının da ortaya konulması gerekmektedir.

21. Anayasa'nın 70. maddesinde kamu hizmetlerine girme hakkı sınırsız bir hak olarak düzenlenmemiş, bu kapsamda maddenin ikinci fıkrasında "Hizmete alınmada, görevin gerektirdiği niteliklerden başka hiçbir ayırım gözetilemez." hükmüne yer verilerek hizmete alınmada görevin gerektirdiği niteliklerin gözetilmesi anılan hak bakımından özel bir sınırlama nedeni olarak öngörülmüştür. Diğer yandan hizmete alınmada görevin gerektirdiği niteliklerin gözetilmesi -hakkın kapsamı gereği- bu niteliklerin kamu hizmetinde bulunma sırasında devam etmesini de içermektedir. Bu bağlamda anılan fıkra ile hizmete alınmada görevin gerektirdiği niteliklerden başka hiçbir ayırım gözetilemeyeceği öngörülerek bir yandan kamu hizmetine alınmada aranacak şartların belirlenmesi hususunda kanun koyucuya takdir yetkisi tanınmış, diğer yandan da söz konusu şartlar belirlenirken bu hakka getirilecek sınırlamaların ancak görevin gerektirdiği niteliklerle uyumlu olması hâlinde mümkün olabileceği ifade edilmiştir. Buna göre kamu hizmetine girme hakkına getirilecek sınırlama görevin gerektirdiği niteliklerden başka bir şarta bağlanamaz. Bu husus, anılan maddenin gerekçesinde "...Kamu hizmetine alınacak memur ve kamu görevlileri ile ilgili düzenlemede bu hakkın kötüye kullanılmasını önleyecek hükümler getirilmiştir" biçiminde vurgulanmıştır (AYM, E.2018/89, K.2019/84, 14/11/2019, § 16).

22. Bu itibarla, kuralla öngörülen düzenlemenin meşru amacının bulunup bulunmadığının saptanması için kolluk personelinin kamu hizmetinden çıkarılması sonucunu doğuran ve disiplin suçunun konusunu teşkil eden fiilin görevin gerektirdiği niteliklerle ilgisinin olup olmadığının tespit edilmesi gerekmektedir.

23. Anayasa koyucu kişisel verilerin korunmasına büyük bir önem vermiş ve kişisel verilerin korunması hakkını Anayasa'nın 20. maddesi kapsamında anayasal güvenceye bağlamıştır. Anılan maddede kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir. Bu kapsamda, veri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esaslar genel olarak 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda düzenlenmiş, bazı kanunlarda da kişisel verilerle ilgili hükümlere yer verilmek suretiyle konuya ilişkin yasal güvencenin sağlanması amaçlanmıştır.

24. Diğer yandan 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nda kişisel verilerin hukuka aykırı olarak ele geçirilmesi fiili özel hayata ve hayatın gizli alanına karşı işlenen suçlar kapsamında düzenlenmiş, anılan Kanun'un 136. maddesinin (1) numaralı fıkrasında kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişinin, iki yıldan dört yıla kadar hapis cezası ile cezalandırılması öngörülmüştür. Ayrıca Kanun'un 137. maddesinin (a) bendinde söz konusu suçun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle işlenmesi hâli cezayı yarı oranında artırıcı nedenler arasında gösterilmiştir.

25. Anayasa'nın 129. maddesinin birinci fıkrasında memurlar ve diğer kamu görevlilerinin Anayasa ve kanunlara sadık kalarak faaliyette bulunmakla yükümlü oldukları hükme bağlanmıştır. Dolayısıyla bireylerin anayasal güvenceye bağlanan temel hak ve özgürlüklerinin, bu kapsamda kişisel verilerinin, herkesten önce devletin resmî makamları tarafından korunması zorunluluğu Anayasa'nın 129. maddesi hükmünün yanı sıra hukuka bağlı devlet olmanın da gereğidir.

26. Toplumda asayiş ve güvenliği sağlamakla görevli olan kolluk teşkilatının bu görevin yerine getirilmesi esnasında ihtiyaç duyulan kişisel verileri sorgulama yetkisine sahip olması hizmetin gereği gibi yerine getirilebilmesi için zorunlu ve kaçınılmazdır. Bununla birlikte görevinin kapsam ve niteliği gözetilmeksizin ve herhangi bir sınırlamaya tabi olmaksızın tüm kolluk personelinin bireylerin kişisel verileri üzerinde sorgulama yapabileceğinin kabulü anayasal güvenceye bağlanan kişisel verilerin korunması hakkının bizzat devlet tarafından ihlal edilmesi anlamına geleceği gibi toplumda kolluk personeline yönelik bu şekilde bir algının oluşması kolluk kuvvetlerine olan güvenin zedelenmesine de yol açabilecektir. Nitekim 7068 sayılı Kanun'la kabul edilen 682 sayılı KHK'nın genel gerekçesinde genel kolluk kuvvetlerinin vatandaşın güvenini kazanarak en iyi şekilde hizmet sunabilmesinin temelinde disiplinli olmasının yer aldığı belirtilmiş ve yapılan düzenlemeyle genel kolluk görevi yürüten kurumların iç disiplinin sağlanmasına ve hukuka uygun hareket etmesine yönelik usul ve esasların belirlenmesinin amaçlandığı ifade edilmiştir.

27. Yukarıda yer verilen açıklamalar çerçevesinde, kişisel verilerin korunmasına yönelik olarak Anayasa'da sağlanan güvencelere uygun şekilde hareket etmenin genel kolluk personelinin hizmetin mahiyeti ve özelliği gereği haiz olması ve görevde bulunduğu sürece de koruması gereken temel niteliklerden olduğu sonucuna varılmaktadır.

28. Bu itibarla kuralla getirilen sınırlamanın Anayasa'nın 70. maddesinde belirtilen sınırlama sebebine uygun olarak öngörüldüğü anlaşılmaktadır.

29. Diğer yandan Anayasa'nın 13. maddesi uyarınca sınırlamanın ölçülü olup olmadığının da değerlendirilmesi gerekir. Anayasa'nın anılan maddesinde güvence altına alınan ölçülülük ilkesi elverişlilik, gereklilik ve orantılılık olmak üzere üç alt ilkeden oluşmaktadır. Elverişlilik öngörülen sınırlamanın ulaşılmak istenen amacı gerçekleştirmeye elverişli olmasını, gereklilik ulaşılmak istenen amaç bakımından sınırlamanın zorunlu olmasını, diğer bir ifadeyle aynı amaca daha hafif bir sınırlama ile ulaşılmamasının mümkün olmamasını, orantılılık ise hakka getirilen sınırlama ile ulaşılmak istenen amaç arasında makul bir dengenin gözetilmesi gerekliliğini ifade etmektedir.

30. Genel kolluk teşkilatlarınca hizmet içinde ve hizmet gereği kullanılan resmî bilişim sisteminde ve bilgisayar kayıtlarında yetkisi olmadığı hâlde hukuka aykırı yollarla kişisel veriler üzerinde sorgulama yapan personelin meslekten çıkarılmasının öngörülmesi, görevin gerektirdiği temel niteliklerle bağdaşmayan bu tür fiillerde bulunulmasını engelleyici ve caydırıcı nitelikte olduğundan itiraz konusu kuralın, bu kuralla ulaşılmak istenen amaç yönünden elverişli ve gerekli olduğu söylenebilir.

31. Kurala konu fiilin işlenmesi hâlinde uygulanması öngörülen meslekten çıkarma cezasının orantılı olup olmadığının tespitinde mesleğin özelliği ile kişinin hak ve menfaatleri üzerinde oluşturduğu tesir ve yaptırımın gerekçesini oluşturan meşru amacın niteliği gözönünde bulundurulmalıdır.

32. Kuralda belirtilen fiil karşılığında öngörülen meslekten çıkarma cezası 7068 sayılı Kanun'da genel kolluk kuvvetleri personeli hakkında muhtelif fiiller karşılığında uygulanabileceği belirtilen disiplin cezaları içinde en ağır ikinci ceza olan ve kişinin emniyet, jandarma ve sahil güvenlik teşkilatlarında bir daha çalıştırılmamak üzere meslekle ilişkisinin kesilmesi sonucunu doğuran bir yaptırımdır. Hukuka aykırılıklarla mücadele etme temeli üzerine oluşturulan kolluk teşkilatlarında yürütülen hizmetin hassasiyeti ve burada görev yapan personelin toplumsal güven ve huzur adına taşıdığı önem gözetildiğinde, devletin, korunmasına özel bir önem göstererek anayasal güvenceye bağladığı kişisel verileri, yetkili olmadığı hâlde mesleğin temel esaslarıyla ve görevin gerektirdiği niteliklerle bağdaşmayacak şekilde hukuka aykırı yöntemlerle elde eden bir kolluk personelinin meslekten

çıkarılmasının, yaptırım ile korunmak istenen hukuki değerler ve elde edilmek istenen kamusal yarar karşısında bireye makul olmayan, orantısız bir külfet yüklediği sonucuna varılmaktadır.

33. Öte yandan personelin emniyet, jandarma ve sahil güvenlik teşkilatlarında bir daha çalıştırılmamak üzere meslekten çıkarılmasının gerekli şartları taşıması kaydıyla diğer kamu kurumlarında çalışabilmesine engel teşkil etmediği de dikkate alındığında itiraz konusu kural ile kamu hizmetlerine girme hakkına getirilen sınırlamanın orantısız olmadığı sonucuna varılmıştır.

34. Açıklanan nedenlerle kural Anayasa'nın 13. ve 70. maddelerine aykırı değildir. İtirazın reddi gerekir.

Kuralın Anayasa'nın 2. maddesine de aykırı olduğu ileri sürülmüş ise de bu bağlamda belirtilen hususların Anayasa'nın 13. ve 70. maddeleri yönünden yapılan değerlendirmeler kapsamında ele alınmış olması nedeniyle Anayasa'nın 2. maddesi yönünden ayrıca bir inceleme yapılmasına gerek görülmemiştir.

IV. HÜKÜM

31/1/2018 tarihli ve 7068 sayılı Genel Kolluk Disiplin Hükümleri Hakkında Kanun Hükmünde Kararnamenin Kabul Edilmesine Dair Kanun'un 8. maddesinin (6) numaralı fıkrasının (aa) bendinde yer alan "...sorgulama yapmak,..." ibaresinin Anayasa'ya aykırı olmadığına ve itirazın REDDİNE 16/12/2021 tarihinde OYBİRLİĞİYLE karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili - Hasan Tahsin GÖKCAN; Kadir ÖZKAYA

Üye: Engin YILDIRIM; Hicabi DURSUN; Celal Mümtaz AKINCI; Muammer TOPAL; M. Emin KUZ;
Rıdvan GÜLEÇ; Recai AKYEL; Yusuf Şevki HAKYEMEZ; Yıldız SEFERİNOĞLU; Selahaddin
MENTEŞ; Basri BAĞCI; İrfan FİDAN

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2021/88

Karar Sayısı: 2021/105

Karar Tarihi: 30.12.2021

R.G.Tarih-Sayısı: 25/2/2022 - 31761

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri Engin ALTAY, Özgür ÖZEL, Engin ÖZKOÇ ile birlikte 132 milletvekili

İPTAL DAVASININ KONUSU: 29/6/2021 tarihli ve (77) numaralı Ekonomi Koordinasyon Kurulu Hakkında Cumhurbaşkanlığı Kararnamesi'nin 6. maddesinin Anayasa'nın 2., 6., 8., 13., 20. ve 104. maddelerine aykırılığı ileri sürülerek iptaline ve yürürlüğünün durdurulmasına karar verilmesi talebidir.

I. İPTALİ İSTENEN CUMHURBAŞKANLIĞI KARARNAMESİ KURALI

Cumhurbaşkanlığı Kararnamesi'nin (CBK) iptali talep edilen 6. maddesi şöyledir:

"Bilgi İsteme

MADDE 6- (1) Kurul, görev alanına giren konularla ilgili her türlü bilgi ve belgeyi, bakanlıklar ve diğer kamu kurum ve kuruluşlarından isteme yetkisine sahiptir. Kamu kurum ve kuruluşları, talep edilen bilgi ve belgeyi Kurulun belirleyeceği şekil ve süre içerisinde vermekle yükümlüdür."

II. İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Kadir Özkaya, Engin YILDIRIM, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĞLU, Selahaddin MENTEŞ, Basri BAĞCI ve İrfan FİDAN'ın katılımlarıyla 22/9/2021 tarihinde yapılan ilk inceleme toplantısında dosyada eksiklik bulunmadığından işin esasının incelenmesine, yürürlüğü durdurma talebinin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

III. ESASIN İNCELENMESİ

2. Dava dilekçesi ve ekleri, Raportör Burak FIRAT tarafından hazırlanan işin esasına ilişkin rapor, dava konusu CBK kuralı, dayanan Anayasa kuralları ile bunların gerekçeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A. Cumhurbaşkanlığı Kararnamelerinin Anayasal Çerçevesi ve Yargısal Denetimi

3. 21/1/2017 tarihli ve 6771 sayılı Türkiye Cumhuriyeti Anayasasında Değişiklik Yapılmasına Dair Kanun ile Anayasa'nın bazı maddelerinde değişiklik yapılmıştır. Yapılan değişikliklerle yeni bir hükümet sistemine geçilmiş ve buna bağlı olarak Cumhurbaşkanı'nın görev ve yetkileri yeniden düzenlenmiştir. Anayasa'nın 8. maddesinde, yürütme yetkisi ve görevinin Cumhurbaşkanı ve Bakanlar Kuruluna ait olduğu ifade edilmekte iken maddede yapılan değişiklikle Bakanlar Kurulu kaldırılarak yürütme yetkisi ve görevi tek başına Cumhurbaşkanı'na verilmiştir. Anayasa'da Bakanlar Kuruluna verilen görev ve yetkilere ilişkin maddelerde de aynı doğrultuda değişiklik yapılarak daha önce Bakanlar Kuruluna ait olan görev ve yetkilerin Cumhurbaşkanı tarafından yerine getirilmesi öngörülmüştür.

4. Yeni hükümet sisteminin en önemli özelliklerinden biri Cumhurbaşkanı'na "Cumhurbaşkanlığı Kararnamesi" adı altında düzenleme yapma yetkisinin tanınmasıdır. CBK'ların en belirgin özelliği ise Cumhurbaşkanı'na belirli konularda ilk elden düzenleme yapma yetkisinin verilmiş olmasıdır. Yürütmenin diğer düzenleyici işlemlerinden farklı olarak Cumhurbaşkanı Anayasa'da belirlenen yetki çerçevesinde herhangi bir kanuna dayanmadan ya da yasama organının onayı olmadan CBK'lar yoluyla düzenleme yapabilecektir.

5. Anayasa'nın 104. maddesinin on yedinci fıkrasının birinci cümlesinde Cumhurbaşkanı'nın yürütme yetkisine ilişkin konularda CBK çıkarabileceği hüküm altına alınmıştır. Düzenlemeyle yürütme yetkisine ilişkin olmak kaydıyla CBK çıkarma konusunda Cumhurbaşkanı'na genel bir yetki verilmiştir. Maddenin gerekçesinde, yeni hükümet sistemi gözetilerek Cumhurbaşkanı'nın genel siyasetin yürütülmesinde yürütme yetkisi ile ilgili olarak ihtiyaç duyduğu konularda CBK çıkarabilmesine imkân tanımak amacıyla ilk elden düzenleme yapma yetkisinin tanındığı ifade edilmiştir.

6. Cumhurbaşkanı'na yürütme yetkisine ilişkin konularda CBK çıkarma yetkisinin genel olarak verilmesinin yanı sıra Anayasa'nın diğer bazı maddelerinde belirtilen kimi konuların CBK ile düzenleneceği ayrıca ifade edilmiştir. Bu kapsamda Anayasa'nın 104. maddesinin dokuzuncu fıkrasında üst kademe kamu yöneticilerinin atanmalarına ilişkin usul ve esasların; 106. maddesinin on birinci fıkrasında bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulmasının; 108. maddesinin dördüncü fıkrasında Devlet Denetleme

Kurulunun işleyişi, üyelerinin görev süresi ve diğer özlük işlerinin; 118. maddesinin altıncı fıkrasında Millî Güvenlik Kurulu Genel Sekreterliğinin teşkilatı ve görevlerinin CBK'larla düzenleneceği hüküm altına alınmıştır. Anayasa'nın 123. maddesinin üçüncü fıkrasında ise kamu tüzel kişiliğinin kanunla veya CBK ile kurulacağı belirtilmiştir.

7. Anayasa'nın 148. maddesinde CBK'ların şekil ve esas bakımından Anayasa'ya uygunluğunun denetlenmesi öngörülmüş, yargısal denetim görev ve yetkisi de Anayasa Mahkemesine verilmiştir.

8. Anayasa'da Cumhurbaşkanı'na CBK çıkarma yetkisi verilmekle birlikte bu yetki sınırsız değildir. Kanunlardan farklı olarak Anayasa'da CBK'yla düzenlenecek konular sınırlandırılmıştır. Konu bakımından yetki yönünden getirilen bu sınırlamalar Anayasa'nın 104. maddesinin on yedinci fıkrasının ilk dört cümlesinde düzenlenmiştir.

9. Anılan fıkranın birinci cümlesinde Cumhurbaşkanı'nın yürütme yetkisine ilişkin konularda CBK çıkarabileceği ifade edilmiştir. Buna göre yürütme yetkisine ilişkin konular dışında CBK ile düzenleme yapılması mümkün değildir.

10. Fıkranın ikinci cümlesinde "Anayasa'nın ikinci kısmının birinci ve ikinci bölümlerinde yer alan temel haklar, kişi hakları ve ödevleriyle dördüncü bölümde yer alan siyasi haklar ve ödevlerin" CBK'yla düzenlenemeyeceği belirtilmiştir. Bu hüküm uyarınca belirtilen alanlarda CBK ile düzenleme yapılamaz.

11. Fıkranın üçüncü cümlesinde de Anayasa'da münhasıran kanunla düzenlenmesi öngörülen konularda CBK çıkarılmayacağı hüküm altına alınmıştır. Ancak Anayasa'da hangi konuların münhasıran kanunla düzenleneceğine ilişkin özel bir hüküm bulunmamaktadır. Bununla birlikte Anayasa Mahkemesinin yerleşik içtihadında anayasa koyucunun kanunla düzenlenmesini öngördüğü konuların bu kapsamda görülmesi gerektiği kabul edilmektedir (AYM, E.2016/150, K.2017/179, 28/12/2017, § 57; E.2016/180, K.2018/4, 18/1/2018, § 17; E.2017/51, K.2017/163, 29/11/2017, § 13; E.2016/139, K.2016/188, 14/12/2016, § 9; E.2013/47, K.2013/72, 6/6/2013). Buna göre Anayasa'da kanunla düzenleneceği belirtilen alanlarda Cumhurbaşkanı'nın CBK çıkarma yetkisi bulunmamaktadır.

12. Fıkranın dördüncü cümlesinde ise kanunda açıkça düzenlenen konularda CBK çıkarılmayacağı ifade edilmiştir. Anılan hükme göre Cumhurbaşkanı'nın yürütme yetkisine ilişkin konularda CBK çıkarabilmesi için CBK'yla düzenlenecek konunun kanunlarda açıkça düzenlenmemiş olması gerekir.

13. CBK'ların yukarıda belirtilen konu bakımından yetki kurallarına uygun olarak çıkarılması gerekmektedir. Aksi takdirde içeriği Anayasa'ya aykırılık oluşturmasa bile bu düzenlemelerin

Anayasa'ya uygunluğundan söz edilemez. Dolayısıyla CBK'ların yargısal denetiminde öncelikle Anayasa'nın 104. maddesinin on yedinci fıkrasında belirtilen konu bakımından yetki kurallarına uygunluğunun ele alınması gerekir. Anılan fıkra yönünden herhangi bir aykırılık tespit edilmemesi durumunda ise bu defa CBK'ların içerik yönünden Anayasa'ya uygunluk denetimi yapılmalıdır.

B. İptal Talebinin Gerekçesi

14. Dava dilekçesinde özetle; Ekonomi Koordinasyon Kurulunun (Kurul) görevleriyle ilgili olarak bakanlıklar ile kamu kurum ve kuruluşlardan talep edeceği bilgi ve belgelerin içinde kişisel verilerin de yer almasının mümkün olduğu, kuralın kişisel verilerin korunmasına ilişkin bir düzenleme içermediği, kişisel verilerin toplanması, işlenmesi, analizi, paylaşılması gibi faaliyetlerin kanunla düzenlenmesi gerektiği, genel çerçevesi, ilke ve esasları belirlenmeden kişiler hakkında bilgi ve veri toplamak için idareye yetki verilmesinin hukuki belirlilik ve öngörülebilirlik ilkelerine aykırı olduğu, kişisel verilerin Anayasa'nın kişi hak ve ödevlerine ilişkin "İkinci Kısım İkinci Bölüm"ünde düzenlendiği, buna göre ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilecek olan kişisel verilerin korunmasına ilişkin esas ve usullerin de kanunla belirlenmesi gerektiği, temel haklar, kişi hakları ve ödevlerinin CBK ile düzenlenemeyeceği, kuralın kanunlarda açıkça düzenlenen hususlara ilişkin hükümler içerdiği, kamu tüzel kişiliği olmayan bir Kurulun kamu kurum ve kuruluşlarından bilgi istemeye yetkili kılındığı, Cumhurbaşkanının yürütme yetkisini Anayasa'ya uygun kullanmadığı belirtilerek kuralın Anayasa'nın 2., 6., 8., 13., 20. ve 104. maddelerine aykırı olduğu ileri sürülmüştür.

C. Anayasa'ya Aykırılık Sorunu

15. Dava dilekçesinde konu bakımından yetki yönünden kuralın Anayasa'nın 2., 6., 8., 13. ve 20. maddesine de aykırı olduğu ileri sürülmüş ise de CBK'ya ilişkin konu bakımından yetki kuralları Anayasa'nın 104. maddesinin on yedinci fıkrasında düzenlendiğinden bu husustaki inceleme anılan fıkra kapsamında yapılacaktır.

16. CBK'nın dava konusu 6. maddesinin birinci cümlesinde Kurulun görev alanına giren konularla ilgili olarak gerekli gördüğü bilgi ve belgeleri bakanlıklar ile diğer kamu kurum ve kuruluşlarından istemeye yetkili olduğu belirtilmiş, ikinci cümlesinde ise kendilerinden bilgi ve belge istenen kamu kurum ve kuruluşlarının bu bilgi ve belgeleri Kurulun belirleyeceği şekil ve süre içinde vermekle yükümlü oldukları hüküm altına alınmıştır.

17. Anayasa'nın 104. maddesinin on yedinci fıkrasının üçüncü cümlesinde Anayasa'da münhasıran kanunla düzenlenmesi öngörülen konularda CBK çıkarılmayacağı hükmüne yer verilmiştir.

Anayasa koyucununun bir konunun kanunla düzenlenmesini özel olarak öngörmesi bu alanın münhasıran kanunla düzenlenmesini istediği anlamına gelir. Bu kapsamda Anayasa bir konunun kanunla düzenleneceğini öngörmüşse bu konuda CBK çıkarılamaz. Bununla birlikte Anayasa'da CBK'larla düzenleneceği özel olarak öngörülen konulara ilişkin Anayasa hükümlerinin açıkça izin verdiği hususlarda CBK'larla düzenleme yapılabilir (AYM, E.2019/105, K.2020/30, 12/6/2020, § 19).

18. Anayasa'nın 123. maddesinin birinci fıkrasına göre "İdare, kuruluş ve görevleriyle bir bütündür ve kanunla düzenlenir." Anayasa'nın anılan maddesinde düzenlenen idarenin kanuniliği ilkesi, idarenin ve organlarının görev ve yetkilerinin kanunla düzenlenmesini gerekli kılar (AYM, E.2013/114, K.2014/184, 4/12/2014, § 136, AYM, E.2012/102, K.2012/207, 27/12/2012). Ancak Anayasa'nın 106. maddesinin on birinci fıkrasında "Bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulması Cumhurbaşkanlığı kararnamesiyle düzenlenir." denilmek suretiyle bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulması yönünden CBK'larla düzenleme yapılmasına açıkça izin verilmiştir.

19. CBK'nın 3. maddesinin (2) numaralı fıkrasında Kurulun Cumhurbaşkanı'nın görevlendireceği Cumhurbaşkanı Yardımcısı başkanlığında Hazine ve Maliye Bakanı, Çalışma ve Sosyal Güvenlik Bakanı, Enerji ve Tabii Kaynaklar Bakanı, Sanayi ve Teknoloji Bakanı, Tarım ve Orman Bakanı, Ticaret Bakanı ve Strateji ve Bütçe Başkanından oluşacağı belirtilmiştir. Anılan CBK'nın 4. maddesinde de ekonomi politikaları alanında genel koordinasyonu sağlamak, ekonomi politikalarının oluşturulması ve uygulanmasında görev ve sorumluluğu bulunan kurum ve kuruluşlar arasında işbirliği ve eşgüdümü sağlamak ve takip etmek, Türkiye ekonomisi ve küresel ekonomi ile ekonomik istikrar ve kalkınma konularında gelişmeleri izlemek ve değerlendirmek, gerektiğinde politika uygulamalarına yönelik etki analizleri yaptırmak ve alt çalışma grupları oluşturmak Kurulun görev ve yetkileri arasında sayılmıştır.

20. Kurulun kuruluşu, görevleri ve üye yapısı dikkate alındığında merkezi idare içinde yer alan, kamu tüzel kişiliği bulunmayan ve Cumhurbaşkanlığı veya herhangi bir bakanlık teşkilatına dâhil olmayan kendine özgü bir idari birim olduğu anlaşılmaktadır.

21. Anayasa Mahkemesinin 22/1/2020 tarihli ve E.2018/125 ve K.2020/4 sayılı kararında ifade edildiği üzere kamu tüzel kişiliği bulunmayan, herhangi bir bakanlığın merkez veya taşra teşkilatına da dâhil olmayan idari bir birimin görev ve yetkilerinin CBK'yla düzenlenmesi Anayasa'nın 106. maddesinin on birinci fıkrasında öngörülen "Bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulması Cumhurbaşkanlığı kararnamesiyle düzenlenir"

şeklindeki kural kapsamında bulunmamaktadır. Ayrıca söz konusu görev ve yetkiler Anayasa'da CBK ile düzenleneceği özel olarak öngörülen diğer konulardan da değildir. Dolayısıyla kamu tüzel kişiliği bulunmayan ve Cumhurbaşkanlığı veya herhangi bir bakanlık teşkilatına dâhil olmayan Kurulun görev ve yetkileri Anayasa'da CBK ile düzenleneceği özel olarak öngörülen konulardan değildir.

22. Kurulun görev alanına giren konularla ilgili her türlü bilgi ve belgeyi bakanlıklar ve diğer kamu kurum ve kuruluşlarından istemeye yetkilendirilmesi, kamu kurum ve kuruluşlarının talep edilen bilgi ve belgeyi vermeye yükümlü kılınması Kurulun görev ve yetkisine ilişkin bir husus olup bunun Anayasa'nın 123. maddesi uyarınca münhasıran kanunla düzenlenmesi gerekmektedir. Bu itibarla kuralda Anayasa'nın 123. maddesi bağlamında 104. maddesinin on yedinci fıkrasının üçüncü cümlesine aykırı şekilde düzenleme yapıldığı anlaşılmaktadır.

23. Açıklanan nedenlerle kural, Anayasa'nın 104. maddesinin on yedinci fıkrasının üçüncü cümlesine aykırıdır. İptali gerekir.

Kural, Anayasa'nın 104. maddesinin on yedinci fıkrasının üçüncü cümlesine aykırı görülerek iptal edildiğinden ayrıca aynı fıkranın birinci, ikinci ve dördüncü cümleleri yönünden incelenmemiştir.

Kural, konu bakımından yetki yönünden Anayasa'nın 104. maddesinin on yedinci fıkrasının üçüncü cümlesine aykırı görülerek iptal edildiğinden içerik yönünden incelenmemiştir.

IV. YÜRÜRLÜĞÜN DURDURULMASI TALEBİ

24. Dava dilekçesinde özetle, dava konusu kuralın uygulanması hâlinde telafisi güç veya imkânsız zararların doğabileceği belirtilerek yürürlüğünün durdurulmasına karar verilmesi talep edilmiştir.

29/6/2021 tarihli ve (77) numaralı Ekonomi Koordinasyon Kurulu Hakkında Cumhurbaşkanlığı Kararnamesi'nin 6. maddesine yönelik yürürlüğün durdurulması talebinin koşulları oluşmadığından REDDİNE 30/12/2021 tarihinde OYBİRLİĞİYLE karar verilmiştir.

V. HÜKÜM

29/6/2021 tarihli ve (77) numaralı Ekonomi Koordinasyon Kurulu Hakkında Cumhurbaşkanlığı Kararnamesi'nin 6. maddesinin konu bakımından yetki yönünden Anayasa'ya aykırı olduğuna ve İPTALİNE 30/12/2021 tarihinde OYBİRLİĞİYLE karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili - Hasan Tahsin GÖKCAN

Başkanvekili - Kadir ÖZKAYA

Üye: Engin YILDIRIM; Hicabi DURSUN; Celal Mümtaz AKINCI; M. Emin KUZ; Rıdvan GÜLEÇ;
Recai AKYEL; Yusuf Şevki HAKYEMEZ; Yıldız SEFERİNOĞLU; Selahaddin MENTEŞ; Basri BAĞCI;
İrfan FİDAN

Anayasa Mahkemesi - 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu Kararı (E. 2021/43)

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2021/43

Karar Sayısı: 2021/74

Karar Tarihi: 13.10.2021

RG Tarih-Sayısı: 3/12/2021-31678

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri Engin ALTAY, Özgür ÖZEL, Engin ÖZKOÇ ile birlikte 132 milletvekili

İPTAL DAVASININ KONUSU: 7/4/2021 tarihli ve 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu'nun;

A. Yok hükmünde olduğunun tespitine,

B. Yok hükmünde olduğunun kabul edilmemesi hâlinde eylemli İçtüzük değişikliği niteliğinde olduğu gerekçesiyle Anayasa'nın 87. ve 88. maddelerine aykırılığı ileri sürülerek iptaline ve yürürlüğünün durdurulmasına,

C. Şekil bakımından Anayasa'nın 88. maddesine aykırılığı ileri sürülerek iptaline ve yürürlüğünün durdurulmasına,

karar verilmesi talebidir.

I. İPTALİ İSTENEN KANUN HÜKÜMLERİ

İptali talep edilen Kanun şöyledir:

“GÜVENLİK SORUŞTURMASI VE ARŞİV ARAŞTIRMASI KANUNU

Kanun No.7315 Kabul Tarihi:7/4/2021

BİRİNCİ BÖLÜM

Amaç, Kapsam ve Tanımlar

Amaç ve kapsam

MADDE 1- (1) Bu Kanun, güvenlik soruşturması ve arşiv araştırmasının yapılmasına ve elde edilecek verilerin kullanılmasına ilişkin temel ilkeleri, kimler hakkında yapılacağını, araştırma konusu edilecek bilgi ve belgelerin neler olduğunu, bu bilgilerin ne şekilde kullanılacağını, hangi mercilerin soruşturma ve araştırma yapacağını, Değerlendirme Komisyonunun oluşumu ve çalışma usul, esaslarını, veri güvenliği ile verilerin saklanma ve silinme sürelerini düzenlemektedir.

Tanımlar

MADDE 2- (1) Bu Kanunda geçen;

- a) Değerlendirme Komisyonu: Güvenlik soruşturması veya arşiv araştırması sonucunda elde edilen kişisel verilerin göreve atanma yönünden değerlendirildiği komisyonu,
 - b) Kurum ve kuruluş: Güvenlik soruşturması ve/veya arşiv araştırması yapılmasını talep eden kamu kurum ve kuruluşları ile milli güvenlik açısından stratejik önemi haiz birim, proje, tesis ve hizmetleri yerine getiren diğer kurum ve kuruluşu,
 - c) Üst kademe kamu yöneticisi: Atanmasına ilişkin usul ve esaslar Cumhurbaşkanlığı kararnamesi ile üst kademe kamu yöneticisi olarak belirlenenini,
- ifade eder.

İKİNCİ BÖLÜM

Güvenlik Soruşturması ve Arşiv Araştırması

Hakkında güvenlik soruşturması ve arşiv araştırması yapılacaklar

MADDE 3- (1) Arşiv araştırması, statüsü veya çalışma şekline bağlı olmaksızın ilk defa veya yeniden memuriyete yahut kamu görevine atanacaklar hakkında yapılır.

(2) Kurum ve kuruluşlarda, yetkili olmayan kişilerin bilgi sahibi olmaları hâlinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile Milli Savunma Bakanlığı, Genelkurmay Başkanlığı, jandarma, emniyet, sahil güvenlik ve istihbarat teşkilatlarında çalıştırılacak kamu personeli ile ceza infaz kurumları ve tutukevlerinde çalışacak personel, kamu kurum ve kuruluşlarında çalışacak öğretmenler, üst kademe kamu yöneticileri, özel kanunları uyarınca güvenlik soruşturması ve arşiv araştırmasına tabi tutulan kişiler ile milli güvenlik açısından stratejik önemi haiz birim, proje, tesis, hizmetlerde statüsü veya çalışma şekline bağlı olmaksızın istihdam edilenler hakkında güvenlik soruşturması ve arşiv araştırması birlikte yapılır.

Arşiv araştırması

MADDE 4- (1) Arşiv araştırması;

- a) Kişinin adli sicil kaydının,
- b) Kişinin kolluk kuvvetleri tarafından hâlen aranıp aranmadığının,
- c) Kişi hakkında herhangi bir tahdit olup olmadığının,
- ç) Kişi hakkında kesinleşmiş mahkeme kararları ve 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun 171 inci maddesinin beşinci ve 231 inci maddesinin onüçüncü fıkraları kapsamında alınan kararlar ile kişi hakkında devam eden veya sonuçlanmış olan soruşturma ya da kovuşturmalar kapsamındaki olguların,
- d) Hakkında kamu görevinden çıkarılma ya da kesinleşmiş memurluktan çıkarma cezası olup olmadığının,

mevcut kayıtlardan tespit edilmesidir.

Güvenlik soruşturması

MADDE 5- (1) Güvenlik soruşturması, arşiv araştırmasındaki hususlara ilave olarak kişinin;

- a) Görevin gerektirdiği niteliklerle ilgili kolluk kuvvetleri ve istihbarat ünitelerindeki olgusal verilerinin,
- b) Yabancı devlet kurumları ve yabancılarla ilişkisinin,
- c) Terör örgütleri veya suç işlemek amacıyla kurulan örgütlerle eylem birliği, irtibat ve iltisak içinde olup olmadığının,

mevcut kayıtlardan ve kişinin görevine yansiyacak hususların denetime elverişli olacak yöntemlerle yerinden araştırılmak suretiyle tespit edilmesidir.

Güvenlik soruşturması ve arşiv araştırmasını yapacak birimler

MADDE 6- (1) Güvenlik soruşturması ve arşiv araştırması, Milli İstihbarat Teşkilatı Başkanlığı, Emniyet Genel Müdürlüğü ve mahalli mülki idare amirlikleri tarafından yapılır.

(2) Güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimler, kendilerine iletilen taleple sınırlı olarak güvenlik soruşturması ve arşiv araştırması kapsamında bakanlıklar ile kamu kurum ve kuruluşları arşivlerinden ve elektronik bilgi işlem merkezlerinden gerekli bilgi ve belgeler ile bu Kanunun 4 üncü maddesinin birinci fıkrasının (ç) bendi kapsamındaki karar ve kayıtları almaya yetkilidir.

(3) Güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimlerde yetkilendirilmiş personel, hukuka aykırı olarak elektronik ortamda veya bilgisayar loglarında kişisel verilerle ilgili sorgulama yapamaz, log kayıtlarını değiştiremez veya silemez, bu şekilde elde edilen bilgileri paylaşamaz veya yayın yoluyla duyuramaz. Görevi gereği öğrendiği veya edindiği kişisel bilgi veya belgeleri yetkisiz kişilerle paylaşamaz ya da basın ve yayın kuruluşlarına veya diğer iletişim kanallarına veremez. Güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimler tarafından bu hususlara ilişkin gerekli tedbirler alınır.

Değerlendirme Komisyonu

MADDE 7- (1) Yaptırılan güvenlik soruşturması ve arşiv araştırması sonucunda elde edilen verilerin değerlendirilmesi amacıyla Değerlendirme Komisyonu kurulur. Değerlendirme Komisyonu; Cumhurbaşkanlığında İdari İşler Başkanının görevlendireceği bir üst kademe yöneticisinin, Türkiye Büyük Millet Meclisi Başkanlığında genel sekreter yardımcısının, bakanlıklarda bakan yardımcısının, diğer kamu kurum ve kuruluşlarında en üst yöneticinin görevlendireceği bir üst kademe yöneticisinin, üniversitelerde rektör yardımcısının, valiliklerde vali yardımcısının başkanlığında, teftiş/denetim, personel ve hukuk birimleri ile uygun görülecek diğer birimlerden birer üyenin katılımıyla başkan dahil en az beş kişiden ve tek sayıda olacak şekilde oluşturulur. Milli güvenlik açısından stratejik önemi haiz birim, proje, tesis ve hizmetlerde istihdam edilecekler hakkındaki değerlendirme, ilgili bakanlık ya da kamu kurumları bünyesindeki Değerlendirme Komisyonunca yapılır.

(2) Memuriyet veya kamu görevlerine uygunluğunun değerlendirilmesini sağlayacak yorum içermeyen olgusal veriler, güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimlerce ilgili kurum ve kuruluş bünyesinde kurulan Değerlendirme Komisyonuna iletilir.

(3) Değerlendirme Komisyonu kendisine iletilen verilere ilişkin nesnel ve gerekçeli değerlendirmelerini yazılı olarak atamaya yetkili amire sunar. Mahkemeler tarafından istenildiğinde bu bilgiler sunulur.

ÜÇÜNCÜ BÖLÜM

Kişisel Verilerin Korunması

Kişisel verilerin korunmasına ilişkin temel ilkeler

MADDE 8- (1) Güvenlik soruşturması ve arşiv araştırması kapsamında kişinin istihbari faaliyetlere konu olmayan kendisiyle ilgili kişisel verileri hakkında bilgilendirilmesi, bu verilere erişmesi, bunların düzeltilmesi ve silinmesi taleplerine ilişkin tedbirler alınır.

(2) Güvenlik soruşturması ve arşiv araştırmasına konu kişisel verilerin doğru ve güncel olması esastır. Bu veriler, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak kullanılır.

(3) Güvenlik soruşturması ve arşiv araştırması kapsamında yürütülen iş ve işlemlerde, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununun 4 üncü maddesinde belirtilen genel ilkelere aykırı hareket edilemez. Ancak millî savunma, millî güvenlik, kamu güvenliği, kamu düzeni ve ekonomik güvenlik ile ilgili istihbarat faaliyetleri kapsamında elde edilen bilgiler kişiye verilemez.

Kişisel veri güvenliği ve gizlilik

MADDE 9- (1) Bu Kanunda belirtilen güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimler ile değerlendirme komisyonları, veri güvenliğine ilişkin önlemleri alır.

(2) Güvenlik soruşturması ve arşiv araştırması işlemlerinin her evresinde gizliliğe uyulur. İlgili bilgi ve belgeler yasal olarak bilmesi gerekenlerden başkasına verilmez ve açıklanmaz.

(3) Bu Kanun kapsamında elde edilen kişisel veriler amacı dışında işlenemez ve aktarılamaz.

Kişisel verilerin silinmesi ve yok edilmesi

MADDE 10- (1) Güvenlik soruşturması ve arşiv araştırması sırasında elde edilen kişisel veriler, işleme amacının ortadan kalkması hâlinde veya her durumda iki yılın sonunda değerlendirme komisyonlarınca silinir ve yok edilir.

(2) Güvenlik soruşturması ve arşiv araştırmasını yapan birimlerdeki istihbari faaliyete konu olmayan ilgisine ait güvenlik soruşturması ve arşiv araştırmasına ait veriler iki yılın sonunda silinir ve yok edilir.

(3) Bu veriler, işleme karşı dava açılması hâlinde karar kesinleşmeden silinemez ve yok edilemez. Mahkemelerin bu konudaki talepleri, Değerlendirme Komisyonunun bünyesinde bulunduğu ilgili kurum ve kuruluş tarafından karşılanır.

DÖRDÜNCÜ BÖLÜM

Çeşitli Hükümler

Cezai hükümler

MADDE 11- (1) Güvenlik soruşturması ve arşiv araştırması yapılması ve değerlendirilmesinde görevli olanlar tarafından kişisel verilerle ilgili suç işlenmesi hâlinde, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde 6698 sayılı Kanunun 17 nci maddesi hükümleri uygulanır.

(2) Güvenlik soruşturması ve arşiv araştırması yapılması ve değerlendirilmesinde görevli olanlar tarafından kişisel verilerle ilgili kabahat işlenmesi hâlinde 6698 sayılı Kanununun 18 inci maddesi hükümleri uygulanır.

Yönetmelik

MADDE 12- (1) Devletin güvenliğini, ulusun varlığını ve bütünlüğünü iç ve dış menfaatlerinin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeler ile gizlilik dereceli kamu personeli ile meslek gruplarının tespiti, birim ve kısımların tanımlarının yapılması, güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak birimler ve değerlendirme komisyonlarının çalışma usul ve esasları ile uygulamaya ilişkin diğer hususlar Cumhurbaşkanınca yürürlüğe konulacak yönetmelik ile düzenlenir.

Değiştirilen ve yürürlükten kaldırılan hükümler

MADDE 13- (1) 24/2/1983 tarihli ve 2802 sayılı Hakimler ve Savcılar Kanununun ek 1 inci maddesinin birinci fıkrasında yer alan "26.10.1994 tarihli ve 4045 sayılı Kanunun 1 inci maddesine göre" ibaresi "Güvenlik Soruşturması ve Arşiv Araştırması Kanununa göre güvenlik soruşturması ve" şeklinde değiştirilmiştir.

(2) 31/7/1970 tarihli ve 1325 sayılı Askeri Okullar, Askeri Öğrenciler, Askeri Fabrikalar ve Bazı Düzenlemeler Hakkında Kanuna aşağıdaki ek madde eklenmiştir.

"Güvenlik soruşturması ve arşiv araştırması

EK MADDE 16- Milli Savunma Bakanlığı nam ve hesabına Bakanlıkça belirlenen eğitim kurumları ile Millî Savunma Üniversitesine bağlı fakülte, yüksekokul, meslek yüksekokulu ve enstitülerde eğitim göreceklere hakkında Güvenlik Soruşturması ve Arşiv Araştırması Kanununa göre güvenlik soruşturması ve arşiv araştırması yapılır."

(3) 9/6/1930 tarihli ve 1700 sayılı Dahiliye Memurları Kanununa aşağıdaki ek madde eklenmiştir.

"EK MADDE 6- Kaymakam adaylığına atanacaklar hakkında Güvenlik Soruşturması ve Arşiv Araştırması Kanununa göre güvenlik soruşturması ve arşiv araştırması yapılır."

(4) 9/7/1982 tarihli ve 2692 sayılı Sahil Güvenlik Komutanlığı Kanununun 7 nci maddesine onbirinci fıkrasından sonra gelmek üzere aşağıdaki fıkra eklenmiştir.

"Sahil Güvenlik Komutanlığı nam ve hesabına eğitim-öğrenim göreceklere hakkında Güvenlik Soruşturması ve Arşiv Araştırması Kanununa göre güvenlik soruşturması ve arşiv araştırması yapılır."

(5) 10/3/1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanununun 13 üncü maddesine aşağıdaki fıkra eklenmiştir.

“Jandarma Genel Komutanlığı nam ve hesabına eğitim-öğrenim görecekle ile Jandarma ve Sahil Güvenlik Akademisi ve buna bağı eğitim-öğretim kurumlarında eğitim-öğrenim görecekle hakkında Güvenlik Soruşturması ve Arşiv Araştırması Kanununa göre güvenlik soruşturması ve arşiv araştırması yapılır.”

(6) 25/4/2001 tarihli ve 4652 sayılı Polis Yüksek Öğretim Kanununa aşağıdaki ek madde eklenmiştir.

“EK MADDE 3- Polis Akademisi ve buna bağı eğitim-öğretim kurumları ile akademi nam ve hesabına diğere eğitim kurumlarında öğrenim görecekle öğrenciler hakkında Güvenlik Soruşturması ve Arşiv Araştırması Kanununa göre güvenlik soruşturması ve arşiv araştırması yapılır.”

(7) 7/7/2010 tarihli ve 6004 sayılı Dışışleri Bakanlığı Personeline İlişkin Bazı Düzenlemeler Hakkında Kanuna aşağıdaki ek madde eklenmiştir.

“EK MADDE 2- (1) Aday meslek memurluğı ile aday konsolosluk ve ihtisas memurluğına atanacaklar ile doğrudan yurtdışı teşkilatında istihdam edilecek personel hakkında Güvenlik Soruşturması ve Arşiv Araştırması Kanununa göre güvenlik soruşturması ve arşiv araştırması yapılır.”

(8) 26/10/1994 tarihli ve 4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun yürürlükten kaldırılmıştır.

Atıflar

MADDE 14- (1) Mevzuatta 4045 sayılı Kanuna yapılan atıflar bu Kanuna yapılmış sayılır.

Yürürlük

MADDE 15- (1) Bu Kanun yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 16- (1) Bu Kanun hükümlerini Cumhurbaşkanı yürütür.”

II. İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Engin YILDIRIM, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĞLU, Selahaddin MENTEŞ,

Basri BAĞCI ve İrfan FİDAN'ın katılımlarıyla 29/4/2021 tarihinde yapılan ilk inceleme toplantısında dosyada eksiklik bulunmadığından işin esasının incelenmesine, yürürlüğü durdurma talebinin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

III. ESASIN İNCELENMESİ

2. Dava dilekçesi ve ekleri, Raportör Gülbin AYNUR tarafından hazırlanan işin esasına ilişkin rapor, dava konusu Kanun, dayanan ve ilgili görülen Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A. Yok Hükmünde Olduğunun Tespiti ile İptal Taleplerinin Gerekçeleri

3. Dava dilekçesinde özetle; 7315 sayılı Kanun'a dayanak teşkil eden teklifin ilk olarak Türkiye Büyük Millet Meclisi (TBMM) Genel Kurulunun 31/3/2021 tarihli 66. Birleşiminde görüşüldüğü, işaret yoluyla yapılan oylamada teklifin maddelerine geçilmesinin reddedildiği, oylama sırasında ya da sonrasında oylamaya ilişkin herhangi bir itirazın yapılmadığı belirtilmiştir. Bu kapsamda Türkiye Büyük Millet Meclisi İçtüzüğü'nün (İçtüzük) 139. maddesi uyarınca oylama sırasında beş milletvekilinin ayağa kalkması suretiyle sayıma itiraz edilmediği, Başkanlık Divanı üyeleri arasında uyuşmazlık bulunduğu dair bir kaydın 141. maddeye göre tutanağa geçirilmediği, bu hususta herhangi bir usul tartışmasının da açılmadığı, nitekim oylamadan sonra verilen aranın bitimini müteakip Birleşimin tekrar açıldığı ve Oturumu yöneten Başkan tarafından gündemin diğer maddesine geçildiği, böylece kanun teklifinin İçtüzük'ün 81. maddesinin beşinci fıkrasına göre reddedildiği ve Genel Kurulun bu yöndeki kararının kesinleştiği hususları ileri sürülmüştür.

4. Ayrıca, anılan Birleşimin ardından Birleşimde Kâtip Üye olarak görev yapan iki milletvekili ile İktidar Partisi Grup Başkanvekilinin İçtüzük'ün 13. maddesi uyarınca oylama sırasındaki yanlışlığın giderilmesi talebiyle TBMM Başkanlığına başvurdukları, itiraz dilekçelerinde; Oturumu yöneten Başkanın milletvekillerinden gelen itirazlar üzerine oyların sayımını yapacağını belirttiği hâlde sayım yapmadan hızlıca hareket ederek teklifin maddelerine geçilmesinin kabul edilmediğini ilan ettiğinin ve Kâtip Üyenin bu konudaki itirazlarını dikkate almadığının belirtildiği, anılan itiraz dilekçeleri üzerine Başkanın Başkanlık Divanını toplantıya çağırdığı ve Başkanlık Divanınca 1/4/2021 tarihinde, oylamada İçtüzük'ün 13. maddesine göre önemli bir yanlışlık olduğunun tespiti ile oylamanın yenilenmesi hususunun Genel Kurulun oyuna sunulmasına karar verildiği ifade edilmiştir.

5. Söz konusu itiraz dilekçelerinde yer alan iddiaların doğru olduğunun kabul edilmesi hâlinde dahi bu durumun yeniden oylama yapılmasına hukuki dayanak oluşturamayacağı zira İçtüzük'ün anılan maddesinde Başkanlık Divanına tanınan görev ve yetkinin yanlışlığın Birleşimden sonra anlaşılması

durumuyla sınırlı olduğu, itiraz dilekçelerinde ise Birleşimin kapanmasından sonra ortaya çıkan yeni bir durumdan bahsedilmediği, iddia edilen hususların Birleşimin devamı sırasında ortaya konulmasının ve bu konuda bir usul tartışması açılmak suretiyle düzeltilmesinin mümkün olduğu hâlde bunun yapılmadığı belirtilerek Başkanlık Divanının İçtüzük tarafından kendisine tanınmayan bir yetkiyi kullanarak aldığı 1/4/2021 tarihli kararın yok hükmünde olduğu, TBMM Başkanlığınca hazırlanan 1/4/2021 tarihli 67. Birleşimin gündeminde anılan kanun teklifine yer verilmediği, belirtilen Birleşimde görüşüleceği önceden bildirilmeyen teklifin gündeme alınması konusunda İçtüzük'ün 49. maddesi gereğince Danışma Kurulundan görüş alınmadığı ve bu hususun Genel Kurulca kararlaştırılmadığına dikkat çekilmiştir.

6. Açıklanan süreç çerçevesinde söz konusu kanun teklifinin görüşmelerine 1/4/2021 tarihinde devam edilmesinin eylemli İçtüzük değişikliği niteliğinde olduğu, TBMM Genel Kurulunun kanun teklifine ilişkin iradesinin 31/3/2021 tarihli 66. Birleşimde teklifin reddi yönünde olduğu, TBMM tarafından reddedilmiş olan kanun tekliflerinin İçtüzük'ün 76. maddesi uyarınca ret tarihinden itibaren bir tam yıl geçmedikçe TBMM'nin aynı yasama dönemi içinde yeniden verilemeyeceği, buna rağmen geçerliliği kalmayan söz konusu kanun teklifinin Başkanlık Divanının müdahalesiyle 1/4/2021 tarihli Birleşimde yeniden gündeme alınarak maddelere geçilmesinin bir kez daha oylandığı, görüşüldüğü ve kabul edildiği, geçersiz bir teklifin İçtüzük hükümlerine aykırı şekilde görüşülmesi durumunda kanunun varlığı için gerekli olan TBMM iradesinin olduğundan söz edilemeyeceği belirtilmiştir.

7. Bu iddialar bağlamında, eylemli İçtüzük değişikliği niteliğindeki işlemlere dayanılarak görüşülüp kabul edilen Kanun'un Anayasa'nın 87. ve 88. maddelerine aykırı olduğu belirtilerek öncelikle yokluğunun tespitine, aksi takdirde iptaline karar verilmesi gerektiği ileri sürülmüştür.

B. Kanun'un Yok Hükmünde Olduğunun Tespiti Talebinin İncelenmesi

8. Anayasa'nın 87. maddesinde kanun koymak, değiştirmek ve kaldırmak, TBMM'nin görev ve yetkileri arasında sayılmış; 89. maddesinde de Cumhurbaşkanının TBMM'ce kabul edilen kanunları on beş gün içinde yayımlayacağı, yayımlanmasını uygun bulmadığı kanunları ise bir daha görüşülmek üzere aynı süre içinde TBMM'ye geri göndereceği belirtilmiştir.

9. Kanun tekliflerinin TBMM'de görüşülerek kabul edilmesi, söz konusu teklifin kanunlaşması sonucunu doğurmakta; bir başka deyişle TBMM'nin teklifin kabulü yönündeki iradesi, kanunun varlık kazanması için gerekli ve yeterli bulunmaktadır. Cumhurbaşkanının bir kanunu yayımlaması, TBMM'nin bu yöndeki kabulü ile vücut bulan kanuna yeniden varlık sağlamadığı gibi bir daha görüşülmek üzere TBMM'ye geri göndermesi de kanunun varlığını ortadan kaldırmamaktadır. Belirtilen nedenle Cumhurbaşkanının kanunu yayımlama iradesi ve kanunun Resmî Gazete'de

yayımlanması, kanunun aleniyet kazanması ve yürürlüğe girmesi bakımından önem taşımaktadır (E.2018/34, K.2018/61, 31/5/2018, § 5).

10. Bir normun yokluğu, hukuk dünyasında hiç doğmamış olduğunun ifadesidir. Normun varlığı ise, o normun yürürlüğe girmesine ve uygulanmasına bağlı bulunmamaktadır. Varlık, yürürlük ve uygulanma kavramları birbirinden farklı olup varlık, bir normun hukuk âleminde vücut bulmasını ifade etmektedir. Kanunlar bakımından yokluk, parlamento iradesinin bulunmaması gibi durumlarda, başka bir ifadeyle bir normun varlığının zorunlu koşulları bulunmadığı takdirde söz konusu olabilecektir (E.2018/34, K.2018/61, 31/5/2018, § 6).

11. Yokluktan farklı olan hukuka aykırılık hâli ise hukuk âleminde var olan normun, hukukun öngördüğü usul ve esaslar çerçevesinde çıkarılmaması anlamını taşımaktadır. Hukuka aykırılık hâli ne kadar ağır ve açık olursa olsun bir normun hukuka aykırı olması, zorunlu koşullarının bulunması suretiyle var olan o normun yokluğu sonucunu doğurmaz. Bu nedenle kanunların veya kanun hükümlerinin Anayasa'ya uygunluk denetimi kapsamında incelenmesi gereken hususlarda Anayasa'ya aykırılığının tespiti, ilgili kanun veya kanun hükümlerinin yokluğunu değil iptalini gerekli kılar (E.2018/34, K.2018/61, 31/5/2018, § 7).

12. Dava dilekçesinde Kanun'un Anayasa'ya aykırılığı yolunda ileri sürülen hususlar Kanun'un varlık kazanmasını imkânsız kılan hâller kapsamına girmediğinden, Kanun'un Anayasa'ya uygunluk denetimi kapsamında incelenmesini ve bu inceleme neticesinde varılacak sonuca göre iptalini ya da iptal talebinin reddini gerekli kılmaktadır.

13. Açıklanan nedenlerle Kanun'un yok hükmünde olduğunun tespiti talebinin reddi gerekir.

Zühtü ARSLAN, Kadir ÖZKAYA ve Yusuf Şevki HAKYEMEZ bu görüşe farklı gerekçeyle katılmışlardır.

C. Kanun'un Şekil Bakımından Anayasa'ya Aykırı Olduğu Gerekçesiyle İptali Talebinin İncelenmesi

14. 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 43. maddesi uyarınca dava konusu Kanun, ilgisi nedeniyle Anayasa'nın 96. maddesi yönünden incelenmiştir.

15. Kanunların esas bakımından Anayasa'ya uygunluk denetimi; kanunun maddi olarak (hukuk dünyasında yarattığı değişiklik itibarıyla) Anayasa'ya uygun olup olmadığını ifade etmektedir. Şekil bakımından uygunluk ise teklifin kanunlaşabilmesi için, diğer bir anlatımla maddi olarak varlık

kazanabilmesi için Anayasa’da öngörülen usullere uyulup uyulmadığının denetimini ifade etmektedir.

16. Anayasa’nın 148. maddesinin ikinci fıkrasında, kanunların şekil bakımından denetlenmesinin son oylamanın öngörülen çoğunlukla yapılıp yapılmadığı hususu ile sınırlı olduğu hükme bağlanmıştır.

17. Anayasa’nın 148. maddesinin gerekçesinde de TBMM Genel Kurulu tarafından yapılan son oylamadan önce vücut bulan şekil bozukluklarını Genel Kurulun bildiği veya bilmesi gerektiğinin varsayıldığı belirtilerek son oylamadan önce yapılan şekil bozukluklarının iptale neden olamayacağı ifade edilmiş ve “Genel Kurulun oylama yapıp kanunu kabul etmesi, şekil bozukluğunu, o kanunu kabul etmemek için yeterli neden saymadığı yolunda bir irade tecellisidir. En büyük organ genel kuruldur. Onun iradesi hilafına bir sonuç çıkarmak hukukun ana esaslarına aykırı düşer. Bu nedenle son oylamadan önceki şekil bozuklukları, iptal sebebi sayılmamıştır.” denilmiştir.

18. Anayasa’nın 148. maddesinin açık hükmü ve gerekçesi karşısında kanunların şekil bakımından denetiminde, son oylamanın öngörülen çoğunlukla yapılıp yapılmadığından başka bir hususun esas alınmasına ve bu suretle kanunların şekil bakımından denetimlerinin yapılabilmesine imkân bulunmamaktadır.

19. Anayasa’nın “Toplantı ve karar yeter sayısı” başlıklı 96. maddesinde “Türkiye Büyük Millet Meclisi, yapacağı seçimler dahil bütün işlerinde üye tamsayısının en az üçte biri ile toplanır. Türkiye Büyük Millet Meclisi, Anayasada başkaca bir hüküm yoksa toplantıya katılanların salt çoğunluğu ile karar verir; ancak karar yeter sayısı hiçbir şekilde üye tamsayısının dörtte birinin bir fazlasından az olamaz.” denilmektedir. Bu çerçevede TBMM’nin bütün işlerinde üye tamsayısının en az üçte biri olan 200 milletvekiliyle toplanması, toplantıya katılanların salt çoğunluğuyla karar vermesi ve karar yeter sayısının hiçbir şekilde üye tamsayısının dörtte birinin bir fazlası olan 151 milletvekilinden az olmaması gerekmektedir.

20. Kanun’un görüşülmesine ilişkin TBMM Genel Kurul tutanaklarının incelenmesinden Kanun’un tümü üzerindeki oylamanın işaretle oylama yöntemiyle yapıldığı anlaşılmaktadır. İşaretle oylama sonucunun rakamsal olarak belirlenmeyip İçtüzük’ün 141. maddesi uyarınca Oturumu yöneten Başkan tarafından Genel Kurula “kabul edilmiştir” veya “kabul edilmemiştir” denilmek suretiyle ilan edilmesi karşısında, Kanun’un kabul edildiği Birleşimin, toplantı yeter sayısının bulunduğu belirtilerek açıldığı, Kanun’un tümünün oylaması sırasında toplantı ve karar yeter sayısının varlığı konusunda Başkanlık Divanınca tereddüde düşülmediği gibi herhangi bir milletvekili tarafından yeter sayının bulunmadığı yönünde bir itirazın da ileri sürülmediği gözetildiğinde son oylamanın Anayasa’nın 96. maddesinde öngörülen çoğunlukla yapıldığının kabulü gerekir.

21. Öte yandan dava dilekçesinde kanun teklifinin, İÇTÜZÜK'te öngörülen usul ve esaslara aykırı şekilde TBMM Genel Kurulunda gündeme alındığı, görüşüldüğü ve kabul edildiği, bu bağlamda; TBMM tarafından reddedilmiş olan kanun tekliflerinin ret tarihinden itibaren bir tam yıl geçmedikçe aynı yasama dönemi içinde yeniden verilemeyeceği, iddia edilen yanlışlığın oylama esnasında ileri sürülebilmesi mümkün olduğundan İÇTÜZÜK'ün 13. maddesi uyarınca işlem tesis edilmesine imkân bulunmadığı, Başkanlık Divanının İÇTÜZÜK tarafından kendisine tanınmayan bir yetkiyi kullanarak aldığı karara istinaden Birleşim gününde görüşüleceği önceden bildirilmeyen teklifin yeniden gündeme alındığı, teklifin gündeme alınması konusunda Danışma Kurulundan görüş alınmadığı ve bu hususun Genel Kurulca kararlaştırılmadığı, anılan durumların eylemli İÇTÜZÜK değişikliği niteliğinde olduğu ve Kanun'un eylemli İÇTÜZÜK değişikliği niteliğindeki bu işlemlere dayandığı ileri sürülmekte ise de bu iddialar Kanun'un şekil bakımından denetimini gerektirmektedir. Bununla birlikte Anayasa'nın 148. maddesinin ikinci fıkrası uyarınca şekil denetiminin son oylamanın öngörülen çoğunlukla yapılıp yapılmadığı hususuyla sınırlı olması nedeniyle yalnızca son oylama çoğunluğuyla ilgili bir denetim yapılmıştır.

22. Açıklanan nedenlerle son oylamasının Anayasa'da öngörülen çoğunlukla yapıldığı açık olan Kanun, Anayasa'nın 96. maddesine aykırı değildir. İptal talebinin reddi gerekir.

Kanun'un Anayasa'nın 87. ve 88. maddeleriyle ilgisi görülmemiştir.

IV. YÜRÜRLÜĞÜN DURDURULMASI TALEBİ

23. Dava dilekçesinde özetle, dava konusu Kanun'un uygulanması hâlinde telafisi güç veya imkânsız zararların doğabileceği belirtilerek yürürlüğünün durdurulmasına karar verilmesi talep edilmiştir.

7/4/2021 tarihli ve 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu'na yönelik iptali talebi 13/10/2021 tarihli ve E.2021/43, K.2021/74 sayılı kararla reddedildiğinden bu Kanun'a ilişkin yürürlüğün durdurulması talebinin REDDİNE 13/10/2021 tarihinde OYBİRLİĞİYLE karar verilmiştir.

V. HÜKÜM

7/4/2021 tarihli ve 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu'nun;

A. Yok hükmünde olduğunun tespiti talebinin REDDİNE,

B. Şekil bakımından Anayasa'ya aykırı olmadığına ve iptali talebinin REDDİNE,

13/10/2021 tarihinde OYBİRLİĞİYLE karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili - Hasan Tahsin GÖKCAN

Başkanvekili - Kadir ÖZKAYA

Üye: Engin YILDIRIM; Hicabi DURSUN; Muammer TOPAL; M. Emin KUZ; Rıdvan GÜLEÇ; Recai AKYEL; Yusuf Şevki HAKYEMEZ; Yıldız SEFERİNOĞLU; Selahaddin MENTEŞ; Basri BAĞCI; İrfan FİDAN

FARKLI GEREKÇE

1. Dava konusu Kanun'un tümünün yok hükmünde olduğunun tespiti talebi yokluk kararı verilmesinin şartları oluşmadığından, çoğunluğun ifadesiyle "ileri sürülen hususlar Kanun'un varlık kazanmasını imkânsız kılan hâller kapsamına girmediğinden" reddedilmiştir (§ 12).

2. Çoğunluğun bu konudaki red kararına Anayasa Mahkemesinin 10/4/2014 tarihli ve E.2014/57, K.2014/81 sayılı kararı ile 31/5/2018 tarihli ve E. 2018/42, K.2018/48 sayılı kararına yazdığım farklı gerekçeyle katılıyorum.

Başkan - Zühtü ARSLAN

FARKLI GEREKÇE

Mahkememiz çoğunluğu, dava dilekçesinde ileri sürülen hususların "Kanun'un varlık kazanmasını imkânsız kılan hâller kapsamına girmediğinden" yok hükmünde olduğunun tespiti yönündeki talebin reddine karar vermiştir.

Çoğunluğun red sonucuna, Anayasa Mahkemesinin 31/5/2018 tarihli ve E.2018/42, K.2018/48 sayılı kararında Başkan Zühtü ARSLAN'ın yazdığı farklı gerekçeyle katılıyorum.

Başkanvekili - Kadir ÖZKAYA

FARKLI GEREKÇE

Mahkememiz çoğunluğunun dava dilekçesinde ileri sürülen hususların "Kanun'un varlık kazanmasını imkânsız kılan hâller kapsamına girmediğinden" 7/4/2021 tarihli ve 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu'nun yok hükmünde olduğunun tespiti yönündeki talebin reddine ilişkin kanaatine Anayasa Mahkemesinin 31/5/2018 tarihli ve E.2018/42, K.2018/48 sayılı kararına Başkan Zühtü ARSLAN'ın yazdığı farklı gerekçe ile katılmaktayım.

Üye - Yusuf Şevki HAKYEMEZ

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2020/41

Karar Sayısı: 2021/91

Karar Tarihi: 16/12/2021

RG Tarih-Sayısı: 25/2/2022 - 31761

İTİRAZ YOLUNA BAŞVURAN: Ankara Bölge İdare Mahkemesi 1. İdare Dava Dairesi

İTİRAZIN KONUSU: 10/3/2011 tarihli ve 6191 sayılı Sözleşmeli Erbaş ve Er Kanunu'nun 3. maddesinin (3) numaralı fıkrasının 1/2/2018 tarihli ve 7078 sayılı Kanun'un 159. maddesiyle değiştirilen (f) bendinin Anayasa'nın 13., 20. ve 128. maddelerine aykırılığı ileri sürülerek iptaline karar verilmesi talebidir.

OLAY: Hakkında yapılan güvenlik soruşturmasının olumlu bulunmadığı gerekçesiyle sözleşmeli er adaylığının sonlandırılmasına ilişkin işlemin iptali talebiyle açılan davada itiraz konusu kuralın Anayasa'ya aykırı olduğu kanısına varan Mahkeme, iptali için başvurmuştur.

I. İPTALİ İSTENEN KANUN HÜKMÜ

Kanun'un itiraz konusu kuralın da yer aldığı 3. maddesi şöyledir:

“Kaynak

MADDE 3- (1) (Değişik: 10/12/2014-6582/ 2 md.) Sözleşmeli er kaynaklarını;

a) En az ilköğretim veya yurt dışındaki dengi okul mezunu olup, askerlik hizmetini erbaş ve er olarak tamamlamış ve düzeltilmemiş nüfus kaydına göre müracaat yapılan yılın ocak ayının ilk günü itibarıyla yirmi beş yaşını bitirmemiş olanlar,

b) En az ortaöğretim veya yurt dışındaki dengi okul mezunu olup, askerlik hizmetine başlamamış veya askerlik hizmetini tamamlamamış olanlardan, düzeltilmemiş nüfus kaydına göre müracaat yapılan yılın ocak ayının ilk günü itibarıyla yirmi yaşından gün almış ve yirmi beş yaşını bitirmemiş olanlar,

teşkil eder.

Ayrıca, (a) bendinde sayılanlardan askerlik hizmetine başlamamış veya askerlik hizmetini tamamlamamış olanların, (b) bendi kapsamında sözleşmeli erliğe alınıp alınmayacakları kaynak ihtiyacı dikkate alınarak Millî Savunma Bakanlığı tarafından belirlenir.

(2) Askerî okullardan ve Türk Silahlı Kuvvetlerinden her ne sebeple olursa olsun ilişkileri kesilen personel sözleşmeli er olarak alınmaz.

(3) Sözleşmeli erlik için aşağıdaki nitelikler aranır:

a) Türk vatandaşı olmak.

b) Bu Kanunda belirtilen öğrenim ile ilgili şartları taşımak.

c) Sağlık ile ilgili Türk Silahlı Kuvvetleri Sağlık Yeteneği Yönetmeliğinde belirtilen şartları taşımak.

ç) Kamusal hakları kullanmaktan yoksun bırakılmamış olmak.

d) Cezaları ertelenmiş, seçenek yaptırımlardan birisine çevrilmiş, genel ya da özel af kanunları kapsamına girmiş veya haklarında hükmün açıklanmasının geri bırakılmasına karar verilmiş olsa dahi;

1) Devletin güvenliğine karşı işlenen suçlar, halkı askerlikten soğutmak, Türk Milletini, Türkiye Cumhuriyeti Devletini, Devletin kurum ve organlarını aşağılama ile zimmet, irtikâp, iftira, rüşvet, hırsızlık, dolandırıcılık, sahtecilik, güveni kötüye kullanma, yalan tanıklık, yalan yere yemin, suç uydurma, cinsel saldırı, cinsel taciz, kişiyi hürriyetinden yoksun bırakmak, fuhuş, gayri tabii mukarenet, hileli iflas gibi yüz kızartıcı veya şeref ve haysiyet kırıcı suçlar ile kaçakçılık, ihaleye fesat karıştırma, Devlet sırlarını açığa vurma suçlarından,

2) Firar, amir veya üste fiilen taarruz, emre itaatsizlikte ısrar, üste hakaret, mukavemet, fesat ve isyan suçlarından,

3) 22/5/1930 tarihli ve 1632 sayılı Askerî Ceza Kanununun 148 inci maddesinde belirtilen suçlardan, birisinden mahkûm olmamak.

e) Taksirli suçlar hariç olmak üzere bir suçtan bir ay veya daha fazla hapis cezası ile mahkûm olmamak.

f) (Değişik: 15/8/2017-KHK-694/164 md.; Aynen kabul: 1/2/2018-7078/159 md.) Güvenlik soruşturması olumlu sonuçlanmış olmak; güvenlik soruşturmasının sonucunun henüz gelmediği hallerde arşiv araştırması olumlu sonuçlanmış olmak.

g) Yapılacak fiziki kabiliyet testi ve mülakatlarda başarılı olmak.

(4) Asgari tugay veya eşidi birlik komutanı veya kurum amiri tarafından haklarında “sözleşmeli erbaş ve er olur” belgesi düzenlenen personelin müracaatları öncelikle kabul edilir.”

II. İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Serdar ÖZGÜLDÜR, Engin YILDIRIM, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĞLU ve Selahattin MENTEŞ’in katılımlarıyla yapılan ilk inceleme toplantısında dosyada eksiklik bulunmadığından işin esasının incelenmesine 6/5/2020 tarihinde OYBİRLİĞİYLE karar verilmiştir.

III. ESASIN İNCELENMESİ

2. Başvuru kararı ve ekleri, Raportör Aydın AYGÜN tarafından hazırlanan işin esasına ilişkin rapor, dava konusu kanun hükmü, dayanan Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A. Sınırlama Sorunu

3. Anayasa'nın 152. ile 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 40. maddelerine göre bir davaya bakmakta olan mahkeme, bu dava sebebiyle uygulanacak bir kanunun veya Cumhurbaşkanlığı kararnamesinin hükümlerini Anayasa'ya aykırı görmesi hâlinde veya taraflardan birinin ileri sürdüğü aykırılık iddiasının ciddi olduğu kanısına varması durumunda bu hükümlerin iptalleri için Anayasa Mahkemesine başvurmaya yetkilidir. Ancak anılan maddeler uyarınca bir mahkemenin Anayasa Mahkemesine başvurabilmesi için elinde yöntemince açılmış ve mahkemenin görevine giren bir davanın bulunması, iptali talep edilen kuralın da o davada uygulanacak olması gerekir. Uygulanacak kural ise bakılmakta olan davanın değişik evrelerinde ortaya çıkan sorunların çözümünde veya davayı sonuçlandırmada olumlu ya da olumsuz yönde etki yapacak nitelikte bulunan kurallardır.

4. Başvuru kararında 6191 sayılı Kanun'un 3. maddesinin (3) numaralı fıkrasının (f) bendinin iptali talep edilmiştir. İtiraz konusu kural sözleşmeli er olabilmek için güvenlik soruşturmasının olumlu sonuçlanmış olmasını, güvenlik soruşturmasının sonucunun henüz gelmediği hâllerde ise arşiv araştırmasının olumlu sonuçlanmış olması şartını öngörmektedir.

5. Kuralın öngördüğü güvenlik soruşturması ve arşiv araştırması faaliyetleri, 26/10/1994 tarihli ve 4045 sayılı Kanun hükümlerine göre yürütülmekte iken anılan Kanun'un 7/4/2021 tarihli ve 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu'yla yürürlükten kaldırılması üzerine

anılan faaliyetler 17/4/2021 tarihinden itibaren 7315 sayılı Kanun hükümlerine göre yürütülmeye devam edilmiştir. Bu itibarla kural hem mülga 4045 sayılı Kanun hem de 7315 sayılı Kanun uyarınca gerçekleştirilen güvenlik soruşturması ve arşiv araştırması faaliyetleri bakımından geçerli, ortak kural niteliğindedir.

6. Bakılmakta olan davanın konusunu ise mülga 4045 sayılı Kanun hükümleri çerçevesinde gerçekleştirilen güvenlik soruşturması ve arşiv araştırması faaliyeti oluşturmaktadır. Bu nedenle kurala ilişkin esas incelemenin “mülga 26/10/1994 tarihli ve 4045 sayılı Kanun uyarınca yapılan güvenlik soruşturması ve arşiv araştırması” yönünden yapılması gerekir.

B. Anlam ve Kapsam

7. İtiraz konusu kuralla sözleşmeli er olabilmek için güvenlik soruşturmasının olumlu sonuçlanmış olması, güvenlik soruşturmasının sonucunun henüz gelmediği hâllerde ise arşiv araştırmasının olumlu sonuçlanmış olması şartı öngörülmekte olup kural “mülga 26/10/1994 tarihli ve 4045 sayılı Kanun uyarınca yapılan güvenlik soruşturması ve arşiv araştırması” yönünden incelenmiştir.

8. Bu itibarla sözleşmeli er olabilmek için her hâlükârda güvenlik soruşturmasının olumlu sonuçlanmış olması gerekmele birlikte güvenlik soruşturmasının henüz sonuçlanmadığı durumlarda arşiv araştırmasının sonucunun olumlu olması şartıyla sözleşmeli er olmaya ilişkin sürecin başlatılması mümkündür. Kuralın gerekçesinde bu durum “...sözleşmeli erbaş ve erlerin güvenlik soruşturmaları sonuçlanmadan eğitimlerine başlatılamamaları nedeniyle, Türk Silahlı Kuvvetlerinin ihtiyaç duyduğu sözleşmeli erbaş ve er temininin kısa vadede gerçekleştirilebilmesi için arşiv araştırması sonucuna göre eğitime başlatılabilmelerine olanak sağlaması amaçlanmaktadır.” şeklinde ifade edilmiştir.

C. İtirazın Gerekçesi

9. Başvuru kararında özetle; itiraz konusu kuralın sözleşmeli er olabilmek için güvenlik soruşturmasının olumlu sonuçlanmasını şartını aradığı ancak güvenlik soruşturması ve arşiv araştırmasını düzenleyen kanunun yalnızca hangi kamu görevlileri bakımından güvenlik soruşturması yapılacağını belirttiği, güvenlik soruşturması ve arşiv araştırmasıyla ilgili diğer hususları yönetmeliğe bıraktığı, güvenlik soruşturması ve arşiv araştırmasına konu bilgi ve belgelerin neler olduğu, bu bilgi ve belgelerin nerelerden elde edileceği, ne suretle ve ne kadar süreyle saklanacağı, kişilerin söz konusu bilgilere itiraz etme imkânının bulunup bulunmadığı konularının kanunda düzenlenmediği, hangi suçlardan mahkûmiyetin ya da kamu davasının açılmasının ertelenmesinin ya da hükmün açıklanmasının geri bırakılmasının güvenlik soruşturmasını olumsuz

etkileyeceği hususunda da bir düzenlemeye yer verilmediği, Anayasa Mahkemesinin yakın tarihte itiraz konusu kuralla benzer düzenlemelerin iptallerine karar verdiği belirtilerek kuralın Anayasa'nın 13., 20. ve 128. maddelerine aykırı olduğu ileri sürülmüştür.

Ç. Anayasa'ya Aykırılık Sorunu

10. Anayasa'nın 20. maddesinin birinci fıkrasında herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş; üçüncü fıkrasında da "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." denilerek kişisel verilerin korunması özel hayatın gizliliğinin korunması kapsamında güvenceye kavuşturulmuştur.

11. Kişisel verilerin korunmasını isteme hakkı, insan onurunun korunması ve bireyin kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır.

12. Anayasa Mahkemesinin yerleşik kararlarında belirtildiği üzere "...adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler..." kişisel veri olarak kabul edilmektedir (AYM, E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2014/74, K.2014/201, 25/12/2014; E.2014/180, K.2015/30, 19/3/2015; E.2015/32, K.2015/102, 12/11/2015).

13. Bu bağlamda güvenlik soruşturması ve arşiv araştırmasıyla elde edilen veriler kişisel veri niteliğindedir. İtiraz konusu kural, güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimler tarafından güvenlik soruşturması ve arşiv araştırması kapsamında kişilerin kişisel veri niteliğindeki özel hayatı, iş ve sosyal yaşamıyla ilgili bilgilerinin alınmasına ve bu kayıtların kullanılmasına imkân tanınması nedeniyle kişisel verilerin korunmasını isteme hakkına sınırlama getirmektedir.

14. Anayasa'nın 20. maddesi uyarınca kişisel veriler ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir. Anayasa'nın 13. maddesinde de "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz." hükmüne yer verilerek temel hak ve özgürlüklerin ancak kanunla sınırlanabileceği ifade edilmiştir. Anayasa'nın 13. ve 20. maddeleri uyarınca kişisel verilerin korunmasını isteme hakkını sınırlamaya yönelik kanuni bir düzenlemenin şeklen var olması yeterli olmayıp yasal kuralların keyfiliğe izin vermeyecek şekilde belirli, ulaşılabilir ve öngörülebilir düzenlemeler niteliğinde olması gerekir.

15. Esasen temel hakları sınırlayan kanunun bu niteliklere sahip olması, Anayasa'nın 2. maddesinde güvenceye bağlanan hukuk devleti ilkesinin de bir gereğidir. Hukuk devletinde, kanuni düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi gerekir. Kanunda bulunması gereken bu nitelikler hukuki güvenliğin sağlanması bakımından da zorunludur. Zira bu ilke hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar (AYM, E.2015/41, K.2017/98, 4/5/2017, §§ 153, 154). Dolayısıyla Anayasa'nın 13. ve 20. maddelerinde sınırlama ölçütü olarak belirtilen kanunilik, Anayasa'nın 2. maddesinde güvenceye bağlanan hukuk devleti ilkesi ışığında yorumlanmalıdır.

16. Anayasa'nın 129. maddesinin birinci fıkrasında memurlar ve kamu görevlilerinin Anayasa ve kanunlara sadık kalarak faaliyette bulunma yükümlülükleri düzenlenmiştir. Belirtilen husus gözetilerek kamu görevinde çalıştırılacak kişiler bakımından güvenlik soruşturması ve arşiv araştırması yapılması yönünde düzenlemeler getirilmesi kanun koyucunun takdir yetkisindedir. Ancak bu alanda düzenleme öngören kuralların kamu makamlarına hangi koşullarda ve hangi sınırlar içinde tedbirler uygulama ve özel hayata saygı gösterilmesini isteme hakkına yönelik müdahalelerde bulunma yetkisi verildiğini yeterince açık olarak göstermesi ve muhtemel kötüye kullanmalara karşı yeterli güvenceleri sağlaması gerekir.

17. Anayasa Mahkemesi 24/7/2019 tarihli ve E.2018/73, K.2019/65 sayılı, 19/2/2020 tarihli ve E.2018/163, K.2020/13 sayılı ile 3/6/2021 tarihli ve E.2020/24, K.2021/39 sayılı kararlarında güvenlik soruşturması ve arşiv araştırması yapılmasını öngören kuralları incelemiştir. Bu kararlarda Anayasa ve kanunlara sadık kalarak faaliyette bulunma yükümlülükleri olan memurların ve kamu

görevlilerinin kamu görevlerine atanmalarında birtakım şartların aranmasının doğal olduğu, bu kapsamda kamu görevine atanmadan önce kişilerin güvenlik soruşturmasının ve arşiv araştırmasının yapılmasını öngören kuralların kanun koyucunun takdir yetkisinde bulunduğu belirtilmiştir. Bununla birlikte anılan kararlarda güvenlik soruşturması ve arşiv araştırmasının yapılmasına ve elde edilecek verilen kullanılmasına ilişkin temel ilkelerin kanunda düzenlenmesi gerektiği ifade edilmiştir (bkz. sırasıyla §§ 170, 171; §§ 15, 16; §§ 47, 48).

18. Kuralla güvenlik soruşturması ve arşiv araştırmasının olumlu sonuçlanmış olması sözleşmeli er alımında bulunması gereken şart olarak düzenlenmesine karşın 17/4/2021 tarihinden önceki süreç yönünden kanunda güvenlik soruşturmasına ve arşiv araştırmasına konu edilecek kişisel veri niteliğindeki bilgi ve belgelerin ne şekilde kullanılacağına, hangi mercilerin soruşturma ve araştırmayı yapacağına, bu bilgilerin ne suretle ve ne kadar süre ile saklanacağına, ilgililerin söz konusu bilgilere itiraz etme imkânının olup olmadığına, bilgilerin bir müddet sonra silinip silinmeyeceğine, silinecekse bu sırada izlenecek usulün ne olduğuna, yetkinin kötüye kullanımını önlemeye yönelik nasıl bir denetim yapılacağına ilişkin herhangi bir düzenlemeye yer verilmemiştir. Diğer bir ifadeyle güvenlik soruşturması ve arşiv araştırmasının yapılmasına, elde edilecek verilerin kullanılmasına ilişkin temel ilkeler belirlenmeksizin kuralla sadece güvenlik soruşturması ve arşiv araştırması yapılması sözleşmeli er alımlarında aranacak şartlar arasında sayılmıştır.

19. Güvenlik soruşturması ve arşiv araştırması sonucunda kişisel veri niteliğindeki bilgilerin alınmasına, kullanılmasına, işlenmesine yönelik güvenceler ve temel ilkeler kanunla belirlenmeksizin bunların alınmasına ve kullanılmasına izin verilmesi Anayasa'nın 13. ve 20. maddeleriyle bağdaşmamaktadır (benzer yöndeki kararlar için bkz. AYM, E.2018/73, K.2019/65, 24/7/2019, §§ 171, 172; E.2018/163, K.2020/13, 19/2/2020, §§ 16, 17; E.2018/91, K.2020/10, 19/2/2020, §§ 133, 134; E.2020/24, K.2021/39, 3/6/2021, §§ 48, 49; Fatih Saraman [GK], B. No: 2014/7256, §§ 89, 90; Turgut Duman, B. No: 2014/15365, § 88).

20. Açıklanan nedenlerle kural Anayasa'nın 13. ve 20. maddelerine aykırıdır. İptali gerekir.

Kural Anayasa'nın 13. ve 20. maddelerine aykırı görülerek iptal edildiğinden ayrıca Anayasa'nın 128. maddesi yönünden incelenmemiştir.

IV. HÜKÜM

10/3/2011 tarihli ve 6191 sayılı Sözleşmeli Erbaş ve Er Kanunu'nun 3. maddesinin (3) numaralı fıkrasının 1/2/2018 tarihli ve 7078 sayılı Kanun'un 159. maddesiyle değiştirilen (f) bendinin;

A. Esasına ilişkin incelemenin “mülga 26/10/1994 tarihli ve 4045 sayılı Kanun uyarınca yapılan güvenlik soruşturması ve arşiv araştırması” yönünden yapılmasına,

B. “mülga 26/10/1994 tarihli ve 4045 sayılı Kanun uyarınca yapılan güvenlik soruşturması ve arşiv araştırması” yönünden Anayasa’ya aykırı olduğuna ve İPTALİNE,

16/12/2021 tarihinde OYBİRLİĞİYLE karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili - Hasan Tahsin GÖKCAN

Başkanvekili - Kadir ÖZKAYA

Üye: Engin YILDIRIM; Hicabi DURSUN; Celal Mümtaz AKINCI; Muammer TOPAL; M. Emin KUZ;
Rıdvan GÜLEÇ; Recai AKYEL; Yusuf Şevki HAKYEMEZ; Yıldız SEFERİNOĞLU; Selahaddin
MENTEŞ; Basri BAĞCI; İrfan FİDAN

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2020/24

Karar Sayısı: 2021/39

Karar Tarihi: 03.06.2021

Resmî Gazete Tarih-Sayısı: 27/7/2021-31550

İTİRAZ YOLUNA BAŞVURANLAR:

1. Ankara Bölge İdare Mahkemesi 1. İdare Dava Dairesi (E.2020/24)
2. Ankara Bölge İdare Mahkemesi 1. İdare Dava Dairesi (E.2020/39)
3. Ankara Bölge İdare Mahkemesi 1. İdare Dava Dairesi (E.2020/40)

İTİRAZLARIN KONUSU: 26/10/1994 tarihli ve 4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun'un 1. maddesinin Anayasa'nın 13., 20. ve 128. maddelerine aykırılığı ileri sürülerek iptaline karar verilmesi talebidir.

OLAY: Davacıların haklarındaki güvenlik soruşturmalarının olumlu bulunmaması nedeniyle infaz ve koruma memurluğu ile uzman erbaşlığa atanma işlemlerinin sonlandırılmasına ilişkin işlemlerin iptalleri talebiyle açtıkları davalarda itiraz konusu kuralın Anayasa'ya aykırı olduğu kanısına varan Mahkeme, iptali için başvurmuştur.

I. İPTALİ İSTENEN KANUN HÜKMÜ

Kanun'un itiraz konusu 1. maddesi şöyledir:

"Madde 1- Güvenlik Soruşturması ve Arşiv Araştırması; kamu kurum ve kuruluşlarında, yetkili olmayan kişilerin bilgi sahibi olmaları halinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile Genelkurmay Başkanlığı, Milli Savunma Bakanlığı, jandarma, emniyet, sahil güvenlik ve istihbarat teşkilatlarında çalıştırılacak kamu personeli ve ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında yapılır.

(Ek:18/10/2018-7148/29 md.) Güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimler, güvenlik soruşturması ve arşiv araştırması kapsamında bakanlıklar ile kamu kurum ve kuruluşları arşivlerinden ve elektronik bilgi işlem merkezlerinden bilgi ve belge almaya, 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun 171 inci maddesinin beşinci ve 231 inci maddesinin onüçüncü fıkraları kapsamında tutulan kayıtlara ulaşmaya, Cumhuriyet başsavcılıkları tarafından yürütülen soruşturma sonuçlarını, kovuşturmaya yer olmadığına dair kararlar ile kesinleşmiş mahkeme kararlarını almaya yetkilidir.

Devletin güvenliğini, ulusun varlığını ve bütünlüğünü iç ve dış menfaatlerinin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeler ile gizlilik dereceli kamu personeli ile meslek gruplarının tespiti, birim ve kısımların tanımlarının yapılması, güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak merciler ve üst kademe yöneticilerinin kimler olduğu Cumhurbaşkanınca yürürlüğe konulacak yönetmelik ile düzenlenir.”

II. İLK İNCELEME

A. E.2020/24 Sayılı Başvuru Yönünden

1. Anayasa Mahkemesi İçtüzüğü (İçtüzük) hükümleri uyarınca Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Recep KÖMÜRCÜ, Serdar ÖZGÜLDÜR, Burhan ÜSTÜN, Engin YILDIRIM, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Kadir ÖZKAYA, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĞLU ve Selahaddin MENTEŞ'in katılımlarıyla 19/2/2020 tarihinde yapılan ilk inceleme toplantısında öncelikle uygulanacak kural ve sınırlama sorunları görüşülmüştür.

2. Anayasa'nın 152. ile 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 40. maddelerine göre bir davaya bakmakta olan mahkeme, bu dava sebebiyle uygulanacak bir kanunun veya Cumhurbaşkanlığı kararnamesinin hükümlerini Anayasa'ya aykırı görmesi hâlinde veya taraflardan birinin ileri sürdüğü aykırılık iddiasının ciddi olduğu kanısına varması durumunda bu hükümlerin iptali için Anayasa Mahkemesine başvurmaya yetkilidir. Ancak anılan maddeler uyarınca bir mahkemenin Anayasa Mahkemesine başvurabilmesi için elinde yöntemince açılmış ve mahkemenin görevine giren bir davanın bulunması, iptali talep edilen kuralın da o davada uygulanacak olması gerekir. Uygulanacak kural ise bakılmakta olan davanın değişik evrelerinde ortaya çıkan sorunların çözümünde veya davayı sonuçlandırmada olumlu ya da olumsuz yönde etki yapacak nitelikte bulunan kurallardır.

3. İtiraz yoluna başvuran Mahkeme 4045 sayılı Kanun'un 1. maddesinin iptalini talep etmiştir.

4. Bakılmakta olan dava, Jandarma Genel Komutanlığına uzman erbaş temini için açılan sınavda başarılı olan ancak hakkında yapılan güvenlik soruşturması ve arşiv araştırmasının olumsuz bulunması nedeniyle uzman erbaş adaylığı sonlandırılan davacının bu yöndeki işlemin iptali talebine ilişkindir.

5. Bakılmakta olan davanın konusunu jandarma personeli hakkında yapılan güvenlik soruşturması ve arşiv araştırması oluşturmaktadır. Dolayısıyla anılan Kanun'un 1. maddesinin birinci fıkrası uyarınca hakkında güvenlik soruşturması ve arşiv araştırması yapılacağı belirtilen diğer personel uyumsuzluk kapsamında değildir.

6. Bu itibarla 4045 sayılı Kanun'un itiraz konusu 1. maddesinin birinci fıkrasının "...kamu kurum ve kuruluşlarında, yetkili olmayan kişilerin bilgi sahibi olmaları halinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile Genelkurmay Başkanlığı, Milli Savunma Bakanlığı, ... emniyet, sahil güvenlik ve istihbarat ... ve ceza infaz kurumları ve tutukevlerinde çalışacak personel..." bölümünün bakılmakta olan davada uygulanma imkânı bulunmadığından bu bölüme ilişkin başvurunun Mahkemenin yetkisizliği nedeniyle reddi gerekir.

7. Öte yandan anılan maddenin birinci fıkrasının kalan kısmı ile ikinci fıkrası, bakılmakta olan davaya konu jandarma personelinin yanı sıra bakılmakta olan davada uygulanma imkânı bulunmayan hakkında güvenlik soruşturması ve arşiv araştırması yapılacak diğer personel bakımından da geçerli ortak kural niteliğindedir. Dolayısıyla bakılmakta olan davanın konusu gözetilerek esas incelemenin birinci fıkrada yer alan "...jandarma,..." ibaresi ile sınırlı olarak yapılması gerekir.

8. Maddenin güvenlik soruşturması ve arşiv araştırmasının usul ve esaslarının yönetmelikle düzenleneceğini öngören üçüncü fıkrası da hakkında güvenlik soruşturması ve arşiv araştırması yapılacak tüm personel bakımından geçerli ortak kural niteliğindedir. Bakılmakta olan davanın konusu gözetilerek anılan fıkranın esasına ilişkin incelemenin "...jandarma,..." ibaresi yönünden yapılması gerekir.

9. Açıklanan nedenlerle 26/10/1994 tarihli ve 4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun'un 1. maddesinin;

A. Birinci fıkrasının;

1. "...kamu kurum ve kuruluşlarında, yetkili olmayan kişilerin bilgi sahibi olmaları halinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile Genelkurmay Başkanlığı, Milli Savunma Bakanlığı, ... emniyet, sahil güvenlik ve istihbarat ... ve ceza infaz kurumları ve tutukevlerinde çalışacak personel..." bölümünün itiraz başvurusunda bulunan Mahkemenin bakmakta olduğu davada uygulanma imkânı bulunmadığından bu bölüme ilişkin başvurunun Mahkemenin yetkisizliği nedeniyle REDDİNE,

2. Kalan kısmının esasının incelenmesine, esasa ilişkin incelemenin "...jandarma,..." ibaresi ile sınırlı olarak yapılmasına,

B. İkinci ve üçüncü fıkralarının esasının incelenmesine, esasa ilişkin incelemenin birinci fıkrada yer alan "...jandarma,..." ibaresi yönünden yapılmasına

OYBİRLİĞİYLE karar verilmiştir.

B. E.2020/39 Sayılı Başvuru Yönünden

10. İhtüzük hükümleri uyarınca Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Serdar ÖZGÜLDÜR, Engin YILDIRIM, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĞLU ve Selahattin MENTEŞ'in katılımlarıyla 6/5/2020 tarihinde yapılan ilk inceleme toplantısında öncelikle uygulanacak kural ve sınırlama sorunları görüşülmüştür.

11. İtiraz yoluna başvuran Mahkeme 4045 sayılı Kanun'un 1. maddesinin iptalini talep etmiştir.

12. Bakılmakta olan dava, Millî Savunma Bakanlığına uzman erbaş temini için açılan sınavda başarılı olan ancak hakkında yapılan güvenlik soruşturması ve arşiv araştırmasının olumsuz bulunması nedeniyle uzman erbaş adaylığı sonlandırılan davacının bu yöndeki işlemin iptali talebine ilişkindir.

13. Bakılmakta olan davanın konusunu Millî Savunma Bakanlığı personeli hakkında yapılan güvenlik soruşturması ve arşiv araştırması oluşturmaktadır. Dolayısıyla anılan Kanun'un 1. maddesinin birinci fıkrası uyarınca hakkında güvenlik soruşturması ve arşiv araştırması yapılacağı belirtilen diğer personel uyumsuzluk kapsamında değildir.

14. Bu itibarla 4045 sayılı Kanun'un itiraz konusu 1. maddesinin birinci fıkrasının "...kamu kurum ve kuruluşlarında, yetkili olmayan kişilerin bilgi sahibi olmaları halinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile Genelkurmay Başkanlığı, ... jandarma, emniyet,

sahil güvenlik ve istihbarat ... ve ceza infaz kurumları ve tutukevlerinde çalışacak personel..." bölümünün bakılmakta olan davada uygulanma imkânı bulunmadığından bu bölüme ilişkin başvurunun Mahkemenin yetkisizliği nedeniyle reddi gerekir.

15. Öte yandan anılan maddenin birinci fıkrasının kalan kısmı, bakılmakta olan davaya konu Millî Savunma Bakanlığı personelinin yanı sıra bakılmakta olan davada uygulanma imkânı bulunmayan hakkında güvenlik soruşturması ve arşiv araştırması yapılacak diğer personel bakımından da geçerli ortak kural niteliğindedir. Dolayısıyla bakılmakta olan davanın konusu gözetilerek esas incelemenin birinci fıkrada yer alan "...Millî Savunma Bakanlığı,..." ibaresi ile sınırlı olarak yapılması gerekir.

16. Kanun'un itiraz konusu 1. maddesinin ikinci fıkrası ise Anayasa Mahkemesinin 19/2/2020 tarihli ve E.2018/163, K.2020/13 sayılı kararıyla iptal edilmiş ve bu iptal kararı 28/4/2020 tarihli ve 31112 sayılı Resmî Gazete'de yayımlanmıştır. Bu nedenle anılan fıkraya yönelik iptal talebi hakkında karar verilmesine yer olmadığına karar vermek gerekir.

17. Maddenin güvenlik soruşturması ve arşiv araştırmasının usul ve esaslarının yönetmelikle düzenleneceğini öngören üçüncü fıkrası ise hakkında güvenlik soruşturması ve arşiv araştırması yapılacak tüm personel bakımından geçerli ortak kural niteliğindedir. Bakılmakta olan davanın konusu gözetilerek anılan fıkranın esasına ilişkin incelemenin "...Millî Savunma Bakanlığı,..." ibaresi yönünden yapılması gerekir.

18. Açıklanan nedenlerle 26/10/1994 tarihli ve 4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun'un 1. maddesinin;

A. Birinci fıkrasının;

1. "...kamu kurum ve kuruluşlarında, yetkili olmayan kişilerin bilgi sahibi olmaları halinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile Genelkurmay Başkanlığı, ... jandarma, emniyet, sahil güvenlik ve istihbarat ... ve ceza infaz kurumları ve tutukevlerinde çalışacak personel..." bölümünün itiraz başvurusunda bulunan Mahkemenin bakılmakta olduğu davada uygulanma imkânı bulunmadığından bu bölüme ilişkin başvurunun Mahkemenin yetkisizliği nedeniyle REDDİNE,

2. Kalan kısmının esasının incelenmesine, esasa ilişkin incelemenin "...Millî Savunma Bakanlığı,..." ibaresi ile sınırlı olarak yapılmasına,

B. İkinci fıkrası hakkında KARAR VERİLMESİNE YER OLMADIĞINA,

C. Üçüncü fıkrasının esasının incelenmesine, esasa ilişkin incelemenin birinci fıkrada yer alan "...Milli Savunma Bakanlığı,..." ibaresi yönünden yapılmasına

OYBİRLİĞİYLE karar verilmiştir.

C. E.2020/40 Sayılı Başvuru Yönünden

19. İçtüzük hükümleri uyarınca Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Serdar ÖZGÜLDÜR, Engin YILDIRIM, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĞLU ve Selahattin MENTEŞ'in katılımlarıyla 6/5/2020 tarihinde yapılan ilk inceleme toplantısında öncelikle uygulanacak kural ve sınırlama sorunları görüşülmüştür.

20. İtiraz yoluna başvuran Mahkeme 4045 sayılı Kanun'un 1. maddesinin iptalini talep etmiştir.

21. Bakılmakta olan dava, infaz ve koruma memuru temini için açılan sınavda başarılı olan ancak hakkında yapılan güvenlik soruşturması ve arşiv araştırmasının olumsuz bulunması nedeniyle ataması iptal edilen davacının bu yöndeki işlemin iptali talebine ilişkindir.

22. Bakılmakta olan davanın konusunu ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında yapılan güvenlik soruşturması ve arşiv araştırması oluşturmaktadır. Dolayısıyla anılan Kanun'un birinci maddesinin birinci fıkrası uyarınca hakkında güvenlik soruşturması ve arşiv araştırması yapılacağı belirtilen diğer personel uyumsuzluk kapsamında değildir.

23. Bu itibarla 4045 sayılı Kanun'un itiraz konusu 1. maddesinin birinci fıkrasının "...kamu kurum ve kuruluşlarında, yetkili olmayan kişilerin bilgi sahibi olmaları halinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile Genelkurmay Başkanlığı, Milli Savunma Bakanlığı, jandarma, emniyet, sahil güvenlik ve istihbarat teşkilatlarında çalıştırılacak kamu personeli..." bölümünün bakılmakta olan davada uygulanma imkânı bulunmadığından bu bölüme ilişkin başvurunun Mahkemenin yetkisizliği nedeniyle reddi gerekir.

24. Öte yandan anılan maddenin birinci fıkrasının kalan kısmı, bakılmakta olan davaya konu ceza infaz kurumları ve tutukevlerinde çalışacak personelin yanı sıra bakılmakta olan davada uygulanma imkânı bulunmayan hakkında güvenlik soruşturması ve arşiv araştırması yapılacak diğer personel bakımından da geçerli ortak kural niteliğindedir. Dolayısıyla bakılmakta olan davanın konusu

gözetilerek esas incelemenin birinci fıkrada yer alan "...ve ceza infaz kurumları ve tutukevlerinde çalışacak personel,..." ibaresi ile sınırlı olarak yapılması gerekir.

25. Kanun'un itiraz konusu 1. maddesinin ikinci fıkrası ise Anayasa Mahkemesinin 19/2/2020 tarihli ve E.2018/163, K.2020/13 sayılı kararıyla iptaline karar verilmiş ve bu iptal kararı 28/4/2020 tarihli ve 31112 sayılı Resmî Gazete'de yayımlanmıştır. Bu nedenle anılan fıkraya yönelik iptal talebi hakkında karar verilmesine yer olmadığına karar vermek gerekir.

26. Maddenin güvenlik soruşturması ve arşiv araştırmasının usul ve esaslarının yönetmelikle düzenleneceğini öngören üçüncü fıkrası ise hakkında güvenlik soruşturması ve arşiv araştırması yapılacak tüm personel bakımından geçerli ortak kural niteliğindedir. Bakılmakta olan davanın konusu gözetilerek anılan fıkranın esasına ilişkin incelemenin "...ve ceza infaz kurumları ve tutukevlerinde çalışacak personel,..." ibaresi yönünden yapılması gerekir.

27. Açıklanan nedenlerle 26/10/1994 tarihli ve 4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun'un 1. maddesinin;

A. Birinci fıkrasının;

1. "...kamu kurum ve kuruluşlarında, yetkili olmayan kişilerin bilgi sahibi olmaları halinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile Genelkurmay Başkanlığı, Milli Savunma Bakanlığı, jandarma, emniyet, sahil güvenlik ve istihbarat teşkilatlarında çalıştırılacak kamu personeli..." bölümünün itiraz başvurusunda bulunan Mahkemenin bakmakta olduğu davada uygulanma imkânı bulunmadığından bu bölüme ilişkin başvurunun Mahkemenin yetkisizliği nedeniyle REDDİNE,

2. Kalan kısmının esasının incelenmesine, esasa ilişkin incelemenin "...ve ceza infaz kurumları ve tutukevlerinde çalışacak personel..." ibaresi ile sınırlı olarak yapılmasına,

B. İkinci fıkrası hakkında KARAR VERİLMESİNE YER OLMADIĞINA,

C. Üçüncü fıkrasının esasının incelenmesine, esasa ilişkin incelemenin birinci fıkrada yer alan "... ve ceza infaz kurumları ve tutukevlerinde çalışacak personel..." ibaresi yönünden yapılmasına

OYBİRLİĞİYLE karar verilmiştir.

III. BİRLEŞTİRME KARARLARI

28. 26/10/1994 tarihli ve 4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun'un 1. maddesinin;

A. Birinci fıkrasında yer alan "...Milli Savunma Bakanlığı,...", "...ve ceza infaz kurumları ve tutukevlerinde çalışacak personel..." ibarelerinin,

B. Üçüncü fıkrasının birinci fıkrada yer alan "...Milli Savunma Bakanlığı,...", "...ve ceza infaz kurumları ve tutukevlerinde çalışacak personel..." ibareleri yönünden

iptallerine karar verilmesi talebiyle yapılan itiraz başvurularına ilişkin E.2020/39 ve E.2020/40 sayılı davaların aralarındaki hukuki irtibat nedeniyle E.2020/24 sayılı dava ile BİRLEŞTİRİLMELERİNE, esaslarının kapatılmasına, esas incelemelerin E.2020/24 sayılı dosya üzerinden yürütülmesine 6/5/2020 tarihinde OYBİRLİĞİYLE karar verilmiştir.

IV. ESASIN İNCELENMESİ

29. Başvuru kararları ve ekleri, Raportör Aydın AYGÜN tarafından hazırlanan işin esasına ilişkin rapor, dava konusu kanun hükmü, dayanılan Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

1. Uygulanacak Kural Sorunu

30. 4045 sayılı Kanun'un 1. maddesinin üçüncü fıkrasında devletin güvenliğini, ulusun varlığını ve bütünlüğünü iç ve dış menfaatlerinin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeler ile gizlilik dereceli kamu personeli ile meslek gruplarının tespitinin, birim ve kısımların tanımlarının yapılmasının ve güvenlik soruşturması ve arşiv araştırmasının usul ve esasları ile bunu yapacak mercilerin ve üst kademe yöneticilerinin kimler olduğunun Cumhurbaşkanınca yürürlüğe konulacak yönetmelik ile düzenleneceği öngörülmektedir.

31. Bakılmakta olan davaların konusu ise jandarma, Millî Savunma Bakanlığı ile ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında güvenlik soruşturması veya arşiv araştırmasının yapılmasıdır. Kanun'un 1. maddesinin birinci fıkrası incelendiğinde bakılmakta olan davaların konusunu oluşturan kamu görevlilerinin dışında kamu kurum ve kuruluşlarında, yetkili olmayan kişilerin bilgi sahibi olmaları halinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimlerde çalışacak personel hakkında da güvenlik soruşturması ve arşiv araştırmasının yapılacağı hüküm altına alınmıştır. Anılan maddenin üçüncü fıkrasında ise devletin güvenliğinin, ulusun varlığını ve bütünlüğünü iç ve dış menfaatlerinin zarar görebileceği veya tehlikeye

düşebileceği bilgi ve belgeler ile gizlilik dereceli kamu personeli ve meslek gruplarının tespitinin, birim ve kısımların tanımlarının yapılmasının yönetmeliğe bırakıldığı belirtilmiştir.

32. Bakılmakta olan davaların konusu gözönünde bulundurulduğunda itiraz konusu üçüncü fıkranın “Devletin güvenliğini, ulusun varlığını ve bütünlüğünü iç ve dış menfaatlerinin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeler ile gizlilik dereceli kamu personeli ile meslek gruplarının tespiti, birim ve kısımların tanımlarının yapılması,…” bölümünün bakılmakta olan davalarda uygulanma imkânı bulunmamaktadır.

33. Açıklanan nedenle 4045 sayılı Kanun’un 1. maddesinin üçüncü fıkrasının “Devletin güvenliğini, ulusun varlığını ve bütünlüğünü iç ve dış menfaatlerinin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeler ile gizlilik dereceli kamu personeli ile meslek gruplarının tespiti, birim ve kısımların tanımlarının yapılması...” bölümüne ilişkin başvurunun Mahkemenin yetkisizliği nedeniyle reddi gerekir.

2. İtirazların Gerekçeleri

34. Başvuru kararlarında özetle; itiraz konusu kurallarda hangi kamu görevlileri bakımından güvenlik soruşturması ve arşiv araştırmasının yapılacağı düzenlendiği, güvenlik soruşturması ve arşiv araştırmasıyla ilgili diğer hususların yönetmeliğe bırakıldığı, güvenlik soruşturması ve arşiv araştırmasına konu bilgi ve belgelerin neler olduğu, bu bilgi ve belgelerin nerelerden elde edileceği, ne suretle ve ne kadar süreyle saklanacağı, kişilerin söz konusu bilgilere itiraz etme imkânının bulunup bulunmadığıyla ilgili herhangi bir yasal düzenlemeye yer verilmediği, hangi suçlardan mahkûmiyetlerin, kamu davasının açılmasının ertelenmesi veya hükmün açıklanmasının geri bırakılması kararlarının güvenlik soruşturması ve arşiv araştırmasına etkisinin ne olacağına kurallarda belirlenmediği belirtilerek kuralların Anayasa’nın 13., 20. ve 128. maddelerine aykırı oldukları ileri sürülmüştür.

3. Anayasa’ya Aykırılık Sorunu

35. 4045 sayılı Kanun’un 1. maddesinin birinci fıkrasında yer alan itiraz konusu ibareler Millî Savunma Bakanlığı, jandarma ve ceza infaz kurumları ile tutukevlerinde çalışacak personel hakkında güvenlik soruşturması ve arşiv araştırmasının yapılmasını öngörmektedir.

36. Anılan maddenin itiraz konusu ikinci fıkrası Anayasa Mahkemesinin 19/2/2020 tarihli ve E.2018/163, K.2020/13 sayılı kararıyla iptal edilmiş olup bu iptal kararı 28/4/2020 tarihli ve 31112 sayılı Resmî Gazete’de yayımlanmıştır. Bu nedenle anılan fıkraya yönelik iptal talebi hakkında karar verilmesine yer olmadığına karar vermek gerekir.

37. Maddenin üçüncü fıkrasının itiraz konusu bölümünde ise güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak mercilerin ve üst kademe yöneticilerinin kimler olduğunun Cumhurbaşkanınca yürürlüğe konulacak yönetmelik ile düzenleneceği hüküm altına alınmış olup anılan bölüm birinci fıkrada yer alan "...Millî Savunma Bakanlığı, jandarma", "...ve ceza infaz kurumları ve tutukevlerinde çalışacak personel..." ibareleri yönünden incelenmiştir.

38. İtiraz konusu kuralların da yer aldığı 4045 sayılı Kanun 7/4/2021 tarihli ve 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu'nun 13. maddesinin (8) numaralı fıkrasıyla yürürlükten kaldırılmıştır. Başvuran Mahkemede bakılmakta olan davalara konu işlemler itiraz konusu kuralların yürürlükte olduğu dönemde bu kurallar uyarınca tesis edilmiştir. 7315 sayılı Kanun, kuralların dayanak teşkil ettiği işlemlerin hukuki etkilerine dair geçmişe yönelik herhangi bir özel hüküm içermemektedir. Hukuka uygunluk karinesinden yararlanan ve iptal edilmediği ya da yürürlükten kaldırılmadığı sürece hukuk alanında varlığını ve etkilerini devam ettiren idari işlemlerin hukuki denetimi, tesis edildiği dönemde yürürlükte bulunan mevzuat hükümleri çerçevesinde gerçekleştirilmektedir. Bu bağlamda başvuran Mahkeme de yürürlükten kalkmış olan kuralları, dava konusu idari işlemlerin hukuki denetimini gerçekleştirirken denetleyici norm olarak gözetmek durumundadır. Başka bir ifadeyle kurallar bakılmakta olan davalarda uyumsuzluğun çözümü için uygulanacak kural olma niteliğini sürdürmektedir. Bu itibarla kuralların yürürlükten kaldırılmış olmalarının esaslarının incelenmesinde herhangi bir etkisi bulunmamaktadır.

39. Kurallar Millî Savunma Bakanlığı, jandarma ve ceza infaz kurumları ile tutukevlerinde çalışacak personel hakkında güvenlik soruşturması ve arşiv araştırmasının yapılmasını, anılan soruşturma ve araştırmanın usul ve esasları ile bunu yapacak merciler ve üst kademe yöneticilerinin kimler olduğunun ise Cumhurbaşkanınca yürürlüğe konulacak yönetmelik ile düzenleneceğini hükme bağlamaktadır.

40. Anayasa Mahkemesi 24/7/2019 tarihli ve E.2018/73, K.2019/65 sayılı, 19/2/2020 tarihli ve E.2018/163, K.2020/13 sayılı kararlarında güvenlik soruşturması ve arşiv araştırması yapılmasını öngören kuralları incelemiştir. Bu kararlarda Anayasa ve kanunlara sadık kalarak faaliyette bulunma yükümlülükleri olan memurların ve kamu görevlilerinin kamu görevlerine atanmalarında birtakım şartların aranmasının doğal olduğu, bu kapsamda kamu görevine atanmadan önce kişilerin güvenlik soruşturmasının ve arşiv araştırmasının yapılmasını öngören kuralların kanun koyucunun takdir yetkisinde bulunduğu belirtilmiştir. Bununla birlikte anılan kararlarda güvenlik soruşturması ve arşiv araştırmasının yapılmasına ve elde edilecek verilerin kullanılmasına ilişkin temel ilkelerin kanunda düzenlenmesi gerektiği ifade edilmiştir (bkz. sırasıyla §§ 170, 171; §§ 15, 16).

41. Anayasa'nın 20. maddesinin birinci fıkrasında herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş; üçüncü fıkrasında da "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir" denilerek kişisel verilerin korunması özel hayatın gizliliğinin korunması kapsamında güvenceye kavuşturulmuştur.

42. Kişisel verilerin korunmasını isteme hakkı, insan onurunun korunması ve bireyin kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır.

43. Anayasa Mahkemesinin yerleşik kararlarında belirtildiği üzere "...adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler..." kişisel veri olarak kabul edilmektedir (AYM, E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2014/74, K.2014/201, 25/12/2014; E.2014/180, K.2015/30, 19/3/2015; E.2015/32, K.2015/102, 12/11/2015).

44. Bu bağlamda güvenlik soruşturması ve arşiv araştırmasıyla elde edilen veriler kişisel veri niteliğindedir. İtiraz konusu kurallar, güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimler tarafından güvenlik soruşturması ve arşiv araştırması kapsamında kişilerin kişisel veri niteliğindeki özel hayatı, iş ve sosyal yaşamıyla ilgili bilgilerinin alınmasına ve bu kayıtların kullanılmasına imkân tanınması nedeniyle kişisel verilerin korunmasını isteme hakkına sınırlama getirmektedir.

45. Anayasa'nın 20. maddesi uyarınca kişisel veriler ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir. Anayasa'nın 13. maddesinde de "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz." hükmüne yer verilerek temel hak ve özgürlüklerin ancak kanunla sınırlanabileceği ifade edilmiştir. Anayasa'nın 13. ve 20.

maddeleri uyarınca kişisel verilerin korunmasını isteme hakkını sınırlamaya yönelik kanuni bir düzenlemenin şeklen var olması yeterli olmayıp yasal kuralların keyfiliğe izin vermeyecek şekilde belirli, ulaşılabilir ve öngörülebilir düzenlemeler niteliğinde olması gerekir.

46. Esasen temel hakları sınırlayan kanunun bu niteliklere sahip olması, Anayasa'nın 2. maddesinde güvenceye bağlanan hukuk devleti ilkesinin de bir gereğidir. Hukuk devletinde, kanuni düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi gerekir. Kanunda bulunması gereken bu nitelikler hukuki güvenliğin sağlanması bakımından da zorunludur. Zira bu ilke hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar (AYM, E.2015/41, K.2017/98, 4/5/2017, §§ 153, 154). Dolayısıyla Anayasa'nın 13. ve 20. maddelerinde sınırlama ölçütü olarak belirtilen kanunilik, Anayasa'nın 2. maddesinde güvenceye bağlanan hukuk devleti ilkesi ışığında yorumlanmalıdır.

47. Anayasa'nın 129. maddesinin birinci fıkrasında memurlar ve kamu görevlilerinin Anayasa ve kanunlara sadık kalarak faaliyette bulunma yükümlülükleri düzenlenmiştir. Belirtilen husus gözetilerek kamu görevinde çalıştırılacak kişiler bakımından güvenlik soruşturması ve arşiv araştırması yapılması yönünde düzenlemeler getirilmesi kanun koyucunun takdir yetkisindedir. Ancak bu alanda düzenleme öngören kuralların kamu makamlarına hangi koşullarda ve hangi sınırlar içinde tedbirler uygulama ve özel hayata saygı gösterilmesini isteme hakkına yönelik müdahalelerde bulunma yetkisi verildiğini yeterince açık olarak göstermesi ve muhtemel kötüye kullanmalara karşı yeterli güvenceleri sağlaması gerekir.

48. Kurallar Millî Savunma Bakanlığı, jandarma ve ceza infaz kurumları ile tutukevlerinde çalışacak personel hakkında güvenlik soruşturması ve arşiv araştırmasının yapılmasını zorunlu kılmıştır. Buna karşın kişisel veri niteliğindeki bu bilgilerin ne şekilde kullanılacağına, hangi mercilerin soruşturma ve araştırmayı yapacağına, bu bilgilerin ne suretle ve ne kadar süre ile saklanacağına, ilgililerin söz konusu bilgilere itiraz etme imkânının olup olmadığına, bilgilerin bir müddet sonra silinip silinmeyeceğine, silinecekse bu sırada izlenecek usulün ne olduğuna, yetkinin kötüye kullanımını önlemeye yönelik nasıl bir denetim yapılacağına ilişkin herhangi bir düzenleme yapılmamıştır. Diğer bir ifadeyle güvenlik soruşturması ve arşiv araştırmasının yapılmasına ve elde edilecek verilerin kullanılmasına ilişkin keyfiliğe izin vermeyecek şekilde belirli ve öngörülebilir kanuni güvenceler

belirlenmeksizin güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak merciler ile üst kademe yöneticilerinin tespiti yönetmeliğe bırakılmıştır.

49. Güvenlik soruşturması ve arşiv araştırması sonucunda kişisel veri niteliğindeki bilgilerin alınmasına, kullanılmasına, işlenmesine yönelik güvenceler ve temel ilkeler kanunla belirlenmeksizin bunların alınmasına ve kullanılmasına izin verilmesi Anayasa'nın 13. ve 20. maddeleriyle bağdaşmamaktadır (benzer yönde bkz. AYM, E.2018/73, K.2019/65, 24/7/2019, §§ 171, 172; AYM, E.2018/163, K.2020/13, 19/2/2020, §§ 16, 17; Fatih Saraman [GK], B. No: 2014/7256, 27/2/2019, §§ 89, 90; Turgut Duman, B. No: 2014/15365, 29/5/2019, § 88).

50. Açıklanan nedenlerle kurallar Anayasa'nın 13. ve 20. maddelerine aykırıdır. İptalleri gerekir.

Kurallar Anayasa'nın 13. ve 20. maddelerine aykırı görülerek iptal edildiğinden ayrıca Anayasa'nın 128. maddesi yönünden incelenmemiştir.

V. HÜKÜM

26/10/1994 tarihli ve 4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun'un 1. maddesinin;

A. Birinci fıkrasında yer alan "...Milli Savunma Bakanlığı, jandarma,..." ve "...ve ceza infaz kurumları ve tutukevlerinde çalışacak personel..." ibarelerinin Anayasa'ya aykırı olduklarına ve İPTALLERİNE,

B. İkinci fıkrası hakkında KARAR VERİLMESİNE YER OLMADIĞINA,

C. Üçüncü fıkrasının;

1. "Devletin güvenliğini, ulusun varlığını ve bütünlüğünü iç ve dış menfaatlerinin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeler ile gizlilik dereceli kamu personeli ile meslek gruplarının tespiti, birim ve kısımların tanımlarının yapılması,..." bölümünün itiraz başvurusunda bulunan Mahkemenin bakmakta olduğu davada uygulanma imkânı bulunmadığından bu bölüme ilişkin başvurunun Mahkemenin yetkisizliği nedeniyle REDDİNE,

2. Kalan kısmının birinci fıkrada yer alan "...Milli Savunma Bakanlığı, jandarma,..." ve "...ve ceza infaz kurumları ve tutukevlerinde çalışacak personel..." ibareleri yönünden Anayasa'ya aykırı olduğuna ve İPTALİNE,

3/6/2021 tarihinde OYBİRLİĞİYLE karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili - Hasan Tahsin GÖKCAN

Başkanvekili - Kadir ÖZKAYA

Üye: Engin YILDIRIM; Hicabi DURSUN; Celal Mümtaz AKINCI; Muammer TOPAL; M. Emin KUZ;
Rıdvan GÜLEÇ; Recai AKYEL; Yusuf Şevki HAKYEMEZ; Yıldız SEFERİNOĞLU; Selahaddin
MENTEŞ; Basri BAĞCI; İrfan FİDAN

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2018/163

Karar Sayısı: 2020/13

Karar Tarihi: 19/2/2020

RG Tarih-Sayı: 28/4/2020-31112

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri Engin ALTAY, Özgür ÖZEL ve Engin ÖZKOÇ ile birlikte 138 milletvekili

İPTAL DAVASININ KONUSU: 18/10/2018 tarihli ve 7148 sayılı Karayolları Trafik Kanunu ile Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun'un 29. maddesiyle 26/10/1994 tarihli ve 4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun'un 1. maddesine eklenen ikinci fıkranın Anayasa'nın 2., 7., 12.,13.,17., 20., 38., 40., 70. ve 129. maddelerine aykırılığı ileri sürülerek iptaline ve yürürlüğünün durdurulmasına karar verilmesi talebidir.

I. İPTALİ İSTENEN KANUN HÜKMÜ

Kanun'un iptali talep edilen 29. maddesiyle ikinci fıkranın eklendiği 4045 sayılı Kanun'un 1. maddesi şöyledir:

"Madde 1- Güvenlik Soruşturması ve Arşiv Araştırması; kamu kurum ve kuruluşlarında, yetkili olmayan kişilerin bilgi sahibi olmaları halinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile Genelkurmay Başkanlığı, Milli Savunma Bakanlığı, jandarma, emniyet, sahil güvenlik ve istihbarat teşkilatlarında çalıştırılacak kamu personeli ve ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında yapılır.

(Ek:18/10/2018-7148/29 md.) Güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimler, güvenlik soruşturması ve arşiv araştırması kapsamında bakanlıklar ile kamu kurum ve kuruluşları arşivlerinden ve elektronik bilgi işlem merkezlerinden bilgi ve belge almaya, 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun 171 inci maddesinin beşinci ve 231 inci maddesinin onüçüncü fıkraları kapsamında tutulan kayıtlara ulaşmaya, Cumhuriyet başsavcılıkları tarafından yürütülen

soruşturma sonuçlarını, kovuşturmaya yer olmadığına dair kararlar ile kesinleşmiş mahkeme kararlarını almaya yetkilidir.

Devletin güvenliğini, ulusun varlığını ve bütünlüğünü iç ve dış menfaatlerinin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeler ile gizlilik dereceli kamu personeli ile meslek gruplarının tespiti, birim ve kısımların tanımlarının yapılması, güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak merciler ve üst kademe yöneticilerinin kimler olduğu Cumhurbaşkanınca yürürlüğe konulacak yönetmelik ile düzenlenir.”

II. İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Zühtü ARSLAN, Burhan ÜSTÜN, Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ, Recep KÖMÜRCÜ, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Rıdvan GÜLEÇ, Recai AKYEL ve Yusuf Şevki HAKYEMEZ'in katılımlarıyla 17/1/2019 tarihinde yapılan ilk inceleme toplantısında dosyada eksiklik bulunmadığından işin esasının incelenmesine, yürürlüğü durdurma talebinin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

III. ESASIN İNCELENMESİ

2. Dava dilekçesi ve ekleri, Raportör Aydın AYGÜN tarafından hazırlanan işin esasına ilişkin rapor, dava konusu kanun hükmü, dayanılan Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

1. Anlam ve Kapsam

3. Dava konusu kural, güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimlerin güvenlik soruşturması ve arşiv araştırması kapsamında bakanlıklar ile kamu kurum ve kuruluşlarının arşivlerinden ve elektronik bilgi işlem merkezlerinden bilgi ve belge almaya, 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu'nun 171. maddesinin (5) ve 231. maddesinin (13) numaralı fıkraları kapsamında tutulan kayıtlara ulaşmaya, Cumhuriyet başsavcılıkları tarafından yürütülen soruşturma sonuçlarını, kovuşturmaya yer olmadığına dair kararlar ile kesinleşmiş mahkeme kararlarını almaya yetkili olduklarını hükme bağlamaktadır.

4. 5271 sayılı Kanun'un 171. maddesi Cumhuriyet savcısının kamu davasını açmadaki takdir yetkisini düzenlemektedir. Bu kapsamda Cumhuriyet savcısı bazı koşullar altında kamu davasının açılmasının ertelenmesine de karar verebilmektedir. Bu yetkinin kullanılması hâlinde ise anılan maddenin (5) numaralı fıkrası gereğince kamu davasının açılmasının ertelenmesine ilişkin kararların bunlara

mahsus sisteme kaydedilmesi zorunludur. Söz konusu kayıtların ise ancak bir soruşturma veya kovuşturmayla bağlantılı olarak Cumhuriyet savcısı, hâkim veya mahkeme tarafından istenmesi mümkündür.

5. Anılan maddenin (4) numaralı fıkrası uyarınca, hakkında kamu davasının açılmasının ertelenmesine karar verilenlerin belirlenen erteleme süresi içinde kasıtlı bir suç işlememesi hâlinde söz konusu soruşturma kovuşturmaya yer olmadığına kararıyla sonuçlandırılır. Bu itibarla kamu davasının açılmasının ertelenmesi, fail hakkında kamu davasının açılmasına yetecek şekilde suç işlediğine dair var olan şüphenin belirli bir süre denetime tabi olmak koşuluyla askıya alınmasını öngörmektedir.

6. Kanun'un 231. maddesinde ise hükmün açıklanmasının geri bırakılması kurumu düzenlenmiştir. Anılan maddeye göre belirli koşulların gerçekleşmesi hâlinde sanık hakkında hükmün açıklanmasının geri bırakılmasına karar verilebilir. Bu durumda da verilen hükmün açıklanmasının geri bırakılması kararları bunlara mahsus bir sisteme kaydedilir. Bu kayıtlar da ancak bir soruşturma veya kovuşturmayla bağlantılı olarak Cumhuriyet savcısı, hâkim veya mahkeme tarafından istenebilir ve istenen kayıtlar bu amacın dışında kullanılamaz.

7. Belirlenen denetim süresi içinde kasıtlı bir suçtan mahkûm olunmaması ve denetimli serbestlik tedbirine ilişkin yükümlülüklerle uygun davranılması hâlinde açıklanması geri bırakılan hüküm ortadan kaldırılarak davanın düşmesine karar verilir. Bu bağlamda sanık hakkında verilen hükmün açıklanmasının geri bırakılması kararı mahkûmiyet hükmü olarak kabul edilemez.

2. İptal Talebinin Gerekçesi

8. Dava dilekçesinde özetle; dava konusu kuralın güvenlik soruşturması ve arşiv araştırması faaliyeti kapsamında kamu idaresine, kamu görevine girme hakkını kullanmak isteyen kişiye ait kişisel verilere sınırsız bir şekilde erişme ve bu verileri toplama, sınıflandırma, işleme ve değerlendirme imkânı verdiği, kişisel verilere ilişkin kanunların kişisel veri niteliğindeki bilgilerin teminine, kullanılabilmesine, işlenebilmesine, ulaşılabilmesine, saklanma süresine, temin edilme gerekçesine, bilgilerin silinmesi ve değiştirilmesine, kötüye kullanımının engellenmesine yönelik birtakım güvenceleri içermesi ve hukuki belirliliğe sahip olması gerektiği, yapılan güvenlik soruşturması sonucunda kişilerin kamu görevine girmesinin engellenebileceği ya da mevcut kamu görevinden çıkarılmasının mümkün olabileceği, bu itibarla düzenlemenin kamu hizmetine girme hakkına öngörülemez bir sınırlama getirdiği belirtilerek kuralın Anayasa'nın 2., 7., 12., 13., 17., 20., 38., 40., 70. ve 129. maddelerine aykırı olduğu ileri sürülmüştür.

3. Anayasa'ya Aykırılık Sorunu

9. Anayasa'nın 20. maddesinin birinci fıkrasında herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş; son fıkrasında da "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." denilerek kişisel verilerin korunması, özel hayata saygı gösterilmesini isteme hakkı kapsamında güvenceye kavuşturulmuştur.

10. Kişisel verilerin korunmasını isteme hakkı, insan onurunun korunması ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır.

11. Anayasa Mahkemesinin yerleşik kararlarında belirtildiği üzere "...adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler..." kişisel veri olarak kabul edilmektedir (AYM, E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2014/74, K.2014/201, 25/12/2014; E.2014/180, K.2015/30, 19/3/2015; E.2015/32, K.2015/102, 12/11/2015).

12. Bu bağlamda güvenlik soruşturması ve arşiv araştırmasıyla elde edilen veriler kişisel veri niteliğindedir. Dava konusu kural, güvenlik soruşturması ve arşiv araştırması yapmakla görevli birimler tarafından güvenlik soruşturması ve arşiv araştırması kapsamında kişilerin kişisel veri niteliğindeki özel hayatı, iş ve sosyal yaşamıyla ilgili bilgilerinin alınmasına, hakkındaki suç işlediğine dair iddiaların değerlendirildiği Cumhuriyet savcılığı, hâkim veya mahkeme kararlarının tutulduğu kayıtlara ulaşılmasına ve bu kayıtların kullanılmasına imkân tanınması nedeniyle kişisel verilerin korunmasını isteme hakkına sınırlama getirmektedir.

13. Anayasa'nın 20. maddesi uyarınca kişisel veriler ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir. Anayasa'nın 13. maddesinde de "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin

ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.” hükmüne yer verilerek temel hak ve özgürlüklerin ancak kanunla sınırlanabileceği ifade edilmiştir. Anayasa'nın 13. ve 20. maddeleri uyarınca kişisel verilerin korunmasını isteme hakkını sınırlamaya yönelik kanuni bir düzenlemenin şeklen var olması yeterli olmayıp yasal kuralların keyfiliğe izin vermeyecek şekilde belirli, ulaşılabilir ve öngörülebilir düzenlemeler niteliğinde olması gerekir.

14. Esasen temel hakları sınırlayan kanunun bu niteliklere sahip olması, Anayasa'nın 2. maddesinde güvenceye bağlanan hukuk devleti ilkesinin de bir gereğidir. Hukuk devletinde, kanuni düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi gerekir. Kanunda bulunması gereken bu nitelikler hukuki güvenliğin sağlanması bakımından da zorunludur. Zira bu ilke hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar (AYM, E.2015/41, K.2017/98, 4/5/2017, §§ 153, 154). Dolayısıyla Anayasa'nın 13. ve 20. maddelerinde sınırlama ölçütü olarak belirtilen kanunilik, Anayasa'nın 2. maddesinde güvenceye bağlanan hukuk devleti ilkesi ışığında yorumlanmalıdır.

15. Anayasa'nın 129. maddesinin birinci fıkrasında memurlar ve kamu görevlilerinin Anayasa ve kanunlara sadık kalarak faaliyette bulunma yükümlülükleri düzenlenmiştir. Belirtilen husus gözetilerek kamu görevinde çalıştırılacak kişiler bakımından güvenlik soruşturması ve arşiv araştırması yapılması yönünde düzenlemeler getirilmesi kanun koyucunun takdir yetkisindedir. Ancak bu alanda düzenleme öngören kuralların kamu makamlarına hangi koşullarda ve hangi sınırlar içinde tedbirler uygulama ve özel hayata saygı gösterilmesini isteme hakkına yönelik müdahalelerde bulunma yetkisi verildiğini yeterince açık olarak göstermesi ve muhtemel kötüye kullanmalara karşı yeterli güvenceleri sağlaması gerekir.

16. Kuralda güvenlik soruşturması ve arşiv araştırması yapmakla görevli olanların bu kapsamda kişisel veri niteliğindeki bilgilere ulaşması öngörülmüşken Kanun'da bu bilgilerin ne şekilde kullanılacağına, hangi mercilerin soruşturma ve araştırmayı yapacağına, bu bilgilerin ne suretle ve ne kadar süre ile saklanacağına, ilgililerin söz konusu bilgilere itiraz etme imkânının olup olmadığına, bilgilerin bir müddet sonra silinip silinmeyeceğine, silinecekse bu sırada izlenecek usulün ne olduğuna, yetkinin kötüye kullanımını önlemeye yönelik nasıl bir denetim yapılacağına ilişkin herhangi bir düzenleme yapılmamıştır. Diğer bir ifadeyle güvenlik soruşturması ve arşiv araştırmasının yapılmasına ve elde edilecek verilerin kullanılmasına ilişkin keyfiliğe izin vermeyecek

şekilde belirli ve öngörülebilir kanuni güvenceler belirlenmeksizin, kuralla güvenlik soruşturması ve arşiv araştırması yapmakla görevli olanların bu soruşturma ve araştırma kapsamında kişisel veri niteliğindeki bilgileri almakla yetkili oldukları belirtilmiştir.

17. Güvenlik soruşturması ve arşiv araştırması sonucunda kişisel veri niteliğindeki bilgilerin alınmasına, kullanılmasına, işlenmesine yönelik güvenceler ve temel ilkeler kanunla belirlenmeksizin bunların alınmasına ve kullanılmasına izin verilmesi Anayasa'nın 13. ve 20. maddeleriyle bağdaşmamaktadır (benzer yönde bkz. AYM, E.2018/73, K.2019/65, 24/7/2019, §§ 171, 172; Fatih Saraman [GK], B. No: 2014/7256, §§ 89, 90; Turgut Duman, B. No: 2014/15365, § 88).

18. Açıklanan nedenlerle kural Anayasa'nın 13. ve 20. maddelerine aykırıdır. İptali gerekir.

Kuralın Anayasa'nın 2. maddesine de aykırı olduğu ileri sürülmüş ise de bu bağlamda belirtilen hususların Anayasa'nın 13. ve 20. maddeleri yönünden yapılan değerlendirmeler kapsamında ele alınmış olması nedeniyle Anayasa'nın 2. maddesi yönünden ayrıca bir inceleme yapılmasına gerek görülmemiştir.

Kural Anayasa'nın 13. ve 20. maddelerine aykırı görülerek iptal edildiğinden ayrıca Anayasa'nın 7., 12., 17., 38., 40., 70. ve 129. maddeleri yönünden incelenmemiştir.

IV. YÜRÜRLÜĞÜN DURDURULMASI TALEBİ

19. Dava dilekçesinde özetle, dava konusu kuralın uygulanması hâlinde telafisi güç veya imkânsız zararlar doğabileceği belirtilerek yürürlüğünün durdurulmasına karar verilmesi talep edilmiştir.

18/10/2018 tarihli ve 7148 sayılı Karayolları Trafik Kanunu ile Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun'un 29. maddesiyle 26/10/1994 tarihli ve 4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun'un 1. maddesine eklenen ikinci fıkraya yönelik yürürlüğün durdurulması talebinin koşulları oluşmadığından REDDİNE 19/2/2020 tarihinde OYBİRLİĞİYLE karar verilmiştir.

V. HÜKÜM

18/10/2018 tarihli ve 7148 sayılı Karayolları Trafik Kanunu ile Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun'un 29. maddesiyle 26/10/1994 tarihli ve 4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun'un

1. maddesine eklenen ikinci fıkranın Anayasa'ya aykırı olduğuna ve İPTALİNE 19/2/2020 tarihinde OYBİRLİĞİYLE karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili - Hasan Tahsin GÖKCAN

Başkanvekili - Recep KÖMÜRCÜ

Üye: Serdar ÖZGÜLDÜR; Burhan ÜSTÜN; Engin YILDIRIM; Hicabi DURSUN; Celal Mümtaz AKINCI; Muammer TOPAL; M. Emin KUZ; Kadir ÖZKAYA; Rıdvan GÜLEÇ; Recai AKYEL; Yusuf Şevki HAKYEMEZ; Yıldız SEFERİNOĞLU; Selahaddin MENTEŞ

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2018/134

Karar Sayısı: 2021/13

Karar Tarihi: 3/3/2021

RG Tarih-Sayısı: 16/6/2021-31513

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri Engin ALTAY, Özgür ÖZEL, Engin ÖZKOÇ ile birlikte 139 milletvekili

İPTAL DAVASININ KONUSU: 23/7/2018 tarihli ve (14) numaralı İletişim Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin;

A. 17. maddesinin (2) numaralı fıkrasının birinci cümlesinde yer alan "...gerekli gördüğü bilgileri..." ibaresinin,

B. 21. maddesinin (3) numaralı fıkrasının üçüncü cümlesinin,

C. 22. maddesinin (1) numaralı fıkrasında yer alan "...yurtdışı ve..." ibaresinin,

Ç. 26. maddesinin (2) numaralı fıkrasının (c) bendiyle 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete'de yayımlanan (1) numaralı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin 485. maddesine eklenen (i) bendinin,

Anayasa'nın 2., 7., 8., 20., 104., 123. ve 128. maddelerine aykırılığı ileri sürülerek iptallerine ve yürürlüklerinin durdurulmasına karar verilmesi talebidir.

I. İPTALİ İSTENEN VE İLGİLİ GÖRÜLEN CUMHURBAŞKANLIĞI KARARNAMESİ KURALLARI İLE KANUN HÜKMÜNDE KARARNAME KURALI

A. İptali İstenen Cumhurbaşkanlığı Kararnamesi Kuralları

Cumhurbaşkanlığı Kararnamesi'nin (CBK) iptali talep edilen kuralların da yer aldığı;

1. 17. maddesi şöyledir:

"İşbirliği ve bilgi toplama

MADDE 17- (1) Başkanlık, görev alanına giren konularda bakanlıklar, kamu kurum ve kuruluşları, kamu iktisadi teşebbüsleri, kamu kurumu niteliğindeki meslek kuruluşları, sivil toplum kuruluşları,

üniversiteler ve diğer gerçek ve tüzel kişiler ile yakın işbirliği içinde bulunur. Başkanlık, kabul edilen planların, yıllık programların ve projelerin uygulanmasındaki uyum ve işbirliğini sağlar.

(2) Başkanlık, görevleri ile ilgili olarak gerekli gördüğü bilgileri bütün kamu kurum ve kuruluşlarından ve diğer gerçek ve tüzel kişilerden doğrudan istemeye yetkilidir. Kendilerinden bilgi istenen bütün kamu kurum ve kuruluşları ile diğer gerçek ve tüzel kişiler bu bilgileri istenilen süre içinde öncelikle ve zamanında vermekle yükümlüdürler.

(3) Bu şekilde elde edilen bilgilerden ticari sır niteliğinde olanların gizliliğine uyulur.”

2. 21. maddesinin (3) numaralı fıkrası şöyledir:

“(3) Başkanlıkta, 657 sayılı Devlet Memurları Kanununa tabi personel istihdam edilir. Ayrıca 27/6/1989 tarihli ve 375 sayılı Kanun Hükmünde Kararnamenin ek 26 ncı maddesi çerçevesinde sözleşmeli personel istihdam edilebilir ve aynı Kanun Hükmünde Kararnamenin ek 25 inci maddesi çerçevesinde Başkanlıkta diğer kurum personeli geçici görevlendirilebilir. Bu suretle çalıştırılacakların sözleşme usul ve esasları ile ücret miktarı ve her çeşit ödemeleri Cumhurbaşkanınca tespit edilir.”

3. 22. maddesinin (1) numaralı fıkrası şöyledir:

“(1) Başkanlık yurtdışı ve taşra teşkilatı kurmaya yetkilidir.”

4. 26. maddesinin (2) numaralı fıkrasının (c) bendiyle (i) bendinin eklendiği (1) numaralı CBK'nın 485. maddesi şöyledir:

“Altyapı Yatırımları Genel Müdürlüğü

MADDE 485- (1) Altyapı Yatırımları Genel Müdürlüğünün görev ve yetkileri şunlardır:

- a) Devletçe yaptırılacak demiryolları, lojistik köy, merkez veya üsler, limanlar, barınaklar, kıyı yapıları, hava meydanlarının plan ve projelerini hazırlamak veya hazırlatmak ve onaylamak,
- b) (a) bendinde belirtilen ulaştırma altyapılarının inşaatını yapmak ve/veya yaptırmak, yapımı tamamlananları ilgili kuruluşlara devretmek,
- c) (a) bendinde belirtilen ulaştırma altyapıları ile sanayi siteleri, fabrikalar, rafineriler, endüstriyel tesisler, organize sanayi bölgeleri, endüstri bölgeleri, teknoloji geliştirme bölgeleri, maden ocakları, sanayi kuruluşları ve benzeri tesislerin demiryolları ile bağlantısını sağlamak üzere iltisak hatlarını yapmak ve/veya yaptırmak gerekli görülmesi hâlinde karayolu bağlantılarını tesis etmek ve/veya ettirmek,

ç) Kamu kurum ve/veya kuruluşları, özel sektör ve/veya tüzel kişiler tarafından tamamlanan veya devam edenler de dâhil olmak üzere (a), (b) ve (c) bentlerinde belirtilen ulaştırma altyapılarının inşaatı ve işletmesinin sağlanması amacıyla Kamu-Özel İşbirliği (KÖİ) modelleri geliştirerek esaslarını belirlemek, proje bazında gerekli görüldüğü hâllerde özel sektör gerçek ve tüzel kişilerle müzakerelerde bulunmak, katkı payları belirlemek, taahhüt vermek ve almak, kiralamak, kiraya vermek, işletmek, işlettirmek, garantiler almak ve vermek, özel sektörün katılımını sağlamak, ortaklık tesis etmek,

d) Kamu kurum ve kuruluşları, belediyeler, il özel idareleri, gerçek ve tüzel kişilerce yaptırılacak (a) bendinde yazılı ulaştırma altyapılarının proje ve şartnamelerini incelemek veya incelettirmek ve onaylamak,

e) Kamu kurum ve kuruluşları, belediyeler, il özel idarelerinin teleferik, finiküler, monoray, metro ve şehir içi raylı ulaşım sistemi kurma taleplerini değerlendirmek ve uygun olanlarını Cumhurbaşkanının iznine sunmak,

f) Kamu kurum ve kuruluşları, belediyeler ve il özel idareleri tarafından yaptırılacak teleferik, finiküler, monoray, metro ve şehir içi raylı ulaşım sistemlerinin proje ve şartnamelerini incelemek veya incelettirmek ve onaylamak,

g) (a) bendinde yazılı ulaştırma altyapıları ile teleferik, finiküler, monoray, metro ve şehir içi raylı ulaşım sistemlerinin standartlarını ve bunlarla ilgili birim fiyatları belirlemek,

ğ) Cumhurbaşkanınca yapımının üstlenilmesine karar verilen teleferik, finiküler, monoray, metro ve şehir içi raylı ulaşım sistemleri ve bunlarla ilgili tesislerin ilgili kuruluşlarla işbirliği yaparak plan, proje ve programlarını hazırlamak, hazırlatmak, incelemek, incelettirmek ve bunları yapmak veya yaptırmak,

h) Deniz altından ulaşımı ve haberleşmeyi sağlayıcı altyapı projelerini yapım ve işletim modelleri de geliştirerek planlamak, bu altyapılarla ilgili proje ve şartnameleri hazırlamak, hazırlatmak, incelemek, incelettirmek ve onaylamak, yapmak veya yaptırmak, yapımı tamamlananları ilgili kuruluşlara devretmek ve işletme esaslarını belirlemek,

ı) Denizleri, gölleri, nehirleri birbirine bağlayarak su yolu işlevi görecektir kanal ve benzeri altyapı projelerini yapım ve işletim modelleri de geliştirerek planlamak, bu altyapılarla ilgili proje ve şartnameleri hazırlamak, hazırlatmak, incelemek, incelettirmek ve onaylamak, yapmak veya yaptırmak, yapımı tamamlananları ilgili kuruluşlara devretmek ve işletme esaslarını belirlemek,

i) (Ek: RG-24/7/2018-30488 - CK-14/26 md.) 474 üncü maddenin birinci fıkrasının (a) bendi ile bu fıkranın (ı) bendinde yazılı projelerin ileri teknoloji veya yüksek maddi kaynak gerektirmesi halinde 8/6/1994 tarihli ve 3996 sayılı Bazı Yatırım ve Hizmetlerin Yap-İşlet-Devret Modeli Çerçevesinde Yaptırılması Hakkında Kanun kapsamı da dahil yap-işlet-devret modeli çerçevesinde sermaye şirketlerinin veya yabancı şirketlerin görevlendirilmesi suretiyle yapılmasını sağlamak,

j) Denetim yapmak veya yaptırmak amacıyla gerekli her türlü fiziki ve teknik altyapı ve tesisleri kurmak, kurdurmak, işletmek, işlettirmek ve bunları denetlemek,

k) Bakan tarafından verilen diğer görevleri yapmak.”

B. İlgili Görülen Kanun Hükmünde Kararname ve Cumhurbaşkanlığı Kararnamesi Kuralları

1. 27/6/1989 tarihli ve 375 sayılı 657 Sayılı Devlet Memurları Kanunu, 926 Sayılı Türk Silahlı Kuvvetleri Personel Kanunu, 2802 Sayılı Hakimler ve Savcılar Kanunu, 2914 Sayılı Yükseköğretim Personel Kanunu, 5434 Sayılı T.C. Emekli Sandığı Kanunu ile Diğer Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması, Devlet Memurları ve Diğer Kamu Görevlilerine Memuriyet Taban Aylığı ve Kıdem Aylığı ile Ek Tazminat Ödenmesi Hakkında Kanun Hükmünde Kararname'nin;

a. Ek 25. maddesi şöyledir:

“Kurumlar arası geçici görevlendirme

Ek Madde 25- (Ek: 2/7/2018 - KHK-703/178 md.)

Hâkim ve savcılar ile bu meslekten sayılanlar hariç olmak üzere, statülerine bakılmaksızın bir kadro veya pozisyona dayalı olarak kamu kurum veya kuruluşlarında istihdam edilenler, kurumlarının muvafakatiyle bir yılı geçmemek üzere diğer kamu kurum ve kuruluşlarında geçici görevlendirilebilir. Bu süre birer yıl olarak uzatılabilir.

Kamu kurum veya kuruluşlarının emrine geçici görevlendirilenler mali ve sosyal hak ve yardımlarını kurumlarından alırlar. Bunlar bu şekilde görevlendirildikleri süre boyunca kurumlarından aylıklı izinli sayılırlar.

Kurum veya kuruluşların kadro veya pozisyonlarına geçici görevlendirmenin yapılabilmesi için, görevlendirileceklerin ilgili mevzuat uyarınca kadro veya pozisyona asaleten atanmada aranan, asaleten atanmada sınav şartı aranılan kadro veya görevler için bu sınavlara girebilme hakkının elde edilmiş olması dahil, tüm şartları bir arada taşımaları gerekir. Bu şekilde görevlendirilenler görevlendirildikleri kadro veya pozisyon için öngörülen mali ve sosyal hak ve yardımlardan emsali

personel gibi faydalandırılır. Bunlar geçici görevlendirildikleri süre boyunca kurumlarından aylıksız izinli sayılırlar. Bunların Sosyal Güvenlik Kurumu ile ilişkileri kendi kurumlarındaki statüleri dikkate alınarak devam ettirilir.

Geçici görevlendirilenlerin özlük hakları devam eder ve bu süreler terfi ve emekliliklerinde hesaba katılır. Terfileri başkaca bir işleme gerek kalmaksızın süresinde yapılır. Bunların geçici görevlendirildikleri kurumda geçirdikleri süreler kendi kurumlarında geçirilmiş sayılır. Akademik unvanların kazanılması için gerekli şartlar saklıdır.

Bu maddeye göre görevlendirilenler, görevlendirildikleri kurumların mevzuatına uymakla yükümlüdür.

Toplamda altı ayı geçen görevlendirmelerde personelin muvafakatinin de alınması şarttır.

Kanunlarda yer alan geçici görevlendirme hükümleri saklıdır.

Bu madde kapsamında görevlendirmeye ilişkin usul ve esaslar Devlet Personel Başkanlığınca hazırlanarak Cumhurbaşkanınca yürürlüğe konulacak yönetmelikle belirlenir.”

b. Ek 26. maddesi şöyledir:

“Yerli veya yabancı sözleşmeli personel istihdamı

Ek Madde 26- (Ek: 2/7/2018 - KHK-703/178 md.)

Cumhurbaşkanlığı, bakanlıklar ile diğer kamu kurum ve kuruluşlarının teşkilatlanmasına ilişkin Cumhurbaşkanlığı kararnamelerinde öngörülmesi kaydıyla; 657 sayılı Devlet Memurları Kanunu ve diğer kanunların sözleşmeli personel çalıştırılması hakkındaki hükümlere bağlı olmaksızın, özel bilgi ve uzmanlık gerektiren geçici mahiyetteki işlerde, yerli veya yabancı personel tam zamanlı, kısmi zamanlı veya projelerle sınırlı olarak sözleşmeyle istihdam edilebilir.

Bunlara verilecek her türlü ödemeler dahil ücretler, 657 sayılı Kanunun 4 üncü maddesinin (B) bendine göre çalıştırılanlar için uygulanmakta olan sözleşme ücreti tavanının beş katını aşmamak üzere Cumhurbaşkanı veya yetkilendireceği makamca ilgililerin yürüteceği görevler göz önüne alınarak tespit edilir. (Mülga cümle:16/7/2020-7250/26 md.) (...)

Bu madde kapsamında sözleşmeli olarak istihdam edilen personel, 31/5/2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 4 üncü maddesinin birinci fıkrasının (a) bendi kapsamında sigortalı sayılır. Ancak teşkilatlanmalara ilişkin Cumhurbaşkanlığı kararnamelerinde öngörülmesi halinde personel 5510 sayılı Kanunun 4 üncü maddesinin birinci fıkrasının (c) bendi ile ilgilendirilir.

Bu madde kapsamında kısmi zamanlı olarak çalıştırılanlar için iş sonu tazminatı ödenmez ve işsizlik sigortası primi yatırılmaz.

Kanunlardaki özel hükümler saklı kalmak kaydıyla, bu statüde çalıştırılma, sözleşme bitiminde kamu kurum ve kuruluşlarında herhangi bir pozisyon, kadro veya statüde çalışma açısından kazanılmış hak teşkil etmez.

Bu kapsamda istihdam edilecek personelde kurumsal hizmetlerin gerektirmesi halinde aranacak öğrenim ve yabancı dil bilgisi şartı ile diğer şartlar, bunların işe alınmaları, sınav ve istisnaları, sözleşme süre, usul ve esasları, görev, yetki ve yükümlülükleri, sözleşmelerinin feshi ile istihdamlarına dair diğer hususlar Devlet Personel Başkanlığının görüşü alınarak kurumlarca çıkarılacak yönetmelikle belirlenir.”

2. (1) numaralı CBK'nın 474. maddesinin (1) numaralı fıkrasının ilgili bölümü şöyledir:

“(1) Ulaştırma ve Altyapı Bakanlığının görev ve yetkileri şunlardır:

a) Ulaştırma, denizcilik, haberleşme ve posta iş ve hizmetleri ile Karadeniz ile Marmara denizini birleştiren ve gemilerin seyrüseferine imkân veren Kanal İstanbul ve benzeri su yolu projelerinin geliştirilmesi, kurulması, kurdurulması, işletilmesi ve işlettilmesi hususlarında, ilgili kurum ve kuruluşlarla koordinasyon içerisinde, milli politika, strateji ve hedeflerin belirlenmesi amacıyla çalışmalar yapmak ve belirlenen hedefleri uygulamak,

..”

II. İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Zühtü ARSLAN, Burhan ÜSTÜN, Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Rıdvan GÜLEÇ, Recai AKYEL ve Yusuf Şevki HAKYEMEZ'in katılımlarıyla 17/10/2018 tarihinde yapılan ilk inceleme toplantısında dosyada eksiklik bulunmadığından işin esasının incelenmesine, yürürlüğü durdurma talebinin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

III. ESASIN İNCELENMESİ

2. Dava dilekçesi ve ekleri, Raportör Fatma KARAMAN ODABAŞI tarafından hazırlanan işin esasına ilişkin rapor, dava konusu ve ilgili görülen CBK kuralları ile Kanun Hükmünde Kararname (KHK)

kuralları, dayanan ve ilgili görülen Anayasa kuralları ile bunların gerekçeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A. Cumhurbaşkanlığı Kararnemelerinin Anayasal Çerçevesi ve Yargısal Denetimi

3. 21/1/2017 tarihli ve 6771 sayılı Türkiye Cumhuriyeti Anayasasında Değişiklik Yapılmasına Dair Kanun ile Anayasa'nın bazı maddelerinde değişiklik yapılmıştır. Yapılan değişikliklerle yeni bir hükümet sistemine geçilmiş ve buna bağlı olarak Cumhurbaşkanı'nın görev ve yetkileri yeniden düzenlenmiştir. Anayasa'nın 8. maddesinde, yürütme yetkisi ve görevinin Cumhurbaşkanı ve Bakanlar Kuruluna ait olduğu ifade edilmekte iken maddede yapılan değişiklikle Bakanlar Kurulu kaldırılarak yürütme yetkisi ve görevi tek başına Cumhurbaşkanı'na verilmiştir. Anayasa'da Bakanlar Kuruluna verilen görev ve yetkilere ilişkin maddelerde de aynı doğrultuda değişiklik yapılarak daha önce Bakanlar Kuruluna ait olan görev ve yetkilerin Cumhurbaşkanı tarafından yerine getirilmesi öngörülmüştür.

4. Yeni hükümet sisteminin en önemli özelliklerinden biri Cumhurbaşkanı'na "Cumhurbaşkanlığı Kararnamesi" adı altında düzenleme yapma yetkisinin tanınmasıdır. CBK'ların en belirgin özelliği ise Cumhurbaşkanı'na belirli konularda ilk elden düzenleme yapma yetkisinin verilmiş olmasıdır. Yürütmenin diğer düzenleyici işlemlerinden farklı olarak Cumhurbaşkanı Anayasa'da belirlenen yetki çerçevesinde herhangi bir kanuna dayanmadan ya da yasama organının onayı olmadan CBK'lar yoluyla düzenleme yapabilecektir.

5. Anayasa'nın 104. maddesinin on yedinci fıkrasının birinci cümlesinde Cumhurbaşkanı'nın yürütme yetkisine ilişkin konularda CBK çıkarabileceği hüküm altına alınmıştır. Düzenlemeyle yürütme yetkisine ilişkin olmak kaydıyla CBK çıkarma konusunda Cumhurbaşkanı'na genel bir yetki verilmiştir. Maddenin gerekçesinde, yeni hükümet sistemi gözetilerek Cumhurbaşkanı'nın genel siyasetin yürütülmesinde yürütme yetkisi ile ilgili olarak ihtiyaç duyduğu konularda CBK çıkarabilmesine imkân tanımak amacıyla ilk elden düzenleme yapma yetkisinin tanındığı ifade edilmiştir.

6. Cumhurbaşkanı'na yürütme yetkisine ilişkin konularda CBK çıkarma yetkisinin genel olarak verilmesinin yanı sıra Anayasa'nın diğer bazı maddelerinde belirtilen kimi konuların CBK ile düzenleneceği ayrıca ifade edilmiştir. Bu kapsamda Anayasa'nın 104. maddesinin dokuzuncu fıkrasında üst kademe kamu yöneticilerinin atanmalarına ilişkin usul ve esasların; 106. maddesinin on birinci fıkrasında bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulmasının; 108. maddesinin dördüncü fıkrasında Devlet Denetleme Kurulunun işleyişi, üyelerinin görev süresi ve diğer özlük işlerinin; 118. maddesinin altıncı fıkrasında

Millî Güvenlik Kurulu Genel Sekreterliğinin teşkilatı ve görevlerinin CBK'larla düzenleneceği hüküm altına alınmıştır. Anayasa'nın 123. maddesinin üçüncü fıkrasında ise kamu tüzel kişiliğinin kanunla veya CBK ile kurulacağı belirtilmiştir.

7. Anayasa'nın 148. maddesinde CBK'ların şekil ve esas bakımından Anayasa'ya uygunluğunun denetlenmesi öngörülmüş, yargısal denetim görev ve yetkisi de Anayasa Mahkemesine verilmiştir.

8. Anayasa'da Cumhurbaşkanı'na CBK çıkarma yetkisi verilmekle birlikte bu yetki sınırsız değildir. Kanunlardan farklı olarak Anayasa'da CBK'yla düzenlenecek konular sınırlandırılmıştır. Konu bakımından yetki yönünden getirilen bu sınırlamalar Anayasa'nın 104. maddesinin on yedinci fıkrasının ilk dört cümlesinde düzenlenmiştir.

9. Anılan fıkranın birinci cümlesinde Cumhurbaşkanı'nın yürütme yetkisine ilişkin konularda CBK çıkarabileceği ifade edilmiştir. Buna göre yürütme yetkisine ilişkin konular dışında CBK ile düzenleme yapılması mümkün değildir.

10. Fıkranın ikinci cümlesinde "Anayasa'nın ikinci kısmının birinci ve ikinci bölümlerinde yer alan temel haklar, kişi hakları ve ödevleriyle dördüncü bölümde yer alan siyasi haklar ve ödevlerin" CBK'yla düzenlenemeyeceği belirtilmiştir. Bu hüküm uyarınca belirtilen alanlarda CBK ile düzenleme yapılamaz.

11. Fıkranın üçüncü cümlesinde de Anayasa'da münhasıran kanunla düzenlenmesi öngörülen konularda CBK çıkarılmayacağı hüküm altına alınmıştır. Ancak Anayasa'da hangi konuların münhasıran kanunla düzenleneceğine ilişkin özel bir hüküm bulunmamaktadır. Bununla birlikte Anayasa Mahkemesinin yerleşik içtihadında anayasa koyucunun kanunla düzenlenmesini öngördüğü konuların bu kapsamda görülmesi gerektiği kabul edilmektedir (AYM, E.2016/150, K.2017/179, 28/12/2017, § 57; E.2016/180, K.2018/4, 18/1/2018, § 17; E.2017/51, K.2017/163, 29/11/2017, § 13; E.2016/139, K.2016/188, 14/12/2016, § 9; E.2013/47, K.2013/72, 6/6/2013). Buna göre Anayasa'da kanunla düzenleneceği belirtilen alanlarda Cumhurbaşkanı'nın CBK çıkarma yetkisi bulunmamaktadır.

12. Fıkranın dördüncü cümlesinde ise kanunda açıkça düzenlenen konularda CBK çıkarılmayacağı ifade edilmiştir. Anılan hükme göre Cumhurbaşkanı'nın yürütme yetkisine ilişkin konularda CBK çıkarabilmesi için CBK'yla düzenlenecek konunun kanunlarda açıkça düzenlenmemiş olması gerekir.

13. CBK'ların yukarıda belirtilen konu bakımından yetki kurallarına uygun olarak çıkarılması gerekmektedir. Aksi takdirde içeriği Anayasa'ya aykırılık oluşturmasa bile bu düzenlemelerin Anayasa'ya uygunluğundan söz edilemez. Dolayısıyla CBK'ların yargısal denetiminde öncelikle

Anayasa'nın 104. maddesinin on yedinci fıkrasında belirtilen konu bakımından yetki kurallarına uygunluğunun ele alınması gerekir. Anılan fıkra yönünden herhangi bir aykırılık tespit edilmemesi durumunda ise bu defa CBK'ların içerik yönünden Anayasa'ya uygunluk denetimi yapılmalıdır.

B. CBK'nın 17. Maddesinin (2) Numaralı Fıkrasının Birinci Cümlesinde Yer Alan "...gerekli gördüğü bilgileri..." İbaresinin İncelenmesi

1. Genel Açıklama

14. Kişisel verilerin korunması hakkı Anayasa'nın 20. maddesi kapsamında anayasal güvenceye bağlanmış olup kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir. Buna göre veri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esaslar bu konuda kabul edilmiş genel kanun niteliğindeki 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda düzenlenmiş, bazı kanunlarda da kişisel verilerle ilgili hükümlere yer verilerek konuya ilişkin yasal güvencenin sağlanması amaçlanmıştır.

15. 6698 sayılı Kanun'un 3. maddesinin (e) bendinde kişisel verilerin elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem kişisel verinin işlenmesi olarak ifade edilmiştir.

16. Anılan Kanun'un 4. maddesinin (1) numaralı fıkrasında kişisel verilerin ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği belirtilmiştir. Yine Kanun'un 4. maddesinin (2) numaralı fıkrası ile 5. ve 6. maddelerinde kişisel verilerin işlenmesinde uyulması zorunlu genel ilkeler, kişisel verilerin ilgili kişinin rızasıyla veya rızaya dayalı olmaksızın işlenmesi şartları düzenlenmiş; kişisel verilerin silinmesi, yok edilmesi, anonim hâle getirilmesi şartları ise Kanun'un 7. maddesinde ayrıca belirtilmiştir. Kanun'un Üçüncü Bölüm'ü ve Beşinci Bölüm'ünde ise kişisel verileri işlenen gerçek kişiler ile kişisel verileri işleyen gerçek veya tüzel kişilerin hak ve yükümlülükleri ile kanun hükümlerine aykırı hareket edenler yönünden uygulanacak cezai hükümlere yer verilmiştir.

17. Kural olarak kişisel verisi işlenen gerçek kişinin açık rızası olmaksızın kişisel verilerin yurt içindeki veya yurt dışındaki üçüncü kişilere aktarılması mümkün olmamakla birlikte Kanun'un 8. ve 9. maddelerinde kişinin açık rızası aranmaksızın kişisel verilerin aktarılması şartları ile buna ilişkin usul ve esaslar düzenlenmiştir. Buna göre kişisel verinin aktarıldığı gerçek veya tüzel kişinin kimliğinden bağımsız olarak kişisel verinin aktarılmasına ilişkin işlemlerin anılan maddelerde belirtilen usul ve esaslar çerçevesinde gerçekleştirilmesi zorunludur.

18. 6698 sayılı Kanun'un uygulanması bakımından genel olarak Kanun'a tabi bulunan kişiler, kurum veya kuruluşlar tek tek belirtmek suretiyle herhangi bir istisna öngörülmemiş olup yalnızca Kanun'un 28. maddesinde kişisel verinin işlenmesindeki amaç ve kapsam yönünden birtakım istisnalara yer verilmiştir. Buna göre anılan Kanun kapsamında kalan ve kişisel veriyi ilk defa elde edenler ile kişisel veriyi herhangi bir surette elinde bulunduran tüm gerçek ve tüzel kişilerin, kurum ve kuruluşlar ile bunların personelinin Kanun'da belirtilen usul ve esaslara uygun hareket etmesi gerekecektir.

2. İptal Talebinin Gerekçesi

19. Dava dilekçesinde özetle; İletişim Başkanlığının (Başkanlık) görevleriyle ilgili olarak gerekli göreceği bilgiler içinde kişisel verilerin de yer almasının mümkün olduğu, kuralın kişisel verilerin korunmasına ilişkin bir düzenleme içermediği, kişisel verilerin toplanması, işlenmesi, analizi, paylaşılması gibi faaliyetlerin kanunla düzenlenmesi gerektiği, genel çerçevesi, ilke ve esasları belirlenmeden kişiler hakkında bilgi ve veri toplamak için idareye yetki verilmesinin hukuki belirlilik ilkesine aykırı olduğu, kişisel verilerin Anayasa'nın kişi hak ve ödevlerine ilişkin İkinci Kısım İkinci Bölüm'ünde düzenlendiği, buna göre ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilecek olan kişisel verilerin korunmasına ilişkin esas ve usullerin de kanunla belirlenmesi gerektiği, temel haklar, kişi hakları ve ödevlerinin CBK ile düzenlenemeyeceği belirtilerek kuralın Anayasa'nın 20. ve 104. maddelerine aykırı olduğu ileri sürülmüştür.

3. Anayasa'ya Aykırılık Sorunu

a. Kuralın Konu Bakımından Yetki Yönünden İncelenmesi

20. Dava dilekçesinde konu bakımından yetki yönünden kuralın Anayasa'nın 20. maddesine de aykırı olduğu ileri sürülmüş ise de CBK'ya ilişkin konu bakımından yetki kuralları Anayasa'nın 104. maddesinin on yedinci fıkrasında düzenlendiğinden bu husustaki inceleme anılan fıkra kapsamında yapılacaktır.

21. CBK'nın 17. maddesinin (2) numaralı fıkrasının birinci cümlesinde Başkanlığın görevleri ile ilgili olarak gerekli gördüğü bilgileri bütün kamu kurum ve kuruluşlarından ve diğer gerçek ve tüzel kişilerden doğrudan istemeye yetkili olduğu belirtilmiş, aynı fıkranın ikinci cümlesinde ise kendilerinden bilgi istenen bütün kamu kurum ve kuruluşları ile diğer gerçek ve tüzel kişilerin bu bilgileri istenen süre içinde öncelikle ve zamanında vermekle yükümlü oldukları öngörülmüştür. Dava konusu kural anılan fıkranın birinci cümlesinde yer alan "...gerekli gördüğü bilgileri..." ibaresidir.

22. CBK'nın 1. maddesi uyarınca Başkanlık doğrudan Cumhurbaşkanlığına bağlı, genel bütçeli bir kamu kurumu olarak kurulmuştur. 3. maddeye göre de Başkanlık ülkenin tanıtılmasına, ulusal ve uluslararası düzeyde kamuoyunun ve ilgili makamların doğru bilgilendirilmesine ve aydınlatılmasına, bu hususta bilgi akışının ve haber takibinin sağlanmasına, iletişim standartlarının belirlenmesine, basın yayın alanındaki faaliyetlerin gerçekleştirilmesine ilişkin görevlere sahiptir. Başkanlığı anılan görevleri kapsamında gerekli gördüğü bilgileri istemeye yetkili kılan kuralın yürütme yetkisine ilişkin konuyu düzenlediği anlaşılmaktadır.

23. Başkanlığın tanıtım, iletişim, bilgilendirme, doğru bilgiyle aydınlatma, iş birliği ve koordinasyon ile basın yayın odaklı görevleri dikkate alındığında gerekli olan bilgileri isteyebilmesinin görevlerini yerine getirebilmesi bakımından gerekli olduğu açıktır. Nitekim istenebilecek bilgiler Başkanlığın görevleriyle ilgili olanlar ile sınırlı tutulmuştur. Bir başka deyişle kural, Başkanlığın belirlenen görevlerinin yerine getirilebilmesinin doğal ve zorunlu bir sonucu olarak bilgi isteme yetkisini düzenlemekte olup kişisel verilere ilişkin bir düzenleme niteliğinde değildir.

24. 6698 sayılı Kanun kapsamında yer alan ve kişisel verilere ilişkin yükümlülükler ile uyulacak usul ve esasları düzenleyen çeşitli hükümlere Genel Açıklama bölümünde yer verilmiştir (bkz. §§ 14-18). Kuralın kişisel verilerin korunmasına ilişkin mevzuat hükümlerinin uygulanmasını engelleyen, sınırlandıran, genişleten, uygulanmasına istisna getiren veya herhangi bir surette bu hükümlere temas eden bir yönü bulunmadığı gibi kişisel verilere ilişkin her türlü işlemin 6698 sayılı Kanun ile kişisel verilere ilişkin diğer kanunlarda yer alan hükümlere uygun olarak gerçekleştirileceği açıktır.

25. Bu itibarla kişisel verilere ilişkin düzenleme içermeyen ve kişisel verilerle ilgili bulunmayan kuralın Anayasa'nın İkinci Kısım Birinci ve İkinci Bölümlerinde yer alan temel haklar, kişi hakları ve ödevleriyle Dördüncü Bölüm'ünde yer alan siyasi haklar ve ödevler kapsamında bulunduğu söylenemez.

26. Anayasa'nın 123. maddesinin birinci fıkrasına göre "İdare, kuruluş ve görevleriyle bir bütündür ve kanunla düzenlenir" Ancak Anayasa'nın 106. maddesinin on birinci fıkrasında "Bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulması Cumhurbaşkanlığı kararnamesiyle düzenlenir" denilmek suretiyle bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulması yönünden CBK'larla düzenleme yapılmasına açıkça izin verilmiştir.

27. Bu bağlamda Anayasa'nın CBK'lar tarafından düzenleneceğini özel olarak öngördüğü bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulmasının düzenlenmesi kapsamında, bu konularla sınırlı olmak üzere

Anayasa'nın 123. maddesinin anılan hükmünde belirtilen hususlarda düzenleme yapılabilir (AYM, E.2019/31, K.2020/5, 23/1/2020, § 31).

28. Anayasa'nın "Cumhurbaşkanı yardımcıları, Cumhurbaşkanına vekâlet ve bakanlar" başlıklı 106. maddesinin on birinci fıkrasında; bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının CBK ile düzenleneceği öngörülmüş olup Cumhurbaşkanlığı merkez teşkilatı ile Cumhurbaşkanlığına bağlı kurum ve kuruluşlara ilişkin ayrıca bir hükme yer verilmemiştir.

29. 6771 sayılı Kanun'la yapılan Anayasa değişikliğinin gerekçesinde Cumhurbaşkanı'na ilk elden CBK çıkarma yetkisi verilmesinin amacı, yeni hükümet sisteminde Cumhurbaşkanı'nın genel siyasetin yürütülmesinde ihtiyaç duyduğu konularda düzenleme yapabilmesini sağlamak olarak açıklanmaktadır (bkz. § 5).

30. Bu kapsamda CBK'lar ile bakanlıkların kurulmasını, kaldırılmasını, görevleri ve yetkilerini, teşkilat yapısını düzenleyebilme yetkisini haiz Cumhurbaşkanı'nın, Cumhurbaşkanlığı merkez teşkilatı ile Cumhurbaşkanlığına bağlı kurum ve kuruluşların da kurulması, kaldırılması, görevleri ve yetkileri ile teşkilat yapısını CBK ile düzenleyebileceği evleviyetle kabul edilmelidir. Kaldı ki Cumhurbaşkanı'nın Anayasa'nın 106. maddesinin on birinci fıkrasına göre bakanlık bünyesinde kurarak teşkilatını düzenleyebileceği bir kurumu tercihen Cumhurbaşkanlığına bağlı kurum veya kuruluş olarak kurması hâlinde ilgili kurum ve kuruluş için Anayasa'nın 123. maddesinde belirtilen sınırlardan dolayı CBK ile düzenleme yapamayacağına kabulü Anayasa'nın genel sistematiğine ve bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulması konusunda CBK çıkarma yetkisi tanıyan anayasal hükmün amacına aykırı olacaktır (AYM, E.2019/71, K.2020/82, 30/12/2020, § 27).

31. Bu itibarla kuralın ilişkin olduğu Cumhurbaşkanlığına bağlı kurum ve kuruluşların görev ve yetkisi konusunun Anayasa'nın 106. maddesinin on birinci fıkrası uyarınca CBK ile düzenlenmesi açıkça hükme bağlanmış olan bakanlıklara dair yetki kapsamında kaldığı değerlendirilmektedir. Dolayısıyla Cumhurbaşkanlığı merkez teşkilatı ile Cumhurbaşkanlığına bağlı kurum ve kuruluşların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulmasına dair düzenlemelerin CBK ile yapılması Anayasa'ya aykırılık teşkil etmemektedir (E.2019/71, K.2020/82, § 28).

32. Buna göre Cumhurbaşkanlığına bağlı olarak CBK ile kurulmuş bulunan Başkanlığın görevleriyle ilgili bilgi isteme yetkisini düzenleyen dava konusu kuralın Anayasa'nın 104. maddesinin on yedinci fıkrasının üçüncü cümlesini ihlal eden bir yönü bulunmamaktadır.

33. Kuralın da yer aldığı CBK, Başkanlığın kurulmasına, teşkilatlanmasına, görev ve yetkilerine ilişkin usul ve esasları düzenlemek amacıyla kabul edilmiştir. Buna göre ilk kez (14) numaralı CBK ile kurulmuş olan Başkanlığın bilgi toplama yetkisine yönelik kuralın kanunda açıkça düzenlenen bir konuya ilişkin olmadığı anlaşılmaktadır.

34. Açıklanan nedenlerle kural Anayasa'nın 104. maddesinin on yedinci fıkrasına aykırı değildir. İptal talebinin reddi gerekir.

Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ ve Yusuf Şevki HAKYEMEZ bu görüşe katılmamışlardır.

b. Kuralın İçerik Yönünden İncelenmesi

35. 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 43. maddesi uyarınca kural, ilgisi nedeniyle Anayasa'nın 2. maddesi yönünden incelenmiştir.

36. Anayasa'nın 2. maddesinde belirtilen hukuk devleti; eylem ve işlemleri hukuka uygun, insan haklarına saygılı, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adil bir hukuk düzeni kurup bunu geliştirerek sürdüren, hukuki güvenliği sağlayan, Anayasa'ya aykırı durum ve tutumlardan kaçınan, hukuk kurallarıyla kendini bağlı sayan ve yargı denetimine açık olan devlettir.

37. Hukuk devletinin temel unsurlarından biri belirlilik ilkesidir. Anayasa Mahkemesinin yerleşik kararlarına göre anılan ilke, yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olmasını gerektirmektedir. Belirlilik ilkesi, hukuksal güvenlikle bağlantılı olup birey, kanundan belirli bir kesinlik içinde hangi somut eylem ve olguya hangi hukuksal yaptırımın veya sonucun bağlandığını, bunların idareye hangi müdahale yetkisini verdiğini bilmesini zorunlu kılmaktadır.

38. Anayasa Mahkemesi birçok kararında belirlilik ilkesinin yalnızca yasal belirliliği değil daha geniş anlamda hukuki belirliliği ifade ettiğini, yasal düzenlemeye dayanarak erişilebilir, bilinebilir ve öngörülebilir olma gibi niteliklere ilişkin gereklilikleri karşılama koşuluyla mahkeme içtihatları ve yürütmenin düzenleyici işlemleri ile de hukuki belirliliğin sağlanabileceğini, asıl olanın muhtemel muhataplarının mevcut şartlar altında belirli bir işlemin ne tür sonuçlar doğurabileceğini öngörmelerini mümkün kılacak bir normun varlığı olduğunu vurgulamıştır. Anılan ilkenin yürütmenin asli düzenleyici işlemi niteliğinde olan CBK'lar bakımından da geçerli olduğunda şüphe bulunmamaktadır.

39. Kuralın Başkanlığın CBK'da açıkça düzenlenmiş olan görevlerini yerine getirebilmesi amacıyla düzenlendiği ve istenebilecek bilgilerin Başkanlığın görevleriyle ilgili ve gerekli olanlarla sınırlandırıldığı anlaşılmaktadır. Gerekli görülen bilgilerin istenmesindeki amaç, kapsam ve sınır açıkça belirlenmiş olup kuralın hem kişiler hem de idare yönünden belirli ve öngörülebilir olduğu açık olduğundan kuralda belirsizlik bulunmamaktadır.

40. Açıklanan nedenlerle kural Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir. Yusuf Şevki HAKYEMEZ iptal talebinin reddine farklı gerekçeyle katılmıştır.

Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM ve M. Emin KUZ bu görüşe katılmamışlardır.

C. CBK'nın 21. Maddesinin (3) Numaralı Fıkrasının Üçüncü Cümlesinin İncelenmesi

1. Anlam ve Kapsam

41. Başkanlığın teşkilat, görev ve yetkilerine ilişkin usul ve esasları düzenleyen CBK'nın dava konusu kuralın da yer aldığı 21. maddesinde Başkanlıkta istihdam edilecek, çalıştırılacak ve görevlendirilecek personele ilişkin kurallara yer verilmiştir.

42. Anılan maddenin (1) ve (2) numaralı fıkralarına göre Başkanlıkta 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu'nun ek 41. maddesine göre iletişim uzmanı ve iletişim uzman yardımcısı istihdam edilecek olup bu personel mali ve sosyal hak ve yardımları ile diğer özlük hakları bakımından 375 sayılı KHK'nın ek 30. maddesi uyarınca adalet uzmanı ve adalet uzman yardımcısına denk olacaktır.

43. Maddenin (3) numaralı fıkrasının birinci cümlesinde Başkanlıkta 657 sayılı Kanun'a tabi personel istihdam edileceği belirtilmiş, ikinci cümlede ise 375 sayılı KHK'nın ek 26. maddesi çerçevesinde Başkanlığın sözleşmeli personel istihdam edebileceği gibi aynı KHK'nın ek 25. maddesi çerçevesinde diğer kurumlardan geçici olarak personel görevlendirebileceği de düzenlenmiştir.

44. Anılan kurallar uyarınca Başkanlık bünyesinde 657 sayılı Kanun'a tabi personel istihdam edileceği gibi 375 sayılı KHK'nın ek 25. maddesi kapsamında bir kadro veya pozisyona dayalı olarak bir kamu kurum veya kuruluşunda istihdam edilenlerin de geçici olarak görevlendirilmeleri mümkün olacak; yine aynı KHK'nın ek 26. maddesi kapsamında özel bilgi ve uzmanlık gerektiren geçici mahiyetteki işlerde ise yerli veya yabancı personel tam zamanlı, kısmi zamanlı veya projelerle sınırlı olarak sözleşmeyle istihdam edilebilecektir. Ancak ek 26. madde uyarınca bu şekilde sözleşmeli olarak

çalışma sözleşme bitiminde kamu kurum ve kuruluşlarında herhangi bir pozisyon, kadro veya statüde çalışma açısından kazanılmış hak teşkil etmeyecektir.

45. 375 sayılı KHK'nın ek 26. maddesinde bu kapsamda çalıştırılacak personelin sözleşme usul ve esasları ile ödeme ve ücret hususlarında birtakım düzenlemelere de yer verilmiştir. Buna göre sözleşmeli personele verilecek her türlü ödemeler dâhil ücretler, 657 sayılı Kanun'un 4. maddesinin (B) bendine göre çalıştırılanlar için uygulanmakta olan sözleşme ücreti tavanının beş katını aşmamak üzere Cumhurbaşkanı veya yetkilendireceği makamca ilgililerin yürüteceği görevler göz önüne alınarak tespit edilecektir. Sözleşmeli personelde kurumsal hizmetlerin gerektirmesi hâlinde aranacak öğrenim ve yabancı dil bilgisi şartı ile diğer şartlar, bunların işe alınmaları, sınav ve istisnaları, sözleşme süre, usul ve esasları, görev, yetki ve yükümlülükleri, sözleşmelerinin feshi ile istihdamlarına dair diğer hususlar kurumlarca çıkarılacak yönetmelikle belirlenecektir.

46. Dava konusu kural CBK'nın 21. maddesinin (3) numaralı fıkrası kapsamında çalıştırılacak personelin sözleşme usul ve esasları ile ücret miktarı ve her çeşit ödemelerinin Cumhurbaşkanınca tespit edileceğini öngörmektedir.

2. İptal Talebinin Gerekçesi

47. Dava dilekçesinde özetle; Başkanlığın Cumhurbaşkanlığına bağlı genel bütçeli bir kamu kurumu olduğu, kurum çalışanlarının da kamu görevlisi niteliğine sahip buldukları, kamu görevlisi olan kurum çalışanlarının sözleşme usul ve esasları ile ücret miktarları ve her çeşit ödemelerinin kanunla düzenlenmesi gerektiği, bu konularda CBK veya Cumhurbaşkanı kararı ile düzenleme veya belirleme yapılamayacağı, kural kapsamında kalan konuların 375 sayılı KHK'nın ek 26. maddesinde düzenlendiği, kanunda açıkça düzenlenen konularda CBK çıkarılamayacağı, yürütme görev ve yetkisinin Anayasa'ya ve kanunlara uygun olarak kullanılması gerektiği belirtilerek kuralın Anayasa'nın 8., 104. ve 128. maddelerine aykırı olduğu ileri sürülmüştür.

3. Anayasa'ya Aykırılık Sorunu

48. Dava dilekçesinde konu bakımından yetki yönünden kuralın Anayasa'nın 8. ve 128. maddelerine de aykırı olduğu ileri sürülmüş ise de CBK'ya ilişkin konu bakımından yetki kuralları Anayasa'nın 104. maddesinin on yedinci fıkrasında düzenlendiğinden bu husustaki inceleme anılan fıkra kapsamında yapılacaktır.

49. Anayasa'nın 104. maddesinin on yedinci fıkrasının dördüncü cümlesinde kanunda açıkça düzenlenen konularda CBK çıkarılamayacağı kurala bağlanmıştır. Türkiye Büyük Millet Meclisinin (TBMM) Anayasa'nın 87. maddesinde düzenlenen kanun koyma yetkisi kapsamında kanun adı

altında yaptığı düzenlemelerin bu kapsamda olduğunda kuşku bulunmadığı gibi Anayasa'nın mülga 91. maddesi kapsamında çıkarılmış olan ve niteliği, getiriliş amacı, Anayasa Mahkemesinin KHK'lara ilişkin içtihadı ve uygulama dikkate alındığında kanun hükmünde oldukları anlaşılan KHK'ların da aynı kapsamda kabul edilmesi gerekmektedir. Dolayısıyla KHK ile açıkça düzenlenen bir konuda da Anayasa'nın 104. maddesinin on yedinci fıkrasının dördüncü cümlesi uyarınca CBK çıkarılmaması gerekir (AYM, E.2019/78, K.2020/6, 23/1/2020, §§ 33-39; E.2019/105, K.2020/30, 12/6/2020, §§ 24-29).

50. Anayasa'nın 104. maddesinin on yedinci fıkrasının dördüncü cümlesi uyarınca yapılacak denetimde karşılaştırmaya esas olabilecek, daha önce çıkarılmış bir kanun olup olmadığının tespit edilmesi gerekir. Sonrasında ise -böyle bir kanun varsa- incelenen CBK kuralının kanunun açıkça düzenlediği konuyu düzenleyip düzenlemediği belirlenmelidir. Bu değerlendirme yapılırken önce ilgili kanunun CBK ile düzenlenen alanda hüküm ifade edip etmediğinin belirlenmesi, ardından da kanundaki düzenlemenin açık olup olmadığının tespit edilmesi gerekir. Bu bağlamda CBK kuralı olmasaydı, karşılaştırmaya esas alınan kanun hükmünün CBK ile düzenleme yapılan konuya uygulanacak olup olmaması, CBK kuralının kanun ile düzenlenen konuda çıkarılıp çıkarılmadığına dair bir gösterge olacaktır (AYM, E.2019/31, K.2020/5, 23/1/2020, § 17; E.2019/105, K.2020/30, 12/6/2020, § 30).

51. 375 sayılı KHK'nın ek 26. maddesinde, dava konusu kural kapsamında çalıştırılacak sözleşmeli personele verilecek her türlü ödemeler dâhil ücretlerin 657 sayılı Kanun'un 4. maddesinin (B) bendine göre çalıştırılanlar için uygulanmakta olan sözleşme ücreti tavanının beş katını aşmamak üzere Cumhurbaşkanı veya yetkilendireceği makamca tespit edileceği, bu şekilde istihdam edilecek personel yönünden kurumsal hizmetlerin gerektirmesi hâlinde aranacak öğrenim ve yabancı dil bilgisi şartı ile diğer şartların, işe alınma, sınav ve istisnaları, sözleşme süre, usul ve esasları, görev, yetki ve yükümlülükleri, sözleşmelerin feshi ile istihdamlarına dair diğer hususların kurumlarca çıkarılacak yönetmelikle belirleneceği ifade edilerek sözleşmeli personelin çalıştırılmasına ilişkin birtakım esaslar belirlenmiştir. Dava konusu CBK kuralının da sözleşmeli personelin sözleşme usul ve esasları ile CBK'nın 21. maddesinin (3) numaralı fıkrası kapsamında çalıştırılacak personelin ücret miktarı ve her çeşit ödemeleriyle ilgili olduğu, 375 sayılı KHK'da açıkça düzenlenen konulara ilişkin bulunduğu anlaşılmaktadır.

52. Nitekim dava konusu CBK kuralının bulunmaması durumunda anılan KHK hükmünün CBK kuralı ile düzenleme yapılan konuya uygulanacağı anlaşılmaktadır.

53. Bu çerçevede KHK'nın açıkça düzenlediği bir konuda düzenleme yapan CBK kuralı Anayasa'nın 104. maddesinin on yedinci fıkrasının dördüncü cümlesine aykırı bir düzenleme getirmektedir.

54. Açıklanan nedenlerle kural Anayasa'nın 104. maddesinin on yedinci fıkrasının dördüncü cümlesine aykırıdır. İptali gerekir.

Kural Anayasa'nın 104. maddesinin on yedinci fıkrasının dördüncü cümlesine aykırı görülerek iptal edildiğinden ayrıca aynı fıkranın birinci, ikinci ve üçüncü cümleleri yönünden incelenmemiştir.

Kural konu bakımından yetki yönünden Anayasa'nın 104. maddesinin on yedinci fıkrasının dördüncü cümlesine aykırı görülerek iptal edildiğinden ayrıca içerik yönünden incelenmemiştir.

Ç. CBK'nın 22. Maddesinin (1) Numaralı Fıkrasında Yer Alan "...yurtdışı ve..." İbaresinin İncelenmesi

1. İptal Talebinin Gerekçesi

55. Dava dilekçesinde özetle; Anayasa'da idarenin kuruluş ve görevleriyle bir bütün olduğunun ve kanunla düzenlenebileceğinin genel kural olarak belirlendiği, CBK ile kamu tüzel kişiliği kurulabilmesinin genel kuralın istisnası olarak ayrıca düzenlendiği, istisnaların dar yorumlanması gerektiği ve yorum yoluyla genişletilemeyeceği, CBK ile kamu tüzel kişiliği kurulmasına imkân veren Anayasa hükmünün yurt dışı teşkilatı kurma yetkisini de kapsadığının söylenemeyeceği, yine yurt dışı teşkilatı kurma yetkisini Başkanlığa tanıyan kuralın yurt dışı teşkilatının bir yürütme işlemiyle kurulmasını mümkün hâle getirdiği belirtilerek kuralın Anayasa'nın 123. maddesine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

a. Kuralın Konu Bakımından Yetki Yönünden İncelenmesi

56. Dava dilekçesinde konu bakımından yetki yönünden kuralın Anayasa'nın 123. maddesine aykırı olduğu ileri sürülmüş ise de CBK'ya ilişkin konu bakımından yetki kuralları Anayasa'nın 104. maddesinin on yedinci fıkrasında düzenlendiğinden bu husustaki inceleme 6216 sayılı Kanun'un 43. maddesi de gözetilerek anılan fıkra kapsamında yapılacaktır.

57. CBK'nın 22. maddesinin (1) numaralı fıkrasında, Başkanlığın yurt dışı ve taşra teşkilatı kurmaya yetkili olduğu hükme bağlanmış olup anılan fıkra da yer alan "...yurtdışı ve..." ibaresi dava konusu kuralı oluşturmaktadır.

58. Kuralın Cumhurbaşkanlığına bağlı olarak CBK ile kurulan ve ayrı bir kamu tüzel kişiliği bulunmayan Başkanlığın teşkilatlanmasıyla ilgili olduğu, yasama ve yargı yetkileriyle ilgili herhangi bir husus içermediği, bu itibarla yürütme yetkisine ilişkin olduğu anlaşılmaktadır.

59. Kural, Anayasa'nın CBK ile düzenlenmesi yasaklanan İkinci Kısım Birinci ve İkinci Bölümlerinde yer alan temel haklar, kişi hakları ve ödevleriyle Dördüncü Bölüm'ünde yer alan siyasi haklar ve ödevler ile ilgili herhangi bir düzenleme de içermemektedir.

60. Daha öncede ifade edildiği üzere Anayasa'nın CBK'lar tarafından düzenleneceğini özel olarak öngördüğü bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulmasının düzenlenmesi kapsamında, bu konularla sınırlı olmak üzere Anayasa'nın 123. maddesinin birinci fıkrasında belirtilen hususlarda düzenleme yapılabilir (bkz. §§ 26-31).

61. Kamu kurumlarının teşkilatı, bu kurumların üstlendikleri görev ve yetkileri ifa edebilmeleri için oluşturulan ve söz konusu hizmetin yürütülmesinde doğrudan ya da dolaylı olarak rol alan, aynı kurum bünyesindeki farklı düzey ve nitelikteki birimlerin bütünü ifade etmektedir. Bu itibarla bir kurumun bu mahiyetteki merkez ve taşra teşkilatının yanı sıra yurt dışı teşkilatı da teşkilat yapısı kavramına dâhildir (AYM, E.2019/105, K.2020/30, 12/6/2020, § 21; E.2018/124, K.2020/56, 15/10/2020, § 21). Buna göre Cumhurbaşkanlığına bağlı olarak CBK ile kurulmuş bulunan Başkanlığa teşkilat yapısının bir parçası olan yurt dışı teşkilatını kurmak konusunda yetki veren kural Anayasa'nın 106. maddesinin on birinci fıkrası kapsamında CBK ile düzenlendiğinden kuralın Anayasa'nın 123. maddesinin birinci fıkrası bağlamında 104. maddesinin on yedinci fıkrasının üçüncü cümlesini ihlal eden bir yönü bulunmamaktadır.

62. Öte yandan kamu kurum ve kuruluşlarının yurt dışı teşkilatının kurulmasına, görevlerine, yetkilerine, idaresine ve merkezle olan ilişkilerine ilişkin esasları düzenleyen 13/12/1983 tarihli ve 189 sayılı Kamu Kurum ve Kuruluşlarının Yurtdışı Teşkilatı Hakkında Kanun Hükmünde Kararname, 2/7/2018 tarihli ve 703 sayılı Anayasada Yapılan Değişikliklere Uyum Sağlanması Amacıyla Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun Hükmünde Kararname'nin 58. maddesiyle yürürlükten kaldırılmıştır. Buna göre Başkanlığın yurt dışı teşkilatı kurabilmesine ilişkin olarak yürürlükte bir kanun hükmü bulunmadığı anlaşılmakta olup bu yönüyle kural kanunda açıkça düzenlenen konulara ilişkin değildir.

63. Açıklanan nedenlerle kural Anayasa'nın 104. maddesinin on yedinci fıkrasına aykırı değildir. İptal talebinin reddi gerekir.

M. Emin KUZ bu görüşe katılmamıştır.

b. Kuralın İçerik Yönünden İncelenmesi

64. Anayasa'nın 106. maddesinin on birinci fıkrasında bakanlıkların kurulmasının, kaldırılmasının, görev ve yetkilerinin, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulmasının CBK ile düzenlenmesi öngörülmüştür. Anılan hüküm uyarınca Cumhurbaşkanı CBK'yla idarenin teşkilatlanması konusunda Anayasa'nın temel ilkelerine ve bu alanla ilgili öngördüğü kurallarına bağlı kalmak koşuluyla bakanlıkların ve bakanlıklara dair yetki kapsamında kaldığı değerlendirilen Cumhurbaşkanlığı merkez teşkilatı ile Cumhurbaşkanlığına bağlı kurum ve kuruluşların teşkilat yapısının ne şekilde olacağını belirleme hususunda takdir yetkisine sahiptir.

65. Anayasa'nın 106. maddesinin on birinci fıkrasında bakanlıkların ve bakanlıklara dair yetki kapsamında kaldığı değerlendirilen Cumhurbaşkanlığı merkez teşkilatı ile Cumhurbaşkanlığına bağlı kurum ve kuruluşların teşkilatı kapsamında yurt dışı teşkilatı kurulması yetkisi CBK'ya tanınmış olup CBK'ya tanınan bu asli yetkinin başka bir idari işleme bırakılması mümkün değildir.

66. Bununla birlikte yürütme organının CBK çıkarmaya yetkili olduğu konuya ilişkin her türlü ayrıntıyı CBK ile düzenlemesi ve bu düzenlemelerin gereğini bizzat yerine getirmesi gerekli olmayıp CBK ile konuya ilişkin temel kuralları belirledikten ve genel çerçeveyi çizdikten sonra bu çerçevenin içinde kalan hususları, düzenleyici nitelikteki diğer işlemlerle belirlemesi ve bu düzenlemeler kapsamında yerine getirilmesi gerekli tasarrufları da ilgili idareye bırakması mümkündür (AYM, E.2019/105, K.2020/30, 12/6/2020, § 36; E.2018/124, K.2020/56, 15/10/2020, § 25).

67. (14) numaralı CBK'da Cumhurbaşkanlığına bağlı ve ayrı bir tüzel kişiliği bulunmayan Başkanlığın kurulması, teşkilat, görev ve yetkilerine ilişkin usul ve esaslar düzenlenmiş; bu kapsamda dava konusu kuralla Başkanlık yurt dışı teşkilatı kurmak konusunda yetkilendirilmiştir. (1) numaralı CBK'nın kamu kurum ve kuruluşlarının teşkilatlanmasına ilişkin diğer hükümleri ile birlikte değerlendirildiğinde kuralın CBK ile oluşturulan söz konusu teşkilatın fiilen faaliyete geçirilmesi için gerekli idari tasarrufların Başkanlık tarafından yerine getirilmesini öngördüğü anlaşılmaktadır. Bunun dışında kural; söz konusu yurt dışı teşkilatının doğrudan düzenlenmesiyle ilgili bir yetkiyi bu kapsamda örneğin yurt dışı teşkilatının niteliği, kurulacağı yer, görevleri, yer itibarıyla görev alanı gibi konularda düzenleme yapma yetkisini Başkanlığa tanımamıştır. Kuralın anılan yetkiyi Başkanlığa bırakmadığı tüm kamu kurum ve kuruluşlarının ve Cumhurbaşkanlığının teşkilatını düzenleyen (1) numaralı CBK'nın Ortak Hükümler başlıklı bölümünde düzenlenen 510/B maddesinin başlığından ve içeriğinden açıkça anlaşılmaktadır. "Yurtdışı teşkilatı kurulma usulü" başlıklı söz konusu maddede "Yurtdışı teşkilatı kurulurken niteliği, kurulacağı yer, görevleri, yer itibarıyla görev alanı, bağlı veya ilgili olacağı misyon, konsolosluk şefliği ve geçici olanların süresi, Cumhurbaşkanı kararında belirtilir." hükmüne yer verilmiştir.

68. Buna göre (1) numaralı CBK, yurt dışı teşkilatının kurulmasına ilişkin olarak yurt dışı teşkilatının niteliği, kurulacağı yer, görevleri, yer itibarıyla görev alanı gibi temel kuralları dava konusu kuralla Başkanlığa bırakmamış; bunların düzenlenme yetkisini 510/B maddesiyle Cumhurbaşkanı kararına tanımıştır. CBK ile söz konusu hususlarda düzenleme yapma yetkisinin anayasal olarak Cumhurbaşkanı kararına bırakılıp bırakılmayacağı bu davanın konusunu oluşturmamakla birlikte bu hüküm anılan konularda doğrudan düzenleme yapma yetkisinin Başkanlığa bırakılmadığını göstermektedir. Dolayısıyla kuralla tanınan yetkinin konuya ilişkin temel kurallar ve genel çerçeve belirlenmeden yurt dışı teşkilatının kurulması veya düzenlenmesini de içerdiğinin söylenemeyeceği anlaşılmaktadır. Bu yönüyle Anayasa'nın 106. maddesinin on birinci fıkrası kapsamında CBK ile oluşturulan Başkanlığın yurt dışı teşkilatına ilişkin olarak doğrudan düzenleme yapma yetkisini Başkanlığa bırakmayan dava konusu kuralın da anılan fıkrayı ihlal eden bir yönü bulunmamaktadır.

69. Açıklanan nedenlerle kural Anayasa'nın 106. maddesine aykırı değildir. İptal talebinin reddi gerekir.

M. Emin KUZ bu sonuca farklı gerekçe ile katılmıştır.

D. CBK'nın 26. Maddesinin (2) Numaralı Fıkrasının (c) Bendiyle (1) Numaralı CBK'nın 485. Maddesine Eklenen (i) Bendinin İncelenmesi

1. Anlam ve Kapsam

70. (1) numaralı CBK'nın 474. maddesinde Ulaştırma ve Altyapı Bakanlığının (Bakanlık) görev ve yetkileri düzenlenmiştir. Anılan madde kapsamında genel olarak Bakanlığın faaliyet alanı ulaştırma, denizcilik, haberleşme ve posta iş ve hizmetleri ile su yolu projelerine ilişkin olarak planlama, geliştirme, kurma, kurdurma, işletme, işletirme, koordinasyon sağlama ve izlemeye ilişkin bir kısım iş ve işlemi yapmak olarak belirlenmiş; anılan maddenin (a) bendinde ulaştırma, denizcilik, haberleşme ve posta iş ve hizmetleri ile Karadeniz ile Marmara Denizi'ni birleştiren ve gemilerin seyrüseferine imkân veren Kanal İstanbul ve benzeri su yolu projelerinin geliştirilmesi, kurulması, kurdurulması, işletilmesi ve işlettirilmesi hususlarında ilgili kurum ve kuruluşlarla koordinasyon içerisinde, millî politika, strateji ve hedeflerin belirlenmesi amacıyla çalışmalar yapmanın ve belirlenen hedefleri uygulamanın Bakanlığın görev ve yetkileri arasında bulunduğu ifade edilmiştir.

71. Dava konusu kural (1) numaralı CBK'nın Bakanlığın hizmet birimlerinden olan Altyapı Yatırımları Genel Müdürlüğü'nün görev ve yetkilerini düzenleyen 485. maddesinde yer almaktadır. Anılan maddenin (1) bendinde denizleri, gölleri, nehirleri birbirine bağlayarak su yolu işlevi görececek kanal ve benzeri altyapı projelerini yapım ve işletim modelleri de geliştirerek planlamanın, bu

altyapılarla ilgili proje ve şartnameleri hazırlamanın, hazırlatmanın, incelemenin, incelettirmenin ve onaylamanın, yapmanın veya yaptırmanın, yapımı tamamlananları ilgili kuruluşlara devretmenin ve işletme esaslarını belirlemenin Altyapı Yatırımları Genel Müdürlüğünün görev ve yetkisinde olduğu belirtilmiştir.

72. Dava konusu kuralla 474. maddenin (a) bendi ile 485. maddenin (1) bendinde yazılı projelerin ileri teknoloji veya yüksek maddi kaynak gerektirmesi hâlinde 8/6/1994 tarihli ve 3996 sayılı Bazı Yatırım ve Hizmetlerin Yap-İşlet-Devret Modeli Çerçevesinde Yaptırılması Hakkında Kanun kapsamı da dâhil yap-işlet-devret modeli çerçevesinde sermaye şirketlerinin veya yabancı şirketlerin görevlendirilmesi suretiyle yapılmasını sağlamanın Altyapı Yatırımları Genel Müdürlüğünün görev ve yetkileri arasında olduğu öngörülmüştür.

73. 474. maddenin (a) bendi ile 485. maddenin (1) bendinde yazılı projeler ulaştırma, denizcilik, haberleşme ve posta iş ve hizmetleri ile Karadeniz ile Marmara Denizi'ni birleştiren ve gemilerin seyrüseferine imkân veren Kanal İstanbul ve benzeri su yolu projeleri ile denizleri, gölleri, nehirleri birbirine bağlayarak su yolu işlevi görecektir kanal ve benzeri altyapı projeleridir.

74. Öte yandan dava konusu kuralın atıfta bulunduğu 3996 sayılı Kanun, kamu iktisadi teşebbüsleri de dâhil olmak üzere kamu kurum ve kuruluşlarınca ifa edilen, ileri teknoloji veya yüksek maddi kaynak gerektiren bazı yatırım ve hizmetlerin yap-işlet-devret modeli çerçevesinde yaptırılmasını sağlamak amacıyla kabul edilmiştir. Anılan Kanun'un 3. maddesine göre yap-işlet-devret modeli, ileri teknoloji ve yüksek maddi kaynak ihtiyacı duyulan projelerin gerçekleştirilmesinde kullanılmak üzere geliştirilen özel bir finansman modeli olup yatırım bedelinin (elde edilecek kâr dâhil) sermaye şirketlerine veya yabancı şirkete, şirketin işletme süresi içerisinde ürettiği mal veya hizmetin idare veya hizmetten yararlananlarca satın alınması suretiyle ödenmesini ifade etmektedir.

75. Kanun'un kapsamı ise 2. maddede belirtilmiştir. Anılan maddeye göre köprü, tünel, baraj, sulama, içme ve kullanma suyu, arıtma tesisi, kanalizasyon, haberleşme, kongre merkezi, kültür ve turizm yatırımları, ticari bina ve tesisler, spor tesisleri, yurtlar, tema parklar, balıkçı barınakları, silo ve depo tesisleri, jeotermal ve atık ısıya dayalı tesisler ve ısıtma sistemleri elektrik üretim, iletim, dağıtım ve ticareti maden ve işletmeleri, fabrika ve benzeri tesisler, çevre kirliliğini önleyici yatırımlar, otoyol, trafiği yoğun kara yolu, demir yolu ve raylı sistemler, gar kompleksi ve istasyonları, teleferik ve telesiyaj tesisleri, lojistik merkezi, yeraltı ve yer üstü otoparkı ve sivil kullanıma yönelik deniz ve hava alanları ve limanları, yük ve/veya yolcu ve yat limanları ile kompleksleri, Kanal İstanbul ve benzeri su yolu projeleri, sınır kapıları ve gümrük tesisleri, millî park (özel kanunu olan hariç), tabiat parkı, tabiatı koruma alanı ve yaban hayatı koruma ve geliştirme sahalarında planlarda öngörülen yapı ve

tesisleri, toptancı halleri ve benzeri yatırım ve hizmetlerin yaptırılması, işletilmesi ve devredilmesi konularında sermaye şirketlerinin veya yabancı şirketlerin yap-işlet-devret modeli çerçevesinde görevlendirilmesine ilişkin usul ve esaslar Kanun'un kapsamında yer almaktadır.

76. Bu bağlamda dava konusu kural; ileri teknoloji ve yüksek maddi kaynak gerektiren ulaştırma, denizcilik, haberleşme ve posta iş ve hizmetleri ile Karadeniz ile Marmara Denizi'ni birleştiren ve gemilerin seyrüseferine imkân veren Kanal İstanbul ve benzeri su yolu projeleri ve denizleri, gölleri, nehirleri birbirine bağlayarak su yolu işlevi görecektir kanal ve benzeri altyapı projeleri ile 3996 sayılı Kanun kapsamında kalan yatırım ve hizmetleri kapsamaktadır. Kuralla Bakanlığın merkez teşkilatı bünyesindeki hizmet birimlerinden olan Altyapı Yatırımları Genel Müdürlüğü, belirtilen projeler ile yatırım ve hizmetlerin yap-işlet-devret modeli çerçevesinde yapılmasını sağlamak bakımından sermaye şirketlerinin veya yabancı şirketlerin görevlendirilmesi hususunda görevli ve yetkili kılınmaktadır.

2. İptal Talebinin Gerekçesi

77. Dava dilekçesinde özetle; daha önce 3996 sayılı Kanun kapsamında bulunmayan denizleri, gölleri, nehirleri birbirine bağlayarak su yolu işlevi görecektir kanal ve benzeri altyapı projelerinin 3996 sayılı Kanun'da değişiklik yapılmaksızın CBK kuralı ile yap-işlet-devret modeli kapsamına alındığı, Bakanlığın bu tür projelerin yapımından sorumlu bakanlık, Altyapı Yatırımları Genel Müdürlüğünün ise yetkili genel müdürlük olarak belirlendiği, 3996 sayılı Kanun'da değişiklik niteliği taşıyan bu kuralların kanunla düzenlenmesi gerektiği, yasama organı tarafından önceden düzenleme yapılmış olan bir alanda CBK ile düzenleme yapılamayacağı, temel ilkeler ve çerçeve belirlenmeden idarelere geniş ve sınırsız yetki veren kuralın hukuki belirlilikten yoksun olduğu, yasama yetkisinin devri niteliği taşıdığı belirtilerek kuralın Anayasa'nın 2., 7. ve 104. maddelerine aykırı olduğu ileri sürülmüştür.

3. Anayasa'ya Aykırılık Sorunu

a. Kuralın Konu Bakımından Yetki Yönünden İncelenmesi

78. Dava dilekçesinde konu bakımından yetki yönünden kuralın Anayasa'nın 7. maddesine de aykırı olduğu ileri sürülmüş ise de CBK'ya ilişkin konu bakımından yetki kuralları Anayasa'nın 104. maddesinin on yedinci fıkrasında düzenlendiğinden bu husustaki inceleme anılan fıkra kapsamında yapılacaktır.

79. Yürütme organının bir unsuru olan Bakanlığın hizmet birimlerinden Altyapı Yatırımları Genel Müdürlüğünün kamu hizmetlerinin yürütülmesiyle bağlantılı olarak görev ve yetkilerine ilişkin düzenleme içeren kuralın yürütme yetkisine ilişkin olduğu anlaşılmaktadır.

80. Altyapı Yatırımları Genel Müdürlüğünün belirtilen projeler ile yatırım ve hizmetlerin yap-işlet-devret modeli çerçevesinde sermaye şirketlerinin veya yabancı şirketlerin görevlendirilmesi suretiyle yapılmasını sağlamak bakımından görevli ve yetkili kılınmasını öngören kural kapsamı itibarıyla Anayasa'nın İkinci Kısım Birinci ve İkinci Bölümlerinde yer alan temel haklar, kişi hakları ve ödevleri ile Dördüncü Bölüm'ünde yer alan siyasi haklar ve ödevler ile ilgili bulunmamaktadır.

81. Anayasa'nın 123. maddesinin birinci fıkrasında idarenin kuruluş ve görevleriyle bir bütün olduğu ve kanunla düzenleneceği belirtilmiş; 106. maddesinin on birinci fıkrasında ise bakanlıkların kurulmasının, kaldırılmasının, görev ve yetkilerinin, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulmasının CBK ile düzenleneceği hükme bağlanmıştır. Dolayısıyla anılan fıkra kapsamındaki konular Anayasa'nın CBK ile düzenlenmesini ayrıca ve özel olarak öngördüğü konulardır. Anayasa'da CBK'larla düzenleneceği özel olarak öngörülen anılan konularda CBK'yla düzenleme yapılması Anayasa'nın 123. maddesinin birinci fıkrası bağlamında 104. maddesinin on yedinci fıkrasının üçüncü cümlesine aykırılık teşkil etmemektedir. Buna göre Bakanlığın hizmet birimlerinden Altyapı Yatırımları Genel Müdürlüğünün görev ve yetkilerinden birini düzenleyen kuralın anılan hükmü ihlal eden bir yönü bulunmamaktadır.

82. Öte yandan Anayasa'nın 47. maddesinin dördüncü fıkrasında "Devlet, kamu iktisadî teşebbüsleri ve diğer kamu tüzelkişileri tarafından yürütülen yatırım ve hizmetlerden hangilerinin özel hukuk sözleşmeleri ile gerçek veya tüzelkişilere yaptırılacağı veya devredilebileceği kanunla belirlenir" denilmiştir. Bu kapsamda 3996 sayılı Kanun, kamu kurum ve kuruluşlarınca (kamu iktisadi teşebbüsleri dâhil) ifa edilen, ileri teknoloji veya yüksek maddi kaynak gerektiren bazı yatırım ve hizmetlerin yap-işlet-devret modeli çerçevesinde yaptırılmasını sağlamak amacıyla kabul edilmiştir.

83. Dava konusu kuralla hangi yatırım ve hizmetlerin yap-işlet-devret modeliyle yaptırılacağı ve bunun kapsamıyla ilgili bir düzenleme öngörülmemekte, kanunla içeriği belirlenen hususa ilişkin kamu hizmetinin Anayasa'nın 106. maddesinin on birinci fıkrası uyarınca hangi bakanlığın hangi hizmet birimi tarafından yerine getirileceği konusunda bakanlıkların teşkilat, görev ve yetkisine ilişkin bir düzenleme getirilmektedir.

84. Bu bağlamda 3996 sayılı Kanun'un 2. maddesinin birinci fıkrasında Kanun'un kapsamında kalan yatırım ve hizmetler sayılmış olup dava konusu kuralda ifade edilen projelerden haberleşme ile Kanal İstanbul ve benzeri su yolu projeleri açıkça 3996 sayılı Kanun'un 2. maddesinde belirtilmiştir. Ayrıca

anılan Kanun kapsamında kalan yatırım ve hizmetler sınırlı olarak sayılmayıp maddede yer alan "...ve benzeri yatırım ve hizmetler..." ibaresiyle maddede sayılanlarla benzer mahiyetteki yatırım ve hizmetlerin de Kanun kapsamında bulunduğu açıklanmıştır. Bu bakımdan kuralın içerik itibarıyla yeni tür yatırımlar, hizmetler veya projeler eklemek ya da yeni koşullar belirlemek suretiyle 3996 sayılı Kanun'un kapsamını genişlettiği söylenemeyeceği gibi Kanun'u daraltan veya herhangi bir surette değiştiren bir yönü de bulunmamaktadır.

85. Bu itibarla Anayasa'nın 47. maddesi bağlamında devlet, kamu iktisadî teşebbüsleri ve diğer kamu tüzelkişileri tarafından yürütülen yatırım ve hizmetlerden hangilerinin özel hukuk sözleşmeleri ile gerçek veya tüzelkişilere yaptırılabilmesi veya devredilebileceği konusunda bir düzenleme öngörmeyen ve anılan konulardaki kamu hizmetini bir teşkilat olarak yerine getirme görev ve yetkisinin Anayasa'nın 106. maddesinin on birinci fıkrası kapsamında hangi Bakanlık birimi tarafından yerine getirileceğini düzenleyen dava konusu kuralın Anayasa'nın 47. maddesinin dördüncü fıkrası bağlamında 104. maddesinin on yedinci fıkrasının üçüncü cümlesini ihlal ettiği söylenemez.

86. Ulaştırma, Denizcilik ve Haberleşme Bakanlığının kuruluş, görev, yetki ve sorumluluklarına ilişkin esasları düzenleyen 26/9/2011 tarihli ve 655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin başlığı 703 sayılı KHK'nın 31. maddesi ile "Ulaştırma ve Altyapı Alanına İlişkin Bazı Düzenlemeler Hakkında Kanun Hükmünde Kararname" olarak değiştirilmiş ve Altyapı Yatırımları Genel Müdürlüğü de dâhil olmak üzere Bakanlığın hizmet birimlerinin görev ve yetkilerini düzenleyen hükümler yürürlükten kaldırılmıştır. Buna göre Bakanlığın hizmet birimlerinden olan Altyapı Yatırımları Genel Müdürlüğünün görev ve yetkilerine ilişkin olarak yürürlükte bir kanun hükmünün bulunmadığı anlaşılmakta olup kural kanunda açıkça düzenlenen konulara ilişkin değildir.

87. Açıklanan nedenlerle kural Anayasa'nın 104. maddesinin on yedinci fıkrasına aykırı değildir. İptal talebinin reddi gerekir.

Zühtü ARSLAN, Hasan Tahsin GÖKCAN, M. Emin KUZ ve Yusuf Şevki HAKYEMEZ bu görüşe katılmamışlardır.

b. Kuralın İçerik Yönünden İncelenmesi

88. Hukuk devletinde kanunlar gibi CBK'lar da kamu yararı amacıyla çıkarılır. Anayasa Mahkemesinin kararlarına göre kamu yararı genel bir ifadeyle bireysel, özel çıkarılardan ayrı ve bunlara üstün olan toplumsal yararı ifade etmektedir. CBK kuralının amaç unsuru bakımından

Anayasa'ya uygun sayılabilmesi için çıkarılmasında kamu yararı dışında bir amacın gözetilmemiş olması gerekir.

89. Kural, Bakanlığın merkez teşkilatı bünyesindeki hizmet birimlerinden olan Altyapı Yatırımları Genel Müdürlüğünün (1) numaralı CBK'nın 474. maddesinin birinci fıkrasının (a) bendi ile 485. maddesinin (1) numaralı fıkrasının (ı) bendinde yazılı projelerin ileri teknoloji veya yüksek maddi kaynak gerektirmesi halinde 3996 sayılı Kanun kapsamı da dahil yap-işlet-devret modeli çerçevesinde sermaye şirketlerinin veya yabancı şirketlerin görevlendirilmesi suretiyle yapılmasını sağlama görevini düzenlemektedir.

90. Kuralla Bakanlığın merkez teşkilatı bünyesindeki hizmet birimlerinden olan Altyapı Yatırımları Genel Müdürlüğünün görevlerinden birisi tanımlanmakta, böylece anılan Bakanlığın görev ve yetkisi kapsamında kalan bir hususun Bakanlığın hangi hizmet birimince yerine getirileceği açıklığa kavuşturulmaktadır. Bu itibarla kuralın kamu yararı dışında bir amaç güttüğü söylenemeyeceğinden hukuk devleti ilkesine aykırı bir yönü bulunmamaktadır.

91. Açıklanan nedenlerle kural Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

IV. YÜRÜRLÜĞÜN DURDURULMASI TALEBİ

92. Dava dilekçesinde özetle, dava konusu kuralların uygulanmaları hâlinde telafisi güç veya imkânsız zararların doğabileceği belirtilerek yürürlüklerinin durdurulmasına karar verilmesi talep edilmiştir.

23/7/2018 tarihli ve (14) numaralı İletişim Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin;

A. 21. maddesinin (3) numaralı fıkrasının üçüncü cümlesine yönelik yürürlüğün durdurulması talebinin, koşulları oluşmadığından REDDİNE,

B. 1. 17. maddesinin (2) numaralı fıkrasının birinci cümlesinde yer alan "...gerekli gördüğü bilgileri..." ibaresine,

2. 22. maddesinin (1) numaralı fıkrasında yer alan "...yurtdışı ve..." ibaresine,

3. 26. maddesinin (2) numaralı fıkrasının (c) bendiyle 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete'de yayımlanan (1) numaralı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin 485. maddesine eklenen (i) bendine,

yönelik iptal talepleri 3/3/2021 tarihli ve E.2018/134, K.2021/13 sayılı kararla reddedildiğinden bu bende ve ibarelere ilişkin yürürlüğün durdurulması taleplerinin REDDİNE,

3/3/2021 tarihinde OYBİRLİĞİYLE karar verilmiştir.

V. HÜKÜM

23/7/2018 tarihli ve (14) numaralı İletişim Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin;

A. 17. maddesinin (2) numaralı fıkrasının birinci cümlesinde yer alan "...gerekli gördüğü bilgileri..." ibaresinin;

1. Konu bakımından yetki yönünden Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ ile Yusuf Şevki HAKYEMEZ'in karşıoyları ve OYÇOKLUĞUYLA,

2. İçeriği itibarıyla Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM ile M. Emin KUZ'un karşıoyları ve OYÇOKLUĞUYLA,

B. 21. maddesinin (3) numaralı fıkrasının üçüncü cümlesinin konu bakımından yetki yönünden Anayasa'ya aykırı olduğuna ve İPTALİNE OYBİRLİĞİYLE,

C. 22. maddesinin (1) numaralı fıkrasında yer alan "...yurtdışı ve..." ibaresinin;

1. Konu bakımından yetki yönünden Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE M. Emin KUZ'un karşıoyu ve OYÇOKLUĞUYLA,

2. İçeriği itibarıyla Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

Ç. 26. maddesinin (2) numaralı fıkrasının (c) bendiyle 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete'de yayımlanan (1) numaralı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin 485. maddesine eklenen (i) bendinin;

1. Konu bakımından yetki yönünden Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE Zühtü ARSLAN, Hasan Tahsin GÖKCAN, M. Emin KUZ ile Yusuf Şevki HAKYEMEZ'in karşıoyları ve OYÇOKLUĞUYLA,

2. İçeriği itibarıyla Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

3/3/2021 tarihinde karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili - Hasan Tahsin GÖKCAN

Başkanvekili - Kadir ÖZKAYA

Üye: Engin YILDIRIM; Hicabi DURSUN; Celal Mümtaz AKINCI; Muammer TOPAL; M. Emin KUZ; Rıdvan GÜLEÇ; Recai AKYEL; Yusuf Şevki HAKYEMEZ; Yıldız SEFERİNOĞLU; Selahaddin MENTEŞ; Basri BAĞCI; İrfan FİDAN

KARŞIOY GEREKÇESİ

1. 23/7/2018 tarihli ve (14) numaralı İletişim Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin (CBK) 17. maddesinin (2) numaralı fıkrasının birinci cümlesinde yer alan "...gerekli gördüğü bilgileri..." ibaresinin ve 26. maddesinin (2) numaralı fıkrasının (c) bendiyle (1) numaralı CBK'nın 485. maddesine eklenen (i) bendinin Anayasa'ya aykırı olmadığına karar verilmiştir. Kurallardan birincisinin hem konu bakımından yetki hem de içerik yönünden, ikincisinin ise konu bakımından yetki yönünden Anayasa'ya aykırı olduğunu düşündüğümünden çoğunluk görüşüne katılma imkânı olmamıştır.

A. CBK'da Yer Alan "...gerekli gördüğü bilgileri..." İbaresini

a. Konu Bakımından Yetki Yönünden

2. İptali istenen ibarenin de bulunduğu fıkranın birinci cümlesinde İletişim Başkanlığına görevleriyle ilgili olarak gerekli gördüğü bilgileri tüm kamu kurum ve kuruluşları ile diğer gerçek ve tüzel kişilerden isteme yetkisi verilmektedir. Anılan fıkranın ikinci cümlesi ise kendilerinden bilgi istenen kişi ve kurumları bu bilgileri istenilen süre içinde öncelikle ve zamanında vermekle yükümlü kılmaktadır.

3. Anayasa'nın 104. maddesinin on yedinci fıkrasının ikinci cümlesi uyarınca temel haklar, kişi hakları ve siyasi haklar CBK ile düzenlenemez. Anayasa'nın 20. maddesinde güvence altına alınan kişisel verilerin korunmasını isteme hakkı, Anayasa'da CBK ile düzenlenemeyeceği öngörülen "yasak alan" kapsamında kalan temel haklar arasındadır. Buradaki düzenleme yasağı, sınırlandırmayı da içine alan ancak onunla sınırlı olmayan ve sınırlama mahiyetinde olmasa da anılan hak ve özgürlüklere yönelik olan her türlü düzenlemeyi içermektedir.

4. Çoğunluğa göre İletişim Başkanlığına kanuni görevlerini yerine getirebilmesi için zorunlu olan "bilgi isteme yetkisi vermek"ten ibaret olan dava konusu kural kişisel verilere ilişkin düzenleme içermemekte ve kişisel verilerle ilgili bulunmamaktadır. Bu görüş kişisel verilere ilişkin düzenlemelerin 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda bulunduğu, kuralın buradaki düzenlemelerin "uygulanmasını engelleyen, sınırlandıran, genişleten, uygulanmasına istisna getiren

veya herhangi bir surette bu hükümlere temas eden bir yönünün bulunmadığı” gerekçesine dayanmaktadır (bkz. §§ 23-25).

5. Bu görüşün ve dayandığı gerekçenin en az üç nedenle isabetli olmadığı düşünülmektedir. Birincisi, kişisel verilerin korunmasına ilişkin kuralların esas itibarıyla 6698 sayılı Kanun’da yer alması, diğer kanunlarda da bu konuda düzenleme yapıl(a)mayacağı anlamına gelmez. Nitekim çoğunluğun da kabul ettiği üzere anılan Kanun dışındaki kanunlarda da kişisel verilere ilişkin düzenlemeler bulunmaktadır. Bu durumda dava konusu kuralda olduğu gibi bilgi talep etme yetkisinin, 6698 sayılı Kanun dışında özel olarak düzenlenmiş olması, söz konusu düzenlemenin kişisel verilerle ilgili olmadığı anlamına gelmez. En fazla aynı konuyu -farklı boyutlarıyla bile olsa- düzenleyen iki farklı yasal düzenlemenin varlığından bahsedilebilir.

6. İkinci olarak bir kamu kuruluşuna diğer kamu kurum ve kuruluşlarından, gerçek ve tüzel kişilerden bilgi isteme yetkisi veren düzenlemenin, bu konudaki temel kanunun sınırlarını aşmadığı için, kişisel verilerin korunması hakkıyla ilgisinin olmadığını söylemek mantiken de mümkün değildir. Zira bu hakkın korunması, en başta kişilere ait olan kişisel verilerin kamu kuruluşlarınca istenebilmesini sağlayan yetkinin açık, sınırlı ve belirli şekilde düzenlenmesini gerektirmektedir. Belirtmek gerekir ki, kişisel verilerin işlenmesinin ilk basamağı bu bilgilerin istenmesi veya bazı durumlarda doğrudan elde edilmesidir. Nitekim 6698 sayılı Kanun’un 3. maddesinin (1) numaralı fıkrasının (e) bendinde “kişisel verilerin işlenmesi” kavramı kişisel verilerin “elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem” şeklinde tanımlanmıştır. Bu nedenle bir kamu otoritesine neredeyse herkesten bilgi isteme, elde etme ve bunları işleme yetkisi veren bir kural, başka bir kanuna aykırı olmasa da kişisel verilerin korunmasını isteme hakkına yönelik bir düzenlemedir.

7. Üçüncüsü ve en önemlisi dava konusu kuralın 6698 sayılı Kanun’a aykırı, onu aşan bir yönünün bulunmaması farklı, kuralın kişisel verilere ilişkin olması farklı şeylerdir. Esasen çoğunluk kuralın 6698 sayılı Kanun’un sınırlarını aşmadığını belirtirken, onun kişisel verilerle ilgili olduğunu da zımnen kabul etmiş olmaktadır. Aksi olsaydı böyle bir açıklamaya da ihtiyaç duyulmazdı. Dahası çoğunluğun bu görüşü kuralın kişisel verilere ilişkin bir düzenleme mahiyetinde olmadığı görüşünün değil, daha ziyade kişisel verilerin korunması hakkını ihlal etmediği, dolayısıyla içerik olarak Anayasa’nın 20. maddesine aykırı olmadığı şeklindeki görüşün gerekçesi olabilir.

8. Öte yandan Anayasa Mahkemesi şu ana kadar, kurumlardan gerçek ve tüzel kişilerden bilgi istenmesine yönelik düzenlemeleri temel hak ve özgürlükler kapsamında incelemiştir. Sözelimi 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'nun 6. maddesinde yer alan ve Bilgi Teknolojileri ve İletişim Kurumu'nun görev ve yetkileri arasında sayılan "işletmeciler, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden ihtiyaç duyacağı her türlü bilgi ve belgeyi almak ve gerekli kayıtları tutmak" şeklindeki hüküm Anayasa'nın 12., 13. ve haberleşme hürriyetini düzenleyen 22. maddesi kapsamında denetlenmiştir (AYM, E.2008/115, K.2011/86, 2/6/2011). Benzer şekilde internet trafik bilgisinin Telekomünikasyon İletişim Başkanlığı tarafından ilgili işletmecilerden alınmasını ve hâkim tarafından karar verilmesi durumunda bu bilginin ilgili mercilere verilmesini düzenleyen kanun hükmü Anayasa'nın 2., 13. ve 20. maddeleri yönünden incelenmiştir (AYM, E.2014/149, K.2014/151, 2/10/2014).

9. Daha yakın tarihli bir kararda da eldeki davada iptali istenen kurala çok benzeyen bir kanun hükmünün Anayasa'ya aykırılığı denetlenmiştir. Anayasa Mahkemesi, 5809 sayılı Kanun'un 60. maddesine eklenen (11) numaralı fıkrada yer alan, Bilgi Teknolojileri ve İletişim Kurumu "görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilir ve değerlendirmesini yapabilir" ve bu çerçevede "istenen her türlü bilgi ve belge talebi; ilgili bakanlık, kurum ve kuruluşlar tarafından gecikmeksizin yerine getirilir." şeklindeki kuralların anayasallık denetimini Anayasa'nın 2., 13. ve 20. maddeleri kapsamında yapmıştır (AYM, E.2017/16, K.2019/64, 24/7/2019, § 61).

10. Anayasa Mahkemesinin konuya ilişkin bu ve benzeri kararlarında denetlenen kuralların bazıları Anayasa'ya uygun bazıları da aykırı bulunmuştur. Bu noktada önemli olan husus Mahkemenin içeriğe ilişkin değerlendirmesi değil, iptali istenen kuralları temel hak ve özgürlükleri düzenleyen anayasal hükümler yönünden incelemesidir. Aslında başka türlü de olamazdı, zira kurallar - Anayasa'ya uygun ya da aykırı olarak- kişisel verileri de içine alan düzenlemeler içermektedir. Tıpkı eldeki davada iptali istenen CBK kuralı gibi. Nitekim Anayasa Mahkemesinin konuya ilişkin bir iptal kararında da belirttiği üzere "devletin yetkili temsilcileri tarafından ilgililer hakkında rızaları olmaksızın bilgi toplanmasının her zaman söz konusu kişinin özel hayatını ilgilendireceği kuşkusuzdur" (AYM, E.2014/87, K.2015/112, 8/12/2015, § 170).

11. Diğer yandan 6698 sayılı Kanun'a göre "kişisel veri", "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi" ifade etmektedir (m. 3/1/d). Bu anlamda sadece kişinin adı ve soyadı, doğum yeri ve tarihi gibi kimlik bilgileri değil, telefon numarası, motorlu taşıt plakası, pasaport numarası, özgeçmiş bilgileri, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, etkileşimde bulunulan kişiler, grup üyelikleri ve aile bağları gibi kişiyi belirlenebilir kılan tüm bilgiler

de kişisel veri kapsamında kalmaktadır (AYM, E.2017/180, K.2018/109, 6/12/2018, § 54; AYM, E.2018/73, K.2019/65, 24/7/2019, § 168).

12. İletişim Başkanlığının görevleriyle ilgili olarak gerekli gördüğü bilgileri isteyebileceğini öngören dava konusu kuralda bu bilgiler arasında kişisel verilerin olmayacağına dair bir sınırlama söz konusu değildir. Buradaki tek sınırlama, istenecek bilgilerin Başkanlığın “görev alanına giren konular”a ilişkin olmasıdır. Dolayısıyla bu bilgiler arasında kişisel verilerin olup olmadığını belirleyebilmek için söz konusu görevlerin mahiyetine ve kapsamına da bakılmalıdır.

13. Başkanlığın görevleri, (14) numaralı CBK'nın 3. maddesinde ayrıntılı olarak sıralanmıştır. Kamuoyunun zamanında ve doğru bilgilerle aydınlatılması için bilgi akışı sağlamaktan basın-yayın mensuplarına basın kartı hazırlamaya, vatandaşların kamu kurum ve kuruluşlarının faaliyetlerine ilişkin talep, görüş ve önerilerini kolayca iletebilmelerine yönelik tedbirleri almaktan Türkiye Medya Veri Tabanını oluşturma ve güncellemeye kadar Başkanlığa verilen görevlerin çok büyük bir kısmı şu ya da bu şekilde kişisel verilerin işlenmesini gerektirebilecek niteliktedir. Bu sebeple Kanun'da sayılan görevlerin yerine getirilmesi sırasında Başkanlığın kurum, kuruluş ve kişilerden talep edeceği bilgiler arasında kişisel verilerin bulunmaması mümkün değildir.

14. Kaldı ki, iptali istenen ibarenin de içinde bulunduğu madde hükmü bir bütün olarak değerlendirildiğinde Başkanlığa ilgili kişi ve kuruluşlardan en “hassas” bilgileri bile isteme yetkisinin verildiği anlaşılmaktadır. Nitekim kuralı izleyen (3) numaralı fıkrada “Bu şekilde elde edilen bilgilerden ticari sır niteliğinde olanların gizliliğine uyulur.” denilmektedir. Bu durumda “ticari sır” mahiyetinde olan bilgilerin de istenebileceği açıktır. “Ticari sır” niteliğindeki bilgilerin “kişisel veri” kapsamında olup olmadığı ve mülkiyet hakkıyla ilişkisi gibi meseleler bir yana bırakılsa bile, mahremiyeti tartışmasız olan bu tür bilgilerin dahi istenebildiği bir yerde, talep edilen bilgiler arasında kaçınılmaz olarak kişisel verilerin de bulunacağını kabul etmek gerekir.

15. Diğer yandan Anayasa'nın 104. maddesinin on yedinci fıkrasının üçüncü cümlesi, Anayasa'da münhasıran kanunla düzenlenmesi öngörülen konularda CBK çıkarılamayacağını öngörmektedir. Esasen ikinci cümleye aykırı olarak bu cümlenin kapsamına giren herhangi bir temel hakla ilgili düzenleme yapan bir CBK, Anayasa'da kanunla düzenlenmesi öngörülen bir konuya dair düzenleme yapmış olacaktır. Anayasa'da sosyal ve ekonomik hakların bir kısmı dışında hemen tüm haklara ilişkin düzenlemelerin kanunla yapılması gerektiği izahtan varestedir. Ayrıca Anayasa'da özel olarak kanunla düzenlenmesi öngörülmemiş hakları da kapsayacak şekilde Anayasa'nın 13. maddesi uyarınca bütün temel hak ve özgürlükler “ancak kanunla sınırlanabilir”.

16. Dava konusu CBK kuralının 6698 sayılı Kanun'a uygun olduğu, onu aşan bir düzenleme getirmediği yönündeki değerlendirme, anayasa koyucunun CBK'lara ilişkin tasarımıyla da bağdaşmamaktadır. Anayasa'da CBK, kanunun uygulanmasını sağlamak üzere çıkarılan yönetmelik gibi türevsel nitelikte bir idari tasarruf olarak düzenlenmemiştir. Tersine CBK, tıpkı kanun gibi, kaynağını doğrudan Anayasa'dan alan asli düzenleme yetkisinin ürünüdür. Bu sebeple anayasallığı denetlenen bir CBK'nın düzenleme alanı belirlenirken onun aynı konuda düzenleme yapan bir kanuna uygunluğuna bakılması CBK kurumunun mantığına da aykırı olacaktır.

17. Sonuç olarak iptali istenen kural, ister kişisel verilerin korunmasını isteme hakkı ister daha genel anlamda özel hayatın gizliliği kapsamında kalsın, her durumda Anayasa'da kanunla düzenlenmesi gereken bir konudur. Bu sebeple kural, içeriğinin Anayasa'ya aykırılığı meselesinden bağımsız olarak, Anayasa'nın 104. maddesinin on yedinci fıkrasının ikinci ve üçüncü cümlelerine aykırıdır.

b. İçerik Yönünden

18. Öncelikle belirtmek gerekir ki, kuralın içerik denetiminin "düzenleme bir kanun hükmü olsaydı" varsayımıyla yapılması zorunludur. Zira temel hak ve özgürlükleri düzenleyen bir CBK'nın, düzenlediği temel hakka ilişkin Anayasa maddesi ve sınırlama rejimini belirleyen Anayasa'nın 13. maddesi kapsamında incelenmesi mümkün değildir. Bununla birlikte bilindiği üzere CBK'ların içerik yönünden anayasallık denetimi, konu bakımından yetki yönünden yapılan denetimden müstakil olarak yapılmaktadır. Dolayısıyla çelişkili gibi görünse de çoğunluğun konu bakımından Anayasa'nın 104. maddesinin on yedinci fıkrasının ikinci cümlesine uygun bulunduğu kuralların içerik denetimi, CBK kuralı adeta "kanun(muş) gibi" değerlendirilerek yapılmalıdır.

19. Bu anlamda kural sadece çoğunluğun incelediği Anayasa'nın 2. maddesine değil, incelemeye 20. maddesine de aykırıdır. Dava dilekçesinde kuralın açıkça Anayasa'nın 20. maddesine aykırı olduğu iddia edilmesine rağmen kararda içerik denetimi yapılırken bu madde yönünden inceleme yapılmamış, ayrıca "inceleme yapılmasına gerek olmadığı" ya da kuralın Anayasa'nın 20. maddesiyle "ilgisi olmadığı" da belirtilmemiştir.

20. Bu durumun kuralın konu bakımından yetki yönünden incelenmesi sırasında kişisel verilerin korunmasını isteme hakkıyla ilgisinin görülmemesinden kaynaklandığı, çoğunluğun içerik yönünden denetimde de açıkça ifade etmese de zımnen bu yaklaşımı sürdürdüğü, dahası sürdürmek zorunda kaldığı anlaşılmaktadır. Bu yaklaşımın ciddi bir açmaza yol açtığını, bu açmaza da ilk düşmanın yanlış iliklenmesiyle girildiğini söylemek yanlış olmaz. Kural doğrudan ve açıkça kişisel veriler konusunda bir düzenleme yaptığı halde, kuralın 6698 sayılı Kanun'a aykırı, onu aşan bir yönünün olmadığı belirtilerek "yasak alan"a girmediği savunulmuştur.

21. Halbuki kişisel verilerin istenmesine dair kurallar konusunda Anayasa Mahkemesinin yukarıda ifade edilen yerleşik içtihadında benimsediği yaklaşımını CBK'ların denetiminde değiştirmesi için herhangi bir neden bulunmamaktadır. Kuralların içerik denetimi bakımından kanunlar ile CBK'lar arasında bir farklılık yoktur. Daha da önemlisi denetlenen kuralın kanun veya CBK hükmü olmasına göre esas alınan ölçü normların değişmesi, çelişkili kararların verilmesine de yol açabilir.

22. Anayasa koyucu, Anayasa'nın 20. maddesinde, "Özel hayatın ... gizliliğine dokunulamaz" şeklinde keskin bir dil kullanmak suretiyle özel hayatın mahremiyetinin önemine işaret etmiştir. Bu gizliliğin özel bir yansıması kişisel verilerin korunmasında karşımıza çıkmaktadır. Anayasa'nın 20. maddesi uyarınca kişinin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı, "kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar."

23. Kişisel veri, kişinin mahremiyetinin en önemli yönlerinden birini, dolayısıyla maddi ve manevi varlığını geliştirme hakkının da ayrılmaz unsurunu oluşturmaktadır. Kişisel verilerin korunması hakkı, Anayasa Mahkemesi kararlarında ifade edildiği üzere, insanın "onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır" (AYM, E.2014/87, K.2015/112, 8/12/2015, § 164).

24. Bununla birlikte kişisel verilerin korunmasını isteme hakkı sınırsız değildir. Anayasa'nın 13. maddesinde öngörülen güvencelere aykırı olmamak kaydıyla söz konusu hak sınırlandırılabilir. Bu güvencelerin başında "kanunla sınırlama" ölçütü gelmektedir. Buna göre, diğer temel hak ve hürriyetler gibi, kişisel verilerin korunması hakkının da sınırlandırılabilmesi kanunla mümkündür. Dahası bu hakkın yer aldığı Anayasa'nın 20. maddesinde "kanunla sınırlama" şartı, "Kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir" şeklinde özel olarak düzenlenmiştir.

25. Buradan hareketle, Anayasa'nın 13. ve 20. maddeleri kapsamında kişisel verilerin korunmasını isteme hakkının ancak kanunla sınırlanabileceği, dolayısıyla bu hakka yönelik müdahalenin kanuni dayanağının bulunmadığı açıktır. Bununla birlikte, sınırlama için kanuni düzenlemenin bulunması da yeterli olmayıp, bu düzenlemenin açık, belirgin ve öngörülebilir olması gerekmektedir. Temel hak ve özgürlükleri sınırlandıran kanunun kaliteli olması, Anayasa'nın 2. maddesinde güvenceye alınan hukuk devletinin de gereğidir. Dolayısıyla sınırlama ölçütü olarak belirtilen kanunilik, Anayasa'nın 2. maddesinde güvenceye alınan hukuk devleti ilkesi ışığında yorumlanmalıdır.

26. Anayasa Mahkemesi kararlarında vurgulandığı üzere hukuk devletinde, kanuni düzenlemelerin “hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfî uygulamalarına karşı koruyucu önlem içermesi gerekir” (AYM, E.2015/41, K.2017/98, 4/5/2017, § 153). Kanunda bulunması gereken bu nitelikler hukuki güvenliğin sağlanması bakımından da zorunludur. Zira bu ilke “hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar” (AYM, E.2015/41, K.2017/98, 4/5/2017, § 154).

27. Belirtmek gerekir ki, temel hak ve özgürlüklere yapılacak müdahale alanı genişledikçe, muhtemel keyfi ve ölçüsüz uygulamalara karşı bireylere güvence sağlayan kuralların daha açık ve belirli olması gerekir. Kişisel verilerin korunması hakkıyla ilgili dava konusu kural bakımından da bu durum geçerlidir. İletişim Başkanlığının görev alanının oldukça geniş olduğu ve dolayısıyla iptali istenen ibarenin geniş bir alanda kişilerin temel haklarına müdahaleye izin verdiği dikkate alındığında, kişisel verilerin korunması hakkını korumaya yönelik güvenceleri karşılayan açıklıkta ve belirlilikte düzenlemeye ihtiyaç olduğu izahtan varestedir.

28. Anayasa'nın 20. maddesi kişisel verilerin “ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla” işlenebileceğini öngörmektedir. Bu anayasal hükümle uyumlu olarak 6698 sayılı Kanun, kişisel verilerin işlenmesi konusunda bir takım genel ilke ve esaslara yer vermekle birlikte, kişilerin açık rızası olmaksızın kişisel verilerin elde edilmesi ve aktarılabilmesi için “kanunlarda açıkça öngörülme”si gerektiğini belirtmiştir (m. 5/2/a, 8/2/a).

29. Bu kapsamda dava konusu “gerekli gördüğü bilgileri” ibaresi belirlilikten uzaktır. Kuşkusuz bu noktada gerekli görülen her türlü bilgi değil, Başkanlığın görev alanına giren konulara ilişkin bilgilerin isteneceği söylenebilir. Ancak, yukarıda ifade edildiği üzere, CBK'nın 3. maddesinde sayılan görevlerin kapsamı oldukça geniştir. Her biri son derece geniş bir alana tekabül eden söz konusu görevler kapsamında gerekli görülen bilgilerin istenmesini öngören kural, neredeyse ilgili kuruma sınırsız bir yetki tanımaktadır. Dolayısıyla “gerekli gördüğü bilgileri” ibaresi hangi bilgilerin ne ölçüde talep edileceği konusunda belirsiz ve öngörülemeyen bir düzenleme niteliğindedir.

30. Öte yandan kuralın kişisel verilerin gizliliğinin korunması bakımından da güvenceler içerdiği kuşkuludur. Nitekim iptali istenen ibarenin de içinde bulunduğu fıkranın devamında (3) numaralı fıkra olarak düzenlenen “Bu şekilde elde edilen bilgilerden ticari sır niteliğinde olanların gizliliğine uyulur.” şeklindeki hüküm, “ticari sır” mahiyetinde olan bilgilerin gizliliğinin korunmasını özel olarak düzenlemiştir. Buna karşılık “ticari sır” niteliğinde olmayan diğer bilgilerin gizliliğinin nasıl

sağlanacağı konusunda herhangi bir düzenlemeye veya atıf yoluna gidilmemiştir. Bu da kuralı belirsiz ve kişisel verilerin korunması bakımından güvencesiz hale getiren hususlardan biridir.

31. Açıklanan gerekçeler ve benzer mahiyette bir kanun hükmünün denetimi kapsamında verilen ve yukarıda (10) nolu paragrafta atıf yapılan karara yazdığım Karşıoy Gerekçesinde yer alan diğer gerekçelerle dava konusu kuralın içerik yönünden de Anayasa'nın 2., 13. ve 20. maddelerine aykırı olduğu kanaatindeyim.

B. (1) Numaralı CBK'nın 485. Maddesine Eklenen (i) Bendi

32. Dava konusu kural Ulaştırma ve Altyapı Bakanlığının görev ve yetkilerinden birini düzenlemektedir. Buna göre "474 üncü maddenin birinci fıkrasının (a) bendi ile bu fıkranın (ı) bendinde yazılı projelerin ileri teknoloji veya yüksek maddi kaynak gerektirmesi halinde 8/6/1994 tarihli ve 3996 sayılı Bazı Yatırım ve Hizmetlerin Yap-İşlet-Devret Modeli Çerçevesinde Yapıtırılması Hakkında Kanun kapsamı da dahil yap-işlet-devret modeli çerçevesinde sermaye şirketlerinin veya yabancı şirketlerin görevlendirilmesi suretiyle yapılmasını sağlamak," Altyapı Yatırımları Genel Müdürlüğü'nün görev ve yetkileri arasına eklenmiştir.

33. Anayasa'nın 104. maddesinin on yedinci fıkrası Anayasa'da münhasıran kanunla düzenlenmesi öngörülen konularda CBK çıkarılmayacağını belirtmektedir. Anayasa'nın 47. maddesinin dördüncü fıkrası uyarınca özel hukuk sözleşmeleriyle gerçek ve tüzel kişilere yaptırılacak kamu yatırımları ve hizmetlerinin hangileri olduğu kanunla belirlenir.

34. Dava konusu kural ileri teknoloji veya yüksek maddi kaynak gerektiren projelerden bazılarının yap-işlet-devret modeliyle şirketlere yaptırılmasını sağlamak görevini düzenlemektedir. Kuralda hangi projelerin bu kapsamda olduğu CBK hükümlerine ve 3996 sayılı Kanun'a atıf yoluyla belirlenmiştir. Dolayısıyla kural, kanunla belirlenmesi gereken bir konu olan bazı yatırım ve hizmetlerin özel hukuk sözleşmeleri kapsamında yap-işlet-devret modeliyle yerli veya yabancı şirketlere yaptırılması konusunda düzenleme yapmaktadır.

35. Çoğunluğa göre iptali istenen kural, Anayasa'nın 47. maddesine göre kanunla belirlenmesi gereken bir düzenleme yapmamakta, sadece 3996 sayılı Kanun'a atıf yapmak suretiyle bu konudaki görevli bakanlık birimini belirlemektedir. Ancak, kural konuya ilişkin Kanun'a atıf yapan, dolayısıyla Kanun'da yer alan hususları "tekrar eden" basit bir görev ve yetki düzenlemesinin ötesine geçmektedir. Nitekim kuralda yer alan 3996 sayılı "Kanun kapsamı da dahil" ibaresi, kuralın kapsamının anılan Kanun'la sınırlı olmadığını göstermektedir. Ayrıca 3996 sayılı Kanun dışında atıf

yapılan ilgili CBK hükümlerinde yazılı projelerin de kapsama alınması kuralın sadece bir yetkilendirme hükmü olmadığına işaret etmektedir.

36. Dava konusu kural ile 3996 sayılı Kanun'un yap-işlet-devret yöntemiyle yaptırılacak yatırım ve hizmetleri saydığı 2. maddesi karşılaştırıldığında CBK kuralının anılan kanunun kapsamını genişleterek yetkilendirme yaptığı anlaşılacaktır. Sözelimi kuralın atıf yaptığı (1) bendinde yer alan "Denizleri, gölleri, nehirleri birbirine bağlayarak su yolu işlevi görececek kanal ve benzeri altyapı projeleri" ibaresi 3996 sayılı Kanun'da bulunmamaktadır.

37. Esasen çoğunluk kararı da kısmen bu görüşü teyit etmektedir. Kararda 3996 sayılı Kanun'un 2. maddesinde yap-işlet-devret yöntemiyle yaptırılacak yatırım ve hizmetlerin sayıldığı, dava konusu kuralda ifade edilen "haberleşme ile Kanal İstanbul ve benzeri su yolu projeleri"nin bu Kanun'un 2. maddesinde zikredildiği, ayrıca Kanun'da yer alan "...ve benzeri yatırım ve hizmetler..." ibaresi nedeniyle söz konusu yatırım ve hizmetlerin maddede sayılanlarla sınırlı olmadığı belirtilmektedir (§ 84).

38. Bu ifadelerden dava konusu kural kapsamındaki projelerin, kuralda yer alıp da 3996 sayılı Kanun'un 2. maddesinde açıkça belirtilen iki projeden ibaret olmadığı, maddede sayılan diğer projelerin ve daha önemlisi benzeri projelerin de aynı kapsamda olduğunun kabul edildiği anlaşılmaktadır. Dava konusu kuralın kapsamının bu şekilde belirlenmesi, Kanun'da açıkça belirtilmese de sayılanlara benzer nitelikteki yatırım ve hizmetlerin de yap-işlet-devret yöntemiyle yerli veya yabancı şirketlere yaptırılacağı yorumuna yol açabilir. Bu durumda benzeri projelerin hangileri olduğuna kimin karar vereceği meselesi gündeme gelecektir.

39. Belirtmek gerekir ki, 3996 sayılı Kanun'da "ve benzeri yatırım ve hizmetler" ibaresine yer verilmesi maddede sayılanlar dışındaki benzeri yatırım ve hizmetlerin hangileri olduğunun CBK ile belirlenebileceği anlamına gelmez. Bu konu CBK veya idari düzenleyici işlemlere bırakılamaz, zira Anayasa'nın 47. maddesi bu görevi kanun koyucuya vermiştir. Nitekim 1999 yılında Anayasa'nın 47. maddesinde yapılan değişiklikten sonra, 3996 sayılı Kanun'un 2. maddesinde muhtelif yıllarda (1999, 2008, 2013 ve 2018) yapılan yasal değişikliklerle yap-işlet-devret modeliyle yaptırılacak yatırım ve hizmetlerin kapsamı sürekli genişletilmiştir.

40. Bu değişikliklerden ilki olan ve 2. maddeye ekleme yapan 20/12/1999 tarihli ve 4493 sayılı Kanun'un genel gerekçesinde düzenlemenin Anayasa'nın 47. maddesindeki değişikliğe uyum sağlanması amacıyla yapıldığı ve 3996 sayılı "Kanun kapsamında sayılan yatırım ve hizmetlerin benzeri olan ve ileri teknoloji ve yüksek finansman gerektiren elektrik üretim, iletim, dağıtım ve ticareti ile ilgili yatırımların yerli veya yabancı şirketlere özel hukuk sözleşmeleriyle yaptırılması"nın

hedeflendiği belirtilmiştir. Aynı şekilde 9/5/2008 tarihli ve 5762 sayılı Kanun'la 3996 sayılı Kanun'un 2. maddesine "otoyol" ibaresinden sonra gelmek üzere bu hizmetin benzeri olduğunda tereddüt bulunmayan "trafiği yoğun karayolu" ibaresi, "demiryolu" ibaresinden sonra gelmek üzere "gar kompleksi, lojistik merkezi" ibareleri eklenmiş, dahası "hava limanları" ibaresi "hava alanları ve limanları" olarak değiştirilmiştir. Bu örneklerden de anlaşılacağı üzere "ve benzeri yatırım ve hizmetler"in hangileri olduğu kanun tarafından belirlenmektedir.

41. Diğer yandan Anayasa'nın 104. maddesinin on yedinci fıkrasının dördüncü cümlesi uyarınca kanunda açıkça düzenlenmiş konularda CBK çıkarılamaz. Yap-işlet-devret yöntemiyle yaptırılacak yatırım ve hizmetler konusu özel olarak 3996 sayılı Kanun'da düzenlenmiştir. Bu Kanun'un sınırlarını aşacak şekilde düzenlenen dava konusu CBK kuralı bu nedenle de konu bakımından yetki yönünden Anayasa'ya aykırıdır.

42. Açıklanan gerekçelerle, dava konusu her iki kuralın da Anayasa'ya aykırı olduğunu düşündüğümden çoğunluğun aksi yöndeki görüşüne katılmıyorum.

Başkan - Zühtü ARSLAN

KARŞIOY GEREKÇESİ

A. 14 Numaralı İletişim Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinin 17. Maddesinin 2 Numaralı Fıkrasının Birinci Cümlesinde Yer Alan "...gerekli gördüğü bilgileri..." İbaresinin Hakkında:

1. Kararnameye göre İletişim Başkanlığı Cumhurbaşkanlığına bağlı, genel bütçeye dahil, merkezi idare kapsamında Devlet tüzel kişiliği içinde yer alan bir kamu kurumudur. Görev alanının da ülkenin tanıtılması, ulusal ve uluslararası düzeyde kamuoyunun ve ilgili makamların doğru bilgilendirilip aydınlatılması ve bu amaçla bilgi ve haber akışı ve takibinin yapılması hususlarını kapsadığı anlaşılmaktadır. Görev alanlarıyla ilgili bilgilerin kamu kurumlarından istenmesinin de yürütmeye ilişkin bulunduğu düşünülmelidir. İncelenen ibare Başkanlığı, görevi gereği bazı kamu hizmetleri veya faaliyetleri hakkında doğru bilgilendirme yapılmasını sağlamak için birtakım bilgileri istemeye yetkili kılmaktadır. Bu konuda yetkilendirme yapılmasının görevin gereği olarak meşru amacı haiz ve kamu yararını taşıdığı kabul edilmelidir. Bununla birlikte çeşitli kurumlarca yürütülen kamu hizmetlerinin bazı bireylerin kişisel verilerine temas etmesi ve istenilen bilgilerin bunları da kapsamaması olasıdır. Nitekim kuralda istenecek bilgiler yönünden bir sınırlama veya ayırım yapılmamış, hatta sonraki bentte ticari sırlarla ilgili ayrık duruma yer verilmiştir.

2. Anayasanın 20/3. maddesinde kişisel veriler özel olarak güvence altına alınmıştır. Bu düzenleme uyarınca kişinin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı, “kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar.” Kişisel veriler esasen maddi ve manevi varlığı koruma ve geliştirme hakkıyla ve insan onuruyla da bağlantılıdır. Nitekim Anayasa Mahkemesi kişisel verilerin “onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak” korunduğunu ifade etmiştir (AYM E.2014/87, K.2015/112, 8/12/2015, § 164). Diğer taraftan bu hak mutlak olmayıp, kişilerin özel hayatlarına ve kişisel verilerine yönelik olarak kanunla sınırlama yapılabilir. Bununla birlikte sınırlamaya yönelik bir kanunun şeklen var olması yeterli değildir. Anayasa’nın 13. ve 20. maddeleri uyarınca yasal kuralların keyfiliğe izin vermeyecek şekilde belirli, ulaşılabilir ve öngörülebilir düzenlemeler niteliğinde olması gerekir (bkz. AYM Tuğba Arslan [GK], B.No: 2014/256, 25/06/2014, § 89).

3. Çoğunluk görüşüyle yazılan gerekçede ibarenin kişisel verileri kapsamadığı savunulmuştur. Böyle değerlendirildiğinde ibarenin açık anlamı karşısında Anayasanın 2. maddesi uyarınca kanunilik ilkesi ve belirlilik alt ilkesi uyarınca kuralın belirsiz olduğu ve bu nedenle iptal edilmesi gerektiği söylenmelidir. Öte yandan diğer bir gerekçe ise 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca İletişim Başkanlığının anılan Kanun uyarınca verileri aktarma ve işleme yetkisi olduğu yorumudur. Ne var ki anılan Kanuna bakıldığında kişisel verilerin rıza aranmaksızın aktarılmasıyla ilgili olarak yasal imkanın; aynı Kanunun 5/2. veya 6/3. maddelerindeki hallerde mümkün olacağı belirtiltiğini görmekteyiz. Bunlardan ilkinde zorunluluk nedeni veya bir hakkın tesisi gibi nedenlerin varlığı halinde veya kanunlarda açıkça öngörülmesi halinde veri işlenebileceği ve 8. madde gereği de aktarılabileceğinin belirtildiği görülmektedir. Dokuzuncu madde verilerin yurt dışına çıkartılması koşullarını düzenlemektedir. Altıncı maddenin 3. fıkrasında ise sağlık ve cinsel hayatla ilgili bilgilerin sağlık hizmeti veya finansmanı amacıyla, diğer bilgilerin ise kanunlarda öngörülen açık rıza aranmaksızın işlenebileceği belirtilmektedir. Dolayısıyla 6698 sayılı Kanun, ilgili kamu kurumlarına yalnızca yürüttükleri kamu hizmetinin zorunlu sonucu olarak veya bir hak tesisi bakımından gerekli hallerde veri işleme yetkisi vermektedir. Ayrıca anılan maddeler incelendiğinde işlenen verilerin başka bir kuruma transferinin ise ilgili kanunda belirtilmesi halinde mümkün olduğu görülmektedir. Dolayısıyla veri transferinin 6698 sayılı Kanun çerçevesinde mümkün olduğu (bkz. Gerekçe, par.24) görüşünün yasal ve anayasal bir dayanağı bulunmamaktadır. Diğer taraftan çoğunluk görüşünde incelenen ibarenin kişisel verileri kapsamadığı söylenmektedir (bkz. par.25). Bu durumda 6698 sayılı Kanunda veri transferi için sözü edilen ilgili kanunda olması beklenen kanuni dayanağın bulunmadığı kabul edilmiştir. Bu yorum karar haline dönüştüğüne göre İletişim Başkanlığı’nın 6698

sayılı Kanun uyarınca veri transferini talep yetkisi de bulunmamaktadır. Bu arada belirtilmelidir ki incelenen ibarenin kişisel verileri kapsadığı kabul edildiğinde ise 6698 sayılı Kanununun 8/2. ve 5/2. maddelerinde “Kanunlarda açıkça öngörülmesi” şartının arandığı, ibarenin ise bu açıklık şartını karşılamadığı dikkate alınmalıdır.

4. Kuralın kişisel verileri de kapsadığını değerlendirdiğimizden, Anayasanın 104. maddesinin 17. fıkrasının ikinci cümlesi uyarınca Cumhurbaşkanlığı Kararnameleriyle temel hak ve özgürlüklerin düzenlenemeyeceği açıktır. Bu nedenle CBK düzenlenemeyecek bir konuyu kapsamaması nedeniyle incelenen kuralın konu bakımından Anayasanın 104/17. maddesi uyarınca iptal edilmesi gerekmektedir.

5. İçerik yönünden ise kişisel verilerin temel hak güvenceleri kapsamında olması nedeniyle, başka bir kamu idaresi veya kurumu nezdinde kaydedilen kişisel verilerin transferinin istenebilmesi için Anayasanın 20/3. maddesi, gerekse Anayasanın 13. maddesi uyarınca kanunla açıkça düzenlenmesi gerekmektedir. Bu yönde düzenlenecek kanunda meşru amacın ve sınırlarının da gösterilmesi gerekir. Belirtilen nedenlerle incelenen kuralın içerik yönünden de anayasaya aykırı olduğu ve iptali gerektiği görüşündeyim.

B. 1 Numaralı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinin 485. Maddesinin 1 Numaralı Fıkrasına (14 Numaralı CBK'nın 26/2-c maddesiyle) Eklenen (i) Bendi Hakkında:

6. İncelenen kuralda Ulaştırma ve Altyapı Bakanlığının görev ve yetkileri kapsamında Bakanlığa, ileri teknoloji veya yüksek maddi kaynak gerektiren projelerin Yap-İşlet-Devret Modeli ile sermaye şirketleri veya yabancı şirketlerin görevlendirilmesi suretiyle yapılmasını sağlama yetkisi verilmektedir.

7. Bilindiği üzere Anayasada verilen yetki kapsamında düzenlenebilecek CBK'lar bakımından bazı yasak alanlar ve sınırlamalar öngörülmüştür. Bu anlamda Anayasanın 104. maddesinin 17. fıkrasının üçüncü ve dördüncü cümlelerinde; “Anayasada münhasıran kanunla düzenlenmesi gereken konularda CBK çıkarılamaz. Kanunda açıkça düzenlenen konularda CBK çıkarılamaz.” denilmektedir. Öte yandan Mahkememiz daha önceki kararlarında “münhasıran kanunla düzenlenmesi gereken konular” ibaresinin; Anayasada bir konunun kanunla düzenlenmesinin zorunlu görüldüğü halleri ifade ettiğini kabul etmiştir.

8. Anayasanın 47/4. maddesi uyarınca Devlet veya kamu tüzel kişilerin yürütülen yatırım veya hizmetlerden hangilerinin özel hukuk sözleşmeleri ile yaptırılacağı veya devredilebileceğinin

kanunla belirleneceği ifade edilmektedir. Bu açık anayasal kuraldan anlaşılacağı üzere bu konuların kanun dışındaki bir düzenleyici işlemle ve bu arada CBK ile düzenlenmesi konu bakımından anayasaya aykırılık oluşturur. Bu zorunluluk ayrıca CBK'leri konu bakımından sınırlayan ilgili Anayasa kuralından (m.104/17-3.c.) kaynaklanmaktadır. Dolayısıyla incelenen kuralın anılan hüküm nedeniyle konu bakımından Anayasaya aykırı olduğundan iptali gerektiği görüşümdedir.

9. İkinci olarak aynı konu 3996 Bazı Yatırım ve Hizmetlerin Yap-İşlet-Devret Modeli Çerçevesinde Yaptırılması Hakkında Kanun tarafından düzenlenmiştir. Bu Kanunun 1. maddesi uyarınca KİT'ler dahil tüm kamu kurum ve kuruluşları tarafından ifa edilen, ileri teknoloji veya yüksek maddi kaynak gerektiren bazı yatırım ve hizmetlerin, yap-işlet-devret modeli çerçevesinde yaptırılması sağlanabilecektir. Diğer taraftan Ulaştırma Bakanlığının kuruluşuyla ilgili 655 sayılı KHK'da değişiklik yapan 703 sayılı KHK ile Bakanlık ve anılan Genel Müdürlüğün görev ve yetkilerine ilişkin kuralların yürürlükten kaldırılması, akabinde ilgili mevzuat kapsamında faaliyete geçirilmiş olan Bakanlığın faaliyetleri bakımından 3996 sayılı Kanun hükümlerinin uygulanmasına engel değildir. Anayasanın 104/17. maddesinin anılan 4. Cümlesi karşısında, bir konunun kanunda açıkça düzenlenmesinden sonra aynı hususun CBK ile düzenlenmesi, anılan anayasal hükme aykırılık oluşturacaktır. Esasen Kanunda Bakanlığa aynı yetkinin veriliyor olması karşısında konunun tekrar düzenlenmesinin hukuken bir gereği de bulunmamaktadır. Buna karşın kanunda düzenlenen bir hususun tekrar CBK ile düzenleniyor olması, Anayasada CBK'lar için öngörülen hukuksal sistemi bozmakta ve bu düzenleme nedeniyle kanundan farklı yorum ve uygulamaya neden olabilmektedir. Öte yandan Anayasada kanunlar ve CBK'ler için öngörülen hukuki rejimin ve kanunlara ilişkin yasama yetkisinin asliliği-genelliği ilkelerinin korunması açısından CBK ile yapılacak düzenlemenin kanunun kapsamını daraltması veya genişletmesinin bir önemi bulunmamaktadır. Kanunda açıkça düzenlenen bir hususun tekrar CBK ile düzenlenmesi hali her durumda konu bakımından Anayasanın anılan kuralına aykırılık oluşturmaktadır. Bu nedenle de kuralın iptali gerekmektedir.

Başkanvekili - Hasan Tahsin GÖKCAN

KARŞIOY GEREKÇESİ

A) Konu Yönünden Anayasa'ya Uygunluk Denetimi

1. (14) Numaralı İletişim Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin (CBK) 17. maddesinin (2) numaralı fıkrasında yer alan "...gerekli gördüğü bilgileri..." ibaresinin

Anayasa'ya aykırılığı iddiasıyla iptal davası açılmıştır. İptali istenen ibarenin yer aldığı fıkranın birinci cümlesinde İletişim Başkanlığı'nın görevleri ile ilgili olarak gerekli gördüğü bilgileri bütün kamu kurum ve kuruluşlarından ve diğer gerçek ve tüzel kişilerden doğrudan istemeye yetkili olduğu belirtilmiştir.

2. Anayasa'nın 104. maddesinin onyedinci fıkrasının birinci cümlesinde, yürütme yetkisine ilişkin olmak şartıyla kararname çıkarma konusunda Cumhurbaşkanına genel bir yetki verilmiştir. Fıkranın ikinci cümlesinde, Anayasanın ikinci kısmının birinci ve ikinci bölümlerinde yer alan temel haklar, kişinin hakları ve ödevleriyle dördüncü bölümde yer alan siyasi haklar ve ödevlerin kararnameyle düzenlenemeyeceği belirtilmiştir. Üçüncü cümlesinde ise, Anayasa'da münhasıran kanunla düzenlenmesi öngörülen konularda kararname çıkarılmayacağı hüküm altına alınmıştır. Son olarak, fıkranın dördüncü cümlesinde de kanunda açıkça düzenlenen konularda kararname çıkarılmayacağı ifade edilmiştir.

3. Dava konusu kuralın İletişim Başkanlığı'nın görevleri kapsamında gerekli gördüğü bilgileri belirtilen gerçek ve tüzel kişilerden istemeye yetkili kılması yürütme yetkisine ilişkin bir konuyu düzenlediğinden, kural bu ölçüt açısından Anayasa'nın 104. maddesinin onyedinci fıkrasının birinci cümlesi ile uyumluluk taşımaktadır.

4. Dava konusu olan "gerekli gördüğü bilgileri" ibaresinde yer alan "bilgileri" kelimesinin kapsamına kişisel verileri içeren bilgiler de girebilmektedir. Anayasa'nın 20. maddesinin birinci fıkrasında "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz." denilerek özel hayatın gizliliği güvence altına alınmıştır. Maddenin üçüncü fıkrasında ise "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilmiştir.

5. Kural kişisel verileri içeren bilgileri de kapsadığından Anayasa'nın 20. maddesini ilgilendiren bir düzenleme getirmektedir. Dolayısıyla Anayasa'nın 104. maddesinin onyedinci fıkrasının ikinci cümlesinde yer verilen hükme aykırılık taşımaktadır. Başka bir ifadeyle, kural, Anayasa'nın ikinci kısmının birinci ve ikinci bölümlerinde yer alan temel haklar, kişinin hakları ve ödevleriyle ilgili bir düzenleme içerdiğinden yasak alan kapsamındadır.

6. Belirtilen gerekçeyle, dava konusu kuralın Anayasa'nın 104. maddesinin onyedinci fıkrasının ikinci cümlesine aykırı olduğu sonucuna ulaştığımdan, çoğunluk kararına katılmıyorum.

B) İçerik Yönünden Anayasa'ya Uygunluk Denetimi

7. Mahkememiz oyçokluğuyla dava konusu kuralın konu yönünden Anayasa'ya uygun olduğuna karar verip, içerik incelemesine geçtiğinden bu bölümde kuralın içerik yönünden Anayasa'ya aykırılık taşıyıp taşımadığı incelenecektir.

8. İletişim Başkanlığına tanınan yetki istenilecek bilgiler arasında kişisel verilerin olması durumunda nasıl bir yol izleneceği, bu verilerin toplanması, işlenmesi, saklanması ve imhası konularında ne gibi güvencelerin sunulacağına dair herhangi hüküm içermediği gibi konuyla doğrudan bağlantılı 6698 sayılı Kişisel Verilerin Korunması Kanunu ve konuyla ilgili özel kanunlara herhangi yollamada bulunmamaktadır.

9. Kişisel veri kavramı kimliği belirli veya belirlenebilir kişiye ilişkin her türlü bilgiyi ifade eder. Kişisel verilerin korunması hakkı, Anayasa Mahkemesi kararlarında vurgulandığı gibi, insanın "onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır" (AYM, E. 2014/87, K. 2015/112, 8/12/2015, § 164). Aynı şekilde Mahkememiz "Özel hayatın gizliliği ve kişisel verilerin korunması hakkı, temel hak ve özgürlükler arasında önemli bir yer tutar...Kişisel verilerin korunması hakkı ise özel hayatın gizliliği hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır" tespitinde de bulunmuştur (AYM E: 2017/16, K. 2019/64, 24/7/2019, § 48).

10. Anayasa Mahkemesi dava konusu kuralla benzer nitelik taşıyan bir kararında (E. 2014/149, K. 2014/151, 2.10.2014) kişisel veri niteliğinde olan ve ciddi suçların tespiti, soruşturulması ve kovuşturulmasında kullanılmak üzere gerçek ve tüzel kişilere ilişkin trafik bilgisinin erişim veya yer sağlayıcılardan, Telekomünikasyon İletişim Başkanlığı (TİB) tarafından herhangi bir gerekçe veya neden göstermeksizin temin edilmesine olanak sağlayan kuralın Anayasanın 2.13. ve 20. maddelerine aykırı olduğu sonucuna ulaşmıştır. Mahkeme, trafik bilgisi adı altında temin edilecek olan bilgilerin birçok temel hakla doğrudan ilgili olup bu bilgilerin TİB tarafından herhangi bir kurala ve sınırlamaya tabi olmaksızın istenildiği zaman ve şekilde elde edilebilir olmasını temel hak ve özgürlüklerin korunması bakımından sorunlu bulmuştur.

11. AYM, başka bir kararında da içerik, yer ve erişim sağlayıcılarını, TİB tarafından talep edilen bilgileri talep edildiği şekilde TİB'e teslim etmekle ve bu kurum tarafından bildirilen tedbirleri

almakla yükümlü kılan kanuni düzenlemeleri, kişisel verilerin korunması hakkının gerektirdiği güvencelerden yoksun olduğu için iptal etmiştir. Anayasa Mahkemesine göre iptali istenen kurallarda, talep edilen bilgilerin verilmesinden ilgili kişilerin haberdar olmalarına ilişkin bir düzenlemeye yer verilmemekte, “TİB’in hangi koşullarda ve hangi gerekçelerle istediği bilgilerin içerik, yer ve erişim sağlayıcılar tarafından Başkanlığa teslim edileceğine ya da verilen bilgilerin ne kadar süre ile TİB’de saklanacağına, talep edilen bilgilerin mahiyetine, içerik, yer ve erişim sağlayıcılara bildirilecek tedbirlere ilişkin herhangi bir belirlilik bulunmamakta”, belirli ve öngörülebilir olmayan düzenlemelerden dolayı kişisel verilerin korunması hakkı ölçsüzce sınırlandırılmaktadır (AYM, E.2014/87, K.2015/112, 8/12/2015, §§ 168-170).

12. Anayasa’nın 20. maddesinde, kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği belirtilmiştir. Dava konusu kuralla İletişim Başkanlığına tanınan yetkinin son derece geniş olması kişisel verileri koruma hakkına yönelik herhangi bir sınırı olmayan müdahalelere neden olma potansiyelini bünyesinde taşımaktadır. Bu nedenle, kişisel verilerin korunması hakkıyla ilgili yasal düzenlemelerin açık, net ve anlaşılabilir olması ve keyfi ve amaca uygun olmayan kullanımlara karşı güvenceler sağlaması gerekmektedir.

13. Devlet kendisinden beklenen işlevleri yerine getirmek için bireylere ait bilgileri çeşitli gerekçelerle kaydetme, saklama, aktarma ve kullanma gibi işlemlerde kullanabilir ama bunun kişi hak ve özgürlüklerini en az sınırlayacak şekilde yapılması gerekir. Kişisel verilerle ilgili yasal düzenlemelerde verilerin toplanması, kullanılması, ne kadar süre ile tutulacağı, amaca uygun kullanılıp, kullanılmadığının nasıl denetleneceği ve imhası gibi hususların açık ve net olarak düzenlenmesi gerekmektedir. Bu durumlarda kötüye kullanımları engellemek ve keyfi uygulamaların önüne geçmek amacıyla belli güvenceler ortaya konulmalı ve bunların etkin bir şekilde işlenmesi sağlanmalıdır. Kişisel verilere dönük müdahalelerin demokratik toplum düzeni gereklerine uygun ve ölçülü olması da anayasal bir zorunluluktur. Modern devlet bilgi açlığını giderirken, iştahını kontrol etmeyi bilmelidir. Aksi takdirde obezite durumuyla karşı karşıya gelebilir ve bu da hukuki, toplumsal, siyasi ve iktisadi sağlık için sorunlara yol açabilir.

14. Anayasa’nın 13. maddesinde, temel hak ve özgürlüklerin özlerine dokunulmaksızın ölçülülük ilkesine uygun şekilde, yasayla sınırlandırılabilmesi belirtilmektedir. Ölçülülük ilkesi sınırlamada başvuru aracının sınırlama amacını gerçekleştirmeye elverişli olmasını; bu aracının sınırlama amacı açısından gerekli olmasını ve araçla amacın ölçsüz bir oran içinde bulunmamasını ifade eder. Burada kısıtlama için kullanılan araçla amaç arasında hak ve özgürlüğü en az sınırlayacak dengeli bir orantı aranmaktadır.

15. Elverişlilik ölçütüne göre bir yasal düzenlemenin sınırlama amacı bakımından elverişli sayılması için bu düzenlemenin arzulanan amaca veya amaçlara katkı yapması gerekmektedir. İncelediğimiz kural bu niteliği taşımaktadır. Gereklik ise bir temel hakkı en az sınırlayan aracın seçilmesini gerektirmekle birlikte dava konusu kuralın hakkı en az sınırlayan bir araç olduğunu söylemek mümkün değildir. Çünkü söz konusu kurallar, çok geniş bir çerçeveyi kapsayarak bireyin her türlü kişisel verisinin toplanmasını, aktarılmasını ve işlenmesini mümkün hale getirmektedir. Kuralın özel hayatın gizliliği ve kişisel verilerin korunması hakları ile kamu yararı amacıyla İletişim Başkanlığına tanınan yetki arasında orantılı makul bir denge kurmayarak, birincisini ikincisi lehine adeta gözden çıkarmaktadır. Dolayısıyla Başkanlığa tanınan yetki kişisel verilerin gizliliği, güvenliği ve korunması açısından hakka yönelik ölçsüz bir müdahaleye neden olmaktadır.

16. Özel hayatın gizliliği ve bu kapsamda kişisel verilerin korunması konusu her şeyden önce insan haysiyetine saygı ve kişilik haklarına dayanmaktadır. Kişisel verilerin toplanması ve işlenmesi sırasında bireyin bu veriler üzerindeki hakkı, onun devlet veya üçüncü kişiler tarafından sıradan bir veri nesnesine indirgenmesini önlemek amacını taşımaktadır. Kişisel verilerin ilgili kişinin açık rızası olmadan toplanması, işlenmesi ve aktarılması, kişinin basit bir veri nesnesi olarak değerlendirilmesine yol açtığından insan haysiyetini de zedelemektedir.

17. Yukarıda açıklanan nedenlerle dava konusu kuralın Anayasa'nın 13. ve 20. maddelerine aykırı olduğu gerekçesiyle karara katılmıyorum.

Üye - Engin YILDIRIM

KARŞIOY GEREKÇESİ VE FARKLI GEREKÇE

(14) numaralı Cumhurbaşkanlığı Kararnamesinin (CBK) 17. maddesinin (2) numaralı fıkrasının birinci cümlesindeki "...gerekli gördüğü bilgileri..." ve 22. maddesinin (1) numaralı fıkrasındaki "...yurtdışı ve..." ibareleri ile 26. maddesiyle (1) numaralı CBK'nın 485. maddesinin (1) numaralı fıkrasına eklenen (i) bendinin konu ve içerik yönünden Anayasaya aykırı olmadığına ve iptal talebinin reddine karar verilmiştir.

A. Yukarıda belirtilen hükümlerin konu yönünden Anayasaya aykırı olmadığı yönündeki çoğunluk görüşüne aşağıdaki sebeplerle karşıyım.

1. CBK'nın 17. maddesinin (2) numaralı ve 22. maddesinin (1) numaralı fıkralarındaki ibarelerin Anayasaya aykırılığı iddiasının konu yönünden reddine ilişkin kararların gerekçelerinde; anılan kurallarda öngörülen hususların yürütme yetkisine ilişkin konulardan olduğu, kuralların

Anayasanın İkinci Kısımının Birinci ve İkinci Bölümlerinde yer alan temel haklar, kişi hakları ve ödevleriyle Dördüncü Bölümünde yer alan siyasî haklara ve ödevlere ilişkin düzenleme içermediği, Anayasanın 123. maddesinin birinci fıkrasında idarenin kuruluş ve görevlerinin kanunla düzenleneceği hükme bağlansa da, 106. maddesinin son fıkrasında bakanlıklar için öngörülen istisnanın Cumhurbaşkanlığı teşkilatı ile Cumhurbaşkanlığına bağlı kuruluşları da kapsamından dolayı Anayasanın bu hükmü uyarınca bu kuruluşların da kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ve merkez ve taşra teşkilatının kurulması konularında CBK ile düzenlemeler yapılmasının Anayasaya aykırılık teşkil etmediği, ayrıca bu konuların daha önce kanunlarda açıkça düzenlenmediği belirtilerek, kuralların konu yönünden Anayasanın 104. maddesine aykırı olmadığı sonucuna varılmıştır.

Bu karar da dahil olmak üzere konuya ilişkin kararlarımızın, CBK'ların anayasal çerçevesine ilişkin genel açıklamalar bölümlerinde belirtildiği üzere, 6771 sayılı Kanunla yapılan Anayasa değişikliği ile hukuk sistemimize giren CBK'ların esasları Anayasanın 104. maddesinin onyedinci fıkrasında düzenlenerek Cumhurbaşkanına yürütme yetkisine ilişkin konularda CBK ile düzenleme yapma yetkisi verilmiştir. Ancak aynı fıkranın ikinci ve üçüncü cümlelerinde; temel haklar, kişinin hakları ve ödevleri ile siyasî hakların CBK ile düzenlenemeyeceği ve Anayasada kanunla düzenlenmesi öngörülen konularda CBK çıkarılamayacağı belirtilmiştir.

a) CBK'nın 17. maddesinin (2) numaralı fıkrasında, İletişim Başkanlığının görevleri ile ilgili olarak gerekli gördüğü bilgileri bütün kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden doğrudan istemeye yetkili olduğu; kendilerinden bilgi istenen bütün kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin de bu bilgileri vermekle yükümlü oldukları hükme bağlanmıştır.

Öncelikle Mahkememizin, (14) numaralı CBK'nın 14. ve 26. maddelerinin iptali talebiyle açılan davanın reddine ilişkin kararıyla ilgili karşıoy gerekçemde ayrıntılı olarak belirtilen sebeplerle, Anayasanın 106. maddesinin son fıkrası kapsamında değerlendirilemeyecek olan mezkûr Başkanlığın görev ve yetkilerinin Anayasanın 123. maddesinin birinci fıkrasına göre kanunla düzenlenmesi gerektiğinden ve bu hususun Anayasanın 106. maddesinin son fıkrasında belirtilen istisnalar kapsamında kabul edilmesi mümkün olmadığından, incelenen hüküm Anayasanın 104. maddesinin onyedinci fıkrasının üçüncü cümlesine aykırıdır (ayrıntılı açıklama için bkz. 30/12/2020 tarihli ve E. 2019/71, K. 2020/82 sayılı karara ilişkin karşıoy gerekçem).

Diğer taraftan, çoğunluğun red gerekçesinde kuralın kişisel verilerin korunmasına ilişkin mevzuat hükümlerinin uygulanmasını engelleyen, sınırlandıran veya uygulanmasına istisna getiren bir yönünün bulunmadığı ve her türlü işlemin kişisel verilere ilişkin kanunlara uygun olarak

gerçekleştirileceği belirtilmekte ise de, Anayasanın 104. maddesinin onyedinci fıkrasının ikinci cümlesinde CBK'lar bakımından belirlenen yasak alanın Anayasanın İkinci Kısımının "Kişinin Hakları ve Ödevleri" başlıklı İkinci Bölümünde yer alan 20. maddedeki hakla ilgili -sınırlama getirmeyen- düzenlemeleri de kapsadığı tartışmasıdır.

Kuralın, red gerekçesinde belirtilenin aksine kişisel verilere ilişkin bir düzenleme içerdiği açıktır. Başka bir deyişle, kuralın, çoğunluğun belirttiği gibi bu hakkı sınırlandırmadığı ve kişisel verilerin korunmasına ilişkin 6698 sayılı Kanunun uygulanmasına istisna getirmediği kabul edilse bile, kişisel verilerle ilgili olmadığı ve bunlara ilişkin düzenleme içermediği yönündeki kabule katılmak mümkün değildir. Anayasanın 104. maddesinin onyedinci fıkrasının ikinci cümlesinde kişi hakları ile ilgili olarak öngörülen yasak alan ise "sınırlama" kavramından daha geniş olan "düzenleme" yasağına ilişkindir.

Bu nedenle, incelenen ibare, Anayasanın 104. maddesinin onyedinci fıkrasının ikinci cümlesine de aykırıdır.

b) CBK'nın 22. maddesinin, İletişim Başkanlığının yurtdışı ve taşra teşkilatı kurmaya yetkili olduğunu hükme bağlayan (1) numaralı fıkrası ve bu kapsamda dava konusu "yurtdışı" ibaresi de yukarıda belirtilen karşıoy gerekçemde açıklanan sebeplerle mezkûr Başkanlık Anayasanın 106. maddesinin son fıkrasında geçen "bakanlık" kavramı kapsamında değerlendirilemeyeceğinden; ayrıca yurtdışı teşkilatının kurulması bakanlıklar için bile Anayasanın söz konusu hükmünde tahdidî olarak sayılan konular arasında yer almadığından, Anayasanın 104. maddesinin onyedinci fıkrasının üçüncü cümlesine aykırıdır (bkz. 12/6/2020 tarihli ve E. 2019/105, K. 2020/30 sayılı karara ilişkin karşıoy gerekçem).

Başka bir anlatımla, genel bütçe içinde Cumhurbaşkanlığının bağlı kuruluşu olarak CBK ile kurulan İletişim Başkanlığının Anayasanın 123. maddesine göre kanunla kurulması, görev ve yetkileri ile teşkilatının ve yurtdışı teşkilatı kurmasının da kanunla düzenlenmesi gerektiğinden, dava konusu kurallar Anayasada kanunla düzenlenmesi öngörülen bir konuya ilişkindir.

Sonuç olarak, incelenen her iki kuralın da, yukarıda (a) ve (b) bölümlerinde açıklanan sebeplerle, konu bakımından yetki yönünden Anayasanın 104. maddesinin onyedinci fıkrasına aykırı olduğu ve iptali gerektiği düşüncesiyle çoğunluğun buna ilişkin red kararlarına katılmıyorum.

2. Çoğunluğun, CBK'nın 26. maddesinin (2) numaralı fıkrasının (c) bendiyle (1) numaralı CBK'nın 485. maddesinin (1) numaralı fıkrasına eklenen (i) bendinin konu yönünden Anayasaya aykırı olmadığına ilişkin gerekçesinde de; kuralın yürütme yetkisine ilişkin olduğu, yasak alan kapsamında

düzenleme içermediği, Bakanlığın merkez teşkilatındaki bir birimin görev ve yetkilerine ilişkin olduğundan Anayasanın 106. maddesinin son fıkrası kapsamında kaldığı, 3996 sayılı Kanunun kapsamını etkileyen veya herhangi bir surette değiştiren bir yönünün bulunmadığı ve kanunda açıkça düzenlenen konulara da ilişkin olmadığı belirtilerek bu kuralın da Anayasanın 104. maddesinin onyedinci fıkrasına aykırı olmadığına hükmedilmiştir.

Bilindiği gibi, (1) numaralı CBK'nın 474. maddesinde Ulaştırma ve Altyapı Bakanlığının görev ve yetkileri düzenlenmiş; Bakanlığın merkez teşkilatında yer alan Altyapı Yatırımları Genel Müdürlüğünün görev ve yetkilerine ilişkin 485. maddesinin (1) numaralı fıkrasının dava konusu (i) bendinde de, 474. maddenin (1) numaralı fıkrasının (a) bendi ile 485. maddenin (1) numaralı fıkrasının (i) bendinde yazılı projelerin ileri teknoloji veya yüksek maddî kaynak gerektirmesi hâlinde 3996 sayılı Kanun kapsamı da dahil yap-işlet-devret modeli çerçevesinde yapılmasını sağlamak bu Genel Müdürlüğün görev ve yetkileri arasında sayılmıştır.

Anayasanın 123. maddesinin, idarenin kuruluş ve görevlerinin kanunla düzenlenmesini öngören birinci fıkrasındaki temel ilkenin istisnalarından birini oluşturan 106. maddenin son fıkrasında, bakanlıkların görevleri ve yetkilerinin CBK ile düzenlenmesine imkân tanındığından, anılan Bakanlığın anahizmet birimlerinin ve bunların görevleri ile yetkilerinin CBK ile belirlenmesinde 123. maddedeki idarenin kanunîliği ilkesiyle bağlantılı olarak Anayasanın 104. maddesinin onyedinci fıkrasının üçüncü cümlesine bir aykırılık bulunmasa da, düzenlemenin Anayasanın 47. maddesi bakımından da incelenmesi gerekir.

Anayasanın 47. maddesinin son fıkrasında; Devlet, kamu iktisadî teşebbüsleri ve diğer kamu tüzelkişileri tarafından yürütülen yatırım ve hizmetlerden özel hukuk sözleşmeleri ile gerçek veya tüzelkişilere yaptırılacak veya devredilebilecek olanların kanunla belirleneceği hükme bağlanmıştır.

Çoğunluğun gerekçesinde, Anayasanın 47. maddesinin son fıkrası uyarınca kanunla düzenlenmesi gereken hususların 3996 sayılı Kanunla düzenlendiği, incelenen kuralın 3996 sayılı Kanunun kapsamını genişleten, daraltan veya değiştiren bir yönünün bulunmadığı, başka bir ifadeyle yap-işlet-devret modeliyle yapılabilecek yatırım ve hizmetlerin kapsamıyla bir ilgisinin bulunmadığı, bu nedenle münhasıran kanunla düzenlenmesi öngörülen bir konuya ilişkin olmadığı için Anayasanın 104. maddesinin onyedinci fıkrasının üçüncü cümlesine aykırılık oluşturmadığı belirtilmekte ise de, incelenen (i) bendinde 3996 sayılı Kanunun "kapsamı da dahil" olmak üzere projelerin yap-işlet-devret modeli çerçevesinde yaptırılması öngörülmek suretiyle anılan Kanunun kapsamında olmayan projelerin de aynı modelle yapılmasına imkân sağlandığı anlaşılmaktadır.

Böylece, çoğunluğun kabulünün aksine, anılan birimin görev ve yetkileri belirlenirken bunu aşacak şekilde Anayasanın 47. maddesinin son fıkrasına göre kanunla düzenlenmesi gereken bir konuda CBK ile düzenleme yapıldığı, ayrıca 3996 sayılı Kanunun kapsamını genişleten bir hüküm getirildiği görülmektedir.

Bu sebeple söz konusu hükmün de konu bakımından Anayasanın 104. maddesinin onyedinci fıkrasına aykırı olduğu ve iptal edilmesi gerektiği düşüncesiyle çoğunluğun aksi yöndeki kararına karşıyım.

B. CBK'nın 17. maddesinin (2) numaralı fıkrasının birinci cümlesindeki ibarenin içerik yönünden Anayasaya aykırı olmadığına ilişkin çoğunluk gerekçesinde; kuralın açık, anlaşılır, öngörülebilir ve uygulanabilir bir şekilde düzenlendiği ve belirlilik ilkesine aykırı bir yönünün bulunmadığı belirtilerek Anayasanın 2. maddesine aykırı olmadığı sonucuna varılmıştır.

Hukuk devletinin temel unsurlarından biri olan belirlilik ilkesi, Mahkememizin yerleşik içtihadına göre, yasal düzenlemelerin herhangi bir tereddüte ve şüpheye yer vermeyecek şekilde açık, net, anlaşılır ve nesnel olmasını ve kamu otoritelerinin keyfî uygulamalarına engel olacak tedbirleri içermesini; hukukî güvenlik ilkesiyle bağlantılı olarak da, kanunda belirli bir kesinlik içinde hangi somut olgulara hangi sonuçların bağlandığının görülebilmesini zorunlu kılmaktadır. Kuşkusuz söz konusu ilke CBK'lar bakımından da geçerlidir.

5809 sayılı Kanunun 60. maddesine eklenen ve Bilgi Teknolojileri ve İletişim Kurumuna "görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alma ve değerlendirme" yetkisi veren, bu kapsamda Kurumun her türlü bilgi ve belge talebinin de ilgili bakanlık, kurum ve kuruluşlar tarafından yerine getirilmesini öngören (11) numaralı fıkra Anayasaya ve bu çerçevede belirlilik ilkesi bakımından Anayasanın 2. maddesine aykırı bulunmamış olmakla birlikte, anılan kararda, fıkranın eklendiği maddede Kurumun kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması için her türlü tedbiri alma görev ve yetkisi ile birlikte değerlendirme yapılarak kuralda belirsizlik bulunmadığı sonucuna varılmıştır (bkz. 24/7/2019 tarihli ve E.2017/16, K.2019/64 sayılı karar).

İncelenen kuralın yer aldığı 17. maddede (veya CBK'nın başka bir hükmünde) kuralın belirsizliğini giderecek ve belirlilik ilkesinin yukarıda belirtilen gereklerine uygun şekilde keyfî uygulamalara engel olacak tedbirleri de içeren açık, anlaşılır ve nesnel bir hükme ise yer verilmemiştir.

Bu sebeple, söz konusu ibarenin içerik yönünden de Anayasaya aykırı olduğu düşüncesiyle çoğunluğun red kararına karşıyım.

C. Çoğunluğun, CBK'nın 22. maddesinin (1) numaralı fıkrasındaki "...yurtdışı ve..." ibaresinin içerik yönünden incelenmesine ilişkin olarak belirttiği gerekçelere ise yukarıda (A) başlığı altında (1), (b) bölümünde açıkladığım karşıoy gerekçemdeki sebeplerle katılmamakla birlikte, kuralın içerik bakımından Anayasaya aykırı olmadığı görüşüne ve iptal talebinin reddi sonucuna, 15/10/2020 tarihli ve E.2018/124, K.2020/56 sayılı karara ilişkin farklı gerekçemdeki sebeplerle farklı gerekçeyle katılıyorum (bkz. anılan farklı gerekçenin (2) numaralı paragrafındaki açıklamalar).

Üye - M. Emin KUZ

KARŞIOY GEREKÇESİ ve FARKLI GEREKÇE

1. Anayasa Mahkemesi çoğunluğunun 23/7/2018 tarihli ve (14) numaralı İletişim Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin iki maddesinin konu bakımından yetki yönüyle iptal isteminin reddine ilişkin görüşüne katılmamaktayım. Ayrıca Cumhurbaşkanlığı Kararnamesi'nde iptali talep edilen bir ibarenin içerik yönünden Anayasa'ya aykırı olmadığına ise farklı gerekçe ile katılmaktayım. Bu konulara ilişkin hukuki dayanaklarım aşağıdaki gibidir:

A. Dava Konusu Cumhurbaşkanlığı Kararnamesi'nin 17. maddesinin (2) numaralı fıkrasının birinci cümlesinde yer alan "...gerekli gördüğü bilgileri..." ibaresinin konu bakımından yetki yönüyle iptali gerektiği şeklindeki karşıoyum ve içerik yönünden Anayasa'ya aykırı olmadığı hususundaki farklı gerekçem:

2. 23/7/2018 tarihli ve (14) numaralı İletişim Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin 17. maddesinin (2) numaralı fıkrasının birinci cümlesinde yer alan "...gerekli gördüğü bilgileri..." ibaresi ile ilgili Anayasa Mahkemesinin gerçekleştirdiği denetimde kuralın "konu bakımından yetki" yönünden incelendiği aşamada Anayasa'ya aykırı olmadığına ilişkin çoğunluk görüşüne katılmamaktayım. Bununla birlikte kuralın içerik yönünden Anayasa'ya aykırı olmadığına ilişkin çoğunluk kararına ise farklı gerekçeyle katılmaktayım.

3. Dava konusu Cumhurbaşkanlığı Kararnamesi hükmü, İletişim Başkanlığının görevleri ile ilgili olarak gerekli gördüğü bilgileri bütün kamu kurum ve kuruluşlarından ve diğer gerçek ve tüzel kişilerden doğrudan istemeye yetkili olduğu hususunu düzenlemektedir. Dolayısıyla burada görevleri ile ilgili olarak İletişim Başkanlığınca gerekli görülüp istenecek bilgilerin kişisel verileri de kapsadığı kanaatindeyim.

4. Nitekim (14) numaralı İletişim Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin 3. maddesinde sıralanan İletişim Başkanlığının görevleri arasındaki birçok maddede kişisel verilerle

doğrudan ve dolaylı olarak ilgili hususlara yer verilmektedir. Örneğin, maddenin (k) ve (l) bendlerindeki “basın-yayın kuruluşu mensuplarına basın kartı düzenlemek ve Basın Kartı Komisyonunun sekretarya faaliyetlerini yürütmek” ve “Türkiye Medya Veri Tabanını oluşturmak ve güncel kalmasını sağlamak için gerekli tedbirleri almak” görevlerinin kişisel verilerle doğrudan ilgili olduğu açıkça fark edilmektedir. Kaldı ki iptali talep edilen ibarenin yer aldığı fıkra hükmü gereğince kendilerinden bilgi istenen bütün kamu kurum ve kuruluşları ile diğer gerçek ve tüzel kişiler bu bilgileri istenilen süre içinde öncelikle ve zamanında vermekle yükümlüdürler. Dolayısıyla kurumun görevlerini yerine getirirken Anayasa’nın 20. maddesi bağlamında kişisel veri olarak görülecek hususlarla iç içe olması kaçınılmazdır.

5. Bundan dolayıdır ki dava konusu Cumhurbaşkanlığı Kararnamesi hükmünün konu bakımından yetki yönü ile Anayasa’ya uygunluğunu denetlerken bu hususu göz önünde tutarak değerlendirme yapmak gerekmektedir.

6. Bu bağlamda Anayasa Mahkemesi çoğunluğunun dava konusu kuralın Anayasa’nın 104. maddesinin onyedinci fıkrasının ilk cümlesindeki yürütme yetkisine ilişkin bir konuyu düzenlediği şeklindeki kanaate katılmaktayım. Ancak Anayasa’nın 104. maddesinin onyedinci fıkrasının ikinci cümlesi yönüyle bakıldığında ise dava konusu ibarenin kişisel verileri de kapsadığı gerekçesiyle bu cümleye aykırılık taşıdığı kanaatindeyim. Zira dava konusu ibarenin yer aldığı 17. maddenin gerek “İşbirliği ve bilgi toplama” şeklindeki başlığı ve gerekse İletişim Başkanlığının görevlerinin düzenlendiği 3. maddesindeki hükümlere bakıldığında “gerekli gördüğü bilgileri” ibaresinin kişi hakları ve ödevleri ile ilgili Anayasa’nın 20. maddesi kapsamında kişisel verileri kapsadığı sonucuna ulaşmak gerekmektedir.

7. Dolayısıyla kişisel verilerle ilgili hususları da kapsamı nedeniyle dava konusu “gerekli gördüğü bilgileri” ibaresinin Cumhurbaşkanlığı Kararnamesi ile düzenlenebilecek konulardan olmadığı anlaşılmaktadır. Bu yönü ile dava konusu ibarenin Anayasa’nın 104. maddesinin onyedinci fıkrasının ikinci cümlesinde belirtilen temel haklar ile ilgili bir konuda düzenleme yaptığından iptali gerekmektedir.

8. Bu gerekçeyle bahse konu Cumhurbaşkanlığı Kararnamesinin Anayasa’ya uygunluk denetimi bağlamında konu yönünden yetki boyutu ile çoğunluk görüşünde ulaşılan kanaate katılmamaktayım.

9. Öte yandan dava konusu kuralın içerik yönünden Anayasa’ya aykırı olmadığına ilişkin çoğunluk kararına ise farklı gerekçe ile katılmaktayım. Çoğunluk kararında dava konusu kuralın içerik yönünden Anayasa’ya uygunluk denetimi sadece Anayasa’nın 2. maddesi bağlamında yapılmış olup kuralın Anayasa’nın 20. maddesi ile ilgisi kurulmamıştır.

10. Oysa, yukarıda da ifade edildiği üzere dava konusu ibarenin kişisel verilerle ilgili olmadığı söylenemeyeceğine göre burada kuralın içerik yönünden Anayasa'ya uygunluk denetiminin yapıldığı aşamada mutlaka Anayasa'nın 20. maddesine uygunluğunun da değerlendirilmesi gerekmektedir.

11. Burada bu görüşü ifade ederken esasında bir yandan kuralın konu bakımından yetki yönü ile Cumhurbaşkanlığı Kararnamesi ile düzenlenemeyecek bir konuda düzenleme yapmış olması nedeniyle iptali gerektiğini ifade ederken, içerik yönüyle de dava konusu Cumhurbaşkanlığı Kararnamesinin Anayasa'nın 20. maddesine uygunluğunun denetimini savunmanın kendi içinde çelişkili bir durum ortaya çıkardığını fark etmemek mümkün değildir. Ancak bu biçimdeki çelişkili durumun Cumhurbaşkanlığı kararnamelerinin Anayasa'ya uygunluk denetimindeki yöntemden kaynaklanmakta olduğunu ifade etmem gerekmektedir.

12. Zira Anayasa Mahkemesince Cumhurbaşkanlığı kararnamesi ile ilgili gerçekleştirilen denetimde ilk olarak konu bakımından yetki boyutu ile bir denetim yapılmakta ve bunun sonucunda bir oylama yapıldıktan sonra eğer dava konusu Cumhurbaşkanlığı kararnamesinin bu aşamada Anayasa'ya aykırı olmadığına hükmediliyorsa bu durumda kuralın içerik yönünden Anayasa'ya uygunluk denetimi aşamasına geçilmektedir. Bu süreçte, konu bakımından yetki boyutu ile iptali gerektiği kanaatinde olursa dahi çoğunluk tarafından bu aşamada kuralın Anayasa'ya aykırı olmadığı görüşünün kabulü halinde, bu ilk aşamadaki kanaate katılmayan bir üye sonraki aşamada dava konusu Cumhurbaşkanlığı Kararnamesinin sadece içerik boyutu ile ilgili Anayasa'ya uygunluğu denetiminde yeni bir değerlendirme yapmak ve bu boyutu ile yapılan oylamada oy kullanmak durumunda kalmaktadır. İşte bu nedenle benim açımdan bu davada gerçekleştirilen Anayasa'ya uygunluk denetiminde Cumhurbaşkanlığı Kararnamesinin denetimi ile ilgili ilk bakışta çelişkilere sebebiyet verdiği izlenimi uyandıran farklı bir durum ortaya çıkmaktadır.

13. Dava konusu "gerekli gördüğü bilgileri" ibaresinin içerik yönünden Anayasa'nın 20. maddesine aykırı olmadığına ilişkin kanaatimi ise Mahkememizin (AYM, E.2017/16, K.2019/64, 24/07/2019, §§ 41-61) kararındaki gerekçeye dayandırmaktayım. Bu nedenle de dava konusu ibarenin içerik yönü ile Anayasa'ya aykırı olmadığı şeklindeki Mahkememiz çoğunluk görüşüne bu farklı gerekçe ile katılmaktayım.

B. (14) numaralı İletişim Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinin 26. maddesinin (2) numaralı fıkrasının (c) bendiyle 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete'de yayımlanan (1) numaralı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin

485. maddesinin (1) numaralı fıkrasına (i) bendinden sonra gelmek üzere eklenen (i) bendinin konu bakımından yetki yönüyle iptali gerektiği yönündeki karşıyım:

14. Dava konusu (i) bendindeki “474 üncü maddenin birinci fıkrasının (a) bendi ile bu fıkranın (i) bendinde yazılı projelerin ileri teknoloji veya yüksek maddi kaynak gerektirmesi halinde 8/6/1994 tarihli ve 3996 sayılı Bazı Yatırım ve Hizmetlerin Yap-İşlet-Devret Modeli Çerçevesinde Yapıtırılması Hakkında Kanun kapsamı da dahil yap-işlet-devret modeli çerçevesinde sermaye şirketlerinin veya yabancı şirketlerin görevlendirilmesi suretiyle yapılmasını sağlamak” şeklindeki görev bağlamında Ulaştırma ve Altyapı Bakanlığının merkez teşkilatı bünyesindeki hizmet birimlerinden biri konumunda olan Altyapı Yatırımları Genel Müdürlüğü, belirtilen projeler ile yatırım ve hizmetlerin yap-işlet-devret modeli çerçevesinde yapılmasını sağlamak bakımından sermaye şirketlerinin veya yabancı şirketlerin görevlendirilmesi hususunda görevli ve yetkili kılınmaktadır.

15. Dava konusu Cumhurbaşkanlığı Kararnamesi hükmünün Ulaştırma ve Altyapı Bakanlığının merkez teşkilatındaki bir hizmet biriminin büyük ölçekli bazı proje ve yatırım hizmetlerini düzenlemesi nedeniyle yürütme yetkisine ilişkin bir konuda olmadığını söylemek mümkün değildir. Öte yandan kuralın Cumhurbaşkanlığı kararnameleri ile düzenlenemeyecek olan Anayasa'nın 104. maddesinin on yedinci fıkrasının ikinci cümlesindeki yasak alan kapsamında kaldığı da söylenemez.

16. Bununla birlikte buradaki temel sorun on yedinci fıkranın üçüncü cümlesinde kendisini göstermektedir. Bu cümleye göre Anayasa'da münhasıran kanunla düzenlenmesi öngörülen konularda Cumhurbaşkanlığı kararnamesi çıkarılamaz. Nitekim Anayasa'nın 47. maddesinin son fıkrasında Devlet, kamu iktisadî teşebbüsleri ve diğer kamu tüzelkişileri tarafından yürütülen yatırım ve hizmetlerden hangilerinin özel hukuk sözleşmeleri ile gerçek veya tüzelkişilere yaptırılabilirliği veya devredilebileceğinin kanunla belirleneceği öngörülmektedir.

17. Bilindiği üzere Anayasa'nın 104. maddesinin on yedinci fıkrasında “yürütme yetkisine ilişkin konular”da Cumhurbaşkanlığı kararnamesi çıkarılabileceği ifade edildikten sonra özel olarak bazı Anayasa maddelerinde (Anayasa'nın 104. maddesinin dokuzuncu fıkrasında, 106. maddesinin on birinci fıkrasında, 108. maddesinin dördüncü fıkrasında ve 118. maddesinin altıncı fıkrasında) belirtilen konularda da Cumhurbaşkanlığı kararnamesi ile düzenleme yapılacağı hüküm altına alınmıştır. Dolayısıyla bunların dışında, Anayasa'da açıkça kanunla düzenleneceği öngörülen konularda Cumhurbaşkanlığı Kararnamesi ile düzenleme yapılamayacağı esası benimsenmiş olduğu dikkate alındığında dava konusu bendin Anayasa'nın 104. maddesinin on yedinci fıkrasının üçüncü cümlesi gereğince iptali gerekmektedir. Nitekim Anayasa'nın 47. maddesinde Devlet, kamu iktisadî teşebbüsleri ve diğer kamu tüzelkişileri tarafından yürütülen yatırım ve hizmetlerden hangilerinin

özel hukuk sözleşmeleri ile gerçek veya tüzelkişilere yaptırılabilceđi veya devredilebileceđinin kanunla belirleneceđi özel olarak vurgulanmaktadır.

18. Bu nedenle dava konusu (i) bendindeki hususlar Anayasa'nın 47 maddesi geređince münhasıran kanunla düzenlenmesi gerektiđinden kuralın konu bakımından yetki yönü ile Anayasa'nın 104. maddesinin on yedinci fıkrasının üçüncü cümlesine aykırılık gerekçesiyle iptal gerekir.

Üye - Yusuf Şevki HAKYEMEZ

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2018/133

Karar Sayısı: 2021/70

Karar Tarihi: 13/10/2021

RG Tarih-Sayısı: 10/12/2021-31685

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri Engin ALTAY, Özgür ÖZEL, Engin ÖZKOÇ ile birlikte 140 milletvekili

İPTAL DAVASININ KONUSU: 23/7/2018 tarihli ve (13) numaralı Strateji ve Bütçe Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin;

A. 15. maddesinin (1) numaralı fıkrasının,

B. 18. maddesinin (1) numaralı fıkrasının birinci cümlesinde yer alan "...gerekli gördüğü bilgileri..." ibaresinin,

Anayasa'nın 20., 104. ve 123. maddelerine aykırılığı ileri sürülerek iptallerine ve yürürlüklerinin durdurulmasına karar verilmesi talebidir.

I. İPTALİ İSTENEN CUMHURBAŞKANLIĞI KARARNAMESİ KURALLARI

Cumhurbaşkanlığı Kararnamesi'nin (CBK) iptali talep edilen kuralların da yer aldığı;

1. 15. maddesinin (1) numaralı fıkrası şöyledir:

"(1) Başkanlık yurtdışı teşkilatı kurmaya yetkilidir."

2. 18. maddesinin (1) numaralı fıkrası şöyledir:

"(1) Başkanlık, görevleri ile ilgili olarak gerekli gördüğü bilgileri bütün kamu kurum ve kuruluşlarından ve diğer gerçek ve tüzel kişilerden doğrudan istemeye yetkilidir. Kendilerinden bilgi istenen bütün kamu kurum ve kuruluşları ile diğer gerçek ve tüzel kişiler bu bilgileri istenilen süre içinde öncelikle ve zamanında vermekle yükümlüdürler."

II. İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Zühtü ARSLAN, Burhan ÜSTÜN, Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ,

Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Rıdvan GÜLEÇ, Recai AKYEL ve Yusuf Şevki HAKYEMEZ'in katılımlarıyla 17/10/2018 tarihinde yapılan ilk inceleme toplantısında dosyada eksiklik bulunmadığından işin esasının incelenmesine, yürürlüğü durdurma talebinin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

III. ESASIN İNCELENMESİ

2. Dava dilekçesi ve ekleri, Raportör Fatma KARAMAN ODABAŞI tarafından hazırlanan işin esasına ilişkin rapor, dava konusu CBK kuralları, dayanılan ve ilgili görülen Anayasa kuralları ile bunların gerekçeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A. Cumhurbaşkanlığı Kararnamelerinin Anayasal Çerçevesi ve Yargısal Denetimi

3. 21/1/2017 tarihli ve 6771 sayılı Türkiye Cumhuriyeti Anayasasında Değişiklik Yapılmasına Dair Kanun ile Anayasa'nın bazı maddelerinde değişiklik yapılmıştır. Yapılan değişikliklerle yeni bir hükümet sistemine geçilmiş ve buna bağlı olarak Cumhurbaşkanı'nın görev ve yetkileri yeniden düzenlenmiştir. Anayasa'nın 8. maddesinde, yürütme yetkisi ve görevinin Cumhurbaşkanı ve Bakanlar Kuruluna ait olduğu ifade edilmekte iken maddede yapılan değişiklikle Bakanlar Kurulu kaldırılarak yürütme yetkisi ve görevi tek başına Cumhurbaşkanı'na verilmiştir. Anayasa'da Bakanlar Kuruluna verilen görev ve yetkilere ilişkin maddelerde de aynı doğrultuda değişiklik yapılarak daha önce Bakanlar Kuruluna ait olan görev ve yetkilerin Cumhurbaşkanı tarafından yerine getirilmesi öngörülmüştür.

4. Yeni hükümet sisteminin en önemli özelliklerinden biri Cumhurbaşkanı'na "Cumhurbaşkanlığı Kararnamesi" adı altında düzenleme yapma yetkisinin tanınmasıdır. CBK'ların en belirgin özelliği ise Cumhurbaşkanı'na belirli konularda ilk elden düzenleme yapma yetkisinin verilmiş olmasıdır. Yürütmenin diğer düzenleyici işlemlerinden farklı olarak Cumhurbaşkanı Anayasa'da belirlenen yetki çerçevesinde herhangi bir kanuna dayanmadan ya da yasama organının onayı olmadan CBK'lar yoluyla düzenleme yapabilecektir.

5. Anayasa'nın 104. maddesinin on yedinci fıkrasının birinci cümlesinde Cumhurbaşkanı'nın yürütme yetkisine ilişkin konularda CBK çıkarabileceği hüküm altına alınmıştır. Düzenlemeyle yürütme yetkisine ilişkin olmak kaydıyla CBK çıkarma konusunda Cumhurbaşkanı'na genel bir yetki verilmiştir. Maddenin gerekçesinde, yeni hükümet sistemi gözetilerek Cumhurbaşkanı'nın genel siyasetin yürütülmesinde yürütme yetkisi ile ilgili olarak ihtiyaç duyduğu konularda

Cumhurbaşkanı'na CBK çıkarabilmesine imkân tanımak amacıyla ilk elden düzenleme yapma yetkisinin tanındığı ifade edilmiştir.

6. Cumhurbaşkanı'na yürütme yetkisine ilişkin konularda CBK çıkarma yetkisinin genel olarak verilmesinin yanı sıra Anayasa'nın diğer bazı maddelerinde belirtilen kimi konuların CBK ile düzenleneceği ayrıca ifade edilmiştir. Bu kapsamda Anayasa'nın 104. maddesinin dokuzuncu fıkrasında üst kademe kamu yöneticilerinin atanmalarına ilişkin usul ve esasların; 106. maddesinin on birinci fıkrasında bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulmasının; 108. maddesinin dördüncü fıkrasında Devlet Denetleme Kurulunun işleyişi, üyelerinin görev süresi ve diğer özlük işlerinin; 118. maddesinin altıncı fıkrasında Millî Güvenlik Kurulu Genel Sekreterliğinin teşkilatı ve görevlerinin CBK'larla düzenleneceği hüküm altına alınmıştır. Anayasa'nın 123. maddesinin üçüncü fıkrasında ise kamu tüzel kişiliğinin kanunla veya CBK ile kurulacağı belirtilmiştir.

7. Anayasa'nın 148. maddesinde CBK'ların şekil ve esas bakımdan Anayasa'ya uygunluğunun denetlenmesi öngörülmüş, yargısal denetim görev ve yetkisi de Anayasa Mahkemesine verilmiştir.

8. Anayasa'da Cumhurbaşkanı'na CBK çıkarma yetkisi verilmekle birlikte bu yetki sınırsız değildir. Kanunlardan farklı olarak Anayasa'da CBK'yla düzenlenecek konular sınırlandırılmıştır. Konu bakımından yetki yönünden getirilen bu sınırlamalar Anayasa'nın 104. maddesinin on yedinci fıkrasının ilk dört cümlesinde düzenlenmiştir.

9. Anılan fıkranın birinci cümlesinde Cumhurbaşkanı'nın yürütme yetkisine ilişkin konularda CBK çıkarabileceği ifade edilmiştir. Buna göre yürütme yetkisine ilişkin konular dışında CBK ile düzenleme yapılması mümkün değildir.

10. Fıkranın ikinci cümlesinde "Anayasa'nın ikinci kısmının birinci ve ikinci bölümlerinde yer alan temel haklar, kişi hakları ve ödevleriyle dördüncü bölümde yer alan siyasi haklar ve ödevlerin" CBK'yla düzenlenemeyeceği belirtilmiştir. Bu hüküm uyarınca belirtilen alanlarda CBK ile düzenleme yapılamaz.

11. Fıkranın üçüncü cümlesinde de Anayasa'da münhasıran kanunla düzenlenmesi öngörülen konularda CBK çıkarılmayacağı hüküm altına alınmıştır. Ancak Anayasa'da hangi konuların münhasıran kanunla düzenleneceğine ilişkin özel bir hüküm bulunmamaktadır. Bununla birlikte Anayasa Mahkemesinin yerleşik içtihadında anayasa koyucunun kanunla düzenlenmesini öngördüğü konuların bu kapsamda görülmesi gerektiği kabul edilmektedir (AYM, E.2016/150, K.2017/179, 28/12/2017, § 57; E.2016/180, K.2018/4, 18/1/2018, § 17; E.2017/51, K.2017/163, 29/11/2017, §

13; E.2016/139, K.2016/188, 14/12/2016, § 9; E.2013/47, K.2013/72, 6/6/2013). Buna göre Anayasa'da kanunla düzenleneceği belirtilen alanlarda Cumhurbaşkanı'nın CBK çıkarma yetkisi bulunmamaktadır.

12. Fıkranın dördüncü cümlesinde ise kanunda açıkça düzenlenen konularda CBK çıkarılmayacağı ifade edilmiştir. Anılan hükme göre Cumhurbaşkanı'nın yürütme yetkisine ilişkin konularda CBK çıkarabilmesi için CBK'yla düzenlenecek konunun kanunlarda açıkça düzenlenmemiş olması gerekir.

13. CBK'ların yukarıda belirtilen konu bakımından yetki kurallarına uygun olarak çıkarılması gerekmektedir. Aksi takdirde içeriği Anayasa'ya aykırılık oluşturmasa bile bu düzenlemelerin Anayasa'ya uygunluğundan söz edilemez. Dolayısıyla CBK'ların yargısal denetiminde öncelikle Anayasa'nın 104. maddesinin on yedinci fıkrasında belirtilen konu bakımından yetki kurallarına uygunluğunun ele alınması gerekir. Anılan fıkra yönünden herhangi bir aykırılık tespit edilmemesi durumunda ise bu defa CBK'ların içerik yönünden Anayasa'ya uygunluk denetimi yapılmalıdır.

B. CBK'nın 15. Maddesinin (1) Numaralı Fıkrasının İncelenmesi

1. İptal Talebinin Gerekçesi

14. Dava dilekçesinde özetle; Anayasa'da idarenin kuruluş ve görevleriyle bir bütün olduğunun ve kanunla düzenleneceğinin genel kural olarak belirlendiği, bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulmasının CBK ile düzenleneceğine ilişkin Anayasa hükmü ile genel kurala istisna getirildiği, istisna yetkinin dar yorumlanması gerekmekte olup Anayasa koyucunun açık onayı olmaksızın yetkinin genişletilemeyeceği, Anayasa'da kamu tüzel kişilerinin yurt dışı teşkilatının CBK ile düzenlenebileceğine ilişkin bir hükme yer verilmediği, buna göre CBK ile yurt dışı teşkilatı kurulmasının mümkün bulunmadığı, kuralla yurt dışı teşkilatı kurma yetkisinin Strateji ve Bütçe Başkanlığına (Başkanlık) verilerek bir yürütme işlemi ile yurt dışı teşkilatının kurulmasına imkân tanındığı belirtilerek kuralın Anayasa'nın 123. maddesine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

a. Kuralın Konu Bakımından Yetki Yönünden İncelenmesi

15. Dava dilekçesinde konu bakımından yetki yönünden kuralın Anayasa'nın 123. maddesine aykırı olduğu ileri sürülmüş ise de CBK'ya ilişkin konu bakımından yetki kuralları Anayasa'nın 104. maddesinin on yedinci fıkrasında düzenlendiğinden 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 43. maddesi uyarınca bu husustaki inceleme anılan fıkra kapsamında yapılacaktır.

16. Dava konusu kuralla Başkanlığın yurt dışı teşkilatı kurmaya yetkili olduğu hükme bağlanmıştır.
17. Kuralın Cumhurbaşkanlığına bağlı olarak CBK ile kurulan ve ayrı bir kamu tüzel kişiliği bulunmayan Başkanlığın teşkilatlanmasıyla ilgili olduğu, bu itibarla yürütme yetkisine ilişkin olduğu anlaşılmaktadır.
18. Kural, Anayasa'nın CBK ile düzenlenmesi yasaklanan İkinci Kısım Birinci ve İkinci Bölümlerinde yer alan temel haklar, kişi hakları ve ödevleriyle Dördüncü Bölümde yer alan siyasi haklar ve ödevler ile ilgili herhangi bir düzenleme de içermemektedir.
19. Anayasa'nın 104. maddesinin on yedinci fıkrasının üçüncü cümlesi uyarınca CBK'lar bakımından aranan bir diğer husus, CBK kuralının Anayasa'da münhasıran kanunla düzenlenmesi gereken konulara ilişkin olmaması gereğidir. Anayasa koyucunun bir konunun kanunla düzenlenmesini özel olarak öngörmesi bu alanın münhasıran kanunla düzenlenmesini istediği anlamına gelir. Bu kapsamda Anayasa bir konunun kanunla düzenleneceğini öngörmüşse bu konuda CBK çıkarılamaz. Bununla birlikte Anayasa'da CBK'larla düzenleneceği özel olarak öngörülen konulara ilişkin Anayasa hükümlerinin açıkça izin verdiği hususlarda CBK'larla düzenleme yapılabilir.
20. Anayasa'nın 123. maddesinin birinci fıkrasına göre "İdare, kuruluş ve görevleriyle bir bütündür ve kanunla düzenlenir." Ancak Anayasa'nın 106. maddesinin on birinci fıkrasında "Bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulması Cumhurbaşkanlığı kararnamesiyle düzenlenir." denilmek suretiyle bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulması yönünden CBK'larla düzenleme yapılmasına açıkça izin verilmiştir.
21. Bu bağlamda Anayasa'nın CBK'lar tarafından düzenleneceğini özel olarak öngördüğü bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulmasının düzenlenmesi kapsamında, bu konularla sınırlı olmak üzere Anayasa'nın 123. maddesinin anılan hükmünde belirtilen hususlarda düzenleme yapılabilir (AYM, E.2019/31, K.2020/5, 23/1/2020, § 31).
22. Anayasa Mahkemesinin önceki kararlarında belirtildiği üzere Anayasa'nın 106. maddesinin on birinci fıkrasında, bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının CBK ile düzenleneceği öngörülmüş ise de Cumhurbaşkanlığı merkez teşkilatı ile Cumhurbaşkanlığına bağlı kurum ve kuruluşlara ilişkin ayrıca bir hükme yer verilmemiştir. CBK'lar ile bakanlıkların kurulmasını, kaldırılmasını, görevleri ve yetkilerini, teşkilat yapısını düzenleyebilme yetkisini haiz Cumhurbaşkanı'nın, Cumhurbaşkanlığı merkez teşkilatı ile

Cumhurbaşkanlığına bağlı kurum ve kuruluşların da kurulması, kaldırılması, görevleri ve yetkileri ile teşkilat yapısını CBK ile düzenleyebileceğinin evleviyetle kabul edilmesi gerekir. Kaldı ki Cumhurbaşkanı'nın Anayasa'nın 106. maddesinin on birinci fıkrasına göre bakanlık bünyesinde kurarak teşkilatını düzenleyebileceği bir kurumu tercihen Cumhurbaşkanlığına bağlı kurum veya kuruluş olarak kurması hâlinde ilgili kurum ve kuruluş için Anayasa'nın 123. maddesinde belirtilen sınırlardan dolayı CBK ile düzenleme yapamayacağının kabulü Anayasa'nın genel sistematığına ve bakanlıkların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulması konusunda CBK çıkarma yetkisi tanıyan anayasal hükmün amacına aykırı olacaktır (AYM, E.2019/71, K.2020/82, 30/12/2020, § 27; E.2018/134, K.2021/13, 3/3/2021, § 30).

23. Bu itibarla kuralın ilişkin olduğu Cumhurbaşkanlığına bağlı kurum ve kuruluşların görev ve yetkisi konusunun Anayasa'nın 106. maddesinin on birinci fıkrası uyarınca CBK ile düzenlenmesi açıkça hükme bağlanmış olan bakanlıklara dair yetki kapsamında kaldığı anlaşılmaktadır. Dolayısıyla Cumhurbaşkanlığı merkez teşkilatı ile Cumhurbaşkanlığına bağlı kurum ve kuruluşların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulmasına dair düzenlemelerin CBK ile yapılması Anayasa'ya aykırılık teşkil etmemektedir (E.2019/71, K.2020/82, § 28; E.2018/134, K.2021/13, § 31).

24. Kamu kurumlarının teşkilatı, bu kurumların üstlendikleri görev ve yetkileri ifa edebilmeleri için oluşturulan ve söz konusu hizmetin yürütülmesinde doğrudan ya da dolaylı olarak rol alan, aynı kurum bünyesindeki farklı düzey ve nitelikteki birimlerin bütünü ifade etmektedir. Bu itibarla bir kurumun bu mahiyetteki merkez ve taşra teşkilatının yanı sıra yurt dışı teşkilatı da teşkilat yapısı kavramına dâhildir (AYM, E.2019/105, K.2020/30, 12/6/2020, § 21; E.2018/124, K.2020/56, 15/10/2020, § 21). Buna göre Cumhurbaşkanlığına bağlı olarak CBK ile kurulan Başkanlığın teşkilat yapısının bir parçası olan yurt dışı teşkilatını kurmak konusunda yetki veren kural Anayasa'nın 106. maddesinin on birinci fıkrası kapsamında CBK ile düzenlendiğinden kuralın Anayasa'nın 123. maddesinin birinci fıkrası bağlamında 104. maddesinin on yedinci fıkrasının üçüncü cümlesini ihlal eden bir yönü bulunmamaktadır.

25. Öte yandan kamu kurum ve kuruluşlarının yurt dışı teşkilatının kurulmasına, görevlerine, yetkilerine, idaresine ve merkezle olan ilişkilerine ilişkin esasları düzenleyen 13/12/1983 tarihli ve 189 sayılı Kamu Kurum ve Kuruluşlarının Yurtdışı Teşkilatı Hakkında Kanun Hükmünde Kararname, 2/7/2018 tarihli ve 703 sayılı Anayasada Yapılan Değişikliklere Uyum Sağlanması Amacıyla Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun Hükmünde Kararname'nin 58. maddesiyle yürürlükten kaldırılmıştır. Buna göre Başkanlığın yurt dışı teşkilatı

kurabilmesine ilişkin yürürlükte bir kanun hükmü bulunmadığı anlaşılmakta olup bu yönüyle kural kanunda açıkça düzenlenen konulara ilişkin değildir.

26. Açıklanan nedenlerle kural, Anayasa'nın 104. maddesinin on yedinci fıkrasına aykırı değildir. İptal talebinin reddi gerekir.

M. Emin KUZ bu görüşe katılmamıştır.

b. Kuralın İçerik Yönünden İncelenmesi

27. 6216 sayılı Kanun'un 43. maddesi uyarınca kural, ilgisi nedeniyle Anayasa'nın 106. maddesi yönünden incelenmiştir.

28. Anayasa'nın 106. maddesinin on birinci fıkrasında bakanlıkların kurulmasının, kaldırılmasının, görev ve yetkilerinin, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulmasının CBK ile düzenlenmesi öngörülmüştür. Anılan hüküm uyarınca Cumhurbaşkanı CBK'yla idarenin teşkilatlanması alanında Anayasa'nın temel ilkelerine ve bu alanla ilgili öngördüğü kurallarına bağlı kalmak koşuluyla bakanlıkların ve bakanlıklara dair yetki kapsamında kaldığı değerlendirilen Cumhurbaşkanlığı merkez teşkilatı ile Cumhurbaşkanlığına bağlı kurum ve kuruluşların teşkilat yapısının ne şekilde olacağını belirleme hususunda takdir yetkisine sahiptir.

29. Anayasa'nın 106. maddesinin on birinci fıkrasında bakanlıkların ve bakanlıklara dair yetki kapsamında kaldığı değerlendirilen Cumhurbaşkanlığı merkez teşkilatı ile Cumhurbaşkanlığına bağlı kurum ve kuruluşların teşkilatı kapsamında yurt dışı teşkilatı kurulması yetkisi CBK'ya tanınmış olup CBK'ya tanınan bu asli yetkinin, başka bir idari işleme bırakılması mümkün değildir.

30. Bununla birlikte yürütme organının CBK çıkarmaya yetkili olduğu konuya ilişkin her türlü ayrıntıyı CBK ile düzenlemesi ve bu düzenlemelerin gereğini bizzat yerine getirmesi gerekli olmayıp CBK ile konuya ilişkin temel kuralları belirledikten ve genel çerçeveyi çizdikten sonra bu çerçevenin içinde kalan hususları, düzenleyici nitelikteki diğer işlemlerle belirlemesi ve bu düzenlemeler kapsamında yerine getirilmesi gerekli tasarrufları da ilgili idareye bırakması mümkündür (AYM, E.2019/105, K.2020/30, 12/6/2020, § 36; E.2018/124, K.2020/56, 15/10/2020, § 25).

31. (13) numaralı CBK'da Cumhurbaşkanlığına bağlı ve ayrı bir tüzel kişiliği bulunmayan Başkanlığın kurulması, teşkilat, görev ve yetkilerine ilişkin usul ve esaslar düzenlenmiş; bu kapsamda dava konusu kuralla başkanlık yurt dışı teşkilatı kurmak konusunda yetkilendirilmiştir. (1) numaralı CBK'nın kamu kurum ve kuruluşlarının teşkilatlanmasına ilişkin diğer hükümleri ile birlikte değerlendirildiğinde kuralın, CBK ile oluşturulan söz konusu teşkilatın fiilen faaliyete geçirilmesi için gerekli idari tasarrufların Başkanlık tarafından yerine getirilmesini öngördüğü anlaşılmaktadır.

Bunun dışında kural söz konusu yurt dışı teşkilatının doğrudan düzenlenmesiyle ilgili bir yetkiyi bu kapsamda örneğin yurt dışı teşkilatının niteliği, kurulacağı yer, görevleri, yer itibarıyla görev alanı gibi konularda düzenleme yapma yetkisini Başkanlığa tanımamıştır. Kuralın anılan yetkiyi Başkanlığa bırakmadığı tüm kamu kurum ve kuruluşlarının ve Cumhurbaşkanlığının teşkilatını düzenleyen (1) numaralı CBK'nın Ortak Hükümler başlıklı bölümünde düzenlenen 510/B maddesinin başlığından ve içeriğinden açıkça anlaşılmaktadır. "Yurtdışı teşkilatı kurulma usulü" başlıklı söz konusu maddede "Yurtdışı teşkilatı kurulurken niteliği, kurulacağı yer, görevleri, yer itibarıyla görev alanı, bağlı veya ilgili olacağı misyon, konsolosluk şefliği ve geçici olanların süresi, Cumhurbaşkanı kararında belirtilir." hükmüne yer verilmiştir.

32. Buna göre (1) numaralı CBK, yurt dışı teşkilatının kurulmasına ilişkin olarak yurt dışı teşkilatının niteliği, kurulacağı yer, görevleri, yer itibarıyla görev alanı gibi temel kuralları dava konusu kuralla Başkanlığa bırakmamış, bunların düzenlenme yetkisini 510/B maddesiyle Cumhurbaşkanı kararına tanımıştır. CBK ile söz konusu hususlarda düzenleme yapma yetkisinin anayasal olarak Cumhurbaşkanı kararına bırakılıp bırakılmayacağı bu davanın konusunu oluşturmamakla birlikte bu hüküm anılan konularda doğrudan düzenleme yapma yetkisinin Başkanlığa bırakılmadığını göstermektedir. Dolayısıyla kuralla tanınan yetkinin konuya ilişkin temel kurallar ve genel çerçeve belirlenmeden yurt dışı teşkilatının kurulması veya düzenlenmesini de içerdiğinin söylenemeyeceği anlaşılmaktadır. Bu yönüyle Anayasa'nın 106. maddesinin on birinci fıkrası kapsamında CBK ile oluşturulan Başkanlığın yurt dışı teşkilatına ilişkin doğrudan düzenleme yapma yetkisini Başkanlığa bırakmayan dava konusu kuralın da anılan fıkrayı ihlal eden bir yönü bulunmamaktadır.

33. Açıklanan nedenlerle kural, Anayasa'nın 106. maddesine aykırı değildir. İptal talebinin reddi gerekir.

M. Emin KUZ bu sonuca farklı gerekçe ile katılmıştır.

C. CBK'nın 18. Maddesinin (1) Numaralı Fıkrasının Birinci Cümlesinde Yer Alan "...gerekli gördüğü bilgileri..." İbaresinin İncelenmesi

1. Genel Açıklama

34. Kişisel verilerin korunması hakkı Anayasa'nın 20. maddesi kapsamında anayasal güvenceye bağlanmış olup kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir. Buna göre veri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esaslar bu konuda kabul edilmiş genel kanun niteliğindeki 24/3/2016 tarihli ve 6698 sayılı Kişisel

Verilerin Korunması Kanunu'nda düzenlenmiş, bazı kanunlarda da kişisel verilerle ilgili hükümlere yer verilerek konuya ilişkin yasal güvencenin sağlanması amaçlanmıştır.

35. 6698 sayılı Kanun'un 3. maddesinin (e) bendinde kişisel verilerin elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem kişisel verinin işlenmesi olarak ifade edilmiştir.

36. Anılan Kanun'un 4. maddesinin (1) numaralı fıkrasında kişisel verilerin ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği belirtilmiştir. Yine Kanun'un 4. maddesinin (2) numaralı fıkrası ile 5. ve 6. maddelerinde kişisel verilerin işlenmesinde uyulması zorunlu genel ilkeler, kişisel verilerin ilgili kişinin rızasıyla veya rızaya dayalı olmaksızın işlenmesi şartları düzenlenmiş; kişisel verilerin silinmesi, yok edilmesi, anonim hâle getirilmesi şartları ise Kanun'un 7. maddesinde ayrıca belirtilmiştir. Kanun'un Üçüncü Bölüm'ü ve Beşinci Bölüm'ünde ise kişisel verileri işlenen gerçek kişiler ile kişisel verileri işleyen gerçek veya tüzel kişilerin hak ve yükümlülükleri ile Kanun hükümlerine aykırı hareket edenler yönünden uygulanacak cezai hükümlere yer verilmiştir.

37. Kural olarak kişisel verilerin kişisel verisi işlenen gerçek kişinin açık rızası olmaksızın yurt içindeki veya yurt dışındaki üçüncü kişilere aktarılması mümkün olmamakla birlikte Kanun'un 8. ve 9. maddelerinde kişinin açık rızası aranmaksızın kişisel verilerin aktarılması şartları ile buna ilişkin usul ve esaslar düzenlenmiştir. Buna göre kişisel verinin aktarıldığı gerçek veya tüzel kişinin kimliğinden bağımsız olarak kişisel verinin aktarılmasına ilişkin işlemlerin anılan maddelerde belirtilen usul ve esaslar çerçevesinde gerçekleştirilmesi zorunludur.

38. 6698 sayılı Kanun'un uygulanması bakımından genel olarak Kanun'a tabi bulunan kişiler, kurum veya kuruluşlar tek tek belirtmek suretiyle herhangi bir istisna öngörülmemiş olup yalnızca Kanun'un 28. maddesinde kişisel verinin işlenmesindeki amaç ve kapsam yönünden birtakım istisnalara yer verilmiştir. Buna göre anılan Kanun kapsamında kalan ve kişisel veriyi ilk defa elde edenler ile kişisel veriyi herhangi bir surette elinde bulunduran tüm gerçek ve tüzel kişilerin, kurum ve kuruluşlar ile bunların personelinin Kanun'da belirtilen usul ve esaslara uygun hareket etmesi gerekecektir.

2. İptal Talebinin Gerekçesi

39. Dava dilekçesinde özetle; kural kapsamında istenecek bilgiler içinde kişisel verilerin de yer almasının mümkün olduğu, kuralın kişisel verilerin korunmasına ilişkin bir düzenleme içermediği,

kişisel verilerin toplanması, işlenmesi, analizi, paylaşılması gibi faaliyetlerin kanunla düzenlenmesi gerektiği, genel çerçevesi, ilke ve esasları belirlenmeden kişiler hakkında bilgi ve veri toplamak için idareye yetki verilmesinin hukuki belirlilik ilkesine aykırı olduğu, kişisel verilerin Anayasa'nın kişi hak ve ödevlerine ilişkin İkinci Kısım İkinci Bölüm'ünde düzenlendiği, buna göre ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilecek olan kişisel verilerin korunmasına ilişkin esas ve usullerin de kanunla belirlenmesi gerektiği, temel haklar, kişi hakları ve ödevlerinin CBK ile düzenlenemeyeceği belirtilerek kuralın Anayasa'nın 20. ve 104. maddelerine aykırı olduğu ileri sürülmüştür.

3. Anayasa'ya Aykırılık Sorunu

a. Kuralın Konu Bakımından Yetki Yönünden İncelenmesi

40. Dava dilekçesinde konu bakımından yetki yönünden kuralın Anayasa'nın 20. maddesine de aykırı olduğu ileri sürülmüş ise de CBK'ya ilişkin konu bakımından yetki kuralları Anayasa'nın 104. maddesinin on yedinci fıkrasında düzenlendiğinden bu husustaki inceleme anılan fıkra kapsamında yapılacaktır.

41. CBK'nın 18. maddesinin (1) numaralı fıkrasının birinci cümlesinde Başkanlığın görevleriyle ilgili olarak gerekli gördüğü bilgileri bütün kamu kurum ve kuruluşlarından ve diğer gerçek ve tüzel kişilerden doğrudan istemeye yetkili olduğu belirtilmiş, aynı fıkranın ikinci cümlesinde ise kendilerinden bilgi istenen bütün kamu kurum ve kuruluşları ile diğer gerçek ve tüzel kişilerin bu bilgileri istenilen süre içinde öncelikle ve zamanında vermekle yükümlü oldukları öngörülmüştür. Dava konusu kural anılan fıkranın birinci cümlesinde yer alan "...gerekli gördüğü bilgileri..." ibaresidir.

42. CBK'nın 1. maddesi uyarınca Başkanlık doğrudan Cumhurbaşkanlığına bağlı, genel bütçeli bir kamu kurumu olarak kurulmuştur. 2. maddeye göre de Başkanlığın Cumhurbaşkanı tarafından belirlenen hedef, ilke ve amaçlar çerçevesinde kalkınma planı, Cumhurbaşkanlığı Programı, orta vadeli program, orta vadeli mali plan, Cumhurbaşkanlığı yıllık programı ile sektörel plan ve programların Hazine ve Maliye Bakanlığıyla birlikte müştereken hazırlanması, uygulanmasının izlenmesi, değerlendirilmesi, değiştirilmesine ilişkin iş ve işlemlerin gerçekleştirilmesi ile stratejik planlara, makroekonomik tahminlere ve stratejilere, bütçeye, harcamalara, ödeneklere, giderlere, kamu yatırım plan ve projelerine ve iktisadi alanda kalan pek çok konuya ilişkin çeşitli çalışmalar yapmak amacıyla kurulduğu anlaşılmaktadır. Buna göre Başkanlığı görevleri kapsamında gerekli gördüğü bilgileri istemeye yetkili kılan kural yürütme yetkisine ilişkin bir konuyu düzenlemektedir.

43. Başkanlığın ağırlıklı olarak plan ve programların hazırlanması, bu konuda uygulamanın takibi ve izlenmesi ile mali konulara ilişkin görev ve yetkileri dikkate alındığında gerekli olan bilgileri isteyebilmesinin görevlerini yerine getirebilmesi bakımından gerekli olduğu açıktır. Nitekim istenebilecek bilgiler Başkanlığın görevleriyle ilgili olanlar ile sınırlı tutulmuştur. Bir başka deyişle kural, Başkanlığın CBK'da belirlenen görevlerinin yerine getirilebilmesinin doğal ve zorunlu bir sonucu olarak bilgi isteme yetkisini düzenlemekte olup kişisel verilere ilişkin bir düzenleme niteliğinde değildir.

44. 6698 sayılı Kanun kapsamında yer alan ve kişisel verilere ilişkin yükümlülükler ile uyulacak usul ve esasları düzenleyen çeşitli hükümlere Genel Açıklama bölümünde yer verilmiştir (bkz. §§ 34-38). Kuralın kişisel verilerin korunmasına ilişkin mevzuat hükümlerinin uygulanmasını engelleyen, sınırlandıran, genişleten, uygulanmasına istisna getiren veya herhangi bir surette bu hükümlere temas eden bir yönü bulunmadığı gibi kişisel verilere ilişkin her türlü işlemin 6698 sayılı Kanun ile kişisel verilere ilişkin diğer kanunlarda yer alan hükümlere uygun olarak gerçekleştirileceği açıktır.

45. Bu itibarla kişisel verilere ilişkin düzenleme içermeyen ve kişisel verilerle ilgili bulunmayan kuralın Anayasa'nın İkinci Kısım Birinci ve İkinci Bölümlerinde yer alan temel haklar, kişi hakları ve ödevleriyle Dördüncü Bölüm'ünde yer alan siyasi haklar ve ödevler kapsamında bulunduğu söylenemez (benzer bir değerlendirme için bkz. AYM, E.2018/134, K.2021/13, 3/3/2021, § 23-25).

46. Daha önce ifade edildiği üzere Cumhurbaşkanlığı merkez teşkilatı ile Cumhurbaşkanlığına bağlı kurum ve kuruluşların kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ile merkez ve taşra teşkilatlarının kurulmasına dair düzenlemelerin CBK ile yapılması mümkündür (bkz. §§ 20-23). Buna göre Cumhurbaşkanlığına bağlı olarak CBK ile kurulmuş bulunan Başkanlığın görevleriyle ilgili bilgi isteme yetkisini düzenleyen kural Anayasa'nın 106. maddesinin on birinci fıkrası kapsamında CBK ile düzenlendiğinden kuralın Anayasa'nın 123. maddesinin birinci fıkrası bağlamında 104. maddesinin on yedinci fıkrasının üçüncü cümlesini ihlal eden bir yönü bulunmamaktadır.

47. Kuralın yer aldığı CBK, Başkanlığın kurulmasına, teşkilatlanmasına, görev ve yetkilerine ilişkin usul ve esasları düzenlemek amacıyla kabul edilmiştir. Buna göre ilk kez (13) numaralı CBK ile kurulmuş olan Başkanlığın bilgi toplama yetkisine yönelik kuralın kanunda açıkça düzenlenen bir konuya ilişkin olmadığı anlaşılmaktadır.

48. Açıklanan nedenlerle kural, Anayasa'nın 104. maddesinin on yedinci fıkrasına aykırı değildir. İptal talebinin reddi gerekir.

Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ ve Yusuf Şevki HAKYEMEZ bu görüşe katılmamışlardır.

b. Kuralın İçerik Yönünden İncelenmesi

49. 6216 sayılı Kanun'un 43. maddesi uyarınca kural, ilgisi nedeniyle Anayasa'nın 2. maddesi yönünden incelenmiştir.

50. Anayasa'nın 2. maddesinde belirtilen hukuk devleti; eylem ve işlemleri hukuka uygun, insan haklarına saygılı, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adil bir hukuk düzeni kurup bunu geliştirerek sürdüren, hukuki güvenliği sağlayan, Anayasa'ya aykırı durum ve tutumlardan kaçınan, hukuk kurallarıyla kendini bağlı sayan ve yargı denetimine açık olan devlettir.

51. Hukuk devletinin temel unsurlarından biri belirlilik ilkesidir. Anayasa Mahkemesinin yerleşik kararlarına göre anılan ilke, yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olmasını gerektirmektedir. Belirlilik ilkesi, hukuksal güvenlikle bağlantılı olup birey, kanundan belirli bir kesinlik içinde hangi somut eylem ve olguya hangi hukuksal yaptırımın veya sonucun bağlandığını, bunların idareye hangi müdahale yetkisini verdiğini bilmesini zorunlu kılmaktadır (AYM, E.2019/35, K.2019/53, 26/6/2019, § 15; E.2018/70, K.2019/54, 26/6/2019, § 10; E.2017/33, K.2019/20, 10/4/2019, § 31; E.2018/1, K.2018/83, 11/7/2018, § 12).

52. Anayasa Mahkemesi birçok kararında belirlilik ilkesinin yalnızca yasal belirliliği değil daha geniş anlamda hukuki belirliliği ifade ettiğini, yasal düzenlemeye dayanarak erişilebilir, bilinebilir ve öngörülebilir olma gibi niteliklere ilişkin gereklilikleri karşılama koşuluyla mahkeme içtihatları ve yürütmenin düzenleyici işlemleri ile de hukuki belirliliğin sağlanabileceğini, asıl olanın muhtemel muhataplarının mevcut şartlar altında belirli bir işlemin ne tür sonuçlar doğurabileceğini öngörmelerini mümkün kılacak bir normun varlığı olduğunu vurgulamıştır. Anılan ilkenin yürütmenin asli düzenleyici işlemi niteliğinde olan CBK'lar bakımından da geçerli olduğunda şüphe bulunmamaktadır.

53. Kuralın Başkanlığın CBK'da açıkça düzenlenmiş olan görev ve yetkilerini yerine getirebilmesi amacıyla düzenlendiği ve istenebilecek bilgilerin Başkanlığın görevleriyle ilgili ve gerekli olanlarla sınırlandırıldığı anlaşılmaktadır. Gerekli görülen bilgilerin istenmesindeki amaç, kapsam ve sınır açıkça belirlenmiş olup kuralın hem kişiler hem de idare yönünden belirli ve öngörülebilir olduğu açık olduğundan kuralda belirsizlik bulunmamaktadır.

54. Açıklanan nedenlerle kural, Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

Yusuf Şevki HAKYEMEZ bu görüşe farklı gerekçeyle katılmıştır.

Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM ve M. Emin KUZ bu görüşe katılmamışlardır.

IV. YÜRÜRLÜĞÜN DURDURULMASI TALEBİ

55. Dava dilekçesinde özetle, dava konusu kuralların uygulanması hâlinde telafisi güç veya imkânsız zararlar doğabileceği belirtilerek yürürlüklerinin durdurulmasına karar verilmesi talep edilmiştir.

23/7/2018 tarihli ve (13) numaralı Strateji ve Bütçe Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin;

A. 15. maddesinin (1) numaralı fıkrasına,

B. 18. maddesinin (1) numaralı fıkrasının birinci cümlesinde yer alan "...gerekli gördüğü bilgileri..." ibaresine,

yönelik iptal talepleri 13/10/2021 tarihli ve E.2018/133, K.2021/70 sayılı kararla reddedildiğinden bu fıkra ve ibareye ilişkin yürürlüğün durdurulması taleplerinin REDDİNE 13/10/2021 tarihinde OYBİRLİĞİYLE karar verilmiştir.

V. HÜKÜM

23/7/2018 tarihli ve (13) numaralı Strateji ve Bütçe Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin;

A. 15. maddesinin (1) numaralı fıkrasının;

1. Konu bakımından yetki yönünden Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, M. Emin KUZ'un karşıoyu ve OYÇOKLUĞUYLA,

2. İçeriği itibarıyla Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

B. 18. maddesinin (1) numaralı fıkrasının birinci cümlesinde yer alan "...gerekli gördüğü bilgileri..." ibaresinin;

1. Konu bakımından yetki yönünden Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, M. Emin KUZ ile Yusuf Şevki HAKYEMEZ'in karşıoyları ve OYÇOKLUĞUYLA,

2. İeriği itibarıyla Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM ile M. Emin KUZ'un karşıoyları ve OYÇOKLUĞUYLA, 13/10/2021 tarihinde karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili - Hasan Tahsin GÖKCAN

Başkanvekili - Kadir ÖZKAYA

Üye: Engin YILDIRIM; Hicabi DURSUN; Celal Mümtaz AKINCI; Muammer TOPAL; M. Emin KUZ; Rıdvan GÜLEÇ; Recai AKYEL; Yusuf Şevki HAKYEMEZ; Yıldız SEFERİNOĞLU; Selahaddin MENTEŞ; Basri BAĞCI; İrfan FİDAN

KARŞIOY GEREKÇESİ

1. Mahkememiz çoğunluğu tarafından (13) numaralı Strateji ve Bütçe Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin (CBK) 18. maddesinin (1) numaralı fıkrasının birinci cümlesinde yer alan "...gerekli gördüğü bilgileri..." ibaresinin Anayasa'ya aykırı olmadığına karar verilmiştir.

2. (13) numaralı CBK'nın dava konusu kuralın da içinde bulunduğu "Bilgi toplama" başlıklı 18. maddesinin birinci fıkrasının birinci cümlesi uyarınca Cumhurbaşkanlığına bağlı olan Strateji ve Bütçe Başkanlığı "görevleri ile ilgili olarak gerekli gördüğü bilgileri bütün kamu kurum ve kuruluşlarından ve diğer gerçek ve tüzel kişilerden doğrudan istemeye yetkilidir." Aynı fıkranın ikinci cümlesi de kendilerinden bilgi istenenlerin bu bilgileri süresi içinde öncelikle ve zamanında vermekle yükümlü olduklarını belirtmektedir.

3. Çoğunluk, kuralın diğer hususlar yanında, (a) kişisel verilere ilişkin düzenleme içermediği ve kişisel verilerle ilgili bulunmadığı gerekçesiyle konu bakımından yetki yönünden, (b) belirsiz olmadığı gerekçesiyle içerik yönünden Anayasa'ya aykırılık teşkil etmediği sonucuna ulaşmıştır.

4. Anayasa Mahkemesinin 3/3/2021 tarihli ve E.2018/134, K.2021/13 sayılı kararına yazdığım karşıoyda açıklanan gerekçelerle (§§ 2-31) kuralın konu bakımından yetki ve içerik yönünden Anayasa'ya aykırı olduğunu düşündüğümden çoğunluğun red kararına katılmıyorum.

Başkan -Zühtü ARSLAN

KARŞIOY GEREKÇESİ

1. Çoğunluk gerekçesinde iptal isteminin reddi gerektiği sonucuna varılan 18. maddenin (1) numaralı fıkrası şöyledir: “(1) Başkanlık, görevleri ile ilgili olarak gerekli gördüğü bilgileri bütün kamu kurum ve kuruluşlarından ve diğer gerçek ve tüzel kişilerden doğrudan istemeye yetkilidir. Kendilerinden bilgi istenen bütün kamu kurum ve kuruluşları ile diğer gerçek ve tüzel kişiler bu bilgileri istenilen süre içinde öncelikle ve zamanında vermekle yükümlüdürler.”

2. Bu düzenleme (14) Numaralı İletişim Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinin 17. maddesinin 2 numaralı fıkrasının birinci cümlesinde yer alan “...gerekli gördüğü bilgileri...” ibaresiyle benzer şekilde idareye yetki vermektedir ve kişisel verileri de kapsar niteliktedir. Anılan bu kural hakkında daha önce 2018/134 E. sayılı karara yazdığım karşıoyda ifade ettiğim gerekçelerle bu dosyada incelenen kuralın da konu bakımından Anayasanın 104. maddesinin 17/2. maddesine aykırı olduğu ve iptal edilmesi gerektiği görüşündeyim.

3. Öte yandan içerik yönünden yaptığım değerlendirmede ise kişisel verilerin temel hak güvenceleri kapsamında olması nedeniyle, başka bir kamu idaresi veya kurumu nezdinde kaydedilen kişisel verilerin transferinin istenebilmesi için gerek Anayasanın 20/3. maddesi, gerekse Anayasanın 13. maddesi uyarınca açıkça kanunla düzenlenmesi gerekmektedir. Bu yönde düzenlenecek kanunda meşru amacın ve sınırlarının da gösterilmesi gerekir. Ne var ki kuralda veri transferi için öngörülen hiçbir güvence bulunmamaktadır. Belirtilen nedenlerle incelenen kuralın içerik yönünden de anayasaya aykırı olduğu ve iptali gerektiği görüşündeyim.

Başkanvekili -Hasan Tahsin GÖKCAN

KARŞIOY GEREKÇESİ

E.2018/134, K.2021/13, KT. 3/3/2021 tarihli kararda karşıoy yazımda belirttiğim gerekçelerle dava konusu “gerekli gördüğü bilgileri” ibaresinin konu bakımından yetki yönünden Anayasa’nın 104. maddesinin on yedinci fıkrasının ikinci ve üçüncü cümlelerine, içerik yönünden de Anayasa’nın 13. ve 20. maddelerine aykırı olduğu kanaatiyle çoğunluk kararına katılmıyorum.

Üye - Engin YILDIRIM

KARŞIOY GEREKÇESİ VE FARKLI GEREKÇE

(13) numaralı Cumhurbaşkanlığı Kararnamesinin (CBK) 15. maddesinin (1) numaralı fıkrasının ve 18. maddesinin (1) numaralı fıkrasındaki "...gerekli gördüğü bilgileri..." ibaresinin konu ve içerik yönünden Anayasaya aykırı olmadığına ve iptal talebinin reddine karar verilmiştir.

1. CBK'nın 15. maddesinin (1) numaralı fıkrasının ve 18. maddesinin (1) numaralı fıkrasındaki ibarenin Anayasaya aykırılığı iddiasının konu yönünden reddine ilişkin kararların gerekçelerinde; anılan kurallarda öngörülen hususların yürütme yetkisine ilişkin konulardan olduğu, kuralların Anayasanın İkinci Kısmının Birinci ve İkinci Bölümlerinde yer alan temel haklar, kişi hakları ve ödevleriyle Dördüncü Bölümünde yer alan siyasî haklara ve ödevlere ilişkin düzenleme içermediği, Anayasanın 123. maddesinin birinci fıkrasında idarenin kuruluş ve görevlerinin kanunla düzenleneceği hükme bağlansa da, 106. maddesinin son fıkrasında bakanlıklar için öngörülen istisnanın Cumhurbaşkanlığı teşkilatı ile Cumhurbaşkanlığına bağlı kuruluşları da kapsamından dolayı Anayasanın bu hükmü uyarınca bu kuruluşların da kurulması, kaldırılması, görevleri ve yetkileri, teşkilat yapısı ve merkez ve taşra teşkilatının kurulması konularında CBK ile düzenlemeler yapılmasının Anayasaya aykırılık teşkil etmediği, ayrıca bu konuların daha önce kanunlarda açıkça düzenlenmediği belirtilerek, kuralların konu yönünden Anayasanın 104. maddesine aykırı olmadığı sonucuna ulaşılmıştır.

Bu karar da dahil olmak üzere konuya ilişkin kararlarımızın, CBK'ların anayasal çerçevesine ilişkin genel açıklamalar bölümlerinde belirtildiği üzere, 6771 sayılı Kanunla yapılan Anayasa değişikliği ile hukuk sistemimize giren CBK'ların esasları Anayasanın 104. maddesinin onyedinci fıkrasında düzenlenerek Cumhurbaşkanına yürütme yetkisine ilişkin konularda CBK ile düzenleme yapma yetkisi verilmiştir. Ancak aynı fıkranın ikinci ve üçüncü cümlelerinde; temel haklar, kişinin hakları ve ödevleri ile siyasî hakların CBK ile düzenlenemeyeceği ve Anayasada kanunla düzenlenmesi öngörülen konularda CBK çıkarılamayacağı belirtilmiştir.

a) CBK'nın 15. maddesinin, Strateji ve Bütçe Başkanlığının yurtdışı teşkilatı kurmaya yetkili olduğunu hükme bağlayan (1) numaralı fıkrası, anılan Başkanlık Anayasanın 106. maddesinin son fıkrasında geçen "bakanlık" kavramı kapsamında değerlendirilemeyeceğinden (ayrıntılı açıklama için bkz. 30/12/2020 tarihli ve E.2019/71, K.2020/82 sayılı karara ilişkin karşıoy gerekçem); ayrıca yurtdışı teşkilatının kurulması bakanlıklar için bile Anayasanın söz konusu hükmünde tahdidî olarak sayılan konular arasında yer almadığından, Anayasanın 104. maddesinin onyedinci fıkrasının üçüncü cümlesine aykırıdır (bkz. 12/6/2020 tarihli ve E. 2019/105, K. 2020/30 sayılı karara ilişkin karşıoy gerekçem).

Başka bir anlatımla, genel bütçe içinde Cumhurbaşkanlığının bağlı kuruluşu olarak CBK ile kurulan Başkanlığın Anayasanın 123. maddesine göre kanunla kurulması, görev ve yetkileri ile teşkilatının ve yurtdışı teşkilatı kurmasının da kanunla düzenlenmesi gerektiğinden, dava konusu kural Anayasada kanunla düzenlenmesi öngörülen bir konuya ilişkindir.

b) CBK'nın 18. maddesinin (1) numaralı fıkrasında, Strateji ve Bütçe Başkanlığının görevleri ile ilgili olarak gerekli gördüğü bilgileri bütün kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden doğrudan istemeye yetkili olduğu; kendilerinden bilgi istenen bütün kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin de bu bilgileri vermekle yükümlü oldukları hükme bağlanmıştır.

Öncelikle yukarıda belirtilen karşıoy gerekçelerimde ayrıntılı olarak açıklanan sebeplerle, Anayasanın 106. maddesinin son fıkrası kapsamında değerlendirilemeyecek olan mezkûr Başkanlığın görev ve yetkilerinin Anayasanın 123. maddesinin birinci fıkrasına göre kanunla düzenlenmesi gerektiğinden ve bu hususun Anayasanın 106. maddesinin son fıkrasında belirtilen istisnalar kapsamında kabul edilmesi mümkün olmadığından, incelenen hüküm Anayasanın 104. maddesinin onyedinci fıkrasının üçüncü cümlesine aykırıdır (ayrıntılı açıklama için bkz. 30/12/2020 tarihli ve E.2019/71, K.2020/82 sayılı karara ilişkin karşıoy gerekçem. Ayrıca aynı yönde açıklama için bkz. 3/3/2021 tarihli ve E.2018/134, K.2021/13 sayılı karara ilişkin karşıoy gerekçem).

Diğer taraftan, çoğunluğun red gerekçesinde kuralın kişisel verilerin korunmasına ilişkin mevzuat hükümlerinin uygulanmasını engelleyen, sınırlandıran veya uygulanmasına istisna getiren bir yönünün bulunmadığı ve her türlü işlemin kişisel verilere ilişkin kanunlara uygun olarak gerçekleştirileceği belirtilmekte ise de, Anayasanın 104. maddesinin onyedinci fıkrasının ikinci cümlesinde CBK'lar bakımından belirlenen yasak alanın Anayasanın İkinci Kısmının "Kişinin Hakları ve Ödevleri" başlıklı İkinci Bölümünde yer alan 20. maddedeki hakla ilgili -sınırlama getirmeyen- düzenlemeleri de kapsadığı ve kuralın, red gerekçesinde belirtilenin aksine kişisel verilere ilişkin bir düzenleme içerdiği açıktır.

Başka bir deyişle, kuralın, çoğunluğun belirttiği gibi bu hakkı sınırlandırmadığı ve kişisel verilerin korunmasına ilişkin 6698 sayılı Kanunun uygulanmasına istisna getirmediği kabul edilse bile, kişisel verilerle ilgili olmadığı ve bunlara ilişkin düzenleme içermediği yönündeki kabule katılmak mümkün değildir. Anayasanın 104. maddesinin onyedinci fıkrasının ikinci cümlesinde kişi hakları ile ilgili olarak öngörülen yasak alan ise "sınırlama" kavramından daha geniş olan "düzenleme" yasağına ilişkindir (aynı yönde bkz. 3/3/2021 tarihli ve E.2018/134, K.2021/13 sayılı karara ilişkin karşıoy gerekçem).

Bu nedenle, incelenen ibare, Anayasanın 104. maddesinin onyedinci fıkrasının ikinci cümlesine de aykırıdır.

Sonuç olarak, incelenen her iki kuralın da, yukarıda (a) ve (b) bölümlerinde açıklanan sebeplerle, konu bakımından yetki yönünden Anayasanın 104. maddesinin onyedinci fıkrasına aykırı olduğu ve iptali gerektiği düşüncesiyle çoğunluğun buna ilişkin red kararlarına katılmıyorum.

2. CBK'nın 18. maddesinin (1) numaralı fıkrasının birinci cümlesindeki ibarenin içerik yönünden Anayasaya aykırı olmadığına ilişkin çoğunluk gerekçesinde; kuralın Başkanlığın CBK'da açıkça düzenlenmiş olan görev ve yetkilerini yerine getirebilmesini amaçladığı ve istenebilecek bilgilerin Başkanlığın görevleriyle ilgili ve gerekli olanlarla sınırlandırıldığına anlaşıldığı, böylece bilgi isteme amacı, kapsamı ve sınırının açıkça belirlendiği, bu nedenle belirli ve öngörülebilir olduğu ve belirlilik ilkesine aykırı bir yönünün bulunmadığı belirtilerek Anayasanın 2. maddesine aykırı olmadığı sonucuna varılmıştır.

Hukuk devletinin temel unsurlarından biri olan belirlilik ilkesi, Mahkememizin yerleşik içtihadına göre, yasal düzenlemelerin herhangi bir tereddüte ve şüpheye yer vermeyecek şekilde açık, net, anlaşılır ve nesnel olmasını ve kamu otoritelerinin keyfî uygulamalarına engel olacak tedbirleri içermesini; hukukî güvenlik ilkesiyle bağlantılı olarak da, kanunda belirli bir kesinlik içinde hangi somut olgulara hangi sonuçların bağlandığının görülebilmesini zorunlu kılmaktadır (bu ilkeyle ilgili ayrıntılı açıklama için bkz. 3/6/2021 tarihli ve E.2020/9, K.2021/37 sayılı karara ilişkin karşıoy gerekçem). Kuşkusuz söz konusu ilke CBK'lar bakımından da geçerlidir.

İncelenen kuralın yer aldığı 18. maddede (veya CBK'nın başka bir hükmünde) kuralın belirsizliğini giderecek ve belirlilik ilkesinin yukarıda belirtilen gereklerine uygun şekilde keyfî uygulamalara engel olacak tedbirleri de içeren açık, anlaşılır ve nesnel bir hükme ise yer verilmemiştir.

Bu sebeple, söz konusu ibarenin içerik yönünden de Anayasanın 2. maddesine aykırı olduğu düşüncesiyle çoğunluğun red kararına karşıyım.

3. Çoğunluğun, CBK'nın 15. maddesinin (1) numaralı fıkrasının içerik yönünden incelenmesine ilişkin olarak belirttiği gerekçelere ise yukarıda (1) numaralı başlığın altında (a) bölümünde açıkladığım karşıoy gerekçemdeki sebeplerle katılmamakla birlikte, kuralın içerik bakımından Anayasaya aykırı olmadığı görüşüne ve iptal talebinin reddi sonucuna, 15/10/2020 tarihli ve E.2018/124, K.2020/56 sayılı karara ilişkin farklı gerekçemdeki sebeplerle farklı gerekçeyle katılmıyorum (bkz. anılan farklı gerekçenin (2) numaralı paragrafındaki açıklamalar).

Üye - M. Emin KUZ

KARŞIOY GEREKÇESİ ve FARKLI GEREKÇE

1. Mahkememiz çoğunluğunun 23/7/2018 tarihli ve (13) numaralı Strateji ve Bütçe Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin 18. maddesinin (1) numaralı fıkrasının birinci cümlesinde yer alan "...gerekli gördüğü bilgileri..." ibaresinin konu bakımından yetki yönüyle iptal isteminin reddine ilişkin görüşüne katılmamaktayım. Cumhurbaşkanlığı Kararnamesi'nde iptali talep edilen ibarenin içerik yönünden Anayasa'ya aykırı olmadığına ise farklı gerekçe ile katılmaktayım.

2. Bu konulara ilişkin hukuki dayanaklarım aşağıdaki gibidir:

3. 23/7/2018 tarihli ve (13) numaralı Strateji ve Bütçe Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin 18. maddesinin (1) numaralı fıkrasının birinci cümlesinde yer alan "gerekli gördüğü bilgileri" ibaresi ile ilgili Anayasa Mahkemesinin gerçekleştirdiği denetimde kuralın "konu bakımından yetki" yönünden incelendiği aşamada Anayasa'ya aykırı olmadığına kara verilmiştir.

4. Dava konusu Cumhurbaşkanlığı Kararnamesi hükmü, Strateji ve Bütçe Başkanlığının görevleri ile ilgili olarak gerekli gördüğü bilgileri bütün kamu kurum ve kuruluşlarından ve diğer gerçek ve tüzel kişilerden doğrudan istemeye yetkili olduğu hususunu düzenlemektedir. Fıkroda, kendilerinden bilgi istenen bütün kamu kurum ve kuruluşları ile diğer gerçek ve tüzel kişilerin bu bilgileri istenilen süre içerisinde öncelikle ve zamanında vermekle yükümlü oldukları da öngörülmektedir.

5. Başkanlığın görevleri ile ilgili olarak doğrudan isteyebileceği ve bütün kamu kurum ve kuruluşları ile diğer gerçek ve tüzel kişilerin istenilen süre içinde öncelikle ve zamanında vermekle yükümlü oldukları bu bilgiler arasında kuralda hiçbir ayırım yapılmamıştır.

6. Dolayısıyla dava konusu CBK hükmü ile istenilebilecek bilgiler içerisinde aynı zamanda Anayasa'nın 20. maddesi kapsamında olan kişisel verilerin de yer almakta olduğunu ifade etmek gerekir. Zira CBK hükmü kategorik biçimde, hiçbir ayırım yapmaksızın Strateji ve Bütçe Başkanlığına görevleri ile ilgili olarak tüm bilgileri doğrudan isteme yetkisi vermektedir.

7. Dava konusu kuralın Anayasa'nın 104. maddesinin on yedinci fıkrasının ilk cümlesindeki yürütme yetkisine ilişkin bir konuyu düzenlediği şeklindeki kanaate katılmaktayım. Bununla birlikte Anayasa'nın 104. maddesinin on yedinci fıkrasının ikinci cümlesi yönüyle bakıldığında dava konusu ibarenin kişisel verileri de kapsadığı için bu cümleye aykırılık taşıdığı kanaatindeyim. Zira dava konusu ibarenin yer aldığı "Bilgi toplama" başlıklı 18. maddesindeki "gerekli gördüğü bilgileri"

ibaresi kişi hakları ve ödevleri ile ilgili Anayasa'nın 20. maddesi kapsamında kişisel verileri de kapsamaktadır.

8. Kişisel verilerle ilgili hususları da kapsamı nedeniyle dava konusu "gerekli gördüğü bilgileri" ibaresinin Cumhurbaşkanlığı Kararnamesi ile düzenlenebilecek konulardan olmadığı anlaşılmaktadır. Bu yönü ile dava konusu ibarenin Anayasa'nın 104. maddesinin on yedinci fıkrasının ikinci cümlesinde belirtilen temel haklar ile ilgili bir konuda düzenleme yaptığından iptali gerekmektedir. Dava konusu ibare on yedinci fıkranın ikinci cümlesine aykırılık taşıdığından "konu bakımından yetki" yönüyle ibarenin, fıkranın üçüncü ve dördüncü cümleleri yönünden ayrıca incelenmesine gerek duyulmamıştır.

9. Bu gerekçeyle bahse konu Cumhurbaşkanlığı Kararnamesinin konu bakımından yetki boyutu ile Anayasa'ya aykırı olmadığına ilişkin çoğunluk görüşünde ulaşılan kanaate katılmamaktayım.

10. Öte yandan dava konusu kuralın içerik yönünden Anayasa'ya aykırı olmadığına ilişkin çoğunluk kararına ise farklı gerekçe ile katılmaktayım. Çoğunluk kararında dava konusu kuralın içerik yönünden Anayasa'ya uygunluk denetimi sadece Anayasa'nın 2. maddesi bağlamında yapılmış olup kuralın Anayasa'nın 20. maddesi ile ilgisi kurulmamıştır.

11. Oysa, yukarıda da ifade edildiği üzere dava konusu ibarenin kişisel verilerle ilgili olmadığı söylenemeyeceğine göre burada kuralın içerik yönünden Anayasa'ya uygunluk denetiminin yapıldığı aşamada mutlaka Anayasa'nın 20. maddesine uygunluğunun da değerlendirilmesi gerekmektedir.

12. Dava konusu "gerekli gördüğü bilgileri" ibaresinin içerik yönünden Anayasa'nın 20. maddesine aykırı olmadığına ilişkin kanaatimi ise Mahkememizin (AYM, E.2017/16, K.2019/64, 24/07/2019, §§ 43-61) kararındaki yaklaşıma dayandırmaktayım. Bu nedenle de dava konusu ibarenin içerik yönü ile Anayasa'ya aykırı olmadığı şeklindeki Mahkememiz çoğunluk görüşüne bu farklı gerekçe ile katılmaktayım.

Üye - Yusuf Şevki HAKYEMEZ

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2018/91

Karar Sayısı: 2020/10

Karar Tarihi: 19/2/2020

R.G. Tarih-Sayısı: 30/4/2020-31114

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri Engin ALTAY, Özgür ÖZEL, Engin KOÇ ile birlikte 113 milletvekili

İPTAL DAVASININ KONUSU: 1/2/2018 tarihli ve 7072 sayılı Olağanüstü Hal Kapsamında Bazı Düzenlemeler Yapılması Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun'un;

A. 5. maddesiyle 24/2/1983 tarihli ve 2802 sayılı Hâkimler ve Savcılar Kanunu'nun 9/A maddesinin beşinci fıkrasının birinci cümlesinde yer alan "...en az yetmiş puan almak kaydıyla..." ibaresinin yürürlükten kaldırılmasının,

B. 7. maddesiyle 2802 sayılı Kanun'a eklenen geçici 20. maddenin,

C. 9. maddesiyle 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu'nun 172. maddesinin değiştirilen (2) numaralı fıkrasının,

Ç. 10. maddesiyle 5271 sayılı Kanun'un 173. maddesinin değiştirilen (6) numaralı fıkrasının,

D. 15. maddesiyle 11/11/1983 tarihli ve 2954 sayılı Türkiye Radyo ve Televizyon Kanunu'nun 50. maddesinin birinci fıkrasının değiştirilen (1) bendinin yedinci cümlesinin,

E. 17. maddesiyle 15/2/2011 tarihli ve 6112 sayılı Radyo ve Televizyonların Kuruluş ve Yayın Hizmetleri Hakkında Kanun'un 8. maddesinin (1) numaralı fıkrasına eklenen (t) bendinin,

F. 18. maddesiyle 6112 sayılı Kanun'un 19. maddesine eklenen (3) numaralı fıkranın,

G. 26. maddesiyle 4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Salâhiyet Kanunu'nun ek 6. maddesine eklenen on sekizinci fıkranın,

Ğ. 75. maddesiyle 10/7/1953 tarihli ve 6132 sayılı At Yarışları Hakkında Kanun'a eklenen ek 2. maddenin birinci fıkrasının,

H. 80. maddesiyle 4/4/1988 tarihli ve 320 sayılı Milli Piyango İdaresi Genel Müdürlüğü Kuruluş ve Görevleri Hakkında Kanun Hükmünde Kararname'nin değiştirilen ek 2. maddesinin birinci cümlesinin,

I. 82. maddesiyle 22/1/1990 tarihli ve 399 sayılı Kamu İktisadi Teşebbüsleri Personel Rejiminin Düzenlenmesi ve 233 Sayılı Kanun Hükmünde Kararnamenin Bazı Maddelerinin Yürürlükten Kaldırılmasına Dair Kanun Hükmünde Kararname'nin 7. maddesinin birinci fıkrasına eklenen (f) bendinin,

İ. 83. maddesiyle 399 sayılı Kanun Hükmünde Kararname'nin 45. maddesinin birinci fıkrasına eklenen (f) bendinde yer alan "...eylem birliği içerisinde olmak,..." ibaresinin,

Anayasa'nın Başlangıç kısmı ile 2., 6., 7., 13., 15., 20., 26., 28., 36., 38., 70., 138., 139. ve 140. maddelerine aykırılığları sürülerek iptallerine ve yürürlüklerinin durdurulmasına karar verilmesi talebidir.

I. İPTALİ İSTENEN KANUN HÜKÜMLERİ

Kanun'un iptali talep edilen kuralların da yer aldığı;

1. 5. maddesi şöyledir:

"MADDE 5- 24/2/1983 tarihli ve 2802 sayılı Hâkimler ve Savcılar Kanununun 9/A maddesinin beşinci fıkrasının birinci cümlesinde yer alan "en az yetmiş puan almak kaydıyla" ibaresi ile aynı fıkranın ikinci cümlesi yürürlükten kaldırılmıştır."

2. 7. maddesiyle 2802 sayılı Kanun'a eklenen geçici 20. madde şöyledir:

"Geçici Madde 20- (Ek: 2/1/2017-KHK-680/8 md.; Aynen kabul: 1/2/2018-7072/7 md.)

Bu maddeyi ihdas eden Kanun Hükmünde Kararnameyle 9/A maddesinin beşinci fıkrasında yapılan değişiklik, bu maddenin yürürlüğe girdiği tarihten önce yapılan ve sonucu açıklanmayan yazılı sınava katılanlar bakımından da uygulanır."

3. 9. maddesiyle (2) numaralı fıkranın değiştirildiği 5271 sayılı Kanun'un 172. maddesi şöyledir:

"Kovuşturmaya yer olmadığına dair karar

Madde 172- (1) Cumhuriyet savcısı, soruşturma evresi sonunda, kamu davasının açılması için yeterli şüphe oluşturacak delil elde edilememesi veya kovuşturma olanağının bulunmaması hâllerinde kovuşturmaya yer olmadığına karar verir. Bu karar, suçtan zarar gören ile önceden ifadesi alınmış veya sorguya çekilmiş şüpheliye bildirilir. Kararda itiraz hakkı, süresi ve mercii gösterilir.

(2) (Değişik: 2/1/2017-KHK-680/10 md.; Aynen kabul: 1/2/2018-7072/9 md.)Kovuşturmaya yer olmadığına dair karar verildikten sonra kamu davasının açılması için yeterli şüphe oluşturacak yeni delil elde edilmedikçe ve bu hususta sulh ceza hâkimliğince bir karar verilmedikçe, aynı fiilden dolayı kamu davası açılmaz.

(3) (Ek: 11/4/2013-6459/19 md.) Kovuşturmaya yer olmadığına dair kararın etkin soruşturma yapılmadan verildiğinin Avrupa İnsan Hakları Mahkemesinin kesinleşmiş kararıyla tespit edilmesi veya bu karar aleyhine Avrupa İnsan Hakları Mahkemesine yapılan başvuru hakkında dostane çözüm ya da tek taraflı deklarasyon sonucunda düşme kararı verilmesi üzerine, kararın kesinleşmesinden itibaren üç ay içinde talep edilmesi hâlinde yeniden soruşturma açılır.”

4. 10. maddesiyle (6) numaralı fıkranın değiştirildiği 5271 sayılı Kanun'un 173. maddesi şöyledir:

“Cumhuriyet savcısının kararına itiraz

Madde 173- (1) Suçtan zarar gören, kovuşturmaya yer olmadığına dair kararın kendisine tebliğ edildiği tarihten itibaren onbeş gün içinde, bu kararı veren Cumhuriyet savcısının yargı çevresinde görev yaptığı ağır ceza mahkemesinin bulunduğu yerdeki sulh ceza hâkimliğine itiraz edebilir.

(2) İtiraz dilekçesinde, kamu davasının açılmasını gerektirebilecek olaylar ve deliller belirtilir.

(3) (Değişik: 18/6/2014-6545/71 md.) Sulh ceza hâkimliği, kararını vermek için soruşturmanın genişletilmesine gerek görür ise bu hususu açıkça belirtmek suretiyle, o yer Cumhuriyet başsavcılığından talepte bulunabilir; kamu davasının açılması için yeterli nedenler bulunmazsa, istemi gerekçeli olarak reddeder; itiraz edeni giderlere mahkûm eder ve dosyayı Cumhuriyet savcısına gönderir. Cumhuriyet savcısı, kararı itiraz edene ve şüpheliye bildirir.

(4) (Değişik: 25/5/2005 - 5353/26 md.) Sulh ceza hâkimliği istemi yerinde bulursa, Cumhuriyet savcısı iddianame düzenleyerek mahkemeye verir.

(5) Cumhuriyet savcısının kamu davasının açılmaması hususunda takdir yetkisini kullandığı hâllerde bu madde hükmü uygulanmaz.

(6) (Değişik: 2/1/2017-KHK-680/11 md.; Aynen kabul: 1/2/2018-7072/10 md.) İtirazın reddedilmesi halinde aynı fiilden dolayı kamu davası açılabilmesi için 172 nci maddenin ikinci fıkrası uygulanır.”

5. 15. maddesiyle 2954 sayılı Kanun'un 50. maddesinin birinci fıkrasının değiştirilen (1) bendi şöyledir:

“1) Sözleşmeli personel; Kurumda radyo-televizyon yayın, yapım, teknik ve bilişim hizmetlerini yürütmek üzere Kurumca yapılacak sınavla istihdam edilen, istihdama ve sözleşmeye ilişkin usul ve esasları Yönetim Kurulunca belirlenen yerli veya yabancı uyruklu personeldir. Bu suretle

çalıştırılacaklar, sosyal güvenlikleri bakımından 31/5/2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 4 üncü maddesinin birinci fıkrasının (a) bendi hükümlerine tabidir. Sözleşmeli personelin ücreti Genel Müdürün teklifi ve Yönetim Kurulu kararı ile tespit edilir. Kurumun yabancı dilde yayın yapan televizyon kanallarında fiilen çalışanlar hariç, sözleşmeli personelin ücretleri 657 sayılı Devlet Memurları Kanununun 4 üncü maddesinin (B) fıkrasına göre istihdam edilenlere uygulanan sözleşme ücreti tavanının dört katını geçemez ve bu ücret dışında herhangi bir ödeme yapılamaz. Bu şekilde istihdam edilecek personel sayısı 300'ü geçemez. Ancak, Kurumun yabancı dilde yayın yapan televizyon kanallarında fiilen çalıştırılmak üzere bu sayıya ilaveten 450'yi geçmemek üzere sözleşmeli personel istihdam edilebilir. Bu bentte belirtilen sözleşmeli personel sayıları Bakanlar Kurulu kararı ile artırılabilir. Yabancı uyruklular dışında kalan sözleşmeli personel yönetici kadrolarında görevlendirilebilir.”

6. 17. maddesiyle 6112 sayılı Kanun'un 8. maddesinin (1) numaralı fıkrasına eklenen (t) bendi şöyledir:

“MADDE 8- (1) Medya hizmet sağlayıcılar, yayın hizmetlerini kamusal sorumluluk anlayışıyla bu fıkroda yer alan ilkelere uygun olarak sunarlar. Yayın hizmetleri;

...

t) (Ek: 2/1/2017-KHK-680/18 md.; Aynen kabul: 1/2/2018-7072/17 md.) Terör eylemini, faillerini ve mağdurlarını terörün amaçlarına hizmet edecek sonuçlar doğuracak şekilde sunamaz.”

7. 18. maddesiyle 6112 sayılı Kanun'un 19. maddesine eklenen (3) numaralı fıkra şöyledir:

“(3) (Ek: 2/1/2017-KHK-680/19 md.; Aynen kabul: 1/2/2018-7072/18 md.) Ortakları ile yönetim kurulu başkan ve üyelerinin terör örgütlerine iltisakı yahut bunlarla irtibatı olduğu Millî İstihbarat Teşkilatı veya Emniyet Genel Müdürlüğü tarafından bildirilen medya hizmet sağlayıcı kuruluşların lisans başvuruları reddedilir.”

8. 26. maddesiyle 2559 sayılı Kanun'un ek 6. maddesine eklenen on sekizinci fıkra şöyledir:

“(Ek fıkra: 2/1/2017-KHK-680/27 md.; Aynen kabul: 1/2/2018-7072/26 md.) Polis, sanal ortamda işlenen suçlarda, yetkili Cumhuriyet başsavcılığının tespiti amacıyla, internet abonelerine ait kimlik bilgilerine ulaşmaya, sanal ortamda araştırma yapmaya yetkilidir. Erişim sağlayıcıları, yer sağlayıcıları ve içerik sağlayıcıları talep edilen bu bilgileri kolluğun bu suçlarla mücadele için oluşturduğu birimine bildirir.”

9. 75. maddesiyle 6132 sayılı Kanun'a eklenen ek 2. madde şöyledir:

“Ek Madde 2- (Ek: 2/1/2017 - KHK - 680/77 md.; Aynen kabul: 1/2/2018-7072/75 md.)

Yurt içinde at yarışları düzenleme, yurt içinde ve yurt dışında düzenlenen at yarışları üzerine yurt içinden ve yurt dışından müşterek bahis kabul etme hak ve yetkilerine ilişkin lisanslar, topluca 1/1/2018 tarihinden itibaren 49 yıl süreyle 19/8/2016 tarihli ve 6741 sayılı Türkiye Varlık Fonu Yönetimi Anonim Şirketinin Kurulması ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun hükümleri uyarınca kurulan Fona verilmiştir.

Gıda, Tarım ve Hayvancılık Bakanlığına at yarışları düzenleme amacına yönelik olarak tahsis edilmiş veya fiilen bu amaçla kullanılan taşınmazlar ile üzerlerindeki yapı ve tesisler, 49 yıl süre boyunca lisans sahibi Fonun kullanımına verilir.

Gıda, Tarım ve Hayvancılık Bakanlığı, lisans süresince yurt içinde at yarışları düzenleyemez, düzenletemez, yurt içinde ve yurt dışında düzenlenen at yarışları üzerine yurt içinden ve yurt dışından müşterek bahis kabul edemez.

Lisans konusu faaliyetlerin ilgili mevzuat hükümlerine uygun olarak yürütülmesini izlemeye ve denetlemeye Gıda, Tarım ve Hayvancılık Bakanlığı yetkilidir.”

10. 80. maddesiyle 320 sayılı Kanun Hükmünde Kararname'nin (KHK) değiştirilen ek 2. maddesi şöyledir:

“Ek Madde 2- (Ek: 1/8/2003-4971/23 md.; Değişik: 2/1/2017 - KHK - 680/82 md.; Aynen kabul: 1/2/2018-7072/80 md.)

Karşılığı nakit olmak üzere oynatılan Piyango, Hemen-Kazan, Sayısal Loto, Şans Topu, On Numara ve Süper Loto oyunları ile ilgili mevzuat çerçevesinde izin verilebilecek olan benzer şans oyunlarına ilişkin lisans, bu maddenin yürürlüğe girdiği tarihten itibaren 49 yıl süreyle 19/8/2016 tarihli ve 6741 sayılı Türkiye Varlık Fonu Yönetimi Anonim Şirketinin Kurulması ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun hükümleri uyarınca kurulan Türkiye Varlık Fonuna verilmiştir. Lisansın Türkiye Varlık Fonu tarafından üçüncü kişilere devredilmesinden sonra, İdare lisansa konu şans oyunlarını düzenleyemez ve bu oyunlar için ayrı bir lisans veremez. Lisans konusu faaliyetlerin ilgili mevzuat hükümlerine uygun olarak yürütülmesini izlemeye ve denetlemeye İdare yetkilidir.”

11. 82. maddesiyle (f) bendinin eklendiği 399 sayılı KHK'nın 7. maddesinin birinci fıkrası şöyledir:

“İşe Alınacaklarda Aranılacak Şartlar

Madde 7 - Sözleşmeli olarak işe alınacak personelin;

a) Kamu haklarından mahrum bulunmaması,

- b) 18 yaşını tamamlamış olmaları,
- c) Taksirli suçlar hariç olmak üzere, ağır hapis veya 6 aydan fazla hapis veyahut affa uğramış olsalar bile Devletin şahsiyetine karşı işlenen suçlarla, zimmet, ihtilas, irtikap, rüşvet, hırsızlık, dolandırıcılık, sahtecilik, inancı kötüye kullanma, dolanlı iflas gibi yüz kızartıcı veya şeref ve haysiyeti kırıcı suçtan veya istimal ve istihlak kaçakçılığı hariç kaçakçılık, resmi ihale ve alım satımlara fesat karıştırma, Devlet sırlarını açığa vurma suçlarından dolayı hükümlü bulunmamaları,
- d) Görevlerini yapmalarına engel olabilecek akıl hastalığı veya bedensel engel ile engelli olmamaları,
- e) En az ortaokul mezunu olmaları,
- f) (Ek: 2/1/2017-KHK-680/84 md.; Aynen kabul: 1/2/2018-7072/82 md.) Güvenlik soruşturması ve/veya arşiv araştırması yapılmış olmak,
- gerekir.”

12. 83. maddesiyle (f) bendinin eklendiği 399 sayılı KHK'nın 45. maddesinin birinci fıkrası şöyledir:

“Sözleşmenin Feshi ve Sona Ermesi

Madde 45- (İptal: Ana.Mah.'nin 4/4/1991 tarih ve E.1990/12, K.1991/7 sayılı Kararıyla; yeniden düzenleme: 5/2/1992 - 3771/8 md.) Teşebbüs veya bağlı ortaklıklarda çalışan sözleşmeli personelin sözleşmesi aşağıdaki hallerde feshedilir:

- a) İzinsiz veya kabul edilebilir bir mazereti olmaksızın kesintisiz 5 gün veya bir sözleşme dönemi içinde kesintili 10 gün göreve gelmemek,
- b) İşe alınma şartlarından herhangi birini taşımadığının anlaşılması veya bu şartlardan birinin sonradan kaybedilmesi,
- c) Görev veya görev yerinin değişmesi halinde belirlenen süre içinde mücbir bir sebep olmaksızın yeni görevine başlamamak,
- d) Bu Kanun Hükmünde Kararname ile sözleşme hükümlerine aykırı davranışlarda bulunmak,
- e) Sicil ve başarı değerlendirmeleri birbirini izleyen iki sözleşme döneminde (D) düzeyinde olmak,
- f) (Ek: 2/1/2017 - KHK - 680/85 md.; Aynen kabul: 1/2/2018-7072/83 md.) Terör örgütleriyle eylem birliği içerisinde olmak, bu örgütlere yardım etmek, kamu imkân ve kaynaklarını bu örgütleri desteklemeye yönelik kullanmak ya da kullandırmak, bu örgütlerin propagandasını yapmak,”

II. İLK İNCELEME

A. 17/5/2018 Tarihli İlk İnceleme Toplantısı

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Zühtü ARSLAN, Burhan ÜSTÜN, Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ, Nuri NECİPOĞLU, Hicabi DURSUN, M. Emin KUZ, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Rıdvan GÜLEÇ, Recai AKYEL ve Yusuf Şevki HAKYEMEZ'in katılımlarıyla 17/5/2018 tarihinde yapılan ilk inceleme toplantısında öncelikle iptali talep edilen kuralların bazılarına yönelik olarak iptal davasının açılmış sayılıp sayılmayacağı sorunu görüşülmüştür.

2. 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 38. maddesinin (6) numaralı fıkrasında "İptal davalarında, Anayasaya aykırılıkları ileri sürülen hükümlerin Anayasanın hangi maddelerine aykırı olduğunun ve gerekçelerinin belirtilmiş olması zorunludur." kuralı yer almıştır. İçtüzük'ün 45. maddesinde de "İptali istenen kurallar ve bunların her birinin Anayasanın hangi maddelerine aykırılık oluşturduğu" ve "Anayasaya aykırılıkları ileri sürülen hükümlerin her birinin Anayasanın hangi maddelerine, hangi nedenlerle aykırı olduğunun ayrı ayrı ve gerekçeleriyle birlikte açıkça gösterilmesi" hususları, dava dilekçesinde yer alması gereken konular arasında sayılmıştır.

3. 6216 sayılı Kanun'un 39. maddesinin (1) numaralı fıkrasında dava dilekçesinin, 38. maddede gösterilen şartları taşıyıp taşımadığının kayıt tarihinden itibaren on gün içinde inceleneceği, başvuru dilekçesindeki eksikliklerin varsa kararla saptanarak on beş günden az olmamak üzere verilecek süre içinde tamamlanması için ilgililere tebliğ olunacağı, aynı maddenin (3) numaralı fıkrasında ise (1) numaralı fıkrada belirtilen süre içinde eksikliklerin tamamlanmaması hâlinde Genel Kurulca iptal davasının açılmamış sayılmasına karar verileceği belirtilmiştir.

4. Yapılan incelemede dava dilekçesinin "DAVANIN KONUSU" ve "SONUÇ VE İSTEM" bölümlerinde, 7072 sayılı Kanun'un 75. maddesiyle 6132 sayılı Kanun'a eklenen ek 2. maddenin tamamının iptaline ve yürürlüğünün durdurulmasına karar verilmesi talep edilmesine rağmen "İPTALİ İSTENEN HÜKÜMLER" bölümünün (9) numaralı sırasında anılan maddenin sadece birinci fıkrasının gerekçelendirilerek iptalinin talep edildiği, dolayısıyla dava dilekçesinin sonuç bölümü ile Anayasa'ya aykırılık gerekçesinin açıklandığı bölüm arasında çelişki bulunduğu saptanmıştır.

5. Açıklanan nedenlerle 6216 sayılı Kanun'un 39. maddesinin (1) numaralı fıkrası ile İçtüzük'ün 49. maddesi uyarınca İstanbul Milletvekili Engin ALTAY, Manisa Milletvekili Özgür ÖZEL, Sakarya Milletvekili Engin ÖZKOÇ'a bildirimde bulunulmasına ve yukarıda belirtilen eksikliklerin giderilmesi için kararın tebliğinden başlayarak 15 (on beş) gün süre verilmesine OYBİRLİĞİYLE karar verilmiştir.

B. 21/6/2018 Tarihli İlk İnceleme Toplantısı

6. İtüzük hükümleri uyarınca Zühtü ARSLAN, Burhan ÜSTÜN, Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRÇÜ, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, M. Emin KUZ, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Rıdvan GÜLEÇ, Recai AKYEL ve Yusuf Şevki HAKYEMEZ'in katılımlarıyla 21/6/2018 tarihinde yapılan ilk inceleme toplantısında 4/6/2018 tarihli ek dava dilekçesinde iptal ve yürürlüğü durdurma talebinin 7072 sayılı Kanun'un 75. maddesiyle 6132 sayılı Kanun'a eklenen ek 2. maddenin birinci fıkrasıyla sınırlı olduğunun belirtildiđi, "DAVANIN KONUSU" ve "SONUÇ VE İSTEM" bölümlerinde maddenin tamamına sehven yer verildiđinin ifade edildiđi ve bu suretle Anayasa Mahkemesinin 17/5/2018 tarihli ara kararında belirtilen eksikliđin giderildiđi anlaşılmađı ile işin esasının incelenmesine, yürürlüğü durdurma talebinin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

III. ESASIN İNCELENMESİ

7. Dava dilekçesi ve ekleri, Raportör Osman KODAL tarafından hazırlanan işin esasına ilişkin rapor, dava konusu kanun hükümleri, dayanılan ve ilgili görülen Anayasa kuralları ve bunların gerekçeleri ile diđer yasama belgeleri okunup incelendikten sonra geređi görüşülüp düşünöldü:

A. Olađanüstü Hâl Düzenlemelerinin Yargısal Denetimi

8. Anayasa'nın 21/1/2017 tarihli ve 6771 sayılı Türkiye Cumhuriyeti Anayasasında Deđişiklik Yapılmasına Dair Kanun'la deđiştirilmeden önceki 148. maddesinin birinci fıkrasının üçüncü cümlesinde "...olađanüstü hallerde, sıkıyönetim ve savaş hallerinde çıkarılan kanun hükmünde kararnamelerin şekil ve esas bakımından Anayasaya aykırılıđı iddiasıyla, Anayasa Mahkemesinde dava açılmaz" hükmüne yer verilerek olađanüstü dönem KHK'ları Anayasa Mahkemesinin yargısal denetiminin dışında bırakılmıştır. Anayasa Mahkemesi 2/11/2016 tarihli ve E.2016/171, K.2016/164 sayılı kararında olađanüstü hâl KHK'larının Anayasa Mahkemesi tarafından denetlenebilmesi için bu yöndeki bir anayasal yetkinin açıkça tanınması gerektiđini ifade ederek Anayasa'nın 148. maddesinin lafzı, Anayasa koyucunun amacı ve ilgili yasama belgeleri gözönünde bulundurulduğunda olađanüstü hâl KHK'larının herhangi bir ad altında yargısal denetiminin mümkün olmadığına karar vermiştir.

9. Bununla birlikte olađanüstü hâl KHK'larının Türkiye Büyük Millet Meclisi (TBMM) tarafından onaylanarak kanunlaşması hâlinde bu kanun hükümlerinin Anayasa'ya aykırılıđı iddiasıyla Anayasa Mahkemesinde dava açılmasının önünde bir engel bulunmamaktadır. İptal davasına konu edilen 7072 sayılı Kanun, olađanüstü hâl kapsamında çıkarılan 2/1/2017 tarihli ve 680 sayılı Olađanüstü Hal Kapsamında Bazı Düzenlemeler Yapılması Hakkında Kanun Hükmünde Kararname'nin TBMM

tarafından onaylanması sonucunda yürürlüğe girmiştir. Bu itibarla dava konusu kurallar diğer kanun hükümleri gibi Anayasa Mahkemesinin denetimine tabi olmakla birlikte bu denetim yapılırken söz konusu kuralların olağanüstü hâle yönelik düzenlemeler içermesi nedeniyle öncelikle inceleme yönteminin belirlenmesi gerekir.

10. Anayasa, temel hak ve özgürlüklerin korunmasına ilişkin olarak olağan ve olağanüstü dönemler için iki ayrı hukuki rejim öngörmektedir. Olağan dönemde temel hak ve özgürlüklerin sınırlandırılması rejimi Anayasa'nın 13. maddesinde düzenlenmişken olağanüstü dönemde temel hak ve özgürlüklerin sınırlandırılması ya da kullanılmasının durdurulması rejimi Anayasa'nın 15. maddesinde düzenlenmiştir.

11. Anayasa'nın 13. maddesine göre "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlandırılabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz."

12. Anayasa'nın 15. maddesine göre ise "Savaş, seferberlik veya olağanüstü hallerde, milletlerarası hukuktan doğan yükümlülükler ihlâl edilmemek kaydıyla, durumun gerektirdiği ölçüde temel hak ve hürriyetlerin kullanılması kısmen veya tamamen durdurulabilir veya bunlar için Anayasada öngörülen güvencelere aykırı tedbirler alınabilir./ Birinci fıkrada belirlenen durumlarda da, savaş hukukuna uygun fiiller sonucu meydana gelen ölümler dışında, kişinin yaşama hakkına, maddî ve manevî varlığının bütünlüğüne dokunulamaz; kimse din, vicdan, düşünce ve kanaatlerini açıklamaya zorlanamaz ve bunlardan dolayı suçlanamaz; suç ve cezalar geçmişe yürütülemez; suçluluğu mahkeme kararı ile saptanıncaya kadar kimse suçlu sayılamaz."

13. Olağan dönemde temel hak ve özgürlüklerin sınırlandırılmasına ilişkin ölçütler Anayasa'nın 13. maddesinde yer alırken savaş, seferberlik ve olağanüstü hâllerde hak ve özgürlüklerin sınırlandırılması hatta kullanılmasının durdurulması özel olarak Anayasa'nın 15. maddesinde düzenlenmiştir. Buna göre savaş, seferberlik veya olağanüstü hâllerde temel hak ve özgürlüklerin kullanılmasının kısmen veya tamamen durdurulması ve bunlar için Anayasa'nın diğer maddelerinde öngörülen güvencelere aykırı tedbirler alınması mümkündür. Ancak Anayasa'nın 15. maddesiyle bu hususta tanınan yetki de sınırsız değildir. Anayasa'nın diğer maddelerinde öngörülen güvencelere aykırı tedbirlerin milletlerarası hukuktan doğan yükümlülükleri ihlal etmemesi ve durumun gerektirdiği ölçüde olması gerekmektedir. Ayrıca bu durumlarda dahi kişinin yaşam hakkına, maddi ve manevi varlığının bütünlüğüne dokunulması, din, vicdan, düşünce ve kanaatlerini açıklamaya

zorlanması ve bunlardan dolayı suçlanması yasaklanmış; suç ve cezaların geriye yürümemesi ilkesi ile masumiyet karinesinin bu hâllerde de geçerli olduğu kabul edilmiştir.

14. Olağanüstü hâl yönetim usullerine başvurulmasındaki temel amaç, bu yönetim rejiminin uygulanmasına neden olan tehdit veya tehlikelerin bertaraf edilmesini sağlamaktır. Devletin veya toplumun varlığının ya da kamu düzeninin ağır tehdit veya tehlikeler altında bulunması nedeniyle olağanüstü yönetim usulünün uygulandığı dönemlerde söz konusu tehdit ya da tehlikelerin bertaraf edilmesi için temel hak ve özgürlüklerin olağan döneme kıyasla daha fazla sınırlandırılması sonucunu doğuran tedbirler alınması gerekebilir. Bu nedenle Anayasa'nın 15. maddesinin uygulanabilmesi için kuralın olağanüstü hâlin gerekli kıldığı durumla ilgisinin bulunması gerekir.

15. Olağanüstü hâl KHK'larının kanunlaşmasından sonra bu kanun hükümlerinin Anayasa'ya uygunluğunun denetlenmesinde ilgili kuralın tabi olduğu sınırlama rejimi tespit edilmelidir. Zira söz konusu düzenlemelerde olağanüstü hâl ile ilgili kuralların yanında olağanüstü hâl ile ilgisi olmayan kurallara da yer verilebilmesi bu tespitin yapılmasını zorunlu kılmaktadır.

16. Kanunlaştırılarak yargısal denetime açılan bir kuralın Anayasa'nın olağanüstü dönem için öngördüğü denetim rejimine tabi olabilmesi için kural, olağanüstü hâlin ilanına sebep olan tehdit veya tehlikelerin bertaraf edilmesine yönelik olmalı ve olağanüstü hâl süresiyle sınırlı uygulanmalıdır. Dolayısıyla ancak bu iki niteliği taşıyan bir kuralın Anayasa'ya uygunluk denetiminde Anayasa'nın olağanüstü hâllerde temel hak ve özgürlüklerin kullanılmasının sınırlandırılması ve durdurulmasını düzenleyen 15. maddesi esas alınabilir.

17. Kuralın olağanüstü hâlin ilanına neden olan tehdit veya tehlikelerin bertaraf edilmesine yönelik olmadığı ya da olağanüstü hâlin süresini aştığı durumlarda ise söz konusu kuralın Anayasa'ya uygunluk denetiminde Anayasa'nın 15. maddesi dikkate alınamaz. Bu durumda kurala ilişkin inceleme sınırlamaya konu hakkın düzenlendiği Anayasa maddesi başta olmak üzere Anayasa'nın ilgili hükümleri ile olağan dönemde hak ve özgürlükleri sınırlama ve güvence rejimi bakımından temel öneme sahip olan 13. maddesi bağlamında yapılmalıdır. Ancak buradaki anayasallık denetiminde varılan sonuç böyle bir düzenlemenin olağanüstü dönemde dahi yapılamayacağı şeklinde anlaşılabilir.

18. 7072 sayılı Kanun'un 7. maddesiyle 2802 sayılı Kanun'a eklenen dava konusu geçici 20. madde hâricindeki dava konusu kuralların olağanüstü hâl süresince uygulanma özelliğini aşan bir niteliğe sahip olduğu anlaşılmaktadır. Bu durum kurallara olağanüstü hâlin dışına taşan genel düzenleme niteliği vermektedir. Bu nedenle kuralların anayasallık denetiminde Anayasa'nın olağanüstü hâllerde temel hak ve özgürlüklerin sınırlandırılması rejimini düzenleyen 15. maddesi uygulama alanı

bulamaz. Kurallara ilişkin incelemenin, sınırlama yapılan hakkın düzenlendiği Anayasa maddesi başta olmak üzere Anayasa'nın diğer ilgili hükümleri ve elbette olağan dönemde hak ve özgürlükleri sınırlama ve güvence rejimi bakımından temel öneme sahip olan 13. maddesi bağlamında yapılması gerekir.

B. Kanun'un 5. Maddesiyle 2802 Sayılı Kanun'un 9/A Maddesinin Beşinci Fıkrasının Birinci Cümlesinde Yer Alan "...en az yetmiş puan almak kaydıyla..." İbaresinin Yürürlükten Kaldırılmasının İncelenmesi

19. Kural, 20/2/2019 tarihli ve 7165 sayılı Ceza Muhakemesi Kanunu ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un 4. maddesiyle 2802 sayılı Kanun'un 9/A maddesinin beşinci fıkrasının birinci cümlesine tekrar eklenmiştir.

20. Açıklanan nedenle konusu kalmayan iptal talebi hakkında karar verilmesine yer olmadığına karar vermek gerekir.

C. Kanun'un 7. Maddesiyle 2802 Sayılı Kanun'a Eklenen Geçici 20. Maddenin İncelenmesi

1. İptal Talebinin Gerekçesi

21. Dava dilekçesinde özetle; kuralla liyakat ölçüsü çerçevesinde yazılı sınavda belirli bir puan barajını aşma koşulu aranmaksızın adayların sözlü mülakata çağrılabilmesinin mümkün hâle getirildiği, bu suretle hâkimlik ve savcılık mesleği açısından mesleki nitelik ölçütünün ve kalitesinin azaltıldığı, düzenlemenin tek amacının hâkim ve savcı açığını kapatmak olduğu, bu durumun hâkimlik ve savcılık mesleğinin saygınlığına zarar verici bir nitelik arz ettiği, bu nedenle getirilen düzenlemenin hâkimlerin bağımsızlığına da zarar verdiği belirtilerek kuralın Anayasa'nın Başlangıç kısmına, 2., 138., 139. ve 140. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

22. 6216 sayılı Kanun'un 43. maddesi uyarınca kural, ilgisi nedeniyle Anayasa'nın 70. ve 128. maddeleri yönünden de incelenmiştir.

23. Kuralla 680 sayılı KHK ile 2802 sayılı Kanun'un 9/A maddesinin beşinci fıkrasında yapılan değişikliğin anılan maddenin yürürlüğe girdiği tarihten önce yapılan ve sonucu açıklanmayan yazılı sınava katılanlar bakımından da uygulanacağı öngörülmüştür.

24. Anayasa'nın 2. maddesinde belirtilen hukuk devleti, eylem ve işlemleri hukuka uygun, insan haklarına saygılı, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adil bir hukuk düzeni

kurup bunu geliştirerek sürdüren, hukuki güvenliği sağlayan, Anayasa'ya aykırı durum ve tutumlardan kaçınan, hukuk kurallarıyla kendini bağlı sayan ve yargı denetimine açık olan devlettir.

25. Hukuk devletinin korumakla yükümlü olduğu evrensel ilkelerden biri hukuki güvenlik ilkesidir. Hukuki güvenlik ilkesi hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılan ortak değerdir.

26. Kural olarak hukuki güvenlik, kanunların geriye yürütülmemesini zorunlu kılar. Daha önce tesis edilmiş bulunan işlemlerin doğurduğu hukuki sonuçları ortadan kaldıracak şekilde yasama tasarrufunda bulunulması, hukuki güvenlik ilkesine aykırılık oluşturur. Kanunların geriye yürümezliği ilkesi uyarınca kanunlar kamu yararı ve kamu düzeninin gerektirmesi, kazanılmış hakların korunması, mali hakların iyileştirilmesi gibi istisnai durumlar dışında ilke olarak yürürlük tarihlerinden sonraki olay, işlem ve eylemlere uygulanmak üzere çıkarılır. Sonradan yürürlüğe giren kanunların geçmişe ve kesin nitelik kazanmış hukuksal durumlara etkili olmaması, hukukun genel ilkelerindedir. Ancak kanun koyucu kişilerin lehine haklar sağlayan kanuni düzenlemeleri geçmişe etkili olacak şekilde yapma konusunda takdir yetkisine sahiptir.

27. Kanunların geriye yürümesi, getirilen yeni kuralın eski kural döneminde tamamlanmış ve hukuki sonuçlarını doğurmuş hukuksal durum, ilişki ve olaylara uygulanmasıdır. Yeni kuralın eski kural yürürlükte iken başlamakla beraber henüz sonuçlanmamış hukuksal durum, ilişki ve olaylara uygulanması ise kanunların geriye yürümesi olarak nitelendirilemez.

28. Kanun koyucu tarafından; hâkim ve savcı ihtiyacını karşılamak, böylece yargı hizmetlerinin aksamasını önlemek amacıyla Kanun'un 5. maddesiyle 2802 sayılı Kanun'un "Yazılı yarışma sınavı ve mülâkatın yapılış şekli" başlıklı 9/A maddesinin beşinci fıkrasının birinci cümlesinde yer alan "...en az yetmiş puan almak kaydıyla..." ibaresi yürürlükten kaldırılmıştır. Bu düzenlemeyle yazılı sınavdan sonra hâkimlik mülakatına çağırılacak adayların belirlenmesinde en az yetmiş puan alma koşulunun aranmaması öngörülmüştür.

29. Dava konusu kuralla 680 sayılı KHK ile 2802 sayılı Kanun'un 9/A maddesinin beşinci fıkrasında yapılan değişikliğin maddenin yürürlüğe girdiği tarihten önce yapılan ve sonucu açıklanmayan yazılı sınava katılanlar bakımından da uygulanacağı öngörüldüğünden, hâkimlik sınavı yapılan ancak henüz sınav sonucu açıklanmayanlardan mülakata çağırılacak olanların belirlenmesinde, yazılı sınavdan en az yetmiş puan almak koşulu uygulanmayacaktır.

30. Dolayısıyla kuralla hâkimlik mesleğine giriş için gerekli olan yazılı sınavın yapıldığı ancak henüz sonuçların açıklanmadığı bir aşamada mülakata çağrılacak adayların belirlenmesinde yazılı sınavdan yetmiş puan alma koşulunun uygulanmamasının öngörülmesi sebebiyle henüz taraflar arasında eski kural döneminde tamamlanmış, sona ermiş bir hukuksal durumdan ve bu bağlamda kazanılmış haktan ya da kesinleşmiş işlemde söz edilemez. Bu nedenle kuralda geriye yürüme söz konusu değildir.

31. Anayasa'nın 70. maddesinde "Her Türk, kamu hizmetlerine girme hakkına sahiptir./ Hizmete alınmada, görevin gerektirdiği niteliklerden başka hiçbir ayırım gözetilemez." hükmü yer almaktadır.

32. Anayasa'nın 128. maddesinin ikinci fıkrasının birinci cümlesinde ise memurların ve diğer kamu görevlilerinin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülükleri, aylık ve ödenekleri ve diğer özlük işlerinin kanunla düzenleneceği belirtilmiştir.

33. Kamu görevlileri ile kamu yönetimleri arasındaki hizmet ilişkileri kural tasarruflarla düzenlenmektedir. Kamu personeli, belirli bir statüde, nesnel kurallara göre hizmet yürütmekte, o statünün sağladığı aylık ücret, atanma, yükselme, nakil gibi kimi öznel haklara sahip olmaktadır. Kamu hizmetine girişin ve hizmet içinde yükselmenin koşulları, statü hukukunun gereği olarak kanunlarla belirlenmektedir. Bu durum Anayasa'nın kamu hizmetine girme hakkının düzenlendiği 70. maddesi ile kamu hizmeti görevlileriyle ilgili genel ilkelerin düzenlendiği 128. maddesinden kaynaklanan bir zorunluluktur. Kanun koyucu, statü hukuku çerçevesinde yürütülen memuriyet hizmetine girme, yükselme, memuriyetin sona ermesi gibi hususlara ilişkin koşulları anayasal ilkelere uygun olarak belirleme yetkisine sahiptir. Kişilerin ise kanunlarla öngörülen bu statüye girip girmeme konusunda tercihte bulunma hakları vardır.

34. Kural, olağanüstü hâl döneminde gerçekleşen meslekten çıkarmalar nedeniyle ortaya çıkan hâkim ve savcı ihtiyacının karşılanması amacıyla mülakata çağrılacak adayların belirlenmesinde, yazılı sınavdan en az yetmiş puan alma koşulunu kaldıran değişikliğin, olağanüstü hâl döneminde yapılarak henüz sonucu açıklanmamış olan yazılı sınava katılanlara da uygulanmasını öngörmektedir. Bu itibarla kural, süreklilik arz etmeyip yazılı sınavdan en az yetmiş puan alma koşulunu kaldıran değişikliğe ilişkin geçiş dönemini düzenlemekte olup hüküm ve sonuçlarını, anılan değişikliğin yürürlüğe girdiği tarihten önce yapılmış ve sonucu açıklanmamış yazılı sınava uygulanmakla tüketmektedir.

35. Kamu görevi niteliğinde olan hâkim ve savcı adaylığına atanabilmenin koşulları 2802 sayılı Kanun'un 8. maddesinde düzenlenmiş olup yazılı yarışma sınavında başarılı olmak da kural olarak anılan koşullar arasında sayılmıştır. Yazılı yarışma sınavında başarılı olmanın şartları ise en yüksek

puandan başlamak üzere sınav ilanında belirtilen kadro sayısının iki katı fazlası arasına girebilmek ve 680 sayılı KHK'yla 2802 sayılı Kanun'un 9/A maddesinin beşinci fıkrasında yapılan değişiklik öncesi en az yetmiş puan almaktır. Anılan değişiklikle adaylığa atanmak için gerekli olan yazılı yarışma sınavından yetmiş puan alma şartının yürürlükten kaldırıldığı ve bu itibarla var olan bir şartın ortadan kaldırılmasının kamu hizmetine girme hakkının sınırlanması sonucuna yol açmadığı, sınavdan belli bir puan alma şartının adaylığa atanma koşulu olarak öngörülüp öngörülmeceği konusunda kanun koyucunun takdir yetkisinin bulunduğu gözetildiğinde hâkimlik sınavı yapılmış ancak henüz sınav sonucu açıklanmamış kişiler bakımından da en az yetmiş puan alma şartının aranmamasını düzenleyen kuralın Anayasa'ya aykırı bir yönünün bulunmadığı anlaşılmaktadır.

36. Açıklanan nedenlerle kural, Anayasa'nın 2., 70. ve 128. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

Hasan Tahsin GÖKCAN ve M. Emin KUZ bu görüşe farklı gerekçeyle katılmışlardır.

Kuralın Anayasa'nın Başlangıç kısmı ile 138., 139. ve 140. maddeleriyle ilgisi görülmemiştir.

Ç. Kanun'un 9. ve 10. Maddeleriyle 5271 Sayılı Kanun'un 172. Maddesinin Değiştirilen (2) Numaralı Fıkrası ile 173. Maddesinin Değiştirilen (6) Numaralı Fıkrasının İncelenmesi

1. İptal Talebinin Gerekçesi

37. Dava dilekçesinde özetle; kurallarla temel hak ve hürriyetlere müdahale oluşturan soruşturma aşamasındaki tedbirler konusunda karar vermesi için yetkilendirilen sulh ceza hâkimliklerine Cumhuriyet savcısının soruşturma yapma yetkilerinin devredildiği, hâlbuki iddia faaliyetinin, şartları oluştuğunda başka bir merci ya da makamın onayı olmadan yargılama aşamasına taşınmasının delillerin ortaya konulması ve tartışılması suretiyle yargılamanın yönlendirilmesine ve çelişmeliliğine imkân sağladığı, bu bağlamda söz konusu düzenlemelerin ceza muhakemesinin öngördüğü sistemle bağdaşmadığı, soruşturma evresinde sulh ceza hâkimlerine bu şekilde yetki devredilmesinin adil yargılanma hakkına aykırılık oluşturduğu belirtilerek kuralların Anayasa'nın 2., 6. ve 36. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

38. 6216 sayılı Kanun'un 43. maddesi uyarınca kurallar, ilgisi nedeniyle Anayasa'nın 40. maddesi yönünden de incelenmiştir.

39. 5271 sayılı Kanun'un 172. maddesinin Kanun'un 9. maddesiyle değiştirilen (2) numaralı fıkrasını oluşturan kuralla, kovuşturmayaya yer olmadığına dair karar verildikten sonra kamu davasının

açılması için yeterli şüphe oluşturacak yeni delil elde edilmedikçe ve bu hususta sulh ceza hâkimliğince bir karar verilmedikçe, aynı fiilden dolayı kamu davası açılmayacağı hükme bağlanmaktadır.

40. 5271 sayılı Kanun'un 173. maddesinin Kanun'un 10. maddesiyle değiştirilen (6) numaralı fıkrası olan diğer kuralla da, kovuşturmayaya yer olmadığına dair karara karşı yapılan itirazın reddedilmesi hâlinde aynı fiilden dolayı kamu davasının açılabilmesi için 5271 sayılı Kanun'un 172. maddesinin (2) numaralı fıkrasının uygulanacağı öngörülmektedir. Bu itibarla kovuşturmayaya yer olmadığına dair karara karşı yapılan itirazın reddedilmesi hâlinde aynı fiilden dolayı kamu davasının açılabilmesi, kural uyarınca yeni delilin elde edilmesi, elde edilen bu delilin kamu davasının açılması için yeterli şüphe oluşturacak derecede önemli olması ve bu hususta sulh ceza hâkimliğince bir karar verilmesi koşullarının varlığı hâlinde mümkün olacaktır.

41. Anayasa'nın 36. maddesinin birinci fıkrasında "Herkes, meşru vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir" hükmüne yer verilmiştir. Buna göre hak arama özgürlüğünün en önemli iki ögesini oluşturan iddia ve savunma haklarını kısıtlayacak, bu hakların kullanımını engelleyecek ve adil yargılanmaya engel olacak kanun hükümlerinin Anayasa'nın 36. maddesine aykırılık oluşturacağı açıktır.

42. Anayasa'nın 40. maddesinde ise Anayasa ile tanınmış hak ve özgürlükleri ihlal edilen herkesin yetkili makama geciktirilmeden başvurma imkânının sağlanmasını isteme hakkı (etkili başvuru hakkı) güvence altına alınmıştır.

43. Etkili başvuru hakkı; anayasal bir hakkının ihlal edildiğini ileri süren herkese hakkın niteliğine uygun olarak iddialarını inceletebileceği makul, erişilebilir, etkili, ihlalin gerçekleşmesini veya devam etmesini engellemeye ya da sonuçlarını ortadan kaldırmaya elverişli idari ve yargısal yollara başvuruda bulunabilme imkânının sağlanmasını teminat altına almaktadır.

44. Ceza muhakemesi hükümleri uyarınca ceza soruşturmasında kural olarak delil yetersizliği nedeniyle kovuşturmayaya yer olmadığına karar verildikten sonra aynı fiilden dolayı kamu davası açılmak üzere iddianame düzenlenmesi mümkün değildir. Ancak istisnai olarak bazı hâllerde delil yetersizliği nedeniyle kovuşturmayaya yer olmadığına karar verildikten sonra aynı fiilden dolayı soruşturma başlatılabilmesi ve kamu davası açılmak üzere iddianame düzenlenebilmesi mümkündür.

45. Kurallarda kovuşturmayaya yer olmadığına karar verildikten ve/veya anılan karara yapılan itirazın reddedilmesinden sonra kamu davasının açılabilmesi, kamu davasının açılması için yeterli şüphe oluşturacak nitelikte yeni delil elde edilmesi ve bu konuda sulh ceza hâkimliğinden karar alınması koşullarına bağlanmıştır.

46. Kuralların gerekçelerinde haklarında kovuşturmayaya yer olmadığına karar verilen kişilerle ilgili tekrar kovuşturma başlatılabilmesinin elde edilen yeni delilin kamu davası açılabilmesi için yeterli şüphe oluşturabilecek derecede önemli olması ölçütüne bağlandığı, ayrıca bu hususta sulh ceza hâkimliğince bir karar verilmesi şartının da getirildiği, böylelikle yalnızca yeni delil elde edildiği gerekçesiyle kişilerin defalarca adli soruşturma tehdidinden kurtulması ve hukuki güvenlik içinde yaşamalarının temininin amaçlandığı belirtilmiştir. Buna göre kurallarla kişilerin aynı fiilden dolayı sonradan elde edilen fakat kamu davası açılması için yeterli olmayan delil nedeniyle yeniden soruşturma geçirmelerinin ve haklarında kamu davasının açılmasının önüne geçilmesinin hedeflendiği anlaşılmaktadır.

47. Öte yandan aynı fiilden dolayı kamu davası açılması için yeterli şüphe oluşturacak yeni delilin elde edilmesi ve bu hususta sulh ceza hâkimliğince bir kararın verilmesi şartlarının aranmasının, şüphelinin haklarının korunması bakımından daha güvenceli bir durumun oluşmasına yönelik olduğu gözetildiğinde kuralların adil yargılanma hakkını sınırlayan bir yönü bulunmamaktadır.

48. Aynı fiilden dolayı kamu davası açılıp açılmayacağı konusunda sulh ceza hâkimliğince verilecek kararda hâkim, yeni elde edilen delilin diğer delillerle birlikte kamu davası açılması için yeterli şüphe oluşturup oluşturmadığını değerlendirecektir. Bu değerlendirmenin hangi makam tarafından yapılacağını belirlemek kanun koyucunun takdir yetkisi kapsamında olmakla birlikte söz konusu değerlendirmenin Cumhuriyet savcısı yerine hâkim tarafından yapılmasının suçun mağdurları olabilecek kişiler bakımından etkili başvuru hakkını sınırlayan bir husus olmadığı da açıktır.

49. Kaldı ki Türk ceza muhakemesi sisteminde ceza soruşturmasını yapmakla görevli ve yetkili kişi Cumhuriyet savcısı olmakla beraber bu durum soruşturma aşamasında Cumhuriyet savcısının sulh ceza hâkimliğinden hiçbir şekilde karar alamayacağı veya almaması gerektiği anlamına gelmemektedir. Nitekim 5271 sayılı Kanun'da soruşturmanın daha sağlıklı yürütebilmesi amacıyla sulh ceza hâkimliğinden karar alınmasına ilişkin birçok düzenleme bulunmaktadır. Kanun'un; yakalama emrini düzenleyen 98., adli kontrol kararını ve hükmedecek mercileri düzenleyen 110., arama kararını düzenleyen 119., el koyma kararını düzenleyen 127. ve iletişimin tespitini düzenleyen 135. maddeleri bu durumun örneklerini oluşturmaktadır.

50. Açıklanan nedenlerle kurallar Anayasa'nın 36. ve 40. maddelerine aykırı değildir. İptal taleplerinin reddi gerekir.

Kuralların Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüş ise de bu bağlamda belirtilen hususların Anayasa'nın 36. maddesi yönünden yapılan değerlendirmeler kapsamında ele alınmış olması nedeniyle Anayasa'nın 2. maddesi yönünden ayrıca bir inceleme yapılmasına gerek görülmemiştir.

Kuralların Anayasa'nın 6. maddesiyle ilgisi görülmemiştir.

D. Kanun'un 15. Maddesiyle 2954 Sayılı Kanun'un 50. Maddesinin Birinci Fıkrasının Değiştirilen

(ı) Bendinin Yedinci Cümlesinin İncelenmesi

51. Kuralın yer aldığı bent 2/7/2018 tarihli ve 703 sayılı Anayasada Yapılan Değişikliklere Uyum Sağlanması Amacıyla Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun Hükmünde Kararname'nin 95. maddesiyle değiştirilmiştir.

52. Açıklanan nedenle konusu kalmayan iptal talebi hakkında karar verilmesine yer olmadığına karar vermek gerekir.

E. Kanun'un 17. Maddesiyle 6112 Sayılı Kanun'un 8. Maddesinin (1) Numaralı Fıkrasına Eklenen

(t) Bendinin İncelenmesi

1. Anlam ve Kapsam

53. 6112 sayılı Kanun'un 1. maddesinde Kanun'un amacının; radyo, televizyon ve isteğe bağlı yayın hizmetlerinin düzenlenmesi ve denetlenmesi, ifade ve haber alma özgürlüğünün sağlanması, medya hizmet sağlayıcılarının idari, mali ve teknik yapıları ve yükümlülükleri ile Radyo ve Televizyon Üst Kurulunun (RTÜK) kuruluşu, teşkilâtı, görev, yetki ve sorumluluklarına ilişkin usul ve esasları belirlemek olduğu belirtilmiştir.

54. Kanun'un "Tanımlar" başlıklı 3. maddesinin (1) numaralı fıkrasının (l) bendinde medya hizmet sağlayıcı, radyo, televizyon ve isteğe bağlı yayın hizmeti içeriğinin seçiminde editoryal sorumluluğu bulunan ve bu hizmetin düzenlenme ve yayınlanma biçimine karar veren tüzel kişi olarak tanımlanmış; kuralda belirtilen yayın hizmeti de aynı fıkranın (ff) bendinde medya hizmet sağlayıcının editoryal sorumluluğu altında ve temel amacı kamuoyunu bilgilendirmek, eğlendirmek veya eğitmek üzere elektronik iletişim şebekeleri yoluyla program sunmak olan, bireysel iletişim hariç olmak üzere, televizyon yayın hizmeti, isteğe bağlı yayın hizmeti ve ticarî iletişim ile radyo yayın hizmeti olarak ifade edilmiştir.

55. Kanun'un 8. maddesinde medya hizmet sağlayıcılarının uymakla yükümlü buldukları yayın hizmeti ilkeleri düzenlenmiştir. Maddenin (1) numaralı fıkrasının (d) bendinde yayın hizmetleri "Terörü övemez ve teşvik edemez, terör örgütlerini güçlü veya haklı gösteremez, terör örgütlerinin korkutucu ve yıldırıcı özelliklerini yansıtıcı nitelikte olamaz" denilmektedir. Bu bağlamda terör örgütlerini öven ve haklı gösteren, terör olaylarını teşvik eden, terör örgütlerini güçlü ve yıldırıcı göstermek suretiyle kamuoyu üzerinde baskı oluşturma amacıyla yapılan yayınlar anılan bent kapsamında değerlendirilmektedir.

56. Öte yandan anılan fıkranın dava konusu kuralı oluşturan (t) bendinde yayın hizmetlerinin terör eylemini, faillerini ve mağdurlarını terörün amaçlarına hizmet edecek sonuçlar doğuracak şekilde sunamayacağı öngörülmüştür. Bu suretle (d) bendinde belirtilen yayın hizmeti ilkesinden bağımsız olarak terör yayınlarıyla ilgili ayrı bir yayın hizmeti ilkesi düzenlenmiştir.

57. Kuralın öngördüğü yayın hizmeti ilkesine uyulmamasının yaptırımını ise Kanun'un 32. maddesinde kademeli olarak düzenlenmiştir. Anılan maddeye göre kuralın hükme bağladığı yayın hizmeti ilkesine aykırı yayın yapan medya hizmet sağlayıcı kuruluşlara, ihlalin ağırlığı ve yayının ortamı ile alanı gözönünde bulundurularak ihlalin tespit edildiği aydan bir önceki aydaki brüt ticari iletişim gelirin yüzde ikisinden beşine kadar idari para cezası verilir. İdari para cezası miktarı, radyo kuruluşları için bin TL'den, televizyon kuruluşları ve isteğe bağlı medya hizmet sağlayıcıları için onbin TL'den az olamaz. Ayrıca idari tedbir olarak ihlale konu programın yayınının beş kereye kadar durdurulmasına, isteğe bağlı yayın hizmetlerinde ihlale konu programın katalogdan çıkarılmasına karar verilir. İhlalin mahiyeti gözönünde bulundurularak idari para cezası ile birlikte idari tedbire karar verilebileceği gibi, sadece idari para cezasına veya tedbire de karar verilebilir. Kanun'un 8. maddesinin (1) numaralı fıkrasının, kuralın oluşturduğu (t) bendinin yanı sıra (a), (b) ve (d) bentleri dışındaki bentlerini, aynı maddenin (2) numaralı fıkrasını ve Kanun'un yayın hizmetlerinde ticari iletişimi düzenleyen hükümlerinden herhangi birini yaptırım kararının tebliğinden itibaren bir yıl içinde yirmiden fazla ihlal eden medya hizmet sağlayıcı kuruluşun yayını beş güne kadar durdurulur. Bir yıl içinde aynı ihlalin tekrarı hâlinde, medya hizmet sağlayıcı kuruluşun yayınının beş günden on güne kadar durdurulmasına; ihlalin ikinci tekrarı hâlinde ise yayın lisansının iptaline karar verilir.

2. İptal Talebinin Gerekçesi

58. Dava dilekçesinde özetle; kuralla radyo ve televizyon yayınlarının terör eylemini, faillerini ve mağdurlarını terörün amaçlarına hizmet edecek sonuçlar doğuracak şekilde sunamayacağı öngörülmek suretiyle Anayasa'da güvence altına alınan ifade ve basın özgürlüğü haklarına sınırlama

getirildiği, kuralda yer alan “...terörün amaçlarına hizmet edecek sonuçlar doğuracak şekilde sunamaz” ibaresinin belirsiz olduğu, müdahaleye izin veren kanunların ancak içeriğinin belirli ve anlamının öngörülebilir olması durumunda kendisinden beklenen faydayı sağlayabileceği, temel haklara müdahaleye izin veren kuralın içeriğinin muğlak ve tanınan yetkinin kapsamının belirsiz olması nedeniyle kuralla getirilen sınırlamanın ölçülü olmadığı, ülkede bir terör eyleminin meydana gelmesi hâlinde medyanın görevinin olay hakkında halkı bilgilendirmek olduğu, bu durumun da basın özgürlüğünün ve halkın haber alma hakkının doğal sonucu olduğu belirtilerek kuralın Anayasa’nın 2., 13., 26. ve 28. maddelerine aykırı olduğu ileri sürülmüştür.

3. Anayasa’ya Aykırılık Sorunu

59. Anayasa’nın 26. maddesinin birinci fıkrasında “Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir” denilmek suretiyle temel hak ve özgürlükler arasında yer alan ifade özgürlüğü güvence altına alınmıştır. Maddenin ikinci fıkrasında ise bu özgürlüğü sınırlama sebeplerine yer verilerek bu hakkın mutlak olmadığı ve maddede belirtilen nedenlerle sınırlanabileceği kabul edilmiştir.

60. Basın özgürlüğünü düzenleyen Anayasa’nın 28. maddesinde de basının hür olduğu, sansür edilemeyeceği, devletin, basın ve haber alma hürriyetlerini sağlayacak tedbirleri alacağı ve basın hürriyetinin sınırlanmasında 26. ve 27. madde hükümlerinin uygulanacağı belirtilmiştir. Buna göre ifade ve basın özgürlüğü ancak millî güvenlik, kamu düzeni, kamu güvenliği ve maddede belirtilen diğer nedenlerle sınırlandırılabilir.

61. Kural, yayın hizmetlerinin terör eylemini, faillerini ve mağdurlarını terörün amaçlarına hizmet edecek sonuçlar doğuracak şekilde sunulamayacağını öngörmek suretiyle ifade ve basın özgürlüğünü sınırlamaktadır.

62. Anayasa’nın 13. maddesinde “Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.” denilmiştir. Buna göre ifade ve basın özgürlüğüne sınırlama getiren düzenlemelerin kanunla yapılması, Anayasa’da öngörülen sınırlama sebebine uygun olması, demokratik toplum düzeninin gereklerine uygun ve ölçülü olması gerekir.

63. Bu kapsamda ifade ve basın özgürlüğünü sınırlamaya yönelik bir kanuni düzenlemenin şeklen var olması yeterli olmayıp yasal kuralların keyfiliğe izin vermeyecek şekilde belirli, ulaşılabilir ve öngörülebilir düzenlemeler niteliğinde olması gerekir.

64. Esasen temel hakları sınırlayan kanunun bu niteliklere sahip olması, Anayasa'nın 2. maddesinde güvenceye alınan hukuk devleti ilkesinin de bir gereğidir. Hukuk devletinde, kanuni düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfî uygulamalarına karşı koruyucu önlem içermesi gerekir. Kanunda bulunması gereken bu nitelikler hukuki güvenliğin sağlanması bakımından da zorunludur. Zira bu ilke hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar (AYM, E.2015/41, K.2017/98, 4/5/2017, §§ 153, 154). Dolayısıyla Anayasa'nın 13. maddesinde sınırlama ölçütü olarak belirtilen kanunilik, Anayasa'nın 2. maddesinde güvenceye alınan hukuk devleti ilkesi ışığında yorumlanmalıdır.

65. Yayın hizmetlerinin terör eylemini, faillerini ve mağdurlarını terörün amaçlarına hizmet edecek sonuçlar doğuracak şekilde sunamayacağını öngören kuralla genel bir çerçeve çizilmiş olmakla birlikte kuralın belirsiz ve öngörülemez nitelikte olduğu söylenemez. Kuralda yer alan terör kavramının tanımı 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu'nun 1. maddesinde yapılmış olmakla birlikte belirli bir anlamı ihtiva eden diğer kavramlarla beraber kuralın hukuki niteliği ve objektif anlamı yargı içtihatlarıyla belirlenebilecek durumdadır.

66. Diğer yandan yayın hizmetlerini terör eylemini, faillerini ve mağdurlarını terörün amaçlarına hizmet edecek sonuçlar doğuracak şekilde sunma, farklı şekillerde ortaya çıkabileceğinden bunların kanun koyucu tarafından önceden belirlenmesi ve kanunda tek tek sayılması zorunluluğundan söz edilemez. Zira kanunların genel ve soyut olması; somut olayın özelliğine göre değişebilecek tüm çözümleri kuralın bünyesinde barındırma, bir başka ifadeyle kuralın amaca uygun sonuca ulaştıracak herhangi bir çözümü dışlamasını önleme ihtiyacından kaynaklanmaktadır. Bu itibarla kuralda temel hak ve özgürlüklerin kanunla sınırlanması gerektiğine ilişkin anayasal ilkeye aykırı bir yön bulunmamaktadır.

67. 3713 sayılı Kanun'un "Terörün tanımı" başlıklı 1. maddesinde terör; cebir ve şiddet kullanarak, baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasa'da belirtilen Cumhuriyetin niteliklerini, siyasi, hukuki, sosyal, laik, ekonomik düzeni değiştirmek, devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemler

olarak tanımlanmıştır. Bu itibarla terör eylemlerinin millî güvenliği ve devletin ülkesi ve milletiyle bölünmez bütünlüğünü hedef aldığı gözetildiğinde yayın hizmetlerinin terör eylemini, faillerini ve mağdurlarını terörün amaçlarına hizmet edecek sonuçlar doğuracak şekilde sunulamayacağını hükme bağlayan kuralla getirilen sınırlamanın Anayasa'nın 26. maddesinin ikinci fıkrasında belirtilen sınırlama sebeplerine uygun olarak öngörüldüğü anlaşılmaktadır.

68. Anayasa'nın 13. maddesi uyarınca demokrasinin işleyişi açısından yaşamsal önemde olan temel hak ve özgürlüklere getirilen sınırlamaların demokratik toplum düzeninin gereklerine uygun olması gerekir. İfade ve basın özgürlüğünün de demokrasinin işleyişi açısından önemi açıktır. Bu çerçevede anılan özgürlüklere getirilen sınırlamanın demokratik toplum düzeninin gereklerine uygun olması, bir başka ifadeyle zorunlu bir toplumsal ihtiyacı karşılaması gerekir.

69. Terörün, millî güvenliği, devletin ülkesi ve milletiyle bölünmez bütünlüğünü tehdit ettiği, boyutları, kullandığı yöntemler ile yayın organlarının kitlelere ulaşmada sağladığı kolaylık ve toplum üzerindeki etkinliği dikkate alındığında, medya hizmet sağlayıcıları tarafından gerçekleştirilen yayın hizmetlerinin terör eylemini, faillerini ve mağdurlarını terörün amaçlarına hizmet edecek sonuçlar doğuracak şekilde sunamayacaklarını öngören kuralla getirilen sınırlamanın demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmadığı söylenemez.

70. Anayasa'nın 13. maddesinde güvence altına alınan ölçülülük ilkesi ise elverişlilik, gereklilik ve orantılılık olmak üzere üç alt ilkeden oluşmaktadır. Elverişlilik öngörülen sınırlamanın ulaşılmak istenen amacı gerçekleştirmeye elverişli olmasını, gereklilik ulaşılmak istenen amaç bakımından sınırlamanın zorunlu olmasını diğer bir ifadeyle aynı amaca daha hafif bir sınırlama ile ulaşılmamasının mümkün olmamasını, orantılılık ise hakka getirilen sınırlama ile ulaşılmak istenen amaç arasında makul bir dengenin gözetilmesi gerekliliğini ifade etmektedir.

71. Kuralın yayın hizmetlerinin terör eylemini, faillerini ve mağdurlarını terörün amaçlarına hizmet edecek sonuçlar doğuracak şekilde sunamayacağını öngörmesiyle radyo, televizyon ve isteğe bağlı yayın hizmetlerinin gerçeğe uygun, doğru ve tarafsız biçimde yerine getirilmesine, söz konusu hizmetlere ilişkin güvenilirliğin sağlanmasına, yayın organlarının kitlelere ulaşmada sağladığı kolaylık ve toplum üzerindeki etkinliğin kötüye kullanımının önlenmesine hizmet etmek suretiyle radyo, televizyon ve isteğe bağlı yayın hizmetlerinin sağlıklı biçimde işleyişine katkıda bulunmayı hedeflediği anlaşılmaktadır. Bu itibarla kuralın millî güvenliğin ve devletin ülkesi ve milletiyle bölünmez bütünlüğünün korunmasına yönelik amaçlara ulaşma bakımından elverişli ve gerekli olmadığı söylenemez.

72. Kuralla getirilen sınırlamayla kişilerin terör olaylarıyla ilgili bilgilendirilme hakkı ortadan kaldırılmamakta, söz konusu olayların terörün amaçlarına hizmet edecek sonuçlar doğuracak biçimde sunulması yasaklanarak anılan konuya ilişkin yayınlarda kişilerin gerçeğe uygun ve doğru bir biçimde bilgilendirilmesi amaçlanmaktadır. Böylece yayın yoluyla bir şekilde terör eyleminin, faillerinin ve mağdurlarının terörün amaçlarına hizmet edecek şekilde sunulmasının engellenmek istendiği anlaşılmaktadır. Kuralın uygulanmasından doğacak uyuşmazlıkların ise yargıya taşınabilmesi mümkündür. Bu kapsamda kural yargı yoluna başvurma güvencesi bakımından herhangi bir sınırlama getirmediğinden kural nedeniyle yaptırıma maruz kalan medya hizmet sağlayıcı kuruluşlarının kuralın öngördüğü koşulun gerçekleşmediği, bir başka deyişle yayın hizmetlerinin terör eylemini, faillerini ve mağdurlarını terörün amaçlarına hizmet edecek sonuçlar doğuracak şekilde sunmadığı iddiasıyla yargı yoluna başvurmalarında ve yargı yerlerince haklı bulunmaları hâlinde yaptırımın iptal edilmesinde bir engel bulunmamaktadır.

73. Buna göre Kanun'da kuralın amacı dışında keyfi olarak kullanılmasını önleyecek yasal güvenceye yer verildiğinden kuralla ulaşılmak istenen amaca ilişkin kamu yararı ile ifade ve basın özgürlüğü arasında bulunması gereken makul dengenin gözetildiği anlaşılmaktadır. Bu itibarla ifade ve basın özgürlüğünü sınırlayan kuralın orantısız bir müdahaleye de neden olmadığı, dolayısıyla anılan haklara ölçüsüz bir sınırlama getirmediği sonucuna ulaşılmıştır.

74. Açıklanan nedenlerle kural Anayasa'nın 13., 26. ve 28. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

Kuralın Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüş ise de bu bağlamda belirtilen hususların Anayasa'nın 13. maddesi yönünden yapılan değerlendirmeler kapsamında ele alınmış olması nedeniyle Anayasa'nın 2. maddesi yönünden ayrıca bir inceleme yapılmasına gerek görülmemiştir.

F. Kanun'un 18. Maddesiyle 6112 Sayılı Kanun'un 19. Maddesine Eklenen (3) Numaralı Fıkranın İncelenmesi

1. İptal Talebinin Gerekçesi

75. Dava dilekçesinde özetle; kuralla ortakları ile yönetim kurulu başkan ve üyelerinin terör örgütlerine iltisakı yahut bunlarla irtibatı olduğu Millî İstihbarat Teşkilatı veya Emniyet Genel Müdürlüğü tarafından bildirilen medya hizmet sağlayıcı kuruluşların lisans başvurularının reddedileceği öngörülmek suretiyle Anayasa'da güvence altına alınan ifade ve basın özgürlüğüne sınırlama getirildiği, kuralda belirtilen irtibat ve iltisak kavramlarının belirsiz olduğu, müdahaleye

izin veren kanunların ancak içeriğinin belirli ve anlamının öngörülebilir olması durumunda kendisinden beklenen faydayı sağlayabileceği, temel haklara müdahaleye izin veren kuralın içeriğinin muğlak ve tanınan yetkinin kapsamının belirsiz olması nedeniyle kuralla getirilen sınırlamanın ölçülü olmadığı, kuralda Millî İstihbarat Teşkilatı veya Emniyet Genel Müdürlüğünün bu belirlemeyi hangi usul ve esaslara göre yapacağını düzenlenmediği, hiçbir usule ilişkin güvence içermemesi nedeniyle keyfî uygulamalara sebebiyet verebileceği belirtilerek kuralın Anayasa'nın 2., 13., 26. ve 28. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

76. Kuralla ortakları ile yönetim kurulu başkan ve üyelerinin terör örgütlerine iltisakı yahut bunlarla irtibatı olduğu Millî İstihbarat Teşkilatı veya Emniyet Genel Müdürlüğü tarafından bildirilen medya hizmet sağlayıcı kuruluşların lisans başvurularının reddedileceği hükme bağlanmıştır.

77. 6112 sayılı Kanun'un 3. maddesinin (1) numaralı fıkrasının (hh) bendinde yayın lisansının, medya hizmet sağlayıcı kuruluşlara, bu Kanun ve bu Kanun'a dayanılarak çıkarılan yönetmelik ve diğer düzenlemelerde belirtilen şartları haiz oldukları takdirde kablo, uydu, karasal ve benzeri ortamlardan her türlü teknoloji ile yayın yapabilmeleri için her bir yayın türü, tekniği ve ortamına ilişkin olarak ayrı ayrı olmak üzere RTÜK'çe verilen izin belgesini ifade ettiği belirtilmiştir.

78. Ortakları ile yönetim kurulu başkan ve üyelerinin terör örgütlerine iltisakı yahut bunlarla irtibatı olduğu Millî İstihbarat Teşkilatı veya Emniyet Genel Müdürlüğü tarafından bildirilen medya hizmet sağlayıcı kuruluşların lisans başvurularının reddedileceğini öngörmekle kural, ifade ve basın özgürlüğünü sınırlamaktadır.

79. Anayasa'nın 13. maddesi uyarınca ifade ve basın özgürlüğüne sınırlama getiren düzenlemelerin kanunla yapılması, Anayasa'da öngörülen sınırlama sebebine uygun ve ölçülü olması gerekir.

80. Buna göre ifade ve basın özgürlüğüne sınırlama getiren düzenlemenin öncelikle kanunilik ölçütünü karşılaması, dolayısıyla belirli ve öngörülebilir nitelikte olması gerekir. Kuralda geçen iltisaklı kavramı kavuşan, bitişen, birleşen; irtibatlı kavramı ise bağlantılı anlamına gelmektedir. Anılan ibareler genel kavram niteliğinde olmakla birlikte Anayasa Mahkemesinin 14/11/2019 tarihli ve E.2018/89, K.2019/84 sayılı kararında belirtilen nedenlerle bunların kategorik olarak belirsiz ve öngörülemez nitelikte olduğu söylenemez.

81. Anayasa'nın 26. ve 28. maddelerinde ifade ve basın özgürlüğü güvence altına alınmış olup 26. maddenin ikinci fıkrasında anılan özgürlüklerin millî güvenlik, kamu düzeni, kamu güvenliği ve fıkra da belirtilen diğer nedenlerle sınırlanabileceği belirtilmiştir. Terör eylemlerinin millî güvenliği

ve devletin ülkesi ve milletiyle bölünmez bütünlüğünü hedef aldığı gözetildiğinde terör örgütlerine iltisakı yahut bunlarla irtibatı olan ortaklar ile yönetim kurulu başkan ve üyelerinden oluşan medya hizmet sağlayıcı kuruluşların lisans başvurularının reddedileceğini hükme bağlayan kuralla getirilen sınırlamanın Anayasa'nın 26. maddesinin ikinci fıkrasında belirtilen sınırlama sebeplerine uygun olarak öngörüldüğü, dolayısıyla anayasal olarak meşru bir sınırlama sebebine dayandığı görülmektedir.

82. Diğer yandan kuralın; ortakları ile yönetim kurulu başkan ve üyelerinin terör örgütlerine iltisakı yahut bunlarla irtibatı olduğu Millî İstihbarat Teşkilatı veya Emniyet Genel Müdürlüğü tarafından bildirilen medya hizmet sağlayıcı kuruluşların lisans başvurularının reddedileceğini öngörmesiyle radyo, televizyon ve isteğe bağlı yayın hizmetlerinin gerçeğe uygun, doğru ve tarafsız biçimde yerine getirilmesine, söz konusu hizmetlere ilişkin güvenilirliğin sağlanmasına, yayın organlarının kitlelere ulaşmada sağladığı kolaylık ve toplum üzerindeki etkinliğin kötüye kullanımının önlenmesine hizmet etmek suretiyle radyo, televizyon ve isteğe bağlı yayın hizmetlerinin sağlıklı biçimde işleyişine katkıda bulunmayı hedeflediği anlaşılmaktadır. Bu itibarla kuralın millî güvenliğin ve devletin ülkesi ve milletiyle bölünmez bütünlüğünün korunmasına yönelik amaçlara ulaşma bakımından elverişli ve gerekli olmadığı da söylenemez.

83. Bununla birlikte kural, ortakları ile yönetim kurulu başkan ve üyelerinin terör örgütlerine iltisakı yahut bunlarla irtibatlı olma bakımından Millî İstihbarat Teşkilatı ve Emniyet Genel Müdürlüğü tarafından yapılan bildirim esas almakta; bu yönde bir bildirim yapılması hâlinde medya hizmet sağlayıcı kuruluşların lisans başvurularının otomatik olarak reddedilmesi sonucunu doğurmaktadır. Medya hizmet sağlayıcı kuruluşlar hakkında ortaya çıkan bu sonuç belli bir süreyle de sınırlı değildir. Ayrıca kuralın, bu konuda yapılacak yargısal denetimin de etkinliğini sınırlayabilecek şekilde düzenlendiği ve yargısal süreçte idari işlem denetlenirken lisans başvurusunda bulunan medya hizmet sağlayıcı kuruluşun ortakları ile yönetim kurulu başkan ve üyelerinin terör örgütlerine iltisakı yahut bunlarla irtibatı olduğu konusunda ilgili kolluk biriminin bildirimini bulunup bulunmadığının tespitiyle sınırlı bir denetim yetkisi verdiği anlaşılmaktadır.

84. Millî İstihbarat Teşkilatı ve Emniyet Genel Müdürlüğü tarafından yapılan bildirim kural olarak ceza soruşturmasına esas alınabilecek nitelikte bilgi ve belgelere dayanma zorunluluğu bulunmamaktadır. Diğer bir ifadeyle bu kapsamdaki değerlendirmeye esas alınan olay ve olguların istihbari nitelikte olması kuvvetle muhtemeldir. Bu nedenle lisans başvurularını değerlendiren idare tarafından tesis edilecek işlemlerle ilgili yargısal denetim daha da önemli hâle gelmektedir. Ceza soruşturmasına esas alınabilecek nitelikte bilgi ve belgelere dayanma zorunluluğu olmayan güvenlik

kurumlarınca yapılacak deęerlendirmenin otomatik sonu doęurması, idareye ve idari iřlemi denetleyecek mahkemelere medya hizmet saęlayıcı kuruluřun ortakları ile ynetim kurulu bařkan ve yelerinin terr rgtlerine iltisakı yahut bunlarla irtibatı bulunup bulunmadığı hususunda deęerlendirme yapma yetkisinin verilmemesi, sz konusu bildirimlerin doęruluęunu denetleme ve gerek duruma gre idari iřlem tesis etme imkânını nemli lde sınırlamaktadır. Kanun'da anılan yetkinin kuralın getiriliř amacına uygun olarak kullanılmasını saęlayacak ve bu konudaki olası keyfilikleri nleyecek yasal gvencelere de yer verilmedięi grlmektedir.

85. Lisans bařvurularını deęerlendiren idare ile bu iřlemleri denetleyecek mahkemelere kural olarak deęerlendirme yapma imkânı vermeyen dzenlemenin yukarıda belirtilen sonuları dikkate alındığında ifade ve basın zgrlęne ynelik orantısız bir sınırlama getirdięi sonucuna varılmıřtır (benzer ynde bkz. AYM, E.2018/90, K.2019/85, 14/11/2019).

86. Bu erevede kuralın olaęan dnemde Anayasa'ya aykırı olduęu ynnde yapılan tespit, kuralın olaęanst dnemde Anayasa'ya aykırı olup olmadığı hususunda herhangi bir deęerlendirmeyi kapsamamaktadır.

87. Aıklanan nedenlerle kural Anayasa'nın 13., 26. ve 28. maddelerine aykırıdır. İptali gerekir.

Kural Anayasa'nın 13., 26. ve 28. maddelerine aykırı grlerek iptal edildięinden Anayasa'nın 2. maddesi ynnden ayrıca incelenmemiřtir.

G. Kanun'un 26. Maddesiyle 2559 Sayılı Kanun'un Ek 6. Maddesine Eklenen On Sekizinci Fıkranın İncelenmesi

1. İptal Talebinin Gerekesi

88. Dava dilekesinde zetle; kuralla sanal ortamda iřlenen sular bakımından soruřturma, arařtırma, inceleme yapma yetkisinin doęrudan adli kolluk grevlilerine bırakıldıęı, sz konusu dzenleme nedeniyle polisin sanal ortamda iřlenen sular ynnden yetkili Cumhuriyet bařsavcılıęının tespiti amacıyla internet abonelerinin kimlik bilgilerine ulařabileceęi, sanal ortamda arařtırma yapabileceęi, bu incelemenin hukuki nitelięi itibarıyla adli bir iřlem olduęu ve adli soruřturmanın bařlatılmasını gerektirdięi, ceza muhakemesi sisteminde soruřturmayı bařlatmaya ve soruřturma iřlemlerini yapmaya yetkili tek kiřinin Cumhuriyet savcısı olduęu, adli kolluęun ise Cumhuriyet savcısının emir ve talimatlarını yerine getirmekle grevli olduęu, bu baęlamda getirilen dzenlemenin ceza muhakemesi sistemiyle baędařmadığı, internet abonelerinin kimlik ve dięer bilgi ve verilerinin doęrudan doęruya polisin takdiri kapsamında incelemeye ve arařtırmaya tabi tutulmasının bireyin zel hayatının gizlilięine, kiřisel verilerin dokunulmazlıęına ynelik lsz bir mdahale

oluşturduğu, hukuk devletinin hak ve özgürlükleri koruyucu niteliğini zedelediği belirtilerek kuralın Anayasa'nın 2., 13.,15. ve 20. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

89. Kuralda polisin, sanal ortamda işlenen suçlarda, yetkili Cumhuriyet başsavcılığının tespiti amacıyla internet abonelerine ait kimlik bilgilerine ulaşmaya, sanal ortamda araştırma yapmaya yetkili olduğu, erişim sağlayıcıları, yer sağlayıcıları ve içerik sağlayıcılarının talep edilen bu bilgileri kolluğun bu suçlarla mücadele için oluşturduğu birimine bildireceği hükme bağlanmıştır.

90. Anayasa'nın 20. maddesinin birinci fıkrasında herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş; üçüncü fıkrasında da "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." denilerek kişisel verilerin korunması özel hayatın gizliliğinin korunması kapsamında güvenceye kavuşturulmuştur.

91. Kişisel verilerin korunmasını isteme hakkı, insan onurunun korunması ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilere müdahaleler sırasında korumayı amaçlamaktadır.

92. Anayasa Mahkemesinin yerleşik kararlarında da belirtildiği üzere "...adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler..." kişisel veri olarak kabul edilmektedir (AYM, E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2014/74, K.2014/201, 25/12/2014; E.2014/180, K.2015/30, 19/3/2015; E.2015/32, K.2015/102, 12/11/2015).

93. Bu bağlamda internet abonelerine ait kimlik bilgileri kişisel veri niteliğindedir. Kural, polise sanal ortamda araştırma yapma yetkisi kapsamında kişisel veri niteliğindeki internet abonelerine ait kimlik bilgilerinin polis tarafından elde edilmesine imkân tanınması ve bu yöndeki bilgilerin erişim, yer ve

içerik sağlayıcıları tarafından kolluğa bildirilmesinin zorunlu olduğunu öngörmesi sebebiyle özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkına sınırlama getirmektedir.

94. Anayasa'nın 20. maddesi uyarınca kişisel veriler ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir. Anayasa'nın 13. maddesinde de "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz." hükmüne yer verilmiştir.

95. Anayasa'nın 13. ve 20. maddeleri uyarınca kişisel verilerin korunmasını isteme hakkını sınırlamaya yönelik kanuni bir düzenlemenin şeklen var olması yeterli olmayıp yasal kuralların keyfiliğe izin vermeyecek şekilde belirli ve öngörülebilir düzenlemeler niteliğinde olması gerekir.

96. Polisin ulaşmaya yetkili olduğu ve erişim, yer ve içerik sağlayıcılarının da bildirmekle yükümlü oldukları kişisel veri niteliğindeki bilgi kuralda açıkça belirlenmiş olup anılan bilgi internet abonelerine ait kimlik bilgilerinden ibarettir. Bir başka deyişle internet abonelerine ait kimlik bilgileri dışındaki bir bilginin polis tarafından talep edilebilmesi veya erişim, yer ve içerik sağlayıcılarının başkaca bir bilgiyi bildirmekle yükümlü olduklarının ileri sürülebilmesi kural uyarınca mümkün değildir.

97. Ayrıca kişisel veri niteliğindeki bilginin ne zaman ve hangi amaçla talep edilebileceği veya ilgililer tarafından bildirileceği hususu da kuralda belirtilmiştir. Buna göre polisin internet abonelerine ait kimlik bilgilerine ulaşmaya yetkili olması her şeyden önce sanal ortamda işlemiş bir suçun varlığına bağlıdır. Diğer bir anlatımla sanal ortamda işlenmiş bir suçun olmadığı durumlarda söz konusu bilgilerin polis tarafından talep edilebilmesi veya ilgililerin bildirimde bulunması söz konusu olmayacaktır. Sanal ortamda işlenmiş bir suçun varlığı hâlinde dahi polis, yalnızca yetkili Cumhuriyet başsavcılığının tespiti amacıyla internet abonelerine ait kimlik bilgilerini talep edebilecek ve ilgililer de bu takdirde söz konusu bilgileri bildirmekle yükümlü olacaklardır. Dolayısıyla bu kapsamda elde edilen bilgiler de yalnızca yetkili Cumhuriyet başsavcılığının tespiti amacıyla kullanılabilir. Anılan açıklamalar gözönünde bulundurulduğunda kuralın belirli ve öngörülebilir olduğu, dolayısıyla kanunilik ölçütünü karşıladığı anlaşılmaktadır.

98. Bununla birlikte Anayasa'nın 13. maddesi uyarınca temel hak ve özgürlüklere yönelik sınırlamanın demokratik toplum düzeninin gereklerine aykırı olmaması da gerekmektedir. Demokratik toplum düzeninin gereklerine uygun olma ölçütü uyarınca Anayasa'da güvence altına alınan bir hakkın sınırlanabilmesi için öngörülen sınırlamanın demokratik bir toplumda zorlayıcı bir toplumsal ihtiyacın karşılanması amacına yönelik olması gerekir. Kuralın bu ölçütü karşılayıp

karşılamađının tespit edilebilmesi için hangi zorunlu toplumsal ihtiyacı karşılamaya yöneldiđinin tespit edilmesi, bu çerçevede 5271 sayılı Kanun'un konuya ilişkin hükümlerinin incelenmesi gerekmektedir.

99. 5271 sayılı Kanun'un "Cumhuriyet savcısının görev ve yetkileri" başlıklı 161. maddesinin (1), (2) ve (4) numaralı fıkralarına göre Cumhuriyet savcısı doğrudan doğruya veya emrindeki adli kolluk görevlileri aracılığı ile her türlü araştırmayı yapabilir, adli soruşturma ile ilgili sonucu ulaşabilmek için bütün kamu görevlilerinden her türlü bilgiyi isteyebilir, Cumhuriyet savcısı, adli görevi geređince nezdinde görev yaptıđı mahkemenin yargı çevresi dışında bir işlem yapmak ihtiyacı ortaya çıkınca da bu hususta o yer Cumhuriyet savcısından söz konusu işlemi yapmasını ister. Adli kolluk görevlileri, el koydukları olayları, yakalanan kişiler ile uygulanan tedbirleri emrinde çalıştıkları Cumhuriyet savcısına derhâl bildirmek ve bu Cumhuriyet savcısının adli işlere ilişkin bütün emirlerini gecikmeksizin yerine getirmekle yükümlüdür. Diđer kamu görevlileri de yürütölmekte olan soruşturma kapsamında ihtiyaç duyulan bilgi ve belgeleri, ilgili Cumhuriyet savcısına vakit geçirmeksizin temin etmek zorundadır.

100. Anılan maddenin (7) numaralı fıkrasında da "Yetkisizlik kararı ile gelen bir soruşturmada Cumhuriyet savcısı, kendisinin de yetkisiz olduđu kanaatine varırsa yetkisizlik kararı verir ve yetkili savcılıđın belirlenmesi için soruşturma dosyasını, yargı çevresinde görev yaptıđı ağır ceza mahkemesine en yakın ağır ceza mahkemesine gönderir. Mahkemece bu konuda verilen karar kesindir." demek suretiyle herhangi bir soruşturmada yetkisiz olduđu kanısına varan Cumhuriyet savcısının yetkisizlik kararı vererek dosyayı yetkili gördüđu Cumhuriyet savcısına göndereceđi, o Cumhuriyet savcısının da kendisini yetkisiz görmesi hâlinde yetki uyuşmazlıđının ilgili ağır ceza mahkemesince çözüme kavuşturulacađı öngörölmüştür.

101. Buna göre sanal ortamda işlenen suçlar da dahil olmak üzere suç soruşturmasını yapacak yetkili Cumhuriyet başsavcılıđının belirlenmesi ve bu konuya ilişkin uyuşmazlıkların çözümü yargı makamlarının görevi kapsamında kalmaktadır. Kanun'da yargı mercilerine, anılan görevin yerine getirilmesini sağlayabilecek bilgiler de dahil olmak üzere suç soruşturması ile ilgili bilgilere erişme yetkisinin de tanındıđı görölmektedir. Dolayısıyla yalnızca yetkili Cumhuriyet başsavcılıđının belirlenmesi amacıyla kolluđa, kişisel verilerin korunmasını isteme hakkını sınırlamak suretiyle kuralda belirtilen yetkiyi tanımanın zorunlu bir toplumsal ihtiyaca karşılık gelmediđi ve bu yönüyle dava konusu kuralla getirilen sınırlamanın demokratik toplum düzeninin gereklerine uygun olmadıđı sonucuna ulaşılmıştır.

102. Öte yandan kişisel verilerin korunmasını isteme hakkına yönelik sınırlamanın zorunlu bir toplumsal ihtiyaca karşılık geldiği hâllerde de Anayasa'ya uygun bir sınırlamanın varlığının kabulü için Anayasa'nın 20. maddesinin üçüncü fıkrasında korunan söz konusu hakkın gerektirdiği özel güvencelerin kişilere sağlanmış olması gerekir. Dava konusu kuralla öngörülen yetkili Cumhuriyet başsavcılığının belirlenmesi için yapılan sınırlamanın zorunlu bir toplumsal ihtiyaca karşılık gelmediği sonucuna varıldığından bu özel güvenceler yönünden ayrıca inceleme yapılmasına gerek görülmemiştir.

103. Bu çerçevede kuralın olağan dönemde Anayasa'ya aykırı olduğu yönünde yapılan tespit, kuralın olağanüstü dönemde Anayasa'ya aykırı olup olmadığı hususunda herhangi bir değerlendirmeyi kapsamamaktadır.

104. Açıklanan nedenlerle kural Anayasa'nın 13. ve 20. maddelerine aykırıdır. İptali gerekir.

Kural Anayasa'nın 13. ve 20. maddelerine aykırı görülerek iptal edildiğinden Anayasa'nın 2. maddesi yönünden ayrıca incelenmemiştir.

Kuralın Anayasa'nın 15. maddesiyle ilgisi görülmemiştir.

Ğ. Kanun'un 75. Maddesiyle 6132 Sayılı Kanun'a Eklenen Ek 2. Maddenin Birinci Fıkrasının İncelenmesi

1. İptal Talebinin Gerekçesi

105. Dava dilekçesinde özetle; kuralda at yarışları düzenleme, düzenlenen at yarışları üzerine müşterek bahis kabul etme hak ve yetkilerine ilişkin lisansların tanımı ve kapsamının tereddüte yer vermeyecek şekilde açık ve net olarak düzenlenmediği, devredildiği belirtilen lisansların Türkiye Varlık Fonu yönetimi tarafından ne şekilde kullanılacağına ve değerlendirileceğine ilişkin temel ilke ve kurallar ile hukuki çerçevenin belirlenmediği, bu durumun keyfî uygulamalara zemin oluşturduğu, düzenlemenin Türkiye Varlık Fonunun amaçlarıyla tutarlı ve uyumlu olmadığı belirtilerek kuralın Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

106. Kuralda yurt içinde at yarışları düzenleme, yurt içinde ve yurt dışında düzenlenen at yarışları üzerine yurt içinden ve yurt dışından müşterek bahis kabul etme hak ve yetkilerine ilişkin lisansların, topluca 1/1/2018 tarihinden itibaren 49 yıl süreyle 19/8/2016 tarihli ve 6741 sayılı Türkiye Varlık Fonu Yönetimi Anonim Şirketinin Kurulması ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun hükümleri uyarınca kurulan Türkiye Varlık Fonuna (Fon) verildiği hükme bağlanmıştır.

107. Fon, 6741 sayılı Kanun'un amaç ve kapsamını belirleyen 1. maddesinde ve genel gerekçesinde belirtildiği üzere sermaye piyasalarında araç çeşitliliği ve derinliğine katkı sağlamak, yurt içinde kamuya ait olan varlıkları ekonomiye kazandırmak, stratejik büyük ölçekli yatırımlara iştirak etmek yanında yurt içi ve yurt dışında finansal risklerin artmasıyla yaşanan ekonomik dalgalanma dönemlerinde, yabancı yatırımcıların gerçekleştirdikleri fon çıkışlarının varlık fiyatlarında sert düşüşlere yol açması ve yerli yatırımcıların spekülâtif döviz talebinin artması, piyasalarda likiditenin azalması ve finansal istikrara yönelik endişelere yol açması gibi sorunları çözmek için finansal stres ortamında piyasalarda düzenleyici bir görev üstlenerek, kamu fonlarının konsolide olarak yönetildiği, ülke tasarruflarının büyüklüğünü ve gücünü görünür kılarak piyasalarda gerekli güven ortamını yaratarak stratejik düzeyde Türk ekonomisinin dışarıdan yönlendirilen müdahalelere karşı kuvvetlenmesinde önemli rol üstlenmek üzere kurulmuştur.

108. Bu amaçlar yanında Kanun'un genel gerekçesinde ifade edildiği gibi Fonun kurulmasıyla büyüme oranına ilave artış sağlanması, sermaye piyasalarının büyüme ve derinleşmesinin hızlandırılması, bazı finans varlıklarının kullanımının yaygınlaşması, yapılacak yatırımlarla ek istihdam sağlanması, savunma, havacılık ve yazılım gibi teknoloji yoğun stratejik sektörlerdeki yerli şirketlerin sermaye ve proje bazında desteklenmesi, küresel piyasalarda olmalarının sağlanması, büyük altyapı projelerine kamu kesimi borcu artırılmadan finansman sağlanması, katılım finansmanı sektör payının artırılması, arz güvenliğini sağlamak üzere Türkiye için önem taşıyan doğal gaz ve petrol gibi yurt dışındaki stratejik sektörlerle kısıtlamalara bağlı olmaksızın doğrudan yatırım yapılabilmesi hedeflenmektedir.

109. Kanun koyucu, yasama yetkisinin genelliği ilkesinin bir gereği olarak Anayasa'da düzenlenmeyen bir alanı doğrudan düzenleyebilir. Bu bağlamda at yarışlarına ilişkin lisansların düzenlenmesi anayasal bir konu olmayıp anayasal sınırlar içinde kalmak kaydıyla kanun koyucunun takdir yetkisi kapsamındadır.

110. Anayasa'nın açıkça kanunla düzenlenmesini öngörmediği konularda kanunda genel ifadelerle düzenleme yapılarak ayrıntının yürütmeye bırakılması mümkündür. Anayasa'da münhasıran kanunla düzenleme yapılması öngörülme-yen konularda da yasamanın asliliği ve Cumhurbaşkanlığı kararnameleri hâricinde geçerli olan yürütmenin türevselliği ilkeleri gereği idari işlemlerin kanuna dayanması zorunluluğu vardır. Ancak bu durumda kanunda belirlenmesi gereken çerçeve, Anayasa'nın kanunla düzenlenmesini öngördüğü durumdakinden çok daha geniş olabilecektir. Başka bir ifadeyle Anayasa'ya göre kanunla düzenlenmesi gerekmeyen bir konu, kanuni dayanağı olmak kaydıyla idarenin düzenleyici işlemlerine bırakılabilir.

111. Anayasa'da, at yarışları lisanslarına ilişkin düzenlemenin kanunla yapılmasını zorunlu kılan bir hüküm bulunmamaktadır. Kuralda at yarışları düzenleme ve yurt dışında düzenlenen at yarışları üzerine yurt içinden ve yurt dışından müşterek bahis kabul etme hak ve yetkisine ilişkin lisansların 49 yıl süreyle Fona verilmesi öngörülmüştür.

112. At yarışları lisanslarının devredildiği Fona yönelik denetim mekanizması da 6741 sayılı Kanun'un 6. maddesinde düzenlenmiştir. Buna göre Fonu temsil eden Türkiye Varlık Fonu Anonim Şirketi (Şirket), bu şirket tarafından kurulacak diğer şirketler, Fon ve Fon bünyesinde kurulacak alt fonlar hakkında üç aşamalı bir denetim öngörülmüştür. Bu bağlamda Fon ve Şirket ile alt fon ve diğer şirketler hakkında öncelikle bağımsız denetim yapılması, ikinci aşamada bunların bağımsız denetimden geçmiş yıllık mali tabloları ile faaliyetlerinin üç merkezî denetim elemanı tarafından bağımsız denetim standartları çerçevesinde denetlenmesi ve üçüncü aşamada bir önceki yıla ait mali tabloları ile faaliyetlerin her yıl Ekim ayında TBMM Plan ve Bütçe Komisyonu tarafından denetlenmesi öngörülmüştür. Dolayısıyla 49 yıl süreyle Fona devredilen at yarışları lisanslarının amacına uygun şekilde kullanılıp kullanılmadığının denetim dışı kalması söz konusu değildir.

113. Bu itibarla 6741 sayılı Kanun'da denetim usulü de belirlenmiş olan Fona devredilen at yarışları lisanslarının kapsamını ve süresini hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir bir şekilde düzenleyen kuralda belirlilik ilkesine aykırılık bulunmamaktadır.

114. Açıklanan nedenlerle kural Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

H. Kanun'un 80. Maddesiyle 320 Sayılı KHK'nın Değiştirilen Ek 2. Maddesinin Birinci Cümlesinin İncelenmesi

1. İptal Talebinin Gerekçesi

115. Dava dilekçesinde özetle; kuralla şans oyunlarına ilişkin lisansın üçüncü kişilere devredilmek üzere Fona verilmesinin öngörüldüğü, ancak özel hukuk hükümlerine tabi Fon yönetimince bu lisansın ne şekilde üçüncü kişilere devredileceğine ilişkin herhangi bir düzenleme yapılmadığı, konuya ilişkin temel ilke ve kurallar ile hukuki çerçeve ve sınırların kanun koyucu tarafından belirlenmediği, bu durumun keyfi uygulamalara zemin oluşturduğu belirtilerek kuralın Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

116. Kuralla karşılığı nakit olmak üzere oynatılan Piyango, Hemen-Kazan, Sayısal Loto, Şans Topu, On Numara ve Süper Loto oyunları ile ilgili mevzuat çerçevesinde izin verilebilecek olan benzer şans oyunlarına ilişkin lisansların, kuralın yürürlüğe girdiği tarihten itibaren 49 yıl süreyle 6741 sayılı Kanun hükümleri uyarınca kurulan Fona verildiği hükme bağlanmıştır.

117. Şans oyunlarının plânlanması, tertibi ve çekilişine ilişkin bir hükmün Anayasa'da yer almaması karşısında bu hususların düzenlenmesi anayasal bir konu olmayıp anayasal sınırlar içinde kalmak kaydıyla yasama yetkisinin genelliği ilkesinin bir gereği olarak kanun koyucunun takdir yetkisi kapsamındadır.

118. Anayasa'nın açıkça kanunla düzenlenmesini öngörmediği konularda kanunda genel ifadelerle düzenleme yapılarak ayrıntının yürütmeye bırakılması mümkündür. Bu durumda kanunda belirlenmesi beklenen çerçeve, Anayasa'nın kanunla düzenlenmesini öngördüğü durumdakinden çok daha geniş olabilecektir.

119. Bu bağlamda Anayasa'da, şans oyunlarının lisanslarının devredilmesine ilişkin düzenlemenin kanunla yapılmasını zorunlu kılan bir hüküm bulunmadığından kanun koyucu yasal çerçeveyi belirlerken daha geniş takdir yetkisine sahiptir. Kuralın yer aldığı 320 sayılı KHK'nın ek 2. maddesinde Fona 49 yıllığına verilen şans oyunlarına ilişkin lisansın üçüncü kişilere devredilmesinden sonra, idarenin lisansa konu şans oyunlarını düzenleyemeyeceği ve bu oyunlar için ayrı bir lisans veremeyeceği, lisans konusu faaliyetlerin ilgili mevzuat hükümlerine uygun olarak yürütülmesini izlemeye ve denetlemeye idarenin yetkili olduğu belirtilmiştir.

120. Lisans, Millî Piyango İdaresi Genel Müdürlüğü tarafından, şans oyunlarını plânlamak, tertip ve çekilişini düzenlemek üzere verilen izindir. Kuralla şans oyunlarına ilişkin lisanslar 49 yıl boyunca Fona verilmiştir. Fon, söz konusu lisansı üçüncü kişilere devredebileceği gibi kendi bünyesinde oluşturduğu şirketler aracılığıyla da bu lisansı kullanabilir. Ancak lisansın Fon tarafından üçüncü kişilere devredilmesinden sonra idare, 320 sayılı KHK'nın ek 2. maddesi uyarınca lisansa konu şans oyunlarını düzenleyemez ve bu oyunlar için başka bir tüzel kişiye ayrı bir lisans veremez.

121. Anılan maddede geçen idare, Millî Piyango İdaresi Genel Müdürlüğü olup lisans konusu faaliyetlerin ilgili mevzuat hükümlerine uygun olarak yürütülmesini izlemeye ve denetlemeye yetkilidir. Dolayısıyla şans oyunlarına ilişkin lisansların Fon tarafından üçüncü kişilere devredilmesi hâlinde de Millî Piyango İdaresi Genel Müdürlüğü'nün denetleme yetkisi devam etmektedir. Fonun, lisansı devredebileceği üçüncü kişiler ise 13/1/2011 tarihli ve 6102 sayılı Türk Ticaret Kanunu'na tâbi şirketler olacağından bunların kuruluşuna ilişkin düzenlemede de bir belirsizlik bulunmamaktadır.

122. Bu itibarla karşılığı nakit olmak üzere oynatılan şans oyunlarına ilişkin lisansların, kuralın yürürlüğe girdiği tarihten itibaren 49 yıl süreyle 6741 sayılı Kanun hükümleri uyarınca kurulan Fona verilmesini öngören kuralda belirlilik ilkesine aykırı bir yön bulunmamaktadır.

123. Açıklanan nedenlerle kural, Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

I. Kanun'un 82. Maddesiyle 399 Sayılı KHK'nın 7. Maddesinin Birinci Fıkrasına Eklenen (f) Bendinin İncelenmesi

1. İptal Talebinin Gerekçesi

124. Dava dilekçesinde özetle; kural gereğince sözleşmeli olarak işe alınacak personel hakkında güvenlik soruşturması ve/veya arşiv araştırması yapılmış olmasının gerektiği, ancak güvenlik soruşturmasının ve arşiv araştırmasının ne olduğunun, hangi hususların, hangi organlarca araştırılacağı ve bu hususlardan hangilerinin kamu görevine alınmaya engel oluşturacağı kanunda düzenlenmediği, bireyin temel hak ve özgürlüklerini esaslı bir şekilde etkileyen ve sınırlandıran bir konunun yasama organının sadece adını koyarak bütün diğer hususların tespit ve tatbikini idareye bırakmasının hukuki belirlilik ve yasama yetkisinin devredilmezliği ilkelerine aykırılık oluşturduğu, kamu hizmetine girilmede görevin gerektirdiği nitelikler dolayısıyla getirilen sınırlamalar ile kamu hizmeti arasında gerçeklere uyan, nesnel ve zorunlu bir neden sonuç ilişkisinin kurulmasının gerektiği, yalnızca güvenlik soruşturması verilerine dayalı olarak idareye bir kişinin anayasal hakkını kullanmasını engelleme yetkisinin verilmesinin keyfiliğe neden olacağı, kuralın liyakat ilkesine aykırılık oluşturduğu, güvenlik soruşturmasında kullanılan bilgilerin tamamının kişisel veri, yoğunluğunun da özel nitelikli kişisel veri olduğu, bu nedenle kişisel verilerin toplanması, işlenmesi ve kullanılmasının da kanunla düzenlenmiş olmasının gerektiği belirtilerek kuralın Anayasa'nın 2., 7., 13., 20. ve 70. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

125. Kuralda sözleşmeli olarak işe alınacak personel hakkında güvenlik soruşturması ve/veya arşiv araştırmasının yapılmış olması gerektiği belirtilmiştir. Buna göre bir kişinin sözleşmeli olarak işe alınabilmesi için güvenlik soruşturması ve/veya arşiv araştırmasının da yapılması gerekmektedir.

126. 399 sayılı KHK'nın 1. maddesinde, 8/6/1984 tarihli ve 233 sayılı Kamu İktisadi Teşebbüsleri Hakkında Kanun Hükmünde Kararname'ye tabi kamu iktisadi teşebbüsleri ve bağlı ortaklıkların personelinin hizmete alınmalarının, görev ve yetkilerinin, niteliklerinin, atanma, ilerleme, yükselme, hak ve yükümlülükleriyle diğer özlük haklarının bu KHK'da düzenlendiği belirtilmiştir. 399 sayılı

KHK'nın 3. maddesinin birinci fıkrasının (a) bendinde teşebbüs ve bağlı ortaklıklarda hizmetlerin memurlar, sözleşmeli personel ve işçiler eliyle gördürüleceği; (c) ve (d) bentlerinde ise sözleşmeli personelin işçi statüsünde olmadığı ve toplu iş sözleşmeleri kapsamına alınamayacakları hükme bağlanmıştır.

127. KHK'nın 4. ve 6. maddelerinde de sözleşmeli statüde istihdam edilecek personele ait pozisyonların unvan ve sayılarının Cumhurbaşkanı kararı ile tespit edileceği, yeni pozisyonların ihdası ile ihdas edilmiş pozisyonların iptal ve değişikliklerinin de Cumhurbaşkanı kararıyla yapılacağı, sözleşmeli personel ile kamu iktisadi teşebbüsleri ve bağlı ortaklıkları arasında yapılan sözleşmenin idari nitelikte olduğu belirtilmiştir.

128. Sözleşmeli personelin işe alınma usul ve şartları, görev ve yer değişikliği, yükümlülükleri, görevden çekilme, görevden uzaklaştırılma ve sözleşmenin fesih sebep ve usulleri, çalışma saatleri, izin, mali ve sosyal hakları, bu kapsamda sözleşmeli personele ödenecek ücretin alt ve üst sınırları ile sicil ve başarı değerlendirme usul ve esasları da KHK'da düzenlenmiştir.

129. Anılan hükümler gözetildiğinde 399 sayılı KHK'ya tabi olarak görev yapan sözleşmeli personelin Anayasa'nın 128. maddesinde yer alan diğer kamu görevlileri kapsamında olduğu anlaşılmaktadır (benzer yönde bkz. AYM, E.2008/19, K.2010/17, 28/1/2010; E.2008/24, K.2010/115, 16/12/2010).

130. Yukarıda açıklandığı üzere güvenlik soruşturması ve/veya arşiv araştırmasıyla elde edilen veriler kişisel veri niteliğindedir. Kural güvenlik soruşturması ve arşiv araştırması kapsamında kamu mercileri tarafından özel yaşamı ile ilgili sorular sorulması da dâhil olmak üzere bir bireyin özel hayatı, iş ve sosyal yaşamıyla ilgili bilgilerinin alınması, kaydedilmesi ve kullanılmasına imkân tanınması nedeniyle kişisel verilerin korunmasını isteme hakkına sınırlama getirmektedir.

131. Anayasa'nın 20. maddesi uyarınca kişisel veriler ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir. Anayasa'nın 13. maddesinde de temel hak ve hürriyetlerin ancak kanunla sınırlanabileceği ifade edilmiştir. Anayasa'nın 13. ve 20. maddeleri uyarınca kişisel verilerin korunmasını isteme hakkını sınırlamaya yönelik kanuni bir düzenlemenin şeklen var olması yeterli olmayıp yasal kuralların keyfiliğe izin vermeyecek şekilde belirli, ulaşılabilir ve öngörülebilir düzenlemeler niteliğinde olması gerekir.

132. Anayasa'nın 129. maddesinin birinci fıkrasında memurlar ve diğer kamu görevlilerinin Anayasa ve kanunlara sadık kalarak faaliyette bulunma yükümlülükleri düzenlenmiştir. Belirtilen hususlar gözetilerek kamu görevlerine alınacak kişiler bakımından birtakım şartlar getirilmesi doğaldır. Bu şekilde aranan nitelikler kamu hizmetinin etkin ve sağlıklı bir biçimde yürütülmesi amacına

yöneliktir. Dolayısıyla kamu görevine alınmadan önce kişilerin güvenlik soruşturması ve/veya arşiv araştırmasının yapılmasını öngören kural kanun koyucunun takdir yetkisindedir. Ancak bu alanda düzenleme getiren kuralların kamu makamlarına hangi koşullarda ve hangi sınırlar içinde tedbirler uygulama ve özel hayatın gizliliğine yönelik müdahalelerde bulunma yetkisi verildiğini yeterince açık olarak göstermesi ve olası kötüye kullanmalara karşı yeterli güvenceleri sağlaması gerekir (AYM, E.2018/73, K.2019/65, 24/7/2019, § 170).

133. Kuralda güvenlik soruşturması ve/veya arşiv araştırması yapılması sözleşmeli personel alımlarında aranacak şartlar arasında sayılmasına karşın güvenlik soruşturmasına ve arşiv araştırmasına konu edilecek bilgi ve belgelerin neler olduğuna, bu bilgilerin ne şekilde kullanılacağına, hangi mercilerin soruşturma ve araştırmayı yapacağına, bu bilgilerin ne suretle ve ne kadar süre ile saklanacağına, ilgililerin söz konusu bilgilere itiraz etme imkânının olup olmadığına, bilgilerin bir müddet sonra silinip silinmeyeceğine, silinecekse bu sırada izlenecek usulün ne olduğuna, yetkinin kötüye kullanımını önlemeye yönelik nasıl bir denetim yapılacağına ilişkin herhangi bir düzenleme yapılmamıştır. Diğer bir ifadeyle güvenlik soruşturması ve arşiv araştırmasının yapılmasına ve elde edilecek verilerin kullanılmasına ilişkin keyfiliğe izin vermeyecek şekilde belirli ve öngörülebilir kanuni güvencelere yer verilmeksizin kuralla sadece güvenlik soruşturması ve/veya arşiv araştırması yapılması sözleşmeli personel alımında aranacak şartlar arasında sayılmıştır.

134. Güvenlik soruşturması ve arşiv araştırması sonucunda kişisel veri niteliğindeki bilgilerin alınmasına, kullanılmasına, işlenmesine yönelik güvenceler ve temel ilkeler kanunla belirlenmeksizin bunların alınmasına ve kullanılmasına izin verilmesi Anayasa'nın 13. ve 20. maddeleriyle bağdaşmamaktadır (benzer yönde bkz. AYM, E.2018/73, K.2019/65, 24/7/2019, §§ 171, 172; Fatih Saraman [GK], B. No: 2014/7256, §§ 89, 90; Turgut Duman, B. No: 2014/15365, § 88).

135. Bu çerçevede kuralın olağan dönemde Anayasa'ya aykırı olduğu yönünde yapılan tespit, kuralın olağanüstü dönemde Anayasa'ya aykırı olup olmadığı hususunda herhangi bir değerlendirmeyi kapsamamaktadır.

136. Açıklanan nedenlerle kural Anayasa'nın 13. ve 20. maddelerine aykırıdır. İptali gerekir.

Kural Anayasa'nın 13. ve 20. maddelerine aykırı görülerek iptal edildiğinden Anayasa'nın 2., 7. ve 70. maddeleri yönünden ayrıca incelenmemiştir.

İ. Kanun'un 83. Maddesiyle 399 Sayılı KHK'nın 45. Maddesinin Birinci Fıkrasına Eklenen (f) Bendinde Yer Alan "...eylem birliği içerisinde olmak,..." İbaresinin İncelenmesi

1. İptal Talebinin Gerekçesi

137. Dava dilekçesinde özetle; kuralda öngörülen eylem birliği içerisinde olmak kavramının içeriğinin belirsiz, öngörülemez ve muğlak olduğu, hangi somut eylemlerin bu disiplin suçunu oluşturduğuna ilişkin hiçbir düzenlemenin bulunmadığı, bu itibarla kamu hizmetine girme hakkına getirilen sınırlamanın da temel hak ve özgürlüklerin ancak kanunla sınırlanabileceğine ilişkin anayasal ilkeyle bağdaşmadığı belirtilerek kuralın Anayasa'nın 2., 13., 38. ve 70. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

138. 6216 sayılı Kanun'un 43. maddesi uyarınca kural, ilgisi nedeniyle Anayasa'nın 128. maddesi yönünden de incelenmiştir.

139. 399 sayılı KHK'nın 45. maddesinin birinci fıkrasının (f) bendinde terör örgütleriyle eylem birliği içerisinde olmak, bu örgütlere yardım etmek, kamu imkân ve kaynaklarını bu örgütleri desteklemeye yönelik kullanmak ya da kullandırmak, bu örgütlerin propagandasını yapmak, 233 sayılı KHK'ya tabi teşebbüs veya bağlı ortaklıklarda çalışan sözleşmeli personelin sözleşmelerinin feshedileceği hâller arasında öngörülmüştür. Anılan bentte yer alan "...eylem birliği içerisinde olmak,..." ibaresi dava konusu kuralı oluşturmaktadır.

140. Anayasa'nın 128. maddesinin ikinci fıkrasında "Memurların ve diğer kamu görevlilerinin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülükleri, aylık ve ödenekleri ve diğer özlük işleri kanunla düzenlenir. Ancak, malî ve sosyal haklara ilişkin toplu sözleşme hükümleri saklıdır" hükmüne yer verilerek memurlar ve diğer kamu görevlilerinin nitelikleri ve atanmalarına ilişkin hususların kanunla düzenleneceği belirtilmiştir. Memurlar ve diğer kamu görevlilerinin statü haklarını doğrudan etkileyen disiplin işlemlerinin anılan fıkrada yer alan diğer özlük işleri kavramı kapsamına girdiğinde kuşku bulunmamaktadır.

141. Disiplin cezaları, kamu hizmetlerinin yürütülmesi ve kamu yararının devamlılığının sağlanması amacıyla yasal olarak düzenlenmiş idari yaptırımlardır. Kamu hizmetlerini yürütenlerin görev anlayışları, yetki ve sorumlulukları kamu hizmeti ve hizmet gerekleri ile sınırlandırılmış; bu sınırlar dışına çıkanların ise disiplin cezaları ile cezalandırılmaları ilgili kanunlarda öngörülmüştür.

142. Anayasa'nın 38. maddesinin birinci fıkrasında "Kimse, işlendiği zaman yürürlükte bulunan kanunun suç saymadığı bir fiilden dolayı cezalandırılmaz" denilerek suçun kanuniliği ilkesi, üçüncü fıkrasında ise "Ceza ve ceza yerine geçen güvenlik tedbirleri ancak kanunla konulur" ifadesine yer verilerek cezanın kanuniliği ilkesi getirilmiştir. Anayasa'nın 38. maddesinde yer alan suçta ve cezada

kanunilik ilkesi uyarınca hangi eylemlerin yasaklandığı ve bu yasak eylemlere verilecek cezaların hiçbir kuşkuyla yer bırakmayacak biçimde kanunda gösterilmesi kuralın açık, anlaşılır ve sınırlarının belli olması gerekmektedir. Kişilerin yasak eylemleri önceden bilmeleri gerektiği düşüncesine dayanan bu ilkeyle temel hak ve özgürlüklerin güvence altına alınması amaçlanmaktadır.

143. Anayasa'nın 38. maddesinde idari suç ve cezalar ile adli suç ve cezalar arasında bir ayırım yapılmadığından her ikisi de bu maddede öngörülen ilkelere tabidir. Adli ve idari suçlarda davranış normlarına aykırı ve haksızlık teşkil eden bir fiille kanun koyucunun koruma altına aldığı bir hukuki değer ihlali söz konusu olup adli ve idari cezaların her ikisi de cebir içermektedir.

144. Korunan hukuki değer ile ihlalin neden olduğu hukuki sonuçların aynı olmaması ise idari suç ve cezalar ile adli suç ve cezalar arasındaki temel farklılığı oluşturmaktadır. Adli para cezalarından daha yüksek miktarlarda idari para cezalarının verilebilmesine imkân tanıyan düzenlemeler de bulunmakla birlikte adli suçlar için öngörülen cezaların idari suçlar için öngörülen cezalardan genellikle daha ağır olması, hürriyeti bağlayıcı cezaların kural olarak adli suçlar yönünden geçerli olabilmesi, idari suçlarda kanun koyucunun daha az önem atfettiği bir hukuki değer ihlal edilmesi ve öngörülen yaptırımın da genellikle idari bir makam tarafından idari usuller izlenerek uygulanması nedeniyle Anayasa'nın 38. maddesindeki ilkelerin aynı boyut ve kapsamıyla idari suçlara da uygulanması işin mahiyetine uygun düşmemektedir. Bu bağlamda yasama organının ağır işleyen yapısı ile ekonomik ve teknik hayatın hızla değişen ve gelişen şartları gözetilerek suç ve cezalarda kanunilik ilkesinin idari suçlar yönünden daha esnek uygulanması gerekmektedir.

145. Buna karşılık suçta ve cezada kanunilik ilkesinin daha esnek uygulandığı idari yaptırımlara ilişkin düzenlemelerin yalnızca kanun metninde yer alması yeterli değildir. Anayasa Mahkemesinin 14/1/2015 tarihli ve E.2014/100, K.2015/6 sayılı kararında da vurgulandığı üzere söz konusu düzenlemelerin içerik bakımından da belirli amacı gerçekleştirmeye elverişli olması gerekir. Bu açıdan kanun, bireylerin hangi somut fiil ve olguya hangi hukuksal yaptırımın veya sonucun bağlandığını belirli bir açıklık ve kesinlikte öngörebilmelerine imkân verecek nitelikte olmalıdır.

146. Terör kavramı 3713 sayılı Kanun'da tanımlanmıştır. Kanun'un 1. maddesine göre terör; cebir ve şiddet kullanarak, baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle Cumhuriyetin Anayasa'da belirtilen niteliklerini, siyasi, hukuki, sosyal, laik, ekonomik düzeni değiştirmek, devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk devletinin ve Cumhuriyet'in varlığını tehlikeye düşürmek, devlet otoritesini zaafa uğratmak, yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç

teşkil eden eylemlerdir. Terör örgütleri de anılan maddede sayılan amaçlara yönelik olarak suç işlemek üzere meydana getirilmiş örgütlerdir.

147. Kuralla terör örgütleriyle eylem birliği içerisinde olmak sözleşmeli personelin sözleşmesinin feshedilmesini gerektiren fiiller arasında sayılmıştır. Kurala göre sözleşmenin feshedilebilmesi için öncelikle 3713 sayılı Kanun'un 1. maddesinde belirtilen amaçlara ulaşmak için meydana getirilmiş bir örgüt tarafından gerçekleştirilen somut bir terör eylemi olması, sözleşmeli personelin de aynı amaçla bu eyleme fiilî olarak müdahil olması gerekmektedir.

148. Terör örgütüyle eylem birliği içinde olmak her bir terör eylemine göre farklılık gösterebilir. Türk devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek amacıyla gerçekleştirilen terör eylemleri ile devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla gerçekleştirilen eylemler, amacı gereği farklı şekilde gerçekleştirilebilir. Dolayısıyla belirtilen amaçlar çerçevesinde gerçekleştirilen eylemlerde kamu görevlilerinin ne tür bir eylem birliği içinde olacaklarının önceden belirlenmesi zordur. Bu nedenle kanun koyucunun genel bir belirleme yaparak terör örgütleriyle eylem birliği içinde bulunan sözleşmeli personelin sözleşmelerinin feshedilmesini öngördüğü anlaşılmaktadır. Bir başka ifadeyle anılan şekilde genel bir belirleme yapılması kuralın belirsizlik taşıdığı veya keyfiliğe karşı gerekli kanuni güvenceyi taşımadığı anlamına gelmemekte, kanun yapma tekniğinin doğasından kaynaklanmaktadır. Zira kanun kurallarının genel olması, somut olayın özelliğine göre değişebilecek tüm çözümleri kuralın bünyesinde barındırma, bir başka ifadeyle kuralın amaca uygun sonuca ulaştıracak herhangi bir çözümü dışlamasını önleme ihtiyacından kaynaklanmaktadır. Terör örgütleriyle eylem birliği içinde olma fiili, somut olayın özelliğine göre kanuna dayalı olarak idare tarafından belirlenecek ise de idarenin bu işlemi mahkeme tarafından denetleneceğinden bu fiilin nihai olarak kapsamı kanuna dayalı olarak yargı kararıyla ortaya konulacaktır. Dolayısıyla kuralın belirsiz ve öngörülemez olduğu söylenemez (benzer yönde bkz. AYM, E.2018/73, K.2019/65, 24/7/2019, § 186).

149. Açıklanan nedenlerle kural Anayasa'nın 38. ve 128. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

Kuralın Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüş ise de bu bağlamda belirtilen hususların Anayasa'nın 38. ve 128. maddeleri yönünden yapılan değerlendirmeler kapsamında ele alınmış olması nedeniyle Anayasa'nın 2. maddesi yönünden ayrıca bir inceleme yapılmasına gerek görülmemiştir.

Kuralın Anayasa'nın 13. ve 70. maddeleriyle ilgisi görülmemiştir.

IV. YÜRÜRLÜĞÜN DURDURULMASI TALEBİ

150. Dava dilekçesinde özetle, dava konusu kuralların bu hâliyle uygulanmalarının telafisi güç veya imkânsız zararların doğmasına sebebiyet vereceği belirtilerek kuralların yürürlüklerinin durdurulmasına karar verilmesi talep edilmiştir.

1/2/2018 tarihli ve 7072 sayılı Olağanüstü Hal Kapsamında Bazı Düzenlemeler Yapılması Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun'un;

A. 1. 18. maddesiyle 15/2/2011 tarihli ve 6112 sayılı Radyo ve Televizyonların Kuruluş ve Yayın Hizmetleri Hakkında Kanun'un 19. maddesine eklenen (3) numaralı fıkraya,

2. 26. maddesiyle 4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Salâhiyet Kanunu'nun ek 6. maddesine eklenen on sekizinci fıkraya,

3. 82. maddesiyle 22/1/1990 tarihli ve 399 sayılı Kamu İktisadi Teşebbüsleri Personel Rejiminin Düzenlenmesi ve 233 Sayılı Kanun Hükmünde Kararnamenin Bazı Maddelerinin Yürürlükten Kaldırılmasına Dair Kanun Hükmünde Kararname'nin 7. maddesinin birinci fıkrasına eklenen (f) bendine,

yönelik yürürlüğün durdurulması taleplerinin, koşulları oluşmadığından REDDİNE,

B. 1. 7. maddesiyle 24/2/1983 tarihli ve 2802 sayılı Hâkimler ve Savcılar Kanunu'na eklenen geçici 20. maddeye,

2. 9. maddesiyle 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu'nun 172. maddesinin değiştirilen (2) numaralı fıkrasına,

3. 10. maddesiyle 5271 sayılı Kanun'un 173. maddesinin değiştirilen (6) numaralı fıkrasına,

4. 17. maddesiyle 6112 sayılı Kanun'un 8. maddesinin (1) numaralı fıkrasına eklenen (t) bendine,

5. 75. maddesiyle 10/7/1953 tarihli ve 6132 sayılı At Yarışları Hakkında Kanun'a eklenen ek 2. maddenin birinci fıkrasına,

6. 80. maddesiyle 4/4/1988 tarihli ve 320 sayılı Milli Piyango İdaresi Genel Müdürlüğü Kuruluş ve Görevleri Hakkında Kanun Hükmünde Kararname'nin değiştirilen ek 2. maddesinin birinci cümlesine,

7. 83. maddesiyle 399 sayılı Kanun Hükmünde Kararname'nin 45. maddesinin birinci fıkrasına eklenen (f) bendinde yer alan "...eylem birliği içerisinde olmak,..." ibaresine,

yönelik iptal talepleri 19/2/2020 tarihli ve E.2018/91, K.2020/10 sayılı kararlarla reddedildiğinden bu maddeye, fıkralara, bende, cümleye ve ibareye ilişkin yürürlüğün durdurulması taleplerinin REDDİNE,

C. 1. 5. maddesiyle 2802 sayılı Kanun'un 9/A maddesinin beşinci fıkrasının birinci cümlesinde yer alan "...en az yetmiş puan almak kaydıyla..." ibaresinin yürürlükten kaldırılması,

2. 15. maddesiyle 11/11/1983 tarihli ve 2954 sayılı Türkiye Radyo ve Televizyon Kanunu'nun 50. maddesinin birinci fıkrasının değiştirilen (1) bendinin yedinci cümlesi,

hakkında 19/2/2020 tarihli ve E.2018/91, K.2020/10 sayılı kararlarla karar verilmesine yer olmadığına karar verildiğinden bu cümle ve yürürlükten kaldırılmaya ilişkin yürürlüğün durdurulması talepleri hakkında KARAR VERİLMESİNE YER OLMADIĞINA,

19/2/2020 tarihinde OYBİRLİĞİYLE karar verilmiştir.

V. HÜKÜM

1/2/2018 tarihli ve 7072 sayılı Olağanüstü Hal Kapsamında Bazı Düzenlemeler Yapılması Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun'un;

A. 5. maddesiyle 24/2/1983 tarihli ve 2802 sayılı Hâkimler ve Savcılar Kanunu'nun 9/A maddesinin beşinci fıkrasının birinci cümlesinde yer alan "...en az yetmiş puan almak kaydıyla..." ibaresinin yürürlükten kaldırılmasına ilişkin iptal talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA,

B. 7. maddesiyle 2802 sayılı Kanun'a eklenen geçici 20. maddenin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE,

C. 9. maddesiyle 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu'nun 172. maddesinin değiştirilen (2) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE,

Ç. 10. maddesiyle 5271 sayılı Kanun'un 173. maddesinin değiştirilen (6) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE,

D. 15. maddesiyle 11/11/1983 tarihli ve 2954 sayılı Türkiye Radyo ve Televizyon Kanunu'nun 50. maddesinin birinci fıkrasının değiştirilen (1) bendinin yedinci cümlesine ilişkin iptal talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA,

E. 17. maddesiyle 15/2/2011 tarihli ve 6112 sayılı Radyo ve Televizyonların Kuruluş ve Yayın Hizmetleri Hakkında Kanun'un 8. maddesinin (1) numaralı fıkrasına eklenen (t) bendinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE,

F. 18. maddesiyle 6112 sayılı Kanun'un 19. maddesine eklenen (3) numaralı fıkranın Anayasa'ya aykırı olduğuna ve İPTALİNE,

G. 26. maddesiyle 4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Salâhiyet Kanunu'nun ek 6. maddesine eklenen on sekizinci fıkranın Anayasa'ya aykırı olduğuna ve İPTALİNE,

Ğ. 75. maddesiyle 10/7/1953 tarihli ve 6132 sayılı At Yarışları Hakkında Kanun'a eklenen ek 2. maddenin birinci fıkrasının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE,

H. 80. maddesiyle 4/4/1988 tarihli ve 320 sayılı Milli Piyango İdaresi Genel Müdürlüğü Kuruluş ve Görevleri Hakkında Kanun Hükmünde Kararname'nin değiştirilen ek 2. maddesinin birinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE,

I. 82. maddesiyle 22/1/1990 tarihli ve 399 sayılı Kamu İktisadi Teşebbüsleri Personel Rejiminin Düzenlenmesi ve 233 Sayılı Kanun Hükmünde Kararnamenin Bazı Maddelerinin Yürürlükten Kaldırılmasına Dair Kanun Hükmünde Kararname'nin 7. maddesinin birinci fıkrasına eklenen (f) bendinin Anayasa'ya aykırı olduğuna ve İPTALİNE,

İ. 83. maddesiyle 399 sayılı Kanun Hükmünde Kararname'nin 45. maddesinin birinci fıkrasına eklenen (f) bendinde yer alan "...eylem birliği içerisinde olmak,..." ibaresinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE,

19/2/2020 tarihinde OYBİRLİĞİYLE karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili - Hasan Tahsin GÖKCAN

Başkanvekili - Recep KÖMÜRCÜ

Üye: Serdar ÖZGÜLDÜR; Burhan ÜSTÜN; Engin YILDIRIM; Hicabi DURSUN; Celal Mümtaz AKINCI; Muammer TOPAL; M. Emin KUZ; Kadir ÖZKAYA; Rıdvan GÜLEÇ; Recai AKYEL; Yusuf Şevki HAKYEMEZ; Yıldız SEFERİNOĞLU; Selahaddin MENTEŞ

FARKLI GEREKÇE

1. 7072 sayılı Kanunun 5. maddesiyle 2802 sayılı Kanunun 9/A maddesindeki "en az yetmiş puan almak kaydıyla" ibaresi yürürlükten kaldırılmıştır. Ancak anılan kural daha sonra 7165 sayılı Kanunun 4. maddesiyle yeniden ihdas edildiği için, anılan kural hakkında Mahkememizce oy birliğiyle Karar Verilmesine Yer Olmadığına karar verilmiştir. İncelenen kural ise 7072 sayılı

Kanunun 7. maddesiyle 2802 sayılı Kanuna eklenen geçici 20. maddedir. Bu kural ile; 2802 sayılı Kanunun 9/A maddesine ilişkin değişikliğin, anılan 7. maddenin yürürlüğe girdiği tarihten önce yapılan ve sonucu açıklanmayan yazılı sınava katılanlar bakımından da uygulanması öngörülmektedir. Kuralın yürürlük tarihi itibarıyla kapsamının olağanüstü hal yönetim şeklinin uygulandığı dönemle sınırlı olduğu anlaşılmaktadır.

2. Geçici bir dönemde uygulanacak da olsa kuralın, bağlantılı olduğu 9/A maddesindeki “en az yetmiş puan almak kaydıyla” ibaresinin yürürlükten kaldırılmasına ilişkin kural bağlamıyla incelenmelidir. Kural, hakim ve savcı adaylarının adaylığa kabulüyle ilgili olarak 2802 sayılı Kanunun 8/1 maddesinde sözü edilen yazılı sınava ilişkin başarı ölçütüyle ilgilidir. Bu nedenle kuralın kamu hizmetine girme hakkını düzenleyen Anayasanın 70. ve memurlar ve diğer kamu görevlilerinin nitelikleri, atanma, görev ve yetkilerinin kanunla düzenlenmesi gerektiğine ilişkin 128. maddeleri ile ilgisi bulunmaktadır.

3. Her ne kadar kanundaki 70 puan şartının kaldırılması nedeniyle temel hakların sınırının genişletildiği ve bu nedenle bir sınırlamadan söz edilemeyeceği ileri sürülebilir ise de kanundaki yazılı yarışma sınavı koşulunun kaldırılmadığı gözetildiğinde 70 ve üzerinde puanla sınavı kazananlar yönünden mülakata daha fazla kişinin çağrılmasına yol açan düzenlemenin, bazı kişiler yönünden sınırlama etkisine neden olacağı açıktır. Bu nedenle Anayasanın 13. maddesi uyarınca gereklilik ve ölçülülük testine tabi tutulması gerekir.

4. Diğer taraftan kanun koyucunun kamu hizmeti ve görevine girişle ilgili koşulları belirleme konusunda takdir yetkisi bulunmakta ise de Anayasanın 70/2. ve 128/2. maddeleri uyarınca hizmetin ve görevin niteliklerine uygun koşulların aranması gerekmektedir. Başka deyişle kamu hizmetine girişte ‘liyakat’ ilkesine uygun koşullar belirlenmelidir. Hakim ve C. savcısı olmak üzere kamu hizmetine alınacak olanlara ilişkin koşulların belirlenmesinde ayrıca Anayasanın 140. maddesinin de ilgili meslek bağlamında dikkate alınması gerekir. AYM bazı kararlarında AY’nın 128 ve 70. maddeleri uyarınca idarenin liyakat ilkesiyle bağlı olduğuna işaret etmiştir (bkz. AYM 2014/87 E. - 2015/112, 8.12.2015, par. 72; AYM 2014/88 E. - 2015/68, 13.7.2015, par. 134). Dolayısıyla kanun gereği yazılı yarışma sınavı yönteminin geçerli olduğu bir sistemde belirli bir puanla başarı şartının kaldırılarak, listede en başarılı görülenler içinden, alımı planlanan sayıdan birkaç kat adayın mülakata çağrılacağı kabul edilmesi, teorik olarak da olsa yazılı sınav başarısı oldukça yetersiz olanların mülakatta tercih edilmesi ihtimaline yol açmaktadır. Dolayısıyla uygulamadan bağımsız olarak, kuralın Anayasal olarak kamu hizmeti ve görevinin nitelikleri için aranması gereken liyakat ilkesinde zafiyete neden olma riski bulunmaktadır.

Buna karşın kuralın olağanüstü dönem koşullarında ortaya çıkan ihtiyacın gerektirmesi sonucu ve bu dönemle sınırlı olarak uygulanacak olması karşısında, olağan döneme ilişkin olarak yapılabilecek değerlendirmelerden bağımsız olarak sayın çoğunluğun ulaştığı ret sonucuna, açıkladığım gerekçelerle iştirak etmekteyim.

Başkanvekili - Hasan Tahsin GÖKCAN

FARKLI GEREKÇE

2802 sayılı Kanunun geçici 20. maddesinin Anayasanın 2., 70. ve 128. maddelerine aykırı olmadığına ve iptal talebinin reddine karar verilmiştir.

Kararın gerekçesinde; 680 sayılı KHK ile 2802 sayılı Kanunun 9/A maddesinin beşinci fıkrasında yapılan değişikliğin, geçici 20. maddenin yürürlüğe girmesinden önce yapılan ve sonucu açıklanmayan yazılı sınava katılanlar bakımından da uygulanmasının öngörüldüğü, böylece daha önce yapılan ancak sonucu açıklanmayan yazılı sınava katılanlardan mülakata çağrılacak olanların belirlenmesinde yazılı sınavdan en az yetmiş puan alma şartının aranmadığı, yazılı sınav sonuçlarının henüz açıklanmadığı bir safhada taban puan şartının kaldırılmasının geriye yürüme niteliğinde olmadığı, 2802 sayılı Kanunun 8. maddesinde yazılı yarışma sınavında başarılı olmanın şartları “en yüksek puandan başlamak üzere ilanda belirtilen kadro sayısının iki katı aday arasına girmek ve en az yetmiş puan almak” şeklinde belirlenmişken taban puan şartının kaldırılmasının kamu hizmetine girme hakkının sınırlanması sonucuna yol açmadığı, sınavdan belli bir puan alma şartının adaylığa atanma koşulu olarak öngörülüp öngörülmeceği konusunda kanun koyucunun takdir yetkisinin bulunduğu, bu sebeplerle kuralın Anayasaya aykırı bir yönünün bulunmadığı belirtilmiştir.

Kararda belirtildiği üzere, hukuk devleti ilkesinin temel unsurlarından biri olan hukukî güvenlik ilkesi; hukuk normlarının öngörülebilir olmasını, bireylerin bütün eylem ve işlemlerde devlete güven duyabilmesini, devletin de kanunî düzenleme yaparken güven duygusunu zedelemekten kaçınmasını gerekli kılmaktadır. Kararda, kanunların geriye yürümezliği ilkesi ve bunun istisnaları ile hukukî güvenlik ilkesine ilişkin boyutları konusunda yapılan genel tespitlere katılmakla beraber, mezkûr ilkenin incelenen kural bakımından Anayasanın 70. ve 128. maddeleri ile birlikte değerlendirilmesi gerektiğinden, red kararına çoğunluktan farklı gerekçeyle katılıyorum.

Bilindiği gibi, Anayasanın 70. maddesinde kamu hizmetlerine girme hakkı düzenlenirken hizmete alınmada görevin gerektirdiği niteliklerden başka bir ayrım gözetilemeyeceği; 128. maddesinde de memurların ve diğer kamu görevlilerinin nitelikleri ile atanmalarının kanunla düzenleneceği hükme

bağlanmıştır. Kararın gerekçesinde belirtildiği üzere, hâkim ve savcı adaylığına atanabilmenin şartları da -Anayasanın 70. ve 128. maddelerinden kaynaklanan bir zorunluluk olarak- 2802 sayılı Kanunun 8. maddesinde düzenlenmiş ve yazılı sınavda başarılı olmak da görevin gerektirdiği niteliklerin belirlenmesi açısından mezkûr şartlar arasında sayılmıştır. Yine kararda belirtildiği gibi, yazılı sınavda başarılı olmanın şartları arasında yer verilen asgari yetmiş puan alma şartı 680 sayılı KHK ile kaldırılmış, daha önce yapılan ve sonucu açıklanmayan sınava katılanlar bakımından da asgari puan şartının aranmayacağı yönünde geçici bir düzenleme yapılmıştır.

Çoğunluğun red gerekçesinde, yazılı sınavın yapıldığı sırada Kanunda öngörülen en az yetmiş puan alma şartının -sınav sonuçları açıklanmadan önce- kaldırılmasının kamu hizmetine girme hakkının sınırlandırılmasına yol açmadığı belirtilmekte ise de, bu durumda taban puanı alamayanların da yazılı sınavda başarılı olmanın ilk şartı olan en yüksek puandan başlamak üzere ilanda belirtilen kadro sayısının iki katı aday arasına girmeleri kaçınılmaz olduğundan, düzenlemenin yetmiş veya daha fazla puan alanların kamu hizmetine girme hakkı açısından bir sınırlamaya yol açtığı açıktır. Başka bir anlatımla, en az yetmiş puan alan aday sayısının, ilan edilen kadro sayısının iki katına ulaşmadığı bir sınavda bu puanı alanların ikinci aşamayı oluşturan sözlü sınavda başarılı olma ve ilan edilen kadrolara atanma ihtimali daha yüksek iken, taban puanın kaldırılması -her hâlükârda kadro sayısının iki katı fazlası aday çağrılacağı için- sınavın yapıldığı tarihte aranan taban puan ve üzerinde puan alan adaylar bakımından kamu hizmetine girme hakkının sınırlandırılması sonucunu doğuracaktır.

Bu nedenle, incelenen geçici madde ile yapılan düzenlemenin, Anayasanın temel hakları ve ödevleri düzenleyen İkinci Kısımın siyasî haklara ve ödevlere ilişkin Dördüncü Bölümünde yer alan 70. maddedeki kamu hizmetine girme hakkının, yazılı sınavdan yetmiş ve üzerinde puan alanlar yönünden sınırlandırılması niteliğinde olduğu açıktır.

Kuşkusuz bu sınırlama yapılırken Anayasanın, temel hak ve hürriyetlerin sınırlandırılması rejimini düzenlenen 13. maddesine uyulması gerekir.

İncelenen geçici hüküm, 15 Temmuz darbe teşebbüsünden yaklaşık altı ay sonra, yani yargı organlarının karşılaştığı büyük çaptaki iş yüküne karşılık önemli ölçüde hâkim-savcı açığının ortaya çıkmasının ve bu açığın hızlı bir şekilde doldurulması ihtiyacının doğmasının ardından 680 sayılı KHK ile 2802 sayılı Kanuna eklenmiştir. Dolayısıyla kuralla yapılan sınırlamanın kamu yararının sağlanmasına yönelik meşru bir amacı bulunmaktadır.

Bununla birlikte, Anayasanın 13. maddesi uyarınca bu sınırlamanın ölçülü olup olmadığının da değerlendirilmesi gerekmektedir. Kararlarımızda elverişlilik, gereklilik ve orantılılık şeklinde alt ilkeleri belirlenen ölçülülüğün “elverişlilik” unsuru bakımından söz konusu düzenlemede bir sorun

bulunmamaktadır. Buna karşılık yukarıda belirtilen meşru amaç bakımından da olsa, yazılı sınavda başarılı sayılmak için aranan yetmiş puanlık alt sınırın -dönemi şartları da dikkate alınarak- takdir yetkisi kapsamında değiştirilerek adayın yeterliğini de gösterecek daha düşük bir taban puan belirlenmeden, geçmişe etkili olacak ve hukukî güvenlik ilkesini de zedeleyecek şekilde tamamen kaldırılmasının Anayasanın 70. maddesinde şart koşulan “görevin gerektirdiği niteliklerin” belirlenmesini neredeyse imkânsız kılması bir yana, ulaşılmak istenen amaç bakımından zorunlu olmadığı ve sınırlama ile ulaşılmak istenen amaç arasında makul bir denge gözetilmediği için, yazılı sınavdan yetmiş ve üzeri puan alanların kamu hizmetine girme hakkını gereksiz ve orantısız bir şekilde sınırladığını belirtmek gerekir.

Kural bu nedenle, Anayasanın 70. maddesinde öngörülen hakka ölçüsüz bir sınırlama getirmekle birlikte, olağanüstü hâllerde temel hak ve hürriyetlerin sınırlandırılmasına ilişkin 15. madde bakımından da incelenmelidir. Kararın olağanüstü hâl düzenlemelerine ilişkin genel açıklamalarında da ifade edildiği üzere, Anayasanın 15. maddesinde belirtilen şartlara uyulmak kaydıyla, olağanüstü hâllerde temel hak ve hürriyetlerin kullanılmasının kısmen veya tamamen durdurulması ve Anayasanın diğer maddelerinde öngörülen güvencelere aykırı tedbirler alınması mümkündür (§§ 13-16).

İncelenen kural olağanüstü hâl döneminde, olağanüstü hâlin ilanına sebep olan tehdit ve tehlikelerin bertaraf edilmesine yönelik olarak yürürlüğe konulmuş; olağanüstü hâl süresiyle sınırlı şekilde uygulanmış ve kararda belirtildiği üzere o tarihte henüz sunucu açıklanmamış olan yazılı sınava uygulanmakla hükmünü icra etmiştir. Kural ayrıca Anayasanın 15. maddesinde olağanüstü hâllerde bile dokunulamayacağı hükme bağlanan bir sınırlama da öngörmemektedir.

Bu itibarla, red kararına çoğunluğun gerekçesinde belirtilen sebeplerden farklı olarak yukarıdaki gerekçelerle katılıyorum.

Üye - M.Emin KUZ

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2018/73

Karar Sayısı: 2019/65

Karar Tarihi: 24/7/2019

RG Tarih - Sayı: 29/11/2019 - 30963

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri Engin ALTAY, Özgür ÖZEL, Engin ÖZKOÇ ile birlikte 114 milletvekili

İPTAL DAVASININ KONUSU: 1/2/2018 tarihli ve 7070 sayılı Olağanüstü Hal Kapsamında Bazı Düzenlemeler Yapılması Hakkında Kanun'un;

A. 1. maddesiyle 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu'nun 149. maddesinin (2) numaralı fıkrasına eklenen cümlelerin,

B. 2. maddesiyle 5271 sayılı Kanun'un 151. maddesinin (4) numaralı fıkrasına eklenen "...avukat hakkındaki soruşturma veya..." ile "...soruşturma veya..." ibarelerinin,

C. 3. maddesiyle 5271 sayılı Kanun'un 154. maddesine eklenen (2) numaralı fıkrada yer alan "...örgüt faaliyeti çerçevesinde işlenen uyuşturucu ve uyarıcı madde imâl ve ticareti suçları..." ibaresinin,

Ç. 4. maddesiyle 5271 sayılı Kanun'un 178. maddesinin (1) numaralı fıkrasına eklenen cümlelerin,

D. 5. maddesiyle 5271 sayılı Kanun'un 188. maddesinin (1) numaralı fıkrasına eklenen cümlelerin,

E. 6. maddesiyle 13/12/2004 tarihli ve 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun'un 59. maddesine eklenen (5), (10) ve (11) numaralı fıkraların,

F. 33. maddesiyle 18/5/1929 tarihli ve 1453 sayılı Zabitan ve Askeri Memurların Maaşatı Hakkında Kanun'a eklenen geçici 1. maddenin ikinci fıkrasının,

G. 48. maddesiyle 31/7/1970 tarihli ve 1325 sayılı Millî Savunma Bakanlığı Görev ve Teşkilâtı Hakkında Kanun'a (2/7/2018 tarihli ve 703 sayılı Kanun Hükmünde Kararname ile "Askeri Okullar, Askeri Öğrenciler, Askeri Fabrikalar ve Bazı Düzenlemeler Hakkında Kanun" şeklinde değiştirilmiştir) eklenen ek 10. maddenin "...Bakanlığın özelliği ve hizmetin gerekli kıldığı şart ve vasıflar göz önüne alınarak Bakanlığa intibak edemedikleri üstlerince teklif edilenlerden Bakanlıkta

oluşturulacak komisyona yaptırılacak tahkikat sonucuna göre Millî Savunma Bakanınca uygun görülenler,...” bölümünün,

Ğ. 56. maddesiyle 10/3/2011 tarihli ve 6191 sayılı Sözleşmeli Erbaş ve Er Kanunu’na eklenen geçici 1. maddenin,

H. 60. maddesiyle 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu’nun 48. maddesinin birinci fıkrasının (A) bendine eklenen (8) numaralı alt bendin,

I. 61. maddesiyle 657 sayılı Kanun’un 125. maddesinin birinci fıkrasının (E) bendine eklenen (I) alt bendinde yer alan “...eylem birliği içerisinde olmak,...” ibaresinin,

İ. 62. maddesiyle 11/10/2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname’ye (703 sayılı Kanun Hükmünde Kararname ile “Sağlık Alanında Bazı Düzenlemeler Hakkında Kanun Hükmünde Kararname” şeklinde değiştirilmiştir) eklenen 45/A maddesinin (2) ve (3) numaralı fıkralarının,

J. 73. maddesiyle 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu’na eklenen geçici 16. maddenin ikinci cümlesinin,

Anayasa’nın Başlangıç kısmı ile 2., 7., 10., 13., 15., 36., 38., 41., 48., 49., 70., 90. ve 128. maddelerine aykırılığı ileri sürülerek iptallerine ve yürürlüklerinin durdurulmasına karar verilmesi talebidir.

I. İPTALİ İSTENEN KANUN HÜKÜMLERİ

Kanun’un iptali talep edilen kuralların da yer aldığı;

1. 1. maddesiyle (2) numaralı fıkrasına cümle eklenen 5271 sayılı Kanun’un 149. maddesi şöyledir:

“Şüphelinin veya sanığın müdafii seçimi

Madde 149 (1) Şüpheli veya sanık, soruşturma ve kovuşturmanın her aşamasında bir veya birden fazla müdafiiin yardımından yararlanabilir; kanunî temsilcisi varsa, o da şüpheliye veya sanığa müdafii seçebilir.

(2) Soruşturma evresinde, ifade almada en çok üç avukat hazır bulunabilir. (Ek cümle: 3/10/2016-KHK-676/1 md.; Aynen kabul: 1/2/2018-7070/1 md.) Örgüt faaliyeti çerçevesinde işlenen suçlar bakımından yürütülen kovuşturmalarda, duruşmada en çok üç avukat hazır bulunabilir.

(3) Soruşturma ve kovuşturma evrelerinin her aşamasında avukatın, şüpheli veya sanıkla görüşme, ifade alma veya sorgu süresince yanında olma ve hukukî yardımda bulunma hakkı engellenemez, kısıtlanamaz.”

2. 2. maddesiyle (4) numaralı fıkrasına ibareler eklenen 5271 sayılı Kanun'un 151. maddesi şöyledir:

“Müdafi görevini yerine getirmediğinde yapılacak işlem ve müdafilik görevinden yasaklanma

Madde 151- (1) 150 nci madde hükmüne göre görevlendirilen müdafi, duruşmada hazır bulunmaz veya vakitsiz olarak duruşmadan çekilir veya görevini yerine getirmekten kaçınırsa, hâkim veya mahkeme derhâl başka bir müdafi görevlendirilmesi için gerekli işlemi yapar. Bu durumda mahkeme oturuma ara verebileceği gibi oturumun ertelenmesine de karar verebilir.

(2) Eğer yeni müdafi savunmasını hazırlamak için yeterli zaman olmadığını açıklarsa oturum ertelenir.

(3) (Ek: 25/5/2005 - 5353/22 md.) 149 uncu maddeye göre seçilen veya 150 nci maddeye göre görevlendirilen ve Türk Ceza Kanununun 220 ve 314 üncü maddesinde sayılan suçlar ile terör suçlarından şüpheli, sanık veya hükümlü olanların müdafilik veya vekillik görevini üstlenen avukat, hakkında bu fıkra da sayılan suçlar nedeniyle soruşturma ya da kovuşturma bulunması halinde müdafilik veya vekillik görevini üstlenmekten yasaklanabilir.

(4) (Ek:25/5/2005 - 5353/22 md.) Cumhuriyet savcısının yasaklamaya ilişkin talebi hakkında, hâkim veya mahkeme tarafından gecikmeksizin karar verilir. Bu kararlara karşı itiraz edilebilir. İtiraz sonucunda yasaklama kararının kaldırılması halinde avukat görevini devam ettirir. Müdafilik görevinden yasaklama kararı, avukat hakkındaki soruşturma veya kovuşturma konusu suçla sınırlı olmak üzere, bir yıl süre ile verilebilir. Ancak, soruşturma veya kovuşturmanın niteliği itibariyle bu süreler altı aydan fazla olmamak üzere en fazla iki defa uzatılabilir. Soruşturma sonunda kovuşturmaya yer olmadığına dair karar verilmesi veya kovuşturma sonunda mahkûmiyet dışında bir karar verilmesi halinde, kesinleşmesi beklenmeksizin yasaklama kararı kendiliğinden kalkar.

(5) (Ek:25/5/2005 - 5353/22 md.) Görevden yasaklama kararı, şüpheli, sanık veya hükümlü ile yeni bir müdafi görevlendirilmesi için derhal ilgili baro başkanlığına bildirilir.

(6) (Ek:25/5/2005 - 5353/22 md.) Müdafi veya vekil görevden yasaklanmış bulunduğu sürece başka davalarla ilgili olsa bile müdafiliğini veya vekilliğini üstlendiği kişiyi ceza infaz kurumunda veya tutukevinde ziyaret edemez.”

3. 3. maddesiyle fıkra eklenen 5271 sayılı Kanun'un 154. maddesi şöyledir:

“Müdafi ile görüşme

Madde 154- (1) Şüpheli veya sanık, vekâletname aranmaksızın müdafii ile her zaman ve konuşulanları başkalarının duyamayacağı bir ortamda görüşebilir. Bu kişilerin müdafii ile yazışmaları denetime tâbi tutulamaz.

(2) (Ek: 3/10/2016-KHK-676/3 md.; Aynen kabul: 1/2/2018-7070/3 md.) Türk Ceza Kanununun İkinci Kitap Dördüncü Kısım Dördüncü, Beşinci, Altıncı ve Yedinci Bölümlerinde tanımlanan suçlar ve Terörle Mücadele Kanunu kapsamına giren suçlar ile örgüt faaliyeti çerçevesinde işlenen uyuşturucu ve uyarıcı madde imâl ve ticareti suçları bakımından gözaltındaki şüphelinin müdafii ile görüşme hakkı Cumhuriyet savcısının istemi üzerine, hâkim kararıyla yirmidört saat süreyle kısıtlanabilir; bu zaman zarfında ifade alınamaz.”

4. 4. maddesiyle (1) numaralı fıkrasına cümle eklenen 5271 sayılı Kanun’un 178. maddesi şöyledir:

“Çağrılması reddedilen tanığın ve uzman kişinin doğrudan mahkemeye getirilmesi

Madde 178- (1) Mahkeme başkanı veya hâkim, sanığın veya katılanın gösterdiği tanık veya uzman kişinin çağrılması hakkındaki dilekçeyi reddettiğinde, sanık veya katılan o kişileri mahkemeye getirebilir. Bu kişiler duruşmada dinlenir. (Ek cümle: 3/10/2016-KHK-676/4 md.; Aynen kabul: 1/2/2018-7070/4 md.) Ancak, davayı uzatmak amacıyla yapılan talepler reddedilir.”

5. 5. maddesiyle (1) numaralı fıkrasına cümle eklenen 5271 sayılı Kanun’un 188. maddesi şöyledir:

“Duruşmada hazır bulunacaklar

Madde 188 - (1) Duruşmada, hükme katılacak hâkimler ve Cumhuriyet savcısı ile zabıt kâtibinin ve Kanunun zorunlu müdafiliği kabul ettiği hâllerde müdafii hazır bulunması şarttır. (Ek cümle: 3/10/2016- KHK-676/5 md.; Aynen kabul: 1/2/2018-7070/5 md.) Müdafii mazeretsiz olarak duruşmaya gelmemesi veya duruşmayı terk etmesi halinde duruşmaya devam edilebilir.

(2) (Mülga: 18/6/2014 - 6545/103 md.)

(3) Bir oturumda bitmeyecek davada, herhangi bir nedenle bulunamayacak üyenin yerine geçmek ve oya katılmak üzere yedek üye bulundurulabilir.”

6. 6. maddesiyle fıkralar eklenen 5275 sayılı Kanun’un 59. maddesi şöyledir:

“Avukat ve noterle görüşme hakkı

MADDE 59.- (1) Hükümlü, avukatlık mesleğinin icrası çerçevesinde avukatları ile vekâletnamesi olmaksızın en çok üç kez görüşme hakkına sahiptir.

(2) Avukat ve noter ile görüşme, meslek kimliklerinin ibrazı üzerine, tatil günleri dışında ve çalışma saatleri içinde, bu iş için ayrılan görüşme yerlerinde, konuşulanların duyulamayacağı, ancak güvenlik nedeniyle görülebileceği bir biçimde yapılır.

(3) Avukatlar, vekâletnameleri olsa da aynı anda birden fazla hükümlü ile görüşme yapamazlar.

(4) (Değişik: 3/10/2016-KHK-676/6 md.; Aynen kabul: 1/2/2018-7070/6 md.) Görüşme sırasında; hükümlünün avukatına veya avukatın hükümlüye verdiği belge veya belge örnekleri, dosyalar ve aralarındaki konuşmaya ilişkin olarak kendilerinin tuttıkları kayıtlar incelenemez; hükümlünün avukatı ile yaptığı görüşme dinlenemez ve kayda alınmaz.

(5) (Ek: 3/10/2016-KHK-676/6 md.; Aynen kabul: 1/2/2018-7070/6 md.) Türk Ceza Kanununun 220 nci maddesinde ve İkinci Kitap Dördüncü Kısım Dördüncü, Beşinci, Altıncı ve Yedinci Bölümlerinde tanımlanan suçlar ile 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu kapsamına giren suçlardan mahkûm olanların avukatları ile görüşmelerinde, toplumun ve ceza infaz kurumunun güvenliğinin tehlikeye düşürüldüğüne, terör örgütü veya diğer suç örgütlerinin yönlendirildiğine, bu örgütlere emir ve tâlimat verildiğine veya yorumları ile gizli, açık ya da şifreli mesajlar iletildiğine ilişkin bilgi, bulgu veya belge elde edilmesi hâlinde, Cumhuriyet başsavcılığının istemi ve infaz hâkiminin kararıyla, üç ay süreyle; görüşmeler teknik cihazla sesli veya görüntülü olarak kaydedilebilir, hükümlü ile avukatın yaptığı görüşmeleri izlemek amacıyla görevli görüşmede hazır bulundurulabilir, hükümlünün avukatına veya avukatın hükümlüye verdiği belge veya belge örnekleri, dosyalar ve aralarındaki konuşmalara ilişkin tuttıkları kayıtlara elkonulabilir veya görüşmelerin gün ve saatleri sınırlandırılabilir.

(6) (Ek: 3/10/2016-KHK-676/6 md.; Aynen kabul: 1/2/2018-7070/6 md.) İnfaz hakimliği hükümlünün; kurallara uyumunu, toplum veya ceza infaz kurumu bakımından arz ettiği tehlikeyi ve rehabilitasyon çalışmalarındaki gelişimini değerlendirerek, kararda belirttiği süreyi üç aydan fazla olmamak üzere müteaddit defa uzatabileceği gibi kısaltılmasına veya sonlandırılmasına da karar verebilir.

(7) (Ek: 3/10/2016-KHK-676/6 md.; Aynen kabul: 1/2/2018-7070/6 md.) Beşinci fıkra kapsamına giren hükümlünün yaptığı görüşmenin, aynı fıkroda belirtilen amaca yönelik yapıldığının anlaşılması hâlinde, görüşmeye derhal son verilerek, bu husus gerekçesiyle birlikte tutanağa bağlanır. Görüşme başlamadan önce taraflar bu hususta uyarılır.

(8) (Ek: 3/10/2016-KHK-676/6 md.; Aynen kabul: 1/2/2018-7070/6 md.) Hükümlü hakkında, yedinci fıkra uyarınca tutanak tutulması hâlinde, Cumhuriyet başsavcılığının istemiyle hükümlünün avukatlarıyla görüşmesi infaz hâkimince altı ay süreyle yasaklanabilir. Yasaklama kararı, hükümlüye

ve yeni bir avukat görevlendirilmesi için derhal ilgili baro başkanlığına bildirilir. Cumhuriyet başsavcılığı baro tarafından bildirilen avukatın değiştirilmesini baro başkanlığından isteyebilir. Bu fıkra hükmüne göre görevlendirilen avukata, 23/3/2005 tarihli ve 5320 sayılı Ceza Muhakemesi Kanununun Yürürlük ve Uygulama Şekli Hakkında Kanunun 13 üncü maddesine göre ücret ödenir.

(9) (Ek: 3/10/2016-KHK-676/6 md.; Aynen kabul: 1/2/2018-7070/6 md.) İnfaz hâkimi tarafından bu madde uyarınca verilen kararlara karşı 4675 sayılı Kanuna göre itiraz edilebilir.

(10) (Ek: 3/10/2016-KHK-676/6 md.; Aynen kabul: 1/2/2018-7070/6 md.) Bu madde hükümleri 9 uncu maddenin üçüncü fıkrasına göre yüksek güvenlikli ceza infaz kurumlarında bulunan hükümlüler ile beşinci fıkradaki suçlardan hükümlü olup, başka bir suçtan dolayı şüpheli veya sanık sıfatıyla avukatıyla görüşen hükümlüler hakkında da uygulanır.

(11) (Ek: 3/10/2016-KHK-676/6 md.; Aynen kabul: 1/2/2018-7070/6 md.) Tutuklular hakkında bu madde hükümlerine göre karar vermeye soruşturma aşamasında sulh ceza hâkimi, kovuşturma aşamasında mahkeme yetkilidir.

(12) (Ek ibare: 25/5/2005-5351/5 md.) Türkiye Cumhuriyetinin taraf olduğu uluslararası sözleşmelere ve karşılıklılık esasına uygun olmak koşuluyla, Yabancı ülkelerde haklarında soruşturma veya kovuşturma yapılmakta olan, yabancı ülke veya uluslararası yargı mercilerinde dava açmak isteyen, leh veya aleyhine açılmış davası olan Türk vatandaşı veya yabancı uyruklu hükümlülerle yabancı uyruklu avukatları, bu soruşturma ve kovuşturma, açılacak veya açılmış davalarla sınırlı olmak ve vekâletname sunmak koşuluyla görüşebilirler. Vekâletnamesi olmayan yabancı uyruklu avukatlar, hükümlü ile Türkiye barolarına kayıtlı bir avukatla birlikte görüşme yapabilirler.”

7. 33. maddesiyle 1453 sayılı Kanun'a eklenen geçici 1. madde şöyledir:

“Geçici Madde 1- - (Ek: 3/10/2016-KHK-676/38 md.; Aynen kabul: 1/2/2018-7070/33 md.)

Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığının 2 nci madde uyarınca 2016 yılı için belirlenmiş olan fiili kadroları 2016 yılı sonuna kadar uygulanır.

Jandarma Genel Komutanlığı, Jandarma ve Sahil Güvenlik Akademisi ile Sahil Güvenlik Komutanlığının 2017 yılı fiili kadroları 2016 yılı sonuna kadar Türkiye Büyük Millet Meclisi Plan ve Bütçe Komisyonunca belirlenir.”

8. 48. maddesiyle 1325 sayılı Kanun'a eklenen ek 10. madde şöyledir:

“Ek Madde 10- (Ek: 3/10/2016-KHK-676/60 md.; Aynen kabul: 1/2/2018-7070/48 md.)

Millî Savunma Bakanlığı fiili kadrosuna dahil 657 sayılı Devlet Memurları Kanununa tabi personelden Bakanlığın özelliği ve hizmetin gerekli kıldığı şart ve vasıflar göz önüne alınarak Bakanlığa intibak edemedikleri üstlerince teklif edilenlerden Bakanlıkta oluşturulacak komisyona yaptırılacak tahkikat sonucuna göre Millî Savunma Bakanınca uygun görülenler, genel hükümlere göre merkezî yönetim bütçe kanununda öngörülen atama sınırlamalarına tabi olmadan Çalışma, Sosyal Hizmetler ve Aile Bakanlığı aracılığıyla başka bir kurum veya kuruluşa naklen atanır.”

9. 56. maddesiyle 6191 sayılı Kanun’a eklenen geçici 1. madde şöyledir:

“GEÇİCİ MADDE 1 - (Ek: 3/102016-KHK-676/70 md.; Aynen kabul: 1/2/2018- 7070/56 md.)

(1) Bu maddenin yürürlüğe girdiği tarihten önce milli güvenliğe tehdit oluşturduğu tespit edilen FETÖ/PDY terör örgütüne aidiyeti, iltisakı veya irtibatı nedeniyle sözleşmeleri feshedilen sözleşmeli erbaş ve erler hakkında 22/7/2016 tarihli ve 667 sayılı Olağanüstü Hal Kapsamında Alınan Tedbirlere İlişkin Kanun Hükmünde Kararnamenin 4 üncü maddesinin ikinci ve üçüncü fıkraları uygulanır.”

10. 60. maddesiyle (A) bendine alt bent eklenen 657 sayılı Kanun’un 48. maddesinin birinci fıkrası şöyledir:

“Genel ve özel şartlar:

Madde 48 - (Değişik: 12/5/1982 - 2670/14 md.)

Devlet memurluğuna alınacaklarda aşağıdaki genel ve özel şartlar aranır.

A) Genel şartlar:

1. Türk Vatandaşı olmak,
2. Bu Kanunun 40 ncı maddesindeki yaş şartlarını taşımak,
3. Bu Kanunun 41 nci maddesindeki öğrenim şartlarını taşımak,
4. Kamu haklarından mahrum bulunmamak,
5. (Değişik: 23/1/2008 - 5728/317 md.) Türk Ceza Kanununun 53 üncü maddesinde belirtilen süreler geçmiş olsa bile; kasten işlenen bir suçtan dolayı bir yıl veya daha fazla süreyle hapis cezasına ya da affa uğramış olsa bile devletin güvenliğine karşı suçlar, Anayasal düzene ve bu düzenin işleyişine karşı suçlar, (...) zimmet, irtikâp, rüşvet, hırsızlık, dolandırıcılık, sahtecilik, güveni kötüye kullanma, hileli iflas, ihaleye fesat karıştırma, edimin ifasına fesat karıştırma, suçtan kaynaklanan malvarlığı değerlerini aklama veya kaçakçılık suçlarından mahkûm olmamak.
6. Askerlik durumu itibariyle;

- a) Askerlikle ilgisi bulunmamak,
- b) Askerlik çağına gelmemiş bulunmak,
- c) Askerlik çağına gelmiş ise muvazzaf askerlik hizmetini yapmış yahut ertelenmiş veya yedek sınıfa geçirilmiş olmak,

7. 53 üncü madde hükümleri saklı kalmak kaydı ile görevini devamlı yapmasına engel olabilecek (...) akıl hastalığı (...) bulunmamak.

8. (Ek: 3/10/2016 - KHK-676/74 md.; Aynen kabul: 1/2/2018-7070/60 md.) Güvenlik soruşturması ve/veya arşiv araştırması yapılmış olmak.

B) Özel şartlar:

- 1. Hizmet göreceği sınıf için 36 ve 41 nci maddelerde belirtilen öğretim ve eğitim kurumlarının birinden diploma almış olmak,
- 2. Kurumların özel kanun veya diğer mevzuatında aranan şartları taşımak.”

11. 61. maddesiyle alt bent eklenen 657 sayılı Kanun'un 125. maddesinin birinci fıkrasının (E) bendi şöyledir:

“E - Devlet memurluğundan çıkarma: Bir daha Devlet memurluğuna atanmamak üzere memurluktan çıkarmaktır.

Devlet memurluğundan çıkarma cezasını gerektiren fiil ve haller şunlardır:

- a) İdeolojik veya siyasi amaçlarla kurumların huzur, sükün ve çalışma düzenini bozmak, boykot, işgal, kamu hizmetlerinin yürütülmesini engelleme, işi yavaşlatma ve grev gibi eylemlere katılmak veya bu amaçlarla toplu olarak göreve gelmemek, bunları tahrik ve teşvik etmek veya yardımda bulunmak,)
- b) Yasaklanmış her türlü yayını veya siyasi veya ideolojik amaçlı bildiri, afiş, pankart, bant ve benzerlerini basmak, çoğaltmak, dağıtmak veya bunları kurumların herhangi bir yerine asmak veya teşhir etmek,
- c) Siyasi partiye girmek,
- d) Özürsüz olarak (...) bir yılda toplam 20 gün göreve gelmemek,
- e) Savaş, olağanüstü hal veya genel afetlere ilişkin konularda amirlerin verdiği görev veya emirleri yapmamak,

- f) (Değişik: 13/2/2011 - 6111/111 md.) Amirlerine, maiyetindekilere ve iş sahiplerine fiili tecavüzde bulunmak,
- g) Memurluk sıfatı ile bağdaşmayacak nitelik ve derecede yüz kızartıcı ve utanç verici hareketlerde bulunmak,
- h) Yetki almadan gizli bilgileri açıklamak,
- ı) Siyasi ve ideolojik eylemlerden arananları görev mahallinde gizlemek,
- j) Yurt dışında Devletin itibarını düşürecek veya görev haysiyetini zedeleyecek tutum ve davranışlarda bulunmak,
- k) 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkındaki Kanuna aykırı fiilleri işlemek.
- l) (Ek: 3/10/2016 - KHK-676/75 md.; Aynen kabul: 1/2/2018-7070/61 md.) Terör örgütleriyle eylem birliği içerisinde olmak, bu örgütlere yardım etmek, kamu imkân ve kaynaklarını bu örgütleri desteklemeye yönelik kullanmak ya da kullandırmak, bu örgütlerin propagandasını yapmak.”

12. 62. maddesiyle 663 sayılı Kanun Hükmünde Kararname'ye (KHK) eklenen 45/A maddesi şöyledir:

“Sözleşmeli sağlık personeli istihdamı

MADDE 45/A- (Ek: 3/10/2016-KHK-676/76 md.; Aynen kabul: 1/2/2018-7070/62 md.)

(1) Bakanlık ve bağlı kuruluşları, merkez teşkilatları hariç olmak üzere ve öncelikle personel istihdamında güçlük çekilen yerlerde, 657 sayılı Devlet Memurları Kanununun 4 üncü maddesinin (B) fıkrası uyarınca ilgili mevzuatı gereği kura ile ataması öngörülenler dışında 190 sayılı Kanun Hükmünde Kararnameye ekli cetvellerde Sağlık Hizmetleri ve Yardımcı Sağlık Hizmetleri Sınıfı kapsamında yer alan unvanlarla vize edilmiş pozisyonlarda bu maddede öngörülen şartlarla sözleşmeli personel istihdam edebilir.

(2) Bu kapsamdaki sözleşmeli sağlık personeli Kamu Personel Seçme Sınavı (KPSS) sonucuna göre Bakanlık ve bağlı kuruluşlarına Öğrenci Seçme ve Yerleştirme Merkezi (ÖSYM) Başkanlığı tarafından yapılacak yerleştirme ile atanabileceği gibi pozisyon ve ihtiyaç durumuna göre KPSS puanı esas alınarak Bakanlık tarafından yapılacak sözlü sınavla da atama yapılabilir. Sözlü sınav ve yerleştirmeye ilişkin usul ve esaslar Bakanlıkça belirlenir.

(3) Bu madde uyarınca atanan sözleşmeli sağlık personeli dört yıl süreyle başka bir yere atanamaz. Aile birliği mazeretine bağlı yer değiştirmelerde bu madde uyarınca istihdam edilen personelin eşi bu personele tabidir. Ancak sözleşmeli sağlık personelinin bulunduğu ilde bir yıl görev yapması ve vizeli pozisyon bulunması durumunda; eşlerin her ikisinin de Bakanlık ve bağlı kuruluşlarında

sözleşmeli veya eşlerden birinin sözleşmeli, diğerinin Bakanlık ve bağlı kuruluşlarında veya diğer bir kamu kurum veya kuruluşunda kadrolu statüde istihdam ediliyor olması halinde hizmet ihtiyacının daha fazla olduğu yere atamaları yapılabilir.

(4) Sözleşmeli sağlık personelinden dört yıllık çalışma süresini tamamlayanlar talepleri halinde buldukları yerde 657 sayılı Kanunun 4 üncü maddesinin (A) bendi kapsamındaki kadrolara atanır. Bu kadrolara atananlar, aynı yerde en az iki yıl daha görev yapar, bunlar hakkında adaylık hükümleri uygulanmaz.

(5) Bu madde hükümlerine göre kadrolara atananların, 657 sayılı Kanunun 4 üncü maddesinin (B) bendi uyarınca sözleşmeli pozisyonlarda geçirdikleri hizmet süreleri, öğrenim durumlarına göre yükselebilecekleri dereceleri aşmamak kaydıyla kazanılmış hak aylık derece ve kademelerinin tespitinde değerlendirilir.

(6) Bu madde kapsamında memur kadrolarına atananlara iş sonu tazminatı ödenmez. Bu personelin önceden iş sonu tazminatı ödenmiş süreleri hariç, iş sonu tazminatına esas olan toplam hizmet süreleri, 8/6/1949 tarihli ve 5434 sayılı Türkiye Cumhuriyeti Emekli Sandığı Kanunu ve 31/5/2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu hükümleri uyarınca ödenecek emekli ikramiyesine esas toplam hizmet süresinin hesabında dikkate alınır.

(7) Bu madde çerçevesinde sözleşmeli personelin atanacağı memur kadroları, 190 sayılı Kanun Hükmünde Kararnameye ekli cetvellerde yer alan sınıf, unvan ve derecelerine uygun olmak şartıyla, başka bir işleme gerek kalmaksızın atama işleminin yapıldığı tarih itibarıyla ihdas edilerek ilgisine göre Bakanlık veya bağlı kuruluşlarının 190 sayılı Kanun Hükmünde Kararnameye ekli cetvellerinin ilgili bölümlerine eklenmiş ve kadrolara atananların pozisyonları başka bir işleme gerek kalmaksızın iptal edilmiş sayılır. İhdas edilen kadrolar ile iptal edilen pozisyonlar; unvanı, sınıfı, adedi, derecesi, teşkilatı ve birimi belirtilmek suretiyle atama tarihinden itibaren iki ay içinde Hazine ve Maliye Bakanlığı ve Devlet Personel Başkanlığına bildirilir.

(8) Bu madde kapsamında sözleşmeli sağlık personeli pozisyonlarına yapılan atama, sözleşmenin imzalanmasıyla geçerlilik kazanır. Sözleşme, imzalanmadan herhangi bir hak doğurmaz.”

13. 73. maddesiyle 3713 sayılı Kanun'a eklenen geçici 16. madde şöyledir:

“Geçici Madde 16- (Ek: 3/10/2016-KHK-676/90 md.; Aynen kabul: 1/2/2018-7070/73 md.)

Bu maddenin yürürlüğe girdiği tarih itibarıyla 21 inci maddenin birinci fıkrasının mülga (1) bendi kapsamında Yüksek Öğrenim Kredi ve Yurtlar Kurumundan burs almakta olanların bursları, normal öğrenim sürelerinin sonuna kadar ilgili mevzuat hükümlerine göre verilir. Söz konusu bende

istinaden yargı mercilerinde Yüksek Öğrenim Kredi ve Yurtlar Kurumu aleyhine açılan davalardan feragat edilmiş sayılır. Feragat nedeniyle mahkemece yargılama giderleri ve vekalet ücretine hükmedilemez, verilmiş olan kararlar üzerine ayrıca herhangi bir işlem yapılmaz.”

II. İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Zühtü ARSLAN, Burhan ÜSTÜN, Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ, Nuri NECİPOĞLU, Hicabi DURSUN, M. Emin KUZ, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Rıdvan GÜLEÇ, Recai AKYEL ve Yusuf Şevki HAKYEMEZ'in katılımlarıyla 17/5/2018 tarihinde yapılan ilk inceleme toplantısında dosyada eksiklik bulunmadığından işin esasının incelenmesine, yürürlüğü durdurma talebinin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

III. ESASIN İNCELENMESİ

2. Dava dilekçesi ve ekleri, Raportör Fatih ŞAHİN tarafından hazırlanan işin esasına ilişkin rapor, dava konusu kanun hükümleri, dayanan ve ilgili görülen Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A. Olağanüstü Hâl Düzenlemelerinin Yargısal Denetimi

3. Anayasa'nın 21/1/2017 tarihli ve 6771 sayılı Türkiye Cumhuriyeti Anayasasında Değişiklik Yapılmasına Dair Kanun'la değiştirilmeden önceki 148. maddesinin birinci fıkrasının üçüncü cümlesinde "...olağanüstü hallerde, sıkıyönetim ve savaş hallerinde çıkarılan kanun hükmünde kararnamelerin şekil ve esas bakımından Anayasaya aykırılığı iddiasıyla, Anayasa Mahkemesinde dava açılmaz" hükmüne yer verilerek olağanüstü dönem kanun hükmünde kararnameleri (KHK) Anayasa Mahkemesinin yargısal denetiminin dışında bırakılmıştır. Anayasa Mahkemesi 2/11/2016 tarihli ve E.2016/171, K.2016/164 sayılı kararında olağanüstü hâl KHK'larının Anayasa Mahkemesi tarafından denetlenebilmesi için bu yöndeki bir anayasal yetkinin açıkça tanınması gerektiğini ifade ederek Anayasa'nın 148. maddesinin lafzı, Anayasa koyucunun amacı ve ilgili yasama belgeleri gözönünde bulundurulduğunda olağanüstü hâl KHK'larının herhangi bir ad altında yargısal denetiminin mümkün olmadığına karar vermiştir.

4. Bununla birlikte olağanüstü hâl KHK'larının Türkiye Büyük Millet Meclisi (TBMM) tarafından onaylanarak kanunlaşması hâlinde bu kanun hükümlerinin Anayasa'ya aykırılığı iddiasıyla Anayasa Mahkemesinde dava açılmasının önünde bir engel bulunmamaktadır. İptal davasına konu edilen 7070 sayılı Kanun, olağanüstü hâl kapsamında çıkarılan 676 sayılı KHK'nın TBMM tarafından

onaylanması sonucunda yürürlüğe girmiştir. Bu itibarla dava konusu kurallar diğer kanun hükümleri gibi Anayasa Mahkemesinin denetimine tabi olmakla birlikte bu denetim yapılırken söz konusu kuralların olağanüstü hâle yönelik düzenlemeler içermesi nedeniyle öncelikle inceleme yönteminin belirlenmesi gerekir.

5. Anayasa, temel hak ve özgürlüklerin korunmasına ilişkin olarak olağan ve olağanüstü dönemler için iki ayrı hukuki rejim öngörmektedir. Olağan dönemde temel hak ve özgürlüklerin sınırlandırılması rejimi Anayasa'nın 13. maddesinde düzenlenmişken olağanüstü dönemde temel hak ve özgürlüklerin sınırlandırılması ya da kullanılmasının durdurulması rejimi Anayasa'nın 15. maddesinde düzenlenmiştir.

6. Anayasa'nın 13. maddesine göre "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlandırılabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz."

7. Anayasa'nın 15. maddesine göre ise "Savaş, seferberlik veya olağanüstü hallerde, milletlerarası hukuktan doğan yükümlülükler ihlâl edilmemek kaydıyla, durumun gerektirdiği ölçüde temel hak ve hürriyetlerin kullanılması kısmen veya tamamen durdurulabilir veya bunlar için Anayasada öngörülen güvencelere aykırı tedbirler alınabilir./ Birinci fıkrada belirlenen durumlarda da, savaş hukukuna uygun fiiller sonucu meydana gelen ölümler dışında, kişinin yaşama hakkına, maddî ve manevî varlığının bütünlüğüne dokunulamaz; kimse din, vicdan, düşünce ve kanaatlerini açıklamaya zorlanamaz ve bunlardan dolayı suçlanamaz; suç ve cezalar geçmişe yürütülemez; suçluluğu mahkeme kararı ile saptanıncaya kadar kimse suçlu sayılamaz."

8. Olağan dönemde temel hak ve özgürlüklerin sınırlandırılmasına ilişkin ölçütler Anayasa'nın 13. maddesinde yer alırken savaş, seferberlik ve olağanüstü hâllerde hak ve özgürlüklerin sınırlandırılması hatta kullanılmasının durdurulması özel olarak Anayasa'nın 15. maddesinde düzenlenmiştir. Buna göre savaş, seferberlik veya olağanüstü hâllerde temel hak ve özgürlüklerin kullanılmasının kısmen veya tamamen durdurulması ve bunlar için Anayasa'nın diğer maddelerinde öngörülen güvencelere aykırı tedbirler alınması mümkündür. Ancak Anayasa'nın 15. maddesiyle bu hususta tanınan yetki de sınırsız değildir. Anayasa'nın diğer maddelerinde öngörülen güvencelere aykırı tedbirlerin milletlerarası hukuktan doğan yükümlülükleri ihlal etmemesi ve durumun gerektirdiği ölçüde olması gerekmektedir. Ayrıca bu durumlarda dahi kişinin yaşam hakkına, maddi ve manevi varlığının bütünlüğüne dokunulması, din, vicdan, düşünce ve kanaatlerini açıklamaya

zorlanması ve bunlardan dolayı suçlanması yasaklanmış; suç ve cezaların geriye yürümemesi ilkesi ile masumiyet karinesinin bu hâllerde de geçerli olduğu kabul edilmiştir.

9. Olağanüstü hâl yönetim usullerine başvurulmasındaki temel amaç, bu yönetim rejiminin uygulanmasına neden olan tehdit veya tehlikelerin bertaraf edilmesini sağlamaktır. Devletin veya toplumun varlığının ya da kamu düzeninin ağır tehdit veya tehlikeler altında bulunması nedeniyle olağanüstü yönetim usulünün uygulandığı dönemlerde söz konusu tehdit veya tehlikelerin bertaraf edilmesi için temel hak ve özgürlüklerin olağan döneme kıyasla daha fazla sınırlandırılması sonucunu doğuran tedbirler alınması gerekebilir. Bu nedenle Anayasa'nın 15. maddesinin uygulanabilmesi için kuralın olağanüstü hâlin gerekli kıldığı durumla ilgisinin bulunması gerekir.

10. Olağanüstü hâl KHK'larının kanunlaşmasından sonra bu kanun hükümlerinin Anayasa'ya uygunluğunun denetlenmesinde ilgili kuralın tabi olduğu sınırlama rejimi tespit edilmelidir. Zira söz konusu düzenlemelerde olağanüstü hâl ile ilgili kuralların yanında olağanüstü hâl ile ilgili olmayan kurallara da yer verilebilmesi bu tespitin yapılmasını zorunlu kılmaktadır.

11. Kanunlaştırılarak yargısal denetime açılan bir kuralın Anayasa'nın olağanüstü dönem için öngördüğü denetim rejimine tabi olabilmesi için kural, olağanüstü hâlin ilanına sebep olan tehdit veya tehlikelerin bertaraf edilmesine yönelik olmalı ve olağanüstü hâl süresiyle sınırlı uygulanmalıdır. Dolayısıyla ancak bu iki niteliği taşıyan bir kuralın Anayasa'ya uygunluk denetiminde olağanüstü hâllerde temel hak ve özgürlüklerin kullanılmasının sınırlandırılması ve durdurulmasını düzenleyen Anayasa'nın 15. maddesi esas alınabilir.

12. Kuralın olağanüstü hâlin ilanına neden olan tehdit veya tehlikelerin bertaraf edilmesine yönelik olmadığı ya da olağanüstü hâlin süresini aştığı durumlarda ise söz konusu kuralın Anayasa'ya uygunluk denetiminde Anayasa'nın 15. maddesi dikkate alınamaz. Bu durumda kurala ilişkin inceleme sınırlamaya konu hakkın düzenlendiği Anayasa maddesi başta olmak üzere Anayasa'nın ilgili hükümleri ile olağan dönemde hak ve özgürlükleri sınırlama ve güvence rejimi bakımından temel öneme sahip olan Anayasa'nın 13. maddesi bağlamında yapılmalıdır. Ancak buradaki anayasallık denetiminde varılan sonuç böyle bir düzenlemenin olağanüstü dönemde dahi yapılamayacağı şeklinde anlaşılabilir.

13. Dava konusu kuralların olağanüstü hâl süresince uygulanma özelliğini aşan bir niteliğe sahip oldukları anlaşılmaktadır. Nitekim kurallar olağan dönemde geçerli olan kanunlarda değişiklik yaptığından sürekli bir etkiye sahiptir. Bu durum kurallara olağanüstü hâlin dışına taşan genel düzenleme niteliği vermektedir. Bu nedenle kuralların anayasallık denetiminde Anayasa'nın olağanüstü hâllerde temel hak ve özgürlüklerin sınırlandırılması rejimini düzenleyen 15. maddesi

uygulama alanı bulamaz. Kurallara ilişkin incelemenin sınırlama yapılan hakkın düzenlendiği Anayasa maddesi başta olmak üzere Anayasa'nın ilgili diğer hükümleri ve olağan dönemde hak ve özgürlükleri sınırlama ve güvence rejimi bakımından temel öneme sahip olan Anayasa'nın 13. maddesi bağlamında yapılması gerekir.

B. Kanun'un 1. Maddesiyle 5271 Sayılı Kanun'un 149. Maddesinin (2) Numaralı Fıkrasına Eklenen Cümlelerin İncelenmesi

1. İptal Talebinin Gerekçesi

14. Dava dilekçesinde özetle; sanığın dilediği sayıda müdafiden yararlanma hakkının silahların eşitliği ilkesinin bir gereği olduğu, dava konusu kuralla örgüt faaliyeti çerçevesinde işlenen suçlar bakımından yürütülen kovuşturmalarda, duruşmada avukat sayısına sınırlama getirilmesinin makul bir gerekçesinin bulunmadığı, daha ağır suçlar bakımından dahi böyle bir sınırlama yokken örgüt suçları bakımından müdafî yardımından yararlanma hakkına sınırlama getirilmesinin hak arama özgürlüğünü ölçsüz şekilde sınırlandırdığı belirtilerek kuralın Anayasa'nın 2., 13. ve 36. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

15. Dava konusu kuralda, örgüt faaliyeti çerçevesinde işlenen suçlar bakımından yürütülen kovuşturmalarda, duruşmada en çok üç avukatın hazır bulunabileceği hüküm altına alınmıştır.

16. Anayasa'nın 2. maddesinde belirtilen hukuk devleti; eylem ve işlemleri hukuka uygun, insan haklarına saygılı, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adil bir hukuk düzeni kurup bunu geliştirerek sürdüren, hukuki güvenliği sağlayan, Anayasa'ya aykırı durum ve tutumlardan kaçınan, hukuk kurallarıyla kendini bağlı sayan ve yargı denetimine açık olan devlettir.

17. Anayasa'nın 36. maddesinin birinci fıkrasında "Herkes, meşru vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir" denilerek yargı organlarına davacı ve davalı olarak başvurabilme hakkı ve bunun doğal sonucu olarak da iddia, savunma ve adil yargılanma hakkı güvence altına alınmıştır.

18. Ceza yargılamasında savunma hakkının güvence altına alınması, hukuk devletinin temel ilkelerindedir. Savunma, ceza adaletinin hakkaniyete uygun olarak gerçekleşmesini sağlayan öğelerden biridir.

19. Savunma hakkının sağladığı güvenceler esasen adil yargılanma hakkı içinde yer almaktadır. Savunma hakkı, hukuk devleti ilkesinin gereklerinden ve adil yargılanma hakkının önemli

güvencelerinden biri olması nedeniyle Anayasa'nın 36. maddesinde açıkça ifade edilmiştir. Anılan hükümde, herkesin meşru vasıta ve yollardan faydalanmak suretiyle savunma hakkına sahip olduğu belirtilmiştir.

20. Şüpheli ve sanığa salt savunma hakkının tanınması yeterli değildir. Şüpheli ve sanığın savunma için Anayasa'nın 36. maddesinde belirtilen meşru vasıta ve yollardan yararlandırılması da gerekir. Savunmada başvurulacak meşru vasıta ve yollar arasında avukatların teknik bilgilerinden ve tecrübelerinden yararlanma imkânı da bulunmaktadır. Bu itibarla müdafî yardımından yararlanma adil yargılanma hakkının kapsam ve içeriğine dâhil ve bu hakkın doğal sonucudur. Dolayısıyla suç isnadı altındaki kişi, adil yargılanma hakkı kapsamında kendisini bizzat savunma veya seçeceği bir müdafinin yardımından yararlanma hakkına sahiptir.

21. Diğer yandan Anayasa'nın 36. maddesine "...adil yargılanma..." ibaresinin eklenmesine ilişkin gerekçede, taraf olduğumuz uluslararası sözleşmelerle de güvence altına alınan adil yargılanma hakkının madde metnine dâhil edildiği vurgulanmıştır. Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) 6. maddesinin (3) numaralı fıkrasının (c) bendinde; bir suç ile itham edilen herkesin kendisini bizzat savunma veya seçeceği bir müdafinin yardımından yararlanma, eğer avukat tutmak için gerekli maddi imkânlardan yoksun ise ve adaletin yerine gelmesi için gerekli görüldüğünde resen atanacak bir avukatın yardımından ücretsiz olarak yararlanabilme hakkı düzenlenmiştir.

22. Anayasa'nın 13. maddesine göre "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz." Buna göre adil yargılanma hakkına sınırlama getiren kanuni düzenlemelerin Anayasa'da öngörülen sınırlama sebebine uygun ve ölçülü olması gerekir.

23. Anayasa'nın 36. maddesinde, adil yargılanma hakkı için herhangi bir sınırlama nedeni öngörülmemiş olmakla birlikte özel sınırlama nedeni öngörülmemiş hakların da hakkın doğasından kaynaklanan bazı sınırlarının bulunduğu kabul edilmektedir. Öte yandan Anayasa'nın başka maddelerinde yer alan kurallara dayanarak da bu hakların sınırlandırılması mümkündür. Bu bağlamda adil yargılanma hakkının kapsamı belirlenirken davaların mümkün olan süratle sonuçlandırılmasını öngören Anayasa'nın 141. maddesinin de gözetilmesi gerekmektedir. Ancak adil yargılanma hakkına getirilen sınırlamalar hiçbir şekilde Anayasa'nın 13. maddesinde yer alan güvencelere aykırı olamaz.

24. Anayasa'nın 13. maddesinin önemli güvencelerinden olan ölçülülük ilkesi elverişlilik, gereklilik ve orantılılık olmak üzere üç alt ilkedен oluşmaktadır. Elverişlilik, öngörülen sınırlamanın ulaşılma istenen amacı gerçekleştirmeye elverişli olmasını; gereklilik, ulaşılma istenen amaç bakımından sınırlamanın zorunlu olmasını, diğеr bir ifadeyle aynı amaca daha hafif bir sınırlama ile ulaşılmasının mümkün olmamasını; orantılılık ise hakka getirilen sınırlama ile ulaşılma istenen amaç arasında makul bir denge nin gözetilmesi gerekliliğini ifade etmektedir.

25. Ceza yargılamasının asıl amacı maddi gerçeğe ulaşılmasıdır. Maddi gerçeğe ulaşılabilmesinin önemli şartlarından birini de adil ve etkin bir şekilde yürütülen ceza kovuşturması oluşturmaktadır. Ceza yargılamasında soruşturma ve kovuşturma evreleri bir bütün olup adil yargılanma hakkı her iki evre yönünden de geçerlidir. Savunma hakkının etkin bir şekilde kullanılması, maddi gerçeğin ortaya çıkarılması ve dolayısıyla etkin kovuşturma bakımından önemlidir. Bu bağlamda savunma hakkının etkin bir şekilde kullanılmasına hizmet eden müdafî yardımından yararlanma hakkı maddi gerçeğe ulaşma amacına da hizmet eder. Başka bir ifadeyle sanığın müdafîi vasıtasıyla kendini savunması, adil bir yargılamaya ve bu yargılama sonucunda verilecek hükmün maddi gerçeğe örtüşmesine katkı yapar.

26. 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun "Tanımlar" başlıklı 6. maddesinin (1) numaralı fıkrasının (j) bendinde, örgüt mensubu suçlu bir suç örgütünü kuran, yöneten, örgüte katılan veya örgüt adına diğеrleriyle birlikte veya tek başına suç işleyen kişi olarak tanımlanmış; 220. maddesinin (1) numaralı fıkrasında, Kanun'un suç saydığı fiilleri işlemek amacıyla örgüt kuranların veya yönetenlerin -örgütün yapısı, sahip bulunduğu üye sayısı ile araç ve gereç bakımından amaç suçları işlemeye elverişli olması hâlinde- iki yıldan altı yıla kadar hapis cezası ile cezalandırılacağı ancak örgütün varlığı için üye sayısının en az üç olması gerektiği belirtilmiştir. Buna göre Kanun'un suç saydığı fiilleri işlemek amacıyla en az üç kişi tarafından kurulan örgütün amacı kapsamında işlenen suçlar örgütlü suçlar kategorisindedir.

27. Dava konusu kuralla örgütlü suçlara ilişkin duruşmalarda avukat sayısı üçle sınırlandırılmıştır. Böylece örgüt kapsamında suç işlediği iddia edilen her bir sanık duruşmada en fazla üç avukatla temsil edilebilecektir.

28. Kural örgütlü suçlar yönünden duruşmada müdafî yardımından yararlanma hakkına bir sınırlama getirmekle birlikte sınırlamanın söz konusu suçların niteliği dikkate alınarak öngörüldüğü anlaşılmaktadır. Bu suçlar kapsamında yürütülen soruşturma ve kovuşturmalarda fail sayısının çok olması ve olayın organize ve karmaşık yapısı nedeniyle yargılama süreleri diğеr suçlara göre daha fazla olabilmektedir. Kanun koyucunun da yargılamanın makul sürede sonuçlanması için

duruşmalarda avukat sayısını sınırladığı anlaşılmaktadır. Müdafî sayısının fazlalığı ve bu yüzden davaların uzaması diğer suçlar yönünden de söz konusu olabilir. Ancak örgütlü suçlarda sanık sayısının fazlalığı gözönünde bulundurulduğunda duruşmaların uzaması olasılığı diğer davalara nazaran daha yüksektir. Dolayısıyla kuralın örgütlü suçlarda yargılamanın makul sürede sonuçlandırılması amacına ulaşılması bakımından elverişli ve gerekli olmadığı söylenemez.

29. Öte yandan kuralla müdafî yardımından yararlanma hakkına getirilen sınırlama, duruşmada hazır bulunabilecek avukat sayısına ilişkindir. Kuralda müdafilerin hak ve yetkileri ile sanıkların müdafilerin yardımından yararlanma güvenceleri bakımından veya duruşma dışında müdafî yardımından yararlanma bakımından herhangi bir sınırlama söz konusu değildir. Buna göre kuralla ulaşılacak istenen amaca ilişkin kamu yararı ile bireyin müdafiden yararlanma hakkı arasında makul bir dengenin gözetildiği anlaşılmaktadır. Bu itibarla örgütlü suçlara ilişkin duruşmalarda avukat sayısını üçle sınırlandıran kuralın orantısız bir müdahaleye de neden olmadığı, dolayısıyla müdafî yardımından yararlanma hakkına ölçüsüz bir sınırlama getirmediği sonucuna ulaşılmıştır.

30. Açıklanan nedenlerle kural Anayasa'nın 2., 13. ve 36. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

C. Kanun'un 2. Maddesiyle 5271 Sayılı Kanun'un 151. Maddesinin (4) Numaralı Fıkrasına Eklenen "...avukat hakkındaki soruşturma veya..." ile "...soruşturma veya..." İbarelerinin İncelenmesi

1. Anlam ve Kapsam

31. Müdafilik görevinden yasaklanma 5271 sayılı Kanun'un 151. maddesinde düzenlenmiştir. Maddenin (3) numaralı fıkrasında, 5237 sayılı Kanun'un 220. ve 314. maddelerinde sayılan suçlar ile terör suçlarından şüpheli, sanık veya hükümlü olanların müdafilik veya vekillik görevini üstlenen avukatın, kendisi hakkında anılan suçlar nedeniyle soruşturma ya da kovuşturma bulunması hâlinde müdafilik veya vekillik görevini üstlenmekten yasaklanabileceği belirtilmiştir. 5237 sayılı Kanun'un 220. maddesinde suç işlemek amacıyla örgüt kurma, örgüte üye olma gibi örgüt suçları, 314. maddesinde de silahlı örgüt kurma, yönetme ve silahlı örgüte üye olma suçları düzenlenmiştir. Buna göre avukat hakkında müdafilik görevinden yasaklama kararı verilebilmesi için öncelikle müdafilik görevini üstlendiği kişinin örgüt veya silahlı örgüt ya da terör suçlarından şüpheli, sanık veya hükümlü olması gerekmektedir. Avukatın müdafilikten yasaklanması için ikinci şart ise kendisi hakkında anılan suçlardan dolayı soruşturma veya kovuşturma açılmış olmasıdır.

32. 5271 sayılı Kanun'un 151. maddesinin (3) numaralı fıkrasında müdafilikten yasaklama kararı verilebilmesi için şüpheli/sanık/hükümlü ve avukatın aynı soruşturma veya kovuşturma kapsamında

suç işlemiş olması gerektiğine ilişkin bir düzenleme yer almamaktadır. Dolayısıyla yasaklama kararı verebilmek için şüpheli/sanık/hükümlü ile avukatın aynı suç kapsamında soruşturma veya kovuşturma geçirmesine gerek bulunmamaktadır.

33. Anılan maddenin (4) numaralı fıkrasında, Cumhuriyet savcısının yasaklamaya ilişkin talebi hakkında hâkim veya mahkeme tarafından gecikmeksizin karar verileceği hüküm altına alınmıştır. Buna göre müdafilikten yasaklama kararı verilebilmesi için öncelikle Cumhuriyet savcısının bu konuda talepte bulunması zorunludur. Mahkeme veya hâkimin resen yasaklama kararı verme yetkisi yoktur.

34. Söz konusu fıkra, müdafilikten yasaklama kararlarına karşı itiraz edilebileceği de belirtilmiştir. Burada itiraz mercii, yasaklama kararının koşullarının gerçekleşip gerçekleşmediğini değerlendirmenin yanı sıra mahkemenin yasaklama kararı verirken takdir yetkisini hukuka uygun şekilde kullanıp kullanmadığını da denetleyecektir.

35. Fıkra, müdafilik görevinden yasaklama kararının avukat hakkındaki kovuşturma konusu suçla sınırlı olmak üzere bir yıl süre ile verilebilmesi, kovuşturmanın niteliği itibarıyla bu sürelerin altı aydan fazla olmamak üzere en fazla iki defa uzatılması öngörülmekte iken fıkra, değişiklik yapılarak avukat hakkında (3) numaralı fıkra, sayılan suçlardan soruşturma açılmış olması da müdafilikten yasaklanma sebepleri arasında sayılmıştır. Kurala göre avukat hakkında örgüt veya silahlı örgüt suçlarından ya da terör suçlarından dolayı soruşturma açılmış olması durumunda da bir yıl süre ile müdafilikten yasaklama kararı verilebilecek ve bu süre soruşturmanın niteliği gözetilerek altı aydan fazla olmamak üzere en fazla iki defa uzatılabilecektir.

2. İptal Taleplerinin Gerekçesi

36. Dava dilekçesinde özetle; dava konusu kurullarla avukatlar hakkında müdafilik görevinden yasaklanma kararı verilebilmesi için bazı suçlardan dolayı haklarında soruşturma açılmasının yeterli görülmesinin yasaklılığın istisna olma özelliğini ortadan kaldırdığı, müdafilikten yasaklamayı kolaylaştırdığı ve yasaklamamanın sınırlarını genişlettiği belirtilerek kurulların Anayasa'nın Başlangıç kısmı ile 2. ve 36. maddelerine aykırı olduğu ileri sürülmüştür.

3. Anayasa'ya Aykırılık Sorunu

37. 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 43. maddesi uyarınca kurullar, ilgisi nedeniyle Anayasa'nın 13. ve 49. maddeleri yönünden de incelenmiştir.

38. Anayasa'nın 2. maddesinde güvence altına alınan hukuk devletinde kanunların kamu yararı gözetilerek çıkarılması zorunludur. Kanunların kamu yararının sağlanması amacına yönelik olması, genel, objektif, adil kurallar içermesi ve hakkaniyet ölçütlerini gözetmesi hukuk devleti olmanın gereğidir. Bu nedenle kanun koyucunun hukuki düzenlemelerde kendisine tanınan takdir yetkisini anayasal sınırlar içinde adalet, hakkaniyet ve kamu yararı ölçütlerini gözönünde tutarak kullanması gerekir.

39. Anayasa'nın 49. maddesinde; çalışmanın herkesin hakkı ve ödevi olduğu, devletin çalışanların hayat seviyesini yükseltmek, çalışma hayatını geliştirmek için çalışanları ve işsizleri korumak, çalışmayı desteklemek, işsizliği önlemeye elverişli ekonomik bir ortam yaratmak ve çalışma barışını sağlamak için gerekli tedbirleri alacağı belirtilmiştir.

40. Müdafilik görevinden yasaklama bir cezalandırma olmayıp özellikle örgütlü suçlar bakımından yargılamanın sağlıklı bir şekilde yürütülmesini amaçlayan bir yargılama tedbiridir. Dava konusu kurallar avukatların belli bir süre müdafilik görevinden yasaklanmasını öngördüğünden müdafi ile temsil edilen kişiler bakımından müdafi yardımından yararlanma hakkına; müdafilik görevinden yasaklama kararı verilen avukat bakımından ise çalışma hakkına sınırlama getirmektedir.

41. Anayasa'nın 5. maddesinde demokrasiyi korumak, kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak, kişinin temel hak ve hürriyetlerini, sosyal hukuk devleti ve adalet ilkeleriyle bağdaşmayacak surette sınırlayan siyasal, ekonomik ve sosyal engelleri kaldırmaya, insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak devletin temel amaç ve görevleri arasında sayılmıştır. Terörle ve örgütlü suçlarla mücadele ederek kişilerin ve toplumun huzur ve güvenliğini sağlamanın devletin yerine getirmekle yükümlü olduğu ödevler kapsamında kaldığında tereddüt bulunmamaktadır. Bu yönüyle millî güvenlik, kamu düzeni ve kamu güvenliğine yönelik önemli tehditler içeren terör suçlarının ve örgütlü suçların önlenmesi amacıyla adil yargılanma ve çalışma haklarına sınırlama getirilmesi mümkündür. Dava konusu kurullarla nihai olarak millî güvenlik, kamu düzeni ve kamu güvenliğinin korunmasının amaçlandığı, dolayısıyla kurulların anayasal olarak meşru bir nedenle Anayasa'nın 36. ve 49. maddelerinde belirtilen hakları sınırlandırdığı söylenebilir.

42. Ancak anayasal bağlamda meşru bir amaca sahip sınırlamaların da Anayasa'nın 13. maddesinde yer alan ölçülülükün alt ilkelerinden olan orantılılık ilkesine uygun olması gerekir. Orantılılık ilkesi kamu yararının korunması ile bireyin hak ve özgürlükleri arasında adil bir dengenin sağlanmasını gerekli kılmaktadır. Öngörülen tedbirin bireyi olağan dışı ve aşırı bir yük altına sokması durumunda

getirilen sınırlamanın orantılı ve dolayısıyla ölçülü olduğundan söz edilemez. Bu itibarla uygulanan tedbirle bireye aşırı ve orantısız bir yük yüklenmemesi gerekmektedir.

43. Avukat hakkında müdafilik görevinden yasaklama kararı verilebilmesi için müdafilik görevini üstlendiği kişinin 5237 sayılı Kanun'un 220. ve 314. maddeleri bağlamında örgüt veya silahlı örgüt suçları ya da terör suçlarından şüpheli, sanık veya hükümlü olması; avukat hakkında da anılan suçlardan dolayı soruşturma veya kovuşturma açılmış olması yeterlidir. Yasaklama kararı verebilmek için müvekkil ile avukatın aynı suç kapsamında soruşturma veya kovuşturma geçirmesine gerek yoktur. Bu bağlamda avukat hakkında yürütülen soruşturma ile müvekkili hakkında yürütülen soruşturma arasında herhangi bir bağlantı bulunmasa dahi Kanun'da belirtilen şartların gerçekleşmesi durumunda avukat hakkında söz konusu yasaklama kararı verilebilecektir.

44. Dava konusu kurallarla müdafilik görevinden yasaklama kararı verilebilmesi için avukat hakkında 5237 sayılı Kanun'un 220. ve 314. maddeleri bağlamında örgüt veya silahlı örgüt suçları ya da terör suçlarından dolayı soruşturma açılmış olması yeterli görülmüştür. Ceza muhakemesinde soruşturma aşaması yetkili mercilerce suç şüphesinin öğrenilmesinden iddianamenin kabulüne kadar geçen evredir. 5271 sayılı Kanun'un 160. maddesinin (1) numaralı fıkrasında Cumhuriyet savcısının, ihbar veya başka bir suretle bir suçun işlendiği izlenimini veren bir hâli öğrenir öğrenmez kamu davasını açmaya yer olup olmadığına karar vermek üzere hemen işin gerçeğini araştırmaya başlayacağı hüküm altına alınmıştır. Buna göre soruşturmaya başlamak için bir suçun işlendiği izlenimini veren bir hâl yeterlidir.

45. Bilgi ve deneyimlerini öncelikle adalet hizmetine vererek adalete ve hakkaniyete uygun çözümler için hukuk kurallarının tam olarak uygulanmasında yargı organlarıyla yetkili kurul ve kurumlara yardımcı olan avukatın hukuk devletinin yargı düzeni içindeki yeri özellik taşımaktadır. Savunma hakkının etkin şekilde kullanılmasına ve maddi gerçeğe ulaşma amacına hizmet eden müdafii, müdafilik görevini üstlendiği kişinin işlediği ileri sürülen suçla herhangi bir bağlantısı bulunmaksızın veya müdafilik görevini kötüye kullandığına ilişkin herhangi bir olgu mevcut olmaksızın basit bir suç şüphesi nedeniyle müdafilik görevinden yasaklanmasına imkân tanıyan kurallar, müdafii yardımından yararlanma ve çalışma hakkı bağlamında bireyi olağan dışı ve aşırı bir yük altına sokmakta; dolayısıyla müdafii yardımından yararlanma ve çalışma hakkına orantısız bir sınırlama getirmektedir.

46. Bu itibarla söz konusu kurallar anılan haklar bağlamında ölçülülük ilkesini ihlal ettiği gibi hukuk devletinin adalet ve hakkaniyet ilkeleriyle de bağdaşmamaktadır.

47. Açıklanan nedenlerle kurallar Anayasa'nın 2., 13., 36. ve 49. maddelerine aykırıdır. İptalleri gerekir.

Kuralların Anayasa'nın Başlangıç kısmıyla ilgisi görülmemiştir.

Ç. Kanun'un 3. Maddesiyle 5271 Sayılı Kanun'un 154. Maddesine Eklenen (2) Numaralı Fıkırdaki Yer Alan "...örgüt faaliyeti çerçevesinde işlenen uyuşturucu ve uyarıcı madde imâl ve ticareti suçları..." İbaresinin İncelenmesi

1. İptal Talebinin Gerekçesi

48. Dava dilekçesinde özetle; dava konusu kuralla örgüt faaliyeti çerçevesinde işlenen uyuşturucu madde imal ve ticareti suçları bakımından soruşturma aşamasında müdafii ile görüşmeye yirmi dört saat süreyle kısıtlama getirilmesinin makul bir gerekçesinin bulunmadığı, suçun ağırlığı nedeniyle henüz soruşturma aşamasında şüphelinin haklarının sınırlandırılmasının peşin bir yaptırım görüntüsü oluşturduğu, bu durumun masumiyet karinesi ve hak arama hürriyetiyle bağdaşmadığı belirtilerek kuralın Anayasa'nın 2., 36. ve 38. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

49. 6216 sayılı Kanun'un 43. maddesi uyarınca kural, ilgisi nedeniyle Anayasa'nın 13. maddesi yönünden de incelenmiştir.

50. Kuralda; örgüt faaliyeti çerçevesinde işlenen uyuşturucu ve uyarıcı madde imal ve ticareti suçları bakımından gözaltındaki şüphelinin müdafii ile görüşme hakkının Cumhuriyet savcısının istemi üzerine hâkim kararıyla yirmi dört saat süreyle kısıtlanabileceği, bu zaman zarfında şüphelinin ifadesinin alınamayacağı hüküm altına alınmıştır.

51. Anayasa'nın 36. maddesinde, adil yargılanma hakkı kapsamında yer alan müdafii yardımından yararlanma hakkı için herhangi bir sınırlama nedeni öngörülmemiş olmakla birlikte özel sınırlama nedeni öngörülmemiş hakların da hakkın doğasından kaynaklanan bazı sınırlarının bulunduğu kabul edilmektedir. Öte yandan Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevler özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebilir. Devletin terörle mücadele ederek kişilerin ve toplumun huzur ve güvenliğini sağlamanın ve maddi gerçeğin ortaya çıkarılarak ceza adaletinin tesis edilmesinin de anayasal hükümler kapsamında devletin yerine getirmekle yükümlü olduğu ödevler kapsamında kaldığında tereddüt bulunmamaktadır. Bu yönüyle terör faaliyetlerinin önlenmesi ve ceza adaletinin sağlanması amacıyla adil yargılanma hakkı kapsamında yer alan müdafii yardımından yararlanma hakkına sınırlama getirilmesi mümkündür.

52. Örgüt faaliyeti çerçevesinde işlenen uyuşturucu ve uyarıcı madde imal ve ticareti suçlarının toplum düzeni yönünden ortaya çıkardığı tehdidin ağırlığı ile çok failli ve organize yapıları nedeniyle bu suçlara ilişkin delillerin ele geçirilmesi ve bu delillerin karartılmaması ayrı bir önem arz etmekte; söz konusu durum gözaltına alınan kişilerin belli bir süreyle dış dünyayla olan iletişimlerinin kesilmesini zorunlu kılabilmektedir. Kuralla getirilen sınırlamanın amacının örgüt faaliyeti çerçevesinde işlenen uyuşturucu ve uyarıcı madde imal ve ticareti suçlarına ilişkin soruşturmanın sağlıklı bir şekilde yürütülmesini sağlamak olduğu, böylece maddi gerçeğin ortaya çıkarılarak ceza adaletinin tesis edilmesinin ve terör faaliyetlerinin önlenmesinin hedeflendiği anlaşılmaktadır. Bu yönüyle kuralın örgütlü suçlara ilişkin soruşturmanın sağlıklı bir şekilde yürütülmesi bakımından elverişli ve gerekli olmadığı söylenemez.

53. Kuralda, gözaltına alınan kişinin yirmi dört saat süreyle müdafii ile görüşme hakkı sınırlandırılırken aynı zamanda bu süre boyunca şüphelinin ifadesinin alınması da yasaklanmıştır. Böylece şüphelilerin müdafilerinden hukuki yardım almaksızın ifade vermeleri önlenmiştir. Bu nedenle kuralla, soruşturmanın amacının tehlikeye düşmesinin önlenmesinin ve maddi gerçeğin ortaya çıkarılmasının amaçlandığını anlaşılmakta; anılan tedbir de sınırlama aracının sanık veya şüpheli üzerinde amacı dışında keyfi biçimde kullanılmasını engellemektedir.

54. Öte yandan kural gereği gözaltındaki kişinin yirmi dört saat süreyle müdafii ile görüşmesinin yasaklanmasının ancak hâkim kararıyla mümkün olması, gözaltındaki kişinin yirmi dört saat süreyle müdafii ile görüştürülmemesini haklı kılacak olguların varlığını gerektirdiğinden söz konusu yasaklamanın gereksiz yere kullanılmasını önlemektedir. Bu itibarla kuralın müdafii yardımından yararlanma hakkına orantısız bir müdahale oluşturduğu, dolayısıyla ölçüsüz olduğu söylenemez.

55. Maddi gerçeğin ortaya çıkarılarak ceza adaletinin tesis edilmesi ve terör faaliyetlerinin önlenmesi amacıyla öngörülen kural yukarıda açıklanan nedenlerle adalet ve hakkaniyet ölçütlerine de uygun olup hukuk devleti ilkesine aykırılık taşımamaktadır.

56. Açıklanan nedenlerle kural, Anayasa'nın 2., 13. ve 36. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

Kuralın Anayasa'nın 38. maddesiyle ilgisi görülmemiştir.

D. Kanun'un 4. Maddesiyle 5271 Sayılı Kanun'un 178. Maddesinin (1) Numaralı Fıkrasına Eklenen Cümlelerin İncelenmesi

1. İptal Talebinin Gerekçesi

57. Dava dilekçesinde özetle; ceza yargılamasının duruşma evresinde tanık veya uzman kişinin dinlenmesi talebinin savunma hakkının bir parçası olduğu, davayı uzatmak amacıyla yapılan tanık veya uzman dinletme taleplerinin reddedileceğini öngören kuralın savunma hakkını kullanılamaz hâle getirdiği, tanık ya da uzman kişi dinletme talebinin davayı uzatmak amacıyla yapıp yapılmadığının subjektif bir değerlendirme gerektirdiği, böyle bir yetkinin mahkemeye tanınmasının savunma hakkının keyfî şekilde sınırlandırılmasına sebebiyet vereceği belirtilerek kuralın Anayasa'nın 36. maddesine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

58. 6216 sayılı Kanun'un 43. maddesi uyarınca kural, ilgisi nedeniyle Anayasa'nın 13. maddesi yönünden de incelenmiştir.

59. 5271 sayılı Kanun'un 178. maddesinin (1) numaralı fıkrasının birinci ve ikinci cümlelerinde, mahkeme başkanı veya hâkim sanığın veya katılanın gösterdiği tanık ya da uzman kişinin çağrılması hakkındaki dilekçeyi reddettiğinde sanık veya katılanın o kişileri mahkemeye getirebileceği ve bu kişilerin duruşmada dinleneceği belirtilmiş; dava konusu üçüncü cümlesinde ise, davayı uzatmak amacıyla yapılan taleplerin reddedileceği hüküm altına alınmıştır.

60. Anayasa'nın 36. maddesinin birinci fıkrasında, herkesin adil yargılanma hakkına sahip olduğu belirtilmiş, ancak tanık dinletme hakkından açıkça söz edilmemiştir. Bununla birlikte adil yargılanma hakkının somut görünüşlerinden biri olan tanık dinletme hakkı esasen Anayasa'nın anılan maddesinde yer verilen adil yargılanma hakkının da zımni bir unsurudur (Ali Fırtına, B. No: 2014/14575, 6/7/2017, § 24).

61. Diğer yandan Anayasa'nın söz konusu maddesine "adil yargılanma" ibaresinin eklenmesine ilişkin gerekçede Türkiye'nin taraf olduğu uluslararası sözleşmelerle de güvence altına alınan adil yargılanma hakkının madde metnine dâhil edildiği vurgulanmıştır. AİHS'in 6. maddesinin (3) numaralı fıkrasının (d) bendinde; bir suç ile itham edilen herkesin iddia tanıklarını sorguya çekme veya çektirme, savunma tanıklarının da iddia tanıklarıyla aynı koşullar altında davet edilmelerinin ve dinlenilmelerinin sağlanmasını isteme hakkı düzenlenmiştir.

62. Tanık ve uzman kişilerin görüşlerine başvurulması da maddi gerçeğin ortaya çıkarılmasını sağlayan araçlar arasındadır. Bu yönüyle sanığın uyuşmazlık konusu olaya ilişkin bilgisi olanların tanıklığına veya uzman görüşüne başvurma hakkı bulunmaktadır. Ancak bu hak, sanığın lehine olan bütün tanıkların ve uzman kişilerin çağrılmasını ve dinlenilmesini gerektirmez. Önemli olan sanığın

aynı koşullar altında ve silahların eşitliği ilkesine uygun olarak tanık dinletme talebinde bulunabilmesinin sağlanmasıdır.

63. Kovuşturma evresinde kural olarak iddianamede gösterilen tanık ve uzman kişiler duruşmaya davet edilmekle birlikte sanık veya katılan da dava konusu olayla ilgili olarak dinlenilmesini istediği tanık veya uzman kişilerin duruşmaya çağrılmasını talep edebilir. 5271 sayılı Kanun'un 177. maddesinin (1) numaralı fıkrasında, sanığın tanık veya bilirkişinin davetini veya savunma delillerinin toplanmasını istediğinde bunların ilişkin olduğu olayları göstermek suretiyle bu husustaki dilekçesini duruşma gününden en az beş gün önce mahkeme başkanına veya hâkime vereceği belirtilmiş; 178. maddesinin (1) numaralı fıkrasında da mahkeme başkanı veya hâkim sanığın veya katılanın gösterdiği tanık veya uzman kişinin çağrılması hakkındaki dilekçeyi reddettiğinde sanık veya katılanın o kişileri mahkemeye getirebileceği ve bu kişilerin duruşmada dinlenileceği hüküm altına alınmıştır. Böylece sanık veya katılanın da dinlenilmesini talep ettiği tanık veya uzman kişilerin duruşmaya katılmasına imkân tanınmıştır.

64. Dava konusu kuralda ise sanık veya katılanın bu yöndeki taleplerinin davayı uzatmak amacıyla yapıldığının anlaşılması durumunda reddedileceği hüküm altına alınmıştır. Kurala göre tanık veya uzman kişi dinlenilmesine ilişkin taleplerin davayı uzatmak amacıyla yapıldığı anlaşılırsa bu talepler reddedilecektir.

65. Kuralda tanık ve uzman kişilerin dinlenilmesi taleplerinin reddine izin verilmesi ile adil yargılanma hakkına sınırlama getirildiği açıktır. Ancak Anayasa'nın 36. maddesinde güvenceye bağlanan adil yargılanma hakkının önemli unsurlarından biri de makul sürede yargılanma hakkıdır. Anayasa'nın 141. maddesinin son fıkrasında "Davaların en az giderle ve mümkün olan süratle sonuçlandırılması yargının görevidir" denilmek suretiyle davaların makul bir süre içinde bitirilmesi gerekliliği açıkça ifade edilmiştir. Bu hak gereğince devlet, yargılamaların gereksiz yere uzamasını engelleyecek etkin çareler oluşturmak zorundadır (AYM, E.2013/4, K.2013/35, 28/2/2013). Taraflarca dinlenilmesi talep edilen tüm tanık ve uzman kişilerin duruşmalarda dinlenilmesi yargılamanın gereksiz yere uzamasına sebebiyet verebilir. Bu yönüyle kanun koyucunun yargılamanın sürüncemede kalmasına yönelik talepleri önlemek suretiyle davaların makul sürede sonuçlandırılmasını sağlamak amacıyla tanık dinletme hakkına sınırlama getirmesi mümkündür.

66. Kuralla davayı uzatmak amacıyla yapılan tanık ve uzman kişi dinletme taleplerinin reddedileceği hüküm altına alınmakta olup getirilen sınırlamanın davaların makul sürede sonuçlandırılması bakımından elverişli ve gerekli olmadığı söylenemez.

67. Kuralda tanık ve uzman kişilerin dinlenilmesi talebine sınırlama getirilmekle birlikte bu hakkın kullanılmasının tümüyle engellenmesi söz konusu değildir. Tanık ve uzman kişilerin dinlenilmesi yönündeki taleplerin reddedilmesi, ancak davayı uzatmak amacıyla yapıldığının anlaşılması durumunda söz konusu olabilecektir. Öte yandan bu konuda yargı mercilerinin anılan yetkiyi keyfi bir şekilde kullanmasını engelleyecek güvencelere de yer verildiği görülmektedir. Bu çerçevede 5271 sayılı Kanun'un 272. maddesinin (2) numaralı fıkrasında, hükümden önce verilip hükme esas teşkil eden veya başka kanun yolu öngörülmemiş olan mahkeme kararlarına karşı hükümlerle birlikte istinaf yoluna başvurulabileceği açıkça düzenlenmiştir. Ayrıca hâkimin kendisine tanınan yetkiyi müdafî yardımından yararlanma hakkını etkisiz kılacak şekilde kullanıp kullanmadığı Anayasa Mahkemesine yapılan bireysel başvurularda da denetlenebilecektir. Bu yönleriyle tanık ve uzman kişilerin dinletilmesine getirilen sınırlamayla amaçlanan kamu yararı ile bireyin adil yargılanma hakkı arasındaki makul dengenin gözetildiği anlaşılmaktadır. Bu itibarla tanık veya uzman kişilerin dinletilmesi talebinin davayı uzatmak amacıyla yapıldığının anlaşılması durumunda anılan taleplerin reddedilmesine imkân tanıyan kuralın, adil yargılanma hakkına orantısız dolayısıyla ölçüsüz bir sınırlama getirdiği söylenemez.

68. Açıklanan nedenlerle kural, Anayasa'nın 13. ve 36. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

Celal Mümtaz AKINCI bu görüşe katılmamıştır.

E. Kanun'un 5. Maddesiyle 5271 Sayılı Kanun'un 188. Maddesinin (1) Numaralı Fıkrasına Eklenen Cümlelerin İncelenmesi

1. İptal Talebinin Gerekçesi

69. Dava dilekçesinde özetle; zorunlu müdafîin duruşmada hazır bulunmasının çelişmeli yargılama ve muhakemenin kolektifliği ilkesinin tabii bir sonucu olduğu, dava konusu kuralla müdafî olmadan duruşmaya devam edilmesine imkân tanınmasının adil yargılama hakkının unsurları olan çelişmeli yargılama ve silahların eşitliği ilkeleriyle bağdaşmadığı belirtilerek kuralın Anayasa'nın 36. maddesine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

70. Dava konusu kuralda müdafîin mazeretsiz olarak duruşmaya gelmemesi veya duruşmayı terk etmesi hâlinde duruşmaya devam edilebileceği hüküm altına alınmıştır.

71. Müdafî yardımından yararlanma hakkı savunma hakkının kullanılması ve maddi gerçeğin ortaya çıkarılması, dolayısıyla etkin kovuşturma bakımından büyük önem taşımakta; başka bir ifadeyle

sanığın müdafisi vasıtasıyla kovuşturma aşamasında kendini savunması, adil bir yargılamaya ve bu yargılama sonucunda verilecek hükmün maddi gerçekle örtüşmesine imkân sağlamaktadır.

72. Öte yandan müdafisi yardımından yararlanma hakkı savunma hakkının etkin bir şekilde kullanılmasını sağlayarak çelişmeli yargılama ve silahların eşitliği ilkelerine de hayat vermektedir. Sanığın suçlu olduğunun ispatlanmasında dahi müdafinin duruşmada hazır bulunarak yargılamanın hukuka uygun bir şekilde yapılmasını gözetme yetkisi bulunmaktadır. Ancak müdafisi yardımından yararlanma hakkı, müdafinin her duruşmada hazır bulunmasını zorunlu kılmamaktadır.

73. 5271 sayılı Kanun'un Üçüncü Kitap Birinci Kısım İkinci Bölümünde ceza muhakemesindeki duruşma süreci düzenlenmiştir. Bu çerçevede Kanun'un "Duruşmada hazır bulunacaklar" kenar başlıklı 188. maddesinin (1) numaralı fıkrasının birinci cümlesinde duruşmada hükme katılacak hâkimler ve Cumhuriyet savcısı ile zabıt kâtibinin ve Kanun'un zorunlu müdafiliği kabul ettiği hâllerde müdafinin hazır bulunmasının şart olduğu hükme bağlanmıştır. Bu kural uyarınca anılan kişilerden herhangi birinin bulunmaması hâlinde duruşma açılması ve bu çerçevede yargılama sonucuna etki edecek esaslı bir işlem olma niteliği taşıyorsa bile duruşmaya ilişkin herhangi bir işlemin yapılması mümkün değildir. Dava konusu kuralla ise anılan hükme zorunlu müdafisi yönünden bir istisna getirilmiş ve müdafinin mazeretsiz olarak duruşmaya gelmemesi veya duruşmayı terk etmesi hâlinde duruşmaya devam edilebileceği hüküm altına alınmıştır. Anılan istisna getirilirken 5271 sayılı Kanun'da müdafisi yardımından yararlanma hakkı yönünden söz konusu kurallarda herhangi bir değişiklik öngörülmemiş; bu bağlamda örneğin 5271 sayılı Kanun'un zorunlu müdafisi olmaksızın sanığın savunmasının alınamayacağını düzenleyen 150. ve 151. maddelerinde bir değişiklik yapılmamıştır. Bu itibarla dava konusu kuralla yapılan değişiklik sonrasında sanığın müdafisinin huzurunda savunması alınmaksızın yargılamanın tamamlanarak hüküm kurulması da mümkün değildir. Dolayısıyla dava konusu kuralın yargılamanın sonucuna etkili esaslı işlemlerin yapıldığı ve bu nedenle müdafisi yardımının etkili olduğu duruşmaların müdafisi yokluğunda yapılabilmesine imkân tanıdığı şeklinde anlaşılması mümkün değildir. Bu çerçevede dava konusu kuralla yapılan düzenlemenin anlam ve kapsamının 5271 sayılı Kanun'un konuyla ilgili diğer hükümleriyle birlikte değerlendirilerek ve özellikle Kanun'da yer alan müdafisi yardımından yararlanma hakkına ilişkin kurallar gözetilerek ortaya konulması gerekmektedir.

74. 5271 sayılı Kanun'un 150. maddesinin (1) numaralı fıkrasında, şüpheli veya sanıktan kendisine bir müdafisi seçmesinin isteneceği, müdafisi seçebilecek durumda olmadığını beyan eden şüpheli veya sanığa talebi hâlinde bir müdafisi görevlendirileceği belirtilmiş; maddenin (2) ve (3) numaralı fıkralarında ise sanık veya şüphelinin çocuk veya kendisini savunamayacak derecede malul ya da

sağır ve dilsiz olması durumunda talep aranmaksızın müdafî görevlendirileceği, ayrıca alt sınırı beş yıldan fazla hapis cezasını gerektiren suçlardan dolayı yapılan soruşturma ve kovuşturmada da aynı şekilde müdafî görevlendirileceği düzenlenerek devletin yargılamaların adil bir şekilde gerçekleştirilmesini sağlama yönündeki pozitif ödevi kapsamında bazı kanuni güvencelere yer verilmiştir.

75. Kanun'un 149. maddesinin (1) numaralı fıkrasında, şüpheli veya sanığın soruşturma ve kovuşturmanın her aşamasında müdafî yardımından yararlanabileceği belirtilmiş; (3) numaralı fıkrasında da soruşturma ve kovuşturma evrelerinin her aşamasında avukatın şüpheli veya sanıkla görüşme, ifade alma veya sorgu süresince yanında olma ve hukuki yardımda bulunma hakkının engellenemeyeceği ve kısıtlanamayacağı hüküm altına alınmıştır.

76. Müdafî görevini yerine getirmediğinde yapılacak işlemler ise Kanun'un 151. maddesinde düzenlenmiştir. Bu çerçevede 150. maddeye göre görevlendirilen müdafî, duruşmada hazır bulunmaz veya vakitsiz olarak duruşmadan çekilir ya da görevini yerine getirmekten kaçınırsa hâkim veya mahkeme derhâl başka bir müdafî görevlendirilmesi için gerekli işlemi yapacaktır. Bu durumda mahkeme oturuma ara verebileceği gibi oturumun ertelenmesine de karar verebilecektir. Eğer yeni müdafî savunmasını hazırlamak için yeterli zaman olmadığını açıklarsa oturum ertelenecektir.

77. Anılan hükümler bir bütün olarak dikkate alındığında zorunlu müdafîin bulunmadığı duruşmada yargılamanın sonucuna etki edebilecek nitelikteki hiçbir esaslı işlemin yapılmasının mümkün olmadığı sonucuna ulaşılmaktadır. Özellikle 151. maddenin (1) numaralı fıkrasında "...müdafî(in) ... vakitsiz olarak duruşmadan çekilme(si)..." ibaresine yer verilerek anılan durumda duruşmaya devam edilemeyeceğinin öngörülmesi ve aynı maddenin (2) numaralı fıkrasında yeni müdafî savunmasını hazırlamak için yeterli zamanının olmadığını açıkladığında oturumun ertelenmesine karar verilmesi zorunluluğunun bulunması anılan anlayışı teyit etmektedir. Öte yandan müdafî huzurunda yapılan duruşmalarda bile müdafînin görevini yapmaktan kaçındığı durumlarda duruşmaya devam edilemeyeceğinin hükme bağlandığı görülmektedir.

78. Söz konusu hükümler 5271 sayılı Kanun'un Birinci Kitabının "Savunma" başlıklı Altıncı Kısımının "Müdafî Seçimi, Görevlendirilmesi, Görev ve Yetkileri" başlıklı Birinci Bölümünde; dava konusu kural ise 5271 sayılı Kanun'un Üçüncü Kitap Birinci Kısımının "Duruşma" başlıklı İkinci Bölümünde yer alan 188. maddesinde düzenlenmiştir. Dava konusu kuralla birlikte bir önceki paragrafta belirtilen ve yargılamanın sonucuna etki edecek nitelikteki esaslı işlemlerin yapıldığı duruşmada zorunlu müdafî yardımından yararlanma hakkının sınırlanamayacağını öngören düzenlemelerde herhangi bir değişiklik yapılmamıştır. Dolayısıyla dava konusu kuralla veya ilişkili başka

düzenlemelerle anılan hükümlerin açık veya zımni olarak ilga edilmesi söz konusu olmayıp kuralın anlam ve kapsamının söz konusu hükümlerle birlikte değerlendirilerek belirlenmesi gerekmektedir. Kanun koyucunun istemesi hâlinde sanığın yargılama aşamasında müdafî yardımından yararlanma hakkını düzenleyen anılan kurallarda değişiklik yaparak zorunlu müdafî yardımından yararlanma hakkını sınırlandırması mümkün iken bu yola gitmeyerek sadece zorunlu müdafî olmaksızın duruşma yapılamayacağını düzenleyen kurala bir istisna getirmesi, dava konusu kuralın müdafî yardımından yararlanma hakkını zedelemeyecek nitelikteki işlemlerin yapıldığı duruşmanın yapılabilmesine imkân tanımak amacıyla getirildiğini göstermektedir.

79. Bu çerçevede dava konusu kuralın yargılamanın sonucuna etkili esaslı herhangi bir işlemin yapıldığı duruşmada müdafî yardımından yararlanma imkânını sınırlamak amacıyla değil, zorunlu müdafîin bulunmaması hâlinde yargılamanın sonucuna etki edecek esaslı bir işlem kalmasa dahi duruşma yapılmasını engelleyen kurala bir istisna sağlanması amacıyla getirildiği anlaşılmaktadır. Diğer bir ifadeyle dava konusu kural ceza adaletinin hakkaniyete uygun bir şekilde gerçekleşmesi için müdafî görevlendirilmesinin zorunlu olduğu hâllerde müdafî yardımı sağlanmaksızın duruşmaya devam edilmesini öngörmemektedir. Bu çerçevede kuralın lafzı ve Kanun'un ilgili diğer hükümleri dikkate alındığında kuralın yargılamanın sonucuna etkili olabilecek esaslı her türlü yargılama işleminin tamamlanmasına rağmen zorunlu müdafîin herhangi bir mazereti olmadığı hâlde davayı uzatmak amacıyla duruşmaya gelmemesi veya duruşmayı terk etmesi nedeniyle yargılamaların zamanında bitirilememesini önlemek amacıyla öngörüldüğü sonucuna ulaşılmaktadır.

80. Daha önce de belirtildiği üzere Anayasa'nın 36. maddesinde güvenceye bağlanan adil yargılanma hakkının önemli unsurlarından biri de makul sürede yargılanma hakkıdır. Anayasa'nın 141. maddesinin son fıkrasında "Davaların en az giderle ve mümkün olan süratle sonuçlandırılması yargının görevidir" denilmek suretiyle davaların makul bir süre içinde bitirilmesi gerekliliği açıkça ifade edilmiştir. Bu hak gereğince devlet, yargılamaların gereksiz yere uzamasını engelleyecek etkin çareler oluşturmak zorundadır (AYM, E.2013/4, K.2013/35, 28/2/2013). Buna göre yargılamaların adil bir şekilde gerçekleştirilmesini sağlamak amacıyla bazı durumlarda sanığa zorunlu müdafî atanması ve sanığın anılan müdafî yardımından yararlandırılması devletin yerine getirmekle yükümlü olduğu pozitif ödevi kapsamında kaldığı gibi yargılamaların gereksiz yere uzamasını engelleyerek makul sürede sonuçlandırılmasını sağlamak da devletin pozitif yükümlülüğü kapsamındadır. Bu durumda her iki yükümlülük arasında makul bir dengenin gözetilip gözetilmediğinin değerlendirilmesi gerekmektedir.

81. Dava konusu kuralla zorunlu müdafinin yokluğunda duruşmaya devam edilebilmesine imkân verilmekle birlikte bu ancak müdafinin herhangi bir mazereti olmaksızın duruşmaya gelmemesi veya duruşmayı terk etmesi hâlinde mümkün olabilecektir. Bir başka ifadeyle kuralın yargılamanın sürüncemede bırakılmasına neden olacak kötü niyetli girişimleri engellemek amacıyla öngörüldüğü anlaşılmaktadır. Öte yandan Kanun'un diğer hükümlerinde yer alan güvenceler, söz konusu iznin yargılamanın sonucuna etkili olan esaslı işlemlerin yapıldığı duruşmada uygulama alanı bulmasına engel olmaktadır. Buna göre yargılamanın adil bir şekilde gerçekleştirilmesini sağlamak amacıyla bazı durumlarda sanığa zorunlu müdafinin atanması ve sanığın müdafinin yardımından yararlandırılmasına ilişkin yükümlülük ile davaların makul sürede bitirilmesi yükümlülüğü arasındaki makul dengenin gözetildiği kuralda Anayasa'nın 36. maddesini ihlal eden bir yön bulunmamaktadır.

82. Açıklanan nedenlerle kural Anayasa'nın 36. maddesine aykırı değildir. İptal talebinin reddi gerekir.

Zühtü ARSLAN, Engin YILDIRIM, Hasan Tahsin GÖKCAN, Recep KÖMÜRCÜ ve Celal Mümtaz AKINCI bu görüşe katılmamışlardır.

F. Kanun'un 6. Maddesiyle 5275 Sayılı Kanun'un 59. Maddesine Eklenen (5) Numaralı Fıkranın İncelenmesi

1. Anlam ve Kapsam

83. 5275 sayılı Kanun'un 59. maddesinde hükümlünün avukatla görüşme hakkına ilişkin usul ve esaslar düzenlenmiştir.

84. Maddenin (1) numaralı fıkrasında, hükümlünün avukatlık mesleğinin icrası çerçevesinde avukatları ile vekâletnamesi olmaksızın en çok üç kez görüşme hakkına sahip olduğu belirtilmiştir.

85. Maddenin (2) numaralı fıkrasında, avukat ile görüşmenin -meslek kimliğinin ibrazı üzerine- tatil günleri dışında ve çalışma saatleri içinde, bu iş için ayrılan görüşme yerlerinde, konuşulanların duyulamayacağı ancak güvenlik nedeniyle görülebileceği bir biçimde yapılacağı belirtilmiştir; (4) numaralı fıkrasında, görüşme sırasında hükümlünün avukatına veya avukatın hükümlüye verdiği belge veya belge örneklerinin, dosyaların ve aralarındaki konuşmaya ilişkin olarak kendilerinin tuttukları kayıtların incelenemeyeceği, hükümlünün avukatı ile yaptığı görüşmenin dinlenemeyeceği ve kayda alınamayacağı ifade edilmiştir. Böylece avukat ile hükümlü arasındaki görüşmelerin gizliliği güvence altına alınmıştır.

86. Dava konusu kuralda ise bu duruma istisna getirilerek 5237 sayılı Kanun'un 220. maddesinde ve İkinci Kitap Dördüncü Kısım Dördüncü, Beşinci, Altıncı ve Yedinci Bölümlerinde tanımlanan suçlar ile 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu kapsamına giren suçlardan mahkûm olanların avukatları ile görüşmelerinde, toplumun ve ceza infaz kurumunun güvenliğinin tehlikeye düşürüldüğüne, terör örgütü veya diğer suç örgütlerinin yönlendirildiğine, bu örgütlere emir ve talimat verildiğine veya yorumları ile gizli, açık ya da şifreli mesajlar iletildiğine ilişkin bilgi, bulgu veya belge elde edilmesi hâlinde Cumhuriyet başsavcılığının istemi ve infaz hâkiminin kararıyla üç ay süreyle; görüşmelerin teknik cihazla sesli veya görüntülü olarak kaydedilebileceği, hükümlü ile avukatın yaptığı görüşmeleri izlemek amacıyla görevlinin görüşmede hazır bulundurulabileceği, hükümlünün avukatına veya avukatın hükümlüye verdiği belgelere veya belge örneklerine, dosyalara ve aralarındaki konuşmalara ilişkin tuttukları kayıtlara elkonulabileceği veya görüşmelerin gün ve saatlerinin sınırlandırılabilceği hüküm altına alınmıştır.

87. Kuralın atıfta bulunduğu 5237 sayılı Kanun'un 220. maddesinde suç işlemek amacıyla örgüt kurma, örgüte üye olma gibi örgüt suçları; İkinci Kitap Dördüncü Kısım Dördüncü, Beşinci, Altıncı ve Yedinci Bölümlerinde ise devletin güvenliğine karşı suçlar, anayasal düzene ve bu düzenin işleyişine karşı suçlar, millî savunmaya karşı suçlar, devlet sırlarına karşı suçlar ve casusluk suçları düzenlenmiştir. Kurala göre bu suçlardan mahkûm olanların avukatlarıyla görüşmeleri yukarıda belirtilen usul ve esaslara göre sınırlandırılacaktır.

2. İptal Talebinin Gerekçesi

88. Dava dilekçesinde özetle; hükümlülerin avukatla serbest bir şekilde görüşme hakkının hak arama hürriyetinin bir uzantısı olduğu, dava konusu kuralla bu hakkın subjektif koşullarla sınırlamalara tabi tutulmasının avukatla görüşme hakkının keyfi şekilde sınırlandırılmasına sebebiyet vereceği, kuralda yer alan sınırlamaların hakkın özüne dokunduğu ve ölçüsüz olduğu belirtilerek kuralın Anayasa'nın 13. ve 36. maddelerine aykırı olduğu ileri sürülmüştür.

3. Anayasa'ya Aykırılık Sorunu

89. 6216 sayılı Kanun'un 43. maddesi uyarınca kural, ilgisi nedeniyle Anayasa'nın 20. maddesi yönünden de incelenmiştir.

90. Anayasa'nın "Özel hayatın gizliliği" başlıklı 20. maddesinin birinci fıkrasında; herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı hüküm altına alınmıştır.

91. Aynı maddenin ikinci fıkrasında ise anılan hakka çeşitli sebeplere bağlı kalınarak sınırlamalar getirilebileceği belirtilerek bu hakkın mutlak olmadığı kabul edilmiştir. Maddede bu sınırlama sebepleri arasında millî güvenliğin ve kamu düzeninin korunması ile suç işlenmesinin önlenmesi sebepleri de sayılmış, böylece bunlara dayalı olarak söz konusu hakkın sınırlandırılabilmesine izin verilmiştir. Ancak 20. maddenin ikinci fıkrasında söz konusu sınırlandırmanın arama tedbirine özgü olarak yapılabileceği belirtildiğinden bu sebepler 20. madde bağlamında dava konusu kural yönünden meşru bir sınırlandırma nedeni olarak kabul edilmeyebilir. Bununla birlikte özel hayatın düzenlendiği maddede dava konusu kural yönünden özel sınırlama sebeplerine yer verilmediğinin kabulü hâlinde dahi bu hakkın Anayasa'da güvence altına alınan diğer temel hak ve özgürlüklerin korunması veya Anayasa'nın diğer maddelerinde devlete bir görev olarak yüklenen millî güvenliğin, kamu düzeninin ve kamu güvenliğinin korunması gibi nedenlerle sınırlandırılması mümkündür.

92. Dava konusu kuralla örgüt kurma suçu ile devletin güvenliğine karşı suçlar, anayasal düzene ve bu düzenin işleyişine karşı suçlar, millî savunmaya karşı suçlar, devlet sırlarına karşı suçlar ve casusluk suçundan mahkûm olanların avukatlarıyla görüşmelerine birtakım kısıtlamalar getirilmiştir. Bu çerçevede kuralın hükümlülerin özel hayatına saygı hakkına sınırlama getirdiği açıktır.

93. Hükümlünün avukatıyla mahremiyet içinde belirli aralıklarla görüşmesi cezanın infazı aşamasında alacağı hukuki yardım bakımından önemli olduğu gibi ceza infaz kurumu dışındaki özel yaşamıyla ilgili doğru kararlar verebilmesi açısından da son derece önemlidir. Bu nedenle 5275 sayılı Kanun'da cezanın infazı aşamasında da avukatla görüşme hakkı özel olarak düzenlenerek güvence altına alınmıştır.

94. Bu kapsamda 5275 sayılı Kanun'un 59. maddesinin (2) numaralı fıkrasında belirtilen güvencelere yer verilerek avukatla hükümlünün görüşmelerinin gizliliği sağlanmıştır.

95. Kuralla yukarıda sayılan suçlardan hükümlü olanların avukatları ile görüşmelerinde toplumun ve ceza infaz kurumunun güvenliğinin tehlikeye düşürüldüğüne, terör örgütü veya diğer suç örgütlerinin yönlendirildiğine, bu örgütlere emir ve talimat verildiğine veya yorumları ile gizli, açık ya da şifreli mesajlar iletildiğine ilişkin bilgi, bulgu veya belge elde edilmesi hâlinde görüşmelere birtakım kısıtlamaların getirilmesi öngörülmüştür. Kuralın ceza infaz kurumlarının güvenliğinin sağlanması, millî güvenlik ve kamu düzeni yönünden önem arz eden suçların işlenmesinin önlenmesi amacıyla öngörüldüğü, bu yönüyle anayasal açıdan meşru bir sınırlama amacına sahip olduğu anlaşılmaktadır.

96. Devletin hükümlülerin özel hayatlarına saygı gösterme yükümlülüğü bulunmakla birlikte ceza infaz kurumlarının güvenliğini ve genel olarak toplumun güvenliğini gözetme yükümlülüğü de bulunmaktadır. Bu yönüyle kuralla getirilen sınırlamanın ceza infaz kurumlarının güvenliğinin sağlanması ile millî güvenlik ve kamu düzeni yönünden önem arz eden suçların işlenmesinin önlenmesi amaçlarına ulaşılması bakımından elverişli ve gerekli olmadığı söylenemez.

97. Öte yandan kuralla yukarıda sayılan suçlardan hükümlü olanların tümü yönünden kategorik bir sınırlama getirilmemekte; bu hükümlülerin avukatları ile görüşmelerinde toplumun ve ceza infaz kurumunun güvenliğinin tehlikeye düşürüldüğüne, terör örgütü veya diğer suç örgütlerinin yönlendirildiğine, bu örgütlere emir ve talimat verildiğine veya yorumları ile gizli, açık ya da şifreli mesajlar iletildiğine ilişkin bilgi, bulgu veya belge elde edilmesi durumunda anılan görüşmelere çeşitli kısıtlamalar getirilmesine izin verilmektedir. Ayrıca kuralda kısıtlama için belli bir süre öngörüldüğü ve kısıtlama kararı verme yetkisinin yargı organlarına bırakıldığı anlaşılmaktadır.

98. Öte yandan infaz hâkimi tarafından verilen kısıtlamaya ilişkin kararlar 5275 sayılı Kanun'un 59. maddesinin (9) numaralı fıkrası uyarınca itiraza tabi tutulmuştur. İlgililer verilen kısıtlama kararının mevzuata aykırı olduğu iddiasıyla infaz hâkimliğinin kurulduğu yer ağır ceza mahkemesine itirazda bulunma hakkına sahiptirler. Bu yönüyle Kanun'da anılan yetkinin keyfî bir şekilde kullanılmasını önleyecek yasal güvencelere de yer verildiği görülmektedir.

99. Anılan güvenceler gözetildiğinde sınırlamayla ulaşılmak istenen amaç ile özel hayata saygı hakkına ilişkin bireysel yarar arasında bulunması gereken makul dengenin gözetildiği anlaşılmaktadır. Bu itibarla hükümlü ile avukatın görüşmesine kısıtlama öngören kuralın özel hayata saygı hakkına orantısız, dolayısıyla da ölçüsüz bir sınırlama getirdiği söylenemez.

100. Açıklanan nedenlerle kural Anayasa'nın 13. ve 20. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

Kuralın Anayasa'nın 36. maddesiyle ilgisi görülmemiştir.

G. Kanun'un 6. Maddesiyle 5275 Sayılı Kanun'un 59. Maddesine Eklenen (10) Numaralı Fıkranın "Bu madde hükümleri 9 uncu maddenin üçüncü fıkrasına göre yüksek güvenlikli ceza infaz kurumlarında bulunan hükümlüler ... hakkında da uygulanır." Bölümünün İncelenmesi

1. İptal Talebinin Gerekçesi

101. Dava dilekçesinde özetle; dava konusu kuralla avukatla görüşme hakkının 5275 sayılı Kanun'un 9. maddesinin üçüncü fıkrasına göre yüksek güvenlikli ceza infaz kurumlarında bulunan hükümlüler yönünden Kanun'un 59. maddesinin (5) numaralı fıkrası çerçevesinde subjektif koşullarla

sınırlamalara tabi tutulmasının anılan hakkın keyfî şekilde sınırlandırılmasına sebebiyet vereceđi, kuralda yer alan sınırlamaların hakkın özüne dokunduđu ve ölçüsüz olduđu belirtilerek kuralın Anayasa'nın 13. ve 36. maddelerine aykırı olduđu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

102. 6216 sayılı Kanun'un 43. maddesi uyarınca kural, ilgisi nedeniyle Anayasa'nın 20. maddesi yönünden de incelenmiştir.

103. Dava konusu kuralda 5275 sayılı Kanun'un 59. maddesinin aynı Kanun'un 9. maddesinin (3) numaralı fıkrasına göre yüksek güvenliikli ceza infaz kurumlarında bulunan hükümlüler hakkında da uygulanacağı hüküm altına alınmıştır.

104. Kanun'un 59. maddesinde hükümlülerin avukatla görüşme hakkına ilişkin usul ve esaslar düzenlenmiştir. Dava dilekçesinde kuralla maddenin (5) numaralı fıkrası çerçevesinde avukatla görüşme hakkına getirilen kısıtlamaların Anayasa'ya aykırılığı ileri sürüldüğünden kural, söz konusu maddenin hükümlünün avukatla görüşmesinde uygulanacak kısıtlamaları düzenleyen (5) numaralı fıkrası yönünden incelenmiştir.

105. 5275 sayılı Kanun'un 9. maddesinin (3) numaralı fıkrasında; eylem ve tutumları nedeniyle tehlikeli hâlde bulunan, özel gözetim ve denetim altında bulundurulmaları gerekli olduđu saptananlar ile buldukları kurumlarda düzen ve disiplini bozanların veya iyileştirme tedbir, araç ve usullerine ısrarla karşı koyanların yüksek güvenliikli ceza infaz kurumlarına gönderileceđi belirtilmiştir. Dava konusu kurala göre Kanun'un 59. maddesinin (5) numaralı fıkrasında sayılan görüşmelerin teknik cihazla sesli veya görüntülü olarak kaydedilmesi, hükümlü ile avukatın yaptığı görüşmeleri izlemek amacıyla görevlinin görüşmede hazır bulundurulabilmesi, hükümlünün avukatına veya avukatın hükümlüye verdiği belge veya belge örneklerine, dosyalar ve aralarındaki konuşmalara ilişkin tuttukları kayıtlara elkonulabilmesi veya görüşmelerin gün ve saatlerinin sınırlandırılabilmesi şeklindeki avukatla görüşme hakkına getirilen kısıtlamalar, Kanun'un 9. maddesinin (3) numaralı fıkrası uyarınca yüksek güvenliikli ceza infaz kurumlarında bulunan hükümlüler hakkında da uygulanacaktır.

106. Bir önceki başlık altında incelenen Kanun'un 59. maddesinin (5) numaralı fıkrasına yönelik gerekçeler, Kanun'un 9 maddesinin (3) numaralı fıkrası uyarınca yüksek güvenliikli ceza infaz kurumlarında kalan hükümlüler için de geçerlidir.

107. Açıklanan nedenlerle kural 5275 sayılı Kanun'un 59. maddesinin (5) numaralı fıkrası yönünden Anayasa'nın 13. ve 20. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

Kuralın Anayasa'nın 36. maddesiyle ilgisi görülmemiştir.

Ğ. Kanun'un 6. Maddesiyle 5275 Sayılı Kanun'un 59. Maddesine Eklenen (10) Numaralı Fıkrasının "...ile beşinci fıkradaki suçlardan hükümlü olup, başka bir suçtan dolayı şüpheli veya sanık sıfatıyla avukatıyla görüşen hükümlüler..." Bölümünün İncelenmesi

1. Anlam ve Kapsam

108. Dava konusu kuralda; 5275 sayılı Kanun'un 59. maddenin (5) numaralı fıkrasındaki suçlardan hükümlü olup başka bir suçtan dolayı şüpheli veya sanık sıfatıyla avukatıyla görüşen hükümlüler hakkında da 59. madde hükümlerinin uygulanacağı hüküm altına alınmıştır.

109. Kanun'un 59. maddesinin (5) numaralı fıkrasında sayılan suçlar, 5237 sayılı Kanun'un 220. maddesinde düzenlenen örgüt suçları, İkinci Kitap Dördüncü Kısım Dördüncü, Beşinci, Altıncı ve Yedinci Bölümlerinde düzenlenen devletin güvenliğine karşı suçlar, anayasal düzene ve bu düzenin işleyişine karşı suçlar, millî savunmaya karşı suçlar, devlet sırlarına karşı suçlar ve casusluk suçlarıdır.

110. Dava konusu kurallara göre 5237 sayılı Kanun'un 220. maddesinde düzenlenen örgüt suçları, devletin güvenliğine karşı suçlar, anayasal düzene ve bu düzenin işleyişine karşı suçlar, millî savunmaya karşı suçlar, devlet sırlarına karşı suçlar ve casusluk suçundan hükümlü olup başka bir suçtan dolayı şüpheli veya sanık avukatıyla görüşen hükümlülerin avukatları ile görüşmelerinde de 5275 sayılı Kanun'un 59. maddesi uygulanacaktır.

2. İptal Talebinin Gerekçesi

111. Dava dilekçesinde özetle; dava konusu kuralla avukatla görüşme hakkının 5275 sayılı Kanun'un 59. maddesinin (5) numaralı fıkrasında belirtilen suçlardan hükümlü olup başka bir suçtan dolayı şüpheli veya sanık sıfatıyla avukatıyla görüşen hükümlüler yönünden anılan fıkra çerçevesinde subjektif koşullarla sınırlamalara tabi tutulmasının anılan hakkın keyfî şekilde sınırlandırılmasına sebebiyet vereceği, kuralda yer alan sınırlamaların hakkın özüne dokunduğu ve ölçsüz olduğu belirtilerek kuralın Anayasa'nın 13. ve 36. maddelerine aykırı olduğu ileri sürülmüştür.

3. Anayasa'ya Aykırılık Sorunu

112. Dava dilekçesinde kuralla anılan maddenin (5) numaralı fıkrasında öngörülen kural çerçevesinde avukatla görüşme hakkına getirilen kısıtlamaların Anayasa'ya aykırılığı ileri sürüldüğünden kural, söz konusu maddenin hükümlünün avukatla görüşmesinde uygulanacak kısıtlamaları düzenleyen (5) numaralı fıkrası yönünden incelenmiştir.

113. Kurala göre Kanun'un 59. maddesinin (5) numaralı fıkrasında sayılan görüşmelerin teknik cihazla sesli veya görüntülü olarak kaydedilmesi, hükümlü ile avukatın yaptığı görüşmeleri izlemek amacıyla görevlinin görüşmede hazır bulundurulabilmesi, hükümlünün avukatına veya avukatın hükümlüye verdiği belge veya belge örneklerine, dosyalar ve aralarındaki konuşmalara ilişkin tuttukları kayıtlara elkonulabilmesi veya görüşmelerin gün ve saatlerinin sınırlandırılabilmesi şeklindeki avukatla görüşme hakkına getirilen kısıtlamalar, 5237 sayılı Kanun'un 220. maddesinde düzenlenen örgüt suçları ile devletin güvenliğine karşı suçlar, anayasal düzene ve bu düzenin işleyişine karşı suçlar, millî savunmaya karşı suçlar, devlet sırlarına karşı suçlar ve casusluk suçundan hükümlü olup başka bir suçtan dolayı şüpheli veya sanık sıfatıyla avukatıyla görüşen hükümlüler hakkında da uygulanacaktır.

114. Kural, Kanun'un 59. maddesinin (5) numaralı fıkrasında belirtilen suçlardan hükümlü olmakla birlikte başka bir suçtan dolayı şüpheli veya sanık sıfatıyla soruşturma ve kovuşturmaları devam eden kişilerin avukatları ile görüşmelerine bazı kısıtlamalar öngörmektedir. Bu yönüyle kural devam eden soruşturma ve kovuşturmalar bakımından müdafî yardımından yararlanma hakkına sınırlama getirmektedir.

115. Anayasa'nın 36. maddesiyle güvence altına alınan müdafî yardımından yararlanma hakkı hem savunma hakkının etkin bir şekilde kullanılmasını sağlamakta hem de çelişmeli yargılama ve silahların eşitliği ilkelerine hayat vermektedir. Müdafî yardımı özellikle şüpheli veya sanığın yaşı, ruhsal durumu veya isnat olunan suçun ağırlığı gibi nedenlerden dolayı savunma makamının özel olarak desteklenmesinin gerektiği hâllerde etkili bir savunma yapabilmesi ve maddi gerçeğin ortaya çıkarılması bakımından önem taşımaktadır.

116. Müdafî yardımından etkili bir şekilde yararlanmanın ilk koşulu ise müdafî ile yapılan görüşmelerin belli bir gizlilik içinde gerçekleştirilmesidir. Şüpheli veya sanığın müdafî ile özgür bir şekilde bilgi alışverişinde bulunması için mahremiyet büyük önem taşımaktadır. Şüpheli veya sanığın müdafî ile yapacağı görüşmelerde mahremiyet olmaması müdafiden alacağı hizmetin faydasını en alt düzeye indirecektir. Bu nedenle meşru amaçlarla avukatla görüşme hakkına kısıtlama getirilirken bu kısıtlamayla savunma hakkı arasındaki denge gözetilmeli, kısıtlama hiçbir şekilde savunma hakkının etkili bir şekilde kullanılmasına engel olmamalıdır. Meşru bir amaçla kısıtlama yapılsa dahi soruşturma ve kovuşturması devam eden kişilere savunma hakkının etkin bir şekilde kullanımı bakımından yeterli güvencelerin tanınması gerekir.

117. Kuralla 5237 sayılı Kanun'un 220. maddesi kapsamındaki örgüt suçları ile devletin güvenliğine karşı suçlar, anayasal düzene ve bu düzenin işleyişine karşı suçlar, millî savunmaya karşı suçlar,

devlet sırlarına karşı suçlar ve casusluk suçundan hükümlü olup başka bir suçtan dolayı şüpheli veya sanık sıfatıyla avukatıyla görüşen hükümlülerin avukatları ile görüşmelerinin teknik cihazla sesli veya görüntülü olarak kaydedilmesine, görüşmeleri izlemek amacıyla görevlinin hazır bulundurulmasına, hükümlülerin avukatına veya avukatın bu kişilere verdiği belge veya belge örneklerine, dosyalar ve aralarındaki konuşmalara ilişkin tuttukları kayıtlara el konulabilmesine, görüşmelerin gün ve saatlerinin sınırlandırılmasına izin verilmektedir. Dolayısıyla kuralla müdafî yardımından yararlanma hakkına sınırlama getirildiği açık olup anılan sınırlamanın Anayasa'nın 13. maddesine uygun olup olmadığının incelenmesi gerekir.

118. Daha önce de belirtildiği üzere Anayasa'nın 36. maddesinde bu hak yönünden özel sınırlama sebeplerine yer verilmemiş ise de bu hakkın Anayasa'da güvence altına alınan diğer temel hak ve özgürlüklerin korunması veya Anayasa'nın diğer maddelerinde devlete bir görev olarak yüklenen millî güvenliğin, kamu düzeninin ve kamu güvenliğinin korunması gibi nedenlerle sınırlandırılması mümkündür. Dava konusu kuralla da 5237 sayılı Kanun'un 220. maddesi kapsamındaki örgüt suçları ile devletin güvenliğine karşı suçlar, anayasal düzene ve bu düzenin işleyişine karşı suçlar, millî savunmaya karşı suçlar, devlet sırlarına karşı suçlar ve casusluk suçundan hükümlü olup başka bir suçtan dolayı şüpheli veya sanık olanların avukatlarıyla görüşmesine bazı kısıtlamalar getirilmekte olup bu sınırlamayla ceza infaz kurumlarının güvenliğinin sağlanması, millî güvenlik, kamu düzeni ve kamu güvenliğine yönelik suçların önlenmesinin amaçlandığı anlaşılmaktadır. Bu yönüyle kuralla getirilen sınırlamanın anayasal olarak meşru bir nedene dayanmadığı söylenemez. Ancak sınırlamanın meşru bir nedene dayalı olması yeterli olmayıp hakkın özüne dokunmaması ve ölçülü de olması gerekir.

119. Bir sınırlamanın hakkın özüne dokunmadığının kabulü için temel hakların kullanılmasını ciddi surette güçleştirip amacına ulaşmasına engel olmaması ve etkisini ortadan kaldıracı bir nitelik taşımaması gerekir.

120. Dava konusu kuralla anılan suçlardan hükümlü olup başka suçlardan şüpheli veya sanık olanların avukatlarıyla tüm görüşmelerinin kısıtlanması düzenlenmemekte, sadece avukatları ile görüşmelerinde toplumun ve ceza infaz kurumunun güvenliğinin tehlikeye düşürüldüğüne, terör örgütü veya diğer suç örgütlerinin yönlendirildiğine, bu örgütlere emir ve talimat verildiğine veya yorumları ile gizli, açık ya da şifreli mesajlar iletildiğine ilişkin bilgi, bulgu veya belge elde edildiği durumlarda görüşmelere bazı kısıtlamaların getirilmesi öngörülmektedir. Bu yönüyle kuralla müdafî yardımından yararlanma hakkının kullanımının ciddi surette güçleştirilip amacına ulaşmasının önlenildiği ileri sürülemeyeceğinden kuralın hakkın özüne dokunduğu söylenemez.

121. Hükümlü ile avukat arasındaki görüşmelerin gün ve saatlerinin kısıtlanması müdafî yardımından yararlanma hakkına sınırlama getirmekle birlikte müdafî yardımından yararlanma hakkı gözetilerek sanığın savunma hakkına zarar vermeyecek şekilde bu kısıtlamanın uygulanması mümkündür. Ayrıca ilgililerin kısıtlama kararının savunma hakkını etkisiz kılacak şekilde verildiği iddiasıyla mahkemeye itirazda bulunma, dolayısıyla bu tedbirin müdafî yardımından yararlanma hakkına uygun olarak uygulanmasını sağlama imkânları da bulunmaktadır. Bu itibarla hükümlü ile avukatın görüşmesinin gün ve saatlerinin kısıtlanmasının yukarıda açıklanan nedenlerle meşru bir amacının bulunduğu anlaşıldığından ve söz konusu tedbirin anılan amaca ulaşma bakımından elverişli, gerekli ve orantılı olmadığı söylenemeyeceğinden bu tedbirin müdafî yardımından yararlanma hakkına ölçsüz bir sınırlama getirdiği ileri sürülemez.

122. Öte yandan şüpheli veya sanık ile avukatın görüşmesinin kaydedilmesi, görüşmede görevlinin hazır bulundurulması ile bilgi ve belgelere elkonulması şeklindeki kısıtlamaların anayasal bakımdan meşru bir amacının bulunduğu ve yapılan sınırlamanın anılan amaca ulaşma bakımından gerekli ve elverişli olduğu söylenebilir. Ancak getirilen sınırlamanın ölçülü olduğunun kabul edilebilmesi için elverişli ve gerekli olması yeterli olmayıp orantılı da olması da gerekmektedir.

123. Belli koşullara bağlı da olsa şüpheli veya sanık ile avukatın görüşmesinin kaydedilmesi, görüşmede görevlinin hazır bulundurulması ile bilgi ve belgelere elkonulması şeklindeki kısıtlamalar doğrudan avukat ve müvekkil arasındaki mahremiyeti ortadan kaldıracak niteliktedir. Belirtilen durumlarda şüpheli veya sanığın avukatı ile mahrem bilgileri paylaşması, bilgi alışverişinde bulunması mümkün olmadığından avukatla görüşme hakkının bu şekilde sınırlanması özellikle savunma makamının özel olarak desteklenmesinin gerektiği hâllerde etkili bir savunma yapılabilmesi imkânını önemli ölçüde azaltabilir. Ayrıca kuralda avukat-müvekkil görüşmesinin gizliliği ortadan kaldırılırken şüpheli veya sanığın etkili bir hukuki yardım alabilmesi ve savunma hakkını etkili bir şekilde kullanması yönünde gerekli olan güvencelerin de öngörülmediği anlaşılmaktadır. Müdafî yardımından yararlanma, dolayısıyla savunma ve adil yargılanma hakkının hukuk devletindeki önemi dikkate alındığında kuralla getirilen sınırlamanın kişiye yüklediği külfetin aşırı ve orantısız olduğu, böylelikle şüpheli ve sanığın müdafî ile görüşmesinin kaydedilmesi, izlenmesi veya bilgi ve belgelere el konulmasının müdafî yardımından yararlanma hakkına ölçsüz bir sınırlama getirdiği sonucuna ulaşılmıştır.

124. Açıklanan nedenlerle kural, 5275 sayılı Kanun'un 59. maddesinin (5) numaralı fıkrasının "...görüşmeler teknik cihazla sesli veya görüntülü olarak kaydedilebilir, hükümlü ile avukatın yaptığı görüşmeleri izlemek amacıyla görevli görüşmede hazır bulundurulabilir, hükümlünün

avukatına veya avukatın hükümlüye verdiği belge veya belge örnekleri, dosyalar ve aralarındaki konuşmalara ilişkin tuttukları kayıtlara elkonulabilir...” bölümü yönünden Anayasa’nın 13. ve 36. maddelerine aykırıdır. İptali gerekir.

125. Kural, 5275 sayılı Kanun’un 59. maddesinin (5) numaralı fıkrasının geri kalan bölümü yönünden ise Anayasa’nın 13. ve 36. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

H. Kanun’un 6. Maddesiyle 5275 Sayılı Kanun’un 59. Maddesine Eklenen (11) Numaralı Fıkranın İncelenmesi

1. İptal Talebinin Gerekçesi

126. Dava dilekçesinde bir önceki başlıkta incelenen kuralla ilgili olarak ileri sürülen gerekçelerle kuralın Anayasa’nın 13. ve 36. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa’ya Aykırılık Sorunu

127. 5275 sayılı Kanun’un 59. maddesinin (5) numaralı fıkrasında 5237 sayılı Kanun’un 220. maddesinde ve İkinci Kitap Dördüncü Kısım Dördüncü, Beşinci, Altıncı ve Yedinci Bölümlerinde tanımlanan suçlar ile 3713 sayılı Kanun kapsamına giren suçlardan mahkûm olanların avukatları ile görüşmelerinde toplumun ve ceza infaz kurumunun güvenliğinin tehlikeye düşürüldüğüne, terör örgütü veya diğer suç örgütlerinin yönlendirildiğine, bu örgütlere emir ve talimat verildiğine veya yorumları ile gizli, açık ya da şifreli mesajlar iletildiğine ilişkin bilgi, bulgu veya belge elde edilmesi hâlinde Cumhuriyet başsavcılığının istemi ve infaz hâkiminin kararıyla üç ay süreyle, görüşmelerin teknik cihazla sesli veya görüntülü olarak kaydedilebileceği, hükümlü ile avukatın yaptığı görüşmeleri izlemek amacıyla görevlinin görüşmede hazır bulundurulabileceği, hükümlünün avukatına veya avukatın hükümlüye verdiği belge veya belge örnekleri, dosyalar ve aralarındaki konuşmalara ilişkin tuttukları kayıtlara el konulabileceği veya görüşmelerin gün ve saatlerinin sınırlandırılabilmesi hüküm altına alınmıştır.

128. Kanun’un anılan maddesinin (10) numaralı fıkrasında da söz konusu maddenin (5) numaralı fıkrasındaki suçlardan hükümlü olup başka bir suçtan dolayı şüpheli veya sanık sıfatıyla avukatıyla görüşen hükümlüler hakkında da 59. madde hükümlerinin uygulanacağı belirtilmiştir.

129. Dava konusu kuralda ise tutuklular hakkında bu madde hükümlerine göre karar vermeye soruşturma aşamasında sulh ceza hâkiminin, kovuşturma aşamasında ise mahkemenin yetkili olduğu hüküm altına alınmıştır.

130. Anayasa'nın 142. maddesinde "Mahkemelerin kuruluşu, görev ve yetkileri, işleyişi ve yargılama usulleri kanunla düzenlenir" hükmüne yer verilmiştir. Buna göre kanun koyucu mahkemelerin kuruluşu, görev ve yetkileri, işleyişi ve yargılama usulleri hakkında Anayasa kurallarına bağlı olmak kaydıyla ihtiyaç duyduğu düzenlemeyi yapma yetkisine sahip bulunmaktadır.

131. Tutuklular hakkında avukatla görüşme hakkına kısıtlama kararı verme yetkisi dava konusu kuralla soruşturma aşamasında sulh ceza hâkimi, kovuşturma aşamasında ise mahkemelere tanınarak müdafî yardımından yararlanma hakkına ilişkin sınırlamalara karar verilmesine yargı güvencesi getirilmiştir. Avukatla görüşme hakkına getirilebilecek sınırlamaların sebepleri, usulü, kapsamı, süresi ve ilgilileri Kanun'un 59. maddesinin (5) ve (10) numaralı fıkralarında hükme bağlanmak suretiyle avukatla görüşme hakkına anılan fıkralarla sınırlama getirilmiştir. Buna karşılık dava konusu kural, söz konusu sınırlamaların yalnızca yargı kararıyla gerçekleşebileceğini öngörmekte olup anılan hakka yönelik sınırlamanın sebebini oluşturmamaktadır. Bir başka deyişle kuralla avukatla görüşme hakkına yönelik bir müdahalede bulunulmamakta, bu başlık altında inceleme konusu olmayan ve anılan hakkın sınırlanması sonucunu doğuran diğer düzenlemelerin gereğinin yargı kararıyla yerine getirilebileceği hükme bağlanmaktadır. Bu itibarla herhangi bir sınırlama öngörmeyen kuralın müdafî yardımından yararlanma veya temel hak ve özgürlüklerin sınırlanma rejimini düzenleyen anayasal hükümlere aykırı bir yönü bulunmamaktadır.

132. Açıklanan nedenlerle kural Anayasa'nın 13. ve 36. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

I. Kanun'un 33. Maddesiyle 1453 Sayılı Kanun'a Eklenen Geçici 1. Maddenin İkinci Fıkrasının İncelenmesi

1. İptal Talebinin Gerekçesi

133. Dava dilekçesinde özetle; Jandarma Genel Komutanlığı, Jandarma ve Sahil Güvenlik Akademisi ile Sahil Güvenlik Komutanlığının genel bütçe kapsamındaki kamu idarelerinden olmaları nedeniyle bu idarelerin kadro ihdaslarının kanunla yapılması gerektiği, dava konusu kuralla bu idarelerin 2017 yılı fiilî kadrolarını ihdas yetkisinin TBMM Plan ve Bütçe Komisyonuna verilmesinin yasama yetkisinin devri niteliği taşıdığı belirtilerek kuralın Anayasa'nın 7. maddesine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

134. 6216 sayılı Kanun'un 43. maddesi uyarınca kural, ilgisi nedeniyle Anayasa'nın 128. maddesi yönünden de incelenmiştir.

135. Dava konusu kuralda; Jandarma Genel Komutanlığı, Jandarma ve Sahil Güvenlik Akademisi ile Sahil Güvenlik Komutanlığının 2017 yılı fiilî kadrolarının 2016 yılı sonuna kadar TBMM Plan ve Bütçe Komisyonunca belirleneceği hüküm altına alınmıştır.

136. Anayasa'nın 7. maddesinde, yasama yetkisinin Türk milleti adına TBMM'ye ait olduğu ve bu yetkinin devredilemeyeceği belirtilmiştir. Yasama yetkisinin genelliği ilkesi uyarınca kanun koyucunun Anayasa'ya aykırı olmamak kaydıyla kural olarak her konuyu kanunla düzenleyebileceği kuşkusuzdur.

137. Anayasa'nın 123. maddesinin birinci ve ikinci fıkralarında "İdare, kuruluş ve görevleriyle bir bütündür ve kanunla düzenlenir./ İdarenin kuruluş ve görevleri, merkezden yönetim ve yerinden yönetim esaslarına dayanır" denilmiştir. Anayasa'nın 128. maddesinin ikinci fıkrasının birinci cümlesinde de "Memurların ve diğer kamu görevlilerinin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülükleri, aylık ve ödenekleri ve diğer özlük işleri kanunla düzenlenir" hükmüne yer verilerek memurlar ve diğer kamu görevlileri özlük hakları bakımından yasal güvenceye kavuşturulmuştur.

138. Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanunu'na ek (I) sayılı Cetvel'de genel bütçe kapsamındaki kamu idareleri arasında sayılmıştır. Jandarma ve Sahil Güvenlik Akademisi de 10/3/1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun 13/A maddesi uyarınca jandarma ve sahil güvenlik teşkilatlarının subay ve astsubay ile diğer personel ihtiyacını karşılamak, ön lisans, lisans ve lisansüstü eğitim-öğretim, bilimsel araştırma, yayın yapmak üzere bünyesinde fakülte, enstitü, astsubay meslek yüksekokulları, eğitim ve araştırma merkezleri ile kurslar bulunan, İçişleri Bakanlığına bağlı bir yükseköğretim kurumu olarak kurulmuştur.

139. Adı geçen kurumlar Anayasa'nın 123. maddesinde ifade edildiği üzere idarenin bütünlüğü içinde yer almaktadır. Bu kurumlarda genel idare esaslarına göre yürütülmekte olan kamu hizmetlerinin gerektirdiği asli ve sürekli görevleri ifa eden personel Anayasa'nın 128. maddesi kapsamında olduğundan bunların kadrolarına, bu kadroların ihdas ve iptaline ilişkin kuralların da Anayasa'nın 128. maddesi uyarınca kanunla düzenlenmesi gerekir.

140. Dava konusu kuralda ise anılan idarelerin 2017 yılı fiilî kadrolarının 2016 yılı sonuna kadar TBMM Plan ve Bütçe Komisyonunca belirlenmesi öngörülmüştür. Kural bu hâliyle yasama yetkisinin devri sonucunu doğurmakta, kamu görevlilerinin statülerinin kanunla düzenlenmesi yolundaki anayasal kurala aykırılık oluşturmaktadır.

141. Açıklanan nedenlerle kural Anayasa'nın 7. ve 128. maddelerine aykırıdır. İptali gerekir.

İ. Kanun'un 48. Maddesiyle 1325 Sayılı Kanun'a Eklenen Ek 10. Maddenin "...Bakanlığın özelliği ve hizmetin gerekli kıldığı şart ve vasıflar göz önüne alınarak Bakanlığa intibak edemedikleri üstlerince teklif edilenlerden Bakanlıkta oluşturulacak komisyona yaptırılacak tahkikat sonucuna göre Millî Savunma Bakanınca uygun görülenler,..." Bölümünün İncelenmesi

1. İptal Talebinin Gerekçesi

142. Dava dilekçesinde özetle; dava konusu kuralda Millî Savunma Bakanlığında (Bakanlık) görev yapan personelin Bakanlığa intibak edip edemediği konusunda nesnel bir ölçüte yer verilmediği, Bakanlığa intibak edemediği ileri sürülen personelin durumunun Tahkikat Komisyonunca değerlendirilmesi öngörülmekle birlikte intibak edemediği tespit edilen personelden sadece Millî Savunma Bakanınca (Bakan) uygun görülenlerin başka kurumlara naklen atanmasının öngörüldüğü, burada yer alan ayırımın objektif bir ölçüt içermediği, Bakanlığa intibak edemedikleri sonucuna varılan sivil personelin başka bir kurum veya kuruluşa naklen atanması konusunda Bakan'a sınırları belirsiz bir yetki verildiği ileri sürülerek kuralın Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

143. 1325 sayılı Kanun'un ek 10. maddesinde, Bakanlık fiilî kadrosuna dâhil, 657 sayılı Kanun'a tabi personelden Bakanlığın özelliği ve hizmetin gerekli kıldığı şart ve vasıflar gözönüne alınarak Bakanlığa intibak edemedikleri üstlerince teklif edilenlerden Bakanlıkta oluşturulacak komisyona yaptırılacak tahkikat sonucuna göre Bakanca uygun görülenlerin genel hükümlere göre Merkezî Yönetim Bütçe Kanunu'nda öngörülen atama sınırlamalarına tabi olmadan Çalışma, Sosyal Hizmetler ve Aile Bakanlığı aracılığıyla başka bir kurum veya kuruluşa naklen atanacağı hüküm altına alınmıştır. Dava konusu kural anılan maddenin "...Bakanlığın özelliği ve hizmetin gerekli kıldığı şart ve vasıflar göz önüne alınarak Bakanlığa intibak edemedikleri üstlerince teklif edilenlerden Bakanlıkta oluşturulacak komisyona yaptırılacak tahkikat sonucuna göre Millî Savunma Bakanınca uygun görülenler,..." şeklindeki bölümüdür.

144. Hukuk devletinin temel ilkelerinden biri belirliliktir. Bu ilkeye göre yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfî uygulamalarına karşı koruyucu önlem içermesi gerekir. Belirlilik ilkesi hukuki güvenlikle bağlantılı olup birey, kanundan belirli bir kesinlik içinde hangi somut eylem ve olguya hangi hukuki yaptırımın veya sonucun

bağlandığını bilmelidir. Birey ancak bu durumda kendisine düşen yükümlülükleri öngörebilir ve davranışlarını ayarlayabilir.

145. Belirlilik ilkesi, yalnızca yasal belirliliği değil daha geniş anlamda hukuki belirliliği de ifade etmektedir. Yasal düzenlemeye dayanarak erişilebilir, bilinebilir ve öngörülebilir olma gibi gereklilikleri karşılması koşuluyla mahkeme içtihatları ve yürütmenin düzenleyici işlemleriyle de hukuki belirlilik sağlanabilir. Hukuki belirlilik ilkesinde asıl olan, bir hukuk normunun uygulanmasıyla ortaya çıkacak sonuçların o hukuk düzeninde öngörülebilir olmasıdır.

146. Devlet memurlarının bir kurumdan diğerine nakli 657 sayılı Kanun'da düzenlenmiştir. Anılan Kanun'un 74. maddesinde, memurların 657 sayılı Kanun'a tabi kurumlar arasında, kurumların muvafakati ile kazanılmış hak dereceleri üzerinden veya Kanun'un 68. maddesinde belirtilen esaslar çerçevesinde derece yükselmesi suretiyle buldukları sınıftan veya öğrenim durumları itibarıyla girebilecekleri sınıftan bir kadroya naklinin mümkün olduğu belirtilmiş; kazanılmış hak derecelerinin altındaki derecelere atanabilmeleri için ise atanacakları kadro derecesi ile kazanılmış hak dereceleri arasındaki farkın 3 dereceden çok olmaması ve memurların isteğinin şart olduğu ifade edilmiştir.

147. Dava konusu kuralda ise anılan duruma istisna getirilerek Bakanlık fiilî kadrosuna dâhil 657 sayılı Kanun'a tabi personelden Bakanlığın özelliği ve hizmetin gerekli kıldığı şart ve vasıflar gözönüne alınarak Bakanlığa intibak edemedikleri üstlerince teklif edilenlerden Bakanlıkta oluşturulacak komisyona yaptırılacak tahkikat sonucuna göre Bakanca uygun görülenlerin genel hükümlere göre Merkezî Yönetim Bütçe Kanunu'nda öngörülen atama sınırlamalarına tabi olmadan başka bir kurum veya kuruluşa naklen atanması öngörülmüştür.

148. Bakanlığın teşkilatı, görev ve yetkileri 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete'de yayımlanan (1) numaralı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi'nin 336 ila 351. maddelerinde düzenlenmiştir. Anılan maddelerde; askerî okullardaki eğitim, askere alma, silah, araç, gereç ve her çeşit lojistik ihtiyaç maddelerinin tedariki, askerî fabrikalar ve tersaneler dâhil harp sanayii hizmetleri gibi ülke savunmasını doğrudan ilgilendiren hizmetler Bakanlığın görevleri arasında sayılmıştır. Dolayısıyla adı geçen Bakanlık ülke savunması bakımından çok önemli bir görev icra etmektedir. Dava konusu kuralla da Bakanlığın belirtilen özelliği ve (1) numaralı Cumhurbaşkanlığı Kararnamesi'nde yerine getirmekle görevlendirildiği hizmetlerin gerekli kıldığı şart ve vasıflar gözönünde bulundurulmak suretiyle Bakanlığa intibak edemediği tespit edilen personelin başka bir kuruma naklen atanmasına imkân tanındığı anlaşılmaktadır.

149. Kuralda Bakanlığın yukarıda sayılan özelliği ve hizmetin gerekli kıldığı şart ve vasıflar gözönüne alınarak Bakanlığa intibak edemeyen personelin başka kurumlara nakledilmesi öngörülmek suretiyle

naklen atama için asgari şartlar belirlenmiştir. Belirtilen şartları taşımadıkları ve Bakanlığa intibak edemedikleri üstlerince teklif edilenlerden Bakanlıkta oluşturulacak komisyona yaptırılacak tahkikat sonucuna göre Bakanca uygun görülenler başka kurum ve kuruluşlara nakledilecektir.

150. Bakanlığa intibak edemeyen personelden Bakanca uygun görülenlerin başka kurum ve kuruluşlara naklen atanması öngörülerek atama konusunda Bakan'a takdir yetkisi tanınmıştır. Ancak bu yetki sınırsız değildir. Bakan atama konusundaki takdir yetkisini kamu yararı ve hizmetin gereklerini gözeterek kullanmak durumundadır.

151. Nitekim Danıştayın yerleşik içtihatlarında da memurların atanmaları konusunda idarelerin takdir yetkisi bulunduğu ifade edilmekle birlikte bu yetkinin ancak kamu yararı ve hizmet gerekleri gözetilerek kullanılabilmesi kabul edilmiştir. Danıştaya göre atama yetkisinin kamu yararı ve hizmet gerekleri gözardı edilerek kullanıldığının kanıtlanması ya da idari yargı merciince saptanması hâlinde atama işlemi sebep ve maksat yönlerinden hukuka aykırı olacaktır (İdari Dava Daireleri Kurulu, E.2016/4927, K.2018/1784, 12/4/2018; 2D, E.2016/8093, K.2019/600, 14/2/2019; 5D, E.2016/18926, K.2019/2680, 10/4/2019).

152. Bu itibarla Bakanlığa intibak edemedikleri üstlerince teklif edilen personelden Bakanlıkta oluşturulacak komisyona yaptırılacak tahkikat sonucuna göre Bakanca uygun görülenlerin başka bir kurum veya kuruluşa naklen atanmasına imkân tanıyan kuralda belirlilik ilkesini ihlal eden bir yön bulunmamaktadır.

153. Açıklanan nedenlerle kural Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

J. Kanun'un 56. Maddesiyle 6191 Sayılı Kanun'a Eklenen Geçici 1. Maddenin İncelenmesi

154. Dava konusu kuralda, kuralın yürürlüğe girdiği tarihten önce millî güvenliğe tehdit oluşturduğu tespit edilen Fetullahçı Terör Örgütü (FETÖ)/Paralel Devlet Yapılanmasına (PDY) aidiyeti, iltisakı veya örgütle irtibatı nedeniyle sözleşmeleri feshedilen sözleşmeli erbaş ve erler hakkında 22/7/2016 tarihli ve 667 sayılı Olağanüstü Hal Kapsamında Alınan Tedbirlere İlişkin Kanun Hükmünde Kararname'nin (OHAL KHK) 4. maddesinin (2) ve (3) numaralı fıkralarının uygulanması öngörülmüştür.

155. 667 sayılı OHAL KHK'sının 4. maddesinin (2) numaralı fıkrasında görevine son verilenlerin bir daha kamu hizmetinde istihdam edilemeyeceği, doğrudan veya dolaylı olarak görevlendirilemeyeceği, görevinden çıkarılanların uhdelelerinde bulunan her türlü müteveli heyet, kurul, komisyon, yönetim kurulu, denetim kurulu, tasfiye kurulu üyeliği ve sair görevlerin de sona

ermiş sayılacağı ifade edilmiş; (3) numaralı fıkrasında da görevlerine son verilenlerin silah ruhsatlarının ve pilot lisanslarının iptal edileceği, oturdukları kamu konutlarından veya vakıf lojmanlarından on beş gün içinde tahliye edileceği, bu kişilerin özel güvenlik şirketlerinin kurucusu, ortağı ve çalışanı olamayacağı hüküm altına alınmıştır.

156. Dava konusu kural uyarınca FETÖ/PDY'ye aidiyeti, iltisakı veya örgütle irtibatı nedeniyle sözleşmeleri feshedilen sözleşmeli erbaş ve erler hakkında 667 sayılı OHAL KHK'sının 4. maddesinin (2) ve (3) numaralı fıkralarında sayılan mezkûr tedbirler uygulanacaktır.

157. Kuralın atıfta bulunduğu 667 sayılı OHAL KHK'sı 6749 sayılı Kanun ile kanunlaşmıştır. Bu çerçevede 667 sayılı OHAL KHK'sının 4. maddesinin (2) numaralı fıkrası da aynen kanunlaşmış, kanunlaştıktan sonra anılan fıkraya 25/7/2018 tarihli ve 7145 sayılı Kanun'un 21. maddesiyle "Birinci fıkra uyarınca kamu görevinden çıkarılan asker kişilerin askerî rütbeleri, mahkeme kararı aranmaksızın karar tarihinden geçerli olmak üzere geri alınır" şeklindeki cümle eklenmiştir.

158. Anılan OHAL KHK'sının 4. maddesinin (3) numaralı fıkrası ise "Bu maddeye göre görevlerine son verilenlerin silah ruhsatları ve pilot lisansları iptal edilir ve bu kişiler oturdukları kamu konutlarından veya vakıf lojmanlarından onbeş gün içinde tahliye edilir. Bu kişiler özel güvenlik şirketlerinin kurucusu, ortağı ve çalışanı olamazlar." şeklinde iken söz konusu fıkra TBMM'de görüşülürken fıkraya "...silah ruhsatları,..." ibaresinden sonra gelmek üzere "...gemi adamlığına ilişkin belgeleri..." ibaresi eklenerek kanunlaşmıştır. Dolayısıyla kuralın atıfta bulunduğu 667 sayılı OHAL KHK'sının 4. maddesinin (2) ve (3) numaralı fıkraları dava tarihinden sonra değişikliğe uğramıştır.

159. Açıklanan nedenle konusu kalmayan maddeye ilişkin iptal talebi hakkında karar verilmesine yer olmadığına karar vermek gerekir.

K. Kanun'un 60. Maddesiyle 657 Sayılı Kanun'un 48. Maddesinin Birinci Fıkrasının (A) Bendine Eklenen (8) Numaralı Alt Bendin İncelenmesi

1. İptal Talebinin Gerekçesi

160. Dava dilekçesinde özetle; kamu hizmetine girme hakkına ilişkin koşulların kanunla düzenlenmesinin zorunlu olduğu, dava konusu kuralla kamu görevine girişte güvenlik soruşturması ve/veya arşiv araştırması yapılması şartı öngörüldüğü hâlde soruşturma ve araştırmanın nasıl yapılacağına ilişkin herhangi bir düzenleme yapılmadığı, bireyin temel hak ve özgürlüklerini esaslı bir şekilde etkileyen ve sınırlandıran bir konuda yasama organının temel düzenlemeleri yapmayarak

uygulamaya ilişkin hususları idareye bırakmasının yasama yetkisinin devrine sebebiyet verdiği belirtilerek kuralın Anayasa'nın 2., 7., 13., 70. ve 128. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

161. 6216 sayılı Kanun'un 43. maddesi uyarınca kural, ilgisi nedeniyle Anayasa'nın 20. maddesi yönünden de incelenmiştir.

162. Kuralla güvenlik soruşturması ve/veya arşiv araştırması yapılması devlet memurluğuna alımlarda genel şartlar arasında sayılmıştır. Buna göre bir kişinin devlet memuru olabilmesi için güvenlik soruşturması ve/veya arşiv araştırmasının da yapılması gerekmektedir.

163. Anayasa'nın 20. maddesinin birinci fıkrasında, herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş; üçüncü fıkrasında da "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir" denilerek kişisel verilerin korunması özel hayatın gizliliğinin korunması kapsamında güvenceye kavuşturulmuştur. Anayasa'nın 13. maddesinde de temel hak ve hürriyetlerin yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği ifade edilmiştir.

164. Anayasa'nın 128. maddesinin ikinci fıkrasında "Memurların ve diğer kamu görevlilerinin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülükleri, aylık ve ödenekleri ve diğer özlük işleri kanunla düzenlenir. Ancak, malî ve sosyal haklara ilişkin toplu sözleşme hükümleri saklıdır" hükmüne yer verilerek memurlar ve diğer kamu görevlilerinin nitelikleri ve atanmalarına ilişkin hususların kanunla düzenleneceği belirtilmiştir.

165. Kanuni düzenleme ilkesi, düzenlenen alanda temel ilkelerin kanunla konulmasını ve çerçevenin kanunla çizilmesini ifade etmektedir. Bu ilke uyarınca kamu görevlilerinin nitelikleri ve atanmalarına ilişkin kuralların kanunda gösterilmesi, kuralın açık, anlaşılır ve sınırlarının belli olması gerekmektedir.

166. Kişisel verilerin korunmasını isteme hakkı, insan onurunun korunması ve bireyin kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır.

167. Anayasa'nın 20. maddesi uyarınca kişisel veriler ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir. Dolayısıyla kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvencenin yaşama geçirilebilmesi için bu hakkı ilgilendiren yasal düzenlemelerin açık, anlaşılabilir ve söz konusu hakkın kullanılabilmesine elverişli olması gerekir. Ancak böyle bir düzenleme ile kişilerin özel hayatlarını ilgilendiren veri, bilgi ve belgelerin resmî makamların keyfî müdahalelerine karşı korunması mümkün hâle gelebilir.

168. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3. maddesine göre kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Anayasa Mahkemesinin yerleşik kararlarında da belirtildiği üzere "...adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler..." kişisel veri olarak kabul edilmektedir (AYM, E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2014/74, K.2014/201, 25/12/2014; E.2014/180, K.2015/30, 19/3/2015; E.2015/32, K.2015/102, 12/11/2015).

169. Bu bağlamda güvenlik soruşturması ve arşiv araştırmasıyla elde edilen veriler kişisel veri niteliğindedir. Kuralla güvenlik soruşturması ve arşiv araştırması kapsamında kamu mercileri tarafından özel yaşamı ile ilgili sorular sorulması da dâhil olmak üzere bir bireyin özel hayatı, iş ve sosyal yaşamıyla ilgili bilgilerinin alınması, kaydedilmesi ve kullanılması özel hayata saygı hakkına sınırlama niteliğindedir.

170. Anayasa'nın 129. maddesinin birinci fıkrasında memurlar ve kamu görevlilerinin Anayasa ve kanunlara sadık kalarak faaliyette bulunma yükümlülükleri düzenlenmiştir. Belirtilen hususlar gözetilerek kamu görevlerine atanacak kişiler bakımından birtakım şartlar getirilmesi doğaldır. Bu şekilde aranan nitelikler kamu hizmetinin etkin ve sağlıklı bir biçimde yürütülmesi amacına yöneliktir. Dolayısıyla kamu görevine atanmadan önce kişilerin güvenlik soruşturması ve arşiv araştırmasının yapılmasını öngören kural kanun koyucunun takdir yetkisindedir. Ancak bu alanda düzenleme getiren kuralların kamu makamlarına hangi koşullarda ve hangi sınırlar içinde tedbirler uygulama ve özel hayatın gizliliğine yönelik müdahalelerde bulunma yetkisi verildiğini yeterince açık olarak göstermesi ve olası kötüye kullanımlara karşı yeterli güvenceleri sağlaması gerekir.

171. Kuralda güvenlik soruşturması ve/veya arşiv araştırması yapılması memurluğa alımlarda genel şartlar arasında sayılmasına karşın güvenlik soruşturmasına ve arşiv araştırmasına konu edilecek

bilgi ve belgelerin neler olduğuna, bu bilgilerin ne şekilde kullanılacağına, hangi mercilerin soruşturma ve araştırmayı yapacağına ilişkin herhangi bir düzenleme yapılmamıştır. Diğer bir ifadeyle güvenlik soruşturması ve arşiv araştırmasının yapılmasına ve elde edilecek verilen kullanılmasına ilişkin temel ilkeler belirlenmeksizin kuralla sadece güvenlik soruşturması ve arşiv araştırması yapılması devlet memurluğuna alımlarda aranacak şartlar arasında sayılmıştır.

172. Güvenlik soruşturması ve arşiv araştırması sonucunda devlet memurluğuna atanmada esas alınacak kişisel veri niteliğindeki bilgilerin alınmasına, kullanılmasına ve işlenmesine yönelik güvenceler ve temel ilkeler kanunla belirlenmeksizin bunların alınmasına ve kullanılmasına izin verilmesi Anayasa'nın 13., 20. ve 128. maddeleriyle bağdaşmamaktadır.

173. Açıklanan nedenlerle kural Anayasa'nın 13., 20. ve 128. maddelerine aykırıdır. İptali gerekir.

M. Emin KUZ bu görüşe katılmamıştır.

Kural Anayasa'nın 13., 20. ve 128. maddelerine aykırı görülerek iptal edildiğinden ayrıca Anayasa'nın 2., 7. ve 70. maddeleri yönünden incelenmemiştir.

L. Kanun'un 61. Maddesiyle 657 Sayılı Kanun'un 125. Maddesinin Birinci Fıkrasının (E) Bendine Eklenen (I) Alt Bendinde Yer Alan "...eylem birliği içerisinde olmak,..." İbaresinin İncelenmesi

1. İptal Talebinin Gerekçesi

174. Dava dilekçesinde özetle; dava konusu kuralla devlet memurluğundan çıkarılma nedeni olarak gösterilen terör örgütleriyle eylem birliği içerisinde olmak kavramının belirsiz ve öngörülemez olduğu, bu suretle kamu görevine girme hakkına ölçsüz bir sınırlama getirildiği belirtilerek kuralın Anayasa'nın 2., 13., 38. ve 70. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

175. 6216 sayılı Kanun'un 43. maddesi uyarınca kural, ilgisi nedeniyle Anayasa'nın 128. maddesi yönünden de incelenmiştir.

176. Kuralda terör örgütleriyle eylem birliği içerisinde olmak devlet memurluğundan çıkarma cezası ile cezalandırılacak fiiller ve hâller arasında sayılmıştır.

177. Anayasa'nın 128. maddesinin ikinci fıkrasında memurlar ve diğer kamu görevlileri özlük hakları bakımından yasal güvenceye kavuşturulmuştur. Memurlar ve diğer kamu görevlilerinin statü haklarını doğrudan etkileyen disiplin işlemlerinin anılan fıkrada yer alan diğer özlük işleri kavramı kapsamına girdiğinde kuşku bulunmamaktadır.

178. Disiplin cezaları, kamu hizmetlerinin yürütülmesi ve kamu yararının devamlılığının sağlanması amacıyla yasal olarak düzenlenmiş idari yaptırımlardır. Kamu hizmetlerini yürütenlerin görev anlayışları, yetki ve sorumlulukları kamu hizmeti ve hizmet gerekleri ile sınırlandırılmış; bu sınırlar dışına çıkanların ise disiplin cezaları ile cezalandırılmaları ilgili kanunlarda öngörülmüştür.

179. Anayasa'nın 38. maddesinin birinci fıkrasında "Kimse, işlendiği zaman yürürlükte bulunan kanunun suç saymadığı bir fiilden dolayı cezalandırılmaz" denilerek suçun kanuniliği ilkesi, üçüncü fıkrasında ise "Ceza ve ceza yerine geçen güvenlik tedbirleri ancak kanunla konulur" ifadesine yer verilerek cezanın kanuniliği ilkesi getirilmiştir. Anayasa'nın 38. maddesinde yer alan suçta ve cezada kanunilik ilkesi uyarınca hangi eylemlerin yasaklandığı ve bu yasak eylemlere verilecek cezaların hiçbir kuşkuyla yer bırakmayacak biçimde kanunda gösterilmesi kuralın açık, anlaşılır ve sınırlarının belli olması gerekmektedir. Kişilerin yasak eylemleri önceden bilmeleri gerektiği düşüncesine dayanan bu ilkeyle temel hak ve özgürlüklerin güvence altına alınması amaçlanmaktadır.

180. Anayasa'nın 38. maddesinde idari suç ve cezalar ile adli suç ve cezalar arasında bir ayrım yapılmadığından her ikisi de bu maddede öngörülen ilkelere tabidir. Adli ve idari suçlarda davranış normlarına aykırı ve haksızlık teşkil eden bir fiille kanun koyucunun koruma altına aldığı bir hukuki değer ihlali söz konusu olup adli ve idari cezaların her ikisi de cebir içermektedir.

181. Korunan hukuki değer ile ihlalin neden olduğu hukuki sonuçların aynı olmaması ise idari suç ve cezalar ile adli suç ve cezalar arasındaki temel farklılığı oluşturmaktadır. Adli para cezalarından daha yüksek miktarlarda idari para cezalarının verilebilmesine imkân tanıyan düzenlemeler de bulunmakla birlikte adli suçlar için öngörülen cezaların idari suçlar için öngörülen cezalardan genellikle daha ağır olması, hürriyeti bağlayıcı cezaların kural olarak adli suçlar yönünden geçerli olabilmesi, idari suçlarda kanun koyucunun daha az önem attığı bir hukuki değer ihlal edilmesi ve öngörülen yaptırımın da genellikle idari bir makam tarafından idari usuller izlenerek uygulanması nedeniyle Anayasa'nın 38. maddesindeki ilkelerin aynı boyut ve kapsamıyla idari suçlara da uygulanması işin mahiyetine uygun düşmemektedir. Bu bağlamda yasama organının ağır işleyen yapısı ile ekonomik ve teknik hayatın hızla değişen ve gelişen şartları gözetilerek suç ve cezalarda kanunilik ilkesinin idari suçlar yönünden daha esnek uygulanması gerekmektedir.

182. Buna karşılık suçta ve cezada kanunilik ilkesinin daha esnek uygulandığı idari yaptırımlara ilişkin düzenlemelerin yalnızca kanun metninde yer alması yeterli değildir. Anayasa Mahkemesinin 14/1/2015 tarihli ve E.2014/100, K.2015/6 sayılı kararında da vurgulandığı üzere söz konusu düzenlemelerin içerik bakımından da belirli amacı gerçekleştirmeye elverişli olması gerekir. Bu

açından kanun, bireylerin hangi somut fiil ve olguya hangi hukuksal yaptırımın veya sonucun bağlandığını belirli bir açıklık ve kesinlikte öngörebilmelerine imkân verecek nitelikte olmalıdır.

183. Hukuk devletinin temel ilkelerinden biri belirliliktir. Belirlilik ilkesi, yalnızca yasal belirliliği değil daha geniş anlamda hukuki belirliliği de ifade etmektedir. Yasal düzenlemeye dayanarak erişilebilir, bilinebilir ve öngörülebilir olma gibi gereklilikleri karşılama koşuluyla mahkeme içtihatları ile de hukuki belirlilik sağlanabilir. Hukuki belirlilik ilkesinde asıl olan, bir hukuk normunun uygulanmasıyla ortaya çıkacak sonuçların o hukuk düzeninde öngörülebilir olmasıdır.

184. Terör kavramı 3713 sayılı Kanun'da tanımlanmıştır. Kanun'un 1. maddesine göre terör; cebir ve şiddet kullanarak, baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Cumhuriyet'in Anayasa'da belirtilen niteliklerini, siyasi, hukuki, sosyal, laik, ekonomik düzeni değiştirmek, devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk devletinin ve Cumhuriyet'in varlığını tehlikeye düşürmek, devlet otoritesini zaafa uğratmak, yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir. Terör örgütleri de anılan maddede sayılan amaçlara yönelik olarak suç işlemek üzere meydana getirilmiş örgütlerdir.

185. Kuralla terör örgütleriyle eylem birliği içerisinde olmak devlet memurluğundan çıkarma cezasını gerektiren fiiller arasında sayılmıştır. Kurala göre devlet memurluğundan çıkarma cezasının uygulanabilmesi için öncelikle 3713 sayılı Kanun'un 1. maddesinde belirtilen amaçlara ulaşmak için meydana getirilmiş bir örgüt tarafından gerçekleştirilen somut bir terör eylemi olması, devlet memurunun da aynı amaçla bu eyleme fiilî olarak müdahil olması gerekmektedir.

186. Terör örgütüyle eylem birliği içinde olmak her bir terör eylemine göre farklılık gösterebilir. Türk devletinin ve Cumhuriyet'in varlığını tehlikeye düşürmek amacıyla gerçekleştirilen terör eylemleri ile devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla gerçekleştirilen eylemler, amacı gereği farklı şekilde gerçekleştirilebilir. Dolayısıyla belirtilen amaçlar çerçevesinde gerçekleştirilen eylemlerde kamu görevlilerinin ne tür bir eylem birliği içinde olacaklarının önceden belirlenmesi zordur. Bu nedenle kanun koyucunun genel bir belirleme yaparak terör örgütleriyle eylem birliği içinde bulunanların devlet memurluğundan çıkarma cezası ile cezalandırılmalarını öngördüğü anlaşılmaktadır. Bir başka ifadeyle anılan şekilde genel bir belirleme yapılması kuralın belirsizlik taşıdığı veya keyfiliğe karşı gerekli kanuni güvenceyi taşımadığı anlamına gelmemekte, kanun yapma tekniğinin doğasından kaynaklanmaktadır. Zira kanun kurallarının genel olması, somut olayın özelliğine göre değişebilecek tüm çözümleri kuralın bünyesinde barındırma, bir başka

ifadeyle kuralın amaca uygun sonuca ulaştıracak herhangi bir çözümü dışlamasını önleme ihtiyacından kaynaklanmaktadır. Terör örgütleriyle eylem birliği içinde olma fiili somut olayın özelliğine göre kanuna dayalı olarak idare tarafından belirlenecek ise de idarenin bu işlemi mahkeme tarafından denetleneceğinden bu fiilin nihai olarak kapsamı kanuna dayalı olarak yargı kararıyla ortaya konulacaktır. Dolayısıyla kuralın belirsiz ve öngörülemez olduğu söylenemez.

187. Açıklanan nedenlerle kural Anayasa'nın 2., 38., ve 128. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

Kuralın Anayasa'nın 13. ve 70. maddeleriyle ilgisi görülmemiştir.

M. Kanun'un 62. Maddesiyle 663 Sayılı Kanun Hükmünde Kararname'ye Eklenen 45/A Maddesinin (2) Numaralı Fıkrasının İncelenmesi

1. İptal Talebinin Gerekçesi

188. Dava dilekçesinde özetle; Sağlık Bakanlığına (Bakanlık) sözleşmeli personel olarak atanmak için 663 sayılı KHK'nın 45/A maddesinin (1) numaralı fıkrasında belirtilen objektif ölçütler dışında dava konusu kuralla sözlü sınavdan başarılı olma şartı getirilerek atama konusunda idareye sınırları belirsiz bir yetki verildiği, Bakanlığın takdirine göre sözleşmeli personel için sözlü sınav şartı getirilmesinin Bakanlıkta görev yapan diğer personelle sözleşmeli personel arasında eşitsizliğe sebebiyet verdiği belirtilerek kuralın Anayasa'nın 2. ve 10. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

189. 6216 sayılı Kanun'un 43. maddesi uyarınca kural, ilgisi nedeniyle Anayasa'nın 7. ve 128. maddeleri yönünden de incelenmiştir.

190. Kuralda, Bakanlıkta ve bağlı kuruluşlarında sağlık hizmetleri ve yardımcı sağlık hizmetleri sınıfında istihdam edilecek sözleşmeli sağlık personelinin Kamu Personeli Seçme Sınavı (KPSS) sonucuna göre Bakanlık ve bağlı kuruluşlarına Ölçme, Seçme ve Yerleştirme Merkezi (ÖSYM) Başkanlığı tarafından yapılacak yerleştirme ile atanabileceği gibi pozisyon ve ihtiyaç durumuna göre KPSS puanı esas alınarak Bakanlık tarafından yapılacak sözlü sınavla da atama yapılabileceği, sözlü sınav ve yerleştirmeye ilişkin usul ve esasların Bakanlıkça belirleneceği hüküm altına alınmıştır.

191. Anayasa'nın 10. maddesinde "Herkes, dil, ırk, renk, cinsiyet, siyasî düşünce, felsefî inanç, din, mezhep ve benzeri sebeplerle ayırım gözetilmeksizin kanun önünde eşittir./ Kadınlar ve erkekler eşit haklara sahiptir. Devlet, bu eşitliğin yaşama geçmesini sağlamakla yükümlüdür. Bu maksatla

alınacak tedbirler eşitlik ilkesine aykırı olarak yorumlanamaz./ Çocuklar, yaşlılar, özürllüer, harp ve vazife şehitlerinin dul ve yetimleri ile malul ve gaziler için alınacak tedbirler eşitlik ilkesine aykırı sayılmaz./ Hiçbir kişiye, aileye, zümreye veya sınıfa imtiyaz tanınamaz./ Devlet organları ve idare makamları bütün işlemlerinde kanun önünde eşitlik ilkesine uygun olarak hareket etmek zorundadırlar.” denilmek suretiyle kanun önünde eşitlik ilkesine yer verilmiştir.

192. Anayasa'nın anılan maddesinde belirtilen kanun önünde eşitlik ilkesi hukuksal durumları aynı olanlar için söz konusudur. Bu ilke ile eylemli değil hukuksal eşitlik öngörölmüştür. Eşitlik ilkesinin amacı aynı durumda bulunan kişilerin kanunlar karşısında aynı işleme bağı tutulmalarını sağlamak, ayırım yapılmasını ve ayrıcalık tanınmasını önlemektir. Bu ilkeyle, aynı durumda bulunan kimi kişi ve topluluklara ayrı kurallar uygulanarak kanun karşısında eşitliğin ihlali yasaklanmıştır. Kanun önünde eşitlik herkesin her yönden aynı kurallara bağı tutulacağı anlamına gelmez. Durumlarındaki özellikler, kimi kişiler ya da topluluklar için değişik kuralları ve uygulamaları gerektirebilir. Aynı hukuksal durumlar aynı, ayrı hukuksal durumlar farklı kurallara bağı tutulursa Anayasa'da öngörülen eşitlik ilkesi zedelenmez.

193. Sağlık hizmetleri niteliğı itibarıyla belli bir düzen içinde sunulması gereken, kişilerin ve toplumun varlığı ve huzuru yönünden vazgeçilemez, ertelenemez ve ikame edilemez hizmetlerdendir. Sözleşmeli personel tarafından sunulacak sağlık hizmetleri devletin genel idare esaslarına göre yürütmekle yükümlü olduğı kamu hizmetinin gerektirdiğı asli ve sürekli görevlerdendir. Bu görevleri yerine getiren sözleşmeli personel Anayasa'nın 128. maddesinde yer alan diğerk kamu görevlisi kapsamındadır. Dolayısıyla sözleşmeli sağlık personelinin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlölükleri, aylık ve ödenekleri ile diğerk özlük işlerine yönelik temel ilkelerin kanunla belirlenmesi gerekmektedir.

194. Kanun koyucu, Anayasa'ya uygun olması koşuluyla kamu görevine girişte yapılacak sınavların türü, biçimi ve usulleri hakkında düzenleme yapma yetkisine sahip olup düzenlemenin kamu yararına, başka bir anlatımla ülke koşullarına uygun olup olmadığının belirlenerek takdir edilmesi kanun koyucuya aittir. Anayasa'ya uygunluk denetiminde kanun koyucunun kamu yararı anlayışının isabetli olup olmadığı değil incelenen kuralın kamu yararı dışında belli bireylerin ya da grupların çıkarları gözetilerek kanunlaştırılmış olup olmadığı incelenebilir.

195. Kamu görevlilerinin devlet ile olan ilişkileri statü hukuku içinde yürütölmektedir. Devlet, statüleri kanunlarla belirlenen ve bu statü kurallarına göre mesleğe alınan kamu görevlilerine atama, yükselme, aylık, ödöl, nakil ve sınav gibi hak veya yükümlölükler getirebilir.

196. Kuralla Bakanlığa KPSS sonucuna göre ya da pozisyon ve ihtiyaç durumuna göre KPSS puanı esas alınarak sözlü sınavla sözleşmeli personel atama yetkisi verilmiştir. Kurala göre sözlü sınavla personel alımı ancak yıl içinde ortaya çıkacak olağan dışı personel ihtiyacını karşılamak amacıyla yapılabilecektir. Bu tercih Bakanlığın anılan görevlere atamada kamu yararını sağlamaya dönük takdir yetkisinin kullanımından ibarettir. Sözlü sınav sonucuna göre personel istihdam edilmesiyle kamu yararının gerçekleşip gerçekleşmeyeceği ise subjektif bir husus olup anayasallık denetiminin kapsamı dışında kalmaktadır.

197. Bakanlık, kural olarak merkezî yerleştirme ile personel alımını gerçekleştirmektedir. Ancak yıl içinde ortaya çıkacak olağan dışı durumlar nedeniyle sözleşmeli personel alımına ihtiyaç duyulabilir. Kuralla bu gibi durumlarda KPSS sonucu esas alınarak sözlü sınavla da personel alımına imkân tanınarak Bakanlığın personel ihtiyacının giderilmesinin hedeflendiği anlaşılmaktadır. Sözlü sınavla alınması öngörülen sözleşmeli personel, atanma sebepleri bakımından diğer personelle aynı konumda değildir.

198. Bu nedenle ihtiyaç durumunda alınması öngörülen sözleşmeli personel için sözlü sınav şartı getirilmesini öngören kuralın birinci cümlesinde hukuk devleti ve eşitlik ilkelerine aykırılık bulunmadığı gibi kuralda anılan şart kanunla öngörüldüğünden kuralın yasama yetkisinin devredilmezliği ve kamu görevlilerinin statülerinin kanunla düzenlenmesi ilkelerini ihlal eden bir yönü de bulunmamaktadır.

199. Kamu görevlisi statüsünde olan sözleşmeli sağlık personelinin sözlü sınavla mesleğe alınması kanun koyucunun takdir yetkisinde olmakla birlikte bu personelin sözlü sınavla mesleğe alınmasına ve yerleştirilmesine ilişkin temel ilkelerin Anayasa'nın 128. maddesi uyarınca kanunla düzenlenmesi ve bu bağlamda Anayasa'nın 7. maddesi uyarınca yasama yetkisinin idareye devredilmemesi gerekir.

200. Kuralın ikinci cümlesinde sözlü sınav ve yerleştirmeye ilişkin usul ve esasların Bakanlıkça belirleneceği öngörülmüştür. Kanun'da sözlü sınavda hangi ölçütlerin gözetileceği hususlarına yer verilmediği gibi sınavı kazanan adayların yerleştirilmesinde uygulanacak esaslara ilişkin herhangi bir düzenleme de yapılmamıştır. Diğer bir ifadeyle Kanun'da sözlü sınav ve sınav sonrası yerleştirmeye ilişkin temel ilkeler belirlenmemiş ve kuralın ikinci cümlesiyle bu hususların düzenlenmesi yönetmeliğe bırakılmıştır.

201. Bakanlıkta istihdam edilecek sözleşmeli personelin sözlü sınavla mesleğe alımına ve yerleştirilmelerine ilişkin temel ilkelerin kanunda belirlenmeksizin yönetmelikle düzenlenmesine imkân tanınması kamu görevlilerinin statülerinin kanunla düzenlenmesine ve yasama yetkisinin devredilmezliğine ilişkin anayasal ilkelerle bağdaşmamaktadır.

202. Açıklanan nedenlerle kuralın birinci cümlesi Anayasa'nın 2., 7., 10. ve 128. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

203. Kuralın ikinci cümlesi Anayasa'nın 7. ve 128. maddelerine aykırıdır. İptali gerekir.

Kuralın ikinci cümlesi Anayasa'nın 7. ve 128. maddelerine aykırı görülerek iptal edildiğinden ayrıca Anayasa'nın 2. ve 10. maddeleri yönünden incelenmemiştir.

N. Kanun'un 62. Maddesiyle 663 Sayılı Kanun Hükmünde Kararname'ye Eklenen 45/A Maddesinin (3) Numaralı Fıkrasının İncelenmesi

204. Kuralda yer alan "...dört..." ibaresi 27/6/2019 tarihli ve 7180 sayılı Kanun'un 19. maddesiyle "...üç..." şeklinde değiştirilmiştir.

205. Açıklanan nedenle konusu kalmayan fıkraya ilişkin iptal talebi hakkında karar verilmesine yer olmadığına karar vermek gerekir.

O. Kanun'un 73. Maddesiyle 3713 Sayılı Kanun'a Eklenen Geçici 16. Maddenin İkinci Cümlesinin İncelenmesi

1. Anlam ve Kapsam

206. 3713 sayılı Kanun'un dava konusu kuralın da atıfta bulunduğu 21. maddesinde terör eylemlerinden zarar gören, terörle mücadelede yaralanan ya da hayatını kaybeden kamu görevlilerine yapılacak yardımlar düzenlenmiştir.

207. Anılan maddede yer alan yardımlardan biri de terörle mücadeleden dolayı köyleri boşaltılan üniversite çağındaki öğrencilere ve ölenlerin çocuklarına burs verilmesidir. Anılan maddenin birinci fıkrasının 29/6/2006 tarihli ve 5532 sayılı Kanun'un 15. maddesiyle değiştirilen (1) bendinde, sözü edilen öğrencilere yüksek öğrenimleri süresince devletçe karşılıksız burs verilmesi öngörülmüştür.

208. Ancak 7070 sayılı Kanun'un 72. maddesiyle 3713 sayılı Kanun'un 21. maddesinin birinci fıkrasının (1) bendi yürürlükten kaldırılarak karşılıksız burs uygulamasına son verilmiştir. Bununla birlikte 7070 sayılı Kanun'un 73. maddesiyle 3713 sayılı Kanun'a geçici 16. madde eklenerek maddenin yürürlüğe girdiği tarih itibarıyla 21. maddenin birinci fıkrasının mülga (1) bendi kapsamında Yüksek Öğrenim Kredi ve Yurtlar Kurumundan (YURTKUR) burs almakta olanların burslarının normal öğrenim sürelerinin sonuna kadar ilgili mevzuat hükümlerine göre verilmesine imkân tanınmıştır.

209. Dava konusu kuralda ise 3713 sayılı Kanun'un 21. maddesinin birinci fıkrasının mülga (1) bendine istinaden yargı mercilerinde YURTKUR aleyhine açılan davalardan feragat edilmiş

sayılacağı hüküm altına alınmıştır. Buna göre karşılıksız burs uygulaması sona ermekle birlikte karşılıksız burs uygulamasının devam ettiği tarihte ilgililer tarafından açılan ancak uygulamanın sona erdiği tarih itibarıyla henüz sonuçlanmamış davalar feragatle sonuçlanmış sayılacaktır.

2. İptal Talebinin Gerekçesi

210. Dava dilekçesinde özetle; dava konusu kuralla tarafların rızası olmaksızın, YURTKUR aleyhine açılan davalardan feragat edilmiş sayılmasının hukuk devleti ilkesine aykırı olduğu, hak arama özgürlüğünün engellendiği belirtilerek kuralın Anayasa'nın 2. ve 36. maddelerine aykırı olduğu ileri sürülmüştür.

3. Anayasa'ya Aykırılık Sorunu

211. 6216 sayılı Kanun'un 43. maddesi uyarınca kural, ilgisi nedeniyle Anayasa'nın 13. maddesi yönünden de incelenmiştir.

212. Anayasa'nın 36. maddesinde düzenlenen adil yargılanma hakkı, kişilere davanın görüldüğü mahkemeden uyuşmazlığa ilişkin bir karar verilmesini isteme güvencesini de içermektedir.

213. Karar hakkı genel itibarıyla mahkeme önüne getirilen uyuşmazlığın karara bağlanmasını isteme hakkını ifade etmektedir. Dava hakkını kullanan bireyin asıl amacı davanın sonunda, uyuşmazlık konusu ettiği talebinin esasıyla ilgili olarak bir karar elde edebilmektir. Dava sonucunda bir karar elde edilemiyorsa dava açmanın da bir anlamı kalmayacaktır. Bununla birlikte karar hakkı bireylerin sadece yargılama sonucunda şekli anlamda bir karar elde etmelerini güvence altına almaz. Bu hak aynı zamanda dava konusu edilen uyuşmazlığa ilişkin esaslı taleplerin yargı merciince bir sonuca bağlanmasını da gerektirir.

214. Diğer taraftan görülmekte olan bir davada tarafların esasa ilişkin taleplerinin her durumda incelenmesi beklenemez. Süre aşımı, düşme veya tarafların kendi rızalarıyla davadan vazgeçmesi gibi usule ilişkin nedenlerden dolayı uyuşmazlığın esasına yönelik karar vermeden de davanın sonlandırılması mümkündür. Söz konusu hakkın sağladığı güvence bakımından önemli olan husus; açıldığı sırada davanın -usule ilişkin sorunlar hariç- uyuşmazlığın esasını çözüme kavuşturma imkânına sahip, bir başka ifadeyle dava açılmasındaki asıl amacı gerçekleştirmeye elverişli olmasıdır. Bu nitelikleri taşıyan bir davada yargılamanın henüz devam ettiği bir süreçte, taraflardan birinin aleyhine olacak ve yargı merciinin uyuşmazlık konusu talep hakkında karar vermesini engelleyecek şekilde davayı ortadan kaldıran ya da davanın incelenmesini durdurarak karara bağlanmasına engel olan kanunlar çıkarılmasının karar hakkına müdahale teşkil edeceği açıktır.

215. Kanun koyucunun uyuşmazlıkların bir an önce sonlandırılması ve yeni uyuşmazlıkların ortaya çıkmasının önüne geçilerek dava sayısının azaltılması suretiyle adalet hizmetlerinin iyi bir şekilde işlemlenmesini sağlamak, böylece toplumsal barışın tesis edilmesine de katkıda bulunarak nihai olarak kamu yararını gerçekleştirmek amacıyla belirli konulardaki uyuşmazlıklara ilişkin davaların ortadan kaldırılmasına yönelik düzenlemeler yapma konusunda takdir yetkisine sahip olduğu tartışmasızdır. Ancak bu yetkinin karar hakkına aykırı olarak kullanılmaması gerekir.

216. Kuralla yargı merciince uyuşmazlığın esasının incelenmesi imkânı ve dolayısıyla bireyin bu hususta bir karar elde etme imkânı ortadan kaldırıldığından kuralın karar hakkına bir sınırlama getirdiği açıktır. Anayasa'nın 13. maddesinde yer alan ölçülülük kriterinin alt ilkelerinden olan orantılılık ilkesi, kamu yararının korunması ile bireyin hak ve özgürlükleri arasında adil bir dengeyi sağlanmasını gerekli kılmaktadır. Öngörülen tedbirin bireyi olağan dışı ve aşırı bir yük altına sokması durumunda getirilen sınırlamanın orantılı ve dolayısıyla ölçülü olduğundan söz edilemez. Bu itibarla uygulanan tedbirle bireye aşırı ve orantısız bir yük yüklenmemesi gerekmektedir. Bu bağlamda bireyin ortadan kaldırılan davayı açmakla elde etmek istediği maddi uyuşmazlığa ilişkin menfaatlerini kısmen de olsa korumaya, telafi etmeye yönelik birtakım imkânlardan faydalandırıldığı durumlarda davanın ortadan kaldırılmasının bireye aşırı ve katlanılamaz bir külfet yüklediği, dolayısıyla müdahalenin ölçüsüz olduğu söylenemez.

217. 6/1/1982 tarihli ve 2577 sayılı İdari Yargılama Usulü Kanunu'nun 31. maddesinin (1) numaralı fıkrasında, bu Kanun'da hüküm bulunmayan hâllerde davadan feragat hakkında Hukuk Usulü Muhakemeleri Kanunu'nun uygulanacağı belirtilmiştir.

218. Davadan feragat 12/1/2011 tarihli ve 6100 sayılı Hukuk Muhakemeleri Kanunu'nda düzenlenmiştir. 6100 sayılı Kanun'un 307. maddesinde feragat "...davacının, talep sonucundan kısmen veya tamamen vazgeçmesidir" şeklinde tanımlanmış; 311. maddesinde de feragatin kesin hüküm gibi sonuç doğuracağı belirtilmiştir. Buna göre idari yargı mercilerinde açılan davalarda davacının kendi iradesiyle talep sonucundan feragat etmesi durumunda uyuşmazlığın esası hakkında bir karar verilmeksizin feragat nedeniyle dava kesin hükümlerle sonuçlanacaktır.

219. Dava konusu kuralda ise 3713 sayılı Kanun'un 21. maddesinin birinci fıkrasının mülga (1) bendine istinaden yargı mercilerinde YURTKUR aleyhine açılan davaların davacının iradesi olmaksızın feragatle sonuçlanacağı hüküm altına alınmıştır. Buna göre söz konusu davalarda davacının talep sonucundan vazgeçmesi kendi iradesine göre değil kanun hükmü nedeniyle gerçekleşmektedir. 7070 sayılı Kanun'un 73. maddesiyle 3713 sayılı Kanun'a geçici 16. madde eklenerek maddenin yürürlüğe girdiği tarih itibarıyla 21. maddenin birinci fıkrasının mülga (1) bendi

kapsamında YURTKUR'dan burs almakta olanların burslarının, normal öğrenim sürelerinin sonuna kadar ilgili mevzuat hükümlerine göre verilmesine imkân tanınmış ise de anılan düzenleme sadece maddenin yürürlüğe girmesinden önce burs almakta olanlara yönelik olup bu şekilde burs almaya devam edenler yönünden dava konusu kuralın önemli bir uygulama alanı bulmayacağı söylenebilir. Zira söz konusu kişiler yönünden bursun ödenmeye devam etmesi öngörüldüğünden bunların bursun ödenmesiyle ilgili dava açmaları beklenecek bir durum olarak görünmemektedir. Ancak 7070 sayılı Kanun'un 72. maddesiyle 3713 sayılı Kanun'un 21. maddesinin birinci fıkrasının (1) bendi yürürlükten kaldırılmadan önce söz konusu bursu alma koşulları oluşan ancak çeşitli nedenlerle burs bağlanmayan, dolayısıyla 3713 sayılı Kanun'un 21. maddesinin birinci fıkrasının mülga (1) bendine istinaden yargı mercilerinde YURTKUR aleyhine açılan davalar yönünden de davacının davasından feragat etmiş sayılmasını öngören dava konusu kuralın esas itibarıyla bu durumda olan davacılar üzerinde etkili olabileceği anlaşılmaktadır.

220. 3713 sayılı Kanun'un geçici 16. maddesi gerekçesiyle birlikte değerlendirildiğinde anılan hükümle 3713 sayılı Kanun'un 21. maddesinin birinci fıkrasının (1) bendi yürürlükten kaldırılmadan önce söz konusu bursu alma koşulları oluşan ancak çeşitli nedenlerle burs sağlanmayan kişiler yönünden uyuşmazlık konusu olgunun esasına dair bir düzenleme getirilmediği, öte yandan yargı merciine de uyuşmazlığın esası hakkında herhangi bir değerlendirme yapma imkânı tanınmamak suretiyle sadece bu hususta açılan mevcut davaların ortadan kaldırılmasının amaçlandığı, bu süreçte ilgililerin söz konusu davayı açmakla elde etmek istedikleri, maddi uyuşmazlığa ilişkin menfaatlerinin kısmen de olsa telafi etmeye yönelik herhangi bir güvenceye yer verilmediği görülmektedir. Üstelik yargılama usulü kurallarına göre doğrudan davacının açık iradesine bağlı kılınan davadan feragat etme hususunda bireye herhangi bir seçenek de tanınmamıştır.

221. Söz konusu davalar hakkında her ne kadar şekli olarak bir karar verilmesi öngörülmüşse de kuralın yukarıda açıklanan çerçevede uyuşmazlığı maddi yönden çözüme kavuşturmadığı, sadece davayı davacının tamamen aleyhine olacak şekilde ve üstelik onun iradesi dışında ortadan kaldırdığı, bu yönüyle kuralın bireyin dava açmaktaki gayesiyle bağdaşmadığı anlaşılmaktadır.

222. Kanun'da bireye, sınırlama ile ortadan kaldırılan davayı açmakla elde etmek istediği menfaatlerini kısmen de olsa telafi etmeye yönelik herhangi bir imkân sağlanmadığı da dikkate alındığında bu durumun bireye aşırı ve orantısız bir külfet yüklediği sonucuna ulaşılmaktadır. Buna göre söz konusu kural karar hakkına orantısız, dolayısıyla ölçüsüz bir sınırlama getirmektedir.

223. Açıklanan nedenlerle kural Anayasa'nın 13. ve 36. maddelerine aykırıdır. İptali gerekir.

Kural Anayasa'nın 13. ve 36. maddelerine aykırı görülerek iptal edildiğinden ayrıca Anayasa'nın 2. maddesi yönünden incelenmemiştir.

IV. İPTALİN DİĞER KURALLARA ETKİSİ

224. 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrasında; başvurunun kanunun, Cumhurbaşkanlığı kararnamesinin veya Türkiye Büyük Millet Meclisi İçtüzüğü'nün sadece belirli madde veya hükümleri aleyhine yapılmış olup da bu madde veya hükümlerin iptalinin kanunun, Cumhurbaşkanlığı kararnamesinin veya Türkiye Büyük Millet Meclisi İçtüzüğü'nün diğer bazı hükümlerinin veya tamamının uygulanamaması sonucunu doğurması hâlinde -keyfiyeti gerekçesinde belirtilmek şartıyla- uygulanma imkânı kalmayan kanunun, Cumhurbaşkanlığı kararnamesinin veya Türkiye Büyük Millet Meclisi İçtüzüğü'nün söz konusu öteki hükümlerinin veya tümünün iptaline Anayasa Mahkemesince karar verilebileceği öngörülmektedir.

225. 7070 sayılı Kanun'un 2. maddesiyle 5271 sayılı Kanun'un 151. maddesinin (4) numaralı fıkrasına eklenen "...avukat hakkındaki soruşturma veya..." ile "...soruşturma veya..." ibarelerinin iptalleri nedeniyle uygulanma imkânı kalmayan 151. maddenin (3) numaralı fıkrasında yer alan "...soruşturma ya da..." ibaresinin de 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrası gereğince iptali gerekir.

226. 7070 sayılı Kanun'un 73. maddesiyle 3713 Kanun'a eklenen geçici 16. maddenin ikinci cümlesinin iptali nedeniyle uygulanma imkânı kalmayan üçüncü cümlesinin de 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrası gereğince iptali gerekir.

V. İPTAL KARARININ YÜRÜRLÜĞE GİRECEĞİ GÜN SORUNU

227. Anayasa'nın 153. maddesinin üçüncü fıkrasında "Kanun, Cumhurbaşkanlığı kararnamesi veya Türkiye Büyük Millet Meclisi İçtüzüğü ya da bunların hükümleri, iptal kararlarının Resmi Gazetede yayımlandığı tarihte yürürlükten kalkar. Gereken hallerde Anayasa Mahkemesi iptal hükmünün yürürlüğe gireceği tarihi ayrıca kararlaştırabilir. Bu tarih, kararın Resmi Gazetede yayımlandığı günden başlayarak bir yılı geçemez" denilmekte, 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrasında da bu kural tekrarlanarak Anayasa Mahkemesinin gerekli gördüğü hâllerde, Resmî Gazete'de yayımlandığı günden başlayarak iptal kararının yürürlüğe gireceği tarihi bir yılı geçmemek üzere ayrıca kararlaştırabileceği belirtilmektedir.

228. 7070 sayılı Kanun'un 62. maddesiyle 663 sayılı KHK'ya eklenen 45/A maddesinin (2) numaralı fıkrasının ikinci cümlesinin iptal edilmesi nedeniyle doğacak hukuksal boşluk kamu yararını ihlal edici nitelikte görüldüğünden Anayasa'nın 153. maddesinin üçüncü fıkrasıyla 6216 sayılı Kanun'un

66. maddesinin (3) numaralı fıkrası gereğince bu cümleye ilişkin iptal hükmünün kararın Resmî Gazete’de yayımlanmasından başlayarak dokuz ay sonra yürürlüğe girmesi uygun görülmüştür.

VI. YÜRÜRLÜĞÜN DURDURULMASI TALEBİ

229. Dava dilekçesinde özetle, dava konusu kuralların uygulanması hâlinde telafisi güç veya imkânsız zararların doğabileceği belirtilerek yürürlüklerinin durdurulmasına karar verilmesi talep edilmiştir.

1/2/2018 tarihli ve 7070 sayılı Kanun’un;

A. 1. 2. maddesiyle 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu’nun 151. maddesinin (4) numaralı fıkrasına eklenen “...avukat hakkındaki soruşturma veya...” ile “...soruşturma veya...” ibarelerine,

2. 6. maddesiyle 13/12/2004 tarihli ve 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun’un 59. maddesine eklenen (10) numaralı fıkranın, 5275 sayılı Kanun’un 59. maddesinin (5) numaralı fıkrasının “...görüşmeler teknik cihazla sesli veya görüntülü olarak kaydedilebilir, hükümlü ile avukatın yaptığı görüşmeleri izlemek amacıyla görevli görüşmede hazır bulundurulabilir, hükümlünün avukatına veya avukatın hükümlüye verdiği belge veya belge örnekleri, dosyalar ve aralarındaki konuşmalara ilişkin tuttıkları kayıtlara elkonulabilir...” bölümü yönünden incelenen “...ile beşinci fıkradaki suçlardan hükümlü olup, başka bir suçtan dolayı şüpheli veya sanık sıfatıyla avukatıyla görüşen hükümlüler...” bölümüne,

3. 33. maddesiyle 18/5/1929 tarihli ve 1453 sayılı Zabitan ve Askeri Memurların Maaşatı Hakkında Kanun’a eklenen geçici 1. maddenin ikinci fıkrasına,

4. 60. maddesiyle 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu’nun 48. maddesinin birinci fıkrasının (A) bendine eklenen (8) numaralı alt bende,

5. 73. maddesiyle 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu’na eklenen geçici 16. maddenin ikinci cümlesine,

yönelik yürürlüğün durdurulması taleplerinin, koşulları oluşmadığından REDDİNE,

B. 62. maddesiyle 11/10/2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname’ye (2/7/2018 tarihli ve 703 sayılı Kanun Hükmünde Kararname ile “Sağlık Alanında Bazı Düzenlemeler Hakkında Kanun Hükmünde Kararname” şeklinde değiştirilmiştir) eklenen 45/A maddesinin (2) numaralı fıkrasının ikinci

cümlesine yönelik iptal hükmünün yürürlüğe girmesinin ertelenmesi nedeniyle bu cümleye ilişkin yürürlüğün durdurulması talebinin REDDİNE,

- C. 1. 1. maddesiyle 5271 sayılı Kanun'un 149. maddesinin (2) numaralı fıkrasına eklenen cümleye,
2. 3. maddesiyle 5271 sayılı Kanun'un 154. maddesine eklenen (2) numaralı fıkrada yer alan "...örgüt faaliyeti çerçevesinde işlenen uyuşturucu ve uyarıcı madde imâl ve ticareti suçları..." ibaresine,
3. 4. maddesiyle 5271 sayılı Kanun'un 178. maddesinin (1) numaralı fıkrasına eklenen cümleye,
4. 5. maddesiyle 5271 sayılı Kanun'un 188. maddesinin (1) numaralı fıkrasına eklenen cümleye,
5. 6. maddesiyle 5275 sayılı Kanun'un 59. maddesine eklenen;
 - a. (5) numaralı fıkraya,
 - b. (10) numaralı fıkranın 5275 sayılı Kanun'un 59. maddesinin (5) numaralı fıkrası yönünden incelenen "Bu madde hükümleri 9 uncu maddenin üçüncü fıkrasına göre yüksek güvenlikli ceza infaz kurumlarında bulunan hükümlüler ... hakkında da uygulanır." bölümüne,
 - c. (10) numaralı fıkranın, 5275 sayılı Kanun'un 59. maddesinin (5) numaralı fıkrasının "...görüşmeler teknik cihazla sesli veya görüntülü olarak kaydedilebilir, hükümlü ile avukatın yaptığı görüşmeleri izlemek amacıyla görevli görüşmede hazır bulundurulabilir, hükümlünün avukatına veya avukatın hükümlüye verdiği belge veya belge örnekleri, dosyalar ve aralarındaki konuşmalara ilişkin tuttukları kayıtlara elkonulabilir..." dışında kalan bölümü yönünden incelenen "...ile beşinci fıkradaki suçlardan hükümlü olup, başka bir suçtan dolayı şüpheli veya sanık sıfatıyla avukatıyla görüşen hükümlüler..." bölümüne,
 - ç. (11) numaralı fıkraya,
6. 48. maddesiyle 31/7/1970 tarihli ve 1325 sayılı Millî Savunma Bakanlığı Görev ve Teşkilâtı Hakkında Kanun'a (703 sayılı Kanun Hükmünde Kararname ile "Askeri Okullar, Askeri Öğrenciler, Askeri Fabrikalar ve Bazı Düzenlemeler Hakkında Kanun" şeklinde değiştirilmiştir) eklenen ek 10. maddenin "...Bakanlığın özelliği ve hizmetin gerekli kıldığı şart ve vasıflar göz önüne alınarak Bakanlığa intibak edemedikleri üstlerince teklif edilenlerden Bakanlıkta oluşturulacak komisyona yaptırılacak tahkikat sonucuna göre Millî Savunma Bakanınca uygun görülenler,..." bölümüne,
7. 61. maddesiyle 657 sayılı Kanun'un 125. maddesinin birinci fıkrasının (E) bendine eklenen (1) alt bendinde yer alan "...eylem birliği içerisinde olmak,..." ibaresine,
8. 62. maddesiyle 663 sayılı Kanun Hükmünde Kararname'ye eklenen 45/A maddesinin (2) numaralı fıkrasının birinci cümlesine,

yönelik iptal talepleri 24/7/2019 tarihli ve E.2018/73, K.2019/65 sayılı kararlarla reddedildiğinden, bu fıkralara, cümlelere, bölümlere ve ibarelere ilişkin yürürlüğün durdurulması taleplerinin REDDİNE, Ç. 1. 56. maddesiyle 10/3/2011 tarihli ve 6191 sayılı Sözleşmeli Erbaş ve Er Kanunu'na eklenen geçici 1. madde,

2. 62. maddesiyle 663 sayılı Kanun Hükmünde Kararname'ye eklenen 45/A maddesinin (3) numaralı fıkrası,

hakkında 24/7/2019 tarihli ve E.2018/73, K.2019/65 sayılı kararlarla karar verilmesine yer olmadığına karar verildiğinden, bu maddeye ve fıkraya ilişkin yürürlüğün durdurulması talepleri hakkında KARAR VERİLMESİNE YER OLMADIĞINA,

24/7/2019 tarihinde OYBİRLİĞİYLE karar verilmiştir.

VII. HÜKÜM

1/2/2018 tarihli ve 7070 sayılı Kanun'un;

A. 1. maddesiyle 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu'nun 149. maddesinin (2) numaralı fıkrasına eklenen cümlelerin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

B. 2. maddesiyle 5271 sayılı Kanun'un 151. maddesinin (4) numaralı fıkrasına eklenen "...avukat hakkındaki soruşturma veya..." ile "...soruşturma veya..." ibarelerinin Anayasa'ya aykırı olduklarına ve İPTALLERİNE, iptal edilen ibareler nedeniyle uygulanma imkânı kalmayan 5271 sayılı Kanun'un 151. maddesinin (3) numaralı fıkrasında yer alan "...soruşturma ya da..." ibaresinin de 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 43. maddesinin (4) numaralı fıkrası gereğince İPTALİNE OYBİRLİĞİYLE,

C. 3. maddesiyle 5271 sayılı Kanun'un 154. maddesine eklenen (2) numaralı fıkrada yer alan "...örgüt faaliyeti çerçevesinde işlenen uyuşturucu ve uyarıcı madde imâl ve ticareti suçları..." ibaresinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

Ç. 4. maddesiyle 5271 sayılı Kanun'un 178. maddesinin (1) numaralı fıkrasına eklenen cümlelerin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Celal Mümtaz AKINCI'nın karşıoyu ve OYÇOKLUĞUYLA,

D. 5. maddesiyle 5271 sayılı Kanun'un 188. maddesinin (1) numaralı fıkrasına eklenen cümlelerin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Zühtü ARSLAN, Engin YILDIRIM, Hasan

Tahsin GÖKCAN, Recep KÖMÜRÇÜ ile Celal Mümtaz AKINCI'nın karşıoyları ve OYÇOKLUĞUYLA,

E. 6. maddesiyle 13/12/2004 tarihli ve 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun'un 59. maddesine eklenen;

1. (5) numaralı fıkranın Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

2. (10) numaralı fıkranın "Bu madde hükümleri 9 uncu maddenin üçüncü fıkrasına göre yüksek güvenlikli ceza infaz kurumlarında bulunan hükümlüler ... hakkında da uygulanır." bölümünün 5275 sayılı Kanun'un 59. maddesinin (5) numaralı fıkrası yönünden Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

3. (10) numaralı fıkranın "...ile beşinci fıkradaki suçlardan hükümlü olup, başka bir suçtan dolayı şüpheli veya sanık sıfatıyla avukatıyla görüşen hükümlüler..." bölümünün;

a. 5275 sayılı Kanun'un 59. maddesinin (5) numaralı fıkrasının "...görüşmeler teknik cihazla sesli veya görüntülü olarak kaydedilebilir, hükümlü ile avukatın yaptığı görüşmeleri izlemek amacıyla görevli görüşmede hazır bulundurulabilir, hükümlünün avukatına veya avukatın hükümlüye verdiği belge veya belge örnekleri, dosyalar ve aralarındaki konuşmalara ilişkin tuttukları kayıtlara elkonulabilir..." bölümü yönünden Anayasa'ya aykırı olduğuna ve İPTALİNE OYBİRLİĞİYLE,

b. 5275 sayılı Kanun'un 59. maddesinin (5) numaralı fıkrasının "...görüşmeler teknik cihazla sesli veya görüntülü olarak kaydedilebilir, hükümlü ile avukatın yaptığı görüşmeleri izlemek amacıyla görevli görüşmede hazır bulundurulabilir, hükümlünün avukatına veya avukatın hükümlüye verdiği belge veya belge örnekleri, dosyalar ve aralarındaki konuşmalara ilişkin tuttukları kayıtlara elkonulabilir..." dışında kalan bölümü yönünden Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

4. (11) numaralı fıkranın Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

F. 33. maddesiyle 18/5/1929 tarihli ve 1453 sayılı Zabitan ve Askeri Memurların Maaşatı Hakkında Kanun'a eklenen geçici 1. maddenin ikinci fıkrasının Anayasa'ya aykırı olduğuna ve İPTALİNE OYBİRLİĞİYLE,

G. 48. maddesiyle 31/7/1970 tarihli ve 1325 sayılı Millî Savunma Bakanlığı Görev ve Teşkilâtı Hakkında Kanun'a (2/7/2018 tarihli ve 703 sayılı Kanun Hükmünde Kararname ile "Askeri Okullar, Askeri Öğrenciler, Askeri Fabrikalar ve Bazı Düzenlemeler Hakkında Kanun" şeklinde değiştirilmiştir) eklenen ek 10. maddenin "...Bakanlığın özelliği ve hizmetin gerekli kıldığı şart ve

vasıflar göz önüne alınarak Bakanlığa intibak edemedikleri üstlerince teklif edilenlerden Bakanlıkta oluşturulacak komisyona yaptırılacak tahkikat sonucuna göre Millî Savunma Bakanınca uygun görülenler,...” bölümünün Anayasa’ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

Ğ. 56. maddesiyle 10/3/2011 tarihli ve 6191 sayılı Sözleşmeli Erbaş ve Er Kanunu’na eklenen geçici 1. maddeye ilişkin iptal talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA OYBİRLİĞİYLE,

H. 60. maddesiyle 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu’nun 48. maddesinin birinci fıkrasının (A) bendine eklenen (8) numaralı alt bendin Anayasa’ya aykırı olduğuna ve İPTALİNE, M. Emin KUZ’un karşıoyu ve OYÇOKLUĞUYLA,

I. 61. maddesiyle 657 sayılı Kanun’un 125. maddesinin birinci fıkrasının (E) bendine eklenen (I) alt bendinde yer alan “...eylem birliği içerisinde olmak,...” ibaresinin Anayasa’ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

İ. 62. maddesiyle 11/10/2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname’ye (703 sayılı Kanun Hükmünde Kararname ile “Sağlık Alanında Bazı Düzenlemeler Hakkında Kanun Hükmünde Kararname” şeklinde değiştirilmiştir) eklenen 45/A maddesinin;

1. (2) numaralı fıkrasının;

a. Birinci cümlesinin Anayasa’ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

b. İkinci cümlesinin Anayasa’ya aykırı olduğuna ve İPTALİNE, iptal hükmünün, Anayasa’nın 153. maddesinin üçüncü fıkrası ile 6216 sayılı Kanun’un 66. maddesinin (3) numaralı fıkrası gereğince, KARARIN RESMÎ GAZETE’DE YAYIMLANMASINDAN BAŞLAYARAK DOKUZ AY SONRA YÜRÜRLÜĞE GİRMESİNE OYBİRLİĞİYLE,

2. (3) numaralı fıkrasına ilişkin iptal talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA OYBİRLİĞİYLE,

J. 73. maddesiyle 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu’na eklenen geçici 16. maddenin ikinci cümlesinin Anayasa’ya aykırı olduğuna ve İPTALİNE; iptal edilen cümle nedeniyle uygulanma imkânı kalmayan 3713 sayılı Kanun’un geçici 16. maddesinin üçüncü cümlesinin de 6216 sayılı Kanun’un 43. maddesinin (4) numaralı fıkrası gereğince İPTALİNE OYBİRLİĞİYLE,

24/7/2019 tarihinde karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili - Engin YILDIRIM

Başkanvekili - Hasan Tahsin GÖKCAN

Üye: Serdar ÖZGÜLDÜR; Recep KÖMÜRCÜ; Hicabi DURSUN; Celal Mümtaz AKINCI; Muammer TOPAL; M. Emin KUZ; Kadir ÖZKAYA; Rıdvan GÜLEÇ; Recai AKYEL; Yusuf Şevki HAKYEMEZ; Yıldız SEFERİNOĞLU

KARŞIOY GEREKÇESİ

1. 1/2/2018 tarihli ve 7070 sayılı Kanun'un 5. maddesiyle 5271 sayılı Ceza Muhakemesi Kanunu'nun 188. maddesinin (1) numaralı fıkrasına eklenen cümlelerin Anayasa'ya aykırı olduğu iddiası Mahkememiz çoğunluğu tarafından reddedilmiştir.

2. Dava konusu cümlelerin de yer aldığı fıkra şu şekildedir: "Madde 188 - (1) Duruşmada, hükme katılacak hâkimler ve Cumhuriyet savcısı ile zabıt kâtibinin ve Kanunun zorunlu müdafiliği kabul ettiği hâllerde müdafii hazır bulunması şarttır. Müdafii mazeretsiz olarak duruşmaya gelmemesi veya duruşmayı terk etmesi halinde duruşmaya devam edilebilir."

3. 5271 sayılı Kanun'un 151. maddesi zorunlu müdafii duruşmada hazır bulunmaması veya vakitsiz olarak duruşmadan çekilmesi durumunda başka bir müdafii görevlendirileceğini, oturuma ara verileceğini veya oturumun erteleneceğini öngörmektedir. Görüldüğü üzere kuralla müdafii duruşmada hazır bulunması zorunluluğuna istisna getirilmekte, mazeretsiz duruşmaya gelmeme veya duruşmayı terk etme durumlarında duruşmaya devam edilebileceği öngörülmektedir.

4. Esasen çoğunluk ile görüş ayrılığımız, öncelikle kuralın anlam ve kapsamı konusunda ortaya çıkmaktadır. Çoğunluğa göre Kanun'un müdafii duruşmada hazır bulunması gerektiğine dair diğer hükümleriyle birlikte değerlendirildiğinde, "dava konusu kuralın yargılamanın sonucuna etkili esaslı işlemlerin yapıldığı ve bu nedenle müdafii yardımının etkili olduğu duruşmaların müdafii yokluğunda yapılabilmesine imkân tanıdığı şeklinde anlaşılması mümkün değildir" (§ 73).

5. Kural çoğunluğun savunduğu görüşün aksine müdafii yokluğunda yargılamanın sonucuna etkili esaslı işlemlerin yapılmasını engelleyecek herhangi bir ifadeye yer vermemektedir. Daha önce ifade edildiği gibi kural zorunlu müdafii bulunmadığı durumda duruşmaya devam edilemeyeceği yönündeki hükümlere istisna getirmektedir. Bu istisnayı getirirken de devam edebileceği söylenen duruşmaları "yargılamanın sonucuna etkili işlemlerin yapıldığı/yapılmadığı duruşmalar" olarak herhangi bir ayrıma tabi tutmamaktadır. Kanun koyucu, çoğunluğun iddia ettiği gibi, sonuca etkili

işlemlerin yapıldığı duruşmaların hiçbir durumda zorunlu müdafii yokluğunda yapılamayacağını murat etseydi bunu açıkça ifade ederdi. Kuralın, bu yöndeki diğer hükümlerde herhangi bir değişiklik yapmadığından hareketle, sadece bir anlamda “önemsiz” ya da “etkisiz” işlemlerin yapıldığı duruşmaların müdafii yokluğunda yapılmasına izin verdiğini söylemek zordur.

6. Müdafii yardımından yararlanma hakkı savunma hakkının, dolayısıyla adil yargılanma hakkının olmazsa olmaz unsuru olarak kabul edilmektedir. Bu hak, aynı zamanda yargılamanın silahların eşitliği ilkesine uygun şekilde gerçekleştirilmesinin de ön şartını teşkil etmektedir. Mahkememizin kararlarında vurgulandığı üzere, “Sanığın müdafii yardımından yararlanması ile aynı zamanda kamu görevlilerinin haksız uygulamalarının önlenmesi, adli hataların oluşmaması, sorgulama veya iddia makamı ile sanık arasında silahların eşitliğinin sağlanması ilkesi başta olmak üzere” adil yargılamanın amaçları sağlanacaktır (Aligül Alkaya ve Diğerleri, B. No: 2013/1138, 27/10/2015, § 134).

7. Dava konusu kuralın müdafii yardımından yararlanma hakkı bakımından yol açabileceği sakıncaları anlayabilmek için zorunlu müdafiliğin hangi durumlarda söz konusu olduğuna bakmak gerekir. Nitekim kural, aynı fıkranın birinci cümlesinde yer alan “Kanunun zorunlu müdafiliği kabul ettiği hâllerde müdafii hazır bulunması şarttır” hükmüne istisna getirmektedir. 5271 sayılı Kanun’un 150. maddesinin ikinci ve üçüncü fıkralarında sanık veya şüphelinin çocuk, kendisini savunamayacak derecede malul veya sağır ve dilsiz olması durumunda ve alt sınırı beş yıldan fazla hapis cezasını gerektiren suçlardan dolayı yapılan soruşturma ve kovuşturmalarda talep aranmaksızın müdafii tayin edileceği düzenlenmektedir.

8. Zorunlu müdafii tayin edildiği her iki durumda da sanığın duruşmalarda müdafii hakkından yararlanma hakkının ne derece hayati olduğu her türlü izahtan varestedir. Kurum olarak zorunlu müdafilik, yaş, engelli olup olmama ve isnat olunan suçun ağırlığı gibi nedenlerle şüpheli veya sanığın kendisini daha iyi savunabilmesi, maddi gerçeğin ortaya çıkarılabilmesi ve adaletin tecellisi için savunma makamının güçlendirilmesini amaçlamaktadır. Müdafii aynı zamanda yargılamanın usulüne uygun şekilde gerçekleşmesine vazgeçilmez katkı sağlayan bir yargılama sujesidir. Tam da bu nedenle Ceza Muhakemesi Kanunu’nun 151. maddesinin (1) numaralı fıkrasında, yukarıda belirtildiği gibi, müdafii duruşmada bulunmaması ya da çekilmesi durumlarında, yeni bir müdafii görevlendirilmeden oturuma devam edilmemesi öngörülmüştür. Kısacası yargılamanın usul ve esas bakımından sağlıklı bir şekilde yapılabilmesi için hayati öneme sahip olan zorunlu müdafilik kurumunu işlevsiz hale getirebilecek kanuni düzenlemelerden kaçınılması gerekmektedir.

9. Hiç kuşkusuz müdafî yardımından yararlanma hakkı mutlak değildir, bazı istisnai durumlarda sınırlandırılabilir. Ancak bu sınırlandırmanın Anayasa'nın 13. maddesi gereğince ölçülü olması zorunludur.

10. Müdafîin yokluğunda duruşmaya devam edilebilmesine yönelik dava konusu kuralın, yargılamanın gereksiz yere uzamasını ve sürüncemede bırakılmasını engellemeye matuf olduğu söylenebilir. Anayasa'nın 141. maddesinde yer alan "Davaların... mümkün olan süratle sonuçlandırılması, yargının görevidir" hükmü de kanun koyucunun bu tür önlemler almasını gerektirebilir. Ancak bu gereklilik, hukuk devletinde hayati önemi haiz olan kişilerin savunma hakkını ölçsüz şekilde sınırlandırmanın gerekçesi olamaz. Anayasa Mahkemesinin önceki kararlarında belirtildiği üzere, yargılamanın makul sürede sonuçlandırılmasına yönelik kanuni tercihlerin "kişilerin savunma hakkını, bu çerçevede müdafî yardımından yararlanma hakkını kullanılamaz hâle getirmemesi gerekir" (AYM, E. 2017/49, K. 2017/113, § 14).

11. Benzer şekilde Avrupa İnsan Hakları Mahkemesi de müdafî yardımından yararlanma hakkına yönelik sınırlamaların ihlale yol açmaması için (a) "zorlayıcı sebeplere" dayanması ve (b) bir bütün olarak yargılamanın hakkaniyetine hâle getirmemesi gerektiğine vurgu yapmaktadır (İbrahim ve Diğerleri/Birleşik Krallık [BD], B.No: 50541/08, 50571/08 50573/08, 40351/09, 13/09/2016, §§ 258-262). Bu çerçevede yargılamanın daha kısa sürede sonuçlandırılması, müdafî yardımından yararlanma hakkını sınırlamanın meşru sebebi olarak görülebilirse de ölçülülük açısından "zorlayıcı sebep" olarak görülmesi zordur.

12. Diğer taraftan yargılamanın makul sürede sonuçlandırılması amacıyla müdafî yardımından yararlanma hakkını sınırlayan dava konusu kural bir bütün olarak yargılamayı adil olmaktan çıkarma riskini taşımaktadır. Zira kural, kendisine zorunlu müdafî tayin edilen sanığın hiçbir kusuru olmadığı halde müdafîin mazeretsiz olarak duruşmaya gelmemesi veya duruşmayı terk etmesi durumunda kendisini savunma imkânını ölçsüz bir şekilde sınırlandırmaktadır.

13. Kuralın istisna getirdiği fıkranın ilk cümlesi uyarınca sanığın duruşmaya katılımının zorunlu olmadığı da dikkate alındığında, sanığın ve müdafîin bulunmadığı bir duruşmada yargılamaya devam edilmesi mümkündür. Bu şekilde tek taraflı bir yargılamanın hakkaniyete uygun bir yargılamayı imkânsız hale getireceği açıktır. Kural müdafîin yokluğunda devam edilmesine karar verilen duruşmalarda yargılamanın sonucuna etkili olacak herhangi bir işlemin yapılmasını engelleyecek güvencelere de yer vermemektedir. Bu nedenle yargılamayı bir bütün olarak adil olmaktan çıkarabilecek bu düzenlemenin kişilerin savunma hakkına, dolayısıyla adil yargılanma hakkına ölçsüz bir sınırlama getirdiği anlaşılmaktadır.

14. Açıklanan gerekçelerle kuralın Anayasa'nın 13. ve 36. maddelerine aykırı olduğunu düşündüğümden çoğunluğun red yönündeki görüşüne katılmıyorum.

Başkan - Zühtü ARSLAN

KARŞIOY GEREKÇESİ

1. 7070 sayılı Kanunun 5. maddesi ile 5271 sayılı Kanunun 188. maddesinin birinci fıkrasına "Müdafiinin mazeretsiz olarak duruşmaya gelmemesi veya duruşmayı terk etmesi halinde duruşmaya devam edilebilir" şeklinde bir cümle eklenmiştir.

2. 5271 sayılı Kanunun 188. maddesinin ilk fıkrasında hükme katılacak hâkimler ve Cumhuriyet savcısı ile zabıt kâtibinin ve Kanunun zorunluğu müdafiliği kabul ettiği hallerde müdafinin hazır bulunması gerektiği belirtilmiştir. İptali istenen kuralla da zorunlu müdafi olmadan da duruşmaya devam edilmesinin önü açılmıştır.

3. Ceza muhakemesi düzenimizde kanun koyucu belli durumlarda ceza yargılamasına ilişkin işlemlerde müdafinin hazır bulunmasını zorunlu tutmuştur. Müdafiin duruşmalara katılması ve yargılamaya müdahil olması, sanığın savunma hakkından yararlanarak adil bir şekilde yargılanmasına katkıda bulunmaktadır.

4. Yargıtay Ceza Genel Kurulu, baro tarafından görevlendirilen müdafiin yokluğunda mahkûmiyet kararı verilmesini sanığın savunma hakkını kısıtladığı gerekçesiyle mutlak bozma nedeni olarak değerlendirmiştir (YCGK, 11/10/20011, E. 2011/10-82, K. 2011/204).

5. Anayasa Mahkemesi de çeşitli kararlarında müdafi yardımından yararlanma hakkının savunma ve çelişmeli yargılanma hakkı ile silahların eşitliği ilkesinin etkin bir şekilde kullanılmasının bir gereği olduğunu vurgulamıştır (E. 2017/32, K. 2018/81, 11/7/2018; Bayram Siviş B.No: 2014/5844, 5/11/2014 § 30; Kazım Albayrak, B. No: 2014/3836, 17/9/2014, § 29). Çelişmeli yargılama taraflara iddia ve karşı iddiaları sunma hususunda imkân sağlarken, silahların eşitliği, davanın taraflarının usul açısından eşit durumda olmalarına ve aralarında hakkaniyete uygun bir dengenin oluşmasına katkı yapmaktadır.

6. Zorunlu müdafilik, şüpheli veya sanığın yaşı ruhsal durumu veya isnat olunan suçun ağırlığı gibi nedenlerle savunma makamının özel olarak korunması ve desteklenmesi gereken hallerde etkili bir savunmanın gerçekleştirilebilmesi ve maddi gerçeğin tespit edilmesi amacıyla oluşturulmuş bir kurumdur.

7. Hakkında bir suç isnadı olan herkesin gerektiği hallerde zorunlu olarak atanan bir müdafî tarafından savunulması adil yargılamanın en önemli unsurlarından birini oluşturmaktadır. İptali istenen kuralla zorunlu müdafîin mazeretsiz olarak duruşmada bulunmaması durumunda duruşmaya devam edilmesine imkân tanınması bu durumdan dolayı hiçbir kusuru olmayan sanığın müdafî yardımından yararlanma hakkını zedelemektedir. Böyle bir durumda sanık herhangi bir şekilde kendisinden kaynaklanmayan bir nedenden dolayı savunma hakkını gerektiği gibi kullanamayacaktır. Dava konusu kural, bir anlamda zorunlu müdafîliği etkisiz ve işlevsiz hale getirmektedir.

8. Zorunlu müdafîin bulunduğu duruşmada sanığın hazır olması gerekmemektedir. Dava konusu kural, müdafîinin duruşmaya katılacağına güvenerek duruşmada hazır bulunmayan sanığın yokluğunda, müdafîinin de mazeretsiz olarak duruşmaya katılmaması durumunda duruşmaya devam edilmesine imkân tanıdığından çelişmeli yargılama ve silahların eşitliği ilkesine aykırı düşmektedir. Savunma makamı temsil edilmeden yapılan bir duruşmanın adil yargılanma olarak nitelendirilmesi de mümkün gözükmemektedir.

9. Sonuç olarak, dava konusu kuralın adil yargılanma hakkına ölçsüz bir müdahalede bulunarak Anayasanın 13. ve 36. maddelerine aykırı olduğu düşüncesiyle çoğunluk kararına katılmadım.

Başkanvekili - Engin YILDIRIM

KARŞIOY GEREKÇESİ

1. Ceza muhakemesinde müdafîlik kurumu, savunma makamının yardımcısıdır. Müdafî, bir hukukçu olan iddia makamı ve hakimin karşısında bilgisiyle savunma lehine dengeyi sağlama işlevi görmektedir. Bu yönüyle müdafînin varlığı ceza yargılamasında silahların eşitliği ve çelişmeli yargılama ilkeleriyle doğrudan bağlantılıdır. Çünkü hukukçu olan iddia makamı ve hüküm merci karşısında ancak yeterli hukuk bilgisi olan bir kimse savunmanın menfaatlerini koruyabilir.

2. Diğer taraftan ceza soruşturma ve kovuşturmasında suç ithamı altındaki kişinin hukuki yardım alma hakkı adil yargılanma hakkı kapsamındadır. AİHS'nin adil yargılanma hakkına ilişkin 6/3-c maddesinde, suçla itham edilen herkesin bizzat savunma veya seçeceği bir müdafîinin yardımından yararlanma ve eğer maddi olanaktan yoksun ve adaletin yerine gelmesi için gerekli ise re'sen atanacak bir avukatın yardımından ücretsiz yararlanma hakkı bulunduğu belirtilmektedir.

3. Avukatın hukuki yardımından yararlanma hakkı soruşturma ve kovuşturmanın bir aşamasına mahsus olmayıp, sürecin tümünü kapsayan bir haktır. AİHM sanığın bulunmadığı bir duruşmada

avukatıyla temsil edilmesinin kabul edilmemesini adil yargılanma hakkının ihlal edeceğine karar vermektedir (AİHM Poitrimol/Fransa, No: 14032/88, 23.11.1993, par. 38). Anayasa Mahkemesi de çeşitli kararlarında müdafî yardımından yararlandırılmama veya müdafî bulunmadan alınan savunma beyanının hükme esas alınması gibi hallerde adil yargılanma hakkının ihlal edildiğine karar vermiştir (bkz. Gürhan Nerse, 30.12.2014, B. No. 2013/5957; Abdulselam Tatal ve Diğ. 8.4.2015, B. No: 2013/2319; Yusuf Karakuş ve Diğ. 8.12.2016, B. No: 2014/12002).

4. Nitekim CMK'da bu hak kapsamında çocuklar ve kendisini savunamayacak derecede malul veya sağır-dilsiz kimselere zorunlu olarak müdafî görevlendirilmesi özel olarak düzenlenmiştir. Yine alt sınırı beş yıldan fazla hapis cezasını gerektiren suçlardan dolayı yapılan soruşturma ve kovuşturmada da zorunlu müdafî görevlendirilmesi gerekmektedir (CMK m. 150/2). Kanunun duruşmada bulunması zorunlu olanlara ilişkin 188. maddesinin birinci fıkrasının ilk cümlesinde zorunlu müdafî de sayılmaktadır. Ne var ki iptali istenen kural buna istisna getirmektedir.

5. İptal istemine konu olan 5271 sayılı Kanunun 188 maddesinin ilk fıkrasının ikinci cümlesinde ise zorunlu müdafîin mazeretsiz olarak duruşmaya gelmemesi veya duruşmayı terk etmesi durumunda duruşmaya devam edilebileceği belirtilmektedir. Bu şekliyle kural, sanığın da bulunmaması durumunda her türlü usul işlemlerinin yapılmasına imkan sağlamaktadır. Mahkememiz kararında CMK'nun 150 ve 151. maddeleri karşısında esaslı işlemlerin müdafî yokluğunda yapılmasına imkan tanındığının söylenemeyeceği ifade edilmiştir. Ne yazık ki bu değerlendirme, atıf yapılan maddelerle uyumlu değildir. Kanunun 150. maddesi müdafî görevlendirilmesi koşulları ve usulünü düzenlemektedir, yokluğunda yapılacak duruşmayla ilgisi bulunmamaktadır. Kanunun 151/1. maddesinde müdafîin görevden çekilmesi, yani görevi kabul etmemesi ya da devamından çekinmesi hali ile görevini yerine getirmekten kaçınması halinde başka müdafî görevlendirilmesi için gerekli işlemlerin yapılacağı düzenlemektedir. Buna karşın 188. maddedeki düzenlemede bir duruşmaya gelmeyen veya duruşmayı terk eden müdafî bulunmadan da duruşmanın sürdürülebileceği belirtilmektedir. Dolayısıyla kural başka bir müdafî görevlendirilmesi gereğini aramaksızın duruşmaya devam konusunda hakime takdir yetkisi vermektedir. Bu nedenle kuralın hukuki yardım alma ve savunma hakkını kısıtlayacağı ve dolayısıyla adil yargılanma hakkına aykırı düşeceği anlaşılmaktadır.

6. Diğer taraftan, müdafî bulunmadan duruşmaya devam edilmesi için sanığın hazır bulunması koşulu da aranmamaktadır. Bilindiği üzere adil yargılanma hakkının alt unsurlarından biri de duruşmada bulunma hakkıdır. Sanık müdafî ile temsil edildiğini bilerek hareket ettiği durumda kendisi ayrıca duruşmada bulunmaya ihtiyaç duymayabilir. Fakat zorunlu müdafîin geçici olarak

katılmaması nedeniyle usul işlemlerinin yürütüldüğü duruşmalarda tedbir alma imkanı olmayan sanığın bulunamaması, duruşma hakkını da ihlal eder niteliktedir.

Açıklanan nedenlerle, kuralın Anayasanın 36. maddesinde düzenlenen adil yargılanma hakkına aykırı bulunduğu görüşündeyiz.

Başkanvekili - Hasan Tahsin GÖKCAN

Üye - Recep KÖMÜRCÜ

KARŞI OY GEREKÇESİ

1/2/2018 tarihli ve 707 sayılı Kanun'un 4. maddesiyle 5271 sayılı CMK'nun 178. maddesinin (1) numaralı fıkrasına eklenen "Ancak, davayı uzatmak amacıyla yapılan talepler reddedilir." cümlesinin Anayasa'ya aykırı olduğu iddiası Mahkememiz çoğunluğunca reddedilmiştir.

1. Kişilere yargı mercileri önünde dava ve savunma hakkı tanınması silahların eşitliği ve çelişmeli yargılama ilkeleri ışığında hakkaniyete uygun yargılamanın da temelini oluşturmaktadır. Silahların eşitliği ilkesi, davanın taraflarının yargılama sırasında usul hükümleri yönünden eşit konumda bulunmasını ve taraflardan birine dezavantaj, diğerine avantaj sağlayacak kurallara yer verilmemesini öngörmekte; diğer bir deyişle davanın tarafları arasında hakkaniyete uygun bir dengeğin varlığını gerekli kılmaktadır. Çelişmeli yargılama ilkesi ise taraflara, dosyaya giren görüşler ile diğer tarafça sunulan deliller hakkında bilgi sahibi olma ve karşı iddialarını sunma hususunda uygun imkânların sağlanması anlamına gelmektedir.

2. Savunma tanıklarının da iddia makamının tanıklarıyla aynı koşullar altında davet edilmelerinin ve dinlenmelerinin sağlanmasını isteme hakkı, silahların eşitliği ilkesinin bir gereğidir. Ancak bu hak, sanığın lehine olan bütün tanıkların çağrılmasını ve dinlenmesini gerektirmez. Önemli olan sanığın aynı koşullar altında ve silahların eşitliği ilkesine uygun olarak tanık dinletme talebinde bulunabilmesinin sağlanmasıdır. Bu bağlamda kural uyarınca sanık veya katılanın tanık ve uzman kişilerin dinletilmesine yönelik taleplerinin reddine imkân tanınması adil yargılanma hakkına müdahale niteliği taşımaktadır.

3. Ceza muhakemesinin amacı maddi gerçeği araştırmaktır. Gerçeğe ulaşma, kolektif yargılama yöntemi ile sağlanabilecektir. Ceza muhakemesinin amacını gerçekleştirmek için sanığın lehine ve aleyhine delillerin toplanması kural olarak soruşturma evresinde gerçekleştirilmektedir. 5271 sayılı Kanun'un 160. maddesinin (2) numaralı fıkrasında, Cumhuriyet savcısının maddi gerçeğin

araştırılması ve adil bir yargılamanın yapılabilmesi için emrindeki adli kolluk görevlileri marifetiyle şüphelinin lehine ve aleyhine olan delilleri toplayarak muhafaza altına almakla ve şüphelinin haklarını korumakla yükümlü olduğu hüküm altına alınmıştır.

4. Tanık ve uzman kişilerin görüşlerine başvurulması da maddi gerçeğin ortaya çıkarılmasını sağlayan araçlar arasındadır. Yargılama esnasında tarafların uyuşmazlık konusu olaya ilişkin bilgisi olanların tanıklığına veya uzman görüşüne başvurulmasını isteme hakları bulunmaktadır. Kovuşturma evresinde kural olarak iddianamede gösterilen tanık ve uzman kişiler duruşmaya davet edilmekle birlikte sanık veya katılan da dava konusu olayla ilgili olarak dinlenilmesini istediği tanık veya uzman kişilerin duruşmaya çağrılmasını talep edebilir.

5. Dava konusu kuralda ise sanık veya katılanın bu yöndeki taleplerinin davayı uzatmak amacıyla yapıldığının anlaşılması durumunda reddedileceği hüküm altına alınmıştır. Kurala göre mahkeme başkanı veya hâkim, tanık ve uzman kişi dinlenilmesine ilişkin taleplerin davayı uzatmak amacıyla yapıldığı kanaatine varırsa bu talepleri reddedecektir.

6. Tanık ve uzman kişilerin dinlenmesi yönündeki taleplerin reddedilmesinin, ancak davayı uzatmak amacıyla yapıldığı kanaatine varılması durumunda söz konusu olabileceği, bu konuda yargı mercilerine sınırsız bir yetki tanınmadığı ifade edilmekte ise de uygulamada bu yetkinin yerinde, isabetli olarak ve nasıl kullanılacağına dair bir belirginlik olmadığı gibi yanlış ve hatalı kullanımını engelleyecek bir mekanizma da bulunmamaktadır. Hakimlerimiz tanık ve uzman dinletme talebinin davayı uzatmak amacıyla yapıp yapılmadığını nasıl anlayacaklardır?

7. Ceza yargılamasının amacı olan gerçeğe ulaşabilmek için tüm taraf delillerinin dosyaya girmesi gerekir. Katılanın ve sanığın dinlenilmesini istediği tanık ve uzman dinletme talebini “davayı uzatmak amacıyla” yapıldığı zehabı ve gerekçesiyle reddedilmesi halinde maddi gerçeği bulma, maddi gerçeğe ulaşma amacı tehlikeye girebilecektir. Kuralla, iddia makamına istediği delillerin toplanıp, dinlenmesini istediği tanıkların “davayı uzatma” endişesi taşınmadan dinlenilmesi avantajı sağlanırken, katılana veya sanığa “davayı uzatma amacı taşıyor” denilerek aynı hakkı vermemek silahların eşitsizliği anlamında kendilerini iddia makamı karşısında dezavantajlı bir duruma düşürecektir.

8. Kuralın bu haliyle uygulanması esnasında davanın uzamasının önüne geçilmek istenirken sanığın veya katılanın, tanık ve uzman kişi dinlenilme talebinin reddi nedeniyle çok önemli hak kayıplarına uğraması söz konusu olabilecektir. Bu mahzurun istinaf aşamasında giderilebileceği düşünülmekte ise de bu durum da şüphelidir. İstinaf Mahkemelerinin elinde bu takdirin yerinde kullanılıp kullanılmadığını ölçecek bir mihenk taşı olmadığına göre kuralın bu haliyle uygulanmasının önemli

hak kayıplarına neden olabileceği tehlikesi dışında tanık, uzman kişi dinleme konusundaki taktir hakkının hatalı olduğunun İstinaf aşamasında anlaşılması halinde tanık veya uzman kişinin İstinaf Mahkemesince dinlenilmesi suretiyle eksikliğin tamamlanmak istenmesi davayı uzatacak, ayrıca tanık ve uzmanın İstinafla farklı mahallerde olması durumunda ise bunların dinlenebilmesi daha fazla masraf ve daha fazla zaman harcanmasına neden olabilecektir.

9. Sunulmaya çalışılan nedenlerle tanık ve uzman kişilerin dinletilmesine getirilen sınırlama ile ulaşılmak istenen amaç arasında makul bir dengenin sağlanamayacağı endişesi taşıdığımdan çoğunluğumuzun aksi yöndeki düşüncesine katılamadım.

10. 7070 sayılı Kanun'un 5. maddesiyle Ceza Muhakemesi Kanunu'nun 188. maddesinin (1) numaralı fıkrasına eklenen "Müdafiin mazeretsiz olarak duruşmaya gelmemesi veya duruşmayı terk etmesi halinde duruşmaya devam edilebilir." Cümlesinin, Anayasa aykırı olduğunu düşünüyor ve bu konuda Anayasa Mahkemesi Başkanı Sayın Zühtü ARSLAN tarafından kaleme alınan karşı oyda ifade olunan gerekçelere aynen katılıyorum.

11. Sonuç olarak Mahkememizin Anayasaya aykırılık ve bireysel başvuru kapsamında verdiği kararlar ve içtihatları göz önüne alındığında, iptal istemine konu her iki kuralın da, Anayasa'nın 13. maddesinde öngörülen "ölçülülük" ve 36. maddesinde ifade olunan "Adil yargılanma hakkı" ilkelerine aykırı ve iptali gerektiği düşüncesinde olduğumdan farklı yöndeki çoğunluk görüşüne katılamadım.

Üye - Celal Mümtaz AKINCI

KARŞIOY GEREKÇESİ

7070 sayılı Kanununun 60. maddesiyle 657 sayılı Kanununun 48. maddesinin birinci fıkrasının (A) bendine eklenen (8) numaralı alt bendin Anayasaya aykırı olduğuna ve iptaline karar verilmiştir.

İptal kararının gerekçesinde; güvenlik soruşturması ve arşiv araştırması kapsamında kamu mercileri tarafından bireyin iş ve sosyal yaşamıyla ilgili bilgilerinin alınması, kaydedilmesi, saklanması ve kullanılmasının özel hayata saygı hakkına sınırlama niteliğinde olduğu, güvenlik soruşturması ve arşiv araştırması yapılmasını öngören bir düzenleme getirilmesi kanun koyucunun takdir yetkisinde olmakla birlikte, bu konudaki kuralların kamu makamlarına hangi şartlarda ve sınırlar içinde tedbirler uygulama ve özel hayatın gizliliğine yönelik müdahalelerde bulunma yetkisi verildiğini yeterince açık olarak göstermesi ve kötüye kullanmalara karşı yeterli güvenceleri sağlaması gerektiği, dava konusu kuralda ise güvenlik soruşturmasına ve arşiv araştırmasına konu edilecek bilgi ve

belgelerin neler olduğuna, bu bilgilerin ne şekilde kullanılacağına ve hangi mercilerin soruşturma ve araştırmayı yapacağına ilişkin herhangi bir düzenleme yapılmadığı, güvenlik soruşturması ve arşiv araştırması yapılmasına ve kişisel veri niteliğindeki bilgilerin alınmasına, kullanılmasına, işlenmesine yönelik güvenceler ile temel ilkeler kanunla belirlenmeksizin bunların alınmasına ve kullanılmasına izin verildiği, bu nedenle kuralın Anayasanın 13., 20. ve 128. maddeleriyle bağdaşmadığı belirtilmiştir.

Anayasanın 20. maddesinin son fıkrasında, herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği ve bu verilerin korunmasına ilişkin usul ve esasların kanunla düzenleneceği; 128. maddesinin ikinci fıkrasında ise, memurların ve diğer kamu görevlilerinin nitelikleri ve atanmalarının da kanunla düzenleneceği hükme bağlanmaktadır.

Kararda da belirtildiği üzere, kanunla düzenleme ilkesi, düzenlenen alanda temel ilkelerin kanunla konulmasını, kuralın açık, anlaşılır ve sınırlarının belirli olmasını ve kişilerin temel haklarını kullanabilmelerine elverişli olmasını gerektirmektedir.

Buna karşılık, söz konusu düzenlemelerin tamamının aynı kanunda yapılması gerekmemekte; yukarıda belirtilen şartları taşıyan düzenlemelerin incelenen kanunun dışındaki kanunlarla yapılmış olması da kanunîlik ilkesi açısından yeterli bulunmaktadır (4/7/2013 tarihli ve E.2012/100, K.2013/84 sayılı; 3/7/2014 tarihli ve E.2013/96, K.2014/118 sayılı; 13/11/2015 tarihli ve E.2013/95, K.2014/176 sayılı kararlarımız).

Bilindiği gibi, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek amacıyla 6698 sayılı Kişisel Verilerin Korunması Kanunu kabul edilerek konuya ilişkin güvenceler yaklaşık otuz maddede ayrıntılı olarak düzenlenmiştir.

Bu çerçevede, 6698 sayılı Kanunun 3. maddesiyle kişisel veriler tanımlanmış; 4. maddesinde kişisel verilerin işlenmesine ve korunmasına ilişkin genel ilkeler, 5. maddesinde işlenme şartları sayılmış; 12. maddesinde de veri güvenliği konusundaki yükümlülükler belirlenerek kişisel verilerin hukuka aykırı olarak işlenmesini, bunlara hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla alınacak tedbirler düzenlenmiştir. Kanunun diğer maddelerinde de kişisel verilerin işlenmesine, korunmasına ve kamu makamlarının keyfî müdahalelerine karşı güvenceye kavuşturulmasına ilişkin düzenlemelere yer verilmiştir.

Bu düzenlemelerin güvenlik soruşturması ve arşiv araştırması neticesinde elde edilecek kişisel veri niteliğindeki bilgi ve belgeler için de geçerli olduğu açıktır. Bu itibarla dava konusu kural özel hayata saygı hakkına ilişkin bir sınırlama öngörmekte ise de -6698 sayılı Kanunla birlikte değerlendirildiğinde- konuyla ilgili temel ilkelerin kanunla konulmuş ve çerçevenin kanunla çizilmiş olması sebebiyle kanunilik şartını sağladığından Anayasanın 13. ve 20. maddelerine aykırı değildir.

Diğer taraftan, 657 sayılı Kanunun Devlet memurluğuna alınacak olanlarda aranacak genel ve özel şartları belirleyen 48. maddesinin birinci fıkrasının (A) bendine eklenen dava konusu kural Anayasanın 128. maddesinin ikinci fıkrasında öngörülen “memurların ve diğer kamu görevlilerinin nitelikleri, atanmaları ... kanunla düzenlenir” ilkesine de uygun, açık, anlaşılır ve tereddüte yer bırakmayan bir düzenleme içermektedir.

Çoğunluğun kararında, güvenlik soruşturmasına ve arşiv araştırmasına konu edilecek bilgi ve belgelerin neler olduğuna, bu bilgilerin ne şekilde kullanılacağına ve hangi mercilerin soruşturma ve araştırmayı yapacağına ilişkin herhangi bir düzenleme yapılmadığı, sadece soruşturma ve araştırma yapılmasının memurluğa alımlarda aranacak şartlar arasında sayıldığı, bu itibarla kuralın kanunilik şartını taşımadığı belirtilmekte ise de -yukarıda da açıklandığı gibi- bu hususların tamamının incelenen kuralla düzenlenmiş olması gerekmemektedir.

Nitekim icra müdür ve müdür yardımcıları ile icra kâtiplerine ilişkin sınav, görevlendirme, nakil, unvan değişikliği, görevde yükselme ve diğer hususların -kanunda herhangi bir esas öngörülmeden- yönetmelikle düzenleneceğini hükme bağlayan bir hükmün iptali talebine ilişkin davada Mahkememizce, esasen memur olan ve 657 sayılı Kanuna tâbi bulunan bu kişiler açısından kanunla düzenlenme şartının anılan Kanunda ve memurlarla ilgili diğer yasal düzenlemelerde yerine getirildiği, kanun koyucunun bu suretle yasal çerçeveyi çizdikten sonra bu çerçevenin içinde kalacak ve değişen şartlara göre farklılık gösterebilecek idare tekniğine ilişkin ayrıntıların düzenlenmesini yürütmeye bırakmasında Anayasanın 128. maddesine aykırı bir yön bulunmadığına karar verilmiştir (4/7/2013 tarihli ve E.2012/100, K.2013/84 sayılı kararımız).

Güvenlik soruşturması ve arşiv araştırması da 26/10/1994 tarihli ve 4045 sayılı Kanunla tanımlanarak düzenlenmiş ve konuya ilişkin usul ve esaslar, anılan Kanuna dayanılarak Bakanlar Kurulu Kararı ile kabul edilen ve Resmî Gazetede yayımlanarak yürürlüğe konulan Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği ile belirlenmiştir. Bu kapsamda mezkûr soruşturma ve araştırmayı yapacak merciler ile araştırılacak hususlar ve konuya ilişkin diğer usul ve esaslar da yönetmelikle ayrıntılı olarak düzenlenmiştir.

Kanunla düzenleme ilkesi açısından esas olan, kuşkusuz düzenlenen konudan yalnız kavram ve kurum olarak söz edilmesi değil, bunların kanun metninde kurallaştırılmasıdır. İncelenen bentte “güvenlik soruşturması ve/veya arşiv araştırması yapılmış olmak” Devlet memurluğuna girecek herkes için açıkça öngörülen bir kuralla genel şart olarak belirlenmiştir. Güvenlik soruşturmasının ve arşiv araştırmasının -tanımları ile usul ve esaslarına ilişkin özel kanun niteliğindeki 4045 sayılı Kanunda yer verilen hükümler de dikkate alındığında- sadece kavram ve kurum olarak belirtilmesiyle yetinilmeyip mezkûr iki kanunda kurallaştırıldığı, konuya ilişkin temel ilkelerin kanunla belirlendiği ve çerçevenin kanunla çizildiği görülmektedir.

Diğer taraftan, Anayasada öngörülen kanunîlik ilkesinin Avrupa İnsan Hakları Sözleşmesinden daha geniş bir koruma sağladığı kabul edilse de birçok kararımızda kanun hükümlerinin, daha ayrıntılı düzenlemeler içeren yönetmelik ve yönerge gibi düzenleyici işlemlerle birlikte değerlendirilmek suretiyle özel hayata saygı hakkına yapılan müdahalenin kanunîlik şartını sağladığına hükmedildiği de bilinmektedir (Bülent Polat [GK], B. No: 2013/7666, 10/12/2015, §§ 82-98, Tefik Türkmen [GK], B. No: 2013/9704, 3/3/2016, §§ 62-64; Adem Yüksel [GK], B. No: 2013/9045, 1/6/2016, §§ 67-70; Bülent Kaya [GK], B. No: 2013/2941, 11/5/2016, §§ 71-78; E.Ç.A [GK], B. No: 2014/5671, 7/6/2018, § 48).

Dolayısıyla 657 sayılı Kanunun iptali talep edilen mezkûr hükmünün -6698 ve 4045 sayılı Kanunlar ile buna dayanılarak çıkarılan Yönetmelik hükümleriyle birlikte değerlendirildiğinde- hukukun keyfî bir şekilde uygulanmasını engelleyecek açıklıkta, ulaşılabilir, öngörülebilir, anlaşılabilir ve belirli bir sınırlama öngördüğü, bu sebeple Anayasanın 13., 20. ve 128. maddelerinde öngörülen kanunîlik şartını taşıdığı açıktır.

Bu itibarla incelenen kuralın Anayasaya aykırı olmadığını düşündüğümden, kişilerin temel haklarına yönelik keyfî müdahalelere karşı yeterli güvenceler ve temel ilkeler kanunla belirlenmeden mezkûr haklara sınırlama getirildiği gerekçesiyle varılan iptal sonucuna katılmıyorum.

Üye - M. Emin KUZ

Anayasa Mahkemesi - 5490 sayılı Nüfus Hizmetleri Kanunu Kararı (2017/180)

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2017/180

Karar Sayısı: 2018/109

Karar Tarihi: 6/12/2018

RG Tarih - Sayı: 23/1/2019 - 30664

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri Engin ALTAY, Özgür ÖZEL, Engin ÖZKOÇ ile birlikte 125 milletvekili

İPTAL DAVASININ KONUSU: 19/10/2017 tarihli ve 7039 sayılı Nüfus Hizmetleri Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un;

A. 6. maddesiyle 25/4/2006 tarihli ve 5490 sayılı Nüfus Hizmetleri Kanunu'nun 22. maddesinin (2) numaralı fıkrasına "...dış temsilciliklere..." ibaresinden sonra gelmek üzere eklenen "...il ve ilçe müftülüklerine..." ibaresinin,

B. 11. maddesiyle değiştirilen 5490 sayılı Kanun'un 45. maddesinin (1) numaralı fıkrasında yer alan "...kimlik verilerini..." ibaresinin,

Anayasa'nın 2., 10., 13., 20., 24., 90. ve 136. maddelerine aykırılığı ileri sürülerek iptallerine ve yürürlüklerinin durdurulmasına karar verilmesi talebidir.

I. İPTALİ İSTENEN KANUN HÜKÜMLERİ

A. 7039 sayılı Kanun'un 6. maddesiyle eklenen ibarenin de bulunduğu 5490 sayılı Kanun'un 22. maddesinin (2) numaralı fıkrası şöyledir:

"Evlendirme yetkisi

MADDE 22- ...

(2) Evlendirme memuru; belediye bulunan yerlerde belediye başkanı veya bu işle görevlendireceği memur, köylerde muhtardır. Bakanlık, il nüfus ve vatandaşlık müdürlüklerine, nüfus müdürlüklerine ve dış temsilciliklere, il ve ilçe müftülüklerine evlendirme memurluğu yetkisi ve görevi verebilir. Eşlerden birinin yabancı olması halinde evlendirmeye, (...) belediye evlendirme memurlukları ile nüfus müdürleri yetkilidir."

B. 7039 sayılı Kanun'un 11. maddesiyle değiştirilen 5490 sayılı Kanun'un 45. maddesi şöyledir:

“Kimlik Paylaşımı Sisteminin kullanılması

MADDE 45-

(1) Bakanlık, merkezî veri tabanında tutulan verileri bu Kanunda belirtilen usul ve esaslar çerçevesinde kurumlarla; kimlik verilerini, kamu hizmeti sunan tüzel kişilikler, 3/6/2007 tarihli ve 5684 sayılı Sigortacılık Kanunu çerçevesinde faaliyette bulunan sigorta ve emeklilik şirketleri, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu çerçevesinde faaliyette bulunan bankalar, Risk Merkezi ve 5411 sayılı Kanununun 73 üncü maddesinin son fıkrası uyarınca bilgi paylaşımı amacıyla kurulmuş şirketler, 21/11/2012 tarihli ve 6361 sayılı Finansal Kiralama, Faktoring ve Finansman Şirketleri Kanunu kapsamındaki finansal kiralama şirketleri ile finansman şirketleri; yerleşim yeri ve diğer adres bilgilerini ise Bakanlıkça belirlenen adrese dayalı kamu hizmeti sunan kuruluşlar, 5684 sayılı Kanun çerçevesinde faaliyette bulunan sigorta ve emeklilik şirketleri, 5411 sayılı Kanun çerçevesinde faaliyette bulunan bankalar, Risk Merkezi ve 5411 sayılı Kanununun 73 üncü maddesinin son fıkrası uyarınca bilgi paylaşımı amacıyla kurulmuş şirketler, 6361 sayılı Finansal Kiralama, Faktoring ve Finansman Şirketleri Kanunu kapsamındaki finansal kiralama şirketleri ve finansman şirketleri ile paylaşabilir.

(2) Veri paylaşımından yararlanacakları belirlemeye, paylaşımın kapsamına ve hangi yöntemle yapılacağına karar vermek üzere Genel Müdürlük bünyesinde Veri Paylaşımı Kurulu oluşturulur. Veri Paylaşımı Kurulunun çalışma usul ve esasları Bakanlıkça çıkarılan yönetmelikle belirlenir.

(3) Birinci fıkrada belirtilenler kendi iş ve işlemlerine esas olmak üzere sadece ilgili kişilerin bilgilerini alabilirler ve aldıkları bilgileri tanımlanmış hizmetlerin yerine getirilmesi dışında başka hiçbir amaçla kullanamaz; ilgilisi veya 44 üncü maddede belirtilenler dışında kimseye veremez. Sistemin bütün aşamalarında görev yapan yetkililer de bu kurallara uymakla yükümlüdür. Bu yükümlülük, kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam eder. Bu fıkra hükümlerine aykırı davranışlar hakkında 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu hükümlerine göre işlem yapılır.

(4) Birinci fıkrada belirtilenler Kimlik Paylaşımı Sisteminden alabilecekleri verileri çevrimdışı olarak talep edemezler. Ancak kamusal hizmetin planlanması ve yürütülmesinde zorunlu bir ihtiyaç olduğunun tespit edilmesi, kullanım amacı ve yasal dayanağının belirtilmesi hâlinde ihtiyaç ile orantılı olarak veri talepleri asgari düzeyde çevrimdışı karşılanabilir.

(5) Genel Müdürlük, kişisel verilerin hukuka aykırı olarak işlenmesini, erişilmesini önlemek ve muhafazasını sağlamak amacıyla uygun güvenlik tedbirlerini alır ve veri talebinde bulunan kurum ve kamu hizmeti sunan tüzel kişilerin de bu tedbirleri almasını takip eder.

(6) Genel Müdürlükten alınan bilgilerin iş ve işlemlerde kullanılmasının hukukî sonuçları bilgiyi alan kurum ve tüzel kişiliğin sorumluluğundadır.

(7) Kimlik Paylaşımı Sistemi üzerinden nüfus kayıt örneği, yerleşim yeri belgesi ve kimlik kartı örneğine erişebilen kurum ve tüzel kişiler bu belgeleri ilgisinden ve nüfus müdürlüğünden talep etmeksizin Kimlik Paylaşımı Sisteminden temin ederler.

(8) Bu Kanun ile kurulan veri tabanlarının istatistik amaçlı kullanımında 10/11/2005 tarihli ve 5429 sayılı Türkiye İstatistik Kanunu hükümleri uygulanır.”

II. İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Zühtü ARSLAN, Burhan ÜSTÜN, Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Rıdvan GÜLEÇ, Recai AKYEL ve Yusuf Şevki HAKYEMEZ'in katılımlarıyla 4/1/2018 tarihinde yapılan ilk inceleme toplantısında dosyada eksiklik bulunmadığından işin esasının incelenmesine; yürürlüğü durdurma talebinin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

III. ESASIN İNCELENMESİ

2. Dava dilekçesi ve ekleri, Raportör Fatih ŞAHİN tarafından hazırlanan işin esasına ilişkin rapor, dava konusu Kanun hükümleri, dayanılan Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A. Kanun'un 6. Maddesiyle 5490 Sayılı Kanun'un 22. Maddesinin (2) Numaralı Fıkrasına "...dış temsilciliklere..." İbaresinden Sonra Gelmek Üzere Eklenen "...il ve ilçe müftülüklerine..." İbaresinin İncelenmesi

1. Kuralın Anlam ve Kapsamı

3. 5490 sayılı Kanun'un 22. maddesinin (1) numaralı fıkrasında, İçişleri Bakanlığının evlendirme işlemlerinin nüfus ve vatandaşlık hizmetlerinin bütünlüğü içinde yürütülmesi için gereken her türlü tedbiri alıp uygulayacağı belirtilmiştir. Maddenin (2) numaralı fıkrasında; evlendirme memurunun belediye bulunan yerlerde belediye başkanı veya bu işle görevlendireceği memur, köylerde ise

muhtar olduđu ifade edildikten sonra Bakanlıđın il nűfus ve vatandařlık műdűrlűklerine, nűfus műdűrlűklerine ve dıř temsilciliklere, il ve ile műftűlűklerine evlendirme memurluđu yetkisi ve gűrevi verebileceđi hűkműne yer verilmiřtir. Aynı fıkrada eřlerden birinin yabancı olması hâlinde evlendirmeye belediye evlendirme memurlukları ile nűfus műdűrlerinin yetkili olduđu da hűkűm altına alınmıřtır. Dava konusu kural, anılan maddenin (2) numaralı fıkrasında yer alan "...il ve ile műftűlűklerine..." ibaresidir.

4. Evlilik hukuku 22/11/2001 tarihli ve 4721 sayılı Tűrk Medenî Kanunu'nda dűzenlenmiřtir. Kanun'un 124. ve 125. maddelerinde evlenme ehliyetine iliřkin kořullar, 129 ila 133. maddelerinde de evlenmeye engel durumlar dűzenlenmiřtir. Diđer taraftan evlilik, řekle tabi bir hukuki iřlem olduđu iin Kanun'da evlenme ehliyeti ve engellerinin yanı sıra evlenme bařvurusu ve tűrenine iliřkin olarak da ayrıntılı dűzenlemelere yer verilmiřtir.

5. Anılan Kanun'un 134. maddesinde, evlenecek erkek ve kadının, ilerinden birinin oturduđu yer evlendirme memurluđuna birlikte bařvurması űngűrűlműř; 135. maddesinde, bařvurunun yazılı veya sűzlű olarak yapılabileceđi belirtilmiř; 136. maddesinde de erkek ve kadından her birinin nűfus cűzdanı ve nűfus kayıt űrneđini, űnceki evliliđi sona ermiř ise buna iliřkin belgeyi, kűek veya kısıtlı ise ayrıca yasal temsilcisinin imzası onaylanmış yazılı izin belgesini ve evlenmeye engel hastalıđının bulunmadıđını gűsteren sađlık raporunu evlendirme memurluđuna vermek zorunda olduđu hűkűm altına alınmıřtır.

6. Kanun'un 137. ve 139. maddelerinde; evlilik bařvurusunun usulűne uygun olarak yapılıp yapılmadıđını veya evleneceklerden her birinin evliliđin maddi řartlarına sahip olup olmadıđını incelemek suretiyle taraflara evlenme izni verme yetki ve gűrevi evlendirme memuruna verilmiřtir. Kanun'un 141. maddesinde, evlendirme tűreninin evlendirme dairesinde veya tarafların istemi űzerine evlendirme memurunun uygun bulacađı diđer bir yerde evlendirme memurunun ve ayırt etme gűcűne sahip ergin iki tađuđın űnűnde aık olarak yapılacađı belirtilmiřtir. Kanun'un 142. maddesinde de evleneceklerden her birine evlendirme memurunca sorulan birbiriyle evlenmek isteyip istemediklerine dair soruya taraflarca olumlu sűzlű cevap verilmesiyle evlenmenin gerekleřeceđi hűkűm altına alınmıřtır. Kanun'un 143. maddesinin ikinci fıkrasında ise aile cűzdanı gűsterilmeden evlenmenin dinî tűreninin yapılamayacađı ifade edilmiřtir.

7. 4721 sayılı Kanun'da evlendirme iřlemleri sıkı řekil řartlarına tabi tutulmuř, bu řekil řartlarının denetiminde ve evlenme tűreninin gerekleřtirilmesinde evlendirme memuru yetkili ve gűrevli kılınmıřtır. Evlendirme memurluđu gűrevini ifa edecek gűrevliler ise 4721 sayılı Kanun ile 5490 sayılı Kanun'da belirlenmiřtir.

8. 4721 sayılı Kanun'un 134. ve 5490 sayılı Kanun'un 22. maddelerine göre evlendirme memuru kural olarak belediye başkanı veya görevlendireceği memur ile muhtarlardır. Ancak İçişleri Bakanlığı dava konusu kural uyarınca il ve ilçe müftülüklerine de evlendirme memurluğu yetkisi ve görevi verebilecektir.

2. İptal Talebinin Gerekçesi

9. Dava dilekçesinde özetle; tamamen İslam dinine ait dinî hizmetleri yürütmekle görevli olan müftülüklere evlendirme memurluğu yetkisi verilmesinin evlenme törenine dinî bir nitelik kazandırdığı, sadece bir inanç grubu için evlenme törenine dinî nitelik tanınmasının bireylerin inanç özgürlüğünü güvence altına alan ve devletin tüm inanç grupları karşısında tarafsız olmasını gerektiren laiklik ilkesine aykırı olduğu, toplumdaki diğer inanç gruplarına böyle bir imkân tanınmamasının din ve vicdan özgürlüğü bakımından ayrımcılık oluşturduğu, Lozan Anlaşması'nın 43. maddesinde Müslüman olmayan azınlıklara mensup Türk vatandaşlarının inançlarına aykırı ya da dinsel ayinlerini bozucu herhangi bir işlem yapmaya zorlanamayacakları güvence altına alınmasına rağmen müftülüklerde nikâh kıydırmak istemeyenler yönünden yeterli güvenceler getirilmeyerek bireylerin din ve vicdan özgürlüklerine ölçüsüz şekilde müdahale edildiği, yapılan düzenlemenin bireylerin toplum ya da aile baskısı dolayısıyla nikâhlarını müftülüklerde kıydırmak gibi bir zorunluluk hissetmelerine sebebiyet verdiği, nikâhını müftüye kıydıranlar ve belediye memuruna kıydıranlar şeklinde toplumun yeni bir ayrışma noktasıyla karşı karşıya bırakıldığı, müftülüklere nikâh kıyma yetkisi verilmesinin Anayasa'nın 174. maddesinde Anayasa'ya aykırılığı ileri sürülemez inkılap kanunları arasında sayılan evlenme töreninin evlendirme memuru önünde yapılacağı hükmüyle bağdaşmadığı, Anayasa'nın 136. maddesinde genel idare içinde yer alan Diyanet İşleri Başkanlığının özel kanununda gösterilen görevleri yerine getireceği öngörülmesine karşın dava konusu kuralla müftülüklere özel kanununda gösterilmeyen bir görev verildiği belirtilerek kuralın Anayasa'nın 2., 10., 24., 90. ve 136. maddelerine aykırı olduğu ileri sürülmüştür.

3. Anayasa'ya Aykırılık Sorunu

10. Anayasa'nın 24. maddesinin birinci, ikinci ve üçüncü fıkralarında "Herkes, vicdan, dinî inanç ve kanaat hürriyetine sahiptir./14 üncü madde hükümlerine aykırı olmamak şartıyla ibadet, dinî âyin ve törenler serbesttir./Kimse, ibadete, dinî âyin ve törenlere katılmaya, dinî inanç ve kanaatlerini açıklamaya zorlanamaz; dinî inanç ve kanaatlerinden dolayı kınanamaz ve suçlanamaz." denilmek suretiyle din ve vicdan özgürlüğü güvence altına alınmıştır.

11. Anılan maddenin son fıkrasında ise “Kimse, Devletin sosyal, ekonomik, siyasî veya hukukî temel düzenini kısmen de olsa, din kurallarına dayandırma veya siyasî veya kişisel çıkar yahut nüfuz sağlama amacıyla her ne suretle olursa olsun dini veya din duygularını yahut dince kutsal sayılan şeyleri istismar edemez ve kötüye kullanamaz.” hükmüne yer verilmiştir. Böylece Anayasa koyucu din ve vicdan özgürlüğünü güvence altına almakla birlikte dinin veya din duygularının yahut dince kutsal sayılan şeylerin siyasi çıkar ya da nüfuz sağlamak amacıyla kullanılmasını men etmiştir.

12. Din ve vicdan özgürlüğü; herkesin din veya inancını açığa vurmasını, bunları değiştirmesini, kişilerin diledikleri inanç ve kanıya sahip olmalarını veya olmamalarını güvenceye almaktadır. Bu bağlamda Anayasa'nın 24. maddesiyle; kişinin herhangi bir inanca sahip olması veya olmaması, inancını serbestçe değiştirebilmesi, inancını açıklamaya zorlanamaması, bunlardan dolayı kınanamaması ve baskı altına alınamaması güvence altına alınarak din özgürlüğünün içsel alanı; aynı şekilde öğretim, uygulama, tek başına veya topluca ibadet ve ayin yapmak suretiyle dinini veya inancını açığa vurma hakkı ile de din özgürlüğünün dışsal alanı tanınıp koruma altına alınmıştır.

13. Anayasa'nın Başlangıç kısmı ile 2., 13., 14., 68., 81., 103., 136. ve 174. maddelerinde yer alan laiklik ilkesi ise devletin dinî inançlar karşısındaki konumunu belirleyen siyasal bir ilke olarak düzenlenmiştir. Laiklik, dini sadece bireyin iç dünyasına hapsedmemekte; onu bireysel ve kolektif kimliğin önemli bir unsuru olarak görmekte, toplumsal görünürlüğüne imkân tanımaktadır. Laik bir siyasal sistemde, dinî konulardaki bireysel tercihler ve bunların şekillendirdiği yaşam tarzları devletin müdahalesi dışında ancak koruması altındadır. Bu anlamda laiklik ilkesi, din ve vicdan özgürlüğünün güvencesidir. Öte yandan devlet, bireylerin din ve vicdan özgürlüklerini diğer bireylerin müdahalelerine karşı da korumak zorundadır. Demokratik ve laik devletin temel amaçlarından biri, toplumsal çeşitliliği koruyarak bireylerin ve toplulukların sahip oldukları inançlarıyla barış içinde bir arada yaşayabilecekleri bir hukuksal ve siyasal düzeni tesis etmektir.

14. Farklı dinî inançlara sahip olanlar ile herhangi bir dinî inanca sahip olmayanlar laik devletin koruması altındadır. Nitekim Anayasa'nın 2. maddesinin gerekçesinde yapılan tanıma göre “Hiçbir zaman dinsizlik anlamına gelmeyen laiklik, her ferdin istediği inanca, mezhebe sahip olabilmesi, ibadetini yapabilmesi ve dini inançlarından dolayı diğer vatandaşlardan farklı bir muameleye tabi kılınmaması anlamına gelir.” Devlet, din ve vicdan özgürlüğünün gerçekleşebileceği ortamı hazırlamak için gerekli önlemleri almak zorundadır.

15. Bu anlamda laiklik, devlete negatif ve pozitif yükümlülükler yüklemektedir. Negatif yükümlülük, bireylerin din özgürlüğüne zorunlu nedenler olmadıkça müdahale edilmemesini gerektirmektedir. Pozitif yükümlülük ise devletin din özgürlüğünün önündeki engelleri kaldırması, kişilerin

inandıkları gibi yaşayabileceği uygun bir ortamı ve bunun için gerekli imkânları sağlaması ödevini beraberinde getirmektedir. Laikliğin devlete yüklediği pozitif yükümlülüğün kaynağı, Anayasa'nın 24. maddesinin yanı sıra 5. maddesidir. Anayasa'nın 5. maddesine göre devletin temel amaç ve görevlerinden biri kişinin temel hak ve hürriyetlerini, sosyal hukuk devleti ve adalet ilkeleriyle bağdaşmayacak surette sınırlayan siyasal, ekonomik ve sosyal engelleri kaldırmaya, insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmaktır.

16. Laik devlet, dinler karşısında tarafsız olmakla birlikte toplumun dinî ihtiyaçlarının karşılanması konusunda kayıtsız değildir. Laiklik ilkesi, doğup geliştiği Batı'da dinin toplumsal ve kamusal alandan tamamen dışlanması sonucunu doğurmamış; dinî ihtiyaçların karşılanmasına yönelik devlet politikalarını beraberinde getirmiştir. Nitekim Anayasa'da, resmî bir dine yer verilmemekle birlikte genel idare içinde bir kamu kuruluşu olarak Diyanet İşleri Başkanlığının kurulması öngörülmüştür.

17. Anayasa'nın 136. maddesinde, Diyanet İşleri Başkanlığının laiklik ilkesi doğrultusunda bütün siyasi görüş ve düşüncülerin dışında kalarak ve milletçe dayanışma ve bütünleşmeyi amaç edinerek özel kanununda gösterilen görevleri yerine getireceği hüküm altına alınmıştır. Diyanet İşleri Başkanlığı; Anayasa'nın atıfta bulunduğu özel kanunu olan 22/6/1965 tarihli ve 633 sayılı Diyanet İşleri Başkanlığı Kuruluş ve Görevleri Hakkında Kanun'un 1. maddesi uyarınca İslam dininin inançları, ibadet ve ahlak esasları ile ilgili işleri yürütmek, din konusunda toplumu aydınlatmak ve ibadet yerlerini yönetmek amacıyla kurulmuştur. Dava konusu kuralla evlendirme memurluğu yetkisi verilen il ve ilçe müftülükleri ise Başkanlığın taşra teşkilatını oluşturmaktadır.

18. Evlendirme memurları, mevzuatta belirlenen usul ve esaslar dâhilinde evlendirme işlemlerini yapma yetkisi ve görevi verilen kişilerdir. 5490 sayılı Kanun'un 22. maddesinin (2) numaralı fıkrasında, evlendirme memurunun belediye bulunan yerlerde belediye başkanı veya bu işle görevlendireceği memur, köylerde ise muhtar olduğu; İçişleri Bakanlığının il nüfus ve vatandaşlık müdürlüklerine, nüfus müdürlüklerine ve dış temsilciliklere evlendirme memurluğu yetkisi ve görevi verebileceği hüküm altına alınmakta iken dava konusu kuralla Diyanet İşleri Başkanlığının taşra teşkilatı olan il ve ilçe müftülüklerine de evlendirme memurluğu yetkisi ve görevi verilebilmesine imkân tanınmıştır. Kuralın yer aldığı 7039 sayılı Kanun'un genel gerekçesinde, vatandaşların evlendirme işlemlerini kolaylaştırmak, daha kolay ve hızlı bir şekilde hizmet almalarını sağlamak amacıyla il ve ilçe müftülüklerine de evlendirme memurluğu yetkisinin verildiği ifade edilmiştir.

19. Evlenmenin maddi ve şekli şartları ile evlilik işlemlerinde uyulması gereken usul ve esaslar Türk Medenî Kanunu'nda düzenlenmiştir. Dolayısıyla kişiler bakımından hukuki sonuç doğuran resmî

evlilik işlemleri anılan Kanun hükümlerine göre gerçekleştirilmektedir. Kanun'un 143. maddesinin birinci fıkrasında, evlenme töreni biter bitmez evlendirme memurunun eşlere bir aile cüzdanı vereceği belirtilmiş; ikinci fıkrasında da aile cüzdanı gösterilmeden evlenmenin dinî töreninin yapılamayacağı hüküm altına alınmıştır. Anılan kural Anayasa'nın 174. maddesinde Türk toplumunu çağdaş uygarlık seviyesinin üstüne çıkarma ve Türkiye Cumhuriyeti'nin laiklik niteliğini koruma amacı güden inkılap kanunları arasında sayılmıştır. Böylece evlilik işlemlerinin evlendirme memuru tarafından gerçekleştirilmesi, dinî törenin ise resmî evlilik işlemlerinden sonra yapılması öngörülmüştür.

20. Dava konusu kuralla müftülükler verilen evlendirme memurluğu yetkisi, resmî evlilik işlemlerinin gerçekleştirilmesine yöneliktir. Müftülük görevlileri resmî evlilik işlemlerini Türk Medenî Kanunu'nun "Evlilik Hukuku" başlıklı kısmında belirlenen usul ve esaslara göre gerçekleştirmekle yükümlüdür. Bir başka deyişle il ve ilçe müftülükleri de kendilerine evlenme talebiyle başvuran kişilerin evlilik işlemlerini belediyeler, muhtarlıklar, nüfus müdürlükleri ve dış temsilcilikler gibi Türk Medenî Kanunu hükümlerine göre gerçekleştirecektir. Evlilik işlemlerinin gerçekleştirilmesi bakımından müftülükler ile diğer evlendirme memurları arasında herhangi bir fark bulunmamaktadır.

21. Anayasa Mahkemesinin 21/10/1971 tarihli ve E.1970/53, K.1971/76 sayılı kararında belirtildiği üzere Diyanet İşleri Başkanlığı, dinî bir teşkilat değil Anayasa'nın 136. maddesinde ifade edildiği gibi genel idare içinde yer almış bir kamu kuruluşudur. Başkanlık bünyesinde görev yapan personel de kamu görevlisi olup 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu'na tabidir. Bu açıdan bakıldığında il ve ilçe müftülüklerinde görev yapan personel, diğer evlendirme memurlarından farklı bir statüde değildir.

22. Yapılan açıklamalar birlikte değerlendirildiğinde dava konusu kuralın evlilik işlemlerini gerçekleştirecek mercinin belirlenmesine yönelik olduğu ve Türk Medenî Kanunu'nda düzenlenen evlilik hukuku hükümlerinde herhangi bir değişiklik öngörmediği anlaşılmaktadır. Dolayısıyla anayasal bir kurum olan ve genel idare içinde faaliyette bulunan Diyanet İşleri Başkanlığının taşra teşkilatı olan il ve ilçe müftülüklerine evlendirme memurluğu yetkisi verilmesinin resmî evlilik işlemlerine dinî bir nitelik kazandırması söz konusu değildir. Bu itibarla kuralda Anayasa'nın 24. maddesinin son fıkrasında yer alan "Devletin sosyal, ekonomik, siyasi veya hukuki temel düzeninin kısmen de olsa, din kurallarına dayandırılmayacağı" hükmüne aykırı bir husus bulunmamaktadır.

23. Türk Medenî Kanunu'nun 143. maddesinde ifade edilen "evlenmenin dinî töreni" ise toplumun büyük bir çoğunluğu tarafından resmî evlilik işlemleri gerçekleştirildikten sonra ayrıca

yapılmaktadır. Birleşmiş Milletler İnsan Hakları Komitesinin 22 No.lu genel görüşünde “Dini veya inancı dışa vurma özgürlüğü, ‘gerek alenen gerekse özel alanda bireysel olarak veya topluluk halinde’ kullanılabilir. Dini veya inancı dışa vurma özgürlüğü, ibadet, dinsel ritüellerin yerine getirilmesi, uygulama ve öğretme gibi çok geniş bir davranış yelpazesini kapsar. İbadet kavramı, bir inancın doğrudan ifade edilmesini sağlayan törensel ve ayinsel eylemleri kapsadığı gibi, bu uygulamalara özgü olan ibadet yerlerinin inşası, ayinsel ifade/duaların ve nesnelere kullanılması, sembollerin sergilenmesi ve bayram ya da dinlenme günlerine uyulmasını da kapsar.” ifadelerine yer verilmiştir. Bu kapsamda evlenmenin dinî töreni sadece İslam dini mensupları için değil belli bir inanca sahip tüm bireyler açısından din ve vicdan özgürlüğünün bir yansımasıdır.

24. Türk Medenî Kanunu’nun 143. maddesinin ikinci fıkrasında da resmî evlilik işlemlerinin gerçekleştirilmesi şartıyla bireylerin evlenmenin dinî törenini yapmaları güvence altına alınmıştır. Anılan fıkrada özellikle dinî tören terimine yer verilerek sadece belli bir inanç grubuna değil farklı inanç gruplarına mensup bireylere de bu Kanun hükümlerine göre evlilik işlemleri tamamlandıktan sonra kendi dinî inançlarına göre tören düzenleme imkânı tanınmıştır.

25. Dava konusu kuralla İslam dininin inançları, ibadet ve ahlak esasları ile ilgili işleri yürütmek amacıyla faaliyette bulunan Diyanet İşleri Başkanlığının taşra teşkilatı olan müftülüklere evlendirme memurluğu yetkisi verilerek toplumun büyük çoğunluğunu oluşturan İslam dinine mensup bireylerin resmî evlilik işlemleri gerçekleştikten sonra aynı ortamda evlenmenin dinî törenini de yaptırılmalarına imkân tanındığı görülmektedir. Böylece evlendirme memurluğu yetkisi verilen müftülük görevlileri, Türk Medenî Kanunu hükümlerine göre resmî evlilik işlemlerini gerçekleştirdikten sonra tarafların talebine göre aynı ortamda evlenmenin dinî törenine de iştirak edebilecektir. Bu yönüyle kuralın İslam dinine mensup bireylerin din ve vicdan özgürlüğü kapsamında olan evlenmenin dinî töreninin yapılmasını kolaylaştırmaya yönelik bir düzenleme olduğu anlaşılmaktadır.

26. Anayasa’da ifadesini bulan laiklik ilkesi bir yandan dinin devletin esaslarını belirlemesini engellemekte, diğer yandan da dinî hizmetlerin devlet eliyle verilmesine imkân tanımaktadır. Bu açıdan bakıldığında il ve ilçe müftülüklerine evlendirme memurluğu yetkisi verilmesi, resmî evlilik işlemlerinde herhangi bir değişiklik öngörmediğinden hukuk düzeninin din kurallarına dayandırılmasına sebebiyet vermediği gibi evlenmenin dinî töreninin yapılmasını kolaylaştırmak suretiyle bireylerin din ve vicdan özgürlüğünü koruyucu bir işlev de görmektedir.

27. Diğer taraftan 5490 sayılı Kanun’un 22. maddesinin (2) numaralı fıkrasında, evlendirme işlemlerini gerçekleştirecek evlendirme memurunun belirlenmesi bakımından bireylere seçenек

tanınmakta olup evlilik işlemlerinin sadece müftülüklerde yapılması gibi bir zorunluluk bulunmamaktadır. Dolayısıyla kural, İslam dini dışındaki inanç sahipleri veya İslam dini inancına sahip olmakla birlikte müftülüklerde evlilik işlemlerini yaptırmak istemeyenler yönünden zorlayıcı bir hüküm içermemektedir.

28. Türk Medenî Kanunu hükümlerine göre gerçekleştirilen resmî evlilik işlemleri herhangi bir dinî unsur veya ritüel barındırmadığından kişilerin evlilik işlemlerinin herhangi bir aşamasında dinî inanç ve kanaatlerini açıklamalarını gerektiren bir durum da bulunmamaktadır. Evlendirme memurlarının evlilik talebiyle başvuruda bulunan çiftlerin inançlarını sorgulama yetkisi yoktur. Bu itibarla kuralın bireylerin dinî inanç ve kanaatlerini açıklama yönünde bir baskı oluşturduğu da söylenemez.

29. Anayasa'nın 136. maddesinde Diyanet İşleri Başkanlığının özel kanununda gösterilen görevleri yerine getireceğinin ifade edilmesi, özel kanunu dışında başka bir kanunla Diyanet İşleri Başkanlığına görev verilmesine engel değildir. Dolayısıyla 5490 sayılı Kanun'la il ve ilçe müftülüklerine evlendirme memurluğu yetkisi ve görevi verilmesinin Anayasa'nın 136. maddesini ihlal eden bir yönü bulunmamaktadır.

30. Anayasa'nın 10. maddesinde yer verilen kanun önünde eşitlik ilkesi hukuksal durumları aynı olanlar için söz konusudur. Bu ilke ile eylemli değil hukuksal eşitlik öngörülmüştür. Eşitlik ilkesinin amacı aynı durumda bulunan kişilerin kanunlar karşısında aynı işleme bağlı tutulmalarını sağlamak, ayırım yapılmasını ve ayrıcalık tanınmasını önlemektir. Kanun önünde eşitlik, herkesin her yönden aynı kurallara bağlı tutulacağı anlamına gelmez. Durumlarındaki özellikler, kimi kişiler ya da topluluklar için değişik kuralları ve uygulamaları gerektirebilir. Aynı hukuksal durumlar aynı, ayrı hukuksal durumlar farklı kurallara bağlı tutulursa Anayasa'da öngörülen eşitlik ilkesi zedelenmez.

31. Toplumu oluşturan bireylerin din ve vicdan özgürlüğü alanındaki yaygın ve müşterek ihtiyaçlarının karşılanmasını kolaylaştıran tedbir ve uygulamalar eşitlik ilkesine aykırı olarak görülemez. Bu bağlamda toplumun büyük çoğunluğunu oluşturan İslam dinine mensup bireylerin inançları, ibadet ve ahlak esasları ile ilgili işleri yürütmek amacıyla Diyanet İşleri Başkanlığı kurulmuş ve Başkanlığa anayasal bir statü tanınmıştır. Dava konusu kural, İslam dinine mensup bireyler tarafından din ve vicdan özgürlüğü kapsamında bir ihtiyaç olarak görülen dinî törenin yapılmasını kolaylaştırmaya yönelik bir düzenleme niteliğindedir.

32. Nitekim Avrupa İnsan Hakları Mahkemesi (AİHM) de objektif ve gerekli olduğu takdirde çoğunluk dininin mensuplarına farklı muamelenin Avrupa İnsan Hakları Sözleşmesi'ne aykırılık teşkil etmeyeceğini kabul etmektedir. Mahkemenin Büyük Dairesi, Lautsi/İtalya davasında Hristiyanlığın sembollerinden olan çarmıha gerilmiş İsa figürünün sınıflarda asılı olmasının

çoğunluk dini olan Hristiyanlığın okul ortamında baskın bir görünürlüğe sahip olması anlamına geldiğini kabul etmiştir. Ancak Mahkeme bu durumun tek başına çoğulculuk ilkelerinden uzaklaşma ve ideoloji aşılama anlamına gelmediği sonucuna ulaşmıştır (B. No: 30814/06, 18/3/2011, §§ 71,76).

33. Dava konusu kural İslam dini dışındaki inanç sahipleri aleyhine bir düzenleme getirmemektedir. Kanun'da evlilik işlemlerini gerçekleştirecek evlendirme memuru konusunda bireylere seçenek tanınmakta olup gayrimüslim azınlıklar da dâhil olmak üzere toplumdaki herhangi bir inanç grubu yönünden evlilik işlemlerinin müftülüklerde yaptırılması gibi bir zorunluluk bulunmamaktadır. Kuralla müftülüklere verilen evlendirme memurluğu yetkisi, Türk Medenî Kanunu hükümlerine göre gerçekleştirilen resmî evlilik işlemlerine yönelik olup medeni nikâh esaslarında herhangi bir değişiklik öngörülmemektedir. Evliliğin hukuki sonuç doğurabilmesi için Türk Medenî Kanunu hükümlerine göre resmî evlilik işlemlerinin gerçekleştirilmesi zorunlu olup bu konuda herhangi bir dinî gruba ayrıcalık tanınmamaktadır. Diğer taraftan anılan Kanun'un 143. maddesinde ayırım gözetmeksizin bireylere, resmî evlilik işlemleri gerçekleştikten sonra kendi inançlarına göre dinî tören yapma imkânı da sağlanmıştır. Dolayısıyla gerek resmî evlilik işlemleri gerekse de evlenmenin dinî töreni bakımından farklı inanç grupları arasında herhangi bir ayrımcılık yapılması söz konusu değildir.

34. Açıklanan nedenlerle kural Anayasa'nın 2., 10., 24. ve 136. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ, Recep KÖMÜRCÜ ile Rıdvan GÜLEÇ bu görüşe farklı gerekçeyle katılmışlardır.

Kuralın Anayasa'nın 90. maddesiyle ilgisi görülmemiştir.

B. Kanun'un 11. Maddesiyle Değiştirilen 5490 Sayılı Kanun'un 45. Maddesinin (1) Numaralı Fıkrasında Yer Alan "...kimlik verilerini..." İbaresinin İncelenmesi

1. Kuralın Anlam ve Kapsamı

35. 5490 sayılı Kanun'un dava konusu kuralın da yer aldığı (1) numaralı fıkrasında İçişleri Bakanlığının (Bakanlık), merkezî veri tabanında tutulan verileri Kanun'da belirtilen usul ve esaslar çerçevesinde kurumlarla; kimlik verilerini, kamu hizmeti sunan tüzel kişilikler,3/6/2007 tarihli ve 5684 sayılı Sigortacılık Kanunu çerçevesinde faaliyette bulunan sigorta ve emeklilik şirketleri, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu çerçevesinde faaliyette bulunan bankalar, Risk Merkezi ve 5411 sayılı Kanun'un 73. maddesinin son fıkrası uyarınca bilgi paylaşımı amacıyla kurulmuş şirketler, 21/11/2012 tarihli ve 6361 sayılı Finansal Kiralama, Faktoring ve Finansman

Şirketleri Kanunu kapsamındaki finansal kiralama şirketleri ile finansman şirketleri; yerleşim yeri ve diğer adres bilgilerini ise Bakanlıkça belirlenen adrese dayalı kamu hizmeti sunan kuruluşlar, 5684 sayılı Kanun çerçevesinde faaliyette bulunan sigorta ve emeklilik şirketleri, 5411 sayılı Kanun çerçevesinde faaliyette bulunan bankalar, Risk Merkezi ve 5411 sayılı Kanunun 73. maddesinin son fıkrası uyarınca bilgi paylaşımı amacıyla kurulmuş şirketler, 6361 sayılı Kanun kapsamındaki finansal kiralama şirketleri ve finansman şirketleri ile paylaşabileceği hüküm altına alınmıştır. Dava konusu kural, anılan fıkrada yer alan "...kimlik verilerini..." ibaresidir.

36. Buna göre Bakanlık, merkezî veri tabanında tutulan kimlik verilerini 5490 sayılı Kanun'da belirtilen usul ve esaslar çerçevesinde, kamu hizmeti sunan tüzel kişilikler, 5684 sayılı Kanun çerçevesinde faaliyette bulunan sigorta ve emeklilik şirketleri, 5411 sayılı Kanun çerçevesinde faaliyette bulunan bankalar, Risk Merkezi ve 5411 sayılı Kanun'un 73. maddesinin son fıkrası uyarınca bilgi paylaşımı amacıyla kurulmuş şirketler, 6361 sayılı Kanun kapsamındaki finansal kiralama şirketleri ve finansman şirketleri ile paylaşabilecektir.

37. Kimlik Paylaşım Sistemi (KPS), merkezî veri tabanında bulunan vatandaşlara ait kişisel verilere kamu kurumları ve diğer tüzel kişilerin güncel ve güvenli bir şekilde online erişmesine imkân sağlamak üzere kurulmuş bir sistemdir. KPS veri tabanındaki veriler; Türk vatandaşlığının ispatında ve belgelendirilmesinde esas olduğu kadar kişinin kimliği, medenî hâli ve aile bağlarının belirlenmesinde de temel resmî bilgilerdir. Bu veriler aksi sabit oluncaya kadar geçerlidir.

38. KPS'nin kullanılmasına ilişkin usul ve esaslar Kanun'un 45. maddesinde düzenlenmiştir. Maddenin (1) numaralı fıkrasında, KPS veri tabanında bulunan verilerin paylaşılacağı kurumlar ve tüzel kişilikler sayılmış; (2) numaralı fıkrasında veri paylaşımından yararlanacakları belirleme, paylaşımın kapsamı ve hangi yöntemle yapılacağı konusunda Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü (Genel Müdürlük) bünyesinde oluşturulan Veri Paylaşımı Kurulunun yetkili olduğu belirtilmiştir.

39. Maddenin (3) numaralı fıkrasında veri paylaşımında bulunan kurum ve tüzel kişiliklerin kendi iş ve işlemlerine esas olmak üzere sadece ilgili kişilerin bilgilerini alabileceği belirtildikten sonra bu bilgilerin tanımlanmış hizmetlerin yerine getirilmesi dışında başka bir amaçla kullanılması ve bu bilgilerin ilgilisi veya Kanun'un 44. maddesinde belirtilenler dışında herhangi bir kimseye verilmesi yasaklanmıştır. Fıkra, sistemin bütün aşamalarında görev yapan yetkililer de bu kurallara uymakla yükümlü kılınmış; bu yükümlülüğün kamu görevlilerinin görevlerinden ayrılmasından sonra da devam etmesi öngörülmüştür. Fıkra hükümlerine aykırı davranışlar hakkında ise 24/3/2016 tarihli

ve 6698 sayılı Kişisel Verilerin Korunması Kanunu hükümlerine göre işlem yapılacağı hüküm altına alınmıştır.

40. Maddenin (4) numaralı fıkrasında KPS'den alınabilecek verilerin çevrim dışı olarak talep edilemeyeceği ancak kamusal hizmetin planlanması ve yürütülmesinde zorunlu bir ihtiyaç olduğunun tespit edilmesi, kullanım amacı ve yasal dayanağının belirtilmesi hâlinde ihtiyaç ile orantılı olarak veri taleplerinin asgari düzeyde çevrim dışı karşılanabileceği belirtilmiştir.

41. Maddenin (5) numaralı fıkrasında, Genel Müdürlük kişisel verilerin hukuka aykırı olarak işlenmesini ve bunlara erişilmesini önlemek ile muhafazasını sağlamak amacıyla uygun güvenlik tedbirlerini almak ve veri talebinde bulunan kurum ve kamu hizmeti sunan tüzel kişilerin de bu tedbirleri almasını takip etmekle yükümlü tutulmuştur. Maddenin (6) numaralı fıkrasında da Genel Müdürlükten alınan bilgilerin iş ve işlemlerde kullanılmasından doğacak hukuki sonuçlardan bilgiyi alan kurum ve tüzel kişilik sorumlu kılınmıştır.

42. Diğer taraftan kişisel verilerin işlenmesinde gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenleyen 6698 sayılı Kanun'un 2. maddesinde Kanun hükümlerinin kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanacağı ifade edilmiştir. Dolayısıyla KPS üzerinden veri paylaşımında da 6698 sayılı Kanun'da yer alan tüm ilke ve kurallar ile güvencelere uyulması zorunludur.

2. İptal Talebinin Gerekçesi

43. Dava dilekçesinde özetle; dava konusu kuralla özel nitelikli bilgiler de dâhil olmak üzere bireylerin kişisel bilgilerinin rızaları olmaksızın kamu kurumları ve özel şirketlerle paylaşılmasına imkân tanındığı, verilerin paylaşılmasında herhangi bir sınırlama getirilmediği gibi özel nitelikli verilerin paylaşılmasını önleyecek herhangi bir tedbir de öngörülmediği, kimlik verilerinin bilgi paylaşımı amacıyla kurulmuş şirketlerle paylaşılmasının bu verilerin kişilerin açık rızası olmaksızın yabancı finans kurumları da dâhil pek çok şirketle paylaşılmasına sebebiyet vereceği, bireylerin özel nitelikli verileri de dâhil olmak üzere kişisel verilerinin yabancı şirketleri kapsayacak şekilde şirket ve kurumlarla paylaşılmasına imkân tanınmasının demokratik bir toplumda gerekli olmadığı belirtilerek kuralın Anayasa'nın 13. ve 20. maddelerine aykırı olduğu ileri sürülmüştür.

3. Anayasa'ya Aykırılık Sorunu

44. Anayasa'nın 20. maddesinin ilk fıkrasında, herkesin özel hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş; son

fıkrasında da “Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.” denilerek kişisel verilerin korunması, özel hayatın gizliliğinin korunması kapsamında güvenceye kavuşturulmuştur.

45. Özel hayatın korunması her şeyden önce özel hayatın gizliliğinin korunması, başkalarının gözleri önüne serilmemesi demektir. Kişinin özel hayatında yaşananların yalnız kendisi veya kendisinin bilmesini istediği kişiler tarafından bilinmesini isteme hakkı, kişinin temel haklarından biridir ve bu niteliği nedeniyle insan haklarına ilişkin beyanname ve sözleşmelerde yer almış, tüm demokratik ülkelerin mevzuatlarında açıkça belirlenen istisnalar dışında devlete, topluma ve diğer kişilere karşı korunmuştur.

46. Kişisel verilerin korunmasını isteme hakkı, kişinin insan onurunun korunması ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Bilişim teknolojilerindeki gelişmeler sonucunda geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi, daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezî olarak bir araya getirilebilmesi, verilerin veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle veriden yeni veriler üretme kapasitesinin artması, verilere erişim ve veri transferinin kolaylaşması, kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde özel sektör unsurlarınca oluşturulan risklerin daha yaygın ve önemli boyutlara ulaşması, terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır.

47. Belirtilen sebeplerle kişisel verilerin en üst seviyede korunması zorunlu olmakla birlikte bu hak mutlak ve sınırsız olmayıp Anayasa'nın 13. ve 20. maddeleri gereğince belirli koşullarda, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmamak üzere kanunla sınırlanabilir.

48. Türkiye'nin imzaladığı 1981 tarihli ve 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Avrupa Konseyi Sözleşmesi'nin 9. maddesinde de devlet güvenliği, kamu güvenliği, devletin ekonomik menfaatlerinin korunması ve suçlarla mücadele edilmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması ile verilerin istatistiki veya bilimsel amaçlarla kullanılması durumlarında kişisel verilerin korunmasına sınırlamalar getirilebileceği öngörülmüştür.

49. Anayasa'nın 20. maddesi uyarınca kişisel veriler ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir. Dolayısıyla kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvencenin yaşama geçirilebilmesi için bu hakkı ilgilendiren yasal düzenlemelerin açık, anlaşılabilir ve kişilerin söz konusu haklarını kullanabilmelerine elverişli olması gerekir. Ancak böyle bir düzenleme ile kişilerin özel hayatlarını ilgilendiren veri, bilgi ve belgelerin resmî makamların keyfî müdahalelerine karşı korunması mümkün hâle getirilebilir.

50. Anayasa'nın 13. maddesinde "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz." denilmektedir. Anayasa'nın 13. maddesi uyarınca kişisel verilerin korunmasını isteme hakkına getirilen sınırlamalar hakkın özüne dokunamayacağı gibi Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamaz.

51. Dokunulamayacak öz, her temel hak ve özgürlük açısından farklılık göstermekle birlikte kanunla getirilen sınırlamanın hakkın özüne dokunmadığının kabulü için temel hakların kullanılmasını ciddi surette güçleştirip amacına ulaşmasına engel olmaması ve etkisini ortadan kaldıracı bir nitelik taşımaması gerekir.

52. Anayasa'nın 13. maddesinde ifade edilen ölçülülük ilkesi, temel hak ve özgürlüklerin sınırlandırılmasına ilişkin başvurularda dikkate alınması gereken bir diğer ilkedir. Demokratik toplum düzeninin gerekleri ve ölçülülük ilkeleri, iki ayrı kriter olarak düzenlenmiş olmakla birlikte bu iki kriter arasında sıkı bir ilişki vardır. Temel hak ve özgürlüklere yönelik herhangi bir sınırlamanın başvurulabilecek en son çare ya da alınabilecek en son önlem olarak temel haklara en az müdahaleye imkân veren ölçülü bir sınırlama niteliğinde olup olmadığının incelenmesi gerekir.

53. Demokratik toplum kişilerin temel hak ve özgürlüklerinin en geniş şekilde güvence altına alındığı bir düzeni gerektirir. Demokrasilerde devlete düşen görev temel hak ve özgürlükleri korumak ve geliştirmek, bunların etkili şekilde kullanılmasını sağlayacak tedbirleri almaktır. Bu kapsamda devlet, özellikle temel hak ve özgürlükleri ortadan kaldıracak veya bunlara ölçsüz müdahale teşkil edecek tutumlardan kaçınmalı ve başkalarından gelebilecek tehditlere karşı bireyleri korumalıdır.

54. 6698 sayılı Kanun'un 3. maddesine göre kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Anayasa Mahkemesinin yerleşik kararlarında da belirtildiği üzere "... adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası,

özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler”kişisel veri olarak kabul edilmektedir (AYM, E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2013/84, K.2014/183, 4/12/2014; E.2014/74, K.2014/201, 25/12/2014; E.2014/180, K.2015/30, 19/3/2015; E.2015/32, K.2015/102, 12/11/2015).

55. Dava konusu kuralla Bakanlık merkezî veri tabanında kayıtlı olan adı, soyadı, doğum tarihi gibi bireylerin kimliğini ortaya koyan kimlik verilerinin, kamu hizmeti sunan tüzel kişilikler, 5684 sayılı Kanun çerçevesinde faaliyette bulunan sigorta ve emeklilik şirketleri, 5411 sayılı Kanun çerçevesinde faaliyette bulunan bankalar, Risk Merkezi ve 5411 sayılı Kanun’un 73. maddesinin son fıkrası uyarınca bilgi paylaşımı amacıyla kurulmuş şirketler, 6361 sayılı Kanun kapsamındaki finansal kiralama şirketleri ile finansman şirketleri ile paylaşılabilmesine imkân tanınmaktadır. Bu yönüyle kuralın kişisel verilerin korunmasını isteme hakkına bir müdahale içerdiği açıktır.

56. Toplumun genel ve ortak gereksinimlerini karşılamak üzere topluma sunulan sürekli ve düzenli etkinlikler olarak tanımlanan kamu hizmeti, Devlet veya diğer kamu tüzel kişileri tarafından yerine getirildiği gibi bunların gözetim ve denetimleri altında özel hukuk kişileri tarafından da yerine getirilmektedir. Bu çerçevede kamu kurumlarının olduğu gibi kamu hizmeti sunan diğer tüzel kişilerin de doğru ve güvenilir bilgiye en kısa sürede ulaşması, kamu hizmetinin etkin ve verimli bir şekilde gerçekleşmesi için büyük bir önem taşımaktadır. Dava konusu kuralın da kamu hizmeti sunan tüzel kişilerle özellikle finans sektöründe faaliyette bulunan sigorta ve emeklilik şirketleri, bankalar, finansal kiralama ve finansman şirketlerinin kendi iş ve işlemlerinde kullanmak üzere ihtiyacı olan verilere en hızlı ve güvenilir şekilde ulaşmalarını sağlamak amacıyla düzenlendiği anlaşılmaktadır. Anılan kuruluşlar faaliyetlerinde, kendi iş ve işlemlerine esas olmak üzere ihtiyacı olan kimlik verilerine KPS üzerinden otomatik olarak online şekilde erişebilecektir. Böylece vatandaşların kamu hizmeti sunan tüzel kişilerle, sigorta, emeklilik, bankacılık, finansal kiralama iş ve işlemleri en kısa sürede sonuçlanacağı gibi kimlik bilgileri merkezî veri tabanında yer alan kimlik bilgileriyle kontrol edileceğinden sahte belgelerle işlem yapılmasının da önüne geçilebilecektir. Bu açıdan bakıldığında kuralın toplumsal bir ihtiyacın karşılanmasına yönelik olarak kamu yararı amacıyla öngörüldüğü anlaşılmaktadır.

57. Kanun’un 45. maddesinin (1) numaralı fıkrasında kimlik verilerinin kimlerle paylaşılacağı genel olarak belirtilmiş, (2) numaralı fıkrasında veri paylaşımından yararlanacakları belirleme konusunda Genel Müdürlük bünyesinde oluşturulan Veri Paylaşım Kurulu yetkili kılınmıştır.

Maddenin (3) numaralı fıkrasında verilerin veri paylaşımından yararlanacak kuruluşların kendi iş ve işlemlerine esas olmak üzere ilgili kişilerin bilgilerini alabilecekleri ve aldıkları bilgileri tanımlanmış hizmetlerin yerine getirilmesi dışında başka hiçbir amaçla kullanamayacakları belirtilerek kimlik verilerinin paylaşımına ve kullanım amacına yönelik çeşitli sınırlamalar getirilmiştir. Diğer taraftan kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenleyen temel kanun olan 6698 sayılı Kanun'un 4. maddesinde, kişisel verilerin hukuka ve dürüstlük kurallarına uygun şekilde belirli, açık ve meşru amaçlar için işlenmesi, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi öngörülmüş; 5. maddesinde verilerin işlenme şartları, 6. maddesinde özel nitelikli kişisel verilerin işlenme şartları, 7. maddesinde verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi, 8. maddesinde kişisel verilerin aktarılması, 9. maddesinde verilerin yurt dışına aktarılması, 10. maddesinde veri sorumlusunun yükümlülükleri, 11. maddesinde de ilgili kişinin hakları düzenlenmiştir. Anılan Kanun hükümlerinin KPS üzerinden yapılacak veri paylaşımında da geçerli olduğunda herhangi bir tereddüt bulunmadığından KPS veri tabanından veri paylaşımı yapanların 6698 sayılı Kanun'da belirtilen usul ve esaslara da uymak zorunda oldukları açıktır.

58. Kanun'un 45. maddesinin (3) numaralı fıkrasında; sistemin bütün aşamalarında görev yapan yetkililerin veri paylaşımına ilişkin olarak Kanun'da belirtilen kurallara uymakla yükümlü olduğu, bu yükümlülüğün kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam edeceği, yükümlülüklerine aykırı davranışlar hakkında 6698 sayılı Kanun hükümlerine göre işlem yapılacağı hüküm altına alınmıştır. 6698 sayılı Kanun'un 17. maddesinde, kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140. maddeleri hükümlerinin uygulanacağı ve Kanun'un 7. maddesi hükmüne aykırı olarak kişisel verileri silmeyen veya anonim hâle getirmeyenlerin 5237 sayılı Kanun'un 138. maddesine göre cezalandırılacağı hükme bağlanmıştır. 5237 sayılı Kanun'un 136. maddesi uyarınca da kişisel verileri hukuka aykırı olarak başkasına vermek, yaymak veya ele geçirmek suç olarak düzenlenmiştir.

59. 5490 sayılı Kanun ve 6698 sayılı Kanun'da yer alan düzenlemeler birlikte değerlendirildiğinde KPS üzerinden paylaşılacak kimlik verilerinin amacı dışında kullanılmasını ve ifşa edilmesini önleyecek yasal güvencenin sağlandığı görülmektedir. Bu bağlamda kişisel verilerin korunması hakkına sınırlama getirilirken Kanun'da sınırlama aracının sınırlama amacına uygun ve orantılı şekilde kullanılmasını sağlayacak yasal güvencelere yer verildiği, böylece hem kişisel verilerin korunmasını isteme hakkının özünün zedelenmesinin önlendiği hem de bu hak ile kamusal

hizmetlerin yürütülmesi arasındaki makul dengenin gözetildiği anlaşılmaktadır. Dolayısıyla dava konusu kuralda kişisel verilerin korunmasını isteme hakkının özüne dokunan ya da bu hakkı ölçüsüz şekilde sınırlandıran bir husus bulunmadığı gibi kuralın demokratik toplum düzeninin gereklerine aykırılık teşkil eden bir yönü de bulunmamaktadır.

60. Açıklanan nedenlerle kural Anayasa'nın 13. ve 20. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

IV. YÜRÜRLÜĞÜN DURDURULMASI TALEBİ

61. Dava dilekçesinde özetle, dava konusu kuralların bu hâliyle uygulanmasının telafisi güç veya imkânsız zararların doğmasına sebebiyet vereceği belirtilerek kuralların yürürlüklerinin durdurulması talep edilmiştir.

19/10/2017 tarihli ve 7039 sayılı Nüfus Hizmetleri Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un;

A. 6. maddesiyle 25/4/2006 tarihli ve 5490 sayılı Nüfus Hizmetleri Kanunu'nun 22. maddesinin (2) numaralı fıkrasına "...dış temsilciliklere..." ibaresinden sonra gelmek üzere eklenen "...il ve ilçe müftülüklerine..." ibaresine,

B. 11. maddesiyle değiştirilen 5490 sayılı Kanun'un 45. maddesinin (1) numaralı fıkrasında yer alan "...kimlik verilerini..." ibaresine

yönelik iptal talepleri 6/12/2018 tarihli ve E.2017/180, K.2018/109 sayılı kararla reddedildiğinden bu ibarelere ilişkin yürürlüğün durdurulması talebinin REDDİNE 6/12/2018 tarihinde OYBİRLİĞİYLE karar verilmiştir.

V. HÜKÜM

19/10/2017 tarihli ve 7039 sayılı Nüfus Hizmetleri Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un;

A. 6. maddesiyle 25/4/2006 tarihli ve 5490 sayılı Nüfus Hizmetleri Kanunu'nun 22. maddesinin (2) numaralı fıkrasına "...dış temsilciliklere..." ibaresinden sonra gelmek üzere eklenen "...il ve ilçe müftülüklerine..." ibaresinin,

B. 11. maddesiyle değiştirilen 5490 sayılı Kanun'un 45. maddesinin (1) numaralı fıkrasında yer alan "...kimlik verilerini..." ibaresinin

Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE 6/12/2018 tarihinde OYBİRLİĞİYLE karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili - Burhan ÜSTÜN

Başkanvekili - Engin YILDIRIM

Üye: Serdar ÖZGÜLDÜR; Serruh KALELİ; Recep KÖMÜRCÜ; Hicabi DURSUN; Celal Mümtaz AKINCI; Muammer TOPAL; M. Emin KUZ; Hasan Tahsin GÖKCAN; Kadir ÖZKAYA; Rıdvan GÜLEÇ; Recai AKYEL; Yusuf Şevki HAKYEMEZ

FARKLI GEREKÇE

1. Dava konusu kural olan "...il ve ilçe müftülüklerine..." ibaresinin Anayasaya aykırı olmadığına Mahkememiz tarafından oybirliğiyle karar verilmiştir. Kural, evlilik işlemlerini gerçekleştirecek yetkililerin belirlenmesine düzenleyerek, il ve ilçe müftülüklerine de evlendirme memurluğu yetkisi ve görevi verilebilmesine imkân tanımaktadır. Kuralla, resmî evlilik işlemlerini içeren Medeni Kanun hükümlerinde herhangi bir değişiklik getirilmemektedir.

2. Kuralın da yer aldığı 7039 sayılı Kanun'un genel gerekçesinde, vatandaşların evlendirme işlemlerini kolaylaştırmak ve daha kolay ve hızlı bir şekilde hizmet almalarını sağlamak amacıyla il ve ilçe müftülüklerine de evlendirme memurluğu yetkisinin verildiği ifade edilmiştir. Dava konusu kuralın gerekçesinde de evlendirme memurları arasına il ve ilçe müftülüklerinin eklendiği belirtilmiştir. Müftülük görevlileri 657 sayılı Devlet Memurlarına tabi kamu görevlisi olup, diğer evlendirme memurlarıyla aynı konumda bulunmaktadır.

3. İptali talep edilen kural, 4721 sayılı Kanun'un 143. maddesinde "evlenmenin dini töreni" olarak ifade edilen ve toplumun büyük bir çoğunluğunu meydana getiren İslam inancına sahip bireylerin önemli bir bölümünce de yerine getirilen uygulamayı kolaylaştırarak resmi evlendirme ile evlenmenin dini törenini birbirine bağlayan bir çeşit köprü olarak yorumlanmamalıdır. Kural, laiklik ilkesinin ve din ve vicdan özgürlüğünün devlete yüklediği pozitif yükümlülükler bağlamında değerlendirilmemelidir. Zira kural, evlenmenin dini töreninden ziyade kanunun genel gerekçesinde de vurgulandığı gibi resmi evlendirme işlemlerini kolaylaştırma amacını taşımaktadır.

4. Burada din hizmetleri sınıfında görev yapan kamu görevlilerine dini bir özellik ve işlev taşımayan bir görev verilmiştir. Müftülüklere böyle bir yetki verilmesi yasa koyucunun takdir yetkisi içindedir.

5. Yukarıda belirtilen gerekçeyle Mahkeme kararına katılmaktayız.

Başkanvekili - Engin YILDIRIM

Üye: Serdar ÖZGÜLDÜR; Serruh KALELİ; Recep KÖMÜRCÜ; Rıdvan GÜLEÇ

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2017/16

Karar Sayısı: 2019/64

Karar Tarihi: 24/7/2019

RG Tarih - Sayı: 13/11/2019 - 30947

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri Engin ALTAY, Levent GÖK, Özgür ÖZEL ile birlikte 121 milletvekili

İPTAL DAVASININ KONUSU: 9/11/2016 tarihli ve 6757 sayılı Kanun'un;

A. 7. maddesiyle 31/7/1970 tarihli ve 1324 sayılı Genelkurmay Başkanının Görev ve Yetkilerine Ait Kanun'un 8. maddesinin değiştirilen birinci fıkrasının,

B. 22. maddesiyle 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'nun 60. maddesine eklenen (11) numaralı fıkranın (28/11/2017 tarihli ve 7061 sayılı Kanun'un 99. maddesiyle aynı maddeye eklenen (9) numaralı fıkra nedeniyle (12) numaralı fıkra şeklinde teselsül ettirilmiştir) birinci ve üçüncü cümlelerinin,

C. 23. maddesiyle 4/6/1937 tarihli ve 3201 sayılı Emniyet Teşkilât Kanunu'nun ek 24. maddesine eklenen üçüncü fıkranın birinci cümlesinde yer alan "...Kamu Personel Seçme Sınavı şartı aranmaksızın,..." ibaresinin,

Ç. 25. maddesiyle 6/1/1982 tarihli ve 2576 sayılı Bölge İdare Mahkemeleri, İdare Mahkemeleri ve Vergi Mahkemelerinin Kuruluşu ve Görevleri Hakkında Kanun'a eklenen geçici 21. maddenin, Anayasa'nın 2., 13., 20., 36., 90., 118., 138., 139., 140. ve 148. maddelerine aykırılığı ileri sürülerek iptallerine ve yürürlüklerinin durdurulmasına karar verilmesi talebidir.

I. İPTALİ İSTENEN KANUN HÜKÜMLERİ

6757 sayılı Kanun'un iptali talep edilen kuralların da yer aldığı;

1. 7. maddesiyle 1324 sayılı Kanun'un 8. maddesinin değiştirilen birinci fıkrası şöyledir:

“(Değişik birinci fıkra: 15/8/2016-KHK-671/8 md.; Aynen kabul: 9/11/2016-6757/7 md.) Genelkurmay Başkanı; orgeneral ve oramiraller arasından, Bakanlar Kurulunun teklifi üzerine Cumhurbaşkanınca atanır.”

2. 22. maddesiyle 5809 sayılı Kanun’un 60. maddesine eklenen (11) numaralı fıkra şöyledir:

“(11) (Ek: 15/8/2016-KHK-671/25 md.; Aynen kabul: 9/11/2016-6757/22 md.) Kurum, görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilir ve değerlendirmesini yapabilir; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilir, bunlarla irtibat kurabilir ve bu kapsamda diğer gerekli önlemleri alabilir veya aldırabilir. Kurum, bu fıkroda belirtilen görevlerin ifasında bakanlıklar, kurum ve kuruluşlar ile işbirliği içerisinde çalışır. Bu kapsamda Kurum tarafından istenen her türlü bilgi ve belge talebi; ilgili bakanlık, kurum ve kuruluşlar tarafından gecikmeksizin yerine getirilir. Bu fıkroya göre bilgi ve belge talebinde bulunulması ve bu taleplerin yerine getirilmesine ilişkin usul ve esaslar ile diğer hususlar Başbakanlıkça belirlenir.”

3. 23. maddesiyle 3201 sayılı Kanun’un ek 24. maddesine eklenen üçüncü fıkra şöyledir:

“(Ek fıkra: 15/8/2016-KHK-671/26 md.; Değişik fıkra: 3/10/2016-KHK-676/28 md.; Aynen kabul: 9/11/2016-6757/23 md.) Özel hareket birimlerinde istihdam edilmek üzere, yirmisekiz yaşından gün almamış olmak kaydıyla, en az lise veya dengi okul mezunları, Kamu Personel Seçme Sınavı şartı aranmaksızın, fiziki yeterlilik ve mülakat sınavları ile polis meslek eğitim merkezlerine alınabilir. Bu fıkra kapsamında alınacak olanların eğitim süresi ve eğitim şekline ilişkin usul ve esaslar ile diğer hususlar Bakanlık tarafından belirlenir.”

4. 25. maddesiyle 2576 sayılı Kanun’a eklenen geçici 21. madde şöyledir:

“Geçici Madde 21- (Ek: 15/8/2016-KHK/671/28 md.; Aynen kabul: 9/11/2016- 6757/25 md.)

31/12/2020 tarihine kadar bölge idare mahkemesi üyeliğine, hâkimlik ve savcılık mesleğinde fiilen en az altı yıl görev yapmış ve üstün başarısı ile bölge idare mahkemesinde yararlı olacağı anlaşılmış bulunan idarî yargı hâkim ve savcıları arasından atama yapılabilir.”

II. İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Zühtü ARSLAN, Burhan ÜSTÜN, Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Recai AKYEL ve Yusuf Şevki HAKYEMEZ’in katılımlarıyla 9/2/2017

tarihinde yapılan ilk inceleme toplantısında, dosyada eksiklik bulunmadığından işin esasının incelenmesine, yürürlüğü durdurma talebinin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

III. ESASIN İNCELENMESİ

2. Dava dilekçesi ve ekleri, Raportör Aydın AYGÜN tarafından hazırlanan işin esasına ilişkin rapor, dava konusu kanun hükümleri, dayanan Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A. Olağanüstü Hâl Yönetim Usulünün Anayasal Çerçevesi

3. Olağanüstü yönetim usulleri; iç karışıklık, ayaklanma, savaş tehlikesinin baş göstermesi, savaş hâli, doğal afet, ağır ekonomik bunalım ve benzeri nedenlerle devletin ve toplumun güvenliğini büyük ölçüde sarsan durumlarla karşılaşıldığında başvuru yönetim şekilleridir. Belirtilen durumların devletin ve toplumun varlığı ve güvenliği bakımından büyük bir tehlike oluşturduğu kuşkusuzdur. Olağan dönemdeki yönetim rejiminin ve hukuk kurallarının bu tehlikelerin giderilmesinde yetersiz kalabilmesi nedeniyle çağdaş hukuk sistemlerinde olağanüstü hâllerde özel yönetim usullerinin uygulanmasına da imkân tanınmaktadır. Bir başka ifadeyle olağanüstü yönetim usulleri bir zaruretten kaynaklanmakta olup demokratik anayasal düzenin korunması ve sürdürülebilmesi için bu yönetim usullerine başvurulması zorunluluğu ortaya çıkabilmektedir. Bu bağlamda olağanüstü yönetimler neden olan tehlikelerin bertaraf edilebilmesi için olaylar karşısında ivedi önlem ve karar alabilme ihtiyacı duyan yürütmenin yetkilerinin artırılması gerekebilmektedir.

4. Bununla birlikte demokratik ülkelerde olağanüstü yönetim usulleri hukuku dışlayan, keyfi yönetim anlamına gelmez. Olağanüstü yönetim usulleri kaynağını Anayasa'da bulmakta, anayasal kurallara göre yürürlüğe konularak yasama ve yargı organlarının denetiminde varlıklarını sürdürmektedir. Olağanüstü yönetimlerin amacı, anayasal düzeni korumak ve savunmaktır. Bu nedenle olağanüstü hâl yürütme organına önemli yetkiler vermesine, hak ve özgürlükleri de önemli ölçüde sınırlandırmasına karşın hukuki bir rejimdir.

5. 21/1/2017 tarihli ve 6771 sayılı Türkiye Cumhuriyeti Anayasasında Değişiklik Yapılmasına Dair Kanun'la yapılan değişiklik öncesinde olağanüstü hâl sebepleri Anayasa'nın 119. ve 120. maddelerinde düzenlenmiş ve 119. maddede "tabii afet, tehlikeli salgın hastalıklar veya ağır ekonomik bunalım halleri"; 120. maddede de "Anayasa ile kurulan hür demokrasi düzenini veya temel hak ve hürriyetleri ortadan kaldırmaya yönelik yaygın şiddet hareketlerine ait ciddi belirtilerin ortaya çıkması veya şiddet olayları sebebiyle kamu düzeninin ciddi şekilde bozulması halleri"

olağanüstü hâl ilan edilme sebepleri olarak öngörülmüştür. Anayasa'nın 119. maddesinde düzenlenen olağanüstü hâl, Cumhurbaşkanının başkanlığında toplanan Bakanlar Kurulunca ilan edilebilirken 120. maddesinde düzenlenen olağanüstü hâl, Cumhurbaşkanının başkanlığında toplanan Bakanlar Kurulunca Millî Güvenlik Kurulunun da görüşü alındıktan sonra ilan edilebilmektedir.

6. Anayasa'nın mülga 121. maddesinin üçüncü fıkrasında "Olağanüstü hal süresince, Cumhurbaşkanının başkanlığında toplanan Bakanlar Kurulu, olağanüstü halin gerekli kıldığı konularda, kanun hükmünde kararnameler çıkarabilir. Bu kararnameler, Resmî Gazetede yayımlanır ve aynı gün Türkiye Büyük Millet Meclisinin onayına sunulur; bunların Meclisce onaylanmasına ilişkin süre ve usul, İçtüzükte belirlenir" denilmektedir. Anılan hüküm uyarınca, olağanüstü hâllerde Cumhurbaşkanının başkanlığında toplanan Bakanlar Kurulu, olağanüstü hâlin gerekli kıldığı konularda kanun hükmünde kararname (KHK) çıkarma yetkisine sahiptir.

7. Anayasa'nın mülga 91. maddesinin birinci fıkrasında, sıkıyönetim ve olağanüstü hâller saklı kalmak üzere Anayasa'nın ikinci kısmının birinci ve ikinci bölümlerinde yer alan temel haklar, kişi hakları ve ödevleri ile dördüncü bölümünde yer alan siyasi haklar ve ödevlerin KHK'larla düzenlenemeyeceği belirtilmekte iken sıkıyönetim ve olağanüstü hâllerde, söz konusu hak ve ödevler yönünden de KHK ile düzenleme yapılmasına bir engel bulunmamaktadır.

8. Anayasa'nın mülga 121. ve 122. maddelerinin üçüncü fıkralarında da olağanüstü hâl ve sıkıyönetim hâlinin gerekli kıldığı konularda çıkarılan KHK'ların Resmî Gazete'de yayımlandıkları gün TBMM'nin onayına sunulacağı, bunların TBMM tarafından onaylanmasına ilişkin süre ve usulün İçtüzük'te belirleneceği öngörülmüştür. TBMM İçtüzüğü'nün 128. maddesinin 9/10/2018 tarihli ve 1200 sayılı Karar'la değiştirilmeden önceki hâline göre "Anayasanın 121 ve 122 nci maddeleri gereğince çıkarılan ve Türkiye Büyük Millet Meclisine sunulan kanun hükmünde kararnameler, Anayasanın ve İçtüzüğün kanun tasarı ve tekliflerinin görüşülmesi için koyduğu kurallara göre ancak, komisyonlarda ve Genel Kurulda diğer kanun hükmünde kararnamelerle, kanun tasarı ve tekliflerinden önce, ivedilikle en geç otuz gün içinde görüşülür ve karara bağlanır./ Komisyonlarda en geç yirmi gün içinde görüşmeleri tamamlanmayan kanun hükmünde kararnameler Meclis Başkanlığınca doğrudan doğruya Genel Kurul gündemine alınır" Söz konusu maddede, olağanüstü dönem KHK'larının da olağan dönem KHK'ları gibi komisyonlarda ve Genel Kurulda öncelikle ve ivedilikle görüşüleceği hükme bağlanmakla birlikte olağan dönem KHK'larından farklı olarak öncelikle ve ivedilikle görüşülme hususu, birtakım sürelerle bağlanarak somutlaştırılmıştır.

B. Olağanüstü Hâl Düzenlemelerinin Yargısal Denetimi

9. Anayasa'nın 6771 sayılı Kanun'la değiştirilmeden önceki 148. maddesinin birinci fıkrasının üçüncü cümlesinde "...olağanüstü hallerde, sıkıyönetim ve savaş hallerinde çıkarılan kanun hükmünde kararnamelerin şekil ve esas bakımından Anayasaya aykırılığı iddiasıyla, Anayasa Mahkemesinde dava açılmaz" hükmüne yer verilerek olağanüstü dönem KHK'ları Anayasa Mahkemesinin yargısal denetiminin dışında bırakılmıştır. Anayasa Mahkemesi 2/11/2016 tarihli ve E.2016/171, K.2016/164 sayılı kararında olağanüstü hâl KHK'larının Anayasa Mahkemesi tarafından denetlenebilmesi için bu yöndeki bir anayasal yetkinin açıkça tanınması gerektiğini ifade ederek Anayasa'nın 148. maddesinin lafzı, Anayasa koyucunun amacı ve ilgili yasama belgeleri gözönünde bulundurulduğunda olağanüstü hâl KHK'larının herhangi bir ad altında yargısal denetiminin mümkün olmadığına karar vermiştir.

10. Bununla birlikte olağanüstü hâl KHK'larının TBMM tarafından onaylanarak kanunlaşması hâlinde bu kanun hükümlerinin Anayasa'ya aykırılığı iddiasıyla Anayasa Mahkemesinde dava açılmasının önünde bir engel bulunmamaktadır. İptal davasına konu edilen 6757 sayılı Kanun, olağanüstü hâl kapsamında çıkarılan 671 sayılı KHK'nın TBMM tarafından onaylanması sonucunda yürürlüğe girmiştir. Bu itibarla dava konusu kurallar diğer kanun hükümleri gibi Anayasa Mahkemesinin denetimine tabi olmakla birlikte bu denetim yapılırken söz konusu kuralların olağanüstü hâle yönelik düzenlemeler içermesi nedeniyle öncelikle inceleme yönteminin belirlenmesi gerekir.

11. Anayasa, temel hak ve özgürlüklerin korunmasına ilişkin olarak olağan ve olağanüstü dönemler için iki ayrı hukuki rejim öngörmektedir. Olağan dönemde temel hak ve özgürlüklerin sınırlanması rejimi Anayasa'nın 13. maddesinde düzenlenmişken olağanüstü dönemde temel hak ve özgürlüklerin sınırlandırılması ya da kullanılmasının durdurulması rejimi Anayasa'nın 15. maddesinde düzenlenmiştir.

12. Anayasa'nın 13. maddesine göre "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz."

13. Anayasa'nın 15. maddesine göre ise "Savaş, seferberlik veya olağanüstü hallerde, milletlerarası hukuktan doğan yükümlülükler ihlâl edilmemek kaydıyla, durumun gerektirdiği ölçüde temel hak ve hürriyetlerin kullanılması kısmen veya tamamen durdurulabilir veya bunlar için Anayasada öngörülen güvencelere aykırı tedbirler alınabilir./ Birinci fıkrada belirlenen durumlarda da, savaş hukukuna uygun fiiller sonucu meydana gelen ölümler dışında, kişinin yaşama hakkına, maddî ve

manevî varlığının bütünlüğüne dokunulamaz; kimse din, vicdan, düşünce ve kanaatlerini açıklamaya zorlanamaz ve bunlardan dolayı suçlanamaz; suç ve cezalar geçmişe yürütülemez; suçluluğu mahkeme kararı ile saptanıncaya kadar kimse suçlu sayılamaz.”

14. Olağan dönemde temel hak ve özgürlüklerin sınırlandırılmasına ilişkin ölçütler Anayasa'nın 13. maddesinde yer alırken savaş, seferberlik ve olağanüstü hâllerde hak ve özgürlüklerin sınırlandırılması, hatta kullanılmasının durdurulması özel olarak Anayasa'nın 15. maddesinde düzenlenmiştir. Buna göre savaş, seferberlik veya olağanüstü hâllerde temel hak ve özgürlüklerin kullanılmasının kısmen veya tamamen durdurulması ve bunlar için Anayasa'nın diğer maddelerinde öngörülen güvencelere aykırı tedbirler alınması mümkündür. Ancak Anayasa'nın 15. maddesiyle bu hususta tanınan yetki de sınırsız değildir. Anayasa'nın diğer maddelerinde öngörülen güvencelere aykırı tedbirlerin milletlerarası hukuktan doğan yükümlülükleri ihlal etmemesi ve durumun gerektirdiği ölçüde olması gerekmektedir. Ayrıca bu durumlarda dahi kişinin yaşam hakkına, maddi ve manevi varlığının bütünlüğüne dokunulması, din, vicdan, düşünce ve kanaatlerini açıklamaya zorlanması ve bunlardan dolayı suçlanması yasaklanmış; suç ve cezaların geriye yürümemesi ilkesi ile masumiyet karinesinin bu hâllerde de geçerli olduğu kabul edilmiştir.

15. Olağanüstü hâl yönetim usullerine başvurulmasındaki temel amaç, bu yönetim rejiminin uygulanmasına neden olan tehdit veya tehlikelerin bertaraf edilmesini sağlamaktır. Devletin veya toplumun varlığının ya da kamu düzeninin ağır tehdit veya tehlikeler altında bulunması nedeniyle olağanüstü yönetim usulünün uygulandığı dönemlerde, söz konusu tehdit veya tehlikelerin bertaraf edilmesi için temel hak ve özgürlüklerin olağan döneme kıyasla daha fazla sınırlandırılması sonucunu doğuran tedbirler alınması gerekebilir. Bu nedenle Anayasa'nın 15. maddesinin uygulanabilmesi için kuralın olağanüstü hâlin gerekli kıldığı durumla ilgisinin bulunması gerekir.

16. Olağanüstü hâl KHK'larının kanunlaşmasından sonra bu kanun hükümlerinin Anayasa'ya uygunluğunun denetlenmesinde ilgili kuralın tabi olduğu sınırlama rejimi tespit edilmelidir. Zira söz konusu düzenlemelerde olağanüstü hâle ilgili kuralların yanında olağanüstü hâle ilgisi olmayan kurallara da yer verilebilmesi bu tespitin yapılmasını zorunlu kılmaktadır.

17. Kanunlaştırılarak yargısal denetime açılan bir kuralın Anayasa'nın olağanüstü dönem için öngördüğü denetim rejimine tabi olabilmesi için kural, olağanüstü hâlin ilanına sebep olan tehdit veya tehlikelerin bertaraf edilmesine yönelik olmalı ve olağanüstü hâl süresiyle sınırlı uygulanmalıdır. Dolayısıyla ancak bu iki niteliği taşıyan bir kuralın Anayasa'ya uygunluk denetiminde olağanüstü hâllerde temel hak ve özgürlüklerin kullanılmasının sınırlandırılmasını ve durdurulmasını düzenleyen Anayasa'nın 15. maddesi esas alınabilir.

18. Kuralın olağanüstü hâlin ilanına neden olan tehdit veya tehlikelerin bertaraf edilmesine yönelik olmadığı ya da olağanüstü hâlin süresini aştığı durumlarda ise söz konusu kuralın Anayasa'ya uygunluk denetiminde Anayasa'nın 15. maddesi dikkate alınamaz. Bu durumda kurala ilişkin inceleme sınırlamaya konu hakkın düzenlendiği Anayasa maddesi başta olmak üzere Anayasa'nın ilgili hükümleri ile olağan dönemde hak ve özgürlükleri sınırlama ve güvence rejimi bakımından temel öneme sahip olan Anayasa'nın 13. maddesi bağlamında yapılmalıdır. Ancak buradaki anayasallık denetiminde varılan sonuç böyle bir düzenlemenin olağanüstü dönemde dahi yapılamayacağı şeklinde anlaşılabilir.

19. Temel hak ve özgürlüklerle ilgili olağanüstü hâl kurallarının anayasallık denetiminde Anayasa'nın 15. maddesinde üç ayrı ölçüt öngörülmüştür. Bu ölçütlerden ilki anılan maddenin ikinci fıkrasında sayılan ve çekirdek alan olarak da ifade edilen temel hak ve özgürlüklere dokunma yasağıdır. Buna göre olağanüstü dönemde de olsa savaş hukukuna uygun fiiller sonucu meydana gelen ölümler dışında kişinin yaşama hakkına, maddi ve manevi varlığının bütünlüğüne dokunulamaz; kimse din, vicdan, düşünce ve kanaatlerini açıklamaya zorlanamaz ve bunlardan dolayı suçlanamaz; suç ve cezalar geçmişe yürütülemez; suçluluğu mahkeme kararı ile saptanıncaya kadar kimse suçlu sayılamaz.

20. Anayasa'nın 15. maddesinde yer alan ikinci ölçüt kuralların milletlerarası hukuktan doğan yükümlülüklerle aykırı olmamasıdır. Bu yükümlülüklerin başında taraf olunan insan haklarına ilişkin uluslararası sözleşmelerden doğan yükümlülükler gelmektedir.

21. İnsan hakları alanında Türkiye'nin taraf olduğu uluslararası sözleşmelerin başında Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme (MSHUS) ve Avrupa İnsan Hakları Sözleşmesi (AİHS) gelmektedir. MSHUS'un 4. ve AİHS'in 15. maddelerine göre milletin yaşamını tehdit eden olağanüstü bir durum meydana geldiğinde devletler, bu sözleşmelerdeki yükümlülüklerini azaltacak tedbirler alabilirler. Ancak MSHUS'un 4. maddesinin (2) numaralı fıkrasında; AİHS'in 15. maddesinin (2) numaralı fıkrasında, AİHS'e ek 7 No.lu Protokol'ün 4., 6 No.lu Protokol'ün 3. ve 13 No.lu Protokol'ün 2. maddelerinde yükümlülük azaltılması mümkün olmayan bazı hak ve özgürlüklere yer verilmiştir. Bunlardan önemli bir kısmı, Anayasa'nın 15. maddesinin ikinci fıkrasında da yer almaktadır. Dolayısıyla bu haklar yönünden yapılacak ikinci inceleme kapsamında Anayasa, MSHUS ve AİHS'te yer alan yükümlülük azaltılması mümkün olmayan ortak hak ve özgürlükler yönünden ayrı bir değerlendirme yapmaya gerek bulunmamaktadır.

22. Bununla birlikte MSHUS'un 4. maddesinin (2) numaralı fıkrası ile AİHS'in 15. maddesinin (2) numaralı fıkrası ve AİHS'e ek 7 No.lu Protokol'ün 4. maddesinde, Anayasa'nın 15. maddesinde yer

almayan bazı hak ve özgürlüklerin de yükümlülük azaltılmasına konu olamayacağı düzenlenmiştir. Buna göre olağanüstü durumlarda da hiç kimse köle veya kul olarak tutulamaz, yalnızca sözleşmeden doğan yükümlülüklerini yerine getiremediği gerekçesiyle hapsedilemez ve kesin bir hükümle mahkûm edildiği ya da beraat ettiği bir suçtan dolayı yeniden yargılamaz veya cezalandırılmaz. Ayrıca bu dönemde de herkes her yerde, hukuk önünde kişi olarak tanınma hakkına sahiptir. Son olarak olağanüstü dönemde alınacak tedbirlerin ırk, renk, cinsiyet, dil, din, toplumsal köken gibi sebeplerle ayrımcılık içermemesi gerekir. Bu nedenle belirtilen hak ve özgürlükler Anayasa'nın 15. maddesinde sayılan çekirdek haklar arasında yer almasa da anılan hak ve özgürlükleri sınırlayan tedbirler, milletlerarası hukuktan kaynaklanan yükümlülüklerle bağdaşmayacağından meşru görülemez. Dolayısıyla bu haklara ilişkin düzenlemelerde sözü edilen sözleşme hükümlerinin gözetileceği tabiidir.

23. Anayasa'nın 15. maddesinde yer alan üçüncü ölçüt ise olağanüstü hâl döneminde temel hak ve özgürlükleri sınırlayan kuralların durumun gerektirdiği ölçüde olmasıdır. Anılan maddedeki ölçülülük olağanüstü yönetim usulünün uygulanmasına neden olan durum karşısında ölçülülüğü ifade etmektedir. Dolayısıyla Anayasa'nın 15. maddesinde belirtilen ölçülülük, Anayasa'nın 13. maddesindeki ölçülülük kriterine göre temel hak ve özgürlükleri daha fazla sınırlamaya izin vermektedir.

24. Anayasa'nın 15. maddesinde yer alan ölçülülük ilkesi, temel hak ve özgürlüklerin kullanılmasının sınırlandırılması veya durdurulması için başvuru aracının amacı gerçekleştirmeye elverişli ve bunun için gerekli olmasını, ayrıca araçla amacın ölçülü bir oran içinde bulunmasını ifade etmektedir. Buna göre tedbir, olağanüstü durumu oluşturan tehdit veya tehlikelerin ortadan kaldırılması amacına ulaşma bakımından elverişli ve bu amacın gerçekleşmesi için gerekli olmalı; ayrıca tedbire konu temel hak ve özgürlüklere yönelik sınırlama durumun gerektirdiği oranda olmalıdır. Bir başka deyişle alınan tedbirle temel hak ve özgürlüklere getirilen sınırlama durumun gerektirdiği oranı aşarak keyfi niteliğe dönüşmemelidir.

25. Ölçülülüğün tespitinde tedbirin alındığı dönemin tüm koşulları birlikte değerlendirilmelidir. Bu kapsamda olağanüstü dönemde temel hak ve özgürlüklere yönelik sınırlama teşkil eden tedbirin ölçülülüğüne ilişkin unsurlar değerlendirilirken olağanüstü yönetim usulünün uygulanmasına neden olan tehdit veya tehlikeler, sınırlamaya konu hak ve özgürlüğün niteliği ve tedbirin alındığı zamanın da gözönünde bulundurulması gerekir.

26. Son olarak Anayasa'nın 15. maddesinde, olağanüstü dönemlerde temel hak ve özgürlüklere yönelik olarak Anayasa'da öngörülen güvencelere aykırı tedbirler alınması dışında temel hak ve

özgürlüklerin kullanılmasının kısmen veya tamamen durdurulabilmesine de izin verilmiştir. Ancak buradaki durdurma kavramı o hakkın tamamen kullanılamaz hâle gelmesi değil, onun kullanımının geçici olarak askıya alınması anlamına gelmektedir. Kuşkusuz temel hak ve özgürlüklerin kullanılmasının durdurulması niteliğindeki tedbirler de ölçülülük ilkesinin yukarıda belirtilen esaslarına uygun olmalıdır.

27. Olağanüstü yönetim usulünün uygulandığı dönemde temel hak ve özgürlüklere yönelik sınırlamayı konu edinen kurallara ilişkin olarak Anayasa'nın 15. maddesinin uygulanması gerektiği durumlarda da bu maddeye ilişkin inceleme yapılmadan önce sınırlamaya konu hakkın düzenlendiği Anayasa maddesi başta olmak üzere Anayasa'nın ilgili hükümleri ve olağan dönemde hak ve özgürlükleri sınırlama ve güvence rejimini düzenleyen Anayasa'nın 13. maddesi kapsamında bir inceleme yapılmalıdır. Zira devletin veya toplumun varlığına ya da kamu düzenine yönelik ciddi tehdit veya tehlikelerin ortaya çıktığı olağanüstü durumlarda olağanüstü yönetim usullerine başvurulması, bu dönemde yürürlüğe konulan ve temel hak ve özgürlükleri sınırlandıran her düzenlemenin olağan dönemin izin verdiği ölçütlerin ötesinde olmasını gerektirmeyebilir. Anılan şekilde inceleme yapılması Anayasa'nın 15. maddesinde yer alan "... Anayasada öngörülen güvencelere aykırı tedbirler alınabilir" hükmünün de bir gereğidir. Nitekim Anayasa Mahkemesinin bireysel başvuru kapsamında bu konuya ilişkin olarak vermiş olduğu ilk karar olan Aydın Yavuz ve diğerleri kararında da aynı inceleme yöntemi benimsenmiştir (Aydın Yavuz ve diğerleri ([GK], B. No: 2016/22169, 20/6/2017, §§ 193-195).

28. Buna göre yapılan incelemede kuralın Anayasa'nın 15. maddesi dışındaki maddelerinde yer alan güvencelere aykırı olmadığı tespit edilmesi durumunda ayrıca Anayasa'nın 15. maddesi yönünden bir inceleme yapılmasına gerek kalmayacaktır. Zira Anayasa'nın 15. maddesi yönünden bir inceleme yapılabilmesi için öncelikle kuralın Anayasa'nın olağan dönem için öngördüğü güvencelere aykırılık taşıdığı tespit edilmesi gerekmektedir. Kuralın temel hak ve özgürlükler için Anayasa'da öngörülen güvencelere aykırı olduğu tespit edildiğinde ise bu kez sınırlamanın savaş, seferberlik veya olağanüstü hâl dönemlerinde temel hak ve özgürlüklerin kullanımının durdurulmasını ve sınırlandırılmasını düzenleyen Anayasa'nın 15. maddesine uygun olup olmadığı hususunda inceleme yapılacaktır.

29. Bununla birlikte Anayasa'da bazı temel hak ve özgürlüklerin olağanüstü dönemlerde sınırlandırılmasında farklılıklar bulunmaktadır. Bu kapsamda bazı temel hak ve özgürlüklerin sınırlandırılmasına ilişkin sebep ve koşullar ilgili maddede özel olarak somutlaştırılmıştır. Bu nedenle anılan nitelikteki temel hak ve özgürlüklere temas eden olağanüstü hâl kurallarının anayasallık

denetiminde Anayasa’da öngörülen güvencelere aykırı tedbirlerin alınıp alınmadığının tespiti bakımından ayrıca Anayasa’nın 13. maddesinde yer alan güvenceler yönünden bir inceleme yapılması gerekli değildir. Bu gibi düzenlemelerin anayasallık denetiminde doğrudan Anayasa’nın 15. maddesindeki ölçütlere uygunluğunun tespit edilmesi gerekir.

C. Kanun’un 7. Maddesiyle 1324 Sayılı Kanun’un 8. Maddesinin Değiştirilen Birinci Fıkrasının İncelenmesi

30. 2/7/2018 tarihli ve 703 sayılı KHK’nın 47. maddesi “31/7/1970 tarihli ve 1324 sayılı Genelkurmay Başkanının Görev ve Yetkilerine Ait Kanun yürürlükten kaldırılmıştır. İlgili Cumhurbaşkanlığı kararnamesi yürürlüğe girinceye kadar söz konusu Kanun hükümlerinin uygulanmasına devam edilir.” hükmünü içermektedir. Bu bağlamda 10/7/2018 tarihli ve 30474 sayılı Resmî Gazete’de yayımlanan 1 numaralı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi’nin 338. maddesinde Genelkurmay Başkanının görev ve yetkileri, aynı tarihli ve sayılı Resmî Gazete’de yayımlanan 3 numaralı Üst Kademe Kamu Yöneticileri ile Kamu Kurum ve Kuruluşlarında Atama Usûllerine Dair Cumhurbaşkanlığı Kararnamesi’nin 9. maddesinin (3) numaralı fıkrasında da Genelkurmay Başkanının atanma usulü ve görev süresi düzenlenmiştir. Anılan hükümler çerçevesinde dava konusu fıkranın uygulanma imkânı kalmamıştır.

31. Açıklanan nedenle konusu kalmayan fıkraya ilişkin iptal talebi hakkında karar verilmesine yer olmadığına karar vermek gerekir.

Ç. Kanun’un 22. Maddesiyle 5809 Sayılı Kanun’un 60. Maddesine Eklenen (11) Numaralı Fıkranın Birinci ve Üçüncü Cümlelerinin İncelenmesi

1. İptal Talebinin Gerekçesi

32. Dava dilekçesinde özetle; dava konusu kuralla Bilgi Teknolojileri ve İletişim Kurumuna verilen yetkinin son derece geniş olduğu, kişisel verilerin korunmasında ulusal ve uluslararası düzenlemeler ile Avrupa İnsan Hakları Mahkemesi içtihatlarında belirtilen kriterlerin kuralda bulunmadığı, kuralla kişisel verilere yapılan müdahalenin demokratik toplumun gerektirdiği şekilde ve ölçüde olmadığı, kişisel verilerin gizliliği ve güvenliğine ilişkin herhangi bir güvencenin bulunmadığı, bu itibarla hakkın özüne dokunduğu belirtilerek kuralın, Anayasa’nın 2., 13., 20. ve 90. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anlam ve Kapsam

33. Dava konusu kurullarla Bilgi Teknolojileri ve İletişim Kurumuna (Kurum) görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilme ve bunları değerlendirme, arşivlerden,

elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilme, bunlarla irtibat kurabilme ve bu kapsamda diğer gerekli önlemleri alabilme veya aldırabilme yetkisi tanınmış; Kurum tarafından istenen her türlü bilgi ve belge talebinin; ilgili bakanlık, kurum ve kuruluşlar tarafından gecikmeksizin yerine getirileceği hükme bağlanmıştır.

34. Kurumun görev ve yetkilerinin çerçevesi 5809 sayılı Kanun'un 6. maddesiyle belirlenmiştir. Anılan maddenin (1) numaralı fıkrasının (1) bendi uyarınca Kurum, elektronik haberleşmeyle ilgili olarak ihtiyaç duyacağı her türlü bilgi ve belgeyi kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden almak ve gerekli kayıtları tutmak görev ve yetkisine sahiptir.

35. Kanun'un 60. maddesinin dava konusu fıkrasından önceki fıkrasında da "Kurum, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır" hükmüne yer verilmek suretiyle Kuruma kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması görevi verilmiş ve bu kapsamda siber saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alma ve aldırma imkânı tanınmıştır.

36. Anılan maddenin iptal davasına konu olan kuralların da yer aldığı fıkrası ise "Kurum, görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilir ve değerlendirmesini yapabilir; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilir, bunlarla irtibat kurabilir ve bu kapsamda diğer gerekli önlemleri alabilir veya aldırabilir. Kurum, bu fıkroda belirtilen görevlerin ifasında bakanlıklar, kurum ve kuruluşlar ile işbirliği içerisinde çalışır. Bu kapsamda Kurum tarafından istenen her türlü bilgi ve belge talebi; ilgili bakanlık, kurum ve kuruluşlar tarafından gecikmeksizin yerine getirilir. Bu fıkraya göre bilgi ve belge talebinde bulunulması ve bu taleplerin yerine getirilmesine ilişkin usul ve esaslar ile diğer hususlar Başbakanlıkça belirlenir." şeklindedir.

37. Dava konusu fıkradan sonraki fıkroda da "Gerçek kişiler ile özel hukuk tüzel kişileri, Kurumun bu maddedeki görevleri ile ilgili taleplerini, tabi oldukları mevzuat hükümlerini gerekçe göstermek suretiyle yerine getirmekten kaçınamazlar" demek suretiyle Kurumun anılan maddedeki görevleriyle ilgili taleplerin yerine getirilmesinin zorunlu olduğu hüküm altına alınmıştır.

38. Kuralların anlam ve kapsamının belirlenmesinde yukarıda belirtilen kuralların bir bütün olarak gözönünde bulundurulması gerekmektedir. Bu itibarla anılan maddede Kuruma siber güvenliği sağlama görevi verildikten sonra söz konusu hükmü izleyen fıkroda Kurumun "...görevi kapsamında..." ilgili yerlerden bilgi, belge, veri ve kayıtları alabilmesinin, değerlendirmesini yapabilmesinin, arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından

yararlanabilmesinin, bunlarla irtibat kurabilmesinin ve bu kapsamda diğerk gerekli önlemleri alabilmesinin veya aldırabilmesinin öngörölmüş olması karşısında Kuruma tanınan bu yetki ve imkânların Kurumun siber güvenliđin sađlanması göreviyle sınırlı olduđu anlaşılmaktadır.

39. Öte yandan aynı maddenin dava konusu kuralların bulunduđu fıkrasını izleyen fıkrasında da Kurumun anılan maddedeki görevleriyle ilgili taleplerinin yerine getirilmesinin zorunlu olduđu hükme bağlanırken "...bu maddedeki görevleri ile ilgili..." ibaresine yer verilmek suretiyle siber güvenliđin sađlanması görevinin verildiđi hükme atıfta bulunulmuş olması da dava konusu kuralların yukarıda belirtilen anlam ve kapsamını teyid etmektedir.

40. Kanun'un 6. maddesinin (1) numaralı fıkrasının (ı) bendine göre Kurumun elektronik haberleşmeyle ilgili olarak her türlü bilgiyi ilgili yerlerden toplama yetkisine sahip olduđunun ayrıca hükme bağlandıđı da (§ 37) gözetildiđinde kurallar uyarınca öngörölen yetki ve imkânların siber güvenliđin sađlanması görevi kapsamında tanındıđı netlik kazanmaktadır.

3. Anayasa'ya Aykırılık Sorunu

41. Bir kuralın Anayasa'nın olađanüstü dönem için öngördüđü denetim rejimine tabi olabilmesi için kuralın olađanüstü hâlin gerekli kıldıđı durumla ilgili olması gerekmektedir. Buna göre kural, olađanüstü hâlin ilanına sebep olan tehdit veya tehlikelerin bertaraf edilmesine yönelik olmalı, bunun yanı sıra olađanüstü hâl süresiyle sınırlı olarak uygulanmalıdır.

42. Dava konusu kuralların olađanüstü hâlin ilanına neden olan tehdit veya tehlikelerin bertaraf edilmesine yönelik olduđu anlaşılmaqla birlikte olađanüstü hâl süresiyle sınırlı olarak uygulanma özelliđini aşan bir niteliđe sahip oldukları anlaşılmaktadır. Nitekim kurallar olađan dönemde geçerli olan bir kanunda deđişiklik yaptıđından sürekli bir etkiye sahiptir. Bu durum kurallara olađanüstü hâlin dışına taşan genel düzenleme niteliđi vermektedir. Bu nedenle kuralların anayasallık denetiminde Anayasa'nın olađanüstü hâllerde temel hak ve özgürlüklerin sınırlandırılması rejimini düzenleyen 15. maddesi uygulama alanı bulamaz. Kurallara ilişkin incelemenin, sınırlamaya konu hakkın düzenlendiđi Anayasa maddesi başta olmak üzere Anayasa'nın ilgili hükümleri ve elbette olađan dönemde hak ve özgürlükleri sınırlama ve güvence rejimi bakımından temel öneme sahip olan Anayasa'nın 13. maddesi bağlamında yapılması gerekir.

43. Anayasa'nın 2. maddesinde belirtilen hukuk devleti eylem ve işlemleri hukuka uygun, insan haklarına saygılı, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adil bir hukuk düzeni kurup bunu geliştirerek sürdüren, hukuki güvenliđi sađlayan, Anayasa'ya aykırı durum ve tutumlardan kaçınan, hukuk kurallarıyla kendini bađlı sayan ve yargı denetimine açık olan devlettir.

44. Hukuk devletinin temel ilkelerinden biri de belirliliktir. Bu ilkeye göre, yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olması, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi gereklidir. Belirlilik ilkesi, hukuksal güvenlikle bağlantılı olup, bu ilke gereği birey hangi somut eylem ve olguya hangi hukuksal yaptırımın veya sonucun bağlandığını, bunların hangi müdahale yetkisini doğurduğunu bilmelidir. Birey ancak bu durumda kendisine düşen yükümlülükleri öngörebilir ve davranışlarını belirler. Hukuk güvenliği, normların öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar.

45. Anayasa'nın 20. maddesinin birinci fıkrasında "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz" denilerek özel hayatın gizliliği hakkı güvence altına alınmıştır.

46. Aynı maddenin ikinci fıkrasında ise özel hayatın gizliliğine çeşitli sebeplere bağlı kalınarak sınırlamalar getirilebileceği belirtilerek bu hakkın mutlak olmadığı kabul edilmiştir. Maddede bu sınırlama sebepleri arasında millî güvenliğin ve kamu düzeninin korunması ile suç işlenmesinin önlenmesi sebepleri de sayılmış, böylece bunlara dayalı olarak anılan hakkın sınırlandırılabilmesine imkân tanınmıştır. Ancak 20. maddenin ikinci fıkrasında söz konusu sınırlandırmanın arama tedbirine özgü olarak yapılabileceği belirtildiğinden, bu sebepler 20. madde bağlamında dava konusu kural yönünden meşru bir sınırlandırma nedeni olarak kabul edilmeyebilir. Bununla birlikte, özel hayatın düzenlendiği maddede dava konusu kuralda belirtilen bilgi toplama yetkisi yönünden özel sınırlama sebeplerine yer verilmediğinin kabulü halinde dahi bu hakkın Anayasa'da güvence altına alınan diğer temel hak ve özgürlüklerin korunması veya Anayasa'nın diğer maddelerinde devlete bir görev olarak yüklenen millî güvenliğin, kamu düzeninin ve kamu güvenliğinin korunması gibi nedenlerle sınırlandırılması mümkündür.

47. Anılan maddenin üçüncü fıkrasında da herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı ifade edilmiştir. Fıkra da ayrıca kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir.

48. Özel hayatın gizliliği ve kişisel verilerin korunması hakkı, temel hak ve özgürlükler arasında önemli bir yer tutar. Özel hayatın gizliliğinin korunması, bu hayatın başkalarının gözleri önüne

serilmemesi demektir. Kişinin özel hayatının, yalnız kendisi veya kendisinin bilmesini istediği kimseler tarafından bilinmesini isteme hakkı, kişinin temel haklarından biridir ve bu niteliği nedeniyle insan haklarına ilişkin beyanname ve sözleşmelerde de yer almış; demokratik ülkelerin mevzuatında açıkça belirlenen istisnalar dışında devlete, topluma ve diğer kişilere karşı korunmuştur. Kişisel verilerin korunması hakkı ise özel hayatın gizliliği hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır.

49. Öte yandan kişisel verilerin korunması hakkı sınırsız olmayıp bu hakkın Anayasa'da güvence altına alınan diğer temel hak ve özgürlüklerin korunması veya Anayasa'nın devlete bir görev olarak yüklediği millî güvenliğin, kamu düzeninin ve kamu güvenliğinin korunması gibi nedenlerle sınırlandırılması mümkündür.

50. Ancak bu sınırlama yapılırken temel hak ve özgürlüklerin sınırlandırılması rejimini belirleyen Anayasa'nın 13. maddesine de uyulması gerekmektedir. Anayasa'nın 13. maddesinde "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz" denilmektedir. Anayasa'nın anılan maddesi uyarınca özel hayatın gizliliği ve kişisel verilerin korunması hakları, yalnızca kanunla ve demokratik bir toplumda gerekli olduğu ölçüde sınırlanabilir. Ayrıca getirilen bu sınırlamalar hakkın özüne dokunamayacağı gibi Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamaz.

51. Dokunulamayacak öz, her temel hak ve özgürlük açısından farklılık göstermekle birlikte kanunla getirilen sınırlamanın hakkın özüne dokunmadığının kabulü için temel hakların kullanılmasını ciddi surette güçleştirip amacına ulaşmasına engel olmaması ve etkisini ortadan kaldıracı bir nitelik taşımaması gerekir.

52. Anayasa'nın 13. maddesinde ifade edilen ölçülülük ilkesi, temel hak ve özgürlüklerin sınırlandırılmasına ilişkin başvurularda dikkate alınması gereken bir diğer ilkedir. Ölçülülük ilkesi elverişlilik, gereklilik ve orantılılık olmak üzere üç alt ilkeden oluşmaktadır. Elverişlilik öngörülen sınırlamanın ulaşılmak istenen amacı gerçekleştirmeye elverişli olmasını, gereklilik ulaşılmak istenen amaç bakımından sınırlamanın zorunlu olmasını diğer bir ifadeyle aynı amaca daha hafif bir sınırlama ile ulaşılmamasının mümkün olmamasını, orantılılık ise hakka getirilen sınırlama ile ulaşılmak istenen amaç arasında makul bir dengenin gözetilmesi gerekliliğini ifade etmektedir.

53. Buna göre kişisel verilerin korunması hakkının sınırlandırılması için seçilen aracın, öngörülen amaca ulaşılabilirliği bakımından elverişli olması gerekir. Ayrıca seçilen araç bu hakkı en az zedeleyici

nitelikte bulunmalıdır. Bununla birlikte hakkı daha az zedeleyen aracın tercih edilmesi gerektiğinin söylenebilmesi için söz konusu araç aynı amacı gerçekleştirmeye elverişli olmalıdır. Daha hafif sınırlama teşkil eden aracın tercih edilmesi hâlinde öngörülen amaç gerçekleşmeyecek ise daha ağır sınırlama oluşturan aracın seçimi hususundaki tercih, Anayasa'ya aykırı olmaz. Bunun dışında hangi sınırlama aracının tercih edileceği hususunda kanun koyucunun takdir yetkisi bulunmaktadır.

54. Kişisel verilerin korunması hakkına yönelik sınırlandırmalar orantılı da olmalıdır. Orantılılık, amaç ile araç arasında adil bir denge kurulmasını gerektirmektedir. Buna göre kişisel verilerin korunması hakkına getirilen sınırlamayla ulaşılmak istenen meşru amaç ve aleyhine anılan hakkı sınırlanan kişinin bu hakkın korunmasındaki bireysel yararı arasında makul bir orantı kurulmalıdır. Hedeflenen amaca ulaşıldığında elde edilecek kamusal yararlar kıyaslandığında, sınırlama ile kişiye yüklenen külfetin aşırı ve orantısız olmaması gerekir. Kişiye yüklenen külfetin aşırı olup olmadığının tespitinde kişinin hak ve menfaatleri üzerinde oluşturduğu tesir ve sınırlamanın gerekçesini oluşturan meşru amacın niteliği göz önünde bulundurulmalıdır.

55. Dava konusu kurallar, Kuruma, görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilme ve bunların değerlendirmesini yapabilme; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilme, bunlarla irtibat kurabilme ve bu kapsamda diğer gerekli önlemleri alabilme veya aldırabilme konularında yetki tanımakta ve bu kapsamda Kurum tarafından istenen her türlü bilgi ve belge talebinin ilgili bakanlık, kurum ve kuruluşlar tarafından gecikmeksizin yerine getirilmesini öngörmektedir. Kurumun yetki ve talebine konu bilgiler genel anlamda belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade eden kişisel veri kavramı kapsamındadır.

56. Bu itibarla kural yukarıda belirtilen kişisel veri niteliğinde olan bilgilerin, Kurum tarafından görevi kapsamında temin edilmesine imkân sağlamaktadır. Kurumun görevleri Kanun'un 6. maddesinde belirtilmiştir. Bununla birlikte Kanun'un 60. maddesinin (11), (12) ve (13) numaralı fıkraları gözetildiğinde söz konusu bilgi temininin, Kurumun siber güvenliği sağlama görevi kapsamında olanlarla sınırlı olduğu anlaşılmaktadır. Siber güvenliğin sağlanması gittikçe artan bir önem taşımaktadır. Zira gelişen teknolojiyle birlikte bilgilerin gizliliğini korumak zorlaşmakta, bu bilgilere ulaşılması millî güvenlik tehditlerinden büyük ekonomik krizlere ve önemli kişisel zararlara varana kadar birçok soruna neden olabilmektedir. Bu nedenle kanun koyucunun bu alanı düzenlemesinin millî güvenliğin, kamu düzeninin ve kamu güvenliğinin korunması yönünden bir zorunluluk olduğu söylenebilir. Kanun koyucunun söz konusu düzenlemeleri gerçekleştirirken kimi

kurum ve kuruluşları yetkilendirmesi ise takdir yetkisi kapsamındadır. Kuşkusuz bu takdir yetkisinin anayasal sınırlar içinde kullanılması gerekir.

57. Anayasa'nın 20. maddesinde, kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği belirtilmiştir. Dolayısıyla bu hakkı ilgilendiren yasal düzenlemelerin; çerçevesi çizilmiş, açık, anlaşılabilir ve kişilerin söz konusu haklarını kullanabilmelerine elverişli olması gerekir. Bunun yanı sıra bu düzenlemeler resmî makamların özel hayatı ilgilendiren veri, bilgi ve belgelere yönelik keyfi müdahalelerine karşı güvence sağlamalıdır. Aksi durumda kamu otoritesinin bireye ilişkin kişisel nitelikteki verilere anayasal güvenceye aykırılık oluşturacak şekilde sınırsız ve mutlak olarak müdahalesi mümkün hâle gelir. Bu bağlamda dava konusu kurallar, Kanun'un 6. maddesi ve 60. maddesinin mezkûr fıkralarıyla birlikte değerlendirildiğinde kişisel veri niteliğindeki bilgilerin temin edilmesindeki amacın, kapsamın ve sınırların Kanun'da açıkça belirlendiği anlaşılmaktadır. Dolayısıyla kuralların belirlilik ilkesiyle çeliştiği söylenemez.

58. Öte yandan kurallar kişisel verilerin korunması hakkına yönelik bir sınırlama getirmektedir. Kurullarla Kuruma verilen bilgileri temin edebilme yetkisinin, Kurumun kuruluş amacı ve faaliyet alanında yer alan siber güvenliğin sağlanması amacıyla sınırlı olarak kullanılabilmesi anlaşıldığından kuralların kişisel verilerin korunması hakkının kullanılmasını ciddi surette güçleştirip amacına ulaşmasını engellediği söylenemez. Dolayısıyla kural hakkın özüne dokunmamaktadır. Bu nedenle değerlendirilmesi gereken husus söz konusu sınırlamanın ölçülülük ilkesine uygun olup olmadığıdır.

59. Bilgi çağı olarak da adlandırılan çağımızda bilgi ve iletişim teknolojisinde büyük ilerlemeler yaşanmakta ve bu gelişmeler toplumu kuşatmaktadır. Bu ilerlemeye koşut olarak siber saldırı ve tehditlerin de artarak devam ettiği görülmektedir. Bu durum siber güvenlik ihtiyacının ortaya çıkmasına neden olmaktadır. Bireylerin güven içinde yaşamalarının sağlanmasında devlete yüklenen ödevler arasında şüphesiz siber güvenliğin sağlanması da yer almaktadır. Dolayısıyla siber güvenliğin sağlanmasının kamu güvenliğinin korunmasına yönelik olduğu anlaşılmaktadır.

60. Hedeflenen amacın gerçekleştirilmesi için kurullarla Kuruma ilgili yerlerden bilgi, belge, veri ve kayıtları alabilme ve değerlendirmesini yapabilme, arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilme, bunlarla irtibat kurabilme ve bu kapsamda diğer gerekli önlemleri alabilme ya da aldırabilme yetkisinin verilmesi ile Kurum tarafından istenen her türlü bilgi ve belge talebinin ilgilisi tarafından gecikmeksizin yerine getirilmesi hükme bağlanmıştır. Siber güvenliğin sağlanması amacıyla getirilen sınırlamanın anılan amaca ulaşmak bakımından gerekli ve elverişli olmadığı söylenemez. Kurumun bilgi temini yetkisinin siber güvenliğin sağlanması

göreviyle sınırlı olduğu ve kişisel bilgilerin gizliliğini ve işletmecilerin ticari sırlarını korumakla yükümlü kılınması dolayısıyla bu yetkisini keyfi olarak kullanmasını önleyecek güvencelerin de sağlanmış olduğu dikkate alındığında kuralların getirdiği sınırlamanın orantısız olduğu da söylenemez.

61. Açıklanan nedenlerle kurallar Anayasa'nın 2., 13. ve 20. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

Zühtü ARSLAN, Engin YILDIRIM ve Hasan Tahsin GÖKCAN bu görüşe katılmamışlardır.

Kuralın Anayasa'nın 90. maddesiyle ilgisi görülmemiştir.

D. Kanun'un 23. Maddesiyle 3201 Sayılı Kanun'un Ek 24. Maddesine Eklenen Üçüncü Fıkranın Birinci Cümlesinde Yer Alan "...Kamu Personel Seçme Sınavı şartı aranmaksızın,..." İbaresinin İncelenmesi

1. İptal Talebinin Gerekçesi

62. Dava dilekçesinde özetle; dava konusu kuralla özel harekât birimine alınacaklar için Kamu Personel Seçme Sınavı (KPSS) şartının aranmamasının öngörüldüğü, bu durumun hiçbir objektif liyakat ölçütünün kullanılmaması sonucunu doğuracağı ve objektif ölçütleri dışlayan, siyasi, şahsi ilişkilerin etkili olduğu keyfi tercih ve uygulamalara neden olabileceği belirtilerek kuralın Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

63. 3201 sayılı Kanun'un ek 24. maddesinin üçüncü fıkrasının birinci cümlesinde özel harekât birimlerinde istihdam edilmek üzere, yirmi sekiz yaşından gün almamış olan, en az lise veya dengi okul mezunlarının KPSS şartı aranmaksızın, fiziki yeterlilik ve mülakat sınavları ile polis meslek eğitim merkezlerine alınabileceği belirtilmiş olup söz konusu cümlede yer alan "...Kamu Personel Seçme Sınavı şartı aranmaksızın,..." ibaresi dava konusu kuralı oluşturmaktadır.

64. Olağanüstü hâl kapsamında alınan tedbirler uyarınca çok sayıda kamu görevlisi meslekten ihraç edilmiştir. Meslekten ihraç edilen kamu görevlileri arasında güvenlik görevlileri de bulunmaktadır. Bu bağlamda söz konusu kuralın olağanüstü hâlin ilanına neden olan tehdit veya tehlikelerin bertaraf edilmesine yönelik olduğu söylenebilir. Ancak kural olağan dönemde geçerli olan bir kanunda değişiklik yaptığından sürekli bir etkiye sahiptir. Bu durum kurala olağanüstü hâlin dışına taşan genel düzenleme niteliği vermektedir. Bu nedenle anayasal denetimin Anayasa'nın olağan hukuk düzeni yönünden öngördüğü kurallar çerçevesinde yapılması gerekir.

65. Kanunların kamu yararının sağlanması amacına yönelik olması, genel, objektif, adil kurallar içermesi ve hakkaniyet ölçütlerini gözetmesi hukuk devleti olmanın gereğidir. Bu nedenle kanun koyucunun hukuki düzenlemelerde kendisine tanınan takdir yetkisini anayasal sınırlar içinde adalet, hakkaniyet ve kamu yararı ölçütlerini göz önünde tutarak kullanması gerekir.

66. Anayasa'ya uygunluk denetiminde kanun koyucunun kamu yararı anlayışının isabetli olup olmadığı değil, incelenen kuralın kamu yararı dışında belli bireylerin ya da grupların çıkarları gözetilerek yasalaştırılmış olup olmadığı incelenebilir.

67. Dava konusu kuralda öngörülen düzenleme, özel harekât biriminde istihdam edilecek adayların tümü için geçerli, soyut ve genel hüküm niteliğindedir. Bunun yanı sıra kanun koyucu kural ile terörle mücadelede etkinliği artırmayı hedeflediğini kuralın gerekçesinde "...terörle mücadelede etkinliği artırmak amacıyla, en az lise ve dengi okul mezunu, yirmisekiz yaşından gün almamış ve askerlik hizmetini tamamlamış isteklilerin fiziki yeterlilik ve mülakat sınavları ile polis meslek eğitimi merkezlerine alınması düzenlenmektedir" demek suretiyle ortaya koymuştur. Dolayısıyla kuralın kamu yararı amacı dışında bir amaçla getirildiği söylenemez.

68. Belirli yaş ve eğitim koşulunu taşıyanlar, fiziki yeterlilik ve mülakat sınavlarında başarılı olmaları hâlinde kural uyarınca KPSS şartı aranmaksızın polis meslek eğitim merkezlerine alınabileceklerdir. Polis meslek eğitim merkezlerine alınan kişiler, öğrenci statüsünde olup bunların kamu görevlisi olarak kabul edilmeleri mümkün değildir. Bu kişilerin polis memuru olarak atanmaları, polis meslek eğitim merkezindeki eğitimlerini başarıyla tamamlamalarına bağlı olduğundan atandıkları tarih itibarıyla kamu görevlisi statüsünü kazanmaları söz konusu olacaktır. Kural kapsamındaki kişilerin kamu görevlisi olmadığı ve özel harekât biriminde görevli polislerce icra edilen görevin özelliği dikkate alındığında, bu birimde görev yapacaklara ilişkin olarak polis memurluğuna atanma öncesi dönem bakımından getirilen kuralla özel harekât birimince yerine getirilen görevin gerektirdiği niteliklere uygun öğrenci alınmasının amaçlandığı anlaşılmaktadır. Söz konusu görevin niteliklerinin gözönünde bulundurulduğu anlaşılan kurala göre ancak belirli bir eğitim koşulunu sağlayanların bu kapsamda başvuru yapabileceği, başvuran kişilerin de bilgi ve liyakatlerinin kuralın öngördüğü fiziki yeterlilik ve mülakat sınavlarıyla değerlendirilmesinin mümkün kılındığı gözetildiğinde kuralın keyfi tercih ve uygulamalara yol açtığı söylenemez. Bu yönüyle daha sonra özel harekât biriminde istihdam edilmek üzere öğrenci statüsü ile polis meslek eğitim merkezine alınacak kişilerin belirlenmesinde KPSS koşulu aranmamasında adalet ve hakkaniyet ölçütlerine aykırı düşen bir yön bulunmamaktadır.

69. Açıklanan nedenlerle kural Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

Hasan Tahsin GÖKCAN, Serdar ÖZGÜLDÜR ve Recep KÖMÜRÇÜ bu görüşe katılmamışlardır.

E. Kanun'un 25. Maddesiyle 2576 Sayılı Kanun'a Eklenen Geçici 21. Maddenin İncelenmesi

1. İptal Talebinin Gerekçesi

70. Dava dilekçesinde özetle; yargı erkinin hukuk devletinin sağlanmasında en önemli fonksiyonu yerine getirdiği, getirilen düzenlemenin bölge idare mahkemesi üyeliğine liyakate ve objektif kriterlere göre atama yapılmasını öngören 2576 sayılı Kanun'daki kuralların terk edilmesine neden olduğu, kuralda yer alan üstün başarı koşulunun kim tarafından ve hangi kriterlere göre belirleneceğinin somut olmadığı, bu nedenle atamalarda sübjektif bir değerlendirmenin öne çıkacağı, bu durumun ise mahkemelerin bağımsızlığı ve hâkimlik teminatı ilkelerini zedelediği, denetim muhakemesinin hak arama hürriyetinin içinde yer aldığı, bu nedenle denetim muhakemesini yapacak hâkimlerin kıdemsiz ve düşük bir liyakat derecesine sahip olmasının hak arama hürriyetini işlevsiz kılacağı belirtilerek kuralın Anayasa'nın 2., 36., 138., 139. ve 140. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

71. Dava konusu kuralla 31/12/2020 tarihine kadar bölge idare mahkemesi üyeliğine, hâkimlik ve savcılık mesleğinde fiilen en az altı yıl görev yapmış ve üstün başarısı ile bölge idare mahkemesinde yararlı olacağı anlaşılmış bulunan idarî yargı hâkim ve savcıları arasından atama yapılabilmesi öngörülmektedir.

72. Olağanüstü hâl kapsamında alınan tedbirler uyarınca çok sayıda adli yargı hâkimi ve Cumhuriyet savcısı ile idari yargı hâkim ve savcıları meslekten ihraç edilmiştir. Bu bağlamda söz konusu kuralın olağanüstü hâlin ilanına neden olan tehdit veya tehlikelerin bertaraf edilmesiyle ilişkili olduğu söylenebilir. Zira anılan mesleklerden yapılan ihraçların -hâkim ve Cumhuriyet savcısı sayıları dikkate alındığında- üst mahkemelerde görev almak için aranan meslek kıdeminin azaltılmasını gerekli kıldığını söylemek mümkündür. Ancak kural olağan dönemde geçerli olan kanunda değişiklik yaptığından olağanüstü hâlin süresini aşar niteliktedir. Bu nedenle anayasal denetimin Anayasa'nın olağan hukuk düzeni yönünden öngördüğü kurallar çerçevesinde yapılması gerekir.

73. Anayasa'nın 36. maddesinin birinci fıkrasında "Herkes, meşru vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir" denilerek yargı organlarına davacı ve davalı olarak başvurabilme hakkı ve bunun doğal sonucu olarak da iddia, savunma ve adil yargılanma hakkı güvence altına alınmıştır.

74. Hukuk devleti ilkesinin temel bileşenlerinden olan yargı bağımsızlığı, insan hakları ve özgürlüklerinin başlıca ve en etkin güvencesidir. Mahkemelerin bağımsızlığı, genellikle hâkimlerin bağımsızlığı kavramı ile eş anlamlı olarak kullanılmakta ve biri diğerinin nedeni ve doğal sonucu olarak anlaşılmaktadır.

75. Anayasa'nın 9. maddesinde yargı yetkisinin bağımsız mahkemelerce kullanılacağı açıkça hükme bağlanmış; 138. maddesinde ise mahkemelerin bağımsızlığından ne anlaşılması gerektiği açıklanmıştır. Buna göre "Hiçbir organ, makam, merci veya kişi, yargı yetkisinin kullanılmasında mahkemelere ve hâkimlere emir ve talimat veremez; genelge gönderemez; tavsiye ve telkinde bulunamaz." Anılan maddeye göre bağımsızlık, mahkemenin bir uyuşmazlığı çözümlerken hiçbir organ, makam, merci veya kişinin etkisi altında olmamasını ifade etmektedir.

76. Hâkim ve savcıların atanmasına ve diğer özlük haklarına ilişkin görevlerin bağımsız bir organa verilmesi yargı bağımsızlığının ön koşuludur. Anayasa'nın 159. maddesinin sekizinci fıkrasında hâkim ve savcıların atanma ve yer değiştirmesinde yetkili merciin Hâkimler ve Savcılar Kurulu (HSK) olduğu belirtilerek bu konuda HSK'ya anayasal bir yetki tanınmıştır. Böylece derece mahkemeleri ile yüksek mahkemelerde görev yapan hâkim ve savcılar arasında bir ayırım gözetilmeksizin tüm hâkim ve savcıların atanması ve yer değiştirmesinde münhasıran HSK yetkili kılınmıştır. Dolayısıyla 2576 sayılı Kanun'da aranan şartlara sahip olan hâkim ve savcılar bölge idare mahkemesi üyeliğine atama yetkisi HSK'ya ait olduğu gibi bu görevden başka bir göreve atama yetkisi de yine HSK'ya aittir.

77. Diğer taraftan Anayasa'nın 139. maddesinde hâkimlik ve savcılık teminatına ilişkin hükümlere yer verilmiş, 140. maddesinde ise hâkim ve savcıların atanma ve yer değiştirmelerinde uygulanacak usul ve esasların mahkemelerin bağımsızlığı ve hâkimlik teminatı esaslarına göre kanunla düzenleneceği hüküm altına alınmıştır. Bu kapsamda, idarî yargıda görev yapan hâkim ve savcıların bölge idare mahkemelerine veya bu görevden başka bir göreve atanmalarında HSK yetkili olup bunun usul ve esaslarını belirleme yetkisi kanun koyucuya aittir.

78. Kural, belirli bir tarihe kadar bölge idare mahkemesi üyeliğine atanacak olan hâkim ve savcıların belirlenmesinde HSK'ya bir takdir yetkisi tanımaktadır. Hâkim ve savcıların hangi koşullar altında birinci sınıfa ayrılacağı ya da sınıf ve kıdemlerinin nasıl belirleneceği 24/2/1983 tarihli ve 2802 sayılı Hakimler ve Savcılar Kanunu'nda belirlenmiştir. 2576 sayılı Kanun'un 3/E maddesinin birinci fıkrasına göre bölge idare mahkemesi üyeleri, en az birinci sınıfa ayrılmış olup birinci sınıfa ayrılmayı gerektiren nitelikleri yitirmemiş idari yargı hâkim ve savcılar arasından HSK'ca atanır. Kural, birinci sınıfa ayrılmış hâkim veya savcı olma koşulunu sağlayan idarî yargı hâkim ve savcılarının yanı sıra 31/12/2020 tarihine kadar hâkimlik ve savcılık mesleğinde fiilen en az altı yıl görev yapmış ve üstün

başarısı ile bölge idare mahkemesinde yararlı olacağı anlaşılmış bulunan idarî yargı hâkim ve savcılarının da bölge idare mahkemesi üyeliklerine atanabilmelerine imkân sağlamaktadır. Bu itibarla kural, bölge idare mahkemesi üyeliklerine atama veya bu görevden alma konusunda HSK'nın münhasır yetkisi bakımından herhangi bir değişiklik getirmemektedir.

79. Adil yargılanma hakkı, öncelikle hâkimlerin mahkemelerin bağımsızlığı ve hâkimlik teminatı esaslarına göre görev ifa edebilmeleri için gerekli güvencelerin oluşturulmasını zorunlu kılar. Belirli bir süre için bölge idare mahkemesi üyeliğine atanabilecek idari yargı hâkim ve savcılarının kapsamını genişletmekten ibaret olan kuralın, mahkemelerin bağımsızlığı ve hâkimlik teminatını sağlayan güvencelerde herhangi bir etkisinin bulunmaması karşısında anılan güvencelere ve adil yargılanma hakkına aykırı olduğu söylenemez.

80. Öte yandan kuralda yer alan "...üstün başarısı..." ibaresinin soyut ve genel bir kavram olması kuralı belirsiz kılmamakta, bu durum kanun yapma tekniğinin doğasından kaynaklanmaktadır. Zira kanun hükümlerinin genel ve soyut olması, somut olayın özelliğine göre değişebilecek tüm çözümleri kuralın bünyesinde barındırma, bir başka ifadeyle kuralın amaca uygun sonuca ulaştıracak herhangi bir çözümü dışlamasını önleme ihtiyacından kaynaklanmaktadır. Hukuk kurallarının belirliliğinin sağlanması yalnızca kanunla düzenleme yapılması anlamına gelmemektedir. Kanuni düzenlemeye dayanarak erişilebilir, bilinebilir ve öngörülebilir olma gibi niteliklere ilişkin gereklilikleri karşılaması şartıyla mahkeme içtihatları ve yürütmenin düzenleyici işlemleri ile de hukuki belirlilik sağlanabilir. Hukuki belirlilik ilkesinde asıl olan, bir hukuk normunun uygulanmasıyla ortaya çıkacak sonuçların o hukuk düzeninde öngörülebilir olmasıdır.

81. Bu bağlamda söz konusu ölçütün içeriği HSK tarafından belirlenmektedir. HSK diğer görevlerinin yanında adlî ve idarî yargı hâkim ve savcılarının yükselme ve birinci sınıfa ayırma işlemlerini yapan anayasal kuruldur. HSK'nın anılan işlemleri gerçekleştirirken gözönünde bulunduracağı kıstaslar 2802 sayılı Kanun'da düzenlenmiştir. Belirtilen nitelikleri itibarıyla kuralın belirsiz ve öngörülemez olduğundan söz edilemeyeceğinden kuralda belirlilik ilkesine aykırılık bulunmamaktadır.

82. Açıklanan nedenlerle kural Anayasa'nın 2., 36., 138. 139. ve 140. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

IV. YÜRÜRLÜĞÜN DURDURULMASI TALEBİ

83. Dava dilekçesinde özetle, dava konusu kuralların uygulanmasının sonradan giderilmesi imkânsız durumların ortaya çıkmasına neden olacağı ve zararlar doğuracağı belirtilerek kuralların yürürlüklerinin durdurulmasına karar verilmesi talep edilmiştir.

9/11/2016 tarihli ve 6757 sayılı Kanun'un;

A. 1. 22. maddesiyle 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'nun 60. maddesine eklenen (11) numaralı fıkranın (28/11/2017 tarihli ve 7061 sayılı Kanun'un 99. maddesiyle aynı maddeye eklenen (9) numaralı fıkra nedeniyle (12) numaralı fıkra şeklinde teselsül ettirilmiştir) birinci ve üçüncü cümlelerine,

2. 23. maddesiyle 4/6/1937 tarihli ve 3201 sayılı Emniyet Teşkilât Kanunu'nun ek 24. maddesine eklenen üçüncü fıkranın birinci cümlesinde yer alan "...Kamu Personel Seçme Sınavı şartı aranmaksızın,..." ibaresine,

3. 25. maddesiyle 6/1/1982 tarihli ve 2576 sayılı Bölge İdare Mahkemeleri, İdare Mahkemeleri ve Vergi Mahkemelerinin Kuruluşu ve Görevleri Hakkında Kanun'a eklenen geçici 21. maddeye, yönelik iptal talepleri 24/7/2019 tarihli ve E.2017/16, K.2019/64 sayılı kararlarla reddedildiğinden, bu maddeye, cümlelere ve ibareye ilişkin yürürlüğün durdurulması taleplerinin REDDİNE,

B. 7. maddesiyle 31/7/1970 tarihli ve 1324 sayılı Genelkurmay Başkanının Görev ve Yetkilerine Ait Kanun'un 8. maddesinin değiştirilen birinci fıkrası hakkında 24/7/2019 tarihli ve E.2017/16, K.2019/64 sayılı kararlar karar verilmesine yer olmadığına karar verildiğinden, bu fıkraya ilişkin yürürlüğün durdurulması talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA,

24/7/2019 tarihinde OYBİRLİĞİYLE karar verilmiştir.

V. HÜKÜM

9/11/2016 tarihli ve 6757 sayılı Kanun'un;

A. 7. maddesiyle 31/7/1970 tarihli ve 1324 sayılı Genelkurmay Başkanının Görev ve Yetkilerine Ait Kanun'un 8. maddesinin değiştirilen birinci fıkrasına ilişkin iptal talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA OYBİRLİĞİYLE,

B. 22. maddesiyle 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'nun 60. maddesine eklenen (11) numaralı fıkranın (28/11/2017 tarihli ve 7061 sayılı Kanun'un 99. maddesiyle aynı maddeye eklenen (9) numaralı fıkra nedeniyle (12) numaralı fıkra şeklinde teselsül ettirilmiştir) birinci ve üçüncü cümlelerinin Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, Zühtü ARSLAN, Engin YILDIRIM ile Hasan Tahsin GÖKCAN'ın karşıoyları ve OYÇOKLUĞUYLA,

C. 23. maddesiyle 4/6/1937 tarihli ve 3201 sayılı Emniyet Teşkilât Kanunu'nun ek 24. maddesine eklenen üçüncü fıkranın birinci cümlesinde yer alan "...Kamu Personel Seçme Sınavı şartı

aranmaksızın,...” ibaresinin Anayasa’ya aykırı olmadığına ve iptal talebinin REDDİNE, Hasan Tahsin GÖKCAN, Serdar ÖZGÜLDÜR ile Recep KÖMÜRCÜ’nün karşıoyları ve OYÇOKLUĞUYLA, Ç. 25. maddesiyle 6/1/1982 tarihli ve 2576 sayılı Bölge İdare Mahkemeleri, İdare Mahkemeleri ve Vergi Mahkemelerinin Kuruluşu ve Görevleri Hakkında Kanun’a eklenen geçici 21. maddenin Anayasa’ya aykırı olmadığına ve iptal talebinin REDDİNE OYBİRLİĞİYLE,

24/7/2019 tarihinde karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili - Engin YILDIRIM

Başkanvekili - Hasan Tahsin GÖKCAN

Üye: Serdar ÖZGÜLDÜR; Recep KÖMÜRCÜ; Hicabi DURSUN; Celal Mümtaz AKINCI; Muammer TOPAL; M. Emin KUZ; Kadir ÖZKAYA; Rıdvan GÜLEÇ; Recai AKYEL; Yusuf Şevki HAKYEMEZ; Yıldız SEFERİNOĞLU

KARŞIOY GEREKÇESİ

1. 9/11/2016 tarihli ve 6757 sayılı Kanun’un 22. maddesiyle 5809 sayılı Elektronik Haberleşme Kanunu’nun 60. maddesine eklenen (11) numaralı (sonraki değişikliklerin ardından 12 numaralı) fıkranın iptali istenen birinci ve üçüncü cümlelerinin Anayasa’ya aykırılık iddiası Mahkememiz çoğunluğu tarafından reddedilmiştir.

2. İptali istenen kurallar şu şekildedir: “Kurum, görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilir ve değerlendirmesini yapabilir; arşivlerden, elektronik Bilgi İşlem Merkezlerinden ve iletişim altyapısından yararlanabilir, bunlarla irtibat kurabilir ve bu kapsamda diğer gerekli önlemleri alabilir veya aldırabilir... Bu kapsamda Kurum tarafından istenen her türlü bilgi ve belge talebi; ilgili bakanlık, kurum ve kuruluşlar tarafından gecikmeksizin yerine getirilir.” Kurallar, bir yandan Bilgi Teknolojileri ve İletişim Kurumuna (Kurum) görevi kapsamında her türlü bilgi, belge, veri ve kayıtları ilgili yerlerden alabilme ve bunları değerlendirme, arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanma yetkisi vermekte, diğer yandan da ilgili bakanlık, kurum ve kuruluşlara da Kurum tarafından yapılan her türlü bilgi ve belge talebini gecikmeksizin yerine getirme yükümlülüğü getirmektedir.

3. Anayasa’nın 20. maddesi özel hayatın gizliliği ve kişisel verilerin korunması hakkını güvenceye almaktadır. Anayasa koyucu “Özel hayatın ... gizliliğine dokunulamaz” şeklinde kesin bir dille özel

hayatın mahremiyetinin önemine işaret etmiştir. Bu gizliliğin özel bir yansıması kişisel verilerin korunmasında karşımıza çıkmaktadır. Anayasa'nın 20. maddesine 2010 yılında eklenen fıkrayla kişisel verilerin korunması hakkı açıkça güvenceye kavuşturulmuştur. Kişinin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı, "kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar".

4. Kimliği belirli veya belirlenebilir kişiye ilişkin her türlü bilgiyi ifade eden kişisel veri, kişinin mahremiyetinin en önemli yönlerinden birini, dolayısıyla maddi ve manevi varlığını geliştirme hakkının da ayrılmaz unsurunu oluşturmaktadır. Kişisel verilerin korunması hakkı, Anayasa Mahkemesi kararlarında ifade edildiği üzere, insanın "onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır" (AYM, E. 2014/87, K. 2015/112, 8/12/2015, § 164).

5. Bununla birlikte kişisel verilerin korunmasını isteme hakkı sınırsız değildir. Anayasa'nın 13. maddesinde öngörülen güvencelere aykırı olmamak kaydıyla söz konusu hak sınırlandırılabilir. Bu güvencelerin başında "kanunla sınırlama" ölçütü gelmektedir. Buna göre, diğer temel hak ve hürriyetler gibi, kişisel verilerin korunması hakkının da sınırlandırılabilmesi kanunla mümkündür. Dahası bu hakkın yer aldığı Anayasa'nın 20. maddesinde "kanunla sınırlama" şartı, "Kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir" şeklinde özel olarak düzenlenmiştir.

6. Bu noktada belirtmek gerekir ki, Anayasa'nın 13. ve 20. maddeleri kapsamında kişisel verilerin korunması hakkını sınırlamaya yönelik bir kanuni düzenlemenin bulunması yeterli değildir. Anayasa Mahkemesinin sıkça vurguladığı gibi temel hakları sınırlayan kanunun şeklen var olması yeterli olmayıp, yasal kuralların keyfiliğe izin vermeyecek şekilde belirli, ulaşılabilir ve öngörülebilir düzenlemeler niteliğinde olması gerekir (bkz. Tuğba Arslan [GK], B.No: 2014/256, 25/06/2014, § 89).

7. Esasen temel hakları sınırlayan kanunun bu niteliklere sahip olması, Anayasa'nın 2. maddesinde güvenceye alınan hukuk devleti ilkesinin de bir gereğidir. Hukuk devletinde, kanuni düzenlemelerin "hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfî uygulamalarına karşı koruyucu önlem içermesi gerekir" (AYM, E.2015/41, K.2017/98, 4/5/2017, § 153). Kanunda bulunması gereken bu nitelikler hukuki güvenliğin sağlanması bakımından da zorunludur. Zira bu ilke "hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden

kaçınmasını gerekli kılar” (AYM, E.2015/41, K.2017/98, 4/5/2017, § 154). Dolayısıyla Anayasa’nın 13. ve 20. maddelerinde sınırlama ölçütü olarak belirtilen kanunilik, Anayasa’nın 2. maddesinde güvenceye alınan hukuk devleti ilkesi ışığında yorumlanmalıdır.

8. Kişilerin özel hayatlarının kamu otoriteleri başta olmak üzere başkalarının keyfi müdahalelerine karşı korunabilmesi için kanuni düzenlemelerin açık, anlaşılabilir ve kişilerin davranışlarını yönlendirebilmesini sağlayacak nitelikte olması gerekir. Bu bağlamda kişisel verilerin korunması hakkını sınırlayan kanuni düzenlemelerin, hangi kapsamda ve amaçla kişisel verilerin isteneceği ve işleneceği, talep edilen verilerin mahiyeti, bu verilerin ne kadar süreyle saklanacağı, bu sürenin sonunda nasıl imha edileceği, verilerin amacına uygun kullanımının denetimi ve kişilerin kişisel verilerin işlendiğinden haberdar edilmesi gibi hususlar bakımından belirli ve öngörülebilir olması gerekmektedir.

9. Mahkememiz yakın tarihte bireysel başvuru kapsamında verdiği bir kararında güvenlik soruşturması ve arşiv araştırmasının dayanağı olan 4045 sayılı Kanun’un Anayasa’nın 13. ve 20. maddelerinin gerektirdiği “kanunilik” şartını sağlayıp sağlamadığını denetlemiştir. Anayasa Mahkemesi, söz konusu Kanun’un “güvenlik soruşturmasına ve arşiv araştırmasına konu edilecek bilgi ve belgelerin neler olduğu, bu bilgilerin nerelerden elde edileceği ve ne suretle ve ne kadar süre ile saklanacağı, kişilerin söz konusu bilgilere itiraz etme olanağı olup olmadığı, bilgilerin bir müddet sonra silinmesinin mümkün olup olmadığı veya silinmesine dair izlenecek usulün ne olduğu, gizlilik dereceli kamu personeli ile meslek gruplarının tespiti, güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak mercilerin kimler olduğu ile ilgili hiçbir düzenleme içermediği”, bireyleri keyfiliğe karşı koruyacak hükümlere yer vermediği, bu anlamda “bireylerin özel hayatına saygı hakkının güvencelerini sağlayacak hükümlerden yoksun olduğu” sonucuna ulaşmıştır (Fatih Saraman, [GK], B.No: 2014/7256, 27/2/2019, § 83).

10. Diğer taraftan Anayasa Mahkemesi norm denetimi kapsamında, iptali istenen kurala benzer iki kuralı anılan kriterler yönünden incelemiş ve Anayasa’ya aykırı bularak iptal etmiştir. Bu kararların ilkinde internet trafik bilgisinin Telekomünikasyon İletişim Başkanlığı (TİB) tarafından ilgili işletmecilerden alınmasını ve hâkim tarafından karar verilmesi durumunda bu bilginin ilgili mercilere verilmesini öngören kuralda “temin edilecek bilgiyle ilgili olarak herhangi bir konu ve amaç sınırlaması bulunmadığı gibi bilginin kapsamı, ne şekilde kullanılacağı, tutulacağı süre, temin edilme gerekçesi gibi hususlarla ilgili olarak da herhangi bir belirlilik bulunmamakta” olduğu tespiti yapılmıştır (AYM, E.2014/149, K.2014/151, 2.10.2014).

11. İkinci kararda ise içerik, yer ve erişim sağlayıcıları, TİB tarafından talep edilen bilgileri talep edildiği şekilde TİB'e teslim etmekle ve bu kurum tarafından bildirilen tedbirleri almakla yükümlü kılan kanuni düzenlemeler, kişisel verilerin korunması hakkının gerektirdiği güvencelerden yoksun olduğu için iptal edilmiştir. Anayasa Mahkemesine göre iptali istenen kurallarda, talep edilen bilgilerin verilmesinden ilgili kişilerin haberdar olmalarına ilişkin bir düzenlemeye yer verilmemekte, "TİB'in hangi koşullarda ve hangi gerekçelerle istediği bilgilerin içerik, yer ve erişim sağlayıcılar tarafından Başkanlığa teslim edileceğine ya da verilen bilgilerin ne kadar süre ile TİB'de saklanacağına, talep edilen bilgilerin mahiyetine, içerik, yer ve erişim sağlayıcılara bildirilecek tedbirlere ilişkin herhangi bir belirlilik bulunmamakta", belirli ve öngörülebilir olmayan düzenlemelerden dolayı kişisel verilerin korunması hakkı ölçüsüzce sınırlandırılmaktadır (AYM, E.2014/87, K.2015/112, 8/12/2015, §§ 168-170).

12. İptali istenen eldeki kuralların denetiminde Mahkememizin önceki kararlarından ayrılmayı gerektiren bir husus bulunmamaktadır.

13. Belirtmek gerekir ki, çoğunluğun kuralların anlam ve kapsamını belirlerken yaptığı değerlendirmeye katılmak mümkün değildir. Bu değerlendirmeye göre birinci cümlede yer alan "görevi kapsamında" ibaresi, Kurumun siber güvenlik kapsamındaki görevini ifade etmektedir. Halbuki Kurum'un görev ve yetkileri siber güvenlikle sınırlı değildir. Siber güvenlik Kurum'un Kanun'un 6. maddesinde sayılan yirmi sekiz görevinden biridir. Kuralda yer alan "görevi kapsamında" ibaresi, Kurum'un siber güvenlik dâhil tüm görevlerini kapsayacak şekilde anlaşılmaya müsaittir. Kurum'un kişisel verileri isteme ve işleme yetkisinin belli bir görevle (siber güvenlik) sınırlandırıldığı ne kuralın lafzından ne de maddenin sistematüğinden anlaşılmaktadır. En iyi ihtimalle ibarenin belirlilikten uzak olduğu söylenebilir. Kanun koyucunun Kurum'un hangi görevleri kapsamında ve hangi amaçla kişisel verileri ilgili yerlerden isteme, işleme ve kullanma yetkisine sahip olduğunu daha açık şekilde ifade etmesi gerekirdi.

14. Hiç kuşkusuz temel hak ve hürriyetlere yapılacak müdahale alanı genişledikçe, muhtemel keyfi ve ölçüsüz uygulamalara karşı bireylere güvence sağlayan kuralların daha açık ve belirli olması gerekir. Kurum'un görev alanının oldukça geniş olduğu ve dolayısıyla da dava konusu kuralların geniş bir alanda kişilerin temel haklarına müdahaleye izin verdiği dikkate alındığında, kişisel verilerin korunması hakkını korumaya yönelik güvenceleri karşılayan açıklıkta ve belirlilikte düzenlemeye ihtiyaç olduğu izahtan varestedir.

15. Diğer yandan Kurum tarafından istenen ve işlenen kişisel verilerin mahiyeti, bu verilerin denetimi, kişilerin durumdan haberdar edilmesi gibi hususlar yönünden de güvencelere yer verilmiş

değildir. Dolayısıyla hakkın korunması için gerekli belirlilik, öngörülebilirlik ve güvencelerden yoksun olan kuralların, kişisel verilerin korunmasını isteme hakkına yönelik keyfi müdahaleyi önleyecek kanuni güvencelere yer vermeksizin sınırlama getirdiği, dolayısıyla Anayasa'nın 13. ve 20. maddelerine aykırı olduğu açıktır.

16. Yukarıda açıklanan gerekçelerle kuralların iptali gerektiğini düşündüğümden çoğunluğun red yönündeki kararına katılmıyorum.

Başkan - Zühtü ARSLAN

KARŞIOY GEREKÇESİ

1. 6757 sayılı Kanun'un 22. maddesi ile 5809 sayılı Kanun'un 60. maddesine eklenen (11)1 numaralı fıkranın birinci cümlesi ile üçüncü cümlesinin Anayasa'ya aykırılığı iddiasıyla iptal davası açılmıştır. Dava konusu kurallar, "Kurum, görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilir ve değerlendirmesini yapabilir; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilir, bunlarla irtibat kurabilir ve bu kapsamda diğer gerekli önlemleri alabilir veya aldirabilir. Bu kapsamda Kurum tarafından istenen her türlü bilgi ve belge talebi, ilgili bakanlık, kurum ve kuruluşlar tarafından gecikmesizin yerine getirilir" düzenlenmesini içermektedir.

2. Bir kişiye ait her türlü bilgi ve veriler onun kişisel verilerini oluşturmaktadır. Devlet, gerçek ve özel hukuk tüzel kişileri bireylere ait bilgileri çeşitli gerekçelerle kaydetme, saklama, aktarma ve kullanma gibi işlemlerde kullanabilir. Kişisel verilerle ilgili yasal düzenlemelerde verilerin toplanması, kullanılması, ne kadar süre ile tutulacağı ve imhası gibi hususların açık ve net olarak düzenlenmesi gerekmektedir. Bu durumlarda kötüye kullanımları engellemek ve keyfi uygulamaların önüne geçmek amacıyla belli güvenceler ortaya konulmalı ve bunların etkin bir şekilde işlemesi sağlanmalıdır. Kişisel verilere dönük müdahalelerin demokratik toplum düzeni gereklerine uygun ve ölçülü olması da anayasal bir zorunluluktur.

3. Çoğunluk, dava konusu kuralların anlam ve kapsamını belirlerken (11) numaralı fıkrada belirtilen "Kurum, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldirır" düzenlemesinden hareketle iptali istenen kuralların "Kurumun görevi kapsamında ilgili yerlerden bilgi, veri ve kayıtları alabilmesi ve bu konuda bazı imkânlar tanınması siber güvenlik görevi ile ilgili ve sınırlı olduğu" düşüncesindedir (§ 42). Bu bağlamda, 5809 sayılı Kanununun 6. maddesinin (1) numaralı fıkrasının (1)

bendini de dikkate alan çoğunluğa göre dava konusu ilk kuraldaki “görev ibaresi siber güvenlik açısından yüklenen sorumluluğu ifade etmektedir” (§ 43).

4. 5809 sayılı Kanunun Kurumun yetkilerini düzenleyen 6. maddesine baktığımızda siber güvenliğin sağlanmasını kuruma verilen görevlerden sadece bir tanesini oluşturduğunu görmekteyiz. Siber güvenliğin sağlanması kurumun görev ve yetkileri arasında olmakla birlikte, kurumun temel görevi elektronik haberleşme alanındaki kamu ve özel kesim faaliyetlerini düzenlemek, denetlemek ve gerektiğinde yaptırım uygulamaktır. Bu nedenle dava konusu kurallarda geçen görev ibaresinin siber güvenlik alanıyla ilgili ve sınırlı olduğu görüşüne katılmak mümkün gözükmemektedir.

5. Çoğunluk görüşü iptali istenen kuralların siber güvenliğin sağlanması üstün kamu yararı çerçevesinde demokratik toplum düzeni gereklerine uygun ve ölçülü olduğu düşüncesini taşımaktadır.

6. Anayasa Mahkemesi dava konusu kurallarla benzer nitelik taşıyan bir kararında (E.2014/149, K.2014/151, 2/10/2014) kişisel veri niteliğinde olan ve ciddi suçların tespiti, soruşturulması ve kovuşturulmasında kullanılmak üzere gerçek ve tüzel kişilere ilişkin trafik bilgisinin erişim veya yer sağlayıcılardan, Telekomünikasyon İletişim Başkanlığı (TİB) tarafından herhangi bir gerekçe veya neden göstermeksizin temin edilmesine olanak sağlayan kuralın Anayasa'nın 2., 13. ve 20. maddelerine aykırı olduğu sonucuna ulaşmıştır. Mahkeme, trafik bilgisi adı altında temin edilecek olan bilgilerin birçok temel hakla doğrudan ilgili olup bu bilgilerin TİB tarafından herhangi bir kurala ve sınırlamaya tabi olmaksızın istenildiği zaman ve şekilde elde edilebilir olmasını temel hak ve özgürlüklerin korunması bakımından sorunlu bulmuştur.

7. Anayasa'nın 20. maddesinin birinci fıkrasında “Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz” denilerek özel hayatın gizliliği güvence altına alınmıştır. Maddenin üçüncü fıkrasında ise herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı hükme bağlanarak kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir.

8. Dava konusu kurallarla Bilgi Teknolojileri ve İletişim Kurumuna son derece geniş yetkiler tanınmakla beraber kişisel verilerin güvenliği ve korunmasına ilişkin herhangi yeterli düzeyde bir düzenlemeye yer verilmemiştir. Kurallarla özel hayatın gizliliği ve kişisel verilerin korunması

haklarına bir müdahalede bulunmaktadır. Kurum, görevi kapsamında ilgili gördüğü yerlerden kişisel verileri alma ve değerlendirme yetkisine sahiptir. Bu müdahale söz konusu hakların kullanılmasını son derece zorlaştırmadığı veya onları kullanılamaz hale getirmediğinden hakkın özüne dokunmamakla beraber, müdahalenin demokratik toplum düzeninin gerekleri ile ölçülülük ilkesine uygun olup olmadığının değerlendirilmesi gerekmektedir.

9. Anayasa'nın 13. maddesinde, temel hak ve özgürlüklerin özlerine dokunulmaksızın ölçülülük ilkesine uygun şekilde, yasayla sınırlandırılabilmesi belirtilmektedir. Ölçülülük ilkesi sınırlamada başvurulan aracın sınırlama amacını gerçekleştirmeye elverişli olmasını; bu aracın sınırlama amacı açısından gerekli olmasını ve araçla amacın ölçüsüz bir oran içinde bulunmamasını ifade eder. Burada kısıtlama için kullanılan araçla amaç arasında hak ve özgürlüğü en az sınırlayacak dengeli bir orantı aranmaktadır.

10. Elverişlilik ölçütüne göre bir yasal düzenlemenin sınırlama amacı bakımından elverişli sayılması için bu düzenlemenin arzulanan amaca veya amaçlara katkı yapması gerekmektedir. İncelediğimiz kurallar bu niteliği taşımaktadır. Gereklilik ise bir temel hakkı en az sınırlayan aracın seçilmesini gerektirmekle birlikte dava konusu kuralların, hakkı en az sınırlayan bir araç olduğunu söylemek mümkün değildir. Çünkü söz konusu kurallar, çok geniş bir çerçeveyi kapsayarak bireyin her türlü kişisel verisinin toplanması, aktarılması, işlenmesini mümkün hale getirmektedir. Kuralların özel hayatın gizliliği ve kişisel verilerin korunması hakları ile kamu yararı amacıyla kurumu tanınan yetkiler arasında orantılı makul bir denge kurmayarak, birincisini ikincisi lehine adeta gözden çıkarmaktadır. Dolayısıyla kuruma tanınan yetkiler kişisel verilerin gizliliği, güvenliği ve korunması açısından hakka yönelik ölçüsüz bir müdahaleye neden olmaktadır.

11. Özel hayatın gizliliği ve bu kapsamda kişisel verilerin korunması konusu her şeyden önce insan onuruna saygı ve kişilik haklarına dayanmaktadır. Bu hak, kişinin saygınlığını ve kişiliğini serbestçe geliştirmesini mümkün kılan şeref ve haysiyet, özel yaşam ve sağlık gibi kişisel değerler üzerindeki çıkarlarını belirterek, bireye kişiliğini dilediği şekilde, serbestçe geliştirebileceği, kendisi ve sevdikleriyle bir arada olabileceği özerk bir yaşam alanına sahip olma şansı vermektedir. Bu alanda birey, maddi ve manevi kişiliğini geliştirmek ve başkaları tarafından bilinmesini istemediği hususların güvence altına alınmasını istemek hakkına sahiptir.

12. Kişisel verilerin toplanması ve işlenmesi sırasında bireyin bu veriler üzerindeki hakkı, onun devlet veya üçüncü kişiler tarafından sıradan bir veri nesnesine indirgenmesini önlemek amacını taşımaktadır. Kişisel verilerin ilgili kişinin açık rızası olmadan toplanması, işlenmesi ve aktarılması, kişinin basit bir veri nesnesi olarak değerlendirilmesine yol açtığından insan haysiyetini

zedelemektedir. Bireyin, ahlaki ve toplumsal kişiliğinin gelişiminde ve diğer insanlarla olan ilişkilerini düzenlemede önemli bir kavram olan mahremiyetin ihlali insan haysiyetinin ve kişiliğinin ihlali anlamına gelmektedir.

13. Kişisel verilerin korunması kişinin maddi ve manevi varlığını geliştirmesine imkân tanıyarak, bireyin hayatını kendi özgür iradesiyle düzenlemesine katkı sağlamaktadır. Bireyin kişisel verileri üzerindeki hakkı yeteri kadar korunmazsa, kişiliğini serbestçe geliştirmesi zora gireceğinden, özgür iradeleriyle yaşamlarını biçimlendiren bireylerden oluşan demokratik bir toplum düzeninin ortaya çıkması ve korunması da güçleşecektir.

14. Yukarıda açıklanan nedenlerle dava konusu kuralların Anayasa'nın 13. ve 20. maddelerine aykırı olduğu gerekçesiyle karara katılmıyorum.

Başkanvekili - Engin YILDIRIM

KARŞIOY GEREKÇESİ

5809 sayılı Elektronik Haberleşme Kanununun 60. maddesine 6757 sayılı Kanunun 22. maddesiyle eklenen (11) numaralı (ekin teselsülü ile 12 numaralı) fıkranın birinci ve üçüncü cümlelerinin iptal istemi Mahkememiz çoğunluğu tarafından reddedilmiştir.

İptali istenen kurallar Bilgi Teknolojileri ve İletişim Kurumuna görevi kapsamına giren her türlü bilgi, belge, veri ve kayıtları ilgili kurumlardan alabilme, bunları değerlendirme, arşiv ve elektronik bilgi işlem merkezlerinden ve iletişim alt yapılarından yararlanma yetkisi vermektedir.

Anayasanın 20. maddesinde özel hayatın gizliliği ve kişisel verilerin korunması hakkı güvenceye alınmış ve kişisel veriler hakkında bilgilendirme, bu veriler erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanıp kullanılmadığını öğrenme hakkı güvence altına alınmıştır. Kişisel veri kavramı kimliği belirli veya belirlenebilir kişiye ait her türlü kişisel bilgiyi içermektedir. Kuşkusuz aynı maddede belirtildiği üzere bu hak kanunla sınırlanabilir. Ancak sınırlayan kanunun Anayasanın 20. maddesindeki güvenceleri içermesi, belirlilik ve öngörülebilirlik unsurlarını taşıması ve sınırlamanın demokratik toplumda gerekli ve ölçülü bulunması gerekir.

Anayasa Mahkemesi daha önce Telekomünikasyon İletişim Başkanlığına kanunla verilen benzer yetkileri denetlediği kararında, iptali istenen kuralda temin edilecek bilginin kapsamı, ne şekilde kullanılacağı ve tutulacağı süre ve temin edilme gerekçesi gibi hususların gösterilmemesi nedeniyle kuralın belirli bulunmadığına işaret etmiştir (AYM 2/10/2014, E.2014/149, K.2014/151). Bu davada

incelenen kuralda da hiçbir yasal sınır belirtilmeksizin Kurumun her türlü bilgiyi temin edip değerlendirebileceği öngörülmüştür. Böylesine geniş ve sınırları belirsiz bir düzenlemenin Anayasanın 20. maddesinde belirtilen güvencelere aykırı bulunduğu açıktır.

Belirtilen nedenlerle incelenen kuralların Anayasanın 13. ve 20. maddelerine aykırı olduğu düşüncesiyle çoğunluk görüşünden ayrı oy kullandım.

Başkanvekili - Hasan Tahsin GÖKCAN

KARŞIOY GEREKÇESİ

9/11/2016 tarih ve 6757 sayılı Kanun'un 23. maddesiyle 3201 sayılı Emniyet Teşkilat Kanunu'nun Ek 24 ncü maddesine eklenen dava konusu ibare ile Emniyet Özel harekât biriminde istihdam edilecek polislerin belirlenmesinde "Kamu Personel Seçme Sınavı (KPSS)" şartı aranmayacak; bu kadrolar için müracaat edecek en az lise veya dengi okul mezunları sadece fiziki yeterlilik ve mülakat sınavları ile Polis Meslek Eğitim merkezlerine alınabilecektir.

KPSS ile kamu görevlisi alımı uygulanmasını öngören düzenleyici tasarruf tek başına soyut norm denetimine esas alınamasa da; özellikli bir kamu görevine giriş için öngörülen koşulların, bu göreve nazaran daha az nitelik ve koşulun arandığı diğer bir kadroya (normal polis statüsüne) göre farklılaştırılarak, onlar için aranan KPSS şartının özel harekât polisi kadrosu statüsüne girecekler için aranmaması ve bunlar yönünden daha hafif şartlarla statüye giriş imkânının öngörülmesi "eşitlik" ilkesini açıkça ihlal eder mahiyettedir.

Konunun diğer bir cephesi, genel bilgi düzeyini ölçen bir sınava tâbi tutulmamanın doğal sonucunun, kamu hizmetine alınmada değerlendirilmeye tâbi tutulacak objektif bir kriterden yoksun kalınacağıdır. Fiziki yeterlilik ve mülâkat gibi getirilen kriterlerin ise genel bilgi düzeyini ve liyakati belirlemeye elverişli olmadığı izahtan varestedir. Alınacak bu kişilerin henüz kamu görevlisi statüsüne girmedikleri, öğrenci statüsünde oldukları düşünülebilirse de, bu durumun dahi sonucu değiştirici bir mahiyeti yoktur. Çünkü, öğrenci statüsünde olsalar da "özel harekat" polis memur adayları ile "normal polis" memuru adayları bakımından aynı karşılaştırma yapılmak durumundadır. Dolayısıyla bu yönde bir gerekçenin de anılan Anayasa'ya aykırılığı bertaraf edici mahiyeti bulunmamaktadır.

Açıklanan nedenlerle; liyakat ölçütlerinin belirlenmesine engel olan, objektifliği sağlamaktan uzak ve emniyet teşkilatı kaynakları arasında makul olmayan bir istisna öngören dava konusu kuralın

Anayasa'nın 2. maddesindeki hukuk devleti ile 10. maddesindeki eşitlik ilkesine aykırı olduđu ve iptali gerektiđi kanaatine vardığımızdan, çoğunluđun aksi yöndeki kararına katılmıyoruz.

Başkanvekili - Hasan Tahsin GÖKCAN

Üye: Serdar ÖZGÜLDÜR; Recep KÖMÜRCÜ

1. 28/11/2017 tarih ve 7061 sayılı kanunla aynı maddeye başkaca fıkralar eklenmesi nedeniyle (12) numaralı fıkra olmuştur.

Anayasa Mahkemesi - 4632 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanunu Kararı

(E. 2016/179)

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2016/179

Karar Sayısı: 2017/176

Karar Tarihi: 28.12.2017

R.G. Tarih-Sayı: 8.2.2018 - 30326

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri Engin ALTAY, Levent GÖK, Özgür ÖZEL ile birlikte 129 milletvekili

İPTAL DAVASININ KONUSU: 10.8.2016 tarihli ve 6740 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanununda Değişiklik Yapılmasına Dair Kanun'un;

A. 1. maddesiyle 28.3.2001 tarihli ve 4632 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanunu'na eklenen ek 2. maddenin;

1. Birinci fıkrasının;

a. Birinci cümlesinin,

b. İkinci cümlesinde yer alan "...Müşteşarlıkça uygun görülen..." ibaresinin,

c. Üçüncü cümlesinin,

2. Beşinci fıkrasının dokuzuncu cümlesinin,

B. 2. maddesiyle 4632 sayılı Kanun'a eklenen geçici 2. maddenin,

Anayasa'nın 2., 7., 10., 13., 20., 35., 48., 60. ve 90. maddelerine aykırılığı ileri sürülerek iptallerine ve yürürlüklerinin durdurulmasına karar verilmesi talebidir.

I. İPTALİ İSTENEN KANUN HÜKÜMLERİ

İptali talep edilen kuralların yer aldığı 6740 sayılı Kanun'un;

1. 1. maddesiyle 4632 sayılı Kanun'a eklenen ek 2. maddenin birinci ve beşinci fıkraları şöyledir:

"Türk vatandaşı veya 29/5/2009 tarihli ve 5901 sayılı Türk Vatandaşlığı Kanununun 28 inci maddesi kapsamında olup kırk beş yaşını doldurmamış olanlardan 31/5/2006 tarihli ve 5510 sayılı Sosyal

Sigortalar ve Genel Sağlık Sigortası Kanununun 4 üncü maddesinin birinci fıkrasının (a) ve (c) bentlerine göre çalışmaya başlayanlar, işverenin bu Kanun hükümlerine göre düzenlediği bir emeklilik sözleşmesiyle emeklilik planına dâhil edilir. İşveren, çalışanını ancak otomatik katılım için emeklilik planı düzenleme konusunda Müsteşarlıkça uygun görülen şirketlerden birinin sunacağı emeklilik planına dâhil edebilir. Bakanlar Kurulu, bu madde uyarınca emeklilik planına dâhil edilecek işyerleri ile çalışanları ve bu kapsamdaki uygulama esaslarını belirlemeye yetkilidir.”

“Çalışan adına bireysel emeklilik hesabına ödenen katkı payları üzerinden ek 1 inci maddedeki usul ve esaslara göre bu madde uyarınca ayrıca Devlet katkısı sağlanır. Çalışanın bu madde kapsamında cayma hakkını kullanmaması hâlinde, sisteme girişte bir defaya mahsus olmak üzere, ek 1 inci maddedeki Devlet katkısı hak etme ve ödeme koşuluna tabi olmak kaydıyla, bin Türk lirası tutarında ilave Devlet katkısı sağlanır. Bakanlar Kurulu, bu tutarı yarısına kadar artırmaya veya yarısına kadar azaltmaya yetkilidir. Emeklilik hakkının kullanılması hâlinde, hesabında bulunan birikimi en az on yıllık, yıllık gelir sigortası sözleşmesi kapsamında almayı tercih eden çalışana, birikiminin yüzde beşi karşılığı ek Devlet katkısı ödemesi yapılır. Bu madde hükmüne göre çalışan katkı payının takip ve tahsil sorumluluğu şirkete aittir. Müsteşarlık takip ve tahsil sorumluluğunun bu amaçla yetkilendirilecek bir kuruluşça yerine getirilmesine karar verebilir. Bankalar, Sosyal Güvenlik Kurumu ve ilgili diğer kamu kurumları, çalışan katkı payının takip ve tahsili ile Devlet katkısının hesaplanması için ihtiyaç duyulan verileri, Müsteşarlıkça belirlenen usul ve esaslara göre emeklilik gözetim merkezi ile bu maddeye göre takip ve tahsil sorumluluğu ile yetkilendirilecek kuruluşça aktarır. Emeklilik gözetim merkezi ile bu maddeye göre yetkilendirilecek kuruluş, söz konusu verileri şirketler ile paylaşabilir. Bu verilerden kişisel nitelikte olanlar, veri sahibinin açık rızasının alınmasına gerek olmaksızın ilgili kuruluşlar arasında paylaşılabilir ve veri paylaşımı, kişisel verilerin korunmasına ilişkin mevzuat hükümlerine aykırılık teşkil etmez.”

2. 2. maddesiyle 4632 sayılı Kanun’a eklenen geçici 2. madde şöyledir:

“Bu maddeyi ihdas eden Kanunun yürürlüğe girdiği tarihte kırk beş yaşını doldurmamış olan çalışanlar, ek 2 nci madde hükümleri çerçevesinde otomatik olarak emeklilik planına dâhil edilir.”

II. İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Zühtü ARSLAN, Burhan ÜSTÜN, Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Rıdvan GÜLEÇ, Recai AKYEL ve Yusuf Şevki HAKYEMEZ’in katılımlarıyla 2.11.2016 tarihinde yapılan ilk inceleme toplantısında dosyada eksiklik

bulunmadığından işin esasının incelenmesine, yürürlüğü durdurma talebinin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

III. ESASIN İNCELENMESİ

2. Dava dilekçesi ve ekleri, Raportör Abuzer YAZICIOĞLU tarafından hazırlanan işin esasına ilişkin rapor, dava konusu kanun hükümleri, dayanılan ve ilgili görülen Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A. Kanun'un 1. Maddesiyle 4632 Sayılı Kanun'a Eklenen Ek 2. Maddenin Birinci Fıkrasının Birinci Cümlesinin İncelenmesi

3. Dava konusu kural, 18.1.2017 tarihli ve 6770 sayılı Türkiye Cumhuriyeti Emekli Sandığı Kanunu ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un 18. maddesiyle değiştirilmiştir. Bu nedenle konusu kalmayan cümleye ilişkin iptal talebi hakkında karar verilmesine yer olmadığına karar vermek gerekir.

B. Kanun'un 1. Maddesiyle 4632 Sayılı Kanun'a Eklenen Ek 2. Maddenin Birinci Fıkrasının İkinci Cümlesinde Yer Alan "...Müsteşarlıkça uygun görülen..." İbaresinin İncelenmesi

1. İptal Talebinin Gerekçesi

4. Dava dilekçesinde özetle, dava konusu kuralın emeklilik şirketleri arasından otomatik katımlı bireysel emeklilik sözleşmesi yapılacak şirketleri belirleme yetkisini idareye verdiği, herhangi bir kriter belirlenmeden verilen bu yetkinin eşitlik ilkesi ve ayrımcılık yasağına aykırı olduğu, sistemde denetim ve gözetim yetkisi bulunan ve 4632 sayılı Kanun hükümleri kapsamında şirketlere kuruluş izni ve faaliyet ruhsatı verilmesinde görevli olan idarenin ayrıca otomatik katımlı bireysel emeklilik sistemine katılacak şirketleri belirleme yetkisine sahip olmasının sözleşme özgürlüğü ile bağdaşmadığı belirtilerek kuralın Anayasa'nın 10. ve 48. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

5. 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 43. maddesi uyarınca kural, ilgisi nedeniyle Anayasa'nın 13. maddesi yönünden de incelenmiştir.

6. Kanun'un ek 2. maddesinin birinci fıkrasının ikinci cümlesinde işverenin, çalışanını ancak otomatik katılım için emeklilik planı düzenleme konusunda Hazine Müsteşarlığınca (Müsteşarlık) uygun görülen şirketlerden birinin sunacağı emeklilik planına dâhil edebileceği öngörülmekte olup cümlede yer alan "...Müsteşarlıkça uygun görülen..." ibaresi dava konusu kuralı oluşturmaktadır.

7. Anayasa'nın 10. maddesinde yer verilen eşitlik ilkesi hukuksal durumları aynı olanlar için söz konusudur. Bu ilkeyle eylemli değil hukuksal eşitlik öngörülmüştür. Eşitlik ilkesinin amacı, aynı durumda bulunan kişilerin kanunlar karşısında aynı işleme bağlı tutulmalarını sağlamak, ayırım yapılmasını ve ayrıcalık tanınmasını önlemektir. Bu ilkeyle, aynı durumda bulunan kimi kişi ve topluluklara ayrı kurallar uygulanarak kanun karşısında eşitliğin ihlali yasaklanmıştır. Kanun önünde eşitlik, herkesin her yönden aynı kurallara bağlı tutulacağı anlamına gelmez. Durumlarındaki özellikler, kimi kişiler ya da topluluklar için değişik kuralları ve uygulamaları gerektirebilir. Aynı hukuksal durumlar aynı, ayrı hukuksal durumlar farklı kurallara bağlı tutulursa Anayasa'da öngörülen eşitlik ilkesi zedelenmez.

8. Anayasa'nın 13. maddesinde "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz." denilmektedir.

9. Anayasa'nın 48. maddesinin birinci fıkrasında "Herkes, dilediği alanda çalışma ve sözleşme hürriyetlerine sahiptir. Özel teşebbüsler kurmak serbesttir." denilmek suretiyle sözleşme özgürlüğü güvenceye bağlanmış ve özel teşebbüsler kurmanın serbest olduğu belirtilmiş ancak devlete, özel teşebbüslerin millî ekonominin gereklerine ve sosyal amaçlara uygun yürümesini sağlayacak tedbirleri alma görevi verilmiştir. Buna göre millî ekonominin gerekleri ve sosyal amaç kapsamında alınacak tedbirler nedeniyle sözleşme özgürlüğünün sınırlandırılması mümkündür. Ancak sözleşme özgürlüğünün sınırlandırılabilmesi için belirtilen nedenlerden birinin varlığı yeterli olmayıp temel hak ve özgürlüklerin sınırlandırılması rejimini belirleyen Anayasa'nın 13. maddesine de uyulması gerekmektedir.

10. Anılan madde uyarınca temel hak ve özgürlükler özlerine dokunulmaksızın yalnızca Anayasa'da öngörülen sebeplerle ve ancak kanunla sınırlanabilir. Dokunulamayacak "öz" her temel hak ve özgürlük açısından farklılık göstermekle birlikte kanunla getirilen sınırlamanın hakkın özüne dokunmadığının kabulü için temel hakların kullanılmasını ciddi surette güçleştirip amacına ulaşmasına engel olmaması ve etkisini ortadan kaldıracı bir nitelik taşımaması gerekir.

11. Temel hak ve özgürlüklerin özlerine dokunulmaksızın yapılan sınırlamalar yönünden ise bu sınırlamaların demokratik toplum düzeninin gerekleri ile ölçülülük ilkesine aykırı olamayacağı belirtilmiştir. Bir başka deyişle öze dokunan sınırlamalar "demokratik toplum düzeninin gerekleri" ve "ölçülülük" ilkelerine evleviyetle aykırı olacağından temel hak ve özgürlüklerin özüne dokunan

sınırlamalar yönünden “demokratik toplum düzeninin gerekleri” ve “ölçülülük” ilkeleri bakımından ayrıca inceleme yapılmasına gerek bulunmamaktadır.

12. Öze dokunma yasağını ihlal etmeyen müdahaleler yönünden gözetilmesi öngörülen “demokratik toplum düzeninin gerekleri” kavramı, öncelikle ilgili hak yönünden getirilen sınırlamaların zorunlu ya da istisnai tedbir niteliğinde olmasını, başvurulabilecek en son çare ya da alınabilecek en son önlem olarak kendisini göstermesini gerektirmektedir. “Demokratik toplum düzeninin gerekleri”nden olma, bir sınırlamanın demokratik bir toplumda zorlayıcı bir toplumsal ihtiyacın karşılanması amacıyla yönelik olmasını ifade etmektedir.

13. Anayasa'nın 13. maddesinde ifade edilen “ölçülülük ilkesi”, temel hak ve özgürlüklerin sınırlandırılmasına ilişkin başvurularda dikkate alınması gereken bir diğer ilkedir. Demokratik toplum düzeninin gerekleri ve ölçülülük ilkeleri, iki ayrı kriter olarak düzenlenmiş olmakla birlikte bu iki kriter arasında sıkı bir ilişki vardır. Temel hak ve özgürlüklere yönelik herhangi bir sınırlamanın demokratik toplum düzeni için gerekli nitelikte, başka bir ifadeyle öngörülen kamu yararı amacını gerçekleştirmekle birlikte temel haklara en az müdahaleye olanak veren ölçülü bir sınırlama niteliğinde olup olmadığının incelenmesi gerekir.

14. Ölçülülük, temel hak ve özgürlüklerin sınırlanma amaçları ile sınırlama araçları arasındaki ilişkiyi yansıtır. Ölçülülük denetimi, ulaşılmak istenen amaçtan yola çıkılarak bu amaca ulaşmak için seçilen aracın denetlenmesidir. Bu sebeple kuralın hedeflenen amaca ulaşabilmek için elverişli, gerekli ve orantılı olup olmadığı değerlendirilmelidir.

15. Belirtilen nitelikleri gereği, Anayasa'nın 13. maddesinde yer alan ve aralarında sıkı bir ilişki bulunan "temel hak ve hürriyetlerin özü", "demokratik toplum düzeninin gerekleri" ve "ölçülülük ilkesi" kavramları, bir bütünün parçaları olup "demokratik bir hukuk devleti"nin özgürlükler rejiminde gözetilmesi gereken temel ölçütleri oluşturmaktadır.

16. 4632 sayılı Kanun'un 8. ve 9. maddelerinde emeklilik şirketlerinin kuruluşu ve faaliyete başlamasına ilişkin usul ve esaslar düzenlenmiştir. Buna göre emeklilik şirketlerinin bireysel emeklilik sistemi kapsamında katılımcılarla sözleşme yapabilmesi için öncelikle Müsteşarlardan kuruluş izni, ardından faaliyet ruhsatı, daha sonrasında ise Sermaye Piyasası Kurumundan fon kurma onayı alması gerekmektedir. Kural, bu şekilde faaliyete başlayan emeklilik şirketlerinin otomatik katılımlı bireysel emeklilik sistemi (OK-BES) kapsamında işverenle sözleşme yapabilmesi için ayrıca emeklilik planı düzenleme konusunda Müsteşarlık tarafından uygun görülmesi şartını hükme bağlamaktadır.

17. Kuruluş izni, faaliyet ruhsatı ve fon kurma onayı almış bulunan emeklilik şirketlerinin isteyen herkesle bireysel emeklilik sözleşmesi yapabilme imkânının devam ettiği, kuralın sadece OK-BES kapsamında yapılacak sözleşmeler ile ilgili olarak emeklilik şirketleri yönünden ilave bir koşul öngördüğü, bu koşulu yerine getiren emeklilik şirketleri arasından da işverenin seçim yapma olanağının bulunduğu gözetildiğinde OK-BES kapsamında sözleşme yapılabilecek emeklilik şirketlerine ilişkin koşulların belirli bir ölçü ve denge gözetilerek belirlenmesinin sözleşme özgürlüğünü ortadan kaldıran veya onu kullanılamayacak ölçüde sınırlayan bir düzenleme olarak nitelendirilemeyeceği açıktır.

18. Kural, bir taraftan emeklilik şirketlerini etkilerken diğer taraftan çalışanların otomatik olarak katıldığı sisteme yatırılan tasarruflarının güvenliğini ilgilendirmektedir. Bu nedenle katılımcıların cayma veya ayrılma hakkını kullanmasına kadar zorunlu olarak yatırılacak katkı paylarının ve devletin katkı payının yer aldığı fonların yönetimini üstlenen emeklilik şirketlerinin emeklilik planı düzenleme konusundaki uygunluğunun tespitinde idareye ek bir yetki verilmesi suretiyle kamu yararının gerçekleştirilmesinin amaçlandığı gözetildiğinde söz konusu sınırlamanın “demokratik toplum düzeninin gerekleri”ne aykırılık taşımadığı anlaşılmaktadır.

19. Öte yandan emeklilik şirketlerinin bireysel emeklilik sisteminde isteyen herkesle sözleşme yapma imkânının ortadan kaldırılmamış olması, dava konusu kuralla getirilen ek koşulun OK-BES kapsamında yapılacak sözleşmelerle sınırlı olması ve işverenin bu ek koşulu yerine getiren emeklilik şirketleri arasında seçim yapma olanağının bulunması nedeniyle sözleşme özgürlüğüne yapılan müdahalenin ölçülü olduğu ve bireylere aşırı bir külfet yüklediği sonucuna ulaşılmaktadır.

20. Ayrıca bireysel emeklilik sisteminde isteyen herkesin emeklilik şirketlerinden dilediğiyle bireysel emeklilik sözleşmesi yapabilmesi mümkün ve tarafların sözleşmeden dönmesi hâlinde özel hukuk çerçevesinde karşılıklı güvence mekanizmaları bulunmakta iken OK-BES kapsamındaki emeklilik sözleşmesinin işveren tarafından yapılması, belirli bir süre zorunlu katkı payının ödenmesi, istek hâlinde katkı payının en kısa zamanda iadesi ile iradesi dışında katılımcı olanların menfaatlerinin korunması söz konusu olduğundan bireysel emeklilik sistemi ile OK-BES arasında eşitlik karşılaştırması yapılması mümkün değildir.

21. Açıklanan nedenlerle kural Anayasa'nın 10., 13. ve 48. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

C. Kanun'un 1. Maddesiyle 4632 Sayılı Kanun'a Eklenen Ek 2. Maddenin Birinci Fıkrasının Üçüncü Cümlesinin İncelenmesi

1. İptal Talebinin Gerekçesi

22. Dava dilekçesinde özetle, dava konusu kuralda sisteme dâhil edilecek işyerleri ve çalışanların belirlenmesi ile ilgili olarak sınırların ve temel ilkelerin ifade edilmesi yerine idareye keyfî ve adaletsiz uygulamalara neden olabilecek, yasama yetkisi kapsamında kalması gereken hususlarda yetki tanıyan bir düzenleme yapıldığı, böylece hukuki belirsizlik oluştuğu ve yasama yetkisinin yürütme organına devredildiği belirtilerek kuralın Anayasa'nın 2. ve 7. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

23. Dava konusu kural, Bakanlar Kurulunun otomatik katımlı bireysel emeklilik planına dâhil edilecek işyerleri ile çalışanları ve bu kapsamdaki uygulama esaslarını belirlemeye yetkili olduğunu öngörmektedir.

24. Anayasa'nın 2. maddesinde belirtilen hukuk devleti insan haklarına dayanan, bu hak ve özgürlükleri koruyup güçlendiren, eylem ve işlemleri hukuka uygun olan, her alanda adaletli bir hukuk düzeni kurup bunu geliştirerek sürdüren, Anayasa'ya aykırı durum ve tutumlardan kaçınan, hukuku tüm devlet organlarına egemen kılan, Anayasa ve kanunlarla kendini bağlı sayan, yargı denetimine açık olan devlettir.

25. Hukuk devletinin temel ilkelerinden biri de "belirlilik"tir. Bu ilkeye göre yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfî uygulamalarına karşı koruyucu önlem içermesi gerekir. Belirlilik ilkesi, hukuksal güvenlikle bağlantılı olup birey yasadaki belirli bir kesinlik içinde hangi somut eylem ve olguya hangi hukuksal yaptırımın veya sonucun bağlandığını bilmelidir. Birey ancak bu durumda kendisine düşen yükümlülükleri öngörebilir ve davranışlarını ayarlar. Hukuk güvenliği; normların öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar.

26. Anayasa'nın 7. maddesinde "Yasama yetkisi Türk Milleti adına Türkiye Büyük Millet Meclisindedir. Bu yetki devredilemez." denilmektedir. Yasama yetkisinin Türkiye Büyük Millet Meclisine ait olması ve bu yetkinin devredilememesi kuvvetler ayrılığı ilkesinin bir gereğidir. Bu hükme yer veren Anayasa'nın 7. maddesinin gerekçesinde yasama yetkisinin parlamentoya ait olması hususu "demokrasi rejimini benimseyen siyasi rejimlerde kaçınılmaz bir durum" olarak nitelendirilmiştir.

27. Anılan madde gerekçesinden de anlaşılacağı üzere, yasama yetkisinin devredilmezliği esasen kanun koyma yetkisinin TBMM dışında başka bir organca kullanılamaması anlamına gelmektedir. Anayasa'nın 7. maddesi ile yasaklanan husus, kanun yapma yetkisinin devredilmesi olup bu madde, yürütme organına hiçbir şekilde düzenleme yapma yetkisi verilemeyeceği anlamına gelmemektedir. Kanun koyucu, yasama yetkisinin genelliği ilkesi uyarınca bir konuyu doğrudan kanunla düzenleyebileceği gibi bu hususta düzenleme yapma yetkisini yürütme organına da bırakabilir.

28. Yürütmenin türevselliği ilkesi gereğince yürütme organının bir konuda düzenleme yapabilmesi için yasama organınca yetkilendirilmesi gerekmektedir. Kural olarak, kanun koyucunun genel ifadelerle yürütme organını yetkilendirmesi yeterli olmakla birlikte Anayasa'da kanunla düzenlenmesi öngörülen konularda genel ifadelerle yürütme organına düzenleme yapma yetkisi verilmesi, yasama yetkisinin devredilmezliği ilkesine aykırılık oluşturabilmektedir. Bu nedenle Anayasa'da temel hak ve özgürlüklerin sınırlandırılması, vergi ve benzeri mali yükümlülüklerin konması ve memurların atanmaları, özlük hakları gibi münhasıran kanunla düzenlenmesi öngörülen konularda, kanunun temel esasları, ilkeleri ve çerçeveyi belirlemiş olması gerekmektedir. Anayasa koyucunun açıkça kanunla düzenlenmesini öngördüğü konularda, yasama organının temel kuralları saptadıktan sonra, uzmanlık ve idare tekniğine ilişkin hususları yürütmeye bırakması, yasama yetkisinin devri olarak yorumlanamaz.

29. Dava konusu kuralla, Bakanlar Kuruluna tanınan yetkilerden biri otomatik katımlı bireysel emeklilik planına dâhil edilecek işyerleri ile çalışanları belirlemek olsa da kuralın yer aldığı fıkranın birinci cümlesinde "Türk vatandaşı veya 29/5/2009 tarihli ve 5901 sayılı Türk Vatandaşlığı Kanununun 28 inci maddesi kapsamında olup kırk beş yaşını doldurmamış olanlardan 31/5/2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 4 üncü maddesinin birinci fıkrasının (a) ve (c) bentlerine göre çalışmaya başlayanlar, işverenin bu Kanun hükümlerine göre düzenlediği bir emeklilik sözleşmesiyle emeklilik planına dâhil edilir." denilmek suretiyle bu hususların kanun koyucu tarafından bizzat düzenlendiği görülmektedir. Anılan cümle, dava tarihinden sonra kabul edilen 6770 sayılı Kanun'un 18. maddesiyle değiştirilmek suretiyle OK-BES kapsamına giren çalışanların kapsamı genişletilmiştir. Bu itibarla Bakanlar Kuruluna tanınan yetkinin farklı bir nitelik taşıdığı ve işyerleri ile çalışanların belirlenmesine yönelik bir yetki olmadığı anlaşılmaktadır. Nitekim Bakanlar Kurulunun 2.1.2017 tarihli ve 2017/9721 sayılı kararı ile çıkarılan yönetmelik hükümleri gereğince sisteme dâhil edilme süreci, Kanun'da nitelikleri belirtilen işyerlerinin çalışan kişi sayısına göre sıralı bir takvime bağlanmıştır.

30. OK-BES kapsamına giren işyerleri ile çalışanların Kanun'un ek 2. maddesinin birinci fıkrasının birinci cümlesinde açıkça düzenlendiği, bu suretle Bakanlar Kurulunu bağlayıcı bir çerçevenin çizildiği, kuralla Bakanlar Kuruluna tanınan yetkinin Kanun'un anılan hükmü uyarınca tespit edilen işyerleri ve çalışanlarının sisteme dâhil edilmesi sürecine ilişkin uygulama esaslarının belirlenmesinden ibaret olduğu anlaşılmaktadır. Kanun'da çizilen çerçeve içinde kalmak kaydıyla çok sayıda çalışanın sisteme girişinde yaşanabilecek risk ve güçlüklerle göre öngörülemeyen, değişken ve teknik konularla ilgili uygulama esaslarını belirleme yetkisinin yürütme organına bırakılması, belirsizlik oluşturduğu anlamına gelmeyeceği gibi yasama yetkisinin devredilmezliği ilkesinin ihlali sonucunu da doğurmaz.

31. Açıklanan nedenlerle kural Anayasa'nın 2. ve 7. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

D. Kanun'un 1. Maddesiyle 4632 Sayılı Kanun'a Eklenen Ek 2. Maddenin Beşinci Fıkrasının Dokuzuncu Cümlesinin İncelenmesi

1. Genel Açıklama

32. Dava konusu kuralın yer aldığı fıkrada, cayma hakkını kullanmayan katılımcının birikimine eklenecek devlet katkısı, bu katkı miktarının hesaplanma yöntemi ve oranı, katkı paylarının takip ve tahsil sorumluluğu, katılımcı katkı payının takip ve tahsili ile devlet katkı payının hesaplanması için ihtiyaç duyulan verilerin paylaşılması ve paylaşılma kapsam ve usulü düzenlenmektedir. Kuralda ise paylaşılması öngörülen verilerden kişisel nitelikte olanların veri sahibinin rızası aranmaksızın ilgili kuruluşlar arasında paylaşılacağı ve bu paylaşımın kişisel verilerin korunmasına ilişkin mevzuat hükümlerine aykırılık oluşturmayacağı belirtilmektedir.

33. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3. maddesinde kişisel veri, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" şeklinde tanımlanmış; 6. maddesinin (1) numaralı fıkrasında da özel nitelikli kişisel veri "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir." biçiminde ifade edilmiştir. Bu itibarla dava konusu kural kapsamında paylaşılması öngörülen veriler "çalışan katkı payının takip ve tahsili ile Devlet katkısının hesaplanması için ihtiyaç duyulan veriler" olarak belirlendiğinden bu bilgilerin 6698 sayılı Kanun kapsamında kaldığı ve özel nitelikli olmayan kişisel veriler olduğu şüphesizdir. Ayrıca bu veriler, yalnızca "çalışan katkı payının takip ve tahsili" ve "Devlet katkı payının hesaplanması" amacıyla paylaşılabilir.

34. Dava konusu kurala göre kişisel verilerin paylaşılması, OK-BES'in işleyişinde yetki ve görev üstlenen organlar ile emeklilik şirketleri arasında söz konusudur. Bu bağlamda, devlet katkı payını hesaplama, Müsteşarlığa bildirme ve devlet katkı payını ilgili emeklilik şirketine aktarma yetkilisi olan ve emeklilik şirketlerini günlük izleme sorumluluğu bulunan emeklilik gözetim merkezi, çalışan katkı payının takip ve tahsil sorumluluğu ile yetkilendirilecek kuruluş ve katılımcı birikimlerini işleten, devreden veya devralan emeklilik şirketleri arasında bilgi paylaşımının hızlı ve düzenli olmasının katılımcıların ekonomik güvenceleri yönünden önemli olduğu anlaşılmaktadır.

2. İptal Talebinin Gerekçesi

35. Dava dilekçesinde özetle, kişisel verilerin veri sahibinin rızası aranmaksızın ilgili kuruluşlar arasında paylaşılacağı, paylaşılacak verilerin kapsamı, niteliği, paylaşım amacının sınırları, bu süreçlerin denetimi ve veri sahibinin bu konularda bilgilendirilmesi konularının açık ve anlaşılır bir şekilde düzenlenmediği, mevcut düzenlemenin hedeflenen amacın ötesinde özel hayatın ve kişisel bilgilerin gizliliğinin keyfi şekilde ihlal edilmesi ve Anayasa'nın sözüne ve ruhuna, ülkemizin taraf olduğu ve uymakla yükümlü bulunduğu uluslararası sözleşmelere aykırılık sonucunu doğurduğu, böylece hukuki belirsizlik oluştuğu ve özel hayatın korunması hakkına yönelik ölçüsüz bir sınırlama getirildiği belirtilerek kuralın Anayasa'nın 2., 13., 20. ve 90. maddelerine aykırı olduğu ileri sürülmüştür.

3. Anayasa'ya Aykırılık Sorunu

36. Dava konusu kural, çalışan katkı payının takip ve tahsili ile devlet katkısının hesaplanması için ihtiyaç duyulan verilerden kişisel nitelikte olanların veri sahibinin açık rızasının alınmasına gerek olmaksızın ilgili kuruluşlar arasında paylaşılabilmesini ve veri paylaşımının kişisel verilerin korunmasına ilişkin mevzuat hükümlerine aykırılık teşkil etmeyeceğini öngörmektedir.

37. Anayasa'nın 2. maddesinde belirtilen hukuk devletinin ön koşulları arasında hukuki güvenlik ile belirlilik ilkeleri bulunmaktadır. Kişilerin hukuki güvenliğini sağlamayı amaçlayan hukuki güvenlik ilkesi; hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar. Belirlilik ilkesi ise yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olmasını, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesini ifade etmektedir. Belirtilen ilkeler doğrultusunda aktarılabilecek kişisel verilerin neden ve hangi gerekçeyle temin edileceğine ilişkin olarak konu ve amaç sınırlamasının yapılması suretiyle bu verilerin kapsamının ve ne şekilde kullanılacağına belirli olması gerekmektedir.

38. Anayasa'nın 20. maddesinin birinci fıkrasında herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı vurgulanmış; ikinci fıkrasında, özel hayatın gizliliğine çeşitli sebeplere bağlı kalınarak sınırlamalar getirilebileceği belirtilmiş bu hakkın mutlak olmadığı kabul edilmiş; üçüncü fıkrasında ise herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı ifade edilmiştir. Ayrıca maddede kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir.

39. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi veya aktarılması sırasında korumayı amaçlamaktadır. Ancak bu hak sınırsız olmayıp kanunda öngörülen hâllerde temel hak ve özgürlüklerin sınırlandırılması rejimini belirleyen Anayasa'nın 13. maddesindeki güvencelere uygun biçimde sınırlandırılabilir.

40. Anayasa'nın 13. maddesi uyarınca özel hayatın gizliliği ve kişisel verilerin korunması hakları, yalnızca kanunla ve demokratik bir toplumda gerekli olduğu ölçüde sınırlanabilir. Ayrıca getirilen bu sınırlamalar, hakkın özüne dokunamayacağı gibi Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamaz.

41. Kural uyarınca OK-BES'e dâhil olan katılımcıların katkı paylarının takip ve tahsil edilmesi ve devlet katkı payının hesaplanması için gerekli olan kişisel verileri, veri sahibinin açık rızasının alınmasına gerek olmaksızın ilgili kuruluşlar arasında paylaşılacak ve bu veri paylaşımı, kişisel verilerin korunmasına ilişkin mevzuat hükümlerine aykırılık teşkil etmeyecektir. Kural kapsamında paylaşımına konu olabilecek kişisel veriler, çalışan katkı payının takip ve tahsili ile devlet katkı payının hesaplanması için ihtiyaç duyulan verilerle sınırlı olup söz konusu veriler yalnızca emeklilik gözetim merkezi, takip ve tahsil sorumluluğu ile yetkilendirilecek kuruluş ve ilgili emeklilik şirketleri arasında paylaşılacaktır.

42. Kuralda; paylaşılacak kişisel verilerin kapsamı, temin edilme sebebi ve amacı, kullanılma şekli ile paylaşım yapabilecek kurum ve kuruluşların açıkça belirlenmiş ve kişisel verilerin usulsüz olarak paylaşılması hâline ilişkin olarak kanuni güvence tanınmış olması nedeniyle söz konusu kuralın belirlilik ve hukuki güvenlik ilkelerine aykırılık teşkil ettiği söylenemez.

43. Diğer yandan OK-BES'e dâhil olan katılımcıların katkı paylarının takip ve tahsil edilmesi ile devlet katkı payının hesaplanması için gerekli olan kişisel verilerin ilgili kuruluşlar arasında paylaşılabilmesinin belirtilmesi nedeniyle kuralla özel hayatın gizliliği ve kişisel verilerin korunması haklarına bir sınırlama getirildiği açıktır. Ancak bu sınırlamayla OK-BES'in işleyişinde aktif rol üstlenen emeklilik gözetim merkezine, takip ve tahsil sorumluluğu ile yetkilendirilecek kuruluşuna ve ilgili emeklilik şirketlerine 4632 sayılı Kanun hükümleriyle verilen görevlerin yani katılımcıların ve devletin ekonomik menfaatlerinin korunmasının, yüksek katımlı ve yoğun işlemlerle sistemde aksaklıkların yaşanmamasının, toplumsal güvene olumsuz biçimde yansıtacak sistem hatalarının doğurabileceği makro ekonomik sonuçların önüne geçme görev ve sorumluluğunun yerine getirilmesinin, dolayısıyla kamu düzeninin sağlanmasının amaçlandığı gözetildiğinde söz konusu sınırlamanın "demokratik toplum düzeninin gerekleri"ne aykırılık taşımadığı açıktır.

44. Anılan kapsamda düzenleme yapılırken "çalışan katkı payının takip ve tahsili ile Devlet katkı payının hesaplanması için ihtiyaç duyulan verilerin" paylaşılacağı belirtilmek suretiyle paylaşılacak kişisel verilerin kapsamı ve paylaşılma amacı ile paylaşımında bulunabilecek kurum ve kuruluşların da emeklilik gözetim merkezi, takip ve tahsil sorumluluğu ile yetkilendirilecek kuruluş ve ilgili emeklilik şirketleri biçiminde açık ve sınırlı bir şekilde belirlenmiş olması nedeniyle kural, sınırlamada kullanılan araç ile hakkın özüne dokunmamakta; amaca uygun dengeli bir orantı oluşturmakta; kamu düzeninin korunması şeklindeki kamu yararı ile kişisel verilerin korunması hakkı arasında makul bir denge kurmaktadır.

45. Öte yandan Kanun'un 23. maddesinin altıncı, yedinci ve sekizinci fıkralarında katılımcılara ait bilgiler "sır" olarak nitelendirilmiş, sistemde görev alan kişi ya da kuruluş mensuplarının sistemin işleyiş sürecinde elde ettiği sırların herhangi bir şekilde açıklanması, kişisel menfaatlerde kullanılması eylemleri suç olarak düzenlenerek cezai yaptırımlara bağlanmıştır. Bu fiillerin sırrı öğrenen kişi tarafından kendi yararına işlenmesi hâlleri ise cezayı ağırlaştırıcı neden olarak öngörülmüştür. Aynı şekilde 5237 sayılı Türk Ceza Kanunu'nun 136. maddesi uyarınca da kişisel verileri hukuka aykırı olarak başkasına vermek, yaymak veya ele geçirmek suç olarak düzenlenmiştir.

46. Anılan hükümlerle dava konusu kural kapsamında elde edilecek bilgilerin amacı dışında kullanılmasını ve kişilerin özel hayatına dair bilgileri ile kişisel verilerin ifşa edilmesini önleyecek kanuni güvencenin sağlandığı da görülmektedir.

47. Diğer taraftan kuralla kişisel verilerin korunmasına ilişkin mevzuat hükümlerinin ve bu bağlamda konuyla ilgili temel kanun olan 6698 sayılı Kanun'un tamamen uygulama dışında bırakıldığı da söylenemez. Kural, paylaşılması öngörülen kişisel verilerin paylaşılma şartlarını kişisel verilerin

korunmasına ilişkin mevzuattan bağımsız olarak düzenlemekte; buna karşılık kişisel verilerin güvenliğine, tarafların hak ve yükümlülüklerine ilişkin hususlarda kişisel verilerin korunmasına ilişkin mevzuat hükümlerinin uygulanmayacağına yönelik bir hüküm öngörmemektedir. Bu itibarla kişisel verilerin korunmasına ilişkin mevzuatın ve bu kapsamda 6698 sayılı Kanun'un dava konusu kuralla açıkça bağışık tutulmuş konu haricindeki diğer hükümlerinin uygulanmasına engel bir durum bulunmamaktadır.

48. Bu yönleriyle kuralla özel hayatın gizliliği ve kişisel verilerin korunması haklarına getirilen sınırlamanın söz konusu hakların özünü zedelediğinden söz edilemeyeceği gibi demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı düştüğü de söylenemez.

49. Açıklanan nedenlerle kural Anayasa'nın 2., 13. ve 20. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

50. Kuralın Anayasa'nın 90. maddesiyle ilgisi görülmemiştir.

E. Kanun'un 2. Maddesiyle 4632 Sayılı Kanun'a Eklenen Geçici 2. Maddenin İncelenmesi

51. Dava konusu kuralda, 6770 sayılı Kanun'un 19. maddesiyle değişiklik yapılmıştır. Bu nedenle konusu kalmayan maddeye ilişkin iptal talebi hakkında karar verilmesine yer olmadığına karar vermek gerekir.

IV. YÜRÜRLÜĞÜN DURDURULMASI TALEBİ

52. Dava dilekçesinde özetle, dava konusu kuralın uygulanması hâlinde Anayasal ilkelerin ihlal edilmiş olacağı ve telafisi imkânsız zararların doğacağı, yürürlüğün durdurulması kararı verilmeden daha sonra verilecek bir iptal kararının etkisiz kalmasının muhtemel olacağı, yürürlüğün durdurulması kararının hukuk sisteminde herhangi bir boşluk oluşturmayacağı belirtilerek kuralın yürürlüğünün durdurulması talep edilmiştir.

10.8.2016 tarihli ve 6740 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanununda Değişiklik Yapılmasına Dair Kanun'un;

A. 1. maddesiyle 28.3.2001 tarihli ve 4632 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanunu'na eklenen ek 2. maddenin;

1. Birinci fıkrasının;

a. İkinci cümlesinde yer alan "...Müsteşarlıkça uygun görülen..." ibaresine,

b. Üçüncü cümlesine,

2. Beşinci fıkrasının dokuzuncu cümlesine,

yönelik iptal talepleri, 28.12.2017 tarihli ve E.2016/179, K.2017/176 sayılı kararlarla reddedildiğinden bu ibare ve cümlelere ilişkin yürürlüğün durdurulması taleplerinin REDDİNE,

B. 1. 1. maddesiyle 4632 sayılı Kanun'a eklenen ek 2. maddenin birinci fıkrasının birinci cümlesi,

2. 2. maddesiyle 4632 sayılı Kanun'a eklenen geçici 2. maddesi,

hakkında 28.12.2017 tarihli ve E.2016/179, K.2017/176 sayılı kararlarla karar verilmesine yer olmadığına karar verildiğinden bu cümle ve maddeye ilişkin yürürlüğün durdurulması talepleri hakkında **KARAR VERİLMESİNE YER OLMADIĞINA,**

28.12.2017 tarihinde OYBİRLİĞİYLE karar verilmiştir.

V. HÜKÜM

10.8.2016 tarihli ve 6740 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanununda Değişiklik Yapılmasına Dair Kanun'un;

A. 1. maddesiyle 28.3.2001 tarihli ve 4632 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanunu'na eklenen ek 2. maddenin;

1. Birinci fıkrasının;

a. Birinci cümlesi, 18.1.2017 tarihli ve 6770 sayılı Kanun'un 18. maddesiyle değiştirildiğinden, konusu kalmayan bu cümleye ilişkin iptal talebi hakkında **KARAR VERİLMESİNE YER OLMADIĞINA,**

b. İkinci cümlesinde yer alan "...Müsteşarlıkça uygun görülen..." ibaresinin Anayasa'ya aykırı olmadığına, iptal talebinin REDDİNE,

c. Üçüncü cümlesinin Anayasa'ya aykırı olmadığına, iptal talebinin REDDİNE,

2. Beşinci fıkrasının dokuzuncu cümlesinin Anayasa'ya aykırı olmadığına, iptal talebinin REDDİNE,

B. 2. maddesiyle 4632 sayılı Kanun'a eklenen geçici 2. maddesi, 18.1.2017 tarihli ve 6770 sayılı Kanun'un 19. maddesiyle değiştirildiğinden, konusu kalmayan bu maddeye ilişkin iptal talebi hakkında **KARAR VERİLMESİNE YER OLMADIĞINA,**

28.12.2017 tarihinde OYBİRLİĞİYLE karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili - Burhan ÜSTÜN

Başkanvekili - Engin YILDIRIM

Üye: Serdar ÖZGÜLDÜR; Serruh KALELİ; Osman Alifeyyaz PAKSÛT; Recep KÖMÛRCÛ; Nuri NECİPOĞLU; Hicabi DURSUN; Celal Mümtaz AKINCI; Muammer TOPAL; M. Emin KUZ; Hasan Tahsin GÖKCAN; Kadir ÖZKAYA; Rıdvan GÜLEÇ; Recai AKYEL; Yusuf Şevki HAKYEMEZ

**Anayasa Mahkemesi - 5809 sayılı Elektronik Haberleşme Kanunu Kararı (Revize-Madde 51) (E.
2015/61)**

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2015/61

Karar Sayısı: 2016/172

Karar Tarihi: 2.11.2016

R.G. Tarih-Sayı: 9.12.2016-29913

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri M. Akif HAMZAÇEBİ, Engin ALTAY ve Levent GÖK ile birlikte 121 milletvekili

İPTAL DAVASININ KONUSU: 27.3.2015 tarihli ve 6639 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun'un;

A- 4. maddesiyle değiştirilen, 24.5.2013 tarihli ve 6487 sayılı Bazı Kanunlar ile 375 Sayılı Kanun Hükmünde Kararnamede Değişiklik Yapılması Hakkında Kanun'un 33. maddesinin (4) numaralı fıkrasının;

1- Birinci cümlesinde yer alan "...10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununun 29 uncu maddesi hükmüne tabi olmaksızın..." ibaresinin,

2- İkinci cümlesinin "...takip eden yıllarda ise her takvim yılı başından geçerli olmak üzere o yıl için 4/1/1961 tarihli ve 213 sayılı Vergi Usul Kanununun mükerrer 298 inci maddesi hükümleri uyarınca tespit ve ilan edilen yeniden değerlendirme oranında artırılarak..."bölümünün,

B- 5. maddesiyle 28.3.1983 tarihli ve 2809 sayılı Yükseköğretim Kurumları Teşkilatı Kanunu'na eklenen ek 158. maddenin;

1- İkinci fıkrasının;

a- Birinci cümlesinde yer alan "...ile Mütevelli Heyetinden..." ibaresinin,

b- İkinci, üçüncü, dördüncü ve beşinci cümlelerinin,

c- Altıncı cümlesinde yer alan "Mütevelli Heyetinin" ibarelerinin,

2- Üçüncü fıkrasının,

3- Dördüncü fıkrasının üçüncü cümlesinde yer alan "Mütevelli Heyetinin teklifi ve..." ibaresinin,

4- Beşinci ve altıncı fıkralarının,

C- 18. maddesiyle 14.3.2013 tarihli ve 6446 sayılı Elektrik Piyasası Kanunu'na eklenen geçici 18. maddenin,

D- 22. maddesiyle 3.6.2011 tarihli ve 638 sayılı Gençlik ve Spor Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'ye eklenen geçici 13. maddenin (1) numaralı fıkrasının birinci cümlesinde yer alan "...Bakanlık Merkez Teşkilatı ile Spor Genel Müdürlüğü ve..." ibaresinin,

E- 23. maddesiyle 27.6.1989 tarihli ve 375 sayılı Kanun Hükmünde Kararname'ye eklenen ek 18. maddenin birinci, ikinci ve üçüncü fıkralarının,

F- 24. maddesiyle 375 sayılı Kanun Hükmünde Kararname'nin eki (I) sayılı Cetvelin "A- Aylıklarını 657 sayılı Devlet Memurları Kanununa Göre Alanlar" kısmının "1-Kadroları Genel İdare Hizmetleri Sınıfında yer alan personel ile Teknik Hizmetler, Sağlık ve Yardımcı Sağlık Hizmetleri ile Avukatlık Hizmetleri sınıflarında bulunan personelden ek ödeme oranları ilgili gruplarında düzenlenmeyen ve kadro unvanları bu bölümde yer alan personel" bölümünün;

1- (d) sırasında yer alan "büyükşehir belediyesi bulunan illerin il özel idaresi genel sekreter yardımcısı, diğer illerin il özel idaresi genel sekreteri," ibaresinin "il özel idaresi genel sekreteri," şeklinde değiştirilmesinin,

2- (e) sırasında yer alan "büyükşehir belediyesi bulunan illerin il özel idaresi I. hukuk müşaviri, büyükşehir belediyesi bulunmayan illerin il özel idaresi genel sekreter yardımcısı," ibaresinin "il özel idaresi genel sekreter yardımcısı," şeklinde değiştirilmesinin,

3- (g) sırasına "il yazı işleri müdürü" ibaresinden önce gelmek üzere eklenen "İl nüfus ve vatandaşlık müdürü," ibaresinin,

G- 28. maddesiyle 4.11.1983 tarihli ve 2942 sayılı Kamulaştırma Kanunu'nun 4. maddesinin ikinci fıkrasının birinci cümlesine "raylı taşıma sistemleri" ibaresinden sonra gelmek üzere eklenen "ile tünel" ibaresinin,

H- 29. maddesiyle 4.5.2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'a eklenen 8/A maddesinin (1) ve (2) numaralı fıkralarının,

I- 32. maddesiyle 5.11.2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'nun yeniden düzenlenen 51. maddesinin;

1- (2) numaralı fıkrasında yer alan "...ilgili mevzuatın ve..." ibaresinin,

2- (6) numaralı fıkrasında yer alan "...ilgili mevzuat hükümleri saklı kalmak kaydıyla,..." ibaresinin,

3- (8) numaralı fıkrasının ikinci cümlesinde yer alan "...İlgili mevzuatın ve..." ibaresinin,

4- (13) numaralı fıkrasının,

Anayasa'nın 2., 5., 10., 13., 20., 22., 26., 28., 35., 36., 40., 46., 55., 70., 87., 90., 123., 125., 128., 130., 132., 138., 153., 161., 162. ve 172. maddelerine aykırılığı ileri sürülerek iptallerine ve yürürlüklerinin durdurulmasına karar verilmesi talebidir.

I- İPTALİ İSTENİLEN KANUN HÜKÜMLERİ

İptali istenilen kuralların yer aldığı 6639 sayılı Kanun'un;

1- 4. maddesiyle değiştirilen 6487 sayılı Kanun'un 33. maddesinin (4) numaralı fıkrası şöyledir:

"(4) Vakfa, amaçlarını gerçekleştirmek üzere, 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununun 29 uncu maddesi hükmüne tabi olmaksızın her yıl ocak ayı içinde aktarılmak üzere Sağlık Bakanlığı bütçesinde ödenek ayrılır. Ayrılacak bu tutar 2015 yılında 15.000.000 TL olarak, takip eden yıllarda ise her takvim yılı başından geçerli olmak üzere o yıl için 4/1/1961 tarihli ve 213 sayılı Vergi Usul Kanununun mükerrer 298 inci maddesi hükümleri uyarınca tespit ve ilan edilen yeniden değerlendirme oranında artırılarak belirlenir."

2- 5. maddesiyle 2809 sayılı Kanun'a eklenen ek 158. madde şöyledir:

"İstanbul'da Sağlık Bilimleri Üniversitesi adıyla yeni bir üniversite kurulmuştur. Bu Üniversite, Rektörlüğe bağlı olarak;

a) Tıp Fakültesi,

b) Hemşirelik Fakültesi,

c) Yaşam Bilimleri Fakültesi,

d) Sağlık Bilimleri Fakültesi,

e) Sağlık Hizmetleri Meslek Yüksek Okulu,

f) Sağlık Bilimleri Enstitüsünden,

oluşur.

Üniversitenin yönetim organları, 2547 sayılı Yükseköğretim Kanununda öngörülen organlar ile Mütevelli Heyetinden oluşur. Mütevelli Heyeti; Sağlık Bakanlığı Müsteşarı, Rektör, Sağlık Bakanının seçeceği iki üye ile Yükseköğretim Kurulu tarafından seçilen profesör unvanına sahip bir üye olmak

üzere, toplam beş üyeden oluşur. Mütevelli Heyetine Sağlık Bakanlığı Müsteşarı, Müsteşarın katılmadığı toplantılara Rektör başkanlık eder. Mütevelli Heyeti, en az dört üye ile toplanır ve salt çoğunlukla karar alır. Bakan ve Yükseköğretim Kurulu tarafından seçilen üyelerin görev süresi dört yıldır. Mütevelli Heyetinin çalışma usul ve esasları, Mütevelli Heyetinin teklifi üzerine Yükseköğretim Kurulu tarafından belirlenir.

Mütevelli Heyetinin görevleri şunlardır:

- a) Üniversitenin stratejik planını ve bütçe teklifini onaylamak.
- b) Kamu kurum ve kuruluşları ve gerçek ve özel hukuk tüzel kişileriyle iş birliği yapılmasına ve ortak projeler yürütülmesine karar vermek.
- c) Yurt içinde ve yurt dışında Üniversiteye ait birimlerin ve bölümlerin kurulmasını teklif etmek.
- d) Rektör tarafından gündeme alınması önerilen konularda karar vermek.

Üniversite, Birleşmiş Milletlerin resmî dil olarak kabul ettiği diller öncelikli olmak üzere, yabancı dilde eğitim veren program açma, yabancı yükseköğretim kurumları ile ortak program yürütme de dâhil olmak üzere yurt dışındaki yükseköğretim kurumlarıyla her türlü iş birliğine dair protokol yapabilir. Yabancı dilde eğitim veren programlara, yurt dışından öğrenci kabul edilebilir. Mütevelli Heyetinin teklifi ve Yükseköğretim Kurulunun uygun görüşü üzerine Bakanlar Kurulu kararı ile yurt dışında Üniversiteye ait birimler kurulabilir. Yurt dışında eğitim yapılabilmesi ve personel istihdam edilebilmesi ile bu birimlerde görevlendirilecek öğretim elemanlarına yapılacak ödemeler, Maliye Bakanlığının uygun görüşü alınarak Üniversite Yönetim Kurulunun belirleyeceği usul ve esaslara göre yapılır.

Üniversite, Türkiye Kamu Hastaneleri Kurumuna bağlı eğitim ve araştırma hastaneleriyle 7/5/1987 tarihli ve 3359 sayılı Sağlık Hizmetleri Temel Kanununun ek 9 uncu maddesi çerçevesinde birlikte kullanım protokolleri yaparak sağlık uygulama ve araştırma faaliyetlerini yürütür. Üniversitenin birlikte kullanım protokolü imzaladığı eğitim ve araştırma hastaneleri, aynı zamanda Üniversitenin uygulama ve araştırma merkezi statüsü kazanır. Üniversiteye tahsis edilecek öğretim elemanı kadroları, temel bilimler hariç olmak üzere, birlikte kullanılan eğitim ve araştırma hastanesinin eğitim birimleri ve ihtiyacı dikkate alınarak, Rektörün önerisi üzerine Mütevelli Heyeti tarafından il bazında belirlenir ve öğretim üyesi atamaları bu kadrolara yapılır. Üniversitenin birimlerine tahsis edilecek öğretim üyesi norm kadro sayısı, Rektörün önerisi ve Mütevelli Heyetinin onayı ile Yükseköğretim Kurulu tarafından tespit edilir.

Mekteb-i Tıbbiyye-i Şâhâne adıyla hizmet vermek üzere inşa edilen ve hâlen Marmara Üniversitesi adına tahsisli olan Haydarpaşa Kampüsü, Sağlık Bilimleri Üniversitesine tahsis edilmiştir.

3- 18. maddesiyle 6446 sayılı Kanun'a eklenen geçici 18. madde şöyledir:

“(1) 1/1/2016 tarihine kadar, teknik ve teknik olmayan kayıplarının oranı ülke ortalamasının üzerinde olan dağıtım bölgelerinde, diğer dağıtım bölgelerinden farklı düzenlemeler yapılmasına, hedef kayıp-kaçak oranlarının bir önceki yılın gerçekleşmeleri dikkate alınarak ve sonraki uygulama dönemleri de dâhil olmak üzere yeniden belirlenmesine Kurul yetkilidir.”

4- 22. maddesiyle 638 sayılı Kanun Hükmünde Kararname'ye eklenen geçici 13. maddenin (1) numaralı fıkrası şöyledir:

“(1) Bu maddenin yürürlüğe girdiği tarihte; Bakanlık Merkez Teşkilatı ile Spor Genel Müdürlüğü ve Yüksek Öğrenim Kredi ve Yurtlar Kurumu Genel Müdürlüğünde; Genel Müdür Yardımcısı, Müşavir, Teftiş Kurulu Başkanı, I. Hukuk Müşaviri, Müstakil/Unvanlı Daire Başkanı, Daire Başkanı, Bölge Müdürü, Bölge Müdür Yardımcısı, Gençlik Hizmetleri ve Spor İl Müdürü, Gençlik Hizmetleri ve Spor İlçe Müdürü, Federasyon Genel Sekreteri, Yurt Müdürü ve Gençlik Merkezi Müdürü kadrolarında bulunanların görevleri hiçbir işleme gerek kalmaksızın sona erer. Bu fıkroda sayılanlar Araştırmacı kadrolarına hâlen buldukları kadro dereceleriyle hiçbir işleme gerek kalmaksızın atanmış sayılır. Ancak, ilgililerin önceki kadroları ile atandıkları yeni kadro arasında mali haklar bakımından bir fark bulunması durumunda bu fark, 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanununun 91 inci maddesinin ikinci fıkrasında düzenlenen usul ve esaslar çerçevesinde aradaki fark kapanıncaya kadar ödenir. Araştırmacı kadro veya pozisyonları atama işleminin yapıldığı tarihte hiçbir işleme gerek kalmaksızın ihdas edilmiş ve herhangi bir sebeple boşalması hâlinde hiçbir işleme gerek kalmaksızın iptal edilmiş sayılır.”

5- 23. maddesiyle 375 sayılı Kanun Hükmünde Kararname'ye eklenen ek 18. maddenin birinci, ikinci ve üçüncü fıkraları şöyledir:

“22/5/2003 tarihli ve 4857 sayılı İş Kanunu ile 27/7/1967 tarihli ve 926 sayılı Türk Silâhlı Kuvvetleri Personel Kanunu hariç olmak üzere, tabi oldukları personel kanununa bakılmaksızın Başbakanlık, bakanlıklar, bağlı ve ilgili kuruluşlar ile başkan ve üyeleri hariç olmak üzere 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununa ekli (III) sayılı Cetvelde sayılan düzenleyici ve denetleyici kurumlar ve Tasarruf Mevduatı Sigorta Fonunda;

a) Görevden alınan veya görev süreleri sona eren müsteşarlar ile ek göstergesi 7600 ve daha yüksek tespit edilen yönetici kadrolarında bulunanlar Başbakanlık merkez müşaviri kadrolarına, ek göstergesi 7000 olan yönetici kadrolarında bulunanlar Başbakanlık müşaviri kadrolarına,

b) (a) bendinde belirtilenler hariç olmak üzere ek göstergesi 6400 ve daha yüksek tespit edilen yönetici kadrolarında veya pozisyonlarında bulunanlardan Başbakanlık Merkez Teşkilatı ile bağlı ve ilgili kuruluşlarında olanlar görevden alındıklarında veya görev süreleri sona erdiğinde Başbakanlık müşaviri, bakanlık merkez teşkilatları ile bağlı ve ilgili kuruluşlarında olanlar bakanlığın müşavir kadrolarına, düzenleyici ve denetleyici kurumlar ile Tasarruf Mevduatı Sigorta Fonunda olanlar kurumlarının müşavir veya danışman kadro veya pozisyonlarına,

c) Ek göstergeleri 3600 (dâhil) ila 6400 (hariç) olarak tespit edilen yönetici kadro veya pozisyonlarında bulunanlar görevden alındıklarında veya görev süreleri sona erdiğinde;

1) Daha önce 657 sayılı Kanunun 36 ncı maddesinin “Ortak Hükümler” bölümünün (A) fıkrasının (11) numaralı bendinde sayılan merkez teşkilatına ait kadrolar ile mesleğe alınmaları, yetiştirilmeleri ve yeterlilikleri aynı veya benzer nitelik arz eden merkez teşkilatına ait kadro veya pozisyonlarda bulunanlar daha önceki bu kadro veya pozisyonlarına,

2) Daha önce (1) numaralı alt bentte belirtilen kadrolarda bulunmayanlardan ek göstergesi 3600 (dâhil) ila 6400 (hariç) olarak tespit edilen yönetici kadro veya pozisyonlarında toplam en az üç yıl görev yapmış olanlar ilgili kuruma ait (1) numaralı alt bentte yer alan kadro veya pozisyonlardan kurumlarınca tespit edilmiş olan kadro veya pozisyonlarına,

3) (2) numaralı alt bentte belirtilenlerden üç yıldan az görev yapmış olanlar, bu maddeye göre ihdas edilmiş sayılan merkez veya taşra teşkilatına ait araştırmacı kadro veya pozisyonlarına,

ç) Ek göstergesi 3600'den daha düşük tespit edilen yönetici kadro veya pozisyonlarında bulunanlar görevden alındıklarında veya görev süreleri sona erdiğinde;

1) Daha önce 657 sayılı Kanunun 36 ncı maddesinin “Ortak Hükümler” bölümünün (A) fıkrasının (11) numaralı bendinde sayılan kadrolar ile mesleğe alınmaları, yetiştirilmeleri ve yeterlilikleri aynı veya benzer nitelik arz eden kadro veya pozisyonlarda bulunanlar daha önceki bu kadro veya pozisyonlarına,

2) Diğerleri, bu maddeye göre ihdas edilmiş sayılan merkez veya taşra teşkilatına ait araştırmacı kadro veya pozisyonlarına,

atanırlar. Bu şekilde atananlardan bir ay içinde talepte bulunanlar, atamaya yetkili amirler tarafından bu fıkra kapsamında yer alan yönetici kadro veya pozisyonları dışındaki daha önce buldukları veya öğrenim durumları itibarıyla ihraz etmiş oldukları unvanlara ilişkin kadro veya pozisyonlara bir ay içinde atanırlar.

Birinci fıkra kapsamında atananlar ile anılan fıkranın son cümlesi uyarınca talep üzerine yapılacak atamalar için uygun boş kadro veya pozisyon bulunmaması hâlinde, bunlar için başka bir işleme gerek kalmaksızın, söz konusu kadro veya pozisyonlar ihdas edilmiş ve kurumların kadro veya pozisyon cetvellerinin ilgili bölümlerine eklenmiş sayılır. Bu şekilde ihdas edilmiş sayılan kadro ve pozisyonlar boşalması hâlinde, herhangi bir işleme gerek kalmaksızın iptal edilmiş sayılır. Anılan kadro ve pozisyonlara atananlar, atamaya yetkili amirleri tarafından belirlenen birimlerde istihdam edilir.

Birinci fıkra hükmü kapsamında atananlardan birinci fıkra kapsamında yer alan yönetici kadro veya pozisyonlarında kesintisiz olarak en az iki yıl fiilen görev yapmış olanların mali hakları, atandıkları söz konusu kadro veya pozisyonlarda bulunmaları kaydıyla, atandıkları tarihi takip eden ay başından itibaren ikinci yılın sonuna kadar fiili çalışmaya bağlı ödemeler hariç, önceki görevine ait ödeme unsurları esas alınarak verilmeye devam edilir.”

6- 24. maddesiyle değiştirilen 375 sayılı Kanun Hükmünde Kararname'nin eki (I) sayılı cetvelin “A- Aylıklarını 657 sayılı Devlet Memurları Kanununa Göre Alanlar” kısmının, “1- Kadroları Genel İdare Hizmetleri Sınıfında yer alan personel ile Teknik Hizmetler, Sağlık ve Yardımcı Sağlık Hizmetleri ile Avukatlık Hizmetleri sınıflarında bulunan personelden ek ödeme oranları ilgili gruplarında düzenlenmeyen ve kadro unvanları bu bölümde yer alan personel” bölümünün (d), (e) ve (g) sıraları şöyledir:

“(I) SAYILI CETVEL

EK ÖDEME ORANLARI

Ek Ödeme Oranı

(%)

Kadro ve Görev Unvanı

d) Genel müdür yardımcısı, il özel idaresi genel sekreteri, büyükşehir belediyesi genel sekreter yardımcısı, ek göstergeleri genel müdür yardımcısı düzeyinde veya daha yüksek tespit edilen I. hukuk müşaviri, başkan yardımcısı ve kurum ve kurul başkanı unvanlı kadrolarda bulunanlar

e) Daire Başkanı, kadrolu yönetim kurulu üyesi, genel sekreter, İş Sağlığı ve Güvenliği Araştırma ve Geliştirme Enstitüsü Başkanı, il özel idaresi genel sekreter yardımcısı, diğer I. hukuk müşaviri, il belediye başkan yardımcısı

g) (...), İl nüfus ve vatandaşlık müdürü, il yazı işleri müdürü, il idare kurulu müdürü, il mahalli idare müdürü, il planlama ve koordinasyon müdürü, dernekler il müdürü, il afet ve acil durum müdürü, hukuk müşaviri, fakülte ve yüksekokul sekreteri, basın ve halkla ilişkiler müşaviri, basın müşaviri, müşavir, müdür, şube müdürü, ilçe müftüsü, başkan, daire başkan yardımcısı, kurum sekreteri, merkez sekreteri, enstitü sekreteri, genel sekreter yardımcısı, tiyatro müdür yardımcısı, Atatürk Kültür Merkezi müdür yardımcısı, opera ve bale müdür yardımcısı, (1) birlik sekreteri, müze başkanı, KİT'lerde başuzman, diğer belediye başkan yardımcıları ve (f) sırasında sayılanların yardımcıları

7- 28. maddesiyle 2942 sayılı Kanun'un değişiklik yapılan 4. maddesi şöyledir:

"İrtifak hakkı kurulması

Madde 4- Taşınmaz malın mülkiyetinin kamulaştırılması yerine, amaç için yeterli olduğu takdirde taşınmaz malın belirli kesimi, yüksekliği, derinliği veya kaynak üzerinde kamulaştırma yoluyla irtifak hakkı kurulabilir.

(Ek fıkra : 10/9/2014 - 6552/99 md.) Ancak, maliklerinin mülkiyet hakkının kullanılmasının engellenmemesi, can ve mal güvenliği bakımından gerekli önlemlerin alınması kaydıyla, kamu yararına dayalı olarak taşınmazların üstünde teleferik ve benzeri ulaşım hatları ile her türlü köprü, taşınmazların altında metro ve benzeri raylı taşıma sistemleri ile tünel yapılabilir. Taşınmazların mülkiyet hakkının kullanımının engellenmemesi hâlinde, taşınmazlara ilişkin herhangi bir kamulaştırma yapılmaz. Yapılan yatırım nedeniyle taşınmaz maliklerinden değer artış bedeli alınmaz."

8- 29. maddesiyle 5651 sayılı Kanun'a eklenen 8/A maddesinin (1) ve (2) numaralı fıkraları şöyledir:

"(1) Yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması sebeplerinden bir veya bir kaçına bağlı olarak hâkim veya gecikmesinde sakınca bulunan hâllerde, Başbakanlık veya millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması

ile ilgili bakanlıkların talebi üzerine Başkanlık tarafından internet ortamında yer alan yayınla ilgili olarak içeriğin çıkarılması ve/veya erişimin engellenmesi kararı verilebilir. Karar, Başkanlık tarafından derhâl erişim sağlayıcılara ve ilgili içerik ve yer sağlayıcılara bildirilir. İçerik çıkartılması ve/veya erişimin engellenmesi kararının gereği, derhâl ve en geç kararın bildirilmesi anından itibaren dört saat içinde yerine getirilir.

(2) Başbakanlık veya ilgili Bakanlıkların talebi üzerine Başkanlık tarafından verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararı, Başkanlık tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi hâlde, karar kendiliğinden kalkar.”

9- 32. maddesiyle 5809 sayılı Kanun'un yeniden düzenlenen 51. maddesi şöyledir:

“Kişisel verilerin işlenmesi ve gizliliğin korunması

MADDE 51- (1) Kişisel verilerin işlenmesinde; hukuka ve dürüstlük kurallarına uygun olması, doğru ve gerektiğinde güncel olması, belirli, açık ve meşru amaçlar için işlenmesi, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ile işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi ilkelerine uyulur.

(2) Elektronik haberleşmenin ve ilgili trafik verisinin gizliliği esas olup, ilgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi yasaktır.

(3) Elektronik haberleşme şebekeleri, haberleşmenin sağlanması dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla işletmeciler tarafından ancak ilgili abonelerin/kullanıcıların verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve açık rızalarının alınması kaydıyla kullanılabilir.

(4) İşletmeciler şebekelerinin, abonelerine/kullanıcılarına ait kişisel verilerin ve sundukları hizmetlerin güvenliğini sağlamak amacıyla uygun teknik ve idari tedbirleri alır.

(5) Bu Kanununun 49 uncu maddesi kapsamında veya kamu yararının sağlanması amacıyla Kurum tarafından işletmecilere getirilen yükümlülüklerin yerine getirilebilmesi için kişisel veriler işlenebilir.

(6) Kişisel verilerin yurt dışına aktarılmasına ilişkin ilgili mevzuat hükümleri saklı kalmak kaydıyla, trafik ve konum verileri ancak ilgili kişilerin açık rızaları alınmak koşuluyla yurt dışına aktarılabilir.

(7) Trafik verileri; trafiğin yönetimi, arabağlantı, faturalama, usulsüzlük/dolandırıcılık tespitleri ve benzeri işlemleri gerçekleştirmek veya tüketici şikâyetleri ile arabağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü amacıyla sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla işlenir ve bu uzlaşmazlıkların çözüm süreci tamamlanıncaya kadar gizliliği ve bütünlüğü sağlanarak saklanır. Katma değerli elektronik haberleşme hizmetlerinin sunulması ya da elektronik haberleşme hizmetlerinin pazarlanması amacıyla ihtiyaç duyulan trafik verileri ile konum verileri anonim hâle getirilerek veya ilgili abonelerin/kullanıcıların açık rızalarının alınması ve sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla, belirtilen faaliyetlerin gerektirdiği ölçü ve sürede işlenebilir.

(8) İşletmeciler konum verilerinin işlenmesinde abonelere/kullanıcılara bu verilerin işlenmesini reddetme imkânı sağlar. İlgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde ancak acil yardım çağruları ile 29/5/2009 tarihli ve 5902 sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanunda tanımlanan afet ve acil durum hâllerinde abonelerin/kullanıcıların açık rızası aranmaksızın konum verileri ve ilgili kişilerin kimlik bilgileri işletmeci tarafından yetkilendirilen kişilerle sınırlı olmak kaydıyla işlenebilir.

(9) Abone/kullanıcı şikâyetlerinin incelenmesi ve denetim faaliyetleri kapsamında trafik ve konum verileri ile kişisel veriler, belirtilen faaliyetlerle sınırlı olmak kaydıyla işlenebilir.

(10) Bu Kanun kapsamında sunulan hizmetlere ilişkin olarak;

a) Soruşturma, inceleme, denetleme veya uzlaşmazlığa konu olan kişisel veriler ilgili süreç tamamlanıncaya kadar,

b) Kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtları iki yıl,

c) Kişisel verilerin işlenmesine yönelik abonelerin/kullanıcıların rızalarını gösteren kayıtlar asgari olarak abonelik süresince,

saklanır. Veri kategorileri ile haberleşmenin yapıldığı tarihten itibaren bir yıldan az ve iki yıldan fazla olmamak üzere verilerin saklanma süreleri yönetmelikle belirlenir.

(11) İşletmeciler, tahsilata ilişkin riskin yönetilmesi ve kötü niyetli kullanımların önlenmesi amacıyla abonelerin elektronik haberleşme hizmetlerine yönelik fatura tutarı ve ödeme bilgilerini diğer işletmecilerle paylaşabilir veya işleyebilir.

(12) Bu Kanun kapsamında kişisel verilerin gizliliğinin, güvenliğinin ve amacı doğrultusunda kullanılmasının temininden işletmeciler sorumludur.

(13) Bu maddenin uygulanmasına ilişkin usul ve esaslar Kurum tarafından belirlenir.”

II- İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Zühtü ARSLAN, Alparslan ALTAN, Burhan ÜSTÜN, Serdar ÖZGÜLDÜR, Serruh KALELİ, Recep KÖMÜRCÜ, Engin YILDIRIM, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Erdal TERCAN, M. Emin KUZ, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA ve Rıdvan GÜLEÇ'in katılımlarıyla 17.6.2015 tarihinde yapılan ilk inceleme toplantısında, dosyada eksiklik bulunmadığından işin esasının incelenmesine, yürürlüğü durdurma talebinin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

III- ESASIN İNCELENMESİ

2. Dava dilekçesi ve ekleri, Raportör Fatih ŞAHİN tarafından hazırlanan işin esasına ilişkin rapor, iptali istenilen kanun hükümleri, dayanılan ve ilgili görülen Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 43. maddesinin (1) numaralı fıkrası gereğince Sağlık Bakanı Prof. Dr. Recep AKDAĞ, Müsteşar Prof. Dr. Eyüp GÜMÜŞ, Müsteşar Yardımcısı Hüseyin ÇELİK, Sağlık Politikaları Kurulu Üyesi Av. Adem KESKİN, İ. Hukuk Müşaviri Av. Erol GÖKDÖL, Türkiye Kamu Hastaneleri Kurumu İ. Hukuk Müşaviri Av. Erol DEMİRCİ, Sağlık Bilimleri Üniversitesi Rektörü Prof. Dr. Cevdet ERDÖL, Türk Tabipleri Birliği Merkez Konseyi İkinci Başkanı Prof. Dr. Sinan ADIYAMAN, Ankara Tabip Odası Bir Önceki Dönem Başkanı Prof. Dr. Çetin ATASOY ve Hukuk Bürosu Avukatı Ziyet ÖZÇELİK'in, 20.10.2016 tarihli sözlü açıklamaları dinlendikten sonra gereği görüşülüp düşünüldü:

A- Kanun'un 4. Maddesiyle Değiştirilen 6487 Sayılı Kanun'un 33. Maddesinin (4) Numaralı Fıkrasının;

1- Birinci Cümlesinde Yer Alan "...10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununun 29 uncu maddesi hükmüne tabi olmaksızın..." İbaresinin İncelenmesi

a. İptal Talebinin Gerekçesi

3. Dava dilekçesinde özetle, dava konusu kuralla Türkiye Yeşilay Vakfına aktarılacak kamu kaynağının amacına uygun kullanılıp kullanılmadığının denetim dışı bırakılmasının kamu yararıyla bağdaşmadığı belirtilerek kuralın, Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

4. Dava konusu kuralla, Sağlık Bakanlığı bütçesinden Türkiye Yeşilay Vakfına aktarılması öngörülen ödeneğin 5018 sayılı Kanun'un 29. maddesine tâbi olmayacağı hüküm altına alınmaktadır.

5. Anayasa'nın 2. maddesinde belirtilen hukuk devleti, insan haklarına dayanan, bu hak ve özgürlükleri koruyup güçlendiren, eylem ve işlemleri hukuka uygun olan, her alanda adaletli bir hukuk düzeni kurup bunu geliştirerek sürdüren, hukuk güvenliğini sağlayan, Anayasa'ya aykırı durum ve tutumlardan kaçınan, hukuku tüm devlet organlarına egemen kılan, Anayasa ve yasalarla kendini bağlı sayan, yargı denetimine açık olan devlettir.

6. Kuvvetler ayrılığı esasına dayanan demokratik yönetim biçiminde, yürütme organına gelir toplama ve harcama yetkisi tanıyan bütçelerin yapımı, halkın temsilcilerinden oluşan yasama organının asli görevlerindedir. Yasama organı açısından aynı zamanda bir hak olan bu görev, yürütmenin bütçe ile ilgili işlemlerinin doğru, güvenilir ve kanunlara uygun bir şekilde yürütülüp yürütülmediğinin denetimini de kaçınılmaz kılmaktadır. Bu bağlamda, yasama organının, halk adına kamu gelirlerini toplama ve yine halk adına bu gelirleri harcama konusunda yürütme organına sınırları belirlenmiş yetki vermesi ve sonuçlarını denetlemesine "bütçe hakkı" denilmektedir. Anayasa'nın 87., 160., 162. ve 164. maddelerine göre bütçe hakkı Türkiye Büyük Millet Meclisi'nindir (TBMM). Bütçe, hükümetin Meclis'e karşı temel sorumluluk mekanizmasıdır. Meclis, bütçe ile hükümete gelir toplama ve gider yapma yetkisi vermekte, bu yetkinin uygun kullanılmasını da bütçe sürecinin bir parçası olan kesin hesap faaliyeti ile denetlemektedir. Bütçe uygulamalarının denetimi görevi, bütçe işlemlerinin gün geçtikçe nitelik ve nicelik itibarıyla artması ve karmaşıklaşması nedeniyle yasama organı adına tarafsız ve uzman kuruluşlar tarafından yerine getirilmektedir. Ülkemizde de bu görev, Anayasa'nın 160. maddesiyle Sayıştay'a verilmiştir. Yasama organının, yürütme organı üzerindeki bütçe denetimi büyük ölçüde Sayıştay tarafından yapılan bu denetimlere dayanmaktadır.

7. Merkezi yönetim kapsamındaki kamu idareleri, sosyal güvenlik kurumları ve mahallî idarelerden oluşan kamu idarelerinin malî yönetimi ve kontrolüne ilişkin usul ve esaslar ise 5018 sayılı Kanun'da düzenlenmiştir. Anılan Kanun'la, kamu kaynaklarının etkili, ekonomik ve verimli bir şekilde elde edilmesi, kullanılması, muhasebeleştirilmesi ve raporlanması, ayrıca kaynakların kötüye kullanımının önlenmesi için yetkili kamu görevlilerinin gerekli önlemlerin alınmasından sorumlu tutulması ve Kanun'da belirtilen yöntemlere uygun olarak kamu otoritelerine hesap vermeleri öngörülmüştür.

8. 5018 sayılı Kanun'un 29. maddesinin birinci fıkrasında, genel yönetim kapsamındaki kamu idarelerinin bütçelerinde öngörülmüş olmak kaydıyla; kamu yararı gözetilerek dernek, vakıf, birlik, kurum, kuruluş, sandık ve benzeri teşekküllere yardım yapılabileceği kural altına alınmış; ikinci

fıkrasında, bu yardımların yapılması, kullanılması, izlenmesi, denetlenmesi ve kamuoyuna açıklanmasına ilişkin esas ve usullerin Maliye Bakanlığınca hazırlanarak Bakanlar Kurulunca çıkarılacak yönetmelikle belirleneceği ifade edilmiştir.

9. 6487 sayılı Kanun'un 33. maddesinin birinci fıkrasında, Türkiye Yeşilay Cemiyeti tarafından Cemiyet ile aynı amaçları gerçekleştirmek üzere merkezi İstanbul'da olan "Türkiye Yeşilay Vakfı" adında Vakıf kurulması öngörülmüş; maddenin (4) numaralı fıkrasında, Vakfa, amaçlarını gerçekleştirmek üzere, her yıl ocak ayı içinde aktarılmak üzere Sağlık Bakanlığı bütçesinde ödenek ayrılacağı belirtilmiş ve dava konusu kuralla, aktarılacak ödeneğin 5018 sayılı Kanun'un 29. maddesi hükmüne tabi olmayacağı hüküm altına alınmıştır.

10. Türkiye Yeşilay Vakfı da diğer vakıflar gibi 5737 sayılı Vakıflar Kanunu'na tâbidir. 5737 sayılı Kanun'un 33. maddesinde, vakıfların denetimine ilişkin usul ve esaslar düzenlenmektedir. Anılan maddenin son fıkrasında, vakıfların amaca ve yasalara uygunluk denetimi ile iktisadî işletmelerinin faaliyet ve mevzuata uygunluk denetiminin Vakıflar Genel Müdürlüğünce yapılacağı belirtilmiş; Kanun'un 10. maddesinde de, vakfın amacı doğrultusunda faaliyette bulunmayan, vakıf mallarını ve gelirlerini amaçlarına uygun olarak kullanmayan vakıf yöneticilerinin vakfın yerleşim yeri asliye hukuk mahkemesince görevlerinden alınabileceği hüküm altına alınmıştır. Dolayısıyla, Sağlık Bakanlığı bütçesinden Türkiye Yeşilay Vakfına aktarılması öngörülen ödeneğin amacına uygun şekilde kullanılıp kullanılmadığı Vakıflar Genel Müdürlüğünün denetimine tabi olup kamu kaynağının denetim dışı kalması söz konusu değildir.

11. Bu itibarla, 5018 sayılı Kanun'un 29. maddesine tabi olmaksızın Sağlık Bakanlığı bütçesinden Türkiye Yeşilay Vakfına ödenek aktarılmasını öngören kuralın, kamu kaynağının keyfi olarak kullanılmasına sebebiyet verdiği söylenemeyeceğinden kuralda hukuk devleti ilkesine aykırı bir husus bulunmamaktadır.

12. Açıklanan nedenlerle kural, Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

2- İkinci Cümlesinin "...takip eden yıllarda ise her takvim yılı başından geçerli olmak üzere o yıl için 4/1/1961 tarihli ve 213 sayılı Vergi Usul Kanununun mükerrer 298 inci maddesi hükümleri uyarınca tespit ve ilan edilen yeniden değerlendirme oranında artırılarak..." Bölümünün İncelenmesi

a. İptal Talebinin Gerekçesi

13. Dava dilekçesinde özetle, Sağlık Bakanlığı bütçesinden Türkiye Yeşilay Vakfına ödenek aktarılmasına ilişkin kuralın nitelik olarak bütçe kanununda düzenlenmesi gerektiği, bu kapsamda,

2016 ve sonrasındaki yıllar için Sağlık Bakanlığı bütçesinden Türkiye Yeşilay Vakfına ödenek aktarılmasına olanak tanınmasının bütçenin yıllık olması ilkesiyle bağdaşmadığı gibi gelecek yıllarda halkın iradesiyle şekillenecek parlamentonun bütçe yapma hakkının da engellendiği belirtilerek kuralın, Anayasa'nın 87., 161. ve 162. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

14. 6487 sayılı Kanun'un 33. maddesinin (4) numaralı fıkrasının dava konusu bölümü içeren ikinci cümlesinde; Türkiye Yeşilay Vakfına, 2015 yılı için Sağlık Bakanlığı bütçesinden 15.000.000 TL ödenek ayrılması öngörülmüş, dava konusu kuralla da 15.000.000 TL tutarındaki ödeneğin, takip eden yıllarda her takvim yılı başından geçerli olmak üzere o yıl için 213 sayılı Vergi Usul Kanunu'nun mükerrer 298. maddesi hükümleri uyarınca tespit ve ilan edilen yeniden değerlendirme oranında artırılarak Yeşilay Vakfına aktarılacağı hüküm altına alınmıştır.

15. Anayasa'nın 87. maddesinde, TBMM'nin "kanun koymak, değiştirmek ve kaldırmak" görev ve yetkisinin yanı sıra "bütçe kanun tasarılarını görüşmek ve kabul etmek" görev ve yetkisine de ayrıca yer verilmiştir. Bütçe kanunlarını öteki kanunlardan ayrı tutan bu kural karşısında, kanun ile düzenlenmesi gereken bir konunun bütçe kanunu ile düzenlenmesi veya herhangi bir kanunda yer alan hükmün bütçe kanunları ile değiştirilmesi ve kaldırılması olanaksızdır.

16. Anayasa'nın 88. maddesinde, kanunların TBMM'de teklif, görüşülme usul ve esasları düzenlenirken, bütçe kanunlarının görüşülme usul ve esasları 162. maddede ayrıca belirtilmiştir. Bu maddeyle bütçe kanun tasarılarının görüşülmesinde ayrı bir yöntem kabul edilmiş, Genel Kurulda üyelerin gider arttırıcı veya gelir azaltıcı tekliflerde bulunmaları önlenmiş ve Anayasa'nın 89. maddesiyle de Cumhurbaşkanı'na bütçe kanunlarını bir daha görüşülmek üzere TBMM'ye geri gönderme yetkisi tanınmamıştır. Öte yandan, Anayasa'nın 163. maddesinde bütçede değişiklik yapılabilmesi esasları ayrıca düzenlenmiş, Bakanlar Kuruluna kanun hükmünde kararname ile bütçede değişiklik yapma yetkisi verilemeyeceği belirtilmiştir.

17. Anayasa'nın anılan maddeleri incelendiğinde, bütçe kanunlarına bütçe ile ilgili olmayan kurallar konulmamasının amaçlandığı anlaşılmaktadır. Anayasa'da birbirinden tamamen ayrı ve değişik olarak düzenlenen bu iki kanunlaştırma yönteminin doğal sonucu olarak, olağan kanun ile düzenlenmesi gereken bir konunun, bütçe kanunu ile düzenlenmesi, değiştirilmesi veya kaldırılması olanaksızdır. Bu durum, Anayasa'nın 161. maddesinde "Bütçe kanununa, bütçe ile ilgili hükümler dışında hiçbir hüküm konulamaz." denilmek suretiyle ifade edilmiştir. "Bütçe ile ilgili hükümler" kavramı, mali nitelikteki hükümleri değil, kanun konusu olabilecek bir kuralı kapsamaması koşuluyla bütçenin uygulanması ile ilgili, uygulamayı kolaylaştırıcı ve açıklayıcı nitelikte hükümleri

ifade etmektedir. Anayasa'nın 161. maddesinin getiriliş amacı, bütçe kanunlarında, yıllık bütçe kavramı dışındaki konulara yer vermemek, böylece bütçe kanunlarını ilgisiz kurallardan uzak tutarak kendi yapısı içinde bütünleştirmektir.

18. Anayasa Mahkemesinin 29.1.2014 tarihli, E:2013/66, K:2014/19 sayılı kararında da vurgulandığı üzere bir kuralın uygulanması sonucu gelir elde edilecek ya da harcama yapılacak olması, o kuralın bütçe kanunu kapsamında yer alması zorunluluğunu doğurmamaktadır. Bu çerçevede, kamu kurumlarının ödeneklerine ilişkin kuralların kanun konusu yapılabilmesine bir engel bulunmamaktadır. Bütçe kanunlarında ilgili kurumun o yıla ait ödenek miktarı ile harcama usul ve esasları düzenlenmekle birlikte, ödeneklere ilişkin genel ve soyut nitelikteki tüm kuralların, bütçe kanununda yer alması zorunlu değildir. Bu kapsamda, Türkiye Yeşilay Vakfına, amaçlarını gerçekleştirmek üzere, 2015 yılı için Sağlık Bakanlığı bütçesinden ayrılan 15.000.000 TL tutarındaki ödeneğin, takip eden yıllarda da yeniden değerlendirilerek artırılarak aktarılmaya devam edilmesini öngören kuralın, Anayasa'nın bütçe ile ilgili kurallarına aykırılığından söz edilemez.

19. Açıklanan nedenlerle kural, Anayasa'nın 87., 161. ve 162. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

B- Kanun'un 5. Maddesiyle 2809 sayılı Kanun'a Eklenen Ek 158. Maddenin;

1- İkinci Fıkrasının Birinci Cümlesinde Yer Alan "...ile Mütevelli Heyetinden..." İbaresinin İncelenmesi

a. İptal Talebinin Gerekçesi

20. Dava dilekçesinde özetle, dava konusu kuralla Sağlık Bilimleri Üniversitesi için üyelerinin çoğunluğunu merkezi idarenin belirlediği üyelerden oluşan Mütevelli Heyeti adı altında bir yönetim organı öngörülmesinin, Üniversitenin bilimsel özerkliğini ortadan kaldırdığı, bu Heyet üzerinden Sağlık Bakanlığı'na, Üniversiteyi dolaylı yoldan kontrol etme yetkisi tanındığı, Anayasa'da sadece Türk Silahlı Kuvvetleri ile emniyet teşkilatına bağlı yükseköğretim kurumlarıyla sınırlı olarak özel düzenlemeler yapılmasına olanak tanındığından Sağlık Bilimleri Üniversitesine diğer Devlet üniversitelerine nazaran özel bir statü verilmesinin mümkün olmadığı belirtilerek kuralın, Anayasa'nın 130. ve 132. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

21. 2809 sayılı Kanun'un ek 158. maddesiyle "Sağlık Bilimleri Üniversitesi" adı altında yeni bir üniversite kurulmuştur. Maddenin ikinci fıkrasının dava konusu ibareyi de içeren birinci cümlesinde, Sağlık Bilimleri Üniversitesi yönetim organlarının, 2547 sayılı Yükseköğretim Kanunu'nda öngörülen

organlar ile Mütevelli Heyetinden oluşacağı hüküm altına alınmakta olup dava konusu kural cümlede yer alan "...ile Mütevelli Heyetinden..." ibaresidir.

22. Anayasa'nın 130. maddesinde, çağdaş eğitim-öğretim esaslarına dayanan bir düzen içinde milletin ve ülkenin ihtiyaçlarına uygun insan gücü yetiştirmek amacı ile; ortaöğretime dayalı çeşitli düzeylerde eğitim-öğretim, bilimsel araştırma, yayın ve danışmanlık yapmak, ülkeye ve insanlığa hizmet etmek üzere çeşitli birimlerden oluşan kamu tüzelkişiliğine ve bilimsel özerkliğe sahip üniversitelerin Devlet tarafından kanunla kurulacağı belirtilmiş; yükseköğretim kurumlarının kuruluş ve organları ile işleyişleri ve bunların seçimleri, görev, yetki ve sorumluluklarının kanunla düzenleneceği hüküm altına alınmıştır. Buna göre, kanun koyucu, anayasal ilkelere uygun olmak koşuluyla, yükseköğretim kurumlarının organları ile işleyişleri ve bunların seçimleri, görev, yetki ve sorumluluklarını belirleme yetkisine sahiptir.

23. Devlet üniversitelerinde yönetim organlarının hangi birimlerden oluşacağı 2547 sayılı Kanun'da düzenlenmiştir. Anılan Kanun'un 13., 14. ve 15. maddelerinde üniversite organları "Rektör, Senato, Üniversite Yönetim Kurulu" olarak belirlenmiştir. Dava konusu kuralda ise Sağlık Bilimleri Üniversitesi yönetim organlarının, 2547 sayılı Kanun'da öngörülen organlar ile Mütevelli Heyetinden oluşacağı hüküm altına alınmıştır. Buna göre anılan Üniversitenin yönetim organları; Rektör, Senato, Üniversite Yönetim Kurulu ve Mütevelli Heyetinden oluşmaktadır.

24. Anayasa'nın 130. maddesinin dokuzuncu fıkrasında yükseköğretim kurumlarının organlarını belirleme yetkisi kanun koyucuya verilmiştir. Kanun koyucu, Anayasa'nın ilgili kurallarına bağlı olarak, yükseköğretim kurumlarının yönetim organlarını belirleyebilir. Bu konuda kanun koyucuyu sınırlandıran anayasal bir kural bulunmamaktadır. Dolayısıyla, Sağlık Bilimleri Üniversitesi için diğer devlet üniversitelerinden farklı bir teşkilatlanma öngörülebilir. Bu itibarla, dava konusu kurala, Sağlık Bilimleri Üniversitesi için 2547 sayılı Kanun'da öngörülen organlara ilave olarak "Mütevelli Heyeti" adı altında bir yönetim organı öngörülmesi, kanun koyucunun yükseköğretim kurumlarının organlarını belirleme kapsamında takdir yetkisinde olup kuralda Anayasa'nın 130. maddesine aykırı bir husus bulunmamaktadır.

25. Dava dilekçesinde, Mütevelli Heyetinin çoğunluğunun merkezi idarenin belirlediği üyelerden oluşmasının, Üniversitenin bilimsel özerkliğini zedeleyeceği ileri sürülmekte ise de dava konusu kuralda sadece Sağlık Bilimleri Üniversitesinin yönetim organlarının hangi birimlerden oluşacağı düzenlenmektedir. Mütevelli Heyetinin kimlerden oluşacağı ise ek 158. maddenin ikinci fıkrasının ikinci cümlesinde düzenlenmektedir. Bu nedenle, adı geçen Üniversite için 2547 sayılı Kanun'da sayılan yönetim organlarına ilave olarak Mütevelli Heyeti şeklinde yeni bir yönetim organı öngören

kuralın, Üniversitenin bilimsel özerkliğini zedelediği söylenemez. Heyetin üye yapısına yönelik Anayasa'ya aykırılık iddialarının dava konusu kural kapsamında değerlendirilmesine olanak bulunmamaktadır.

26. Anayasa'nın 132. maddesinde, Türk Silahlı Kuvvetleri ve emniyet teşkilatına bağlı yükseköğretim kurumlarının özel kanunlarının hükümlerine tâbi olacağı belirtilmek suretiyle anılan kurumlar tarafından kurulacak yükseköğretim kurumlarının kendine özgü koşulları da dikkate alınarak diğer üniversitelerden farklı bir hukuki rejime tabi tutulmasına olanak tanınmıştır.

27. Dava konusu kuralla, Sağlık Bilimleri Üniversitesi için Mütevelli Heyeti adı altında yeni bir yönetim organı oluşturulması anılan üniversiteye özel bir statü verildiği anlamına gelmemektedir. Nitekim Sağlık Bilimleri Üniversitesi de tıpkı diğer Devlet üniversiteleri gibi Anayasa'nın 130. ve 131. maddelerinde yükseköğretim kurumları için öngörülen kurallara tabi olduğu gibi kuruluş kanununda belirtilen hükümler hariç olmak üzere yükseköğretim kurumlarının teşkilatlanma, işleyiş, görev, yetki ve sorumluluklarını düzenleyen 2547 sayılı Kanun'a tabidir.

28. Açıklanan nedenlerle kural, Anayasa'nın 130. ve 132. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

2- İkinci Fıkrasının Dördüncü Cümlesinin ve Altıncı Cümlesinde Yer Alan "Mütevelli Heyetinin" İbarelerinin İncelenmesi

a. İptal Taleplerinin Gerekçesi

29. Dava dilekçesinde özetle, 2809 sayılı Kanun'un ek 158. maddesinin ikinci fıkrasının birinci cümlesinde yer alan "...ile Mütevelli Heyetinden..." ibaresine yönelik gerekçelerle kuralların, Anayasa'nın 130. ve 132. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

30. Dava konusu kurallarda, Mütevelli Heyetinin, en az dört üye ile toplanıp salt çoğunlukla karar alacağı ve Mütevelli Heyetinin çalışma usul ve esaslarının, Mütevelli Heyetinin teklifi üzerine Yükseköğretim Kurulu (YÖK) tarafından belirleneceği hüküm altına alınmıştır.

31. Sağlık Bilimleri Üniversitesinde Mütevelli Heyeti adı altında yeni bir yönetim organı oluşturulmasını öngören 2809 sayılı Kanun'un ek 158. maddesinin ikinci fıkrasının birinci cümlesinde yer alan "...ile Mütevelli Heyetinden..." ibaresine ilişkin gerekçeler dava konusu kurallar yönünden de geçerlidir. Anayasa'nın 130. maddesi uyarınca kanun koyucu, anayasal ilkelere uygun olmak

koşuluyla, yükseköğretim kurumlarına ait organların işleyişlerine yönelik usul ve esasları belirleme yetkisine sahiptir.

32. Bu bağlamda, Sağlık Bilimleri Üniversitesi için bir yönetim organı olarak öngörülen Mütevelli Heyetinin en az dört üye ile toplanıp salt çoğunlukla karar almasını öngören kural ile Heyetin, çalışma usul ve esaslarının belirlenmesi konusunda YÖK'e teklifte bulunma yetkisi tanıyan kurallar, yükseköğretim kurumlarına ait organların çalışma düzenlerinin belirlenmesine yönelik olup, kanun koyucunun takdir yetkisi kapsamındadır. Kaldı ki Heyetin çalışma usul ve esaslarının belirlenmesinde nihai yetki YÖK'e aittir. Mütevelli Heyetinin bu konudaki yetkisi sadece teklif sunmaktan ibarettir.

33. Açıklanan nedenlerle kurallar, Anayasa'nın 130. ve 132. maddelerine aykırı değildir. İptal taleplerinin reddi gerekir.

3- Üçüncü Fıkrası ile Dördüncü Fıkrasının Üçüncü Cümlesinde Yer Alan "Mütevelli Heyetinin teklifi ve..." İbaresinin İncelenmesi

a. İptal Taleplerinin Gerekçesi

34. Dava dilekçesinde özetle, 2547 sayılı Kanun'da, Devlet üniversitelerinin yönetim organlarına ait olan yetkilerin, dava konusu kurullarla Sağlık Bilimleri Üniversitesinde, Sağlık Bakanlığının kontrolü altında olan Mütevelli Heyetine verilmesinin, üniversite özerkliğiyle bağdaşmadığı, Mütevelli Heyetine yurtdışında üniversiteye ait birimler kurmayı teklif etme görevi verilmesinin, diğer Devlet üniversitelerinde görev yapan personel ile Sağlık Bilimleri Üniversitesinde görev yapan personel arasında ayrımcılığa neden olduğu belirtilerek kurulların, Anayasa'nın 10., 130. ve 132. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

35. Dava konusu üçüncü fıkrayla, Sağlık Bilimleri Üniversitesi için yönetim organlarından biri olarak öngörülen Mütevelli Heyetine; Üniversitenin stratejik planını ve bütçe teklifini onaylama, kamu kurum ve kuruluşları ile gerçek ve özel hukuk tüzel kişileriyle işbirliği yapılmasına ve ortak projeler yürütülmesine karar verme, yurt içinde ve yurt dışında Üniversiteye ait birimlerin ve bölümlerin kurulması için YÖK'e teklifte bulunma, Rektör tarafından gündeme alınması önerilen konularda karar verme yetkisi tanınmaktadır. Dördüncü fıkranın üçüncü cümlesinde ise Bakanlar Kurulu kararıyla yurt dışında Üniversiteye ait birimler kurulabilmesi için, Mütevelli Heyetinin teklifi ve Yükseköğretim Kurulunun uygun görüşü aranmakta olup "Mütevelli Heyetinin teklifi ve" ibaresi dava konusunu oluşturmaktadır.

36. Sağlık Bilimleri Üniversitesinde Mütevelli Heyeti adı altında yeni bir yönetim organı oluşturulmasını öngören 2809 sayılı Kanun'un ek 158. maddesinin ikinci fıkrasının birinci cümlesinde yer alan "...ile Mütevelli Heyetinden..." ibaresine ilişkin gerekçeler bu kurallar yönünden de geçerlidir. Anayasa'nın 130. maddesinin dokuzuncu fıkrasında, yükseköğretim kurumlarının kuruluş ve organları ile bunların görev, yetki ve sorumluluklarının kanunla düzenleneceği hüküm altına alınmıştır. Buna göre kanun koyucu, Sağlık Bilimleri Üniversitesi için bir yönetim organı olarak öngörülen Mütevelli Heyetinin görevlerini belirleme konusunda takdir yetkisine sahiptir.

37. Dava konusu kurallarla Mütevelli Heyetine verilen görev ve yetkiler, Üniversitenin genel idari faaliyetlerine yöneliktir. Bu yetki ve görevlerin, hangi yönetim organı tarafından kullanılacağını belirleme yetkisi Anayasa'nın 130. maddesi uyarınca kanun koyucuya aittir. Dolayısıyla, yukarıda anılan görev ve yetkilerin Sağlık Bilimleri Üniversitesi için bir yönetim organı olarak öngörülen Mütevelli Heyeti tarafından yerine getirilmesini öngören kurallar yükseköğretim kurumlarına ait organların görev, yetki ve sorumluluklarının belirlenmesi kapsamında olup, kanun koyucunun takdir yetkisinde kalmaktadır.

38. Açıklanan nedenlerle kurallar, Anayasa'nın 130. ve 132. maddelerine aykırı değildir. İptal taleplerinin reddi gerekir.

39. Kuralların Anayasa'nın 10. maddesiyle ilgisi görülmemiştir.

4- İkinci Fıkrasının İkinci ve Üçüncü Cümlelerinin İncelenmesi

a. İptal Taleplerinin Gerekçesi

40. Dava dilekçesinde özetle, Sağlık Bilimleri Üniversitesi için yönetim organı olarak öngörülen Mütevelli Heyetinin, başkan dahil üç üyesinin Sağlık Bakanlığı Müsteşarı ile Sağlık Bakanı tarafından atanacak iki kişiden oluşmasının, Üniversitenin, Sağlık Bakanlığının kontrolüne geçmesine sebebiyet vereceği, bu durumun ise üniversite özerkliğiyle bağdaşmadığı belirtilerek kuralların, Anayasa'nın 130. ve 132. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

41. Dava konusu kurallarda, Sağlık Bilimleri Üniversitesi Mütevelli Heyetinin; Sağlık Bakanlığı Müsteşarı, Rektör, Sağlık Bakanının seçeceği iki üye ile YÖK tarafından seçilen profesör unvanına sahip bir üye olmak üzere toplam beş üyeden oluşacağı, Mütevelli Heyetine Sağlık Bakanlığı Müsteşarının, Müsteşarın katılmadığı toplantılara ise Rektörün başkanlık etmesi öngörülmüştür.

42. Anayasa'nın 130. maddesinde üniversiteler anayasal bir kuruluş olarak kabul edilmiş ve maddenin birinci fıkrasında, üniversitelerle ilgili başlıca kurallar belirlenmiştir. Anılan fıkrada, üniversitelerin, "kamu tüzelkişiliğine ve bilimsel özerkliğe sahip olmaları" ve "Devlet tarafından kanunla kurulmaları" öngörülmüştür. Maddenin dokuzuncu fıkrasında da yükseköğretim kurumlarının kuruluş ve organları ile işleyişleri ve bunların seçimleri, görev, yetki ve sorumluluklarının kanunla düzenleneceği hüküm altına alınmıştır. Buna göre, yükseköğretim kurumlarının yönetim organlarının kimlerden oluşacağını belirleme yetkisi kanun koyucuya aittir. Ancak, kanun koyucunun bu yetkisini anayasal sınırlar içinde özellikle üniversitelerin bilimsel özerkliğini göz önünde tutarak kullanması gerekir.

43. Bilimsel özerklik, bilimsel çalışmaların üniversite ortamında yürütülebilmesinin olmazsa olmaz koşulu olup üniversite mensuplarının, ekonomik ve siyasi yönden nüfuz sahibi bulunan kişi ve kurumların baskısı, yönlendirmesi olmadan ve toplumda hâkim olan düşünce ve kabuller doğrultusunda sonuçlara varmak gibi bir zorunluluk hissetmeden sadece bilimsel ölçütler ve etik kurallar çerçevesinde eğitim, öğretim, araştırma ve yayın yapabilme olanaklarına sahip bulunmalarını ifade etmektedir. Üniversitelerin bilimsel özerkliği, üniversitelerde yürütülen eğitim, araştırma, yayın ve benzeri etkinliklerin planlanması, düzenlenmesi ve icra edilmesi aşamalarında, yönetim yetkisinin serbestçe kullanılabilmesini, belirtilen faaliyetlerle ilgili üniversite kaynaklarının kullanımına yönelik kararların üniversite yönetim organlarıca serbestçe alınabilmesini gerektirmektedir.

44. Anayasa'nın 130. maddesinin birinci fıkrasında, üniversitelerin bilimsel özerkliğe sahip kamu tüzelkişileri olarak tanımlanması ve bunların ancak Devlet tarafından kanunla kurulabileceklerinin hükme bağlanması ile güdülen amacın, siyasal çevrelerin, özellikle iktidarların ve değişik baskı gruplarının, üniversite çalışmaları ile eğitim ve öğretimi etki altında tutabilme yolunu kapatmak ve bu çalışmaların bilimsel gerekler ve gereksinimlerden başka, herhangi bir dış etkiden uzak kalacak bir ortamda sürdürülmesini sağlamak olduğunda kuşku bulunmamaktadır.

45. Yukarıda yer alan tanımdan da anlaşılacağı üzere bilimsel özerklik, idari ve mali özerklikle birlikte üniversitelerin özerkliği için olmazsa olmaz nitelikte bir bütünün parçalarını oluşturmaktadır. Bu unsurlardan herhangi birine yapılacak müdahale diğer unsurların da olumsuz şekilde etkilenmesine sebebiyet verecektir. Bu bağlamda, üniversite yönetim organlarının, merkezi idarenin müdahalesine olanak verecek şekilde yapılandırılması, diğer bir ifadeyle üniversitelerin, merkezi idare tarafından doğrudan atanan kişiler tarafından yönetilmesi, bu kurumların bilimsel özerkliğini de doğrudan etkileyecektir. Zira, üniversite mensuplarının, bilimsel ölçütler ve etik kurallar çerçevesinde eğitim,

öğretim, araştırma ve yayın yapabilmesi için, herhangi bir dış etkiden uzak kalacak bir ortamın bulunması zorunludur.

46. 2547 sayılı Kanun'da Devlet üniversiteleri için yönetim organları Rektör, Yönetim Kurulu ve Senato olarak belirlenmiştir. Bu organlar, akademik kadrolardan teşekkül etmektedir. 2809 sayılı Kanun'un ek 158. maddesinin ikinci fıkrasının dava konusu ikinci cümlesinde ise Sağlık Bilimleri Üniversitesinin yönetim organlarından biri olarak öngörülen Mütevelli Heyetinin; Sağlık Bakanlığı Müsteşarı, Rektör, Sağlık Bakanının seçeceği iki üye ile YÖK tarafından seçilen profesör unvanına sahip bir üye olmak üzere, toplam beş üyeden oluşması öngörülmüştür. Mütevelli Heyetinin, görev ve yetki alanına giren konularda salt çoğunlukla karar alabileceği göz önünde bulundurulduğunda, merkezi idareyi temsil eden Sağlık Bakanlığının Müsteşarı ile Sağlık Bakanının doğrudan seçeceği üyeler, karar alma sürecinde belirleyici olacaktır.

47. Kanun'un ek 158. maddesinin üçüncü ve devamı fıkralarında Mütevelli Heyetinin görev ve yetkileri sıralanmıştır. Mütevelli Heyetine, üniversitenin stratejik planını onaylama ve üniversiteye tahsis edilecek öğretim elemanı kadrolarını, birlikte kullanılan eğitim ve araştırma hastanesinin ihtiyacını da dikkate almak suretiyle il bazında belirleme, norm kadro sayısını onaylama gibi yetkiler verilmiştir. Anılan hükümler bir bütün halinde değerlendirildiğinde, Mütevelli Heyetine, Üniversite yönetiminde söz hakkı tanındığı anlaşılmaktadır.

48. Mütevelli Heyetinin üniversite yönetimine ilişkin mevcut yetkileri ve Mütevelli Heyetinin en az dört üye ile toplanıp salt çoğunlukla karar alabileceği göz önünde bulundurulduğunda, heyet üyelerinin çoğunluğunun Sağlık Bakanlığı Müsteşarı ile Sağlık Bakanının seçeceği iki üyeden oluşmasının, merkezi idareye, Mütevelli Heyeti kanalıyla üniversite yönetimine ilişkin karar alma sürecinde belirleyici olacak şekilde söz hakkı tanıyacağı açıktır. Merkezi idareye, üniversite üzerinde denetim ve gözetim yetkisini aşan nitelikte bir yetki tanınması ise Anayasa'nın 130. maddesiyle güvence altına alınan bilimsel özerklik ilkesiyle bağdaşmamaktadır.

49. Açıklanan nedenlerle 2809 sayılı Kanun'un ek 158. maddesinin ikinci fıkrasının ikinci cümlesi, Anayasa'nın 130. maddesine aykırıdır. İptali gerekir.

50. Kural, Anayasa'nın 130. maddesine aykırı bulunarak iptal edildiğinden, Anayasa'nın 132. maddesi yönünden ayrıca incelenmesine gerek görülmemiştir.

51. 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrasında, kanunun belirli kurallarının iptali, diğer kurallarının veya tümünün uygulanmaması sonucunu doğuruyorsa, bunların da Anayasa Mahkemesince iptaline karar verilebileceği öngörülmektedir.

52. Mütevelli Heyetinin üye yapısını düzenleyen Kanun'un ek 158. maddesinin ikinci fıkrasının ikinci cümlesinin iptali nedeniyle, kuralla doğrudan ilgili olan, Mütevelli Heyetine, Sağlık Bakanlığı Müsteşarının, Müsteşarın katılmadığı toplantılara Rektörün başkanlık edeceğini düzenleyen ek 158. maddenin ikinci fıkrasının üçüncü cümlesinin uygulanma olanağı kalmadığından, bu cümlenin de 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrası gereğince iptali gerekir.

53. Hicabi DURSUN, Muammer TOPAL, Recai AKYEL ve Yusuf Şevki HAKYEMEZ 2809 sayılı Kanun'un ek 158. maddesinin ikinci fıkrasının üçüncü cümlesinin iptali yönündeki görüşe katılmamışlardır.

5- İkinci Fıkrasının Beşinci Cümlesinin İncelenmesi

a. İptal Talebinin Gerekçesi

54. Dava dilekçesinde özetle, 2809 sayılı Kanun'un ek 158. maddesinin ikinci fıkrasının ikinci ve üçüncü cümlelerine yönelik gerekçelerle kuralın, Anayasa'nın 130. ve 132. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

55. Dava konusu kuralda, Mütevelli Heyetine, Bakan ve YÖK tarafından seçilen üyelerin görev süresinin dört yıl olduğu belirtilmiştir.

56. Sağlık Bilimleri Üniversitesinde Mütevelli Heyeti adı altında yeni bir yönetim organı oluşturulmasını öngören 2809 sayılı Kanun'un ek 158. maddesinin ikinci fıkrasının birinci cümlesinde yer alan "...ile Mütevelli Heyetinden..." ibaresine ilişkin gerekçeler dava konusu kural yönünden de geçerlidir. Anayasa'nın 130. maddesi uyarınca kanun koyucu, anayasal ilkelere uygun olmak koşuluyla, yükseköğretim kurumlarının organları ile bunların görev, yetki ve sorumluluğuna yönelik usul ve esasları belirleme yetkisine sahiptir.

57. Bu bağlamda, Sağlık Bilimleri Üniversitesi için bir yönetim organı olarak öngörülen Mütevelli Heyeti üyelerinin görev sürelerini düzenleyen kural, yükseköğretim kurumlarına ait organların çalışma düzenlerinin belirlenmesine yönelik olup, kanun koyucunun takdir yetkisi kapsamındadır. Kural, Mütevelli Heyetinin oluşumunu düzenleyen Kanun'un ek 158. maddesinin ikinci fıkrasının ikinci cümlesinden bağımsız şekilde değerlendirildiğinde, Anayasa'nın yükseköğretim kurumlarını düzenleyen kurallarına aykırı bir husus taşımamaktadır.

58. Açıklanan nedenlerle kural, Anayasa'nın 130. ve 132. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

6- Beşinci Fıkrasının Birinci ve İkinci Cümlelerinin İncelenmesi

a. İptal Taleplerinin Gerekçesi

59. Dava dilekçesinde özetle, dava konusu kurallarla Türkiye Kamu Hastaneleri Kurumuna bağlı eğitim ve araştırma hastanelerinin tamamının, Sağlık Bakanlığının kontrolünde olan Sağlık Bilimleri Üniversitesinin uygulama ve araştırma merkezi haline getirilmesinin üniversitelerin özerkliğiyle bağdaşmadığı, Üniversitedeki tıp eğitiminin teorik kısmının İstanbul'daki merkez kampüste, araştırma ve uygulama kısmının ise eğitim araştırma hastanelerinin bulunduğu illerde verilmesinin eğitim bütünlüğünü bozduğu, belirtilen eğitimin nasıl yapılacağı konusunda belirlilik bulunmadığı, ayrıca dava konusu kuralların diğer Devlet Üniversitelerinin, eğitim ve araştırma hastaneleriyle işbirliği yapmalarını da engellediği belirtilerek kuralların, Anayasa'nın 2. ve 130. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

60. Dava konusu kurallarla, Sağlık Bilimleri Üniversitesinin, Türkiye Kamu Hastaneleri Kurumuna bağlı eğitim ve araştırma hastaneleriyle 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun ek 9. maddesi çerçevesinde birlikte kullanım protokolleri yaparak uygulama ve araştırma faaliyetlerini yürüteceği, Üniversitenin birlikte kullanım protokolü imzaladığı eğitim ve araştırma hastanelerinin aynı zamanda Üniversitenin uygulama ve araştırma merkezi statüsünü kazanacağı hüküm altına alınmaktadır.

61. Anayasa'nın 130. maddesinin dokuzuncu fıkrasında, yükseköğretim kurumlarının kamu kuruluşları ve diğer kurumlarla ilişkilerinin kanunla düzenleneceği hüküm altına alınmıştır. Buna göre kanun koyucu, anayasal ilkelere uygun olmak koşuluyla, yükseköğretim kurumları ile kamu kurum ve kuruluşları arasında ne tür bir işbirliği yapılabileceğini ve bu işbirliğinin usul ve esaslarını belirleme konusunda takdir yetkisine sahiptir.

62. 3359 sayılı Kanun'un ek 9. maddesiyle, Türkiye Kamu Hastaneleri Kurumuna bağlı sağlık tesisleri ile üniversitelerin ilgili birimlerinin karşılıklı olarak işbirliği çerçevesinde birlikte kullanılabilmesine olanak tanınmış ve birlikte kullanıma ilişkin usul ve esaslar düzenlenmiştir. Maddede, birlikte kullanılacak sağlık birimlerinde, sağlık hizmetinin yanı sıra hem lisans hem de uzmanlık eğitimi verilmesi öngörülmüştür.

63. Dava konusu kurallarla, Sağlık Bilimleri Üniversitesinin de diğer üniversiteler gibi Türkiye Kamu Hastaneleri Kurumuna bağlı eğitim ve araştırma hastaneleriyle kullanım protokolleri yapabilmesi sağlanmıştır. Buna göre adı geçen Üniversite, Türkiye Kamu Hastaneleri Kurumuna bağlı eğitim ve

araştırma hastaneleriyle protokol yapabilecek ve protokol yapılan hastaneler Üniversitenin uygulama ve araştırma merkezi statüsünde olacaktır.

64. Sağlık Bilimleri Üniversitesine de diğer üniversiteler gibi Türkiye Kamu Hastaneleri Kurumuna bağlı eğitim ve araştırma hastaneleriyle birlikte kullanım protokolleri yapma olanağı tanıyan ve bu hastanelerin üniversitenin uygulama ve araştırma merkezine dönüştürülmesini öngören kurallar yükseköğretim kurumları ile kamu kurum ve kuruluşları arasında yapılacak işbirliğine yönelik olup, Anayasa'nın 130. maddesinin dokuzuncu fıkrası kapsamında kanun koyucunun takdir yetkisindedir.

65. Dava dilekçesinde, uygulama ve araştırma merkezlerinde tıp eğitiminin nasıl yapılacağı konusunda belirsizlik bulunduğu ileri sürülmekte ise de, Türkiye Kamu Hastaneleri Kurumuna bağlı eğitim ve araştırma hastanelerinin, Üniversite ile birlikte kullanımına ilişkin usul ve esaslar 3359 sayılı Kanun'un ek 9. maddesinde düzenlenmektedir. Dolayısıyla, bu iddianın, dava konusu kurallar kapsamında değerlendirilmesine olanak bulunmamaktadır.

66. Sağlık Bilimleri Üniversitesinin merkez kampüsünün İstanbul'da olması nedeniyle teorik eğitimin İstanbul'da, uygulamaya yönelik eğitimin başka bir şehirdeki eğitim ve araştırma hastanesinde verilmesinin tıp eğitiminin bütünlüğünü bozacağına yönelik iddianın incelenmesi ise yerindelik denetiminin kapsamında bulunduğundan bu husus anayasallık denetiminin kapsamı dışındadır.

67. Diğer taraftan dava konusu kurallarda, eğitim ve araştırma hastanelerinin yalnızca Sağlık Bilimleri Üniversitesi ile protokol yapabileceğine ilişkin herhangi bir düzenleme yer almamaktadır. Dolayısıyla dava konusu kurallar, diğer üniversitelerin eğitim ve araştırma hastaneleriyle imzaladıkları protokollerin sona ermesine neden olmadığı gibi diğer üniversiteler ile eğitim ve araştırma hastaneleri arasında yeni protokoller yapılmasına da engel oluşturmamaktadır.

68. Açıklanan nedenlerle kurallar, Anayasa'nın 130. maddesine aykırı değildir. İptal taleplerinin reddi gerekir.

69. Kuralların Anayasa'nın 2. maddesiyle ilgisi görülmemiştir.

7- Beşinci Fıkrasının Üçüncü ve Dördüncü Cümlelerinin İncelenmesi

a. İptal Taleplerinin Gerekçesi

70. Dava dilekçesinde özetle, Sağlık Bilimleri Üniversitesine ait birimlere tahsis edilecek kadroları il bazında belirleme ve Üniversite birimlerine tahsis edilecek öğretim üyesi norm kadro sayısını onaylama yetkisinin Sağlık Bakanlığının kontrolündeki Mütevelli Heyetine verilmesinin, tıp

eğitiminin Sağlık Bakanlığına devredilmesi anlamına geldiği, bu durumun üniversite özerkliği ile bağdaşmadığı belirtilerek kuralların, Anayasa'nın 130. maddesine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

71. Dava konusu kurallarla, Sağlık Bilimleri Üniversitesine tahsis edilecek öğretim elemanı kadrolarının, temel bilimler hariç olmak üzere, birlikte kullanılan eğitim ve araştırma hastanesinin eğitim birimleri ve ihtiyacı dikkate alınarak, Rektörün önerisi üzerine Mütevelli Heyeti tarafından il bazında belirleneceği ve öğretim üyesi atamalarının bu kadrolara yapılacağı, Üniversitenin birimlerine tahsis edilecek öğretim üyesi norm kadro sayısının, Rektörün önerisi ve Mütevelli Heyetinin onayı ile YÖK tarafından tespit edileceği belirtilmiştir.

72. 2809 sayılı Kanun'un ek 158. maddesinin ikinci fıkrasının birinci cümlesinde yer alan "...ile Mütevelli Heyetinden..." ibaresine ilişkin gerekçeler bu kurallar yönünden de geçerlidir. Anayasa'nın 130. maddesinin dokuzuncu fıkrasına göre kanun koyucu anayasal sınırlar içinde Mütevelli Heyetinin görevlerini belirleme konusunda takdir yetkisine sahiptir. Bu bağlamda, Sağlık Bilimleri Üniversitesine tahsis edilecek öğretim elemanı kadrolarının, temel bilimler hariç olmak üzere, birlikte kullanılan eğitim ve araştırma hastanesinin eğitim birimleri ve ihtiyacı dikkate alınarak, Rektörün önerisi üzerine Mütevelli Heyeti tarafından il bazında belirlenmesini ve öğretim üyesi atamalarının bu kadrolara yapılmasını, Üniversitenin birimlerine tahsis edilecek öğretim üyesi norm kadro sayısının Rektörün önerisi ve Mütevelli Heyetinin onayı üzerine YÖK tarafından tespit edilmesini öngören kurallar, kanun koyucunun takdir yetkisi kapsamındadır.

73. Diğer taraftan, üniversitelerde istihdam edilecek öğretim elemanlarının kadrolarının belirlenmesinde üniversite yönetim organlarına yetki verilmesi Anayasa'nın 130. maddesiyle üniversitelere tanınan bilimsel özerklikle de uyumludur. Sağlık Bilimleri Üniversitesinde bu yetkinin, Üniversitenin yönetim organı olan Mütevelli Heyetine verilmesi ise kanun koyucunun takdir yetkisindedir. Kaldı ki, norm kadro sayısının tespiti bakımından nihai yetki de YÖK'everilmiştir.

74. Dava dilekçesinde, öğretim elemanı kadrolarının belirlenmesinde yetkinin Sağlık Bakanlığının kontrolündeki Mütevelli Heyetine verilmesinin tıp eğitiminin Sağlık Bakanlığına devredilmesi anlamına geldiği ileri sürülmekte ise de Mütevelli Heyetinde Sağlık Bakanlığının belirleyici olmasını sağlayan kural iptal edildiğinden, böyle bir sakıncanın meydana gelmesi de söz konusu değildir.

75. Açıklanan nedenlerle kurallar, Anayasa'nın 130. maddesine aykırı değildir. İptal taleplerinin reddi gerekir.

76. M. Emin KUZ 2809 sayılı Kanun'un ek 158. maddesinin beşinci fıkrasının üçüncü cümlesi yönünden bu görüşe katılmamıştır.

8- Altıncı Fıkrasının İncelenmesi

a. İptal Talebinin Gerekçesi

77. Dava dilekçesinde özetle, Marmara Üniversitesine tahsisli olan Haydarpaşa Kampüsünün, tahsis amacı ortadan kalkmadan veya tahsis amacı dışında kullanıldığı tespit edilmeden Sağlık Bilimleri Üniversitesine tahsis edilmesinin kamu yararıyla bağdaşmadığı, niteliği itibarıyla idari işlem olan ve idarenin yetkisinde bulunan tahsis işlemine karşı yargı yolunu kapatmak amacıyla tahsisin kanun hükmüyle yapıldığı, Marmara Üniversitesinin uygun görüşünü almadan ve başka bir bina tahsis edilmeden Kampüsün devredilmesinin, Üniversitenin eğitim hizmetlerini yerine getirmesine de engel olduğu belirtilerek kuralın, Anayasa'nın 2., 36., 123., 125. ve 130. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

78. Dava konusu kuralla, Mekteb-i Tıbbiye-i Şâhâne adıyla hizmet vermek üzere inşa edilen ve hâlen Marmara Üniversitesi adına tahsisli olan Haydarpaşa Kampüsünün, Sağlık Bilimleri Üniversitesine tahsis edilmesi öngörülmektedir.

79. Yasamanın genelliği ilkesi gereğince Anayasa'nın temel ilkeleri ile yasaklayıcı hükümlerine aykırı olmamak kaydıyla kanun koyucu her konuda düzenleme yapma yetkisine sahiptir.

80. Kanunların kamu yararının sağlanması amacına yönelik olması, hukuk devleti olmanın gereğidir. Anayasa'nın çeşitli hükümlerinde yer alan kamu yararı kavramının Anayasa'da bir tanımı yapılmamıştır. Anayasa Mahkemesi kararlarında belirtildiği gibi, kamu yararı, bireysel, özel çıkarlardan ayrı ve bunlara üstün olan toplumsal yarardır. Kamu yararı düşüncesi olmaksızın, yalnız özel çıkarlar için veya yalnız belli kişilerin yararına olarak kanun hükmü konulamaz. Böyle bir durumun açık bir biçimde ve kesin olarak saptanması halinde, söz konusu kanun hükmü Anayasa'nın 2. maddesine aykırı düşer. Açıklanan ayırık hâl dışında, bir kanun hükmünün ülke gereksinimlerine uygun olup olmadığı ve hangi araç ve yöntemlerle kamu yararının sağlanabileceği bir siyasî tercih sorunu olarak kanun koyucunun takdirinde olduğundan, bu kapsamda kamu yararı değerlendirmesi yapmak anayasa yargısıyla bağdaşmaz.

81. Anayasa'nın hak arama hürriyetini düzenleyen 36. maddesinin birinci fıkrasında, "Herkes, meşru vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve

savunma ile adil yargılanma hakkına sahiptir.” denilerek, yargı mercilerine başvurabilme ve bunun doğal sonucu olarak da iddia, savunma ve adil yargılanma hakkı güvence altına alınmıştır.

82. Tahsis, kamu idareleri ve Hazinesinin özel mülkiyetinde bulunan taşınmazlar ile Devletin hüküm ve tasarrufu altında bulunan taşınmazların, kamu hizmetlerinin yerine getirilmesi için mülkiyeti kendilerinde kalmak koşuluyla kamu idareleri veya köy tüzel kişiliklerinin kullanımına bırakılmasını ifade etmektedir. Anayasa’da, söz konusu taşınmazların tahsisine ilişkin bir düzenleme bulunmadığından kanun koyucu, anayasal sınırlar içinde kalmak, kamu yararı ve hizmetin gereklerini dikkate almak koşuluyla kamu mallarının tahsisine ilişkin kuralları belirleme yetkisine sahiptir.

83. Hazinesinin özel mülkiyetindeki taşınmazların kamu idarelerine veya köy tüzel kişiliklerine tahsisine ilişkin kurallar 5018 sayılı Kanun’da düzenlenmiştir. Anılan Kanun’un 47. maddesinin birinci fıkrasında, kamu idarelerinin, kanunlarında belirtilen kamu hizmetlerini yerine getirebilmek için mülkiyetlerindeki taşınmazları, birbirlerine ve köy tüzel kişiliklerine bedelsiz olarak tahsis edebileceği belirtildikten sonra ikinci fıkrasında, Hazinesinin özel mülkiyetindeki taşınmazları tahsis etmeye, kamu ihtiyaçları için gerekli olmayanların tahsisini kaldırmaya Maliye Bakanlığının yetkili olduğu belirtilmiştir.

84. Dava konusu kuralda ise Marmara Üniversitesine tahsisli olan Haydarpaşa kampüsünün, Sağlık Bilimleri Üniversitesine tahsis edilmesi öngörülmektedir. Kuralın gerekçesinde, ülkemizin ilk modern tıp fakültesi olan Mekteb-i Tıbbiye-i Şâhâne için inşa edilen ve uzun yıllar tıp fakültesi olarak hizmet veren ve halen Marmara Üniversitesine tahsisli olan Haydarpaşa Kampüsünün, yeni kurulan Sağlık Bilimleri Üniversitesine tahsis edilmesiyle, büyük mimari değeri yanında ülkemizde tıp eğitimi alanında tarihten gelen özel bir konumu da bulunan bu binanın misyonuna uygun olarak tarihi adıyla birlikte yaşatılması amacıyla Kampüsün ilk kurulduğu adla hizmet vermek üzere, yeni kurulan Sağlık Bilimleri Üniversitesine tahsisinin sağlandığı ifade edilmiştir. Bu yönüyle kuralın kamu yararına aykırı bir amaçla ihdas edildiği söylenemez. Bu itibarla, kamu yararı amacı dışında bir amaç gözettiği saptanamayan ve kanun koyucunun takdir yetkisi kapsamında kalan kuralda, hukuk devleti ilkesine aykırılık bulunmamaktadır.

85. Yasamanın genelliği ilkesi gereğince kanun koyucu, hazinenin özel mülkiyetindeki taşınmazların tahsisini kanunla yapabileceği gibi esas ve usulleri kanunda gösterilmek koşuluyla idari işlemle yapılmasına da olanak tanıyabilir. Bu bağlamda, Haydarpaşa kampüsü kanun koyucu tarafından dava konusu kuralla Sağlık Bilimleri Üniversitesine tahsis edilmiştir. Kanuni bir düzenlemeyle oluşturulan bu durumun, hukuka uygun olup olmadığının tespiti ise anayasal bir sorun olup, kanun

hükümünün Anayasa'ya uygunluğunun denetimini Anayasa Mahkemesi yapmaktadır. Dolayısıyla, Haydarpaşa Kampüsünün idari bir işlem yerine kanun hükmüyle Sağlık Bilimleri Üniversitesine tahsis edilmesinin hak arama hürriyetini ortadan kaldırdığı söylenemez.

86. Açıklanan nedenlerle kural, Anayasa'nın 2. ve 36. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

87. Kuralın Anayasa'nın 123., 125. ve 130. maddeleriyle ilgisi görülmemiştir.

C- Kanun'un 18. Maddesiyle 6446 Sayılı Kanun'a Eklenen Geçici 18. Maddenin İncelenmesi

1. İptal Talebinin Gerekçesi

88. Dava dilekçesinde özetle, dava konusu kuralla Enerji Piyasası Düzenleme Kuruluna (EPDK) elektrik enerjisinin dağıtımında ortaya çıkan kayıp-kaçakların azaltılmasına ilişkin detayları belli olmayan muğlak bir yetki tanındığı, elektrik dağıtım piyasasının özelleştirilmesi sonucu ihaleyi kazanan şirketlerin kayıp-kaçak oranlarını azaltmak için verdiği hedefleri yakalayamaması nedeniyle oluşan zararın tüketicilere yansıtılmasına yasal zemin oluşturulduğu, bu durumun aynı zamanda özelleştirme şartnamesine de müdahale anlamına geldiği, bu şekilde kamu yararından ziyade elektrik piyasasında faaliyet gösteren işletmelerin çıkarlarının gözetildiği, faturalarını düzenli şekilde ödeyen elektrik abonelerine kayıp-kaçak bedeli altında ek mali yükümlülükler getirilmesinin anayasal bir dayanağının bulunmadığı, Yargıtay Hukuk Genel Kurulunun kayıp-kaçak bedelinin tüketicilere iade edilmesine yönelik kararının da dava konusu kuralla etkisiz hale getirildiği belirtilerek kuralın, Anayasa'nın 2., 138. ve 172. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

89. 6216 sayılı Kanun'un 43. maddesi uyarınca, ilgisi nedeniyle dava konusu kural Anayasa'nın 48. ve 167. maddeleri yönünden de incelenmiştir.

90. Dava konusu kuralla, 1.1.2016 tarihine kadar, teknik ve teknik olmayan kayıplarının oranı ülke ortalamasının üzerinde olan dağıtım bölgelerinde, diğer dağıtım bölgelerinden farklı düzenlemeler yapılmasına, hedef kayıp-kaçak oranlarının bir önceki yılın gerçekleştirmeleri dikkate alınarak ve sonraki uygulama dönemleri de dâhil olmak üzere yeniden belirlenmesine EPDK'nın yetkili olduğu belirtilmektedir.

91. Anayasa'nın 2. maddesinde, Türkiye Cumhuriyeti'nin sosyal bir hukuk devleti olduğu belirtilmiştir. Sosyal devlet, sosyal adaletin, sosyal refahın ve sosyal güvenliğin gerçekleşmesini sağlayan devlettir. Ekonomik ve malî politikalar sosyal devletin gerçekleşmesini sağlayan araçlardır.

92. Anayasa'nın 48. maddesinde herkesin, dilediği alanda çalışma ve sözleşme, özel teşebbüsler kurma hürriyetine sahip olduğu ve Devletin, özel teşebbüslerin millî ekonominin gereklerine ve sosyal amaçlara uygun yürümesini, güvenlik ve kararlılık içinde çalışmasını sağlayacak tedbirleri alacağı belirtilmektedir. Anayasa'nın 167. maddesinde de, Devletin, para, kredi, sermaye, mal ve hizmet piyasalarının sağlıklı ve düzenli işlemlerini sağlayıcı ve geliştirici tedbirleri alacağı ifade edilerek, ekonomik hayatın işleyişini düzenlemek, gerektiğinde bu alana müdahale etmek hususunda görevli kılındığı anlaşılmaktadır.

93. Türkiye'de elektrik dağıtım sektöründe rekabetçi bir yapı oluşturmak amacıyla, elektrik dağıtımında tekel konumunda bulunan Türkiye Elektrik Dağıtım A.Ş'nin özelleştirilmesi öngörülmüştür. Bu çerçevede özelleştirmenin etkinliği için elektrik dağıtım bakımından ülke 21 bölgeye ayrılmış ve bölgesel düzeyde dağıtım faaliyetlerinin özelleştirilmesine karar verilmiştir. Özelleştirme ile kayıp-kaçak oranlarının azaltılması ve sektördeki kamu tekelinin zayıflatılarak rekabetin artırılması amaçlanmıştır.

94. Teknik ve teknik olmayan kayıp şeklinde de ifade edilen "kayıp-kaçak elektrik", dağıtım sistemine giren toplam enerji ile tüketicilere fatura edilen enerji arasındaki fark şeklinde tanımlanmaktadır. Bu kayıp, elektriğin dağıtım esnasında meydana gelen teknik sorunlardan meydana gelebileceği gibi elektriğin mevzuata aykırı şekilde kullanılmasından da kaynaklanabilmektedir. Özellikle kaçak elektrik kullanımı olarak da ifade edilen elektriğin mevzuata aykırı şekilde kullanımı nedeniyle oluşan kayıp oranları dağıtım bölgeleri arasında farklılık göstermekte, bu oran bazı dağıtım bölgelerinde ülke ortalamasının çok üzerine çıkabilmektedir.

95. Dava konusu kuralla, dağıtım bölgelerindeki sosyoekonomik şartlar ve tüketici alışkanlıkları da gözetilerek teknik ve teknik olmayan kayıplarının oranı ülke ortalamasının üzerinde olan dağıtım bölgelerinde gerekli tedbirleri alma ve hedef kayıp-kaçak oranlarını belirleme konusunda elektrik piyasasını düzenlemek ve denetlemekle görevli olan Enerji Piyasası Düzenleme Kurulunun yetkili kılındığı anlaşılmaktadır. Böylece, Kurul, her bir dağıtım bölgesinin bir yıl önceki kayıp-kaçak oranlarını dikkate alarak bölgesel bazda kayıp-kaçakla mücadele eylem planı hazırlayabilecek ve hedef kayıp-kaçak oranlarını belirleyebilecektir.

96. Kuralın gerekçesinde de, yapılan düzenlemeyle kayıp-kaçak oranının yüksek olduğu bölgeler için bölgelerin sosyoekonomik şartları ve tüketici alışkanlıkları da gözetilmek suretiyle fiili kayıp-kaçak değerleri dikkate alınarak kayıp hedeflerinin belirli süreyle yeniden tespitinin amaçlandığı, teknik ve teknik olmayan kayıp oranları Türkiye ortalamasının çok üzerinde olan dağıtım bölgelerinde, kayıplarla etkin mücadele edilmesi ve kayıp-kaçak oranlarının düşürülmesi için mevcut ikincil

düzenlemelerin ötesinde ek önlemlerin alınması gerektiğinden, bu önlemlerin alınabilmesine yasal zemin oluşturmak amacıyla kuralın ihdas edildiği belirtilmiştir.

97. Anayasa'nın 48. ve 167. maddeleri gereğince Devlet, elektrik enerjisinin kaliteli, sürekli, kesintisiz, düşük maliyetli şekilde tüketicilerin kullanımına sunulması ve bu sayede istikrarlı bir elektrik enerjisi piyasasının oluşturulması amacıyla gerekli tedbirleri almakla yükümlüdür. Dava konusu kuralın da elektrik enerjisi piyasasının sağlıklı bir şekilde işlemlerini sağlamaya yönelik tedbirler kapsamında ihdas edildiği anlaşılmaktadır. Kurala ilişkin yasama belgelerinin incelenmesinden ve kuralın objektif anlamından kamu yararı dışında bir amaç güttüğüne dair bir sonuca ulaşılamamaktadır.

98. Bu itibarla, tüketicilere güvenilir, kaliteli ve kesintisiz elektrik enerjisi hizmeti verilmesi için gerekli düzenlemeleri yapmakla görevli olan Enerji Piyasası Düzenleme Kuruluna, kayıp-kaçak oranının yüksek olduğu dağıtım bölgelerinde sosyoekonomik şartları da gözetenek diğer dağıtım bölgelerinden farklı düzenlemeler yapma ve hedef kayıp-kaçak oranlarını belirleme yetkisi veren kural, kanun koyucunun takdir yetkisi kapsamında olup hukuk devleti ilkesine aykırı olmadığı gibi, Devletin, milli ekonominin gereklerine uygun şekilde mal ve hizmet piyasalarının sağlıklı ve düzenli işlemlerini sağlayıcı tedbirler almasını öngören Anayasa'nın 48. ve 167. maddelerinin de gereğidir.

99. Kayıp-kaçak oranlarının azaltılabilmesi için alınması gereken tedbirler uzmanlık ve teknik bilgi gerektirmektedir. Bu nedenle dava konusu kuralla, teknik ve teknik olmayan kayıplarının oranı ülke ortalamasının üzerinde olan dağıtım bölgelerinde farklı düzenlemeler yapma konusunda EPDK yetkili kılınmış ve hedef kayıp-kaçak oranları belirlenirken bir önceki yılın gerçekleştirmelerinin de dikkate alınacağı belirtilmiştir. Bu tedbirlerin neler olduğunun kanun koyucu tarafından tek tek belirlenmesi mümkün değildir. Dolayısıyla, EPDK'ya dağıtım bölgeleri arasında farklı düzenlemeler yapma ve kayıp-kaçak oranlarının belirlenmesi konusunda sınırları belirsiz bir yetki verilmesi söz konusu değildir.

100. EPDK'ya verilen yetki, kamu yararının sağlanmasının yanı sıra hizmet gerekleri ve yetkiyi veren Kanun'un amacının gerçekleştirilmesi ile sınırlıdır. Kurul, takdir yetkisini kullanırken, hukukun genel ilkelerine ve hakkaniyete de uygun davranmak zorunda olup işlemleri yargı denetimine tâbidir. Anayasa'nın 125. maddesinde, "İdarenin her türlü eylem ve işlemlerine karşı yargı yolu açıktır." denilerek, idarenin hukuka bağlılığı, yargı denetimi sayesinde etkili biçimde sağlanmış ve idare edilenler, idarenin kanunsuz ve keyfi davranışlarına karşı korunmuştur.

101. Diğer taraftan, dava dilekçesinde, kuralın, faturalarını düzenli şekilde ödeyen elektrik abonelerine kayıp-kaçak bedeli olarak ek mali yükümlülükler getirilmesine yasal zemin oluşturduğu belirtilerek, kural uyarınca tüketicilere kayıp-kaçak bedeli adı altında ek bir mali yükümlülük

getirilmesinin Anayasa'ya aykırı olduğu ileri sürülmekte ise de, dava konusu kuralda, tüketicilerden kayıp-kaçak bedeli alınacağına ilişkin herhangi bir düzenleme yer almadığından, kayıp-kaçak bedeli alınmasına yönelik Anayasa'ya aykırılık iddialarının dava konusu kural kapsamında değerlendirilmesine olanak bulunmamaktadır.

102. Açıklanan nedenlerle kural, Anayasa'nın 2., 48. ve 167. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

103. Kuralın Anayasa'nın 138. ve 172. maddeleriyle ilgisi görülmemiştir.

D- Kanun'un 22. Maddesiyle 638 Sayılı KHK'ya Eklenen Geçici 13. Maddenin (1) Numaralı Fıkrasının Birinci Cümlesinde Yer Alan "...Bakanlık Merkez Teşkilatı ile Spor Genel Müdürlüğü ve..." İbaresinin İncelenmesi

1. İptal Talebinin Gerekçesi

104. Dava dilekçesinde özetle, Gençlik ve Spor Bakanlığı ile Spor Genel Müdürlüğü'nün teşkilat yapılarında herhangi bir değişiklik olmamasına rağmen adı geçen kurumlarda genel müdür yardımcılarında şube müdürlerine kadar görev yapanların görevlerine son verilerek daha alt bir göreve atanmalarının hukuki güvenlik ilkesini ihlalettiği, statü hukukunun temelindeki liyakat ilkesiyle bağdaşmadığı, bu kişilerin yargı mercileri önünde dava açma haklarının engellendiği belirtilerek kuralın, Anayasa'nın 2., 36, 70. ve 125. maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

105. 638 sayılı KHK'nın geçici 13. maddesinin (1) numaralı fıkrasının birinci cümlesinde, Gençlik ve Spor Bakanlığı Merkez Teşkilatı ile Spor Genel Müdürlüğünde ve Yüksek Öğrenim Kredi ve Yurtlar Kurumu Genel Müdürlüğünde; Genel Müdür Yardımcısı, Müşavir, Teftiş Kurulu Başkanı, I. Hukuk Müşaviri, Müstakil/Unvanlı Daire Başkanı, Daire Başkanı, Gençlik Hizmetleri ve Spor İl Müdürü, Gençlik Hizmetleri ve Spor İlçe Müdürü, Federasyon Genel Sekreteri ve Gençlik Merkezi Müdürü kadrolarında bulunanların görevlerinin hiçbir işleme gerek kalmaksızın sona ereceği hüküm altına alınmakta olup cümlede yer alan "Gençlik ve Spor Bakanlığı Merkez Teşkilatı ile Spor Genel Müdürlüğünde ve" ibaresi dava konusu kuralı oluşturmaktadır.

106. Anayasa'nın 2. maddesinde yer alan hukuk devletinin gereklerinden olan hukukî güvenlik ilkesi, normların öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar.

107. Kamu personeli olarak görev yapan kişilerin buldukları görevlerden alınmalarını gerektiren haklı bir neden olmadıkça görevlerine son verilememesi, hukukî güvenlik ilkesinin bir gereğidir. Kamu personelinin buldukları görevden alınma ve başka bir göreve atanmalarının, haklarında bu yönde idari işlem tesis edilmesi ile gerçekleşmesi kural olmakla birlikte, hukukî ve fiilî zorunluluk hallerinde bu hususlarda yasal düzenlemeler yapılabileceği de kabul edilmektedir. Söz konusu zorunluluklar nedeniyle getirilen ve ilgililerin kazanılmış haklarını ihlal etmeyen düzenlemeler, hukukî güvenlik ilkesine aykırılık oluşturmaz.

108. Kamu kurum ve kuruluşlarının yeniden yapılandırılmaları kapsamında, teşkilat yapısı değiştirilen kurum ve kuruluşların bazı kadrolarında görev yapan kamu görevlilerinin, görevlerinin sona erdirilerek başka kadrolara atanmalarının öngörülmesi, söz konusu hukukî ve fiilî zorunluluklar nedeniyle getirilen yasal düzenlemelerin bir örneğini oluşturmaktadır. Böyle bir durumda, ilgililerin başka kadrolara atanmalarının sebep unsuru, ilgili kurumun ya da kuruluşun yeniden teşkilatlandırılması olup, yürürlükte bulunan kanunlara dayanılarak ve kamu görevlisinin öznel durumu dikkate alınarak idarece tesis edilen naklen atama işlemlerinden farklıdır. Söz konusu hukukî ve fiilî zorunluluklar nedeniyle kazanılmış haklar korunarak başka kadrolara atama yapılması, kanun koyucunun takdir yetkisi kapsamındadır.

109. Dava konusu kuralla, Gençlik ve Spor Bakanlığı merkez teşkilatı ile Bakanlığın bağlı kuruluşu olan Spor Genel Müdürlüğü merkez ve taşra teşkilatında yer alan bazı kadrolarda görev yapanların, görevlerinin hiçbir işleme gerek kalmaksızın sona ermesi öngörülmektedir.

110. 6639 sayılı Kanun'un 22. maddesiyle 638 sayılı KHK'ya eklenen geçici 12. maddede, Gençlik ve Spor Bakanlığının bağlı kuruluşu olan Yüksek Öğrenim Kredi ve Yurtlar Kurumu Genel Müdürlüğüne ait Bölge Müdürlüklerinin kapatılması ve kapatılan Bölge Müdürlüklerinin kullanımında olan her türlü taşınır ile taşıt, araç, gereç ve malzeme, varsa her türlü borç ve alacaklar, yazılı ve elektronik ortamdaki her türlü kayıtlar ve diğer dokümanlar ile personelin Kredi ve Yurtlar İl Müdürlüklerine devredilmesi öngörülmüş, Gençlik ve Spor Bakanlığı ile Spor Genel Müdürlüğünün teşkilat yapısına ilişkin herhangi bir değişikliğe gidilmemiştir. Yüksek Öğrenim Kredi ve Yurtlar Kurumu Genel Müdürlüğü teşkilatında yapılan değişiklikler ise Gençlik ve Spor Bakanlığı merkez teşkilatı ile Spor Genel Müdürlüğünün merkez ve taşra teşkilatında yer alan bazı kadrolarda bulunanların görevlerinin sona ermesini gerektiren hukukî ve fiilî zorunluluk olarak değerlendirilemez.

111. Bu itibarla, Gençlik ve Spor Bakanlığı merkez teşkilatı ile Spor Genel Müdürlüğünde dava konusu kuralın yer aldığı fıkrada belirtilen kadrolarda görev yapan kişilerin, bu görevlerine hiçbir

işleme gerek kalmaksızın son verilmesini öngören kural hukukî güvenlik ilkesiyle bağdaşmamaktadır.

112. Açıklanan nedenlerle kural, Anayasa'nın 2. maddesine aykırıdır. İptali gerekir.

113. Osman Alifeyyaz PAKSÜT, Hicabi DURSUN, Kadir ÖZKAYA, Rıdvan GÜLEÇ ile Recai AKYEL bu görüşe katılmamışlardır.

114. Kural, Anayasa'nın 2.maddesine aykırı bulunarak iptal edildiğinden, Anayasa'nın 36., 70. ve 125. maddeleri yönünden ayrıca incelenmesine gerek görülmemiştir.

E- Kanun'un 23. Maddesiyle 375 Sayılı KHK'ya Eklenen Ek 18. Maddenin;

1- Birinci Fıkrasının, (c) Bendinin (2) Numaralı Alt Bendi Dışında Kalan Bölümünün İncelenmesi

a. İptal Talebinin Gerekçesi

115. Dava dilekçesinde özetle, dava konusu kuralla liyakat ilkesine dayanan personel rejiminin yağma sistemine dönüştürüldüğü, görevlerinden alınan veya görev süresi sona eren yönetici kadrosundaki kamu görevlilerinin, ek göstergelerine göre buldukları görevden düşük statülü kadrolara atanmalarına olanak tanınarak bu kişilerin kazanılmış hak ve meşru beklentilerinin korunmadığı, böylece, kamu hizmetlerinin, tarafsız, tüm yurttaşlara eşit, hukuka ve kamu yararına uygun şekilde sunulması güvencesinin ortadan kaldırıldığı, ayrıca atama işlemine karşı idari yargı mercileri önünde dava açma hakkının da sınırlandırıldığı belirtilerek kuralın, Anayasa'nın 2., 5., 36., 70., 125. ve 128. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

116. Dava konusu kuralla, 4857 sayılı İş Kanunu ile 926 sayılı Türk Silâhlı Kuvvetleri Personel Kanunu hariç olmak üzere, tabi oldukları personel kanununa bakılmaksızın Başbakanlık, bakanlıklar, bağlı ve ilgili kuruluşlar ile başkan ve üyeleri hariç olmak üzere düzenleyici ve denetleyici kurumlar ve Tasarruf Mevduatı Sigorta Fonunda, yönetici pozisyonunda çalışan kamu görevlilerinin, görevden alınmaları veya görevlerinin sona ermesi durumunda atanabilecekleri kadrolar düzenlenmektedir. Kuralda, anılan kamu kurum ve kuruluşlarında görevden alınan veya görev süreleri sona eren;

- Müsteşarlar ile ek göstergesi 7600 ve daha yüksek tespit edilen yönetici kadrolarında bulunanların Başbakanlık merkez müşaviri kadrolarına, ek göstergesi 7000 olan yönetici kadrolarında bulunanların Başbakanlık müşaviri kadrolarına,

- Yukarıda belirtilenler hariç olmak üzere ek göstergesi 6400 ve daha yüksek tespit edilen yönetici kadrolarında veya pozisyonlarında bulunanlardan Başbakanlık Merkez Teşkilatı ile bağlı ve ilgili

kuruluşlarında olanların Başbakanlık müşaviri, bakanlık merkez teşkilatları ile bağlı ve ilgili kuruluşlarında olanların bakanlık müşaviri kadrolarına, düzenleyici ve denetleyici kurumlar ile Tasarruf Mevduatı Sigorta Fonunda görev yapanların ise kurumlarının müşavir veya danışman kadro veya pozisyonlarına,

- Ek göstergeleri 3600 (dâhil) ila 6400 (hariç) olarak tespit edilen yönetici kadro veya pozisyonlarında bulunanlardan, daha önce 657 sayılı Devlet Memurları Kanunu'nun 36. maddesinin "Ortak Hükümler" bölümünün (A) fıkrasının (11) numaralı bendinde sayılan merkez teşkilatına ait kadrolar ile mesleğe alınmaları, yetiştirilmeleri ve yeterlilikleri aynı veya benzer nitelik arz eden merkez teşkilatına ait kadro veya pozisyonlarda bulunanların, daha önceki bu kadro veya pozisyonlarına,

- Ek göstergeleri 3600 (dâhil) ila 6400 (hariç) olarak tespit edilen yönetici kadro veya pozisyonlarında üç yıldan az görev yapmış olanlardan, daha önce 657 sayılı Devlet Memurları Kanunu'nun 36. maddesinin "Ortak Hükümler" bölümünün (A) fıkrasının (11) numaralı bendinde sayılan merkez teşkilatına ait kadrolar ile mesleğe alınmaları, yetiştirilmeleri ve yeterlilikleri aynı veya benzer nitelik arz eden merkez teşkilatına ait kadro veya pozisyonlarda bulunmayanların, merkez veya taşra teşkilatına ait araştırmacı kadro veya pozisyonlarına,

- Ek göstergesi 3600'den daha düşük tespit edilen yönetici kadro veya pozisyonlarında bulunanlardan, daha önce 657 sayılı Kanunun 36. maddesinin "Ortak Hükümler" bölümünün (A) fıkrasının (11) numaralı bendinde sayılan merkez teşkilatına ait kadrolar ile mesleğe alınmaları, yetiştirilmeleri ve yeterlilikleri aynı veya benzer nitelik arz eden kadro veya pozisyonlarda bulunanların daha önceki bu kadro veya pozisyonlarına, diğerlerinin ise merkez veya taşra teşkilatına ait araştırmacı kadro veya pozisyonlarına,

atanmaları öngörülmüş, bu şekilde atananlardan bir ay içinde talepte bulunanların ise atamaya yetkili amirler tarafından bu fıkra kapsamında yer alan yönetici kadro veya pozisyonları dışındaki daha önce buldukları veya öğrenim durumları itibarıyla ihraz etmiş oldukları unvanlara ilişkin kadro veya pozisyonlara bir ay içinde atanmaları hüküm altına alınmıştır.

117. Anayasa'nın 128. maddesinde, Devletin, kamu iktisadi teşebbüsleri ve diğer kamu tüzel kişilerinin genel idare esaslarına göre yürütmekle yükümlü oldukları kamu hizmetlerinin gerektirdiği asli ve sürekli görevlerinin, memurlar ve diğer kamu görevlileri eliyle görüleceği, memurların ve diğer kamu görevlilerinin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülükleri, aylık ve ödenekleri ile diğer özlük işlerinin mali ve sosyal haklara ilişkin toplu sözleşme hükümleri saklı kalmak kaydıyla kanunla düzenleneceği, üst kademe yöneticilerinin yetiştirilme usul ve esaslarının da kanunla özel olarak düzenleneceği hükme bağlanmıştır.

118. Memurların atanması, görev ve yetkileri, aylıkları ve ödenekleri ile diğer özlük işleri, kural olarak 657 sayılı Kanun'da düzenlenmiştir. Bu Kanun, bütün memurlar yönünden genel kanun niteliğindedir. Kanun'un 4. maddesinin (A) fıkrasına göre memurlar, mevcut kuruluş biçimine bakılmaksızın, Devlet ve diğer kamu tüzel kişiliklerince genel idare esaslarına göre yürütülen asli ve sürekli kamu hizmetlerini ifa ile görevlendirilmişlerdir.

119. Memur ile idare arasındaki ilişki, yasama organı tarafından hizmetin gereklerine göre kanunla düzenlenmektedir. Memur, belirli bir statüde, kanunla çerçevesi belirlenmiş nesnel kurallara göre hizmet yürütmekte, o statünün sağladığı aylık, ücret, atanma, yükselme, nakil gibi kimi öznel haklara sahip olmaktadır. Kanun koyucu, bir kamu hizmetinde, görevin gerektirdiği nitelikleri ve koşulları saptamayı ya da saptanmış olanları değiştirmeyi, anayasal ilkeler içerisinde kalmak kaydıyla, görevin ve ülkenin gereklerine göre serbestçe takdir edebilir. Bu çerçevede, memurların yönetici kadro veya pozisyonlarına veya bu görevlerden alınarak başka bir kadroya atanma usulleri ile görevin kapsamı ve süresi ile ilgili konularda anayasal ilkelere aykırı olmamak kaydıyla kanun koyucu tarafından düzenleme yapılabilir.

120. Anayasa'nın 2. maddesinde yer alan hukuk devleti ilkesinin temel gereklerinden biri kazanılmış haklara saygı gösterilmesidir. Kazanılmış haklara saygı, hukuk güvenliği ilkesinin bir sonucudur. Kamu görevlilerinin kazanılmış hakları, istihdam türüne bağlı olarak tahakkuk etmiş ve kendisi yönünden kesinleşmiş ve kişisel alacak niteliğine dönüşmüş haklardır. Objektif ve genel hukuksal durumun, şart işlemle özel hukuksal duruma dönüşmesi kazanılmış hak yönünden yeterli değildir. Kural işlemler her zaman değiştirilebilir ya da yargı organları tarafından Anayasa'ya veya kanuna aykırı görülerek iptal edilebilir. Bir statüye bağlı olarak ileriye dönük, beklenen haklar kazanılmış hak kapsamında değerlendirilmez.

121. 657 sayılı Kanun'un 76. maddesinin birinci fıkrasında, kurumların, görev ve unvan eşitliği gözetmeden kazanılmış hak aylık dereceleriyle memurları buldukları kadro derecelerine eşit veya 68. maddedeki esaslar çerçevesinde daha üst, kurum içinde aynı veya başka yerlerdeki diğer kadrolara naklen atayabilecekleri hüküm altına alınmakla birlikte, yönetici kadro veya pozisyonunda görev yapmakta iken görevden alınan veya görev süresi sona eren kamu görevlilerinin hangi pozisyona atanabileceğini düzenleyen bir norm bulunmamaktadır. Bu durum, görevden alınan veya görev süresi sona eren kamu görevlisinin atanacağı pozisyon bakımından idareler arasında farklı uygulamalara sebebiyet verebilmektedir. Dava konusu kurullarla bu duruma son verilerek, başbakanlık, bakanlıklar, bağlı ve ilgili kuruluşlar ile başkan ve üyeleri hariç olmak üzere düzenleyici ve denetleyici kurumlar ve Tasarruf Mevduatı Sigorta Fonunda, yönetici kadro veya pozisyonunda

çalışan kamu görevlilerinin, görevden alınmaları veya görevlerinin sona ermesi durumunda atanabilecekleri kadrolar ayrıntılı bir şekilde düzenlenmiştir. Böylece, yönetici kadro veya pozisyonunda görev yapmakta iken görevden alınan veya görev süresi sona eren kamu görevlilerinin atanacağı kadrolar önceden belirlenerek bu kişilerin atanabileceği kadrolar yönünden belirsizlik ortadan kaldırıldığı gibi kamu kurumları arasındaki farklı uygulamaların da önüne geçilmesi sağlanmıştır.

122. İdarenin, yönetici kadro veya pozisyonlarına atadığı kişileri meslek hayatları boyunca bu kadrolarda çalıştırma gibi bir zorunluluğu bulunmamaktadır. Bu nedenle, yönetici kadro veya pozisyonlarına atanan kişiler yönünden bulunduğu statülerden doğan, tahakkuk etmiş ve kendileri yönünden kesinleşmiş ve kişisel alacak niteliğine dönüşmüş haklardan yahut bu durumunun devam edeceği yönündeki haklı beklentiden söz edilemez. Dolayısıyla, yönetici kadro veya pozisyonunda görev yapmakta iken görev süresi dolan veya görevden alınan kamu görevlilerinin atanacakları kadroları belirleyen dava konusu kuralın kazanılmış hak veya genel olarak hukuk güvenliği ilkesini ihlal eden bir yönü bulunmamaktadır.

123. Anayasa'nın "Hak arama hürriyeti" başlıklı 36. maddesinin birinci fıkrasında, "Herkes, meşrû vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir." denilerek söz konusu haklar güvence altına alınmıştır. Anayasa'nın 125. maddesinde ise "İdarenin her türlü eylem ve işlemlerine karşı yargı yolu açıktır..." denilmektedir. Her iki maddeyle güvence altına alınan dava yoluyla hak arama özgürlüğü, kendisi bir temel hak niteliği taşımasının ötesinde diğer temel hak ve özgürlüklerden gereken şekilde yararlanılmasını ve bunların korunmasını sağlayan en etkili güvencelerden biridir. Kişilere yargı mercileri önünde dava hakkı tanınması adil yargılamanın ön koşulunu oluşturur.

124. Dava konusu kuralla yönetici kadro veya pozisyonunda görev yapan kamu görevlilerinin kuralda belirtilen kadrolara atanmış sayılması değil, idari bir işlemle görevden alınması veya görev süresinin sona ermesi durumunda atanacağı pozisyonlar düzenlenmektedir. Dolayısıyla dava konusu kuralın doğrudan uygulanma kabiliyeti bulunmamakta olup kuralların uygulanabilmesi için idarenin kamu görevlileri hakkında işlem tesis etmesi gerekmektedir. Anayasa'nın 125. maddesi uyarınca kural olarak tüm idari işlemlerde olduğu gibi anılan idari işlemler yönünden de kişilerin yargı mercilerine başvurması mümkün olduğundan kuralın hak arama özgürlüğünü zedeleyen bir yönü bulunmamaktadır.

125. Açıklanan nedenlerle kural, Anayasa'nın 2., 36., 125. ve 128. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

126. Kuralın Anayasa'nın 5. ve 70. maddeleriyle ilgisi görülmemiştir.

2- Birinci Fıkrasının (c) Bendinin (2) Numaralı Alt Bendinin İncelenmesi

a. İptal Talebinin Gerekçesi

127. Dava dilekçesinde özetle, kariyer mesleklerin giriş şartları, mesleki nitelik ve özellikleri ile kamu yönetimindeki işlevleri gözetildiğinde daha önce kariyer meslek sınıfında görev yapmayan yönetici pozisyonundaki kamu görevlilerinin, görevden alındıktan sonra kariyer meslek sınıfına atanmalarına olanak tanınmasının, hukuk devleti ilkesiyle bağdaşmadığı, bu kişilerin kariyer mesleklere sınavla girip belli bir eğitimden sonra atanmalarla aynı konuma getirilmelerinin eşitlik ilkesini zedelediği belirtilerek kuralın, Anayasa'nın 2. ve 10. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

128. Dava konusu kural, daha önce 657 sayılı Kanunun 36. maddesinin "Ortak Hükümler" bölümünün (A) fıkrasının (11) numaralı bendinde sayılan merkez teşkilatına ait kadrolar ile mesleğe alınmaları, yetiştirilmeleri ve yeterlilikleri aynı veya benzer nitelik arz eden kadro veya pozisyonlarda bulunmamakla birlikte ek göstergeleri 3600 (dâhil) ila 6400 (hariç) olarak tespit edilen yönetici kadro veya pozisyonlarında toplam en az üç yıl görev yapmış olanların, görevden alınmaları veya görev sürelerinin sona ermesi durumunda anılan kadrolara atanmalarını öngörmektedir

129. Bir önceki başlık altında belirtilen gerekçeler dava konusu kural yönünden de geçerli olup, kanun koyucu, kamu yararı ve hizmetin gereklerini dikkate alarak kamu görevlilerinin statüsünde, unvanlarında, görev ve yetkilerinde değişiklikler yapabileceği gibi bu statüye atanma koşullarında da değişiklikler yapabilir.

130. Dava konusu kuralla daha önce kariyer meslek kadrosunda görev yapmayan yönetici kadro veya pozisyonundaki kamu görevlilerinin, yönetici kadro veya pozisyonunda belli bir süre görev yaptıktan sonra yeterli birikime ve deneyime sahip oldukları düşüncesiyle kariyer meslek kadrolarına atanabilmelerine olanak tanınmaktadır. Kuralla bu kadrolardaki kişilerin kariyer meslek kadrolarına atanabilmesine olanak tanınmasıyla kamu yararının gerçekleşip gerçekleşmeyeceği ise anayasallık denetiminin kapsamı dışındadır. Bu itibarla, daha önce 657 sayılı Kanunun 36. maddesinin "Ortak Hükümler" bölümünün (A) fıkrasının (11) numaralı bendinde sayılan merkez teşkilatına ait kadrolar ile mesleğe alınmaları, yetiştirilmeleri ve yeterlilikleri aynı veya benzer nitelik arz eden kadro veya pozisyonlarda bulunmamakla birlikte toplam en az üç yıl süreyle ek göstergesi 3600 (dâhil) ila 6400 (hariç) olarak tespit edilen yönetici kadro veya pozisyonlarında bulunan kamu

görevlilerinin, anılan kadrolara atanmalarına olanak tanıyan kural kanun koyucunun takdir yetkisi kapsamında olup, kuralda hukuk devleti ilkesine aykırılık bulunmamaktadır.

131. Diğer taraftan, toplam en az üç yıl süreyle yönetici kadro veya pozisyonunda görev yaparak belli bir yetkinliğe sahip olduktan sonra kariyer meslek kadrolarına atanmaya hak kazanan kamu görevlileriyle mesleğe, özel bir yarışma sınavını kazanarak, belli bir eğitim ve yeterlilik sürecini başarıyla tamamladıktan sonra atanmaya hak kazananlar aynı hukuksal konumda bulunmamaktadır. Bu nedenle, en az üç yıl süreyle yönetici kadro veya pozisyonunda görev yaparak belli bir yetkinliğe sahip olduktan sonra kariyer meslek kadrolarına atanan kamu görevlileriyle mesleğe, özel bir yarışma sınavını kazanarak, belli bir eğitim ve yeterlilik sürecini başarıyla tamamladıktan sonra atananlar arasında eşitlik karşılaştırması yapılamaz.

132. Açıklanan nedenlerle kural, Anayasa'nın 2. ve 10. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

3- İkinci Fıkrasının İncelenmesi

a. İptal Talebinin Gerekçesi

133. Dava dilekçesinde özetle, 375 sayılı KHK'nın ek 18. maddesinin birinci fıkrasının Anayasa'ya aykırılığı yönünden belirtilen gerekçelerle kuralın, Anayasa'nın 2., 5., 36., 70., 125. ve 128. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

134. Dava konusu kuralda, yönetici kadro veya pozisyonunda görev yapmakta iken görevden alınan veya görev süresi sona eren kamu görevlilerinin, 375 sayılı KHK'nın ek 18. maddesinin birinci fıkrasında belirtilen kadrolara atamalarının yapılabilmesi için uygun boş kadro veya pozisyon bulunmaması hâlinde, bunlar için başka bir işleme gerek kalmaksızın, söz konusu kadro veya pozisyonların kendiliğinden ihdas edilmiş ve kurumların kadro veya pozisyon cetvellerinin ilgili bölümlerine eklenmiş sayılacağı, bu şekilde ihdas edilmiş sayılan kadro ve pozisyonların boşalması halinde, herhangi bir işleme gerek kalmaksızın iptal edilmiş sayılacağı, anılan kadro ve pozisyonlara atananların, atamaya yetkili amirleri tarafından belirlenen birimlerde istihdam edileceği hüküm altına alınmaktadır.

135. KHK'nın ek 18. maddesinin birinci fıkrası için belirtilen gerekçeler dava konusu kural yönünden de geçerli olup, Anayasa'ya uygun olmak kaydıyla, kamu hizmetinin yürütülmesine ilişkin koşulları belirleyerek kadro düzenlemesi yapma yetkisi kanun koyucuya aittir. Bu bağlamda, kanun koyucu,

kamu hizmetinin gerekleri yönünden ve kamu yararı amacıyla yeni kadrolar ihdas edebileceği gibi mevcut bazı kadroları birleştirebilir ya da kaldırabilir.

136. Yönetici kadro veya pozisyonunda görev yapmakta iken görevden alınan veya görev süresi sona eren kamu görevlilerinin, KHK'nın ek 18. maddesinin birinci fıkrasında belirtilen kadrolara atanabilmesi için uygun boş kadronun bulunması gerekmektedir. Bu durum kuşkusuz kadrosuz memur çalıştırılmayacağı kuralının da bir sonucudur. Dava konusu kuralla, görev süresi sona eren veya görevden alınan kamu görevlisinin atanacağı uygun boş kadro bulunmaması durumunda bu kadroların ihdas edilmiş sayılması öngörülmektedir. Yönetici kadro veya pozisyonundaki kamu görevlilerinin, görevden alınması veya görev süresinin sona ermesi durumunda bir an önce yeni kadrolarına atamalarının yapılmasına olanak tanınması, Anayasa'nın 128. maddesi kapsamında kanun koyucunun takdir yetkisinde olup, kuralda hukuk devleti ilkesi ile çelişen bir yön bulunmamaktadır.

137. Açıklanan nedenlerle kural, Anayasa'nın 2. ve 128. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

138. Kuralın Anayasa'nın, 5., 36., 70. ve 125. maddeleriyle ilgisi görülmemiştir.

4- Üçüncü Fıkrasının İncelenmesi

a. İptal Talebinin Gerekçesi

139. Dava dilekçesinde özetle, KHK'nın ek 18. maddesinin birinci fıkrasının Anayasa'ya aykırılığı yönünden belirtilen gerekçelerle kuralın, Anayasa'nın 2., 5., 36., 70., 125. ve 128. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

140. Dava konusu kuralda, yönetici kadro veya pozisyonunda görev yapmakta iken görevden alınan veya görev süresi sona eren kamu görevlilerine, yönetici kadro veya pozisyonlarında kesintisiz olarak en az iki yıl fiilen görev yapmış olanların mali haklarının, KHK'nın ek 18. maddesinin birinci fıkrası uyarınca atandıkları kadro veya pozisyonlarda bulunmaları kaydıyla, atandıkları tarihi takip eden ay başından itibaren ikinci yılın sonuna kadar fiili çalışmaya bağlı ödemeler hariç, önceki görevine ait ödeme unsurları esas alınarak verilmeye devam edileceği öngörülmektedir.

141. KHK'nın ek 18. maddesinin birinci fıkrası için belirtilen gerekçeler, dava konusu kural yönünden de geçerli olup, kanun koyucu statü hukuku çerçevesinde, görevden alınan veya görev süresi sona eren yönetici kadro veya pozisyonundaki kamu görevlilerinin mali haklarına ilişkin koşulları

anayasal ilkelere uygun olarak belirleme yetkisine sahiptir. Kanun koyucu kamu görevlilerinin mali haklarını düzenlerken özellikle kazanılmış hak ilkesine riayet etmek zorundadır.

142. Kamu görevlilerinin kazanılmış hakları, istihdam türüne bağlı olarak tahakkuk etmiş ve kendisi yönünden kesinleşmiş ve kişisel alacak niteliğine dönüşmüş haklardır. Bir statüye bağlı olarak ileriye dönük, beklenen haklar ise bu nitelikte değildir. Diğer bir ifadeyle, bir kamu görevlisinin daha önce görev yaptığı unvana bağlı olarak elde ettiği mali haklar, ileriye dönük kazanılmış hak şeklinde değerlendirilemez. Bu nedenle, yönetici kadro veya pozisyonunda görev yapmakta iken görevden alınan veya görev süresi sona eren kamu görevlilerinin bu görevler nedeniyle elde ettikleri mali hakların, görevden ayrıldıktan sonra atandığı kadro bakımından kazanılmış hak olarak değerlendirilmesine olanak bulunmamaktadır.

143. Dava konusu kuralın, belli bir süre yönetici kadro veya pozisyonunda görev yaptıktan sonra görevden alınan veya görev süresi sona eren kamu görevlilerinin, bir süre daha eski görevine ait mali haklardan yararlanmasını sağlamak amacıyla ihdas edildiği anlaşılmaktadır. Kural gereğince, kamu görevlileri, ancak kesintisiz olarak en az iki yıl fiilen yönetici kadro veya pozisyonunda görev yapmak ve KHK'nın ek 18. maddesinin birinci fıkrası uyarınca atandıkları kadro veya pozisyonlarda bulunmak kaydıyla, atandıkları tarihi takip eden ay başından itibaren iki yıl süreyle önceki görevine ait mali haklardan yararlanmaya devam edecektir.

144. Buna göre, yönetici kadro veya pozisyonunda görev yapmakta iken görevden alınan veya görev süresi sona eren kamu görevlilerinin, belli şartlar altında eski görevine ait mali haklardan iki yıl süreyle daha yararlandırılması, şartları taşımayan kamu görevlilerinin ise bu haklardan yararlandırılmaması Anayasa'nın 128. maddesi kapsamında kanun koyucunun takdir yetkisinde olup, kuralda kazanılmış hak ilkesini ihlal eden bir yön bulunmamaktadır.

145. Açıklanan nedenlerle kural, Anayasa'nın 2. ve 128. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

146. Kuralın Anayasa'nın 5., 36., 70. ve 125. maddeleriyle ilgisi görülmemiştir.

F- Kanun'un 24. Maddesiyle 375 Sayılı KHK'nın Eki (I) Sayılı Cetvel'in "A- Aylıklarını 657 sayılı Devlet Memurları Kanununa Göre Alanlar" Kısımının "1-Kadroları Genel İdare Hizmetleri Sınıfında yer alan personel ile Teknik Hizmetler, Sağlık ve Yardımcı Sağlık Hizmetleri ile Avukatlık Hizmetleri sınıflarında bulunan personelden ek ödeme oranları ilgili gruplarında düzenlenmeyen ve kadro unvanları bu bölümde yer alan personel" Bölümünün;

1- (d) Sırasında Yer Alan "büyükşehir belediyesi bulunan illerin il özel idaresi genel sekreter yardımcısı, diğer illerin il özel idaresi genel sekreteri," İbaresinin "il özel idaresi genel sekreteri," Şeklinde;(e) Sırasında Yer Alan "büyükşehir belediyesi bulunan illerin il özel idaresi I. hukuk müşaviri, büyükşehir belediyesi bulunmayan illerin il özel idaresi genel sekreter yardımcısı," İbaresinin "il özel idaresi genel sekreter yardımcısı," Şeklinde Değiştirilmesinin İncelenmesi

a. Genel Açıklama

147. 11.10.2011 tarihli ve 666 sayılı KHK ile 375 sayılı KHK'ya ilave edilen ek 9. ve ek 10. maddeler ile kamu görevlilerine yapılan aylık ve ek ödemelere ilişkin köklü değişikliklere gidilmiştir.

148. 375 sayılı KHK'nın ek 9. maddesiyle, kamu personeli için kurumsal ek ödemelerden kaynaklanan farklılıkların giderilmesi amacıyla tüm kurumsal ek ödemeler kaldırılarak tek bir ek ödeme sistemi getirilmiştir. KHK'ya ek (I) sayılı cetvelde de ek ödeme yapılacak kamu görevlilerinin kadro ve görev unvanları ile ek ödeme oranları gösterilmiştir.

149. 375 sayılı KHK'nın ek 10. maddesinde ise kamu idarelerinin merkez teşkilatları için ihdas edilen uzman kadroları ile merkez ve taşra teşkilatlarının bazı yönetici kademelerinde görev yapan personelin aylıklarındaki kurumlararası farklılıkların ortadan kaldırılması amacıyla ücret ve tazminat unsurlarından oluşan yeni bir ödeme sistemi getirilmiştir. Maddeye göre, KHK'ya ek (II) sayılı cetvelde sayılan kadrolarda görev yapanlara, kadro unvanlarına karşılık gelen gösterge rakamlarının memur aylık katsayısı ile çarpımı sonucu bulunacak tutarlarda ücret ve tazminat ödemesi yapılması öngörülmüştür.

150. 5302 sayılı İl Özel İdaresi Kanunu'nun 36. maddesinin dördüncü fıkrasında, büyükşehir olmayan illerde genel sekreter kadrosuna atananların genel idare hizmetleri sınıfına dahil bakanlık müstakil daire başkanları, genel sekreter yardımcısı kadrosuna atananların ise genel idare hizmetleri sınıfına dahil bakanlık daire başkanları için ilgili mevzuatında öngörülen ek gösterge, makam, görev ve temsil tazminatları ile 657 sayılı Kanun'un 152. maddesi uyarınca ödenen zam ve tazminatlardan aynı usul ve esaslar dahilinde yararlanacakları hüküm altına alınmıştır. Kurala göre il özel idaresi genel sekreteri ile yardımcılarının aylıklarının hesabında, bakanlık müstakil daire başkanları ile bakanlık daire başkanları için öngörülen ek gösterge, makam, görev ve temsil tazminatları ile 657 sayılı Kanun'un 152. maddesi uyarınca ödenen zam ve tazminatlar göz önünde bulundurulacak ve bu oranlara göre aylıkları hesaplanacaktır. Ayrıca dava konusu kurullarla, aylıklarına ilave olarak il özel idaresi genel sekreterine % 190, genel sekreter yardımcısına da % 185 oranında ek ödeme yapılacaktır.

151. Bakanlık müstakil daire başkanları ile bakanlık daire başkanları ise 375 sayılı KHK'ya ek (II) sayılı cetvelde yer aldığından, bu görevlerde bulunanlar (II) sayılı cetvelde unvanlarına karşılık gelen ücret ve tazminat göstergeleri üzerinden aylıklarını alacaklardır. Bakanlık müstakil daire başkanlığı kadrosu (II) sayılı cetvelin (7) numaralı sırasında; bakanlık daire başkanlığı kadrosu ise (8) numaralı sırada düzenlenmiştir. Bu kapsamda bakanlık müstakil daire başkanlarına ek (II) sayılı cetvelin (7) numaralı sırasında bulunan kadrolar için öngörülen 54.300 ücret ve 30.000 tazminat göstergesi, bakanlık daire başkanlarına ise (8) numaralı sırasında bulunan kadrolar için öngörülen 51.900 ücret ve 28.575 tazminat göstergesi üzerinden hesaplanacak tutarda aylık ödenecektir.

b. İptal Taleplerinin Gerekçesi

152. Dava dilekçesinde özetle, 5302 sayılı Kanun'un 36. maddesinin dördüncü fıkrasında, büyükşehir olmayan illerde görev yapan il özel idaresi genel sekreterlerinin, genel idare hizmetlerine dahil bakanlık müstakil daire başkanları; genel sekreter yardımcılarının ise bakanlık daire başkanları için ilgili mevzuatında öngörülen ek gösterge, makam, görev ve temsil tazminatları ile 657 sayılı Kanun'un 152. maddesi uyarınca ödenen zam ve tazminatlardan aynı usul ve esaslar dahilinde yararlandırılmasının öngörüldüğü, bu doğrultuda, il özel idaresi genel sekreterinin, bakanlık müstakil daire başkanlarının bulunduğu 375 sayılı KHK'nın eki (II) sayılı cetvelin (7) numaralı sırasında; il özel idaresi genel sekreter yardımcısının ise bakanlık daire başkanlarının bulunduğu (8) numaralı sırasında yer alması gerekirken anılan kadroların ek (I) sayılı cetvelde düzenlendiği, bu durumun eşdeğer görev olan Bakanlık müstakil daire başkanlığı ile bakanlık daire başkanlığında görev yapanlara nazaran daha düşük maaş almalarına sebebiyet verdiği belirtilerek kuralların, Anayasa'nın 2., 10. ve 55. maddelerine aykırı olduğu ileri sürülmüştür.

c. Anayasa'ya Aykırılık Sorunu

153. 6216 sayılı Kanun'un 43. maddesi uyarınca, dava konusu kurallar ilgisi nedeniyle Anayasa'nın 128. maddesi yönünden de incelenmiştir.

154. Dava konusu kurallarla il özel idaresi genel sekreteri ile genel sekreter yardımcısı kadrolarında görev yapanlara 375 sayılı KHK'ya ek (I) sayılı cetvelde yer verilerek aylıklarına ilave olarak % 190 ve % 185 oranında ek ödeme yapılması öngörülmektedir. Uyuşmazlığın özünü, il özel idaresi genel sekreteri ile yardımcılarının, 375 sayılı KHK'nın (I) sayılı cetveli yerine eşdeğer görev olduğu ileri sürülen bakanlık müstakil daire başkanları ile bakanlık daire başkanlarının yer aldığı (II) sayılı cetvelde yer alması gerektiği hususu oluşturmaktadır.

155. Anayasa'nın 2. maddesinde belirtilen hukuk devleti, insan haklarına dayanan, bu hak ve özgürlükleri koruyup güçlendiren, eylem ve işlemleri hukuka uygun olan, her alanda adaletli bir hukuk düzeni kurup bunu geliştirerek sürdüren, hukuki güvenliği sağlayan, Anayasa'ya aykırı durum ve tutumlardan kaçınan, hukuku tüm devlet organlarına egemen kılan, Anayasa ve kanunlarla kendini bağlı sayan, yargı denetimine açık olan devlettir. Hukuk devletinde kanun koyucunun kazanılmış hakları ihlal etmemek koşuluyla kamu hizmetinin yürütülmesine ilişkin koşulları belirlemesine engel bulunmamaktadır.

156. Anayasa'nın "Ücrette adalet sağlanması" başlıklı 55. maddesinde "Ücret emeğin karşılığıdır. Devlet, çalışanların yaptıkları işe uygun adaletli bir ücret elde etmeleri ve diğer sosyal yardımlardan yararlanmaları için gerekli tedbirleri alır. Asgarî ücretin tespitinde çalışanların geçim şartları ile ülkenin ekonomik durumu da gözönünde bulundurulur." denilmektedir. Maddeyle, emeğin karşılıksız bırakılmaması ve emeğin karşılığının ücret olarak verilmesi amaçlanmaktadır.

157. Kamu görevlileri ile kamu yönetimleri arasındaki ilişkiler kural tasarruflarla düzenlenmektedir. Kamu personeli, belirli bir statüde, nesnel kurallara göre hizmet yürütmekte, o statünün sağladığı ücret, atanma, yükselme gibi kimi haklara sahip olmaktadır. Kamu hizmetine giriş, hizmet içinde yükselme ve bulunulan statünün sağladığı haklar, statü hukukunun gereği olarak kanunlarla belirlenmektedir. Bu durum, Anayasa'nın kamu görevlileriyle ilgili genel ilkelerin düzenlendiği 128. maddesinden kaynaklanan bir zorunluluktur. Kanun koyucu, statü hukuku çerçevesinde yürütülen memuriyet hizmetine girmeye, memuriyette yükselmeye, özlük haklarına ve bunun gibi diğer hususlara ilişkin koşulları anayasal ilkelere uygun olarak belirleme yetkisine sahiptir.

158. 5302 sayılı Kanun'un 35. maddesinin ikinci fıkrasında, il özel idaresi genel sekreterinin, il özel idaresi hizmetlerini vali adına ve onun emirleri yönünde, mevzuat hükümlerine, il genel meclisi ve il encümeni kararlarına, il özel idaresinin amaç ve politikalarına, stratejik plan ve yıllık çalışma programına göre düzenleyip yürütmekle görevli olduğu belirtilmiş, maddenin dördüncü fıkrasında da toplam nüfusu 3.000.000'a kadar olan illerde ihtiyaca göre en fazla iki, nüfusu bunun üzerinde olan illerde ise en fazla dört genel sekreter yardımcılığı kadrosunun ihdas edilebileceği ifade edilmiştir.

159. 5302 sayılı Kanun'un 36. maddesinin dördüncü fıkrasında, büyükşehir olmayan illerde genel sekreter kadrosuna atananların genel idare hizmetleri sınıfına dahil bakanlık müstakil daire başkanları, genel sekreter yardımcısı kadrosuna atananların ise bakanlık daire başkanları için ilgili mevzuatında öngörülen ek gösterge, makam, görev ve temsil tazminatları ile 657 sayılı Kanun'un 152.

maddesi uyarınca ödenen zam ve tazminatlardan aynı usul ve esaslar dahilinde yararlanacakları hüküm altına alınmıştır.

160. Dava konusu kurallarda ise aylıklarına ilave olarak il özel idaresi genel sekreterine % 190, genel sekreter yardımcısına %185 oranında ek ödeme yapılması öngörülmüştür. Buna göre anılan kadrolarda görev yapanların aylıkları 5302 sayılı Kanun'un 36. maddesinin dördüncü fıkrası uyarınca hesaplanmaya devam edecek, dava konusu kurullarla da aylıklarına ilaveten kadrolarına karşılık gelen oranlarda ek ödeme yapılacaktır. Bu açıdan bakıldığında kurulların, il özel idaresi genel sekreteri ve yardımcılarının mali haklarında bir azalmaya sebebiyet verdiği söylenemez. Bu itibarla, il özel idaresi genel sekreteri ile sekreter yardımcısının aylıklarına ilave olarak ek ödeme yapılmasına olanak tanıyan kurullar, statü hukuku çerçevesinde kamu görevlilerinin özlük haklarının belirlenmesi kapsamında kanun koyucunun takdir yetkisinde olup, kurullarda hukuk devleti ilkesi ile emeğin karşılıksız bırakılmamasını amaçlayan Anayasa'nın 55. maddesine aykırılık bulunmamaktadır.

161. Anayasa'nın 10. maddesinde belirtilen "kanun önünde eşitlik ilkesi" hukuksal durumları aynı olanlar için söz konusudur. Bu ilke ile eylemli değil, hukuksal eşitlik öngörülmüştür. Eşitlik ilkesinin amacı, aynı durumda bulunan kişilerin kanunlar karşısında aynı işleme bağlı tutulmalarını sağlamak, ayırım yapılmasını ve ayrıcalık tanınmasını önlemektir. Belirtilen ilkeyle, aynı durumda bulunan kimi kişi ve topluluklara ayrı kurullar uygulanarak yasa karşısında eşitliğin ihlali yasaklanmıştır. Kanun önünde eşitlik, herkesin her yönden aynı kurullara bağlı tutulacağı anlamına gelmez. Durumlarındaki özellikler, kimi kişiler ya da topluluklar için değişik kurulları ve uygulamaları gerektirebilir. Aynı hukuksal durumlar aynı, ayrı hukuksal durumlar farklı kurullara bağlı tutulursa Anayasa'da öngörülen eşitlik ilkesi zedelenmez.

162. İl özel idaresi genel sekreteri ile yardımcıları, mahalli idare olarak örgütlenen il özel idaresi bünyesinde 5302 sayılı Kanun'la kendilerine verilen görevleri yapmaktadırlar. Genel idare hizmetleri sınıfına dahil olan bakanlık müstakil daire başkanları ile bakanlık daire başkanları ise kuruluş kanunlarında kendilerine verilen görevleri yerine getirmektedir. Dolayısıyla, bir mahalli idare olan il özel idaresi bünyesinde görev yapan il özel idaresi genel sekreteri ve yardımcıları ile genel idare hizmetleri sınıfına dahil olan bakanlık müstakil daire başkanı ve bakanlık daire başkanlarının aynı hukuki konumda buldukları söylenemez.

163. 5302 sayılı Kanun'un 36. maddesinin dördüncü fıkrasında, il özel idaresi genel sekreter kadrosuna atananların genel idare hizmetleri sınıfına dahil bakanlık müstakil daire başkanları, genel sekreter yardımcısı kadrosuna atananların ise bakanlık daire başkanları için ilgili mevzuatında öngörülen ek gösterge, makam, görev ve temsil tazminatları ile 657 sayılı Kanun'un 152. maddesi

uyarınca ödenen zam ve tazminatlardan aynı usul ve esaslar dahilinde yararlandırılması öngörülmekte ise de anılan düzenleme, il özel idaresi genel sekreteri ile yardımcılarının, bakanlık müstakil daire başkanları ile bakanlık daire başkanlarıyla eşdeğer görevde oldukları ve aynı mali haklardan yararlanacakları anlamına gelmemektedir.

164. Dolayısıyla, il özel idaresi genel sekreteri ve yardımcılarının, bakanlık müstakil daire başkanı ile bakanlık daire başkanlarından farklı bir hukuki konumda bulunmaları nedeniyle farklı kurallara tabi tutulmalarında Anayasa'nın 10. maddesinde öngörülen eşitlik ilkesine aykırılık bulunmamaktadır.

165. Açıklanan nedenlerle kurallar, Anayasa'nın 2., 10., 55. ve 128. maddelerine aykırı değildir. İptal taleplerinin reddi gerekir.

2- (g) Sırasına "il yazı işleri müdürü" İbaresinden Önce Gelmek Üzere Eklenen "İl nüfus ve vatandaşlık müdürü" İbaresinin İncelenmesi

a. İptal Talebinin Gerekçesi

166. Dava dilekçesinde özetle, il nüfus ve vatandaşlık müdürlüğü kadrosunun, İçişleri Bakanlığına bağlı bakanlık il müdürü statüsünde olduğu, bu nedenle il nüfus ve vatandaşlık müdürlerinin 375 sayılı KHK'ya ek (II) sayılı cetvelin 9. sırasında yer alan bakanlık il müdürleri için öngörülen gösterge rakamları üzerinden ücret ve tazminat alması gerekmekte iken dava konusu kuralla nüfus ve vatandaşlık işleri müdürlerine ek (I) sayılı cetvelde yer verildiği, bu durumun ise diğer bakanlık il müdürlerine nazaran daha düşük maaş almalarına sebebiyet verdiği belirtilerek kuralın, Anayasa'nın 2., 10. ve 55. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

167. 6216 sayılı Kanun'un 43. maddesi uyarınca, dava konusu kural ilgisi nedeniyle Anayasa'nın 128. maddesi yönünden de incelenmiştir.

168. Dava konusu kuralla il nüfus ve vatandaşlık müdürü olarak görev yapanlara 375 sayılı KHK'ya ek (I) sayılı cetvelde yer verilerek bu kişilerin aylıklarına ilave olarak % 170 oranında ek ödeme yapılması öngörülmektedir. Uyuşmazlığın özünü, il nüfus ve vatandaşlık müdürünün, 375 sayılı KHK'nın (I) sayılı cetveli yerine eşdeğer görev olduğu ileri sürülen bakanlık il müdürlerinin yer aldığı (II) sayılı cetvelde yer alması gerektiği hususu oluşturmaktadır.

169. (155) numaralı paragrafta da ifade edildiği üzere kanun koyucu, Anayasa'nın 128. maddesi uyarınca kamu görevlilerinin özlük haklarına ilişkin koşulları anayasal ilkelere uygun olarak belirleme yetkisine sahiptir. Bu çerçevede, il nüfus ve vatandaşlık müdürlerinin mali haklarını

belirleme yetkisi de kamu görevlilerinin özlük haklarının belirlenmesi kapsamında kanun koyucuya ait olup, bu kadroya 375 sayılı KHK'ya ek (I) sayılı cetvelde yer verilmek suretiyle, aylıklarına ilave olarak % 170 oranında ek ödeme yapılmasını öngören kuralda Anayasa'nın 2. maddesinde yer alan hukuk devleti ilkesi ile ve emeğin karşılıksız bırakılmamasını amaçlayan 55. maddesine aykırılık bulunmamaktadır.

170. 3152 sayılı İçişleri Bakanlığı Teşkilat ve Görevleri Hakkında Kanun'un 3. maddesinde, İçişleri Bakanlığı teşkilatının, merkez ve taşra teşkilatı ile bağlı kuruluşlardan meydana geleceği belirtilmiş; 8. maddesinde, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, Bakanlığın ana hizmet birimi olarak öngörülmüştür. Kanun'un 10. maddesinin birinci fıkrasının (c) bendinde, nüfus hizmetlerini düzenlemek, yürütmek, takip etmek, denetlemek ve değerlendirmek Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü'nün görevleri arasında sayılmıştır. Kanun'un 28. maddesinin birinci fıkrasında, İçişleri Bakanlığının, taşra teşkilatı kurmaya yetkili olduğu, ikinci fıkrasında da nüfus ve vatandaşlık hizmetlerini yürütmek üzere, illerde il nüfus ve vatandaşlık müdürlükleri, ilçelerde ilçe nüfus müdürlükleri kurabileceği hüküm altına alınmıştır. Buna göre, il nüfus ve vatandaşlık işleri müdürlüğü esasında, İçişleri Bakanlığının ana hizmet birimi olan Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü'nün taşra teşkilatını oluşturmaktadır.

171. Bakanlık il müdürleri, bağlı oldukları bakanlıkların, kuruluş kanunlarındaki görev ve yetkilerini, il bazında yerine getirmekle sorumludurlar. İl nüfus ve vatandaşlık müdürleri ise İçişleri Bakanlığının ana hizmet birimlerinden olan Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü'nün görev ve sorumluluğunda bulunan nüfus ve vatandaşlık hizmetlerine ilişkin işlemlerin il bazında yürütülmesinden sorumludurlar. Dolayısıyla, il nüfus ve vatandaşlık müdürlerinin görev ve yetkileri itibarıyla, bakanlık il müdürlerinden farklı hukuki konumda buldukları açıktır. Bu nedenle, il nüfus ve vatandaşlık işleri müdürlerinin, bakanlık il müdürlerinden farklı kurallara tabi tutulmalarında Anayasa'nın 10. maddesinde öngörülen eşitlik ilkesine aykırı bir husus bulunmamaktadır.

172. Açıklanan nedenlerle kural, Anayasa'nın 2., 10., 55. ve 128. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

G- Kanun'un 28. Maddesiyle 2942 Sayılı Kanun'un 4. Maddesinin İkinci Fıkrasının Birinci Cümlesine "...raylı taşıma sistemleri..." İbaresinden Sonra Gelmek Üzere Eklenen "...ile tünel..." İbaresinin İncelenmesi

1. İptal Talebinin Gerekçesi

173. Dava dilekçesinde özetle, günümüz şartlarında taşınmazların altında tünel yapılmasında kamu yararının bulunduğu, ancak mülkiyet hakkının bu yolla sınırlanmasının Anayasa'ya uygun olabilmesi için taşınmaz üzerinde idare lehine irtifak hakkı kurulması ve taşınmazın belirli kesimi, yüksekliği, derinliği veya kaynak üzerindeki fiili kamulaştırmanın gerçek karşılığının ödenmesi gerektiği, taşınmazın değer kaybı için taşınmaz sahiplerine kamulaştırma, tazminat ve benzeri nam altında herhangi bir ücret ödenmeyecek olmasının Anayasa ve Avrupa İnsan Hakları Sözleşmesinde güvence altına alınan mülkiyet hakkının ölçüsüzce sınırlandırılması sonucunu doğurduğu, bu durumun devletin her alanda adaletli bir hukuk düzeni kurması ve hukuk güvenliğini sağlaması yükümlülüğüyle bağdaşmadığı gibi mahkemeye erişimi de sonuçsuz bıraktığı belirtilerek kuralın, Anayasa'nın 2., 13., 35., 36., 46. ve 90.maddelerine aykırı olduğu ileri sürülmüştür.

2. Anayasa'ya Aykırılık Sorunu

174. 2942 sayılı Kanun'un 4. maddesinin ikinci fıkrasının dava konusu ibarenin de bulunduğu birinci cümlesinde, maliklerinin mülkiyet hakkının kullanılmasının engellenmemesi, can ve mal güvenliği bakımından gerekli önlemlerin alınması kaydıyla, kamu yararına dayalı olarak taşınmazların üstünde teleferik ve benzeri ulaşım hatları ile her türlü köprü, taşınmazların altında metro ve benzeri raylı taşıma sistemleri ile tünel yapılabileceği hüküm altına alınmaktadır. Dava konusu kural, cümlede yer alan "ile tünel" ibaresidir.

175. Mülkiyet hakkı, kişiye başkasının hakkına zarar vermemek ve kanunların koyduğu sınırlamalara uymak koşuluyla, sahibi olduğu şeyi dilediği gibi kullanma, ürünlerinden yararlanma ve tasarruf olanağı veren temel bir haktır. Anayasa'nın 35. maddesinde, "Herkes, mülkiyet ve miras haklarına sahiptir. Bu haklar, ancak kamu yararı amacıyla, kanunla sınırlanabilir. Mülkiyet hakkının kullanılması toplum yararına aykırı olamaz." denilmek suretiyle güvenceye bağlanan mülkiyet hakkı, bireye emeğinin karşılığına sahip olma ve geleceğe yönelik planlar yapma olanağı tanıyan temel bir hak olup maddi varlığı bulunan taşınır ve taşınmaz malvarlığını kapsadığı gibi maddi bir varlığı bulunmayan hak ve alacakları da içermektedir.

176. Anayasa'nın 35. maddesinde mülkiyet hakkı sınırsız bir hak olarak düzenlenmemiş, kamu yararı amacıyla ve kanunla sınırlandırılabilmesi öngörülmüştür. Ancak bu amaçla yapılan müdahalenin Anayasa'nın 13. maddesinde düzenlenen ilkelere uygun olması gerekmektedir. Buna göre mülkiyet hakkına yönelik sınırlamalar, demokratik toplum gereklerine ve ölçülülük ilkesine aykırı olamaz. Ölçülülük ilkesi, amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder.

177. 2942 sayılı Kanun'un "İrtifak hakkı kurulması" başlıklı 4. maddesinin birinci fıkrasında, taşınmaz malın mülkiyetinin kamulaştırılması yerine, amaç için yeterli olduğu takdirde taşınmaz malın belirli kesimi, yüksekliği, derinliği veya kaynak üzerinde kamulaştırma yoluyla irtifak hakkı kurulabileceği hüküm altına alınmıştır. Maddenin ikinci fıkrasının dava konusu kuralın da yer aldığı birinci cümlesinde, maliklerinin mülkiyet hakkının kullanılmasının engellenmemesi, can ve mal güvenliği bakımından gerekli önlemlerin alınması kaydıyla, kamu yararına dayalı olarak taşınmazların altında tünel yapılabilmesi belirtilmiştir.

178. Kamu hizmetinin gereği gibi yürütülmesi bakımından tünel gibi yatırımların yapılmasında kamu yararı bulunduğu hususunda tereddüt bulunmamaktadır. Dolayısıyla, bu tür yatırımların yapılması amacıyla mülkiyet hakkına yapılan müdahale meşru bir amaca dayanmaktadır. Öte yandan, taşınmazın değerini azaltan her türlü müdahalede kamu yararı ile bireysel yarar arasındaki denge, kural olarak malikin ekonomik kayıpları telafi edilmek suretiyle sağlanabilir. Bu bağlamda, taşınmazın altında tünel yapılması suretiyle mülkiyet hakkına yapılan müdahalenin ölçülülüğünden söz edilebilmesi için malike ekonomik kayıpları karşılığında uygun bir tazminatın ödenmesi gerekmektedir. Aksi takdirde malikin katlanmak zorunda olduğu külfet yönünden bir dengesizlik doğacak ve bu durum mülkiyet hakkına müdahaleyi ölçsüz kılacaktır.

179. Dava dilekçesinde de taşınmazın altında tünel yapılmasında kamu yararı bulunduğu kabul edilmekle birlikte, Kanun'un 4. maddesinin ikinci fıkrasının üçüncü cümlesi uyarınca, taşınmaz sahiplerine bu işlem nedeniyle kamulaştırma, tazminat ve benzeri nam altında herhangi bir ücret ödenmeyecek olmasının mülkiyet hakkına ölçsüz bir müdahale oluşturduğu ileri sürülmüştür. Ancak, taşınmazın değer kaybı için taşınmaz sahiplerine kamulaştırma, tazminat ve benzeri nam altında herhangi bir ücret ödenmeyeceğini öngören kural Anayasa Mahkemesinin 14.5.2015 tarihli ve E.2014/177, K.2015/49 sayılı kararıyla iptal edilmiştir. Dolayısıyla, taşınmazın altında tünel yapılması suretiyle taşınmazda oluşacak değer kaybı için taşınmaz sahiplerine tazminat ödenmesine herhangi bir engel bulunmamaktadır.

180. Bu itibarla, maliklerinin mülkiyet hakkının kullanılmasının engellenmemesi, can ve mal güvenliği bakımından gerekli önlemlerin alınması kaydıyla, kamu yararına dayalı olarak taşınmazların altında tünel yapılabilmesini öngören kuralın mülkiyet hakkına ölçsüz bir müdahale niteliği taşıdığı söylenemez.

181. Açıklanan nedenlerle kural, Anayasa'nın 13. ve 35. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

182. Osman Alifeyyaz PAKSÜT bu görüşe katılmamıştır.

183. Kuralın, Anayasa'nın 2., 36. ve 90. maddeleriyle ilgisi görülmemiştir.

H- Kanun'un 29. Maddesiyle 5651 Sayılı Kanun'a Eklenen 8/A Maddesinin (1) ve (2) Numaralı Fıkralarının İncelenmesi

184. Dava konusu kurallar, 15.8.2016 tarihli ve 671 sayılı Olağanüstü Hal Kapsamında Bazı Kurum ve Kuruluşlara İlişkin Düzenleme Yapılması Hakkında Kanun Hükmünde Kararname'nin 21. maddesiyle değiştirilmiştir.

185. Bu nedenle, konusu kalmayan fıkralara ilişkin iptal talepleri hakkında karar verilmesine yer olmadığına karar verilmesi gerekir.

I- Kanun'un 32. Maddesiyle 5809 Sayılı Kanun'un Yeniden Düzenlenen 51. Maddesinin; (2) Numaralı Fıkrasında Yer Alan "...ilgili mevzuatın ve...", (6) Numaralı Fıkrasında Yer Alan "...ilgili mevzuat hükümleri saklı kalmak kaydıyla,..." ve (8) Numaralı Fıkrasının İkinci Cümlesinde Yer Alan "...İlgili mevzuatın ve..." İbareleri İle (13) Numaralı Fıkrasının İncelenmesi

1. Genel Açıklama

186. 5809 sayılı Kanun'un 51. maddesinde, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esaslar düzenlenmektedir. Maddenin ilk hâlinde yer alan, kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirleme yetkisinin Bilgi Teknolojileri ve İletişim Kurulu'na (BTK) ait olduğu yolundaki hükmün, Anayasa'nın 20. maddesine aykırı bulunarak Anayasa Mahkemesinin 9.4.2014 tarihli ve E.2013/122, K.2014/74 sayılı kararıyla iptal edilmesi üzerine haberleşmeyle ilgili kişisel verilerin işlenmesi ve korunmasına ilişkin usul ve esaslar 6639 sayılı Kanun'la yeniden düzenlenmiştir.

187. Maddenin (1) numaralı fıkrasında, kişisel verilerin işlenmesinde uyulması gereken ilkeler sayılmış; (2) numaralı fıkrasında ilgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesinin yasak olduğu belirtilmiş; (6) numaralı fıkrasında, kişisel verilerin yurt dışına aktarılmasına ilişkin ilgili mevzuat hükümleri saklı kalmak kaydıyla, trafik ve konum verilerinin ancak ilgili kişilerin açık rızaları alınmak koşuluyla yurt dışına aktarılabilmesi öngörülmüş; (8) numaralı fıkrasında, ilgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde ancak acil yardım çağrıları ile 29/5/2009 tarihli ve 5902 sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanunda tanımlanan afet ve acil durum hâllerinde abonelerin/kullanıcıların açık rızası aranmaksızın konum verileri ve ilgili kişilerin kimlik bilgilerinin işletmeci tarafından yetkilendirilen kişilerle sınırlı olmak kaydıyla işlenebilmesine

olanak tanınmış; (13) numaralı fıkrasında ise maddenin uygulanmasına ilişkin usul ve esasların BTK tarafından belirleneceği hüküm altına alınmıştır.

2- (2) Numaralı Fıkroda Yer Alan "...ilgili mevzuatın ve..." İbaresinin İncelenmesi

a. İptal Talebinin Gerekçesi

188. Dava dilekçesinde özetle, Anayasa'nın 20. maddesine göre, kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği, dava konusu "ilgili mevzuat" ibaresinin ise belirsiz olduğu, konuya ilişkin olarak yürürlükte bulunan mevzuatın karmaşıklığı dikkate alındığında, dava konusu kuralla elektronik haberleşmenin ve ilgili trafik verisinin, haberleşmeye taraf olanların rızası olmadan dinlenmesine, kaydedilmesine, saklanmasına olanak tanındığı, bu durumun ise özel hayatın gizliliğine orantısız ve keyfi şekilde müdahalede bulunulmasına sebebiyet verdiği belirtilerek kuralın, Anayasa'nın 2., 13. ve 20. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

189. 5809 sayılı Kanun'un 51. maddesinin (2) numaralı fıkrasında, elektronik haberleşmenin ve ilgili trafik verisinin gizliliğinin esas olup ilgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesinin yasak olduğu hüküm altına alınmıştır. Dava konusu kural, fıkroda geçen "...ilgili mevzuatın ve..." ibaresidir.

190. Anayasa'nın 2. maddesinde düzenlenen hukuk devletinin temel ilkelerinden biri de "belirlilik"tir. Belirlilik ilkesi ise yalnızca yasal belirliliği değil, daha geniş anlamda hukuki belirliliği ifade etmektedir. Yasal düzenlemeye dayanarak erişilebilir, bilinebilir ve öngörülebilir gibi niteliksel gereklilikleri karşılaması koşuluyla, mahkeme içtihatları ve yürütmenin düzenleyici işlemleri ile de hukuki belirlilik sağlanabilir. Hukuki belirlilik ilkesinde asıl olan, bir hukuk normunun uygulanmasıyla ortaya çıkacak sonuçların o hukuk düzeninde öngörülebilir olmasıdır.

191. Anayasa'nın 20. maddesinin üçüncü fıkrasında, herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu; bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı belirtildikten sonra kişisel verilerin, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği, kişisel verilerin korunmasına ilişkin esas ve usullerin de kanunla düzenleneceği hüküm altına alınmıştır. Böylece kişisel verilerin korunması hakkı anayasal güvenceye bağlanmıştır.

192. Kişisel verilerin korunması hakkı, insan onurunun korunması ve kişiliğin serbestçe geliştirilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Anayasa'nın 20. maddesinin üçüncü fıkrası uyarınca kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Türkiye'nin taraf olduğu 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Avrupa Konseyi Sözleşmesi'nin 9. maddesinde de devlet güvenliği, kamu güvenliği, devletin ekonomik menfaatlerinin korunması ve suçlarla mücadele edilmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması ile verilerin istatistiki veya bilimsel amaçlarla kullanılması durumlarında kişisel verilerin korunmasına sınırlamalar getirilebileceği öngörülmüştür. Ancak bu sınırlamalar, Anayasa'nın 13. maddesinde yer alan güvencelere aykırı olamaz. Anayasa'nın 13. maddesine göre temel hak ve özgürlüklere yönelik sınırlamalar, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacağı gibi hak ve özgürlüklerin özlerine de dokunamaz.

193. Kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvencenin yaşama geçirilebilmesi için, bu hakkı ilgilendiren yasal düzenlemelerin, açık, anlaşılabilir ve kişilerin sözü konusu haklarını kullanabilmelerine elverişli olması gerekir. Ancak böyle bir düzenleme ile kişilerin özel hayatlarını ilgilendiren veri ve bilgilerin resmi makamların keyfi müdahalelerine karşı korunması olanaklı hâle getirilebilir.

194. Kanun'un 51. maddesinin (2) numaralı fıkrasında, elektronik haberleşmenin ve ilgili trafik verisinin gizliliğinin esas olduğu ifade edildikten sonra, dava konusu kuralla "ilgili mevzuatın" öngördüğü durumlar istisna tutularak, haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi yasaklanmıştır. Böylece, kişisel verilerin işlenmesi kural olarak yasaklanmış olmakla beraber ilgili mevzuatın öngördüğü durumlarda haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi mümkün kılınmıştır.

195. Anayasa'nın 20. maddesinin üçüncü fıkrasında, kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin rızasıyla işlenebilmesine olanak tanınmış, Anayasa Mahkemesinin yukarıda anılan 9.4.2014 tarihli ve E.2013/122, K.2014/74 sayılı kararında da bu husus teyit edilerek kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceği ifade edilmiştir. Anayasa'nın 20. maddesinin açık hükmü ve Anayasa Mahkemesinin anılan kararı gözetildiğinde, kanunla bir belirleme ve sınırlama yapılmaksızın yürütmenin düzenleyici işlemleriyle haberleşmeye ilişkin kişisel verilerin işlenmesine anayasal açıdan olanak bulunmamaktadır. Bu bağlamda,

elektronik haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesine olanak tanıyan kuralda yer alan “ilgili mevzuat” ibaresiyle de kişisel verilerin işlenmesiyle ilgili düzenlemeler öngören diğer kanun hükümlerinin kastedildiği anlaşılmaktadır. Nitekim, kuralın gerekçesinde de Anayasa’nın 20. maddesi uyarınca kişisel verilerin işlenmesi konusunun kanunla düzenlenmesi gerektiğinden elektronik haberleşme sektöründe kişisel verilerin işlenmesi ve gizliliğine yönelik hususlara ilişkin olarak yeni bir kanun tasarısı hazırlandığı ifade edilmiştir. Ayrıca kişisel verilerin korunması konusunda çerçeve kanun niteliği taşıyan 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun 4. maddesinin (1) numaralı fıkrasında da, kişisel verilerin ancak kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği hüküm altına alınmıştır.

196. Dolayısıyla, kuralda yer alan “ilgili mevzuat” kavramı, elektronik haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesiyle ilgili yasal düzenlemeleri ifade ettiğinden, dava konusu kuralda, kişisel verilerin korunmasına ilişkin usul ve esasların kanunla düzenlenmesini öngören Anayasa’nın 20. maddesine aykırı bir yön bulunmamaktadır.

197. Günümüzde, milli güvenlik, istihbarat, suçla mücadele gibi çok farklı nedenlerle kişisel verilerin işlenmesine ihtiyaç duyulabilmektedir. Ayrıca zaman içerisinde gelişen teknolojiyle birlikte bu konuda yeni kanuni düzenlemeler yapılması da gerekebilir. Bu nedenle, haberleşmeye ilişkin kişisel verilerin hangi durumlarda işlenebileceğinin kanunla tek tek sayılmak suretiyle belirlenmesi mümkün değildir. Dava konusu kuralda da genel bir belirleme yapılarak haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesinin yasak olduğu hüküm altına alındıktan sonra, elektronik haberleşmeye ilişkin kişisel verilerin işlenmesine olanak tanıyan ilgili kanun hükümleri saklı tutulmuştur.

198. Diğer taraftan, dava konusu kuralla, konuyla ilgili kanunlarda haberleşmeye ilişkin kişisel verilerin işlenmesine olanak tanınmakla birlikte bu konuda kanun koyucunun sınırsız bir takdir yetkisi bulunmamaktadır. Nitekim, 5809 sayılı Kanun’un 51. maddesinin (1) numaralı fıkrasında, kişisel verilerin işlenmesinde; hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işleme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uyulması gerektiği belirtilmiş, Kişisel Verilerin Korunması Kanunu’nun 4. maddesinde de, benzer ilkelere yer verilerek kişisel verilerin işlenmesinde gözetilmesi gereken hususlar ayrıntılı bir şekilde düzenlenmiştir. Dolayısıyla, dava konusu kuralın kişisel verilerin işlenmesi noktasında kanun koyucuya sınırsız bir takdir hakkı verdiği söylenemez.

199. Bu itibarla, ilgili kanunların öngördüğü durumlarda, haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesine olanak tanıyan kuralda belirsizlik bulunmadığı gibi, kişisel verilerin korunmasını isteme hakkının özüne dokunan ya da bu hakkı ölçsüz şekilde sınırlandıran bir husus bulunmamaktadır.

200. Açıklanan nedenlerle kural, Anayasa'nın 2., 13. ve 20. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

3- (6) Numaralı Fıkroda Yer Alan "...ilgili mevzuat hükümleri saklı kalmak kaydıyla,..." İbaresini ile (8) Numaralı Fıkrasının İkinci Cümlesinde Yer Alan "...İlgili mevzuatın ve..." İbaresinin İncelenmesi

a. İptal Taleplerinin Gerekçesi

201. Dava dilekçesinde özetle, 5809 sayılı Kanun'un 51. maddesinin (2) numaralı fıkrasında yer alan "...ilgili mevzuatın ve..." ibaresine ilişkin gerekçelerle kuralların, Anayasa'nın 2., 13. ve 20. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

202. 5809 sayılı Kanun'un 51. maddesinin (6) numaralı fıkrasında, kişisel verilerin yurt dışına aktarılmasına ilişkin ilgili mevzuat hükümleri saklı kalmak kaydıyla, trafik ve konum verilerinin ancak ilgili kişilerin açık rızaları alınmak koşuluyla yurt dışına aktarılacağı belirtilmiş, (8) numaralı fıkrasının ikinci cümlesinde de, ilgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde ancak acil yardım çağruları ile 29.5.2009 tarihli ve 5902 sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanunda tanımlanan afet ve acil durum hâllerinde abonelerin/kullanıcıların açık rızası aranmaksızın konum verileri ve ilgili kişilerin kimlik bilgilerinin işletmeciler tarafından yetkilendirilen kişilerle sınırlı olmak kaydıyla işlenebileceği hüküm altına alınmıştır. Dava konusu kurallar, anılan fıkralarda yer alan "...ilgili mevzuat hükümleri saklı kalmak kaydıyla,..." ve "İlgili mevzuatın ve..." ibareleridir.

203. 5809 sayılı Kanun'un 51. maddesinin (2) numaralı fıkrasında yer alan "...ilgili mevzuatın ve..." ibaresine ilişkin bir önceki başlık altında belirtilen gerekçeler bu kurallar yönünden de geçerlidir.

204. Açıklanan nedenlerle kurallar, Anayasa'nın 2., 13. ve 20. maddelerine aykırı değildir. İptal taleplerinin reddi gerekir.

4- (13) Numaralı Fıkranın İncelenmesi

a. İptal Talebinin Gerekçesi

205. Dava dilekçesinde özetle, Anayasa Mahkemesinin 9.4.2014 tarihli ve E.2013/122, K.2014/74 sayılı kararıyla, BTK'ya elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğin korunmasına yönelik usul ve esasları belirleme yetkisi verilmesinin Anayasa'ya aykırı olduğuna karar verilmesine karşın anılan kararın görmezden gelinerek dava konusu kuralla yetkinin yeniden BTK'ya verildiği belirtilerek kuralın, Anayasa'nın 2. ve 153. maddelerine aykırı olduğu ileri sürülmüştür.

b. Anayasa'ya Aykırılık Sorunu

206. 6216 sayılı Kanun'un 43. maddesi uyarınca, dava konusu kural ilgisi nedeniyle Anayasa'nın 7. maddesi yönünden de incelenmiştir.

207. Dava konusu kuralla, elektronik haberleşme sektöründe kişisel verilerin işlenmesi ve gizliliğin korunmasına ilişkin kuralları düzenleyen 51. maddenin uygulanmasına ilişkin usul ve esasların BTK tarafından belirleneceği hüküm altına alınmaktadır.

208. Anayasa'nın 7. maddesinde, "Yasama yetkisi Türk Milleti adına Türkiye Büyük Millet Meclisindedir. Bu yetki devredilemez." denilmektedir. Yasama yetkisinin Türkiye Büyük Millet Meclisine ait olması ve bu yetkinin devredilememesi, kuvvetler ayrılığı ilkesinin bir gereğidir. Bu hükme yer veren Anayasa'nın 7. maddesinin gerekçesinde yasama yetkisinin parlamentoya ait olması "demokrasi rejimini benimseyen siyasi rejimlerde kaçınılmaz bir durum" olarak nitelendirilmiştir.

209. Anayasa'nın 7. maddesi ile yasaklanan husus, kanun yapma yetkisinin devredilmesi olup bu madde, yürütme organına hiçbir şekilde düzenleme yapma yetkisi verilemeyeceği anlamına gelmemektedir. Kanun koyucu, yasama yetkisinin genelliği ilkesi uyarınca, bir konuyu doğrudan kanunla düzenleyebileceği gibi bu hususta düzenleme yapma yetkisini yürütme organına da bırakabilir.

210. Yürütmenin türevselliği ilkesi gereğince, yürütme organının bir konuda düzenleme yapabilmesi için yasama organınca yetkilendirilmesi zorunludur. Kural olarak, Anayasa'da münhasıran kanunla düzenlenmesi öngörülen konularda, kanunun temel esasları, ilkeleri ve çerçeveyi belirlemiş olması gerekmektedir. Anayasa koyucunun açıkça kanunla düzenlenmesini öngördüğü konularda, yasama organının temel kuralları saptadıktan sonra, uzmanlık ve idare tekniğine ilişkin hususları yürütmeye bırakması, yasama yetkisinin devri olarak yorumlanamaz.

211. Anayasa'nın 20. maddesinin üçüncü fıkrasının son cümlesinde, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilerek kişisel verilerin korunması hakkı anayasal güvenceye bağlanmış ve bu şekilde kamu makamlarının keyfi müdahalelerine karşı koruma altına

alınmıştır. Buna göre, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve korunmasına yönelik temel kuralların kanunla düzenlenmesi zorunludur. Nitekim Anayasa Mahkemesi de yukarıda tarih ve sayısı belirtilen kararında, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasların belirlenmesi konusunda BTK'ya doğrudan ve ilk elden düzenleyici işlem yapma yetkisi verilmesinin Anayasa'nın 20. maddesine aykırı olduğuna karar vermiştir.

212. Bu bağlamda, Kanun'un yeniden düzenlenen 51. maddesinde, elektronik haberleşme sektöründe, kişisel verilerin işlenmesinde uyulması gereken ilkeler sayıldıktan sonra, kişisel verilerin işlenmesi ve gizliliğinin korunmasına ilişkin kurallar herhangi bir duraksamaya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir şekilde düzenlenerek konuya ilişkin temel kurallar belirlenmiştir. Maddede belirlenen usul ve esaslar çerçevesinde kişisel verilerin işlenmesi ve korunmasına ilişkin teknik ve uygulamayı esas alan detayların belirlenmesi konusunda BTK'ya yetki verilmesini öngören kuralda belirsizlik bulunmadığı gibi yasama yetkisinin devri de söz konusu değildir.

213. Açıklanan nedenlerle kural, Anayasa'nın 2. ve 7.maddelerine aykırı değildir. İptal talebinin reddi gerekir.

214. Kuralın Anayasa'nın 153. maddesiyle ilgisi görülmemiştir.

IV- YÜRÜRLÜĞÜN DURDURULMASI TALEBİ

215. Dava dilekçesinde özetle, Türkiye Yeşilay Vakfına aktarılacak kamu kaynağının amacına uygun kullanılıp kullanılmadığının denetim dışı bırakılmasının kamu yararıyla bağdaşmadığı, Sağlık Bakanlığı bütçesinden Türkiye Yeşilay Vakfına aktarılacak ödeneğe ilişkin düzenlemenin bütçe kanununda yer alması gerektiği, Sağlık Bilimleri Üniversitesinde çoğunluğu merkezi idare tarafından belirlenen üyelerden oluşan Mütevelli Heyeti adı altında bir yönetim organı öngörülmesinin, Üniversitenin bilimsel özerkliğini ortadan kaldırdığı, Sağlık Bilimleri Üniversitesine diğer Devlet üniversitelerine nazaran özel bir statü verilmesinin Anayasa'nın 132. maddesiyle bağdaşmadığı, Türkiye Kamu Hastaneleri Kurumuna bağlı eğitim ve araştırma hastanelerinin tamamının, Sağlık Bakanlığının kontrolünde olan Sağlık Bilimleri Üniversitesinin uygulama ve araştırma merkezi haline getirilmesinin üniversite özerkliğini zedelediği, Sağlık Bilimleri Üniversitesine tahsis edilecek kadroları belirleme yetkisinin Sağlık Bakanlığının kontrolündeki Mütevelli Heyetine verilmesinin, tıp eğitimini Sağlık Bakanlığına devretmek anlamına geldiği, halen Marmara Üniversitesine tahsisli olan Haydarpaşa Kampüsünün, tahsis amacı ortadan kalkmadan veya tahsis amacı dışında kullanıldığı tespit edilmeden Sağlık Bilimleri Üniversitesine tahsis edilmesinin kamu yararıyla bağdaşmadığı, EPDK'ya kayıp-kaçak elektrik oranlarının belirlenmesi konusunda verilen yetkinin muğlak olduğu,

elektrik dağıtım piyasasının özelleştirilmesi esnasında ihaleyi kazanan şirketlerin kayıp-kaçak oranlarını azaltmak için verdiği hedefleri yakalayamaması nedeniyle oluşan zararın tüketicilere yansıtılmasına yasal zemin oluşturulduğu, bu durumun aynı zamanda özelleştirme şartnamesine de müdahale anlamına geldiği, faturalarını düzenli şekilde ödeyen elektrik abonelerine kayıp-kaçak bedeli altında ek mali yükümlülükler getirilmesinin anayasal bir dayanağının bulunmadığı, Gençlik ve Spor Bakanlığı ile Spor Genel Müdürlüğü'nün teşkilat yapısında herhangi bir değişiklik olmadığı halde adı geçen kurumlarda genel müdür yardımcılarında şube müdürlerine kadar görev yapanların görevlerine son verilerek daha alt bir göreve atanmalarının hukuki güvenlik ilkesini ihlal ettiği, tabi oldukları personel kanununa bakılmaksızın Başbakanlık, bakanlıklar, bağlı ve ilgili kuruluşlar ile başkan ve üyeleri hariç olmak üzere düzenleyici ve denetleyici kurumlar ve Tasarruf Mevduatı Sigorta Fonunda, yönetici kadro veya pozisyonunda çalışan kamu görevlilerinin, görevden alınmaları veya görev süresinin sona ermesi durumunda, ek göstergelerine göre buldukları görevden düşük statülü kadrolara atanmalarına olanak tanınmasının kazanılmış hak ilkesini ihlal ettiği, daha önce kariyer meslek sınıfında görev yapmayan yönetici pozisyonundaki kamu görevlilerinin, görevden alındıktan sonra kariyer meslek sınıfına atanmalarına olanak tanınmasının hukuk devleti ilkesiyle bağdaşmadığı, büyükşehir olmayan illerde görev yapan il özel idaresi genel sekreterlerinin, genel idare hizmetlerine dahil bakanlık müstakil daire başkanları; genel sekreter yardımcılarının ise bakanlık daire başkanları ile eşdeğer görevde olmasına rağmen aynı mali haklardan yararlandırılmamasının hukuk devleti ve ücrette adaletin sağlanması ilkelerine aykırı olduğu, il nüfus ve vatandaşlık müdürlerinin bakanlık il müdürlüğü statüsünde olmasına rağmen bakanlık il müdürlerine sağlanan mali haklardan faydalandırılmamalarının kazanılmış hak ilkesini ihlal ettiği, özel mülkiyete konu taşınmazın altında tünel yapılması karşılığında taşınmaz malikine herhangi bir ücret ödenmemesinin mülkiyet hakkıyla bağdaşmadığı, gecikmesinde sakınca bulunan hallerde internet ortamında yer alan yayımla ilgili olarak içeriğin çıkarılması ve/veya erişimin engellenmesinde TİB'e sınırları belirsiz bir yetki verilmesinin, haberleşme, ifade ve basın hürriyetine keyfi olarak müdahale edilmesine sebebiyet verdiği, TİB tarafından verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararlarına karşı sulh ceza hakimine sadece onaylama yetkisi verilmesinin adil yargılanma hakkına aykırı olduğu, ilgili mevzuat uyarınca haberleşmeye ilişkin kişisel verilerin işlenmesine olanak tanınmasının özel hayatın gizliliğine orantısız ve keyfi şekilde müdahalede bulunulmasına sebebiyet verdiği, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğin korunmasına yönelik usul ve esasları belirleme konusunda BTK'nın yetkili kılınarak Anayasa Mahkemesinin konuyla ilgili daha önce verdiği kararın etkisiz hale getirildiği, bu

çerçeve de dava konusu kuralların bu haliyle uygulanmasının telafisi güç veya imkânsız zararların doğmasına sebebiyet vereceği belirtilerek kuralların yürürlüklerinin durdurulması talep edilmiştir.

27.3.2015 tarihli ve 6639 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun'un;

A- 22. maddesiyle, 3.6.2011 tarihli ve 638 sayılı Gençlik ve Spor Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'ye eklenen geçici 13. maddenin (1) numaralı fıkrasının birinci cümlesinde yer alan "...Bakanlık Merkez Teşkilatı ile Spor Genel Müdürlüğü ve..." ibaresine yönelik yürürlüğün durdurulması talebinin, koşulları oluşmadığından REDDİNE,

B- 5. maddesiyle, 28.3.1983 tarihli ve 2809 sayılı Yükseköğretim Kurumları Teşkilatı Kanunu'na eklenen ek 158. maddenin; ikinci fıkrasının ikinci ve üçüncü cümlelerine yönelik iptal hükümlerinin yürürlüğe girmelerinin ertelenmeleri nedeniyle bu cümlelere ilişkin yürürlüğün durdurulması taleplerinin, REDDİNE,

C- 4. maddesiyle değiştirilen, 24.5.2013 tarihli ve 6487 sayılı Bazı Kanunlar ile 375 Sayılı Kanun Hükmünde Kararnamede Değişiklik Yapılması Hakkında Kanun'un 33. maddesinin (4) numaralı fıkrasının;

1- Birinci cümlesinde yer alan "...10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununun 29 uncu maddesi hükmüne tabi olmaksızın..." ibaresine,

2- İkinci cümlesinin "...takip eden yıllarda ise her takvim yılı başından geçerli olmak üzere o yıl için 4/1/1961 tarihli ve 213 sayılı Vergi Usul Kanununun mükerrer 298 inci maddesi hükümleri uyarınca tespit ve ilan edilen yeniden değerlendirme oranında artırılarak..." bölümüne,

D- 5. maddesiyle, 28.3.1983 tarihli ve 2809 sayılı Yükseköğretim Kurumları Teşkilatı Kanunu'na eklenen ek 158. maddenin;

1- İkinci fıkrasının;

a- Birinci cümlesinde yer alan "...ile Mütevelli Heyetinden" ibaresine,

b- Dördüncü ve beşinci cümlelerine,

c- Altıncı cümlesinde yer alan "Mütevelli Heyetinin" ibarelerine,

2- Üçüncü fıkrasına,

3- Dördüncü fıkrasının üçüncü cümlesinde yer alan "Mütevelli Heyetinin teklifi ve..." ibaresine,

4- Beşinci ve altıncı fıkralarına,

E- 18. maddesiyle, 14.3.2013 tarihli ve 6446 sayılı Elektrik Piyasası Kanunu'na eklenen geçici 18. maddesine,

F- 23. maddesiyle, 27.6.1989 tarihli ve 375 sayılı KHK'ya eklenen ek 18. maddenin birinci, ikinci ve üçüncü fıkralarına,

G- 24. maddesiyle, 375 sayılı Kanun Hükmünde Kararname'nin eki (I) sayılı Cetvelin "A- Aylıklarını 657 sayılı Devlet Memurları Kanununa Göre Alanlar" kısmının "1- Kadroları Genel İdare Hizmetleri Sınıfında yer alan personel ile Teknik Hizmetler, Sağlık ve Yardımcı Sağlık Hizmetleri ile Avukatlık Hizmetleri sınıflarında bulunan personelden ek ödeme oranları ilgili gruplarında düzenlenmeyen ve kadro unvanları bu bölümde yer alan personel"bölümünün;

1- (d) sırasında yer alan "büyükşehir belediyesi bulunan illerin il özel idaresi genel sekreter yardımcısı, diğer illerin il özel idaresi genel sekreteri," ibaresinin "il özel idaresi genel sekreteri," şeklinde değiştirilmesine,

2- (e) sırasında yer alan "büyükşehir belediyesi bulunan illerin il özel idaresi I. hukuk müşaviri, büyükşehir belediyesi bulunmayan illerin il özel idaresi genel sekreter yardımcısı," ibaresinin "il özel idaresi genel sekreter yardımcısı," şeklinde değiştirilmesine,

3- (g) sırasına "il yazı işleri müdürü" ibaresinden önce gelmek üzere eklenen "İl nüfus ve vatandaşlık müdürü,"ibaresine,

H- 28. maddesiyle 4.11.1983 tarihli ve 2942 sayılı Kamulaştırma Kanunu'nun 4. maddesinin ikinci fıkrasının birinci cümlesine "raylı taşıma sistemleri" ibaresinden sonra gelmek üzere eklenen "ile tünel" ibaresine,

I- 32. maddesiyle, 5.11.2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'nun yeniden düzenlenen 51. maddesinin;

1- (2) numaralı fıkrasında yer alan "...ilgili mevzuatın ve..." ibaresine,

2- (6) numaralı fıkrasında yer alan "...ilgili mevzuat hükümleri saklı kalmak kaydıyla,..." ibaresine,

3- (8) numaralı fıkrasının ikinci cümlesinde yer alan "...İlgili mevzuatın ve..." ibaresine,

4- (13) numaralı fıkrasına,

yönelik iptal talepleri 2.11.2016 tarihli ve E.2015/61, K.2016/172 sayılı kararla reddedildiğinden, bu fıkra, cümle, bölüm, ibare ve değişikliklere ilişkin yürürlüğün durdurulması taleplerinin REDDİNE,

J- 29. maddesiyle, 4.5.2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'a eklenen 8/A maddesinin (1) ve (2) numaralı fıkraları hakkında, 2.11.2016 tarihli ve E.2015/61, K.2016/172 sayılı kararla karar verilmesine yer olmadığına karar verildiğinden, bu fıkralara ilişkin yürürlüğün durdurulması talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA,

2.11.2016 tarihinde OYBİRLİĞİYLE karar verilmiştir.

V- İPTAL KARARININ YÜRÜRLÜĞE GİRECEĞİ GÜN SORUNU

216. Anayasa'nın 153. maddesinin üçüncü fıkrasında, "Kanun, kanun hükmünde kararname veya Türkiye Büyük Millet Meclisi İçtüzüğü ya da bunların hükümleri, iptal kararlarının Resmi Gazetede yayımlandığı tarihte yürürlükten kalkar. Gereken hallerde Anayasa Mahkemesi iptal hükmünün yürürlüğe gireceği tarihi ayrıca kararlaştırabilir. Bu tarih, kararın Resmi Gazetede yayımlandığı günden başlayarak bir yılı geçemez." denilmekte, 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrasında da bu kural tekrarlanarak, Mahkemenin gerekli gördüğü hâllerde, Resmî Gazete'de yayımlandığı günden başlayarak iptal kararının yürürlüğe gireceği tarihi bir yılı geçmemek üzere ayrıca kararlaştırabileceği belirtilmektedir.

217. 6639 sayılı Kanun'un 5. maddesiyle 2809 sayılı Kanun'a eklenen ek 158. maddenin; ikinci fıkrasının ikinci ve üçüncü cümlelerinin iptal edilmesi nedeniyle doğacak hukuksal boşluk kamu yararını ihlal edici nitelikte görüldüğünden, Anayasa'nın 153. maddesinin üçüncü fıkrasıyla 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince bu cümlelere ilişkin iptal hükümlerinin, kararın Resmî Gazete'de yayımlanmasından başlayarak altı ay sonra yürürlüğe girmesi uygun görülmüştür.

VI- HÜKÜM

27.3.2015 tarihli ve 6639 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun'un;

A- 4. maddesiyle değiştirilen, 24.5.2013 tarihli ve 6487 sayılı Bazı Kanunlar ile 375 Sayılı Kanun Hükmünde Kararnamede Değişiklik Yapılması Hakkında Kanun'un 33. maddesinin (4) numaralı fıkrasının;

1-Birinci cümlesinde yer alan "...10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununun 29 uncu maddesi hükmüne tabi olmaksızın..." ibaresinin,

2- İkinci cümlesinin "...takip eden yıllarda ise her takvim yılı başından geçerli olmak üzere o yıl için 4/1/1961 tarihli ve 213 sayılı Vergi Usul Kanununun mükerrer 298 inci maddesi hükümleri uyarınca tespit ve ilan edilen yeniden değerlendirme oranında artırılarak..."bölümünün,

Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

B- 5. maddesiyle 28.3.1983 tarihli ve 2809 sayılı Yükseköğretim Kurumları Teşkilatı Kanunu'na eklenen ek 158. maddenin;

1- İkinci fıkrasının;

a- Birinci cümlesinde yer alan "...ile Mütevelli Heyetinden" ibaresinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, OYBİRLİĞİYLE,

b- İkinci cümlesinin Anayasa'ya aykırı olduğuna ve İPTALİNE, iptal hükmünün, Anayasa'nın 153. maddesinin üçüncü fıkrası ile 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince, KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAŞLAYARAK ALTI AY SONRA YÜRÜRLÜĞE GİRMESİNE, OYBİRLİĞİYLE,

c- Üçüncü cümlesinin 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrası gereğince İPTALİNE, Hicabi DURSUN, Muammer TOPAL, Recai AKYEL ile Yusuf Şevki HAKYEMEZ'in karşıoyları ve OYÇOKLUĞUYLA, iptal hükmünün, Anayasa'nın 153. maddesinin üçüncü fıkrası ile 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince, KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAŞLAYARAK ALTI AY SONRA YÜRÜRLÜĞE GİRMESİNE, OYBİRLİĞİYLE,

d- Dördüncü ve beşinci cümlelerinin Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

e- Altıncı cümlesinde yer alan "Mütevelli Heyetinin" ibarelerinin Anayasa'ya aykırı olmadığına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

2- Üçüncü fıkrasının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, OYBİRLİĞİYLE,

3- Dördüncü fıkrasının üçüncü cümlesinde yer alan "Mütevelli Heyetinin teklifi ve..." ibaresinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, OYBİRLİĞİYLE,

4- Beşinci fıkrasının;

a- Birinci ve ikinci cümlelerinin Anayasa'ya aykırı olmadığına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

b- Üçüncü cümlesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, M. Emin KUZ'un karşılığı ve OYÇOKLUĞUYLA,

c- Dördüncü cümlesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, OYBİRLİĞİYLE,

5- Altıncı fıkrasının Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, OYBİRLİĞİYLE,

C- 18. maddesiyle 14.3.2013 tarihli ve 6446 sayılı Elektrik Piyasası Kanunu'na eklenen geçici 18. maddenin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, OYBİRLİĞİYLE,

D- 22. maddesiyle 3.6.2011 tarihli ve 638 sayılı Gençlik ve Spor Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'ye eklenen geçici 13. maddenin (1) numaralı fıkrasının birinci cümlesinde yer alan "...Bakanlık Merkez Teşkilatı ile Spor Genel Müdürlüğü ve..." ibaresinin Anayasa'ya aykırı olduğuna ve İPTALİNE, Osman Alifeyyaz PAKSÜT, Hicabi DURSUN, Kadir ÖZKAYA, Rıdvan GÜLEÇ ile Recai AKYEL'in karşılıkları ve OYÇOKLUĞUYLA,

E- 23. maddesiyle 27.6.1989 tarihli ve 375 sayılı Kanun Hükmünde Kararname'ye eklenen ek 18. maddenin birinci, ikinci ve üçüncü fıkralarının Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

F- 24. maddesiyle 375 sayılı Kanun Hükmünde Kararname'nin eki (I) sayılı Cetvelin "A- Aylıklarını 657 sayılı Devlet Memurları Kanununa Göre Alanlar" kısmının "1- Kadroları Genel İdare Hizmetleri Sınıfında yer alan personel ile Teknik Hizmetler, Sağlık ve Yardımcı Sağlık Hizmetleri ile Avukatlık Hizmetleri sınıflarında bulunan personelden ek ödeme oranları ilgili gruplarında düzenlenmeyen ve kadro unvanları bu bölümde yer alan personel"bölümünün;

1- (d) sırasında yer alan "büyükşehir belediyesi bulunan illerin il özel idaresi genel sekreter yardımcısı, diğer illerin il özel idaresi genel sekreteri," ibaresinin "il özel idaresi genel sekreteri," şeklinde değiştirilmesinin,

2- (e) sırasında yer alan "büyükşehir belediyesi bulunan illerin il özel idaresi I. hukuk müşaviri, büyükşehir belediyesi bulunmayan illerin il özel idaresi genel sekreter yardımcısı," ibaresinin "il özel idaresi genel sekreter yardımcısı," şeklinde değiştirilmesinin,

3- (g) sırasına "il yazı işleri müdürü" ibaresinden önce gelmek üzere eklenen "İl nüfus ve vatandaşlık müdürü," ibaresinin,

Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

G- 28. maddesiyle 4.11.1983 tarihli ve 2942 sayılı Kamulaştırma Kanunu'nun 4. maddesinin ikinci fıkrasının birinci cümlesine "raylı taşıma sistemleri" ibaresinden sonra gelmek üzere eklenen "ile

tünel" ibaresinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Osman Alifeyyaz PAKSÜT'ün karşıoyu ve OYÇOKLUĞUYLA,

H- 29. maddesiyle 4.5.2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'a eklenen 8/A maddesinin (1) ve (2) numaralı fıkraları, 15.8.2016 tarihli ve 671 sayılı Olağanüstü Hal Kapsamında Bazı Kurum ve Kuruluşlara İlişkin Düzenleme Yapılması Hakkında Kanun Hükmünde Kararname'nin 21. maddesiyle değiştirildiğinden, bu fıkralara ilişkin iptal talepleri hakkında KARAR VERİLMESİNE YER OLMADIĞINA, OYBİRLİĞİYLE,

I- 32. maddesiyle 5.11.2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'nun yeniden düzenlenen 51. maddesinin;

1- (2) numaralı fıkrasında yer alan "...ilgili mevzuatın ve..." ibaresinin,

2- (6) numaralı fıkrasında yer alan "...ilgili mevzuat hükümleri saklı kalmak kaydıyla,..." ibaresinin,

3- (8) numaralı fıkrasının ikinci cümlesinde yer alan "...İlgili mevzuatın ve..." ibaresinin,

4- (13) numaralı fıkrasının,

Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

2.11.2016 tarihinde karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili - Burhan ÜSTÜN

Başkanvekili - Engin YILDIRIM

Üye: Serdar ÖZGÜLDÜR; Serruh KALELİ; Osman Alifeyyaz PAKSÜT; Recep KÖMÜRCÜ; Nuri NECİPOĞLU; Hicabi DURSUN; Celal Mümtaz AKINCI; Muammer TOPAL; M. Emin KUZ; Hasan Tahsin GÖKCAN; Kadir ÖZKAYA; Rıdvan GÜLEÇ; Recai AKYEL; Yusuf Şevki HAKYEMEZ

KARŞIOY GEREKÇESİ

27.3.2015 tarihli ve 6639 sayılı Kanun'un 28. maddesiyle, 2942 sayılı Kanun'un 4. maddesinin ikinci fıkrasının birinci cümlesine "...raylı taşıma sistemleri..." ibaresinden sonra gelmek üzere eklenen "...ile tünel..."ibaresi:

1. 27.3.2015 tarihli ve 6639 sayılı Kanun'un 28. maddesiyle, 2942 sayılı Kanun'un 4. maddesinin ikinci fıkrasının birinci cümlesine "...raylı taşıma sistemleri..." ibaresinden sonra gelmek üzere "...ile

tünel...” ibaresi eklenmiştir. Buna göre, maliklerin mülkiyet hakkının kullanılmasının engellenmemesi, can ve mal güvenliği bakımından gerekli önlemlerin alınması kaydıyla, kamu yararına dayalı olarak, taşınmazların altında tünel yapılabilecektir. Maddenin ikinci fıkrasının ikinci cümlesinde taşınmazların mülkiyet hakkının kullanımının engellenmemesi halinde, taşınmazlara ilişkin her hangi kamulaştırma yapılmayacağı da kural altına alınmış olduğundan, tünel inşası durumunda da kamulaştırma yapılmayacaktır.

2. Bahse konu 4. maddenin ilk halinde mülkiyet hakkının kullanımının engellenmemesi kaydıyla taşınmazların üzerinde teleferik ve benzeri ulaşım hatları ile her türlü köprü, taşınmazların altında metro ve benzeri raylı taşıma sistemleri yapılması durumunda taşınmaz sahiplerine bu işlemler nedeniyle kamulaştırma, tazminat ve benzeri nam altında herhangi bir ücret ödenmeyeceği hükmü yer almakta iken anılan cümlenin iptali istemiyle açılan davada Anayasa Mahkemesinin 14.5.2015 tarihli, E:2014/177, K:2015/49 sayılı kararıyla, teleferik ve benzeri ulaşım hatları, her türlü köprü, metro ve benzeri raylı taşıma sistemleri gibi, ilgili bölgede yaşayan tüm kişiler bakımından yararlar sağlayan yatırımların külfetinin bir kısım taşınmaz maliklerine yüklenmesinin adalet ve hakkaniyet ölçüleriyle bağdaşmayacağı, bu nedenle anılan taşınmazların değerinde oluşan azalma nedeniyle taşınmaz maliklerine uygun bir tazminat ödenmesinin mülkiyet hakkının gereği olduğunu belirtilerek, malikin tazminat hakkından mahrum bırakılmasının Anayasa’ya aykırı olduğuna karar verilmiştir. Buna göre, bahse konu inşaat işleri meyanında tünel inşaatı dolayısıyla taşınmazlarının değerinde azalma oluşacak kişiler, İdareden tazminat talep edebileceklerdir. Ancak, iptali istenen kural gereğince, İdare vatandaşın mağduriyetini gidermek amacıyla istese de kamulaştırma yapamayacaktır.

3. Mülkiyet hakkına devletçe yapılabilecek müdahalelerin güvencesi Anayasa’nın 46. maddesinde düzenlenmiş olan kamulaştırma müessesesidir. Anayasa’ya göre temel ilke, kamu yararının gerektirdiği hallerde, gerçek karşılıkları peşin ödenmek şartıyla, kamulaştırma yapılması veya irtifak kurulmasıdır. Yine Anayasanın 46. maddesine göre, nakden ve peşin olarak ödenmesi gereken kamulaştırma ve kesin hükme bağlanan artırım bedelleri, bazı özel şartların mevcudiyeti halinde beş yılı aşmayacak şekilde taksitle ödenebilecektir. Bu haller Anayasa’da tahdidi olarak sayılmış olup, bunlar tarım reformunun uygulanması, büyük enerji ve sulama projeleri ile iskan projelerinin gerçekleştirilmesi, yeni ormanların yetiştirilmesi, kıyıların korunması ve turizmden ibarettir. Diğer bir ifadeyle mülkiyet hakkı yönünden metro, teleferik ve tünel gibi inşaatlar bu anayasal istisnanın dışında kalan, bedeli peşin ödenmesi gereken kamu müdahaleleridir.

4. Mülkiyet hakkı, bir malı dilediğince kullanma, semerelerinden faydalanma ve mal üzerinde dilediği gibi tasarrufta bulunmayı kapsayan bir haktır. Bir taşınmazın maliki de kanunlar çerçevesinde konut olarak kullanmak istediği bir yeri kullanırken aynı zamanda özel yaşamı güvence altına alan Anayasa'nın 20. maddesi ile Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinin koruması altındadır. A.İ.H.M. bu bağlamda "konutunda rahatsız edilmeden yaşamak hakkı"nı esas almak suretiyle, çevresel etkilerin ve müdahalelerin dahi özel hayatın korunmasına ilişkin Sözleşme hükmünün ihlali olarak değerlendirmektedir (Taşkın ve diğerleri/Türkiye, 46117/99).Altında tünel inşa edilen bir taşınmaz malın konut olarak kullanılması halinde AİHM'nin bahse konu içtihadı kapsamında incelenmesi gerekeceği açıktır.

5. Kuralla. tünel inşaatından mülkiyet hakkı olumsuz etkilenen bir kişinin mağduriyetinin, peşin ödeme yapılarak kamulaştırma yöntemiyle giderilmesi yerine kişinin ancak zararlarını tazminat yoluyla karşılamaya icbar edilmesinde Anayasa'nın 35. maddesiyle bağdaşmayan, aşırı bir sınırlandırma yapıldığı anlaşılmaktadır. Kural, bu nedenle Anayasa'nın 35. maddesine aykırıdır.

6. Öte yandan, böyle bir durumda yargısal yollara başvurulup uzun süreçlerin tamamlanmasından sonra tazminat elde edilse bile, Anayasa'nın 46. maddesinde yer alan peşin ödeme ilkesine Anayasa'da öngörülen haller dışında yasa ile istisna getiren kural, Anayasa'nın 46. maddesine de aykırıdır.

Açıklanan nedenlerle çoğunluk görüşüne katılmamaktayım.

Üye - Osman Alifeyyaz PAKSÜT

KARŞIOY GEREKÇESİ

27.3.2015 tarihli ve 6693 sayılı Kanun'un 22. maddesiyle 638 sayılı KHK'ya eklenen Geçici 13. maddenin (1) numaralı fıkrasının birinci cümlesinde yer alan "...Bakanlık Merkez Teşkilatı ile Spor Genel Müdürlüğü ve..." ibaresi:

1. Yasa ile yapılan düzenleme sonucunda Gençlik ve Spor Bakanlığının bağlı kuruluşu olan Yüksek Öğrenim Kredi ve Yurtlar Kurumu Genel Müdürlüğüne ait bölge müdürlükleri kapatılmış, Bakanlık Merkez Teşkilatı ile Spor Genel Müdürlüğü teşkilatında her hangi bir değişikliğe gidilmemiştir. Buna göre Anayasa Mahkemesi çoğunluğunca, iptali istenen kuralın öngördüğü şekilde yasa ile göreve son verme işlemlerinde hukuki ve fiili zorunluluk bulunmadığı düşüncesiyle kuralın, hukuki güvenlik ilkesini ihlal ettiği sonucuna varılmıştır.

2. Bununla birlikte yasa ile görevden alma işlemlerinde yeni bir yapılanmadan kaynaklanan hukuki ve fiili zorunluluğun takdiri, dar bir yoruma elverişli değildir. Yasa ile Gençlik ve Spor Bakanlığının bağlı kuruluşu olan Kredi ve Yurtlar Kurumunun teşkilatında önemli değişiklikler yapılmıştır. Buna bağlı olarak kimi kamu görevlilerinin de yer değiştirmesi, başka görevlere atanması gerekebilecek olup bunlardan bir kısmının, teşkilat yapısında bir değişiklik yapılmasa da Bakanlık Merkez Teşkilatı veya Spor Genel Müdürlüğünde hizmetine ihtiyaç duyulabilecektir.

3. Görevlerine son verilenlerin kazanılmış haklarını ihlal etmeyen, ancak buldukları kadro derecesiyle araştırmacı kadrolarına atanacaklarını öngören düzenlemenin, İdarede etkin ve verimli çalışmaya elverişli görevlendirme yapılması için Bakanlığın bütünü çerçevesinde bir personel düzenlemesi amacıyla yasalaştırıldığı anlaşılmaktadır. Kaldı ki araştırmacı kadrolarına yasa ile atanmış sayılanların idari işlemlerle yeniden eski görevlerine atanmalarına da bir engel bulunmamaktadır. Bu durumda bir zorunluluğa dayanmadığı, başka bir ifadeyle keyfi olduğu yolunda net bir yargıya ulaşılması mümkün olmayan kuralın Anayasa'nın "hukuki güvenlik" ilkesine de aykırı olduğundan söz edilemeyeceği kanaatindeyiz.

Üye; Osman Alifeyyaz PAKSÜT; Hicabi DURSUN; Kadir ÖZKAYA; Rıdvan GÜLEÇ; Recai AKYEL

KARŞIOY GEREKÇESİ

1. Anayasa Mahkemesince 2809 sayılı Kanun'un ek 158. maddesinin ikinci fıkrasının Mütevelli Heyetinin oluşumunu düzenleyen ikinci cümlesi oybirliğiyle iptal edilmiştir. İptal edilen hüküm "Mütevelli Heyeti; Sağlık Bakanlığı Müsteşarı, Rektör, Sağlık Bakanının seçeceği iki üye ile Yükseköğretim Kurulu tarafından seçilen profesör unvanına sahip bir üye olmak üzere, toplam beş üyeden oluşur". şeklindeydi.

2. Dava konusu hükmün iptal gerekçesinde Mütevelli Heyetinin üniversite yönetimine ilişkin mevcut yetkileri ve Mütevelli Heyetinin en az dört üye ile toplanıp salt çoğunlukla karar alabileceği göz önünde bulundurulduğunda, Mütevelli Heyeti üyelerinin çoğunluğunun Sağlık Bakanlığı Müsteşarı ile Sağlık Bakanının seçeceği iki üyeden oluşmasının merkezî idareye Mütevelli Heyeti kanalıyla üniversite yönetimine ilişkin karar alma sürecinde belirleyici olacak şekilde söz hakkı tanıyacağı, merkezî idareye üniversite yönetimi üzerinde denetim ve gözetim yetkisini aşan nitelikte bir yetki tanınmasının Anayasa'nın 130. maddesiyle güvence altına alınan bilimsel özerklikle bağdaşmadığı hususlarına yer verilmiştir.

3. Dięer bir ifadeyle Anayasa Mahkemesi; Mtevell Heyetinin oluřumunu, Mtevell Heyetinde bulunan kiřilerin bu heyette yer almamas gerektięi gerekesiyle deęil toplam say olarak beř olan Mtevell Heyeti yelerinin oęunluęunun Saęlık Bakanlıęı Msteřari ve Saęlık Bakannn seeceęi iki ye olarak belirlenmesinin merkez idareye, Mtevell Heyeti kanalıyla ynetimde sz hakk tanımakta olduęunu ve bunun Anayasa'nn 130. maddesiyle gvence altına alınan zerklik ilkesiyle baędařmadıęını belirterek iptal etmiřtir.

4. Anayasa Mahkemesi kararında daha sonra 2809 sayılı Kanun'un ek 158. maddesinin ikinci fıkrasının cnc cmlesi, 6216 sayılı Kanun'un 43. maddesinin drdnc fıkrası gereęince iptal edilmiřtir. İptal edilen cmle "Mtevell Heyetine Saęlık Bakanlıęı Msteřari, Msteřarin katılmadıęı toplantılara Rektr başkanlık eder." řeklindedir.

5. Kanaatimizce 2809 sayılı Kanun'un ek 158. maddesinin ikinci fıkrasının ikinci cmlesinin iptali sonrasında bile dava konusu cnc cmlenin uygulanma kabiliyeti halen devam etmektedir. Zira Anayasa Mahkemesinin iptal kararını dikkate alarak yasama organ tarafından yeni Mtevell Heyeti oluřumu tesis edilmesi durumunda Mtevell Heyetine yine Saęlık Bakanlıęı Msteřari, Msteřarin katılmadıęı toplantılara Rektr başkanlık edebilecektir. Dolayısıyla Mtevell Heyetinin oluřumunun iptali sonrasında da bu kuralın uygulanma kabiliyeti mevcuttur.

6. Bu nedenle Mtevell Heyetinin ye yapısını dzenleyen Kanun'un ek 158. maddesinin ikinci fıkrasının ikinci cmlesinin iptali nedeniyle kuralla doęrudan ilgili olan Mtevell Heyetine Saęlık Bakanlıęı Msteřarinn, Msteřarin katılmadıęı toplantılara Rektrn başkanlık edeceęini dzenleyen ek 158. maddesinin ikinci fıkrasının cnc cmlesinin uygulanma kabiliyeti kalmadıęından bu cmlenin de 6216 sayılı Kanun'un 43. maddesinin drdnc fıkrası gereęince iptali gerektięine ynelik oęunluk grřne katılmamaktayız.

ye: Hicabi DURSUN; Recai AKYEL; Yusuf řevki HAKYEMEZ

KARŐI OY

6639 sayılı Yasa'nn 5. maddesiyle 2809 sayılı Yasa'ya eklenen 158. maddenin ikinci fıkrasının cnc cmlesinde yer alan "Mtevell Heyetine Saęlık Bakanlıęı Msteřari, Msteřar'ın katılmadıęı toplantılara Rektr başkanlık eder" hkm oęunluk kararıyla, uygulama kabiliyetinin kalmadıęı gerekesiyle iptal edilmiřtir.

oęunluk kararında iptal edilen hkmn uygulama kabiliyetinin kalmadıęının gerekesi olarak, sz konusu hkmden nce gelen "Mtevell Heyeti; Saęlık Bakanlıęı Msteřari, Rektr, Saęlık

Bakanının seçeceği iki üye ile Yüksek Öğretim Kurulu tarafından seçilen profesör unvanına sahip bir üye olmak üzere, toplam beş üyeden oluşur.” hükmünün iptal edilmiş olması gösterilmektedir.

6216 sayılı Yasa'nın 43. maddesinin dördüncü fıkrasında, iptal veya itiraz başvurusu kanunun sadece belirli madde veya hükümleri aleyhine yapılmış olup da, bu madde veya hükümlerin iptali, kanunun diğer bazı hükümlerinin veya tamamının uygulanamaması sonucunu doğuruyorsa, Mahkemenin, uygulama kabiliyeti kalmayan kanunun bahis konusu öteki hükümlerinin veya tümünün iptaline karar verebileceği hüküm altına alınmıştır.

Uygulama kabiliyeti kalmadığı gerekçesiyle iptaline karar verilen hükmün, işbu başvuruda iptal edilmesi hususunda başvuruda bulunulduğunda ve hükmün kendisinden önce gelen hükümden bağımsız anlam ifade ettiği hususunda tereddüt bulunmamaktadır. Tartışmanın esası, kendinden önce gelen hükmün iptal edilmesinin, anılan düzenlemenin de iptalini gerektirip gerektirmeyeceği noktasında toplanmaktadır.

Hükmün uygulama kabiliyeti kalmadığı gerekçesiyle iptaline gerekçe oluşturan önceki hüküm, üniversitenin organlarından mütevelli heyetinin oluşumunu düzenlemekte olup Sağlık Bakanı'nın seçeceği iki üye ile birlikte Müsteşar'ın heyette bulunmasının idareye belirleyici şekilde söz hakkı üstünlüğü sağlayacağı, bu nedenle, Rektör ve profesör unvanlı bir üyenin heyette etkisiz kalacağı gerekçesiyle iptal edilmiştir. İptal kararı yayımlandıktan sonra yapılacak düzenlemede de Müsteşarın heyette kalması mümkündür. Çünkü iptal gerekçesinde, Müsteşarın heyette bulunmasının hukuken dayanaksız olduğundan söz edilmemekte, Müsteşarla birlikte Sağlık Bakanı'nın atayacağı iki üyenin, öğretim üyelerine sayısal üstünlük sağlamasının Anayasaya aykırılık oluşturduğu belirtilmektedir. Bu durumda bu hükmün iptalinin, Müsteşarın Mütevelli Heyetine başkanlık etmesini düzenleyen hükmün iptalini gerektirdiği söylenemeyeceğinden, bu hükmün önceki hükümden bağımsız olarak incelenmesi gerektiği düşünülmektedir.

Açıklanan nedenlerle, Sağlık Bakanlığı Müsteşarı'nın mütevelli heyetine başkanlık edeceğini düzenleyen hükmün uygulama kabiliyetinin kalmadığı gerekçesiyle iptaline ilişkin çoğunluk kararına katılmamıştır.

Üye - Muammer TOPAL

KARŞIOY GEREKÇESİ

6639 sayılı Kanunla 2809 sayılı Yükseköğretim Kurumları Teşkilatı Kanununa ilave edilen ek 158. maddenin iptali talep edilen beşinci fıkrasının Anayasaya aykırı olmadığına ve iptal talebinin reddine karar verilmiştir.

Anılan fıkranın üçüncü cümlesinde, Sağlık Bilimleri Üniversitesine tahsis edilecek öğretim elemanı kadrolarının Rektörün önerisi üzerine Mütevelli Heyeti tarafından il bazında belirlenmesi ve öğretim üyesi atamalarının bu kadrolara yapılması öngörülmektedir.

Kararın gerekçesinde maddenin ikinci fıkrasının birinci cümlesinde yer alan "...ile Mütevelli Heyetinden..." ibaresinin Anayasaya aykırılığı iddiasının reddine ilişkin gerekçelerin beşinci fıkranın üçüncü ve dördüncü cümleleri yönünden de geçerli olduğu, Anayasanın 130. maddesinin dokuzuncu fıkrasına göre kanun koyucunun anayasal sınırlar içinde Mütevelli Heyetinin görevlerini belirleme konusunda takdir yetkisine sahip olduğu, bu bağlamda Üniversiteye tahsis edilecek öğretim elemanı kadrolarının, temel bilimler hariç olmak üzere, birlikte kullanılan eğitim ve araştırma hastanesinin eğitim birimleri ve ihtiyacı dikkate alınarak, Rektörün önerisi üzerine Mütevelli Heyeti tarafından il bazında belirlenmesini ve öğretim üyesi atamalarının bu kadrolara yapılmasını öngören kuralın da kanun koyucunun takdir yetkisi kapsamında olduğu ve kuralda Anayasaya aykırı bir hususun bulunmadığı belirtilmektedir.

İkinci fıkranın birinci cümlesindeki ibarenin reddine ilişkin gerekçede ise, Anayasanın 130. maddesinin dokuzuncu fıkrasında yükseköğretim kurumlarının organları ile bunların görev, yetki ve sorumluluklarını belirleme yetkisinin kanun koyucuya verildiği, kanun koyucunun Anayasanın ilgili kurallarına bağlı olarak yükseköğretim kurumlarının yönetim organlarını belirleyebileceği, bu konuda kanun koyucuyu sınırlandıran anayasal bir ilke bulunmadığından düzenlemenin Üniversitenin bilimsel özerkliğini zedelediği ifade edilmektedir.

Maddenin ikinci fıkrasının birinci cümlesinde yer alan ibarenin iptali talebinin reddine ilişkin karara ve yukarıda özetlenen gerekçeye katılmakla birlikte, yükseköğretim kurumlarının organlarının görev, yetki ve sorumluluklarının belirlenmesi konusunda yasama organının takdir yetkisini sınırlandıran anayasal bir ilke bulunmadığı yönündeki tespiti katılmamıza imkân bulunmamaktadır.

Bu çerçevede, kuralın Anayasanın 131. maddesi yönünden de incelenmesi gerektiği düşünülmektedir.

Bilindiği gibi, Anayasanın 131. maddesinde yükseköğretim kurumlarının öğretimini planlamak, düzenlemek, yönetmek, denetlemek, yükseköğretim kurumlarındaki eğitim-öğretim ve bilimsel araştırma faaliyetlerini yönlendirmek, bu kurumların kanunda belirtilen amaç ve ilkeler

doğrultusunda kurulmasını, geliştirilmesini ve üniversitelere tahsis edilen kaynakların etkili bir biçimde kullanılmasını sağlamak ve öğretim elemanlarının yetiştirilmesi için planlama yapmak maksadı ile Yükseköğretim Kurulunun (YÖK) kurulacağı belirtilerek YÖK'e yükseköğretimin planlanması, düzenlenmesi, yönetilmesi, denetlenmesi ve yönlendirilmesi görevi verilmiş bulunmaktadır.

YÖK'ün Anayasa ile verilen bu görevleri yerine getirebilmesi bakımından, 2547 sayılı Kanunla üniversitelerin ihtiyaçlarını, eğitim-öğretim programlarını, bilim dallarının niteliklerini, araştırma faaliyetlerini, uygulama alanlarını, fizikî imkânlarını, öğrenci sayılarını ve ilgili diğer hususları dikkate alarak öğretim üyesi kadrolarını dengeli bir oranda tespit etme görevi de YÖK'e verilmiş bulunmaktadır.

Üniversitelere tahsis edilen öğretim üyesi kadrolarına atama yapılmasının usul ve esasları da 2547 sayılı Kanunda belirlenmekte ve atamalar yukarıda belirtilen ilke çerçevesinde yapılmaktadır.

İncelenen maddenin beşinci fıkrasının üçüncü cümlesinde ise, öğretim üyesi kadroları da dahil olmak üzere öğretim elemanı kadrolarının Mütevelli Heyeti tarafından il bazında belirlenerek öğretim üyesi atamalarının bu kadrolara yapılacağı öngörülmek suretiyle yetki doğrudan Mütevelli Heyetine verilmektedir.

Anayasanın 131. maddesine göre yükseköğretimin planlanması ve eğitim-öğretim ve araştırma faaliyetlerinin yönlendirilmesi kapsamında YÖK'ün, öğretim üyelerinin üniversiteler ve üniversitelerin birimleri arasında dengeli bir şekilde dağılımını tespit etmekle sorumlu olduğu dikkate alındığında, üçüncü cümlede öngörülen hükmün Anayasanın 131. maddesine aykırı olduğu düşünülmektedir.

Bu itibarla, beşinci fıkranın üçüncü cümlesinin Anayasanın 131. maddesine aykırılığından dolayı iptal edilmesi gerektiği düşüncesiyle, çoğunluğun red yönündeki görüşüne katılmıyorum.

Üye - M. Emin KUZ

Anayasa Mahkemesi - 5237 sayılı Türk Ceza Kanunu Kararı (E. 2015/32)

Ceza Mevzuatında Kişisel Verilerle İlgili Bir Tanım ve Sınırlandırma Yapılmamasının Suçta ve Cezada Kanunilik İlkesini İhlal Etmediğine İlişkin Anayasa Mahkemesi Kararı

ANAYASA MAHKEMESİ KARARI

Esas Sayısı : 2015/32

Karar Sayısı : 2015/102

Karar Tarihi : 12.11.2015

RG Tarih-Sayı: 02.12.2015 - 29550

İTİRAZ YOLUNA BAŞVURAN: Batman 2. Asliye Ceza Mahkemesi

İTİRAZIN KONUSU: 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun, 21.2.2014 tarihli ve 6526 sayılı Kanun'un 4. maddesiyle değişik 136. maddesinin (1) numaralı fıkrasının, Anayasa'nın 38. maddesine aykırılığı ileri sürülerek iptaline karar verilmesi talebidir.

OLAY: Sanık hakkında kişisel verileri hukuka aykırı olarak ele geçirme ve yayma suçundan açılan kamu davasında, itiraz konusu kuralın Anayasa'ya aykırı olduğu kanısına varan Mahkeme, iptali için başvurmuştur.

I- İPTALİ İSTENİLEN KANUN HÜKMÜ

Kanun'un itiraz konusu 136. maddesi şöyledir:

"Madde 136- (1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır."

II- İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri gereğince Zühtü ARSLAN, Serruh KALELİ, Alparslan ALTAN, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ, Burhan ÜSTÜN, Engin YILDIRIM, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Erdal TERCAN, Muammer TOPAL, M. Emin KUZ, Hasan Tahsin GÖKCAN ve Kadir ÖZKAYA'nın katılımlarıyla 1.4.2015 tarihinde yapılan ilk inceleme toplantısında, dosyada eksiklik bulunmadığından işin esasının incelenmesine OYBİRLİĞİYLE karar verilmiştir.

III- ESASIN İNCELENMESİ

2. Başvuru kararı ve ekleri, Raportör Berrak YILMAZ tarafından hazırlanan işin esasına ilişkin rapor, itiraz konusu kanun hükmü, dayanan ve ilgili görülen Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü.

A- İtirazın Gerekçesi

3. Başvuru kararında özetle, ceza mevzuatında kişisel verilerle ilgili bir tanım ve sınırlandırma yapılmadığından, itiraz konusu kuralın suçta ve cezada kanunilik ve belirlilik ilkelerine ve Anayasa'nın 38. maddesine aykırı olduğu ileri sürülmüştür.

B- Anayasa'ya Aykırılık Sorunu

4. 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 43. maddesi uyarınca, kural Anayasa'nın 20. maddesi yönünden de incelenmiştir.

5. İtiraz konusu kuralla, kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişinin, iki yıldan dört yıla kadar hapis cezası ile cezalandırılması öngörülmektedir.

6. Anayasa'nın 20. maddesinin birinci fıkrasında, herkesin, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş; üçüncü fıkrasında da "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." denilerek kişisel verilerin korunması, özel hayatın gizliliğinin korunması kapsamında güvenceye kavuşturulmuştur.

7. Anayasa'nın 38. maddesinin ilk fıkrasında "Kimse, işlendiği zaman yürürlükte bulunan kanunun suç saymadığı bir fiilden dolayı cezalandırılmaz..." denilerek "suçun kanuniliği"; üçüncü fıkrasında da "Ceza ve ceza yerine geçen güvenlik tedbirleri ancak kanunla konulur." denilerek, "cezanın kanuniliği" ilkesi getirilmiştir. Aynı şekilde 5237 sayılı Türk Ceza Kanunu'nun 2. maddesinde yer alan "Kanunun açıkça suç saymadığı bir fiil için kimseye ceza verilemez ve güvenlik tedbiri uygulanamaz. Kanunda yazılı cezalardan ve güvenlik tedbirlerinden başka bir ceza ve güvenlik tedbirine hükmolünamaz." hükmü ile ceza hukukumuzda da "suçta ve cezada kanunilik" ilkesi kabul edilmiştir. Bu ilke uyarınca hangi eylemlerin yasaklandığı ve bu yasak eylemlere verilecek cezaların hiçbir kuşkuyla yer bırakmayacak biçimde yasada gösterilmesi, kuralın açık, anlaşılır ve sınırlarının

belli olması gerekmektedir. Kişilerin suç sayılan eylemleri önceden bilmeleri gerektiği düşüncesine dayanan bu ilke, aynı zamanda temel hak ve özgürlükleri en geniş biçimiyle gerçekleştirip güvence altına almakla yükümlü olan hukuk devletinin esas aldığı değerlerden olup, uluslararası hukukta ve insan hakları belgelerinde de özel bir yere ve öneme sahip bulunmaktadır. Kanunilik ilkesi, özgürlüğün sınırlarının önceden bilinerek, insanın davranışlarını bu çerçevede düzenlemesini temin için getirilmiştir. Kanunilik ilkesi aynı zamanda kıyas yoluyla yeni bir suç ihdasına ve ceza normlarının genişletilmesine engel oluşturur.

8. 5237 sayılı Kanun'un "Kişisel verilerin kaydedilmesi" başlıklı 135. maddesinin gerekçesinde, gerçek kişiyle ilgili her türlü bilginin kişisel veri olarak kabul edilmesi gerektiği belirtilmiştir. Ayrıca, Kanun'un 134. ilâ 139. maddeleri arasında kişisel verilerin korunmasına yönelik hükümler yer almaktadır. Söz konusu maddelerde kişisel verilerin açık bir tanımı yer almamakla birlikte kişisel verilere yönelik olarak "kişilerin özel hayatına ilişkin görüntü veya sesler", "siyasi, felsefi veya dini görüş", "ırki köken", "ahlaki eğilim", "cinsel yaşam", "sağlık durumu" ve "sendikal bağlantılar" gibi kavramlara yer verilmektedir.

9. Anayasa Mahkemesinin kararlarında da belirtildiği üzere, "kişisel veri", "belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler" kişisel veri olarak kabul edilmektedir (E.2013/122, K.2014/74, 9.4.2014; E.2014/149, K.2014/151, 2.10.2014; E.2013/84, K.2014/183, 4.12.2014; E.2014/74, K.2014/201, 25.12.2014; E.2014/180, K.2015/30, 19.3.2015).

10. Türkiye'nin imzaladığı ancak uygulama kanununun yürürlüğe konmaması nedeniyle henüz taraf olmadığı 1981 tarihli ve 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Avrupa Konseyi Sözleşmesi'nin 2. maddesinde "kişisel veri", "kimliği belirli veya belirlenebilecek verinin öznesi olan gerçek kişiyle ilgili tüm bilgiler" şeklinde tanımlanmaktadır. Sözleşme'nin "özellikli veri kategorileri" başlıklı 6. maddesinde ise "iç hukukta uygun güvenceler sağlanmadıkça, ırk menşesini, politik düşünceleri, dinî veya diğer inançları ortaya koyan kişisel nitelikteki verilerle sağlık veya cinsel yaşamla ilgili kişisel nitelikteki veriler ve ceza mahkûmiyetleri, otomatik bilgi işlemine tâbi tutulamazlar" demek suretiyle söz konusu verilerin kişisel veri kapsamında olduğunu belirlemektedir. Ekonomik Kalkınma ve İşbirliği Örgütü'nün

(OECD) yayınladığı Kişisel Verilerin Korunması Rehber İlkeleri'nde "kişisel veri", "belirli veya belirlenebilir bir gerçek kişiye ilişkin tüm bilgiler" şeklinde tanımlanmaktadır. Avrupa Birliği'nin 95/46/EC sayılı Veri Koruma Direktifi'nin 2. maddesinde de "kişisel veri", "belirli ya da kimliği belirlenebilir gerçek kişi ile ilişkilendirilebilen her türlü bilgi" şeklinde tanımlandıktan sonra "bir kişinin doğrudan veya dolaylı olarak tanımlanabilmesine imkân sağlayan kişinin kimlik numarası, fiziksel, psikolojik, duygusal, ekonomik ve kültürel kimliği veya sosyal kimliğin"nin bu kapsamda değerlendirildiği ifade edilmektedir.

11. "Kişisel veri" kavramı tarafı olduğumuz Avrupa İnsan Hakları Sözleşmesi'nde (AİHS) açık bir şekilde düzenlenmemekle birlikte, Sözleşme'nin uygulanmasına ilişkin Avrupa İnsan Hakları Mahkemesi (AİHM) kararlarında Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşme'ye atıfta bulunulmakta ve bu verilerin özel yaşamın gizliliğinin bir parçası olduğu kabul edilmektedir. AİHM kararlarında kişilere ait "görüntü", "fotoğraf", "parmak izi", "DNA profili", "hücre örnekleri", "ev adresi"ve "yaş, doğum tarihi ve fiziksel özellikler" "kişisel veri" kapsamında değerlendirilmektedir (Peck/Birleşik Krallık, B.No: 44647/98, 28.01.2003; Sciacca/İtalya, B.No:50774/99, 11.01.2005; S. ve Marper/Birleşik Krallık, (Büyük Daire), B.No: 30562/04, 30566/04, 04.12.2008; Alkaya/Türkiye, B.No:42811/06, 09.10.2012; K.U./Finlandiya, B.No:2872/02, 02.12.2008).

12. İtiraz konusu kuralla, kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişinin iki yıldan dört yıla kadar hapis cezası ile cezalandırılacağı düzenlenmiştir. Kanun koyucunun kuralla, gerekçede de ifade edildiği gibi Anayasa'nın 20. maddesi ile güvence altına alınan kişisel verilerin ve özel hayatın daha etkin bir şekilde korunmasını sağlamayı amaçladığı anlaşılmaktadır. Zira kişisel verilerin korunması hakkı, kişinin insan onurunun korunması ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, kişisel verilerin işlenmesi sırasında bireyin hak ve özgürlüklerini korumayı amaçlamaktadır.

13. Kuralda yer alan "kişisel veri" kavramı teknolojik gelişmelere bağlı olarak çok farklı şekillerde ortaya çıkabileceğinden bu kapsama giren tüm verilerin kanun koyucu tarafından önceden öngörülebilmesi ve tek tek sayılabilmesi mümkün değildir. Bununla birlikte gerek ulusal ve uluslararası mevzuat gerekse yargı içtihatları çerçevesinde "kişisel veri" kavramının, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade ettiği kabul edilmektedir.

14. "Kişisel veri" kavramının bu çerçevede doktrin, uygulama ve yargı kararlarında belirlenerek anlam ve içeriğinin gelişip değişeceğinde kuşku yoktur. Dolayısıyla başvuru kararında her ne kadar ceza mevzuatında "kişisel veri" ile ilgili bir tanım ve sınırlandırmanın yapılmadığı, bu nedenle itiraz

konusu kuralın belirsiz olduđu ileri sürülmüş ise de ulusal ve uluslararası mevzuat ile yargı içtihatları dikkate alındığında kuralın belirsiz olduğundan söz edilemeyeceği açıktır. Ayrıca itiraz konusu kuralla "kişisel verileri, hukuka aykırı olarak bir başkasına verme, yayma veya ele geçirme" eylemi suç olarak kabul edilmekte ve bu eylem nedeniyle verilecek ceza kuralda açıkça belirlendiğinden kuralla hangi somut eylem ve olguya hangi hukuksal yaptırımın bağlandığı açıkça ortaya konulmaktadır. Dolayısıyla itiraz konusu kuralda suçta ve cezada kanunilik ilkesi ile özel hayatın gizliliği ilkesine aykırılık bulunmamaktadır.

15. Açıklanan nedenlerle kural, Anayasa'nın 20. ve 38. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

IV- HÜKÜM

26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun, 21.2.2014 tarihli ve 6526 sayılı Kanun'un 4. maddesiyle değiştirilen 136. maddesinin (1) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve itirazın REDDİNE, 12.11.2015 tarihinde OYBİRLİĞİYLE karar verildi.

Başkan

Zühtü ARSLAN

Başkanvekili

Burhan ÜSTÜN

Başkanvekili

Engin YILDIRIM

Üye

Serdar ÖZGÜLDÜR

Üye

Serruh KALELİ

Üye

Osman Alifeyyaz PAKSÜT

Üye

Recep KÖMÜRCÜ

Üye

Alparslan ALTAN

Üye

Nuri NECİPOĞLU

Üye

Hicabi DURSUN

Üye

Celal Mümtaz AKINCI

Üye

Erdal TERCAN

Üye

Muammer TOPAL

Üye

M. Emin KUZ

Üye

Hasan Tahsin GÖKCAN

Üye

Kadir ÖZKAYA

Üye

Rıdvan GÜLEÇ

**Anayasa Mahkemesi - 6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun
Kararı (E. 2014/196)**

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2014/196

Karar Sayısı: 2015/103

Karar Tarihi: 12.11.2015

RG Tarih - Sayı: 16.12.2015 - 29564

İTİRAZ YOLUNA BAŞVURAN: Ankara 16. Tüketici Mahkemesi

İTİRAZIN KONUSU: 31.3.2011 tarihli ve 6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun'un 5. maddesinin;

1- (4) numaralı fıkrasının ikinci, üçüncü, dördüncü ve beşinci cümlelerinin,

2- (11) numaralı fıkrasının,

Anayasa'nın 10., 17., 20. ve 59. maddelerine aykırılığı ileri sürülerek iptallerine karar verilmesi talebidir.

OLAY: 6222 sayılı Kanun'un 5. maddesi uyarınca gerçekleştirilen elektronik kart uygulamasının durdurulması, ihlal ettiği hakların tespiti, neden olduğu hukuka aykırılıkların giderilmesi ve bu uygulama nedeniyle zorla imzalatırılan sözleşmelerin geçersizliğine karar verilmesi talebiyle açılan davada, itiraza konu kuralların Anayasa'ya aykırı olduğu kanısına varan Mahkeme, iptalleri için başvurmuştur.

I- İPTALİ İSTENİLEN KANUN HÜKÜMLERİ

6222 sayılı Kanun'un itiraz konusu kuralların da yer aldığı 5. maddesi şöyledir:

"Spor alanlarının güvenlik ve düzenine ilişkin tedbirler

MADDE 5- (1) Ev sahibi spor kulüpleri;

a) Spor alanlarında sağlık ve güvenliğe,

b) Müsabakanın yapılacağı yerde konuk takım seyircilerine bağımsız bir bölüm ayırmak ve taraftarlar arasında temas olmamasını sağlamaya yönelik olarak, ilgili spor federasyonları ve uluslararası spor federasyonları tarafından belirlenen önlemleri almakla yükümlüdür.

(2) Spor kulüpleri, müsabakanın güvenliğini sağlamak amacıyla il veya ilçe spor güvenlik kurullarının kendileriyle ilgili olarak aldığı kararları yerine getirmekle yükümlüdür.

(3) Birinci ve ikinci fıkralar kapsamındaki yükümlülüklerin yerine getirilmesi amacıyla özellikle;

a) Spor alanlarına, seyri engellemeyecek şekilde ve federasyonun bağlı olduğu uluslararası federasyonun talimatlarına uygun olarak seyirci ile müsabakanın yapıldığı yer arasında tel, duvar, bariyer ve benzeri fizikî engeller konulabilir.

b) Fizikî engeller, ilgili spor güvenlik biriminin görüşü alınarak, il veya ilçe spor güvenlik kurullarının kararı ile kaldırılabilir.

c) Spor alanlarında, çocuklar ve engellilerin müsabakaları izleyebilmeleri için durumlarına uygun yerler tahsis edilir.

ç) Spor alanlarında seyircilerin oturma yerleri numaralandırılır. Bilet satışları koltuk numarasıyla ilişkilendirilerek yapılır. Müsabaka alanlarına kapasitenin üzerinde veya biletsiz seyirci alınamaz.

(4) Spor müsabakalarının yapıldığı alanlara girişi sağlayacak biletler, elektronik sistem üzerinden oluşturulur. Bilet satın almak isteyen kişilerle ilgili olarak, üzerinde adı, soyadı, Türkiye Cumhuriyeti kimlik numarası ve fotoğrafı olan bir elektronik kart oluşturulur. Kişinin yabancı olması halinde kart üzerinde Türkiye Cumhuriyeti kimlik numarası yerine uyruğu olduğu devletin adı ile Türkiye'ye giriş yaptığı pasaportun seri numarası kaydedilir. Bilet satışları kişilere özgü elektronik kart üzerinden yapılabilir. Spor müsabakalarına, kişi ancak adına düzenlenen elektronik kart ile izleyici olarak girebilir. Spor müsabakasına izleyici olarak girecek kişilerin kontrolünü ev sahibi kulüp yapmakla yükümlüdür. Bu yükümlülük ev sahibi olmayan müsabakalarda, müsabakaya katılan her iki kulüp; milli müsabakalarda ise, ilgili federasyon tarafından yerine getirilir.

(5) Spor alanlarında; güvenliğin sağlanması ve bu Kanuna aykırı davranışların tespiti amacıyla, gerekli teknik donanımlar kurulur. Kameralar ve benzeri teknik donanımların yerleştirilecekleri yerler ve sayıları il veya ilçe spor güvenlik kurulları tarafından belirlenir.

(6) Futbol dalında en üst lig ile bir altındaki ligde bulunan kulüpler, dördüncü ve beşinci fıkralardaki sistemle ilgili teknik donanımları kendi kullanımındaki spor alanlarında kurmakla yükümlüdür. Elektronik karta ilişkin hükümler hariç olmak üzere aynı yükümlülükler, basketbol, voleybol ve hentbol dallarındaki en üst ligde bulunan kulüplerin kendi kullanımındaki spor alanları bakımından da geçerlidir.

(7) Futbolda en üst profesyonel lig ve bir altındaki ligde bulunan kulüplerin müsabakalarının yapıldığı spor alanlarında; bu Kanunda sayılan diğer spor branşlarında ise uluslararası spor müsabakalarının yapıldığı spor alanlarında ev sahibi ve misafir takım için ayrı ayrı olmak ve gerektiğinde kullanılmak üzere azami yirmi kişi kapasiteli en az iki tane bekletme odası ile genel kolluk görevlileri ile özel güvenlik görevlilerinin kullanımına açık tutulacak güvenlik kameraları ve anons sistemlerinin yönetildiği yeteri kadar kontrol odasının oluşturulması zorunludur. Kontrol odasında federasyon ve spor kulübü temsilcileri de bulunur. Kayıt altına alınan görüntü ve dokümanların birer örneği, müsabakanın sonunda ilgili spor güvenlik birimine, federasyona ve her iki kulüp temsilcisine verilir.

(8) Dördüncü, beşinci ve yedinci fıkralarda belirtilen güvenlik sistemlerinin ve odalarının giderleri, en üst profesyonel futbol ligi ve bir altındaki ligdeki kulüplerin kendileri tarafından; basketbol, voleybol ve hentbol dalları için ise spor tesisinin kullanım hakkına sahip olan kulüp ya da kuruluş tarafından karşılanır.

(9) Spor alanlarında hangi güvenlik sistemi veya teknik donanımın uygulanacağı ilgili federasyonun bağlı olduğu uluslararası spor örgütlerinin düzenlemeleri çerçevesinde yönetmelikle belirlenir.

(10) Spor alanları ile çevresinde; bu alanlara sokulması yasak maddelere ve eşyalara, yasak olan davranışlara ve bu alanlarda elektronik takibin yapıldığına ilişkin uyarı levhalarına yer verilir. Bu yükümlülük ilgili spor alanı kullanımında olan spor kulübü tarafından yerine getirilir.

(11) Dördüncü fıkrada belirtilen elektronik kart uygulaması ile ilgili olarak;

a) Bilet organizasyonu ve seyircilerin müsabaka alanlarına giriş ve çıkışına ilişkin kontrol ve denetim yetkisi federasyonlara ait olup federasyonlar bu amaçla bünyelerinde merkezi kontrol sistemi oluşturur. Elektronik kart oluşturulmak amacıyla alınacak kişisel bilgiler federasyon bünyesinde oluşturulan merkezi veri tabanında tutulur. Bu veri tabanı Maliye Bakanlığı ve İçişleri Bakanlığı erişimine açıktır.

b) Elektronik kart ile elektronik kart kapsamında satışı gerçekleştirilecek biletlerin basım, satış ve dağıtımına ilişkin yerel uygulamalar kulüpler tarafından, sistem üzerinden merkezi satışları ise ilgili federasyonlar tarafından gerçekleştirilir.

c) Elektronik kart bilgilerinin kulüpler adına reklam ve pazarlamasında ilgili federasyonlar yetkilidir. Merkezi pazarlama ve bilet satışından elde edilecek gelirler kulüplere ait olup federasyon ya da yetki verdiği üçüncü kişiler nezdinde oluşacak bu gelirler kamu kurum ve kuruluşlara ilişkin alacaklar

hariç olmak üzere haczedilemez, devir ve temlik edilemez. Federasyonlar bu fıkra kapsamında belirtilen yetkilerini kısmen veya tamamen üçüncü kişilere devredebilir."

II- İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Haşim KILIÇ, Serruh KALELİ, Alparslan ALTAN, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ, Burhan ÜSTÜN, Engin YILDIRIM, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Erdal TERCAN, Muammer TOPAL, Zühtü ARSLAN, M. Emin KUZ ve Hasan Tahsin GÖKCAN'ın katılımlarıyla 25.12.2014 tarihinde yapılan ilk inceleme toplantısında, dosyada eksiklik bulunmadığından işin esasının incelenmesine OYBİRLİĞİYLE karar verilmiştir.

III- ESASIN İNCELENMESİ

2. Başvuru kararı ve ekleri, Raportör Ümit DENİZ tarafından hazırlanan işin esasına ilişkin rapor, itiraz konusu kanun hükümleri, dayanılan ve ilgili görülen Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü.

A- Uygulanacak Kural Sorunu

3. Anayasa'nın 152. ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 40. maddelerine göre, mahkemeler, bakmakta oldukları davalarda uygulayacakları kanun ya da kanun hükmünde kararname kurallarını Anayasa'ya aykırı görürler veya taraflardan birinin ileri sürdüğü aykırılık iddiasının ciddi olduğu kanısına varırlarsa, o hükmün iptali için Anayasa Mahkemesine başvurmaya yetkilidirler. Ancak, bu kurallar uyarınca bir mahkemenin Anayasa Mahkemesine başvurabilmesi için elinde yöntemince açılmış ve mahkemenin görevine giren bir davanın bulunması ve iptali istenen kuralların da o davada uygulanacak olması gerekmektedir. Uygulanacak yasa kuralları, davanın değişik evrelerinde ortaya çıkan sorunların çözümünde veya davayı sonuçlandırmada olumlu ya da olumsuz yönde etki yapacak nitelikte bulunan kurallardır.

4. İtiraz yoluna başvuran Mahkeme, 5. maddenin (11) numaralı fıkrasının (c) bendinin ikinci cümlesinin de iptalini istemiştir. Anılan cümle, merkezi pazarlama ve bilet satışından elde edilecek gelirlerin kulüplere ait olduğunu ve federasyon veya yetki verdiği üçüncü kişiler nezdinde oluşacak bu gelirlerin, kamu kurum ya da kuruluşlarına ilişkin alacaklar hariç olmak üzere haczedilemeyeceğini, devir ve temlik edilemeyeceğini öngörmektedir. İtiraz yoluna başvuran Mahkemedeki bakılmakta olan dava ise elektronik kart ve biletin somut uygulamasının ihlal ettiği hakların tespiti, neden olduğu hukuka aykırılıkların giderilmesi ve bu uygulama nedeniyle zorla imzalatırılan sözleşmelerin geçersizliğine karar verilmesine ilişkindir. Söz konusu davanın

kulüplerin haklarına yönelik değil, bizatihi taraftar haklarına yönelik olduğu anlaşılmaktadır. Bu durumda, elektronik kart ve biletin taraftar yönünden uygulaması ile ilgisi bulunmayan bu cümlenin bakılmakta olan davadaki uyuşmazlığın çözümüne bir etkisi yoktur. Dolayısıyla belirtilen kuralın, itiraz başvurusunda bulunan Mahkemenin bakmakta olduğu davada uygulanma olanağı bulunmamaktadır.

5. Açıklanan nedenle, 31.3.2011 tarihli ve 6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun'un 5. maddesinin (11) numaralı fıkrasının (c) bendinin ikinci cümlesinin, itiraz başvurusunda bulunan Mahkemenin bakmakta olduğu davada uygulanma olanağı bulunmadığından, bu cümleye ilişkin başvurunun Mahkemenin yetkisizliği nedeniyle REDDİNE, OYBİRLİĞİYLE karar verilmiştir.

B- Kanun'un 5. Maddesinin (4) Numaralı Fıkrasının İkinci, Üçüncü, Dördüncü ve Beşinci Cümleleri ve (11) Numaralı Fıkrasının (a) Bendinin Birinci Cümlesi ile (b) Bendinin İncelenmesi

1- İtirazın Gerekçesi

6. Başvuru kararında özetle, bilim, sanat ve müzik gibi insanlığın pozitif müşterek birikimlerinden biri olan sporun birçok ırk, mezhep, cinsiyet, sosyal kesim ve farklı insanları bir araya getirmesi nedeniyle evrensel bir nitelik taşıdığı, ayrıca eğlenme ve dinlenme haklarını içeren başlı başına temel bir hak ve hürriyet olduğu, bunların yanında insan haysiyeti ve şahsiyetinin serbestçe gelişmesi için zaruri olan ekonomik, sosyal ve kültürel haklardan biri olarak kabul edildiği, bu hakkın haberleşme ve seyahat özgürlükleri ile özel hayat ve aile hayatına saygı hakkı ile de ilgili olduğu, sporda şiddetin ulusal ve uluslararası alanda büyük sorun teşkil ettiği, şiddetten sporcuların yanı sıra sportif faaliyetleri izlemek isteyenlerin de mağdur olduğu, kanun koyucunun şiddeti önlemek için yaptığı yasal düzenlemelerin yeterli olmadığı ve bu düzenlemelerin şiddet mağduru bireylerin mağduriyetlerini artırdığı, şiddetin masum ve mağdur insanların temel hak ve özgürlüklerinin kısıtlanması suretiyle önlenemeyeceği, temel bir hak ile ilgili düzenlemelerin evrensel normlar dikkate alınarak gerçekleştirilmesi gerektiği halde elektronik kart uygulamasının gerçek sporseverlerin haklarını ihlal ettiği, kısıtlıların vasilerinin izni olmaksızın kendi başlarına kart alamaları nedeniyle spor müsabakalarını izlemelerinin engellenmesinin reşit olmayanlar ile kısıtlıların haklarını ihlal ettiği, ayrıca uygulamanın sadece futbol ve bu branşın da süper lig ve birinci ligiyle sınırlı olup diğer ligler ile basketbol, voleybol, hentbol ile diğer branşlarda uygulanmamasının kanun önünde eşitlik ilkesine aykırı olduğu, elektronik kart ile toplu bilet alımı olmadığından, kimsenin başkasını maça davet etme olanağının kalmamasının toplumumuzda var olan ikram kültürünü ortadan kaldırdığı, uygulamanın özgür irade ve hareket serbestisine ciddi bir müdahale

oluşturduğu belirtilerek kuralların, Anayasa'nın 10., 17., 20. ve 59. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

7. 6216 sayılı Kanun'un 43. maddesi uyarınca, itiraz konusu kurallar ilgileri nedeniyle Anayasa'nın 2. maddesi yönünden de incelenmiştir.

8. Kanun'un itiraz konusu kuralları da içeren 5. maddesi, spor alanlarının güvenlik ve düzeni için başta ev sahibi olmak üzere spor kulüplerinin yerine getirmesi gereken yükümlülükleri, alınacak güvenlik tedbirlerini, elektronik kart ve bilet uygulamasını ve gerçekleştirilme usullerini düzenlemektedir.

9. 5. maddenin (4) numaralı fıkrasında, elektronik bilet ve kart uygulaması ile spor müsabakasına gireceklerin kontrolüne ilişkin yükümlülükler öngörülmekte olup itiraz konusu cümlelerde, elektronik bilet satın almak isteyen kişilerle ilgili olarak, üzerinde adı, soyadı, Türkiye Cumhuriyeti kimlik numarası ve fotoğrafı olan bir elektronik kart oluşturulacağı, kişinin yabancı olması halinde kart üzerinde Türkiye Cumhuriyeti kimlik numarası yerine uyruğu olduğu devletin adı ile Türkiye'ye giriş yaptığı pasaportun seri numarasının kaydedileceği, bilet satışlarının kişilere özgü elektronik kart üzerinden yapılabileceği ve spor müsabakalarına, kişinin ancak adına düzenlenen elektronik kart ile izleyici olarak girebileceği düzenlenmektedir.

10. Anılan maddenin itiraz konusu (11) numaralı fıkrası ise elektronik bilet uygulamasının ayrıntılarını düzenlemekte olup fıkranın (a) bendinin birinci cümlesinde bilet organizasyonu ve seyircilerin müsabaka alanlarına giriş ve çıkışına ilişkin kontrol ve denetim yetkisinin federasyonlara ait olduğu ve federasyonların bu amaçla bünyelerinde merkezi kontrol sistemi oluşturacakları, (b) bendinde de, elektronik kart ve elektronik kart kapsamında satışı gerçekleştirilecek biletlerin basım, satış ve dağıtımına ilişkin yerel uygulamaların kulüpler tarafından, sistem üzerinden merkezi satışların ise ilgili federasyonlar tarafından gerçekleştirileceği öngörülmektedir.

11. Anayasa'nın 2. maddesinde belirtilen hukuk devleti, eylem ve işlemleri hukuka uygun, insan haklarına saygılı, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adaletli bir hukuk düzeni kurup bunu geliştirerek sürdüren, Anayasa'ya aykırı durum ve tutumlardan kaçınan, Anayasa ve hukukun üstün kurallarıyla kendini bağlı sayan, yargı denetimine açık olan devlettir.

12. Kanun koyucu düzenlemeler yaparken hukuk devleti ilkesinin bir gereği olan ölçülülük ilkesiyle bağlıdır. Bu ilke ise "elverişlilik", "gereklilik" ve "orantılılık" olmak üzere üç alt ilkeden oluşmaktadır. "Elverişlilik", başvuru önlemin ulaşılmak istenen amaç için elverişli olmasını, "gereklilik"

başvurulan önlemin ulaşılmak istenen amaç bakımından gerekli olmasını, "orantılılık" ise başvurulan önlem ve ulaşılmak istenen amaç arasında olması gereken ölçüyü ifade etmektedir. Bir kurala uyulmaması nedeniyle kanun koyucu tarafından öngörülen yaptırım ile ulaşılmak istenen amaç arasında da "ölçülülük ilkesi" gereğince makul bir dengenin bulunması zorunludur.

13. Anayasa'nın 10. maddesinde belirtilen "kanun önünde eşitlik ilkesi" hukuksal durumları aynı olanlar için söz konusudur. Bu ilke ile eylemli değil, hukuksal eşitlik öngörülmüştür. Eşitlik ilkesinin amacı, aynı durumda bulunan kişilerin kanunlar karşısında aynı işleme bağlı tutulmalarını sağlamak, ayırım yapılmasını ve ayrıcalık tanınmasını önlemektir. Bu ilkeyle, aynı durumda bulunan kimi kişi ve topluluklara ayrı kurallar uygulanarak kanun karşısında eşitliğin ihlâli yasaklanmıştır. Kanun önünde eşitlik, herkesin her yönden aynı kurallara bağlı tutulacağı anlamına gelmez. Durumlarındaki özellikler, kimi kişiler ya da topluluklar için değişik kuralları ve uygulamaları gerektirebilir. Aynı hukuksal durumlar aynı, ayrı hukuksal durumlar farklı kurallara bağlı tutulursa Anayasa'da öngörülen eşitlik ilkesi zedelenmez.

14. Anayasa'nın 59. maddesinin birinci fıkrasına göre, "Devlet, her yaştaki Türk vatandaşlarının beden ve ruh sağlığını geliştirecek tedbirleri alır, sporun kitlelere yayılmasını teşvik eder." Bu maddenin gerekçesinde de "Sporun geliştirilmesi sadece fiilen spor yapanlara değil, seyircileri için de eğitici ve sağlık kurallarına uygun bir ortamda yaşamaya sevk edici etkileri sebebiyle Devletçe ele alınması için bir başka sebeptir." denilmektedir. Bu düzenlemeye göre vatandaşlarını spora teşvik etmek ve ona uygun olarak vatandaşların ihtiyaçlarını karşılayacak her türlü yatırımı ve altyapıyı hazırlamak Devletin pozitif yükümlülükleri arasındadır. Ancak kamu düzeninin sağlanmadığı bir ortamda, hak ve özgürlüklerden gereği gibi yararlanılması mümkün değildir. Dolayısıyla, Devletin vatandaşlarını spora teşvik etme ve ona uygun olarak vatandaşların ihtiyaçlarını karşılama yükümlülüğünün yanında kamu düzenini sağlama görevi de bulunmaktadır. Bu nedenle, sporda şiddetin ve suç işlenmesinin önlenmesi amacıyla çeşitli tedbirler almak, Anayasa'nın 59. maddesiyle Devlete yüklenen yükümlülüğün bir gereğidir.

15. Yasamanın genelliği ilkesi gereğince Anayasa'da düzenlenmemiş bir alanın kanun koyucunun takdirine bırakıldığı, Anayasa'nın temel ilkeleri ile yasaklayıcı hükümlerine aykırı olmamak kaydıyla, bu konudaki tercihin kanun koyucunun takdiri kapsamında kaldığı kabul edilmelidir. Spor müsabakalarına giriş ve çıkışların kontrolü ve bilet basım, satış ve dağıtımına ilişkin olarak Anayasa'da bir düzenleme bulunmamaktadır. Anayasa'da düzenlenmeyen bir konunun öngörülebilir ve uygulanabilir şekilde kanunla düzenlenmesi kanun koyucunun takdirindedir. Bunun yanında hukuk devletinde, ülkenin sosyal, kültürel yapısı, etik değerleri ve ekonomik hayatın

gerekleri dikkate alınarak ceza siyasetini, idari yaptırımları, kamu düzeninin sağlanması için alınacak idari önlemleri belirleme yetkisi de kanun koyucuya aittir. Kanun koyucu, kendisine tanınan takdir yetkisini anayasal sınırlar içinde kullanarak ve adalet, hakkaniyet ve kamu yararı ölçütlerini gözönünde tutarak çeşitli düzenlemeler yapabilir.

16. Anayasa Mahkemesince "kamu yararı" konusunda yapılacak inceleme, kanunun kamu yararı amacıyla yapılıp yapılmadığının araştırılmasıyla sınırlıdır. Anayasa'nın çeşitli hükümlerinde yer alan kamu yararı kavramının Anayasa'da bir tanımı yapılmamıştır. Ancak Anayasa Mahkemesinin kararlarında da belirtildiği gibi, kamu yararı, bireysel, özel çıkarlardan ayrı ve bunlara üstün olan toplumsal yarardır. Kamu yararı düşüncesi olmaksızın, yalnız özel çıkarlar için veya yalnız belli kişilerin yararına olarak kanun hükmü konulamaz. Böyle bir durumun açık bir biçimde ve kesin olarak saptanması halinde, söz konusu kanun hükmü Anayasa'nın 2. maddesine aykırı düşer. Açıklanan ayrık hâl dışında, bir kanun hükmünün ülke gereksinimlerine uygun olup olmadığı ve hangi araç ve yöntemlerle kamu yararının sağlanabileceği bir siyasî tercih sorunu olarak kanun koyucunun takdirinde olduğundan, bu kapsamda kamu yararı değerlendirmesi yapmak anayasa yargısıyla bağdaşmaz.

17. Kanun koyucunun, kamu düzeni ve güvenliği açısından büyük önem arz eden sporda şiddetin önlenmesi için tedbir alabileceği de kuşkusuzdur. Nitekim gerekçesine bakıldığında itiraz konusu kuralların, kamu düzenini korumak, toplumun, refah, huzur ve mutluluğunu etkileyen sporda şiddetin önlenmesini sağlamak, dolayısıyla kişilerin can ve mal güvenliğini de korumak amacıyla öngörüldüğü anlaşılmaktadır. Bu sebeple anılan düzenlemelerin anayasal sınırlar içinde kanun koyucunun takdirinde olduğu açıktır.

18. Kanun koyucu, itiraz konusu kurallarla Anayasa'nın 59. maddesinin öngördüğü yükümlülük nedeniyle sportif faaliyetlerde gerçekleşen şiddetin toplum üzerinde oluşturduğu tehlikeyi ve sportif faaliyetlerde işlenen suçlardaki artışı dikkate alarak elektronik kart uygulamasını tercih etmiştir. Böylece bilet satın almak isteyenler için üzerinde adı, soyadı, Türkiye Cumhuriyeti kimlik numarası ve fotoğrafının olduğu bir elektronik kart oluşturulacak, bilet almak isteyen kişinin yabancı olması hâlinde elektronik kartın üzerine Türkiye Cumhuriyeti kimlik numarası yerine uyruğu olduğu devletin adı ile pasaportunun seri numarası yazılacak, bilet satışları sadece elektronik kart üzerinden yapılabilecek ve spor müsabakasına kişi ancak adına düzenlenmiş elektronik kart ile girebilecektir. Bilet organizasyonu, seyircilerin müsabakalara giriş ve çıkış kontrolleri ilgili federasyonlarca gerçekleştirilecektir. Ayrıca belirtilen kart ve biletlerin basım, satış ve dağıtımına ilişkin yerel uygulamalar kulüplerce; sistem üzerinden merkezi satışlar ise ilgili federasyonlarca yapılacaktır.

Uygulama ile harici bilet satışı ya da taraftar gruplarına toplu bilet temini mümkün olmayacak, bir kişi ancak kendi adına düzenlenmiş kart ile müsabakalara girebileceğinden yasaklanan kişilerin başkasına ait bilet ile müsabakalara girmeleri engellenebilecektir. Üstelik kart ve bilet satışı ile kontroller ilgili federasyonlar tarafından gerçekleştirilecektir. Böylece elektronik kart ve bilet satışı ile denetimler, uygulamanın düzenli ve kurallara uygun olmasını, her alanda yeknesaklığın sağlanabilmesini temin edecektir. Ayrıca, güvenliğin yanında vergisel olarak mali denetim de daha kolay yapılabilecektir.

19. Elektronik kart ve bilet uygulaması ile bu kapsamda biletlerin basımı, satışı ve dağıtımlarına ilişkin olarak kulüplere verilen görevler ve biletlerin merkezi satışları ile bilet organizasyonu ve seyircilerin müsabaka alanlarına giriş ve çıkışlarının kontrol ve denetimi federasyonlara verilen görevlerin, gelişen, büyüyen, çeşitlenen ve çoğalan, zamanında ve etkin tedbir alınmadığı takdirde engellenmesi daha da güçleşecek olan sporda şiddet sorununu çözüme ve sporseverlerin kurallara uymalarını sağlama amacı için gerekli ve elverişli olmadığı söylenemez. Dolayısıyla bu uygulama ile sporda şiddetin önlenmesine katkı sağlanabileceğinden, söz konusu düzenlemelerin toplumu oluşturan bireylerin can ve mal güvenliğini temin etmek, kamu düzenini ve güvenliğini sağlamak için kamu yararı amacıyla yapıldığı sonucuna da ulaşılmaktadır.

20. Öte yandan sportif müsabakaları izleyecek olanların faaliyetlerini engelleyecek, sınırlayacak nitelikte bir uygulama olmayan, günümüz teknolojisine uygun olarak bilet yüklenmesini ve denetimini kolaylaştıran, tüm spor müsabakalarında aynı kuralların uygulanması sonucu bütünlüğü sağlayan, içerisinde güvenlik amaçlı sınırlı sayıda bilgi barındıran elektronik kart uygulamasının getirilmesi ile daha önce kullanılan basılı bilet kullanılarak gerçekleştirilen uygulama arasında ulaşılmak istenen amaç bakımından bir orantısızlık olduğundan da söz edilemez.

21. Diğer taraftan başvuru kararında, elektronik bilet uygulamasının sadece futbol müsabakalarında ve bu branşın süper lig ve birinci liginde uygulanmakta olduğu, diğer spor dallarında uygulanmamasının eşitlik ilkesine aykırı olduğu belirtilmiştir. Oysa, spor alanlarının güvenlik ve düzeninin sağlanması kapsamında Kanun'un 5. maddesinin (4) numaralı fıkrasında branş ayrımı olmaksızın tüm spor müsabakalarının yapıldığı alanlara girişi sağlamak üzere elektronik kart ve bilet uygulaması öngörülmüştür. Bu nedenle, itiraz konusu kurallar sadece futbol ile sınırlı olmayıp diğer spor dallarındaki müsabakalar için de geçerlidir. Ayrıca reşit olmayanlar ile kısıtlı olanlar yönünden kuralların eşitlik ilkesine aykırı olduğu ileri sürülmüş ise de kurallarda bu kişilere ilişkin özel bir düzenleme bulunmadığı, belirtilen hususun bu kişilerin hak ve fiil ehliyetine yönelik düzenlemeler

içeren diğer hukuk kurallarının uygulanmasından ibaret olduğu anlaşılmaktadır. Dolayısıyla, itiraz konusu kuralların eşitlik ilkesini düzenleyen Anayasa'nın 10. maddesine aykırı olduğu söylenemez.

22. Açıklanan nedenlerle itiraz konusu kurallar, Anayasa'nın 2., 10. ve 59. maddelerine aykırı değildir. İptal taleplerinin reddi gerekir.

23. Serdar ÖZGÜLDÜR bu görüşe katılmamıştır.

24. Kuralın Anayasa'nın 17. ve 20. maddeleriyle ilgisi görülmemiştir.

C- Kanun'un 5. Maddesinin (11) Numaralı Fıkrasının Kalan Kısımlarının İncelenmesi

1- İtirazın Gerekçesi

25. Elektronik kart uygulamasının reşit-reşit olmayan ya da kısıtlı-kısıtlı olmayan ayrımı olmaksızın tüm elektronik bilet alanların özel hayat ve aile hayatının gizliliğini ihlal ettiği, şiddeti önlemek amacıyla getirilen ve kişisel verileri içeren elektronik kart bilgilerinin kulüpler adına reklam ve pazarlanmasında federasyonlara yetki verilmesinin, elektronik kartı ve elektronik kart uygulamasını ticari bir meta haline getirdiği, spordan gelir elde edenlerin elektronik kart uygulaması ile gelir kaybına uğrayacakları, insanların doğrudan harcama ile ulaşmaları gereken alana kart zorunluluğu nedeniyle kısıtlanarak ulaşabilmelerinin hak ihlali olduğu, Devletin yükümlülüğü gereği spora ulaşım engel olan unsurları ortadan kaldırması gerektiği belirtilerek kuralların, Anayasa'nın 17., 20. ve 59. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

a- (11) Numaralı Fıkranın (a) Bendinin İkinci ve Üçüncü Cümlelerinin İncelenmesi

26. 6216 sayılı Kanun'un 43. maddesine göre, itiraz konusu kurallar ilgileri nedeniyle Anayasa'nın 2. ve 13. maddeleri yönünden de incelenmiştir.

27. İtiraz konusu (11) numaralı fıkranın (a) bendinin ikinci cümlesinde, elektronik kart oluşturulması amacıyla alınan kişisel bilgilerin federasyon bünyesinde oluşturulan merkezi veri tabanında tutulacağı, üçüncü cümlesinde ise belirtilen veri tabanının Maliye Bakanlığı ve İçişleri Bakanlığının erişimine açık olacağı öngörülmektedir.

28. Anayasa'nın 20. maddesinin birinci fıkrasında, herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş; üçüncü fıkrasında da "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları

doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." denilerek kişisel verilerin korunması hakkı, özel hayatın gizliliğinin korunması kapsamında anayasal güvenceye kavuşturulmuş ve kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenleneceği belirtilmiştir.

29. Özel hayatın gizliliği kapsamında kişisel verilerin korunması amacıyla Anayasa'nın 20. maddesinde düzenlenen "kişisel verilerin korunması hakkı" mutlak ve sınırsız bir hak olmayıp Anayasa'nın 13. ve 20. maddeleri gereğince hakkın özüne dokunulmaksızın ve demokratik toplum düzeninin gerekleri ile ölçülülük ilkesine aykırı olmamak üzere kanunla sınırlanabilir. Nitekim Türkiye'nin imzaladığı ancak onaylanmasının henüz bir kanunla uygun bulunmadığı ve bu nedenle taraf olamadığı 1981 tarihli ve 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Avrupa Konseyi Sözleşmesi'nin 9. maddesinde de devlet güvenliği, kamu güvenliği, devletin ekonomik menfaatlerinin korunması ve suçlarla mücadele edilmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması ile verilerin istatistikî veya bilimsel amaçlarla kullanılması durumlarında kişisel verilerin korunmasına sınırlamalar getirilebileceği öngörülmüştür.

30. Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır. Kurallarda yer alan merkezi veri tabanında yer alacak bilgiler ilgili kişinin adı, soyadı, Türkiye Cumhuriyeti kimlik numarası ve fotoğrafıdır. Bilet almak isteyen kişinin yabancı olması hâlinde ise üzerinde kimlik numarası yerine uyruğu olduğu devletin adı ile Türkiye'ye giriş yaptığı pasaportunun seri numarası kaydedilecektir. Dolayısıyla elektronik kart üzerinde yer alan bu kişisel verilerin, politik düşünce, dini inanç, sağlık, cinsel yaşam veya ceza mahkûmiyetlerine ilişkin olanlar gibi hassas veri niteliği taşımadığı açıktır.

31. Vatandaşlarının beden ve ruh sağlığını geliştirecek tedbirleri almak ve sporun kitlelere yayılmasını teşvik etmek için sporda şiddetin önlenmesi amacıyla çeşitli tedbirler almanın Anayasa'nın 59. maddesi uyarınca Devlete verilen yükümlülüğün gereği olduğu açıktır. Kanun koyucunun, bu yükümlülüğü gerçekleştirmek üzere getirdiği elektronik kart uygulamasının etkin

olabilmesi için kartta yer alan bilgilerle müsabakaya giren kişilerin bilgilerinin karşılaştırılması amacıyla bilgilerin yer aldığı veri tabanının oluşturulmasının öngörüldüğü anlaşılmaktadır. Bu veri tabanı kullanılarak gerek bilet alanlar gerekse vergi denetimi bakımından bilet içeriği ve bedeli kontrol edilebilir hâle gelebilecektir. Veri tabanı olmaksızın güvenlik kontrolünün gerçekleştirilmesi, buna bağlı olarak da spor müsabakasına girmeleri yasaklananların, müsabaka sırasında suç işleyenlerin tespiti ve haklarında yasal işlem yapılması olanağı azalacağından elektronik kart ve bilet uygulaması ile ulaşılmak istenilen amaç gerçekleşmeyebilecektir. Dolayısıyla sınırlı sayıdaki kişisel verinin, kamu güvenliği, sportif faaliyetlere katılanların hak ve özgürlüklerinin korunması; suçların önlenmesi, araştırılması, soruşturulması ve kovuşturulması, ülkenin ekonomik veya mali çıkarının korunması amacıyla tutulduğu anlaşılmaktadır. Ayrıca kuralların amaçlarına ve gerekçelerine bakıldığında kanun koyucunun elektronik kart uygulamasını içeren itiraz konusu kuralları, sporda şiddetin önlenmesine katkı sağlayabileceğini düşünerek toplumu oluşturan bireylerin can ve mal güvenliğini temin etmek, kamu düzenini ve güvenliğini sağlamak, vergi kaçırılmasını engellemek için kamu yararı amacıyla düzenlediği sonucuna ulaşılmaktadır. Bu bağlamda federasyonların bünyesinde ortak veri tabanının bulunmasının, elektronik kart uygulaması ile ulaşılmak istenilen amaçları gerçekleştirmek için zorunlu olduğu anlaşılmaktadır.

32. Diğer taraftan spor federasyonları, teknik ve idari bakımdan bir veya birden fazla spor dalının bağlı olduğu, spor dalı ile ilgili faaliyetleri ulusal ve uluslararası kurallara göre yürütmek, gelişmesini sağlamak, sporcu sağlığı ile ilgili konularda gerekli önlemleri almak, teşkilatlandırmak ve Tahkim Kurulu kararlarını uygulamakla görevli ve yetkili, özel hukuk hükümlerine tabi kuruluşlardır. Dolayısıyla veri tabanının, görevleri arasında ilgili spor dalında organizasyon ve birlikteliğin sağlanması bulunan federasyonların bünyesinde tutulması federasyonların işlevlerinin bir gereğidir.

33. Anayasa'nın 2. maddesinde belirtilen hukuk devletinin ön koşulları arasında hukuki güvenlik ile belirlilik ilkeleri bulunmaktadır. Kişilerin hukuki güvenliğini sağlamayı amaçlayan hukuki güvenlik ilkesi, hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar. Belirlilik ilkesi ise yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olmasını, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesini ifade etmektedir. Belirtilen ilkeler doğrultusunda temin edilecek kişisel verilerin neden ve hangi gerekçeyle temin edileceğine ilişkin olarak konu ve amaç sınırlamasının yapılması suretiyle bu verilerin kapsamının ve ne şekilde kullanılacağına belirli olması gerekmektedir.

34. Söz konusu veriler, gerek kamu güvenliğinin gerekse vergi denetiminin sağlanması bakımından tutulmaktadır. Söz konusu veri tabanının, vatandaşların çok daha ayrıntılı ve hassas verilerinin bulunduğu Maliye ve İçişleri Bakanlıklarının erişimine açılması veri güvenliği açısından sorun teşkil etmez. Elektronik kart almak isteyenlerin başvuruları sonucu elde edilen verilerin amaç ve kapsam dışında depolanması ve kullanılması hâlinde, 5237 sayılı Türk Ceza Kanunu'ndaki kişisel verilerin korunmasına ilişkin ceza hükümlerinin uygulanacak olması nedeniyle bu konuda kanuni güvence de bulunmaktadır. Belirtilen amaçlarla sınırlı olarak ve spor müsabakalarının güvenli bir biçimde gerçekleştirilmesini sağlamaya yönelik olarak tutulan bu verilerin, temin edilme sebebine ilişkin olarak konu, amaç sınırlaması ve bu verilerin kapsamı ile kullanılma şekline dair bir belirsizlik bulunmadığından söz konusu kurallar hukuki güvenlik ilkesine aykırılık teşkil etmez.

35. İtiraz konusu kurallar, sporda şiddetin önlenmesi, kamu düzeninin ve güvenliğinin sağlanması, bireylerin can ve mal güvenliğinin temin edilmesi, vergi kaçırılmasını engellemek gibi demokratik toplum düzeni yönünden zorlayıcı toplumsal ihtiyaçları karşılamaya yöneliktir. Kurallar ile özel hayatın ve kişisel verilerin korunması haklarına bir sınırlama getirilmiş ise de bu sınırlandırma Anayasa ile Devlete yüklenen demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır. Ayrıca öngörülen sınırlandırma için kullanılan araç, hak ve özgürlüğü en az sınırlayacak, amaca uygun dengeli bir orantı oluşturmakta, kamu düzeni ve güvenliğinin korunması şeklindeki kamu yararı ile kişisel verilerin korunması hakkı arasında makul denge kurmaktadır. Dolayısıyla sınırlamanın, ölçülülük ve demokratik toplum düzeninin gereklerine aykırılık teşkil ettiği söylenemez.

36. Açıklanan nedenlerle itiraz konusu kural, Anayasa'nın 2., 13., 20. ve 59. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

37. Kuralın Anayasa'nın 17. maddesiyle ilgisi görülmemiştir.

38. Serdar ÖZGÜLDÜR ve Engin YILDIRIM (11) numaralı fıkranın (a) bendinin ikinci ve üçüncü cümleleri yönünden, Osman Alifeyyaz PAKSÜT ve Alparslan ALTAN ise (11) numaralı fıkranın (a) bendinin üçüncü cümlesi yönünden bu görüşe katılmamışlardır.

b- Kanun'un 5. Maddesinin (11) Numaralı Fıkrasının (c) Bendinin Birinci Cümlesinin İncelenmesi

39. 6216 sayılı Kanun'un 43. maddesine göre, itiraz konusu kural ilgisi nedeniyle Anayasa'nın 13. maddesi yönünden de incelenmiştir.

40. Kanun'un 5. maddesinin (11) numaralı fıkrasının (c) bendinin itiraz konusu birinci cümlesi, elektronik kart bilgilerinin kulüpler adına reklam ve pazarlamasında ilgili federasyonların yetkili

olmasını öngörmektedir. Reklam ve pazarlaması yapılabilecek olan bilgiler, (4) numaralı fıkranın ikinci cümlesi uyarınca kişinin adı, soyadı, Türkiye Cumhuriyeti kimlik numarası, fotoğrafı, kişinin yabancı olması durumunda kimlik numarası yerine uyruğu olduğu devletin adı ile Türkiye'ye giriş yaptığı pasaportunun seri numarasıdır. Dolayısıyla kulüpler adına reklam ve pazarlanması mümkün olan bilgiler kişisel verilerdir.

41. Anayasa'nın 13. maddesinde, temel hak ve hürriyetlerin, özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği, bu sınırlamaların Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamayacağı belirtilmiştir. Ölçülülük amaç ve araç arasında hakkaniyete uygun bir denge bulunması gereğini ifade eder. Ölçülülük, aynı zamanda yasal önlemin sınırlama amacına ulaşmaya elverişli olmasını, amaç ve aracın ölçülü bir oranı kapsamasını ve sınırlayıcı önlemin demokratik toplum düzeni bakımından zorunluluk taşımasını da içeren bir ilkedir.

42. Anayasa'nın 20. maddesinin gerekçesinde de belirtildiği üzere özel hayatın korunması her şeyden önce bu hayatın gizliliğinin korunması, başkalarının gözleri önüne serilmemesi demektir. Kişinin özel hayatında yaşananların, yalnız kendisi veya kendisinin rıza gösterdiği kimseler tarafından bilinmesini isteme hakkı, kişinin temel haklarından biridir ve bu niteliği nedeniyle insan haklarına ilişkin beyanname ve sözleşmelerde yer almış, tüm demokratik ülkelerin mevzuatlarında açıkça belirlenen istisnalar dışında devlete, topluma ve diğer kişilere karşı korunmuştur. Bu koruma bireyin kendisine ilişkin herhangi bir bilginin rızası olmaksızın açıklanmamasını, yayılmamasını, nakledilmemesini ve bu bilgilere başkalarının ulaşamamalarını da kapsamaktadır.

43. Kişisel verilerin ilgili üçüncü kişiler ya da kamu kurum ve kuruluşları ile paylaşılabilmesi için, söz konusu kişi ve kurumların bu verilere erişebilme hususunda kanunen yetkilendirilmiş olmaları ve bu verilerin ilgili kurum ve kişilerin görevlerini yapması için gerekli olmasının yanı sıra bu görevlerin yerine getirilmesi ile de sınırlı olması gerekir. Bu bağlamda sportif faaliyetleri izlemek isteyenlerin kişisel verilerinin de sadece Kanun'da öngörülen amaçla ve bu kayıtların hizmetin devamı için zorunlu olduğu müddetle sınırlı olarak tutulması zorunludur. Kişisel verilere ilişkin kuralların aynı zamanda kişisel veri niteliğindeki bilgilerin teminine, kullanılabilmesine, işlenebilmesine, ulaşılabilmesine, saklanma süresine, temin edilme gerekçesine ilişkin hususlarda bir belirlilik içermesi gerekmektedir. Diğer taraftan kuralın objektif olarak amaçlanan kamu yararını gerçekleştirmeye elverişli ve bu amacın gerçekleştirilmesi için zorunlu olması gerekir.

44. İtiraz konusu kural uyarınca kişisel veriler, ilgili federasyon tarafından kulüpler adına reklam ve pazarlamada kullanılabilir. Böylece spor müsabakalarını izlemek amacıyla verilen kişisel

verilerin üçüncü kişilere aktarılması olanaklı hâle gelmektedir. Ancak kişisel verilerin elektronik kart almak üzere verilmiş olması, söz konusu verilerin üçüncü kişilere aktarımına rıza gösterildiği anlamına gelmez. Dolayısıyla Anayasa'nın 20. maddesinde kişisel verilerin "ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği"nin açıkça ifade edilmesi karşısında, kişisel veri niteliğinde bulunan elektronik kart bilgilerinin, ilgili kişilerin rızaları alınmaksızın, federasyon tarafından reklam ve pazarlama amacıyla üçüncü kişilere verilmesi sonucuna yol açan kuralın özel hayatın ve kişisel verilerin korunması haklarına bir sınırlama getirdiği açıktır.

45. Öte yandan demokratik toplum düzeninin oluşturulması, korunması ve geliştirilmesi açısından, sportif faaliyetlerde yaşanan şiddet önlenirken bireylerin haklarının ölçüsüz şekilde sınırlandırılmaması için gerekli özenin gösterilmesi hayati öneme sahiptir. Ancak kişisel verilerin rıza olmaksızın üçüncü kişilere aktarımı sonucunu doğuracak şekilde elektronik kart bilgilerinin kulüpler adına reklam ve pazarlamasında ilgili federasyonların yetkili kılınmasının, sporda şiddetin önlenmesi için demokratik toplum düzeni bakımından alınması gereken tedbirlerden olduğu söylenemez. Aynı zamanda söz konusu yetkinin federasyona verilmesi suretiyle özel hayatın ve kişisel verilerin korunması haklarına getirilen sınırlandırma, sportif faaliyetlerde yaşanan şiddeti önleme amacını gerçekleştirmeye elverişli de değildir. Dolayısıyla belirtilen amaç için gerekli ve elverişli olmayan kuralın, ölçülülük ilkesine uygun olmadığı açıktır.

46. Açıklanan nedenlerle, itiraz konusu kural Anayasa'nın 13. ve 20. maddelerine aykırıdır. İptali gerekir.

47. Kurallar, Anayasa'nın 13. ve 20. maddelerine aykırı bulunarak iptal edildiğinden, Anayasa'nın 17. ve 59. maddeleri yönünden ayrıca incelenmesine gerek görülmemiştir.

c- Kanun'un 5. Maddesinin (11) Numaralı Fıkrasının (c) Bendinin Üçüncü Cümlesinin İncelenmesi

48. 6216 sayılı Kanun'un 43. maddesine göre, itiraz konusu kural ilgisi nedeniyle Anayasa'nın 13. maddesi yönünden de incelenmiştir.

49. Kanun'un 5. maddesinin (11) numaralı fıkrasının (c) bendinin itiraz konusu üçüncü cümlesi, federasyonların fıkra kapsamındaki yetkilerini kısmen ya da tamamen üçüncü kişilere devredebileceğini öngörmektedir. Üçüncü kişilere kısmen ya da tamamen devredilebilecek yetkiler şunlardır:

a- Bilet organizasyonu ve seyircilerin müsabaka alanlarına giriş ve çıkışına ilişkin kontrolü ve denetimi yapmak ile bu amaçla merkezi kontrol sistemi oluşturulması,

b- Elektronik kart oluşturmak amacıyla alınan kişisel bilgilerin merkezi veri tabanında tutulması,

- c- Elektronik kart ve elektronik kart kapsamında satışı gerçekleştirilecek biletlerin basım, satış ve dağıtımına ilişkin sistem üzerinden merkezi satışlar gerçekleştirilmesi,
- d- Elektronik kart bilgilerinin kulüpler adına reklam ve pazarlanması.

50. Yasamanın genelliği ilkesi gereğince Anayasa'da düzenlenmemiş bir alanın, Anayasa'nın temel ilkeleri ile yasaklayıcı hükümlerine aykırı olmamak kaydıyla öngörülebilir ve uygulanabilir şekilde kanunla düzenlenmesi kanun koyucunun takdirinde olup kanun koyucu, kendisine tanınan takdir yetkisi çerçevesinde düzenlemeler yapabilir. Spor müsabakalarına giriş, girişlerin kontrolü, bilet basım, satış ve dağıtımına ilişkin olarak da Anayasa'da bir düzenleme bulunmamaktadır.

51. Kuralda devredilmesi öngörülen bilet organizasyonu ve seyircilerin müsabaka alanlarına giriş ve çıkışına ilişkin kontrol ve denetim yetkisi ile bu amaçla merkezi kontrol sistemi oluşturma ve elektronik kart ve elektronik kart kapsamında satışı gerçekleştirilecek biletlerin basım, satış ve dağıtımına ilişkin sistem üzerinden merkezi satışlar gerçekleştirme yetkisi, Devletin, kamu iktisadî teşebbüslerinin ve diğer kamu tüzelkişilerinin genel idare esaslarına göre yürütmekle yükümlü oldukları kamu hizmetlerinden değildir. Bu nedenle belirtilen bu görevlerin özel hukuk tüzel kişilerin yerine getirilmesi mümkündür. Spor federasyonları da özel hukuk hükümlerine tabi bağımsız nitelikte kuruluşlardır. Dolayısıyla tamamen özel hukuk alanında kalan, genel idare esaslarına göre yürütülmesi zorunlu olan kamu hizmetlerinin gerektirdiği asli ve sürekli görev niteliği taşımayan görevlerin idarece yerine getirilme zorunluluğu olmadığı gibi bizatihi federasyonlar eliyle yürütülmesi de gerekmemektedir. Söz konusu yetkilerin devri, Devlete verilen yükümlülükleri öngören Anayasa'nın 59. maddesine aykırılık oluşturmadığı gibi özel hayatın ve kişisel verilerin korunması hakkını engelleyecek bir nitelik de taşımamaktadır. Bu nedenle kuralın belirtilen görev dolayısıyla federasyonlara tanınan yetkinin devredilebilmesine olanak sağlamasında Anayasa'ya aykırılık bulunmamaktadır.

52. Elektronik kart bilgilerinin kulüpler adına reklam ve pazarlanması yetkisinin ilgili federasyonlara verilmesini öngören (11) numaralı fıkrasının (c) bendinin birinci cümlesi Anayasa'ya aykırı bulunarak iptal edildiğinden belirtilen bu yetkinin üçüncü kişilere devrinin Anayasa'ya uygunluğunun ayrıca incelenmesine gerek görülmemiştir.

53. Öte yandan üçüncü kişilere devredilebilecek yetkiler arasında elektronik kart oluşturmak amacıyla alınan kişisel bilgileri merkezi veri tabanında tutmak da bulunmaktadır. Bu yetki uyarınca sportif faaliyetleri izlemek isteyenlerin kişisel verilerin bulunduğu veri tabanı ilgili federasyon tarafından üçüncü kişilere devredilebilecektir. Üstelik bu işlem için kişisel veri sahibi ilgilinin veri paylaşımına rızasının bulunması koşulu da aranmamaktadır. Ayrıca kişisel veri tabanının devri

sonrasında kime, hangi amaçlarla aktarılacağı konusunda da denetim imkânı öngörülmemiştir. Diğer anlatımla kural, kötüye kullanım olasılığını engelleyici etkili ve yeterli tedbirlere de yer vermemektedir. Bu durum kuralı öngörülme amacının ötesinde kişisel bilgilerin gizliliğinin keyfi şekilde ihlal edilmesi sonucunu doğurabilecek bir araca dönüştürmektedir.

54. İptali istenilen düzenlemenin temel amacının sporda şiddeti önlemek ve bu şekilde kamu düzeni ve güvenliğini korumak olduğu görülmektedir. Bu meşru amaç için öngörülen düzenleme uyarınca gerçekleştirilen veri tabanının üçüncü kişilere devrinin özel hayatın ve kişisel verilerin korunması hakkını sınırlandırdığı açıktır. Ancak kişisel verilerin üçüncü kişilere devri sonucu gerçekleşecek bu sınırlandırmanın elektronik kart ve bilet uygulaması ile gerçekleştirilmek istenilen sporda şiddetin önlenmesine hiçbir katkısı bulunmamaktadır. Hakkı sınırlayan düzenlemeyle, ilgili federasyona, ihtiyaç duyulandan çok daha geniş bir yetki verilmektedir. Bu durum sınırlama aracıyla sınırlama amacı arasında bulunması gereken makul dengeyi bozmakta, özel hayatın ve kişisel verilerin korunmasını isteme haklarına kuralda belirtilen sınırlama amacı dışında ölçsüz bir şekilde müdahale edilebilmesine imkân tanımaktadır. Öte yandan, temel hak ve hürriyetlere getirilen sınırlamaların, demokratik toplum düzeni bakımından zorlayıcı bir toplumsal ihtiyaçtan kaynaklanması gerekmektedir. İtiraz konusu kuralla, özel hayatın gizliliğine ve kişisel verilerin korunması hakkına sınırlama getirilirken sınırlama aracının sınırlama amacına uygun ve orantılı olarak kullanılmasını temin edecek güvencelere yer verilmemesi demokratik toplum düzeninde gerekli olmayan ölçsüz bir sınırlama niteliğindedir.

55. Açıklanan nedenlerle itiraz konusu kural, (11) numaralı fıkranın (a) bendinin ikinci cümlesi yönünden Anayasa'nın 13., 20. ve 59. maddelerine aykırıdır. Kuralın bu cümle ile federasyona verilen yetkinin üçüncü kişilere devri yönünden iptali gerekir.

56. Kural, (11) numaralı fıkranın (a) bendinin ikinci cümlesi dışındaki hükümler yönünden ise Anayasa'nın 13., 20. ve 59. maddelerine aykırı değildir. Belirtilen hükümlerle federasyonlara verilen yetkilerin üçüncü kişilere devri yönünden iptal talebinin reddi gerekir.

57. Serdar ÖZGÜLDÜR, kuralın iptaline ilişkin görüşe farklı gerekçeyle katılmış, iptal talebinin reddine ilişkin görüşe ise katılmamıştır.

58. Kuralın Anayasa'nın 17. maddesiyle ilgisi görülmemiştir.

IV- HÜKÜM

31.3.2011 tarihli ve 6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun'un 5. maddesinin;

A- (11) numaralı fıkrasının (c) bendinin ikinci cümlesinin, itiraz başvurusunda bulunan Mahkemenin bakmakta olduğu davada uygulanma olanağı bulunmadığından, bu cümleye ilişkin başvurunun Mahkemenin yetkisizliği nedeniyle REDDİNE, OYBİRLİĞİYLE,

B- (4) numaralı fıkrasının ikinci, üçüncü, dördüncü ve beşinci cümlelerinin Anayasa'ya aykırı olmadıklarına ve itirazın REDDİNE, Serdar ÖZGÜLDÜR'ün karşıoyu ve OYÇOKLUĞUYLA,

C- (11) numaralı fıkrasının;

1- (a) bendinin;

a- Birinci cümlesinin Anayasa'ya aykırı olmadığına ve itirazın REDDİNE, Serdar ÖZGÜLDÜR'ün karşıoyu ve OYÇOKLUĞUYLA,

b- İkinci cümlesinin Anayasa'ya aykırı olmadığına ve itirazın REDDİNE, Engin YILDIRIM ile Serdar ÖZGÜLDÜR'ün karşıoyları ve OYÇOKLUĞUYLA,

c- Üçüncü cümlesinin Anayasa'ya aykırı olmadığına ve itirazın REDDİNE, Engin YILDIRIM, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT ile Alparslan ALTAN'ın karşıoyları ve OYÇOKLUĞUYLA,

2- (b) bendinin Anayasa'ya aykırı olmadığına ve itirazın REDDİNE, Serdar ÖZGÜLDÜR'ün karşıoyu ve OYÇOKLUĞUYLA,

3- (c) bendinin;

a- Birinci cümlesinin Anayasa'ya aykırı olduğuna ve İPTALİNE, OYBİRLİĞİYLE,

b- Üçüncü cümlesinin;

ba- (11) numaralı fıkranın (a) bendinin ikinci cümlesi yönünden Anayasa'ya aykırı olduğuna ve İPTALİNE, OYBİRLİĞİYLE,

bb- (11) numaralı fıkranın (a) bendinin ikinci cümlesi dışındaki hükümler yönünden Anayasa'ya aykırı olmadığına ve itirazın REDDİNE, Serdar ÖZGÜLDÜR'ün karşıoyu ve OYÇOKLUĞUYLA,

12.11.2015 tarihinde karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili - Burhan ÜSTÜN

Başkanvekili - Engin YILDIRIM

Üye: Serdar ÖZGÜLDÜR; Serruh KALELİ; Osman Alifeyyaz PAKSÜT; Recep KÖMÜRCÜ; Alparslan ALTAN; Nuri NECİPOĞLU; Hicabi DURSUN; Celal Mümtaz AKINCI; Erdal TERCAN; Muammer TOPAL; M. Emin KUZ; Hasan Tahsin GÖKCAN; Kadir ÖZKAYA; Rıdvan GÜLEÇ

KARŞIOY GÖRÜŞÜ

6222 sayılı Kanun'un 11. maddesinin (a) fıkrasında "...Elektronik kart oluşturulmak amacıyla alınacak kişisel bilgiler federasyon bünyesinde oluşturulan merkezi veri tabanında tutulur. Bu veri tabanı Maliye Bakanlığı ve İçişleri Bakanlığı erişimine açıktır" düzenlemesi yer almaktadır.

1981 tarihli ve 108 sayılı, Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Avrupa Konseyi Sözleşmesi'nin 2. maddesi, kişisel veriyi belirli veya belirlenebilir bir kişiye ait tüm bilgiler şeklinde tanımlamaktadır. Anayasa Mahkemesi de bu tanımlı çeşitli kararlarında benimsemiştir. Elektronik kartta bilet satın almak isteyen kişilerin adı, soyadı, T.C. kimlik numarası ve fotoğrafı bulunmaktadır. Bu tür veriler Anayasa Mahkemesinin E.2013/122, K.2014/74 sayılı kararında da belirtildiği gibi kişisel veri kapsamındadır.

Kişisel verilerin toplanması ve işlenmesinde dikkat edilmesi gereken en önemli hususlardan biri verilerin amacın gerektirdiğinden daha uzun bir süre tutulmamasıdır. Ülkemizde kişisel verilerin korunmasını denetleyecek bağımsız bir kurul ya da devlet kuruluşu bulunmamaktadır. Kişisel verilerin korunması ancak dava yoluyla gerçekleştirilebilmektedir. Kişisel verilerin korunması kişinin maddi ve manevi varlığını geliştirmesine imkân tanıyarak, bireyin hayatını kendi özgür iradesiyle düzenlemesine katkı sağlamaktadır. Bireyin kişisel verileri üzerindeki hakkı yeteri kadar korunmazsa, kişiliğini serbestçe geliştirmesi zora gireceğinden, özgür iradeleriyle yaşamlarını biçimlendiren bireylerden oluşan demokratik bir toplum düzeninin ortaya çıkması ve korunması da güçleşecektir. Kişisel verilerin korunmasıyla, kişisel veri toplanması, saklanması ve işlenmesi sırasında bireyin hak ve özgürlüklerinin korunarak demokratik toplum düzeninin oluşmasına katkı yapmak hedeflenmektedir. Anayasa'nın 20. maddesinin son fıkrası çok açık bir şekilde kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceğini hüküm altına almakla birlikte ülkemizde kişisel verilerin korunmasını düzenleyen çerçeve bir kanun bulunmamaktadır.

İtiraz konusu kural uyarınca ilgili federasyonlar bünyesinde elektronik kart üzerinde yer alan bilgilerin yer alacağı bir merkezi veri tabanı oluşturulacaktır. (Somut olarak TFF tarafından oluşturulmuştur.) Bu veri tabanı da İçişleri ve Maliye Bakanlıklarının erişimine açık olacaktır. Dolayısıyla belirtilen bilgilere ulaşılması bu bakanlıklar yönünden mümkün hâle gelmektedir. Bu

durumda kişilerin özel hayatlarına müdahale olduğu açıktır. Kişisel verilerin tutulduğu veri tabanının Maliye ve İçişleri Bakanlıklarının denetimine açılması vergi denetimi ve kamu güvenliği gibi meşru amaçlar taşısa bile demokratik toplum düzeninin gerekleri açısından herhangi bir acil ve baskın toplumsal ihtiyaca denk gelmemektedir.

Belirtilen nedenlerle itiraz konusu kuralın Anayasa'nın 13. ve 20. maddelerine aykırı olduğu düşüncesiyle, çoğunluk kararına muhalefet edilmiştir.

Başkanvekili - Engin YILDIRIM

KARŞIOY ve FARKLI GEREKÇE

1. "Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun Tasarısı" Türkiye Büyük Millet Meclisi'nce (TBMM) 31.3.2011 tarih ve 6222 sayılı Kanun olarak kabul edilmiş ve 14.4.2011 tarih ve 27905 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir.

Bu Kanunun "Spor alanlarının güvenlik ve düzenine ilişkin tedbirler" başlıklı 5. maddenin (11) numaralı fıkrası anılan Kanun Tasarısı'nda yer almadığı gibi, TBMM Adalet Komisyon'unca kabul edilen metinde de yer almadığı ve TBMM Genel Kurulu'nda verilen bir önergenin kabulüyle kanun metnine eklendiği anlaşılmaktadır.

Anayasa'nın 88. maddesinde "Kanun teklif etmeye Bakanlar Kurulu ve milletvekilleri yetkilidir.

Kanun tasarı ve tekliflerinin Türkiye Büyük Millet Meclisinde görüşülme usul ve esasları İçtüzükle düzenlenir." denilmektedir. Anayasa'nın 88. maddesinin birinci fıkrasının ihlâli sonucu bir yasalaştırma söz konusuysa, bu konudaki ihlâl Anayasa'nın 148. maddesi anlamında bir "şekil sakatlığı"na değil, doğrudan 88. maddesine aykırı düşer ve yapılacak anayasal denetimin, "şekil bakımından" değil, "esas bakımından" söz konusu olması gerekir. 88. maddenin ikinci fıkrasındaki "Kanun tasarı ve tekliflerinin Türkiye Büyük Millet Meclisinde görüşülme usul ve esasları İçtüzükle düzenlenir" hükmünün de, bu açıklama çerçevesinde yorumlanması ve bu düzenlemenin aynı maddenin birinci fıkrasındaki anayasal hüküm doğrultusunda anlaşılması ve hüküm ifade etmesi gerekir. Yani, birinci fıkraya aykırı bir durum söz konusu ise artık ortada doğrudan bir Anayasa ihlâli söz konusu olacak ve Anayasa'nın bu hükmünün bir tekrarından ibaret olan TBMM İçzülüğü'nün 35. maddesinin ihlâli nedeniyle, Anayasa'nın 148. maddesinde belirtilen (ve son oylamaya ilişkin olmadığından kanunun iptalini gerektirmeyen) bir şekil sakatlığından ve şekil denetiminden değil; 88. maddenin birinci fıkrasının ihlâli sonucu esas ilgilendiren bir sakatlıktan ve esas denetimden söz edilebilecektir.

Davanın somutu ile ilgili olarak düzenleme öngören TBMM İÇtüzüğü'nün "Komisyonların yetkisi, toplantı yeri ve zamanı" başlıklı 35. maddesinin ilgili bölümleri şöyledir: "Komisyonlar, kendilerine havale edilen kanun tasarı ve/veya tekliflerini aynen veya değiştirerek kabul veya reddedebilirler; birbirleriyle ilgili gördüklerini birleştirerek görüşebilirler ve Türkiye Büyük Millet Meclisi Başkanlığınca kendilerine ayrılan salonlarda toplanırlar.

Ancak, komisyonlar, 92 nci maddedeki özel durum dışında kanun teklif edemezler, kendilerine havale edilenler dışında kalan işlerle uğraşamazlar. Başkanlık Divanının kararı olmaksızın Genel Kurulun toplantı saatlerinde görüşme yapamazlar ve kanun tasarı ve tekliflerini bölerek ayrı ayrı metinler halinde Genel Kurula sunamazlar."

İÇtüzüğün 35. maddesinin yukarıdaki açık metninden de açıkça anlaşılacağı üzere, komisyonların kendilerine havale edilen kanun tasarı ve tekliflerini görüşme yetkileri sınırlandırılmış olup, komisyonların İÇtüzüğün 92 nci maddesindeki özel durum dışında (genel veya özel af ilanını içeren kanun tasarı ve teklifleri) kanun teklif etme yetkileri yoktur. Yukarıda belirtilen yasa değişiklikleri Bakanlar Kurulunca önerilen Tasarı metninde olmadığı halde TBMM Genel Kurulunda Tasarı metnine ilave edilerek kanunlaştırıldığından; bu durum Anayasa'nın 88. maddesinin birinci fıkrasına (dolayısıyla de bu hükmün açıklaması mahiyetinde bulunan TBMM İÇtüzüğü'nün 35 inci maddesine) açıkça aykırı düşmektedir.

Anayasa'nın 88. maddesinin birinci fıkrasının açık âmir hükmü karşısında, TBMM İÇtüzüğü'nün 87 nci maddesi gerekçe gösterilerek, görüşülmekte olan bir tasarı veya teklifin konusu olmayan "başka" kanunlarda ek ve değişiklik getiren "yeni bir kanun teklifi mahiyetindeki" değişikliklerin "Genel Kurul" tarafından da yapılamayacağı açıktır.

Anayasa'nın 148. maddesindeki "Kanunların şekil bakımından denetlenmesi, son oylamanın, öngörülen çoğunlukla yapılıp yapılmadığı. hususları ile sınırlıdır." hükmünün de bu belirlemeye etkisinin olamayacağı kuşkusuzdur. Gerçekten, 88 nci maddenin birinci fıkrasına açıkça aykırı bir yasama faaliyeti sözkonusu olduğundan, Genel Kurulca öngörülen çoğunlukla yapılacak bir "son oylama"nın belirtilen Anayasa'ya aykırılığı düzeltereği kabul edilemez. Ancak 88 inci maddenin birinci fıkrasına uygun bir yasama faaliyeti içerisinde 148 inci maddedeki "şekil denetimi" kuralı işletilebilir. Davanın somutunda ise yukarıda açıklandığı üzere, aksi yönde bir yasama faaliyeti bulunduğu görüldüğünden; 148 inci maddenin bu davanın somutunda uygulama kabiliyeti bulunmamaktadır. (Bu konudaki bir inceleme için bkz.: Torba Yasalar ve Yasama sürecindeki İÇtüzük Hükümlerinin Şekil Denetimi Sorunu, Hıfzı DEVECİ, TBB Dergisi, 2015 (117) s. 55-90)

Esasen Anayasa Mahkemesinin 25.12.2008 tarih ve E.2008/71, K.2008/183 sayılı kararına (RG 9.4.2009, Sayı:27195) konu iptal davası başvurusunun içeriğinden de, bu şekildeki bir uygulamanın TBMM İktüzüğü'nün 35. maddesine aykırı düştüğünün TBMM Başkanlığınca saptandığı ve ilgili komisyona kabul edilen tasarı metninin iade edilmesine karşılık, ilgili komisyonca iade edilen tasarı metninin yeniden bir üst yazı ile Genel Kurulun onayına sunulmak üzere TBMM Başkanlığına geri gönderildiği ve akabinde yasalaştığı anlaşılmaktadır.

Açıklanan nedenlerle; anılan kuralın Anayasa'nın 88. maddesine aykırı düşmesi nedeniyle iptali gerektiği kanaatine vardığımdan; Kurulca uygulanacak kural olmadığına karar verilen 2. cümle dışındaki fıkranın tamamının bu nedenle iptali gerektiğini değerlendiriyorum.

2. Anayasa'nın "Sporun geliştirilmesi ve tahkim" başlıklı 59. maddesi "Devlet, her yaştaki Türk vatandaşlarının beden ve ruh sağlığını geliştirecek tedbirleri alır, sporun kitlelere yayılmasını teşvik eder." hükmü öngörmekte; anılan maddenin gerekçesinde ise "sağlık hizmetlerinin bir parçası, beden sağlığının spor yaptırarak korunmasıdır. Sporun kitlelere yayılması bu amacın teminine yarayacak araçlardan biridir. Sporun geliştirilmesi sadece fiilen spor yapanlara değil, seyircileri için de eğitici ve sağlıklı uygun bir ortamda yaşamaya sevkedici etkileri sebebiyle Devletçe ele alınması için bir başka sebeptir." denilmektedir.

Yine Anayasa'nın "Özel hayatın gizliliği" başlıklı 20. maddesinin son fıkrasında "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak Kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin usul ve esaslar kanunla düzenlenir." Hükmünü taşımakta; anılan düzenlemenin gerekçesinde de "Anayasada kişisel verilerin korunmasına yönelik dolaylı hükümler bulunmakla birlikte yeterli değildir. Mukayeseli hukukta ve tarafı olduğumuz uluslararası belgelerde ve kişisel verilerin korunması önemle vurgulanmaktadır. Maddeyle, herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı, anayasal bir hak olarak teminat altına alınmaktadır. Bu bağlamda, bireylerin kendilerini ilgilendiren kişisel veriler üzerinde hangi hak ve yetkilere sahip olduğu ve kişisel veriler hangi hallerde işlenebileceği hükme bağlanırken, kişisel verilerin korunmasına ilişkin esas ve usullerin Kanunla düzenleneceği öngörülmektedir." denilmektedir.

Anayasa'nın 20. maddesinin çıkarılmasını öngördüğü kanun ise henüz çıkarılmamıştır. Ancak, örneğin Türk Ceza Kanunu'nun 135-140. maddesinde kişisel verilen hukuka aykırı olarak kaydedilmesi ve işlenmesi halleri suç olarak düzenlenmiş ve yaptırıma bağlanmıştır.

Öte yandan, bir çok uluslararası sözleşmede de kişisel verilerle ilgili düzenlemeler yapılmış ve konunun önemi bu uluslararası metinlere yansımıştır. Örneğin, Türkiye'nin 1981'de imzalamasına karşın henüz onaylamadığı, Avrupa Konseyi'nin 28.1.1981 tarih ve 108 numaralı "Kişisel Nitelikli Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme"nin 6. maddesine göre, iç hukukta uygun güvenceler sağlanmadıkça, ırk menşesini, politik düşünceleri, dini veya diğer inançları ortaya koyan verilerle diğer kişisel nitelikteki veriler, sağlık veya cinsel yaşamla ilgili kişisel nitelikteki veriler ve ceza mahkumiyetleri, otomatik bilgi işlemine tâbi tutulamazlar. Anılan Sözleşme'nin 2. maddesine göre "Kişisel Veri: kimliği belirtilen veya belirtebilen gerçek kişiyle ilgili tüm bilgiler"dir. Kişinin kimlik numarası, fiziksel, psikolojik, duygusal, ekonomik ve kültürel kimliği veya sosyal kimliği, isim, telefon numarası, elektronik posta adresi, doğum tarihi, parmak izi, DNA bilgileri, adresi, sosyal güvenlik numarası gibi bilgiler kişisel veri olarak değerlendirilmektedir. Yine Avrupa Birliği'nin 24 Ekim 1995 tarihli "Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması Yönergesi (95/46/EC)"nde de siyasi, dini felsefi görüşler veya uyuşturucu, alkol bağımlılığı veya sağlık gibi hassas verilerin korunmasına ilişkin düzenlemelere yer verilmiştir. Avrupa İnsan Hakları Mahkemesi de kişilerin fiziki ve sosyal kimlikleri, kişisel bilgileri, cinsiyetleri, şahıslarına ait özerk sahaları, adları, medeni hali, parmak izi, fotoğrafları, fiziki ve sosyal bütünlükleri (sağlık/tıbbi bilgileri), iş ilişkileri, sosyal etkinlikleri, kişisel gelişimi, fiziki ve moral güvenliği, dış çevrede insanlarla ilişkileri gibi hususları, Sözleşme'nin "Özel hayatın ve aile hayatının korunması" başlıklı 8. maddesi kapsamında "özel hayat" kavramı içinde değerlendirmektedir.

Anayasa Mahkemesi de aşağıda işaret edilen kararlarında, söz konusu yasal düzenlemelerin ilgili kurallarını, kişisel verilerin korunmasına ilişkin Anayasa'nın 20. maddesine aykırı bularak iptali yoluna gitmiştir:

- 5429 sayılı Türkiye İstatistik Kurumu Kanunu'nun 8. ve 54/b maddelerinin iptaline dair 20.3.2008 tarih ve E.2006/167, K.2008/86 sayılı karar (R.G. 25.6.2008; Sayı: 26917),
- Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında 663 sayılı Kanun Hükmünde Kararname'nin 16. maddesinin (2) nolu fıkrasının birinci cümlesinde yer alan "gerçek" ve "gizli olsa dahi" ibareleri ile 47. maddesinin (1), (2) ve (3) no'lu fıkralarının iptaline dair 14.2.2013 tarih ve E.2011/150, K.2013/30 sayılı karar (R.G. 25.6.2013; Sayı: 28688),
- 5809 sayılı Elektronik Haberleşme Kanunu'nun 51. maddesinin iptaline dair 9.4.2014 tarih ve E.2013/122, K.2014/74 sayılı karar (R.G. 26.7.2014, Sayı: 29072),
- 6552 sayılı İş Kanunu ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması ile Bazı Alacakların Yeniden Yapılandırılmasına Dair Kanun'un 126. maddesi ile değiştirilen 5651

sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlar Mücadele Edilmesi Hakkında Kanun'un 3. maddesinin (4) no'lu fıkrasının iptaline dair 2.10.2014 tarih ve E.2014/149, K.2014/151 sayılı karar (R.G. 1.1.2015, Sayı: 29223),

- 6475 sayılı Posta Hizmetleri Kanunu'nun 3. maddesinin (1) no'lu fıkrasının (a) bendindeki ".ilgili mevzuatı saklı kalmak kaydıyla." ibaresinden sonra gelen ".gerçek." ibaresinin iptaline dair 4.12.2014 tarih ve E.2013/84, K.2014/183 sayılı karar (R.G. 13.3.2015, Sayı: 29294),

- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanun'unun 78. maddesinin 2. fıkrasının 2. cümlesi ile son cümlesinin iptaline dair 25.12.2014 tarih ve E.2014/74, K.2014/201 sayılı karar (R.G. 23.5.2014, ayı: 29364).

Yukarıdaki açıklamalar ışığında davanın somutuna dönüldüğünde; 6222 sayılı Kanun'un 5. maddesinin dördüncü fıkrasının iptali istenen ikinci, üçüncü ve dördüncü cümlelerinin, spor müsabakalarına girişte elektronik kart alınması uygulamasıyla ilgili genel çerçeveyi çizdiği, ilk nazarda sadece kimlik ya da pasaport numarası verilmesinin bunun için yeterli olduğu izlenimini verdiği ve yasanın diğer maddeleriyle birlikte değerlendirilmemesi halinde Anayasa'ya aykırı bir yönünün olmayabileceği düşünülebilirse de; 5. maddesinin (11) no'lu fıkrasında aynı elektronik kart uygulamasıyla ilgili olarak öngörülen "Elektronik kart oluşturulmak amacıyla alınacak kişisel bilgiler federasyon bünyesinde oluşturulan merkezi veri tabanında tutular", "Bu veri tabanı Maliye Bakanlığı ve İçişleri Bakanlığı erişimine açıktır", "Federasyonlar bu fıkra kapsamında belirtilen yetkilerini kısmen veya tamamen üçüncü kişilere devredebilir" şeklindeki kurallar dikkate alındığında, öngörülen sistemin salt bir "isim, kimlik tespiti"nden ibaret olmadığı, uygulamada da Türkiye Futbol Federasyonu'nun bir özel bankayla anlaşmak suretiyle seyircilere ilişkin tüm kişisel bilgilerin bu banka ile yapılan kredi sözleşmesine dercedildiği ve isim, adres, telefon numarası, elektronik posta adresi gibi kişisel verilerin depolandığı ve bu bilgilerin iki Bakanlığın erişimine açık olduğu gerçeği karşısında, iptali istenen kuralların bir bütün olarak değerlendirilmesi gerektiği açıktır.

Kişisel verilerin sistematik biçimde kayıt altına alınabilmesi için, verilerin korunmasına ilişkin usul ve esasların da kanunda gösterilmesi gerekir. Keza, kişisel verilerin alınması ve işlenmesinin demokratik bir toplumda gerekli olması, amaçla orantılı ve ölçülü bir tedbir olması da gerekmektedir. İtiraz konusu düzenlemede elektronik kart uygulaması sonucu toplanacak kişisel verilerin toplanması, işlenmesi ve korunması konularında hiçbir belirlilik olmadığı gibi, bilakis Anayasa'nın 20. maddesiyle tanınan kişisel verilerin korunması hakkını önemli ölçüde zedeleyen mahiyeti itibarıyla kuralın ölçüsüz olduğu ve bu yönü itibarıyla aynı zamanda hukuk devleti ilkesiyle bağdaşmadığı görülmektedir.

Öte yandan, anılan kuralla getirilen zorlaştırmacı mahiyetteki tedbirler nedeniyle, sporun kitlelere yayılmasının teşvik edilmesini öngören Anayasa'nın 20. maddesinin de ihlâl edildiği açık olduğu gibi; "sporda şiddet ve düzensizliğin önlenmesi" düşüncesi de anılan anayasal kuralın ihmaline gerekçe teşkil edemez.

Açıklanan nedenlerle; anılan düzenlemelerin Anayasa'nın 2., 13., 20. ve 59. maddelerine aykırı olduğu ve iptali gerektiği kanaatine vardığımdan; çoğunluğun aksi yöndeki kararına katılmıyorum.

Üye - Serdar ÖZGÜLDÜR

KARŞIOY GEREKÇESİ

6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun'un 5. maddesinin (11) numaralı fıkrasının (a) bendinde federasyonların bir merkezi kontrol sistemi oluşturacakları ve elektronik kart oluşturulmak üzere alınacak kişisel bilgilerin merkezi veri tabanında tutulacağı belirtildikten sonra, bahse konu veri tabanının Maliye ve İçişleri Bakanlıklarının erişimine açık olacağı öngörülmektedir. Adı geçen Bakanlıkların veri tabanına erişimi konusu, bendin son cümlesi olarak düzenlenmiştir.

Veri tabanının kişisel bilgileri ihtiva etmesi, bu kişisel bilgilerin Anayasa'nın 20. maddesinin güvencesi altında olması, bilgilerin kullanımının konu ile ilgisi bulunmayan ve hangi amaçla, ne şekilde bu verileri kullanacakları belli olmayan idare birimlerine açılmasının 20. maddede belirtilen temel hakkın sınırlandırılmasına ilişkin nedenler kapsamına girmemesi ve yine Anayasa'nın 13. maddesinde öngörülen, demokratik bir toplumda zorunluluk ölçütlerini karşılamaması nedeniyle iptali gerektiği düşüncesiyle, çoğunluk görüşüne katılmamaktayım.

Üye - Osman Alifeyyaz PAKSÜT

KARŞIOY GEREKÇESİ

6222 sayılı Kanun'un itiraz konusu (11) numaralı fıkranın (a) bendinin ikinci ve üçüncü cümlelerinde "...Elektronik kart oluşturulmak amacıyla alınacak kişisel bilgiler federasyon bünyesinde oluşturulan merkezi veri tabanında tutulur. Bu veri tabanı Maliye Bakanlığı ve İçişleri Bakanlığı erişimine açıktır" düzenlemesine yer verilerek, elektronik kart oluşturulmak amacıyla alınan kişisel bilgilerin federasyon bünyesinde oluşturulan merkezi veri tabanında tutulacağı, üçüncü cümlesinde ise belirtilen veri tabanının Maliye Bakanlığı ve İçişleri Bakanlığının erişimine açık olacağı öngörülmektedir. Federasyon bünyesinde oluşturulması ve Maliye ve İçişleri Bakanlıklarının

erişimine açık olması öngörülen "kişisel bilgiler"in "kişisel veri" kapsamında olduğu hususunda tereddüt bulunmamaktadır.

Anayasa'nın 20. maddesinin birinci fıkrasında, herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiştir. Maddenin üçüncü fıkrasında ise "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." denilerek kişisel verilerin korunması hakkı, özel hayatın gizliliğinin korunması kapsamında anayasal güvenceye kavuşturulmuş ve kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenleneceği öngörülmek suretiyle bu hak kamu makamlarının kanuni olmayan müdahalelerine karşı koruma altına alınmıştır.

Anayasa'nın 20. maddesinin gerekçesinde de belirtildiği üzere özel hayatın korunması her şeyden önce bu hayatın gizliliğinin korunması, başkalarının gözleri önüne serilmemesi demektir. Kişinin özel hayatında yaşananların, yalnız kendisi veya kendisinin rıza gösterdiği kişiler tarafından bilinmesini isteme hakkı, kişinin temel haklarından biridir ve bu niteliği nedeniyle insan haklarına ilişkin beyanname ve sözleşmelerde yer almış, tüm demokratik ülkelerin mevzuatlarında açıkça belirlenen istisnalar dışında devlete, topluma ve diğer kişilere karşı korunmuştur. Bu koruma bireyin kendisine ilişkin herhangi bir bilginin rızası olmaksızın açıklanmamasını, yayılmamasını, nakledilmemesini ve bu bilgilere başkalarının ulaşamamalarını da kapsamaktadır.

Çağdaş demokrasiler temel hak ve özgürlüklerin en geniş ölçüde sağlanıp güvence altına alındığı rejimlerdir. Temel hak ve özgürlükleri büyük ölçüde kısıtlayan ve kullanılamaz hale getiren sınırlamalar hakkın özüne dokunur. Temel hak ve özgürlüklere getirilen sınırlamaların yalnız ölçüsü değil, koşulları, nedeni, yöntemi, kısıtlamaya karşı öngörülen kanun yolları gibi güvenceler hep demokratik toplum düzeni kavramı içinde değerlendirilmelidir.

Anayasa'nın 2. maddesinde belirtilen hukuk devletinin ön koşulları arasında hukuki güvenlik ile belirlilik ilkeleri bulunmaktadır. Kişilerin hukuki güvenliğini sağlamayı amaçlayan hukuki güvenlik ilkesi, hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar. Belirlilik ilkesi ise yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir

olmasını, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesini ifade etmektedir.

Konu kişisel veriler olunca, Anayasa tarafından kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvencenin ve Anayasanın 2. maddesinde esasları düzenlenen hukuk devletinin ön koşulları arasında yer alan hukuki güvenlik ile belirlilik ilkelerinin gereklerinin yerine getirilebilmesi için bu hakkı ilgilendiren yasal düzenlemelerin, açık, anlaşılabilir ve kişilerin söz konusu haklarını kullanabilmelerine elverişli olması gerekir. Ancak böyle bir düzenleme ile kişilerin özel hayatlarını ilgilendiren veri, bilgi ve belgelerin resmi makamların keyfi müdahalelerine karşı korunması olanaklı hale getirilebilir. Belirtilen ilkeler doğrultusunda, kişisel verileri düzenleyen kanunlarda kişisel verilerin neden ve hangi gerekçeyle temin edileceğine ilişkin olarak konu ve amaç sınırlamasının yapılması yanında bu verilerin kapsamının ve ne şekilde kullanılacağına da belirlenmiş olması gerekmektedir.

Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun Tasarısı ile Adalet Komisyonu Raporunda, 5149 sayılı Kanunun uygulanması döneminde ortaya çıkan eksikliklerin giderilmesi, uluslararası sözleşmelere ve gelişmelere paralellik sağlanması ve sporda şiddet ve düzensizliğin önlenmesi amacıyla; konuya ilişkin diğer ülkelerin ve uluslararası spor örgütlerinin düzenlemeleri ve teamülleri göz önünde bulundurularak bu tasarının hazırlandığı belirtilmiştir.

Tasarı metninde bulunmayan itiraz konusu kuralın da içerisinde yer aldığı 5. madde 31.3.2011 tarihinde Türkiye Büyük Millet Meclisinin 23. Dönem 5. Yasama Yılı 85. Birleşiminde verilen bir önergeyle metne dahil edilmiştir. Önergenin gerekçesinde, "yapılan teklifle, elektronik kart ve elektronik karta dayalı bilet uygulamasına ilişkin koşullara açıklık getirilmekte" olduğunun belirtilmesi ile yetinilmiştir. Tasarı, Rapor ve görüşmelerde sporda şiddetin önlenmesinden bahsedilmekle birlikte genel olarak kamu güvenliğinin ve vergi denetiminin sağlanması ile ilgili herhangi bir açıklamaya yer verilmemiştir. Bu durum karşısında, çoğunluk gerekçesinde yer verilen "itiraz konusu kural ile kişisel verilerin kamu güvenliği ve vergi denetiminin sağlanması bakımından tutulduğuna, sözkonusu veri tabanının, vatandaşların çok daha ayrıntılı, mahrem ve hassas verilerinin bulunduğu Maliye ve İçişleri Bakanlıklarının erişimine açılmasının veri güvenliği açısından sorun teşkil etmeyeceğine" yönelik açıklama ve argümanlar yasama belgeleri ve "kişisel verilerin korunmasını isteme hakkı"nın anayasal niteliğiyle de bağdaşmamaktadır. Burada önemli olan Maliye ve İçişleri Bakanlıklarının elinde vatandaşlara ait çok fazla kişisel verinin olup olmaması değil, sporda şiddetin önlenmesi amacıyla kanunla öngörülen sınırlı bir amaçla ve sınırlı bir alanda

elde edilecek verilerin amacı, ölçüsü, sınırı ve kapsamı belirtilmeksizin başka kamu makamlarının erişimine ve kullanımına açılmış olmasıdır.

Öte yandan, kişisel verilerin amaç ve kapsam dışında depolanması ve kullanılması halinde 5237 sayılı Türk Ceza Kanunundaki kişisel verilerin korunmasına ilişkin ceza hükümlerinin uygulanacak olması nedeniyle bu konuda kanuni güvencenin bulunduğuna yönelik çoğunluk gerekçesine de katılma olanağı bulunmamaktadır. Zira, kişisel verilerin korunması hakkı, buna yönelik ihlallerin cezalandırılmasını isteme hakkından daha kapsamlı bir hak niteliğindedir. Başka bir anlatımla, kamu makamları veya yasakoyucu yalnızca ceza kanunlarında kötüye kullanımları müeyyideye bağlayan ceza kuralları koyarak kişisel verilerin korunması ile ilgili yükümlülüklerini yerine getirmiş sayılamazlar. Zira, bu koruma daha geniş bir alanı, bireyin kendisine ilişkin herhangi bir bilginin rızası olmaksızın açıklanmamasını, yayılmamasını, nakledilmemesini ve bu bilgilere başkalarının ulaşamamalarını kapsamaktadır.

Mahkememiz 2.10.2014 tarih ve E.2014/149, K.2014/151 sayılı kararında, internet trafik bilgisinin TİB tarafından ilgili işletmecilerden herhangi bir hukuki inceleme ya da sürece dahil olmadan alınmasını ve hâkim tarafındankarar verilmesi durumunda bu bilginin ilgili mercilere verilmesini düzenleyen 5651 sayılı Kanun'un 3. maddesinin (4) numaralı fıkrasının iptaline karar verirken dayandığı gerekçelerden bazıları şöyledir: ".Kuralda, temin edilecek bilgiyle ilgili olarak herhangi bir konu ve amaç sınırlaması bulunmadığı gibi bilginin kapsamı, ne şekilde kullanılacağı, tutulacağı süre, temin edilme gerekçesi gibi hususlarla ilgili olarak da herhangi bir belirlilik bulunmamaktadır...Bu durumda verilerin işlenebileceği hallerin kanunda açıkça yer alması zorunluluğu bulunmasına karşın, kuralda herhangi bir belirleme ve sınırlama yapılmaksızın doğrudan kişisel veri niteliğindeki trafik bilgisinin temin edilmesine ve işlenmesine olanak sağlanmasının bu yönüyle Anayasa'nın 20. maddesine aykırı olduğu açıktır...Anayasa'nın 13. ve 20. maddelerinde yer alan güvencelere rağmen dava konusu kural ile kişiler, bilgi toplama, saklama, işleme ve değiştirme yetkisi olan idareye ve diğer kişilere karşı korumasız bırakılmış, veri toplamanın amaç, gerekçe, kapsam ve sınırlama yasal düzenlemede yer verilmemiştir..."

Anayasa Mahkemesinin kişisel verilerin korunması ile ilgili olarak verdiği diğer kararlarda da ortaya koyduğu bu gerekçeler dikkate alındığında, kişisel verilerin ilgili üçüncü kişiler ya da kamu kurum ve kuruluşları ile paylaşılabilmesi için, söz konusu kişi ve kurumların bu verilere erişebileceği hususunda kanunen yetkilendirilmiş olmaları ve bu verilerin ilgili kurum ve kişilerin görevlerini yapması için gerekli olmasının yanı sıra bu görevlerin yerine getirilmesi ile de sınırlı olması gerekir. Kişisel verilere ilişkin kuralların aynı zamanda kişisel veri niteliğindeki bilgilerin teminine,

kullanılabilmesine, işlenebilmesine, ulaşılabilmesine, saklanma süresine, temin edilme gerekçesine ilişkin hususlarda bir belirlilik içermesi de gerekmektedir.

Bu ilkelere göre itiraz konusu kurala bakıldığında, sportif faaliyetleri izlemek isteyenlerin kişisel verilerinin de sadece Kanun'da öngörülen amaçla ve bu kayıtların hizmetin devamı için zorunlu olduğu müddetle sınırlı olarak tutulması zorunludur. İtiraz konusu düzenlemede elektronik kart oluşturulmak amacıyla alınan kişisel bilgilerden oluşan ve federasyon bünyesinde oluşturulan merkezi veri tabanının Maliye Bakanlığı ve İçişleri Bakanlığının erişimine açık olacağı öngörülmektedir. Ancak, kuralda Maliye ve İçişleri Bakanlıklarınınbu verilerle ilgili erişim, işleme, paylaşma, kullanma yetki ve sınırları ile bu verilerin korunmasına ilişkin usul ve esaslara yer verilmemiştir. Bu anlamda kişisel veri niteliğindeki bilgilerden oluşan veri tabanını amaç, kapsam, kullanım ve işleme yetkileri açısından gereksiz, ölçsüz ve belirsiz biçimde Maliye Bakanlığı ve İçişleri Bakanlığının erişimine açan kural Anayasa'nın 2., 13. ve 20. maddelerine aykırıdır.

Açıklanan nedenlerle, itiraz konusu kuralın Anayasa'ya aykırı olması nedeniyle iptal edilmesi gerektiği düşüncesinde olduğumdan aksi yöndeki çoğunluk görüşüne katılmadım.

Üye - Alparslan ALTAN

**Anayasa Mahkemesi - 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu Kararı (E.
2014/180)**

*Biyometrik Yöntemlerle Kimlik Doğrulaması Yapılmasını Öngören Kanun Hükümünün Anayasa Aykırılığına
İlişkin Anayasa Mahkemesi Kararı*

ANAYASA MAHKEMESİ KARARI

Esas Sayısı : 2014/180

Karar Sayısı : 2015/30

Karar Tarihi : 19.3.2015

RG Tarih-Sayı: 3.4.2015-29315

İTİRAZ YOLUNA BAŞVURAN: Danıştay Onbeşinci Dairesi

İTİRAZIN KONUSU: 31.5.2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun 67. maddesinin üçüncü fıkrasına, 1.3.2012 tarihli ve 6283 sayılı Kanun'un 1. maddesiyle eklenen ".biyometrik yöntemlerle kimlik doğrulamasının yapılması ve/veya." ibaresinin Anayasa'nın 2., 13. ve 20. maddelerine aykırılığı ileri sürülerek iptaline karar verilmesi istemidir.

I- OLAY

Genel sağlık sigortalısı davacı tarafından, biyometrik kimlik doğrulama sistemine tanımlanmaksızın hizmet sunmayan özel hastane başhekimliğinin uygulamasının bildiri niteliğinde olan işlemin ve dayanak gösterdiği mevzuatın iptali istemiyle Sosyal Güvenlik Kurumu Başkanlığı aleyhine açılan davada, itiraz konusu kuralın Anayasa'ya aykırı olduğu kanısına varan Mahkeme, iptali için başvurmuştur.

III- YASA METİNLERİ

A- İtiraz Konusu Yasa Kuralı

Kanun'un itiraz konusu kuralı da içeren 67. maddesinin üçüncü fıkrası şöyledir:

"Ayrıca genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişilerin sağlık hizmetlerinden ve diğer haklardan yararlanabilmeleri için sağlık hizmet sunucularına başvurduklarında acil haller hariç olmak üzere (acil hallerde ise acil halin sona ermesinden sonra); biyometrik yöntemlerle kimlik

doğrulamasının yapılması ve/veya nüfus cüzdanı, sürücü belgesi, evlenme cüzdanı, pasaport veya Kurum tarafından verilen resimli sağlık kartı belgelerinden birinin gösterilmesi zorunludur."

B- Dayanılan Anayasa Kuralları

Başvuru kararında, Anayasa'nın 2., 13. ve 20. maddelerine dayanılmıştır.

IV- İLK İNCELEME

Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Serruh KALELİ, Alparslan ALTAN, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ, Burhan ÜSTÜN, Engin YILDIRIM, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Erdal TERCAN, Muammer TOPAL, M. Emin KUZ ve Hasan Tahsin GÖKCAN'ın katılımlarıyla 4.12.2014 tarihinde yapılan ilk inceleme toplantısında, dosyada eksiklik bulunmadığından işin esasının incelenmesine OYBİRLİĞİYLE karar verilmiştir.

V- ESASIN İNCELENMESİ

Başvuru kararı ve ekleri, Raportör Berrak YILMAZ tarafından hazırlanan işin esasına ilişkin rapor, itiraz konusu yasa kuralı, dayanılan Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

Başvuru kararında, biyometrik yöntemlerle yapılacak kimlik doğrulaması sonucu elde edilecek kişisel verilerin toplanması ve işlenmesinin kapsamı ile bu verilerin korunmasına ilişkin usul ve esasların belirli olmadığı, yasama organı tarafından temel ilkeleri koyulmadan, çerçevesi çizilmeden biyometrik veri toplanmasına olanak veren itiraz konusu kuralın, Anayasa'nın 2., 13. ve 20. maddelerine aykırı olduğu ileri sürülmüştür.

Kanun'un 67. maddesinin itiraz konusu kuralı da içeren üçüncü fıkrasında, genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişilerin sağlık hizmetlerinden ve diğer haklardan yararlanabilmeleri için sağlık hizmet sunucularına başvurduklarında acil hâller hariç olmak üzere (acil hâllerde ise acil hâlin sona ermesinden sonra); biyometrik yöntemlerle kimlik doğrulamasının yapılması ve/veya nüfus cüzdanı, sürücü belgesi, evlenme cüzdanı, pasaport veya Kurum tarafından verilen resimli sağlık kartı belgelerinden birinin gösterilmesinin zorunlu olduğu öngörülmüştür.

Biyometrik yöntemlerle kimlik doğrulama, hizmet talep eden bir kullanıcının, ölçülebilir fizyolojik ve bireysel özellikler yoluyla gerçekleştirilen ve otomatik olarak doğrulanabilen kimlik denetleme yoluyla gerçek kullanıcı olup olmadığının doğrulanması anlamına gelmektedir.

Anayasa'nın 2. maddesinde belirtilen hukuk devleti, insan haklarına dayanan, bu hak ve özgürlükleri koruyup güçlendiren, eylem ve işlemleri hukuka uygun olan, her alanda adaletli bir hukuk düzeni kurup bunu geliştirerek sürdüren, Anayasa'ya aykırı durum ve tutumlardan kaçınan, hukuku tüm devlet organlarına egemen kılan, Anayasa ve kanunlarla kendini bağlı sayan, yargı denetimine açık olan devlettir. Kanun koyucu, Anayasa'ya ve hukukun genel ilkelerine aykırı olmamak kaydıyla her türlü düzenlemeyi yapma konusunda takdir yetkisine sahiptir. Kanun koyucunun hukuki düzenlemelerde kendisine tanınan takdir yetkisini anayasal sınırlar içinde adalet, hakkaniyet ve kamu yararı ölçütlerini göz önünde tutarak kullanması ve keyfi davranmaması gerekir.

Anayasa'nın 2. maddesinde yer alan hukuk devletinin temel ilkelerinden biri "belirlilik"tir. Belirlilik ilkesi, yalnızca yasal belirliliği değil, daha geniş anlamda hukuki belirliliği de ifade etmektedir. Yasal düzenlemeye dayanarak erişilebilir, bilinebilir ve öngörülebilir gibi niteliksel gereklilikleri karşılaması koşuluyla, mahkeme içtihatları ve yürütmenin düzenleyici işlemleri ile de hukuki belirlilik sağlanabilir. Aslolan muhtemel muhataplarının mevcut şartlar altında belirli bir işlemin ne tür sonuçlar doğurabileceğini öngörmelerini mümkün kılacak bir normun varlığıdır.

Anayasa'nın 20. maddesinin birinci fıkrasında, herkesin, özel hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş; üçüncü fıkrasında da "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." denilerek kişisel verilerin korunması, özel hayatın gizliliğinin korunması kapsamında güvenceye kavuşturulmuştur.

Anayasa'nın 13. maddesinde, temel hak ve hürriyetlerin, özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği, bu sınırlamaların Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacağı belirtilmiştir.

Kişisel verilerin korunması hakkı, kişinin insan onurunun korunması ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Ancak söz konusu hak mutlak ve sınırsız olmayıp Anayasa'nın 13. ve 20. maddeleri gereğince belirli koşullarda, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmamak üzere kanunla sınırlanabilir. Nitekim Türkiye'nin imzaladığı ancak uygulama kanununun yürürlüğe konamaması nedeniyle taraf olmadığı 1981 tarihli

ve 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Avrupa Konseyi Sözleşmesi'nin 9. maddesinde de devlet güvenliği, kamu güvenliği, devletin ekonomik menfaatlerinin korunması ve suçlarla mücadele edilmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması ile verilerin istatistiki veya bilimsel amaçlarla kullanılması durumlarında kişisel verilerin korunmasına sınırlamalar getirilebileceği öngörülmüştür. Bu nedenle, kişisel verilerin korunması temel hakkına kamu yararı nedenlerine dayalı olarak müdahale edilebilmesine olanak tanınmaktadır.

İtiraz konusu kuralla, genel sağlık sigortalısı olanlar ve bakmakla yükümlü olduğu kişilerin sağlık hizmetlerinden ve diğer haklardan yararlanabilmeleri için hastane gibi kurumlara başvurduğunda, nüfus cüzdanı, sürücü belgesi, evlenme cüzdanı, pasaport veya verilmiş ise çalıştığı Kurum sağlık kartı belgelerinden biriyle kimlik tespitinin yanında veya sadece biyometrik yöntemlerle kimlik doğrulaması yapılması öngörülmektedir.

Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır. Bu bağlamda itiraz konusu kuralla öngörülen biyometrik yöntemle elde edilen verilerin kişisel veri olduğunda kuşku yoktur. Bununla birlikte söz konusu verilerin, 108 sayılı Sözleşme'nin 6. maddesinde özel olarak belirtilen politik düşünce, dini inanç, sağlık, cinsel yaşam veya ceza mahkûmiyetlerine ilişkin veriler gibi çok hassas verilerden olduğu da söylenemez.

Biyometrik yöntemlerle kimlik doğrulama, kişinin kendi özelliklerini esas alması nedeniyle izinsiz kullanımlara karşı güvenli, kamu kuruluşlarına yönelik yolsuzluk ve bunların neden olduğu zararlara karşı etkili ve sosyal güvenliği olan kişiler bakımından da güvenli hizmet alınmasını sağlayan bir yöntemdir. İtiraz konusu kuralla öngörülen yöntemin sağlık sektöründeki suiistimallerin engellenmesi ve bu konudaki sahteciliğin önlenmesi amacıyla önemli bir güvenlik önlemi olduğunda şüphe yoktur. Nitekim itiraz konusu kuralın gerekçesinde sağlık hizmetlerinin elektronik ortamda güvenilir altyapılar üzerinden sağlanması ve hizmetten yararlananların kimliklerinin saptanmasında geleneksel yöntemlerin eksiklikleri nedeniyle ortaya çıkan kötüye kullanımların önlenmesinin amaçlandığı belirtilmiştir. Dolayısıyla kuralla öngörülen yöntemin etkin bir şekilde

kullanılmasının, Sosyal Güvenlik Kurumundan haksız menfaat temin edilmesini engellemeye yönelik olduğu ve kuralda kamu yararı bulunduğu açıktır.

Bu bağlamda itiraz konusu kuralla özel hayatın ve kişisel verilerin korunması haklarına yönelik olarak yapılan müdahalenin, öngörülen amaçla orantılı olduğu, müdahale edilen hakların özüne dokunmadığı ve demokratik toplum düzeninin gereklerine aykırılık teşkil etmediği anlaşıldığından Anayasa'ya aykırı bir yönü yoktur.

Öte yandan itiraz konusu kuralla öngörülen yöntemin sadece sağlık sektöründe bu hizmetten yararlanma amacıyla kullanılabileceği, bu nedenle elde edilen verilerin sadece bu amaçla sınırlı olarak ve hizmetin devamı için zorunlu olduğu müddetle sınırlı olmak üzere tutulabileceği dikkate alındığında, bu verilerin neden ve hangi gerekçeyle temin edileceğine ilişkin olarak konu, amaç ve kapsamı ile ne şekilde ve hangi süreyle kullanılacaklarına dair bir belirsizlik olduğu söylenemez.

Ayrıca itiraz konusu kuralda öngörülen yöntemle elde edilen verilerin amaç ve kapsam dışında depolanması ve kullanılması hâlinde 5237 sayılı Türk Ceza Kanunu'ndaki kişisel verilerin korunmasına ilişkin ceza hükümlerinin uygulanacak olması nedeniyle bu konuda kanuni güvence de bulunmaktadır.

Açıklanan nedenlerle, itiraz konusu kural Anayasa'nın 2., 13. ve 20. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Serruh KALELİ, Alparslan ALTAN, Serdar ÖZGÜLDÜR, Engin YILDIRIM ve Erdal TERCAN bu görüşe katılmamışlardır.

VI- SONUÇ

31.5.2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun 67. maddesinin üçüncü fıkrasına, 1.3.2012 tarihli ve 6283 sayılı Kanun'un 1. maddesiyle eklenen ".biyometrik yöntemlerle kimlik doğrulamasının yapılması ve/veya." ibaresinin, Anayasa'ya aykırı olmadığına ve itirazın REDDİNE, Serruh KALELİ, Alparslan ALTAN, Serdar ÖZGÜLDÜR, Engin YILDIRIM ile Erdal TERCAN'ın karşıoyları ve OYÇOKLUĞUYLA, 19.3.2015 tarihinde karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili - Serruh KALELİ

Başkanvekili - Alparslan ALTAN

Üye: Serdar ÖZGÜLDÜR; Osman Alifeyyaz PAKSÜT; Recep KÖMÜRÇÜ; Burhan ÜSTÜN; Engin YILDIRIM; Nuri NECİPOĞLU; Hicabi DURSUN; Celal Mümtaz AKINCI; Erdal TERCAN; Muammer TOPAL; M. Emin KUZ; Hasan Tahsin GÖKCAN; Kadir ÖZKAYA

KARŞIOY GEREKÇESİ

5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun 67. maddesinin üçüncü fıkrasına, 6283 sayılı Kanun'un 1. maddesiyle eklenen ". biyometrik yöntemlerle kimlik doğrulamasının yapılması ve/veya." ibaresinin Anayasa'ya aykırılığı ileri sürülmüştür.

Kural, sağlık sigortalısı ve bakmakla yükümlü olduğu kişilerin sağlık hizmetlerinden yararlanmak amacıyla sağlık hizmet sunucularına başvurduklarında biyometrik yöntemlerle meşru bir kullanıcı olup, olmadıklarını tespit etmeyi amaçlamaktadır. Kuralda "ve/veya" bağlacının kullanılması, kimliği tespit etmek ve denetlemek amacıyla biyometrik yöntemlerin kullanılmasının zorunlu olmadığını, belirtilen diğer belge ve usullerle de kimlik doğrulamasının yapılabileceğini ortaya koymaktaysa da; Sosyal Güvenlik Kurumu Sağlık Uygulama Tebliği'nde "ve/veya" bağlacı yerine "ve" bağlacı kullanıldığından biyometrik yöntemlerle kimlik doğrulaması uygulamada zorunlu hale getirilmiştir. Sağlık hizmetinden yararlanmak isteyenler biyometrik kimlik doğrulamasını kabul etmediklerinde sağlık hizmeti alamamaktadır. Bu da sağlık hizmeti almak isteyenlerden zorla kişisel veri alınması ile eşanlamlıdır. Hasta sağlık hizmeti almak için biyometrik yöntemle boyun eğmek zorunda bırakılmakta, bu yöntemle elde edilen kişisel verilerinin ne amaçla kimler tarafından kullanılacağını bilmemekte, verilerine ulaşma, düzeltilmesini ya da silinmesini isteme haklarından mahrum bulunmaktadır.

"Özel hayatın gizliliği" başlıklı Anayasa'nın 20. maddesinin 7.5.2010 tarih ve 5982 sayılı Kanun'la eklenen son fıkrasında "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." denilmektedir. Anılan hükmün gerekçesinde de "Anayasada kişisel verilerin korunmasına yönelik dolaylı hükümler bulunmakla birlikte yeterli değildir. Mukayeseli hukukta ve tarafı olduğumuz uluslararası belgelerde de kişisel verilerin korunması önemle vurgulanmaktadır. Maddeyle, herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı, anayasal bir hak olarak teminat altına alınmaktadır. Bu bağlamda, bireylerin kendilerini ilgilendiren kişisel veriler üzerinde hangi hak ve yetkilere sahip

olduğu ve kişisel verilen hangi hallerde işlenebileceği hükme bağlanırken, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği öngörülmektedir." şeklinde değerlendirmenin yer aldığı görülmektedir. Anayasa'nın 20. maddesinin çıkarılmasını öngördüğü kanun ise henüz çıkarılmamıştır. Ancak, örneğin Türk Ceza Kanunu'nun 135 - 140. maddelerinde kişisel verilerin hukuka aykırı olarak kaydedilmesi ve işlenmesi halleri suç olarak düzenlenmiş ve yaptırıma bağlanmıştır.

Öte yandan, birçok uluslar arası sözleşmede de kişisel verilerle ilgili düzenlemeler yapılmış ve konunun önemi bu uluslararası metinlere yansımıştır. Örneğin, Türkiye'nin de 1981'de imzalamasına karşın henüz onaylamadığı, Avrupa Konseyi'nin 28.1.1981 tarih ve 108 Numaralı "Kişisel Nitelikli Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme"nin 6. maddesine göre, iç hukukta uygun güvenceler sağlanmadıkça, ırk menşeyini, politik düşünceleri, dini veya diğer inançları ortaya koyan kişisel nitelikli verilerle, sağlık veya cinsel yaşamla ilgili kişisel nitelikteki veriler ve ceza mahkumiyetleri, otomatik bilgi işlemine tâbi tutulamazlar. Yine Avrupa Birliği'nin 24 Ekim 1995 tarihli "Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması Yönergesi (95/46/EC)"nde de, siyasi, dini, felsefi görüşler veya uyuşturucu, alkol bağımlılığı veya sağlık gibi hassas verilerin korunmasına ilişkin düzenlemelere yer verilmiştir.

Avrupa İnsan Hakları Mahkemesi de, kişilerin fiziki ve sosyal kimlikleri, kişisel bilgileri, cinsiyetleri, şahıslarına ait özerk sahaları, adları, fiziki ve ruhsal bütünlükleri (sağlık/tıbbi bilgileri) iş ilişkileri, sosyal etkinlikleri, kişisel gelişimi, fiziki ve moral güvenliği, dış çevrede insanlarla ilişkileri gibi hususları, sözleşmenin "Özel hayatın ve aile hayatının korunması" başlıklı 8. maddesi kapsamında "özel hayat" kavramı içinde değerlendirmektedir. Avrupa İnsan Hakları Mahkemesinin birçok kararında da, tıbbi verilerin ve bilgilerin Sözleşmenin 8. maddesinin koruması altında olduğu, bunların korunması ve güvenliğinin üye ülkelerin sorumluluğunda bulunduğu, bu bilgi ve verilerin başkalarının eline geçmemesi için gerekli tüm yasal düzenlemelerin ve güvencelerin mevcudiyetinin gerektiği, keza parmak izi, DNA analizi vb. gibi biyometrik verilerin salt kimlik tespitine ve güvenlik nedenine yönelik durumlar müstesna, hassas kişisel veri olarak korunmaları gerektiği içtihat olarak ortaya konulmuştur. Bir örnek olmak üzere, Avrupa İnsan Hakları Mahkemesinin S. ve Marper'in Birleşik Krallığa karşı yaptığı başvuru sonucunda verdiği kararında; gözaltına alınan kişilerin kan, hücre örnekleri ve parmak izinin alınması fakat daha sonradan bu kişilerin kendilerine isnat edilen suçla ilişkilerinin kalmaması durumunda, halen bu bilgilerin tutulmaya devam edilmesini bu ölçüt açısından değerlendirmiş ve durumu Avrupa İnsan Hakları Mahkemesi Sözleşmesinin 8. maddesinin ihlâli olarak görmüştür. Mahkeme, kişisel verilerin muhafazası, tutulma süresi, kullanımı, üçüncü

kişilerin erişimine açık olup, olmaması verilerin gizliliği ve silinmesi konularında açık ve ayrıntılı asgari güvencelerin sağlanması gerektiğini vurgulamıştır. (Case of S.and Marper v. The United Kingdom, Başvuru No: 30562/04 ve 30566/04, Karar Tarihi: 4 Aralık 2008 paragraf 99.)

Anayasa Mahkemesi de aşağıda işaret edilen kararlarında, sözkonusu yasal düzenlemelerde yer alan düzenlemeleri, kişisel verilerin korunmasına ilişkin Anayasa'nın 20. maddesi ile 13. maddesine aykırı bularak iptali yoluna gitmiştir:

- ". İtiraz konusu kuralla, Bilgi Teknolojileri ve İletişim Kurumunun elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesine ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkili olduğu hükme bağlanmıştır. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunması ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Bilişim teknolojilerindeki gelişmeler sonucunda, geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi; daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tâbi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması; verilere erişim ve veri transferinin kolaylaşması; kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması, terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler, günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır. Bu bağlamda Anayasa'nın 20. maddesinin üçüncü fıkrasının son cümlesinde 'Kişisel verilerin korunmasına ilişkin usul ve esaslar kanunla düzenlenir.' hükmüne yer verilerek, kişisel verilerin korunması hakkı anayasal güvenceye bağlanmış ve bu şekilde kamu makamlarının keyfi müdahalelerine karşı koruma altına alınmıştır. Yasama yetkisinin devredilemezliği ilkesi gereğince, Anayasa'nın açıkça kanunla düzenlenmesini öngördüğü konularda yürütme organına doğrudan ve ilk elden düzenleyici işlem yapma yetkisi verilemez. Elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirleme yetkisini Bilgi Teknolojileri ve İletişim Kurumuna veren itiraz konusu kural, Anayasa'nın 20. maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceğine ilişkin güvenceye aykırıdır. Açıklanan nedenlerle, itiraz konusu kural Anayasa'nın 20. maddesine aykırıdır. İptali gerekir..." (Any. Mah.nin 9.4.2013 tarih ve E.2013/122, K.2014/74 sayılı kararı; RG. 26.7.2014, Sayı: 29072)

-"... Dava konusu kural, internet trafik bilgisinin TİB tarafından ilgili işletmecilerden herhangi bir hukuki inceleme ya da sürece dahil olmadan alınmasını ve hâkim tarafından karar verilmesi

durumunda bu bilginin ilgili mercilere verilmesini düzenlemektedir... Kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvencenin yaşama geçirilebilmesi için, bu hakkı ilgilendiren yasal düzenlemelerin, açık, anlaşılabilir ve kişilerin söz konusu haklarını kullanabilmelerine elverişli olması gerekir. Ancak böyle bir düzenleme ile kişilerin özel hayatlarını ilgilendiren veri, bilgi ve belgelerin resmi makamların keyfi müdahalelerine karşı korunması olanaklı hale getirilebilir... Çağdaş demokrasiler temel hak ve özgürlüklerin en geniş ölçüde sağlanıp güvence altına alındığı rejimlerdir. Temel hak ve özgürlükleri büyük ölçüde kısıtlayan ve kullanılamaz hale getiren sınırlamalar hakkın özüne dokunur. Temel hak ve özgürlüklere getirilen sınırlamaların yalnız ölçüsü değil, koşulları, nedeni, yöntemi, kısıtlamaya karşı öngörülen kanun yolları gibi güvenceler hep demokratik toplum düzeni kavramı içinde değerlendirilmelidir... Özel hayatın korunması her şeyden önce bu hayatın gizliliğinin korunması, başkalarının gözleri önüne serilmemesi demektir. Kişinin özel hayatında yaşananların, yalnız kendisi veya kendisinin bilmesini istediği kimseler tarafından bilinmesini isteme hakkı, kişinin temel haklarında biridir ve bu niteliği nedeniyle insan haklarına ilişkin beyanname ve sözleşmelerde yer almış, tüm demokratik ülkelerin mevzuatlarında açıkça belirlenen istisnalar dışında devlete, topluma ve diğer kişilere karşı korunmuştur... Trafik bilgisi adı altında istenen bilgiler genel anlamda belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ihtiva eden kişisel veri kavramı içerisinde yer almaktadır. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır... Dava konusu kural, yukarıda belirtilen kişisel veri niteliğinde olan ve çok ciddi suçların tespiti, soruşturulması ve kovuşturulmasında kullanılmak üzere gerçek ve tüzel kişilere ilişkin trafik bilgisinin, işlenmemiş veri halinde süreli olarak muhafaza edildiği erişim veya yer sağlayıcılardan, TİB tarafından herhangi bir gerekçe veya neden göstermeksizin temin edilmesine olanak sağlamaktadır. Söz konusu veriler ulaşılabilirlik, kişilerin tercihleri, düşünceleri ve davranışları hakkında fikir verebileceğinden kişilerin özel hayatlarına müdahale edilme riskini içermektedir. Kuralda, temin edilecek bilgiyle ilgili olarak herhangi bir konu ve amaç sınırlaması bulunmadığı gibi bilginin kapsamı, ne şekilde kullanılacağı, tutulacağı süre, temin edilme gerekçesi gibi hususlarla ilgili olarak da herhangi bir belirlilik bulunmamaktadır... Bu durumda verilerin işlenebileceği hallerin kanunda açıkça yer alması zorunluluğu bulunmasına karşın, kuralda herhangi bir belirleme ve sınırlama yapılmaksızın doğrudan kişisel veri niteliğindeki trafik bilgisinin temin edilmesine ve işlenmesine olanak sağlanmasının bu yönüyle Anayasa'nın 20. maddesine aykırı olduğu açıktır... Anayasa'nın 13. ve 20. maddelerinde yer alan güvencelere rağmen dava konusu kural ile kişiler, bilgi toplama, saklama, işleme ve değiştirme yetkisi olan idareye ve diğer kişilere karşı korumasız bırakılmış, veri

toplamanın amaç, gerekçe, kapsam ve sınırlama yasal düzenlemede yer verilmemiştir. Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 13. ve 20. maddelerine aykırıdır. İptali gerekir..." (Any. Mah.nin 2.10.2014 tarih ve E.2014/149, K.2014/151 sayılı kararı, RG. 1.1.2015, Sayı: 29223)

"... Dava konusu ibarenin de yer aldığı (a) bendinde, aynı Kanun'un 22. maddesinin (1) numaralı fıkrasında PTT'nin faaliyetleri arasında belirtilen "Adres bilgi kayıt sistemi"nin neyi ifade ettiği husus belirtilmiştir. Buna göre, adres bilgi kayıt sistemi 25.4.2006 günlü, 5490 sayılı Nüfus Hizmetleri Kanunu ve ilgili mevzuatı saklı kalmak kaydıyla, gerçek kişilerin rızası alınarak gerçek ve tüzel kişiler ile kamu kurum ve kuruluşlarına ait fiziki ve elektronik adreslerin, reklâm ve tanıtım amacıyla PTT hizmetlerinden yararlananlara ücret karşılığı kullandırılmasına yönelik olarak oluşturulan PTT'ye ait veri tabanını ifade etmektedir. Dava konusu ibare, adres bilgi kayıt sisteminde, gerçek kişilerin rızasını aramaktadır. Dolayısıyla, ibarenin mefhumu muhalifinden, tüzel kişiler yönünden onların rızalarının alınmasına gerek bulunmadığı anlamı çıkmaktadır. Kişisel verilerin korunması temel hakkı, Anayasa hukukunda esas olarak yüksek kişilik değerlerini korumaya yönelik bireysel haklara ilişkindir. Bu hak, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda, bir kişinin kendisinin veya ailesinin sürekli veya geçici olarak konakladığı, ikamet ettiği yerlere ait bilgiler (fiziki adresleri) de kişisel veri niteliğindedir. Aynı şekilde, elektronik posta olarak adlandırılan ve elektronik iletişim ağı üzerinden gönderilen ve internette ya da kullanıcının bilgisayarında kaydedilebilen her türlü yazı, ses, resim ya da dil iletilerinin de kişisel veri niteliğinde olduğu kabul edilmektedir. (Anayasa'nın 20. maddesi) metninde kişisel verilerle ilgili olarak 'herkes'tabirinin kullanılması dikkate alındığında, tüzel kişilere ilişkin verilerinde 20. madde kapsamında değerlendirilmesi gerekeceği açıktır. Bu durumda, tüzel kişilerin kişisel veri niteliğinde bulunan fiziki veya elektronik adreslerinin, yetkili kişi ya da organlarının rızaları alınmaksızın, dava konusu kural uyarınca PTT A.Ş. tarafından reklâm veya tanıtım amacıyla toplanıp kaydedilmesinin ve bunların üçüncü kişilere verilmesinin, Anayasa'nın 20. maddesine aykırılık oluşturduğu açıktır. Açıklanan nedenlerle, dava konusu kural Anayasa'nın 20. maddesine aykırıdır. İptali gerekir." (Any. Mah.nin 4.12.2014 tarih ve E.2013/84, K.2014/183 sayılı kararı; RG.13.3.2015, Sayı: 29294.)

- Nihayet Anayasa Mahkemesi, henüz gerekçesi yayımlanmayan 4.12.2014 tarih ve E.2013/114, K.2014/184 sayılı kararı ile 12.7.2013 tarih ve 6495 sayılı Kanun'la değiştirilen Sağlık Bakanlığı ve Bağlı

Kuruluşlarının Teşkilat ve Görevleri Hakkındaki 663 sayılı Kanun Hükmünde Kararname'nin 47. maddesinin aşağıda metnine yer verilen (1), (2) ve (3) numaralı fıkralarının iptaline karar vermiştir:

" (1) Bakanlık ve bağlı kuruluşları, mevzuatla kendilerine verilen görevleri, e-devlet uygulamalarına uygun olarak daha etkin ve daha hızlı biçimde yerine getirebilmek için, bütün kamu ve özel sağlık kurum ve kuruluşlarından; sağlık hizmeti alanların, aldıkları sağlık hizmetinin gereği olarak ilgili sağlık kurum ve kuruluşuna vermek zorunda oldukları kişisel bilgileri ve bu kimselere verilen hizmete ilişkin bilgileri her türlü vasıtayla toplamaya, işlemeye ve paylaşmaya yetkilidir.

(2) Bakanlık ve bağlı kuruluşları kişisel sağlık verilerini ilgili üçüncü kişiler ve kamu kurum ve kuruluşları ile ancak bu kişi ve kurumların bu verilere erişebileceği hususunda kanun en yetkili olması halinde görevlerinin yapmalarına yetecek derecede paylaşabilir.

(3) Bakanlık ve bağlı kuruluşları, mevzuatla kendilerine verilen görevleri yerine getirebilmek için gereken bilgileri, kamu ve özel ilgili bütün kişi ve kuruluşlardan istemeye yetkilidir. İlgili kişi ve kuruluşlar istenilen bilgileri vermekle yükümlüdür."

Yukarıdan beri yapılan açıklamalar ışığında ilk tespiti gereken husus, dava konusu kuralın (biyometrik yöntemlerle kimlik doğrulamasının yapılması ve/veya) salt bir kimlik tespitine yönelik düzenleme mahiyetinde olup olmadığı, kişisel sağlık verilerinin bu yolla depolanıp işlenmesi ve paylaşılması sonucunu doğurup doğurmayacağına ortaya konulmasıdır. Sosyal Güvenlik Kurumunun (SGK), kendisine sağlık hizmeti sunulanlar yönünden bir kimlik tespiti ihtiyacı olduğunda kuşku yoksa da; kuralda bu amaca yönelik bir düzenleme öngörülürken, sigortalıların ve bakmakla yükümlü oldukları yakınlarının hassas kişisel veri mahiyetindeki "sağlık bilgilerinin" korunmasına yönelik düzenlemelerin yapılması gerektiği açıktır. Çünkü, biyometrik yöntemlerle kimlik bilgilerinin sağlık hizmeti sunucularınca tespiti, beraberinde o kişinin tüm sağlık verilerinin yetkisiz ellere geçmesi ihtimalini de getirmekte; aynı şekilde SGK'da toplanan bu kimlik verilerinin başkalarıyla paylaşılmaması, başka kişi ya da yerlere iletilmemesi gerekmektedir. Oysa dava konusu kuralda bu yönde hiçbir belirlilik bulunmamakta, bilakis kural bu mahiyeti itibariyle her türlü kötüye kullanmaya müsait görünmektedir.

Sigortalı kişilerden alınacak biyometrik örnekler, kişinin sağlık hizmetine ihtiyaç duyduğu süre boyunca, yani yaşamın sonuna değin elektronik sistemde saklanacaktır. Kuvvetli suç şüphesi halinde dahi amaçla orantılı bir sürede saklanabilen bu verilerin, prim ödeyerek sağlık hizmetinden yararlanan yurttaşlar yönünden süresiz olarak saklanması süre yönünden de ölçsüz bir tedbir olduğu açıktır. Dolayısıyla kuralın belirlilik ilkesiyle ve dolayısıyla hukuk devleti ilkesiyle bağdaşmadığı söylenemez.

Anayasa'nın 13. maddesinde, temel hak ve özgürlüklerin özlerine dokunulmaksızın ölçülülük ilkesine uygun şekilde, yasayla sınırlandırılabilmesi belirtilmektedir. Ölçülülük ilkesi sınırlamada başvurulan aracın sınırlama amacını gerçekleştirmeye elverişli olmasını; bu aracın sınırlama amacı açısından gerekli olmasını ve araçla amacın ölçsüz bir oran içinde bulunmamasını ifade eder. Burada kısıtlama için kullanılan araçla amaç arasında hak ve özgürlüğü en az sınırlayacak dengeli bir orantı aranmaktadır.

Özel hayatın gizliliği ve bu kapsamda kişisel verilerin korunması konusu her şeyden önce insan onuruna saygı ve kişilik haklarına dayanmaktadır. Bu hak, kişinin saygınlığını ve kişiliğini serbestçe geliştirmesini mümkün kılan şeref ve haysiyet, özel yaşam ve sağlık gibi kişisel değerler üzerindeki çıkarlarını belirterek, bireye kişiliğini dilediği şekilde, serbestçe geliştirebileceği, kendisi ve sevdikleriyle bir arada olabileceği özerk bir yaşam alanına sahip olma şansı vermektedir. Bu alanda birey, maddi ve manevi kişiliğini geliştirmek ve başkaları tarafından bilinmesini istemediği hususların güvence altına alınmasını istemek hakkına sahiptir.

Sosyal Güvenlik Kurumu tarafından özel sağlık kuruluşlarına başvuran hastalardan talep edilen biyometrik veriler, Anayasa'nın 20. maddesinde düzenlenen, 'özel hayatın gizliliği' ilkesinin mutlak koruması altındadır. Bireylerin sağlığına veya fiziksel/biyolojik özelliklerine ilişkin bilgilerin kişisel veri kapsamında olduğunda ise şüphe yoktur.

Kişisel verilerin sistematik biçimde kayıt altına alınabilmesi için verilerin korunmasına ilişkin esas ve usullerin kanunla düzenlenmesi ön koşuldur. Başka bir deyişle kişisel verilerin korunmasına ilişkin gerekli yasal düzenlemeye ve teknik olanaklara sahip olmayan bir kamu otoritesinin, yasallık ve kişinin rızası koşullarını sağlaması halinde dahi veri işlemenin hukuka uygunluğundan söz etmek olanaklı olmayacaktır. Kişisel verilerin alınması ve işlenmesinin demokratik bir toplumda gerekli olması, amaçla orantılı ve ölçülü bir tedbir olması gerekmektedir. İtiraz konusu düzenlemede biyometrik yöntemlerle yapılacak kimlik doğrulaması sonucu elde edilen kişisel verilerin toplanması ve işlenmesinin kapsamı ile bu verilerin korunmasına ilişkin usul ve esaslara yer verilmemiştir.

Devlet Denetleme Kurulu da, Sağlık Bakanlığı ve Sosyal Güvenlik Kurumunu da kapsayan kişisel verilerle ilgili raporunda; kişisel verilerin hangi ilkeler kapsamında toplanacağı, ne şekilde korunacağı, kimlerle ve ne şekilde paylaşılabilmesi, nasıl silineceği, kişilerin Anayasa ile getirilen haklarını kullanabilmeleri için kurumların ne tür önlemler alması gerektiği gibi pek çok konuda önemli sorunlar olduğuna dikkat çekmiştir.

(Devlet Denetleme Kurulunun; "Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen

Denetim Çalışmaları" hakkında hazırlanan 27/11/2013 tarih ve 2013/3 sayılı Denetleme Raporu Özeti, <http://www.tccb.gov.tr/ddk26.pdf>, erişim tarihi 25.3.2015)

Kuralın Anayasa'nın 13. maddesi bakımından yapılan değerlendirilmesinde, ölçülü ve gerekli olmadığı da açıktır. SGK yönünden sağlık suistimalleri gerekçe gösterilerek bu düzenlemenin yapıldığı kuralın gerekçesinden öne sürülmekteyse de; resmi kimlik belgelerini bir anlamda geçersiz kılan kuralın ölçülü ve gerekli olduğu kabul edilemez. Ayrıca Anayasa'nın 20. maddesinde belirtilen esaslı unsurlar da kuralda (yasada) yer olmadığından, kuralın Anayasa'nın 20. maddesinin de ihlâli sonucuna yol açtığı ve Anayasa Mahkemesinin yukarıda işaret edilen iptal kararlarındaki ölçütleri taşımadığı görülmektedir.

Açıklanan nedenlerle, ilk nazarda sadece bir kimlik tespiti yöntemi gibi görünse de, gerçekte sigortalıların tüm sağlık bilgilerinin (hassas kişisel verilerinin) deşifre edilmesi, işlenmesi, kötüye kullanılması ihtimalini barındıran ve esaslı hiçbir ölçüt ve güvence ihtiva etmeyen kuralın Anayasa'nın 2., 13. ve 20. maddelerine aykırı olduğu ve iptali gerektiği kanaatine vardığımızdan; çoğunluğun aksi yöndeki kararına katılmıyoruz.

Başkanvekili - Serruh KALELİ

Başkanvekili - Alparslan ALTAN

Üye: Serdar ÖZGÜLDÜR; Engin YILDIRIM; Erdal TERCAN

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2014/149

Karar Sayısı: 2014/151

Karar Günü: 2.10.2014

RG Tarih-Sayı: 1.1.2015-29223

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri M. Akif HAMZAÇEBİ ve Engin ALTAY ile birlikte 123 milletvekili

İPTAL DAVASININ KONUSU: 10.9.2014 günlü, 6552 sayılı İş Kanunu ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması ile Bazı Alacakların Yeniden Yapılandırılmasına Dair Kanun'un;

A- 97. maddesiyle, 6.1.1982 günlü, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 28. maddesinin;

1- (1) numaralı fıkrasının değiştirilen üçüncü cümlesinin ". 23/4/1981 tarihli ve 2451 sayılı Bakanlıklar ve Bağlı Kuruluşlarda Atama Usulüne İlişkin Kanuna ekli (1) ve (2) sayılı cetvellerde gösterilen unvanları taşıyan görevler ile farklı atama usullerine tabi olsalar dâhi daire başkanı ve üstü görevlere, sivil memurlar hariç kolluk teşkilatlarının kadrolarına; açıktan, naklen veya vekâleten yapılan atama ve bu görevlerden alınma, bu görevlerle ilgili yer değiştirme, görev ve unvan değişikliği işlemleri hakkında verilen mahkeme kararlarının gereği, ilgilinin kazanılmış hak aylık derecesine uygun başka bir kadroya atanması suretiyle iki yıl içinde yerine getirilir." bölümünün,

2- (1) numaralı fıkrasının değiştirilen dördüncü cümlesinin,

3- (1) numaralı fıkrasına eklenen cümlenin "Bu fıkranın üçüncü cümlesinde belirtilen işlemlerle ilgili mahkeme kararlarının yerine getirilmemesi ceza soruşturması ve kovuşturmasına konu edilemez; ." bölümünün,

B- 109. maddesiyle, 24.11.1994 günlü, 4046 sayılı Özelleştirme Uygulamaları Hakkında Kanun'a eklenen geçici 26. maddenin,

C- 126. maddesiyle değiştirilen, 4.5.2007 günlü, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 3. maddesinin (4) numaralı fıkrasının,

D- 127. maddesiyle, 5651 sayılı Kanun'un;

1- 8. maddesinin (5) numaralı fıkrasının değiştirilen "dört saat" ibaresinin,

2- 8. maddesine eklenen (16) numaralı fıkranın,

Anayasa'nın 2., 10., 13., 20., 22., 26., 28., 36., 40., 125. ve 138. maddelerine aykırılığı ileri sürülerek iptallerine ve yürürlüklerinin durdurulmasına karar verilmesi istemidir.

II- YASA METİNLERİ

A- İptali İstenilen Yasa Kuralları

Kanun'un;

1- 97. maddesiyle değiştirilen 2577 sayılı Kanun'un dava konusu kuralları da içeren 28. maddesi şöyledir :

"Kararların sonuçları

Madde 28- 1.(Değişik:10/6/1994-4001/13 md.) Danıştay, bölge idare mahkemeleri, idare ve vergi mahkemelerinin esasa ve yürütmenin durdurulmasına ilişkin kararlarının icaplarına göre idare, gecikmeksizin işlem tesis etmeye veya eylemde bulunmaya mecburdur. Bu süre hiçbir şekilde kararın idareye tebliğinden başlayarak otuz günü geçemez. (İptal cümle: Anayasa Mahkemesi'nin 10/7/2013 tarihli ve E.: 2012/107 K.: 2013/90 sayılı Kararı ile.)(.)(Ek cümleler: 21/2/2014-6526/18 md.; Değişik üçüncü ve dördüncü cümleler: 10/9/2014-6552/97 md.) Ancak, 23/4/1981 tarihli ve 2451 sayılı Bakanlıklar ve Bağlı Kuruluşlarda Atama Usulüne İlişkin Kanuna ekli (1) ve (2) sayılı cetvellerde gösterilen unvanları taşıyan görevler ile farklı atama usullerine tabi olsalar dâhi daire başkanı ve üstü görevlere, sivil memurlar hariç kolluk teşkilatlarının kadrolarına; açıktan, naklen veya vekâleten yapılan atama ve bu görevlerden alınma, bu görevlerle ilgili yer değiştirme, görev ve unvan değişikliği işlemleri hakkında verilen mahkeme kararlarının gereği, ilgilinin kazanılmış hak aylık derecesine uygun başka bir kadroya atanması suretiyle iki yıl içinde yerine getirilir. Bu görevliler hakkındaki mezkur işlemlerin uygulanması, telafisi güç veya imkânsız zararları doğuran hâllerden sayılmaz. (Ek cümle: 10/9/2014-6552/97 md.) Bu fıkranın üçüncü cümlesinde belirtilen işlemlerle ilgili mahkeme kararlarının yerine getirilmemesi ceza soruşturması ve kovuşturmasına konu edilemez; ancak disiplin hükümleri saklıdır.

2. (Değişik: 2/7/2012 - 6352/58 md.) Konusu belli bir miktar paranın ödenmesini gerektiren davalarda hükmedilen miktar ile her türlü davalarda hükmedilen vekalet ücreti ve yargılama giderleri, davacının veya vekilinin davalı idareye yazılı şekilde bildireceği banka hesap numarasına, bu

bildirim tarihinden itibaren, birinci fıkrada belirtilen usul ve esaslar çerçevesinde yatırılır. Birinci fıkrada belirtilen süreler içinde ödeme yapılmaması halinde, genel hükümler dairesinde infaz ve icra olunur.

3. Danıştay, bölge idare mahkemeleri, idare ve vergi mahkemeleri kararlarına göre işlem tesis edilmeyen veya eylemde bulunulmayan hallerde idare aleyhine Danıştay ve ilgili idari mahkemede maddi ve manevi tazminat davası açılabilir.

4. (Değişik: 21/2/2014-6526/18 md.) Mahkeme kararlarının süresi içinde kamu görevlilerince yerine getirilmemesi hâlinde tazminat davası ancak ilgili idare aleyhine açılabilir.

5. Vergi uyuşmazlıklarına ilişkin mahkeme kararlarının idareye tebliğinden sonra bu kararlara göre tespit edilecek vergi, resim, harçlar ve benzeri mali yükümler ile zam ve cezaların miktarı ilgili idarece mükellefe bildirilir.

6. (Değişik: 2/7/2012 - 6352/58 md.) Tazminat ve vergi davalarında idarece, mahkeme kararının tebliğ tarihi ile ödeme tarihi arasındaki süreye 21/7/1953 tarihli ve 6183 sayılı Amme Alacaklarının Tahsil Usulü Hakkında Kanununun 48 inci maddesine göre belirlenen tecil faizi oranında hesaplanacak faiz ödenir. Ancak mahkeme kararının davacıya tebliği ile banka hesap numarasının idareye bildirildiği tarih arasında geçecek süre için faiz işlemez."

2- 109. maddesiyle, 4046 sayılı Kanun'a eklenen dava konusu geçici 26. madde şöyledir:

"Geçici Madde 26- (Ek: 10/9/2014-6552/109 md.)

Bu maddenin yayımı tarihi itibarıyla devir ve teslim işlemlerinin tamamlanmasının üzerinden beş yıl geçmiş olan özelleştirmeler hakkında verilmiş olan yargı kararları ile ilgili olarak sözleşmelerinde belirtilen hâller dışında bu kuruluşların geri alınması yönünde herhangi bir işlem tesis edilmez."

3- 126. maddesiyle değiştirilen, 5651 sayılı Kanun'un dava konusu kuralı da içeren 3. maddesi şöyledir:

"Bilgilendirme yükümlülüğü

MADDE 3- (1) İçerik, yer ve erişim sağlayıcıları, yönetmelikle belirlenen esas ve usûller çerçevesinde tanıtıcı bilgilerini kendilerine ait internet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlüdür.

(2) Yukarıdaki fıkrada belirtilen yükümlülüğü yerine getirmeyen içerik, yer veya erişim sağlayıcısına Başkanlık tarafından iki bin Türk lirasından elli bin Türk lirasına kadar idarî para cezası verilir.

(3) (Ek: 6/2/2014-6518/86 md.) Bu Kanun kapsamındaki faaliyetleri yurt içinden ya da yurt dışından yürütenlere, internet sayfalarındaki iletişim araçları, alan adı, IP adresi ve benzeri kaynaklarla elde edilen bilgiler üzerinden elektronik posta veya diğer iletişim araçları ile bildirim yapılabilir.

(4) (Ek: 26/2/2014-6527/16 md.; Değişik: 10/9/2014-6552/126 md.) Trafik bilgisi Telekomünikasyon İletişim Başkanlığı tarafından ilgili işletmecilerden temin edilir ve hâkim tarafından karar verilmesi hâlinde ilgili mercilere verilir.

4- 127. maddesiyle değiştirilen, 5651 sayılı Kanun'un dava konusu kuralları da içeren 8. maddesi şöyledir:

"Erişimin engellenmesi kararı ve yerine getirilmesi

MADDE 8- (1) İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir:

a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;

1) İntihara yönlendirme (madde 84),

2) Çocukların cinsel istismarı (madde 103, birinci fıkra),

3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),

4) Sağlık için tehlikeli madde temini (madde 194),

5) Müstehcenlik (madde 226),

6) Fuhuş (madde 227),

7) Kumar oynanması için yer ve imkân sağlama (madde 228),

suçları.

b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

(2) Erişimin engellenmesi kararı, soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme tarafından verilir.

Soruşturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da erişimin engellenmesine karar verilebilir. Bu durumda Cumhuriyet savcısı kararını yirmidört saat içinde hâkimin onayına sunar ve hâkim, kararını en geç yirmidört saat içinde verir. Bu süre içinde kararın onaylanmaması halinde tedbir, Cumhuriyet savcısı tarafından derhal kaldırılır. (Ek cümle: 6/2/2014-6518/92 md.) Erişimin engellenmesi kararı, amacı gerçekleştirecek nitelikte görülürse belirli

bir süreyle sınırlı olarak da verilebilir. Koruma tedbiri olarak verilen erişimin engellenmesine ilişkin karara 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz edilebilir.

(3) Hâkim, mahkeme veya Cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararının birer örneği, gereği yapılmak üzere Başkanlığa gönderilir.

(4) İçeriği birinci fıkrada belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulursa bile, içeriği birinci fıkranın (a) bendinin (2) ve (5) ve (6) numaralı alt bentlerinde yazılı suçları oluşturan yayınlara ilişkin olarak erişimin engellenmesi kararı re'sen Başkanlık tarafından verilir. Bu karar, erişim sağlayıcısına bildirilerek gereğinin yerine getirilmesi istenir.

(5) Erişimin engellenmesi kararının gereği, derhal ve en geç kararın bildirilmesi anından itibaren dört saat içinde yerine getirilir.

(6) Başkanlık tarafından verilen erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi halinde, Başkanlık tarafından, Cumhuriyet başsavcılığına suç duyurusunda bulunulur.

(7) Soruşturma sonucunda kovuşturmaya yer olmadığı kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda Cumhuriyet savcısı, kovuşturmaya yer olmadığı kararının bir örneğini Başkanlığa gönderir.

(8) Kovuşturma evresinde beraat kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda mahkemece beraat kararının bir örneği Başkanlığa gönderilir.

(9) Konusu birinci fıkrada sayılan suçları oluşturan içeriğin yayından çıkarılması halinde; erişimin engellenmesi kararı, soruşturma evresinde Cumhuriyet savcısı, kovuşturma evresinde mahkeme tarafından kaldırılır.

(10) Koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen yer veya erişim sağlayıcılarının sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır.

(11) İdarî tedbir olarak verilen erişimin engellenmesi kararının yerine getirilmemesi halinde, Başkanlık tarafından erişim sağlayıcısına, onbin Yeni Türk Lirasından yüzbin Yeni Türk Lirasına kadar idarî para cezası verilir. İdarî para cezasının verildiği andan itibaren yirmidört saat içinde kararın yerine getirilmemesi halinde ise Başkanlığın talebi üzerine Kurum tarafından yetkilendirmenin iptaline karar verilebilir.

(12) Bu Kanunda tanımlanan kabahatler dolayısıyla Başkanlık veya Kurum tarafından verilen idarî para cezalarına ilişkin kararlara karşı, 6/1/1982 tarihli ve 2577 sayılı İdarî Yargılama Usulü Kanunu hükümlerine göre kanun yoluna başvurulabilir.

(13) (Ek: 5/11/2008-5809/67 md.) İşlemlerin yürütülmesi için Başkanlığa gönderilen hakim ve mahkeme kararlarına 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre Başkanlıkça itiraz edilebilir.

(14) (Ek: 12/7/2013-6495/47 md.) 14/3/2007 tarihli ve 5602 sayılı Şans Oyunları Hasılatından Alınan Vergi, Fon ve Payların Düzenlenmesi Hakkında Kanununun 3 üncü maddesinin birinci fıkrasının (ç) bendinde tanımlanan kurum ve kuruluşlar, kendi görev alanına giren suçların internet ortamında işlendiğini tespit etmeleri hâlinde, bu yayınlarla ilgili olarak erişimin engellenmesi kararı alabilirler. Erişimin engellenmesi kararları uygulanmak üzere Telekomünikasyon İletişim Başkanlığına gönderilir.

(15) (Ek: 26/2/2014-6527/17 md.) Bu maddeye göre soruşturma aşamasında verilen hâkim kararı ile 9 uncu ve 9/A maddesine göre verilen hâkim kararı birden fazla sulh ceza mahkemesi bulunan yerlerde Hâkimler ve Savcılar Yüksek Kurulu tarafından belirlenen sulh ceza mahkemeleri tarafından verilir.

(16) (Ek: 10/9/2014-6552/127 md.) Millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi nedenlerinden bir veya bir kaçına bağlı olarak gecikmesinde sakınca bulunan hâllerde, erişimin engellenmesi Başkanın talimatı üzerine Başkanlık tarafından yapılır. Erişim sağlayıcıları Başkanlıktan gelen erişimin engellenmesi taleplerini en geç dört saat içinde yerine getirir. Başkan tarafından verilen erişimin engellenmesi kararı, Başkanlık tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar."

B- Dayanılan Anayasa Kuralları

Dava dilekçesinde, Anayasa'nın 2., 10., 13., 20., 22., 26., 28., 36., 40., 125. ve 138. maddelerine dayanılmıştır.

III- İLK İNCELEME

Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Haşim KILIÇ, Serruh KALELİ, Alparslan ALTAN, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT, Zehra Ayla PERKTAŞ, Recep KÖMÜRCÜ, Burhan ÜSTÜN, Engin YILDIRIM, Nuri NECİPOĞLU, Hicabi DURSUN, Erdal TERCAN, Muammer TOPAL, Zühtü ARSLAN, M. Emin KUZ ve Hasan Tahsin GÖKCAN'ın katılımlarıyla 25.9.2014 gününde yapılan ilk inceleme toplantısında, dosyada eksiklik bulunmadığından işin esasının incelenmesine,

yürürlüğü durdurma isteminin ise esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

IV- ESASIN İNCELENMESİ

Dava dilekçesi ve ekleri, Raportör Erhan TUTAL tarafından hazırlanan işin esasına ilişkin rapor, iptali istenilen yasa kuralları, dayanan Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A- Kanun'un 97. Maddesiyle, 2577 sayılı Kanun'un 28. Maddesinin (1) Numaralı Fıkrasının Değiştirilen Üçüncü Cümlesinin ".23/4/1981 tarihli ve 2451 sayılı Bakanlıklar ve Bağlı Kuruluşlarda Atama Usulüne İlişkin Kanuna ekli (1) ve (2) sayılı cetvellerde gösterilen unvanları taşıyan görevler ile farklı atama usullerine tabi olsalar dâhi daire başkanı ve üstü görevlere, sivil memurlar hariç kolluk teşkilatlarının kadrolarına; açıktan, naklen veya vekâleten yapılan atama ve bu görevlerden alınma, bu görevlerle ilgili yer değiştirme, görev ve unvan değişikliği işlemleri hakkında verilen mahkeme kararlarının gereği, ilgilinin kazanılmış hak aylık derecesine uygun başka bir kadroya atanması suretiyle iki yıl içinde yerine getirilir." Bölümünün İncelenmesi

Dava dilekçesinde, Anayasa'ya göre mahkeme kararlarının aynen ve geciktirilmeksizin uygulanmasının zorunlu olduğu, dava konusu düzenleme ile aynen uygulanması gereken mahkeme kararlarının iki yıl içinde ve değiştirilerek uygulanmasının öngörüldüğü, yargı kararlarının uygulanmasının herhangi bir şarta bağlanmaksızın idareler açısından bağlayıcı olduğu ve bu kararların derhal uygulanması gerektiği belirtilerek kuralın, Anayasa'nın 2., 36., 125. ve 138. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kural, 2451 sayılı Kanun'a ekli (1) ve (2) sayılı cetvellerdeki unvanlı görevler ile atama usulleri farklı olsa da daire başkanı ve üstü görevlere, kolluk teşkilatlarının kadrolarına (sivil memurlar hariç), açıktan, naklen veya vekâleten yapılan atama ve bu görevlerden alınma, bu görevlerle ilgili yer değiştirme, görev ve unvan değişikliği işlemleri hakkında verilen mahkeme kararlarının gereğinin iki yıl içinde ve kazanılmış hak aylık derecesine uygun başka bir kadroya atanma suretiyle yerine getirileceğini düzenlemektedir.

Anayasa'nın 2. maddesinde, Türkiye Cumhuriyeti'nin bir hukuk devleti olduğu belirtilmiştir. Hukuk devleti, eylem ve işlemleri hukuka uygun olan, insan haklarına saygılı, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adil bir hukuk düzeni kurup bunu geliştirerek sürdüren, Anayasa'ya aykırı durum ve tutumlardan kaçınan, hukukun üstün kurallarıyla kendini bağlı sayan ve yargı denetimine açık olan devlettir.

Hukuk devletinde kişilerin temel hak ve özgürlüklerinin sağlanması ve korunması esas olduğundan, kişilere etkili hak arama imkânı sağlayan güvencelerin de tanınması gerekmektedir. Bu çerçevede Anayasa'nın "Hak arama hürriyeti" başlıklı 36. maddesinin birinci fıkrasında, "Herkes, meşru vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir." denilerek, herkese, adaleti bulma, hakkı olanı elde etme ve haksızlığı giderme imkânı sağlanmıştır. Böylece kişilerin hukuki güvenlikleri etkin bir koruma mekanizmasına kavuşturulmuştur. Mahkeme kararlarının değiştirilememesi, yasamanın ve yürütmenin kesinleşmiş yargı kararlarıyla oluşmuş hukuksal durumlara dokunamaması ya da bunları ortadan kaldıramaması hukuk devletinin temel ilkelerindedir. Nitekim, Anayasa'nın 138. maddesinin son fıkrasında da "Yasama ve yürütme organları ile idare, mahkeme kararlarına uymak zorundadır; bu organlar ve idare, mahkeme kararını hiçbir suretle değiştiremez ve bunların yerine getirilmesini geciktiremez." hükmüne yer verilmiştir. Bu nedenle, davaya taraf olan kişinin anayasal güvencelerinin etkin olarak korunması ve hukuka uygunluğun sağlanması için, idarenin kendisi hakkında verilen nihai yargı kararlarına uyması gerekmektedir.

Adaletle olan inancın ve güven duygusunun sarsılması, Devletin temeli sayılan adaleti koruyan ve sağlamakla görevli yargı organını işlevsiz hâle getirecek, yargı kararının bağlayıcılık ifade etmemesi algısı yaratıldığında ise idareye keyfi davranış sergileme imkânı verilmiş olacaktır.

Bir uyuşmazlığı mahkeme önüne götürme, mahkemece verilen kararın uygulanmasını isteme, yargılamanın sonuç doğurmasını sağlayan hak arama hürriyetinin olmazsa olmaz koşuludur. Hak arama özgürlüğünün bir gereği olan mahkemeye erişim hakkı, yargılama sonunda verilen kararın etkili bir şekilde aynen ve gecikmeksizin uygulanmasını da gerektirmektedir. Mahkeme kararlarını uygulanamaz hâle getiren düzenlemeler, mahkemeye erişim hakkını da anlamsız kılacaktır.

Kişilerin, Devlete güven duymaları, maddi ve manevi varlıklarını geliştirebilmeleri, temel hak ve özgürlüklerden yararlanabilmeleri ancak hukuk güvenliği ve üstünlüğünün sağlandığı bir hukuk düzeninde gerçekleşebilir. Hukuk güvenliğinin ve hukukun üstünlüğünün sağlanması için Devletin işlem ve eylemlerine karşı yargı yolunun açık tutulması yeterli olmayıp yargı mercileri tarafından verilen kararların gecikmeksizin uygulanması da gerekir. Bir işlemin hukuka aykırı olduğu yapılan yargısal denetim neticesinde tespit edilmesine rağmen işlemin iptali yönündeki yargısal kararın uygulanmaması, Devletin işlem ve eylemlerine karşı yargı yolunun açık tutulmasını anlamsız hâle getirir. Zira hukuk güvenliği ve hukukun üstünlüğü sadece hukuka aykırılıkların tespit edilmesiyle değil, bunların tüm sonuçlarıyla ortadan kaldırılmasıyla sağlanabilir. Mahkeme kararlarının

bağlayıcılığını ve gecikmeksizin uygulanmasını sağlayacak etkili tedbirlerin alınması hukuk devletinin asgari gereklerindedir.

Bilindiği gibi idari yargıdaki iptal kararları, işlemin tesis edildiği tarihten önceki hukuki durumun geçerliliğini sağlamaktadır. Başka bir ifadeyle idari yargı mercilerince verilen iptal kararlarının dava konusu işlem üzerinde biri, davaya konu idari işlemle ona bağlı olarak tesis edilen diğer işlemlerin yapıldıkları tarihten itibaren geçerli olarak ortadan kaldırılması; diğeri işlemin tesisinden önceki hukuki durumun geri gelmesi ve böylece hukuk düzeninin hiç bozulmamış hâle getirilmesi olmak üzere iki tür etkisi vardır.

Dava konusu kuralda, birtakım unvanlı görevler ile kolluk teşkilatlarının (sivil memurlar hariç) kadroları hakkında tesis edilen atama, görevden alma gibi bazı idari işlemler hakkında verilen yargı kararlarının uygulanması için ilgilinin iki yıl içinde başka bir kadroya atanmasına ilişkin düzenlemeler getirilmektedir. Böylece, anılan işlemlere ilişkin uygulamalar sonucunda verilen yargı kararlarının ilgili idarelerce aynen ve gecikmeksizin yerine getirilmesinin yolu kapatılmış ve söz konusu kişiler hakkında idari yargı mercilerince verilmiş olan mahkeme kararlarının sonuçsuz kalmasının yolu açılmıştır.

Hak arama özgürlüğü bakımından kişilerin idareye karşı sahip oldukları en etkili yargısal koruma mekanizması iptal davasıdır. İptal davasında, idari işlemin hukuk kurallarına aykırılığının belirlenmesi hâlinde iptali yoluna gidilmekte ve bunun sonucunda idarenin hukuka bağlılığı ve hukuk düzeninin korunması sağlanmaktadır. Bu bağlamda hak arama yollarına başvuran bireylerin elde etmek istedikleri hukuki sonuçların yasama tasarruflarıyla etkisizleştirilmesi, Devlete olan güven duygusunu ortadan kaldırmaktadır. Bu durum hak arama özgürlüğüne, hukuki güvenlik ve hukuk devleti ilkelerine uygun düşmemektedir.

İdarenin, mahkeme kararlarını yerine getirmesi, Anayasa'nın 138. maddesinde öngörülen bağlayıcılık ilkesi gereği temel bir ödevi olup kararları geciktirme ya da uygulamama gibi bir tercih hakkı bulunmamaktadır.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 36. ve 138. maddelerine aykırıdır. İptali gerekir.

Kural, Anayasa'nın 2., 36. ve 138. maddelerine aykırı görülerek iptal edildiğinden dolayı Anayasa'nın 125. maddesi yönünden ayrıca incelenmesine gerek görülmemiştir.

B- Kanun'un 97. Maddesiyle, 2577 sayılı Kanun'un 28. Maddesinin (1) Numaralı Fıkrasının Değiştirilen Dördüncü Cümlesinin İncelenmesi

Dava dilekçesinde, idari yargı mercilerince yürütmenin durdurulması kararı verilmesi için Anayasa'da öngörülen şartlardan birinin kanun koyucu tarafından yokluğunun peşinen kabul edilmesi suretiyle belli konulara ilişkin yürütmenin durdurulması kararı verilmesinin engellendiği ve böylece hak arama hürriyeti ile yargısal denetimin kısıtlandığı belirtilerek kuralın, Anayasa'nın 2., 10., 36., 125. ve 138. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kural, 2451 sayılı Kanun'a ekli (1) ve (2) sayılı cetvellerdeki unvanlı görevler ile atama usulleri farklı olsa da daire başkanı ve üstü görevlere ve kolluk teşkilatlarının kadrolarına (sivil memurlar hariç) ilişkin her türlü atama, görevden alınma veya görev ve unvan değişikliği işlemlerinin uygulanmasının telafisi güç veya imkânsız zarar doğuran hâllerden sayılamayacağını düzenlemektedir.

Hak arama özgürlüğü bakımından kişilerin idareye karşı sahip oldukları en etkili yargısal koruma mekanizması iptal davasıdır. İptal davasında, idari işlemin hukuk kurallarına aykırılığının belirlenmesi hâlinde iptali yoluna gidilmekte ve bunun sonucunda idarenin hukuka bağlılığı ve hukuk düzeninin korunması sağlanmaktadır. Genel ilke, iptal kararlarının geriye yürütülmesi ve iptal edilen işlemi başından itibaren ortadan kaldırması, bu işleme ve ona dayanan sonuçların hiç mevcut olmamış gibi kabul edilmesi olmakla birlikte, bu ilke, idari işlemin iptal kararı verilinceye kadar mevcudiyetini sürdürmesine ve etki doğurmasına engel değildir. Bu nedenle, kişileri iptal davası sonuçlanıncaya kadar hukuka aykırı idari işlemin olumsuz etkilerinden korumak, ileride giderilmesi veya düzeltilmesi imkânsız veya zor olan durumları önlemek, idarenin hem olası bir tazmin yükünden kurtarılması hem de hukuk sınırları içinde kalması sağlanarak hukuk devletinin kesintiye uğramadan devamını temin etmek amacıyla yürütmenin durdurulması kurumu öngörülmüştür.

Yürütmenin durdurulması kurumu, yargının denetim etkinliğini artırıcı bir araç olarak dava hakkının bir parçasını oluşturduğu gibi kamu yararı ve kamu düzenini de sağlamaktadır. Yürütmenin durdurulması kararı ile dava konusu olan işlemin yapıldığı andan önceki durumun geri gelmesi sağlanmakta ve kişiler dava sonuçlanıncaya kadar bu işlemin olumsuz etkilerinden korunmaktadır.

Anayasa'nın 125. maddesinin birinci fıkrasında, "İdarenin her türlü eylem ve işlemlerine karşı yargı yolu açıktır." denilerek etkili bir yargı denetimi amaçlanmıştır. Çünkü yargı denetimi hukuk devletinin olmazsa olmaz koşuludur. Bu kural, idarenin kamu hukuku ya da özel hukuk alanına giren tüm eylem ve işlemlerini kapsamaktadır. Anayasa'nın 125. maddesinin beşinci fıkrasında, idari işlemin uygulanması hâlinde telafisi güç veya imkânsız zararların doğması ve idari işlemin açıkça hukuka aykırı olması şartlarının birlikte gerçekleşmesi durumunda gerekçe gösterilerek yürütmenin

durdurulmasına karar verilebileceği; altıncı fıkrasında ise yürütmenin durdurulması kararı verilmesinin olağanüstü hal, sıkıyönetim, seferberlik ve savaş hâli ile milli güvenlik, kamu düzeni ve genel sağlık nedenlerine bağlı olarak kanunla sınırlanabileceği hükme bağlanmıştır. Ancak, Anayasa'nın 125. maddesinin altıncı fıkrasında belirtilen nedenlerden birine dayanılması, kanun koyucuya, yürütmenin durdurulması kararı verilmesine istisna getirme konusunda sınırsız yetki vermez. Zira Anayasa'nın 125. maddesinin beşinci fıkrası gereğince yürütmenin durdurulması kararı, idari işlemin açıkça hukuka aykırı olması ve uygulanması hâlinde telafisi güç veya imkânsız zararların doğması şartlarının birlikte gerçekleşmesi durumunda verilebilecektir.

Dava konusu kuralda belirtilen işlemlerin diğer idari işlemlerden farklı bir özelliğinin bulunmaması ve Anayasa'nın 125. maddesinin beşinci fıkrası gereğince yürütmenin durdurulması kararının idari işlemin açıkça hukuka aykırı olması ve uygulanması hâlinde telafisi güç veya imkânsız zararların doğması şartlarının birlikte gerçekleşmesi durumunda verilebilmesi göz önüne alındığında, bazı işlemlerin telafisi güç veya imkânsız zarar doğurmayacağına peşinen kabulü suretiyle yürütmenin durdurulması kararı verilmesinin engellenmesinin kamu yararı ve kamu düzenini korumayacağı açıktır. Kamu düzeni, hukukun dışlandığı, yargının etkisiz kaldığı yerde daha çok bozulur.

Dava konusu kural, idarece tesis edilen bazı işlemlerin, ilgilileri hakkında telafisi güç veya imkânsız zarar doğuran hâllerden sayılmayacağını düzenlemektedir. Böylece yürütmenin durdurulması kararı verilebilmesi için gerekli koşullardan birisi olan "telafisi güç veya imkânsız zarar doğmak" şartı kanun koyucu tarafından yok sayılmakta, dolayısıyla idari yargı yerlerinde yürütmenin durdurulması kararı verilmesi engellenmektedir. Kural uyarınca, yürütmenin durdurulması yetkisinin kullanılmasının engellenmesi bu yetkinin Anayasa'nın 125. maddesinin altıncı fıkrasında öngörülen biçimde sınırlanması sebeplerini aşan, hakkın özünü zedeleyen bir durum olduğu gibi idari yargının en güçlü araçlarından birinin elinden alınması suretiyle yargısal denetimin kısıtlanmasına da yol açmaktadır.

İdari işlemin uygulanmasıyla telafisi güç veya imkânsız zararların doğacağı durumlarda, yürütmenin durdurulması kararı verilebilmesi, kişilerin hak arama özgürlüklerini etkili biçimde kullanabilmelerini sağlayan önemli bir imkân olup bu imkânı ortadan kaldıran veya etkisiz hâle getiren bir düzenleme, Anayasa'nın 36. maddesinde yer alan hak arama özgürlüğüne aykırılık teşkil edecektir.

Belirtilen hususlar dikkate alındığında, dava konusu kuralla, bireylerin, hak arama özgürlüklerini daha etkili biçimde kullanabilmelerini sağlayan yürütmeyi durdurma kurumundan Anayasa'ya aykırı olarak yoksun bırakıldıkları sonucuna varılmaktadır.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 36. ve 125. maddelerine aykırıdır. İptali gerekir.

Kural, Anayasa'nın 2., 36. ve 125. maddelerine aykırı görülerek iptal edildiğinden dolayı, Anayasa'nın 10. ve 138. maddeleri yönünden ayrıca incelenmesine gerek görülmemiştir.

C- Kanun'un 97. Maddesiyle, 2577 sayılı Kanun'un 28. Maddesinin (1) Numaralı Fıkrasına Eklenen Cümlelerin "Bu fıkranın üçüncü cümlesinde belirtilen işlemlerle ilgili mahkeme kararlarının yerine getirilmemesi ceza soruşturması ve kovuşturmasına konu edilemez;" Bölümünün İncelenmesi

Dava dilekçesinde, yargı kararlarının idareler açısından bağlayıcı olduğu ve hiçbir suretle değiştirilemeyeceği gibi yerine getirilmelerinin de geciktirilemeyeceği, kararların uygulanmasının herhangi bir şarta bağlanamayacağı, uygulamamanın suç olduğu, bir kısım mahkeme kararlarının uygulanması zorunlu iken bazı kararların uygulanmamasının suç olmaktan çıkarılması suretiyle kanun önünde eşitsizlik oluşturulduğu, hiçbir kişiye imtiyaz tanınamayacağı belirtilerek kuralın, Anayasa'nın 2., 10. ve 125. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kural ile 2451 sayılı Kanun'a ekli (1) ve (2) sayılı cetvellerdeki unvanlı görevler ile atama usulleri farklı olsa da daire başkanı ve üstü görevlere ve kolluk teşkilatlarının kadrolarına (sivil memurlar hariç) ilişkin her türlü atama, görevden alınma veya görev ve unvan değişikliği işlemleri ile ilgili mahkeme kararlarının gereğinin yerine getirilmemesinin ceza soruşturması ve kovuşturmasına konu edilemeyeceği düzenlenmektedir. Başka bir ifadeyle anılan işlemlere ilişkin yargı kararlarını yerine getirmeyen kamu görevlilerinin ceza soruşturması ve kovuşturmasına konu edilmesi yasaklanmaktadır.

Anayasa'nın 125. maddesinin birinci fıkrasında, "İdarenin her türlü eylem ve işlemlerine karşı yargı yolu açıktır." denilerek etkili bir yargı denetimi amaçlanmıştır. Çünkü yargı denetimi hukuk devletinin olmazsa olmaz koşuludur. Mahkeme kararlarının uygulanması da, yargılama sürecini tamamlayan ve yargılamanın sonuç doğurmasını sağlayan bir unsurdur. Kararın uygulanmaması hâlinde yargılamanın da bir anlamı kalmayacaktır.

Yargı kararlarının uygulanması "mahkemeye erişim hakkı" kapsamında değerlendirilmektedir. Buna göre, yargılama sonucunda mahkemenin bir karar vermiş olması yeterli olmayıp ayrıca bu kararın etkili bir şekilde uygulanması da gerekir. Hukuk sisteminde, nihai mahkeme kararlarını, taraflardan birinin aleyhine sonuç doğuracak şekilde uygulanamaz hâle getiren düzenlemeler bulunması veya

mahkeme kararlarının icrasının herhangi bir şekilde engellenmesi hâllerinde, "mahkemeye erişim hakkı" da anlamını yitirir.

Yargı kararının geciktirilmeksizin uygulanması, Anayasa'nın 138. maddesinin dördüncü fıkrasında mahkemelerin bağımsızlığının bir parçası olarak görülmekte ve Devlete yargı kararlarını değiştirmeden ve geciktirmeden uygulama yükümlülüğü getirilmektedir.

Anayasa'nın 138. maddesinde mahkeme kararlarına uyma, bu kararları değiştirmeksizin yerine getirme hususunda yasama ve yürütme organları ile idare makamları lehine herhangi bir istisna kuralına yer verilmemiştir. Yargı kararlarının ilgili kamu otoritelerince zamanında yerine getirilmediği bir devlette, bireylerin yargı kararıyla kendilerine sağlanan hak ve özgürlükleri tam anlamıyla kullanabilmeleri mümkün olmaz. Dolayısıyla devlet, yargı kararlarının zamanında icra edilmesini sağlayarak bireyler aleyhine oluşabilecek hak kayıplarını engellemekle ve bu yolla bireylerin kamu otoritelerine ve hukuk sistemine olan güven ve saygılarını korumakla yükümlüdür. Bu sebeple hukukun üstünlüğünün geçerli olduğu bir devlette, bireylerin kamu otoritesi ve hukuk sistemine olan güven ve saygılarını koruma adına vazgeçilemez bir görev ifa eden yargı kararlarının zamanında icra edilmeyerek, sonuçsuz bırakılması kabul edilemez.

Kesin hükme saygı ilkesi, uluslararası hukuk düzenine özgü hukukun genel ilkelerinden biri olarak kabul görmektedir. Anayasa'nın 138. maddesinin son fıkrasında düzenlenen yargı kararlarının geciktirilmeksizin uygulanması yükümlülüğü, hukukun genel ilkelerinden biri olarak da kabul edilen kesin hükme saygı ilkesinin de bir gereğidir. Çünkü bir hukuk sisteminde yargının verdiği ve bağlayıcı olan kesin hüküm zarar gören taraflardan biri açısından işlevsiz duruma getirilmişse, adil yargılanma hakkının sağladığı güvencelerin bir anlamı kalmayacaktır.

Dava konusu kuralda, fıkranın üçüncü cümlesinde belirtilen işlemlere ilişkin olarak verilen yargı kararlarının gereğinin yerine getirilmemesinin ceza soruşturması ve kovuşturmasına konu edilemeyeceği düzenlenerek mahkeme kararlarının uygulanması zorunluluğu bertaraf edilmekte; konusu suç oluşturan bir fiilin cezasız bırakılmasına olanak sağlanmaktadır. Bu bağlamda kural, 2577 sayılı Kanun'un 28. maddesinin (1) numaralı fıkrasının üçüncü cümlesinde yer alan mahkeme kararlarının uygulanması ile yakından ilgili olup 2577 sayılı Kanun'un 28. maddenin (1) numaralı fıkrasının üçüncü cümlesinin Anayasa'ya uygunluğu bakımından yapılan değerlendirmeler ve varılan sonuç, dava konusu kural yönünden de geçerlidir.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 125. ve 138. maddelerine aykırıdır. İptali gerekir.

Kural, Anayasa'nın 2., 125. ve 138. maddelerine aykırı görülerek iptal edildiğinden dolayı, Anayasa'nın 10. maddesi yönünden ayrıca incelenmesine gerek görülmemiştir.

D- Kanun'un 109. Maddesiyle, 4046 sayılı Kanun'a Eklenen Geçici 26. Maddenin İncelenmesi

Dava dilekçesinde, özelleştirme uygulamaları sona eren kuruluşlar hakkında verilen yargı kararlarının uygulanmasına yönelik olarak tesis edilecek işlemler konusunda Bakanlar Kuruluna yetki verilmesini öngören kuralın Anayasa Mahkemesince iptal edilmesine rağmen aynı nitelikteki düzenlemenin tekrar getirildiği, yargı kararlarının uygulanmasının zorunlu olduğu, adli veya idari yargı mercilerince verilmiş olan mahkeme kararlarının sonuçsuz kalmasının yolunun açıldığı belirtilerek kuralın, Anayasa'nın 2., 125. ve 138. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kural ile düzenlemenin yayımı tarihi itibarıyla devir ve teslim işlemlerinin tamamlanmasının üzerinden beş yıl geçmiş olan özelleştirmeler hakkında verilmiş olan yargı kararları ile ilgili olarak sözleşmelerinde belirtilen hâller dışında bu kuruluşların geri alınması yönünde herhangi bir işlem tesis edilemeyeceği öngörülmektedir.

Dava konusu kuralda, devir ve teslim işlemlerinin tamamlanmasının üzerinden beş yıl geçmiş olan özelleştirmeler hakkında verilmiş olan geri almaya ilişkin yargı kararlarının uygulanmamasına dair düzenleme getirilmektedir. Bu bağlamda kural, 2577 sayılı Kanun'un 28. maddesinin (1) numaralı fıkrasının üçüncü cümlesinde yer alan mahkeme kararlarının uygulanması ile ilgili olduğundan 2577 sayılı Kanun'un 28. maddenin (1) numaralı fıkrasının üçüncü cümlesi ile aynı fıkranın son cümlesinin Anayasa'ya uygunluğu bakımından yapılan değerlendirmeler ve varılan sonuç, dava konusu kural yönünden de geçerlidir.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 125. ve 138. maddelerine aykırıdır. İptali gerekir.

E- Kanun'un 126. Maddesiyle Değiştirilen, 5651 sayılı Kanun'un 3. Maddesinin (4) Numaralı Fıkrasının İncelenmesi

Dava dilekçesinde, trafik bilgileri temin edilecek olan ilgili işletmeciler ile trafik bilgileri kendilerine verilecek olan ilgili mercilerin hangileri olduğunun somut bir biçimde belirtilmediği, trafik bilgilerinin temini ve verilmesi konusunda kapsamı ve mâhiyeti değişebilen sınırları belirsiz, muğlâk, ucu-açık ve geniş yetkiyle hukuki belirsizlik oluşturulduğu, Telekomünikasyon İletişim Başkanlığı (TİB) tarafından herhangi bir ihbar, iddia, şikâyet, talep ya da başvuru olmaksızın trafik bilgilerinin ilgili mercilerden temin edilmesinin yolunun açıldığı, özel hayatın gizliliği ve korunması ilkesinin ihlal edildiği, kişisel bilgilerin ilgilinin açık rızası olmaksızın veya kanunda açıkça belirtilen hâller

haricinde işlenemeyeceği, temel hak ve hürriyetlerin ölçüsüzce sınırlandırıldığı belirtilerek kuralın, Anayasa'nın 2., 13. ve 20. maddelerine aykırılığı ileri sürülmüştür.

Dava konusu kural, internet trafik bilgisinin TİB tarafından ilgili işletmecilerden herhangi bir hukuki inceleme ya da sürece dahil olmadan alınmasını ve hâkim tarafından karar verilmesi durumunda bu bilginin ilgili mercilere verilmesini düzenlemektedir.

Anayasa'nın 20. maddesinin ilk fıkrasında, herkesin, özel hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş; son fıkrasında da "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." denilerek kişisel verilerin korunması, özel hayatın gizliliğinin korunması kapsamında güvenceye kavuşturulmuştur.

Kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvencenin yaşama geçirilebilmesi için, bu hakkı ilgilendiren yasal düzenlemelerin, açık, anlaşılabilir ve kişilerin söz konusu haklarını kullanabilmelerine elverişli olması gerekir. Ancak böyle bir düzenleme ile kişilerin özel hayatlarını ilgilendiren veri, bilgi ve belgelerin resmi makamların keyfi müdahalelerine karşı korunması olanaklı hâle getirilebilir.

Anayasa'nın 13. maddesinde, temel hak ve hürriyetlerin, özlere dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği, bu sınırlamaların Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacağı belirtilmiştir.

Çağdaş demokrasiler, temel hak ve özgürlüklerin en geniş ölçüde sağlanıp güvence altına alındığı rejimlerdir. Temel hak ve özgürlükleri büyük ölçüde kısıtlayan ve kullanılamaz hâle getiren sınırlamalar hakkın özüne dokunur. Temel hak ve özgürlüklere getirilen sınırlamaların yalnız ölçüsü değil, koşulları, nedeni, yöntemi, kısıtlamaya karşı öngörülen kanun yolları gibi güvenceler hep demokratik toplum düzeni kavramı içinde değerlendirilmelidir. Bu nedenle, temel hak ve özgürlükler, istisnai olarak ve ancak özüne dokunmamak koşuluyla demokratik toplum düzeninin gerekleri için zorunlu olduğu ölçüde ve ancak kanunla sınırlandırılabilirler.

Özel hayatın korunması her şeyden önce bu hayatın gizliliğinin korunması, başkalarının gözleri önüne serilmemesi demektir. Kişinin özel hayatında yaşananların, yalnız kendisi veya kendisinin

bilmesini istediği kimseler tarafından bilinmesini isteme hakkı, kişinin temel haklarından biridir ve bu niteliği nedeniyle insan haklarına ilişkin beyanname ve sözleşmelerde yer almış, tüm demokratik ülkelerin mevzuatlarında açıkça belirlenen istisnalar dışında devlete, topluma ve diğer kişilere karşı korunmuştur.

Nitekim, İnsan Hakları Evrensel Bildirisi'nin 12. maddesinde "Hiç kimse özel hayatı, ailesi, konutu veya yazışması konusunda, keyfî karışmalara, şeref ve şöhretine karşı saldırılara maruz bırakılamaz. Herkesin bu saldırı ve karışmalara karşı yasa ile korunmaya hakkı vardır."; Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde de, "1. Herkes özel hayatına ve aile hayatına saygı gösterilmesi hakkına sahiptir; 2. Bu hakkın kullanılmasında bir kamu otoritesi tarafından müdahale, demokratik bir toplumda ancak ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, dirlik ve düzenliğin korunması, suç işlenmesinin önlenmesi, sağlığın ve ahlâkın veya başkalarının hak ve özgürlüklerinin korunması için zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir." denilerek özel yaşamın dokunulmazlığı sağlanmıştır.

Dava konusu kuralda geçen trafik bilgisi, 5651 sayılı Kanun'un 2. maddesinin (j) bendinde, taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgileri şeklinde tanımlanmıştır. Dolayısıyla trafik bilgisi adı altında istenen bilgiler genel anlamda belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade eden kişisel veri kavramı içerisindedir. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır.

AİHM kararlarında da belirtildiği gibi, özel hayat bütün unsurlarıyla tanımlanamayacak kadar geniş bir kavram olup devletin yetkili temsilcileri tarafından ilgililer hakkında rızası olmaksızın bilgi toplamasının her zaman söz konusu kişinin özel hayatını ilgilendireceği kuşkusuzdur.

Dava konusu kural, yukarıda belirtilen kişisel veri niteliğinde olan ve ciddi suçların tespiti, soruşturulması ve kovuşturulmasında kullanılmak üzere gerçek ve tüzel kişilere ilişkin trafik bilgisinin, işlenmemiş veri hâlinde süreli olarak muhafaza edildiği erişim veya yer sağlayıcılardan, TİB tarafından herhangi bir gerekçe veya neden göstermeksizin temin edilmesine olanak sağlamaktadır. Söz konusu verilere ulaşılabilirlik, kişilerin tercihleri, düşünceleri ve davranışları hakkında fikir verebileceğinden kişilerin özel hayatlarına müdahale edilme riskini içermektedir. Kuralda, temin edilecek bilgiyle ilgili olarak herhangi bir konu ve amaç sınırlaması bulunmadığı gibi bilginin kapsamı, ne şekilde kullanılacağı, tutulacağı süre, temin edilme gerekçesi gibi hususlarla ilgili olarak da herhangi bir belirlilik bulunmamaktadır.

Anayasa'nın 20. maddesi, kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvenceyi, kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği şeklinde belirtmiştir. Dolayısıyla bu hakkı ilgilendiren yasal düzenlemelerin, çerçevesi çizilmiş, açık, anlaşılabilir, kişilerin söz konusu haklarını kullanabilmelerine elverişli ve özel hayatlarını ilgilendiren veri, bilgi ve belgelerin resmi makamların keyfi müdahalelerine karşı korunmasını olanaklı hâle getirilmesi gerekmektedir. Bu durumda, verilerin işlenebileceği hâllerin kanunda açıkça yer alması zorunluluğu bulunmasına karşın, kuralda herhangi bir belirleme ve sınırlama yapılmaksızın doğrudan kişisel veri niteliğindeki trafik bilgisinin temin edilmesine ve işlenmesine olanak sağlanmasının bu yönüyle Anayasa'nın 20. maddesine aykırı olduğu açıktır.

Trafik bilgisi adı altında temin edilecek olan bilgiler Anayasa ile teminat altına alınan iletişimin gizliliği, düşünce ve ifadeyi yayma özgürlüğü, haberleşme özgürlüğü, kişisel verilerin korunması gibi birçok temel hakla doğrudan ilgili olup bu bilgilerin TİB tarafından herhangi bir kurala ve sınırlamaya tabi olmaksızın istenildiği zaman ve şekilde elde edilebilir olması temel hak ve özgürlüklerin doğrudan ihlaline sebebiyet vermektedir.

Anayasa'nın 13. ve 20. maddelerinde yer alan güvencele rağmen dava konusu kural ile kişiler, bilgi toplama, saklama, işleme ve değiştirme yetkisi olan idareye ve diğer kişilere karşı korumasız bırakılmış, veri toplamanın amaç, gerekçe, kapsam ve sınırlarına yasal düzenlemede yer verilmemiştir.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 13. ve 20. maddelerine aykırıdır. İptali gerekir.

Hicabi DURSUN bu görüşe katılmamıştır.

F- Kanun'un 127. Maddesiyle, 5651 sayılı Kanun'un 8. Maddesinin (5) Numaralı Fıkrasının Değiştirilen "dört saat" İbaresinin İncelenmesi

1- Genel Açıklama

Telekomünikasyon İletişim Başkanlığı (TİB), Türkiye'de telekomünikasyon yoluyla yapılan iletişimin içeriğini kontrol etmekle yükümlü kurumdur. TİB ayrıca 5651 sayılı Kanun'a göre internet içeriğinin izlenmesi/denetlenmesinden ve hâkim, mahkeme ve Cumhuriyet savcılar tarafından verilmiş erişim engelleme kararlarının uygulanmasından da sorumludur.

TİB, 5651 sayılı Kanun kapsamına giren suçları oluşturan içeriğe sahip faaliyet ve yayınları önlemeye yönelik çalışmalar yapmak, internet ortamında yapılan yayınların içeriklerini izleyerek, 5651 sayılı

Kanun kapsamına giren suçların işlendiğinin tespiti hâlinde, bu yayınlara erişimin engellenmesine yönelik olarak anılan Kanun'da öngörülen gerekli tedbirleri almakla da görevlidir.

Erişim engelleme, internet ortamında yayın yapan bir siteye girişin çeşitli yöntemlerle önlenmesidir. Başka bir ifadeyle, çeşitli tekniklerle kullanıcıların bir internet sitesine ulaşımının engellenmesidir. Hakkında erişim engelleme kararı verilen bir sitenin internet ortamında yayını kapatılmamakta, birtakım teknik yollar izlenerek ve yalnızca Türkiye sınırları içerisinde siteye ulaşılmasının önüne geçilmektedir.

5651 sayılı Kanun, esasen internet yayıncılığına ilişkin hükümler ve önemli tanımlamalar getirmekle birlikte, daha çok sitelerin erişime engellenmesi konusunda öne çıkmaktadır. Kanun, 8. maddesi ile sitelere erişim engelleme kararının verilmesi, bu karara konu olabilecek suçları ve bu kararın uygulanmasını düzenlemektedir. Erişim engelleme kararına konu olabilecek suçlar, anılan maddenin (1) numaralı fıkrasında sınırlı olarak sayılmıştır.

Bir internet sitesi hakkında erişim engelleme kararı vermeye, soruşturma safhasında hâkim (ve gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı); kovuşturma aşamasında ise mahkeme yetkilidir. Ayrıca Kanun'da öngörülmüş bazı durumlarda TİB tarafından da erişim engelleme kararı verilebilecektir. Mahkeme/hâkim tarafından verilen erişim engelleme kararları koruma tedbiri; TİB tarafından verilen kararlar ise idari tedbir niteliğindedir.

Soruşturma aşamasında hâkim, kovuşturma aşamasında mahkeme, 8. maddede sayılan katalogdaki suçlardan dolayı her zaman erişim engelleme tedbirine hükmedebilir. Ayrıca yine soruşturma aşamasında Cumhuriyet savcısı da gecikmesinde sakınca bulunan hâllerde erişim engelleme kararı verebilir. Cumhuriyet savcısı, bu yetkisini kullandıktan sonra kararı yirmi dört saat içinde hâkim onayına sunar ve bu karar, hâkim tarafından yirmi dört saat içerisinde onaylanmazsa, kendiliğinden ortadan kalkar.

Kanun, erişim engelleme kararı verebilecek yetkili bir organ olarak, ayrıca TİB'i belirlemiştir. TİB, katalogda sayılan suçlardan dolayı içerik ve/veya yer sağlayıcının yurtdışında olması hâlinde kendiliğinden erişim engelleme kararı verebilecektir. Ayrıca, çocukların cinsel istismarı, müstehcenlik ve fuhuş suçlarını oluşturan içerikler söz konusu ise içerik ve/veya yer sağlayıcı yurt içinde bulunsa dahi, TİB tarafından erişim engelleme kararı verilebilecektir.

Erişim engelleme kararları iki şekilde uygulanır. Şayet erişim engelleme kararı hâkim/mahkeme yahut Cumhuriyet savcısı tarafından verilmişse, kararın bir örneği gereği yapılmak üzere TİB'e gönderilir. TİB ise kararı erişim sağlayıcılara bildirerek uygulanmasını sağlayacak mercidir. TİB'in

resen engelleme kararı verdiği durumlarda da yine bu karar TİB tarafından erişim sağlayıcılara bildirilmektedir.

Erişim sağlayıcı, kararı uygulayarak ilgili internet sitesini TİB tarafından önceden hazırlanmış bir sayfaya yönlendirir. TİB'in hazırlanmış olduğu bu sayfada, sitenin erişime engellenmiş bulunduğu ve kararı veren mercinin adı ile tarih ve numarası da bulunur.

Erişime engelleme kararı, erişim sağlayıcı tarafından kendisine bildirilmesinden itibaren dört saat içinde yerine getirilmek zorundadır. Bunun aksine hareket için cezai hükümler getirilmiştir. Kanun'un 8. maddesine göre, koruma tedbiri niteliğindeki erişim engelleme kararını yerine getirmeyen erişim sağlayıcı sorumluları için para cezası öngörülmüştür. İdari tedbir niteliğindeki erişim engelleme kararlarının uygulanmaması durumundaysa, idari para cezasının yanında yetki belgesinin iptaline de karar verilebilecektir.

2- Anayasa'ya Aykırılık

Dava dilekçesinde, erişimin engellenmesi kararlarının yerine getirilmesini hızlandıran, kolaylaştıran ve internet ortamında yapılacak engellemeleri arttıracak olan bir düzenleme öngörüldüğü, bunun demokratik ve özgürlükçü bir yaklaşım olmadığı, çağdaş ve demokratik toplum düzeni ve "hukuk devleti" ilkesi ile bağdaşmadığı, kuraldaki sınırlamanın ölçülü olmadığı belirtilerek kuralın, Anayasa'nın 2., 13., 22., 26., 28. ve 40. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kural ile usulüne uygun olarak verilen bir erişimin engellenmesi kararının gereğinin en geç dört saat içerisinde yerine getirilmesi gerektiği düzenlenmektedir.

Anayasa Mahkemesi'nin pek çok kararında da belirtildiği üzere, yasamanın genelliği ve asliliği ilkesi uyarınca Anayasa'da bir konuda emredici ya da yasaklayıcı bir kural konulmamışsa, bu konunun düzenlenmesi anayasal ilkeler içinde kanun koyucunun takdirindedir.

Dava konusu düzenlemede, 5651 sayılı Kanun'da sayılan bazı durumlarda yine bu Kanun'da belirtilen merciler tarafından hukuka aykırı olduğu tespit edilen bir içerik veya internet sitesinin erişiminin engellenmesine karar verilmesi hâlinde bu kararın gereğinin süratle yerine getirilmesini temin etmek bakımından uygulama süresi belirlenmektedir. Daha önceki düzenlemede "yirmidört saat" olarak öngörülen bu süre Kanun metninde derhal ve en geç dört saat olarak değiştirilmiştir. Söz konusu sürenin belirlenmesi kanun koyucunun takdir yetkisi içerisinde. Dolayısıyla kanun koyucu tarafından yasama yetkisinin genelliği ve asliliği ilkelerine dayanılarak, usulüne uygun olarak verilmiş bir erişimin engellenmesi kararının uygulanma süresinin dört saat olarak belirlenmesi

suretiyle hukuka aykırı içerik nedeniyle mağdur olan kişilerin lehine bir düzenleme getirilmiştir. Bu nedenle kuralın, hukuk devleti ilkesiyle çelişen bir yönü bulunmamaktadır.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2. maddesine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 13., 22., 26., 28. ve 40. maddeleriyle ilgisi görülmemiştir.

G- Kanun'un 127. Maddesiyle, 5651 sayılı Kanun'un 8. Maddesine Eklenen (16) Numaralı Fıkrasının İncelenmesi

Dava dilekçesinde, Başkanlık tarafından yapılacak erişimin engellenmesinin sınırlarının nerede başlayıp, nerede biteceğinin madde metninde açıklanmadığı, erişimin engellenmesi faaliyetlerine ilişkin hukuki düzenlemelerin açık, net, anlaşılabilir ve çerçevesinin çizilmiş olması gerektiği, kural olarak hangi hâllerde erişimin engellenmesine karar verileceğinin 5651 sayılı Kanun'un 8. maddesinin (1) numaralı fıkrasında sarahaten ve tâdâdî olarak belirtildiği, 5651 sayılı Kanun'un 8. maddesinin ikinci cümlesi, gecikmesinde sakınca bulunan hâllerde, en geç yirmidört saat içinde, hâkimin onay vermediği sürece kaldırılacak olan bir erişimin engellenmesi tedbiri için Cumhuriyet savcısını yetkili görürken, dava konusu kuralın, Telekomünikasyon İletişim Başkanı'nın (Başkan) tâlimatı üzerine verilen erişimin engellenmesi kararının doğrudan Telekomünikasyon Kurumu bünyesinde bulunan Telekomünikasyon İletişim Başkanlığı (Başkanlık), yâni idare tarafından yerine getirileceğini öngördüğü, dolayısıyla 5651 sayılı Kanun'un 8. maddesinin (1) numaralı fıkrasının (a) ve (b) alt bentlerinde yer alan, 5237 sayılı Türk Ceza Kanunu'nda daha ağır yaptırımlara bağlanmış katalog suçlardan herhangi birinin internet ortamında işlendiği konusunda yeterli şüphe sebebi bulunan yayımlarla ilgili olarak öngörülmüş erişimin engellenmesine ilişkin tedbir süreci, 5651 sayılı Kanun'un 8. maddesine eklenen (16) numaralı fıkrasının birinci cümlesinde öngörülen, "Millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi nedenlerinden bir veya bir kaçına bağlı olarak gecikmesinde sakınca bulunan hâller"de erişimin engellenmesi kararı verilebilmesi sürecinin, daha sıkı bir yargı denetimine tâbi kılındığı, hukuk düzeni tarafından daha ciddi yaptırımlarla korunan bir menfaatin olduğu hâllerde (katalog suçlarda), 5651 sayılı Kanun'un 8. maddesi, tedbir uygulama konusunda daha sıkı bir yargı denetimi öngörürken, bu suçlardan daha hafif bir yaptırıma tâbi tutulmuş bulunan ve muhtevâsında daha soyut ve daha muğlak kavramları barındıran millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi nedenlerinden bir veya bir kaçına bağlı olarak gecikmesinde sakınca bulunan hâllerde öngörülen dava konusu düzenlemenin, erişimin engellenmesi suretiyle ifade, haberleşme ve basın hürriyetlerini kısıtlamaya yönelik olarak daha hızlandırılmış bir süreç getirmesinin, "ölçülülük ilkesi" ve korunmak istenen menfaatler ile

bağdaşmadığı belirtilerek kuralın, Anayasa'nın 2., 13., 22., 26., 28. ve 40. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralda, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi nedenlerinden bir veya bir kaçına bağlı olarak gecikmesinde sakınca bulunan hâllerde, erişimin engellenmesinin Başkan'ın talimatı üzerine Başkanlık tarafından yapılacağı; erişim sağlayıcılarının Başkanlıktan gelen erişimin engellenmesi taleplerini en geç dört saat içinde yerine getireceği ve Başkan tarafından verilen erişimin engellenmesi kararının, Başkanlık tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulacağı ve hâkimin de kararını kırk sekiz saat içinde açıklayacağı düzenlenmektedir.

Erişimin engellenmesi, Anayasa'nın 22. maddesindeki haberleşme hürriyeti ve 26. maddesindeki düşüncüyü açıklama ve yayma hürriyeti ile doğrudan ilgili olup Anayasa'nın 22. maddesinde, "Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.

İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir."; "Düşüncüyü açıklama ve yayma hürriyeti" başlıklı 26. maddesinde de, "Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet resmi makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar.

Bu hürriyetlerin kullanılması, milli güvenlik, kamu düzeni, kamu güvenliği, Cumhuriyetin temel nitelikleri ve Devletin ülkesi ve milleti ile bölünmez bütünlüğünün korunması, suçların önlenmesi, suçluların cezalandırılması, Devlet sırrı olarak usulünce belirtilmiş bilgilerin açıklanmaması, başkalarının şöhret veya haklarının, özel ve aile hayatlarının yahut kanunun öngördüğü meslek sırlarının korunması veya yargılama görevinin gereğine uygun olarak yerine getirilmesi amaçlarıyla sınırlanabilir.

Haber ve düşünceleri yayma araçlarının kullanılmasına ilişkin düzenleyici hükümler, bunların yayımını engellemek kaydıyla, düşüncüyü açıklama ve yayma hürriyetinin sınırlanması sayılmaz.

Düşünceyi açıklama ve yayma hürriyetinin kullanılmasında uygulanacak şekil, şart ve usuller kanunla düzenlenir." denilmek suretiyle temel hak ve özgürlükler arasında yer alan ifade özgürlüğü güvence altına alınmıştır.

İfade özgürlüğü, sadece "düşünce ve kanaate sahip olma" özgürlüğünü değil, aynı zamanda sahip olunan "düşünce ve kanaati (görüşü) açıklama ve yayma", buna bağlı olarak "haber veya görüş alma ve verme" özgürlüklerini de kapsamaktadır. Bu çerçevede ifade özgürlüğü bireylerin serbestçe haber ve bilgilere, başkalarının fikirlerine ulaşabilmesi, edindiği düşünce ve kanaatlerden dolayı kınanmaması ve bunları tek başına veya başkalarıyla birlikte çeşitli yollarla serbestçe ifade edebilmesi, anlatabilmesi, savunabilmesi ve yayabilmesi anlamına gelir.

İfade özgürlüğünün, toplumsal ve bireysel işlevini yerine getirebilmesi için AİHM'in de ifade özgürlüğüne ilişkin kararlarında sıkça belirttiği gibi, sadece toplumun ve devletin olumlu, doğru ya da zararsız gördüğü "haber" ve "düşüncelerin" değil, devletin veya halkın bir bölümünün olumsuz ya da yanlış bulduğu, onları rahatsız eden haber ve düşüncelerin de serbestçe ifade edilebilmesi ve bireylerin bu ifadeler nedeniyle herhangi bir yaptırıma tabi tutulmayacağından emin olmaları gerekir. İfade özgürlüğü, çoğulculuğun, hoşgörünün ve açık fikirliliğin temeli olup bu özgürlük olmaksızın "demokratik toplumdaki" bahsedilemez.

İnternet, modern demokrasilerde başta ifade özgürlüğü olmak üzere temel hak ve özgürlüklerin kullanılması bakımından önemli bir değere sahip bulunmaktadır. İnternetin sağladığı zemin, bilgiye ulaşma, kişilerin bilgi ve düşüncelerini açıklama, karşılıklı paylaşma ve yaymaları için vazgeçilmez niteliktedir. Bu nedenle sadece düşünceyi açıklamanın değil, aynı zamanda bilginin elde edilmesi açısından günümüzde en etkili ve yaygın yöntemlerden biri hâline gelen internet konusunda yapılacak düzenleme ve uygulamalarda devletin ve idari makamların çok hassas davranmaları gerektiği açıktır.

Türkiye'de telekomünikasyon yoluyla yapılan iletişimin içeriğini kontrol etmekle yükümlü TİB'in oluşturulmasındaki temel amaç, iletişimin izlenmesi ve tespit edilmesi uygulamalarında yetkileri merkezileştirmektir. 5651 sayılı Kanun'a göre TİB, internet içeriğinin izlenmesi/denetlenmesi ile hâkim, mahkeme ve Cumhuriyet savcıları tarafından verilmiş erişim engelleme kararlarının uygulanmasından sorumludur. Ayrıca TİB, Türkiye'de barındırılan belli bazı internet içeriklerine ve 8. maddede sayılan suçlar bağlamında Türkiye dışında barındırılan içeriğe erişimi, bazı suçlar yönünden idari kararlarla engelleme yetkisine de sahiptir. TİB'in ayrıca internetteki içerik izleme sistemlerinin yapısı, zamanlaması ve yöntemlerini, filtreleme, engelleme ve izleme için kullanılacak yazılım ya da donanımın üretimine ilişkin asgari ölçütleri belirleme yetkisi de vardır. Ancak TİB gerek

kuruluş mevzuatı gerekse de bu Kanun kapsamında yürüttüğü görevler bakımından ne bir regülasyon otoritesi ne de bir adli ve idari kolluktur.

Demokratik ülkelerde çocuk pornografisi, çocukların cinsel istismarı ve ırkçılık gibi ağır suçlar için konulan "erişimin engellenmesi" tedbiri, yargı kararı ile yargılama sürecinin bir parçası olarak uygulanan zorunlu ve istisnai bir tedbir olarak düzenlenmektedir. 5651 sayılı Kanun'daki erişim engelleme kararları cezai ve idari yaptırım niteliğinde olmayıp tedbir niteliğindedir.

Dava konusu kural, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi nedenlerinden bir veya bir kaçına bağlı olarak gecikmesinde sakınca bulunan hâllerde Başkan'a erişimin engellenmesi yetkisi vermektedir. Kuralda geçen "millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi" gibi ayrıntılı olarak somutlaştırılması ve önceden öngörülmesi mümkün olmayan durumları ifade eden ibarelerin içerik ve kapsamlarının kanun koyucu tarafından önceden tek tek belirlenmesi mümkün değildir. Söz konusu ibarelere, uygulama ve yargı kararlarıyla zaman içerisinde anlam kazandırılarak ibarelerin genel çerçevesi belirlenmekte ve içerikleri somutlaştırılmaktadır.

Anayasa'nın 22. maddesinin ikinci fıkrasında belirtilen durumlarda kanunla yetkili kılınmış merciin yazılı emriyle haberleşmenin engellenebileceği belirtilmektedir. Burada belirtilen yetkili merciin tespitinde yasa koyucunun sınırsız bir yetkiye sahip olmadığı açıktır. Belirlenecek yetkili merciin fıkrada belirtilen sebepler konusunda değerlendirme yapabilecek ve karar alabilecek yetkinliğe sahip olması gerekir.

Dava konusu kuralda geçen "millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi" ibarelerine dayanarak temel hak ve hürriyetleri sınırlandırması sonucunu doğuran erişimin engellenmesi yetkisi Başkan'a verilmektedir. Böylece kuralda sayılan oldukça önemli konularda belirtilen hâllerin varlığına ilişkin değerlendirme yapma ve karar verme yetkisi TİB'e bırakılmaktadır. Ancak, genel olarak Cumhuriyet savcısı, hâkim ve mahkemelerce verilen erişimin engellenmesi kararlarının uygulanmasına yönelik aracı kurum olarak görev yapan TİB'in kuralda yer alan ibarelerde belirtilen durumların varlığı veya yokluğunu belirleme noktasında tek başına değerlendirme yapacak konumda olmadığı açıktır. Milli güvenlik, kamu düzeninin korunması, suç işlenmesinin önlenmesi konularında ilgili ve yetkili kurumların değerlendirme ve karar verme yetkileri gözetilmeksizin tek başına TİB'e erişimin engellenmesi yetkisi verilmesi Anayasa'ya aykırılık oluşturur.

Haberleşme özgürlüğü ile düşüncüyü açıklama ve yayma özgürlüğünün kullanılması demokratik bir toplumda, zorunlu tedbirler niteliğinde ve Anayasa'nın ilgili maddelerinde belirtilen nedenlere bağlı

olarak, kanunla, belli koşullara, sınırlamalara bağlanabilir. Ancak, getirilen bu sınırlamalar hakların özüne dokunamaz, Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamaz.

Anayasal açıdan dokunulamayacak özün, her temel hak ve özgürlük açısından farklılık göstermekle birlikte kanunla getirilen sınırlamanın hakkın özüne dokunmadığının kabulü için temel hakların kullanılmasını ciddi surette güçleştirip, amacına ulaşmasına engel olmaması ve etkisini ortadan kaldıracı bir nitelik taşımaması gerekir.

Anayasa'nın 13. maddesinde yer alan ölçülülük ilkesi, amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder. Ölçülülük, aynı zamanda yasal önlemin sınırlama amacına ulaşmaya elverişli olmasını, amaç ve aracın ölçülü bir oranı kapsamasını ve sınırlayıcı önlemin demokratik toplum düzeni bakımından zorunluluk taşımasını da içeren bir ilkedir.

Anayasa'da güvence altına alınan haklara kamu gücü tarafından bir sınırlama (resen erişimin engellenmesi) imkânı getirildiği hâllerde ilgili Kanun'da böyle bir yetkinin kullanılmasına ilişkin kapsam ve usullerin yeterli bir açıklıkla belirtilmesi de gerekmektedir.

Hukukun genel prensibi gereği "hukuken korunması gereken amaçla", bu amacı gerçekleştirmek için kanunda tanımlı "hukuki himaye yönteminin yani aracın" orantılı olması aranmalıdır. Bir başka deyişle, hakkın kullanılmasında aşırıya kaçma riski olan, bir başkasının hak ve menfaatlerini zedeleme tehlikesi taşıyan hukuki himaye araçlarının amaç-araç dengesi bakımından hukuka uygun olmadığı kabul edilmektedir. Kuralda yer alan "millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi" ibarelerine dayanarak verilmesi öngörülen erişimin engellenmesi tedbiri; "amaç-araç" dengesi bakımından Anayasa ve Türkiye'nin taraf olduğu uluslararası sözleşmelerde tanımlı olan ifade özgürlüğü, haberleşme hürriyeti, düşünce ve ifadeyi yayma özgürlüğü noktasında bireylere tanınan temel hak ve özgürlüklerini ölçüsüzce sınırlandırma tehlikesini taşıyan bir hukuki himaye vasıtasıdır.

Erişimin engellenmesinde seçilen araç, hedeflenen gayeyi gerçekleştirmeye elverişli, yani o aracın yardımıyla gerçekleşmesinden korkulan tehlikenin yöneldiği hukuksal değer etkin bir şekilde korunabiliyorsa, isabetli bir araç seçilmiş demektir. Ancak ölçülülük değerlendirmesi için bu yeterli değildir. Elverişli aracın zorunlu olması da şarttır. Eğer bireyin ya da bireylerin hak ve özgürlüklerine daha az zarar verebilecek bir tedbir varsa onunla yetinilmelidir. Bir sitede yer alan sakıncalı içerik nedeniyle şartları oluşmadan öncelikle en ağır yaptırım olan sitenin bütününün erişime engellenmesi ölçülülük ilkesine aykırılık oluşturacaktır.

Bu durumda dava konusu kural ile TİB, belirtilen sebeplere baęlı olarak, sadece milli güvenlięi, suç işlenmesinin önlenmesi veya kamu düzenini tehdit ettięi deęerlendirilen ilgili yayına eriřimin engellenmesi kapsamında tüm internet sitesine eriřimi engelleyebilecektir. Kanun'un 9. maddesinde yargıya verilen eriřimin engellenmesi yetkisinin bile sınırları çizilmiř ve bu yetkinin ölçülülük ilkesi gereęince kademeli olarak kullanılacaęı belirtilmiřken, dava konusu düzenlemede bu tür bir sınırlama ve kademelendirmenin yapılmadıęı görölmektedir. Bunun da sınırlı bir alanda idareye çok geniř bir müdahale imkânı verdięi açıktır.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 13., 22. ve 26. maddelerine aykırıdır. İptali gerekir.

Kural, Anayasa'nın 2., 13., 22. ve 26. maddelerine aykırı görülerek iptal edildięinden dolayı, Anayasa'nın 28. maddesi yönünden ayrıca incelenmesine gerek görölmemiřtir.

Kuralın Anayasa'nın 40. maddesiyle ilgisi görölmemiřtir.

Nuri NECİPOęLU, Hicabi DURSUN, M. Emin KUZ ve Hasan Tahsin GÖKCAN bu görüře katılmamıřlardır.

V- YÜRÜRLÜęÜN DURDURULMASI İSTEMİ

10.9.2014 günlü, 6552 sayılı İş Kanunu ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Deęişiklik Yapılması ile Bazı Alacakların Yeniden Yapılandırılmasına Dair Kanun'un;

A- 97. maddesiyle, 6.1.1982 günlü, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 28. maddesinin;

1- a- (1) numaralı fıkrasının deęiřtirilen üçüncü cümlesinin ".23/4/1981 tarihli ve 2451 sayılı Bakanlıklar ve Baęlı Kuruluşlarda Atama Usulüne İliřkin Kanuna ekli (1) ve (2) sayılı cetvellerde gösterilen unvanları taşıyan görevler ile farklı atama usullerine tabi olsalar dâhi daire bařkanı ve üstü görevlere, sivil memurlar hariç kolluk teřkilatlarının kadrolarına; açıktan, naklen veya vekâleten yapılan atama ve bu görevlerden alınma, bu görevlerle ilgili yer deęiřtirme, görev ve unvan deęiřiklięi işlemleri hakkında verilen mahkeme kararlarının gereęi, ilgilinin kazanılmıř hak aylık derecesine uygun bařka bir kadroya atanması suretiyle iki yıl içinde yerine getirilir." bölümü,

b- (1) numaralı fıkrasının deęiřtirilen dördüncü cümlesi,

c- (1) numaralı fıkrasına eklenen cümlelerin "Bu fıkranın üçüncü cümlesinde belirtilen işlemlerle ilgili mahkeme kararlarının yerine getirilmemesi ceza soruřturması ve kovuřturmasına konu edilemez;" bölümü,

2.10.2014 günlü, E.2014/149, K.2014/151 sayılı kararla iptal edildiğinden, bu bölümlerin ve cümlenin, uygulanmalarından doğacak sonradan giderilmesi güç veya olanaksız durum ve zararların önlenmesi ve iptal kararının sonuçsuz kalmaması için kararın Resmî Gazete'de yayımlanacağı güne kadar YÜRÜRLÜKLERİNİN DURDURULMASINA, OYBİRLİĞİYLE,

B- 109. maddesiyle, 24.11.1994 günlü, 4046 sayılı Özelleştirme Uygulamaları Hakkında Kanun'a eklenen geçici 26. maddeye yönelik yürürlüğün durdurulması isteminin, koşulları oluşmadığından REDDİNE, OYBİRLİĞİYLE,

C- 126. maddesiyle değiştirilen, 4.5.2007 günlü, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 3. maddesinin (4) numaralı fıkrası, 2.10.2014 günlü, E.2014/149, K.2014/151 sayılı kararla iptal edildiğinden, bu fıkranın, uygulanmasından doğacak sonradan giderilmesi güç veya olanaksız durum ve zararların önlenmesi ve iptal kararının sonuçsuz kalmaması için kararın Resmî Gazete'de yayımlanacağı güne kadar YÜRÜRLÜĞÜNÜN DURDURULMASINA, Hicabi DURSUN'un karşıoyu ve OYÇOKLUĞUYLA,

D- 127. maddesiyle, 5651 sayılı Kanun'un 8. maddesinin (5) numaralı fıkrasının değiştirilen "dört saat" ibaresine yönelik iptal istemi, 2.10.2014 günlü, E.2014/149, K.2014/151 sayılı kararla reddedildiğinden, bu ibareye ilişkin yürürlüğün durdurulması isteminin REDDİNE, OYBİRLİĞİYLE,

E- 127. maddesiyle, 5651 sayılı Kanun'un 8. maddesine eklenen (16) numaralı fıkraya yönelik yürürlüğün durdurulması isteminin, koşulları oluşmadığından REDDİNE, OYBİRLİĞİYLE,

2.10.2014 gününde karar verilmiştir.

VI- SONUÇ

10.9.2014 günlü, 6552 sayılı İş Kanunu ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması ile Bazı Alacakların Yeniden Yapılandırılmasına Dair Kanun'un;

A- 97. maddesiyle, 6.1.1982 günlü, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 28. maddesinin;

1- (1) numaralı fıkrasının değiştirilen üçüncü cümlesinin ".23/4/1981 tarihli ve 2451 sayılı Bakanlıklar ve Bağlı Kuruluşlarda Atama Usulüne İlişkin Kanuna ekli (1) ve (2) sayılı cetvellerde gösterilen unvanları taşıyan görevler ile farklı atama usullerine tabi olsalar dâhi daire başkanı ve üstü görevlere, sivil memurlar hariç kolluk teşkilatlarının kadrolarına; açıktan, naklen veya vekâleten yapılan atama ve bu görevlerden alınma, bu görevlerle ilgili yer değiştirme, görev ve unvan değişikliği işlemleri hakkında verilen mahkeme kararlarının gereği, ilgilinin kazanılmış hak aylık derecesine uygun başka

bir kadroya atanması suretiyle iki yıl içinde yerine getirilir." bölümünün Anayasa'ya aykırı olduğuna ve İPTALİNE, OYBİRLİĞİYLE,

2- (1) numaralı fıkrasının değiştirilen dördüncü cümlesinin Anayasa'ya aykırı olduğuna ve İPTALİNE, OYBİRLİĞİYLE,

3- (1) numaralı fıkrasına eklenen cümlelerin "Bu fıkranın üçüncü cümlesinde belirtilen işlemlerle ilgili mahkeme kararlarının yerine getirilmemesi ceza soruşturması ve kovuşturmasına konu edilemez;" bölümünün Anayasa'ya aykırı olduğuna ve İPTALİNE, OYBİRLİĞİYLE,

B- 109. maddesiyle, 24.11.1994 günlü, 4046 sayılı Özelleştirme Uygulamaları Hakkında Kanun'a eklenen geçici 26. maddenin Anayasa'ya aykırı olduğuna ve İPTALİNE, OYBİRLİĞİYLE,

C- 126. maddesiyle değiştirilen, 4.5.2007 günlü, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 3. maddesinin (4) numaralı fıkrasının Anayasa'ya aykırı olduğuna ve İPTALİNE, Hicabi DURSUN'un karşıoyu ve OYÇOKLUĞUYLA,

D- 127. maddesiyle, 5651 sayılı Kanun'un;

1- 8. maddesinin (5) numaralı fıkrasının değiştirilen "dört saat" ibaresinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

2- 8. maddesine eklenen (16) numaralı fıkranın Anayasa'ya aykırı olduğuna ve İPTALİNE, Nuri NECİPOĞLU, Hicabi DURSUN, M. Emin KUZ ve Hasan Tahsin GÖKCAN'ın karşıoyları ve OYÇOKLUĞUYLA,

2.10.2014 gününde karar verildi.

Başkan - Haşim KILIÇ

Başkanvekili - Serruh KALELİ

Başkanvekili - Alparslan ALTAN

Üye: Serdar ÖZGÜLDÜR; Osman Alifeyyaz PAKSÜT; Zehra Ayla PERKTAŞ; Recep KÖMÜRCÜ; Burhan ÜSTÜN; Engin YILDIRIM; Nuri NECİPOĞLU; Hicabi DURSUN; Erdal TERCAN; Muammer TOPAL; Zühtü ARSLAN; M. Emin KUZ; Hasan Tahsin GÖKCAN

KARŞIOY GEREKÇESİ

5651 sayılı Kanununun 8. maddesine eklenen (16) numaralı fıkranın Anayasanın 2., 13., 22. ve 26. maddelerine aykırı olduğuna ve iptaline karar verilmiştir.

Erişimin engellenmesi kararını düzenleyen 8. maddenin (1) numaralı fıkrasında, internet ortamında yapılan yayınlarla ilgili olarak erişimin engellenmesine karar verilmesini gerektirecek suçlar sayılmakta; (2) numaralı fıkrasında, erişimin engellenmesi kararının soruşturma evresinde hâkim, kovuşturma evresinde mahkeme ve soruşturma evresinde gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından verileceği belirtilmekte; (4) numaralı fıkrasında, birinci fıkrada belirtilen suçları oluşturan yayınların içerik ve yer sağlayıcısının yurt dışında olması hâlinde veya bunlar yurt içinde olsalar bile anılan suçlardan dördüncü fıkrada belirtilenlerin işlenmesi hâlinde erişimin engellenmesi kararının re'sen Başkanlık tarafından verilmesi öngörülmekte ve diğer fıkralarda bu kararların yerine getirilmesine ilişkin usuller düzenlenmektedir.

8. maddeye eklenen (16) numaralı fıkrada da millî güvenlik ve kamu düzeninin korunması ile suç işlenmesinin önlenmesi sebeplerinden birine veya birkaçına bağlı olarak gecikmesinde sakınca bulunan hâllerde erişimin engellenmesinin Başkanın talimatı üzerine Başkanlık tarafından yapılması ve bu kararın Başkanlık tarafından yirmidört saat içinde sulh ceza hâkiminin onayına sunulması hâkimin kararını kırksekiz saat içinde açıklaması öngörülmektedir.

Dava konusu kuralın aykırı bulunduğu Anayasanın 22. maddesinde haberleşme hürriyetinin ikinci fıkrada sayılan sınırlama sebeplerine bağlı olarak hâkim kararı ile, yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hâllerde de kanunla yetkili kılınmış merciin emriyle sınırlanabileceği hükme bağlanmakta; 26. maddesinde ise sınırlama sebepleri belirtilirken buna yetkili olan merci konusunda hüküm bulunmamaktadır.

Dava konusu kuralda ise, Anayasanın anılan hükümlerindeki sınırlama sebeplerinden üçüne yer verilirken, gecikmesinde sakınca bulunan hâllerde engelleme kararını vermeye yetkili merci Başkanlık olarak belirlenmektedir.

Kararın gerekçesinde de belirtildiği üzere, millî güvenlik ve kamu düzeninin korunması ile suç işlenmesinin önlenmesi şeklinde belirlenen sınırlama sebeplerinin önceden ayrıntılı olarak somutlaştırılması ve bunları gerektiren durumların ve kapsamlarının kanun koyucu tarafından tek tek sayılması mümkün olmadığından, söz konusu ibarelerin genel çerçevesi uygulama ve yargı kararlarıyla belirlenerek somutlaşmaktadır. Anayasa koyucu, hâkim kararı yanında, yukarıda belirtilen sınırlama sebeplerine bağlı olarak gecikmesinde sakınca bulunan hâllerde "kanunla yetkili kılınmış merciin" de bu kararı alabileceğini belirttiğinden, kanunla Başkanlığın sözü edilen hâllerde yetkili kılınmasında da Anayasaya aykırı bir yön bulunmamaktadır.

Kararın gerekçesinde, yetkili merciin tesbitinde kanun koyucunun sınırsız bir yetkiye sahip olmadığı ve belirlenecek merciin fıkrada belirtilen sebepler konusunda değerlendirme yapabilecek ve karar alabilecek yetkinliğe sahip olması gerektiği belirtilerek, dava konusu kuralda geçen sınırlama sebeplerinin varlığı veya yokluğunu belirleme konusunda tek başına değerlendirme yapacak konumda olmayan TİB'e, bu konularda ilgili ve yetkili olan kurumların değerlendirme ve karar verme yetkileri gözetilmeden, erişimin engellenmesi yetkisi verilmesinin Anayasaya aykırı olduğu sonucuna varılmaktadır.

Öncelikle 5651 sayılı Kanunla verilen görevleri yerine getirmek üzere kurulan TİB'in Anayasanın 22. maddesinin ikinci fıkrasında belirtilen "yetkili merci" olarak belirlenip belirlenemeyeceği ve kanun koyucunun bu konudaki takdir yetkisini ne şekilde kullanacağı konusundaki bu değerlendirmelerin yerindelikle ilgili olduğu düşünülmektedir. Anayasanın anılan hükmüne dayanılarak kanunla yetkili merci olarak belirlenen TİB'in bu uzmanlığa ve birikime sahip olup olmadığı Anayasaya uygunluk denetiminde değerlendirme konusu yapılamaz. Anayasa Mahkemesi kararlarında da belirtildiği üzere, yasamanın genelliği ve asliliği ilkesi uyarınca Anayasada emredici ve yasaklayıcı hüküm bulunmayan hâllerde bir konunun düzenlenmesi kanun koyucunun takdir yetkisi içindedir. TİB'i, internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi konularında uzmanlık kuruluşu olarak belirleyen kanun koyucunun, Anayasanın 22. maddesinin ikinci fıkrasında öngörülen "yetkili merci" olarak belirleme konusunda da takdir yetkisi bulunduğu açıktır.

Diğer taraftan, dava konusu fıkrada, millî güvenlik ve kamu düzeninin korunması ile suç işlenmesinin önlenmesi sebeplerinin bulunup bulunmadığının tek başına TİB tarafından değerlendirilip belirleneceğine ilişkin bir hüküm de bulunmamaktadır. Kuralla TİB'e bırakılan yetki erişimin engellenmesine karar verme yetkisidir. Fıkrada TİB'in bu yetkiyi re'sen kullanacağına dair bir hüküm olmadığı gibi millî güvenlik ve kamu düzeninin korunması ile suç işlenmesinin önlenmesi konularında ilgili ve yetkili kurumların değerlendirme ve karar verme yetkilerinin gözetilmeyeceğine dair bir kural da getirilmemektedir. Esasen bu sınırlama sebeplerinin değerlendirilmesi konusunda yetkili olan kurumların teklif ve talepleri üzerine mezkûr kararların alınacağı da tabiidir. Dava konusu kuralda ise bunun aksini düşündürecek bir hükme yer verilmemektedir.

Kararın gerekçesinde, Kanununun 9. maddesinde yargıya verilen erişimin engellenmesi yetkisinin bile sınırları çizilmiş ve bu yetkinin kademeli olarak kullanılacağı belirtilmişken, dava konusu düzenlemede bu tür bir sınırlama ve kademelendirmenin yapılmadığı, bunun da idareye çok geniş bir müdahale imkânı verdiği belirtilmektedir.

Oysa, erişimin engellenmesi kararının kapsamı bakımından böyle bir kademelendirme yapılmasının Anayasal bir dayanağı olmadığı gibi, muhtevaları tamamen farklı olan mezkûr maddelerin karşılaştırılması suretiyle yapılan ölçülülük değerlendirmesinde de isabet bulunmamaktadır. Kaldı ki, 8. maddenin ikinci fıkrasında Cumhuriyet savcısı, hâkim ve mahkemeye, dördüncü fıkrasında Başkanlığa verilen erişimin engellenmesine karar verme yetkisinin de kapsamı belirtilmemekte ve bu maddede, gerekçede belirtilen şekilde bir kademelendirme de öngörülmemektedir.

Kanunun 9. maddesinde erişimin engellenmesi kararlarının, ihlalin gerçekleştiği yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanacağı ve zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik olarak engelleme kararı verilemeyeceği hükme bağlanmakta ise de, bu madde 8. maddeden tamamen farklı bir düzenleme içermektedir.

Yukarıda da açıklandığı üzere, 8. maddede, internet ortamında yapılan ve birinci fıkrada belirtilen suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesi düzenlenirken, 9. maddede ve 9/A maddesinde internet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ve özel hayatının gizliliğinin ihlal edildiğini iddia eden kişilerin talepleri sonucunda verilecek erişimin engellenmesi kararlarına ilişkin usul ve esaslar düzenlenmektedir. Mezkûr maddelerin muhtevaları tamamen farklı olduğundan, anılan düzenlemelerin karşılaştırılarak, iptal edilen fıkrada da 9. maddeye benzer şekilde bir kademelendirilme yapılmamasının ölçülülük ilkesine aykırılık oluşturduğu yönündeki kabule katılmak mümkün görünmemektedir.

Esasen ölçülülük incelemesinde, iptal edilen fıkrada öngörülen tedbir ile 9. maddede öngörülen engelleme tedbiri arasında yapılacak bir kıyaslamanın değil, kuralda öngörülen tedbirin kapsamının ve etkisinin dikkate alınması gerekir.

Kanun koyucu, 9 ve 9/A maddelerinde erişimin engellenmesi kararlarının URL bazlı olarak verilip uygulanacağını ve zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik engelleme kararı verilemeyeceğini hükme bağlarken, 8. maddede böyle bir sınırlama öngörmemiş ve 8. maddenin (4) ve (16) numaralı fıkralarında da erişimin engellenmesi kararının kapsamı konusunda Başkanlığa takdir yetkisi tanımıştır.

Başkanlığın, (16) numaralı fıkraya göre takdir yetkisini kullanarak vereceği erişimin engellenmesi kararı da yargı denetimine tâbi kılınmıştır. Başkanlığın engelleme kararı verirken dayandığı sınırlama sebebinin bulunup bulunmadığı, erişimin engellenmesi kararının hangi kurumun ve hangi gerekçelerle yaptığı teklif üzerine verildiği, içeriğe erişimin engellenmesinin amacın gerçekleşmesi

için yeterli olup olmadığı hususlarındaki değerlendirmeleri, herhangi bir talebe bağlı olmadan engelleme kararının Başkanlık tarafından yirmidört saat içinde onayına sunulduğu sulh ceza hâkimince incelenerek, bu konudaki kararların ölçülülük ilkesine uygunluğu da dahil olmak üzere hukuka uygun olup olmadığının Anayasada yetkilendirilen hâkimler tarafından karara bağlanması öngörülmüştür.

Erişimin engellenmesinde seçilen aracın amacı gerçekleştirmek için zorunlu ve elverişli olup olmadığı da, idarece alınan tedbir kararının sadece içerikle sınırlı olması yeterli iken bununla yetinilmeyip sitenin bütününe erişimin engellenmesi kararı verilmesinin ölçülük ilkesine aykırılık oluşturduğu da, sulh ceza hâkimi tarafından yapılan incelemede çok kısa sürede, süratli bir şekilde tesbit edilebilir. Bu inceleme sonunda, engelleme kararında ölçülülük ilkesine aykırılık belirlendiği takdirde, bunun, kararın dayanağını oluşturan kuralın da ölçülülük ilkesine aykırı olduğu anlamına gelmeyeceği açıktır.

Yukarıda belirtilen sebeplerle, 5651 sayılı Kanunun 8. maddesinin (16) nolu fıkrasının Anayasaya aykırı olmadığı düşüncesiyle, iptal yönündeki çoğunluk görüşüne katılmıyoruz.

Üye - Nuri NECİPOĞLU

Üye - M. Emin KUZ

KARŞIOY YAZISI

A- 6552 sayılı Kanun'un 126. Maddesiyle Değiştirilen, 5651 sayılı Kanun'un 3. Maddesinin (4) Numaralı Fıkrasının İncelenmesi

Kanun'un 3. maddesinin (4) numaralı fıkrasında, trafik bilgisinin TİB tarafından ilgili işletmecilerden temin edileceği ve hâkim tarafından karar verilmesi hâlinde ilgili mercilere verileceği belirtilmektedir. Kanun'un 3. maddesine göre trafik bilgisi, taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini ifade etmektedir. Dolayısıyla, kural uyarınca, taraflara ilişkin IP adresinin, verilen hizmetin başlama ve bitiş zamanının, yararlanılan hizmetin türünün, aktarılan veri miktarı ve varsa abone kimlik bilgilerinin işletmeciler tarafından TİB'e verilmesi gerekmektedir.

Anayasa'nın 20. maddesinin üçüncü fıkrasında, "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda

kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır.

Bu itibarla, iptali istenen kuralda TİB'e verilmesi öngörülen IP adresinin, verilen hizmetin başlama ve bitiş zamanının, yararlanılan hizmetin türünün, aktarılan veri miktarı ve abone kimlik bilgilerinin kişisel veri kapsamında olduğu açıktır. Dolayısıyla, iptali istenen kuralla kişisel verilerin korunması hakkına müdahalede bulunulduğu tartışmasızdır. Ancak bu müdahale, suç işlenmesinin önlenmesi gibi meşru anayasal bir amaca dayanmaktadır.

Nitekim Anayasa Mahkemesi, 5809 sayılı Elektronik Haberleşme Kanunu'nun; Bilgi Teknolojileri ve İletişim Kurumunun işletmeciler, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden elektronik haberleşmeyle ilgili olarak, ihtiyaç duyacağı her türlü bilgi ve belgeyi alabilmesini öngören 6. maddesinin (1) numaralı fıkrasının (1) bendini şu gerekçeyle Anayasa'ya uygun bulmuştur.

"İptali istenen ibare ile Kuruma verilen 'işletmeciler, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden ihtiyaç duyacağı her türlü bilgi ve belgeyi alma yetkisi'nin, Kurumun kuruluş amacı ve faaliyet alanında yer alan elektronik haberleşme sektörü ile ilgili şikâyetleri değerlendirme ve denetim işlevlerini gerektiği gibi yerine getirebilmesi amacıyla sınırlı olarak kullanılabileceği, ayrıca Kurumun abone, kullanıcı, tüketici ve son kullanıcıların kişisel bilgilerinin gizliliğini ve işletmecilerin ticari sırlarını korumakla görevli olduğu dikkate alındığında, iptali istenen ibare ile Kuruma gerçek ya da tüzel kişilerden özel hayatın gizliliğini ya da haberleşme özgürlüğünü ihlal eden bilgi ve belgeleri alma konusunda yetki verildiği söylenemez. Bu nedenle iptali istenen kuralın özel hayatın gizliliği hakkını ve haberleşme özgürlüğünü sınırlayan bir yönü bulunmamaktadır."

Görüldüğü üzere, Anayasa Mahkemesi, elektronik haberleşme sektörü ile ilgili şikâyetleri değerlendirme ve denetim işlevlerini gerektiği gibi yerine getirebilmesi amacıyla sınırlı olarak kullanılmak üzere Kuruma, işletmeciler, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden elektronik haberleşmeyle ilgili olarak, ihtiyaç duyacağı her türlü bilgi ve belgeyi alabilme yetkisi verilmesinin Anayasa'ya aykırı olmadığını vurgulamıştır. İtiraz konusu kuralda da Kurumun bir

birimi olan TİB'e, trafik bilgisinin ilgili işletmecilerden temin etme yetkisi verilmiştir. TİB'in temin ettiği trafik bilgilerini ancak hâkim tarafından karar verilmesi hâlinde ilgili mercilere verileceği hükme bağlanarak bunların gelişigüzel başka kurumlarla paylaşılması da engellenmiştir.

Bu itibarla, suç işlenmesini önlemek amacıyla TİB'in trafik bilgilerini işletmecilerden temin etmekten ibaret kalan müdahalenin, bu bilgilerin başka kurumlarla paylaşılmasının ancak mahkeme kararıyla mümkün olması karşısında, orantılı olmadığı söylenemez.

Öte yandan, 22.4.2014 günlü, 6533 sayılı Kanun ile onaylanması uygun bulunan Sanal Ortamda İşlenen Suçlar Sözleşmesi 16. maddesine göre, taraf devletler, bilgisayar veri kayıplarına veya değişikliklerine karşı özellikle korunmasız olma ihtimalinin bulunduğu bilgisayar sistemi aracılığıyla depolanan trafik verisi de dahil olmak üzere, belirlenmiş bilgisayar verisinin süratli bir şekilde korunması talimatını verecek veya benzer biçimde bu korumayı gerçekleştirecek yasal tedbirleri ve diğer idari tedbirleri alacaktır.

Aynı Sözleşme'nin 17. maddesinde ise her bir taraf devletin, trafik verilerinin korunmasını süratli şekilde teminat altına aldıktan sonra ilgili taraf devletin yetkili makamının veya bu makamın belirlediği kişinin haberleşmelerin hangi hizmet sağlayıcı ve hangi yol vasıtasıyla gerçekleştirildiğini tespit etmesine imkan verecek yeterli miktardaki trafik verilerinin de süratli şekilde açıklanmasının sağlanması için gerekli yasal tedbirleri ve diğer idari tedbirleri kabul edeceği belirtilmiştir.

İptale konu kuralın, sözü edilen Sözleşmenin ilgili hükümleriyle içerik itibarıyla uyarlı olduğu ve Türkiye'nin, anılan Sözleşmeyle uluslararası alanda taahhüt ettiği yükümlülüklerin gereği olarak yapılmış bir düzenleme olduğu anlaşılmaktadır.

B- Kanun'un 127. Maddesiyle, 5651 sayılı Kanun'un 8. Maddesine Eklenen (16) Numaralı Fıkranın İncelenmesi

Anayasa'nın 22. maddesinin "Haberleşme hürriyeti"ni düzenleyen 22. maddesinin birinci fıkrasında, "Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır." denilmek suretiyle haberleşme hürriyeti güvenceye bağlanmıştır.

"Haberleşme özgürlüğü", kişinin kesintiye uğramadan ve sansür edilmeden başkalarıyla iletişim kurma hakkıdır.

Modern toplumlarda diğer kişi haklarında olduğu gibi haberleşme özgürlüğü de sınırsız bir hak niteliğinde değildir. Bazı hallerde bu haklara da müdahale edilmesi gerekebilmekte, kişiler de önemli nedenlerle yapılan bu müdahalelere katlanmak durumunda kalmaktadırlar.

Nitekim Anayasa, haberleşme hürriyetini mutlak bir hak olarak düzenlememiş, millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması amacıyla sınırlandırılmasına imkân tanımıştır. Anayasa'nın 22. maddesinin ikinci fıkrasında, bu sınırlamanın ne şekilde yapılacağı da belirtilmiştir. Buna göre, haberleşme özgürlüğünün engellenmesi veya haberleşmenin gizliliğine dokunulabilmesi, 22. maddenin ikinci fıkrasında belirtilen sebeplerden biri veya birkaçına dayanılarak ve kural olarak ancak usulüne göre verilmiş hâkim kararıyla mümkün olabilmektedir. Anayasa, gecikmesinde sakınca bulunan hallerde ise hakim kararı gerekmeksizin kanunla yetkili kılınmış merciin yazılı emriyle de haberleşme özgürlüğünün sınırlandırılmasına imkan sağlamıştır. Ancak bu halde yetkili merciin kararının yirmidört saat içinde görevli hâkimin onayına sunulması ve hâkimin, kararını kırksekiz saat içinde açıklaması zorunlu kılınmıştır. Aksi halde, kararın kendiliğinden kalkması öngörülmüştür.

Anayasa, haberleşme özgürlüğünün sınırlandırılma usulüne ilişkin detaylı hükümlere yer vermekle birlikte, iki noktada takdiri kanun koyucuya bırakmıştır. Bunlardan birincisi, yetkili hakim kim olduğu, ikincisi ise gecikmesinde sakınca bulunan hallerde haberleşme özgürlüğüne dokunulabilmesi için hangi merciin gereken emri vermekle yetkilendirileceği hususudur. Kanun koyucu hukuk devleti ilkesini de gözeterek yetkili mercii tayin hususunda takdir yetkisine sahiptir.

İptali istenen kuralda, "millî güvenlik", "kamu düzeninin korunması", "suç işlenmesinin önlenmesi" nedenlerinden bir veya bir kaçına bağlı olarak "gecikmesinde sakınca bulunan hâllerde", erişimin engellenmesinin TİB Başkanın talimatı üzerine Başkanlık tarafından yapılacağı belirtilmiş, erişim sağlayıcılarının Başkanlıktan gelen erişimin engellenmesi taleplerini en geç dört saat içinde yerine getireceği ifade edilmiş, Başkan tarafından verilen erişimin engellenmesi kararının, Başkanlık tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulacağı ve Hâkimin, kararını kırk sekiz saat içinde açıklayacağı kurala bağlanmıştır.

İptali istenen kuralla, haberleşme özgürlüğünün sınırlandırılma usulüne ilişkin olarak Anayasa'nın 22. maddesiyle paralel bir düzenleme yapıldığı açıktır. Kanun koyucu, Anayasa koyucunun takdiri kendisine bıraktığı, gecikmesinde sakınca bulunan hallerde haberleşme özgürlüğüne dokunulabilmesi için gereken emri vermekle yetkili makamı da tayin etmiş ve bu hususta yetkili kişi olarak TİB Başkanını belirlemiştir.

TİB, 5651 sayılı Kanun'la Bilgi Teknolojileri ve İletişim Kurumu bünyesinde kurulan bir idari birimdir. Anılan Kanun'un temel amacı olan internet üzerinden işlenen suçlarla mücadele çerçevesinde öngörülen görevlerin ifası ve yetkilerin kullanımı TİB'in sorumluluğuna bırakılmıştır. Bu kadar

hassas alanlara ilişkin yetkilerle donatılan TİB Başkanı'nın atamasının da müşterek kararnameyle yapılması öngörölmüştür (5651 S.K. Ek.m.10).

Kanun koyucu, gecikmesinde sakınca bulunan hallerde haberleşme özgürlüğüne dokunulabilmesi için gereken emri verme yetkisini, Bakan, Başbakan ve Cumhurbaşkanı'nın güvenine mazhar olmuş ve onların ortak imzasıyla atanan TİB Başkanı'na vermiştir. Bu yetkinin, internet üzerinden işlenen suçlarla mücadeleyle görevlendirilen birim olan TİB'in Başkanı'na bırakılması işin mahiyeti gereğidir. Anayasa Mahkemesinin (AYM), kanun koyucunun bu takdirini sorgulayacak derecede aktivist davranması, güçler ayrılığı ilkesine aykırı düştüğü gibi demokratik devlet ilkesiyle de bağdaşmaz.

Çoğunluk kararında, yetkili merciin fıkrada belirtilen sebepler konusunda ("millî güvenlik", "kamu düzeninin korunması", "suç işlenmesinin önlenmesi") değerlendirme yapabilecek ve karar alabilecek yetkinliğe sahip olması gerektiği, TİB'in ise bu konularda tek başına değerlendirme yapacak konumda bulunmadığı belirtilmiş ve yetkili kurumların değerlendirme ve karar verme yetkileri gözetilmeksizin tek başına TİB'e erişimin engellenmesi yetkisi verilmesinin Anayasa'ya aykırı olduğu ifade edilmiştir. Çoğunluk kararında da vurgulandığı üzere, kuralda yer alan "millî güvenlik", "kamu düzeninin korunması", "suç işlenmesinin önlenmesi" ibarelerinin içerik ve kapsamının kanun koyucu tarafından önceden tek tek belirlenmesi mümkün olmayıp bu kavramların içeriği doktrin, uygulama ve yargı içtihatlarıyla belirlenecek ve somutlaştırılacaktır.

5651 sayılı Kanun'un uygulanmasından sorumlu idari birimlerden birinin de TİB olduğu açıktır. TİB Başkanının, bu yetkisini kullanırken işin doğası gereği emri altındaki uzman personelden yararlanacağı ve bunların görüş, öneri ve raporlarını gözönünde bulundurularak bir karara varacağı tabiidir. Ayrıca "millî güvenlik", "kamu düzeninin korunması", "suç işlenmesinin önlenmesi" gibi kavramların mahiyeti hususunda uzmanlaşmış tek bir kurum bulunmadığı gibi, bu kavramların yorumlanması tekeli de herhangi bir kuruma bırakılmamıştır. Asgari hukuki bilgi ve muhakeme yeteneğine sahip bir insanın bu kavramlardan ne anlaşılması gerektiğini saptaması mümkündür. Nitekim benzer kavramlar, hak ve hürriyetlerin sınırlandırılması sebebi olarak başka birçok kanunda da yer almakta ve ilgili idari merciler, başka bir idarenin görüşüne başvurmaksızın bu kavramları yorumlama ve değerlendirme yetkisine sahip olmaktadır.

Öte yandan erişimin engellenmesi kararı Başkanlık tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulacak olup TİB başkanının yorum ve değerlendirmesinin hatalı olması durumunda, hakim tarafından erişimin engellenmesi kararının kaldırılacağı muhakkaktır. Dolayısıyla TİB'in bu konularda tek başına değerlendirme yapacak konumda bulunmadığından

bahisle tek başına erişimin engellenmesi kararı veremeyeceği görüşünün anayasal bir temeli bulunmamaktadır.

Diğer taraftan, kanuna aykırı içeriklerin internet üzerinden çarpan etkisiyle çok hızlı bir şekilde yayılabildiği gerçeği gözetilerek mümkün olduğunca kısa bir sürede gerekli önlemlerin alınması için TİB Başkanı'na erişimin engellenmesi yetkisi tanınmıştır. Hızlı ve süratli bir şekilde karar alınmasını gerektiren bu tip durumlarda TİB'in başka kurumların görüş ve değerlendirmelerine başvurması, kuralın amacıyla bağdaşmadığı gibi kimi durumlarda hukuka aykırı içerikten zarar gören kişilerin haklarının zedelenmesine de yol açabilecektir.

Çoğunluk kararında, bir sitede yer alan sakıncalı içerik nedeniyle öncelikle en ağır yaptırım olan sitenin bütünüyle engellenmesinin ölçülü olmadığı belirtilmiştir. 5651 sayılı Kanun'da erişimin engellenmesi hususunda iki türlü tedbir öngörülmüştür: Birincisi, internet sitesinin hukuka aykırı unsurlar taşıyan bölümüyle ilgili (URL) içeriğe erişimin engellenmesi, ikincisi ise internet sitesindeki tüm yayınlara yönelik içeriğe erişimin engellenmesi şeklindedir. Dava konusu kuralın, birinci tedbiri dışladığı söylenemez. TİB Başkanı'nun dava konusu kural kapsamında URL bazlı erişimin engellenmesi kararı vermesi de mümkündür. Fakat kuralla TİB Başkanı'na tanınan yetkinin aciliyet gerektiren işlere münhasır olduğu gözetildiğinde, URL bazlı erişimin engellenmesi kararını uygulamasının mümkün olmaması durumunda sitenin tüm yayınlarına erişimi engelleme yoluna da başvurabilir. Dolayısıyla TİB Başkanı'nun, sözü edilen iki tedbirden hangisini uyguladığı, kurulan kendisiyle ilgili anayasal bir mesele olmayıp uygulanmasına ilişkin bir sorundur. Ayrıca erişimin engellenmesi kararının yirmi dört saat içinde sulh ceza hâkiminin onayına sunulması gerektiği ve sulh ceza hakimince, erişimin bütünüyle engellemesinin koşullarının oluşmadığı kanaatine varılması veya ölçüsüz bulunması durumunda kaldırılabilmesi dikkate alındığında, kuralla öngörülen tedbirin orantısız olmadığı anlaşılmaktadır.

Açıklanan nedenlerle, 5651 sayılı Kanun'un 3. maddesinin (4) numaralı fıkrası ile 8. maddesinin (16) numaralı fıkrasının Anayasa'ya aykırı olmadığı gerekçesiyle anılan kuralların iptali yolundaki çoğunluk görüşüne katılmıyorum.

Üye - Hicabi DURSUN

KARŞIOY GEREKÇESİ

Kanunun 127. maddesiyle, 5651 sayılı Kanunun 8. maddesine eklenen 16. fıkrası şöyledir :

"(16) Millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi nedenlerinden bir veya bir kaçına bağlı olarak gecikmesinde sakınca bulunan hâllerde, erişimin engellenmesi Başkanın talimatı üzerine Başkanlık tarafından yapılır. Erişim sağlayıcıları Başkanlıktan gelen erişimin engellenmesi taleplerini en geç dört saat içinde yerine getirir. Başkan tarafından verilen erişimin engellenmesi kararı, Başkanlık tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar."

İptali istenilen kuralda, internet ortamına erişimin engellenmesi konusunda Telekomünikasyon İletişim Başkanlığına istisnai bir yetki verilmektedir.

Esasen erişimin engellenmesi konusunu düzenleyen 8. maddenin 1 ila 3. fıkralarında erişimin engellenmesi hususu, (1. fıkrada sayılan suçlarla ilgili olarak) soruşturma veya kovuşturma evrelerinde hakim veya mahkeme ve gecikmede sakınca görülen hallerde ise C. Savcısının kararına bağlanmıştır. Bundan başka, aynı maddenin 4. fıkrasında; içeriği 1. fıkrada belirtilen suçları oluşturan yayınların; a) içerik veya yer sağlayıcısının yurt dışında bulunması halinde, b) veya içerik veya yer sağlayıcısı yurt içinde bulursa dahi 1. fıkranın (a) bendinin 2, 5 ve 6 numaralı alt bentlerinde yazılı suçları oluşturan yayınlara ilişkin olarak, erişimin engellenmesi kararının re'sen Başkanlık (TİB) tarafından verileceği ve 11. fıkrada da TİB tarafından verilen kararın yerine getirilmemesi halinde idari para cezası verileceği hükme bağlanmıştır. Diğer taraftan, 2. fıkranın 2 numaralı paragrafında bir anlamda ölçülülük ilkesine yer verilmiş ve amacı gerçekleştirebilecek ise erişimin engellenmesinin belirli bir süreyle sınırlı olabileceği ifade edilmiştir.

İnternet erişiminin haberleşme hakkını sağlaması karşısında, konunun Anayasa'nın 22. maddesi çerçevesinde incelenmesi gerekir. Anılan 22. maddenin 2. fıkrasında; "Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakim onayına sunulur. Hakim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar." ve 3. fıkrada ise "İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir." hükümleri yer almaktadır.

Görüleceği üzere Anayasa'nın 22. maddesinde haberleşme hürriyetinin, belirtilen amaçlarla kural olarak hakim kararıyla ve gecikmede sakınca bulunan halde ise yetkili merciin yazılı emri ile engellenebileceği belirtilmektedir. Nitekim, 5651 sayılı Kanunun, yukarıda açıklanan 8. maddesinin ilgili fıkralarında kural olarak hakim kararıyla ve istisnaen de yetkili idari merci kararıyla internet

erişiminin engellenebileceği düzenlenmiştir. Kuralda gecikmesinde sakınca bulunan hallerle sınırlı olarak erişimin engellenmesine dayanak olacak meşru amaçlar Anayasa'ya uygun olarak sayılmış ve Anayasa'nın 22/3. maddesinde belirtildiği üzere, bu konuda yetkili idari merci gösterilmiştir.

Mahkememiz çoğunluğunun iptal gerekçesinde, düzenlemenin bu yönleriyle Anayasa'ya uygunluğu kabul edilmekle birlikte, yetkinin sınırlarının belirlenmemesi ve yetki verilen idari merciin bu kavramları değerlendirme noktasında (TİB'in) doğru bir mercii olmadığı ileri sürülmektedir. İlk olarak belirtelim ki, verilen yetkinin kuralda belirtilen amaçlara uygun ve ölçülü olarak kullanılması zorunluluğu, kuralın kendi bünyesinden çıkmaktadır. Bundan ayrıca, Kanununun 2/1. maddesinin o bendinde; "(Ek. 6/2/2014-6518/85 md.) Erişimin engellenmesi: Alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi ve benzeri yöntemler kullanılarak erişimin engellenmesini, ifade eder" denilmiş, böylece Kanunda Kuruma verilen erişimin engellenmesi yetkisinin ne şekilde kullanılacağı açıkça gösterilmiştir. Kanun koyucu idareye, bu tanımda belirtilen yöntemlerden, amaca en uygun (elverişli ve ölçülü) olanın tercih edilmesi konusunda yetki vermiştir. Hatta, 8. maddenin 2. fıkrasındaki, "amacı gerçekleştirecek .belirli bir süreyle sınırlı engellenmesi" şeklindeki kural da ölçülülükle ilgilidir. İdarenin bu yetkiyi maksadına aykırı ve ölçüsüz olarak kullanması durumunda ise, kuralın ikinci cümlesi uyarınca konunun yargısal denetime tabi olması nedeniyle Anayasa'nın 13. maddesine aykırılığın bulunmadığı görüşümdedir.

Diğer taraftan, 5651 sayılı Kanun ile internet ortamında yapılan yayınların düzenlenmesi, bu konuda gerek mahkemeler ve C. Başsavcılıklarının ve gerekse ilgili idari mercilerin aldıkları erişimi engelleme kararlarını uygulama yetkisi TİB'e verilmiştir. Hatta yukarıda izah edildiği üzere 8. maddenin 4. ve 11. fıkralarında, sayılan katalog suçların varlığı durumunda TİB'e idari tedbir olarak re'sen erişimi engelleme kararı verme ve bu kararı uygulamayanlara idari para cezası kesme yetkileri verilmiştir. Başka deyişle, adli bir makam olmayan TİB'e katalogda sayılı birtakım suçların var olup olmadığı konusunda değerlendirme yapma yetkisi verilmiştir. Esasen iptal gerekçesinin ilgili yerinde, TİB'in kanunen "internet içeriğinin izlenmesi ve denetlenmesi" konusunda yetkili olduğu da ifade edilmektedir. Denetim yetkisi, ilgili kanunlar bakımından konunun değerlendirilmesini de içermektedir.

Bunda ayrıca, Anayasa'nın 22/2. maddesinde erişimin engellenmesi konusunda yetkinin, "kanunla yetkili kılınmış mercie" verileceği belirtilmektedir. Bu hüküm Mahkememiz çoğunluğunca, "konuyla ilgili yetkileri olan bir mercii" biçiminde anlaşılmış ise de, Anayasa hükmü açıkça, yetkili merciin kanunla yetkili kılınmış olacağına işaret etmektedir. Nitekim 5651 sayılı Kanuna eklenen 16. fıkra ile de Kurum, "kanunla yetkili kılınmış" bulunduğundan, kuralın Anayasa'ya aykırı bulunduğu ileri

sürülemez. Anayasa bu yetkinin ilgili idari merciler arasında paylaşılmasını da öngörmemektedir. Yine, çoğunluk gerekçesinde kural ile, "yargılama makamı olmayan ve idarenin bir parçası olan Başkan'a" yetki verilmiş olması Anayasa'ya aykırı görülmüştür ki, bu değerlendirmenin Anayasa'nın 22/2. maddesiyle bağdaşmadığı ortadadır. Dolayısıyla, TİB'in milli güvenlik, kamu düzeninin korunması ve suçun önlenmesi konularında değerlendirme yapamayacağını ileri sürülmesi, Anayasal denetim açısından geçerli bir dayanak teşkil etmemektedir. Anayasal çerçeve ve Kanunla verilen görevleri gözetildiğinde bu yetkinin TİB'e verilmesinde bir çelişki bulunmadığı gibi, kural bizatihi bu yetkiyi içermektedir. Düşüncemize göre, kural ile TİB'e verilen yetki, Anayasa'nın 2., 22. ve 26. maddelerine aykırılık teşkil etmemektedir.

Açıkladığım hukuki nedenler dolayısıyla iptal isteminin reddi gerektiği görüşünde olduğumdan, sayın çoğunluğun iptal gerekçesine katılmamaktayım.

Üye - Hasan Tahsin GÖKCAN

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2014/122

Karar Sayısı: 2015/123

Karar Tarihi: 30.12.2015

R.G. Tarih-Sayı: 01.03.2016 - 29640

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri M. Akif HAMZAÇEBİ, Engin ALTAY, Muharrem İNCE, Ahmet TOPTAŞ ile birlikte 121 milletvekili

İPTAL DAVASININ KONUSU: 17.4.2014 tarihli ve 6532 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun'un;

A- 1. maddesiyle, 1.11.1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu'nun 4. maddesinin birinci fıkrasına eklenen (h) bendinde yer alan ".Bakanlar Kurulunca verilen görevleri yerine getirmek." ibaresinin,

B- 3. maddesiyle 2937 sayılı Kanun'un;

1- 6. maddesinin değiştirilen birinci fıkrasının;

a- (a) bendinde yer alan "., uygun koordinasyon yöntemlerini uygulayabilir" ibaresinin,

b- (b) bendinin,

c- (c) bendinin,

d- (i) bendinde yer alan ".alan veya." ibaresinin,

2- 6. maddesine eklenen onbirinci fıkrada yer alan ".yukarıdaki hükümlere ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın; MİT Müsteşarı veya yardımcısının onayıyla." ibaresinin,

C- 6. maddesiyle 2937 sayılı Kanun'un 26. maddesine eklenen;

1-İkinci fıkranın ikinci cümlesinin,

2- Üçüncü fıkrada yer alan "İsimsiz, imzasız, adresiz yahut takma adla yapıldığı anlaşılan ya da." ve ".delilleri ve dayanakları gösterilmeyen ." ibarelerinin,

3- Dördüncü fıkranın birinci cümlesinin,

4- Sekizinci fıkranın,

D- 7. maddesiyle değiştirilen 2937 sayılı Kanun'un 27. maddesinin;

1- Birinci fıkrasında yer alan ".yetkisiz olarak alan, temin eden, ." ibaresinin,

2- Üçüncü fıkrasının,

3- Dördüncü fıkrasında yer alan ".ihmal veya." ve ".yükümlülüklerini yerine getirmeyenlere." ibarelerinin,

E- 8. maddesiyle 2937 sayılı Kanun'un başlığıyla birlikte değiştirilen 28. maddesinin birinci fıkrasında yer alan "., bu talepleri yerine getirenlerin hukuki ve cezai sorumluluğu doğmaz" ibaresinin,

F- 9. maddesiyle değiştirilen 2937 sayılı Kanun'un 29. maddesinin birinci fıkrasının;

1- Birinci cümlesinin,

2- İkinci cümlesinde yer alan "Ancak, ." ibaresinin,

G- 11. maddesiyle 2937 sayılı Kanun'a eklenen ek 1. maddenin;

1- Birinci fıkrasının,

2- İkinci fıkrasının,

Anayasa'nın 2., 5., 7., 10., 12., 13., 17., 20., 22., 26., 28., 29., 36., 38., 74., 125., 138., 140. ve 148. maddelerine aykırılığı ileri sürülerek iptallerine ve yürürlüklerinin durdurulmasına karar verilmesi talebidir.

I- İPTALİ İSTENİLEN KANUN HÜKÜMLERİ

Dava konusu kuralların yer aldığı 6532 sayılı Kanun'un;

1- 1. maddesiyle değiştirilen, 2937 sayılı Kanun'un "Millî İstihbarat Teşkilatının görevleri " başlıklı 4. maddesi şöyledir:

"a) Türkiye Cumhuriyetinin ülkesi ve milleti ile bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, Anayasal düzenine ve millî gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkında millî güvenlik istihbaratını Devlet çapında oluşturmak ve bu istihbaratı Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Millî Güvenlik Kurulu Genel Sekreteri ile gerekli kuruluşlara ulaştırmak.

b) Devletin millî güvenlik siyasetiyle ilgili planların hazırlanması ve yürütülmesinde; Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Millî Güvenlik Kurulu Genel Sekreteri ile ilgili bakanlıkların istihbarat istek ve ihtiyaçlarını karşılamak.

c) Kamu kurum ve kuruluşlarının istihbarat faaliyetlerinin yönlendirilmesi için Millî Güvenlik Kurulu ve Başbakanca tekliflerde bulunmak.

d) Kamu kurum ve kuruluşlarının istihbarat ve istihbarata karşı koyma faaliyetlerine teknik konularda müşavirlik yapmak ve koordinasyonun sağlanmasında yardımcı olmak.

e) Genelkurmay Başkanlığınca Silahlı Kuvvetler için lüzum görülecek haber ve istihbaratı, yapılacak protokole göre Genelkurmay Başkanlığına ulaştırmak.

f) Millî Güvenlik Kurulunda belirlenecek diğer görevleri yapmak.

g) İstihbarata karşı koymak.

h) (Ek: 17/4/2014-6532/1 md.) Dış güvenlik, terörle mücadele ve millî güvenliğe ilişkin konularda Bakanlar Kurulunca verilen görevleri yerine getirmek.

i) (Ek: 17/4/2014-6532/1 md.) Dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak.

j) (Ek: 17/4/2014-6532/1 md.) İstihbarat kapasitesini, niteliğini ve etkinliğini artırmak amacıyla çağdaş istihbarat usul ve yöntemlerini araştırmak, teknolojik gelişmeleri takip etmek ve uygun görülenleri temin etmek.

(Değişik birinci cümle: 17/4/2014-6532/1 md.) Millî İstihbarat Teşkilatına bu görevler dışında görev verilemez. Millî İstihbarat Teşkilatı birimlerinin görev, yetki ve sorumlulukları Başbakanca onaylanacak bir yönetmelikte belirtilir."

2- 3. maddesiyle değiştirilen 2937 sayılı Kanun'un "Yetkiler" başlıklı 6. maddesi şöyledir:

"(Değişik birinci fıkra: 17/4/2014-6532/3 md.) Millî İstihbarat Teşkilatı bu Kanun kapsamındaki görevlerini yerine getirirken aşağıdaki yetkileri kullanır:

a) Yerli ve yabancı her türlü kurum ve kuruluş, tüm örgüt veya oluşumlar ve kişilerle doğrudan ilişki kurabilir, uygun koordinasyon yöntemlerini uygulayabilir.

b) Kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu kapsamındaki kurum ve kuruluşlar ile diğer tüzel kişiler ve tüzel kişiliği bulunmayan kuruluşlardan bilgi, belge, veri ve kayıtları alabilir, bunlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim alt yapısından yararlanabilir ve bunlarla irtibat

kurabilir. Bu kapsamda talepte bulunulanlar, kendi mevzuatlarındaki hükümleri gerekçe göstermek suretiyle talebin yerine getirilmesinden kaçınamazlar.

c) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun İkinci Kitap Dördüncü Kısım Dört, Beş, Altı ve Yedinci bölümlerinde yer alan suçlara (318, 319, 324, 325 ve 332 nci maddeleri hariç olmak üzere) ilişkin soruşturma ve kovuşturmalarda ifade tutanaklarına, her türlü bilgi ve belgeye erişebilir, bunlardan örnek alabilir.

d) Görevlerini yerine getirirken gizli çalışma usul, prensip ve tekniklerini kullanabilir.

e) İstihbari faaliyetler için görevlendirilenlerin kimliklerini değiştirebilir, kimliğin gizlenmesi için her türlü önlemi alabilir, tüzel kişilikler kurabilir. Kimliğin oluşturulması veya tüzel kişiliğin kurulması ve devam ettirilmesi için zorunlu olması durumunda gerekli belge, kayıt ve dokümanlar ile araç ve gereçler hazırlayabilir, değiştirebilir ve kullanabilir.

f) Yabancıların ülkeye giriş ve çıkış ile vize, ikamet, çalışma izni ve sınır dışı edilmesi gibi konularda, ilgili kurum ve kuruluşlardan talepte bulunabilir.

g) Telekomünikasyon kanallarından geçen dış istihbarat, millî savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplayabilir.

h) Yabancı unsurların ülkenin ve vatandaşların iletişim güvenliğini tehdit eden faaliyetlerinin engellenmesine yönelik çalışmalar yapabilir, ilgili kurum ve kuruluşlardan talepte bulunabilir.

i) MİT'te görev alan veya alacak kişilerin güvenilirliklerini ve uygunluklarını belirlemek için yalan makinası uygulaması dâhil test teknik ve yöntemlerini kullanabilir.

j) MİT mensupları görevlerini yerine getirirken ceza ve infaz kurumlarındaki tutuklu ve hükümlülerle önceden bilgi vermek suretiyle görüşebilir, görüşmeler yaptırabilir, görevinin gereği terör örgütleri dâhil olmak üzere millî güvenliği tehdit eden bütün yapılarla irtibat kurabilir.

(Ek fıkra: 3/7/2005 - 5397/3 md.) Bu Kanunun 4 üncü maddesinde sayılan görevlerin yerine getirilmesi amacıyla Anayasanın 2 nci maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde Devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, Devlet sırrının ifşasının tespiti ve terörist faaliyetlerin önlenmesine ilişkin olarak, hâkim kararı veya gecikmesinde sakınca bulunan hallerde MİT Müsteşarı veya yardımcısının yazılı emriyle telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir. Gecikmesinde sakınca bulunan hallerde verilen yazılı emir, yirmidört saat içinde yetkili ve görevli hâkimin onayına sunulur. Hâkim, kararını en geç yirmidört

saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde tedbir derhal kaldırılır. Bu halde dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir. Bu işlemler, MİT tarafından kurulan merkez veya 4.7.1934 tarihli ve 2559 sayılı Polis Vazife ve Selahiyet Kanununun ek 7 nci maddesinin onuncu fıkrası hükmüne göre kurulan merkez tarafından yürütülür. (Değişik son cümle: 4/5/2007-5651/12 md.) 4/12/2004 ta-rih-li ve 5271 sa-yı-lı Ce-za Mu-ha-ke-me-si Ka-nu-nu-nun 135 in-ci mad-de-si-nin al-tın-cı fık-ra-sı-nın (a) ben-di-nin (14) nu-ma-ra-lı alt ben-di kap-sa-mın-da ya-pı-la-cak din-le-me-ler de bu mer-kezler üze-rin-den ya-pı-lır.

(Ek fıkra: 3/7/2005 - 5397/3 md.; Değişik üçüncü fıkra: 17/4/2014-6532/3 md.) Yetkili ve görevli hâkim, Ankara ağır ceza mahkemesinin üyesidir.

(Ek fıkra: 3/7/2005 - 5397/3 md.) Kararda ve yazılı emirde, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, kullandığı telefon numaraları veya iletişim bağlantısını tespiti imkân veren kodundan belirlenebilenler ile tedbirin türü, kapsamı ve süresi ile tedbire başvurulmasını gerektiren nedenler belirtilir. Kararlar, en fazla üç ay için verilebilir; bu süre aynı usûlle üçer ayı geçmeyecek şekilde en fazla üç defa uzatılabilir. Ancak, ca-sus-luk fa-ali-yet-le-ri-nin tes-pi-ti ve terör örgütünün faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi halinde, hâkim üç aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebilir.(1)

(Ek fıkra: 3/7/2005 - 5397/3 md.) Uygulanan tedbirin sona ermesi halinde, dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir.

(Ek fıkra: 3/7/2005 - 5397/3 md.) Bu fıkra hükümlerine göre yürütülen faaliyetler çerçevesinde elde edilen kayıtlar, bu Kanunda belirtilen amaçlar dışında kullanılamaz. Elde edilen bilgi ve kayıtların saklanması ve korunmasında gizlilik ilkesi geçerlidir. (Mülga son cümle: 17/4/2014-6532/3 md.)

(Ek fıkra: 3/7/2005 - 5397/3 md.) Hâkim kararları ve yazılı emirler, MİT Müsteşarlığı görevlilerince yerine getirilir. İşlemin başladığı ve bitirildiği tarih ve saat ile işlemi yapanın kimliği bir tutanakla saptanır.

(Ek fıkra: 3/7/2005 - 5397/3 md.) Bu maddede yer alan faaliyetlerin denetimi, sıralı kurum amirleri, Başbakanlık teftiş elemanları (.) (1) tarafından yapılır. (1)

(Ek fıkra: 3/7/2005 - 5397/3 md.) Bu maddede belirlenen usûl ve esaslara aykırı dinlemeler hukuken geçerli sayılmaz ve bu şekilde dinleme yapanlar hakkında 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu hükümlerine göre işlem yapılır.

(Ek fıkra: 3/7/2005 - 5397/3 md.) Bu maddenin uygulanmasına ilişkin esas ve usûller Adalet, İçişleri ve Ulaştırma bakanlıkları ile MİT Müsteşarlığının görüşü alınmak suretiyle Başbakanlık tarafından üç ay içinde çıkarılacak yönetmelikle düzenlenir.

(Ek fıkra: 17/4/2014 - 6532/3 md.) Önleyici istihbarat elde etmek ve analiz yapabilmek amacıyla yukarıdaki hükümlere ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın; MİT Müsteşarı veya yardımcısının onayıyla yurt dışında veya yabancılar tarafından gerçekleştirilen iletişim ile ankesörlü telefonlarla gerçekleştirilen iletişim ve MİT mensuplarının, MİT'te görev almış olanların veya görev almak üzere başvuruların iletişimi tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir.

(Ek fıkra: 17/4/2014 - 6532/3 md.) Bu Kanundaki görevlerin ifası ve yetkilerin kullanılmasına ilişkin usul ve esaslar yönetmelikle düzenlenir.

Bu Kanunda yazılı görevlerin yerine getirilmesi sırasında genel zabıtaya tanınmış olan hak ve yetkilerin, MİT mensuplarından kimlere tanınacağı, yönetmelikte belirtilir."

3- 6. maddesiyle değiştirilen, 2937 sayılı Kanun'un "Soruşturma izni ve yargılama " başlıklı26. maddesi şöyledir:

"MİT mensuplarının veya belirli bir görevi ifa etmek üzere kamu görevlileri arasından Başbakan tarafından görevlendirilenlerin; görevlerini yerine getirirken, görevin niteliğinden doğan veya görevin ifası sırasında işledikleri iddia olunan suçlardan dolayı ya da 5271 sayılı Kanunun 250 nci maddesinin birinci fıkrasına göre kurulan ağır ceza mahkemelerinin görev alanına giren suçları işledikleri iddiasıyla haklarında soruşturma yapılması Başbakanın iznine bağlıdır.

(Ek fıkra: 17/4/2014 - 6532/6 md.) Cumhuriyet savcıları, MİT görev ve faaliyetleri ile mensuplarına ilişkin herhangi bir ihbar veya şikâyet aldıklarında veya böyle bir durumu öğrendiklerinde MİT Müsteşarlığına bildirirler. MİT Müsteşarlığının, konunun görev ve faaliyetlerine ilişkin olduğunu belirtmesi veya belgelendirmesi hâlinde adli yönden başkaca bir işlem yapılmaz ve herhangi bir koruma tedbiri uygulanmaz. Ancak birinci fıkra hükümlerine göre işlem yapılabilir.

(Ek fıkra: 17/4/2014 - 6532/6 md.) İsimsiz, imzasız, adresiz yahut takma adla yapıldığı anlaşılan ya da belli bir olayı ve nedeni içermeyen, delilleri ve dayanakları gösterilmeyen ihbar ve şikâyetler, Cumhuriyet savcılarınca işleme konulmaz.

(Ek fıkra: 17/4/2014 - 6532/6 md.) MİT Müsteşarı hakkındaki soruşturmalarda 25/10/1963 tarihli ve 353 sayılı Askeri Mahkemeler Kuruluşu ve Yargılama Usulü Kanununun 15/A maddesinin üçüncü

fıkrasının son iki cümlesi ile beş, altı ve yedinci fıkralarında yer alan usul ve hükümler uygulanır. MİT Müsteşarı hakkındaki yargılama Yargıtay ilgili dairesince yapılır.

(Ek fıkra: 17/4/2014 - 6532/6 md.) Aynı konuya ilişkin yeni ve somut bir delil ortaya çıkmadan yeniden soruşturma yapılamaz.

(Ek fıkra: 17/4/2014 - 6532/6 md.) MİT mensupları ile istihbarat hizmetlerine yardımları tevsih edilenler ve bunların eş, çocuk, ana, baba ve kardeşleri MİT Müsteşarının onayıyla 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanununda yer alan koruma tedbirlerinden yararlandırılabilir.

(Ek fıkra: 17/4/2014 - 6532/6 md.) MİT mensuplarının görevlerini yerine getirirken, görevin niteliği gereği veya görevin ifası sebebiyle diğer kişilere vermiş oldukları zararlar idare tarafından tazmin edilir. Tazmin, zararın göreve ilişkin bir husustan doğması ve ilgili personelin kasıt veya ağır kusurunun bulunmaması hâlinde rücu işlemine konu edilmez.

(Ek fıkra: 17/4/2014 - 6532/6 md.) Türk vatandaşları hariç olmak üzere, tutuklu veya hükümlü bulunanlar, millî güvenliğin veya ülke menfaatlerinin gerektirdiği hâllerde Dışişleri Bakanının talebi üzerine, Adalet Bakanının teklifi ve Başbakanın onayı ile başka bir ülkeye iade edilebilir veya başka bir ülkede tutuklu ve hükümlü bulunanlar ile takas edilebilir."

4- 7. maddesiyle değiştirilen, 2937 sayılı Kanun'un "Cezai hükümler" başlıklı 27. maddesi şöyledir:

"Millî İstihbarat Teşkilatının görev ve faaliyetlerine ilişkin bilgi ve belgeleri, yetkisiz olarak alan, temin eden, çalan, sahte olarak üreten, bunlar üzerinde sahtecilik yapan ve bunları yok eden kişiye dört yıldan on yıla kadar hapis cezası verilir.

MİT mensupları ve ailelerinin kimliklerini herhangi bir yolla ifşa edenler ile MİT mensuplarının kimliklerini sahte olarak düzenleyen veya değiştiren ya da bu sahte belgeleri kullananlara üç yıldan yedi yıla kadar hapis cezası verilir.

Birinci ve ikinci fıkra kapsamındaki bilgi ve belgelerin; radyo, televizyon, internet, sosyal medya, gazete, dergi, kitap ve diğer tüm medya araçları ile her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim araçları vasıtasıyla yayımlanması, yayılması veya açıklanması hâlinde; 9/6/2004 tarihli ve 5187 sayılı Basın Kanununun 11 inci maddesi ile 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 4 üncü ve 6 ncı maddeleri hükümlerine göre sorumlulukları belirlenenler ile bunları yayanlar hakkında üç yıldan dokuz yıla kadar hapis cezası verilir.

Bu Kanun kapsamındaki görev ve yetkilerin kullanılmasını engelleyenlere üç yıldan beş yıla kadar, ihmal veya suistimal suretiyle önleyenlerle yükümlülüklerini yerine getirmeyenlere iki yıldan dört yıla kadar hapis cezası verilir.

Söz konusu fiillerin MİT mensuplarınca işlenmesi hâlinde verilecek ceza üçte biri oranına kadar artırılır."

5- 8. maddesiyle değiştirilen, 2937 sayılı Kanun'un "Taleplerin karşılanması" başlıklı 28. maddesi şöyledir:

"Bu Kanunda MİT'e verilen görev ve yetkiler çerçevesinde yapılan her türlü talep öncelikli olarak yerine getirilir, bu talepleri yerine getirenlerin hukuki ve cezai sorumluluğu doğmaz.

Bu Kanun ile diğer kanunlarda aynı konuyu düzenleyen farklı hükümler bulunması hâlinde bu Kanun hükümleri uygulanır."

6- 9. maddesiyle değiştirilen, 2937 sayılı Kanun'un "Tanıklık" başlıklı 29. maddesi şöyledir:

"MİT mensupları ile MİT'te görev yapmış olanlar, MİT'in görev ve faaliyetlerine ilişkin hususlarda tanıklık yapamaz. Ancak, Devletin çıkarlarının zorunlu kıldığı hâllerde MİT mensuplarının tanıklığı MİT Müsteşarının, MİT Müsteşarının tanıklığı ise Başbakanın iznine bağlıdır."

7- 11. maddesiyle 2937 sayılı Kanun'a eklenen ek 1. madde şöyledir:

"Millî İstihbarat Teşkilatı uhdesindeki istihbari nitelikteki bilgi, belge, veri ve kayıtlar ile yapılan analizler, Türk Ceza Kanununun İkinci Kitap Dördüncü Kısım Yedinci Bölümünde yer alan suçlar hariç olmak üzere, adli mercilerce istenemez.

6 ncı maddenin birinci fıkrasının (e) bendine göre kimlikleri değiştirilenler, MİT'in görev ve faaliyetlerine yardımcı olanlar veya istihbarat hizmetlerinde istifade edilenler, kamu görevlisi olup olmadıklarına bakılmaksızın; görev, faaliyet ve yardımları sebebiyle sorumlu tutulamaz.

Teşkilat uhdesindeki bilgi ve belgelerin gizlilik derecelerinin ve sürelerinin tespit edilmesine, birim ve kısımlara ayrılmasına, kullanıma veya paylaşımına açılmasına ve bunların akademik çalışmalar ile her türlü yayın ve edebî eserde kullanılmasına Müsteşar tarafından oluşturulacak bir Komisyonca karar verilir."

II- İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca, Haşim KILIÇ, Serruh KALELİ, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT, Zehra Ayla PERKTAŞ, Recep KÖMÜRCÜ, Burhan ÜSTÜN, Engin YILDIRIM, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Erdal

TERCAN, Muammer TOPAL, Zühtü ARSLAN, M. Emin KUZ ve Hasan Tahsin GÖKCAN'ın katılmalarıyla 10.7.2014 tarihinde yapılan ilk inceleme toplantısında, dosyada eksiklik bulunmadığından işin esasının incelenmesine, yürürlüğü durdurma talebinin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

III- ESASIN İNCELENMESİ

2. Dava dilekçesi, Raportör Hamit YELKEN tarafından hazırlanan işin esasına ilişkin Rapor ve Ek Rapor, dava konusu kanun hükümleri, dayanılan ve ilgili görülen Anayasa kuralları, bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 43. maddesinin (1) numaralı fıkrası uyarınca Millî İstihbarat Teşkilatı Müsteşarı Hakan FİDAN ile diğer yetkililerin 30.12.2015 tarihli sözlü açıklamaları dinlendikten sonra gereği görüşülüp düşünüldü:

A- Kanun'un 1. Maddesiyle 2937 Sayılı Kanun'un 4. Maddesinin Birinci Fıkrasına Eklenen (h) Bendinde Yer Alan ".Bakanlar Kurulunca verilen görevleri yerine getirmek." İbaresinin İncelenmesi

1- İptal Talebinin Gerekçesi

3. Dava dilekçesinde özetle dava konusu kuralla MİT'e dış güvenlik, terörle mücadele ve millî güvenliğe ilişkin konularda Bakanlar Kurulunca verilen görevleri yerine getirme görevinin verildiği, ancak düzenlemede Bakanlar Kurulunca verilecek söz konusu görevlerin kapsam ve sınırları gösterilmeyerek hukuki belirsizliğe ve keyfilığe neden olduğu belirtilerek kuralın, Anayasa'nın 2. maddesinde yer alan hukuk devleti ilkesine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

4. Anayasa'nın 2. maddesinde, Türkiye Cumhuriyeti bir hukuk devleti olarak nitelendirilmiştir. Hukuk devletinin temel ilkelerinden biri "belirlilik"tir. Bu ilkeye göre, yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfi uygulamalarına imkân tanımaması gerekir. Belirlilik ilkesi, hukuksal güvenlikle bağlantılı olup birey, yasadan belirli bir kesinlik içinde, hangi somut eylem ve olguya hangi hukuksal yaptırımın veya sonucun bağlandığını bilmelidir. Birey ancak bu durumda kendisine düşen yükümlülükleri öngörebilir ve davranışlarını düzenleyebilir. Hukuk güvenliği, normların öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar.

5. Dava konusu kuralda, MİT'in Bakanlar Kurulunca verilen görevleri yerine getireceği düzenlenmiş ve bu düzenleme yapılırken söz konusu görevin sadece dış güvenlik, terörle mücadele ve millî güvenliğe ilişkin konularda olabileceği belirtilerek verilecek görevin kapsamı, sınırları ve içeriği hem kişiler hem de idare yönünden herhangi bir tereddüde yer bırakmayacak şekilde açık, anlaşılabilir ve uygulanabilir şekilde belirlenmiştir.

6. Kuralda yer alan "görev" veya bu görevi niteleyerek içeriğini belirleyen "dış güvenlik", "terörle mücadele" ve "millî güvenlik" ibarelerinin soyut ve genel kavramlar olması ise kuralın belirsizlik taşıması anlamına gelmemekte, yasa yapma tekniğinin doğasından kaynaklanmaktadır. Zira yasa kurallarının genel ve soyut olması, somut olayın özelliğine göre değişebilecek tüm çözümleri kuralın bünyesinde barındırma, bir başka ifadeyle, kuralın amaca uygun sonuca ulaştıracak herhangi bir çözümü dışlamasını önleme ihtiyacından kaynaklanmaktadır.

7. Öte yandan, Anayasa'nın 117. maddesinde, "Millî güvenliğin sağlanmasından . Türkiye Büyük Millet Meclisine karşı, Bakanlar Kurulu sorumludur." hükmüne yer verilmiştir. Bu çerçevede, millî güvenliği sağlama sorumluluğu bulunan Bakanlar Kurulunun, Anayasa tarafından kendisine verilen bu sorumluluğun gereğini yerine getirmek üzere millî güvenlik ile millî güvenliği doğrudan ilgilendiren "dış güvenlik" ve "terörle mücadele" konularında MİT'e görev verme yetkisine sahip kılınması doğaldır.

8. Yürütme yetkisi ve görevi Cumhurbaşkanı ile birlikte Bakanlar Kuruluna ait olup Anayasa'nın 8. maddesi uyarınca bu yetki ve görev Anayasa ve kanunlara uygun olarak kullanılır ve yerine getirilir. Dolayısıyla düzenlemenin genel ve soyut niteliğinden Bakanlar Kuruluna MİT'e hukuka aykırılık oluşturabilecek nitelikte bir görev verme yetkisinin verildiği sonucunun çıkarılması mümkün değildir.

9. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

B- Kanun'un 3. Maddesiyle Değiştirilen 2937 Sayılı Kanun'un 6. Maddesinin Birinci Fıkrasının (a) Bendinde Yer Alan ", uygun koordinasyon yöntemlerini uygulayabilir " İbaresinin İncelenmesi

1- İptal Talebinin Gerekçesi

10. Dava dilekçesinde özetle dava konusu ibareyi içeren kuralla MİT'e görevlerini yerine getirirken uygun koordinasyon yöntemlerini uygulayabilme yetkisinin verildiği, ancak Kanun'da "uygun koordinasyon yöntemleri" ibaresiyle ne kastedildiğinin belirtilmediği, bu durumun belirsizliğe ve

MİT'in keyfi uygulamalarına imkân tanıdığı belirtilerek kuralın, Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

11. Dava konusu ibareyle MİT'e "uygun koordinasyon yöntemleri uygulayabilme" yetkisi verilmiş ve bu düzenleme yapılırken Kanun'un 6. maddesinde söz konusu yetkinin ancak MİT'in görevlerinin yerine getirilmesi kapsamında ve yerli, yabancı her türlü kurum, kuruluş, örgüt, oluşum ve kişilerle doğrudan ilişki kurabilme şeklinde kullanılabileceği belirtilerek anılan yetkinin kapsamı, sınırları ve içeriği hem kişiler hem de idare yönünden açık olarak belirlenmiştir.

12. Kuralda yer alan "uygun koordinasyon yöntemlerini uygulayabilme" ibaresinin soyut ve genel bir kavram olmasının ise bir önceki kuralın Anayasa'ya aykırılık sorununun incelendiği bölümde belirtilen gerekçeye dayandığı anlaşılmaktadır.

13. Günümüzde istihbarat servisleri sadece ülkelerin istihbarat ihtiyaçlarının karşılanması görevlerini yerine getirmemekte, arabuluculuk başta olmak üzere çeşitli diplomasi araçları açısından da işlev görebilmektedirler. Bu çerçevede, MİT'e verilen her türlü kurum, kuruluş, örgüt, oluşum ve kişilerle ilişki kurabilme yetkisinin, veriliş amacına uygun ve etkin olarak kullanılabilmesi için, karmaşık ve çok boyutlu ilişkiler içeren temaslarda, farklı durumlara göre farklı ve uygun yöntemlerin uygulanması gereği ortaya çıkabilmektedir. Bu itibarla görevin niteliğinden kaynaklanan esnekliği sağlamak üzere dava konusu kuralın düzenlenmesinde, hukuki belirlilik ilkesine aykırı düşen bir yön bulunmamaktadır.

14. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

C- Kanun'un 3. Maddesiyle Değiştirilen 2937 Sayılı Kanun'un 6. Maddesinin Birinci Fıkrasının (b) Bendinin İncelenmesi

1- İptal Talebinin Gerekçesi

15. Dava dilekçesinde özetle dava konusu kuralla MİT'e kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, Bankacılık Kanunu kapsamındaki kurum ve kuruluşlar ile diğer tüzel kişiler ve tüzel kişiliği bulunmayan kuruluşlardan bilgi, belge, veri ve kayıtları alabilme, bunlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim alt yapısından yararlanabilme ve bunlarla irtibat kurabilme yetkisinin verildiği, ayrıca kuralda anılan kurum ve kuruluşların kendi mevzuatlarındaki hükümleri gerekçe göstermek suretiyle talebin yerine getirilmesinden kaçınamayacaklarının düzenlendiği, bu durumun anılan kuruluşların uhdesinde bulunan ve kişilerin

özel hayatına ilişkin gizli kalması gereken bilgilerin MİT'in eline geçmesi sonucunu doğuracağı, dolayısıyla kuralın özel hayatın gizliliği ve hukuk devleti ilkelerini zedeleyeceği, öte yandan, kuralda yer alan tüzel kişiliği bulunmayan kuruluş ibaresiyle ne kastedildiğinin açık olmadığı, bu nedenle kuralın belirsizlik taşıdığı belirtilerek Anayasa'nın 2. ve 20. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

16. 6216 sayılı Kanun'un 43. maddesi uyarınca dava konusu kural, ilgisi nedeniyle Anayasa'nın 13. maddesi yönünden de incelenmiştir.

17. Dava konusu kuralda, MİT'in kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, Bankacılık Kanunu kapsamındaki kurum ve kuruluşlar ile diğer tüzel kişiler ve tüzel kişiliği bulunmayan kuruluşlardan bilgi, belge, veri ve kayıtları alabileceği, bunlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim alt yapısından yararlanabileceği ve bunlarla irtibat kurabileceği, bu kapsamda talepte bulunulanların, kendi mevzuatlarındaki hükümleri gerekçe göstermek suretiyle talebin yerine getirilmesinden kaçınamayacakları düzenlenmektedir. Buna göre, kural uyarınca bilgi, belge, veri ve kayıt verme yükümlülüğü bulunanlar arasında gerçek kişilerin bulunmadığı açık olup kurulla gerçek kişiler dışındaki kurum ve kuruluşlar yönünden bir yükümlülük getirilmektedir.

18. Anayasa'nın 20. maddesinin birinci fıkrasında, "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz." denilerek özel hayatın gizliliği hakkı güvence altına alınmıştır. Ancak aynı maddenin ikinci fıkrasında, özel hayatın gizliliğine çeşitli sebeplere bağlı kalınarak sınırlamalar getirilebileceği belirtilerek bu hakkın mutlak olmadığı kabul edilmiştir. Maddede bu sınırlama sebepleri arasında millî güvenliğin ve kamu düzeninin korunması ile suç işlenmesinin önlenmesi sebepleri de sayılmış, böylece bunlara dayalı olarak anılan hakkın sınırlandırılabilmesine imkân tanınmıştır. Ancak 20. maddenin ikinci fıkrasında söz konusu sınırlandırmanın "arama" tedbirine özgü olarak yapılabileceği belirtildiğinden, bu sebepler 20. madde bağlamında dava konusu kural yönünden meşru bir sınırlandırma nedeni olarak kabul edilmeyebilir. Bununla birlikte, özel hayatın düzenlendiği maddede dava konusu kuralda belirtilen bilgi toplama yetkisi yönünden özel sınırlama sebeplerine yer verilmediğinin kabulü halinde bile bu hakkın Anayasa'nın diğer maddelerinde devlete bir görev olarak yüklenen millî güvenliğin ve kamu düzeninin sağlanması ile suç işlenmesinin önlenmesi amaçlarıyla sınırlandırılması mümkündür.

19. Anayasa'nın 20. maddesinin üçüncü fıkrasında ise herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı ifade edilmiştir. Maddede ayrıca kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir.

20. Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Ancak bu hak sınırsız olmayıp Anayasa'da güvence altına alınan temel hak ve özgürlüklerin korunması veya Anayasa'nın devlete bir görev olarak yüklediği millî güvenliğin, kamu düzeninin korunması ya da suç işlenmesinin önlenmesi gibi nedenlerle sınırlandırılabilir.

21. Nitekim Türkiye Cumhuriyeti'nin imzaladığı ancak uygulama kanununun yürürlüğe konamaması nedeniyle taraf olmadığı 1981 tarihli ve 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Avrupa Konseyi Sözleşmesi'nin 9. maddesinde de devlet güvenliği, kamu güvenliği, devletin ekonomik menfaatlerinin korunması ve suçlarla mücadele edilmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması ile verilerin istatistikî veya bilimsel amaçlarla kullanılması durumlarında kişisel verilerin korunmasına sınırlamalar getirilebileceği öngörülmüştür.

22. Ancak bu sınırlama yapılırken temel hak ve özgürlüklerin sınırlandırılması rejimini belirleyen Anayasa'nın 13. maddesine de uyulması gerekmektedir. Anayasa'nın 13. maddesi uyarınca özel hayatın gizliliği ve kişisel verilerin korunması hakları, yalnızca kanunla ve demokratik bir toplumda gerekli olduğu ölçüde sınırlandırılabilir. Ayrıca getirilen bu sınırlamalar, hakkın özüne dokunamayacağı gibi Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamaz.

23. Dava konusu kuralda, kamu kurum ve kuruluşlarıyla özel kurum ve kuruluşların uhdesinde bulunan bilgi, belge, veri ve kayıtların MİT tarafından temin edilebileceği belirtilmektedir. İstenilebilecek bu bilgiler arasında özel hayatın gizliliği kapsamında kalacak bilgiler ve kişisel veriler de bulunabileceğinden, kuralla özel hayatın gizliliği ve kişisel verilerin korunması haklarına sınırlama getirildiği açıktır. Ancak bu sınırlama, 2937 sayılı Kanun'un 4. maddesiyle MİT'e verilen görevlerin, yani ülkenin varlığına, bağımsızlığına, güvenliğine ve anayasal düzenine karşı içten ve

dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkında millî güvenlik istihbaratını devlet çapında oluşturma ve istihbarata karşı koyma görev ve sorumluluğunun yerine getirilebilmesini, dolayısıyla millî güvenliği, kamu düzenini ve suç işlenmesinin önlenmesini sağlamak amacıyla getirilmekte olup demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır.

24. Anılan kapsamda sınırlama yapılırken Kanun'da sınırlama aracının sınırlama amacına uygun ve orantılı şekilde kullanılmasını sağlayacak yasal güvencelere de yer verildiği, böylece hem özel hayatın gizliliği ve kişisel verilerin korunması haklarının özünün zedelenmesinin önlendiği, hem de bu haklar ile millî güvenliğin, kamu düzeninin sağlanması ve suç işlenmesinin önlenmesi gerekleri arasındaki makul dengenin kurulduğu görülmektedir.

25. Bu bağlamda, Kanun'un 6. maddesinin birinci fıkrasında, bilgi, belge, veri ve kayıt isteme yetkisinin, ancak MİT'in Kanun'da belirtilen görevlerini yerine getirirken kullanabileceği belirtilmiş, dolayısıyla bu yetki, MİT'in Kanun ile belirlenen görevlerini yerine getirirken ihtiyaç duyacağı bilgilerle sınırlandırılmıştır.

26. Aynı maddenin altıncı fıkrasında da madde hükümlerine göre yürütülen faaliyetler çerçevesinde elde edilen kayıtların, bu Kanun'da belirtilen amaçlar dışında kullanılamayacağı ve elde edilen bilgi ve kayıtların saklanmasında ve korunmasında gizlilik ilkesinin geçerli olacağı hükme bağlanmıştır. Böylece MİT'e verilen yetki kapsamında elde edilen bilgilerin gizliliğinin korunması teminat altına alınırken bunların sadece istihbarat faaliyetleri çerçevesinde kullanılabileceği belirtilerek anılan bilgilerin kural olarak adli soruşturma ve kovuşturmalarda kullanılmasının önüne geçilmiştir. Bu çerçevede örneğin savunma ve kişilerin kendilerini veya yakınlarını suçlayan beyanda bulunmaya zorlanamaması hakları kapsamında kalan bilgilerin yargılamada kullanılamaması güvence altına alınmıştır.

27. Bu konudaki bir başka güvence de Kanun'un ek 1. maddesinin birinci fıkrasında öngörülmüştür. Buna göre, MİT uhdesindeki istihbari nitelikteki bilgi, belge, veri ve kayıtlar ile yapılan analizler, Türk Ceza Kanununun İkinci Kitap Dördüncü Kısım Yedinci Bölümünde yer alan suçlar hariç olmak üzere, adli mercilerce istenemeyecektir.

28. Kanun'un 27. maddesinde ise MİT'in görev ve faaliyetleri kapsamında elde ettiği bilgi ve belgelerin herhangi bir şekilde yetkisiz kişilerce alınması veya bunların medya veya kitle iletişim araçlarıyla ifşa edilmesi veya yayılması eylemleri suç olarak düzenlenerek ağır cezai yaptırımlara bağlanmıştır. Bu fiillerin MİT mensupları tarafından işlenmesi halleri ise cezayı ağırlaştırıcı neden olarak öngörülmüştür. Aynı şekilde, 5237 sayılı Türk Ceza Kanunu'nun 136. maddesi uyarınca da

kişisel verileri hukuka aykırı olarak başkasına vermek, yaymak veya ele geçirmek suç olarak düzenlenmiştir.

29. Anılan hükümlerle dava konusu kural kapsamında elde edilecek bilgilerin amacı dışında kullanılmasını önleyecek ve kişilerin özel hayatına dair bilgilerin ve kişisel verilerin ifşa edilmesini önleyecek yasal güvencenin sağlandığı görülmektedir.

30. Kanunda, dava konusu kural kapsamında elde edilen bilgilerin gizliliğinin korunması ve amacı dışında kullanılmasını önleyecek yasal güvencelere yer verildiği gibi, bu bilgilerin kötüye kullanılıp kullanılmadığını denetleyecek mekanizmalara da yer verilmiştir. Bu bağlamda 2937 sayılı Kanun'un 6. maddesinin sekizinci fıkrasında, "Bu maddede yer alan faaliyetlerin denetimi, sıralı kurum amirleri, Başbakanlık teftiş elemanları (.) tarafından yapılır." denilerek dava konusu kural kapsamında elde edilen bilgilerin amacına uygun olarak kullanılıp kullanılmadığını başta Başbakan olmak üzere diğer sıralı amirlerin ve Başbakanlık Teftiş Kurulu elemanlarının denetleyebileceği hükme bağlanmıştır.

31. Aynı şekilde, 1.4.1981 tarihli ve 2443 sayılı Devlet Denetleme Kurulu Kurulması Hakkında Kanun'un 2. maddesi uyarınca Devlet Denetleme Kurulu da MİT'in görev ve faaliyetine ilişkin olarak her türlü inceleme, araştırma ve denetleme yapma görev ve yetkisine sahip olup aynı Kanun'un 6. maddesi uyarınca tespit edilen hukuka aykırılıklarla ilgili gerekli idari ve adli sürecin başlatılması mümkün bulunmaktadır.

32. Bunların dışında, 6532 sayılı Kanun'un 12. maddesiyle 2937 sayılı Kanun'a eklenen ek 2. maddeyle MİT de dâhil olmak üzere güvenlik faaliyetleri ve istihbari nitelikteki faaliyetler konusunda çalışmak üzere Türkiye Büyük Millet Meclisi (TBMM) bünyesinde, siyasi parti gruplarının güçleri oranında temsil edildiği TBMM üyelerinden oluşan Güvenlik ve İstihbarat Komisyonunun kurulduğu görülmektedir. Güvenlik ve istihbarat faaliyetlerine ilişkin yıllık rapor hazırlayarak bunu Meclis Başkanlığına sunma görev ve yetkisine sahip olan bu Komisyonun, güvenlik ve istihbarat hizmetleri sırasında elde edilen kişisel verilerin güvenliğini ve bireyin hak ve özgürlüklerini koruyucu öneriler geliştirme yetkisi de bulunmaktadır. Bu çerçevede dava konusu kural kapsamında elde edilen bilgilerin kötüye kullanılmasını önlemeye yönelik Meclis denetimini sağlayacak mekanizmanın da kurulduğu görülmektedir.

33. Bu yönleriyle dava konusu kuralla özel hayatın gizliliği ve kişisel verilerin korunması haklarına getirilen sınırlamanın, söz konusu hakların özünü zedelediğinden söz edilemeyeceği gibi demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı düşüğü de söylenemez.

34. Öte yandan, Türk hukuk sisteminde, kamu kurum ve kuruluşlarının veya özel kuruluşların tüzel kişiliğe sahip olma zorunlulukları bulunmamakta olup tüzel kişiliği bulunmayan kuruluşlara da yer verilmiş bulunmaktadır. Dava konusu bendin birinci cümlesinde yer alan "tüzel kişiliği bulunmayan kuruluş" ibaresiyle, tüzel kişiliği bulunmayan kamu veya özel nitelikli kuruluşların kastedildiği açık olup bu yönüyle kuralın belirsizliğe neden olan bir yönü de bulunmamaktadır.

35. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2., 13. ve 20. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

36. Alparslan ALTAN ve Erdal TERCAN bendin ikinci cümlesi yönünden bu görüşe katılmamışlardır.

Ç- Kanun'un 3. Maddesiyle Değiştirilen 2937 Sayılı Kanun'un 6. Maddesinin Birinci Fıkrasının (c) Bendinin İncelenmesi

1- İptal Talebinin Gerekçesi

37. Dava dilekçesinde özetle dava konusu kuralla MİT'e bazı soruşturma ve kovuşturma dosyalarından bilgi ve belge alma yetkisinin verildiği, bu durumun soruşturma ve kovuşturmalardaki bilgilerin ve uygulanacak tedbirlerin açığa çıkmasıyla birlikte soruşturma ve kovuşturmanın amacına ulaşmasına engel olacağı belirtilerek kuralın, Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

38. 6216 sayılı Kanun'un 43. maddesi uyarınca dava konusu kural, Anayasa'nın 36. maddesi yönünden de incelenmiştir.

39. Dava konusu kuralda, MİT'e 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun İkinci Kitap Dördüncü Kısım Dört, Beş, Altı ve Yedinci bölümlerinde yer alan suçlara (318., 319., 324., 325. ve 332. maddeleri hariç olmak üzere) ilişkin soruşturma ve kovuşturmalarda, ifade tutanaklarına, her türlü bilgi ve belgeye erişebilme ve bunlardan örnek alabilme yetkisi tanınmaktadır.

40. Anayasa'nın 2. maddesinde, Türkiye Cumhuriyeti, bir hukuk devleti olarak nitelendirilmiştir. Hukuk devleti, eylem ve işlemleri hukuka uygun, insan haklarına dayanan, bu hak ve özgürlükleri koruyup güçlendiren her alanda adaletli bir hukuk düzeni kurup bunu geliştirerek sürdüren, Anayasa'ya aykırı durum ve tutumlardan kaçınan, hukuku tüm devlet organlarına egemen kılan, Anayasa ve hukuk kurallarıyla kendini bağlı sayıp yargı denetimine açık olan devlettir.

41. İnsan haklarına dayanan, bu hak ve özgürlükleri koruyup güçlendiren ve her alanda adaletli bir hukuk düzeni kurup bunu korumakla yükümlü olan hukuk devletinin önemli gereklerinden biri de hiç şüphesiz insan hak ve özgürlükleri yönünden tehdit içeren suçla etkin bir şekilde mücadele etmektir. Ancak bu mücadele yapılırken Anayasa'nın 36. maddesinde güvence altına alınan "adil yargılanma hakkı" uyarınca şüpheli ve sanık haklarının ihlal edilmesinin önlenmesi, bu çerçevede suçun soruşturulması ve kovuşturulması süreçlerinin etkin ve adil bir şekilde işletilmesini sağlayacak tedbirlerin alınması gerekir.

42. Etkin ve adil bir soruşturmanın koşullarından biri, soruşturmanın gizliliği ilkesidir. Bu ilke sayesinde, bir taraftan soruşturma işlemlerinin açığa çıkmasının önüne geçilerek delillerin karartılması ve soruşturmanın amacının tehlikeye düşmesi önlenmekte, diğer taraftan da kişilerin kamuoyunda suçlu olarak gösterilmesinin önüne geçilmektedir. Bu yönüyle soruşturmanın gizliliği, hem maddi gerçeğin ortaya çıkarılması için bir zorunluluk arz etmekte, hem de Anayasa'nın 38. maddesinde güvence altına alınan "suçsuzluk karinesi"nin gereklerinin yerine getirilmesine yardımcı olmaktadır.

43. Kovuşturma aşaması yönünden ise kural olarak alenilik ilkesi geçerli olup bu süreçle ilgili olarak yargılamanın kamuya açık ve kamunun denetiminde gerçekleşmesi gerekmektedir.

44. Dava konusu kuralla MİT'e bazı suçlara ilişkin soruşturma ve kovuşturmalarda ifade tutanaklarına, her türlü bilgi ve belgeye erişebilme ve bunlardan örnek alma yetkisi verilerek soruşturmanın gizliliği ilkesine bir istisna getirilmekte, ayrıca kovuşturma aşamasıyla ilgili olarak sadece ilgililerine tanınan belge alma yetkisi MİT'e de tanınmış bulunmaktadır. Ancak bu yetki tanınırken kuralda bir sınırlama öngörülmekte ve tüm suçlara ilişkin soruşturma ve kovuşturmalara ilişkin değil, sadece devletin güvenliğine, anayasal düzene, bu düzenin işleyişine, millî savunmaya ve devletin sırlarına karşı işlenen suçlara yönelik bir yetki verilmektedir.

45. 2937 sayılı Kanun'un 4. maddesinde MİT'in görevleri sayılmış ve bu görevler arasında ülkenin varlığına, bağımsızlığına, güvenliğine ve anayasal düzenine karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkında millî güvenlik istihbaratını devlet çapında oluşturma ve istihbarata karşı koyma görev ve sorumluluğunun da bulunduğu belirtilmiştir.

46. Kuralda MİT'e verilen yetkinin anılan suçlarla sınırlandırılması, bu suçların doğrudan MİT'in görev alanıyla ilgili olanları kapsamaması ve kuralın objektif metni ile gerekçesi bir bütün olarak değerlendirildiğinde bu yetkinin, MİT'e yukarıda anılan görevleri etkin bir şekilde yerine getirmek üzere verildiğini göstermektedir.

47. MİT'e verilen bu görevlerin niteliği dikkate alındığında ise bunların, kişilerin temel hak ve özgürlüklerini, anayasal düzeni ve toplumun güvenliğini tesis etmekle görevli devletin varlığı, bağımsızlığı ve anayasal düzenin devamı yönünden önemli olduğu, dolayısıyla bu görevlerin etkin bir şekilde yürütülmesinde, önemli bir kamu yararının bulunduğu sonucuna ulaşılmaktadır.

48. Kuralla bu şekilde kamu yararının sağlanması amacıyla MİT'e söz konusu bilgilere erişim yetkisi tanınırken, Kanun'un diğer hükümleriyle bu yetkinin amacı dışında kullanılmasını ve kişilerin kamuoyunda suçlu olarak gösterilmesini önleyecek tedbirlere yer verildiği görülmekte, böylece kuralın ölçülü olmasının sağlandığı anlaşılmaktadır.

49. Bu bağlamda, 5237 sayılı Türk Ceza Kanunu'nun 285. maddesi uyarınca soruşturmanın gizliliğini ihlal etmek suçtur ve bu suçun dava konusu kural nedeniyle gizli soruşturma işlemleri hakkında bilgi sahibi olan MİT mensupları yönünden de geçerli olduğu hususunda bir kuşku bulunmamaktadır. 2937 sayılı Kanun'un 6. maddesinde de MİT'in elde ettiği bilgi ve belgelerin gizliliği hükümlerine yer verilmiş ve 27. maddesinde MİT'in görev ve faaliyetleri kapsamında elde ettiği bilgi ve belgelerin herhangi bir şekilde yetkisiz kişilerce alınması veya bunların medya veya kitle iletişim araçlarıyla ifşa edilmesi veya yayılması eylemleri suç olarak düzenlenerek ağır cezai yaptırımlara bağlanmıştır. Bu fiillerin MİT mensupları tarafından işlenmesi halleri ise cezayı ağırlaştırıcı neden olarak öngörülmüştür.

50. Dava konusu kural uyarınca temin edilmesi öngörülen bilgiler de bu kapsamda kalmakta olup söz konusu bilgilerin amacı dışında ve kişilerin kamuoyunda suçlu olarak gösterilmelerine neden olacak şekilde kullanılmasını önleyecek yasal güvence sağlanmıştır.

51. Aynı gerekçelerle kuralın gizli soruşturma işlemlerini açığa çıkarması, dolayısıyla delillerin karartılması ve soruşturmanın amacına ulaşmasını tehlikeye düşürmesi de söz konusu değildir. Ayrıca MİT görevlilerinin de soruşturmada görev alan kolluk görevlileri gibi genel görevli güvenlik kurumu personeli olduklarının dikkate alınması gerekir.

52. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2. ve 36. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

D- Kanun'un 3. Maddesiyle Değiştirilen 2937 Sayılı Kanun'un 6. Maddesinin Birinci Fıkrasının (i) Bendinde Yer Alan ". alan veya ." İbaresinin İncelenmesi

1- İptal Talebinin Gerekçesi

53. Dava dilekçesinde özetle dava konusu kuralla MİT'e, hâlen görev yapmakta olan mensuplarına güvenilirliklerini ve uygunluklarını belirlemek üzere test teknik ve yöntemlerini uygulama yetkisinin

verildiği, oysa bu kişilerin, daha önce güvenilirlikleri ve uygunlukları tespit edilerek mesleğe alındıkları, dolayısıyla güvenilirlikleri ve mesleğe uygunlukları tespit edilerek göreve alınan bu kişilerin yeniden böyle bir teste tabi tutulmasına imkân tanınmasının, kişilerin insan onuruna aykırı bir muameleye maruz kalması sonucunu doğurduğu belirtilerek kuralın, Anayasa'nın 2. ve 17. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

54. Anayasa'nın 17. maddesinin birinci fıkrasında, "Herkes yaşama, maddî ve manevî varlığını koruma ve geliştirme hakkına sahiptir." denilmiş, üçüncü fıkrasında ise ".kimse insan haysiyetiyle bağdaşmayan bir cezaya veya muameleye tâbi tutulamaz." hükmüne yer verilmiştir.

55. Buna göre, kişinin maddî ve manevî varlığının korunması ve geliştirilmesi hakkının doğal bir sonucu olarak insan onuruna saygı gösterilmesi ve kimsenin insan onuruyla bağdaşmayan bir muameleye tabi tutulmaması gerekir. İnsan onuruna saygı gösterilmesi ise insanın ne durumda, hangi şartlar altında bulunursa bulunsun sırf insan oluşunun kazandırdığı değer tanınmasını ifade eder.

56. Dava konusu kuralla MİT'e, bünyesinde görev alan kişilerin güvenilirliklerini ve uygunluklarını belirlemek için yalan makinesi uygulaması dâhil test teknik ve yöntemlerini kullanabilme yetkisi tanınmaktadır.

57. Devletin millî güvenliği açısından önemli ve çoğu kez gizli olan bilgilere vâkıf olan istihbarat teşkilatı mensuplarının, bu bilgileri yetkisiz kişi ve kuruluşlarla paylaşmalarının, devletin millî güvenliği açısından ciddi tehditler yaratabileceği açıktır. Bu nedenle istihbarat teşkilatlarında, millî güvenlik açısından oldukça önemli ve gizli olan bu bilgilerin yetkisiz kişi ve kuruluşların eline geçmesinin önlenmesi için en üst düzeyde güvenlik önlemlerinin alınması gerekebilmekte ve bu gereklilik istihbarat teşkilatlarının diğer kamu kuruluşlarından farklı güvenlik standartlarını geliştirmelerine neden olabilmektedir.

58. Öte yandan, istihbarat teşkilatlarının elindeki bilgilerin öneminin ve mahiyetinin onları yabancı istihbarat teşkilatlarının hedefi haline getirmesi, bu farklı güvenlik standardının belirlenmesi zarureti arttıran bir unsur olarak ortaya çıkmaktadır.

59. Dava konusu kuralla anılan farklı güvenlik standardının zorunlu bir gereği olarak MİT'e söz konusu yetkinin verildiği anlaşılmaktadır.

60. Kuralda anılan test ve tekniklerin, MİT'te görev alan bazı kişilere değil, herhangi bir ayırım yapmaksızın herkese uygulanabileceği düzenlenmiştir. Bu da kuralla özel olarak bazı kişilerin hedef

alınmadığını, düzenlemenin MİT tarafından yürütülen görevin doğasından kaynaklanan bir zorunluluğa dayandığını göstermektedir.

61. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2. ve 17. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

E- Kanun'un 3. Maddesiyle 2937 Sayılı Kanun'un 6. Maddesine Eklenen Onbirinci Fıkrafta Yer Alan ".yukarıdaki hükümlere ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın; MİT Müsteşarı veya yardımcısının onayıyla." İbaresinin İncelenmesi

1- İptal Talebinin Gerekçesi

62. Dava dilekçesinde özetle dava konusu ibarenin de yer aldığı kuralla MİT'e 2937 sayılı Kanun'un 6. maddesindeki ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın; MİT Müsteşarı veya yardımcısının onayıyla yurt dışında veya yabancılar tarafından gerçekleştirilen iletişim ile ankesörlü telefonlarla gerçekleştirilen iletişimin ve MİT mensuplarının, MİT'te görev almış olanların veya görev almak üzere başvuranların iletişiminin denetlenmesi yetkisinin verildiği, verilen bu yetkinin sınırsız ve belirsiz olduğu, kuralla MİT'e 2937 sayılı Kanun'un 6. maddesindeki ve diğer kanunlardaki düzenlemelere bağlı kalmama yetkisinin verilmesinin yasama yetkisinin devri anlamına geldiği, ayrıca kuralla bu şekilde herhangi bir sınır olmaksızın kişilerin iletişiminin denetlenmesine izin verilmesinin özel hayatın korunması hakkını ve haberleşme hürriyetini zedelediği belirtilerek kuralın, Anayasa'nın 2., 7., 20. ve 22. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

63. 6216 sayılı Kanun'un 43. maddesi uyarınca dava konusu kural, ilgisi nedeniyle Anayasa'nın 13. maddesi yönünden de incelenmiştir.

64. Kanun'un dava konusu ibareyi de içeren onbirinci fıkrasında, önleyici istihbarat elde etmek ve analiz yapabilmek amacıyla Kanun'un 6. maddesindeki hükümlere ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın; MİT Müsteşarı veya yardımcısının onayıyla yurt dışında veya yabancılar tarafından gerçekleştirilen iletişim ile ankesörlü telefonlarla gerçekleştirilen iletişimin ve MİT mensuplarının, MİT'te görev almış olanların veya görev almak üzere başvuranların iletişiminin tespit edilebileceği, dinlenebileceği, sinyal bilgilerinin değerlendirilebileceği ve kayda alınabileceği (iletişimin denetlenebileceği) düzenlenmektedir.

65. Anayasa'nın 2. maddesinde yer alan hukuk devletinin temel ilkelerinden biri "belirlilik ilkesi"dir. Bu ilkeye göre, yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya

ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olması, ayrıca kamu otoritelerinin keyfi uygulamalarına imkân tanımaması gerekir.

66. Anayasa'nın 7. maddesinde, "Yasama yetkisi Türk Milleti adına Türkiye Büyük Millet Meclisinindir. Bu yetki devredilemez." denilmiştir. Buna göre, Anayasa'da kanun ile düzenlenmesi öngörülen konularda yürütme organına genel ve sınırları belirsiz bir düzenleme yetkisinin verilmesi olanaklı değildir.

67. Dava konusu ibarenin de yer aldığı fıkrayla MİT'e görev ve yetkisi kapsamında kalan önleyici istihbarat elde etme ve analiz yapabilme amacıyla iletişimi denetleme yetkisi verilmekte olup bu yetki verilirken yetkinin hangi amaçla, hangi hallerde, ne şekilde, hangi mercilerin ne tür izniyle ve kimleri kapsayacak şekilde kullanılacağına ilişkin kurallar hem kişiler hem de idare yönünden açık şekilde düzenlenerek konuya ilişkin temel kurallar kanunla belirlenmiştir.

68. Fıkroda, MİT'in bu yetkiyi, "Önleyici istihbarat elde etmek ve analiz yapabilmek amacıyla yukarıdaki hükümlere ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın" kullanabileceğinin belirtilmiş olması ise kuşkusuz MİT'in bu yetkiyi dilediği şekilde ve herhangi bir kurala bağlı olmaksızın kullanabileceği anlamında değil, iletişimin denetlenmesiyle ilgili mevzuatta bulunan diğer hükümlere bağlı olmaksızın ve fakat fıkroda yer alan kurallara bağlı kalarak kullanabileceğini belirtmek içindir.

69. Aynı hukuki kurumla ilgili farklı düzenlemeler yapılırken esas alınacak kuralların birbirine karıştırılmaması veya bir diğerine uygulanmaması için zaman zaman uygulanan bu yöntemin, kanun yapma tekniğinin zorunlu bir sonucu olduğu açık olup bununla MİT'e, kanunların üstünde genel ve sınırları belirsiz bir yetkinin verildiğinin kabul edilmesi mümkün değildir.

70. Öte yandan, Anayasa'nın 20. maddesinin birinci fıkrasında, "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz." ve 22. maddesinin birinci fıkrasında, "Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır." denilmek suretiyle temel hak ve özgürlükler arasında yer alan özel hayatın ve haberleşmenin gizliliği hakları güvence altına alınmıştır. Anılan maddelerin ikinci fıkralarında ise bu hakların çeşitli sebeplere bağlı kalınarak sınırlandırılabilmesi belirtilerek, bu hakların mutlak olmadığı ve maddelerinde belirtilen sebeplerle sınırlandırılabilmesi kabul edilmiştir. Maddelerde bu sınırlama sebepleri arasında millî güvenliğin ve kamu düzeninin sağlanması sebepleri de sayılmış böylece bunlara dayalı olarak anılan hakların sınırlandırılabilmesine imkân tanınmıştır. 20. maddenin ikinci fıkrasında söz konusu sınırlandırma nedenlerinin "arama" tedbirine özgü olarak

uygulanabileceği kabul edilse bile 18. paragrafta belirtilen gerekçelerle bu hakkın da millî güvenliğin ve kamu düzeninin sağlanması amaçlarıyla sınırlandırılması mümkündür.

71. Ayrıca haberleşme hürriyetinin özel olarak düzenlendiği 22. maddenin ikinci fıkrasında, söz konusu sınırlama sebeplerine bağlı kalınarak yapılacak sınırlamanın ancak usulüne uygun olarak verilecek hâkim kararıyla mümkün olabileceği belirtildikten sonra üçüncü fıkrasında "İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir." denilerek bu kuralın da mutlak olmadığı ve bu kurala bazı kurumlar yönünden kanunla sınırlamalar getirilebileceği açıkça belirtilmiştir.

72. Ancak özel hayatın ve haberleşmenin gizliliği haklarının sınırlandırılabilmesi için maddelerinde belirtilen sebeplerin varlığı yeterli olmayıp temel hak ve özgürlüklerin sınırlandırılması rejimini belirleyen Anayasa'nın 13. maddesine de uyulması gerekmektedir. Anayasa'nın 13. maddesi uyarınca özel hayatın ve haberleşmenin gizliliği hakları, yalnızca kanunla ve demokratik bir toplumda gerekli olduğu ölçüde sınırlandırılabilir. Ayrıca getirilen bu sınırlamalar, hakkın özüne dokunamayacağı gibi Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamaz.

73. Anayasal açıdan dokunulamayacak öz, her temel hak ve özgürlük açısından farklılık göstermekle birlikte kanunla getirilen sınırlamanın hakkın özüne dokunmadığının kabulü için temel hakların kullanılmasını ciddi surette güçleştirip, amacına ulaşmasına engel olmaması ve etkisini ortadan kaldıracı bir nitelik taşımaması gerekir. Ancak bu durumda sınırlamanın demokratik toplum düzeninin gereklerine uygun olduğu söylenebilir.

74. Ölçülülük ise amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder. Ölçülülük, aynı zamanda yasal önlemin sınırlama amacına ulaşmaya elverişli olmasını, amaç ve aracın ölçülü bir oranı kapsamasını ve sınırlayıcı önlemin demokratik toplum düzeni bakımından zorunluluk taşımasını da içeren bir ilkedir.

75. Dava konusu ibareyi de içeren kuralla, MİT Müsteşarı veya yardımcısının onayıyla bazı koşullarda kişilerin iletişiminin tespit edilmesi, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesine izin verilerek özel hayatın ve haberleşmenin gizliliği haklarına bir sınırlama getirilmektedir.

76. Ancak bu sınırlama getirilirken Kanun'da sınırlama aracının sınırlama amacına uygun ve orantılı şekilde kullanılmasını sağlayacak yasal önlemlere yer verildiği, böylece hem özel hayatın ve haberleşmenin gizliliği haklarının özünün zedelenmesinin önlendiği, hem de bu hakların korunması

ile millî güvenliğin ve kamu düzeninin sağlanması arasındaki makul dengenin kurulduğu görülmektedir.

77. Bu bağlamda, kuralla 2937 sayılı Kanun'un 4. maddesiyle MİT'e verilen görevlerin, yani ülkenin varlığına, bağımsızlığına, güvenliğine ve anayasal düzenine karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkında millî güvenlik istihbaratını devlet çapında oluşturma ve istihbarata karşı koyma görev ve sorumluluğunun yerine getirilebilmesini teminen ve sadece önleyici istihbarat elde etmek ve analiz yapabilmek, dolayısıyla millî güvenliğin ve kamu düzeninin sağlanması amacıyla özel hayatın ve haberleşmenin gizliliği haklarına bir sınırlama getirildiği ve bu sınırlamanın, demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kaldığı anlaşılmaktadır.

78. Zira demokratik ülkelerde örnekleri görüldüğü üzere bazı istisnai durumlarda, özellikle de millî güvenliği tehdit eden terör ve casusluk faaliyetlerine karşı telekomünikasyon yoluyla yapılan iletişimin denetlenmesine ihtiyaç duyulabilmektedir. Bu çerçevede, ülkenin varlığına, bağımsızlığına, güvenliğine ve anayasal düzenine karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkında millî güvenlik istihbaratını devlet çapında oluşturabilmek için ve bu amaçların gerçekleştirilmesiyle sınırlı olmak üzere yurtdışında veya yabancılar tarafından yurt içinde gerçekleştirilen iletişim ile ankesörlü telefonlarla gerçekleştirilen iletişimin veya millî güvenlik açısından son derece önemli ve gizli bilgilere vâkıf olan MİT mensuplarının gerçekleştirdiği iletişimin denetlenmesi önlemine başvurulması gerekebilir.

79. Bu yönüyle, kanun koyucunun, herkesi kapsamayacak şekilde ve sadece kuralda belirtilen sınırlı alanla ilgili olarak MİT'i, Anayasa'nın 22. maddesinin üçüncü fıkrasında belirtilen istisnaları uygulayabilecek kamu kuruluşu niteliğinde sayması mümkün görülmektedir.

80. Ayrıca daha önce de belirtildiği üzere Kanun'un 27. maddesinde MİT'in görev ve faaliyetleri kapsamında elde ettiği bilgilerin gizliliği prensibi benimsenmiş ve bunların herhangi bir şekilde yetkisiz kişilerce alınması veya medya ya da kitle iletişim araçlarıyla ifşa edilmesi veya yayılması eylemleri suç olarak düzenlenerek ağır cezai yaptırımlara bağlanmıştır. Bu fiillerin MİT mensupları tarafından işlenmesi halleri ise cezayı ağırlaştırıcı neden olarak öngörülmüştür. Aynı şekilde, 5237 sayılı Türk Ceza Kanunu'nun 132. maddesi uyarınca da kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa etmek suç olarak düzenlenmiş olup bu hüküm de haberleşmenin ve özel hayatın gizliliğinin korunmasında önemli bir güvence sağlamaktadır. Öte yandan, anılan yetki sadece önleyici istihbarat elde etmek ve analiz yapabilmek amacıyla verildiğinden bu yetkinin kullanılması

sonucu elde edilen bilgilerin anılan amaç dışında kullanılması, örneğin adli soruşturma ve kovuşturmalarda kullanılması mümkün değildir.

81. Mevzuatta dava konusu kural kapsamında elde edilen bilgilerin gizliliğinin korunması ve amacı dışında kullanılmasını önleyecek yasal güvencelere yer verildiği gibi bu bilgilerin kötüye kullanılıp kullanılmadığını denetleyecek güvencelere de yer verildiği görülmektedir. Bu bağlamda anılan yetkinin veya bu yetki nedeniyle elde edilen bilgilerin amacı dışında kullanılması, bir başka ifadeyle millî güvenlik istihbaratını oluşturmak üzere önleyici istihbarat elde edilmesi veya analiz yapılması amaçları dışında kullanılması hâlinde kişilerin yargı yoluna başvurmaları mümkündür.

82. Bunların dışında, 2937 sayılı Kanun'un ek 2. maddesiyle TBMM bünyesinde kurulan Güvenlik ve İstihbarat Komisyonunun dava konusu kural kapsamındaki uygulamanın kötüye kullanılmasını önlemeye yönelik Meclis denetimi yapma yetkisine sahip olduğunun da belirtilmesi gerekir.

83. Bu çerçevede anılan hükümlerle söz konusu bilgilerin amacı dışında kullanılmasını ve kişilerin özel hayatına dair bilgilerin ifşa edilmesini önleyecek yasal güvencenin sağlandığı söylenebilir.

84. Bu yönleriyle dava konusu ibareyle özel hayat ve haberleşme hürriyetinin gizliliği haklarına getirilen sınırlamanın, söz konusu hakların özünü zedelediğinden söz edilemeyeceği gibi demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı düştüğü de söylenemez.

85. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2., 7., 13., 20. ve 22. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

86. Serruh KALELİ bu sonuca farklı gerekçeyle katılmıştır.

87. Zühtü ARSLAN, Engin YILDIRIM, Alparslan ALTAN, Erdal TERCAN ve M. Emin KUZ fıkrada yer alan ".yurt dışında veya yabancılar tarafından gerçekleştirilen iletişim ile ankesörlü telefonlarla gerçekleştirilen iletişim." ibaresi yönünden bu görüşe katılmamışlardır.

F- Kanun'un 6. Maddesiyle 2937 Sayılı Kanun'un 26. Maddesine Eklenen İkinci Fıkranın İkinci Cümlesinin İncelenmesi

1- İptal Talebinin Gerekçesi

88. Dava dilekçesinde özetle dava konusu kuralla MİT'in görev ve faaliyeti kapsamında olduğunu belirttiği veya belgelendirdiği eylemlerle ilgili olarak Cumhuriyet savcılarının soruşturma yapma ve kamu davası açma yetkisinin kaldırıldığı, bu durumun hukuk devleti ilkesiyle çeliştiği, kuralla MİT'e diğer hiçbir kişi ve kurumda bulunmayan bir ayrıcalık tanındığı, bunun kanun önünde eşitlik ilkesini zedelediği, ayrıca kuralla MİT'in görev ve faaliyeti kapsamında kalan eylemlerinin yargı denetimi

dışında bırakılmasının, idarenin tüm eylem ve işlemlerinin yargı denetimine açık olması gerektiği yönündeki anayasal kuralı ihlal ettiği belirtilerek dava konusu kuralın, Anayasa'nın 2., 10. ve 125. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

89. 2937 sayılı Kanun'un 26. maddesinin ikinci fıkrasının birinci cümlesinde Cumhuriyet savcılarının, MİT görev ve faaliyetleri ile mensuplarına ilişkin herhangi bir ihbar veya şikâyet aldıklarında veya böyle bir durumu öğrendiklerinde konuyu MİT Müsteşarlığına bildirecekleri belirtilmekte, dava konusu ikinci cümlesinde ise MİT Müsteşarlığının, konunun görev ve faaliyetlerine ilişkin olduğunu belirtmesi veya belgelendirmesi hâlinde adli yönden başkaca bir işlem yapılmayacağı ve herhangi bir koruma tedbirinin uygulanmayacağı düzenlenmektedir.

90. Anayasa'nın 2. maddesinde, Türkiye Cumhuriyeti bir hukuk devleti olarak nitelendirilmiş, 10. maddesinde kanun önünde eşitlik ilkesine yer verilmiş ve 125. maddesinin birinci fıkrasında "İdarenin her türlü eylem ve işlemlerine karşı yargı yolu açıktır." denilerek, idarenin tüm eylem ve işlemlerinin yargı denetimine tabi olacağı ilkesi kural olarak benimsenmiştir.

91. Çağdaş hukuk sistemlerinde, ceza yargılaması alanında, yaş, görev, unvan gibi kişilerin belli vasıfları dikkate alınarak bazı kişiler yönünden genel soruşturma ve kovuşturma usullerinden ayrı özel soruşturma ve kovuşturma usulleri belirlenebilmektedir. Bu tür kuralların getiriliş amacı ise bazı kişiler yönünden ayrıcalıklı/imtiyazlı bir sınıf oluşturmak değil genel olarak daha adil bir yargılama yapılmasını sağlamaktır.

92. Türk hukuk sistemi açısından konuya bakıldığında da 5271 sayılı Ceza Muhakemesi Kanunu'nun, herkes hakkında geçerli olan ceza soruşturması ve kovuşturması hükümlerine yer verdiği görülmektedir. Ancak anayasa koyucu ve kanun koyucu, uluslararası hukuk ve iç hukuktan kaynaklanan bazı nedenlere dayanarak bu genel kurallara istisnalar getirmiştir. Buna göre, suç isnadı yapılan herkes hakkında uygulanması gereken genel düzenlemeleri içeren 5271 sayılı Kanun hükümleri bazı kişiler bakımından uygulanmayacak, bunlar hakkında ilgili kanunlarındaki özel soruşturma ve kovuşturma usulleri geçerli olacaktır. Bu usullerin tanınması, uygulanacak kişilere bir zümre ya da sınıf olarak imtiyaz tanımak anlamına gelmeyip yapılan görevin niteliğinden kaynaklanmaktadır. Böylece, hem yapılan görevin en iyi şekilde ve etkin olarak yerine getirilmesi sağlanacak, hem de gereksiz şikâyetlere maruz kalınarak görülen hizmetin kesintiye uğraması engellenecektir.

93. Esasen Anayasa'nın 129. maddesinin son fıkrasında da "Memurlar ve diğer kamu görevlileri hakkında işledikleri iddia edilen suçlardan ötürü ceza kovuşturması açılması, kanunla belirlenen istisnalar dışında, kanunun gösterdiği idarî merciin iznine bağlıdır." denilmek suretiyle, kamu görevlileri yönünden özel soruşturma usullerinin uygulanması anayasal güvenceye kavuşturulmuş bulunmaktadır.

94. Dava konusu kuralda da millî güvenlik yönünden son derece önemli görevler yürüten MİT mensuplarının, yürüttükleri görevin niteliği nedeniyle özel bir soruşturma usulüne tabi kılındıkları anlaşılmaktadır.

95. Bu çerçevede, 2937 sayılı Kanun'un 26. maddesinin birinci fıkrasında, MİT mensuplarının görev suçları yönünden özel soruşturma usulü belirlenerek bu kişilerin soruşturulabilmesi için Başbakan'dan izin alınması gerektiğinin düzenlendiği, dava konusu kuralın yer aldığı ikinci fıkrasında ise bu usulün nasıl uygulanacağına açıklığa kavuşturulduğu görülmektedir.

96. Buna göre, Cumhuriyet savcıları, MİT görev ve faaliyetleri ile mensuplarına ilişkin herhangi bir ihbar veya şikâyet aldıklarında veya böyle bir durumu öğrendiklerinde, MİT Müsteşarlığına bildirimde bulunacaklar ve bu bildirim üzerine, MİT Müsteşarlığının, konunun görev ve faaliyetlerine ilişkin olduğunu belirtmesi veya belgelendirmesi hâlinde adli yönden başkaca bir işlem yapamayacak ve herhangi bir koruma tedbiri uygulayamayacaklardır. Ancak bu durumda da maddenin ilk fıkrasında belirtilen kural gereği görev suçu olduğu anlaşılan eylem yönünden Başbakan'dan izin alınarak soruşturma yapılabilecek ve Başbakan tarafından izin verilmemesi halinde bu işleme karşı idari yargı yoluna başvurulabilecektir.

97. Dava konusu kural, görev suçlarıyla ilgili olup MİT mensuplarının görevi dışındaki şahsi suçlarını düzenlememektedir. Ancak MİT mensuplarının görev suçlarıyla şahsi suçları arasında ayırım yapmanın, diğer kamu görevlilerine nazaran zor olduğunun da dikkate alınması gerekmektedir. Zira MİT'in görevlerinin niteliği nedeniyle birçok faaliyeti gizli olup bunların MİT'in yetkilileri dışındaki kimselerce bilinmesi söz konusu olmamaktadır. Kuralın lafzından ve madde gerekçesinden kuralla MİT'in görev ve faaliyetlerine ilişkin bu özellik nedeniyle kuralda belirtilen özel soruşturma usulünün belirlendiği, böylece millî güvenlik açısından gizli kalması gereken MİT görev ve faaliyetlerinin açığa çıkarılmasının veya engellenmesinin önlenmeye çalışıldığı anlaşılmaktadır.

98. Bu usulün benimsenmesi nedeniyle MİT'in, mensuplarının şahsi suçlarını da görev suçu kapsamında kaldığını belirterek Kanun'un başka bir hukuki müessese için öngördüğü usulün öngörmediği bir alanda kullanılabilmesine neden olabileceği, bunun da keyfiliğe yol açacağı düşünülebilir. Ancak Kanun'da bu sakıncanın ortaya çıkmasını engelleyecek yasal güvenceye yer

verildiği, dolayısıyla bir taraftan MİT'in gizli kalması gereken görev ve faaliyetlerinin açığa çıkması önlenirken diğer taraftan bunun keyfiliğe neden olmasının önüne geçecek tedbirlerin alındığı görülmektedir.

99. Bu bağlamda, öncelikle demokratik bir hukuk devletinde bir kamu kuruluşunun, mensuplarının şahsi suçlarını görev suçu olarak göstermesinin beklenemeyeceğinin belirtilmesi gerekir. Ancak MİT, bir mensubunun şahsi suçunu görev suçu olarak gösterse dâhi Cumhuriyet savcısının söz konusu kişiyle ilgili soruşturma yapma imkânı ortadan kalkmamakta, 2937 sayılı Kanun'un 26. maddesinin ikinci fıkrasının son cümlesi uyarınca görev suçu olduğu bildirilen eylemle ilgili olarak Başbakan'dan soruşturma izni istemesi ve Başbakanın da eylemi görev kapsamında kabul edip izin vermemesi hâlinde idari yargı yoluna başvurması mümkün bulunmaktadır. Dolayısıyla Başbakanın bu denetiminin ve akabindeki yargı denetiminin aslında kişisel suç kapsamında olan eylemlerin görev suçu kapsamında gösterilmesini önleyebilecek nitelikteki güvenceleri sağladığı açıktır.

100. Kanun koyucunun, izlediği ceza politikası uyarınca kanunlarla belirlenen görevlerini en iyi şekilde ve etkin olarak yerine getirmesini sağlamak, millî güvenliğe ilişkin gizli kalması gereken görev ve faaliyetlerin açığa çıkmasını ve görülen hizmetin kesintiye uğramasını önlemek üzere MİT mensupları yönünden görevin niteliğinden kaynaklanan farklı bir soruşturma usulü benimsemesi, takdir yetkisi kapsamında kalmakta olup bu yönüyle dava konusu kuralın, hukuk devleti ve kanun önünde eşitlik ilkesine aykırı düşen bir yönü bulunmamaktadır (Aynı yönde değerlendirmeler içeren kararlar için bkz. Anayasa Mahkemesinin 17.1.2013 tarihli ve E. 2012/19, K. 2013/17; 4.7.2013 tarihli ve E. 2012/100, K. 2013/84 sayılı kararları).

101. Öte yandan, düzenlemeyle MİT'in görevi kapsamındaki işlem ve faaliyetlerin yargı denetimi dışına çıkarılması da söz konusu değildir. Zira maddede atıfta bulunulan kişilerin görev suçları yönünden soruşturma yapılmasının izne bağlanması, söz konusu kişilerin işledikleri suçların yargı denetimi dışına çıkarılması sonucunu doğurmamaktadır. Bu kişilere ilişkin soruşturma izni verilmemesi kararı da bir idari işlem olup her idari işlem gibi bu işlem de Anayasa'nın 125. maddesi uyarınca yargı denetimine tabi bulunmaktadır. Dolayısıyla söz konusu kişiler hakkında soruşturma izninin verilmemesi hâllerinde idari yargı yoluna başvurmak suretiyle bu kararın kaldırılması ve bu kişiler hakkında yargılama yapılması mümkün bulunmaktadır.

102. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2., 10. ve 125. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

103. Alparslan ALTAN ve Erdal TERCAN bu görüşe katılmamışlardır.

G- Kanun'un 6. Maddesiyle 2937 Sayılı Kanun'un 26. Maddesine Eklenen Üçüncü Fıkırdaki Yer Alan "İsimsiz, imzasız, adresiz yahut takma adla yapıldığı anlaşılan ya da." ve ".delilleri ve dayanakları gösterilmeyen." İbarelerinin İncelenmesi

1- İptal Talebinin Gerekçesi

104. Dava dilekçesinde özetle dava konusu kuralla MİT'in görev ve faaliyetleri ile mensuplarına ilişkin isimsiz, imzasız, adresiz yahut takma adla yapıldığı anlaşılan ya da delilleri ve dayanakları gösterilmeyen ihbar ve şikâyetlerin, Cumhuriyet savcılarınca işleme konulmayacağına öngörüldüğü, bu durumun suç ve suçlunun kovuşturulması imkânını ortadan kaldırdığı, hak arama özgürlüğünü ve dilekçe hakkını ihlal ettiği, ayrıca 5271 sayılı Kanun'un 160. maddesi uyarınca Cumhuriyet savcısının ihbar veya başka bir suretle bir suçun işlendiği izlenimini veren bir hâli öğrenir öğrenmez kamu davasını açmaya yer olup olmadığına karar vermek üzere hemen işin gerçeğini araştırmak ve gerekli gördüğü takdirde ihbarın, şikâyetin, suç işlendiği izlenimi veren hâlin niteliğine ve türüne bakmaksızın iddianame tanzim edip kamu davasını açması gerektiği, dava konusu kuralla buna sınırlamalar getirilmesinin kanun önünde eşitlik ilkesini de zedelediği belirtilerek dava konusu kuralın, Anayasa'nın 2., 10., 36. ve 74. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

105. Dava konusu ibarelerin yer aldığı kuralda, MİT'in görev ve faaliyetleri ile mensuplarına ilişkin isimsiz, imzasız, adresiz yahut takma adla yapıldığı anlaşılan ya da belli bir olayı ve nedeni içermeyen, delilleri ve dayanakları gösterilmeyen ihbar ve şikâyetlerin, Cumhuriyet savcılarınca işleme konulmayacağı belirtilmekte, böylece anılan faaliyetlere ve görevlilere ilişkin ihbar ve şikâyete bağlı olarak soruşturma açılmasının şartları düzenlenmektedir.

106. İhbar ve şikâyet, suçları soruşturmakla görevli mercilerin herhangi bir suçun işlendiğini öğrenme yollarındandır. Ayrıca görevli mercilerin, basın yayın yoluyla, suçun işlendiğini öğrenen başka mercilerin bildirmesiyle veya doğrudan doğruya suç işlendiğini öğrenme yolları da vardır. İhbar, bir kimsenin suç işlendiğini yazılı veya sözlü olarak yetkili makamlara bildirmesidir. Şikâyet ise suçtan zarar gören kimsenin yazılı veya sözlü olarak yetkili makamlara başvurarak soruşturma açılmasını istemesidir. 5271 sayılı Ceza Muhakemesi Kanunu'nda, ceza ve disiplin soruşturmalarına ilişkin diğer özel kanunlarda ve kimi düzenleyici işlemlerde, ihbar ve şikâyetlerin şekil şartları, ihbar ve şikâyetlerin değerlendirilmesi yöntemleri ve hukuki sonuçları ayrıntılı olarak düzenlenmiştir.

107. Hukuk devletinde ceza soruşturmasına ilişkin kurallar, ceza muhakemesi hukukunun ana ilkeleri ile Anayasa'nın konuya ilişkin kuralları başta olmak üzere, ülkenin sosyal, kültürel yapısı, etik değerleri, sosyal ve hukuki ihtiyaçlar göz önüne alınarak saptanacak suç ve ceza siyasetine göre belirlenir. Kanun koyucu, takip ettiği suç ve ceza politikasının bir gereği olarak suç işlediği ileri sürülen kamu görevlilerinin cezasız kalmamaları ile bunların haksız yere soruşturulmamaları gereklerini gözeterek, bunlar arasında âdil bir denge kurabilir.

108. İhbar ve şikâyetle bulunma, Anayasa'nın 36. ve 74. maddelerinde güvence altına alınan hak arama özgürlüğünün ve dilekçe hakkının gerçekleştirilmesinin önemli araçları olmakla birlikte bunların kötüye kullanılarak kamu hizmetinin işleyişinin kısıtlanmasına veya engellenmesine yahut hakkında suç isnadında bulunulan kamu görevlisinin kişisel haklarının zedelenmesine neden olacak şekilde kullanılmasının hukuk düzenince himaye edilmesi düşünülemez. Bu nedenle yapılacak yasal düzenlemelerde anılan haklarla kamu hizmetlerinin aksatılmaması ve kamu görevlilerinin kişisel haklarının zarar görmemesi arasındaki âdil dengenin kurulması gerekmektedir.

109. Dava konusu kuralla MİT'in görev ve faaliyetleri ile mensuplarının görev ve faaliyetlerine ilişkin isimsiz, imzasız, adresiz yahut takma adla yapıldığı anlaşılan ya da delilleri ve dayanakları gösterilmeyen ihbar ve şikâyetlerin, Cumhuriyet savcılarınca işleme konulmayacağı öngörülmekle asılsız iddialarla kamu hizmetlerinin aksatılmasının önüne geçilmeye çalışıldığı anlaşılmaktadır. Öte yandan, kuralla asılsız ihbar ve şikâyetler nedeniyle soruşturulan veya yargılanan kamu görevlisinin şerefine, mesleki saygınlığının ve kişisel haklarının zarara uğraması durumunda kimin sorumlu olacağının bilinmesi temin edilerek kötü niyetli ihbar ve şikâyetlerin önlenmesi amaçlanmaktadır.

110. Kuralla bu şekilde tüm ihbar ve şikâyetler yönünden değil, sadece asılsız veya kötü niyetli olabilecek ihbar ve şikâyetler yönünden bir sınırlama getirilmiş olması, bir yandan kişilerin hak arama özgürlüğü ve dilekçe haklarını kullanmalarına imkân tanırken öteki yandan kamu hizmetlerinin aksatılmaması ve kamu görevlilerinin kişisel haklarının zarar görmemesi şeklindeki kamu yararının korunmasını sağlamaktadır. Böylece kuralla anılan haklar ve kamu yararı arasındaki âdil dengenin kurulması amaçlanmaktadır.

111. Kaldı ki kuralla Cumhuriyet savcısının hangi olay ve olguları ciddi bularak soruşturmaya başlayacağı yönündeki takdir yetkisi sınırlandırılmamakta, sadece isimsiz, imzasız, adresiz yahut takma adla yapıldığı anlaşılan ya da delilleri ve dayanakları gösterilmeyen ihbar ve şikâyetleri işleme koyma zorunluluğu ortadan kaldırılmaktadır. Zira Cumhuriyet savcısının soruşturmayı başlatmasının tek yolu aldığı ihbar ve şikâyetler olmayıp kendisi de herhangi bir şekilde öğrendiği bir olayla ilgili olarak resen soruşturma başlatma yetkisine sahip bulunmaktadır. Dava konusu kural

sadece ihbar ve şikâyetlere ilişkin olup Cumhuriyet savcısının resen başlatacağı soruşturmalara ilişkin bir hüküm içermemektedir.

112. Yasama yetkisinin genelliği ilkesi ve suç ve ceza siyasetini belirleme yetki ve görevi uyarınca, kamu görevlileri hakkında suç işlediklerine dair yapılan ihbar ve şikâyetlerin işleme konulabilmesi için gerekli koşulları belirlemek anayasal sınırlar içinde yasama organının takdir yetkisi içinde kalmaktadır. Dolayısıyla MİT'in görev ve faaliyetleri ile mensuplarına ilişkin ihbar ve şikâyetlerin işleme konulması yönünden dava konusu kuralla anılan koşulların düzenlenmesinde, hukuk devleti ilkesine, hak arama özgürlüğüne ve dilekçe hakkının gereklerine aykırı düşen bir yön bulunmamaktadır.

113. Ayrıca mevzuatta kamu görevlileri hakkında suç işlediklerine dair yapılan ihbar ve şikâyetlerin işleme konulabilmesi için gerekli koşulların neler olacağı hususu sadece MİT mensupları yönünden düzenlenmemiş, diğer tüm kamu görevlileri yönünden 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun'un 4. maddesinde ve bazı özel kanunlarda benzer şekilde hüküm altına alınmıştır. Buna göre, 4483 sayılı Kanun kapsamında tüm memur ve kamu görevlileriyle ilgili olarak bir soruşturma başlatılabilmesi için yapılan ihbar ve şikâyetin soyut ve genel nitelikte olmaması, ihbar veya şikâyetlerde kişi veya olay belirtilmesi, iddiaların ciddi bulgu ve belgelere dayanması, ihbar veya şikâyet dilekçesinde dilekçe sahibinin doğru ad, soyad ve imzası ile iş veya ikametgâh adresinin bulunması gerekmektedir. Bu yönüyle dava konusu kuralla MİT mensupları yönünden bir ayrıcalığın yapılması veya kanun önünde bir eşitsizliğin yaratılması söz konusu değildir.

114. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2., 10., 36. ve 74. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

Ğ- Kanun'un 6. Maddesiyle 2937 Sayılı Kanun'un 26. Maddesine Eklenen Dördüncü Fıkranın Birinci Cümlesinin İncelenmesi

a- Cümlenin 353 Sayılı Kanun'un 15/A Maddesinin Üçüncü Fıkrasının Son Cümlesi ile Yedinci Fıkrasının Son Cümlesine Atıfta Bulunan Bölümü

115. Dava konusu kuralda, 25.10.1963 gün ve 353 sayılı Askeri Mahkemeler Kuruluşu ve Yargılama Usulü Kanunu'nun 15/A maddesinin üçüncü fıkrasının son iki cümlesi ile beş, altı ve yedinci fıkralarına atıfta bulunularak buradaki usul ve hükümlerin MİT Müsteşarı hakkında da uygulanacağı belirtilmiştir.

116. Dava konusu kuralla atıfta bulunulan 353 sayılı Kanun'un 15/A maddesinin üçüncü fıkrasının son cümlesi ile yedinci fıkrasının son cümlesi Anayasa Mahkemesinin 14.1.2015 tarihli ve E. 2014/89, K. 2015/3 sayılı kararıyla iptal edilmiş ve bu hükümlerin iptaliyle dava konusu kuralın bu hükümlere atıfta bulunan bölümlerinin uygulanma kabiliyeti kalmamıştır.

117. Açıklanan nedenle dava konusu cümlenin, 353 sayılı Kanun'un 15/A maddesinin üçüncü fıkrasının son cümlesi ile yedinci fıkrasının son cümlesine atıfta bulunan bölümüne ilişkin iptal talebi hakkında karar verilmesine yer olmadığına karar verilmesi gerekir.

b- Cümlenin Kalan Bölümü

1- Kuralın Anlam ve Kapsamı

118. 2937 sayılı Kanun'un 26. maddesinin dava konusu kuralı içeren dördüncü fıkrasının birinci cümlesinde, MİT Müsteşarına ilişkin özel bir soruşturma usulü düzenlenmektedir.

119. 2937 sayılı Kanun'un 26. maddesinin birinci fıkrası uyarınca, tüm MİT mensuplarının bu arada MİT Müsteşarının görevlerini yerine getirirken görevin niteliğinden doğan veya görevin ifası sırasında işledikleri iddia olunan suçlardan dolayı soruşturulabilmeleri Başbakanın iznine bağlı bulunmaktadır.

120. Dava konusu kuralda, hem bu izin usulüne hem de izin verilmesi halinde yürütülecek soruşturmaya ilişkin olarak MİT Müsteşarı yönünden yeni kurallar belirlenmekte, böylece MİT Müsteşarının soruşturulabilmesi, diğer MİT mensuplarına göre ayrı bir soruşturma usulüne bağlanmaktadır. Bu çerçevede, kural uyarınca MİT Müsteşarı hakkındaki soruşturmalarda, 353 sayılı Kanun'un 15/A maddesinin üçüncü fıkrasının son iki cümlesi ile beş, altı ve yedinci fıkralarında yer alan usul ve hükümler uygulanacak, ancak atıfta bulunulan hükümlerden 353 sayılı Kanun'un 15/A maddesinin üçüncü fıkrasının son cümlesi ile yedinci fıkrasının son cümlesi, Anayasa Mahkemesinin 14.1.2015 tarihli ve E. 2014/89, K. 2015/3 sayılı kararıyla iptal edildiğinden uygulanma imkânı bulmayacaktır.

121. Buna göre, MİT Müsteşarının görevini yerine getirirken, görevin niteliğinden doğan veya görevin ifası sırasında işlediği iddia olunan suçlar hakkındaki soruşturmalarda Başbakanın soruşturma izni istenecek, Başbakanın kararı vermeden önce araştırma veya ön inceleme yapabilecek ve bu araştırma ve ön incelemeyi bizzat yapabileceği gibi görevlendireceği denetim elemanları eliyle de yaptırabilecektir. Bu şekilde görevlendirilen kişiler, 4483 sayılı Kanun'da ön inceleme ile görevlendirilen kişilere tanınan yetkilere sahip olacaklardır. Başbakanın vereceği izin

verme veya vermeme kararına karşı ilgililer on gün içinde Cumhurbaşkanlığına itiraz edebileceklerdir.

122. Cumhurbaşkanının soruşturma izni verilmemesi kararına yapılan itirazı kabul etmesi veya Başbakanın soruşturma izni verilmesine ilişkin kararına süresinde itiraz edilmemesi ya da bu itirazın Cumhurbaşkanı tarafından reddedilmesi hâllerinde MİT Müsteşarı hakkında soruşturma aşamasına geçilecek, fakat bu soruşturmayı ilgili Cumhuriyet savcısı değil Başbakanın denetim elemanları arasından belirleyeceği üç kişilik soruşturma kurulu yapacaktır.

123. Soruşturma Kurulu, bu soruşturmayı yürütürken 5271 sayılı Ceza Muhakemesi Kanunu'nun Cumhuriyet savcısına tanıdığı bütün yetkilere sahip olacak ve soruşturma sırasında hâkim kararı alınması gereken hususlarda yetkili mahkemelere başvurabilecektir. Kurul, yaptığı soruşturma sonucunu bir rapor ile tespit ederek Başbakana sunacak, Başbakan, kamu davasının açılmasına gerek görürse ilgili Yargıtay dairesinde dava açılacak, ancak gerek görmezse kovuşturma yapılmasına yer olmadığına karar verecektir.

2- İptal Talebinin Gerekçesi

124. Dava dilekçesinde özetle dava konusu kuralla MİT Müsteşarı hakkındaki soruşturmalarda 353 sayılı Kanun'un 15/A maddesinin üçüncü fıkrasının son iki cümlesi ile beş, altı ve yedinci fıkralarında yer alan usul ve hükümlerin uygulanacağına düzenlendiği, anılan hükümlerde belirtilen usul ve hükümlerin Anayasa'nın 148. maddesinin yedinci fıkrası uyarınca sadece Yüce Divan yargılamasına tabi Genelkurmay Başkanı ile kuvvet komutanları için geçerli olabileceği, dava konusu kuralla MİT Müsteşarı yönünden de bu usul ve esasların geçerli kılınmasının Anayasa'nın 148. maddesine aykırı olduğu ileri sürülmüştür.

3- Anayasa'ya Aykırılık Sorunu

125. 6216 sayılı Kanun'un 43. maddesi uyarınca dava konusu kural, ilgisi nedeniyle Anayasa'nın 2. maddesi yönünden de incelenmiştir.

126. Dava konusu kuralda MİT Müsteşarının görev suçlarına ilişkin olarak özel bir soruşturma usulü düzenlenmektedir.

127. 91., 92. ve 93. paragraflarda açıklandığı üzere, anayasa koyucu ve kanun koyucu, bazı kişiler yönünden uluslararası hukuk ve iç hukuktan kaynaklanan kimi nedenlere dayanarak genel soruşturma ve kovuşturma usulü kurallarına istisnalar getirebilmekte ve bunlar yönünden özel soruşturma ve kovuşturma usulleri belirleyebilmektedir. Bu usullerin tanınması, uygulanacak kişilere imtiyaz tanımak anlamına gelmeyip yapılan görevin niteliğinden kaynaklanmaktadır.

128. Dava konusu kuralda da anılan çerçevede millî güvenlik yönünden son derece önemli ve kritik görevler yürüten MİT Müsteşarının yürüttüğü görevin niteliği nedeniyle özel bir soruşturma usulüne tabi kılındığı anlaşılmaktadır.

129. Kanun koyucunun, izlediği ceza politikası uyarınca kanunlarla belirlenen görevini en iyi şekilde ve etkin olarak yerine getirmesini sağlamak, gereksiz şikâyetlere maruz kalınarak görülen hizmetin kesintiye uğramasını önlemek üzere MİT Müsteşarı yönünden farklı bir soruşturma usulü benimsemesi, takdir yetkisi kapsamında kalmakta olup bu yönüyle dava konusu kuralın, hukuk devleti ilkesiyle çelişen bir yönü bulunmamaktadır.

130. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

131. Öte yandan, Anayasa Mahkemesinin görev ve yetkilerinin düzenlendiği Anayasa'nın 148. maddesinin yedinci fıkrasında "Genelkurmay Başkanı, Kara, Deniz ve Hava Kuvvetleri Komutanları ile Jandarma Genel Komutanı da görevleriyle ilgili suçlardan dolayı Yüce Divanda yargılanırlar." hükmüne yer verilmiştir. Buna göre, anılan kişilerin görev suçlarına ilişkin olarak yargılama görev ve yetkisi Yüce Divan sıfatıyla Anayasa Mahkemesine ait olup kanunlarla bu hükme aykırı bir düzenleme getirilmesi mümkün değildir.

132. 353 sayılı Kanun'un 15/A maddesinin birinci fıkrasında bu anayasal düzenlemeye paralel olarak anılan kişilerin görev suçlarıyla ilgili yargılamanın Yüce Divanda yapılacağı belirtilmiş, kalan fıkralarında ise anılan kişilerle ilgili olarak özel bir soruşturma usulü düzenlenmiştir.

133. Dava konusu kuralda, 353 sayılı Kanun'un 15/A maddesinin üçüncü fıkrasının son iki cümlesi ile beş, altı ve yedinci fıkralarına atıfta bulunularak anılan kişiler yönünden belirlenen özel soruşturma usul ve hükümlerinin MİT Müsteşarı hakkındaki soruşturmalarda da uygulanacağı belirtilmekte, Genelkurmay Başkanı, Kara, Deniz ve Hava Kuvvetleri komutanları ile Jandarma Genel Komutanının görevleriyle ilgili suçlardan dolayı Yüce Divanda yargılanacağını düzenleyen birinci fıkrasına herhangi bir atıfta bulunulmamaktadır.

134. Dava konusu kuralda, MİT Müsteşarının yargılmasının Yüce Divanda yapılabileceğine ilişkin herhangi bir düzenlemeye yer verilmediğinden kuralın, Anayasa Mahkemesinin görev ve yetkilerinin düzenlendiği Anayasa'nın 148. maddesiyle ilgisi bulunmamaktadır.

135. Alparslan ALTAN ve Erdal TERCAN Anayasa'nın 2. maddesi yönünden bu görüşe katılmamışlardır.

H- Kanun'un 6. Maddesiyle 2937 Sayılı Kanun'un 26. Maddesine Eklenen Sekizinci Fıkranın İncelenmesi

1- İptal Talebinin Gerekçesi

136. Dava dilekçesinde özetle dava konusu kuralla Türkiye'de tutuklu veya hükümlü bulunan yabancıların, millî güvenliğin veya ülke menfaatlerinin gerektirdiği hâllerde 5237 sayılı Türk Ceza Kanunu'nun (TCK) 18. maddesinde belirtilen kurallara ve usule aykırı olarak Dışişleri Bakanının talebi üzerine, Adalet Bakanının teklifi ve Başbakanın onayı ile başka bir ülkeye iade edilebilmesine veya başka bir ülkede tutuklu ve hükümlü bulunanlar ile takas edilebilmesine imkân tanındığı, bu durumun anılan maddedeki güvenceleri etkisiz hâle getirerek kişilerin temel hak ve özgürlüklerinin zedelenmesine yol açtığı, bu yönüyle kuralın hukuk devleti ilkesini ihlal ettiği, iade işleminin kuralda yer alan millî güvenlik veya ülke menfaatleri gibi muğlâk ifadelerle bağlanmasının belirsizliğe neden olduğu, ayrıca kuralın anılan güvencelere aykırı olarak yabancıların iadesine imkân tanınarak suç işleyen yabancılara cezadan kurtulma veya daha az ceza alma olanağı sağladığı, bu durumun da mağdurların haklarının korunmasını önleyerek cezaların şahsiliği ilkesini zedelediği belirtilerek dava konusu kuralın, Anayasa'nın 2. ve 38. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

137. 6216 sayılı Kanun'un 43. maddesi uyarınca dava konusu kural, ilgisi nedeniyle Anayasa'nın 36. maddesi yönünden de incelenmiştir.

138. Dava konusu kuralda, Türk vatandaşları hariç olmak üzere, tutuklu veya hükümlü bulunanların millî güvenliğin veya ülke menfaatlerinin gerektirdiği hâllerde Dışişleri Bakanının talebi üzerine, Adalet Bakanının teklifi ve Başbakanın onayı ile başka bir ülkeye iade edilebileceği veya başka bir ülkede tutuklu ve hükümlü bulunanlar ile takas edilebileceği düzenlenmektedir.

139. Anayasa'nın hak arama hürriyetini düzenleyen 36. maddesinin birinci fıkrasında, kişilerin hak arama özgürlükleri güvence altına alınmıştır. Hak arama özgürlüğü, toplumsal barışı güçlendiren dayanaklardan biri olmanın yanında bireyin adaleti bulma, hakkı olanı elde etme ve haksızlığı giderme yoludur. İnsan varlığını soyut ve somut değerleriyle koruyup geliştirmek amacıyla hukuksal olanakları kapsamlı biçimde sağlama, bu konuda tüm yollardan yararlanma hakkını içeren hak arama özgürlüğü, hukuk devletinin ve çağdaş demokrasinin vazgeçilmez koşullarından biridir.

140. Suçluların iadesi usulü ve koşulları TCK'nın 18. maddesinde düzenlenmiş olup kural olarak yabancı bir ülkede işlenen veya işlendiği iddia edilen bir suç nedeniyle hakkında ceza soruşturması

veya kovuşturması başlatılan veya mahkûmiyet kararı verilmiş olan yabancının anılan usul ve koşullara uyulmaksızın talep eden ülkeye iade edilmesi mümkün bulunmamaktadır.

141. Dava konusu kuralla TCK'nın 18. maddesinde düzenlenen suçluların iadesi usulünden, ilkeleri itibariyle oldukça ayrılan farklı bir usule yer verilmektedir. Zira TCK'nın 18. maddesinde ve uluslararası hukukta kabul edilen suçluların iadesinde, kural olarak suçun yurt dışında işlenen bir suç olması, suçun işlendiği yer devletinin bunu kovuşturmak veya hüküm vermişse cezayı infaz etmek üzere faili istemesi gerekmektedir. Ayrıca iadesi talep edilen failin, Türkiye'de tutuklu veya hükümlü olmasına gerek bulunmamaktadır.

142. Dava konusu kural uyarınca benimsenen iade usulünde, bir yabancının yurt dışında suç işlemesi gerekmemekte, yurt içinde suç işlemiş olsa bile iade edilmesine imkân tanınmaktadır. Ayrıca kişinin sadece yargılanması veya cezasının infaz edilmesi amaçlarıyla iadesi şartı aranmamakta, kişinin yargılanma veya cezasının infazı dışındaki amaçlarla da iadesi mümkün bulunmaktadır. Ancak bunun için kişinin Türk vatandaşı olmaması ve Türkiye'de tutuklu veya hükümlü olması, millî güvenlik veya ülke menfaatleri yönünden gereklilik bulunması şartları birlikte aranmakta ve bu usulde iadeye, kişinin bulunduğu yer Ağır Ceza Mahkemesi tarafından değil Dışişleri Bakanının talebi üzerine, Adalet Bakanının teklifi ve Başbakanın onayı ile karar verilmektedir.

143. Dolayısıyla dava konusu kuralın hem teknik anlamda iadeye, yani yurt dışında suç işleyen yabancılardan yargılanması veya cezalarının infaz edilebilmesi için iadeye, hem de işlediği suç nedeniyle yargılanması ve cezasının infaz edilmesi amacı olmaksızın iadeye imkân tanıdığı görülmektedir.

144. Kuralda, talep eden devlete geri verilmesi hâlinde işkenceye, insanlık dışı ya da onur kırıcı ceza veya muameleye tabi tutulacağı veya ırkı, dini, tabiiyeti, belli bir toplumsal gruba mensubiyeti veya siyasi fikirleri dolayısıyla hayatının veya hürriyetinin tehdit altında bulunacağına dair kuvvetli şüphe sebepleri bulunan kişilerin iade edilemeyeceği yönünde güvenceye yer verilmediği görülmektedir. Bu durumun kişilerin Anayasa'da güvence altına alınan yaşam hakkı başta olmak üzere düşünce, kanaat ve din özgürlüğü ile ayrımcılık, kötü muamele ve işkence yasağı haklarını ihlal edebileceği açıktır. Ayrıca aynı hak ihlallerinin takas yoluyla yapılacak iadelerde de gerçekleşmesi mümkündür.

145. Öte yandan, Anayasa'nın 125. maddesi uyarınca bu karara ilişkin idari işlem de diğer tüm idari işlemler gibi yargı denetimine tabi olduğundan bu işleme karşı idari yargı yoluna başvurulması mümkün bulunmaktadır. Ancak kuralla öngörülen, tutuklu ve hükümlülerin iadesi ve takası (yurt dışına teslimi) olduğundan bu konuda sadece yargı yollarının öngörülmüş olması yeterli olmamakta, ilgili kişilerin bu yolu etkili bir şekilde kullanabilmelerini sağlayacak güvencelerin de sağlanmış

olması gerekmektedir. Aksi takdirde söz konusu kişilerin sınır dışı edilmesinden sonra yargı denetimi yapılmasının hiçbir anlamı olmayacaktır.

146. Nitekim Anayasa Mahkemesi, sınır dışı ve suçluların iadesi işlemlerine ilişkin yapılan tedbir talepli bireysel başvurularda, anılan etkili yargısal güvenceyi sağlamak amacıyla söz konusu işlemlerin yürürlüğünü derhâl durdurmaktadır (Akhmad Khalimov [TAK], B. No: 2016/1129, 20.1.2016). Aynı şekilde, Avrupa İnsan Hakları Mahkemesi (AİHM) de sınır dışı işlemlerinde bu prensibi uygulamakta ve anılan işleme karşı yapılan başvuru sonuçlanmadan kişinin sınır dışı edilmesi hâlinde etkili bir başvuru yolunun öngörülmemesi nedeniyle ihlal kararları verebilmektedir (bkz. A.D ve diğerleri/Türkiye, B. No: 22681/09, 22.7.2014, §§ 95-104; Gebremedhin/Fransa, B. No: 25389/05, 26.4.2007, § 66).

147. Mevzuatta da anılan nitelikte kurallar yer almakta olup 4.4.2013 tarihli ve 6458 sayılı Yabancılar ve Uluslararası Koruma Kanunu'nun 53. maddesinde, sınır dışı etme yönünden etkili bir başvuru yolu öngörülmüş bulunmaktadır. Buna göre, sınır dışı etme kararının gerekçeleriyle birlikte hakkında sınır dışı etme kararı alınan yabancıya veya yasal temsilcisine ya da avukatına tebliğ edilmesi, hakkında sınır dışı etme kararı alınan yabancı, bir avukat tarafından temsil edilmiyorsa kendisi veya yasal temsilcisine, kararın sonucu, itiraz usulleri ve süreleri hakkında bilgilendirme yapılması ve yabancının rızası saklı kalmak kaydıyla, dava açma süresi içinde veya yargı yoluna başvurulması hâlinde yargılama sonuçlanıncaya kadar sınır dışı edilmemesi gerekmektedir.

148. 2937 sayılı Kanun'da, tutuklu ve hükümlülerin iade ve takas işlemlerine karşı yargı yollarını kullanabilme yönünden etkili bir başvuru yolu oluşturulmaksızın dava konusu kuralla söz konusu istisnai usulün benimsendiği görülmektedir.

149. Dava konusu kuralla anılan nitelikte güvenceler ve konuya ilişkin benzeri teminatlar öngörülmeden koşulları ve sınırları belirsiz bir yetkinin düzenlenmesi, kişilerin hukuki güvenliklerini ve hak arama hürriyetlerini ihlal etmektedir.

150. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2. ve 36. maddelerine aykırıdır. İptali gerekir.

151. Kuralın, Anayasa'nın 38. maddesiyle ilgisi görülmemiştir.

I- Kanun'un 7. Maddesiyle Değiştirilen 2937 Sayılı Kanun'un 27. Maddesinin Birinci Fıkrasında Yer Alan ".yetkisiz olarak alan, temin eden,." İbaresini İle Üçüncü Fıkrasının İncelenmesi

1- İptal Taleplerinin Gerekçeleri

152. Dava dilekçesinde özetle dava konusu kurallarla MİT'in görev ve faaliyetlerine ilişkin bilgi ve belgeleri, yetkisiz olarak almak ve temin etmek ile 2937 sayılı Kanun'un 27. maddesinin birinci ve ikinci fıkraları kapsamında kalan bilgilerin yayımlanması, yayılması veya açıklanması fillerinin suç olarak düzenlenip cezai müeyyideye bağlandığı, bu durumun kişilerin haberleşme, ifade ve basın hürriyetleri ile bilgi edinme haklarını zedelediği, ayrıca 27. maddenin üçüncü fıkrasında düzenlenen suç yönünden üç yıldan altı yıla kadar hapis cezası öngörülmesinin anılan hakların ölçüsüzce sınırlandırılmasına neden olduğu, öte yandan, aynı kuralla MİT mensuplarının ailelerinin kimliklerini ifşa etmenin suç olarak düzenlenmesinin, anılan kişilerin ailelerine yönelik olarak imtiyaz tanınması sonucunu doğurarak kanun önünde eşitlik ilkesini ihlal ettiği belirtilerek dava konusu kuralların, Anayasa'nın 2., 5., 10., 22., 26., 28., 29. ve 74. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

153. 6216 sayılı Kanun'un 43. maddesi uyarınca dava konusu kurallar, ilgisi nedeniyle Anayasa'nın 13. maddesi yönünden de incelenmiştir.

154. 2937 sayılı Kanun'un 27. maddesinin dava konusu ibareyi de içeren birinci fıkrasında, MİT'in görev ve faaliyetlerine ilişkin bilgi ve belgeleri, yetkisiz olarak alan, temin eden, çalan, sahte olarak üreten, bunlar üzerinde sahtecilik yapan ve bunları yok edenlerin dört yıldan on yıla kadar hapis cezası ile cezalandırılacağı düzenlenmekte olup dava konusu kuralı ".yetkisiz olarak alan, temin eden." ibareleri oluşturmaktadır.

155. Aynı maddenin dava konusu üçüncü fıkrasında ise MİT'in görev ve faaliyetlerine ilişkin bilgi ve belgelerle MİT mensuplarının veya ailelerinin kimliklerine ilişkin bilgi ve belgelerin radyo, televizyon, internet, sosyal medya, gazete, dergi, kitap ve diğer tüm medya araçları ile her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim araçları vasıtasıyla yayımlanması, yayılması veya açıklanması suç olarak düzenlenmekte ve bu suça ilişkin olarak 5187 sayılı Basın Kanunu'nun 11. maddesi ile 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 4. ve 6. maddeleri hükümlerine göre sorumlulukları belirlenenlerin ve bunları yayanların üç yıldan dokuz yıla kadar hapis cezasıyla cezalandırılacağı öngörülmektedir.

156. Anayasa'nın "Düşünceyi açıklama ve yayma hürriyeti" kenar başlıklı 26. maddesinin birinci fıkrasında, "Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar." ve "Basın hürriyeti" kenar başlıklı 28.

maddesinin birinci ve üçüncü fıkralarında, "Basın hürdür, sansür edilemez. Basımevi kurmak izin alma ve malî teminat yatırma şartına bağlanamaz. Devlet, basın ve haber alma hürriyetlerini sağlayacak tedbirleri alır." denilmek suretiyle temel hak ve hürriyetler arasında yer alan "ifade hürriyeti" ve "basın hürriyeti" güvence altına alınmıştır. Anılan maddelerin sırasıyla ikinci ve dördüncü fıkralarında ise bu hürriyetlerin millî güvenlik, kamu düzeni, kamu güvenliği, Cumhuriyetin temel nitelikleri ve devletin ülkesi ve milleti ile bölünmez bütünlüğünün korunması, suçların önlenmesi, suçluların cezalandırılması, devlet sırrı olarak usulünce belirtilmiş bilgilerin açıklanmaması, başkalarının şöhret veya haklarının, özel ve aile hayatlarının yahut kanunun öngördüğü meslek sırlarının korunması veya yargılama görevinin gereğine uygun olarak yerine getirilmesi amaçlarıyla sınırlanabileceği, 28. maddenin beşinci fıkrasında ise devletin iç ve dış güvenliğini, ülkesi ve milletiyle bölünmez bütünlüğünü tehdit eden veya suç işlemeye ya da ayaklanma veya isyana teşvik eder nitelikte olan veya devlete ait gizli bilgilere ilişkin bulunan her türlü haber veya yazıyı yazarların veya bastırانların veya aynı amaçla basanların, başkasına verenlerin, bu suçlara ait kanun hükümleri uyarınca sorumlu tutulabileceği belirtilerek bu hürriyetlerin mutlak olmadığı ve anılan nedenlere dayalı olarak sınırlandırılabilceği kabul edilmiştir.

157. Benzer şekilde, Anayasa'nın "Dilekçe, bilgi edinme ve kamu denetçisine başvurma hakkı" kenar başlıklı 74. maddesinin dördüncü fıkrasında bilgi edinme hakkı güvence altına alınmış, aynı maddenin son fıkrasında ise "Bu maddede sayılan hakların kullanılma biçimi . kanunla düzenlenir." denilmek suretiyle bu hakka ilişkin kuralın norm alanını belirleme yetkisi kanun koyucunun takdirine bırakılmıştır. Dolayısıyla bu hakkın da kanunda belirlenecek nedenlere dayalı olarak sınırlandırılması mümkün bulunmaktadır.

158. Ancak anılan hak ve hürriyetlerin sınırlandırılabilmesi için yukarıda belirtilen nedenlerin varlığı yeterli olmayıp temel hak ve hürriyetlerin sınırlandırılması rejimini belirleyen Anayasa'nın 13. maddesine de uyulması gerekmektedir. Anayasa'nın 13. maddesi uyarınca, ifade ve basın hürriyeti ile bilgi edinme hakkı yalnızca kanunla ve demokratik bir toplumda gerekli olduğu ölçüde sınırlanabilir. Ayrıca getirilen bu sınırlamalar, hakkın özüne dokunamayacağı gibi Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamaz.

159. Dava konusu kurallarla MİT'in görev ve faaliyetleri kapsamında elde ettiği veya hazırladığı ve doğası itibariyle gizli olan, bu nedenle de sadece yetkili kişilerle paylaşılabilen bilgi ve belgelerin elde edilmesi veya temin edilmesi ile bunların ve MİT mensuplarının veya ailelerinin kimliklerinin her türlü medya veya kitle iletişim araçları vasıtasıyla yayımlanması, yayılması veya açıklanması suç

olarak düzenlenerek ifade ve basın hürriyetleri ile bilgi edinme hakkına bir sınırlama getirilmektedir. Fakat bu sınırlama, millî güvenlik istihbaratını devlet çapında oluşturabilmek ve karşı istihbarat faaliyetlerinde bulunabilmek amacıyla elde edilen, bu yönüyle millî güvenliğin korunmasına ilişkin devlet sırlarını ve kişilerin özel hayatına ilişkin hususları da içeren bilgi ve belgelerin gizliliği ile görevlerini yerine getirebilmelerinin zorunlu gereği olarak kimliklerini gizleyerek çalışan MİT mensuplarının görev, şahıs ve aile güvenliklerinin sağlanmasına yönelik bir düzenlemedir. Dolayısıyla anılan sınırlama millî güvenlik, kamu düzeni ve kamu güvenliğinin tesis edilmesi ve korunması amaçlarıyla getirilmekte olup demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır.

160. Bu şekilde, demokratik toplum düzeni bakımından alınması gerekli tedbirler kapsamında anılan hak ve hürriyetlere sınırlama getirilirken kurallarda bunun sadece MİT'in görev ve faaliyetleri kapsamında elde ettiği ve doğası itibariyle gizli olan ve bu nedenle sadece yetkili kişilerle paylaşılabilen bilgi ve belgeler ile MİT mensuplarının veya ailelerinin kimlikleriyle sınırlandırılmış olması, hem anılan hakların kullanımını ciddi surette güçleştirip amacına ulaşmasına engel olarak hakların özünün zedelenmesini önlemekte, hem de sınırlama aracının sınırlama amacına uygun ve orantılı şekilde kullanılmasını temin ederek anılan haklar ile millî güvenliğin, kamu düzeninin, kamu güvenliğinin ve kişilerin özel hayatına ilişkin bilgilerin korunması arasındaki makul dengenin kurulmasını sağlamaktadır.

161. Öte yandan, hukuk devletinde ceza ve ceza yargılamasına ilişkin kurallar, ceza hukukunun ana ilkeleri ile Anayasa'nın konuya ilişkin kuralları başta olmak üzere, ülkenin sosyal, kültürel yapısı, etik değerleri ve ekonomik hayatın gereksinimleri göz önüne alınarak saptanacak ceza siyasetine göre belirlenir. Kanun koyucu, cezalandırma yetkisini kullanırken toplumda hangi eylemlerin suç sayılacağı, bunun hangi tür ve ölçüdeki ceza yaptırımını ile karşılanacağı, nelerin ağırlaştırıcı veya hafifletici sebep olarak kabul edilebileceği konusunda takdir yetkisine sahip bulunmaktadır. Dolayısıyla dava konusu kurallarla söz konusu eylemlerin suç olarak düzenlenip bunun için kurallarda belirtilen nitelik ve ölçüde cezalar belirlenmesinde hukuk devleti ilkesiyle çelişen bir yön bulunmamaktadır.

162. Ayrıca maddenin dava konusu üçüncü fıkrasında, anılan suçu işleyenlerin üç yıldan dokuz yıla kadar hapis cezasıyla cezalandırılması öngörülmekte olup TCK'nın 61. maddesi uyarınca hâkim somut olayın özelliğine göre suçun işleniş biçimini, suçun işlenmesinde kullanılan araçları, suçun işlendiği zaman ve yeri, suçun konusunun önem ve değerini, meydana gelen zarar veya tehlikenin ağırlığını, failin kast veya taksire dayalı kusurunun ağırlığını, failin güttüğü amaç ve saiki dikkate

olarak suçun kanuni tanımında öngörülen cezasının alt ve üst sınırı arasında temel cezayı belirlemekle yükümlü bulunmaktadır. Dolayısıyla yukarıdaki kriterler esas alınmaksızın keyfi olarak suç faillerinden kimine alt sınırdan kimine üst sınırdan ceza uygulanması mümkün değildir. Dava konusu kuralla farklı suç faillerine farklı cezalar verilebilmesine imkân tanınmasının nedeni, cezanın suçun işleniş biçimi, suç konusunun önem ve değeri, meydana gelen zarar ve tehlikenin ağırlığı gibi somut olaya göre değişebilecek durumlara uygunluğunun sağlanması, böylece ceza adaletinin tesis edilmesidir.

163. Kanun'da bu şekilde güvencelere yer verilerek dava konusu kuraldaki cezanın ancak anılan objektif kriterler esas alınarak belirlenebilmesine izin verilmesi, kurala konu sınırlama aracının sınırlama amacına uygun ve orantılı şekilde uygulanmasına imkân tanımakta, böylece kuralın ceza yaptırımını yönüyle de ölçülülüğünü sağlamaktadır.

164. Bu yönleriyle dava konusu kurallarla anılan haklara getirilen sınırlamanın, hakkın özünü zedelediğinden söz edilemeyeceği gibi demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı düştüğü de söylenemez.

165. Anayasa'nın 10. maddesinde kanun önünde eşitlik ilkesine yer verilmiştir. Buna göre, eşitlik ilkesi hukuksal durumları aynı olanlar için söz konusudur. Bu ilke ile eylemli değil, hukuksal eşitlik öngörülmüştür. Eşitlik ilkesinin amacı, aynı durumda bulunan kişilerin kanunlar karşısında aynı işleme bağlı tutulmalarını sağlamak, ayırım yapılmasını ve ayrıcalık tanınmasını önlemektir. Bu ilkeyle, aynı durumda bulunan kimi kişi ve topluluklara ayrı kurallar uygulanarak kanun karşısında eşitliğin ihlali yasaklanmıştır. Kanun önünde eşitlik, herkesin her yönden aynı kurallara bağlı tutulacağı anlamına gelmez. Durumlarındaki özellikler, kimi kişiler ya da topluluklar için değişik kuralları ve uygulamaları gerektirebilir. Aynı hukuksal durumlar aynı, ayrı hukuksal durumlar farklı kurallara bağlı tutulursa Anayasa'da öngörülen eşitlik ilkesi zedelenmez.

166. Maddenin üçüncü fıkrasında düzenlenen dava konusu kuralla MİT mensuplarının ve ailelerinin kimliklerinin ifşa edilmesinin suç olarak öngörülme nedeninin, bu kişilere ve ailelerine kendileriyle aynı durumda bulunan kişilere nazaran özel bir imtiyaz ve ayrıcalık tanımak değil, yürüttükleri görevler nedeniyle kimliklerinin ifşa olmasının, MİT mensuplarının görevlerini yerine getirme imkânını ortadan kaldırması ve kendileri ile birlikte ailelerinin güvenliklerini tehdit altına sokmasıdır. Dolayısıyla dava konusu kuralla anılan kişilerin özel durumundan kaynaklanan nedenlere dayalı olarak farklı bir kuralın düzenlenmesi söz konusu olup bunun eşitlik ilkesini zedeleyen bir yönü bulunmamaktadır.

167. Açıklanan nedenlerle dava konusu kurallar, Anayasa'nın 2., 10., 13., 26., 28. ve 74. maddelerine aykırı değildir. İptal taleplerinin reddi gerekir.

168. Kuralların, Anayasa'nın 5., 22. ve 29. maddeleriyle ilgisi görülmemiştir.

İ- Kanun'un 7. Maddesiyle Değiştirilen 2937 Sayılı Kanun'un 27. Maddesinin Dördüncü Fıkrasında Yer Alan ".ihmal veya." ve ".yükümlülüklerini yerine getirmeyenlere." İbarelerinin İncelenmesi

1- İptal Talebinin Gerekçesi

169. Dava dilekçesinde özetle 2937 sayılı Kanun kapsamındaki görev ve yetkilerin yerine getirilmesini ihmal suretiyle önleyenlerin ve aynı Kanun kapsamındaki yükümlülüklerini yerine getirmeyenlerin iki yıldan dört yıla kadar hapis cezası ile cezalandırılmasını öngören dava konusu kuralın, adil ve ölçülü olmadığı belirtilerek Anayasa'nın 2. ve 13. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

170. 2937 sayılı Kanun'un 27. maddesinin dava konusu ibareleri de içeren dördüncü fıkrasında, 2937 sayılı Kanun ile belirlenen görev ve yetkilerin kullanılmasının engellenmesine yönelik eylemler suç olarak düzenlenmekte ve bunlar cezai müeyyideye bağlanmaktadır. Buna göre, 2937 sayılı Kanun kapsamındaki görev ve yetkilerin kullanılmasını engelleyenlerin, üç yıldan beş yıla kadar hapis cezasıyla ihmal veya suistimal suretiyle önleyenlerle yükümlülüklerini yerine getirmeyenlerin, iki yıldan dört yıla kadar hapis cezası ile cezalandırılması öngörülmektedir.

171. Ceza hukukunun, toplumun kültür ve uygarlık düzeyi, sosyal ve ekonomik yaşantısıyla ilgili bulunması nedeniyle suç ve suçlulukla mücadele amacıyla ceza ve ceza muhakemesi alanında sistem tercihinde bulunulması devletin ceza siyaseti ile ilgilidir. Bu bağlamda hukuk devletinde, ceza hukukuna ilişkin düzenlemeler bakımından kanun koyucu Anayasa'nın temel ilkelerine ve ceza hukukunun ana kurallarına bağlı kalmak koşuluyla, toplumda belli eylemlerin suç sayılıp sayılmaması, suç sayıldıkları takdirde hangi çeşit ve ölçülerdeki ceza yaptırımlarıyla karşılanmaları gerektiği, hangi hâl ve hareketlerin ağırlaştırıcı ya da hafifletici öge olarak kabul edileceği gibi konularda takdir yetkisine sahip bulunmaktadır. Ancak kanun koyucu, söz konusu takdir yetkisinin kullanılmasında suç ve ceza arasındaki adil dengenin korunmasını ve öngörülen cezanın, cezalandırmada güdülen amacı gerçekleştirmeye elverişli olmasını da dikkate almak zorundadır. Bu nedenle eylemin suç olarak düzenlenmesinde ve cezalandırılmasında güdülen amaç ile bunun için seçilen araç arasında makul ve adil bir oranın bulunması, bir başka ifadeyle cezalandırma yetkisi kullanılırken de ölçülülük ilkesine uygun davranılması gerekmektedir.

172. Dava konusu ibarelere ilişkin kuralla 2937 sayılı Kanun kapsamında kalan görev ve yetkiler ile yükümlülüklerin yerine getirilmesinin engellenmesine yönelik fiillerin suç olarak nitelendirilip cezalandırılmasında güdülen amacın, millî güvenliği ve kamu düzenini korumak olduğu açıktır. Nitekim Kanun'un 4., 5. ve 6. maddelerinde düzenlenen bu görev ve yetkiler incelendiğinde bunların bir bütün olarak ülkenin millî güvenlik siyasetinin, dolayısıyla kamu güvenliği ve düzeninin sağlanmasında ve yürütülmesinde son derece önemli görev ve yetkiler olduğu anlaşılmaktadır.

173. Anılan nitelikteki görev, yetki ve yükümlülüklerin yerine getirilmesi, kamu görevi kapsamı dışında kalan kişilerin eylemleriyle önlenebileceği gibi bunlarla ilişkili görevlerin veya yükümlülüklerin ihmal edilmesi veya icrai hareketlerle yerine getirilmemesi eylemleriyle de engellenebilir. Bu yönüyle kanun koyucunun anılan amacı gerçekleştirmeye elverişli olacak şekilde dava konusu kuralda belirtilen eylemleri suç olarak düzenleyip bunlar yönünden izlediği caza siyasetine bağlı olarak takdir yetkisi kapsamında kuralda belirtilen ölçü ve nitelikte cezalar belirlemesinde, hukuk devleti ve ölçülülük ilkelerine aykırı düşen bir yön bulunmamaktadır.

174. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

175. Kuralın, Anayasa'nın 13. maddesiyle ilgisi görülmemiştir.

J- Kanun'un 8. Maddesiyle 2937 Sayılı Kanun'un Başlığıyla Birlikte Değiştirilen 28. Maddesinin Birinci Fıkrasında Yer Alan ", bu talepleri yerine getirenlerin hukuki ve cezai sorumluluğu doğmaz." İbaresini ile 11. Maddesiyle 2937 Sayılı Kanun'a Eklenen Ek 1. Maddenin İkinci Fıkrasının İncelenmesi

1- İptal Taleplerinin Gerekçeleri

176. Dava dilekçesinde özetle dava konusu kurallarla MİT'e verilen görev ve yetkiler çerçevesinde MİT tarafından yapılan herhangi bir talebi yerine getirenlerin, MİT tarafından istihbari faaliyetler için görevlendirilenlerden kimlikleri değiştirilenlerin, MİT'in görev ve faaliyetlerine yardımcı olanların veya istihbarat hizmetlerinde istifade edilenlerin hukuki ve cezai sorumluluklarının doğmamasının öngörüldüğü, bunun, hukuk yargılaması açısından aleyhlerine dava açılmaması nedeniyle haksız olanın, ceza yargılaması açısından ise ön inceleme ve soruşturma evresine geçilememesi nedeniyle, varsa suçun ve suçlunun ortaya çıkarılmasını engelleyeceği ve anılan kişilere hukukumuzda başka hiçbir gerçek veya tüzel kişiye tanınmayan bir ayrıcalık ve dokunulmazlık sağlayacağı, ayrıca söz konusu kişilerin hukuka aykırı işlemlerine karşı yargı yoluna başvurulması imkânını da ortadan

kaldıracağı belirtilerek kuralların, Anayasa'nın 2., 10. ve 125. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

177. 2937 sayılı Kanun'un "Taleplerin karşılanması" başlıklı 28. maddesinin dava konusu ibareleri de içeren birinci fıkrasında "Bu Kanunda MİT'e verilen görev ve yetkiler çerçevesinde yapılan her türlü talep öncelikli olarak yerine getirilir, bu talepleri yerine getirenlerin hukuki ve cezai sorumluluğu doğmaz." denilmiş, ek 1. maddesinin dava konusu ikinci fıkrasında ise "6 ncı maddenin birinci fıkrasının (e) bendine göre kimlikleri değiştirilenler, MİT'in görev ve faaliyetlerine yardımcı olanlar veya istihbarat hizmetlerinde istifade edilenler, kamu görevlisi olup olmadıklarına bakılmaksızın; görev, faaliyet ve yardımları sebebiyle sorumlu tutulamaz." hükmüne yer verilmiştir.

178. Buna göre, 2937 sayılı Kanun'da MİT'e verilen görev ve yetkiler çerçevesinde yapılan her türlü talep öncelikli olarak yerine getirilecek ve bu talepleri yerine getirenlerin hukuki ve cezai sorumluluğu doğmayacaktır. Aynı şekilde, MİT tarafından istihbari faaliyetler için görevlendirilenlerden kimlikleri değiştirilenlerin, MİT'in görev ve faaliyetlerine yardımcı olanların ve istihbarat hizmetlerinde istifade edilenlerin, kamu görevlisi olup olmadıklarına bakılmaksızın, görev, faaliyet ve yardımları sebebiyle sorumlu tutulmaları bir başka ifadeyle hukuki ve ceza sorumluluklarının doğması söz konusu olamayacaktır.

179. Kurullarla anılan kişilerin MİT'in istemi doğrultusunda yerine getirdiği her türlü talep, faaliyet, görev ve yardımlar, bu çerçevede olası kanun dışı hatta suç teşkil eden eylemler yönünden sorumlu olmayacaklarının öngörüldüğünün kabul edilmesi hâlinde kurulların başta hukuk devleti ilkesi olmak üzere birçok anayasal ilke ve kurala aykırılık teşkil edeceği açıktır.

180. Ancak kurulların lafzı ve yer aldığı Kanun'un diğer hükümleriyle birlikte taşıdığı anlam ve kapsam dikkate alındığında, kurullardan böyle bir sonuç çıkarmanın mümkün olmadığı anlaşılmaktadır.

181. Zira Kanun'un 28. maddesinin birinci fıkrasındaki dava konusu kuralda, hiçbir sınırlamaya tabi olmaksızın MİT'in tüm taleplerinin yerine getirileceği öngörülmemekte, sadece "Bu Kanun'da MİT'e verilen görev ve yetkiler çerçevesinde" yapılan taleplerin yerine getirileceği belirtilmektedir. Aynı şekilde Kanun'un ek 1. maddesinin ikinci fıkrasındaki dava konusu kuralda, 6. maddenin birinci fıkrasının (e) bendi uyarınca istihbari faaliyetler için görevlendirilenlerin tüm fiillerinin değil, bu fiillerden sadece MİT'in görevleri kapsamında kalanlarının hukuki ve cezai sorumluluk doğurmayacağı ifade edilmektedir. Dolayısıyla Kanun'la MİT'e verilen görev ve yetkiler dışında

MİT'in herhangi bir kişi veya kuruluştan talepte bulunması mümkün olmadığı gibi, MİT'in Kanun'da belirtilen görevleri dışında kalan fiiller yönünden herhangi bir kimseye hukuki ve cezai bağışıklık tanınması da mümkün değildir. Kanun'da, MİT'e hukuka aykırı, haksız fiil veya suç işleme görev veya yetkisinin verilmediği ve verilemeyeceği açık olduğuna göre, dava konusu kurallar uyarınca MİT'in haksız fiil teşkil eden yasa dışı taleplerini veya suç teşkil eden taleplerini yerine getirenlerin ve MİT'e görev ve faaliyetlerinde yardımcı olanların haksız fiil teşkil eden eylemlerinden veya suç teşkil eden fiillerinden sorumlu olacaklarının ve kuralların buna engel olan bir yönünün bulunmadığının kabulü gerekir.

182. Aksi takdirde Anayasa ve kanunların hiç kimseye, bu çerçevede Cumhurbaşkanı, Başbakan, TBMM üyeleri ve konu bağlamında MİT'in görev ve yetkilerini doğrudan yerine getiren görevlilerine bile vermediği bir bağışıklığı, MİT'in görevlendirdiği veya talepte bulunduğu kişilere tanıdığını kabul etmek gerekir ki bunun, başta kuralların yer aldığı Kanun'un genel mantığı olmak üzere hukuk anlayışı ve sistematığıyla bağdaştırılması olanaksızdır.

183. Dava konusu kuralların düzenlenme ihtiyacının, MİT'in görev ve yetkilerinin özelliğinden kaynaklandığı anlaşılmaktadır. MİT'e verilen yetki ve görevler, kural olarak yasaklanmış olan ancak Kanun'un verdiği açık yetki nedeniyle hukuka uygun hale gelen fiilleri içerebilmektedir. MİT görevlilerinin Kanun'da kendilerine verilen yetkiye istinaden birtakım faaliyetler yürütmesi, bu çerçevede örneğin 2937 sayılı Kanun'un 6. maddesinin birinci fıkrasının (c) bendi uyarınca bazı suçlara mahsus olmak üzere kural olarak gizli olan soruşturma dosyalarından bilgi ve belge istemeleri mümkün bulunmakta ve MİT görevlilerinin bu yetkilerini kullanma noktasında herhangi bir tereddütleri bulunmamaktadır. Ancak aynı durum, bu talepleri karşılamak zorunda olan kişiler yönünden, verilen örnek bağlamında soruşturma savcılarını yönünden geçerli değildir. Zira soruşturma savcısının, 2937 sayılı Kanun'un 6. maddesinin birinci fıkrasının (c) bendi uyarınca bu bilgileri verme yükümlülüğü bulunduğu gibi 5271 sayılı Ceza Muhakemesi Kanunu uyarınca soruşturmanın gizliliğini sağlama zorunluluğu da bulunmaktadır. Dolayısıyla soruşturma savcısının kanunun kendisine yüklediği iki yükümlülükten birini tercih etmesinin sorumluluğuna neden olabileceği, verilen örnek bağlamında anılan bilgilerin MİT'e verilmesi nedeniyle sorumlu tutulabileceği yönünde tereddütleri bulunabilir. Aynı şekilde yasa dışı bir terör örgütünün yapacağı olası eylemlerden önceden haber alınabilmesi amacıyla örgüte üye olan bir MİT görevlisinin "örgüte üye olma" fiilinin suç teşkil etmeyeceği açıktır. Ancak aynı durum kamu görevlisi sıfatı bulunmayan ve MİT'in görevlendirdiği kişiler yönünden bu ölçüde açık ve belirgin değildir. Kanun'un ek 1. maddesindeki kuralla MİT'in görevlendirdiği veya yardımını talep ettiği kamu görevlisi olmayan

kişilerin de MİT'in görev ve yetkisi kapsamında kalan yardım ve faaliyetlerden tıpkı MİT görevlileri gibi sorumlu olmaması esasının sağlanmak istendiği anlaşılmaktadır. Sonuç itibarıyla, dava konusu kurallarla yapılan düzenlemelerin, bu gibi tereddütleri gidermeye yönelik olduğu anlaşılmakta olup bunların kuralların düzenlenişi için makul nedenler olmadığı söylenemez.

184. Öte yandan, dava konusu kurallarla anılan kişilerin yerine getirdikleri talepler ile görev, faaliyet ve yardımları sebebiyle sorumlu tutulmamalarının sebebi, bu kişilerin haksız fiil veya suç teşkil eden eylemlerine hukuki ve cezai bağışıklık tanıyarak bunlara kendileriyle aynı durumda bulunan kişilere nazaran özel bir imtiyaz ve ayrıcalık vermek değildir. Bunun nedeni, çeşitli gereklerle dayalı olarak Kanun'un hukuka uygunluk niteliği tanıdığı, dolayısıyla haksız fiil veya suç oluşturmayan görev ve faaliyetlerin bu kişiler tarafından herhangi bir endişe ve tereddüt duyulmadan yerine getirilmesini sağlamaktır. Dolayısıyla dava konusu kurallarda, anılan görev ve faaliyetlerin yerine getirilmesi için tanınan hukuka uygunluk nedenine dayalı olarak tamamlayıcı bir sorumluluk hukuku kuralının düzenlenmesi söz konusu olup bunun eşitlik ilkesini zedeleyen bir yönü bulunmamaktadır.

185. Açıklanan nedenlerle dava konusu kurallar, Anayasa'nın 2. ve 10. maddelerine aykırı değildir. İptal taleplerinin reddi gerekir.

186. Kuralların, Anayasa'nın 125. maddesiyle ilgisi görülmemiştir.

K- Kanun'un 9. Maddesiyle Değiştirilen 2937 Sayılı Kanun'un 29. Maddesinin Birinci Fıkrasının Birinci Cümlesinin İncelenmesi

1- İptal Talebinin Gerekçesi

187. Dava dilekçesinde özetle dava konusu kuralla MİT mensupları ile MİT'te görev yapmış olanların MİT'in görev ve faaliyetlerine ilişkin hususlarda tanıklık yapmasının yasaklandığı, bu durumun anılan konulara ilişkin olarak maddi gerçeğin ortaya çıkartılmasını önleyeceği, bunun ise hukuk devleti ilkesine aykırı olduğu, ayrıca Anayasa'nın 38. maddesinin beşinci fıkrasında, "Hiç kimse kendisini ve kanunda gösterilen yakınlarını suçlayan bir beyanda bulunmaya veya bu yolda delil göstermeye zorlanamaz." hükmüne yer verildiği, bu hükmün mefhumu muhalifinden belirtilen istisna dışında herkesin tanıklık yapma yükümlülüğünün bulunduğu kabul edilmesi gerektiği ve yine Anayasa'nın 12. maddesinde "Temel hak ve hürriyetler, kişinin topluma, ailesine ve diğer kişilere karşı ödev ve sorumluluklarını da ihtiva eder." denildiği, dolayısıyla anılan kişilerle ilgili olarak tanıklıkta bulunma yükümlülüğünün kaldırılmasının belirtilen anayasal hükümlerle de çeliştiği belirtilerek dava konusu kuralın, Anayasa'nın 2., 12. ve 38. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

188. 6216 sayılı Kanun'un 43. maddesi uyarınca dava konusu kural, ilgisi nedeniyle Anayasa'nın 13. ve 36. maddeleri yönünden de incelenmiştir.

189. Dava konusu cümlenin de yer aldığı kuralla 2937 sayılı Kanun'un 29. maddesinde yer alan ve görevin gizliliği ile devletin çıkarlarının zorunlu kıldığı hâllerde MİT mensuplarının tanık olarak dinlenebilmesini MİT Müsteşarının iznine bağlayan düzenlemede değişiklik yapılmakta ve devletin çıkarlarının zorunlu kıldığı hâller hariç olmak üzere MİT mensupları ile MİT'te görev yapmış olanların, MİT'in görev ve faaliyetlerine ilişkin hususlarda tanıklık yapamayacağı düzenlenmektedir.

190. Buna göre, düzenlemenin önceki hâlinde kural olarak MİT mensuplarının tanıklığına başvurulması mümkünken ve ancak görevin gizliliği ve devletin çıkarlarının zorunlu kıldığı istisnai hâlde bu kişilerin tanıklığına izin verilmeyebilirken, dava konusu kuralla MİT mensupları ile MİT'te görev yapmış olanların, MİT'in görev ve faaliyetlerine ilişkin hususlarda tanıklık yapması kural olarak yasaklanmakta ve sadece devletin çıkarlarının zorunlu kıldığı istisnai hâlde bu tanıklığa izin verilebilmektedir.

191. Bu çerçevede dava konusu kural, MİT'in görev ve faaliyetlerine ilişkin olan, ancak görevin gizliliği ve devletin çıkarları yönünden alenileşmesinde bir sakınca bulunmayan konularda da MİT mensupları ile MİT'te görev yapmış olanların tanıklığına başvurulmasını önlemektedir.

192. Anayasa'nın hak arama hürriyetini düzenleyen 36. maddesinin birinci fıkrasında, kişilerin hak arama özgürlükleri güvence altına alınmıştır. Hukuksal olanakları kapsamlı biçimde kullanabilme ve bu konuda tüm yollardan yararlanma hakkını içeren hak arama özgürlüğünün, hukuki uyumsuzluklara ilişkin olarak etkili bir soruşturma ve kovuşturma yapılarak maddi gerçeğin ortaya çıkarılmasını isteme hakkını da bünyesinde barındırdığında kuşku bulunmamaktadır. Bu yönüyle maddi gerçeğin ortaya çıkarılmasını önleyen kuralların, adaletin gerçekleşmesini önleyerek hak arama özgürlüğü ve hukuk devleti ilkesine zarar vereceği açıktır.

193. Maddi gerçeğin ortaya çıkarılmasını sağlayan araçlar arasında tanık delili de mevcut olup bu yönüyle kişilerin, uyumsuzluk konusu olaya ilişkin bilgisi olanların tanıklığına başvurma hakları bulunmaktadır.

194. Öte yandan, Anayasa'nın hak arama hürriyetini düzenleyen 36. maddesine 2001 değişiklikleriyle eklenen "adil yargılanma" ibaresine ilişkin gerekçede, taraf olduğumuz uluslararası sözleşmelerde de güvence altına alınan adil yargılanma hakkının madde metnine dâhil edildiği vurgulanmıştır. Bu

sözleşmelerden Avrupa İnsan Hakları Sözleşmesi ile AİHM uygulamasındaki adil yargılanma hakkı güvencelerinden birini de tanık dinletme ve sorgulama hakkı oluşturmaktadır.

195. Elbette ki bu hak mutlak olmayıp birtakım haklı ve makul nedenlerin bulunması hâlinde ve Anayasa'nın 13. maddesinde belirtilen güvencelere uygun olarak sınırlandırılabilir. Bu yönüyle Anayasa'nın 38. maddesinin beşinci fıkrası uyarınca kimsenin kendisi veya kanunda belirtilen yakınları aleyhine tanıklık yapmaya zorlanması mümkün olmadığı gibi, kişilerin özel hayatının korunması amacıyla veya devletin Anayasa'da belirtilen yükümlülükleri yerine getirmek üzere yürüttüğü görevlerin zorunlu kıldığı hâllerde de buna sınırlamalar getirilebilir.

196. Dava konusu kuralla MİT mensuplarının, MİT'in görev ve faaliyetlerine ilişkin tüm konularda tanıklık yapması kural olarak yasaklanmakta, sadece devletin menfaatlerinin zorunlu kıldığı hallerde bu kişilerin anılan konularda tanıklık yapması yetkili merciin iznine bırakılmaktadır. Oysa MİT'in görev ve faaliyet alanı çok geniş olup MİT'in görev ve faaliyetlerine ilişkin olup açıklanmasında devletin yürüttüğü göreve zarar vermeyecek fakat maddi gerçeğin ortaya çıkartılmasına, dolayısıyla sadece devletin çıkarlarının değil, bireylerin haklarının tespit edilerek korunabilmesine katkı sağlayacak konuların da bulunması mümkündür.

197. Dava konusu kuralda bu husus gözetilmeyerek açıklanmasında devletin yürüttüğü göreve zarar vermeyecek, fakat bireylerin haklarının tespit edilerek korunabilmesine katkı sağlayacak konularda da tanıklık yapılması yasaklanmaktadır. Bu durum, haklı ve makul bir nedene dayalı olmaksızın tanık deliline başvurma hakkına ölçülü olmayan bir sınırlama getirilmesi sonucunu doğurmakta ve maddi gerçeğin ortaya çıkartılmasını önleyerek hak arama özgürlüğü, adil yargılanma hakkı ve hukuk devleti ilkesinin zedelenmesine yol açmaktadır.

198. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2., 13. ve 36. maddelerine aykırıdır. İptali gerekir.

199. Kuralın, Anayasa'nın 12. ve 38. maddeleriyle ilgisi görülmemiştir.

L- Kanun'un 11. Maddesiyle 2937 Sayılı Kanun'a Eklenen Ek 1. Maddenin Birinci Fıkrasının İncelenmesi

1- İptal Talebinin Gerekçesi

200. Dava dilekçesinde özetle dava konusu kuralla MİT'in uhdesinde bulunan istihbari nitelikteki bilgi, belge, veri ve kayıtlar ile yapılan analizlerin, bazı suçlar hâriç olmak üzere adli mercilerce istenemeyeceği düzenlemesine yer verildiği, bu durumun resen araştırma ilkesinin geçerli olduğu ceza yargılamasında maddi gerçeğe ulaşılmasını engelleyeceği, ayrıca yargı organlarının bağımsızlığı

nedeniyle maddi gerçeği ortaya çıkarabilmeleri amacıyla her türlü bilgi, belge, veri ve kayıt, rapor, değerlendirme ve analizlere ulaşabilmeleri gerekirken anılan kuralla bunun engellendiği belirtilerek dava konusu kuralın, Anayasa'nın 2., 138. ve 140. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

201. 6216 sayılı Kanun'un 43. maddesi uyarınca dava konusu kural, ilgisi nedeniyle Anayasa'nın 36. maddesi yönünden de incelenmiştir.

202. Dava konusu kuralda, adli mercilerce TCK'nın İkinci Kitap, Dördüncü Kısım, Yedinci Bölümünde yer alan suçlarla ilgili olanlar hâriç olmak üzere MİT uhdesindeki istihbari nitelikteki bilgi, belge, veri ve kayıtlar ile yapılan analizlerin istenemeyeceği düzenlenmektedir.

203. Anayasa'nın 36. maddesi uyarınca hukuksal olanakları kapsamlı biçimde kullanabilme ve bu konuda tüm yollardan yararlanma hakkını içeren hak arama özgürlüğü, kişilere hukuki uyumsuzluklara ilişkin olarak etkili bir soruşturma ve kovuşturma yapılarak maddi gerçeğin ortaya çıkarılmasını isteme hakkını tanımaktadır. Bu yönüyle maddi gerçeğin ortaya çıkarılmasını önleyen kuralların adaletin gerçekleşmesini önleyerek hukuk devleti ve hak arama özgürlüğü ilkelerine zarar vereceği açıktır.

204. Diğer ülkelerdeki istihbarat teşkilatlarında olduğu gibi MİT'in de elde ettiği istihbarat bilgilerinin önemli bir kısmı doğası gereği kesin olmayan, bu nedenle adli işlemlerin tesisinde esas alınamayan ve delil değeri taşımayan bilgilerden oluşmaktadır. Ancak adli işlemlerin tesisinde esas alınamayan bu bilgiler, millî güvenlik siyasetinin belirlenmesinde ve önleyici güvenlik önlemlerinin alınması ile karşı istihbarat faaliyetlerinin organize edilmesinde önemli faydalar sağlayabilmekte ve doğası gereği bu bilgilerin gizliliğinin sağlanması gerekmektedir.

205. Dava konusu kuralla MİT'in uhdesinde bulunan istihbari bilgilerin kural olarak adli mercilerce istenemeyeceği düzenlenerek maddi gerçeğin ortaya çıkarılması yönünde herhangi bir katkısı olmayacak, ancak aleniyet kazanması halinde istihbarat faaliyetlerini aksatabilecek bilgilerin gizliliğinin muhafaza edilmeye çalışıldığı anlaşılmaktadır.

206. Kuralla bu şekilde bir taraftan adli mercilerce MİT uhdesindeki istihbari nitelikteki bilgi, belge, veri ve kayıtlar ile yapılan analizlerin istenmesi sınırlandırılırken, öbür taraftan bu sınırlamanın MİT'in esas çalışma alanına ilişkin suçlarla ilgili olan ve MİT dışında başka bir kurum veya kuruluşta bulunmayacak bilgiler yönünden (TCK'nın İkinci Kitap, Dördüncü Kısım, Yedinci Bölümünde yer alan suçlar) uygulanmayacağı düzenlenmiş, böylece maddi gerçeğin ortaya çıkarılmasına katkı sunabilecek bilgiler yönünden bir sınırlama yapılmasına izin verilmemiştir.

207. Bu çerçevede kuralın, işlenen suçlara yönelik olarak maddi gerçeğin araştırılmasını önleyen bir yönü bulunmamaktadır.

208. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2. ve 36. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

209. Kuralın, Anayasa'nın 138. ve 140. maddeleriyle ilgisi görülmemiştir.

IV- İPTALİN DİĞER KURALLARA ETKİSİ

210. 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrasında, kanunun belirli kurallarının iptali, diğer kurallarının veya tümünün uygulanmaması sonucunu doğuruyorsa, bunların da Anayasa Mahkemesince iptaline karar verilebileceği öngörülmektedir.

211. 2937 sayılı Kanun'un 29. maddesinin birinci fıkrasının birinci cümlesinin iptali nedeniyle uygulanma olanağı kalmayan ikinci cümlesinde yer alan "Ancak." ibaresinin de 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrası gereğince iptali gerekir.

V- YÜRÜRLÜĞÜN DURDURULMASI TALEBİ

212. Dava dilekçesinde özetle dava konusu kuralların Anayasa'ya açıkça aykırı olduğu ve yürürlüklerinin durdurulmaması hâlinde hukuk devleti yönünden giderilmesi olanaksız durum ve zararların ortaya çıkacağı, bu nedenle kuralların yürürlüklerinin durdurulmasına karar verilmesi gerektiği ileri sürülmüştür.

17.4.2014 tarihli ve 6532 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun'un;

A- 9. maddesiyle değiştirilen, 1.11.1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu'nun 29. maddesinin birinci fıkrasının ikinci cümlesinde yer alan "Ancak,." ibaresine yönelik yürürlüğün durdurulması talebinin, koşulları oluşmadığından REDDİNE,

B- 1- 6. maddesiyle 2937 sayılı Kanun'un 26. maddesine eklenen sekizinci fıkrasına,

2- 9. maddesiyle değiştirilen 2937 sayılı Kanun'un 29. maddesinin birinci fıkrasının birinci cümlesine, yönelik iptal hükümlerinin yürürlüğe girmelerinin ertelenmeleri nedeniyle bu fıkra ve cümleye ilişkin yürürlüğün durdurulması taleplerinin REDDİNE,

C- 1- 1. maddesiyle 2937 sayılı Kanun'un 4. maddesinin birinci fıkrasına eklenen (h) bendinde yer alan ".Bakanlar Kurulunca verilen görevleri yerine getirmek." ibaresine,

2- 3. maddesiyle 2937 sayılı Kanun'un;

a- 6. maddesinin deęiřtirilen birinci fıkrasının;

aa- (a) bendinde yer alan "., uygun koordinasyon yöntemlerini uygulayabilir" ibaresine,

ab- (b) bendine,

ac- (c) bendine,

ad- (i) bendinde yer alan ".alan veya." ibaresine,

b- 6. maddesine eklenen onbirinci fıkrada yer alan ".yukarıdaki hükümlere ve dięer kanunlardaki düzenlemelere baęlı kalmaksızın; MİT Müsteřarı veya yardımcısının onayıyla." ibaresine,

3- 6. maddesiyle 2937 sayılı Kanun'un 26. maddesine eklenen;

a- İkinci fıkranın ikinci cümlesine,

b- Üçüncü fıkrada yer alan "İsimsiz, imzasız, adresiz yahut takma adla yapıldığı anlaşılan ya da." ve ".delilleri ve dayanakları gösterilmeyen." ibarelerine,

c- Dördüncü fıkranın birinci cümlesinin, 25.10.1963 tarihli ve 353 sayılı Askeri Mahkemeler Kuruluşu ve Yargılama Usulü Kanunu'nun 15/A maddesinin üçüncü fıkrasının son cümlesi ile yedinci fıkrasının son cümlesine atıfta bulunulan bölümü dışında kalan kısmına,

4- 7. maddesiyle deęiřtirilen 2937 sayılı Kanun'un 27. maddesinin;

a- Birinci fıkrasında yer alan ".yetkisiz olarak alan, temin eden,." ibaresine,

b- Üçüncü fıkrasına,

c- Dördüncü fıkrasında yer alan ".ihmal veya." ve ".yükümlülüklerini yerine getirmeyenlere." ibarelerine,

5- 8. maddesiyle 2937 sayılı Kanun'un bařlığıyla birlikte deęiřtirilen 28. maddesinin birinci fıkrasında yer alan "., bu talepleri yerine getirenlerin hukuki ve cezai sorumluluęu doğmaz" ibaresine,

6- 11. maddesiyle 2937 sayılı Kanun'a eklenen ek 1. maddenin birinci ve ikinci fıkralarına,

yönelik iptal talepleri, 30.12.2015 tarihli ve E.2014/122, K.2015/123 sayılı kararla reddedildięinden, bu fıkra, bent, cümle, bölüm ve ibarelere iliřkin yürürlüęün durdurulması taleplerinin REDDİNE,

D- 6. maddesiyle 2937 sayılı Kanun'un 26. maddesine eklenen dördüncü fıkranın birinci cümlesinin, 353 sayılı Kanun'un 15/A maddesinin üçüncü fıkrasının son cümlesi ile yedinci fıkrasının son cümlesine atıfta bulunulan bölümü hakkında, 30.12.2015 tarihli ve E.2014/122, K.2015/123 sayılı

kararla karar verilmesine yer olmadığına karar verildiğinden, bu bölüme ilişkin yürürlüğün durdurulması talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA,

30.12.2015 tarihinde OYBİRLİĞİYLE karar verilmiştir.

VI- İPTAL KARARININ YÜRÜRLÜĞE GİRECEĞİ GÜN SORUNU

213. Anayasa'nın 153. maddesinin üçüncü fıkrasında, "Kanun, kanun hükmünde kararname veya Türkiye Büyük Millet Meclisi İçtüzüğü ya da bunların hükümleri, iptal kararlarının Resmi Gazetede yayımlandığı tarihte yürürlükten kalkar. Gereken hallerde Anayasa Mahkemesi iptal hükmünün yürürlüğe gireceği tarihi ayrıca kararlaştırabilir. Bu tarih, kararın Resmi Gazetede yayımlandığı günden başlayarak bir yılı geçemez." denilmekte, 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 66. maddesinin (3) numaralı fıkrasında da bu kural tekrarlanarak, Mahkemenin gerekli gördüğü hâllerde, Resmî Gazetede yayımlandığı günden başlayarak iptal kararının yürürlüğe gireceği tarihi bir yılı geçmemek üzere ayrıca kararlaştırabileceği belirtilmektedir.

214. 6352 sayılı Kanun'un 6. maddesiyle 2937 sayılı Kanun'un 26. maddesine eklenen sekizinci fıkranın ve aynı Kanun'un 9. maddesiyle değiştirilen 2937 Sayılı Kanun'un 29. maddesinin birinci fıkrasının birinci cümlesinin iptal edilmesi nedeniyle doğacak hukuksal boşluk kamu yararını ihlal edici nitelikte görüldüğünden, Anayasa'nın 153. maddesinin üçüncü fıkrasıyla 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince İPTAL HÜKÜMLERİNİN, KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAŞLAYARAK ALTI AY SONRA YÜRÜRLÜĞE GİRMESİNE, OYBİRLİĞİYLE, 30.12.2015 tarihinde karar verilmiştir.

VII- HÜKÜM

17.4.2014 tarihli ve 6532 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun'un;

A- 1. maddesiyle, 1.11.1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu'nun 4. maddesinin birinci fıkrasına eklenen (h) bendinde yer alan ".Bakanlar Kurulunca verilen görevleri yerine getirmek." ibaresinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, OYBİRLİĞİYLE,

B- 3. maddesiyle 2937 sayılı Kanun'un;

1- 6. maddesinin değiştirilen birinci fıkrasının;

a- (a) bendinde yer alan "., uygun koordinasyon yöntemlerini uygulayabilir" ibaresinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, OYBİRLİĞİYLE,

b- (b) bendinin,

ba- Birinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, OYBİRLİĞİYLE,

bb- İkinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Alparslan ALTAN ile Erdal TERCAN'ın karşıoyları ve OYÇOKLUĞUYLA,

c- (c) bendinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, OYBİRLİĞİYLE,

d- (i) bendinde yer alan ".alan veya." ibaresinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, OYBİRLİĞİYLE,

2- 6. maddesine eklenen onbirinci fıkrada yer alan ".yukarıdaki hükümlere ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın; MİT Müsteşarı veya yardımcısının onayıyla." ibaresinin;

a- Fıkrada yer alan ".yurt dışında veya yabancılar tarafından gerçekleştirilen iletişim ile ankesörlü telefonlarla gerçekleştirilen iletişim." ibaresi yönünden Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Zühtü ARSLAN, Engin YILDIRIM, Alparslan ALTAN, Erdal TERCAN ile M. Emin KUZ'un karşıoyları ve OYÇOKLUĞUYLA,

b- Fıkranın kalan bölümü yönünden Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, OYBİRLİĞİYLE,

C- 6. maddesiyle 2937 sayılı Kanun'un 26. maddesine eklenen;

1- İkinci fıkranın ikinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Alparslan ALTAN ile Erdal TERCAN'ın karşıoyları ve OYÇOKLUĞUYLA,

2- Üçüncü fıkrada yer alan "İsimsiz, imzasız, adressiz yahut takma adla yapıldığı anlaşılan ya da." ve ".delilleri ve dayanakları gösterilmeyen." ibarelerinin Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

3- Dördüncü fıkranın birinci cümlesinin;

a- 25.10.1963 tarihli ve 353 sayılı Askeri Mahkemeler Kuruluşu ve Yargılama Usulü Kanunu'nun 15/A maddesinin üçüncü fıkrasının son cümlesi ile yedinci fıkrasının son cümlesine atıfta bulunulan bölümüne ilişkin iptal talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA, OYBİRLİĞİYLE,

b- Kalan bölümünün Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Alparslan ALTAN ile Erdal TERCAN'ın karşıoyları ve OYÇOKLUĞUYLA,

4- Sekizinci fıkranın Anayasa'ya aykırı olduğuna ve İPTALİNE, iptal hükmünün, Anayasa'nın 153. maddesinin üçüncü fıkrası ile 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince, KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAŞLAYARAK ALTI AY SONRA YÜRÜRLÜĞE GİRMESİNE, OYBİRLİĞİYLE,

D- 7. maddesiyle değiştirilen 2937 sayılı Kanun'un 27. maddesinin;

1- Birinci fıkrasında yer alan ".yetkisiz olarak alan, temin eden,." ibaresinin,

2- Üçüncü fıkrasının,

3- Dördüncü fıkrasında yer alan ".ihmal veya." ve ".yükümlülüklerini yerine getirmeyenlere." ibarelerinin,

Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

E- 8. maddesiyle 2937 sayılı Kanun'un başlığıyla birlikte değiştirilen 28. maddesinin birinci fıkrasında yer alan "., bu talepleri yerine getirenlerin hukuki ve cezai sorumluluğu doğmaz" ibaresinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, OYBİRLİĞİYLE,

F- 9. maddesiyle değiştirilen 2937 sayılı Kanun'un 29. maddesinin birinci fıkrasının;

1- Birinci cümlesinin Anayasa'ya aykırı olduğuna ve İPTALİNE, iptal hükmünün, Anayasa'nın 153. maddesinin üçüncü fıkrası ile 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince, KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAŞLAYARAK ALTI AY SONRA YÜRÜRLÜĞE GİRMESİNE, OYBİRLİĞİYLE,

2- İkinci cümlesinde yer alan "Ancak,." ibaresinin, 2937 sayılı Kanun'un 29. maddesinin birinci fıkrasının birinci cümlesinin iptali nedeniyle uygulanma olanağı kalmadığından, 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrası gereğince İPTALİNE, OYBİRLİĞİYLE,

G- 11. maddesiyle 2937 sayılı Kanun'a eklenen ek 1. maddenin birinci ve ikinci fıkralarının Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

30.12.2015 tarihinde karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili - Burhan ÜSTÜN

Başkanvekili - Engin YILDIRIM

Üye: Serdar ÖZGÜLDÜR; Serruh KALELİ; Osman Alifeyyaz PAKSÜT; Recep KÖMÜRCÜ; Alparslan ALTAN; Nuri NECİPOĞLU; Hicabi DURSUN; Celal Mümtaz AKINCI; Erdal TERCAN; Muammer TOPAL; M. Emin KUZ; Hasan Tahsin GÖKCAN; Kadir ÖZKAYA; Rıdvan GÜLEÇ

KARŞIOY GEREKÇESİ

1. 2937 sayılı Kanun'un 6. maddesine, 17/4/2014 tarihli ve 6532 sayılı Kanun'un 3. maddesiyle eklenen fıkrada yer alan ". yukarıdaki hükümlere ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın; MİT Müsteşarı veya yardımcısının onayıyla." ibaresinin iptali istenmiştir.

2. İptali istenen ibarenin de içinde bulunduğu ek fıkra şu şekildedir: "Önleyici istihbarat elde etmek ve analiz yapabilmek amacıyla yukarıdaki hükümlere ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın; MİT Müsteşarı veya yardımcısının onayıyla yurt dışında veya yabancılar tarafından gerçekleştirilen iletişim ile ankesörlü telefonlarla gerçekleştirilen iletişim ve MİT mensuplarının, MİT'te görev almış olanların veya görev almak üzere başvuranların iletişimi tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir."

3. Öncelikle kuralın anlam ve kapsamını belirlemek gerekir. Kuralla önleyici istihbarat elde etmek ve analiz yapabilmek amacıyla MİT Müsteşarının veya yardımcısının onayıyla, aynı maddede ve diğer kanunlarda öngörülen hükümlere bağlı olmaksızın, fıkrada belirtilen kişilerin iletişimlerinin tespit edilebileceği, dinlenebileceği, sinyal bilgilerinin değerlendirilebileceği ve kayda alınabileceği düzenlenmektedir. Kurala göre iletişimleri denetlenebilecek kişileri iki grupta değerlendirmek mümkündür. Birinci grupta (a) yurt dışında bulunan herkes, (b) yurt içindeki yabancılar ve (c) ankesörlü telefon kullanan herkes yer almaktadır. İkinci grupta ise (a) MİT mensupları, (b) MİT'te görev almış olanlar ve (c) MİT'te görev almak için başvuranlar bulunmaktadır. Kuralın Anayasa'ya uygunluğu denetlenirken bu iki grup açısından farklı değerlendirmeler yapılması kaçınılmazdır.

4. Haberleşme hürriyetinin demokratik toplumlarda vazgeçilmez ve ikame edilemez bir öneme sahip olduğu bilinmektedir. Bu hürriyet, kişilerin özel hayatına ilişkin bilgileri sadece istediği kişilerle paylaşmasına imkân tanımaktadır. Mahremiyetin korunması, kişilerin dış müdahaleden masun özerk alanlarının korunması amacına hizmet eder. Bu nedenle, haberleşmenin gizliliğinin ihlali kişisel özerklik ve özgürlük alanına ağır bir müdahaledir.

5. Haberleşmenin gizliliğine müdahale, ancak belli meşru amaçların zorunlu kıldığı çok istisnai durumlarda ve ölçüde haklılaştırılabilir. Genel olarak ifade etmek gerekir ki milli güvenliğin korunması, organize suçlarla ve özellikle de terörle mücadele edilmesi gibi sebepler kişilerin özel

hayatlarına ve özellikle de haberleşmelerine müdahale edilmesini gerekli kılabilmektedir. Başta yaşama hakkı olmak üzere temel hak ve hürriyetlerin ve demokratik düzenin korunması amacıyla iletişimin denetlenmesi gerekebilir. Bu bağlamda, özel hayatın ve haberleşmenin gizliliği hakkının sınırsız olmadığı açıktır. Ancak, iletişimi denetleme yetkisinin kontrolsüz bir şekilde idari makamlara tanınması ve yetkinin kötüye kullanılması, bizzat korunmak istenen değerleri ortadan kaldıracak sonuçlar doğurabilir. Bu nedenle yetkinin kapsamının, sınırlarının ve kötüye kullanılmasını önleyecek ya da kötüye kullanımın zararlarını telafi edecek etkili denetim mekanizmalarının hukuk sisteminde öngörülmesi gereklidir. Nitekim anayasal hükümler, özel hayata saygı hakkının ve haberleşme hürriyetinin belli amaçlarla sınırlandırılabilceğini, ancak bu sınırlamaların kanunilik, meşru amaç, demokratik toplum düzeninde gereklilik ve ölçülülük kriterlerine uygun olması gerektiğini açıkça belirtmektedir.

6. Anayasa'nın haberleşme hürriyetini düzenleyen 22. maddesinin birinci fıkrasına göre "Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır". Aynı maddenin ikinci fıkrasına göre ise "Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar."

7. Anayasa'nın 22. maddesinin "İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir." şeklindeki üçüncü fıkrasının yorumu, somut davada belirleyici niteliktedir. Fıkra biri geniş, diğeri dar olmak üzere iki şekilde yorumlanabilir. Geniş yorum benimsendiğinde, hâkim kararıyla denetleme kuralına kanunla bazı kamu kurum ve kuruluşları yönünden istisna getirilebilir, bu kamu kurum ve kuruluşları hâkim kararına ihtiyaç olmaksızın kurum içinde veya dışında bulunan belli kişilerin haberleşmelerini denetleyebilirler. Bu anayasa hükmünün dar yorumu ise, hâkim kararıyla iletişimin denetlenmesine getirilen istisnanın ancak kanun tarafından öngörülen kamu kurum ve kuruluşlarında disiplini ya da milli güvenliği koruma gibi amaçlara yönelik olduğunun kabulünü gerektirir.

8. Mahkememiz çoğunluğunun, açıkça tartışmamakla birlikte, söz konusu anayasal hükmü geniş yorumladığı anlaşılmaktadır. Gerek hükmün lafzının, gerekse anayasa koyucunun amacının söz konusu hükmün bu kadar geniş yorumlanmasına müsait olmadığını düşünüyoruz. Öncelikle, fıkra

istisnaların "uygulanacağı kamu kurum ve kuruluşları"ndan, başka bir ifadeyle istisnaların uygulanacağı "yer"den bahsetmektedir. Danışma Meclisi'nin taslağında yer almayan bu hükmü maddeye ekleyen Milli Güvenlik Konseyi Anayasa Komisyonu'nun gerekçesi bu durumu daha net bir şekilde ortaya koymaktadır. Bu gerekçe şu şekildedir: "Maddeye 'İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir' fıkrası eklenmiştir. Böylece, haberleşme hürriyetinin ve gizliliğinin istisnaî olarak kısıtlanabileceği kamu kurum ve kuruluşlarının kanunla belirtileceği öngörülmüştür."

9. Diğer yandan, anayasa koyucunun amacının da özel hayata ve haberleşmeye müdahalede hâkim kararının alınması gerektiğine ilişkin ilkeyi işlevsiz kılacak bir hüküm ihdas etmek olduğu söylenemez. Anayasa'da "Özel hayatın gizliliği ve korunması" başlığı altında yer alan, özel hayatın gizliliği (m.20), konut dokunulmazlığı (m.21) ve haberleşme hürriyeti (m.22) hükümleri bir bütün olarak değerlendirildiğinde, kişilerin bireysel özerklikleri ile maddi ve manevi varlıklarını koruma ve geliştirmede bu derece önemli olan söz konusu hak ve hürriyetlerin sınırlandırılmasında, idareden bağımsız şekilde hâkim kararı güvencesi sağlandığı görülmektedir. Nitekim, Danışma Meclisi'nin maddeye ilişkin gerekçesinde bu husus şu şekilde vurgulanmıştır: "Özel hayatın gizliliğinin korunması ve konut dokunulmazlığında olduğu gibi, haberleşmenin gizliliği de ancak hâkim kararıyla kaldırılabilir; fakat kanunun açıkça yetkili kıldığı başka bir merci dahi, acele hallerde, istisnaen, bu yolda emir verebilecektir."

10. Anayasanın 22. maddesinin son fıkrasının, kanunla öngörülen belli kurumlarda ve kurumla ilgili kişilerin iletişimlerinin denetlenmesinin ötesinde, hemen herkesi hâkim kararı olmadan dinleme sonucunu doğuracak şekilde geniş anlaşılması, hâkim kararıyla dinleme ilkesini istisnalarla işlevsiz kılabilir, dolayısıyla söz konusu hak ve özgürlükleri korumasız bırakabilecektir. Bu nedenle 22. maddenin son fıkrasının özgürlükçü bir yaklaşımla dar yorumlanması gerekir. Bu istisnai kuralın amacı, cezaevi gibi sıkı disiplin kurallarının uygulandığı bazı kamu kurum ve kuruluşlarında iletişimin denetiminin hâkim kararı olmadan yapılabilmesini sağlamaktır.

11. İptali istenen kuralda, hâkim kararı olmadan MİT Müsteşarının veya yardımcısının onayıyla iletişimi denetlenebilecek olan ikinci gruptaki kişiler kurumda çalışan, çalışmış veya çalışacak olanlardır. Anayasa'nın 22. maddesinin son fıkrası gereği, kanun koyucunun MİT Müsteşarı ya da yardımcısına, önleyici istihbarat elde etmek ve analiz yapabilmek amacıyla, bu kişilerin iletişimlerinin denetlenmesi yetkisi vermesinde Anayasa'ya aykırılık bulunmamaktadır. MİT mensuplarının, MİT'te çalışmış veya çalışacak olanların iletişimlerinin denetimi, kurum içi disiplin ve istihbarata karşı koyma (kontrespiyonaj) çalışmaları kapsamında gerekli ve ölçülü olarak kabul edilebilir.

12. Buna karşılık, birinci grupta yer alan kişilerin iletişimlerinin denetlenmesi söz konusu olduğunda aynı sonuca ulaşmak mümkün değildir. MİT'le hiçbir şekilde ilgili bulunmayan çok geniş bir kesimi kapsayan bu kişilerin iletişimleri, ancak Anayasa'nın 22. maddesinin ikinci fıkrası kapsamında hâkim kararıyla; gecikmesinde sakınca bulunan durumlarda da en geç yirmidört saat içinde hâkim onayına sunulmak kaydıyla, yetkili merciin emriyle denetlenebilir. Bu nedenle, iptali istenen ibare, birinci grupta yer alan kişiler yönünden Anayasa'nın 22. maddesine aykırıdır ve iptali gerekir.

13. Bir an için 22. maddenin son fıkrasının hâkim kararı olmaksızın MİT Müsteşarı ve yardımcısına birinci grupta yer alan kişilerin de iletişimlerini denetleme konusunda yetki verdiği kabul edilse bile kuralın Anayasa'nın 13. maddesi ışığında değerlendirilmesi ve iptal edilmesi gerekirdi. Burada verilen yetkinin gerçekten istisnai nitelikte olup olmadığını, başka bir ifadeyle haberleşme hürriyetine yönelik müdahalenin 13. maddede güvenceye alınan kriterlere uygun olup olmadığını belirlemek gerekir.

14. Öncelikle MİT Müsteşarı veya yardımcısına verilen yetki kullanılarak iletişimlerini denetlenecek kişilerin, gerçekten de istisnanın anlamına uygun olacak şekilde, dar bir alanda sınırlı sayıda kişiyi kapsayıp kapsamadığı incelenmelidir. Kuralla iletişimlerinin denetlenmesine hâkim kararı olmaksızın izin verilen grubun yurt dışında bulunan vatandaş olsun olmasın herkesi, yurtiçindeki tüm yabancıları ve ankesörlü telefonla görüşen herkesi içine alacak şekilde geniş bir kesimi kapsadığı görülmektedir. Üstelik bu kişilerin belli bir suçu işlediği ya da işleyeceği şüphesi, terör örgütlerine ya da yabancı istihbarat teşkilatlarına mensup olup olmadıkları gibi hususlara bakılmaksızın "önleyici istihbarat elde etmek" veya "analiz yapabilmek" amacı gibi oldukça geniş bir çerçevede kapsamın belirlenmesi yoluna gidilmiştir.

15. Diğer yandan, kuralda iletişimin denetlenmesinin belli bir süreyle sınırlandırılması ve denetleme tedbiri sona erdikten sonra içeriklerin imha edilmesi gibi güvencelere yer verilmemiştir.

16. Anayasa'nın 20., 21. ve 22. maddelerinin ikinci fıkraları, kişilerin özel hayatlarına saygı ve konut dokunulmazlığı hakları ile haberleşme hürriyetlerinin millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın veya başkalarının hak ve özgürlüklerinin korunması amacıyla sınırlandırılabilirliğini öngörmektedir. Bu kapsamda, iletişimin denetlenmesinin özellikle terörle mücadele ve demokratik düzenin korunması bakımından gerekli olduğu hususu izahtan varestedir. Ancak Avrupa İnsan Hakları Mahkemesi'nin (AİHM) kararlarında da belirtildiği üzere, demokrasiyi korumak için başvuru bu tedbirlerin kötüye kullanılması durumunda, "polis devleti" uygulaması haline geleceği ve bizzat korunmak istenen demokrasiyi yok edebilecek potansiyele sahip olduğu da bir gerçektir. Bu nedenle, iletişimin denetlenmesi tedbirinin kötüye kullanılması

karşısında yeterli ve etkili güvencelerin sağlanması bir zorunluluktur (bkz. Klass ve diğerleri/Almanya, B.No: 5029/71, 6 Eylül 1978, §§ 42, 49, 50; Roman Zakharov/Rusya, B.No: 47143/06, 4 Aralık 2015, § 232, 233).

17. Kuşkusuz bu güvencelerin başında yargısal denetim gelmektedir. AİHM'e göre, iletişimin denetlenmesi talimatının verilmesi, denetlemenin uygulanması ve tamamlanmasından sonrası olmak üzere üç aşamada denetim kararını alan ve uygulayan idareden bağımsız bir denetim ve gözetimin yapılması gerekir. Bu denetim, prensip olarak ve tercihen yargı tarafından yapılmalıdır. Zira demokratik toplumun temel niteliklerinden biri olan ve Avrupa İnsan Hakları Sözleşmesi'nin Dibacesinde açıkça atıf yapılan hukukun üstünlüğü, idari organların bireysel haklara yönelik müdahalelerinin bağımsızlık, tarafsızlık ve gerekli usul güvencesini en iyi şekilde sağlayan yargının denetimine tâbi tutulmasını gerektirir (Klass ve diğerleri/Almanya, § 55).

18. AİHM, Klass kararında, idareden tamamen bağımsız olarak görev yapan "Parlamento Kurulu" ve onun oluşturduğu "G 10 Komisyonu"nun sağladığı güvenceleri dikkate alarak, iletişimin denetlenmesi aşamalarında yargısal kontrolün olmamasını demokratik toplumda sınırı aşan bir eksiklik olarak görmemiştir (Klass ve diğerleri/Almanya, § 56). Bununla birlikte, kural olarak, kişilerin iletişiminin denetlenmesinin her aşamada yargısal kontrolünün yapılması gerekir. Nitekim AİHM, kısa bir süre önce verdiği kararda, iletişimin denetlenmesinin hâkim kararıyla yapılması ve denetlenmesi gerekliliğini daha net bir şekilde vurgulamıştır. AİHM'e göre, harici yargısal denetimin gecikme riski taşıyacağı çok acil durumlarda, hâkim kararı olmadan da idari emirle iletişimin denetlenmesi yoluna gidilebilir. Ancak iletişimin denetlenmesi talimatının verildiği sırada yargısal onayın aranmadığı bu tür acil durumlarda alınan tedbirlerin, bilahare mutlaka yargısal nitelikte bir denetime tabi tutulması gerekir (bkz. Szabó ve Vissy/Macaristan, B.No: 37138/14, 12 Ocak 2016, § 81).

19. Esasen, iptali istenen kuralın da içinde bulunduğu Kanun'un 6. maddesine, 3/7/2005 tarihli ve 5397 sayılı Kanun'un 3. maddesiyle eklenen fıkranın birinci cümlesine göre, MİT'e Kanunla verilen görevlerin yerine getirilmesi amacıyla, "Anayasanın 2 nci maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde Devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, Devlet sırrının ifşasının tespiti ve terörist faaliyetlerin önlenmesine ilişkin olarak, hâkim kararı veya gecikmesinde sakınca bulunan hallerde MİT Müsteşarı veya yardımcısının yazılı emriyle telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir."

20. Aynı fıkranın devamında, gecikmesinde sakınca bulunan durumlarda MİT Müsteşarı veya yardımcısı tarafından verilen yazılı emrin yirmidört saat içinde yetkili ve görevli hâkimin onayına

sunulacağı, hâkimin kararını en geç yirmidört saat içinde vereceği, sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde tedbirin derhal kaldırılacağı, bu halde dinlemenin içeriğine ilişkin kayıtların en geç on gün içinde yok edileceği, durumun bir tutanakla tespit edilip tutanağın denetimde ibraz edilmek üzere muhafaza edileceği belirtilmektedir.

21. Müteakip fıkrada iletişimin denetlenmesinin ne kadar süreyle yapılabileceğine dair hükümler yer almaktadır. Buna göre, iletişimin denetlenmesine yönelik kararlar en fazla üç ay için verilebilecek, bu süre her defasında üçer ayı geçmeyecek şekilde en fazla üç defa uzatılabilecek, ancak casusluk faaliyetlerinin tespiti ve terör örgütünün faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi halinde, hâkim üç aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebilecektir.

22. Öte yandan, iptali istenen kuralın aksine, burada dinleme tedbirinden sonra elde edilen bilgilerin akıbeti hakkında da önemli güvencelere yer verilmiştir. Buna göre, "Uygulanan tedbirin sona ermesi halinde, dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir." Ayrıca elde edilen kayıtların Kanunda belirtilen amaçlar dışında kullanılamayacağı, bilgi ve kayıtların saklanmasında ve korunmasında gizlilik ilkesinin geçerli olacağı hükme bağlanmıştır.

23. Dava konusu kuralda ise bu güvencelerden hiçbirine yer verilmemiştir. Kural "yukarıdaki hükümlere ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın" ibaresiyle, sadece denetlemenin hâkim kararıyla olması ya da sonradan hâkim onayına sunulması şeklindeki güvenceyi değil, aynı zamanda denetim emrinin verilmesi, emrin icrası ve denetim sonrası aşamalarda haberleşme hürriyetini korumaya yönelik diğer teminatları da devre dışı bırakmıştır.

24. Tüm bu açıklamalar çerçevesinde, kuralın haberleşme hürriyetine demokratik toplumda gerekli ve ölçülü olmayan bir sınırlama getirdiği, dolayısıyla Anayasa'nın 22. maddesine aykırı olduğu anlaşılmaktadır.

Açıklanan gerekçelerle, fıkrada yer alan ".yurt dışında veya yabancılar tarafından gerçekleştirilen iletişim ile ankesörlü telefonlarla gerçekleştirilen iletişim." ibaresi yönünden çoğunluğun red yönündeki görüşüne katılmıyoruz.

Başkan - Zühtü ARSLAN

Başkanvekili - Engin YILDIRIM

Üye: M.Emin KUZ

FARKLI GEREKÇE

2937 sayılı Kanun'un 6. maddesine eklenen on birinci fıkrada yer alan ".yukarıdaki hükümlere ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın; MİT Müsteşarı veya yardımcısının onayıyla." ibaresi Mahkememizce incelenmiş kuralın iddia edildiği gibi, Anayasa'nın 2., 7., 20. ve 22. maddelerine aykırı olmadığına beş'e karşı on iki oyçokluğu ile karar verilmiştir.

Benimde katıldığım Mahkememiz red gerekçesine kısmi yetersizliği nedenleri ile karara aşağıda açıklanan ek gerekçeler dahilinde katılmıştır.

İptali istenen dava konusu kurala göre;

MİT'nin önleyici istihbarat elde etmek için analiz yapabilmek amacı ile halen mevzuatımızda (telekomünikasyon aracılığı ile kişilerin iletişiminin tespit edilebilmesi için CMK 135. maddesi ya da 2559 ile 2803 sayılı Kanun'da ve de 2937 sayılı Kanun'un 6. maddesinin iki ila onbirinci fıkralarında) belirtilen şartlar gerçekleşmese de MİT müsteşarı ya da yardımcısının onayı ile yurt dışında gerçekleştirilen / yabancılar tarafından gerçekleştirilen / ankesörlü telefonlar ile gerçekleştirilen / MİT mensupları, MİT'te görev almış olanlar veya görev almak üzere başvuranlarca gerçekleştirilenlerin / iletişimleri tespit edilebilecek, sinyal bilgileri değerlendirilebilecek ve kayda alınabilecektir.

İletişimin tespiti için mevcut düzenlemelerde aranan hakim kararı, kural kapsamındaki yönünden MİT müsteşar ve yardımcısının onay yeterliliği içine alınmış, düzenlemelerde iletişimin tespiti kararı verilebilmesi için aranan diğer suç işlendiğine dair kuvvetli şüphesi ya da demokratik hukuk devletine yönelik ciddi tehlikenin varlığı şartları yerine de yine iptali istenen kural kapsamındaki kişi ya da eylemin gerçekleştirildiği yer ve araçlar yönünden önleyici istihbarat elde etmek ve analiz kabiliyeti amaçlarının unsur olarak eklendiği görülmektedir.

MİT, ülkenin varlığına, bağımsızlığına, güvenliğine ve Anayasal düzenine, milli gücünü meydana getiren bütün unsurlara karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkında istihbarat oluşturmak, bunu ilgili kamu kurumları ile paylaşmak, demokratik toplum düzeni bakımından zorunlu milli güvenliğin, kamu düzeninin var olması için suç işlenmesinin önlenmesini sağlamak şeklinde yasal bir görev alanına sahiptir.

Mahkememiz yaptığı değerlendirmede;

Önleyici istihbarat elde etmek ve analiz amacı ile MİT'e iletişim tespit ve kayda alınmasında diğer kanunlardaki düzenlemelere bağlı kalmaksızın bir yetki verildiğini, verilen yetkinin özel hayatın ve

haberleşmenin gizliliği haklarına bir sınırlama getirdiğinin açık olduğunu ancak demokratik ülkelerde terör ve casusluk faaliyetlerine karşı istisnai durumlarda iletişimin denetlenmesine ihtiyaç duyulabildiğini, Anayasa'nın 22. maddesinde yer alan haberleşme özgürlüğü hakkına vaki bir müdahalede, sınırlama rejiminin saydığı nedenlerle bağlı olarak MİT'in bunu uygulayabilecek nitelikte bir kurum sayılacağını, Anayasa'nın 20. ve 22. maddesi kapsamında, kural ile gelen müdahalede hakların korunması ile milli güvenliğin ve kamu düzeninin sağlanması arasındaki makul dengenin kurulduğu ve amaca ulaşmada ölçülü olduğunu kabul etmektedir. Ayrıca, bu sonuca ulaşırken denetim ilkeleri kapsamı dışında tutulacak dava konusu kural kapsamında elde edilen bilgilerin gizliliğinin korunacağı amacı dışında ya da kötüye kullanılmasını önleyecek, denetleyecek yasal güvencelerin varlığı da ölçülülüğe gerekçe yapılmıştır.

Sorun kural kapsamında elde edilen bilgilerin akıbetinden ziyade kural ile gelen iletişimin denetlenmesi ve değerlendirilmesinde ilgili yasaların bugün aradığı ve şart koştuğu unsurları aşan bir yetkinin MİT Müsteşar ve yardımcısına verilmesi noktasındadır.

Bu yetkinin amaç ve kapsamı belirlenmeli, kuralın Anayasal haklara getirdiği müdahalenin kanuniliği, gerekliliği ve ölçülülüğü değerlendirilmesi yapılmalıdır. Kararda demokratik toplumda gereklilik değerlendirilmesi yeterince yapılmamış Anayasa'nın 16. maddesinde değerlendirmeye alınmamıştır.

Sınırlamanın MİT'e verilen görev kapsamı içinde "alınması gerekli tedbirler" den olduğuna ilişkin müdahale alanı yönünden başvuru alanı ile ulaşılmak istenen amaç değerlendirilmesi yapıldığında; kanun koyucunun kuralda belirttiği sınırlı alan içinde kalanlardan, yurt dışında bulunanların ülke dışında yaşadıkları süreçte ülke aleyhine yasa dışı faaliyetlerde bulunma kolaylıklarına karşı takipte ve önlemlerde hukuki zorluklar, yurt içinde yaşayan yabancılar yönünden ise bunların ülkede yerleşik düzen nedeniyle bulunmamaları, onların ise yabancı tabiyet ve kimlik taşımalarının getirdiği farklı hukuki koruma alanları, yabancıların ülke milli menfaatlerinin korunması ve yaşatılmasında beklenilmesi doğal diyemeyeceğimiz hassasiyet yoklukları, farklı duyarlılık ölçütleri ile Anayasa'nın 16. maddesinde öngörülen, yabancının hak ve hürriyetlerinin vatandaştan farklı olarak sınırlanıp düzenlenebilmesine verdiği yetki karşısında getirilen sınırlamanın anılan hakların özünü zedeleyen bir niteliğinden bahsedilemeyeceği ve MİT'in görevlerini yerine getirmesinde gerekli ve zorunlu olduğu görülmektedir.

Ayrıca MİT mensuplarının, MİT'de görev almış olanların veya almak üzere başvuranlar hakkında da kurumun önemi, ödevi, amacı karşısında önleyici istihbarat elde etme ve analiz etme anlamında verilen yetkinin hakka ölçüsüz bir müdahale niteliği taşıdığı söylenemeyecektir.

Yukarıda açıklanan nedenler ile, kural ile gelen müdahale bizatihi demokratik düzenin varlığının ispatı vücudu için gerekli ve korunması amacına erişmek için lüzumlu sınırı aşmamakta ve Anayasa'nın 16. maddesinin öngördüğü yetki sınırı içinde kaldığından çoğunluk görüşüne anılan nedenlerle farklı gerekçe ile katılmıştır.

Üye - Serruh KALELİ

KARŞIOY GEREKÇESİ

1- 17.4.2014 tarihli ve 6532 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun'un 3. Maddesiyle 2937 Sayılı Kanun'un 6. Maddesinin Değiştirilen Birinci Fıkrasının (b) Bendinin İkinci Cümlesi Yönünden

1. 2937 sayılı Kanun'un birinci fıkrasının (b) bendinin birinci cümlesinde, MİT'in kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, Bankacılık Kanunu kapsamındaki kurum ve kuruluşlar ile diğer tüzel kişiler ve tüzel kişiliği bulunmayan kuruluşlardan bilgi, belge, veri ve kayıtları alabileceği, bunlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim alt yapısından yararlanabileceği ve bunlarla irtibat kurabileceği belirtildikten sonra iptali istenen ikinci cümlesinde, bu kapsamda talepte bulunulanların, kendi mevzuatlarındaki hükümleri gerekçe göstermek suretiyle talebin yerine getirilmesinden kaçınamayacaklarına ilişkin bir düzenlemeye yer verilmiştir.

2. Anayasa'nın 25., 26., 27. ve 28. maddelerinde ifade ve kanaat hürriyeti ve basın özgürlüğü; 36. maddesinin birinci fıkrasında, "Herkes, meşrû vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir" denilerek adil yargılanma ve savunma hakkı; 38. maddesinin beşinci fıkrasında "Hiç kimse kendisini ve kanunda gösterilen yakınlarını suçlayan bir beyanda bulunmaya veya bu yolda delil göstermeye zorlanamaz." denilerek kişinin kendisini ve yakınlarını suçlamaya zorlanamaması hakkı güvence altına alınmıştır.

3. Yine Anayasa'nın 20. maddesinin ilk fıkrasında herkesin, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu ve özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş; ikinci fıkrasında, millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili

kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstünün, özel kâğıtlarının ve eşyasının aranamayacağı ve bunlara el konulamayacağı, yetkili merciin kararının yirmidört saat içinde görevli hâkimin onayına sunulacağı, hâkimin, kararını el koymadan itibaren kırksekiz saat içinde açıklayacağı; aksi halde, el koymanın kendiliğinden kalkacağı; üçüncü fıkrasında ise herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın, kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı, kişisel verilerin, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir.

4. Anayasa'da düzenlenen bu haklar, mutlak olmayıp Anayasa'nın ilgili maddelerinde ve diğer maddelerinde belirtilen gereklere dayalı olarak sınırlandırılabilir. Kuşkusuz bu sınırlama yönünden de Anayasa'nın 13. maddesinde yer alan güvencelere uygun davranılması gerekir.

5. Anayasa'nın 20. maddesinde millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, bir kimsenin üstünün, özel kâğıtlarının ve eşyasının aranabilmesi ve bunlara el konulabilmesi için usulüne göre verilmiş hâkim kararı bulunması şartını aramıştır. Hakim kararı şartı yönünden Anayasa'nın "Kişinin Hakları ve Ödevleri" başlıklı İkinci Bölümünün IV. Başlığı olan "Özel hayatın gizliliği ve korunması" başlığı altında düzenlenen özel hayatın gizliliği(m.20), konut dokunulmazlığı(m.21) ve haberleşme hürriyeti(m.22) ortak hükümler içermektedir.

6. Anayasa'da kişisel verilerin, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir.

7. Kişisel verilere ilişkin kuralların aynı zamanda kişisel veri niteliğindeki bilgilerin teminine, kullanılabilmesine, işlenebilmesine, ulaşılabilmesine, saklanma süresine, temin edilme gerekçesine ilişkin hususlarda bir belirlilik içermesi gerekmektedir. Ancak iptali istenilen düzenlemede kişisel verileri koruyucu herhangi bir kurala yer verilmeksizin, kapsamı ve sınırları alabildiğine geniş bir alanda tüm kamu ve özel kurum ve kuruluşlarda bulunan kişisel verilere, veri sahipleri ile birlikte bu kurum ve kuruluşların rıza ve muvafakatleri olmasa ve hatta mevzuatta buna engel düzenlemeler bulunsada dahi, güvenlik nedeniyle bir kamu kurumuna bu verileri de içerebilecek bilgi ve belgeleri verme zorunluluğu getirilmesi belirtilen anayasal güvence ile de bağdaşmaz.

8. Anayasa'nın 20. maddesinin gerekçesinde de belirtildiği üzere özel hayatın korunması, her şeyden önce bu hayatın gizliliğinin korunmasını, başkalarının gözleri önüne serilmemesini gerektirir. Kişinin özel hayatında yaşananların, yalnız kendisi veya kendisinin rıza gösterdiği kimseler tarafından bilinmesini isteme hakkı, kişinin temel haklarından biridir ve bu niteliği nedeniyle insan haklarına ilişkin beyanname ve sözleşmelerde yer almış, tüm demokratik ülkelerin mevzuatlarında açıkça belirlenen istisnalar dışında devlete, topluma ve diğer kişilere karşı korunmuştur. Bu koruma bireyinkendisine ilişkin herhangi bir bilginin rızası olmaksızın açıklanmamasını, yayılmamasını, nakledilmemesini ve bu bilgilere başkalarının ulaşamamalarını da kapsamaktadır.

9. Çağdaş demokrasiler temel hak ve özgürlüklerin en geniş ölçüde sağlanıp güvence altına alındığı rejimlerdir. Temel hak ve özgürlükleri büyük ölçüde kısıtlayan ve kullanılamaz hale getiren sınırlamalar hakkın özüne dokunur. Temel hak ve özgürlüklere getirilen sınırlamaların yalnız ölçüsü değil, şartları, nedeni, yöntemi, kısıtlamaya karşı öngörülen kanun yolları gibi güvenceler hep demokratik toplum düzeni kavramı içinde değerlendirilmelidir.

10. Anayasa'nın 2. maddesinde belirtilen hukuk devletinin ön koşulları arasında hukuki güvenlik ile belirlilik ilkeleri bulunmaktadır. Kişilerin hukuki güvenliğini sağlamayı amaçlayan hukuki güvenlik ilkesi, hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar. Belirlilik ilkesi ise yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olmasını, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesini ifade etmektedir.

11. Konu kişisel veriler olunca, Anayasa tarafından kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvencenin ve Anayasa'nın 2. maddesinde esasları düzenlenen hukuk devletinin ön koşulları arasında yer alan hukuki güvenlik ile belirlilik ilkelerinin gereklerinin yerine getirilebilmesi için bu hakkı ilgilendiren yasal düzenlemelerin, açık, anlaşılabilir ve kişilerin söz konusu haklarını kullanabilmelerine elverişli olması gerekir. Ancak böyle bir düzenleme ile kişilerin özel hayatlarını ilgilendiren veri, bilgi ve belgelerin resmi makamların keyfi müdahalelerine karşı korunması olanaklı hale getirilebilir. Belirtilen ilkeler doğrultusunda, kişisel verileri düzenleyen kanunlarda kişisel verilerin neden ve hangi gerekçeyle temin edileceğine ilişkin olarak konu ve amaç sınırlamasının yapılması yanında bu verilerin kapsamının ve ne şekilde kullanılacağına da belirlenmiş olması gerekmektedir.

12. Mahkememiz 2.10.2014 tarih ve E.2014/149, K.2014/151 sayılı kararında,internet trafik bilgisinin TİB tarafından ilgili işletmecilerden herhangi bir hukuki inceleme ya da sürece dahil olmadan alınmasını ve hâkim tarafından karar verilmesi durumunda bu bilginin ilgili mercilere verilmesini düzenleyen 5651 sayılı Kanun'un 3. maddesinin (4) numaralı fıkrasının iptaline karar verirken dayandığı gerekçelerden bazıları şöyledir: "Kuralda, temin edilecek bilgiyle ilgili olarak herhangi bir konu ve amaç sınırlaması bulunmadığı gibi bilginin kapsamı, ne şekilde kullanılacağı, tutulacağı süre, temin edilme gerekçesi gibi hususlarla ilgili olarak da herhangi bir belirlilik bulunmamaktadır...Bu durumda verilerin işlenebileceği hallerin kanunda açıkça yer alması zorunluluğu bulunmasına karşın, kuralda herhangi bir belirleme ve sınırlama yapılmaksızın doğrudan kişisel veri niteliğindeki trafik bilgisinin temin edilmesine ve işlenmesine olanak sağlanmasının bu yönüyle Anayasa'nın 20. maddesine aykırı olduğu açıktır...Anayasa'nın 13. ve 20. maddelerinde yer alan güvencelere rağmen dava konusu kural ile kişiler, bilgi toplama, saklama, işleme ve değiştirme yetkisi olan idareye ve diğer kişilere karşı korumasız bırakılmış, veri toplamanın amaç, gerekçe, kapsam ve sınırlama yasal düzenlemede yer verilmemiştir...".

13. Anayasa Mahkemesinin kişisel verilerin korunması ile ilgili olarak verdiği diğer kararlarda da ortaya koyduğu bu gerekçeler dikkate alındığında, kişisel verilerin ilgili üçüncü kişiler ya da kamu kurum ve kuruluşları ile paylaşılabilmesi için, söz konusu kişi ve kurumların bu verilere erişebileceği hususunda kanunen yetkilendirilmiş olmaları ve bu verilerin ilgili kurum ve kişilerin görevlerini yapması için gerekli olmasının yanı sıra bu görevlerin yerine getirilmesi ile de sınırlı olması gerekir. Kişisel verilere ilişkin kuralların aynı zamanda kişisel veri niteliğindeki bilgilerin teminine, kullanılabilmesine, işlenebilmesine, ulaşılabilmesine, saklanma süresine, temin edilme gerekçesine ilişkin hususlarda bir belirlilik içermesi de gerekmektedir.

14. Buna göre maddenin iptali istenen ikinci cümlesindeki, kendilerinden talepte bulunulan kurum ve kuruluşların, kendi mevzuatlarındaki hükümleri gerekçe göstermek suretiyle talebin yerine getirilmesinden kaçınamayacaklarına ilişkin düzenleme, bentteki kuralın uygulama kapsamını genişleterek kişileri, kendileri veya yakınları aleyhine suçlayıcı nitelikte delil göstermeye veya meslekleri nedeniyle öğrendikleri ve kişilerin savunma hakkına ilişkin sırları içeren bilgi, belge, veri ve kayıtları vermeye zorlamakta ve böylece anılan anayasal kural ve güvencelerle bağdaşmayacak sonuçların ortaya çıkmasına neden olabilecek bir nitelik taşımaktadır.

15. Mevzuatımızda sır saklama yükümlülüğüne, bir kimsenin kendisini ve yakınlarını suçlayıcı nitelikte beyanda bulunmama hakkı kapsamında düzenlemelere yer verilmiştir. Sözgelimi 1136 sayılı Avukatlık Kanunu'nun "Sır saklama" başlıklı 36. maddesinde, avukatlara meslekleri nedeniyle

öğrendikleri savunmaya ilişkin bilgilerin mahremiyetini koruma ödevi verilmiştir. Basın Kanunu'nun "Haber kaynağı" başlıklı 12. maddesinde süreli yayın sahibinin, sorumlu müdürün ve eser sahibinin, bilgi ve belge dahil her türlü haber kaynaklarını açıklamaya ve bu konuda tanıklık yapmaya zorlanamayacağı belirtilmiştir. Aynı şekilde, 5271 sayılı Ceza Muhakemesi Usulü Kanunu'nun 45. maddesinde, kişilerin kendilerini ve yakınlarını suçlayan beyanda bulunmaya zorlanamayacağını öngören düzenlemeler bulunmaktadır. Dava konusu bendin ikinci cümlesindeki kuralla bu bilgileri vermekle yükümlü kuruluşların anılan mevzuatı mazeret göstererek söz konusu bilgileri vermektan kaçınamayacaklarının aksi takdirde hürriyeti bağlayıcı ceza ile cezalandırılacaklarının düzenlenmesi, kişileri anılan nitelikteki (savunmaya ve kişilerin kendilerini ve yakınlarını suçlayıcı nitelikteki) bilgi ve belgeleri de vermeye zorlayabilecek nitelikte olup, bunun anılan haklara ölçsüz bir müdahaleye neden olacağı açıktır.

16. Kanun'da kişilerin sır saklama, savunma ve kişilerin kendilerini veya yakınlarını suçlayan beyanda bulunmaya zorlanamama gibi anayasal hakları kapsamında kalan bilgilerin sadece istihbari amaçla kullanılıp başka bir amaçla kullanılmayacağına ilişkin bir güvenceye de yer verilmiş değildir.

17. Bu ilkelere göre itiraz konusu kurala bakıldığında, itiraz konusu düzenlemenin de içerisinde bulunduğu (b) bendi ile MİT'e verilen yetkinin kapsamı hem muhatap kurumlar, hem de üzerinde yetki kullanılacak alan bakımından alabildiğince geniş kapsamlıdır. Buna göre, MİT'e muhatap kurumlar; kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, 5411 sayılı Bankacılık Kanunu kapsamındaki kurum ve kuruluşlar ile diğer tüzel kişiler ve tüzel kişiliği bulunmayan kuruluşlardan oluşmaktadır. Bu belirlemeye göre tüm kurum ve kuruluşlar kapsamda bulunmaktadır. Düzenlemeye göre, MİT bu kuruluşlardan bilgi, belge, veri ve kayıtları alabilecek, bunlara ait arşivlerden, elektronik bilgi merkezlerinden ve iletişim altyapılarından yararlanabilecek ve bunlarla irtibat kurabilecektir.

18. Milli güvenlik gerekçeleriyle MİT'in erişimine açılan bu alanda kişilerin temel hak ve hürriyetlerini, anayasal haklarını, kişisel verilerini doğrudan ilgilendiren birçok husus bulunduğu kuşku yoktur. Güvenlik amacıyla bireylerin temel hak ve hürriyetlerine müdahalenin sözkonusu olduğu hallerde kamu makamlarına yetki verilirken temel hak ve hürriyetlerin yeterince korunmasına özen gösterilmesi hukuk devleti olmanın bir gereğidir. Aksi takdirde anayasal güvencelerin bir anlamı kalmaz. MİT'e bu şekilde milli güvenlik amacıyla geniş bir yetki verilecekse, yapılan görevle doğrudan bağlantılı, talebin amacıyla sınırlı ve zorunlu hallerde bu yetkinin kullanılabilmesinin de öngörülmesi, bu sınırların korunmasını sağlayacak ve amaç dışı kullanımına engel olacak tedbirlerin alınması gerekir.

19. Ancak, iptali istenilen kuralda MİT'e kişilerin anayasal hakları, temel hak ve özgürlükleri ve bu kapsamda olmak üzere kişisel verileriyle ilgili çok geniş bir alanda verilen erişim, işleme, paylaşma, kullanma yetki ve sınırları ile bu verilerin korunmasına ilişkin usul ve esaslara yer verilmemiştir. Bu anlamda kişisel veri niteliğindeki bilgi ve belgeleri, arşiv ve kayıtları ve elektronik bilgi merkezleri ile iletişim altyapılarını amaç, kapsam, kullanım ve işleme yetkileri açısından gereksiz, ölçüsüz ve belirsiz biçimde MİT'in erişimine açan kural Anayasa'nın 2., 13., 20., 28. ve 38. maddelerine aykırıdır.

2- 6. Maddesine Eklenen Onbirinci Fıkra da Yer Alan ".yukarıdaki hükümlere ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın; MİT Müsteşarı veya yardımcısının onayıyla." İbaresinin Fıkra da Yer Alan ".yurt dışında veya yabancılar tarafından gerçekleştirilen iletişim ile ankesörlü telefonlarla gerçekleştirilen iletişim." İbaresinin Yönünden

20. 2937 sayılı Kanun'un 6. maddesinin iptali istenen ibareleri de içeren onbirinci fıkrası ile MİT'e "önleyici istihbarat elde etmek ve analiz yapabilmek" amacıyla hâkim kararı olmaksızın iletişimi tespit etme yetkisi verilmektedir.

21. Kişilerin iletişiminin tespit edilmesine ilişkin genel düzenlemeler 5271 sayılı Ceza Muhakemesi Kanunu'nda yer almaktadır. Buna göre, CMK'nın 135. maddesi uyarınca, bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve iletişimin tespiti dışında başka suretle delil elde etme imkânının bulunmaması halinde ağır ceza mahkemesi veya gecikmesinde sakınca bulunan hâllerde derhal mahkemeye sunulmak üzere Cumhuriyet savcısının kararı ile şüpheli veya sanığın telekomünikasyon yoluyla iletişimi dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir. Bu tedbire ancak ağır ceza mahkemesinin oybirliğiyle karar verilebilecektir. Ayrıca maddede bu tedbire başvurulacak durumlar, süresi, şekli ve uygulanması ile ilgili olarak çok ayrıntılı düzenlemelere yer verilmiş, ayrıca, CMK'nın 135. maddesinin (8) numaralı fıkrasında, "Bu maddede belirlenen esas ve usuller dışında hiç kimse, bir başkasının telekomünikasyon yoluyla iletişimini dinleyemez ve kayda alamaz." kuralına da yer verilmek suretiyle, genel hüküm niteliğinde olmak üzere CMK'daki koşullar olmaksızın herhangi bir kimsenin telekomünikasyon yoluyla iletişiminin dinlenilmesi yasaklanmıştır.

22. Ancak, 3.7.2005 günlü, 5397 sayılı Kanun'un 1., 2. ve 3. maddeleriyle 2559 sayılı Polis Vazife ve Selahiyet Kanunu'nun Ek 7. maddesine, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanununun Ek 5. maddesine ve 2937 sayılı Kanun'un 6. maddesine eklenen fıkralar ve ek maddeyle CMK'nın 135. maddesinde belirtilen bu hükümlere istisnalar getirilerek anılan kurumların görevleri kapsamındaki faaliyetlerle ilgili olmak üzere iletişimin tespitine yönelik düzenlemeler yapılmıştır.

23. 5397 sayılı Kanunla, 1.11.1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu'nun 6. maddesinde yapılan değişikliğin gerekçesinde şu açıklamalara yer verilmiştir;

"Avrupa Birliği (AB) müktesebatı; siyasi kriterler, adalet hizmetleri, iç ve dış güvenlik olmak üzere üç temel sütundan oluşmaktadır. Üçüncü sütunda yer alan "iç ve dış güvenliğin korunması", devletin istihbarat hizmetlerinin düzenlenmesini gerekli kılmaktadır. Günümüzde, toplum ve devlete gelecek olan tehlikelerin önceden sezilmesi ve bunların önlenmesi için tedbir alınması, demokratik hukuk devletinin korunması açısından, kaçınılmaz bir zorunluluk olmuştur.

Anayasanın koruma altına aldığı özel hayat ve haberleşme özgürlüğüne, devlet tarafından, suç öncesi yapılacak olan müdahalelerin, AB standartlarına uygun olarak bir kanunla yapılması ve sınırlama sebeplerinin bu kanunda gösterilmesi gerekmektedir.

3.10.2001 tarihli ve 4709 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinin Değiştirilmesi Hakkında Kanun ile, Anayasanın özel hayat, konut dokunulmazlığı ve haberleşme hürriyetine ilişkin 20, 21 ve 22 nci maddeleri yeniden düzenlenmiştir. Bu alanlara Devletin müdahale edebilmesi için; milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmalı, yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de, kanunla yetkili kılınmış merciin yazılı emri bulunmalıdır. Bunlar bulunmadıkça, kişinin özel hayatına dokunulamaz, konutuna girilemez, haberleşmesi engellenemez ve gizliliğine dokunulamaz. Anayasanın 22 nci maddesi, haberleşme hürriyeti açısından istisnalar olabileceğini kabul etmiş ve bunun kanunla belirlenmesini öngörmüştür.

Suç ve suçluluk ile mücadelede istihbarat vazgeçilmez bir araçtır. İstihbarat çalışmaları ise, bilgi toplamak ve depolamak şeklinde olduğundan, özel hayat ve aile hayatı ile yakından ilgilidir. Elektronik yoldan yapılan iletişimin suç öncesi alanda dinlenmesi ise, haberleşme hürriyeti ile ilgilidir. Anayasanın bu düzenlemesi karşısında, Türkiye'de istihbarat hizmetlerinin yapılabilmesi için, kanunla düzenleme yapılması ihtiyacı bir zorunluluk oluşturmaktadır.

Ülkemizde önleyici amaçlı istihbarat dinlemesi düzenlenmediğinden, hazırlanan Teklif ile, bu önemli eksiklik giderilecektir. İletişimin her ne sebeple olursa olsun dinlenmesi, Anayasamızın 20 ve Avrupa İnsan Hakları Sözleşmesinin 8 inci maddeleri ile garanti altına alınmış bulunan "özel hayatın gizliliği ve aile hayatına saygı gösterilmesini isteme hakkına" uygun olarak yapılacaktır".

24. Görüldüğü üzere, kanun koyucu gerek suçların takibi ve suçluların tespiti ve gerekse önleyici amaçlı istihbarat dinlemesi bakımından hakim güvencesinin Anayasa'daki özel hayatın gizliliği ve aile hayatına saygı gösterilmesini isteme hakkına ilişkin 20. maddenin bir gereği olduğunu kabul etmiştir. Nitekim sözkonusu gerekçelerle Anayasa'nın 20. maddesi de dikkate alınarak 2937 sayılı Kanun'un 6. maddesinin ikinci fıkrasında yapılan düzenleme şöyledir;

"Bu Kanunun 4 üncü maddesinde sayılan görevlerin yerine getirilmesi amacıyla Anayasanın 2 nci maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde Devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, Devlet sırrının ifşasının tespiti ve terörist faaliyetlerin önlenmesine ilişkin olarak, hâkim kararı veya gecikmesinde sakınca bulunan hallerde MİT Müsteşarı veya yardımcısının yazılı emriyle telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir. Gecikmesinde sakınca bulunan hallerde verilen yazılı emir, yirmidört saat içinde yetkili ve görevli hâkimin onayına sunulur. Hâkim, kararını en geç yirmidört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde tedbir derhal kaldırılır. Bu halde dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir."

25. Bu düzenlemeye göre 5397 sayılı Kanun'la değişen 2937 sayılı Kanun'un 4. maddesinde sayılan görevlerin yerine getirilmesini sağlamak amacıyla, Anayasanın 2. maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde Devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, Devlet sırrının ifşasının tespiti ve terörist faaliyetlerin önlenmesine ilişkin olarak, hâkim kararı veya gecikmesinde sakınca bulunan hallerde MİT Müsteşarı veya yardımcısının yazılı emriyle telekomünikasyon yoluyla yapılan iletişim tespit edilebilecektir.

26. Fakat gecikmesinde sakınca bulunan hallerde MİT Müsteşarı veya yardımcısının yazılı emriyle verilen yazılı emir, yirmidört saat içinde yetkili ve görevli hâkimin onayına sunulacak, yirmidört saatlik sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde tedbir derhal kaldırılacak ve bu halde dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilip durum bir tutanakla tespit edilecektir.

27. Uygulanan tedbirin sona ermesi halinde, dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilecek; durum bir tutanakla tespit edilecek ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilecektir.

28. Anılan fıkra hükümlerine göre yürütülen faaliyetler çerçevesinde elde edilen kayıtlar, 2937 sayılı Kanun'da belirtilen amaçlar dışında, yani istihbari amaçlar dışında kullanılamayacak ve elde edilen bilgi ve kayıtların saklanması ve korunmasında gizlilik ilkesi geçerli olacaktır.

29. Ayrıca, anılan (Kanun'un 6. maddesinde belirtilen) usul ve esaslara aykırı dinlemeler, hukuken geçerli sayılmayacak ve bu şekilde dinleme yapanlar hakkında 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu hükümlerine göre işlem yapılacaktır.

30. 2559 sayılı Polis Vazife ve Selahiyet Kanunu'nun Ek 7. Maddesi ile 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun Ek 5. Maddesinde de iletişimin tespiti için aynı yöntem benimsenmiş bulunmaktadır. Buna göre, mevzuatımızda telekomünikasyon aracılığıyla kişilerin iletişiminin tespit edilebilmesi için ya CMK'nın 135. maddesinde belirtilen şartların yahut 2559 ile 2803 sayılı Kanun'da ve 2937 sayılı Kanun'unun 6. maddesinin iki ila onbirinci fıkralarında belirtilen şartların gerçekleşmesi gerekmektedir.

31. İptali istenen ibarelerin de bulunduğu kuralla ise bu hükümlerden farklı bir istisna getirilmekte ve CMK'nın 135., 2559 sayılı Kanun'un Ek. 7., 2803 sayılı Kanun Ek 5. maddelerinde belirtilen şartlar yahut 2937 sayılı Kanun'unun 6. maddesinin iki ila onbirinci fıkralarında belirtilen şartlar gerçekleşmese de kişilerin iletişiminin tespitine imkan sağlayan yeni bir düzenlemeye yer verilmektedir.

32. Buna göre, MİT, önleyici istihbarat elde etmek ve analiz yapabilmek amacıyla yukarıda belirtilen şartlara ve düzenlemelere (özellikle de CMK'nın 135. maddesi ve 2937 sayılı Kanun'unun 6. maddesinin iki ila onbirinci fıkrası arasındaki düzenlemelere) bağlı kalmaksızın, MİT Müsteşarı veya yardımcısının onayıyla yurt dışında gerçekleştirilen, yabancılar tarafından gerçekleştirilen, ankesörlü telefonlarla gerçekleştirilen, MİT mensupları, MİT'te görev almış olanlar veya görev almak üzere başvuranlarca gerçekleştirilen iletişimlerin tespit edilebilecek, dinlenebilecek, sinyal bilgileri değerlendirilebilecek ve kayda alınabilecektir.

33. Görüldüğü üzere, iletişimin tespiti yönünden dava konusu kuralla getirilen düzenlemenin, daha önce var olan iki ayrı düzenlemelerden (CMK 135. ve 2937 s.K'nun 6. maddesinin ikinci ve onbirinci fıkraları arasındaki düzenleme) şu iki temel farkı bulunmaktadır:

1. Diğer iki düzenleme uyarınca, iletişimin tespit edilebilmesi için kural olarak "hâkim kararı" aranmaktayken, dava konusu düzenlemede "MİT Müsteşarı veya yardımcısının onayı" yeterli görülmekte,

2. İletişimin tespitine karar verilebilmesi için;

a. CMK'nın 135. maddesindeki düzenleme uyarınca, "suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı",

b. 2937 sayılı Kanun'un 6. maddesinin ikinci fıkrasındaki düzenleme uyarınca "Anayasanın 2. maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı",

şartları aranmaktayken, dava konusu kuralda, yalnızca "önleyici istihbarat elde etmek ve analiz yapabilmek amacıyla" iletişimin tespitine imkan sağlanmaktadır.

34. Yani, değişiklikten önce iletişimin tespit edilebilmesi için CMK'nın 135. maddesindeki düzenleme uyarınca bir suç işlenmesi ve iletişimi tespit edilecek kişinin bu suçu işlediğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ya da 2937 sayılı Kanun gereği bir suç işlenmemiş olsa bile Anayasa'nın 2. maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı ve her iki düzenlemede de gecikmesinde sakınca bulunan hallerde yetkili merciin yazılı emriyle olsa bile sonuçta hâkim kararı aranmaktayken, dava konusu kurala ilişkin düzenlemede bu koşullar oluşmaksızın da önleyici istihbarat elde etmek ve analiz yapabilmek amacıyla ve hâkim kararı yerine MİT Müsteşarı veya yardımcısının onayıyla iletişimin tespit edilmesine imkân tanınmaktadır.

35. Kanun'un dava konusu ibareyi de içeren onbirinci fıkrasında, önleyici istihbarat elde etmek ve analiz yapabilmek amacıyla Kanun'un 6. maddesinin iki ila onbirinci fıkralarındaki ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın; MİT Müsteşarı veya yardımcısının onayıyla MİT mensuplarının, MİT'te görev almış olanların veya görev almak üzere başvuranların iletişiminin tespit edilebileceği, dinlenebileceği, sinyal bilgilerinin değerlendirilebileceği ve kayda alınabileceği düzenlenmektedir.

36. Anayasa'nın 2. maddesinde yer alan hukuk devletinin temel ilkelerinden biri 'belirlilik ilkesi'dir. Bu ilkeye göre, yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olması ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi gerekir.

37. Öte yandan, özel hayatın ve haberleşmenin gizliliğinin sınırlandırılmasında ilgili Anayasa maddelerinde belirtilen sebeplerin varlığı yanında temel hak ve özgürlüklerin sınırlandırılması rejimini belirleyen Anayasa'nın 13. maddesine de uyulması gerekmektedir. Anayasa'nın 13. maddesi uyarınca özel hayatın ve haberleşmenin gizliliği hakları, yalnızca kanunla ve demokratik bir toplumda gerekli olduğu ölçüde sınırlandırılabilir. Ayrıca getirilen bu sınırlamalar, hakkın özüne

dokunamayacağı gibi Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamaz.

38. Anayasal açıdan dokunulamayacak öz, her temel hak ve özgürlük açısından farklılık göstermekle birlikte kanunla getirilen sınırlamanın hakkın özüne dokunmadığının kabulü için temel hakların kullanılmasını ciddi surette güçleştirip, amacına ulaşmasına engel olmaması ve etkisini ortadan kaldıracı bir nitelik taşımaması gerekir. Ancak bu durumda sınırlamanın demokratik toplum düzeninin gereklerine uygun olduğu söylenebilir.

39. Ölçülülük ise amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder. Ölçülülük, aynı zamanda yasal önlemin sınırlama amacına ulaşmaya elverişli olmasını, amaç ve aracın ölçülü bir oranı kapsamasını ve sınırlayıcı önlemin demokratik toplum düzeni bakımından zorunluluk taşımasını da içeren bir ilkedir (Anayasa Mahkemesinin 26.12.2013 günlü, E. 2013/67, K. 2013/164 sayılı kararı).

40. Anayasa'nın 22. maddesinin ikinci fıkrasında, maddede belirtilen sebeplere bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşmenin gizliliğine dokunulamayacağı, müdahalenin yetkili merciin kararı ile yapılması halinde ise bunun yirmidört saat içinde görevli hâkimin onayına sunulması gerektiği belirtilerek hâkim kararı olmaksızın haberleşme hürriyetinin gizliliğine dokunulamayacağı anayasal güvenceye bağlanmıştır.

41. Maddenin üçüncü fıkrasında ise "İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir." denilerek bu kuralın da mutlak olmadığı ve bu kurala da bazı kurumlar yönünden sınırlamalar getirilebileceği belirtilmiştir.

42. Ancak bu istisna, aktif bir süje olarak haberleşme hürriyetini hâkim kararı olmaksızın sınırlayabilecek kurumlar yönünden değil, pasif bir nesne olarak hürriyeti sınırlanabilecek kurumlar yönünden tanınmıştır. Bir başka ifadeyle, bu istisna ile herhangi bir kuruma başkalarının iletişimine hâkim kararı olmaksızın müdahale etme yetkisi verilmemekte, cezaevleri gibi özel niteliği bulunan bazı kurumlarda hâkim kararı olmaksızın iletişime müdahale edilmesi yetkisi verilebileceği düzenlenmektedir.

43. Nitekim madde gerekçesinde, "Maddeye 'İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir.' fıkrası eklenmiştir. Böylece haberleşme hürriyetinin ve gizliliğinin istisnai olarak kısıtlanabileceği kamu kurum ve kuruluşlarının kanunla belirleneceği öngörülmüştür." denilmek suretiyle bu husus açıkça vurgulanmıştır.

44. Buna göre, anılan istisna uyarınca hâkim kararı olmaksızın bazı kurumlarda haberleşme hürriyetine ve gizliliğine sınırlamalar getirilmesi mümkünse de herhangi bir kurum veya kuruluşun hâkim kararı olmaksızın veya sonradan hâkim onayına sunulmak üzere yetkili merciin emri olmaksızın başkalarının haberleşme hürriyetine ve gizliliğine müdahale etmesi mümkün değildir.

45. İptali istenen kuralla MİT'e, "önleyici istihbarat elde etmek ve analiz yapabilmek" gibi tamamen belirsiz ve geniş bir alanda ve Kanunun bu konuda sınırları ortaya koyan nitelikteki düzenlemelerine ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın iletişimin dinlenmesi yetkisi verilmiştir. Anayasa'nın özel hayatın gizliliği ve haberleşme özgürlüğüyle ilgili 20. ve 22. maddelerinde bu hak ve özgürlüklerin ancak "millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak" usulüne göre verilmiş hâkim kararı ya da yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınmış merciin yazılı emri ile sınırlamaya cevaz verirken, iptali istenen düzenlemede öngörülen sınırlama nedeni Anayasadaki sınırlama nedenlerinden milli güvenlik ve kamu düzeni ile ilgili olmakla birlikte bunları aşan "önleyici istihbarat elde etmek ve analiz yapabilmek" gibi tamamen belirsiz ve geniş bir alana ilişkin bir nedenle hakim güvencesi de olmaksızın iletişimin tespitine imkan vermektedir.

46. Ayrıca, dava konusu ibareyle hiçbir sınırlama ve ayırım ölçütü kullanılmaksızın yurt içindeki tüm yabancıların iletişimi ile yurtdışındaki herkesin iletişiminin, bu çerçevede örneğin yurt dışına seyahat etmek üzere çıkan vatandaşların iletişiminin tespit edilmesine, dinlenebilmesine, kayda alınmasına ve iletişim sinyal bilgilerinin değerlendirilmesine izin verilmesi, sınırlandırma aracı ile sınırlandırma amacı arasında bulunması gereken makul dengeyi ortadan kaldırmakta ve Anayasa'nın 20. ve 22. maddesiyle güvence altına alınan özel hayatın ve haberleşmenin gizliliği haklarının ölçsüz şekilde sınırlandırılmasına neden olmaktadır.

47. Açıklanan nedenlerle iptali istenen ibarelerle oluşan düzenleme Anayasa'nın 2., 13., 20. ve 22. maddelerine aykırıdır. İptali gerekir.

3- Kanun'un 6. Maddesiyle 2937 Sayılı Kanun'un 26. Maddesine Eklenen İkinci Fıkranın İkinci Cümlesi

48. 2937 sayılı Kanun'un 26. maddesinde, MİT mensuplarına ilişkin özel soruşturma ve kovuşturma usulleri düzenlenmektedir.

49. Bu değişiklikten önce de mevcut olan, maddenin birinci fıkrası uyarınca, MİT mensuplarının veya belirli bir görevi ifa etmek üzere kamu görevlileri arasından Başbakan tarafından görevlendirilenlerin

görevlerini yerine getirirken, görevin niteliğinden doğan veya görevin ifası sırasında işledikleri iddia olunan suçlardan dolayı haklarında soruşturma yapılması Başbakanın iznine bırakılmıştır. Buna göre, Başbakanın izni olmaksızın herhangi bir MİT görevlisi hakkında işlediği görev suçuyla ilgili bir soruşturma başlatılması veya yürütülmesi mümkün bulunmamaktadır. İptali istenen Kanunla bu düzenlemeden sonra gelmek üzere eklenen fıkrada dava konusu cümleyi de içeren şu kurala yer verilmiştir;

"Cumhuriyet savcıları, MİT görev ve faaliyetleri ile mensuplarına ilişkin herhangi bir ihbar veya şikâyet aldıklarında veya böyle bir durumu öğrendiklerinde MİT Müsteşarlığına bildirirler. MİT Müsteşarlığının, konunun görev ve faaliyetlerine ilişkin olduğunu belirtmesi veya belgelendirmesi hâlinde adli yönden başkaca bir işlem yapılmaz ve herhangi bir koruma tedbiri uygulanmaz. Ancak birinci fıkra hükümlerine göre işlem yapılabilir."

50. Fıkra ile "MİT görev ve faaliyetleri ile mensuplarına ilişkin" tüm soruşturma işlemleri bakımından "MİT Müsteşarlığının, konunun görev ve faaliyetlerine ilişkin olduğunu belirtmesi veya belgelendirmesi hâlinde" mutlak bir koruma sistemi öngörmekte, bu durumda kurum ve mensupları hakkında adli yönden koruma tedbirleri de dahil olmak üzere herhangi bir işlem yapılması yasaklanmaktadır. Böylece suçların takibi, soruşturma ve kovuşturma işlemleri bakımından adli mercilerin yetkileri ortadan kaldırılarak inisiyatif tamamen MİT'e verilmektedir.

51. Fıkroda geçen "ile mensuplarına" ibaresinin kendinden önce gelen "MİT görev ve faaliyetleri" ibarelerine ve birinci fıkraya izafeten kullanıldığı, dolayısıyla bu ibarenin kendinden önce gelen ibarelerden ve fıkradan bağımsız/ilgisiz olamayacağı ve kendisinden önce gelen ibare ve fıkrayla birlikte değerlendirildiğinde, ibarenin "ile mensuplarının görev ve faaliyetleri" anlamında kullanıldığının tespiti hâlinde, kuralın sadece görev suçlarına ilişkin bir izin sistemini içerdiği söylenebilirse de, düzenlemede buna ilişkin bir belirginlik sözkonusu olmadığı gibi görev suçları yönünden zaten bir önceki fıkrada düzenleme olması nedeniyle kuralla örtülü olarak kişisel suçları da kapsayan bir izin sisteminin öngörüldüğü sonucuna ulaşılmaktadır.

52. Kural gereğince Cumhuriyet savcıları, MİT görev ve faaliyetleri ile mensuplarının görev ve faaliyetlerine ilişkin herhangi bir ihbar veya şikâyet aldıklarında veya böyle bir durumu öğrendiklerinde MİT Müsteşarlığına bildirimde bulunacaklar ve bu bildirim üzerine, MİT Müsteşarlığının, konunun görev ve faaliyetlerine ilişkin olduğunu belirtmesi veya belgelendirmesi hâlinde adli yönden başkaca bir işlem yapamayacak ve herhangi bir koruma tedbiri uygulayamayacaklardır. Ancak bu durumda da maddenin ilk fıkrasında belirtilen kural gereği görev

suçu olduğu anlaşılan eylemin soruşturulabilmesi için Başbakan'dan izin alarak soruşturma yapabileceklerdir.

53. Görüldüğü üzere, dava konusu kuralın da bulunduğu fıkrayla, MİT mensuplarının görev suçlarına ilişkin maddenin birinci fıkrasında düzenlenen soruşturma usulünde herhangi bir değişiklik yapılmamaktadır. Soruşturma izni, bir ceza muhakemesi müessesesi olup kural olarak bu izin alınmadan herhangi bir soruşturma işleminin yapılması mümkün bulunmamaktadır. Nitekim bu hususları tüm memurlar ve kamu görevlileri yönünden genel olarak düzenleyen 2.12.1999 günlü, 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun'un 4. maddesinin birinci fıkrasında, "Cumhuriyet başsavcılarını, memurlar ve diğer kamu görevlilerinin bu Kanun kapsamına giren suçlarına ilişkin herhangi bir ihbar veya şikâyet aldıklarında veya böyle bir durumu öğrendiklerinde ivedilikle toplanması gerekli ve kaybolma ihtimali bulunan delilleri tespitinden başka hiçbir işlem yapmayarak ve hakkında ihbar veya şikâyet bulunan memur veya diğer kamu görevlisinin ifadesine başvurmaksızın evrakın bir örneğini ilgili makama göndererek soruşturma izni isterler." denilmek suretiyle bu husus açıkça ortaya konulmuştur.

54. Belirtilen açıklamalar karşısında dava konusu kuralın yer aldığı fıkra hiç düzenlenmemiş olsaydı bile maddenin birinci fıkrasının amir hükmü gereği, MİT mensuplarının görev suçlarıyla ilgili soruşturma izni alınmadan bunlar hakkında adli bir işlem yapılması veya bir koruma tedbirinin uygulanması zaten mümkün bulunmaktaydı. Dolayısıyla bu kuralın yalnızca görev suçlarını kapsayacak şekilde anlaşılması halinde birinci fıkrada düzenlenen durumun farklı şekilde ifade edilmesine neden ihtiyaç duyulduğu sorusu açıkta kalacaktır. Bu nedenle burada amacın, birinci fıkradaki korumanın hem suçlar hem de korumaya alınan kişiler açısından genişletilmesi olduğu anlaşılmaktadır. Bir an için fıkrada düzenlenen durumun görev suçlarına ilişkin olduğu düşünülse bile burada kişisel suç-görev suçu ayrımının yapılmasında dahi inisiyatif tamamen MİT'e bırakılmış bulunmaktadır.

55. 5271 sayılı CMK'nın 160. ve devamı maddelerine bakıldığında bir eylemin kamu davası açılmasını gerektirecek nitelikte bir suça vücut verip vermediği ve suçun nitelendirmesini yapma, bu yönüyle suçun görev suçu olup olmadığını belirleme yetkisinin Cumhuriyet savcısına bırakıldığı görülmektedir.

56. İptali istenen kural gereğince, bir suç şüphesi durumunda Cumhuriyet savcısının, suçun MİT mensuplarının görev ve faaliyetlerine ilişkin olup olmadığına bakmaksızın bir başka ifadeyle kişisel suçlar yönünden de eylemin MİT'in görevi kapsamında kalıp kalmadığını MİT Müsteşarlığına sorması ve eğer yanıt olumlu olursa hiçbir adli işlem yapmaksızın tıpkı görev suçlarında olduğu gibi

soruşturma izni istemesi gerekmektedir. Yani bu durumda, Cumhuriyet Savcısı yargı yetkisini kullanabilip kullanamayacağını MİT'e sorarak öğrenecek, MİT'in cevaz vermesi halinde ve verdiği kapsamda bu yetkisini kullanabilecektir. Bu durum, Kanun'un bir başka hukuki müessese için kabul ettiği bir usulün, öngörülmeven başka bir alanda kullanılabilmesine neden olabilecektir ki, bu durumun keyfiliğe neden olması ihtimali karşısında Devletin her türlü işlem ve eyleminin hukuka uygun olması gerektiği yönündeki hukuk devleti anlayışıyla bağdaştırılması olanaksızdır.

57. Anayasa'nın 2. maddesinde Türkiye Cumhuriyeti bir hukuk devleti olarak nitelendirilmiş ve 125. maddesinin birinci fıkrasında "İdarenin her türlü eylem ve işlemlerine karşı yargı yolu açıktır." denilerek, idarenin tüm işlem ve eylemlerinin yargı denetimine tabi olacağı ilkesi kural olarak benimsenmiştir.

58. Çağdaş hukuk sistemlerinde, ceza yargılaması alanında, yaş, görev, ünvan gibi kişilerin belli vasıfları dikkate alınarak genel soruşturma ve kovuşturma usullerinden ayrılan özel soruşturma ve kovuşturma usullerine yer verilebilmekte, bu çerçevede kamu görevlileri yönünden genel yetki kurallarından ayrılarak ve çeşitli kriterler baz alınarak "kişi bakımından yetki kuralları" belirlenebilmektedir. Anayasa koyucu ve kanun koyucu, uluslararası hukuk ve iç hukuktan kaynaklanan kimi nedenlere dayanarak bu genel kurallara istisnalar getirmiştir. Buna göre, suç işleyen her kişi hakkında uygulanması gereken genel düzenlemeleri içeren 5271 sayılı Kanun hükümleri bazı suç failleri bakımından uygulanmayacak, bunlar hakkında ilgili kanunlarındaki özel soruşturma ve kovuşturma usulleri geçerli olacaktır. Bu usullerin tanınması, uygulanacak kişilere bir zümre ya da sınıf olarak imtiyaz tanımak anlamına gelmeyip, yapılan görevin niteliğinden kaynaklanmaktadır. Böylece, hem yapılan görevin en iyi şekilde ve etkin olarak yerine getirilmesi sağlanacak hem de gereksiz şikâyetlere maruz kalınarak görülen hizmetin kesintiye uğraması engellenecektir. (Anayasa Mahkemesinin 17.1.2013 günlü, E. 2012/19, K.2013/17 sayılı kararı).

59. Nitekim Anayasa'nın 128. maddesinin son fıkrasında "Memurlar ve diğer kamu görevlileri hakkında işledikleri iddia edilen suçlardan ötürü ceza kovuşturması açılması, kanunla belirlenen istisnalar dışında, kanunun gösterdiği idarî merciin iznine bağlıdır." denilmek suretiyle kamu görevlileri yönünden özel soruşturma usullerinin uygulanması anayasal güvenceye kavuşturulmuştur.

60. İptali istenen kuralda da anılan çerçevede milli güvenlik yönünden önemli görevler yürüten MİT mensuplarının yürüttükleri görevin niteliği nedeniyle özel bir soruşturma usulüne tabi kılınmak istendiği anlaşılmaktadır. Kanun koyucunun, izlediği ceza politikası uyarınca kanunlarla belirlenen görevlerini en iyi şekilde ve etkin olarak yerine getirmesini sağlamak ve gereksiz şikâyetlere maruz

kalınarak görülen hizmetin kesintiye uğramasını önlemek üzere MİT mensupları yönünden farklı bir soruşturma usulü benimsemesinin takdir yetkisi kapsamında olduğu açıktır.

61. Ancak yapılan düzenlemeye bakıldığında, kural gereği Cumhuriyet savcısı, MİT mensuplarının sadece görev ve faaliyetlerine ilişkin eylemlerine değil, suç konusu olabilecek herhangi bir eylemine bu arada şahsi suçlarına konu olabilecek eylemlerine ilişkin bir ihbar veya şikâyet aldığında veya böyle bir durumu öğrendiğinde de bunların MİT'in görev ve faaliyetleri kapsamında kalıp kalmadığını MİT Müsteşarlığına soracak ve eylemin görev kapsamında kaldığının belirtilmesi durumunda, eylemin şahsi suç kapsamında kaldığını tespit etmiş olsa bile hiçbir adli işlem yapamayacaktır. Yalnızca, görev suçları için öngörülen prosedürü işleterek eylemin soruşturulabilmesi için Başbakan'dan veya Müsteşar'dan soruşturma izni isteyebilecektir. Bu prosedür uygulanmadan önce Cumhuriyet savcısının adli yönden hiçbir işlem yapamaması ve herhangi bir koruma tedbirinin uygulanamaması nedeniyle izin alınmış olsa dahi yürütülecek soruşturmanın sağlıklı ve etkili olabilmesi de mümkün değildir.

62. Yani bu halde, yasama dokunulmazlığına sahip bir milletvekili bile ağır ceza mahkemesinin görev alanına giren meşhud bir şahsi suç işlediğinde hakkında derhal soruşturma başlatılabilirken, bir MİT mensubu aynı suçu işlediğinde soruşturma başlatılamayacak, bu eylemin MİT'in görevi kapsamında kalıp kalmadığı sorulacak ve eğer MİT, eylemin görevi kapsamında kaldığını belirtirse hiçbir adli işlem yapılamayacak, sadece söz konusu eylem için soruşturma izni istenebilecektir.

63. Kuralla CMK'nın 160. ve devamı maddeleri uyarınca Cumhuriyet savcılarının, eylemin kamu davası açılmasını gerektirecek nitelikte bir suça vücut verip vermediğini ve suçun nitelendirmesini yapma, bu yönüyle suçun görev suçu olup olmadığını belirleme yetkisi, MİT mensupları yönünden ortadan kaldırılmakta ve bu yetki MİT Müsteşarlığına verilmektedir.

64. Bu durum karşısında dava konusu kuralla MİT mensuplarının her türlü eylemini değerlendirme, bu yönüyle bu eylemlerin görev suçu kapsamında kalıp kalmadığına karar verme yetkisinin yargı mercilerinden alınarak MİT'e verilmesi, MİT'e bazı şahsi suçları, görev suçu kapsamında değerlendirerek bunların özel bir soruşturma usulüne tabi kılınabilmesi imkânını tanımakta, bu yönüyle Kanun'un başka bir hukuki müessese için kabul ettiği usulün, öngörülme-yen bir alanda kullanılması keyfiliğine izin vermektedir. Kanun'un öngördüğü yeni usul, çok geniş bir alanla ilgili olarak suç teşkil edebilecek eylemlerin gerçekleşme şartlarının ve olası cezai sorumlulukların belirlenmesi imkânını ortadan kaldıracak bir nitelik taşımaktadır. Bu nitelikteki bir düzenlemeyi hakimlerin görevlerinde bağımsız olduklarını, Anayasa'ya, kanuna ve hukuka uygun olarak vicdani kanaatlerine göre hüküm vereceklerini, hiçbir organ, makam, merci veya kişinin yargı yetkisinin

kullanılmasında mahkemelere ve hakimlere emir ve talimat veremeyeceğini, genelge gönderemeyeceğini, tavsiye ve telkinde bulunamayacağını öngören Anayasa'nın 138. maddesi ile bağdaştırmak mümkün değildir.

65. Hukuk devletinde, Devletin her türlü işlem ve faaliyetinin hukuka uygun olması, kamu görevlilerinin hukuk dışına çıkan eylemlerinin etkili biçimde soruşturulması ve yargı bağımsızlığının en üst seviyede korunması gerekir. İptali istenen ibare bu niteliklere tamamen aykırı bir düzenleme içerdiğinden hukuk devleti ilkesiyle de bağdaşmamaktadır.

66. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2. ve 138. maddelerine aykırıdır.

4- Kanun'un 6. Maddesiyle 2937 Sayılı Kanun'un 26. Maddesine Eklenen Dördüncü Fıkrasının Birinci Cümlesi

67. 2937 sayılı Kanun'un 26. maddesinin dava konusu kuralı içeren dördüncü fıkrasının birinci cümlesinde, MİT Müsteşarına ilişkin olarak özel bir soruşturma usulü düzenlenmektedir.

68. Daha önce belirtildiği üzere 2937 sayılı Kanun'un 26. maddesinin birinci fıkrası uyarınca tüm MİT mensuplarının bu arada MİT Müsteşarının görevini yerine getirirken, görevin niteliğinden doğan veya görevin ifası sırasında işlediği iddia olunan suçlardan dolayı soruşturulabilmesi Başbakanın iznine bağlı bulunmaktadır.

69. Dava konusu kuralda, hem bu izin usulüne hem de izin verilmesi halinde yürütülecek soruşturmaya ilişkin olarak MİT Müsteşarı yönünden yeni kurallar belirlenmekte, böylece MİT Müsteşarı, diğer MİT mensuplarına göre ayrı bir soruşturma rejimine bağlanmaktadır. Bu çerçevede, kural uyarınca MİT Müsteşarı hakkındaki soruşturmalarda, 25.10.1963 günlü ve 353 sayılı Askeri Mahkemeler Kuruluşu ve Yargılama Usulü Kanunu'nun 15/A maddesinin üçüncü fıkrasının son iki cümlesi ile beş, altı ve yedinci fıkralarında yer alan usul ve hükümler uygulanacaktır.

70. Buna göre, MİT Müsteşarının görevini yerine getirirken, görevin niteliğinden doğan veya görevin ifası sırasında işlediği iddia olunan suçlar hakkındaki soruşturmalarda Başbakandan soruşturma izni istenecek, Başbakanın vereceği "izin verme veya vermeme" kararına karşı ilgililer on gün içinde Cumhurbaşkanlığına itiraz edebilecek ve itiraz sonucu Cumhurbaşkanının verdiği karar kesin olacaktır. Yani bu karara karşı yargı yolu kapalı olacaktır. MİT müsteşarı hakkında soruşturma izni verilmemesine ilişkin Cumhurbaşkanınca verilecek karar üzerine herhangi bir soruşturma açılması mümkün olmayacaktır.

71. Cumhurbaşkanının soruşturmaya izin yönünde karar vermesi veya Başbakanın soruşturma izni verilmesine ilişkin kararına süresinde itiraz edilmemesi hallerinde ise MİT müsteşarı hakkında

soruşturma aşamasına geçilecek, fakat bu soruşturmayı ilgili Cumhuriyet savcısı değil Başbakanın denetim elemanları arasından belirleyeceği üç kişilik soruşturma kurulu yapacaktır.

72. Soruşturma kurulu, bu soruşturmayı yürütürken 5271 sayılı Ceza Muhakemesi Kanunu'nun Cumhuriyet savcısına tanıdığı bütün yetkilere sahip olacak ve soruşturma sırasında hâkim kararı alınması gereken hususlarda yetkili mahkemelere başvurabilecektir. Kurul, yaptığı soruşturma sonucunu bir rapor ile tespit ederek Başbakana sunacak, Başbakan, kamu davasının açılmasına gerek görürse ilgili Yargıtay dairesinde dava açılacak, ancak gerek görmezse kovuşturma yapılmasına yer olmadığına karar verecek ve bu karar kesin olacaktır. Bir başka ifadeyle Başbakanın kovuşturma yapılmasına yer olmadığı yönündeki kararına karşı yargı yolu kapalı olacaktır. Görüldüğü üzere dava konusu kuralla sadece MİT Müsteşarının soruşturulmasına ilişkin izin prosedürünün nasıl işleyeceği düzenlenmemekte, aynı zamanda izin verilmesi halinde söz konusu soruşturmanın yapılmasına ilişkin olarak özellikle soruşturmayı yürütecek merci yönünden genel kurallardan ayrılan özel bir soruşturma usulü benimsenmektedir.

73. 6519 sayılı Kanun'un 61. maddesiyle 353 sayılı Kanun'a 15. maddesinden sonra gelmek üzere eklenen 15/A maddesi ile ilgili olarak Mahkememizce verilen 14.1.2015 günlü, E:2014/89 ve K:2015/3 sayılı kararda, iptali istenilen ibare ile itiraz makamı olarak Cumhurbaşkanlığı makamının belirlenmiş olması nedeniyle, hem suçtan zarar görenlerin hem de soruşturulacak kimselerin soruşturma izni verilmesi veya verilmemesi kararlarına karşı yargısal denetime başvurma imkânının ortadan kaldırılmış olduğu, bu haliyle Başbakanın ve İçişleri Bakanının anılan işlemlerinin yargı denetimi dışına çıkarılmasının, Anayasa'nın Cumhuriyetin nitelikleri arasında saydığı, kişi ya da kurumların yanı sıra idarenin ve yasama organının da anayasal ilkelerle bağlı olduğu anlamına gelen "hukuk devleti", "hak arama özgürlüğü" ve "idarenin işlemlerine karşı yargı yolunun açık olması" ilkelerine aykırılık oluşturacağı gerekçesiyle Anayasa'nın 2., 36., 105. ve 125. maddelerine aykırı olduğu ve fıkranın son cümlesi ile birlikte iptali gerektiği düşüncesiyle çoğunluk görüşüne katılmamıştık. İptali istenen düzenleme 353 sayılı Kanun'a 15. maddesinden sonra gelmek üzere eklenen 15/A maddesine yollama yaptığından anılan karşıoy gerekçeleri burada da geçerlidir.

74. Belirtilen gerekçelerle kuralın iptaline karar verilmesi gerektiğini düşündüğümüzden çoğunluğun aksi yöndeki kararına katılmadık.

75. Açıklanan nedenlerle, 17.4.2014 tarihli ve 6532 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun'un yukarıda belirtilen kuralları ile yapılan düzenlemelerin Anayasa'ya aykırı olduğu ve iptali gerektiği kanaatinde olduğumuzdan çoğunluğun aksi yöndeki kararına katılmıyoruz.

Üye - Alparslan ALTAN

Üye - Erdal TERCAN

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2014/87

Karar Sayısı: 2015/112

Karar Tarihi: 8.12.2015

R.G. Tarih-Sayı: 28.01.2016 - 29607

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri M. Akif HAMZAÇEBİ, Engin ALTAY ve Muharrem İNCE ile birlikte 121 milletvekili

İPTAL DAVASININ KONUSU: 6.2.2014 tarihli ve 6518 sayılı Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un;

A- 8. maddesiyle değiştirilen, 4.1.1961 tarihli ve 213 sayılı Vergi Usul Kanunu'nun mükerrer 257. maddesinin birinci fıkrasının (6) numaralı bendinin ".mükelleflerin Maliye Bakanlığına bağlı vergi dairelerine vadesi geçmiş borcu bulunmadığına ilişkin belge arama zorunluluğu getirmeye, bu zorunluluk kapsamına girecek amme alacaklarını tür ve tutar itibarıyla tespit etmeye ve hangi hâllerde bu zorunluluğun aranılmayacağına,." bölümünün,

B- 47. maddesiyle değiştirilen, 4.1.2002 tarihli ve 4734 sayılı Kamu İhale Kanunu'nun 38. maddesinin;

1- İkinci fıkrasında yer alan "...gibi hususlarda..." ibaresinin,

2- Üçüncü fıkrasının birinci cümlesinde yer alan ".açıklama istenilmeksizin sonuçlandırılabilmesine." ve ".açıklama istenilmeksizin reddedilmesine ilişkin." ibarelerinin,

C- 48. maddesiyle 4734 sayılı Kanun'un 43. maddesine eklenen fıkrada yer alan ".yaklaşık maliyetin ." ve ".az ve %15'inden." ibarelerinin,

D- 80. maddesiyle 16.5.2006 tarihli ve 5502 sayılı Sosyal Güvenlik Kurumu Kanunu'nun 30. maddesine eklenen fıkranın,

E- 85. maddesiyle 4.5.2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 2. maddesinin (1) numaralı fıkrasına eklenen (n) ve (r) bentlerinin ve (o) bendinde yer alan "...ve benzeri yöntemler kullanılarak..." ibaresinin,

- F- 86. maddesiyle 5651 sayılı Kanun'un 3. maddesine eklenen (3) numaralı fıkranın,
- G- 87. maddesiyle 5651 sayılı Kanun'un 4. maddesine eklenen (3) numaralı fıkranın,
- H- 88. maddesiyle 5651 sayılı Kanun'un 5. maddesine eklenen (3), (4), (5) ve (6) numaralı fıkraların,
- I- 89. maddesiyle 5651 sayılı Kanun'un 6. maddesinin (1) numaralı fıkrasına eklenen (ç) ve (d) bentlerinin,
- İ- 90. maddesiyle 5651 sayılı Kanun'a eklenen 6/A maddesinin,
- J- 91. maddesiyle 5651 sayılı Kanun'un 7. maddesinin;
- 1- Değiştirilen (2) ve (3) numaralı fıkralarının,
- 2- Eklenen (4) numaralı fıkrasının,
- K- 93. maddesiyle 5651 sayılı Kanun'un değiştirilen 9. maddesinin (5), (8) ve (9) numaralı fıkralarının,
- L- 94. maddesiyle 5651 sayılı Kanun'a eklenen 9/A maddesinin (1), (2), (3), (4), (5), (6), (7) ve (8) numaralı fıkralarının,
- M- 97. maddesiyle 5651 sayılı Kanun'un ek 1. maddesine eklenen (5) numaralı fıkranın birinci cümlesinde yer alan "...hâkim ve savcılar ise kendilerinin..." ibaresinin,
- N- 100. maddesiyle 5651 sayılı Kanun'a eklenen geçici 3. maddenin,
- Anayasa'nın Başlangıç kısmı ile 2., 5., 7., 10., 13., 20., 22., 26., 28., 33., 36., 38., 40., 48., 51., 70., 123., 138., 140. ve 167. maddelerine aykırılığı ileri sürülerek iptallerine ve yürürlüklerinin durdurulmasına karar verilmesi talebidir.

1- İPTALİ İSTENİLEN KANUN HÜKÜMLERİ

İptali istenilen kuralların yer aldığı 6518 sayılı Kanun'un;

1- 8. maddesiyle 213 sayılı Kanun'un mükerrer 257. maddesinin birinci fıkrasının değiştirilen (6) numaralı bendi şöyledir:

"Mükerrer Madde 257- (Değişik birinci fıkra: 22/7/1998 - 4369/5 md.) Maliye Bakanlığı;

(...)

6. (Ek: 3/7/2005 - 5398/23 md.; Değişik: 6/2/2014 - 6518/8 md.) Vergi güvenliğini sağlamak amacıyla niteliklerini belirleyip onayladığı elektrikli, elektronik, manyetik ve benzeri cihazlar ve sistemleri kullandırmaya, bu cihaz ve sistemler vasıtasıyla bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretlerin kullanılmasına ilişkin zorunluluk getirmeye, mükelleflere

bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretlerin verilmesinde, mükelleflerin Maliye Bakanlığına bağlı vergi dairelerine vadesi geçmiş borcu bulunmadığına ilişkin belge arama zorunluluğu getirmeye, bu zorunluluk kapsamına girecek amme alacaklarını tür ve tutar itibarıyla tespit etmeye ve hangi hâllerde bu zorunluluğun aranılmayacağına, bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretlerin basımı, dağıtımı ile sistemin kurulması ve işletilmesi hizmetlerinin, 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununa tabi olmaksızın, süresi 5 yılı geçmemek üzere ve 4/1/2002 tarihli ve 4734 sayılı Kamu İhale Kanunu (5 inci maddesinin beşinci fıkrası hariç) hükümleri çerçevesinde; yetkilendirilecek gerçek veya tüzel kişiler tarafından yerine getirilmesine, bu hizmetlerde ve yetkilendirilecek gerçek veya tüzel kişilerde bulunması gereken özellikleri, yetkilendirilecek gerçek veya tüzel kişilerin faaliyetlerinin yönlendirilmesi, izlenmesi, denetlenmesi, yetkilendirmenin sonlandırılması ve bunların uygulanmasına ilişkin usul ve esasları belirlemeye,

(...)

Yetkilidir."

2- 47. maddesiyle 4734 sayılı Kanun'un değiştirilen 38. maddesi şöyledir:

"Aşırı düşük teklifler

Madde 38- İhale komisyonu verilen teklifleri (.) değerlendirdikten sonra, diğer tekliflere veya idarenin tespit ettiği yaklaşık maliyete göre teklif fiyatı aşırı düşük olanları tespit eder. Bu teklifleri reddetmeden önce, belirlediği süre içinde teklif sahiplerinden teklifte önemli olduğunu tespit ettiği bileşenler ile ilgili ayrıntıları yazılı olarak ister.

İhale komisyonu;

- a) İmalat sürecinin, verilen hizmetin ve yapım yönteminin ekonomik olması,
- b) Seçilen teknik çözümler ve teklif sahibinin mal ve hizmetlerin temini veya yapım işinin yerine getirilmesinde kullanacağı avantajlı koşullar,
- c) Teklif edilen mal, hizmet veya yapım işinin özgünlüğü,

gibi hususlarda yapılan yazılı açıklamaları dikkate alarak, aşırı düşük teklifleri değerlendirir. Bu değerlendirme sonucunda, açıklamaları yeterli görülmeyen veya yazılı açıklamada bulunmayan isteklilerin teklifleri reddedilir.

(Ek fıkra: 20/11/2008-5812/12 md.; Değişik üçüncü fıkra: 6/2/2014-6518/47 md.) Kurum, ihale konusu işin türü, niteliği ve yaklaşık maliyeti ile ihale edilme usulüne göre aşırı düşük tekliflerin tespiti,

değerlendirilmesi ve ekonomik açıdan en avantajlı teklifin belirlenmesi amacıyla sınır değerler ve sorgulama kriterleri belirlemeye, ihalenin bu maddede öngörülen açıklama istenilmeksizin sonuçlandırılabilmesine, ayrıca yaklaşık maliyeti 8 inci maddede öngörülen eşik değerlerin yarısına kadar olan hizmet alımları ile yapım işleri ihalelerinde sınır değer altında olan tekliflerin bu maddede öngörülen açıklama istenilmeksizin reddedilmesine ilişkin düzenlemeler yapmaya yetkilidir. İhale komisyonu bu maddenin uygulanmasında Kurum tarafından yapılan düzenlemeleri esas alır."

3- 48. maddesiyle 4734 sayılı Kanun'un 43. maddesine eklenen üçüncü fıkra şöyledir:

"Kurum, ihale üzerinde kalan isteklinin teklifinin sınır değer altında olması hâlinde, bu istekliden yaklaşık maliyetin % 6'sından az ve % 15'inden fazla olmamak üzere alınacak kesin teminat oranına ilişkin düzenlemeler yapabilir."

4- 80. maddesiyle 5502 sayılı Kanun'un 30. maddesine eklenen fıkra şöyledir:

"Başkanlık merkez teşkilatında genel müdür yardımcısı, daire başkanı veya taşra teşkilatında il müdürü kadrolarında toplam en az üç yıl görev yapmış olanlar, atama tarihi itibarıyla fiilen bu kadrolardan birinde bulunmak şartıyla Sosyal Güvenlik Uzmanı kadrosuna atanabilir."

5- 85. maddesiyle 5651 sayılı Kanun'un 2. maddesine eklenen (n), (o) ve (r) bentleri şöyledir:

" MADDE 2- (1) Bu Kanunun uygulamasında;

(...)

n) Birlik: Erişim Sağlayıcıları Birliğini,

o) Erişimin engellenmesi: Alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi ve benzeri yöntemler kullanılarak erişimin engellenmesini,

r) Uyarı yöntemi: İnternet ortamında yapılan yayın içeriği nedeniyle haklarının ihlal edildiğini iddia eden kişiler tarafından içeriğin yayından çıkarılması amacıyla öncelikle içerik sağlayıcısına, makul sürede sonuç alınamaması hâlinde yer sağlayıcısına iletişim adresleri üzerinden gerçekleştirilecek bildirim yöntemini,

(...)

ifade eder."

6- 86. maddesiyle 5651 sayılı Kanun'un 3. maddesine eklenen (3) numaralı fıkra şöyledir:

"(3) Bu Kanun kapsamındaki faaliyetleri yurt içinden ya da yurt dışından yürütenlere, internet sayfalarındaki iletişim araçları, alan adı, IP adresi ve benzeri kaynaklarla elde edilen bilgiler üzerinden elektronik posta veya diğer iletişim araçları ile bildirim yapılabilir."

7- 87. maddesiyle 5651 sayılı Kanun'un 4. maddesine eklenen (3) numaralı fıkra şöyledir:

"(3) İçerik sağlayıcı, Başkanlığın bu Kanun ve diğer kanunlarla verilen görevlerinin ifası kapsamında; talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim eder ve Başkanlıkça bildirilen tedbirleri alır."

8- 88. maddesiyle 5651 sayılı Kanun'un 5. maddesine eklenen (3), (4), (5) ve (6) numaralı fıkralar şöyledir:

"(3) Yer sağlayıcı, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür.

(4) Yer sağlayıcılar, yönetmelikle belirlenecek usul ve esaslar çerçevesinde yaptıkları işin niteliğine göre sınıflandırılabilir ve hak ve yükümlülükleri itibarıyla farklılaştırılabilirler.

(5) Yer sağlayıcı, Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla yükümlüdür.

(6) Yer sağlayıcılık bildiriminde bulunmayan veya bu Kanundaki yükümlülüklerini yerine getirmeyen yer sağlayıcı hakkında Başkanlık tarafından on bin Türk Lirasından yüz bin Türk Lirasına kadar idari para cezası verilir."

9- 89. maddesiyle (1) numaralı fıkrasına (ç) ve (d) bentleri eklenen 5651 sayılı Kanun'un 6. maddesi şöyledir:

"Erişim sağlayıcının yükümlülükleri

MADDE 6- (1) Erişim sağlayıcı;

a) Herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, bu Kanun hükümlerine uygun olarak haberdar edilmesi halinde (.) erişimi engellemekle,

b) Sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla,

c) Faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma, içerik sağlayıcılarına ve müşterilerine bildirmek ve trafik bilgilerine ilişkin kayıtları yönetmelikte belirtilen esas ve usûllere uygun olarak Kuruma teslim etmekle,

ç) Erişimi engelleme kararı verilen yayınlarla ilgili olarak alternatif erişim yollarını engelleyici tedbirleri almakla,

d) Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla,

yükümlüdür.

(2) Erişim sağlayıcı, kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü değildir.

(3) Birinci fıkranın (b), (c), (ç) ve (d) bentlerinde yer alan yükümlülüklerden birini yerine getirmeyen erişim sağlayıcısına Başkanlık tarafından onbin Yeni Türk Lirasından ellibin Yeni Türk Lirasına kadar idarî para cezası verilir."

10- 90. maddesiyle 5651 sayılı Kanun'a eklenen 6/A maddesi şöyledir:

"Erişim Sağlayıcıları Birliği

MADDE 6/A- (1) Bu Kanunun 8 inci maddesi kapsamı dışındaki erişimin engellenmesi kararlarının uygulanmasını sağlamak üzere Erişim Sağlayıcıları Birliği kurulmuştur.

(2) Birlik özel hukuk tüzel kişiliğini haizdir. Birliğin merkezi Ankara'dır.

(3) Birliğin çalışma usul ve esasları Kurum tarafından onaylanacak Tüzükle belirlenir. Tüzük değişiklikleri de Kurumun onayına tabidir.

(4) Birlik, Tüzüğünün Kurum tarafından incelenerek uygun bulunmasını müteakip faaliyete başlar.

(5) Birlik, 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu kapsamında yetkilendirilen tüm internet servis sağlayıcıları ile internet erişim hizmeti veren diğer işletmecilerin katılımıyla oluşan ve koordinasyonu sağlayan bir kuruluştur.

(6) Bu Kanunun 8 inci maddesi kapsamı dışındaki erişimin engellenmesi kararları erişim sağlayıcılar tarafından yerine getirilir. Kararların uygulanması amacıyla gerekli her türlü donanım ve yazılım erişim sağlayıcıların kendileri tarafından sağlanır.

(7) Bu Kanunun 8 inci maddesi kapsamı dışındaki erişimin engellenmesi kararları gereği için Birliğe gönderilir. Bu kapsamda Birliğe yapılan tebligat erişim sağlayıcılara yapılmış sayılır.

(8) Birlik, kendisine gönderilen mevzuata uygun olmadığını düşündüğü kararlara itiraz edebilir.

(9) Birliğin gelirleri, üyeleri tarafından ödenecek ücretlerden oluşur. Alınacak ücretler, Birliğin giderlerini karşılayacak miktarda belirlenir. Bir üyenin ödeyeceği ücret, üyelerin tamamının net satış tutarı toplamı içindeki o üyenin net satışı oranında belirlenir. Üyelerin ödeme dönemleri, yeni katılan üyelerin ne zamandan itibaren ödemeye başlayacağı ve ödemelere ilişkin diğer hususlar Birlik Tüzüğünde belirlenir. Süresinde ödenmeyen ücretler Birlikçe kanuni faizi ile birlikte tahsil edilir.

(10) Birliğe üye olmayan internet servis sağlayıcıları faaliyette bulunamaz."

11- 91. maddesiyle (2) ve (3) numaralı fıkraları değiştirilen ve (4) numaralı fıkra eklenen 5651 sayılı Kanun'un 7. maddesi şöyledir:

"Toplu kullanım sağlayıcıların yükümlülükleri

MADDE 7- (1) Ticarî amaçla toplu kullanım sağlayıcılar, mahallî mülkî amirden izin belgesi almakla yükümlüdür. İzne ilişkin bilgiler otuz gün içinde mahallî mülkî amir tarafından Kuruma bildirilir. Bunların denetimi mahallî mülkî amirler tarafından yapılır. İzin belgesinin verilmesine ve denetime ilişkin esas ve usûller, yönetmelikle düzenlenir.

(2) Ticari amaçla olup olmadığına bakılmaksızın bütün internet toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimin engellenmesi ve kullanıma ilişkin erişim kayıtlarının tutulması hususlarında yönetmelikle belirlenen tedbirleri almakla yükümlüdür.

(3) Ticari amaçla toplu kullanım sağlayıcılar, ailenin ve çocukların korunması, suçun önlenmesi ve suçluların tespiti kapsamında usul ve esasları yönetmelikte belirlenen tedbirleri almakla yükümlüdür.

(4) Bu maddede belirtilen yükümlülükleri ihlal eden ticari amaçla toplu kullanım sağlayıcılarına, ihlalin ağırlığına göre yönetmelikle belirlenecek usul ve esaslar çerçevesinde uyarma, bin Türk Lirasından on beş bin Türk Lirasına kadar idari para cezası verme veya üç güne kadar ticari faaliyetlerini durdurma müeyyidelerinden birine karar vermeye mahalli mülki amir yetkilidir."

12- 93. maddesiyle değiştirilen, 5651 sayılı Kanun'un 9. maddesi şöyledir:

"İçeriğin yayından çıkarılması ve erişimin engellenmesi

MADDE 9-

(1) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer

sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğe erişimin engellenmesini de isteyebilir.

(2) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişilerin talepleri, içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılır.

(3) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talepleri doğrultusunda hâkim bu maddede belirtilen kapsamda erişimin engellenmesine karar verebilir.

(4) Hâkim, bu madde kapsamında vereceği erişimin engellenmesi kararlarını esas olarak, yalnızca kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verir. Zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemez. Ancak, hâkim URL adresi belirtilerek içeriğe erişimin engellenmesi yöntemiyle ihlalin engellenemeyeceğine kanaat getirmesi hâlinde, gerekçesini de belirtmek kaydıyla, internet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilir.

(5) Hâkimin bu madde kapsamında verdiği erişimin engellenmesi kararları doğrudan Birliğe gönderilir.

(6) Hâkim bu madde kapsamında yapılan başvuruyu en geç yirmi dört saat içinde duruşma yapmaksızın karara bağlar. Bu karara karşı 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir.

(7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır. (8) Birlik tarafından erişim sağlayıcıya gönderilen içeriğe erişimin engellenmesi kararının gereği derhâl, en geç dört saat içinde erişim sağlayıcı tarafından yerine getirilir.

(8) Birlik tarafından erişim sağlayıcıya gönderilen içeriğe erişimin engellenmesi kararının gereği derhâl, en geç dört saat içinde erişim sağlayıcı tarafından yerine getirilir.

(9) Bu madde kapsamında hâkimin verdiği erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının veya aynı mahiyetteki yayınların başka internet adreslerinde de yayımlanması durumunda ilgili kişi tarafından Birliğe müracaat edilmesi hâlinde mevcut karar bu adresler için de uygulanır.

(10) Sulh ceza hâkiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişi, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır."

13- 94. maddesiyle 5651 sayılı Kanun'a eklenen 9/A maddesi şöyledir:

"Özel hayatın gizliliği nedeniyle içeriğe erişimin engellenmesi

MADDE 9/A- (1) İnternet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, Başkanlığa doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilir.

(2) Yapılan bu istekte; hakkın ihlaline neden olan yayının tam adresi (URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilere yer verilir. Bu bilgilerde eksiklik olması hâlinde talep işleme konulmaz.

(3) Başkanlık, kendisine gelen bu talebi uygulanmak üzere derhâl Birliğe bildirir, erişim sağlayıcılar bu tedbir talebini derhâl, en geç dört saat içinde yerine getirir.

(4) Erişimin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanır.

(5) Erişimin engellenmesini talep eden kişiler, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebini talepte bulunduğu saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunar. Hâkim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklar ve doğrudan Başkanlığa gönderir; aksi hâlde, erişimin engellenmesi tedbiri kendiliğinden kalkar.

(6) Hâkim tarafından verilen bu karara karşı Başkanlık tarafından 5271 sayılı Kanun hükümlerine göre itiraz yoluna gidilebilir.

(7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

(8) Özel hayatın gizliliğinin ihlaline bağlı olarak gecikmesinde sakınca bulunan hâllerde doğrudan Başkanın emri üzerine erişimin engellenmesi Başkanlık tarafından yapılır. (Mülga cümle: 26/2/2014-6527/18 md.)

(9) (Ek: 26/2/2014-6527/18 md.) Bu maddenin sekizinci fıkrası kapsamında Başkan tarafından verilen erişimin engellenmesi kararı, Başkanlık tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar."

14- 97. maddesiyle 5651 sayılı Kanun'un ek 1. maddesine eklenen (5) numaralı fıkra şöyledir:

"(5) 8/6/1984 tarihli ve 217 sayılı Devlet Personel Başkanlığı Kuruluş ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 2 nci maddesinde sayılan kamu kurum ve kuruluşlarında çalışanlar kurumlarının, hâkim ve savcılar ise kendilerinin muvafakati ile aylık, ödenek, her türlü zam ve tazminatlar ile diğer mali ve sosyal hak ve yardımları kurumlarınca ödenmek kaydıyla geçici olarak Telekomünikasyon İletişim Başkanlığı emrinde görevlendirilebilir. Bu kapsamda görevlendirilen personel sayısı Kurumun kadro sayısının yüzde yirmisini geçemez. Bu personel kurumlarından izinli sayılır. İzinli oldukları sürece memuriyetleri ile ilgili özlük hakları devam eder ve bu süreler terfi ve emekliliklerinde hesaba katılır. Terfileri başkaca bir işleme gerek kalmaksızın süresinde yapılır."

15- 100. maddesiyle 5651 sayılı Kanun'a eklenen geçici 3. madde şöyledir:

"GEÇİCİ MADDE 3 -

- (1) Birliğin kuruluşu bu Kanunun yayımı tarihinden itibaren üç ay içinde tamamlanır.
- (2) Birlik, mevcut internet servis sağlayıcıları ile erişim hizmeti veren işletmecilerin en az dörtte birinin katılımıyla imzalanan Birlik Tüzüğü'nün Kurum tarafından incelenerek uygun bulunmasını müteakip faaliyete başlar. Birliğin kurulmasını müteakip en geç bir ay içinde hâlen üye olmayan internet servis sağlayıcıları ve erişim hizmeti veren işletmeciler üyeliklerini tamamlamak zorundadır.
- (3) Belirtilen sürede Birliğin kuruluşunu tamamlayamaması hâlinde, Kurum tarafından internet servis sağlayıcılarına ve internet erişim hizmeti veren diğer işletmecilere bir önceki takvim yılındaki net satışlarının yüzde biri oranında idari para cezası uygulanır.
- (4) Birliğin kurulmasını müteakip bir ay içinde üye olmayan internet servis sağlayıcılarına veya internet erişim hizmeti veren diğer işletmecilere, Kurum tarafından bir önceki takvim yılındaki net satışlarının yüzde biri oranında idari para cezası uygulanır."

II- İLK İNCELEME

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Serruh KALELİ, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ, Burhan ÜSTÜN, Engin YILDIRIM, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Erdal TERCAN, Muammer TOPAL, Zühtü ARSLAN, M. Emin KUZ ve Hasan Tahsin GÖKCAN'ın katılımlarıyla 14.5.2014 tarihinde yapılan ilk inceleme toplantısında, dosyada eksiklik bulunmadığından işin esasının incelenmesine, yürürlüğü durdurma talebinin ise esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

III- ESASIN İNCELENMESİ

2. Dava dilekçesi ile ekleri, Başraportör Ayşegül ATALAY tarafından hazırlanan işin esasına ilişkin rapor, iptali istenilen kanun hükümleri, dayanılan ve ilgili görülen Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 43. maddesinin (1) numaralı fıkrası uyarınca Ulaştırma, Denizcilik ve Haberleşme Bakanı Binali YILDIRIM, Bilgi Teknolojileri ve İletişim Kurumu (BTK) Başkanı Dr. Ömer Fatih SAYAN, Telekomünikasyon İletişim Başkanı Ahmet Cemalettin ÇELİK, Daire Başkanı Ahmet KILIÇ, Daire Başkanı Ali ERDEM, Bilişim Danışmanı Sinan ÜLKER, Erişim Sağlayıcıları Birliği Genel Sekreteri Doç. Dr. Bülent KENT, Erişim Sağlayıcıları Birliği Hukuktan Sorumlu Genel Sekreter Yardımcısı Av. Yadigar Seda UYSAL, Serbest Telekomünikasyon İşletmecileri Derneği Başkanı Yusuf Ata ARIAK, Serbest Telekomünikasyon İşletmecileri Derneği Hukuk Danışmanı Av. Gökhan CANDOĞAN'ın 8.12.2015 tarihli sözlü açıklamaları dinlendikten sonragereği görüşülüp düşünüldü:

A- Kanun'un 8. Maddesiyle Değiştirilen, 213 Sayılı Vergi Usul Kanunu'nun mükerrer 257. Maddesinin Birinci Fıkrasının (6) Numaralı Bendinin ".mükelleflerin Maliye Bakanlığına bağlı vergi dairelerine vadesi geçmiş borcu bulunmadığına ilişkin belge arama zorunluluğu getirmeye, bu zorunluluk kapsamına girecek amme alacaklarını tür ve tutar itibarıyla tespit etmeye ve hangi hâllerde bu zorunluluğun aranılmayacağına, ." Bölümünün İncelenmesi

1- ".mükelleflerin Maliye Bakanlığına bağlı vergi dairelerine vadesi geçmiş borcu bulunmadığına ilişkin belge arama zorunluluğu getirmeye,..." Bölümü

a- İptal Talebinin Gerekçesi

3. Dava dilekçesinde özetle, iptali istenilen kural uyarınca mükelleflerin ticari faaliyette bulunabilmeleri veya faaliyetlerini sürdürebilmeleri için alınması zorunlu olan bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretlerin mükelleflere verilmesinin vergi dairelerine vadesi geçmiş vergi borcu bulunmadığına ilişkin belge koşuluna bağlanmasının, vergi ödeme gücüne ulaşma amacı için elverişli ve gerekli olmadığı, mükelleflerin bu şekilde ticari faaliyette bulunmalarının engellenmesinin adil ve hakkaniyete uygun olmadığı gibi orantılılık ilkesi ile de bağdaşmadığı, vadesi geçmiş vergi borcunun tahsilatı için mükelleflerin ticari faaliyette bulunmalarını engelleyecek düzenlemeler yoluyla piyasadan çekilmeye zorlanmalarının Devlete verilen görevlerle uyum sağlamadığı, bu durumun vadesi geçmiş vergi borcunun tahsilatının hiç sağlanamaması riskini de taşıdığı, iptali istenilen bölümün adalet, hakkaniyet ve kamu yararı ölçütlerine uymadığı, çalışma ve sözleşme hürriyetini demokratik toplum düzeninin gereklerine ve

ölçülülük ilkesine aykırı olacak şekilde ortadan kaldırdığı belirtilerek kuralın, Anayasa'nın 2., 13. ve 48. maddelerine aykırı olduğu ileri sürülmüştür.

b- Anayasa'ya Aykırılık Sorunu

4. Kuralın birinci fıkrasının iptali istenilen bölümün de bulunduğu (6) numaralı bendinde, Maliye Bakanlığının, vergi güvenliğini sağlamak amacıyla niteliklerini belirleyip onayladığı elektrikli, elektronik, manyetik ve benzeri cihazlar ve sistemleri kullandırmaya, bu cihaz ve sistemler vasıtasıyla bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretlerin kullanılmasına ilişkin zorunluluk getirmeye, mükelleflere bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretlerin verilmesinde, mükelleflerin Maliye Bakanlığına bağlı vergi dairelerine vadesi geçmiş borcu bulunmadığına ilişkin belge arama zorunluluğu getirmeye yetkili olduğu belirtilmiştir.

5. Anayasa'nın 2. maddesinde belirtilen hukuk devleti, eylem ve işlemleri hukuka uygun, insan haklarına saygılı, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adaletli bir hukuk düzeni kurup bunu geliştirerek sürdüren, Anayasa'ya aykırı durum ve tutumlardan kaçınan, Anayasa ve hukukun üstün kurallarıyla kendini bağlı sayan, yargı denetimine açık olan devlettir.

6. Anayasa'nın 48. maddesinin birinci fıkrasında "Herkes, dilediği alanda çalışma ve sözleşme hürriyetlerine sahiptir. Özel teşebbüsler kurmak serbesttir." denilmiştir.

7. Anayasa'nın 48. maddesinde, çalışma ve sözleşme hürriyeti için herhangi bir sınırlama nedeni öngörülmemiştir. Anayasanın ilgili maddesinde özel bir sınırlama nedeni öngörülmemiş hakların da hakkın doğasından kaynaklanan bazı sınırlarının bulunduğu kabul edilmektedir. Öte yandan düzenlendiği maddede hiçbir sınırlama nedenine yer verilmeyen hakların diğer anayasal hükümler nedeniyle sınırlandırılması da mümkün bulunmaktadır.

8. Anayasa'nın 13. maddesinde, temel hak ve özgürlüklerin, özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği, bu sınırlamaların Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacağı belirtilmiştir.

9. Çağdaş demokrasiler, temel hak ve özgürlüklerin en geniş ölçüde sağlanıp güvence altına alındığı rejimlerdir. Temel hak ve özgürlükleri büyük ölçüde kısıtlayan ve kullanılamaz hâle getiren sınırlamalar hakkın özüne dokunur. Temel hak ve özgürlüklere getirilen sınırlamaların yalnız ölçüsü değil, koşulları, nedeni, yöntemi, kısıtlamaya karşı öngörülen kanun yolları gibi güvenceler demokratik toplum düzeni kavramı içinde değerlendirilmelidir. Bu nedenle, temel hak ve

özgürlükler, istisnaî olarak ve özüne dokunmamak koşuluyla demokratik toplum düzeninin gerekleri için zorunlu olduğu ölçüde ve ancak kanunla sınırlandırılabilirler.

10. Demokratik bir toplumda temel hak ve özgürlüklere getirilen sınırlamanın, bu sınırlamayla güdülen amacın gerektirdiğinden fazla olması düşünülemez. Demokratik hukuk devletinde güdülen amaç ne olursa olsun, kısıtlamaların, bu rejimlere özgü olmayan yöntemlerle yapılmaması ve belli bir özgürlüğün kullanılmasını önemli ölçüde zorlaştıracak ya da ortadan kaldıracak düzeye vardırılmaması gerekir.

11. 213 sayılı Kanun'un mükerrer 257. maddesinin birinci fıkrasının (6) numaralı bendinde, Maliye Bakanlığına, vergi güvenliğini sağlamak amacıyla niteliklerini belirleyip onayladığı elektrikli, elektronik, manyetik ve benzeri cihazlar ve sistemleri kullandırma, bu cihaz ve sistemler vasıtasıyla bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretlerin kullanılmasına ilişkin zorunluluk getirme, iptali istenilen kuralda ise mükelleflere bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel işaretlerin verilmesinde, mükelleflerin Maliye Bakanlığına bağlı vergi dairelerine vadesi geçmiş borçlarının bulunmadığına ilişkin belge arama zorunluluğu getirme yetkisi verilmektedir. Maliye Bakanlığına söz konusu yetkilerin verilmesi, mükelleflerin mali güçlerinin saptanmasını ve vergi yükünün adaletli ve dengeli dağılımını ve kamu borçlarının ödenmesini sağlamak için kamu yararı amacına yönelik olup, kanun koyucu bu konuda anayasal sınırlar içinde takdir yetkisini haizdir.

12. İptali istenilen kural ile Maliye Bakanlığına verilen yetki, çalışma özgürlüğünün güvence alanının kanun koyucu tarafından daraltılması niteliğinde olduğundan Anayasa'nın 13. maddesi anlamında bir sınırlandırma niteliğindedir. Bu sınırlama ticaret yapmak isteyen kişilerin vergi borcu dahil kamuya olan borçlarını ödemeye zorlayıcı nitelik taşıdığından anayasal açıdan meşru bir amaca dayanmaktadır. Ancak iptali istenilen kural ile getirilen sınırlamanın demokratik toplum düzeni için gerekli nitelikte, başka bir ifadeyle güdülen kamu yararı amacını gerçekleştirmekle birlikte, temel haklara en az müdahaleye olanak veren ölçülü bir sınırlama niteliğinde olup olmadığının incelenmesi gerekir.

13. Söz konusu sınırlamanın, amacı itibarıyla Anayasa'nın 73. maddesi uyarınca ödev olarak belirlenen vergi borcu ile diğer kamu borçlarının düzenli ve sürekli bir biçimde tahsilini, kamu alacağının güvence altına alınmasını ve tahsilatın hızlandırılmasını sağlamaya yönelik olduğu görülmektedir. Anayasa ve kanunlarla, kamu giderlerinin karşılanabilmesi için bir ödev olarak öngörülen vergi ödeme yükümlülüğünün, zamanında ve eksiksiz yerine getirilmesi durumunda, kanunlarla idareye yüklenen kamu hizmetlerinin, buna bağlı olarak kamu düzeninin ve başkalarının

hak ve özgürlüklerini korumanın aksatılmadan sürdürülmesi mümkün olacaktır. Dolayısıyla, demokratik toplum düzeni bakımından alınması gerekli tedbirler kapsamında olan, keyfi ya da hakkın özüne dokunacak bir sınırlama getirmeyen, temel hakkın kullanımını ortadan kaldırmayan iptali istenen kural, istisnai bir alanda ve dar kapsamlı olduğundan sınırlı ve ölçülüdür.

14. Açıklanan nedenlerle kural, Anayasa'nın 2., 13. ve 48. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

15. Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Alparslan ALTAN ve Erdal TERCAN bu görüşe katılmamışlardır.

2- ".bu zorunluluk kapsamına girecek amme alacaklarını tür ve tutar itibarıyla tespit etmeye ve hangi hâllerde bu zorunluluğun aranılmayacağına," Bölümü

a- İptal Talebinin Gerekçesi

16. Dava dilekçesinde özetle, Anayasa'nın 48. maddesinde koruma altına alınan çalışma hürriyeti kapsamında, mükelleflerin ticari faaliyette bulunabilmeleri veya faaliyetlerini sürdürebilmeleri için Maliye Bakanlığına verilen, vergi dairelerine vadesi geçmiş vergi borcu bulunmadığına ilişkin belge arama zorunluluğu getirme yetkisi bağlamında, bu zorunluluk kapsamına girecek vadesi geçmiş vergi borcunun ötesinde amme alacaklarının tür ve tutarlarının ve vadesi geçmiş vergi borcu belgesinin aranılmayacağı hallerin kanunla belirlenmesi yerine, tüm bu hususlarda düzenleme yapma ile usul ve esasları belirleme yetkisinin Maliye Bakanlığına bırakılmasının, yasama yetkisinin devri sonucunu doğurduğu ve idarenin kanuniliği ilkesi ile bağdaşmadığı belirtilerek iptali istenilen bölümün, Anayasa'nın 7. ve 123. maddelerine aykırı olduğu ileri sürülmüştür.

b- Anayasa'ya Aykırılık Sorunu

17. İptali istenilen hükmün de yer aldığı kuralda, Maliye Bakanlığının, mükelleflere bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretlerin verilmesinde, mükelleflerin Maliye Bakanlığına bağlı vergi dairelerine vadesi geçmiş borcu bulunmadığına ilişkin belge arama zorunluluğu getirmeye, bu zorunluluk kapsamına girecek amme alacaklarını tür ve tutar itibarıyla tespit etmeye ve hangi hâllerde bu zorunluluğun aranılmayacağına belirlenmesinde yetkili olduğu belirtilmiştir.

18. Anayasa'nın 7. maddesinde, yasama yetkisinin Türkiye Büyük Millet Meclisine ait olduğu ve bu yetkinin devredilemeyeceği öngörülmüştür. Buna göre, kanun ile düzenlenmesi öngörülen konularda, yürütme organına, genel, sınırsız, esasları ve çerçevesi belirsiz bir düzenleme yetkisi verilmesi, yasama yetkisinin devri anlamına geleceğinden Anayasa'nın 7. maddesine aykırı düşer.

Ancak, kanunda temel esasların ve çerçevenin belirlenmesi koşuluyla, uzmanlık ve teknik konulara ilişkin ayrıntıların düzenlenmesinin yürütmeye bırakılması Anayasa'ya aykırılık oluşturmaz. Esasen Anayasa'nın 8. maddesinde yer alan, "yürütme yetkisi ve görevi Anayasa'ya ve kanunlara uygun olarak kullanılır ve yerine getirilir" hükmünün anlamı da budur.

19. Kanun koyucu, vergi hukuku alanında yetkisini kullanırken, Anayasa'nın temel ilkelerine ve vergi ile ilgili kurallarına bağlı kalmak koşuluyla, kamu gelirlerinin doğru, etkin ve verimli biçimde nasıl ve hangi yöntemlerle sağlanacağı konusunda takdir yetkisine sahiptir.

20. İptali istenilen kuralda, ek bir vergi veya vergi benzeri mali yükümlülük getirilmediği gibi, Maliye Bakanlığına vergi ve mali yük konulması konusunda bir yetki de verilmemiştir. Kuralın, vergi yükümlülüğü ile ilgisi bulunmamaktadır. İptali istenilen kural ile Maliye Bakanlığına verilen yetki, mükelleflere bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretlerin verilmesinde, mükelleflerin Maliye Bakanlığına bağlı vergi dairelerine vadesi geçmiş borçlarının bulunmadığına ilişkin belge arama zorunluluğu getirilmesi ile ilgili olarak, bu kapsama girecek amme alacaklarını tür ve tutar itibarıyla tespit etmeye ve hangi hâllerde bu zorunluluğun aranılmayacağına ilişkindir.

21. İptali istenilen kuralda, kanun koyucu tarafından Maliye Bakanlığına bırakılan düzenleme alanı, vergilendirme ile ilgili temel kurallar olmayıp, kanunda belirlenen mükelleflerin Maliye Bakanlığına bağlı vergi dairelerine vadesi geçmiş borcu bulunmadığına ilişkin belge arama zorunluluğun uygulanmasına ilişkin teknik düzenlemeler ve ayrıntıları içermektedir. Bu bağlamda, kanunla düzenlenmesi gerekmeyen bir konu hakkında Maliye Bakanlığına yetki verilmesi yasama yetkisinin devri niteliğinde değildir.

22. Açıklanan nedenlerle kural, Anayasa'nın 7. maddesine aykırı değildir. İptal talebinin reddi gerekir.

23. Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Alparslan ALTAN ve Erdal TERCAN bu görüşe katılmamışlardır.

24. Kuralın Anayasa'nın 123. maddesiyle bir ilgisi görülmemiştir.

B- Kanun'un 47. Maddesiyle Değiştirilen, 4734 Sayılı Kamu İhale Kanunu'nun 38. Maddesinin İkinci Fıkrasında Yer Alan "...gibi hususlarda..." İbaresinin İncelenmesi

1- İptal Talebinin Gerekçesi

25. Dava dilekçesinde özetle, iptali istenilen ibareyle ihale komisyonlarına, komisyonların aşırı düşük teklif değerlendirilmesi sırasında, her ihaleye ve istekliye göre değişebilen, bu yönüyle de istekliler tarafından önceden bilinmeyen ve bilinmesi de mümkün olmayan ve dolayısıyla hukuki belirlilik ile ihalede saydamlık, rekabet ve eşit muamele ilkeleriyle bağdaşmayan kriterler belirleme, belirlediği kriterler temelinde aşırı düşük teklif değerlendirilmesi yapma ve belgelendirilmemiş cevaplara dayandırma yetkisi verilerek ihale komisyonlarının keyfi uygulamalarının önünün açıldığı, bu hukuksal belirsizlik içinde her ihaleye ve her istekliye göre değişebilen öngörülemez kriterler ile isteklilerin hukuksal güvenliklerinin ortadan kaldırıldığı, Devletin kamu ihaleleri bağlamında kendisine verilen görevleri yerine getirmesinin kamu ihalelerinde saydamlık, rekabet ve eşit muamele ilkelerini hayata geçirecek kurallar koymasından geçtiği, iptali istenilen ibarenin bu ilkelerle bağdaşmadığı belirtilerek kuralın, Anayasa'nın 2., 48. ve 167. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

26. Kanun'un 38. maddesinin birinci fıkrasında, ihale komisyonunun verilen teklifleri değerlendirdikten sonra, diğer tekliflere veya idarenin tespit ettiği yaklaşık maliyete göre teklif fiyatı aşırı düşük olanları tespit edeceği, bu teklifleri reddetmeden önce, belirlediği süre içinde teklif sahiplerinden teklifte önemli olduğunu tespit ettiği bileşenler ile ilgili ayrıntıları yazılı olarak isteyeceği belirtilmektedir. Maddenin, iptali istenilen ibarenin de bulunduğu ikinci fıkrasında ise ihale komisyonunun, aşırı düşük teklifleri, imalat sürecinin, verilen hizmetin ve yapım yönteminin ekonomik olması, seçilen teknik çözümler ve teklif sahibinin mal ve hizmetlerin temini veya yapım işinin yerine getirilmesinde kullanacağı avantajlı koşullar, teklif edilen mal, hizmet veya yapım işinin özgünlüğü gibi hususlarda yapılan yazılı açıklamaları dikkate alarak değerlendireceği, bu değerlendirme sonucunda açıklamaları yeterli görülmeyen veya yazılı açıklamada bulunmayan isteklilerin tekliflerinin reddedileceği öngörülmekte olup fıkrada yer alan "...gibi hususlarda..." ibaresi dava konusu kuralı oluşturmaktadır.

27. Anayasa'nın 2. maddesinde hukuk devleti ilkesi düzenlenmiştir. Kanunların kamu yararının sağlanması amacıyla yönelik olması, genel, objektif, adil kurallar içermesi ve hakkaniyet ölçütlerini gözetmesi hukuk devleti olmanın gereğidir. Bu nedenle, kanun koyucunun hukuki düzenlemelerde kendisine tanınan takdir yetkisini anayasal sınırlar içinde adalet, hakkaniyet ve kamu yararı ölçütlerini göz önünde tutarak kullanması gerekir.

28. Hukuki güvenlik ile belirlilik ilkeleri, hukuk devletinin önkoşullarındandır. Kişilerin hukuki güvenliğini sağlamayı amaçlayan hukuki güvenlik ilkesi, hukuk normlarının öngörülebilir olmasını,

bireylerin tüm eylem ve işlemlerinde Devlete güven duyabilmesini, Devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar. Belirlilik ilkesi ise yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olmasını, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesini ifade etmektedir.

29. Yasama yetkisinin genelliği ilkesi uyarınca, yasama organı, kanun yaparken bütün ihtimalleri göz önünde bulundurarak ayrıntılı hükümler koyabilir ya da Anayasa'nın kanunla düzenlenmesini zorunlu kıldığı hususlar dışında bir konuyu isterse soyut bir şekilde düzenleyerek genel ilkeleri ve çerçeveyi belirleyip ayrıntıları alt düzenleyici işlemlere bırakabilir. Bu husus kanun koyucunun takdir yetkisi içindedir.

30. Kanun'un 38. maddesinin birinci ve ikinci fıkrasında öngörülen düzenlemeler, ihale komisyonunun yetkilerine ilişkin hususlardır. İptali istenilen "...gibi hususlarda..." ibaresi ile ihale komisyonunun aşırı düşük teklifleri değerlendirirken bentlerde belirtilen sebepler dışında diğer nedenleri de tekliflerin aşırı düşük olması nedeni olarak açıklama kapsamında kabul edebilmesi imkânı getirilmiştir.

31. Aşırı düşük teklif tespit ve sorgulama süreci tüm çağdaş ihale sistemlerinde var olan, fiyat rekabeti ile kaynakların verimli kullanılması ve kamu tarafından yapılan ödemenin karşılığının alınması ilkelerini dengeleyen vazgeçilmez bir aşamayı ifade etmektedir.

32. Kanun'un 38. maddesinin birinci fıkrasında, ihale komisyonunun verilen teklifleri değerlendirdikten sonra aşırı düşük teklifleri diğer tekliflere veya yaklaşık maliyete göre tespit edeceği belirtilmiştir. Kamu kaynaklarının en iyi şekilde kullanılması anlayışı içerisinde tüm ihale kanunlarında en düşük fiyatın değil, işin yapılabilirlik değerine karşılık gelen fiyatın kabul edilmesi ilkesi benimsenmiştir. 4734 sayılı Kanunda bu ilke "ekonomik açıdan en avantajlı teklif" olarak adlandırılmıştır. Konuya ilişkin olarak, 4734 sayılı Kanun'un 40. maddesinde,"37 ve 38. maddelere göre yapılan değerlendirme sonucunda ihale, ekonomik açıdan en avantajlı teklifi veren istekli üzerinde bırakılır." hükmü yer almaktadır.

33. Ekonomik açıdan en avantajlı teklife ise Kanun'un 38. maddesinde hüküm altına alınan aşırı düşük tekliflerin tespit edilmesi ve sorgulanması işlemlerinden sonra ulaşılmakta, bir başka ifadeyle ekonomik açıdan en avantajlı teklif, verilen en düşük fiyat teklifini değil, aşırı düşük tekliflerden arındırılmış teklifler içerisindeki en düşük fiyat teklifini ifade etmektedir. Bu nedenle, aşırı düşük tekliflerin değerlendirilerek ekonomik açıdan en avantajlı teklifin belirlenmesi gerekmektedir. İptali istenilen ibarenin bulunduğu kuralda da, ihale komisyonunun aşırı düşük teklifleri değerlendirirken

bu teklifler nedeniyle sözleşmenin yürümesini sıkıntıya düşürmemek, verilen aşırı düşük tekliflerle işin yapılabilirliğini belirleyebilmek için dikkate alacağı hususlar belirtilmiştir. Ancak bu hususlar tahdidi olarak sayılmayıp, "...gibi hususlarda..." denilmek suretiyle işin özelliğinden kaynaklanan ve teklifte önemli olduğu tespit edilen, fakat kuralda belirtilmeyen hususlarda açıklama yapılmasının sağlanması amaçlanmıştır. Her şeyden önce sayma yönteminin tercih edilmesi durumunda, daima bazı hususların eksik kalma olasılığı söz konusu olacaktır. Özellikle yapılan işin özelliğine göre değişik bileşenlerin söz konusu olduğu ihale hukukunda bu hususları kanunda saymanın mümkün olmadığı açıktır.

34. Öte yandan, belirlilik ilkesi, yalnızca yasal belirliliği değil, daha geniş anlamda hukuki belirliliği ifade etmektedir. Erişilebilir, bilinebilir ve öngörülebilir gibi niteliksel gereklilikleri karşılama koşuluyla kanunlara dayanılarak çıkarılan yürütmenin düzenleyici işlemleri ile de hukuki belirlilik sağlanabilir. Hukuki belirlilik ilkesinde asıl olan, bir hukuk normunun uygulanmasıyla ortaya çıkacak sonuçların o hukuk düzeninde öngörülebilir olmasıdır.

35. İptali istenilen ibare, ihalelerde saydamlık, rekabet ve eşit muamele ilkelerini ortadan kaldırmayan, kuralda belirtilenlerin dışında yer alan aşırı düşük teklifleri değerlendirme kriterlerini ifade etmektedir. Bu çerçevede, İhale Komisyonunun aşırı düşük teklifleri incelerken hangi hususları değerlendirebileceği Kanun'da sayılmakla birlikte, sayılmayan hususlar açısından da, Kamu İhale Kanunu'nun 5. maddesinde idareler tarafından gözetilmesi gereken ihalelerde saydamlık, rekabet, eşit muamele, güvenilirlik, gizlilik, kamuoyu denetimi, ihtiyaçların uygun şartlarla karşılanması ve kaynakların verimli kullanılması gibi temel ilkeleri ve Kamu İhale Kurumu'nun bu konudaki düzenleyici işlemlerini göz önüne alacağı şüphesizdir. Bu nedenle, aynı konudaki farklı ihalelerde ihale komisyonlarının farklı değerlendirmelerde bulunma durumu da ortadan kalkmış olacaktır. Bu hususlar gözetildiğinde, iptali istenilen ibarenin belirsiz olduğundan söz edilemez.

36. Kaldı ki, idarelerce bu işlemlerin hem 4734 sayılı Kanun'a hem de Kurum tarafından yayınlanan yönetmelik, tebliğ, tip şartname, tip sözleşme ve düzenleyici kararlara uygun olarak yapılmaması halinde, Kanun'un 54., 55. ve 56. maddelerine göre ihale sürecindeki hukuka aykırı işlem veya eylemler nedeniyle bir hak kaybına veya zarara uğradığını veya zarara uğramasının muhtemel olduğunu iddia eden aday veya istekli ile istekli olabileceklerin, şikayet ve itirazın şikayet başvurusunda bulunabilecekleri belirtilmektedir. Şikayetler ile ilgili Kurum tarafından verilen nihai kararlar da Kanun'un 57. maddesi uyarınca yargı denetimine tâbi bulunmaktadır.

37. Açıklanan nedenlerle iptali istenilen ibare, Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

38. Kuralın Anayasa'nın 48. ve 167. maddeleriyle bir ilgisi görülmemiştir.

C- Kanun'un 47. Maddesiyle Değiştirilen, 4734 Sayılı Kanun'un 38. Maddesinin Üçüncü Fıkrasının Birinci Cümlesinde Yer Alan ".açıklama istenilmeksizin sonuçlandırılabilmesine." ve ".açıklama istenilmeksizin reddedilmesine ilişkin." İbarelerinin İncelenmesi

1- İptal Talebinin Gerekçesi

39. Dava dilekçesinde özetle, iptali istenilen ibareler ile Kamu İhale Kurumuna aşırı düşük teklifler ile ilgili olarak, isteklilerden yazılı açıklama istenilmeksizin ve dolayısıyla isteklilerin teknolojik farktan kaynaklanan maliyet avantajlarını belgeleriyle ortaya koymalarına imkân verilmeksizin sonuçlandırılabilmesine ve hatta reddedilmesine ilişkin düzenleme yapma yetkisinin verildiği, böylece teknolojik farktan kaynaklanabilecek maliyet farklılıklarının dışlanarak 4734 sayılı Kanun'un, ihtiyaçların uygun şartlarla ve zamanında karşılanması ile kaynakların verimli kullanılması ilkesi yanında, Devlete verilen anayasal görevlerle de bağdaşmayan ihale uygulamalarına yol açıldığı, iptali istenilen düzenlemenin maliyet avantajlı üretim teknikleriyle çalışan firmalara karşı negatif ayrımcılık yapılmasına sebep olduğu, adalet, hakkaniyet ve kamu yararı ölçütleri ile bağdaşmadığı, kamu alımları yoluyla piyasaya müdahale eden veya en azından piyasayı yönlendiren Devletin, maliyet avantajlı üretim teknikleriyle çalışan firmaları teşvik etmesi gerekirken, teknolojik farktan kaynaklanan aşırı düşük tekliflerin ihale dışında bırakılmasına ilişkin düzenlemeler yapılmasının önünün açılmasının, Devlete verilen görevlerle uyuşmadığı belirtilerek kuralın, Anayasa'nın 2., 48. ve 167. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

40. Kanun'un 38. maddesinin iptali istenilen ibarelerin de bulunduğu üçüncü fıkrasında, Kamu İhale Kurumunun, ihale konusu işin türü, niteliği ve yaklaşık maliyeti ile ihale edilme usulüne göre aşırı düşük tekliflerin tespiti, değerlendirilmesi ve ekonomik açıdan en avantajlı teklifin belirlenmesi amacıyla sınır değerler ve sorgulama kriterleri belirlemeye, ihalenin Kanun'un 38. maddesinde öngörülen açıklama istenilmeksizin sonuçlandırılabilmesine, ayrıca yaklaşık maliyeti 8. maddede öngörülen eşik değerlerin yarısına kadar olan hizmet alımları ile yapım işleri ihalelerinde sınır değer altında olan tekliflerin Kanun'un 38. maddesinde öngörülen açıklama istenilmeksizin reddedilmesine ilişkin düzenlemeler yapmaya yetkili olduğu, ihale komisyonunun bu maddenin uygulanmasında Kamu İhale Kurumu tarafından yapılan düzenlemeleri esas alacağı öngörülmektedir. Kuralda yer alan "...açıklama istenilmeksizin sonuçlandırılabilmesine..." ve "...açıklama istenilmeksizin reddedilmesine ilişkin..." ibareleri dava konusu kuralları oluşturmaktadır.

41. Anayasa'nın 2. maddesindeki "hukuk devleti" ilkesi gereğince, yasama işlemlerinin kişisel yararları değil kamu yararını gerçekleştirmek amacıyla yapılması zorunludur. Bir kuralın Anayasa'ya aykırılık sorunu çözümlenirken "kamu yararı" konusunda Anayasa Mahkemesinin yapacağı inceleme, kanunun kamu yararı amacıyla yapıp yapılmadığı ile sınırlıdır. Kanun ile kamu yararının gerçekleşip gerçekleşmeyeceğini denetlemenin anayasa yargısıyla bağdaşmayacağı, bunun kanun koyucunun takdirinde olduğu açıktır.

42. Kural ile Kamu İhale Kurumuna genel olarak, aşırı düşük tekliflerin tespiti, değerlendirilmesi ve ekonomik açıdan en avantajlı teklifin belirlenmesi amacıyla sınır değerler ve sorgulama kriterleri belirleme, aşırı düşük tekliflerin açıklama istenilmeksizin sonuçlandırılabilmesine, yaklaşık maliyeti 8. maddede öngörülen eşik değerlerin yarısına kadar olan hizmet alımları ile yapım işleri ihalelerinde sınır değer altındaki tekliflerin açıklama istenilmeksizin reddedilmesine ilişkin düzenlemeler yapma konusunda yetki verilmekte, ihale komisyonlarının da Kamu İhale Kurumu tarafından belirlenen düzenlemeleri esas alarak uygulama yapacağı belirtilmektedir.

43. 4734 sayılı Kanun'un 53. maddesinde, "Bu Kanuna ve Kamu İhale Sözleşmeleri Kanununa ilişkin bütün mevzuatı, standart ihale dokümanlarını ve tip sözleşmeleri hazırlamak, geliştirmek ve uygulamayı yönlendirmek." Kurum'un görev ve yetkileri arasında sayılmış, Kurum'un, Kurul kararıyla bu Kanun'un ve Kamu İhale Sözleşmeleri Kanunu'nun uygulanmasına ilişkin standart ihale dokümanı, tip sözleşme, yönetmelik ve tebliğler çıkarmaya yetkili olduğu, Kurul ve Kurum'un yetkilerini, düzenleyici işlemler tesis ederek ve özel nitelikli kararlar alarak kullanacağı, standart ihale dokümanları, tip sözleşmeler, yönetmelik ve tebliğlerin Resmî Gazetede yayımlanarak yürürlüğe konulacağı belirtilmiştir. İptali istenilen ibarelerin bulunduğu kuralın da, bu kapsamda Kurum'a verilen görev ve yetkileri içerdiği anlaşılmaktadır.

44. Diğer taraftan Kamu İhale Kurumuna verilen yetki, kamu yararının sağlanmasının yanı sıra hizmet gerekleri ve yetkiyi veren Kanun'un amacının gerçekleştirilmesi ile sınırlıdır. Kurum takdir yetkisini kullanırken, hukukun genel ilkelerine ve hakkaniyete de uygun davranmak zorundadır.

45. Belirtilen özel ve genel sınırlamalara uygun hareket edilip edilmediği, Kamu İhale Kurumuna verilen yetkinin keyfi kullanılıp kullanılmadığı ise yargı denetimine tabidir. Anayasa'nın 125. maddesinde, "İdarenin her türlü eylem ve işlemlerine karşı yargı yolu açıktır." denilerek, idarenin hukuka bağlılığı, yargı denetimi sayesinde etkili biçimde sağlanmış ve idare edilenler, idarenin kanunsuz ve keyfi davranışlarına karşı korunmuştur.

46. Bunun yanında madde gerekçesinden kuralın, nispeten küçük işlerin ihalelerinin daha hızlı bir şekilde sonuçlandırılması ve büyük işlere göre mali yönden daha güçsüz isteklilerin iştirak ettiği bu

ihaleler sonucunda, aşırı düşük tekliflerden kaynaklanan tasfiye riskinin azaltılmasını sağlamak amacıyla çıkarıldığı anlaşılmaktadır. Bu bağlamda, kanun koyucunun takdir yetkisi kapsamında kamu yararı amacıyla çıkarılan iptali istenilen ibareler Anayasa'nın 2. maddesinde düzenlenen hukuk devleti ilkesine aykırı değildir.

47. Anayasa'nın 48. maddesinde, "Herkes dilediği alanda çalışma ve sözleşme hürriyetlerine sahiptir. Özel teşebbüsler kurmak serbesttir. Devlet, özel teşebbüslerin milli ekonominin gereklerine ve sosyal amaçlara uygun yürümesini, güvenlik ve kararlılık içinde çalışmasını sağlayacak tedbirleri alır." denilmektedir.

48. Anayasa'nın 167. maddesinde ise Devlete, para, kredi, sermaye, mal ve hizmet piyasalarının sağlıklı ve düzenli işlemlerini sağlayıcı ve geliştirici önlemleri alma görevi verilmiştir.

49. İhalelere teklif veren gerçek ve tüzel kişiler, Anayasa'nın 48. maddesinin birinci fıkrasında düzenlenen özel teşebbüs kapsamındadır. Kamu İhale Kurumunun kuruluş amacı ve görevi, kamu ihalelerinin daha sağlıklı ve düzenli bir biçimde yapılmasını sağlamak için çalışmalar yapmaktır. Bunu sağlıklı bir biçimde gerçekleştirmek için 4734 sayılı Kanun'un kendisine verdiği görevleri yerine getirirken görev alanı ve Kanun'da belirtilen diğer hükümler ile bağlıdır. Kamu İhale Kurumu ihalenin açıklama istenilmeksizin reddedilmesine ve sonuçlandırılabilmesine ilişkin düzenlemeleri belirlerken kuralları, ihale konusu işin türü, niteliği ve yaklaşık maliyeti ile ihale edilme usulüne göre belirleyecektir. Ayrıca, söz konusu maddede öngörülen açıklama istenilmeksizin reddedilmesine ilişkin düzenlemeleri, yaklaşık maliyeti 8. maddede öngörülen eşik değerlerin yarısına kadar olan hizmet alımları ile yapım işleri ihalelerinde sınır değerinin altında olan teklifler için yapabilecektir. Bu hususların tek tek kanunda düzenlenmesi ise işin teknik özelliği gereği mümkün değildir.

50. Öte yandan, Kamu İhale Kurumu tarafından yapılan düzenleyici işlemler kamu ihalesine katılacak tüm kişiler için geçerli ve ortak kuralları içermektedir. Devletin kamu ihalelerinin sağlıklı ve düzenli işlemesi için oluşturduğu Kamu İhale Kurumu'nun, görev alanı ile ilgili konularda ilgili Kanun hükümlerini de gözetmek kaydı ile düzenleme yapmasında ise Anayasa'nın 48. ve 167. maddelerine aykırılık bulunmamaktadır.

51. Açıklanan nedenlerle iptali istenilen ibareler, Anayasa'nın 2., 48. ve 167. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

D- Kanun'un 48. Maddesiyle, 4734 Sayılı Kanun'un 43. Maddesine Eklenen Fıkırdaki Yer Alan ".yaklaşık maliyetin ." ve ".az ve %15'inden." İbarelerinin İncelenmesi

1- İptal Talebinin Gerekçesi

52. Dava dilekçesinde özetle, ihale üzerinde kalan isteklinin teklifinin sınır değerinin altında kalması halinde, kesin teminatın yüklenim altına girilen sözleşme/ihale bedeli yerine, referans bir değer olan yaklaşık maliyet üzerinden ve % 6 yerine, % 6 ile % 15 arasındaki bir oranda kesilmesinin öngörülmesi ve böylece düşük teklifte bulunanların ek faiz maliyeti üzerinden cezalandırılarak, yüksek teklifte bulunmanın teşvik edilmesinin kamu maliyesi açısından Hazine zararına, rekabetin engellenmesine ve teknolojik gelişmenin cezalandırılmasına yol açacağı, bu durumun ise adalet, hakkaniyet ve kamu yararı ölçütleri ile bağdaşmadığı, iptali istenilen ibarelerin bulunduğu kuralın elverişli, ölçülü ve orantılı olmadığı, sınır değerinin üzerinde olan ihalelerde kesin teminat, ihale bedelinin % 6'sı oranında alınırken, sınır değerinin altında olan ihalelerde ihale bedeli yerine, referans bir değer olan yaklaşık maliyetin ve bu maliyetin % 6'sı yerine, % 6 ile % 15'i arasındaki bir oran üzerinden alınmasının teknolojik üstünlüğü olan firmaların negatif ayrımcılığa tabi tutulmaları anlamına geldiği, aynı zamanda kamu alımları yoluyla piyasaya müdahale eden veya en azından piyasayı yönlendiren Devletin, maliyet avantajlı üretim teknikleriyle çalışan firmaları teşvik etmesi gerekirken teknolojik üstünlüğünden dolayı teklifi sınır değerinin altında kalan firmaları, kesin teminat üzerinden cezalandırmayı öngören düzenlemeler yaparak ülke ekonomisini teknolojik ilerlemeden koparacak yollara başvurmasının Anayasa'nın Devlete verdiği görevlerle bağdaşmadığı belirtilerek iptali istenilen ibarelerin, Anayasa'nın 2., 10., 48. ve 167. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

53. "Kesin teminat" hususunun düzenlendiği Kanun'un 43. maddesinin birinci fıkrasında, taahhüdün sözleşme ve ihale dokümanı hükümlerine uygun olarak yerine getirilmesini sağlamak amacıyla, sözleşmenin yapılmasından önce ihale üzerinde kalan istekliden ihale bedeli üzerinden hesaplanmak suretiyle % 6 oranında kesin teminat alınacağı öngörülmüştür. Maddenin, iptali istenilen ibarelerin bulunduğu üçüncü fıkrasında ise Kurumun, ihale üzerinde kalan isteklinin teklifinin sınır değerinin altında olması halinde, bu istekliden yaklaşık maliyetin % 6'sından az ve % 15'inden fazla olmamak üzere alınacak kesin teminat oranına ilişkin düzenlemeler yapabileceği hüküm altına alınmıştır. Dava konusu ibareler, kuralda yer alan ".yaklaşık maliyetin ." ve ".az ve %15'inden." ibareleridir.

54. Anayasa'nın 2. maddesinde Türkiye Cumhuriyetinin bir hukuk devleti olduğu belirtilmiş olup, kanun koyucu düzenlemeler yaparken hukuk devleti ilkesinin bir gereği olan ölçülülük ilkesiyle bağlıdır. Bu ilke ise "elverişlilik", "gereklilik" ve "orantılılık" olmak üzere üç alt ilkeden oluşmaktadır. "Elverişlilik", başvuru önlemin ulaşılmak istenen amaç için elverişli olmasını, "gereklilik" başvuru önlemin ulaşılmak istenen amaç bakımından gerekli olmasını ve "orantılılık" ise başvuru önlem ve ulaşılmak istenen amaç arasında olması gereken ölçüyü ifade etmektedir.

55. Anayasa'nın 10. maddesinde öngörülen eşitlik ilkesi hukuksal durumları aynı olanlar için söz konusudur. Bu ilke ile eylemli değil hukuksal eşitlik öngörülmektedir. Eşitlik ilkesinin amacı, aynı durumda bulunan kişilerin aynı işleme bağlı tutulmalarını sağlamak ve kişilere kanun karşısında ayırım yapılmasını ve ayrıcalık tanınmasını önlemektir. Bu ilkeyle, aynı durumda bulunan kimi kişi ve topluluklara ayrı kurallar uygulanarak kanun karşısında eşitliğin ihlali yasaklanmıştır. Kanun önünde eşitlik, herkesin her yönden aynı kurallara bağlı tutulacağı anlamına gelmez. Durum ve konumlarındaki özellikler, kimi kişiler ya da topluluklar için değişik kuralları gerekli kılabilir. Aynı hukuksal durumlar aynı, ayrı hukuksal durumlar farklı kurallara bağlı tutulursa Anayasa'nın öngördüğü eşitlik ilkesi ihlal edilmiş olmaz.

56. Sözleşme düzenlenmesi aşamasında idarece yükleniciden kesin teminat alınması, yüklenicinin yükümlülüğünü sözleşme hükümlerine uygun olarak yerine getirmesini sağlamak amacını gütmektedir. İptali istenilen ibarelerin bulunduğu kural uyarınca da, normal koşullar altında, ihale bedeli üzerinden % 6 oranında alınacak olan kesin teminat miktarı, ihalenin aşırı düşük teklif sunan istekli üzerinde kalması halinde Kurum'un, bu istekliden yaklaşık maliyetin % 6'sı ile % 15'i arasında bir oran üzerinden kesin teminat alınmasına ilişkin düzenlemeler yapabilmesine imkân tanımaktadır.

57. Sınır değer, ihale mevzuatında risk oluşturacak değer olarak tanımlanmaktadır. Sınır değerinin altında olan teklifler ihale komisyonunca aşırı düşük teklif olarak değerlendirilmektedir. Aşırı düşük tekliflerin kamuya görünmeyen maliyetleri bulunmakta ve idarenin bu maliyetleri yüklenmesi söz konusu olabilmektedir. Bunun yanında aşırı düşük teklifte projenin istenildiği gibi bitirilememe riski de mevcuttur. Bir ihale, aşırı düşük teklif verene bırakıldığı ve söz konusu proje yapılamadığı takdirde idare bu ihale nedeniyle zarar görebilir. İhale bedeli olarak aşırı düşük teklif verildiği için bu teklif üzerinden kesin teminat yatırılmış olması da idarenin zararını karşılamayabilir. Bu nedenle, aşırı düşük teklifler diğer tekliflere nazaran daha riskli olduğundan ve ihale yüklenicisi ile idarenin korunması amaçlandığından, ihale üzerinde kalan istekliden ihale bedeli yerine, yaklaşık maliyet üzerinden daha fazla oranda teminat alınmak suretiyle oluşabilecek zarar en aza indirgenmek istenmiştir. Böyle bir oranın belirlenmesi ve bu oranın yaklaşık maliyet üzerinden belirlenecek olması, aşırı düşük teklif verilmeden önce isteklinin daha iyi düşünmesini, araştırmasını ve aynı zamanda herhangi bir zarar meydana gelirse idarenin buna karşı korunmasını sağlayacaktır. Kamu yararı amacıyla çıkarılan bu düzenleme kanun koyucunun takdir yetkisi kapsamındadır.

58. Kamu İhale Kanunu'nda, kamuya ait parasal kaynakların kullanılması hususu da gözetilerek, kamu ihalelerinde rekabetçi bir ortamın yaratılması ve ihaleye katılanlar arasında fırsat eşitliğinin sağlanması amaçlanmaktadır. İptali istenilen ibareler ile belirtilen amaçları sağlayabilmek için

getirilen önlemin, Kamu İhale Kanunu ile ulaşılmak istenen amaç için elverişsiz ve gereksiz olduğundan söz edilemez. Ayrıca kanun koyucunun, takdir yetkisi kapsamında aşırı düşük tekliflerin taşıdığı riskin en aza indirilmesi ve oluşacak kamu zararının azaltılması ve kamu kaynaklarının verimli kullanılmasını sağlamak amacıyla düzenlediği kuralın, amaç ve araç arasında makul ve uygun bir ilişki kurduğu ve düzenlemenin amacına ulaşmaya elverişli ve orantılı olduğu anlaşıldığından kuralda ölçülülük ilkesine aykırı bir yön bulunmamaktadır.

59. Bunun yanında, Kamu İhale Kurumu kendisine verilen bu yetkiyi, 4734 sayılı Kanun'un 5. maddesinde belirtilen temel ilkeleri ve diğer hükümleri gözeterek kullanacağından ve Kurumun belirleyeceği kesin teminat oranı, teklifleri sınır değerinin altında olan tüm istekliler için geçerli olacağından, ihale konusu işin bitirilememe riski gözetilerek ihalenin aşırı düşük teklif verenin üzerinde kalması durumunda kesin teminat oranının özel olarak düzenlenmesi eşitlik ilkesine aykırı değildir.

60. Anayasa'nın 48. maddesinin ikinci fıkrasında, "Devlet, özel teşebbüslerin millî ekonominin gereklerine ve sosyal amaçlara uygun yürümesini, güvenlik ve kararlılık içinde çalışmasını sağlayacak tedbirleri alır.", 167. maddesinin birinci fıkrasında, "Devlet, para, kredi, sermaye, mal ve hizmet piyasalarının sağlıklı ve düzenli işlemelerini sağlayıcı ve geliştirici tedbirleri alır..." kurallarına yer verilmiştir.

61. Buna göre, ihalelerin piyasaların sağlıklı ve düzenli işleyişine uygun ve verimli bir şekilde gerçekleşmesi ve hem idareyi hem de ihale yüklenicisini korumak amacıyla böyle bir düzenleme yapılması Devletin görevleri kapsamında olup, kuralda Anayasa'nın 48. ve 167. maddelerine aykırılık bulunmamaktadır.

62. Açıklanan nedenlerle iptali istenilen ibareler, Anayasa'nın 2., 10., 48. ve 167. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

E- Kanun'un 80. Maddesiyle, 5502 Sayılı Sosyal Güvenlik Kurumu Kanunu'nun 30. Maddesine Eklenen Fıkranın İncelenmesi

1- İptal Talebinin Gerekçesi

63. Dava dilekçesinde özetle, iptali istenilen kuralın siyasal iktidarın ideolojisine ters düşenlerin Sosyal Güvenlik Uzmanı kadrolarına atanmasını amaçladığı, genel müdür yardımcısı, daire başkanı ve il müdürü kadrolarında bulunanlar açısından daha üst görevlere atanmak değilse de en azından buldukları kadrolara ait görev güvencelerinin sağlanmasının hukuk güvenliklerine yönelik mutlak bir kazanılmış hak olduğu, kazanılmış hak olarak değerlendirilmese dahi meşru beklentilerin

karşılanması gerektiği, statü hukukuna ve kariyer ilkesine dayanan bir personel rejiminde kanunla daha alt bir göreve atanarak statü kaybına uğratılmalarının hukuk güvenliklerinin ihlali sonucunu doğurduğu, kanunların kanun koyucunun keyfine göre değil, kamu yararı amacıyla çıkarılmasının zorunlu olduğu, kuralın statü hukukunun temelindeki liyakat ilkesi ile bağdaşmadığı, iptali istenilen düzenlemenin söz konusu kadrolarda en az toplam üç yıl görev yapanların tamamını değil, bazılarını Sosyal Güvenlik Uzmanı kadrolarına atamayı öngörerek aynı hukuksal durumda olan kişileri farklı kurallara tabi tuttuğu, yasal atamaya karşı eşitsizliğe muhatap olan kişilerin hak arama yollarını kapatarak hak arama özgürlüklerini kullanılamaz hâle getirdiği, söz konusu kişilerin Sosyal Güvenlik Uzmanı kadrolarına atanmaları durumunda reel ücret bir yana, nominal ücret kaybına da uğrayacakları belirtilerek kuralın, Anayasa'nın 2., 10., 36. ve 70. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

64. İptali istenilen kuralda; başkanlık merkez teşkilatında genel müdür yardımcısı, daire başkanı veya taşra teşkilatında il müdürü kadrolarında toplam en az üç yıl görev yapmış olanların, atama tarihi itibarıyla fiilen bu kadrolardan birinde bulunmak şartıyla Sosyal Güvenlik Uzmanı kadrosuna atanabilecekleri öngörülmüştür.

65. Anayasa'nın 2. maddesinde belirtilen hukuk devleti ilkesinin temel gereklerinden biri kazanılmış haklara saygı gösterilmesidir. Kazanılmış haklara saygı, hukuk güvenliği ilkesinin bir sonucudur. Kazanılmış hak, kişinin bulunduğu statüden doğan, tahakkuk etmiş ve kendisi yönünden kesinleşmiş, kişisel alacak niteliğine dönüşmüş haktır.

66. Hukuk güvenliği, normların öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde Devlete güven duyabilmesini, Devletin de yasal düzenlemelerde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar. Kanunlara güvenerek hayatını yönlendiren, hukuki iş ve işlemlere girişen bireyin, bu kanunların uygulanmasına devam edileceği yolunda oluşan beklentisinin mümkün olduğunca korunması hukuki güvenlik ilkesinin gereğidir. Ancak güvenin korunması, mevcut bir hukuki durumun dokunulmazlığı anlamında da değerlendirilmemelidir. Hukuki güvenliğin mevcut bir hukuki durum için dokunulmazlık şeklinde algılanması, dinamik toplum yapısının kurallarla statik, durağan hâle getirilmesi sonucunu doğurur ki bu da toplumun çağın gerisinde kalmasına neden olabilir. Bu nedenle kanun koyucu, Anayasa'da öngörülen koşullar çerçevesinde diğer alanlarda olduğu gibi kamu görevlilerinin durumları ile ilgili olarak da kamu yararı amacıyla bazı değişiklikler yapabilir.

67. Genel müdür yardımcısı, daire başkanı ve il müdürü kadrolarının Sosyal Güvenlik Uzmanlığı gibi kariyer mesleklerden gelenler ve idari görevlerden yükselerek gelenler olmak üzere iki ayrı kaynağı bulunmaktadır. Kariyer meslek kaynağından gelen kişilerin kendi kadrolarına eşit veya daha düşük statüdeki Sosyal Güvenlik Uzmanı kadrolarına atanabilmeleri için kuralda belirtilen koşullara tabi tutulmayacakları açıktır. Dolayısıyla iptali istenilen kural, anılan koşullar aranmaksızın mevcut duruma göre Sosyal Güvenlik Uzmanlığına atanma imkânına sahip kariyer meslek kaynağından gelenleri değil, önceki görevi ve kadro unvanı itibarıyla Sosyal Güvenlik Uzmanlığına atanma imkânına sahip bulunmayan kişileri kapsamaktadır.

68. Sosyal Güvenlik Uzmanlığı kariyer bir meslek olup, bu göreve atanabilmek için Kanun'da belirtilen koşulların taşınması gerekmektedir. İptali istenilen kural ise Sosyal Güvenlik Uzmanı olma koşullarını taşımayan genel müdür yardımcısı, daire başkanı ve il müdürlerine, kariyer bir meslek olan Sosyal Güvenlik Uzmanı olma hakkı tanımaktadır. Ayrıca, bakanlık merkez teşkilatında genel müdür yardımcısı, daire başkanı ve taşra teşkilatında il müdürü olan kişilerin iptali istenilen kuraldan yararlanabilmeleri için bu kadrolarda toplam en az üç yıl görev yapmış olmaları ve atama tarihi itibarıyla bu kadrolardan birinde bulunmaları gerekmektedir. Bununla birlikte, bu koşullar gerçekleşse dahi bu kişilerin Sosyal Güvenlik Uzmanlığına atanmaları konusunda idarenin takdir yetkisi bulunmaktadır.

69. Genel müdür yardımcısı, daire başkanı ve il müdürü kadroları idareci (yönetici) kadroları olup idarenin bu kadrolara bir kere atadığı kişileri meslek hayatları boyunca bu kadrolarda çalıştırma zorunluluğunun bulunmayacağı açıktır. Dolayısıyla bu kadrolara atanan kişiler yönünden, buldukları statülerden doğan, tahakkuk etmiş, kendileri yönünden kesinleşmiş ve kişisel alacak niteliğine dönüşmüş haklardan yahut bu durumun devam edeceği yönündeki haklı beklentiden söz edilemez. Bu nedenle, kamu yararı ve hizmetin gerekleri dikkate alınarak bu kişilerin idarecilik görevlerine son verilmesi ve kariyer meslek kadrolarından gelenlerin kendi kadrolarına, kariyer mesleklerden gelmeyenlerin ise bazı koşulları taşımak kaydıyla, geldiği kadrodan daha üst bir görev olan Sosyal Güvenlik Uzmanlığı kadrolarına atanmaları mümkün olup bunu düzenleyen kuralın kazanılmış hakları veya genel olarak hukuk güvenliği ilkesini ihlal eden bir yönü bulunmamaktadır.

70. Öte yandan, Anayasa'nın 2. maddesindeki "hukuk devleti" ilkesi gereğince, yasama işlemlerinin kişisel yararları değil kamu yararını gerçekleştirmek amacıyla yapılması zorunludur. Bir kuralın Anayasa'ya aykırılık sorunu çözümlenirken "kamu yararı" konusunda Anayasa Mahkemesinin yapacağı inceleme yalnızca kanunun kamu yararı amacıyla yapılıp yapılmadığı ile sınırlıdır. Kanun

ile kamu yararının gerçekleşip gerçekleşmeyeceğini denetlemenin anayasa yargısıyla bağdaşmayacağı, bunun kanun koyucunun takdirinde olduğu açıktır.

71. Kanun koyucu, kamu yararı ve hizmetin gereklerini dikkate alarak kamu görevlilerinin statüsünde, bunların unvanlarında, görev ve yetkilerinde olduğu gibi bu statülere atanma koşullarında da değişiklikler yapabilir. İptali istenilen kural ile kariyer meslek kaynağından gelmeyen ve Sosyal Güvenlik Uzmanlığına atanma imkânına sahip olmayanlardan hizmetine ihtiyaç duyulanların, kuralda belirtilen genel müdür yardımcılığı, daire başkanlığı veya taşra teşkilatında il müdürlüğünü en az üç yıl ifa etmeleri ve atama tarihi itibarıyla fiilen bu kadrolardan birinde bulunmak şartıyla kariyer meslek olan Sosyal Güvenlik Uzmanlığına atanabilmelerinin sağlanmak istendiği ve düzenlemenin bu amaçla çıkarıldığı anlaşılmaktadır. Bu amacın kamu yararına yönelik olmadığı söylenemez. İptali istenilen kural ile amaçlanan kamu yararının gerçekleşip gerçekleşmeyeceği ise anayasallık denetiminin kapsamı dışındadır.

72. İptali istenilen kuralda genel müdür yardımcısı, daire başkanı veya taşra teşkilatında il müdürü olanların tümünün değil, en az üç yıl görev yapmış olanların ve atama tarihi itibarıyla fiilen bu kadrolardan birinde bulunanların Sosyal Güvenlik Uzmanlığına atanabileceği belirtilmiştir. İdare hukukunun genel ilkeleri uyarınca idarenin bu yetkisini kullanırken kuralda belirtilen şartları taşıyanlar yönünden de kamu hizmetinin daha iyi işlemesi veya kamu yararı esasına göre ayırım yaparak atama yapmak zorunda olduğu açıktır. Kamu hizmetinin daha iyi işlemesi veya kamu yararı amacıyla atama yapabilmesi için ise söz konusu kadrolarda çalışanların başarısı, liyakatı gibi çeşitli ayırt edici kriterlerin kullanılması gerekir. Bu nedenle, bu kriterleri taşıyan kişilerle taşımayanlar aynı hukuki durumda bulunmadıklarından iptali istenilen kural uyarınca bunlar arasında ayırım yapılarak bunların farklı kurallara tabi kılınmasında eşitlik ilkesine aykırılıktan söz edilemez.

73. Diğer taraftan, Anayasa'nın "Hak arama hürriyeti" başlıklı 36. maddesinin birinci fıkrasında, "Herkes, meşrû vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir." denilerek yargı organlarına davacı ve davalı olarak başvurabilme ve bunun doğal sonucu olarak da iddia, savunma ve adil yargılanma hakkı güvence altına alınmıştır. Anayasa'nın 125. maddesinde ise "İdarenin her türlü eylem ve işlemlerine karşı yargı yolu açıktır..." denilmektedir. Her iki maddeyle güvence altına alınan dava yoluyla hak arama özgürlüğü, kendisi bir temel hak niteliği taşımasının ötesinde diğer temel hak ve özgürlüklerden gereken şekilde yararlanılmasını ve bunların korunmasını sağlayan en etkili güvencelerden biridir. Kişilere yargı mercileri önünde dava hakkı tanınması adil bir yargılamanın ön koşulunu oluşturur.

74. İptali istenilen kural ile idare tarafından Başkanlık merkez teşkilatında genel müdür yardımcısı, daire başkanı veya taşra teşkilatında il müdürü kadrolarında çalışanların Sosyal Güvenlik Uzmanı olarak atanmış sayılması değil, bu kadrolarda çalışanlardan kuralda belirtilen koşulları taşıyanların idare tarafından Sosyal Güvenlik Uzmanı olarak atanabilmesi düzenlenmektedir. Dolayısıyla söz konusu kuralın uygulanabilmesi için idari işlem tesis edilmesi gerekmektedir. Anayasa'nın 125. maddesi uyarınca da, idari işlemler yönünden kişilerin yargı yoluna başvurmaları mümkün olduğundan, iptali istenilen kuralda Anayasa'nın 36. maddesinde düzenlenen hak arama özgürlüğüne aykırılık bulunmamaktadır.

75. Açıklanan nedenlerle kural, Anayasa'nın 2., 10. ve 36. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

76. Serdar ÖZGÜLDÜR bu görüşe katılmamıştır.

77. Kuralın Anayasa'nın 70. maddesiyle bir ilgisi görülmemiştir.

F- Kanun'un 85. Maddesiyle, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un; 2. Maddesinin (1) Numaralı Fıkrasına Eklenen (n) Bendi ile 90. Maddesiyle 5651 Sayılı Kanun'a Eklenen 6/A Maddesinin (1), (2), (3) (4), (5), (6), (8), (9), (10) Numaralı Fıkraları ve 93. Maddesiyle 5651 Sayılı Kanun'un Değiştirilen 9. Maddesinin (5) ve (8) Numaralı Fıkraları ve 100. Maddesiyle 5651 Sayılı Kanun'a Eklenen Geçici 3. Maddesinin (1), (3), (4) Numaralı Fıkraları ile (2) Numaralı Fıkrasının İkinci Cümlesinin İncelenmesi

1- Kuralların Anlam ve Kapsamları

78. Erişim Sağlayıcıları Birliği (ESB), Kanun'un 6/A maddesi ile bir özel hukuk tüzel kişisi olarak, Kanun'un 8. maddesi kapsamı dışındaki erişimin engellenmesi kararlarının uygulanmasını sağlamak üzere kurulmuştur.

79. Kanun'un 2. maddesinin iptali istenilen (n) bendinde; Birliğin, Erişim Sağlayıcıları Birliğini ifade ettiği belirtilmiştir.

80. Kanun'un iptali istenilen 6/A maddesinde ise, ESB ile ilgili düzenlemeler yer almaktadır. Maddenin (1) numaralı fıkrasında 5651 sayılı Kanun'un 8. maddesi kapsamı dışındaki erişimin engellenmesi kararlarının uygulanmasını sağlamak üzere Erişim Sağlayıcıları Birliğinin kurulduğu, (2) numaralı fıkrasında Birliğin özel hukuk tüzel kişiliğini haiz ve merkezinin Ankara olduğu, (3) numaralı fıkrasında Birliğin çalışma usul ve esaslarının Kurum (BTK) tarafından onaylanacak Tüzükle belirleneceği ve Tüzük değişikliklerinin Kurumun onayına tabi olduğu, (4) numaralı

fıkrasında Birliğin, Tüzüğün Kurum tarafından incelenerek uygun bulunmasını müteakip faaliyete başlayacağı, (5) numaralı fıkrasında Birliğin 5.11.2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu kapsamında yetkilendirilen tüm internet servis sağlayıcıları ile internet erişim hizmeti veren diğer işletmecilerin katılmasıyla oluşan ve koordinasyonu sağlayan bir kuruluş olduğu, (6) numaralı fıkrasında 5651 sayılı Kanun'un 8. maddesi kapsamı dışındaki erişimin engellenmesi kararlarının erişim sağlayıcılar tarafından yerine getirileceği, kararların uygulanması amacıyla gerekli her türlü donanım ve yazılımın erişim sağlayıcıların kendileri tarafından sağlanacağı, (8) numaralı fıkrasında Birliğin kendisine gönderilen mevzuata uygun olmadığını düşündüğü kararlara itiraz edebileceği, (9) numaralı fıkrasında Birliğin gelirlerinin, üyeleri tarafından ödenecek ücretlerden oluşacağı, alınacak ücretlerin, Birliğin giderlerini karşılayacak miktarda belirleneceği, bir üyenin ödeyeceği ücretin, üyelerin tamamının net satış tutarı toplamı içindeki o üyenin net satışı oranında belirleneceği, üyelerin ödeme dönemleri, yeni katılan üyelerin ne zamandan itibaren ödemeye başlayacağı ve ödemelere ilişkin diğer hususların Birlik Tüzüğünde belirleneceği, süresinde ödenmeyen ücretlerin Birlikçe kanuni faizi ile birlikte tahsil edileceği, (10) numaralı fıkrasında Birliğe üye olmayan internet servis sağlayıcılarının faaliyette bulunamayacağı öngörülmüştür.

81. Kanun'un iptali istenilen geçici 3. maddesinin (1) numaralı fıkrasında ise Birliğin kuruluşunun bu Kanunun yayımı tarihinden itibaren üç ay içinde tamamlanacağı, (2) numaralı fıkrasının ikinci cümlesinde Birliğin kurulmasını müteakip en geç bir ay içinde halen üye olmayan internet servis sağlayıcıları ve erişim hizmeti veren işletmecilerin üyeliklerini tamamlamak zorunda oldukları, (3) numaralı fıkrasında belirtilen sürede Birliğin kuruluşunu tamamlayamaması halinde, Kurum tarafından internet servis sağlayıcılarına ve internet erişim hizmeti veren diğer işletmecilere bir önceki takvim yılındaki net satışların yüzde biri oranında idari para cezası uygulanacağı, (4) numaralı fıkrasında ise Birliğin kurulmasını müteakip bir ay içinde üye olmayan internet servis sağlayıcılarına veya internet erişim hizmeti veren diğer işletmecilere Kurum tarafından bir önceki takvim yılındaki net satışların yüzde biri oranında idari para cezası uygulanacağı ifade edilmektedir.

82. Kanun'un 9. maddesinin iptali istenilen (5) numaralı fıkrasında da hâkimin 9. madde kapsamında kişilik hakkının ihlal edilmesi nedeniyle verdiği erişimin engellenmesi kararlarının doğrudan Birliğe gönderileceği, (8) numaralı fıkrasında Birlik tarafından erişim sağlayıcıya gönderilen içeriğe erişimin engellenmesi kararının gereğinin derhal, en geç dört saat içinde erişim sağlayıcı tarafından yerine getirileceği belirtilmektedir.

83. ESB, 19 Mayıs 2014 tarihinde faaliyete başlamıştır. Birliğin asıl görevi, Kanun'un 8. maddesi kapsamında olan katalog suçlara ilişkin koruma ve idari tedbir dışındaki erişimin engellenmesi

kararlarının uygulanmasını sağlamaktır. Birlik, 5809 sayılı Elektronik Haberleşme Kanunu kapsamında yetkilendirilen tüm internet servis sağlayıcıları ile internet erişim hizmeti veren diğer işletmecilerin katılımıyla oluşan ve bunlar arasındaki koordinasyonu sağlayan bir kuruluştur. Birliğe üye olmayan erişim sağlayıcılar faaliyette bulunamazlar. Bu özelliklere bakıldığında, ESB dernek veya vakıf statüsünde değildir.

84. Anayasa'nın 135. maddesinde, "Kamu kurumu niteliğindeki meslek kuruluşları ve üst kuruluşları; belli bir mesleğe mensup olanların müşterek ihtiyaçlarını karşılamak, meslekî faaliyetlerini kolaylaştırmak, mesleğin genel menfaatlere uygun olarak gelişmesini sağlamak, meslek mensuplarının birbirleri ile ve halk ile olan ilişkilerinde dürüstlüğü ve güveni hâkim kılmak üzere meslek disiplini ve ahlâkını korumak maksadı ile kanunla kurulan ve organları kendi üyeleri tarafından kanunda gösterilen usullere göre yargı gözetimi altında, gizli oyla seçilen kamu tüzelkişilikleridir." denilmektedir. ESB'nin, kamu tüzel kişisi olmaması ve oluşturulma amacının, 5651 sayılı Kanun'un 8. maddesi kapsamı dışındaki erişimin engellenmesi kararlarını yerine getirmek olması göz önüne alındığında, kamu kurumu niteliğindeki meslek kuruluşları kapsamında da değerlendirilemeyeceği açıktır.

85. İnternetteki hukuka aykırılıkların giderilebilmesi ancak erişimin engellenmesi yoluyla yapılabilmekte, erişimin engellenmesi ise ancak erişim sağlayıcılar üzerinden gerçekleştirilebilmektedir. İçeriğin yayından çıkartılması ve içeriğe erişimin engellenmesi kararlarının mevcut uygulamalar yönüyle ortaya koyduğu sorunlar, infaz edilememelik ve muhatap belirsizliği gibi engellerin ortadan kaldırılmasını sağlamak için kamu yararı amacıyla ESB kurulmuştur. ESB, erişim sağlayıcıları ile bağlantıyı sağlamakta ve erişimin engellenmesi ile ilgili kararları erişim sağlayıcılara iletmekle görevli bulunmaktadır.

86. ESB'nin, Kanun'da özel hukuk tüzel kişiliğini haiz olduğunun belirtilmesi ve özel hukuk tüzel kişilerinden oluşması, kuruluşunun kanunla yapılmış olması, faaliyete başlayabilmesi için Tüzüğünün BTK tarafından onaylanmasının gerekmesi ve Tüzük değişikliklerinin BTK'nun onayına tabi tutulması, kurulmasının ve üyeliğin zorunlu tutularak idari yaptırım öngörülmesi, yapacağı görevlerin kamusal yanının ağır basması gibi hususlar gözetildiğinde, idari teşkilat yapısı içinde yer almayan, kanunla kurulmuş kendine özgü bir kurum olduğu söylenebilir.

2- İptal Taleplerinin Gerekçeleri

87. Dava dilekçesinde özetle,

a. Kanun gerekçesinde "Erişim Sağlayıcıları Birliği" adı altında, özel hukuk tüzel kişiliğine ve kamusal yetkilere sahip, nev'i şahsına münhasır bir yapının kurulmasının esas amacının, içeriğin yayından çıkarılması ve içeriğe erişimin engellenmesi kararlarının infazında yaşanan sorunların giderilmesi olduğunun belirtildiği, Kanun'un 6/A maddesinin yedinci fıkrasının ikinci cümlesinde yer alan "Bu kapsamda Birliğe yapılan tebligatın erişim sağlayıcılara yapılmış sayılacağı" ibaresi ile bunun amaçlandığı ve bu konuda uluslararası uygulamaların esas alındığı ifade edilmiş ise de başka ülkelerde benzeri bir örneğe rastlamanın mümkün olmadığı,

b. Maddenin beşinci fıkrasında tüm internet servis sağlayıcıları ile internet erişim hizmeti veren diğer işletmecilerin katılımını mecbur kılan ve onuncu fıkrasında Birliğe üye olmayan internet servis sağlayıcılarının faaliyette bulunamayacağını öngören bir tüzel kişiliğin, hukuka uygun ve meşru bir tüzel kişilik olarak kabul edilemeyeceği, söz konusu Birliğin, Telekomünikasyon İletişim Başkanı'nın emir ve talimatını yerine getirmekten öte bir işlevi olmayacak bir kurum mesabesine indirildiği, tüm internet servis sağlayıcıları ile erişim hizmeti veren işletmecilerin Birliğe üye olma zorunluluğu getiren bu düzenlemenin, sektörde faaliyette bulunmak için yeni bir "koşul" getirilmesi anlamına geldiği, Birliği hem kurmanın hem de bu Birliğe üye olmanın, servis sağlayıcılar açısından açıkça zorunlu hale getirilmiş olmasının, ulusal ve uluslararası hukuk ile teminat altına alınmış olan ve hiç kimsenin iradesi dışında bir örgüte üye olmaya zorlanamayacağını da içeren örgütlenme özgürlüğünün ihlali anlamına geleceği ve girişim özgürlüğünü de ihlal ettiği, ilgili alanda girişimde bulunmak isteyen gerçek ve tüzel kişiler için yeni bir "piyasaya giriş şartı" getirildiği, Birliğin Kanun'un 6/A maddesinin ikinci fıkrasında özel hukuk tüzel kişiliğini haiz olduğunun açıkça belirtildiği, Birliğe üye olmayan internet servis sağlayıcılarını Devlet eliyle sektör dışı bırakmanın hem rekabet hukukunu ihlal edici, hem de böyle bir erişim sağlayıcının müktesep hakkını gasp edici nitelikte olduğu, bu nedenle 6/A maddesinin beşinci ve onuncu fıkralarının dernek kurma hürriyetine aykırı olduğu, öte yandan anılan düzenlemelerin girişim özgürlüğünü kısıtladığı ve demokratik bir toplumda gerekli ve zorunlu olmadıkları,

c. Kanun'un 6/A maddesinin altıncı fıkrası uyarınca, işletmelerin, iradeleri dışında dâhil oldukları ve kamusal nitelikte bir yükümlülüğü yerine getirecek olan Birliğin ve engelleme tedbirlerinin bütün külfet ve giderlerinden sorumlu tutulmalarının hakka ve hakkaniyete aykırı olup, hukuk devleti ilkesiyle bağdaşmadığı, kamusal yükümlülüğün erişim sağlayıcılara devredilmesine ek olarak, erişim engelleme tedbirlerinin yüksek maliyetli alt yapılar gerektiriyor olması karşısında, bu tedbirlerin ancak, piyasada hâkim durumda olan veya etkin piyasa gücüne sahip internet servis sağlayıcıları ile internet erişim hizmeti veren işletmeciler tarafından yerine getirilebilmesinin, piyasaya yeni giren ve

daha küçük çapta faaliyet gösteren işletmecilerin, elektronik haberleşme hizmeti sunamamaları ile sonuçlanacağı, bu tedbirlerin piyasada hâkim durumda olan veya etkin piyasa gücünü elinde bulunduran internet servis sağlayıcıları ile internet erişim hizmeti veren işletmeciler tarafından yerine getirilmesinin tekelleşme ve kartelleşmenin önünün açılmasını sağlayacağı,

d. 6/A maddesinin birinci, beşinci, altıncı ve onuncu fıkralarının Anayasa'ya aykırılığının aynı maddenin iptali istenilen diğer fıkralarına da sirayet ettiği ve anılan fıkraların da kaçınılmaz bir şekilde sakatlanması ve Anayasa'ya aykırı olması sonucunu doğuracağı, bu fıkralar hakkında ileri sürülen bütün Anayasa'ya aykırılık gerekçelerinin aynı maddenin diğer fıkra hükümleri yönünden de aynen geçerli olduğu,

e. Kanun'un 6/A maddesinin iptali ile ilgili olarak ileri sürülen tüm Anayasa'ya aykırılık gerekçelerinin, Kanun'un 2. maddesinin (1) numaralı fıkrasına eklenen (n) bendi ile 9. maddenin iptali istenilen fıkraları için de geçerli olduğu, zira belirtilen maddeler arasında organik bir bağ bulunduğu, maddelerin varlıklarını sürdürmelerinin birbirlerine bağlı olduğu,

f. "Birliğin kurulmasını müteakip en geç bir ay içinde halen üye olmayan internet servis sağlayıcıları ve erişim hizmeti veren işletmeciler üyeliklerini tamamlamak zorundadır" hükmünün, halen Birliğe üye olmayan internet servis sağlayıcılarına ve erişim hizmeti veren işletmecilere Birliğe üye olma zorunluluğu getirdiği, bu mecburiyete uymamanın müeyyidelerinin ise geçici 3. maddenin (3) ve (4) numaralı fıkralarında gösterildiği, halen üye olmayan internet servis sağlayıcıları ile erişim hizmeti veren işletmecilerin Birliğin kurulmasını müteakip en geç bir ay içinde üyeliklerini tamamlamak zorunda bırakılmalarının dernek kurma hürriyetine, "Çalışma ve sözleşme hürriyeti"ne ve "Sendika kurma hakkı"na açıkça aykırı olduğu, diğer yandan Kanun'un 6/A maddesi hakkında ileri sürülen bütün Anayasa'ya aykırılık gerekçelerinin geçici 3. madde yönünden de aynen geçerli olduğu,

belirtilerek kuralların, Anayasa'nın 2., 5., 33., 36., 40., 48., 51. ve 167. maddelerine aykırı olduğu ileri sürülmüştür.

3- Anayasa'ya Aykırılık Sorunu

88. Anayasa'nın 2. maddesinde belirtilen hukuk devletinin temel ilkelerinden biri "belirlilik"tir. Bu ilkeye göre, yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olması, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi gerekir. Belirlilik ilkesi, bireylerin hukuksal güvenliğinin sağlanması bakımından da önem arz etmektedir.

89. Kanun koyucunun ESB'yi, içeriğin yayından çıkartılması ve içeriğe erişimin engellenmesi kararlarının infaz edilememelik ve muhatap belirsizliği gibi sorunların ortadan kaldırılması ve işin teknik özelliğinden dolayı bu görevi yapabilecek başka bir kurumun bulunmamasını da gözeterek, erişimin engellenmesi kararlarının bir an önce yerine getirilmesini sağlamak amacıyla kurduğu anlaşılmaktadır. Bu şekilde düzenlemeler yapılması ise anayasal sınırlar içinde kanun koyucunun takdir yetkisi kapsamındadır.

90. ESB söz konusu erişimin engellenmesi kararlarını doğrudan yerine getirmemekte, yalnızca erişim sağlayıcılar ile söz konusu kararın muhatapları arasında aracılık görevi yapmaktadır. Birliğe üye olunmasının zorunlu olması ise Birliğe verilen görevin bir gereği olup, zorunluluk getirilmemesi halinde erişimin engellenmesi kararlarının yerine getirilmesinin mümkün olmamasından kaynaklanmaktadır. ESB'nin çalışma usul ve esasları Kurum tarafından onaylanacak Tüzükle belirlenmekte, tüzük değişiklikleri de Kurumun onayına tabi bulunmaktadır. Ayrıca ESB, Tüzüğü'nün BTK tarafından uygun bulunmasını müteakip faaliyete geçmektedir. Bu nedenle, Birliğin Devlet tarafından gözetim ve denetimi de söz konusu olmaktadır. Dolayısıyla, 5651 sayılı Kanun'un 8. maddesi kapsamı dışındaki erişimin engellenmesi kararlarının uygulanmasını sağlamak için kurulan Birliğin yapısı, işleyişi ve kurulması ile ilgili olarak getirilen kurallar belirli ve öngörülebilirdir.

91. Anayasa'nın 48. maddesinde "Herkes, dilediği alanda çalışma ve sözleşme hürriyetlerine sahiptir. Özel teşebbüsler kurmak serbesttir. Devlet, özel teşebbüslerin milli ekonominin gereklerine ve sosyal amaçlara uygun yürümesini, güvenlik ve kararlılık içinde çalışmasını sağlayacak tedbirleri alır." denilmektedir.

92. Erişim sağlayıcılar, Anayasa'nın 48. maddesinin birinci fıkrasında düzenlenen özel teşebbüs kapsamındadır. Aynı maddenin ikinci fıkrasına göre Devlet özel teşebbüslerin milli ekonominin gereklerine ve sosyal amaçlara uygun yürümesini, güvenlik ve kararlılık içinde çalışmasını sağlayacak tedbirleri alır. Erişim sağlayıcılarının ESB'ye üye olma zorunluluğunun getirilme amacı gözetildiğinde, bu amaca ancak tüm erişim sağlayıcıların söz konusu Birliğe üye olması ile ulaşılacağı açıktır. Bu nedenle, kanun koyucu tarafından getirilen kurallar da bu kapsamda olup, erişimin engellenmesi kararlarının yerine getirilmesindeki muhatap belirsizliğini ortadan kaldırmak, kararların bir an önce yerine getirilmesini sağlamaya yöneliktir. Aksi takdirde söz konusu sistemin işlemesi mümkün olmayacaktır. Kaldı ki, Anayasa'nın 138. maddesinde yer alan "Yasama ve yürütme organları ile idare, mahkeme kararlarına uymak zorundadır; bu organlar ve idare, mahkeme kararlarını hiçbir surette değiştiremez ve bunların yerine getirilmesini geciktiremez." hükmü

gözetildiğinde, mahkeme kararlarının bir an önce yerine getirilmesini sağlamak için erişim sağlayıcıların ESB'ye üye olma zorunluluğunun getirilmesi, Devletin pozitif yükümlülüklerinin bir sonucu olup, kişilerin özel teşebbüs kurma haklarını zedeleyen bir yönü bulunmamaktadır.

93. İnternet piyasası yazılım ve donanım sistemi üzerine kurulmuştur. Erişim sağlayıcıların faaliyetlerini gerçekleştirebilmeleri için, gerekli olan yazılım ve donanıma sahip olmaları gerekmektedir. Kanun'un iptali istenilen 6/A maddesinin (6) numaralı fıkrasında da, kararların uygulanması amacıyla gerekli her türlü donanım ve yazılımın erişim sağlayıcıların kendileri tarafından sağlanacağı belirtilmiştir.

94. Anayasa Mahkemesi'nin birçok kararında da belirtildiği gibi, sosyal devlet ekonomik açıdan müdahaleci devlettir. Anayasamız, mülkiyet hakkını, özel girişim özgürlüğünü kabul etmekte, aynı zamanda bütün çağdaş anayasalarda olduğu gibi kamu yararı amacıyla bunlara sınırlamalar getirilebilmesini ve özel teşebbüslerin millî ekonominin gereklerine ve sosyal amaçlara uygun yürümesini sağlayacak önlemlerin alınmasını öngörmektedir. Anayasa'nın, "kişilerin ve toplumun refah huzur ve mutluluğunu sağlamak" görevini Devlete veren 5. maddesi, "özel teşebbüslerin millî ekonominin gerekleri ve sosyal amaçlara uygun yürümesini, güvenlik ve kararlılık içinde çalışmasını sağlayacak tedbirleri" almakla görevlendiren 48. maddesi hükümleri, Devletin gerektiğinde çalışma hayatına müdahale edebileceğini göstermektedir. Devlet, internet ortamında yapılan yayınlar nedeniyle kişilik hakları ve özel hayatının gizliliği ihlal edilen kişilerin korunmasını sağlamakla görevlidir. Bunun için de bu hakları ihlal edilen kişilere yönelik yayınlara erişimin engellenmesini sağlamak için iptali istenilen kural ile ESB'ni kurmuştur. Bu kapsamda, erişimin engellenmesi için gerekli olan her türlü donanımın ve yazılımın erişim sağlayıcılarının kendileri tarafından karşılanmasına yönelik hüküm de Devletin aldığı tedbirler kapsamında olup bu hususlarda düzenleme yapılması kanun koyucunun takdir yetkisi içindedir. Belirtilen nedenlerle söz konusu kural Anayasa'nın 2., 5. ve 48. maddelerine aykırı değildir.

95. İptali istenilen kurallardan 6/A maddesinin (8) numaralı fıkrası uyarınca Birliğe, gereği yerine getirilmek üzere gönderilen kararlardan mevzuata uygun olmadığını düşündüklerine itiraz hakkının tanınması ise kamu yararını sağlamaya yönelik bir düzenlemedir. Birliğe itiraz hakkı tanınmak suretiyle, verilen erişimin engellenmesi kararının tekrar gözden geçirilmesi sağlanmak istenmiştir. İptali istenilen kurallardan 6/A maddesinin (9) numaralı fıkrasında düzenlenen, Birliğin gelirlerinin, üyeleri tarafından ödenecek ücretlerden oluşacağı, alınacak ücretlerin, Birliğin giderlerini karşılayacak miktarda belirleneceği, bir üyenin ödeyeceği ücretin, üyelerin tamamının net satış tutarı toplamı içindeki o üyenin net satış oranında belirleneceği, üyelerin ödeme dönemleri, yeni katılan

üyelerin ne zamandan itibaren ödemeye başlayacağı ve ödemelere ilişkin diğer hususların Birlik Tüzüğünde belirleneceği, süresinde ödenmeyen ücretlerin Birlikçe kanuni faizi ile birlikte tahsil edileceği hususları ESB'nin varlığını devam ettirmesi ve kendisine yüklenen erişimin engellenmesi görevinin yerine getirilmesini sağlamaya yöneliktir. Kamu yararı amacı ile çıkarılan bu düzenlemeler de anayasal sınırlar içinde kanun koyucunun takdirindedir.

96. Açıklanan nedenlerle kurallar, Anayasa'nın 2., 5. ve 48. maddelerine aykırı değildir. İptal taleplerinin reddi gerekir.

97. Kuralların, Anayasa'nın 33., 36., 40., 51. ve 167. maddeleriyle ilgisi görülmemiştir.

G- Kanun'un 90. Maddesiyle 5651 Sayılı Kanun'a Eklenen 6/A Maddesinin (7) Numaralı Fıkrasının İncelenmesi

1- İptal Talebinin Gerekçesi

98. Dava dilekçesinde özetle, kuralın tebligat mevzuatına aykırı olduğu gibi uluslararası anlaşmalarla korunan hukuki menfaatleri ve tebligat güvenliğini zedeler mahiyette olduğu, kuralın uygulanması durumunda Birliğe yapılan tebligatın muhatabı olan erişim sağlayıcıya gidip gitmediği, muhatabına ulaşip ulaşmadığı, ulaştı ise içeriğine ne zaman vakıf olduğu, tebligatın tebellüğ yetkisine sahip olanlarca alınıp alınmadığının muallakta kalacağı, geçerli tebligatlara bağlanan süreler ve süreçlerin tüm erişim sağlayıcılar için geçerli olmak üzere Birliğe yapılan tebligat ile sağlanmasının hukuki güvenliği sarstığı, düzenleme ile bir çok hukuki sürecin ilgili tarafın tebligat içeriğinin farkında dahi olmadan önce başlayabileceği, bu durumun ise hak arama hürriyetini ciddi bir şekilde tehdit edebileceği, gerçek ve tüzel kişilerin haklarını doğrudan etkileme kapasitesine sahip olan tedbir/yaptırım kararlarının, başka bir özel hukuk tüzel kişisine tebliğ edilmesinin geçerli addedilmesinin savunma hakkının etkin kullanımını engellediği, 5651 sayılı Kanun kapsamında internet servis sağlayıcılık faaliyeti yapanlara Birlik vasıtasıyla yapılacak bildirim muhatabına ulaşmaması halinde, bu muhatapların meşru vasıta ve yollardan yararlanmak suretiyle yargı mercileri önünde davacı, davalı, müşteki veya muteriz olarak iddia ve savunma hakları ile adil yargılanma hakkının elinden alınması ve dolayısıyla hak arama hürriyetinden mahrum bırakılmaları anlamına geleceği, ayrıca kuralda Anayasa ile güvence altına alınmış hak ve hürriyetlerin ihlal edildiğini iddia eden gerçek veya tüzel kişilere yetkili makama geciktirilmeden başvurma imkanının sağlanmasını isteme hakkının tanınmadığı ve yine benzer durumlarda ilgili gerçek veya tüzel kişilere hangi kanun yolları ve mercilere başvuracağı ve sürelerinin gösterilmediği belirtilerek kuralın, Anayasa'nın 2., 36. ve 40. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

99. Kanun'un 6/A maddesinin iptali istenilen (7) numaralı fıkrasının birinci cümlesinde, 5651 sayılı Kanun'un 8. maddesi kapsamı dışındaki erişimin engellenmesi kararlarının gereği için Birliğe gönderileceği, ikinci cümlesinde ise bu kapsamda Birliğe yapılan tebligatın erişim sağlayıcılara yapılmış sayılacağı öngörülmektedir.

100. Anayasa'nın 2. maddesinde yer alan hukuk devletinin temel ilkelerinden biri "hukuk güvenliği" ilkesidir. Hukuk güvenliği, normların öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar.

101. Anayasa'nın hak arama hürriyetini düzenleyen 36. maddesinin birinci fıkrasında, "Herkes, meşru vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir." denilerek yargı mercilerine davacı ve davalı olarak başvurabilme ve bunun doğal sonucu olarak da iddia, savunma ve adil yargılanma hakkı güvence altına alınmıştır. Maddeyle korunan hak arama özgürlüğü, kendisi bir temel hak niteliği taşımasının ötesinde, Anayasa'nın 40. maddesi uyarınca diğer temel hak ve özgürlüklerden gereken şekilde yararlanılmasını ve bunların korunmasını sağlayan en etkili güvencelerden biridir. Kişinin uğradığı bir haksızlığa veya zarara karşı kendisini savunabilmesinin ya da maruz kaldığı haksız bir uygulama veya işleme karşı haklılığını ileri sürüp kanıtlayabilmesinin, zararını giderebilmesinin etkili yolu, yargı mercileri önünde dava hakkını kullanabilmesidir.

102. Tebligat, yetkili makamlarca birtakım hukuki işlemlerin, bu işlemlerin hukuki sonuçlarından etkilenmeleri amaçlanan kişilere kanuna uygun şekilde bildirim ve bu bildirim usulüne uygun olarak yapıldığının belgelendirilmesidir. İşlemlerin kendilerine bağlanan hukuki sonuçları doğrurabilmesi için usulüne uygun olarak muhatabına bildirilmesi gerekir. Bu şekilde yapılan tebligat, Anayasa'da güvence altına alınmış olan iddia ve savunma hakkının tam olarak kullanılabilmesinin ve bireylere tanınan hak arama hürriyetinin önemli güvencelerinden biridir.

103. Kanun'un 6/A maddesinin iptali istenilen (7) numaralı fıkrasının birinci cümlesi uyarınca erişimin engellenmesi için verilen kararlar, gereğinin yerine getirilmesi için Birliğe gönderilecektir. ESB, erişim sağlayıcılar ile mahkemeler ve idare arasında koordinasyonu sağlayan bir kuruluştur. Kural ile kararların en kısa sürede yerine getirilmesi ve bu konudaki muhatap belirsizliğinin kaldırılması amaçlanmıştır. Erişim sağlayıcıların sayısının her gün artması, bunları takip etmenin ve adreslerine ulaşarak tebligat yapılmasının zorluğu hususları gözetildiğinde, sistemin en iyi şekilde işlemesi için erişimin engellenmesi kararlarının gereği için ESB'ye gönderilmesi zorunlu

bulunmaktadır. Kaldı ki ESB, yalnızca erişim sağlayıcılar ile koordinasyonu sağlamaktadır. Böyle bir düzenleme de anayasal sınırlar içinde kanun koyucunun takdir yetkisi kapsamındadır.

104. Kanun'un 6/A maddesinin iptali istenilen ikinci cümlesinde ise 5651 sayılı Kanun'un 8. maddesi kapsamı dışındaki erişimin engellenmesi kararlarının gereği için Birliğe gönderilen tebligatın, erişim sağlayıcılara yapılmış sayılacağı belirtilmektedir. Birliğe yapılan tebligat tarihi, erişim sağlayıcıya yapılmış tebligat tarihi sayılmaktadır. 5651 sayılı Kanun'un 9. maddesinin (8) numaralı fıkrası ve 9/A maddesinin (3) numaralı fıkrası uyarınca erişim sağlayıcılar, bu kararları en geç dört saat içinde yerine getirmekle görevlidir.

105. Kişi hak ve özgürlüklerinin zarar görmesinin engellenmesi amacıyla erişimin engellenmesi kararlarının yerine getirilmesinde ortaya çıkacak gecikme, telafisi imkânsız sonuçlara yol açabilecektir. Bu nedenle, erişimin engellenmesi kararlarının en kısa sürede yerine getirilmesi gerekmektedir. Bunu sağlamak için iptali istenilen kural ile ESB'ne yapılan tebligatın erişim sağlayıcılara yapılmış sayılacağı kabul edilmiştir. Getirilen sistem ile mahkemelerce ve idare tarafından verilen kararlar ESB'ye elektronik ortamda doğrudan iletilmekte, ESB de erişim sağlayıcılar ile kurmuş olduğu sistem üzerinden, bu kararları aynı anda erişim sağlayıcıların bildirilen elektronik adreslerine iletmektedir. Söz konusu tebligatın erişim sağlayıcılara ulaştığı da sistemden görülmektedir. Yapılan işin özelliği gereği en kısa sürede yerine getirilmesinin gerekmesi, teknolojik alanda meydana gelen hızlı değişim, ESB'nin ve erişim sağlayıcıların söz konusu tebligattan haberdar olduklarının tespit edilebilmesi hususları göz önüne alındığında iptali istenilen düzenlemeler kanun koyucunun takdir yetkisi kapsamında olup, kuralların hukuki güvenlik ilkesine ve hak arama özgürlüğüne aykırı olduğu söylenemez.

106. Açıklanan nedenlerle kurallar, Anayasa'nın 2., 36. ve 40. maddelerine aykırı değildir. İptal taleplerinin reddi gerekir.

107. Erdal TERCAN, Kanun'un 6/A maddesinin (7) numaralı fıkrasının ikinci cümlesi yönünden bu görüşe katılmamıştır.

H- Kanun'un 93. Maddesiyle 5651 Sayılı Kanun'un Değiştirilen 9. Maddesinin (9) Numaralı Fıkrasının İncelenmesi

1- İptal Talebinin Gerekçesi

108. Dava dilekçesinde özetle, Kanun'un 6/A maddesi kapsamında belirtilen gerekçelerle kuralın, Anayasa'nın 2., 33., 36. ve 40. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

109. 6216 sayılı Kanun'un 43. maddesi uyarınca, iptali istenilen kural ilgisi nedeniyle Anayasa'nın 13. ve 26. maddeleri yönünden de incelenmiştir.

110. Kanun'un 9. maddesinin iptali istenilen (9) numaralı fıkrasında, anılan madde kapsamında hâkimin verdiği erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının veya aynı mahiyetteki yayınların başka internet adreslerinde de yayınlanması durumunda ilgili kişi tarafından Birliğe müracaat edilmesi halinde mevcut kararın bu adresler için de uygulanacağı öngörülmektedir.

111. Anayasa'nın "Düşünceyi açıklama ve yayma hürriyeti" başlıklı 26. maddesinin birinci fıkrasında, "Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Bu fıkra hükmü, radyo, televizyon, sinema veya benzeri yollarla yapılan yayımların izin sistemine bağlanmasına engel değildir." denilerek düşünceyi açıklama ve yayma hürriyetinin kapsamı belirtilmiştir.

112. Anayasa'nın 26. maddesinde düzenlenen "düşünceyi açıklama ve yayma hürriyeti"nin sınırları ise maddenin ikinci fıkrasında düzenlenmiştir. Buna göre, bu özgürlüğün kullanılması, millî güvenlik, kamu düzeni, kamu güvenliği, Cumhuriyetin temel nitelikleri ve Devletin ülkesi ve milleti ile bölünmez bütünlüğünün korunması, suçların önlenmesi, suçluların cezalandırılması, Devlet sırrı olarak usulünce belirtilmiş bilgilerin açıklanmaması, başkalarının şöhret veya haklarının, özel ve aile hayatlarının yahut kanunun öngördüğü meslek sırlarının korunması veya yargılama görevinin gereğine uygun olarak yerine getirilmesi amaçlarıyla sınırlanabilir.

113. Anılan düzenlemeler uyarınca ifade özgürlüğü, sadece "düşünce ve kanaate sahip olma" özgürlüğünü değil, aynı zamanda sahip olunan "düşünce ve kanaati (görüşü) açıklama ve yayma", buna bağlı olarak "haber veya görüş alma ve verme" özgürlüklerini de kapsamaktadır. Bu çerçevede ifade özgürlüğü bireylerin serbestçe haber ve bilgilere, başkalarının fikirlerine ulaşabilmesi, edindiği düşünce ve kanaatlerden dolayı kınanmaması ve bunları tek başına veya başkalarıyla birlikte çeşitli yollarla serbestçe ifade edebilmesi, anlatabilmesi, savunabilmesi, başkalarına aktarabilmesi ve yayabilmesi anlamına gelir.

114. Anayasa'nın 26. maddesinde düşünceyi açıklama ve yayma özgürlüğünün kullanımında başvurulabilecek araçlar "söz, yazı, resim veya başka yollar" olarak ifade edilmiş ve "başka yollar" ifadesiyle her türlü ifade aracının anayasal koruma altında olduğu gösterilmiştir.

115. Öte yandan, düşünceyi açıklama ve yayma özgürlüğü mutlak ve sınırsız değildir. Nitekim Anayasa'nın 26. ve 28. maddelerinin koruma altına aldığı düşünceyi açıklama ve yayma hürriyeti Anayasa'nın 13. maddesindeki koşullara uygun olarak, bu maddelerde belirtilen sebeplerle sınırlandırılabilir. Anayasa'nın 13. maddesine göre temel hak ve özgürlüklere yönelik sınırlamalar ancak kanunla yapılabilir ve demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamayacağı gibi hak ve özgürlüklerin özlerine de dokunamaz.

116. İnternet, modern demokrasilerde başta ifade özgürlüğü olmak üzere temel hak ve özgürlüklerin kullanılması bakımından önemli bir değere sahip bulunmaktadır. Sosyal medya, medya içeriğini oluşturmak, yayınlamak ve yorumlamak şeklinde bireysel katılıma imkân veren şeffaf ve karşılıklı iletişim kurulan bir platform şeklindeki medya kanalıdır. İnternetin sağladığı sosyal medya zemini, kişilerin bilgi ve düşüncelerini açıklama, paylaşma ve yaymaları için vazgeçilemez niteliktedir.

117. Bir internet sitesine erişimin engellenmesine karar verildiği hallerde hukuk devletinin önkoşullarından olan hukuki güvenlik ve hukuki belirlilik ilkelerinin göz önünde bulundurulması zorunludur.

118. İptali istenilen kural uyarınca, erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının aynısı ya da aynı mahiyetteki yayının başka internet adreslerinde de yayınlaması durumunda Birlik, bir değerlendirme yapacak ve yargı organınca yeni bir karar alınmaksızın, ilgili kişinin Birliğe müracaat etmesi halinde hâkimin vermiş olduğu karar, bu adresler için de uygulanacaktır.

119. Hâkimin verdiği erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının aynısının bir başka internet adresinde yayınlaması durumunda Birlik tarafından kararın bu adresler için de uygulanmasında sorun bulunmamaktadır. Bu durumda mevcut kararın bu adresler için de uygulanması, söz konusu hâkim kararının yerine getirilmesinden ibarettir. Çünkü belirtilen yayının kişilik hakkını ihlal ettiği mahkeme tarafından tespit edilmiş durumdadır. Birliğin burada yapacağı şey, söz konusu yayının aynı olup olmadığını ve ihlale konu yayının belirtilen internet adresinde aynen veya bir parçasının yayınlanıp yayınlanmadığını belirlemekten ibarettir. Ayrıca, hâkim kararını etkisiz kılacak şekilde çok küçük değişiklikler yapılmak suretiyle aynı eylemin gerçekleştirilmesi halinde de ihlale konu yayının aynı olduğu kabul edilmelidir. Burada Birlik tarafından hukuki bir değerlendirme yapılması söz konusu olmayıp maddi olay tespit edilecektir. Bu durumda da erişimin engellenmesi kararının uygulanacağı yayın, daha önce hâkim kararıyla tespit edilmiş olduğundan herhangi bir belirsizlikten bahsedilemeyeceği gibi ifade hürriyetinin keyfi veya ölçüsüz şekilde sınırlandırılmasından da söz edilemez.

120. Ancak, hâkimin 9. madde kapsamında verdiği erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin "aynı mahiyetteki yayınların" başka internet adreslerinde yayınlanması durumunda ilgili kişinin Birliğe başvurması halinde bunun tespiti de Birliğe bırakılmaktadır. Aynı mahiyetin tespiti, yayının aynı olmasından farklı olup, bu yayının içeriğinin değerlendirilmesini gerektirmektedir. "Aynı mahiyetteki yayınlar", hâkimin vermiş olduğu erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayın ile aynı olmayan, ancak yöneldiği sonuç bakımından ilgilinin kişilik hakkını ihlal edebilecek mahiyette olan yayınlardır. Kişilik hakkının kapsamı ve hangi eylemlerin kişilik hakkını ihlal ettiği ise ilgili tarafların toplumsal, ekonomik, siyasal ve hukuki konuları, söz konusu yayının ulaştığı kitle ve bu yayının ifade özgürlüğü kapsamında bulunup bulunmadığı gibi birçok hukuki konunun değerlendirilmesini ve buna göre karar verilmesini gerektirmektedir. Bu kapsamda iptali istenilen kuralla aynı mahiyetteki yayınların ESB'ye erişimin engellenmesine yönelik olarak verilen yetki, kanunilik ilkesinin asgari şartı olan kanunun anlaşılır, açık ve net olması zorunluluğunu karşılamadığı gibi kapsam ve sınırları da belirsizdir. Kural "aynı mahiyetteki yayınlar" yönünden belirli ve öngörülebilir değildir.

121. Öte yandan, Birlik tarafından hakimın verdiği erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin aynı mahiyetteki yayınların başka internet sitesinde yayınlanması halinde bu siteler hakkında da erişimin engellenmesi kararının uygulanması, bu sitelerden yararlanılmasını engellediğinden ifade özgürlüğünü de ölçüsüzce sınırlandırmaktadır.

122. Açıklanan nedenlerle iptali istenilen kuralda yer alan ".veya aynı mahiyetteki yayınların." ibaresi, Anayasa'nın 2., 13. ve 26. maddelerine aykırıdır. İptali gerekir.

123. Kuralın kalan bölümü ise Anayasa'nın 2., 13. ve 26. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

124. Serdar ÖZGÜLDÜR kuralda yer alan "...veya aynı mahiyetteki yayınların..." ibaresinin iptali ile ilgili sonuca farklı gerekçe ile katılmış, kuralın "...veya aynı mahiyetteki yayınların..." ibaresi dışında kalan bölümü için bu görüşe katılmamıştır.

125. Hicabi DURSUN, Kadir ÖZKAYA ile Rıdvan GÜLEÇ kuralda yer alan "...veya aynı mahiyetteki yayınların..." ibaresinin iptali ile ilgili bu görüşe katılmamışlardır.

126. Kuralın Anayasa'nın 33., 36. ve 40. maddeleriyle bir ilgisi görülmemiştir.

I- Kanun'un 100. Maddesiyle, 5651 sayılı Kanun'a Eklenen Geçici 3. Maddesinin (2) Numaralı Fıkrasının Birinci Cümlesinin İncelenmesi

127. 5651 sayılı Kanun'a 6518 sayılı Kanun'un 100. maddesiyle eklenen geçici 3. maddenin ikinci fıkrasının birinci cümlesi, 27.3.2015 tarihli, 6639 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun'un 30. maddesiyle değiştirilmiştir.

128. Bu nedenle, konusu kalmayan bu cümleye ilişkin iptal talebi hakkında karar verilmesine yer olmadığına karar verilmesi gerekir.

İ- Kanun'un 85. Maddesiyle, 5651 Sayılı Kanun'un 2. Maddesinin (1) Numaralı Fıkrasına Eklenen (o) Bendinde Yer Alan "...ve benzeri yöntemler kullanılarak..." İbaresinin İncelenmesi

1- İptal Talebinin Gerekçesi

129. Dava dilekçesinde özetle, erişimin engellenmesi tanımıyla erişimin engellenmesi sırasında kimi yöntemlerden "benzeri yöntemler" olarak söz edilmesinin 5651 sayılı Kanun'un amacı ve kapsamı ile çeliştiği ve hukuki belirsizliğe sebebiyet verdiği, internet ortamında yapılan yayınların düzenlenmesi, içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin normların açık, anlaşılabilir ve sınırları belirli kurallar içermesi gerektiği belirtilerek kuralın, Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

130. İptali istenilen ibarenin bulunduğu kuralda erişimin engellenmesinin tanımı yapılarak, erişimin engellenmesinin, alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi ve benzeri yöntemler kullanılarak erişimin engellenmesini ifade ettiği belirtilmektedir. İptali istenilen kural "...ve benzeri yöntemler kullanılarak..." ibaresidir.

131. Anayasa'nın 2. maddesinde yer alan hukuk devletinin temel ilkelerinden biri "belirlilik"tir. Bu ilkeye göre, yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olması, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi de gereklidir. Belirlilik ilkesi, hukuksal güvenlikle bağlantılı olup birey, yasadın, belirli bir kesinlik içinde, hangi somut eylem ve olguya hangi hukuksal yaptırımın veya sonucun bağlandığını, bunların idareye hangi müdahale yetkisini doğurduğunu bilmelidir. Ancak bu durumda kendisine düşen yükümlülükleri öngörebilir ve davranışlarını ayarlayabilir. Hukuk güvenliği, normların öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar.

132. Erişim engelleme, internet ortamında yayın yapan bir siteye girişin çeşitli yöntemlerle önlenmesidir. Başka bir ifadeyle, çeşitli tekniklerle kullanıcıların bir internet sitesine ulaşımının engellenmesidir. İnternet sitelerine erişimin engellenmesi için kullanılan tek bir yöntem bulunmamaktadır. Engellemenin kapsamı, kullanılan teknik, engelleme süresi, engelleme öncesi ve sonrası takip edilen süreç teknolojik gelişmeye göre değişmektedir.

133. Kanun koyucu, toplumsal ihtiyaçlar doğrultusunda internet faaliyetleri konusundaki gelişmeleri gözeterek düzenleme yapma yetkisine sahiptir. Ancak, kanun koyucunun hukuki düzenlemelerde kendisine tanınan bu takdir yetkisini anayasal sınırlar içinde adalet, hakkaniyet ve kamu yararı ölçütlerini göz önünde tutarak kullanması gerekir.

134. Gelişen koşul ve durumlara göre sık sık değişik önlemler alma, bunları kaldırma ve süratli biçimde hareket etme zorunluluğunun bulunduğu alanlarda, yasama organının temel kuralları saptadıktan sonra, uzmanlık ve idare tekniğine ilişkin hususları yürütmeye bırakması, yasama yetkisinin devri olarak yorumlanamayacağı gibi yürütme organının yasama organı tarafından çerçevesi çizilmiş alanda ve değişen koşullara uyum sağlayabilecek esnekliğe sahip kriterlere uygun olarak, genel nitelikte hukuksal tasarruflarda bulunması, hukuk devletinin belirlilik ilkesine de aykırı olarak değerlendirilemez.

135. İptali istenilen ibarenin bulunduğu kuralın, internet ortamındaki gelişmelerin dinamik ve değişken olması gözetilerek, meydana gelen bilimsel ve teknolojik gelişmelerden faydalanmak suretiyle değişen koşullara uyularak erişimin engellenmesinin yapılabilmesi için kamu yararı amacıyla getirildiği anlaşılmıştır.

136. İptali istenilen ibarenin bulunduğu kuralda, erişimin engellenmesinin tanımı yapılırken alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi yöntemleri sayılmış ve devamında "...ve benzeri yöntemler kullanılarak..." erişimin engellenebileceği belirtilmiştir. Erişimin engellenmesi usulleri, özel bir uzmanlık ve teknik bilgi isteyen, hızlı, teknolojik ve bilimsel gelişmeler karşısında çok hızlı değişen ve gelişen tekniklerdir. Bu nedenle, bu tedbirlerin neler olduğunun kanun koyucu tarafından önceden tek tek belirlenmesi mümkün değildir. Kanun koyucunun erişimin engellenmesi yöntemlerini açık bir şekilde saydıktan sonra bu engelleme yöntemlerine benzer biçimde yapılan erişimin engellenmesini de bu kapsamda değerlendirmesinde hukuk devletine aykırılık bulunmamaktadır. Dolayısıyla, "... ve benzeri yöntemler kullanılarak..." ibaresinin belirsiz olduğundan ve keyfi uygulamalara yol açacağından söz edilemez.

137. Açıklanan nedenlerle kural, Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

J- Kanun'un 85. Maddesiyle 5651 Sayılı Kanun'un 2. Maddesinin (1) Numaralı Fıkrasına Eklenen (r) Bendinin İncelenmesi

1- İptal Talebinin Gerekçesi

138. Dava dilekçesinde özetle, gerek yurt içinde gerekse yurt dışında faaliyet yürütenlere internet sayfalarında bulunan e-mail adreslerinden geçerli tebligat yapılabilmesine olanak sağlayan düzenlemenin ülkemizin tebligat mevzuatına aykırı olduğu gibi uluslararası anlaşmalarla korunan hukuki menfaatleri ve tebligat güvenliğini de zedelediği, hukuk devleti ilkesiyle çeliştiği, 5651 sayılı Kanun kapsamındaki faaliyetleri yurt içinden veya yurt dışından yürütenlere internet sayfalarındaki iletişim araçları, alan adı, IP adresi ve benzeri kaynaklarla elde edilen bilgiler üzerinden elektronik posta yoluyla bildirim yapılması durumunda, gönderilen e-mailin gidip gitmediği, muhatabına ulaşip ulaşmadığı, ulaştı ise ne zaman görülüp açıldığı, açıldı ise tebellüğ yetkisine sahip olanlar tarafından alınıp alınmadığı hususları yanında, ayrıca yurt dışında bulunan hizmet sağlayıcısının tabi olduğu kamu hukukunu ihlal edebilecek bir düzenleme olduğu, 6518 sayılı Kanun'un 86. maddesiyle 5651 sayılı Kanun'un 3. maddesine eklenen üçüncü fıkranın Anayasa'ya aykırılığının, bu düzenlemenin Kanun metninde ifadesini bulduğu Kanun'un 2. maddesinin birinci fıkrasına eklenen (r) bendinin de kaçınılmaz bir biçimde sakatlanması ve Anayasa'ya aykırı olması sonucunu doğuracağı, ayrıca bu şekilde bir uygulamanın birçok hukuki sürecin ilgili tarafın haberi olmadan başlayabileceği anlamını taşıdığı gibi hak arama hürriyetini ciddi bir şekilde tehdit edebileceği, birçok durumda, idari eylem ve işlemlerin muhatabı olan kişilerin dava, itiraz v.s. süreleri kaçırabileceği ve hak arama özgürlüğünden mahrum kalacakları, hak arama hürriyeti ihlalinin beraberinde Anayasa'nın 40. maddesinin ihlal edilmesi sonucunu doğuracağı, iptali istenilen kurallar ile hak arama hürriyetinin ihlali halinde idari işlemlerin muhataplarının yetkili makama geciktirilmeden başvurma imkanının sağlanmasını isteme hakkının tanınmadığı ve anılan hükümlerle ilgili kişilerin hangi kanun yolları ve mercilere başvuracağına ve süresine yer verilmediği belirtilerek kuralın, Anayasa'nın 2., 36. ve 40. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

139. Kanun'un 2. maddesinin (1) numaralı fıkrasının iptali istenilen (r) bendinde, uyarı yöntemi tanımlanmış ve uyarı yönteminin; internet ortamında yapılan yayın içeriği nedeniyle haklarının ihlal edildiğini iddia eden kişiler tarafından içeriğin yayından çıkarılması amacıyla, öncelikle içerik

sağlayıcısına, makul sürede sonuç alınamaması hâlinde yer sağlayıcısına, iletişim adresleri üzerinden gerçekleştirilecek bildirim yöntemini ifade ettiği belirtilmiştir.

140. Uyarı yöntemi, Kanun'un 9. maddesinin (1) numaralı fıkrası ile ilgili bulunmakta ve bu fıkroda; internet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşların, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğe erişimin engellenmesini de isteyebileceği öngörülmektedir. İptali istenilen kural da, uyarı yönteminin nasıl yapılacağına ilişkin bir hükümdür.

141. Kanun'un 2. maddesinin (r) bendinde belirtilen uyarı yönteminde, kişilik haklarının ihlal edildiğini iddia eden kişiler, içeriğin yayından çıkarılması amacıyla öncelikle içerik sağlayıcısına, makul sürede sonuç alınamaması hâlinde yer sağlayıcısına iletişim adresleri üzerinden başvuracaklardır. Kanun'un 9. maddesinin (2) numaralı fıkrasında yer alan, "İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişilerin talepleri, içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılır." hükmü karşısında içerik ve (veya) yer sağlayıcısı, içeriğin yayından çıkarılması talebini 24 saat içinde cevaplamalıdır. İçerik ve yer sağlayıcısına başvurma hakkı zorunlu bir hak olmayıp, kişilik hakkının ihlal edildiğini iddia eden kişi, içeriğe erişimin engellenmesini doğrudan sulh ceza hâkimine başvurarak da isteyebilir.

142. İptali istenilen kuralda, yetkili makamlarca yapılacak bir bildirimden değil, internet ortamında yapılan yayın içeriği nedeniyle, haklarının ihlal edildiğini iddia eden kişiler tarafından yapılacak, içeriğin yayından çıkarılmasına ilişkin bir bildirim yönteminden bahsedilmekte ve bu bildirim içerik veya yer sağlayıcıların iletişim adreslerine yapılacağı öngörülmektedir. Kişilik haklarının ihlal edildiğini iddia eden kişilerin uyarı yöntemine başvurma zorunluluğu bulunmamakta, bu kişilerin içerik veya yer sağlayıcılara başvurmadan doğrudan sulh ceza hâkimine başvurarak içeriğin yayından kaldırılmasını talep etme hakları da bulunmaktadır. Dolayısıyla, söz konusu hüküm sebebiyle yapılacak bildirim sonucunda kişilerin hak arama özgürlüğünü olumsuz etkileyecek bir durum söz konusu değildir.

143. Öte yandan, Kanun'un 2. maddesinin (r) bendinde belirtilen "uyarı yöntemi"ne ilişkin tanımda, kişilik haklarının ihlal edildiğini iddia eden kişiler tarafından içerik ve yer sağlayıcısının iletişim adresleri üzerinden bildirim yapmaları öngörülmektedir. İletişim adresi ise içerik ve yer sağlayıcıya ulaşılacak belli adresler olup bu hususta düzenleme yapılması anayasal sınırlar içinde kanun koyucunun takdir yetkisi kapsamındadır.

144. Açıklanan nedenlerle kural, Anayasa'nın 2. ve 36. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

145. Kuralın Anayasa'nın 40. maddesiyle bir ilgisi görülmemiştir.

K- Kanun'un 86. Maddesiyle 5651 Sayılı Kanun'un 3. Maddesine Eklenen (3) Numaralı Fıkranın İncelenmesi

1- İptal Talebinin Gerekçesi

146. Dava dilekçesinde özetle, Kanun'un 2. maddesinin (1) numaralı fıkrasının (r) bendi kapsamında belirtilen gerekçelerle kuralın, Anayasa'nın 2., 36. ve 40. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

147. Kanun'un 3. maddesinin iptali istenilen (3) numaralı fıkrasında, Kanun kapsamındaki faaliyetleri yurt içinden ya da yurt dışından yürütenlere, internet sayfalarındaki iletişim araçları, alan adı, IP adresi ve benzeri kaynaklarla elde edilen bilgiler üzerinden elektronik posta veya diğer iletişim araçları ile bildirim yapılabileceği öngörülmüştür.

148. Günümüzde elektronik sistem oldukça yaygınlaşmış ve hayatın her alanında kullanılır hale gelmiştir. Gelişen teknolojiye uygun olarak tebligatlarda da elektronik ortamın kullanılması gündeme gelmekte, hatta bazı alanlarda elektronik tebligatın uygulanması zorunluluğunu gerektirmektedir.

149. 5651 sayılı Kanun'un 1. maddesinde bu Kanun'un amaç ve kapsamının, içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlara içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemek olduğu belirtilmiştir. İptali istenilen kural ile de 5651 sayılı Kanun kapsamındaki faaliyetleri yurt içinden ya da yurt dışından yürütenlere elektronik ortamda veya diğer iletişim araçları ile bildirim yapılabileceği öngörülmüştür. Kanun'un 3. maddesinin (1) numaralı fıkrasında, içerik, yer ve erişim sağlayıcılarının yönetmelikle belirlenen esas ve usuller çerçevesinde tanıtıcı bilgilerini kendilerine ait internet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlü oldukları, aynı maddenin (2) numaralı fıkrası uyarınca da bu yükümlülüğü yerine getirmeyen içerik, yer ve erişim sağlayıcısına Başkanlık tarafından idari para cezası verileceği belirtilmiştir. Bu madde kapsamında yer alan içerik, yer, erişim ve toplu kullanım sağlayıcılar belirtilen hüküm gereği kendilerine ulaşılacak şekilde tanıtım bilgilerini internet sayfasında güncel olarak bulundurmakla zorunludurlar.

150. İçerik, yer, erişim ve toplu kullanım sağlayıcıların yapmış oldukları işin bilişim sistemine ait olması, yerine getirdikleri hizmetler açısından yapılacak bildirimlerin en kısa sürede kendilerine ulaşmasının gerekmesi, teknolojik alanda meydana gelen hızlı değişim ve bilişim sistemlerinin ilerlemesi göz önüne alındığında iptali istenilen kuralın bu kişilere yapılacak bildirim en hızlı ve en kısa sürede gerçekleştirilmesini sağlamak için kamu yararı amacına yönelik olarak çıkarıldığı anlaşılmaktadır.

151. Kuralda belirtilen kişilere elektronik posta veya diğer iletişim araçları ile yapılabilecek olan bildirim, kendilerine ulaştığının tespit edilebilmesi karşısında, iptali istenilen kuralda hukuki güvenlik ilkesine ve hak arama özgürlüğüne aykırılık bulunmamaktadır.

152. Öte yandan, içerik, yer, erişim ve toplu kullanım sağlayıcılara elektronik posta ile yapılacak olan bildirimler, internet sayfalarındaki iletişim araçları, alan adı, IP adresi ve benzeri kaynaklarla elde edilen bilgiler üzerinden yapılabilecektir. İptali istenilen kuralda, benzeri kaynaklarla elde edilen bilgiler üzerinden elektronik posta ile bildirim yapılabilmesinin belirtilmesinin, yeni teknolojik gelişmelerin ortaya çıkması halinde değişen koşullara uyum sağlanarak bildirim yapılabilmesine olanak sağlanması amacıyla yapıldığı anlaşılmaktadır. Benzeri kaynaklarla elde edilen bilgilerden kastedilenin ise kuralda sayılan internet sayfalarındaki iletişim araçları, alan adı, IP adresi gibi internetten belirlenebilecek hususlar olduğu açıktır. Bu nedenle, kuralın bu yönüyle belirsiz olduğundan söz edilemez.

153. Açıklanan nedenlerle kural, Anayasa'nın 2., ve 36. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

154. Kuralın Anayasa'nın 40. maddesiyle bir ilgisi görülmemiştir.

L- Kanun'un 87. Maddesiyle 5651 Sayılı Kanun'un 4. Maddesine Eklenen (3) Numaralı Fıkranın ve Kanun'un 88. Maddesiyle 5651 Sayılı Kanun'un 5. Maddesine Eklenen (5) Numaralı Fıkranın ve Kanun'un 89. Maddesi ile 5651 Sayılı Kanunun 6. Maddesinin (1) Numaralı Fıkrasına Eklenen (d) Bendinin İncelenmesi

1- İptal Taleplerinin Gerekçeleri

155. Dava dilekçesinde özetle, iptali istenilen hükümlerin, Telekomünikasyon İletişim Başkanlığı'nın, tüm internet kullanıcılarının iletişim verilerinin, herhangi bir hukuki sınırlama veya engelleme olmadan toplamasını mümkün hale getirmek için düzenlendiği, tüm bu süreç boyunca kısıtlamanın muhatabı olan kişilerin hiçbir şekilde bilgi akışından haberinin olmayacağı, idarenin tamamen keyfi olarak verdiği bu karar nedeniyle zarar görecektir kişilerin itiraz etmesinin mümkün olmadığı gibi yer

ve erişim sağlayıcının da bu karara itiraz etmekte bir menfaatinin bulunmadığı, özel hayata müdahaleye sebep olacak bu uygulamanın hak arama hürriyetini ortadan kaldırmasının ötesinde, Avrupa İnsan Hakları Sözleşmesi'nin 13. maddesinde öngörülen etkili başvuru yolunu kullanılamaz hale getirdiği, iptali istenilen kuralların Anayasa'nın "Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir." kuralına çok açık bir biçimde aykırılık teşkil ettiği, ".kanunda öngörülen haller"in nelerden ibaret olduğunun 6518 sayılı Kanun'un hiçbir maddesinde belirtilmediği, öte yandan Telekomünikasyon İletişim Başkanlığı (TİB) tarafından içerik (yer ve erişim) sağlayıcısından talep edilecek olan bilgilerin mahiyetinin belirsiz olmasının yanı sıra, talep yönteminin de net ve sarih olmadığı, bilginin hassas bilgi, şahsi bilgi, gizli bilgi, ticari sır gibi çeşitli türlerinin bulunduğu, bu tür bilgilerin hangisinin hangi yöntemlerle talep edileceğinin kişisel hakların, mahremiyetin ve özel hayatın gizliliğinin korunması için elzem olduğu, iptali istenilen hükümlerde Başkanlıkça bildirilen tedbirleri almakla yükümlü olduğu öngörülse de bu tedbirlerin ne olduğunun açıklanmadığı, dolayısı ile belirsiz olduğu, Anayasa'nın 13. maddesine göre, temel hak ve hürriyetlerin ancak kanunla sınırlanabileceği, oysa iptali istenilen kurallarda içerik, yer ve erişim sağlayıcılar tarafından, talebi halinde Başkanlığa teslim edilecek kişisel bilgilere Başkanlığın erişimini sınırlandıracak herhangi bir düzenlemeye yer verilmediği, temel bir hakka müdahale niteliğindeki bir işlemin objektif olarak amaçlanan kamu yararını gerçekleştirmeye elverişli ve bu amaç doğrultusunda zorunlu olmasının gerektiği, iptali istenilen hükümler uyarınca içerik, yer ve erişim sağlayıcıları TİB'in talep ettiği özel hayata ilişkin bütün bilgiler de dahil olmak üzere her türlü bilgiyi Başkanlığa teslim etmek zorunda olduklarından hak arama hürriyetinin ortadan kaldırıldığı, bu anayasal hakkı ihlal edilenlerin hangi kanun yollarını kullanarak, hangi mercilere başvuracağı ve sürelerinin gösterilmediği belirtilerek kuralların, Anayasa'nın 2., 13., 20., 36. ve 40. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

156. Kanun'un 4. maddesinin (3) numaralı fıkrasında, içerik sağlayıcının, Telekomünikasyon İletişim Başkanlığının, bu Kanun ve diğer kanunlarla verilen görevlerinin ifası kapsamında talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim edeceği ve Başkanlıkça bildirilen tedbirleri alacağı öngörülmektedir.

157. Kanun'un 5. maddesinin (5) numaralı fıkrası ile 6. maddesinin (1) numaralı fıkrasının (d) bendinde ise, yer ve erişim sağlayıcıların Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla yükümlü oldukları belirtilmektedir. Söz konusu kurallarda Kanun'un 4. maddesinin (3) numaralı fıkrasında belirtilen

"Başkanlığın bu Kanun ve diğer kanunlarla verilen görevlerinin ifası kapsamında" ibaresi yer almamaktadır.

158. İptali istenilen kurallar uyarınca içerik, yer ve erişim sağlayıcılar, TİB tarafından talep edilen bilgileri talep edildiği şekilde TİB'e teslim etmekle ve TİB tarafından bildirilen tedbirleri almakla yükümlü tutulmuşlardır.

159. Anayasa'nın 20. maddesinin ilk fıkrasında, herkesin, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş; son fıkrasında da, herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı ifade edilmiştir. Maddede ayrıca kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hükmüne de yer verilmiştir. Madde gerekçesinde de, özel hayatın korunmasının her şeyden önce bu hayatın gizliliğinin korunması, resmi makamların özel hayata müdahale edememesi anlamına geldiği belirtilmiştir.

160. Özel hayatın gizliliği ve korunması özgürlüğünün kullanılması demokratik bir toplumda, Anayasa'nın ilgili maddelerinde belirtilen nedenlere bağlı olarak, kanunla, belli koşullara, sınırlamalara bağlanabilir. Ancak, getirilen ve zorunlu tedbir niteliğinde olan bu sınırlamalar Anayasa'nın 13. maddesinde yer alan güvencelere aykırı olamaz.

161. Temel hak ve özgürlüklere getirilen sınırlamalar hakların özüne dokunamaz. Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamaz. Anayasal açıdan dokunulamayacak öz, her temel hak ve özgürlük açısından farklılık göstermekle birlikte kanunla getirilen sınırlamanın hakkın özüne dokunmadığının kabulü için temel hakların kullanılmasını ciddi surette güçleştirip, amacına ulaşmasına engel olmaması ve etkisini ortadan kaldıracı bir nitelik taşımaması gerekir.

162. Anayasa'nın 13. maddesinde yer alan ölçülülük ilkesi, amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder. Ölçülülük, aynı zamanda yasal önlemin sınırlama amacına ulaşmaya elverişli olmasını, amaç ve aracın ölçülü bir oranı kapsamamasını ve sınırlayıcı önlemin demokratik toplum düzeni bakımından zorunluluk taşımasını da içeren bir ilkedir.

163. Anayasa'da güvence altına alınan haklara kamu gücü tarafından bir sınırlama imkânı getirildiği hâllerde ilgili Kanun'da böyle bir yetkinin kullanılmasına ilişkin kapsam ve usullerin yeterli bir açıklıkla belirtilmesi gerekmektedir.

164. İptali istenen kurallarda geçen "bilgi" kelimesi en kısa tanımıyla "işlenmiş veri"dir. Kişisel veri kavramı ise belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Dolayısıyla iptali istenilen kurallarda geçen bilgi kelimesi kişisel verileri de kapsamaktadır. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Ancak söz konusu hak sınırsız değildir. Kişisel verilerin korunması hakkı, veri sahibinin mutlak ve sınırsız bir veri hâkimiyetini mümkün kılmamaktadır. Nitekim Türkiye'nin imzaladığı ancak uygulama kanununun yürürlüğe konmaması nedeniyle taraf olmadığı 1981 tarihli ve 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Avrupa Konseyi Sözleşmesi'nin 9. maddesinde de devlet güvenliği, kamu güvenliği, devletin ekonomik menfaatlerinin korunması ve suçlarla mücadele edilmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması ile verilerin istatistiki veya bilimsel amaçlarla kullanılması durumlarında, kişisel verilerin korunmasına sınırlamalar getirilebileceği öngörülmüştür.

165. Bilgi ve iletişim teknolojileri sayesinde, kişisel verilerin derleme, sınıflandırma, saklama işlemlerine tabi tutulması ve istendiğinde kolayca sunulabilmesi kolaylaşmış ve bunun sonucunda özel yaşamla ilgili bu bilgilerin haksız olarak kullanılması riski de ortaya çıkmıştır. Bu teknolojiler, kişisel verilerin kişinin rızası alınmadan başkalarına açıklanmasına ve bilginin bulunduğu yerden başka yerlere aktarılmasına imkân sağlamaktadır.

166. İnternet, ticaretten siyasete, basın-yayımdan devlet işlemlerine kadar hayatımızın her alanında çok yoğun kullanılan bir iletişim aracıdır. Bireylerin hak ve hürriyetlerini kullanırken devletin müdahalesine uğrayacakları endişesine sahip olmaları, bu hak ve hürriyetlerini serbestçe kullanmalarını engellemekte, bireylerin demokratik toplum düzeninin temellerini inşa etme fonksiyonunu geri dönülmez biçimde zedelemektedir. Bireyler interneti Anayasa'da tanımlı birçok hak ve hürriyetin kullanılması noktasında araçsallaştırmaktadır. Örneğin bireyler haberleşme özgürlüğünü, düşünce ve ifadeyi yayma özgürlüğünü, eğitim ve öğrenim hürriyetini, haber alma hürriyetini, iktisadi girişim hürriyetini internet yoluyla kullanabilmektedirler. Bu hürriyetlerin sınırlandırılma sebepleri de her bir hürriyeti düzenleyen Anayasa hükmünde yer almaktadır.

167. Türkiye'de telekomünikasyon yoluyla yapılan iletişimin içeriğini kontrol etmekle yükümlü TİB'in oluşturulmasındaki temel amaç, iletişimin izlenmesi ve tespit edilmesi uygulamalarında yetkileri merkezileştirmektir. 5651 sayılı Kanun'a göre TİB, internet içeriğinin izlenmesi ve denetlenmesi ile hâkim, mahkeme ve Cumhuriyet savcıları tarafından verilmiş erişim engelleme kararlarının uygulanmasından sorumludur. Ayrıca TİB, Türkiye'de bulunan belli bazı internet içeriklerine ve 8. maddede sayılan suçlar bağlamında Türkiye dışında yer alan içeriğe erişimi, bazı suçlar yönünden idari kararlar engelleme yetkisine de sahiptir. TİB'in ayrıca internetteki içerik izleme sistemlerinin yapısı, zamanlaması ve yöntemlerini, filtreleme, engelleme ve izleme için kullanılacak yazılım ya da donanımın üretimine ilişkin asgari ölçütleri belirleme yetkisi de vardır.

168. İptali istenilen hükümlerde yalnızca talep edilen bilgidan bahsedildiği ve bu konuda açıklayıcı bir düzenleme olmadığı için, "kişisel veri" veya "isteme bağlı veri" olarak adlandırılan, belirli veya belirlenebilir kişilerle ilgili her türlü bilgilerin TİB tarafından istenebileceği kuşkusuzdur. Yine Kanun'un 5. maddesinin (3) numaralı fıkrasında ve 6. maddesinin (1) numaralı fıkrasının (b) bendinde, yer ve erişim sağlayıcıların internet trafik bilgilerini saklama görevleri kapsamında trafik bilgilerinin de TİB tarafından istenilecek bilgi kapsamında olduğu açıktır. Bunun yanında, iptali istenilen kurallarda belirtilen yükümlülüklerini yerine getirmedikleri takdirde yer sağlayıcılar Kanun'un 5. maddesinin (6) numaralı fıkrası, erişim sağlayıcılar ise Kanun'un 6. maddenin (3) numaralı fıkrası uyarınca idari para cezaları ile cezalandırılacaklardır. Diğer yandan, madde hükümlerine göre içerik, yer ve erişim sağlayıcılar tarafından talep edilen bilgilerin verilmesinden ilgili kişilerin haberdar olmalarına ilişkin bir düzenleme de Kanun'da bulunmamaktadır. Dolayısıyla kişilerin kendileri ile ilgili bilgilerin TİB'e verilmesinden haberdar olmaları da söz konusu olmayacaktır.

169. Telekomünikasyon İletişim Başkanlığının, internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi ve kendisine verilen görevleri yerine getirebilmesi için kişisel veriler de dâhil olmak üzere bir takım bilgi ve belgelere ihtiyacının bulunması kaçınılmazdır. Ancak iptali istenilen kurallarda, TİB'in Kanun'daki görevlerini yerine getirme noktasında içerik, yer ve erişim sağlayıcılardan isteyeceği bilginin kapsamı ve getirebileceği yükümlülüklerin çerçevesi belirlenmemiş, içerik, yer ve erişim sağlayıcılardan bilgi talep etme yetkisinin kapsamı kişisel verilerin korunmasına ilişkin gerekli teminatlar sağlanarak sınırlandırılmamış ve bildirilen tedbirleri alma noktasında da kapsamı belirlenemeyen yükümlülükler yüklenmiştir. Kanun'un 4. maddesinin iptali istenilen (3) numaralı fıkrasında "Başkanlığın bu Kanun ve diğer kanunlarla verilen görevlerinin ifası kapsamında;" denilerek genel

bir belirleme yapılmıştır. Ancak bu genel belirleme, Kanun'un; iptali istenilen 5. maddesinin (5) numaralı fıkrası ile 6. maddesinin (1) numaralı fıkrasının (d) bendinde yer almamaktadır. Bu çerçevede iptali istenilen kurallarda, TİB'in hangi koşullarda ve hangi gerekçelerle istediği bilgilerin içerik, yer ve erişim sağlayıcılar tarafından Başkanlığa teslim edileceğine ya da verilen bilgilerin ne kadar süre ile TİB'de saklanacağına, talep edilen bilgilerin mahiyetine, içerik, yer ve erişim sağlayıcılara bildirilecek tedbirlere ilişkin herhangi bir belirlilik bulunmamaktadır. Kurallar bu yönleriyle belirli ve öngörülebilir değildirler.

170. Özel hayat bütün unsurlarıyla tanımlanamayacak kadar geniş bir kavram olup devletin yetkili temsilcileri tarafından ilgililer hakkında rızaları olmaksızın bilgi toplanmasının her zaman söz konusu kişinin özel hayatını ilgilendireceği kuşkusuzdur. İptali istenilen kurallar, kişinin açık rızası olmaksızın kişisel verilerine ulaşılmasına ve bu kişisel verilerin işlenip, bilgi halinde TİB'e teslim edilmesine olanak tanımaktadır. Anayasa'nın 20. maddesinin üçüncü fıkrasında "Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." denilmektedir. Anayasa'nın bu hükmünde yer alan kişisel verilerin işlenmesine ilişkin "kanunda öngörülen haller"in nelerden ibaret olduğu 5651 sayılı Kanun'da açıkça belirtilmemiştir. İptali istenilen kurallar, Anayasa'da yer alan güvenceye rağmen, kişilere ait her türlü kişisel veri, bilgi ve belgelerin konu, amaç ve kapsam bakımından yeterli sınırlamaya tabi kılınmaksızın koşulsuz olarak TİB'e verilmesine imkân tanımakta, böylece kişiler idareye karşı korumasız hale getirilmektedirler. Dolayısıyla iptali istenilen kurallar, belirli ve öngörülebilir olmadığından kişilerin kişisel verilerin korunması hakkını ölçüsüzce sınırlandırmakta ve Anayasa'nın 20. maddesine aykırılık teşkil etmektedir.

171. Açıklanan nedenlerle kurallar, Anayasa'nın 2., 13. ve 20. maddelerine aykırıdır. İptali gerekir.

172. Serruh KALELİ, Hicabi DURSUN, Muammer TOPAL, Kadir ÖZKAYA ile Rıdvan GÜLEÇ bu görüşe katılmamışlardır.

173. Kuralların Anayasa'nın 36. ve 40. maddeleri ile bir ilgisi görülmemiştir.

M- Kanun'un 88. Maddesiyle, 5651 Sayılı Kanun'un 5. Maddesine Eklenen (3) Numaralı Fıkranın İncelenmesi

1- İptal Talebinin Gerekçesi

174. Dava dilekçesinde özetle, Kanun'un 5. maddesinin (3) numaralı fıkrasında öngörülen saklama süresinin uluslararası ve Avrupa hukuku düzenlemelerine nazaran uzun ve geniş kapsamlı olmasına ek olarak saklanan verilerin güvenliği ile ilgili herhangi bir önleme de işaret edilmemiş olmasının

ifade özgürlüğü ve özel yaşamın gizliliği açısından ciddi bir tehlike doğurduğu, ifade özgürlüğü açısından bu bilgilerin her an erişime açık bir şekilde saklanması, muhalif görüşlerin özel alanda dahi ifade edilmesini engelleyecek boyutta bir otosansür uygulamasına ve korku toplumuna yol açabilecek nitelikte olduğu, kanun değişiklikleriyle verilerin saklanması ile ilgili yeterli korumanın getirilmemiş olmasının özel hayatın gizliliğinin, yalnızca kamuya mal olmuş insanların ve bilgiye erişim hakkının önüne geçebildiği ölçüde gündeme getirildiği izlenimini verdiği, anılan düzenlemenin internet erişim sağlayıcılarının üzerinde mali bir yük oluşturacağı ve internet kullanım maliyetlerini artıracacağı, iptali istenilen kuralla yer sağlayıcı yönünden getirilen yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklama ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlama yükümlüğünün belirli ve öngörülebilir kurallara bağlanmaksızın idareye yetki verilmesi suretiyle sağlanmaya çalışıldığı, süreleri belirleme yetkisinin genel, sınırsız, esasları ve çerçevesi belirsiz şekilde idareye bırakılmasının yasama yetkisinin devri niteliğinde olduğu, Anayasa'nın 13. maddesine göre temel hak ve özgürlüklere ilişkin sınırlandırmaların kanunla öngörülmesi ve sınırlamaların kanuna uygun olması gerektiği prensibi nazara alındığında, yer sağlayıcıya, yer sağladığı hizmetlere ilişkin trafik bilgilerini saklama ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlama yükümlülüğüne ilişkin sürenin belirlenmesinin yönetmeliğe bırakılmasının Anayasa'ya aykırı olduğu belirtilerek kuralın, Anayasa'nın 2., 7., 13., 20. ve 26. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

175. Kanun'un 5. maddesinin iptali istenilen (3) numaralı fıkrasında, yer sağlayıcının, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlü olduğu belirtilmiştir.

176. Anayasa'nın 7. maddesinde, yasama yetkisinin Türkiye Büyük Millet Meclisine ait olduğu ve bu yetkinin devredilemeyeceği öngörülmüştür. Anayasa'da kanun ile düzenlenmesi öngörülen konularda yürütme organına genel ve sınırları belirsiz bir düzenleme yetkisinin verilmesi olanaklı değildir.

177. İnternet ortamında işlenen suçların takibi ve tespiti amacıyla kişisel veriler de dâhil olmak üzere internet trafik bilgilerine ihtiyaç bulunmaktadır. Trafik bilgisinin tanımı, 5651 sayılı Kanun'un 2. maddesinin (1) numaralı fıkrasının (j) bendinde yapılmıştır. Buna göre trafik bilgisi, taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı

ve varsa abone kimlik bilgilerini ifade etmektedir. Kişisel veri kavramı da, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri içermektedir. Dolayısıyla trafik bilgisinin kapsamına, kişisel veriler de girmektedir. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Ancak söz konusu hak sınırsız değildir. Kişisel verilerin korunması hakkı, veri sahibinin mutlak ve sınırsız bir veri hâkimiyetini mümkün kılmamaktadır. Kanun koyucu, iptali istenilen kuralı, internet üzerinden işlenen suçlarla mücadele edilmesi açısından önemli ve gerekli olan bilgilerin kaybolmasının önlenmesi ve faillerin ortaya çıkarılmasının sağlanması amacıyla düzenlemiştir. Anılan düzenlemenin anayasal sınırlar içinde kanun koyucunun takdirinde olduğu açıktır.

178. Trafik bilgisi, bir internet kullanıcısının özel hayatı ile ilgili birçok detayı, kişisel tercihleri, politik eğilimlerini, sağlık bilgilerini, ticari sırlarını ifşa edebilecek nitelikte kritik bilgiler içeren bir veri türüdür. Bu nedenle, trafik bilgileri ile bir kişinin hayatı ile ilgili neredeyse her detayın kolayca tespit edilmesine imkân bulunmaktadır. Ancak yer sağlayıcılar, yer sağladıkları hizmetlere ilişkin trafik bilgilerine yaptıkları işin doğası gereği zaten sahip bulunmaktadırlar. Söz konusu kural yer sağlayıcıları sadece bu bilgileri belirtilen süre saklama, bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlü kılmaktadır. Trafik bilgilerinin yer sağlayıcılar tarafından amacına aykırı kullanılması halinde Türk Medeni Kanunu'nun ve Türk Ceza Kanunu'nun ilgili hükümlerinin bunlar için de uygulanacağı tabiidir.

179. İptali istenilen kural uyarınca yer sağlayıcılar tarafından trafik bilgileri belirtilen süre saklanacak, bu arada söz konusu bilgilerin doğruluğu, bütünlüğü ve gizliliği de sağlanacaktır. Yer sağlayıcıya bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlama yükümlülüğünün verilmesi, yer sağlayıcının görevinden kaynaklanan ve kişilerin temel hak ve özgürlüklerini korumaya yönelik bir sorumluluktur. Aynı zamanda, söz konusu bilgilerin gizliliğinin sağlanması usulleri gelişen teknoloji ile çok değişik önlemlerin alınmasını gerektirici nitelikte olup devamlı olarak değişebilecek niteliktedir. Belirtilen bu hususlar, teknik ve uygulamayı esas alan detaylarla ilgili olup, kural bu yönüyle belirli ve öngörülebilirdir. Bu nedenle, iptali istenilen kural hukuki güvenlik ilkesine aykırı değildir.

180. Ayrıca kuralda, kişisel verilerin korunmasını isteme hakkını aşırı derecede zorlaştıran ya da ortadan kaldıran ve hakkın özüne dokunan bir sınırlama bulunmadığından kişisel verilerin korunmasıyla ilgili olarak Anayasa'nın 20. maddesinde belirtilen güvencelere aykırılık da bulunmamaktadır.

181. Öte yandan, iptali istenilen kuralda yer sağlayıcıların trafik bilgilerini ne kadar süre ile saklayacağı, alt ve üst sınırlar belirtilmek suretiyle gösterilmiştir. Buna göre, trafik bilgileri bir yıldan az olmamak üzere iki yıla kadar yönetmelikte belirlenecek süre saklanacaktır. Dolayısıyla, idarenin düzenlenmesine bırakılan alanın çerçevesi çizilmiş bulunmaktadır. Bu nedenle, alt ve üst sınır göstermek suretiyle yönetmelikle belirlenecek olan sürenin sınırları gösterildiğinden yürütmeye verilen yetki yasama yetkisinin devri niteliğinde değildir.

182. Açıklanan nedenlerle kural, Anayasa'nın 2., 7., 13. ve 20. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

183. Kuralın Anayasa'nın 26. maddesiyle bir ilgisi görülmemiştir.

N- Kanun'un 88. Maddesiyle, 5651 Sayılı Kanun'un 5. Maddesine Eklenen (4) Numaralı Fıkranın İncelenmesi

1- İptal Talebinin Gerekçesi

184. Dava dilekçesinde özetle, iptali istenilen kural uyarınca yer sağlayıcıların sınıflandırılabilmesinin ve farklılaştırılabilmesinin usul ve esaslarının belirlenmesinin yönetmeliğe bırakıldığı ve böylece bu konudaki düzenlemenin belirli ve öngörülebilir kurallara bağlanmaksızın idareye yetki verilmek suretiyle sağlanmaya çalışıldığı, bu düzenlemenin yasama yetkisinin yürütmeye devri anlamına geldiği, ayrıca kural ile yer sağlayıcıların kategorize edilmesinin kanun ile değil de kim tarafından çıkartılacağı belli dahi olmayan yönetmeliğe bırakılmasının internet aktörleri arasında eko-sisteme en fazla katkıda bulunan yer sağlayıcılarının önemine oranla yanlış olduğu gibi normlar hiyerarşisine de aykırı olduğu ve idareye keyfi bir hareket alanı tanıdığı, dolayısıyla böyle bir düzenleme ile hukuki güvenliğin sağlanabilmesinin mümkün olmadığı, diğer yandan Anayasa'nın 13. maddesine göre temel hak ve özgürlüklere ilişkin sınırlandırmaların kanunla öngörülmesi ve sınırlamaların kanuna uygun olması gerektiği prensibi nazara alındığında, yer sağlayıcıların sınıflandırılabilmesinin ve farklılaştırılabilmesinin usul ve esaslarının belirlenmesinin yönetmeliğe bırakılmasının Anayasa'ya uygun olmadığı belirtilerek kuralın, Anayasa'nın 2., 7. ve 13. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

185. Kanun'un 5. maddesinin iptali istenilen (4) numaralı fıkrasında, yer sağlayıcıların, yönetmelikle belirlenecek usul ve esaslar çerçevesinde yaptıkları işin niteliğine göre sınıflandırılacakları ve hak ve yükümlülükleri itibarıyla farklılaştırılacakları öngörülmektedir.

186. Yer sağlayıcıların birçoğunun sunucularını yurt dışında barındırdığı, bu durumun ise yasa dışı ve zararlı içerikle mücadelede sorun oluşturduğu, bu nedenle kanun koyucunun, yer sağlayıcıların kayıt altına alınarak yasa dışı ve zararlı içerikle mücadeleyi arttırmak, ekonomiye katkıda bulunulması ve yer sağlayıcılara teşvik politikalarının uygulanmasını sağlamak için kamu yararı amacıyla söz konusu hükmü çıkardığı anlaşılmaktadır. Bu hükümle, yer sağlayıcılar için yurt içi yer sağlayıcılık hizmetlerinin vergi yükünün azaltılması, altyapının geliştirilerek bağlantı hızının artırılması ve kayıtlı yer sağlayıcılara, özel bir tarife üzerinden elektrik enerjisi verilmesi gibi politikalarla teşvik edilmesi imkânı sağlanabilecektir.

187. Kanun'un 2. maddesinin (m) bendinde yer sağlayıcının tanımı yapılmakta, 5. maddesinde ise yer sağlayıcıların yükümlülükleri ayrıntılı bir şekilde belirtilmiş bulunmaktadır. İptali istenilen kuralda ise yer sağlayıcıların sınıflandırılmasında yaptıkları işin niteliğinin değerlendirileceği ve farklılaştırma yapılırken de hak ve yükümlülüklerinin göz önüne alınacağı belirtilmiştir. Dolayısıyla yönetmelikte belirlenen usul ve esaslar açısından Kanun'da çerçeve belirlenmiş bulunmaktadır. Ayrıca, iptali istenilen kuralda belirtilen yönetmelikle belirlenecek usul ve esaslar kanunla düzenlenmesi gerekmeyen, uzmanlık gerektiren ve teknik ayrıntılara ilişkin hususlardır. Bu hususların düzenlenmesinin yönetmeliğe bırakılması ise yasama yetkisinin devri ya da idareye Anayasa'dan kaynaklanmayan bir yetkinin kullanılması şeklinde nitelendirilemez.

188. Diğer taraftan, dava dilekçesinde söz konusu yönetmeliğin kim tarafından çıkarılacağına dahi belli olmadığı ileri sürülmüş ise de, Kanun'un 11. maddesinin (2) numaralı fıkrasında, yer sağlayıcıların yükümlülüklerine ilişkin esas ve usullerin, Kurum tarafından çıkarılacak yönetmelikle düzenleneceği öngörülmüştür. Kurum'un da Bilgi Teknolojileri ve İletişim Kurumunu ifade ettiği 5651 sayılı Kanun'un 2. maddesinin (ı) bendi ile 5809 sayılı Kanun'un 3. maddesinin (ee) bendi ile 65. maddesinin (3) numaralı fıkrasında belirtilmiştir.

189. Açıklanan nedenlerle kural, Anayasa'nın 2. ve 7. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

190. Kuralın Anayasa'nın 13. maddesiyle ilgisi görülmemiştir.

O- Kanun'un 88. Maddesiyle, 5651 Sayılı Kanun'un 5. Maddesine Eklenen (6) Numaralı Fıkranın İncelenmesi

1- İptal Talebinin Gerekçesi

191. Dava dilekçesinde özetle, iptali istenilen kural uyarınca TİB tarafından yer sağlayıcılara idari para cezası verilebileceği, idari nitelikte bile olsa, para cezasını öngören bir yaptırımın idare

tarafından değil, mahkemeler tarafından verilmesi gerektiği, maddede öngörülen para cezasının alt ve üst haddi arasında "on katı" gibi fahiş bir fark bulunduğu, öngörülen idari para cezasının "suç ve cezaların öngörülebilir ve orantılı olma" prensibine aykırı olduğu, Mahkemelerin bile ceza verirken kanunlarda belirtilen ölçütleri gözeterek ve gerekçesini de kararlarında göstererek vermeleri gerekirken, TİB'e hem fahiş hem de keyfi olabilecek nitelikte ve üstelik on kat fark olan bir ceza verme yetkisi verilmesinin ceza hukukunun temel prensiplerine aykırı olduğu belirtilerek kuralın, Anayasa'nın 38. maddesine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

192. 6216 sayılı Kanun'un 43. maddesi uyarınca, kural ilgisi nedeniyle Anayasa'nın 2. maddesi yönünden de incelenmiştir.

193. İptali istenilen kuralda, yer sağlayıcılık bildiriminde bulunmayan veya bu Kanundaki yükümlülükleri yerine getirmeyen yer sağlayıcı hakkında Başkanlık tarafından on bin Türk Lirasından yüz bin Türk Lirasına kadar idari para cezası verileceği öngörülmektedir.

194. Anayasa'nın 38. maddesinin birinci fıkrasında, "Kimse, işlendiği zaman yürürlükte bulunan kanunun suç saymadığı bir fiilden dolayı cezalandırılmaz" denilerek "suçun kanuniliği", üçüncü fıkrasında da "Ceza ve ceza yerine geçen güvenlik tedbirleri ancak kanunla konulur" denilerek, "cezanın kanuniliği" ilkesi getirilmiştir. Anayasa'da öngörülen suçta ve cezada kanunilik ilkesi, insan hak ve özgürlüklerini esas alan bir anlayışın öne çıktığı günümüzde, ceza hukukunun da temel ilkelerinden birini oluşturmaktadır. Suçta ve cezada kanunilik ilkesi uyarınca, hangi fiillerin suç sayıldığı ve suç sayılan bu fiillere verilecek cezaların hiçbir kuşkuya yer bırakmayacak bir şekilde kanunda gösterilmesi, kuralın açık, anlaşılır ve sınırlarının belli olması gerekmektedir.

195. Değişen sosyal, siyasal ve ekonomik koşullar kimi durumlarda idarelere bir takım hakların tanınması gereğini ortaya çıkarmıştır. Gelişen, büyüyen, çeşitlenen ve çoğalan toplumsal gereksinimleri yerinde, zamanında ve etkin bir biçimde karşılayabilmek için çağdaş yönetimlerde idareye değişik alanlarda yaptırım uygulama yetkileri tanınmaktadır. İdari para cezası, kabahat sayılan eylemin işlenmesini önlemeye yönelik caydırıcılık fonksiyonu gördüğü gibi kamu açısından oluşan zararın giderilmesi amacına da hizmet etmektedir.

196. Hukuk devletinde ceza hukukuna ilişkin düzenlemelerde olduğu gibi kabahatler hukuku açısından da Anayasa'ya bağlı kalmak koşuluyla hangi eylemlerin kabahat sayılacağı, bunlara uygulanacak yaptırımın türü ve ölçüsü, yaptırımın ağırlaştırıcı ve hafifletici nedenlerinin belirlenmesi

ve idareye yaptırım uygulama yetkisinin verilmesi gibi konularda kanun koyucunun takdir yetkisi bulunmaktadır.

197. İdarelerin, kanunlarla verilen görevleri yerine getirirken ne tür kararlar almaları gerektiğinin, her türlü olay ve olgu göz önünde bulundurularak önceden hukuk kurallarıyla belirlenmesi mümkün olmadığı gibi kamu hizmetlerinin ve toplumsal ihtiyaçların değişkenliği dikkate alındığında uygun bir yöntem de değildir. Bu nedenle, idarelerin karşılaştıkları farklı durumlar karşısında en uygun çözümü üretebilmeleri için takdir yetkisiyle donatılmaları zorunludur. Takdir yetkisinin amacı, idareye farklı çözümler arasından uygun ve yerinde olanı seçme serbestisi tanımaktır.

198. İdareye takdir yetkisi tanınması, idarenin "keyfi" olarak hareket edebileceği anlamına gelmez. İdareye tanınan takdir yetkisinin, somut olayın özellikleri, eylemin ağırlığı, oluşan zararın büyüklüğü gibi durumlar göz önünde bulundurularak eşitlik, kamu yararı ve hizmet gereklerine uygun olarak kullanılması ve işlenen fiil ile tayin edilecek ceza arasında adil bir dengenin gözetilmesi, hukukun genel ilkelerindedir. İdare, cezanın alt sınırının üzerine çıktığında, bunun nedenlerini ortaya koymak ve gerekçelerini açıklamak zorundadır. İdarenin, alt sınırın üzerinde ceza tayin etmesinin gerekçesini açıklayamaması veya açıklanan gerekçenin makul ve haklı olmaması, eylem ile ceza arasında olması gereken dengeye dikkat etmemesi veya bu dengeyi ölçsüz bir şekilde kurması durumunda, cezanın yargı yerlerince iptal edilebileceği tabiidir.

199. İptali istenilen kural ile düzenlenen idari para cezası, internet ortamındaki kullanıcılara yer sağlayan kuruluşlara verilen yükümlülüklerin yerine getirilmemesi halinde Telekomünikasyon İletişim Başkanlığı tarafından uygulanacak olan bir idari yaptırımdır. Böyle bir düzenlemenin anayasal sınırlar içinde kanun koyucunun takdirinde olduğu da açıktır.

200. Yer sağlayıcılara idari yaptırım uygulanabilecek eylemler 5651 sayılı Kanun'da gösterilmiş, uygulanacak para cezasının alt ve üst sınırı Kanun'da belirtilmiştir. Yer sağlayıcılardan gösterilen kabahatleri işlemeleri durumunda ne kadar para cezasına muhatap olabileceklerini öngörebilir ve bilebilir durumdadırlar. Bu nedenle iptali istenilen kuralda, cezanın türü ve miktarı yönünden herhangi bir belirsizlik söz konusu olmadığı gibi suçların ve cezaların kanuniliği ilkesine de aykırılık bulunmamaktadır.

201. İptali istenilen kuralda alt ve üst sınırları gösterilen idari para cezası belirlenirken hangi kıstasların göz önüne alınacağı belirtilmemiştir. Ancak, 5326 sayılı Kabahatler Kanunu'nun 3. maddesinde, anılan Kanun'un genel hükümlerinin idari para cezası yaptırımını gerektiren bütün fiiller hakkında uygulanacağı hükme bağlanmış, aynı Kanun'un 17. maddesinin (2) numaralı fıkrasında da, idari para cezasının, alt ve üst sınırı gösterilmek suretiyle belirlendiği durumlarda, idari

para cezasının miktarı belirlenirken işlenen kabahatin haksızlık içeriği ile failin kusuru ve ekonomik durumunun birlikte göz önünde bulundurulacağı belirtilmiştir. Bu nedenle TİB, yer sağlayıcılara verilecek idari para cezasının miktarını belirlerken Kabahatler Kanunu'nun 17. maddesinde belirtilen ölçütlere ve ayrıca hukukun genel ilkelerine de uymak zorundadır. Dolayısıyla idari para cezasının tayininde hiçbir ölçütün belirlenmediği ve idarenin keyfi bir şekilde ceza takdir etmesine olanak sağlandığı söylenemez. Bu nedenle, kural hukuk devleti ilkesine aykırı değildir.

202. Açıklanan nedenlerle kural, Anayasa'nın 2. ve 38. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

Ö- Kanun'un 89. Maddesiyle, 5651 Sayılı Kanun'un 6. Maddesinin (1) Numaralı Fıkrasına Eklenen (ç) Bendinin İncelenmesi

1- İptal Talebinin Gerekçesi

203. Dava dilekçesinde özetle, kamuoyunda ve basında "Gezi önlemi" olarak nitelendirilen bu düzenlemenin ne anlama geldiğinin anlaşılamadığı, erişim sağlayıcının hangi alternatif erişim yollarını, hangi araçları kullanarak engelleyeceği hususunun uygulayıcının keyfine bırakıldığı, kuralda bu konuda açıklık ve netlik bulunmadığı, "erişimi engelleme kararı verilen yayınlarla ilgili olarak alternatif erişim yolları"nın neler olduğunun Kanun metninde açık bir şekilde ifade edilmesi gerektiği belirtilerek kuralın, Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

204. İptali istenilen kuralın yer aldığı Kanun'un 6. maddesinin (1) numaralı fıkrasında, erişim sağlayıcılarının yükümlülükleri ile ilgili düzenlemeler yer almaktadır. İptali istenilen kuralda da, erişim sağlayıcının, erişimi engelleme kararı verilen yayınlarla ilgili olarak alternatif erişim yollarını engelleyici tedbirleri almakla yükümlü olduğu belirtilmektedir.

205. Erişimin engellenmesi, internet ortamında yayın yapan bir siteye girişin çeşitli yöntemlerle önlenmesidir. Erişimi engelleme kararı uygulansa dahi, internet kullanıcıları erişimi engellenen yayına çeşitli teknikleri kullanmak suretiyle ulaşabilmekte ve erişimin engellenmesi kararını etkisiz hale getirebilmektedir. İptali istenilen kural bu kapsamda erişim sağlayıcıya, erişimi engelleme kararı verilen yayınlara ulaşılmasını engelleyecek alternatif erişim yollarını engelleyici tedbirleri alma yükümlülüğü getirmektedir. Böylece erişimin engellenmesi kararı verilen yayınlara farklı yöntemlerle ulaşan kullanıcıların bu yayınlara ulaşmaları erişim sağlayıcıların kullanacağı alternatif tedbirlerle engellenebilecek ve erişimin engellenmesi kararlarının etkisiz hale gelmesi önenebilecektir.

206. İptali istenilen kural, erişimi engelleme kararı verilen yayınlarla ilgili olarak, bu kararların etkili bir şekilde uygulanmasını sağlamak için TİB'in görevlerinin ifası kapsamında ihtiyaç duyulan verilerin erişim sağlayıcı tarafından karşılanması noktasında ortaya çıkan sorunların giderilmesi amacıyla çıkarılmıştır. Bu kapsamda, erişim sağlayıcının erişimi engelleme kararı verilen yayınlarla ilgili olarak erişim yollarını engelleyici tedbirleri almakla yükümlü kılınması kanun koyucunun takdir yetkisi içinde kalmaktadır.

207. Alternatif erişim yollarını engelleyici tedbirler özel bir uzmanlık ve teknik bilgi isteyen, hızlı, teknolojik ve bilimsel gelişmeler karşısında çok hızlı değişen ve gelişen tedbirlerdir. Bu nedenle, bu tedbirlerin neler olduğunun kanun koyucu tarafından önceden tek tek belirlenmesi mümkün değildir. Ayrıca erişim sağlayıcılar söz konusu alternatif tedbirleri, erişimin engellenmesi kararı verilmiş yayınlar hakkında uygulayacaklardır. İptali istenilen kural ile erişim sağlayıcılara doğrudan erişimin engellenmesi yetkisi verilmiş değildir. Erişim sağlayıcılara yüklenen görev daha önce verilen erişimin engellenmesi kararının etkili bir şekilde yerine getirilmesinden ibarettir. Dolayısıyla, iptali istenilen kuralda hukuki güvenlik ve belirlilik ilkelerine aykırı bir yön bulunmamaktadır.

208. Açıklanan nedenlerle kural, Anayasa'nın 2. maddesine aykırı değildir. İptal talebinin reddi gerekir.

P- Kanun'un 91. Maddesiyle 5651 Sayılı Kanun'un 7. Maddesinin Değiştirilen (2) ve (3) Numaralı Fıkraları ile Maddeye Eklenen (4) Numaralı Fıkranın İncelenmesi

1- Kuralların Anlam ve Kapsamları

209. Kanun'un 7. maddesinde toplu kullanım sağlayıcılarının yükümlülükleri düzenlenmiştir. Toplu kullanım sağlayıcı da, Kanun'un 2. maddesinin (i) bendinde, kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan ifade eder şeklinde belirtilmiştir.

210. Kanun'un 7. maddesinin (1) numaralı fıkrasında, ticari amaçla toplu kullanım sağlayıcıların mahalli mülki amirden izin belgesi almakla yükümlü oldukları, izne ilişkin bilgilerin otuz gün içinde mahalli mülki amir tarafından Kurum'a bildirileceği, bunların denetiminin mahalli mülki amirler tarafından yapılacağı, izin belgesinin verilmesine ve denetimine ilişkin esas ve usullerin yönetmelikle düzenleneceği, iptali istenilen (2) numaralı fıkrasında ticari amaçla olup olmadığına bakılmaksızın bütün internet toplu kullanım sağlayıcıların, konusu suç oluşturan içeriklere erişimin engellenmesi ve kullanıma ilişkin erişim kayıtlarının tutulması hususlarında yönetmelikle belirlenen tedbirleri almakla yükümlü oldukları, iptali istenilen (3) numaralı fıkrasında ticari amaçla toplu kullanım sağlayıcıların, ailenin ve çocukların korunması, suçun önlenmesi ve suçluların tespiti kapsamında

usul ve esasları yönetmelikte belirlenen tedbirleri almakla yükümlü oldukları, iptali istenilen (4) numaralı fıkrasında ise bu maddede belirtilen yükümlülükleri ihlal eden ticari amaçla toplu kullanım sağlayıcılarına, ihlalin ağırlığına göre yönetmelikle belirlenecek usul ve esaslar çerçevesinde uyarma, bin Türk Lirasından on beş bin Türk Lirasına kadar idari para cezası verme veya üç güne kadar ticari faaliyetlerini durdurma müeyyidelerinden birine karar vermeye mahalli mülki amirin yetkili olduğu hüküm altına alınmıştır.

211. Kanun'un 7. maddesinin (4) numaralı fıkrasında belirtilen idari cezaların ticari amaçla toplu kullanım sağlayıcılarına uygulanabilmesi için aynı maddede belirtilen yükümlülüklerin ihlal edilmesi gerekmektedir. Kanun'un 7. maddesinde ticari amaçla toplu kullanım sağlayıcıların yerine getirmesi gereken yükümlülükler şunlardır:

a- Mahalli mülki amirden izin belgesi almak,

b- Konusu suç oluşturan içeriklere erişimin engellenmesi ve kullanıma ilişkin erişim kayıtlarının tutulması hususlarında yönetmelikte belirlenen tedbirleri almak,

c- Ailenin ve çocukların korunması, suçun önlenmesi ve suçluların tespiti kapsamında usul ve esasları yönetmelikte belirlenen tedbirleri almak.

2- İptal Taleplerinin Gerekçesi

212. Dava dilekçesinde özetle, düzenlemelerin belirli ve öngörülebilir kurallara bağlanmaksızın idareye yetki verilmek suretiyle sağlanmaya çalışıldığı, böyle bir düzenlemenin hukuki güvenliği sağlayamayacağı, internet toplu kullanım sağlayıcılarına anılan maddede getirilen yükümlülükleri ve öngörülen müeyyideleri belirleme yetkisinin genel, sınırsız, esasları ve çerçevesi belirsiz bir şekilde idareye bırakılmasının "yasama yetkisinin devri" niteliğinde olduğu, Anayasa'nın 13. maddesine göre temel hak ve özgürlüklere ilişkin sınırlandırmaların kanunla öngörülmesi ve sınırlamaların kanuna uygun olması gerektiği prensibi nazara alındığında iptali istenilen kuralların Anayasa'nın 13. maddesine de aykırı olduğu, idari nitelikte bile olsa, para cezasını öngören bir müeyyidenin idare birimleri tarafından değil de mahkemeler tarafından verilmesi gerektiği, maddede öngörülen para cezasının alt ve üst haddi arasında "onbeş katı" gibi fahiş bir fark olduğu ve hangi sınırdan verilmesinin takdirinin çok hassas ve ayrıntılı bir muhakeme faaliyetini gerekli kıldığı, bu nedenle bu yetkinin idareye değil, mahkemelere ait olması gerektiği, mahalli mülki amir tarafından ticari amaçla toplu kullanım sağlayıcılarına bin Türk lirasından on beş bin Türk lirasına kadar idari para cezası verilmesinin "suç ve cezaların öngörülebilir ve orantılı olma" prensibine de aykırı olduğu, ülkemizde ceza mahkemelerinin bile cezanın belirlenmesi ve bireyselleştirilmesi sırasında Türk Ceza

Kanunu'nun 61. maddesinde belirtilen hususları kararında göstermesi gerekirken idareye bağı bir görevliye hem fahiş, hem de keyfi olabilecek nitelikte ve üstelik arada on beş kat fark olan bir cezaya hükmetme yetkisinin verilmesinin ceza hukukunun temel prensiplerine uygun olmadığı, Anayasa'nın 38. maddesinin üçüncü fıkrasında, "Ceza ve ceza yerine geçen güvenlik tedbirleri ancak kanunla konulur" denildiği, kanunla konulması gereken bir cezanın ise mahkemelerce verilmesi gerektiği belirtilerek kuralların, Anayasa'nın 2., 7., 13. ve 38. maddelerine aykırı olduğu ileri sürülmüştür.

3- Anayasa'ya Aykırılık Sorunu

213. Kanun'un 7. maddesinin iptali istenilen (2) ve (3) numaralı fıkraları ile toplu kullanım sağlayıcıların sunmuş oldukları hizmet nedeniyle özellikle çocukların internetteki zararlı ve yasal olmayan içerik-ten ko-run-ma-sı, suçların işlenmesinin önlenmesi, suçlunun tespitinde önemli işlev görecektir olan kayıt bilgilerinin tutulması ve kamera kayıtlarının belirli süre saklanmasına ilişkin yasal dayanakların güçlendirilmesi amaçlanmaktadır. Bu itibarla, internet toplu kullanım sağlayıcıları ve ticari amaçla toplu kullanım sağlayıcılarına iptali istenilen kurallarda gösterilen çerçevede belirtilen tedbirleri alma yükümlülüğünün yüklenmesi, anayasal sınırlar içinde kalmak kaydıyla kanun koyucunun takdir yetkisi kapsamındadır.

214. Kanun'un 7. maddesinin iptali istenilen (2) numaralı fıkrasında bütün internet toplu kullanım sağlayıcılarına, yönetmelikle belirlenen tedbirleri alma yükümlülüğü verilmiştir. Ancak söz konusu kuralda alınması gereken tedbirlerin konusunun suç oluşturan içeriklere erişimin engellenmesi ve kullanımına ilişkin erişim kayıtlarının tutulması hususlarına yönelik olduğu belirtilmek suretiyle çerçevesi belirlenmiştir. Yine, aynı maddenin (3) numaralı fıkrasında ticari amaçla toplu kullanım sağlayıcılarına yönetmelikte belirlenen tedbirleri alma yükümlülüğü verilmekte, bu yükümlülüklerin kapsamı da ailenin ve çocukların korunması, suçun önlenmesi ve suçluların tespiti olarak belirtilmektedir. Yönetmelikle belirlenecek olan tedbirlere ilişkin çerçeve iptali istenilen kurallarda gösterilmiş olup idare söz konusu tedbirleri belirlerken iptali istenilen kurallarda belirtilen amaçlarla sınırlı olarak bu yetkisini kullanacaktır. Bu nedenle iptali istenilen kurallar, belirli ve öngörülebilirdir.

215. Ayrıca, yönetmelikle belirlenecek olan tedbirlerin teknolojideki gelişmelere göre sık sık değişebilecek olması gözetildiğinde, uzmanlık ve idare tekniğine ilişkin hususları belirleme yetkisinin idareye verilmesi, yasama yetkisinin devri olarak nitelendirilemez.

216. Kanun'un 7. maddesinin iptali istenilen (4) numaralı fıkrasında ise, bu maddede belirtilen yükümlülükleri ihlal eden ticari amaçla toplu kullanım sağlayıcılarına, ihlalin ağırlığına göre yönetmelikle belirlenecek usul ve esaslar çerçevesinde uyarma, bin Türk Lirasından on beş bin Türk

Lirasına kadar idari para cezası verme veya üç güne kadar ticari faaliyetlerini durdurma müeyyidelerinden birine karar vermeye mahalli mülki amirin yetkili olduğu hüküm altına alınmıştır.

217. Kanun koyucu, suçların niteliği, işleme biçimi, içerik ve yoğunluğu, kamu düzenini ihlal derecesi ve cezaların caydırıcılığı gibi nedenleri gözeterek, Anayasa ve ceza hukukunun temel ilkeleri çerçevesinde, hangi eylemlerin suç sayılacağını ve bunlara verilecek cezaların tür ve miktarını saptayabileceği gibi toplumsal sonuçları bakımından doğurduğu tehlikenin ağırlığına göre, kimi eylemlere hürriyeti bağlayıcı cezalar dışında, idari yaptırımlar uygulanmasını da öngörebilir.

218. İptali istenilen kuralla ticari amaçla toplu kullanım sağlayıcılarının, Kanun'un 7. maddesinde belirtilen yükümlülükleri ihlal etme eylemi, kabahat olarak kabul edilmiş ve seçenekli yaptırım öngörülmüştür. Söz konusu yükümlülüklerin kapsamı da Kanun'un 7. maddesinin (1), (2) ve (3) numaralı fıkralarında düzenlenmiş ve bu yükümlülükler uymaması halinde verilebilecek cezalar iptali istenilen kuralda açıkça belirtilmiştir. Kural bu yönüyle belirli ve öngörülebilirdir.

219. Suç sayılan eylem ve cezası kanunda gösterildikten sonra yasama organının uzmanlık ve yönetim tekniğine ilişkin konularda önlemler alınması amacıyla yürütme organına yetki vermesi, suçun idari düzenlemelerle ortaya konulması anlamına gelmez. Ayrıca, iptali istenilen kuralda ticari amaçla toplu kullanım sağlayıcılarına 7. maddedeki yükümlülükleri ihlal etmesi halinde yönetmelikle belirlenecek usul ve esaslar çerçevesinde verilecek olan cezaların ihlalin ağırlığına göre belirleneceği ve söz konusu cezanın mahalli mülki amir tarafından verileceği belirtilmektedir.

220. Öte yandan, iptali istenilen kuralda düzenlenen kabahatler, 5326 sayılı Kabahatler Kanunu'na tabi olup anılan Kanun'un genel hükümleri içinde yer alan 17. maddesinde, idari para cezası uygulanırken hangi ölçütlerin esas alınacağı gösterilmiştir. Söz konusu maddenin (2) numaralı fıkrasına göre, idarî para cezasının, kanunda alt ve üst sınırı gösterilmek suretiyle belirlendiği durumlarda, idarî para cezasının miktarı tespit edilirken işlenen kabahatin haksızlık içeriği ile failin kusuru ve ekonomik durumu birlikte göz önünde bulundurulur. Dolayısıyla kuralda belirtilen yaptırımların tayininde hiçbir ölçütün belirlenmediği ve idarenin keyfi bir şekilde ceza takdir etmesine olanak sağlandığı söylenemez. Yükümlülükleri yerine getirmeyen ticari amaçla toplu kullanım sağlayıcılara uygulanacak cezaların seçenekli olarak gösterildiği ve ihlalin ağırlığı ile Kabahatler Kanunu'nda gösterilen hususlar göz önüne alınarak bu cezalardan biri belirleneceğinden kuralın ölçüsüz olduğundan da söz edilemez. Bu nedenle, gerek kabahatin, gerekse yaptırımların kanunla düzenlenmiş olması karşısında kuralda belirsizlik ve öngörümezlikten söz edilemeyeceği gibi suç ve cezaların kanuniliği ilkesine aykırılık da bulunmamaktadır.

221. Açıklanan nedenlerle kurallar, Anayasa'nın 2., 7. ve 38. maddelerine aykırı değildir. İptal taleplerinin reddi gerekir.

222. Kuralların Anayasa'nın 13. maddesi ile bir ilgisi görülmemiştir.

R- Kanun'un 94. Maddesiyle, 5651 Sayılı Kanun'a Eklenen 9/A Maddesinin (1), (2), (3), (4), (5), (6), (7) ve (8) Numaralı Fıkralarının İncelenmesi

1- İptal Taleplerinin Gerekçeleri

223. Dava dilekçesinde özetle, TİB uygulamaları üzerindeki yargısal denetimin hafifletilmiş olmasının ulusal ve uluslararası hukuk ile çeliştiği, anılan maddede diğer düzenlemelerin aksine 5237 sayılı Türk Ceza Kanunu'na herhangi bir atıf yapılmamış olmasının ve kişilik hakkının içinde yer alan özel hayatın gizliliğinin ihlali olgusunun ayrı bir maddede düzenlenmesinin, subjektif kavram olan özel hayatın gizliliğinin hangi tanımının esas alınacağı sorusunu gündeme getirdiği, yeni düzenlemeye göre "özel hayatın gizliliğinin" ihlaline ilişkin bir mağduriyet iddiasının herhangi bir merciin değerlendirmesine yer bırakmadan süreci re'sen başlatacağı, düzenlemedeki belirsizliğin kabul edilebilir nitelikte olmadığı, iptali istenilen kuralda Başkanlığın verdiği erişimin engellenmesi tedbirinin onaylanmasına ilişkin sulh ceza mahkemesinin kararına karşı içerik sahibi de dâhil kimseye itiraz hakkının tanınmadığı ve gidilebilecek itiraz yolunun gösterilmediği, dolayısı ile bu düzenlemenin hak arama hürriyetine aykırı olduğu, 9/A maddesinin altıncı fıkrasında ise Başkanlığın verdiği erişimin engellenmesi tedbirinin kaldırılmasına ilişkin sulh ceza hâkiminin kararına karşı itiraz yolu gösterildiği, ancak itirazda bulunma hakkının sadece Başkanlığa tanındığı, oysa özel hayatın ihlal edildiğini ileri sürerek Başkanlığa doğrudan müracaat ederek içeriğin kaldırılması talebinde bulunan kişinin talebi üzerine Başkanlıkça verilen tedbir kararının kaldırılmasını öngören sulh ceza hâkiminin kararının, asıl özel hayatının ihlal edildiğini iddia eden kişinin aleyhine olmasına rağmen, maddede bu kişiye hiçbir itiraz hakkının tanınmadığı, bu hususun da hak arama hürriyetine ve Anayasa'nın 40. maddesinin birinci ve ikinci fıkralarına aykırı olduğu, iptali istenilen kuralın sekizinci fıkrasında yer alan hükmün ise tam bir "sansür" hükmü olup TİB'e doğrudan erişimin engellenmesi kararı verme yetkisi tanıdığı, bu düzenlemeye göre özel hayatın gizliliği veya başkalarının hak ve özgürlüklerinin korunması sebeplerine bağlı olarak gecikmesinde sakınca bulunan hallerde TİB Başkanının herhangi bir ihbar, iddia, şikayet ya da başvuru olmaksızın, herhangi bir kişinin talebi bulunmaksızın erişimin engellenmesine ilişkin tedbir kararına re'sen karar verebileceği, bu durumun hukuk devleti ilkesine aykırı olduğu, böyle bir yetki verilmesinin Anayasa'nın 26., 22. ve 28. maddelerinin çok ağır bir şekilde ihlali anlamına geldiği belirtilmiştir. Ayrıca, 9/A maddesinin sekizinci fıkrası hükmü ile TİB Başkanına temel hak ve hürriyetlerden biri

sayılan "ifade hürriyetine" doğrudan müdahale ederek bu hürriyetin kullanımını engelleme konusunda emir verme yetkisi tanındığı, bu durumun ifade özgürlüğünün kanun dışı bir yolla sınırlanması anlamına geldiği, ayrıca düzenlemenin ölçülülük ilkesiyle ve düzenleme ile korunmak istenen menfaatlerle bağdaşmadığı, belirtilen Anayasaya aykırılık gerekçelerinin maddenin birinci, üçüncü, dördüncü fıkrası için de geçerli olduğu, söz konusu Anayasa'ya aykırılığının aynı maddenin iptal konusu yapılan ikinci, beşinci ve yedinci fıkralarına da sirayet ettiği ve anılan fıkralarında kaçınılmaz bir biçimde sakatlanması ve Anayasa'ya aykırı olması sonucunu doğurduğu, belirtilen gerekçelerin bu kurallar için de geçerli olduğu, diğer yandan, 6216 sayılı Kanun'un 43/4 maddesi uyarınca 9/A maddesinin birinci, üçüncü, dördüncü, altıncı ve sekizinci fıkralarının iptaline karar verilmesi halinde uygulanma kabiliyeti kalmayan aynı maddenin ikinci, beşinci ve yedinci fıkralarının da iptaline karar verilmesi gerektiği belirtilerek kuralların, Anayasa'nın 2., 13., 22., 26., 28., 36. ve 40. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

224. Kanun'un iptali istenilen 9/A maddesinin (1) numaralı fıkrasında, internet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişilerin, Başkanlığa doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebileceği, (2) numaralı fıkrasında, yapılan bu istekte hakkın ihlaline neden olan yayının tam adresine (URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklamaya ve kimlik bilgilerini ispatlayacak bilgilere yer verileceği, bu bilgilerde eksiklik olması hâlinde talebin işleme konulmayacağı, (3) numaralı fıkrasında, Başkanlığın kendisine gelen bu talebi uygulanmak üzere derhâl Birliğe bildireceği, erişim sağlayıcıların bu tedbir talebini derhâl, en geç dört saat içinde yerine getireceği, (4) numaralı fıkrasında, erişimin engellenmesinin, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanacağı, (5) numaralı fıkrasında, erişimin engellenmesini talep eden kişilerin, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebini talepte bulunduğu saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunacağı, hâkimin, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklayacağı ve doğrudan Başkanlığa göndereceği; aksi hâlde, erişimin engellenmesi tedbirinin kendiliğinden kalkacağı, (6) numaralı fıkrasında, hâkim tarafından verilen bu karara karşı Başkanlık tarafından 5271 sayılı Kanun hükümlerine göre itiraz yoluna gidilebileceği, (7) numaralı fıkrasında, erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararının kendiliğinden hükümsüz kalacağı,

(8) numaralı fıkrasında ise, özel hayatın gizliliğinin ihlaline bağlı olarak gecikmesinde sakınca bulunan hâllerde doğrudan Başkanın emri üzerine erişimin engellenmesinin Başkanlık tarafından yapılacağı öngörülmüştür.

225. Özel hayatın gizliliği, Anayasa'nın 20. maddesinde "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz"; haberleşme özgürlüğü ise Anayasa'nın 22. maddesinde "Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır" denilerek koruma altına alınmıştır.

226. Özel hayatın korunması her şeyden önce özel hayatın gizliliğinin korunması, başkalarının gözleri önüne serilmemesi demektir. Kişinin özel hayatında yaşananların, yalnız kendisinin istediği kimseler tarafından bilinmesini isteme hakkı, kişinin temel haklarından biridir ve bu niteliği nedeniyle insan haklarına ilişkin beyanname ve sözleşmelerde yer almış, tüm demokratik ülkelerin mevzuatlarında açıkça belirlenen istisnalar dışında devlete, topluma ve kişilere karşı korunmuştur.

227. Haberleşme özgürlüğü, kişinin kesintiye uğramadan ve sansür edilmeden başkalarıyla iletişim kurma hakkıdır. Bu özgürlük, çok daha geniş bir alanı kaplayan "özel hayatın" bir parçasını oluşturur.

228. Modern toplumlarda diğer kişi haklarında olduğu gibi özel hayatın gizliliği ve haberleşme özgürlüğü de sınırsız bir hak niteliğinde değildir. Bazı hallerde bu haklara da müdahale edilebilmesi mümkün olmakta ve kişiler de bu müdahalelere katlanmak durumundadırlar.

229. Anayasa'nın 22. maddesinin ikinci fıkrasında haberleşme hürriyetine, ancak millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı ile ya da gecikmesinde sakınca bulunan hallerde yine bu sebeplere bağlı olarak kanunla yetkili kılınmış merciin yazılı emri ile müdahalede bulunulabileceği; kararın yetkili merci tarafından verilmesi halinde yirmi dört saat içinde görevli hâkimin onayına sunulması ve hâkimin de kararını kırk sekiz saat içinde açıklaması gerektiği; aksi halde verilen kararın kendiliğinden kalkacağı hükme bağlanmıştır.

230. Anayasa'nın düşünceyi açıklama ve yayma hürriyeti başlıklı 26. maddesinde de herkesin, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahip olduğu, ancak bu hürriyetlerin kullanılmasının, milli güvenlik, kamu düzeni, kamu güvenliği, Cumhuriyetin temel nitelikleri ve Devletin ülkesi ve milleti ile bölünmez bütünlüğünün korunması, suçların önlenmesi, suçluların cezalandırılması, Devlet sırrı olarak usulünce belirtilmiş bilgilerin açıklanmaması, başkalarının şöhret veya haklarının, özel ve aile

hayatlarının yahut kanunun öngördüğü meslek sırlarının korunması veya yargılama görevinin gereğine uygun olarak yerine getirilmesi amaçlarıyla sınırlanabileceği belirtilmiştir.

231. İfade özgürlüğü konusunda devletin pozitif ve negatif yükümlülükleri bulunmaktadır. Kamu makamları negatif yükümlülük kapsamında Anayasa'nın 13. ve 26. maddeleri kapsamında zorunlu olmadıkça düşüncenin açıklanmasını ve yayılmasını yasaklamamalı ve yaptırımlara tabi tutmamalı; pozitif yükümlülük kapsamında ise ifade özgürlüğünün gerçek ve etkili korunması için gereken tedbirleri almalıdır. Ancak, düşünceyi açıklama ve yayma özgürlüğü mutlak ve sınırsız değildir. Nitekim Anayasa'nın 22., 26. ve 28. maddelerinin koruma altına aldığı düşünceyi açıklama ve yayma hürriyeti Anayasa'nın 13. maddesindeki koşullara uygun olarak, bu maddelerde belirtilen sebeplerle sınırlandırılabilir. Anayasa'nın 13. maddesine göre temel hak ve özgürlüklere yönelik sınırlamalar, ancak kanunla yapılabilir ve hak ve özgürlüklerin özlerine dokunamayacağı gibi demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamaz.

232. Anayasal haklara yönelik müdahalenin bir kanuna dayanması yeterli olmayıp, bu kanunun belirlilik ve öngörülebilirlik gibi belli niteliklere sahip olması gerekir. Başka bir ifadeyle kanun, ilgili kişinin davranışlarını belirlemesi amacıyla, kolayca ulaşabileceği, gerektiğinde profesyonel yardım almak suretiyle de olsa anlayabileceği, açık, net ve yeterince belirgin nitelikte olmalıdır.

233. Anayasa'da güvence altına alınan haklara kamu gücü tarafından bu konuda bir sınırlama imkânı getirildiği hallerde ilgili Kanun'da böyle bir yetkinin kullanılmasına ilişkin kapsam ve usullerin yeterli bir açıklıkla tanımlanması gerekmektedir.

234. Kanun'un birinci maddesinde, Kanun'un amaçlarından birinin internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemek olduğu belirtilmiştir.

235. Kanun'un 9/A maddesinde, özel hayatın gizliliği nedeniyle erişimin engellenmesine ilişkin hükümler düzenlenmiştir. Bu madde uyarınca erişimin engellenmesine karar verilebilmesi, söz konusu içeriğin özel hayatın gizliliğinin ihlal edilmesi hali ile sınırlıdır.

236. Kanun koyucunun özel hayata verdiği önemin bir göstergesi olarak, özel hayatın gizliliğinin ihlal edildiği durumlarda bu hakkı ihlal edilenin başvurması ve söz konusu başvurunun usulüne uygun olması halinde derhal internet ortamında yapılan yayın içeriğine erişimin engellenmesini sağlayarak, özel hayatın gizliliğini korumak istediği anlaşılmaktadır. Bu bağlamda, anayasal sınırlar içinde kalmak şartıyla internet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişilerin Başkanlığa doğrudan başvurarak içeriğe erişimin engellenmesi

tedbirinin uygulanmasını istemelerini öngören hüküm ve bu başvuru talebinde hangi hususların gösterileceğinin ve kararın ne şekilde uygulanacağı ve başvuru yollarının belirlenmesi konularında kanun koyucu takdir yetkisine sahiptir.

237. Anayasa'nın 22. maddesinde haberleşme hürriyetinin başkalarının hak ve özgürlüklerinin korunmasına bağlı olarak gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınmış merciin yazılı emri ile Anayasa'nın 26. maddesinde ise ifade hürriyetinin başkalarının şöhret veya haklarının, özel ve aile hayatlarının korunması amacıyla sınırlanabileceği belirtilmektedir. Anayasa'nın 28. maddesinde de, basın hürriyetinin sınırlanmasında, Anayasa'nın 26. ve 27. maddeleri hükümlerinin uygulanacağı öngörülmektedir. İptali istenilen kurallar ile getirilen bu sınırlamayla Anayasa'nın 22., 26. ve 28. maddelerinde belirtilen sınırlama sebeplerine bağlı kalındığı ve sınırlamanın başkalarının hak ve özgürlüklerinin korunması nedeniyle meşru bir amaca dayandığı hususunda tereddüt bulunmamaktadır. Bunun yanında, Anayasa'nın 22. maddesi kapsamında, yetkili kılınmış merci ile yapılacak olan sınırlamada özel hayatın gizliliğinin ihlal edilmesi halinin de gecikmesinde sakınca bulunan hallerden biri olarak nitelendirileceği açıktır. Dolayısıyla, özel hayatın gizliliğine keyfi ya da hakkın özüne dokunacak bir sınırlama getirmeyen kurallar, demokratik toplum düzeninin gereklerine uygun ve ulaşılmak istenen amaçla sınırlı ve ölçülüdür.

238. Diğer taraftan, iptali istenilen kurallarda erişimin engellenmesi ile ilgili olarak idareye verilen yetkinin kapsam ve usulleri ile bu yetkiyi nasıl kullanacağı ve erişimin engellenmesini ne şekilde uygulayacağı ayrıntılı bir şekilde gösterilmiştir. Kurallar bu yönüyle belirli ve öngörülebilir olduklarından, hukuk devleti ilkesine aykırılık bulunmamaktadır.

239. Kanun'un 9/A maddesinin (5) numaralı fıkrası uyarınca TİB'in erişimi engelleme tedbirinin yargısal denetimi, sulh ceza hâkimi tarafından yapılmaktadır. Özel hayatın gizliliğinin ihlal edildiğini iddia eden kişi talepte bulunduğu saatten itibaren 24 saat içinde sulh ceza mahkemesine başvurmalıdır. Hâkim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklayacak ve doğrudan Başkanlığa gönderecektir. Aksi halde, erişimin engellenmesi tedbiri kendiliğinden ortadan kalkacaktır. Kanun'un iptali istenilen 9/A maddesinin (5) numaralı fıkrası ile getirilen düzenleme, Anayasa'nın 22. maddesinin ikinci fıkrası gereği olduğundan kuralda Anayasa'ya aykırılık bulunmamaktadır.

240. Dava dilekçesinde, itirazda bulunma hakkının sadece Başkanlığa tanındığı, özel hayatı ihlal edilen kişiye itiraz hakkı tanınmadığı belirtilerek Kanun'un 9/A maddesinin (6) numaralı fıkrasının Anayasa'ya aykırı olduğu ileri sürülmüştür. İptali istenilen kuralın (6) numaralı fıkrasında, hâkimin

verdiği karara karşı TİB'in Ceza Muhakemesi Kanunu (CMK) hükümlerine göre itiraz edebileceği düzenlenmesine karşın, başvuruda bulunana yönelik itiraz hakkı ile ilgili bir düzenleme bulunmamaktadır. Ancak, 5271 sayılı CMK'nın 267. maddesi uyarınca, hâkim kararlarına karşı itiraz yoluna gidilebilir. CMK'nın 268. maddesi uyarınca da, itiraz hakkı ilgililere tanınmıştır. Mağdurun bu ilgililer kapsamında olduğu açıktır. Dolayısıyla, mağdurun da CMK hükümleri uyarınca itiraz hakkının bulunması karşısında iptali istenilen kural, hak arama hürriyetine ve Anayasa'nın 40. maddesine aykırı değildir.

241. Kanun'un 9/A maddesinin (7) numaralı fıkrası uyarınca, erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda söz konusu ihlal ortadan kalktığından ve özel hayatın korunmasını gerektiren bir durum kalmadığından, hâkim kararının kendiliğinden hükümsüz kalması ise işin doğası gereği olup kural, Anayasa'ya aykırılık içermemektedir.

242. İptali istenilen kuralın (8) numaralı fıkrasında ise özel hayatın gizliliğinin ihlaline bağlı olarak gecikmesinde sakınca bulunan hallerde doğrudan Başkanın emri üzerine erişimin engellenmesinin Başkanlık tarafından yapılacağı öngörülmektedir.

243. Kuralda yer alan "özel hayatın gizliliğinin ihlali" ve "gecikmesinde sakınca bulunan haller" ibarelerinin içerik ve kapsamının kanun koyucu tarafından önceden tek tek belirlenmesi mümkün değildir. Ancak, özel hayatın gizliliğinin ihlal edilmesi hallerinin tamamının, gecikmesinde sakınca bulunan haller olarak nitelendirileceği de açıktır.

244. Kanun koyucu, özel hayatın gizliliğinin ihlaline bağlı olarak gecikmesinde sakınca bulunan hallerin hızlı ve seri karar alınmayı gerektiren bir özellik arz etmesini göz önüne alarak, iptali istenilen kural ile kişinin kendisinin dahi haberinin olmadığı ya da kamuya mal olmuş kişilerin özel hayatlarının gizliliğinin ihlal edildiği durumlarda, kamu düzeni ve kamu yararını korumak amacıyla TİB Başkanına erişimin engellenmesine karar verme yetkisi tanımıştır. Böyle bir düzenleme ise anayasal sınırlar içinde kanun koyucunun takdir yetkisi kapsamındadır.

245. TİB Başkanının söz konusu yetkiyi, özel hayatın gizliliğinin ihlaline bağlı olarak ve gecikmesinde sakınca bulunan hallerde kullanacağı açıktır. Her ne kadar kuralda TİB Başkanının erişimin engellenmesi ile ilgili olarak hangi yolla erişimin engelleneceği açık bir şekilde belirtilmemiş ise de, Kanun'un 9/A maddesinin (4) numaralı fıkrasında erişimin engellenmesinin, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla yapılacağına ilişkin hükmün TİB Başkanı için de geçerli olduğu açıktır. Kanun'un 9/A maddesi ile erişimin engellenmesi için gerekli durum ve şartların temel esasları ve çerçevesi belirlenmiş bulunmakta olup, kural bu haliyle belirli ve öngörülebilir niteliktedir.

246. Ayrıca, TİB Başkanının Kanun'un 9/A maddesinin (8) numaralı fıkrası uyarınca vermiş olduğu erişimin engellenmesi kararı, aynı maddenin (9) numaralı fıkrası uyarınca yargı denetimine tâbidir. Başkan tarafından verilen erişimin engellenmesi kararı, Başkanlık tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulacak ve hâkim kararını kırk sekiz saat içinde açıklayacaktır.

247. Açıklanan nedenlerle kurallar, Anayasa'nın 2., 13., 22., 26., 28., 36. ve 40. maddelerine aykırı değildir. İptal taleplerinin reddi gerekir.

S- Kanun'un 97. Maddesiyle, 5651 Sayılı Kanun'un Ek 1. Maddesine Eklenen (5) Numaralı Fıkranın Birinci Cümlesinde Yer Alan "...hâkim ve savcılar ise kendilerinin..."İbaresinin İncelenmesi

1- İptal Talebinin Gerekçesi

248. Dava dilekçesinde özetle, yargı organının unsurları ve şüphesiz en etkin figürleri olan hâkim ve savcılarının bir idarenin emrinde görevlendirilmelerinin Anayasa'ya açıkça aykırı olduğu, mevzuata göre yalnızca Adalet Bakanlığı bünyesinde, adli hizmete ilişkin görevlendirilmeleri söz konusu olan hâkim ve savcılarının TİB veya başka bir idare emrinde görevlendirilebilmelerinin mümkün olmadığı, iptali istenilen düzenlemede geçen "emrinde" ibaresinin dahi başlı başına yargı bağımsızlığı ve kuvvetler ayrılığı ilkesi ile bağdaşamaz nitelikte olduğu, "Mahkemelerin bağımsızlığı" ilkesine gölge düşürdüğü, ayrıca iptali istenilen ibarenin Anayasa'nın 140. maddesinin beşinci fıkrasında belirtilen "Anayasal düzene uygun bir kanun" kapsamında kabul edilemeyeceği, "Mahkemenin bağımsızlığı" ve "Hâkimlik teminatı" ilkelerini ihlal eden bir düzenlemenin Anayasa'nın Başlangıç bölümünün 4. paragrafında ifade edilen "kuvvetler ayrılığı" prensibine de aykırılık teşkil ettiği belirtilerek kuralın, Anayasa'nın Başlangıç kısmı ile 2., 138. ve 140. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

249. İptali istenilen ibarenin bulunduğu kuralda, 8.6.1984 tarihli ve 217 sayılı Devlet Personel Başkanlığı Kuruluş ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 2. maddesinde sayılan kamu kurum ve kuruluşlarında çalışanların kurumlarının, hâkim ve savcılarının ise kendilerinin muvafakati ile aylık, ödenek, her türlü zam ve tazminatlar ile diğer mali ve sosyal hak ve yardımları kurumlarınca ödenmek kaydıyla geçici olarak Telekomünikasyon İletişim Başkanlığı emrinde görevlendirilebileceği öngörülmektedir. Kuralda yer alan "...hâkim ve savcılar ise kendilerinin..."ibaresi, dava konusu kuralı oluşturmaktadır.

250. Anayasa'nın 2. maddesinde belirtilen hukuk devletinin en önemli ögesi sayılan yargı bağımsızlığı, mahkemelerin bağımsızlığı üzerine kurulur. Hâkimler de, mahkemelerin bağımsızlığı ve hâkimlik güvencesi esaslarına göre görevlerini yerine getirirler. Mahkemelerin bağımsızlığı ile

hâkimlerin görevlerinde bağımsız olmaları, birbirleriyle eş anlamlı, biri öbürünün nedeni ve doğal sayılacak ilkelerdir. Hâkimlik güvencesi de bu hukuksal bileşkenin gereğidir.

251. Anayasa'nın 138. maddesinde "Mahkemelerin bağımsızlığı", 139. maddesinde "Hâkimlik ve savcılık teminatı" ilkeleri yer almış; 140. maddesinin ikinci fıkrasında da, hâkimlerin görevlerini, mahkemelerin bağımsızlığı ve hâkimlik teminatı esaslarına göre yerine getirecekleri belirtilmiştir.

252. Hukuk devleti ilkesinin temel bileşenlerinden olan yargı bağımsızlığı, insan haklarının ve özgürlüklerinin başlıca ve en etkin güvencesidir. Mahkemelerin bağımsızlığı ilkesi, hâkimlerin görevlerinde bağımsız olduklarını ifade etmektedir. Hâkimlerin görevlerinde bağımsızlıkları ise onlara tanınan bir ayrıcalık olmayıp, adaletin, dolaylı dolaysız her türlü etki, baskı, yönlendirme ve kuşkudan uzak şekilde dağıtılması amacını gütmektedir. Yargının bir karakteri olan bağımsızlık, hâkimin, çekinmeden ve endişe duymadan, Anayasa'nın öngördüğü gereklerden başka herhangi bir dış etki altında kalmadan, yansız tutumla, özgürce karar verebilmesidir.

253. Hâkimlik teminatı da aynı amaca yönelik olup, hâkim ve savcılarının azledilmelerine, kendileri istemedikçe Anayasa'da öngörülen yaştan önce emekliye ayrılmalarına, herhangi bir sebeple aylık, ödenek ve diğer özlük haklarından yoksun bırakılmalarına engel oluşturmaktadır.

254. Gerek mahkemelerin bağımsızlığı gerekse hâkimlik teminatı ilkeleri, yargılama faaliyetine ilişkin ilkeler olup esas olarak adil bir yargılama sistemini sağlama amacını gütmektedirler.

255. Anayasa'nın 140. maddesinin beşinci fıkrasında "Hâkimler ve savcılar, kanunda belirtilenlerden başka, resmî ve özel hiçbir görev alamazlar" denilmektedir. Buna göre, hâkim ve savcılarının kanunda belirtilmek koşulu ile resmi ve özel görev alabilecekleri Anayasa koyucu tarafından kabul edilmiştir. Bu bağlamda, bir hâkim veya savcının başka bir kurum veya kuruluşta görevlendirilebilmesi için öncelikle hâkim veya savcının görevlendirileceği kurum veya kuruluşun kanununda açıkça görevlendirme yapılabileceğine dair bir düzenlemenin bulunması gerekmektedir. Dolayısıyla, bir hâkim veya savcının görevlendirileceği kurum veya kuruluşun kanununda görevlendirme yapılabileceğine dair bir düzenleme yoksa hâkim veya savcının geçici yetki veya görevlendirme ile o kurum veya kuruluşta görevlendirilebilmesi mümkün değildir. Bu şekilde geçici yetki veya herhangi bir görevlendirmeye başka bir kurum veya kuruluşta görevlendirilen hâkim veya savcının kadroları ile ilişkileri devam etmekte ve hâkim ve savcı statüleri korunmaktadır. Nitekim, bu hâkim ve savcılarının özlük işlemleri 2802 sayılı Kanun'a göre yapıлып Anayasa'da teminat altına alınan güvencelerden de yararlanmaktadırlar. Bu nedenle, Anayasa'nın 140. maddesinin beşinci fıkrası gereğince ancak bir kanunun açık hükmüne göre geçici yetki veya herhangi bir görevlendirmeye

başka bir kurum veya kuruluşta görevlendirilebilen hâkim ve savcının, 2802 sayılı Kanun'da tanımlanan hâkim ve savcı tanımının içerisinde yer almadığı söylenemez.

256. Kanunlarla belirlenecek resmi ve özel görevlerin belirlenmesinde ise kanun koyucunun yargı bağımsızlığı ve tarafsızlığı, hâkim ve savcılık teminatı ve bağımsızlığı ilkelerini içeren anayasal düzenlemeleri gözetmesi gerektiği açıktır.

257. İptali istenilen kural uyarınca hâkim ve savcılar kendilerinin uygun bulması ile Telekomünikasyon İletişim Başkanlığı emrinde görevlendirilebileceklerdir. Bu görevlendirme geçici olup, hâkim ve savcılarının aylık, ödenek, her türlü zam ve tazminatlar ile diğer mali ve sosyal hak ve yardımları kendi kurumları tarafından ödenecektir. Ayrıca, hâkim ve savcılar kurumlarından izinli sayılacaklar ve izinli oldukları sürece de meslekleri ile ilgili özlük hakları devam edecektir. Bunun yanında, Telekomünikasyon İletişim Başkanlığında görev yaptıkları süre de terfi ve emekliliklerinde hesaba katılacaktır. Terfileri başkaca bir işleme gerek kalmaksızın süresinde yapılacaktır.

258. Hâkim ve savcılarının TİB'de görevlendirilebilmeleri için 6087 sayılı Hâkim ve Savcılar Yüksek Kurulu (HSYK) Kanunu hükümleri uyarınca HSYK İkinci Dairesinin izin vermesi gerekmektedir. 6087 sayılı Kanun'un 9. maddesinin (2) numaralı fıkrasında HSYK İkinci Dairesinin görevleri yer almakta olup, aynı kuralın (a) bendinin beşinci sırasında ise, "Diğer kurumların geçici görevlendirme ve nakil taleplerine ilişkin izin işlemlerini yürütme" görevi İkinci Dairenin görevleri arasında düzenlenmiştir. Belirtilen bu hüküm uyarınca, muvafakatleri bulunan hâkim ve savcılarının TİB'de görevlendirilmelerine ilişkin izin işlemlerini HSYK İkinci Dairesi yapacaktır.

259. Hâkim ve savcılarının TİB'de görevlendirilmelerine ilişkin hüküm kanunla düzenlenmiş bulunmaktadır. Bunun yanında hâkimlik teminatı gereğince, görevlendirme yapılabilmesi için hâkim ve savcılarının kendi muvafakatlerinin bulunması şart koşulmuştur. Ayrıca, Telekomünikasyon İletişim Başkanlığının görev alanı ve hukukla olan ilişkisi gözetildiğinde, hâkim ve savcılarının mesleki bilgi ve birikimlerinden yararlanmak amacıyla Başkanlık emrinde görevlendirilmelerinde Anayasa'ya aykırılık bulunmamaktadır.

260. Açıklanan nedenlerle iptali istenilen ibare, Anayasa'nın 2., 138. ve 140. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

261. Serdar ÖZGÜLDÜR bu görüşe katılmamıştır.

262. Kuralın Anayasa'nın Başlangıç kısmı ile ilgisi görülmemiştir.

IV- YÜRÜRLÜĞÜN DURDURULMASI TALEBİ

263. Dava dilekçesinde özetle, iptali istenilen kuralların Anayasaya açıkça aykırı olduğu ve yürürlüklerinin durdurulmaması halinde hukuk devleti yönünden telafisi imkansız durum ve zararların ortaya çıkacağı, 6518 sayılı Kanun'un 5651 sayılı Kanun'da yaptığı değişikliklerle bilgi toplumuna giden yolda ciddi engeller yaratıldığı, ifade özgürlüğü, insan hakları ve temel hak ve hürriyetlerin korunması gibi temel konularda Avrupa Birliği Hukuku'na aykırı uygulamalara sebep olduğu, Anayasa'da teminat altına alınmış özel hayatın gizliliği, haberleşme hürriyeti, ifade hürriyeti, basın hürriyeti, dernek kurma/derneğe üye olup olmama hürriyeti, sendika kurma/sendikaya üye olup olmama hürriyeti, çalışma sözleşme hürriyeti, hak arama hürriyeti ve temel hak ve hürriyetlerin korunması ve temel hak ve hürriyetlerin ancak kanunla sınırlandırılabilmesi gibi temel insan hak ve hürriyetlerini daha da kısıtlayıcı ve sınırlandırıcı bir hale getirdiği, bu menfi durumun toplumda bilgi birikiminin sağlanması, bilgi ekonomisinin oluşturulması ve son olarak Türkiye'nin Bilişim Toplumu olarak küresel rekabette yerini alma hedefi ile bağdaşmadığı, erişim engelleme tedbiri hükmedilmesine imkan tanıyan söz konusu değişikliklerin oranlılık ve ölçülülük ilkelerinin uygulanmasını sağlamaktan uzak olduğu, özel hayatın gizliliği nedeniyle erişimin engellenmesi tedbirinin uygulanabilmesine imkan veren ve son derece suistimale açık bir durum ortaya koyan düzenleme ile TİB Başkanının emriyle ölçsüz şekilde erişimin engellenmesi tedbirinin uygulanabileceği bir durum yaratıldığı, bu düzenlemeler kapsamında verilecek erişimin engellenmesi kararlarının ESB eliyle uygulanmasının da son derece sakıncalı olduğu, bir yandan TİB'e sınırsız yetkiler verildiği, bir yandan da ifade özgürlüğü, dernek kurma/derneğe üye olup olmama özgürlüğü, haberleşme özgürlüğü, basın özgürlüğünün ihlal edildiği, özel hayatın gizliliği ihlal edilen kişilere başvuracak hiçbir kanun yolu öngörülmediği, 6518 sayılı Kanun'la getirilen sınırlamaların fazlasıyla geniş ve veri saklama süresi de dahil olmak üzere diğer tüm ayrıntıların düzenleyici işlemlerle idare tarafından belirlendiği, iptali istenilen kuralların özel hayata önemli nitelikte müdahale niteliğinde olduğu belirtilerek kuralların, yürürlüklerinin durdurulmasına karar verilmesi talep edilmiştir.

6.2.2014 tarihli ve 6518 sayılı Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un;

A- 93. maddesiyle 4.5.2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un değiştirilen 9. maddesinin (9) numaralı fıkrasında yer alan ".veya aynı mahiyetteki yayınların."ibaresine yönelik yürürlüğün durdurulması talebinin, koşulları oluşmadığından REDDİNE,

- B-** 1- 87. maddesiyle 5651 sayılı Kanun'un 4. maddesine eklenen (3) numaralı fıkraya,
- 2- 88. maddesiyle 5651 sayılı Kanun'un 5. maddesine eklenen (5) numaralı fıkraya,
- 3- 89. maddesiyle 5651 sayılı Kanun'un 6. maddesinin (1) numaralı fıkrasına eklenen (d) bendine,
- yönelik iptal hükümlerinin yürürlüğe girmelerinin ertelenmeleri nedeniyle bu fıkralara ve bende ilişkin yürürlüğün durdurulması talebinin REDDİNE,
- C-** 1- 8. maddesiyle değiştirilen, 4.1.1961 tarihli ve 213 sayılı Vergi Usul Kanunu'nun Mükerrer 257. maddesinin birinci fıkrasının (6) numaralı bendinin ".mükelleflerin Maliye Bakanlığına bağlı vergi dairelerine vadesi geçmiş borcu bulunmadığına ilişkin belge arama zorunluluğu getirmeye, bu zorunluluk kapsamına girecek amme alacaklarını tür ve tutar itibarıyla tespit etmeye ve hangi hâllerde bu zorunluluğun aranılmayacağına,." bölümüne,
- 2- 47. maddesiyle değiştirilen, 4.1.2002 tarihli ve 4734 sayılı Kamu İhale Kanunu'nun 38. maddesinin;
- a- İkinci fıkrasında yer alan ".gibi hususlarda." ibaresine,
- b- Üçüncü fıkrasının birinci cümlesinde yer alan ".açıklama istenilmeksizin sonuçlandırılabilmesine." ve ".açıklama istenilmeksizin reddedilmesine ilişkin." ibarelerine,
- 3- 48. maddesiyle 4734 sayılı Kanun'un 43. maddesine eklenen fıkrada yer alan ".yaklaşık maliyetin ." ve ".az ve %15'inden." ibarelerine,
- 4- 80. maddesiyle, 16.5.2006 tarihli ve 5502 sayılı Sosyal Güvenlik Kurumu Kanunu'nun 30. maddesine eklenen fıkraya,
- 5- 85. maddesiyle 5651 sayılı Kanun'un 2. maddesinin (1) numaralı fıkrasına eklenen (n) ve (r) bentlerine ve (o) bendinde yer alan "...ve benzeri yöntemler kullanılarak..." ibaresine,
- 6- 86. maddesiyle 5651 sayılı Kanun'un 3. maddesine eklenen (3) numaralı fıkraya,
- 7- 88. maddesiyle 5651 sayılı Kanun'un 5. maddesine eklenen (3), (4) ve (6) numaralı fıkralara,
- 8- 89. maddesiyle 5651 sayılı Kanun'un 6. maddesinin (1) numaralı fıkrasına eklenen (ç) bendine,
- 9- 90. maddesiyle 5651 sayılı Kanun'a eklenen 6/A maddesine,
- 10- 91. maddesiyle 5651 sayılı Kanun'un 7. maddesinin;
- a- Değiştirilen (2) ve (3) numaralı fıkralarına,
- b- Eklenen (4) numaralı fıkrasına,

11- 93. maddesiyle 5651 sayılı Kanun'un deęiřtirilen 9. maddesinin (5) ve (8) numaralı fıkralarına ve (9) numaralı fıkrasının ".veya aynı mahiyetteki yayınların." ibaresi dıřında kalan bölümüne,

12- 94. maddesiyle 5651 sayılı Kanun'a eklenen 9/A maddesinin (1), (2), (3), (4), (5), (6), (7) ve (8) numaralı fıkralarına,

13- 97. maddesiyle 5651 sayılı Kanun'un ek 1. maddesine eklenen (5) numaralı fıkranın birinci cümlesinde yer alan "...hâkim ve savcılar ise kendilerinin..." ibaresine,

14- 100. maddesiyle 5651 sayılı Kanun'a eklenen geçici 3. maddenin (1), (3) ve (4) numaralı fıkralarına ve (2) numaralı fıkrasının ikinci cümlesine,

yönelik iptal talepleri, 8.12.2015 tarihli, E.2014/87, K.2015/112 sayılı kararla reddediđinden, bu fıkra, bent, cümle, bölüm ve ibarelere iliřkin yürürlüđün durdurulması taleplerinin REDDİNE,

D- 100. maddesiyle 5651 sayılı Kanun'a eklenen geçici 3. maddenin (2) numaralı fıkrasının birinci cümlesi hakkında, 8.12.2015 tarihli ve E.2014/87, K.2015/112 sayılı kararla karar verilmesine yer olmadığına karar verildiđinden, bu cümleye iliřkin yürürlüđün durdurulması talebi hakkında **KARAR VERİLMESİNE YER OLMADIĐINA,**

8.12.2015 tarihinde OYBİRLİĐİYLE karar verilmiřtir.

V- İPTALİN DİĐER KURALLARA ETKİSİ

264. 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrasında, kanunun belirli kurallarının iptali, diđer kurallarının veya tümünün uygulanmaması sonucunu dođuruyorsa, bunların da Anayasa Mahkemesince iptaline karar verilebileceđi öngörülmektedir.

265. 6518 sayılı Kanun'un 89. maddesiyle 5651 sayılı Kanun'un 6. maddesinin (1) numaralı fıkrasına eklenen (d) bendinin iptali nedeniyle uygulanma olanađı kalmayan aynı maddenin (3) numaralı fıkrasında yer alan ". ve (d)." ibaresinin de 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrası geređince iptali gerekir.

VI- İPTAL HÜKMÜNÜN YÜRÜRLÜĐE GİRECEĐİ GÜN SORUNU

266. Anayasa'nın 153. maddesinin üçüncü fıkrasında, "Kanun, kanun hükmünde kararname ve Türkiye Büyük Millet Meclisi İçtüzüğü ya da bunların hükümleri, iptal kararlarının Resmî Gazetede yayımlandığı tarihte yürürlükten kalkar. Gereken hallerde Anayasa Mahkemesi iptal hükmünün yürürlüđe gireceđi tarihi ayrıca kararlařtırabilir. Bu tarih, kararın Resmî Gazetede yayımlandığı günden başlayarak bir yılı geçemez." denilmekte, 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrasında da bu kural tekrarlanmaktadır.

267. 6.2.2014 tarihli ve 6518 sayılı Kanun'un 87. maddesiyle 5651 sayılı Kanun'un 4. maddesine eklenen (3) numaralı fıkranın, 88. maddesiyle 5651 sayılı Kanun'un 5. maddesine eklenen (5) numaralı fıkranın, 89. maddesiyle 5651 sayılı Kanun'un 6. maddesinin; (1) numaralı fıkrasına eklenen (d) bendinin ve (3) numaralı fıkrasında yer alan "...ve (d)..." ibaresinin iptal edilmesi nedeniyle doğacak hukuksal boşluk kamu yararını ihlal edecek nitelikte görüldüğünden, Anayasa'nın 153. maddesinin üçüncü fıkrası ile 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince bu fıkralara, bende ve ibareye ilişkin iptal hükmünün, kararın Resmî Gazete'de yayımlanmasından başlayarak bir yıl sonra yürürlüğe girmesi uygun görülmüştür.

VII- HÜKÜM

6.2.2014 tarihli ve 6518 sayılı Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un;

A- 8. maddesiyle değiştirilen, 4.1.1961 tarihli ve 213 sayılı Vergi Usul Kanunu'nun Mükerrer 257. maddesinin birinci fıkrasının (6) numaralı bendinin;

1- ".mükelleflerin Maliye Bakanlığına bağlı vergi dairelerine vadesi geçmiş borcu bulunmadığına ilişkin belge arama zorunluluğu getirmeye," bölümünün Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Alparıslan ALTAN ile Erdal TERCAN'ın karşıoyları ve OYÇOKLUĞUYLA,

2- ".bu zorunluluk kapsamına girecek amme alacaklarını tür ve tutar itibarıyla tespit etmeye ve hangi hâllerde bu zorunluluğun aranılmayacağına," bölümünün Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Alparıslan ALTAN ile Erdal TERCAN'ın karşıoyları ve OYÇOKLUĞUYLA,

B- 47. maddesiyle değiştirilen, 4.1.2002 tarihli ve 4734 sayılı Kamu İhale Kanunu'nun 38. maddesinin;

1- İkinci fıkrasında yer alan ".gibi hususlarda." ibaresinin,

2- Üçüncü fıkrasının birinci cümlesinde yer alan ".açıklama istenilmeksizin sonuçlandırılabilmesine." ve ".açıklama istenilmeksizin reddedilmesine ilişkin." ibarelerinin,

Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

C- 48. maddesiyle 4734 sayılı Kanun'un 43. maddesine eklenen fıkrada yer alan ".yaklaşık maliyetin ." ve ".az ve %15'inden." ibarelerinin Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

D- 80. maddesiyle, 16.5.2006 tarihli ve 5502 sayılı Sosyal Güvenlik Kurumu Kanunu'nun 30. maddesine eklenen fıkranın Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Serdar ÖZGÜLDÜR'ün karşıoyu ve OYÇOKLUĞUYLA,

E- 85. maddesiyle, 4.5.2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 2. maddesinin (1) numaralı fıkrasına eklenen (n) ve (r) bentlerinin ve (o) bendinde yer alan "...ve benzeri yöntemler kullanılarak..." ibaresinin Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

F- 86. maddesiyle 5651 sayılı Kanun'un 3. maddesine eklenen (3) numaralı fıkranın Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, OYBİRLİĞİYLE,

G- 87. maddesiyle 5651 sayılı Kanun'un 4. maddesine eklenen (3) numaralı fıkranın Anayasa'ya aykırı olduğuna ve İPTALİNE, Serruh KALELİ, Hicabi DURSUN, Muammer TOPAL, Kadir ÖZKAYA ile Rıdvan GÜLEÇ'in karşıoyları ve OYÇOKLUĞUYLA, iptal hükmünün, Anayasa'nın 153. maddesinin üçüncü fıkrası ile 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince, KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAŞLAYARAK BİR YIL SONRA YÜRÜRLÜĞE GİRMESİNE, OYBİRLİĞİYLE,

H- 88. maddesiyle 5651 sayılı Kanun'un 5. maddesine eklenen;

1- (3), (4) ve (6) numaralı fıkraların Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

2- (5) numaralı fıkranın Anayasa'ya aykırı olduğuna ve İPTALİNE, Serruh KALELİ, Hicabi DURSUN, Muammer TOPAL, Kadir ÖZKAYA ile Rıdvan GÜLEÇ'in karşıoyları ve OYÇOKLUĞUYLA, iptal hükmünün, Anayasa'nın 153. maddesinin üçüncü fıkrası ile 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince, KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAŞLAYARAK BİR YIL SONRA YÜRÜRLÜĞE GİRMESİNE, OYBİRLİĞİYLE,

I- 89. maddesiyle 5651 sayılı Kanun'un 6. maddesinin (1) numaralı fıkrasına eklenen;

1- (ç) bendinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, OYBİRLİĞİYLE,

2- (d) bendinin Anayasa'ya aykırı olduğuna ve İPTALİNE, Serruh KALELİ, Hicabi DURSUN, Muammer TOPAL, Kadir ÖZKAYA ile Rıdvan GÜLEÇ'in karşıoyları ve OYÇOKLUĞUYLA, iptal hükmünün, Anayasa'nın 153. maddesinin üçüncü fıkrası ile 6216 sayılı Kanun'un 66. maddesinin (3)

numaralı fıkrası gereğince, KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAŞLAYARAK BİR YIL SONRA YÜRÜRLÜĞE GİRMESİNE, OYBİRLİĞİYLE,

3- (d) bendinin iptali nedeniyle uygulanma olanağı kalmayan aynı kuralın (3) numaralı fıkrasında yer alan ".ve (d)." ibaresinin de, 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrası gereğince İPTALİNE, iptal hükmünün, Anayasa'nın 153. maddesinin üçüncü fıkrası ile 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince, KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAŞLAYARAK BİR YIL SONRA YÜRÜRLÜĞE GİRMESİNE, OYBİRLİĞİYLE,

J- 90. maddesiyle 5651 sayılı Kanun'a eklenen 6/A maddesinin;

1- (1), (2), (3), (4), (5), (6), (8), (9) ve (10) numaralı fıkralarının Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

2- (7) numaralı fıkrasının;

a- Birinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, OYBİRLİĞİYLE,

b- İkinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Erdal TERCAN'ın karşıoyu ve OYÇOKLUĞUYLA,

K- 91. maddesiyle 5651 sayılı Kanun'un 7. maddesinin;

1- Değiştirilen (2) ve (3) numaralı fıkralarının,

2- Eklenen (4) numaralı fıkrasının,

Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

L- 93. maddesiyle 5651 sayılı Kanun'un değiştirilen 9. maddesinin;

1- (5) ve (8) numaralı fıkralarının Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

2- (9) numaralı fıkrasının;

a- ".veya aynı mahiyetteki yayınların." ibaresinin Anayasa'ya aykırı olduğuna ve İPTALİNE, Hicabi DURSUN, Kadir ÖZKAYA ile Rıdvan GÜLEÇ'in karşıoyları ve OYÇOKLUĞUYLA,

b- Kalan bölümünün Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Serdar ÖZGÜLDÜR'ün karşıoyu ve OYÇOKLUĞUYLA,

M- 94. maddesiyle 5651 sayılı Kanun'a eklenen 9/A maddesinin (1), (2), (3), (4), (5), (6), (7) ve (8) numaralı fıkralarının Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

N- 97. maddesiyle 5651 sayılı Kanun'un ek 1. maddesine eklenen (5) numaralı fıkranın birinci cümlesinde yer alan "...hâkim ve savcılar ise kendilerinin..." ibaresinin, Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, Serdar ÖZGÜLDÜR'ün karşıoyu ve OYÇOKLUĞUYLA,

O- 100. maddesiyle 5651 sayılı Kanun'a eklenen geçici 3. maddenin;

1- (1), (3), (4) numaralı fıkralarının Anayasa'ya aykırı olmadıklarına ve iptal taleplerinin REDDİNE, OYBİRLİĞİYLE,

2- (2) numaralı fıkrasının;

a- Birinci cümlesi, 27.3.2015 tarihli ve 6639 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun'un 30. maddesi ile değiştirildiğinden, konusu kalmayan bu cümleye ilişkin iptal talebi hakkında KARAR VERİLMESİNE YER OLMADIĞINA, OYBİRLİĞİYLE,

b- İkinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal talebinin REDDİNE, OYBİRLİĞİYLE,

8.12.2015 tarihinde karar verildi.

Başkan - Zühtü ARSLAN

Başkanvekili- Burhan ÜSTÜN

Başkanvekili- Engin YILDIRIM

Üye: Serdar ÖZGÜLDÜR; Serruh KALELİ; Osman Alifeyyaz PAKSÜT; Recep KÖMÜRCÜ; Alparslan ALTAN; Hicabi DURSUN; Celal Mümtaz AKINCI; Erdal TERCAN; Muammer TOPAL; M. Emin KUZ; Hasan Tahsin GÖKCAN; Kadir ÖZKAYA; Rıdvan GÜLEÇ

KARŞIOY GEREKÇESİ VE DEĞİŞİK GEREKÇE

1. "Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun Tasarısı" ile milletvekillerince verilen 10 ayrı "Kanun Teklifi", Türkiye Büyük Millet Meclisi (TBMM) Plân ve Bütçe Komisyonunda birleştirilerek görüşülmüş ve TBMM Genel Kurulu'na sevk edilmiş ve 6.2.2014 tarih ve 6518 sayılı "Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun" olarak kabul edilmiş ve 19.2.2014 tarih ve 28918 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir.

Bu Kanun'un 80. maddesi ile 5502 sayılı Kanun'un 30. maddesine eklenen fıkranın ve Kanun'un 93. maddesi ile 4.5.2007 tarih ve 5651 sayılı Kanun'un deęiştirilen 9. maddesinin (9) numaralı fıkrasının, keza Kanun'un 97. maddesi ile 5651 sayılı Kanun'un Ek-1. maddesine eklenen (5) numaralı fıkradaki iptali istenen ibarenin "Kanun Tasarısı"nda ve "Kanun Tekliflerinde" yer almadığı ve bu düzenlemelerin TBMM Plân ve Bütçe Komisyonunca birleřtirilen metne eklendięi anlařılmaktadır.

Anayasa'nın 88. maddesinde "Kanun teklif etmeye Bakanlar Kurulu ve milletvekilleri yetkilidir.

Kanun tasarı ve tekliflerinin Türkiye Büyük Millet Meclisinde görüřülme usul ve esasları İřtüzükle düzenlenir." denilmektedir. Anayasa'nın 88. maddesinin birinci fıkrasının ihlâli sonucu bir yasalařtırma söz konusuysa, bu konudaki ihlâl Anayasa'nın 148. maddesi anlamında bir "řekil sakatlığı"na deęil, doğrudan 88. maddesine aykırı düşer ve yapılacak anayasal denetimin, "řekil bakımından" deęil, "esas bakımından" söz konusu olması gerekir. 88. maddenin ikinci fıkrasındaki "Kanun tasarı ve tekliflerinin Türkiye Büyük Millet Meclisinde görüřülme usul ve esasları İřtüzükle düzenlenir" hükmünün de, bu açıklama çerçevesinde yorumlanması ve bu düzenlemenin aynı maddenin birinci fıkrasındaki anayasal hüküm doğrultusunda anlařılması ve hüküm ifade etmesi gerekir. Yani, birinci fıkraya aykırı bir durum söz konusu ise artık ortada doğrudan bir Anayasa ihlâli söz konusu olacak ve Anayasa'nın bu hükmünün bir tekrarından ibaret olan TBMM İřzüğü'nün 35. maddesinin ihlâli nedeniyle, Anayasa'nın 148. maddesinde belirtilen (ve son oylamaya iliřkin olmadığından kanunun iptalini gerektirmeyen) bir řekil sakatlığından ve řekil denetiminden deęil; 88. maddenin birinci fıkrasının ihlâli sonucu esası ilgilendiren bir sakatlıktan ve esas denetimden söz edilebilecektir.

Davanın somutu ile ilgili olarak düzenleme öngören TBMM İřtüzüğü'nün "Komisyonların yetkisi, toplantı yeri ve zamanı" bařlıklı 35. maddesinin ilgili bölümleri řöyledir: "Komisyonlar, kendilerine havale edilen kanun tasarı ve/veya tekliflerini aynen veya deęiřtirerek kabul veya reddedebilirler; birbirleriyle ilgili gördüklerini birleřtirerek görüřebilirler ve Türkiye Büyük Millet Meclisi Bařkanlığınca kendilerine ayrılan salonlarda toplanırlar.

Ancak, komisyonlar, 92 nci maddedeki özel durum dıřında kanun teklif edemezler, kendilerine havale edilenler dıřında kalan iřlerle uğrařamazlar. Bařkanlık Divanının kararı olmaksızın Genel Kurulun toplantı saatlerinde görüřme yapamazlar ve kanun tasarı ve tekliflerini bölerek ayrı ayrı metinler halinde Genel Kurula sunamazlar."

İřtüzüğün 35. maddesinin yukarıdaki açık metninden de açıkça anlařılacağı üzere, komisyonların kendilerine havale edilen kanun tasarı ve tekliflerini görüřme yetkileri sınırlandırılmış olup, komisyonların İřtüzüğün 92 nci maddesindeki özel durum dıřında (genel veya özel af ilanını içeren

kanun tasarı ve teklifleri) kanun teklif etme yetkileri yoktur. Yukarıda belirtilen yasa değişiklikleri Bakanlar Kurulunca önerilen Tasarı metninde olmadığı halde ve teklif metinlerinde Plân ve Bütçe Komisyonu tarafından Tasarı metnine ilave edilerek kanunlaştırıldığından; bu durum Anayasa'nın 88. maddesinin birinci fıkrasına (dolayısıyla de bu hükmün açıklaması mahiyetinde bulunan TBMM İÇTÜZÜĞÜ'nün 35 inci maddesine) açıkça aykırı düşmektedir.

Anayasa'nın 88. maddesinin birinci fıkrasının açık âmir hükmü karşısında, TBMM İÇTÜZÜĞÜ'nün 87 nci maddesi gerekçe gösterilerek, görüşülmekte olan bir tasarı veya teklifin konusu olmayan "başka" kanunlarda ek ve değişiklik getiren "yeni bir kanun teklifi mahiyetindeki" değişikliklerin "Genel Kurul" tarafından da yapılamayacağı açıktır.

Anayasa'nın 148. maddesindeki "Kanunların şekil bakımından denetlenmesi, son oylamanın, öngörülen çoğunlukla yapılıp yapılmadığı. hususları ile sınırlıdır." hükmünün de bu belirlemeye etkisinin olamayacağı kuşkusuzdur. Gerçekten, 88 nci maddenin birinci fıkrasına açıkça aykırı bir yasama faaliyeti sözkonusu olduğundan, Genel Kurulca öngörülen çoğunlukla yapılacak bir "son oylama"nın belirtilen Anayasa'ya aykırılığı düzeltereği kabul edilemez. Ancak 88 inci maddenin birinci fıkrasına uygun bir yasama faaliyeti içerisinde 148 inci maddedeki "şekil denetimi" kuralı işletilebilir. Davanın somutunda ise yukarıda açıklandığı üzere, aksi yönde bir yasama faaliyeti bulunduğu görüldüğünden; 148 inci maddenin bu davanın somutunda uygulama kabiliyeti bulunmamaktadır. (Bu konudaki bir inceleme için bkz.: Torba Yasalar ve Yasama sürecindeki İÇTÜZÜK Hükümlerinin Şekil Denetimi Sorunu, Hıfzı DEVECİ, TBB Dergisi, 2015 (117) s. 55-90)

Esasen Anayasa Mahkemesinin 25.12.2008 tarih ve E.2008/71, K.2008/183 sayılı kararına (RG 9.4.2009, Sayı:27195) konu iptal davası başvurusunun içeriğinden de, bu şekildeki bir uygulamanın TBMM İÇTÜZÜĞÜ'nün 35. maddesine aykırı düştüğünün TBMM Başkanlığınca saptandığı ve ilgili komisyona kabul edilen tasarı metninin iade edilmesine karşılık, ilgili komisyonca iade edilen tasarı metninin yeniden bir üst yazı ile Genel Kurulun onayına sunulmak üzere TBMM Başkanlığına geri gönderildiği ve akabinde yasalastığı anlaşılmaktadır.

Açıklanan nedenlerle; 6518 sayılı Kanun'un 80. maddesi ile 5502 sayılı Kanun'un 30. maddesine eklenen fıkranın ve Kanun'un 93. maddesi ile 5651 sayılı Kanun'un değiştirilen 9. maddesinin (9) numaralı fıkrasının ".veya aynı mahiyetteki yayınların." ibaresi dışında kalan bölümünün, Kanun'un 97. maddesi ile 5651 sayılı Kanun'un Ek-1. maddesine eklenen (5) numaralı fıkradaki iptali istenen ibarenin Anayasa'nın 88. maddesine aykırı düşmesi nedeniyle iptaline karar verilmesi gerektiği kanaatine ulaştığımdan; çoğunluğun aksi yöndeki kararına katılmıyorum.

Keza, Kanun'un 93. maddesi ile 5651 sayılı Kanun'un deęiřtirilen 9. maddesinin (9) numaralı fıkrasında yer alan ".veya aynı mahiyetteki yayınların." ibaresinin iptali yolundaki karara da yukarıdaki deęiřik gerekçeyle katılıyorum.

2. 6518 sayılı Kanun'un 8. maddesi ile deęiřtirilen 213 sayılı Kanun'un Mükerrer 257. maddesinin birinci fıkrasının (6) numaralı bendinin iptali istenen bölümüyle mükelleflere, vergi dairelerine olan borçlarının bulunması halinde bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel işaretlerin verilmesi yasaklanmakta ve bu konuda Maliye Bakanlığı gerekli düzenlemeleri yapmakla yetkili kılınmaktadır.

Anayasa Mahkemesinin 18.10.2007 tarih ve E.2007/4, K.2007/81; 14.2.2013 tarih ve E.2011/63, K.2013/28 sayılı kararlarında, iptal istemine konu kurala benzer yasal düzenlemeler "ölçülülük" ilkesine aykırı bulunarak iptal edilmiştir.

Anılan kararlarda da işaret edildięi üzere dava konusu kuralın "... mükelleflerin Maliye Bakanlığına baęlı vergi dairelerine vadesi geçmiş borcu bulunmadığına ilişkin belge arama zorunluluęu getirmeye ..." bölümünün, vatandaşlık ödevi kapsamında bulunan vergi borcu ve bu kapsamda bulunmayan kamu alacakları yönünden "ölçülü" bir sınırlama olmadığı açık olduęu gibi, bu alacakların tahsilini kolaylařtırmaya yönelik olsa da, mükelleflere anılan özel işaretlerin verilmemesi Anayasa'nın 48. maddesinde teminat altına alınan Çalışma ve Sözleşme Özgürlüęünün açık ihlali sonucunu doğurmaktadır. Dolayısıyla kuralın bu bölümünün Anayasa'nın 48. maddesine aykırılığı nedeniyle iptali gerekmektedir.

Kuralın bu bölümünün iptali durumunda geriye kalan "... bu zorunluluk kapsamına girecek amme alacaklarını tür ve tutar itibarıyla tespit etmeye ve hangi hallerde bu zorunluluęun aranılmayacağına ..." bölümünün de uygulanma olanağı kalmayacağından; bu bölümün de 6216 sayılı Kanun'un 43. maddesinin (4) numaralı fıkrası uyarınca iptali gerekmektedir.

Açıklanan nedenlerle; Anayasa'nın 48. maddesine aykırı olan kuralın iptaline karar verilmesi gerektięi kanaatine vardığımdan, çoęunluęun aksi yöndeki kararına katılmıyorum.

Üye - Serdar ÖZGÜLDÜR

KARŞIOY

5651 sayılı Kanun'un 4. maddesine eklenen üçüncü fıkrada içinde yer alan "Talep ettięi bilgileri talep edilen şekilde başkanlığa teslim eder" ibaresi ile yine aynı Yasa'nın 5. maddesine eklenen (5) numaralı

fıkrasında ve 6. maddesine eklenen (1) numaralı fıkranın (d) bendinde yer alan aynı ibarenin, Mahkememizce Anayasa'nın 2., 13. ve 20. maddelerine aykırı görülerek oyçokluğu iptal eden çoğunluk görüşüne katılmamıştır.

Dava dilekçesinde, talep halinde TİB Başkanlığınca yer, erişim ve içerik sağlayıcılar tarafından, teslim edilecek bilgilere erişimi sınırlandıracak bir düzenlemeye yer verilmediği, her türlü bilgiyi teslim etmenin hak arama hürriyetini ortadan kaldırdığı, hakkı ihlal edilenin hangi kanun yolunu kullanarak hangi merciye başvuracağı ve sürelerinin gösterilmediği nedenleri ile Anayasanın ilgili maddelerine aykırılığı ileri sürülmüştür.

İptali istenilen maddelere konu talep edilen bilgilerin, bir an için kişilerle ilgili belirlenmiş her türlü bilgi olduğu düşünülebilirse de, Anayasa Mahkemesinin 2.10.2014 gün ve 2011/149 Esas, 2014/151 Karar sayılı İPTAL kararı karşısında, yer ve erişim sağlayıcıların temin ettiği, Anayasa ile teminat altına alınan, iletişimin gizliliği, düşünce ve ifadeyi yayma özgürlüğü, haberleşme özgürlüğü, kişisel verilerin korunması gibi bir çok temel hakla doğrudan ilintili edinilmiş trafik bilgilerinin, kural ve sınırlamaya tabi olmaksızın TİB Başkanlığınca edinilmesinin Anayasa'ya aykırı kabul edildiği hukuksal durum karşısında ayrıca TİB tarafından talep edilecek bilgilerin korumadan yoksun bilgi kapsamında olamayacağı açıktır.

Nitekim TİB yetkililerinin talep edilen bilgilerin kişisel verilere ilişkin olmayıp içerik ve yer sağlayıcıların güncel adres bilgileri ile sınırlı ve uygulamanın da bu şekilde olduğu ifadeleri dikkate alınmalıdır. Ayrıca; Başkanlığın talep edeceği bilgilerin, kendisine bu Kanun ve diğer kanunlarla verilen görevlerin ifası kapsamında sınırlandırıldığı, 5651 sayılı Yasa'nın 4. maddesine eklenen üçüncü fıkrasından da anlaşılmaktadır. Söz konusu düzenleme karşısında kuralda tanınmış yetkinin sınırlanmadığı da söylenemeyecektir.

Kanun kapsamı irdelendiğinde, internetin güvenli kullanımını sağlama, kanun kapsamına giren suçları oluşturan içeriğe sahip faaliyet ve yayınları önleme amaçlı olduğu bunun için esas ve usul belirleyerek gerekli tedbir alma kriter belirleme görevi bulunduğu, kolluk ve soruşturma mercilerine yardımda bulunmak bu maksatlarla içerik yer ve erişim sağlayıcılar ile koordinasyon içinde faaliyette bulunulacağına yönelik olduğu görülecektir.

Anayasa'nın 20. maddesinde belirtilen özel hayatın gizliliği, 22. maddesindeki haberleşme özgürlüğü, 26. maddesindeki düşünceyi açıklama ve yayma gibi kural kapsamında ilintili görülen haklar sınırsız temel haklar değildir.

Kişisel verilen korunması hakkı insanın maddi ve manevi bütünlüğünün gelişiminde ne kadar temel ve öncelikli olsa da, bu hak veri sahibine mutlak ve sınırsız bir hakimiyet alanı bırakmamaktadır. 1981 tarih ve 108 sayılı kişisel verilerin otomatik işleme tabi tutulması karşısında kişilerin korunmasına dair Avrupa Konseyi Sözleşmesi'nin 9. maddesinde devlet, kamu, güvenlik, ekonomik menfaatlerin korunması ve SUÇLARLA MÜCADELE KAPSAMINDA kişisel verilerin korunmasına sınırlama getirilebileceği kabul edilmiştir. Yine Sözleşme'nin 5. maddesinde göre kişisel veriler açıkça belirlenmiş meşru amaçlar için, toplanma gerekçesiyle sınırlı olmak ve gerekli süreyi aşmamak şartlarıyla tutulabileceği kabul edilmiştir. Nitekim 5651 sayılı Yasa 5. maddesinin üçüncü fıkrasında sağlanmış trafik bilgilerinin gizliliğinin sağlanarak ne kadar süre ile saklanabilecekleri açıkça ifade edilmektedir.

TİB Başkanlığına ulaştırılmış bilgilerin, kanunun verdiği yetki ve belirlenmiş görev alanı kapsamında sınırlandırıldığı düşünüldüğünde bilgilerin amaç-araç kapsamında yöntem sınırlaması yapılmadan ölçsüz bir biçimde saklandığı ve kullanılabilir halde bulduğunu söyleme olanağı yoktur.

İptali istenen hükmün TİB Başkanlığının tüm internet kullanıcılarının iletişim verilerinin her hangi bir sınırlama getirilmeden toplanmasının mümkün hale getirdiğini, özel hayata müdahaleye sebep olan uygulamanın hak arama hürriyetini ortadan kaldırdığı, TİB Başkanlığınca talep edilen bilgilerin mahiyeti, talep yönteminin belirsizliği, bilginin içinde özel hayat bilgisi de olup bununda talep halinde verileceği ileri sürülmüş ise de; 5651 sayılı Yasa'nın 2. maddesinin (e), (f) ve (j) bentleri, kapsamında yer alan yer, hizmet ve erişim sağlayıcıların; taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş anı, yararlanılan hizmetin türü, aktarılan veri miktarı ve abone kimlik bilgileri, bu olanakları sağlayanlar, kullanıcıya sunulan bilgileri üreten, değiştiren gerçek ya da tüzel kişiliklere ait veriler, yasanın erişeceği bilginin sınırları olarak belirlediğinden, özel kişisel hayat bilgisi, şahsi, gizli, ticari sır nitelikli bir bilgiyi edinme ve toplama gibi bir yetkilerinin bulunmadığı görülmelidir. Kanun, görev kapsamında edinilebilecek bilgi yetkisinin sınırlarını açıkça tanım maddesinde ifade etmiştir.

5809 sayılı Elektronik Haberleşme Yasası'nın 6. maddesinin (ı) bendinde yer alan Bilgi Teknolojileri ve İletişim Kurumunun elektronik haberleşme ile ilgili olarak ihtiyaç duyacağı her türlü bilgi ve belgeyi gerçek ve tüzel kişilerden alabilmesine ilişkin kuralın, iptali istemiyle geldiği Mahkememizde kurumun amaç ve görev alanında yer alan sektör ve ilgili şikayetleri değerlendirme ve denetim işlevlerinin gereği gibi yerine getirilebilmesi amacı ile sınırlı olarak, abone ve kullanıcıların kişisel bilgilerin gizliliği ve ticari sırları da koruma görevi olduğu da düşünüldüğünde, kuralın verdiği yetkinin özel hayat ve haberleşme özgürlüğüne yönelik olduğunun düşünülmemeyeceği ve bu hakları

sınırlamadığı gerekçeler ile 2008/115 Esas, 2011/86 Karar sayılı dosyada Anayasa'ya uygun bulunduğuna dikkat çekmek gerekir.

Günümüzde, iletişim ve bilgiye ulaşımında oluşan teknolojik kolaylıklar ile oluşabilecek hukuksuzluklar karşısında, kendisini oluşturan kişi ve devlet varlığını yaşatma ve koruma sorumluluğunda oluşan olağanüstü yoğunluk ve teknolojik çağda, hakların korunması ve birey/devlet arası hakların korunmasının dengelenmesinde aşırı hassasiyet eşiğine ulaşılmıştır. Demokratik toplum inşasında, yıkılmasının önüne geçecek tedbirleri alma zorunluluğu gözetilmeden hürriyetler kendilerinin sınırsız hakimiyet alanına terk edilemez.

Elbette Anayasal hak ve hürriyetlerin demokratik toplum gereklerine uygun şekilde ve ölçüsüz bir müdahaleye uğramadan kullanılması, hissedilmesi demokratik toplum temel öğelerinden varsayılmakta ise de Anayasa'da yazılı çerçevesi içerisinde hak kullanımının da bir sınırının bulunduğu kişi bilincinde yer almalı ve gözden uzak tutulmamalıdır.

Mahkememiz karar gerekçesinde Anayasa'nın 20. maddesinde yer alan özel ve aile hayatına saygı kapsamında, herkesin kendisi ile ilgili veriler hakkında bilgilenme, erişme amacı doğrultusunda kullanılıp kullanılmadığını öğrenme hakkı olduğuna değindikten sonra iptali istenen kuralda geçen "bilgi" kelimesinin, kişiye ait BÜTÜN bilgileri (kişisel verileri) kapsadığını değerlendirmekte, bunlarında TİB tarafından istenebileceğini talep edilen bilgilerden kişilerin haberdar olmalarına ilişkin bir düzenlemenin de bulunmadığını ifade etmektedir.

İptali istenen kuralda geçen kişisel veri, yukarıda da açıklandığı gibi kişiye özel, gizli, saklı, sır, özel hayat bilgisi olmayıp, internet kullanıcısının bu ortamda yer alması dolayısıyla yararlandığı yer, erişim ve hizmet sağlayıcıların 5651 sayılı Yasa'nın 2. maddesinde sayılı kişilik tipleri ve kullanılan elektronik ortama ilişkin teknik bilgileri ile sınırlıdır. Yasanın görev ve yetki alanı dışında bilgi edinilmesi mümkün olmadığı düşünüldüğünde edinilmesi mümkün olmayan bilginin aktarılması ya da talebi de mümkün değildir.

Kişinin, TİB Başkanlığından istenecek bilgisinin aktarılmasından haberdar edilme keyfiyetine ilişkin bir açıklık olmadığı yönündeki gerekçeye de katılmamıştır. Kullanıcının elektronik ortama girdiğinde nelerle karşılaşabileceği yasada açıkça yazdığına göre kendisi için sürpriz olmayacak bu hukuki açıklık karşısında somutta haberdar edilme mutlak bir zorunluluk olmaktan çıkmaktadır. Kaldı ki Yasa'nın 3. maddesinde bildirim yükümlülüğünün nasıl yerine getirileceği de açıklamış bu hükmün Anayasa'ya aykırılık iddiası da Mahkememizce reddedilmiştir.

YİNE Mahkememiz gerekçesinde, Anayasa'nın 20. maddesinin üçüncü fıkrasında yer alan kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızası ile işlenebilir kuralı karşısında iptali istenen düzenlemede, kanunda öngörülen hallerin neler olduğu 5651 sayılı Yasa'da açıkça belirtilmediği ifade edilmiş ise de, TİB Başkanlığının Yasa'nın 4. maddesinin Ek 3. fıkrasında, bu kanun ve diğer kanunlarda verilen görevlerin ifası kapsamında talep edeceği bilgiler hakkında gerektiğinde tedbir almakla yetkili olduğu düşünüldüğünde tedbir yani varsayılan hakkın kullanımına gelen sınırlama ya da yegane müdahale nedenlerinin (yani kanunda öngörülen haller) neler olduğu Yasa'nın 8. maddesinde açıklanmaktadır.

Bir koruma tedbiri olarak verilen erişimin engellenmesi, yani tedbir kararına neden ihtiyaç duyulacağı, kanunun birinci maddesinde yer alan amaç bölümü ve genel gerekçesi ile birlikte ve bir bütün olarak incelendiğinde ve internetin güvenli kullanımının sağlanması, kanun kapsamına giren suçlarla mücadele, kolluk ve soruşturma mercilerine yardım olarak açıklandığı düşünüldüğünde, TİB' e verilen yetkinin öngörülmemiş ve meşru amaç zemini dışında, ölçsüz olduğunu söylemeye imkan bulunmamaktadır.

Bu anlamda TİB'e verilen tedbir alma yetkisinin esasları belirli, çerçevesi çizilmiş, bağlı bir yetki olduğu düşünüldüğünde bunun yetki devri niteliği bulunmamaktadır.

Anayasa'nın 26. maddesinin ikinci fıkrası hükmü de gözetildiğinde kural Anayasa'ya aykırı bulunmamıştır.

Kanun'un 8. maddesiyle değiştirilen 213 sayılı Vergi Usul Kanunu mükerrer 257. maddesinin birinci fıkrasının (6) numaralı bendinde ".mükelleflerin Maliye Bakanlığına bağlı vergi dairelerine vadesi geçmiş borcu bulunmadığına ilişkin belge arama zorunluluğu getirmeye, bu zorunluluk kapsamına girecek amme alacaklarını tür tutar itibarıyla tespit etmeye ve hangi hallerde bu zorunluluğun aranılmayacağına,..." hükmü yer almakta ve iptali istenmektedir.

Kurala göre, vergi dairelerine vadesi geçmiş borcu bulunmadığına ilişkin belge getirmeyen mükelleflere bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretler verilmeyecek, dolayısıyla mükellef bu zorunluluğa uymadığı için ticaret yapamayacaktır.

Anayasa'nın 48. maddesinde herkesin dilediği alanda çalışma ve sözleşme hürriyeti ile sahip olduğu özel teşebbüs kurma serbestiyesine sahip olduğu, devletinde özel teşebbüsleri güvenli ve kararlılık içerisinde sosyal amaçlarına uygun çalışmasını temin edecek tedbirler almakla yükümlü olduğu ifade edilmiştir. Madde de ayrıca bir sınırlama sebebi de sayılmamaktadır.

Kural ile gelen müdahale, özel teşebbüsün çalışma hakkını zedelemekten öte ortadan kaldırmakta, zaten devlete bir borcu olan mükellefi ödemeye zorlamadan öte, ticaret yapmaktan, kazanmaktan, maddi ve manevi bütünlüğünü geliştirme ve koruma haklarından yoksun bırakmaktadır.

Çağdaş demokrasiler, demokratik hukuk devletlerinde hak ve özgürlüklerin EN GENİŞ şekilde sağlanıp güvence altına alındığı rejimler ise, haklara müdahale eden kuralların anılan nitelemeye uygun biçimde dar yorumundan kaçınarak değerlendirilmesi gerekir. Hukuk devletinden, hak ve özgürlükleri koruması her alanda güçlenerek, adaletli bir düzen sağlaması, hakka saygılı, hakkın elde edilmesini kolaylaştıran önündeki engelleri kaldıran, mutluluğu amaç edinen hakkaniyetli, müdahale eden kural içeriğinin, bireyin davranış direncine izin verecek ölçekte olması beklendiğinde, kamu yararı ile birey hakları arasında adil bir dengenin de gözetilmiş olması zorunludur.

Ancak kural kendinden olmasa da, hakkın doğasından gelen bir sınırlama sebebi ile müdahale edilebilen bir alan içerisine alındığında ise, müdahale hakkın kullanılmasına mutlak engel teşkil etmemelidir. Demokratik toplum düzeninde özgürlükler asıl, sınırlamalar istisnadır. Hakkın özüne dokunma yasağının ölçüğü de Anayasa'nın ruh ve sözüne, insan hakkına saygıya dayalı ölçülülük ilkesidir.

Maliye Bakanlığına kural ile getirilen yetki, devlete borçlu olana ticaret yaptırmama yasağıdır. Mükellefin devlete olan vergi borcunu, kamu alacağının görece üstünlüğü karşısında güvence altına almak kaygısıyla, tahsilatı hızlandırmaya yönelik meşru bir amacı olduğu kabul edilse bile, anılan müdahalede amaca erişmek için lüzumlu sınır aşılmalı, yani daha hafif bir önlemlerle amaca erişmek etkili olacak iken iptali istenen kuralda bu yönde bir yol seçilmemiş olması ölçülülüğün gereklilik ilkesini karşılamamaktadır.

Kaldı ki, makul ve dengeli olmayan müdahalenin, mükellefin ticaret hayatını bitiren, yaşam kalitesini engelleyen sonuçlar doğuracağı da düşünüldüğünde orantılı olduğu da söylenemeyecektir.

Demokratik hukuk devletinde güdülen amaç ne olursa olsun özgürlük kısıtlamalarının bu rejimlere özgü olmayan yöntemlerle yapılmaması ve belirli bir özgürlüğün ortadan kaldırılması düzeyine vardinilmemesi gerekir. Pekala, vergi borçlusunun borcunu tahsil etmede sayısız kamu gücü üstünlüğü sağlayan yollar ve usuller mevcut olup, geçici süre, sayısal sınırlamalar, tekerrür hallerine yönelik değişik yaptırım türleri gibi amaca erişmeye yönelik hakkın özünü zedelemeyen önlemler mevcut iken doğrudan hakkın kullanımını ortadan kaldıran iptali istenen kural, demokratik düzenin gerekli kıldığından fazla ve ulaşılmak istenen amaçtan ötedir.

Kuralda yer alan, bu zorunluluk kapsamına girecek amme alacaklarını, tür ve tutar itibariyle tespit etmeye ve hangi hallerde bu zorunluluğun aranılmayacağına ilişkin bölüme ilişkin olarak kuralın geri kalan bölümünün Anayasa'ya aykırı olduğu ve iptal edilmesi gerektiğini tarafımdan düşündüğünde, uygulama alanı kalmayacak bu bölüm yönünden de 6216 sayılı Yasa'nın 43. maddesinin üçüncü fıkrası uyarınca iptal edilmesi gerekeceği düşüncesi oluşacaktır.

Yukarıda anlatılan nedenler ile kuralın Anayasa'nın 2., 13. ve 48. maddelerine aykırı olduğu nedenleri ile çoğunluk görüşüne katılmamıştır.

Üye - Serruh KALELİ

KARŞIOY YAZISI

1. 6518 sayılı Kanun'un 8. maddesiyle, 213 sayılı Vergi Usul Kanunu'nun mükerrer 257. maddesinin birinci fıkrasının değiştirilen (6) numaralı bendinde Maliye Bakanlığının vergi güvenliğini sağlamak amacıyla niteliklerini belirleyip onayladığı, elektrikli, elektronik, manyetik ve benzeri cihazlar ve sistemleri kullanılmaya, bu cihaz ve sistemler vasıtasıyla bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretlerin verilmesinde, "mükelleflerin Maliye Bakanlığına bağlı vergi dairelerine vadesi geçmiş borcu bulunmadığına ilişkin belge arama zorunluluğu getirmeye, bu zorunluluk kapsamına girecek amme alacaklarını tür ve tutar itibariyle tespit etmeye ve hangi hallerde bu zorunluluğun aranılmayacağına" ilişkin usul ve esasları belirlemeye yetkili olacağı öngörülmektedir. Kuralın Anayasa'ya uygunluğu iki bölüm halinde denetlenmiş olmakla birlikte cümlenin tümü için geçerli olan karşı görüşümüz aşağıda açıklanmıştır.

2. İptali istenen kural uyarınca Maliye Bakanlığına bağlı vergi dairelerine vadesi geçmiş borcu bulunmadığını belge ile kanıtlayamayan kişilere, yasada sayılan özel etiket ve işaretler verilmeyecektir. Buna göre, yaptıkları ticaret icabı bu özel işaret ve etiketleri temin etmek, aksi takdirde idari veya cezai yaptırımlarla karşılaşmak zorunda bulunan kişilerin Maliye'ye borçlarını ödemedikleri müddetçe ticaretlerini sürdürmeleri mümkün olamayacaktır.

3. Anayasa'nın 48. maddesinde "Herkes, dilediği alanda çalışma ve sözleşme hürriyetlerine sahiptir. Özel teşebbüsler kurmak serbesttir" denilmiştir; bu hürriyetler için herhangi bir sınırlama nedeni de öngörülmemiştir.

4. Anayasa'nın 13. maddesinde, temel hak ve özgürlüklerin özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği,

bu sınırlamaların Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacağı belirtilmiştir.

5. Öte yandan, Anayasa'nın ilgili maddesinde özel bir sınırlama nedeni öngörülmeven hakların da hakkın doğasından kaynaklanan bazı sınırlarının bulunduğu tereddüt yoktur. Bu haklar, diğer Anayasal hükümler nedeniyle sınırlandırılabilir. Bu kapsamda, her ne kadar vergiyi bir vatandaşlık ödevi olarak kabul eden Anayasa'nın 73. maddesinin, bu ödevin yerine getirilmesi amacıyla serbestçe ticaret yapma hakkına bir sınırlama getirdiği öne sürülebilirse de bu sınırlamanın yine Anayasa'nın 13. maddesindeki ilkelere göre demokratik bir toplumda zorunlu ve ölçülü olması gerekir.

6. Kanunlarda, vergi borçlarının ve diğer amme alacaklarının tahsili için özel yöntemler ve gecikme halinde uygulanacak yüksek faizler öngörülmüş, diğer taraftan uzlaşma, erteleme, taksitlendirme gibi kolaylıklar da gözetilmiştir. Vergi tahsilatının amacının, mükellefi mali yönden çökertmek pahasına da olsa her türlü zorlayıcı yöntemi kullanarak vergiyi süratle almak olmadığı, kamu hizmetlerinin yürütülmesi için gerekli olan Maliye'ye düzenli vergi geliri sağlanması ile çalışanların ve müteşebbislerin rahatça işlerini sürdürebilmeleri ihtiyacı arasında adil bir dengenin kurulması gerektiği açıktır. Nitekim Anayasa'nın 5. maddesiyle Devlete verilen görevler de bunu gerektirmektedir. Bu nedenledir ki mükelleflerin çok ağır gelen vergilerini ödemekte geciktikleri ve artan borçları defaten kapatma imkanını kaybettikleri ve bu durumun genel bir soruna dönüştüğü hallerde yasa koyucu müteaddit defalar, özel yasalarla vergi affı, erteleme, taksitlendirme gibi kolaylıklar sağlamıştır.

7. İptali istenen kural, çeşitli nedenlerle vergi borcu bulunan ve ticaretlerini sürdürebilmek için yasada sayılan özel etiket ve işaretlere ihtiyacı bulunan kişilerin bu etiket ve işaretleri temin ettikten sonra elde edecekleri kazançları ile Maliye'ye borçlarını ödemesine de imkan bırakmamaktadır. Buna göre kişi, ihtiyaç duyduğu özel etiket ve işaretleri alamadığı için işine ara vermek zorunda kalabilecek, ancak mali durumu böylece daha da kötüleşeceğinden, vergi borçlarını ödemesi de güçleşecektir. Bu durumda kuralın, gözetilen amaca elverişli olduğu da söylenemez. Nitekim Anayasa Mahkemesinin Esas: 2007/4, Karar: 2007/81 sayılı kararında kişilerin vergi borcu nedeniyle yurt dışına çıkışlarının yasaklanmasına ilişkin yasa kuralının iptali gerekçeleri arasında, yurt dışına çıkışı yasaklamanın, vergi tahsilatını sağlamaya yeterli olmadığına da dikkat çekilerek, amaçla araç arasında ilişki bulunmadığı belirtilmiştir.

8. Vergi ve diğer amme alacaklarının tahsilatının hızlandırılması amacıyla çalışma özgürlüğüne bir müdahalede bulunan kuralın, Anayasa'nın 13. maddesindeki ölçütleri karşıladığından söz edilemez.

9. Bu nedenle kuralın, Anayasa'nın 13. ve 48. maddelerine aykırı olduğu ve iptali gerektiği düşüncesindeyim.

Üye - Osman Alifeyyaz PAKSÜT

KARŞIOY GEREKÇESİ

6.2.2014 tarihli ve 6518 sayılı Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un bazı madde ve fıkralarının Anayasa'ya aykırı olduğu gerekçesiyle iptali istenmiştir. Mahkememiz çoğunluğu tarafından, sözkonusu Kanun'un 8. maddesiyle değiştirilen 213 sayılı Vergi Usul Kanunu'nun mükerrer 257. maddesinin birinci fıkrasının 6. bendindeki değişikliklerin bir kısmının iptali talebinin reddine karar verilmiştir. Ancak aşağıda açıklanan nedenlerle belirtilen kısmın Anayasa'ya aykırı olduğu ve iptali gerektiği kanaatinde olduğumuzdan, çoğunluk görüşüne katılmamız mümkün olmamıştır:

213 sayılı Vergi Usul Kanunu'nun mükerrer 257. maddesinin iptali istenilen bölümün de bulunduğu birinci fıkrasının 6. bendi şöyledir:

Maliye Bakanlığı;

"6. (Ek: 3/7/2005 - 5398/23 md.; Değişik: 6/2/2014 - 6518/8 md.) Vergi güvenliğini sağlamak amacıyla niteliklerini belirleyip onayladığı elektrikli, elektronik, manyetik ve benzeri cihazlar ve sistemleri kullandırmaya, bu cihaz ve sistemler vasıtasıyla bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretlerin kullanılmasına ilişkin zorunluluk getirmeye, mükelleflere bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretlerin verilmesinde, mükelleflerin Maliye Bakanlığına bağlı vergi dairelerine vadesi geçmiş borcu bulunmadığına ilişkin belge arama zorunluluğu getirmeye, bu zorunluluk kapsamına girecek amme alacaklarını tür ve tutar itibarıyla tespit etmeye ve hangi hâllerde bu zorunluluğun aranılmayacağına, bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretlerin basımı, dağıtımı ile sistemin kurulması ve işletilmesi hizmetlerinin, 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununa tabi olmaksızın, süresi 5 yılı geçmemek üzere ve 4/1/2002 tarihli ve 4734 sayılı Kamu İhale Kanunu (5 inci maddesinin beşinci fıkrası hariç) hükümleri çerçevesinde; yetkilendirilecek gerçek veya tüzel kişiler tarafından yerine getirilmesine, bu hizmetlerde ve yetkilendirilecek gerçek veya tüzel kişilerde bulunması gereken özellikleri, yetkilendirilecek gerçek veya tüzel kişilerin

faaliyetlerinin yönlendirilmesi, izlenmesi, denetlenmesi, yetkilendirmenin sonlandırılması ve bunların uygulanmasına ilişkin usul ve esasları belirlemeye,"

Yetkilidir.

Hükümdeki ".mükelleflerin Maliye Bakanlığına bağlı vergi dairelerine vadesi geçmiş borcu bulunmadığına ilişkin belge arama zorunluluğu getirmeye, bu zorunluluk kapsamına girecek amme alacaklarını tür ve tutar itibarıyla tespit etmeye ve hangi hâllerde bu zorunluluğun aranılmayacağına,.." kısmının iptali istenmiştir.

Mahkememiz çoğunluğu, kuralı Anayasa'ya aykırı görmemiş, iptal talebini reddetmiştir.

İptali istenilen kuralın gerekçesinde konu ile ilgili olarak:

"213 sayılı Vergi Usul Kanununda değişiklik yapılması suretiyle, kayıt dışı ekonominin yüksek olduğu sektörlerde kayıp ve kaçak ile mücadele edilmesi amacıyla Bandrollü ürün İzleme Sisteminin getirilmesinin, söz konusu sistemin işletilmesinin ve sistem içindeki firmaların vergi borcunun daha etkin bir şekilde takibinin sağlanması amaçlanmıştır" denilmiştir.

Görüldüğü gibi, iptali istenen kısımlarla birlikte hüküm, Maliye Bakanlığına verilen bazı yetkileri düzenlemektedir. Maliye Bakanlığının; vergi güvenliğini sağlamak amacıyla niteliklerini belirleyip onayladığı elektrikli, elektronik, manyetik ve benzeri cihazlar ve sistemleri kullanılmaya, bu cihaz ve sistemler vasıtasıyla bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretlerin kullanılmasına ilişkin zorunluluk getirmeye, mükelleflere bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretlerin verilmesinde, mükelleflerin Maliye Bakanlığına bağlı vergi dairelerine vadesi geçmiş borcu bulunmadığına ilişkin belge arama zorunluluğu getirmeye, bu zorunluluk kapsamına girecek amme alacaklarını tür ve tutar itibarıyla tespit etmeye ve hangi hâllerde bu zorunluluğun aranılmayacağına yetkili olduğu belirtilmiştir.

Kuralın uygulanmasının bir sonucu olarak, vergi dairelerine vadesi geçmiş borcu bulunmadığına ilişkin belge getirmeyen mükelleflere bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretler verilmeyecek, dolayısıyla mükellefler bu zorunluluğa uymadıkları için ticaret yapamayacaklardır. Kural uyarınca mükelleflere bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretlerin verilebilmesi için vergi dairelerine vadesi geçmiş borçlarının bulunmaması gerekmektedir.

Kuralda, bu zorunluluk kapsamına girecek olan alacaklardan "amme alacakları" olarak bahsedilmiştir. 6183 sayılı Kanun'un 1. maddesinde, kamu alacağı, Devlete, vilayet hususi idarelerine ve belediyelere ait vergi, resim, harç, ceza tahkik ve takiplerine ait muhakeme masrafı, vergi cezası,

para cezası gibi asli, gecikme zammı, faiz gibi fer'i amme alacakları ve aynı idarelerin akitten, haksız fiil ve haksız iktisaptan doğanlar dışında kalan ve amme hizmetleri tatbikatından mütevellit olan diğer alacakları ile; bunların takip masrafları olarak tanımlanmıştır.

Kurala göre Maliye Bakanlığı, bu zorunluluk kapsamına girecek amme alacaklarını tür ve tutar itibarıyla tespit etmeye ve hangi hâllerde bu zorunluluğun aranılmayacağını belirlemeye yetkilidir. Böylece, Maliye Bakanlığı hangi tutarın altında veya üstünde bulunan kamu alacaklarının bu kapsamda olduğunu belirleyebileceği gibi, kamu alacaklarından hangilerinin bu kapsamda bulunduğunu tespiti de yetkili kılınmıştır.

Ayrıca, 213 sayılı Kanun'un mükerrer 257. maddesi hükmüne uyulmaması halinde aynı Kanun'un mükerrer 355. maddesi uyarınca özel usulsüzlük cezası kesileceği kabul edilmiştir.

Anayasa'nın 2. maddesinde belirtilen hukuk devleti, eylem ve işlemleri hukuka uygun, insan haklarına saygılı, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adaletli bir hukuk düzeni kurup bunu geliştirerek sürdüren, Anayasa'ya aykırı durum ve tutumlardan kaçınan, Anayasa ve hukukun üstün kurallarıyla kendini bağlı sayan, yargı denetimine açık olan devlettir.

Anayasa'nın 48. maddesinin birinci fıkrasında "Herkes, dilediği alanda çalışma ve sözleşme hürriyetlerine sahiptir. Özel teşebbüsler kurmak serbesttir." denilmiştir. Birey bu özgürlüğünü kullanarak çalışmak için dilediği alanı ve işi seçebilir, gerekli sözleşme ve işlemleri yapabilir. Devlet de, bireylerin bu özgürlüğünü kullanabilmesi için gerekli düzenlemeleri yapmalı ve tedbirleri almalıdır.

Anayasa'nın 13. maddesinde, temel hak ve özgürlüklerin, özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği, bu sınırlamaların Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacağı belirtilmiştir. Bu nedenle, temel hak ve özgürlükler, istisnâ olarak ve özüne dokunulmadan demokratik toplum düzeninin gerekleri için zorunlu olduğu ölçüde ve ancak kanunla sınırlandırılabilirler.

Demokratik bir toplumda temel hak ve özgürlüklere getirilen sınırlamanın, bu sınırlamayla güdülen amacın gerektirdiğinden fazla olması düşünülemez. Demokratik hukuk devletinde güdülen amaç ne olursa olsun, kısıtlamaların, bu rejimlere özgü olmayan yöntemlerle yapılmaması ve belli bir özgürlüğün kullanılmasını önemli ölçüde zorlaştıracak ya da ortadan kaldıracak düzeye vardiirilmaması gerekir.

İptali istenen kuralla Maliye Bakanlığına, vergi güvenliğini ve tahsilatını sağlamak amacıyla niteliklerini belirleyip onayladığı elektrikli, elektronik, manyetik ve benzeri cihazlar ve sistemleri kullandırma, bu cihaz ve sistemler vasıtasıyla bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretlerin kullanılmasına ilişkin zorunluluk getirme yetkisi verilmektedir. Mükelleflerin mali güçlerinin saptanması ve vergi yükünün adaletli ve dengeli dağılımını sağlamak için kamu yararı amacıyla kanun koyucu gerektiğinde Maliye Bakanlığına da yetki verebilir, bu konuda anayasal sınırlar içinde takdir yetkisini haizdir.

İptali istenilen kuralda ise, genel ve soyut olarak mükelleflere vergi dairelerine olan borçlarının bulunması halinde bandrol, pul, barkod, hologram, kupür, damga, sembol gibi özel işaretlerin verilmesi yasaklanmaktadır. Bu yasaklama ise mükelleflerin söz konusu özel işaretlerin verilmemesi sonucu ticaret yapmalarını engelleyici niteliktedir. Anayasa'nın 48. maddesinde, çalışma ve sözleşme hürriyetleri için herhangi bir sınırlama nedeni öngörülmemiştir. Maddede sınırlama nedenlerinin gösterilmemesi, kanun koyucunun çalışma özgürlüğünü sınırlandıracak düzenlemeler yapamayacağını göstermektedir. Dava konusu kuralda öngörülen yasaklama, çalışma özgürlüğünün güvence alanının kanun koyucu tarafından daraltılması niteliğinde olduğundan Anayasa'nın 13. maddesi anlamında ölçsüz bir sınırlandırma niteliğindedir. Bu yasaklama ticaret yapmak isteyen kişilerin kamuya olan borçlarını ödemedi, sözkonusu bandrol, pul, barkod vd. bağlı olan ticari faaliyetlerini yapmalarını yasaklamaktadır. Söz konusu sınırlamanın, Anayasa'nın 73. maddesi uyarınca ödev olarak belirlenen vergi borcu ile diğer kamu borçlarının ödenmesini sağlamak için meşru bir amaca yönelik olduğu söylenebilir. Ancak, kamu hizmetlerinin yürütülmesinde gerekli kaynağın elde edilmesi için vergi ve diğer kamu alacaklarının takip ve tahsiline yönelik özel hukuki düzenlemeler, kolaylık ve hızlilik sağlanmasının doğal olduğu kabul edilmekle birlikte, bu konuda bireylerin hakları ve hukukun genel ilkelerinin de göz önünde bulundurulması hukuk devletinin bir gereğidir.

6183 sayılı Amme Alacaklarının Tahsil Usulü Hakkında Kanun hükümleri ve yine diğer kanunlarla getirilen, vergi cezaları ve gecikme faiz ve zammı uygulamaları göz önüne alındığında, mükelleflerin vergi borcunun ödenmesi ve kamu alacaklarının tahsili konusunda yasal düzenlemelerin bulunduğu, ayrıca bu alacakların niteliğine bağlı olarak, takip konusunda normal bir alacağa nazaran önemli bir takım ayrıcalıklar da tanındığı görülmektedir.

İptali istenilen kuralda, Anayasa'nın 73. maddesinde vatandaşlık ödevi olarak belirlenen vergi yanında, kamu alacakları da yer almaktadır. Dava konusu kuralın, vergi borcu da dâhil, borcu olmadığına ilişkin belge getiremeyen mükelleflere Maliye Bakanlığının zorunlu tuttuğu bandrol, pul,

barkod, hologram, kupür, damga, sembol gibi özel etiket ve işaretlerin verilmemesi sonucunu doğurduğu, bu durumun ise kişilerin çalışma özgürlüğünü zedeleyen bir etkisinin bulunduğu açıktır.

Çalışma ve sözleşme özgürlüğüne getirilen sınırlamada, sınırlamanın amacı, vergi borcunun tahsilinin sağlanması, araç ise çalışma ve sözleşme yapma özgürlüğünün yahut daha somut haliyle ticaret yapmanın belirli konularda yasaklanmasıdır. Amaç ile araç arasında makul bir ilişkinin bulunduğu söylenmesi için ticaretin engellenmesi ile vergi alacağının tahsilinin zorluğu veya imkânsızlığı arasında makul bir tercih nedeninin bulunması gereği açıktır. Yasak, hiçbir şart öngörmeksizin, hatta vergi borcunun tutarı dahi belirtilmeden, vergi borcunun ödenmemesine bağlı olarak kendiliğinden uygulandığı zaman amaç ile araç arasındaki makul ilişki ve denge ortadan kalkar.

İptali istenilen kuralla, kamu alacaklarının tahsilinin sağlanmasının amaçlandığı bu yönüyle kamu yararını amaçladığı görülmektedir. Ancak, dava konusu kural olmasa dahi yukarıda belirtildiği üzere, 6183 sayılı Kanunla kamu alacaklarının tahsili için özel hükümler ve kolaylıklar zaten kabul edilmiştir. Ayrıca, ticaretini yapıp kazanç elde edemeyen kimselerin vergi borcunu ödemesi de kolay değildir. Bu açıdan, iptali istenen hükümlerin dolaylı olarak, kamu alacağının daha kolay tahsiline de bu açıdan engel olduğu da söylenebilir.

İptali istenen hüküm, vatandaşlık ödevi kapsamında bulunan vergi borcu ve bu kapsamda bulunmayan kamu alacakları yönünden ölçülü bir sınırlama olmadığı gibi, bu alacakların tahsili amacıyla mükelleflere kuralda belirtilen özel işaretlerin verilmemesinin Anayasa'nın 48. maddesinde güvence altına alınan çalışma ve sözleşme özgürlüğü alanına yapılmış bir sınırlama olduğu, bu sınırlamanın Anayasa'nın 13. maddesi kapsamında demokratik bir toplum düzeni için gerekli olmadığı, bir an için gerekli olduğu kabul edilse bile ölçülülük ilkesine uygun olmadığı açıktır.

Nitekim benzer şekilde, 5682 sayılı Pasaport Kanunu'nun, 28.5.1988 günlü, 3463 sayılı Yasa ile değiştirilen 22. maddesinin birinci fıkrasındaki, vergiden borçlu olduğu pasaport vermeye yetkili makamlara bildirilenlere pasaport veya seyahat vesikası verilmeyeceğine ilişkin kısmın iptali istenmiş; Anayasa Mahkemesinin 18.10.2007 tarihli, 2007/4 Esas, 2007/81 Karar sayılı kararıyla kuralın Anayasa'nın 2., 13. ve 23. maddelerine aykırı olduğu gerekçesiyle iptaline karar verilmiştir.

Açıklanan nedenlerle, 213 sayılı Kanun'un mükerrer 257. maddesinin birinci fıkrasının (6) numaralı bendinin iptali istenilen ".mükelleflerin Maliye Bakanlığına bağlı vergi dairelerine vadesi geçmiş borcu bulunmadığına ilişkin belge arama zorunluluğu getirmeye, bu zorunluluk kapsamına girecek amme alacaklarını tür ve tutar itibarıyla tespit etmeye ve hangi hâllerde bu zorunluluğun

aranılmayacağına."şeklindeki kısımlarının, Anayasa'nın 2., 13. ve 48. maddelerine aykırı olduğu ve iptali gerektiği kanaatinde olduğumuzdan Çoğunluğun görüşüne katılmamız mümkün olmamıştır.

Üye - Alparslan ALTAN

Üye - Erdal TERCAN

KARŞIOY GEREKÇESİ

1. 6.2.2014 tarihli ve 6518 sayılı Kanun'un 87. maddesiyle 5651 sayılı Kanun'un 4. maddesine eklenen (3) numaralı fıkrası ve Kanun'un 88. maddesiyle 5651 Sayılı Kanun'a eklenen 5. maddenin (5) numaralı fıkrası ve Kanun'un 89. maddesi ile 5651 sayılı Kanun'un 6. maddesinin (1) mumaralı fıkrasına eklenen (d) bendi Mahkememiz çoğunluğunca iptal edilmiştir.

2. İptal edilen kurallar internet platformunda içerik, yer ve erişim sağlayıcı olarak faaliyet gösterenlere getirilen yükümlülüklerle ilişkin bulunduğundan iptali istenilen kuralların anlam ve kapsamının belirlenmesi bakımından öncelikle internetin anlam ve kapsamının irdelenmesi gerekmektedir.

3. İnternet 1969 yılında bir askeri proje olarak ortaya çıkmış, 1983 yılında sivil kullanıma açılmış ve 1990'lardan itibaren de küresel bir ağ haline gelmiştir.

4. Bilinen geleneksel iletişim türlerinden farklı olarak, iletişime çok büyük bir hız kazandırmış, farklı kesimlerce üretilen etkileşimli multimedya içeriklerinin, dünyanın herhangi bir yerinden sayısız başka yerlerine saniyeler içerisinde ulaşılabilmesini sağlamıştır. Bilginin çok daha hızlı ve ucuz bir şekilde yayılmasına olanak sağladığı için de, toplumların geleneksel, ekonomik, siyasal kültürel yapılarını etkilemiş, böylece köklü değişim ve dönüşümlerin önünü açmış, yönetimden siyasete, ekonomiden hukuka, aileden arkadaşlık ilişkilerine, insanların tutum, davranış ve alışkanlıklarında önemli değişmelere sebep olmuştur. Bu değişim ve dönüşümler de işin doğası gereği yeni yönetsel ve hukuksal sorunları ortaya çıkarmıştır.

5. İnternet uygulamasında "ulusal sınır" gerçeğinin olmaması nedeniyle, dünyanın herhangi bir yerinde herhangi biri tarafından üretilen içerikler serbestçe yayına konulup dünya genelinde milyonlarca kişiye ulaşabilmektedir. Buradaki "ulusal sınır"sızlık ile internetin teknik alt yapısı ve yayılmış ağ yapısı ve paylaşım ve erişim kolaylığı da, internete bağlanabilen her kişinin, istemesi halinde yasa dışı içerik oluşturup, bu içerikleri çok hızlı bir şekilde dünyanın dört bir yanına yaymasına, gerçek kimliğini gizleyebilmesine olanak sağlamaktadır. Ayrıca, internet platformu

herhangi bir doğrulama mekanizması barındırmadığından, iletişim, bilgi edinme, paylaşım ve eğlence gibi iyi ve zararsız amaçlarla kullanılmasının yanında, sahte isim ve hesaplarla yasa dışı içerik oluşturup paylaşılma amacıyla da kullanılabilir. Bu da suç ve suçlulara kendilerini kolayca gizleyerek yasa dışı iş ve eylemleri hayata geçirebilmelerine fırsat vermektedir. Yani, bir kısım terör ve suç örgütleri bir kısım faaliyetlerini internet ortamına taşıyabilmekte, siber saldırılar yanında ülkelerin milli güvenlik ve kamu düzenlerini yok etmeyi hedef alan içeriklerini çok kısa zamanda çok geniş kitlelere ulaştırabilmektedirler. Ayrıca başka bir kısım içeriklerle de mahremiyet ihlallerine, bilgi hırsızlığına, telif hakları ihlallerine, özel hayatın gizliliğinin ortadan kaldırılmasına, dolandırıcılığa, kişilik haklarına saldırılara, bahis, kumar, fuhuş, çocukların cinsel istismarı, pornografi, intihar ve uyuşturucuya yönlendirme, siber zorbalık, şiddet, ırkçılık, ayrımcılık ve nefret söylemi gibi yasalara aykırı veya zararlı kabul edilen bir takım durumların geniş kitlelerin önüne getirilmesine, onların etkilenimlerine, böylece de sosyal dokunun zedelenmesine, ahlaki yapının bozulmasına ve hukuksal sorunların çıkmasına neden olabilmektedir.

6. Belirtildiği üzere internetin diğer kitle iletişim araçlarından farklı olan ve yukarıda sözü edilen doğası ve özellikleri, çok boyutlu, çok aktörlü dinamik ve dağıtık yapısı, tekniği, işleyiş biçimi, alt yapısı ve "ulusal sınır"sızlık/uluslararası niteliği, suç yeri ve zamanı ve suçlu yönünden kendine has özellikler sergilemekte, bu da internet platformunun düzenlenmesini ve bu alana ilişkin bazı sınırlamalar getirilmesini zorunlu kılmaktadır. Bu zorunluluk, internetin kendine özgü yapısından ve teknik özelliklerinden kaynaklanan bir zorunluluk olmasına rağmen, ifade özgürlüğü ve bilgiye erişim özgürlüğü bağlamında, bilgi ve düşüncenin serbest dolaşımına engel olacağı kanaatiyle, internetin düzenlenmesinde erişimin engellenmesi gibi bir takım yaptırımlar uygulanması ciddi eleştirilerle karşılaşmıştır.

7. Getirilen tüm eleştirilere karşın, toplumun, özellikle de çocukların korunmasının, bilgi güvenliğinin sağlanmasının, suç oluşumunun önlenmesinin, suç oluştuktan sonraki süreçte yapılacak araştırma ve incelemelere olanak sağlanmasının, suçlu ve sorumluların ortaya çıkmasının vazgeçilemez bir zorunluluk olması nedeniyle, gerçek hayatta kurulan sistemin internet ortamında (sanal ortamda) da kurulması gerektiği söylenmektedir.

8. Mukayeseli hukuk açısından başka ülkelere bakıldığında da, toplumun tümünün ve özellikle de çocuklar ile gençlerin ve ailelerin bu alandaki risk ve tehlikelere karşı korunması amacıyla internetin güvenli kullanımının sağlanmasına yönelik tedbirler alındığı, internetle ilgili strateji ve politikalar geliştirildiği, farklı biçimlerde de olsa giderek artan bir oranda internetle ilgili müdahaleler içeren uygulamalara gidildiğinin görüldüğü belirtilmektedir[1].

9. Öte yandan ülkeler bazında içerik düzenlemesi için farklı yaklaşımlar sergileniyor olsa da, hem yöntem hem de düzenlemeye konu içeriklerin türleri konusunda bir uzlaşma sağlandığı, bu kapsamda, içerik düzenlemelerinde uyar - kaldır (notice and takedown -NTD) yönteminin benimsendiği ve internetin güvenli kullanımı konusunda bilinçlendirme çalışmalarının yapılmasının, telif hakkı ihlalleri, çocukların cinsel istismarı, ırkçılık, ayrımcılık, nefret ve şiddet uyandıran içerikler ile ekstrem pornografi içerikleri konusunda her bir ülkenin kendisinin düzenlemeler yapabileceğinin, sektöre ilişkin uluslararası arenada genel bir kabul gördüğü ifade edilmektedir.

10. Bununla birlikte, hızlı gelişen teknoloji ile birlikte, içeriğin düzenlenmesinde kullanılan yöntemleri aşmaya yönelik alternatif yöntemlerin de sürekli olarak geliştiği de ifade edilmekte, bunun da internetin düzenlenmesi hususunu daha da karmaşık hale getirdiği, bu sebeple, ihtiyaçlara tam olarak cevap veren bir yasal mevzuatın var olmasının yanında, içeriğin düzenlenmesinde etkin bir şekilde kullanılacak farklı yöntemlere sahip olmanın ve dinamik bir idari yapı oluşturmanın gerekliliği vurgulanmaktadır.

11. Bir taraftan belirtilen bu durumlar söz konusu iken, diğer taraftan internetin doğası ("ulusal sınırsızlık" özelliği) gereğince ulus devletler için internetin denetim ve kontrolünde başka bir takım zorlukların da bulunduğu, bu zorlukların en önemlilerinden birisinin internetin, devletin klasik ulusal egemenlik anlayışına meydan okuyan karmaşık, dağıtık, çok değişkenli, dinamik ve sınır tanımayan küresel yapısı olduğu, devletlerin ülke sınırları içerisinde hukuk kuralı koyma ve bunu uygulama meşruiyetlerini esas alan klasik ulusal egemenlik yaklaşımlarına dayalı mevzuatın, ulusal sınır tanımayan bu teknoloji karşısında çoğu zaman sıkıntılar yaşar hale geldiği belirtilmektedir.

12. Diğer yandan da, konunun bilimsel otoritelerine göre yaygınlaşan ve etkinleşen internetin sosyal, siyasal ve ekonomik hayatı yönlendiren etkili bir araç olduğunun iyice ortaya çıkmasıyla birlikte[2] devletler, internet üzerindeki etkilerini ve etkinliklerini hem ulusal, hem de uluslararası düzeyde arttırmaya gayretine girmişler; internetteki (e-) ticaretin milyarlarca dolarlık hacme ulaşması, alan adlarının değerlendirilmesi, çeşitli telif hakkı ihlallerine yol açılması, internet üzerinden veri iletişiminin ulusal güvenliğin bir parçası olarak görülmesi ve zararlı içeriğin denetlenmesi gibi nedenlerle alan adları ve IP adreslerinin yönetimi (internet üzerinde söz sahibi olma, alan adları ile IP numaralandırma politikalarını belirleme ve kontrol etme) sadece devletlerle özel sektör arasında değil, devletler arasında da bir menfaat ve bir anlamda da ideolojik bir sorun alanı haline gelmiş bulunmaktadır. Yine aynı otoritelere göre, siber uzayın mimarisi bu teknolojileri geliştiren ve üreten devletlerin politikaları doğrultusunda şekillenmekte, dolayısıyla bu alanın sınırları ve kuralları

büyük oranda, bu alanda teknoloji üreten ülkelerin özel ve kamusal güçleri tarafından belirlenmektedir.

13. Durum böyle olmakla birlikte, internet trafiğinin, farklı ülkeleri saniyeler içerisinde geçerek akması, böylesine karmaşık bir yapı içerisinde belli bir noktadaki bir sorunun, dünyanın uzak başka bir noktasındaki internet trafiğini olumsuz yönde etkileyebilmesi, web sitelerini barındıran sunucuların dünyanın her tarafına yayılmış durumda olması, genel veya bölgesel internet noktalarının kontrol ve bakımına ihtiyaç duyması, hat sayılarının artırılması ve böylece internetin işlerliğinin devamının sağlanması amacıyla tüm devletlerin aktif katılımının, uluslararası iş birliğinin ve koordinasyonun sağlanması gerektiğine işaret edilmektedir.

14. Ayrıca, internet ortamının fiziki bir coğrafya ile sınırlı olmaması durumuna bağlı olarak, internet üzerinden işlenen suçlarla mücadelenin, gerçek sorumlu veya suçlularını bulup cezalandırmanın ulusal mevzuata göre gerçekleştirilmesinin her zaman mümkün olmaması nedeniyle, sözkonusu sanal ortamın zararlı etkilerinden korunmak ve "serbest suç işleme bölgeleri"nin oluşumunu engellemek amacıyla da uluslararası iş birliğinin ve her ülke için geçerli olacak yeknesak ortak kurallar oluşturmanın zorunlu olduğu belirtilmektedir.

15. İptal edilen kuralların anlam ve kapsamına ve kurallara ilişkin anayasal değerlendirmeye gelince:

16. Kanun'un 4. maddesinin (3) numaralı fıkrasında içerik sağlayıcılar, Telekomünikasyon İletişim Başkanlığının (TİB) bu kanun ve diğer kanunlarla kendisine verilen görevlerin ifası kapsamında talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla yükümlü tutulurken, 5. maddesinin (5) numaralı fıkrası ile 6. maddesinin (1) numaralı fıkrasının (d) bendinde yer ve erişim sağlayıcılar TİB'in talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlık tarafından bildirilen tedbirleri almakla yükümlü tutulmuşlardır.

17. Öncelikle belirtmek gerekir ki, her ne kadar 4. maddenin (3) numaralı fıkrasında yer alan "Başkanlığın bu Kanun ve diğer kanunlarla verilen görevlerinin ifası kapsamında" ibaresi, 5. maddenin (5) numaralı fıkrası ile 6. maddenin (1) numaralı fıkrasının (d) bendinde yer almamış ise de, konunun doğası gereğince, bu ibarenin 5 ve 6. maddelerin iptal edilen kuralları içinde geçerli olduğunun kabulü gerekmektedir.

18. Öte yandan, iptal edilen düzenlemelerde TİB tarafından talep edilecek bilginin niteliği belirtilmemiş ise de, ilgili mevzuat bir bütün olarak incelenip değerlendirildiğinde, iptal edilen kurallar uyarınca, içerik, yer ve erişim sağlayıcılar tarafından TİB'e verilmesi öngörülen bilgilerin

kişisel veri kapsamında olduğu ve bu bilgilerin en basit şekliyle bir yerden başka bir yere aktarılması sağlandığından da kişisel verilere bir müdahalenin söz konusu olduğu anlaşılmaktadır.

19. Kurallar, Mahkememiz çoğunluğunca, özetle, Anayasa'da yer alan güvenceye rağmen, kişilere ait her türlü kişisel veri, bilgi ve belgelerin, konu, amaç ve kapsam sınırlaması olmaksızın koşulsuz olarak TİB'e verilmesine imkân tanıdığı, böylece kişilerin idareye karşı korumasız hale getirildiği, dolayısıyla da kişilerin özel ve aile hayatının gizliliğini ölçüsüzce sınırlandırdığı, TİB'e, çerçevesi çizilmemiş, esasları belirlenmemiş bir alanda hiçbir sınırlamaya bağlı olmaksızın geniş yetkiler tanıdığı, bunun da yasama yetkisinin devri niteliği taşıdığı gerekçesiyle iptal edilmiş bulunmaktadır.

20. Çoğunluk görüşüne dayalı iptal kararında Anayasa'nın 13 ve 20. maddelerinin anlam ve kapsamına, özel hayatın gizliliği ve korunması özgürlüğünün kullanılmasına ve temel hak ve özgürlüklere getirilebilecek olan sınırlamalara ilişkin genel açıklamalara tarafımızca da aynen katılmaktadır.

21. Çoğunluk görüşünden ayrıldığımız husus, iptal edilen kuralların anlam ve kapsamı ile kurallarla TİB'e müdahale imkanı verilen kişisel verilerin niteliği ve internetin anlam ve kapsamı dikkate alındığında bu verilere yapılan müdahalenin ölçülü olup olmadığı noktasındadır.

22. İptal edilen düzenlemelerde TİB tarafından talep edilecek bilginin niteliği belirtilmemiş olsa da, ilgili mevzuat bir bütün olarak değerlendirildiğinde, söz konusu kurallar uyarınca TİB'in içerik, yer ve erişim sağlayıcılardan, kendiliğinden, genel, sürekli, düzenli ve periyodik olarak bilgi talep etmeyeceği, yalnızca ya yasal görevlerinin ifası kapsamında kendiliğinden, yahut tekil olay ve konularla ilgili olarak başka kurumların talebi üzerine bu yola başvuracağı ve bu kapsamda içerik, yer ve erişim sağlayıcılardan;

- 5651 sayılı Kanununun 8. maddesinin altıncı fıkrası ile 8/A maddesinin dördüncü fıkrasının TİB'e yüklediği, suça konu internet içeriklerini oluşturan ve yayanlar hakkında, Cumhuriyet Başsavcılığına suç duyurusunda bulunma görevinin ifası için, ilgili içerik, yer ve erişim sağlayıcılardan, suç duyurusunda kullanılmak üzere Cumhuriyet Başsavcılıklarına gerekli olan (IP adresi, kullanıcı ve iletişim bilgisi, hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı gibi) bilgileri,

- Suçu ve suçluyu tespite yönelik olarak Cumhuriyet Savcılıklarından gelen taleplerin karşılanmasına ilişkin bilgileri,

isteyebileceği,

- Yasadışı içeriklerin kullanımdan kaldırılmasını teminen, içerik sağlayıcılara uyar-kaldır yöntemiyle bildirimlerde bulunabileceği,
 - Kullanımdaki internet hizmetinin daha güvenli ve kaliteli olması bakımından, içerik, yer ve erişim sağlayıcılarca alınması gereken önlemlerin belirlenmesi bağlamında bildirimlerde bulunabileceği,
 - Siber saldırıların tespiti ve önlenmesi bağlamında içerik, yer ve erişim sağlayıcılardan bazı tedbirleri almalarını isteyebileceği,
- sonucuna varılmaktadır.

23. Ayrıca, internet trafik bilgilerinin ilgili mevzuat uyarınca ancak mahkeme kararı ile alınabildiği, bu tür trafik bilgilerinin TİB'e uğramaksızın, işletmeciden alınıp doğrudan ilgili mahkemeye gönderildiği, TİB'in bu konuda, mahkemeden gelen talepleri işletmeciye iletme, işletmeciden gelen bilgiyi de doğrudan mahkemeye iletme dışında bir işlev ifa etmediği gözetildiğinde de, iptal edilen kurallar kapsamında istenebilecek bilgilerin trafik bilgisi niteliğinde bilgiler olmadığı da anlaşılmaktadır.

24. Bu bakımdan, TİB'in temin ettiği bilgilerin, ancak 5651 sayılı Kanun'un 10. maddesinde belirlenen görevler kapsamında ve diğer yasaların belirlediği yetkiler çerçevesinde ilgili mercilerle koordinasyon kapsamında verilebileceği, bunların gelişigüzel başka kurum ve kişilerle paylaşılmasının veya başka amaçlarla depolanıp kullanılmasının yasal olarak mümkün olmadığı, aksi durumun ilgililerin sorumluluklarını doğuracağına duraksama bulunmamaktadır.

25. 5651 sayılı Kanun'un iptal edilen hükümleri ile 5271 sayılı Ceza Muhakemeleri Kanunu'nun ilgili düzenlemelerini birlikte gözetildiğinde, TİB'in kanunu icra noktasında içerik, yer ve erişim sağlayıcılardan isteyeceği bilginin kapsamının ve getirebileceği yükümlülüklerin çerçevesinin belirlenmediği, bilgi talep etme yetkisinin kapsamının kişisel verilerin korunmasına ilişkin gerekli teminatlar sağlanarak sınırlandırılmadığı ve kişilere neler olduğu belirlenemeyen yükümlülükler yüklediği de söylenemez.

26. Ayrıca yine yukarıda ayrıntılı bir biçimde açıklandığı üzere, internet platformu, olumlu ya da olumsuz her türlü bilgi ya da bilgi niteliği taşımayan içeriğin, zararlı ve suç niteliğindeki uygulamaların yer aldığı, internet kullanan hemen herkesin kişisel verilerinin, bilinen ya da bilinmeyen bir çok yerde kaydedildiği ve istenildiğinde ilgili internet aktörlerince çeşitli amaçlarla kullanılabilirdiği çok geniş bir alandan oluşmaktadır ve bu platform, fiziksel ortamdaki suçların izlerini ülkesel sınırları tanımadan çok süratli bir şekilde sanal ortamda dolaştırmaktadır. Böyle bir dünyada

suç ve suçlularla mücadele, ahlakın ve sağlığın korunması, özellikle çocuk haklarının korunması büyük bir önem arz etmektedir.

27. Durum böyle olunca da, kamu düzenini sağlama, suç ve suçlularla mücadele etme, toplumun huzur ve refahı, temel hak ve özgürlükleri koruma görevleri bulunan ve Anayasa'da belirlenen ilkeler ve meşru amaçlar çerçevesinde temel hak ve özgürlükleri sınırlayıcı uygulamaları her türlü denetime açık olan devletin, sanal ortamdaki suçlarla mücadele etme sürecinde görevlendirdiği kurumuna "internet yayınlarının düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi amacıyla koordinasyon, önleme, yayın engelleme, internet yayın kalitesini denetleme, filtreleme ve bloke etme sistemlerini geliştirme, izleme, siber saldırılara karşı önlem alma" gibi yetkiler verirken, ilgili işletmelerden bilgi alma ve tedbir talep etme yetkisinin çok sınırlı bir şekilde verilmesi gerektiğini söylemek tutarlı bir uygulama olarak değerlendirilememektedir.

28. Kaldı ki internetin anlam ve kapsamına ilişkin olarak yukarıda yapılan anlatımlara göre, kişisel veriler internet platformuna girdiği andan itibaren, kişilerin münhasır özel alanından çıkmaktadır. Söz konusu veriler, internet kullanımında kendisinden yararlanan yer sağlayıcı, içerik sağlayıcı, erişim sağlayıcı, yönlendirici (router), internet değişim noktası (internet exchange point), veri merkezleri gibi bir dizi ortakla paylaşılmaktadır. Bu kapsamda "gizlilik kuralları" paydaşlar arasında onaylanmakta, fakat internet hizmetinden yararlanmak isteyen kişinin gizlilik anlaşmasını onaylama iradesinin özgürlüğü sorgulanmamaktadır. Bu açıdan değerlendirildiğinde sanal ortamdaki kişisel bilgilerin ve verilerin devletin bir kurumunda toplanması ile özel hayata ölçüsüzce müdahalede bulunduğu kabul edilmesi, sanal dünyanın gerçekliği ile bağdaşmamaktadır.

29. Bu itibarla, iptal edilen kurallarla yapılan müdahalenin, hem kişilerin kendi yararları açısından, hem de toplum ve ailenin korunması bakımından gerekli ve ölçülü olduğu, düzenlemelerde Anayasa'nın 7., 13. ve 20. maddelerine aykırı bir yön bulunmadığı sonucuna varılmaktadır.

30. Açıklanan nedenlerle iptale ilişkin çoğunluk görüşüne katılmıyoruz.

Üye: Hicabi DURSUN; Muammer TOPAL; Kadir ÖZKAYA; Rıdvan GÜLEÇ

KARŞIOY GEREKÇESİ

1. Davada, 6.2.2014 tarihli ve 6518 sayılı Kanun'un 93. maddesiyle değiştirilen 5651 sayılı Kanun'un 9. maddesinin "Bu madde kapsamında hâkimin verdiği erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının veya aynı mahiyetteki yayınların başka internet adreslerinde de yayınlanması durumunda ilgili kişi tarafından Birliğe müracaat edilmesi hâlinde mevcut karar bu

adresler için de uygulanır." hükmünü içeren (9) numaralı fıkrasının iptali istenilmiş, Mahkememiz çoğunluğunca ".veya aynı mahiyetteki yayınların." ibaresi Anayasa'nın 2., 13. ve 26. maddelerine aykırı bulunarak iptal edilmiş, fıkranın kalan bölümüne ilişkin iptal istemi ise oybirliği ile reddedilmiştir.

2. ".veya aynı mahiyetteki yayınların." ibaresinin iptaline ilişkin kararda, kuralın, hâkimin 9. madde kapsamında verdiği erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin "aynı mahiyetteki yayınların" başka internet adreslerinde yayımlanması ve ilgili kişinin de Birliğe başvurması durumunda, bunun tespitini Birliğe bıraktığı, aynı mahiyetin tespitinin, yayının aynı olmasından farklı olduğu, "Aynı mahiyetteki yayınlar"ın, hâkimin vermiş olduğu erişimin engellenmesine kararına konu kişilik hakkının ihlaline ilişkin yayın ile aynı olmayan ancak yöneldiği sonuç bakımından ilgilinin kişilik hakkını ihlal eder mahiyette olan yayınlar olduğu, kişilik hakkının kapsamının ve hangi eylemlerin kişilik hakkını ihlal ettiğinin, ilgili tarafların toplumsal, ekonomik, siyasal ve hukuki konuları, söz konusu yayının ulaştığı kitle ve bu yayının ifade özgürlüğü kapsamında bulunup bulunmadığı gibi birçok hukuki konunun değerlendirilmesini ve buna göre karar verilmesini gerektirdiği, kuralla verilen yetkinin, kanunilik ilkesinin asgari şartı olan kanunun anlaşılır, açık ve net olması zorunluluğunu karşılamadığı, bu itibarla da kuralın, "aynı mahiyetteki yayınlar" yönünden belirli ve öngörülebilir nitelikte olmadığı; ayrıca, Birlik tarafından, kişilik hakkının ihlaline ilişkin aynı mahiyetteki yayınların başka internet sitesinde yayımlanması halinde bu siteler hakkında da erişimin engellenmesi kararının uygulanmasının, bu sitelerden yararlanmayı engellemesi nedeniyle ifade özgürlüğünü de ölçüsüzce sınırlandırdığı gerekçesine dayanılmıştır.

3. Öncelikle belirtmek gerekir ki kuralda sözü edilen birlik, özel hukuk tüzel kişisi olarak Kanun'un 8. maddesi kapsamı dışındaki erişimin engellenmesi kararlarının uygulanmasını sağlamak üzere, Kanun'un 6/A maddesi ile kurulmuş Erişim Sağlayıcıları Birliği'dir. Birliğin asıl görevi, Kanun'un 8. maddesi kapsamında olan katalog suçlara ilişkin koruma ve idari tedbir dışındaki erişimin engellenmesi kararlarının uygulanmasını sağlamaktır. Birlik, 5809 sayılı Elektronik Haberleşme Kanunu kapsamında yetkilendirilen tüm internet servis sağlayıcıları ile internet erişim hizmeti veren diğer işletmecilerin katılmasıyla oluşan ve bunlar arasındaki koordinasyonu sağlayan bir kuruluştur. Birliğe üye olmayan erişim sağlayıcıları faaliyette bulunamamaktadırlar.

4. Mahkememiz çoğunluğunca ".veya aynı mahiyetteki yayınların." ibaresinin iptaline karar verilen Kanun'un 9. maddesinin (9) numaralı fıkrasında, hâkimin verdiği erişimin engellenmesi kararının internet ortamında uygulanması düzenlenmiştir. Fıkarda, hâkimin söz konusu 9. madde kapsamında verdiği erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının veya aynı

mahiyetteki yayınların başka internet adreslerinde de yayınlanması durumunda ilgili kişi tarafından Birliğe müracaat edilmesi halinde mevcut kararın bu adresler için de uygulanacağı öngörülmektedir. Fıkranın ".veya aynı mahiyetteki yayınların." ibaresinin dışında kalan kısmında Mahkememiz çoğunluğunca da anayasal bir sorun görülmediğinden ve tarafımızca da aynı görüş paylaşıldığından bu kısma ilişkin olarak burada bir değerlendirme yapılmayacaktır.

5. Kuralla ilgili değerlendirmeye geçmeden önce, ilgisi nedeniyle öncelikle internetle ilgili kısa bir değerlendirme yapılması gerekmektedir. Buna göre, anlam ve kapsamı bir önceki (5651 sayılı Kanun'un 4. maddesinin, 3 ve 5. maddesinin (5) numaralı fıkrası ile 6. maddesinin (1) numaralı fıkrasının (d) bendine ilişkin) karşı oyumuzda ayrıntılı olarak anlatılan internetin, modern demokrasilerde, başta ifade özgürlüğü olmak üzere, temel hak ve özgürlüklerin kullanılması bakımından önemli bir değere sahip bulunduğu, medya içeriği oluşturmak, yayınlamak ve yorumlamak şeklinde bireysel katılıma imkân veren şeffaf ve karşılıklı iletişim kurulan bir platform şeklinde işleyen bir medya kanalı olduğunda, sağladığı sosyal medya zemininin, kişilerin bilgi ve düşüncelerini açıklama, paylaşma ve yaymaları için vazgeçilemez nitelikte olduğunda kuşku bulunmamaktadır. Bu nedenle de kanaatimizce teşvik edilmesi, geliştirilmesi gereken bir alandır. Ancak, aynı platformun kimi zaman kimilerince manipülasyon amaçlı ve iftira niteliğinde üretilen yanlış bilgi ve yalanların saniyeler içerisinde mekân engeline takılmadan dünyanın dört bir yanına yayılmasına olanak sağladığı, böylelikle de kimi kişiler hakkında telafisi imkansız zararların oluşmasına neden olabilecek şekilde kullanılabilirdiği de unutulmamalıdır.

6. ".veya aynı mahiyetteki yayınların." ibaresine gelince:

7. Farklı kişilerle ilgili hazırlanmış aynı mahiyetteki içeriklerle veya aynı kişiyle ilgili hazırlanmış farklı bir içerikle ilgili yeniden hâkim kararı alınmaksızın erişimin engellenmesi uygulamasının Erişim Sağlayıcıları Birliği'ne verilmesinin, Birliğe yargı yetkisi verme niteliğinde olacağında şüphe yoktur. Bu nedenle, kanaatimizce "aynı mahiyetteki yayınlar" ibaresinden, daha önce hâkim denetiminden ve hukuki değerlendirmesinden geçmiş bir içeriğin değişik versiyonlarının anlaşılması gerekmektedir.

8. İnternet dünyasının genişliği, kullanıcı yoğunluğu, kullanıcı profiline çeşitliliği, takip ve denetiminin zorluğu, fiziki ortamda saatler sürebilecek doğru bilgi ya da manipülasyon amaçlı ve iftira niteliğindeki yanlış bilgi ve yalan akışının internette saniyeler içerisinde mekân engeline takılmadan sağlanabildiği gerçeği ile bu gerçeklik ortamında suç ve suçlularla mücadelede sağlanılmak zorunda olunan başarı birlikte düşünüldüğünde, iptal istemine konu fıkrada belirtilen nitelikteki yayınlar hakkında da öncelikle yargısal sürecin işletilmesi gerektiğinin söylenilmesi,

yargısal denetimin sonuçlanmasına ilişkin süreyi göz ardı edilmemesi gereken bir durum olarak ortaya çıkarmaktadır. Zira, hızlı bir şekilde karar alınıp bu kararın uygulanmasını gerektiren kimi durumlarda sürecin işleyişinin yavaşlaması/yavaşlatılması, hukuka aykırı içerikten zarar gören kişilerin haklarının telafisi imkansız ve ağır bir biçimde zedelenmesine de yol açabilecektir.

9. Öte yandan daha önce yargı denetimine konu olmuş bir içerikle ilgili küçük değişiklikler yapılarak internetin farklı adreslerine servis edilen yayınların her biri hakkında hâkim kararı aranması, internet dünyasındaki suç ve suçlularla mücadeleyi oldukça zorlaştıracaktır. Birliğin, yargı denetimi sonrası erişimin engellenmesi kararına konu içerikle aynı olan yayınları tespit edip tedbir uygulaması kabul edilirken, kişi ve konu birliği aynı mahiyette olanları tespit edemeyeceğinin düşünülmesi izahı zor bir durum olarak ortaya çıkmaktadır. Kaldı ki iptale konu düzenleme olmasa bile, hâkim kararı ile erişimi engellenen yayınlara ilgili kişi ve konu birliği bulunmak şartıyla, Birlik tarafından diğer internet adresleri hakkında tedbir yetkisinin kabul edilmesi, usul ekonomisi, yargı kararlarının etkililiği ve verimliliği açısından bir zorunluluk olarak da görülebilir.

10. Ayrıca "aynı mahiyetteki yayınlar" hakkındaki erişimin engellenmesi kararının itiraz üzerine yargı denetimine tabi tutulmasına bir engel bulunmaması, Birlik tarafından verilen tedbir kararının koşullarının oluşmadığı kanaatine varılması veya ölçüsüz bulunması durumunda kaldırılabilceği dikkate alındığında, kuralla öngörülen tedbirin orantısız olmadığı da görülmektedir.

11. Kaldı ki, yargı kararlarının infazı aşamasında karşılaşılan tartışmalı durumlar ve açıklamaya muhtaç hususlarla ilgili yargı makamlarından görüş istenmesi her zaman mümkündür. Hatta infaz aşamasında ortaya çıkacak hak ihlallerinin tekrar yargıya götürülmesine de bir engel bulunmamaktadır. Hal böyle olunca kuralın belirsizliğinden de söz edilemez.

12. Açıklanan nedenlerle, 5651 sayılı Kanun'un 9. maddesinin (9) numaralı fıkrasında geçen "... veya aynı mahiyetteki yayınların ..." ibaresinin Anayasa'ya aykırı olmadığı gerekçesiyle anılan kuralların iptali yolundaki çoğunluk görüşüne katılmıyoruz.

Üye: Hicabi DURSUN; Kadir ÖZKAYA; Rıdvan GÜLEÇ

KARŞIOY GEREKÇESİ

6.2.2014 tarihli ve 6518 sayılı Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un bazı madde ve fıkralarının Anayasaya aykırı olduğu gerekçesiyle iptali istenmiştir. Bu kapsamda, sözkonusu Kanun'un 90. maddesiyle 5651 sayılı İnternet Ortamında

Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'a eklenen 6/A maddesinin de iptali istenmiş; maddenin yedinci fıkrasının ikinci cümlesi dışındaki iptal talebi oybirliği ile reddedilmiş, ancak ikinci cümlenin Anayasaya aykırı olduğu ve iptali gerektiği kanaatinde olduğumdan, Mahkememiz Çoğunluğunun görüşüne katılmam mümkün olmamıştır.

5651 sayılı Kanun'a eklenen 6/A maddesinin yedinci fıkrası şu şekildedir: "Bu Kanunun 8 inci maddesi kapsamı dışındaki erişimin engellenmesi kararları gereği için Birliğe gönderilir. Bu kapsamda Birliğe yapılan tebligat erişim sağlayıcılara yapılmış sayılır."

Maddenin gerekçesinde bu konuya ilişkin olarak ayrıca bir açıklık getirilmemiştir.

Fıkranın ilk cümlesi ile Kanun'un 8. maddesi dışındaki erişimin engellenmesi kararlarının yerine getirilmesini sağlamak için Erişim Sağlayıcıları Birliğine (ESB) gönderilmesi kabul edilmiştir. Belirtmek gerekir ki, erişimin engellenmesi kararlarının gereği esas itibarı ile erişim sağlayıcıları tarafından yerine getirilecektir. Ancak bu kararların gereğinin yerine getirilip getirilmediğini denetlemek için ESB'ne ayrıca gönderilmesi isabetli olmuştur. Fıkranın ikinci cümlesi ile de erişimin engellenmesine ilişkin kararların, mahkemelerce ya da ilgili kurumlarca ESB'ne tebliğ edilmesi halinde, bu tebligatın aynı zamanda erişim sağlayıcılara da yapılmış sayılması kabul edilmiştir. Bu durumda, erişimin engellenmesi kararını asıl olarak yerine getirecek olan erişim sağlayıcılara ayrı bir tebligat yapılması öngörülmemiştir.

Mahkememiz çoğunluğu, ikinci cümleyi de Anayasa'ya aykırı görmemiş ve iptal talebini reddetmiştir. Çoğunluk, ret gerekçesinde, erişimin engellenmesi kararlarının en kısa sürede yerine getirilmesinin gerekliliğini, bunu sağlamak için iptali istenilen kural ile ESB'ne yapılan tebligatın erişim sağlayıcılara yapılmış sayılacağına kabul edildiğini, getirilen sistem ile mahkemelerce ve idare tarafından verilen kararların ESB'ye elektronik ortamda doğrudan iletildiğini, ESB'nin de erişim sağlayıcılar ile kurmuş olduğu sistem üzerinden bu kararları aynı anda erişim sağlayıcıların bildirilen elektronik adreslerine iletildiğini, söz konusu tebligatın erişim sağlayıcılara ulaştığının da sistemden görüldüğünü, teknolojik alanda meydana gelen hızlı değişim ve erişim sağlayıcıların söz konusu tebligattan haberdar olmaları göz önüne alındığında, iptali istenilen düzenlemelerin kanun koyucunun takdir yetkisi kapsamında olduğunu belirtmiştir.

Tebliğat, tebligatı yapan makamca, muhataba, ilgili işlemi usulüne göre bildirmesi ve bu bildirme işleminin de belgelendirilmesidir. Tebligat kural olarak muhataba, bilinen en son adresinde yapılır (Teb.K.m.10). Ancak muhatap adresinde bulunmazsa, muhatapın adresi bulunamazsa vb. tebligatın mümkün olmadığı hallerde, tebligatın ne şekilde yapılacağı Tebligat Kanunu'nda ayrıca

düzenlenmiştir (bkz. m.16,21,31). Ancak bu hallerde dahi, tebliğ konusu işlem, muhatabın tasarruf alanına mümkün olduğunca sokulmaya çalışılmakta, muhatabın işlemi öğrenmesi için çaba sarfedilmektedir. Ayrıca, bu hallerde, yani tebligatın muhatabın kendisine değil de bir başkasına yahut başka yere yapılmasında bir zorunluluk bulunmaktadır.

İptali istenen cümleye bu açıdan bakıldığında, tebligat, muhataba yani erişimin engellenmesi kararının gereğini yerine getirmekle sorumlu erişim sağlayıcılara yapılmamakta, onun yerine ESB'ne yapılmaktadır. Bilindiği gibi, ESB özel hukuk tüzel kişisi olup, erişim sağlayıcılardan ayrı bir kişiliği vardır. ESB, erişim sağlayıcıların kanuni yahut iradi temsilcisi de değildir.

Mahkememiz çoğunluğu, kararların ESB'ne tebliğ edilmesinin yeterli olduğunu, erişim sağlayıcılara ayrıca tebligat yapılmamasının gerekçesini, kararların bir an önce yerine getirilmesinin gerekliliği ve ESB'nin oluşturulan sistemle kararı zaten hemen erişim sağlayıcılara da iletildiği ve bunun sistem üzerinden görülebildiği, şeklinde açıklamaktadır. Ancak, bu gerekçeler, tebligatın muhataba değil de ESB'ne yapılmasını haklı kılmaktan uzaktır.

Öncelikle böyle bir sistemin kabul edilmesinin gerekçesi olarak çoğunluk, fıkranın ilk cümlesinin iptali talebinin reddine ilişkin gerekçede "Erişim sağlayıcıların sayısının her gün artması, bunları takip etmenin ve adreslerine ulaşarak tebligat yapılmasının zorluğu hususları gözetildiğinde sistemin en iyi şekilde işlemesi için erişimin engellenmesi kararlarının gereği için ESB'ye gönderilmesi zorunlu bulunmaktadır" demektedir. Buna göre, demek ki, ESB erişimin engellenmesi kararlarını her zaman anında erişim sağlayıcılara ulaştıramamaktadır. Kaldı ki, erişim sağlayıcısı olabilmek için BTK'dan lisans almak zorunludur. Lisans verilirken, gerekli adres ve iletişim bilgileri de erişim sağlayıcı tarafından BTK'ya bildirilmektedir. Erişim sağlayıcının sertifika alırken bildirmek zorunda olduğu elektronik adresine çok rahat tebligat yapılabilir ve bu durum zaman kaybına da neden olmaz. Eğer ESB, belirtildiği şekilde kendisine tebliğ edilen kararı hemen erişim sağlayıcılara ulaştırıyorsa bu takdirde, tebligata ilişkin temel kuraldan yani tebligatın muhataba yapılması gerektiğine ilişkin kuraldan ayrılmanın anlamı yoktur; ESB'nin, kararı erişim sağlayıcılara ulaştırdığı tarihin, tebligat tarihi olarak kabul edilmesi mümkündür. ESB, oluşturulan sistem üzerinden erişim sağlayıcıların kararı öğrenip öğrenmediklerini de kontrol edebildiğinden, tebligat tarihini ispat etmek zor olmayacaktır. ESB, oluşturulan sistemle, kararı otomatik olarak hemen erişim sağlayıcılara gönderiyorsa, kararın gereğinin yerine getirilmesi için zaman kaybı da yaşanmamaktadır,

ESB, kararı oluşturulan sistemle hemen erişim sağlayıcılara ulaştırıyorsa, erişim sağlayıcılarının hak kaybı yaşamaması sözkonusu olmayabilir. Ancak ESB, kararı erişim sağlayıcılara hemen gönderemezse, göndermede gecikme yaşanır, erişim sağlayıcının adresinde sıkıntı varsa, bu takdirde, iptali istenen

hüküm etkisini gösterecek, erişim sağlayıcıya hiç tebligat yapılmasa yahut geç tebligat yapılsa dahi, ESB'ne yapılan tebligat kendisine yapılmış sayılacak ve tebligata bağlı olarak ortaya çıkabilecek sorumluluklar devreye girecektir. Bu bağlamda belirtmek gerekir ki, 5651 sayılı Kanun'un 9. maddesinin (8) numaralı fıkrası ve 9/A maddesinin (3) numaralı fıkrası uyarınca erişim sağlayıcılar, bu kararları dört saat içinde yerine getirmekle yükümlüdür; yerine getirmediğinde adli para cezası ile karşılaşmaktadır.

Anayasa'nın 2. maddesinde yer alan hukuk devletinin temel ilkelerinden biri "hukuk güvenliği" ilkesidir. Hukuk güvenliği, kuralların öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar.

Anayasa'nın hak arama özgürlüğünü düzenleyen 36. maddesinin birinci fıkrasında, "Herkes, meşru vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir" denilerek yargı mercilerine davacı ve davalı olarak başvurabilme ve bunun doğal sonucu olarak da iddia, savunma ve adil yargılanma hakkı güvence altına alınmıştır. Maddeyle korunan hak arama özgürlüğü, kendisi bir temel hak niteliği taşımasının ötesinde, Anayasa'nın 40. maddesi uyarınca diğer temel hak ve özgürlüklerden gereken şekilde yararlanılmasını ve bunların korunmasını sağlayan en etkili güvencelerden biridir. Kişinin uğradığı bir haksızlığa veya zarara karşı kendisini savunabilmesinin ya da maruz kaldığı haksız bir uygulama veya işleme karşı haklılığını ileri sürüp ispatlayabilmesinin, zararını giderebilmesinin etkili yolu, yargı mercileri önünde dava hakkını kullanabilmesidir.

Mahkemenin yahut tebligat yapacak makamın, tebligat konusu işlemi muhataba usulüne göre yapması gerekir. Usulüne uygun işlemlerin kendilerine bağlanan hukuki sonuçları doğurabilmesi için muhatabına bildirilmesi gerekir. Böylece tebligata bağlanan süre işlemesi, bazı yükümlülüklere katlanması vb. muhataptan beklenebilir hale gelsin. Usulüne uygun olarak yapılan tebligat, Anayasa'da güvence altına alınmış olan iddia ve savunma hakkının tam olarak kullanılabilmesinin ve bireylere tanınan hak arama özgürlüğünün en önemli güvencelerinden biridir. Muhatabın, tebligat konusu işlemde usulüne uygun olarak bilgilendirilmesi, hakkaniyete uygun yargılamanın da bir gereğidir.

İptali istenilen cümlede, Kanun'un 8. maddesi kapsamı dışındaki erişimin engellenmesi kararlarının, erişim sağlayıcılara ayrıca tebliğ edilmemesi, ESB'ne yapılacak tebligatın yeterli görülmesi yahut ESB'ne yapılan tebligatın erişim sağlayıcılara yapılmış sayılması şeklinde bir sistem öngörülmüştür. Buna göre, ESB'ne yapılan tebligat erişim sağlayıcılara da yapılmış sayıldığından, erişim

sağlayıcıların kararın gereğini yerine getirmek için kanunda öngörülen süre, ESB'ne yapılan tebligat tarihinden itibaren işlemeye başlayacaktır. Yukarıda belirtildiği üzere, 5651 sayılı Kanun'un 9. maddesinin (8) numaralı fıkrası ve 9/A maddesinin (3) numaralı fıkrası uyarınca erişim sağlayıcılar, bu kararları dört saat içinde yerine getirmekle yükümlüdür; yerine getirmedikleri takdirde 5651 sayılı Kanun'un 9. maddesinin (10) numaralı fıkrası uyarınca adli para cezası ile karşılaşmaktadırlar. Erişim sağlayıcıları, ESB'nin kusuruyla yahut teknik nedenlerle erişimi engelleme kararlarının kendilerine bildirilmemesi veya geç bildirilmesi halinde, kendilerinin bir kusuru olmamasına, kendilerine fiilen herhangi bir bildirim ve tebligat yapılmamasına rağmen, yukarıda belirtilen yaptırıma maruz bırakılmış olmaktadır. Bu durumun, erişim sağlayıcılarının, sözkonusu yaptırıma karşı yargı mercileri nezdinde itiraz edebilme gibi bazı haklarını kullanamamalarına neden olması da mümkündür. Şu halde iptali istenilen cümle, erişim sağlayıcılarını, kendilerinden kaynaklanmayan gecikmelere karşı yeterince koruma sağlamadığı için hukuki güvenlik ilkesine aykırılık oluşturduğu gibi, hak arama özgürlüğünün özünü de zedelemektedir.

Yukarıda belirtilen nedenlerle, 5651 sayılı Kanun'un 6/A maddesinin (7) numaralı fıkrasının "Bu kapsamda Birliğe yapılan tebligat erişim sağlayıcılara yapılmış sayılır" şeklindeki ikinci cümlesinin, Anayasa'nın 2. ve 36. maddelerine aykırı olduğu ve iptali gerektiği kanaatinde olduğumdan çoğunluk görüşüne katılmadım.

Üye - Erdal TERCAN

[1] Bu düzenlemeler yapılırken bireylerin internetin sunduğu engin fırsat ve imkanlardan en yaygın ve etkin biçimde yararlanmalarına olanak sağlanması ile vatandaşların ve toplumun internet ortamının meydana getirdiği/getireceği risk ve tehlikelerden korunması arasında, makul, adil kabul edilebilir bir dengenin gözetilmesi diğer bir deyişle özgürlük ile güvenlik arasında dengeli hukuki düzenlemelerin yapılması gerekeceği tabiidir.

[2] Günümüz itibarıyla dünya genelindeki internet kullanıcı sayısının 3 milyar 346 milyona, ülkemizde ise 47 milyona ulaştığı, ülkemizdeki internet kullanıcılarının "video izleme" eyleminde %93,6'lık oranla dünya 1. si ; %70'lik oranla "spor sitelerini ziyaret" eyleminde de Avrupa 1.si oldukları; günde ortalama 4,9 saat kişisel bilgisayarları üzerinden, 1,9 saat mobil cihazlar aracılığıyla internet ortamında buldukları (Global Dijital Statistics 2014) ; sosyal medyada geçirilen günlük ortalama sürenin 2,5 saat olduğu, %94'ünün en az bir sosyal paylaşım ve iletişim platformunda sayfasının bulunduğu, bu oranın çocuk internet kullanıcılarında %85 olduğu ve bu çocukların %42'sinin sosyal paylaşım sitesindeki hesaplarını kendi kişisel bilgilerinin herkes tarafından görülebileceği "herkese

açık" seçeneği ile kullandıkları (Avrupa Çevrimiçi Çocuklar Araştırma Projesi Türkiye Sonuçları 2010) belirtilmektedir. Yine günümüz itibarıyla internet ortamında dünya genelinde yaklaşık 950 milyon alan adı, 750 milyon web sitesi ki bunun yaklaşık 1 milyon 300 bininin yerli web sitesi 45 milyar web sayfası olduğu, sosyal paylaşım platformlarının birisinde bir saatte yaklaşık 350 milyon fotoğraf paylaşılırken, bir başkasında bir günde yaklaşık 1 milyar video izlendiği ifade edilmektedir.

Anayasa Mahkemesi - 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu (Madde 78)

Kararı (E. 2014/74)

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2014/74

Karar Sayısı: 2014/201

Karar Tarihi: 25.12.2014

R.G. Tarih-Sayı: 23.5.2015-29364

İTİRAZ YOLUNA BAŞVURAN: Danıştay Onbeşinci Dairesi

İTİRAZIN KONUSU: 31.5.2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun 78. maddesinin;

1- Birinci fıkrasının,

2- İkinci fıkrasının;

a- İkinci cümlesinin,

b- 17.4.2008 tarihli ve 5754 sayılı Kanun'un 66. maddesinin birinci fıkrasının (f) bendiyle eklenen son cümlesinin,

Anayasanın 2., 7., 13. ve 20. maddelerine aykırılığı ileri sürülerek iptallerine karar verilmesi istemidir.

I- OLAY

Davacılar tarafından 11.7.2012 tarihli ve 28350 sayılı Resmî Gazete'de yayımlanan Genel Sağlık Sigortası Verilerinin Güvenliği ve Paylaşımına İlişkin Yönetmelik'in bazı maddelerinin iptali ve yürütmenin durdurulması istemiyle açılan davada, itiraz konusu kuralların Anayasa'ya aykırı olduğu kanısına varan Mahkeme, iptalleri için başvurmuştur.

III- YASA METİNLERİ

A- İtiraz Konusu Yasa Kuralı

Kanunu'nun itiraz konusu kuralları da içeren 78. maddesi şöyledir:

"Sağlık hizmeti sunucularının kayıt ve bildirim zorunluluğu ve kontrol yetkisi

MADDE 78- Kurum ile sözleşmesi olan, tüm sağlık hizmeti sunucuları, sağlık hizmeti sunduğu tüm kişilere ait sözleşme hükümlerinde yer verilen bilgileri, belirlenen yöntemlere ve süreye uygun biçimde elektronik ortamda veya yazılı olarak Kuruma göndermek zorundadır. Bu bilgiler gönderilmeksizin talep edilen sağlık hizmeti bedelleri, bilgiler gönderilinceye kadar ödenmez.

Genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişinin sağlık bilgilerinin gizliliği esastır. Sağlık bilgilerinin ne şekilde korunacağı, ulusal güvenlik nedeniyle sağlık bilgisi paylaşımına açılmayacak kişilerin tespiti ilgili bakanlıkların önerisi üzerine Bakanlıkça tespit edilir. (Ek cümle: 17/4/2008-5754/66 md.) Bu kişi ve grupların sağlık bilgilerinin nasıl tutulacağı ilgili kuruluşların görüşleri alınarak hazırlanacak yönetmelik ile düzenlenir.

Kurum, genel sağlık sigortası hükümlerinin uygulanmasıyla ilgili olarak işverenler, sağlık hizmeti sunucuları ve diğer gerçek ve tüzel kişiler nezdindeki defter, belge ve bilgileri inceleyebilir, ibrazını isteyebilir.

Kurum, bu Kanunda belirtilen görevleriyle ilgili olarak sağlık hizmeti sunucularının yürüttüğü hizmet ve işlemleri kontrol yetkisine sahiptir. Kurum, bu yetkisini görevlendirdiği personeli vasıtasıyla veya kamu kurumları ve özel kurumlardan hizmet satın almak suretiyle kullanabilir."

B- Dayanılan Anayasa Kuralları

Başvuru kararında, Anayasa'nın 2., 7., 13. ve 20. maddelerine dayanılmıştır.

IV- İLK İNCELEME

Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Serruh KALELİ, Alparslan ALTAN, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT, Zehra Ayla PERKTAŞ, Recep KÖMÜRCÜ, Burhan ÜSTÜN, Engin YILDIRIM, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Erdal TERCAN, Muammer TOPAL, Zühtü ARSLAN ve M. Emin KUZ'un katılımlarıyla 22.4.2014 tarihinde yapılan ilk inceleme toplantısında, dosyada eksiklik bulunmadığından işin esasının incelenmesine OYBİRLİĞİYLE karar verilmiştir.

V- ESASIN İNCELENMESİ

Başvuru kararı ve ekleri, Raportör Hakan ATASOY tarafından hazırlanan işin esasına ilişkin rapor, itiraz konusu yasa kuralları, dayanılan Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A- Kanun'un 78. Maddesinin Birinci Fıkrasının İncelenmesi

Başvuru kararında, itiraz konusu kurallar ile kişisel veri kapsamında olan sağlık verilerinin işlenmesi, gizliliğinin korunması ve paylaşılmasına yönelik usul ve esasları belirleme ve bu konuda düzenleme yapma yetkisinin bütünüyle yürütme organına bırakıldığı, yasama organı tarafından, temel ilkeleri koyulmadan, çerçevesi çizilmeden, sınırsız, belirsiz, geniş bir alanı düzenleme yetkisinin yürütme organına bırakılmasının, Anayasa'nın 7., 13. ve 20. maddelerine ve sonuçta Anayasa'nın 2. maddesindeki hukuk devleti ilkesine aykırı olduğu ileri sürülmüştür.

Kanun'un 78. maddesinin itiraz konusu olan birinci fıkrasında, Sosyal Güvenlik Kurumu (Kurum) ile sözleşmesi olan tüm sağlık hizmeti sunucularının, sağlık hizmeti sunduğu tüm kişilere ait sözleşme hükümlerinde yer verilen bilgileri, belirlenen yöntemlere ve süreye uygun biçimde elektronik ortamda veya yazılı olarak Kuruma göndermek zorunda oldukları, bu bilgiler gönderilmeksizin talep edilen sağlık hizmeti bedellerinin, bilgiler gönderilinceye kadar ödenmeyeceği hüküm altına alınmıştır.

Anayasa'nın 13. maddesinde, temel hak ve özgürlüklerin, özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği, bu sınırlamaların da Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacağı ifade edilmiştir.

Anayasa'nın 13. maddesinde yer alan ölçülülük ilkesi, kişilerin temel hak ve özgürlüklerinden mahrum bırakılmaları halinde, elde edilmek istenen kamu yararı ile temel hakkından mahrum bırakılan bireyin hakları arasında adil bir denge kurulması gereğini ifade eder.

Anayasa'nın 20. maddesinde, özel hayatın gizliliği ve korunması güvence altına alınmıştır. Maddenin birinci fıkrasında, herkesin, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu ve özel hayatın ve aile hayatının gizliliğine dokunulamayacağı ifade edilmiş; ikinci fıkrasında ise özel hayatın gizliliğine ilişkin hakkın sınırlanma koşulları düzenlenmiştir. Dolayısıyla söz konusu hak mutlak ve sınırsız olmayıp, Anayasa'nın 13. ve 20. maddeleri gereğince belirli koşullarda, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmamak üzere kanunla sınırlanabilir.

5502 sayılı Sosyal Güvenlik Kurumu Kanunu'nun;

1. maddesinde; "Bu Kanunun amacı, Sosyal Güvenlik Kurumunun kuruluş, teşkilât, görev ve yetkilerine ilişkin usûl ve esasları düzenlemektir.

Bu Kanun ile Kuruma görev ve yetki veren diğer kanunların hükümlerini uygulamak üzere; kamu tüzel kişiliğini haiz, idarî ve malî açıdan özerk, bu Kanunda hüküm bulunmayan durumlarda özel

hukuk hükümlerine tâbi Sosyal Güvenlik Kurumu kurulmuştur. Kurum, Çalışma ve Sosyal Güvenlik Bakanlığının ilgili kuruluşudur. Kurumun merkezi Ankara'dadır.

Kurum, Sayıştay'ın denetimine tâbidir."

denilerek Kurumun kuruluş amacı ve statüsü;

3. maddesinde ise "Kurumun temel amacı; sosyal sigortacılık ilkelerine dayalı, etkin, adil, kolay erişilebilir, aktüeryal ve malî açıdan sürdürülebilir, çağdaş standartlarda sosyal güvenlik sistemini yürütmektir.

Kurumun görevleri şunlardır:

- a) Ulusal kalkınma strateji ve politikaları ile yıllık uygulama programlarını dikkate alarak sosyal güvenlik politikalarını uygulamak, bu politikaların geliştirilmesine yönelik çalışmalar yapmak.
- b) Hizmet sunduğu gerçek ve tüzel kişileri hak ve yükümlülükleri konusunda bilgilendirmek, haklarının kullanılmasını ve yükümlülüklerinin yerine getirilmesini kolaylaştırmak.
- c) Sosyal güvenliğe ilişkin konularda; uluslararası gelişmeleri izlemek, Avrupa Birliği ve uluslararası kuruluşlar ile işbirliği yapmak, yabancı ülkelerle yapılacak sosyal güvenlik sözleşmelerine ilişkin gerekli çalışmaları yürütmek, usûlüne göre yürürlüğe konulmuş uluslararası antlaşmaları uygulamak.
- ç) Sosyal güvenlik alanında, eğitim, araştırma ve danışmanlık faaliyetleri yapmak ve yaptırmak, kamu idareleri arasında koordinasyon ve işbirliğini sağlamak.
- d) Bu Kanun ve diğer kanunlar ile Kuruma verilen görevleri yapmak."

denilerek Kurumun amacı ve görevleri belirtilmiştir.

İtiraz konusu kural gereğince, kişilerin özel hayatlarını ilgilendiren sağlık verilerinin Kurum tarafından alınması, özel hayatın gizliliği hakkının sınırlanması sonucunu doğurmaktadır. Bu sınırlamanın Anayasa'ya uygun olabilmesi için Anayasa'nın 13. maddesinde öngörülen temel hakların sınırlandırılmasına ilişkin ilkelere aykırı olmaması ve bu bağlamda kamu yararı ile özel hayatın gizliliği hakkı arasında adil bir denge kurması gerekir.

İtiraz konusu kuralla Kurum ile sözleşmesi olan sağlık hizmeti sunucularının, Kuruma göndermek zorunda oldukları bilgilerin, Kurum ile sağlık hizmeti sunucuları arasında yapılan sağlık hizmeti alınmasına ilişkin sözleşme hükümlerinde yer alan bilgiler olduğu ifade edilmiştir. Buna göre bu bilgiler, Kanun kapsamında sağlık hizmetinden faydalanan kimselerin kimlik ve ikamet bilgileri ile tanı veya

ön tanı, muayene, tetkik, tahlil, tedavi gibi sağlıklarıyla ilgili hususlara ilişkin bilgilerden oluşmaktadır.

Kurumun faaliyet alanındaki görevlerini yerine getirebilmesi için, sosyal sigortaların ve genel sağlık sigortasının işleyişi ile ilgili verilere ihtiyacı bulunduğu şüphe yoktur. Kurumun söz konusu verilere sahip olmadan, sağlık hizmetinden faydalanacak kişilerin tespiti; sağlık hizmeti sunucularına verdikleri hizmet karşılığında ödeme yapılması; denetim ve kontrol görevinin yerine getirilmesi ve sosyal güvenlik politikalarının geliştirilmesine yönelik çalışmalar yapması mümkün değildir. Bu nedenle, özel hayatın gizliliği hakkını kamu yararı amacıyla sınırlandırdığı anlaşılan kuralın, demokratik toplum düzeninde gerekli bir müdahale niteliği taşıdığı kuşku bulunmamaktadır.

Öte yandan, itiraz konusu kural ile Kuruma verilen sağlık bilgisi toplama yetkisinin çerçevesi, Kurumun kuruluş amacı ve faaliyet alanı ile belirlenmiş ve bu şekilde kamu yararı ile özel hayatın gizliliği hakkı arasında adil bir denge kurulmuştur. Bu nedenle, Kuruma verilen kişilerin sağlık verilerini alma yetkisinin ölçülülük ilkesine aykırı bir yönü de bulunmamaktadır.

Açıklanan nedenlerle, itiraz konusu kural Anayasa'nın 13. ve 20. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın Anayasa'nın 2. ve 7. maddeleriyle ilgisi görülmemiştir.

Osman Alifeyyaz PAKSÜT ile Engin YILDIRIM bu görüşe katılmamıştır.

B- Kanun'un 78. Maddesinin İkinci Fıkrasının, İkinci Cümlesi ile 5754 Sayılı Kanun'un 66. Maddesinin Birinci Fıkrasının (f) Bendiyle Eklenen Son Cümlesinin İncelenmesi

Başvuru kararında, kuralların, Kanun'un 78. maddesinin birinci fıkrasında belirtilen gerekçelerle Anayasa'nın 2., 7., 13. ve 20. maddelerine aykırı olduğu ileri sürülmüştür.

Kanun'un 78. maddesinin ikinci fıkrasının birinci cümlesinde, genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişinin sağlık bilgilerinin gizliliğinin esas olduğu ifade edildikten sonra, itiraz konusu ikinci cümlesinde, sağlık bilgilerinin ne şekilde korunacağını ve ulusal güvenlik nedeniyle sağlık bilgisi paylaşımına açılmayacak kişilerin tespitinin ilgili bakanlıkların önerisi üzerine Çalışma ve Sosyal Güvenlik Bakanlığınca tespit edileceği; 5754 sayılı Kanun'un 66. maddesinin birinci fıkrasının (f) bendiyle eklenen itiraz konusu son cümlesinde ise bu kişi ve grupların sağlık bilgilerinin nasıl tutulacağını ilgili kuruluşların görüşleri alınarak hazırlanacak yönetmelik ile düzenleneceği hüküm altına alınmıştır.

Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır. Kişinin bedensel ya da zihinsel sağlığına ilişkin kayıt edilmiş bilgilerinin tamamından oluşan sağlık bilgileri, aralarında bireyin ırk, siyasî düşünce, felsefî inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, özel yaşamları ve her türlü mahkûmiyetleri ile ilgili verilerin de bulunduğu "hassas" veya "özel niteliği olan" kişisel veriler kategorisinde yer almakta olup, bu yönüyle özel bir öneme sahiptir.

Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Bilişim teknolojilerindeki gelişmeler sonucunda, geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi; daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması; verilere erişim ve veri transferinin kolaylaşması; kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler, günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır. Bu bağlamda Anayasa'nın 20. maddesinin üçüncü fıkrasının son cümlesinde, "Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilerek kişisel verilerin korunması hakkı anayasal güvenceye bağlanmış ve bu şekilde kamu makamlarının keyfi müdahalelerine karşı koruma altına alınmıştır.

Yasama yetkisinin devredilemezliği ilkesi gereğince, Anayasa'nın açıkça kanunla düzenlenmesini öngördüğü konularda yürütme organına doğrudan ve ilk elden düzenleyici işlem yapma yetkisi verilemez. Kurumun faaliyet alanı kapsamında elde ettiği sağlık bilgilerinin korunması, paylaşılması ve tutulmasına yönelik usul ve esasları belirleme yetkisini Çalışma ve Sosyal Güvenlik Bakanlığına veren itiraz konusu kurallar, Anayasa'nın 20. maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceğine ilişkin güvenceye aykırıdır.

Açıklanan nedenlerle, itiraz konusu kurallar Anayasa'nın 20. maddesine aykırıdır. İptalleri gerekir.

Kurallar, Anayasa'nın 20. maddesine aykırı bulunarak iptal edildiğinden dolayı Anayasa'nın 2., 7. ve 13. maddeleri yönünden ayrıca incelenmesine gerek görülmemiştir.

VI- SONUÇ

31.5.2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun 78. maddesinin;

A- Birinci fıkrasının Anayasa'ya aykırı olmadığına ve itirazın REDDİNE, Osman Alifeyyaz PAKSÜT ile Engin YILDIRIM'ın karşıoyları ve OYÇOKLUĞUYLA,

B- İkinci fıkrasının;

1- İkinci cümlesinin,

2- 17.4.2008 tarihli ve 5754 sayılı Kanun'un 66. maddesinin birinci fıkrasının (f) bendiyle eklenen son cümlesinin,

Anayasa'ya aykırı olduklarına ve İPTALLERİNE, OYBİRLİĞİYLE,

25.12.2014 tarihinde karar verildi.

Başkan - Haşim KILIÇ

Başkanvekili - Serruh KALELİ

Başkanvekili - Alparslan ALTAN

Üye: Serdar ÖZGÜLDÜR; Osman Alifeyyaz PAKSÜT; Recep KÖMÜRCÜ; Burhan ÜSTÜN; Engin YILDIRIM; Nuri NECİPOĞLU; Hicabi DURSUN; Celal Mümtaz AKINCI; Erdal TERCAN; Muammer TOPAL; Zühtü ARSLAN; M. Emin KUZ; Hasan Tahsin GÖKCAN

KARŞIOY GEREKÇESİ

5510 sayılı sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun 78. maddesinin birinci fıkrasında, Kurum ile sözleşmesi olan tüm sağlık hizmeti sunucularının, sağlık hizmeti sunduğu tüm kişilere ait sözleşme hükümlerinde yer verilen bilgileri, belirlenen yöntemlere ve süreye uygun biçimde elektronik ortamda veya yazılı olarak Kuruma göndermek zorunda olduğu, bu bilgiler gönderilmeksizin talep edilen sağlık hizmeti bedellerinin, bilgiler gönderilinceye kadar ödenmeyeceği belirtilmektedir.

Bahse konu bilgiler, Kanun kapsamında sağlık hizmetlerinden faydalanan kimselerin kimlik ve ikamet bilgileri ile tanı veya ön tanı, muayene, tetkik, tahlil, tedavi gibi, sağlıklarıyla ilgili bilgilerdir. Buna göre, Kuruma iletilecek bilgilerin "kişisel veri" olduğunda tereddüt bulunmamaktadır.

Anayasa'nın 20. maddesinde özel hayatın gizliliği güvence altına alınmış, herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir.

İptali istenen kuralla, sağlık hizmeti sunucularının Kurumla yapacakları sözleşme kapsamındaki kişisel bilgilerin tamamını Kuruma iletmeleri öngörülmele birlikte bu verilerin korunmasına ilişkin bir düzenlemeye yer verilmemiştir. Sözleşmede yer alan bilgileri belirleme ve bunları kullanmada İdare'ye ucu açık, çerçevesi çizilmemiş, sınırsız bir yetki verildiği anlaşılmaktadır. Kurumun kuruluş alanı ve faaliyetlerinin yasa ile belirlenmiş olması, Anayasa'nın 20. maddesinin öngördüğü anlamda kişisel verilerin korunması için yeterli bir yasal düzenleme olarak kabul edilemez. Bu durumda iptali istenen kuralın, Anayasa'ya aykırı olduğu açıktır.

Açıklanan nedenle kuralın iptali gerektiği düşüncesiyle çoğunluk görüşüne katılmamaktayım.

Üye - Osman Alifeyyaz PAKSÜT

KARŞIOY GEREKÇESİ

5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun 78. maddesinin birinci fıkrası "Kurum ile sözleşmesi olup olmadığına bakılmaksızın tüm sağlık hizmeti sunucuları, sağlık hizmeti sunduğu tüm kişilere ait sözleşme hükümlerinde yer verilen bilgileri, belirlenen yöntemlere ve süreye uygun biçimde elektronik ortamda veya yazılı olarak Kuruma göndermek zorundadır. Bu bilgiler gönderilmeksizin talep edilen sağlık hizmeti bedelleri, bilgiler gönderilinceye kadar ödenmez" düzenlemesini içermektedir.

İtiraz konusu kuralla, Sosyal Güvenlik Kurumu sağlık hizmeti sunucularından Kanun kapsamındaki sağlık hizmetinden yararlanan kimselerin kimlik ve ikamet bilgileri ile tanı veya ön tanı, muayene, tetkik, tahlil, tedavi gibi sağlıklarıyla ilgili hususlara ilişkin bilgileri alabilmektedir. Hassas veri kategorisinde olan ve bireyin sağlığına ilişkin bilgileri içeren kişisel sağlık verilerinin herhangi bir sınırlama yapılmadan, kapsam ve şartları belirlenmeden toplanması ve işlenmesi Anayasa'nın 20. maddesine aykırıdır. Özel hayata saygı hakkını düzenleyen bu maddede, herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu ve bu hakkın, kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı belirtilmektedir.

Sosyal Güvenlik Kurumu'nun görevlerini yerine getirebilmesi için genel sağlık sigortası ile ilgili verilere ihtiyacı olduğu açıktır. Her ne kadar Çoğunluk, kuralla Sosyal Güvenlik Kurumu'na kişilerin özel hayatlarının gizliliğini ihlal eden bilgileri alma konusunda yetki verildiğinin söylenemeyeceğini iddia etse de, kural kapsamındaki verilerin çoğunun özel korumaya ihtiyaç duyan hassas kişisel veriler olduğundan kuşku duyulmamalıdır.

Anayasa'nın 20. maddesinin son fıkrası çok açık bir şekilde kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceğini hüküm altına almakla birlikte ülkemizde kişisel verilerin korunmasını düzenleyen çerçeve bir kanun henüz yasalaşmamıştır. İtiraz konusu kuralla, Sosyal Güvenlik Kurumu'na tanınan kişisel veri toplama ve işleme yetkisinin nasıl kullanılacağıyla ilgili Genel Sağlık Sigortası ve Paylaşımına İlişkin Yönetmelikte bazı güvencelere yer verilmiştir. Ancak, 20. maddenin son fıkrası gereği, bu güvencelerin kanun düzeyinde sağlanması gerekmektedir. Kişisel verilerin işlenmesinin genel ilke ve esaslarının, kişilerin haklarını korumalarına yardımcı olacak mekanizmaların ve ilgili kuruluşların kişisel verilerin işlenmesi sırasında hakka aykırı davranışlarda bulunmamalarını önleyerek şikâyetleri değerlendirecek kanunla oluşturulmuş süreçlerin yokluğu, kamu kurumlarının veri toplama iştahlarını neredeyse sınırsız bir şekilde kabartmaktadır.

Anayasa'nın 13. maddesinde, temel hak ve özgürlüklerin özlerine dokunulmaksızın ölçülülük ilkesine uygun şekilde, yasayla sınırlandırılabilmesi belirtilmektedir. Ölçülülük ilkesi sınırlamada başvurulan aracın sınırlama amacını gerçekleştirmeye elverişli olmasını; bu aracın sınırlama amacı açısından gerekli olmasını ve araçla amacın ölçüsüz bir oran içinde bulunmamasını ifade eder. Burada kısıtlama için kullanılan araçla amaç arasında hak ve özgürlüğü en az sınırlayacak dengeli bir orantı aranmaktadır. Elverişlilik ölçütüne göre bir yasal düzenlemenin sınırlama amacı bakımından elverişli sayılması için bu düzenlemenin arzulanan amaca katkı yapması gerekmektedir. Konumuz açısından bakıldığında, veri toplanmasının Kurum'un amaçlarını gerçekleştirmesine katkı yaptığını söyleyebiliriz. Gereklilik ise bir temel hakkı en az sınırlayan aracın seçilmesini gerektirmekle birlikte itiraz konusu kuralın, hakkı en az sınırlayan yumuşak bir araç olduğunu söylemek mümkün değildir. Çünkü söz konusu kural, çok geniş ve sınırsız bir çerçeveyi kapsayarak bireyin neredeyse her türlü kişisel sağlık verisinin toplanması ve işlenmesini kapsamı dâhilinde görmektedir. Orantılılıkta aranan ise araç ve amacın birbirine karşı ölçüsüz bir oran içerisinde olmamasıdır. Herhangi bir bağımsız denetime tabi olmadan, veri toplanması ve işlenmesi bir orantısızlık yaratmaktadır. Bireyin özel alanının tehlikeye girmesi, onun hakkında veri toplanması kadar, kime, hangi amaçlarla bunların aktarılacağı konusunda denetim imkânını da kaybetmesinde yatmaktadır.

Demokratik toplumda gereklilikten anlaşılması gereken başvurulan tedbirin demokratik toplumu açıklayan ilkelerle uyumlu olup, olmamasıdır. Bu ilkelerin değerini azaltan her uygulama demokratik toplum için gerekli değildir. Demokratik toplum, ayrıca hak ve özgürlüklere karşı gerçekleştirilen her müdahaleye karşı kişilere bir takım güvencelerin de sağlanmasını gerektirir. Oysa itirazı talep edilen kural, kötüye kullanım olasılığı karşısında engelleyici etkili ve yeterli tedbirlere yer vermemektedir.

Özel hayatın gizliliği ve bu kapsamda kişisel verilerin korunması konusu her şeyden önce insan onuruna saygı ve kişilik haklarına dayanmaktadır. Bu hak, kişinin saygınlığını ve kişiliğini serbestçe geliştirmesini mümkün kılan şeref ve haysiyet, özel yaşam ve sağlık gibi kişisel değerler üzerindeki çıkarlarını belirterek, bireye kişiliğini dilediği şekilde, serbestçe geliştirebileceği, kendisi ve sevdikleriyle bir arada olabileceği özerk bir yaşam alanına sahip olma şansı vermektedir. Bu alanda birey, maddi ve manevi kişiliğini geliştirmek ve başkaları tarafından bilinmesini istemediği hususların güvence altına alınmasını istemek hakkına sahiptir. Kişisel verilerin korunması kişinin maddi ve manevi varlığını geliştirmesine imkân tanıyarak, bireyin hayatını kendi özgür iradesiyle düzenlemesine katkı sağlamaktadır. Bireyin kişisel verileri üzerindeki hakkı yeteri kadar korunmazsa, kişiliğini serbestçe geliştirmesi zora gireceğinden, özgür iradeleriyle yaşamlarını biçimlendiren bireylerden oluşan demokratik bir toplum düzeninin ortaya çıkması ve korunması da güçleşecektir. Kişisel verilerin korunmasıyla, kişisel veri toplanması, saklanması ve işlenmesi sırasında bireyin hak ve özgürlüklerinin korunarak demokratik toplum düzeninin oluşmasına katkı yapmak hedeflenmektedir.

Kişisel verilerin toplanması ve işlenmesi sırasında bireyin bu veriler üzerindeki hakkı, onun devlet veya üçüncü kişiler tarafından sıradan bir veri nesnesine indirgenmesini önlemek amacını taşımaktadır. Sağlıkla ilgili kişisel verilerin hiçbir sınırlamaya tabi tutulmadan toplanması, işlenmesi ve aktarılması, kişinin basit bir veri nesnesi yapılarak kişi olma vasfının dikkate alınmaması insan haysiyetini zedeleyici bir faaliyettir. Bireyin, ahlaki ve toplumsal kişiliğinin gelişiminde ve diğer insanlarla olan ilişkilerini düzenlemede önemli bir kavram olan mahremiyetin ihlali insan onurunun ve kişiliğinin ihlali anlamına gelmektedir.

Kişisel verilerin korunması, bir özgürlük sorunudur ve özel hayatın gizliliği, yalnız kalma hakkından kişinin kendisi hakkındaki veri ve bilgileri kontrol hakkını içerir bir şekle dönüşmektedir. Kişinin maddi ve manevi varlığını geliştirmesi, ancak ve ancak, faaliyetlerini özgürce gerçekleştirmesi ile mümkündür. Bireylere hayatlarını diledikleri gibi düzenleme fırsatı sunan bir alan yaratma imkânı tanıyan özel yaşamın gizliliği hakkı, kişinin özerk bir birey olması açısından son derece önemlidir. Bu

hak, başkaları ve devlet tarafından ihlal edilmemesi, saygı gösterilmesi gereken bir çeşit onursal duvar yaratmaktadır.

Anayasa Mahkemesi, Türkiye İstatistik Kanunuyla ilgili bir kararında (E: 2006/167, K:2008/86), istenecek bilgilerin kapsam ya da sınırlarının belirsizliğinin, bireyi İdare'ye karşı korumasız bıraktığını, bunun da Anayasa'nın özel hayatın gizliliğini koruyan hükümlerine aykırı olduğunu tespit etmiştir. AİHM de, hangi koşullar altında, hangi amaçla, ne kadar süreyle kamu otoritelerinin özel hayatla ilgili bilgileri saklayacağı ve kullanacağını belirsizliğini, istismarlara karşı hiçbir önlem alınmamasını, kötüye kullanımı engellemeye yönelik etkili denetim mekanizmalarının öngörülmemesini ve verilerin değerlendirilmesine ilişkin hukuki sınırlar çizilmemesini, AİHS'in 8. maddesinin (ve 13. maddesinin) ihlali olarak görmüştür (Rotaru/Romanya, Başvuru no: 28341/95, ECHR 2000-V, IHRL 2923 (ECHR 2000), 4 Mayıs 2000, para.57 ve 59).

Yukarıda açıklanan gerekçelerden dolayı itiraz konusu kuralın iptal edilmesi gerektiği düşüncesiyle çoğunluk görüşüne katılmadım.

Üye - Engin YILDIRIM

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2013/114

Karar Sayısı: 2014/184

Karar Tarihi: 4.12.2014

R.G. Tarih-Sayı: 16.07.2015-29418

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri Engin ALTAY ve Muharrem İNCE ile birlikte 126 milletvekili

İTİRAZ YOLUNA BAŞVURAN: Trabzon İdare Mahkemesi (E. 2014/134)

DAVA VE İTİRAZIN KONUSU: 12.7.2013 tarihli ve 6495 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un;

A- 26. maddesiyle değiştirilen, 4.11.1983 tarihli ve 2942 sayılı Kamulaştırma Kanunu'nun 22. maddesinin birinci fıkrasının son iki cümlesinin,

B- 27. maddesiyle 2942 sayılı Kanun'un 25. maddesine eklenen fıkranın,

C- 28. maddesiyle 2942 sayılı Kanun'a eklenen geçici 8. maddenin,

D- 33. maddesiyle, 9.10.2003 tarihli ve 4982 sayılı Bilgi Edinme Hakkı Kanunu'nun 2. maddesine eklenen fıkranın,

E- 43. maddesiyle, 22.6.2006 tarihli ve 5525 sayılı Memurlar ile Diğer Kamu Görevlilerinin Bazı Disiplin Cezalarının Affı Hakkında Kanun'a eklenen ek 1. maddenin;

1- Birinci fıkrasının " 28/2/1997 tarihinden sonra . 28/8/1999 tarihli ve 4455 sayılı Memurlar İle Diğer Kamu Görevlilerinin Disiplin Cezalarının Affı Hakkında Kanun veya bu Kanun hükümlerinden yararlanmış olanların; " bölümünün,

2- İkinci fıkrasının ". 1/1/1990 ile...657 sayılı Kanununun 125 inci maddesinin birinci fıkrasının (A) bendinin (g) alt bendinde yer alan fiili işlediği gerekçesiyle anılan Kanununun 56 ve 57 nci maddeleri uyarınca disiplin cezası veya olumsuz sicil almış olmaları nedeniyle. " bölümünün,

F- 59. maddesiyle, 13.12.1983 tarihli ve 178 sayılı Maliye Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 43. maddesine eklenen fıkranın,

G- 73. maddesinin;

1- (h) fıkrasının;

a- (1) numaralı bendiyle deęiřtirilen, 11.10.2011 tarihli ve 663 sayılı Saęlık Bakanlıęı ve Baęlı Kuruluşlarının Teřkilat ve Grevleri Hakkında Kanun Hkmnde Kararname'nin 23. maddesinin (7) numaralı fıkrasının (c) ve () bentlerinin,

b- (3) numaralı bendiyle deęiřtirilen 663 sayılı Kanun Hkmnde Kararname'nin 47. maddesinin (1), (2) ve (3) numaralı fıkralarının,

2- (p) fıkrasının;

a- (1) numaralı bendiyle, 3.5.1985 tarihli ve 3194 sayılı İmar Kanunu'nun 8. maddesine eklenen (ı), (i) ve (j) bentlerinin,

b- (3) numaralı bendiyle deęiřtirilen 3194 sayılı Kanun'un ek 4. maddesinin,

3- (r) fıkrasının;

a- (1) numaralı bendiyle deęiřtirilen, 7.6.1985 tarihli ve 3224 sayılı Trk Diř Hekimleri Birlięi Kanunu'nun 11. maddesinin birinci fıkrasının (f) bendinde yer alan ".rehber ." ibaresinin,

b- (2) numaralı bendiyle deęiřtirilen 3224 sayılı Kanun'un 26. maddesinin birinci fıkrasının (e) bendinde yer alan ".rehber." ibaresinin,

c- (3) numaralı bendiyle deęiřtirilen 3224 sayılı Kanun'un 40. maddesinin bařlıęında yer alan "Rehber." ibaresi ile birinci ve ikinci fıkralarında yer alan ".rehber." ibarelerinin,

4- (bb) fıkrasıyla, 7.7.2010 tarihli ve 6004 sayılı Dıřiřleri Bakanlıęının Kuruluş ve Grevleri Hakkında Kanun'un 12. maddesinin;

a- (2) numaralı fıkrasının deęiřtirilen (d) bendinin,

b- (3) numaralı fıkrasının (a) bendine eklenen cmlenin,

5- (cc) fıkrasıyla deęiřtirilen, 3.12.2010 tarihli ve 6085 sayılı Sayıřtay Kanunu'nun 4. maddesinin (1) numaralı fıkrasının;

a- (a) bendinde yer alan ". % 50'den fazla olan ." ibaresinin,

b- (b) bendindeki " Kamu payı % 50'den az olmamak kaydıyla ." ibaresinin,

Anayasa'nın 2., 5., 7., 9., 10., 13., 20., 35., 36., 38., 45., 46., 48., 49., 56., 60., 64., 70., 74., 90., 135. ve 160. maddelerine aykırılığı ileri sürülerek iptallerine ve yürürlüklerinin durdurulmasına karar verilmesi talebidir.

I- İPTALİ İSTENİLEN KANUN HÜKÜMLERİ

6545 sayılı Kanun'un;

1- 26. maddesiyle değiştirilen, 2942 sayılı Kanun'un dava konusu kuralların da yer aldığı "Vazgeçme, iade ve devir" başlıklı 22. maddesi şöyledir:

"(Değişik birinci fıkra: 24/4/2001 - 4650/13 md.) Kamulaştırmanın ve bedelinin kesinleşmesinden sonra taşınmaz malların kamulaştırma amacına veya kamu yararına yönelik herhangi bir ihtiyaca tahsisi lüzumu kalmaması halinde, keyfiyet idarece mal sahibi veya mirasçılarına 7201 sayılı Tebligat Kanunu hükümlerine göre duyurulur. Bu duyurma üzerine mal sahibi veya mirasçuları, aldığı kamulaştırma bedelini üç ay içinde ödeyerek taşınmaz malını geri alabilir. (Ek cümle: 14/2/2013 - 6427/3 md.; Değişik: 12/7/2013-6495/26 md.) Kamulaştırmayı yapan idarece kamulaştırma amacına uygun tesisat, yapı veya donatı yapıldıktan ve en az 5 yıl kullanıldıktan sonra bu ihtiyacın ortadan kalkması nedeniyle kamulaştırma amacında kullanılmayan taşınmazlar önceki mal sahibi veya mirasçılarına iade edilmez. Bu taşınmazların kamulaştırma amacı dışında idarece tasarruf edilmesi hâlinde, önceki mal sahibi veya mirasçuları tarafından idareden herhangi bir hak, bedel veya tazminat talebinde bulunulamaz.

Ancak, kamulaştırılan taşınmaz mala kamulaştırmayı yapan idare dışında başka bir idare, kamulaştırma yoluyla gerçekleştirebileceği bir kamu hizmeti amacıyla istekli olduğu takdirde, yukarıdaki fıkra hükmü uygulanmayarak bu Kanununun 30 uncu veya 1050 sayılı Muhasebe Umumiye Kanununun 23 üncü maddesine göre işlem yapılır. "

2- 27. maddesiyle dava konusu fıkranın eklendiği 2942 sayılı Kanun'un "Hakların sınırlandırılması ve mülkiyetin idareye geçmesi" başlıklı 25. maddesi şöyledir:

" Hakların kullanılması ve borçların yerine getirilmesi bakımından kamulaştırma işlemi, mal sahibi için 10 uncu madde uyarınca mahkemece yapılan tebligatla başlar. Mülkiyetin idareye geçmesi, mahkemece verilen tescil kararı ile olur.

Mahkemece verilen tescil kararı tarihinden itibaren taşınmaz mal sahibinin, kamulaştırılması kararlaştırılan taşınmaz malda yeni inşaat veya ekim yapmak veya mevcut inşaatla esaslı değişiklikler meydana getirmek gibi kullanma hakları kalkar. Bundan sonra yapılanların değeri dikkate alınmaz.

(Ek fıkra: 12/7/2013-6495/27 md.)Baraj, sulama şebekeleri ve boru hatları, karayolu, demiryolu, liman ve havaalanı gibi gelecek yıllara sari büyük projelerde kamu yararı kararı kamulaştırılacak taşınmazların bulunduğu mahalle ve/veya köy muhtarlığında on beş gün süre ile asılmak suretiyle ilan edilir. Kamu yararı kararının ilan süresinin bitiminden itibaren, kamulaştırılacak taşınmazlar üzerine yapılan sabit tesisler ile dikilen ağaçların bedeli, kamulaştırma bedelinin tespitinde dikkate alınmaz. Taşınmazlardaki bu sınırlama ilan tarihinin bitiminden itibaren beş yılı geçemez. "

3- 28. maddesiyle 2942 sayılı Kanun'a eklenen dava konusu geçici 8. maddesi şöyledir:

" Bu Kanunun 22 nci maddesinin birinci fıkrasının son cümlesi hükmü, bu maddenin yürürlüğe girdiği tarihten önce gerçekleştirilen kamulaştırma işlemleri nedeniyle, kamulaştırılan taşınmazların eski malikleri veya mirasçıları tarafından bu taşınmazların geri alınması, bedel veya tazminat talebiyle açılan ve henüz kesinleşmeyen davalarda da uygulanır. "

4- 33. maddesiyle, dava konusu fıkranın eklendiği 4982 sayılı Kanun'un "Kapsam" başlıklı 2. maddesi şöyledir:

" Bu Kanun; kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının faaliyetlerinde uygulanır.

1.11.1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun hükümleri saklıdır.

(Ek fıkra: 12/7/2013-6495/33 md.) Ölçme, Seçme ve Yerleştirme Merkezi Başkanlığı tarafından uygulanan sınavlara ait soru ve cevaplar bu Kanun kapsamı dışındadır. "

5- 43. maddesiyle, 5525 sayılı Kanun'a eklenen ve dava konusu kurallarında yer aldığı ek 1. madde şöyledir:

" 28/2/1997 tarihinden sonra verilen disiplin cezaları nedeniyle memuriyetten çıkarılanlardan 28/8/1999 tarihli ve 4455 sayılı Memurlar İle Diğer Kamu Görevlilerinin Disiplin Cezalarının Affı Hakkında Kanun veya bu Kanun hükümlerinden yararlanmış olanların ;

a) Memuriyete giriş şartlarını kaybetmemiş olmaları,

b) Durumlarına uygun boş kadro veya pozisyon bulunması,

c) Bu kadro ve pozisyonlara ait nitelikleri taşımaları,

ç) Üç ay içinde müracaat etmeleri,

kaydıyla yeniden göreve alınmalarında 20/12/2012 tarihli ve 6363 sayılı 2013 Yılı Merkezi Yönetim Bütçe Kanununun eki (İ) Cetvelinde yer alan atama sayısı sınırlaması uygulanmaz.

657 sayılı Devlet Memurları Kanununa tabi aday memur statüsünde görev yapmakta iken 1/1/1990 ile bu maddenin yürürlüğe girdiği tarih arasında 657 sayılı Kanunun 125 inci maddesinin birinci fıkrasının (A) bendinin (g) alt bendinde yer alan fiili işlediği gerekçesiyle anılan Kanunun 56 ve 57 nci maddeleri uyarınca disiplin cezası veya olumsuz sicil almış olmaları nedeniyle memurlukla ilişkisi kesilip asli memurluğa atanamayanlar, bu maddenin yürürlüğe girdiği tarihten itibaren üç ay içinde eski kurumlarına müracaat etmeleri hâlinde, 657 sayılı Kanunun 48 inci maddesinde belirtilen genel şartları taşımaları koşuluyla kurumlarında daha önce işgal ettikleri aynı veya benzer unvanlı kadrolara iki ay içinde atanırlar.

4/11/1981 tarihli ve 2547 sayılı Yükseköğretim Kanunu ve 2547 sayılı Yükseköğretim Kanununa atıf yapan Yüksek Öğretim Kurumları Öğrenci Disiplin Yönetmeliği hükümlerine göre aldıkları disiplin cezaları nedeniyle yükseköğretim kurumlarından ilişkisi kesilip, anılan Kanunun geçici 40 ıncı, geçici 43 üncü, geçici 45 inci, geçici 46 ncı, geçici 48 inci, geçici 50 nci, geçici 56 ncı ve geçici 58 inci madde hükümlerinden yararlanmak suretiyle önlisans veya lisans öğrenimini söz konusu maddelerde öngörülen şartlar dâhilinde; bu maddenin yürürlüğe girdiği tarihten önce bitirmiş olanlar için bu maddenin yürürlüğe girdiği tarihten itibaren iki yıl süreyle, 31/12/2015 tarihine kadar bitirecek olanlar için ise öğrenimlerini bitirdikleri tarihten itibaren iki yıl süreyle, kamu görevlerine giriş için ilgili mevzuatında öngörülen yaş şartı aranmaz."

6- 59. maddesiyle, dava konusu fıkranın eklendiği 178 sayılı Kanun Hükmünde Kararname (KHK)'nin "Maliye Uzmanlığı ve Defterdarlık Uzmanlığı" başlıklı 43. maddesi şöyledir:

" Bakanlık merkez teşkilatında Maliye Uzmanı ve Maliye Uzman Yardımcısı çalıştırılabilir. Maliye Uzmanı ve Maliye Uzman Yardımcılarına diğer görevlerinin yanısıra görev yaptıkları başkanlık ve genel müdürlüklerin görev alanına giren konularda ilgili kuruluşlar nezdinde araştırma, inceleme ve analiz işleri ile mevzuatla kendilerine verilen diğer görevler yaptırılabilir. Bütçe ve Mali Kontrol Genel Müdürlüğü, Muhasebat Genel Müdürlüğü, Milli Emlak Genel Müdürlüğü ve Personel Genel Müdürlüğünde görev yapan Maliye Uzmanlarına, yönetmelikle belirlenen usul ve esaslar çerçevesinde genel müdürlüklerin görev alanına giren konularda teftiş, denetim, inceleme ve soruşturma işleri yaptırılabilir.

Bakanlık taşra teşkilatında Defterdarlık Uzmanı ve Defterdarlık Uzman Yardımcısı çalıştırılabilir. Defterdarlık Uzmanı ve Defterdarlık Uzman Yardımcılarına diğer görevlerinin yanısıra genel bütçe kapsamındaki kamu idareleri ile özel bütçeli idareler ve bunlara bağlı işletmelerdeki saymanlıklar ve defterdarlık birimlerinde yönetmelikle belirlenen usul ve esaslar çerçevesinde denetim ve inceleme yaptırılabilir. Defterdarlık uzmanlarından denetim yapmakla görevlendirilenler yer değiştirme

suretiyle atamaya tabi olup, bunların görevlendirme, çalışma ve yer deęiřtirmelerine iliřkin usul ve esaslar yönetmelikle düzenlenir.

(Deęişik fıkra: 12/7/2013-6495/59 md.) Defterdarlık Uzman Yardımcılığına atanabilmek için 657 sayılı Kanununun 48 inci maddesinde sayılan genel şartlara ek olarak en az dört yıllık eğitim veren yükseköğretim kurumlarının hukuk, siyasal bilgiler, iktisat, işletme, iktisadi ve idari bilimler fakülteleri ile Bakanlığın görev alanına giren ve yönetmelikle belirlenen yükseköğretim kurumlarından ya da bunlara denklięi Yükseköğretim Kurulunca kabul edilen yükseköğretim kurumlarından mezun olmak ve yapılacak özel yarışma sınavında başarılı olmak gerekir. Defterdarlık Uzman Yardımcılığı yarışma sınavı, yazılı ve sözlü aşamalardan oluşur.

(Mülga fıkra: 12/7/2013-6495/59 md.) (.)

Defterdarlık Uzman Yardımcılığına atananlar, en az üç yıl fiilen çalışmak kaydıyla açılacak yeterlik sınavına girme hakkını kazanırlar. Sınavda başarılı olamayanlar veya geçerli mazereti olmaksızın sınav hakkını kullanmayanlara, bir yıl içinde ikinci kez sınav hakkı verilir. İkinci sınavda başarı gösteremeyen veya sınav hakkını kullanmayanlar Defterdarlık Uzman Yardımcısı unvanını kaybederler ve durumlarına uygun memur unvanlı kadrolara atanırlar.

Bu madde kapsamında bulunan uzman ve uzman yardımcılara teftiş, denetim, inceleme ve soruşturma işlerine iliřkin görevlendirmelerinde, 10/2/1954 tarihli ve 6245 sayılı Harcırah Kanununun 33 üncü maddesinin (b) fıkrası hükmü uygulanır.

(Deęişik fıkra: 12/7/2013-6495/59 md.) Defterdarlık Uzmanı ve Defterdarlık Uzman Yardımcılarının mesleęe alınmaları, yarışma ve yeterlik sınavları, komisyonların oluşumu, yetiřtirilmeleri, atanmaları, eğitimleri, çalışma ve görevlendirilmelerine iliřkin usul ve esaslar ile dięer hususlar yönetmelikle düzenlenir.

(Ek fıkra: 12/7/2013-6495/59 md.) Bakanlık merkez teşkilatında daire başkanı, genel müdür yardımcısı ve başkan yardımcısı veya taşra teşkilatında defterdar kadrolarında toplam en az üç yıl görev yapmış olanlar, atama tarihi itibarıyla fiilen bu kadrolardan birinde bulunmak şartıyla Maliye Uzmanı kadrosuna atanabilir. "

7- 73. maddesinin (h) fıkrasının (1) numaralı bendiyle deęiřtirilen 663 sayılı KHK'nın dava konusu kuralları da içeren "Saęlık Meslekleri Kurulu" başlıklı23. maddesi şöyledir:

" (1) Saęlık mesleklerinde eğitim müfredatı, meslekî alan ve dal belirlemesi gibi meslekî düzenlemelerde ve istihdam planlamalarında görüş bildirmek, meslekî yeterlilik deęerlendirmesi

yapmak, meslekî müeyyide uygulamak, etik ilkeleri belirlemek ve uyumu denetlemek üzere Sağlık Meslekleri Kurulu teşkil olunmuştur.

(2) Kurul aşağıdaki üyelerden oluşur:

- a) Müsteşar veya görevlendireceği müsteşar yardımcısı ile Sağlık Hizmetleri Genel Müdürü veya görevlendireceği bir yetkili temsilci, I. Hukuk Müşaviri veya görevlendireceği hukuk müşaviri, Türkiye Halk Sağlığı Kurumu ve Türkiye Kamu Hastaneleri Kurumu Başkanları veya görevlendirecekleri yardımcıları,
- b) Bakanın seçeceği en az doktora seviyesinde eğitim almış 5 ayrı sağlık meslek mensubu üye,
- c) En az genel müdür yardımcısı seviyesinde Milli Eğitim Bakanlığı temsilcisi bir üye,
- ç) Yükseköğretim Kurulunun seçeceği iki üye,
- d) Meslekî Yeterlilik Kurumu temsilcisi bir üye,
- e) Kanunla kurulan sağlık meslek birliklerinden birer üye.

(3) Sağlık meslek birliklerinin temsilcileri yalnızca kendi meslek mensupları ile ilgili konuların görüşüleceği toplantılara katılabilir ve kendi meslek alanları ile ilgili konularda oy kullanır.

(4) Seçilmiş üyelerin görev süresi iki yıldır. Kurul toplantılarına üst üste iki kez mazeretsiz olarak katılmayanların üyeliği düşer. İlgili kurumlar bir ay içinde üyelerini seçerek Bakanlığa bildirmediği takdirde o dönem için ilgili kuruma ait üyelik düşer ve üye sayısında dikkate alınmaz.

(5) Kurul, Müsteşar veya müsteşar yardımcısının başkanlığında üye tam sayısının çoğunluğu ile toplanır ve oy çokluğu ile karar alır. Oylamalarda çekimser oy kullanılamaz. Oyların eşitliği hâlinde başkanın oyu yönünde karar alınmış sayılır.

(6) Kurulun görevleri şunlardır:

- a) Yeni bir sağlık mesleğinin veya dalının ihdasında görüş bildirmek.
- b) Sağlık mesleklerinin eğitim müfredatı hakkında görüş bildirmek.
- c) Sağlık mesleklerinin etik ilkelerini belirlemek.
- ç) Meslek mensuplarının meslekî yeterlilik ve etik eğitimi ile hasta hakları eğitimine tâbi tutulmasına ve eğitimlerin süresine ve müfredatına karar vermek.
- d) Sağlık engeli sebebiyle mesleğin icrasının yasaklanmasına karar vermek.
- e) Meslekten geçici veya sürekli men etmeye karar vermek.

(7) Meslekî yetersizliğe ilişkin ihbar ve şikâyetler Kurulca doğrudan değerlendirmeye alınmaz. Bu ihbar ve şikâyetler öncelikle denetim görevlileri veya il ve ilçe sağlık müdürlüklerince incelemeye tâbi tutulur. Yapılan inceleme neticesinde fiilin meslekî yeterlilik değerlendirmesi yapılması veya meslekî müeyyide uygulanması gerektirdiğinin tespit edilmesi hâlinde kanaat raporunu içeren inceleme dosyası Kurula gönderilir. Ayrıca fiil hakkında adlî kovuşturma yapılmış ise, verilen kararlar da Kurula intikal ettirilir. İdarî inceleme veya varsa adlî kovuşturma kapsamında elde edilen bilgi ve belgeler de değerlendirilerek, genel hükümler saklı kalmak üzere Kurulca;

a) Mesleğinde yetersizliği tespit edilenler ile dikkatsiz ve özensiz davranışla ölüme veya vücut fonksiyon kaybına sebep olanların yetersiz görüldükleri alanda meslekî yeterlilik eğitimine tâbi tutulmalarına karar verilir. Bu eğitim, yetersiz görülen alanda teorik ve/veya pratik eğitim ve/veya başka bir sağlık meslek mensubunun nezaret ve sorumluluğunda meslek icrası şeklinde yaptırılabilir. Yeterlilik eğitimine tâbi tutulanlar eğitim sonunda Kurulun belirleyeceği teorik ve/veya uygulamalı sınava tâbi tutulur. Bu sınavda başarılı olanlar mesleğini icraya devam eder; başarısız olanlar meslek icrasından men edilir. Meslekten men edilenler, durumlarına göre Kurulca belirlenen eğitime devam ettirilerek veya eğitime tâbi tutulmadan yapılacak müteakip sınavlarda başarı gösterdiği takdirde meslek icra etme hakkını yeniden kazanır.

b) Hasta hakları uygulamalarına veya etik ilkelere aykırı davranışı sebebiyle ikiden fazla yazılı ikaz edilen veya ilgili mevzuatına göre disiplin cezası uygulanan sağlık meslek mensubu, hasta hakları veya etik ilkeler eğitim programına tâbi tutulur.

c) (İptal: Anayasa Mahkemesi'nin 14/2/2013 tarihli ve E.: 2011/150, K. 2013/30 Sayılı Kararı ile.; Değişik: 12/7/2013-6495/73 md.) Meslek icrası esnasında sonucunu öngörerek veya görevinin gereklerine aykırı hareket ederek veyahut görevinin gereklerini yapmakta ihmal veya gecikme göstererek bir kişinin ağır derecede olmayan engelliliğine sebebiyet verenlerin üç aydan bir yıla kadar meslekten geçici men edilmesine karar verilir. Bu fiillerin beş yıl içinde tekrarı hâlinde verilecek cezalarda alt ve üst sınırlar iki katı olarak uygulanır.

ç) (İptal: Anayasa Mahkemesi'nin 14/2/2013 tarihli ve E.: 2011/150, K. 2013/30 Sayılı Kararı ile.; Değişik: 12/7/2013-6495/73 md.) Meslek icrası esnasında sonucunu öngörerek veya görevinin gereklerine aykırı hareket ederek veyahut görevinin gereklerini yapmakta ihmal veya gecikme göstererek bir kişinin ağır engelliliğine veya ölümüne sebebiyet verenlerin bir yıldan üç yıla kadar meslekten geçici menine karar verilir. Bu fiillerin beş yıl içinde tekrarı hâlinde meslekten sürekli men kararı verilir.

(8) Mesleğini icra etmesine mâni ve iyileşmesi mümkün olmayan aklî, ruhî ve bedenî hastalığı ortaya konulan sağlık meslek mensupları, Kurulun kararı ile mesleğini icradan yasaklanabilir.

(9) Meslekî yetersizliğinden dolayı bir uzmanlık dalında mesleğini icra edemeyeceğine karar verilen meslek mensuplarının yetersizliğinin niteliğine göre uzmanlık öncesi sahip olduğu sağlık mesleğini icra edebilmelerine karar verilebilir.

(10) Aynı olaydan dolayı ilgili hakkında ceza takibatına veya disiplin soruşturmasına başlanmış olması bu maddeye göre işlem yapılmasını geciktirmez ve engellemez; ilgilinin mahkûm olması veya olmaması ile disiplin cezası verilmiş veya verilmemiş olması hâlleri, ayrıca meslekî müeyyide uygulanmasını etkilemez.

(11) Kanunla kurulmuş meslek odalarının ve birliklerinin kuruluş kanunlarındaki disiplin hükümleri saklıdır. Ancak fiilin her iki kanuna göre de müeyyide gerektirmesi hâlinde bu Kanun hükümleri uygulanır.

(12) Meslekten geçici men edilmesine karar verilen Devlet memurları, men müddetince aylıksız izinli sayılır veya talepleri hâlinde aynı süreyle mesleği ile ilişkisi bulunmayan durumlarına uygun başka bir kadroya atanır. Sözleşmeli olanların sözleşmeleri men müddetince ücretsiz olarak askıya alınır. Meslekten sürekli men edilmesine karar verilen Devlet memurları istekleri hâlinde, mesleği ile ilişkisi bulunmayan durumlarına uygun başka bir kadroya atanır, aksi halde görevleri sona erer. Meslekten sürekli men edilmesine karar verilen sözleşmeli personelin sözleşmeleri sona erer.

(13) Bu maddeye göre mesleğini geçici olarak sürdüremeyeceklerin durumları kayıtlara işlenir. Meslekten sürekli men edilmesine karar verilenlerin veya mesleğini icra etmekten yasaklananların diplomaları, uzmanlık veya meslek belgeleri Bakanlıkça iptal edilir ve sistemden kaydı silinir.

(14) Bu maddenin uygulanmasına ilişkin usûl ve esaslar Bakanlık tarafından çıkarılacak yönetmelikle düzenlenir."

8- 73. maddesinin (h) fıkrasının (3) numaralı bendiyle değiştirilen 663 sayılı Kanun Hükmünde Kararname'nin dava konusu kuralları da içeren " Bilgi toplama, işleme ve paylaşma yetkisi " başlıklı 47. maddesi şöyledir:

"1) (Değişik: 12/7/2013-6495/73 md.) Bakanlık ve bağlı kuruluşları, mevzuatla kendilerine verilen görevleri, e-devlet uygulamalarına uygun olarak daha etkin ve daha hızlı biçimde yerine getirebilmek için, bütün kamu ve özel sağlık kurum ve kuruluşlarından; sağlık hizmeti alanların, aldıkları sağlık hizmetinin gereği olarak ilgili sağlık kurum ve kuruluşuna vermek zorunda oldukları kişisel bilgileri

ve bu kimselere verilen hizmete ilişkin bilgileri her türlü vasıta ile toplamaya, işlemeye ve paylaşmaya yetkilidir.

(2) (Değişik: 12/7/2013-6495/73 md.) Bakanlık ve bağlı kuruluşları işlediği kişisel sağlık verilerini ilgili üçüncü kişiler ve kamu kurum ve kuruluşları ile ancak bu kişi ve kurumların bu verilere erişebileceği hususunda kanunen yetkili olması hâlinde görevlerini yapmalarına yetecek derecede paylaşabilir.

(3) (Değişik: 12/7/2013-6495/73 md.) Bakanlık ve bağlı kuruluşları, mevzuatla kendilerine verilen görevleri yerine getirebilmek için gereken bilgileri, kamu ve özel ilgili bütün kişi ve kuruluşlardan istemeye yetkilidir. İlgili kişi ve kuruluşlar istenilen bilgileri vermekle yükümlüdür.

(4) Sağlık personeli istihdam eden kamu kurum ve kuruluşları ile özel hukuk tüzel kişileri ve gerçek kişiler, istihdam ettiği personeli ve personel hareketlerini Bakanlığa bildirmekle yükümlüdür.

(5) Bu maddenin uygulanmasına ilişkin hususlar Bakanlıkça çıkarılacak yönetmelikle düzenlenir."

9- 73. maddesinin (p) fıkrasının (1) numaralı bendiyle değiştirilen 3194 sayılı Kanun'un dava konusu kuralları da içeren " Planların hazırlanması ve yürürlüğe konulması" başlıklı 8. maddesi şöyledir:

" Planların hazırlanmasında ve yürürlüğe konulmasında aşağıda belirtilen esaslara uyulur.

a) Bölge planları; sosyo - ekonomik gelişme eğilimlerini, yerleşmelerin gelişme potansiyelini, sektörel hedefleri, faaliyetlerin ve alt yapıların dağılımını belirlemek üzere hazırlanacak bölge planlarını, gerekli gördüğü hallerde Devlet Planlama Teşkilatı yapar veya yaptırır.

b) İmar Planları; Nazım İmar Planı ve Uygulama İmar Planından meydana gelir. Mevcut ise bölge planı ve çevre düzeni plan kararlarına uygunluğu sağlanarak, belediye sınırları içinde kalan yerlerin nazım ve uygulama imar planları ilgili belediyelerce yapılır veya yaptırılır. Belediye meclisince onaylanarak yürürlüğe girer. (Yeniden düzenleme dördüncü cümle: 12/7/2013-6495/73 md.) Bu planlar onay tarihinden itibaren belediye başkanlığınca tespit edilen ilan yerlerinde ve ilgili idarelerin internet sayfalarında bir ay süreyle eş zamanlı olarak ilan edilir. Bir aylık ilan süresi içinde planlara itiraz edilebilir. Belediye başkanlığınca belediye meclisine gönderilen itirazlar ve planları belediye meclisi onbeş gün içinde inceleyerek kesin karara bağlar.

Belediye ve mücavir alan dışında kalan yerlerde yapılacak planlar valilik veya ilgisince yapılır veya yaptırılır. Valilikçe uygun görüldüğü takdirde onaylanarak yürürlüğe girer . (Yeniden düzenleme üçüncü cümle: 12/7/2013-6495/73 md.) Onay tarihinden itibaren valilikçe tespit edilen ilan yerinde ve ilgili idarelerin internet sayfalarında bir ay süreyle eş zamanlı olarak ilan edilir. Bir aylık ilan süresi

içinde planlara itiraz edilebilir. İtirazlar valiliğe yapılır, valilik itirazları ve planları onbeş gün içerisinde inceleyerek kesin karara bağlar.

Onaylanmış planlarda yapılacak değişiklikler de yukarıdaki usullere tabidir.

Kesinleşen imar planlarının bir kopyası, Bakanlığa gönderilir.

İmar planları alenidir. Bu aleniyeti sağlamak ilgili idarelerin görevidir. Belediye Başkanlığı ve mülki amirlikler, imar planının tamamını veya bir kısmını kopyalar veya kitapçıklar haline getirip çoğaltarak tespit edilecek ücret karşılığında isteyenlere verir.

c) (Ek: 3/7/2005 - 5403/25 md.) Tarım arazileri, Toprak Koruma ve Arazi Kullanımı Kanununda belirtilen izinler alınmadan tarımsal amaç dışında kullanılmak üzere plânlanamaz.

(Ek: 12/7/2013-6495/73 md.) Bakanlıkça belirlenen tanımlar ve esaslara göre hazırlanıp onaylanan halihazır haritalar, plan, plan değişikliği ve revizyonları, parselasyon planları, yapı ruhsatı ve yapı kullanma izin belgeleri ile imar mevzuatına konu edilen diğer coğrafi veri ve bilgilerin, ilgili idareler ile kurum ve kuruluşlarca; Bakanlar Kurulunca belirlenen usul ve esaslara uygun şekilde ve sayısal olarak; üretilmesi, elektronik ortamda ilan edilmesi, Bakanlıkça tesis edilecek elektronik ortam üzerinden paylaşılması, arşivlenmesi ve güncellenmesi zorunludur. Yapı ruhsatına ilişkin işlemlerde bu veriler esas alınır.

d) (Ek: 12/7/2013-6495/73 md.) Arazi kullanımı ve yapılaşmada sadece mekânsal strateji planları, çevre düzeni planları ve imar planları kararlarına uyulur. Üst kademe planları Bakanlıkça onaylanan bu Kanunun istisnası olan alanlar ile korumaya yönelik diğer özel kanunlara tabi alanlara ilişkin alt kademe planların onay, askı ve kesinleşme işlemleri bu Kanunun 9 uncu maddesine göre gerçekleştirilir. Alt kademe planların, üst kademe planların kesinleştiği tarihten itibaren en geç bir yıl içinde ilgili idarece üst kademe planlara uygun hale getirilmesi zorunludur. Aksi halde, üst kademe planları onaylayan kurum ve kuruluşlar alt kademe planları en geç altı ay içinde uygun hale getirir ve resen onaylar. Bu süre içinde ruhsat işlemleri, yürürlükte olan uygulama imar planına göre gerçekleştirilir. Bu bent uyarınca yapılacak işlemlerde bu maddenin (c) bendi hükümlerine uyulur.

e) (Ek: 12/7/2013-6495/73 md.) Kamu kurum ve kuruluşları veya plan müellifleri; ilgili kamu kurum ve kuruluşlarından plana ilişkin görüşlerini alır. Kurum ve kuruluşlar, görüşlerini en geç otuz gün içerisinde bildirmek zorundadır. Görüş bildirilmesi için etüt ve analiz gibi uzun süreli çalışma yapılması gereken hallerde ilgili kamu kurum ve kuruluşlarının talebi üzerine otuz günü geçmemek üzere ilave süre verilir. Bu süre içerisinde görüş bildirilmediği takdirde plan hakkında olumsuz bir görüşün bulunmadığı kabul edilir.

f) (Ek: 12/7/2013-6495/73 md.) Kentsel asgari standartlar, Bakanlıkça belirlenen esaslar doğrultusunda çevre düzeni planı ile belirlenebilir. Uygulamaya ilişkin kararlar, yörenin koşulları, parselin bulunduğu bölgenin genel özellikleri, yapının niteliği ve ihtiyacı, erişilebilirlik, sürdürülebilirlik, çevreye etkisi dikkate alınarak ve ölçüleri verilerek Bakanlıkça belirlenen esaslara göre uygulama imar planında belirlenir.

g) (Ek: 12/7/2013-6495/73 md.) Bakanlık; ilgili idareler, kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler tarafından yapılan mekansal planlamaya, harita ve parselasyona, etüt ve projelendirmeye, yapı ruhsatı ve yapı kullanma izni düzenlemeye, enerji kimlik belgesi hazırlanmasına ilişkin iş ve işlemler ile yapı malzemelerini; denetlemeye, aykırılıklar hakkında işlem tesis etmeye, aykırılıkları gidererek mevzuata uygun hale getirmeye yönelik değişiklik yapmaya ve onaylamaya, yapı tatil tutanağı tanzim etmeye, mühürlemeye, yıkım kararı almaya ve yıkımı gerçekleştirmeye, ilgililer hakkında idari yaptırım kararı vermeye yetkilidir. Bu görevlerden, yapı tatil tutanağı tanzim etmeye, mühürlemeye ve yıkım kararına ilişkin rapor düzenleme işi ile denetlemeye ilişkin görevler, Bakanlığın merkez ve taşra teşkilatında, denetçi belgesini haiz personel tarafından gerçekleştirilir. İlgililer Bakanlık denetçileri tarafından istenilen her türlü bilgi ve belgeyi, istenilen süre içerisinde vermek zorundadırlar. Bakanlık denetçilerinin seçimi, eğitimleri, görev, yetki ve sorumlulukları ile çalışma usul ve esasları Bakanlıkça belirlenir.

ğ) (Ek: 12/7/2013-6495/73 md.) Büyükşehir belediyesi sınırının il sınırı olması nedeniyle mahalleye dönüşen, nüfusu 5.000'in altında kalan ve kırsal yerleşim özelliği devam eden yerlerdeki uygulamalar, büyükşehir belediye meclisince aksine bir karar alınmadıkça, uygulama imar planı yapılıncaya kadar 27 nci madde hükümlerine göre yürütülür. Kırsal alanlarda iş yeri açma ve çalışma izni; kadimden kalan veya yapıldığı tarihteki mevzuat kapsamında yola cephesi olmaksızın inşa edilen yapılar ile köy yerleşik alanlarda kalan yapılara kırsal yapı belgesine, yerleşik alan sınırı dışındaki diğer yapılara ise yapı kullanma izin belgesine göre verilir. Köylerde bulunan konutlarda, iş yeri açma ve çalışma izni alınarak ev pansiyonculuğu yapılabilir. Kamuya ait bir yaya veya taşıt yoluna cephe sağlanmadan yapı inşa edilemez, parsel oluşturulamaz. Yerleşme ve yapılaşma özellikleri, mimari doku ve karakteri, gelişme düzey ve potansiyeli açısından önem arz eden köylerde bu özellikleri korumak, geliştirmek ve yaşatmak amacıyla muhtarlık katılımı ile ilgili idarelerce köy tasarım rehberleri hazırlanabilir. Köy tasarım rehberleri ilgili idare meclisi kararı ile onaylanır ve uygulanır.

h) (Ek: 12/7/2013-6495/73 md.) Köylerde ve kırsal özellik gösteren diğer yerleşmelerde yapıların etüt ve projeleri ilgili idarenin veya Bakanlığın taşra teşkilatının mimar ve mühendisleri tarafından

hazırlanabilir. Bakanlıkça; bu Kanun kapsamındaki yerleşmelere ilişkin enerji verimli, iklim duyarlı ve ekolojik özellikli plan ve projeler hazırlanabilir veya hazırlattırılabilir, bu nitelikli yapılar inşa edilebilir veya uzun vadeli kredilendirilmek suretiyle desteklenebilir.

ı) (Ek: 12/7/2013-6495/73 md.) Harita, plan, etüt ve projeler; idare ve ilgili kanunlarında açıkça belirtilen yetkili kuruluşlar dışında meslek odaları dahil başka bir kurum veya kuruluşun vize veya onayına tabi tutulamaz, tutulması istenemez. Vize veya onay yaptırılmaması ve benzeri nedenlerle müellifler veya bunlara ait kuruluşların büro tescilleri iptal edilemez veya yenilenmesi hiçbir şekilde geciktirilemez. Müelliflerden bu hükmü ortadan kaldıracak şekilde taahhütname talep edilemez.

ı) (Ek: 12/7/2013-6495/73 md.) İdarelerce onaylanmış; mevcut durumu gösteren halihazır haritalar, parselasyon planları ile teknik ve idari düzenlemeleri içeren bu Kanun kapsamındaki planların değişiklik ve revizyonlarında ilk müellifin görüşü veya izni aranmaz.

j) (Ek: 12/7/2013-6495/73 md.) İlgili idareler, Bakanlıkça belirlenen esaslara, göre mimari estetik komisyonu kurar. Komisyon, yapıların ve onaylı mimari projelerinin özgün fikir ifade edip etmediğine karar vermeye yetkilidir. Özgün fikir ifade etmeyenlerde yapılacak değişikliklerde ilk müellifin görüşü aranmaz. Özgün fikir ifade eden mimarlık eser ve projelerinde; eser sözleşmesinde işleme izni verilenler ile eserin bütünlüğünü bozmadığına, estetik görünümünü değiştirmedığıne, teknik, yönetsel amaçlar ve kullanım amacı nedeniyle zorunlu olduğuna karar verilen değişiklikler müellifinin izni alınmaksızın yapılabilir. Bu durumda ilk müellif tarafından talep edilebilecek telif ücreti; ilgili meslek odasının belirlenen mimari proje asgari hizmet bedelinin, tamamlanan yapılarda yüzde yirmisini, inşaatı süren yapılarda yüzde on beşini geçemez. "

10- 73. maddesinin (p) fıkrasının (3) numaralı bendiyle değiştirilen 3194 sayılı Kanun'un dava konusu ek 4. maddesi şöyledir:

" Mera, yaylak ve kırsal alanların geleneksel kullanım amacıyla geçici yerleşme yeri olarak uygun görülen kısımları valilikçe bu amaçla kurulacak bir komisyon tarafından tespit edilir. Bu yerlerin ot bedeli alınmaksızın tahsis amacı değiştirilerek tapuda Hazine adına tescilleri yapılır. Bu taşınmazlar, bu madde kapsamında kullanılmak ve değerlendirilmek üzere, belediye ve mücavir alan sınırları içinde kalanlar ilgili belediyelerine, diğer alanlarda kalanlar ise il özel idarelerine veya özel kanunlarla belirlenen ilgili idarelere tahsis edilir. Özel kanunlar kapsamı dışında kalan alanlarda belediyesince veya il özel idaresince geçici yerleşme alanının vaziyet planı ve yapılaşma şartları hazırlanır ve onaylanır. Bu taşınmazlardan kamu hizmetleri için gerekli olanların dışındakiler, il özel idaresince veya belediyesince ve özel kanunlarla belirlenmiş alanlarda ilgili idarece kadaströ verileri işlenmiş hâlihazır haritalar üzerine yapılmış vaziyet planına veya onaylı imar planına uygun olarak talep

sahiplerine bedeli karşılığında yirmi dokuz yıla kadar tahsis edilebilir. Bu yerlerde umumi ve kamusal yapılar hariç, inşa edilecek yapıların kat adedi bodrum hariç olmak üzere ikiyi, yapı inşaat alanı 200 metrekareyi geçemez. Bu yapıların yöresel mimariye uygun ve yöresel malzeme kullanılmak suretiyle yapılması zorunludur. Bu fıkranın uygulanmasına, bu fıkra kapsamında tahsis edilecek mera, yaylak ve kışlakların il genelindeki toplam mera, yaylak ve kışlakların binde beşini geçmemek üzere oranının belirlenmesine, bu yerlerin kiralanmak suretiyle tahsisine, tahsis sürelerine, yıllık kira bedeli taşınmazın emlak vergisine esas metrekare birim bedeli toplamının yüzde birinden az olmamak üzere tahsis bedellerinin belirlenmesine, tahsil edilen bedellerinin yarısı Hazine payı olarak genel bütçeye gelir kaydedilmek, diğer yarısı ise ilgili belediyeye veya il özel idaresine ait olmak üzere gelirlerin kullanım şekline, tahsis süresinin sona ermesine, komisyonun oluşumuna ve diğer konulara ilişkin esas ve usuller, İçişleri Bakanlığı, Maliye Bakanlığı, Gıda, Tarım ve Hayvancılık Bakanlığı, Orman ve Su İşleri Bakanlığı ile Kültür ve Turizm Bakanlığının uygun görüşleri alınarak Bakanlıkça hazırlanan yönetmelikle belirlenir.

Mera, yaylak ve kışlakların 2634 sayılı Kanun uyarınca ilan edilen turizm merkezleri ile kültür ve turizm gelişim bölgeleri kapsamında kalan kısımları, ot bedeli alınmaksızın tahsis amacı değiştirilerek tapuda Hazine adına tescil edilir ve bu yerler, 2634 sayılı Kanun çerçevesinde kullanılmak ve değerlendirilmek üzere Kültür ve Turizm Bakanlığına tahsis edilir. "

11- 73. maddesinin (r) fıkrasının (1), (2) ve (3) numaralı bentleriyle değiştirilen, 3224 sayılı Kanun'un dava konusu ibareleri de içeren 11., 26. ve 40. maddeleri şöyledir:

"Oda Yönetim Kurulunun görevleri

Madde 11- Oda Yönetim Kurulunun görevleri şunlardır:

- a) Oda Genel Kurulu gündemini hazırlayıp, Genel Kurulu toplantıya çağırmak,
- b) Odanın dönem bilançosu, faaliyet raporu ile tahmini bütçesini hazırlayıp Genel Kurula sunmak; bilanço ve faaliyetleri konusunda ibrasını istemek,
- c) Birlik ve Oda Genel Kurul kararlarını uygulamak,
- d) Dış Hekimliği ile ilgili mevzuatın ve meslek kurallarının gereği gibi uygulanmasına yardımcı olmak,
- e) Dış Hekimlerinin, hastalarla dış hekimleri arasında aracılık yapmayı meslek edinenlerle işbirliği yapmasını, Merkez Yönetim Kurulunca şekli belirlenmiş örneğe uymayan tabelaların kullanılmasını

ve her türlü araçla veya kişiyle reklam yapılmasını; meslektaşlar arasında gayrimeşru menfaat sağlanmasını önlemek,

f) (İptal ikinci fıkra: Anayasa Mahkemesi'nin 14/2/2013 tarihli ve E.: 2011/150, K.: 2013/30 sayılı Kararı ile.; Değişik: 12/7/2013-6495/73 md.) Faaliyet alanı içindeki muayene ve tedavi ücretlerine ilişkin rehber tarife teklifi hazırlayarak Birlik Merkez Yönetim Kuruluna göndermek,

g) Meslek mensuplarının birbirleriyle hastalarla veya hasta sahipleri arasında çıkacak ihtilafları uzlaştırmaya veya hakem usulüne başvurarak çözüme kavuşturmaya çalışmak,

h) Meslek mensuplarının daha yüksek bir mesleki kültür düzeyine ulaşabilmeleri için gerekli teşebbüslerde bulunmak,

i) Meslek mensuplarını bölgeleri içinde meslekleriyle ilgili sağlık sorunları üzerinde inceleme ve araştırma yapmaya teşvik ederek bunlardan çıkan sonuçları ilgili kurum ve kuruluşlara iletme,

j) Dış hekimliği mesleğinin onurunu, genel hak ve menfaatlerini ilgili merciler nezdinde savunmak,

k) İhtiyaca göre, faaliyet alanı içindeki il veya ilçelerde yönetmelikle gösterilecek esaslar dairesinde faaliyette bulunmak üzere temsilcilikler kurulmasına karar vermek,

l) Oda üyeleri hakkında, disiplin cezası uygulamasını gerektiren veya suç teşkil eden fiillerinin öğrenilmesi halinde inceleme yaparak sonucu Disiplin Kuruluna tevdi etmek,

m) Üyelerin meslek kayıtlarını tutmak; onur üyeliği için Birlik Merkez Yönetim Kuruluna öneride bulunmak,

n) Hastaların resmi tatil günlerinde ve mesai saatleri dışında da meslek hizmetlerinden yararlanabilmeleri için meslek mensuplarıyla işbirliği yapmak,

o) Gelirleri noter tasdikli makbuz mukabili toplamak ve harcamaları belgeye dayalı olarak yaparak gelir ve harcamaları noter tasdikli defterlere işlemek,

p) Oda adına taşınır ve taşınmaz mal almak, satmak, ipotek etmek ve bunlar üzerinde her türlü aynı hak tesis etmek, kaldırmak gibi konularda Oda Başkanına veya bir Yönetim Kurulu üyesine yetki vermek,

r) Oda Genel Kurul toplantı tutanaklarının bir örneğini Birlik Merkez Yönetim Kuruluna göndermek,

s) Bu Kanun ve diğer mevzuatla verilen görevleri yerine getirmek.

(.)

Birlik Merkez Yönetim Kurulunun görevleri

Madde 26- Birlik Merkez Yönetim Kurulunun görevleri şunlardır:

- a) Birlik Genel Kurulunun gündemini hazırlayıp Genel Kurulu toplantıya çağırmak,
- b) Birliğin dönem bilançosunu, faaliyet raporu ile tahmini bütçesini hazırlayıp Birlik Genel Kuruluna sunmak; bilanço ve faaliyetleri konusunda ibrasını istemek,
- c) Birlik Genel Kurul kararlarını uygulamak,
- d) Kanuna, tüzük ve yönetmeliklere uymayan Odaları uyarmak, gerekirse sorumluları Yüksek Disiplin Kuruluna sevk etmek,
- e) (İptal ikinci fıkra: Anayasa Mahkemesi'nin 14/2/2013 tarihli ve E.: 2011/150, K.: 2013/30 sayılı Kararı ile.; Değişik: 12/7/2013-6495/73 md.) Odaların faaliyet alanı içindeki muayene ve tedavi ücretlerine ilişkin rehber tarife tekliflerini tasdik etmek,
- f) Diş hekimlerinin kullanacakları tabela örneğini tespit etmek, bu örneğe uymayan tabelaların kullanımını ve Tıbbi Deontoloji Tüzüğüne aykırı ilan ve reklam yapılmasını önlemek,
- g) Birlik adına taşınır ve taşınmaz mal almak, satmak, ipotek etmek ve bunlar üzerinde her türlü ayni hak tesis etmek, kaldırmak; bu konularda Genel Başkan veya bir Merkez Yönetim Kurulu üyesine yetki vermek,
- h) Bu Kanunun uygulanmasına esas olacak tüzük ve yönetmelikleri çıkarmak için gerekli faaliyetlerde bulunmak,
- i) Bu Kanun ve diğer mevzuatla verilen görevleri yerine getirmek.

(.)

Rehber tarife belirlenmesi

Madde 40- (İptal ikinci fıkra: Anayasa Mahkemesi'nin 14/2/2013 tarihli ve E.: 2011/150, K.: 2013/30 sayılı Kararı ile.; Değişik: 12/7/2013-6495/73 md.)

Oda Yönetim Kurulları her yıl aralık ayı içinde, diş hekimlerinin uygulayacakları muayene ve tedavi ücretlerine ilişkin bir rehber tarife hazırlayarak Birlik Merkez Yönetim Kuruluna gönderirler.

Birlik Merkez Yönetim Kurulu, rehber tarife tekliflerini aynen veya gerekli gördüğü değişiklikleri yaparak tasdik eder ve bu tarifeleri Sağlık Bakanlığına bildirir. "

12- 73. maddesinin (bb) fıkrasıyla değiştirilen 6004 sayılı Kanun'un dava konusu kuralları da içeren "Yurtdışı teşkilatında unvanlar ve görev süreleri" başlıklı 12. maddesi şöyledir:

" (1) Bakanlık memurlarının merkez teşkilatından yurtdışı teşkilatına, yurtdışı teşkilatındaki bir temsilcilikten diğer bir temsilciliğe ve yurtdışı teşkilatından merkez teşkilatına sürekli görevle atanmalarında, 23/4/1981 tarihli ve 2451 sayılı Bakanlıklar ve Bağlı Kuruluşlarda Atama Usulüne İlişkin Kanunda belirtilen usuller uygulanır. Bakanlığın yurtdışı teşkilatında görevli meslek memurları ile konsolosluk ve ihtisas memurları, ekli (3) ve (4) sayılı listelerde sayılan unvanları, temsil görevinin diplomatik veya konsüler niteliğine göre, aşağıdaki fıkralarda belirtilen esaslar çerçevesinde taşırlar.

(2) Büyükelçi unvanına ilişkin esaslar şunlardır:

a) Büyükelçi, nezdinde görevli bulunduğu ve akredite edildiği ülkelerde Türkiye Cumhuriyeti Devletini, Cumhurbaşkanı ve Hükümeti temsil eder.

b) Büyükelçi, görev yaptığı ülkede büyükelçiliğe bağlı tüm birimlerin amiridir.

c) Büyükelçiliğe hiyerarşik olarak bağlı bulunmamakla birlikte, diğer kamu kurum ve kuruluşlarının yurtdışındaki temsilcileri veya birimleri de yürüttükleri faaliyetler bağlamında büyükelçinin gözetimine tabi olup, bu faaliyetler hakkında büyükelçiyi bilgilendirir.

ç) Meslek memurlarınının 14 üncü maddenin beşinci fıkrasına göre belirlenen dış temsilcilik gruplandırması gözetilmeksizin büyükelçi olarak atanabilmeleri için, merkez teşkilatında elçi veya yurtdışı teşkilatında elçi, elçi-müsteşar, elçi-daimi temsilci yardımcısı ve birinci sınıf başkonsolos unvanlarından biriyle, başarılı şekilde en az bir yıl görev yapmış olmaları gerekir. Bu unvanları henüz almamış birinci unvan grubundaki meslek memurları ile ikinci ve üçüncü derece kadrodaki meslek memurları dış temsilcilik gruplandırmasında sondaki üç grupta yer alan temsilciliklere büyükelçi olarak atanabilir.

d) (Değişik: 12/7/2013-6495/73 md.) 657 sayılı Kanunun 59 uncu maddesi çerçevesinde büyükelçi olarak atananlardan Bakanlığa veya diğer kamu kurum ve kuruluşlarına mensup olanlar ile açıktan atananlar, merkeze döndüklerinde, Bakanlıkta çalışabilirler, Bakanlıktaki görevleri süresince büyükelçi unvanını kullanmaya devam ederler ve Bakanlıkta yönetici kadrolarına atanma dâhil meslek mensubu olanlar arasından büyükelçiliğe atananlarla aynı hükümlere tâbi olur ve aynı haklardan yararlanırlar.

(3) Daimi temsilci unvanına ilişkin esaslar şunlardır:

a) Daimi temsilci, bir uluslararası kuruluşta Türkiye Cumhuriyeti Hükümetini temsil etmek üzere atanan memurdur. Meslek memurlarınının daimi temsilci olarak atanma şartları, büyükelçi olarak atanma şartları ile aynıdır. Daimi temsilci, aynı zamanda büyükelçi unvanını da taşır. Bunlardan

meslek memuru olanlar, merkez görevine döndüklerinde büyükelçi unvanını kullanmaya devam eder. (Ek cümle: 12/7/2013-6495/73 md.) 657 sayılı Kanununun 59 uncu maddesi çerçevesinde daimi temsilci olarak atananlardan Bakanlığa veya diğer kamu kurum ve kuruluşlarına mensup olanlar ile açıktan atananlar, merkeze döndüklerinde, Bakanlıkta çalışabilirler, Bakanlıktaki görevleri süresince büyükelçi unvanını kullanmaya devam ederler ve Bakanlıkta yönetici kadrolarına atanma dâhil meslek mensubu olanlar arasından büyükelçiliğe atananlarla aynı hükümlere tâbi olur ve aynı haklardan yararlanırlar.

b) Bakanlığın gerekli görmesi halinde, Birleşmiş Milletler Nezdinde Türkiye Daimi Temsilciliğine, büyükelçi-daimi temsilcinin yanı sıra, meslek memuru statüsündeki bir büyükelçi, büyükelçi-daimi temsilci yardımcısı unvanıyla atanabilir.

c) Nezdinde daimi temsilcilik açılmamış bulunan milletlerarası kuruluşlarda meslek memurlarına temsilcilik görevi verilebilir.

(4) Özel temsilci unvanına ilişkin esaslar şunlardır:

a) Özel temsilci, dış politika gereklilikleri çerçevesinde özel bir görevi ifa etmek üzere görevlendirilen, büyükelçi veya elçi unvanını taşıyan temsilcilerdir. Büyükelçi veya elçi unvanı taşımayanlar da geçici bazı görevler için özel temsilci sıfatıyla görevlendirilebilir.

b) Özel temsilciler Bakanlar Kurulu kararı ile görevlendirilir.

(5) Maslahatgüzar ve geçici maslahatgüzar unvanlarına ilişkin esaslar şunlardır:

a) Bir ülkedeki siyasi temsil düzeyi büyükelçi veya elçi seviyesinde değilse birinci, ikinci ve üçüncü unvan grubundaki meslek memurları arasından o ülke nezdinde görev yapmak üzere maslahatgüzar atanabilir.

b) Misyon şefinin geçici olarak yokluğunda, geçici maslahatgüzarlık görevinin temsilcilikteki hangi memur tarafından üstlenileceği yönetmelikle belirlenir.

c) Maslahatgüzar veya geçici maslahatgüzar, görevli oldukları ülkede diplomatik misyon şefinin tüm yetki ve sorumluluklarına sahiptir.

(6) Elçi-müsteşar, elçi-daimi temsilci yardımcısı ve daimi temsilci yardımcısı unvanlarına ilişkin esaslar şunlardır:

a) Elçi-müsteşar ve elçi-daimi temsilci yardımcısı unvanları, büyükelçiliklerde ve daimi temsilciliklerde misyon şefinden sonra öndegelim sırasındaki birinci meslek memuru tarafından taşınabilir. Birinci unvan grubundaki meslek memurları Bakanlık Komisyonunun teklifi ve Bakan

onayı üzerine, ilgili mevzuat hükümlerine göre elçi-müsteşar veya elçi-daimi temsilci yardımcısı olarak atanabilir. Büyükelçiliklerde ve daimi temsilciliklerde birinci müsteşar olarak görev yapmakta olan veya bu unvanla atanmış ancak fiilen göreve başlamamış bulunan birinci unvan grubundaki meslek memurlarına da Bakanlık Komisyonunun teklifi ve Bakan onayı ile elçi-müsteşar veya elçi-daimi temsilci yardımcısı unvanı verilebilir.

b) Elçi unvanı taşımayacak daimi temsilci yardımcılarını da birinci unvan grubundaki meslek memurları arasında Bakanlık Komisyonunun teklifi ve Bakan onayı ile belirlenir.

c) Dış politika gereklerine göre, elçi-müsteşar ve elçi-daimi temsilci yardımcısı atanabilecek büyükelçilikler ve daimi temsilcilikler, Bakanlık Komisyonunun teklifi ve Bakan onayı ile belirlenir. Bu unvanlar merkez teşkilatında kullanılmaz. Daha önce bu unvanları almış olanlar, ancak elçi-müsteşar veya elçi-daimi temsilci yardımcısı atanması mümkün olan diplomatik temsilciliklerde yeniden görevlendirildikleri ve bu temsilciliklerde söz konusu unvanları taşıyan başka bir meslek memuru bulunmadığı takdirde bu unvanları kullanabilir.

(7) Birinci sınıf başkonsolos ve başkonsolos unvanlarına ilişkin esaslar şunlardır:

a) Birinci sınıf başkonsolos veya başkonsolos, başkonsoloslukların en üst amiridir. Meslek memurlarının yanı sıra konsolosluk ve ihtisas memurları da başkonsolos olarak atanabilir. Birinci derece kadrodaki meslek memurları, Bakanlık Komisyonunun teklifi ve Bakan onayı üzerine, ilgili mevzuat hükümlerine göre birinci sınıf başkonsolos olarak atanabilir. Başkonsolos olarak görev yapmakta olan veya bu unvanla atanmış ancak fiilen göreve başlamamış bulunan birinci unvan grubundaki meslek memurlarına da Bakanlık Komisyonunun teklifi ve Bakan onayı ile birinci sınıf başkonsolos unvanı verilebilir.

b) Daha önce büyükelçilik yapmış meslek memurları ile merkez teşkilatında elçi veya yurtdışı teşkilatında elçi-müsteşar ya da elçi-daimi temsilci yardımcısı unvanıyla görev yapmış olan meslek memurları, konsolosluk şefi olarak atandıklarında birinci sınıf başkonsolos unvanını taşır. Büyükelçi unvanını daha önce kazanmış olanlar, büyükelçi unvanlarını da muhafaza eder.

(8) Ekli (1) ve (2) sayılı listeler çerçevesinde, meslek memurları ile konsolosluk ve ihtisas memurlarınca diplomatik temsilciliklerde kullanılacak diğer unvanlar, birinci müsteşar, müsteşar, başkatip, ikinci katip, üçüncü katip ve ataşe; konsolosluk temsilciliklerinde kullanılacak diğer unvanlar ise başkonsolos yardımcısı, konsolos, muavin konsolos ve ataşedir.

(9) Büyükelçi unvanı taşımayan meslek memurları ve büyükelçi unvanını da koruyan birinci sınıf başkonsoloslar ile konsolosluk ve ihtisas memurlarının, hukuk müşavirlerinin ve danışmanların

görev süreleri, hizmetin gerektirdiği istisnalar dışında, yurtdışı teşkilatında en çok beş yıl, merkez teşkilatında en az iki yıldır.

(10) Aday memurlar yurtdışına sürekli görevle atanamaz.

(11) Meslek memurları ile konsolosluk ve ihtisas memurları merkez teşkilatından yurtdışı teşkilatına veya yurtdışı teşkilatından merkez teşkilatına, sahip buldukları kadro dereceleriyle ve buldukları unvan grubuyla atanır.

(12) Uzman müşavirlerin görev süresi, hizmetin gerektirdiği istisnalar dışında en çok dört yıldır. Yurtdışı görevleri sona eren uzman müşavirler, Bakanlık ile ilişkileri kesilerek daha önceden bağlı buldukları kamu kurum veya kuruluşundaki kadrolarına iade edilir. Uzman müşavirler, diplomatik temsilciliklerde müşavir veya müşavir yardımcısı; konsolosluklarda ataşe veya ataşe yardımcısı unvanlarını taşır. "

13- 73. maddesinin (cc) fıkrasıyla değiştirilen, 6085 sayılı Kanun'un dava konusu ibareleri de içeren "Denetim alanı" başlıklı 4. maddesi şöyledir:

" (1) Sayıştay;

a) (Değişik: 12/7/2013-6495/73 md.) Merkezi yönetim bütçesi kapsamındaki kamu idareleri ile sosyal güvenlik kurumlarını, mahallî idareleri, sermayesindeki kamu payı doğrudan veya dolaylı olarak %50'den fazla olan özel kanunlar ile kurulmuş anonim ortaklıkları, diğer kamu idarelerini (kamu kurumu niteliğindeki meslek kuruluşları hariç),

b) (Değişik: 12/7/2013-6495/73 md.) Kamu payı %50'den az olmamak kaydıyla (a) bendinde sayılan idarelere bağlı veya bu idarelerin kurdukları veya doğrudan doğruya ya da dolaylı olarak ortak oldukları her çeşit idare, kuruluş, müessese, birlik, işletme ve şirketleri,

c) Kamu idareleri tarafından yapılan her türlü iç ve dış borçlanma, borç verilmesi, borç geri ödemeleri, yurt dışından alınan hibelerin kullanımı, hibe verilmesi, Hazine garantileri, Hazine alacakları, nakit yönetimi ve bunlarla ilgili diğer hususları; tüm kaynak aktarımları ve kullanımları ile Avrupa Birliği fonları dahil yurt içi ve yurt dışından sağlanan diğer kaynakların ve fonların kullanımını,

ç) Kamu idareleri bütçelerinde yer alıp almadığına bakılmaksızın özel hesaplar dahil tüm kamu hesapları, fonları, kaynakları ve faaliyetlerini,

denetler.

(2) Sayıştay; yapılan andlaşma veya sözleşmedeki esaslar çerçevesinde uluslararası kuruluş ve örgütlerin hesap ve işlemlerini de denetler.

(3) 2/4/1987 tarihli ve 3346 sayılı Kamu İktisadi Teşebbüsleri ile Fonların Türkiye Büyük Millet Meclisince Denetlenmesinin Düzenlenmesi Hakkında Kanununun 2 nci maddesi kapsamına giren kamu kurum, kuruluş ve ortaklıklarının Türkiye Büyük Millet Meclisince denetlenmesi, bu Kanun ve diğer kanunlarda belirtilen usul ve esaslar çerçevesinde yerine getirilir ."

II- İLK İNCELEME

A- 2013/114 Sayılı İptal Davası Yönünden

1. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca, Haşim KILIÇ, Serruh KALELİ, Alparslan ALTAN, Mehmet ERTEN, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT, Zehra Ayla PERKTAŞ, Recep KÖMÜRCÜ, Burhan ÜSTÜN, Engin YILDIRIM, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Erdal TERCAN, Muammer TOPAL, Zühtü ARSLAN ve M. Emin KUZ'un katılımlarıyla 28.11.2013 tarihinde yapılan ilk inceleme toplantısında öncelikle dava konusu kuralların bazılarına yönelik olarak iptal davasının açılmış sayılıp sayılmayacağı sorunu görüşülmüştür.

2. 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 38. maddesinin (6) numaralı fıkrasında, " İptal davalarında, Anayasaya aykırılıkları ileri sürülen hükümlerin Anayasanın hangi maddelerine aykırı olduğunun ve gerekçelerinin belirtilmiş olması zorunludur. " kuralına yer verilmiş, Anayasa Mahkemesi İçtüzüğü'nün 45. maddesinde ise " Anayasaya aykırılıkları ileri sürülen hükümlerin her birinin Anayasanın hangi maddelerine, hangi nedenlerle aykırı olduğunun ayrı ayrı ve gerekçeleriyle birlikte açıkça gösterilmesi " iptal davası başvuru dilekçesinde yer alması gereken hususlar arasında sayılmıştır.

3. 6216 sayılı Kanun'un 39. maddesi ile İçtüzüğü'nün 49. maddesinde, dava dilekçesinde eksikliklerin bulunması hâlinde, bu hususun kararla saptanarak onbeş günden az olmamak üzere verilecek süre içinde tamamlanması için ilgililere tebliğ olunacağı ve belirtilen süre içinde eksikliklerin tamamlanmaması hâlinde Genel Kurulca iptal davasının açılmamış sayılmasına karar verileceği hükme bağlanmıştır.

4. Dava dilekçesinde, iptali istenen kuralların bir kısmına yönelik olarak Anayasa'ya aykırılık gerekçelerine yer verilmediği anlaşıldığından, 6216 sayılı Kanun'un 39. maddesinin (1) numaralı fıkrası ile İçtüzüğü'nün 49. maddesi uyarınca Sinop Milletvekili Engin ALTAY ile Yalova Milletvekili Muharrem İNCE'ye bildirimde bulunulmasına ve söz konusu eksikliklerin giderilmesi için kararın tebliğinden başlayarak 15 (onbeş) gün süre verilmesine karar verilmiştir. İlgililer tarafından, kararda belirlenen süre içinde 13.11.2013 tarihinde verilen dilekçede, dava dilekçesinde iptali istenilen ancak

Anayasa'ya aykırılık gerekçesine yer verilmeyen hükümlerden 6495 sayılı Kanun'un 73. maddesinin (p) fıkrasının (1) numaralı bendiyle, 3194 sayılı Kanun'un 8. maddesine eklenen (j) bendinin dördüncü cümlesinde yer alan ". eser sözleşmesinde işleme izni verilenler ile. " ibaresi ve son cümlesi yönünden saptanan gerekçe eksikliği giderilmiştir. Ancak 6495 sayılı Kanun'un 43. maddesiyle, 22.6.2006 tarihli ve 5525 sayılı Memurlar ile Diğer Kamu Görevlilerinin Bazı Disiplin Cezalarının Affı Hakkında Kanun'a eklenen ek 1. maddenin birinci fıkrasının ". 28/8/1999 tarihli ve 4455 sayılı Memurlar İle Diğer Kamu Görevlilerinin Disiplin Cezalarının Affı Hakkında Kanun veya bu Kanun hükümlerinden yararlanmış olanların; " bölümünün dava dilekçesine sehven yazıldığı ve bu hükümlerin iptali yönünde herhangi bir taleplerinin bulunmadığı belirtilmiş ve böylece bu konudaki eksiklik giderilmemiş olduğundan, söz konusu bölüme yönelik iptal davasının açılmamış sayılmasına karar vermek gerekmiştir.

5. Açıklanan nedenlerle, 12.7.2013 tarihli ve 6495 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un;

A- 43. maddesiyle, 22.6.2006 tarihli ve 5525 sayılı Memurlar ile Diğer Kamu Görevlilerinin Bazı Disiplin Cezalarının Affı Hakkında Kanun'a eklenen ek 1. maddenin birinci fıkrasının ". 28/8/1999 tarihli ve 4455 sayılı Memurlar İle Diğer Kamu Görevlilerinin Disiplin Cezalarının Affı Hakkında Kanun veya bu Kanun hükümlerinden yararlanmış olanların;" bölümüne yönelik iptal davasının, 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 39. maddesinin (3) numaralı fıkrası uyarınca AÇILMAMIŞ SAYILMASINA,

B- 1- 26. maddesiyle değiştirilen, 4.11.1983 tarihli ve 2942 sayılı Kamulaştırma Kanunu'nun 22. maddesinin birinci fıkrasının son iki cümlesinin,

2- 27. maddesiyle 2942 sayılı Kanun'un 25. maddesine eklenen fıkranın,

3- 28. maddesiyle 2942 sayılı Kanun'a eklenen geçici 8. maddenin,

4- 33. maddesiyle, 9.10.2003 tarihli ve 4982 sayılı Bilgi Edinme Hakkı Kanunu'nun 2. maddesine eklenen fıkranın,

5- 43. maddesiyle 5525 sayılı Kanun'a eklenen ek 1. maddenin;

a- Birinci fıkrasında yer alan "28/2/1997 tarihinden sonra." ibaresinin,

b - İkinci fıkrasının ".1/1/1990 ile..657 sayılı Kanununun 125 inci maddesinin birinci fıkrasının (A) bendinin (g) alt bendinde yer alan fiili işlediği gerekçesiyle anılan Kanununun 56 ve 57 nci maddeleri uyarınca disiplin cezası veya olumsuz sicil almış olmaları nedeniyle." bölümünün,

6- 59. maddesiyle, 13.12.1983 tarihli ve 178 sayılı Maliye Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 43. maddesine eklenen fıkranın,

7- 73. maddesinin;

a- (h) fıkrasının;

aa- (1) numaralı bendiyle değiştirilen, 11.10.2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 23. maddesinin yedinci fıkrasının (c) ve (ç) bentlerinin,

ab- (3) numaralı bendiyle değiştirilen 663 sayılı Kanun Hükmünde Kararname'nin 47. maddesinin (1), (2) ve (3) numaralı fıkralarının,

b- (p) fıkrasının;

ba- (1) numaralı bendiyle, 3.5.1985 tarihli ve 3194 sayılı İmar Kanunu'nun 8. maddesine eklenen (ı), (i) ve (j) bentlerinin,

bb- (3) numaralı bendiyle değiştirilen 3194 sayılı Kanun'un ek 4. maddesinin,

c- (r) fıkrasının;

ca- (1) numaralı bendiyle değiştirilen, 7.6.1985 tarihli ve 3224 sayılı Türk Dış Hekimleri Birliği Kanunu'nun 11. maddesinin birinci fıkrasının (f) bendinde yer alan ".rehber ." ibaresinin,

cb- (2) numaralı bendiyle değiştirilen 3224 sayılı Kanun'un 26. maddesinin birinci fıkrasının (e) bendinde yer alan ".rehber." ibaresinin,

cc- (3) numaralı bendiyle değiştirilen 3224 sayılı Kanun'un 40. maddesinin başlığında yer alan "Rehber." ibaresi ile birinci ve ikinci fıkralarında yer alan ".rehber." ibarelerinin,

d- (bb) fıkrasıyla, 7.7.2010 tarihli ve 6004 sayılı Dışişleri Bakanlığının Kuruluş ve Görevleri Hakkında Kanun'un 12. maddesinin;

da- (2) numaralı fıkrasının değiştirilen (d) bendinin,

db- (3) numaralı fıkrasının (a) bendine eklenen cümlelerin,

e- (cc) fıkrasıyla değiştirilen, 3.12.2010 tarihli ve 6085 sayılı Sayıştay Kanunu'nun 4. maddesinin (1) numaralı fıkrasının;

ea- (a) bendinde yer alan ".% 50'den fazla olan." ibaresinin,

eb- (b) bendinde yer alan "Kamu payı % 50'den az olmamak kaydıyla." ibaresinin,

dosyada eksiklik bulunmadığından esasının incelenmesine, yürürlüklerinin durdurulması isteminin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

B- 2014/134 Sayılı İtiraz Başvurusu Yönünden

6. Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca, Haşim KILIÇ, Serruh KALELİ, Alparslan ALTAN, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ, Engin YILDIRIM, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Erdal TERCAN, Muammer TOPAL, Zühtü ARSLAN, M. Emin KUZ ve Hasan Tahsin GÖKCAN'ın katılımlarıyla 23.7.2014 tarihinde yapılan ilk inceleme toplantısında, dosyada eksiklik bulunmadığından işin esasının incelenmesine OYBİRLİĞİYLE karar verilmiştir.

III- BİRLEŞTİRME KARARI

7. 22.6.2006 tarihli ve 5525 sayılı Memurlar ile Diğer Kamu Görevlilerinin Bazı Disiplin Cezalarının Affı Hakkında Kanun'a, 12.7.2013 tarihli ve 6495 sayılı Kanun'un 43. maddesiyle eklenen ek 1. maddenin ikinci fıkrasında yer alan ". 125 inci maddesinin birinci fıkrasının (A) bendinin (g) alt bendinde yer alan fiili işlediği gerekçesiyle ." ibaresinin iptaline karar verilmesi istemiyle yapılan itiraz başvurusuna ilişkin davanın, aralarındaki hukuki irtibat nedeniyle E.2013/114 sayılı dava ile BİRLEŞTİRİLMESİNE, E.2014/134 sayılı dosyanın esasının kapatılmasına, esas incelemenin E.2013/114 sayılı dosya üzerinden yürütülmesine, 23.7.2014 tarihinde OYBİRLİĞİYLE karar verilmiştir.

IV- ESASIN İNCELENMESİ

8. Dava ve ek dava dilekçeleri, başvuru kararı ile ekleri, Raportör Hamit YELKEN tarafından hazırlanan işin esasına ilişkin rapor, dava ve itiraz konusu kanun hükümleri, dayanılan ve ilgili görülen Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A- Kanun'un 26. Maddesiyle Değiştirilen 2942 Sayılı Kanun'un 22. Maddesinin Birinci Fıkrasının Üçüncü ve Dördüncü Cümlelerinin (Son İki Cümlesinin) İncelenmesi

9. 10.9.2014 tarihli ve 6552 sayılı İş Kanunu ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması ile Bazı Alacakların Yeniden Yapılandırılmasına Dair Kanun'un 100. maddesinin birinci fıkrasının (a) bendiyle, 2942 sayılı Kanun'un 22. maddesinin birinci fıkrasının dava konusu üçüncü cümlesi değiştirilmiş, dördüncü cümlesi ise yürürlükten kaldırılmıştır.

10. Bu nedenlerle konusu kalmayan bu cümlelere ilişkin iptal talepleri hakkında karar verilmesine yer olmadığına karar vermek gerekir.

B- Kanun'un 27. Maddesiyle 2942 Sayılı Kanun'un 25. Maddesine Eklenen Fıkranın İncelenmesi

1- İptal Talebine İlişkin Gerekçe

11. Dava dilekçesinde özetle, dava konusu kuralla bazı büyük projelerde taşınmazların kamulaştırılmasına ilişkin kamu yararı kararının ilanından itibaren bu taşınmazlar üzerinde beş yıl süreyle yapılacak sabit tesislerin ve dikilecek ağaçların kamulaştırma bedelinin tespitinde dikkate alınmayacağına düzenlendiği, bunun kamulaştırmanın gerçek karşılığı üzerinden yapılmasını önlediği ve mülkiyet hakkından kaynaklanan tasarruf yetkisini Anayasa'nın sözüne, ruhuna ve demokratik toplum düzeninin gereklerine aykırı şekilde ölçsüzce sınırlandırdığı, kuralla konu kamu yararı kararının ve bunun ilan şeklinin belirsizlik içerdiği ayrıca kamulaştırma sürecinde bir hazırlık işlemi olan, dolayısıyla icrai niteliği bulunmayan, hatta dava konusu dahi yapılamayan bir idari işlemin, hukuken yoklukla malul bir suretle ilan edilmesi öngörülerek mülkiyet hakkına sınırlamalar getirilmesinin demokratik hukuk devleti ilkesi ile de bağdaşmadığı belirtilerek kuralın, Anayasa'nın 2., 13., 35. ve 46. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

12. Anayasa'nın 2. maddesinde, Türkiye Cumhuriyeti'nin bir hukuk devleti olduğu belirtilmiştir. Hukuk devleti, eylem ve işlemleri hukuka uygun olan, insan haklarına saygılı, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adil bir hukuk düzeni kurup bunu geliştirerek sürdüren, Anayasa'ya aykırı durum ve tutumlardan kaçınan, hukukun üstün kurallarıyla kendini bağlı sayan ve yargı denetimine açık olan devlettir.

13. Anayasa'nın 35. maddesinin birinci fıkrasında, "Herkes, mülkiyet ve miras haklarına sahiptir." denilmek suretiyle temel hak ve özgürlükler arasında yer alan mülkiyet hakkı güvence altına alınmıştır. Maddenin ikinci ve üçüncü fıkralarında ise bu hakkın, kamu yararı amacıyla ve kanunla sınırlandırılabilmesi ve mülkiyet hakkının kullanımının toplum yararına aykırı olamayacağı belirtilerek bu hakkın mutlak olmadığı ve kamu yararı amacıyla sınırlandırılabilmesi kabul edilmiştir. Ancak mülkiyet hakkının sınırlandırılabilmesi için kamu yararının varlığı yeterli olmayıp temel hak ve özgürlüklerin sınırlandırılması rejimini belirleyen Anayasa'nın 13. maddesine de uyulması gerekmektedir. Anayasa'nın 13. maddesi uyarınca mülkiyet hakkı, Anayasa'nın 35. maddesinde belirtilen kamu yararı amacına bağlı olarak yalnızca kanunla ve demokratik bir toplumda gerekli olduğu ölçüde sınırlandırılabilir. Ayrıca getirilen bu sınırlamalar, hakkın özüne

dokunamayacağı gibi Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamaz.

14. Anayasal açıdan dokunulamayacak öz, her temel hak ve özgürlük açısından farklılık göstermekle birlikte kanunla getirilen sınırlamanın hakkın özüne dokunmadığının kabulü için temel hakların kullanılmasını ciddi surette güçleştirip, amacına ulaşmasına engel olmaması ve etkisini ortadan kaldıracı bir nitelik taşımaması gerekir. Ancak bu durumda sınırlamanın demokratik toplum düzeninin gereklerine uygun olduğu söylenebilir.

15. Ölçülülük ise amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder. Ölçülülük, aynı zamanda yasal önlemin sınırlama amacına ulaşmaya elverişli olmasını, amaç ve aracın ölçülü bir oranı kapsamasını ve sınırlayıcı önlemin demokratik toplum düzeni bakımından zorunluluk taşımasını da içeren bir ilkedir.

16. Anayasa'nın 46. maddesi uyarınca, Devlet ve kamu tüzel kişileri ancak kamu yararının gerektirdiği hallerde, gerçek karşılıklarını peşin ödemek şartıyla ve kanunla gösterilen esas ve usullere uymak suretiyle kamulaştırma yetkisine sahip bulunmaktadır.

17. Dava konusu kuralla baraj, sulama şebekeleri, boru hatları, karayolu, demiryolu, liman ve havaalanı gibi uzun yıllar süren büyük projelerde, taşınmazların kamulaştırılmasına ilişkin kamu yararı kararının ilanından sonra kamulaştırılacak taşınmazlar üzerine yapılan sabit tesisler ile dikilen ağaçların bedelinin kamulaştırma bedelinin tespitinde dikkate alınmayacağı belirtilerek mülkiyet hakkına bir sınırlama getirilmiştir. Kanun'un gerekçesinde bu sınırlamanın nedeni açıklanmış ve bunun baraj rezervuarları gibi kamulaştırma işlemlerinin uzun süre devam ettiği durumlarda kötü niyetli kişiler tarafından herhangi bir amaca hizmet etmeyen ve sırf kamulaştırma bedeli almak için yapılan sabit eserlerin inşa edilmesini önlemeye yönelik olduğu belirtilmiştir.

18. Büyük kamulaştırma projeleri kapsamında kısa süre sonra ortadan kalkacağı aşikâr olan (örneğin baraj suları altında kalacak) yerlere sabit tesisler yapılmasının, ülke kaynaklarının israf edilmesi ve idarenin haksız yere yüksek bedelle kamulaştırma yapması sonucunu doğurarak kamuyu zarara uğratacağı açık olduğundan hiçbir hukuk düzeninin bu nevi kötü niyetli davranışları koruması beklenemez.

19. Bu çerçevede kuralla mülkiyet hakkına bir sınırlama getirilmekteyse de bu sınırlamanın, kamunun haksız yere zarara uğratılmasının önlenmesi amacıyla, dolayısıyla Anayasa'nın 35. maddesinde belirtilen özel sınırlama nedenine bağlı kalınarak yapıldığı anlaşılmaktadır.

20. Kuralla kamulaştırılması planlanan tüm taşınmazlar üzerinde inşa edilecek sabit tesisler yönünden değil, sadece uzun yıllar süren büyük projelerde kamu yararı kararı alınan taşınmazlar üzerine belli bir süre içerisinde inşa edilecek sabit tesisler yönünden bir sınırlama getirildiğinden, bunun mülkiyet hakkının kullanımını ciddi surette güçleştirip amacına ulaşmasına engel olmadığı, dolayısıyla hakkın özüne zarar vermediği de ortadadır.

21. Kuralla sırf daha yüksek kamulaştırma bedeli almak amacıyla hiçbir amaca hizmet etmeyen tesislerin yapılmasının, dolayısıyla ülke kaynaklarının israf edilerek idarenin haksız yere yüksek bedelle kamulaştırma yaparak zarara uğratılmasının önlenmesi amacıyla mülkiyet hakkına bir sınırlama getirilmekte olup bu sınırlama, kamu yararının sağlanması amacıyla demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır.

22. Bu şekilde, demokratik toplum düzeni bakımından alınması gerekli tedbirler kapsamında bireylerin mülkiyet hakkı sınırlandırılırken, bu sınırlamanın, ancak uzun yıllar süren büyük projelerde kamu yararı kararı alınan taşınmazlar üzerine inşa edilecek sabit tesisler yönünden geçerli olacağı ve bu sınırlamanın her halükarda taşınmazın kamulaştırılmasına ilişkin kamu yararı kararının ilan tarihinin bitiminden itibaren beş yıllık süreyi geçmemesi şartlarına bağlanmış olması, sınırlama aracının sınırlama amacına uygun ve orantılı şekilde kullanılmasını amaçlamakta ve böylece kamunun zarara uğramasının önlenmesi şeklindeki kamu yararı ile kişilerin mülkiyet hakkı arasındaki makul denge kurulmuş olmaktadır.

23. Kanun'da ayrıca, kurala konu uygulamaya karşı yargı yolu da açık tutulmuş, böylece idarenin sınırlama aracını sınırlama amacına ve Kanun'a aykırı şekilde keyfi olarak kullanmasının önüne geçecek güvence de sağlanmıştır.

24. Bu yönleriyle kuralla mülkiyet hakkına getirilen sınırlamanın, hakkın özünü zedelediğinden sözü edilemeyeceği gibi bunun demokratik toplum düzeninin ve hukuk devletinin gereklerine ve ölçülülük ilkesine aykırı düştüğü de söylenemez.

25. Öte yandan, hukuk devletinin temel ilkelerinden biri de "belirlilik"tir. Bu ilkeye göre, yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi de gerekir. Belirlilik ilkesi, hukuksal güvenlikle bağlantılı olup birey, kanundan, belirli bir kesinlik içinde, hangi somut eylem ve olguya hangi hukuksal sonucun bağlandığını bilmelidir. Birey ancak bu durumda kendisine düşen yükümlülükleri öngörebilir ve davranışlarını ayarlayabilir. Hukuk güvenliği, normların öngörülebilir olmasını,

bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar.

26. Dava konusu kuralla kamunun haksız yere zarara uğratılmasının önlenmesi amacıyla mülkiyet hakkına bir sınırlama getirilmekte olup kuralda bu sınırlamanın konusu, kapsamı ve hangi şartlarda uygulanacağı, dolayısıyla hangi somut eyleme hangi hukuksal sonucun bağlandığı herhangi bir kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel şekilde açıklanmıştır.

27. Kuralda sınırlamanın başlangıç tarihinin kamu yararı kararının ilan süresinin bitiminden itibaren başlatılması ve bu kararın, taşınmazın bulunduğu yerin mahalle ve/veya köy muhtarlığında on beş gün süre ile asılmak suretiyle ilan edilmesi de işin esasına uygun olup bunun taşınmaz maliklerinin söz konusu sınırlamadan etkin ve yeterli şekilde haberdar olmasını önleyeceği söylenemez. Zira baraj, sulama şebekeleri, boru hatları, karayolu, demiryolu, liman ve havaalanı gibi büyük projelere ilişkin kamulaştırma işlemlerinin yürütüldüğü yerlerde taşınmazı bulunan ve bunlar üzerinde sabit tesis yatırımı yapmayı düşünen kişilerin buralarda kamulaştırma yapılacağını öğrenmemiş olmaları beklenemez.

28. Esasen, kuralda sınırlamanın kamu yararı kararının ilan süresinin bitiminden itibaren başlatılması, herkes için aynı anda başlayan ve aynı anda biten objektif tarihlerin belirlenmesi ihtiyacından kaynaklanmakta olup bunun yerine kişilere tek tek tebligat yapılması usulünün benimsenmesinin, tebligatın farklı kişilere farklı tarihlerde ulaşacak olması nedeniyle sınırlamanın kişilere göre değişen tarihlerde başlaması sonucunu doğurabileceği anlaşılmaktadır.

29. Bu yönleriyle kuralla benimsenen ilan usulü, herhangi bir belirsizlik içermemekte ve bu usulün hukuk devleti ilkesini zedeleyen bir yönü de bulunmamaktadır.

30. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2., 13., 35. ve 46. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

C- Kanun'un 28. Maddesiyle 2942 Sayılı Kanun'a Eklenen Geçici 8. Maddenin İncelenmesi

31. Dava konusu kuralda, 6495 sayılı Kanun'un 26. maddesiyle değiştirilen 2942 sayılı Kanun'un 22. maddesinin birinci fıkrasının son cümlesine atıfta bulunularak buradaki hükmün, maddenin yürürlüğe girdiği tarihten önce gerçekleştirilen kamulaştırma işlemleri nedeniyle açılan ve henüz kesinleşmeyen taşınmazların geri alınması, bedel veya tazminat davaları yönünden de uygulanacağı düzenlemesine yer verilmiştir.

32. Dava konusu kuralla atıfta bulunulan 22. maddenin birinci fıkrasının son cümlesi, 6552 sayılı Kanun'un 100. maddesinin birinci fıkrasının (a) bendiyle yürürlükten kaldırılmış ve bu hükmün yürürlükten kaldırılmasıyla dava konusu geçici 8. maddenin de uygulanma kabiliyeti kalmamıştır.

33. Açıklanan nedenle, uygulanma imkânı kalmayan bu maddeye ilişkin iptal talebi hakkında karar verilmesine yer olmadığına karar vermek gerekir.

Ç- Kanun'un 33. Maddesiyle 4982 Sayılı Kanun'un 2. Maddesine Eklenen Fıkranın İncelenmesi

1- İptal Talebine İlişkin Gerekçe

34. Dava dilekçesinde özetle, ÖSYM tarafından uygulanan sınavlara ait soru ve cevapların kamunun erişimine açık olmasında, sınavların şaibelerden uzak olması ile ölçme ve değerlendirmenin nesnellüğünün sağlanması bakımından zorunluluk bulunduğu, dava konusu kuralla bu sınavlara ait soru ve cevapların 4982 sayılı Bilgi Edinme Hakkı Kanunu kapsamı dışına çıkarılmasının, hak arama hürriyeti ve bilgi edinme haklarını, anayasal bir gerekçeye dayanmadan ve uygulanabilirliği olmayacak şekilde nedensiz, tutarsız ve ölçüsüzce sınırlandığı ve demokratik toplum düzeniyle bağdaşmayacak derecede anılan hakların özünü ortadan kaldırdığı, ayrıca bu durumun uluslararası sözleşme hükümleriyle de çeliştiği belirtilerek kuralın, Anayasanın 2., 13., 36., 74. ve 90. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

35. Anayasa'nın "Hak arama hürriyeti" başlıklı 36. maddesinde, herkesin gerekli araç ve yollardan yararlanarak yargı organları önünde davacı ya da davalı olarak iddia ve savunma hakkının bulunduğu belirtilmektedir. Maddeyle güvence altına alınan dava yoluyla hak arama özgürlüğü, kendisi bir temel hak niteliği taşımasının ötesinde, diğer temel hak ve özgürlüklerden gereken şekilde yararlanılmasını ve bunların korunmasını sağlayan en etkili güvencelerden biridir.

36. Anayasa'nın "Dilekçe, bilgi edinme ve kamu denetçisine başvurma hakkı" başlıklı 74. maddesinin dördüncü fıkrasında ise " Herkes, bilgi edinme ve kamu denetçisine başvurma hakkına sahiptir. " denilmek suretiyle bilgi edinme hakkı anayasal güvenceye kavuşturulmuştur.

37. Bilgi edinme hakkı, yönetilenlerin yönetenleri denetleyebilmesinin, dolayısıyla hukukun üstünlüğünün sağlanabilmesinin çok önemli bir aracı olarak işlev görmektedir. Bilgi edinme hakkı, devletin demokratik niteliğinin geliştirilmesi ve bireyin temel hak ve özgürlüklerinin korunması hususlarında önemli bir rol oynadığından, demokratik hukuk devletinde vazgeçilmez bir hak niteliğine sahip bulunmaktadır. Bu hakkın sınırlandırılmasını öngören düzenlemelerin de Anayasa'nın

13. maddesinde belirtilen güvencelere ve bu bağlamda ölçülülük ilkesine uygun olması gerektiği açıktır.

38. Dava konusu kuralla Anayasa'nın 74. maddesinde güvence altına alınan bilgi edinme hakkına bir sınırlama getirilmekte ve ÖSYM tarafından uygulanan sınavlara ait soru ve cevaplara ilişkin bilgi edinme imkânı ortadan kaldırılmaktadır. Yasama belgelerinden ve ÖSYM'nin dosyaya sunduğu yazı içeriğinden, bu düzenlemenin Kurumun soru havuzu oluşturma ve daha önce sorduğu soruları yeniden sorabilme olanağına sahip olabilmesi amacıyla yapıldığı anlaşılmaktadır. Anılan yazıda, sınava giren kişilere sorulan konuların aynı olduğu ve aynı konulara ilişkin sürekli yeni sorular oluşturmanın zor olduğu, bunun zaman içinde sınava giren kişilerin bilgilerini ölçmeye yaramayan soruların sorulmasına neden olduğu, dolayısıyla daha önce sorulan soru ve cevapların kişilere verilmeksizin yeniden sorulabilmesi amacıyla söz konusu düzenlemenin yapıldığı ifade edilmektedir.

39. Konular değişmediği hâlde sürekli yeni sorular oluşturmanın zor olduğu, bu yönüyle soruların ölçme kalitesini düşürmemek amacıyla yeniden sorulmasını sağlamakta kamu yararı bulunduğu açıktır. Ancak yapılan sınavlara ilişkin olarak kişilerin bilgi sahibi olması da son derece önemli olup kişilerin bu soru ve cevapların doğru olarak tespit edilip edilmediğini öğrenme ve buna göre yanlış olarak belirlenen soru ve cevaplara karşı hak arama özgürlüğünü kullanabilmesinde de ciddi bir kamu yararı bulunmaktadır. Zira kişilerin eğitim veya iş hayatı bakımından geleceklerini belirleyen bu sınavların, doğru olarak uygulanıp uygulanmadığını denetleyebilmeleri ve buna ilişkin hak arama özgürlüklerini kullanabilmeleri için anılan soru ve cevaplara erişebilmeleri gerekmektedir.

40. Öte yandan, çeşitli tedbirler alınarak veya yöntemler kullanılarak, sorulacak soruların ölçme kalitesini düşürmemek veya kamuoyunun bilgisine sunulmuş, dolayısıyla tüm adayların eşit şekilde bilgi sahibi olduğu soruların bir kısmının veya benzerlerinin yıllar içinde yeniden sorulması mümkün bulunmaktayken anılan hakların sınırlandırılması yönteminin tercih edilmesi, kurala konu sınırlamanın demokratik bir hukuk devletinde alınması gerekli zorunlu tedbirler kapsamında kalmadığını göstermektedir.

41. Bu yönleriyle dava konusu kuralda ulaşılmak istenen kamu yararı ile bilgi edinme hakkı ve hak arama özgürlüğü arasındaki makul dengenin kurulamadığı ve kurala konu sınırlayıcı önlemin zorunlu bir toplumsal ihtiyaçtan kaynaklanmadığı, dolayısıyla kuralın bilgi edinme hakkının ve hak arama özgürlüğünün ölçüsüzce sınırlandırılmasına neden olduğu anlaşılmaktadır.

42. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2., 13., 36. ve 74. maddelerine aykırıdır. İptali gerekir.

43. Engin YILDIRIM, Celal Mümtaz AKINCI ve Muammer TOPAL bu görüşe katılmamışlardır.

44. Kuralın Anayasa'nın 90. maddesiyle ilgisi görülmemiştir.

D- Kanun'un 43. Maddesiyle 5525 Sayılı Kanun'a Eklenen Ek 1. Maddenin Birinci Fıkrasında Yer Alan "28/2/1997 tarihinden sonra." İbaresiyile, İkinci Fıkrasının ". 1/1/1990 ile...657 sayılı Kanunun 125 inci maddesinin birinci fıkrasının (A) bendinin (g) alt bendinde yer alan fiili işlediği gerekçesiyle anılan Kanunun 56 ve 57 nci maddeleri uyarınca disiplin cezası veya olumsuz sicil almış olmaları nedeniyle. " İbarelerinin İncelenmesi

1- İptal Talebine İlişkin Gerekçeler

45. Dava dilekçesinde özetle, dava konusu kurallarla daha önce aldıkları disiplin cezaları nedeniyle memuriyetten uzaklaştırılan kişilerin yeniden memuriyete alınmalarının sağlandığı, ancak bu düzenleme yapılırken tüm memurların değil, sadece 28.2.1997 tarihinden sonra aldıkları disiplin cezaları nedeniyle memuriyetle ilişkisi kesilen memurlar ile kılık kıyafet kurallarına aykırılık nedeniyle 1.1.1990 tarihinden sonra görevine son verilen aday memurların memuriyete dönüşlerinin sağlandığı, halbuki Türkiye'de konuya ilişkin mağduriyetlerin anılan tarihlerden itibaren başlamadığı, bu tarihlerden önce de birçok memurun farklı fiillerinden dolayı aldıkları disiplin cezaları nedeniyle memuriyetine son verildiği, bunun aynı durumda olan kişiler arasında keyfi olarak farklı uygulamalar yapılması sonucunu doğurduğu, bu farklı muamele ve keyfi uygulamanın adalet ve hakkaniyet ölçüleriyle bağdaşmadığı, ayrıca bu düzenlemelerin uluslararası sözleşme hükümleriyle de çeliştiği belirtilerek kuralların, Anayasa'nın 2., 10. ve 90. maddelerine aykırı olduğu ileri sürülmüştür.

46. Trabzon İdare Mahkemesinin başvuru kararında ise özetle, 6495 sayılı Kanun'un 43. maddesiyle 5525 sayılı Kanun'a eklenen ek 1. maddenin ikinci fıkrasında yer alan ". 125 inci maddesinin birinci fıkrasının (A) bendinin (g) alt bendinde yer alan fiili işlediği gerekçesiyle ." ibaresinin, sadece kılık kıyafet nedeniyle mesleğine son verilen aday memurların mesleğine dönmesine imkân tanıdığı, bunun anlaşılabilir ve adil bir düzenleme olmadığı, benzer durumda bulunan kişilere de bu imkânın tanınması gerektiği belirtilerek kuralın, Anayasa'nın 2. ve 10. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

47. Kanun'un 43. maddesiyle 5525 sayılı Kanun'a eklenen ek 1. maddenin dava konusu ibareleri de içeren birinci fıkrasında, 28.2.1997 tarihinden sonra verilen disiplin cezaları nedeniyle memuriyet görevine son verilenlerin yeniden göreve alınmalarının esasları düzenlenmektedir.

48. Buna göre, 28.2.1997 tarihinden sonra verilen herhangi bir disiplin cezası nedeniyle memuriyetten çıkarılanlardan 28.8.1999 tarihli ve 4455 sayılı Memurlar İle Diğer Kamu Görevlilerinin Disiplin Cezalarının Affı Hakkında Kanun veya 5525 sayılı Kanun hükümlerinden yararlanarak disiplin cezaları affedilen kişilerin; memuriyete giriş şartlarını kaybetmemiş olmaları, durumlarına uygun boş kadro veya pozisyon bulunması, bu kadro ve pozisyonlara ait nitelikleri taşımaları, üç ay içinde müracaat etmeleri kaydıyla yeniden göreve alınmalarında, 20.12.2012 tarihli ve 6363 sayılı 2013 Yılı Merkezi Yönetim Bütçe Kanununun eki (İ) Cetvelinde yer alan atama sayısı sınırlaması uygulanmayacaktır.

49. Ek 1. maddenin dava ve itiraz konusu ibareleri de içeren ikinci fıkrasında ise 657 sayılı Devlet Memurları Kanunu'na tabi aday memur statüsünde görev yapmakta iken 1.1.1990 ile bu maddenin yürürlüğe girdiği 2.8.2013 tarihleri arasında 657 sayılı Kanun'un 125. maddesinin birinci fıkrasının (A) bendinin (g) alt bendinde yer alan kılık ve kıyafet hükümlerine aykırı davranma fiilini işlediği gerekçesiyle anılan Kanun'un 56. ve 57. maddeleri uyarınca disiplin cezası veya olumsuz sicil almış olmaları nedeniyle memurlukla ilişkisi kesilip asli memurluğa atanamayanların, bu maddenin yürürlüğe girdiği tarihten itibaren üç ay içinde eski kurumlarına müracaat etmeleri hâlinde, 657 sayılı Kanunun 48. maddesinde belirtilen genel şartları taşımaları koşuluyla kurumlarında daha önce işgal ettikleri aynı veya benzer unvanlı kadrolara iki ay içinde atanacakları düzenlenmektedir.

50. Kaynağını Anayasa'nın 7. maddesinden alan yasama yetkisinin genelliği ilkesi uyarınca, kanun koyucu Anayasa'ya aykırı olmamak kaydıyla dilediği konuda düzenleme yapma yetkisine sahiptir. Kanun koyucunun kamu yararını gerçekleştirmek amacıyla çözümlenmesi gereken bir sorun olarak gördüğü konuları bir tarih belirleyerek çözüme kavuşturması da takdir yetkisi kapsamında kalmakta olup bu çerçevede belli bir tarihten sonra işlenmiş disiplin cezaları nedeniyle memuriyetlerine son verilen memurlar ile kılık kıyafet hükümlerine aykırı davranma fiili nedeniyle görevine son verilen aday memurların yeniden memuriyete dönüşlerini düzenleyen kurallar belirlemesinde, hukuk devleti ilkesine aykırı düşen bir yön bulunmamaktadır.

51. Öte yandan, Anayasa Mahkemesi, Anayasa'ya aykırı bulduğu kuralları iptal ederek yürürlükten kalkmasını sağlar. Kanun koyucu gibi davranarak yeni bir uygulamaya yol açacak biçimde hüküm kuramaz. Anayasa'nın öngördüğü ve mutlak düzenlenmesini istediği hususlara yer vermeme durumu dışında, kanun koyucunun isterse getirebileceği bir kuralı getirmemesi, iptal nedeni olamaz. İsterse yer verip isterse yer vermeyeceği bu tür hususlar kanun koyucunun takdir yetkisi içindedir. Anayasa'nın öngördüğü, düzenlenmesini zorunlu kıldığı bir konu, aykırılık nedeni sayılarak iptal

nedeni yapılmakla birlikte, kanun koyucunun anayasal ilkelere aykırı düşmeyen bir düzenlemeyi aynı veya benzer durumdaki kişiler yönünden öngörmemesi, iptal nedeni olarak kabul edilemez.

52. Dava dilekçesinde ve itiraz başvurusunda disiplin cezaları nedeniyle memuriyetlerine son verilen memurlar ile kılık kıyafet hükümlerine aykırı davranma fiili nedeniyle görevine son verilen aday memurların yeniden memuriyete dönüşlerinin düzenlenmesinin iptali istenmemekte, bu imkânın sadece belli bir tarihten sonra ve yine sadece kılık kıyafet hükümlerine aykırı davranma fiili nedeniyle memuriyetine son verilenler yönünden tanınmasının, Anayasa'ya aykırı olduğu ileri sürülmektedir. Dolayısıyla dilekçede ve kararda düzenlemedeki bazı ibarelerin iptali istenerek kuralın uygulama alanının genişletilmesi ve bu imkândan yararlanmayan kişilere de aynı avantajın sağlanması talep edilmektedir.

53. Dava ve itiraz konusu kurallarla kanun koyucunun isterse düzenleme yapabileceği bir alana ilişkin olarak anayasal ilkelere aykırı düşmeyen bir imkân getirilmekte olup bu yapılırken belli bir tarihin veya belli bir disiplin suçunun esas alınması kanun koyucunun takdirinde kalmaktadır.

54. Açıklanan nedenlerle dava ve itiraz konusu kurallar, Anayasa'nın 2. ve 10. maddelerine aykırı değildir. İptal taleplerinin reddi gerekir.

55. Kuralların, Anayasa'nın 90. maddesiyle ilgisi görülmemiştir.

E- Kanun'un 59. Maddesiyle, 178 Sayılı KHK'nin 43. Maddesine Eklenen Fıkranın İncelenmesi

1- İptal Talebine İlişkin Gerekçe

56. Dava dilekçesinde özetle, dava konusu kuralla Maliye Bakanlığı bünyesinde çalışan daire başkanı, genel müdür yardımcısı, başkan yardımcısı ve defterdarların daha düşük statüde bir görev olan maliye uzmanı kadrosuna atanabilmesine imkân tanındığı, bu durumun, anılan nitelikte görev yapan kişilerin görev güvencelerinin sağlanamaması, kazanılmış haklarının ihlal edilmesi ve meşru beklentilerinin karşılanamamasına neden olduğu, bunun ise hukuki güvenlik ilkesine aykırı olduğu, düzenlemenin amacının kamu yararı olmayıp siyasi iradenin ideolojisine ters düşenlerin daha alt statüdeki görevlere atanması olduğu, ayrıca kuralda bu görevlerde bulunanların tümünün değil, bir kısmının atanacağı belirtilmesinin eşitlik ilkesiyle bağdaşmadığı ve idari işlemle yapılacak tasarrufun kanunla yapılarak kişilerin bu işlemlere karşı yargı mercilerine başvurmalarının önlenmediği belirtilerek dava konusu kuralların, Anayasa'nın 2., 10., 36. ve 70. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

57. Anayasa'nın 2. maddesinde yer alan hukuk devleti ilkesinin temel gereklerinden biri de kazanılmış haklara saygı gösterilmesidir. Kazanılmış haklara saygı, hukuk güvenliği ilkesinin bir sonucudur. Kazanılmış hak, kişinin bulunduğu statüden doğan, tahakkuk etmiş ve kendisi yönünden kesinleşmiş, kişisel alacak niteliğine dönüşmüş haktır.

58. Hukuk güvenliği ilkesi aynı zamanda hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar. Kanunlara güvenerek hayatını yönlendiren, hukuki iş ve işlemlere girişen bireyin, bu kanunların uygulanmasına devam edileceği yolunda oluşan beklentisinin mümkün olduğunca korunması hukuki güvenlik ilkesinin gereğidir.

59. Dava konusu kurala Maliye Bakanlığının merkez teşkilatında daire başkanı, genel müdür yardımcısı, başkan yardımcısı veya taşra teşkilatında defterdar kadrolarında toplam en az üç yıl görev yapmış olanların, atama tarihi itibarıyla fiilen bu kadrolardan birinde bulunmak şartıyla maliye uzmanı kadrosuna atanabileceği düzenlenmektedir.

60. Daire başkanlığı, genel müdür yardımcılığı, başkan yardımcılığı ve defterdarlık kadrolarının vergi müfettişliği, maliye uzmanlığı gibi kariyer mesleklerden gelenler ve idari görevlerden yükselerek gelenler olmak üzere iki ayrı kaynağı bulunmaktadır. Kariyer meslek kaynağından gelen kişilerin kendi kadrolarına eşit veya daha düşük statüdeki maliye uzmanlığı kadrosuna atanabilmeleri için kuralda belirtilen koşullara tabi tutulmayacakları açıktır. Dolayısıyla dava konusu kural, anılan koşullar aranmaksızın zaten maliye uzmanlığına atanma imkânına sahip kariyer meslek kaynağından gelenleri değil, sadece önceki görevi ve kadrosu itibarıyla maliye uzmanlığına atanma imkânına sahip bulunmayan kişileri kapsamaktadır.

61. Daire başkanlığı, genel müdür yardımcılığı, başkan yardımcılığı ve defterdarlık kadroları idarecilik (yöneticilik) kadroları olup idarenin bu kadrolara bir kere atadığı kişileri meslek hayatları boyunca bu kadrolarda çalıştırma zorunluluğunun bulunmayacağı açıktır. Dolayısıyla bu kadrolara atanan kişiler yönünden, buldukları statülerden doğan, tahakkuk etmiş, kendileri yönünden kesinleşmiş ve kişisel alacak niteliğine dönüşmüş haklardan yahut bu durumun devam edeceği yönündeki haklı beklentiden söz edilemez. Bu nedenle, kamu yararı ve hizmetin gerekleri dikkate alınarak bu kişilerin idarecilik görevlerine son verilmesi ve kariyer meslek kadrolarından gelenlerin kendi kadrolarına, kariyer mesleklerden gelmeyenlerin ise bazı koşulları taşımak kaydıyla geldiği kadrodan daha üst bir görev olan maliye uzmanı kadrolarına atanmaları mümkün olup bunu düzenleyen kuralın kazanılmış hakları veya genel olarak hukuk güvenliği ilkesini ihlal eden bir yönü bulunmamaktadır.

62. Öte yandan, Anayasa'nın 2. maddesindeki "hukuk devleti" ilkesi gereğince, yasama işlemlerinin kişisel yararları değil, kamu yararını gerçekleştirmek amacıyla yapılması zorunludur. Bir kuralın Anayasa'ya aykırılık sorunu çözümlenirken "kamu yararı" konusunda Anayasa Mahkemesinin yapacağı inceleme, yalnızca kanunun kamu yararı amacıyla yapılıp yapılmadığı ile sınırlıdır. Kanun ile kamu yararının ne kadar gerçekleşip gerçekleşmeyeceğini denetlemenin ise anayasa yargısıyla bağdaşmayacağı ve bunun kanun koyucunun takdirinde olduğu açıktır.

63. Kanun koyucu, kamu yararı ve hizmetin gereklerini dikkate alarak kamu görevlilerinin statüsünde, bunların unvanlarında, görev ve yetkilerinde olduğu gibi bu statülere atanma koşullarında da değişiklikler yapabilir. Dava konusu düzenlemeyle kariyer meslek kaynağından gelmeyen ve maliye uzmanlığına atanma imkânına sahip olmayanlardan hizmetine ihtiyaç duyulanların, kuralda belirtilen üst düzey görevleri belli bir süre ifa etmeleri şartıyla kariyer meslek olan maliye uzmanlığına atanabilmelerinin sağlanmak istendiği ve düzenlemenin bu amaçla çıkarıldığı anlaşılmaktadır. Bu amacın kamu yararına yönelik olmadığı söylenemez. Dava konusu kuralla anılan kadrolardaki kişilerin maliye uzmanı olarak atanabilmesine imkân tanınmasıyla kamu yararının gerçekleşip gerçekleşmeyeceği ise anayasallık denetiminin kapsamı dışındadır.

64. Anayasa'nın 10. maddesinde yer verilen eşitlik ilkesi ise hukuksal durumları aynı olanlar için söz konusudur. Bu ilke ile eylemli değil, hukuksal eşitlik öngörülmüştür. Eşitlik ilkesinin amacı, aynı durumda bulunan kişilerin kanunlar karşısında aynı işleme bağlı tutulmalarını sağlamak, ayırım yapılmasını ve ayrıcalık tanınmasını önlemektir. Bu ilkeyle, aynı durumda bulunan kimi kişi ve topluluklara ayrı kurallar uygulanarak kanun karşısında eşitliğin ihlali yasaklanmıştır. Kanun önünde eşitlik, herkesin her yönden aynı kurallara bağlı tutulacağı anlamına gelmez. Durumlarındaki özellikler, kimi kişiler ya da topluluklar için değişik kuralları ve uygulamaları gerektirebilir. Aynı hukuksal durumlar aynı, ayrı hukuksal durumlar farklı kurallara bağlı tutulursa Anayasa'da öngörülen eşitlik ilkesi zedelenmez.

65. Dava konusu kuralda Maliye Bakanlığının merkez teşkilatında daire başkanı, genel müdür yardımcısı ve başkan yardımcısı veya taşra teşkilatında defterdar kadrolarında çalışanların tümünün değil, kuralda belirtilen şartları taşıyanların maliye uzmanı olarak atanabilmesine imkân tanınmaktadır. İdare hukukunun genel ilkeleri uyarınca idarenin bu yetkisini kullanırken kuralda belirtilen şartları taşıyanlar yönünden de kamu hizmetinin daha iyi işlemesi veya kamu yararı esasına göre ayırım yaparak atama yapmak zorunda olduğu aşikârdır. Kamu hizmetinin daha iyi işlemesi veya kamu yararı amacıyla atama yapabilmesi için ise söz konusu kadrolarda çalışanların başarısı, liyakati gibi çeşitli ayırt edici kriterlerin kullanılması gerekir. Bu kriterleri taşıyan kişilerle

taşımayanların aynı hukuki durumda bulunmadığında kuşku olmadığına göre dava konusu kural uyarınca bunlar arasında ayırım yapılarak bunların farklı kurallara tabi kılınmasında eşitlik ilkesine aykırılıktan söz edilemez.

66. Diğer taraftan, Anayasa'nın hak arama hürriyetini düzenleyen 36. maddesinin birinci fıkrasında, " Herkes, meşru vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir. " denilerek yargı mercilerine davacı ve davalı olarak başvurabilme ve bunun doğal sonucu olarak da iddia, savunma ve adil yargılanma hakkı güvence altına alınmıştır.

67. Dava konusu kuralda, Maliye Bakanlığının merkez teşkilatında daire başkanı, genel müdür yardımcısı ve başkan yardımcısı veya taşra teşkilatında defterdar kadrolarında çalışanların maliye uzmanı olarak atanmış sayılması değil, bu kadrolarda çalışanlardan kuralda belirtilen koşulları taşıyanların idare tarafından maliye uzmanı olarak atanabilmesi düzenlenmektedir. Dolayısıyla dava konusu kuralın uygulanabilmesi için idarenin idari bir işlem tesis etmesi gerekmektedir. Anayasa'nın 125. maddesi uyarınca kural olarak tüm idari işlemlerde olduğu gibi anılan idari işlemler yönünden de kişilerin yargı mercilerine başvurması mümkün olduğundan, kuralın hak arama özgürlüğünü zedeleyen bir yönü bulunmamaktadır.

68. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2., 10. ve 36. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

69. Kuralın, Anayasa'nın 70. maddesiyle ilgisi görülmemiştir.

F- Kanun'un 73. Maddesinin (h) Fıkrasının (1) Numaralı Bendiyle Değiştirilen 663 Sayılı KHK'nın 23. Maddesinin (7) Numaralı Fıkrasının (c) ve (ç) Bentleri

1- İptal Talebine İlişkin Gerekçe

70. Dava dilekçesinde özetle, dava konusu kurallarla sağlık mesleklerinde uygulanacak meslekten geçici ve sürekli men etme müeyyidelerinin düzenlendiği, ancak bu düzenlemeler yapılırken karşılığında ceza uygulanacak fiillerin kesin ve açık şekilde belirtilmediği, bu durumun hukuki belirlilik ve güvenlik ile suçun yasallığı ilkelerine aykırı düştüğü, dava konusu kurallarla Anayasa'nın 48. ve 49. maddelerinde düzenlenen çalışma özgürlüğü ve çalışma hakkına ölçsüz bir müdahale getirildiği ve anılan hakların özünün ortadan kaldırıldığı, kurallarda meslekten geçici ve sürekli men etme cezasını gerektiren fiillerin oluşup oluşmadığını belirleme yetkisinin Sağlık Meslekleri Kuruluna bırakıldığı, oysa bu görevin bir tür yargı görevi niteliği taşıdığı, bu nedenle bağımsız ve tarafsız mahkemelerce yerine getirilmesi gerektiği, ayrıca söz konusu Kurul üyelerinin önemli bir

kısının yürütme tarafından atanması nedeniyle Kurulun tarafsızlığından ve bağımsızlığından söz edilemeyeceği, 5237 sayılı Türk Ceza Kanunu'nun 53. maddesinin altıncı fıkrasında belli bir meslek veya sanatın gerektirdiği dikkat ve özen yükümlülüğüne aykırılık dolayısıyla işlenen taksirli suçtan mahkûmiyet halinde meslek veya sanatın icrasının yasaklanmasına karar verilebileceğinin öngörüldüğü, bu şekilde bir düzenleme varken bu eylemlerin aynı zamanda dava konusu kurallarla da cezalandırılmasının aynı eylemden dolayı birden fazla ceza verilemeyeceği yönündeki ilkeyle ve Türkiye'nin imzalamış olduğu Avrupa İnsan Hakları Sözleşmesi'yle çeliştiği belirtilerek kuralların, Anayasa'nın 2., 9., 13., 38., 48., 49., 90. ve 135. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

71. Dava konusu kurallarda, sağlık meslekleri yönünden uygulanacak meslekten geçici ve sürekli men etme cezaları, bu cezaları gerektirecek eylemler ve bu eylemler karşılığında uygulanacak men cezalarının niteliği ve süresi düzenlenmektedir.

72. Anayasa'nın 2. maddesinde, Türkiye Cumhuriyeti, bir hukuk devleti olarak nitelendirilmiştir. Hukuk devletinin temel ilkelerinden biri de "belirlilik"tir. Bu ilkeye göre, yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi gerekir. Belirlilik ilkesi, hukuksal güvenlikle bağlantılı olup birey, kanundan, belirli bir kesinlik içinde, hangi somut eylem ve olguya hangi hukuksal yaptırımın veya sonucun bağlandığını bilmelidir. Birey ancak bu durumda kendisine düşen yükümlülükleri öngörebilir ve davranışlarını ayarlayabilir. Hukuk güvenliği, normların öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar.

73. Anayasa'nın 38. maddesinin ilk fıkrasında, "Kimse, ... kanunun suç saymadığı bir fiilden dolayı cezalandırılmaz" denilerek "suçun kanuniliği"; üçüncü fıkrasında da " ceza ve ceza yerine geçen güvenlik tedbirleri ancak kanunla konulur " denilerek " cezanın kanuniliği " ilkesi getirilmiştir. Anayasa'da öngörülen suçta ve cezada kanunilik ilkesi, insan hak ve özgürlüklerini esas alan bir anlayışın öne çıktığı günümüzde, ceza hukukunun da temel ilkelerinden birini oluşturmaktadır. Anayasa'nın 38. maddesine paralel olarak 5237 sayılı Türk Ceza Kanunu'nun 2. maddesinde yer alan "suçta ve cezada kanunilik" ilkesi uyarınca, hangi eylemlerin yasaklandığı ve bu yasak eylemlere verilecek cezaların hiçbir kuşkuya yer bırakmayacak biçimde kanunda gösterilmesi, kuralın açık, anlaşılır ve sınırlarının belli olması gerekmektedir. Kişilerin yasak eylemleri önceden bilmeleri düşüncesine dayanan bu ilkeyle temel hak ve özgürlüklerin güvence altına alınması

amaçlanmaktadır. Anayasa'nın 38. maddesinde idari ve adli cezalar arasında bir ayırım yapılmadığından disiplin suç ve cezaları da bu maddede öngörülen ilkelere tâbidir.

74. Dava konusu kurallarda sağlık meslekleri yönünden disiplin cezası olarak meslekten geçici ve sürekli men etme cezaları düzenlenmiştir. Bu düzenleme yapılırken, meslek icrası esnasında sonucunu öngörerek veya görevinin gereklerine aykırı hareket ederek veyahut görevinin gereklerini yapmakta ihmal veya gecikme göstererek bir kişinin ağır derecede olmayan engelliliğine sebebiyet verenlerin, Sağlık Meslekleri Kurulu tarafından üç aydan bir yıla, ağır engelliliğe veya ölüme sebebiyet verenlerin ise bir yıldan üç yıla kadar meslekten geçici olarak men edilecekleri; ağır derecede olmayan engelliliğe sebebiyet verenlerin bu fiillerini beş yıl içinde tekrar etmeleri halinde verilecek cezalarda alt ve üst sınırların iki kat olarak uygulanacağı; ağır engelliliğe veya ölüme sebebiyet verenlerin bu fiillerini beş yıl içinde tekrar etmeleri halinde ise meslekten sürekli men edilecekleri belirtilmek suretiyle anılan disiplin cezalarının hangi fiiller sonucu ve hangi koşullarda verilebileceği herhangi bir tereddüde yer vermeyecek şekilde açık, anlaşılır, uygulanabilir ve nesnel olarak kanunla belirlenmiştir. Bu fiiller sonucu uygulanacak cezanın türü ve süresi de aynı şekilde açıklanmıştır.

75. Bu nedenle dava konusu kurallarda hukuki güvenlik ve kanunilik ilkelerine aykırı düşen bir yön bulunmamaktadır.

76. Anayasa'nın 48. maddesinin birinci fıkrasının ilk cümlesinde, " Herkes, dilediği alanda çalışma ve sözleşme hürriyetlerine sahiptir. " denilmek suretiyle temel hak ve özgürlükler arasında yer alan çalışma ve sözleşme hürriyeti güvence altına alınmış, Anayasa'nın 13. maddesinde ise temel hak ve özgürlüklerin ancak Anayasa'nın ilgili maddelerinde belirtilen nedenlere bağlı olarak sınırlanabileceği öngörülmüştür. Ancak bu, düzenlendiği maddede hiçbir sınırlama nedenine yer verilmeyen hakların mutlak olduğunu ve bunların hiçbir şekilde sınırlanamayacağı anlamını taşımamaktadır. Anayasa Mahkemesinin birçok kararında da belirtildiği gibi, temel hak ve hürriyetlerin doğasından kaynaklanan bazı sınırları bulunduğu gibi Anayasa'nın başka maddelerinde yer alan kurallar da temel hak ve hürriyetlerin sınırını oluşturur. Bir başka deyişle, temel hak ve özgürlüklerin kapsamının ve objektif uygulama alanının her bir norm yönünden bağımsız olarak değil, Anayasa'nın bütünü içerisindeki anlama göre belirlenmesi gerekir.

77. Dava konusu kurallarda, meslek icrası esnasında sonucunu öngörerek veya görevinin gereklerine aykırı hareket ederek veyahut görevinin gereklerini yapmakta ihmal veya gecikme göstererek kişilerin engelliliğine veya ölümüne sebebiyet verenlerin meslekten geçici ve sürekli olarak men edilmeleri düzenlenmekte olup bu kuralların, kişilerin Anayasa'nın 17. maddesinde güvence altına

alınan yaşam ve vücut bütünlüğü haklarını korumaya yöneldiği açıktır. Dolayısıyla çalışma hürriyetinin düzenlendiği Anayasa'nın 48. maddesinde özel bir sınırlama nedenine yer verilmemişse de Anayasa'nın 17. maddesinde belirtilen yaşam ve vücut bütünlüğü haklarının korunması nedenleriyle bu hürriyetin sınırlandırılabilmesi mümkündür.

78. Ancak çalışma hürriyetinin sınırlandırılması için belirtilen nedenin varlığı yeterli olmayıp temel hak ve özgürlüklerin sınırlandırılması rejimini belirleyen Anayasa'nın 13. maddesindeki diğer güvencelere de uyulması gerekmektedir. Anayasa'nın 13. maddesi uyarınca çalışma hürriyeti, yalnızca kanunla ve demokratik bir toplumda gerekli olduğu ölçüde sınırlandırılabilir. Ayrıca getirilen bu sınırlamalar, hakkın özüne dokunamayacağı gibi Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamaz.

79. Dava konusu kurallarla getirilen sınırlamayla kişilerin her alandaki çalışma hürriyetleri değil, sadece sonucunu öngörerek veya görevinin gereklerine aykırı hareket ederek veyahut görevinin gereklerini yapmakta ihmal veya gecikme göstererek birden fazla olacak şekilde kişilerin ağır engelliliğine veya ölümüne sebebiyet verenlerin sağlık mesleği icra etmeleri yasaklanmakta olup bu sınırlamanın, çalışma hürriyetinin kullanımını bütünüyle ortadan kaldırmadığı veya ciddi surette güçleştirip amacına ulaşmasına engel olmadığı açıktır.

80. Kurallarla kişilerin yaşam ve vücut bütünlüğü haklarının korunması amacıyla çalışma hürriyetine bir sınırlama getirildiğinden bu sınırlama, demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır.

81. Bu şekilde, demokratik toplum düzeni bakımından alınması gerekli tedbirler kapsamında kişilerin çalışma hürriyeti sınırlandırılırken, Kanun'da sınırlama aracının sınırlama amacına uygun ve orantılı şekilde kullanılmasını sağlayacak yasal güvencelere yer verilmiş, böylece kişilerin yaşam ve vücut bütünlüğü haklarının korunması şeklindeki kamu yararı ile kişilerin çalışma hürriyeti arasında makul denge de kurulmuştur.

82. Bu bağlamda, Kanunda meslekten geçici ve sürekli men etme cezasını gerektirecek fiiller düzenlenirken kişilerin engelliliğine veya ölümüne neden olacak her türlü davranışın değil, sadece sonucunu öngörerek veya görevinin gereklerine aykırı hareket ederek veyahut görevinin gereklerini yapmakta ihmal veya gecikme göstererek kişinin engelliliğine veya ölümüne neden olacak "kusurlu" davranışın anılan müeyyidelerle cezalandırılmasına izin verilmiştir. Ayrıca, bu cezaların kişide meydana gelecek zararın ağırlığı dikkate alınarak belirlendiği, bu yönüyle fiil ile ceza arasında makul dengenin kurularak ceza miktarının kusur oranını aşmamasına özen gösterildiği de görülmektedir. Bu çerçevede, ağır derecede olmayan engelliliğe sebebiyet verenlerin üç aydan bir yıla, ağır engelliliğe

veya ölüme sebebiyet verenlerin ise bir yıldan üç yıla kadar meslekten geçici olarak men edilmelerine izin verilmişken, ağır derecede olmayan engelliliğe sebebiyet verenlerin bu fiillerini beş yıl içinde tekrar etmeleri halinde verilecek cezalarda alt ve üst sınırların iki kat olarak uygulanacağı, ağır engelliliğe veya ölüme sebebiyet verenlerin bu fiillerini beş yıl içinde tekrar etmeleri halinde ise meslekten sürekli men edilecekleri düzenlenmiştir.

83. Kanun'da kurallara konu disiplin suçu ve cezasının uygulanmasına karşı yargı yolunun da açık tutulduğu böylece idarenin sınırlama aracını sınırlama amacına ve Kanun'a aykırı şekilde kullanmasının önüne geçecek güvencenin de sağlandığı görülmektedir. Bu yönleriyle kurullarla çalışma hürriyetine getirilen sınırlamanın, hakkın özünü zedelediği veya bunun demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı düştüğü de söylenemez.

84. Ayrıca, kurullarda meslekten geçici ve sürekli men etme cezasını gerektiren fiillerin oluşup oluşmadığını belirleme yetkisinin Sağlık Meslekleri Kuruluna bırakıldığı, oysa bu görevin bir tür yargı görevi niteliği taşıdığı, bu nedenle bağımsız ve tarafsız mahkemelerce yerine getirilmesi gerektiği ileri sürülmüş ise de dava konusu kurullarda disiplin suç ve cezalarının unsurlarının belirlenmesi idareye bırakılmayıp kanunilik ilkesinin gereği olarak kanunla düzenlenmektedir. Böyle bir düzenlemeden sonra disiplin suç ve cezalarının kanunda belirtilen tipikliğe uyup uymadığını belirleme yetkisinin idareye bırakılmasında Anayasa'ya aykırı bir yön bulunmamaktadır.

85. Öte yandan, bir fiilin hem idari bir yaptırımın hem de adli bir cezanın veya güvenlik tedbirinin konusunu oluşturması mümkün olup bu durum, fiilin mükerrer şekilde cezalandırıldığı anlamına gelmemektedir.

86. Açıklanan nedenlerle dava konusu kurullar, Anayasa'nın 2., 13., 38. ve 48. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

87. Kurulların, Anayasa'nın 9., 49., 90. ve 135. maddeleriyle ilgisi görülmemiştir.

G- Kanun'un 73. Maddesinin (h) Fıkrasının (3) Numaralı Bendiyle Değiştirilen 663 Sayılı KHK'nin 47. Maddesinin (1), (2) ve (3) Numaralı Fıkralarının İncelenmesi

1- İptal Talebine İlişkin Gerekçe

88. Dava dilekçesinde özetle, dava konusu kurullarla Sağlık Bakanlığı ve bağlı kuruluşlarına kişisel verileri toplama, saklama, işleme ve paylaşma yetkisinin verildiği, bu durumun özel hayatın gizliliği ve kişisel verilerin korunması haklarının özüne müdahale edilmesi ve ölçüsüzce sınırlandırılması sonucunu doğurduğu belirtilerek kurulların, Anayasa'nın 2., 13., 20. ve 90. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

89. Dava konusu kurallarda, Sağlık Bakanlığı ve bağlı kuruluşlarına, görevlerini yürütebilmeleri için gerekli olan bilgileri toplama, işleme, paylaşma yetkisi verilmekte ve bu yetkinin kapsam ve sınırları düzenlenmektedir.

90. Anayasa'nın 20. maddesinin ilk fıkrasında, herkesin, özel hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş; son fıkrasında da " Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir. " denilerek kişisel verilerin korunması, özel hayatın gizliliğinin korunması kapsamında güvenceye kavuşturulmuştur.

91. Kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvencenin yaşama geçirilebilmesi için, bu hakkı ilgilendiren yasal düzenlemelerin, açık, anlaşılabilir ve kişilerin söz konusu haklarını kullanabilmelerine elverişli olması gerekir. Ancak böyle bir düzenleme ile kişilerin özel hayatlarını ilgilendiren veri, bilgi ve belgelerin keyfi müdahalelere karşı korunması olanaklı hâle getirilebilir.

92. Anayasa'nın 13. maddesinde, temel hak ve hürriyetlerin, özlere dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği, bu sınırlamaların Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamayacağı belirtilmiştir.

93. Anayasal açıdan dokunulamayacak öz, her temel hak ve özgürlük açısından farklılık göstermekle birlikte kanunla getirilen sınırlamanın hakkın özüne dokunmadığının kabulü için temel hakların kullanılmasını ciddi surette güçleştirip, amacına ulaşmasına engel olmaması ve etkisini ortadan kaldıracı bir nitelik taşımaması gerekir.

94. Ölçülülük ise amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder. Ölçülülük, aynı zamanda yasal önlemin sınırlama amacına ulaşmaya elverişli olmasını, amaç ve aracın ölçülü bir oranı kapsamasını ve sınırlayıcı önlemin demokratik toplum düzeni bakımından zorunluluk taşımasını da içeren bir ilkedir.

95. Anayasa'nın 20. maddesinin gerekçesinde de belirtildiği üzere özel hayatın korunması her şeyden önce bu hayatın gizliliğinin korunması, başkalarının gözleri önüne serilmemesi demektir. Kişinin özel

hayatında yaşananların, yalnız kendisi veya kendisinin rıza gösterdiği kimseler tarafından bilinmesini isteme hakkı, kişinin temel haklarından biridir ve bu niteliği nedeniyle insan haklarına ilişkin beyanname ve sözleşmelerde yer almış, tüm demokratik ülkelerin mevzuatlarında açıkça belirlenen istisnalar dışında devlete, topluma ve diğer kişilere karşı korunmuştur.

96. 663 sayılı KHK'nın 47. maddesinin dava konusu (1) numaralı fıkrasıyla Bakanlık ve bağlı kuruluşlarına, mevzuatla kendilerine verilen görevleri, e-devlet uygulamalarına uygun olarak daha etkin ve daha hızlı biçimde yerine getirebilmeleri amacıyla bütün kamu ve özel sağlık kurum ve kuruluşlarından; sağlık hizmeti alanların, hizmetin gereği olarak ilgili sağlık kurum ve kuruluşuna vermek zorunda oldukları kişisel bilgileri ve bu kimselere verilen hizmete ilişkin bilgileri her türlü vasıtayla toplama, işleme ve paylaşma yetkisi verilmektedir.

97. Verilen yetkiyle özel hayatın ve kişisel verilerin korunması haklarına bir sınırlama getirildiği açık olup bu sınırlama, demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır. Zira kuralın yöneldiği, sağlık hizmetlerinin etkin ve hızlı biçimde yerine getirilerek herkesin hayatını beden ve ruh sağlığı içinde sürdürmesini sağlama görevi, Anayasa ile devlete yüklenen ve toplum düzeninin korunması için alınması gereken zorunlu tedbirlerdendir.

98. Anılan sınırlamayla, kişilerin her türlü kişisel bilgilerinin değil, sadece sağlık hizmetinin gereği olarak ilgili sağlık kurum ve kuruluşuna vermek zorunda oldukları bilgilerin toplanması, işlenmesi ve paylaşılması yetkisi verilmektedir. Dolayısıyla bu sınırlamanın özel hayatın ve kişisel verilerin korunması haklarını bütünüyle ortadan kaldırmadığı veya ciddi surette güçleştirip amacına ulaşmasına engel olmadığı da açıktır.

99. Ancak kuralda söz konusu kişisel bilgilerin "her türlü vasıtayla" toplanmasına, işlenmesine ve paylaşılmasına izin verilmesi, sınırlamayı, öngörülme amacının ötesinde kişisel bilgilerin gizliliğinin keyfi şekilde ihlal edilmesi sonucunu doğurabilecek bir araca dönüştürmektedir. Bu ise sınırlama amacıyla sınırlama amacı arasında bulunması gereken makul dengeyi bozmakta, özel hayatın ve kişisel verilerin korunmasını isteme haklarına kuralda belirtilen sınırlama amacı dışında ölçüsüz bir şekilde müdahale edilebilmesine imkân tanımaktadır.

100. 47. maddenin dava konusu (2) numaralı fıkrasında da (1) numaralı fıkrada belirtilen yöntemlerle toplanan ve işlenen kişisel verilerin ilgili üçüncü kişiler ile kamu kurum ve kuruluşlarıyla paylaşılması öngörüldüğünden yukarıda belirtilen aynı gerekçelerle bu düzenleme de ölçülülük ilkesini ihlal etmektedir.

101. 47. maddenin dava konusu (3) numaralı fıkrasında ise Bakanlık ve bağılı kuruluşlarının, mevzuatla kendilerine verilen görevleri yerine getirebilmek için gereken bilgileri, kamu ve özel ilgili bütün kişi ve kuruluşlardan istemeye yetkili olduğu ve ilgili kişi ve kuruluşların istenilen bilgileri vermekle yükümlü oldukları düzenlenmektedir.

102. Bakanlık ve bağılı kuruluşlarına verilen görevler çok geniş bir alanı kapsamakta olup bu görevlerin tamamının kişilerin özel hayatlarına müdahale edilmesini gerektirecek bir toplumsal zorunluluğu bünyesinde barındırdığı söylenemez. Dolayısıyla dava konusu kuralla sadece demokratik toplum düzeni yönünden zorunlu olan sınırlamalara değil, özel hayatın ve kişisel verilerin korunması haklarına yapılabilecek her türlü sınırlamaya izin verilmesi, bir başka ifadeyle, kuralda anılan haklara sınırlama getirilirken sınırlama aracının sınırlama amacına uygun ve orantılı olarak kullanılmasını temin edecek güvencelere yer verilmemesi ölçülülük ilkesine aykırı düşmektedir.

103. Açıklanan nedenlerle dava konusu kurallar, Anayasa'nın 2., 13. ve 20. maddelerine aykırıdır. İptali gerekir.

104. Nuri NECİPOĞLU, Hicabi DURSUN ve Celal Mümtaz AKINCI bu görüşe katılmamışlardır.

105. Kuralın, Anayasa'nın 90. maddesi ile ilgisi görülmemiştir.

Ğ- Kanun'un 73. Maddesinin (p) Fıkrasının (1) Numaralı Bendiyle 3194 Sayılı Kanun'un 8. Maddesine Eklenen (ı), (i) ve (j) Bentlerinin İncelenmesi

1- Maddenin (ı) Bendi

a- İptal Talebine İlişkin Gerekçe

106. Dava dilekçesinde özetle, dava konusu kuralla kamu tüzel kişisi meslek odalarının, üyeleri üzerindeki denetim görevini yerine getirme imkânının ortadan kaldırıldığı, bu durumun Anayasa'nın 2. ve 135. maddelerine aykırı olduğu ileri sürülmüştür.

b- Anayasa'ya Aykırılık Sorunu

107. Dava konusu kuralda, harita, plan, etüt ve projelerin idare ve ilgili kanunlarında açıkça belirtilen yetkili kuruluşlar haricinde meslek odaları dâhil başka bir kurum veya kuruluşun vize veya onayına tabi tutulamayacağı; vize veya onay yaptırılmaması ve benzeri nedenlerle müelliflerin veya bunlara ait kuruluşların büro tescillerinin iptal edilemeyeceği; tescillerin yenilenmesinin hiçbir şekilde geciktirilemeyeceği ve müelliflerden bu hükmü ortadan kaldıracak şekilde taahhütname istenemeyeceği düzenlenmektedir.

108. Anayasa'nın " Kamu Kurumu niteliğindeki meslek kuruluşları " başlıklı 135. maddesinin birinci fıkrasında, " Kamu kurumu niteliğindeki meslek kuruluşları ve üst kuruluşları; belli bir mesleğe mensup olanların müşterek ihtiyaçlarını karşılamak, meslekî faaliyetlerini kolaylaştırmak, mesleğin genel menfaatlere uygun olarak gelişmesini sağlamak, meslek mensuplarının birbirleri ile ve halk ile olan ilişkilerinde dürüstlüğü ve güveni hâkim kılmak üzere meslek disiplini ve ahlâkını korumak maksadı ile kanunla kurulan ve organları kendi üyeleri tarafından kanunda gösterilen usullere göre yargı gözetimi altında, gizli oyla seçilen kamu tüzelkişilikleridir. " denilmek suretiyle, kamu kurumu niteliğindeki meslek kuruluşlarının kuruluş amaçları ve nitelikleri hüküm altına alınmıştır.

109. Anayasa'nın 7. maddesinde ifadesini bulan yasamanın genelliği ilkesi uyarınca kanun koyucu, Anayasa'ya aykırı olmamak kaydıyla dilediği konuda düzenleme yapma yetkisine sahip bulunmaktadır. Dava konusu fıkranın birinci cümlesinde, 3194 sayılı Kanun kapsamındaki harita, plan, etüt ve projelerin idare ve ilgili kanunlarında açıkça belirtilen yetkili kuruluşlar haricinde meslek odaları dâhil başka bir kurum veya kuruluşun vize veya onayına tabi tutulamayacağı belirtilmekte olup Anayasa'da bu konudaki yetkinin münhasıran kamu idareleri ve kanunda açıkça belirtilen kuruluşlara bırakılmasını yasaklayan bir hüküm bulunmamaktadır. Dolayısıyla bu yetkinin kanunda belirtilen idare ve kuruluşlara bırakılmasında Anayasa'ya aykırı bir yön olduğu söylenemez.

110. Vize ve onay işlemlerinin yaptırılmaması, müelliflerin veya bunlara ait kuruluşların büro tescillerinin iptal edilememesi, tescillerin yenilenmesinin geciktirilememesi ve müelliflerden bu hükmü ortadan kaldıracak şekilde taahhütname istenememesi yönündeki hüküm ise fıkranın birinci cümlesindeki düzenlemenin doğal bir sonucu olup bununla vize ve onay işlemlerinin yaptırılmasıyla ilgisiz kuruluşların, özellikle de meslek kuruluşlarının bu nedenlerle üyeleri üzerinde mesleki yaptırımlar uygulamasının önüne geçilmesinin amaçlandığı anlaşılmaktadır.

111. Kamu kurumu niteliğindeki meslek kuruluşlarının Anayasa'da belirtilen kuruluş amaçları dikkate alındığında üyeleri üzerinde denetim yapma yetkisine sahip oldukları tartışmasızdır. Ancak bu denetim yetkisi Anayasa'nın anılan maddesindeki amaçların gerçekleştirilmesiyle sınırlı olup bu sınırın aşılması Anayasa'da belirtilen amaçlar dışında üyeler üzerinde herhangi bir denetim veya yaptırım uygulanması mümkün değildir. Dava konusu kuralla meslek kuruluşları yönünden getirilen sınırlama, Anayasa'nın 135. maddesindeki amaçların gerçekleştirilmesine ilişkin olarak meslek kuruluşlarına verilen denetim göreviyle ilgili bulunmamaktadır. Bu yönüyle kuralla meslek odalarının üyeleri üzerindeki denetim görevinin yerine getirilmesi imkânının ortadan kaldırılması söz konusu değildir.

112. Ayrıca, kuralla vize ve onay yaptırılmasıyla ilgisiz olan ve müelliflerin büro tescillerinin iptalini gerektiren diğer konularla ilgili herhangi bir sınırlama getirilmediğinden kuralın meslek kuruluşlarının bu konulardaki denetim ve yaptırım uygulama yetkisini etkileyen bir yönü bulunmamaktadır.

113. Açıklanan nedenlerle kural, Anayasa'nın 2. ve 135. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

2- Maddenin (i) Bendi

a- İptal Talebine İlişkin Gerekçe

114. Dava dilekçesinde özetle, idarelerce onaylanmış; mevcut durumu gösteren halihazır haritalar, parselasyon planları ile teknik ve idari düzenlemeleri içeren 3194 sayılı Kanun kapsamındaki planların değişiklik ve revizyonlarında ilk müellifin görüş veya izninin aranmayacağı kuralına yer verildiği, bunun eser sahibinin fikri mülkiyet hakkının özüne müdahale edilmesi ve ölçüsüzce sınırlandırılması sonucunu doğurduğu belirtilerek kuralın, Anayasa'nın 2., 13., 35. ve 90. maddelerine aykırı olduğu ileri sürülmüştür.

b- Anayasa'ya Aykırılık Sorunu

115. Anayasa'nın 35. maddesinde, " Herkes, mülkiyet ve miras haklarına sahiptir. Bu haklar, ancak kamu yararı amacıyla, kanunla sınırlanabilir. Mülkiyet hakkının kullanılması toplum yararına aykırı olamaz. " denilmek suretiyle mülkiyet ve miras hakları güvence altına alınmıştır.

116. Mülkiyet hakkı, kişiye başkalarının hakkına zarar vermemek ve kanunların koyduğu sınırlamalara uymak koşuluyla, sahibi olduğu şeyi dilediği gibi kullanma, ürünlerinden yararlanma ve tasarruf olanağı veren bir haktır. Mülkiyet hakkının konusunu, maddi ve gayrimaddi mallar oluşturmaktadır. Taşınır ve taşınmaz mallar, maddi mallar kapsamında iken, fikri ve sınai mülkiyet hakları gayrimaddi mallar kapsamında yer almaktadır.

117. Fikri ve sınai mülkiyet haklarını düzenleyen, 5.12.1951 tarihli ve 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun 14. ve devamı maddeleri uyarınca, fikir ve sanat eserleri üzerinde eseri meydana getiren eser sahiplerinin "manevi" ve "mali" olmak üzere temel iki hakkı bulunmaktadır. Bu bağlamda, " eserde değişiklik yapılmasını men hakkı " da manevi haklar içinde yer almakta olup anılan Kanun'un 16. maddesi uyarınca eser sahibinin izni olmaksızın eserde değişiklik yapılması mümkün değildir.

118. Öte yandan, 5846 sayılı Kanun'un 1/B maddesinin birinci fıkrasının (a) bendinde, sahibinin hususiyetini taşıyan, ilim ve edebiyat, musiki, güzel sanatlar veya sinema eserleri olarak sayılan her

nevi fikir ve sanat mahsullerinin "eser" olduğu belirtilmiş, " İlim ve edebiyat eserleri " kenar başlıklı 2. maddesinin birinci fıkrasının (3) numaralı bendinde ise her nevi harita ve planın "ilim ve edebiyat eseri" olduğu kuralına yer verilmiştir. Buna göre, 5846 sayılı Kanun çerçevesinde ilim ve edebiyat eseri niteliğini haiz bulunan her nevi "harita ve planın" değişikliğinde eser sahibinin izninin alınması, kişinin fikri mülkiyet hakkının önemli bir unsurunu oluşturmaktadır.

119. Dava konusu kuralda, idarelerce onaylanmış; mevcut durumu gösteren hâlihazır haritalar, parselasyon planları ile teknik ve idari düzenlemeleri içeren 3194 sayılı Kanun kapsamındaki planların değişiklik ve revizyonlarında ilk müellifin görüş veya izninin aranmayacağı düzenlenmiş, dolayısıyla anılan harita ve planlara ilişkin olarak eser sahiplerinin fikri mülkiyet haklarına bir sınırlama getirilmiştir.

120. 3194 sayılı Kanun kapsamındaki planlar, aynı Kanun'un 8. maddesinde sayılmıştır. Buna göre bölge planları, mekânsal strateji planları, çevre düzeni planları ve imar planları 3194 sayılı Kanun kapsamındaki planlar olup bunlar, bir bütün olarak yapıldığı yerdeki halkın ihtiyaçlarını karşılamak, dolayısıyla kamu yararını gerçekleştirmek üzere kentsel organizasyonu ve gelişmeyi belirleyen, yapımında müellifinin yanı sıra birçok kamu kurum ve kuruluşun etkili olduğu ve yetkili idarelerin onaylamasıyla idari ve teknik düzenleme niteliği kazanan mekânsal planları ifade etmektedir.

121. Bir yerdeki tüm arazilerin nasıl kullanılacağını ve yapılaşmanın nasıl ve hangi yoğunlukta olacağını belirleyen bu planların oluşturulması sürecinde, sadece planı hazırlayan ilk müellif etkili olmamakta, kamu idarelerinin halkın seçimiyle işbaşına gelen yetkili organları da rol almakta ve esas itibariyle bunların onaylamasıyla bu planlar demokratik meşruiyet ve hukuki geçerlilik kazanabilmektedir. Dolayısıyla kamu idarelerinin onaylamasıyla düzenleyici bir idari işlem haline gelen bu planların sadece ilk müellifine özgülenmesi mümkün olmayıp yetkili idarelerin kamu yararı amacıyla bu plarlarda yapacağı değişikliklerde ilk müellifin görüş ve iznini alma mecburiyetinin bulunması, bu değişikliklerin yapılamamasına ve sonuç itibariyle kamu yararının zedelenmesine yol açabilecektir.

122. Öte yandan, bu durum, bir yerin kentsel gelişimine ilişkin kararın ve yönetim hakkının planı hazırlayan ilk müellife bırakılması anlamını taşıyacaktır ki bunun Anayasa'nın 2. maddesinde ifadesini bulan demokratik yönetim anlayışıyla bağdaştırılması olanaklı değildir.

123. Parselasyon planları ise 2.11.1985 tarihli ve 18916 mükerrer sayılı Resmi Gazetede yayımlanan İmar Kanununun 18 inci Maddesi Uyarınca Yapılacak Arazi ve Arsa Düzenlenmesi İle İlgili Esaslar Hakkında Yönetmelik'in 4. maddesinin (k) bendinde " İmar plânının araziye uygulanmasından sonra yapılacak rövele ölçülerine göre boyut değiştirmeyen paftalar üzerinde çizilen, kesin parselasyon

durumunu gösteren ve tapuya tescil işlemlerine esas alınan plân " şeklinde tanımlanmış olup bunların 3194 sayılı Kanun'un 8. maddesinin (d) bendi uyarınca yukarıda belirtilen bölge planları, mekânsal strateji planları, çevre düzeni planları ve imar planları gibi üst kademe mekânsal planlarda yapılacak değişikliklere uygun olarak değiştirilmesi zorunluluğu bulunmaktadır. Dolayısıyla parselasyon planları, idari düzenleme niteliği bulunan üst kademe mekânsal planlama işlemlerine bağlı olarak tesis edilen idari işlemler niteliğini haiz bulunmakta, tıpkı mekânsal planlar gibi yetkili idarelerce onaylanmakta, askı ve itiraz süreçleri sonunda kesinlik kazanmakta ve en önemlisi bunlar kişilerin mülkiyet haklarını doğrudan etkileyebilmektedir. Bu nedenle, mekânsal planlara ilişkin olarak yapılan açıklamalardaki gerekçelerle, parselasyon planlarının da ilk müellifine özgülenmesi, dolayısıyla değişikliklerinde ilk müellifin görüş ve izninin alınması mecburiyetinin bulunması, kamu yararını zedeleyebilir.

124. Haritalar yönünden de kuralda her türlü haritaya değil, sadece idarelerce onaylanmış ve mevcut durumu gösteren hâlihazır haritalara, dolayısıyla yetkili idarelerce belirlenen yöntemlere göre hazırlanan ve müellifine göre değişmesi söz konusu olmayan haritalara ilişkin bir düzenleme getirilmekte olup bunların değişiklik ve revizyonlarında da ilk müellifin görüş veya izninin aranma mecburiyetinin bulunmasının işin doğasına uygun düşmeyebileceği, bunun da çeşitli teknik ve idari zorunluluklar nedeniyle yapılması gereken değişiklikleri önleyebileceği açıktır.

125. Anayasa'nın 17. maddesinde, herkesin maddi ve manevi bütünlüğünü koruma hakkına sahip olduğu ifade edilmiş; 5. maddesinde, kişilerin maddi ve manevi bütünlüğünü koruma ve geliştirme görevi bir ödev olarak Devlete yüklenmiş; 56. maddesinde ise herkesin, sağlıklı ve dengeli bir çevrede yaşama hakkına sahip olduğu ve çevreyi geliştirme, çevre sağlığını korumanın Devletin ve vatandaşların ödevi olduğu vurgulanmıştır.

126. Buna göre, kişilerin maddi ve manevi bütünlüklerinin korunması ve geliştirilmesiyle sağlıklı ve dengeli bir çevrede yaşama haklarının sağlanması, Devletin görevleri arasında bulunmakta olup bu görevleri yerine getirmek üzere kentsel planlama araçlarının kullanılması zorunludur. Bu çerçevede, ilgili kamu idarelerinin sağlıklı, güvenli ve düzenli bir kent dokusunu kurmak ve geliştirmek, dolayısıyla kamu yararını gerçekleştirmek amacıyla idarelerce onaylanmış harita ve planlarda değişiklik yapma yetkisine sahip kılınması, bir zorunluluğa dayanmaktadır. Bu zorunluluk nedeniyle dava konusu kuralla fikri mülkiyet hakkına getirilen sınırlama, demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır.

127. Bu şekilde, demokratik toplum düzeni bakımından alınması gerekli tedbirler kapsamında kişilerin mülkiyet hakkı sınırlandırılırken, Kanun'da sınırlama aracının sınırlama amacına uygun ve

orantılı şekilde kullanılmasını sağlayacak yasal güvencelere de yer verilmiş; böylece hem kişilerin mülkiyet hakkının özünün zedelenmesi önlenmiş hem de mülkiyet hakkının korunması ile kişilerin maddi ve manevi varlıklarının korunması/geliştirilmesi ve sağlıklı bir çevrede yaşama haklarının sağlanması biçimindeki kamu yararı arasındaki makul denge kurulmuştur.

128. Bu bağlamda, kuralda sadece idarelerce onaylanmış, dolayısıyla artık teknik ve idari bir düzenleme niteliğini kazanmış planlar ile mevcut durumu gösteren hâlihazır haritaların değişikliğinde ilk müellifin görüş ve izninin alınmayacağı belirtilmiş, bunun dışındaki harita ve planlar ile ilgili herhangi bir sınırlama getirilmemiştir.

129. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2., 13. ve 35. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

130. Kuralın, Anayasa'nın 90. maddesiyle ilgisi görülmemiştir.

3- Maddenin (j) Bendi

a- İptal Talebine İlişkin Gerekçe

131. Dava dilekçesinde özetle, dava konusu kuralla ilgili idarelerin, Bakanlıkça belirlenen esaslara göre mimari estetik komisyonu kurmalarının öngörüldüğü, ancak bu düzenleme yapılırken kanunda komisyon üyelerinin kimlerden oluşacağı, hangi kriterlere göre tespit edileceği ve çalışma düzeninin nasıl olacağını belirtilmediği, bunun idarenin kanuniliği ve yasama yetkisinin devredilmezliği ilkelerine ters düştüğü, yine kuralla yapıların ve onaylı mimari projelerinin özgün fikir ifade edip etmediğine karar verme yetkisinin adı geçen komisyona verildiği, ancak bu düzenleme yapılırken de fikri haklar kapsamında olan yapıların ve onaylı mimari projelerinin özgün fikir ifade edip etmediğine hangi kriterler esas alınarak nasıl karar verileceğinin belirtilmediği, kuralın bu yönüyle de yasama yetkisinin devrine ve belirsizliğe neden olduğu, kuralda nelerin sanat eseri olup olmadığını belirleme yetkisinin Devlete verildiği, bunun bilim ve sanat özgürlüğüne açık bir aykırılık teşkil ettiği, ayrıca kuralda bir yandan özgün fikir ifade etmeyen yapı ve projelerde yapılacak değişikliklerde ilk müellifin görüşü aranmazken, diğer yandan özgün fikir ifade eden mimarlık eser ve projelerinde bazı koşullarda değişikliklerin müellifinin muvafakati alınmaksızın yapılabileceğine izin verilmesinin, fikri mülkiyet hakkının özünü zedeleyen bir müdahaleye neden olduğu, kuralın, idare bünyesinde oluşturulacak komisyonlarca verilecek eserin özgün bir fikir ifade etmediğine ilişkin kararlar nedeniyle eser sahiplerinin başkalarının tecavüzlerine karşı haklarını yargı yoluyla tespit ettirip zararlarını tazmin imkânını ortadan kaldırdığı ve eser sahiplerinin haklarının korunması

gerektiği yönündeki anayasal hükümle çeliştiği belirtilerek Anayasa'nın 2., 7., 10., 13., 35., 36., 64., 90. ve 123. maddelerine aykırı olduğu ileri sürülmüştür.

b- Anayasa'ya Aykırılık Sorunu

b1- Bendin ". eser sözleşmesinde işleme izni verilenler ile. " İbaresinin Dışında Kalan Bölümü

132. 6216 sayılı Kanun'un 43. maddesi uyarınca, iptali istenen kural ilgisini nedeniyle, Anayasa'nın 48. maddesi yönünden de incelenmiştir.

133. Dava konusu kuralda, ilgili idarelerin, Bakanlıkça belirlenen esaslara göre mimari estetik komisyonu kuracağı, komisyonun, yapıların ve onaylı mimari projelerin özgün fikir ifade edip etmediğine karar vermeye yetkili olacağı, özgün fikir ifade etmeyenlerde yapılacak değişikliklerde ilk müellifin görüşünün aranmayacağı, özgün fikir ifade eden mimarlık eser ve projelerinde ise eserin bütünlüğünü bozmadığına, estetik görünümünü değiştirmediklerine, teknik, yönetsel amaçlar ve kullanım amacı nedeniyle zorunlu olduğuna karar verilen değişikliklerin müellifinin izni alınmaksızın yapılabileceği, bu durumda ilk müellif tarafından talep edilebilecek telif ücretinin ilgili meslek odasının belirlenen mimari proje asgari hizmet bedelinin, tamamlanan yapılarda yüzde yirmisini, inşaatı süren yapılarda yüzde on beşini geçemeyeceği düzenlenmektedir.

134. Anayasa'nın 2. maddesinde yer alan hukuk devletinin temel ilkelerinden biri "belirlilik ilkesi"dir. Bu ilkeye göre, yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olması, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi gerekir.

135. Anayasa'nın 7. maddesinde, " Yasama yetkisi Türk Milleti adına Türkiye Büyük Millet Meclisindedir. Bu yetki devredilemez. " denilmiştir. Buna göre, Anayasa'da kanun ile düzenlenmesi öngörülen konularda yürütme organına genel ve sınırları belirsiz bir düzenleme yetkisinin verilmesi olanaklı değildir. Ancak yasama organının temel kuralları saptadıktan sonra, uzmanlık ve idare tekniğine ilişkin hususları yürütmeye bırakması, yasama yetkisinin devri olarak yorumlanamayacağı gibi yürütme organının yasama organı tarafından çerçevesi çizilmiş alanda genel nitelikte hukuksal tasarruflarda bulunması, hukuk devletinin belirlilik ilkesine de aykırı düşmez.

136. Anayasa'nın 123. maddesinin birinci fıkrasında ise " İdare, kuruluş ve görevleriyle bir bütündür ve kanunla düzenlenir. " hükmü yer almaktadır. Bu maddede yer alan düzenleme, idarenin kanuniliği ilkesine vücut vermektedir. İdarenin kanuniliği ilkesi, idarenin ve organlarının görev ve yetkilerinin kanunla düzenlenmesini gerekli kılar.

137. Dava konusu kuralda, mimari estetik komisyonunun hangi maksatla, ne tür bir görev ve yetkiyi ifa etmek üzere, hangi faaliyet konularında ve hangi idareler tarafından kurulacağına ilişkin hususlar, hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek biçimde açık, net, anlaşılır ve uygulanabilir şekilde düzenlenerek konuya ilişkin temel kurallar kanunla belirlenmiştir.

138. Kanun koyucunun bu şekilde konuyla ilgili temel kuralları belirleyip kanuni çerçeveyi çizdikten sonra, bu çerçevenin içinde kalacak hususların düzenlenmesini idareye bırakmasında, hukuki belirlilik, idarenin kanuniliği ve yasama yetkisinin devredilmezliği ilkelerine aykırı düşen bir yön bulunmamaktadır.

139. Söz konusu komisyonda kimlerin yer alacağı veya komisyonun görevini yerine getirirken hangi kriterleri esas alacağı konuları da kanunla çizilen çerçeve içerisinde belirlenebilecek hususlar olup idareye bu konuda verilen düzenleme yetkisinin yargı denetimine tabi olduğu, dolayısıyla bu yetkinin hukuka ve işin esasına aykırı kullanılmasını önleyecek yasal güvencenin de bulunduğu görülmektedir.

140. Öte yandan, Anayasa'nın 64. maddesinde, " Devlet, sanat faaliyetlerini ve sanatçıyı korur. Sanat eserlerinin ve sanatçının korunması, değerlendirilmesi, desteklenmesi ve sanat sevgisinin yayılması için gereken tedbirleri alır. " denilmek suretiyle Devletin sanat faaliyetlerini ve sanatçıyı koruma görevi anayasal güvenceye kavuşturulmuştur.

141. Dava konusu kuralda, nelerin sanat eseri olduğu ve nelerin olmadığı yönünde bir düzenleme getirilmemiş, sadece idareye yapıların ve onaylı mimari projelerinin değişiklik ve revizyonlarına esas olmak üzere bunların özgün fikir ifade edip etmediğini tespit etme yetkisi tanınmıştır.

142. Her türlü yapı ve mimari projenin eser niteliğine sahip olmadığı, bunların eser niteliğine sahip olabilmesi için özgün olması, bir başka ifadeyle, sahibinin hususiyetini taşıması gerektiği tartışmasızdır. Bu nedenle dava konusu kuralla özgün niteliği olmayan, dolayısıyla sahibine özgülenmesi ve eser olarak nitelendirilmesi mümkün bulunmayan yapılarda ve bunların mimari projelerinde yapılacak değişiklik ve revizyonlarda ilk müellifin görüşünün aranmayacağına düzenlenmesinde, fikri mülkiyet hakkına bir sınırlama getirilmediği ve düzenlemenin Devletin sanat faaliyetlerini ve sanatçıyı koruma görevine aykırı düşen bir yönünün bulunmadığı açıktır.

143. Kuralla sadece özgün fikir ifade etmeyen, dolayısıyla eser niteliği bulunmayan yapı ve mimari projelerin değil, bu niteliğe sahip olanlar yönünden de ilk müellifin izninin aranmayacağı durumlara yer verilmiş ve bu yönden fikri mülkiyet hakkına bir sınırlama getirilmiştir. Fakat bu sınırlama

getirilirken, yapı ve bunların onaylı mimari projelerinin tümünde değil, sadece eserin bütünlüğünü bozmadığına, estetik görünümünü değiştirmedikine, teknik, yönetsel amaçlar ve kullanım amacı nedeniyle zorunlu olduğuna karar verilenlere ilişkin değişiklik ve revizyonlarda ilk müellifin izninin aranmayacağı belirtilmiştir. Bu nedenle sınırlamanın, kişilerin mülkiyet hakkını bütünüyle ortadan kaldırmadığı veya ciddi surette güçleştirip amacına ulaşmasına engel olmadığı açıktır.

144. Kuralla yapı ve onaylanmış mimari projelerde teknik, yönetsel amaçlar ve kullanım amacı nedeniyle zorunlu olan değişikliklerin yapılması, dolayısıyla kamu yararı amacıyla, mülkiyet hakkına bir sınırlama getirilmekte olup bu sınırlama, demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır.

145. Bu şekilde, demokratik toplum düzeni bakımından alınması gerekli tedbirler kapsamında kişilerin mülkiyet hakkı sınırlandırılırken, Kanun'da sınırlama aracının sınırlama amacına uygun ve orantılı şekilde kullanılmasını sağlayacak yasal güvencelere yer verilmiş, böylece kişilerin mülkiyet hakkının korunması ile yapı ve mimari projelerde teknik, yönetsel amaçlar ve kullanım amacı nedeniyle zamanla ortaya çıkan değişiklik ihtiyacının giderilmesi biçimindeki kamu yararı arasında makul denge de kurulmuştur.

146. Bu bağlamda, kuralda sadece eserin bütünlüğünü bozmadığına, estetik görünümünü değiştirmedikine, teknik, yönetsel amaçlar ve kullanım amacı nedeniyle zorunlu olduğuna karar verilen değişikliklerin müellifin izni alınmaksızın yapılabilmesine imkân tanınmış ve bu hallerde eser sahibine telif ücretinin ödeneceği açıkça belirtilmiştir.

147. Ancak bu düzenleme yapılırken müellif tarafından talep edilebilecek telif ücretinin; ilgili meslek odasının belirlenen mimari proje asgari hizmet bedelinin, tamamlanan yapılarda yüzde yirmisini, inşaatı süren yapılarda yüzde on beşini geçemeyeceği belirtilmek suretiyle sözleşme hürriyetine bir sınırlama getirildiğinden, bu sınırlamanın da Anayasa'nın 13. maddesinde belirtilen güvencelere uygun olarak yapılıp yapılmadığının incelenmesi gerekmektedir.

148. Anayasa'nın 48. maddesinde, herkesin dilediği alanda çalışma ve sözleşme hürriyetine sahip olduğu belirtilmiş ve maddede bu hürriyetin sınırlandırılmasına ilişkin herhangi bir nedene yer verilmemiştir. Ancak daha önce de belirtildiği üzere düzenlendiği maddede hiçbir sınırlama nedenine yer verilmeyen haklar da mutlak olmayıp bunların diğer anayasal hükümler nedeniyle sınırlandırılması mümkün bulunmaktadır.

149. Anayasa'nın 17. maddesinde herkesin maddi ve manevi bütünlüğünü koruma hakkına sahip olduğu ifade edilmiş; 5. maddesinde kişilerin maddi ve manevi bütünlüğünü koruma ve geliştirme

görevi bir ödev olarak Devlete yüklenmiş; 56. maddesinde ise herkesin, sağlıklı ve dengeli bir çevrede yaşama hakkına sahip olduğu ve çevreyi geliştirme, çevre sağlığını koruma ve çevre kirlenmesini önlemenin Devletin ve vatandaşların ödevi olduğu vurgulanmıştır.

150. Dava konusu kuralda yapı ve onaylanmış mimari projelerde teknik, yönetsel amaçlar ve kullanım amacı nedeniyle zorunlu olan değişikliklerin yapılması, dolayısıyla sağlıklı, güvenli, düzenli, kullanışlı ve estetik bir kent dokusunun kurulması ve geliştirilmesi amacıyla sözleşme hürriyetine bir sınırlama getirilmektedir. Bu sınırlama, kişilerin maddi ve manevi varlıklarının korunması/geliştirilmesi ve herkesin sağlıklı ve dengeli bir çevrede yaşamasının sağlanmasına yönelik önemleri içerdiğinden, demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır.

151. Bu şekilde, demokratik toplum düzeni bakımından alınması gerekli tedbirler kapsamında kişilerin sözleşme hürriyeti sınırlandırılırken, Kanun'da hakkın özünün zedelenmesini önleyecek ve sınırlama aracının sınırlama amacına uygun ve orantılı şekilde kullanılmasını sağlayacak yasal güvencelere yer verilmiş, böylece kişilerin sözleşme hürriyetinin korunması ile kişilerin maddi ve manevi varlıklarının korunması/geliştirilmesi ve sağlıklı bir çevrede yaşama hakkı arasındaki makul denge de kurulmuştur.

152. Bu bağlamda, kuralda sadece eserin bütünlüğünü bozmadığına, estetik görünümünü değiştirmedigine, teknik, yönetsel amaçlar ve kullanım amacı nedeniyle zorunlu olduğuna karar verilen değişikliklerin telif ücreti sınırlamasına tabi olabileceği düzenlenmiş, fakat bu hâllerde dahi eser sahibine ödenecek telif ücretinin ilgili meslek odasınınca belirlenen mimari proje asgari hizmet bedelinin; tamamlanan yapılarda yüzde yirmisine, inşaatı süren yapılarda ise yüzde on beşine kadar belirlenebileceği düzenlenerek söz konusu hürriyetin özünün zedelenmesi önlenmiş ve ölçülü şekilde sınırlandırılması sağlanmıştır.

153. Öte yandan, anılan telif ücreti sınırlamasının makul nedenlere dayandığı anlaşılmaktadır. Zira söz konusu yapı ve mimari projelerde telif ücreti sınırlaması getirilen değişiklikler, ya teknik, yönetsel amaçlar ve kullanım amacı nedeniyle bir zorunluluğa dayanmakta veya eserin bütünlüğünü bozmayan ve estetik görünümünü değiştirmeyenleri oluşturmaktadır. Bunlardan teknik, yönetsel amaçlar ve kullanım amacı nedeniyle zaruri olanlarda değişiklik yapılması zorunlu olup eser sahibinin bu zorunluluğu istismar ederek yüksek telif ücreti talep etmesi önlenmek istenmiştir. Eserin bütünlüğünü bozmayan ve estetik görünümünü değiştirmeyenlerde ise önemli bir değişiklik yapılmayacağından bu konuda bir sınırlama getirilmesi işin esasına uygun düşmektedir.

154. Açıklanan nedenlerle kural, Anayasa'nın 2., 7., 13., 35., 48., 64. ve 123. maddelerine aykırı değildir. İptal talebinin reddi gerekir.

155. Kuralın, Anayasa'nın 10., 36. ve 90. maddeleriyle ilgisi görülmemiştir.

b2- Bentte Yer Alan " eser sözleşmesinde işleme izni verilenler ile " İbaresini

156. Dava konusu ibarenin de yer aldığı kuralda, eser sözleşmesinde işleme izni verilen mimarlık eser ve projelerinde müellifin izni alınmaksızın değişiklik yapılabileceği, bu durumda ilk müellif tarafından talep edilebilecek telif ücretinin ilgili meslek odasının belirlenen mimari proje asgari hizmet bedelinin; tamamlanan yapılarda yüzde yirmisini, inşaatı süren yapılarda ise yüzde on beşini geçemeyeceği düzenlenmektedir.

157. Belirtildiği üzere fikri ve sınai mülkiyet haklarını düzenleyen 5846 sayılı Kanun'un 14. maddesi uyarınca, fikir ve sanat eserleri üzerinde eseri meydana getiren eser sahiplerine " manevi ve mali haklar " üst başlıkları altında çeşitli haklar tanınmıştır.

158. Bu çerçevede " eserde değişiklik yapılmasını men hakkı " manevi haklar içinde yer almakta ve Kanun'un 16. maddesi uyarınca eser sahibinin izni olmaksızın eserde değişiklik yapılmasını önlemek için, "işleme hakkı" mali haklar kapsamında kalmakta ve eser sahibine onu işlemek suretiyle faydalanma şeklinde münhasır bir hak tanımaktadır. Dolayısıyla başkasının bu eseri işlemesi için eser sahibinden işleme izni alması gerekmektedir.

159. Bu yönleriyle eserde değişiklik yapmakla, eseri işlemek farklı kavramlar olup 5846 sayılı Kanun'un 1/B maddesinin (c) bendi ve 6. maddesinin (1) numaralı fıkrası uyarınca işleme eser, " Diğer bir eserden istifade suretiyle vücuda getirilip de bu esere nispetle müstakil olmayan ve işleyenin hususiyetini taşıyan fikir ve sanat mahsullerini " ifade etmektedir. Bir diğer ifadeyle, öğretilerde de belirtildiği üzere işlemede, başka bir eserden faydalanılarak ikinci bir eser meydana getirilmekte ve işleme eser, esas eseri özünde taşımakla birlikte işleyenin hususiyetini katmasıyla esas eserden başka, yeni bir eser olarak ortaya çıkmaktadır. Oysa eser değişikliğinde, bir eserden faydalanılarak yeni bir eser ortaya çıkarılması değil, mevcut eser üzerinde değişiklik yapılması söz konusu olmaktadır. Yani eser değişikliğinde, önceki eserin özünün korunması mecburiyeti bulunmadığı gibi, yapılacak değişikliğin yeni bir esere vücut vermesi de gerekmemektedir. Bu nedenle değişiklik izni ile işleme izni verilmesinin çok farklı sonuçları bulunmakta olup işleme izni değişiklik izninden çok daha dar kapsamlı ve eserin özünü koruyan bir nitelik arz etmektedir. Dolayısıyla işleme izni verilmesiyle eserde değişiklik izninin de verildiği kabul edilemez.

160. 5846 sayılı Kanun'un 2. maddesinin birinci fıkrasının (3) numaralı ve 4. maddesinin birinci fıkrasının (3) numaralı bentlerinde, her nevi proje, ilim ve edebiyat eseri; mimarlık eserleri ise güzel sanat eseri olarak nitelendirilmiştir. Dolayısıyla dava konusu kuralda belirtilen mimarlık eser ve projeleri de eser niteliğini haiz olup eser sahiplerinin bunlar üzerinde fikri mülkiyet haklarının bulunduğu ve bu eserlerin değişikliğinde eser sahibinden değişiklik izninin alınması gerektiği açıktır.

161. Anayasa'nın 35. maddesinde güvence altına alınan mülkiyet hakkı, mutlak olmayıp kamu yararı nedeniyle sınırlandırılabilir ve mimarlık eser ve projelerinde değişiklik yapılmasında bazı hallerde kamu yararı bulunabilir ise de kamu yararının bulunması tek başına bu hakkın sınırlandırılması için yeterli değildir. Bunun için temel hak ve özgürlüklerin sınırlandırılması rejimini belirleyen Anayasa'nın 13. maddesindeki güvencelere de uyulması gerekmektedir.

162. Bu güvencelerin en önemlilerinden biri olan ölçülülük ilkesi uyarınca, bir hakkın sınırlandırılabilmesi için sınırlama amacı ile aracı arasında hakkaniyete uygun bir dengenin bulunması, yasal önlemin sınırlama amacına ulaşmaya elverişli olması, amaç ve aracın ölçülü bir oranı kapsamı ve sınırlayıcı önlemin demokratik toplum düzeni bakımından zorunluluk taşıması gerekmektedir.

163. Dava konusu ibarenin de yer aldığı kuralda, eser sözleşmesinde işleme izni verilen mimarlık eser ve projelerinde müellifinin izni alınmaksızın değişiklik yapılabileceği belirtilmekle eser sahibinin fikri mülkiyet hakkına açık bir sınırlama getirilmektedir. Ancak bu sınırlama yapılırken, eser sahibinin mali hakları kapsamında verdiği " eserde işleme izni ", manevi haklarından olan " eserde değişiklik yapılmasını men etme hakkı "nı kısıtlayacak şekilde kullanılmakta, dolayısıyla sınırlama amacı ile ilgisiz, orantısız ve hakkaniyete aykırı bir sınırlama aracı kullanılarak fikri mülkiyet hakkına ölçüsüz bir müdahalede bulunulmaktadır.

164. Açıklanan nedenlerle dava konusu ". eser sözleşmesinde işleme izni verilenler ile. " ibaresi, Anayasa'nın 2., 13. ve 35. maddelerine aykırıdır. İptali gerekir.

165. Kuralın Anayasa'nın 7., 10., 36., 64., 90. ve 123. maddeleri ile ilgisi görülmemiştir.

H- Kanun'un 73. Maddesinin (p) Fıkrasının (3) Numaralı Bendiyle Değiştirilen 3194 Sayılı Kanun'un Ek 4. Maddesinin İncelenmesi

1- Maddenin Birinci Fıkrası

a- İptal Talebine İlişkin Gerekçe

166. Dava dilekçesinde özetle, dava konusu kurallarla mera, yaylak ve kışlakların amaç dışı kullanılmak üzere yerleşme ve yapılaşmaya açılmasına izin verildiği, bunun anılan yerlerin tahrip edilmesine, bu alanların daraltılmasına ve hayvansal üretimin düşmesine neden olacağı belirtilerek kuralların, Anayasa'nın 45. maddesine aykırı olduğu ileri sürülmüştür.

b- Anayasa'ya Aykırılık Sorunu

167. 6216 sayılı Kanun'un 43. maddesine göre, ilgisi nedeniyle dava konusu kural Anayasa'nın 56. maddesi yönünden de incelenmiştir.

168. Dava konusu kuralla mera, yaylak ve kışlakların uygun görülen kısımlarının, il genelindeki toplam mera, yaylak ve kışlakların binde beşini geçmemesi kaydıyla geçici yerleşme yeri olarak ve geleneksel kullanım amacıyla mera, yaylak ve kışlak vasfından çıkarılıp Hazine adına tescil edilmesine ve talep sahiplerine bedeli karşılığında yirmi dokuz yıla kadar tahsis edilebilmesine imkân tanınmaktadır.

169. Anayasa'nın " Tarım, hayvancılık ve bu üretim dallarında çalışanların korunması " başlıklı 45. maddesinde, " Devlet tarım arazileri ile çayır ve meraların amaç dışı kullanılmasını ve tahribini önlemek için gereken tedbirleri alır. " hükmüne yer verilmiş, maddenin gerekçesinde ise " Madde, Devlete tarım arazilerinin ve çayırlarla meraların amaç dışı kullanılmasını önleme görevini yüklemektedir. Bu ifadeyle amaçlanan tarım arazilerinin endüstri ve şehirleşme sebebiyle yok edilmesinin önlenmesidir. Devlet, bu amaçla yasal düzenleme yapmalıdır. " denilmiştir. Dolayısıyla çayır ve meraların amaç dışı kullanılmasının ve tahribinin önlenmesinin Devlete bir görev olarak yüklendiği açıktır. Bununla birlikte, Anayasa Mahkemesinin kimi kararlarında belirtildiği üzere, bu görevin yerine getirilmesi için gerekli tedbirlerin türü ile uygulanma yöntemi kanun koyucunun takdirine bırakılmıştır.

170. Anayasa'nın 56. maddesinde ise herkesin, sağlıklı ve dengeli bir çevrede yaşama hakkına sahip olduğu belirtilmiş; çevreyi geliştirmek, çevre sağlığını koruma ve çevre kirlenmesini önlemenin Devletin ve vatandaşların ödevi olduğu vurgulanmıştır.

171. 4342 sayılı Kanunla Anayasa'nın 45. maddesinde belirtilen yerlere ilişkin korumanın nasıl sağlanacağı düzenlenmiştir. Bu kapsamda anılan Kanun'un 14. maddesinde, mera, yaylak ve kışlaklardan Kanun'da gösterilenden başka şekilde yararlanılamayacağı belirtilmiş ve Kanunla buralarda inşaat yapılması yasaklandığı gibi bu yerlerin yerleşim yeri olarak iskâna açılmasına da izin verilmemiştir. Bu düzenlemelerin Anayasa'nın 45. maddesinde belirtilen mera ve çayırların amaç dışı kullanılmasının ve tahribinin önlenmesi bakımından gerekli olduğu, bu yerleri başka türlü

korumanın zor olduđu ve bu yerlerin korunamamasının hem yöre halkının geçim kaynaklarından olan hayvancılığı hem de Anayasa'nın 56. maddesinde güvence altına alınan çevreyi olumsuz yönde etkileyeceđi açıktır.

172. Bununla birlikte kanun koyucunun Devletin Anayasa'da belirtilen görevlerini yerine getirmek amacıyla, bir başka ifadeyle, kamu yararının zorunlu kıldığı durumlarda Anayasa'nın 45. maddesinde belirtilen ve 4342 sayılı Kanunla koruma altına alınan yerlere ilişkin tasarrufta bulunması ve bunların tahsis amacını deđiştirmesi de mümkün bulunmaktadır. Ancak bunu yaparken anılan yerlerin tahsis amacının deđiştirilmesini gerekli kılan kamu yararı ile anılan yerlerin amaç dışı kullanılmasının ve tahribinin önlenmesi biçimindeki kamu yararı arasındaki makul dengenin kurulması gerekir.

173. Dava konusu kurala göre mera, yaylak ve kışlakların geleneksel kullanım amacıyla geçici yerleşme yeri olarak uygun görülen kısımları il genelindeki toplam mera, yaylak ve kışlakların binde beşini geçmemesi kaydıyla mera, yaylak ve kışlak vasfından çıkarılıp Hazine adına tescil edilebilecek ve talep sahiplerine bedeli karşılığında yirmi dokuz yıla kadar tahsis edilebilecektir.

174. Kuralda, bu yerlerin tahsis amacının deđiştirilmesini gerekli kılan nedenin ne olduđu belirtilmemiştir. Maddenin kanunlaşmadan önceki KHK gerekçesinde ise düzenlemenin amacının " mera, yaylak ve kışlak gibi alanların sosyo-ekonomik ve sosyo-kültürel durumu gözetilerek buralarda yapılaşma ile ilgili usul ve esasları " düzenlemek olduđu belirtilmiştir. Ancak gerekçede, bu yerlerin yapılaşmaya açılmasını gerekli kılan sosyo-ekonomik ve sosyo-kültürel nedenin ne olduđu açıklanmamıştır.

175. Yasama belgeleriyle birlikte kuralın lafzı ve gerekçesi dikkate alındığında, dava konusu kuralın düzenlenme amacının; mera, yaylak ve kışlaklarda yapılaşmanın önlenememesi nedeniyle buralarda mevcut yerleşmelere hukuki statü kazandırmak ve böylece daha önce bedelsiz olarak kullanılan yerleri bedeli karşılığında ve geleneksel amacına uygun olarak kullanılmak üzere isteklilere tahsis etmek olduđu anlaşılmaktadır.

176. Mera, yaylak ve kışlaklarda kanuna aykırı yapıların önlenememesi veya buralarda inşa edilen yapılardan veya yerleşmelerden ekonomik gelir temin edilmesi nedenleriyle mera, yaylak ve kışlakların tahsis amacının deđiştirilerek Anayasa'nın 45. ve 56. maddeleriyle güvence altına alınan yerlerin ve doğal çevrenin tahrip edilmesinde, kamu yararının gerektirdiđi bir zorunluluđun bulunmadığı ve bunun Anayasa'nın 45. ve 56. maddeleriyle Devlete yüklenen ödevin yerine getirilmesi imkânını önemli ölçüde ortadan kaldıracığı açıktır. Zira kanuna aykırı yapıların önlenememesi gerekçesiyle yapı sahiplerine hak tanınması, bu yerlerin tümüyle yok olmasına neden

olacak, dolayısıyla Anayasa'nın Devlete bu yerleri korumaya yönelik olarak yüklediği görev yerine getirilemeyecektir. Ekonomik gelir temininde ise Devletin aynı geliri doğal çevrenin geri dönüşü olmayacak biçimde tahrip edilmesine yol açmayacak alternatif faaliyetlerden elde etmesi mümkün bulunduğundan mera, yaylak ve kışlakların yapılaşmaya açılmasını gerektirecek bir zorunluluğun varlığından söz etmek mümkün değildir. Dolayısıyla kamu yararının gerektirdiği bir zorunluluğa dayanmaksızın dava konusu kuralla Anayasa'nın 45. ve 56. maddeleriyle güvence altına yerlerin ve çevrenin tahribine neden olacak düzenlemeler yapılması, Anayasa'ya aykırılık teşkil etmektedir.

177. Ayrıca, kuralda bu yerlerin sadece geleneksel kullanım amacıyla, yani sadece hayvanların otlatılması ve barındırılması amacıyla tahsis edileceği belirtilmişse de Kanun'da bu amacın gerçekleşmesine yönelik önlemlere yer verilmemesi ve aksine söz konusu tahsisten yörede oturan ve öteden beri hayvancılıkla uğraşan çiftçilerle sınırlı olmayacak biçimde istekli olan herkesin yararlandırılacağına öngörülmüş olması karşısında bu amacın da gerçekleşme imkânının sağlanamadığı görülmektedir.

178. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 45. ve 56. maddelerine aykırıdır. İptali gerekir.

2- Maddenin İkinci Fıkrası

179. Dava konusu kuralla mera, yaylak ve kışlakların 2634 sayılı Kanun uyarınca ilan edilen turizm merkezleri ile kültür ve turizm gelişim bölgeleri kapsamında kalan kısımlarının, tahsis amacı değiştirilerek tapuda Hazine adına tescil edileceği ve bu yerlerin, 2634 sayılı Kanun çerçevesinde kullanılmak ve değerlendirilmek üzere Kültür ve Turizm Bakanlığına tahsis edileceği düzenlenmektedir.

180. 2634 sayılı Kanun uyarınca bir bölgenin turizm potansiyelinin yüksek olduğunun Bakanlığın önerisi ve Bakanlar Kurulu kararıyla tespit edilmesi halinde tümüyle kültür ve turizm koruma ve gelişim bölgesi veya turizm merkezi ilan edilmesi mümkün bulunmaktadır. Dava konusu kuralla bir bölgenin kültür ve turizm koruma ve gelişim bölgesi veya turizm merkezi ilan edilmesi halinde söz konusu bölgede bulunan mera, yaylak ve kışlaklar ne kadar büyük ve ne kadar geniş bir çiftçi kesiminin ihtiyacını karşılar nitelikte olursa olsun bunların mera, yaylak ve kışlak vasfından tümüyle çıkarılması mümkün hale gelmektedir.

181. Milli gelirin artırılması, dolayısıyla halkın genel refah düzeyinin yükseltilmesi amacıyla turizm yatırımlarının yapılması ve bu çerçevede mera, yaylak ve kışlakların tahsis amacının değiştirilmesinde kamu yararının bulunduğu açık ise de bu yararın Anayasa'nın 45. ve 56.

maddeleriyle devlete yüklenen çayır ve meralar ile çevrenin korunması yönündeki ödevi ortadan kaldırması söz konusu olamaz. Bu nedenle turizm yatırımları yoluyla milli gelirin arttırılması şeklindeki kamu yararı ile çayır, meralar ve çevrenin korunmasına yönelik kamu yararı arasındaki makul dengenin kurulması gerekir.

182. Dava konusu kuralla kültür ve turizm koruma ve gelişim bölgesi veya turizm merkezi ilan edilen yerlerin sınırları içinde kalan mera, yaylak ve kışlakların herhangi bir sınırlamaya tabi olmaksızın tümüyle mera, yaylak ve kışlak vasfından çıkarılmasına olanak tanınması, Anayasa'nın 45. ve 56. maddeleriyle çayır, meralar ve çevrenin korunması yönünde devlete yüklenen görevin yerine getirilmesi imkânını ortadan kaldırmakta ve turizm yatırımları yoluyla milli gelirin arttırılması şeklindeki kamu yararı ile çayır, meralar ve çevrenin korunmasına yönelik kamu yararı arasında bulunması gereken makul dengeyi çayır ve meralar ile çevrenin korunması aleyhine bozmaktadır.

183. Açıklanan nedenlerle dava konusu kural, Anayasa'nın 45. ve 56. maddelerine aykırıdır. İptali gerekir.

I- Kanun'un 73. Maddesinin (r) Fıkrasıyla Değiştirilen 3224 Sayılı Kanun'un 11. Maddesinin Birinci Fıkrasının (f) Bendinde, 26. Maddesinin Birinci Fıkrasının (e) Bendinde, 40. Maddesinin Başlığı ile Birinci ve İkinci Fıkralarında Yer Alan ".Rehber." İbarelerinin İncelenmesi

1- İptal Talebine İlişkin Gerekçe

184. Dava dilekçesinde özetle, dava konusu ibarelerle serbest çalışan dış hekimlerinin uygulayacakları muayene ve tedavi ücretlerine ilişkin "asgari ücret tarifesi"nin "rehber ücret tarifesi"ne dönüştürüldüğü, dolayısıyla hekimlerin tarifeye uyma mecburiyetinin ortadan kaldırıldığı, bunun hekimler arasında ücret üzerinden rekabet yapılmasına neden olacağı, verilecek sağlık hizmetinin kalitesini düşürerek kişilerin nitelikli sağlık hizmeti almalarını önleyeceği ve meslek kuruluşu olan Türk Dış Hekimleri Birliğinin (TDB) üyeleri üzerindeki denetim yetkisini sınırlayacağı belirtilerek kuralın, Anayasa'nın 2., 5., 56., 60. ve 135. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

185. Dava konusu düzenlemelerle serbest çalışan dış hekimlerinin uygulayacakları muayene ve tedavi ücretlerine ilişkin " asgari ücret tarifesi ", "rehber ücret tarifesi"ne dönüştürülmekte, böylece serbest çalışan dış hekimlerinin sundukları hizmet karşılığında alacakları ücreti, herhangi bir sınırlamaya tabi olmaksızın serbestçe belirlemeleri imkânı sağlanmaktadır.

186. 6216 sayılı Kanun'un 43. maddesine göre dava konusu kurallar ilgisi nedeniyle Anayasa'nın 17. maddesi yönünden de incelenmiştir.

187. Anayasa'nın 17. maddesinin birinci fıkrasında " Herkes, yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkına sahiptir. " denilerek, kişinin yaşam ve vücut dokunulmazlığı güvence altına alınmıştır. İnsanın hastalıklara yakalanması veya çeşitli nedenlerle yaralanması mümkün olup kişinin bu hastalıklardan ve yaralanmalardan kurtulmayı istemesi de, bir başka ifadeyle "sağlık hakkı" da kişinin " yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkı " kapsamında kalmaktadır.

188. Anayasa'nın 56. maddesinin üçüncü ve dördüncü fıkralarında, " Devlet, herkesin hayatını, beden ve ruh sağlığı içinde sürdürmesini sağlamak; insan ve madde gücünde tasarruf ve verimi artırarak, işbirliğini gerçekleştirmek amacıyla sağlık kuruluşlarını tek elden planlayıp hizmet vermesini düzenler. Devlet, bu görevini kamu ve özel kesimlerdeki sağlık ve sosyal kurumlarından yararlanarak, onları denetleyerek yerine getirir. " hükümlerine yer verilerek, Devlete sağlık hizmetlerini herkesin hayatını beden ve ruh sağlığı içinde sürdürmesini sağlayacak şekilde düzenleme ve denetleme görevi yüklenmiştir.

189. Anılan hükümler gözetildiğinde, kişinin yakalandığı hastalıklardan kurtulması veya hayatını beden ve ruh sağlığı içinde sürdürmesini temin etmek üzere gerekli düzenlemelerin yapılarak kişinin sağlık hizmetlerinden etkin ve verimli bir şekilde yararlanmasını sağlamanın, Devletin anayasal bir yükümlülüğü olduğu açıktır.

190. Ağız ve diş sağlığına ilişkin olarak serbest diş hekimlerinin sunacakları hizmetlerle ilgili asgari bir ücret tarifesinin belirlenmesi ise bu alandaki sağlık hizmetlerinin etkin ve verimli olarak sunulabilmesinin zorunlu bir şartını oluşturmamakta; kanun koyucunun bu hizmetler konusunda serbest diş hekimleri yönünden asgari bir ücret tarifesi belirleyip belirlememesi takdir yetkisi kapsamında kalmaktadır.

191. Bu çerçevede kanun koyucunun dava konusu kurullarla serbest diş hekimlerinin sundukları sağlık hizmetleri yönünden uyulması zorunlu asgari bir ücret tarifesi belirleme uygulamasından vazgeçerek, bunun yerine uyulması ihtiyari olan bir rehber ücret tarifesi öngörmesinde, kişinin yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkına veya Devletin sağlık hizmetlerinin herkesin hayatını beden ve ruh sağlığı içinde sürdürmesini sağlayacak şekilde düzenleme ve denetleme yapma görevine aykırı düşen bir yön bulunmamaktadır.

192. Öte yandan Anayasa'nın " Kamu kurumu niteliğindeki meslek kuruluşları" başlıklı 135. maddesinin birinci fıkrasında, "Kamu kurumu niteliğindeki meslek kuruluşları ve üst kuruluşları; belli bir mesleğe mensup olanların müşterek ihtiyaçlarını karşılamak, meslekî faaliyetlerini kolaylaştırmak, mesleğin genel menfaatlere uygun olarak gelişmesini sağlamak, meslek

mensuplarının birbirleri ile ve halk ile olan ilişkilerinde dürüstlüğü ve güveni hâkim kılmak üzere meslek disiplini ve ahlâkını korumak maksadı ile kanunla kurulan ve organları kendi üyeleri tarafından kanunda gösterilen usullere göre yargı gözetimi altında, gizli oyla seçilen kamu tüzelkişilikleridir. " denilerek, kamu kurumu niteliğindeki meslek kuruluşlarının hangi amaçlar doğrultusunda faaliyet gösterecekleri ve hangi usulle kurulacakları hükme bağlanmıştır.

193. Meslek kuruluşlarının üyelerinin sağladığı hizmetlere ilişkin olarak ücret tarifeleri belirlemesi de, anılan hükümde belirtilen meslekî faaliyetleri kolaylaştırmak, mesleğin genel menfaatlere uygun olarak gelişmesini sağlamak, meslek mensuplarının birbirleri ve halk ile olan ilişkilerinde dürüstlüğü ve güveni hâkim kılmak üzere meslek disiplini ve ahlâkını koruma amaçları çerçevesinde yürütülen bir faaliyet olarak nitelendirilebilir. Ancak Anayasa'da meslek kuruluşlarına üyelerinin sundukları hizmete ilişkin olarak ücret tarifeleri belirlerken bağlayıcı nitelikte asgari ücret tarifesi belirleme görevi ve yetkisi verilmemiştir. Ayrıca objektif olarak bu şekilde bir ücret rejiminin belirlenmemesinin maddede anılan amaçların gerçekleşmesini önleyeceğini söylemek de mümkün görünmemektedir.

194. Esasen meslek kuruluşlarının üyeleri yönünden asgari bir ücret tarifesi belirlemelerinin, Anayasa'nın 135. maddesinde belirtilen amaçların gerçekleşmesine katkıda bulunup bulunmayacağı, objektif ve hukuki bir değerlendirmeyi değil, subjektif ve siyasi bir değerlendirmeyi gerektirmektedir. Bu değerlendirmeyi yapma yetkisi de Anayasa'nın 2. maddesinde ifadesini bulan demokratik yönetim ilkesi uyarınca kanun koyucunun takdirinde kalmaktadır.

195. Açıklanan nedenlerle dava konusu kurallar, Anayasa'nın 2., 17., 56. ve 135. maddelerine aykırı değildir. İptal taleplerinin reddi gerekir.

196. Kuralların, Anayasa'nın 60. maddesiyle ilgisi görülmemiş, 5. madde yönünden ise inceleme yapılmasına gerek görülmemiştir.

İ- Kanun'un 73. Maddesinin (bb) Fıkrasıyla Değiştirilen 6004 Sayılı Kanun'un 12. Maddesinin (2) Numaralı Fıkrasının (d) Bendi ve (3) Numaralı Fıkrasının (a) Bendine Eklenen Cümlelerin İncelenmesi

1- İptal Talebine İlişkin Gerekçe

197. Dava dilekçesinde özetle, dava konusu kurallarla 657 sayılı Kanun'un 59. maddesine göre diğer kamu idarelerinden veya açıktan büyükelçilik veya daimi temsilcilik görevlerine atananların merkeze döndüklerinde Dışişleri Bakanlığında çalışmaya devam ederek meslek mensubu büyükelçiler gibi büyükelçi unvanlarını kazanılmış hak olarak korumalarının, meslek mensubu büyükelçilerle mesleki kariyer ve liyakata dayalı müsteşarlık, müsteşar yardımcılığı, genel müdürlük gibi idari kadrolara

atanma dahil aynı kurallara tabi olmalarının ve aynı haklardan yararlanmalarının öngörüldüğü, büyükelçilik ve daimi temsilcilik görevleri hükümetin dış politikasının yürütülmesine ilişkin siyasi görevler olduğundan bu görevlere 657 sayılı Kanun'daki atama, sınavlar, kademe ilerlemesi ve derece yükselmesine ilişkin hükümlerle bağlı olmaksızın atama yapılması hukuka uygun ise de buraya atanan kişilerin merkeze döndüklerinde Bakanlıkta çalışmaya devam ederek meslek mensubu büyükelçiler gibi büyükelçi unvanına bağlı tüm hakları kullanabilmelerinin ve büyükelçilerin atanabildikleri üst düzey idari kadrolara atanabilmelerinin adalet ve hakkaniyete aykırı olduğu, zira bu görevlerin siyasi değil, kariyer ve liyakat esaslarına göre yürütülen bürokratik görevler olduğu, bu durumun aynı zamanda atama, sınavlar, kademe ilerlemesi ve derece yükselmesine ilişkin hükümlere tabi meslek mensupları aleyhine eşitsizlik yarattığı belirtilerek kuralların, Anayasa'nın 2., 10. ve 70. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

198. Dava konusu kurallarda, 657 sayılı Kanun'un 59. maddesi çerçevesinde büyükelçi ve daimi temsilci olarak atanarlardan Bakanlığa veya diğer kamu kurum ve kuruluşlarına mensup olanlar ile açıktan atanarlardan, merkeze döndüklerinde Bakanlıkta çalışabilecekleri, Bakanlıktaki görevleri süresince büyükelçi unvanını kullanmaya devam edecekleri ve Bakanlıkta yönetici kadrolarına atanma dâhil meslek mensubu olanlar arasından büyükelçiliğe atanarlardan aynı hükümlere tâbi olacakları ve aynı haklardan yararlanacakları düzenlenmektedir.

199. Kaynağını Anayasa'nın 7. maddesinden alan yasama yetkisinin genelliği ilkesi uyarınca, kanun koyucu Anayasa'ya aykırı olmamak kaydıyla dilediği konuda düzenleme yapma hususunda takdir yetkisine sahip bulunmaktadır. Ancak kanunların kamu yararının sağlanması amacına yönelik olması, genel, objektif, adil kurallar içermesi ve hakkaniyet ölçütlerini gözetmesi, Anayasa'nın 2. maddesinde tanımlanan hukuk devletinin bir gereği olup kanun koyucunun kendisine tanınan takdir yetkisini anayasal sınırlar içinde adalet, hakkaniyet ve kamu yararı ölçütlerini göz önünde tutarak kullanması gerekir.

200. 657 sayılı Devlet Memurları Kanunu'nun " İstisnai memurluklar " başlıklı 59. maddesinde, valilik, bakan yardımcılığı gibi sayma yoluyla belirtilen bazı istisnai memurluklara, 657 sayılı Kanun'da belirtilen atama, sınavlar, kademe ilerlemesi ve derece yükselmesine ilişkin hükümlere bağlı olmaksızın atama yapabilme hususunda yürütme organına yetki verilmiştir. Demokratik yöntemlerle yönetim yetkisini kazanan ve halka hesap verme sorumluluğu bulunan yürütme organına kamu hizmetlerini düzenleyebilme ve sunma amacıyla verilen bu yetkinin kamu yararıyla çelişen bir yönü bulunmamaktadır.

201. Dava konusu kurallara konu büyükelçilik ve daimi temsilcilik unvanları da 657 sayılı Kanun'un 59. maddesinde sayılan istisnai memurluklar kapsamında kalmakta olup 6004 sayılı Kanun'un 12. maddesi uyarınca büyükelçi atandığı ülkede Türkiye Cumhuriyeti Devletini, Cumhurbaşkanını ve Hükümetini, daimi temsilci ise ilgili uluslararası kuruluşta Türkiye Cumhuriyeti Hükümetini temsil etmek üzere atanmaktadır. Görev yaptığı ülkede büyükelçiliğe bağlı tüm birimlerin amiri olan, büyükelçiliğe bağlı olmayan diğer kamu kurum ve kuruluşlarının ise gözetimiyle yetkili bulunan büyükelçilerin ve uluslararası kuruluşlarda hükümeti en üst düzeyde temsil eden daimi temsilcilerin, önemli görevler yürüttükleri konusunda bir tereddüt bulunmamakta ve bu kişiler bu statülere geçici veya sözleşmeli olarak değil, bu unvanların sağladığı tüm hak ve yetkilerle birlikte kadrolarıyla atanmaktadır.

202. Bu kadar önemli görevlere tüm hak ve yetkileriyle atanıp bu statüleri kazanan kişilerin merkeze alındıklarında yurt dışında taşıdıkları unvanlara ve bu unvanlara bağlı haklara yurt içinde de sahip olabilmeleri doğal olup kanun koyucunun takdir yetkisi kapsamında dava konusu kurallarla buna olanak tanınmasında, adalet ve hakkaniyet ölçülerine aykırı düşen bir yön bulunmamaktadır.

203. Öte yandan dava konusu kurallarla atama, sınavlar, kademe ilerlemesi ve derece yükselmesine ilişkin hükümlere tabi meslek mensupları aleyhine bir eşitsizlik yaratılması da söz konusu değildir. Zira dava konusu kurallarla yurt dışına büyükelçi ve daimi temsilci olarak atanan meslek mensuplarının merkeze döndüklerinde bu unvanları ve bu unvanlara bağlı hakları kullanmalarını önleyecek bir düzenleme öngörülmemekte, dolayısıyla aynı hukuki durumda bulunan kişiler yönünden farklı kuralların düzenlenmesi söz konusu olmamaktadır.

204. Yurt dışına atanacak büyükelçi ve daimi temsilcilerin belli koşulları taşıyan meslek mensuplarının yanı sıra bu koşulları taşımayan kişilerden atanabilmesi ise dava konusu kuralların değil, 657 sayılı Kanun'un 59. ve devamı maddelerindeki kuralların konusunu oluşturmaktadır.

205. Açıklanan nedenlerle dava konusu kurallar, Anayasa'nın 2. ve 10. maddelerine aykırı değildir. İptal taleplerinin reddi gerekir.

206. Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT ve Engin YILDIRIM bu görüşe katılmamışlardır.

207. Kuralların, Anayasa'nın 70. maddesiyle ilgisi görülmemiştir.

J- Kanun'un 73. Maddesinin (cc) Fıkrasıyla Değiştirilen, 6085 Sayılı Kanun'un 4. Maddesinin (1) Numaralı Fıkrasının (a) Bendinde Yer Alan ".% 50'den fazla olan." İbaresini ile (b) Bendinde Yer Alan "Kamu payı % 50'den az olmamak kaydıyla." İbaresinin İncelenmesi

1- İptal Talebine İlişkin Gerekçe

208. Dava dilekçesinde özetle, dava konusu düzenlemelerle Sayıştayın sermayesindeki kamu payı doğrudan veya dolaylı olarak % 50'den az olan anonim ortaklıkları ile merkezi yönetim bütçesi kapsamındaki kamu idareleri, sosyal güvenlik kurumları ve mahallî idarelerin kurdukları veya doğrudan doğruya ya da dolaylı olarak ortak oldukları her çeşit idare, kuruluş, müessese, birlik, işletme ve şirketlerden kamu payı % 50'nin altına düşmüş olanları, "ortaklık hakları yönüyle" denetleme görev ve yetkisinin ortadan kaldırıldığı, bu durumun demokratik hukuk devletinin gereklerinden olan saydamlık ve hesap verebilirlik ilkeleriyle örtüşmediği belirtilerek kuralların, Anayasa'nın 2. ve 160. maddelerine aykırı olduğu ileri sürülmüştür.

2- Anayasa'ya Aykırılık Sorunu

209. 6085 sayılı Kanun'un 4. maddesinde, Sayıştayın denetimine tabi kurum ve kuruluşlar arasında, özel kanunlar ile kurulmuş anonim ortaklıklar ile maddenin (a) bendinde sayılan idarelere bağlı veya bu idarelerin kurdukları veya doğrudan doğruya ya da dolaylı olarak bunların ortak oldukları her çeşit idare, kuruluş, müessese, birlik, işletme ve şirketler de sayılmış, ancak dava konusu ibarelerle anılan bu kuruluşların Sayıştay tarafından denetlenebilmesi için bunların sermayesindeki kamu payının % 50'den fazla olması kuralına yer verilerek Sayıştayın bu kuruluşlara ilişkin denetim yetkisi sınırlandırılmıştır.

210. Anayasa'nın "Sayıştay" başlıklı 160. maddesinin birinci fıkrasının ilk cümlesinde " Sayıştay, merkezi yönetim bütçesi kapsamındaki kamu idareleri ile sosyal güvenlik kurumlarının bütün gelir ve giderleri ile mallarını Türkiye Büyük Millet Meclisi adına denetlemek ve sorumluların hesap ve işlemlerini kesin hükme bağlamak ve kanunlarla verilen inceleme, denetleme ve hükme bağlama işlerini yapmakla görevlidir. " denilmiş; üçüncü fıkrasında, " Mahalli idarelerin hesap ve işlemlerinin denetimi ve kesin hükme bağlanması Sayıştay tarafından yapılır. " hükmüne yer verilmiş; 2. maddesinde ise Türkiye Cumhuriyetinin demokratik bir hukuk devleti olduğu vurgulanmıştır.

211. Buna göre, merkezi yönetim bütçesi kapsamındaki kamu idareleri ve sosyal güvenlik kurumlarının bütün gelir ve giderleri ile mallarının ve mahalli idarelerin hesap ve işlemlerinin denetimi ve kesin hükme bağlanması görevlerinin, Türkiye Büyük Millet Meclisi adına Sayıştay tarafından yerine getirilmesi gerekmektedir.

212. Anayasa'da, Sayıştay denetiminin kapsamı ve niteliğine ilişkin herhangi bir hüküm bulunmamasıyla birlikte bu denetimin, demokrasinin temel gereklerinden olan şeffaflık, saydamlık,

yasamanın yürütmeyi denetleme hakkı ve yürütmenin yasamaya ve halka hesap verme sorumluluğu anlayışına uygun olarak yapılması gerektiği açıktır.

213. Kuvvetler ayrılığı esasına dayanan demokratik yönetim biçiminde, yürütme organına gelir toplama ve harcama yetkisi tanıyan bütçelerin yapımı, halkın temsilcilerinden oluşan yasama organının asli görevlerindedir. Yasama organı açısından aynı zamanda bir hak olan bu görev, yürütmenin bütçe ile ilgili işlemlerinin doğru, güvenilir ve kanunlara uygun bir şekilde yürütülüp yürütülmediğinin denetimini de kaçınılmaz kılmaktadır. Bu bağlamda, yasama organının, halk adına kamu gelirlerini toplama ve yine halk adına bu gelirleri harcama konusunda yürütme organına sınırları belirlenmiş yetki vermesi ve sonuçlarını denetlemesine "bütçe hakkı" denilmektedir. Bütçe hakkı, vergi ve benzeri gelirlerle kamu harcamalarının çeşit ve miktarını belirleme ve onaylama hakkıdır. Bu hak, demokratik parlamenter yönetim sistemini benimsemiş olan ülkelerde, halk tarafından seçilen temsilcilerden oluşan ve en yetkili organ olan yasama organına ait bulunmaktadır. Anayasa'nın 87., 160., 162. ve 164. maddelerine göre bütçe hakkı TBMM'nindir. Bütçe, hükümetin Meclis'e karşı temel sorumluluk mekanizmasıdır. Meclis, bütçe ile hükümete gelir toplama ve gider yapma yetkisi vermekte, bu yetkinin uygun kullanılmasını da bütçe sürecinin bir parçası olan kesin hesap faaliyeti ile denetlemektedir. Bütçe uygulamalarının denetimi görevi, bütçe işlemlerinin gün geçtikçe nitelik ve nicelik itibarıyla artması ve karmaşıklaşması nedeniyle yasama organı adına tarafsız ve uzman kuruluşlar tarafından yerine getirilmektedir. Ülkemizde de bu görev, Anayasa'nın 160. maddesiyle Sayıştaya verilmiştir. Yasama organının, yürütme organı üzerindeki bütçe denetimi büyük ölçüde Sayıştay tarafından yapılan bu denetimlere dayanmaktadır. Dolayısıyla, yasama organının işlevini etkin ve sağlıklı bir biçimde yürütmesinde Sayıştay denetiminin önemi yadsınamaz. Öte yandan, Sayıştay denetimi, demokratik devlet ilkesinin bir gereği olarak yürütmenin, halka ve yasama organına hesap verme sorumluluğunun işlevselleştirilmesinin en önemli araçlarından biridir.

214. 6085 sayılı Kanun'un 4. maddesinde, Sayıştay'ın denetimine tabi kurum ve kuruluşlar arasında, sermayesinde kamu payı bulunan ve özel kanunlarla kurulmuş anonim ortaklıkları ile maddenin (a) bendinde sayılan idarelere bağlı veya bu idarelerin kurdukları veya doğrudan doğruya ya da dolaylı olarak bunların ortak oldukları her çeşit idare, kuruluş, müessese, birlik, işletme ve şirketler de sayılmış olmasına rağmen dava konusu ibarelerle anılan bu kuruluşların Sayıştay tarafından denetlenebilmesi için bunların sermayesindeki kamu payının % 50'den fazla olması kuralına yer verilmektedir. Bu durum, Sayıştay'ın anılan kamu kaynaklarının kullanımına ilişkin denetim yetkisini ortadan kaldırmakta, dolayısıyla yasama organının yürütmenin bütçe ile ilgili işlemlerini kanunlara

uygun bir şekilde yürütüp yürütmediğini denetleme imkânını sınırlayarak demokratik devlet ilkesine zarar vermektedir.

215. Açıklanan nedenlerle dava konusu ibareler, Anayasa'nın 2. ve 160. maddelerine aykırıdır. İptali gerekir.

216. Hicabi DURSUN, Muammer TOPAL ve M. Emin KUZ bu görüşe katılmamışlardır.

V- YÜRÜRLÜĞÜN DURDURULMASI TALEBİ

217. Dava dilekçesinde özetle, dava konusu kuralların Anayasaya açıkça aykırı olduğu ve yürürlüklerinin durdurulmaması halinde hukuk devleti yönünden giderilmesi olanaksız durum ve zararların ortaya çıkacağı, bu nedenle kuralların yürürlüklerinin durdurulmasına karar verilmesi gerektiği ileri sürülmüştür.

218. 12.7.2013 tarihli ve 6495 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un;

A- 1- 33. maddesiyle, 9.10.2003 tarihli ve 4982 sayılı Bilgi Edinme Hakkı Kanunu'nun 2. maddesine eklenen fıkra, 4.12.2014 tarihli ve E.2013/114, K.2014/184 sayılı kararla iptal edildiğinden, bu fıkranın, uygulanmasından doğacak, sonradan giderilmesi güç veya olanaksız durum ve zararların önlenmesi ve iptal kararının sonuçsuz kalmaması için kararın Resmî Gazete'de yayımlanacağı güne kadar YÜRÜRLÜĞÜNÜN DURDURULMASINA, OYBİRLİĞİYLE,

2- 73. maddesinin (h) fıkrasının (3) numaralı bendiyle değiştirilen 663 sayılı Kanun Hükmünde Kararname'nin 47. maddesinin (1), (2) ve (3) numaralı fıkraları, 4.12.2014 tarihli ve E.2013/114, K.2014/184 sayılı kararla iptal edildiğinden, bu fıkraların, uygulanmalarından doğacak, sonradan giderilmesi güç veya olanaksız durum ve zararların önlenmesi ve iptal kararının sonuçsuz kalmaması için kararın Resmi Gazete'de yayımlanacağı güne kadar YÜRÜRLÜKLERİNİN DURDURULMASINA, Burhan ÜSTÜN, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL ile M. Emin KUZ'un karşıoyları ve OYÇOKLUĞUYLA,

3- 73. maddesinin (p) fıkrasının (3) numaralı bendiyle değiştirilen 3194 sayılı Kanun'un ek 4. maddesi, 4.12.2014 tarihli ve E.2013/114, K.2014/184 sayılı kararla iptal edildiğinden, bu maddenin, uygulanmasından doğacak, sonradan giderilmesi güç veya olanaksız durum ve zararların önlenmesi ve iptal kararlarının sonuçsuz kalmaması için kararın Resmi Gazete'de yayımlanacağı güne kadar YÜRÜRLÜĞÜNÜN DURDURULMASINA, OYBİRLİĞİYLE,

B- 73. maddesinin (p) fıkrasının (1) numaralı bendiyle, 3.5.1985 tarihli ve 3194 sayılı İmar Kanunu'nun 8. maddesine eklenen (j) bendinin dördüncü cümlesinde yer alan ".eser sözleşmesinde işleme izni verilenler ile." ibaresine yönelik yürürlüğün durdurulması isteminin, koşulları oluşmadığından REDDİNE, OYBİRLİĞİYLE,

C- 73. maddesinin (cc) fıkrasıyla değiştirilen, 3.12.2010 tarihli ve 6085 sayılı Sayıştay Kanunu'nun 4. maddesinin (1) numaralı fıkrasının;

a- (a) bendinde yer alan ".% 50'den fazla olan." ibaresine,

b- (b) bendinde yer alan "Kamu payı % 50'den az olmamak kaydıyla." ibaresine,

yönelik iptal hükümlerinin yürürlüğe girmelerinin ertelenmeleri nedeniyle bu ibarelere ilişkin yürürlüğün durdurulması istemlerinin REDDİNE, OYBİRLİĞİYLE,

D- 1- 27. maddesiyle 2942 sayılı Kanun'un 25. maddesine eklenen fıkraya,

2- 43. maddesiyle, 22.6.2006 tarihli ve 5525 sayılı Memurlar ile Diğer Kamu Görevlilerinin Bazı Disiplin Cezalarının Affı Hakkında Kanun'a eklenen ek 1. maddenin;

a- Birinci fıkrasında yer alan "28/2/1997 tarihinden sonra." ibaresine,

b- İkinci fıkrasının ".1/1/1990 ile...657 sayılı Kanunun 125 inci maddesinin birinci fıkrasının (A) bendinin (g) alt bendinde yer alan fiili işlediği gerekçesiyle anılan Kanunun 56 ve 57 nci maddeleri uyarınca disiplin cezası veya olumsuz sicil almış olmaları nedeniyle." bölümüne,

3- 59. maddesiyle, 13.12.1983 tarihli ve 178 sayılı Maliye Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 43. maddesine eklenen fıkraya,

4- 73. maddesinin;

a- (h) fıkrasının (1) numaralı bendiyle değiştirilen, 11.10.2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 23. maddesinin (7) numaralı fıkrasının (c) ve (ç) bentlerine,

b- (p) fıkrasının (1) numaralı bendiyle, 3194 sayılı Kanun'un 8. maddesine eklenen;

ba- (ı) ve (i) bentlerine,

bb- (j) bendinin dördüncü cümlesinde yer alan ".eser sözleşmesinde işleme izni verilenler ile." ibaresi dışında kalan bölümüne,

c- (r) fıkrasının;

ca- (1) numaralı bendiyle değiştirilen, 7.6.1985 tarihli ve 3224 sayılı Türk Diş Hekimleri Birliđi Kanunu'nun 11. maddesinin birinci fıkrasının (f) bendinde yer alan ".rehber." ibaresine,

cb- (2) numaralı bendiyle değiştirilen 3224 sayılı Kanun'un 26. maddesinin birinci fıkrasının (e) bendinde yer alan ".rehber." ibaresine,

cc- (3) numaralı bendiyle değiştirilen 3224 sayılı Kanun'un 40. maddesinin başlığında yer alan "Rehber." ibaresi ile birinci ve ikinci fıkralarında yer alan ".rehber." ibarelerine,

d- (bb) fıkrasıyla, 7.7.2010 tarihli ve 6004 sayılı Dışışleri Bakanlıđının Kuruluş ve Görevleri Hakkında Kanun'un 12. maddesinin;

da - (2) numaralı fıkrasının değiştirilen (d) bendine,

db- (3) numaralı fıkrasının (a) bendine eklenen cümleye,

yönelik iptal istemleri, 4.12.2014 tarihli ve E.2013/114, K.2014/184 sayılı kararla reddedildiđinden, bu fıkralara bölümlere, bentlere, cümleye ve ibarelere ilişkin yürürlüđün durdurulması istemlerinin REDDİNE, OYBİRLİĞİYLE,

E- 1- 26. maddesiyle değiştirilen, 4.11.1983 tarihli ve 2942 sayılı Kamulaştırma Kanunu'nun 22. maddesinin birinci fıkrasının üçüncü ve dördüncü cümleleri,

2- 28. maddesiyle 2942 sayılı Kanun'a eklenen geçici 8. madde,

hakkında, 4.12.2014 tarihli ve E.2013/114, K.2014/184 sayılı kararla karar verilmesine yer olmadığına karar verildiđinden, bu maddeye ve cümlelere ilişkin yürürlüđün durdurulması istemleri hakkında KARAR VERİLMESİNE YER OLMADIĞINA, OYBİRLİĞİYLE,

4.12.2014 tarihinde karar verilmiştir.

VI- İPTAL KARARININ YÜRÜRLÜĞE GİRECEĞİ GÜN SORUNU

219. Anayasa'nın 153. maddesinin üçüncü fıkrasında, " Kanun, kanun hükmünde kararname veya Türkiye Büyük Millet Meclisi İçtüzüğü ya da bunların hükümleri, iptal kararlarının Resmi Gazetede yayımlandığı tarihte yürürlükten kalkar. Gereken hallerde Anayasa Mahkemesi iptal hükmünün yürürlüğe gireceği tarihi ayrıca kararlaştırabilir. Bu tarih, kararın Resmi Gazetede yayımlandığı günden başlayarak bir yılı geçemez. " denilmekte, 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 66. maddesinin (3) numaralı fıkrasında da bu kural tekrarlanarak, Mahkemenin gerekli gördüğü hâllerde, Resmî Gazetede yayımlandığı günden başlayarak iptal kararının yürürlüğe gireceği tarihi bir yılı geçmemek üzere ayrıca kararlaştırabileceği belirtilmektedir.

220. 12.7.2013 tarihli ve 6495 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Deęişiklik Yapılmasına Dair Kanun'un 73. maddesinin (cc) fıkrasıyla deęiştirilen, 3.12.2010 tarihli ve 6085 sayılı Sayıřtay Kanunu'nun 4. maddesinin (1) numaralı fıkrasının (a) bendinde yer alan ".% 50'den fazla olan." ibaresi ile (b) bendinde yer alan "Kamu payı % 50'den az olmamak kaydıyla." ibaresinin iptal edilmesi nedeniyle doęacak hukuksal boşluk kamu yararını ihlal edici nitelikte görüldüęünden, Anayasa'nın 153. maddesinin üçüncü fıkrasıyla 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrası gereęince İPTAL HÜKMÜNÜN, KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAřLAYARAK ALTI AY SONRA YÜRÜRLÜĖE GİRMESİNE, OYBİRLİĖİYLE, 4.12.2014 tarihinde karar verilmiřtir.

VII- HÜKÜM

12.7.2013 tarihli ve 6495 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Deęişiklik Yapılmasına Dair Kanun'un;

A- 26. maddesiyle deęiştirilen, 4.11.1983 tarihli ve 2942 sayılı Kamulařtırma Kanunu'nun 22. maddesinin birinci fıkrasının;

1- Üçüncü cümlesi, 10.9.2014 tarihli ve 6552 sayılı İş Kanunu ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Deęişiklik Yapılması ile Bazı Alacakların Yeniden Yapılandırılmasına Dair Kanun'un 100. maddesinin birinci fıkrasının (a) bendiyle deęiştirildięinden,

2- Dördüncü cümlesi, 6552 sayılı Kanun'un 100. maddesinin birinci fıkrasının (a) bendiyle yürürlükten kaldırıldıęından,

konusu kalmayan bu cümlelere iliřkin iptal istemleri hakkında KARAR VERİLMESİNE YER OLMADIĖINA, OYBİRLİĖİYLE,

B- 27. maddesiyle 2942 sayılı Kanun'un 25. maddesine eklenen fıkranın Anayasa'ya aykırı olmadığına ve iptal istemininREDDİNE, OYBİRLİĖİYLE,

C- 28. maddesiyle 2942 sayılı Kanun'a eklenen geçiçi 8. maddenin, atıfta bulunduęu aynı Kanun'un 22. maddesinin birinci fıkrasının dördüncü cümlesi, 6552 sayılı Kanun'un 100. maddesinin birinci fıkrasının (a) bendiyle yürürlükten kaldırıldıęından, uygulama imkânı kalmayan bu maddeye iliřkin iptal istemi hakkında KARAR VERİLMESİNE YER OLMADIĖINA, OYBİRLİĖİYLE,

D- 33. maddesiyle, 9.10.2003 tarihli ve 4982 sayılı Bilgi Edinme Hakkı Kanunu'nun 2. maddesine eklenen fıkranın Anayasa'ya aykırı olduęuna ve İPTALİNE, Engin YILDIRIM, Celal Mümtaz AKINCI ile Muammer TOPAL'ın karřioyları ve OYÇOKLUĖUYLA,

E- 43. maddesiyle, 22.6.2006 tarihli ve 5525 sayılı Memurlar ile Diğer Kamu Görevlilerinin Bazı Disiplin Cezalarının Affı Hakkında Kanun'a eklenen ek 1. maddenin;

1- Birinci fıkrasında yer alan "28/2/1997 tarihinden sonra." ibaresinin,

2- İkinci fıkrasının ".1/1/1990 ile...657 sayılı Kanunun 125 inci maddesinin birinci fıkrasının (A) bendinin (g) alt bendinde yer alan fiili işlediği gerekçesiyle anılan Kanunun 56 ve 57 nci maddeleri uyarınca disiplin cezası veya olumsuz sicil almış olmaları nedeniyle." bölümünün Anayasa'ya aykırı olmadıklarına ve iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

F- 59. maddesiyle, 13.12.1983 tarihli ve 178 sayılı Maliye Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 43. maddesine eklenen fıkranın Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

G- 73. maddesinin;

1- (h) fıkrasının;

a- (1) numaralı bendiyle değiştirilen, 11.10.2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 23. maddesinin (7) numaralı fıkrasının (c) ve (ç) bentlerinin Anayasa'ya aykırı olmadıklarına ve iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

b- (3) numaralı bendiyle değiştirilen 663 sayılı Kanun Hükmünde Kararname'nin 47. maddesinin (1), (2) ve (3) numaralı fıkralarının Anayasa'ya aykırı olduklarına ve İPTALLERİNE, Nuri NECİPOĞLU, Hicabi DURSUN ile Celal Mümtaz AKINCI'nın karşıoyları ve OYÇOKLUĞUYLA,

2- (p) fıkrasının;

a- (1) numaralı bendiyle, 3.5.1985 tarihli ve 3194 sayılı İmar Kanunu'nun 8. maddesine eklenen;

aa- (ı) ve (i) bentlerinin Anayasa'ya aykırı olmadıklarına ve iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

ab- (j) bendinin;

aba- Dördüncü cümlesinde yer alan ".eser sözleşmesinde işleme izni verilenler ile." ibaresinin Anayasa'ya aykırı olduğuna ve İPTALİNE, OYBİRLİĞİYLE,

abb- Kalan bölümünün Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

b- (3) numaralı bendiyle değiştirilen 3194 sayılı Kanun'un ek 4. maddesinin Anayasa'ya aykırı olduğuna ve İPTALİNE, OYBİRLİĞİYLE,

3- (r) fıkrasının;

a- (1) numaralı bendiyle deęiştirilen, 7.6.1985 tarihli ve 3224 sayılı Türk Diş Hekimleri Birlięi Kanunu'nun 11. maddesinin birinci fıkrasının (f) bendinde yer alan ".rehber." ibaresinin,

b- (2) numaralı bendiyle deęiştirilen 3224 sayılı Kanun'un 26. maddesinin birinci fıkrasının (e) bendinde yer alan ".rehber." ibaresinin,

c- (3) numaralı bendiyle deęiştirilen 3224 sayılı Kanun'un 40. maddesinin bařlıęında yer alan "Rehber." ibaresi ile birinci ve ikinci fıkralarında yer alan ".rehber." ibarelerinin,

Anayasa'ya aykırı olmadıklarına ve iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

4- (bb) fıkrasıyla, 7.7.2010 tarihli ve 6004 sayılı Dıřıřleri Bakanlıęının Kuruluş ve Görevleri Hakkında Kanun'un 12. maddesinin;

a - (2) numaralı fıkrasının deęiştirilen (d) bendinin,

b- (3) numaralı fıkrasının (a) bendine eklenen cümlelerin,

Anayasa'ya aykırı olmadıklarına ve iptal istemlerinin REDDİNE, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT ile Engin YILDIRIM'ın karřıoyları ve OYÇOKLUĞUYLA,

5- (cc) fıkrasıyla deęiştirilen, 3.12.2010 tarihli ve 6085 sayılı Sayıřtay Kanunu'nun 4. maddesinin (1) numaralı fıkrasının;

a- (a) bendinde yer alan ".% 50'den fazla olan." ibaresinin,

b- (b) bendinde yer alan "Kamu payı % 50'den az olmamak kaydıyla." ibaresinin,

Anayasa'ya aykırı olduklarına ve İPTALLERİNE, Hicabi DURSUN, Muammer TOPAL ile M. Emin KUZ'un karřıoyları ve OYÇOKLUĞUYLA, bu ibarelere iliřkin iptal hükümlerinin, Anayasa'nın 153. maddesinin üçüncü fıkrası ile 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrası gereęince, KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAřLAYARAK ALTI AY SONRA YÜRÜRLÜĞE GİRMESİNE, OYBİRLİĞİYLE,

4.12.2014 tarihinde karar verildi.

Başkanvekili - Serruh KALELİ

Başkanvekili - Alparslan ALTAN

Üye: Serdar ÖZGÜLDÜR; Osman Alifeyyaz PAKSÜT; Recep KÖMÜRCÜ; Burhan ÜSTÜN; Engin YILDIRIM; Nuri NECİPOĞLU; Hicabi DURSUN; Celal Mümtaz AKINCI; Erdal TERCAN; Muammer TOPAL; M. Emin KUZ; Hasan Tahsin GÖKCAN

KARŞIOY GEREKÇESİ

12.7.2013 tarih ve 6495 sayılı Kanun'un 73. maddesinin (bb) fıkrasıyla, 7.7.2010 tarih ve 6004 sayılı Dışişleri Bakanlığının Kuruluş ve Görevleri Hakkında Kanun'un 12. maddesinin (2) ve (3) numaralı fıkraları değiştirilmiş ve 657 sayılı Kanun'un 59. maddesi çerçevesinde "Büyükelçi" veya "Daimi temsilci" olarak atananlardan Dışişleri Bakanlığına veya diğer kamu kurum ve kuruluşlarına mensup olanlar ile açıktan atananların, merkeze döndüklerinde, Dışişleri Bakanlığında çalışabilecekleri, Bakanlıktaki görevleri süresince büyükelçi unvanını kullanmaya devam edebilecekleri ve Bakanlıkta yönetici kadrolarına atanma dahil, meslek mensubu olanlar arasından büyükelçiliğe atananlarla aynı hükümlere tâbi olup aynı haklardan yararlanacakları hüküm altına alınmıştır.

657 sayılı Devlet Memurları Kanunu'nun "istisnai memurluklar" başlıklı 59. maddesinde sayılan birçok memuriyet kadrosu ile birlikte " büyükelçiliklere, elçiliklere, daimi temsilciliklere", bu Kanun'un atanma, sınavlar, kademe ilerlemesi ve derece yükselmesine ilişkin hükümleriyle bağlı olmaksızın, tahsis edilmiş derece aylığı ile (açıktan) memur atanması yapılabileceği, bu kadroların emeklilik aylığının hesabında ve memurluklara naklen atanmalarında herhangi bir sınıf için kazanılmış hak sayılmayacağı, bu görevlerde bulunan memurların emeklilik kıdemlerinin yürümeye devam edeceği hükmü yer almakta; 60. maddesinde ise istisnai devlet memurluklarına yapılacak atamalarda bu Kanun'un 48. maddesinde öngörülen genel şartların mevcudiyetinin de aranacağı belirtilmektedir.

6495 sayılı Kanun'la getirilen düzenlemelerden önce 657 sayılı Kanun'un 59. maddesi uyarınca "açıktan" atama yoluyla "Büyükelçi" istihdamı konusundaki düzenlemelere kısa bir göz atmakta yarar bulunmaktadır:

24.6.1994 tarih ve 4009 sayılı Mülga Dışişleri Bakanlığının Kuruluş ve Görevleri Hakkında Kanun'un "Büyükelçilerin Görevlerinin Sona Ermesi" başlıklı 25. maddesinin ikinci fıkrası "657 sayılı Devlet Memurları Kanunu'nun 59. maddesi uyarınca Büyükelçi atananlar merkeze nakledildiklerinde Dışişleri Bakanlığı ile ilişkileri kesilir. Bunlardan diğer kurum ve kuruluşlarına mensup olanların kurumlarındaki kadroları saklı tutulur ve bunlar merkeze döndüklerinde kurumlarına iade olurlar." denilmekte idi.

6004 sayılı Dışişleri Bakanlığının Kuruluş ve Görevleri Hakkında Kanun'un 6495 sayılı Kanun'la değiştirilmeden önceki 12. maddesinin (d) bendinde ise "657 sayılı Kanunun 59. maddesi çerçevesinde büyükelçi olarak atananlardan diğer kamu kurum ve kuruluşlarına mensup olanlar, merkeze

döndüklerinde, hizmetlerine ihtiyaç duyulması halinde, Bakanlıkta çalışmaya ve bu görevleri süresince büyükelçi unvanını kullanmaya devam ederler. Bunlardan hizmetlerine ihtiyaç duyulmayanlar, Bakanlık ile ilişkileri kesilerek daha önceden bağlı buldukları kamu kurum ve kuruluşlarındaki kadrolarına iade edilir." hükmü yer almaktaydı.

İptal istemine konu düzenlemelerde ise 657 sayılı Kanun'un 59. maddesine göre istisnai olarak diğer kamu idarelerinden veya açıktan büyükelçilik veya daimi temsilcilik görevlerine atananların, merkeze döndüklerinde, kurumlarına iade veya ilişkilerinin kesilmesi yerine, Bakanlıkta çalışmaya devam ederek meslek mensubu büyükelçiler gibi büyükelçi unvanlarını kazanılmış hak olarak korumaları, meslek mensubu büyükelçilerle mesleki kariyer ve liyakata dayalı müsteşarlık, müsteşar yardımcılığı, genel müdürlük gibi idari kadrolara atanma dahil aynı kurallara tâbi olmaları ve aynı haklardan yararlanmaları (Örneğin 6004 sayılı Kanun'un 15/1-e maddesine göre valiler için belirlenen ek gösterge ve makam tazminatını almaları) öngörülmektedir.

4009 sayılı Kanun'da olduğu gibi 6004 sayılı Kanun'da da Dışişleri Meslek Memurluğu bir " kariyer meslek" olarak düzenlenmiş olup, 6004 sayılı Kanun'un 10. maddesi uyarınca kadro unvanları, aday meslek memurluğundan müsteşara kadar bir liste halinde (Kanuna Ekli 3 sayılı Liste) belirlenmiş, hiyerarşi, sınıflandırma, disiplin, liyakat ve sınav (başkatiplik ve konsolosluk unvanlarına yükselebilmek için zorunlu şart) gibi hususlar dikkate alınmak suretiyle, başarı düzeyi, mesleki gelişim ve görev motivasyonunun dikkate alındığı bir statü söz konusudur. Meslek memurluğunun özelliği ve niteliğinden kaynaklanan mesleki hiyerarşi ve kariyere dayalı katı kuralların mevcudiyetine karşın, 657 sayılı Kanun'un 59. maddesine göre büyükelçi veya daimi temsilci olarak atananlarda bu özellikler aranmamakta ve yapılan yasal düzenlemeyle bu konumdakiler, meslek memurluğundan yetişen büyükelçi ve daimi temsilcilerle aynı statü ve haklara kavuşturulmaktadır.

Anayasa'nın 70. maddesinde "Her Türk, kamu hizmetlerine girme hakkına sahiptir. Hizmete alınmada, görevin gerektirdiği niteliklerden başka bir ayrım gözetilemez." denilmektedir. Anayasa Mahkemesinin 9.4.2014 tarih ve E.2014/34, K.2014/79 sayılı kararında (R.G. 9.9.2014, Sayı: 29114) bu dava konusu ile paralellik gösteren Anayasa'nın 2. ve 70. maddeleri yönünden şu saptamalarda bulunulmuştur:

"...Kanunların kamu yararının sağlanması amacına yönelik olması, genel, objektif, adil kurallar içermesi ve hakkaniyet ölçütlerini gözetmesi hukuk devleti olmanın gereğidir. Bu nedenle kanun koyucunun hukuki düzenlemelerde kendisine tanınan takdir yetkisini anayasal sınırlar içinde adalet, hakkaniyet ve kamu yararı ölçütlerini gözönünde tutarak kullanması gerekir. Anayasa'nın kamu hizmetine girme hakkını düzenleyen 70. maddesinin birinci fıkrasında 'Her Türk, kamu hizmetine

girme hakkında sahiptir' denilmiř; ikinci fıkrasında ise 'Hizmete alınmada grevin gerektirdiđi niteliklerden bařka hibir ayırım gzetilemez.' hkmne yer verilmiřtir. Hizmete alınmada, grevin gerektirdiđi niteliklerden bařka hibir ayırım gzetilemeyeceđi hkm getirilmekle, bir yandan kamu hizmetine alımda aranacak kořulların belirlenmesi hususunda kanun koyucuya takdir yetkisi tanınmakta, diđer yandan da ngrlecek kořulların gerektirdiđi niteliklerle uyumlu olması geređi vurgulanacak kanun koyucunun bu takdiri sınırlandırılmaktadır... Ancak ngrlen Őartların... mesleklerinin gerektirdiđi niteliklerle uyumlu olması ve ayrıca hukuk devleti ilkesinin bir geređi olarak adalet ve hakkaniyet lsn zedelememesi gerekir..."

Anılan Anayasa Mahkemesi kararı gerekesinden de aıka anlařılacađı zere, bir yasa kuralının kamu yararına olması gerekliliđinin yanı sıra, adalet ve hakkaniyet ltlerini de beraberinde tařıması Hukuk Devleti İlkesinin dođal geređidir. Ayrıca, kamu hizmetine alınmada ve dođal olarak bu staty kazandıktan sonra tanınacak hak ve olanakların saptanmasında yasa koyucuya tanınan takdir hakkının belirlenmesinde, ngrlen kořullarda sađlanan imkanların, ngrlen kamu greviyle (statsyle) uyum ierisinde olması gerektiđi de aıktır. Diđer taraftan, hibir kimseye imtiyaz tanınamayacađını ngren Anayasa'nın 10. maddesinin drdnc fıkrası hkm uyarınca da kamu hizmetinin dzenlenmesinde "imtiyaz" teřkil edecek dzenlemelerden kaınılması gerektiđi izahtan varestedir.

Yukarıda yapılan aıklamalar ıřıđında, 657 sayılı Kanun'un 59. maddesi uyarınca atanan Bykeli ve Daimi temsilcilere, bu grevleri sona erdikten ve merkeze dndkten sonra, bir kariyer meslek olan dıřıřleri meslek memurluđundan liyakat ve kariyer esasına gre yetiřerek Bykeli statsne ulařanlara tanınan hak ve imknların tanınması Őeklindeki iptal istemine konu dzenlemelerin Anayasa'nın 2., 10. ve 70. maddelerine aykırı olduđu ve iptali gerektiđi kanaatine vardığımızdan; ođunluđun aksi yndeki kararına katılmıyoruz.

ye: Serdar ZGLDR; Osman Alifeyyaz PAKST; Engin YILDIRIM

MUHALEFET ŐERHİ

Dava konusu 663 sayılı Kanun Hkmnde Kararname'nin 47. maddesi Őyledir:

" 1) (Deđiřik: 12/7/2013-6495/73 md.) Bakanlık ve bađlı kuruluřları, mevzuatla kendilerine verilen grevleri, e-devlet uygulamalarına uygun olarak daha etkin ve daha hızlı biimde yerine getirebilmek iin, btn kamu ve zel sađlık kurum ve kuruluřlarından; sađlık hizmeti alanların, aldıkları sađlık hizmetinin geređi olarak ilgili sađlık kurum ve kuruluřuna vermek zorunda oldukları kiřisel bilgileri

ve bu kimselere verilen hizmete ilişkin bilgileri her türlü vasıta ile toplamaya, işlemeye ve paylaşmaya yetkilidir.

(2) (Değişik: 12/7/2013-6495/73 md.) Bakanlık ve bağlı kuruluşları işlediği kişisel sağlık verilerini ilgili üçüncü kişiler ve kamu kurum ve kuruluşları ile ancak bu kişi ve kurumların bu verilere erişebileceği hususunda kanunen yetkili olması hâlinde görevlerini yapmalarına yetecek derecede paylaşabilir.

(3) (Değişik: 12/7/2013-6495/73 md.) Bakanlık ve bağlı kuruluşları, mevzuatla kendilerine verilen görevleri yerine getirebilmek için gereken bilgileri, kamu ve özel ilgili bütün kişi ve kuruluşlardan istemeye yetkilidir. İlgili kişi ve kuruluşlar istenilen bilgileri vermekle yükümlüdür.

(4) Sağlık personeli istihdam eden kamu kurum ve kuruluşları ile özel hukuk tüzel kişileri ve gerçek kişiler, istihdam ettiği personeli ve personel hareketlerini Bakanlığa bildirmekle yükümlüdür.

(5) Bu maddenin uygulanmasına ilişkin hususlar Bakanlıkça çıkarılacak yönetmelikle düzenlenir."

Dava dilekçesinde özetle, dava konusu kurullarla Sağlık Bakanlığı ve bağlı kuruluşlarına kişisel verileri toplama, saklama, işleme ve paylaşma yetkisinin verildiği, bu durumun özel hayatın gizliliği ve kişisel verilerin korunması haklarının özüne müdahale edilmesi ve ölçüsüzce sınırlandırılması sonucunu doğurduğu belirtilerek kurulların, Anayasa'nın 2., 13., 20. ve 90. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kurullarla, Sağlık Bakanlığı ve bağlı kuruluşlarına, görevlerini yürütebilmeleri için gerekli olan bilgileri toplama, işleme ve paylaşma yetkisi verilmekte ve bu yetkinin kapsam ve sınırları düzenlenmektedir.

Anayasa'nın 20. maddesinin üçüncü fıkrasının ilk cümlesinde, " Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. " denilmek suretiyle kişisel verilerin korunması hakkı güvence altına alınmıştır. Fıkranın üçüncü cümlesinde ise bu verilerin kanunda öngörülen hallerde veya kişinin rızasıyla işlenebileceği belirtilerek bu hakkın mutlak olmadığı ve kanun koyucunun gerekli gördüğü nedenlerle bu konuda düzenleme yapabileceği ve kişisel verilerin korunmasını isteme hakkına sınırlama getirilebileceği kabul edilmiştir. Belirtmek gerekir ki ilgili maddede sadece bilgilerin işlenebilmesi yönünden sınırlandırma nedenine yer verilmişse de Anayasa Mahkemesinin içtihatları uyarınca Anayasa'nın diğer hükümlerinin gerektirmesi nedeniyle bu hakkın işleme dışındaki nedenlerle de sınırlandırılabilmesi mümkün bulunmaktadır. Ancak, bu hak yönünden de sınırlamanın Anayasa'nın 13. maddesinde belirtilen güvencelere bağlı kalınarak yapılması gerekmektedir.

Dava konusu kurallarla getirilen sınırlamayla, kişilerin her türlü kişisel verilerinin değil sadece sağlık hizmetinin gereği olarak ilgili sağlık kurum ve kuruluşuna vermek zorunda oldukları ve Bakanlık ve bağlı kuruluşların mevzuatla kendilerine verilen görevleri yerine getirebilmeleri için gereken bilgilerin toplanması, işlenmesi ve paylaşılması yetkisi verilmekte olup bu sınırlandırmanın kişisel verilerin korunması hakkını bütünüyle ortadan kaldırmadığı veya ciddi surette güçleştirip amacına ulaşmasına engel olmadığı açıktır.

Kurallarla Sağlık Bakanlığı ve bağlı kuruluşların, mevzuatla kendilerine verilen görevleri, e-devlet uygulamalarına uygun olarak daha etkin ve daha hızlı biçimde yerine getirebilmeleri amacıyla kişisel verilerin korunması hakkına bir sınırlama getirilmekte olup bu sınırlama, demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır. Zira sağlık hizmetlerinin etkin ve hızlı biçimde yerine getirilerek herkesin hayatını beden ve ruh sağlığı içinde sürdürmesini sağlama görevi, Anayasa ile devlete yüklenen ve toplum düzeninin korunması için alınması gereken zorunlu tedbirlerdendir.

Bu şekilde, demokratik toplum düzeni bakımından alınması gerekli tedbirler kapsamında kişisel verilerin korunması hakkı sınırlandırılırken, Kanun'da sınırlandırma aracının sınırlandırma amacına uygun ve orantılı şekilde kullanılmasını sağlayacak yasal güvencelere de yer verilmiş, böylece toplumun genel sağlığı ve kişilerin sağlıklarının korunması şeklindeki kamu yararı ile kişisel verilerin korunması hakkı arasındaki makul denge kurulmuştur.

Bu bağlamda, Kanun'da Sağlık Bakanlığına ve bağlı kuruluşlarına sadece bunların görevlerini yerine getirebilme ve sağlık hizmetlerinin yürütebilmelerini sağlamak için gerekli olan kişisel bilgileri toplama, işleme ve paylaşma yetkisi verilmiş olup bu hizmetlerin yürütülmesi için gerekli olmayan bir bilginin toplanması ve işlenmesine izin verilmemiştir.

Ayrıca, Bakanlığın ve bağlı kuruluşların işledikleri kişisel sağlık verilerini ilgili üçüncü kişiler ve kamu kurum ve kuruluşları ile paylaşabilmesi için söz konusu kişi ve kurumların bu verilere erişebileceği hususunda kanunen yetkilendirilmiş olmaları, bu verilerin ilgili kurum ve kişilerin görevlerini yapması için gerekli olması ve verilerin ilgili kişi ve kurumların görevlerini yapmaya yetecek kadarıyla sınırlı olarak paylaşılması gerekmektedir.

Kanun'da kurallara konu kişisel verilerin saklanması, işlenmesi ve toplanması işlemlerine karşı yargı yolu da açık tutulmuş, böylece idarenin sınırlandırma aracını sınırlandırma amacına ve Kanun'a aykırı şekilde kullanmasının önüne geçecek güvence de sağlanmıştır.

Bu yönleriyle kurallarla özel verilerin korunmasını isteme hakkına getirilen sınırlandırmanın, hakkın özünü zedelediğinden söz edilemeyeceği gibi demokratik toplum düzenini ve hukuk devleti gereklerine ve ölçülülük ilkesine aykırı düştüğü de söylenemez.

Öte yandan, dava konusu kuralların Anayasa'nın 90. maddesi ile ilgisi bulunmamaktadır.

Açıklanan nedenlerle dava konusu kurallar, Anayasa'nın 2., 13. ve 20. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir, düşüncesiyle çoğunluğun kararına katılmıyoruz.

Üye: Nuri NECİPOĞLU; Hicabi DURSUN; Celal Mümtaz AKINCI

KARŞI OY YAZISI

Dava konusu ibareleri de içeren 6085 sayılı Kanun'un "Denetim alanı " başlıklı 4. maddesi şöyledir:

" (1) Sayıştay;

a) (Değişik: 12/7/2013-6495/73 md.) Merkezi yönetim bütçesi kapsamındaki kamu idareleri ile sosyal güvenlik kurumlarını, mahallî idareleri, sermayesindeki kamu payı doğrudan veya dolaylı olarak %50'den fazla olan özel kanunlar ile kurulmuş anonim ortaklıkları, diğer kamu idarelerini (kamu kurumu niteliğindeki meslek kuruluşları hariç),

b) (Değişik: 12/7/2013-6495/73 md.) Kamu payı %50'den az olmamak kaydıyla (a) bendinde sayılan idarelere bağlı veya bu idarelerin kurdukları veya doğrudan doğruya ya da dolaylı olarak ortak oldukları her çeşit idare, kuruluş, müessese, birlik, işletme ve şirketleri,

c) Kamu idareleri tarafından yapılan her türlü iç ve dış borçlanma, borç verilmesi, borç geri ödemeleri, yurt dışından alınan hibelerin kullanımı, hibe verilmesi, Hazine garantileri, Hazine alacakları, nakit yönetimi ve bunlarla ilgili diğer hususları; tüm kaynak aktarımları ve kullanımları ile Avrupa Birliği fonları dahil yurt içi ve yurt dışından sağlanan diğer kaynakların ve fonların kullanımını,

ç) Kamu idareleri bütçelerinde yer alıp almadığına bakılmaksızın özel hesaplar dahil tüm kamu hesapları, fonları, kaynakları ve faaliyetlerini,

denetler.

(2) Sayıştay; yapılan andlaşma veya sözleşmedeki esaslar çerçevesinde uluslararası kuruluş ve örgütlerin hesap ve işlemlerini de denetler.

(3) 2/4/1987 tarihli ve 3346 sayılı Kamu İktisadi Teşebbüsleri ile Fonların Türkiye Büyük Millet Meclisince Denetlenmesinin Düzenlenmesi Hakkında Kanununun 2 nci maddesi kapsamına giren kamu

kurum, kuruluş ve ortaklıklarının Türkiye Büyük Millet Meclisince denetlenmesi, bu Kanun ve diğer kanunlarda belirtilen usul ve esaslar çerçevesinde yerine getirilir. "

Anayasa'nın "Sayıştay" başlıklı 160. maddesinin birinci fıkrasının ilk cümlesinde " Sayıştay, merkezi yönetim bütçesi kapsamındaki kamu idareleri ile sosyal güvenlik kurumlarının bütün gelir ve giderleri ile mallarını Türkiye Büyük Millet Meclisi adına denetlemek ve sorumluların hesap ve işlemlerini kesin hükme bağlamak ve kanunlarla verilen inceleme, denetleme ve hükme bağlama işlerini yapmakla görevlidir. " denilmiş, üçüncü fıkrasında ise " Mahalli idarelerin hesap ve işlemlerinin denetimi ve kesin hükme bağlanması Sayıştay tarafından yapılır. " kuralına yer verilmiştir.

Buna göre, merkezi yönetim bütçesi kapsamındaki kamu idareleri ve sosyal güvenlik kurumlarının bütün gelir ve giderleriyle mallarının ve mahalli idarelerin hesap ve işlemlerinin denetimi ve kesin hükme bağlanması görevlerinin, Sayıştay tarafından yerine getirilmesi anayasal bir zorunluluk olup belirtilen idare ve kurumların Sayıştay tarafından denetlenmesi görevini ortadan kaldıracak bir düzenleme yapılması Anayasa'nın 160. maddesine aykırılık teşkil edecektir.

Sayıştayın anılan idare ve kurumların denetlenmesi, hesap ve işlemlerinin kesin hükme bağlanması dışındaki görevleri yönünden ise Anayasa'da bir düzenleme yapılmamış ve 160. maddenin birinci fıkrasının ilk cümlesinde ". ve kanunlarla verilen inceleme, denetleme ve hükme bağlama işlerini yapmakla görevlidir." denilmek suretiyle bu görevleri belirleme yetkisi kanun koyucunun takdirine bırakılmıştır. Bu çerçevede kanun koyucunun kamu idareleri, sosyal güvenlik kurumları ve mahalli idarelerin hesap ve işlemlerinin denetimi ve kesin hükme bağlanması dışında kalan görevlerini belirleme dolayısıyla anılan idare ve kuruluşlar dışında kalanların denetlenmesi görevini Sayıştaya verip vermeme konusunda takdir yetkisine sahip olduğu açıktır.

6085 sayılı Kanun'un "Denetim alanı" başlıklı 4. maddesinde, merkezi yönetim bütçesi kapsamındaki kamu idareleri, sosyal güvenlik kurumları ve mahallî idarelerin Sayıştay tarafından denetleneceği belirtilmek suretiyle Anayasa'nın 160. maddesindeki zorunluluk yerine getirilmiştir. Ancak maddede bunlar dışında kalan bazı idare ve kuruluşların denetiminin de Sayıştay tarafından yapılması öngörülmüş böylece Anayasa'nın 160. maddesinde belirtilen zorunlu görevler dışındaki bazı görevlerin de Sayıştay tarafından yerine getirilmesi esası benimsenmiştir.

Anayasal zorunluluk olmadığı halde Sayıştayın denetim görevi kapsamına, özel kanunlarla kurulmuş ve sermayesindeki kamu payı %50'den fazla olan anonim ortaklıkları ile merkezi yönetim bütçesi kapsamındaki kamu idarelerine, sosyal güvenlik kurumlarına ve mahallî idarelere bağlı veya

bu idarelerin kurdukları veya doğrudan doğruya ya da dolaylı olarak ortak oldukları her çeşit kuruluştan kamu payı %50'den az olmayanlar da alınmıştır.

Kanun koyucunun anılan nitelikteki ve sermayesinde belli bir miktarda kamu payı bulunan anonim ortaklıkları ile her çeşit kuruluşu Sayıştay denetimine tabi kılıp kılmama konusunda takdir yetkisi bulunmakta olup bu çerçevede Anayasa'nın 160. maddesinde belirtilenler dışında kalan idare ve kuruluşlardan özel kanunla kurulan anonim ortaklıkları ile merkezi yönetim bütçesi kapsamındaki kamu idarelerine, sosyal güvenlik kurumlarına ve mahallî idarelere bağlı veya bu idarelerin kurdukları veya doğrudan doğruya ya da dolaylı olarak ortak oldukları her çeşit kuruluştan kamu payı %50'den fazla olanları denetleme yetkisini Sayıştaya vermesinde veya kamu payı %50'den az olanları ortaklık hakları yönüyle de olsa Sayıştayın denetimine tabi kılmamasında Anayasa'nın 160. maddesine aykırı düşen bir yön bulunmamaktadır.

Öte yandan Anayasa'nın 160. maddesinde belirtilen idare ve kuruluşlar dışında kalan idare ve kuruluşlara ilişkin kamu kaynaklarının kamu yararına yönelik olarak hukuka uygun bir şekilde kullanılıp kullanılmadığının denetlenmesi de Anayasa'nın 2. maddesinde düzenlenen hukuk devletinin bir gereği olmakla birlikte Anayasa'da bu denetimin hangi kurum aracılığıyla ve hangi usullerle yapılacağı konusunda bir düzenleme bulunmamaktadır. Dolayısıyla bu denetimin ille de Sayıştay aracılığıyla yapılması zorunlu olmayıp bu denetim yetkisinin hangi kurum aracılığıyla ve hangi usulle yaptıracağı hususu kanun koyucunun takdir yetkisi kapsamında kalmaktadır.

Bu çerçevede dava konusu kurullarla Anayasa'nın 160. maddesinde belirtilen idare ve kuruluşlar dışında kalan ve kamu payı %50'den az olan anonim ortaklıkları ile her çeşit idare, kuruluş, müessese, birlik, işletme ve şirketlerin Sayıştay denetimi dışında tutulmasında, Anayasa'nın 2. maddesine de aykırı düşen bir yön bulunmamakta ve iptal isteminin reddi gerekmektedir.

Açıklanan nedenlerle, dava konusu ibarelerin Anayasa'ya aykırı olmadığı gerekçesiyle anılan kurulların iptali yolundaki çoğunluk görüşüne katılmıyoruz.

Üye: Hicabi DURSUN; Muammer TOPAL

KARŞI OY GEREKÇESİ

6085 sayılı Sayıştay Kanununun "Denetim alanı" başlıklı 4. maddesinin birinci fıkrasının 6495 sayılı Kanunla değişik (a) bendindeki ". % 50'den fazla olan ." ibaresi ile (b) bendindeki "Kamu payı % 50'den az olmamak kaydıyla ." ibaresinin Anayasanın 2. ve 160. maddelerine aykırı olduğuna ve iptaline karar verilmiştir.

Anayasanın 160. maddesine göre Sayıştay, merkezî yönetim bütçesi kapsamındaki kamu idareleri ile sosyal güvenlik kurumlarının bütün gelir ve giderleri ile mallarını TBMM adına denetlemek ve kanunlarla verilen inceleme, denetleme ve hükme bağlama işlerini yapmakla görevlidir. Anayasada hangi idare ve kurumların merkezî yönetim bütçesi kapsamındaki kamu idareleri ile sosyal güvenlik kurumları olduğu belirtilmediğinden, bunları belirleme yetkisi de; 160. maddede kanuna yapılan açık atıf sebebiyle denetim kapsamındaki diğer idare, kurum ve kuruluşları tespit etme yetkisi de yasama organına aittir.

Anayasanın bu hükmüne uygun olarak Sayıştayın denetim alanı, 6085 sayılı Kanunda belirtilen idare, kurum ve kuruluşlar ile faaliyet, işlem ve hesapları kapsamaktadır.

Anılan Kanunun 4. maddesinde Sayıştayın denetim alanı, merkezî yönetim bütçesi kapsamındaki kamu idareleri (bunlar da yasama organı tarafından 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununda belirlenmektedir) ile sosyal güvenlik kurumları, mahallî idareler, diğer kamu idareleri (kamu kurumu niteliğindeki meslek kuruluşları) ve kamu hesapları, fonları, kaynakları ve faaliyetleri şeklinde tespit edilmekte; ayrıca Anayasanın 165. maddesi gereğince TBMM tarafından denetlenmesi öngörülen sermayesindeki kamu payı % 50'den fazla olan özel kanunlarla kurulmuş anonim ortaklıklar ile kamu payı % 50'den az olmamak kaydıyla yukarıda belirtilen idarelere bağlı veya bunların kurdukları ya da ortak oldukları her çeşit idare, kuruluş, müessese, birlik, işletme ve şirketler de Sayıştay denetimi kapsamında sayılmaktadır.

Bu düzenlemelerden de anlaşılacağı üzere, Anayasada Sayıştayın denetim alanında bulunduğu açıkça hükme bağlanan idare ve kurumlar ile bunların dışındaki idare, kurum, kuruluş ve ortaklıklar kanunla belirlenmiş bulunmaktadır.

Kararın gerekçesinde, iptaline karar verilen ibarelerin, bazı kamu kaynaklarının kullanılmasına ilişkin olarak Sayıştayın denetim yetkisini ortadan kaldırdığı, dolayısıyla yasama organının, yürütmenin bütçe ile ilgili işlemlerini kanunlara uygun bir şekilde yürütüp yürütmediğini denetleme imkânını sınırlayarak demokratik devlet ilkesine zarar verdiği belirtilerek Anayasanın 2. ve 160. maddelerine aykırı bulunduğu sonucuna varılmıştır.

Kuşkusuz, bütün kamu gelirlerinin, giderlerinin, mallarının, işlemlerinin ve hesaplarının şeffaflık ve hesap verebilirlik ilkelerine uygun olarak denetlenmesi gerekmektedir. Ancak, bu denetimin anayasal dayanağını oluşturan 160. ve 165. maddelerde, kamu payı % 50'nin altında olan kuruluş ve ortaklıkların Sayıştayca denetlenmesini öngören bir hüküm bulunmadığını belirtmek gerekir. Yukarıda da açıklandığı üzere, 160. maddede belirtilen idareler dışında hangi idare, kurum, kuruluş ve ortaklıkların TBMM adına Sayıştayca denetleneceğini ve denetimin kapsamını belirleme yetkisi

kanunlara bırakılmış; 165. maddede ise sermayesinin yarısından fazlası Devlete ait olan kamu kuruluş ve ortaklıklarının TBMM tarafından denetlenmesi esaslarının kanunla düzenleneceği hükme bağlanmıştır.

Kararda da belirtildiği üzere, bütçe hakkına sahip olan yasama organının işlevlerini etkin ve sağlıklı bir şekilde yürütmesinde Sayıştay denetiminin büyük bir önemi bulunmakta ise de, bu denetimin kapsamının belirlenmesi konusundaki takdir yetkisi de Anayasanın 160. maddesine göre yine yasama organına aittir.

İptal edilen ibarelerdeki "kamu payı"nın Anayasanın 160. maddesinde belirtilen idare ve kurumların "malları" kapsamında değerlendirilmesi gerektiği, dolayısıyla kamu payının % 50'den az olması hâlinde de Anayasanın 160. maddesine göre Sayıştayca denetlenmesinde zorunluluk bulunduğu düşünülebilirse de, Anayasanın bu hükmü kamu payının bulunduğu kuruluş ve ortaklıkların değil, sadece kamu payının denetimine imkân verdiği için, kamu payının % 50'den az olduğu kuruluş ve ortaklıkların Sayıştayın denetimi kapsamına dahil edilip edilmeyeceği hususunda, 160. madde gereğince yasama organı takdir yetkisine sahiptir.

Kanunun 4. maddesinde daha önce yer alan ve kamu payının % 50'den az olması hâlinde "ortaklık hakları yönüyle" Sayıştay denetimine imkân veren hüküm, bütçe hakkına sahip olan ve Anayasanın 160. maddesine göre merkezi yönetim bütçesi kapsamındaki kamu idareleri ile sosyal güvenlik kurumları ve mahallî idareler dışında Sayıştay denetimine tâbi idare, kurum, kuruluş ve ortaklıkları belirleme yetkisine sahip olan yasama organı tarafından kaldırılarak denetimin kapsamı, dava konusu kuraldaki gibi belirlenmiştir.

Mezkûr ibarelerin iptali 6085 sayılı Kanunun "Denetim alanı" başlıklı 4. maddesinin birinci fıkrasının (a) ve (b) bentlerinin kapsamını, dolayısıyla da Sayıştayın denetim alanını yasama organının öngörmediği ölçüde genişletmektedir. Anayasanın 153. maddesinde, Anayasa Mahkemesinin bir kanun hükmünü iptal ederken, kanun koyucu gibi hareketle, yeni bir uygulamaya yol açacak şekilde hüküm tesis edemeyeceği hükme bağlanmaktadır. Buna göre, kanun koyucunun isterse getirebileceği bir kuralı getirmemesinin takdir yetkisi içinde olduğu ve kuralın uygulama alanını genişletecek şekilde bir iptal kararı verilemeyeceği açıktır. 6085 sayılı Kanunun 4. maddesinin birinci fıkrasının (a) ve (b) bentlerindeki mezkûr ibarelerin iptali ile anılan hükümlerin kapsamı, kanun koyucunun öngörmediği şekilde genişletilmiştir.

Bu sebeplerle, dava konusu ibarelere yönelik iptal talebinin reddine karar verilmesi gerektiğini düşündüğümden, iptal yönündeki çoğunluk görüşüne katılmıyorum.

Üye - M. Emin KUZ

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2013/122

Karar Sayısı: 2014/74

Karar Günü: 9.4.2014

R.G. Tarih-Sayı: 26.7.2014-29072

İTİRAZ YOLUNA BAŞVURAN: Danıştay İdari Dava Daireleri Kurulu

İTİRAZIN KONUSU: 5.11.2008 günlü, 5809 sayılı Elektronik Haberleşme Kanunu'nun 51. maddesinin Anayasa'nın 2., 7., 13. ve 20. maddelerine aykırılığı ileri sürülerek iptaline ve yürürlüğünün durdurulmasına karar verilmesi istemidir.

I- OLAY

Davacı şirket tarafından 24.7.2012 günlü Resmî Gazete'de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik'in bazı maddelerinin iptali ve yürütmenin durdurulması için açılan davada, Danıştay Onüçüncü Dairesince yürütmenin durdurulması isteminin reddine karar verilmesi üzerine davacı, kararın kaldırılması ve dava konusu Yönetmelik'in yürütmesinin durdurulması istemiyle itiraz etmiştir. Devam eden yargılama sırasında itiraz konusu kuralın Anayasa'ya aykırı olduğu kanısına varan Danıştay İdari Dava Daireleri Kurulu, iptali için başvurmuştur.

III- YASA METİNLERİ

A- İtiraz Konusu Yasa Kuralı

Kanun'un itiraz konusu kural olan 51. maddesi şöyledir:

"MADDE 51- (1) Kurum, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkilidir."

B- Dayanılan Anayasa Kuralları

Başvuru kararında, Anayasa'nın 2., 7., 13. ve 20. maddelerine dayanılmıştır.

IV- İLK İNCELEME

Anayasa Mahkemesi İÇtüzüğü hükümleri uyarınca Haşim KILIÇ, Serruh KALELİ, Alparslan ALTAN, Mehmet ERTEN, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT, Zehra Ayla PERKTAŞ, Recep KÖMÜRCÜ, Burhan ÜSTÜN, Engin YILDIRIM, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Erdal TERCAN, Muammer TOPAL, Zühtü ARSLAN ve M. Emin KUZ'un katılımlarıyla 14.11.2013 gününde yapılan ilk inceleme toplantısında, dosyada eksiklik bulunmadığından işin esasının incelenmesine, yürürlüğü durdurma isteminin esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

V- ESASIN İNCELENMESİ

Başvuru kararı ve ekleri, Raportör Hakan ATASOY tarafından hazırlanan işin esasına ilişkin rapor, itiraz konusu yasa kuralı, dayanılan Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

Başvuru kararında, itiraz konusu kural ile kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirleme ve bu konuda düzenleme yapma yetkisinin bütünüyle yürütme organına bırakıldığı, yasama organı tarafından temel ilkeleri koyulmadan, çerçevesi çizilmeden, sınırsız, belirsiz, geniş bir alanı düzenleme yetkisinin yürütme organına bırakılmasının Anayasa'nın 7., 13. ve 20. maddelerine ve sonuçta Anayasa'nın 2. maddesindeki hukuk devleti ilkesine aykırı olduğu ileri sürülmüştür.

İtiraz konusu kuralla, Bilgi Teknolojileri ve İletişim Kurumunun elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkili olduğu hükme bağlanmıştır.

Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır.

Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Bilişim teknolojilerindeki gelişmeler sonucunda, geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi; daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri

eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması; verilere erişim ve veri transferinin kolaylaşması; kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler, günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır. Bu bağlamda Anayasa'nın 20. maddesinin üçüncü fıkrasının son cümlesinde, "Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilerek kişisel verilerin korunması hakkı anayasal güvenceye bağlanmış ve bu şekilde kamu makamlarının keyfi müdahalelerine karşı koruma altına alınmıştır.

Yasama yetkisinin devredilemezliği ilkesi gereğince, Anayasa'nın açıkça kanunla düzenlenmesini öngördüğü konularda yürütme organına doğrudan ve ilk elden düzenleyici işlem yapma yetkisi verilemez. Elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirleme yetkisini Bilgi Teknolojileri ve İletişim Kurumuna veren itiraz konusu kural, Anayasa'nın 20. maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceğine ilişkin güvenceye aykırıdır.

Açıklanan nedenlerle, itiraz konusu kural Anayasa'nın 20. maddesine aykırıdır. İptali gerekir.

Kural, Anayasa'nın 20. maddesine aykırı bulunarak iptal edildiğinden dolayı Anayasa'nın 2., 7. ve 13. maddeleri yönünden ayrıca incelenmesine gerek görülmemiştir.

VI- İPTAL KARARININ YÜRÜRLÜĞE GİRECEĞİ GÜN SORUNU

Anayasa'nın 153. maddesinin üçüncü fıkrasında, "Kanun, kanun hükmünde kararname veya Türkiye Büyük Millet Meclisi İçtüzüğü ya da bunların hükümleri, iptal kararlarının Resmî Gazetede yayımlandığı tarihte yürürlükten kalkar. Gereken hallerde Anayasa Mahkemesi iptal hükmünün yürürlüğe gireceği tarihi ayrıca kararlaştırabilir. Bu tarih, kararın Resmî Gazetede yayımlandığı günden başlayarak bir yılı geçemez." denilmekte, 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 66. maddesinin (3) numaralı fıkrasında da bu kural tekrarlanmaktadır.

5.11.2008 günlü, 5809 sayılı Elektronik Haberleşme Kanunu'nun 51. maddesinin iptal edilmesi nedeniyle doğacak hukuksal boşluk kamu yararını ihlal edecek nitelikte görüldüğünden, Anayasa'nın 153. maddesinin üçüncü fıkrası ile 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince bu maddeye ilişkin iptal hükmünün, kararın Resmî Gazete'de yayımlanmasından başlayarak altı ay sonra yürürlüğe girmesine OYBİRLİĞİYLE karar verilmiştir.

VII- YÜRÜRLÜĞÜN DURDURULMASI İSTEMİ

5.11.2008 günlü, 5809 sayılı Elektronik Haberleşme Kanunu'nun 51. maddesine ilişkin iptal hükmünün yürürlüğe girmesinin ertelenmesi nedeniyle bu maddeye yönelik yürürlüğün durdurulması isteminin REDDİNE, 9.4.2014 gününde OYBİRLİĞİYLE karar verilmiştir.

VIII- SONUÇ

5.11.2008 günlü, 5809 sayılı Elektronik Haberleşme Kanunu'nun 51. maddesinin Anayasa'ya aykırı olduğuna ve İPTALİNE, iptal hükmünün, Anayasa'nın 153. maddesinin üçüncü fıkrası ile 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince, KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAŞLAYARAK ALTI AY SONRA YÜRÜRLÜĞE GİRMESİNE, 9.4.2014 gününde OYBİRLİĞİYLE karar verildi.

Başkan - Haşim KILIÇ

Başkanvekili - Serruh KALELİ

Başkanvekili - Alparslan ALTAN

Üye: Serdar ÖZGÜLDÜR; Osman Alifeyyaz PAKSÜT; Zehra Ayla PERKTAŞ; Recep KÖMÜRCÜ; Burhan ÜSTÜN; Engin YILDIRIM; Nuri NECİPOĞLU; Hicabi DURSUN; Celal Mümtaz AKINCI; Erdal TERCAN; Muammer TOPAL; Zühtü ARSLAN; M. Emin KUZ

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2013/84

Karar Sayısı: 2014/183

Karar Günü: 4.12.2014

R.G. Tarih-Sayı: 13.3.2015-29294

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi Üyeleri M. Akif HAMZAÇEBİ, Engin ALTAY ile birlikte 126 milletvekili

İPTAL DAVASININ KONUSU: 9.5.2013 günlü, 6475 sayılı Posta Hizmetleri Kanunu'nun;

1- 3. maddesinin (1) numaralı fıkrasının;

a- (a) bendindeki "...ilgili mevzuatı saklı kalmak kaydıyla," ibaresinden sonra gelen "...gerçek..." ibaresinin

b- (h) ve (ı) bentlerinin,

2- 4. maddesinin (1) numaralı fıkrasının (ç) bendinde yer alan "...millî güvenlik, kamu düzeni ve genel sağlığın korunmasını teminen..." ve "...posta yoluyla gönderilmesi yasak maddeler ile kabulü şarta bağlı gönderiler için..." ibarelerinin,

3- 6. maddesinin (1) numaralı fıkrasının,

4- 7. maddesinin (1) numaralı fıkrasında yer alan "...ve posta hizmetleri ile ilgili ilişkileri..." ibaresinin,

5- 9. maddesinin;

a- (3) numaralı fıkrasının,

b- (6) numaralı fıkrasında yer alan "...veya millî güvenlik, kamu düzeni ve genel sağlık gerekçeleri ile..." ibaresinin,

c- (8) numaralı fıkrasının,

6- 17. maddesinin (2) numaralı fıkrasının,

7- 23. maddesinin (1) numaralı fıkrasının (a) bendinin,

8- 24. maddesinin,

9- 25. maddesinin (6) numaralı fıkrasının,

10- 29. maddesinin (2) ve (3) numaralı fıkralarının,

11- Geçici 3. maddesinin,

12- Geçici 6. maddesinin (1) numaralı fıkrasında yer alan "...Yönetim Kurulunca belirlenen esaslar çerçevesinde..." ve "...ile geçmesi uygun görülmeyenler..."ibarelerinin,

Anayasa'nın 2., 5., 6., 7., 10., 11., 13., 22., 74., 123., 129., 167. ve 172. maddelerine aykırılıkları ileri sürülerek iptallerine ve iptal davası sonuçlanıncaya kadar yürürlüklerinin durdurulmasına karar verilmesi istemidir.

II- YASA METİNLERİ

A- İptali İstenen Yasa Kuralları

1- Kanun'un 3. maddesinin (1) numaralı fıkrasının;

a- Dava konusu ibareyi de içeren (a) bendi şöyledir:

"a) Adres bilgi kayıt sistemi: 25/4/2006 tarihli ve 5490 sayılı Nüfus Hizmetleri Kanunu ve ilgili mevzuatı saklı kalmak kaydıyla, gerçek kişilerin rızası alınarak gerçek ve tüzel kişiler ile kamu kurum ve kuruluşlarına ait fiziki ve elektronik adreslerin, reklam ve tanıtım amacıyla PTT hizmetlerinden yararlananlara ücret karşılığı kullandırılmasına yönelik olarak oluşturulan PTT'ye ait veri tabanını,"

b- Dava konusu (h) ve (ı) bentleri şöyledir:

"h) Evrensel posta hizmet yükümlüsü: Evrensel posta hizmetini görev sözleşmesi uyarınca sağlamakla yükümlü kılınan hizmet sağlayıcısını,"

"ı) Görev sözleşmesi: PTT'nin posta hizmetlerini sunmak üzere hak ve yükümlülüklerini belirleyen sözleşmeyi,"

2- Kanun'un 4. maddesinin (1) numaralı fıkrasının iptali istenen ibareleri de içeren (ç) bendi şöyledir:

"ç) Posta hizmetlerinde millî güvenlik, kamu düzeni ve genel sağlığın korunmasını teminen ilgili idari birimlerle iş birliği yaparak gerekli tedbirleri almak, posta yoluyla gönderilmesi yasak maddeler ile kabulü şarta bağlı gönderiler için düzenlemeler yapmak"

3- Kanun'un 6. maddesinin dava konusu (1) numaralı fıkrası şöyledir:

"(1) Aşağıdaki hizmetler evrensel posta hizmet yükümlüsünün tekelindedir:

a) Temel ücret göz önünde bulundurularak Kurumun önerisi ve Bakanlığın teklifi ile Bakanlar Kurulu tarafından ağırlığı veya ücreti belirlenen yurt içi ve yurt dışı haberleşme gönderilerinin kabulü, toplanması, işlenmesi, sevki, dağıtımı ve teslimi.

b) 4/1/1961 tarihli ve 213 sayılı Vergi Usul Kanununun elektronik tebliğe ilişkin hükümleri saklı kalmak kaydıyla, 7201 sayılı Kanun ve diğer kanunlar kapsamındaki elektronik ortam dâhil her türlü tebligatın kabulü, toplanması, işlenmesi, sevki, dağıtımı ve teslimi.

c) Barışta Türk Silahlı Kuvvetlerinin posta hizmetleri.

ç) Postada alınacak ücretleri gösteren posta pulları, kişisel pul, anma pulları, posta kartları ve ilk gün zarflarının bastırılıp satışa çıkarılması."

4- Kanun'un 7. maddesinin dava konusu ibareyi de içeren (1) numaralı fıkrası şöyledir:

"Hizmet sağlayıcıları ile posta hizmetlerinde çalışanlar veya herhangi bir şekilde posta hizmetleri ile ilgili bilgiye sahip olanların, bu bilgileri ve posta hizmetleri ile ilgili ilişkileri açığa vurmaları, gönderileri açmaları, içlerinde ne olduğunu araştırmaları, üçüncü kişilere bilgi vermeleri veya herhangi birinin bunları yapmasına neden olmaları, gönderileri zapt veya yok etmeleri yasaktır."

5- Kanun'un 9. maddesinin;

a- Dava konusu (3) numaralı fıkrası şöyledir:

"(3) PTT, bu Kanun çerçevesinde yurt içi ve yurt dışında posta hizmetlerini yürütmeye ve gerekli altyapıyı kurmaya yetkilidir. PTT'nin söz konusu yetkiye ilişkin hak ve yükümlülükleri Kurum ile imzalanacak görev sözleşmesi ile belirlenir. Bu sözleşme damga vergisi ve harçtan müstesnadır."

b- Dava konusu ibareyi de içeren (6) numaralı fıkrası şöyledir:

"(6) Kurum, yetkilendirme taleplerini, gerekli şartların sağlanamaması nedeniyle veya millî güvenlik, kamu düzeni ve genel sağlık gerekçeleri ile reddedebilir."

c- Dava konusu (8) numaralı fıkrası şöyledir:

"(8) Kurum, millî güvenlik, kamu düzeni ve genel sağlık gereklerinden kaynaklanan sebeplerin tespiti hâlinde, şirketlerin posta sektöründe faaliyete geçmelerini veya posta hizmeti sağlamalarını engelleyebilir."

6- Kanun'un 17. maddesinin dava konusu (2) numaralı fıkrası şöyledir:

"(2) Millî güvenlik ile kamu düzeni gereklerine ve acil durum ihtiyaçlarına ait düzenlemeler, ilgili bakanlıkların ihtiyaçları ve görüşleri dikkate alınarak Bakanlığın teklifi ve Bakanlar Kurulu kararıyla belirlenir."

7- Kanun'un dava konusu (a) bendini de içeren 23. maddesi şöyledir:

" (1) PTT'nin organları şunlardır:

a) Genel Kurul

b) Yönetim Kurulu

c) Genel Müdürlük"

8- Kanun'un dava konusu 24. maddesi şöyledir:

"(1) Genel Kurul; yıllık faaliyet raporu ile bilanço ve kâr zarar hesaplarını inceleyerek Yönetim Kurulunun ibrasını karara bağlar. Genel Kurul ayrıca, bu Kanun hükümleri saklı kalmak kaydıyla, 6102 sayılı Kanun ve ilgili kanunlarda belirtilen görevleri yapar ve yetkileri kullanır."

9- Kanun'un 25. maddesinin dava konusu (6) numaralı fıkrası şöyledir:

"(6) PTT Genel Müdürü ve Yönetim Kurulu üyelerinin görevleri sebebiyle işledikleri suçlardan dolayı yargılanmaları, ilgili Bakanın iznine bağlı olup, bu konuda 2/12/1999 tarihli ve 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun hükümleri uygulanır."

10- Kanun'un 29. maddesinin dava konusu (2) ve (3) numaralı fıkraları şöyledir:

"(2) PTT hizmetleri ile ilgili olarak herhangi bir talepte bulunmak ve PTT'nin sorumlu olduğu hâllerde dava etme hakkı o hizmetten yararlanana aittir.

(3) PTT hizmetleri ile ilgili olarak talepte bulunma ve dava açma hakkı faaliyet konusu işlemin tesisi tarihinden itibaren bir yılın sonunda zamanaşımına uğrar. Bu süre, PTT'ye başvuru ile kesilir ve yapılan inceleme ve araştırmaların sonucunun ilgililere bildirildiği tarihte kesildiği yerden yeniden başlar. Bu süre yeni bir başvuru ile tekrar kesilmez."

11- Kanun'un dava konusu geçici 3. maddesi şöyledir:

"(1) Görev sözleşmesi bu Kanunun yürürlüğe girdiği tarihten itibaren iki ay içinde düşüncesi alınmak üzere Danıştaya gönderilir. Danıştayın iki ay içinde düşüncesini bildirmesini müteakip, görev sözleşmesi PTT ile Kurum arasında imzalanarak yürürlüğe girer.

(2) Evrensel posta hizmet yükümlülüğü, görev sözleşmesi imzalanıncaya kadar, PTT tarafından yürütülür."

12- Kanun'un geçici 6. maddesinin dava konusu ibareleri de içeren (1) numaralı fıkrası şöyledir:

"(1) Mülga T.C. Posta ve Telgraf Teşkilatı Genel Müdürlüğünde 5510 sayılı Kanunun 4 üncü maddesinin birinci fıkrasının (c) bendine tabi olarak çalışan ve mevcut statülerinde PTT'de istihdamına devam olunan personel ile işçi statüsünde istihdam edilen personelden isteyenler Yönetim Kurulunca belirlenen esaslar çerçevesinde bu Kanunda tanımlanan sözleşmeli personel statüsüne geçirilebilir, geçmek istemeyenler ile geçmesi uygun görülmeyenlerin tabi olduğu mevzuatına göre istihdamına devam olunur."

B- Dayanılan ve İlgili Görülen Anayasa Kuralları

Dava dilekçesinde, Anayasa'nın 2., 5., 6., 7., 10., 11., 13., 22., 74., 123., 129., 167. ve 172. maddelerine dayanılmış, Anayasa'nın 20., 36. ve 142. maddeleri ise ilgili görülmüştür.

III- İLK İNCELEME

Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca Haşim KILIÇ, Serruh KALELİ, Alparslan ALTAN, Mehmet ERTEN, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT, Zehra Ayla PERKTAŞ, Recep KÖMÜRCÜ, Burhan ÜSTÜN, Engin YILDIRIM, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Erdal TERCAN, Muammer TOPAL ve Zühtü ARSLAN'ın katılımlarıyla 5.9.2013 gününde yapılan ilk inceleme toplantısında, dosyada eksiklik bulunmadığından işin esasının incelenmesine, yürürlüğü durdurma isteminin ise esas inceleme aşamasında karara bağlanmasına OYBİRLİĞİYLE karar verilmiştir.

IV- ESASIN İNCELENMESİ

Dava dilekçesi ile ekleri, Başraportör Mustafa ÇAĞATAY tarafından hazırlanan işin esasına ilişkin rapor, dava konusu yasa kuralları, dayanılan ve ilgili görülen Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

1- Kanun'un 3. Maddesinin (1) Numaralı Fıkrasının (a) Bendindeki "...ilgili mevzuatı saklı kalmak kaydıyla," İbaresinden Sonra Gelen "...gerçek..." İbaresinin İncelenmesi

Dava dilekçesinde, kuralla "adres bilgi kayıt sistemi" adı altında, gerçek ve tüzel kişiler ile kamu kurum ve kuruluşlarına ait fiziki ve elektronik adreslerin, reklam ve tanıtım amacıyla PTT hizmetlerinden yararlananlara ücret karşılığı kullandırılmasına yönelik olarak veri tabanı oluşturulduğu, ticari amaçlarla veri tabanı oluşturulmasında gerçek kişilerin rızası aranırken, tüzel kişilerin rızasının aranmadığı, kuralın tüzel kişilerin reklam ve tanıtım amacıyla fiziki ve elektronik adreslerini kullandırmak istemeseler dahi rızaları dışında kanunla kullandırma yetkisinin verildiği,

ayrıca posta ve kargo taşımacılığı sektöründe faaliyet gösteren özel hukuk tüzel kişisi ticari işletmesi olan PTT A.Ş. ile aynı sektörde faaliyet gösteren diğer özel hukuk tüzel kişisi ticari işletmeler arasında sermayeye sahiplik dışında hukuken hiçbir fark bulunmadığı hâlde PTT A.Ş.'ye ayrıcalık tanındığı belirtilerek kuralın, Anayasa'nın 2. ve 10. maddelerine aykırı olduğu ileri sürülmüştür.

6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 43. maddesine göre, ilgisi nedeniyle dava konusu kural Anayasa'nın 20. maddesi yönünden de incelenmiştir.

Kanun'un 3. maddesinde, Kanun'da geçen bazı sözcük, ibare ve kavramların ne anlama geldiğine ilişkin tanımlamalara yer verilmiştir. Dava konusu ibarenin de yer aldığı (a) bendinde, aynı Kanun'un 22. maddesinin (1) numaralı fıkrasında PTT'nin faaliyetleri arasında belirtilen "Adres bilgi kayıt sistemi"nin neyi ifade ettiği hususu belirtilmiştir. Buna göre, adres bilgi kayıt sistemi, 25.4.2006 günlü, 5490 sayılı Nüfus Hizmetleri Kanunu ve ilgili mevzuatı saklı kalmak kaydıyla, gerçek kişilerin rızası alınarak gerçek ve tüzel kişiler ile kamu kurum ve kuruluşlarına ait fiziki ve elektronik adreslerin, reklam ve tanıtım amacıyla PTT hizmetlerinden yararlananlara ücret karşılığında kullanılarak oluşturulan PTT'ye ait veri tabanını ifade etmektedir. Dava konusu ibare, adres bilgi kayıt sisteminde, gerçek kişilerin rızasını aramaktadır. Dolayısıyla, ibarenin mefhumu muhalifinden, tüzel kişiler yönünden onların rızalarının alınmasına gerek bulunmadığı anlamı çıkmaktadır.

Anayasa'nın 20. maddesinde, herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı ifade edilmiştir. Maddede ayrıca kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hükmüne de yer verilmiştir.

Kişisel verilerin korunması temel hakkı, anayasa hukukunda esas olarak yüksek kişilik değerlerini korumaya yönelik bireysel haklara ilişkindir. Bu hak, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır.

Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda, bir kişinin kendisinin veya ailesinin sürekli ve geçici olarak konakladığı, ikamet ettiği yerlere ait bilgiler (fiziki adresler) de kişisel veri niteliğindedir. Aynı şekilde, elektronik posta olarak adlandırılan ve elektronik iletişim ağı üzerinden gönderilen ve

internette ya da kullanıcının bilgisayarında kaydedilebilen her türlü yazı, ses, resim ya da dil iletilerinin de kişisel veri niteliğinde olduğu kabul edilmektedir.

Anayasa'nın 20. maddesinde kişisel verilerin kişi bakımından korunma alanının gerçek kişiler ya da tüzel kişileri veya her ikisini içine alıp almadığı konusunda bir açıklık bulunmamaktadır. Maddenin gerekçesinde de buna ilişkin bir değerlendirme yoktur. Her ne kadar Anayasa'nın 20. maddesinde daha ziyade gerçek kişilerin özel hayatı ve bu bağlamda gerçek kişilere ilişkin kişisel verilerin korunma altında bulundurulduğu ileri sürülebilir ise de madde metninde kişisel verilerle ilgili olarak "herkes" tabirinin kullanılması dikkate alındığında, tüzel kişilere ilişkin verilerin de 20. madde kapsamında değerlendirilmesi gerekeceği açıktır.

Anayasa'nın 148. maddesinin üçüncü ve 6216 sayılı Kanun'un 45. maddesinin (1) numaralı fıkraları uyarınca, Anayasa'da güvence altına alınmış temel hak ve özgürlüklerinden, Avrupa İnsan Hakları Sözleşmesi ve buna ek Türkiye'nin taraf olduğu protokoller kapsamındaki herhangi birinin kamu gücü tarafından ihlal edildiğini iddia eden herkese Anayasa Mahkemesine bireysel başvuru yapma hakkı tanınmıştır. Buna göre, medeni haklara sahip gerçek kişilerin yanında tüzel kişilerin de bireysel başvuru yönünden dava ehliyetine sahip oldukları açıktır.

4721 sayılı Türk Medeni Kanunu'nun "Hak ehliyeti" başlıklı 48. maddesinde ise "Tüzel kişiler, cins, yaş, hısımlık gibi yaradılış gereği insana özgü niteliklere bağlı olanlar dışındaki bütün haklara ve borçlara ehildirler." denilmektedir.

Esasen her ne kadar 95/46/EC sayılı Avrupa Veri Koruması Direktifi'nde yer alan tanım, tüzel kişilere ilişkin verileri dışlamakta ve kişisel veri kapsamına yalnızca gerçek kişilere ilişkin bilgilerin gireceğini kabul etmekte ise de, gerek "Elektronik haberleşme sektöründe kişisel bilgilerin işlenmesi ve gizliliğinin korunması" hakkında 12.7.2002 gün ve 2002/58/EC sayılı Avrupa Parlamentosu ve Konsey Direktifi'nde, yalnızca elektronik haberleşme sektörüne ilişkin olarak, hem gerçek kişilerin hem de tüzel kişilerin veri sahibi kabul edileceğinin ifade edilmesi; gerekse son yıllarda kabul edilen bazı ülke kanunlarında tüzel kişilerin de kişisel verilerin korunma alanına dâhil edilmesi bir bütün olarak dikkate alındığında, Avrupa ve Dünyadaki gelişimin kişisel verilerin korunmasında tüzel kişilerin de kapsamda yer alması gerektiği yönünde olduğu görülmektedir.

Bu durumda, Anayasa'nın 20. maddesinde kişisel verilerin "ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği"nin açıkça ifade edilmesi karşısında, tüzel kişilerin kişisel veri niteliğinde bulunan fiziki veya elektronik adreslerinin, yetkili kişi ya da organlarının rızaları alınmaksızın, dava konusu kural uyarınca PTT A.Ş. tarafından reklam ve tanıtım amacıyla toplanıp kaydedilmesinin ve bunların üçüncü kişilere verilmesinin, Anayasa'nın 20. maddesine aykırılık

oluşturduğu açıktır. Tüzel kişilere ilişkin kişisel verilerin ilgili kanunlar gereği ya da kişilerin kendilerince kamuya açıklanmış olması veya açık sicillerde yer almış olması, söz konusu verilerin ticari amaçlarla üçüncü kişilere aktarımına rıza gösterildiği anlamına gelmez.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 20. maddesine aykırıdır. İptali gerekir.

Hicabi DURSUN, Muammer TOPAL, M. Emin KUZ ile Hasan Tahsin GÖKCAN bu görüşe katılmamışlardır.

Kural, Anayasa'nın 20. maddesine aykırı görülerek iptal edildiğinden dolayı Anayasa'nın 2. ve 10. maddeleri yönünden ayrıca incelenmesine gerek görülmemiştir.

2- Kanun'un 3. Maddesinin (1) Numaralı Fıkrasının (h) ve (ı) Bentlerinin, 6. Maddesinin (1) Numaralı Fıkrasının, 9. Maddesinin (3) Numaralı Fıkrasının ve Geçici 3. Maddesinin incelenmesi

a- Posta Sektörünün Düzenlenmesine İlişkin Genel Açıklamalar

1990'lardan itibaren posta hizmetleri piyasalarının serbestleştirilerek rekabete açılmasına yönelik yaklaşımların Dünya genelinde uygulama alanı bulmaya başladığı gözlemlenmektedir. Bu tür serbestleşmeye yönelik uygulamalarda ekonomik ve sosyal gerekçelerle birlikte, Avrupa Birliği gibi birliklerde hem ülkeler hem de piyasalar açısından sınırların kaldırılması düşüncesinin de önde gelen faktörlerden biri olduğu görülmektedir. Bu faktörlerin yanında, gelişen iletişim teknolojileri ve küreselleşme eğilimi de posta piyasalarının serbestleştirilmesi ve rekabete açılmasında önemli bir paya sahiptir.

Ancak bu sektörlerin devlet tarafından tekel olarak işletilmesinin istenilen verimi ve toplumsal refaha beklenen katkıyı sağlayamaması gibi nedenlerle, devletin özelleştirme ve serbestleştirme yolu ile bu piyasalardan çekilmesi ile tekelci özellik gösteren bu piyasalarda devletçi politikalar, yerini düzenlenmiş piyasalara bırakmakta ve bu alanlar faaliyet gösterdikleri sektörlerin siyasi-idarî etkilenmelerden uzak objektif, şeffaf ve öngörülebilir kurallar ile çalışmasını sağlamak amacıyla kurulmuş olan bağımsız düzenleyici kurumlar tarafından doldurulmaktadır.

Bu bağlamda, Kanunla ülke genelinde posta hizmetlerinin kaliteli, sürekli, tüm kullanıcılar için karşılanabilir bir ücretle ve etkin rekabete dayalı esaslar çerçevesinde sunulmasını sağlamak amacıyla posta sektörünün serbestleştirilmesi ile mali açıdan güçlü, istikrarlı ve şeffaflığı sağlanmış sektörde düzenleme ve denetimin gerçekleştirilmesi hedeflenmiştir.

Mülga 5584 sayılı Posta Kanunu'nda, tüm açık ve kapalı mektuplar ile ağırlık ve ücret limiti olmaksızın üzerinde haberleşme mahiyetinde yazı bulunan kartlar, 7201 sayılı Tebligat Kanunu

kapsamındaki her türlü tebliğ evrakının kabulü, toplanması, işlenmesi, sevk ve dağıtım ile postada alınacak ücretleri gösteren posta pulları, anma pulları, posta kartları, ilk ve özel gün zarflarını bastırıp satışa çıkarmak PTT'nin tekeli kapsamında iken piyasada fiili bir durum meydana gelmiş ve çeşitli koli-kurye şirketleri PTT'nin yaptığı işleri yapmaya başlamışlardır. Ancak bu hizmetleri verirken bu şirket ya da kuruluşların herhangi bir yasal bir mevzuatı ve dayanağı bulunmamaktaydı. Sektörde yaşanan bu fiili durumun önlenmesi ve bu durumun çözüme kavuşturulması amacıyla, Türkiye'nin AB üyeliği sürecinde ve AB'nin bu konuda geçerli direktifleri de dikkate alınarak, 6475 sayılı Kanunla yapılan düzenlemelerle sektörde faaliyet sürdüren koli-kurye şirketlerinin durumu yasal bir zemine kavuşturulmuş, ayrıca sektörde PTT dışında başka işletmeler de faaliyetlerini sürdüreceği için sektörün düzenlenmesi görevi Bilgi Teknolojileri ve İletişim Kurumuna (BTK) verilmiştir.

Kanun'un 4. maddesiyle, BTK, posta hizmetlerinin; güvenilir, kesintisiz bir şekilde verilmesinin sağlanması, yetki belgelerinin kapsamı, verilmesi, denetlenmesi, rekabeti tesis etme ve rekabeti engelleyici, bozucu veya kısıtlayıcı uygulamaları giderme ve bu amaçla ilgili pazarlarda etkin piyasa gücüne sahip hizmet sağlayıcılara ve gerekli hâllerde diğer hizmet sağlayıcılara yükümlülükler getirme ve tedbirler alma yetkisini haiz düzenleyici ve denetleyici bir üst kurum olarak görevlendirilmiştir.

Yurtiçi ve yurtdışı posta hizmetlerini, belirlenmiş ilke ve kurallarla ülke genelinde bütün yerleşim birimlerinde, her iş gününde, herkese, eşit ücretle sunan ve bu anlamda fiili olarak evrensel hizmet sağlayıcısı konumundaki PTT, Kanunla evrensel posta hizmet yükümlüsü olarak, diğer özel hukuk tüzel kişileri ise BTK'dan alacakları yetki belgesi çerçevesinde evrensel hizmet sağlayıcısı olarak faaliyette bulunacaklardır.

b- Kuralların Anlam ve Kapsamı

Dava konusu kurallarda; evrensel posta hizmet yükümlüsünün tanımı ve bu yükümlülüğü görev sözleşmesi uyarınca yerine getirecek olan, kuruluş ve tescile ilişkin hükümleri hariç olmak üzere 6102 sayılı Türk Ticaret Kanunu ve özel hukuk hükümlerine tabi, sermayesinin tamamı hazineye ait olan "kamu kurumu niteliği ağır basan" bir anonim şirket statüsünde yapılandırılan PTT A.Ş.'nin, AB Direktifleri ile Katılım Ortaklığı Belgeleri'nde ülkemizin taahhütleri arasında yer alan posta sektörünün rekabete açılması amacıyla kontrollü ve kademeli olarak serbestleştirilmesinin sağlanmasına paralel olarak, görev ve tekel kapsamında sunacağı hizmetlere ilişkin düzenlemeler yer almaktadır. Buna göre, Kanun'un 3. maddesinin (1) numaralı fıkrasının (h) ve (ı) bentleriyle, PTT, evrensel posta hizmetini görev sözleşmesi uyarınca sağlamakla yükümlü "evrensel posta hizmeti yükümlüsü" olarak görevlendirilmiştir. Kanun'un 6. maddesinin (1) numaralı fıkrasında, PTT'nin

evrensel hizmet yükümlüsü olarak sahip olduğu tekel hizmetinin kapsam ve sınırları belirtilmiş, Kanun'un 9. maddesinin (3) numaralı fıkrası ile geçici 3. maddesinde ise PTT ile BTK arasında imzalanacak görev sözleşmesi ve bunun yürürlük prosedürüne ilişkin hükümlere yer verilmiştir

Kanun'un 3. maddesinin (1) numaralı fıkrasının dava konusu edilmeyen (g) bendinde, belirlenmiş ilke ve kurallar çerçevesinde, bir posta hizmetinin coğrafi alan farkı gözetilmeksizin ülke sınırları içerisinde tüm kullanıcılar için karşılanabilir ücretlerle kesintisiz olarak sağlanması olarak tanımlanan "evrensel posta hizmeti"nin, "evrensel posta hizmet sağlayıcıları" ve "evrensel posta hizmet yükümlüsü" tarafından yerine getirilmesi öngörülmüş ve Kanun'un 3. maddesinin (1) numaralı fıkrasının dava konusu (h) bendinde ise evrensel posta hizmet yükümlüsünün, evrensel posta hizmetini görev sözleşmesi uyarınca sağlamakla yükümlü kılınan hizmet sağlayıcısı olduğu ifade edilmiştir.

Kanun'un 3. maddesinin (1) numaralı fıkrasının dava konusu (ı) bendinde, Kanun'da geçen görev sözleşmesi kavramının ne anlama geldiği belirtilmiştir. Buna göre, görev sözleşmesi, PTT'nin posta hizmetlerini sunmak üzere hak ve yükümlülüklerini belirleyen sözleşme olarak tanımlanmıştır.

Kanun'un dava konusu geçici 3. maddesinin (1) numaralı fıkrasında, görev sözleşmesinin Kanun'un yürürlüğe girdiği tarihten itibaren iki ay içinde düşüncesi alınmak üzere Danıştaya gönderileceği ve Danıştayın iki ay içinde düşüncesini bildirmesini müteakip, PTT ile BTK arasında imzalanarak yürürlüğe gireceği hüküm altına alınmıştır. Aynı maddenin (2) numaralı fıkrasında ise evrensel posta hizmet yükümlülüğünün, görev sözleşmesi imzalanıncaya kadar PTT tarafından yürütüleceği hükme bağlanmıştır.

Kanun'un 6. maddesinde, posta tekeline ilişkin hükümlere yer verilmiştir. Maddenin dava konusu (1) numaralı fıkrasında ise evrensel posta hizmet yükümlüsü olan PTT'nin tekeli kapsamında kalan hususlar sınırlı olarak belirtilmiştir. Buna göre;

- Temel ücret göz önünde bulundurularak BTK'nın önerisi ve Ulaştırma, Denizcilik ve Haberleşme Bakanlığının teklifi ile Bakanlar Kurulu tarafından ağırlığı veya ücreti belirlenen yurt içi ve yurt dışı haberleşme gönderilerinin kabulü, toplanması, işlenmesi, sevki, dağıtımı ve teslimi,

- 4.1.1961 günlü, 213 sayılı Vergi Usul Kanunu'nun elektronik tebliğe ilişkin hükümleri saklı kalmak kaydıyla, 7201 sayılı Kanun ve diğer kanunlar kapsamındaki elektronik ortam dâhil her türlü tebligatın kabulü, toplanması, işlenmesi, sevki, dağıtımı ve teslimi,

- Barışta Türk Silahlı Kuvvetlerinin posta hizmetleri,

- Postada alınacak ücretleri gösteren posta pulları, kişisel pul, anma pulları, posta kartları ve ilk gün zarflarının bastırılıp satışı çıkarılması,

biçimindeki hizmetler, evrensel posta hizmet yükümlüsü olan PTT'nin tekeli altında yerine getirilecektir.

c- Anayasa'ya Aykırılık Sorunu

ca- Anayasa'nın 167. ve 172. Maddeleri Yönünden İnceleme

Dava dilekçesinde, posta işletmeciliği sektörünün, ancak Anayasa'nın 22. maddesinde belirtilen "gizliliği" güvence altına almak amacıyla ve "kamu yararı" gerekçesi ile kamu tekeli kapsamına alınabileceği, bu şekilde tekel kapsamına alınan posta hizmetinin ise sermayesinin tamamı Devlete ait özel hukuk tüzel kişisi ticari işletme lehine değil sermayesinin tamamı Devlete ait olup tekel niteliğindeki mal ve hizmetleri kamu yararı gözeterek üretmek ve pazarlamak üzere kurulan ve gördüğü bu kamu hizmeti dolayısıyla ürettiği mal ve hizmetler imtiyaz sayılan kamu iktisadi teşebbüsü lehine oluşturulması gerektiği, dava konusu kurullarla kamu yararı gerekçesine dayalı kamu hizmeti kapsamına alma olmadan, rekabetçi posta hizmetleri sektörünün tekel kapsamına alınarak, sektörel rekabetin ve dolayısıyla ekonomik etkinlik ile tüketici refahının dışlandığı belirtilerek kurulların, Anayasa'nın 167. ve 172. maddelerine aykırı olduğu ileri sürülmüştür.

Anayasa'nın 167. maddesinde, "Devlet, para, kredi, sermaye, mal ve hizmet piyasalarının sağlıklı ve düzenli işlemelerini sağlayıcı ve geliştirici tedbirleri alır; piyasalarda fiilî veya anlaşma sonucu doğacak tekelleşme ve kartelleşmeyi önler.

Dış ticaretin ülke ekonomisinin yararına olmak üzere düzenlenmesi amacıyla ithalat, ihracat ve diğer dış ticaret işlemleri üzerine vergi ve benzeri yükümlülükler dışında ek mali yükümlülükler koymaya ve bunları kaldırmaya kanunla Bakanlar Kuruluna yetki verilebilir." denilmektedir.

Bu hükümlerle yalnız fiilen oluşacak tekelleşme ve kartelleşmenin değil, anlaşma sonucu doğacak tekelleşme ve kartelleşmenin de önlenmesi görevi Devlete verilmiştir. Madde gerekçesinde, "tekelleşme" kavramı açıklanırken, yalnız tekellerin değil, tekel benzeri gruplaşmaların da bu kapsamda görüldüğü belirtilmiştir. Ayrıca, tekelleşmenin önlenmesinin tüketim sektörü yanında hizmet sektörü yönünden de gerekliliği vurgulanmış, bu görevin "sağlıklı bir toplum" ve "sağlıklı bir demokrasinin" vazgeçilmez koşulu olduğu belirtilmiştir. Buna göre, tekelciliğin her türünün zararından bireyleri ve toplumu korumak "kişinin ve toplumun huzuru ve refahı" ile de ilgilidir. Maddede yalnız, tekelleşme değil, tekel oluşturmayan üretim ve hizmet kuruluşlarının "fiyat anlaşmaları", "coğrafi bölge paylaşma" ve "benzeri suretle" gerçekleştirilecek kartelleşme de

yasaklanmış; Devlet, bunu engelleyici önlemleri almakla yükümlü tutulmuştur. Böylece, rekabetin ortadan kaldırılması, tekellerin ve kartellerin fiyatları oluşturması ve etkilemesi önlenmek istenmiştir.

Devletin tekelleşmeyi ve kartelleşmeyi önlemek görevi, temelde tüketiciyi koruma amacı gütmektedir. Anayasa'nın 172. maddesi ile Devlete verilen tüketicileri koruma görevi ancak, tekelleşme ve kartelleşmelerin önlenerek özgür rekabet ortamının sağlanması ile güvenceye alınabilir. Piyasa ekonomisinin etkinliği, serbest rekabet koşullarının varlığına bağlıdır. Tekelleşmeye veya kartelleşmeye olanak veren ortamlarda piyasa ekonomisi etkinliğini yitirir. Tekel konumundaki bir kuruluş önlem alınmadan özelleştirildiğinde, kamu tekelinin yerini özel tekelin alması kaçınılmazdır. Üstelik kamu tekeli konumundaki mal ve hizmet üretiminde Devletin doğrudan karışması olanağı varken, özel tekel durumunda bu olanak da söz konusu olmayacak, mal ve hizmet fiyatları kamu tekelinde olduğundan daha yüksekte belirleneceği gibi kalite de bundan olumsuz etkilenecektir. Bu nedenle, özelleştirmeye ilişkin yasal düzenlemelerde, tekelleşme ve kartelleşmeyi önlemeye, dolayısıyla bireyleri ve toplumu korumaya yönelik kuralların bulunması zorunludur.

Toplumun günlük yaşamında önemli bir yere sahip olan ve teknolojik gelişmelerin hızlı bir şekilde yaşandığı enerji, gaz, su ve haberleşme gibi mal ve hizmetlerin üretildiği piyasaların, Devletin herhangi bir müdahalesi olmaksızın pazar koşullarına terk edilmesi, bu piyasalarda aksaklıklara yol açması nedeniyle kabul edilmemektedir. Bu nedenle rekabetin yaşanmadığı, piyasa aksaklıklarının olduğu durumlarda veya bazı sosyal gerekçelerle, piyasa ekonomisini bir sistem tercihi olarak ortaya koyan ülkelerde dahi devletler, piyasanın işleyişine çeşitli vasıtalarla ve belirli sınırlar içinde müdahale etmektedir. Devletlerin bu piyasalara müdahalesi, bazı sektörlerin kamu tarafından tekel olarak işletilmesi ya da bu sektörlerdeki özel işletmelerin regülasyonu şeklinde olmaktadır.

Dava konusu kurallarla yapılmak istenen de posta sektörünün serbestleştirilmesi durumunda, toplumun tüm kesimlerine sürekli ve belirlenmiş bir kalite standardında ve karşılanabilir fiyatlarla posta hizmeti sunumunun Devlet tarafından garanti altına alınmasıdır. Zira, evrensel posta hizmetinin sağlanmasının garanti altına alınması, Devletin temel bir yükümlülüğüdür. Toplum ve ihtiyaçları değişip geliştikçe Devlet, sunumunda kamu yararı görülen hizmetler de dâhil olmak üzere haberleşme hakkı gibi vatandaşlık haklarının temel bileşenleri olan değişik hizmetlerin sunumunun devamının sağlanmasını garanti altına almakla yükümlüdür. Diğer taraftan söz konusu hizmetlerin evrenselliği nedeniyle hizmetlerin bir milletin bütün fertlerine sunumu, yaşadıkları bölge, ırk, din, sosyal statü gibi unsurlardan bağımsız olmak üzere garanti altına alınmalıdır.

Kanun'un 6. maddesinde, PTT lehine getirilen tekel, evrensel posta hizmetinin ülkenin her tarafına kesintisiz ve makul ücretlerle götürülebilmesinin hem garanti altına alınması hem de bu hizmetin

getirdiği mali yükün bu şekilde hafifletilmesi amacına yöneliktir. Nitekim PTT'ye verilen tekel kapsamındaki hizmetler ve bunlar için ağırlık sınırlamaları öngörülmesi, üye devletlerin belli alanlarda evrensel hizmet yükümlüsü lehine tekel oluşturabileceği yönündeki AB'nin 97/67/CE sayılı Direktifi'yle de uyumlu olduğu anlaşılmaktadır. Bu durumun Anayasa'nın 167. ve 172. maddelerine aykırı bir yönünün bulunmadığı açıktır.

Diğer taraftan, dava konusu kurallarla, dava dilekçesinde belirtildiği üzere, özel hukuk tüzelkişisi lehine bir tekel oluşturulması da söz konusu değildir. Zira, sermayesinin tamamı Hazineye ait olan PTT'nin "kamu kurumu niteliği ağır basan" bir anonim şirket statüsünde bulunduğu dikkate alındığında, dava konusu kurallarla bir kamu hizmeti olan posta hizmetlerinin yine bir kamu kurumunun özel hukuk hükümlerine göre faaliyet gösteren bir birimi tarafından yerine getirilmesi sağlanmaktadır. Bir başka ifadeyle, mülga 5584 sayılı Posta Kanunu'nda, ağırlık ve ücret limiti olmaksızın, tüm açık ve kapalı mektuplar ile haberleşme mahiyetinde yazı içeren kartlar üzerinde bulunan tekel hakkı bir KİT olan PTT'ye ait iken; bu kez aynı tekel hakkı AB Direktifleri doğrultusunda Bakanlar Kurulu tarafından belirlenecek belli ağırlık veya ücretlerle sınırlı olarak daraltılmak suretiyle yine kamu kurumu niteliği ağır basan anonim şirket statüsündeki PTT A.Ş.'ye verilmektedir.

Açıklanan nedenlerle, dava konusu kurallar Anayasa'nın 167. ve 172. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir.

cb- Anayasa'nın 10. Maddesi Yönünden İnceleme

Dava dilekçesinde, kamu yararı gerekçesi ile kanunla kamu tekeline alınarak kamu hizmeti statüsü tanınan bir hizmetin özel hukuk tüzel kişileri tarafından yürütülebilmesinin tüm sorumluluk lehine tekel tesis edilen kamu idaresi üzerinde kalmak kaydıyla, onun sürekli gözetimi ve denetimi altında, belli yasal usullerle kamu tekeli imtiyazının devri suretiyle mümkün olabileceği hâlde imtiyazın devri ihalesi açılmadan posta tekeli imtiyazının kanunla da olsa ve sermayesi Devlete de ait bulunsa herhangi bir özel hukuk tüzel kişisi olan bir ticari şirkete verilmesinin eşitlik ilkesine aykırı olduğu belirtilerek kuralların, Anayasa'nın 10. maddesine aykırı olduğu ileri sürülmüştür.

Kamu hukukunun genel ilkeleri gereğince, kamu hizmet ve faaliyetlerinin bizâtihi idare kuruluş ve kurumları eliyle, kamusal yönetim biçimine göre yürütülmesi asıl ve olağandır. Ancak, bu hizmet ve faaliyetlerden kamu gücüne özgü olmayanlar ile özel yönetim biçimiyle gerçekleştirilmeye elverişli bulunanlar, tüm sorumluluk yine ilgili idare üzerinde kalmak kaydıyla, onun sürekli gözetimi ve denetimi altında, belli yasal usullerle özel müteşebbislere yaptırılabilir. Özel yönetim biçimiyle yürütülmeye elverişli olan kamu faaliyet ve hizmetlerinin, özel teşebbüse gördürülebilmesi ise bunun

kanunlarda öngörölmüş bulunmasına baęlıdır; yürütme ve idare kendilięinden bu yolu seçemez ve diledięi yöntemi kullanamaz. Konusu, kamu hizmetinin kurulmasını ve/veya işletilmesini bir özel kişiye devretmek olan sözleşmeler "kamu hizmeti imtiyaz sözleşmeleri" olarak tanımlanmaktadır.

Kamu hizmeti imtiyaz sözleşmeleri, gerek konusunun bir kamu hizmetinin kurulması ve/veya işletilmesi olması, gerekse hizmetin yürütülmesini sağlamak için hizmeti yapanlara kamu gücüne dayanan kimi yetkiler tanınması, aynı zamanda idarenin, hizmetin düzenli ve istikrarlı biçimde yürütülmesini sağlamak için denetim ve gözetim yetkisine sahip olması yönünden idarî sözleşmelerin tüm niteliklerini taşırlar.

Kanun'un dava konusu 3. maddesinin (1) numaralı fıkrasının (1) bendinde, 9. maddesinin (3) numaralı fıkrasında ve geçici 3. maddesinde öngörölen ve PTT ile BTK arasında imzalanacak olan görev sözleşmesinin, idari sözleşme türlerinden olan bir "imtiyazın devri sözleşmesi" niteliğinde olmadığı açıktır. Zira, imtiyaz sözleşmelerinde idari sözleşmenin bir tarafında kamu idaresi, dięer tarafında ise özel hukuk kişisi bulunmaktadır. Oysa, PTT ile BTK arasında imzalanan ve dayanaęını kanundan alan görev sözleşmesinin her iki tarafı da kamu kurumudur. Yukarıda belirtildięi üzere burada, bir kamu hizmeti olan evrensel posta hizmeti, yine kamu kurumu nitelięi ağır basan ve sermayesinin tamamı Devlete ait olan ancak özel hukuk hükümlerine göre faaliyetlerini sürdüren PTT A.Ş. tarafından yerine getirilmektedir. Bir başka ifadeyle imtiyaz sözleşmelerinde olduğu gibi kamu idaresi tarafından yürütölmekte olan bir kamu hizmetinin özel hukuk tüzel kişisine gördürölmesi gibi bir durum söz konusu olmaması nedeniyle, PTT A.Ş.'ye dięer özel hukuk tüzel kişileri karşısında bir ayrıcalık tanınmasının söz konusu olmadığı, dolayısıyla da eşitlik ilkesine aykırı bir durumdan söz edilemeyeceęi açıktır.

Öte yandan, tekel döneminden serbest rekabet dönemine geçişin hukuk güvenliğini zedelemeyen gerçekleştirilebilmesi kimi şirketler için farklı düzenlemeleri gerekli kılabilir. Bir başka ifadeyle, Anayasa'nın 167. maddesi ile Devlete verilen para, kredi, sermaye, mal ve hizmet piyasalarının sağlıklı ve düzenli işlemlerini sağlayıcı ve geliştirici tedbirleri alma görevi böyle bir düzenlemeyi gerektirebilir. Dolayısıyla, bu düzenlemelere baęlı tutulanların serbest piyasa düzeni içinde faaliyet gösteren şirketlerle aynı konumda oldukları düşünölemez.

Açıklanan nedenlerle, dava konusu kurallar Anayasa'nın 10. maddesine aykırı değildir. İptal istemlerinin reddi gerekir.

3- Kanun'un 4. Maddesinin (1) Numaralı Fıkrasının (ç) Bendinde Yer Alan ".milli güvenlik, kamu düzeni ve genel saęlığın korunmasını teminen." İbaresini ile ".posta yoluyla gönderilmesi yasak maddeler ile kabulü şartta baęlı gönderiler için." İbaresinin İncelenmesi

Dava dilekçesinde, kuralda geçen "millî güvenlik", "kamu düzeni" ve "genel sağlığın korunması" gibi kavramların belirsiz olduğu, ayrıca kuralda "posta yoluyla gönderilmesi yasak maddeler ile kabulü şarta bağlı gönderiler" in neler olduğu belirtilmeksizin BTK'ya bu konuda yetki verilmesinin yasama yetkisinin devri anlamına geleceği ve ayrıca bu durumun idarenin kanuniliği ilkesiyle de bağdaşmayacağı belirtilerek kuralın, Anayasa'nın 2., 7. ve 123. maddelerine aykırı olduğu ileri sürülmüştür.

Kanun'un 4. maddesinin dava konusu ibarelerin de yer aldığı (1) numaralı fıkrasının (ç) bendinde, BTK'nın posta sektörünün posta hizmetlerinde millî güvenlik, kamu düzeni ve genel sağlığın korunmasını sağlamak amacıyla ilgili idari birimlerle iş birliği yaparak gerekli tedbirleri alma ve posta yoluyla gönderilmesi yasak maddeler ile kabulü şarta bağlı gönderiler için düzenlemeler yapma görevinin olduğu hükme bağlanmaktadır.

Anayasa'nın 2. maddesinde öngörülen hukuk devletinin temel ilkelerinden biri "belirlilik"tir. Bu ilkeye göre, yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır, uygulanabilir ve nesnel olması, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi gerekir. Belirlilik ilkesi, hukuksal güvenlikle bağlantılı olup birey, kanundan, belirli bir kesinlik içinde, hangi somut eylem ve olguya hangi hukuksal yaptırımın veya sonucun bağlandığını bilmelidir. Birey ancak bu durumda kendisine düşen yükümlülükleri öngörebilir ve davranışlarını ayarlar. Hukuk güvenliği, normların öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar.

Uygulamada yerleşmiş, uygulama ve öğretinin yardımıyla açıklık kazanmış, hukuk ve anayasa diline girmiş "millî güvenlik", "kamu düzeni" ve "genel sağlığın korunması" gibi kavramların anlamlarının yoruma muhtaç olduğu ya da belirsiz olduğu söylenemez.

Anayasa'nın 7. maddesinde, yasama yetkisinin Türk Milleti adına Türkiye Büyük Millet Meclisine ait olduğu vebu yetkinindevredilemeyeceği belirtilmiştir.

Anayasa'da kanunla düzenlenmesi öngörülen konularda, yürütme organına genel ve sınırları belirsiz bir düzenleme yetkisinin verilmesi olanaklı değildir. Yürütmenin düzenleme yetkisi, sınırlı, tamamlayıcı ve bağımlı bir yetkidir. Ayrıca, yürütme organına düzenleme yetkisi veren bir yasa kuralının Anayasa'nın 7. maddesine uygun olabilmesi için temel ilkeleri koyması, çerçeveyi çizmesi, sınırsız, belirsiz, geniş bir alanı yürütmenin düzenlemesine bırakmaması gerekir.

Farklı kořul ve durumlara göre sık sık deęişik önlemler alma, bunları kaldırma ve süratli biçimde hareket etme zorunluluęunun bulunduęu alanlarda, yasama organının temel kuralları saptadıktan sonra, uzmanlık ve teknik konulara iliřkin hususları yürütmeye bırakması, yasama yetkisinin devri olarak yorumlanamaz.

Anayasa'nın 123. maddesinde ise idarenin, kuruluş ve görevleriyle bir bütün olduęu ve "kanunla" düzenleneceęi kurala bağlanmıştır. Bu maddede yer alan düzenleme, idarenin kanunilięi ilkesine işaret etmektedir. İdarenin kanunilięi ilkesi, idarenin ve organlarının görev ve yetkilerinin hiçbir duraksamaya yer vermeyecek şekilde, açık bir biçimde kanunla düzenlenmesini gerekli kılar.

Telekomünikasyon sektörünü düzenleme ve denetleme fonksiyonunun baęımsız bir idari otorite tarafından yürütülmesi amacıyla 5.4.1983 günlü, 2813 sayılı Telsiz Kanunu'nda deęişiklik yapan 27.1.2000 günlü, 4502 sayılı Kanunla Telekomünikasyon Kurumu kurulmuř ve daha sonra 10.11.2008 günlü, 5809 sayılı Elektronik Haberleřme Kanunu ile yeni bir düzenlemeye tabi tutularak adı Bilgi Teknolojileri ve İletişim Kurumu olarak deęiřtirilmiştir. Kendisine verilen görev ve yetkiler çerçevesinde, temel işlevi telekomünikasyon alanındaki kamusal ve özel kesim etkinliklerini kurallar koyarak düzenlemek, konulan kurallara uyulup uyulmadığını izlemek, denetlemek ve bu kurallara uyulmaması hâlinde de ya doğrudan doğruya yaptırım uygulamak veya bazen de kanunlarda gösterilen yaptırımların uygulanması için adli mercileri harekete geçirmek olan Bilgi Teknolojileri ve İletişim Kurumu, idarenin bütünlüęü içerisinde yer alan, kamu tüzel kişilięine sahip, görev alanına iliřkin sektörde kamu hukuku ilke ve düzenlemelerine baęlı olarak, kamu yararı amacıyla düzenleyici işlemler yapan, genel idare esaslarına göre faaliyet gösteren, gördüęü hizmet sürekli ve asli nitelik taşıyan bir kuruluřtur.

Söz konusu Kuruma 6475 sayılı Kanun'un 4. maddesiyle, posta hizmetlerinin; güvenilir, kesintisiz bir şekilde verilmesinin saęlanması, yetki belgelerinin kapsamı, verilmesi, denetlenmesi, rekabeti tesis etme ve rekabeti engelleyici, bozucu veya kısıtlayıcı uygulamaları giderme ve bu amaçla ilgili pazarlarda etkin piyasa gücüne sahip hizmet saęlayıcılara ve gerekli hallerde dięer hizmet saęlayıcılara yükümlülükler getirme ve tedbirler alma yetki ve görevi de verilmiştir.

Posta hizmetleri sektöründe düzenleyici ve denetleyici bir otorite olarak görev yapan ve Anayasa'nın 123. maddesi kapsamında bir kamu kurumu olan BTK'nın Anayasa'da kanunla düzenlenmesi zorunlu olmayan ve BTK'nın faaliyet alanının kapsamında kalan dava konusu kuralda belirtilen posta hizmetlerinde millî güvenlik, kamu düzeni ve genel saęlığın korunmasını saęlamak amacıyla ilgili idari birimlerle iş birlięi yaparak gerekli tedbirleri alma görevini ifa etmesinin ve teknik konuları içeren ve bu yönüyle uzmanlık gerektiren bir yetki nitelięinde bulunan posta yoluyla gönderilmesi

yasak maddeler ile kabulü şarta bağlı gönderilerle ilgili düzenlemeler yapmasının, yasama yetkisinin devri anlamına gelmeyeceği ve Anayasa'nın 123. maddesinde öngörülen idarenin kanuniliği ilkesine aykırı bir yönünün bulunmadığı açıktır.

Açıklanan nedenlerle, dava konusu ibareler Anayasa'nın 2., 7. ve 123. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir.

4- Kanun'un 7. Maddesinin (1) Numaralı Fıkrasında Yer Alan ". ve posta hizmetleri ile ilgili ilişkileri ." İbaresinin İncelenmesi

Dava dilekçesinde, dava konusu ibarenin posta gönderilerinin sahibi ve muhatabı kişiler arasındaki münasebetleri mi yoksa Kanun'daki ifadeyle "posta hizmetleri ile ilgili ilişkileri" mi açığa vurulmasını koruma altına aldığı hususunun belirsiz olduğu, ibarenin posta hizmetlerinde vuku bulacak her türlü ilişkinin örneğin ihaleler ve satın almalar ile hizmetin yürütülmesindeki muhtemel usulsüzlük, yolsuzluk gibi durumların açığa vurulmasını da yasak kapsamına alarak kural dışı ilişkilere koruma sağlayıcı bir işlev gördüğü, Anayasa'nın 22. maddesinde posta hizmetleri ile ilgili ilişkilerin değil haberleşmenin gizliliğinin güvence altına alındığı, ayrıca ibarenin bu tür kural dışı ilişkileri gizlilik kapsamına alması nedeniyle vatandaşların posta hizmetleri ile ilgili ilişkiler hakkındaki dilekçe ve bilgi edinme hakkını da ölçüsüzce sınırlandırdığı belirtilerek kuralın, Anayasa'nın 2., 13., 22. ve 74. maddelerine aykırı olduğu ileri sürülmüştür.

Kanun'un 7. maddesinin (1) numaralı fıkrasında, hizmet sağlayıcıları ile posta hizmetlerinde çalışanlar veya herhangi bir şekilde posta hizmetleri ile ilgili bilgiye sahip olanların, bu bilgileri ve posta hizmetleri ile ilgili ilişkileri açığa vurmaları, gönderileri açmaları, içlerinde ne olduğunu araştırmaları, üçüncü kişilere bilgi vermeleri veya herhangi birinin bunları yapmasına neden olmaları, gönderileri zapt veya yok etmeleri yasaklanmaktadır. Dava konusu ibarede ise belirtilen kişilerin posta hizmetleri ile ilgili ilişkileri açığa vurmaları yasaklanmaktadır.

Kanun'un 5. maddesinin (1) numaralı fıkrasında, posta hizmetleri kavramının, posta gönderilerinin kabulü, toplanması, işlenmesi, sevki, dağıtımı ve teslimini içerdiği ifade edilmiştir. Bu bağlamda "posta hizmetleri ile ilgili ilişkiler" kavramının da Kanun'un 5. maddesinde içeriği belirtilen posta hizmetlerine ilişkin her türlü ilişkiyi ifade ettiği açıktır. Dolayısıyla, kuralın belirsizliğinden söz edilemez.

Dava dilekçesinde, Anayasa'nın 22. maddesinde haberleşme hürriyetinin gizliliğinin güvence altına alındığı, dava konusu kuralda öngörülen posta hizmetleri ile ilgili ilişkilerin gizliliğinin bu kapsamda değerlendirilemeyeceği ileri sürülmüştür.

Haberleşme hürriyetini düzenleyen Anayasa'nın 22. maddesinin birinci fıkrasında yer alan "Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır." biçimindeki hüküm, posta hizmetleriyle ilgili ilişkilerin de gizliliğini güvence altına almaktadır. Nitekim, Anayasa'nın 22. maddesinin gerekçesinde de "Burada söz konusu olan haberleşme, kişilerin kendi aralarında P.T.T. araçları aracılığıyla serbestçe haberleşebilmesidir." denilmek suretiyle, posta hizmetleri kapsamında PTT araçları ile yapılan haberleşmenin 22. maddenin koruması altında olduğu ifade edilmiştir. Esasen, posta hizmetleri haberleşme hakkının yerine getirilebilmesi için önemli bir altyapı şebekesi olarak değerlendirilmektedir.

Diğer taraftan, dava konusu kural, Anayasa'nın 22. maddesinde güvence altına alınan haberleşmenin gizliliğini daraltan değil, tam aksine kişiler lehine genişleten düzenleme niteliğinde bulunduğundan, Anayasa'nın 13. maddesine aykırı bir durumdan söz edilemeyeceği de açıktır. Nitekim dava konusu kuralın da içinde bulunduğu maddenin gerekçesinde "Haberleşme hürriyeti Anayasa ile teminat altına alınmış temel hürriyetlerdendir ve Anayasanın 22 nci maddesinde de belirtildiği üzere, haberleşmenin gizliliği esastır. Madde ile, Anayasaya paralel bir düzenlemeyle posta hizmetlerinin gizliliği ve güvenliğinin sağlanmasının hukuki zemine oturtulması amaçlanmaktadır." denilmiştir.

Anayasa'nın 74. maddesinin birinci fıkrasında, "Vatandaşlar ve karşılıklılık esası gözetilmek kaydıyla Türkiye'de ikamet eden yabancılar kendileriyle veya kamu ile ilgili dilek ve şikayetleri hakkında, yetkili makamlara ve Türkiye Büyük Millet Meclisine yazı ile başvurma hakkına sahiptir." denildikten sonra, aynı maddenin son fıkrasında "Bu maddede sayılan hakların kullanılma biçimi, ilişkin usul ve esaslar kanunla düzenlenir." hükmüne yer verilmiştir.

Anayasa'nın 13. maddesinde temel hak ve özgürlüklerin sınırlandırılması, Anayasa'nın ilgili maddelerinde özel sınırlandırma nedeni bulunmasına bağlı tutulmuş ve Anayasa'nın 74. maddesinde de bu hakkın sınırlandırılması için özel bir neden öngörülmemiş ise de anayasanın bütünlüğü ilkesi uyarınca, bir anayasa normu diğerine aykırı olamaz. Dava konusu kuralın dayanağı, Anayasa'nın 22. maddesinin birinci fıkrasında yer alan "Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır." biçimindeki hükümdür. Bir başka ifadeyle Anayasa'nın 74. maddesinde, Anayasa'nın 22. maddesinden kaynaklanan bir anayasal sınırlama söz konusudur. Anayasal sınırlamaların en belirgin özelliği ise kanun koyucunun bu konularda aksine bir düzenleme yapma yetkisinin bulunmaması, öngörülen sınırlama ya da yasaklamalara uygun düzenleme ya da yaptırım getirmek zorunda olmasıdır. Bu bağlamda, kurala ilişkin gerekçede de ifade edildiği üzere, dava konusu kuraldaki düzenlemenin Anayasa'nın 22. maddesinden kaynaklanan bir zorunluluk nedeniyle

yapıldığı dikkate alındığında kuralın, Anayasa'nın 74. maddesine aykırı bir yönünün bulunmadığı açıktır.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 13., 22. ve 74. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

5- Kanun'un 9. Maddesinin (6) Numaralı Fıkrasında Yer Alan ". veya milli güvenlik, kamu düzeni ve genel sağlık gerekçeleri ile ." İbaresini ile (8) Numaralı Fıkrasının İncelenmesi

Dava dilekçesinde, milli güvenlik, kamu düzeni ve genel sağlık gerekçeleri gibi belirsiz kavramlara dayanarak BTK'ya yetki belgesi verilmesi ya da verilmiş yetki belgesinin iptal edilebilmesi yetkisinin verildiği, bu durumun ise belirlilik, yasama yetkisinin devri ve idarenin kanuniliği ilkeleriyle bağdaşmadığı belirtilerek kuralların, Anayasa'nın 2., 7. ve 123. maddelerine aykırı olduğu ileri sürülmüştür.

Kanun'un 9. maddesinin (1) numaralı fıkrasında, posta sektöründe faaliyet gösterecek firmaların, posta hizmeti verebilmeleri veya bunun için gerekli altyapıyı kurup işletebilmeleri için BTK tarafından yetkilendirilmeleri gerektiği ifade edilmiştir. Maddenin (2) numaralı fıkrasında, BTK tarafından yapılacak yetkilendirmenin firmalara yetki belgesi verilmesi yoluyla yapılacağı ve yetki belgesi almak isteyen şirketlerin faaliyetlerine başlamadan önce BTK'ya başvurmaları gerektiği kurala bağlanmıştır. Aynı maddenin (4) numaralı fıkrasında ise yetki belgesinin ücreti, kapsamı, süresi ve şekli ile yetki belgesi sahiplerinin sahip olması gereken mali ve mesleki yeterlik şartları, bu hizmet için kurulması gereken asgari altyapıya ilişkin usul ve esasların BTK tarafından yürürlüğe konulan yönetmelikle belirleneceği hükmüne yer verilmiştir.

Dava konusu ibarenin de yer aldığı (6) numaralı fıkrada yetki belgesi almak isteyen firmaların bu taleplerinin BTK tarafından "milli güvenlik, kamu düzeni ve genel sağlık" gerekçeleriyle reddedilebileceği; dava konusu (8) numaralı fıkrada ise BTK'nın yetki belgesi almış şirketlerin faaliyete geçmeleri ya da posta hizmetlerini sağlamasını aynı gerekçelerle engelleyebileceği kurala bağlanmıştır.

Kanun'un 4. maddesinin (1) numaralı fıkrasının dava konusu ibareleri de içeren (ç) bendinin incelendiği bölümde belirtilen aynı gerekçelerle, dava konusu kurallarda geçen "milli güvenlik, kamu düzeni ve genel sağlık" kavramları belirsiz olmadığı gibi posta hizmetleri sektöründe düzenleyici ve denetleyici bir otorite olarak görev yapan ve Anayasa'nın 123. maddesi kapsamında bir kamu kurumu olan BTK'nın bağımsız idari otorite olmasının bir gereği olarak yetkili bulunduğu alana ilişkin kural koyma, bu kuralları uygulama ve yaptırım uygulama yetkileri kapsamında yetki belgesi

isteklerini reddetmesi ya da yetki belgesi verdiği firmaların faaliyetlerini kuralda belirtilen gerekçelerle engellemesinin yasama yetkisinin devri anlamına gelmediği açıktır. Esasen dava konusu kurallarda BTK'ya tanınan yetki belgesi verilmesi ya da verilmiş yetki belgesi çerçevesinde faaliyette bulunan şirketlerin faaliyetlerinin engellenmesi yetkisinin ancak "mevzuata aykırılık ve millî güvenlik, kamu düzeni ve genel sağlık" gerekçelerine dayalı olarak kullanılabilmesi açıkça ifade edilmiş ve böylece BTK'ya kanunla sınırları çizilmiş bir yetki verilmiştir.

Açıklanan nedenlerle, dava konusu kurallar Anayasa'nın 2., 7. ve 123. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir.

6- Kanun'un 17. Maddesinin (2) Numaralı Fıkrasının İncelenmesi

Dava dilekçesinde, dava konusu kuralda geçen "millî güvenlik ile kamu düzeni gereklerine ve acil durum ihtiyaçları" kavramlarının belirsiz olduğu, kanunda bunların tanımlanmaması nedeniyle kuralın, Anayasa'nın 2., 7. ve 123. maddelerine aykırı olduğu ileri sürülmüştür.

Kanun'un dava konusu kuralın da yer aldığı 17. maddesinde, posta hizmetlerinin sunulmasında uygulanacak tarifelerin BTK tarafından belirlenmesi ile söz konusu tarifelerin uygulanması ve kullanıcıların korunmasına ilişkin usul ve esasların neler olduğuna ilişkin düzenlemeler yer almaktadır. Maddenin dava konusu (2) numaralı fıkrasında ise tarifeler ve kullanıcıların korunmasına ilişkin olarak BTK'nın düzenleme yetkisine bir istisna getirilmektedir. Buna göre, millî güvenlik ile kamu düzeni gereklerine ve acil durum ihtiyaçlarına ait düzenlemeler, ilgili bakanlıkların ihtiyaçları ve görüşleri dikkate alınarak Ulaştırma, Denizcilik ve Haberleşme Bakanlığının teklifi ve Bakanlar Kurulu kararıyla belirlenecektir. Bir başka ifadeyle dava konusu kuralda, millî güvenlik ile kamu düzeni gereklerine ve acil durum ihtiyaçlarına ait düzenlemeler yapma yetkisi BTK'ya değil, Bakanlar Kuruluna verilmektedir.

Kanun'un 4. maddesinin (1) numaralı fıkrasının (ç) bendinin incelendiği bölümde, millî güvenlik, kamu düzeni ve genel sağlığın korunması kavramlarına yönelik Anayasa'ya aykırılık iddiası yerinde görülmediğinden, aynı gerekçelerle dava konusu kural da Anayasa'nın 2. ve 7. maddelerine aykırı değildir.

Diğer taraftan, dava konusu kuralda, Bakanlar Kurulunun tarifelerle ilgili düzenleme yetkisinin ancak millî güvenlik, kamu düzeni gerekleri ve acil durum ihtiyaçları çerçevesinde olabileceği belirtildiğinden, Bakanlar Kuruluna sınırları belirsiz bir yetki verildiğinden söz edilemez. Bakanlar Kuruluna verilen takdir yetkisi, kamu yararının sağlanmasının yanı sıra hizmet gerekleri ve yetkiyi veren Kanun'un amacının gerçekleştirilmesi ile sınırlıdır. Bakanlar Kurulu takdir yetkisini

kullanırken, hukukun genel ilkelerine ve hakkaniyete de uymak zorundadır. Her idari eylem ve işlemde olduğu gibi Bakanlar Kurulunun, dava konusu kuraldaki takdir yetkisini kullanırken de bu genel ilkelere ve sınırlamalara uygun hareket edilmesi gerekir.

Kaldı ki, Bakanlar Kuruluna verilen yetkinin keyfi kullanılıp kullanılmadığı yargı denetimine de tabidir. Anayasa'nın 125. maddesinde, "İdarenin her türlü eylem ve işlemlerine karşı yargı yolu açıktır." denilerek, idarenin hukuka bağlılığı, yargı denetimi sayesinde etkili biçimde sağlanmış ve idare edilenler, idarenin kanunsuz ve keyfi davranışlarına karşı korunmuştur. Dolayısıyla kuralla, belirsizlik oluşturularak hukuk güvenliği ilkesinin zedelendiği, yürütme organına genel ve sınırları belirsiz bir düzenleme yetkisi verilerek yasama yetkisinin devredildiği söylenemez.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 7. ve 123. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

7- Kanun'un 23. Maddesinin (1) Numaralı Fıkrasının (a) Bendi ile 24. Maddesinin İncelenmesi

Dava dilekçesinde, sermayesinin tamamı Hazineye ait olan PTT'nin pay sahipliğine dayanan oy, yönetim, temsil, denetim gibi hak ve yetkilerini Hazine Müsteşarlığına ya da başka bir bakanlığa kullandırmasının kanun koyucunun takdirinde olduğu ancak, bu pay sahipliğinden dolayı oy ve temsilin gereği olarak oluşturulan ve esas sözleşmenin onaylanması, Yönetim Kurulunun atanması, yıllık faaliyet raporu ile bilanço ve kâr zarar hesaplarını inceleyerek Yönetim Kurulunun ibrasına karar verilmesi ile 6102 sayılı Kanun'un 408. maddesindeki yetkileri kullanacak Genel Kurul üyelerinin taşımaları gereken nitelikleri ile kaç kişiden oluşacaklarının ve seçilme/atanma usullerinin 6475 sayılı Kanun'da düzenlenmeyerek idareye bırakılmasının kaynağını Anayasa'dan almayan bir yetkinin kullanımı ve yasama yetkisinin devri anlamına geldiği belirtilerek kuralların, Anayasa'nın 6., 7. ve 11. maddelerine aykırı olduğu ileri sürülmüştür.

6216 sayılı Kanun'un 43. maddesine göre, ilgisi nedeniyle dava konusu kurallar Anayasa'nın 2. maddesi yönünden de incelenmiştir.

Kanun'un 23. maddesinde, PTT'nin organlarının neler olduğu belirtilmektedir. Buna göre, PTT'nin organları, Genel Kurul, Yönetim Kurulu ve genel müdürlükten oluşmaktadır. Kanun'un 24. maddesinde ise Genel Kurulun görevleri düzenlenmektedir. Kuralda Genel Kurulun, yıllık faaliyet raporu ile bilanço ve kâr zarar hesaplarını inceleyerek Yönetim Kurulunun ibrasını karara bağlayacağı, ayrıca Kanun hükümleri saklı kalmak kaydıyla, 6102 sayılı Kanun ve ilgili kanunlarda belirtilen görevleri yapacağı ve yetkileri kullanacağı hükme bağlanmıştır.

Anayasa'nın 6. maddesinde, hiçbir kimse veya organın kaynağını Anayasa'dan almayan bir Devlet yetkisi kullanamayacağı belirtilmiş; 7. maddesinde ise yasama yetkisinin Türk Milleti adına Türkiye Büyük Millet Meclisince kullanılacağı hüküm altına alınmıştır.

Anayasa'da bir konuda emredici ya da yasaklayıcı bir kural konulmamışsa, bu konunun düzenlenmesi anayasal ilkeler içinde kanun koyucunun takdirine bırakılmıştır. Anayasa'da engelleyici bir hüküm bulunmaması durumunda kanun koyucunun genel düzenleme yapma yetkisine dayanarak kural koyması kaynağını Anayasa'dan almayan bir yetkinin kullanılması anlamına gelmez. Kanun koyucu, yasamanın asliliği ve genelliği ilkesinin bir gereği olarak, Anayasa'da düzenlenmeyen bir alanı doğrudan düzenleyebilir.

Yine, Anayasa'da kanunla düzenlenmesi öngörülen konularda, yürütme organına genel ve sınırları belirsiz bir düzenleme yetkisinin verilmesi olanaklı değildir. Yürütmenin düzenleme yetkisi, sınırlı, tamamlayıcı ve bağımlı bir yetkidir. Ayrıca, yürütme organına düzenleme yetkisi veren bir yasa kuralının Anayasa'nın 7. maddesine uygun olabilmesi için temel ilkeleri koyması, çerçeveyi çizmesi, sınırsız, belirsiz, geniş bir alanı yürütmenin düzenlemesine bırakmaması gerekir. Farklı koşul ve durumlara göre sık sık değişik önlemler alma, bunları kaldırma ve süratli biçimde hareket etme zorunluluğunun bulunduğu alanlarda, yasama organının temel kuralları saptadıktan sonra, uzmanlık ve teknik konulara ilişkin hususları yürütmeye bırakması, yasama yetkisinin devri olarak yorumlanamaz.

Bu bağlamda, Anayasa'da kamunun sahip olduğu ve özel hukuk hükümlerine göre faaliyetlerini sürdüren tüzel kişilerin organları ve bunların nitelikleri konusunda bir belirlemenin bulunmadığı dikkate alındığında, dava konusu kurallarda öngörülen PTT'nin Genel Kurulunun üye sayısının ve üyelerinin niteliklerinin Kanun'da ayrıntılı bir biçimde düzenlenmeyerek bu konuda idareye takdir hakkı verilmesi yasama yetkisinin devri ya da kaynağını Anayasa'dan almayan bir yetkinin kullanımı olarak değerlendirilemez.

Diğer taraftan, dava dilekçesinde ileri sürüldüğünün aksine Kanun'un 21. maddesinin (1) ve (2) numaralı fıkraları ile geçici 9. maddesinin (1) numaralı fıkrasında, PTT'nin sermayesinin tamamının Hazine Müsteşarlığına ait olduğu, bir başka ifadeyle şirketin tek bir sahibinin bulunduğu, buna ilişkin yetkinin de Bakanlık tarafından kullanılacağı, esasen 3046 sayılı Kanun'un 21. maddesinin birinci ve 38. maddesinin birinci fıkraları uyarınca bakanlığın en üst amiri olan bakanın ya da yetkilendireceği bakanlık görevlisinin genel kurulu temsil edebileceği, 6102 sayılı Kanun'un 338. maddesinin (1) numaralı fıkrası gereğince bir kişinin pay sahipliğiyle dahi anonim şirket kurulabileceği ve aynı Kanun'un 415. maddesinde de genel kurulda yönetim kurulu tarafından düzenlenen hazır bulunanlar

listesinde adı bulunan pay sahiplerinin bulunabileceği, bu Kanun'da öngörülen kuruluş ve tescile ilişkin istisnai hükümleri dışında PTT hakkında 6102 sayılı Kanun hükümlerinin uygulanacağı gibi hükümler birlikte değerlendirildiğinde, Genel Kurulun sayısı ve nitelikleri konusunda dava konusu kurallarda bir belirsizlik bulunmadığı gibi yasama yetkisinin devrinden de söz edilemeyeceği açıktır. Açıklanan nedenlerle, dava konusu kurallar Anayasa'nın 2., 6. ve 7. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir.

Kuralların Anayasa'nın 11. maddesiyle ilgisi görülmemiştir.

8- Kanun'un 25. Maddesinin (6) Numaralı Fıkrasının İncelenmesi

Dava dilekçesinde, 6102 sayılı Kanun ve özel hukuk hükümlerine tabi özel hukuk tüzel kişisi ticari işletmesi/tacir olan PTT A.Ş.'nin çalışanlarından genel müdür ve yönetim kurulu üyelerinin, Anayasa'nın 129. maddesinde münhasıran memurlar ve diğer kamu görevlileri için getirilmiş bulunan istisnai hükmün kapsamı içine alınmasının Anayasa'nın 129. maddesine aykırı olduğu gibi kaynağını Anayasa'dan almayan bir yetkinin kullanılması sonucunu doğurduğu, ayrıca PTT A.Ş. çalışanlarından sadece genel müdür ile yönetim kurulu üyelerinin istisnai hükmün kapsamına alınıp, diğerlerinin alınmaması ve posta sektöründe faaliyet gösteren diğer ticari şirketlerin genel müdür ve yönetim kurulu üyelerinin istisnai hükmün kapsamı dışında tutulması suretiyle üyelere ayrıcalık tanındığı belirtilerek kuralın, Anayasa'nın 6., 10. ve 129. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralda, PTT Genel Müdürü ve Yönetim Kurulu üyelerinin görevleri sebebiyle bir suç işlediklerinde yargılanmalarına ilişkin usul düzenlenmektedir. Buna göre, kuralda belirtilen kişilerin, görevleri sebebiyle bir suç işlemeleri durumunda yargılanabilmeleri için Ulaştırma, Denizcilik ve Haberleşme Bakanı'nın izni gerekmektedir. Kuralda ayrıca bu konuda 2.12.1999 günlü, 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun hükümlerine göre hareket edileceği de ifade edilmiştir.

Anayasa'nın 129. maddesinin son fıkrasında "Memurlar ve diğer kamu görevlileri hakkında işledikleri iddia edilen suçlardan ötürü ceza kovuşturması açılması, kanunla belirlenen istisnalar dışında, kanunun gösterdiği idari merciin iznine bağlıdır." hükmü yer almaktadır. Bu hüküm, Anayasa'nın 128. maddesi anlamında memur ve diğer kamu görevlilerinin işledikleri iddia edilen suçlardan ötürü ceza kovuşturması açılabilmesini, kural olarak, idari merciin iznine bağlamaktadır. Bir başka ifadeyle memurlar ve diğer kamu görevlilerinin suç işlemeleri durumunda, yargılanabilmeleri için asıl olan, idari mercilerin izninin bulunmasıdır. Ancak, istisnai durumlarda

kanuni düzenlemelerle bu hükmün dışında izin almaksızın genel hükümler çerçevesinde düzenleme yapılması mümkündür.

Anayasa'nın söz konusu hükmü, Anayasa'nın 128. maddesi anlamında memur ve diğer kamu görevlisi niteliğini taşımayanlar için memur ve diğer kamu görevlileri için öngörülen izin sistemi ya da usul hükümlerinin uygulanmasını yasaklamamaktadır. Bir başka ifadeyle Anayasa'nın 129. maddesi, kamu görevlilerinin görevlerini aksatmadan yapabilmeleri ve yersiz şikâyetlerle uğraşmak zorunda kalıp yerine getirmek zorunda oldukları kamu hizmetlerinin aksatılmaması düşüncesiyle memurlar ve diğer kamu görevlilerine bir güvence getirmektedir. Aynı güvencenin memur veya diğer kamu görevlileri dışında kalanlara tanınmayacağına ilişkin bir yasaklama ise bulunmamaktadır. Kanun koyucunun yasama ilkesinin asliliği ve genelliği ilkesi uyarınca, sahip olduğu yetkisine dayanarak memur ve diğer kamu görevlisi kapsamında bulunmayanlar yönünden de izlediği ceza siyasetine göre kamu yararını gözeterek, aynı güvenceyi içeren düzenlemeler yapması, Anayasa'nın 6. ve 129. maddelerine aykırılık oluşturmaz. Nitekim mevzuatımızda da Anayasa'nın 128. maddesi anlamında Devletle arasında herhangi bir statüer ilişki bulunmayan ve bu manada memur ve diğer kamu görevlileri statüsünde bulunmayan farklı kamu hizmetlerini yerine getiren kişiler ya da meslek mensupları yönünden genel soruşturma usulünden farklı olarak özel soruşturma usullerinin öngörüldüğü görülmektedir.

Dava konusu kuralın, "kamu kurumu niteliği ağır basan" bir anonim şirket statüsünde bulunan, evrensel hizmet yükümlüsü olarak bir kamu hizmeti olan posta hizmetlerini ülkenin her tarafına ulaştırmakla yükümlü kılınan, bu kapsamda kendisine kısmi tekel hakkı tanınan, posta hizmetlerinden bankacılık hizmetlerine kadar pek çok alanda faaliyette bulunan PTT'nin karar organı olan Yönetim Kurulu üyelerinin yapılan bu kamu hizmetlerinin aksamaması amacıyla yasalaştırıldığı dikkate alındığında kuralın, Anayasa'nın 129. maddesine aykırı bir yönünün bulunmadığı açıktır.

Dava dilekçesinde, dava konusu kuralla PTT A.Ş. çalışanlarından sadece Genel Müdür ile Yönetim Kurulu üyelerinin istisnai hükmün kapsamına alınıp, diğerlerinin alınmaması ve posta sektöründe faaliyet gösteren diğer ticari şirketlerin genel müdür ve yönetim kurulu üyelerinin istisnai hükmün kapsamı dışında tutulması suretiyle belirtilen üyelere ayrıcalık tanındığı ve kuralın eşitlik ilkesine aykırı olduğu ileri sürülmüştür.

"Kamu kurumu niteliği ağır basan" bir anonim şirket statüsünde bulunan ve evrensel hizmet yükümlüsü olarak bir kamu hizmetini yerine getiren PTT ile posta hizmeti sektöründe faaliyet gösteren diğer firmalar aynı konumda bulunmadıklarından dolayı bunlar arasında bir eşitlik

karşılaştırması yapılamayacağından, dava konusu kuralın eşitlik ilkesine aykırılığından söz edilemez.

Yine dava dilekçesinde dava konusu kuralla getirilen soruşturma usulünün PTT'nin sadece Yönetim Kurulu üyelerini kapsamaması nedeniyle eşitlik ilkesine aykırı olduğu ileri sürülmüş ise de PTT'nin karar organı olan Yönetim Kurulu'nda yer alan üyeler ile diğer personelin hukuki statülerinin farklı olması nedeniyle, bu kişilerin farklı kurallara tabi tutulması eşitlik ilkesine aykırılık oluşturmamaktadır. Kaldı ki, PTT'nin mevcut hâlinde dahi 14.7.1965 günlü, 657 sayılı Devlet Memurları Kanunu'na tabi olarak çalışan kamu görevlilerinin de bulunduğu ve bunlar hakkında 4483 sayılı Kanun hükümlerinin uygulanacağı açıktır.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 6., 10. ve 129. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Osman Alifeyyaz PAKSÜT bu görüşe katılmamıştır.

9- Kanun'un 29. Maddesinin (2) ve (3) Numaralı Fıkralarının İncelenmesi

a- Kuralların Anlam ve Kapsamı

Dava konusu (2) numaralı fıkrada, PTT'ye karşı yapılacak talep ve PTT'ye karşı açılacak davalarla ilgili bazı düzenlemeler yapılmaktadır. Buna göre, PTT'nin yapmış olduğu hizmetlerle ilgili olarak herhangi bir talepte bulunabilmek ve sorumlu olduğu durumlarda PTT'ye karşı dava açabilmek için, o hizmetten yararlanan kişi konumunda bulunmak gerekmektedir. Kuralda geçen "PTT hizmetleri ile ilgili" ifadesinin ne anlama geldiği ise Kanun'un 22. maddesinin (1) numaralı fıkrasında belirtilmiştir. Buna göre, PTT'nin, yurt içinde ve yurt dışında her türlü taşımacılık hizmetlerini de içerecek şekilde posta, koli, kargo ve lojistik hizmetleri, pul basımı ve satımı, denetlemeye ilişkin hükümleri saklı kalmak kaydıyla, 5411 sayılı Kanun'a tabi olmaksızın, anılan Kanun kapsamında belirtilen faaliyet konuları ile ilgili olarak bankalarla yapacağı sözleşmeler doğrultusunda bankalara destek hizmeti, parasal posta hizmeti, ödeme hizmeti sunma, adres bilgi kayıt sistemi ve elektronik sertifika hizmet sağlayıcılığı, elektronik ortam dâhil her türlü tebligat ve telgraf hizmetine ilişkin faaliyetler ile esas sözleşmesinde belirlenen diğer faaliyetleri, PTT'nin hizmetleridir. Bir başka ifadeyle PTT'nin, Kanun'da ve esas sözleşmesinde gösterilen posta, lojistik ve bankacılık işlemleri alanlarında yaptığı tüm hizmetler, PTT hizmetleridir.

Dava konusu (3) numaralı fıkrada ise PTT hizmetleri ile ilgili olarak talep ve dava zamanaşımına ilişkin hükümlere yer verilmiştir. Fıkranın birinci cümlesinde, talep ve dava açma hakkının işlemin tesisi tarihinden itibaren bir yıl içinde zamanaşımına uğrayacağı ifade edilmiştir. Söz konusu

hükümde, dava açma hakkına ilişkin bu sürenin zamanaşımı süresi olduğu açıkça ifade edilmiştir. Dava açma süresinin zamanaşımı süresi olarak belirtilmesinin en önemli sonucu, zamanaşımının hukuk usulünde hâkim tarafından resen değil, ancak bir def'i olarak ileri sürülmesi durumunda dikkate alınacak olmasıdır. Fıkranın ikinci cümlesinde, zamanaşımının kesilmesine ilişkin bir durum öngörülmekte ve zamanaşımının PTT'ye başvuru yapılmasıyla kesileceği, incelemenin ve araştırmanın sonucunun ilgililere bildirilmesiyle de zamanaşımı süresinin kesildiği andan itibaren yeniden işlemeye başlayacağı ifade edilmiştir. Fıkranın son cümlesinde ise zamanaşımı süresinin yeni bir başvuru yapılması durumunda tekrar kesilmeyeceği ifade edilmek suretiyle, zamanaşımı nedeniyle kesilmenin ancak bir kez mümkün olabileceği hüküm altına alınmıştır.

b- Anayasa'ya Aykırılık Sorunu

ba- Anayasa'nın 2., 5. ve 10. Maddeleri Yönünden İnceleme

Dava dilekçesinde, dava konusu kurallarla 4077 sayılı Tüketicinin Korunması Hakkında Kanun'da yer alan güvencelere PTT A.Ş. lehine istisnai düzenlemeler yapıldığı, dava konusu kuralların aynı durum ve statüde olan herkesi kapsayan 4077 sayılı Kanun'daki kuralları işlemez kılmayı, tüketiciler aleyhine ve PTT A.Ş. lehine, PTT A.Ş.'ye özel bir ayrıcalığı yasalaştırması suretiyle yasaların genelliği ilkesine de aykırı davranıldığı, ayrıca PTT'nin faaliyet alanı içinde bulunan işleri yürüten firmalarla, para transferi, ödeme ve bankacılık hizmetlerini yürüten çok sayıda bankanın bulunduğu ve bunların tamamının yürüttüğü hizmetlerden dolayı 4077 sayılı Kanun hükümlerine tabi olduğu, oysa dava konusu kurallarla PTT'nin farklı kurallara tabi tutulduğu belirtilerek kuralların, Anayasa'nın 2., 5. ve 10. maddelerine aykırı olduğu ileri sürülmüştür.

Bir hukuk düzeni içinde genel kurala istisna getiren özel kurallar, özel kural ile öngörülen istisnaya da istisna getiren daha özel kurallar bulunması hukuk düzeninin doğasında vardır. O nedenle bir yasa kuralının başka bir norm ile uyumlu olmaması onun iptal edilmesini gerektiren bir durum değildir. Daha alt düzeydeki bir norm olan yönetmelikle düzenlenmiş bir konuda kanun ile farklı bir hüküm getirilmişse normlar hiyerarşisinde daha üst düzeyde olan kanun hükümlerinin uygulanacağı açıktır. Anayasa Mahkemesi kanunların başka kanunlara ya da daha alt düzeydeki diğer normlara uyumluluğunu değil, kanunların Anayasa'ya uygunluğunu denetlemektedir. Bu nedenle, dava konusu kuralda PTT'ye karşı dava açma zamanaşımının 4077 sayılı Kanun hükümlerinden farklı bir şekilde düzenlenmesi, ayrıca dava açmanın hangi durumlarda mümkün olacağını özel bir hükümle belirtilmesi, kuralın sırf bu nedenle Anayasa'ya aykırı olduğu anlamına gelmez.

Kaldı ki PTT'nin yapmış olduğu hizmetlerle ilgili olarak herhangi bir talepte bulunabilmek ve sorumlu olduğu durumlarda PTT'ye karşı dava açabilmek için, o hizmetten yararlanan kişi

konumunda bulunulması gerektiğini ifade eden dava konusu (2) numaralı fıkra, PTT'ye özel bir düzenleme niteliğinde de değildir. Kural, aslında, taraf sıfatını öngören genel hukuk usulü kuralının Kanun'da özel olarak ifade edilmesinden başkaca bir anlam ifade etmemektedir. Kurala ilişkin gerekçede kuralın dava açma ve sorumluluk konusunda açıklık ve şeffaflığın sağlanması amacıyla yasalaştırıldığı ifade edilmiştir.

Diğer taraftan, dava dilekçesinde ileri sürülen PTT'nin 4077 sayılı Kanun hükümlerine tabi tutulmamasının PTT'ye özel bir düzenleme niteliğinde olduğu iddiası da yerinde değildir. Zira, kanun koyucu takdir yetkisine dayanarak PTT'nin yerine getirilen hizmetlerin kapsamını ve niteliğini gözeterek PTT'nin 4077 sayılı Kanun hükümlerine tabi olmamasını öngörmüştür. Bu bağlamda dava konusu kuralların eşitlik ilkesine bu yönüyle de aykırı bir tarafının bulunmadığı açıktır.

Açıklanan nedenlerle, dava konusu kurallar Anayasa'nın 2., 5. ve 10. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir.

Osman Alifeyyaz PAKSÜT ve Celal Mümtaz AKINCI bu görüşe katılmamıştır.

bb- Anayasa'nın 13., 36., 142. ve 172. Maddeleri Yönünden İnceleme

Dava dilekçesinde, 4077 sayılı Kanun hükümlerine göre, tüketici haklarının ihlali durumunda sadece hizmetten yararlanan tüketici değil, tüketici örgütleri ile Gümrük ve Ticaret Bakanlığı da dava açabilmekte ve zamanaşımı süresinin ise ayıplı hizmetten dolayı yapılacak taleplerde hizmetin ifasından itibaren iki yıl, ayıplı hizmetin neden olduğu zarardan dolayı ise üç yıl olarak belirlendiği hâlde, dava konusu kurallarla PTT hizmetleri ile ilgili olarak herhangi bir talepte bulunma ve PTT'nin sorumlu olduğu hâllerde dava açmayı hizmetten yararlananla sınırlandırıldığı, bu durumun ise Anayasa'nın Devlete yüklediği tüketicilerin kendilerini koruyucu girişimlerini teşvik etme ve tüketicileri koruma göreviyle bağdaşmadığı belirtilerek kuralların, Anayasa'nın 172. maddesine aykırı olduğu ileri sürülmüştür.

6216 sayılı Kanun'un 43. maddesine göre, ilgisi nedeniyle dava konusu kurallar Anayasa'nın 13., 36. ve 142.maddeleri yönünden de incelenmiştir.

Anayasa'nın 172. maddesinde, Devletin tüketicileri koruyucu ve aydınlatıcı tedbirleri alacağı, tüketicilerin kendilerini koruyucu girişimleri teşvik edeceği ifade edilmiştir. Anayasa'nın 172. maddesinde öngörülen tüketicilerin korunmasına ilişkin olarak Devlete verilen düzenleme yetkisinin içeriğinin ve sınırlarının belirlenmesinde, Anayasa'nın bütünlüğü ilkesi uyarınca Anayasa'nın diğer hükümlerinin de gözetilmesi gerektiği açıktır. Bir başka ifadeyle Anayasa'nın 172. maddesi,

tüketicinin korunması adına herkese sonsuz bir dava açma hakkı tanımaz. Öncelikle, 172. maddenin içerik ve sınırlarının tayininde Anayasa'nın 142. maddesinin de dikkate alınması gerekmektedir.

Anayasa'nın 142. maddesi uyarınca, dava açma süresini belirleyip belirlememe yetkisi, Anayasa'daki kurallara bağlı kalmak ve adalet, hakkaniyet ve kamu yararı ölçütlerini gözetmek koşuluyla kanun koyucunun takdirindedir. Bu bağlamda, dava konusu kuralda öngörülen bir yıllık dava zamanaşımı süresinin de belirlenmesi hususu, kanun koyucunun takdir yetkisi kapsamındadır. Ancak, kanun koyucu bu takdir yetkisini kullanırken, Anayasa'nın 36. maddesinde öngörülen hak arama hürriyetinin kullanımını ölçsüz bir biçimde sınırlandırmaktan kaçınmalıdır.

Anayasa'nın 36. maddesinde, hak arama özgürlüğü güvence altına alınmıştır. Hak arama özgürlüğünün temel unsurlarından biri mahkemeye erişim hakkıdır. Bu hak, hukuki bir uyuşmazlığın bu konuda karar verme yetkisine sahip bir mahkeme önüne taşınması hakkını da kapsar. Anayasa'nın 36. maddesinde, hak arama özgürlüğü için herhangi bir sınırlama nedeni öngörülmemiş olmakla birlikte, bunun hiçbir şekilde sınırlandırılması mümkün olmayan mutlak bir hak olduğu söylenemez. Özel sınırlama nedeni öngörülmemiş hakların da hakkın doğasından kaynaklanan bazı sınırları bulunduğu kabul edilmektedir. Ayrıca hakkı düzenleyen maddede herhangi bir sınırlama nedenine yer verilmemiş olsa da, Anayasa'nın başka maddelerinde yer alan kurallara dayanarak bu hakların sınırlandırılması da mümkün olabilir. Dava açma hakkının kapsamına ve kullanım koşullarına ilişkin bir kısım düzenlemelerin hak arama özgürlüğünün doğasından kaynaklanan sınırları ortaya koyan ve hakkın norm alanını belirleyen kurallar olduğu açıktır. Ancak bu sınırlamalar Anayasa'nın 13. maddesinde yer alan güvencelere aykırı olamaz.

Dava konusu (3) numaralı fıkranın birinci cümlesinde PTT hizmetleriyle ilgili olarak öngörülen bir yıllık, talepte bulunma ve dava zamanaşımı süresi, her şeyden önce ilgililerin talepte bulunma veya dava açma hakkını bütünüyle ortadan kaldırmamakta, sadece belli bir süreyle sınırlandırmaktadır. Bu düzenlemenin, PTT'nin gereksiz ve ilgili olmayan kişilerce açılacak davalarla meşgul edilmemesi, böylece yaptığı kamu hizmetinin kesintiye uğratılmaması amacıyla öngörüldüğü ve bu anlamda kamu yararı amacına dayandığı anlaşılmaktadır. Kuralda öngörülen bir yıllık zamanaşımı süresinin PTT tarafından işlemin tesis edildiği tarihten itibaren başlayacağı ve günümüzde iletişim ve kargo hizmetlerinde kaydedilen hız ve kişilerin PTT yoluyla aldıkları hizmetleri sorgulayabilmeleri bir bütün olarak dikkate alındığında ve kişilerin söz konusu işlemlerden en azından gönderici tarafın bizzat başvuran kişi olarak bilgi sahibi olması nedeniyle taraflara talepte bulunabilmek veya dava açmak için yeterli düşünme ve hazırlanma imkânı tanıyan bir zaman dilimi olduğu, dolayısıyla bu sürenin hak arama özgürlüğünün özüne dokunan bir sınırlama olmadığı da açıktır.

Öte yandan, yukarıda belirtildiği üzere, PTT'nin tacir olması ve dava konusu kuralda belirtilen işlerinin de ticari iş olması nedeniyle dava konusu kurallarda talepte bulunanlar veya dava açanlar ve zamanaşımı süresi yönünden diğer kanunlardan farklı hükümler öngörülmesinin, Anayasa'nın 172. maddesine aykırı bir yönü bulunmamaktadır.

Açıklanan nedenlerle, dava konusu kurallar Anayasa'nın 13., 36., 142. ve 172. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir.

Osman Alifeyyaz PAKSÜT ve Celal Mümtaz AKINCI bu görüşe katılmamıştır.

10- Kanun'un Geçici 6. Maddesinin (1) Numaralı Fıkrasında Yer Alan ".Yönetim Kurulunca belirlenen esaslar çerçevesinde." ve ".ile geçmesi uygun görülmeyenlerin." İbarelerinin İncelenmesi

Dava dilekçesinde, sözleşmeli personel statüsüne geçişin esasları ile sözleşmeli personel statüsüne geçmesi uygun bulunmayanları belirleme yetkisinin hiçbir sınırlamaya tabi tutulmadan, esasları belirtilmeden ve çerçevesi çizilmeden Yönetim Kurulu'na verilmesinin, adaletli olmadığı, bir hukuk kuralında bulunması gereken, belirlilik, öngörülebilirlik, genellik ve soyutluk kriterlerini taşımadığı, ayrıca dava konusu ibarelerin yasama yetkisinin devri sonucunu doğurduğu belirtilerek kuralların, Anayasa'nın 2. ve 7. maddelerine aykırı olduğu ileri sürülmüştür.

Kanunla PTT'nin yeniden yapılandırılması kapsamında personelinin Kanun'un 27. maddesi uyarınca idari sözleşme ile sözleşmeli personel olarak istihdam edilmesi öngörülmüş; geçici 5. maddede ise mevcut personelin mevcut statüleriyle istihdam edilmesine devam olunacağı ifade edilmiştir. Kanun'un dava konusu kuralın da yer aldığı geçici 6. maddesinde ise mevcut personelden istekli olanların PTT'nin yeniden yapılandırılan hâlinde sözleşmeli personel olarak çalıştırılabileceği ve buna ilişkin usul ve esaslar düzenlenmiştir.

Buna göre, mülga T.C. Posta ve Telgraf Teşkilatı Genel Müdürlüğünde 31.5.2006 günlü, 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun 4. maddesinin birinci fıkrasının (c) bendine tabi olarak çalışan ve mevcut statülerinde PTT'de istihdamına devam olunan personel ile işçi statüsünde istihdam edilen personelden isteyenler Yönetim Kurulunca belirlenen esaslar çerçevesinde bu Kanun'da tanımlanan sözleşmeli personel statüsüne geçirilebilecektir. Buna karşılık, sözleşmeli personel statüsüne geçmek istemeyenler ile geçmesi uygun görülmeyenlerin tabi olduğu mevzuatına göre istihdamına devam olunacaktır. Görüldüğü üzere dava konusu ibarelerle, mevcut personelin sözleşmeli personel olarak istihdam edilebilmeleri, yönetim kurulunca belirlenecek esaslar

çerçevesinde mümkün hâle getirilmekte; yönetim kurulunca sözleşmeli personel olarak çalıştırılması uygun görülmeyenlerin ise eski statülerinde çalışmalarına olanak tanınmaktadır.

Maddenin dava konusu edilmeyen diğer fıkralarında ise birinci fıkra uyarınca sözleşmeli personel olarak çalıştırılan kişilerin mevcut kazanılmış haklarının korunmasına ilişkin güvenceleri içeren düzenlemelere yer verilmiştir.

Anayasa'da kamunun sahip olduğu ve özel hukuk hükümlerine göre faaliyetlerini sürdüren tüzel kişilerde idari hizmet sözleşmesi ile personel çalıştırılması konusunda bir belirlemenin bulunmadığı dikkate alındığında, dava konusu ibarelerle mevcut personelden Kanun'da tanımlanan sözleşmeli personel statüsünde çalışmak isteyenleri belirleme konusunda ayrıntılı bir biçimde düzenlemenin yapılmamış olması ve bu konuda Yönetim Kurulu'na takdir hakkı verilmesi yasama yetkisinin devri ya da kaynağını Anayasa'dan almayan bir yetkinin kullanımı olarak görülemez.

Öte yandan dava konusu ibareler, mevcut personele yeni statüye geçmesi için bir zorlamada bulunmamakta, bilakis onlara bir tercih hakkı tanımaktadır. Personelin eski statüde çalışmak istemesi ya da yönetim kurulunca yeni statüde istihdam edilme talebinin yerinde görülmemesi durumunda, mevcut statüsü içinde çalışması güvence altına alınmaktadır. Kaldı ki, talebi reddedilen kişinin yargı yoluna başvurmasına engel bir durum da bulunmamaktadır.

Dava konusu ibarelerde, idare hukukunda ilgilinin talepte bulunması hâlinde yapılabilen isteğe bağlı işlemlere benzer bir durum söz konusudur. Bu tür işlemlerde, yarar ya da yükümlülük getiren bazı işlemlerin yapılabilmesi, ilgilinin talebine bağlıdır. İlgilinin talebinin bulunmaması işlemi hukuka aykırı hâle getirir. İlgilinin talebi, işlemin oluşumunu sağlayıcı bir irade beyanı değil, işlemin sebebidir. Asıl işlem ise idare tarafından tek yanlı yapılan bir irade açıklamasıyla gerçekleşmektedir. Bu bağlamda, dava konusu ibarelerle personelin istekli olması durumunda Yönetim Kurulu'na yeni statüye geçilmesi konusunda takdir yetkisi verilmesinin bu yönüyle de hukuk devleti ilkesine aykırı bir yönü yoktur.

Açıklanan nedenlerle, dava konusu kurallar Anayasa'nın 2. ve 7. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

V- YÜRÜRLÜĞÜN DURDURULMASI İSTEMİ

9.5.2013 günlü, 6475 sayılı Posta Hizmetleri Kanunu'nun;

A- 3. maddesinin (1) numaralı fıkrasının (a) bendindeki "...ilgili mevzuatı saklı kalmak kaydıyla," ibaresinden sonra gelen "...gerçek..." ibaresine yönelik yürürlüğün durdurulması isteminin, koşulları oluşmadığından REDDİNE,

B- 1- 3. maddesinin (1) numaralı fıkrasının (h) ve (ı) bentlerine,
2- 4. maddesinin (1) numaralı fıkrasının (ç) bendinde yer alan "...millî güvenlik, kamu düzeni ve genel sağlığın korunmasını teminen..." ve "...posta yoluyla gönderilmesi yasak maddeler ile kabulü şarta bağlı gönderiler için..." ibarelerine,
3- 6. maddesinin (1) numaralı fıkrasına,
4- 7. maddesinin (1) numaralı fıkrasında yer alan "...ve posta hizmetleri ile ilgili ilişkileri..." ibaresine,
5- 9. maddesinin (3) numaralı fıkrasına, (6) numaralı fıkrasında yer alan "...veya millî güvenlik, kamu düzeni ve genel sağlık gerekçeleri ile..." ibaresine ve (8) numaralı fıkrasına,
6- 17. maddesinin (2) numaralı fıkrasına,
7- 23. maddesinin (1) numaralı fıkrasının (a) bendine,
8- 24. maddesine,
9- 25. maddesinin (6) numaralı fıkrasına,
10- 29. maddesinin (2) ve (3) numaralı fıkralarına,
11- Geçici 3. maddesine,
12- Geçici 6. maddesinin (1) numaralı fıkrasında yer alan "...Yönetim Kurulunca belirlenen esaslar çerçevesinde..." ve "...ile geçmesi uygun görülmeyenlerin..." ibarelerine,
yönelik iptal istemleri, 4.12.2014 günlü, E.2013/84, K.2014/183 sayılı kararla reddedildiğinden, bu maddelere, fıkralara, bentlere ve ibarelere ilişkin yürürlüğün durdurulması istemlerinin REDDİNE, 4.12.2014 gününde OYBİRLİĞİYLE karar verilmiştir.

VI- SONUÇ

9.5.2013 günlü, 6475 sayılı Posta Hizmetleri Kanunu'nun;

A- 3. maddesinin (1) numaralı fıkrasının;

1- (a) bendindeki "...ilgili mevzuatı saklı kalmak kaydıyla," ibaresinden sonra gelen "...gerçek..." ibaresinin Anayasa'ya aykırı olduğuna ve İPTALİNE, Hicabi DURSUN, Muammer TOPAL, M. Emin KUZ ile Hasan Tahsin GÖKCAN'ın karşıoyları ve OYÇOKLUĞUYLA,
2- (h) ve (ı) bentlerinin Anayasa'ya aykırı olmadıklarına ve iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

B- 4. maddesinin (1) numaralı fıkrasının (ç) bendinde yer alan "...millî güvenlik, kamu düzeni ve genel sağlığın korunmasını teminen..." ve "...posta yoluyla gönderilmesi yasak maddeler ile kabulü şarta bağlı gönderiler için..." ibarelerinin Anayasa'ya aykırı olmadıklarına ve iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

C- 6. maddesinin (1) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

D- 7. maddesinin (1) numaralı fıkrasında yer alan "...ve posta hizmetleri ile ilgili ilişkileri..." ibaresinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

E- 9. maddesinin;

1-(3) numaralı fıkrasının,

2- (6) numaralı fıkrasında yer alan "...veya millî güvenlik, kamu düzeni ve genel sağlık gerekçeleri ile..." ibaresinin,

3- (8) numaralı fıkrasının,

Anayasa'ya aykırı olmadıklarına ve iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

F- 17. maddesinin (2) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

G- 23. maddesinin (1) numaralı fıkrasının (a) bendinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

H- 24. maddesinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

I- 25. maddesinin (6) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, Osman Alifeyyaz PAKSÜT'ün karşıoyu ve OYÇOKLUĞUYLA,

J- 29. maddesinin (2) ve (3) numaralı fıkralarının Anayasa'ya aykırı olmadıklarına ve iptal istemlerinin REDDİNE, Osman Alifeyyaz PAKSÜT ile Celal Mümtaz AKINCI'nın karşıoyları ve OYÇOKLUĞUYLA,

K- Geçici 3. maddesinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

L- Geçici 6. maddesinin (1) numaralı fıkrasında yer alan "...Yönetim Kurulunca belirlenen esaslar çerçevesinde..." ve "...ile geçmesi uygun görülmeyenlerin..." ibarelerinin Anayasa'ya aykırı olmadıklarına ve iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

4.12.2014 gününde karar verildi.

Başkanvekili - Serruh KALELİ

Başkanvekili - Alparslan ALTAN

Üye: Serdar ÖZGÜLDÜR; Osman Alifeyyaz PAKSÜT; Recep KÖMÜRCÜ; Burhan ÜSTÜN; Engin YILDIRIM; Nuri NECİPOĞLU; Hicabi DURSUN; Celal Mümtaz AKINCI; Erdal TERCAN; Muammer TOPAL; M. Emin KUZ; Hasan Tahsin GÖKCAN

KARŞIOY GEREKÇESİ

1- PTT'nin Genel Müdür ve Yönetim Kurulu üyelerinin görevleri sebebiyle işledikleri suçlardan dolayı yargılanmalarının Ulaştırma, Denizcilik ve Haberleşme Bakanı'nun iznine bağlanmasını ve yargılamanın 4483 sayılı Kanun'a göre yapılmasını öngören 25. maddenin (6) numaralı fıkrasının Anayasa'ya aykırı olmadığına dair çoğunluk görüşüne şu nedenlerle katılmıyorum:

Anayasa'nın 129. maddesinde memurlar ve diğer kamu görevlilerinin sorumlulukları, disiplin ve ceza kovuşturmalarının yapılmasında uygulanacak esaslar düzenlenmektedir. Bu kapsama girmeyen kişilerin, memurlar ve diğer kamu görevlileri için Anayasa'nın getirdiği bazı güvencelerden yararlandırılmasının "yasamanın asliliği" ve "Anayasada aksine bir hüküm bulunmayışı" gibi gerekçelerle açıklanması mümkün değildir. Zira Anayasanın özel hükümleri ancak Anayasanın diğer maddeleri ve özellikle "Genel Esaslar" başlıklı Birinci Kısım ile birlikte değerlendirildiklerinde anlam ifade ederler.

Türkiye Cumhuriyeti'nin demokratik bir hukuk devleti olduğuna dair 2. madde, egemenliğin yetkili organlar tarafından kullanılacağına ilişkin 6. madde, yargı yetkisinin bağımsız kullanımına ilişkin 9. madde, kanun önünde eşitliği öngören 10. madde, idarenin bütünlüğünü belirten 123. madde ile birlikte değerlendirildiğinde, yasa koyucunun, memurlar ve diğer kamu görevlileri hakkında Anayasa'nın 129. maddesinde yer alan özel düzenlemeleri, kapsam dışındaki kişilere teşmil etmekte geniş bir takdir hakkına sahip olmadığını kabul etmek gerekir. Aksi düşüncenin benimsenmesi, istisnaların dar yorumlanmasının hukukta genel kural olduğuna dair evrensel yorum esaslarına, "aksi ile kanıt-argumentum a contrario" gibi en basit yorum yöntemlerine dahi ters düşer. Anayasa'da açıkça yer alan bir özel hükmün yalnızca düzenlediği işle ilgili olarak uygulanması gerekirken, "aksinin yapılması yasaklanmamış ki" mantığıyla, memurlar ve diğer kamu görevlileri için genel esaslara getirilen istisnanın, hiçbir sıfat ve özelliği olmayan kişilere dahi teşmili mümkün hale gelir ki, bunun da hukuk devleti olmaktan çıkmakla eş anlam taşıyacağı açıktır.

Anayasa'da memurlar ve diğer kamu görevlileri için öngörülen soruşturma usulü, idarenin bütünlüğü içinde hiyerarşik bir ilişki yapısında, emir ve talimatla görev yapan kişiler için öngörülmüştür. Ticari bir şirket olan ve Genel İdare içinde yer almayan PTT'nin Genel Müdürü ve Yönetim Kurulu üyeleri, izin mercii olan Bakan'la hiyerarşik bir ilişki içerisinde değildir. Bakan, bu kişilerin disiplin amiri de değildir. Bu nedenle, Anayasa'da öngörülen sistemin amacına aykırı olarak, bir özel hukuk tüzel kişinin organları olan kişilere ceza soruşturmasında diğer ticari şirket müdür ve yöneticilerine oranla daha fazla koruma getiren kural, Anayasa'nın 2., 10. ve 129. maddelerine aykırıdır.

2- Kanun'un 129. maddesinin iptali istenen(2) numaralı fıkrası ile PTT'nin yapmış olduğu hizmetlerle ilgili olarak her hangi bir talepte bulunabilmek ve sorumlu olduğu durumlarda PTT'ye karşı dava açabilmek için o hizmetten yararlanan kişi konumunda bulunmak gerektiği hükme bağlanmış; (3) numaralı fıkrada ise talep ve dava açma hakkının, işlemin tesisi tarihinden itibaren bir yıl içinde zamanaşımına uğrayacağı belirtilmiştir.

İptali istenen yukarıdaki kurallara göre, 4077 sayılı Tüketicinin Korunması Hakkında Kanun'un tüketicilere tanıdığı olanaklara PTT lehine bazı sınırlamalar getirilmiş yani PTT, bir anlamda 4077 sayılı Kanun kapsamından çıkarılmıştır. Buna göre, yasa koyucunun, benzer hizmetleri sağlayan diğer ticari şirketlere oranla PTT'yi, tüketici talep ve davalarına karşı özel olarak korumayı tercih ettiği anlaşılmaktadır.

PTT'nin yaptığı faaliyetin kamusal niteliğinin ağır basmasının böyle bir özel düzenlemenin haklı nedenini teşkil ettiği şeklindeki düşünceye katılmak mümkün değildir. Zira PTT, yaptığı hizmetlere karşılık ticari esaslara göre ücret almakta ve karlılık esasına göre çalışmaktadır. Başka bir deyişle kendisine Devletçe yüklenen ve diğer özel şirketlerin yapmaktan kaçındıkları bir külfet söz konusu değildir.

Anayasa'nın 172. maddesinde Devletin tüketicileri koruyucu tedbirleri alacağı hükme bağlanmıştır. Bu, Devlete verilmiş özel bir görevdir. 4077 sayılı Kanun da bu anayasal gereğin yerine getirilmesi amacıyla çıkarılmıştır. Anayasa'nın emrinin gereğinin yapılması, bu doğrultuda çıkarılacak yasaların, kanunların genelliği ilkesinin de icabı olarak, tüketicilere hizmet veren bütün tacirlere eşit biçimde uygulanmasına bağlıdır. Anayasa'nın bu gereğinden bir tacirin ayırık tutulması için çok açık bir haklı neden ve kamu yararı bulunması gerekir. PTT'nin yaptığı işlerin kamusal boyutunun da bulunması, bu ticari şirketin lehine fakat tüketicinin aleyhine özel yasa çıkarılması için yeterli bir neden sayılamaz.

Konunun, Anayasa'nın 142. maddesi ile ilgisi bulunmamaktadır. Kaldı ki 142. madde, yasa koyucuya, her özel iş ve çikara göre farklı usul kuralları koyma yetkisi vermemektedir.

Yukarıda açıklanan nedenlerle kuralların, Anayasa'nın 2. ve 172. maddelerine aykırı olduğu düşüncesindeyim.

Üye - Osman Alifeyyaz PAKSÜT

KARŞIOY GEREKÇESİ

6475 sayılı Posta Hizmetleri Kanununun 3. maddesinin birinci fıkrasının (a) bendinde yer alan ". ilgili mevzuatı saklı kalmak kaydıyla, gerçek kişilerin rızası alınarak ..." ibaresindeki "gerçek" kelimesinin Anayasanın 20. maddesine aykırı olduğuna ve iptaline karar verilmiştir.

Anılan bentte "adres bilgi kayıt sistemi", gerçek kişilerin rızası alınarak gerçek ve tüzel kişiler ile kamu kurum ve kuruluşlarına ait fizikî ve elektronik adreslerin, reklâm ve tanıtım amacıyla PTT hizmetlerinden yararlananlara ücret karşılığı kullanırılmasına yönelik olarak oluşturulan PTT'ye ait veri tabanı olarak tanımlanmakta ve böylece adres bilgi kayıt sistemi için gerçek kişilerin rızası aranırken tüzel kişiler ile kamu kurum ve kuruluşları yönünden böyle bir şart öngörülmemektedir.

Kararın gerekçesinde, Anayasanın 20. maddesinde kişisel verilerin korunması bakımından gerçek ve tüzel kişilerle ilgili bir açıklık bulunmadığı, ancak madde metninde "herkes" tabirinin kullanılması sebebiyle tüzel kişilere ilişkin verilerin de 20. madde kapsamında değerlendirilmesi gerektiği belirtilmektedir.

Fizikî ve elektronik adreslerin Anayasanın 20. maddesi kapsamında kişisel veri niteliğinde olduğu açıktır. Ancak kararda da belirtildiği üzere, anılan hükümde de, maddenin gerekçesinde de kişisel verilerin korunmasının tüzel kişileri kapsayıp kapsamadığı ile ilgili bir açıklık bulunmamaktadır.

Diğer taraftan, Avrupa İnsan Hakları Sözleşmesinde açık bir hüküm olmamasına rağmen Avrupa İnsan Hakları Mahkemesi (AİHM)'nin kişisel verilerin korunmasını isteme hakkını kapsamında değerlendirdiği Sözleşmenin 8. maddesinde de Anayasanın 20. maddesinde olduğu gibi "herkes" kavramı kullanılmakta; ancak AİHM kararlarına da dayanılarak, maddenin temel amacının "bireyi" korumak olduğu, bu madde kapsamındaki hakkın kolektif olmaktan çok bireysel bir niteliğinin bulunduğu, maddede özne olarak "herkes" terimi tercih edildiğinden yaş, temyiz kudreti, vatandaşlık veya cinsiyet temelinde istisna olmaksızın her bireyin bu haktan yararlanabileceği, buna karşılık bu hakkın dört alt kategorisinden sadece "konuta saygı hakkının" öznesinin hem gerçek hem de tüzel

kişiler olabileceği, "özel yaşama saygı hakkı", "aile yaşamına saygı hakkı" ve "haberleşmeye saygı hakkı"ndan ise doğaları gereği ancak gerçek kişilerin yararlanabileceği belirtilmektedir (Gülay Arslan Öncü, Özel Yaşama ve Aile Yaşamına Saygı Hakkı, İnsan Hakları Avrupa Sözleşmesi ve Anayasa, Anayasa Mahkemesine Bireysel Başvuru Kapsamında Bir İnceleme, Sibel İnceoğlu (Ed.), Ankara 2013, s.301). Kişisel veriler, "özel yaşama saygı hakkı" kapsamında korunan hukukî menfaatler arasında bulunan "bireyin mahremiyetinin korunması hakkı"nın konusu olarak ele alınmaktadır (Öncü, age., s.311-312). İncelenen kuralda kamu tüzel kişileri ile özel hukuk tüzel kişilerini kapsayacak şekilde geçen "tüzel kişiler" in ise adresleri bakımından "mahremiyet hakkı" söz konusu olmadığı gibi kuruluş gayeleri itibariyle mümkün olduğunca alenî olmaları gerekmektedir.

Nitekim, kararın gerekçesinde atıf yapılan 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Konusunda Bireylerin Korunması Hakkındaki Avrupa Direktifinin 2. maddesinde de kişisel veriler "kimliği belirli veya belirlenebilir gerçek kişilere ait bilgi" olarak tanımlanmakta ve elektronik haberleşme sektörüne ilişkin olarak tüzel kişileri de koruma kapsamında kabul eden 2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkındaki Avrupa Direktifinin Başlangıç kısmınının 12. paragrafında bu Direktif ile üye devletlere 95/46/EC sayılı Direktifin uygulama alanını tüzel kişileri de kapsayacak şekilde genişletme yükümlülüğü getirilmediği belirtilmektedir. 95/46/EC sayılı Direktifin 8. maddesinde, özel hukuk tüzel kişilerinin faaliyetleri esnasında yapılan işlemler ile daha önce kamuya açıklanmış veya kanunî hakların tesisi için gerekli verilerin işlenmesinde hukuka uygunluk nedenlerinin bulunduğu da kabul edilmektedir.

Kuralda geçen "tüzel kişiler"den olan şirketlerin, Türk Ticaret Kanunu ve Kooperatifler Kanununa göre Ticaret Siciline tescil ile tüzel kişilik kazanacakları ve bunların merkezleri ile ortaklarının adreslerinin de Ticaret Sicili Gazetesinde ilân edileceği; ayrıca Türk Ticaret Kanununun 39. maddesine göre ticarî işletmeyle ilgili ticarî mektuplarda ve ticarî defterlere yapılan kayıtların dayandığı belgelerde sicil numarası, ticaret unvanı, işletmenin merkezi ile tescil edilen internet sitesinin adresinin gösterileceği; vakıfların Türk Medenî Kanununun 102. maddesine göre sicile tescil ile tüzel kişilik kazanacağı ve ilgili Tüzük uyarınca vakfın yerleşim yerini de belirtecek şekilde Resmî Gazetede ilân edileceği ve nihayet derneklerin de diğer bilgileri ile birlikte ilgili mevzuat uyarınca sicile kaydedildiği dikkate alındığında özel hukuk tüzel kişilerinin adresleri bakımından mahremiyet hakkından söz edilemeyeceği açıktır. Kamu tüzel kişileri de kamu gücü kullanan, mevzuatla yetki ve görevleri belirlenen ve bu itibarla yetki ve görevleri gibi adresleri de alenî olması gereken kuruluşlardır.

Dolayısıyla, Anayasanın 20. maddesinin son fıkrasında ayrıca düzenlenen kişisel verilerin korunmasını isteme hakkının tüzel kişileri kapsamadığını belirtmek, AİHM kararlarına da dayanılarak yapılan yukarıdaki tespitlerle çelişmeyecektir.

Yukarıda da açıklandığı üzere, itiraz konusu kuralla yapılan düzenlemenin özel hukuk ve kamu tüzel kişileri bakımından, önceden halka duyurulan ve herkese açık olan verilere ilişkin olması, başka bir ifadeyle gizliliği değil, aleniyeti esas olan adres bilgilerini kapsamaması sebebiyle, incelenen hükümde tüzel kişilerin rızasının aranmamasında Anayasanın 20. maddesine bir aykırılık bulunmamaktadır.

Diğer taraftan, Anayasanın mezkûr hükmünde kişisel verilerin "ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla" işlenebileceği hükme bağlandığından, belirtilen bu iki durumdan birinin varlığı kişisel verilerin işlenebilmesi için yeterli görülmekte ve kanunda istisna olarak öngörülen hâllerde kişinin açık rızasının da aranması gerekmemektedir.

Ayrıca, kararın gerekçesinde tüzel kişilere ait kişisel verilerin ilgili kanunlar gereği veya kişilerin kendilerince kamuya açıklanmış ya da açık sicillerde yer almış olmasının, söz konusu verilerin ücret karşılığında üçüncü kişilere aktarılmasına rıza gösterildiği anlamına gelmediği belirtilmekte ise de, veri tabanından yararlananlardan bir ücret alınıp alınmaması kişisel verilerin korunmasını isteme hakkı bakımından belirleyici bir unsur değildir.

Bu sebeplerle, 6475 sayılı Kanunun 3. maddesinin birinci fıkrasının (a) bendinde yer alan ". ilgili mevzuatı saklı kalmak kaydıyla, gerçek kişilerin rızası alınarak ..." ibaresindeki "gerçek" kelimesinin iptaline ilişkin talebin reddine karar verilmesi gerektiği düşüncesiyle, iptal yönündeki çoğunluk görüşüne katılmıyoruz.

Üye: Hicabi DURSUN; Muammer TOPAL; M. Emin KUZ

KARŞIOY GEREKÇESİ

6475 sayılı Posta Hizmetleri Kanunu'nun 29. maddesinin (2) numaralı fıkrasıyla, PTT hizmetleri ile ilgili olarak herhangi bir talepte bulunmak ve PTT'nin sorumlu olduğu hallerde dava açmak sadece o hizmetten yararlanan ile sınırlandırılırken; (3) numaralı fıkrasında ise, PTT hizmetleri ile ilgili olarak talepte bulunma ve dava açma hakkının, faaliyet konusu işlemin tesisi tarihinden itibaren bir yılın sonunda zamanaşımına uğrayacağı; bu sürenin PTT'ye başvuru ile kesileceği ve yapılan inceleme ve araştırmaların sonucunun ilgililere bildirildiği tarihte kesildiği yerden yeniden başlayacağı ile sürenin yeni bir başvuruyla tekrar kesilmeyeceği kurallarına yer verilmiştir.

Anayasanın 172. maddesinde Devlete, tüketicileri koruyucu ve aydınlatıcı tedbirleri alma ve tüketicilerin kendilerini koruyucu girişimlerini teşvik etme görevi verilmiş, bu görevleri hayata geçirmek için ise 4077 sayılı Tüketicinin Korunması Hakkında Kanun çıkarılmıştır. Bu Kanun hükümlerine göre, tüketici haklarının ihlali durumunda sadece hizmetten yararlanan tüketici değil, tüketici örgütleri ile Gümrük ve Ticaret Bakanlığı da dava açabilmekte; zamanaşımı süresi ise, ayıplı hizmetten dolayı yapılacak taleplerde hizmetin ifasından itibaren iki yıl, ayıplı hizmetin neden olduğu zarardan dolayı ise üç yıl olarak kurallaştırılmış bulunmaktadır.

6475 sayılı Kanununun, PTT hizmetleri ile ilgili olarak herhangi bir talepte bulunma ve PTT'nin sorumlu olduğu hallerde dava açmayı hizmetten yararlanan ile sınırlandıran 29. maddesinin (2) numaralı fıkrası, Anayasanın Devlete yüklediği tüketicilerin kendilerini koruyucu girişimlerini teşvik etme göreviyle; talepte bulunma ve dava açma süresini bir yıla sınırlayan (3) numaralı fıkrası ise, Devletin tüketicileri koruma göreviyle bağdaşmamaktadır.

Yasalar arasında aynı konuda farklı kurallar konulması yasa koyucunun takdir hakkı içindedir ve Anayasa Mahkemesi yasaların denetimini yasalara göre değil, Anayasal kurallara uygunluğa göre yapar denilebilir. Ancak, yasa koyucu takdir hakkını kullanırken Anayasal kurallara uymak zorundadır.

Anayasanın 172. maddesinin gereği olarak tüketici haklarını güvence altına almak üzere çıkarılan 4077 sayılı Tüketicinin Korunması Hakkında Kanunda yer alan güvencelere PTT A.Ş. lehine istisnai düzenlemeler getiren 6475 sayılı Posta Hizmetleri Kanunu'nun 29. maddesinin (2) ve (3) numaralı fıkralarındaki hükümler, Anayasanın 2. Maddesindeki kurallarla bağdaşmamaktadır.

Anayasanın 2. maddesinde hukuk devleti ilkesine de yer verilmiştir. Anayasanın 2. maddesindeki hukuk devleti, eylem ve işlemleri hukuka uygun olan, insan haklarına saygı gösteren, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adaletli bir hukuk düzeni kurup bunu geliştirerek sürdüren, Anayasaya aykırı durum ve tutumlardan kaçınan, hukuku tüm devlet organlarına egemen kılan, Anayasa ve hukukun üstün kurallarıyla kendini bağlı sayan, yargı denetimine açık olan devlettir.

Anayasa Mahkemesinin 20.11.1996 tarih, E.1996/58, K.1996/43 sayılı kararında da belirtildiği üzere, "hukuk Devleti olabilmenin en önemli göstergelerinden biri yasaların genelliği ilkesine uyulmasıdır. Yasaların genelliği ilkesi, özel, aktüel ve geçici bir durumu gözetmeyen, belli bir kişi veya kuruluşu hedef almayan, aynı statü ve durumda olan herkesi kapsayan kuralların getirilmesini zorunlu kılar. "Aynı durumve statüde olan herkesi kapsayan 4077 sayılı Kanundaki kuralları işlemez kılmayı, tüketiciler aleyhine ve PTT A.Ş. lehine, serbest piyasa ilkelerine aykırı, haksız rekabet oluşturacak

nitelikte, PTT A.Ş.'yi korumaya yönelik, özel, PTT A.Ş.'ye tanınan bir ayrıcalık, yasalaştırılarak yasaların genelliği ilkesinden ayrılmış olduğundan, kural Anayasanın 2. maddesindeki hukuk devleti ilkesine aykırılık taşımaktadır.

6475 sayılı Kanun'un 22. maddesinin (1) numaralı fıkrasında, PTT'nin faaliyet konuları; yurt içinde ve yurt dışında her türlü taşımacılık hizmetlerini de içerecek şekilde posta, koli, kargo ve lojistik hizmetleri; pul basımı ve satımı; 5411 sayılı Bankacılık Kanunu kapsamındaki faaliyet konuları ile ilgili bankalarla yapacağı sözleşmeler doğrultusunda bankalara destek hizmetleri, parasal posta hizmeti, ödeme hizmeti, adres bilgi kayıt sistemi ve elektronik sertifika hizmet sağlayıcılığı, elektronik ortam dahil her türlü tebligat ve telgraf hizmetlerine ilişkin faaliyetler ile esas sözleşmesinde belirlenen diğer faaliyetler olarak sıralanmıştır.

PTT'nin faaliyet alanı içinde bulunan yurtiçi ve yurtdışı koli ve kargo taşımacılığı hizmetlerini yürüten çok sayıda koli ve kargo taşımacılığı ile lojistik hizmeti firmaları; para transferi, ödeme ve bankacılık hizmetlerini yürüten çok sayıda banka vardır ve bunların tamamı yürüttüğü hizmetlerden dolayı, 4077 sayılı Tüketicinin Korunması Hakkında Kanun hükümlerine tabi bulunmaktadır.

PTT ile taşımacılık ve lojistik firmaları ve bankalar arasında sermayeye sahiplik dışında hukuken bir fark bulunmayıp, hukuk karşısında bunlar özdeş durumdadır.

Anayasa Mahkemesinin birçok kararında vurgulandığı üzere, Anayasanın 10. maddesinde öngörülen yasa önünde eşitlik ilkesi, birbirinin aynı durumda olanlara ayrı kuralların uygulanması ve ayrıcalıklı kişi ve toplulukların yaratılmasını engellemeyi amaçlamaktadır. Aynı durumda olanlar için ayrı düzenleme Anayasaya aykırılık oluşturur. Anayasanın amaçladığı eşitlik, eylemli değil hukuksal eşitliktir ve aynı hukuksal durumların aynı, ayrı hukuksal durumlar ayrı kurallara bağlı tutulmasını gerektirir.

PTT A.Ş.'nin faaliyet yürüttüğü taşımacılık, lojistik ve bankacılık sektörlerinde, faaliyette bulunan diğer firmalardan hukuki bir farklılığı yok iken, ayrı kurallara tabi tutularak ayrıcalıklı kılınmasını öngören 6475 sayılı Kanun'un 29. maddesinin (2) ve (3) numaralı fıkraları Anayasanın 10 uncu maddesine de aykırılık taşımaktadır.

Yukarıda açıklandığı üzere, 6475 sayılı Posta Hizmetleri Kanunu'nun 29. maddesinin (2) ve (3) numaralı fıkralarının, Anayasanın 2., 10. ve 172. maddelerine aykırı olduğunu düşündüğümden çoğunluk görüşüne katılmadım.

Üye - Celal Mümtaz AKINCI

KARŞIOY GEREKÇESİ

Mahkememiz çoğunluğu tarafından, iptal istemine konu 6475 sayılı Posta Hizmetleri Kanununun 3. maddesinin (a) bendinde yer alan 'gerçek' ibaresinin, kuralda tüzelkişiler yönünden rıza öğesine yer verilmemesi ve bu şekilde kişisel verilerinin korunmaması dolayısıyla Anayasa'nın 10. ve 20. maddelerine aykırı görülerek iptali gerektiği sonucuna ulaşılmış olmakla birlikte, aşağıda yazılı nedenlerle bu görüşe iştirak edememekteyim.

İncelemeye konu kural şöyledir : "a) Adres bilgi kayıt sistemi: 25.4.2006 tarihli ve 5490 sayılı Nüfus Hizmetleri Kanunu ve ilgili mevzuatı saklı kalmak kaydıyla, gerçek kişilerin rızası alınarak, gerçek ve tüzel kişiler ile kamu kurum ve kuruluşlarına ait fiziki ve elektronik adreslerin, reklam ve tanıtım amacıyla PTT hizmetlerinden yararlananlara ücret karşılığı kullandırılmasına yönelik olarak oluşturulan PTT'ye ait veri tabanını,"

5982 sayılı Kanunun 2. maddesiyle Anayasa'nın 20. maddesine eklenen 3. fıkra uyarınca, "herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. ... kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir..." Anayasa'daki bu düzenleme elbette tüzelkişileri de kapsamaktadır. Ancak düşünceme göre, gerçek kişiler ile tüzelkişiler bakımından nelerin kişisel veri sayılacağı konusunda tam bir paralellik kurulamaz.

Kişisel veri kavramı esasında gerçek kişiler için geliştirilmiştir. Bu kavramın ortaya çıkmasından önce gerçek kişiler bakımından hukuki koruma, kişilik haklarının korunması ve 'özel hayatın gizliliği' (mahremiyet hakkı) kavramları çerçevesinde sağlanmıştır. Gelişen insan hakları hukukuna paralel olarak insan onuru, bireyin özerkliği ve bilgilerin geleceğini belirleme hakkı gibi kavramlar geliştirilmiştir. Son kırk yılda Birleşmiş Milletler, OECD ve Avrupa Konseyi çalışmaları ve uluslararası metinlerde kişisel veri kavramı yerleşmiştir (bkz.; Elif Küzeci, *Kişisel Verilerin Korunması*, Ankara 2010, s. 67 vd., 116 vd.; Hayrunnisa Özdemir, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*, Ankara 2009, s. 26 vd.; Selen Uncular, *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, Ankara 2014, s. 29 vd.; Doğan Kılınç, *Anayasal Bir Hak Olarak Kişisel Verilerin Korunması*, AÜHFD Y. 61, S. 3, 2012, s. 1089 vd.). Nitekim Avrupa Birliği ülkelerinde veri koruma düzenlemelerinin temelini teşkil eden 94/46-EC sayılı Avrupa Veri Koruma Direktifinde gerçek kişiler bakımından kişisel verilerin korunması esas alınmış, ancak 2002/58 - EC sayılı Avrupa Parlamentosu ve Konsey Direktifi'nde yalnızca elektronik haberleşme sektörüne ilişkin olarak gerçek ve tüzel kişilerin veri sahibi kabul edilebileceği belirtilmiştir.

Avrupa Konseyi tarafından hazırlanan "Kişisel Nitelikteki Verilerin Otomatik işleme Tabi Tutulması Karsısında Şahısların Korunmasına Dair Sözleşme"nin 2. maddesinde kişisel veri; "Kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm bilgiler" olarak tanımlanmıştır (Kılınç, agm. s. 1094.).

Kişisel veri terimi ile genel olarak; kimliği belirli veya belirlenebilir bir kişiye ait her türlü bilgiyi ifade etmektedir. Bu anlamda gerçek kişilerin nüfus ve sağlık bilgileri, sosyal ve kültürel ilişkilerine ilişkin bilgiler, cinsel hayatlarına, gelir-giderlerine, aile yapıları ve bağlarına ilişkin bilgiler, inanç ve felsefi düşüncelerine, adreslerine dair bilgilerin kişisel veri olduğu söylenilmelidir. Bu kapsamda, gerçek kişiler yönünden adres bilgilerinin kişisel veri olarak kabul edilmesi doğaldır. Tüzelkişiler bakımından da, kişiliklerini ilgilendiren konularla ilgili olarak örneğin ticari varlıklarını ve ticari ilişkilerini ya da faaliyetleri ve faaliyetleri sırasında ilişki kurdukları gerçek ve tüzelkişilerle ilgili bilgilerini kişisel veri kapsamında değerlendirmek mümkün olabilir. Fakat tüzelkişiler bakımından adres bilgilerinin kişisel veri olarak kabul edilmesi, kişisel veri hukukunun amacını aşan ve hukukla bağdaşmayan aşırı bir yorum niteliğindedir. Diğer taraftan, ticari hayatta faaliyet gösteren şirketler ile kooperatifler kuruluş ve adresleri ticaret sicil gazetesinde ilan edilerek ve Medeni Kanun kapsamında kurulan vakıflar da tescil ve ilanı Resmi Gazete'de yayımlanarak aleniyet kazanmaktadır. Benzer biçimde dernekler de kamu yararı veya belirli bir amaçla faaliyet göstermek üzere kurulan ve topluma kendilerini bu isim ve adresleriyle duyuran özel hukuk tüzel kişileridir. Belirtilen tüzelkişiler bakımından aleniyet kazanan faaliyet adreslerinin kişisel veri olduğu ve anayasal koruma içerisinde bulunduğu görüşü tarafımda paylaşılmamaktadır. Buna karşın bir tüzel kişinin faaliyeti kapsamında herkesin bilmesine kapalı tutulan bazı adreslerin (örn. şirket toplantı yeri, üretim veya ticari planlama adresi, bir derneğin veya vakfın deposunun adresi vb.) kişisel veri olarak korunması söz konusu olabilir. Ancak kuralda söz konusu olan hukuken aleniyet kazanmış kuruluş adreslerine ilişkin bilgilerdir.

Anayasa'nın 10. maddesi yönünden ise, hukuk düzenindeki varlıkları, haklar ve borçlara ehliyetleri bakımından gerçek ve tüzelkişilerin eşit olduğu söylenebilir ise de, varoluş nedenleri gereği doğal olarak birtakım haklar bakımından farklı düzenlemelere ihtiyaç olacağı açıktır. Örneğin gerçek kişi için söz konusu olan seyahat hürriyetinin veya toplantı ve gösteri yürüyüşü hakkının tüzel kişi bakımından geçerli olduğu ve eşit düzenlemeleri gerektirdiği ileri sürülemez. Bu nedenle, kişisel veri bakımından aynı hukuki durumda bulunmayan gerçek ve tüzel kişiler arasında eşitlik karşılaştırmasının yapılamayacağı görüşündeyim. Diğer taraftan çoğunluk gerekçesinde tüzel kişiye ait adres bilgilerinin ticari kullanımının hukuka aykırı olduğu ileri sürülmüştür. Tüzel kişilere ilişkin hukuk kurallarında alenileşmesi öngörülen adres bilgilerinin, söz gelimi internet ortamında herhangi

bir kiři tarafından, "Türkiye'deki Çocuk ve Kadın Vakıfları ve Adresleri" başlıđı altında reklam gelirlerini haiz bir arama motoruyla tanıtılıyor olması hukuka aykırı olmayacağı gibi, incelenen Kanundaki düzenlemenin bu bakımdan aykırı bulunması da o derece mümkün olmayacaktır.

Açıklanan nedenlerle, incelenen kuralın Anayasa'ya aykırı olmadığı ve iptal başvurusunun reddi gerektiđi görüşünde olduğumdan, sayın çoğunluğun iptal kararına iřtirak edememekteyim.

Üye - Hasan Tahsin GÖKCAN

Anayasa Mahkemesi - 2004 sayılı İcra ve İflas Kanunu Kararı (E. 2012/100)

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2012/100

Karar Sayısı: 2013/84

Karar Günü: 4.7.2013

R.G. Tarih-Sayı: 02.08.2013-28726

İPTAL DAVASINI AÇANLAR: Türkiye Büyük Millet Meclisi üyeleri Emine Ülker TARHAN ve Dilek AKAGÜN YILMAZ ile birlikte 123 milletvekili

DAVANIN KONUSU: 2.7.2012 günlü, 6352 sayılı Yargı Hizmetlerinin Etkinleştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılması ve Basın Yayın Yoluyla İşlenen Suçlara İlişkin Dava ve Cezaların Ertelenmesi Hakkında Kanun'un:

- 1- 1. maddesiyle 9.6.1932 günlü, 2004 sayılı İcra ve İflas Kanunu'nun başlığı ile birlikte değiştirilen 1. maddesinin beşinci fıkrasının,
- 2- 3. maddesiyle 2004 sayılı Kanun'a eklenen 8/a maddesinin ikinci fıkrasının,
- 3- 21. maddesiyle değiştirilen 2004 sayılı Kanun'un 106. maddesinin birinci fıkrasının,
- 4- 22. maddesiyle değiştirilen 2004 sayılı Kanun'un 110. maddesinin birinci fıkrasının,
- 5- 24. maddesiyle 2004 sayılı Kanun'un 114. maddesine eklenen dördüncü fıkranın 'Açık artırmaya elektronik ortamdan teklif verme yoluyla başlanır.' biçimindeki birinci cümlesinin,
- 6- 25. maddesiyle 2004 sayılı Kanun'un başlığı ile birlikte değiştirilen 115. maddesinin,
- 7- 28. maddesiyle değiştirilen 2004 sayılı Kanun'un 124. maddesinin üçüncü fıkrasının,
- 8- 29. maddesiyle 2004 sayılı Kanun'un başlığı ile birlikte değiştirilen 126. maddesinin dördüncü fıkrasının,
- 9- 31. maddesiyle değiştirilen 2004 sayılı Kanun'un 129. maddesinin,
- 10- 44. maddesiyle 6.1.1982 günlü, 2575 sayılı Danıştay Kanunu'nun 8. maddesinin;
 - a- (1) numaralı fıkrasının,
 - aa- (d) bendine eklenen 'Türkiye Büyük Millet Meclisi Genel Sekreterliği,' ibaresinin,

- ab- (e) bendine eklenen 'ile düzenleyici ve denetleyici kurumların başkanlıkları,' ibaresinin,
- ac- Değiştirilen (g) bendinin,
- b- (3) numaralı fıkrasındaki değiştirilen 'onbeş yıl' ibaresinin,
- 11- 45. maddesiyle değiştirilen 2575 sayılı Kanun'un 24. maddesinin (1) numaralı fıkrasının (c) bendinin,
- 12- 46. maddesiyle değiştirilen 2575 sayılı Kanun'un 60. maddesinin (1) numaralı fıkrasının,
- 13- 47. maddesiyle değiştirilen 2575 sayılı Kanun'un 61. maddesinin (1) ve (3) numaralı fıkralarının,
- 14- 57. maddesiyle;
- a- 6.1.1982 günlü, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 27. maddesinin değiştirilen (2) numaralı fıkrasının,
- b- 2577 sayılı Kanun'un 27. maddesine eklenen (3) ve (10) numaralı fıkraların,
- 15- 58. maddesiyle değiştirilen 2577 sayılı Kanun'un 28. maddesinin (2) ve (6) numaralı fıkralarının,
- 16- 72. maddesiyle 24.2.1983 günlü, 2802 sayılı Hâkimler ve Savcılar Kanunu'nun 37. maddesinin birinci fıkrasına eklenen (c) bendinin,
- 17- 74. maddesiyle 12.4.1991 günlü, 3713 sayılı Terörle Mücadele Kanunu'nun 2. maddesinin ikinci fıkrasında yer alan 've örgüt mensupları gibi cezalandırılırlar' ibaresinin madde metninden çıkarılmasının,
- 18- 75. maddesiyle 3713 sayılı Kanun'un başlığı ile birlikte değiştirilen 10. maddesinin,
- 19- 77. maddesiyle 9.6.2004 günlü, 5187 sayılı Basın Kanunu'nun 26. maddesinin birinci ve altıncı fıkralarında yapılan değişikliklerin,
- 20- 85. maddesiyle değiştirilen 26.9.2004 günlü, 5237 sayılı Türk Ceza Kanunu'nun 220. maddesinin (6) ve (7) numaralı fıkralarının,
- 21- 90. maddesiyle 5237 sayılı Kanun'un başlığı ile birlikte değiştirilen 277. maddesinin,
- 22- 92. maddesiyle değiştirilen 5237 sayılı Kanun'un 285. maddesinin,
- 23- 93. maddesiyle değiştirilen 5237 sayılı Kanun'un 288. maddesinin,
- 24- 95. maddesiyle 4.12.2004 günlü, 5271 sayılı Ceza Muhakemesi Kanunu'na eklenen 38/A maddesinin,
- 25- 105. maddesinin,

26- Geçici 1. maddesinin,

27- Geçici 2. maddesinin (4), (5), (6) ve (7) numaralı fıkralarının,

28- Geçici 3. maddesinin,

Anayasa'nın Başlangıç'ı ile 2., 4., 5., 6., 7., 8., 9., 10., 11., 12., 13.,17., 20., 36., 37., 38., 40., 87., 90., 125., 128., 138., 139., 140. ve 153. maddelerine aykırılığı ileri sürülerek iptallerine ve yürürlüklerinin durdurulmasına karar verilmesi istemidir.

II- YASA METİNLERİ

A- İptali İstenilen Yasa Kuralları

2.7.2012 günlü, 6352 sayılı Yargı Hizmetlerinin Etkinleştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılması ve Basın Yayın Yoluyla İşlenen Suçlara İlişkin Dava ve Cezaların Ertelenmesi Hakkında Kanun'un:

1- 1. maddesiyle değiştirilen 9.6.1932 günlü, 2004 sayılı İcra ve İflas Kanunu'nun iptali istenen kuralın da yer aldığı 'İcra daireleri' başlıklı 1. maddesi şöyledir:

'Her asliye mahkemesinin yargı çevresinde yeteri kadar icra dairesi bulunur.

Her icra dairesinde Adalet Bakanlığı tarafından atanacak bir icra müdürü, yeteri kadar icra müdür yardımcısı, icra katibi ile adli yargı ilk derece mahkemesi adalet komisyonları tarafından görevlendirilecek mübaşir ve hizmetli bulunur.

İcra müdür ve icra müdür yardımcıları, Adalet Bakanlığı tarafından yaptırılacak yazılı sınav ve Adalet Bakanlığı tarafından yapılacak sözlü sınav sonucuna göre atanırlar. İcra katipleri arasından Adalet Bakanlığı tarafından yaptırılacak yazılı sınav ve Adalet Bakanlığı tarafından yapılacak sözlü sınav sonucuna göre de icra müdür veya icra müdür yardımcılığı kadrolarına atama yapılabilir.

İcra katipliğine ilk defa atanacaklar, kamu görevlerine ilk defa atanacaklar için yapılacak merkezî sınavda başarılı olanlar arasından Adalet Bakanlığının bu konuda yetki vereceği adli yargı ilk derece mahkemesi adalet komisyonları tarafından yapılacak uygulama ve sözlü sınav sonucuna göre; unvan değişikliği suretiyle atanacaklar ise uygulama ve sözlü sınav sonucuna göre atanırlar. Unvan değişikliği suretiyle icra katipliğine atanacaklar tahsis edilen kadronun yüzde ellisini geçemez.

İcra müdür ve icra müdür yardımcıları ile icra katiplerinin, yazılı sınav, sözlü sınav, görevlendirme, nakil, unvan değişikliği, görevde yükselme ve diğer hususları yönetmelikle düzenlenir.

İcra dairelerinde, gerektiğinde, Adalet Bakanlığı tarafından belirlenecek esaslar çerçevesinde, adli yargı ilk derece mahkemesi adalet komisyonu tarafından zabıt katibi, mübaşir ve hizmetli görevlendirilir.

İcra müdürü, icra müdür yardımcısı veya icra katibinin herhangi bir nedenden dolayı yokluğu halinde görev ve yetkileri, adli yargı ilk derece mahkemesi adalet komisyonu tarafından görevlendirilecek yazı işleri müdürü veya zabıt katibi tarafından yerine getirilir.

Adalet Bakanlığı, icra dairelerini bir arada bulundurmaya ve aynı icra mahkemesine bağlamaya yetkilidir.'

2- 3. maddesiyle, 2004 sayılı Kanun'a eklenen ve iptali istenen kuralın da yer aldığı 'Elektronik işlemler' başlıklı 8/a maddesi şöyledir:

'İcra ve iflas dairelerince yapılacak her türlü icra ve iflas iş ve işlemlerinde Ulusal Yargı Ağı Bilişim Sistemi kullanılır; her türlü veri, bilgi, belge ve karar, Ulusal Yargı Ağı Bilişim Sistemi vasıtasıyla işlenir, kaydedilir ve saklanır.

Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir. Güvenli elektronik imza, elle atılan imza ile aynı ispat gücünü haizdir. Güvenli elektronik imza, kanunlarda güvenli elektronik imza ile yapılamayacağı açıkça belirtilmiş olan işlemler dışında, elle atılan imza yerine kullanılabilir. Güvenli elektronik imzayla oluşturulan belge ve kararlarda, kanunlarda birden fazla nüshanın düzenlenmesi ve mühürleme işlemini öngören hükümler uygulanmaz.

Zorunlu nedenlerden dolayı fiziki olarak düzenlenen belge veya kararlar, yetkili kişilerce güvenli elektronik imzayla imzalanarak Ulusal Yargı Ağı Bilişim Sistemine aktarılır ve gerektiğinde Ulusal Yargı Ağı Bilişim Sistemi vasıtasıyla ilgili birimlere iletilir. Bu şekilde elektronik ortama aktarılarak ilgili birimlere iletilen belge ve kararların asılları, gönderen icra ve iflas dairesinde saklanır, ayrıca fiziki olarak gönderilmez. Ancak, belge veya kararın aslının incelenmesinin zorunlu olduğu hâller saklıdır.

Elektronik ortamdan fiziki örnek çıkartılması gereken hâllerde, icra müdürü veya görevlendirdiği personel tarafından belgenin aslının aynı olduğu belirtilerek, imzalanır ve mühürlenir.

Elektronik ortamda yapılan işlemlerde süre gün sonunda biter.

Elektronik işlemlerin Ulusal Yargı Ağı Bilişim Sistemi vasıtasıyla yapılmasına dair usul ve esaslar, Adalet Bakanlığı tarafından çıkarılan yönetmelikle düzenlenir.'

3- 21. maddesiyle deęiřtirilen 2004 sayılı Kanun'un iptali istenen kuralın da yer aldıęı 'Talep için müddetler' bařlıklı 106. maddesi řoyledir:

'Alacaklı, haczolunan mal tařınır ise hacizden itibaren altı ay, tařınmaz ise hacizden itibaren bir yıl içinde satılmasını isteyebilir.

Borçlunun üçüncü řahıslardaki alacaęı tařınır hükmündedir.'

4- 22. maddesiyle deęiřtirilen 2004 sayılı Kanun'un iptali istenen kuralların da yer aldıęı 'Haczin kalkması' bařlıklı 110. maddesi řoyledir:

'Bir malın satılması kanuni müddet içinde istenmez veya icra müdürü tarafından verilecek karar gereęi gerekli gider onbeř gün içinde depo edilmezse veya talep geri alınıp da kanuni müddet içinde yenilenmezse o mal üzerindeki haciz kalkar. Hacizli malın satılması yönündeki talep bir defa geri alınabilir.

Haczedilen resmi sicile kayıtlı malların, icra dairesiyle yapılacak yazıřmalar sonucunda haczinin kalktıęının tespit edilmesi hâlinde, sicili tutan idare tarafından haciz řerhi terkin edilir ve iřlem ilgili icra dairesine bildirilir.

Birinci fıkraya gereęince haczin kalkmasına sebebiyet veren alacaklı o mala yönelik olarak, haczin konulması ve muhafazası gibi tüm giderlerden sorumlu olur.'

5- 24. maddesiyle deęiřtirilen 2004 sayılı Kanun'un iptali istenen kuralın da yer aldıęı 'Arttırma hazırlık tedbirleri' bařlıklı 114. maddesi řoyledir:

'(Deęiřik birinci fıkraya: 17/7/2003-4949/27 md.) Satıř açık artırma ile yapılır. Birinci ve ikinci artırmanın yapılacaęı yer, gün ve saat daha önceden ilân edilir.

İlanın řekli, artırmanın tarzı, yer ve günü ve gazete ile yapılıp yapılmıyacaęı icra memurluęunca alakadarların menfaatlerine en muvafık geleni nazarı dikkate alınarak tayin olunur. (Ek cümle: 17/7/2003-4949/27 md.) İlanın yurt düzeyinde yayımlanan bir gazete ile yapılmasına karar verilmesi hâlinde bu ilân satıř talebi tarihinde tirajı ellibinin (50.000) üzerinde olan ve yurt düzeyinde daęıtımı yapılan gazetelerden biriyle yapılır.

(Ek: 18/2/1965'538/57 md.) Gazete ile yapılacak ilanlara satıř řartnamesi eklentisiyle geçirilmeyip, satılacak řeyin cinsi, mahiyeti, önemli vasıfları, muhammen kıymeti, bulunduęu yer ve ikinci artırmanın gün ve saati, satıř řartnamesinin vesair bilginin nereden ve ne suretle öęrenilebileceęi, talep halinde ve ilanda gösterilen masrafı verilmek řartıyla řartnamenin bir örneęinin gönderilebileceęi hususları yazılmakla iktifa olunur. İcra dairesince yapılması zaruri ilanlar dıřında,

tarafklar Őartnamenin tamamını, masrafı kendilerine ait olmak üzere, diledikleri vasıtalarla ilan edebilirler. Ancak hususi mahiyetteki bu ilan resmi muameleye tesir etmez. (Ek cümle: 2/7/2012'6352/24 md.) Satış ilanı elektronik ortamda da yapılır.

(Ek 2/7/2012'6352/24 md.) Açık artırmaya elektronik ortamda teklif verme yoluyla başlanır. Elektronik ortamda teklif verme, birinci ihale tarihinden on gün önce başlar, ihalenin tamamlanacağı günden önceki gün sonunda sona erer; ikinci ihalede ise elektronik ortamda teklif verme birinci ihaleden sonraki beşinci gün başlar, en az on gün sonrası için belirlenecek ikinci ihalenin tamamlanacağı günden önceki gün sonunda sona erer. Elektronik ortamda verilecek teklifler haczedilen malın tahmin edilen kıymetinin yüzde ellisinden az olamaz; teklif vermeden önce, haczedilen malın tahmin edilen kıymetinin yüzde yirmisi nispetinde teminat gösterilmesi zorunludur.

(Ek 2/7/2012'6352/24 md.) Satışa çıkarılan taşınır üzerinde hakkı olan alacaklının alacağı yukarıdaki fıkrada yazılı oranda ise artırmaya iştiraki halinde ayrıca pey akçesi ve teminat aranmaz.'

6- 25. maddesiyle değiştirilen 2004 sayılı Kanun'un 'İhalenin yapılması:' başlıklı 115. maddesi şöyledir:

(Değişik: 2/7/2012'6352/25 md.) Birinci ve ikinci ihale icra memuru tarafından, ilanda belirlenen yer, gün ve saatte, elektronik ortamda verilen en yüksek teklif üzerinden başlatılır. Satışa çıkarılan mal üç defa bağırdıktan sonra, elektronik ortamda verilen en yüksek teklif de değerlendirilerek, en çok artırana ihale edilir. Şu kadar ki, artırma bedelinin malın tahmin edilen bedelinin yüzde ellisini bulması ve satış isteyen alacağına rüçhanı olan diğer alacaklar o malla temin edilmişse bu suretle rüçhanı olan alacakların mecmuundan fazla olması ve bundan başka paraya çevirme ve paraların paylaşılması masraflarını aşması gerekir.

Birinci ihalede, alıcı çıkmazsa veya bu maddede yazılı miktara ulaşılmazsa satış icra memuru tarafından geri bırakılır.

İkinci ihalede, alıcı çıkmazsa veya bu maddede yazılı şartlar gerçekleşmezse satış talebi düşer.'

7- 28. maddesiyle değiştirilen 2004 sayılı Kanun'un iptali istenen kuralın da yer aldığı '1- Şartnamenin açık bulundurulması' başlıklı 124. maddesi şöyledir:

'İcra dairesi taşınmazların bulunduğu yerin adetlerine göre en elverişli tarzda artırma şartlarını tesbit eder.

Bunları ihtiva eden şartname artırmadan evvel en az on gün müddetle icra dairesinde herkesin görmesi için açık bulundurulur.

(Değişik: 2/7/2012'6352/28 md.) Şartnameye, artırmaya iştirak edeceklerin taşınmazın tahmin edilen kıymetinin yüzde yirmisi nispetinde pey akçesi veya milli bir bankanın teminat mektubunu tevdi etmeleri, elektronik ortamda teklif vererek artırmaya katılacakların teminat göstermeleri gerektiği ve elektronik ortamda teklif vermeye ilişkin hususlar yazılır.

Satılığa çıkarılan taşınmaz üzerinde hakkı olan alacaklının alacağı yukarkı fıkrada yazılı nispet raddesinde ise artırmaya iştiraki halinde ayrıca pey akçesi ve teminat aranmaz.'

8- 29. maddesiyle değiştirilen 2004 sayılı Kanun'un iptali istenen kuralın da yer aldığı 'Artırma ilanı, artırma hazırlıkları ve ilgililere ihtar' başlıklı 126. maddesi şöyledir:

'Satış, açık artırma ile yapılır. Birinci ve ikinci ihalenin yapılacağı yer, gün ve saat önceden ilan edilir.

İlan, birinci ihale tarihinden en az bir ay önce yapılır. İlan edilen metnin esasa müessir olmayan maddi hatalar nedeniyle tekrarlanması gerektiğinde, ihale tarihi değiştirilmeksizin hata ilan edilene düzeltilir. Ancak bu düzeltme ilanının tarihi ile ihale tarihi arasında yedi günden az zaman kalmış ise daha önce ilan edilen günden yedi iş günü sonrası için tespit edilecek günde satış yapılacağı düzeltme ilanında belirtilir. Bu düzeltme ilanı ilgililere ayrıca tebliğ edilmez.

Yapılacak ilana, satılacak şeyin cinsi, mahiyeti, önemli vasıfları, tahmin edilen kıymeti, bulunduğu yer; birinci ve ikinci ihalenin yapılacağı yer, gün ve saat; artırmaya iştirak edeceklerin haczedilen malın tahmin edilen kıymetinin yüzde yirmisi nispetinde pey akçesi veya milli bir bankanın teminat mektubunu tevdi etmeleri gerektiği; diğer bilgilerin nereden ve ne suretle öğrenilebileceği hususları yazılır. Ayrıca, ipotek sahibi alacaklılarla diğer ilgililerin taşınmaz üzerindeki haklarını, hususiyle faiz ve masrafa dair olan iddialarını evrakı müsbiteleri ile onbeş gün içinde icra dairesine bildirmeleri gerektiği yazılır; aksi halde, hakları tapu siciliyle sabit olmadıkça, satış bedelinin paylaşmasından hariç kalacakları da ilave edilir. Bu ihtar irtifak hakkı sahiplerine de yapılır.

Açık artırmaya elektronik ortamda teklif verme yoluyla başlanır. Elektronik ortamda teklif verme, birinci ihale tarihinden yirmi gün önce başlar, ihalenin tamamlanacağı günden önceki gün sonunda sona erer; ikinci ihalede ise elektronik ortamda teklif verme birinci ihaleden sonraki beşinci gün başlar, en az yirmi gün sonrası için belirlenecek ikinci ihalenin tamamlanacağı günden önceki gün sonunda sona erer. Elektronik ortamda verilecek teklifler haczedilen malın tahmin edilen kıymetinin yüzde ellisinden az olamaz; teklif vermeden önce, haczedilen malın tahmin edilen kıymetinin yüzde yirmisi nispetinde teminat gösterilmesi zorunludur.

Satışa çıkarılan taşınmaz üzerinde hakkı olan alacaklının alacağı yukarıdaki fıkrada yazılı oranda ise artırmaya iştiraki halinde ayrıca pey akçesi ve teminat aranmaz.

114 üncü maddenin ikinci ve üçüncü fıkraları taşınmazın satış ilanı hakkında da uygulanır.'

9- 31. maddesiyle değiştirilen 2004 Sayılı Kanun'un 'İhale' başlıklı 129. maddesi şöyledir:

'(Değişik 2/7/2012'6352/28 md.) Birinci ve ikinci ihale icra memuru tarafından, ilanda belirlenen yer, gün ve saatte, elektronik ortamda verilen en yüksek teklif üzerinden başlatılır. Taşınmaz üç defa bağırıldıktan sonra, elektronik ortamda verilen en yüksek teklif de değerlendirilerek, en çok artırana ihale edilir. Şu kadar ki, artırma bedelinin malın tahmin edilen bedelinin yüzde ellisini bulması ve satış isteyen alacağına rüçhanı olan diğer alacaklar o malla temin edilmişse bu suretle rüçhanı olan alacakların mecmuundan fazla olması ve bundan başka paraya çevirme ve paraların paylaşılması masraflarını aşması gerekir.

Birinci ihalede, alıcı çıkmazsa veya bu maddede yazılı miktara ulaşılmazsa satış icra memuru tarafından geri bırakılır.

İkinci ihalede, alıcı çıkmazsa veya bu maddede yazılı şartlar gerçekleşmezse satış talebi düşer.'

10- 44. maddesiyle değiştirilen 6.1.1982 günlü, 2575 sayılı Danıştay Kanunu'nun iptali istenen kuralların da yer aldığı 'Danıştay üyelerinin nitelikleri ' başlıklı 8 maddesi şöyledir:

'1. Danıştay üyeleri:

a) İdari yargı hakim ve savcılığı,

b) Bakanlık, müsteşarlık, müsteşar yardımcılığı, elçilik, valilik,

c) Generallik, amirallik,

d)Cumhurbaşkanlığı Genel Sekreterliği, Türkiye Büyük Millet Meclisi Genel Sekreterliği,

e) Genel ve katma bütçeli dairelerde veya kamu kuruluşlarında genel müdürlük veya en az bu derecedeki tetkik ve teftiş kurul başkanlıkları, ile düzenleyici ve denetleyici kurumların başkanlıkları,

f) Yükseköğrenim kurumlarında hukuk, iktisat, maliye, kamu yönetimi profesörlüğü,

g) (Değişik: 2/7/2012-6352/44 md.) Kamu kurum ve kuruluşlarının başhukuk müşavirliği, birinci hukuk müşavirliği, hukuk hizmetleri başkanlığı ve hukuk işleri müdürlüğü,

Görevlerini yapanlar arasından seçilir.

2. İdari yargı hakim ve savcılarının Danıştay üyeliğine seçilebilmeleri için birinci sınıfa ayrıldıktan sonra en az üç yıl bu görevlerde başarı ile çalışmış olmaları ve birinci sınıfa ayrılma niteliğini kaybetmemeleri gereklidir.

3. İdari görevlerden Danıştay üyeliğine seçileceklerin yükseköğrenimlerini tamamladıktan sonra Devlet hizmetlerinde onbeş yıl (') çalışmış bulunmaları, birinci derece aylığını kazanılmış hak olarak almaları ve hakimliğin gerektirdiği ahlak ve seciyeye sahip olmaları şarttır.'

11- 45. maddesiyle değiştirilen 2575 sayılı Kanun'un ipali istenen kuralın da yer aldığı 'İlk derece mahkemesi olarak Danıştayda görülecek davalar' başlıklı 24. maddesi şöyledir:

'1. Danıştay ilk derece mahkemesi olarak:

a) Bakanlar Kurulu kararlarına,

b) (Değişik: 2/6/2004 - 5183/4 md.)Başbakanlık, bakanlıklar ve diğer kamu kurum ve kuruluşlarının müsteşarlarıyla ilgili müşterek kararnamelere,

c) (Değişik: 2/7/2012-6352/45 md.) Bakanlıklar ile kamu kuruluşları veya kamu kurumu niteliğindeki meslek kuruluşlarınca çıkarılan ve ülke çapında uygulanacak düzenleyici işlemlere,

d) Danıştay İdari Dairesince veya İdari İşler Kurulunca verilen kararlar üzerine uygulanan eylem ve işlemlere,

e) Birden çok idare veya vergi mahkemesinin yetki alanına giren işlere,

f) Danıştay Yüksek Disiplin Kurulu kararları ile bu Kurulun görev alanı ile ilgili Danıştay Başkanlığı işlemlerine,

Karşı açılacak iptal ve tam yargı davaları ile tahkim yolu öngörülmeven kamu hizmetleri ile ilgili imtiyaz şartlaşma ve sözleşmelerinden doğan idari davaları karara bağlar.

2. Danıştay, belediyeler ile il özel idarelerinin seçimle gelen organlarının organlık sıfatlarını kaybetmeleri hakkındaki istemleri inceler ve karara bağlar.'

12- 46. maddesiyle değiştirilen 2575 sayılı Kanun'un ipali istenen kuralın da yer aldığı 'Danıştay Başsavcısının görevleri' başlıklı 60. maddesi şöyledir:

'1. (Değişik birinci cümle: 2/7/2012-6352/46 md.) Başsavcı, ilk derece mahkemesi sıfatıyla Danıştayda görülen dava dosyalarını, esas hakkındaki düşüncelerini bildirmek üzere, uygun göreceği görev ayırımına göre savcılara havale eder. Düşüncelerinin vaktinde bildirilmesini ve savcılar ile Başsavcılıkta görevli diğer memurların devamlarını ve intizamla çalışmalarını sağlar, gelen dosyaların kaydı ve saklanması ile işi bitenlerin ilgili yerlere geciktirilmeden gönderilmesi için gerekli tedbirleri alır.

2. Başsavcı, incelediği dava dosyaları hakkında düşüncelerini bildirir ve kanunlarla kendisine verilen diğer görevleri yapar.

3. Başsavcı her takvim yılı sonunda, işlerin durumu ve bunların yürütülmesinde aksaklık varsa sebepleri hakkında Danıştay Başkanlığına bir rapor verir ve alınmasını lüzumlu gördüğü idari tedbirleri bildirir.

4. Başsavcı, savcılardan birini, idari işlerde kendisine yardım etmekte görevlendirebilir'

13- 47. maddesiyle değiştirilen 2575 sayılı Kanun'un 61. maddesinin iptali istenen kuralların da yer aldığı 'Savcıların görevleri' başlıklı 61. maddesi şöyledir:

'1. (Değişik: 2/7/2012-6352/47 md.) Savcılar, ilk derece mahkemesi sıfatıyla Danıştayda görülen dava dosyalarından kendilerine havale olunanları Başsavcı adına incelerler ve esas hakkındaki düşüncelerini, bir ay içinde gerekçeli ve yazılı olarak verirler. Bu süreler geçirilirse durumu sebepleriyle birlikte Başsavcıya bildirirler. Danıştay Başkanının ve Başsavcısının vereceği diğer görevleri yerine getirir; çalışma düzeninin korunması ve iş veriminin artırılması için Başsavcının alacağı tedbirlere uyarlar.

2. Savcılar, ilgili yerlerden Danıştay Başkanlığı aracılığı ile her türlü bilgileri isteyebilecekleri gibi işlem dosyalarını da getirebilirler.

3. (Değişik: 2/7/2012-6352/47 md.) Dava dairelerince gerekli görüldüğü takdirde, Danıştay savcıları, önceden haber verilmek suretiyle, düşüncelerini sözlü olarak da açıklarlar.'

14- 57. maddesiyle değiştirilen 6.1.1982 günlü, 2577 sayılı İdari Yargılama Usulü Kanunu'nun iptali istenen kuralların da yer aldığı 'Yürütmenin durdurulması' başlıklı 27. maddesi şöyledir:

'1. Danıştayda veya idari mahkemelerde dava açılması dava edilen idari işlemin yürütülmesini durdurmaz.

2. (Değişik: 2/7/2012 - 6352/57 md.) Danıştay veya idari mahkemeler, idari işlemin uygulanması halinde telafisi güç veya imkânsız zararların doğması ve idari işlemin açıkça hukuka aykırı olması şartlarının birlikte gerçekleşmesi durumunda, davalı idarenin savunması alındıktan veya savunma süresi geçtikten sonra gerekçe göstererek yürütmenin durdurulmasına karar verebilirler. Uygulanmakla etkisi tükenecek olan idari işlemlerin yürütülmesi, savunma alındıktan sonra yeniden karar verilmek üzere, idarenin savunması alınmaksızın da durdurulabilir. Yürütmenin durdurulması kararlarında idari işlemin hangi gerekçelerle hukuka açıkça aykırı olduğu ve işlemin uygulanması halinde doğacak telafisi güç veya imkânsız zararların neler olduğunun belirtilmesi zorunludur.

Sadece ilgili kanun hükmünün iptali istemiyle Anayasa Mahkemesine başvurulduğu gerekçesiyle yürütmenin durdurulması kararı verilemez.

3. (Ek: 2/7/2012 - 6352/57 md.) Dava dilekçesi ve eklerinden yürütmenin durdurulması isteminin yerinde olmadığı anlaşılırsa, davalı idarenin savunması alınmaksızın istem reddedilebilir.

4. Vergi mahkemelerinde, vergi uyuşmazlıklarından doğan davaların açılması, tarh edilen vergi, resim ve harçlar ile benzeri mali yükümlerin ve bunların zam ve cezalarının dava konusu edilen bölümünün tahsil işlemlerini durdurur. Ancak, 26 ncı maddenin 3 üncü fıkrasına göre işlemden kaldırılan vergi davası dosyalarında tahsil işlemi devam eder. Bu şekilde işlemden kaldırılan dosyanın yeniden işleme konulması ile ihtirazi kayıtla verilen beyannameler üzerine yapılan işlemlerle tahsilat işlemlerinden dolayı açılan davalar, tahsil işlemini durdurmaz. Bunlar hakkında yürütmenin durdurulması istenebilir.

5. Yürütmenin durdurulması istemli davalarda 16 ncı maddede yazılı süreler kısaltılabileceği gibi, tebliğin memur eliyle yapılmasına da karar verilebilir.

6. Yürütmenin durdurulması kararları teminat karşılığında verilir; ancak, durumun gereklerine göre teminat aranmayabilir. Taraflar arasında teminata ilişkin olarak çıkan anlaşmazlıklar, yürütmenin durdurulması hakkında karar veren daire, mahkeme veya hakim tarafından çözümlenir. İdareden ve adli yardımdan faydalanan kimselerden teminat alınmaz.

7. Yürütmenin durdurulması istemleri hakkında verilen kararlar; Danıştay dava dairelerince verilmişse konusuna göre İdari veya Vergi Dava Daireleri Kurullarına, bölge idare mahkemesi kararlarına karşı en yakın bölge idare mahkemesine, idare ve vergi mahkemeleri ile tek hakim tarafından verilen kararlara karşı bölge idare mahkemesine, çalışmaya ara verme süresi içinde ise idare ve vergi mahkemeleri tarafından verilen kararlara en yakın nöbetçi mahkemeye veya kararı veren hakimin katılmadığı nöbetçi mahkemeye, kararın tebliğini izleyen günden itibaren yedi gün içinde bir defaya mahsus olmak üzere itiraz edilebilir. İtiraz edilen merciler, dosyanın kendisine gelişinden itibaren yedi gün içinde karar vermek zorundadır. İtiraz üzerine verilen kararlar kesindir.

8. Yürütmenin durdurulması kararı verilen dava dosyaları öncelikle incelenir ve karara bağlanır.

9. (Ek: 2/7/2012 - 6352/57 md.) Yürütmenin durdurulmasına dair verilen kararlar onbeş gün içinde yazılır ve imzalanır.

10. (Ek: 2/7/2012 - 6352/57 md.) Aynı sebeplere dayanılarak ikinci kez yürütmenin durdurulması isteminde bulunulamaz.'

15- 58. maddesiyle deęiřtirilen 2577 sayılı Kanun'un iptali istenen kuralların da yer aldıęı 'Kararların sonuçları' bařlıklı 28. maddesi řoyledir:

'1.(Deęiřik:10/6/1994-4001/13 md.) Danıřtay, blge idare mahkemeleri, idare ve vergi mahkemelerinin esasa ve yrtmenin durdurulmasına iliřkin kararlarının icaplarına gre idare, gecikmeksizin iřlem tesis etmeye veya eylemde bulunmaya mecburdur. Bu sre hiřbir řekilde kararın idareye teblięinden bařlayarak otuz gn geemez. Ancak, haciz veya ihtiyati haciz uygulamaları ile ilgili davalarda verilen kararlar hakkında, bu kararların kesinleřmesinden sonra idarece iřlem tesis edilir.

2. (Deęiřik: 2/7/2012 - 6352/58 md.)Konusu belli bir miktar paranın denmesini gerektiren davalarda hkmedilen miktar ile her trl davalarda hkmedilen vekalet creti ve yargılama giderleri, davacının veya vekilinin davalı idareye yazılı řekilde bildireceęi banka hesap numarasına, bu bildirim tarihinden itibaren, birinci fıkrada belirtilen usul ve esaslar erevesinde yatırılır. Birinci fıkrada belirtilen sreler iinde deme yapılmaması halinde, genel hkmler dairesinde infaz ve icra olunur.

3. Danıřtay, blge idare mahkemeleri, idare ve vergi mahkemeleri kararlarına gre iřlem tesis edilmeyen veya eylemde bulunulmayan hallerde idare aleyhine Danıřtay ve ilgili idari mahkemede maddi ve manevi tazminat davası aılabilir.

4. Mahkeme kararlarının (otuz) (1) gn iinde kamu grevlilerince kasten yerine getirilmemesi halinde ilgili, idare aleyhine dava aabileceęi gibi,kararı yerine getirmeyen kamu grevlisi aleyhine de tazminat davası aılabilir.

5. Vergi uyuřmazlıklarına iliřkin mahkeme kararlarının idareye teblięinden sonra bu kararlara gre tespit edilecek vergi, resim, harlar ve benzeri mali ykmler ile zam ve cezaların miktarı ilgili idarece mkellefe bildirilir.

6. (Deęiřik: 2/7/2012 - 6352/58 md.) Tazminat ve vergi davalarında idarece, mahkeme kararının teblię tarihi ile deme tarihi arasındaki sreye 21/7/1953 tarihli ve 6183 sayılı Amme Alacaklarının Tahsil Usul Hakkında Kanununun 48 inci maddesine gre belirlenen tecil faizi oranında hesaplanacak faiz denir. Ancak mahkeme kararının davacıya teblięi ile banka hesap numarasının idareye bildirildięi tarih arasında geecek sre iin faiz iřlemez.'

16- 72. maddesiyle deęiřtirilen 24.2.1983 gnl, 2802 sayılı Hkimler ve Savcılar Kanunu'nun iptali istenen kuralın da yer aldıęı 'Adalet Bakanlıęı merkez kuruluşuna atama řartları ve řekli ' bařlıklı 37. maddesi řoyledir:

'Adalet Bakanlıęı merkez kuruluşunda:

a) Bakanlık tetkik hâkimliğine, hâkimlik ve savcılık mesleğinde fiilen en az beş yıl görev yapmış ve üstün başarısı ile Bakanlık hizmetlerinde yararlı olacağı anlaşılmış bulunanlar arasında muvafakatlari ile Adalet Bakanı tarafından atama yapılır.

b) 1. Adalet müfettişliğine, hâkimlik ve savcılık mesleğinde fiilen en az beş yıl görev yapmış ve üstün başarısı ile adalet müfettişliği hizmetinde yararlı olacağı anlaşılmış bulunanlar arasında muvafakatlari alınarak,

2. Adalet Bakanlığı Müsteşarlığına, yüksek müşavirliklerine, müsteşar yardımcılıklarına, Teftiş Kurulu Başkanlığına, genel müdürlüklerine, Araştırma, Plânlama ve Koordinasyon Kurulu Başkanlığına, Teftiş Kurulu başkan yardımcılıklarına, Yargıtay ve Danıştay üyeliğine seçilme hakkını kaybetmemiş bulunan birinci sınıf; müstakil daire başkanlıklarına, genel müdür yardımcılıklarına ve İşyurtları Kurumu Daire Başkanlığına ise birinci sınıfa ayrılmış hâkim ve savcılar arasından,

Bakan, Başbakan ve Cumhurbaşkanının imzasını taşıyan müşterek karar ile atama yapılır.

c) (Ek: 2/7/2012-6352/72 md.) Bakanlık iç denetçiliğine, 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanunundaki atama şartlarına tabi olmaksızın, hâkimlik ve savcılık mesleğinde fiilen en az altı yıl görev yapmış ve üstün başarısı ile iç denetim hizmetlerinde yararlı olacağı anlaşılmış bulunanlar arasında, muvafakatlari alınarak, Müsteşarın teklifi üzerine Bakan tarafından atama yapılır. Bu şekilde atananlar İç Denetim Koordinasyon Kurulu tarafından en az iki aylık eğitime tabi tutulur ve eğitim sonunda bunlara kendi idarelerinde geçerli Kamu İç Denetçi Sertifikası verilir.

Genel müdürlük daire başkanlıkları ile Araştırma, Plânlama ve Koordinasyon Kurulu üyeliklerine ise meslekte fiilen en az sekiz yıl çalışmış ve ikinci dereceye yükselmiş bulunan hâkim ve savcılar arasından Bakan onayı ile atama yapılır.

Bakanlık müşavirliklerine yapılacak atamalar Bakan onayı ile gerçekleştirilir.

Bakanlık merkez teşkilâtında olmayıp, yargı görevinden bu görevlere atanacakların muvafakati alınır.

(Ek fıkra: 8/8/2011-KHK-650/18 md.) Bakanlıkta görev yapan hâkim ve savcılarının diğer kanunlar uyarınca Bakanlık dışındaki bir göreve atanabilmeleri Bakanın muvafakatine bağlıdır.'

17- 74. maddesiyle 12.4.1991 günlü, 3713 sayılı Terörle Mücadele Kanunu'nun 'Terör suçlusu' başlıklı 2. maddesinin ikinci fıkrasında yer alan ve iptale konu 've örgüt mensupları gibi cezalandırılırlar' ibaresinin madde metninden çıkarılmış hâli şöyledir:

'Birinci maddede belirlenen amaçlara ulaşmak için meydana getirilmiş örgütlerin mensubu olup da, bu amaçlar doğrultusunda diğerleri ile beraber veya tek başına suç işleyen veya amaçlanan suçu işlemese dahi örgütlerin mensubu olan kişi terör suçlusudur.

Terör örgütüne mensup olmasa dahi örgüt adına suç işleyenler de terör suçlusudur (').'

18- 75. maddesiyle değiştirilen ve iptali istenen 3713 sayılı Kanun'un 'Görev ve yargı çevresinin belirlenmesi, soruşturma ve kovuşturma usulü' başlıklı 10. maddesi şöyledir:

'Bu Kanun kapsamına giren suçlar dolayısıyla açılan davalar; Adalet Bakanlığının teklifi üzerine Hâkimler ve Savcılar Yüksek Kurulunca yargı çevresi birden çok ili kapsayabilecek şekilde belirlenecek illerde görevlendirilecek ağır ceza mahkemelerinde görülür. Bu mahkemelerin başkan ve üyeleri adli yargı adalet komisyonunca, bu mahkemelerden başka mahkemelerde veya işlerde görevlendirilemez.

Anayasa Mahkemesi ve Yargıtayın yargılayacağı kişilere ilişkin hükümler ile askerî mahkemelerin görevlerine ilişkin hükümler saklıdır.

Bu Kanun kapsamına giren suçlarla ilgili olarak;

a) Soruşturma, Hâkimler ve Savcılar Yüksek Kurulunca bu suçların soruşturma ve kovuşturmasında görevlendirilen Cumhuriyet savcılarınca bizzat yapılır. Bu Cumhuriyet savcılarını, Cumhuriyet başsavcılığınca başka mahkemelerde veya işlerde görevlendirilemez.

b) Türk Ceza Kanununun 302, 309, 311, 312, 313, 314, 315 ve 316 ncı maddelerinde düzenlenen suçlar hakkında, görev sırasında veya görevinden dolayı işlenmiş olsa bile Cumhuriyet savcılarınca doğrudan soruşturma yapılır. 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 26 ncı maddesi hükmü saklıdır.

c) Yürütülen soruşturmalarda hâkim tarafından verilmesi gerekli kararları almak, bu kararlara karşı yapılan itirazları incelemek ve sadece bu işlere bakmak üzere yeteri kadar hâkim görevlendirilir.

ç) Ceza Muhakemesi Kanununun 91 inci maddesinin birinci fıkrasındaki yirmidört saat olan gözaltı süresi kırksekiz saat olarak uygulanır.

d) Soruşturmanın amacı tehlikeye düşebilecek ise yakalanan veya gözaltına alınan veya gözaltı süresi uzatılan kişinin durumu hakkında Cumhuriyet savcısının emriyle sadece bir yakınına bilgi verilir.

e) Gözaltındaki şüphelinin müdafii ile görüşme hakkı, Cumhuriyet savcısının istemi üzerine, hâkim kararıyla yirmidört saat süre ile kısıtlanabilir; bu zaman zarfında ifade alınamaz.

f) Kolluk tarafından düzenlenen tutanaklara, ilgili görevlilerin açık kimlikleri yerine sadece sicil numaraları yazılır. Kolluk görevlilerinin ifadesine başvurulması gerektiği hallerde çıkarılan davetiye veya çağrı kâğıdı, kolluk görevlisinin iş adresine tebliğ edilir. Bu kişilere ait ifade ve duruşma tutanaklarında adres olarak iş yeri adresleri gösterilir.

g) Güvenliğin sağlanması bakımından duruşmanın başka bir yerde yapılmasına karar verilebilir.

ğ) Açılan davalara adli tatilde de bakılır.

h) Ceza Muhakemesi Kanununun 135 inci maddesinin altıncı fıkrasının (a) bendinin (8) numaralı alt bendindeki, 139 uncu maddesinin yedinci fıkrasının (a) bendinin (2) numaralı alt bendindeki ve 140 nci maddesinin birinci fıkrasının (a) bendinin (5) numaralı alt bendindeki istisnalar uygulanmaz.

Türk Ceza Kanununda yer alan;

a) Örgüt faaliyeti çerçevesinde işlenen uyuşturucu ve uyarıcı madde imâl ve ticareti suçu veya suçtan kaynaklanan malvarlığı değerini aklama suçu,

b) Haksız ekonomik çıkar sağlamak amacıyla kurulmuş bir örgütün faaliyeti çerçevesinde cebir ve tehdit uygulanarak işlenen suçlar,

c) İkinci Kitap Dördüncü Kısımın Dört, Beş, Altı ve Yedinci Bölümünde tanımlanan suçlar (305, 318, 319, 323, 324, 325 ve 332 nci maddeler hariç),

dolayısıyla açılan davalar, birinci fıkra hükmüne göre görevlendirilen mahkemelerde görülür. Üçüncü fıkranın (d), (e), (f) ve (h) bentleri hariç olmak üzere, bu madde hükümleri, bu suçlardan dolayı yapılan soruşturma ve kovuşturmalarda da uygulanır.

Türk Ceza Kanununun 305, 318, 319, 323, 324, 325 ve 332 nci maddeleri hariç olmak üzere, İkinci Kitap Dördüncü Kısımın Dört, Beş, Altı ve Yedinci Bölümünde tanımlanan suçlarda, Ceza Muhakemesi Kanununda öngörülen tutuklama süresi iki kat olarak uygulanır.

Çocuklar, bu madde hükümleri uyarınca kurulan mahkemelerde yargılanamaz; bu mahkemelere özgü soruşturma ve kovuşturma hükümleri çocuklar bakımından uygulanmaz.'

19- 77. maddesiyle değişik 9.6.2004 günlü, 5187 sayılı Basın Kanunu'nun iptali istenen kuralların da yer aldığı 'Dava süreleri' başlıklı 26. maddesi şöyledir:

'Basılmış eserler yoluyla işlenen veya bu Kanunda öngörülen diğer suçlarla ilgili ceza davalarının bir muhakeme şartı olarak, günlük süreli yayınlar yönünden dört ay, diğer basılmış eserler yönünden altı ay içinde açılması zorunludur.

Bu süreler basılmış eserlerin Cumhuriyet Başsavcılığına teslim edildiği tarihten başlar. Basılmış eserlerin Cumhuriyet Başsavcılığına teslim edilmemesi halinde yukarıdaki sürelerin başlama tarihi, suçu oluşturan fiilin Cumhuriyet Başsavcılığı tarafından öğrenildiği tarihtir. Ancak bu süreler, Türk Ceza Kanununun dava zamanaşımına ilişkin maddesinde öngörülen süreleri aşamaz.

Sorumlu müdürün ve sorumlu müdürün bağlı olduğu yetkilinin karşı çıkmasına rağmen yayımlatıldığı iddia edilen eserden dolayı yayımlatan aleyhine açılacak dava yönünden süre, sorumlu müdür ve sorumlu müdürün bağlı olduğu yetkili hakkında verilecek beraat kararının kesinleşmesinden itibaren başlar.

Sorumlu müdürün yayımlanan eserin sahibini bildirmesi durumunda, eser sahibi aleyhine açılacak davada süre, bildirim tarihinden itibaren başlar.

Kovuşturulması şikâyete bağlı suçlarda dava açma süreleri, suç için kanunun öngördüğü dava zamanaşımı süresini aşmamak şartıyla, suçun işlendiğinin öğrenildiği tarihten başlar.

Kamu davasının açılması izin veya karar alınmasına bağlı olan suçlarda, izin veya karar için gerekli başvurunun yapılmasıyla dava açma süresi durur. Durma süresi dört ayı geçemez.'

20- 85. maddesiyle değiştirilen 26.9.2004 günlü, 5237 sayılı Türk Ceza Kanunu'nun iptali istenen kuralların da yer aldığı 'Suç işlemek amacıyla örgüt kurma' başlıklı 220. maddesi şöyledir:

'(1) Kanunun suç saydığı fiilleri işlemek amacıyla örgüt kuranlar veya yönetenler, örgütün yapısı, sahip bulunduğu üye sayısı ile araç ve gereç bakımından amaç suçları işlemeye elverişli olması halinde, iki yıldan altı yıla kadar hapis cezası ile cezalandırılır. Ancak, örgütün varlığı için üye sayısının en az üç kişi olması gerekir.

(2) Suç işlemek amacıyla kurulmuş olan örgüte üye olanlar, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Örgütün silahlı olması halinde, yukarıdaki fıkralara göre verilecek ceza dörtte birinden yarısına kadar artırılır.

(4) Örgütün faaliyeti çerçevesinde suç işlenmesi halinde, ayrıca bu suçlardan dolayı da cezaya hükmolunur.

(5) Örgüt yöneticileri, örgütün faaliyeti çerçevesinde işlenen bütün suçlardan dolayı ayrıca fail olarak cezalandırılır.

(6) Örgüte üye olmamakla birlikte örgüt adına suç işleyen kişi, ayrıca örgüte üye olmak suçundan da cezalandırılır. Örgüte üye olmak suçundan dolayı verilecek ceza yarısına kadar indirilebilir. (Ek cümle 6459 S.K. 11. madde) Bu fıkra hükmü sadece silahlı örgütler hakkında uygulanır.

(7) Örgüt içindeki hiyerarşik yapıya dahil olmamakla birlikte, örgüte bilerek ve isteyerek yardım eden kişi, örgüt üyesi olarak cezalandırılır. Örgüt üyeliğinden dolayı verilecek ceza, yapılan yardımın niteliğine göre üçte birine kadar indirilebilir.

(8) (6459 S.K. 11. maddesi ile değişik) Örgütün cebir, şiddet veya tehdit içeren yöntemlerini meşru gösterecek veya övecek ya da bu yöntemlere başvurmayı teşvik edecek şekilde propagandasını yapan kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu suçun basın ve yayın yolu ile işlenmesi halinde, verilecek ceza yarı oranında artırılır.'

21- 90. maddesiyle değişik 5237 sayılı Kanun'un iptali istenen 'Yargı görevi yapanı, bilirkişiyi veya tanığı etkilemeye teşebbüs' başlıklı 277. maddesi şöyledir:

'(1) Görülmekte olan bir davada veya yapılmakta olan bir soruşturmada, gerçeğin ortaya çıkmasını engellemek veya bir haksızlık oluşturmak amacıyla, davanın taraflarından birinin, şüpheli veya sanığın, katılanın veya mağdurun lehine veya aleyhine sonuç doğuracak bir karar vermesi veya bir işlem tesis etmesi ya da beyanda bulunması için, yargı görevi yapanı, bilirkişiyi veya tanığı hukuka aykırı olarak etkilemeye teşebbüs eden kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.

(2) Birinci fıkradaki suçu oluşturan fiilin başka bir suçu da oluşturması halinde, fikri içtima hükümlerine göre verilecek ceza yarısına kadar artırılır.'

22- 92. maddesiyle değişik 5237 sayılı Kanun'un iptali istenen 'Gizliliğin ihlali' başlıklı 285. maddesi şöyledir:

'(1) Soruşturmanın gizliliğini alenen ihlal eden kişi, bir yıldan üç yıla kadar hapis veya adli para cezası ile cezalandırılır. Bu suçun oluşabilmesi için;

a) Soruşturma evresinde yapılan işlemin içeriğinin açıklanması suretiyle, suçlu sayılmama karinesinden yararlanma hakkının veya haberleşmenin gizliliğinin ya da özel hayatın gizliliğinin ihlal edilmesi,

b) Soruşturma evresinde yapılan işlemin içeriğine ilişkin olarak yapılan açıklamanın maddi gerçeğin ortaya çıkmasını engellemeye elverişli olması,
gerekir.

(2) Soruşturma evresinde alınan ve soruşturmanın tarafı olan kişilere karşı gizli tutulması gereken kararların ve bunların gereği olarak yapılan işlemlerin gizliliğini ihlal eden kişi, bir yıldan üç yıla kadar hapis veya adli para cezası ile cezalandırılır.

(3) Kanuna göre kapalı yapılması gereken veya kapalı yapılmasına karar verilen duruşmadaki açıklama veya görüntülerin gizliliğini alenen ihlal eden kişi, birinci fıkra hükmüne göre cezalandırılır. Ancak, bu suçun oluşması için, tanığın korunmasına ilişkin olarak alınan gizlilik kararına aykırılık açısından aleniyetin gerçekleşmesi aranmaz.

(4) Yukarıdaki fıkralarda tanımlanan suçların kamu görevlisi tarafından görevinin sağladığı kolaylıktan yararlanılarak işlenmesi halinde, ceza yarısına kadar artırılır.

(5) Soruşturma ve kovuşturma evresinde kişilerin suçlu olarak algılanmalarına yol açacak şekilde görüntülerinin yayınlanması halinde, altı aydan iki yıla kadar hapis cezasına hükmolunur.

(6) Soruşturma ve kovuşturma işlemlerinin haber verme sınırları aşılmaksızın haber konusu yapılması suç oluşturmaz.'

23- 93. maddesiyle değişik 5237 sayılı Kanun'un iptali istenen 'Adil yargılamayı etkilemeye teşebbüs' başlıklı 288. maddesi şöyledir:

'(1) Görülmekte olan bir davada veya yapılmakta olan bir soruşturmada, hukuka aykırı bir karar vermesi veya bir işlem tesis etmesi ya da gerçeğe aykırı beyanda bulunması için, yargı görevi yapanı, bilirkişiyi veya tanığı hukuka aykırı olarak etkilemek amacıyla alenen sözlü veya yazılı beyanda bulunan kişi, elli günden az olmamak üzere adli para cezası ile cezalandırılır.'

24- 95. maddesiyle 4.12.2004 günlü, 5271 sayılı Ceza Muhakemesi Kanunu'na eklenen 'Elektronik işlemler' başlıklı iptali istenen 38/A maddesi şöyledir:

'(1) Her türlü ceza muhakemesi işlemlerinde Ulusal Yargı Ağı Bilişim Sistemi (UYAP) kullanılır. Bu işlemlere ilişkin her türlü veri, bilgi, belge ve karar, UYAP vasıtasıyla işlenir, kaydedilir ve saklanır.

(2) Kanunlarda gösterilen istisnalar hariç olmak üzere, dosyalar güvenli elektronik imza kullanılarak UYAP'tan incelenebilir ve her türlü ceza muhakemesi işlemi yapılabilir.

(3) Bu Kanun kapsamında fiziki olarak hazırlanması öngörülen her türlü belge ve karar elektronik ortamda düzenlenebilir, işlenebilir, saklanabilir ve güvenli elektronik imza ile imzalanabilir.

(4) Güvenli elektronik imza ile imzalanan belge ve kararlar diğer kişi veya kurumlara elektronik ortamda gönderilir. Güvenli elektronik imza ile imzalanarak gönderilen belge veya kararlar, gerekmedikçe fiziki olarak ayrıca düzenlenmez ve ilgili kurum ve kişilere gönderilmez.

(5) Elektronik imzalı belgenin elle atılan imzalı belgeyle çelişmesi halinde UYAP'ta kayıtlı olan güvenli elektronik imzalı belge geçerli kabul edilir.

(6) Güvenli elektronik imza ile imzalanan belge ve kararlarda, mühürleme işlemi ile kanunlarda birden fazla nüshanın düzenlenmesini öngören hükümler uygulanmaz.

(7) Zorunlu nedenlerle fiziki olarak düzenlenmiş belge veya kararlar, yetkili kişilerce taranarak UYAP'a aktarılır ve gerektiğinde ilgili birimlere elektronik ortamda gönderilir.

(8) Elektronik ortamdan fiziki örnek çıkartılması gereken hallerde tutanak veya belgenin aslının aynı olduğu belirtilerek hâkim, Cumhuriyet savcısı veya görevlendirilen yetkili kişi tarafından imzalanır ve mühürlenir.

(9) Elektronik ortamda yapılan işlemlerde süre gün sonunda biter.

(10) Yargı birimlerinin ihtiyaç duyduğu nüfus, tapu, adlî sicil kaydı gibi dış bilişim sistemlerinden UYAP vasıtasıyla temin edilen bilgi, belge ve kayıtlar, zorunlu olmadıkça ayrıca fiziki olarak istenilmez. UYAP'tan dış bilişim sistemlerine gönderilen bilgi ve belgeler ayrıca zorunlu olmadıkça fiziki ortamda gönderilmez.

(11) Ceza muhakemesi işlemlerinin UYAP'ta yapılmasına dair usul ve esaslar, Adalet Bakanlığı tarafından çıkarılacak yönetmelikle düzenlenir.'

25- İptali istenen 105. maddesi şöyledir:

'Aşağıdaki hükümler yürürlükten kaldırılmıştır:

1) 9/6/1932 tarihli ve 2004 sayılı İcra ve İflas Kanununun 12 nci ve 116 ncı maddeleri,

2) 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanununun;

a) 6 ncı maddesinin beşinci fıkrası,

b) 9 ve 13 üncü maddeleri,

3) 4/12/2003 tarihli ve 5015 sayılı Petrol Piyasası Kanununun 19 uncu maddesinin yedinci fıkrası,

4) 9/6/2004 tarihli ve 5187 sayılı Basın Kanununun 19 uncu maddesi,

5) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun;

a) 141 inci maddesinin ikinci fıkrası,

b) 257 nci maddesinin üçüncü fıkrası,

6) 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun 250, 251 ve 252 nci maddeleri,

7) 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununun 128 inci maddesinin birinci fıkrasının birinci cümlesi,

8) 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun 61 inci maddesinin birinci fıkrasının üçüncü cümlesi.'

26- 'Dava ve cezaların ertelenmesi' başlıklı geçici 1. maddesi şöyledir:

'(1) 31/12/2011 tarihine kadar, basın ve yayın yoluyla ya da sair düşünce ve kanaat açıklama yöntemleriyle işlenmiş olup; temel şekli itibarıyla adlî para cezasını ya da üst sınırı beş yıldan fazla olmayan hapis cezasını gerektiren bir suçtan dolayı;

a) Soruşturma evresinde, 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun 171 inci maddesindeki şartlar aranmaksızın kamu davasının açılmasının ertelenmesine,

b) Kovuşturma evresinde, kovuşturmanın ertelenmesine,

c) Kesinleşmiş olan mahkûmiyet hükmünün infazının ertelenmesine,

karar verilir.

(2) Hakkında kamu davasının açılmasının veya kovuşturmanın ertelenmesi kararı verilen kişinin, erteleme kararının verildiği tarihten itibaren üç yıl içinde birinci fıkra kapsamına giren yeni bir suç işlememesi hâlinde, kovuşturmaya yer olmadığı veya düşme kararı verilir. Bu süre zarfında birinci fıkra kapsamına giren yeni bir suç işlenmesi hâlinde, bu suçtan dolayı kesinleşmiş hükümlerle cezaya mahkûm olduğu takdirde, ertelenen soruşturma veya kovuşturmaya devam olunur.

(3) Mahkûmiyet hükmünün infazı ertelenen kişi hakkında bu mahkûmiyete bağlı olarak herhangi bir hak yoksunluğu doğmaz. Ancak bu kişinin, erteleme kararının verildiği tarihten itibaren üç yıl içinde birinci fıkra kapsamına giren yeni bir suç işlemesi hâlinde, bu suçtan dolayı kesinleşmiş hükümlerle cezaya mahkûm olduğu takdirde, ertelenen mahkûmiyet hükmüne bağlı hukuki sonuçlar kişi üzerinde doğar ve ceza infaz olunur.

(4) Bu madde hükümlerine göre cezanın infazının ertelenmesi hâlinde erteleme süresince ceza zamanaşımı durur; kamu davasının açılmasının veya kovuşturmanın ertelenmesi hâlinde, erteleme süresince dava zamanaşımı ve dava süreleri durur.

(5) Birinci fıkra kapsamına giren suçlardan dolayı hükmün açıklanmasının geri bırakılması kararının verilmiş olması hâlinde dahi, bu madde hükümleri uygulanır.

(6) Birinci fıkra kapsamına giren suçlardan dolayı verilmiş mahkûmiyet hükmünün infazının tamamlanmış olması hâlinde bu mahkûmiyet hükmüne bağlı yasaklanmış hakların 25/5/2005 tarihli

ve 5352 sayılı Adli Sicil Kanununun 13/A maddesindeki şartlar aranmaksızın geri verilmesine karar verilir.

(7) Bu madde hükümlerine göre verilen kamu davasının açılmasının, kovuşturmanın veya cezanın infazının ertelenmesi kararları adli sicilde bunlara mahsus bir sisteme kaydedilir. Bu kayıtlar, ancak bir soruşturma veya kovuşturmayla bağlantılı olarak Cumhuriyet savcısı, hâkim veya mahkeme tarafından istenmesi hâlinde, bu maddede belirtilen amaç için kullanılabilir.

(8) Bu madde hükümlerine göre kamu davasının açılmasının, kovuşturmanın veya cezanın infazının ertelenmesi kararlarının verildiği hâllerde, bu suçlar 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun erteleme ve tekrüre ilişkin hükümlerinin uygulanmasında göz önünde bulundurulmaz.'

27- İptali istenen kuralların da yer aldığı geçici 2. maddesi şöyledir:

'(1) Bu Kanunda yapılan değişiklikler karşısında; ilgili suçlardan dolayı açılan ve temyiz aşamasında bulunan dava dosyalarından Yargıtay Cumhuriyet Başsavcılığında bulunanlar, Yargıtay Cumhuriyet Başsavcılığınca; Yargıtay ilgili dairesinde bulunan dosyalar ise bu dairece, hükmü veren mahkemeye gönderilir.

(2) Abonelik esasına göre yararlanılabilen elektrik enerjisinin, suyun ve doğal gazın sahibinin rızası olmaksızın ve tüketim miktarının belirlenmesini engelleyecek şekilde tüketilmesi dolayısıyla bu Kanunun yürürlüğe girdiği tarih itibarıyla hakkında hırsızlık suçundan dolayı kovuşturma yapılan veya kesinleşmiş olup olmadığına bakılmaksızın hakkında hüküm verilen kişinin, bu Kanun yürürlüğe girdiği tarihten itibaren altı ay içinde, zararı tamamen tazmin etmesi hâlinde, hakkında cezaya hükmolunmaz, verilen ceza tüm sonuçlarıyla ortadan kalkar.

(3) Bu maddenin yürürlüğe girdiği tarih itibarıyla koşullu salıverilmelerine bir yıldan az süre kalan ve açık ceza infaz kurumunda bulunan iyi hallî hükümlülerin talepleri hâlinde, cezalarının koşullu salıverilme tarihine kadar olan kısmının denetimli serbestlik tedbiri uygulanmak suretiyle infazına karar verilebilir.

(4) Ceza Muhakemesi Kanununun yürürlükten kaldırılan 250 nci maddesinin birinci fıkrasına göre görevlendirilen mahkemelerde açılmış olan davalara, kesin hükümle sonuçlandırılıncaya kadar bu mahkemelerce bakmaya devam olunur. Bu davalarda, yetkisizlik veya görevsizlik kararı verilemez. 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanununun 10 uncu maddesinin kovuşturmayla ilişkin hükümleri bu davalarda da uygulanır.

(5) Ceza Muhakemesi Kanununun 251 inci maddesinin birinci fıkrasına göre görevlendirilen Cumhuriyet savcıları yürütmekte oldukları soruşturmalara, Hâkimler ve Savcılar Yüksek Kurulunca Terörle Mücadele Kanununun 10 uncu maddesi uyarınca görevlendirilen Cumhuriyet savcıları göreve başlayıncaya kadar devam ederler.

(6) Terörle Mücadele Kanununun 10 uncu maddesi kapsamına giren suçlarla ilgili olarak bu maddenin yürürlüğe girdiği tarih itibarıyla açılmış olan davalarda, sanığın taşıdığı kamu görevlisi sıfatı dolayısıyla hakkında soruşturma yapılabilmesi için izin veya karar alınması gerektiğinden bahisle durma veya düşme kararı verilemez.

(7) Mevzuatta Ceza Muhakemesi Kanununun 250 nci maddesinin birinci fıkrasına göre kurulan ağır ceza mahkemelerine yapılmış olan atıflar, Terörle Mücadele Kanununun 10 uncu maddesinin birinci fıkrasında belirtilen ağır ceza mahkemelerine yapılmış sayılır.'

28- İptali istenen Geçici 3. maddesi şöyledir:

'(1) 12 Eylül 1980 tarihinden önce işlenmiş olan suçlardan dolayı lehe Kanun, 1/3/1926 tarihli ve 765 sayılı Türk Ceza Kanununun cezaların ıçtimaina ilişkin hükümleri uygulandıktan sonra ortaya çıkan sonuç ceza göz önünde bulundurularak belirlenir. Belirlenen bu ceza infaz bakımından lehe hükümler içeren kanuna göre infaz edilir.

(2) Terör suçları, örgüt faaliyeti kapsamında işlenen suçlar ile cinsel dokunulmazlığa karşı işlenen suçlar hariç olmak üzere;

a) Kasıtlı suçlardan toplam üç yıl veya daha az hapis cezasına mahkûm olanların,

b) Taksirli suçlardan toplam beş yıl veya daha az süreyle hapis cezasına mahkûm olanların,

c) Adli para cezasının infazı sürecinde tazyik hapsine tabi tutulanların,

cezaları doğrudan açık ceza infaz kurumlarında yerine getirilir. Bu fıkra hükümleri 31/12/2017 tarihine kadar uygulanır.'

B- Dayanılan Anayasa Kuralları

Dava dilekçesinde, Anayasa'nın Başlangıç'ı ile 2., 4., 5., 6., 7., 8., 9., 10., 11., 12., 13., 17., 20., 36., 37., 38., 40., 87., 90., 125., 128., 138., 139., 140. ve 153. maddelerine dayanılmıştır.

III- İLK İNCELEME

Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca, Haşim KILIÇ, Serruh KALELİ, Alparslan ALTAN, Fulya KANTARCIOĞLU, Mehmet ERTEN, Serdar ÖZGÜLDÜR, Osman Alifeyyaz

PAKSÜT, Zehra Ayla PERKTAŞ, Recep KÖMÜRCÜ, Burhan ÜSTÜN, Engin YILDIRIM, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Erdal TERCAN ve Muammer TOPAL'ın katılmalarıyla 8.11.2012 günü yapılan ilk inceleme toplantısında öncelikle dava konusu kuralların bazılarına yönelik olarak iptal davasının açılmış sayılıp sayılmayacağı ile şekil yönünden Anayasa'ya aykırılığı ileri sürülen Kanun'un geçici 3. maddesine yönelik iptal başvurusunun süresinde yapıp yapılmadığı sorunu görüşülmüştür.

6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 38. maddesinin (6) numaralı fıkrasında, 'İptal davalarında, Anayasaya aykırılıkları ileri sürülen hükümlerin Anayasanın hangi maddelerine aykırı olduğunun ve gerekçelerinin belirtilmiş olması zorunludur.' kuralına yer verilmiş, Anayasa Mahkemesi İçtüzüğü'nün 45. maddesinde ise 'Anayasaya aykırılıkları ileri sürülen hükümlerin her birinin Anayasanın hangi maddelerine, hangi nedenlerle aykırı olduğunun ayrı ayrı ve gerekçeleriyle birlikte açıkça gösterilmesi' ve 'Yürürlüğü durdurma talebi varsa yürürlüğün durdurulmaması durumundaki doğacak telafisi imkânsız zararların açıklanması' iptal davası başvuru dilekçesinde yer alması gereken hususlar arasında sayılmıştır.

6216 sayılı Kanun'un 39. maddesi ile İçtüzüğü'nün 49. maddesinde, dava dilekçesinde eksikliklerin bulunması hâlinde, bu hususun kararla saptanarak onbeş günden az olmamak üzere verilecek süre içinde tamamlanması için ilgililere tebliğ olunacağı ve belirtilen süre içinde eksikliklerin tamamlanmaması hâlinde Genel Kurulca iptal davasının açılmamış sayılmasına karar verileceği hükme bağlanmıştır.

Dava dilekçesinde, iptali istenen kuralların bir kısmına yönelik olarak Anayasa'ya aykırılık gerekçelerine ve yürürlüğün durdurulmaması durumundaki doğacak telafisi imkânsız zararların açıklanmasına ilişkin gerekçelere yer verilmediği anlaşıldığından, 6216 sayılı Kanun'un 39. maddesinin (1) numaralı fıkrası ile İçtüzüğü'nün 49. maddesi uyarınca Ankara Milletvekili Emine Ülker TARHAN ile Uşak Milletvekili Dilek AKAGÜN YILMAZ'a bildirimde bulunulmasına ve söz konusu eksikliklerin giderilmesi için kararın tebliğinden başlayarak 15 (onbeş) gün süre verilmesine karar verilmiştir. İlgililer tarafından kararda belirlenen süre içinde 23.10.2012 gününde verilen dilekçede yürürlüğün durdurulmasına ilişkin gerekçe eksikliği giderilmiş ancak kuralların Anayasa'ya aykırılık gerekçesine ilişkin eksiklik giderilmemiş olduğundan, söz konusu kurallara yönelik iptal davasının açılmamış sayılmasına karar vermek gerekmiştir.

Diğer taraftan, dava dilekçesinde 6352 sayılı Kanun'un geçici 3. maddesinin Anayasa'ya esas bakımından aykırı olduğunun ileri sürülmesinin yanında, düzenlemenin özel af yasası niteliği

taşıdığı ve Anayasa'nın 87. maddesinin birinci fıkrası uyarınca nitelikli çoğunlukla kabul edilmesi gerektiği yönünden şekil bakımından da Anayasa'ya aykırılığı ileri sürülmüştür.

Anayasa'nın 148. maddesinin ikinci fıkrası ile 6216 sayılı Kanun'un 37. maddesinin (1) numaralı fıkrasında, kanunların, Resmî Gazete'de yayımlanmalarından başlayarak on gün geçtikten sonra bunların şekil yönünden Anayasa'ya aykırılıkları iddiası ile iptal davası açılmayacağı belirtilmiştir.

6352 sayılı Kanun, 5.7.2012 günlü, 28344 sayılı Resmî Gazete'de yayımlanmış, iptal davası ise 3.9.2012 gününde açılmıştır. Bu durumda, bu maddenin şekil bakımından Anayasa'ya aykırı olduğuna ilişkin başvuru, süresi içinde yapılmadığından, bu maddenin şekil bakımından Anayasa'ya aykırılığına ilişkin iptal isteminin reddedilmesi gerekmiştir.

Açıklanan nedenlerle, 2.7.2012 günlü, 6352 sayılı Yargı Hizmetlerinin Etkinleştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılması ve Basın Yayın Yoluyla İşlenen Suçlara İlişkin Dava ve Cezaların Ertelenmesi Hakkında Kanun'un:

A) 1- 28. maddesiyle değiştirilen, 9.6.1932 günlü, 2004 sayılı İcra ve İflas Kanunu'nun 124. maddesinin üçüncü fıkrasının, "elektronik ortamda teklif vererek artırmaya katılacakların teminat göstermeleri gerektiği ve elektronik ortamda teklif vermeye ilişkin hususlar yazılır." ibaresi dışında kalan bölümüne,

2- 47. maddesiyle değiştirilen, 6.1.1982 günlü, 2575 sayılı Danıştay Kanunu'nun 61. maddesinin (1) numaralı fıkrasının üçüncü cümlesine,

3- 57. maddesiyle, 6.1.1982 günlü, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 27. maddesinin değiştirilen (2) numaralı fıkrasının birinci cümlesinin "davalı idarenin savunması alındıktan veya savunma süresi geçtikten sonra" ibaresi dışında kalan bölümü ile üçüncü ve dördüncü cümlelerine,

4- 58. maddesiyle değiştirilen, 2577 sayılı Kanun'un 28. maddesinin (6) numaralı fıkrasının birinci cümlesine,

5- 72. maddesiyle, 24.2.1983 günlü, 2802 sayılı Hâkimler ve Savcılar Kanunu'nun 37. maddesinin birinci fıkrasına eklenen (c) bendinin "üstün başarısı ile iç denetim hizmetlerinde yararlı olacağı anlaşılmış bulunanlar arasından'Müsteşarın teklifi üzerine Bakan tarafından atama yapılır." ibareleri dışında kalan bölümüne,

6- 74. maddesiyle, 12.4.1991 günlü, 3713 sayılı Terörle Mücadele Kanunu'nun 2. maddesinin ikinci fıkrasında yer alan 've örgüt mensupları gibi cezalandırılırlar' ibaresinin madde metninden çıkarılmasına,

7- 92. maddesiyle deęiřtirilen, 26.9.2004 gnl, 5237 sayılı Trk Ceza Kanunu'nun 285. maddesinin (3) ve (4) numaralı fıkralarına,

8- 105. maddesinin, (2) numaralı fıkrasının (b) bendinde yer alan "13 nc" ibaresi dıřında kalan maddenin tmne,

9- Geici 2. maddesinin (5) ve (7) numaralı fıkralarına,

10- Geici 3. maddesinin (2) numaralı fıkrasına,

iliřkin iptal davasının, 6216 sayılı Anayasa Mahkemesinin Kuruluđu ve Yargılama Usulleri Hakkında Kanun'un 39. maddesinin (3) numaralı fıkrası uyarınca AILMAMIŐ SAYILMASINA,

B) Geici 3. maddesinin Őekil bakımından Anayasa'ya aykırı olduęuna ve bu ynden iptaline iliřkin bařvurunun sre ařımı nedeniyle REDDİNE,

C) 1- 1. maddesiyle, 9.6.1932 gnl, 2004 sayılı İcra ve İflas Kanunu'nun bařlıęı ile birlikte deęiřtirilen 1. maddesinin beřinci fıkrasının,

2- 3. maddesiyle, 2004 sayılı Kanun'a eklenen 8/a maddesinin ikinci fıkrasının,

3- 21. maddesiyle deęiřtirilen 2004 sayılı Kanun'un 106. maddesinin birinci fıkrasının,

4- 22. maddesiyle deęiřtirilen 2004 sayılı Kanun'un 110. maddesinin birinci fıkrasının,

5- 24. maddesiyle, 2004 sayılı Kanun'un 114. maddesine eklenen drdnc fıkranın 'Aık artırmaya elektronik ortamdan teklif verme yoluyla bařlanır.' biimindeki birinci cmlesinin,

6- 25. maddesiyle 2004 sayılı Kanun'un bařlıęı ile birlikte deęiřtirilen 115. maddesinin,

7- 28. maddesiyle deęiřtirilen 2004 sayılı Kanun'un 124. maddesinin nc fıkrasının, "elektronik ortamda teklif vererek artırmaya katılacakların teminat gstermeleri gerektięi ve elektronik ortamda teklif vermeye iliřkin hususlar yazılır.' ibaresinin,

8- 29. maddesiyle 2004 sayılı Kanun'un bařlıęı ile birlikte deęiřtirilen 126. maddesinin drdnc fıkrasının,

9- 31. maddesiyle deęiřtirilen 2004 sayılı Kanun'un 129. maddesinin,

10- 44. maddesiyle, 6.1.1982 gnl, 2575 sayılı Danıřtay Kanunu'nun 8. maddesinin;

1- (1) numaralı fıkrasının,

a- (d) bendine eklenen 'Trkiye Byk Millet Meclisi Genel Sekreterlięi,' ibaresinin,

b- (e) bendine eklenen 'ile dzenleyici ve denetleyici kurumların bařkanlıkları,' ibaresinin,

c- Deęiřtirilen (g) bendinin,

2- (3) numaralı fıkrasındaki deęiřtirilen 'onbeř yıl' ibaresinin,

11- 45. maddesiyle deęiřtirilen 2575 sayılı Kanun'un 24. maddesinin (1) numaralı fıkrasının (c) bendinin,

12- 46. maddesiyle deęiřtirilen 2575 sayılı Kanun'un 60. maddesinin (1) numaralı fıkrasının,

13- 47. maddesiyle deęiřtirilen 2575 sayılı Kanun'un 61. maddesinin, (1) numaralı fıkrasının birinci ve ikinci cümleleri ile (3) numaralı fıkrasının,

14- 57. maddesiyle;

a- 2577 sayılı Kanun'un 27. maddesinin deęiřtirilen (2) numaralı fıkrasının, birinci cümlesinde yer alan "davalı idarenin savunması alındıktan veya savunma süresi geçtikten sonra" ibaresi ile ikinci cümlesinin,

b- 2577 sayılı Kanun'un 27. maddesine eklenen (3) ve (10) numaralı fıkraların,

15- 58. maddesiyle deęiřtirilen 2577 sayılı Kanun'un 28. maddesinin (2) numaralı fıkrası ile (6) numaralı fıkrasının ikinci cümlesinin,

16- 72. maddesiyle 2802 sayılı Kanun'un 37. maddesinin birinci fıkrasına eklenen (c) bendinde yer alan " üstün başarısı ile iç denetim hizmetlerinde yararlı olacağı anlaşılmıř bulunanlar arasından 'Müsteřarın teklifi üzerine Bakan tarafından atama yapılır.' ibarelerinin,

17- 75. maddesiyle 3713 sayılı Kanun'un bařlıęı ile birlikte deęiřtirilen 10. maddesinin,

18- 77. maddesiyle, 9.6.2004 günlü, 5187 sayılı Basın Kanunu'nun 26. maddesinin birinci ve altıncı fıkralarında yapılan deęiřikliklerin,

19- 85. maddesiyle deęiřtirilen, 26.9.2004 günlü, 5237 sayılı Türk Ceza Kanunu'nun 220. maddesinin (6) ve (7) numaralı fıkralarının,

20- 90. maddesiyle 5237 sayılı Kanun'un bařlıęı ile birlikte deęiřtirilen 277. maddesinin,

21- 92. maddesiyle deęiřtirilen 5237 sayılı Kanun'un 285. maddesinin (1), (2), (5) ve (6) numaralı fıkralarının,

22- 93. maddesiyle deęiřtirilen 5237 sayılı Kanun'un 288. maddesinin,

23- 95. maddesiyle, 4.12.2004 günlü, 5271 sayılı Ceza Muhakemesi Kanunu'na eklenen 38/A maddesinin,

24- 105. maddesinin (2) numaralı fıkrasının (b) bendinde yer alan "13 üncü" ibaresinin,

25- Geçici 1. maddesinin,

26- Geçici 2. maddesinin (4) ve (6) numaralı fıkralarının,

27- Geçici 3. maddesinin (1) numaralı fıkrasının,

dosyada eksiklik bulmadığından esasının incelenmesine, yürürlüklerinin durdurulması isteminin esas inceleme aşamasında karara bağlanmasına, OYBİRLİĞİYLE karar verilmiştir.

IV- ESASIN İNCELENMESİ

Dava dilekçesi ve ekleri, Raportör Hamit YELKEN tarafından hazırlanan işin esasına ilişkin rapor, dava konusu yasa kuralları, dayanan ve ilgili görülen Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A) Kanun'un 1. Maddesiyle Değiştirilen 2004 Sayılı Kanun'un 1. Maddesinin Beşinci Fıkrasının İncelenmesi

Dava dilekçesinde, Anayasa'nın 128. maddesinin ikinci fıkrası uyarınca memurların özlük haklarının kanunla düzenlenmesi gerektiği hâlde memur olan icra müdür ve icra müdür yardımcıları ile icra kâtiplerinin özlük haklarının düzenlenmesinin dava konusu kuralla yönetmeliğe bırakıldığı belirtilerek kuralın, Anayasa'nın 128. maddesine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralda, icra müdür ve icra müdür yardımcıları ile icra kâtiplerine ilişkin yazılı sınav, sözlü sınav, görevlendirme, nakil, unvan değişikliği, görevde yükselme ve diğer hususların yönetmelikle düzenleneceği belirtilmiştir.

Anayasa'nın 128. maddesinin ikinci fıkrasına göre, memurların ve diğer kamu görevlilerinin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülükleri, aylık ve ödenekleri ve diğer özlük işlerinin kanunla düzenlenmesi gerekmektedir. Kanun ile düzenlenmesi öngörülen konularda, yürütme organına, genel, sınırsız, esasları ve çerçevesi belirsiz bir düzenleme yetkisi verilmez. Ancak kanunda temel esasların belirlenerek çerçevesinin çizilmiş olması koşuluyla uzmanlık ve teknik konulara ilişkin hususların düzenlenmesinin yürütme organına bırakılması, Anayasa'nın 128. maddesine aykırılık oluşturmaz.

Dava dilekçesinde de belirtildiği gibi memur olan icra müdürü ve icra müdür yardımcıları ile icra kâtipleri esasen 657 sayılı Devlet Memurları Kanunu'na tabi olduklarından, bunlar açısından da kanunla düzenlenme şartı, anılan Kanun'da ve memurlara ilişkin diğer yasal düzenlemelerde ayrıntılı olarak yerine getirilmiş durumdadır.

Diğer taraftan, dava konusu fıkrada yönetmelikle düzenleneceği belirtilen yazılı ve sözlü sınavın esasları, 2004 sayılı Kanun'un 1. maddesinin üçüncü ve dördüncü fıkralarında; görevlendirme, nakil, unvan değişikliği ve görevde yükselmeye ilişkin esaslar ise bu madde yanında 657 sayılı Kanun'da belirlenmiş bulunmaktadır.

Dava konusu kural ise, 2004 sayılı Kanun'un 1. maddesi ve 657 sayılı Kanun'un ilgili maddeleri ile esasları belirlenerek yasal çerçevesi çizilmiş bulunan hususlarda yönetmelikle düzenleme yapılmasını öngörmektedir.

Kanun koyucunun dava konusu kuralla düzenlenmesi yönetmeliğe bırakılan hususlarda belirtilen kanun hükümleri ile temel kuralları belirleyip yasal çerçeveyi çizdikten sonra, bu çerçevenin içinde kalacak ve değişen koşullara göre farklılık gösterebilecek uzmanlık ve idare tekniğine ilişkin ayrıntıların düzenlenmesini yürütmeye bırakmasında, Anayasa'nın 128. maddelerine aykırı bir yön bulunmamaktadır. İptal isteminin reddi gerekir.

Mehmet ERTEN ile Zehra Ayla PERKTAŞ bu görüşe katılmamışlardır.

B- Kanun'un 3. Maddesiyle 2004 Sayılı Kanun'a Eklenen 8/a Maddesinin İkinci Fıkrasının İncelenmesi

Dava dilekçesinde, dava konusu kuralla güvenli elektronik imza ile oluşturulan elektronik verilerin senet hükmünde kabul edildiği ve elektronik imzanın elle atılan imza ile aynı ispat gücünü haiz kılındığı belirtilerek, elektronik ortamdaki bazı bilgilerin kötü niyetli kişiler tarafından elde edilebileceği ve kullanılabilmesi, ıslak imzanın ise bir başkası tarafından atılmasının mümkün olmadığı, bu nedenle elektronik imza ve verilere bu kadar büyük bir işlev yükleyen söz konusu kuralın, Anayasa'nın 20. maddesinin üçüncü fıkrasında yer alan kişisel verilerin korunmasını isteme hakkına aykırılık teşkil ettiği ileri sürülmüştür.

Dava konusu kuralda, usulüne göre güvenli elektronik imza ile oluşturulan elektronik verilerin senet hükmünde olacağı, güvenli elektronik imzanın elle atılan imza ile aynı ispat gücünü haiz olacağı, güvenli elektronik imzanın kanunlarda güvenli elektronik imza ile yapılamayacağı açıkça belirtilmiş olan işlemler dışında elle atılan imza yerine kullanılabilmesi ve güvenli elektronik imzayla oluşturulan belge ve kararlarda, kanunlarda birden fazla nüshanın düzenlenmesi ve mühürleme işlemini öngören hükümlerin uygulanmayacağı düzenlenmektedir.

Anayasa'nın 20. maddesinin üçüncü fıkrasının birinci cümlesinde 'Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir.' hükmüne yer verilerek kişisel verilerin korunması hakkı anayasal güvenceye bağlanmıştır.

Dava konusu kuralda, elektronik imzanın hukuki bağlayıcılığı düzenlenerek ve bu yöntemle işlem yapılması ile bağdaşmayan bazı hükümler kaldırılarak, ulusal yargı ağı projesiyle (UYAP) tüm yargı birimlerinde uygulanmaya başlanan elektronik ortamda işlem yapma kolaylığının, icra iflas işlemlerinde de uygulanması amaçlanmaktadır.

Elektronik imza yönteminde, izin verilmeyen kişilerin belgeye ulaşabilmesini engelleyen 'erişim kontrolü fonksiyonu'nun bulunması nedeniyle, kişisel veri niteliği bulunabilecek elektronik imzalı belgelere başkalarının erişmesi önlenmektedir. Dolayısıyla, kuralın, Anayasa'nın 20. maddesinde belirtilen kişisel verilerin korunmasını isteme hakkına aykırılık oluşturacak bir müdahaleye zemin hazırlaması ya da bu hakkı sınırlandırması söz konusu değildir.

Diğer taraftan, Anayasa'nın 7. maddesi uyarınca, Anayasa'da belirtilen istisnalar dışında ve Anayasa'ya aykırı olmamak kaydıyla yasama organı istediği alanda ve istediği içerikte kanun çıkarma yetkisine sahiptir. Anayasa'da, dava konusu kuralla getirilen elektronik imzaya ilişkin düzenlemeleri yasaklayan ya da sınırlandıran bir hüküm bulunmamaktadır. Bu durumda, kanun koyucunun yasamanın genelliği ilkesi uyarınca iptali istenen kuralla getirdiği elektronik imzaya ilişkin düzenlemelerin, Anayasa'nın 20. maddesine aykırı bir yönünün bulunmadığı açıktır.

Kuralın elektronik ortamda icra iflas işlemlerinin yapılabilmesi kolaylığını sağlamasına karşın elektronik imzanın kötü niyetli kişiler tarafından ele geçirilebileceği ve kullanılabileceği, oysa ıslak imzanın başkası tarafından atılmasının veya kötüye kullanılmasının mümkün olmadığı ve bu yönüyle elektronik imzayla yapılan işlemlerin fiziki ortamda yapılan işlemlere nazaran daha güvensiz olduğu da söylenemez. Zira, bilimsel çevrelerde elektronik imzanın, ıslak imzanın işlevini aynen icra etmenin yanında hukuki işlemlerde güvenlik ve istikrarı korumak üzere daha üstün özelliklere sahip olduğu kabul edilmektedir.

Esasen güvenlik problemlerinin varlığı hem fiziki ortam hem de elektronik ortamda gerçekleştirilen işlemler için her zaman mümkün olup hangi ortamdaki işlemlerin daha güvenli olacağı hususu subjektif ve teknik bir değerlendirmeyi gerektirmekte, elektronik ortamdaki işlemlere hukuki geçerlilik sağlamanın doğru olup olmayacağı, bu tür konularda mevcut seçenekler arasında hangisinin tercih edileceği ve hangi tercihin daha güvenli ve yararlı sonuçlar doğuracağı hususu ise kanun koyucunun takdirinde kalmaktadır.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 20. maddesine aykırı değildir. İptal isteminin reddi gerekir.

C- Kanun'un 21. Maddesiyle Değiştirilen 2004 Sayılı Kanun'un 106. Maddesinin Birinci Fıkrasının İncelenmesi

Dava dilekçesinde, dava konusu kuralla, hacizli mallara ilişkin satış talebinde bulunma süresinin kısaltıldığı belirtilerek, bu süreler içinde satış işlemlerinin yapılmasının mümkün olmadığı, bu haliyle alacaklıların haklarına kavuşmasını engelleyecek ve gereksiz yere masraf yapılmasına neden olabilecek kuralın, Anayasa'nın 36. maddesinde belirtilen hak arama özgürlüğü ve 40. maddesinde belirtilen temel hak ve hürriyetlerin korunması ilkelerine aykırılık teşkil ettiği ileri sürülmüştür.

Dava konusu kuralda, icra takiplerinde hacizli malların satışı için alacaklıya tanınan satış talebinde bulunma süresi yeniden düzenlenmekte ve taşınır mallar için bir yıl olarak belirlenen süre altı aya ve taşınmaz mallar için iki yıl olarak belirlenen süre bir yıla düşürülmektedir.

Anayasa'nın 36. maddesinin birinci fıkrasında, 'Herkes, meşru vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı ve davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir.' hükmüne yer verilmiştir. Maddeyle güvence altına alınan hak arama özgürlüğü ve adil yargılanma hakkı, kendisi bir temel hak niteliği taşımasının yanında, diğer temel hak ve özgürlüklerden gereken şekilde yararlanılmasını ve bunların korunmasını sağlayan en etkili güvencelerden biridir.

Dava konusu kuralla hacizli malların satışı için alacaklıya tanınan satış talebinde bulunma süreleri yarıya indirilerek borçlunun malı üzerindeki tasarruf yetkisinin uzun süre sürüncemede kalması önlenmekte ve icra dairelerinin daha hızlı ve etkin bir şekilde çalışması imkânı getirilerek alacağın daha kısa sürede tahsil edilmesi amaçlanmaktadır.

Kural uyarınca hacizli bir malın satışı için gerekli olan şartların hazırlanmamış olması satış talebinde bulunmayı önlememekte ve bir kere satış talebinde bulunulduktan sonra malın satışı için gerekli şartların tamamlanması veya satışın gerçekleşmesi, kuralda belirtilen sürelerle tabi olmamaktadır. Dolayısıyla, dava dilekçesinde ileri sürüldüğü üzere, satış için gerekli hazırlıkların tamamlanamamasının satış talebinde bulunmaya herhangi bir etkisi bulunmadığı gibi bu sebeple satış talebinde bulunma süresinin geçirilmesi de söz konusu değildir. Bu nedenle kuralla kişilerin hak arama özgürlüklerinin sınırlandırıldığından söz edilemez.

Açıklanan nedenlerle, dava konusu kural, Anayasa'nın 36. maddesine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın Anayasa'nın 40. maddesiyle ilgisi görülmemiştir.

Ç- Kanun'un 22. Maddesiyle Değiştirilen 2004 Sayılı Kanun'un 110. Maddesinin Birinci Fıkrasının İncelenmesi

Dava dilekçesinde, dava konusu kuralla yapılan düzenlemenin sulh ve anlaşmaları engelleyici nitelikte olduğu ve alacaklının alacağını alamaması sonucunu doğurabileceği belirtilerek kuralın, Anayasa'nın 36. ve 40. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralda, mal üzerindeki haczin kaldırılmasını gerektiren hâller ile satış talebinin geri alınmasının hüküm ve sonuçları düzenlenmektedir.

Borçlunun malı üzerindeki mülkiyet ve tasarruf hakkını sınırlayan ve alacaklının alacağına kavuşmasına yönelik haciz işleminin süresiz olarak devam etmesi hukuki belirlilik ve istikrar ilkelerinin temeli olan hukuk devletinde kabul edilemez. Bu nedenle, borçlunun malı üzerindeki tasarruf yetkisini sınırlayan tüm işlemler gibi haciz işleminin de hangi koşullarda uygulanabileceğinin, bu işlemin nasıl gerçekleştirileceğinin ve bu işlemin hangi şartlarda kalkacağına herhangi bir duraksamaya yer verilmeksizin açık bir şekilde önceden kurala bağlanması gerekir. Ancak, mal üzerine haciz konulması ve haczin devam etmesi için belirlenen şartlar alacaklı tarafından yerine getirilmesi mümkün olmayan ya da alacaklıdan ifa etmesi beklenemeyecek derecede ağır şartlar ise o zaman söz konusu şartların hak arama özgürlüğünü sınırladığından bahsedilebilir.

Dava konusu kuralda, mal üzerindeki haczin hangi şartlarda kalkacağı açık bir şekilde belirtilmiştir. Buna göre, kanunda belirtilen süre içerisinde satış talebinde bulunulmaması veya satış talebinde bulunulduğu halde bu talepten itibaren onbeş gün içinde satış masraflarının yatırılmaması ya da satış talebinin geri alınıp bu talebin yenilenmemesi hâllerinde mal üzerindeki haciz kalkacaktır. Anlaşılacağı üzere bu şartların hiçbiri alacaklı tarafından yerine getirilmesi mümkün olmayan veya alacaklıdan ifa etmesi beklenemeyecek derecede ağır şartlar değildir. Dolayısıyla, mal üzerindeki haczin kaldırılmasını düzenleyen bu şartların hak arama özgürlüğünü sınırlayan bir yönünün bulunduğu söylenemez.

Öte yandan, kuralda, alacaklının satış talebini ancak bir kez geri alabileceği hükmüne yer verilmiştir. Bu hüküm, hiçbir şekilde alacaklının satıştan vazgeçme hakkını ortadan kaldırmamakta, ancak alacaklının yeniden satış isteme hakkını yitirmeksizin sadece bir kez satış talebini geri alabileceğini düzenlemektedir. Diğer bir ifadeyle, kuralla bir kez satış talebinde bulunduktan sonra satış talebini geri alan ve yeniden satış talebinde bulunan alacaklının satıştan tekrar vazgeçmesi değil, sadece yeniden satış talebinde bulunması yasaklanmaktadır. Dolayısıyla, dava dilekçesinde belirtildiğinin aksine bu hükmün alacaklının satış talebinden vazgeçmesi yönündeki iradesine rağmen hacizli malın

satışını zorunlu hâle getirmesi ve alacaklı ile borçlu arasında meydana gelebilecek olası anlaşmayı önlemesi söz konusu değildir.

Esas itibariyle kuralla bir taraftan satış talebinin geri alınması hakkı tanınarak anlaşma ve benzeri sebeplerle alacaklıya hacizli malların satışını önleme yetkisi verilirken, diğer taraftan bu yetkinin kullanılması bir defa ile sınırlandırılarak bu hakkın kötüye kullanılmasının ve icra dairelerinin gereksiz yere işlerinin artırılmasının önlenmeye çalışıldığı anlaşılmaktadır.

Açıklanan nedenlerle, dava konusu kural, Anayasa'nın 36. maddesine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 40. maddesiyle ilgisi görülmemiştir.

D- Kanun'un 24. Maddesiyle 2004 Sayılı Kanun'un 114. Maddesine Eklenen Dördüncü Fıkranın 'Açık artırmaya elektronik ortamdan teklif verme yoluyla başlanır.' Biçimindeki Birinci Cümlesinin, 25. Maddesiyle 2004 Sayılı Kanun'un Başlığı İle Birlikte Değiştirilen 115. Maddesinin, 28. Maddesiyle Değiştirilen 2004 Sayılı Kanun'un 124. Maddesinin Üçüncü Fıkrasında Yer Alan "elektronik ortamda teklif vererek artırmaya katılacakların teminat göstermeleri gerektiği ve elektronik ortamda teklif vermeye ilişkin hususlar yazılır.' İbaresinin, 29. Maddesiyle 2004 Sayılı Kanun'un Başlığı ile Birlikte Değiştirilen 126. Maddesinin Dördüncü Fıkrasının ve 31. Maddesiyle Değiştirilen 2004 Sayılı Kanun'un 129. Maddesinin İncelenmesi

Dava dilekçesinde, elektronik ortamda ihaleye katılma imkânını tanıyan dava konusu kuralların, ihalenin herkesin tatmin olacağı bir şekilde hiçbir kuşkuya yer bırakmayacak koşullarda aleni ve açık şekilde yapılması ilkelerini zedeleyebileceği gibi adalete olan güveni sarsabileceği ve ihaleye fesat karıştırma iddialarını artırabileceği, öte yandan elektronik ortamdaki verilerin her zaman bozulabileceği ya da bunlara dışarıdan müdahale edilebileceği, ayrıca ihale yapılırken hem ilk satış hem de ikinci satış sırasında hacizli malın tahmin edilen bedelinin asgari olarak yüzde ellisi üzerinden ihale edilmesini öngören hükümlerin, ikinci satışı işlevsiz hale getireceği ve zaman kaybına yol açabileceği belirtilerek kuralların, Anayasa'nın 36. ve 40. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kurallar, taşınır ve taşınmaz malların cebri icra yoluyla satılması sürecinde, elektronik ortamda ihaleye katılabilme imkânını ve bu imkânla birlikte değişen ihale sürecini düzenlemektedir.

Dava konusu kurallarla hacizli malların satışının sınırlı bir alıcı çevresinden kurtarılarak fiziki ortam yanında ilgili elektronik ortam kullanıcılarının katılımına açık hale getirilmesi sağlanmakta, böylece rekabetçi ve yaygın katılımcı bir ortamda malın gerçek değerinde satılmasına imkân tanınmasının amaçlandığı anlaşılmaktadır. Bu durum, hem alacaklının hem de borçlunun menfaatlerini koruyan

ve icra takibinin amacına uygun şekilde sonuçlanmasına hizmet eden bir sisteme işlerlik kazandırılmaktadır.

İhalenin sadece fiziki ortamdaki teklifler üzerinden değil, elektronik ortamdaki teklifler üzerinden de yapılabilecek olması, ihalenin icra dairesi görevlileri dışındaki ilgililerin giremeyeceği ve denetleyemeyeceği kapalı bir elektronik ortamda yapılması anlamına da gelmeyip, bu tüm ilgililerin rahatlıkla girebildiği ve yapılan işlemleri izleyebildiği, denetime açık bir ortam sağlamaktadır.

Dolayısıyla, dava konusu kurallarla getirilen elektronik ortamda satışa katılma imkânının, ihalenin aleniliği ve açıklığı ilkelerini zedeleyen bir yönü olmadığı gibi alacaklı ile borçlunun menfaatlerinin daha iyi korunmasını sağlayan bir mekanizmaya işlerlik kazandırdığı açıktır.

Ayrıca, elektronik ortamda satışa katılmanın ancak elektronik imza kullanılmak suretiyle mümkün olabilmesi ve günümüzde elektronik imzanın güvenli işlem yapma konusunda ulaştığı başarı dikkate alındığında bu yöntemle oluşturulan verilerin fiziki ortamdaki verilere nazaran daha güvensiz olduğu söylenemez.

Öte yandan, dava konusu kurallarla ihale yapılırken hem ilk hem de ikinci ihale sırasında hacizli malın tahmin edilen değerinin en az yüzde ellisi üzerinden ihale edilebileceğini öngören hükümlerin, ikinci satışı işlevsiz hale getireceği ve zaman kaybına yol açacağı, dolayısıyla tarafların hak arama özgürlüğünü sınırlayacağından da söz edilemez. Zira, dava konusu kurallardan önce ikinci ihalede malın tahmin edilen değerinin en az yüzde kırkı oranında satılmasına imkân tanınması sebebiyle, alıcılar özellikle birinci ihalede yüksek teklifler vermeyerek malın ikinci ihalede daha ucuza alınmasını sağlama yoluna gidebilmekte, malın ucuza satılması ise hem alacaklının hem borçlunun menfaatlerine aykırı sonuçlar doğurmaktaydı. Esasen malın ikinci ihalede daha ucuza alınabileceği beklentisi, birinci ihalede malın satılmasında önleyici bir rol oynamaktaydı. Dava konusu düzenlemelerle ikinci ihalenin de malın tahmin edilen bedelinin en az yüzde ellisi üzerinden ihale edilebilmesi sağlanarak bu önleyici rolün bertaraf edilmesi yoluna gidildiği anlaşılmaktadır.

Açıklanan nedenlerle dava konusu kurallar, Anayasa'nın 36. maddesine aykırı değildir. İptal istemlerinin reddi gerekir.

Kuralların, Anayasa'nın 40. maddesiyle ilgisi görülmemiştir.

E- Kanun'un 44. Maddesiyle 2575 Sayılı Kanun'un 8. Maddesinin (1) Numaralı Fıkrasının (d) Bendine Eklenen 'Türkiye Büyük Millet Meclisi Genel Sekreterliği,' İbaresinin, (e) Bendine Eklenen 'ile düzenleyici ve denetleyici kurumların başkanlıkları,' İbaresinin, Değiştirilen (g)

Bendinin ve (3) Numaralı Fıkrasında Yer Alan 'yirmi yıl' İbaresinin 'onbeş yıl' Şeklinde Değiştirilmesinin İncelenmesi

Dava dilekçesinde, Danıştay üyeliğine hâkimlik mesleği dışından idareden üye seçilmesi uygulamasının, bu kaynaktan gelenlerin idareden edindikleri bilgi birikimi ve deneyimlerini Danıştaya aktarmaları amacıyla düzenlendiği, dava konusu kurallarla, Danıştaya üye seçiminde yararlanılacak idari kaynağa Türkiye Büyük Millet Meclisi Genel Sekreterliği, düzenleyici ve denetleyici kurumların başkanlıkları gibi yeni statüler eklendiği ve idari kaynaktan gelenler yönünden söz konusu göreve seçilebilmek için kamu hizmetinde geçirilmesi gereken sürenin hâkimlik mesleğinden gelenlere nazaran daha az bir süreye tekabül edecek şekilde yirmi yıldan onbeş yıla düşürüldüğü, böylece yeterli tecrübeye sahip olunmadan bu göreve atanmanın mümkün hale getirildiği ve anılan amacın yerine getirilmesinin önlenildiği belirtilerek kuralların, Anayasa'nın 2., 6., 8., 9., 10., 11., 138., 139., 140. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kurallarda, Danıştayda boşalan her dört üyelikten biri için, Cumhurbaşkanı tarafından hâkimlik mesleği dışından seçilecek kamu görevlisi kaynağına, Türkiye Büyük Millet Meclisi Genel Sekreterliği, düzenleyici ve denetleyici kurum başkanlıkları, kamu kurum ve kuruluşlarının başhukuk müşavirliği, birinci hukuk müşavirliği, hukuk hizmetleri başkanlığı ve hukuk işleri müdürlüğü statüleri eklenmekte, ayrıca söz konusu göreve seçilmek için aranan şartlardan biri olan devlet hizmetinde çalışmış olma süresi yirmi yıldan on beş yıla düşürülmektedir.

6216 sayılı Kanun'un 43. maddesi uyarınca, iptali istenen kurallar ilgisiz nedeniyle, Anayasa'nın 155. maddesi yönünden de incelenmiştir.

Anayasa'nın 155. maddesinin üçüncü fıkrasında 'Danıştay üyelerinin dörtte üçü, birinci sınıf idari yargı hâkim ve savcıları ile bu meslekten sayılanlar arasından Hakimler ve Savcılar Yüksek Kurulu; dörtte biri, nitelikleri kanunda belirtilen görevliler arasından Cumhurbaşkanı; tarafından seçilir.' hükmüne yer verilmiş, son fıkrasında ise 'Danıştayın, kuruluşu, işleyişi, Başkan, Başsavcı, başkanvekilleri, daire başkanları ile üyelerinin nitelikleri ve seçim usulleri, idari yargının özelliği, mahkemelerin bağımsızlığı ve hâkimlik teminatı esaslarına göre kanunla düzenlenir.' denilmek suretiyle, kanun koyucunun idari yargının özelliği, mahkemelerin bağımsızlığı ve hakimlik teminatı esaslarını gözetmek koşuluyla, Danıştaya seçilecek üyelerin niteliklerini ve söz konusu üyeliğe seçilme usullerini belirleme konusunda takdir yetkisine sahip olduğu belirtilmiştir.

Bu çerçevede kanun koyucunun Anayasa'nın 155. maddesinde belirtilen Danıştaya seçilecek üyelerin niteliklerini ve seçilme usullerini belirleme konusundaki takdir yetkisini kullanmak suretiyle

düzenlediği dava konusu kuralların, mahkemelerin bağımsızlığı, hâkimlik teminatı ve idari yargının özellikleriyle bağdaşmayan bir yönü bulunmamaktadır.

Öte yandan, Anayasa'nın 10. maddesinde yer verilen eşitlik ilkesi hukuksal durumları aynı olanlar için söz konusudur. Bu ilke ile eylemli değil, hukuksal eşitlik öngörülmüştür. Eşitlik ilkesinin amacı, aynı durumda bulunan kişilerin yasalar karşısında aynı işleme bağlı tutulmalarını sağlamak, ayırım yapılmasını ve ayrıcalık tanınmasını önlemektir. Bu ilkeyle, aynı durumda bulunan kimi kişi ve topluluklara ayrı kurallar uygulanarak kanun karşısında eşitliğin ihlali yasaklanmıştır. Kanun önünde eşitlik, herkesin her yönden aynı kurallara bağlı tutulacağı anlamına gelmez. Durumlarındaki özellikler, kimi kişiler ya da topluluklar için değişik kuralları ve uygulamaları gerektirebilir. Aynı hukuksal durumlar aynı, ayrı hukuksal durumlar farklı kurallara bağlı tutulursa Anayasa'da öngörülen eşitlik ilkesi zedelenmez.

Bu ilke çerçevesinde dava konusu kural incelendiğinde, Danıştay üyeliğine atanabilmek için hâkimlik mesleği dışından seçilen kişiler yönünden kamu hizmetinde geçirilmesi gereken sürenin yirmi yıldan onbeş yıla düşürülmesiyle, hâkimlik mesleğinden gelen kişiler aleyhine bir eşitsizlik yaratıldığı söylenemez. Zira, Anayasa'ya göre Danıştay üyesi kadrosunun dörtte üçünü hâkimlik mesleğinden, dörtte birlik kısmını ise hâkimlik mesleği dışında nitelikleri kanunda belirtilen görevliler arasından seçilen kişiler oluşturmaktadır. Anayasa koyucu, Danıştayın bu şekilde farklı kariyerlerden gelenlerce oluşturulmasını takdir etmiş, buna göre de Danıştayın oluşumunda belli bir oranı esas alarak iki ayrı kategori belirlemiştir. Bu iki ayrı kategorideki kişilerin hukuksal durumları aynı olmadığından, eşitlik ilkesi gereği bu iki ayrı kategorinin tümüyle aynı kurallara tabi tutulması gerekmemektedir.

Açıklanan nedenlerle dava konusu kurallar, Anayasa'nın 10. ve 155. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir.

Zehra Ayla PERKTAŞ maddenin (3) numaralı fıkrasında yapılan değişiklik yönünden bu görüşe katılmamıştır.

Kuralların, Anayasa'nın 2., 6., 8., 9., 11., 138., 139. ve 140. maddeleriyle ilgisi görülmemiştir.

F- Kanun'un 45. Maddesiyle Değiştirilen 2575 Sayılı Kanun'un 24. Maddesinin (1) Numaralı Fıkrasının (c) Bendinin İncelenmesi

Dava dilekçesinde, dava konusu kuralın Bakanlıkların ülke çapında uygulanacak düzenleyici işlemlerine karşı Danıştayda, diğer işlemlerine karşı ise konularına göre idare ve vergi mahkemelerinde dava açılmasını düzenleyerek Danıştayın görev alanını daralttığı, Bakanlıkların

belli bir coğrafyada uygulanacak düzenleyici işlemlerin (Kültür ve Turizm Bakanlığınca yapılan planlar gibi) çoğu kez bazı kişi veya gruplara rant sağlayacak niteliğinin bulunduğu, bu sebeple söz konusu düzenleyici işlemlere karşı açılacak davalara bakma görevinin Danıştayın siyasi müdahaleye olanak vermeyecek göreceli güçlü yapısı dikkate alındığında idare ve vergi mahkemelerine verilmesinin uygun olmadığı, ülke çapında uygulanacak düzenleyici işlem ile yerel düzenleyici işlem arasında ayırım yapmanın zor olduğu ve bunun mahkemeler arasında görev uyuşmazlığına sahip olabileceği, ayrıca genel ve yerel düzenleyici işlemlere karşı açılacak davalara farklı mahkemelerce bakılmasının içtihat birliğini bozacağı belirtilerek kuralın, Anayasa'nın 2., 6., 8., 9., 10., 11., 138., 139., 140. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralda, Danıştayın ilk derece mahkeme sıfatıyla bakanlıklar ile kamu kuruluşları veya kamu kurumu niteliğindeki meslek kuruluşlarınca çıkarılan ve ülke çapında uygulanacak düzenleyici işlemlere karşı açılacak davalara bakma yönündeki görevi düzenlenmektedir. Buna göre, dava konusu kuraldan önce bakanlıkların tüm düzenleyici işlemlerine karşı açılan davalar Danıştayda görülmekteyken, dava konusu kural ile sadece ülke çapında uygulanacak düzenleyici işlemlere karşı açılacak davaların Danıştayda görülmesi esası benimsenmiştir.

Anayasa'nın 2. maddesinde Türkiye Cumhuriyetinin bir hukuk devleti olduğu; 9. maddesinde, yargı yetkisinin, Türk Milleti adına bağımsız mahkemelerce kullanılacağı; 138. maddesinin birinci fıkrasında, hâkimlerin görevlerinde bağımsız oldukları ve Anayasa'ya, kanuna ve hukuka uygun olarak vicdanî kanaatlerine göre hüküm verecekleri, ikinci fıkrasında ise hiçbir organ, makam, merci veya kişinin, yargı yetkisinin kullanılmasında mahkemelere ve hâkimlere emir ve talimat veremeyeceği, genelge gönderemeyeceği, tavsiye ve telkinde bulunamayacağı belirtilerek hukuk devleti olmanın zorunlu bir gereği olan mahkemelerin bağımsızlığı teminat altına alınmıştır.

Anayasa'nın 142. maddesinde, 'Mahkemelerin kuruluşu, görev ve yetkileri, işleyişi ve yargılama usulleri kanunla düzenlenir.' denilmek suretiyle, kanun koyucunun genel olarak mahkemelerin görev ve yetkilerine ilişkin düzenlemeler yapma hususunda takdir yetkisine sahip olduğu belirtilmiş, Anayasa'nın 155. maddesinin birinci fıkrasında ise 'Danıştay, idari mahkemelerce verilen ve kanunun başka bir idari yargı merciine bırakmadığı karar ve hükümlerin son inceleme merciidir. Kanunla gösterilen belli davalara da ilk ve son derece mahkemesi olarak bakar.' denilmek suretiyle Danıştayın hangi davalara ilk ve son derece mahkemesi sıfatıyla bakacağıının kanun koyucu tarafından belirleneceği açıkça vurgulanmıştır.

Bu çerçevede, kanun koyucunun mahkemelerin görev alanına ilişkin düzenleme yapma hususundaki takdir yetkisini kullanarak dava konusu kuralla bakanlıkların ülke çapında uygulanmayacak

düzenleyici işlemlerine karşı açılacak davalar konusunda, Danıştayın ilk derece mahkemesi sıfatıyla bu davalara bakma yönündeki görevini kaldırarak bu hususta idare ve vergi mahkemelerini görevlendirmesinde, hukuk devleti ilkesine aykırı bir yön bulunmamaktadır.

Öte yandan, hukuk devleti olmanın yargı bağımsızlığını sağlamayı bir ön şart olarak gerektirdiği gözetildiğinde, bu şartın hem yüksek mahkemeler hem de ilk derece mahkemeleri yönünden aynı oranda geçerli olduğu kuşkusuzdur. Mahkemelere verilen görev ve yetkileri kullanan hâkimlerin tarafsızlığı, bağımsızlığı, Anayasa ve kanunlara bağlılıkları açısından aralarında bir farklılığın bulunduğu kabul edilemez. Bu çerçevede idare ve vergi mahkemelerinin Danıştaya nazaran siyasi etkilere daha açık olduğu, dolayısıyla bu mahkemelerin yetkilerinin genişletilmesinin mahkemelerin bağımsızlığına müdahale sonucunu doğuracağı iddiasının hukuki bir dayanağı bulunmamaktadır.

Dava dilekçesinde, düzenlemenin mahkemeler arasında görev uyuşmazlığına ve içtihat farklılığına neden olabileceği gerekçesiyle Anayasa'ya aykırı olduğu ileri sürülmüş ise de herhangi bir düzenlemenin mahkemeler arasında görev veya içtihat uyuşmazlıklarına neden olması yargılama hukukunun doğası gereği her zaman mümkün olup bu durumun anayasal bir sorun oluşturması söz konusu değildir. Kaldı ki hukuk sistemi içerisinde mahkemeler arasındaki görev ve içtihat uyuşmazlıklarını çözecek hukuki yollara yer verilmiştir.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 9. ve 138. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŞ bu görüşe katılmamışlardır.

Kuralın, Anayasa'nın 6., 8., 10., 11., 139. ve 140. maddeleriyle ilgisi görülmemiştir.

G- Kanun'un 46. ve 47. Maddeleriyle Değiştirilen 2575 Sayılı Kanun'un 60. Maddesinin (1) Numaralı Fıkrasının Birinci Cümlesi ile 61. Maddesinin (1) Numaralı Fıkrasının Birinci ve İkinci Cümleleri ile (3) Numaralı Fıkrasının İncelenmesi

Dava dilekçesinde, dava konusu kurallarla Danıştay savcılarının yürütmenin durdurulması talepleriyle ilgili tüm dava dosyaları ile temyiz ve karar düzeltme incelemesi için Danıştayda bulunan dosyalar hakkında görüş bildirmeleri usulünden vazgeçildiği, bunun Kanun gerekçesinde belirtildiği gibi yargıyı hızlandırma amacına hizmet etmeyeceği, Danıştay savcılarının temyiz ve karar düzeltme istemli dosyalar yönünden görüş bildirmesinin davayla ilgili belge ve bilgilerin farklı bir gözle incelenmesini sağladığı ve böylece adil yargılamanın gerçekleşmesine yardımcı olduğu, ayrıca Danıştay savcılarının içtihadın gelişmesini izleyerek ülkede hukuk birliğinin ve kanun önünde eşitlik ilkesinin gerçekleşmesine, dolayısıyla hukukun gelişmesine katkıda buldukları, bunun yanında ilk

derece mahkemelerde görevli idari yargıçların, çoğunlukla kıdem ve deneyim yönünden Danıştay meslek mensuplarının gerisinde olduğu, bu sebeple bu mahkemelerde verilen kararların bir kez de Danıştay savcılarınca incelenip değerlendirilmesinde fayda bulunduğu belirtilerek kuralların, Anayasa'nın 2., 6., 9., 138. ve 139. maddelerine aykırı olduğu ileri sürülmüştür.

6216 sayılı Kanun'un 43. maddesi uyarınca, iptali istenen kurallar ilgisi nedeniyle, Anayasa'nın 36. maddesi yönünden de incelenmiştir.

Dava konusu kurallarla, Danıştayda görülen tüm davaların esası ve yürütmenin durdurulması istemleri hakkında Danıştay savcılarının görüş bildirmeleri usulünden vazgeçilmekte ve sadece Danıştayda ilk derece mahkeme sıfatıyla görülen davalarda esas hakkında görüş bildirmeleri usulü benimsenmektedir.

Hukuk devletinde, kanun koyucu, yargılama hukukuna ilişkin kurallar belirleme ve bu çerçevede mahkemelerin kuruluşu, görev ve yetkileri, işleyişi, yargılama usulleri ve yapısı hakkında Anayasa kurallarına bağlı olmak koşuluyla ihtiyaç duyduğu düzenlemeyi yapma konusunda takdir yetkisine sahip bulunmaktadır. Nitekim Anayasa'nın 142. maddesinde, 'Mahkemelerin kuruluşu, görev ve yetkileri, işleyişi ve yargılama usulleri kanunla düzenlenir.' denilmek suretiyle bu husus hüküm altına alınmıştır.

Danıştay savcılarının dava dosyalarıyla ilgili görüş belirtip belirtmeyeceği hususu da mahkemelerin işleyişi ve yargılama usulüne ilişkin olup bu hususta kanun koyucunun takdir yetkisine dayanarak ihtiyaç duyduğu düzenlemeyi yapmasında hukuk devleti ilkesine aykırı bir yön bulunmamaktadır.

Diğer taraftan, dava konusu kuralların, Kanun'un gerekçesinde belirtilen yargıyı hızlandırma amacını yerine getirmeye elverişli olmaması iddiası anayasallık denetimi açısından sınırlı bir işleve sahiptir. Anayasa'nın açıkça amaç öngörmediği durumlarda Anayasa'nın 2. maddesindeki 'hukuk devleti' ilkesi gereğince, yasama işlemlerinin kişisel yararları değil kamu yararını gerçekleştirmek amacıyla yapılması zorunludur. Kamu yararının sübjektif niteliği dolayısıyla bir yasanın kamu yararı dışında bir amaç güttüğü ancak açıkça görülebilen durumlarda Anayasa'ya aykırılık nedeni olarak görülebilir. Amaç yönünden Anayasa'ya aykırılıktan söz edilebilmesi için kamu yararı dışında özel bir çıkarın gözetildiğinin tespiti gerekir.

Kanun koyucunun kamu yararı amacıyla hareket edip etmediği ise ancak ilgili yasama belgelerinin incelenmesinden ve kuralın objektif anlamından çıkarılabilir. Kanun'un genel ve ilgili madde gerekçelerinde dava konusu kuralların yargıyı hızlandırmak amacıyla düzenlendiği belirtilmiştir. Kuralların objektif anlamı da dikkate alındığında söz konusu kuralların kamu yararı dışında, yani

yargıyı hızlandırmaktan başka özel bir çıkar amacıyla düzenlendiğine ilişkin bir sonuca varmanın mümkün olmadığı anlaşılmaktadır. Dolayısıyla, dava konusu kuralların amaç yönüyle de Anayasa'ya aykırı bir yönü bulunmamaktadır.

Öte yandan, Anayasa'nın 'Hak arama hürriyeti' başlıklı 36. maddesinin birinci fıkrasında, 'Herkes, meşru vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir' denilerek yargı organlarına davacı ve davalı olarak başvurabilme ve bunun doğal sonucu olarak da iddia, savunma ve adil yargılanma hakkı güvence altına alınmıştır.

Anayasa'nın 9. maddesinde 'Yargı yetkisi, Türk Milleti adına bağımsız mahkemelerce kullanılır'; 142. maddesinde 'Mahkemelerin kuruluşu, görev ve yetkileri, işleyişi ve yargılama usulleri kanunla düzenlenir' denilmekte; Avrupa İnsan Hakları Sözleşmesi'nin 'Adil yargılanma hakkı' başlıklı 6. maddesinin birinci fıkrasında da herkesin kanuni, bağımsız ve tarafsız bir mahkeme tarafından davasının dinlenilmesini isteme hakkı olduğu ifade edilmektedir.

Yasayla kurulmuş bağımsız ve tarafsız mahkemeler, adil yargılanma hakkının temelidir. Anayasa'da ve uluslararası sözleşmelerde 'mahkeme' kavramı için belirli bir şekil şartı aranmamakta; yasayla kurulmuş, bağımsız, tarafsız ve yargılama usulü güvencesine sahip yargı yeri, mahkeme olarak kabul edilmektedir. Bu ilkelere aykırı olmamak şartı ile kanun koyucunun mahkemelerin oluşum, kuruluş, çalışma ve yargılama usullerini serbestçe belirlemesi mümkündür. Dolayısıyla bazı tür davalar ve kararlar yönünden savcılıktan görüş alınmasından vazgeçilmesinin, adil yargılanma hakkı ilkesiyle çelişen bir yönü bulunmamaktadır.

Açıklanan nedenlerle, dava konusu kurallar, Anayasa'nın 2. ve 36. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir.

Osman Alifeyyaz PAKSÜT bu görüşe katılmamıştır.

Kuralların, Anayasa'nın 6., 9., 138. ve 139. maddeleriyle ilgisi görülmemiştir.

Ğ- Kanun'un 46. Maddesiyle Değiştirilen 2575 Sayılı Kanun'un 60. Maddesinin (1) Numaralı Fıkrasının İkinci Cümlesinin İncelenmesi

Dava dilekçesinde, dava konusu kuralla ilgili olarak herhangi bir gerekçe belirtilmeden kuralın, Anayasa'nın 2., 6., 9., 138. ve 139. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralda, Danıştay Başsavcılığında görevli savcılar ile diğer memurların çalışma düzenlerinin sağlanması ile Danıştaya gelen dosyaların işlem görmesi, muhafazası ve ilgili yerlere

gönderilmesiyle ilgili alınması gereken tedbirlere ilişkin Danıştay Başsavcısı'nın görevleri düzenlenmektedir.

Anayasa'nın 151. maddesinde, 'Anayasa Mahkemesinde doğrudan doğruya iptal davası açma hakkı, iptali istenen kanun, kanun hükmünde kararname veya içtüzüğün Resmi Gazetede yayımlanmasından başlayarak altmış gün sonra düşer.' denilmiş; 6216 sayılı Kanun'un 37. maddesinin (1) numaralı fıkrasında ise 'Anayasa değişiklikleri ile kanunların şekil yönünden Anayasaya aykırılıkları iddiası ile doğrudan doğruya iptal davası açma hakkı, bunların Resmî Gazetede yayımlanmalarından başlayarak on gün; kanun hükmünde kararnamelerle Türkiye Büyük Millet Meclisi İçtüzüğünün veya bunların belli madde ve hükümlerinin şekil ve esas, kanunların ise sadece esas yönlerinden Anayasaya aykırılıkları iddiasıyla doğrudan doğruya iptal davası açma hakkı, bunların Resmî Gazetede yayımlanmalarından başlayarak altmış gün sonra düşer.' hükmüne yer verilmiştir. Buna göre, kanunların esas yönünden Anayasa'ya aykırılıkları iddiasına dayalı iptal davalarının bunların Resmi Gazete'de yayınlanmasından itibaren altmış gün içinde açılması gerekmektedir.

Dava konusu kural, 20.1.1982 günlü, 17580 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiş olup, söz konusu tarihten bu yana kuralda her hangi bir değişiklik yapılmamıştır. Kurala ilişkin dava ise 3.9.2012 gününde açılmıştır.

Kuralın Resmi Gazete'de yayımlandığı tarihten itibaren altmış günlük dava açma süresi geçirilmiş olduğundan bu kurala yönelik iptal isteminin süre yönünden reddi gerekir.

H- Kanun'un 57. Maddesiyle 2577 Sayılı Kanun'un 27. Maddesinin Değiştirilen (2) Numaralı Fıkrasının Birinci Cümlesinde Yer Alan "davalı idarenin savunması alındıktan veya savunma süresi geçtikten sonra" İbaresini ile İkinci Cümlesinin ve Aynı Maddeyle 2577 Sayılı Kanun'un 27. Maddesine Eklenen (3) ve (10) Numaralı Fıkraların İncelenmesi

Dava dilekçesinde, dava konusu kuralların idari yargıda açık hukuka aykırılık hâllerinde davalı idarenin savunmasının alınmaksızın yürütmenin durdurulmasına karar verilmesi imkânını ortadan kaldırdığı, bunun ise yürütmenin durdurulması kararı verilmesi için Anayasa'da belirtilen şartlara yeni bir şart eklemek anlamına geldiği ve yürütmenin durdurulması kurumunu işlevsiz hale getirip bireylerin idare karşısında haklarının korunmasını önlediği, aynı sebeplere dayanılarak ikinci kez yürütmenin durdurulması isteminde bulunulamayacağı yolundaki düzenlemenin, yargılama makamının kararını gözden geçirme olanağını ortadan kaldırdığı ve bu yönüyle yargılama ve hukuk güvenliği ilkesine aykırılık teşkil ettiği, söz konusu kuralların idarenin savunma verebilmesi için gerekli zaman dilimini araya koymak suretiyle yürütülmesi derhal durdurulması gereken idari

işlemlerin bir süre daha uygulanmasına olanak sağlamak amacıyla düzenlendiği, kurallarda yürütmenin durdurulması yönünden uygulanmakla etkisi tükenecek işlemler ve uygulanmakla etkisi tükenmeyecek işlemler şeklinde iki ayrı kategori oluşturulduğu, oysa bunların birbirinden ayırt edilmesinin zor olması nedeniyle içtihat farklılıklarının oluşabileceği ve bu durumun kanun önünde eşitlik ilkesine aykırı sonuçlar doğuracağı, ayrıca söz konusu kurallarda yer alan, dava dilekçesi ve eklerinden talebin reddedilmesi gerektiğinin anlaşıldığı hâllerde idarenin savunmasının beklenmeyebileceği yönündeki düzenlemenin idare lehine çifte standart yaratması niteliğiyle eşitlik ilkesine ve silahların eşitliği ilkesine aykırı olduğu, zira bunun idare lehine bir karar verildiğinde yargılamanın hızlanması, ama birey lehine bir karar verilmesi hâlinde yargının yavaş işlemesi sonucunu doğuracağı belirtilerek kuralların, Anayasa'nın 2., 10., 36. ve 125. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu 2577 sayılı Kanun'un 27. maddesinin (2) numaralı fıkrasında, yürütmenin durdurulması kararlarının kural olarak idarenin savunması alındıktan veya savunma süresi geçtikten sonra verilebileceği ve uygulanmakla etkisi tükenecek olan idari işlemlerin yürütülmesinin savunma alındıktan sonra yeniden karar verilmek üzere, idarenin savunması alınmaksızın da durdurulabileceği; (3) numaralı fıkrasında, dava dilekçesi ve eklerinden yürütmenin durdurulması isteminin yerinde olmadığına anlaşılmaması halinde davalı idarenin savunması alınmaksızın da istemin reddedilebileceği; (10) numaralı fıkrasında ise aynı sebeplere dayanılarak ikinci kez yürütmenin durdurulması isteminde bulunulamayacağı düzenlenmektedir.

Anayasa'nın 142. maddesi uyarınca mahkemelerin kuruluşu, görev ve yetkileri, işleyişi ve yargılama usullerinin belirlenmesi kanun koyucunun takdirindedir. Mahkemelerin hukuka aykırılık hallerinde kişilerin telafisi zor veya imkânsız zararlarla karşılaşmasını önlemek amacıyla ve ileride verecekleri nihai kararların uygulanabilirliğini ve geçerliliğini sağlamak üzere alacakları önlemler yargılama usulü kuralları arasındadır. Yürütmenin durdurulması ile ilgili kurallar da diğer yargılama usulü kuralları gibi kanun koyucu tarafından serbestçe düzenlenebilir. Ancak, kanun koyucunun bu yetkisini kullanırken belirleyeceği kuralların Anayasa'nın 125. maddesinde belirtilen şartlara ve diğer Anayasa kurallarına aykırı olmaması gerekir.

Anayasa'nın 125. maddesinin beşinci fıkrasında, 'İdari işlemin uygulanması halinde telafisi güç veya imkânsız zararların doğması ve idari işlemin açıkça hukuka aykırı olması şartlarının birlikte gerçekleşmesi durumunda gerekçe gösterilerek yürütmenin durdurulmasına karar verilebilir.' hükmüne yer verilmiştir.

Dava konusu kurallarda, yürütmenin durdurulması kararı verilmeden önce idarenin savunmasının alınmasının öngörüldüğü, ancak bunun tüm idari işlemler yönünden mutlak olarak aranmayıp sadece 'uygulanmakla etkisi tükenmeyecek idari işlemler' yönünden arandığı, diğer işlemler yönünden ise mahkemelere idarenin savunması alındıktan sonra yeniden karar verilmek üzere savunma alınmaksızın da yürütmenin durdurulması kararı verme yetkisinin tanındığı görülmektedir. Dolayısıyla kurallarda mahkemelerin yürütmenin durdurulması kararı vermeden önce sadece 'uygulanmakla etkisi tükenmeyecek idari işlemler' yönünden savunma alma zorunluluğu getirilmiş olup diğer işlemler yönünden savunma almaksızın karar verme imkânı kaldırılmamıştır.

Kurallarda 'uygulanmakla etkisi tükenmeyecek idari işlemler' yönünden idarenin savunmasının alınmasının öngörülmesi ise Anayasa'nın 125. maddesinde belirtilen koşulları değiştiren veya bu koşullara aykırılık teşkil eden bir düzenleme olmayıp idareye yöneltilen iddia karşısında kendisini savunabilme imkânı sağlamaktadır. Bu yönüyle kuralların Anayasa'nın 125. maddesine aykırı bir yönü bulunmamaktadır.

Anayasa'nın hak arama hürriyetini düzenleyen 36. maddesinin birinci fıkrasında, kişilerin hak arama özgürlükleri güvence altına alınmıştır. Hak arama özgürlüğü, toplumsal barışı güçlendiren dayanaklardan biri olmasının yanında bireyin adaleti bulma, hakkı olanı elde etme ve haksızlığı giderme yoludur. İnsan varlığını soyut ve somut değerleriyle koruyup geliştirmek amacıyla hukuksal olanakları kapsamlı biçimde sağlama, bu konuda tüm yollardan yararlanma hakkını içeren hak arama özgürlüğü, hukuk devletinin ve çağdaş demokrasinin vazgeçilmez koşullarından biridir.

İdari işlemin uygulanmasıyla telafisi güç veya imkânsız zararların doğacağı durumlarda, yürütmenin durdurulması kararı verilebilmesi, kişilerin hak arama özgürlüklerini etkili biçimde kullanabilmelerini sağlayan önemli bir imkân olup bu imkânı ortadan kaldıran veya etkisiz hale getiren bir düzenleme, Anayasa'nın 36. maddesinde yer alan hak arama özgürlüğüne aykırılık teşkil edecektir.

Bu çerçevede dava konusu kurallar ele alındığında, kurallarda, uygulandığı anda telafisi güç veya imkânsız zararların doğması ihtimali bulunan 'uygulanmakla etkisi tükenmeyecek idari işlemler' yönünden, idarenin savunması alınmaksızın yürütmenin durdurulması kararının verilebilmesine imkân tanındığı, böylece idarenin savunmasının alınması sebebiyle oluşabilecek gecikmeye izin verilmeyerek bu tür idari işlemler yönünden telafisi güç veya imkânsız zararların doğması ihtimalinin bertaraf edildiği görülmektedir.

Kurallarda, sadece uygulandığı anda telafisi güç veya imkânsız zararlar doğurması ihtimali bulunmayan ancak belli bir süre uygulanmakla telafisi güç veya imkânsız zararlar doğurma ihtimali olan 'uygulanmakla etkisi tükenmeyecek idari işlemler' yönünden idarenin savunmasının alınması şartının getirildiği, fakat bu tür idari işlemlerin niteliği sebebiyle bunlar yönünden idarenin savunmasının alınması nedeniyle meydana gelecek gecikmenin, kişilerin telafisi güç veya imkânsız zararlarla karşılaşması sonucunu doğurmayacağı, dolayısıyla bu yönden de kuralların hak arama özgürlüğünü sınırlayan bir yönünün bulunmadığı görülmektedir.

2577 sayılı Kanun'un 27. maddesinin dava konusu (10) numaralı fıkrasında aynı sebeplere dayanılarak ikinci kez yürütmenin durdurulması isteminde bulunulamayacağı kuralına yer verilmiştir. Hukuk devletinde, herkesin etkili bir şekilde hakkını arama ve iddiasına ilişkin olarak adil bir yargılanma yapılmasını isteme hakkı bulunmakla birlikte, bu haklar aynı mahkemenin daha önce karar verdiği hususta bir kez daha inceleme yapıp karar vermesini gerektirmemektedir. Mahkemenin daha önce karar verdiği aynı hususu bir kez daha inceleyip incelemeyeceği konusu, yargılama usulüne ilişkin olup bu konuda ne tür bir düzenleme yapılacağı kanun koyucunun takdirinde bulunmaktadır.

Kaldı ki, yürütmenin durdurulması istemine ilişkin kararın bir kez daha gözden geçirilmesi ihtiyacı, istemin daha üst bir mercide değerlendirilmesini sağlayacak mekanizmalar oluşturulması suretiyle çok daha etkili bir şekilde karşılanmaktadır. Bu çerçevede kuralın yargılama makamının kararını gözden geçirme olanağını ortadan kaldırdığı ve bu yönüyle yargılama ve hukuk güvenliği ilkesine aykırılık teşkil ettiği yönündeki iddianın hukuki bir dayanağı bulunmamaktadır.

Diğer taraftan, söz konusu kuralların idarenin savunma verebilmesi için gerekli zaman dilimini araya koymak suretiyle, yürütmesi derhal durdurulması gereken idari işlemlerin bir süre daha uygulanmasına olanak sağlamak amacıyla düzenlendiği ve bu kuralların bu nedenle Anayasa'ya aykırı olduğu yönündeki iddianın da haklı bir temeli bulunmamaktadır. Zira bir düzenlemenin amaç yönünden Anayasa'ya aykırı olduğunun söylenebilmesi için düzenlemenin kamu yararı dışında özel bir amaçla yapıldığının tespit edilmesi gerekir. Oysa dava konusu kuralların genel ve madde gerekçeleri ile kuralların objektif anlamı dikkate alındığında, bunların idareye savunma hakkı tanımak, böylece adil bir karar verilebilmesini sağlamak amacıyla düzenlendiği anlaşılmaktadır. Dolayısıyla, bu kuralların kamu yararı dışında bir amaçla, bu çerçevede yürütmesi derhal durdurulması gereken idari işlemlerin bir süre daha uygulanmasına olanak sağlamak amacıyla düzenlendiği söylenemez.

Dava konusu kurallarda, uygulanmakla etkisi tükenecek işlemler ve uygulanmakla etkisi tükenmeyecek işlemler şeklinde iki ayrı kategori oluşturulmasının içtihat birliğini bozacağı ve bunun kanun önünde eşitlik ilkesine aykırı sonuçlar doğuracağını söylemek de mümkün değildir. Zira bir düzenlemenin mahkemeler tarafından farklı yorumlanması her zaman mümkün olup yargı sistemi içerisinde bu yorumlardan hangisinin nihai olarak bağlayıcı olacağını belirleyecek ve söz konusu yorum farklılıklarını gidererek uygulama birliğini sağlayacak hukuki yollar bulunmaktadır. Dolayısıyla, herhangi bir düzenlemenin mahkemeler arasında içtihat farklılığına neden olması yargılama hukukunun doğası gereği her zaman mümkün olup bu durumun anayasal bir sorun oluşturması veya kanun önünde eşitlik ilkesine aykırı sonuçlar doğurması söz konusu değildir.

Anayasa'nın hak arama hürriyetini düzenleyen 36. maddesine 2001 değişiklikleriyle eklenen 'adil yargılanma' ibaresine ilişkin gerekçede, taraf olduğumuz uluslararası sözleşmelerce de güvence altına alınan adil yargılama hakkının madde metnine dâhil edildiği vurgulanmıştır. Bu sözleşmelerden Avrupa İnsan Hakları Sözleşmesi ile Avrupa İnsan Hakları Mahkemesi uygulamasındaki adil yargılama ölçütleri içerisinde çekişmeli yargılama, gerekçeli karar, duruşmada hazır bulunma, susma hakkı ve diğer sanık hakları yanında 'silahların eşitliği' ilkesi de bulunmaktadır.

'Adil yargılanma hakkı'nın ulusal üstü düzeyde genel kabul görmüş ölçütleri arasında önemli bir yer tutan 'silahların eşitliği' ilkesi, davanın tarafları arasında yargılama sırasında usul hükümleri yönünden eşit konumda bulunma, taraflardan birine dezavantaj diğerine avantaj sağlayacak kurallara yer vermeme esasını içermekte, diğer bir deyişle davanın tarafları arasında hakkaniyete uygun bir dengeyi varlığını gerekli kılmaktadır.

Dava konusu kurallar arasında yer alan dava dilekçesi ve eklerinden talebin reddedilmesi gerektiğinin anlaşıldığı hallerde idarenin savunmasının beklenemeyeceği yönündeki kural, savunma alınmadan dahi yürütmenin durdurulması isteminin yerinde olmadığına anlaşılabildiği hâllerde ayrıca idarenin savunmasının alınması zorunluluğunu ortadan kaldırarak söz konusu kararın verilmesine etkisi olmayacak bir işlem sebebiyle kararın gecikmesinin önlenmesini sağlamaktadır. Bu çerçevede söz konusu kuralın idare lehine bir çifte standart yaratması veya kanun önünde eşitlik veya silahların eşitliği ilkelerine aykırı bir durum yaratması söz konusu değildir. Zira, silahların eşitliği ilkesine aykırı davranıldığına kabul edilebilmesi için davanın tarafları arasında yargılama sırasında usul hükümleri yönünden bir eşitsizlik yaratılması ve taraflardan birine avantaj sağlayacak kurallara yer verilmiş olması gerekir. Oysa dava konusu kuralda, davacı tarafın iddiasına karşı davalı idarenin savunmada bulunma hakkından vazgeçilmesi düzenlenmektedir. Dolayısıyla

kuralda davacı tarafın 'iddia silahına' karşı davalı idarenin belli bir kararla sınırlı da olsa 'savunma silahından' vazgeçilmesi söz konusudur. Burada idare aleyhine dezavantajlı bir durumun yaratılmasından bahsedilebilirse de idarenin savunmasının alınmasından, idare lehine vazgeçildiği; başka bir ifadeyle söz konusu savunma alınmaksızın da talebin reddedilmesi gerektiği dava evrakından anlaşıldığı ve bunun idare aleyhine bir durum yaratması mümkün olmadığı için idare açısından da silahların eşitliği ilkesinin ihlali sonucu doğmaz.

Açıklanan nedenlerle, dava konusu kurallar, Anayasa'nın 2., 10., 36. ve 125. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir.

Mehmet ERTEN, Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŞ maddenin (2) numaralı fıkrasının birinci cümlesinde yer alan "davalı idarenin savunması alındıktan veya savunma süresi geçtikten sonra" ibaresi yönünden bu görüşe katılmamışlardır.

Kuralın Anayasa'nın 153. maddesi ile ilgisi görülmemiştir.

I- Kanun'un 58. Maddesiyle Değiştirilen 2577 Sayılı Kanun'un 28. Maddesinin (2) Numaralı Fıkrası ile (6) Numaralı Fıkrasının İkinci Cümlesinin İncelenmesi:

Dava dilekçesinde, dava konusu kurallarla, borcun alacaklının konutunda ödeneceği yönündeki genel kurala idare lehine istisna getirildiği, Kanun'da mahkeme kararının yerine getirilmesi için düzenlenen otuz günlük sürenin fiilen uzatıldığı ve idarenin temyizi aşamasındaki 'yürütmenin durdurulması' kararlarının uygulanmasına ilişkin olarak idareye ek süre kazandırıldığı, öte yandan, 2577 sayılı Kanun'un 28. maddesinin (1) numaralı fıkrasında mahkeme kararlarının yerine getirilmesi için belirlenen sürenin, iptal ve yürütmenin durdurulması kararları için geçerli olduğu, dolayısıyla belli bir paranın ödenmesine ilişkin davalarda bu sürenin beklenmeksizin idare tarafından ödenmesi gerektiği, oysa dava konusu kuralların bu tür davalar yönünden de otuz günlük süreyi öngördüğü belirtilerek kuralların, Anayasa'nın 2., 36. ve 125. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kurallar, 2577 sayılı Kanun'un 28. maddesinin (2) ve (6) numaralı fıkralarındaki değişiklikleri kapsamaktadır. 2577 sayılı Kanun'un 28. maddesinin (1) numaralı fıkrasının birinci cümlesinde, Danıştay, bölge idare mahkemeleri, idare ve vergi mahkemelerinin esasa ve yürütmenin durdurulmasına ilişkin kararlarının icaplarına göre idarenin, gecikmeksizin işlem tesis etmeye veya eylemde bulunmaya mecbur olduğu belirtilmiş, ikinci cümlesinde ise bu sürenin hiçbir şekilde kararın idareye tebliğinden başlayarak otuz günü geçemeyeceği düzenlenmek suretiyle idareye, yargı kararının gereğini, tebliğ tarihinden itibaren en geç otuz gün içinde yerine getirme yükümlülüğü yüklenmiştir.

Dava konusu (2) numaralı fıkrada ise konusu belli bir miktar paranın ödenmesini gerektiren davalarda hükmedilen miktar ile her türlü davalarda hükmedilen vekâlet ücreti ve yargılama giderleri yönünden bu kurala bir istisna getirilmiştir. Buna göre, konusu belli bir miktar paranın ödenmesini gerektiren davalarda hükmedilen miktar ile her türlü davalarda hükmedilen vekâlet ücreti ve yargılama giderleri, davacının veya vekilinin davalı idareye yazılı şekilde bildireceği banka hesap numarasına, bu bildirim tarihinden itibaren, birinci fıkrada belirtilen usul ve esaslar çerçevesinde yatırılacaktır. Dolayısıyla, konusu belli bir miktar paranın idare tarafından davacıya ödenmesini öngören ilamların icrası, kararın tebliğ tarihinden değil, davacı veya vekilinin banka hesap numarasını idareye bildirdiği tarihten itibaren en geç otuz gün içinde yerine getirilecektir. İdarece, banka hesap numarasının bildirildiği tarihten itibaren otuz gün içinde ödeme yapılmaması durumunda kararın icrası genel hükümler çerçevesinde gerçekleştirilecektir.

Ayrıca, aynı maddenin (6) numaralı fıkrasının birinci cümlesinde, tazminat ve vergi davalarında idarece, mahkeme kararının tebliğ tarihi ile ödeme tarihi arasındaki süreye 6183 sayılı Amme Alacaklarının Tahsil Usulü Hakkında Kanunu'nun 48. maddesine göre belirlenen tecil faizi oranında hesaplanacak faizin ödeneceği belirtilmiş, dava konusu ikinci cümlesinde ise mahkeme kararının davacıya tebliği ile banka hesap numarasının idareye bildirildiği tarih arasında geçecek süre için faiz işlemeyeceği kuralına yer verilmiştir.

Hukuk devletinde, kanun koyucunun, yargılama hukukuna ilişkin kuralları belirleme ve bu çerçevede mahkemelerin kuruluşu, görev ve yetkileri, işleyişi ve yargılama usulleri hakkında Anayasa kurallarına bağlı olmak koşuluyla ihtiyaç duyduğu düzenlemeyi yapma yetkisi bulunduğu gibi mahkeme ilamlarının nasıl icra edileceğine ilişkin kurallar belirleme hususunda da takdir yetkisi bulunmaktadır.

Dava konusu kurallar mahkeme ilamlarının nasıl icra edileceğine ilişkin olup kanun koyucunun bu hususta takdir yetkisine dayanarak düzenlemeler yapmasında Anayasa'nın 2. maddesine aykırı bir yön bulunmamaktadır.

Diğer taraftan, Kanun'un 28. maddesinin dava konusu (2) numaralı fıkrasıyla, mahkeme kararlarının en geç otuz gün içinde yerine getirilmesi yönündeki sürenin başlangıcının, konusu belli bir miktar paranın ödenmesini gerektiren davalarda hükmedilen miktar ile her türlü davalarda hükmedilen vekâlet ücreti ve yargılama giderleri yönünden değiştirildiği açık ise de davacının hesap numarasını idareye zamanında bildirmesi hâlinde bunun mahkeme kararlarının yerine getirilme süresi üzerinde bir etki yaratması mümkün değildir. Zira, alacağın tahsili yönündeki ilamların mahkeme tarafından

idareye tebliğinden önce veya aynı sırada davacının idareye başvurarak hesap numarasını bildirmesi ve söz konusu süreyi mahkeme kararının tebliğinden itibaren başlatması mümkündür.

Davacının hesap numarasını idareye bildirmesi gereği ise, idarenin paranın yatırılacağı davacıya ait hesabı bilemeyeceği ve bu nedenle alacağın tahsilinin gecikmesinden sorumlu tutulmayacağı gerçeği karşısında makul ve ölçülü bir külfettir.

Aynı durum 28. maddenin altıncı fıkrasındaki dava konusu kural yönünden de geçerli olup, tazminat ve vergi davasına ilişkin ilamın mahkeme tarafından idareye tebliğinden önce veya aynı sırada davacının idareye başvurarak hesap numarasını bildirmesi ve tecil faizinin işlemesine ilişkin süreyi mahkeme kararının tebliğinden itibaren başlatması mümkündür.

Bu nedenlerle, dava konusu kuralların Kanun'da otuz gün olarak belirlenen mahkeme kararının yerine getirilme süresini davacının bu husustaki bildirim yükümlülüğünü zamanında yerine getirmesine rağmen fiilen uzatması ve temyiz aşamasındaki yürütmenin durdurulması kararlarının uygulanmasına ilişkin olarak idareye ek süre kazandırması mümkün değildir. Dolayısıyla, kuralların hak arama özgürlüğünü sınırladığından veya yürütmenin durdurulması kararlarının uygulanmasını geciktirdiğinden söz edilemez.

Öte yandan, 2577 sayılı Kanun'un 28. maddesinin (1) numaralı fıkrasında mahkeme kararlarının yerine getirilmesi için belirlenen süre, hiçbir ayırım yapılmaksızın tüm idari yargı kararları için geçerli olup, bu konuda Kanun'da belli bir paranın ödenmesine ilişkin ilamlarda söz konusu sürenin uygulanmayacağını düzenleyen bir hüküm bulunmamaktadır.

Açıklanan nedenlerle, dava konusu kurallar Anayasa'nın 2., 36. ve 125. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Mehmet ERTEN bu görüşe katılmamıştır.

İ- Kanun'un 72. Maddesiyle 2802 Sayılı Kanun'un 37. Maddesinin Birinci Fıkrasına Eklenen (c) Bendinin Birinci Cümlesinde Yer Alan "üstün başarısı ile iç denetim hizmetlerinde yararlı olacağı anlaşılmış bulunanlar arasından" Müsteşarın teklifi üzerine Bakan tarafından atama yapılır.' İbarelerinin İncelenmesi

Dava dilekçesinde, dava konusu kuralda yer alan, iç denetçilerin 'üstün başarısı ile iç denetim hizmetlerinde yararlı olacağı anlaşılmış bulunanlar arasından' seçilmesi biçimindeki kriterin belirsiz olduğu ve bu kavramla kimlerin hangi ölçütlere göre atanacağı hususunda idareye geniş bir takdir hakkı tanındığı belirtilerek kuralın, Anayasa'nın 2. ve 138. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu ibarenin de yer aldığı 2802 sayılı Kanun'un 37. maddesinin (c) bendinde, Adalet Bakanlığı iç denetçiliğine atanma usul ve şartları düzenlenmektedir. Söz konusu bendin dava konusu olmayan bölümlerinde, Adalet Bakanlığı iç denetçiliğine ancak hâkimlik ve savcılık mesleğinde fiilen en az altı yıl görev yapmış kişilerin, muvafakatleri alınmak suretiyle ve 5018 sayılı Kanun'daki atama şartlarına tabi olmaksızın atanacağı kurala bağlanmış, dava konusu ibarede ise söz konusu göreve atanacakların üstün başarısı ile iç denetim hizmetlerinde yararlı olacağı anlaşılmış bulunanlar arasından, Adalet Bakanlığı Müsteşarının teklifi üzerine Adalet Bakanı tarafından atanacağı hükmüne yer verilmiştir.

Anayasa'nın 2. maddesinde yer alan hukuk devletinin temel ilkelerinden biri 'belirlilik ilkesi'dir. Bu ilkeye göre, yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olması, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi gerekir. Ancak gelişen koşul ve durumlara göre sık sık değişik önlemler alma, bunları kaldırma ve süratli biçimde hareket etme zorunluluğunun bulunduğu alanlarda, yasama organının temel kuralları saptadıktan sonra, uzmanlık ve idare tekniğine ilişkin hususları yürütmeye bırakmasında ve yürütme organının yasama organı tarafından çerçevesi çizilmiş alanda genel nitelikte hukuksal tasarruflarda bulunmasında, hukuk devletinin belirlilik ilkesine aykırılık oluşmaz.

2802 sayılı Kanun'un 27. maddesinin (c) bendinde, Adalet Bakanlığı iç denetçiliğine sadece hâkim ve savcıların atanabileceği belirtilmek suretiyle kimlerin atanabileceği, atanacak hâkim ve savcılarının meslekte fiilen en az altı yıl görev yapmış olmaları gerektiği belirtilerek, hangi nitelikleri taşıyan hâkim ve savcıların atanabileceği, bu kişilerin Müsteşarın teklifi üzerine Bakan tarafından atanacağı ve bu atama sırasında 5018 sayılı Kanun'daki atama şartlarına tabi olunmayacağı belirtilmek suretiyle de bu kişilerin hangi usulle atanacağı yönündeki temel kuralların ve yasal çerçevenin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir şekilde belirlendiği görülmektedir.

Söz konusu bentte iç denetçiliğe atanmak için yukarıda belirtilen şartlara ilave olarak, göreve atanacak hâkim ve savcılarının daha önce gösterdikleri üstün başarısı ile iç denetim hizmetlerinde yararlı olacağı anlaşılanlar arasından seçileceği şartına da yer verilmiştir. Ancak, kuralda iç denetim hizmetinde yararlı olmayı sağlayacak üstün başarının ne olduğu tanımlanmamıştır.

Kanunda bu tanıma yer verilmemesi kuralın belirsizlik taşıdığı anlamına gelmemektedir. Zira yukarıda açıklandığı üzere kanun koyucu tarafından söz konusu göreve seçilmek için bulunması gereken temel şartlar zaten belirlenmiştir. 'Üstün başarı' kavramının ne olduğu ise özellikle sabit bir

tanıma bağlanmayarak, iç denetim hizmetinin değişebilecek koşul ve durumlarına göre idareye farklı nitelikler belirleyebilme imkânı sağlanmıştır. Ancak, bu imkân tanınırken yine de idareye sınırsız bir tasarruf alanı bırakılmamış, idarenin söz konusu nitelikleri belirlerken içinde hareket edeceği yasal çerçeve belirlenmiştir. Bu yasal çerçeve 'iç denetim hizmetinde yararlı olmayı sağlayacak üstün başarı' çerçevesidir. Bu çerçeve uyarınca idarenin belirleyeceği niteliklerin iç denetim hizmetiyle ilgisiz başka bir niteliği içermesi mümkün değildir. İdarenin bu yasal çerçeve içerisinde hareket edip etmediği ise idari yargı tarafından her zaman denetlenebilecektir.

Öte yandan, kural uyarınca Adalet Bakanlığı bünyesinde görev yapacak ve Bakanlığın işlem ve faaliyetleri ile adalet hizmetlerini idari yönden denetleyecek iç denetçilerin, hâkim ve savcılık mesleğinde bulunanlar arasından muvafakatleri alınmak suretiyle Adalet Bakanı tarafından atanmasında yargı bağımsızlığı ilkesine de aykırı bir yön bulunmamaktadır. Zira iç denetçiler tarafından ifa edilecek görev yargısal değil idari bir görevdir. Kaldı ki, hâkim ve savcılarının rızaları hilafına bu göreve atanmaları da mümkün değildir. Esasen bu görevi yapacak kişilerin hâkimlik ve savcılık mesleğinden olması ve bunların Adalet Bakanı tarafından atanması, Anayasa'nın 159. maddesinin onikinci fıkrasındaki Anayasal hükmün kanunlaştırılmasından başka bir şey değildir.

Açıklanan nedenlerle, dava konusu kural, Anayasa'nın 2. ve 138. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

J- Kanun'un 75. Maddesiyle 3713 Sayılı Terörle Mücadele Kanunu'nun Başlığı İle Birlikte Değiştirilen 10. Maddesinin İncelenmesi

a- Maddenin Beşinci Fıkrası

aa- Anlam ve Kapsam

Dava konusu kuralda, 3713 sayılı Kanun'un 10. maddesiyle görevli ağır ceza mahkemelerinin görev alanına giren bazı suçlarda uygulanacak azami tutuklama süresi düzenlenmektedir.

Anayasa'nın 19. maddesinde kişi özgürlüğü ve güvenliği hakkını sınırlayan bir tedbir olarak tutuklama kurumuna, bu kurumun uygulanma koşullarına ve sebeplerine yer verilmiş, ancak tutuklama yönünden uygulanması gereken somut bir azami süre belirlenmemiştir. 5271 sayılı Ceza Muhakemesi Kanunu'nun 102. maddesinde, azami tutuklama süreleri düzenlenmiş, böylece tutuklama süresine yasal düzeyde bir üst sınır getirilmiştir.

5271 sayılı Kanun'un 102. maddesinin (1) numaralı fıkrasında, 'Ağır ceza mahkemesinin görevine girmeyen işlerde tutukluluk süresi en çok bir yıldır. Ancak bu süre, zorunlu hallerde gerekçeleri gösterilerek altı ay daha uzatılabilir.' denilmek suretiyle ağır ceza mahkemesinin görevine girmeyen

işlerde tutukluluk süresinin en çok bir yıl altı ay olarak uygulanacağı belirtilmiş; (2) numaralı fıkrasında ise 'Ağır ceza mahkemesinin görevine giren işlerde, tutukluluk süresi en çok iki yıldır. Bu süre, zorunlu hallerde, gerekçesi gösterilerek uzatılabilir; uzatma süresi toplam üç yılı geçemez.' denilmek suretiyle ağır ceza mahkemesinin görevine giren işlerde bu sürenin en fazla beş yıl olarak uygulanacağı kuralına yer verilmiştir.

Dava konusu 10. maddenin beşinci fıkrasında ise genel hüküm niteliği bulunan 5271 sayılı Kanun'un 102. maddesine bir istisna getirilmiş ve 5237 sayılı Türk Ceza Kanunu'nun İkinci Kitap Dördüncü Kısımın Dört, Beş, Altı ve Yedinci Bölümünde tanımlanan, devletin güvenliğine, anayasal düzene ve bu düzenin işleyişine, milli savunmaya ve devletin sırlarına karşı işlenen ve Kanun'un 305.,318., 319., 323., 324., 325. ve 332. maddeler hariç olmak üzere 302. maddesi ile 339. maddesi arasında yer alan suçlarda, 5271 sayılı Kanun'da öngörülen tutuklama sürelerinin iki kat olarak uygulanacağı hüküm altına alınmıştır. Buna göre ağır cezalı suçlarda beş yıl olan azami tutukluluk süresi, dava konusu kuralda sayılan suçlar yönünden on yıl olarak uygulanacaktır.

ab- Anayasa'ya Aykırılık Sorunu

Dava dilekçesinde, dava konusu kuralın sanıkların temel hak ve özgürlüklerini Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olarak sınırlandırdığı belirtilerek kuralın Anayasa'nın 2. ve 13. maddelerine aykırı olduğu ileri sürülmüştür. 6216 sayılı Kanun'un 43. maddesine göre, iptali istenen kural ilgisiz nedeniyle, Anayasa'nın 19. maddesi yönünden de incelenmiştir.

Anayasa'nın 2. maddesinde yer alan hukuk devleti, eylem ve işlemleri hukuka uygun olan, insan haklarına dayanan, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adaletli bir hukuk düzeni kurup bunu geliştirerek sürdüren, Anayasa'ya aykırı durum ve tutumlardan kaçınan, hukuku tüm devlet organlarına egemen kılan, Anayasa ve yasalarla kendini bağlı sayan, yargı denetimine açık olan devlettir.

Anayasa'nın 19. maddesinin birinci fıkrasında herkesin kişi özgürlüğü ve güvenliği hakkına sahip olduğu ilke olarak belirtildikten sonra, ikinci ve üçüncü fıkralarında şekil ve şartları kanunda gösterilmek kaydıyla kişilerin özgürlüğünden mahrum bırakılabileceği durumlar sınırlı olarak sayılmıştır. Dolayısıyla kişilerin özgürlük ve güvenlik hakkının sınırlandırılması, ancak Anayasa'nın anılan maddesi kapsamında belirlenen durumlardan herhangi birinin varlığı hâlinde söz konusu olabilir.

Maddenin üçüncü fıkrasında kişilerin özgürlüklerinden mahrum bırakılabileceği durumlar arasında, kişilerin mahkeme kararına dayalı olarak tutuklanması da sayılmış, böylece tutuklama tedbirine özgürlük ve güvenlik hakkını sınırlayabilen bir istisna niteliği tanınmıştır. Aynı fıkroda bu tedbire hangi koşullarda ve hangi sebeplerle başvurulabileceği de açıklanmıştır. Buna göre, tutuklama ancak suçluluğu hakkında kuvvetli belirti bulunan kişinin kaçmasının veya delilleri karartmasının önlenmesi veya bunlar gibi tutuklamayı zorunlu kılan ve kanunda gösterilen diğer sebeplerin gerçekleşmesi hâlinde hâkim kararıyla uygulanabilecektir.

Öte yandan, özgürlük ve güvenlik hakkının sınırlandırılabilmesi için Anayasa'nın 19. maddesinde belirtilen koşulların yanısıra temel hak ve hürriyetlerin sınırlandırılması rejimini belirleyen Anayasa'nın 13. maddesine de uyulması gerekmektedir. Anayasa'nın 13. maddesi uyarınca kişi hürriyeti ve güvenliği hakkı, Anayasa'nın 19. maddesinde belirtilen nedenlere bağlı olarak, kanunla ve demokratik bir toplumda gerekli olduğu ölçüde sınırlanabilir. Ancak getirilen bu sınırlamalar hakkın özüne dokunamayacağı gibi, Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine de aykırı olamaz.

Ölçülülük ilkesi, amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder. Ölçülülük, aynı zamanda yasal önlemin sınırlama amacına ulaşmaya elverişli olmasını, amaç ve aracın ölçülü bir oranı kapsamasını ve sınırlayıcı önlemin zorunluluk taşımasını da içerir.

Suçluluğu hakkında kuvvetli belirti bulunan kişilerin, belirtilen koşullara ve sebeplere uygun olarak tutuklanabilmesi, adil ve etkili bir yargılamanın sağlanması amacıyla demokratik toplum düzeni bakımından alınması gereken zorunlu tedbirlerdendir. Nitekim tüm çağdaş demokratik devletlerin mevzuatında ve Avrupa İnsan Hakları Sözleşmesi'nde bu tedbire özgürlük ve güvenlik hakkını sınırlayan bir istisna olarak yer verilmiştir. Ancak tutuklama tedbirinin demokratik toplumda gerekli olması yeterli olmayıp ölçülü de olması gerekir. Bu çerçevede adil ve etkili bir yargılamanın sağlanması şeklindeki kamu yararı ile kişilerin özgürlük ve güvenlik hakkı arasında makul bir dengenin kurulması ve tutuklama tedbirinin kişi yönünden bir cezaya dönüşecek şekilde orantısız olarak uygulanmasına izin verilmemesi gerekir.

Anayasa'nın 19. maddesinin yedinci fıkrasının birinci cümlesinde de 'Tutuklanan kişilerin, makul süre içinde yargılanmayı ve soruşturma veya kovuşturma sırasında serbest bırakılmayı isteme hakları vardır.' denilmek suretiyle, kişilerin 'makul süre içinde yargılanma' ve 'makul süreyi aşan sürelerle tutuklu kalmama' hakları anayasal güvenceye bağlanmıştır. Bu çerçevede tutuklama tedbirinin ölçülü olması Anayasa'nın 13. maddesinin olduğu kadar 19. maddesinin de zorunlu bir gereğidir.

Dava konusu kuralda, Türk Ceza Kanunu'nun 305., 318., 319., 323., 324., 325. ve 332. maddeleri hariç olmak üzere, İkinci Kitap Dördüncü Kısımın Dört, Beş, Altı ve Yedinci Bölümünde tanımlanan suçlar yönünden zorunlu sebeplerin bulunması halinde bir kimsenin on yıla kadar tutuklu kalabilmesine izin verilmekte, böylece suçluluğu henüz sabit olmamış kişilerin on yıl gibi uzun bir süre boyunca özgürlüklerinden mahrum bırakılabilmemesine imkân tanınmaktadır.

Ceza hukukunun, toplumun kültür ve uygarlık düzeyi, sosyal ve ekonomik yaşantısıyla ilgili bulunması nedeniyle suç ve suçlulukla mücadele amacıyla ceza ve ceza muhakemesi alanında sistem tercihinde bulunulması devletin ceza siyaseti ile ilgilidir. Bu bağlamda hukuk devletinde, ceza hukukuna ilişkin düzenlemeler bakımından kanun koyucu Anayasa'nın temel ilkelerine ve ceza hukukunun ana kurallarına bağlı kalmak koşuluyla, toplumda belli eylemlerin suç sayılıp sayılmaması, suç sayıldıkları takdirde hangi çeşit ve ölçülerdeki ceza yaptırımlarıyla karşılanmaları gerektiği, hangi hal ve hareketlerin ağırlaştırıcı ya da hafifletici öge olarak kabul edileceği gibi konularda takdir yetkisine sahip olduğu gibi ceza yargılamasına ilişkin kurallar belirleme ve bu çerçevede mahkemelerin kuruluşu, görev ve yetkileri, işleyişi, yargılama usulleri ve yapısı hakkında da Anayasa kurallarına bağlı olmak koşuluyla ihtiyaç duyduğu düzenlemeyi yapma yetkisine sahiptir.

Ceza yargılamasına ilişkin kuralları ve bu kapsamda suç türlerine göre tutukluluk sürelerini belirlemek kanun koyucunun takdir yetkisi kapsamında bulunmakla birlikte, gerek ulusal mevzuatta ve uygulamada gerekse de Avrupa İnsan Hakları Sözleşmesi ve Avrupa İnsan Hakları Mahkemesi kararlarında, ilk derece mahkemelerince sanığın suçlu bulunarak mahkûm edilmesinden sonraki sürecin tutukluluk olarak değerlendirilmediği de nazara alındığında, dava konusu kuralda düzenlenen azami tutukluluk süresinin demokratik bir hukuk devletinde kabul edilemeyecek kadar uzun olduğu, bu yönüyle kuralda tutuklamanın adeta bir ceza olarak uygulanabilmesine imkân tanınarak, tutuklama tedbiriyile ulaşılmak istenen hukuki yarar ile kişi özgürlüğü ve güvenliği hakkı arasındaki makul dengenin kişi özgürlüğü ve güvenliği hakkı aleyhine bozulmasına neden olduğu görülmektedir.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 13. ve 19. maddelerine aykırıdır. İptali gerekir.

b- Maddenin Kalan Bölümü

ba- Anlam ve Kapsam

Dava konusu kuralları içeren 3713 sayılı Kanun'un 'Görev ve yargı çevresinin belirlenmesi, soruşturma ve kovuşturma usulü' başlıklı 10. maddesinde, bazı suçlara mahsus kovuşturma yapmakla görevlendirilen ağır ceza mahkemeleri ile bunların görev alanları ve görev alanına giren suçlarda uygulanacak özel soruşturma ve kovuşturma usulleri düzenlenmektedir.

Maddenin birinci fıkrası ve üçüncü fıkrasının (a) bendi uyarınca, bu mahkemeler yargı çevresi birden fazla ili kapsayacak şekilde kurulmuş olup anılan mahkemelerde görevli hâkimlerin ve söz konusu mahkemelerin görevine giren suçları soruşturmakla görevli savcılarının, başka mahkemelerde veya işlerde görevlendirilmeleri yasaklanmıştır.

Maddenin birinci fıkrası gereği, esas itibarıyla bu mahkemelerin görev alanını 3713 sayılı Kanun kapsamına giren suçlar oluşturmaktadır. Bu suçlar 3713 sayılı Kanun'un 2. ve 3. maddelerinde sayılan terör ve terör amacı ile işlenen suçlardır.

Maddenin dördüncü fıkrasında ayrıca;

-Örgüt faaliyeti çerçevesinde 5237 sayılı Kanun'un 188. maddesinde düzenlenen uyuşturucu ve uyarıcı madde imâl ve ticareti ile 282. maddesinde düzenlenen suçtan kaynaklanan malvarlığı değerini aklama suçları,

-Haksız ekonomik çıkar sağlamak amacıyla kurulmuş bir örgütün faaliyeti çerçevesinde cebir ve tehdit uygulanarak işlenen suçlar,

-5237 sayılı Kanun'un 305., 318., 319., 323., 324., 325. ve 332. maddeler hariç olmak üzere İkinci Kitap Dördüncü Kısımın Dört, Beş, Altı ve Yedinci Bölümünde tanımlanan suçlar,

dolayısıyla açılan davaların da bu mahkemelerde görülmesi kuralına yer verilmiş, ancak terör suçları yönünden bu maddede öngörülen özel soruşturma ve kovuşturma usullerinin bir kısmının bu suçlara ilişkin davalarda uygulanmaması esası benimsenmiştir.

Maddenin birinci ve dördüncü fıkralarında, anılan suçların kovuşturulmasının bu madde uyarınca görevlendirilecek ağır ceza mahkemelerince yürütüleceği belirtildikten sonra, ikinci fıkrasında bu kuralın istisnalarına yer verilmiştir. Buna göre Anayasa Mahkemesinin, Yargıtayın ve askeri mahkemelerin yargılayacağı kişilere ilişkin görev alanlarındaki suçlarda 3713 sayılı Kanun'un 10. maddesi uyarınca görevli mahkemeler değil, anılan mahkemeler kovuşturma yapacaktır.

Maddenin üçüncü fıkrasının (b) bendinde, sadece Türk Ceza Kanunu'nun 302, 309, 311, 312, 313, 314, 315 ve 316. maddelerinde düzenlenen ve görev sırasında veya görevinden dolayı işlenen suçlar

hakkında Cumhuriyet savcılarınca doğrudan soruşturma yapılması kuralı benimsenmiş, bu suçlar dışında kalanlar yönünden ise savcıların doğrudan soruşturma yapma yetkisi kaldırılmıştır.

Doğrudan soruşturma yapılabilecek suçlara yönelik olarak yapılan düzenlemede, 1.11.1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nun 26. maddesi saklı tutulmuştur. Bu çerçevede söz konusu suçların Milli İstihbarat Teşkilatı mensupları veya belirli bir görevi ifa etmek üzere kamu görevlileri arasından Başbakan tarafından görevlendirilenler tarafından görev sırasında işlenmesi hâlinde, bunlar yönünden doğrudan soruşturma yapılamayacağı kuralına yer verilmiştir.

Maddede düzenlenen bir başka husus, yakalanan, gözaltına alınan veya gözaltı süresi uzatılan kişilerin yakınlarına haber verilmesi hakkıyla ilgilidir. Anayasa'nın 19. maddesinde kişinin yakalanması veya tutuklanması halinde bunun derhal yakınlarına bildirilmesi gerektiği kuralına yer verilmiştir. 5271 sayılı Kanun'un 95. maddesinin (1) numaralı fıkrasında ise 'Şüpheli veya sanık yakalandığında, gözaltına alındığında veya gözaltı süresi uzatıldığında, Cumhuriyet savcısının emriyle bir yakınına veya belirlediği bir kişiye gecikmeksizin haber verilir.' denilmek suretiyle Anayasa'da belirtilen bu hakkın ötesine geçilmiş ve kişinin yakını yerine kendisinin belirlediği herhangi bir kişiye de haber verilebilmesi imkânı getirilmiştir. Maddenin dava konusu üçüncü fıkrasının (d) bendinde ise sadece terör suçları yönünden 5271 sayılı Kanun'dan ayrılan özel bir düzenlemeye yer verilmiş ve kişinin belirlediği herhangi bir kişiye haber verilmesinin soruşturmanın amacını tehlikeye düşürebileceği hallerde sadece bir yakınına bilgi verilmesi esası benimsenmiştir. Böylece 5271 sayılı Kanun'la tanınan kişinin yakını dışında kendisinin belirlediği kişiye haber verilmesi terör suçları yönünden ve soruşturmanın amacının tehlikeye düşeceği durumlarda sadece yakınına haber verilmesiyle sınırlandırılmıştır.

Maddenin üçüncü fıkrasının (h) bendinde ise Türk Ceza Kanunu'nun 220. maddesi kapsamındaki iletişimin dinlenilmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi ile gizli soruşturmacı görevlendirilmesi ve teknik araçlarla izleme yapılabilecek suç kataloğuna dâhil bulunmayan bazı suçların terör suçu olması halinde bahsi geçen yöntemlerle takip edilebileceği kuralına yer verilmiştir.

Kural olarak, 5271 sayılı Kanun'un 135., 139. ve 140. maddeleri uyarınca bir şüpheli hakkında iletişimin dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi ile gizli soruşturmacı görevlendirilmesi ve teknik araçlarla izleme yapılması kararı verilebilmesi için, işlendiği iddia olunan suçun söz konusu maddelerde sınırlı sayıda belirtilen katalog suçlardan olması gerekmektedir. Bu katalogda yer alan suçlardan birini de 5237 sayılı Kanun'un 220. maddesinde genel olarak düzenlenen ve bünyesinde birçok suçu barındıran 'suç işlemek amacıyla örgüt kurulması' suçu oluşturmaktadır.

Ancak bahsi geçen iletişimin dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi ile gizli soruşturmacı görevlendirilmesi ve teknik araçlarla izleme yapılması kararları, yasa gereği 220. maddede düzenlenen tüm suçlar için verilememekte sadece örgüt kurmak, örgüt yönetmek ve örgüt adına suç işlemek suçları yönünden verilebilmektedir. Bir başka deyişle, 220. maddede düzenlenen örgüte üye olma, örgüte yardım etme ve örgüt propagandasını yapma suçları, sözü geçen maddelerde belirtilen katalogta bulunmamaktadır. Ancak dava konusu 10. maddenin üçüncü fıkrasının (h) bendinde, suçun terör suçu olması hâlinde 5237 sayılı Kanun'un 220. maddesinde yer alan örgüte üye olma, örgüte yardım etme ve örgüt propagandasını yapma suçları yönünden de söz konusu kararların alınabilmesine imkân tanınmış, böylelikle terör suçları yönünden iletişimin dinlenilmesi, gizli soruşturmacı görevlendirilmesi ve teknik araçlarla izleme yapılması kararı verilebilecek suç kataloğu genişletilmiştir.

Yukarıda belirtilen kurallar dışında maddenin üçüncü fıkrasının;

- (c) bendinde, 3713 sayılı Kanun'un 10. maddesiyle görevli mahkemelerin görev alanına ilişkin olarak yürütülen soruşturmalarda, hâkim tarafından verilmesi gereken tüm kararların Hâkimler ve Savcılar Yüksek Kurulu tarafından sadece bu işle görevlendirilen hâkimler tarafından verileceği,

- (ç) bendinde, 3713 sayılı Kanun'un 10. maddesiyle görevli mahkemelerin görev alanına giren suçlar yönünden, 5271 sayılı Ceza Muhakemesi Kanunu'nun 91. maddesinin birinci fıkrasındaki yirmidört saat olan gözaltı süresinin kırksekiz saat olarak uygulanacağı,

- (e) bendinde, sadece terör suçları yönünden gözaltındaki şüphelinin müdafisi ile görüşme hakkının, Cumhuriyet savcısının istemi üzerine, hâkim kararıyla yirmidört saat süreyle kısıtlanabileceği,

- (f) bendinde, 3713 sayılı Kanun'un 2. ve 3. maddesinde belirtilen terör suçları soruşturmalarında görev alan kolluk görevlileri tarafından düzenlenen tutanaklarda, ilgili görevlilerin açık kimlikleri yerine sadece sicil numaralarının yazılacağı, ayrıca anılan kolluk görevlilerinin ifadesine başvurulması gerektiği hallerde çıkarılan çağrı kâğıtlarının, kolluk görevlisinin iş adresine tebliğ edileceği ve bu kişilere ait ifade ve duruşma tutanaklarında adres olarak yine iş yeri adreslerinin gösterileceği,

- (g) bendinde, 3713 sayılı Kanun'un 10. maddesiyle görevli mahkemelerin görev alanına giren suçların yargılamasına ilişkin olarak güvenlik sorunları söz konusu olduğunda, yargılamayı yapacak mahkemenin güvenliğin sağlanması bakımından duruşmanın başka bir yerde yapılmasına karar verilebileceği,

- (ğ) bendinde, 3713 sayılı Kanun'un 10. maddesiyle görevli mahkemelerin görev alanındaki suçlara ilişkin davaların adli tatile tabi olmayacağı ve adli tatilde de bu davalara bakılmaya devam edileceği, düzenlenmiştir.

Son olarak maddenin altınca fıkrasında, çocuklara ilişkin bir hükme yer verilmiş ve çocukların bu madde hükümleri uyarınca kurulan mahkemelerde yargılanamayacağı ve bu mahkemelere özgü soruşturma ve kovuşturma hükümlerinin çocuklar bakımından uygulanmayacağı belirtilmiştir.

bb- Anayasa'nın 6., 7. ve 11. Maddeleri Yönünden İnceleme

Dava dilekçesinde 7.5.2004 günlü, 5170 sayılı Kanun'un 9. maddesi uyarınca Anayasa'nın 143. maddesinde yapılan değişiklikle, Devlet Güvenlik Mahkemelerinin kaldırıldığı, bu değişiklikten sonra Anayasa'da özel yetkili mahkemelerin kurulmasına imkân tanıyacak anayasal bir dayanağın kalmadığı, dolayısıyla dava konusu kurullarla özel yetkili mahkemelerin kurulmasının, Anayasa'nın bağlayıcılığı ve üstünlüğünü düzenleyen 11. maddesine aykırı olduğu ileri sürülmüştür.

6216 sayılı Kanun'un 43. maddesine göre, iptali istenen kurullar ilgisi nedeniyle, Anayasa'nın 6. ve 7. maddeleri yönünden incelenmiştir.

Anayasa'nın 6. maddesinde hiçbir kimse veya organın kaynağını Anayasa'dan almayan bir devlet yetkisi kullanamayacağı belirtilmiş, 7. maddesinde ise yasama yetkisinin Türk Milleti adına Türkiye Büyük Millet Meclisi'nce kullanılacağı hüküm altına alınmıştır.

Dava konusu kurullarda, belli bazı suçlara bakmak üzere bir ihtisas mahkemesi ve savcılığının görevlendirilmesi ve bunların yargılama usulleri düzenlenmekte olup bu şekilde bir düzenleme yapılabilmesi için Anayasa'da kanun koyucuya yetki veren özel bir hükmün bulunması gerekmektedir. Zira Anayasa'nın 7. maddesi Anayasa'ya aykırı olmamak koşuluyla bu düzenlemeleri de kapsayacak şekilde her türlü düzenlemeyi yapma konusunda kanun koyucuya gerekli yetkiyi vermektedir.

Kaldı ki düzenleme mahkemelerin kuruluşu, görev ve yetkileri, işleyişi ve yargılama usullerine ilişkin olup, Anayasa'nın 142. maddesinde kanun koyucunun söz konusu konularda düzenleme yapma yetkisinin bulunduğu açıkça belirtilmiştir.

Açıklanan nedenlerle dava konusu kurullar, Anayasa'nın 6. ve 7. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kurulların Anayasa'nın 11. maddesiyle ilgisi görülmemiştir.

bc-Anayasa'nın 2., 13., 17., 19., 20., 22., ve 36. Maddeleri Yönünden İnceleme

Dava dilekçesinde, dava konusu kurallarla özel yetkili mahkemelere ve bu mahkemelerin görevleri ile uygulayacağı özel yargılama usullerine yer verildiği, söz konusu kurallarda belirlenen usullerin yargılama makamının yetkilerini artırırken sanıkların temel hak ve özgürlüklerini Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olarak sınırlandırdığı, öte yandan, gözaltındaki şüphelinin müdafii ile görüşme hakkının, yirmidört saat süre ile kısıtlanabileceğini düzenleyen kuralın savunma hakkını kısıtladığı ve bu durumun adil yargılanma hakkı ilkesine aykırı olduğu, ayrıca söz konusu kuralda bu sınırlamayı haklı kılacak bir gereklilik ve aciliyet ölçütüne yer verilmediği, görüşmenin ne zaman engelleneceği ve birden fazla uygulanıp uygulanmayacağına belli olmadığı, dolayısıyla düzenlemenin aynı zamanda kötü muamele yasağına da aykırı olduğu belirtilerek kuralların, Anayasa'nın 2., 13., 17. ve 36. maddelerine aykırı olduğu ileri sürülmüştür.

6216 sayılı Kanun'un 43. maddesi uyarınca, iptali istenen kurallar ilgisi nedeniyle, Anayasa'nın 19., 20. ve 22. maddeleri yönünden de incelenmiştir.

Anayasa'nın 13. maddesinde temel hak ve hürriyetlerin uluslararası sözleşmelerde ve uygulamalarda kabul edildiği üzere mutlak ve sınırsız olmadığı ve bunların çeşitli şartlar altında sınırlandırılabilirliği kabul edilmiştir. Ancak bu hak ve özgürlükler sınırlandırılırken sınırlamanın, Anayasa'nın ilgili maddelerinde belirtilen nedenlere bağlı olarak kanunla yapılması ve hakların özüne dokunmaması, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmaması gerekir.

Bir sınırlamanın hakkın özüne dokunmadığının ve demokratik toplum düzeninin gereklerine uygun olduğunun kabulü için temel hakların kullanılmasını ciddi surette güçleştirip, amacına ulaşmasına engel olmaması ve etkisini ortadan kaldırıcı bir nitelik taşıması gerekir.

Sınırlamanın ölçülülük ilkesine uygun olduğunun kabulü için ise amaç ve araç arasında hakkaniyete uygun bir denge kurması gerekir. Ölçülülük, aynı zamanda yasal önlemin sınırlama amacına ulaşmaya elverişli olmasını, amaç ve aracın ölçülü bir oranı kapsamasını ve sınırlayıcı önlemin zorunluluk taşımasını da içerir.

Öte yandan, temel hak ve özgürlükler ancak Anayasa'nın ilgili maddelerinde belirtilen nedenlere bağlı olarak sınırlandırılabilir. Ancak bu, düzenlendiği maddede hiçbir sınırlama nedenine yer verilmeyen hakların tamamının mutlak olduğunu ve bu hakların hiçbir şekilde sınırlandırılmayacağı anlamını taşımamaktadır. Anayasa Mahkemesinin önceki kararlarında da belirtildiği gibi temel hak ve hürriyetlerin doğasından kaynaklanan bazı sınırları bulunduğu gibi Anayasa'nın başka maddelerinde yer alan kurallar da temel hak ve hürriyetlerin doğal sınırını

oluşturur. Bir başka deyişle, temel hak ve özgürlüklerin kapsamının ve objektif uygulama alanının her bir norm yönünden bağımsız olarak değil Anayasa'nın bütünü içerisindeki anlama göre belirlenmesi gerekir.

Dava konusu kurallarla genel olarak adil ve etkili bir yargılama yapılmasını sağlamak ve böylece suç mağdurlarının hakları ile toplumun huzur ve güvenliğini korumak amacıyla devletin güvenliğine, anayasal düzene ve bu düzenin işleyişine, milli savunmaya ve devletin sırlarına karşı işlenen suçlar ile terör ve örgütlü suçları kovuşturmak üzere ihtisas mahkemeleri ve bu mahkemelerin soruşturmalarını yürütecek savcılıkların kurulduğu ve söz konusu mahkemelerin görev alanına giren suçlara ilişkin olarak bazı hususlarda genel mahkemelerdeki yargılama usullerinden ayrılan usullerin benimsendiği anlaşılmaktadır.

Bu çerçevede maddede;

- Genel mahkemelerde uygulanan yirmidört saatlik gözaltı süresinin, bu mahkemelerin görev alanına tabi suçlarda kırksekiz saat olarak uygulanabileceği,
- Soruşturmanın amacının tehlikeye düşebilecek olması durumunda ve sadece terör suçlarında uygulanmak üzere yakalanan veya gözaltına alınan veya gözaltı süresi uzatılan kişinin durumu hakkında Cumhuriyet savcısının emriyle sadece bir yakınına bilgi verilebileceği,
- Sadece terör suçlarında geçerli olmak üzere, gözaltındaki şüphelinin müdafisi ile görüşme hakkının, Cumhuriyet savcısının istemi üzerine, hâkim kararıyla yirmidört saat süre ile kısıtlanabileceği,
- Bu mahkemelerin görev alanına tabi suçlarda güvenliğin sağlanması bakımından duruşmanın başka bir yerde yapılmasına karar verilebileceği,
- Türk Ceza Kanunu'nun 220. maddesi kapsamındaki iletişimin dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi ile gizli soruşturmacı görevlendirilmesi ve teknik araçlarla izleme yapılabilecek suç kataloğuna dâhil bulunmayan bazı suçların da terör suçu olması halinde bu yöntemlerle takip edilebileceği,

kurala bağlanmıştır.

Bu düzenlemeler arasında bulunan ve maddenin üçüncü fıkrasının (ç) bendinde yer alan gözaltı süresine ilişkin düzenleme, Anayasa'nın 19. maddesinde düzenlenen kişi hürriyeti ve güvenliği hakkına ilişkindir.

Anayasa'nın 19. maddesinin birinci fıkrasında, herkesin kişi özgürlüğü ve güvenliği hakkına sahip olduğu ilke olarak belirlenmiş, ikinci ve üçüncü fıkralarında, maddede belirtilen nedenlerle kişilerin

yakalanabileceği belirtilmek suretiyle gözaltı tedbirine özgürlük ve güvenlik hakkını sınırlayabilen bir istisna niteliği tanınmıştır. Maddenin beşinci fıkrasında ise kişinin bireysel suçlarda en fazla kırksekiz saat, toplu suçlarda ise en fazla dört güne kadar gözaltında tutulabileceği belirtilerek, bizzat Anayasa hükmü tarafından kişinin özgürlük ve güvenlik hakkının bireysel suçlarda en fazla ne kadar süreyle sınırlandırılabilmesi hüküm altına alınmıştır.

Dava konusu kuralın üçüncü fıkrasının (ç) bendinde de azami gözaltı süresi Anayasa'nın 19. maddesinde düzenlendiği şekilde kırksekiz saat olarak belirlenmiştir. Buna göre kuralla düzenlenen gözaltı süresi Anayasa ile uyumludur.

Dava konusu kuralın üçüncü fıkrasının (d) bendi, 'Kişinin yakalandığı ve tutuklandığının yakınlarına haber verilmesi hakkı'na ilişkindir. Bu hak, Anayasa'nın 19. maddesinin altıncı fıkrasında 'Kişinin yakalandığı veya tutuklandığı, yakınlarına derhal bildirilir.' şeklinde düzenlenmiştir.

Dava konusu kuralın üçüncü fıkrasının (d) bendinde yer alan 'Soruşturmanın amacı tehlikeye düşebilecek ise yakalanan veya gözaltına alınan veya gözaltı süresi uzatılan kişinin durumu hakkında Cumhuriyet savcısının emriyle sadece bir yakınına bilgi verilir.' şeklindeki hüküm, Anayasa'nın anılan hükmüyle paralellik arz etmektedir. Anayasa'da haber verilecek yakın sayısına ilişkin herhangi bir düzenlemeye yer verilmediğinden, dava konusu kuralda haber verilecek yakın sayısının bir kişi olarak belirlenmesi hakkın düzenlenmesi niteliğindedir. Genel mahkemelerin görev alanına giren suçlarda kişinin bu hakkını yakınları dışında, yakını olmayan herhangi bir kimse için de kullanmasının mümkün olması, ilgili Anayasa maddesindeki hakkın da bu şekilde yorumlanmasını gerektirmemektedir.

Dava konusu kuralın üçüncü fıkrasının (e) bendinde yer alan gözaltındaki şüphelinin müdafisi ile görüşme hakkının, Cumhuriyet savcısının istemi üzerine, hâkim kararıyla yirmidört saat süre ile sınırlandırılabilmesine ilişkin hüküm, 'müdafisi yardımından yararlanma hakkı'na ilişkindir.

Anayasa'nın 'Hak arama hürriyeti' başlığını taşıyan 36. maddesine 3.10.2001 günlü, 4709 sayılı Kanun ile 'adil yargılanma' ibaresinin eklenmesine ilişkin gerekçede, taraf olduğumuz uluslararası sözleşmelerde de güvence altına alınan adil yargılanma hakkının madde metnine dâhil edildiği vurgulanmıştır. Anılan sözleşmelerden Avrupa İnsan Hakları Sözleşmesi ile bunun uygulanmasına ilişkin Avrupa İnsan Hakları Mahkemesi içtihatlarında, adil yargılanma hakkı kapsamında suç isnat edilen kişinin 'müdafisi yardımından yararlanma hakkı' da yer almaktadır. Dolayısıyla suç isnadı altındaki kişinin müdafisi yardımından yararlanma hakkının, Anayasa'nın 36. maddesi kapsamında korunan bir hak olduğu kuşkusuzdur.

Bu aşamada çözümlenmesi gereken sorun, Anayasa'nın 36. maddesi kapsamında korunan 'müdafî yardımından yararlanma hakkı'nın maddede herhangi bir sınırlandırma nedenine yer verilmemiş olması nedeniyle sınırlandırılıp sınırlandırılmayacağıdır.

Daha önce de belirtildiği üzere, hakkın düzenlendiği ilgili Anayasa maddesinde herhangi bir sınırlama nedenine yer verilmemesi bu maddedeki hakkın sınırsız olduğunu göstermemekte ve söz konusu hak, doğasından kaynaklanan sınırlar veya Anayasa'nın başka maddelerinde yer alan kurallar nedeniyle sınırlandırılabilir.

Anayasa'nın 36. maddesinde düzenlenen adil yargılanma hakkının, müdafî yardımından yararlanma hakkını güvence altına alırken, etkin bir soruşturma ve kovuşturma yapılarak suç mağdurlarının haklarının korunması gereğini dışladığı söylenemez. Bu nedenle etkin bir soruşturma ve kovuşturma yapılarak suç mağdurlarının haklarının korunması için kimi düzenlemeler yapılması mümkündür. Dolayısıyla kuralın Anayasa'nın 13. maddesinde belirtilen 'ilgili Anayasa maddesindeki sınırlama sebebine dayanma zorunluluğu' ölçütüne aykırı bir yönü bulunmamaktadır.

Öte yandan, kuralla bazı suçlar yönünden müdafî yardımından yararlanma hakkına bir sınırlama getirilmekle birlikte, getirilen sınırlamanın söz konusu suçların niteliğinden kaynaklanan bir zorunluluğa dayandığı anlaşılmaktadır. Zira, söz konusu suçlar terör suçları olup, bu suçların kişi hak ve özgürlükleri ile demokratik toplum düzeni ve güvenliği yönünden ortaya çıkardığı tehdidin ağırlığı ile çok failli, organize ve karmaşık yapıları nedeniyle bu suçlara ilişkin delillerin ele geçirilmesi ve bu delillerin karartılmaması ayrı bir önem arz etmekte ve bu durum gözaltına alınan kişilerin belli bir süreyle dış dünyayla olan iletişimlerinin kesilmesini zorunlu kılabilir.

Ancak bu zorunluluğun varlığı tek başına müdafî yardımından yararlanma hakkının sınırlandırılması için yeterli olmamakta, bu sınırlandırmanın hakkın özüne dokunmaması, demokratik toplum düzeni gereklerine ve ölçülülük ilkesine uygun olması için kanunda gerekli önlemlere yer verilmiş olması da gerekmektedir.

Dava konusu kuralda, gözaltına alınan kişinin yirmidört saat süreyle müdafiiyle görüşme hakkı sınırlandırılırken aynı zamanda bu süre boyunca şüpheli veya sanığın savunmasının alınmasının da yasaklandığı, böylece bu kişilerin müdafilerinden hukuki yardım almaksızın savunma yapmalarının önlenmesi görülmektedir.

Müdafî ile görüşülemeyen süre boyunca savunma alınmasının yasaklanmış olması, yapılan sınırlamanın soruşturmanın amacının tehlikeye düşmesini önlemeyi ve maddi gerçeğin ortaya

çkarılmasını amaçladığını göstermekte ve sınırlama aracının sanık veya şüpheli üzerinde baskı unsuru olarak amacı dışında keyfi biçimde kullanılmasını engellemektedir.

Kural gereği gözaltındaki kişinin yirmidört saat süreyle müdafiiyle görüşmesinin yasaklanması ancak hâkim kararıyla mümkün olabilmektedir. Bu durum ise hem gözaltındaki kişinin yirmidört saat süreyle müdafiiyle görüştürülmemesini haklı kılacak olguların varlığını gerektirmekte, hem de söz konusu yasaklamanın gereksiz yere birden fazla kullanılmasını önlemektedir.

Dava konusu kuralda demokratik toplum düzeni bakımından alınması gereken zorunlu tedbir kapsamında bir taraftan müdafii yardımından yararlanma hakkı kısıtlanırken, diğer taraftan belirtilen önlemlerle bu sınırlamanın hakkın özüne zarar vermesi ve keyfi uygulamalara yol açması engellenmiş, aynı zamanda sınırlamanın demokratik toplum düzeni gereklerine ve ölçülülük ilkesine uygun olması da sağlanmıştır.

Dava konusu maddenin üçüncü fıkrasının (g) bendinde, 'Güvenliğin sağlanması bakımından duruşmanın başka bir yerde yapılmasına karar verilebilir.' kuralına yer verilmiştir. Bu kuralda düzenlenen husus bağımsız olarak temel bir hakkın konusu olmayıp, Anayasa'da duruşmanın mutlaka belli bir yerde icra edilmesi zorunluluğunu gerektiren bir hüküm bulunmamaktadır.

Kişinin suç işlemesi halinde yargılanacağı mahkemenin önceden belli olması ve kişinin suç işledikten sonra yargılanacağı mahkemenin değiştirilmemesi hususu ise kanuni hâkim güvencesi ile ilgili olup, dava konusu kuralın bu güvenceyle ilgisi bulunmamaktadır. Zira dava konusu kuralda, suçun kovuşturmasını yapacak hâkimlerin değişmesi öngörülmemekte, sadece güvenlik nedeniyle duruşmanın yapılacağı yerin değişmesi düzenlenmektedir.

Dava konusu kuralın üçüncü fıkrasının (h) bendinde ise iletişimin dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi ile gizli soruşturmacı görevlendirme ve teknik araçlarla izleme yapılabilecek suç kataloğuna dâhil bulunmayan örgüt üyesi olma, örgüte bilerek yardım etme ve örgüt propagandası yapma suçlarının terör suçu kapsamında işlenmesi hâlinde, anılan yöntemlerle takip edilebilmesine imkân tanıyan hüküm yer almaktadır. Bu kural ile 'özel hayatın gizliliği' ve 'haberleşme hürriyeti'ne yönelik sınırlandırmalar yapılmaktadır.

Anayasa'nın 22. maddesinin birinci fıkrasında, 'haberleşme hürriyeti'ne, ikinci fıkrasında ise bu hakkın sınırlandırılması sebeplerine yer verilmiş ve bunlar arasında 'kamu düzeninin korunması ve suç işlenmesinin önlenmesi' de sayılmıştır.

Anayasa'nın 20. maddesinde ise özel hayatın gizliliği hakkına yer verilmiş ve bu hakkın 22. maddede öngörüldüğü gibi 'kamu düzeninin korunması ve suç işlenmesinin önlenmesi' sebepleriyle

sınırlandırılabilceđi belirtilmiřtir. Ancak maddede bu sınırlandırmanın 'arama' tedbirine özgü olarak yapılabileceđi belirtildiđinden, bu sebeplerin dava konusu kural yönünden meřru bir sınırlandırma nedeni olarak kabul edilmesi mümkün görülmemektedir. Buna karřılık, özel hayatın düzenlendiđi maddede dava konusu kuralda belirtilen ceza muhakemesi iřlemleri yönünden özel sınırlama sebeplerine yer verilmediđinin kabulü halinde bile bu hakkın Anayasa'nın 36. maddesi kapsamındaki etkin ve adil bir yargılanma yapılması gerekçesiyle sınırlandırılması mümkün olup kuralda da söz konusu hakkın sınırlandırılma amacının bu olduđu anlařılmaktadır. Dolayısıyla kuralın Anayasa'nın 13. maddesinde belirtilen 'ilgili Anayasa maddesindeki sınırlama sebebine dayanma zorunluluđu' ölçütüne aykırı bir yönü bulunmamaktadır.

Diđer taraftan, kuralla bazı suçlar yönünden özel hayatın gizliliđi hakkına ve haberleřme hürriyetine bir sınırlama getirilmekle birlikte getirilen sınırlama söz konusu suçların niteliđinden kaynaklanan bir zorunluluđa dayanmaktadır. Zira, söz konusu suçlar örgütlü terör suçları olup, bu suçların kiři hak ve özgürlükleri ile demokratik toplum düzeni ve güvenliđi yönünden ortaya çıkardığı tehdidin ađırlığı nedeniyle bu suçlara iliřkin delillerin ele geçirilmesi ve bu delillerin karartılmaması ayrı bir önem arz etmekte ve bu durum kuralda belirtilen suç soruřturmalarında, bazı hallerde iletiřimin dinlenmesi, kayda alınması veya sinyal bilgilerinin deđerlendirilmesi ile gizli soruřturmacı görevlendirilmesi ve teknik takip tedbirine bařvurulması zorunluluđunu ortaya çıkarmaktadır.

Ancak bu zorunluluđuğun varlığı tek bařına özel hayatın gizliliđi hakkının ve haberleřme hürriyetinin sınırlandırılması için yeterli olmamakta, bu sınırlamanın hakkın özüne dokunmaması, demokratik toplum düzeni gereklerine ve ölçünlülük ilkesine uygun olması için kanunda gerekli önlemlere yer verilmiř olması da gerekmektedir.

Dava konusu kural ve 5271 sayılı Kanun'un 135., 139., ve 140. maddeleri incelendiđinde söz konusu güvencelere ayrıntılı bir řekilde yer verildiđi böylece kuralda, demokratik toplum düzeni bakımından alınması gereken zorunlu tedbirler kapsamında bir taraftan özel hayatın gizliliđi hakkı ve haberleřme hürriyeti sınırlandırılırken, diđer taraftan yasada belirtilen önlemlerle sınırlandırmaların hakların özüne dokunmaması ve ölçülü olmasının sađlandığı görülmektedir.

Açıklanan nedenlerle dava konusu kurallar, Anayasa'nın 2., 13.,19., 20., 22. ve 36. maddelerine aykırı deđildir. İptal istemlerinin reddi gerekir.

Maddenin üçüncü fıkrasının (e) bendi yönünden, Mehmet ERTEN, Osman Alifeyyaz PAKSÜT ve Zehra Ayla PERKTAř bu görüşe katılmamıřlardır.

Kuralların, Anayasa'nın 17. maddesi ile ilgisi görülmemiřtir.

bd- Anayasa'nın 10. Maddesi Yönünden İnceleme

Dava dilekçesinde, dava konusu kurallarla bazı suçlar yönünden kişilerin hak ve özgürlüklerinin genel mahkemelerdeki yargılama kurallarına göre daha fazla daraltıldığı belirtilerek kuralların, Anayasa'nın 10. maddesine aykırı olduğu ileri sürülmüştür.

Dava konusu kurallarda, 3713 sayılı Kanun'un 10. maddesiyle görevli mahkemelerin görev alanına giren suçların failleriyle diğer suç failleri arasında bu kişilere uygulanacak ceza yargılaması usullerinde ayrıma gidildiği açık ise de bunun kanun önünde eşitlik ilkesine aykırılık oluşturduğu söylenemez. Zira her iki kategorideki kişilerin hukuksal konumları farklı olup, durumlarındaki farklılık nedeniyle haklarında farklı kurallar uygulanmaktadır.

Açıklanan nedenle dava konusu kuralların, Anayasa'nın 10. maddesine aykırı bir yönü bulunmamaktadır. İptal isteminin reddi gerekir.

be- Anayasa'nın 2., 4. ve 6. Maddeleri Yönünden İnceleme (Maddenin Üçüncü Fıkrasının (b) Bendinin Son Cümlesi Uyarınca 2937 Sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu Yönünden Getirilen İstisna Yönünden)

Dava dilekçesinde, 3713 sayılı Kanun'un 10. maddesinin üçüncü fıkrasının (b) bendinde yer alan dava konusu kuralla, 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu yönünden getirilen istisnanın, devletin bazı işlem ve faaliyetlerinin yargının denetimi dışına çıkarılması ve bir keyfilik ve sorumsuzluk alanı yaratılması sonucunu doğurduğu, bunun ise Anayasa'nın 2. maddesinde güvence altına alınan hukuk devleti ilkesine aykırı olduğu, ayrıca kuralla devletin belli bir alana ilişkin egemenlik yetkisi kullanımının belli kişi, zümre veya sınıfa bırakıldığı ve bazı kişi, zümre veya sınıflara kaynağını Anayasa'dan almayan devlet yetkilerini kullanma yetkisinin verildiği, bunun ise Anayasa'nın değiştirilemeyecek hükümlerini düzenleyen 4. maddesine ve egemenliği düzenleyen 6. maddesine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralda, Türk Ceza Kanunu'nun 302., 309., 311., 312., 313., 314., 315. ve 316. maddelerinde düzenlenen suçlara ilişkin olarak görev sırasında veya görevinden dolayı işlenmiş olsa bile Cumhuriyet savcılarınca doğrudan soruşturma yapılacağı hükmüne yer verilmiş, ancak kuralda 1.11.1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nun 26. maddesi saklı tutulmuştur.

2937 sayılı Kanun'un 'Soruşturma İzni' başlıklı 26. maddesinde, MIT mensuplarının veya belirli bir görevi ifa etmek üzere kamu görevlileri arasından Başbakan tarafından görevlendirilenlerin görevlerini yerine getirirken, görevin niteliğinden doğan veya görevin ifası sırasında işledikleri iddia

olunan suçlardan dolayı ya da 5271 sayılı Kanun'un 250. maddesinin (1) numaralı fıkrasına göre kurulan ağır ceza mahkemelerinin görev alanına giren suçları işledikleri iddiasıyla haklarında soruşturma yapılmasının Başbakan'ın iznine bağlı olduğu hükme bağlanmıştır.

2937 sayılı Kanun'un 26. maddesinin yürürlüğe girmesinden sonra 6352 sayılı Kanun yürürlüğe girmiş ve 105. maddesinin (6) numaralı fıkrası ile 5271 sayılı Kanun'un 250. maddesi yürürlükten kaldırılmıştır. Ancak, anılan Kanun'un geçici 2. maddesinin (7) numaralı fıkrasında, 'Mevzuatta Ceza Muhakemesi Kanununun 250 nci maddesinin birinci fıkrasına göre kurulan ağır ceza mahkemelerine yapılmış olan atıflar, Terörle Mücadele Kanununun 10 uncu maddesinin birinci fıkrasında belirtilen ağır ceza mahkemelerine yapılmış sayılır.' denilmiştir. Dolayısıyla, dava konusu kuraldaki 5271 sayılı Kanun'un 250. maddesinin (1) numaralı fıkrasına yapılan atıf, 3713 sayılı Kanun'un 10. maddesinde belirtilen ağır ceza mahkemelerine yapılmış olmaktadır.

Sonuç itibariyle kuralda, Türk Ceza Kanunu'nun 302., 309., 311., 312., 313., 314., 315. ve 316. maddeleri yönünden getirilen doğrudan soruşturma yapma usulünün 2937 sayılı Kanun'un 26. maddesinde belirtilen kişileri kapsamayacağı yönünde özel bir soruşturma usulü benimsenmektedir.

5271 sayılı Kanun, herkes hakkında geçerli olan ceza soruşturması ve kovuşturması hükümlerini içermektedir. Ancak, kanun koyucu, uluslararası hukuk ve iç hukuktan kaynaklanan kimi nedenlere dayanarak bu genel kurallara istisnalar getirmiştir. Buna göre, suç işleyen her kişi hakkında uygulanması gereken genel düzenlemeleri içeren 5271 sayılı Kanun hükümleri bazı suç failleri bakımından uygulanmayacak, bunlar hakkında ilgili kanunlarındaki özel soruşturma ve kovuşturma usulleri geçerli olacaktır. Bu usullerin tanınması, uygulanacak kişilere bir zümre ya da sınıf olarak imtiyaz tanımak anlamına gelmeyip, yapılan görevin niteliğinden kaynaklanmaktadır. Böylece, hem yapılan görevin en iyi şekilde ve etkin olarak yerine getirilmesi sağlanacak hem de gereksiz şikâyetlere maruz kalınarak görülen hizmetin kesintiye uğraması engellenecektir.

Hukuk devletinde, kanun koyucunun, ceza siyaseti gereği kimlerin özel soruşturma usulüne tabi olacağını belirleme hususunda takdir yetkisi vardır.

Buna göre, MİT mensuplarının veya belirli bir görevi ifa etmek üzere kamu görevlileri arasından Başbakan tarafından görevlendirilenlerin, Türk Ceza Kanunu'nun 302., 309., 311., 312., 313.,314., 315. ve 316. maddelerinde belirtilen suçları işleseler bile haklarında soruşturma yapılmasının Başbakan'ın iznine bağlı tutulması hususunun, kanun koyucunun takdir yetkisi içinde kaldığı açıktır.

Açıklanan nedenlerle dava konusu kural Anayasa'nın 2. maddesine aykırı değildir. İptal isteminin reddi gerekir.

Mehmet ERTEN ve Zehra Ayla PERKTAŞ bu görüşe katılmamışlardır.

Kuralın Anayasa'nın 4. ve 6. maddeleriyle ilgisi görülmemiştir.

K- Kanun'un 77. Maddesiyle 5187 Sayılı Kanun'un 26. Maddesinin Birinci ve Altıncı Fıkralarında Yapılan Değişikliklerin İncelenmesi

Dava dilekçesinde, dava konusu düzenlemelerde basılmış eserler yoluyla işlenen veya 5187 sayılı Kanun'da öngörülen diğer suçlarla ilgili ceza davalarının açılması için öngörülen sürelerin ve bu sürelerin işleminin tabi kılındığı durma süresinin kısa ve yetersiz olduğu, bunun kişilerin hak arama özgürlüklerini sınırlandıracağı, öte yandan Anayasa Mahkemesinin 28.4.2011 günlü, E.2009/66, K.2011/72 sayılı kararıyla basılmış eserler yoluyla işlenen veya 5187 sayılı Kanun'da öngörülen suçlarla ilgili dava açma süresini iki ayla sınırlayan düzenlemeyi iptal ettiği ve bu iptal kararının Anayasa'nın 153. maddesinin altıncı fıkrası uyarınca yasama organı yönünden bağlayıcı olduğu, kanun koyucunun bu bağlayıcılığa rağmen söz konusu süreyi yeniden kısa ve yetersiz olarak düzenlediği belirtilerek kuralların, Anayasa'nın 2., 36. ve 153. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kurallarla, basılmış eserler yoluyla işlenen veya 5187 sayılı Kanun'da öngörülen diğer suçlarla ilgili ceza davalarının açılması için öngörülen hak düşürücü süre, bir muhakeme şartı olarak günlük süreli yayınlar yönünden dört ay, diğer basılmış eserler yönünden ise altı ay olarak belirlenmiş; kamu davasının izin veya karar alınması şartına bağlı tutulduğu suçlarda, izin veya karar için gerekli başvurunun yapılmasından itibaren dava açma süresinin en fazla dört ay süreyle duracağı hükme bağlanmıştır.

Anayasa'nın 2. maddesinde belirtilen hukuk devleti, eylem ve işlemleri hukuka uygun, insan haklarına dayanan, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adaletli bir hukuk düzeni kurup bunu geliştirerek sürdüren, hukuk güvenliğini sağlayan, bütün etkinliklerinde hukuka ve Anayasa'ya uyan, işlem ve eylemleri bağımsız yargı denetimine bağlı olan devlettir. Yasaların kamu yararının sağlanması amacına yönelik olması, genel, objektif, adil kurallar içermesi ve hakkaniyet ölçütlerini gözetmesi hukuk devleti olmanın gereğidir. Bu nedenle kanun koyucunun hukuki düzenlemelerde kendisine tanınan takdir yetkisini anayasal sınırlar içinde adalet, hakkaniyet ve kamu yararı ölçütlerini göz önünde tutarak kullanması gerekir.

Anayasa'nın 'Hak arama hürriyeti' başlıklı 36. maddesinde, herkesin gerekli araç ve yollardan yararlanarak yargı organları önünde davacı ya da davalı olarak iddia ve savunma hakkı bulunduğu belirtilmektedir. Maddeyle güvence altına alınan dava yoluyla hak arama özgürlüğü, kendisi bir

temel hak niteliği taşımasının ötesinde, diğer temel hak ve özgürlüklerden gereken şekilde yararlanılmasını ve bunların korunmasını sağlayan en etkili güvencelerden biridir.

Dava konusu kurallarda düzenlenen dava açma süreleri, ceza muhakemesi şartlarından olup, yargılama usulüne ilişkindir. Anayasa'nın 142. maddesi uyarınca yargılama usulüne ilişkin düzenlemeler yapma ve bu çerçevede basın suçlarında dava açma sürelerini belirleme yetkisi kanun koyucunun takdir yetkisi kapsamında kalmaktadır.

Günümüzde hemen hemen bütün ülkelerin basın kanunlarında, basın davalarında gecikmelerin önlenerek basın özgürlüğünün zedelenmesine engel olmak amacıyla, basın suçlarına ilişkin davaların açılması için özel sürelerle yer verildiği görülmektedir. Dava konusu kurallarda da basılmış eserler yoluyla işlenen veya Basın Kanunu'nda öngörülen diğer suçlardan dolayı bu alanda faaliyet gösterenleri uzun süre ceza tehdidi ile karşı karşıya bırakmamak ve böylece basın özgürlüğünü güvence altına almak amacıyla söz konusu suçlar nedeniyle açılacak davalar için belirli süreler öngörüldüğü anlaşılmaktadır.

Kanun koyucu basın suçlarında dava açılmasını belirli bir süreyle sınırlama konusundaki takdir yetkisini, Anayasa'da belirlenen kurallara bağlı kalmak ve adalet, hakkaniyet ve kamu yararı ölçütlerini gözetmek koşuluyla kullanabilecektir. Bir başka ifadeyle, bir yandan basın mensuplarının uzun süre ceza tehdidi altında bulunmalarına engel olunması, diğer yandan da suçtan mağdur olanların hak arama özgürlüklerinin zarar görmemesi amacıyla basın suçlarında dava açma süresinin makul bir süre olarak belirlenmesi suretiyle, basın hürriyeti ile hak arama hürriyeti arasında adil bir dengenin kurulması gerekir. Yine, basın suçlarında Cumhuriyet savcılığınca resen dava açılmasıyla korunmak istenen hukuki yarar ile basın hürriyetinin korunmasındaki hukuki yarar arasında da makul bir denge bulunmalıdır.

Dava konusu kurallarda, basılmış eserler yoluyla işlenen veya 5187 sayılı Kanun'da öngörülen diğer suçlarla ilgili ceza davalarının açılması için öngörülen hak düşürücü süreler, günlük süreli yayınlar yönünden dört ay, diğer basılmış eserler yönünden ise altı ay olarak belirlenmiştir. Kurallarda belirlenen bu sürelerin hem basın mensuplarının uzun süre ceza tehdidi altında kalmasını önleyen, hem de suçtan mağdur olanların hak arama özgürlüklerini kullanabilmelerine imkân tanıyan makul süreler olduğu görülmektedir. Zira bu süreler, Cumhuriyet savcısının dava açmak üzere gerekli hazırlıkları yapması için yeterli olduğu gibi basın mensuplarının uzun süre ceza tehdidi altında kalmasını önlemeye de elverişlidir.

Diğer taraftan, kamu davasının izin veya karar alınması şartına bağlı tutulduğu suçlarda, izin veya karar için gerekli başvurunun yapılmasından itibaren dava açma süresinin en fazla dört ay süreyle

durmasını düzenleyen kural da hem basın mensuplarının uzun süre ceza tehdidi altında kalmasını önlemeye, hem de dava açma iznini veya kararını verecek mercilere söz konusu kararı vermek üzere yeterli hazırlığı yapma imkânını sağlamaya elverişlidir.

Açıklanan nedenlerle, dava konusu kurallar, Anayasa'nın 2. ve 36. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir.

Kuralın Anayasa'nın 153. maddesiyle ilgisi görülmemiştir.

L- Kanun'un 85. Maddesiyle Değiştirilen 5237 Sayılı Kanun'un 220. Maddesinin (6) Numaralı Fıkrasının İncelenmesi

Dava dilekçesinde, Kanun'un 85. maddesiyle değiştirilen, 5237 sayılı Kanun'un 220. maddesinin (6) numaralı fıkrasının, Anayasa'nın 2., 12., 13., 36., 37., 38., 40. ve 138. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kural, 11.4.2013 günlü, 6459 sayılı İnsan Hakları ve İfade Özgürlüğü Bağlamında Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un 11. maddesi ile değiştirildiğinden, konusu kalmayan kurala ilişkin iptal istemi hakkında karar verilmesine yer olmadığına kararı verilmesi gerekir.

M- Kanun'un 85. Maddesiyle Değiştirilen 5237 Sayılı Kanun'un 220. Maddesinin (7) Numaralı Fıkrasının İncelenmesi

Dava dilekçesinde, dava konusu kuralda, örgüt üyesi olmadığı hâlde örgüte yardım edenlerin hem işledikleri suçtan hem de örgüt üyesi olma suçundan cezalandırılmasının öngörüldüğü, bu durumun ceza hukukunun genel ilkelerine aykırı olduğu, zira, ceza hukukunun genel ilkelerinden 'mükerrer yargılama yasağı' ilkesi uyarınca bir kişinin aynı fiilden dolayı ancak bir kez yargılanıp cezalandırılabileceği, oysa dava konusu kural nedeniyle kişinin mükerrer olarak yargılanmasına ve cezalandırılmasına izin verildiği, örgüte üye olmayan birinin, farazi bir yaklaşımla örgüt üyesi kabul edilmesinin ceza hukukunda kanuni karinelere yer olmadığı ilkesiyle ve dolayısıyla ceza sorumluluğunun şahsiliği ilkesiyle de çeliştiği belirtilerek söz konusu kuralın, Anayasanın 2., 12., 13., 36., 37., 38., 40. ve 138. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralda, örgüt içindeki hiyerarşik yapıya dâhil olmamakla birlikte örgüte bilerek ve isteyerek yardım edenlerin örgüt üyesi olma suçundan cezalandırılacakları ve örgüt üyeliğinden dolayı verilecek cezanın, yapılan yardımın niteliğine göre üçte birine kadar indirilebileceği düzenlenmektedir.

Daha önce de belirtildiği üzere, kanun koyucu, cezalandırma yetkisini kullanırken toplumda hangi eylemlerin suç sayılacağı, bunun hangi tür ve ölçüdeki ceza yaptırımını ile karşılanacağı, nelerin ağırlaştırıcı veya hafifletici sebep olarak kabul edilebileceği konusunda takdir yetkisine sahip bulunmaktadır.

Dava konusu kuralda, örgütlü suçlarla etkin mücadele edilmesinin sağlanması amacıyla örgütün hiyerarşik yapısına dâhil olmasa bile örgütün amacına ulaşmasını sağlamak üzere örgüte bilerek ve isteyerek yardım edenler yönünden bağımsız bir suç tipi oluşturulmakta ve bu fiil örgüte üye olmakla ortaya çıkan tehlikeye eşdeğer görülerek, örgüt üyeliği suçuyla aynı şekilde cezalandırılmaktadır. Dolayısıyla kuralda aynı eyleme ilişkin mükerrer bir yargılama ve cezalandırmanın söz konusu olmadığı açıktır. Bu yönüyle kanun koyucunun izlediği ceza politikası uyarınca yaptığı değerlendirme sonucunda örgüte yardım etme eylemini bağımsız bir suç olarak nitelemesi ve bu eylemi suç olarak tanımladığı başka bir eylemle aynı tehlikede görerek aynı şekilde cezalandırmasında Anayasa'ya ve ceza hukukunun genel ilkelerine aykırı bir yön bulunmamaktadır.

Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2. maddesine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 12., 13., 36., 37., 38., 40. ve 138. maddeleriyle ilgisi görülmemiştir.

N- Kanun'un 90. Maddesiyle Değiştirilen 5237 Sayılı Kanun'un 277. Maddesi ve 93. Maddesiyle Değiştirilen 5237 Sayılı Kanun'un 288. Maddesinin İncelenmesi

Dava dilekçesinde, dava konusu kurallarla, 5237 sayılı Kanun'un 277. ve 288. maddelerindeki suçların yeniden düzenlendiği; 277. maddede, önceki düzenlemede suçun maddi unsurları arasında sayılan 'emir vermek, baskı yapmak, nüfuz icra etmek' gibi ibarelere yer verilmediği, bunun ise yargılamanın belirli güç odakları karşısında adil bir şekilde görülmesini sağlama imkânını ortadan kaldırdığı, düzenlemeyle suçun manevi unsurlarında da ciddi değişiklikler yapılarak failin saikine dair çok sayıda belirleme yapıldığı, bunun da suçun oluşumunu neredeyse imkansız hâle getirdiği, maddede yer alan 'bir haksızlık oluşturma' kavramının belirsiz olduğu, maddenin ikinci fıkrasındaki fikri içtimaya ilişkin hükmün, 5237 sayılı Kanun'un genel hükümlerinde düzenlenen fikri içtima kuralıyla çeliştiği, 277. ve 288. maddelerde düzenlenen suçların benzer olmasına rağmen bu suçların cezaları arasında ciddi farklılıklara gidilmesinin yerinde olmadığı, öte yandan 288. maddedeki suçun belirsiz ve cezasının fazla olması nedeniyle bir çok vesileyle kişilerin bu suçlamayla karşılaşabileceği, maddede bilirkişiyi, hâkimleri ve mahkeme kararını eleştirmenin suç hâline getirildiği, dolayısıyla düzenlemelerle bir bütün olarak hukuk devleti ve hukuk güvenliği ilkelerinin zedelendiği ve yargı

bağımsızlığının devlete karşı korunması gereğinin ihmal edildiği belirtilerek kuralların Anayasa'nın 2., 5., 6., 9., 37. ve 138. maddelerine aykırı olduğu ileri sürülmüştür.

5237 sayılı Kanun'un 'Yargı görevi yapanı, bilirkişiyi veya tanığı etkilemeye teşebbüs' başlıklı 277. maddesinde, görülmekte olan bir davada veya yapılmakta olan bir soruşturmada, gerçeğin ortaya çıkmasını engellemek veya bir haksızlık oluşturmak amacıyla, davanın taraflarından birinin, şüphelinin, sanığın, katılanın veya mağdurun lehine veya aleyhine sonuç doğuracak bir karar vermesi veya bir işlem tesis etmesi ya da beyanda bulunması için, yargı görevi yapanı, bilirkişiyi veya tanığı hukuka aykırı olarak etkilemeye teşebbüs eden kişinin, iki yıldan dört yıla kadar hapis cezası ile cezalandırılacağı ve maddede belirtilen suçu oluşturan fiilin başka bir suçu da oluşturması hâlinde, fikri içtima hükümlerine göre verilecek cezanın yarısına kadar artırılacağı düzenlenmektedir.

Kanun'un 'Adil yargılamayı etkilemeye teşebbüs' başlıklı 288. maddesinde ise görülmekte olan bir davada veya yapılmakta olan bir soruşturmada hukuka aykırı bir karar verilmesi veya bir işlem tesis edilmesi ya da gerçeğe aykırı beyanda bulunulması için, yargı görevi yapanı, bilirkişiyi veya tanığı hukuka aykırı olarak etkilemek amacıyla alenen sözlü veya yazılı beyanda bulunanların elli günden az olmamak üzere adli para cezası ile cezalandırılacağı hükme bağlanmıştır.

Anayasa'nın 2. maddesinde hukuk devleti, 138. maddesinde ise mahkemelerin bağımsızlığı ilkeleri düzenlenmiştir. Hukuk devleti ilkesinin temel unsurlarından olan yargı bağımsızlığı, insan haklarının ve özgürlüklerinin en etkin güvencesidir. Mahkemelerin bağımsızlığı, hâkimin, çekinmeden ve endişe duymadan, Anayasa'nın öngördüğü gereklerden başka herhangi bir dış etki altında kalmadan, yansız tutumla, özgürce karar verebilmesidir. Bağımsızlığın, demokratik bir toplumda, devlet yapısı içinde tüm kurum ve kuruluşlar ile kişilere karşı düşünülüp sağlanması gerekir.

Dava konusu kurallarda, yargının herhangi bir dış etki altında kalmasını önlemek ve adil bir şekilde işlemlerini sağlamak üzere yargı görevini yapanlar ile bu süreçte yer alan ve yargı kararının ortaya çıkmasına katkı sağlayan kişilere yönelik etkileme fiillerinin, suç olarak düzenlendiği görülmektedir.

Daha önce de belirtildiği üzere hukuk devletinde ceza siyasetinin ve bu siyasetin unsurlarının belirlenmesi yetkisi kanun koyucuya aittir. Dolayısıyla kanun koyucunun bu yetkiye istinaden dava konusu kurallarla genel olarak adil yargılama yapılması ve maddi gerçeğe ulaşılmasını önlemeye yönelik yargıyı etkileme suçlarını yeniden düzenlemesinde ve bu düzenlemeyi yaparken suçun maddi ve manevi unsurları ile bunlar için öngörülen cezaları, izlediği ceza siyaseti uyarınca ihtiyaç duyduğu şekilde belirlemesinde hukuk devleti ilkesine aykırı bir yön bulunmamaktadır.

Öte yandan, daha önce 277. maddedeki suçun maddi unsurları arasında sayılan 'emir vermek, baskı yapmak, nüfuz icra etmek' gibi ibarelere, yeni düzenlemede yer verilmemiştir. Ancak kuralda bu ibarelere yer verilmemesi, bu yöntemlerle yapılacak yargılamayı etkileme girişimlerini suç olmaktan çıkarmamaktadır. Zira yeni düzenlemede anılan ibarelere yer verilmemişse de yargı görevi yapan kişileri, 'hukuka aykırı olarak etkilemek' şeklindeki suçun maddi unsurunda herhangi bir değişiklik yapılmamış ve bu unsur aynen korunmuştur. Hukuka aykırı olarak yargı görevi yapanları etkileme ise bu görevi yapanlara emir verme, baskı yapma veya nüfuz icra etmeyi de içeren geniş bir kavramdır. Dolayısıyla söz konusu ibarelerin madde metninden çıkarılmasının, maddenin uygulanmasında herhangi bir farklılık yaratması ve dava dilekçesinde ileri sürüldüğü gibi yargılamanın belirli güç odakları karşısında adil bir şekilde görülmesini sağlama imkânını ortadan kaldırması söz konusu değildir.

Dava konusu kurallarla 277. maddedeki suçun manevi unsurlarında yapılan değişikliklerin, suçun oluşumunu imkânsız hale getirmesi de söz konusu değildir. Zira suçun oluşumu için kuralda aranan 'failin gerçeğin ortaya çıkmasını engellemek veya bir haksızlık oluşturmak amacıyla, davanın taraflarından birinin aleyhine sonuç doğuracak bir karar verilmesi veya bir işlem tesis edilmesi ya da beyanda bulunulmasını sağlamak' şeklindeki özel kast, suçla korunmak istenen hukuki değerle uyum içerisinde olup bunun, suçun oluşumunu imkânsız hale getirdiği söylenemez.

Dava konusu 277. maddede yer alan 'suçun haksızlık oluşturmak amacıyla işlenmesi' şeklindeki unsurunun da açık, net, anlaşılır ve uygulanabilir olduğu görülmektedir. Anılan unsurun soyut olduğu ileri sürülebilirse de hukuk kurallarının kapsayıcı olma zorunluluğunun, onların belli bir düzeyde soyut olmalarını gerektirdiği ve bunun hukuk kurallarının belirsiz olması sonucunu doğurmayacağı açıktır.

Türk Ceza Kanunu'nda özel hükümlerle genel hükümlerden ayrılan özel düzenlemeler yapılabilir. Anayasa'da bu tür özel düzenlemeler yapılmasını engelleyen bir hüküm bulunmamakta ve kanun koyucunun güttüğü ceza siyaseti uyarınca ceza hukukuna ilişkin kuralları belirlemede takdir yetkisi bulunmaktadır.

Esasen Türk Ceza Kanunu sistematigi uyarınca genel hükümler, ancak özel hükümlerde bir düzenleme bulunmaması halinde uygulama kabiliyeti bulmaktadır. Dolayısıyla bazı suçlar yönünden fiilin işlenmesiyle birden fazla suçun oluştuğu durumlarda sadece söz konusu suçlar arasında en ağır cezayı gerektiren suçun cezasıyla failin cezalandırılması, Türk Ceza Kanunu sistematigine uygun bir düzenleme olup bunun herhangi bir çelişkiye meydan vermesi söz konusu değildir.

Ayrıca, dava konusu 288. madde de yer alan; görülmekte olan bir davada veya yapılmakta olan bir soruşturmada hukuka aykırı bir karar verilmesi veya bir işlem tesis edilmesi ya da gerçeğe aykırı beyanda bulunulması için, yargı görevi yapanı, bilirkişiyi veya tanığı hukuka aykırı olarak etkilemek amacıyla alenen sözlü veya yazılı beyanda bulunmak, şeklindeki suçun maddi ve manevi unsurları herhangi bir duraksamaya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir niteliktedir.

Bu kuralla, soruşturma ve kovuşturma ile ilgili yapılan her türlü açıklama değil, sadece hukuka aykırı yapılan açıklamalar suç olarak düzenlenmiştir. Bu çerçevede kural uyarınca düşünce ve ifade özgürlüğü veya basın özgürlüğü hakkına dayalı olarak eleştiri amacıyla yapılan açıklamalar suç oluşturmamakta, sırf yargı görevi yapanın, bilirkişinin ve tanığın hukuka aykırı bir işlem tesis etmesi veya gerçeğe aykırı beyanda bulunmasını sağlamak üzere özel kastla yapılan açıklamalar cezalandırılmaktadır. Bu yönüyle dava dilekçesinde ileri sürüldüğü gibi kuralın, bilirkişileri, hâkimleri ve mahkeme kararlarını eleştirmeyi suç haline getirmesi söz konusu değildir.

Sonuç itibarıyla dava konusu kurallarda, herhangi bir belirsizliğin bulunmaması nedeniyle, hukuk güvenliği ilkesine ve yargı bağımsızlığına aykırı bir yön bulunmamaktadır.

Açıklanan nedenlerle dava konusu kurallar, Anayasa'nın 2. ve 138. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralların Anayasa'nın 5., 6., 9. ve 37. maddeleriyle ilgisi görülmemiştir.

O- Kanun'un 92. Maddesiyle Değiştirilen 5237 Sayılı Kanun'un 285. Maddesinin (1), (2), (5) ve (6) Numaralı Fıkralarının İncelenmesi

Dava dilekçesinde, 285. maddedeki soruşturmanın gizliliğini ihlal suçunun yeniden düzenlendiği, bu düzenleme yapılırken suç için öngörülen cezanın hapis veya para cezası olmak üzere seçimlik olarak belirlendiği, bunun ise cezada bir orantısızlığa sebebiyet verdiği, maddede suçun unsurları arasında sayılan 'suçlu sayılmama karinesinden yararlanma hakkının ihlali' ve 'maddi gerçeğin ortaya çıkmasını engellemeye elverişli olma' gibi unsurların soyut olduğu ve bunların maddenin uygulanma alanını belirsizleştirdiği, bu unsurlarla birlikte suçun, basın özgürlüğü ve lekelenmeme hakkını etkin bir şekilde koruma imkânını ortadan kaldırdığı ve keyfilige neden olduğu, çünkü söz konusu unsurların bazen bir soruşturmaya ilgili herhangi bir haberin 'suçlu sayılmama karinesinden yararlanma hakkının ihlali' gerekçesiyle suç sayılması, bazen de soruşturmaya ilgili yapılan sistematik yayınların 'maddi gerçeğin ortaya çıkmasını engellemeye elverişli' olmadığı gerekçesiyle suç sayılmaması gibi istenmeyen sonuçlara sebebiyet verebileceği, maddede, suçun oluşumunun haberleşmenin ya da özel hayatın gizliliğinin ihlal edilmesi şartına bağlanmasının yerinde olmadığı,

zira bu hususların 5237 sayılı Kanun'da başka suçlar olarak öngörüldüğü ve bunların koruduğu hukuki değerlerin farklı olduğu, maddenin birinci fıkrasında üçüncü kişiler yönünden soruşturmanın gizliliğinin ihlal edilmesi suçunun; ikinci fıkrasında ise taraflar yönünden gizliliğin ihlal edilmesi suçunun düzenlendiği, ancak bu düzenleme yapılırken asıl ihlali oluşturan birinci fıkradaki suçun aksine istisnai ihlali oluşturan ikinci fıkradaki suçun kolayca gerçekleşecek şartlara bağlanıp ağır şekilde cezalandırıldığı, bunun dürüst yargılama ilkesine aykırı olduğu, maddede soruşturma ve kovuşturma evresinde kişilerin suçlu olarak algılanmalarına yol açacak şekilde görüntülerinin yayınlanmasının cezalandırıldığı, oysa görüntülerin yayınlanması dışındaki yöntemlerle de kişilerin suçlu olarak algılanmasına sebep olunabileceği, suçun basın ve yayın yoluyla işlenmesi halinde cezanın artırılacağına ilişkin hükme yeni düzenlemede yer verilmediği, bunun ise suçun basın ve yayın yoluyla işlenmesi ile bu vasıtalar olmaksızın işlenmesini aynı düzeye indirmediği, oysa suçun basın ve yayın yoluyla işlenmesi hâlinde korunan hukuki menfaat bakımından çok daha ağır bir tehlikenin ortaya çıktığı, bu yönüyle düzenlemenin eksik olduğu belirtilerek kuralların, Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüştür.

5237 sayılı Kanun'un dava konusu 285. maddesinin (1) numaralı fıkrasında, soruşturmanın tarafları dışındaki kişilere karşı gizli tutulan soruşturma işlemleri ile ilgili gizliliğin ihlali suçu düzenlenmektedir. Buna göre, maddi gerçeğin ortaya çıkmasını engellemeye elverişli olacak şekilde, soruşturma evresinde yapılan işlemin içeriğini alenen açıklayarak suçlu sayılmama karinesinden yararlanma hakkını veya haberleşmenin ya da özel hayatın gizliliğini ihlal eden kişi bir yıldan üç yıla kadar hapis veya adli para cezası ile cezalandırılacaktır.

Maddenin (2) numaralı fıkrasında ise soruşturmanın taraflarına karşı gizli tutulan işlemlere ilişkin gizliliğin ihlali suçu düzenlenmektedir. Bu fıkrada soruşturma evresinde alınan ve soruşturmanın tarafı olan kişilere karşı gizli tutulması gereken kararların ve bunların gereği olarak yapılan işlemlerin gizliliğini ihlal eden kişinin, bir yıldan üç yıla kadar hapis veya adli para cezası ile cezalandırılacağı öngörülmüştür.

Maddenin dava konusu (5) numaralı fıkrasında, soruşturma ve kovuşturma evresinde kişilerin suçlu olarak algılanmalarına yol açacak şekilde görüntülerinin yayınlanması hâli de ayrı bir suç tipi olarak düzenlenmiş ve kuralda bu eylemin altı aydan iki yıla kadar hapis cezasıyla cezalandırılacağı belirtilmiştir.

Maddenin dava konusu (6) numaralı fıkrası ise soruşturma ve kovuşturma işlemlerinin haber verme sınırları aşılmaksızın haber konusu yapılmasının suç oluşturmayacağı kuralını içermektedir.

Hukuk devletinde, ceza ve ceza yargılamasına ilişkin kurallar, ceza hukukunun ana ilkeleri ile Anayasa'nın konuya ilişkin kuralları başta olmak üzere, ülkenin sosyal, kültürel yapısı, etik değerleri ve ekonomik hayatın gereksinimleri göz önüne alınarak saptanacak ceza siyasetine göre belirlenir. Bu çerçevede kanun koyucu, cezalandırma yetkisini kullanırken 'soruşturmanın gizliliğini ihlal' başlığı altında çeşitli suç tipleri düzenleyebileceği gibi bu suç tiplerini düzenlerken bunların maddi ve manevi unsurlarını, ağırlaştırıcı ve hafifletici nedenlerini, hangi eylemlerin bu kapsamda kalıp kalmayacağını, bu suçlar için öngörülecek cezanın türünü, ağırlığını ve cezanın seçimlik olup olmayacağını izlediği ceza politikası uyarınca ihtiyaç duyduğu şekilde düzenleyebilir.

5237 sayılı Kanun'un 285. maddesinin dava konusu (1) numaralı fıkrasında yer alan suçun oluşabilmesi için, soruşturma evresindeki işleme ilişkin yapılan aleni açıklamanın 'maddi gerçeğin ortaya çıkmasını engellemeye elverişli olma'sı yeterli olmayıp açıklamayla aynı zamanda 'suçlu sayılmama karinesinden yararlanma' veya 'haberleşmenin gizliliği' ya da 'özel hayatın gizliliği'nin ihlal edilmesi de gerekmektedir. Bu yönüyle kuralda suçun hangi koşullarda oluşacağı açık olup, dava dilekçesinde ileri sürüldüğü üzere kuralın herhangi bir belirsizliğe veya keyfiliğe yol açması söz konusu değildir.

5237 sayılı Kanun'da haberleşmenin ve özel hayatın gizliliğinin ihlal edilmesi fiillerinin bağımsız suçlar olarak düzenlenmesi sebebiyle bunların dava konusu suçun unsurlarını oluşturmasında da Anayasa'ya aykırı bir yön bulunmamaktadır. Zira kanun koyucu, izlediği ceza siyaseti doğrultusunda farklı hukuki yararları gerçekleştirmek üzere suçun unsurlarını ihtiyaç duyduğu şekilde düzenleyebilir. Kaldı ki, 5237 sayılı Kanun'un genel hükümlerinde bu tür durumlarda hangi suça ilişkin kanun maddesinin uygulanacağına ilişkin kurallara yer verilmiş olup bu durumun herhangi bir karışıklığa ve belirsizliğe neden olması söz konusu değildir.

Açıklanan nedenlerle dava konusu kurallar, Anayasa'nın 2. maddesine aykırı değildir. İptal isteminin reddi gerekir.

Ö- Kanun'un 95. Maddesiyle, 4.12.2004 Günlü, 5271 Sayılı Ceza Muhakemesi Kanunu'na Eklenen 38/A Maddesinin İncelenmesi

Dava dilekçesinde, Kanun ile 5271 sayılı Kanun'a 38. maddesinden sonra gelmek üzere 'Elektronik işlemler' başlığıyla 38/A maddesinin eklendiği, elektronik işlemler konusunun Ceza Muhakemesi Kanunu'nda düzenlenmesinin yersiz olduğu, maddeyle güvenli elektronik imza ile imzalanmış belge ile ıslak imzalı belgenin içeriğinin çelişmesi hâlinde Ulusal Yargı Ağı Bilişim Sisteminde kayıtlı olan güvenli elektronik imzalı nüshanın geçerli kabul edileceği yönünde ispat bakımından karineler oluşturulmasının, ceza muhakemesindeki 'delillerin serbestliği' ilkesiyle çeliştiği, halen Ulusal Yargı

Ađı Biliřim Sistemi'nin idarenin bir unsuru olan Adalet Bakanlıđı Bilgi İřlem Dairesi Bařkanlıđı tarafından yonetildiđi, bunun bütun adli verilerin siyasi iktidarın eline geçmesi sonucunu dođurduđu, dava konusu maddeyle bu fiili durumun yasallařtırıldıđı ve bađımsız yargı organlarının elinde bulunması gereken adli verileri elde tutma yetkisinin yürütmenin bir unsuru olan Adalet Bakanlıđına devredildiđi, bunun ise yürütmeye, adli verilere, dolayısıyla adalet dađıtımına nüfuz etme imkanını sađladıđı, bu durumun 'güçler ayrılıđı' ilkesine ters düřtüđu belirtilerek dava konusu kuralların, Anayasa'nın Bařlangıç'ı ile 2., 6., 7., 8., 9. ve 138. maddelerine aykırı olduđu ileri sürülmüřtür.

5271 sayılı Kanun'un dava konusu 38/A maddesinde, ceza muhakemesi iřlemlerinin elektronik ortamda gerçekteřtirilmesi, kaydedilmesi ve saklanması ile bu hususların tabi olduđu kurallar düzenlenmektedir.

Bu çerçevede dava konusu maddenin;

(1) numaralı fıkrasında, UYAP sisteminin ceza muhakemesi alanındaki her türlü iřlemde kullanılması ve anılan iřlemlere iliřkin her türlü veri, bilgi, belge ve kararın UYAP sistemi aracılıđıyla elektronik ortama aktarılması, kaydedilmesi ve saklanması,

(2) numaralı fıkrasında, kanunlarda gösterilen istisnalar hariç olmak üzere, ceza mahkemesi dosyalarının güvenli elektronik imza kullanılarak UYAP'tan incelenebilmesi ve her türlü ceza muhakemesi iřleminin elektronik imza ile gerçekteřtirilebilmesi,

(3) numaralı fıkrasında, 5271 sayılı Kanun kapsamında fiziki olarak hazırlanması öngörülen her türlü belge ve kararın elektronik ortamda düzenlenebileceđi, iřlenebileceđi, saklanabileceđi ve elektronik imza ile imzalanabileceđi,

(4) numaralı fıkrasında, güvenli elektronik imza ile imzalanan belge ve kararların diđer kiři veya kurumlara elektronik ortamda gönderileceđi, güvenli elektronik imza ile imzalanarak gönderilen belge veya kararların, gerekmedikçe fiziki olarak ayrıca düzenlenmeyeceđi ve ilgili kurum ve kiřilere gönderilmeyeceđi,

(5) numaralı fıkrasında, elektronik imzalı belgenin elle atılan imzalı belgeyle çeliřmesi halinde UYAP'ta kayıtlı olan elektronik imzalı belgenin geçerli kabul edileceđi,

(6) numaralı fıkrasında, güvenli elektronik imza ile imzalanan belge ve kararlarda, mühürleme iřlemine gerek olmadıđı ve kanunlarda birden fazla nüshanın düzenlenmesini öngören hükümlerin söz konusu belge ve kararlarda uygulanmayacađı,

(7) numaralı fıkrasında, zorunlu nedenlerle fiziki olarak düzenlenmiş belge veya kararların, yetkili kişilerce taranarak UYAP'a aktarılacağı ve gerektiğinde ilgili birimlere elektronik ortamda gönderileceği,

(8) numaralı fıkrasında, elektronik ortamdan fiziki örnek çıkartılması gereken hallerde söz konusu örneğin geçerli olabilmesi için yerine getirilmesi gereken koşullar, bu çerçevede UYAP sisteminden çıkartılan belgenin geçerli olabilmesi için bunun aslının aynı olduğu belirtilmek suretiyle konusuna göre ilgili hâkim, Cumhuriyet savcısı veya görevlendirilen yetkili kişi tarafından imzalanıp, mühürlenmesi gereği,

(9) numaralı fıkrasında, elektronik ortamda yapılan işlemlerde sürenin fiziki ortamda yapılan işlemlerden farklı olarak mesai saati bitiminde değil, gün sonunda biteceği,

(10) numaralı fıkrasında, yargı birimlerinin ihtiyaç duyduğu nüfus, tapu, adlî sicil kaydı gibi dış bilişim sistemlerinden UYAP vasıtasıyla temin edilen bilgi, belge ve kayıtların, zorunlu olmadıkça ayrıca fiziki olarak istenilmeyeceği ve UYAP'tan dış bilişim sistemlerine gönderilen bilgi ve belgelerin de yine zorunlu olmadıkça fiziki ortamda ayrıca gönderilmeyeceği,

düzenlenmektedir.

Maddenin (11) numaralı fıkrasında ise ceza muhakemesi işlemlerinin UYAP'ta yapılmasına dair usul ve esasların, Adalet Bakanlığı tarafından çıkarılacak yönetmelikle düzenleneceği kuralına yer verilmiştir.

Anayasa'nın 7. maddesinde yasama yetkisinin Türkiye Büyük Millet Meclisi, 8. maddesinde yürütme yetkisinin Cumhurbaşkanı ve bakanlar kurulu, 9. maddesinde yargı yetkisinin bağımsız mahkemeler tarafından kullanılacağı belirtilmiş, Başlangıç'ında ise erkler arasındaki kuvvetler ayrımının, devlet organları arasında üstünlük sıralaması anlamına gelmeyip, belli devlet yetki ve görevlerinin kullanılmasından ibaret ve bununla sınırlı medeni bir işbölümü ve işbirliği olduğu ve üstünlüğün ancak Anayasa ve kanunlarda olduğu hükmüne yer verilmiştir. Anayasa'nın 138. maddesinde ise mahkemelerin bağımsızlığı güvence altına alınmıştır.

Hukuk devletinde kanun koyucunun ceza yargılamasına ilişkin kurallar belirleme, bu çerçevede mahkemelerin kuruluşu, görev ve yetkileri, işleyişi ve yargılama usulleri hakkında Anayasa kurallarına bağlı olmak koşuluyla ihtiyaç duyduğu düzenlemeyi yapma hususunda takdir yetkisi bulunmaktadır.

Ceza muhakemesi işlemlerinin elektronik işlemler bağlamında nasıl işleyeceğine ve hangi kurallara tabi olacağı hususlarını düzenleyen dava konusu kurallar da mahkemelerin yargılama usulü ve

işleyişi kapsamında kalmakta olup kuşkusuz kanun koyucu bu hususlarda da Anayasa'ya aykırı olmamak kaydıyla ihtiyaç duyduğu düzenlemeyi yapabilir.

Maddi gerçeğe ulaşılmasını sağlamada önemli bir rol oynayan 'delil serbestliği' ilkesi uyarınca kanuna aykırı olarak elde edilmemesi koşuluyla, ceza muhakemesinde her şeyin delil olması mümkündür. Nitekim 5271 sayılı Ceza Muhakemesi Usulü Kanunu'nun 206. maddesinin (2) numaralı fıkrasında hangi delillerin reddolunacağı sınırlı sayıda belirtilmek suretiyle ceza muhakemesinde her şeyin delil olabileceği kabul edilmiş, 217. maddesinin (1) numaralı fıkrasında ise delillerin hâkimin vicdanî kanaatiyle serbestçe takdir edileceği hükmüne yer verilmiştir.

5271 sayılı Kanun'un 38/A maddesinin dava konusu (5) numaralı fıkrasında, güvenli elektronik imza ile imzalanmış belge ile elle atılan imzalı belgenin içeriğinin çelişmesi hâlinde, Ulusal Yargı Ağı Bilişim Sisteminde kayıtlı olan güvenli elektronik imzalı nüshanın geçerli kabul edileceği kuralına yer verilmiştir. Ancak bu kural elektronik imzalı belge ile ıslak imzalı belge arasında fark bulunması hâlinde elektronik imzalı belgenin geçerli olacağı yönünde aksi her zaman ispatlanabilecek bir karine hükmünde olup bunun ceza muhakemesinde ıslak imzalı belgenin delil olarak değerlendirilmesini önleyen bir yönü bulunmamaktadır. Dolayısıyla ıslak imzalı belge ile elektronik imzalı belgenin çeliştiği bir hususun, ceza muhakemesi davasına konu olması hâlinde, ıslak imzalı belgenin doğruluğunu iddia eden tarafın iddiasını her türlü delille ispatlaması mümkün olduğu gibi, tarafların içeriği elektronik imzalı belgeyle çelişen ıslak imzalı belgeyi delil olarak göstermesine engel bir durum da bulunmamaktadır. Bu nedenle kuralın ceza muhakemesinde her şeyin delil olabileceği yönündeki 'delil serbestliği' ilkesine aykırı bir yönü bulunmamaktadır.

UYAP sisteminin Adalet Bakanlığı Bilgi İşlem Dairesi Başkanlığı tarafından yönetilmesi nedeniyle bütün adli verilerin siyasi iktidarın eline geçtiği ve bu nedenle 'hukuk devleti' 'yargı bağımsızlığı' ve 'kuvvetler ayrılığı' ilkelerinin zedelendiği iddiasının hukuki bir dayanağı da bulunmamaktadır. UYAP bir bilişim sistemi olup, bu sistemin teknik alt yapısının Adalet Bakanlığının bir birimi tarafından sağlanması ve yönetilmesi bu sisteme aktarılan adli bilgilerin, bu birimin çalışanlarına veya yöneticilerine, dolayısıyla yürütme erkine açık olduğu anlamına gelmemektedir. Bilgi İşlem Dairesi yetkilileri, sadece UYAP ile ilgili teknik alt yapı bilgilerine ulaşabilmektedir. Söz konusu adli verilere UYAP üzerinden erişme, bu bilgileri oluşturma ve bunları yönetme yetkisi münhasıran mevzuatın izin verdiği kişilere (hâkim, savcı, avukat, katip, davacı, davalı vb.) ait bulunmaktadır.

Belirtmek gerekir ki kuvvetler ayrılığı ilkesi erklerin birbirleriyle bağlantısız bir şekilde çalışmalarını değil, aksine Anayasa'nın Başlangıç'ında belirtildiği üzere medeni bir iş bölümü ve işbirliği içerisinde çalışmalarını gerektirmektedir. Bu çerçevede erklerin yetki alanları içerisindeki faaliyetlerinin zaman

zaman birbirleriyle kesişmesi mümkün olup gözetilmesi gereken hususun her erkin Anayasa tarafından belirlenmiş yetki sahasında kalmasının ve diğer erklerin yetkisine müdahale etmemesinin sağlanmasıdır. Bu bağlamda adalet hizmetlerinin sunulmasında yürütmenin idari görevlerinin bulunduğu tartışmasız olup dava konusu kurallarda bu idari görevleri aşan herhangi bir yargısal yetkinin verilmesi veya yargı erkine müdahale sonucunu doğuracak bir uygulamaya izin verilmesi söz konusu değildir.

Dava konusu kurallarda, daha önce fiziki ortamda gerçekleştirilen ve saklanan ceza muhakemesi işlemlerine ilişkin karar ve belgelerin fiziki ortamın yanı sıra UYAP sistemi aracılığıyla elektronik ortamda gerçekleştirilip saklanacağı düzenlenmektedir. Yukarıda açıklanan ilkeler karşısında kanun koyucunun bu şekilde bir düzenleme yapabilmesi için Anayasa'da kanun koyucuya yetki veren özel bir hükmün bulunması gerekmektedir. Zira Anayasa'nın 7. maddesi Anayasa'ya aykırı olmamak koşuluyla bu düzenlemeyi de kapsayacak şekilde her türlü düzenlemeyi yapma konusunda kanun koyucuya gerekli yetkiyi vermektedir.

Açıklanan nedenlerle, dava konusu kuralların, Anayasa'nın Başlangıç'ı ile 2., 6., 7., 8., 9. ve 138. maddelerine aykırı bir yönü bulunmamaktadır. İptal istemlerinin reddi gerekir.

P- Kanun'un 105. Maddesinin Birinci Fıkrasının (2) Numaralı Bendinin (b) Alt Bendinde Yer Alan "13 üncü" İbaresinin İncelenmesi

Dava dilekçesinde, 'hükmün açıklanmasının ertelenmesi', 'cezanın ertelenmesi' gibi kurumlara ilişkin uygulamaların belli bir miktardaki hapis cezasının altındaki tüm suçlar bakımından geçerli olduğu, bazı suçlar yönünden buna istisna getirilmesinin eşitsizliğe ve adaletsizliğe yol açtığı ve 5237 sayılı Türk Ceza Kanunu'ndaki genel hükümlerin suç ve ceza içeren tüm kanunlara uygulanacağına ilişkin düzenlemeye uygun düşmediği belirtilerek dava konusu kuralın, Anayasa'nın 2. ve 10. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralla, 3713 sayılı Terörle Mücadele Kanunu'nun kapsamına giren suçlarla ilgili olarak hükmün açıklanmasının geri bırakılması kararı verilemeyeceği, hapis cezasının seçenek tedbirlere çevrilemeyeceği ve ertelenmeyeceği yönündeki hüküm kaldırılarak, bu Kanun kapsamındaki suçlar yönünden de söz konusu hukuki müesseselerin uygulanmasına imkân tanınmaktadır.

Dolayısıyla söz konusu değişiklikle, dava dilekçesinde belirtilenin aksine 'hükmün açıklanmasının geri bırakılması', 'hapis cezasının seçenek tedbirlere çevrilmesi' ve 'ertelenmesi' müesseselerinin uygulanabilmesi yönünden bir istisna getirilmemekte, bilakis tanınan istisnanın ortadan kaldırılması

düzenlenmektedir. Bu nedenle dava dilekçesinde belirtildiği üzere dava konusu kuralın herhangi bir eşitsizlik veya adaletsizlik yaratması da söz konusu değildir.

Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2. ve 10. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

R- Kanun'un Geçici 1. Maddesinin İncelenmesi

Dava dilekçesinde, 6352 sayılı Kanun'un geçici 1. maddesiyle kamu davasının açılmasının ertelenmesi, kovuşturmanın ertelenmesi ve infazın ertelenmesi adı altında bir af düzenlemesine gidildiği, bu düzenlemede bazı suçlar yönünden erteleme hükümlerine yer verilirken daha ağır suçların bu kapsama alınmadığı, bunun eşitlik ilkesine aykırı olduğu, eşitlik ilkesine uygun bir düzenleme yapılabilmesi için temel şekli itibarıyla adli para cezasını ya da üst sınırı beş yıldan fazla olmayan hapis cezasını gerektiren ve yasanın yürürlük tarihine kadar işlenmiş olan tüm suçların kapsama alınması gerektiği, maddenin (3) numaralı fıkrasındaki düzenlemeyle 5237 sayılı Kanun'un 51. maddesinin son fıkrasından ayrılan bir düzenlemeye gidilerek bazı suçlar yönünden farklı ve istisnai bir düzenlemeye gidildiği, bunun eşitlik ilkesine aykırı olduğu, maddedeki 'sair düşünce ve kanaat açıklama yöntemleriyle işlenmiş' suç kavramının belirsiz olduğu ve bunun affın kapsamını genişleteceği, maddenin (5) numaralı fıkrasında hükmün açıklanmasının geri bırakılmasına karar verilmesi hallerinde de bu maddenin uygulanacağı yönündeki kuralın, her iki düzenlemenin uygulama koşullarının farklı olması nedeniyle belirsizliğe ve karmaşaya yol açtığı, ayrıca Anayasa Mahkemesinin aynı konuyu içeren 28.8.1999 günlü, 4454 sayılı "Basın ve Yayın Yoluyla İşlenen Suçlara İlişkin Dava ve Cezaların Ertelenmesine Dair Kanun'un 1. maddesinin birinci fıkrasının "... basın yoluyla yahut sözlü veya görüntülü yayın araçlarıyla işlenmiş olup ..." ibarelerini 19.9.2000 günlü, E.1999/39, K.2000/23 sayılı kararıyla iptal etmesine rağmen dava konusu düzenlemeyle aynı hususların yeniden düzenlendiği belirtilerek dava konusu kuralların, Anayasa'nın 2., 10. ve 153. maddelerine aykırı olduğu ileri sürülmüştür.

Kanun'un dava konusu geçici 1. maddesinde basın ve yayın yoluyla ya da sair düşünce ve kanaat açıklama yöntemleriyle işlenmiş suçlara ilişkin soruşturmaların, kovuşturmaların ve cezaların infazının ertelenmesi düzenlenmektedir.

Daha önce de belirtildiği üzere hukuk devletinde ceza siyasetinin ve bu siyasetin unsurlarının belirlenmesi yetkisi kanun koyucuya aittir. Kanun koyucu, cezalandırma yetkisini kullanırken toplumda hangi eylemlerin suç sayılacağı, bunun hangi tür ve ölçüdeki ceza yaptırımını ile karşılanacağı, nelerin ağırlaştırıcı veya hafifletici sebep olarak kabul edilebileceği konusunda takdir

yetkisine sahip olduđu gibi kimi suçları işleyenler için "erteleme" adı altında bir düzenleme de öngörebilir.

Bu çerçevede kanun koyucunun dava konusu kurallarla belli bir tarihe kadar, basın ve yayın yoluyla ya da sair düşünce ve kanaat açıklama yöntemleriyle işlenmiş olup temel şekli itibarıyla adli para cezasını ya da üst sınırı beş yıldan fazla olmayan hapis cezasını gerektiren suçlar yönünden soruşturmanın, kovuşturmanın veya infazın ertelenmesi yönünde kurallar belirlemede hukuk devleti ilkesine aykırı bir yön bulunmamaktadır.

Öte yandan Anayasa'nın 10. maddesinde 'kanun önünde eşitlik' ilkesine yer verilmiştir. Anayasa'nın 10. maddesinde yer verilen eşitlik ilkesi hukuksal durumları aynı olanlar için söz konusudur. Bu ilke ile eylemli değil, hukuksal eşitlik öngörülmüştür. Eşitlik ilkesinin amacı, aynı durumda bulunan kişilerin kanunlar karşısında aynı işleme bağlı tutulmalarını sağlamak, haklı bir nedene dayanmayan ayırım yapılmasını ve ayrıcalık tanınmasını önlemektir. Bu ilkeyle, aynı durumda bulunan kimi kişi ve topluluklara ayrı kurallar uygulanarak kanun karşısında eşitliğin ihlali yasaklanmıştır. Kanun önünde eşitlik, herkesin her yönden aynı kurallara bağlı tutulacağı anlamına gelmez. Durumlarındaki özellikler, kimi kişiler ya da topluluklar için değişik kuralları ve uygulamaları gerektirebilir. Aynı hukuksal durumlar aynı, ayrı hukuksal durumlar farklı kurallara bağlı tutulursa Anayasa'da öngörülen eşitlik ilkesi zedelenmez.

Dava konusu kurallarda, basın ve yayın yoluyla ya da sair düşünce ve kanaat açıklama yöntemleriyle işlenmiş olup belli bir cezayı gerektiren suçların faileri yönünden erteleme olanağının getirilmesi, diğer suç faileri yönünden ise bu olanağın sağlanmamasında eşitlik ilkesine aykırı bir yön bulunmamaktadır. Zira dava konusu kurallarda ayrıma tabi tutulan kişilerin hukuksal durumları farklı olup, durumlarındaki farklılık nedeniyle haklarında ayrı kurallar uygulanmaktadır. Dava konusu kuralda ayrıma tabi tutulan kişiler incelendiğinde bir tarafta basın, yayın ya da sair düşünce açıklama yöntemleriyle belli orandaki cezayı gerektiren suçları işleyen kişilerin diğer tarafta ise anılan yöntem dışında suç işleyen kişilerin bulunduğu dolayısıyla bu kişilerin hukuksal durumlarının farklı olduğu görülmektedir.

Kaldı ki, kanun koyucunun hiçbir neden yokken böyle bir düzenlemeye gitmediği, ifade ve basın özgürlüğünün sağlanması ve korunması gibi haklı bir nedene dayalı olarak dava konusu kuralları düzenlediği anlaşılmaktadır. Nitekim madde gerekçesinde de düzenlemenin temel hak ve hürriyetlerden kabul edilen ifade ve basın özgürlüğünün korunması amacıyla yapıldığı, basının yahut sözlü veya görüntülü yayınların, ifade özgürlüğünün en önemli kullanım araçları arasında bulunduğu, dolayısıyla bu araçların amacına uygun olarak işlevlerini yerine getirmeleri bakımından

korunmalarının demokratik toplumun gereklerinden olduđu, bu yönüyle basın ve yayın özgürlüğü için güvenceler sağlanması çerçevesinde yapılan düzenlemenin, haber ve düşüncenin özgür kılınmasını hedeflediğı belirtilmiştir.

Anayasa'nın 26. maddesinde 'düşünceyi açıklama ve yayma hürriyeti' güvence altına alınmıştır. Anayasa'nın 28. maddesinde ise 'basın özgürlüğü' düzenlenmiş ve maddenin üçüncü fıkrasında devletin basın özgürlüğünü sağlayacak tedbirleri alması gerektiğı belirtilmiştir.

Günümüzde ifade özgürlüğünün çok önemli araçlarından olan basın ve yayın özgürlüğü, demokratik toplumun en önemli gereklerinden biri olarak kabul edilmekte ve bu özgürlüğün korunması için ulusal ve uluslararası düzeyde ek güvenceler sağlanmaktadır. Uluslararası sözleşmelerde ve Avrupa İnsan Hakları Mahkemesinin içtihatlarında da bu özgürlük önemle ele alınmakta ve korunmaktadır.

Dava konusu kurallarda erteleme kapsamına alınan suçların ayrı bir uygulamaya tabi tutulmasıyla, yukarıda belirtilen anayasal ilkeler çerçevesinde basın ve yayın özgürlüğünün korunması ve bu konuda meydana gelen ihlallerin önlenmesinin amaçlandığı anlaşılmaktadır. Bu çerçevede kanun koyucunun basın özgürlüğünün korunması yönündeki haklı nedene dayalı olarak bu yöntemle işlenen suçlar yönünden bu yöntemle suç işleyen failerle diğer failer arasında ayrıma gitmesinde eşitlik ilkesine aykırı bir yön bulunmamaktadır.

Kanun koyucunun, 5237 sayılı Türk Ceza Kanunu'nun 51. maddesinde düzenlenen 'hapis cezasının ertelenmesi' ile dava konusu kurallarda düzenlenen 'ceza ve davaların ertelenmesi'ni farklı hukuki kurumlar olarak düzenlemesinde ve bunlara farklı hukuki sonuçlar bağlamasında da eşitlik ilkesine aykırı bir yön bulunmamaktadır. Her iki kurum farklı hukuki yararları gerçekleştirmek üzere düzenlenmiş olup, bu kurumlardan faydalanan failerin hukuksal durumları da farklıdır. Dolayısıyla farklı hukuksal durumdaki bu kişilere farklı kuralların uygulanması eşitlik ilkesine aykırı bir durum oluşturmamaktadır.

Dava konusu maddede yer alan 'sair düşünce ve kanaat açıklama yöntemleriyle işlenmiş suç' kavramının açık ve uygulanabilir olduğı ve bunun maddenin uygulanmasını belirsizleştirmesinin söz konusu olmadığı açıktır.

Anayasa'nın 153. maddesinin son fıkrasında, Anayasa Mahkemesi kararlarının yasama, yürütme ve yargı organları ile idare makamlarını, gerçek ve tüzelkişileri bağlayacağı hükmüne yer verilmiştir. Anayasa'nın bu kuralı Mahkemenin somut olarak Anayasa'ya aykırı bularak iptal ettiği hükümlerin bağlayıcılığıyla sınırlı olup, bu bağlayıcılık yasa koyucunun iptal edilen konuyla ilgili olarak ileriye yönelik farklı bir kanunda yeni bir düzenleme yapamayacağı ve eğer yaparsa yeni düzenlemenin sırf

bu nedenle Anayasa'ya aykırı hale geleceği anlamına gelmemektedir. Bu yönüyle kuralın, Anayasa'nın 153. maddesine aykırılığundan söz edilemez.

Açıklanan nedenlerle dava konusu kurallar, Anayasa'nın 2., 10. ve 153. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

S- Kanun'un Geçici 2. Maddesinin (4) ve (6) Numaralı Fıkralarının İncelenmesi

Dava dilekçesinde, dava konusu kurallar uyarınca, Kanun'un yürürlüğe girdiği 4.7.2012 tarihine kadar 5271 sayılı Kanun'un 250. maddesi ile görevlendirilen mahkemelerde açılan davaların kesin hükümle sonuçlandırılıncaya kadar bu mahkemelerde görülmeye devam edeceği ve bu mahkemelerin yetkisizlik ve görevsizlik kararı vermeyecekleri, bu tarihten sonra açılacak davaların ise 3713 sayılı Kanun'un 10. maddesi ile görevli mahkemelerde görüleceği, bunun da zamanaşımı süresi boyunca aynı yetkilerle donatılmış iki ayrı yargı kurumunun fiilen ve hukuken varlığını sürdürmesi anlamına geleceği, geçici 2. maddenin (4) numaralı fıkrasındaki, 5271 sayılı Kanun'un 250. maddesi ile görevli mahkemelerde devam edecek olan yargılamalarda görevsizlik ve yetkisizlik kararı verilemeyeceği yönündeki hükmün, hukukun evrensel ilke ve esaslarından olan ve Anayasa tarafından güvence altına alınan 'kanuni hakim ve mahkeme güvencesi', 'yargı bağımsızlığı' ve 'eşitlik' ilkelerine aykırı olduğu, bu hükümle söz konusu mahkemelerin bakmaması gereken bir davaya bakmak zorunda bırakıldığı, öte yandan düzenlemeyle kamu görevlilerinin doğrudan soruşturulamaması için getirilen izin sisteminin görülmekte olan davalardaki sanıklara tanınmamasının ceza usul kurallarının yürürlüğe girdiği anda uygulanması gerektiği kuralına ve eşitlik ilkesine aykırı olduğu belirtilerek kuralların, Anayasa'nın 2., 10., 36., 37. ve 138. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kurallarda, 5271 sayılı Kanun'un yürürlükten kaldırılan 250. maddesinin birinci fıkrasına göre görevlendirilen mahkemelerde açılmış olan davalara, kesin hükümle sonuçlanıncaya kadar bu mahkemelerce bakılmaya devam edileceği, bu davalarda, yetkisizlik veya görevsizlik kararı verilemeyeceği, 3713 sayılı Kanun'un 10. maddesinin kovuşturmaya ilişkin hükümlerinin bu davalarda da uygulanacağı, anılan madde kapsamına giren suçlarla ilgili olarak bu hükmün yürürlüğe girdiği tarih itibarıyla açılmış olan davalarda, sanığın taşıdığı kamu görevlisi sıfatı dolayısıyla hakkında soruşturma yapılabilmesi için izin veya karar alınması gerektiğinden bahisle durma veya düşme kararı verilemeyeceği düzenlenmektedir.

Hukuk devletinde, kanun koyucu ceza yargılamasına ilişkin kurallar belirleme ve bu çerçevede mahkemelerin kuruluşu, görev ve yetkileri, işleyişi, yargılama usulleri ve yapısı hakkında Anayasa kurallarına bağlı olmak koşuluyla ihtiyaç duyduğu düzenlemeyi yapma yetkisine sahiptir. Nitekim

Anayasa'nın konuyla ilgili 142. maddesinde mahkemelerin kuruluşu, görev ve yetkileri, işleyişi ve yargılama usullerinin kanunla düzenleneceği açıkça hüküm altına alınmıştır.

Kanun koyucunun mahkemelerin görev yetki ve yargılama usullerini belirleme yetkisi kapsamında, belli türdeki davalar yönünden görevli mahkemelerin kaldırılması ve bunlar yerine yeni mahkemeler kurulması nedeniyle, dava konusu kurallarla, devam etmekte olan davalara daha önce görevli olan mahkemelerin bakacağını düzenlemesinde ve bu mahkemelerde hangi yargılama usullerinin uygulanacağını belirlemesinde Anayasa'nın 2. maddesine aykırı bir yön bulunmamaktadır.

6352 sayılı Kanun ile yapılan değişiklikle 3713 sayılı Kanun'un 10. maddesi kapsamındaki bazı suçlar yönünden kamu görevlileri hakkında soruşturma yapılmadan önce izin alınması şartı getirilmiş böylece söz konusu suçlar yönünden, Cumhuriyet savcılarının doğrudan soruşturma yapma yetkileri kaldırılmıştır. Dava konusu kuralda ise getirilen bu yeni şart sebebiyle Kanun'un yürürlüğe girmesinden önce soruşturması tamamlanıp yargılanmasına başlanılan davalarda düşme veya durma kararı verilemeyeceği düzenlenmiş, böylece soruşturma izni ile ilgili kuralın Kanun'un yürürlüğe girmesinden sonraki soruşturmaları kapsayacağı açıkça vurgulanmıştır. Dolayısıyla söz konusu kural, Kanun'un yürürlüğe girmesinden sonraki tüm soruşturmalarda ve herkese aynı şekilde uygulanacak olduğundan, eşitlik ilkesine aykırı bir durumdan söz edilemez.

Kanun'un yürürlüğe girmesinden önce açılmış olan davalarda soruşturma iznine ilişkin kuralın uygulanmaması nedeniyle, bu tarihten önce yapılan soruşturmalardaki kamu görevlileriyle bu tarihten sonra yapılan soruşturmalardaki kamu görevlileri arasında yapılan ayırımın da eşitlik ilkesine aykırı bir yönü bulunmamaktadır. Zira eşitlik ilkesine aykırı bir durumun oluşabilmesi için aynı hukuksal durumda bulunan kişi ve topluluklara ayrı kuralların uygulanması gerekmektedir. Oysa dava konusu kuralda ayırma tabi tutulan kişilerin hukuksal durumları farklıdır. Dolayısıyla, farklı hukuksal durumdaki bu kişilerin farklı kurallara tabi tutulmasında kanun önünde eşitlik ilkesine aykırı bir yön bulunmamaktadır.

Kaldı ki, kamu görevlileriyle ilgili soruşturma yapılmadan önce izin alınması şartı yargılama usulüne ilişkin kurallardan olup, bu tür kurallar maddi ceza hukuku kurallarından farklı olarak yürürlüğe girdikten sonraki işlemlere uygulanabilmekte ve bunların yürürlük tarihinden önceki işlemlere uygulanma imkânı bulunmamaktadır. Dolayısıyla kural bu yönüyle genel yargılama hukuku ilkelerine de uygunluk göstermektedir.

Anayasa'nın 'Kanuni hâkim güvencesi' başlıklı 37. maddesinde, 'Hiç kimse kanunen tâbi olduğu mahkemeden başka bir merci önüne çıkarılamaz. Bir kimseyi kanunen tâbi olduğu mahkemeden

başka bir merci önüne çıkarma sonucunu doğuran yargı yetkisine sahip olağanüstü merciler kurulamaz.' denilmiştir.

Anayasa Mahkemesinin önceki kararlarında belirtildiği gibi, 'kanuni hâkim güvencesi' suçun işlenmesinden veya çekişmenin doğmasından önce davayı görecek yargı yerini kanunun belirlemesi şeklinde tanımlanmaktadır. Başka bir anlatımla 'kanuni hâkim güvencesi', yargılama makamlarının suçun işlenmesinden veya çekişmenin meydana gelmesinden sonra özel olarak kurulmasına veya hâkimin atanmasına engel oluşturmaktadır.

Kanun'un geçici 2. maddesinin dava konusu (4) numaralı fıkrasında, Kanun'un yürürlüğe girdiği tarihte açılmış ve devam etmekte olan davaların, 5271 sayılı Kanun'un 250. maddesi ile kurulmuş ağır ceza mahkemelerinde devam edeceği ve bu mahkemelerin yeni kurulan mahkemeler nedeniyle görevsizlik ve yetkisizlik kararı veremeyecekleri belirtilmekte, böylece uzun süredir devam eden davalarda başa dönülmesinin ve suçun işlenmesinden sonra yargı yerinin değiştirilmesinin önüne geçilmektedir. Dolayısıyla kuralla suçun işlenmesinden sonra yargı yeri belirlenmemekte, aksine suçun işlenmesinden sonra kurulan mahkemelere davaların görevsizlik veya yetkisizlikle gönderilmesi önlenerek, suçun işlenmesinden önce kurulan mahkemelerde davanın devam etmesi sağlanmaktadır. Bu nedenle kuralın 'kanuni hâkim güvencesi' ile çelişen bir yönü bulunmamaktadır.

Açıklanan nedenlerle dava konusu kurallar, Anayasa'nın 2., 10., ve 37. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Osman Alifeyyaz PAKSÜT maddenin (4) numaralı fıkrası yönünden bu görüşe katılmamıştır.

Kuralların Anayasa'nın 36. ve 138. maddeleriyle ilgisi görülmemiştir.

Ş- Kanun'un Geçici 3. Maddesinin (1) Numaralı Fıkrasının İncelenmesi

Dava dilekçesinde, dava konusu kuralda lehe kanunun belirlenmesine ilişkin olarak getirilen düzenlemenin, 5237 sayılı Kanun'un 7. maddesinin (2) numaralı fıkrası ve 5252 sayılı Türk Ceza Kanununun Yürürlük ve Uygulama Şekli Hakkında Kanun'un 9. maddesinin (3) numaralı fıkrasındaki genel kurala aykırı olduğu, kuralın özel af niteliği taşıdığı ve belli bazı kişilerin tahliyesine neden olduğu, oysa bu suçların insanlığa karşı suç niteliğinde olduğu ve insanlığa karşı suçların Birleşmiş Milletlerin savaş ve insanlığa karşı suçlardan suçlu bulunanların yargılanması ile ilgili uluslararası prensipleri uyarınca nasıl zamanaşımına uğramaması gerektiği kabul edilmekteyse affedilemeyeceğinin de kabul edilmesi gerektiği, ayrıca bu tahliyelerin mahkeme kararlarının yerine getirilmemesi sonucunu doğurduğu, bu yönüyle kuralın, Anayasa'nın 90. maddesi ile 138. maddesine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralda, 12 Eylül 1980 tarihinden önce işlenmiş olan suçlardan dolayı lehe kanununun, 1.3.1926 günlü ve 765 sayılı Türk Ceza Kanunu'nun cezaların içtimasına ilişkin hükümleri uygulandıktan sonra ortaya çıkan sonuç ceza göz önünde bulundurularak belirleneceği ve belirlenen bu cezanın infaz bakımından lehe hükümler içeren kanuna göre infaz edileceği düzenlenmektedir.

Hukuk devletinde, ceza ve ceza yargılamasına ilişkin kurallar, ceza hukukunun ana ilkeleri ile Anayasa'nın konuya ilişkin kuralları başta olmak üzere, ülkenin sosyal, kültürel yapısı, etik değerleri ve ekonomik hayatın gereksinimleri göz önüne alınarak saptanacak ceza siyasetine göre belirlenir. Kanun koyucu, cezalandırma yetkisini kullanırken toplumda hangi eylemlerin suç sayılacağı, bunun hangi tür ve ölçüdeki ceza yaptırımını ile karşılanacağı, nelerin ağırlaştırıcı veya hafifletici sebep olarak kabul edilebileceği konusunda takdir yetkisine sahip olduğu gibi belli bir tarihten önce işlenen suçlar yönünden lehe kanun hükümlerinin belirlenmesinde hangi usulün uygulanacağını belirleme konusunda da takdir yetkisine sahiptir. Bu çerçevede kanun koyucunun dava konusu kural ile lehe kanunun nasıl belirleneceğine ilişkin ceza kanunundaki mevcut usulden ayrılan bir düzenleme benimsemesi de kuşkusuz takdir yetkisi kapsamında kalmaktadır.

Anayasa'nın 138. maddesinin son fıkrasına göre, 'Yasama ve yürütme organları ile idare, mahkeme kararlarına uymak zorundadır; bu organlar ve idare, mahkeme kararlarını hiçbir suretle değiştiremez ve bunların yerine getirilmesini geciktiremez.'

Dava konusu kuralla, içtimayı gerektiren cezaların infazı bakımından belli bir tarihe kadar işlenen suçlar yönünden lehe kanun belirlenmesi ile ilgili daha önce adli davalara konu olan husus, yasal düzenleme konusu yapılmıştır. Yasamanın genelliği ilkesi uyarınca kanun koyucunun Anayasa'ya aykırı olmamak kaydıyla her konuyu kanunla düzenleme yetkisi bulunmaktadır. Bu çerçevede, kanun koyucu tarafından getirilen ve genel, objektif nitelik taşıdığı görülen kuralın, Anayasa'nın 138. maddesine aykırı bir yönü bulunmamaktadır.

Kaldı ki dava konusu kural farklı kanunlar arasında lehe kanunun nasıl belirleneceğini gösteren, bu yönüyle çoğu zaman kesinleşmiş kararlara da uygulanması gereken kurallardan olup bu nevi kararlar doğası gereği kesinleşmiş kararları etkileyebilmekte ve bu hususta 'uyarlama yargılamaları' yapılmasını gerektirebilmektedir. Söz konusu kuralların doğası itibarıyla kesinleşmiş kararlar üzerinde etki doğurabilmesi ve bu etkiyi de ancak verilecek mahkeme kararları aracılığıyla gerçekleştirebilmesi, bunların yasama yetkisinin genelliği ilkesine istisna oluşturmalarını gerektirmemekte ve bu alanda kanuni düzenleme yapılabilmesini engellememektedir.

Açıklanan nedenlerle dava konusu kural, Anayasa'nın 138. maddesine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 90. maddesiyle ilgisi görülmemiştir.

V- YÜRÜRLÜĞÜN DURDURULMASI İSTEMLERİNİN İNCELENMESİ

2.7.2012 günlü, 6352 sayılı Yargı Hizmetlerinin Etkinleştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılması ve Basın Yayın Yoluyla İşlenen Suçlara İlişkin Dava ve Cezaların Ertelenmesi Hakkında Kanun'un;

A- 1- 1. maddesiyle 9.6.1932 günlü, 2004 sayılı İcra ve İflas Kanunu'nun başlığı ile birlikte değiştirilen 1. maddesinin beşinci fıkrasına,

2- 3. maddesiyle 2004 sayılı Kanun'a eklenen 8/a maddesinin ikinci fıkrasına,

3- 21. maddesiyle değiştirilen 2004 sayılı Kanun'un 106. maddesinin birinci fıkrasına,

4- 22. maddesiyle değiştirilen 2004 sayılı Kanun'un 110. maddesinin birinci fıkrasına,

5- 24. maddesiyle 2004 sayılı Kanun'un 114. maddesine eklenen dördüncü fıkranın 'Açık artırmaya elektronik ortamdan teklif verme yoluyla başlanır.' biçimindeki birinci cümlesine,

6- 25. maddesiyle 2004 sayılı Kanun'un başlığı ile birlikte değiştirilen 115. maddesine,

7- 28. maddesiyle değiştirilen 2004 sayılı Kanun'un 124. maddesinin üçüncü fıkrasında yer alan 'elektronik ortamda teklif vererek artırmaya katılacakların teminat göstermeleri gerektiği ve elektronik ortamda teklif vermeye ilişkin hususlar yazılır.' ibaresine,

8- 29. maddesiyle 2004 sayılı Kanun'un başlığı ile birlikte değiştirilen 126. maddesinin dördüncü fıkrasına,

9- 31. maddesiyle değiştirilen 2004 sayılı Kanun'un 129. maddesine,

10- 44. maddesiyle 6.1.1982 günlü, 2575 sayılı Danıştay Kanunu'nun 8. maddesinin;

a- (1) numaralı fıkrasının (d) bendine eklenen 'Türkiye Büyük Millet Meclisi Genel Sekreterliği,' ibaresine, (e) bendine eklenen 'ile düzenleyici ve denetleyici kurumların başkanlıkları,' ibaresine ve değiştirilen (g) bendine,

b- (3) numaralı fıkrasında yer alan 'yirmi yıl' ibaresinin 'onbeş yıl' şeklinde değiştirilmesine,

11- 45. maddesiyle değiştirilen 2575 sayılı Kanun'un 24. maddesinin (1) numaralı fıkrasının (c) bendine,

12- 46. maddesiyle değiştirilen 2575 sayılı Kanun'un 60. maddesinin (1) numaralı fıkrasına,

- 13- 47. maddesiyle deęiřtirilen 2575 sayılı Kanun'un 61. maddesinin (1) numaralı fıkrasının birinci ve ikinci cümleleri ile (3) numaralı fıkrasına,
- 14- 57. maddesiyle 6.1.1982 günlü, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 27. maddesinin;
- a- Deęiřtirilen (2) numaralı fıkrasının birinci cümlesinde yer alan "davalı idarenin savunması alındıktan veya savunma süresi geçtikten sonra" ibaresine ve ikinci cümlesine,
- b- Eklenen (3) ve (10) numaralı fıkralarına,
- 15- 58. maddesiyle deęiřtirilen 2577 sayılı Kanun'un 28. maddesinin (2) numaralı fıkrası ile (6) numaralı fıkrasının ikinci cümlesine,
- 16- 72. maddesiyle 24.2.1983 günlü, 2802 sayılı Hâkimler ve Savcılar Kanunu'nun 37. maddesinin birinci fıkrasına eklenen (c) bendinin birinci cümlesinde yer alan "üstün başarısı ile iç denetim hizmetlerinde yararlı olacağı anlaşılmıř bulunanlar arasından'Müsteřarın teklifi üzerine Bakan tarafından atama yapılır.' ibarelerine,
- 17- 75. maddesiyle 12.4.1991 günlü, 3713 sayılı Terörle Mücadele Kanunu'nun bařlıęı ile birlikte deęiřtirilen 10. maddesinin 'Türk Ceza Kanununun 305, 318, 319, 323, 324, 325 ve 332 nci maddeleri hariç olmak üzere, İkinci Kitap Dördüncü Kısımın Dört, Beř, Altı ve Yedinci Bölümünde tanımlanan suçlarda, Ceza Muhakemesi Kanununda öngörülen tutuklama süresi iki kat olarak uygulanır.' biçimindeki beřinci fıkrası dışında kalan bölümüne,
- 18- 77. maddesiyle 9.6.2004 günlü, 5187 sayılı Basın Kanunu'nun 26. maddesinin birinci ve altıncı fıkralarında yapılan deęiřikliklere,
- 19- 85. maddesiyle deęiřtirilen 26.9.2004 günlü, 5237 sayılı Türk Ceza Kanunu'nun 220. maddesinin (7) numaralı fıkrasına,
- 20- 90. maddesiyle 5237 sayılı Kanun'un bařlıęı ile birlikte deęiřtirilen 277. maddesine,
- 21- 92. maddesiyle deęiřtirilen 5237 sayılı Kanun'un 285. maddesinin (1), (2), (5) ve (6) numaralı fıkralarına,
- 22- 93. maddesiyle deęiřtirilen 5237 sayılı Kanun'un 288. maddesine,
- 23- 95. maddesiyle 4.12.2004 günlü, 5271 sayılı Ceza Muhakemesi Kanunu'na eklenen 38/A maddesine,
- 24- 105. maddesinin birinci fıkrasının (2) numaralı bendinin (b) alt bendinde yer alan "13 üncü" ibaresine,

25- Geçici 1. maddesine,

26- Geçici 2. maddesinin (4) ve (6) numaralı fıkralarına,

27- Geçici 3. maddesinin (1) numaralı fıkrasına,

yönelik iptal istemleri, 4.7.2013 günlü, E.2012/100, K.2013/84 sayılı kararla reddedildiğinden, bu maddelere, fıkralara, bentlere, cümlelere, bölüme, ibarelere ve değişikliklere ilişkin yürürlüğün durdurulması istemlerinin REDDİNE,

B- 75. maddesiyle 3713 sayılı Kanun'un başlığı ile birlikte değiştirilen 10. maddesinin beşinci fıkrasına ilişkin iptal hükmünün yürürlüğe girmesinin ertelenmesi nedeniyle bu fıkra ile ilişkin yürürlüğün durdurulması isteminin REDDİNE,

C- 85. maddesiyle değiştirilen 5237 sayılı Kanun'un 220. maddesinin (6) numaralı fıkrası hakkında, 4.7.2013 günlü, E.2012/100, K.2013/84 sayılı kararla karar verilmesine yer olmadığına karar verildiğinden, bu fıkra ile ilişkin yürürlüğün durdurulması istemi hakkında **KARAR VERİLMESİNE YER OLMADIĞINA,**

4.7.2013 gününde **OYBİRLİĞİYLE,** karar verilmiştir.

VI- İPTAL KARARININ YÜRÜRLÜĞE GİRECEĞİ GÜN SORUNU

Anayasa'nın 153. maddesinin üçüncü fıkrasında, 'Kanun, kanun hükmünde kararname veya Türkiye Büyük Millet Meclisi İçtüzüğü ya da bunların hükümleri, iptal kararlarının Resmi Gazetede yayımlandığı tarihte yürürlükten kalkar. Gereken hallerde Anayasa Mahkemesi iptal hükmünün yürürlüğe gireceği tarihi ayrıca kararlaştırabilir. Bu tarih, kararın Resmi Gazetede yayımlandığı günden başlayarak bir yılı geçemez.' denilmekte, 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 66. maddesinin (3) numaralı fıkrasında da bu kural tekrarlanarak, Mahkemenin gerekli gördüğü hâllerde, Resmî Gazetede yayımlandığı günden başlayarak iptal kararının yürürlüğe gireceği tarihi bir yılı geçmemek üzere ayrıca kararlaştırabileceği belirtilmektedir.

2.7.2012 günlü, 6352 sayılı Yargı Hizmetlerinin Etkinleştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılması ve Basın Yayın Yoluyla İşlenen Suçlara İlişkin Dava ve Cezaların Ertelenmesi Hakkında Kanun'un 75. maddesiyle 12.4.1991 günlü, 3713 sayılı Terörle Mücadele Kanunu'nun başlığı ile birlikte değiştirilen 10. maddesinin 'Türk Ceza Kanununun 305, 318, 319, 323, 324, 325 ve 332 nci maddeleri hariç olmak üzere, İkinci Kitap Dördüncü Kısımın Dört, Beş, Altı ve Yedinci Bölümünde tanımlanan suçlarda, Ceza Muhakemesi Kanununda öngörülen tutuklama süresi iki kat olarak

uygulanır.' biçimindeki beşinci fıkrasının iptal edilmesi yönündeki kararın derhal uygulanması kamu düzenini ihlal edici nitelikte görüldüğünden, Anayasa'nın 153. maddesinin üçüncü fıkrasıyla 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince İPTAL HÜKMÜNÜN, KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAŞLAYARAK BİR YIL SONRA YÜRÜRLÜĞE GİRMESİNE, OYBİRLİĞİYLE, 4.7.2013 gününde karar verilmiştir.

VII- SONUÇ

2.7.2012 günlü, 6352 sayılı Yargı Hizmetlerinin Etkinleştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılması ve Basın Yayın Yoluyla İşlenen Suçlara İlişkin Dava ve Cezaların Ertelenmesi Hakkında Kanun'un;

A- 1. maddesiyle 9.6.1932 günlü, 2004 sayılı İcra ve İflas Kanunu'nun başlığı ile birlikte değiştirilen 1. maddesinin beşinci fıkrasının Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, Mehmet ERTEN ile Zehra Ayla PERKTAŞ'ın karşıoyları ve OYÇOKLUĞUYLA,

B- 3. maddesiyle 2004 sayılı Kanun'a eklenen 8/a maddesinin ikinci fıkrasının Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

C- 21. maddesiyle değiştirilen 2004 sayılı Kanun'un 106. maddesinin birinci fıkrasının Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

Ç- 22. maddesiyle değiştirilen 2004 sayılı Kanun'un 110. maddesinin birinci fıkrasının Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

D- 24. maddesiyle 2004 sayılı Kanun'un 114. maddesine eklenen dördüncü fıkranın 'Açık artırmaya elektronik ortamdan teklif verme yoluyla başlanır.' biçimindeki birinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

E- 25. maddesiyle 2004 sayılı Kanun'un başlığı ile birlikte değiştirilen 115. maddesinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

F- 28. maddesiyle değiştirilen 2004 sayılı Kanun'un 124. maddesinin üçüncü fıkrasında yer alan "elektronik ortamda teklif vererek artırmaya katılacakların teminat göstermeleri gerektiği ve elektronik ortamda teklif vermeye ilişkin hususlar yazılır." ibaresinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

G- 29. maddesiyle 2004 sayılı Kanun'un başlığı ile birlikte değiştirilen 126. maddesinin dördüncü fıkrasının Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

Ğ- 31. maddesiyle deęiřtirilen 2004 sayılı Kanun'un 129. maddesinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

H- 44. maddesiyle 6.1.1982 günlü, 2575 sayılı Danıřtay Kanunu'nun 8. maddesinin;

1- (1) numaralı fıkrasının;

a- (d) bendine eklenen 'Türkiye Büyük Millet Meclisi Genel Sekreterlięi,' ibaresinin,

b- (e) bendine eklenen 'ile düzenleyici ve denetleyici kurumların başkanlıkları,' ibaresinin,

c- Deęiřtirilen (g) bendinin,

Anayasa'ya aykırı olmadıklarına ve iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

2- (3) numaralı fıkrasında yer alan 'yirmi yıl' ibaresinin 'onbeř yıl' řeklinde deęiřtirilmesinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, Zehra Ayla PERKTAŐ'ın karřıoyu ve OYÇOKLUĞUYLA,

I- 45. maddesiyle deęiřtirilen 2575 sayılı Kanun'un 24. maddesinin (1) numaralı fıkrasının (c) bendinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŐ'ın karřıoyları ve OYÇOKLUĞUYLA,

İ- 46. maddesiyle deęiřtirilen 2575 sayılı Kanun'un 60. maddesinin (1) numaralı fıkrasının;

1- Birinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, Osman Alifeyyaz PAKSÜT'ün karřıoyu ve OYÇOKLUĞUYLA,

2- İkinci cümlesinin süre yönünden REDDİNE, OYBİRLİĞİYLE,

J- 47. maddesiyle deęiřtirilen 2575 sayılı Kanun'un 61. maddesinin;

1- (1) numaralı fıkrasının birinci ve ikinci cümlelerinin,

2- (3) numaralı fıkrasının,

Anayasa'ya aykırı olmadıklarına ve iptal istemlerinin REDDİNE, Osman Alifeyyaz PAKSÜT'ün karřıoyu ve OYÇOKLUĞUYLA,

K- 57. maddesiyle;

1- 6.1.1982 günlü, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 27. maddesinin;

a- Deęiřtirilen (2) numaralı fıkrasının birinci cümlesinde yer alan "davalı idarenin savunması alındıktan veya savunma süresi geçtikten sonra" ibaresinin Anayasa'ya aykırı olmadığına ve iptal

isteminin REDDİNE, Mehmet ERTEN, Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŞ'ın karşıoyları ve OYÇOKLUĞUYLA,

b- Değiştirilen (2) numaralı fıkrasının ikinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

2- Eklenen (3) ve (10) numaralı fıkralarının Anayasa'ya aykırı olmadıklarına ve iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

L- 58. maddesiyle değiştirilen 2577 sayılı Kanun'un 28. maddesinin (2) numaralı fıkrası ile (6) numaralı fıkrasının ikinci cümlesinin Anayasa'ya aykırı olmadıklarına ve iptal istemlerinin REDDİNE, Mehmet ERTEN'in karşıoyu ve OYÇOKLUĞUYLA,

M- 72. maddesiyle 24.2.1983 günlü, 2802 sayılı Hâkimler ve Savcılar Kanunu'nun 37. maddesinin birinci fıkrasına eklenen (c) bendinin birinci cümlesinde yer alan "üstün başarısı ile iç denetim hizmetlerinde yararlı olacağı anlaşılmış bulunanlar arasından'Müsteşarın teklifi üzerine Bakan tarafından atama yapılır.' ibarelerinin Anayasa'ya aykırı olmadıklarına ve iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

N- 75. maddesiyle 12.4.1991 günlü, 3713 sayılı Terörle Mücadele Kanunu'nun başlığı ile birlikte değiştirilen 10. maddesinin;

1- Üçüncü fıkrasının;

a- (b) bendinin son cümlesinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, Mehmet ERTEN ile Zehra Ayla PERKTAŞ'ın karşıoyları ve OYÇOKLUĞUYLA,

b- (e) bendinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, Mehmet ERTEN, Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŞ'ın karşıoyları ve OYÇOKLUĞUYLA,

2- 'Türk Ceza Kanununun 305, 318, 319, 323, 324, 325 ve 332 nci maddeleri hariç olmak üzere, İkinci Kitap Dördüncü Kısımın Dört, Beş, Altı ve Yedinci Bölümünde tanımlanan suçlarda, Ceza Muhakemesi Kanununda öngörülen tutuklama süresi iki kat olarak uygulanır.' biçimindeki beşinci fıkrasının İPTALİNE; iptal hükmünün, Anayasa'nın 153. maddesinin üçüncü fıkrasıyla 30.3.2011 günlü, 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince, KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAŞLAYARAK BİR YIL SONRA YÜRÜRLÜĞE GİRMESİNE, OYBİRLİĞİYLE,

3- Kalan bölümünün Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

O- 77. maddesiyle 9.6.2004 günlü, 5187 sayılı Basın Kanunu'nun 26. maddesinin birinci ve altıncı fıkralarında yapılan değişikliklerin Anayasa'ya aykırı olmadıklarına ve iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

Ö- 85. maddesiyle değiştirilen 26.9.2004 günlü, 5237 sayılı Türk Ceza Kanunu'nun 220. maddesinin;
1- (6) numaralı fıkrası 11.4.2013 günlü, 6459 sayılı İnsan Hakları ve İfade Özgürlüğü Bağlamında Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un 11. maddesi ile değiştirildiğinden, konusu kalmayan bu fıkra ile ilişkin iptal istemi hakkında KARAR VERİLMESİNE YER OLMADIĞINA, OYBİRLİĞİYLE,

2- (7) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

P- 90. maddesiyle 5237 sayılı Kanun'un başlığı ile birlikte değiştirilen 277. maddesinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

R- 92. maddesiyle değiştirilen 5237 sayılı Kanun'un 285. maddesinin (1), (2), (5) ve (6) numaralı fıkralarının Anayasa'ya aykırı olmadıklarına ve iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

S- 93. maddesiyle değiştirilen 5237 sayılı Kanun'un 288. maddesinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

Ş- 95. maddesiyle 4.12.2004 günlü, 5271 sayılı Ceza Muhakemesi Kanunu'na eklenen 38/A maddesinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

T- 105. maddesinin birinci fıkrasının (2) numaralı bendinin (b) alt bendinde yer alan "13 üncü" ibaresinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

U- Geçici 1. maddesinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

Ü- Geçici 2. maddesinin;

1- (4) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, Osman Alifeyyaz PAKSÜT'ün karşıoyu ve OYÇOKLUĞUYLA,

2- (6) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

V- Geçici 3. maddesinin (1) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

4.7.2013 gününde karar verildi.

Başkan - Haşim KILIÇ

Başkanvekili - Serruh KALELİ

Başkanvekili - Alparslan ALTAN

Üye: Mehmet ERTEN; Serdar ÖZGÜLDÜR; Osman Alifeyyaz PAKSÜT; Zehra Ayla PERKTAŞ; Recep KÖMÜRCÜ; Burhan ÜSTÜN; Nuri NECİPOĞLU; Hicabi DURSUN; Celal Mümtaz AKINCI; Erdal TERCAN; Muammer TOPAL; Zühtü ARSLAN; M. Emin KUZ

KARŞIOY GEREKÇESİ

I- 2004 sayılı Kanunu'nun değişik 1. maddesinin iptali istenen beşinci fıkrasında;

'İcra müdür ve icra müdür yardımcıları ile icra kâtiplerinin, yazılı sınav, sözlü sınav, görevlendirme, nakil, unvan değişikliği, görevde yükselme ve diğer hususları yönetmelikle düzenlenir.' denilmektedir.

Kuralda yer alan, icra müdür ve icra müdür yardımcıları ile icra kâtiplerinin adli nitelikteki kamu hizmetinin gerektirdiği asli ve sürekli görevleri yerine getirmekle ödevli kamu görevlileri olduklarında duraksama bulunmamaktadır.

Anayasa'nın 128. maddesinin ikinci fıkrasında ' Memurların ve diğer kamu görevlilerinin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülükleri, aylık ve ödenekleri ve diğer özlük işleri kanunla düzenlenir' denilerek, kamu görevlileriyle ilgili statü esaslarının kanunla düzenleneceği öngörülmektedir. Buna göre, kamu görevlilerinin nitelik, atanma, görev ve yetkileri gibi hususların kanunla düzenlenmesi Anayasal bir zorunluluktur.

İptali istenen kuralda ise kamu görevlileri olan icra müdürü, icra müdür yardımcıları ve icra kâtiplerinin atanma, görevlendirme, görevde yükselme gibi özlük işleri ile ilgili hususların yönetmelikle düzenleneceği ifade edilmektedir.

Kanunla düzenlenmesi gereken bir hususu yönetmeliğe bırakan kural, bu nedenle Anayasa'nın 128. maddesine aykırıdır.

II- 2577 sayılı Kanun'un 27. maddesinin değişik (2) numaralı fıkrasının koyu renkle gösterilen ve iptali istenen sözcüklerin de yer aldığı birinci cümlesinde;

'Danıştay veya idari mahkemeler, idari işlemin uygulanması halinde telafisi güç veya imkânsız zararların doğması ve idari işlemin açıkça hukuka aykırı olması şartlarının birlikte gerçekleşmesi durumunda, davalı idarenin savunması alındıktan veya savunma süresi geçtikten sonra gerekçe göstererek yürütmenin durdurulmasına karar verebilirler.' kuralı yer almaktadır.

Kural uyarınca, Danıştay ve idari mahkemeler idari bir işlemin yürütülmesinin durdurulabilmesine karar verebilmeleri için, kuralda öngörülen diğer şartların yanı sıra, davalı idarenin savunmasının alınmış veya savunma süresinin geçirilmiş olması koşulunun da gerçekleşmesini aramaları gerekmektedir.

Anayasa Mahkemesinin 22.2.2006 günlü, E:2006/20 K:2006/25 sayılı 10.1.2007-26399 tarihli Resmî Gazete'de 9.3.2006 günlü, E:2006/33 K:2006/36 sayılı 10.1.2007-26399 tarihli Resmî Gazete'de yayımlanan kararlarında belirtilen iptal gerekçeleri, iptali istenen bu sözcükler bakımından da geçerli olduğundan, "davalı idarenin savunması alındıktan veya savunma süresi geçtikten sonra" sözcükleri de belirtilen kararlardaki gerekçeyle Anayasa'nın 125. maddesine aykırıdır.

III- 2577 sayılı Kanun'un değişik 28. maddesinin iptali istenen (2) numaralı fıkrası ile (6) numaralı fıkrasının ikinci cümlesinde;

'Konusu belli bir miktar paranın ödenmesini gerektiren davalarda hükmedilen miktar ile her türlü davalarda hükmedilen vekâlet ücreti ve yargılama giderleri, davacının veya vekilinin davalı idareye yazılı şekilde bildireceği banka hesap numarasına, bu bildirim tarihinden itibaren, birinci fıkrada belirtilen usul ve esaslar çerçevesinde yatırılır. Birinci fıkrada belirtilen süreler içinde ödeme yapılmaması halinde, genel hükümler dairesinde infaz ve icra olunur.'

'Ancak mahkeme kararının davacıya tebliği ile banka hesap numarasının idareye bildirildiği tarih arasında geçecek süre için faiz işlemez.'denilmektedir.

Dava konusu kurallar mahkeme ilamlarının ne suretle infaz ve icra edileceğini düzenlemektedir.

Anayasa'nın 'Hak arama hürriyeti' başlıklı 36. maddesinde 'Herkes, meşrû vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir.' denilmektedir. Buna göre, herkesin davacı veya davalı olarak adil yargılanma hakkının bulunduğu, bu hak kapsamında hakka ulaşma hakkının da yer aldığı açıktır.

İptali istenen kural, mahkemelerce hükmedilen bir miktar para ile vekâlet ücreti ve yargılama giderlerinin, davacı veya vekilinin davalı idareye bildireceği banka hesap numarasına 2577 sayılı Kanun'un 28. maddesinin birinci fıkrasında öngörülen süre zarfında yatırılacağı, süresinde yatırılmaması halinde ilâmın genel hükümler çerçevesinde infaz ve icra edileceğini öngörmektedir. Kurala göre, mahkemece hükmedilen para ile vekâlet ücreti ve yargılama giderleri hükmün kesinleşmesinden hemen sonra genel hükümlere göre infaz ve icrası mümkün bir ilâm haline gelmesine rağmen, kural farklı bir ödeme yöntemi getirerek, genel hükümlerin uygulanmasını belli bir süre için durdurmakta ve hak sahiplerinin hakka ulaşmalarını belli bir süre engellemektedir.

Anayasa'da öngörülen adil yargılanma hakkı sınırlandırılması mümkün olmayan hakka koşulsuz ulaşma hakkını da güvence altına alan temel bir haktır.

Kural, bu hakkın kullanılmasını engellediği için Anayasa'nın 36. maddesine aykırıdır.

Yine, kararın tebliği ile hesap numarasının bildirilmesi sırasında geçecek sürede faiz işletilmemesine ilişkin kural ise aykırı olduğu kabul edilen kurala bağlı bir düzenleme olduğundan, aynı gerekçeyle Anayasa'ya aykırıdır.

IV- 3713 sayılı Kanun'un 10. maddesinin üçüncü fıkrasının b) bendinin iptali istenilen ikinci cümlesinde ve e) bendinde;

'b) 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 26 ncı maddesi hükmü saklıdır.'

'e) Gözaltındaki şüphelinin müdafisi ile görüşme hakkı, Cumhuriyet savcısının istemi üzerine, hâkim kararıyla yirmi dört saat süre ile kısıtlanabilir; bu zaman zarfında ifade alınamaz.' denilmektedir.

- 3713 sayılı Kanun'un 10. maddesinin üçüncü fıkrasının b) bendinin ikinci cümlesindeki kural, Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 26. maddesi hükmünü saklı tutarak, 2937 sayılı Yasa kapsamında görevli bulunan kimi kişilerin 3713 sayılı yasada belirtilen suçlar bakımından Cumhuriyet savcılarınca doğrudan soruşturma yapılmasını önlenmektedir.

Saklı tutulan bu kural, Anayasa Mahkemesinin 17.1.2013 günlü E: 2012/19 K: 2013/17 sayılı, 12.05.2013-28645 tarihli Resmi Gazetede yayımlanan kararında yer alan ve iptali gerektiğine ilişkin karşı oy gerekçemde belirttiğim nedenlerle Anayasa'ya aykırıdır.

- 3713 sayılı Kanun'un 10. maddesinin üçüncü fıkrasının e) bendi, 3713 sayılı Kanun kapsamındaki suçlarla ilgili olarak gözaltına alınan şüphelilerin, müdafisi ile görüşmelerinin hakim kararıyla belli bir süre için kısıtlanabileceğini öngörmektedir.

Anayasa'nın 36. maddesi, herkesin meşrû vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahip olduğunu ifade etmektedir. Savunma hakkını da kapsayan adil yargılanma hakkı, maddede öngörülmediği için sınırlandırılması mümkün olmayan temel bir haktır.

Kural ile 3713 sayılı Kanun kapsamındaki suçlarla ilgili olarak gözaltına alınan şüphelinin müdafisi ile görüşmesi belli bir süre engellenerek savunma hakkı kısıtlanmaktadır.

Hâkim kararıyla ve belli bir süre için de olsa, savunma hakkının kısıtlanması Anayasa'da öngörülen adil yargılanma hakkına aykırıdır.

V- Yukarda her bir bölümde açıklanan nedenlerle Anayasa'ya aykırı oldukları belirtilen kuralların iptali gerekir.

Üye - Mehmet ERTEN

KARŞIOY YAZISI

I- Kanun'un 45. maddesiyle 2575 sayılı Kanun'un 24. maddesinin (1) numaralı fıkrasının (c) bendinde yapılan değişikliğin Anayasaya aykırılığı:

İlk derece mahkemesi olarak Danıştayda görülecek davaların belirlendiği maddede yer alan kuralla, Bakanlıklar ile kamu kuruluşları veya kamu kurumu niteliğindeki meslek kuruluşlarınca çıkarılan ve ülke çapında uygulanacak düzenleyici işlemlere karşı açılacak iptal ve tam yargı davalarına Danıştayda bakılması öngörülmüştür. Buna göre, davanın ilk derece mahkemesi olarak Danıştay'da görülmesini belirleyecek kıstasın, düzenleyici işlemin yetki, sebep, şekil, konu ve amaç gibi hukuksal özelliklerinin değil, düzenleyici işlemi yapan bakanlık veya kamu kuruluşunun kendi takdiriyle belirlediği idari uygulama alanı olduğu anlaşılmaktadır. Daha açık bir anlatımla, iptali istenen kuralın öngördüğü ölçütlere göre, düzenleyici işlemin Türkiye'nin bir ilini hatta tek bir ilçesini hariç tutacak şekilde yapılması halinde Danıştay görevli olmayacaktır. Bu durumda aynı nitelikte ve önemde davaların, davalı idarenin tercihiyle, farklı yargı mercileri önüne gelmesi söz konusudur.

Anayasa'nın 125. maddesinde idarenin her türlü eylem ve işlemlerine karşı yargı yolunun açık olduğu, 142. maddesinde mahkemelerin kuruluşunun, görev ve yetkilerinin, işleyişinin, yargılama usullerinin kanunla düzenleneceği belirtilmiş; 155. maddesinde Danıştayın kanunda gösterilen belli davalara da ilk ve son derece mahkemesi olarak bakacağı öngörülmüştür. Kuralla, düzenleyici işlemlerin geçerli olacağı idari ve coğrafi bölgeyi serbestçe belirleyecek olan idareye, bunun tabi olacağı yargı yerini de seçmek hakkı da tanındığından, Anayasa'nın 142. ve 155. maddeleri anlamında Danıştayın görev ve yetkisinin kanunla belirlendiği söylemez.

Bu nedenle kural, Anayasa'nın 142. ve 155. maddelerine aykırıdır.

II- Kanun'un 46. ve 47. maddeleriyle 2575 sayılı Kanun'da Danıştay Başsavcısı ve savcılarının görevlerinde yapılan değişikliklerin Anayasa'ya aykırılığı:

Kanunun 46. maddesiyle, Danıştay başsavcısının, esas hakkındaki düşüncelerini bildirmek üzere savcılara havale edeceği dava dosyaları Danıştay'ın ilk derece mahkemesi sıfatıyla göreceği dava

dosyaları ile sınırlandırılmış, 47. maddesiyle savcılarının görevlerinin Danıştayda ilk derece mahkemesi sıfatıyla görülecek dava dosyaları ile sınırlı olduğu tekrar edilmiştir.

Anayasa'nın 155. maddesinde 'Danıştay, idari mahkemelerce verilen ve kanunun başka bir idari yargı merciine bırakmadığı karar ve hükümlerin son inceleme merciidir. Kanunda gösterilen belli davalara da ilk ve son derece mahkemesi olarak bakar' denilmiştir. Buna göre Danıştay, idari yargının temyiz ve içtihat mercii olup, bu işlevin yerine getirilmesi Danıştay'ın asli görevidir.

İdari yargı savcılığı Anayasa'da düzenlenmiş bir kurum olup, Anayasa'nın 140., 155. ve 159. maddelerinde açıkça yer almaktadır. Bu nedenle Danıştay savcıları, idari yargının anayasal görev yapan asli unsurlarındandır.

Asli görevi idari yargının temyiz ve içtihat mercii olarak anayasada belirlenen Danıştay'ın bu görevini yine anayasal bir yargı unsuru olan Danıştay savcılarının devre dışı bırakılması suretiyle yerine getirmesini öngören bir yasa kuralında Anayasa'ya uyarlık bulunduğu söylenemez. Bu nedenle kural, Anayasa'nın 155. maddesine aykırıdır.

Öte yandan, Anayasa'nın 125. maddesinde idarenin her türlü eylem ve işlemine karşı yargı yolu güvencesi öngörülmüş, 36. maddesinde adil yargılanma hakkına yer verilmiştir. Temyiz hakkı kapsamında incelemesi yapılacak dosyaların, anayasal bir kurum ve adil yargının ek bir güvencesi olan Danıştay savcılarının katkısı ve incelemesi olmaksızın karara bağlanması, hukuka uygun karar verme ve isabetli içtihatlar tesis etme yönünden Danıştay kararlarının etki ve değerini olduğu kadar, davacıların haklarını da olumsuz yönde etkileyebilecektir. Bu nedenle kural, Anayasa'nın 36. maddesine de aykırıdır.

III- Kanun'un 57. maddesiyle 2577 sayılı Kanun'un 27. maddesinin (2) numaralı fıkrasında yapılan değişikliğin Anayasa'ya aykırılığı:

Yapılan ve iptali istenen değişiklik, hukukun ve idari yargının temel kurumlarından olan yürütmenin durdurulması kurumunun uygulanabilirliğinin, idarenin savunmasının alınması veya avunma süresinin geçmesi koşuluna bağlanmasına ilişkindir.

Hukukun temel prensiplerine ve evrensel bir hukuk ilkesi olan tedbirin amaçlarına bütünüyle aykırı olan ve idari yargı güvencesini büyük ölçüde işlevsiz hale getiren kural her ne kadar müteakip cümlede yapılan uygulanmakla etkisi tükenen olan idari işlemlerin yürütülmesi, savunma alındıktan sonra yeniden karar verilmek üzere, idarenin savunması alınmaksızın da durdurulabilir' düzenlemesi ile dengelenmiş gözükmekte ise de kuralın anayasaya aykırılığı bu şekilde giderilmiş olmamaktadır. Telifisi imkansız veya güç zararların mutlaka uygulanmakla etkisi tükenen

işlemlerden kaynaklanmayabileceği, süreklilik taşıyan işlemlerin de kimi durumlarda kişilerin telafisi imkansız zararlarına yol açabileceği gözetildiğinde, iptali istenen kuralın Anayasa'nın 125. maddesine açıkça aykırı olduğu anlaşılmaktadır. Kuralın iptali gerekir.

IV- Kanun'un 75. maddesiyle 3713 sayılı Kanun'un 10. maddesinin üçüncü fıkrasının (e) bendinde yapılan değişikliğin Anayasa'ya aykırılığı:

Kuralla getirilen değişiklikle, gözaltındaki şüphelinin müdafii ile görüşme hakkının, Cumhuriyet savcısının istemi üzerine, hakim kararıyla yirmidört saat süre ile kısıtlanabileceği, bu süre zarfında ifade alınamayacağı öngörülmüştür.

Anayasa'nın 19. maddesinde kişi hürriyeti ve güvenliği, 36. maddesinde adil yargılanma hakkı düzenlenmiştir. Avrupa İnsan Hakları Sözleşmesi'nin 6. maddesinde adil yargılanma hakkı kapsamında bir müdafiiin yardımından yararlanmak hakkı güvence altına alınmıştır.

Anayasa'nın 36. maddesinin müdafii yardımından faydalanma hakkını kapsadığında şüphe bulunmamaktadır. Avrupa İnsan Hakları Mahkemesinin (AİHM) içtihatlarıyla oluşan, tarafı olduğumuz insan hakları sisteminde savunma hakkının, kişinin özgürlüğünün kısıtlandığı anda başladığı kabul edilmektedir. Gözaltına alınma ile başlayan bir sürecin, tutuklanma ve kesin hükümle mahkumiyetle sonuçlanabilecek olduğu gözetildiğinde, bu sürecin bazı aşamalarında kişi aleyhine istisnalar öngörülmesinin söz konusu olamayacağı açıktır. AİHM'nin 7377/03 sayılı Dayanan v. Türkiyedavasında şüphelinin, polis tarafından yakalanma ve yargılama öncesi tutuklama dahil, hürriyetinden alıkonulduğu anda avukat yardımından yararlanma hakkının doğduğuna (para.31) ve bu sürede sorgunun yapılıp yapılmamasının önem taşımadığına (para.32) hükmedilmiş, sonuç olarak başvuru sahibinin adil yargılanma hakkının ihlal edildiğine oybirliğiyle karar verilmiştir.

Şüphelinin müdafii ile görüştürülmediği 24 saatlik süre içerisinde ifade alınmayacak olması, kuralı anayasaya uygun hale getirmeyeceği gibi, aksine, bu sürenin 5271 sayılı Ceza Muhakemesi Kanunu'nun 138. maddesi ile yasaklanan sorgu öncesi yorma ve benzeri fiziksel veya ruhsal müdahaleler kapsamında değerlendirilmesi gerekmektedir.

Açıklanan nedenlerle kural Anayasa'nın 36. maddesine aykırıdır.

V- Kanun'un GEÇİCİ MADDE 2'sinin (4) numaralı fıkrasının Anayasa'ya aykırılığı:

Geçici Madde 2'nin (4) numaralı fıkrasıyla, 'Ceza Muhakemesi Kanunu'nun yürürlükten kaldırılan 250nci maddesinin birinci fıkrasına göre görevlendirilen mahkemelerde açılmış olan davalara, kesin hükümle sonuçlandırılıncaya kadar, bu mahkemelerce bakmaya devam olunur. Bu davalarda, yetkisizlik veya görevsizlik kararı verilemez. 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele

Kanununun 10 uncu maddesinin kovuşturmayla ilgili hükümleri bu davalarda da uygulanır.' kuralı getirilmiştir. Buna göre, CMK'nun 250 maddesi ile görevli mahkemeler kaldırılmış ve adalet sistemimizden çıkartılmış olmasına rağmen bakmakta oldukları davaları hükme bağlayacakları gibi, temyiz aşamasında bozularak gelen kararlar üzerine de davaya bakmaya devam edeceklerdir.

Anayasa'nın 2. maddesinde Türkiye Cumhuriyeti'nin bir hukuk devleti olduğu, 36. maddesinde herkesin adil yargılanma hakkına sahip bulunduğu, 37. maddesinde hiç kimsenin kanunen tabi olduğu mahkemeden başka bir merci önüne çıkarılamayacağı, 142. maddesinde mahkemelerin kuruluşu, görev ve yetkileri, işleyişi, yargılama usullerinin kanunla düzenleneceği belirtilmiştir.

Ceza Muhakemesi Kanunu'nun mülga 250. maddesi ile görevli ağır ceza mahkemeleri 5.7.2012 tarihi itibarıyla 6352 sayılı Kanun'un 105. maddesi ile kaldırılmış, bunların yerine söz konusu suçları kovuşturmak üzere 3713 sayılı Kanun'un 10. maddesiyle görevli ağır ceza mahkemeleri kurulmuştur. Kuralın gerekçesinin, yeni düzenlemeler nedeniyle karmaşık ve çok sanıklı mevcut davaların yeni mahkemelere devredilmesi nedeniyle birçok usuli işlemlerin tekrarlanması ve yargılamaların uzaması gibi durumlara sebebiyet verilmemesi olduğu belirtilmektedir. Ancak mahkemelerin kaldırılmış olmaları halinde dahi ellerindeki dosyaları sonuçlandırınca kadar faaliyetlerine devam etmeleri, hukukun evrensel bir kuralı olmadığı gibi, uygulamada bir yargılamanın kesin hükümle sonuçlanmasına kadar mahkemede aynı heyetin görev başında kalması da beklenemez. Nitekim bahse konu mahkemelerde de gerek yargıçlar gerek savcılar, soruşturmaların başlamasından bu güne kadar HSYK kararlarıyla pek çok kez değiştirilmiştir. Hem hukukun genel ilkeleri arasında, hem de ceza usul mevzuatımızda, bir yargılamanın mahkemesinden alınarak başka bir mahkemeye verilmesi (davanın nakli) veya temyiz aşamasında bozma kararından sonra başka bir mahkemeye gönderilmesi halleri öngörülmüştür. Bunlar, iptali istenen kuralın gerekçelerini büyük ölçüde çürüten, genel hukuk kurallarıdır. Kaldı ki usuli işlemlerin tekrarına sebebiyet verilmemesi ve yargılamanın uzamaması gibi gerekçeler ancak hüküm verilinceye kadar geçerli olabilir, kesin hükme kadar geçecek aşamalarda dosyanın birçok kez mahkeme ile Yargıtay arasında gidip gelmesi söz konusu olabileceğinden, kaldırılmış olan mahkemelerin yıllarca göreve devam etmesinin herhangi bir yararı ve haklı nedeni bulunmamaktadır.

Kaldırılan mahkemelerde devam edecek olan davalar ve bunların sanıkları bellidir ve bu mahkemelerde yeni davalar açılmayacağından, sadece bu kişileri yargılamak için mevcudiyetlerini sürdüreceklerdir.

Bir hukuk devletinde yasalar kamu yararı amacıyla yapılır. Bunun anlamı, yasaların belli kişilerin lehinde veya aleyhinde belli sonuçlar veya durumlar yaratılması anlamıyla yasa çıkarılmamasıdır.

Ancak iptali istenen kuralla, sadece sanık durumunda olan belli kişiler etkilenmiş, benzer suçlardan yargılanan diğer kişilerden farklı bir yerde yargılanmış olacaklardır. Bu nedenle, kuralın kamu yararı amacıyla getirilmediği sonucuna varmak gerekir.

Yasa koyucunun anayasanın ilkelerine ve hukukun evrensel kurallarına aykırı düşecek bir konuda takdir yetkisi bulunduğundan söz edilemez. Bu nedenle, kuralla getirilen düzenleme Anayasa'nın 142. maddesi ile yasa koyucuya verilen takdir yetkisinin kapsamına girmemektedir.

Açıklanan nedenlerle kural, Anayasa'nın 2. ve 36. maddelerine aykırıdır, iptali gerekir.

Üye - Osman Alifeyyaz PAKSÜT

KARŞIOY GEREKÇESİ

2.7.2012 günlü, 6352 sayılı Yargı Hizmetlerinin Etkinleştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılması ve Basın Yoluyla İşlenen Suçlara İlişkin Dava ve Cezaların Ertelenmesi Hakkında Kanun'un;

1) 1. maddesi ile değiştirilen 9.6.1932 günlü 2004 sayılı Kanun'un 1. maddesinin beşinci fıkrasının incelenmesi;

Fıkra; 'İcra müdür ve icra müdür yardımcıları ve icra katiplerinin yazılı sınav, sözlü sınav, görevlendirme, nakil, unvan değişikliği, görevde yükselme ve diğer hususları yönetmelikle düzenlenir.' denilmektedir.

Anayasa'nın 7. maddesinde yasama yetkisinin Türk milleti adına Türkiye Büyük Millet Meclisine ait olduğu ve bu yetkinin devredilemeyeceği belirtilmiş, 128. maddesinin ikinci fıkrasında ise 'Memurların ve diğer kamu görevlilerinin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülükleri, aylık ve ödenekleri ve diğer özlük işleri kanunla düzenlenir' hükmü yer almıştır.

Bu durumda kamu görevlisi olduklarında kuşku bulunmayan icra müdür, icra müdür yardımcıları ve icra katiplerinin sınav, atanma, görevlendirme, unvan değişikliği, nakil ve diğer özlük hakları ile ilgili hususların kanunla düzenlenmesi gerekirken idari tasarruf niteliğindeki yönetmelikle düzenlenmesini öngören dava konusu fıkra Anayasa'nın 7. ve 128./2 maddesine aykırıdır.

2) 44. maddesi ile 6.1.1982 gün ve 2575 sayılı Danıştay Kanunu'nun değiştirilen 8. maddesinin (3) numaralı fıkrasında yer alan 'onbeş yıl' ibaresinin incelenmesi;

2577 sayılı Yasa'nın üye seçimi başlıklı 9. maddesinde 'Danıştayda boşalan üyeliklerin dörtte üçünün idari yargı hakim ve savcılığında, dörtte biri ise diğer görevliler arasından seçilir.' denilmekte; 8.

maddesinde ise 'Danıştay üyelerinin nitelikleri' sayılmaktadır. Madde hükmünde idari yargı hakim ve savcılarının Danıştay üyesi seçilebilmek için birinci sınıfa ayrıldıktan sonra en az üç yıl bu görevlerde başarı ile çalışmış olmaları ve birinci sınıfa ayrılma niteliğini kaybetmemeleri şartı aranırken, idari görevlerden Danıştay üyeliğine seçileceklerin ise yükseköğrenimlerini tamamladıktan sonra devlet hizmetlerinde onbeş yıl çalışmış bulunmaları ve birinci derece aylığını kazanılmış hak olarak almaları şartı aranmaktadır.

Dava konusu maddede değişiklikten önce idari görevlerden Danıştay üyeliğine seçileceklerde yirmi yıl kamu hizmetlerinde çalışmış olma şartı aranmakta idi.

Anayasa'nın 2. maddesinde Türkiye Cumhuriyeti demokratik bir hukuk devleti olduğu belirtilmiştir. Buna göre Devletin tüm organları Anayasa ve hukukun üstün kuralları ile bağlıdır. Hukuk devleti devlet etkinliklerinin özenle sürdürülebilmesi için gerekli olan hukuksal alt yapıyı oluşturmak suretiyle aynı zamanda istikrarı da sağlar. Bu istikrarın özü hukuki güvenlik ve öngörülebilirliktir. Hukuki güvenlik ve öngörülebilirlik sağlanabilmesi ise kuralların genel, eşit ve nesnel olmalarına bağlıdır.

Dava konusu düzenlemede yer alan ibare ile, Danıştay üyesi seçilebilmek için aranan deneyim ve tecrübe şartının idari görevlerden gelenler yönünden 'onbeş yıl' olarak düzenlenmesi, idari hakim ve savcıların üye seçilebilmek için mesleki beklentilerini zedelediği açıktır.

Kaldı ki 27.6.2013 gün ve 6494 sayılı Yasa ile hakim ve savcıların üye seçilebilmeleri için yirmi yıl meslekte çalışmış olma koşulu aranmaktadır.

Netice olarak Danıştay üyesi seçilebilmek için idari görevlerden gelenler bakımından aranan devlet hizmetinde çalışma koşulunu 'onbeş yıl' a indiren ibare idari yargı hakim ve savcılarının Danıştay üyesi seçilebilmelerinde mesleki öngörülebilirliği ve sonuçta hukuki güvenliğini zedelediğinden Anayasa'nın 2.maddesine aykırı bulunmaktadır.

3) 45. maddesi ile değiştirilen 2575 sayılı Kanun'un 24. maddesinin (1) numaralı fıkrasının (c) bendinin incelenmesi;

İlk derece mahkemesi olarak Danıştay'da görülecek davaları düzenleyen 24. maddenin (1) numaralı fıkrasının (c) bendinde; 'Bakanlıklar veya kamu kurumu niteliğindeki meslek kuruluşlarınca çıkarılan ve ülke çapında uygulanacak düzenleyici işlemlere karşı açılan davaların Danıştayda ilk derece mahkemesi olarak görüleceği belirtilmektedir.

Sözü geçen bend deęişmeden önce 'Bakanlıkların düzenleyici işlemleri ile kamu kuruluşları veya kamu kurumu kuruluşları veya kamu kurumu niteliğindeki meslek kuruluşlarınca çıkarılan ve ülke çapında uygulanacak düzenleyici işlemlere' şeklinde idi.

Buna göre sözü geçen bentde yapılan deęişlikten önce Bakanlıkların tüm düzenleyici işlemlerine karşı açılacak ilk derece davaların Danıştayda görülmesi mümkün iken, dava konusu kural ile sadece ülke çapında uygulama kabiliyetine sahip düzenleyici işlemlere karşı açılacak davaların Danıştayda görülmesi esası getirilmiştir.

Anayasa'nın 2. maddesinde Türkiye Cumhuriyeti demokratik bir hukuk devleti olduğu belirtilmiştir. Buna göre devletin tüm organları anayasa ve hukukun üstün kuralları ile bağlıdır.

İptali istenilen düzenleme ile Bakanlıkların ve kamu kuruluşlarının sadece ülke çapında uygulanacak işlemlerine karşı açılacak davaların Danıştayda görüleceği belirtildiğinden, Danıştayda ilk derece Mahkemesi olarak görülecek davaların sınırlanmasına neden olduğu açıktır.

Açıklanan nedenle kural Anayasa'nın 2. maddesine aykırıdır.

4) 57 maddesi ile 2577 sayılı Kanun'un 27. maddesine eklenen 2 numaralı fıkrada yer alan 'davalı idarenin savunması alındıktan sonra' ibaresinin incelenmesi;

2577 sayılı Kanun'un 27. maddesinin deęişik (2) numaralı fıkrasında 'Danıştay veya idari mahkemeler, idari işlemin uygulanması halinde telafisi güç veya imkansız zararların doğması ve idari işlemin açıkça hukuka aykırı olması şartlarının birlikte gerçekleşmesi durumunda, davalı idarenin savunması alındıktan veya savunma süresi geçtikten sonra gerekçe göstererek yürütmenin durdurulmasına karar verebilirler.' denilmektedir.

Kuralda, Danıştay ve idari mahkemeler idari bir işlemin yürütülmesinin durdurulabilmesi için; uygulanması halinde telafisi güç veya imkansız zararların doğması ve idari işlemin açıkça hukuka aykırı olması şartlarının birlikte gerçekleşmiş olması halinde bu şartların yanı sıra davalı idarenin de savunmasının alınmış olması veya savunma süresinin geçirilmiş olması koşulunun da gerçekleşmesi gerekmektedir.

Anayasa'nın 'yargı yolu' başlıklı 125. maddesinin beşinci fıkrasında 'idari işlemin uygulanması halinde telafisi güç ve imkansız zararların doğması ve idari işlemin açıkça hukuka aykırı olması şartlarının birlikte gerçekleşmesi durumunda gerekçe gösterilerek yürütmenin durdurulmasına karar verilebilir.' hükmü yer almış, maddenin gerekçesinde de yürütmenin durdurulması ile ilgili olarak "hangi hallerde yürütmenin durdurulması kararı verilebileceği açıklıkla belirtilmek yoluna gidilmiştir. Bu şekilde, yürütmenin durdurulması kararı verilebilmesi için madde de gösterilen iki

şartın bir arada bulunması ve ayrıca gerekçe gösterilmesi gerekmektedir.' denilmiştir. Buna göre yürütmenin durdurulması kararı verebilmesi için idari işlemin uygulanması halinde telafisi güç veya imkansız zararın doğması' ve 'idari işlemin açıkça hukuka aykırı olması' koşullarının birlikte gerçekleşmesi gereklidir. Anayasa'da yürütmenin durdurulması ile ilgili olarak başka bir koşul bulunmamaktadır.

Bu durumda iptali istenilen kuralda her ne kadar yürütmenin durdurulması koşulları değiştirilmemekte ise de, bu konuda karar verilmesi için 'davalı idarenin savunması alındıktan veya savunma süresi geçtikten sonra " denilmek suretiyle mahkemelerin bu konuda karar vermesi geciktirilmekte, böylece kişilerin telafisi imkansız zararlarla karşılaşmalarına, bu durumun ise Anayasa'nın 125. maddesinin beşinci fıkrasında öngörülen 'idari işlemin uygulanması halinde telafisi güç veya imkansız zararın doğması' koşulunu etkisiz kılacağı açıktır.

Açıklanan nedenle kural Anayasa'nın 125. maddesine aykırıdır.

5) 75. maddesi ile 3713 sayılı Kanun'un 10. maddesinin üçüncü fıkrasının (b) bendinin ikinci cümlesinin incelenmesi;

3713 sayılı Kanun'un üçüncü fıkrasının (b) bendinde 'Türk Ceza Kanununun 302, 309, 311, 312, 313, 314, 315 ve 316'ncü maddelerinde düzenlenen suçlar hakkında, görev sırasında veya görevinden dolayı işlenmiş olsa bile Cumhuriyet savcılarınca doğrudan soruşturma yapılır. 1.11.1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 26. maddesi hükmü saklıdır.' denilmektedir.

Madde hükmü ile Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nun 26. maddesi hükmü saklı tutulmak suretiyle, 2937 sayılı Yasa kapsamında görevli bulunan bazı kişilerin 3713 sayılı Yasa'da belirtilen suçlar bakımından Cumhuriyet savcılarınca doğrudan soruşturma yapılması önlenmektedir.

Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanun'un 26. maddesinin iptali talebiyle açılan davada Anayasa Mahkemesinin 17.1.2013 günlü, Esas: 2012-19, Karar: 2013-17 sayılı kararında yer alan ve iptali gerektiğine ilişkin karşıoy gerekçemde belirttiğim nedenlerle kural Anayasa'nın 2. maddesine aykırıdır.

6) 75 maddesi ile 3713 sayılı Kanun'un 10. maddesinin üçüncü fıkrasının (e) bendinin incelenmesi;

3713 sayılı Kanun'un 10. maddesinin üçüncü fıkrasının (e) bendinde; 'Gözetimdeki şüphelinin müdafii ile görüşme hakkı, Cumhuriyet savcısının istemi üzerine hakim kararıyla yirmidört saat süre ile kısıtlanabilir; bu zaman zarfında ifade alınamaz' denilmektedir.

Anayasa'nın 36. maddesinde herkesin meşru vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı ve davalı olarak iddia ve savunma ile adil yargılanma hakkına sahip oldukları hükme bağlanmıştır. Savunma hakkını da kapsayan adil yargılanma hakkı sınırlandırılması mümkün olmayan temel bir haktır.

Dava konusu kuralda ise 3713 sayılı Kanun kapsamındaki suçlarla ilgili olarak gözaltına alınan şüphelinin müdafii ile görüşmesi belli bir süre engellenmek suretiyle savunma hakkı kısıtlanmaktadır. Bu nedenle kural Anayasa'nın 36. maddesinde düzenlenen adil yargılanma hakkına aykırıdır.

Açıklanan nedenlerle yukarıda her bölümde açıklanan gerekçelerle Anayasa'ya aykırı olduğu belirtilen kural ve ibarelerin iptali gerektiği düşüncesi ile çoğunluk görüşüne katılmıyorum.

Üye - Zehra Ayla PERKTAŞ

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2011/150

Karar Sayısı: 2013/30

Karar Günü: 14.2.2013

R.G. Tarih-Sayı: 25.06.2013-28688

İPTAL DAVASINI AÇAN: Türkiye Büyük Millet Meclisi üyeleri Emine Ülker TARHAN ve Muharrem İNCE ile birlikte 116 milletvekili

İTİRAZ YOLUNA BAŞVURANLAR:

- 1- Yozgat İdare Mahkemesi (E.2012/41)
- 2- Adana 2. İdare Mahkemesi (E.2012/43, E.2012/44)
- 3- Diyarbakır 1. İdare Mahkemesi (E.2012/53)
- 4- Kastamonu İdare Mahkemesi (E.2012/99)
- 5- Sivas İdare Mahkemesi (E.2012/126)
- 6- Konya 1. İdare Mahkemesi (E.2012/159)

DAVA VE İTİRAZLARIN KONUSU: 11.10.2011 günlü, 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin;

A- İlk ve esas incelemelerinde 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 59. ve 60. maddeleri uyarınca Anayasa Mahkemesi Başkanı Haşim KILIÇ'ın reddine,

B- Tümünün ve ayrı ayrı tüm maddeleri ile eki (I), (II) ve (III) sayılı cetveller ile (1), (2) ve (3) sayılı listelerin Anayasa'nın Başlangıç'ı ile 2., 6., 7., 8., 87. ve 91. maddelerine aykırılığını ileri sürerek iptallerine ve yürürlüklerinin durdurulmasına,

C- 1- 2. maddesinin (2) numaralı fıkrasının sonunda yer alan 'ile ilgili olarak' ibaresinin,

2- 6. maddesinin (1) ve (2) numaralı fıkralarının,

3- 7. maddesinin (1) numaralı fıkrasının (ğ) bendinin,

4- 8. maddesinin (1) numaralı fıkrasının;

a- (c) bendinde yer alan "gerektiğinde süreli veya süresiz iptal etmek" ibaresinin,

b- (ç) bendinin,

c- (e) bendinde yer alan "politika ve düzenlemelerine" ve "gerekli" ibarelerinin,

d- (g), (ğ), (i) ve (k) bentlerinin,

e- (n) bendinde yer alan "sertifikalı eğitim", "ve benzeri eğitimleri" ile "kredilendirme, " ibarelerinin,

f- (o) bendinin,

5- 13. maddesinin (1) numaralı fıkrasının (e) bendinin,

6- 16., 21., 23., 24. ve 26. maddelerinin,

7- 27. maddesinin;

a- (2) numaralı fıkrasının (b) ve (d) bentlerinin,

b- (2) numaralı fıkrasının (ğ) bendinde yer alan 'yaptırmak' sözcüğünün,

c- (2) numaralı fıkrasının (ı) bendinin,

d- (3) numaralı fıkrasının (e) bendinin,

8- 29., 30., 31. ve 32. maddelerinin,

9- 33. maddesinin;

a- (1) numaralı fıkrasının ikinci cümlesinin,

b- (5) numaralı fıkrasının,

10- 34. maddesinin,

11- 36. maddesinin (2) numaralı fıkrasının (b) bendinde yer alan "ikincil düzenlemeleri yapmak," ibaresinin,

12- 45. maddesinin (1) ve (4) numaralı fıkralarının,

13- 47. maddesinin,

14- 48. maddesinin;

a- (1) numaralı fıkrasının (c) bendinin,

b- (2) ve (3) numaralı fıkralarının,

- 15- 49. maddesinin,
- 16- 51. maddesinin (1) ve (3) numaralı fıkralarının,
- 17- 52., 55. ve 56. maddelerinin,
- 18- 57. maddesinin (1) ve (2) numaralı fıkralarının,
- 19- 58. maddesinin;
- a- (6) numaralı fıkrasının (e) bendinin,
- b- (7) numaralı fıkrasının (a) bendiyle deęiřtirilen 7.5.1987 gnl, 3359 sayılı Saęlık Hizmetleri Temel Kanunu'nun ek 1. maddesinin nc fıkrasının,
- c- (7) numaralı fıkrasının (c) bendiyle deęiřtirilen 3359 sayılı Kanun'un ek 9. maddesinin,
- d- (8) numaralı fıkrasının;
- da- (a) bendiyle deęiřtirilen 11.4.1928 gnl, 1219 sayılı Tababet ve řuabatı San'atlarının Tarzı İcrasına Dair Kanun'un 1. maddesinin,
- db- (b) bendiyle;
- dba- 11.4.1928 gnl, 1219 sayılı Kanun'un 4. maddesinin birinci cmlesindeki 'Trk Hekimlerinin' ibaresinin 'hekimlerin' řeklinde deęiřtirilmesinin,
- dbb- 1219 sayılı Kanun'a eklenen Geici Madde 9'un,
- e- (12) numaralı fıkrasının (a), (b) ve (c) bentleriyle 7.6.1985 gnl, 3224 sayılı Trk Diř Hekimleri Birlięi Kanunu'nun 11., 26. ve 40. maddelerinde yapılan deęiřikliklerinin,
- f- (13) numaralı fıkrasının;
- fa- (b) bendiyle deęiřtirilen 4.1.1961 gnl, 209 sayılı Saęlık Bakanlıęına Baęlı Saęlık Kurumları ile Esenlendirme (Rehabilitasyon) Tesislerine Verilecek Dner Sermaye Hakkında Kanun'un 3. maddesinin birinci fıkrasının (d) bendinin,
- fb- () bendiyle deęiřtirilen 209 sayılı Kanun'un 5. maddesinin ikinci fıkrasının,
- g- (14) numaralı fıkrasının (ę) bendinin,
- 20- Geici 4. maddesinin (1), (3) ve (4) numaralı fıkralarının,
- 21- Geici 6. maddesinin,

Anayasa'nın Başlangıç'ı ile 2., 5., 6., 7., 9., 10., 11., 13., 17., 18., 20., 23., 36., 38., 47., 48., 49., 50., 55., 56., 63., 70., 91., 112., 123., 124., 125., 126., 128., 130., 131., 135., 138., 153. ve 168. maddelerine aykırılığı ileri sürülerek iptallerine ve yürürlüklerinin durdurulmasına karar verilmesi istemidir.

II- YASA METİNLERİ

A- Dava ve İtiraz Konusu Kanun Hükmünde Kararname Kuralları

11.10.2011 günlü, 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin iptali istenen kuralları şöyledir:

'MADDE 1- (1) Bu Kanun Hükmünde Kararnamenin amacı; Sağlık Bakanlığı ve bağlı kuruluşlarının teşkilat, görev, yetki ve sorumluluklarını düzenlemektir.

MADDE 2- (1) Bakanlığın görevi; herkesin bedenî, zihnî ve sosyal bakımdan tam bir iyilik hâli içinde hayatını sürdürmesini sağlamaktır.

(2) Bu kapsamda Bakanlık;

- a) Halk sağlığının korunması ve geliştirilmesi, hastalık risklerinin azaltılması ve önlenmesi,
- b) Teşhis, tedavi ve rehabilite edici sağlık hizmetlerinin yürütülmesi,
- c) Uluslararası önemi haiz halk sağlığı risklerinin ülkeye girmesinin önlenmesi,
- ç) Sağlık eğitimi ve araştırma faaliyetlerinin geliştirilmesi,
- d) Sağlık hizmetlerinde kullanılan ilaçlar, özel ürünler, ulusal ve uluslararası kontrole tâbi maddeler, ilaç üretiminde kullanılan etken ve yardımcı maddeler, kozmetikler ve tıbbî cihazların güvenli ve kaliteli bir şekilde piyasada bulunması, halka ulaştırılması ve fiyatlarının belirlenmesi,
- e) İnsan gücünde ve maddî kaynaklarda tasarruf sağlamak ve verimi artırmak, sağlık insan gücünün ülke sathında dengeli dağılımını sağlamak ve bütün paydaşlar arasında işbirliğini gerçekleştirmek suretiyle yurt sathında eşit, kaliteli ve verimli hizmet sunumunun sağlanması,
- f) Kamu ve özel hukuk tüzel kişileri ile gerçek kişiler tarafından açılacak sağlık kuruluşlarının ülke sathında planlanması ve yaygınlaştırılması,

ile ilgili olarak sağlık sistemini yönetir ve politikaları belirler.

(3) Bakanlık bu amaçla;

- a) Strateji ve hedefleri belirler, planlama, düzenleme ve koordinasyon yapar.
- b) Uluslararası ve sektörler arası işbirliği yapar.

- c) Rehberlik, izleme, değerlendirme, teşvik, yönlendirme ve denetleme yapar, müeyyide uygular.
- ç) Acil durum ve afet hallerinde sağlık hizmetlerini planlar ve yürütür.
- d) Bölgesel farklılıkları gidermeye ve herkesin sağlık hizmetine erişimini sağlamaya yönelik tedbirler alır.
- e) İlgili kurum ve kuruluşların insan sağlığını doğrudan ve dolaylı olarak etkileyen faktörler ve sosyal belirleyicilerle ilgili uygulamalarına ve düzenlemelerine yön verir, bunu teminen gerekli bildirimleri yapar, görüş bildirir ve müeyyide uygular.
- f) Görevin ve hizmetin gerektirdiği her türlü tedbiri alır.

(4) İlaç fiyatlarının belirlenmesine ilişkin usûl ve esaslar Bakanlığın teklifi üzerine Bakanlar Kurulunca belirlenir.

MADDE 3- (1) Bakanlık merkez ve taşra teşkilatı ile bağlı kuruluşlardan oluşur.

(2) Bakanlık merkez teşkilatı ekli (I) sayılı cetvelde gösterilmiştir.

MADDE 4- (1) Bakanlık teşkilatının en üst amiri olan Bakan, Bakanlık icraatından ve emri altındakilerin faaliyet ve işlemlerinden Başbakanı karşı sorumlu olup aşağıdaki görev, yetki ve sorumluluklara sahiptir:

- a) Bakanlığın, Anayasaya, kanunlara, hükümet programına ve Bakanlar Kurulunca belirlenen politika ve stratejilere uygun olarak yönetmek.
- b) Bakanlığın görev alanına giren konularda politika ve stratejiler geliştirmek, bunlara uygun olarak yıllık amaç ve hedefler oluşturmak, performans ölçütleri belirlemek, Bakanlık bütçesini hazırlamak, gerekli kanunî ve idarî düzenleme çalışmalarını yapmak, belirlenen stratejiler, amaçlar ve performans ölçütleri doğrultusunda uygulamayı koordine etmek, izlemek ve değerlendirmek.
- c) Bakanlık faaliyetlerini ve işlemlerini denetlemek, yönetim sistemlerini gözden geçirmek, teşkilat yapısı ve yönetim süreçlerinin etkililiğini gözetmek ve yönetimin geliştirilmesini sağlamak.
- ç) Faaliyet alanına giren konularda diğer bakanlıklar ile kamu kurum ve kuruluşları arasında işbirliği ve koordinasyonu sağlamak.

MADDE 5- (1) Müsteşar, Bakandan sonra gelen en üst düzey kamu görevlisi olup Bakanlık hizmetlerini, Bakan adına ve onun emir ve yönlendirmesi doğrultusunda, mevzuat hükümlerine, Bakanlığın amaç ve politikaları ile stratejik planına uygun olarak düzenler ve yürütür. Bu amaçla,

Bakanlık birimlerine gereken emirleri verir, bunların uygulanmasını gözetir ve sağlar. Müsteşar, bu hizmetlerin yürütülmesinden Bakana karşı sorumludur.

(2) Müsteşara yardımcı olmak üzere beş Müsteşar yardımcısı görevlendirilebilir.

MADDE 6- (1) Sağlık Politikaları Kurulu, Bakanlığın sağlık sistemi yönetimi ve politika belirleme ile ilgili temel görevlerini yerine getirmek üzere görevlendirilen onbir üye ile Müsteşar ve müsteşar yardımcılardan meydana gelir.

(2) Kurul üyeleri en az dört yıllık yüksek okul mezunu ve sekiz yıl iş tecrübesi bulunanlar arasından Bakan tarafından görevlendirilir. Görev süresi iki yıldır ve süresi sona eren üyeler yeniden görevlendirilebilir. Kurula Müsteşar veya görevlendireceği yardımcılardan biri başkanlık eder.

(3) Uhdesinde kamu görevi bulunmayan Kurul üyelerine (85.000) gösterge rakamının memur aylık katsayısı ile çarpımı sonucu bulunacak tutarı geçmemek üzere Bakan onayıyla belirlenen tutarda net ödeme yapılır. Bakanlıktan veya diğer kamu kurumlarından görevlendirilen Kurul üyelerine, kadrolarına göre malî haklar kapsamında fiilen yapılmakta olan her türlü ödemeler toplamı ile uhdesinde kamu görevi bulunmayanlara ödenmek üzere bu fıkraya göre belirlenen tutar arasındaki fark ayrıca ödenir.

(4) Kurul toplantılarına, görüşlerini almak üzere üniversiteler, meslek kuruluşları, sendikalar, sivil toplum kuruluşları ile bağlı kuruluşlardan ve Bakanlık birimlerinden yönetici veya uzman kişiler davet edilebilir.

(5) Kurul bünyesinde, Bakanlığın görev alanı ile ilgili olarak bilimsel ve uzmanlık gerektiren konularda çalışma yapmak ve görüş bildirmek üzere danışma kurulları ve komisyonlar oluşturulabilir.

(6) Danışma kurullarında ve komisyonlarda, Bakanlık ve bağlı kuruluşlarının personeli ile üniversitelerden ve diğer kamu ve özel kurum ve kuruluşlarından veya yabancı uzmanlardan görevlendirme yapılabilir.

(7) Kurulun, danışma kurullarının ve komisyonların çalışma usûl ve esasları Bakanlıkça düzenlenir.

MADDE 7- (1) Bakanlığın hizmet birimleri şunlardır:

a) Sağlık Hizmetleri Genel Müdürlüğü.

b) Acil Sağlık Hizmetleri Genel Müdürlüğü.

c) Sağlık Geliştirilmesi Genel Müdürlüğü.

- ç) Sağlık Bilgi Sistemleri Genel Müdürlüğü.
- d) Sağlık Araştırmaları Genel Müdürlüğü.
- e) Sağlık Yatırımları Genel Müdürlüğü.
- f) Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü.
- g) Hukuk Müşavirliği.
- ğ) Denetim Hizmetleri Başkanlığı.
- h) Strateji Geliştirme Başkanlığı.
- ı) Yönetim Hizmetleri Genel Müdürlüğü.
- i) Özel Kalem Müdürlüğü.

MADDE 8- (1) Sağlık Hizmetleri Genel Müdürlüğünün görevleri şunlardır:

- a) Her türlü koruyucu, teşhis, tedavi ve rehabilite edici sağlık hizmetlerini planlamak, teknik düzenleme yapmak, standartları belirlemek ve bu hizmetler ile sunucularını sınıflandırmak, bununla ilgili iş ve işlemleri yaptırmak.
- b) Organ ve doku nakli, kan ve kan ürünleri, diyaliz, üremeye yardımcı tedavi, evde sağlık, yanık, yoğun bakım gibi özellikli planlama gerektiren sağlık hizmetlerini planlamak ve bu hizmetleri sunan kurum ve kuruluşlar arasında koordinasyonu sağlamak.
- c) Kamu ve özel hukuk tüzel kişileri ile gerçek kişilere ait sağlık kurum ve kuruluşlarına izin vermek ve ruhsatlandırmak, bu izin ve ruhsatları gerektiğinde süreli veya süresiz iptal etmek.
- ç) Sağlık hizmetlerinin ücret tarifelerini belirlemek veya tasdik etmek.
- d) Hasta hakları ile hasta ve çalışan güvenliğine yönelik düzenleme yapmak.
- e) Sağlık kurum ve kuruluşlarının mevzuata, Bakanlık politika ve düzenlemelerine uyumunu denetlemek, gerekli yaptırımları uygulamak.
- f) Planlama ve standartlar oluşturulması için gerekli komisyonları kurmak.
- g) Sağlık kurum ve kuruluşları ile hizmetten faydalananlar arasında doğabilecek ihtilafların çözümüne yönelik usûlleri belirlemek.
- ğ) Geleneksel, tamamlayıcı ve alternatif tıp uygulamaları ile ilgili düzenleme yapmak ve sağlık beyanı ile yapılacak her türlü uygulamalara izin vermek ve denetlemek, düzenleme ve izinlere aykırı faaliyetleri ve tanıtımları durdurmak.

h) İlaç, tıbbî cihaz ve ürünler dışında kalan alanlarda yapılacak klinik araştırmalarla ilgili düzenlemeleri yapmak, izin vermek ve denetlemek.

ı) Sağlık hizmetlerinde kalite ve akreditasyon kuralları belirlemek ve uygulamasını sağlamak.

i) Sağlık turizmi uygulamalarının geliştirilmesine yönelik düzenlemeler yapmak, ilgili kurumlarla koordinasyon sağlamak.

j) İlgili mevzuat çerçevesinde kişisel verilerin korunmasına ve veri mahremiyetinin sağlanmasına yönelik düzenleme yapmak.

k) Tıpta uzmanlık eğitimi ile ilgili iş ve işlemleri yürütmek.

l) Sağlık insan gücü planlaması yapmak, sayı ve nitelik olarak ihtiyaca uygun insan gücü yetiştirilmesi için ilgili kurum ve kuruluşlarla işbirliği yapmak.

m) Mevcut sağlık insan gücünü, kamu ve özel kurum ve kuruluşlar düzeyinde planlamak ve istihdamın bu plan çerçevesinde yürütülmesini denetlemek.

n) Sağlık meslek mensuplarının uyum, hizmet içi eğitim, sertifikalı eğitim, görevde yükselme ve unvan değişikliği eğitimleri ve benzeri eğitimleri ile ilgili düzenlemeleri yapmak, koordine etmek, kredilendirme, izleme ve denetimini sağlamak.

o) İlgili kuruluşlarla işbirliği yaparak sağlık mesleklerinin standartlarını belirlemek, eğitim müfredatlarının kanuta dayalı olarak güncellenmesini ve geliştirilmesini sağlamak, sağlık meslek mensuplarının sertifikasyonu ile ilgili işleri yapmak veya yaptırmak.

ö) Sağlık meslek mensuplarının tescil işlemlerini yapmak, kayıtlarını tutmak, personel hareketlerini takip etmek.

p) Bağlı kuruluşların sağlık hizmetleri sınıfına ait personelinin ihtiyaç planlamasını yapmak.

r) Kura ile ataması yapılan sağlık personelinin planlama ve yerleştirme işlemlerini yapmak.

s) Bakan tarafından verilen benzeri görevleri yapmak.

MADDE 9- (1) Acil Sağlık Hizmetleri Genel Müdürlüğünün görevleri şunlardır:

a) Afetlerde ve acil durumlarda ülke genelinde sağlık hizmetlerini planlamak ve yürütmek.

b) Hastane öncesi acil sağlık hizmetlerine ait birimleri kurmak ve işletmek, gerektiğinde hastane acil servisleri ile entegre etmek, ilgili birimlerin faaliyetlerini izlemek, değerlendirmek, hasta nakil ve sevk koordinasyonunu sağlamak.

c) Kara, hava ve deniz ambulanslarının temin, tahsis, sevk ve idaresini sağlamak.

- ç) Yurtiçinde meydana gelen afet ve acil durumlardaki tıbbî kurtarma ve acil sağlık hizmetlerini ilgili tüm taraflarla işbirliği ve koordinasyon içinde sağlamak.
- d) Yurtdışında meydana gelen afet ve acil durumlarda ulusal ve uluslararası kuruluşlar ve sivil toplum örgütleri ile işbirliği içinde sağlık ve insanî yardım faaliyetlerine katılmak.
- e) Afet ve acil durumlara yönelik sağlık hizmetlerinin sunumunda ihtiyaç duyulacak haberleşme, ilaç, tıbbî ve teknik malzemelere yönelik planlama, tedarik, dağıtım ve depolama faaliyetlerini yürütmek.
- f) Tehlikeli kimyasal ve biyolojik maddelere bağlı sağlık tehditlerine yönelik hazırlık ve cevap geliştirilmesi amacıyla gerekli organizasyonu sağlamak.
- g) Toplumun ilkyardım bilgi ve becerisinin geliştirilmesi amacıyla gerekli eğitim faaliyetlerini planlamak ve yürütmek.
- ğ) Görev ve sorumluluk alanı ile ilgili personelin yetiştirilmesi için ilgili kurum ve kuruluşlarla işbirliği içinde eğitim programı hazırlamak ve uygulamak, tatbikat organizasyonları yapmak, ulusal ve uluslararası tatbikatlara katılmak.
- h) Bakan tarafından verilen benzeri görevleri yapmak.

MADDE 10- (1) Sağlık Geliştirilmesi Genel Müdürlüğünün görevleri şunlardır:

- a) Toplumun ve bireyin sağlığı ile ilgili bilgi, farkındalık ve kontrol yeteneklerini artırmak ve bu konuda sorumluluk almalarını ve karar süreçlerine katılmalarını teşvik etmek.
- b) Sağlığı doğrudan ve dolaylı olarak etkileyen faktörlerin ve sosyal belirleyicilerin iyileştirilmesine yardım edecek düzenlemeler yaparak birey sağlığının korunması ve sağlık düzeyinin yükseltilmesine yönelik davranış değişikliği oluşturmak ve sürdürmek.
- c) Sağlığın teşviki ve geliştirilmesine yönelik bilimsel çalışmalar yapmak veya yaptırmak, eğitim kurumları ve basın yayın organları aracılığı ile toplumu bilgilendirmek, kampanyalar yapmak veya yaptırmak.
- ç) Halk sağlığının korunması ve geliştirilmesi, hastalık risklerinin azaltılması, önlenmesi ve teşhis, tedavi ve rehabilite edici sağlık hizmetlerinin daha verimli kullanılabilmesi için uyarıcı, bilgilendirici ve eğitici mahiyette programlar hazırlamak veya hazırlatmak.
- d) Bakanlığın basın ve halkla ilişkilerini ve bilgi edinme hizmetlerini yürütmek.
- e) Bakan tarafından verilen benzeri görevleri yapmak.

MADDE 11- (1) Sağlık Bilgi Sistemleri Genel Müdürlüğünün görevleri şunlardır:

- a) Sağlık alanında kullanılan bilişim sistemleri ve iletişim teknolojileri ile ilgili ülke çapında politika, strateji ve standartları belirlemek.
- b) Kişisel sağlık verileri ile ülke düzeyinde sağlık durumu ve sağlık hizmetlerine ilişkin veri ve bilgi akışını içeren her türden bilgi sistemleri ve projelerini yapmak ve yaptırmak.
- c) Sağlık bilgi sistemleri ve teknolojileri alanında uluslararası gelişmeleri izlemek, ülke uygulamalarını ve tecrübelerini paylaşmak, gerektiğinde uluslararası kuruluşlarla işbirliği yapmak.
- ç) Sağlık bilişimi ve teknolojisi alanında çalışacak kamu ve özel hukuk tüzel kişileri ile gerçek kişilerin uyacakları kuralları belirlemek, uygulamak, gerektiğinde bunların yazılım ve ürünlerinin uygunluğuna karar vermek ve müelliflerini yetkilendirmek.
- d) Bakan tarafından verilen benzeri görevleri yapmak.

MADDE 12- (1) Sağlık Araştırmaları Genel Müdürlüğünün görevleri şunlardır:

- a) Sağlık politikalarının belirlenmesi, izlenmesi, değerlendirilmesi, ülkenin sağlık düzeyinin yükseltilmesi ve sağlık hizmetlerinin geliştirilmesine yönelik ihtiyaç duyulan alanlarda araştırmalar yapmak veya yaptırmak.
- b) Araştırma sonuçlarının ulusal veya uluslararası düzeyde yayımlanmasını sağlamak.
- c) Yurtiçinde ve yurtdışında üretilen sağlık istatistiklerinin derlenmesi, veri kalitesinin değerlendirilmesi, yayımlanması, ulusal ve uluslararası kurumlarla paylaşılması, uluslararası kurumlar tarafından ülkemiz ile ilgili yayımlanan istatistiklerin izlenmesi ve değerlendirilmesini sağlamak, sağlık istatistikleri ile ilgili konularda koordinasyonu sağlamak.
- ç) Sağlık hizmetlerinde çalışan personelin meslekî eğitimi ve gelişimi için eğitim materyallerini hazırlamak, eğitim vermek, seminer, sempozyum, konferans, araştırma ve benzeri etkinlikler düzenlemek.
- d) Uluslararası kurum ve kuruluşların sağlık alanındaki gelişmelerle ilgili yayınlarını takip etmek, gerekli görülenleri tercüme ettirerek yayımlamak.
- e) Koruyucu, rehabilite edici hizmetler, teşhis ve tedavi metotlarının etkililiği, verimliliği, klinik, etik, sosyal, hukukî, organizasyonel ve ekonomik etkileri konularında değerlendirmeler yapmak veya yaptırmak, kanıta dayalı tıp uygulamaları ve klinik rehberler geliştirilmesi ve yaygınlaştırılması faaliyetlerini yürütmek.
- f) Bakan tarafından verilen benzeri görevleri yapmak.

MADDE 13- (1) Sağlık Yatırımları Genel Müdürlüğünün görevleri şunlardır:

- a) Bakanlığın ve bağlı kuruluşların hizmetlerinde kullanılacak binalar için belirlenen ihtiyaç programlarına uygun olarak mühendislik hizmetlerini yürütmek, projelerini hazırlamak veya hazırlatmak.
- b) Gerektiğinde ön veya tam proje ile inşaat ihalelerini yapmak ve bu hizmetler için müşavirlik hizmeti satın almak.
- c) Gerektiğinde Bakanlık ve bağlı kuruluşların inşaatlarının kontrollüğünü yapmak veya yaptırmak.
- ç) Sağlık yapılarının standartlarını belirlemek ve mimarisini geliştirmeye yönelik çalışmalar yapmak.
- d) Bakanlığın ihtiyaç duyduğu taşınmazların kamulaştırma işlemlerini yürütmek.
- e) Bakanlığın ve bağlı kuruluşların ihtiyacı olan tesislerin yapımını ve mevcut tesislerin yenilenmesini kamu özel ortaklığı modeli veya diğer usûller ile gerçekleştirmek.
- f) Sağlık hizmeti sunumunda ihtiyaç duyulan ve ileri teknoloji gerektiren tıbbî cihaz, ürün ve hizmetlerin üretimine, teknolojilerinin geliştirilmesine ve yurtdışından transferine yönelik yerli ve yabancı yatırım ve teknoloji imkânlarını araştırmak, teşvik etmek ve bu ürünlerin off'set ticaretini düzenlemek.
- g) Bakan tarafından verilen benzeri görevleri yapmak.

MADDE 14- (1) Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğünün görevleri şunlardır:

- a) Sağlık alanında yabancı ülkelerle ve uluslararası kuruluşlarla ilişkileri yürütmek, geliştirmek ve bunlarla ilgili hukukî ve idarî düzenlemelere ilişkin çalışmaları yürütmek.
- b) İkili ve çok taraflı anlaşma ve sözleşmelere ilişkin işlemleri yürütmek.
- c) Avrupa Birliği ile ilişkileri, Bakanlığın ilgili birimleri arasında ve Bakanlık ile diğer kurumlar arasında koordinasyonu gerçekleştirmek suretiyle yürütmek.
- ç) Uluslararası nitelikteki kongre, konferans ve toplantılar düzenlemek.
- d) Bakanlığın yurtdışına yönelik iş ve işlemlerini yürütmek.
- e) Bakan tarafından verilen benzeri görevleri yapmak.

MADDE 15- (1) Hukuk Müşavirliğinin görevleri şunlardır:

a) 659 sayılı Genel Bütçe Kapsamındaki Kamu İdareleri ve Özel Bütçeli İdarelerde Hukuk Hizmetlerinin Yürütülmesine İlişkin Kanun Hükmünde Kararname hükümlerine göre hukuk birimlerine verilen görevleri yapmak.

b) Bakan tarafından verilen benzeri görevleri yapmak.

MADDE 16- (1) Denetim Hizmetleri Başkanlığının görevleri şunlardır:

a) Denetime ilişkin yöntem ve teknikleri geliştirmek, denetim alanındaki standart ve ilkelerin oluşturulmasını sağlamak, denetim rehberleri hazırlamak, denetimlerin etkinliğini ve verimliliğini artırıcı tedbirler almak.

b) Bakanlık teşkilatı ile gerektiğinde bağlı kuruluşlarının performans denetimini yapmak.

c) Bakanlık teşkilatı ile gerektiğinde bağlı kuruluşların ve bunların denetimi altındaki kurum ve kuruluşların iş ve işlemleri hakkında denetim, inceleme ve soruşturma yapmak.

ç) Bakan tarafından verilen benzeri görevleri yapmak.

(2) Denetime tâbi olan gerçek ve tüzel kişiler, gizli dahi olsa bütün belge, defter ve bilgileri talep edildiği takdirde ibraz etmek, para ve para hükmündeki evrakı ve ayniyatı ilk talep hâlinde göstermek, sayılmasına ve incelenmesine yardımcı olmak zorundadır. Sağlık Denetçileri, görevleri sırasında kamu kurum ve kuruluşları ve kamuya yararlı dernekler ile gerçek ve tüzel kişilerden gerekli yardım, bilgi, evrak, kayıt ve belgeleri istemeye yetkili olup kanunî engel bulunmadıkça bu talebin yerine getirilmesi zorunludur.

MADDE 17- (1) Strateji Geliştirme Başkanlığının görevleri şunlardır:

a) 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanunu ile 22/12/2005 tarihli ve 5436 sayılı Kanunun 15 inci maddesi ve diğer mevzuatla strateji geliştirme ve malî hizmetler birimlerine verilen görevleri yapmak.

b) Bakanlık Merkez Döner Sermaye İşletmesince elde edilen gelirler ile Döner Sermaye Muhasebe Birimi hesabına aktarılan tutarların tahsisini yapmak.

c) Bakanlığın ve bağlı kuruluşların malî kaynaklarının geliştirilmesi, etkili ve verimli bir şekilde kullanılması yönünde araştırmalar yapmak veya yaptırmak ve gerekli tedbirleri almak.

ç) Bakan tarafından verilen benzeri görevleri yapmak.

MADDE 18- (1) Yönetim Hizmetleri Genel Müdürlüğünün görevleri şunlardır:

- a) Bakanlığın insan gücü planlaması ile insan kaynakları sisteminin geliştirilmesi ve performans ölçütlerinin oluşturulması konusunda çalışmalar yapmak ve tekliflerde bulunmak.
- b) Bakanlık personelinin atama, nakil, terfi, emeklilik ve benzeri özlük işlemlerini yürütmek.
- c) 5018 sayılı Kanun hükümleri çerçevesinde, kiralama ve satın alma işlerini yürütmek, temizlik, güvenlik, aydınlatma, ısınma, onarım, taşıma ve benzeri hizmetleri yapmak veya yaptırmak.
- ç) Bakanlığın taşınır ve taşınmazlarına ilişkin işlemleri ilgili mevzuat çerçevesinde yürütmek.
- d) Genel evrak ve arşiv faaliyetlerini düzenlemek ve yürütmek.
- e) Bakanlık sivil savunma ve seferberlik hizmetlerini planlamak ve yürütmek.
- f) Bakan tarafından verilen benzeri görevleri yapmak.

MADDE 19- (1) Özel Kalem Müdürlüğünün görevleri şunlardır:

- a) Bakanın çalışma programını düzenlemek.
- b) Bakanın resmî ve özel yazışmalarını, protokol ve tören işlerini düzenlemek ve yürütmek.
- c) Bakan tarafından verilen benzeri görevleri yapmak.

MADDE 20- (1) Bakanlıkta, özel önem ve öncelik taşıyan konularda Bakana yardımcı olmak üzere otuz Bakanlık Müşaviri atanabilir.

MADDE 21- (1) Sağlık meslek mensuplarının mesleklerini icra ederken ortaya çıkan adli konularda mahkemelere görüş vermek ve idarî soruşturmacılar ve uzlaşma komisyonları için bilirkişi listesi belirlemek üzere onbeş üyeli Yüksek Sağlık Şûrası kurulmuştur.

(2) Şûra üyelerinin onüçü Bakan tarafından ülkede sağlık hizmetleri veya eserleri ile tanınmış kişiler arasından seçilir.

(3) Müsteşar veya görevlendireceği Müsteşar Yardımcısı ile I.Hukuk Müşaviri veya görevlendireceği hukuk müşaviri, Şûranın doğal üyesidir. Müsteşar veya görevlendireceği Müsteşar Yardımcısı Şûraya başkanlık eder.

(4) Şûra üyelerinin görev süresi iki yıldır. Şûra toplantılarına üst üste iki kez mazeretsiz olarak katılmayanların üyeliği düşer.

(5) Şûra yılda en az dört kere toplanır. Başkan lüzum gördüğü hallerde Şûrayı toplantıya çağırabilir.

(6) Şûra, en az sekiz üyenin katılımıyla toplanır ve oy çokluğu ile karar alır. Oylamalarda çekimser oy kullanılamaz. Oyların eşitliği halinde başkanın oyu yönünde karar alınmış sayılır.

(7) Bakanlık, Şûraya bağlı olarak danışma kurulları ve sağlık mesleklerinin icrasından doğan adli konularda dosyaları inceleyip Şûraya sunmak üzere ihtisas komisyonları oluşturur. Kurul ve Komisyon Başkanları, Şûra toplantılarına oy hakkı bulunmaksızın doğal üye olarak katılır. İhtisas komisyonlarınca hazırlanan rapor ve görüşler, Şûra üyelerince müzakere edilir ve karara bağlanır.

(8) Şûranın toplanmadığı zamanlarda acele işleri karara bağlamak üzere Şûra kendi üyeleri arasından üç kişilik bir alt kurul seçer.

(9) Görev süresi sona eren üyeler ile evvelce üyelik yapmış olanlara Yüksek Sağlık Şûrası Fahrî Üyesi ve başkanlarına da Onursal Başkan unvanı verilir.

(10) Şûranın, danışma kurullarının ve ihtisas komisyonlarının çalışma usûl ve esasları Bakanlık tarafından belirlenir.

MADDE 22- (1) Tıpta ve diş hekimliğinde uzmanlık eğitimi yapacak eğitim kurumlarına eğitim yetkisi verilmesi ve eğitim yetkisinin kaldırılmasına ilişkin teklifleri karara bağlamak, uzmanlık dallarının rotasyonlarını belirlemek, yabancı ülkelerde uzmanlık eğitimi alanların bilimsel değerlendirilmesini yapacak fakülteleri ve eğitim hastanelerini belirlemek, tıpta uzmanlık eğitimi ve uzman insan gücü ile ilgili görüşler vermekle görevli olmak üzere, Tıpta Uzmanlık Kurulu teşkil olunmuştur.

(2) Tıpta Uzmanlık Kurulu;

a) Bakanlık Müsteşarı veya görevlendireceği Müsteşar Yardımcısı, Sağlık Hizmetleri Genel Müdürü ile I. Hukuk Müşaviri veya görevlendireceği hukuk müşaviri,

b) Biri diş tabibi olmak üzere eğitim hastanelerinden Bakanın seçeceği beş,

c) Dört tıp fakültesinden ve bir diş hekimliği fakültesinden Yükseköğretim Kurulunun seçeceği birer,

ç) Gülhane Askeri Tıp Fakültesinin seçeceği bir,

d) Türk Tabipleri Birliğinin seçeceği bir,

e) Türk Diş Hekimleri Birliğinin seçeceği bir,

üyeden oluşur. Asıl üye sayısı kadar yedek üye de belirlenir.

(3) Üye seçecek kurumlar üyeliğin herhangi bir nedenle boşaldığı tarihten itibaren bir ay içinde üye seçerek Bakanlığa bildirmediği takdirde o dönem için ilgili üyelik düşer ve üye sayısında dikkate alınmaz.

(4) Kurula seçilecek asıl ve yedek üyelerin uzman olmaları, ayrıca en az üç yıllık eğitim görevlisi ya da profesör unvanına sahip bulunmaları şarttır. Üyelerin görev süreleri iki yıldır. Süresi bitenler yeniden seçilebilir.

(5) Kurul, Müsteşarın daveti üzerine yılda en az iki kez toplanır; üyelerden en az beşinin teklifi ile de olağanüstü toplanır. Kurula, Müsteşar veya görevlendireceği Müsteşar Yardımcısı veya yapılacak ilk toplantıda üyeler arasından seçilecek başkan vekili başkanlık eder.

(6) Kurul, en az dokuz üyenin katılımı ile toplanır ve oy çokluğuyla karar alır. Oylamalarda çekimser oy kullanılmaz. Oyların eşitliği halinde başkanın bulunduğu taraf çoğunluğu sağlamış sayılır. Türk Tabipleri Birliği temsilcisi yalnızca tabiplerle ilgili, Türk Diş Hekimleri Birliği temsilcisi de yalnızca diş tabipleri ile ilgili konuların görüşüleceği toplantılara katılabilir ve kendi meslek alanları ile ilgili konularda oy kullanır.

(7) Kurul toplantılarına üst üste iki kez mazeretsiz olarak katılmayanların üyeliği düşer.

(8) Kurulun çalışma usûl ve esasları ile ilgili diğer hususlar, ihtisas belgelerinin alınması ve uzmanlık eğitimi ile ilgili diğer usûl ve esaslar yönetmelikle düzenlenir.

MADDE 23- (1) Sağlık mesleklerinde eğitim müfredatı, meslekî alan ve dal belirlemesi gibi meslekî düzenlemelerde ve istihdam planlamalarında görüş bildirmek, meslekî yeterlilik değerlendirmesi yapmak, meslekî müeyyide uygulamak, etik ilkeleri belirlemek ve uyumu denetlemek üzere Sağlık Meslekleri Kurulu teşkil olunmuştur.

(2) Kurul aşağıdaki üyelerden oluşur:

a) Müsteşar veya görevlendireceği müsteşar yardımcısı ile Sağlık Hizmetleri Genel Müdürü veya görevlendireceği bir yetkili temsilci, I. Hukuk Müşaviri veya görevlendireceği hukuk müşaviri, Türkiye Halk Sağlığı Kurumu ve Türkiye Kamu Hastaneleri Kurumu Başkanları veya görevlendirecekleri yardımcısı,

b) Bakanın seçeceği en az doktora seviyesinde eğitim almış 5 ayrı sağlık meslek mensubu üye,

c) En az genel müdür yardımcısı seviyesinde Milli Eğitim Bakanlığı temsilcisi bir üye,

ç) Yükseköğretim Kurulunun seçeceği iki üye,

d) Meslekî Yeterlilik Kurumu temsilcisi bir üye,

e) Kanunla kurulan sağlık meslek birliklerinden birer üye.

(3) Sağlık meslek birliklerinin temsilcileri yalnızca kendi meslek mensupları ile ilgili konuların görüşüleceği toplantılara katılabilir ve kendi meslek alanları ile ilgili konularda oy kullanır.

(4) Seçilmiş üyelerin görev süresi iki yıldır. Kurul toplantılarına üst üste iki kez mazeretsiz olarak katılmayanların üyeliği düşer. İlgili kurumlar bir ay içinde üyelerini seçerek Bakanlığa bildirmediği takdirde o dönem için ilgili kuruma ait üyelik düşer ve üye sayısında dikkate alınmaz.

(5) Kurul, Müsteşar veya müsteşar yardımcısının başkanlığında üye tam sayısının çoğunluğu ile toplanır ve oy çokluğu ile karar alır. Oylamalarda çekimser oy kullanılamaz. Oyların eşitliği hâlinde başkanın oyu yönünde karar alınmış sayılır.

(6) Kurulun görevleri şunlardır:

a) Yeni bir sağlık mesleğinin veya dalının ihdasında görüş bildirmek.

b) Sağlık mesleklerinin eğitim müfredatı hakkında görüş bildirmek.

c) Sağlık mesleklerinin etik ilkelerini belirlemek.

ç) Meslek mensuplarının meslekî yeterlilik ve etik eğitimi ile hasta hakları eğitimine tâbi tutulmasına ve eğitimlerin süresine ve müfredatına karar vermek.

d) Sağlık engeli sebebiyle mesleğin icrasının yasaklanmasına karar vermek.

e) Meslekten geçici veya sürekli men etmeye karar vermek.

(7) Meslekî yetersizliğe ilişkin ihbar ve şikâyetler Kurulca doğrudan değerlendirmeye alınmaz. Bu ihbar ve şikâyetler öncelikle denetim görevlileri veya il ve ilçe sağlık müdürlüklerince incelemeye tâbi tutulur. Yapılan inceleme neticesinde fiilin meslekî yeterlilik değerlendirmesi yapılması veya meslekî müeyyide uygulanması gerektirdiğinin tespit edilmesi hâlinde kanaat raporunu içeren inceleme dosyası Kurula gönderilir. Ayrıca fiil hakkında adlî kovuşturma yapılmış ise, verilen kararlar da Kurula intikal ettirilir. İdarî inceleme veya varsa adlî kovuşturma kapsamında elde edilen bilgi ve belgeler de değerlendirilerek, genel hükümler saklı kalmak üzere Kurulca;

a) Mesleğinde yetersizliği tespit edilenler ile dikkatsiz ve özensiz davranışla ölüme veya vücut fonksiyon kaybına sebep olanların yetersiz görüldükleri alanda meslekî yeterlilik eğitimine tâbi tutulmalarına karar verilir. Bu eğitim, yetersiz görülen alanda teorik ve/veya pratik eğitim ve/veya başka bir sağlık meslek mensubunun nezaret ve sorumluluğunda meslek icrası şeklinde yaptırılabilir. Yeterlilik eğitimine tâbi tutulanlar eğitim sonunda Kurulun belirleyeceği teorik ve/veya uygulamalı sınava tâbi tutulur. Bu sınavda başarılı olanlar mesleğini icraya devam eder; başarısız olanlar meslek icrasından men edilir. Meslekten men edilenler, durumlarına göre Kurulca belirlenen eğitime devam

ettirilerek veya eğitime tâbi tutulmadan yapılacak müteakip sınavlarda başarı gösterdiği takdirde meslek icra etme hakkını yeniden kazanır.

b) Hasta hakları uygulamalarına veya etik ilkelere aykırı davranışı sebebiyle ikiden fazla yazılı ikaz edilen veya ilgili mevzuatına göre disiplin cezası uygulanan sağlık meslek mensubu, hasta hakları veya etik ilkeler eğitim programına tâbi tutulur.

c) Meslek icrası esnasında neticesini öngörerek veya görevinin gereklerine aykırı hareket ederek veyahut görevinin gereklerini yapmakta ihmal veya gecikme göstererek bir kişinin ağır derecede olmayan özür lülüğüne sebebiyet verenlerin üç aydan bir yıla kadar meslekten geçici men edilmesine karar verilir. Bu fiillerin beş yıl içinde tekrarı hâlinde verilecek cezalarda alt ve üst sınırlar iki katı olarak uygulanır.

ç) Meslek icrası esnasında neticesini öngörerek veya görevinin gereklerine aykırı hareket ederek veyahut görevinin gereklerini yapmakta ihmal veya gecikme göstererek bir kişinin ağır özür lülüğüne veya ölümüne sebebiyet verenlerin bir yıldan üç yıla kadar meslekten geçici menine karar verilir. Bu fiillerin beş yıl içinde tekrarı hâlinde meslekten sürekli men kararı verilir.

(8) Mesleğini icra etmesine mâni ve iyileşmesi mümkün olmayan aklî, ruhî ve bedenî hastalığı ortaya konulan sağlık meslek mensupları, Kurulun kararı ile mesleğini icradan yasaklanabilir.

(9) Meslekî yetersizliğinden dolayı bir uzmanlık dalında mesleğini icra edemeyeceğine karar verilen meslek mensuplarının yetersizliğinin niteliğine göre uzmanlık öncesi sahip olduğu sağlık mesleğini icra edebilmelerine karar verilebilir.

(10) Aynı olaydan dolayı ilgili hakkında ceza takibatına veya disiplin soruşturmasına başlanmış olması bu maddeye göre işlem yapılmasını geciktirmez ve engellemez; ilgilinin mahkûm olması veya olmaması ile disiplin cezası verilmiş veya verilmemiş olması hâlleri, ayrıca meslekî müeyyide uygulanmasını etkilemez.

(11) Kanunla kurulmuş meslek odalarının ve birliklerinin kuruluş kanunlarındaki disiplin hükümleri saklıdır. Ancak fiilin her iki kanuna göre de müeyyide gerektirmesi hâlinde bu Kanun hükümleri uygulanır.

(12) Meslekten geçici men edilmesine karar verilen Devlet memurları, men müddetince aylıksız izinli sayılır veya talepleri hâlinde aynı süreyle mesleği ile ilişkisi bulunmayan durumlarına uygun başka bir kadroya atanır. Sözleşmeli olanların sözleşmeleri men müddetince ücretsiz olarak askıya alınır. Meslekten sürekli men edilmesine karar verilen Devlet memurları istekleri hâlinde, mesleği ile ilişkisi

bulunmayan durumlarına uygun başka bir kadroya atanır, aksi halde görevleri sona erer. Meslekten sürekli men edilmesine karar verilen sözleşmeli personelin sözleşmeleri sona erer.

(13) Bu maddeye göre mesleğini geçici olarak sürdüremeyeceklerin durumları kayıtlara işlenir. Meslekten sürekli men edilmesine karar verilenlerin veya mesleğini icra etmekten yasaklananların diplomaları, uzmanlık veya meslek belgeleri Bakanlıkça iptal edilir ve sistemden kaydı silinir.

(14) Bu maddenin uygulanmasına ilişkin usûl ve esaslar Bakanlık tarafından çıkarılacak yönetmelikle düzenlenir.

MADDE 24- (1) Sağlık mesleklerinin uygulanmasından dolayı zarara uğradığını iddia edenlerin dava açma süresi içerisinde bu madde kapsamında yapacakları maddî ve manevî tazminat başvuruları Bakanlık tarafından aşağıdaki şekilde uzlaşma yoluyla halledilir.

- a) Tazminat talebinde bulunan veya bunların birden fazla olması hâlinde aralarından seçecekleri bir temsilci,
- b) Zarar verdiği iddia olunan ilgili meslek mensubu veya bunların birden fazla olması hâlinde aralarından seçecekleri bir temsilci,
- c) Varsa ilgili meslek mensuplarının meslekî malî sorumluluk sigortasını yapan sigorta şirketinin temsilcisi veya bunların birden fazla olması hâlinde ise aralarından seçecekleri bir temsilci,

Bakanlık tarafından uzlaşmaya davet edilir. Tarafların uzlaşma yolunu kabul etmeleri hâlinde, üzerinde anlaşmışları bir hukukçu uzlaştırıcı marifetiyle uzlaşma süreci başlatılır. Uzlaşma en fazla üç ayda sonuçlandırılır. Bu süre bilirkişi görüşleri alınmadığı hallerde tarafların kabulü ile altı aya kadar uzatılabilir. Uzlaşma müracaatı dava açma süresini durdurur. Uzlaşma sağlanamaması hâlinde taraflarca tanzim edilecek tutanak veya taraflardan birinin talebi üzerine Bakanlık tarafından taraflara tebliğ edilerek verilecek belge tarihinden itibaren dava açma süresi yeniden başlar. Uzlaşma sağlanırsa, uzlaşma konusunu, yerini, tarihini, yerine getirilmesi gereken hususları içeren uzlaşma tutanağı tanzim edilir. Bu tutanak 9/6/1932 tarihli ve 2004 sayılı İcra ve İflas Kanununun 38 inci maddesi anlamında ilâm niteliğindedir. Uzlaştırma masrafları ve arabulucu ücreti taraflarca karşılanır. Uzlaşma neticesinde belli bir bedel üzerinde uzlaşma sağlandığında bu bedel doğrudan sigortacı, sigortasının bulunmaması durumunda ilgili personel tarafından ödenir. Bakanlıkça bu madde kapsamında herhangi bir ödeme yapılmaz.

(2) Uzlaştırıcı, meslekî kusur bulunup bulunmadığı hususunda Yüksek Sağlık Şûrasının belirlediği bilirkişilerin; uğranıldığı iddia edilen zarar miktarının hesaplanmasında adlî yargı adalet

komisyonları tarafından her yıl düzenlenecek olan listelerde yer alan bilirkişilerin görüşüne başvurabilir.

MADDE 25- (1) Bakanlığın taşra teşkilâtı; illerde kurulan il sağlık müdürlükleri ile ihtiyaca göre ilçelerde kurulan ilçe sağlık müdürlüklerinden oluşur. İl sağlık müdürleri Bakanlığın ildeki temsilcisi ve valinin sağlık müşaviridir.

(2) İl sağlık müdürlüğü, bağlı kuruluşların il teşkilatının koordinasyonunu yapar ve uyumlu çalışmasını gözetir. Sağlık hizmetleri yönünden ilin durumunu Bakanlıkça belirlenen aralıklarla Bakanlığa rapor eder.

(3) Acil sağlık hizmetleri il ve ilçe sağlık müdürlükleri tarafından yürütülür. Bu müdürlükler söz konusu hizmetlerin yürütülmesi için kamu ve özel hukuk tüzel kişileri ile gerçek kişilere ait tüm sağlık kurum ve kuruluşlarının sevk ve idaresinden sorumlu ve bu konuda yetkilidir.

(4) İl ve ilçe sağlık müdürlüğü yetki devri çerçevesinde Bakanlıkça yürütülen görevleri il ve ilçe düzeyinde yerine getirir, yapılan düzenlemelere uyumu denetler ve gerekli müeyyideleri uygular.

(5) Birden fazla ildeki sağlık hizmetlerinin bir arada değerlendirilmesi, gelişmişlik farklarının giderilmesi ve hizmetlerin ve ihtiyaçların müşterek planlanması amacıyla Bakanlıkça belirlenen illerdeki müdürlerden biri koordinatör olarak görevlendirilebilir.

(6) İlçe sağlık müdürlüğünün kurulmadığı yerlerde sağlık grup başkanlıkları oluşturulabilir. Bu başkanlıklara ayrıca kadro tahsisi yapılmaz ve buralarda gerek duyulan hizmetler ilgili ilçede bulunan personel eliyle yürütülür.

MADDE 26- (1) Bakanlık politika ve hedeflerine uygun olarak, temel sağlık hizmetlerini yürütmekle görevli, Bakanlığa bağlı Türkiye Halk Sağlığı Kurumu kurulmuştur.

(2) Kurumun görev, yetki ve sorumlulukları şunlardır:

a) Halk sağlığını korumak ve geliştirmek, sağlık için risk oluşturan faktörlerle mücadele etmek.

b) Birinci basamak sağlık hizmetlerini yürütmek, bu hususta gerekli düzenlemeleri yapmak.

c) Bulaşıcı, bulaşıcı olmayan, kronik hastalıklar ve kanser ile anne, çocuk, ergen, yaşlı ve engelli gibi risk gruplarıyla ilgili olarak izleme, sürveyans, inceleme, araştırma, bağışıklama ve kontrol çalışmaları yapmak, bununla ilgili verilerin toplanmasını sağlamak, belirlenen hedefler doğrultusunda plan ve programlar hazırlamak, uygulamaya koymak, denetlenmesini sağlamak, değerlendirmek, gerekli önlemleri almak, bu konuda politika ve düzenlemelerin oluşturulması için Bakanlığa teklifte bulunmak.

ç) Yaşam kalitesini yükseltecek alışkanlıkları kazandırarak toplumdaki tüm bireylerin sağlığını geliştirmek; hatalı beslenme alışkanlıkları, obezite, sigara ve benzeri zararlı maddelerin yol açtığı sağlık riskleri ve tehditleri ile mücadele etmek, bu hususları izlemek, araştırmak, veri toplanmasını sağlamak ve değerlendirmek.

d) Birey, toplum ve çevre sağlığını etkileyen ve genel sağlığı ilgilendiren her tür etkeni incelemek, teşhis etmek, değerlendirmek ve kontrol etmek üzere gerekli laboratuvar hizmetlerinin organizasyonunu sağlamak ve ulusal referans laboratuvarı kurmak ve işletmek, içme suları, biyosidal ürünler gibi görev alanına giren konularda tüketici güvenliği ile ilgili tedbirleri almak ve buna yönelik her türlü iş ve işlemleri tesis etmek.

e) Sağlık tehditlerine yönelik erken uyarı ve cevap geliştirilmesi amacıyla gerekli organizasyonu sağlamak, halk sağlığını tehdit eden konularda gereken tüm tedbirleri almak ve gerektiğinde müeyyide uygulamak.

f) Biyolojik ürünler ve test materyali ile benzeri ürünlerle ilgili araştırma ve geliştirme faaliyetlerinde bulunmak, bu ürünleri temin etmek veya edilmesini sağlamak, üretirmek ve gerektiğinde üretmek.

g) Görev ve sorumluluk alanıyla ilgili olarak hizmet standardizasyonunu sağlamak, meslek personelinin yetişmesi için ilgili kurumlarla işbirliğiyle eğitim programları hazırlamak, eğitim ve yayın faaliyetinde bulunmak.

ğ) Görev alanı ile ilgili konularda ulusal veya uluslararası, kamu veya özel kurum ve kuruluşlarla bilimsel ve teknik işbirliği yapmak.

h) Kurum personelinin atama, nakil, özlük, ücret, emeklilik ve benzeri işlemlerini yürütmek.

ı) Kurum hizmetlerinin gerektirdiği her türlü satın alma, kiralama, bakım ve onarım, arşiv, idarî ve malî hizmetleri yürütmek.

MADDE 27- (1) Bakanlık politika ve hedeflerine uygun olarak ilaçlar, ilaç üretiminde kullanılan etken ve yardımcı maddeler, ulusal ve uluslararası kontrole tabi maddeler, tıbbî cihazlar, vücut dışı tıbbî tanı cihazları, geleneksel bitkisel tıbbî ürünler, kozmetik ürünler, homeopatik tıbbî ürünler ve özel amaçlı diyet gıdalar hakkında düzenleme yapmakla görevli, Bakanlığa bağlı, özel bütçeli, kamu tüzel kişiliğini haiz, Türkiye İlaç ve Tıbbî Cihaz Kurumu kurulmuştur.

(2) Kurumun görev, yetki ve sorumlulukları şunlardır:

a) Görev alanına giren ürünlerin ruhsatlandırılması, üretimi, depolanması, satışı, ithalatı, ihracatı, piyasaya arzı, dağıtımı, hizmete sunulması, toplatılması ve kullanımları ile ilgili kural ve standartları

belirlemek, bu faaliyetleri yürütecek kamu ve özel hukuk tüzel kişileri ile gerçek kişilere izin vermek, ruhsatlandırmak, denetlemek ve gerektiğinde yaptırım uygulamak, laboratuvar analizlerini yapmak veya yaptırmak.

b) Sağlık beyanı ile satışa sunulacak ürünlerin sağlık beyanlarını inceleyerek bu beyanlara izin vermek, izinsiz veya gerçeğe aykırı sağlık beyanı ile yapılan satışları denetlemek, gerektiğinde durdurma, toplama, toplatma ve imha iş ve işlemlerini yapmak veya yaptırmak, izin ve sağlık beyanları yönünden bunların her türlü reklam ve tanıtımlarını denetlemek ve aykırı olanları durdurmak, piyasaya arz edilen ilaç, tıbbî cihaz ve ürünlerin reklam ve tanıtımının usûl ve esaslarını belirlemek ve uygulamasını denetlemek.

c) Görev alanına giren ilaç, tıbbî cihaz ve ürünlere ilişkin klinik araştırmalarla ilgili düzenlemeleri yapmak, izin vermek ve denetlemek.

ç) Türk Farmakopesini hazırlamak.

d) Hayati önemi haiz ilaç, tıbbî cihaz ve ürünlerin piyasada sürekli bulunabilmesi için gerekli tedbirleri almak.

e) Tıbbî cihazlar için onaylanmış kuruluşları belirlemek, lisans, ruhsat veya izin vermek, denetim yapmak ve gerektiğinde yaptırım uygulamak.

f) Görev alanına giren ilaç, tıbbî cihaz ve ürünlerle ilgili uyarı sistemlerini kurmak veya kurdurmak, işletmek veya işlettirmek.

g) Kurum personelinin uluslararası karşılıklı tanınma ve akreditasyonunu sağlamak.

ğ) Görev alanına giren ilaç, tıbbî cihaz ve ürünlerin piyasa gözetimi ve denetimini yapmak, gerektiğinde toplatmak, imha etmek veya ettirmek, piyasadaki ürünler için güvenlilik bildirim yöntemlerini belirlemek, gerekli bildirimleri yapmak, laboratuvar analizlerini yapmak veya yaptırmak.

h) İlaç fiyatlarının belirlenmesi için farmako-ekonomik değerlendirme ve çalışmalar yapmak.

ı) Görev alanına giren ilaç, tıbbî cihaz ve ürünleri üretenler, satanlar ve faydalananlar arasında doğabilecek ihtilafların çözümüne yönelik usûlleri belirlemek.

i) Görev alanı ile ilgili faaliyetleri izlemek, değerlendirmek, iyi uygulama örneklerini yaygınlaştırmak, politika üretilmesi ve gerekli düzenlemelerin yapılması için Bakanlığa teklifte bulunmak.

j) Görev alanı ile ilgili konularda ulusal veya uluslararası, kamu kurumları ve üniversiteler ile özel kuruluşlarla bilimsel ve teknik işbirliği yapmak, müşterek çalışmalar yürütmek.

k) Kurum personelinin atama, nakil, özlük, ücret, emeklilik ve benzeri işlemlerini yürütmek.

l) Kurum hizmetlerinin gerektirdiği her türlü satın alma, kiralama, bakım ve onarım, arşiv, idarî ve malî hizmetleri yürütmek.

(3) Kurumun gelirleri şunlardır:

a) Her tür mal ve hizmetin üretim ve sunumu karşılığında elde edilen gelirler.

b) Genel bütçeden yapılacak yardımlar.

c) Kurum gelirlerinin değerlendirilmesinden elde edilen gelirler.

ç) Kuruma ait taşınır ve taşınmazların satış ve kiralanmasından veya işletilmesinden elde edilen gelirler.

d) Görev alanı ile ilgili olarak verilecek kurs, seminer, eğitim, araştırma, yayın, danışmanlık ve benzer hizmetlerden ve kayıt, izin, ruhsat ve sertifikasyon belgelendirmelerinden elde edilen gelirler.

e) Kuruma yapılacak bağışlar ve yardımlar.

f) Diğer gelirler.

MADDE 28- (1) Türk boğazları, hudut ve sahilleri ile ilgili uluslararası sözleşme ve mevzuat hükümlerinden kaynaklanan yükümlülükleri yerine getirmekle görevli, Bakanlığa bağlı, özel bütçeli, kamu tüzel kişiliğini haiz, Türkiye Hudut ve Sahiller Sağlık Genel Müdürlüğü kurulmuştur.

(2) Genel Müdürlüğün görev, yetki ve sorumlulukları şunlardır:

a) Uluslararası önemi haiz halk sağlığı risklerinin ülkemize girmesini önlemek amacıyla, uluslararası giriş noktaları ve bunların gümrüklü alanlarında gerekli her türlü sağlık tedbirini almak veya aldırarak, halk sağlığını etkileyecek etkenlere karşı alınacak kontrol önlemlerinin standardını belirlemek, belgelendirmek, denetlemek.

b) Uluslararası giriş noktalarında hac, göç veya seyahat gibi toplu nüfus hareketlerinde gerekli sağlık tedbirlerini almak veya aldırarak, riskli cenazelerin yurda girişine izin vermek.

c) Malî yılbaşında, sağlık resmi tarifelerini belirlemek, bu gelirler ve diğer sağlık gelirleri ile para cezalarının tarh, tahakkuk ve tahsil işlemlerinin gerçekleştirilmesini sağlamak, gelirlerinden ülke sağlık hizmetlerine katkı sağlamak.

ç) Uluslararası nakil vasıtalarının ve bu vasıtalarda görevli personelin sağlık şartlarını belirleyerek sağlık raporlarıyla ilgili iş ve işlemleri düzenlemek.

d) Görev alanı ile ilgili olarak Dünya Sağlık Örgütü, Uluslararası Denizcilik Örgütü, Uluslararası Sivil Havacılık Örgütü ve diğer ulusal ve uluslararası kuruluşlar ile işbirliği yapmak.

e) Uluslararası önemi haiz halk sağlığı riski olan ülkelere giden insanlara seyahat sağlığı hizmeti vermek.

f) Ulusal ve uluslararası sularda seyir eden gemilere uzaktan sağlık yardımı ve desteği vermek.

g) Uluslararası giriş noktalarında yapılması gereken tüm sağlık hizmetleri, sağlık denetimleri ve çevre sağlığı işlemlerini yürütmek, usûl ve esaslarını belirlemek.

ğ) Kurum personelinin atama, nakil, özlük, ücret, emeklilik ve benzeri işlemlerini yürütmek.

h) Kurum hizmetlerinin gerektirdiği her türlü satın alma, kiralama, bakım ve onarım, arşiv, idarî ve malî hizmetleri yürütmek.

(3) Genel Müdürlük taşradaki görevlerini, Genel Müdürlüğe bağlı sağlık denetleme merkezleri mârifetiyle yerine getirir.

(4) Genel Müdürlükte çalışan memurlar ile sözleşmeli personelden, taşra teşkilatında görev yapan tabipler için en yüksek Devlet memuru aylığının (ek gösterge dâhil) % 400'ünü, merkez ve taşra teşkilatında görev yapan diğer personel için % 200'ünü geçmemek üzere ek ödeme yapılabilir. Ek ödemenin oranı ile usûl ve esasları; görev yapılan birim ve iş hacmi, görevin önem ve güçlüğü, çalışma süresi, personelin sınıfı, kadro unvanı, derecesi ve atanma biçimi gibi kriterler ile personele aylık ve özlük hakları dışında ilgili mevzuatına göre yapılan diğer ilave ödemeler dikkate alınmak suretiyle Maliye Bakanlığının uygun görüşü üzerine Sağlık Bakanlığınca belirlenir. Bu ödemelerden damga vergisi hariç herhangi bir vergi kesilmez.

(5) Genel Müdürlüğün gelirleri şunlardır:

a) 2548 sayılı Gemi Sağlık Resmi Kanunu ve Montrö Boğazlar Mukavelenamesine göre elde edilen gelirler.

b) Her tür mal ve hizmetin üretim ve sunumu karşılığında elde edilen gelirler.

c) Genel bütçeden yapılacak yardımlar.

ç) Genel Müdürlük gelirlerinin değerlendirilmesinden elde edilen gelirler.

- d) Genel Müdürlüğe ait taşınır ve taşınmazların satış ve kiralanmasından veya işletilmesinden elde edilen gelirler.
- e) Görev alanı ile ilgili olarak verilecek kurs, seminer, eğitim, araştırma, yayın, danışmanlık ve benzer hizmetlerden ve kayıt, izin, ruhsat ve sertifikasyon belgelendirmelerinden elde edilen gelirler.
- f) Genel Müdürlüğe yapılacak bağışlar, yardım ve vasiyetler.
- g) Diğer gelirler.

MADDE 29- (1) Bakanlık politika ve hedeflerine uygun olarak, ikinci ve üçüncü basamak sağlık hizmetlerini vermek üzere hastanelerin, ağız ve diş sağlığı merkezlerinin ve benzeri sağlık kuruluşlarının açılması, işletilmesi, faaliyetlerinin izlenmesi, değerlendirilmesi ve denetlenmesi, bu hastanelerde her türlü koruyucu, teşhis, tedavi ve rehabilite edici sağlık hizmetlerinin verilmesini sağlamakla görevli, Bakanlığa bağlı Türkiye Kamu Hastaneleri Kurumu kurulmuştur.

(2) Kurumun görev, yetki ve sorumlulukları şunlardır:

- a) Kuruma bağlı hastaneleri, ağız ve diş sağlığı merkezlerini ve benzeri sağlık kuruluşlarını kurmak ve işletmek, gerektiğinde bunları birleştirmek, ayırmak, nakletmek veya kapatmak.
- b) Kuruma bağlı sağlık kuruluşlarında her türlü koruyucu, teşhis, tedavi ve rehabilite edici sağlık hizmetlerinin yürütülmesini sağlamak, faaliyetlerini izlemek ve değerlendirmek, iyi uygulama örneklerini yaygınlaştırmak, düzenleme yapılması ve politika oluşturulması maksadıyla Bakanlığa teklifte bulunmak.
- c) Performans değerlendirmesi yapmak, rapor hazırlamak, değerlendirme sistematığı için her türlü alt yapıyı kurmak.
- ç) Kendisine bağlı sağlık kuruluşlarında hasta haklarına, hasta ve çalışanların sağlığına ve güvenliğine yönelik iyileştirme çalışmaları yapmak.
- d) Görev alanı ile ilgili konularda ulusal veya uluslararası kamu veya özel kurum ve kuruluşlarla bilimsel ve teknik işbirliği yapmak, müşterek çalışma yürütmek.
- e) Hastane hizmetleriyle ilgili yapılacak çalışmalarda gerekli komisyonları kurmak.
- f) Kurum personelinin atama, nakil, özlük, ücret, emeklilik ve benzeri işlemlerini yürütmek.
- g) Kurum hizmetlerinin gerektirdiği her türlü satın alma, kiralama, bakım ve onarım, arşiv, idarî ve malî hizmetleri yürütmek.

MADDE 30- (1) Kurum tarafından, kaynakların etkili ve verimli kullanılması amacıyla Kuruma bağı ikinci ve üçüncü basamak sağlık kurumları, il düzeyinde Kamu Hastaneleri Birlikleri kurularak işletilir. Hizmetin büyüklüğü gözönünde bulundurulmak suretiyle aynı ilde birden fazla birlik kurulabilir ve bir ilde Birlik kapsamı dışında sağlık kurumu bırakılamaz. Birden fazla Birlik kurulan illerdeki ve belli bölgelerdeki birliklerden biri koordinatör olarak görevlendirilebilir.

(2) Birlik teşkilatı, genel sekreterlik ve hastane yöneticiliklerinden oluşur.

(3) Genel sekreterlik birliğin en üst karar ve yürütme organıdır. Genel sekreterlik bünyesinde tıbbî hizmetler, idarî hizmetler ve malî hizmetler başkanlıkları kurulur.

(4) Birliğe bağı hastaneler hastane yöneticisi tarafından yönetilir. Hastane yöneticisine bağı olarak başhekimlik, idarî ve malî işler ile sağlık bakım hizmetleri müdürlükleri kurulur. Kurum tarafından, birliklerin ve hastanelerin büyüklükleri dikkate alınarak belirlenen hallerde, birlik ve hastanelerdeki yönetim görevleri tek kişiye verilebilir, hastanedeki müdürlüklerin sayısı dörde kadar artırılabilir ve bu durumda görev dağılımları yeniden belirlenir.

(5) Kurumca tespit edilen norm ve standardı aşmamak kaydıyla genel sekreter tarafından belirlenen sayıda başhekim yardımcılıkları ve müdür yardımcılıkları oluşturulur.

MADDE 31- (1) Genel sekreterin görevleri şunlardır:

a) Birliğı belirlenen hedef, politika ve stratejilere, ilgili düzenlemelere ve performans programına göre yönetmek.

b) Birliğin faaliyet ve işlemlerini denetlemek, yönetim sistemlerini değerlendirmek, işleyiş ve yönetim süreçlerinin etkililiğini gözetmek, yönetimin, kalitenin ve verimliliğin geliştirilmesini sağlamak.

c) Birlik bünyesindeki sağlık kurumlarında etkili ve verimli hizmet sunumunu sağlamak, bu amaçla kaynak ve personel ihtiyaçlarını tespit etmek, istihdam planlaması yapmak ve personel hareketlerini gerçekleştirmek.

ç) Hastaneler arası koordinasyon ve diğ er kurum ve kuruluşlarla işbirliğini sağlamak.

d) Bütçe ve yatırım tekliflerini hazırlayarak Kuruma sunmak.

e) Birlik ile ilgili istatistikî bilgilerin takibini sağlamak, birliğin malî tablolarını birleştirmek ve alınabilecek önlemler hakkında Kuruma önerilerde bulunmak.

f) Hasta hakları, hasta ve çalışan memnuniyeti ve hastaların sosyal ihtiyaçlarına yönelik hizmetlerin geliştirilmesini, tıp ve kamu görevlileri etik ilkelerinin uygulanmasını sağlamak.

g) İlgili mevzuat çerçevesinde birlik gelirlerinin tahakkuk ettirilmesini, gelir ve alacakların takip ve tahsili ile harcama işlemleri ve muhasebe hizmetlerinin yürütülmesini sağlamak.

ğ) Birlik ile ilgili diğer görevleri yürütmek.

(2) Genel sekreter gerektiğinde sınırlarını yazılı olarak belirlemek suretiyle yetkilerinden bir kısmını alt birim yöneticilerine devredebilir.

(3) Hastane yöneticisi, hastane ölçeğinde Genel Sekreterin görev, yetki ve sorumluluklarına sahip olup, hastanede tüm hizmetlerin verimli ve mevzuata uygun şekilde yürütülmesinden Genel Sekretere karşı sorumludur.

MADDE 32- (1) Birliklerde, ekli (II) sayılı cetvelde belirtilen pozisyonlarda sözleşmeli statüde personel istihdam edilir. Sözleşmeli personelde 657 sayılı Devlet Memurları Kanununun 48 inci maddesinde sayılan genel şartlar aranır. Birliklerdeki diğer personel, 657 sayılı Kanun ve 10/7/2003 tarihli ve 4924 sayılı Eleman Temininde Güçlük Çekilen Yerlerde Sözleşmeli Sağlık Personeli Çalıştırılması ile Bazı Kanun ve Kanun Hükmünde Karamanelerde Değişiklik Yapılması Hakkında Kanuna tabi olarak çalışır.

(2) Genel sekreter, idarî ve malî hizmetler başkanları, hastane yöneticisi, müdür ve müdür yardımcısı olabilmek için en az dört yıllık eğitim veren yükseköğretim kurumlarından veya bunlara denkliği Yükseköğretim Kurulunca kabul edilmiş yurt dışındaki yükseköğretim kurumlarından mezun olmak ve kamu veya özel sektörde, genel sekreter için 8 yıl, idarî ve malî hizmetler başkanları, hastane yöneticisi ve müdürler için en az 5 yıl iş tecrübesine sahip olmak şarttır.

(3) Tıbbî hizmetler başkanının, tıp alanında doçent veya profesör unvanlı tabip, uzman tabip veya tıp alanında doktora yapmış tabip veyahut hukuk, kamu yönetimi, işletme ve sağlık yönetimi alanında lisans, yüksek lisans veya doktora eğitimi almış tabip; eğitim ve araştırma hastaneleri başhekiminin eğitim görevlisi tabip veya tıp alanında doçent veya profesör unvanlı tabip; diğer hastane başhekimlerinin uzman tabip veya tıp alanında doktora yapmış tabip veyahut hukuk, kamu yönetimi, işletme, sağlık yönetimi alanında lisans, yüksek lisans veya doktora eğitimi almış tabip; yüz yatağın altındaki hastane başhekimlerinin tabip; ağız ve diş sağlığı ile ilgili hastanelerde başhekimin diş hekimi olması; başhekim yardımcılarının ise tıp, diş hekimliği veya eczacılık öğrenimi almış olması veya lisansüstü eğitim yapmış olmaları kaydıyla sağlık bilimleri lisansiyeri olması gerekir.

(4) Genel Sekreterlikte uzman olarak istihdam edilecek personelin alanında en az lisans düzeyinde öğrenim görmüş olması ve kamu veya özel sektörde en az 3 yıl iş tecrübesine sahip olması gerekir. Açıktan alınacak uzman ve büro görevlilerinin Kamu Personeli Seçme Sınavından en az yetmiş puan

almış olmaları şarttır. Uzman ve büro görevlilerinin Birliklere dağılımı, işe alınma usûl ve esasları Kurum tarafından belirlenir. Açıktan istihdam edilen uzmanların oranı Birliğin toplam uzman sayısının yüzde ellisini geçemez.

(5) Sözleşmeli statüde istihdam edilecek personelle yapılacak sözleşme ekinde kurumsal hedefler ve performans değerlendirme kriterleri de gözetilerek hazırlanan bireysel performans kriterleri ve hedefleri belirtilir. Kurum Başkanı, genel sekreterle doğrudan; başkanlar, hastane yöneticileri, başhekim ve müdürlerle genel sekreterin teklifi üzerine sözleşme yapar. Uzman personel ile büro görevlilerinin sözleşmeleri genel sekreter tarafından yapılır. Başhekim yardımcılarıyla başhekimin, müdür yardımcılarıyla ilgili müdürün teklifi üzerine hastane yöneticisi tarafından sözleşme yapılır. Sözleşmelerin süresi iki yıldan dört yıla kadar olabilir. Süre sonunda tekrar sözleşme yapılabilir. Sözleşme eki performans hedeflerindeki gerçekleştirmelere bağlı olarak süresinden önce de sözleşmeler sona erdirilebilir. Başarısızlık sebebiyle genel sekreterin değişmesi halinde başkanların ve başarısızlığa sebebiyet veren hastane yöneticilerinin sözleşmeleri kendiliğinden sona erer. Ancak bunlar yeni görevlendirmeler yapılıncaya kadar görev yapar. Yeni hastane yöneticisinin göreve başlamasından itibaren, ilgili hastane başhekimini, müdürleri, başhekim yardımcıları ve müdür yardımcılarının; yeni başhekim ve müdürlerin göreve başlamasından itibaren de yardımcıların bir ay sonunda sözleşmeleri kendiliğinden sona erer. Sözleşmeleri bu suretle sona eren personel ile yeniden sözleşme yapılabilir. Ekli (II) sayılı cetvelde belirtilen pozisyonlarda açıktan istihdam edilen personelin herhangi bir suretle sözleşmeleri sona erdiğinde birlik ile ilişkileri kesilir. Açıktan sözleşmeli istihdam, memurluk veya diğer personel istihdam şekillerinden birine geçiş bakımından kazanılmış hak teşkil etmez.

(6) Kamu kurum ve kuruluşlarında memur olarak istihdam edilenlerden uygun niteliklere sahip olanlar, kendilerinin isteği ve kurumlarının muvafakati ile ekli (II) sayılı cetvelde belirtilen pozisyonlarda sözleşmeli statüde istihdam edilebilir. Bu şekilde istihdam edilenler kurumlarından aylıksız izinli sayılır. Söz konusu personel aylıksız izinli sayıldıkları kadro unvanları dikkate alınmak suretiyle 5510 sayılı Kanununun 4 üncü maddesinin birinci fıkrasının (c) bendine tabi olmaya devam ederler. Bu görevlerde geçen hizmetleri kazanılmış hak aylık ve derecelerinde değerlendirilir. Sözleşmeleri herhangi bir surette sona eren personel, bir ay içinde kurumuna müracaatı halinde, kurumunca bir ay içinde kadrosuna atanır.

(7) Sözleşmeli personel statüsünde istihdam edilenlerden bu maddenin altıncı fıkrası kapsamına girmeyenler, sosyal güvenlik açısından 5510 sayılı Kanununun 4 üncü maddesinin birinci fıkrasının (a) bendi kapsamında kabul edilirler.

MADDE 33- (1) Ekli (II) sayılı cetvelde belirtilen personele, 657 sayılı Kanunun 4 üncü maddesinin (B) fıkrasına göre belirlenen tavan ücret esas alınarak genel bütçeden ekli (III) sayılı cetvelde belirlenen oranlarda peşin olarak ücret ödenir. Ayrıca personelin katkısıyla elde edilen döner sermaye gelirlerinden aynı cetvelde belirlenen tavan oranları geçmemek kaydıyla ek ödeme yapılabilir. Bakanlıkça belirlenen hizmet sunum şartları ve kriterleri de dikkate alınmak suretiyle, bu ödemenin oranı ile usûl ve esasları; hastanenin grubu, personelin görevi, eğitim durumu, çalışma şartları ve çalışma süreleri, hizmete katkısı, performansı gibi unsurlar esas alınarak Maliye Bakanlığının uygun görüşü üzerine Bakanlıkça belirlenir.

(2) Sözleşmeli personele yapılacak ek ödemeler, çalışmayı takip eden ayın başında yapılır. Sözleşmeli personele yukarıda sayılanlar dışında herhangi bir ad altında ödeme yapılamaz ve sözleşmelere bu hususta hüküm konulamaz.

(3) Sözleşmeli personel; kazanç getirici başka bir iş yapamaz, resmî veya özel herhangi bir müessesede maaşlı, ücretli veya sözleşmeli olarak görev alamaz, serbest olarak sanat ve mesleklerini icra edemez, 657 sayılı Kanunda Devlet memurları için yasaklanmış bulunan eylemlerde bulunamaz.

(4) Sözleşmeli personelin haftalık çalışma süresi emsali Devlet memurları ile aynıdır.

(5) Sözleşmeli personel ihtiyaç halinde Kurumun ve Bakanlığın merkez teşkilatında süreli olarak görevlendirilebilir ve bu husus sözleşmelerde belirtilir.

(6) Sözleşmeli personelin izinleri ve iş sonu tazminatı hususlarında 657 sayılı Kanunun 4 üncü maddesinin (B) fıkrasına göre istihdam edilen sözleşmeli personele ilişkin hükümler uygulanır. Söz konusu personel için işsizlik sigortası primi ödenmez.

MADDE 34- (1) Hastaneler; tıbbî ve malî kriterler ile kalite, hasta ve çalışan güvenliği ve eğitim kriterleri çerçevesinde Kurumca belirlenecek usûl ve esaslara göre altı aylık veya bir yıllık sürelerle değerlendirmeye tabi tutulur. Bu değerlendirme, kamu veya özel değerlendirme kuruluşlarına da yaptırılabilir. Değerlendirme sonuçlarına göre hastaneler yukarıdan aşağıya doğru (A), (B), (C), (D) ve (E) şeklinde gruplandırılır. Birliğin grubu, hastanelerinin ağırlıklı ortalamasına göre belirlenir.

(2) Yapılan değerlendirme sonuçlarına göre birliğin;

a) Grup düşürülmesi,

b) (D) grubunda devralınması halinde, üçüncü değerlendirmede üst gruba çıkarılamaması,

c) (E) grubunda devralınması halinde, ikinci değerlendirmede üst gruba çıkarılamaması,

ç) Bünyesindeki hastanelerden birinin ard arda yapılan iki değerlendirmede de grup düşürülmesi,

d) (E) grubu hastane ile devralınması halinde, ikinci deęerlendirmede bu hastanenin bir üst gruba çıkarılamaması,

hallerinde Kurumca genel sekreterin görevine son verilir. Bu fıkranın (a), (b) ve (c) bentlerinde sayılan hallerin hastane ölçeğinde gerçekleşmesi durumunda ise, genel sekreterce hastane yöneticisinin görevine son verilir.

(3) Yapılan deęerlendirmeler sonucu belirlenen birliklerin ağırlıklı ortalaması, Kurum Başkanının performansının ölçülmesinde esas alınır.

MADDE 35- (1) Türkiye İlaç ve Tıbbî Cihaz Kurumu merkez teşkilatından, dięer baęlı kuruluşlar, merkez ve taşra teşkilatından meydana gelir.

(2) Merkez teşkilatları;

a) Türkiye Hudut ve Sahiller Sağlık Genel Müdürlüğü Genel Müdür, iki genel müdür yardımcılığı, daire başkanlıkları ile strateji geliştirme daire başkanlığından,

b) Başkanlıklar, Başkan, beşer başkan yardımcılığı, daire başkanlıkları, ihtiyaca göre kurulacak danışma ve denetim birimleri ile strateji geliştirme daire başkanlıklarından, meydana gelir.

(3) Baęlı kuruluşların taşra teşkilatı ilgili mevzuatına göre kurulan hizmet birimlerinden meydana gelir. Baęlı kuruluşlardan Türkiye Halk Sağlığı Kurumunun taşradaki yönetim görevi halk sağlığı müdürlüklerince, Türkiye Kamu Hastaneleri Kurumunun taşradaki yönetim görevi kamu hastane birliklerince Kurumlarına baęlı olarak yerine getirilir.

(4) Baęlı kuruluşların taşra teşkilatında çalışan personel, lüzumu halinde bir yılı aşmamak üzere baęlı kuruluşlar arasında 5442 sayılı İl İdaresi Kanunu çerçevesinde geçici olarak görevlendirilebilir. Yapılan görevlendirme personelin Kurumuna bildirilir ve on gün içinde uygun görülmediğine dair bildirim yapılmadığı takdirde görevlendirme işlemi uygulamaya konulur. Gecikmesinde sakınca bulunan hallerde, on günlük süre beklenmeden görevlendirme işlemi uygulamaya konulabilir.

(5) Baęlı kuruluşların personeli 657 sayılı Kanuna tâbidir.

MADDE 36- (1) Baęlı kuruluşların en üst amiri olan Başkanlar ve Genel Müdür, yürütülen hizmetlerden ve emri altındakilerin faaliyet ve işlemlerinden Bakana karşı sorumludur.

(2) Başkanların ve Genel Müdürün görev, yetki ve sorumlulukları şunlardır:

- a) Kurum hizmetlerini mevzuat hükümlerine, kurumun amaç ve politikalarına, stratejik planına uygun olarak yönetmek.
- b) Bakanlık politikalarına uygun şekilde, ikincil düzenlemeleri yapmak, stratejik plan, yıllık performans programları ve faaliyet raporlarını hazırlamak ve uygulamak.
- c) Kurumun faaliyetlerini etkin, etkili, kolay ulaşılabilir ve halkın ve sektörün ihtiyaç ve beklentilerine uygun, ayırım gözetmeyen, şeffaf ve hesap verebilir şekilde yürütmek ve yürütülmesini sağlamak.
- ç) Kurumu temsil etmek.
- d) Kurum bütçesini hazırlamak.
- e) Kurumun görev alanına giren konularda bağlı kuruluşlar ve diğer kurum ve kuruluşlar ile işbirliği yapmak ve koordinasyonu sağlamak.

(3) Başkan yardımcıları ile Genel Müdür yardımcıları, kurumun görevlerinin yürütülmesinde Başkana ve Genel Müdüre yardımcı olmak üzere görevlendirilir ve Başkana ve Genel Müdüre karşı sorumludur.

(4) Hizmet birimlerinin görev tanımları, yetki ve sorumlulukları ile çalışma usûl ve esasları Bakanlıkça çıkarılacak yönetmelikle belirlenir.

MADDE 37- (1) Bakanlık merkez ve taşra teşkilatı ile bağlı kuruluşların her kademedeki yöneticileri, görevlerini mevzuata, stratejik plan ve programlara, performans ölçütlerine ve hizmet kalite standartlarına uygun olarak yürütmekten üst kademelere karşı sorumludur.

MADDE 38- (1) Bakan, Müsteşar ve her kademedeki Bakanlık ve bağlı kuruluş yöneticileri, sınırlarını açıkça belirlemek ve yazılı olmak kaydıyla, yetkilerinden bir kısmını alt kademelere devredebilir. Yetki devri, uygun araçlarla ilgililere duyurulur.

MADDE 39- (1) Bakanlık, hizmet ve görevleriyle ilgili konularda, diğer bakanlıkların ve kamu kurum ve kuruluşlarının uyacakları esasları mevzuata uygun olarak belirlemekle, kaynak israfını önleyecek ve koordinasyonu sağlayacak tedbirleri almakla görevli ve yetkilidir.

(2) Bakanlık, diğer bakanlıkların hizmet alanına giren konulara ilişkin faaliyetlerinde, ilgili bakanlıklara danışmak ve gerekli işbirliği ve koordinasyonu sağlamaktan sorumludur.

(3) Bakanlık, hizmet alanına giren konularda mahallî idarelerle koordinasyonu sağlar.

MADDE 40- (1) Bakanlık ve bağlı kuruluşlar görev, yetki ve sorumluluk alanına giren ve önceden kanunla düzenlenmiş konularda idarî düzenlemeler yapabilir.

MADDE 41- (1) Bakanlık ve bağılı kuruluşlarında;

a) Bakan; Müsteşarın,

b) Müsteşar; müsteşar yardımcıları, kurum başkanları, Sağlık Politikaları Kurulu üyeleri, müstakil birim amirleri ve il müdürlerinin,

c) Başkan ve Genel Müdür; başkan yardımcısı, genel müdür yardımcısı, genel sekreter ve halk sağlığı müdürünün,

ç) Diğer yöneticiler; hiyerarşik olarak kendilerine bağılı bir alt kademedeki personelin,

performanslarını, verilen görevlere ve belirlenen hedeflere göre değerlendirir.

(2) Stratejik planlar, performans programları ve faaliyet raporları 5018 sayılı Kanuna uygun olarak oluşturulur ve ilgili kurumlara iletilir.

MADDE 42- (1) Bakanlık ve bağılı kuruluşlarında, 23/4/1981 tarihli ve 2451 sayılı Bakanlıklar ve Bağılı Kuruluşlarda Atama Usulüne İlişkin Kanunun eki cetvellerde sayılanlar dışında kalan memurların atamaları Bakan tarafından yapılır.

(2) Bakan, gerekli gördüğü hâllerde atama yetkisini merkez teşkilatında alt kademelere ve bağılı kuruluşların üst yöneticilerine, illerde valilere devredebilir.

MADDE 43- (1) Kadroların tespiti, ihdası, kullanımı ve iptali ile kadrolara ilişkin diğer hususlar, 190 sayılı Genel Kadro ve Usulü Hakkında Kanun Hükmünde Kararname hükümlerine göre düzenlenir.

MADDE 44- (1) Bakanlık ve bağılı kuruluşların merkez teşkilatında; Sağlık Uzmanları ve Uzman Yardımcıları ile Sağlık Denetçileri ve Denetçi Yardımcıları istihdam edilir.

(2) Uzman Yardımcılığı ve Denetçi Yardımcılığına atanabilmek için 657 sayılı Devlet Memurları Kanununun 48 inci maddesinde sayılan genel şartlara ek olarak aşağıdaki şartlar aranır:

a) Bakanlık ve bağılı kuruluşlarının görev alanına giren ve yönetmelikle belirlenen alanlarda en az dört yıllık lisans eğitimi veren yükseköğretim kurumlarından veya bunlara denkliği Yükseköğretim Kurulu tarafından kabul edilen yurtiçindeki veya yurtdışındaki yükseköğretim kurumlarından mezun olmak.

b) Yapılacak yarışma sınavında başarılı olmak.

(3) Uzman Yardımcılığı ve Denetçi Yardımcılığına atananlar, en az üç yıl fiilen çalışmak ve istihdam edildikleri birimlerce belirlenecek konularda hazırlayacakları tezin oluşturulacak tez jürisi tarafından kabul edilmesi kaydıyla, yapılacak yeterlik sınavına girmeye hak kazanırlar. Süresi içinde tezlerini

sunmayan veya tezleri kabul edilmeyenlere tezlerini sunmaları veya yeni bir tez hazırlamaları için altı ayı aşmamak üzere ilâve süre verilir. Yeterlik sınavında başarılı olanların Sağlık Uzmanı ve Sağlık Denetçisi kadrolarına atanabilmeleri, Kamu Personeli Yabancı Dil Bilgisi Seviye Tespit Sınavından asgarî (C) düzeyinde veya dil yeterliği bakımından buna denkliği kabul edilen ve uluslararası geçerliliği bulunan başka bir belgeye yeterlik sınavından itibaren en geç iki yıl içinde sahip olma şartına bağlıdır. Sınavda başarılı olamayanlara veya sınava girmeye hak kazandığı hâlde geçerli mazereti olmaksızın sınav hakkını kullanmayanlara, bir yıl içinde ikinci kez sınav hakkı verilir. Verilen ilave süre içinde tezlerini sunmayan veya ikinci defa hazırladıkları tezleri de kabul edilmeyenler, ikinci sınavda da başarı gösteremeyen veya sınav hakkını kullanmayanlar ile süresi içinde yabancı dil yeterliği şartını yerine getirmeyenler Uzman Yardımcısı ve Denetçi Yardımcısı unvanını kaybeder ve Bakanlıkta veya bağlı kuruluşlarında durumlarına uygun başka kadrolara atanırlar.

(4) Uzman Yardımcıları ve Denetçi Yardımcılarının mesleğe alınmaları, yetiştirilmeleri, yarışma sınavı, tez hazırlama ve yeterlik sınavı ile diğer hususlar yönetmelikle düzenlenir.

MADDE 45- (1) Bakanlık ve bağlı kuruluşlarında özel bilgi ve ihtisas gerektiren nitelikli bir işin yapılması veya proje hazırlanması veya yürütülmesi için 657 sayılı Kanun ve diğer kanunların sözleşmeli personel çalıştırılması hakkındaki hükümlerine bağlı olmaksızın proje süresince ve her halde üç yıla kadar sözleşme ile yerli ve yabancı uzman çalıştırılabilir.

(2) Bu şekilde çalıştırılacak personel sayısı yüzelliyi geçemez ve bunların Bakanlık ve bağlı kuruluşlarına dağılımı Bakan tarafından belirlenir.

(3) Sözleşmeli olarak çalıştırılacaklara ödenecek ücret 657 sayılı Kanununun 4 üncü maddesinin (B) fıkrasına göre çalıştırılanlar için uygulanmakta olan sözleşme ücreti tavanının beş katını geçemez. Bu personel, sosyal güvenlik yönünden 5510 sayılı Kanununun 4 üncü maddesinin birinci fıkrasının (a) bendi kapsamında sigortalı sayılır.

(4) Bu suretle çalıştırılacak uzmanların nitelikleri, alınma usûlü ve sözleşme ücretlerinin tespiti ile sözleşme usûl ve esasları Bakanlık ve Maliye Bakanlığınca müştereken belirlenir.

MADDE 46- (1) Bilimsel ve akademik nitelikleri dikkate alınarak Bakan tarafından bilimsel nitelikli komisyonlar ve ruhsatlandırma komisyonlarında görevlendirilenlere (6.500) gösterge rakamının memur aylık katsayısı ile çarpımı sonucu bulunacak tutarı geçmemek üzere ödeme yapılır. Bu ödemelerin usûl, esas ve miktarı Bakanlık ve Maliye Bakanlığınca müştereken belirlenir.

MADDE 47- (1) Bakanlık ve bağılı kuruluşları, mevzuatla kendilerine verilen görevleri, e-devlet uygulamalarına uygun olarak daha etkin ve hızlı biçimde yerine getirebilmek için, bütün kamu ve özel sağlık kurum ve kuruluşlarından; sağlık hizmeti alanların, aldıkları sağlık hizmetinin gereği olarak ilgili sağlık kurum ve kuruluşuna vermek zorunda oldukları kişisel bilgileri ve bu kimselere verilen hizmete ilişkin bilgileri her türlü vasıtayla toplamaya, işlemeye ve paylaşmaya yetkilidir.

(2) Bakanlık ve bağılı kuruluşları işlediği kişisel sağlık verilerini ilgili üçüncü kişiler ve kamu kurum ve kuruluşları ile ancak bu kişi ve kurumların bu verilere erişebileceği hususunda kanunen yetkili olması halinde ve görevlerini yapmalarına yetecek derecede paylaşabilir.

(3) Bakanlık ve bağılı kuruluşları, mevzuatla kendilerine verilen görevleri yerine getirebilmek için gereken bilgileri, kamu ve özel ilgili bütün kişi ve kuruluşlardan istemeye yetkilidir. İlgili kişi ve kuruluşlar istenilen bilgileri vermekle yükümlüdür.

(4) Sağlık personeli istihdam eden kamu kurum ve kuruluşları ile özel hukuk tüzel kişileri ve gerçek kişiler, istihdam ettiği personeli ve personel hareketlerini Bakanlığa bildirmekle yükümlüdür.

(5) Bu maddenin uygulanmasına ilişkin hususlar Bakanlıkça çıkarılacak yönetmelikle düzenlenir.

MADDE 48- (1) İhtiyaç duyulan her türlü tesis, hastane, sağlık eğitim tesisi, sağlık kampüsü, sosyal donatılar ve diğer tesisler, Bakanlık ve bağılı kuruluşları tarafından yaptırılabilir. Bu tesisler, bedelleri;

a) Bakanlığın veya kurumların bütçelerinin ilgili tertiplerine bu amaçla konulan ödeneklerden,

b) Döner sermaye gelirlerinden,

c) Kurumların mülkiyetindeki taşınmazlar veya Maliye Bakanlığının görüşü alınarak Hazinesinin özel mülkiyetindeki taşınmazlardan Bakanlığa veya Kurumlara tahsisli olan taşınmazların üzerindeki yapılarla birlikte devredilmesi suretiyle,

karşılanmak üzere düzenlenecek protokol esasları çerçevesinde Toplu Konut İdaresi Başkanlığına veya inşaat işleriyle ilgili araştırma, proje, taahhüt, finansman ve yapım işlemleri konusunda görevli ve yetkili kamu tüzel kişiliğine sahip diğer kurum ve kuruluşlara da doğrudan yaptırılabilir.

(2) Bakanlık, kamu kurum ve kuruluşlarına ait veya tahsisli taşınmazların kendisine tahsisini veya devrini talep edebilir veya kullanım protokolleri yapabilir. Bu protokoller ile oluşan yükümlülüklerini Toplu Konut İdaresi Başkanlığına veya inşaat işleri ile ilgili araştırma, proje, taahhüt, finansman ve yapım işlemleri konusunda görevli ve yetkili kamu tüzel kişiliğine sahip diğer kurum ve kuruluşlara yaptırabilir.

(3) Bakanlıkça sađlık hizmetlerinde kullanılmakta olan binalardan, Bakanlıkça oluşturulacak komisyon tarafından fonksiyonellik ve/veya onarım-tadilat maliyeti aısından yapılan deęerlendirme sonucunda yıkımının uygun olduęuna karar verilen binalar yıkılabilir. Yıkım kararı verecek komisyonun teřekli ile alıřma usl ve esasları Bakanlıka belirlenir.

Madde 49- (1) Bakanlık, lkenin sađlık alanında blgesel bir cazibe merkezi haline getirilmesi, yabancı sermaye ve yksek tıbbi teknoloji giriřinin hızlandırılması amacıyla, 6/6/1985 tarihli ve 3218 sayılı Serbest Blgeler Kanunu hkmleri erevesinde, sađlık serbest blgelerinin kurulması ve ynetilmesine iliřkin usl ve esaslar Bakanlar Kurulunca belirlenir.

(2) Serbest blgelerde verilecek sađlık hizmetlerine iliřkin usl ve esaslar Bakanlıka belirlenir.

(3) Serbest blgelerde faaliyet gsteren sađlık kurum ve kuruluřlarının aylık gayrisafi hsılatının binde beřini gememek zere Bakanlar Kurulunca belirlenecek oran zerinden hesaplanacak tutar, 3218 sayılı Kanun hkmleri erevesinde ilgili serbest blge idaresi tarafından iřletmecilerinden tahsil edilerek takip eden ayın yirmisine kadar Ekonomi Bakanlıęı merkez muhasebe birimi hesaplarına aktarılır ve genel btye gelir kaydedilir.

Madde 50- (1) Bakanlık, ileri teknoloji gerektirenler bařta olmak zere, lkenin sađlık sektrndeki tıbbi cihaz, rn, hizmet ve ila sanayisinin geliřtirilmesine ve desteklenmesine ynelik politikaları belirler ve uygular. Bu amala giriřimcileri ynlendirir, yerli sanayiye mal ve dięer teřvikleri uygulayabilir, yerli sanayinin teknolojik altyapı ve yeteneklerini arařtırır, bunların geliřtirilmesine ynelik nlemleri alır, gerektięinde yurtdıřından yerli sanayiye teknoloji transferi yapılmasını saęlar.

(2) Bakanlık ve baęlı kuruluřları, sađlık hizmeti sunumunda ihtiya duyulan tıbbi cihaz, ila ve dięer rn ve hizmetlerin alımında mmkn olduęunca yurtii sanayi imkanlarından faydalanır, bu amala yurtii firmalara arařtırma, geliřtirme, prototip ve seri retim faaliyetlerini yaptırır. İhtiya halinde yerli ve yabancı gerek ve tzel kiřilerle alım garantili szleřmeler yapılabilir ve yedi yıla kadar gelecek yıllara yaygın yklenmeye giriřilebilir.

(3) Sađlık hizmeti sunumunda ihtiya duyulan tıbbi cihaz, ila ve dięer rn ve hizmetlerin yurtdıřından alınması ya da bu ynde yurtdıřı kaynaklı yatırım yapılması durumunda, karřılıęında satıcı firmadan yerli sanayi katılımı, Ar-Ge, teknolojik iřbirlięi ve off-set ykmllę istenmesine iliřkin hususlar Bakanlıka dzenlenir.

MADDE 51- (1) Bakanlık ve baęlı kuruluřları insan ve teknik yardım amacıyla yurt dıřında geici sađlık hizmet birimleri kurabilir, kurdurabilir, iřletebilir ve iřlettirebilir; bu amala ulusal ve

uluslararası sivil toplum kuruluşları, finans ve yardım kuruluşları ile işbirliği ve ortak çalışma yapabilir, insan ve malî kaynakları ile destek sağlayabilir.

(2) Bu amaçla görevlendirilen personelin yurt dışındaki görevleri Devlet hizmeti yükümlülüğünden sayılır. Bunlara yurtdışındaki görevleri süresince gündelik verilmez ve gittikleri ülkelerde sürekli görevle bulunan ve dokuzuncu derecenin birinci kademesinden aylık alan meslek memurlarına ödenmekte olan yurt dışı aylığını geçmemek üzere unvanları itibarıyla Bakanlar Kurulu kararıyla belirlenen tutarda aylık ödeme yapılır. Ayrıca, bu personel asıl kadrolarına bağlı olarak aldığı ek ödemesi dâhil her türlü malî ve özlük haklar ile sosyal haklardan faydalanmaya devam eder.

(3) Birinci fıkra kapsamında hizmet alımı veya kamu özel ortaklığı modeliyle özel sektör tarafından işletilen sağlık hizmet birimlerinde ve bölümlerinde çalıştırılacak Bakanlık personeli beş yılı geçmemek üzere çalıştıkları sürede aylıksız izinli sayılır.

MADDE 52- (1) Sağlık hizmeti sunmaya yetkili gerçek ve tüzel kişilerce sosyal dayanışma ve yardımlaşma amacıyla gönüllü ve ücretsiz olarak sağlık hizmeti verilebilir.

(2) Bu hizmeti yürüteceklere Bakanlıkça izin verilir. İzin talebinde bulunanlara gerekli değerlendirmeler yapıldıktan sonra sağlık gönüllüsü yetki belgesi düzenlenir.

(3) Sağlık gönüllüsü gerçek kişiler hastanelerdeki hizmetlerini hastane yetkilisinin belirlediği şartlarda verebilir. Bu hizmet hastanelerin doğrudan sağlık hizmeti olmayan hasta karşılama ve bilgilendirme, refakat, kişisel bakım ve sosyal ihtiyaçların karşılanması gibi destek hizmeti şeklinde de verilebilir. Bu halde sağlık gönüllüsünün sağlık meslek mensubu olma mecburiyeti yoktur.

(4) Gönüllü sağlık hizmeti sunumu ile gönüllülere ait bilgilerin kamuoyu ile paylaşımına dair usûl ve esaslar Bakanlıkça belirlenir.

(5) Sağlık kurum ve kuruluşlarında hizmetin geliştirilmesi amacıyla Bakanlık, hizmetten faydalananların gönüllülük esasına göre yapacakları gözlemlerini değerlendirmek üzere gerekli düzenlemeleri yapar.

MADDE 53- (1) Bakanlık halk sağlığının korunması ve geliştirilmesi, hastalık risklerinin azaltılması ve önlenmesi ile teşhis, tedavi ve rehabilite edici sağlık hizmetlerinin daha verimli kullanılabilmesi için uyarıcı, bilgilendirici ve eğitici mahiyette programlar hazırlar veya hazırlatır. Bu programlar Bakanlıkça, Türkiye Radyo ve Televizyon Kurumu ile ulusal, bölgesel ve yerel yayın yapan özel televizyon kuruluşları ve radyolara gönderilir. Her bir yayın kuruluşu tarafından sözkonusu programlar ayda doksan dakikadan az olmamak üzere 08:00-22:00 saatleri arasında yayınlanır. Bu yayınların asgari otuz dakikası 17:00-22:00 saatleri arasında yapılır. Belirlenen saatler dışında yapılan

yayımlar, aylık doksan dakikalık süreye dâhil edilemez. Bu yayımların ve sürelerinin denetimi Radyo ve Televizyon Üst Kurulunca yapılır.

MADDE 54- (1) Bakanlık ve bağılı kuruluşlarında; sağılık hizmeti sunumu sırasında veya bu görevlerden dolayı personele karşı işlenen suçlar sebebiyle ceza hukuku kapsamında yürütölmekte olan işlemler ve davalarda personelin talebi üzerine Bakanlık ve bağılı kuruluşlarınca hukukî yardım yapılır. Bu yardımın usûl ve esasları Bakanlıkça belirlenir.

MADDE 55- (1) Bakanlık, kamu ve özel bütün sağılık kuruluşlarında çalışmakta olan sağılık personeli için görevli olduğı kuruluşun bulunduğı yerleşim yeri sınırları içinde ikamet etme mecburiyeti getirebilir. Bu mecburiyetin usûl ve esasları Bakanlıkça belirlenir.

MADDE 56- (1) Bakanlık veya bağılı kuruluşlarının kadrolarında tıpta ve diş hekimliğinde uzmanlık mevzuatına göre diğerk kamu kurum ve kuruluşlarında uzmanlık eğitimi veya yan dal uzmanlık eğitimi yaptırılabilir. Bu şekilde eğitim yapmak isteyenler, döner sermaye ek ödemesi hariç her türlü malî ve sosyal hakları Bakanlık veya bağılı kuruluşları tarafından karşılanmak üzere ilgili kurum ve kuruluşlarda görevlendirilebilir. Bunlar, eğitimlerini tamamladıklarında görevlendirme süresi kadar Bakanlık veya bağılı kuruluşlarında hizmet yapmakla yükümlüdür. Söz konusu personelden örneğı Maliye Bakanlığı tarafından hazırlanmış, yüklenme senedi ile muteber imzalı müteselsil kefalet senedi alınır. Bunların hizmet yükümlölüğünü yerine getirmeden görevinden ayrılması, müstafi sayılması, görevine son verilmesi veya Devlet memurluğundan çıkarılması halinde, kendileri için Bakanlıkça yapılmış olan her türlü ödemeler toplamından, varsa hizmetin tamamlanan kısmı için hesaplanan miktar indirildikten sonra bakiye miktar kendilerinden kanuni faizi ile birlikte tahsil edilir. Tahsilat, borç miktarı ve ilgilinin durumu dikkate alınarak azami beş yıla kadar taksitlendirilerek yapılır.

(2) İlgililerin uzmanlık eğitiminde başarısızlığı veya kendi istekleri ile uzmanlık eğitimini bırakmaları durumunda ise, görevlendirme süresi kadar Bakanlığa hizmet yapmaları zorunludur. Belirtilen hizmet süresi kadar Bakanlığa hizmet yapmak istemeyenlere yapılmış olan her türlü masrafların tamamı birinci fıkradaki esaslara göre ödettirilir.

MADDE 57- (1) Bakanlık ve bağılı kuruluşlarınca düzenlenecek veya onaylanacak her türlü ruhsatlandırma, ürün üretim ve satış izin belgesi ve mesul müdürlük belgesi ile permi ve sertifikalar üzerinden yüzellibin Türk Lirasını geçmemek üzere Bakanlıkça belirlenecek tarifelere göre ücret alınır. Ancak Bakanlıkça alınması teşvik edilen belgelerden ücret alınmayabilir. Bu tarifeler her yıl güncellenir ve ücretler 213 sayılı Vergi Usûl Kanununa göre belirlenen yeniden değerlendirme oranında artırılır.

(2) Bakanlık veya bağı kuruluşlarınca düzenlenecek, Bakanlık ve bağı kuruluşlarının planlamaları çerçevesinde, gerçek veya tüzel kişilere sağlık alanında belirli bir hizmeti verebilme veya hastane ve benzeri sağlık kuruluşları açabilme yetkisi veren lisansları açık arttırma ile belirlenecek bedel karşılığında verilir. Lisans verilmesi ilgili faaliyet için gerekli olan izin veya ruhsat yerine geçmez. Lisans verilmesinin usûl ve esasları Bakanlıkça belirlenir.

(3) Bu madde kapsamında tahsil edilen tutarlar ilgisine göre genel bütçeye veya özel bütçeli bağı kuruluşların bütçelerine gelir kaydedilir.

MADDE 58- (1) 23/4/1981 tarihli ve 2451 sayılı Bakanlıklar ve Bağı Kuruluşlarda Atama Usûlüne İlişkin Kanunun eki (2) sayılı cetvele 'Vergi Dairesi Başkanları,' ibaresinden sonra gelmek üzere 'Türkiye Kamu Hastaneleri Kurumu Başkanı ve Başkan Yardımcıları, Türkiye İlaç ve Tıbbî Cihaz Kurumu Başkanı ve Başkan Yardımcıları, Türkiye Halk Sağlığı Kurumu Başkanı ve Başkan Yardımcıları,' ibaresi eklenmiştir.

(2) 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununa ekli (I) Sayılı Cetvele '53) Türkiye Halk Sağlığı Kurumu' ve '54) Türkiye Kamu Hastaneleri Kurumu' sıraları eklenmiş; (II) Sayılı Cetvelin 'B) Özel Bütçeli Diğer İdareler' bölümünün 18 numaralı sırasında yer alan 'Hudut ve Sahiller Sağlık Genel Müdürlüğü' ibaresi 'Türkiye Hudut ve Sahiller Sağlık Genel Müdürlüğü' olarak değiştirilmiş ve aynı Cetvele '44) Türkiye İlaç ve Tıbbî Cihaz Kurumu' sırası eklenmiştir.

(3) 190 sayılı Kanun Hükmünde Kararnamenin eki (I) sayılı Cetvelde yer alan Refik Saydam Hıfzıssıhha Merkezi Başkanlığı ve Hudut ve Sahiller Sağlık Genel Müdürlüğü kadroları ile birlikte çıkarılmış; Sağlık Bakanlığına ait kadrolar iptal edilmiştir.

(4) Ekli (1) sayılı listede yer alan kadrolar ihdas edilerek 190 sayılı Kanun Hükmünde Kararnamenin eki cetvellere, Sağlık Bakanlığı, Türkiye Kamu Hastaneleri Kurumu, Türkiye Halk Sağlığı Kurumu, Türkiye İlaç ve Tıbbî Cihaz Kurumu, Türkiye Hudut ve Sahiller Sağlık Genel Müdürlüğü bölümleri olarak eklenmiştir.

(5) 10/2/1954 tarihli ve 6245 sayılı Harcırah Kanununun 33 üncü maddesinin (b) fıkrasına 'Millî Eğitim Denetçileri ve Millî Eğitim Denetçi Yardımcıları ile İl Eğitim Denetmenleri ve İl Eğitim Denetmen Yardımcıları,' ibaresinden sonra gelmek üzere 'Sağlık Denetçileri ve Sağlık Denetçi Yardımcıları' ibaresi eklenmiştir.

(6) 657 sayılı Devlet Memurları Kanununun;

a) 36 ncı maddesinin 'Ortak Hükümler' bölümünün (A) fıkrasının (11) numaralı bendine 'Millî Eğitim Uzman Yardımcıları ve Millî Eğitim Denetçi Yardımcıları,' ibaresinden sonra gelmek üzere 'Sağlık

Uzman Yardımcıları ve Sağlık Denetçi Yardımcıları'; 'Millî Eğitim Uzmanlığına ve Millî Eğitim Denetçiliğine,' ibaresinden sonra gelmek üzere 'Sağlık Uzmanlığına ve Sağlık Denetçiliğine'

b) 152 nci maddesinin 'II- Tazminatlar' kısmının 'A- Özel Hizmet Tazminatı' bölümünün (b/1) bendindeki 'klinik şefi, klinik şef yardımcısı' ibareleri 'Eğitim görevlisi,' şeklinde değiştirilmiştir; (g) bendine 'Millî Eğitim Denetçi ve Denetçi Yardımcıları' ibaresinden sonra gelmek üzere 'Sağlık Denetçi ve Denetçi Yardımcıları'; (h) bendine 'İl Eğitim Denetmenleri' ibaresinden sonra gelmek üzere 'Sağlık Uzmanları'

c) Eki (I) sayılı Ek Gösterge Cetvelinin;

1) 'I- Genel İdare Hizmetleri Sınıfı' bölümünün (d) bendine 'Müsteşar Yardımcıları ve Genel Müdürler' ibaresinden sonra gelmek üzere ', Türkiye Halk Sağlığı Kurumu Başkanı, Türkiye İlaç ve Tıbbî Cihaz Kurumu Başkanı, Türkiye Kamu Hastaneleri Kurumu Başkanı';(g) bendine 'Denizcilik Uzmanları' ibaresinden sonra gelmek üzere ', Sağlık Uzmanları ve Sağlık Denetçileri,'

ç) Eki (II) sayılı Ek Gösterge Cetvelinin '2. Yargı Kuruluşları, Bağlı ve İlgili Kuruluşlar ile Yüksek Öğretim Kuruluşlarında' başlıklı bölümünde yer alan 'Devlet Personel Başkanlığı Başkan Yardımcısı' ibaresinden sonra gelmek üzere 'Türkiye Halk Sağlığı Kurumu Başkan Yardımcısı, Türkiye İlaç ve Tıbbî Cihaz Kurumu Başkan Yardımcısı, Türkiye Kamu Hastaneleri Kurumu Başkan Yardımcısı'

d) Eki (IV) sayılı Makam Tazminatı Cetvelinin 8 inci sırasının (a) bendine 'Millî Eğitim Denetçileri' ibaresinden sonra gelmek üzere 'Sağlık Denetçileri' ile (b) bendine 'Millî Eğitim Uzmanları' ibaresinden sonra gelmek üzere 'Sağlık Uzmanları'

ibareleri eklenmiştir;

e) Ek 33 üncü maddesindeki tablonun (a) sırasında geçen 'Klinik şefi, şef yardımcısı' ibareleri 'Eğitim görevlisi' şeklinde değiştirilmiştir.

(7) 7/5/1987 tarihli ve 3359 sayılı Kanunun;

a) Ek 1 inci maddesi aşağıdaki şekilde değiştirilmiştir.

'Ek Madde 1- Kamu kurum ve kuruluşlarının uzman tabip, tıpta uzmanlık mevzuatına göre uzman ve tabip kadro ve pozisyonlarına yapılacak açıktan atamalar, açıktan atama izni alınmaksızın mevzuatta öngörülen işlemlerin tamamlanmasından sonra gerçekleştirilir ve bunların yerleştirilmeleri Sağlık Bakanlığınca sınavsız ve kura ile yapılır. Kura ile yapılacak atamalara ilişkin usûl ve esaslar Sağlık Bakanlığınca çıkarılacak yönetmelikle belirlenir.

Tıpta ve diş hekimliğinde uzmanlık eğitimi, ilgili dalda tıpta uzmanlık mevzuatına göre uzman olan profesör, doçent, yardımcı doçent, eğitim görevlisi ve başasistanlar tarafından verilir. Yardımcı doçent ve başasistanların tıpta uzmanlık eğitim verebilmeleri için bu kadrolarda bir yıl çalışmaları şarttır.

Eğitim ve araştırma hastanelerinde eğitim görevlilerinden biri hastane yöneticisi tarafından bir yıllık süre için ilgili birimin eğitim sorumlusu olarak görevlendirilir, idarî sorumlusu ise aynı süreyle ilgili daldaki uzmanlar arasından seçilir. Birimin eğitim sorumlusuna idarî sorumluluk görevi de verilebilir.

Eğitim görevlisi, başasistan ve asistan kadrolarına açıktan atama izni alınmaksızın ilgili mevzuatı çerçevesinde atama yapılır.

Başasistan kadrolarına atamalar, ilgili dalda uzman olan ve meslekî çalışma, bilimsel yayın ve yabancı dilde yeterliliği bulunan tabip, diş tabipleri ve tıpta uzmanlık mevzuatına göre uzman olanlar arasından Kurumca yapılacak veya yaptırılacak meslekî sınavla yapılır.

Profesör veya doçentlerin eğitim ve araştırma hastanelerine eğitim görevlisi olarak atanmaları, Kurumca yapılacak ilan üzerine müracaat eden adayların bilimsel çalışmaları ve eğitici nitelikleri değerlendirilerek yapılır. Adayların bilimsel çalışmalarını ve eğitici niteliklerini değerlendirmek üzere ilgili uzmanlık alanlarında üç profesör tespit edilir. Bunlar adaylar hakkındaki mütalaalarını, öncelik sıralaması yaparak ayrı ayrı bildirir ve bu mütalaalara göre görevlendirme yapılır.

Başasistan olarak atanma ve yeterlilik kriterleri ile sınavlara ilişkin usûl ve esaslar Sağlık Bakanlığı tarafından yönetmelik ile düzenlenir.'

b) Ek 7 nci maddesinin birinci fıkrasının sonuna aşağıdaki cümle eklenmiştir.

'Değeri yirmi milyon Türk Lirasına kadar olan tesislerin bu madde kapsamında yaptırılmasına Sağlık Bakanınca karar verilebilir.'

c) Ek 9 uncu maddesi aşağıdaki şekilde değiştirilmiştir.

'Ek Madde 9- Sağlık Bakanlığı ve bağlı kuruluşlarına ait kurum ve kuruluşlar ile üniversitelerin ilgili birimleri, karşılıklı olarak işbirliği çerçevesinde birlikte kullanılabilir. Üniversite tarafından, birlikte kullanılan kurum ve kuruluşlarda görevli personelin profesör ve doçent kadrolarına atanabilmesi için Bakanlığa ve bağlı kuruluşlarına ait eğitim görevlisi kadroları da kullanılabilir. Birlikte kullanım ve işbirliğine ilişkin usûl ve esaslar ile ilgili mevzuat hükümleri çerçevesinde döner sermaye

gelirlerinden personele yapılacak ek ödemelere ilişkin esaslar Maliye Bakanlığı ve Yükseköğretim Kurulunun görüşü alınarak Sağlık Bakanlığı tarafından çıkarılacak yönetmelikle belirlenir.'

(8) 11/4/1928 tarihli ve 1219 sayılı Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanunun;

a) 1 inci maddesi aşağıdaki şekilde değiştirilmiştir.

'Madde 1- Türkiye Cumhuriyeti dâhilinde tababet icra ve her hangi surette olursa olsun hasta tedavi edebilmek için tıp fakültesinden diploma sahibi olmak şarttır.'

b) 4 üncü maddesinin birinci cümlesindeki 'Türk hekimlerinin' ibaresi 'hekimlerin' şeklinde değiştirilmiş ve aynı Kanuna aşağıdaki geçici madde eklenmiştir.

'Geçici Madde 9- 1/1/2020 tarihine kadar, 24/11/2004 tarihli ve 5258 sayılı Kanun hükümlerine göre sözleşmeli aile hekimi olarak çalışmakta olanlar, tıpta uzmanlık sınavı sonuçlarına göre, merkezi yerleştirmeye tabi olmaksızın, Tıpta Uzmanlık Kurulunca belirlenen esaslar çerçevesinde aile hekimliği uzmanlık eğitimi yapabilir. Bu eğitim uzaktan ve/veya kısmî zamanlı eğitim metotları da uygulanmak suretiyle yapılabilir ve en az altı yılda tamamlanır. Eğitim süresince aile hekimliği sözleşmesi devam eder. Uzmanlık eğitimi ile beraber aile hekimliği hizmetlerinin yürütülmesine, ilgililere ve eğitim sorumlularına ödenecek ücretlere ilişkin usûl ve esasları 5258 sayılı Kanunun 8 inci maddesine göre hazırlanan yönetmeliklerle belirlenir.

Bu maddeye göre yapılacak aile hekimliği uzmanlık eğitiminde çekirdek eğitim müfredatının ve rotasyonların uygulanması ve eğitimin şekli ile sair hususlar Tıpta Uzmanlık Kurulunca belirlenir.'

(9) 25/2/1954 tarihli ve 6283 sayılı Hemşirelik Kanununun 3 üncü maddesi aşağıdaki şekilde değiştirilmiştir.

'Madde 3- Bu Kanun hükümlerine göre hemşire unvanı kazanmış olanların dışında hiç kimse Türkiye'de hemşirelik mesleğini icra edemez.'

(10) 24/11/2004 tarihli ve 5258 sayılı Aile Hekimliği Pilot Uygulaması Hakkında Kanunun;

a) Adı 'Aile Hekimliği Kanunu' olarak değiştirilmiş ve 1 inci maddesinde geçen 'pilot olarak' ibaresi yürürlükten kaldırılmıştır.

b) 3 üncü maddesinin birinci fıkrasındaki 'görevlendirmeye' ibaresinden sonra gelmek üzere 'veya aile hekimliği uzmanlık eğitimi veren kurumlarla sözleşme yapmaya' ibaresi eklenmiş, üçüncü fıkrasının ikinci cümlesi aşağıdaki şekilde değiştirilmiş, yedinci fıkrasında yer alan 'karşılınmayan gider unsurları' ibaresinden sonra gelmek üzere ', belirlenen standartlar çerçevesinde sağlığın geliştirilmesi, hastalıkların önlenmesi, takibi ve kontrolündeki başarı oranı' ibaresi eklenmiştir.

'Bu personelin, sözleşmeli statüde geçen süreleri kazanılmış hak derece ve kademelerinde veya kıdemlerinde değerlendirilerek her yıl işlem yapılır ve bunlar talepleri halinde eski görevlerine atanırlar.'

c) 5 inci maddesinin ikinci fıkrasının dördüncü cümlesinden sonra gelmek üzere aşağıdaki cümle eklenmiştir.

'Aile hekimliği hizmetleri dışında kalan birinci basamak sağlık hizmetleri toplum sağlığı merkezleri tarafından verilir ve bu merkezlerin organizasyonu, kadroları, görevleri ile çalışma usûl ve esasları Türkiye Halk Sağlığı Kurumunca belirlenir.'

(11) 24/4/1930 tarihli ve 1593 sayılı Umumi Hıfzıssıhha Kanununun;

a) 126 ncı maddesi aşağıdaki şekilde değiştirilmiştir.

'Madde 126- Gıda üretim ve satış yerleri ve toplu tüketim yerleri ile insan bedenine temasın söz konusu olduğu temizlik hizmetlerine yönelik sanatların ifa edildiği iş yeri sahipleri ve bu iş yerlerinin işletenleri, çalışanlarına, hijyen konusunda bu iş yerlerindeki meslek ve faaliyetin gerektirdiği eğitimi vermeye veya çalışanların bu eğitimi almalarını sağlamaya, belirtilen eğitimleri almış kişileri çalıştırmaya, çalışan kişiler ise bu eğitimleri almaya mecburdurlar. Bizzat çalışmaları durumunda, iş yeri sahipleri ve işletenleri de bu fıkra kapsamındadır.

Bulaşıcı bir hastalığı olduğu belgelenenler ile iş yerinin faaliyet ve hizmetlerinden doğrudan yararlananları rahatsız edecek nitelikte ve görünür şekilde açık yara veya cilt hastalığı bulunanlar, bizzat çalışan iş yeri sahipleri ve işletenleri de dâhil olmak üzere, alınacak bir raporla hastalıklarının iyileştiği belgeleninceye kadar, birinci fıkrada belirtilen iş yerlerinde çalışamaz ve çalıştırılmazlar. Çalışanlar, hastalıkları konusunda işverene bilgi vermekle yükümlüdür.'

b) 127 nci maddesi aşağıdaki şekilde düzenlenmiş ve Kanuna aşağıdaki geçici madde eklenmiştir.

'Madde 127- 126 ncı maddede belirtilen iş yerlerindeki hijyen eğitimine yönelik hususlara, bu iş yerlerinde çalışmaya engel bulaşıcı hastalıkların ve cilt hastalıklarının neler olduğuna, iyileşme hâlinin belirlenmesine, hangi meslek ve sanat erbabının 126 ncı madde kapsamında olduğuna ilişkin usûl ve esaslar, Sağlık, İçişleri ve Gıda, Tarım ve Hayvancılık Bakanlıklarınca müştereken çıkarılacak yönetmelikle düzenlenir.

126 ncı maddede belirtilen iş yerlerinde bulaşıcı bir hastalık veya bir salgın hastalık çıkması durumunda, bu hastalıkla alakalı gerekli incelemeler, analiz masrafları iş yeri sahipleri ve işletenlerince karşılanmak üzere ilgili kurumlar tarafından yapılır.

126 ncı maddede belirtilen iş yerlerinde bulaşıcı bir hastalık veya bir salgın hastalık çıkması hâlinde doğacak hukukî sorumluluklar ile bu durumdan zarar gören kişi veya kurumların hukukî yol vasıtasıyla talep edebilecekleri tazminat ödemeleri veya olabilecek diğer ödemeler iş yeri sahiplerine ve işletenlerine aittir.'

'GEÇİCİ MADDE 1- 127 nci maddede belirtilen yönetmelik, bu maddenin yayımı tarihinden itibaren altı ay içinde yürürlüğe konulur ve anılan yönetmelik yürürlüğe girinceye kadar ilgili mevzuat hükümlerinin uygulanmasına devam edilir.'

(12) 7/6/1985 tarihli ve 3224 sayılı Türk Diş Hekimleri Birliği Kanununun;

a) 11 inci maddesinin birinci fıkrasının (f) bendi aşağıdaki şekilde değiştirilmiştir.

'f) Faaliyet alanı içerisindeki muayene ve tedavi ücretlerine ilişkin rehber tarife teklifi hazırlayarak Birlik Merkez Yönetim Kuruluna göndermek,'

b) 26 ncı maddesinin birinci fıkrasının (e) bendi aşağıdaki şekilde değiştirilmiştir.

'e) Odaların faaliyet alanı içerisindeki muayene ve tedavi ücretlerine ilişkin rehber tarife tekliflerini tasdik etmek,'

c) 40 ıncı maddesi başlığıyla birlikte aşağıdaki şekilde değiştirilmiştir.

'Rehber tarife belirlenmesi

Madde 40- Oda Yönetim Kurulları her yıl aralık ayı içinde, diş hekimlerinin uygulayacakları muayene ve tedavi ücretlerine ilişkin bir rehber tarife hazırlayarak Birlik Merkez Yönetim Kuruluna gönderirler.

Birlik Merkez Yönetim Kurulu, rehber tarife tekliflerini aynen veya gerekli gördüğü değişiklikleri yaparak tasdik eder ve bu tarifeleri Sağlık Bakanlığına bildirir.'

(13) 4/1/1961 tarihli ve 209 sayılı Sağlık Bakanlığına Bağlı Sağlık Kurumları ile Esenlendirme (Rehabilitasyon) Tesislerine Verilecek Döner Sermaye Hakkında Kanunun;

a) 1 inci maddesi aşağıdaki şekilde değiştirilmiştir.

'Madde 1- Bakanlık ve bağlı kuruluşların (Türkiye Hudut ve Sahiller Sağlık Genel Müdürlüğü ile Türkiye İlaç ve Tıbbî Cihaz Kurumu hariç) merkez ve taşra teşkilatında döner sermaye işletmesi kurulabilir. Bakanlık merkez ve taşra teşkilatı için tahsis edilen döner sermaye miktarı bir milyar; Türkiye Halk Sağlığı Kurumu merkez ve taşra teşkilatı için bir milyar; Türkiye Kamu Hastaneleri Kurumu merkez ve taşra teşkilatı için sekiz milyar Türk Lirasıdır. Bu miktar her bütçe yılı içinde

Bakanlar Kurulunca ihtiyaca göre artırılabilir. İl Sağlık Müdürlüğü ile Türkiye Halk Sağlığı Kurumunun taşra teşkilatı için müşterek döner sermaye işletmeleri kurulabilir. Müşterek döner sermaye işletmelerinin kurulması ve işletilmesine dair usûl ve esaslar Bakanlıkça belirlenir.'

b) 3 üncü maddesinin birinci fıkrasının (d) ve (i) bentleri aşağıdaki şekilde değiştirilmiş, anılan fıkra ile üçüncü fıkrasının sonuna aşağıdaki bentler eklenmiş ve dördüncü fıkrası aşağıdaki şekilde değiştirilmiştir.

'd) Yabancı hastalara verilen sağlık hizmetlerini,'

'i) Gecikme zamları ve faiz gelirleri,'

'j) Diğer gelirler,'

'i)Yurt içi, yurt dışı eğitim giderleri,

j) Araştırma-geliştirme, danışmanlık ve bilirkişilik giderleri,

k) Bakanlık Merkez Döner Sermaye hesabına aktarılan tutarlar,

l) Diğer giderler,'

'Bu Kanuna tâbi döner sermayeli işletmeler, gerekli gördükleri hallerde ihtiyaç duydukları mal ve hizmetleri belirleyecekleri fiyat üzerinden, birbirlerinden temin edebilirler.'

c) 4 üncü maddesi aşağıdaki şekilde değiştirilmiştir.

'Madde 4- Bakanlık ve bağlı kuruluşların merkezinde, muhasebe iş ve işlemleri yürütmek ve mali yılın sonundan itibaren 4 ay içerisinde işletmelerin umumi bilançolarını konsolide ederek Sayıştaya ve Maliye Bakanlığına göndermek üzere merkez döner sermaye saymanlıkları kurulur.'

ç) 5 inci maddesi aşağıdaki şekilde değiştirilmiştir.

'Madde 5- Personelin katkısıyla elde edilen döner sermaye gelirlerinden, döner sermayeli sağlık kurum ve kuruluşlarında görev yapan memurlar ve sözleşmeli personel ile açıktan vekil olarak atanarlara mesai içi veya mesai dışı ayrımı yapılmaksızın ek ödeme yapılabilir. Sağlık kurum ve kuruluşlarında Bakanlıkça belirlenen hizmet sunum şartları ve kriterleri de dikkate alınmak suretiyle, bu ödemenin oranı ile esas ve usûlleri; personelin unvanı, görevi, çalışma şartları ve süresi, hizmete katkısı, performansı, tetkik, eğitim-öğretim ve araştırma faaliyetleri ile muayene, ameliyat, anestezi, girişimsel işlemler ve özellik arz eden riskli bölümlerde çalışma gibi unsurlar esas alınarak Maliye Bakanlığının uygun görüşü üzerine Sağlık Bakanlığınca çıkarılacak yönetmelikle belirlenir.'

Bakanlık merkez teşkilatı ile Türkiye Halk Sağlığı Kurumu (laboratuvarlar hariç) ve Türkiye Kamu Hastaneleri Kurumunun merkez teşkilatında görev yapanlar dışındaki personele, ilgili personelin katkısıyla elde edilen döner sermaye gelirlerinden bir ayda yapılacak ek ödemenin tutarı, ilgili personelin bir ayda alacağı aylık (ek gösterge dâhil), yan ödeme ve her türlü tazminat (makam, temsil ve görev tazminatı ile yabancı dil tazminatı hariç) toplamının; eğitim görevlisi ile uzman tabip kadrosuna atanan profesör ve doçentlerde yüzde 800'ünü, uzman tabip ve tıpta uzmanlık mevzuatında belirtilen dallarda bu mevzuat hükümlerine göre uzman olanlar ile uzman dış tabiplerinde yüzde 700'ünü, pratisyen tabip ve dış tabiplerinde yüzde 500'ünü, idarî sağlık müdür yardımcısı, hastane müdürü ve eczacılarda yüzde 250'sini, başhemşirelerde yüzde 200'ünü, diğer personelde ise yüzde 150'sini geçemez. İşin ve hizmetin özelliği dikkate alınarak yoğun bakım, doğumhane, yeni doğan, süt çocuğu, yanık, diyaliz, ameliyathane, enfeksiyon, özel bakım gerektiren ruh sağlığı, organ ve doku nakli, acil servis ve benzeri sağlık hizmetlerinde çalışan personel için yüzde 150 oranı, yüzde 200 olarak uygulanır. Nöbet hizmetleri hariç olmak üzere mesai saatleri dışında gelir getirici çalışmalarından doğan katkılarına karşılık olarak tabip, dış tabibi ve tıpta uzmanlık mevzuatına göre uzman olanlara bu fıkradaki oranların yüzde 30'unu, diğer personele yüzde 20'sini geçmeyecek şekilde ayrıca ek ödeme yapılır. Sözleşmeli olarak istihdam edilen personele yapılacak ek ödemenin tutarı ise, aynı birimde aynı unvanlı kadroda çalışan ve hizmet yılı aynı olan emsali personel esas alınarak belirlenir ve bunlara yapılacak ek ödeme hiçbir şekilde emsaline yapılabilecek ek ödeme üst sınırını geçemez. Bu fıkra uyarınca personele her ay yapılacak ek ödeme tutarı, 375 sayılı Kanun Hükmünde Kararnamenin ek 3 üncü maddesi uyarınca kadro ve görev unvanı veya pozisyon unvanı itibarıyla belirlenmiş olan ek ödeme tutarından az olamaz. Bu kapsamdaki personel için 375 sayılı Kanun Hükmünde Kararnamenin ek 3 üncü maddesinin üçüncü fıkrası hükmü uygulanmaz.

Bakanlık taşra teşkilatı ile Türkiye Halk Sağlığı Kurumu taşra teşkilatı, döner sermaye gelirleri ile nakit kaynaklarını personele ek ödeme dağıtımında kullanabilir. İkinci ve üçüncü basamak sağlık kurumlarında ise personelin katkısı ile elde edilen döner sermaye gelirlerinden, o birimde görevli personele yapılacak ek ödeme toplamı, ilgili birimin carî yıldaki döner sermaye gelirinin yüzde 50'sini aşamaz.

Bakanlık ve bağlı kuruluşların merkez ve taşra teşkilatında kurulan döner sermaye işletmeleri, sağlık hizmetlerinin iyileştirilmesi, kaliteli ve verimli hizmet sunumunun teşvik edilmesi, sağlık kurum ve kuruluşlarının kendi imkânlarıyla karşılayamadıkları ihtiyaçların giderilmesi, eğitim, araştırma ve geliştirme faaliyetlerinin desteklenmesi, Bakanlık taşra teşkilatı ile Türkiye Halk Sağlığı Kurumu

taşra teşkilatının desteklenmesi, Bakanlık merkez ve taşra teşkilatında ve Türkiye Halk Sağlığı Kurumu merkez ve taşra teşkilatı ile Türkiye Kamu Hastaneleri Kurumunun merkez teşkilatında görev yapan memurlar ile sözleşmeli personele ek ödemede bulunulması amacıyla yapılacak giderlere iştirak etmek için aylık gayrisafi hasıllardan aylık tahsil edilen tutarın yüzde 6'sını geçmemek üzere Bakanlıkça belirlenecek oranı Bakanlık Döner Sermaye Merkez Saymanlığı hesabına aktarırlar. Bu hesaplarda toplanacak tutarların dağılım ve harcanmasına ilişkin kriterler ile altıncı fıkra uyarınca personele yapılacak ek ödemenin oran, esas ve usûlleri Maliye Bakanlığının uygun görüşü üzerine Sağlık Bakanlığınca belirlenir.

Bakanlık merkez teşkilatı ile Türkiye Halk Sağlığı Kurumu ve Türkiye Kamu Hastaneleri Kurumunun merkez teşkilatında görev yapan personele yapılacak ek ödemenin tutarı en yüksek devlet memuru aylığının (ek gösterge dâhil) % 200'ünü geçemez. Ek ödeme tutarı, görev yapılan birim ve iş hacmi, görevin önem ve güçlüğü, çalışma süresi, personelin sınıfı, kadro unvanı, derecesi ve atanma biçimi gibi kriterler ile personele aylık ve özlük hakları dışında ilgili mevzuatına göre yapılan diğer ilave ödemeler dikkate alınarak belirlenir. Merkez teşkilatında görev yapan personele bu fıkra kapsamında yapılacak toplam ek ödeme, döner sermaye işletmelerinden cari yılda aktarılan tutarın yüzde ellisini geçemez ve bu ödemeler gelir vergisine tabi tutulmaz. Türkiye Halk Sağlığı Kurumu merkez ve taşra teşkilatı ile Türkiye Kamu Hastaneleri Kurumunun merkez teşkilatında görev yapan personele bu madde uyarınca yapılacak ek ödeme amacıyla Bakanlık tarafından kaynak aktarılabilir. Türkiye İlaç ve Tıbbî Cihaz Kurumu personeline bu fıkroda belirtilen usûl ve esaslara göre Kurum bütçesinden ek ödeme yapılır.

4/11/1981 tarihli ve 2547 sayılı Yükseköğretim Kanununun 38 inci maddesine göre Sağlık Bakanlığı merkez teşkilatı ve bağlı sağlık kurum ve kuruluşlarında görevlendirilenler, aynı maddede belirtilen ilave ödemelerden yararlanmamak kaydıyla, Bakanlık merkez veya bağlı sağlık kurum ve kuruluşlarında görev yaptıkları unvan için belirlenen ek ödemeden faydalandırılır. Sağlık kurum ve kuruluşlarında ihtiyaç duyulması halinde, ilgilinin isteği ve kurumlarının muvafakatiyle diğer kamu kurum ve kuruluşlarında görevli sağlık personeli haftanın belirli gün veya saatlerinde veyahut belirli vakalar ve işler için görevlendirilebilirler. Yıl veya ay itibarıyla belirli bir süre için görevlendirme halinde bu kişilere, sadece görevlendirildikleri sağlık kuruluşundaki döner sermaye işletmesinden ödeme yapılır. Belirli bir vaka ve iş için görevlendirilenlere ise, kadrosunun bulunduğu kurumdaki döner sermaye işletmesinden yapılan ödemenin yanı sıra, katkı sağladıkları vaka ve iş dolayısıyla görevlendirildiği sağlık kuruluşundaki döner sermaye işletmesinden, birinci ve ikinci fıkra esasları

çerçevesinde ve toplamda tavan oranları geçmemek üzere döner sermayeden ek ödeme yapılır. Bu görevlendirmeye ilişkin usûl ve esaslar Sağlık Bakanlığınca belirlenir.

Döner sermayeli işletmelerin malî imkânı elverişli olanlarından, malî durumu yetersiz olanlara karşılıksız veya borç olarak kaynak aktarmaya Sağlık Bakanı yetkilidir.

Bakanlık ve bağlı kuruluşları ile kamu kurum ve kuruluşları haricindeki kuruluş veya kişilerce, sağlık hizmetleri dışında, kurum içinde veya hizmetin gerektirdiği yerde, kurumdan istenecek bilimsel görüş, proje, araştırma ve benzeri hizmetler Kurumca kabul edilecek esaslara bağlı olmak üzere yapılabilir. Bu hususta alınacak ücretler döner sermayeye gelir kaydedilir. Bu şekilde elde edilen gelirin safi tutarının % 65'ine kadar tutar Bakanlıkça belirlenecek esaslar çerçevesinde projeyi yürüten personele ödenir. Bu ödemenin yapılmasında ikinci fıkrada öngörülen tavan sınırlamaları dikkate alınmaz.'

d) Ek 3 üncü maddesi aşağıdaki şekilde değiştirilmiştir.

'Bakanlık ve bağlı kuruluşlarının kadro ve pozisyonlarına (döner sermaye dâhil) atanan ve 5 inci madde (altıncı fıkrası hariç) gereğince döner sermaye gelirlerinden ek ödeme alan eğitim görevlilerine en yüksek Devlet memuru aylığının (ek gösterge dâhil) % 410'u, uzman tabip, tıpta uzmanlık mevzuatına göre uzman olanlar ile uzman dış tabiplerine % 335'i ve pratisyen tabip ve dış tabiplerine ise % 180'i oranında, her ay herhangi bir katkıya bağlı olmaksızın döner sermaye gelirlerinden ek ödeme yapılır. Kamu hastane birliklerinde ve hastanelerin sözleşmeli pozisyonlarında istihdam edilen tabipler için de bu hüküm uygulanır. Bu ödemeye hak kazanılmasında ve ödenmesinde aylıklara ilişkin hükümler uygulanır.

Bu madde kapsamında yapılan aylık ek ödeme tutarı, 5 inci madde ile Sağlık Bakanlığı ve Bağlı Kuruluşların Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 33 üncü maddesi uyarınca aynı aya ilişkin olarak yapılacak ek ödeme tutarından mahsup edilir. Bu maddeye göre yapılan ek ödemenin 5 inci madde ile Sağlık Bakanlığı ve Bağlı Kuruluşların Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 33 üncü maddesi uyarınca aynı aya ilişkin olarak yapılacak ek ödemeden fazla olması halinde aradaki fark geri alınmaz. Bu madde kapsamında ödeme yapılanlara 375 sayılı Kanun Hükmünde Kararnamenin ek 3 üncü maddesi hükümlerine göre ek ödeme yapılmaz. '

(14) Bu maddenin yayımı tarihinde;

a) 13/12/1983 tarihli ve 181 sayılı Sağlık Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname,

b) 30/12/1940 tarihli ve 3959 sayılı Türkiye Cumhuriyeti Merkez Hıfzıssıhha Müessesesi Teşkiline Dair Kanun,

c) 3/3/1926 tarihli ve 767 sayılı Türk Kodeksi Hakkında Kanun,

ç) 9/7/1943 tarihli ve 4459 sayılı Köy Ebeleri ve Köy Sağlık Memurları Teşkilatı Yapılmasına ve 3017 Numaralı Sıhhat ve İctimai Muavenet Vekaleti Teşkilat ve Memurin Kanununun Bazı Maddelerinin Değiştirilmesine Dair Kanun,

d) 24/4/1530 tarihli ve 1593 sayılı Umumi Hıfzıssıhha Kanununun 10 ilâ 15 inci maddeleri, 17 nci maddesi ve 180 inci maddesi,

e) 7/5/1987 tarihli ve 3359 sayılı Sağlık Hizmetleri Temel Kanununun 5 inci, 6 ncı, 7 nci ve 8 inci maddeleri ile 9 uncu maddesinin (a) bendi,

f) 11/4/1928 tarihli ve 1219 sayılı Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanunun 9 uncu maddesi,

g) 4/1/1961 tarihli ve 209 sayılı Sağlık Bakanlığına Bağlı Sağlık Kurumları ile Esenlendirme (Rehabilitasyon) Tesislerine Verilecek Döner Sermaye Hakkında Kanunun 7 nci, 8 inci, 9 uncu ve 11 inci maddeleri ile 12 nci maddesinin ikinci fıkrası ile ek 4 üncü maddesi,

ğ) 23/1/1953 tarihli ve 6023 sayılı Türk Tabipleri Birliği Kanununun 1 inci maddesinde geçen 'tabipliğin kamu ve kişi yararına uygulanıp geliştirilmesini sağlamak' ibaresi,

yürürlükten kaldırılmıştır.

(15) Mevzuatta, bu Kanun Hükmünde Kararname ile yürürlükten kaldırılan kanun, kanun hükmünde kararname veya maddelerine yapılan atıflar, bu Kanun Hükmünde Kararnameye veya ilgili hükümlerine; Sağlık Bakanlığı, Refik Saydam Hıfzıssıhha Merkezi Başkanlığı ve Hudut ve Sahiller Sağlık Genel Müdürlüğüne yapılan atıflar, bu Kanun Hükmünde Kararname ile yeniden yapılandırılan Sağlık Bakanlığı veya görev ve faaliyet alanlarına göre ilgili bağlı kuruluşlarına yapılmış sayılır.

GEÇİCİ MADDE 1- (1) Bakanlık ve bağlı kuruluşlar teşkilat ve kadrolarını bu maddenin yayımı tarihinden itibaren en geç 1 yıl içinde bu Kanun Hükmünde Kararname hükümlerine uygun hale getirir. Kadrolar bu Kanun Hükmünde Kararnameye uygun hale getirilinceye kadar, Bakanlık ve bağlı kuruluşlara verilen görevler daha önce bu görevleri yapmakta olan birimler ve personel tarafından; harcama ve ödemeler de ilgili bütçesinden yapılmaya devam edilir.

GEÇİCİ MADDE 2- (1) Bu Kanun Hükmünde Kararnamede belirtilen düzenleyici işlemler bu maddenin yayımı tarihinden itibaren en geç 1 yıl içinde yürürlüğe konulur. Anılan düzenlemeler yürürlüğe konuluncaya kadar, mevcut düzenlemelerin bu Kanun Hükmünde Kararnameye aykırı olmayan hükümlerinin uygulanmasına devam edilir.

GEÇİCİ MADDE 3- (1) Bu Kanun Hükmünde Kararname ile yeniden yapılandırılan Bakanlık, kaldırılan Refik Saydam Hıfzıssıhha Merkezi Başkanlığı ve Hudut ve Sahiller Sağlık Genel Müdürlüğünün üçüncü kişilerle yapmış olduğu veya taraf olduğu her türlü taahhüt, sözleşme, hak, alacak ve borçları ile dava ve icra tâkipleri, teşkilatlarını bu Kanun Hükmünde Kararname hükümlerine uygun hale getirdikten sonra Bakanlık ve ilgisine göre bağlı kuruluşlara devredilmiş sayılır.

(2) Maliye Bakanlığı uhdesinde Hazine Avukatları tarafından Bakanlık ve Refik Saydam Hıfzıssıhha Merkezi Başkanlığının görevlerine ilişkin takip edilen dosyalar Maliye Bakanlığı ve Bakanlıkça müştereken belirlenecek esaslara göre bu maddenin yayımı tarihinden itibaren bir yıl içinde Bakanlığa ve ilgisine göre bağlı kuruluşlara devredilir. Bu şekilde devredilen dava ve icra takipleri ile ilgili olarak devir tarihine kadar yapılmış her türlü işlem Bakanlık adına yapılmış sayılır.

GEÇİCİ MADDE 4- (1) Bu maddenin yayımı tarihinde görevde bulunan, Sağlık Bakanlığı, Hudut ve Sahiller Sağlık Genel Müdürlüğü ve Refik Saydam Hıfzıssıhha Merkezi Başkanlığının merkez, taşra ve döner sermaye kadrolarına atanmış olan ve kadroları iptal edilen personelden; Teftiş Kurulu Başkanı, Genel Müdür, Genel Müdür Yardımcısı, Müstakil Daire Başkanı, Bakanlık Müşaviri, Daire Başkanı, Özel Kalem Müdürü, Basın ve Halkla İlişkiler Müşaviri, Başkan Yardımcısı, Döner Sermaye Merkez Müdürü, İl Sağlık Müdürü, İl Sağlık Müdür Yardımcısı, Şube Müdürü ile Müdür ve Müdür Yardımcısı unvanlı kadrolarda bulunanların görevleri, bu maddenin yayımı tarihinde sona erer. Bu fıkra uyarınca görevleri sona erenlerden Teftiş Kurulu Başkanı, Genel Müdür, Genel Müdür Yardımcısı, Müstakil Daire Başkanı, Bakanlık Müşaviri, Daire Başkanı, Özel Kalem Müdürü, Basın ve Halkla İlişkiler Müşaviri, Başkan Yardımcısı ve İl Sağlık Müdürü kadrolarında bulunanlar ekli (2) sayılı liste ile ihdas edilen Bakanlık Müşaviri kadrolarına; diğerlerinden merkez teşkilatında bulunanlar ekli (2) sayılı liste ile ihdas edilen Araştırmacı, taşra teşkilatında bulunanlar ekli (3) sayılı liste ile ihdas edilen Araştırmacı kadrolarına halen buldukları kadro dereceleriyle atanmış sayılır. Bu madde uyarınca ihdas edilen Bakanlık Müşaviri ile Araştırmacı kadroları herhangi bir sebeple boşalması halinde hiçbir işleme gerek kalmaksızın iptal edilmiş sayılır. Bu fıkraya göre Bakanlık Müşaviri ve Araştırmacı kadrolarına atanmış sayılanlar, Bakanın uygun göreceği merkez veya taşra teşkilatına ait birimlerde çalıştırılabilir.

(2) Birinci fıkrada sayılanlar dışında kalanlardan Bakan Yardımcısı, Müsteşar, Müsteşar Yardımcısı, Strateji Geliştirme Başkanı ve I. Hukuk Müşaviri Bakanlıktaki aynı unvanlı kadrolara, kadro unvanı değişmeyen diğer personel Bakanlık ve bağlı kuruluşlardaki aynı unvanlı kadrolara atanmış sayılır. Diğer personel bu maddenin yayımı tarihini izleyen bir yıl içinde, öğrenim durumları, hizmet sınıfları ve halen buldukları teşkilatlar itibarıyla Bakanlık veya bağlı kuruluşlarının merkez, taşra ve döner sermaye teşkilatı kadrolarına, kazanılmış hak aylık derecelerine uygun kadrolara atanır. Bunlar atama yapıluncaya kadar mevcut kadrolarına ait aylık, ek gösterge, her türlü zam ve tazminatları ile diğer malî haklarını almaya devam eder ve bu süre içerisinde durumlarına uygun işlerde görevlendirilir. Bu fıkra kapsamındaki işlemler Bakanlık tarafından oluşturulacak komisyon tarafından sonuçlandırılır.

(3) Bu maddenin yayımı tarihinde başmüfettiş, müfettiş ve müfettiş yardımcısı kadrolarında bulunanlar, durumlarına göre buldukları kadro dereceleriyle Bakanlık ve bağlı kuruluşlarının sağlık başdenetçisi, sağlık denetçisi ve sağlık denetçi yardımcısı kadrolarına atanırlar. Bunların başmüfettiş, müfettiş ve müfettiş yardımcısı kadrolarında geçirdikleri süreler sağlık başdenetçisi, sağlık denetçisi ve sağlık denetçi yardımcısı kadrolarında geçmiş sayılır.

(4) Birinci fıkra uyarınca atanan veya atanmış sayılan personelin yeni kadrolarına atandıkları veya atanmış sayıldıkları tarih itibarıyla eski kadrolarına ilişkin olarak en son ayda sözleşme ücreti, aylık, ek gösterge, ikramiye (bir aya isabet eden net tutarı), her türlü zam ve tazminatları, makam tazminatı, temsil tazminatı, görev tazminatı, ek ücret, ek ödeme ve benzeri adlarla yapılan her türlü ödemelerin (ilgili mevzuatı uyarınca fiili çalışmaya bağlı fazla mesai ücreti ve performansla bağlı döner sermaye ek ödemesi hariç) toplam net tutarının (Bu tutar sabit bir değer olarak esas alınır.); yeni atandıkları veya atanmış sayıldıkları kadrolara ait aylık, ek gösterge, ikramiye (bir aya isabet eden net tutarı), her türlü zam ve tazminatları, makam tazminatı, temsil tazminatı, görev tazminatı, ek ücret, ek ödeme ve benzeri adlarla yapılan her türlü ödemelerin (ilgili mevzuatı uyarınca fiili çalışmaya bağlı fazla mesai ücreti ve performansla bağlı döner sermaye ek ödemesi hariç) toplam net tutarından fazla olması halinde aradaki fark tutarı, herhangi bir vergi ve kesintiye tâbi tutulmaksızın fark kapanuncaya kadar ayrıca tazminat olarak ödenir. Atandıkları veya atanmış sayıldıkları kadro unvanlarında isteğe bağlı olarak herhangi bir değişiklik olanlarla, kendi istekleriyle başka kurumlara atanana fark tazminatı ödenmesine son verilir.

(5) Bu maddenin yayımı tarihinde Sağlık Bakanlığı, Hudut ve Sahiller Sağlık Genel Müdürlüğü ve Refik Saydam Hıfzıssıhha Merkezi Başkanlığında 4924 sayılı Kanun, 657 sayılı Kanunun 4 üncü maddesinin (B) ve (C) fıkraları uyarınca vizeli pozisyonlarda çalıştırılan sözleşmeli ve geçici personel

ile sürekli ve geçici işçiler, çalıştığı birim ve teşkilatı esas alınarak mevcut pozisyon ve kadrolarıyla Bakanlık ve bağlı kuruluşlara başkaca bir işleme gerek kalmaksızın devredilmiş sayılır. Anılan idarelere ait boş kadro ve pozisyonlar, bu Kanun Hükmünde Kararnamenin yürürlüğe girdiği tarihte başkaca bir işleme gerek kalmaksızın, buldukları teşkilatlar esas alınarak Bakanlık ve bağlı kuruluşlarına devredilmiş sayılır. Bu fıkra kapsamındaki işlemler Bakanlık tarafından oluşturulacak komisyon tarafından bu maddenin yayımı tarihinden itibaren altı ay içinde sonuçlandırılır.

(6) Bu Kanun Hükmünde Kararname ile kadroları kaldırılan ve (2) ve (3) sayılı listedeki kadrolara atanan personel dâhil, kadrolarının iptali sebebiyle yeni kadrolara atanacaklar, kadro standartları uygun olmak ve altı ay içinde müracaatta bulunmak kaydıyla, bir defaya mahsus olmak üzere, mevzuattaki atama ve nakillerle ilgili kısıtlamalara bağlı olmaksızın istedikleri il ve ya ilçelerdeki birimlerin durumlarına uygun kadrolarına atama ve nakilleri gerçekleştirilir.

(7) Bu maddenin yayımı tarihinden itibaren bir yıl süreyle 190 sayılı Kanun Hükmünde Kararnamenin 9 uncu maddesinin son fıkrasında yer alan sınırlama ile bağlı olmaksızın boş kadrolarda sınıf, unvan ve derece, dolu kadrolarda derece değişikliği yapmaya Bakanlar Kurulu yetkilidir.

GEÇİCİ MADDE 5- (1) Bu maddenin yayımı tarihinden itibaren bir yıl içinde Bakanın onayıyla Kamu Hastane Birlikleri oluşturulur. Birlik teşkiline ilişkin onayın alındığı tarihte ilgili birlik kapsamındaki sağlık kurumlarında bulunan baştabip, baştabip yardımcısı, hastane müdürü, hastane müdür yardımcısı ve başhemşire kadrolarında bulunanların bu görevleri sona erer. Görevleri sona eren personelden hastane müdür ve müdür yardımcıları ekli (3) sayılı listede ihdas edilen Kurumun taşra teşkilatı kadrolarına hâlen buldukları kadro dereceleriyle hiçbir işleme gerek kalmaksızın atanmış sayılır. Bunlar durumlarına göre Bakanlıkta ve bağlı kuruluşlarında uygun görülen işlerde çalıştırılır. Bu şekilde atananların kadroları, herhangi bir sebeple boşaldığında hiçbir işleme gerek kalmaksızın iptal edilmiş sayılır. Baştabip, baştabip yardımcısı ve başhemşire kadrolarında bulunanlar meslekleri ile ilgili hizmet sınıflarındaki durumlarına uygun kadrolara atanırlar. Bu Kanun Hükmünde Kararname uyarınca birlik kapsamına alınan sağlık kurumlarında baştabip, baştabip yardımcısı, hastane müdürü, hastane müdür yardımcısı ve başhemşire görevlerini ikinci görev, vekâlet veya görevlendirme suretiyle yürüten personelin bu görevleri kendiliğinden sona erer.

(2) Birinci fıkra uyarınca ekli (3) sayılı listede ihdas edilen kadrolara atananların bu kadrolara atandıkları veya atanmış sayıldıkları tarih itibarıyla eski kadrolarına ilişkin olarak en son ayda sözleşme ücreti, aylık, ek gösterge, ikramiye (bir aya isabet eden net tutarı), her türlü zam ve tazminatları, makam tazminatı, temsil tazminatı, görev tazminatı, ek ücret, ek ödeme ve benzeri

adlarla yapılan her türlü ödemelerin (ilgili mevzuatı uyarınca fiili çalışmaya bağlı fazla mesai ücreti ve performansa bağlı döner sermaye ek ödemesi hariç) toplam net tutarının (Bu tutar sabit bir değer olarak esas alınır.); yeni atandıkları veya atanmış sayıldıkları kadrolara ilişkin aylık, ek gösterge, ikramiye (bir aya isabet eden net tutarı), her türlü zam ve tazminatları, makam tazminatı, temsil tazminatı, görev tazminatı, ek ücret, ek ödeme ve benzeri adlarla yapılan her türlü ödemelerin (ilgili mevzuatı uyarınca fiili çalışmaya bağlı fazla mesai ücreti ve performansa bağlı döner sermaye ek ödemesi hariç) toplam net tutarından fazla olması halinde aradaki fark tutarı, herhangi bir vergi ve kesintiye tâbi tutulmaksızın fark kapanıncaya kadar ayrıca tazminat olarak ödenir. Atandıkları veya atanmış sayıldıkları kadro unvanlarında isteğe bağlı olarak herhangi bir değişiklik olanlarla, kendi istekleriyle başka kurumlara atanana fark tazminatı ödenmesine son verilir.

GEÇİCİ MADDE 6- (1) Bu maddenin yayımı tarihinde görevde bulunan klinik şefi ve klinik şef yardımcılarının görevleri bu maddenin yayımı tarihinde sona erer. Bunlar eğitim görevlisi kadrolarına kazanılmış hak aylık dereceleriyle atanmış sayılır.

GEÇİCİ MADDE 7- (1) Bağlı kuruluşlara devredilen sağlık kuruluşlarında muhasebe hizmetlerini yürüten ve Maliye Bakanlığı kadrolarında bulunan personelden ihtiyaç duyulanlar, kurumların talebi ve Maliye Bakanlığının uygun görüşü üzerine, bu maddenin yayımı tarihinden itibaren üç yılı geçmemek üzere görev yapmaya devam eder. Bu şekilde görevlendirilen personele döner sermayeden herhangi bir ödeme yapılmaz.

GEÇİCİ MADDE 8- (1) Bu Kanun Hükmündeki Kararname ile kaldırılan Sağlık Bakanlığının kullanımındaki bütün taşınır ve taşınmazlar Bakanlığa devredilir. Bunlardan ihtiyaç fazlası hâline gelenler Bakanlık tarafından oluşturulacak komisyonlar ve belirlenecek usûl ve esaslar çerçevesinde ihtiyaçlarına göre bağlı kuruluşlara bedelsiz olarak devredilir. Mülkiyeti Hazineye ait veya Devletin hüküm ve tasarrufu altındaki taşınmazlardan Maliye Bakanlığınca, Bakanlığa tahsis edilmiş olan taşınmazlar, tahsis amacıyla kullanılmak üzere Bakanlığa tahsis edilmiş sayılır.

(2) Bu Kanun Hükmündeki Kararname ile kaldırılan Hudut ve Sahiller Sağlık Genel Müdürlüğünün mülkiyetindeki taşınır ve taşınmazlar Türkiye Hudut ve Sahiller Sağlık Genel Müdürlüğüne devredilir. Refik Saydam Hıfzıssıhha Merkezi Başkanlığına ait taşınır ve taşınmazlar Türkiye Halk Sağlığı Kurumuna devredilir. Mülkiyeti Hazineye ait veya Devletin hüküm ve tasarrufu altındaki taşınmazlardan bu Kanun Hükmündeki Kararname ile kaldırılan Hudut ve Sahiller Sağlık Genel Müdürlüğü ve Refik Saydam Hıfzıssıhha Merkezi Başkanlığına tahsis edilmiş olan taşınmazlar ise, ilgisine göre Türkiye Hudut ve Sahiller Sağlık Genel Müdürlüğüne ve Türkiye Halk Sağlığı Kurumuna tahsis edilmiş sayılır.

GEÇİCİ MADDE 9- (1) Bu maddenin yayımı tarihinde Bakanlık ve bağlı kuruluşlarının kullanımında bulunan taşınırlardan HEK'e ayrılanlar edinme şekline bakılmaksızın satışı yapılarak ilgili bütçelerine gelir kaydedilir.

GEÇİCİ MADDE 10- (1) Bu Kanun Hükmünde Kararname gereğince yapılacak personel, taşınır ve taşınmaz mal, taşıt ve sair araç ve gereçlerin devri, nakli, tahsisi ve benzeri iş ve işlemleri yürütmek üzere; Bakanlık merkezinde müsteşar yardımcısı başkanlığında en az beş kişiden oluşan devir komisyonu oluşturulur.

GEÇİCİ MADDE 11- (1) Bu maddenin yayımı tarihinde Sağlık Bakanlığında 657 sayılı Kanununun 86 ncı maddesine göre vekil ebe ve hemşire olarak en az bir yıldan beri çalışmakta olan ve anılan Kanununun 48 inci maddesinde belirtilen genel şartları taşıyanlardan bu maddenin yayımı tarihinden itibaren otuz gün içinde yazılı olarak başvuranlar, çalıştığı pozisyon unvanlarına göre, 657 sayılı Kanununun 4 üncü maddesinin (B) fıkrası kapsamında vizelenecek ebe ve hemşire unvanlı sözleşmeli personel pozisyonlarına geçirilir.

(2) Bu madde hükümlerine göre sözleşmeli personel pozisyonlarına geçirilenlerin vekil olarak çalıştıkları hizmet süreleri, ebe ve hemşire unvanlı sözleşmeli personel pozisyonlarında geçirilmiş sayılır.

GEÇİCİ MADDE 12- (1) 6/4/2011 tarihi itibarıyla dış hekimliği fakültelerinde doktora eğitimine başlamış veya doktora eğitimi kontenjanına yerleşmiş olanlardan isteyenler 56 ncı madde çerçevesinde eğitimlerine devam edebilir.

MADDE 59- (1) Bu Kanun Hükmünde Kararname yayımı tarihinde yürürlüğe girer.

MADDE 60- (1) Bu Kanun Hükmünde Kararname hükümlerini Bakanlar Kurulu yürütür.

-kadro cetvelleri-

B- Dayanılan Anayasa Kuralları

Dava dilekçesi ve başvuru kararlarında, Anayasa'nın Başlangıç'ı ile 2., 5., 6., 7., 8., 9., 10., 11., 13., 17., 18., 20., 23., 36., 38., 47., 48., 49., 50., 55., 56., 63., 70., 87., 91., 112., 123., 124., 125., 126., 128., 130., 131., 135., 138., 153. ve 168. maddelerine dayanılmıştır.

III- İLK İNCELEME

A- Anayasa Mahkemesi İçtüzüğü'nün 8. maddesi gereğince Serruh KALELİ, Alparslan ALTAN, Fulya KANTARCIOĞLU, Mehmet ERTEN, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT, Zehra Ayla PERKTAŞ, Recep KÖMÜRCÜ, Burhan ÜSTÜN, Engin YILDIRIM, Nuri NECİPOĞLU, Hicabi

DURSUN, Celal Mümtaz AKINCI ve Erdal TERCAN'ın katılımlarıyla yapılan ilk inceleme toplantılarında öncelikle Anayasa Mahkemesi Başkanı Haşim KILIÇ hakkındaki reddi hakim talebi görüşülmüştür.

Dava dilekçesinde, Anayasa Mahkemesi Başkanı Haşim KILIÇ'ın, kamuoyunda Wikileaks belgeleri olarak bilinen ve bir internet sitesinde yer alan bilgilere göre, 2003 yılında ABD Büyükelçisine Cumhuriyet Halk Partisi aleyhinde bir takım beyanlarda bulunduğu, 25.4.2011 tarihinde Anayasa Mahkemesinin 49. Kuruluş Yıldönümünde yaptığı açılış konuşmasında 'Ümit ediyorum ki bu gayret, Anayasa Mahkemesine dava açmak suretiyle sorun çözme kolaycılığını da ortadan kaldıracaktır.' ifadelerine yer verdiği, ayrıca 6223 sayılı Yetki Kanunu'nun iptali istemiyle açılan davada verilen kararda açıklanan görüşünün daha önceki kararlarda yer alan görüşlerinden farklı olduğu, bu nedenlerle Cumhuriyet Halk Partisinin tarafı olduğu davalarda tarafsız olarak karar veremeyeceği ileri sürülerek 6216 sayılı Kanun'un 59. maddesinin birinci fıkrasının (d) bendi ile 60. maddesinin (1) numaralı fıkrası uyarınca reddi talep edilmiştir.

Hakimin reddi kurumu, hakimin tarafsız kalamayacağı şüphesi bulunan bir davaya bakmamasını sağlamaya yönelik olup temel bir hak olan adil yargılanma hakkıyla ilişkilidir. Nitekim adil yargılanma hakkı tarafsız bir mahkeme önünde yargılanma hakkını da içerir. Bu nedenle hukukumuzda, hakimin tarafsız kalamayacağı varsayılan veya tarafsızlığından kuşku duyulabilecek durumlarda ya davaya bakması yasaklanmış ya da taraflarca reddedilebileceği kabul edilmiştir.

6216 sayılı Kanun'un 59. maddesinin (1) numaralı fıkrasının (d) bendinde, Anayasa Mahkemesi Başkanı ve üyelerinin, istişarî görüş ve düşüncelerini ifade etmiş olduğu dava ve işlere bakamayacakları; 60. maddesinin (1) numaralı fıkrasında, Anayasa Mahkemesi Başkanı ve üyelerinin tarafsız hareket edemeyecekleri kanısını haklı kılan hallerin olduğu iddiası ile reddolunabileceği; (2) numaralı fıkrasında, bu takdirde, Genel Kurul ya da bölümlerde ilgili üye katılmaksızın ret konusu hakkında kesin karar verileceği; (5) numaralı fıkrasında ise ret talebinin kötü niyetle yapıldığının anlaşılması ve esas yönünden kabul edilmemesi hâlinde, talepte bulunanların her birine Mahkemece beşyüz Türk Lirasından beşbin Türk Lirasına kadar disiplin para cezası verileceği kurala bağlanmıştır.

Dava dilekçesinde hakimin reddi talebi yönünden dayanılan hususlardan biri Wikileaks belgeleri olarak bilinen belgelerde yer aldığı ileri sürülen bilgilerdir. Ancak bu belgelerin gerçekte var olup olmadığı kanıtlanamadığı gibi, içerdiği bilgilerin doğru olup olmadığı da ortaya konulabilmiş değildir. Aksine, belgelerde ismi geçen birçok kişi gibi Anayasa Mahkemesi Başkanı Haşim KILIÇ tarafından da kamuoyunun bilgisine sunuldukları ilk andan itibaren anılan belgelerde var olduğu

ileri sürülen bilgiler açıkça yalanlanmıştır. Ret talebi yönünden dayanılan hususlardan biri olan açılış konuşmasındaki sözler, Türk siyasal yaşamındaki uzlaşma kültürü eksikliğine ve temel siyasal sorunların siyasi arenada çözümü yerine yargı kurumlarına havale edilmesi eğilimine yönelik genel ve kişisel nitelikte bir eleştiri olup somut bir davaya ilişkin herhangi bir görüş veya düşünce içermemektedir. Ret talebine dayanak yapılan hususlardan sonuncusu olan Anayasa Mahkemesi Başkanı Haşim KILIÇ'ın geçmişte kimi dava dosyalarında kullandığı oylar, tamamen hakimin yargısal görevine ilişkindir. Hakimin geçmişte verdiği kararlar ve kullandığı oyların ret sebebi olarak kabul edilemeyeceği açıktır. Dolayısıyla dava dilekçesinde hakimin reddi nedeni olarak ileri sürülen hususlar, Kanun'da düzenlenen davaya bakılması yasak bir hal veya ret sebebi olarak kabul edilemez. Öte yandan, her hak gibi hakimin reddini talep etme hakkının da amacına uygun olarak kullanılması gerekir. Aksi halde hakkın kötüye kullanılması söz konusu olur. Somut dava dosyasında, varlığı ve içerdiği bilgilerin doğruluğu kanıtlanmamış aksine yalanlanmış olan hukuken delil değeri bulunmadığı açık bir takım bilgi ve belgelere, yine ret sebebi olmadığı açık olan hakimin önceki dava dosyalarında kullandığı oylara dayanılarak ret talebinde bulunulmuş olması, hakimin reddini talep etme hakkının iyi niyetle ve amacına uygun olarak kullanılmadığını ortaya koymaktadır. Bu nedenle 6216 sayılı Kanun'un 60. maddesinin (5) numaralı fıkrası gereğince ret talebinde bulunanlara takdiren 500 TL disiplin para cezası uygulanmasına karar verilmesi gerekmiştir.

Açıklanan nedenlerle:

- 1- Hakimin reddi talebinin esastan REDDİNE, OYBİRLİĞİYLE,
- 2- Talebin kötü niyetle yapıldığının KABULÜNE ve 6216 sayılı Kanun'un 60. maddesinin (5) numaralı fıkrası gereğince DİSİPLİN PARA CEZASI UYGULANMASINA, Fulya KANTARCIOĞLU, Mehmet ERTEN, Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŞ'ın karşıoyları ve OYÇOKLUĞUYLA,
- 3- Disiplin para cezasının talepte bulunan davacıya verilmesine, Serruh KALELİ, Burhan ÜSTÜN ile Nuri NECİPOĞLU'nun 'Para cezasının talepte bulunanların her birine verilmesi gerektiği' yolundaki karşıoyları ve OYÇOKLUĞUYLA,
- 4- Para cezası miktarının 500 Türk Lirası olarak esas alınmasına, OYBİRLİĞİYLE,

12.1.2012 gününde karar verilmiştir.

B- Anayasa Mahkemesi İçtüzüğü hükümleri uyarınca, E.2011/150 sayılı dosyanın 12.1.2012 gününde, E.2012/41, E.2012/43, E.2012/44 ve E.2012/53 sayılı dosyaların 17.5.2012 gününde, E.2012/99 sayılı dosyanın 3.10.2012 gününde, E.2012/126 sayılı dosyanın 8.11.2012 gününde, E.2012/159 sayılı dosyanın ise 17.1.2013 gününde yapılan ilk inceleme toplantılarında başvurularda eksiklik

bulunmadığından işin esasının incelenmesine, E.2011/150, E.2012/43 ve E.2012/44 sayılı dosyalarda yürürlüğü durdurma isteminin esas inceleme aşamasında karara bağlanmasına, OYBİRLİĞİYLE karar verilmiştir.

IV- BİRLEŞTİRME KARARLARI

E.2012/41, E.2012/43, E.2012/44 ve E.2012/53 sayılı itiraz başvurularının 17.5.2012 gününde, E.2012/99 sayılı itiraz başvurusunun 3.10.2012 gününde, E.2012/126 sayılı itiraz başvurusunun 8.11.2012 gününde ve E.2012/159 sayılı itiraz başvurusunun 17.1.2013 gününde, aralarındaki hukuki irtibat nedeniyle E.2011/150 sayılı dava ile birleştirilmesine, esaslarının kapatılmasına, esas incelemenin E.2011/150 sayılı dosya üzerinden yürütülmesine OYBİRLİĞİYLE karar verilmiştir.

V- ESASIN İNCELENMESİ

Dava dilekçesi ve ekleri, Raportör Hikmet TÜLEN tarafından hazırlanan işin esasına ilişkin rapor, dava konusu Kanun Hükmünde Kararname kuralları, dayanan Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A- İptal Başvurusundan Önce Değiştirilen 209 Sayılı Kanun'un 5. Maddesinin İkinci Fıkrası

KHK'nin 58. maddesinin (13) numaralı fıkrasının (ç) bendiyle değiştirilen 209 sayılı Kanun'un 5. maddesinin ikinci fıkrasında yer alan 'Bu fıkra uyarınca personele her ay yapılacak ek ödeme tutarı, 375 sayılı Kanun Hükmünde Kararnamenin ek 3 üncü maddesi uyarınca kadro ve görev unvanı veya pozisyon unvanı itibarıyla belirlenmiş olan ek ödeme tutarından az olamaz. Bu kapsamdaki personel için 375 sayılı Kanun Hükmünde Kararnamenin ek 3 üncü maddesinin üçüncü fıkrası hükmü uygulanmaz.' ibaresi, 30.12.2011 günlü başvuru tarihinden önce yürürlüğe giren 666 sayılı KHK'nin 5. maddesinin (c) fıkrasının (1) numaralı alt bendi ile değiştirildiğinden, bu fıkraya yönelik iptal isteminin başvuranın yetkisizliği nedeniyle reddi gerekir.

B- İptal Başvurusundan Sonra Yapılan Değişikliklerin İptal Konusu Kurallara Etkisi

KHK'nin 8. maddesinin (1) numaralı fıkrasının (h) ve (r) bentleri, 4.7.2012 günlü, 6354 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un 20. maddesiyle yürürlükten kaldırıldığından,

KHK'nin 25. maddesinin (1) numaralı fıkrasının ikinci cümlesi, 6354 sayılı Kanun'un 21. maddesiyle yürürlükten kaldırıldığından,

KHK'nin 33. maddesinin (5) numaralı fıkrası, 6354 sayılı Kanun'un 16. maddesiyle değiştirildiğinden,

KHK'nin 58. maddesinin (7) numaralı fıkrasının (a) bendiyle deęiştirilen, 7.5.1987 gnl, 3359 sayılı Saęlık Hizmetleri Temel Kanunu'nun ek 1. maddesinin birinci fıkrası, 6354 sayılı Kanun'un 7. maddesiyle deęiştirildięinden,

KHK'nin 58. maddesinin (7) numaralı fıkrasının (c) bendiyle deęiştirilen 3359 sayılı Kanun'un ek 9. maddesi, 6354 sayılı Kanun'un 8. maddesiyle deęiştirildięinden,

KHK'nin 58. maddesinin (13) numaralı fıkrasının () bendiyle deęiştirilen, 4.1.1961 gnl, 209 sayılı Saęlık Bakanlıęına Baęlı Saęlık Kurumları ile Esenlendirme (Rehabilitasyon) Tesislerine Verilecek Dner Sermaye Hakkında Kanun'un 5. maddesinin altıncı fıkrası, 11.10.2011 gnl, 666 sayılı Kamu Grevlilerinin Mali Haklarının Dzenlenmesi Amacıyla Bazı Kanun ve Kanun Hkmnde Kararnamelerde Deęiřiklik Yapılmasına Dair Kanun Hkmnde Kararname'nin 5. maddesinin (c) fıkrasının (1) numaralı alt bendi ile deęiştirildięinden,

konusu kalmayan bu maddeye, fıkralara, bentlere ve cmleye ynelik iptal istemleri hakkında karar verilmesine yer olmadıęına karar vermek gerekir.

C- Kanun Hkmnde Kararnamelerin Yargısal Denetimi Hakkında Genel Aıklama

Anayasa'nın 91. maddesinde dzenlenen kanun hkmnde kararnameler, iřlevsel ynden yasama iřlemi nitelięinde olduęundan yargısal denetimlerinin yapılması grev ve yetkisi Anayasa'nın 148. maddesi ile Anayasa Mahkemesine verilmiřtir. Yargısal denetimde kanun hkmnde kararnamenin, ncelikle yetki kanununa sonra da Anayasa'ya uygunluęu sorunlarının zmlenmesi gerekir. Her ne kadar, Anayasa'nın 148. maddesinde kanun hkmnde kararnamelerin yetki kanunlarına uygunluęunun denetlenmesinden deęil, yalnızca Anayasa'ya biim ve esas bakımlarından uygunluęunun denetlenmesinden sz edilmekte ise de Anayasa'ya uygunluk denetiminin ierisine ncelikle kanun hkmnde kararnamenin yetki kanununa uygunluęunun denetimi de girer. nk Anayasa'da, Bakanlar Kuruluna ancak yetki kanununda belirtilen sınırlar ierisinde kanun hkmnde kararname ıkarma yetkisi verilmesi ngrlmřtir. Yetkinin dıřına ıkılması, kanun hkmnde kararnameyi Anayasa'ya aykırı duruma getirir.

Dayanaklarını doęrudan doęruya Anayasa'dan alan olaęanst hal kanun hkmnde kararnamelerinden farklı olarak, olaęan dnemlerdeki kanun hkmnde kararnamelerin bir yetki kanununa dayanması zorunludur. Bu nedenle, kanun hkmnde kararnameler ile dayandıkları yetki kanunu arasında ok sıkı bir baę vardır. Kanun hkmnde kararnamenin yetki kanunu ile olan baęı, kanun hkmnde kararnameyi aynen ya da deęiřtirerek kabul eden kanun ile kesilir. Kanun hkmnde kararnamenin Anayasa'ya uygun bir yetki kanununa dayanması, geerlilięinin n

koşuludur. Bir yetki kanununa dayanmadan çıkartılan veya dayandığı yetki kanunu iptal edilen kanun hükmünde kararnamelerin içeriği Anayasa'ya aykırılık oluşturmasa bile bunların Anayasa'ya uygunluğundan söz edilemez.

Kanun hükmünde kararnamelerin Anayasa'ya uygunluk denetimi, kanunların denetiminden farklıdır. Anayasa'nın 11. maddesinde, 'Kanunlar Anayasaya aykırı olamaz.' denilmektedir. Bu nedenle kanunların denetiminde, onların yalnızca Anayasa kurallarına uygun olup olmadıkları saptanır. Kanun hükmünde kararnameler ise konu, amaç, kapsam ve ilkeleri yönünden hem dayandıkları yetki kanununa hem de Anayasa'ya uygun olmak zorundadırlar.

Anayasa'da kimi konuların kanun hükmünde kararnamelerle düzenlenmesi yasaklanmaktadır. Anayasa'nın 91. maddesinin birinci fıkrasında, 'Sıkıyönetim ve olağanüstü haller saklı kalmak üzere, Anayasanın ikinci kısmının birinci ve ikinci bölümlerinde yer alan temel haklar, kişi hakları ve ödevleri ile dördüncü bölümde yer alan siyasî haklar ve ödevler...'in kanun hükmünde kararnamelerle düzenlenemeyeceği belirtilmiştir. Bu kural gereğince, Türkiye Büyük Millet Meclisi, 'Bakanlar Kurulu'na ancak kanun hükmünde kararnameyle düzenlenmesi yasaklanmış alana girmeyen konularda kanun hükmünde kararname çıkarma yetkisi verebilir.

Anayasa'nın herhangi bir maddesinde kanunla düzenleneceği öngörülen bir konunun, Anayasa'nın 91. maddesinin birinci fıkrasının açıkça yasakladığı hükümler ile ilgili olmadıkça ya da Anayasa'nın 163. maddesinde olduğu gibi kanun hükmünde kararname çıkarılamayacağı açıkça belirtilmedikçe kanun hükmünde kararname ile düzenlenmesi Anayasa'ya aykırılık oluşturmaz.

D- Kanun Hükmünde Kararname'nin Ayrı Ayrı Tüm Maddeleri ve Eki (I), (II) ve (III) Sayılı Cetveller ile Listelerin 6223 Sayılı Yetki Kanunu Kapsamında Olup Olmadığının İncelenmesi

Dava dilekçesinde, KHK'nin ayrı ayrı tüm maddelerinin ve eki (I), (II) ve (III) sayılı cetveller ile listelerin 6223 sayılı Yetki Kanunu kapsamında olmadığı ve acil, ivedi, önemli ve zorunlu konuları düzenlemediği belirtilerek Anayasa'nın Başlangıcı ile 2., 6., 7. 8., 87. ve 91. maddelerine aykırı oldukları ileri sürülmüştür.

6223 sayılı Yetki Kanunu'nun amaç ve kapsamını düzenleyen 1. maddesinde Kanun'un amacı, kamu hizmetlerinin düzenli, süratli, etkin, verimli ve ekonomik bir şekilde yürütülmesini sağlamak olarak belirlenmiş ve yetkinin kapsamı iki başlık altında tespit edilmiştir. Yetkinin kapsamına ilk olarak kamu hizmetlerinin bakanlıklar arasındaki dağılımının yeniden belirlenmesi girmektedir. Bu çerçevede gerekli görülmesi halinde yeni bakanlıklar kurulması, var olan bakanlıkların

birleştirilmesi, bakanlıkların bağlı, ilgili ve ilişkili kuruluşlarının yeniden belirlenmesi için KHK çıkarma yetkisi verilmiştir. Bu amaçla;

1- Mevcut bakanlıkların birleştirilmesine veya kaldırılmasına, yeni bakanlıklar kurulmasına, anılan bakanlıkların bağlı, ilgili ve ilişkili kuruluşlarıyla hiyerarşik ilişkilerine,

2- Mevcut bağlı, ilgili ve ilişkili kuruluşların bağlılık ve ilgilerinin yeniden belirlenmesine veya bunların mevcut, birleştirilen veya yeni kurulan bakanlıklar bünyesinde hizmet birimi olarak yeniden düzenlenmesine,

3- Mevcut bakanlıklar ile birleştirilen veya yeni kurulan bakanlıkların görev, yetki, teşkilat ve kadrolarının düzenlenmesine, taşrada ve yurt dışında teşkilatlanma esaslarına,

ilişkin kanun hükmünde kararname çıkarılabilecektir.

İkinci olarak kamu kurum ve kuruluşlarında istihdam edilen memurlar, işçiler, sözleşmeli personel ile diğer kamu görevlilerinin atanma, nakil, görevlendirilme, seçilme, terfi, yükselme, görevden alınma ve emekliye sevk edilme usul ve esaslarına ilişkin olarak değişiklikler ve yeni düzenlemeler yapılması için KHK çıkarma yetkisi verilmiştir.

1- KHK'nin 58. Maddesinin (12) Numaralı Fıkrası

KHK'nin 58. maddesinin (12) numaralı fıkrasıyla, 7.6.1985 günlü, 3224 sayılı Türk Diş Hekimleri Birliği Kanunu'nun 11., 26. ve 40. maddelerinde değişiklikler yapılmıştır. Dava konusu kurallar uyarınca, serbest çalışan diş hekimlerinin muayene ve tedavi ücretlerine ilişkin rehber tarife teklifleri diş hekimleri odalarının hazırlanacak ve bu rehber tarife teklifleri Türk Diş Hekimleri Birliği (TDB) Merkez Yönetim Kurulunca tasdik edilerek uygulamaya konulacaktır. Dava konusu kurullarla, Sağlık Bakanlığı, tarifelerin belirlenmesi sürecinde onay makamı olmaktan çıkarılmış, sadece, TDB'nin onayladığı rehber tarifenin Sağlık Bakanlığına bildirileceği kuralına yer verilmiştir.

6223 sayılı Yetki Kanunuyla kamu hizmetlerinin bakanlıklar arasındaki dağılımının yeniden belirlenmesi amacıyla Bakanlar Kuruluna verilen kanun hükmünde kararname çıkarma yetkisi, Bakanlıklar ile bağlı, ilgili ve ilişkili kuruluşları kapsamakta olup Bakanlık veya bağlı, ilgili ve ilişkili kuruluş niteliğinde olmayan kamu kurum ve kuruluşları kapsamına almamaktadır. Bakanlar Kurulunun, 6223 sayılı Yetki Kanunu'na dayanarak bakanlık veya bağlı, ilgili ve ilişkili kuruluş niteliğinde olmayan kamu kurum ve kuruluşlarının görev, yetki, teşkilat ve kadrolarına ilişkin düzenleme yapması mümkün değildir.

KHK'nin dava konusu kuralıyla, TDB'nin görev ve yetkilerinin düzenlendiği 3224 sayılı Türk Diş Hekimleri Birliđi Kanunu'nda deđişiklikler yapılmaktadır. TDB, Anayasa'nın 135. maddesi uyarınca kanunla kurulmuş, tüzel kişiliđe sahip, kamu kurumu niteliğinde bir meslek kuruluşudur. Merkezî idare, kamu kurumu niteliğinde meslek kuruluşları üzerinde vesayet yetkisine sahip olmakla birlikte bu durum, meslek kuruluşlarını merkezi idarenin bađlı, ilgili veya iliřkili kuruluşu haline getirmemektedir. Bu itibarla, kamu kurumu niteliğinde meslek kuruluşu olan TDB'nin görevinde deđişiklik öngören dava konusu kural, 6223 sayılı Yetki Kanunu kapsamında deđildir. İptali gerekir.

2- KHK'nin 58. Maddesinin (14) Numaralı Fıkrasının (ğ) Bendi

KHK'nin 58. maddesinin (14) numaralı fıkrasının (ğ) bendiyle, 23.1.1953 günlü, 6023 sayılı Türk Tabipleri Birliđi Kanunu'nun, Türk Tabipler Birliđini (TTB) tanımlayan 1. maddesinde geçen 'tabipliđin kamu ve kişi yararına uygulanıp geliştirilmesini sađlamak' ibaresi yürürlükten kaldırılmıştır.

TTB, Anayasa'nın 135. maddesi uyarınca kanunla kurulmuş, tüzel kişiliđe sahip, kamu kurumu niteliğinde bir meslek kuruluşu olup 6223 sayılı Yetki Kanunu kapsamında kamu kurumu niteliğinde meslek kuruluşlarının statülerine iliřkin düzenleme yapılması mümkün deđildir.

Açıklanan nedenlerle, kamu kurumu niteliğinde meslek kuruluşu olan TTB'nin statüsüne iliřkin düzenleme içeren kural, 6223 sayılı Yetki Kanunu kapsamında deđildir. İptali gerekir.

3- KHK'nin Diđer Kuralları

Yukarıdaki açıklamalar çerçevesinde yapılan inceleme sonucunda; KHK'nin, 6223 sayılı Yetki Kanunu kapsamında olmadığı gerekçesiyle iptal edilen kuralları ile hakkında karar verilmesine yer olmadığına karar verilenler dışında kalan diđer kurallarının 6223 sayılı Yetki Kanunu'nun kapsamında olduđu anlaşıldığından bu maddelere, fıkralara, bentlere, bölümlere, cetvellere ve listelere iliřkin iptal isteminin reddi gerekir.

Serruh KALELİ, Mehmet ERTEN, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŞ, KHK'nin 58. maddesinin (8) numaralı fıkrasının (b) bendi ile 11.4.1928 günlü, 1219 sayılı Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanun'un 4. maddesinin birinci cümlesindeki 'Türk Hekimlerinin' ibaresinin 'hekimlerin' şeklinde deđiřtirilmesi ile (9) numaralı fıkrası yönünden bu görüşe katılmamışlardır.

E- Kanun Hükmünde Kararname'nin Tüm Maddelerinin Anayasa'nın 91. Maddesi Yönünden İncelenmesi

Dava dilekçesinde, KHK'nin ayrı ayrı tüm maddelerinin ve eki (I), (II) ve (III) sayılı cetveller ile listelerin Anayasa'nın 91. maddesinin birinci fıkrasında kanun hükmünde kararnameyle düzenlenmesi yasaklanmış alanlara ilişkin düzenleme içerdiği, bu nedenle Anayasa'nın Başlangıç'ı ile 2., 6., 7. 8., 87. ve 91. maddelerine aykırı oldukları ileri sürülmüştür.

1- KHK'nin 16. Maddesinin (2) Numaralı Fıkrasının Birinci Cümlesinde Yer Alan "gerçek ve", "gizli dahi olsa" İbareleri

KHK'nin 16. maddesinde, Rehberlik ve Teftiş Başkanlığı düzenlenmiştir. Anılan maddenin (1) numaralı fıkrasında Başkanlığın görevleri sayıldıktan sonra dava konusu kuralı da içeren (2) numaralı fıkrasının birinci cümlesinde, denetime tâbi olan gerçek ve tüzel kişilere, gizli dahi olsa bütün belge, defter ve bilgilerin talep edilmesi durumunda ibraz etme, para ve para hükmündeki evrakı ve ayniyatı ilk talep hâlinde gösterme, sayılmasına ve incelenmesine yardımcı olma ödevi yüklenmiştir.

Anayasa'nın 91. maddesinin birinci fıkrasında 'Sıkıyönetim ve olağanüstü haller saklı kalmak üzere, Anayasanın ikinci kısmının birinci ve ikinci bölümlerinde yer alan temel haklar, kişi hakları ve ödevleri ile dördüncü bölümde yer alan siyasî haklar ve ödevler...'in kanun hükmünde kararnamelerle düzenlenemeyeceği belirtilmiştir.

Anayasa'nın 'Özel Hayatın Gizliliği' başlıklı 20. maddesinin birinci fıkrasında, 'Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.' hükmüne yer verilmiş, üçüncü fıkrasında ise 'Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.' denilmiştir. Buna göre, Anayasa'nın 20. maddesinde düzenlenen ve 'Kişinin Hakları ve Ödevleri' başlıklı ikinci bölümünde yer alan özel hayatın gizliliği ve kişisel verilerin korunması hakkına ilişkin olarak kanun hükmünde kararname ile düzenleme yapılması mümkün değildir.

KHK'nin 16. maddesinin (2) numaralı fıkrasının birinci cümlesiyle gerçek kişilerinin gizli bilgilerinin sağlık denetçilerine ibrazı zorunluluğunun getirilmiş olması, özel hayatın gizliliği ve kişisel verilerin korunması hakkına ilişkin bir düzenleme niteliğindedir. Dolayısıyla kural, Anayasa'nın 91. maddesinin birinci fıkrasına aykırıdır. İptali gerekir.

2- KHK'nin 23. Maddesinin (7) Numaralı Fıkrasının (c) ve (ç) Bentleri

KHK'nin 23. maddesinde, Sağlık Hizmetleri Kurulunun oluşumu, görev, yetki ve sorumlulukları ile sağlık meslek mensubuna uygulanacak yaptırımlar düzenlenmektedir. Anılan maddenin (6) numaralı fıkrasının (e) bendinde, meslekten geçici veya sürekli men etmeye karar vermek Kurulun görevleri arasında sayılmış, (7) numaralı fıkrasının (c) bendinde, meslek icrası esnasında neticesini öngörerek veya görevinin gereklerine aykırı hareket ederek veyahut görevinin gereklerini yapmakta ihmal veya gecikme göstererek bir kişinin ağır derecede olmayan özürüllüğüne sebebiyet verenlerin üç aydan bir yıla kadar meslekten geçici men edilmesine karar verileceği, bu fiillerin beş yıl içinde tekrarı hâlinde verilecek cezalarda alt ve üst sınırların iki katı olarak uygulanacağı hükme bağlanmış, (ç) bendinde ise meslek icrası esnasında neticesini öngörerek veya görevinin gereklerine aykırı hareket ederek veyahut görevinin gereklerini yapmakta ihmal veya gecikme göstererek bir kişinin ağır özürüllüğüne veya ölümüne sebebiyet verenlerin bir yıldan üç yıla kadar meslekten geçici olarak men edilmesine karar verileceği, bu fiillerin beş yıl içinde tekrarı hâlinde meslekten sürekli men kararı verileceği belirtilmiştir.

Anayasa'nın 'Suç ve cezalara ilişkin esaslar' başlıklı 38. maddesinin üçüncü fıkrasında, 'Ceza ve ceza yerine geçen güvenlik tedbirleri ancak kanunla konulur.' hükmüne yer verilmiştir. Anayasa'nın 38. maddesinde düzenlenen ve ikinci kısmının 'Kişinin Hakları ve Ödevleri' başlıklı ikinci bölümünde yer alan suç ve cezalara ilişkin hükümlerin kanun hükmünde kararnameyle düzenlenmesi mümkün değildir.

Dava konusu kurallar, Anayasa'nın 38. maddesi kapsamında değerlendirilmesi gereken sağlık meslek mensuplarının meslekten geçici men ve meslekten men edilmesini gerektiren fiiller ile bu fiillere uygulanacak yaptırımlara ilişkin hükümler içerdiğinden, Anayasa'nın 91. maddesinin birinci fıkrasına aykırıdır. İptali gerekir.

3- KHK'nin 44. Maddesinin (2), (3) ve (4) Numaralı Fıkraları

KHK'nin 44. maddesinin (1) numaralı fıkrasıyla, Sağlık Bakanlığı ve bağlı kuruluşların merkez teşkilatı bünyesinde Sağlık Uzmanlığı, Sağlık Uzman Yardımcılığı, Sağlık Denetçiliği ve Sağlık Denetçi Yardımcılığı kadroları ihdas edilmiş; (2) numaralı fıkrasında Uzman Yardımcılığı ve Denetçi Yardımcılığı kadrolarına atanabilme koşulları düzenlenmiş; (3) numaralı fıkrasında Uzman Yardımcılığı ve Denetçi Yardımcılığından Uzman ve Denetçiliğe geçiş koşulları belirlenmiş; (4) numaralı fıkrasında ise bu kadrolarda görev yapanların mesleğe alınmaları, yetiştirilmeleri, yarışma sınavı, tez hazırlama ve yeterlik sınavı ile diğer hususların yönetmelikle düzenlenmesi öngörülmüştür.

Anayasa'nın 'Kamu hizmetlerine girme hakkı' başlıklı 70. maddesinin birinci fıkrasında, her Türk'ün, kamu hizmetlerine girme hakkına sahip olduğu belirtildikten sonra ikinci fıkrasında ise hizmete alınmada, görevin gerektirdiği niteliklerden başka hiçbir ayırım gözetilemeyeceği kurala bağlanmıştır. Buna göre, Anayasa'nın 70. maddesinde düzenlenen ve ikinci kısmının 'Siyasi Haklar ve Ödevler' başlıklı dördüncü bölümünde yer alan kamu hizmetlerine girme hakkına ilişkin olarak kanun hükmünde kararname ile düzenleme yapılması mümkün değildir.

Sağlık Uzmanlığı, Sağlık Uzman Yardımcılığı, Sağlık Denetçiliği ve Sağlık Denetçi Yardımcılığı kadrolarına giriş koşullarının belirlenmesi, Anayasa'nın 70. maddesine göre kamu hizmetine girme hakkına ilişkin bir düzenleme olduğundan KHK'nin 44. maddesinin (2), (3) ve (4) numaralı fıkraları, Anayasa'nın 91. maddesinin birinci fıkrasına aykırıdır. İptalleri gerekir.

Serdar ÖZGÜLDÜR ve Burhan ÜSTÜN değişik gerekçeyle bu görüşe katılmışlardır.

Haşim KILIÇ, Alparslan ALTAN, Engin YILDIRIM, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI ile Muammer TOPAL bu görüşe katılmamışlardır.

4- KHK'nin 47. Maddesinin (1), (2) ve (3) Numaralı Fıkraları

KHK'nin 47. maddesinde, Bakanlığın bilgi toplama, işleme ve paylaşma yetkisine ilişkin hükümler düzenlenmiştir. Anılan maddenin (1) numaralı fıkrasıyla, Bakanlık ve bağlı kuruluşlarına, mevzuatla kendilerine verilen görevleri, e-devlet uygulamalarına uygun olarak daha etkin ve hızlı biçimde yerine getirebilmek için, bütün kamu ve özel sağlık kurum ve kuruluşlarından; sağlık hizmeti alanların, aldıkları sağlık hizmetinin gereği olarak ilgili sağlık kurum ve kuruluşuna vermek zorunda oldukları kişisel bilgileri ve bu kimselere verilen hizmete ilişkin bilgileri her türlü vasıta ile toplama, işleme ve paylaşma yetkisi verilmiştir. Maddenin (2) numaralı fıkrasında, Bakanlık ve bağlı kuruluşlarının işlediği kişisel sağlık verilerini ilgili üçüncü kişiler ve kamu kurum ve kuruluşları ile ancak bu kişi ve kurumların bu verilere erişebileceği hususunda kanunen yetkili olması halinde ve görevlerini yapmalarına yetecek derecede paylaşabilecekleri belirtilmiştir. Maddenin (3) numaralı fıkrasında ise Bakanlık ve bağlı kuruluşlarının, mevzuatla kendilerine verilen görevleri yerine getirebilmek için gereken bilgileri, kamu ve özel ilgili bütün kişi ve kuruluşlardan istemeye yetkili oldukları ve ilgili kişi ve kuruluşların istenilen bilgileri vermekle yükümlü oldukları kurala bağlanmıştır.

Anayasa'nın ikinci kısmının 'Kişinin Hakları ve Ödevleri' başlıklı ikinci bölümünde yer alan 20. maddesiyle güvenceye bağlanan özel hayatın gizliliği ve kişisel verilerin korunması hakkına ilişkin düzenlemeler içeren dava konusu kurallar, KHK'nin 16. maddesinin (2) numaralı fıkrasının birinci

cümlesinde yer alan "gerçek ve", "gizli dahi olsa" ibareleri için açıklanan gerekçelerle, Anayasa'nın 91. maddesinin birinci fıkrasına aykırıdır. İptali gerekir.

5- KHK'nin 55. Maddesi

KHK'nin 55. maddesiyle, Sağlık Bakanlığına, gerek kamuya ait gerekse özel kişi ve kuruluşlara ait bütün sağlık kuruluşlarında çalışmakta olan her kademedeki sağlık personeli için görevli olduğu sağlık kuruluşunun bulunduğu yerleşim yeri sınırları içinde ikamet etme mecburiyeti getirme yetkisi tanınmıştır. Bu mecburiyetin usul ve esaslarının ise Bakanlıkça belirlenmesi öngörülmüştür.

Sağlık personeline çalıştığı yerde ikamet mecburiyeti getirilmesi hususu, Anayasa'nın 23. maddesinde düzenlenmiş bulunan 'yerleşme ve seyahat hürriyeti' ile yakından ilgilidir. Bu madde, Anayasa'nın ikinci kısmının ikinci bölümünde düzenlenmiştir. Anayasa'nın 91. maddesi gereğince bu bölümde yer alan hak ve hürriyetlerin KHK'lerle düzenlenmesi mümkün değildir.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 91. maddesinin birinci fıkrasına aykırıdır. İptali gerekir.

6- KHK'nin Diğer Kuralları

KHK'nin 16. maddesinin (2) numaralı fıkrasının birinci cümlesinde yer alan "gerçek ve", "gizli dahi olsa" ibareleri, 23. maddesinin (7) numaralı fıkrasının (c) ve (ç) bentleri, 44. maddesinin (2), (3) ve (4) numaralı fıkraları, 47. maddesinin (1), (2) ve (3) numaralı fıkraları ve 55. maddesi ile 6223 sayılı Yetki Kanunu kapsamında bulunmadıkları gerekçesiyle iptal edilenler ve ayrıca hakkında karar verilmesine yer olmadığına karar verilenler dışında kalan diğer kurallarında Anayasa'nın 91. maddesinin birinci fıkrası uyarınca kanun hükmünde kararname ile düzenlenmesi yasaklanmış alanlara ilişkin herhangi bir düzenlemeye yer verilmediği anlaşıldığından bu maddelere, fıkralara, bentlere, bölümlere, cetvellere ve listelere ilişkin iptal isteminin reddi gerekir.

KHK'nin;

6. maddesinin (2) ve (3) numaralı fıkraları yönünden Mehmet ERTEN, Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŞ,

20. maddesi yönünden Mehmet ERTEN,

23. maddesinin (7) numaralı fıkrasının (a) bendi yönünden Serruh KALELİ, Mehmet ERTEN, Osman Alifeyyaz PAKSÜT, Zehra Ayla PERKTAŞ ile Zühtü ARSLAN,

23. maddesinin (8), (10), (11), (12) ve (13) fıkraları yönünden Mehmet ERTEN,

24. maddesi yönünden Osman Alifeyyaz PAKSÜT,

32. maddesinin (2), (4) ve (5) numaralı fıkraları yönünden Mehmet ERTEN, Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŞ,

33. maddesinin (1), (2), (3), (4) ve (6) numaralı fıkraları yönünden Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŞ,

45. maddesi yönünden Mehmet ERTEN, Serdar ÖZGÜLDÜR ile Zehra Ayla PERKTAŞ,

bu görüşe katılmamışlardır.

F- Kanun Hükmünde Kararname'nin İçerik Yönünden İncelenmesi

1- KHK'nin 2. Maddesinin (2) Numaralı Fıkrasının Sonunda Yer Alan 'ile ilgili olarak' İbaresini

Dava dilekçesinde, sağlık hizmetlerinin üretilmesi ve sunulmasında, örgütlenme yöntemi bakımından 'bağlı kuruluş' modelinin tercih edildiği, bu kapsamda Türkiye Halk Sağlığı Kurumu ile Türkiye Kamu Hastaneleri Kurumunun kurulduğu, önceki yasal düzenlemelerde Sağlık Bakanlığının görevleri içinde yer alan koruyucu, tedavi ve rehabilite edici hizmetlerin bu iki kuruma devredildiği, her iki bağlı kuruluşun Bakanlıktan ayrı bir teşkilat yapısına sahip olduğu, bu düzenlemelerle Sağlık Bakanlığının bir tür düzenleyici kurula dönüştürülerek, kamu sağlık hizmetinin yürütülmesi görevinin merkezi idareden adeta bağımsız hale getirilen bağlı kuruluşlara devredildiği belirtilerek kuralın, Anayasa'nın 2., 17., 56., 123. ve 126. maddelerine aykırı olduğu ileri sürülmüştür.

KHK'nin 2. maddesinde, Sağlık Bakanlığının görevleri düzenlenmiştir. Maddenin (1) numaralı fıkrasında, Bakanlığın görevinin, herkesin bedenî, zihnî ve sosyal bakımdan tam bir iyilik hâli içinde hayatını sürdürmesini sağlamak olduğu belirtildikten sonra dava konusu kuralı da içeren (2) numaralı fıkrasında, Sağlık Bakanlığının, yedi bent halinde sayılan hususlar 'ile ilgili olarak' sağlık sistemini yöneteceği ve politikaları belirleyeceği ifade edilmiş, fakat sağlık hizmetini yerine getirecek teşkilatın yapısına dair herhangi bir düzenlemeye yer verilmemiştir. Dava dilekçesinde sözü edilen bağlı kuruluşlar ise KHK'nin müteakip maddelerinde düzenlenmiştir. Bu itibarla, anılan (2) numaralı fıkradaki bentlerde yer alan hususları tek bir yüküleme bağlamak dışında hiçbir fonksiyonu olmayan 'ile ilgili olarak' ibaresinin, Anayasa'ya aykırı bir yönü bulunmamaktadır. İptal isteminin reddi gerekir.

2- KHK'nin 6. Maddesinin (1) ve (2) Numaralı Fıkraları

Dava dilekçesinde, Sağlık Politikaları Kuruluna, sağlık hizmetinin yürütülmesinde temel değerde olan yönetim ve politika belirleme yetkisinin verildiği, bu nedenle Kurul üyelerinin de görevin gerektirdiği niteliklere sahip olmalarının zorunlu olduğu, buna karşılık dava konusu kurallarda

Kurul üyelerinin sağlık hizmetinin gerektirdiği eğitimi almış olmalarına, bu alanda deneyim ve beceri sahibi olmalarına ilişkin herhangi bir ilkenin konulmadığı belirtilerek kuralların, Anayasa'nın 2. ve 128. maddelerine aykırı olduğu ileri sürülmüştür.

KHK'nin 6. maddesinde, Sağlık Politikaları Kurulu düzenlenmektedir. Maddenin iptali istenilen (1) ve (2) numaralı fıkralarında, Sağlık Politikaları Kurulunun oluşumu, Kurul üyelerinde aranacak nitelikler, üyelerin görev süresine ilişkin hükümlere yer verilmektedir. Buna göre, Sağlık Politikaları Kurulu, Bakanlığın sağlık sistemi yönetimi ve politika belirlemek ile ilgili temel görevlerini yerine getirmek üzere görevlendirilen on bir üye ile Müsteşar ve müsteşar yardımcılarında oluşmaktadır. Kurul üyeleri en az dört yıllık yüksek okul mezunu ve sekiz yıl iş tecrübesi bulunanlar arasında Bakan tarafından görevlendirilmektedir. Görev süresi iki yıl olup süresi sona eren üyelerin yeniden görevlendirilmeleri mümkündür. Kurula, Müsteşar veya görevlendireceği yardımcılardan biri başkanlık eder.

Anayasa'nın 2. maddesinde yer alan hukuk devletinin temel ilkelerinden biri 'belirlilik ilkesi'dir. Bu ilkeye göre, yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olması ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi gerekir.

Anayasa'nın 128. maddesinde, 'Devletin, kamu iktisadî teşebbüsleri ve diğer kamu tüzelkişilerinin genel idare esaslarına göre yürütmekle yükümlü oldukları kamu hizmetlerinin gerektirdiği aslî ve sürekli görevler, memurlar ve diğer kamu görevlileri eliyle görülür. Memurların ve diğer kamu görevlilerinin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülükleri, aylık ve ödenekleri ve diğer özlük işleri kanunla düzenlenir. Üst kademe yöneticilerinin yetiştirilme usul ve esasları, kanunla özel olarak düzenlenir.' denilmektedir. Buna göre, Anayasa'nın 128. maddesinin birinci fıkrası kapsamındaki görevleri yürüten bütün personelin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülüklerinin kanunla düzenlenmesi gerekir. Ancak kanunla düzenlenme şartı, memurlar ve diğer kamu görevlilerinin görev, yetki ve sorumlulukları ile özlük haklarının her türlü ayrıntısının kanunla belirlenmesi anlamına gelmemektedir. Kanun koyucunun, gerektiğinde sınırlarını belirlemek koşuluyla bazı konuların düzenlenmesini idareye bırakması Anayasa'nın 128. maddesine aykırı olmaz.

Sağlık sistemi yönetimi ve politika belirleme ile ilgili temel görevleri ifa etmek üzere kurulan Sağlık Politikaları Kurulu üyelerinin, Anayasa'nın 128. maddesi kapsamında devletin genel idare esaslarına göre yükümlü olduğu asli ve sürekli görevleri yürüten kamu görevlisi niteliğinde olduklarında kuşku bulunmamaktadır.

Dava konusu kuralda, bu Kurulun sađlık sistemi yonnetimi ve politika belirleme ile ilgili temel goevleri ifa edeceđi belirtilmiřtir. Ote yandan Kurulun, Bakan tarafından goevlendirilecek on bir uye ile Muřteřar ve muřteřar yardımcılarında oluşacađı, Bakan tarafından seęilecek uyelerin en az doirt yıllık yuksek okul mezunu ve sekiz yıl iř tecrubesinin bulunması gerektiđi belirtilerek uyelerinin nitelikleri ile atama usulu duzenlenmiřtir. Ayrıca maddenin dava konusu olmayan fıkralarında Kurulun ozluk hakları, yetkileri ile ęalıřma usul ve esaslarına iliřkin genel ilkeler belirlenmiřtir. Dolayısıyla Kurul uyelerinin nitelikleri, atanmaları, goev ve yetkileri, hakları ve yukumluluklerinin genel çerçevesinin kanunla belirlendiđi aęıktır.

Ote yandan, Kurul uyeliđine atanacak kiřilerin nitelik ve kabiliyetlerinin saptanması kanun koyucunun takdirinde olup, dava konusu kuralda Kurul uyeliđine atanacaklar için ongoruilen kořulların Kurula verilen goev ve yetkilerle uyumlu olup olmadıđı veya bu niteliklere sahip kiřilerin KHK'de belirlenen yetkileri kullanmaya ehil olup olmadıkları sorunu anayasallık denetiminin kapsamı dıřında kalmaktadır.

Aęıklanan nedenlerle, dava konusu kurallar Anayasa'nın 2. ve 128. maddelerine aykırı deđildir. İptal istemlerinin reddi gerekir.

Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŐ bu goruře katılmamıřlardır.

3- KHK'nin 7. Maddesinin (1) Numaralı Fıkrasının (ğ) Bendi ile 16. Maddesinin (2) Numaralı Fıkrasının Birinci Cümlesinde Yer Alan "gerçek ve", "gizli dahi olsa" İbareleri Dıřında Kalan Bölümü

Dava dilekçesinde, mülga 181 sayılı KHK döneminde danıřma ve denetim birimi olarak dođrudan bakana bađlı olan Teftiř Kurulu Başkanlıđının dava konusu kurallarla, Denetim Hizmetleri Başkanlıđına dönüřtürüldüđu ve hiyerarřik yapılanmada muřteřar yardımcısına bađlandıđı, bu durumun 3046 sayılı Kanun'a uygun olmadıđı ve hukuk devleti ilkesiyle ęeliřtiđi, Bakan adına ve dođrudan bakana bađlı olarak yürütülmesi gereken denetim, teftiř ve soruřturma goevlerinin Bakanlık merkezinde muřteřar yardımcısına, bađlı kuruluřlarda ise genel müdür ya da başkana veya bunların yardımcılara bađlı olarak yürütülmesinin denetimin bađımsızlıđı ve tarafsızlıđı ile bađdařmayacađı belirtilerek kuralın, Anayasa'nın 2. ve 112. maddelerine aykırı olduđu ileri sürülmüřtür.

6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 43. maddesine göre, ilgisi nedeniyle dava konusu kural, Anayasa'nın 113. maddesi yönünden de incelenmiştir.

KHK'nin 7. maddesinde, Bakanlığın hizmet birimleri sıralanmış ve bu maddenin (ğ) bendinde, Denetim Hizmetleri Başkanlığı da Bakanlığın hizmet birimleri arasında gösterilmiştir. 13.12.1983 günlü, mülga 181 sayılı Sağlık Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnameyle doğrudan Bakan'a bağlı olarak teşkil edilen Teftiş Kurulu Başkanlığının yerine kurulduğu anlaşılan Denetim Hizmetleri Başkanlığı, Bakanlığın hizmet birimleri arasında gösterilmek suretiyle Teftiş Kurulu Başkanlığından farklı olarak Bakan'a değil Müsteşara bağlı hale gelmiştir.

KHK'nin 16. maddesinde Denetim Hizmetleri Başkanlığının görev ve yetkileri düzenlenmiştir. Buna göre, Bakanlığın ve bağlı kuruluşlarının iş ve işlemleri hakkında yapılacak denetim, inceleme ve soruşturmalar ile bu kuruluşların performans denetiminin yapılması görevi Denetim Hizmetleri Başkanlığına aittir. Maddenin (2) numaralı fıkrasının, Anayasa'nın 91. maddesine aykırı bulunarak iptal edilen ibareleri dışında kalan bölümü uyarınca, denetime tâbi olan tüzel kişilerin, bütün belge, defter ve bilgileri talep edildiği takdirde ibraz edeceği, para ve para hükmündeki evrakı ve ayniyatı ilk talep hâlinde göstereceği, sayılmasına ve incelenmesine yardımcı olacağı açıktır.

Anayasa'nın 2. maddesindeki 'hukuk devleti' ilkesi gereğince, yasama işlemlerinin kişisel yararları değil kamu yararını gerçekleştirmek amacıyla yapılması zorunludur. Bir kuralın Anayasa'ya aykırılık sorunu çözümlenirken 'kamu yararı' konusunda Anayasa Mahkemesinin yapacağı inceleme yalnızca kanunun kamu yararı amacıyla yapılıp yapılmadığı ile sınırlıdır. Kanun ile kamu yararının gerçekleşip gerçekleşmeyeceğini denetlemenin anayasa yargısıyla bağdaşmayacağı, bunun kanun koyucunun takdirinde olduğu açıktır.

Anayasa'nın 113. maddesinin birinci fıkrasında, 'Bakanlıkların kurulması, kaldırılması, görevleri, yetkileri ve teşkilatı kanunla düzenlenir.' hükmüne yer verilmiştir. Bu hüküm gereğince Bakanlık teşkilatının kanunla kurulması zorunlu olmakla birlikte, Anayasa'da bakanlığa verilen denetim görevinin nasıl bir idari teşkilatlanmayı gerektirdiği konusunda herhangi bir hüküm bulunmamaktadır. Dolayısıyla denetim görevini yürütecek teşkilatın niteliğinin ve yapısının belirlenmesinin kanun koyucunun takdirine bırakıldığı kabulü gerekir. Kanun koyucunun bu yetkisini, kamu yararı ve denetim hizmetinin gerektirdiği bağımsızlık ve tarafsızlık ilkelerine uygun olarak kullanması gerektiği tabiidir.

Bu itibarla, dava konusu kuralla, yürürlükten kaldırılan 181 sayılı KHK döneminde danışma ve denetim birimi olarak doğrudan Bakan'a bağlı olan Teftiş Kurulu Başkanlığı kaldırılarak, denetim hizmetlerini yürütmek üzere Denetim Hizmetleri Başkanlığının kurulması hususu kanun koyucunun takdir yetkisi kapsamındadır. Denetim Hizmetleri Başkanlığının doğrudan Bakan'a bağlı olmayıp Müsteşar'a bağlı olması, denetim hizmetlerinin bağımsızlığını ve tarafsızlığını etkileyen bir durum değildir. Zira denetim hizmetinin işleyişi sırasında bağımsızlık ve tarafsızlık ilkesine uyulması koşuluyla, bu hizmeti yürüten birimin hiyerarşik olarak Bakan'a veya Müsteşar'a bağlı olmasının anayasal bir önemi bulunmamaktadır.

Dava dilekçesinde, Denetim Hizmetleri Başkanlığının Müsteşar'a bağlanmasının 3046 sayılı Kanun'a uygun olmadığı ileri sürülmüş ise de anılan Kanun'un Anayasa'ya uygunluk denetiminde ölçü norm teşkil etmeyeceği açıktır.

Açıklanan nedenlerle, dava konusu kurallar Anayasa'nın 2. ve 113. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir.

Kuralların, Anayasa'nın 112. maddesiyle ilgisi görülmemiştir.

4- KHK'nin 8. Maddesinin (1) Numaralı Fıkrasının (c) Bendinde Yer Alan "gerektiğinde süreli veya süresiz iptal etmek" İbaresini

Dava dilekçesinde, Sağlık Hizmetleri Genel Müdürlüğünün, izin ve ruhsatları iptal etme yetkisinin hangi hallerde kullanılabileceğinin KHK metninde açık olarak sayılmayıp 'gerektiğinde' bu yetkinin kullanılabileceğinin belirtilmiş olmasının hukuk devleti ilkesiyle bağdaşmadığı, düzenlemenin kişilerin çalışma hakkının sınırlandırılması konusunda idareye sınırsız bir takdir yetkisi verdiği belirtilerek kuralın, Anayasa'nın 2., 13. ve 48. maddelerine aykırı olduğu ileri sürülmüştür.

KHK'nin 8. maddesinde, Sağlık Hizmetleri Genel Müdürlüğünün görevleri düzenlenmiştir. Maddenin (1) numaralı fıkrasının dava konusu kuralı da içeren (c) bendiyle, anılan Genel Müdürlüğe, kamu ve özel hukuk tüzel kişileri ile gerçek kişilere ait sağlık kurum ve kuruluşlarına izin verme ve ruhsatlandırma, bu izin ve ruhsatları gerektiğinde süreli veya süresiz iptal etme görev ve yetkisi verilmiştir.

Dava konusu kuralla, sağlık hizmeti sunan kamu ve özel hukuk tüzel kişileri ile gerçek kişilerin izin ve ruhsatlarının gerektiğinde süreli veya süresiz iptal edilmesine olanak tanınmıştır. Sağlık hizmeti sunan kişi ve kuruluşlara izin ve ruhsat verilmesi usulü ile bu izin ve ruhsatların hangi koşullarda iptal edileceğine ilişkin hükümler ise 1219 sayılı Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanun ve ilgili diğer kanunlarda açıkça düzenlenmiştir. Dava konusu kural, söz konusu kanunlarda

Bakanlığa verilen izin ve ruhsat iptali yetkisinin Bakanlığın bir birimi olan Sağlık Hizmetleri Genel Müdürlüğü tarafından kullanılacağını ifade etmektedir. Sağlık Hizmetleri Genel Müdürlüğünün bu yetkisini ilgili mevzuatta öngörülen koşullar çerçevesinde kullanacağı tabiidir. Bu durumda, kuralda geçen 'gerektiğinde' sözcüğünden, ilgili mevzuatta öngörülen koşulların varlığı olarak anlaşılması gerektiği açıktır.

Anayasa'nın 48. maddesinde, 'Herkes, dilediği alanda çalışma ve sözleşme hürriyetlerine sahiptir.' hükmüne yer verilerek çalışma özgürlüğü güvence altına alınmıştır. Çalışma özgürlüğü, herkesin dilediği mesleği seçmede özgür olduğunu ve hiç kimsenin zorla çalıştırılmayacağını ifade etmektedir. Birey bu özgürlüğünü kullanarak dilediği alanı ve işi seçebilir. Çalışma hakkı ise bireyin özgür iradesiyle seçtiği mesleği veya işi icra etmesi, devletin de çalışmak isteyenlere iş temin etmek için gereken tedbirleri alması olarak tanımlanabilir.

Anayasa'nın 48. maddesinde, çalışma özgürlüğü için herhangi bir sınırlama nedeni öngörülmemiş olmakla birlikte, bunun hiçbir şekilde sınırlandırılması mümkün olmayan mutlak bir hak olduğu söylenemez. Özel sınırlama nedeni öngörülmemiş hakların da hakkın doğasından kaynaklanan bazı sınırları bulunduğu kabul edilmektedir. Ayrıca hakkı düzenleyen maddede herhangi bir sınırlama nedenine yer verilmemiş olsa da, Anayasa'nın başka maddelerinde yer alan kurallara dayanarak bu hakların sınırlandırılması da mümkün olabilir. Ancak bu sınırlamalar Anayasa'nın 13. maddesinde yer alan güvencelere aykırı olamaz. Anayasa'nın 13. maddesine göre temel hak ve özgürlüklere yönelik sınırlamalar, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacağı gibi hak ve özgürlüklerin özlerine de dokunamaz.

Dava konusu kuralla, Sağlık Hizmetleri Genel Müdürlüğüne tanınan sağlık hizmeti sunan kişi ve kuruluşlarının izin ve ruhsatlarını iptal etme yetkisinin çalışma özgürlüğüne müdahale niteliği taşıdığı tartışmasızdır. Ancak kuralla, bu özgürlüğün sınırlandırılmasına ilişkin maddi koşullar düzenlenmemiş olup bu yetkiyi kullanacak idari birim gösterilmiştir. Sağlık hizmeti sunan kişi ve kuruluşların çalışma özgürlüğünün sınırlandırılmasına ilişkin kurallar, ilgili diğer kanunlarda düzenlenmiştir. Dolayısıyla dava konusu kural yönünden çalışma özgürlüğüne getirilen bir sınırlama söz konusu değildir.

Açıklanan nedenle, dava konusu kural Anayasa'nın 2., 13. ve 48. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

5- KHK'nin 8. Maddesinin (1) Numaralı Fıkrasının (ç) Bendi

Dava dilekçesinde, kamu kurumu niteliğinde meslek kuruluşu olan Türk Tabipleri Birliği ve Türk Diş Hekimleri Birliğine ait olan sağlık hizmetlerinin ücret tarifesinin belirlenmesi veya tasdik edilmesi yetkisinin Sağlık Hizmetleri Genel Müdürlüğüne tanınmış olmasının, anayasal güvence altında olan kamu kurumu niteliğinde meslek kuruluşlarının görev alanına müdahale niteliği taşıdığı belirtilerek kuralın, Anayasa'nın 2. ve 135. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralla, Sağlık Hizmetleri Genel Müdürlüğüne, sağlık hizmetlerinin ücret tarifelerini belirleme veya tasdik etme yetkisi verildiği görülmektedir. Kuralda sözü edilen sağlık hizmetlerinin ücret tarifelerini belirleme yetkisi, meslek kuruluşlarınca hazırlanan tarifelerin anılan Genel Müdürlük tarafından vesayet yetkisi kapsamında denetlenmesi ve gözden geçirilmesini ifade etmekte olup, bu tarifelerin hazırlanmasının bütünüyle Genel Müdürlüğüne devredildiği anlamına gelmediği açıktır.

Anayasa'nın 135. maddesinde kamu kurumu niteliğindeki meslek kuruluşları ve üst kuruluşları tanımlanmıştır. Buna göre, kamu kurumu niteliğindeki meslek kuruluşları, belli bir mesleğe mensup olanların müşterek ihtiyaçlarını karşılamak, mesleki faaliyetlerini kolaylaştırmak, mesleğin genel menfaatlere uygun olarak gelişmesini sağlamak, meslek mensuplarının birbirleri ve halk ile olan ilişkilerinde dürüstlüğü ve güveni hâkim kılmak üzere meslek disiplini ve ahlakını korumak maksadı ile kanunla kurulan ve organları kendi üyeleri tarafından kanunda gösterilen usullere göre yargı gözetimi altında, gizli oyla seçilen kamu tüzelkişileridir. Anılan maddenin beşinci fıkrasına göre, meslek kuruluşları üzerinde devletin idari ve mali denetimine ilişkin kurallar kanunla düzenlenir.

Anayasa'nın 135. maddesinde, meslek kuruluşlarının karar ve yönetim organlarının seçimle göreve gelmesinin öngörülmesi, devletin idari ve mali denetimine tabi olduklarının belirtilmesi ve sorumlu organlarının görevlerine ancak yargı kararıyla son verilebileceğinin kurala bağlanması, bu idarelerin özerkliğine işaret etmektedir.

Meslek kuruluşlarının özerkliği, merkezi idareden bağımsız olarak karar ve yürütme organlarını seçebilme, ilgili mesleki faaliyetlerle sınırlı olmak üzere üyelerini ve örgütlerini bağlayıcı karar alma ve uygulama, meslek mensuplarının uyacağı ilke ve kuralları belirleme ve üyeleri hakkında disiplin tedbirleri uygulama hak ve yetkisini içermektedir. Ancak özerklik, meslek kuruluşlarının işlemlerinin idari vesayet yoluyla merkezî idarenin denetimine tabi kılınmasına engel değildir. Kanun koyucunun, idarenin bütünlüğü ilkesi uyarınca, merkezî idareye, bir idari vesayet yetkisi olarak meslek kuruluşu işlemlerini iptal etme, onama, yürürlüğünü erteleme, tekrar görüşülmesini isteme ve düzeltme yetkisi tanınması Anayasa'ya aykırı olmaz.

Kamu kurumu niteliğinde meslek kuruluşlarına üye meslek mensuplarınca sunulan hizmetin bedeline ilişkin tarifelerin belirlenmesi, meslek kuruluşlarının özerkliğinin gereğidir. Ancak bu durum, bu tarifelerin belirlenmesinin tamamen meslek kuruluşlarının inisiyatifine bırakılacağı ve merkezî idarenin hiçbir şekilde bu tarifelere müdahalede bulunamayacağı anlamına gelmez. Ücret tarifelerinin belirlenmesi, sadece meslek mensuplarının menfaatini ilgilendiren bir durum olmayıp, bunlardan hizmet satın alarak ücret ödeyen kişilerin de menfaatini etkilemektedir. Sağlık hizmeti satın alan bireylerin, meslek kuruluşlarının tek taraflı fiyatlandırma politikasıyla karşı karşıya bırakılması, Anayasa'nın 5. maddesiyle devlete yüklenen ödevle bağdaşmamaktadır. Kanun koyucunun, meslek mensuplarından hizmet satın alan bireylerin menfaatlerinin de gözetilmesi bakımından, merkezî idareyi de ücret tarifelerinin belirlenmesi sürecine dâhil etmesi Anayasa'ya aykırı görülemez.

Dava konusu kuralla, Sağlık Hizmetleri Genel Müdürlüğüne, meslek kuruluşlarınca hazırlanan ücret tarifelerini tasdik etme yetkisi tanınmasının, bireylerin meslek kuruluşlarının tek taraflı fiyatlandırma politikasıyla karşı karşıya bırakılmaması amacıyla alınan bir tedbir olduğu anlaşılmaktadır. Yukarıda belirtilen nedenlerle, meslek kuruluşlarının ücret tarifelerinin yürürlüğe girebilmesinin, bir idari vesayet yetkisi olarak merkezî idarenin tasdik etmesine bağlı kılınmasında Anayasa'ya aykırılık söz konusu değildir.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 135. maddesine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 2. maddesiyle bir ilgisi görülmemiştir.

6- KHK'nin 8. Maddesinin (1) Numaralı Fıkrasının (e) Bendinde Yer Alan "politika ve düzenlemelerine" ve "gerekli" İbareleri

Dava dilekçesinde, dava konusu kurallarla, konunun muhataplarının sadece mevzuata değil bakanlık politika ve düzenlemelerine de uygun hareket etmek durumunda bırakıldıkları ve bunlara aykırılık halinde ise niteliği önceden bilinmeyen 'gerekli' yaptırımlara tabi tutulmalarına olanak sağlandığı belirtilerek kuralların, Anayasa'nın 2. ve 38. maddelerine aykırı olduğu ileri sürülmüştür.

KHK'nin 8. maddesinin (1) numaralı fıkrasının dava konusu ibareleri de içeren (e) bendinde, Sağlık Hizmetleri Genel Müdürlüğüne, sağlık kurum ve kuruluşlarının mevzuata, Bakanlık politika ve düzenlemelerine uyumunu denetleme, gerekli yaptırımları uygulama görev ve yetkisi verilmiştir.

Anayasa'nın 38. maddesinin ilk fıkrasında, 'Kimse, ... kanunun suç saymadığı bir fiilden dolayı cezalandırılmaz' denilerek 'suçun kanuniliği', üçüncü fıkrasında da 'Ceza ve ceza yerine geçen

güvenlik tedbirleri ancak kanunla konular' denilerek 'cezanın kanuniliği' ilkesi kabul edilmiştir. Anayasa'da öngörülen suçta ve cezada kanunilik ilkesi, insan hak ve özgürlüklerini esas alan bir anlayışın öne çıktığı günümüzde, ceza hukukunun da temel ilkelerinden birini oluşturmaktadır.

Dava konusu kuralda sözü edilen Bakanlık politikaları, kanunlara ve idari düzenlemelere yansımış politikalar olup mevzuatta öngörülenler dışında Bakanlığın sağlık kurum ve kuruluşlarına yükümlülük getirmesi mümkün değildir. Aynı şekilde 'gerekli' yaptırımlardan da ancak önceden usulüne göre yürürlüğe konulmuş yasal ve idari düzenlemelerde yer alan yaptırımların anlaşılması gerektiği izahtan varestedir. Dolayısıyla 'gerekli' sözcüğü ile yeni bir suç, ceza veya bir idari yaptırımın vazedilmesi veya bu alanda bir belirsizliğin yaratılmış olması söz konusu değildir.

Açıklanan nedenlerle, dava konusu kurallar Anayasa'nın 2. ve 38. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir.

7- KHK'nin 8. Maddesinin (1) Numaralı Fıkrasının (g) Bendi

Dava dilekçesinde, dava konusu kuralla, hukuki sorunların çözümünde idareye bir tür yargısal yetki kullanma imkânının tanındığı, fakat bu yetkinin nasıl, hangi kapsamda, hangi niteliklere sahip kişiler tarafından ve ne tür sonuçlar doğuracak biçimde kullanılacağı belirlenmediği, yargılama öncesi uyuşmazlık çözüm yöntemlerinin tercihe bağlı olması gerektiği halde dava konusu kuralda yetkinin kesin olarak düzenlenmesi nedeniyle zorunlu hale gelmiş olduğu, bu durumun hukuk devleti ilkesi ile yargı yetkisinin bağımsız mahkemelerce kullanılmasını öngören anayasal ilkelere uygun düşmediği belirtilerek kuralın, Anayasa'nın 2., 7., 9., 36. ve 138. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralla, Sağlık Hizmetleri Genel Müdürlüğüne, sağlık kurum ve kuruluşları ile hizmetten faydalananlar arasında doğabilecek ihtilafların çözümüne yönelik usulleri belirleme görev ve yetkisi verilmiştir.

Anayasa'nın 36. maddesinde, hak arama özgürlüğü güvence altına alınmıştır. Hak arama özgürlüğünün temel unsurlarından biri de mahkemeye erişim hakkıdır. Mahkemeye erişim hakkı, hukuki bir uyuşmazlığın bu konuda karar verme yetkisine sahip bir mahkeme önüne götürülmesi hakkını da kapsar.

Dava konusu düzenleme ile konuyla ilgili somut bir ihtilaf çözme yöntemi belirlenmemiş ve yargı denetimini engelleyen bir ibareye de yer verilmemiştir. Düzenleme, münhasıran, söz konusu alanda ihtilafların çözümüne yönelik usullerin hangi birim tarafından belirleneceği ile ilgilidir. Bakanlığın

belirleyeceği usulün zorunlu tutulması söz konusu olmadığı gibi, yargı yoluna başvurulmasına da engel teşkil etmemektedir.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 36. maddesine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 2., 7., 9. ve 138. maddeleriyle ilgisi görülmemiştir.

8- KHK'nin 8. Maddesinin (1) Numaralı Fıkrasının (ğ) Bendi

Dava dilekçesinde, dava konusu kuralla, insan sağlığına zarar vermediği ve yararlılığı bilimsel olarak kanıtlanmamış, ticari amaçlarla insanların umutlarının sömürülmesine dayalı bilim dışı uygulamaların yasallaştırılmasının söz konusu olduğu, ayrıca dava konusu kuralda yer alan 'sağlık beyanı' kavramının tanımının yapılmadığı, bunun ne anlama geldiğinin belli olmadığı, kanun koyucunun sağlık beyanı kavramı ile ilgili hiçbir açıklama yapmadan ve ölçüt getirmeden kavramın içeriğini belirleme yetkisini idareye bıraktığı, bu durumun ise kanuni düzenlemelerin öngörülebilir ve belirlenebilir nitelikte olması bakımından hukuk devleti ilkesi ile bağdaşmadığı belirtilerek kuralın, Anayasanın 2., 5., 17. ve 56. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralla, Sağlık Hizmetleri Genel Müdürlüğüne, geleneksel, tamamlayıcı ve alternatif tıp uygulamaları ile ilgili düzenleme yapma ve sağlık beyanı ile ilgili yapılacak her türlü uygulamalara izin verme ve denetleme, düzenleme ve izinlere aykırı faaliyetleri ve tanıtımları durdurma görev ve yetkisi verilmiştir.

Anayasa'nın 5., 17. ve 56. maddeleriyle kişilere, yaşama, maddi ve manevi varlığını koruma ve geliştirme ve hayatını beden ve ruh sağlığı içinde sürdürebilme hakkı tanınmış ve devlete de, herkesin maddi ve manevi varlığını geliştirmesi için gerekli şartları hazırlama, kişilerin hayatını, beden ve ruh sağlığı içinde sürdürmesini sağlama görevi verilmiştir. Kişilerin maddi ve manevi varlıklarını geliştirilebilmelerinin, mutlu ve huzurlu olabilmelerinin başlıca şartı, ihtiyaç duydukları anda sağlık hizmetlerine ulaşım ihtiyacı duydukları oranda bu hizmetlerden yararlanabilmeleridir. Devlet için bir görev ve kişiler için de bir hak olan bu amacın gerçekleştirilmesinde, bu haktan yararlanmayı zorlaştırıcı ya da zayıflatıcı düzenlemeler Anayasa'ya aykırı düşer.

Dava konusu düzenlemenin, geleneksel, tamamlayıcı ve alternatif tıp uygulamalarının tıp biliminin ışığı altında disipline edilmesi, sağlık ve yaşam hakkının korunması, hastaların zor durumlarından faydalanılarak sömürülmelerinin engellenmesi amacıyla bu husustaki boşluğu doldurmak üzere getirildiği anlaşılmış olup, kuralla bilim dışı uygulamaların yasallaştırılması söz konusu değildir.

Sağlık beyanı ile satışa sunulan ürün, ilaç niteliğinde olmayan ancak, piyasada, çeşitli hastalıklara veya genel olarak sağlığa faydalı olduğu ileri sürülerek tanıtımı ve satışı yapılan ürünler olup, dava konusu kuralla bu tür uygulamalara izin verme, bunları denetleme, düzenleme ve izinlere aykırı faaliyetleri ve tanıtımları durdurma görev ve yetkisi Sağlık Hizmetleri Genel Müdürlüğüne verilmiştir. Birey sağlığı üzerinde ciddi sonuçlar doğurabilecek bu tür ürünlerin tanıtımı ve satışının Bakanlığın izin ve denetimine bağlanması, devletin, bireyin beden ve ruh sağlığının korunmasını sağlayıcı tedbirler alma yükümlülüğünün bir gereğidir.

Anayasa'nın 2. maddesinde yer alan hukuk devletinin önemli bir unsuru olan belirlilik ilkesi, bireylerin hukuk kurallarını önceden bilmeleri, davranış ve tutumlarını bu kurallara göre güvenle düzene sokabilmelerini gerektirmekte olup, hukuk kurallarının belirliliğinin sağlanması yalnızca kanunla düzenleme yapılması anlamına gelmemektedir. Önceden uygun araçlarla duyurulmak kaydıyla idari düzenleyici işlemlerle de hukuk kuralları belirli kılınabilir. Özellikle idari ve teknik meselelerde, kamu hizmetlerinin değişen toplumsal ihtiyaçlara süratli bir biçimde uyarlanabilmesi için bu konudaki düzenleme yetkisinin yürütme organına bırakılması zorunludur. Bu itibarla, sağlık beyanının tıp tekniğini ilgilendirmesi nedeniyle bu konudaki usul ve esasların idari düzenleyici işlemlerle belirlenmesinde, hukuk devleti ilkesine aykırılık söz konusu değildir.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 5., 17. ve 56. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

9- KHK'nin 8. Maddesinin (1) Numaralı Fıkrasının (i) Bendi

Dava dilekçesinde, Sağlık Bakanlığının diğer ülkelerin vatandaşlarının ülkemizde sağlık hizmetlerine erişmesine yönelik görev üstlenmesinin, Anayasa'nın 5., 123. ve 126. maddelerine aykırı olduğu ileri sürülmüştür.

6216 sayılı Kanun'un 43. maddesine göre, ilgisi nedeniyle dava konusu kural, Anayasa'nın 56. maddesi yönünden de incelenmiştir.

Dava konusu kuralla, Sağlık Hizmetleri Genel Müdürlüğüne, sağlık turizmi uygulamalarının geliştirilmesine yönelik düzenlemeler yapma ve ilgili kurumlarla koordinasyon sağlama görev ve yetkisi verilmiştir.

Anayasa'nın 'Sağlık hizmetleri ve çevrenin korunması' kenar başlığını taşıyan 56. maddesinde, 'Herkes, sağlıklı ve dengeli bir çevrede yaşama hakkına sahiptir. ' Devlet, herkesin hayatını, beden ve ruh sağlığı içinde sürdürmesini sağlamak ' amacıyla sağlık kuruluşlarını tek elden planlayıp hizmet vermesini düzenler' hükmü yer almaktadır. Maddede bu hakkın öznesi olarak 'herkes' gösterilmiş,

bu hak, Türk vatandaşlarına özgülenmemiştir. Anayasa'da yer alan bu düzenlemeye paralel olarak KHK'nin 2. maddesinde, 'Bakanlığın görevi; herkesin bedenî, zihnî ve sosyal bakımdan tam bir iyilik hâli içinde hayatını sürdürmesini sağlamaktır' ifadesine yer verilmiştir. Bu itibarla, devletin, sadece Türk vatandaşlarının değil, Türkiye'ye sağlık hizmeti için gelen yabancıların da sağlık hizmetlerine erişimini düzenlemesi ve bunu bir kamu hizmeti olarak üstlenmesinde Anayasa'ya aykırı bir yönü bulunmamaktadır.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 56. maddesine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 5., 123. ve 126. maddeleriyle ilgisi görülmemiştir.

10- KHK'nin 8. Maddesinin (1) Numaralı Fıkrasının (k) Bendi

Dava dilekçesinde, dava konusu kuralla, üniversitelerin tıp fakültelerince de verilen uzmanlık eğitiminde Sağlık Bakanlığının tek düzenleyici kurum olarak belirlendiği, bu durumun Sağlık Bakanlığının yükseköğretim kurumlarına müdahalede bulunması anlamına geldiği belirtilerek kuralın, Anayasa'nın 2., 130. ve 131. maddelerine aykırı olduğu ileri sürülmüştür.

6216 sayılı Kanun'un 43. maddesine göre, ilgisi nedeniyle dava konusu kural, Anayasa'nın 56. maddesi yönünden de incelenmiştir.

Dava konusu kuralla, Sağlık Hizmetleri Genel Müdürlüğüne tıpta uzmanlık eğitimi ile ilgili iş ve işlemleri yürütme görev ve yetkisi verilmiştir.

Anayasa'nın 56. maddesinin üçüncü fıkrasında, 'Devlet, herkesin hayatını, beden ve ruh sağlığı içinde sürdürmesini sağlamak; insan ve madde gücünde tasarruf ve verimi artırarak, işbirliğini gerçekleştirmek amacıyla sağlık kuruluşlarını tek elden planlayıp hizmet vermesini düzenler.' denilerek, devletin sağlık kuruluşlarını tek elden planlayıp hizmet vermesini düzenleyeceği açıkça belirtilmiştir. Buna göre, sağlık hizmetlerinde asli bir unsur olan hekimlerin tıpta uzmanlıklarının sağlanması hususunun da Anayasa'nın 56. maddesiyle devlete sağlık hizmetlerine dair verilen görevler kapsamında olduğu açıktır.

Anayasa'nın 131. maddesinin birinci fıkrasında, 'Yükseköğretim kurumlarının öğretimini planlamak, düzenlemek, yönetmek, denetlemek, yükseköğretim kurumlarındaki eğitim-öğretim ve bilimsel araştırma faaliyetlerini yönlendirmek, bu kurumların kanunda belirtilen amaç ve ilkeler doğrultusunda kurulmasını, geliştirilmesini ve üniversitelere tahsis edilen kaynakların etkili bir biçimde kullanılmasını sağlamak ve öğretim elemanlarının yetiştirilmesi için planlama yapmak maksadı ile Yükseköğretim Kurulu kurulur.' denilmiştir.

4.11.1981 günlü, 2547 sayılı Yükseköğretim Kanunu'nun 3. maddesinin (t) bendinde 'Lisans Üstü: Yüksek lisans, doktora, tıpta uzmanlık ve sanatta yeterlik eğitimini kapsar ve aşağıdaki kademelere ayrılır.' denildikten sonra (t) bendinin (3) numaralı alt bendinde tıpta uzmanlık, 'Sağlık ve Sosyal Yardım Bakanlığı tarafından düzenlenen esaslara göre yürütülen ve tıp doktorlarına belirli alanlarda özel yetenek ve yetki sağlamayı amaçlayan bir yükseköğretimdir.' şeklinde tanımlanmıştır. 2547 sayılı Kanun'un 3. maddesinde, 'Sağlık Bakanlığı tarafından düzenlenen esaslara göre yürütülme' tıpta uzmanlığın temel bir özelliği olarak vurgulanmıştır.

Yükseköğretim Kurumunun (YÖK) görevlerini belirleyen Anayasa'nın 131. maddesinde tıpta uzmanlık eğitimi ile ilgili iş ve işlemleri yürütme görevinin YÖK'e verilmesini zorunlu kılan hüküm bulunmadığı gibi bu görevin Sağlık Bakanlığına verilmesi diğer ilgili mevzuatta yer alan hükümlerle de uyumludur.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 56. ve 131. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 2. ve 130. maddeleriyle ilgisi görülmemiştir.

11- KHK'nin 8. Maddesinin (1) Numaralı Fıkrasının (n) Bendinde Yer Alan "sertifikalı eğitim", "ve benzeri eğitimleri" ile "kredilendirme," İbareleri

Dava dilekçesinde, dava konusu kuralla, özel olarak yükseköğretim, mesleki yetkilendirme ve yetkiye dayalı faaliyette bulunma, genel olarak da çalışma hakkı ile son derece yakından ilgili bir alanda Sağlık Bakanlığına tek başına düzenleme yapma ve bu eğitimlerin içeriğini, kapsamını belirleme ve eğitimleri verecek kişi ve kurumları saptama, eğitimleri kredilendirme, izleme ve denetleme yetkisi verilmesinin, hukuk devleti ve yasama yetkisinin devredilmezliği ilkeleri ile yükseköğretime ve kamu kurumu niteliğindeki meslek kuruluşlarının görev ve yetkilerine ilişkin anayasal düzenlemelerle çeliştiği belirtilerek kuralın, Anayasa'nın 2., 7., 130. ve 135. maddelerine aykırı olduğu ileri sürülmüştür.

KHK'nin 8. maddesinin (1) numaralı fıkrasının dava konusu ibareleri de içeren (n) bendinde, Sağlık Hizmetleri Genel Müdürlüğüne, sağlık meslek mensuplarının uyum, hizmet içi eğitim, sertifikalı eğitim, görevde yükselme ve unvan değişikliği eğitimleri ve benzeri eğitimleri ile ilgili düzenlemeleri yapma, koordine etme, kredilendirme, izleme ve denetimini sağlama görev ve yetkisi verilmiştir.

Dava dilekçesinde dava konusu kuralla ilişkin iptal gerekçesinin özü, sağlık meslekleri mensuplarının eğitimleri konusunda Sağlık Bakanlığı'na yetki ve görev verilmesinin Anayasaya uygun düşmediği,

bu alanda öncelikle Yükseköğretim Kurulu ve üniversiteler ile TTB ve diğer meslek kuruluşlarının yetkili ve görevli olmaları gerektiği yolundadır.

KHK'nin 8. maddesinin (1) numaralı fıkrasının (k) bendi için açıklanan gerekçelerle, dava konusu kural Anayasa'nın 131. maddesine aykırı değildir.

Meslek kuruluşlarının özerkliği, merkezi idareden bağımsız olarak karar ve yürütme organlarını seçebilme, ilgili meslekî faaliyetlerle sınırlı olmak üzere üyelerini ve örgütlerini bağlayıcı karar alma ve uygulama, meslek mensuplarının uyacağı ilke ve kuralları belirleme ve üyeleri hakkında disiplin tedbirleri uygulama hak ve yetkisini içermektedir. Sağlık meslek mensuplarına sertifikalı eğitim ve benzeri diğer eğitimlerin verilmesi ile bu eğitimlerin kredilendirilmesi, meslek kuruluşlarına tanınan özerk alan kapsamına giren bir görev olmadığından bu görevin Sağlık Hizmetleri Genel Müdürlüğüne verilmesinde Anayasa'ya aykırı bir yön bulunmamaktadır.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 131. ve 135. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın Anayasa'nın 2. ve 7. maddeleriyle ilgisi görülmemiştir.

12- KHK'nin 8. Maddesinin (1) Numaralı Fıkrasının (o) Bendi

Dava dilekçesinde, üst başlıkta incelenen (n) bendinde yer alan "sertifikalı eğitim", "ve benzeri eğitimleri" ile "kredilendirme," ibareleri ile ilgili Anayasa'ya aykırılık gerekçelerine atıf yapılarak kuralın, Anayasa'nın 2., 7., 130. ve 135. maddelerine aykırı olduğu ileri sürülmüştür.

6216 sayılı Kanun'un 43. maddesine göre, ilgisi nedeniyle dava konusu kural, Anayasa'nın 131. maddesi yönünden de incelenmiştir.

Dava konusu kuralla, Sağlık Hizmetleri Genel Müdürlüğüne ilgili kuruluşlarla işbirliği yaparak sağlık mesleklerinin standartlarını belirleme, eğitim müfredatlarının kanıta dayalı olarak güncellenmesini ve geliştirilmesini sağlama, sağlık meslek mensuplarının sertifikasyonu ile ilgili işleri yapma veya yaptırma görev ve yetkisi verilmiştir.

KHK'nin 8. maddesinin (1) numaralı fıkrasının (n) bendinde yer alan "sertifikalı eğitim", "ve benzeri eğitimleri" ile "kredilendirme," ibareleri için açıklanan gerekçelerle dava konusu kural, Anayasa'nın 131. ve 135. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 2., 7. ve 130. maddeleriyle ilgisi görülmemiştir.

13- KHK'nin 13. Maddesinin (1) Numaralı Fıkrasının (e) Bendi

Dava dilekçesinde, sağlık tesislerinin kurulup işletilmesinde kamu özel ortaklığı modelinin de uygulanabileceği yönünde bir düzenlemenin temel esaslarının belirtilmediği ve bu durumun, Anayasa'nın 2., 5., 7., 10., 17., 47., 55., 56. ve 128. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralla, Sağlık Yatırımları Genel Müdürlüğüne, Bakanlığın ve bağlı kuruluşların ihtiyacı olan tesislerin yapımını ve mevcut tesislerin yenilenmesini kamu özel ortaklığı modeli veya diğer usuller ile gerçekleştirme görevi verilmiştir.

Anayasa'nın 128. maddesinin birinci fıkrasında, 'Devletin, kamu iktisadî teşebbüsleri ve diğer kamu tüzelkişilerinin genel idare esaslarına göre yürütmekle yükümlü oldukları kamu hizmetlerinin gerektirdiği aslî ve sürekli görevler, memurlar ve diğer kamu görevlileri eliyle görülür...' denilmektedir. Bu hüküm uyarınca, kamu hukuku kurallarına göre yürütülen kamu hizmetlerinin gerektirdiği görevlerden asli ve sürekli nitelik taşıyanların, memurlar ve diğer kamu görevlileri eliyle görülmesi zorunludur.

Anayasa'nın 47. maddesinin son fıkrasında, 'Devlet, kamu iktisadi teşebbüsleri ve diğer kamu tüzel kişileri tarafından yürütülen yatırım ve hizmetlerden hangilerinin özel hukuk sözleşmeleri ile gerçek veya tüzel kişilere yaptırılabilmesi veya devredilebileceği kanunla belirlenir' denilerek kamu hizmetlerinin sunulmasında özel hukuk sözleşmeleriyle gerçek veya tüzel kişilerin hizmetin sunumuna dâhil edilmelerine imkân tanınmıştır.

Buna göre, idarelerin, genel idare esasları uyarınca yürütmekle yükümlü oldukları asli ve sürekli görevleri dışında kalan alanlardaki hizmetleri, özel hukuk sözleşmeleriyle özel kişilere gördürmeleri olanaklıdır. Anayasa'nın 47. maddesinde, bu sözleşmelerin hukuki niteliğine ilişkin herhangi bir sınırlama yapılmamıştır. Dolayısıyla, kamu hizmetlerinin ne tür özel hukuk sözleşmeleriyle özel kişilere gördürüleceğinin belirlenmesi kanun koyucunun takdirindedir. Bununla birlikte, özel hukuk sözleşmeleriyle yürütülecek yatırım ve hizmetlerin neler olduğunun kanunla belirlenmesi zorunludur.

Dava konusu kuralla, Bakanlığın ve bağlı kuruluşların ihtiyacı olan tesislerin yapımının ve mevcut tesislerin yenilenmesinin kamu özel ortaklığı (KÖO) modeliyle gerçekleştirilmesine olanak tanınmıştır. KÖO modeli, özel sektörle kamu idaresi arasında, bir hizmetin tasarlanması, yapımı, kiralanması, ortaklık kurulması ve finansmanının sağlanması, işletilmesi gibi unsurların bileşiminden oluşan ve özel hukuk hükümlerine tabi sözleşmeler üzerinden uygulanan bir işbirliği modelidir. KÖO bir üst kavram olup, özel hukuk sözleşmeleri yoluyla yap-işlet-devret, yap-kirala, yap-işlet, işletme hakkı devri, tasarla-yap, yap-işlet-sahip ol-devret, tasarla-yap-finanse et-devret, ortaklık gibi birçok modelin birlikte veya ayrı ayrı uygulanmasına imkân vermektedir.

Türkiye'de, KÖO uygulamalarına ilişkin çerçeve bir kanun bulunmamakla birlikte 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun ek 7. maddesinde sağlık alanında KÖO modelinin uygulanmasına olanak tanıyan hükümler mevcuttur. Anılan madde uyarınca, yapılmasının gerekli olduğuna Yüksek Planlama Kurulu tarafından karar verilen sağlık tesislerinin, Sağlık Bakanlığınca verilecek ön proje ve belirlenecek temel standartlar çerçevesinde, kendisine veya Hazineye ait taşınmazlar üzerinde ihale ile belirlenecek gerçek veya özel hukuk tüzel kişilerine kırk dokuz yılı geçmemek şartıyla belirli süre ve bedel üzerinden kiralama karşılığı yaptırılması mümkündür. Bu amaçla Maliye Bakanlığınca, gerçek veya özel hukuk tüzel kişilerine Hazineye ait taşınmazlar bedelsiz devredilebilir. Bu şekilde yapılacak kiralama işlemlerine ait kira bedelleri Sağlık Bakanlığınca bağlı döner sermaye işletmelerince ödenir. Sağlık Bakanlığının kullanımında bulunan sağlık tesislerinin, öngörülecek proje ve belirlenecek esaslar doğrultusunda yenilenmesi; tesislerdeki tıbbi hizmet alanları dışındaki hizmet ve alanların işletilmesi karşılığında, sözleşmeyle gerçek veya özel hukuk tüzel kişilerine yaptırılabilir.

Dava konusu kuralda sözü edilen 'kamu özel ortaklığı' modelinin, kapsamının ve çerçevesinin 3359 sayılı Kanun'un ek 7. maddesinde belirlendiği, kuralla Sağlık Yatırımları Genel Müdürlüğüne verilen görevin ise anılan maddeyle Sağlık Bakanlığınca tanınan yetkilerin kullanılmasından ibaret olduğu anlaşılmaktadır. Dolayısıyla kuralda, belirsizlik ve yasama yetkisinin devredilmezliği ilkesine aykırılık söz konusu değildir.

Bakanlığın ve bağlı kuruluşların ihtiyacı olan tesislerin yapımı ve mevcut tesislerin yenilenmesine ilişkin hizmetlerin KÖO modeliyle gerçekleştirileceği belirtilmek suretiyle, hangi hizmetlerin özel hukuk sözleşmesiyle gördürüleceği kuralda açıkça belirlenmiştir. Söz konusu hizmetlerin kamu gücü kullanımını gerektiren ve icrai yetkiler içeren görevlerden olmadığı da açıktır. Anayasa'nın 47. maddesinde, bu sözleşmelerin hukuki niteliğine ilişkin herhangi bir sınırlama olmadığından, bu hizmetlerin KÖO modeliyle gördürülmesinde Anayasa'ya aykırı bir yön bulunmamaktadır.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 7., 47. ve 128. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, 5., 10., 17., 55. ve 56. maddeleriyle ilgisi görülmemiştir.

14- KHK'nin 21. Maddesi

Dava dilekçesinde, Yüksek Sağlık Şûrası üyeliğine seçilecek kişilerde aranacak niteliklerin belirgin olmadığı, Şûra bünyesinde, sağlık mesleklerinin her birinden yeterli sayıda uzmana yer verilmediği, çeşitli uzmanlık alanlarında çalışan kişilerin mesleklerini icra ederken hatalı tıbbi uygulamalar yapıp

yapmadıkları konusunda karar verme yetkisine sahip olan Şûranın oluşumunun, işlevine uygun olmadığı, düzenlemenin adil yargılanma hakkını zedeleyen bir içeriğe sahip olduğu belirtilerek kuralın, Anayasanın 2., 36., 123., 126. ve 138. maddelerine aykırı olduğu ileri sürülmüştür.

KHK'nin 21. maddesinde, Yüksek Sağlık Şûrasının oluşumu, görev ve yetkileri ile çalışma usulleri düzenlenmektedir. Buna göre, Yüksek Sağlık Şûrası, sağlık meslek mensuplarının mesleklerini icra ederken ortaya çıkan adli konularda mahkemelere görüş vermek ve idari soruşturmacılar ve uzlaşma komisyonları için bilirkişi listesi belirlemekle görevli olup on beş üyeden oluşmaktadır. Üyelerin on üçü Bakan tarafından ülkede sağlık hizmetleri veya eserleri ile tanınmış kişiler arasından seçilecektir. Müsteşar ve I. Hukuk Müşaviri ise Şûranın doğal üyesidir. Şûraya bağlı olarak danışma kurulları ve sağlık mesleklerinin icrasından doğan adli konularda dosyaları inceleyip Şûraya sunmak üzere ihtisas komisyonları kurulması öngörülmüştür.

Dava konusu kuralla, Bakan tarafından seçim yoluyla Yüksek Sağlık Şûrası üyeliği görevine getirilecek on üç üyenin ülkede sağlık hizmetleri veya eserleri ile tanınmış olması gerektiği öngörülerek bu kişilerde aranacak niteliklerin çerçevesi makul ölçüde belirlenmiştir. Ayrıca üyelik görevinin de iki yıla sınırlandırıldığı görülmektedir. Söz konusu kurul ve komisyonların oluşumu ve buralarda görev alabilecek kişilerin nitelikleri konusunda kuralda ayrıntılı hükümlere yer verilmemiş ise de uzmanlık ve idare tekniğine ilişkin olan diğer hususların idarenin düzenleyici işlemleriyle belirlenecek olmasının hukuk devleti ilkesine aykırı bir yönü bulunmamaktadır.

Anayasa'nın hak arama hürriyetini düzenleyen 36. maddesinin birinci fıkrasında, 'Herkes, meşru vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir.' denilmiştir.

Sağlık meslek mensuplarının mesleklerini icra ederken ortaya çıkan adli konularda talep halinde bilirkişilik görevini yapmak ve yargı yetkisi bulunmayan idari soruşturmacılar ve uzlaşma komisyonlarınca yürütülen işler için somut olayın özelliğine göre doğru bilirkişilerin kimler olduğunu göstermek üzere bilirkişi listeleri hazırlamakla görevli olan Yüksek Sağlık Şûrasının on üç üyesinin ülkede sağlık hizmetleri veya eserleri ile tanınmış kişiler arasından seçilmesi öngörülmüştür. Ayrıca, Şûraya yardımcı olmak üzere danışma kurulları ve ihtisas komisyonlarının Şûraya bağlı olarak çalışmalarını olanaklı hale getirilmiştir. Bütün bunlar gözetildiğinde, Şûranın oluşumu ve yapısının, mahkemeye sunulacak bilirkişi raporlarının somut olayın niteliğine uygun düşen uzmanlarca hazırlanmasına olanak sağlayacak şekilde belirlendiği ve bu haliyle adil yargılamanın gerçekleşmesine katkı sağlayacak nitelikte olduğu anlaşılmaktadır. Kaldı ki, Şûranın görüşü mahkemeyi bağlayıcı olmayıp takdiri delil niteliğindedir.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2. ve 36. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 123., 126. ve 138. maddeleriyle ilgisi görülmemiştir.

15- KHK'nin 23. Maddesinin (7) Numaralı Fıkrasının (c) ve (ç) Bentleri Dışında Kalan Bölümü

Dava dilekçesinde, sağlık meslek mensuplarını mesleklerini icra etmekten geçici veya sürekli olarak men etmeye kadar varabilen önemli kararlar alma yetkisiyle donatılan Sağlık Meslekleri Kurulunda, sağlık meslekleriyle ilgisi olmayan Milli Eğitim Bakanlığı temsilcisine yer verildiği, Kurulda yer alacak YÖK temsilcilerinde aranacak niteliklerin gösterilmediği, Sağlık Bakanı tarafından seçilecek Kurulun beş üyesinin de çok çeşitli sağlık mesleklerinin mensuplarını ve farklı uzmanlık alanlarını temsil ehliyetine sahip olamayacakları, Kurul üyelerinin ağırlıklı olarak idare tarafından belirlenmesinin meslek örgütlerini işlevsiz kılacağı, kuralda, uygulanacak yaptırımlar tek tek belirlendiği halde hangi eylemlerin yaptırım gerektirdiğinin açık bir şekilde düzenlenmediği, suç ve cezaların yönetmelikle düzenlenmesine olanak tanındığı, düzenlemenin, sağlık meslek mensuplarının aynı eylemleri nedeniyle hem meslek kuruluşu hem de Bakanlık tarafından cezalandırılması sonucunu doğurduğu, ceza mahkemelerinin, suçun oluşmadığı gerekçesine dayanan beraat kararlarının disiplin soruşturmacılarını da bağlaması gerektiği halde kuralda aksine düzenlemeye yer verildiği, Kurulun, meslek mensubuna bir yıldan üç yıla kadar geçici men ve sürekli men cezası verebilmesinin ölçülü olmadığı, ayrıca meslek mensuplarının mesleki yeterlilik ve etik eğitimi ile hasta hakları eğitimine tabi tutulmasına ve eğitimlerin süresine ve müfredatına karar vermenin Yükseköğretim Kurumunun anayasal yetkisi kapsamında kaldığı belirtilerek kuralın, Anayasa'nın 2., 6., 7., 38., 123., 131. ve 135. maddelerine aykırı olduğu ileri sürülmüştür.

KHK'nin 23. maddesiyle, Sağlık Bakanlığı bünyesinde, sağlık mesleklerinde eğitim müfredatı, mesleki alan ve dal belirlemesi gibi mesleki düzenlemelerde ve istihdam planlamalarında görüş bildirmek, mesleki yeterlilik değerlendirmesi yapmak, mesleki müeyyide uygulamak, etik ilkeleri belirlemek ve uyumu denetlemek üzere 'Sağlık Meslekleri Kurulu' adıyla yeni bir idari birim teşkil edilmiştir. Maddede, bu Kurulun oluşumu, görev ve yetkileri, çalışma usulleri düzenlenmiştir. Kurulun, müsteşar veya görevlendireceği müsteşar yardımcısı ile Sağlık Hizmetleri Genel Müdürü veya görevlendireceği bir yetkili temsilci, I. Hukuk Müşaviri veya görevlendireceği hukuk müşaviri, Türkiye Halk Sağlığı Kurumu ve Türkiye Kamu Hastaneleri Kurumu Başkanları veya görevlendirecekleri yardımcıları, Bakan'ın seçeceği en az doktora seviyesinde eğitim almış beş ayrı sağlık meslek mensubu üye, en az genel müdür yardımcısı seviyesinde Milli Eğitim Bakanlığı temsilcisi bir üye, Yükseköğretim Kurulunun seçeceği iki üye, Mesleki Yeterlilik Kurumu temsilcisi

bir üye ve kanunla kurulan sağlık meslek birliklerinden birer üyeden oluşması öngörülmüştür. Sağlık meslek birliklerinin temsilcileri yalnızca kendi meslek mensupları ile ilgili konuların görüşüleceği toplantılara katılabilmekte ve kendi meslek alanları ile ilgili konularda oy kullanabilmektedirler.

Maddenin (6) numaralı fıkrasında, Kurulun görevleri sayılmıştır. Bu kapsamda, fıkranın (ç) bendiyle meslek mensuplarının mesleki yeterlilik ve etik eğitimi ile hasta hakları eğitimine tâbi tutulmasına ve eğitimlerin süresine ve müfredatına karar vermenin Kurulun görevleri arasında olduğu belirtilmiştir.

Maddenin (7) numaralı fıkrasında, sağlık meslek mensuplarına uygulanacak yaptırımlar düzenlenmiştir. Buna göre, Kurul, yeterlilik eğitimine tabi tutma, hasta hakları ve etik ilkeleri eğitim programına tabi tutma, geçici ve sürekli men cezaları gibi yaptırımlar uygulayabilecektir.

Maddenin (10) numaralı fıkrasına göre, aynı olaydan dolayı ilgili hakkında ceza takibatına veya disiplin soruşturmasına başlanmış olması bu maddeye göre işlem yapılmasını geciktirmez ve engellemez; ilgilinin mahkûm olması veya olmaması ile disiplin cezası verilmiş veya verilmemiş olması hâlleri, ayrıca mesleki müeyyide uygulanmasını etkilemez.

Kuralın (14) numaralı son fıkrasıyla, bu maddenin uygulanmasına ilişkin usul ve esasların Bakanlık tarafından çıkarılacak yönetmelikle düzenlenmesi öngörülmüştür.

Maddenin, geçici ve sürekli men cezalarını düzenleyen (7) numaralı fıkrasının (c) ve (ç) bentleri, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı bulunarak iptal edildiğinden bu fıkralara yönelik olarak öne sürülen Anayasa'ya aykırılık iddiaları incelenmemiştir.

Dava konusu kuralda, Sağlık Meslekleri Kurulunun kimlerden oluşacağı açıklanmıştır. İlgili kurumlardan gelen yönetici ve diğer temsilcilerin nitelikleri özel kanunlarında gösterilmiştir. Bakan tarafından seçilecek beş sağlık meslek mensubunun ise en az doktora seviyesinde eğitim almış olması gerektiği kuralda ifade edilmiştir. Kurulun oluşumu ve üyelerinin niteliklerinin genel çerçevesi bu şekilde belirlendikten sonra, idare tekniğine ilişkin usul ve esasların düzenlenmesinin yönetmeliğe bırakılmış olması, yasama yetkisinin devri sayılamayacağı gibi, hukuk devleti ilkesine de aykırılık oluşturmaz.

Öte yandan, sağlık mesleklerinde eğitimin planlanmasıyla ilgili kimi görevleri bulunan Kurulda Milli Eğitim Bakanlığının temsilcisine de yer verilmiş olması kanun koyucunun takdirindedir.

Dava dilekçesinde, ceza mahkemelerinin, suçun oluşmadığı gerekçesine dayanan beraat kararlarının disiplin soruşturmacılarını da bağlaması gerektiği halde (10) numaralı fıkrada aksine düzenlemeye yer verildiği ileri sürülmüştür. Ceza yaptırımı ile idari yaptırım, sebep, sonuç, hukuksal dayanak, amaç ve usul açılarından birbirinden farklıdır. Bu nedenle, aynı eylem için ceza yaptırımı

uygulanmasını gerektiren koşulların oluşup oluşmadığı ile idari yaptırım uygulanmasının şartlarının gerçekleşip gerçekleşmediğinin birbirinden bağımsız olarak değerlendirilmesi gerekmektedir. Bununla birlikte, maddi gerçeğin ortaya çıkarılmasını esas alan ceza yargılamasında hâkime tanınan yetkilerin genişliği gözetildiğinde, bir eylemin sabit olmadığı yolundaki ceza mahkemesi kararının, idari yaptırım uygulamaya yetkili makam tarafından da dikkate alınması, adalet ve hakkaniyete daha uygun düşmektedir. Dava konusu kuralda, idari yaptırım uygulamaya yetkili makamın, ceza mahkemesinin bu nitelikteki kararlarını dikkate almasını engelleyen herhangi bir düzenleme bulunmamaktadır.

Dava dilekçesinde, düzenlemenin, sağlık meslek mensuplarının aynı eylemleri nedeniyle hem meslek kuruluşu hem de Bakanlık tarafından cezalandırılması sonucunu doğurduğu ve ayrıca meslek kuruluşlarının görev alanına müdahale niteliği taşıdığı ileri sürülmüştür. Dava konusu 23. maddenin (11) numaralı fıkrasında 'Kanunla kurulmuş meslek odalarının ve birliklerinin kuruluş kanunlarındaki disiplin hükümleri saklıdır. Ancak fiilin her iki kanuna göre de müeyyide gerektirmesi hâlinde bu Kanun hükümleri uygulanır.' hükmüne yer verilerek kanunla kurulmuş meslek odalarının ve birliklerinin kuruluş kanunlarındaki disiplin hükümleri mahfuz tutulmuştur. Dolayısıyla mükerrer yaptırım uygulanması söz konusu değildir.

Diğer taraftan, dava konusu kuralla, sağlık meslek mensuplarının mesleki disiplin kurallarına aykırı eylemlerine değil, bireyin vücut bütünlüğünün ihlali sonucunu doğuran veya doğurma potansiyeli bulunan eylemlerine idari yaptırım uygulanmasının öngörüldüğü anlaşılmaktadır. Sağlık hizmetinden yararlananların vücut bütünlüğünün ihlaline yol açan eylemler nedeniyle meslek mensubuna idari tedbir uygulanması, meslek kuruluşlarına tanınan özerk alan kapsamında değerlendirilemez.

Dava dilekçesinde, (6) numaralı fıkranın (b) bendinde yer alan ve Sağlık Meslekleri Kuruluna sağlık mesleklerinin eğitim müfredatı hakkında görüş bildirme yetkisi veren düzenlemenin Anayasanın 131. maddesine aykırı olduğu ileri sürülmüştür. Dava konusu düzenlemede, Kurula 'sağlık mesleklerinin eğitim müfredatı hakkında görüş bildirmek' görev ve yetkisi verilmiştir. Görüş bildirme yetkisinin bağlayıcı karar alma yetkisine sahip olmak anlamına gelmediği açıktır. Anayasa'nın 56. maddesi uyarınca sağlık hizmeti sunmakla görevli olan Sağlık Bakanlığının hangi bilgi, beceri ve yetenekleri haiz sağlık meslek mensubuna ihtiyacı olduğuna dair önerilerde bulunabilmesi doğaldır.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 7., 38., 131. ve 135. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 6. ve 123. maddeleriyle ilgisi görülmemiştir.

16- KHK'nin 24. Maddesi

Dava dilekçesinde, dava konusu kuralla getirilen uzlaşma usulünde tarafsızlık ve bağımsızlık unsurlarının sağlanmadığı, uzlaşmanın yönteminin her bir taraf ve uzlaştırıcı yönünden ayrı ayrı ve tereddüt yaratmayacak bir biçimde belirlenmemiş olduğu, uzlaşma olsa da yargısal yollara başvuru hakkının bulunup bulunmadığının açık olmadığı, zorunlu sigortası olmayan sağlık personelinin uzlaşma sonunda zararı kendisinin karşılamak zorunda kalacağı, uzlaşma sürecinde idarenin kusurunun hiç tartışılmayacağı belirtilerek kuralın, Anayasa'nın 2., 9., 36. ve 138. maddelerine aykırı olduğu ileri sürülmüştür.

6216 sayılı Kanun'un 43. maddesi uyarınca, ilgisi nedeniyle dava konusu kural Anayasa'nın 141. maddesi yönünden de incelenmiştir.

KHK'nin 24. maddesi uzlaştırma prosedürünü düzenlemektedir. Buna göre, sağlık mesleklerinin uygulanmasından dolayı zarara uğradığını iddia edenlerin dava açma süresi içerisinde bu madde kapsamında yapacakları maddi ve manevi tazminat başvurularının Bakanlık tarafından kuralda öngörülen şekilde uzlaşma yoluyla halledilmesi öngörülmüştür. Tarafların, Bakanlığın uzlaşma davetini kabul etmeleri hâlinde, üzerinde anlaştıkları bir hukukçu uzlaştırıcı marifetiyle uzlaşma süreci başlatılır. Uzlaşmanın en fazla üç ayda sonuçlandırılması, ancak bu sürenin, bilirkişi görüşleri alınmadığı hallerde tarafların kabulü ile altı aya kadar uzatılabilmesi kurala bağlanmıştır. Uzlaşma müracaatının dava açma süresini durduracağı, uzlaşma sağlanamaması hâlinde taraflarca tanzim edilecek tutanak veya taraflardan birinin talebi üzerine Bakanlık tarafından taraflara tebliğ edilerek verilecek belge tarihinden itibaren dava açma süresinin yeniden işlemeye başlayacağı belirtilmiştir. Uzlaşmanın sağlanması durumunda ise uzlaşmanın konusunu, yerini, tarihini, yerine getirilmesi gereken hususları içeren uzlaşma tutanağının tanzim edilmesi ve bu tutanağın 9.6.1932 günlü, 2004 sayılı İcra ve İflas Kanunu'nun 38. maddesi anlamında ilam niteliğinde olması öngörülmüştür. Uzlaştırma masrafları ve arabulucu ücreti taraflarca karşılanacaktır. Uzlaşma neticesinde belli bir bedel üzerinde uzlaşma sağlandığında bu bedel doğrudan sigortacı, sigortasının bulunmaması durumunda ise ilgili personel tarafından ödenecektir.

Uzlaştırıcı, mesleki kusur bulunup bulunmadığı hususunda Yüksek Sağlık Şûrasının belirlediği bilirkişilerin; uğranıldığı iddia edilen zarar miktarının hesaplanmasında ise adli yargı adalet komisyonları tarafından her yıl düzenlenecek olan listelerde yer alan bilirkişilerin görüşüne başvurabilecektir.

Anayasa'nın 2. maddesinde belirtilen hukuk devleti eylem ve işlemleri hukuka uygun, insan haklarına saygılı, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adaletli bir hukuk düzeni kurup bunu geliştirerek sürdüren, Anayasa'ya aykırı durum ve tutumlardan kaçınan, Anayasa ve hukukun üstün kurallarıyla kendini bağlı sayan, yargı denetimine açık olan devlettir.

Anayasa'nın 9. maddesinde, yargı yetkisinin Türk Milleti adına bağımsız mahkemelerce kullanılacağı öngörülmüştür. Anayasa'nın hak arama hürriyetini düzenleyen 36. maddesinin birinci fıkrasında ise 'Herkes, meşru vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir.' denilmiştir.

Anayasa, Türkiye Cumhuriyeti'nin demokratik bir hukuk devleti olduğunu vurgularken, devlet içinde tüm kamusal yaşam ve yönetimin yargı denetimine bağlı olmasını amaçlamıştır. Yargı denetimi demokratik hukuk devletinin 'olmazsa olmaz' koşuludur. Kişinin uğradığı bir haksızlığa veya zarara karşı kendisini savunabilmesinin ya da maruz kaldığı haksız bir uygulama veya işleme karşı haklılığını ileri sürüp kanıtlayabilmesinin, zararını giderebilmesinin en etkili ve güvenceli yolu, yargı mercileri önünde dava hakkını kullanabilmesidir. Kişilere yargı mercileri önünde dava hakkı tanınması hak arama özgürlüğünün de bir gereğidir.

Anayasa'nın 141. maddesiyle de davaların en az giderle ve mümkün olan süratle sonuçlandırılması görevi yargıya verilmiştir. Bu görevin ağır iş yükü altında yerine getirilmesi zorlaştıkça, uyuşmazlıkların çözümü için alternatif yöntemlerin yaşama geçirilmesi, yargıya ilişkin anayasal kuralların etkililiğinin sağlanması bakımından gerekli görülebilir. Kanun koyucunun, taraflara görevli ve yetkili mahkemeye başvurmadan önce aralarındaki uyuşmazlığı kısa sürede çözmek üzere kanunla oluşturulan uzlaşma mekanizmalarına başvurma yükümlülüğü getirmesi, bu aşamadan sonra kararı benimsemeyen tarafa yargı yolunun açık tutulması, mekanizmanın oluşumunun ve çalışma yönteminin, uzmanlığın önemi de gözetilerek hukuk devleti ilkeleriyle uyum içinde düzenlenmesi koşuluyla Anayasa'ya aykırı olmaz.

Dava konusu kuralla, sağlık mesleklerinin uygulanmasından dolayı zarara uğradığını iddia edenlerin dava açma süresi içerisinde bu madde kapsamında yapacakları maddi ve manevi tazminat başvurularının, Bakanlık tarafından kuralda öngörülen şekilde uzlaşma yoluyla halledilmesi olanaklı kılınmakla birlikte, tarafların uzlaşma yoluna başvurmaları zorunlu tutulmadığı gibi, uzlaşma sonucu belirlenen tazminat tutarından tatmin olmayan tarafın yargı yoluna başvurması da engellenmemiştir. Öte yandan, uzlaşma görüşmelerinin, tarafların üzerinde uzlaşacağı ve hukukçu unvanını taşıyan bir uzlaştırıcının gözetiminde, ilgili tüm taraflar ile varsa sigorta şirketinin temsilcilerinin katılımıyla yapılması öngörülerek ve uzlaştırıcı hukukçunun, mesleki kusur bulunup

bulunmadığı hususunda Yüksek Sağlık Şûrasının belirlediği bilirkişilere, zarar miktarının hesaplanması hususunda ise adli yargı adalet komisyonları tarafından her yıl düzenlenecek olan listelerde yer alan bilirkişilerin görüşüne başvurması imkânı getirilerek, uzlaşma görüşmeleri sonucu adil ve hakkaniyete uygun bir karar verilmesinin hedeflendiği anlaşılmıştır.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 9., 36. ve 141. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 138. maddesiyle ilgisi görülmemiştir.

Erdal TERCAN bu görüşe katılmamıştır.

17- KHK'nin 26. ve 29. Maddeleri

Dava dilekçesinde, temel sağlık hizmetleri ile ikinci ve üçüncü basamak sağlık hizmetlerini vermek üzere iki ayrı bağlı kuruluş oluşturulduğu, bu kuruluşların sunacakları hizmetlerin bütünselliğini ve birbirini tamamlamasını sağlayacak yönetsel organizasyona ilişkin bir düzenleme yapılmadığı, bağımsız işleyişe sahip bağlı kuruluş modelinin sağlık hizmetlerinin bütünselliğine ve kamu yararına aykırı olduğu, Sağlık Bakanlığının bir tür düzenleyici kurula dönüştürülerek, kamu sağlık hizmetinin yürütülmesi görevinin, merkezî idareden adeta bağımsız hâle getirilen bağlı kuruluşlara devredilmesinin, Anayasa'nın 2., 6., 17., 56., 123. ve 126. maddelerine aykırı olduğu ileri sürülmüştür.

KHK'nin 26. maddesiyle, tüm birinci basamak koruyucu ve tedavi edici sağlık hizmetlerini sunmak üzere, Bakanlığa bağlı Türkiye Halk Sağlığı Kurumu kurulmuş ve bu Kurumun görev, yetki ve sorumlulukları düzenlenmiştir.

KHK'nin 29. maddesiyle de ikinci ve üçüncü basamak sağlık hizmetlerini vermek üzere hastanelerin, ağız ve diş sağlığı merkezlerinin ve benzeri sağlık kuruluşlarının açılması, işletilmesi, faaliyetlerinin izlenmesi, değerlendirilmesi ve denetlenmesi, bu hastanelerde her türlü koruyucu, teşhis, tedavi ve rehabilite edici sağlık hizmetlerinin verilmesini sağlamakla görevli ve Bakanlığa bağlı Türkiye Kamu Hastaneleri Kurumu kurulmuş ve bu Kurumun görev, yetki ve sorumlulukları düzenlenmiştir.

Anayasa'nın 56. maddesinde, 'Devlet, herkesin hayatını, beden ve ruh sağlığı içinde sürdürmesini sağlamak; insan ve madde gücünde tasarruf ve verimi artırarak, işbirliğini gerçekleştirmek amacıyla sağlık kuruluşlarını tek elden planlayıp hizmet vermesini düzenler. Devlet, bu görevini kamu ve özel kesimlerdeki sağlık ve sosyal kurumlarından yararlanarak, onları denetleyerek yerine getirir.' hükmü yer almaktadır. Buna göre, devletin görevi sağlık kuruluşlarını tek elden planlayıp hizmet vermesini sağlamak ve bu kurumları denetlemektir.

Kamu hizmetlerinin, hizmetin nitelik ve özelliği ile ihtiyaçlar dikkate alınarak, Bakanlık merkez teşkilatında ana hizmet birimleri ya da bağlı kuruluşlarca sunulmasının öngörülmesi kanun koyucunun takdirindedir. Dava konusu kurallarda yer alan bağlı kuruluşlar, Bakanlık ve merkezî idare dışında değildir. Bağlı kuruluş modelinin tercih edilmesinde idarenin bütünlüğü ilkesine aykırı bir yön de bulunmamaktadır. Öte yandan, bu kuruluşlar arasındaki koordinasyonu sağlama görevi merkezde Bakanlık merkez teşkilatına, taşrada ise il sağlık müdürlüklerine verilerek hizmetlerin bir bütünlük ve uyum içinde yürütülmesinin amaçlandığı anlaşılmaktadır.

Açıklanan nedenlerle, dava konusu kurallar Anayasa'nın 56. maddesine aykırı değildir. İptal istemlerinin reddi gerekir.

Kuralların, Anayasa'nın 2., 6., 17., 123. ve 126. maddeleriyle ilgisi görülmemiştir.

18- KHK'nin 27. Maddesinin (2) Numaralı Fıkrasının (b) Bendi

Dava dilekçesinde, dava konusu kuralda yer alan, içeriği ve kapsamı tanımlanmamış olan 'sağlık beyanı' kavramı yoluyla kimi ilaç, ürün ve tıbbi cihazların ruhsat koşulları aranmadan satışına olanak tanındığı, kuralla gerek 'sağlık beyanı' kapsamında değerlendirilen ürünlerin gerekse diğer ilaç, tıbbi cihaz ve ürünlerin reklamına izin verildiği, ilaç reklamına izin verilmesinin kişi ve toplum sağlığı bakımından yaratacağı sakıncalar nedeniyle kuralın, Anayasa'nın 2., 17., 56. ve 138. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralla, Türkiye İlaç ve Tıbbî Cihaz Kurumuna, sağlık beyanı ile satışa sunulacak ürünlerin sağlık beyanlarını inceleyerek bu beyanlara izin verme, izinsiz veya gerçeğe aykırı sağlık beyanı ile yapılan satışları denetleme, gerektiğinde durdurma, toplama, toplatma ve imha iş ve işlemlerini yapma veya yaptırma, izin ve sağlık beyanları yönünden bunların her türlü reklam ve tanıtımlarını denetleme ve aykırı olanları durdurma, piyasaya arz edilen ilaç, tıbbi cihaz ve ürünlerin reklam ve tanıtımının usul ve esaslarını belirleme ve uygulamasını denetleme görev ve yetkisi verilmiştir.

1262 sayılı İspençiyari ve Tıbbi Müstahzarlar Kanunu'nun 13. maddesi uyarınca reçeteli-reçetesiz ayrımı yapılmaksızın hiçbir ilacın reklamının yapılamayacağı hükme bağlanmış olup dava konusu kuralla, anılan hükme dokunulmadığı gibi ilaç reklamına izin verilmesi de söz konusu değildir.

Dava konusu kuralın amacının, ilaç niteliğinde olmayan ancak, piyasada, çeşitli hastalıklara veya genel olarak sağlığa faydalı olduğu ileri sürülerek tanıtımı ve satışı yapılan ürünlere ilişkin sağlık beyanlarının, doğruluk yönünden Kurumun denetimine tabi kılınması ve gerçeği yansıtması şartıyla bu yoldaki beyanlara izin verilmesinin sağlanması olduğu anlaşılmaktadır. Bu kapsamda Kuruma

verilen görev, bu ürünlerin satışına izin vermek olmayıp bunlarla ilgili sağlık beyanlarına izin verilmesidir. İlaç niteliğinde olmayan bu ürünlerin satışına izin verilmesi ve ruhsata bağlanması, ilgili mevzuat uyarınca diğer kurum ve kuruluşlara ait bir görev ve yetkidir. Sağlık beyanıyla satışa sunulan ürünlerin genel olarak halk sağlığı açısından sakınca teşkil etmesi durumunda, sorumlu kurum ve kuruluşlar tarafından gereken tedbirlerin alınacağı tabiidir.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 17. ve 56. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 2. ve 138. maddeleriyle ilgisi görülmemiştir.

19- KHK'nin 27. Maddesinin (2) Numaralı Fıkrasının (d) Bendi

Dava dilekçesinde, sosyal devlet ilkesinin gereği olarak özellikle dezavantajlı kesimlerin, yoksulların sağlık hizmetine erişebilmesi konusunda devletin pozitif yükümlülüklerinin bulunduğu, ilaç, tıbbi cihaz ve ürünlerin fiyatlarının toplumun erişebileceği şekilde belirlenmesi konusunda devletin sorumluluk üstlenmesi gerektiği halde dava konusu kuralda devlete bu yönde bir görev verilmediği, devletin bu konudaki sorumluluğunun sadece sözü edilen ilaçların piyasada bulunması konusunda gerekli tedbirleri almakla sınırlı tutulduğu belirtilerek kuralın, Anayasa'nın 2. ve 56. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralla, Türkiye İlaç ve Tıbbî Cihaz Kurumuna, hayati önemi haiz ilaç, tıbbi cihaz ve ürünlerin piyasada sürekli bulunabilmesi için gerekli tedbirleri alma görev ve yetkisi verilmiştir.

KHK'nin 2. maddenin (2) numaralı fıkrasının (d) bendine göre, sağlık hizmetlerinde kullanılan ilaçlar, özel ürünler, ulusal ve uluslararası kontrole tabi maddeler, ilaç üretiminde kullanılan etken ve yardımcı maddeler, kozmetikler ve tıbbi cihazların halka ulaştırılması ve fiyatlarının belirlenmesi, Sağlık Bakanlığının görevleri arasındadır. Anılan 2. maddenin (4) numaralı fıkrasında ise 'İlaç fiyatlarının belirlenmesine ilişkin usûl ve esaslar Bakanlığın teklifi üzerine Bakanlar Kurulunca belirlenir.' hükmü yer almaktadır. Bu kapsamda KHK'nin 27. maddenin (2) numaralı fıkrasının (h) bendiyle, ilaç fiyatlarının belirlenmesi için farmako-ekonomik değerlendirme ve çalışmaların yapılması, bir görev olarak Türkiye İlaç ve Tıbbî Cihaz Kurumuna verilmiştir.

Buna göre, ilaç fiyatlarının belirlenmesi konusunda devletin farklı kurumlarına çeşitli görev ve yetkiler verilmiştir. Bu nedenle, devletin ilaç, tıbbi cihaz ve ürünlerin fiyatlarını belirlemek konusunda herhangi bir ödev üstlenmediğinin söylenmesi mümkün değildir. Ayrıca, sosyoekonomik yönden dezavantajlı durumda olan kişilerin sağlık hizmetlerinden yararlanabilmeleri için sosyal

devlet ilkesinin geređi olan tedbirlerin alınması ve bunların nelerden ibaret olacađı ve hangi alanlarda uygulanacađı, kanun koyucunun takdir yetkisi kapsamındadır.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2. ve 56. maddelerine aykırı deđildir. İptal isteminin reddi gerekir.

20- KHK'nin 27. Maddesinin (2) Numaralı Fıkrasının (ğ) Bendinde Yer Alan 'yaptırmak' Sözcüğü

Dava dilekçesinde, 'yaptırmak' sözcüğüyle, Türkiye İlaç ve Tıbbî Cihaz Kurumuna verilmiş olan gözetim ve denetim yetkisinin devrine olanak tanındığı, laboratuvar analizlerini gerçekleştirecek birimlerin niteliğinin belirtilmediđi, bu kapsamda yürütmeye sınırsız bir takdir yetkisi tanındığı belirtilerek kuralın, Anayasa'nın 2., 7., 56. ve 123. maddelerine aykırı olduđu ileri sürülmüştür.

Dava konusu kuralı da içeren KHK'nin 27. maddesinin (2) numaralı fıkrasının (ğ) bendiyle, Türkiye İlaç ve Tıbbî Cihaz Kurumuna, görev alanına giren ilaç, tıbbi cihaz ve ürünlerin piyasa gözetimi ve denetimini yapma, gerektiğinde toplatma, imha etme veya ettirme, piyasadaki ürünler için güvenilirlik bildirim yöntemlerini belirleme, gerekli bildirimleri yapma, laboratuvar analizlerini yapma veya yaptıрма görev ve yetkisi verilmiştir. İptali istenen 'yaptırmak' sözcüğü, Türkiye İlaç ve Tıbbî Cihaz Kurumunun, görev alanına giren ilaç, tıbbi cihaz ve ürünlerin laboratuvar analizlerini özel hukuk kişilerine yaptıрма olanađı tanımaktadır.

Anayasa'nın 56. maddesinde, 'devlet, herkesin hayatını, beden ve ruh sađlığı içinde sürdürmesini sađlamak (') amacıyla sađlık kuruluşlarını tek elden planlayıp hizmet vermesini düzenler. Devlet, bu görevini kamu ve özel kesimlerdeki sađlık ve sosyal kurumlarından yararlanarak, onları denetleyerek yerine getirir.' hükmü yer almaktadır. Bu düzenlemeden, devletin asıl görevinin, 'düzenleme ve denetleme' olduđu, sađlık hizmetleri alanında devlete yüklenmiş olan bu görevlerin yerine getirilmesinde 'kamu ve özel kesimlerdeki sađlık ve sosyal yardım kurumlarından' yararlanılacađı anlaşılmaktadır. Bu itibarla, sađlık alanındaki hizmetlerin mutlaka klasik idari usullere göre, bizzat idare tarafından ve idarenin kendi personeli eliyle yürütülmesi gerektiğine dair anayasal bir zorunluluk bulunmamaktadır. Kaldı ki, iptali istenilen sözcüğün, piyasadaki ilaç ve tıbbi ürünlerin laboratuvar analizinin yapılması ile ilgili olduđu görülmektedir. Teknik bir tespit yapılmasına dair laboratuvar analizinin bizzat Kurumca yapılması ya da Kurum tarafından uygun/yetkin laboratuvarlara yaptırılmasının, denetim yetkisinin devrine izin verilmesi şeklinde anlaşılması mümkün deđildir.

Anayasa'nın 7. maddesinde, 'Yasama yetkisi Türk Milleti adına Türkiye Büyük Millet Meclisinindir. Bu yetki devredilemez.' denilmektedir. Buna göre, Anayasa'da yasa ile düzenlenmesi öngörülen

konularda yürütme organına genel ve sınırları belirsiz bir düzenleme yetkisinin verilmesi olanaklı değildir. Farklı koşul ve durumlara göre sık sık değişik önlemler alma, bunları kaldırma ve süratli biçimde hareket etme zorunluluğunun bulunduğu alanlarda, yasama organının temel kuralları saptadıktan sonra, uzmanlık ve idare tekniğine ilişkin hususları yürütmeye bırakması, yasama yetkisinin devri olarak yorumlanamaz.

İlaç, tıbbi cihaz ve ürünlerin laboratuvar analizlerinin yapılması tıp tekniğini ilgilendiren ve uzmanlık gerektiren bir mesele olup analiz ölçütlerinin belirlenmesi ve bu analizleri yapacak özel kuruluşların haiz olması gereken nitelik ve standartların saptanmasının yürütmeye bırakılmış olması, yasama yetkisinin devri olarak görülemez.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 7. ve 56. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 2. ve 123. maddeleriyle ilgisi görülmemiştir.

21- KHK'nin 27. Maddesinin (2) Numaralı Fıkrasının (1) Bendi

Dava dilekçesinde, KHK'nin 8. maddesinin (1) numaralı fıkrasının (g) bendi için açıklanan gerekçelerle kuralın, Anayasa'nın 2., 9., 36. ve 138. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralla, Türkiye İlaç ve Tıbbî Cihaz Kurumuna, görev alanına giren ilaç, tıbbi cihaz ve ürünleri üretenler, satanlar ve faydalananlar arasında doğabilecek ihtilafların çözümüne yönelik usulleri belirleme görev ve yetkisi verilmiştir.

KHK'nin 8. maddesinin (1) numaralı fıkrasının (g) bendi için açıklanan gerekçelerle dava konusu kural, Anayasa'nın 36. maddesine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 2., 9. ve 138. maddeleriyle ilgisi görülmemiştir.

22- KHK'nin 27. Maddesinin (3) Numaralı Fıkrasının (e) Bendi

Dava dilekçesinde, Türkiye İlaç ve Tıbbî Cihaz Kurumunun, etki altında kalınmaksızın bağımsızlık içinde hizmetleri yürütebilmesi için ilaç ve medikal cihaz ve ürün için ruhsat başvurusunda bulunan gerçek ve tüzel kişilerden bağış kabul edememesi gerektiği, dava konusu kuralda bu yönde bir hükme yer verilmemesinin Anayasa'nın 2., 5. ve 56. maddelerine aykırı olduğu ileri sürülmüştür.

KHK'nin 27. maddesinin dava konusu kuralı da içeren (3) numaralı fıkrasında, Türkiye İlaç ve Tıbbî Cihaz Kurumunun gelirleri sayılmış, dava konusu (e) bendinde ise 'Kuruma yapılacak bağışlar ve yardımlar' da Kurumun gelirleri arasında gösterilmiştir.

5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'nun 'Bağış ve yardımlar' başlıklı 40. maddesinin birinci fıkrasında, herhangi bir gerçek veya tüzel kişi tarafından, kamu hizmetinin karşılığı olarak veya kamu hizmetleriyle ilişkilendirilerek bağış veya yardım toplanamayacağı ve benzeri adlar altında tahsilât yapılamayacağı hükme bağlanmıştır. Buna göre, 5018 sayılı Kanun'a tabi bir idare olarak Türkiye İlaç ve Tıbbi Cihaz Kurumunun, görev alanında bulunan ürün gruplarını temsil eden sektörden, firmalardan bağış ve yardım kabul etmesi mümkün değildir.

Bunun yanı sıra, ilaçları ruhsatlandırarak merciin, bağış veya yardım yapılıp yapılmadığına bakmaksızın, bunun etkisi altında olmaksızın hareket etmek zorunda olduğu, aksine davranışın ilgililerin cezai ve idari sorumluluklarını gündeme getireceği, aynı şekilde, ilgili Kuruma bağış yapılıp yapılmadığına bakılarak ruhsat verildiği ya da verilmediğinin ortaya konulması hâlinde, söz konusu işlemlerin denetiminin de mümkün olabileceği açıktır.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2. ve 56. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 5. maddesiyle ilgisi görülmemiştir.

23- KHK'nin 30. Maddesi

Dava dilekçesinde, KHK'nin 26. ve 29. maddeleri için açıklanan gerekçelerle dava konusu kuralın, Anayasa'nın 2., 17., 56., 123. ve 126. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralda, Türkiye Kamu Hastaneleri Kurumuna bağlı olarak il düzeyinde kurulacak olan Kamu Hastaneleri Birliklerinin kuruluşuna ve bu Birliklerin teşkilat yapısına ilişkin hükümler yer almaktadır.

KHK'nin 26. ve 29. maddeleri için açıklanan gerekçelerle dava konusu kural, Anayasa'nın 56. maddesine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 2., 6., 17., 123. ve 126. maddeleriyle ilgisi görülmemiştir.

24- KHK'nin 31. Maddesi

Dava dilekçesinde, KHK'nin 30. maddesi için açıklanan Anayasa'ya aykırılık gerekçelerine ek olarak, 31. maddenin (1) numaralı fıkrasının (c) bendinde yer alan 'personel hareketlerini gerçekleştirmek' görev ve yetkisinin kapsamı, süresi, sınırları ve ilkelerinin belirsiz olduğu, istihdam planlaması yapma, personel hareketlerini gerçekleştirme konusunda idareye, kapsamı ve çerçevesi belirsiz bir yetki tanındığı belirtilerek kuralın, Anayasa'nın 2., 17., 56., 123., 126. ve 128. maddelerine aykırı olduğu ileri sürülmüştür.

KHK'nin 31. maddesinde, Kamu Hastaneleri Birliklerinde görev yapacak olan 'genel sekreter' ile genel sekretere bađlı olarak görev yapacak olan 'hastane yöneticisi'nin görev, yetki ve sorumlulukları düzenlenmiş; (1) numaralı fıkrasının (c) bendinde ise Birlik bünyesindeki sađlık kurumlarında etkili ve verimli hizmet sunumunu sađlayanın, bu amaçla kaynak ve personel ihtiyaçlarını tespit etmenin, istihdam planlaması yapma ve personel hareketlerini gerçekleřtirmenin Birliđin görevlerinden olduđu belirtilmiřtir.

KHK'nin 26. ve 29. maddeleri için açıklanan gerekçelerle dava konusu kural, Anayasa'nın 56. maddesine aykırı deđildir.

Anayasa'nın 128. maddesinin ikinci fıkrasında, 'Memurların ve diđer kamu görevlilerinin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülükleri, aylık ve ödenekleri ve diđer özlük işleri kanunla düzenlenir. Ancak, mali ve sosyal haklara iliřkin toplu sözleşme hükümleri saklıdır. Üst kademe yöneticilerinin yetiřtirilme usul ve esasları, kanunla özel olarak düzenlenir.' denilmiřtir.

Dava konusu kuralda, personel yönetimi bađlamında ilgili kanunlar uyarınca yapılması gereken işlemleri icraya yetkili idari makamlar belirlenmiřtir. Kuralda, sađlık personelinin tabi olacađı statü ve atanma kořullarına iliřkin herhangi bir hükme yer verilmemiřtir. Sađlık personelinin tabi olacađı atanma usulü, bunların hakları ve ödevleri, çalıřma kořulları gibi hususlar yönünden 657 sayılı Devlet Memurları Kanunu, 4924 sayılı Eleman Temininde Güçlük Çekilen Yerlerde Sözleşmeli Sađlık Personeli Çalıřtırılması ile Bazı Kanun ve Kanun Hükmünde Kararnelerde Deđişiklik Yapılması Hakkında Kanun ve ilgili diđer kanunlar uygulanmaya devam edilmektedir. Dolayısıyla yürütmeye sınırsız ve kapsamı belirsiz bir yetki tanındıđından söz edilemez.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 56. ve 128. maddelerine aykırı deđildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 2., 17., 123., ve 126. maddeleriyle ilgisi görülmemiřtir.

25- KHK'nin 32. Maddesi

Dava dilekçesinde, birlik genel sekreteri, idari ve mali hizmetler başkanları, hastane yöneticisi, müdür ve müdür yardımcısı olabilmek için aranan řartların, hastanelerin yönetimini içeren yetkilerin gerektirdiđi nitelikleri karřılamaktan uzak olduđu, sözleşmeli personelin sözleşmelerinin performans kriterleri ve hedeflerindeki başarı oranlarına göre sona erdirilmesi ve bu kriterlere bađlayıcılık atfedilmesinin bu personeli kamusal güvenceden mahrum bıraktıđı, başarısızlık sebebiyle genel sekreterin deđiřmesi halinde genel sekretere bađlı çalıřan diđer bazı yöneticilerin sözleşmelerinin de kendiliđinden sona ereceđine iliřkin düzenlemenin kamu personel rejimine iliřkin anayasal ilkelere

aykırı olduđu, dava konusu kuralın, kamu görevlileri ile devlet arasındaki sözleşmeli statüde çalışma/çalıştırma ilişkisinde, çalışma koşullarını düzenleyen kuralları belirlemek noktasında idareye geniş takdir yetkisi tanıdığı belirtilerek kuralın, Anayasa'nın 2., 7. ve 128. maddelerine aykırı olduđu ileri sürülmüştür.

KHK'nin 32. maddesinde, Kamu Hastaneleri Birliklerinde görev yapacak olan Birlik personelinin niteliđi ve statüsü düzenlenmiştir. Anılan maddenin (2) numaralı fıkrasında, genel sekreter, idari ve mali hizmetler başkanları, hastane yöneticisi, müdür ve müdür yardımcısı olabilmek için aranacak nitelikler gösterilmiştir. Buna göre, anılan görevlere gelebilmek için dört yıllık yükseköğrenim görmek ve genel sekreter için 8, diđer yöneticiler için ise 5 yıl kamuda ya da özel sektörde iş tecrübesine sahip olmak şartları aranmıştır.

Maddenin (5) numaralı fıkrasında ise sözleşmeli statüde istihdam edilecek personelle yapılacak sözleşmelerin içeriđi, yapılış şekli, süresi, sona erme nedenleri ve başarısızlık nedeniyle genel sekreterin sözleşmesinin sona erdirilmesinin diđer yöneticilerin sözleşmelerine etkisi gibi hususlar düzenlenmiştir. Buna göre, sözleşmeli statüde istihdam edilecek personelle yapılacak sözleşme ekinde kurumsal hedefler ve performans değerlendirme kriterleri de gözetilerek hazırlanan bireysel performans kriterleri ve hedeflerinin belirtilmesi öngörülmüştür. Genel sekreterin doğrudan; başkanlar, hastane yöneticileri, başhekim ve müdürlerin ise genel sekreterin teklifi üzerine Kurum Başkanıyla sözleşme yapacakları belirtilmiştir. Uzman personel ile büro görevlilerinin sözleşmelerinin ise genel sekreter tarafından yapılacağı kurala bağlanmıştır. Başhekim yardımcılarının başhekimin, müdür yardımcılarının sözleşmelerinin ise ilgili müdürün teklifi üzerine hastane yöneticisi tarafından yapılacağı düzenlenmiştir. Sözleşmelerin süresinin iki yıldan dört yıla kadar olacağı ve sürenin sonunda tekrar sözleşme yapılabileceđi belirtilmiştir. Sözleşme eki performans hedeflerindeki gerçekleştirmelere bağlı olarak süresinden önce de sözleşmelerin sona erdirilebilmesi olanaklı kılınmıştır. Başarısızlık sebebiyle genel sekreterin deđişmesi halinde başkanların ve başarısızlığa sebebiyet veren hastane yöneticilerinin sözleşmelerinin kendiliğinden sona ermesi öngörülmüştür. Yeni hastane yöneticisinin göreve başlamasından itibaren, ilgili hastane başhekimini, müdürleri, başhekim yardımcılarını ve müdür yardımcılarının; yeni başhekim ve müdürlerin göreve başlamasından itibaren de yardımcılarının bir ay sonunda sözleşmelerinin kendiliğinden sona ereceđi kurala bağlanmıştır. Sözleşmeleri bu suretle sona eren personel ile yeniden sözleşme yapılması mümkündür. Ekli (II) sayılı cetvelde belirtilen pozisyonlarda açıktan istihdam edilen personelin herhangi bir suretle sözleşmeleri sona erdiğinde birlik ile ilişkilerinin

kesileceđi ve aıktan szleřmeli istihdam, memurluk veya diđer personel istihdam řekillerinden birine geiř bakımından kazanılmıř hak teřkil etmeyeceđi dzenlenmiřtir.

Maddenin (2) numaralı fıkrasında, Kamu Hastaneleri Birliklerinde grev yapacak genel sekreter, idari ve mali hizmetler bařkanları, hastane yneticisi, mdr ve mdr yardımcısı olabilmek iin aranacak nitelikler aıka gsterilmiřtir. Anılan personel iin belirlenen niteliklerin, bunlara yklenen sorumluluklarla uyumlu olup olmadıđı bir yerindelik sorunu olup anayasallık denetiminin kapsamı dıřında kalmaktadır.

Maddenin (5) numaralı fıkrasında, szleřmelerin nasıl yapılacađı, ne kadar sreyle geerli olacađı, hangi řartlara bađlı olarak sona ereceđi belirlenmiřtir. Bu ereveye uygun olarak hazırlanacak her bir szleřme metninde, KHK'de sayılan hususların somut olarak da gsterileceđi tabiidir. Diđer bir ifadeyle szleřmenin tarafları, szleřmenin ieriđini szleřmeyi yaparken bilebilecek durumdadır. Bu nedenle dava konusu kuralın belirlilik ve ngrlebilirlik unsurları ynnden hukuk devleti ilkesine aykırı bir yn bulunmamaktadır.

te yandan, szleřmeli statde istihdam edilen personelin, Kamu Hastaneleri Kurumuna bađlı olarak, birbirinden farklı hastanelerde grev yapacađı gzetildiđinde, her bir hastane yneticisi, bařhekimisi ve diđer szleřmeli personel iin geerli olacak kurumsal ve bireysel performans hedef ve kriterlerinin KHK metninde belirlenmesi olanaksızdır. İdari ve teknik yn ađır basan performans hedef ve kriterlerinin KHK'de ngrlen esas ve usullere uygun olarak idarece belirlenmesi iřin niteliđi geređi olup, yasama yetkisinin devri olarak yorumlanamaz.

Ayrıca bařarısızlık sebebiyle genel sekreterin deđiřmesi halinde bařkanların ve bařarısızlıđa sebebiyet veren hastane yneticilerinin szleřmelerinin kendiliđinden sona ermesi ngrlmř ise de performans kriter ve hedeflerine ulařmada yetersizlikleri nedeniyle genel sekreterin bařarısızlıđına iřtirak ettiđi tespit edilecek olanların grevlerinin sona erdirilebileceđinde kuřku bulunmamaktadır. İdareci konumunda bulunanların, yetersizlik veya bařarısızlıklarının saptanması durumunda, bunların yneticilik vasıflarının zerlerinden alınarak derece ve sınıflarına uygun kadrolara atanmalarında Anayasa'ya aykırı bir yn bulunmamaktadır.

Aıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 7. ve 128. maddelerine aykırı deđildir. İptal isteminin reddi gerekir.

26- KHK'nin 33. Maddesinin (1) Numaralı Fıkrasının İkinici Cmlesi

Dava dilekçesinde, kamu görevlilerinin aylık ve ödeneklerinin de kanunla düzenlenmesi gerektiği, performansa dayalı ek ödemenin oran, usul ve esaslarının belirlenmesinin idarenin takdirine bırakıldığı belirtilerek kuralın, Anayasa'nın 128. maddesine aykırı olduğu ileri sürülmüştür.

KHK'nin 33. maddesinde, Kamu Hastaneleri Kurumunda sözleşmeli olarak çalışan personelin mali hakları ve yükümlülükleri düzenlenmektedir. Anılan maddenin (1) numaralı fıkrasının birinci cümlesinde, ekli (II) sayılı cetvelde belirtilen personele, 657 sayılı Kanun'un 4. maddesinin (B) fıkrasına göre belirlenen tavan ücret esas alınarak genel bütçeden ekli (III) sayılı cetvelde belirlenen oranlarda peşin olarak ücret ödeneceği belirtilmiş; dava konusu ikinci cümlede de, ayrıca personelin katkısıyla elde edilen döner sermaye gelirlerinden aynı cetvelde belirlenen tavan oranları geçmemek kaydıyla ek ödeme yapılabileceği ifade edilmiştir. Fıkranın son cümlesiyle ise Bakanlıkça belirlenen hizmet sunum şartları ve kriterleri de dikkate alınmak suretiyle, bu ödemenin oranı ile usul ve esaslarının; hastanenin grubu, personelin görevi, eğitim durumu, çalışma şartları ve çalışma süreleri, hizmete katkısı, performansı gibi unsurlar esas alınarak belirleme yetkisi, Maliye Bakanlığının uygun görüşü alınmak koşuluyla Bakanlığa verilmiştir.

Dava konusu kuralda, sözleşmeli personele ödenecek döner sermaye ek ödemelerinin tavan oranları gösterilmiştir. Ayrıca, bu ödemelerin oranı ile usul ve esaslarının, hangi kriterler esas alınarak belirleneceği KHK metninde açıklanmıştır. Öte yandan, kuralda, ödenecek 'asgari oran'a ilişkin herhangi bir hükme yer verilmemiş ise de KHK'nin 58. maddesiyle 209 sayılı Sağlık Bakanlığına Bağlı Sağlık Kurumları ile Esenlendirme (Rehabilitasyon) Tesislerine Verilecek Döner Sermaye Hakkında Kanun'un 5. maddesinin ikinci fıkrasına ilave edilen bir cümleyle, döner sermayeli sağlık kurum ve kuruluşlarında görev yapan memurlar ile sözleşmeli personele, personelin katkısıyla elde edilen döner sermaye gelirlerinden yapılacak ek ödemenin net tutarının, 375 sayılı KHK'nin ek 9. maddesi uyarınca kadro ve görev unvanı veya pozisyon unvanı itibarıyla belirlenmiş olan ek ödeme net tutarından az olamayacağı kurala bağlanmak suretiyle personele verilecek döner sermaye ek ödemesinin asgari tutarı da belirginleştirilmiştir.

Sözleşmeli personele yapılacak ek ödemenin alt ve üst sınırları ile hesaplanma kriterleri açıkça kanunla gösterildikten sonra, bu ödemenin usul ve esaslarının belirlenmesi yetkisinin yürütmeye bırakılmasında, Anayasa'ya aykırı bir yön bulunmamaktadır.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 128. maddesine aykırı değildir. İptal isteminin reddi gerekir.

27- KHK'nin 34. Maddesi

Dava dilekçesinde, hastanelerin tıbbi ve mali kriterler ile kalite, hasta ve çalışan güvenliği ve eğitim kriterleri çerçevesinde değerlendirilmesinin özü itibariyle bir denetim işlemi olduğu, memurlar ve diğer kamu görevlileri eliyle yerine getirilmesi gereken denetim görevinin özel denetim kuruluşları aracılığıyla ifasına olanak sağlanmasının Anayasa'ya uygun düşmediği, değerlendirme ve gruplandırma sonuçlarına göre kamu hastaneleri birlikleri ile kamu hastaneleri yöneticilerinin sözleşmelerinin sona erdirilebilecek olmasının memuriyet güvencesiyle bağdaşmadığı, hastanelerin ve birliklerin sınıflandırılmasının kamu hizmetinin verilmesinde eşitlik ilkesine aykırı sonuçlar doğurabileceği belirtilerek kuralın, Anayasa'nın 2., 6., 17., 56. ve 128. maddelerine aykırı olduğu ileri sürülmüştür.

KHK'nin 34. maddesinde, Birlik hastanelerinin gruplandırılması ve denetimi düzenlenmektedir. Buna göre hastaneler; tıbbi ve mali kriterler ile kalite, hasta ve çalışan güvenliği ve eğitim kriterleri çerçevesinde Kurumca belirlenecek usul ve esaslara göre altı aylık veya bir yıllık sürelerle değerlendirmeye tabi tutulur. Bu değerlendirmenin, kamu veya özel değerlendirme kuruluşlarına da yaptırılması olanaklı kılınmıştır. Değerlendirme sonuçlarına göre hastanelerin yukarıdan aşağıya doğru (A), (B), (C), (D) ve (E) şeklinde gruplandırılması öngörülmüş ve ayrıca KHK'de açıklanan hallerin oluşması durumunda, genel sekreterin ve ilgili hastane yöneticisinin görevine son verileceği belirtilmiştir.

Dava konusu kuralda, sözü edilen hastanelerin değerlendirilmesi faaliyeti, hastanelerin, KHK'de gösterilen gruptan hangisine dahil olacağına ortaya çıkarılması amacıyla, belirlenen kriterler çerçevesinde mevcut durumlarının tespit edilmesine yönelik teknik bir inceleme mahiyetinde olup denetim olarak nitelendirilmesi olanaksızdır.

Hastanelerin değerlendirilmesi işleminin usul ve esaslarının Kamu Hastaneleri Kurumu tarafından belirleneceği kuralda açıkça ifade edilmiştir. Ayrıca, hastanelerin gruplandırılmasına ilişkin işlemlerin yapılması ve bu konuda karar verilmesi yetkisinin Kamu Hastaneleri Kurumuna ait olduğu anlaşılmaktadır. Değerlendirme yapma görevi verilebilecek özel değerlendirme kuruluşunun fonksiyonu ise teknik inceleme yaparak ilgili yerlere raporlama yapmaktan ibarettir.

Değerlendirme şirketince hazırlanan rapor dikkate alınarak hastanelerin gruplandırılmasına ilişkin nihai kararı verme yetkisi Kamu Hastaneleri Kurumuna ait olduğundan, teknik destek sağlamaktan ibaret, hazırlık işlemi niteliğinde bir görev olduğu anlaşılan hastanelerin Kurumca belirlenen kriterlere göre değerlendirilmesi görevinin üçüncü kişilere gördürülmesinde Anayasa'ya aykırı bir yön bulunmamaktadır.

KHK'nin 32. maddesi için açıklanan gerekçeler, dava konusu kuralın, değerlendirme sonuçlarına göre genel sekreterin ve ilgili hastane yöneticisinin görevine son verilmesine olanak sağlayan bölümü yönünden de geçerlidir.

Diğer taraftan, hastanelerin, teknik donanım, personel ve benzeri durumlar yönünden aynı nitelik ve standartlara sahip olmadığı bilinen bir gerçektir. Dava konusu kuralla, hastanelerin, tıbbi ve mali kriterler ile kalite, hasta ve çalışan güvenliği ve eğitim kriterleri çerçevesinde değerlendirmeye tabi tutularak gruplandırılması öngörülmekle birlikte, sorumlu yöneticileri, hastanelerin kalite standartlarını artırmaya yönelik çabalarda bulunmaya zorlayan çeşitli hükümler de sevk edilerek, hastanelerin teknik donanım, personel ve hizmet kalitesi yönünden birbirleriyle eşitlenmesi amaçlanmıştır. Hastanelerin gruplandırılması, sağlık hizmeti alacak bireyler yönünden sağlık hizmetine erişimde herhangi bir sınırlamaya yol açmamaktadır.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 56. ve 128. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 6. ve 17. maddeleriyle ilgisi görülmemiştir.

28- KHK'nin 36. Maddesinin (2) Numaralı Fıkrasının (b) Bendinde Yer Alan "ikincil düzenlemeleri yapmak," İbaresini

Dava dilekçesinde, Anayasa'nın 115. maddesi uyarınca tüzük çıkarma yetkisinin Bakanlar Kuruluna ait olduğu, 124. maddesine göre ise Başbakanlık, bakanlıklar ve kamu tüzelkişilerinin yönetmelik çıkarabileceği, bağlı kuruluşlardan Türkiye Hudut ve Sahiller Sağlık Genel Müdürlüğü ve Türkiye İlaç ve Tıbbî Cihaz Kurumu dışındaki diğer bağlı kuruluşların tüzel kişiliği bulunmadığından bunlara yönetmelik çıkarma yetkisi tanınamayacağı belirtilerek kuralın, Anayasa'nın 2., 6., 7., 115. ve 124. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralla, Sağlık Bakanlığı bağlı kuruluşların en üst amiri olan başkanlar ve genel müdürlere, Bakanlık politikalarına uygun şekilde, ikincil düzenlemeleri yapma görev ve yetkisi verilmiştir.

Anayasa'nın 115. maddesinde, 'Bakanlar Kurulu, kanunun uygulanmasını göstermek veya emrettiği işleri belirtmek üzere, kanunlara aykırı olmamak ve Danıştayın incelemesinden geçirilmek şartıyla tüzükler çıkarabilir.' denilmiştir; 124. maddesinde ise 'Başbakanlık, bakanlıklar ve kamu tüzelkişileri, kendi görev alanlarını ilgilendiren kanunların ve tüzüklerin uygulanmasını sağlamak üzere ve bunlara aykırı olmamak şartıyla, yönetmelikler çıkarabilirler.' hükmüne yer verilmiştir.

Dava konusu kuralla, bağılı kuruluşların başkan ve genel müdürlerine, ikincil düzenlemeleri yapma yetkisi tanınmıştır. İkincil düzenlemeden kasıt, yürütme organınca kanunlara dayanılarak yürürlüğe konulan düzenleyici işlemlerdir. İdarenin düzenleyici işlemleri tüzük ve yönetmelikten ibaret olmayıp tebliğ, genel tebliğ, genelge, yönerge, sirküler, genel yazı ve benzeri adlarla çıkarılan ve öğretide adsız düzenleyici işlemler olarak nitelenen ikincil düzenlemeler de bulunmaktadır. Nitekim Anayasa Mahkemesi kararları da, düzenleyici işlemlerin Anayasa'da ismen sayılanlardan ibaret olmadığı, idarenin başka isimler altında da düzenleyici işlemler yapmaya yetkili olduğu yönündedir.

Anayasa'da ismen zikredilenlerin dışında kalan diğer düzenleyici işlemlerin icrai karar alma yetkisine sahip olan her kurum tarafından yapılabileceği öğretide ve uygulamada kabul edilmektedir. Bu bakımdan, bağılı kuruluşlar tarafından, kendi görev alanlarıyla ilgili tüzük ve yönetmeliklerin uygulanmasında uyum sağlanması, belirli konulara açıklık getirilmesi, ilgili mevzuatın hatırlatılması şeklindeki amaçlarla ikincil nitelikte olan, diğer bir ifadeyle tüzük ve yönetmelikleri ayrıntılandırılan, bunların uygulanmasında ortaya çıkabilecek tereddütleri gideren tebliğ, genelge, yönerge ve benzeri adlar taşıyan düzenlemeler yapılmasının Anayasa'ya aykırı bir yönü bulunmamaktadır.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 115. ve 124. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 2., 6. ve 7. maddeleriyle ilgisi görülmemiştir.

29- KHK'nin 45. Maddesinin (1) ve (4) Numaralı Fıkraları

Dava dilekçesinde, dava konusu kurallarla, sözleşmeli uzman çalıştırılmasına ilişkin temel ilkeler belirlenmeden tüm yetkinin idareye devredildiği, bu çerçevede yabancı uzman istihdamının öngörüldüğü ancak, bu kişilerin hukuki durumlarının, meslek ve çalışma alanlarının, yaşları ve uzmanlık konularının, eğitimlerinin, denklik durumunun belirsiz bırakıldığı, Anayasa Mahkemesinin 19.12.2005 günlü, E.2005/143, K.2005/99 sayılı kararıyla aynı içerikteki başka bir düzenlemenin iptal edildiği belirtilerek kuralların, Anayasa'nın 7. ve 128. maddelerine aykırı olduğu ileri sürülmüştür.

KHK'nin dava konusu kuralları da içeren 45. maddesinde, Sağlık Bakanlığı ve bağılı kuruluşlarında sözleşmeli uzman çalıştırılmasına ilişkin usul ve esaslar düzenlenmektedir. Maddenin iptali istenen (1) numaralı fıkrasıyla, Bakanlık ve bağılı kuruluşlarında özel bilgi ve ihtisas gerektiren nitelikli bir işin yapılması veya proje hazırlanması veya yürütülmesi için proje süresince sözleşme ile yerli ve yabancı uzman çalıştırılabilmesi olanaklı kılınmıştır. Sözleşme süresi üç yıla sınırlandırılmıştır. Bu

hüküm uyarınca istihdam edilecek personel, 657 sayılı Kanun ve diğer kanunların sözleşmeli personel çalıştırılması hakkındaki hükümlerine tabi olmayacaktır.

Maddenin iptali istenen (4) numaralı fıkrasında, bu suretle çalıştırılacak uzmanların nitelikleri, alınma usulü ve sözleşme ücretlerinin tespiti ile sözleşme usul ve esaslarının Sağlık Bakanlığı ve Maliye Bakanlığınca müştereken belirlenmesi öngörülmüştür.

Dava konusu kuralları da içeren KHK'nin 45. maddesinde, istihdam edilecek sözleşmeli personelin özel bilgi ve ihtisas gerektiren nitelikli bir işin yapılması veya proje hazırlanması veya yürütülmesi için çalıştırılabileceği, bu kişilerin proje süresince ve her halde en fazla üç yıllığına çalışabileceği, bu şekilde çalıştırılacak personelin sayısının yüz elliye geçemeyeceği, sözleşmeli olarak çalıştırılacaklara ödenecek ücretin 657 sayılı Kanun'un 4. maddesinin (B) fıkrasına göre çalıştırılanlar için uygulanmakta olan sözleşme ücreti tavanının beş katını geçemeyeceği düzenlenmek suretiyle, Sağlık Bakanlığı ve bağlı kuruluşlarında sözleşmeli personel istihdamına ilişkin genel esaslar belirlenmiştir. Kanun koyucunun, genel çerçevesini bu şekilde kanunla belirledikten sonra, bu suretle çalıştırılacak uzmanların nitelikleri, alınma usulü ve sözleşme ücretlerinin tespiti ile sözleşme usul ve esaslarıyla ilgili hususların düzenlenmesini yürütmeye bırakmış olması yasama yetkisinin devri olarak yorumlanamaz.

Açıklanan nedenlerle, dava konusu kurallar Anayasa'nın 7. ve 128. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir.

30- KHK'nin 47. Maddesinin (4) ve (5) Numaralı Fıkraları

Dava dilekçesinde, dava konusu kurallarla, kişilerin sağlık bilgilerinin toplanmasında hiçbir ayırt edici ölçünün kullanılmadığı, özel ya da kamu sağlık kuruluşlarının, kendisine başvuranlara ilişkin kişisel bilgileri ve sağlık bilgilerini Bakanlığa ve bağlı kuruluşlara iletmekle yükümlü kılındığı, oysa sağlıkla ilgili bilgilerin kişisel veriler kapsamında korunduğu, kişilerin toplumdaki insanların hayatını tehdit eden ve bu nedenle bilinmesinde üstün kamu yararı bulunan kimi hastalıklar dışında sağlıkları ile ilgili bütün bilgilerin Devletten dahi gizli tutulmasını isteme haklarının bulunduğu, buna karşılık dava konusu kurallarla sağlıkla ilgili kişisel bilgilerin her türünün her durumda istenip işlenebilmesine olanak tanındığı belirtilerek kuralların, Anayasa'nın 17. ve 20. maddelerine aykırı olduğu ileri sürülmüştür.

KHK'nin 47. maddesinde, Sağlık Bakanlığı ve bağlı kuruluşlarına tanınan bilgi toplama, işleme ve paylaşma yetkisi düzenlenmektedir.

Maddenin, Sağlık Bakanlığı ve bağlı kuruluşlarının kişisel verileri toplama yetkisinin amacını, kapsamını, bunların toplanmasını ve paylaşılmasını düzenleyen (1), (2) ve (3) numaralı fıkraları, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı bulunarak iptal edildiğinden bu fıkralara yönelik olarak öne sürülen Anayasa'ya aykırılık iddiaları incelenmemiştir.

Maddenin (4) numaralı fıkrasında, sağlık personeli istihdam eden kamu kurum ve kuruluşları ile özel hukuk tüzel kişileri ve gerçek kişilerinin, istihdam ettiği personeli ve personel hareketlerini Bakanlığa bildirmekle yükümlü oldukları belirtilmiştir. (5) numaralı fıkrada ise maddenin uygulanmasına ilişkin hususların Bakanlıkça çıkarılacak yönetmelikle düzenleneceği kuralına yer verilmiştir.

Dava dilekçesinde ileri sürülen iddialar, maddenin (1), (2) ve (3) numaralı fıkralarına yönelik olup (4) ve (5) numaralı fıkralarının hangi yönlerden Anayasa'ya aykırı olduğu hususunda dilekçede herhangi bir açıklama yer almamaktadır. Anılan fıkralarda düzenlenen hususların, istihdam edilen sağlık personelinin kurumsal kimliğiyle ilgili bilgilerin ve sağlık personeli hareketlerinin toplanmasına ilişkin olduğu ve bu nedenle Anayasa'nın 17. ve 20. maddeleriyle ilgisinin bulunmadığı anlaşılmaktadır.

31- KHK'nin 48. Maddesinin (1) Numaralı Fıkrasının (c) Bendi ile (2) ve (3) Numaralı Fıkraları

Dava dilekçesinde, dava konusu kurallar ile Sağlık Bakanlığına, kamu kurum ve kuruluşlarına ait veya tahsisli bütün taşınmazların kendisine tahsisini veya devrini talep edebilme yetkisinin verildiği, Bakanlığa verilen bu yetkinin kamu taşınmazları üzerinde sınırları belirsiz bir tasarruf yetkisinin kullanılması anlamına geldiği, bu durumun hukuk devleti ve yasama yetkisinin devredilmezliği ilkeleriyle çeliştiği belirtilerek kuralların, Anayasa'nın 2. ve 7. maddelerine aykırı olduğu ileri sürülmüştür.

KHK'nin 48. maddesinde, Bakanlığın, hizmet binası ve sağlık tesisi yaptırmasına ilişkin usul ve esaslar düzenlenmiştir. Maddenin (1) numaralı fıkrasının iptali istenen (c) bendiyle, Sağlık Bakanlığı ve bağlı kuruluşlarınca yaptırılacak hizmet binası ve sağlık tesislerinin bedellerinin kurumların mülkiyetindeki taşınmazlar veya Maliye Bakanlığının görüşü alınarak Hazine'nin özel mülkiyetindeki taşınmazlardan Bakanlığa veya Kurumlara tahsisli olan taşınmazların üzerindeki yapılarla birlikte devredilmesi suretiyle karşılanmak üzere düzenlenecek protokol esasları çerçevesinde Toplu Konut İdaresi Başkanlığına veya inşaat işleriyle ilgili araştırma, proje, taahhüt, finansman ve yapım işlemleri konusunda görevli ve yetkili kamu tüzel kişiliğine sahip diğer kurum ve kuruluşlara da doğrudan yaptırılabilmesi olanaklı kılınmıştır.

Maddenin iptali istenen (2) numaralı fıkrasında, (1) numaralı fıkranın (c) bendiyle bağlantılı olarak, Sağlık Bakanlığının, hizmet binası ve sağlık tesisi yaptırmak üzere, kamu kurum ve kuruluşlarına ait veya tahsisli taşınmazların kendisine tahsis edilmesini veya devredilmesini talep edebileceği ya da kullanım protokolleri yapabileceği, bu protokoller ile oluşan yükümlülüklerini Toplu Konut İdaresi Başkanlığına veya inşaat işleri ile ilgili araştırma, proje, taahhüt, finansman ve yapım işlemleri konusunda görevli ve yetkili kamu tüzel kişiliğine sahip diğer kurum ve kuruluşlara yaptırabileceği kurala bağlanmıştır.

İptali istenen (3) numaralı fıkrada ise sağlık hizmetlerinde kullanılmakta olan binalardan, Bakanlıkça oluşturulacak komisyon tarafından fonksiyonellik ve/veya onarım-tadilat maliyeti açısından yapılan değerlendirme sonucunda yıkımının uygun olduğuna karar verilenlerin yıkılabileceği, yıkım kararı verecek komisyonun teşkili ile çalışma usul ve esaslarının Bakanlıkça belirleneceği düzenlenmiştir.

Dava konusu kurallarla, Sağlık Bakanlığına tanınan yetki, kamu kurum ve kuruluşlarına ait taşınmazların kendisine tahsis edilmesini veya devredilmesini talep edebilme yetkisidir. Bu talepler hakkında nihai kararı verecek olan merci Sağlık Bakanlığı veya bağlı kuruluşları olmayıp, ilgisine göre Maliye Bakanlığı ya da diğer kamu idareleridir. Hazine ve diğer kamu idarelerinin mülkiyetinde bulunan taşınmazlar ile devletin hüküm ve tasarrufu altında bulunan taşınmazların tahsisi ve devri konusu, 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu ve anılan Kanun'a dayanılarak çıkarılan yönetmeliklerde yer almaktadır.

Dava konusu kurallarla Sağlık Bakanlığına tanınan tahsis ya da devre ilişkin talepte bulunma yetkisinin kullanımı da 5018 sayılı Kanun çerçevesinde gerçekleşeceğinden hukuk devleti ve yasama yetkisinin devredilmezliği ilkelerine aykırılık söz konusu değildir.

Açıklanan nedenlerle, dava konusu kurallar Anayasa'nın 2. ve 7. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir.

32- KHK'nin 49. Maddesi

Dava dilekçesinde, ülkemizde 1980'li yıllarda kurulmaya başlanan serbest bölgelerin ülkedeki ticaret hacminin artmasında ve istihdam yaratılmasında önemli bir katkısının olmadığı, keza yabancı yatırımı ve teknoloji transferini sağlama ve kalkınma açısından da beklenen yararların ortaya çıkmadığı, dava konusu kuralla kurulması öngörülen serbest sağlık bölgelerinde sunulacak sağlık hizmetlerinin kamusal nitelikte olmayıp kâr amaçlı olduğu, ayrıca serbest sağlık bölgelerinin nerede, nasıl kurulacağı, nasıl işleyeceği, serbest bölgelerden yararlanma şartlarının ne olacağı, serbest bölgelerde çalıştırılacak kişilerin statüsü, niteliği, verilecek hizmetin organizasyonu ve denetiminin

kim tarafından nasıl sağlanacağına dair hiçbir düzenleme yapılmadığı, bu alanların düzenlenmesinin idari düzenleyici işlemlere bırakıldığı belirtilerek kuralın, Anayasa'nın 2., 5., 7., 17., 49., 56., 63. ve 168. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralla, ülkenin sağlık alanında bölgesel bir cazibe merkezi haline getirilmesi, yabancı sermaye ve yüksek tıbbi teknoloji girişinin hızlandırılması amacıyla, sağlık serbest bölgelerinin (SSB) kurulması öngörülmektedir. SSB, 6.6.1985 günlü, 3218 sayılı Serbest Bölgeler Kanunu hükümleri çerçevesinde kurulabilecektir. SSB'nin kurulması ve yönetilmesine ilişkin usul ve esaslar Bakanlar Kurulunca, SSB'de verilecek sağlık hizmetlerine ilişkin usul ve esaslar ise Sağlık Bakanlığınca belirlenecektir.

Serbest bölgelerin kurulması, ekonomi politikasıyla ilgili bir konudur. Anayasa'da SSB'nin kurulmasını emreden ya da yasaklayan hiçbir kural bulunmadığı gibi ülkede nasıl bir ekonomik kalkınma modeli takip edileceği konusunda da emredici bir düzenleme yer almamaktadır. Bu bağlamda, serbest bölgelerin kurulması ve buralarda gerçekleştirilecek faaliyetlerin çerçevesinin çizilmesi konusunda siyasal iktidarların karar verme yetkisine sahip oldukları hususunda duraksama bulunmamaktadır. Serbest bölgelerin ticaret hacminin artırılmasında ve istihdam yaratılmasında ne oranda katkısının olacağı gibi hususların irdelenmesi bir yerindelik sorunu olup anayasallık denetiminin kapsamı dışındadır.

Dava konusu kuralda, sağlık serbest bölgelerinin 6.6.1985 günlü, 3218 sayılı Serbest Bölgeler Kanunu hükümlerine göre Bakanlar Kurulunca belirlenecek usul ve esaslar çerçevesinde kurulacağı ve yönetileceği ifade edilmiştir. Atıf yapılan 3218 sayılı Kanun'da, serbest bölgelerin kurulması, yer ve sınırlarının belirlenmesi, kimler tarafından kurulup işletilebileceği, hangi mevzuatın uygulanacağı ve nasıl denetlenecekleri, yatırımcılara arazi tahsisinin ne şekilde yapılacağı gibi hususlar ayrıntılı bir şekilde düzenlenmiştir. Dolayısıyla genel çerçevesi dava konusu kural ve 3218 sayılı Kanun'da saptanan sağlık serbest bölgelerinin kurulması ve yönetilmesi ile buralarda verilecek sağlık hizmetlerine ilişkin usul ve esasların belirlenmesi hususunda yürütme organına yetki tanınması, yasama yetkisinin devri olarak görülemez.

Açıklanan nedenlerle dava konusu kural, Anayasa'nın 2., 5. ve 7. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 17., 49., 56., 63. ve 168. maddeleriyle ilgisi görülmemiştir.

33- KHK'nin 51. Maddesinin (1) ve (3) Numaralı Fıkraları

Dava dilekçesinde, acil durumlar, doğal afetler, salgın hastalık gibi dayanışmayı gerektiren hallerin dışında yurtdışı sağlık hizmetlerinin kalıcı hâle getirilmesinin Anayasa'ya uygun düşmediği, yurtdışı sağlık hizmet birimlerine hangi yasal dayanak ile atamaların yapılacağı belirsiz olduğu, sağlık personelinin, hizmet alımı veya kamu özel ortaklığı modeliyle özel sektör tarafından işletilen bir birimde çalışmasının memurluğun ana ilkelerini ihlal edeceği, aylıksız izinli sayılan bu kamu çalışanlarının ücretlerinin ne şekilde ödeneceğinin ve diğer özlük haklarının nasıl düzenleneceğinin belirsiz olduğu, sağlık tesislerinin kurulup işletilmesinde kamu özel ortaklığı modelinin de uygulanabileceği yönünde bir düzenlemenin temel esaslarının gösterilmediği belirtilerek kurulların, Anayasa'nın 2., 5., 7., 10., 17., 47., 55., 56. ve 128. maddelerine aykırı olduğu ileri sürülmüştür.

KHK'nin iptali istenen kurulları da içeren 51. maddesinde, yurt dışı sağlık hizmet birimleri düzenlenmektedir. Dava konusu kurulla, Bakanlık ve bağlı kuruluşlarına, insani ve teknik yardım amacıyla yurt dışında geçici sağlık hizmet birimleri kurma, kurdurma, işletme ve işletirme yetkisi tanınmıştır. Bakanlık ve bağlı kuruluşlarının, bu amaçla ulusal ve uluslararası sivil toplum kuruluşları, finans ve yardım kuruluşları ile işbirliği ve ortak çalışma yapabilmesi, insan ve mali kaynakları ile destek sağlayabilmesi olanaklı kılınmıştır. Yurt dışında geçici sağlık hizmet birimlerinin kurulması ve işletilmesinin hizmet alımı veya kamu özel ortaklığı modeliyle özel sektöre yaptırılması mümkündür. Bu suretle özel sektör tarafından işletilen sağlık hizmet birimlerinde ve bölümlerinde Bakanlık personelinin de çalıştırılması olanaklı hale getirilmiş ve bu şekilde çalıştırılan personelin beş yılı geçmemek üzere çalıştıkları sürede aylıksız izinli sayılmaları öngörülmüştür.

Anayasa'da devletin yurt dışında sağlık hizmeti sunmasını engelleyen herhangi bir hüküm yer almadığından, yurt dışı sağlık birimlerinin oluşturulması ve bu birimler aracılığıyla sağlık hizmeti sunulmasının öngörülmesi kanun koyucunun takdirindedir.

Yurt dışı sağlık hizmet birimlerinde görevlendirilecek personelin aylık ve diğer özlük hakları konusu, 51. maddenin dava konusu yapılmayan (2) numaralı fıkrasında düzenlenmiştir. Buna göre, sözü edilen sağlık personeli, asıl kadrolarına bağlı olarak aldıkları ek ödeme dâhil her türlü mali ve özlük haklar ile sosyal haklardan faydalanmaya devam edeceklerdir. Bunun yanı sıra gittikleri ülkede sürekli görevle bulunan ve dokuzuncu derecenin birinci kademesinden aylık alan meslek memurlarına ödenmekte olan yurtdışı aylığını geçmemek üzere unvanları itibarıyla Bakanlar Kurulu kararı ile belirlenen tutarda aylık ödeme alacaklardır. Dolayısıyla, yurt dışı sağlık hizmet birimlerinde görevlendirilecek personelin aylık ve diğer özlük hakları konusunda herhangi bir belirsizlik söz konusu değildir.

KHK'nin 13. maddesinin (1) numaralı fıkrasının (e) bendi için açıklanan gerekçeler, dava konusu kuralın yurt dışı sağlık birimlerinin kamu özel ortaklığı modeliyle kurulup işletilmesine olanak tanıyan bölümü yönünden de geçerlidir.

Dava dilekçesinde, kamu görevlilerinin özel sektör tarafından işletilen bir birimde çalışmasının Anayasa'nın 128. maddesine aykırı olduğu ileri sürülmüştür. KÖO modeliyle kurulup işletilen yurt dışı sağlık birimlerinde çalıştırılan Bakanlık personelinin aylıksız izinli sayılması öngörülmüştür. Bu personelin aylıksız izinli olduğu dönemde Bakanlıkla ilişkisinin kesileceği açıktır. Bu kişilerin ücreti, yurt dışı sağlık biriminin işletme hakkını elde eden kişi veya kuruluş tarafından, taraflar arasında akdedilen özel hukuk sözleşmesi çerçevesinde ödenecektir. Dolayısıyla, Bakanlık personelinin özel sektör tarafından işletilen bir projede çalıştırıldığından söz edilemez. Öte yandan, memuriyet güvencelerine sahip Bakanlık personelinin rızası dışında aylıksız izinli sayılarak özel sektörde işletilen bir projede çalıştırılmayacağı da tabiidir. Bakanlık personelinin özgür iradesine dayanılarak bu şekilde çalıştırılmasında Anayasa'ya aykırı bir yön bulunmamaktadır.

Açıklanan nedenlerle, dava konusu kurallar Anayasa'nın 2., 7., 47. ve 128. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir.

Kuralların, Anayasa'nın 5., 10., 17., 55. ve 56. maddeleriyle ilgisi görülmemiştir.

34- KHK'nin 52. Maddesi

Dava dilekçesinde, sağlık gönüllülerinin verecekleri hizmetlerin kapsamına ilişkin bir sınırlama olmadığı, düzenlemenin kişiye özel hizmet sunumlarının önünü açacağı, bu durumun ise hukuk devleti ilkesi ile bağdaşmadığı, sağlık hizmetinin kamusal bir hizmet olduğu, sürekli, eşit, ulaşılabilir, nitelikli bir hizmet sunumu için, asli ve sürekli olarak çalışan, hakları sorumlulukları ve nitelikleri kanun ile belirlenmiş, ortak denetim ve yaptırım süreçlerine tabi kılınmış sağlık hizmet ekibi tarafından verilmesi gerektiği, gönüllü sağlık hizmeti sunumu ile ilgili bilgilerin kamuoyu ile paylaşılmasına ilişkin düzenlemelerin kimi kurum ve kuruluşların yardımlarının tanıtılması ve bu suretle bunların bilinir kılınmasına hizmet edeceği belirtilerek kuralın, Anayasa'nın 2., 5., 56., 123., 126. ve 128. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralla, sağlık hizmeti sunmaya yetkili gerçek ve tüzel kişilerce sosyal dayanışma ve yardımlaşma amacıyla gönüllü ve ücretsiz olarak sağlık hizmeti verilebilmesine imkân sağlanmıştır. Bu hizmetin, Bakanlıkça gerekli değerlendirmeler yapıldıktan sonra ve izin mahiyetinde olmak üzere verilecek sağlık gönüllüsü belgesine istinaden yapılması öngörülmüştür. Sağlık gönüllüsü gerçek kişiler, hastanelerdeki hizmetlerini, hastane yetkilisinin belirlediği şartlarda yerine getireceklerdir.

Sağlık hizmeti olmayan, hasta karşılama ve bilgilendirme, refakat, kişisel bakım ve sosyal ihtiyaçların karşılanması gibi destek hizmeti sunan sağlık gönüllüsünün sağlık meslek mensubu olması gerekmemektedir. Buna karşılık, sağlık hizmeti sunan sağlık gönüllüsünün, sağlık meslek mensubu olması zorunludur. Gönüllü sağlık hizmeti sunumu ile gönüllülere ait bilgilerin kamuoyu ile paylaşımına dair usul ve esasların Bakanlıkça belirlenmesi öngörülmüştür.

Öte yandan, dava konusu 52. maddenin son fıkrasında ise sağlık gözlemciliğine ilişkin bir düzenlemeye yer verilmiştir. Buna göre, sağlık kurum ve kuruluşlarında verilen hizmetlerden yararlananlar, hizmetin geliştirilmesi amacıyla gönüllülük esasına göre gözlemlerde bulunabilecekler ve bunların değerlendirilmesi için Bakanlık gerekli düzenlemeleri yapacaktır.

Anayasa'nın 56. maddesinin üçüncü ve dördüncü fıkralarında, 'Devlet, herkesin hayatını, beden ve ruh sağlığı içinde sürdürmesini sağlamak; insan ve madde gücünde tasarruf ve verimi artırarak, işbirliğini gerçekleştirmek amacıyla sağlık kuruluşlarını tek elden planlayıp hizmet vermesini düzenler. Devlet, bu görevini kamu ve özel kesimlerdeki sağlık ve sosyal kurumlarından yararlanarak, onları denetleyerek yerine getirir.' hükmü yer almaktadır. Bu hükümden de anlaşılacağı üzere devletin görevi sağlık kuruluşlarını tek elden planlayıp hizmet vermesini sağlamak ve bu kurumları denetlemektir.

Anayasa'da sağlık hizmetleri bir kamu hizmeti olarak düzenlenmekle birlikte, bu hizmetlerin sunulması devletin tekeline verilmemiş, devletin denetimine tabi olmak kaydıyla özel kesim tarafından da sağlık hizmeti sunulmasına olanak tanınmıştır. Dolayısıyla, memur ve diğer kamu görevlisi olmayan sağlık gönüllüleri tarafından sağlık hizmeti sunulmasına imkân verilmesinde Anayasa'ya aykırılık bulunmamaktadır.

Kamu otoritelerince verilen izin ve belgeye istinaden çalışan sağlık gönüllülerinin varlığı, devletin, asli bir kamu hizmeti olarak sağlık hizmeti sunma yükümlülüğünü ortadan kaldırmadığı gibi bireyin kamu hastanelerinde sunulan sağlık hizmetine erişim hakkını da sınırlamamaktadır. Kaldı ki, dava konusu kuralla, gönüllü ve ücretsiz sağlık hizmeti sunumları belli bir esasa bağlanmış ve bu alandaki hizmetlerin kamunun denetimi altına alınması sağlanmıştır.

Öte yandan, sağlık gönüllülerinin, kamu kaynaklarını kullanmadan ve hizmetten yararlandıktan herhangi bir ücret de almadan kişiye özel hizmet sunmaları, devletin müdahalesini gerektiren bir durum olarak görülemez.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 56. ve 128. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 2., 5., 123. ve 126. maddeleriyle ilgisi görülmemiştir.

35- KHK'nin 56. Maddesi

Dava dilekçesinde, uzmanlık eğitimlerini üniversitelerin (tıp fakültelerinin) kadrolarında ya da Sağlık Bakanlığına bağlı hastanelerde yapan hekimlerin ilave mecburi hizmet yükümlülüğü bulunmadığı hâlde Sağlık Bakanlığı adına uzmanlık eğitimi yaptırılan hekimlerin, eğitim süresi kadar Bakanlık veya bağlı kuruluşlarında mecburi hizmet yapmakla yükümlü kılınmalarının, hukuk devleti ve eşitlik ilkeleriyle bağdamadığı gibi, devletin temel amaç ve görevlerine ilişkin anayasal hükümler, çalışma hak ve özgürlüğü, zorla çalıştırma yasağı, kişinin maddi ve manevi varlığını koruma ve geliştirme hakkının ihlaline yol açtığı belirtilerek kuralın, Anayasa'nın 2., 5., 10., 17., 18. ve 48. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralla, Sağlık Bakanlığı kadrolarında bulunup Bakanlık adına üniversitelerde görevlendirilerek uzmanlık ve yan dal uzmanlığı eğitimi alacak olan hekim ve diş hekimleri, eğitimlerini tamamladıktan sonra eğitim süreleri kadar Bakanlık veya bağlı kuruluşlarında görev yapmakla yükümlü kılınmaktadır. Bu yükümlülüğün yerine getirilmemesi ya da eğitimin yarıda bırakılması veya başarısız olunması halinde ise ilgili kişilere uzmanlık eğitimi süresince Sağlık Bakanlığınca yapılan her türlü ödemenin kanuni faizi ile birlikte geri alınması öngörülmektedir. Borcun miktarı ve kişinin durumu dikkate alınarak ödemelerin en fazla beş yıl içinde taksitler halinde yapılması mümkündür.

Sağlık Bakanlığı, uzman hekim ihtiyacını, Bakanlığa bağlı eğitim ve araştırma hastanelerinde verilen uzmanlık eğitimiyle karşılamaktadır. Ancak, Sağlık Bakanlığının eğitim ve araştırma hastanelerinde verilemeyen bazı uzmanlık eğitimlerinin yaptırılmasında ise tıp fakültelerinin imkânlarından yararlanılmaktadır. Bu çerçevede ilgili hekimler, kadro ve özlük hakları Bakanlıkça karşılanmak kaydıyla üniversitelerde uzmanlık eğitimi almak üzere görevlendirilmektedir.

Anayasa'nın 48. maddesinin birinci fıkrasında, herkesin dilediği alanda çalışma ve sözleşme hürriyetine sahip olduğu belirtilmektedir. Anayasa'nın 49. maddesinin birinci fıkrasında belirtildiği üzere çalışma, herkesin hakkı ve ödevidir. Söz konusu madde gerekçesinde çalışmanın 'ödev' yönü, 'Çalışmak, başlı başına ahlaki bir vazifedir, ferdin kendisine ve toplumuna karşı olan saygısının bir sonucudur.' şeklinde ifade edilmiştir.

Anayasa'nın 18. maddesinde, 'Hiç kimse zorla çalıştırılmaz. Angarya yasaktır. Şekil ve şartları kanunla düzenlenmek üzere hükümlülük veya tutukluluk süreleri içindeki çalıştırmalar, olağanüstü

hallerde vatandaşlardan istenecek hizmetler; ülke ihtiyaçlarının zorunlu kıldığı alanlarda öngörülen vatandaşlık ödevi niteliğindeki beden ve fikir çalışmaları, zorla çalıştırma sayılmaz.' denilmektedir.

Kanunların kamu yararının sağlanması amacına yönelik olması, genel, objektif, adil kurallar içermesi ve hakkaniyet ölçütlerini gözetmesi hukuk devleti olmanın gereğidir. Bu nedenle kanun koyucunun hukuki düzenlemelerde kendisine tanınan takdir yetkisini anayasal sınırlar içinde adalet, hakkaniyet ve kamu yararı ölçütlerini göz önünde tutarak kullanması gerekir.

Kanun koyucu, düzenlemeler yaparken hukuk devleti ilkesinin bir gereği olan ölçülülük ilkesiyle bağlıdır. Bu ilke ise 'elverişlilik', 'gereklilik' ve 'orantılılık' olmak üzere üç alt ilkeden oluşmaktadır. 'Elverişlilik', başvuru önlemin ulaşılmak istenen amaç için elverişli olmasını; 'gereklilik', başvuru önlemin ulaşılmak istenen amaç bakımından gerekli olmasını ve 'orantılılık' ise başvuru önlem ve ulaşılmak istenen amaç arasında olması gereken ölçüyü ifade etmektedir.

Anayasa'nın 18. maddesinin gerekçesinde angarya, kişinin emeğinin karşılığını almadan zorla çalıştırılması olarak tanımlanmıştır. Anayasa Mahkemesinin çeşitli kararlarında da angarya, bir maldan ya da bir kişinin çalışmasından karşılıksız yararlanma biçiminde tanımlanmıştır. Zorunlu hizmet yükümlüsü hekim ve dış hekimlerinin hizmetlerinin karşılığında kendilerine ücret ödendiği gözetildiğinde, bu yükümlülük kapsamındaki çalışmaların angarya olarak nitelendirilmesi mümkün değildir.

Anayasa'da 'zorla çalıştırma' yasaklanmakla birlikte bu kavramın tanımı yapılmamıştır. Bu kavramın tanımı ve içeriği belirlenirken, temel insan haklarına ilişkin uluslararası sözleşmelerden ve ilgili uluslararası otoritelerin yorum ve uygulamalarından yararlanılabilir. Zorla çalıştırma yasağına ilişkin uluslararası kurallar, 29 Numaralı Cebri ve Mecburi Çalıştırmaya İlişkin ILO Sözleşmesi'nde düzenlenmiştir. Anılan Sözleşme'nin 2. maddesinde yapılan ve Avrupa İnsan Hakları Mahkemesince de Avrupa İnsan Hakları Sözleşmesi'nin 4. maddesinde yer alan zorla çalıştırma yasağının kapsamının belirlenmesinde esas alınan tanıma göre, zorla çalıştırma, 'herhangi bir kişinin ceza tehdidi altında ve bu kişinin tam isteği olmadan mecbur edildiği tüm iş veya hizmetleri' ifade etmektedir. Buna göre, zorla çalıştırmadan söz edilebilmesi için, kişinin ceza tehdidi altında ve rızası bulunmaksızın çalıştırılması gerekmektedir.

Sağlık Bakanlığı kadrolarında bulunup Bakanlık adına üniversitelerde görevlendirilerek uzmanlık ve yan dal uzmanlığı eğitimi alacak olan hekim ve dış hekimlerinin bu amaçla görevlendirilmeleri, ÖSYM tarafından yapılan tıpta eğitim uzmanları giriş sınavıyla gerçekleşmektedir. ÖSYM tarafından hazırlanan sınav kılavuzlarında üniversitelerin tıp fakülteleri ile Sağlık Bakanlığına bağlı eğitim ve araştırma hastanelerinin araştırma görevlisi (asistan) kontenjanları açıklanmakta ve sınavlara giren

adaylar yaptıkları tercihlere ve aldıkları puanlara göre bu kontenjanlara yerleştirilmektedir. ÖSYM tarafından hazırlanan Tıpta Uzmanlık Sınavı (TUS) başvuru kılavuzlarında Sağlık Bakanlığı adına tıp fakültelerinde uzmanlık eğitimi yaptırılması için tahsis edilen kadrolar hakkında adaylar bilgilendirilmektedir. Dolayısıyla, adaylar bu kadroları tercih ettikleri takdirde hangi haklara sahip ve hangi yükümlülüklerle tabi olacaklarını önceden bilmekte ve tercihlerini kendi özgür iradeleriyle bilerek ve isteyerek yapmaktadır. Adayların serbest iradeleriyle yaptıkları tercihin sonucu olarak aldıkları uzmanlık eğitimi süresi kadar mecburi hizmet yükümlülüğü altına girmeleri zorla çalıştırma olarak değerlendirilemez.

Ayrıca, Sağlık Bakanlığı adına tıp fakültelerinde uzmanlık eğitimi yapanlara 'uzmanlık eğitimi süresi kadar' bir mecburi hizmet yükümlülüğü öngörüldüğü dikkate alındığında, mecburi hizmet yükümlülüğünün orantısız olduğu da söylenemez.

Anayasa'nın 10. maddesinde öngörülen eşitlik ilkesi, hukuksal durumları aynı olanlar için söz konusudur. Bu ilke ile eylemleri değil hukuksal eşitlik öngörülmektedir. Eşitlik ilkesinin amacı, aynı durumda bulunan kişilerin yasalarca aynı işleme bağlı tutulmalarını sağlamak ve kişilere kanun karşısında ayırım yapılmasını ve ayrıcalık tanınmasını önlemektir. Bu ilkeyle, aynı durumda bulunan kimi kişi ve topluluklara ayrı kurallar uygulanarak kanun karşısında eşitliğin ihlali yasaklanmıştır. Kanun önünde eşitlik, herkesin her yönden ayrı kurallara bağlı tutulacağı anlamına gelmez. Durum ve konumlarındaki özellikler, kimi kişiler ya da topluluklar için değişik kuralları gerekli kılabilir. Aynı hukuksal durumlar aynı, ayrı hukuksal durumlar farklı kurallara bağlı tutulursa Anayasa'nın öngördüğü eşitlik ilkesi ihlal edilmiş olmaz.

Sağlık Bakanlığı kadrolarında bulunup bu Bakanlık adına uzmanlık eğitimi almak üzere üniversitelere bağlı tıp fakültelerinde uzmanlık ve yan dal eğitimi için görevlendirilen hekim ve dış hekimlerinin masrafları Sağlık Bakanlığı tarafından karşılandığı halde, bunların hizmetinden tıp fakülteleri yararlanmaktadır. Sağlık Bakanlığı adına tıp fakültelerinde görevlendirilen hekimler ile doğrudan kadrolarında buldukları tıp fakülteleri veya Sağlık Bakanlığına bağlı eğitim ve araştırma hastanelerinde uzmanlık ve yan dal eğitimi yapan hekimlerin aynı statüde görülmesi mümkün olmadığından bunlar arasında eşitlik karşılaştırması yapılamaz.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 10., 18. ve 48. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 5. ve 17. maddeleriyle ilgisi görülmemiştir.

36- KHK'nin 57. Maddesinin (1) ve (2) Numaralı Fıkraları

Dava dilekçesinde, serbest hekimler tarafından açılan muayenehane, poliklinik ve laboratuvarları da kapsayacak şekilde bu kuruluşlara verilecek ruhsatlar için alt sınır olmaksızın yüzellibin Türk Lirasına kadar ücret alınmasına yetki verilmesinin sağlık çalışanlarının bağımsız olarak çalışma hak ve hürriyetlerini ortadan kaldıracığı, ayrıca bu durumun idareye kapsamı ve sınırları belli olmayan bir yetkinin verilmesi anlamına geldiği, gerçek veya tüzel kişilerin sağlık alanında belirli bir hizmeti verebilmesinin açık artırma ile belirlenecek bedel karşılığında alınacak lisansa bağlı kılınmak suretiyle sağlık meslek mensuplarının diplomalarına dayalı olarak ve bir işverene bağlı olmaksızın çalışma haklarının ortadan kaldırıldığı belirtilerek kuralların, Anayasa'nın 2., 5., 7., 17., 48., 49. ve 56. maddelerine aykırı olduğu ileri sürülmüştür.

KHK'nin 57. maddesinin dava konusu (1) numaralı fıkrasıyla, Bakanlık ve bağlı kuruluşlarınca düzenlenecek veya onaylanacak her türlü ruhsatlandırma, ürün üretim ve satış izin belgesi ve mesul müdürlük belgesi ile permi ve sertifikalar üzerinden yüzellibin Türk Lirasını geçmemek üzere Bakanlıkça belirlenecek tarifelere göre ücret alınması öngörülmüştür. Bu tarifelerin her yıl güncelleneceği ve ücretlerin 213 sayılı Vergi Usul Kanunu'na göre belirlenen yeniden değerlendirme oranında artırılacağı belirtilmiştir.

Maddenin dava konusu (2) numaralı fıkrasında ise gerçek veya tüzel kişilere sağlık alanında belirli bir hizmeti verebilme veya hastane ve benzeri sağlık kuruluşları açabilme yetkisini veren lisansların açık artırma ile belirlenecek bedel karşılığında verileceği düzenlenmiştir. Söz konusu fıkrada ayrıca, lisans verilmesinin ilgili faaliyet için gerekli olan izin veya ruhsat yerine geçmeyeceği, lisans verilmesinin usul ve esaslarının Bakanlıkça belirleneceği ifade edilmiştir. Kural bir bütün olarak değerlendirildiğinde, lisans usulünün; hastane, tıp merkezi, sağlık merkezi gibi adlar altında oluşturulan ve belli standart ve nitelikler aranan sağlık hizmeti sunumu yapılan teşekküller (kuruluşlar) yönünden geçerli olduğu, herhangi bir teşekkül çatısı altında olmaksızın bireysel bir faaliyet biçiminde sağlık hizmeti sunan muayenehane ve benzeri yerleri ise kapsamadığı açıktır.

Anayasa'nın 2. maddesinde, Türkiye Cumhuriyeti'nin sosyal bir hukuk devleti olduğu belirtilmiş; 5. maddesinde de kişilerin ve toplumun refah huzur ve mutluluğunu sağlamak üzere siyasal, ekonomik ve sosyal engellerin kaldırılması devletin temel görevleri arasında sayılmıştır. Sosyal devlet, sosyal adaletin, sosyal refahın ve sosyal güvenliğin gerçekleşmesini sağlayan devlettir. Ekonomik ve mali politikalar sosyal devletin gerçekleşmesini sağlayan araçlardır.

Sosyal hukuk devleti de insan hak ve özgürlüklerine saygı gösteren, ferdin huzur ve refahını gerçekleştiren ve güvence altına alan, kişiyle toplum arasında denge kuran, özel teşebbüsün güvenlik ve kararlılık içinde çalışmasını sağlayan, çalışma hayatının gelişmesi için sosyal, iktisadi ve mali

önlemler alarak çalışanları koruyan, milli gelirin adil biçimde dağılmasını temin eden, hukuka bağlı ve gerçekçi bir özgürlük rejimini uygulayan devlettir.

Kanun koyucu, Anayasa'nın 5. maddesinde belirtilen devletin temel amaç ve görevlerini yerine getirebilmesi için anayasal ilkelere aykırı olmaması koşuluyla kamu otoritelerince yapılan iş ve işlemler karşılığında, hizmetten yararlananlardan belli bir ücret alınmasını öngörebilir. Bu itibarla Bakanlık ve bağlı kuruluşlarınca düzenlenecek veya onaylanacak her türlü ruhsatlandırma, ürün üretim ve satış izin belgesi ve mesul müdürlük belgesi ile permi ve sertifikalar karşılığında ücret alınmasının öngörülmesinin Anayasa'ya aykırı bir yönü bulunmamaktadır.

Dava konusu (1) numaralı fıkrada, hangi işlemlerin ücrete tabi olduğu tek tek sayılarak gösterilmiştir. Ayrıca, bu işlemler için alınabilecek ücretin üst sınırı yüzellibin Türk Lirası olarak belirlenmek suretiyle Bakanlığa tanınan yetkinin kapsamı ve sınırları çizilmiştir. Dolayısıyla, yürütme organına sınırsız bir yetki verildiğinden söz edilemez.

Anayasanın 56. maddesinde, 'Devlet, herkesin hayatını, beden ve ruh sağlığı içinde sürdürmesini sağlamak; insan ve madde gücünde tasarruf ve verimi artırarak, işbirliğini gerçekleştirmek amacıyla sağlık kuruluşlarını tek elden planlayıp hizmet vermesini düzenler. Devlet, bu görevini kamu ve özel kesimlerdeki sağlık ve sosyal yardım kurumlarından yararlanarak, onları denetleyerek yerine getirir.' denilmiştir. Sağlık kuruluşlarının ülke çapında dengeli bir şekilde dağılımını sağlamak üzere planlamalar yapmakla görevli olan Sağlık Bakanlığının, özel hastane ve benzeri sağlık kuruluşu açmak isteyen gerçek ve tüzel kişilerin uymakla yükümlü olacakları kuralları da belirlemesinin, kişilerin sağlığının korunması ve geliştirilmesi görevinin bir parçası olduğu açıktır. Bu çerçevede belli bir sağlık hizmetini verebilmek için veya hastane ve benzeri sağlık kuruluşları açabilmek için lisans verilmesi yönteminin uygulanması da, sağlık hizmetlerinin planlanması ve bu alanda hizmet sunmak isteyenlerin tabi olacağı kuralların belirlenmesi anlamına gelmektedir. Anayasa'da sağlık kamu hizmetinin görülüş usulü bağlamında lisans yönteminin uygulanmasını engelleyen bir düzenleme de bulunmadığından hastane, tıp merkezi, sağlık merkezi gibi adlar altında oluşturulmuş kuruluşlar aracılığıyla özel sağlık hizmeti sunulabilmesi için lisans usulünün öngörülmesinde Anayasa'ya aykırı bir yön bulunmamaktadır.

Açıklanan nedenlerle, dava konusu kurallar Anayasa'nın 2., 5., 7., 48 ve 56. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir.

Kuralların, Anayasa'nın 17. ve 49. maddeleriyle ilgisi görülmemiştir.

37- KHK'nin 58. Maddesinin (6) Numaralı Fıkrasının (e) Bendi ile (7) Numaralı Fıkrasının (a) Bendiyle Değiştirilen 3359 Sayılı Kanun'un Ek 1. Maddesinin Üçüncü Fıkrası ve Geçici 6. Maddesi

Dava dilekçesinde, dava konusu kurallarla, klinik şefi ve şef yardımcılarının kadro ve unvanlarının kaldırıldığı ve karşılığında eşdeğer bir kadronun oluşturulmadığı, eğitim görevlisi kadrolarına kazanılmış hak aylık dereceleriyle atanmış olmalarına rağmen klinik şefleri ve şef yardımcılarının hiyerarşik konumu, klinik içerisindeki amirlik pozisyonlarının gözetilmediği, ayrıca kurallarla yeni bir kadro ihdas edilerek göreve başlama ve göreve son verme işlemlerinin kanun ile tesis edilmiş olduğu, KHK ile getirilen hastane yöneticilerinin eğitimci, hatta hekim bile olma zorunluluğunun olmadığı, bu kişilerin Sağlık Bakanlığına bağlı eğitim ve araştırma hastanelerinde eğitim sorumlusu ve idari sorumlu uzmanını seçme yetkisine sahip kılınmasının yüksek öğretime ilişkin anayasal ilkelere aykırı olduğu belirtilerek kuralların, Anayasa'nın 2., 17., 36., 56. ve 128. maddelerine aykırı olduğu ileri sürülmüştür.

7.5.1987 günlü, 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun ek 1. maddesinin önceki hâlinde, Sağlık Bakanlığı eğitim ve araştırma hastanelerinde tıpta uzmanlık eğitimi vermek üzere klinik şefi ve klinik şef yardımcısı kadrolarına yer verilmiş ve bu kadrolarda görev yapan kişilerin aynı zamanda eğitim sorumlusu olmaları öngörülmüştür. KHK'nin 58. maddenin (7) numaralı fıkrasının (a) bendiyle, 3359 sayılı Kanun'un ek 1. maddesi bütünüyle değiştirilmiş ve maddenin yeni hâlinde klinik şefi ve klinik şef yardımcısı kadrolarına yer verilmemiştir. Ayrıca, önceki düzenlemeye göre klinik şefi ve klinik şef yardımcısında toplanan eğitim sorumluluğu ve idari sorumluluk birbirinden ayrılmıştır. Anılan maddenin dava konusu üçüncü fıkrasıyla, Sağlık Bakanlığına bağlı eğitim ve araştırma hastanelerinde, ilgili birimin eğitim sorumlusunun, eğitim görevlileri arasından; idari sorumlusunun da ilgili daldaki uzmanlar arasından hastane yöneticisi tarafından bir yıl süreyle görevlendirileceği, birimin eğitim sorumlusuna aynı zamanda idari sorumluluk da verilebileceği düzenlenmiştir.

Buna paralel olarak KHK'nin 58. maddesinin dava konusu (6) numaralı fıkrasıyla, 657 sayılı Kanun'un ek 33. maddesindeki tablonun (a) sırasında geçen 'Klinik şefi, şef yardımcısı' ibareleri 'Eğitim görevlisi' şeklinde değiştirilmiştir.

Ayrıca KHK'nin geçici 6. maddesiyle, KHK'nin yayımlandığı tarihte görevde bulunan şef ve şef yardımcılarının bu görevlerinin sona ermesi ve bunların eğitim görevlisi olarak atanmış sayılmaları öngörülmüştür.

Anayasa'nın 2. maddesinde belirtilen hukuk devleti, eylem ve işlemleri hukuka uygun, insan haklarına dayanan, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adaletli bir hukuk düzeni

kurup bunu geliştirerek sürdüren, hukuk güvenliğini sağlayan, bütün etkinliklerinde hukuka ve Anayasa'ya uyan, işlem ve eylemleri bağımsız yargı denetimine bağlı olan devlettir. Kanunların kamu yararının sağlanması amacına yönelik olması, genel, objektif, adil kurallar içermesi ve hakkaniyet ölçütlerini gözetmesi hukuk devleti olmanın gereğidir. Bu nedenle kanun koyucunun hukuki düzenlemelerde kendisine tanınan takdir yetkisini anayasal sınırlar içinde adalet, hakkaniyet ve kamu yararı ölçütlerini göz önünde tutarak kullanması gerekir.

Anayasa'nın 2. maddesindeki 'hukuk devleti' ilkesi gereğince, yasama işlemlerinin kişisel yararları değil kamu yararını gerçekleştirmek amacıyla yapılması zorunludur. Bir kuralın Anayasa'ya aykırılık sorunu çözümlenirken 'kamu yararı' konusunda Anayasa Mahkemesinin yapacağı inceleme yalnızca kanunun kamu yararı amacıyla yapılıp yapılmadığı ile sınırlıdır. Kanun ile kamu yararının ne kadar gerçekleşip gerçekleşmeyeceğini denetlemenin anayasa yargısıyla bağdaşmayacağı, bunun kanun koyucunun takdirinde olduğu açıktır.

KHK ile Sağlık Bakanlığına bağlı hastanelerin yönetiminde yeni bir sisteme geçilmiştir. Yeni sistemde, önceki mevzuatta olmayan, kamu hastaneleri birliği genel sekreteri, hastane yöneticisi gibi birçok yeni yöneticiye yer verilmiştir. Dava konusu kurullarla da önceki dönemde klinik şefi ve şef yardımcısı olarak istihdam edilen ve bu nedenle çalıştıkları birimlerde yönetici pozisyonunda bulunan bir kısım görevlilerin unvanı eğitim görevlisi olarak değiştirilmiş ve bunların yeni düzende eğitim görevlisi hekim olarak çalışmalarını öngörülmesi, buna karşılık gerek eğitim sorumlusu gerekse idari sorumlu biçimindeki yönetici konumları sona erdirilmiştir.

Kanun koyucu, kamu yararı ve hizmetin gereklerini dikkate alarak kamu görevlilerinin statüsünde, bunların unvanlarında, görev ve yetkilerinde değişiklikler yapabilir. KHK'nin genel gerekçesinden anlaşılacağı üzere, sağlık politikalarının belirlenmesi, düzenleme ve denetim yapılması, hizmet sunumu görev ve yetkilerinin merkezî bir yapıyla Sağlık Bakanlığında toplanmasının yarattığı sakıncaların giderilmesi ve çağdaş bir yönetim anlayışının bir gereği olarak Bakanlıkça sunulan hizmetlerin fonksiyonel olarak tasnifi amacıyla Sağlık Bakanlığının teşkilat yapısının değiştirildiği, bununla bağlantılı olarak yeni bazı unvanların oluşturulduğu ve eski bazı unvanların ise kaldırıldığı anlaşılmaktadır. Gösterilen bu amacın kamu yararına dönük olduğu açıktır. Yeni teşkilat yapısıyla kamu yararının gerçekleşip gerçekleşmeyeceği anayasallık denetiminin kapsamı dışındadır. Öte yandan, yönetici durumda bulunan bir kamu görevlisinin (hekimin) bütün meslek hayatı boyunca aynı konumu sürdürmesini gerektiren bir anayasal zorunluluk bulunmadığından klinik şefi ve şef yardımcılarının unvanlarının eğitim görevlisi olarak değiştirilmesinde Anayasa'ya aykırı bir yön yoktur.

Dava dilekçesinde, Sağlık Bakanlığına bağlı eğitim ve araştırma hastanelerinde uzman hekim yetiştirilmesinde görev alacak olan eğitim görevlilerinin seçiminde hastane yöneticisinin belirleyici olmasının bilimsel özerklik ilkesiyle bağdaşmadığı ileri sürülmüştür.

Üniversitelerde ya da Sağlık Bakanlığına bağlı bir birimde yöneticilik görevine getirilecek kişilerin atanmalarında veya görevlendirilmelerinde bir idari birimin görevli ve yetkili olması kaçınılmaz olup, bu idari birim yöneticisinin sağlık meslek mensubu olup olmamasının bilimsel özerklik ilkesiyle bir ilgisi bulunmamaktadır.

Dava konusu kurallarla tek bir kişi hakkında bireysel nitelikte bir yürütme işlemi tesis edilmeyip, aksine genel ve soyut bir kural getirilmektedir. Soyut bir kuralın gerçekte tek bir kişiyi ya da sınırlı sayıda kişiyi ilgilendiriyor olması onun soyut niteliğini ortadan kaldırmaz. Bireysel nitelikte bir işlemde söz edilebilmesi için somut olarak bir kişinin hukuki durumunda değişiklik yapan bir irade açıklamasının bulunması gerekir. Dava konusu kuralla doğrudan somut bazı kişilerin hukuki durumunda değişiklik yapılmasına yönelik bir düzenleme bulunmadığından bireysel işlemin varlığından söz edilemez. Kuralda belirtilen kadrolarda görev yapan kişilerin hukuki durumlarının, düzenlemenin sonucundan etkilenmiş olması bu neticeyi değiştirmez.

Ayrıca, KHK'nin geçici 6. maddesiyle, KHK'nin yayımlandığı tarihte görevde bulunan şef ve şef yardımcılarının bu görevlerinin sona ermesi ve bunların eğitim görevlisi olarak atanmış sayılmalarının öngörülmesi, anılan kadroların kaldırılması sonucu ortaya çıkan hukuki ve fiili zorunluluklar nedeniyledir. Buna göre, söz konusu işlemin sebep unsuru, Sağlık Bakanlığının teşkilatının değiştirilmesi olup yürürlükte bulunan kanunlara dayanılarak ve kamu görevlisinin öznel durumu dikkate alınarak idarece tesis edilen naklen atama işlemlerinden tamamen farklıdır. Söz konusu hukuki ve fiili zorunluluklar nedeniyle kazanılmış haklar korunarak başka kadrolara atama yapılması, kanun koyucunun takdir alanı içindedir.

Açıklanan nedenlerle, dava konusu kurallar Anayasa'nın 2. ve 36. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir.

Kuralların, Anayasa'nın 17., 56. ve 128. maddeleriyle ilgisi görülmemiştir.

Mehmet ERTEN, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŞ bu görüşe katılmamışlardır.

38- KHK'nin 58. Maddesinin (8) Numaralı Fıkrasının (a) Bendiyle Değiştirilen 1219 Sayılı Kanun'un 1. Maddesi ile (b) Bendiyle 1219 Sayılı Kanun'un 4. Maddesinin Birinci Cümlesinde Yapılan Değişiklik

Dava dilekçesinde, hekim olarak çalışabilmek için gerekli vatandaşlık koşulunun kaldırılmasının, dışarıdan yabancı sağlık personelinin gelmesine değil, yabancı sağlık personeli çalıştırılabileceği tazyiki ile ülkemizdeki çalışanların ücretlerinin düşürülmesine yönelik olduğu, yabancı hekimlerin ülkemizde çalışmalarına yönelik yeterli derecede Türkçe dil bilgisinin aranmasına, mesleki disiplin ve yaptırımlara, yeterlilik ölçümüne, mesleki kusurlarda zarar görenlerin haklarının güvence altına alınmasına yönelik düzenlemelerin yapılmadığı, doğru tanı konulabilmesi ve hastanın rızasının alınabilmesi için hastayla hekimin kullandığı dilin ortak olmasına ihtiyaç bulunduğu, yabancı hekimlerin ülkemizde çalışmalarına yönelik yeterli derecede Türkçe dil bilgisinin aranmamasının kişinin maddi ve manevi varlığını geliştirme hakkının ihlal edilmesi sonucunu yaratacağı, ülkemizde hekim sayısında yetersizlik olmadığı, kimi yerlerdeki sağlık personeli azlığının dağılımdaki dengesizlikten kaynaklandığı, yabancı hekim çalıştırılmasının Türk vatandaşı hekimlerin haklarının korunmadığı anlamına geldiği belirtilerek dava konusu kuralların, Anayasa'nın 2., 5., 17., 49. ve 56. maddelerine aykırı olduğu ileri sürülmüştür.

6216 sayılı Kanun'un 43. maddesine göre, ilgisi nedeniyle dava konusu kural, Anayasa'nın 16. ve 48. maddeleri yönünden de incelenmiştir.

KHK'nin 58. maddesinin (8) numaralı fıkrasının (a) bendiyle 1219 sayılı Kanun'un 'Türkiye Cumhuriyeti dâhilinde tababet icra ve her hangi surette olursa olsun hasta tedavi edebilmek için Türkiye Darülfünunu Tıp Fakültesinden diploma sahibi olmak ve Türk bulunmak şarttır. 'biçimindeki 1. maddesi, 'Türkiye Cumhuriyeti dâhilinde tababet icra ve her hangi surette olursa olsun hasta tedavi edebilmek için tıp fakültesinden diploma sahibi olmak şarttır.' şeklinde değiştirilmek suretiyle Türkiye'de hekim olarak çalışabilmek için Türk vatandaşı olma şartının kaldırıldığı anlaşılmıştır.

KHK'nin 58. maddesinin (8) numaralı fıkrasının (b) bendiyle, aynı Kanun'un 4. maddesinin, yabancı memleketlerin tıp fakültelerinden mezun Türk hekimlerinin Türkiye'de hekimlik yapabilme koşullarını düzenleyen birinci cümlesindeki 'Türk hekimlerinin' ibaresi 'hekimlerin' şeklinde değiştirilerek yurt dışındaki üniversitelerin tıp fakültelerinden mezun olan yabancıların da Türkiye'de hekimlik yapabilmeleri olanaklı kılınmıştır.

Anayasa'nın 48. maddesinde 'Herkes dilediği alanda çalışma ve sözleşme hürriyetine sahiptir.' hükmü yer almaktadır. Bu maddede düzenlenen çalışma hakkının öznesi 'herkes' olarak belirlenmek suretiyle bu hak sadece Türk vatandaşları için değil, kural olarak yabancılar yönünden de güvence altına alınmıştır. Ancak, Anayasa'nın 16. maddesine göre, yabancıların çalışma hakları milletlerarası hukuka uygun olarak kanunla sınırlanabilir. Nitekim Türk hukukunda birçok iş ya da mesleğin icrası

çeşitli kanunlarla yabancılara yasaklanmıştır. Bununla birlikte Anayasa'nın 16. maddesinde yabancıların hak ve hürriyetlerinin sınırlandırılması emredilmemekte bu konuda yasama organına izin verilmektedir. Dolayısıyla kanun koyucu, ülkenin koşullarını dikkate alarak yabancıların hangi iş ya da meslekleri yapıp yapamayacakları konusunda karar vermeye yetkilidir.

Anayasa'nın 56. maddesiyle devlete yüklenen herkesin hayatını, beden ve ruh sağlığı içinde sürdürmesini sağlama ödevi, ülkede yeterli miktarda nitelikli sağlık personeli istihdamı için gerekli her türlü tedbirin alınmasını gerektirmektedir. Bu anayasal gerekler dikkate alınarak sağlık hizmetlerinin asli unsuru olan hekim ihtiyacının karşılanması amacıyla yabancı doktorlara yönelik Türkiye'de çalışma yasağının kaldırılması, çalışacaklarda aranan nitelikler ve çalışma şartlarının düzenlenmesinin kanun koyucunun takdir yetkisi kapsamında olduğu açıktır.

Açıklanan nedenlerle, dava konusu kurallar Anayasa'nın 16., 48. ve 56. maddelerine aykırı değildir. İptal istemlerinin reddi gerekir.

Kuralların Anayasa'nın 2., 5., 17. ve 49. maddeleriyle ilgisi görülmemiştir.

Serdar ÖZGÜLDÜR ile Osman Alifeyyaz PAKSÜT bu görüşe katılmamışlardır.

39- KHK'nin 58. Maddesinin (8) Numaralı Fıkrasının (b) Bendiyle 1219 Sayılı Kanun'a Eklenen Geçici Madde 9

Dava dilekçesinde, aile hekimliğinin bir uzmanlık dalı olduğu, tıp fakültesi mezuniyetini takiben girilebilen TUS ile hak kazanılan üç yıllık bir uzmanlık eğitiminden sonra aile hekimliği uzmanı unvanının kazanılabildiği, bu uzmanlık eğitiminin teorik eğitimin yanında uygulamalı tıp eğitimi de içerdiği, aile hekimliği uzmanlık eğitiminin, diğer uzmanlık eğitimleri gibi eğitim kurumlarında tam gün esasına göre ve eğitim sorumlularının nezaretinde yürütüldüğü, bu yöntemden yalnızca sözleşmeli aile hekimi olarak çalışan hekimler yönünden ayrılmayı gerektiren bir nedenin olmadığı, bu hekimlerin farklı koşullara tabi tutularak hizmet içi eğitim sonucunda uzmanlık yetkisi almasının, Anayasa'nın 2., 10. ve 130. maddelerine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralla, 24.11.2004 günlü, 5258 sayılı Aile Hekimliği Kanunu hükümlerine göre sözleşmeli aile hekimi olarak çalışmakta olanların, tıpta uzmanlık sınavı sonuçlarına göre, merkezî yerleştirmeye tabi olmaksızın, Tıpta Uzmanlık Kurulunca belirlenen esaslar çerçevesinde aile hekimliği uzmanlık eğitimi yapabilmeleri olanaklı kılınmıştır. Sözleşmeli aile hekimlerine yönelik olarak getirilen bu olanak, 1.1.2020 tarihiyle sınırlandırılmıştır. Bu eğitim, uzaktan ve/veya kısmi zamanlı eğitim metotları da uygulanmak suretiyle yapılabilecek ve en az altı yılda tamamlanacaktır. Uzmanlık eğitimi süresince aile hekimliği sözleşmesi devam edecektir. Uzmanlık eğitimi ile beraber

aile hekimliđi hizmetlerinin yrtlmesine ve ilgililere denecek cretlere iliřkin usul ve esaslar ıkarılacak ynetmelikle belirlenecektir. Bu erevede yapılacak aile hekimliđi uzmanlık eđitiminde ekirdek eđitim mfredatı, rotasyonların uygulanması ve eđitimin řekli ile diđer hususlar Tıpta Uzmanlık Kurulunca saptanacaktır.

Dava konusu kuralla, szleřmeli aile hekimleri ynnden olađan aile hekimliđi uzmanlık eđitimine nazaran daha farklı bir eđitim ynteminin ngrldđ aıktır. Bu noktada en belirgin farklılık, sz edilen kiřilerin bir yandan szleřmeli aile hekimi olarak alıřmaya devam ederken, diđer yandan da aile hekimliđi uzmanlık eđitimini alabilecek olmalarıdır. Ayrıca, olađan aile hekimliđi uzmanlık eđitiminin sresi  yıl olarak ngrlmřken, szleřmeli aile hekimleri, aile hekimliđi uzmanlık eđitimini en az altı yılda tamamlayabileceklerdir. Bu sre farklılıđı szleřmeli aile hekimlerinin bir yandan aile hekimi olarak alıřıp diđer yandan da aile hekimliđi uzmanlık eđitimi alacak olmalarından kaynaklanmaktadır. Bu eđitim, uzaktan eđitim ve kısmi zamanlı eđitim metotları da uygulanarak gerekleřtirilebileceđi iin eđitimin daha geniř bir zamana yayılmasına ihtiya duyulduđu anlařılmaktadır. Bununla birlikte, aile hekimliđi uzmanlık eđitiminin ieriđi ve ařamalarının szleřmeli aile hekimleri ynnden deđiřtirilmesi sz konusu deđildir. Diđer bir ifadeyle bir aile hekimliđi uzmanı hangi ařamalardan geip de uzman oluyorsa szleřmeli aile hekimleri de aynı ařamalardan geeceklerdir.

Ayrıca, szleřmeli aile hekimlerinin alacađı aile hekimliđi uzmanlık eđitiminin Tıpta Uzmanlık Kurulunca belirlenecek esaslar erevesinde yrtleceđi ve eđitim mfredatı ile rotasyonların uygulanması ve eđitimin řekli ile sair hususların Kurul tarafından belirleneceđi kuralda aıka ifade edilmiřtir. Bu itibarla, aile hekimi aıđının giderilmesi amacıyla ve geici bir sreyle, olađan aile hekimliđi uzmanlıđı eđitimi ynteminden farklı olarak daha esnek bir eđitim metodunun uygulanmasının Anayasa'ya aykırı bir yn bulunmamaktadır.

Aıklanan nedenlerle, dava konusu kural Anayasa'nın 2. ve 130. maddelerine aykırı deđildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 10. maddesiyle ilgisi grlmemiřtir.

40- KHK'nin 58. Maddesinin (13) Numaralı Fıkrasının (b) Bendiyle Deđiřtirilen 209 Sayılı Kanun'un 3. Maddesinin Birinci Fıkrasının (d) Bendi

Dava dilekesinde, kamu hastanelerinin iřlevinin ikinci ve nc basamak sađlık hizmetlerini nitelikli, eřit ve ulařılabilir bir biimde lkemizdeki insanlara sunmak olduđu, bu hastanelerin birer ticarethane olmadıđı, yabancı hastalardan gelir elde etmek zere rgtlenip ynetilemeyeceđi, dava

konusu düzenlemenin devletin temel amacını sađlıđı korumaktan kâr elde etmeye dönüştürdüđü belirtilerek kuralın, Anayasa'nın 2., 5. ve 56. maddelerine aykırı olduđu ileri sürülmüştür.

KHK'nin 58. maddesinin (13) numaralı fıkrasının (b) bendiyle, 209 sayılı Kanun'un 3. maddesinde deđişiklik yapılmıştır. 209 sayılı Kanun'un 3. maddesi, Sađlık Bakanlıđına bađlı kurum ve kuruluşlar ile bađlı kuruluşlardaki hangi mal ve hizmetlerden elde edilecek gelirlerin döner sermayeye gelir kaydedileceđini düzenlemektedir. Anılan maddenin dava konusu (d) bendinde yer alan düzenleme uyarınca Sađlık Bakanlıđı, yabancı hastalara verilen sađlık hizmetlerini fiyatlandırmaya ve bu hizmetlerden elde edilecek gelirleri döner sermayeye gelir kaydettirmeye yetkilidir.

Anayasa'da sađlık hizmetlerinden faydalanma hakkı, sadece vatandaşların sahip olduđu bir hak olarak deđil, 'herkes'in sahip olduđu bir hak olarak düzenlenmiştir. Bu haktan yararlanan vatandaşlar dahi, sosyal güvenlik sistemine dâhil olsalar bile faydalandıkları hizmetin karşılıđı olarak belli bir katkı payı ödemektedir. Bu durum karşısında yabancıların ülkemizdeki kamu hastanelerinden sađlık hizmeti almaları halinde bu hizmetin bedelinin tamamının veya bir kısmının kendilerinden istenilmesinde ve bunun da döner sermayeye gelir kaydedilmesinde Anayasa'ya aykırı bir yön bulunmamaktadır.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 5. ve 56. maddelerine aykırı deđildir. İptal isteminin reddi gerekir.

41- KHK'nin Geçici 4. Maddesinin (1) Numaralı Fıkrası

Dava dilekçesinde ve başvuru kararlarında, kuralın, kamu yararının gerektirdiđi zorunluluk nedeniyle deđil, sadece mevcut idarecileri görevden almak ve kadrolaşmak amacıyla getirildiđi, bu hükümlerle görevleri sona erdirilerek bakanlık müşaviri ve araştırmacı unvanlı kadrolara atanan kişilerin ücretleri dondurularak kazanılmış haklarının ihlal edildiđi, idari bir işlemle yapılması gereken görevden alma işleminin kanun ile yapıldıđı ve bu yolla dava açma hakkının engellendiđi, bakanlık müşaviri ve araştırmacı olarak atananların Bakanın uygun göreceđi merkez veya taşra teşkilatına ait birimlerde çalıştırılmasının öngörülmesinin keyfi uygulamalara yol açabileceđi, adı geçenlerin görev tanımlarının belli olmadığı belirtilerek kuralın, Anayasa'nın 2., 36. ve 125. maddelerine aykırı olduđu ileri sürülmüştür.

KHK ile Sađlık Bakanlıđı ve bađlı kuruluşları yeniden yapılandırılmış, önceki teşkilat yapısından farklı yeni hizmet birimleri oluşturulmuş, Türkiye Kamu Hastaneleri Kurumu, Türkiye Halk Sađlığı Kurumu, Türkiye İlaç ve Tıbbî Cihaz Kurumu, Türkiye Hudut ve Sahiller Sađlık Genel Müdürlüğü adlarını taşıyan yeni bađlı kuruluşlar meydana getirilmiştir. Teşkilat yapısında meydana gelen bu

değişiklikler mevcut personelin hukuki durumlarını da etkilemiştir. KHK'nin geçici 4. maddesinin dava konusu kural olan (1) numaralı fıkrasında, Bakanlığın ve bağlı kuruluşlarının teşkilat yapısının değiştirilmesi sonucu açığa çıkan yönetici personelin durumu düzenlenmektedir. Buna göre, Bakanlık ve bağlı kuruluşlarının merkez ve taşra teşkilatında üst düzey görevlerde bulunan kamu görevlilerinin bu görevlerinin sona ermesi ve bunlardan il sağlık müdürlüğü ve üstü kadrolarında bulunanların Bakanlık müşaviri, diğerlerinin ise araştırmacı kadrolarına hâlen buldukları kadro dereceleriyle atanmış sayılmaları öngörülmektedir. Bu madde uyarınca ihdas edilen bakanlık müşaviri ile araştırmacı kadrolarının herhangi bir sebeple boşalması halinde hiçbir işleme gerek kalmaksızın iptal edilmiş sayılacakları belirtilmiştir. Bu fıkra göre bakanlık müşaviri ve araştırmacı kadrolarına atanmış sayılanların, Bakanın uygun göreceği merkez veya taşra teşkilatına ait birimlerde çalıştırılabileceği kuralına yer verilmiştir.

Anayasa'nın 2. maddesindeki 'hukuk devleti' ilkesi gereğince, yasama işlemlerinin kişisel yararları değil kamu yararını gerçekleştirmek amacıyla yapılması zorunludur. Bir kuralın Anayasa'ya aykırılık sorunu çözümlenirken 'kamu yararı' konusunda Anayasa Mahkemesinin yapacağı inceleme yalnızca kanunun kamu yararı amacıyla yapılıp yapılmadığı ile sınırlıdır. Kanun ile kamu yararının gerçekleşip gerçekleşmeyeceğini denetlemenin anayasa yargısıyla bağdaşmayacağı, bunun kanun koyucunun takdirinde olduğu açıktır.

KHK'nin genel gerekçesinde, halihazır yapıya göre sağlık politikalarının belirlenmesi, düzenleme ve denetim yapılması, hizmet sunumu görev ve yetkilerinin merkeziyetçi bir yapıyla Sağlık Bakanlığında toplandığı belirtilerek bu durumun yarattığı sakıncalardan söz edildikten sonra söz konusu olumsuzlukların giderilmesi ve çağdaş bir yönetim anlayışının bir gereği olarak Bakanlıkça sunulan hizmetlerin fonksiyonel olarak tasnifi amacıyla KHK'nin hazırlandığı ifade edilmiştir. Dolayısıyla, kanun koyucunun amacının kamu yararını sağlamaya dönük olduğu anlaşılmaktadır. Bunun ötesinde yapılan somut düzenlemenin bu amaçları etkin bir şekilde gerçekleştirmeye elverişli olup olmadığı yönündeki bir değerlendirme ise anayasallık denetiminin kapsamı dışındadır.

Anayasa'nın 2. maddesinde yer alan hukuk devleti ilkesinin temel gereklerinden biri kazanılmış haklara saygı gösterilmesidir. Kazanılmış haklara saygı, hukuk güvenliği ilkesinin bir sonucudur. Kazanılmış hak, kişinin bulunduğu statüden doğan, tahakkuk etmiş ve kendisi yönünden kesinleşmiş ve kişisel alacak niteliğine dönüşmüş haktır. Dava konusu kuralda kişilerin bulunduğu statülerden doğan, tahakkuk etmiş ve kendileri yönünden kesinleşmiş ve kişisel alacak niteliğine dönüşmüş haklara yönelik bir düzenleme öngörülmediğinden kazanılmış hakları ihlal eden bir müdahale söz konusu değildir.

Bu kişilerin Bakanın uygun göreceği merkez veya taşra teşkilatına ait birimlerde çalıştırılabilmesinin olanaklı kılınmasının hukuki güvenlik ilkesinin ihlaline yol açtığı da söylenemez. Zira dava konusu kuralla oluşturulan şahsa bağlı Bakan müşaviri ve araştırmacı kadroları esas itibarıyla anılan kadrolarla ilişkilendirilenlerin kazanılmış mali haklarının korunması amacına yönelik olup yerine getirilmesi gereken görevler yönünden herhangi bir hak bahşetmemektedir. Bu kişilerin Bakan müşaviri ve araştırmacı kadrolarına tanınan mali haklardan yararlanmaları, kendi hizmet sınıfına ve sınıfının içindeki derecesine uygun görevlerde çalıştırılmalarına engel teşkil etmemektedir. Hangi hizmet sınıfına ve derecesine ne tür görevler bağlandığı kanunlarda ve ilgili ikincil mevzuatta açıkça belirlenmiştir. Dava konusu kuralla Bakan müşaviri ve araştırmacı kadrolarına atananların, kendi hizmet sınıfı ve derecesine uygun olarak kanunlarda öngörülen görevlerde çalıştırılabilecekleri açık olduğundan hukuki güvenlik ilkesinin ihlalinin söz edilemez.

Diğer taraftan, dava konusu kuralla tek bir kişi hakkında bireysel nitelikte bir yürütme işlemi tesis edilmeyip, aksine genel ve soyut bir kural getirilmektedir. Soyut bir kuralın gerçekte tek bir kişiyi ya da sınırlı sayıda kişiyi ilgilendiriyor olması onun soyut niteliğini ortadan kaldırmaz. Bireysel nitelikte bir işlemde söz edilebilmesi için somut olarak bir kişinin hukuki durumunda değişiklik yapan bir irade açıklamasının bulunması gerekir. Dava konusu kuralla doğrudan somut bazı kişilerin hukuki durumunda değişiklik yapılmasına yönelik bir irade açıklamasında bulunulmadığından bireysel işlemin varlığından söz edilemez. Kuralda belirtilen kadrolarda görev yapan kişilerin hukuki durumlarının düzenlemenin sonucundan etkilenmiş olması, bu neticeyi değiştirmez.

Ayrıca, dava konusu kuralla, teşkilat yapısı değiştirilen Sağlık Bakanlığı ve bağlı kuruluşlarının bazı kadrolarında görev yapan kamu görevlilerinin bakanlık müşaviri ve araştırmacı kadrolarına atanmış sayılmalarının öngörülmesi, anılan Bakanlığın yeniden teşkilatlandırılması sonucu ortaya çıkan hukuki ve fiilî zorunluluklar nedeniyledir. Buna göre, söz konusu işlemin sebep unsuru, Sağlık Bakanlığının yeniden teşkilatlandırılması olup yürürlükte bulunan kanunlara dayanılarak ve kamu görevlisinin öznel durumu dikkate alınarak idarece tesis edilen naklen atama işlemlerinden tamamen farklıdır. Söz konusu hukuki ve fiilî zorunluluklar nedeniyle kazanılmış haklar korunarak başka kadrolara atama yapılması, kanun koyucunun takdir alanı içindedir.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 36. ve 125. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

42- KHK'nin Geçici 4. Maddesinin (3) Numaralı Fıkrası

Dava dilekçesinde, Sağlık Bakanlığında önceden müfettiş unvanıyla çalışan kişilerin unvanlarının sağlık denetçisine dönüştürülmesinin kazanılmış hakların ihlali anlamına geldiği belirtilerek kuralın, Anayasanın 2. ve 112. maddelerine aykırı olduğu ileri sürülmüştür.

KHK ile mülga 181 sayılı KHK döneminde danışma ve denetim birimi olarak doğrudan bakana bağlı faaliyet gösteren Teftiş Kurulu Başkanlığı kaldırılarak, denetim hizmetlerini yürütmek üzere Denetim Hizmetleri Başkanlığı kurulmuştur. Ayrıca, önceki düzenlemeye göre denetim hizmetlerini yürütmek üzere oluşturulan başmüfettiş, müfettiş ve müfettiş yardımcısı kadroları da sağlık başdenetçisi, sağlık denetçisi ve sağlık denetçi yardımcısı kadrolarına dönüştürülmüştür.

Dava konusu kuralla, maddenin yayımı tarihinde başmüfettiş, müfettiş ve müfettiş yardımcısı kadrolarında bulunanların buldukları kadro dereceleriyle Bakanlık ve bağlı kuruluşlarının sağlık başdenetçisi, sağlık denetçisi ve sağlık denetçi yardımcısı kadrolarına atanacakları ifade edilmiştir. Bunların başmüfettiş, müfettiş ve müfettiş yardımcısı kadrolarında geçirdikleri sürelerin sağlık başdenetçisi, sağlık denetçisi ve sağlık denetçi yardımcısı kadrolarında geçmiş sayılacağı kuralına yer verilmiştir.

Kamu hukuku alanında gerek kanunla gerekse düzenleyici işlemlerle konulmuş kuralların, kamu yararı ve hizmetin gerekleri dikkate alınarak her zaman değiştirilebileceği veya kaldırılabilirliği açıktır. Hukuk alanında meydana gelebilecek bu değişiklik, daha önce kural tasarrufların doğurmuş olduğu objektif ve genel hukuki durumlara da uygulanabilecektir. Soyut ve genel hukuki durumların (statülerin) en önemli özelliği bunların daima değişebilmesi ve bu değişikliğin de herkese karşı geçerli olmasıdır. Hukuk alanında meydana gelen ve hukuki statüde değişiklik yapan bu düzenlemeler, eski düzenleme uyarınca statü kazanmış ve statüsü devam eden bireyleri de kapsar. Dolayısıyla, nesnel hukuki durumların (statülerin) kazanılmış hak bahşetmesi mümkün değildir.

Dava konusu kuralla, önceden başmüfettiş, müfettiş ya da müfettiş yardımcısı unvanlı kadrolarda çalışmakta olan kişiler, sağlık başdenetçisi, sağlık denetçisi ya da sağlık denetçi yardımcısı unvanlı kadrolara aktarılmışlardır. Kuralda, anılan kişilerin bulunduğu statülerden doğan, tahakkuk etmiş ve kendileri yönünden kesinleşmiş ve kişisel alacak niteliğine dönüşmüş haklara yönelik bir düzenleme öngörülmediğinden kazanılmış hakları ihlal eden bir müdahale söz konusu değildir. Bu kişilerin yeni atandıkları kadrodaki mali haklarında herhangi bir değişiklik olmamış, bunların önceki maaş ve diğer özlük hakları aynen korunmuştur. Bu nedenle maddede sayılan görevlerde bulunanların kadrolarının değiştirilmesini öngören kuralın kazanılmış hakları ihlal ettiği söylenemez.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2. maddesine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın, Anayasa'nın 112. maddesiyle ilgisi görülmemiştir.

Serdar ÖZGÜLDÜR, Zehra Ayla PERKTAŞ ile Celal Mümtaz AKINCI bu görüşe katılmamışlardır.

43- KHK'nin Geçici 4. Maddesinin (4) Numaralı Fıkrası

Dava dilekçesinde, görevleri sona erdirilerek Bakanlık müşaviri ve araştırmacı unvanlı kadrolara atanan kişilerin, dava konusu kuralla ücretleri dondurulmak suretiyle kazanılmış mali haklarının da ihlal edildiği belirtilerek kuralın, Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüştür.

Dava konusu kuralla, Bakanlık müşaviri ve araştırmacı kadrolarına atanmış sayılan personele, eski kadrolarına ilişkin olarak en son ayda yapılan her türlü ödemelerin toplam net tutarının; yeni atandıkları kadrolara ait her türlü ödemelerin toplam net tutarından fazla olması halinde aradaki fark tutarın, herhangi bir vergi ve kesintiye tabi tutulmaksızın fark kapanıncaya kadar ayrıca tazminat olarak ödenmesi öngörülmektedir. Fiili çalışmaya bağlı fazla mesai ücreti ve performansa bağlı döner sermaye ek ödemesi bu hesaplamalara dâhil edilmeyecektir. Yeni atandıkları kadro unvanlarında isteğe bağlı olarak herhangi bir değişiklik olanlarla, kendi istekleriyle başka kurumlara atanarlara fark tazminatı ödenmesine son verilecektir.

Memuriyet kadro derecesine bağlanan mali haklar, o dereceye ulaşan kişi yönünden tahakkuk etmiş ve kesinleşmiş alacak niteliğine dönüştüğünden kazanılmış hak teşkil eder. Kadro derecesine bağlanan mali haklar unvandan bağımsız olduğundan, unvan değişse bile bunların hukuken korunması gerekmektedir. Buna karşılık bir görevin fiilen yapılması karşılığında ödenen mali haklar ise kazanılmış hak oluşturmaz. Bu gibi mali haklar, ilgilinin o görevi fiilen yerine getirdiği süreyle sınırlı olarak ödenir.

Dava konusu kuralda, Bakanlık müşaviri ve araştırmacı kadrolarına atanan kişilerin bulunduğu statülerden doğan, tahakkuk etmiş ve kendileri yönünden kesinleşmiş ve kişisel alacak niteliğine dönüşmüş mali haklarının (ücret ve özel hizmet tazminatı toplamının), mevcut kadrolarındakine göre daha düşük olması halinde yeni kadrolarındaki gelirlerine eşitleninceye kadar aradaki farkın ödenmesi öngörülmek suretiyle kazanılmış hakları korunmuştur. Anılan kişilerin kazanılmış mali haklarının belirlenmesinde, fiilen çalışmaya ve performansa bağlı olarak ödenen nöbet ücreti ya da döner sermaye ek ödemesinin dikkate alınmamasının Anayasa'ya aykırı bir yönü bulunmamaktadır.

Öte yandan, korunması gereken mali haklar, atama tarihinde elde edilen parasal haklar olup atama tarihinden itibaren kamu görevlisinin önceki memuriyet kadrosuyla ilişkisi kesildiğinden, bu tarihten

sonra önceki kadroya bağlanan mali hak değişikliklerinden yararlanması mümkün değildir. Dolayısıyla, dava konusu kuralla atama tarihinde elde edilen tüm parasal haklar toplamının sabit bir değer olarak kabul edilmesi, kazanılmış hak ihlaline yol açmaz.

Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2. maddesine aykırı değildir. İptal isteminin reddi gerekir.

V- YÜRÜRLÜĞÜN DURDURULMASI İSTEMİ

11.10.2011 günlü, 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin;

A- 1- 8. maddesinin (1) numaralı fıkrasının (h) ve (r) bentleri,

2- 25. maddesinin (1) numaralı fıkrasının ikinci cümlesi,

3- 33. maddesinin (5) numaralı fıkrası,

4- 58. maddesinin;

a - (7) numaralı fıkrasının;

aa- (a) bendiyle değiştirilen, 7.5.1987 günlü, 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun ek 1. maddesinin birinci fıkrası,

ab- (c) bendiyle değiştirilen 3359 sayılı Kanun'un ek 9. maddesi,

b- (13) numaralı fıkrasının (ç) bendiyle değiştirilen, 4.1.1961 günlü, 209 sayılı Sağlık Bakanlığına Bağlı Sağlık Kurumları ile Esenlendirme (Rehabilitasyon) Tesislerine Verilecek Döner Sermaye Hakkında Kanun'un 5. maddesinin altıncı fıkrası,

hakkında, 14.2.2013 günlü, E.2011/150, K.2013/30 sayılı kararla karar verilmesine yer olmadığına karar verildiğinden, bu maddeye, fıkralara, bentlere ve cümleye ilişkin yürürlüğün durdurulması istemleri hakkında KARAR VERİLMESİNE YER OLMADIĞINA,

B- Kapsam yönünden,

1- 1., 2., 3., 4., 5., 6., 7. maddeleri, 8. maddesinin (1) numaralı fıkrasının (h) ve (r) bentleri dışında kalan bölümü, 9., 10., 11., 12., 13., 14., 15. maddeleri, 16. maddesinin (2) numaralı fıkrasının birinci cümlesinde yer alan "gerçek ve", "gizli dahi olsa" ibareleri dışında kalan bölümü, 17., 18., 19., 20., 21., 22. maddeleri, 23. maddesinin (2) numaralı fıkrasının (c) ve (ç) bentleri dışında kalan bölümü ile (1), (2), (3), (4), (5), (6), (8), (9), (10), (11), (12), (13) ve (14) numaralı fıkraları, 24. maddesi, 25. maddesinin (1) numaralı fıkrasının birinci cümlesi ile (2), (3), (4), (5) ve (6) numaralı fıkraları, 26., 27., 28., 29., 30.,

31., 32. maddeleri, 33. maddesinin (5) numaralı fıkrası dışında kalan bölümü, 34., 35., 36., 37., 38., 39., 40., 41., 42., 43. maddeleri, 44. maddesinin (1) numaralı fıkrası, 45., 46. maddeleri, 47. maddesinin (4) ve (5) numaralı fıkraları, 48., 49., 50., 51., 52., 53., 54., 56., 57. maddeleri, 58. maddesinin (1), (2), (3), (4), (5), (6) numaralı fıkraları, (7) numaralı fıkrasının (a) bendiyle değiştirilen 3359 sayılı Kanun'un ek 1. maddesinin birinci fıkrası dışında kalan bölümü, (b) bendi, (8) numaralı fıkrasının (a) bendi, (b) ile 1219 sayılı Kanun'a eklenen geçici 9. madde (9), (10) ve (11) numaralı fıkraları, (13) numaralı fıkrasının (a), (b), (c) bentleri, (ç) bendiyle değiştirilen 209 sayılı Kanun'un 5. maddesinin ikinci fıkrasının 5. ve 6. cümleleri ile altıncı fıkrası dışında kalan bölümü, (d) bendi, (14) numaralı fıkrasının (ğ) bendi dışında kalan bölümü ile (15) numaralı fıkrası, geçici 1., geçici 2., geçici 3., geçici 4., geçici 5., geçici 6., geçici 7., geçici 8., geçici 9., geçici 10., geçici 11., geçici 12., 59., 60. maddeleri, eki (I) Sayılı Cetvel, (II) Sayılı Cetvel, (III) Sayılı Cetvel ile (1), (2) ve (3) sayılı listelere yönelik iptal istemleri, 14.2.2013 günlü, E.2011/150, K.2013/30 sayılı kararlarla reddedildiğinden, bu maddelere, fıkralara, bentlere, cümlelere, bölümlere, cetvellere ve listelere ilişkin yürürlüğün durdurulması istemlerinin REDDİNE,

2- 58. maddesinin (12) numaralı fıkrası ile (14) numaralı fıkrasının (ğ) bendinin, yürürlüğünün durdurulması istemlerinin koşulları oluşmadığından REDDİNE,

C- Anayasa'nın 91. maddesinin birinci fıkrası yönünden;

1- 1., 2., 3., 4., 5., 6. 7. maddeleri, 8. maddesinin (1) numaralı fıkrasının (h) ve (r) bentleri dışında kalan bölümü, 9., 10., 11., 12., 13., 14., 15. maddeleri, 16. maddesinin (2) numaralı fıkrasının birinci cümlesinde yer alan "gerçek ve", "gizli dahi olsa" ibareleri dışında kalan bölümü, 17., 18., 19., 20., 21., 22. maddeleri, 23. maddesinin (7) numaralı fıkrasının (c) ve (ç) bentleri dışında kalan bölümü ile (1), (2), (3), (4), (5), (6), (8), (9), (10), (11), (12), (13) ve (14) numaralı fıkraları, 24. maddesi, 25. maddesinin (1) numaralı fıkrasının birinci cümlesi ile (2), (3), (4), (5) ve (6) numaralı fıkraları, 26., 27., 28., 29., 30., 31., 32., 33., 34., 35., 36., 37., 38., 39., 40., 41., 42., 43. maddeleri, 44. maddesinin (1) numaralı fıkrası, 45., 46. maddeleri, 47. maddesinin (4) ve (5) numaralı fıkraları, 48., 49., 50., 51., 52., 53., 54., 56., 57. maddeleri, 58. maddesinin (1), (2), (3), (4), (5), (6) numaralı fıkraları, (7) numaralı fıkrasının (a) bendiyle değiştirilen 3359 sayılı Kanun'un ek 1. maddesinin birinci fıkrası dışında kalan bölümü, (b) bendi, (8) numaralı fıkrasının (a) bendi, (b) bendi ile 1219 sayılı Kanun'a eklenen geçici 9. madde, (9), (10) ve (11) numaralı fıkraları, (13) numaralı fıkrasının (a), (b), (c) bentleri, (ç) bendiyle değiştirilen 209 sayılı Kanun'un 5. maddesinin ikinci fıkrasının 5. ve 6. cümleleri ile altıncı fıkrası dışında kalan bölümü, (d) bendi, (14) numaralı fıkrasının (ğ) bendi dışında kalan bölümü ile (15) numaralı fıkrası, geçici 1., geçici 2., geçici 3., geçici 4., geçici 5., geçici 6., geçici 7., geçici 8., geçici 9., geçici 10., geçici 11., geçici 12., 59., 60. maddeleri, eki (I) Sayılı Cetvel, (II) Sayılı Cetvel, (III) Sayılı Cetvel ile (1), (2) ve (3)

sayılı listelere yönelik iptal istemleri, 14.2.2013 günlü, E.2011/150, K.2013/30 sayılı kararla reddedildiğinden, bu maddelere, fıkralara, bentlere, cümlelere, bölümlere, cetvellere ve listelere ilişkin yürürlüğün durdurulması isteminin REDDİNE,

2- 16. maddesinin (2) numaralı fıkrasının birinci cümlesinde yer alan "gerçek ve" ve "gizli dahi olsa" ibarelerinin yürürlüklerin durdurulması istemlerinin koşulları oluşmadığından REDDİNE,

3- 23. maddesinin (7) numaralı fıkrasının (c) ve (ç) bentlerinin yürürlüklerinin durdurulması istemlerinin koşulları oluşmadığından REDDİNE,

4- a- 44. maddesinin (2), (3) ve (4) numaralı fıkralarına,

b- 47. maddesinin (1), (2) ve (3) numaralı fıkralarına,

c- 55. maddesine,

ilişkin iptal hükümlerinin yürürlüğe girmelerinin ertelenmeleri nedeniyle, bu maddeye ve fıkralara ilişkin yürürlüğün durdurulması istemlerinin REDDİNE,

Ç- İçerikleri itibariyle Anayasa'ya aykırılığı ileri sürülen;

1- 2. maddesinin (2) numaralı fıkrasının sonunda yer alan 'ile ilgili olarak' ibaresine,

2- 6. maddesinin (1) ve (2) numaralı fıkralarına,

3- 7. maddesinin (1) numaralı fıkrasının (ğ) bendine,

4- 8. maddesinin (1) numaralı fıkrasının;

a- (c) bendinde yer alan "gerektiğinde süreli veya süresiz iptal etmek" ibaresine,

b- (ç) bendine,

c- (e) bendinde yer alan "politika ve düzenlemelerine" ve "gerekli" ibarelerine,

ç- (g), (ğ), (i) ve (k) bentlerine,

d- (n) bendinde yer alan "sertifikalı eğitim", "ve benzeri eğitimleri" ile "kredilendirme," ibarelerine,

e- (o) bendine,

5- 13. maddesinin (1) numaralı fıkrasının (e) bendine,

6- 16. maddesinin (2) numaralı fıkrasının birinci cümlesinde yer alan "gerçek ve", "gizli dahi olsa" ibareleri dışında kalan bölümüne,

7- 21. maddesine,

8- 23. maddesinin (7) numaralı fıkrasının (c) ve (ç) bentleri dışında kalan bölümüne,
9- 24. ve 26. maddelerine,
10- 27. maddesinin;
a- (2) numaralı fıkrasının (b) ve (d) bentlerine,
b- (2) numaralı fıkrasının (ğ) bendinde yer alan 'yaptırmak' sözcüğüne,
c- (2) numaralı fıkrasının (ı) bendine,
ç- (3) numaralı fıkrasının (e) bendine,
11- 29., 30., 31. ve 32. maddelerine,
12- 33. maddesinin (1) numaralı fıkrasının ikinci cümlesine,
13- 34. maddesine,
14- 36. maddesinin (2) numaralı fıkrasının (b) bendinde yer alan "ikincil düzenlemeleri yapmak,'
ibaresine,
15- 45. maddesinin (1) ve (4) numaralı fıkralarına,
16- 47. maddesinin (4) ve (5) numaralı fıkralarına,
17- 48. maddesinin (1) numaralı fıkrasının (c) bendi ile (2) ve (3) numaralı fıkralarına,
18- 49. maddesine,
19- 51. maddesinin (1) ve (3) numaralı fıkralarına,
20- 52. ve 56. maddelerine,
21- 57. maddesinin (1) ve (2) numaralı fıkralarına,
22- 58. maddesinin;
a- (6) numaralı fıkrasının (e) bendine,
b- (7) numaralı fıkrasının (a) bendiyle değiştirilen 3359 sayılı Kanun'un ek 1. maddesinin üçüncü fıkrasına,
c - (8) numaralı fıkrasının;
ca- (a) bendiyle değiştirilen 1219 sayılı Kanun'un 1. maddesine,
cb- (b) bendiyle 1219 sayılı Kanun'un 4. maddesinin birinci cümlesinde yapılan değişikliğe ve aynı Kanun'a eklenen Geçici Madde 9'a,

ç- (13) numaralı fıkrasının (b) bendi ile değiştirilen 209 sayılı Kanun'un 3. maddesinin birinci fıkrasının (d) bendine,

23- Geçici 4. maddesinin (1), (3) ve (4) numaralı fıkralarına,

24- Geçici 6. maddesine,

yönelik iptal istemleri, 14.2.2013 günlü, E.2011/150, K.2013/30 sayılı kararlarla reddedildiğinden, bu maddelere, fıkralara, bentlere, ibarelere, cümleye, bölümlere, sözcüğe ve değişikliğe ilişkin yürürlüğün durdurulması istemlerinin REDDİNE,

14.2.2013 gününde OYBİRLİĞİYLE karar verilmiştir.

VI- İPTAL HÜKMÜNÜN YÜRÜRLÜĞE GİRECEĞİ GÜN SORUNU

Anayasa'nın 153. maddesinin üçüncü fıkrasında, 'Kanun, kanun hükmünde kararname ve Türkiye Büyük Millet Meclisi İçtüzüğü ya da bunların hükümleri, iptal kararlarının Resmî Gazetede yayımlandığı tarihte yürürlükten kalkar. Gereken hallerde Anayasa Mahkemesi iptal hükmünün yürürlüğe gireceği tarihi ayrıca kararlaştırabilir. Bu tarih, kararın Resmî Gazetede yayımlandığı günden başlayarak bir yılı geçemez' denilmekte, 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 66. maddesinin (3) numaralı fıkrasında da bu kural tekrarlanmaktadır.

11.10.2011 günlü, 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 44. maddesinin (2), (3) ve (4) numaralı fıkralarının, 47. maddesinin (1), (2) ve (3) numaralı fıkralarının ve 55. maddesinin iptal edilmeleri nedeniyle doğacak hukuksal boşluk kamu yararını ihlal edecek nitelikte görüldüğünden, Anayasa'nın 153. maddesinin üçüncü fıkrasıyla 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince bu maddelere ilişkin iptal hükmünün, kararın Resmî Gazete'de yayımlanmasından başlayarak dokuz ay sonra yürürlüğe girmesi uygun görülmüştür.

VII- SONUÇ

11.10.2011 günlü, 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin;

A- 58. maddesinin (13) numaralı fıkrasının (ç) bendiyle değiştirilen 209 sayılı Kanun'un 5. maddesinin ikinci fıkrasında yer alan 'Bu fıkra uyarınca personele her ay yapılacak ek ödeme tutarı, 375 sayılı Kanun Hükmünde Kararnamenin ek 3 üncü maddesi uyarınca kadro ve görev unvanı veya pozisyon unvanı itibarıyla belirlenmiş olan ek ödeme tutarından az olamaz. Bu kapsamdaki personel için 375

sayılı Kanun Hükmünde Kararnamenin ek 3 üncü maddesinin üçüncü fıkrası hükmü uygulanmaz.' ibaresi, 30.12.2011 günlü başvuru tarihinden önce yürürlüğe giren 666 sayılı Kanun Hükmünde Kararname'nin 5. maddesinin (c) fıkrasının (1) numaralı alt bendi ile değiştirildiğinden, bu fıkra ya yönelik iptal isteminin başvuranın yetkisizliği nedeniyle REDDİNE, OYBİRLİĞİYLE,

B- 1- 8. maddesinin (1) numaralı fıkrasının (h) ve (r) bentleri, 4.7.2012 günlü, 6354 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un 20. maddesiyle yürürlükten kaldırıldığından,

2- 25. maddesinin (1) numaralı fıkrasının ikinci cümlesi, 6354 sayılı Kanun'un 21. maddesiyle yürürlükten kaldırıldığından,

3- 33. maddesinin (5) numaralı fıkrası, 6354 sayılı Kanun'un 16. maddesiyle değiştirildiğinden,

4- 58. maddesinin;

a - (7) numaralı fıkrasının;

aa- (a) bendiyle değiştirilen, 7.5.1987 günlü, 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun ek 1. maddesinin birinci fıkrası, 6354 sayılı Kanun'un 7. maddesiyle değiştirildiğinden,

ab- (c) bendiyle değiştirilen 3359 sayılı Kanun'un ek 9. maddesi, 6354 sayılı Kanun'un 8. maddesiyle değiştirildiğinden,

b- (13) numaralı fıkrasının (ç) bendiyle değiştirilen, 4.1.1961 günlü, 209 sayılı Sağlık Bakanlığına Bağlı Sağlık Kurumları ile Esenlendirme (Rehabilitasyon) Tesislerine Verilecek Döner Sermaye Hakkında Kanun'un 5. maddesinin altıncı fıkrası, 11.10.2011 günlü, 666 sayılı Kamu Görevlilerinin Mali Haklarının Düzenlenmesi Amacıyla Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun Hükmünde Kararname'nin 5. maddesinin (c) fıkrasının (1) numaralı alt bendi ile değiştirildiğinden,

konusu kalmayan bu maddeye, fıkralara, bentlere ve cümleye ilişkin iptal istemleri hakkında KARAR VERİLMESİNE YER OLMADIĞINA, OYBİRLİĞİYLE,

C- 1- 1., 2., 3., 4., 5., 6., 7. maddeleri, 8. maddesinin (1) numaralı fıkrasının (h) ve (r) bentleri dışında kalan bölümü, 9., 10., 11., 12., 13., 14., 15. maddeleri, 16. maddesinin (2) numaralı fıkrasının birinci cümlesinde yer alan "gerçek ve", "gizli dahi olsa" ibareleri dışında kalan bölümü, 17., 18., 19., 20., 21., 22. maddeleri, 23. maddesinin (7) numaralı fıkrasının (c) ve (ç) bentleri dışında kalan bölümü ile (1), (2), (3), (4), (5), (6), (8), (9), (10), (11), (12), (13) ve (14) numaralı fıkraları, 24. maddesi, 25. maddesinin

(1) numaralı fıkrasının birinci cümlesi ile (2), (3), (4), (5) ve (6) numaralı fıkraları, 26., 27., 28., 29., 30., 31., 32. maddeleri, 33. maddesinin (5) numaralı fıkrası dışında kalan bölümü, 34., 35., 36., 37., 38., 39., 40., 41., 42., 43. maddeleri, 44. maddesinin (1) numaralı fıkrası, 45., 46. maddeleri, 47. maddesinin (4) ve (5) numaralı fıkraları, 48., 49., 50., 51., 52., 53., 54., 56., 57. maddeleri, 58. maddesinin (1), (2), (3), (4), (5), (6) numaralı fıkraları, (7) numaralı fıkrasının (a) bendiyle değiştirilen 3359 sayılı Kanun'un ek 1. maddesinin birinci fıkrası dışında kalan bölümü, (b) bendi, (8) numaralı fıkrasının (a) bendi, (b) bendi ile 1219 sayılı Kanun'a eklenen geçici 9. madde, (9), (10) ve (11) numaralı fıkraları, (13) numaralı fıkrasının (a), (b), (c) bentleri, (ç) bendiyle değiştirilen 209 sayılı Kanun'un 5. maddesinin ikinci fıkrasının 5. ve 6. cümleleri ile altıncı fıkrası dışında kalan bölümü, (d) bendi, (14) numaralı fıkrasının (ğ) bendi dışında kalan bölümü ile (15) numaralı fıkrası, geçici 1., geçici 2., geçici 3., geçici 4., geçici 5., geçici 6., geçici 7., geçici 8., geçici 9., geçici 10., geçici 11., geçici 12., 59., 60. maddeleri, eki (I) Sayılı Cetvel, (II) Sayılı Cetvel, (III) Sayılı Cetvel ile (1), (2) ve (3) sayılı listelerin, 6.4.2011 günlü, 6223 sayılı Kamu Hizmetlerinin Düzenli, Etkin ve Verimli Bir Şekilde Yürütülmesini Sağlamak Üzere Kamu Kurum ve Kuruluşlarının Teşkilat, Görev ve Yetkileri ile Kamu Görevlilerine İlişkin Konularda Yetki Kanunu kapsamında olduğundan Anayasa'ya aykırı olmadığına ve bu maddelere, fıkralara, bentlere, cümleye, bölümlere, cetvellere ve listelere ilişkin iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

2- 58. maddesinin;

aa- (8) numaralı fıkrasının (b) bendi ile 11.4.1928 günlü, 1219 sayılı Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanun'un 4. maddesinin birinci cümlesindeki 'Türk Hekimlerinin' ibaresinin 'hekimlerin' şeklinde değiştirilmesi,

ab- (9) numaralı fıkrası,

6223 sayılı Kanun kapsamında olduğundan Anayasa'ya aykırı olmadığına bu fıkraya ve değişikliğe ilişkin iptal istemlerinin REDDİNE, Serruh KALELİ, Mehmet ERTEN, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŞ'ın karşıoyları ve OYÇOKLUĞUYLA,

b- (12) numaralı fıkrası, 6223 sayılı Kanun kapsamında olmadığından, bu fıkranın Anayasa'ya aykırı olduğuna ve İPTALİNE, OYBİRLİĞİYLE,

c- (14) numaralı fıkrasının (ğ) bendi, 6223 sayılı Kanun kapsamında olmadığından, bu bendin Anayasa'ya aykırı olduğuna ve İPTALİNE, OYBİRLİĞİYLE,

ç- 1- 1., 2., 3., 4., 5. maddeleri, 6. maddesinin (1), (4), (5), (6) ve (7) numaralı fıkraları, 7. maddesi, 8. maddesinin (1) numaralı fıkrasının (h) ve (r) bentleri dışında kalan bölümü, 9., 10., 11., 12., 13., 14., 15. maddeleri, 16. maddesinin (2) numaralı fıkrasının birinci cümlesinde yer alan "gerçek ve", "gizli dahi

olsa" ibareleri dışında kalan bölümü, 17., 18., 19., 21., 22. maddeleri, 25. maddesinin (1) numaralı fıkrasının birinci cümlesi ile (2), (3), (4), (5) ve (6) numaralı fıkraları, 26., 27., 28., 29., 30., 31., 34., 35., 36., 37., 38., 39., 40., 41., 42., 43., 46., 48., 49., 50., 51., 52., 53., 54., 56., 57. maddeleri, 58. maddesinin (1), (2), (3), (4), (5), (6) numaralı fıkraları, (7) numaralı fıkrasının (a) bendiyle değiştirilen 3359 sayılı Kanun'un ek 1. maddesinin birinci fıkrası dışında kalan bölümü, (b) bendi, (8) numaralı fıkrasının (a) bendi, (b) bendi ile 1219 sayılı Kanun'a eklenen geçici 9. madde, (9), (10) ve (11) numaralı fıkraları, (13) numaralı fıkrasının (a), (b), (c) bentleri, (ç) bendiyle değiştirilen 209 sayılı Kanun'un 5. maddesinin ikinci fıkrasının 5. ve 6. cümleleri ile altıncı fıkrası dışında kalan bölümü, (d) bendi, (14) numaralı fıkrasının (ğ) bendi dışında kalan bölümü ile (15) numaralı fıkrası, geçici 1., geçici 2., geçici 3., geçici 4., geçici 5., geçici 6., geçici 7., geçici 8., geçici 9., geçici 10., geçici 11., geçici 12., 59., 60. maddeleri, eki (I) Sayılı Cetvel, (II) Sayılı Cetvel, (III) Sayılı Cetvel ile (1), (2) ve (3) sayılı listelerin, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olmadığına ve bu maddelere, fıkralara, bentlere, cümleye, bölümlere, cetvellere ve listelere ilişkin iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

2- 6. maddesinin (2) ve (3) numaralı fıkraları, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olmadığına ve bu fıkralara ilişkin iptal istemlerinin REDDİNE, Mehmet ERTEN, Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŞ'ın karşıoyları ve OYÇOKLUĞUYLA,

3- 16. maddesinin (2) numaralı fıkrasının birinci cümlesinde yer alan "gerçek ve", "gizli dahi olsa" ibarelerinin, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olduklarına ve İPTALLERİNE, OYBİRLİĞİYLE,

4- 20. maddesinin, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olmadığına ve bu maddeye ilişkin iptal isteminin REDDİNE, Mehmet ERTEN'in karşıoyu ve OYÇOKLUĞUYLA,

5- 23. maddesinin;

a- (1), (2), (3), (4), (5) ve (6) numaralı fıkralarının, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olmadıklarına ve bu fıkralara ilişkin iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

b- (7) numaralı fıkrasının;

ba- (a) bendinin, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olmadığına ve bu bende ilişkin iptal isteminin REDDİNE, Serruh KALELİ, Mehmet ERTEN, Osman Alifeyyaz PAKSÜT, Zehra Ayla PERKTAŞ ile Zühtü ARSLAN'ın karşıoyları ve OYÇOKLUĞUYLA,

bb- (b) bendinin Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olmadığına ve bu bende ilişkin iptal isteminin REDDİNE, OYBİRLİĞİYLE,

bc- (c) ve (ç) bentlerinin, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olduklarına ve İPTALLERİNE, OYBİRLİĞİYLE,

c- (8), (10), (11), (12) ve (13) fıkralarının, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olmadıklarına ve bu fıkralara ilişkin iptal istemlerinin REDDİNE, Mehmet ERTEN'in karşıoyu ve OYÇOKLUĞUYLA,

ç- (9) ve (14) numaralı fıkralarının, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olmadıklarına ve bu fıkralara ilişkin iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

6- 24. maddesinin, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olmadığına ve bu maddeye ilişkin iptal isteminin REDDİNE, Osman Alifeyyaz PAKSÜT'ün karşıoyu ve OYÇOKLUĞUYLA,

7- 32. maddesinin;

a- (1), (3), (6) ve (7) numaralı fıkralarının, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olmadıklarına ve bu fıkralara ilişkin iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

b- (2), (4) ve (5) numaralı fıkralarının, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olmadıklarına ve bu fıkralara ilişkin iptal istemlerinin REDDİNE, Mehmet ERTEN, Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŞ'ın karşıoyları ve OYÇOKLUĞUYLA,

8- 33. maddesinin (1), (2), (3), (4) ve (6) numaralı fıkralarının, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olmadıklarına ve bu fıkralara ilişkin iptal istemlerinin REDDİNE, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŞ'ın karşıoyları ve OYÇOKLUĞUYLA,

9- 44. maddesinin;

a- (1) numaralı fıkrasının, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olmadığına ve bu fıkraya ilişkin iptal isteminin REDDİNE, OYBİRLİĞİYLE,

b- (2), (3) ve (4) numaralı fıkralarının, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olduklarına ve İPTALLERİNE, Haşim KILIÇ, Alparslan ALTAN, Engin YILDIRIM, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI ile Muammer TOPAL'ın karşıoyları ve OYÇOKLUĞUYLA; iptal hükümlerinin, Anayasa'nın 153. maddesinin üçüncü fıkrasıyla 30.3.2011 günlü, 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince, KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAŞLAYARAK DOKUZ AY SONRA YÜRÜRLÜĞE GİRMESİNE, OYBİRLİĞİYLE,

10- 45. maddesinin, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olmadığına ve bu maddeye ilişkin iptal isteminin REDDİNE, Mehmet ERTEN, Serdar ÖZGÜLDÜR ile Zehra Ayla PERKTAŞ'ın karşıoyları ve OYÇOKLUĞUYLA,

11- 47. maddesinin;

a- (1), (2) ve (3) numaralı fıkralarının, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olduklarına ve İPTALLERİNE; iptal hükümlerinin, Anayasa'nın 153. maddesinin üçüncü fıkrasıyla 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince, KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAŞLAYARAK DOKUZ AY SONRA YÜRÜRLÜĞE GİRMESİNE, OYBİRLİĞİYLE,

b- (4) ve (5) numaralı fıkralarının, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olmadıklarına ve bu fıkralara ilişkin iptal isteminin REDDİNE, OYBİRLİĞİYLE,

12- 55. maddesinin, Anayasa'nın 91. maddesinin birinci fıkrası uyarınca Anayasa'ya aykırı olduğuna ve İPTALİNE; iptal hükmünün, Anayasa'nın 153. maddesinin üçüncü fıkrasıyla 6216 sayılı Kanun'un 66. maddesinin (3) numaralı fıkrası gereğince, KARARIN RESMÎ GAZETE'DE YAYIMLANMASINDAN BAŞLAYARAK DOKUZ AY SONRA YÜRÜRLÜĞE GİRMESİNE, OYBİRLİĞİYLE,

D- İçerikleri itibariyle Anayasa'ya aykırılığı ileri sürülen;

1- 2. maddesinin (2) numaralı fıkrasının sonunda yer alan 'ile ilgili olarak' ibaresinin, Anayasa'ya aykırı olmadığına ve bu ibareye ilişkin iptal isteminin REDDİNE, OYBİRLİĞİYLE,

2- 6. maddesinin (1) ve (2) numaralı fıkralarının, Anayasa'ya aykırı olmadıklarına ve bu fıkralara ilişkin iptal istemlerinin REDDİNE, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÛT ile Zehra Ayla PERKTAŞ'ın karşıoyları ve OYÇOKLUĞUYLA,

3- a- 7. maddesinin (1) numaralı fıkrasının (ğ) bendinin,

b- 8. maddesinin (1) numaralı fıkrasının;

ba- (c) bendinde yer alan "gerektiğinde süreli veya süresiz iptal etmek" ibaresinin,

bb- (ç) bendinin,

bc- (e) bendinde yer alan "politika ve düzenlemelerine" ve "gerekli" ibarelerinin,

bç- (g), (ğ), (i) ve (k) bentlerinin,

bd- (n) bendinde yer alan "sertifikalı eğitim", "ve benzeri eğitimleri" ile "kredilendirme," ibarelerinin,

be- (o) bendinin,

c- 13. maddesinin (1) numaralı fıkrasının (e) bendinin,

ç- 16. maddesinin (2) numaralı fıkrasının birinci cümlesinde yer alan "gerçek ve", "gizli dahi olsa" ibareleri dışında kalan bölümünün,

d- 21. maddesinin,

e- 23. maddesinin (7) numaralı fıkrasının (c) ve (ç) bentleri dışında kalan bölümünün,

Anayasa'ya aykırı olmadıklarına ve bu maddeye, bentlere, bölümlere ve ibarelere ilişkin iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

4- 24. maddesinin, Anayasa'ya aykırı olmadığına ve bu maddeye ilişkin iptal isteminin REDDİNE, Erdal TERCAN'ın karşıoyu ve OYÇOKLUĞUYLA,

5- a- 26. maddesinin,

b- 27. maddesinin;

ba- (2) numaralı fıkrasının (b) ve (d) bentlerinin,

bb- (2) numaralı fıkrasının (ğ) bendinde yer alan 'yaptırmak' sözcüğünün,

bc- (2) numaralı fıkrasının (ı) bendinin,

bç- (3) numaralı fıkrasının (e) bendinin,

c- 29., 30., 31. ve 32. maddelerinin,

ç- 33. maddesinin (1) numaralı fıkrasının ikinci cümlesinin,

d- 34. maddesinin,

e- 36. maddesinin (2) numaralı fıkrasının (b) bendinde yer alan "ikincil düzenlemeleri yapmak," ibaresinin,

f- 45. maddesinin (1) ve (4) numaralı fıkralarının,

g- 47. maddesinin (4) ve (5) numaralı fıkralarının,

ğ- 48. maddesinin (1) numaralı fıkrasının (c) bendi ile (2) ve (3) numaralı fıkralarının,

h- 49. maddesinin,

ı- 51. maddesinin (1) ve (3) numaralı fıkralarının,

i- 52. ve 56. maddelerinin,

j- 57. maddesinin (1) ve (2) numaralı fıkralarının,

Anayasa'ya aykırı olmadığına ve bu maddelere, fıkralara, bentlere, cümleye, ibareye ve sözcüğe ilişkin iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

6- 58. maddesinin;

a- (6) numaralı fıkrasının (e) bendinin, Anayasa'ya aykırı olmadığına ve bu bende ilişkin iptal isteminin REDDİNE, Mehmet ERTEN, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŞ'ın karşıoyları ve OYÇOKLUĞUYLA,

b- (7) numaralı fıkrasının (a) bendiyle değiştirilen 3359 sayılı Kanun'un ek 1. maddesinin üçüncü fıkrasının, Anayasa'ya aykırı olmadığına ve bu fıkra ile ilişkin iptal isteminin REDDİNE, Mehmet ERTEN, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŞ'ın karşıoyları ve OYÇOKLUĞUYLA,

c- (8) numaralı fıkrasının;

ca- (a) bendiyle değiştirilen 1219 sayılı Kanun'un 1. maddesinin, Anayasa'ya aykırı olmadığına ve bu maddeye ilişkin iptal isteminin REDDİNE, Serdar ÖZGÜLDÜR ile Osman Alifeyyaz PAKSÜT'ün karşıoyları ve OYÇOKLUĞUYLA,

cb- (b) bendiyle 1219 sayılı Kanun'un 4. maddesinin birinci cümlesinde yapılan değişikliğin ve aynı Kanun'a eklenen Geçici Madde 9'un Anayasa'ya aykırı olmadıklarına ve bu maddeye ve değişikliğe ilişkin iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

ç- (13) numaralı fıkrasının (b) bendi ile değiştirilen 209 sayılı Kanun'un 3. maddesinin birinci fıkrasının (d) bendinin Anayasa'ya aykırı olmadığına ve bu bende ilişkin iptal isteminin REDDİNE, OYBİRLİĞİYLE,

7- Geçici 4. maddesinin;

a- (1) ve (4) numaralı fıkralarının, Anayasa'ya aykırı olmadığına ve bu fıkralara ilişkin iptal istemlerinin REDDİNE, OYBİRLİĞİYLE,

b- (3) numaralı fıkrasının, Anayasa'ya aykırı olmadığına ve bu fıkra ile ilişkin iptal isteminin REDDİNE, Serdar ÖZGÜLDÜR, Zehra Ayla PERKTAŞ ile Celal Mümtaz AKINCI'nın karşıoyları ve OYÇOKLUĞUYLA,

8- Geçici 6. maddesinin, Anayasa'ya aykırı olmadığına ve bu maddeye ilişkin iptal isteminin REDDİNE, Mehmet ERTEN, Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT ile Zehra Ayla PERKTAŞ'ın karşıoyları ve OYÇOKLUĞUYLA,

14.2.2013 gününde karar verildi.

Başkan - Haşim KILIÇ

Başkanvekili - Serruh KALELİ

Başkanvekili - Alparslan ALTAN

Üye; Mehmet ERTEN; Serdar ÖZGÜLDÜR; Osman Alifeyyaz PAKSÜT; Zehra Ayla PERKTAŞ;
Burhan ÜSTÜN; Engin YILDIRIM; Nuri NECİPOĞLU; Hicabi DURSUN; Celal Mümtaz AKINCI;
Erdal TERCAN; Muammer TOPAL; Zühtü ARSLAN

KARŞIOY YAZISI

11.10.2011 günlü, 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat Ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 44. maddesinin (2), (3) ve (4) numaralı fıkraları çoğunluk kararıyla Anayasa'nın 91. maddesine aykırı bulunarak iptal edilmiştir.

663 sayılı KHK'nin 44. maddesinde Bakanlık ve bağlı kuruluşların merkez teşkilatında 'sağlık uzmanları ve uzman yardımcıları' ile 'sağlık denetçileri ve denetçi yardımcıları' istihdam edilebileceği belirtilmiş ve bu görevlere atanabilmek için aranan şartlar ile yardımcı olarak göreve başlayanların uzman ve denetçi olarak atanabilmeleri için gerekli şartlar düzenlenmiştir. Bu kişilerin mesleğe alınmaları, yetiştirilmeleri, yarışma sınavı, tez hazırlama ve yeterlik sınavı ile diğer hususların yönetmelikle düzenleneceği belirtilmiştir.

6223 sayılı Yetki Kanunu'nun 1. maddesinin (1) numaralı fıkrasının (a-3) bendinde, kanunun amaçlarından birinin kamu hizmetlerinin bakanlıklar arasındaki dağılımının yeniden belirlenerek, mevcut bakanlıklar ile birleştirilen veya yeni kurulan bakanlıkların görev, yetki, teşkilat ve kadrolarının düzenlenmesine, taşrada ve yurt dışında teşkilatlanma esaslarına ilişkin konularda düzenlemelerde bulunmak üzere Bakanlar Kuruluna kanun hükmünde kararname çıkarma yetkisi vermek olduğu belirtilmiş ve aynı Kanun'un (2) numaralı fıkrasında da ilgili kanun ve kanun hükmünde kararnamelerde değişiklik yapılabileceği belirtilmiştir.

663 sayılı KHK'nin 44. maddesinde Bakanlık ve bağlı kuruluşların merkez teşkilatında 'sağlık uzmanları ve uzman yardımcıları' ile 'sağlık denetçileri ve denetçi yardımcıları' istihdamının öngörülmesi ve bunların kadrolarının oluşturulması teşkilat ve kadroların belirlenmesine ilişkin bir husus olduğundan Yetki Kanunu'na aykırılık bulunmamaktadır.

Kamu görevlilerinin kadrolarının ve bu kadrolara atanacak kişilerde bulunması gereken niteliklerin de kanunla düzenlenmesi gerekmektedir. Ancak, kamu görevlisi olarak atanacak kişilerle ilgili tüm ayrıntıların sadece yasayla düzenlenmesi gerektiği ve bu konuda idarî düzenlemeler yapılmasının Anayasa'nın 128. maddesinin ikinci fıkrasına aykırı düşeceği iddiası yerinde değildir. Anayasa'nın bir maddesinin yasayla düzenleneceğini öngördüğü bir konunun, Anayasa'nın 91. maddesinin birinci fıkrasının açıkça yasakladığı hükümler ile doğrudan ilgili olmadıkça, ya da KHK ile düzenlenemeyeceği Anayasa'da özel olarak belirtilmedikçe KHK ile düzenlenmesi Anayasa'ya aykırı değildir.

Anayasa'nın 70. maddesine göre, 'her Türk kamu hizmetine girme hakkına sahiptir. Hizmete alınmada görevin gerektirdiği niteliklerden başka hiçbir ayırım gözetilemez'. Maddede Türkiye Cumhuriyeti Devletine vatandaşlık bağı ile bağlı olan herkesin görevin gerektirdiği nitelikler dışında, dil, din, mezhep, renk, siyasi düşünce, cinsiyet ve benzeri ayırım gözetilmeksizin kamu hizmetlerine girme hakkına sahip buldukları belirtilmiştir. Böylece 'kamu hizmetlerine girme hakkı' siyasi hak ve ödevler kapsamında, vatandaşlık bağına bağlı olarak kullanılabilir bir hak olarak düzenlenmiştir. Düzenlemenin temel hakka ilişkin niteliği bundan ibarettir. Yoksa, bunun dışında kamu görevlerine giriş, atanma, görev değişikliğine ilişkin tüm düzenleme ve uygulamaların temel hakkın düzenlenmesi ve 91. madde anlamında yasak alan kapsamında görülmesi yerinde değildir.

Anayasa'nın 91. maddesinin birinci fıkrasında, Anayasanın ikinci kısmının birinci ve ikinci bölümlerinde yer alan temel haklar, kişi hakları ve ödevleri ile dördüncü bölümünde yer alan siyasî haklar ve ödevlerin kanun hükmünde kararnamelerle düzenlenemeyeceği belirtilmiştir. Anayasanın belirtilen bölümlerinde birçok temel hak ve özgürlük düzenlenmiş bulunmaktadır. Söz konusu temel hak ve özgürlüklerin kapsama alanları ve ilgili oldukları hususlar geniş bir biçimde yorumlandığında KHK'lerle yapılacak tüm düzenlemelerin bu hak ve özgürlüklerle bağlantılarının bulunduğu ileri sürülebilir. Böyle bir yorumdan hareket edilmesi halinde yasak alan kapsamı oldukça genişleyecek ve KHK ile düzenlenebilecek alan kalmayacaktır. Nitekim Anayasa Mahkemesinin, 6.1.1987 günlü, E:1986/15 ve K:1987/1 sayılı kararında, dolaylı biçimde kişi hak ve özgürlüklerini ilgilendirmeyecek bir düzenleme düşünmenin oldukça güç olduğu, bu nedenle de dolaylı bir ilginin varlığına dayanılarak sonuca gitmenin isabetli sayılamayacağı belirtilmiştir. Buna göre, yasak alanın kapsamının, temel hak ve özgürlüklerle doğrudan ilgili düzenlemeleri kapsayacak, dolaylı olarak ilgili düzenlemeleri ise kapsam dışında bırakacak şekilde belirlenmesi gerekir.

Anayasa Mahkemesi, 16.5.1989 günlü, E:1989/4 ve K:1989/24 sayılı kararında, 3.11.1988 günlü, 347 sayılı '233 Sayılı Kamu İktisadi Teşebbüsleri Hakkında Kanun Hükmünde Kararnamenin Bir

Maddesinde Değişiklik Yapılmasına Dair Kanun Hükmünde Kararname'nin Genel Müdür olarak atanabilmek için, 'yükseköğrenim görmüş olmak, dört yılı kamuda, altı yılı özel sektörde geçmek şartıyla en az on yıl hizmeti bulunmak, kamu hizmeti bulunmayanlarda ise özel sektörde asgari onbeş yıl çalışmış olmak, Genel müdürlük görevini yerine getirebilecek yetenek, bilgi ve tecrübeye sahip olmak' şartlarını getiren 1. maddesine yönelik iptal istemini reddetmiştir.

Anayasa'nın 91. maddesi kapsamına giren alanlarda düzenleme yapılmış olmasından söz edilebilmesi için 91. maddede belirtilen hak ve alanlarla ilgili doğrudan bir düzenleme yapılmış olması gerekir.

İptaline karar verilen kurallarda Yetki Kanunu kapsamında ilgili kurumda ilk defa Bakanlık ve bağlı kuruluşların merkez teşkilatında 'sağlık uzmanları ve uzman yardımcıları' ile 'sağlık denetçileri ve denetçi yardımcıları' kadroları oluşturulduğundan, zorunlu olarak bu kadrolara girişin koşulları da düzenlenmiştir. Bu nedenle anılan kuralların Anayasa'nın 91. maddesinde belirtilen yasak alana ilişkin düzenlemeler içerdiğinden söz etmek mümkün değildir.

Belirtilen nedenlerle, itiraz konusu kurallara yönelik iptal isteminin reddine karar verilmesi gerektiği düşüncesiyle kuralın iptaline yönelik çoğunluk görüşüne katılmadık.

Başkan - Haşim KILIÇ

Başkanvekili - Alparslan ALTAN

Üye: Engin YILDIRIM; Nuri NECİPOĞLU; Hicabi DURSUN; Celal Mümtaz AKINCI; Muammer TOPAL

KARŞIOY

(Reddi Hakim)

Mahkememize 2011/150 esas sayısı ile T.B.M.M. üyesi 116 milletvekili tarafından açılan 11.10.2011 tarih ve 663 sayılı Kanun Hükmünde Kararname'nin iptali davasının da Anayasa mahkemesi Başkanı Haşim Kılıç'ın reddi talebi yer almış ise de, dosyanın 12.1.2012 tarihli ilk incelemesinde hakimin reddi talebi esastan reddedilmiş, talebin kötü niyetle yapıldığı oyçokluğu ile kabul edilmiş ise de, bu gibi hallerde uygulanacak para cezasının talepte bulunanlar dışında cezanın SOYUT bir niteleme ile sadece davacıya verilmesi yönündeki çoğunluk görüşüne aşağıdaki nedenler ile katılmamıştır.

Reddi hakim talebinin kötü niyetle yapıldığının kabulü halinde, bu kasta yaptırım uygulanması hukuk düzenince makul kabul görmeyen bir fiilin cezalandırılması isteminin gereğidir. Nitekim

hukukun temel ilkelerinden bakıldığında HMK'nun 42. maddesi hukuksuz eyleme meşruiyet kazandırmamak için ceza öngörüsünde bulunmuş ve başvuruda bulunanlara bunlar arasında nasıl bir hukuksal ilişki olduğuna bakmaksızın talepte bulunanlar yönünden her birinin cezalandırılması gerektiğini ifade etmiştir.

Nitekim genel usul hukuku hükümleri yanında özel nitelik taşıyan 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 60. maddesinin (5) numaralı fıkrasında Anayasa Mahkemesinde yapılacak hakimin reddi taleplerinin kötü niyetle yapıldığının anlaşılması halinde BAŞVURUCULARIN HER BİRİNE disiplin para cezası verileceği hükmü çok açıktır.

Davacılar; Anayasanın 150. maddesince siyasi parti kimliklerine bakılmaksızın kendilerine iptal davası açma hakkı tanınan meclis üye tamsayısının 1/5 oranındaki asgari 110 milletvekilidir. Açılan davaların kabul görebilmesi için alt sınır 110 olup beklenmeyip üstünde olması haline ilişkin bir sınırlama bulunmamaktadır. Nitekim Türkiye Büyük Millet Meclisi tarafından imzalanarak tasdik edilen belge ile görülen bu davayı açanların Meclis üyeleri oldukları teyit edilmiş ve görülen bu davayı da asgari 116 kişinin bir araya gelerek açtığı anlaşılmıştır.

Bir an için dava açma için bir araya gelen iradenin zorunlu bir birliktelik içinde oldukları kabul edilse bile bu beraberlik açılmış davanın mahkemece kabulünün ön şartıdır. Örneğin değişik siyasi gruplardan 140 kişinin bir araya gelmesi ile açılan bir davada dava açan belgeye imza atanlardan 40 kişinin diğer talepler yanında reddi hakim talebinde bulunmamış veya bilahare feragat olmaları halinde görülen davada dava, kalan 100 kişi davacı yönünden 110 kişilik dava açma şartını oluşturmadığı için açılmamış mı sayılacaktır' veya dava tüm diğer talepler yönünden düşmüş mü olacaktır'

Dava açanların iradesi açılmış davanın kabul şartından bağımsız nitelikte olup dava açanlar arasında ki hukuksal ilişkiden kaynaklı bir zorunluluk değildir. Reddi hakim talebinden çekilenler yönünden kötü niyet araştırması yapılamayacak ve para cezası verilemeyecek olması ' talepte bulunan ve bulunmayanlar arasında nasıl bir hukuki tespit yapmayı gerektiriyorsa da dava açıp hakimin reddi talebinde bulunanların bu yöndeki iradesi dava açma için bir araya gelme zorunluluğunda bağımsız bir fikir 'bir irade tezahürüdür.

Dava açanlar, açma yönünden gerekli biçimsel bir zorunluluk, dava konusu talepler yönünden ise ihtiyari bir birliktelik içindedirler. Davacılar arasında şekli bakımından mecburi dava arkadaşlığı vardır.

Mecburi dava arkadaşlığında; dava konusu hukuki ilişkide farklı davranmalarını önleyecek çok sıkı, iştirak halinde bir ortaklık olup, dava arkadaşları aynı şekilde ve birlikte hareket etmek zorundadırlar. İştirak halinde mülkiyet, adi ortaklık, miras şirketi gibi veya ilgililer hakkında tek bir karar verilmesi zorunluluğunu doğuran davalarda davacılar şekli bakımından mecbur dava arkadaşı durumundadırlar ve dava konusu hak ile aralarında zorunlu ilişki vardır.

Özel yasasına tabii olan Anayasa Mahkemesine iptal davası açma şeklinde izah edildiği anlamda dava açan asgari 110 kişinin hukuk usulü nitelemesi ile mecburi dava arkadaşı oldukları söylenemeyecektir. Aralarında şekli bakımından olan bu zorunlu birliktelik nedeniyle dava açma şartı yerine getirildikten sonra dava açanlar yönünden dava açmada asgari sayısal zorunluluk şartının altına düşmedikçe talep konusu haklar yönünden bağımsız ihtiyari davranmalarının önüne geçecek kısıtlayıcı bir hüküm mevzuatta yoktur.

Kaldı ki, davanın konusu, dava açanlar arası şahsa bağlı sıkı bir medeni hukuk ilişkisinden değil Kamu hukukundan doğan ve toplumun tümünü ilgilendiren bir yasa uygulamasının, demokratik toplum öznelerinden Anayasal denetim talebine ilişkin olup bu yönüyle de mecburi dava arkadaşlığı nitelemesinden ayrıldığı düşünülmektedir.

Aktif süje olan davanın konusu, toplumun tümünü ilgilendiren içerik taşıdığından, pasif süje olan dava açanlar olup, dava açmada birliktelik zorunluluğu içinde iseler de hak, yetki ve taleplerini hukuka uygun sorumluluk bilinci dahilinde kullanmak zorundadırlar, Aksine davranışın cezalandırılacağı öngörüldüğü hallerde ceza vermenin sınırını adaletle şekillendirilmiş toplumsal yarar düşüncesi oluşturur, ve cezaların önleme iyileştirme amaçları da göz önüne alınarak adaletli bir ölçü içinde biçimlenir. Hedef cezanın yaratacağı korkutuculuk ve caydırıcılıktan toplum adına yararlanma ilkesidir.

Ceza önlemi kimi suçlardan, niteliği, işleme biçimi, Devlet için zarar alanı, SUÇTAN ZARAR GÖRENİN KİMLİĞİ vb nedenler ile farklı düzenlemeler içerebilir.

Başkanvekili - Serruh KALELİ

KARŞIOY GEREKÇESİ

663 sayılı Kanun Hükmünde Kararname'nin (KHK) 58. maddesinin (8) numaralı fıkrasının (b) bendi ile 11.4.1928 tarihli ve 1219 sayılı Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanun'un 4. maddesinin birinci cümlesindeki 'Türk hekimlerinin' ibaresi 'hekimlerin' şeklinde değiştirilmiş; 58. maddesinin (9) numaralı fıkrası ile de 25.2.1954 tarihli ve 6283 sayılı Hemşirelik Kanunu'nun 3.

maddesi 'Bu Kanun hükümlerine göre hemşire unvanı kazanmış olanların dışında hiç kimse Türkiye'de hemşirelik mesleğini icra edemez' şeklinde yeniden düzenlenmiştir.

Dava konusu KHK kurallarıyla, Türkiye'de hekim ya da hemşire olarak çalışabilmek için evvelce anılan kanunlarda aranan Türk vatandaşı olma şartının kaldırıldığı anlaşılmaktadır.

6.4.2011 günlü, 6223 sayılı Yetki Kanunu'nun 1. maddesinin birinci fıkrasının (a) bendi, 'Kamu hizmetlerinin bakanlıklar arasındaki dağılımının yeniden düzenlenmesi konusunda Bakanlar Kuruluna yetki vermekte; keza (b) bendi ise 'Kamu kurum ve kuruluşlarında istihdam edilen memurlar, işçiler, sözleşmeli personel ile diğer kamu görevlilerinin çalışmalarında etkinliği arttırmak üzere, bunların atanma, nakil, görevlendirme, seçilme, terfi, yükselme, görevden alınma ve emekliye sevk edilme usul ve esaslarına' ilişkin konularda düzenlemelerde bulunmak üzere, Bakanlar Kuruluna Kanun Hükmünde Kararname çıkarma yetkisi tanımaktadır. Yine 6223 sayılı Kanun'un 1. maddesinin ikinci fıkrasının (a) bendi, kamu hizmetlerinin bakanlıklar arasındaki dağılımının yeniden belirlenmesine ilişkin olarak (20) bent halinde sayılan Kanun ve KHK'lerde değişiklik yapılabilmesine imkân tanımakta, (b) bendi ise kamu kurum ve kuruluşlarında istihdam edilen memurlar, işçiler, sözleşmeli personel ile diğer kamu görevlilerinin atanma, nakil, görevlendirilme, seçilme, terfi, yükselme, görevden alınma ve emekliye sevk edilme usul ve esaslarına ilişkin olarak (7) bent halinde sayılan Kanun ve KHK'lerde değişiklik yapılabilmesi imkânını getirmektedir.

663 sayılı KHK'nin 58. maddesinin (8) numaralı fıkrasının (b) bendi ile 1219 sayılı Kanun'un 4. maddesinin birinci cümlesinde yapılan değişiklik ile 6283 sayılı Kanun'un 3. maddesini değiştiren (9) numaralı fıkrasındaki düzenlemeler incelendiğinde; bunların kamu hizmetlerinin bakanlıklar arasındaki dağılımı ile ilgisi olmadığı gibi halen kamu kurum ve kuruluşlarında istihdam edilen memurlar, işçiler, sözleşmeli personel ile diğer kamu görevlileri konusunda bir düzenleme öngörmediği açıkça görülmektedir. Türkiye'de hekim ya da hemşire olarak çalışabilmek için evvelce mevzuatta aranan 'Türk vatandaşı olma' şartının değiştirilebilmesi konusunda yasa koyucunun bir tercih ve değerlendirmesi olacaksa, bunun yolu Yetki Kanunu ile öngörülmeleyen bir yetkinin kullanılması suretiyle değil; ayrı bir yasal düzenleme yapmak biçiminde olmalıdır. Oysa belirtilen düzenlemelerle 6223 sayılı Yetki Kanunu ile öngörülmeleyen konular bu kapsama dahil edilmiştir.

Açıklanan nedenlerle, Anayasa'nın 91. maddesine aykırı olduğunu değerlendirdiğimiz anılan düzenlemelerin iptali gerektiği kanısına vardığımızdan; aksi yöndeki çoğunluk görüşüne katılmıyoruz.

Başkanvekili - Serruh KALELİ

KARŞIOY GEREKÇESİ

663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin dava konusu kuralın da içinde yer aldığı 23. maddesi, Sağlık Meslekleri Kurulunun kuruluş ve görevlerini düzenlemektedir. Kurul'un 'meslekî yeterlilik değerlendirmesi yapmak, meslekî müeyyide uygulamak' ve bu bağlamda 'meslekten geçici veya sürekli men etmeye karar vermek' gibi görevleri bulunmaktadır.

Maddenin (7) numaralı fıkrasında, bir yandan Kurul aşamasından önce yapılacak olan idari incelemelerin prosedürü, diğer yandan da 'İdarî inceleme veya varsa adlî kovuşturma kapsamında elde edilen bilgi ve belgeler de değerlendirilerek, genel hükümler saklı kalmak üzere Kurulca' sağlık meslek mensuplarına uygulanacak idari yaptırımlar belirtilmektedir..

Dava konusu kural olan (7) numaralı fıkranın (a) bendi, mesleğinde yetersizliği tespit edilenler ile dikkatsiz ve özensiz davranışla ölüme ve vücut fonksiyon kaybına sebep olan sağlık mensuplarının mesleki yeterlilik eğitimine tabi tutulacaklarını, bu eğitimi takiben yapılacak sınavda başarısız olanların da meslek icrasından menedileceğini düzenlemektedir.

Görüldüğü üzere kural, meslekten men gibi son derece ağır bir idari yaptırımı düzenlemektedir. Bu yaptırımın, mesleki yetersizliğin ve dikkatsizlik ve özensiz davranışla ölüme ve vücut fonksiyon kaybına sebep olma fiilinin sonucu olarak ortaya çıkan bir disiplin cezası niteliğinde olduğu açıktır. Bu yönüyle kural, Mahkememizce oybirliğiyle iptal edilen aynı fıkranın (c) ve (ç) bentlerinde yer alan düzenlemelerle aynı mahiyettedir. İdarenin yetersiz, dikkatsiz ve özensiz olanları belli bir eğitim ve sınav sürecine tabi tutarak yaptırımlar uygulaması veya mesleği icradan menedilenlerin yeniden sınava tabi tutularak mesleğe kabul edilebilmeleri sonucu değiştirmemektedir.

Anayasa'nın 91. maddesi uyarınca, 'sıkıyönetim ve olağanüstü haller saklı kalmak üzere, Anayasanın ikinci kısmının birinci ve ikinci bölümlerinde yer alan temel haklar, kişi hakları ve ödevleri ile dördüncü bölümünde yer alan siyasî haklar ve ödevler kanun hükmünde kararnamelerle düzenlenemez.' Esasen bu hüküm, temel hak ve hürriyetlerin sınırlandırılması konusunda Anayasa'nın 13. maddesiyle getirilen kanunilik şartına paraleldir. Olağan dönemlerde, sosyal ve ekonomik haklar dışında kalan temel hak ve hürriyetlerin, kanuna göre istisnai bir tasarruf olan kanun hükmünde kararnameyle düzenlenemeyeceğinin belirtilmesi, bu hak ve hürriyetleri daha fazla güvence altına almaya yöneliktir.

Diğer yandan, Anayasa'nın 91. maddesindeki kanun hükmünde kararname ile düzenleme yasağını sadece 'sınırlama' olarak anlamamak gerekir. Anayasa koyucunun, 'sınırlama'yı da kapsayan çok daha geniş bir kavram olan 'düzenleme'yi seçmesi bilinçli bir tercihi yansıtmaktadır. Aksi yorum, temel hak ve hürriyetlere yönelik hangi düzenlemenin sınırlama, hangisinin genişletme olduğu konusunda belirsiz bir alan doğmasına ve gereksiz tartışmalara yol açabilir. Bu nedenle, Anayasa'nın 91. maddesinde belirtilen hak ve hürriyetler, sınırlama ya da genişletme amacıyla, hiç bir şekilde kanun hükmünde kararnamelerle düzenlenememelidir.

Dava konusu kural, ceza adaletinin ve adil yargılama hakkının ilkelerine yer veren Anayasa'nın 38. maddesiyle ilgilidir. Bu maddeye göre, 'Ceza ve ceza yerine geçen güvenlik tedbirleri ancak kanunla konulur'. 38. maddedeki suç ve cezaların kanuniliği, masumiyet karinesi ve ceza sorumluluğunun şahsiliği gibi ilkelere ilişkin hususlar, kanun hükmünde kararname ile düzenlenemeyecek 'yasak alan' içinde kalmaktadır. Nitekim, Mahkememiz, (7) numaralı fıkranın (c) ve (ç) bentlerini 'Anayasa'nın 38. maddesi kapsamında değerlendirilmesi gereken sağlık meslek mensuplarının meslekten geçici men ve meslekten men edilmesini gerektiren fiiller ile bu fiillere uygulanacak yaptırımlara ilişkin hükümler içerdiğinden, Anayasa'nın 91. maddesinin birinci fıkrasına aykırı' bularak oybirliğiyle iptal etmiştir.

Aynı gerekçeyle, (7) numaralı fıkranın (a) bendinin de iptal edilmesi gerektiğini düşündüğümüzden çoğunluğun red yönündeki kararına katılmıyoruz.

Başkanvekili - Serruh KALELİ

Üye - Zühtü ARSLAN

KARŞIOY GEREKÇESİ

6216 sayılı Kanun'un 60. maddesinin (5) numaralı fıkrasında ret talebinin 'kötü niyetle yapıldığının anlaşılması' ve 'esas yönünden kabul edilmemesi' hâlinde, 'disiplin para cezası' verileceği öngörülmekte, (6) numaralı fıkrasında da ret talebinin 'açıkça' kötüye kullanıldığının tespiti aranmaktadır.

Söz konusu kurallar uyarınca disiplin para cezasına hükmedilebilmesi için, ret talebinin kötü niyetle yapılması ve ret talebi olarak gösterilen sebeplerin esastan kabul edilmemesi şartlarının birlikte gerçekleşmesi gerekmektedir.

Bu şartlardan birinin gerçekleşmesi disiplin para cezası verilebilmesi için yeterli olamayacağı gibi ret talebinin açıkça kötüye kullanıldığının da tespit edilmesi gerekmektedir.

Davacı ret sebeplerini,

- Kamuoyunda 'WikiLeaks Belgeleri' olarak bilinen belgelere göre, 2003 yılında ABD Büyükelçisine Cumhuriyet Halk Partisi aleyhinde bir takım beyanlarda bulunduğu iddiası,

- 'Ümit ediyorum ki bu gayret, Anayasa Mahkemesine dava açmak suretiyle sorun çözme kolaycılığını da ortadan kaldıracaktır' biçimindeki 25 Nisan 2011 tarihli konuşma metninden yapılan alıntı,

ve bunları pekiştiren

- 6223 sayılı Yetki Kanunu'nun iptali başvurusunda istikrar kazanmış görüşünden vazgeçerek iptal isteminin reddi yönünde kullandığı oy,

olarak gösterdikten sonra, bu sebeplerin Cumhuriyet Halk Partisi'nin tarafı olduğu davalarda, reddedilenin tarafsız davranamayacağına ilişkin kuşkulara neden olduğunu ileri sürmüştür.

İleri sürülen bu iddia, 6216 sayılı Kanun'un 60. maddesinin (1) numaralı fıkrası çerçevesinde incelenerek, söz konusu sebeplerin tarafsız hareket edemeyeceği kanısını haklı kılan hâl kapsamında olmadığı düşüncesiyle Davacının ret talebi esastan reddedilmiştir.

Ret talebinin esastan reddedilmiş olması, talebin kötü niyetle yapıldığı anlamını taşımayacağı gibi salt reddedilme nedeniyle disiplin para cezası verilemeyeceği de açıktır. Disiplin para cezası verilebilmesi için kanunun tanıdığı bu hakkın açıkça kötüye kullanıldığının (kötü niyetle yapıldığının) tespit edilmesi gerekmektedir.

Ret talebinin, kimi internet sitelerinden elde edilebilmesi mümkün olan ret sebeplerine dayanması, belirtilen ret sebeplerinin içerikleri, ret talebinin sunulmuş biçimi, anlatım düzeni ve yargılama sürecindeki ileri sürülüş zamanı, Davacı tarafından açılan ve ret taleplerini de içeren diğer iptal davalarının konuları arasındaki benzerlik ve bu iptal başvurularındaki ret taleplerinin başvuru yönteminin ve ret sebeplerinin ayırimsız aynı olması dikkatle incelendiğinde, ret talebi başvurusunun, kanunun tanıdığı bir hakkın kanuni sınırlar içinde kullanıldığını ve yargılamanın düzenli biçimde işleyişini önlemek ve kamu düzenini bozmak gibi bir amaç taşımadığını, dolayısıyla da bu hakkın açıkça kötüye kullanılmadığını göstermektedir.

Açıklanan nedenle Davacıya disiplin para cezası verilmesi yönündeki çoğunluk görüşüne katılmıyorum.

KARŞIOY GEREKÇESİ

6223 sayılı Yetki Yasası'na dayanılarak kararlaştırılan 663 sayılı Kanun Hükmünde Kararname'nin (KHK) ;

1- 6. maddesinin:

(2) numaralı fıkrasında;

'Kurul üyeleri en az dört yıllık yüksek okul mezunu ve sekiz yıl iş tecrübesi bulunanlar arasından Bakan tarafından görevlendirilir. Görev süresi iki yıldır ve süresi sona eren üyeler yeniden görevlendirilebilir. Kurula Müsteşar veya görevlendireceği yardımcılarında biri başkanlık eder.'

(3) numaralı fıkrasında;

'Uhdesinde kamu görevi bulunmayan Kurul üyelerine (85.000) gösterge rakamının memur aylık katsayısı ile çarpımı sonucu bulunacak tutarı geçmemek üzere Bakan onayıyla belirlenen tutarda net ödeme yapılır. Bakanlıktan veya diğer kamu kurumlarından görevlendirilen Kurul üyelerine, kadrolarına göre malî haklar kapsamında fiilen yapılmakta olan her türlü ödemeler toplamı ile uhdesinde kamu görevi bulunmayanlara ödenmek üzere bu fıkra göre belirlenen tutar arasındaki fark ayrıca ödenir.'

2- 20. maddesinin:

(1) numaralı fıkrasında;

'Bakanlıkta, özel önem ve öncelik taşıyan konularda Bakana yardımcı olmak üzere otuz Bakanlık Müşaviri atanabilir.'

3- 23. maddesinin:

(7) numaralı fıkrasının a) bendinde;

'Mesleğinde yetersizliği tespit edilenler ile dikkatsiz ve özensiz davranışla ölüme veya vücut fonksiyon kaybına sebep olanların yetersiz görüldükleri alanda meslekî yeterlilik eğitimine tâbi tutulmalarına karar verilir. Bu eğitim, yetersiz görülen alanda teorik ve/veya pratik eğitim ve/veya başka bir sağlık meslek mensubunun nezaret ve sorumluluğunda meslek icrası şeklinde yaptırılabilir. Yeterlilik eğitimine tâbi tutulanlar eğitim sonunda Kurulun belirleyeceği teorik ve/veya uygulamalı sınava tâbi tutulur. Bu sınavda başarılı olanlar mesleğini icraya devam eder; başarısız olanlar meslek

icrasından men edilir. Meslekten men edilenler, durumlarına göre Kurulca belirlenen eğitime devam ettirilerek veya eğitime tâbi tutulmadan yapılacak müteakip sınavlarda başarı gösterdiği takdirde meslek icra etme hakkını yeniden kazanır.'

(8) numaralı fıkrasında;

'Mesleğini icra etmesine mâni ve iyileşmesi mümkün olmayan aklî, ruhî ve bedenî hastalığı ortaya konulan sağlık meslek mensupları, Kurulun kararı ile mesleğini icradan yasaklanabilir.'

(10) numaralı fıkrasında;

'Aynı olaydan dolayı ilgili hakkında ceza takibatına veya disiplin soruşturmasına başlanmış olması bu maddeye göre işlem yapılmasını geciktirmez ve engellemez; ilgilinin mahkûm olması veya olmaması ile disiplin cezası verilmiş veya verilmemiş olması hâlleri, ayrıca meslekî müeyyide uygulanmasını etkilemez.'

(11) numaralı fıkrasında;

'Kanunla kurulmuş meslek odalarının ve birliklerinin kuruluş kanunlarındaki disiplin hükümleri saklıdır. Ancak fiilin her iki kanuna göre de müeyyide gerektirmesi hâlinde bu Kanun hükümleri uygulanır.'

(12) numaralı fıkrasında;

'Meslekten geçici men edilmesine karar verilen Devlet memurları, men müddetince aylıksız izinli sayılır veya talepleri hâlinde aynı süreyle mesleği ile ilişkisi bulunmayan durumlarına uygun başka bir kadroya atanır. Sözleşmeli olanların sözleşmeleri men müddetince ücretsiz olarak askıya alınır. Meslekten sürekli men edilmesine karar verilen Devlet memurları istekleri hâlinde, mesleği ile ilişkisi bulunmayan durumlarına uygun başka bir kadroya atanır, aksi halde görevleri sona erer. Meslekten sürekli men edilmesine karar verilen sözleşmeli personelin sözleşmeleri sona erer.'

(13) numaralı fıkrasında;

'Bu maddeye göre mesleğini geçici olarak sürdüremeyeceklerin durumları kayıtlara işlenir. Meslekten sürekli men edilmesine karar verilenlerin veya mesleğini icra etmekten yasaklananların diplomaları, uzmanlık veya meslek belgeleri Bakanlıkça iptal edilir ve sistemden kaydı silinir.'

4- 32. maddesinin:

(2) numaralı fıkrasında;

'Genel sekreter, idarî ve malî hizmetler başkanları, hastane yöneticisi, müdür ve müdür yardımcısı olabilmek için en az dört yıllık eğitim veren yükseköğretim kurumlarından veya bunlara denkliği Yükseköğretim Kurulunca kabul edilmiş yurt dışındaki yükseköğretim kurumlarından mezun olmak ve kamu veya özel sektörde, genel sekreter için 8 yıl, idarî ve malî hizmetler başkanları, hastane yöneticisi ve müdürler için en az 5 yıl iş tecrübesine sahip olmak şarttır.'

(4) numaralı fıkrasında;

'Genel Sekreterlikte uzman olarak istihdam edilecek personelin alanında en az lisans düzeyinde öğrenim görmüş olması ve kamu veya özel sektörde en az 3 yıl iş tecrübesine sahip olması gerekir. Açıktan alınacak uzman ve büro görevlilerinin Kamu Personeli Seçme Sınavından en az yetmiş puan almış olmaları şarttır. Uzman ve büro görevlilerinin Birliklere dağılımı, işe alınma usûl ve esasları Kurum tarafından belirlenir. Açıktan istihdam edilen uzmanların oranı Birliğin toplam uzman sayısının yüzde ellisini geçemez.'

(5) numaralı fıkrasında;

' 'Ekli (II) sayılı cetvelde belirtilen pozisyonlarda açıktan istihdam edilen personelin herhangi bir suretle sözleşmeleri sona erdiğinde birlik ile ilişkileri kesilir. Açıktan sözleşmeli istihdam, memurluk veya diğer personel istihdam şekillerinden birine geçiş bakımından kazanılmış hak teşkil etmez.'

5- 45. maddesinin

(1) numaralı fıkrasında;

'Bakanlık ve bağlı kuruluşlarında özel bilgi ve ihtisas gerektiren nitelikli bir işin yapılması veya proje hazırlanması veya yürütülmesi için 657 sayılı Kanun ve diğer kanunların sözleşmeli personel çalıştırılması hakkındaki hükümlerine bağlı olmaksızın proje süresince ve her halde üç yıla kadar sözleşme ile yerli ve yabancı uzman çalıştırılabilir.'

(2) numaralı fıkrasında;

'Bu şekilde çalıştırılacak personel sayısı yüzelliyi geçemez ve bunların Bakanlık ve bağlı kuruluşlarına dağılımı Bakan tarafından belirlenir.'

(3) numaralı fıkrasında;

'Sözleşmeli olarak çalıştırılacaklara ödenecek ücret 657 sayılı Kanunun 4 üncü maddesinin (B) fıkrasına göre çalıştırılanlar için uygulanmakta olan sözleşme ücreti tavanının beş katını geçemez. Bu personel, sosyal güvenlik yönünden 5510 sayılı Kanunun 4 üncü maddesinin birinci fıkrasının (a) bendi kapsamında sigortalı sayılır.'

(4) numaralı fıkrasında;

'Bu suretle çalıştırılacak uzmanların nitelikleri, alınma usûlü ve sözleşme ücretlerinin tespiti ile sözleşme usûl ve esasları Bakanlık ve Maliye Bakanlığınca müştereken belirlenir.'

6- 58. maddesinin:

(6) numaralı fıkrasında;

657 sayılı Devlet Memurları Kanununun;

'e) Ek 33 üncü maddesindeki tablonun (a) sırasında geçen 'Klinik şefi, şef yardımcısı' ibareleri 'Eğitim görevlisi' şeklinde değiştirilmiştir.'

(7) numaralı fıkrasında;

7/5/1987 tarihli ve 3359 sayılı Kanunun;

a) Ek 1 inci maddesi aşağıdaki şekilde değiştirilmiştir.

'Ek Madde 1-

Eğitim ve araştırma hastanelerinde eğitim görevlilerinden biri hastane yöneticisi tarafından bir yıllık süre için ilgili birimin eğitim sorumlusu olarak görevlendirilir, idarî sorumlusu ise aynı süreyle ilgili daldaki uzmanlar arasından seçilir. Birimin eğitim sorumlusuna idarî sorumluluk görevi de verilebilir.'

(8) numaralı fıkrasında;

11/4/1928 tarihli ve 1219 sayılı Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanun'un;

'b) 4 üncü maddesinin birinci cümlesindeki 'Türk hekimlerinin' ibaresi 'hekimlerin' şeklinde değiştirilmiş "

7- Geçici 6. maddesinde:

'Bu maddenin yayımı tarihinde görevde bulunan klinik şefi ve klinik şef yardımcılarının görevleri bu maddenin yayımı tarihinde sona erer.'

denilmektedir.

Anayasa'nın 91. maddesinde, olağan dönemde çıkarılacak kanun hükmünde kararnameler ile Anayasanın ikinci kısmının birinci ve ikinci bölümlerinde yer alan temel haklar, kişi hakları ve ödevleri ile dördüncü bölümde yer alan siyasi haklar ve ödevlerin düzenlenemeyeceği öngörülmüştür.

Anayasa'nın 'Hizmete girme' başlıklı 70. maddesinde 'Her Türk, kamu hizmetlerine girme hakkına sahiptir. Hizmete alınmada, görevin gerektirdiği niteliklerden başka hiçbir ayırım gözetilemez.' denilmekte ve söz konusu kural, Anayasa'nın dördüncü bölümündeki siyasi haklar ve ödevler ile ilgi düzenlemeler içinde yer almaktadır.

663 sayılı KHK'nin;

6. maddesinin (2) ve (3) fıkralarında, Sağlık Politikaları Kurul üyeliklerine Bakan tarafından görevlendirme yapılabileceği,

20. maddesinde, Bakanlara, Bakanlık Müşavirleri atanabileceği,

32. maddesinin (2) ve (4) numaralı fıkraları ile (5) numaralı fıkrasının son iki cümlesinde, belirtilen koşulları taşıyanların Kamu Hastaneleri Birliklerine sözleşmeli olarak atanabileceği,

45. maddesinde, Bakanlık ve bağlı kuruluşlarında sözleşmeli olarak yerli ve yabancı uzmanların çalışabileceği,

58. maddesinin (8) numaralı fıkrasının, a) bendi, Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanununun 1. maddesinde 'Türk hekimlerinin' ibaresi 'hekimlerin' şeklinde değiştirilerek yabancı hekimlerin Devlet hastanelerinde çalışabileceği öngörülmektedir.

Yukarda ki kurallarda belirtilen görevlerin, kamu hizmetine ilişkin oldukları ve bu görevlere atanacakların niteliklerinin belirtilmemesi nedeniyle daha önce kamu hizmetinde bulunmayanların da açıktan bu görevlere atanabilmelerinin mümkün olduğu anlaşılmaktadır.

İptali istenilen kuralların, kamu hizmetine girme hakkına ilişkin düzenlemeler oldukları ve bu hakkın da Anayasa'nın dördüncü bölümündeki siyasi haklar ve ödevler ile ilgi yasaklanan alan içinde yer aldıkları konusunda duraksama bulunmamaktadır.

Buna göre, 663 sayılı KHK'nin 6. maddesinin (2) ve (3) fıkraları, 20. maddesi, 32. maddesinin (2) ve (4) numaralı fıkraları ile (5) numaralı fıkrasının son iki cümlesi, 45. maddesi, 58. maddesinin (8) numaralı fıkrasının, a) bendi olağan dönemde çıkarılacak kanun hükmünde kararnameler için yasaklanan alanı düzenlemekte ve bu haliyle Anayasa'nın 91. maddesine aykırılık oluşturmaktadır.

Yine, 663 sayılı KHK'nin;

23. maddesinin, (7) numaralı fıkrasının a) bendi ile (8), (10), (11), (12) ve (13) numaralı fıkralarında, Sağlık Meslekleri Kurulu'nun meslekî yeterlilik değerlendirmesi sonucu uygulayacağı müeyyideler ve bağlantılı hükümler yer almaktadır.

Anayasa'nın 'Suç ve cezalara ilişkin esaslar' başlıklı 38. maddesinde, suç ve ceza belirlenirken uyulması gereken temel ilke ve esasların neler olduğu gösterilmiştir. Suç ve cezaya ilişkin ilkeleri içeren bu kural, Anayasa'nın ikinci kısım ikinci bölümünde 'Kişinin Hakları ve Ödevleri' ile ilgili düzenlemeler içinde yer almaktadır.

663 sayılı KHK' nin 23. maddesinin, (7) numaralı fıkrasının a) bendi ile (8), (10), (11), (12) ve (13) numaralı fıkralarında meslek icrasından geçici ya da sürekli olarak men edilme, sözleşmeli olanlarda sözleşmenin askıya alınması ya da sona ermesi, meslekle ilişkisi olmayan başka bir kadroya atanma ya da görevin sona ermesi, diploma, uzmanlık veya meslek belgesinin iptal edilmesi şeklinde müeyyideler yer almaktadır.

İptali istenilen bu düzenlemelerin, suç ve cezaya ilişkin kurallar olduğunda ve Anayasa'nın ikinci kısım ikinci bölümündeki kişi hakları ve ödevleriyle ilgi yasaklanan alan içinde yer aldıklarında duraksama bulunmamaktadır. Buna göre, 663 sayılı KHK'nin 23. maddesinin belirtilen bent ve fıkraları, olağan dönemde çıkarılacak kanun hükmünde kararname için yasaklanan alanı düzenlemekte ve bu haliyle de Anayasa'nın 91. maddesine aykırılık oluşturmaktadır.

Yine, 663 sayılı KHK'nin;

58. maddesinin (6) numaralı fıkrasının e) bendinde, 657 sayılı Devlet Memurları Kanununun, Ek 33. maddesindeki tablonun (a) sırasında geçen 'Klinik şefi, şef yardımcısı' ibarelerinin 'Eğitim görevlisi' şeklinde değiştirilmesi, (7) fıkrasının a) bendi ile 3359 sayılı Kanun'un Ek 1.maddesinin değişik üçüncü fıkrasında, eğitim ve araştırma hastanelerinde eğitim görevlilerinden birinin hastane yöneticisi tarafından ilgili birimin eğitim sorumlusu olarak görevlendirilebileceği, idari sorumluluk da verilebileceği, GEÇİCİ MADDE 6. da klinik şefi ve klinik şef yardımcılarının görevlerinin bu maddenin yayımı tarihinde sona ereceği ve eğitim görevlisi kadrolarına kazanılmış hak aylık dereceleriyle atanacağı öngörülmektedir.

Dava konusu düzenlemelerle Sağlık Bakanlığı'na bağlı eğitim ve araştırma hastanelerinde klinik şefi ve şef yardımcılıkları kaldırılarak, yerlerine eğitim görevlisi kadrosu getirilmekte ve Geçici 6. maddenin yayımı tarihinde klinik şefi ve şef yardımcılarının görevleri sona erdirilerek, eğitim görevlisi kadrolarına kazanılmış hak aylık dereceleriyle atanmış sayılacakları hükme bağlanmaktadır.

Anayasa'nın 2. maddesinde öngörülen hukuk devleti, hukuk kurallarında sınırsız değişiklik yapma yetkisi vermemekte, ayrıca, yapılan değişikliklerde mevcut hukuki durumun ve oluşmuş bulunan istikrarın gözetilmesini de gerekli kılmaktadır. Hukuk normlarının öngörülebilir olması, devlete

güven duyulabilmesi ve yasal düzenlemelerinde bu güven duygusunu koruması hukuk devleti olmanın kaçınılmaz gereklerindedir. Hukuki güvenlik sadece devlet faaliyetlerine duyulan güveni değil, aynı zamanda yürürlükteki mevzuatın süreceğine duyulan güveni de kapsar.

Anayasa'nın 130. maddesi, eğitim-öğretim, bilimsel araştırma, yayın ve danışmanlık yapmak, ülkeye ve insanlığa hizmet etmek üzere bilimsel özerkliğe sahip üniversitelerin, Devlet tarafından kurulacağını öngörmektedir.

İptali istenilen kurallar, klinik şefi ve şef yardımcılarının kazanılmış hak aylık dereceleriyle eğitim görevlisi kadrolarına atanmalarını hükme bağlamış olsa da bunların klinik içerisindeki önceki pozisyonlarına ve bilimsel statülerine uygun bir atamayı gerçekleştirmemesi nedeniyle istikrar kazanan hukuki durumlarını korumadığı, böylece Anayasa'nın 2. maddesinde yer alan hukuk devleti ilkesinin ihlal edildiği anlaşılmaktadır.

Ayrıca, eğitim ve araştırma hastaneleri yöneticilerine, eğitim sorumlusu ve idari sorumlu uzmanı seçme yetkisinin verilmesi, tıpta uzmanlık ve yan dal uzmanlığı eğitiminin bir yükseköğretim türü olduğu gözetildiğinde, yüksek öğretime ilişkin anayasal gereklere uygun düşmemektedir. Eğitim ve araştırma hastanelerinde verilecek eğitim faaliyetlerinin de üniversite öğretim üyelerinde olduğu gibi her türlü etkiden uzak, özgür bir ortamda bilim gereklerine uygun olarak yapılması gerekir. Bu durumun göz ardı edilmesi, uzmanlık eğitiminin kalitesinin düşmesine dolaylı olarak da insan sağlığının tehlikeye girmesine neden olacağı açıktır. Bilimsel özerkliğe sahip olmayan bir eğitimle tıpta uzmanlık ve yan dal uzmanlığı eğitiminin verilmesi Anayasa'nın 130. maddesine aykırılık oluşturmaktadır.

Açıklanan nedenlerle yukarıda belirtilen kuralların iptali gerekir.

Üye - Mehmet ERTEN

KARŞIOY GEREKÇESİ

663 sayılı KHK'nin içerik bakımından Anayasa'ya aykırılığı ileri sürülen 58. maddesinin (8) numaralı fıkrasının (a) bendiyle değiştirilen 11.4.1928 tarihli ve 1219 sayılı Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanun'un 1. maddesinde 'Türkiye Cumhuriyeti dahilinde tababet icra ve herhangi surette olursa olsun hasta tedavi edebilmek için tıp fakültesinden diploma sahibi olmak şarttır.' denilmektedir. Anılan düzenlemeden önce 1219 sayılı Kanun'un 1. maddesi metni ise şöyleydi: 'Türkiye Cumhuriyeti dahilinde tababet icra ve herhangi surette olursa olsun hasta tedavi edebilmek için Türkiye Darülfünunu Tıp Fakültesinden diploma sahibi olmak ve Türk bulunmak şarttır.'

Dava konusu KHK kuralıyla Türkiye'de hekimlik yapabilmek için Türk vatandaşı olma şartına son verilmiş; ayrıca hekimlik icrası için Türk Tıp Fakültelerinden diploma sahibi olmak koşulu da kaldırılmıştır. Anayasa'nın Başlangıç bölümünde 'Türk milli menfaatleri' Anayasa'nın yorumunda dikkate alınması gerekli bir kriter olarak öngörülmüş; 56. maddesinde de Devlete sağlık hizmetlerinin yürütülmesi ve sürdürülmesinde önemli bir görev ve misyon yüklenmiştir. Birçok kanunda Türk vatandaşı olma şartı yürürlüğünü korurken (657 sayılı Kanun Md.48/A-1; 1136 sayılı Avukatlık Kanunu Md.3/a; Noterlik Kanunu Md.7/1 vb.) ve bu alanlarda sadece Türk vatandaşlarının görev yapması esası benimsenmişken, sağlık hizmeti gibi tüm Türk vatandaşlarını ilgilendiren bir alanda yabancı hekim çalıştırılmasının ve bu hekimler yönünden sadece Sağlık Bakanlığının belirleyeceği ilke ve kriterlere göre istihdam öngörülmesinin Anayasa'nın Başlangıç'ı ile 2. ve 56. maddelerine aykırı olduğu kanaatine vardığımdan, aksi yöndeki çoğunluk kararına katılmıyorum.

Üye - Serdar ÖZGÜLDÜR

KARŞIOY GEREKÇESİ

663 sayılı KHK'nin Geçici 4. maddesinin (3) numaralı fıkrasında 'Bu maddenin yayımı tarihinde başmüfettiş, müfettiş ve müfettiş yardımcısı kadrolarında bulunanlar, durumlarına göre buldukları kadro dereceleriyle Bakanlık ve bağlı kuruluşlarının sağlık başdenetçisi, sağlık denetçisi ve sağlık denetçi yardımcısı kadrolarına atanırlar. Bunların başmüfettiş, müfettiş ve müfettiş yardımcısı kadrolarında geçirdikleri süreler sağlık başdenetçisi, sağlık denetçisi ve sağlık denetçi yardımcısı kadrolarında geçmiş sayılır.' denilmektedir.

Sağlık Bakanlığının kuruluş ve görevleriyle ilgili mülga 181 sayılı KHK döneminde Sağlık Bakanlığı Teftiş Kurulu Başkanlığının doğrudan Bakanlık ve bağlı olduğu, bu Başkanlığın Bakanlık danışma ve denetim birimi olarak tanımlandığı, müfettiş yardımcılığı, müfettişlik ve başmüfettişlik unvanlarının kariyer meslek esaslarına göre belli prosedür sonucu kazanılmış unvanlar olduğu, 663 sayılı KHK ile yapılan yeni düzenlemede ise bu başkanlığın 'Denetim Hizmetleri Başkanlığı'na dönüştürüldüğü ve hiyerarşik yapılanmada müsteşar yardımcısına bağlandığı, önceki 'müfettiş' unvanlarını kazananların ise 'denetçi' unvanlarına intibak ettirildikleri anlaşılmaktadır.

Anayasa'nın 2. maddesinde, Türkiye Cumhuriyeti'nin nitelikleri arasında sayılan Hukuk Devleti ilkesi, hukuk güvenliğinin ve adaletin sağlanmasına yönelik hukuk anlayışını yaratmakta, yasaların kamu yararı amacıyla çıkarılmasını zorunlu kılmaktadır. Hukuk güvenliği ve adalet kavramları ile istikrar arasında sıkı bir bağ bulunmaktadır. Hukuk güvenliği ve adalet, çağdaş kamu yönetimi

anlayışında, istikrar olgusunun temelini oluşturmaktadır. Hukuk güvenliği, kamu görevlileri yönünden önemli bir güvencedir. 663 sayılı KHK değişikliğinden önceki düzenlemede, müfettiş yardımcılarını, müfettiş ve başmüfettişlerin belli koşulları sağlayarak ve süre kaydı olmaksızın atandıkları anılan görevlerden yaş haddinden önce bu statülerinin sona erdirilemeyeceği konusunda yasal bir güvenceye sahip oldukları anlaşılmaktadır. Yasayla elde edilen bu statünün müfettiş yardımcılarını, müfettişler ve başmüfettişler yönünden kazanılmış hak olarak değerlendirilmesi olanaklı olmasa da, statülerinin devam edeceği yolunda meşru bir beklentiye sahip oldukları, bu beklentinin ise hukuki güvenlik, adalet ve belirlilik ilkeleri gereğince korunması gerektiğinin kabulü zorunludur. Nitekim Anayasa Mahkemesinin konuya ilişkin içtihatları da bu doğrultudadır. (Any.Mah.nin 16.7.2010 tarih ve E.2010/29, K.2010/90; 9.6.2011 tarih ve E.2008/31, K.2011/94 sayılı kararları)

Davanın somutunda da görüleceği üzere, dava konusu düzenlemeyle Sağlık Bakanlığındaki müfettiş yardımcılarını, müfettişleri ve başmüfettişlerinin mevcut bu haklı beklentileri hiç dikkate alınmadan statülerine son verildiği ve yeni öngörülen sisteme sağlık denetçi yardımcısı, sağlık denetçisi ve sağlık başdenetçisi unvanlarına intibak ettirildikleri açık olduğundan; bu düzenlemenin Anayasa'nın 2. maddesine aykırı düştüğü ve iptali gerektiği kanısına vardığımızdan; çoğunluğun aksi yöndeki kararına katılmıyoruz.

Üye: Serdar ÖZGÜLDÜR; Zehra Ayla PERKTAŞ; Celal Mümtaz AKINCI

KARŞIOY GEREKÇESİ

1- 663 sayılı Kanun Hükmünde Kararname'nin (KHK) 33. maddesinin (1), (2), (3), (4) ve (6) numaralı fıkralarında 'sözleşmeli personel'e ilişkin birtakım mali düzenlemelerde bulunduğu görülmektedir. 6.4.2011 günlü, 6223 sayılı Yetki Kanunu'nun 'Amaç ve Kapsam' başlıklı 1. maddesinde, 'Kamu hizmetlerinin bakanlıklar arasındaki dağılımının yeniden belirlenmesi' ve 'Kamu kurum ve kuruluşlarında istihdam edilen memurlar, işçiler, sözleşmeli personel ile diğer kamu görevlilerinin çalışmalarında etkinliği arttırmak üzere, bunların atanma, nakil, görevlendirilme, seçilme, terfi, yükselme görevden alınma ve emekliye sevk edilme usul ve esaslarına' ilişkin konularda düzenlemelerde bulunmak üzere, Bakanlar Kuruluna KHK çıkarma yetkisi verildiği; ancak mali konularda düzenleme yapılması konusunda herhangi bir hükme yer verilmediği anlaşılmaktadır. Bu durumda, sözleşmeli personele ilişkin tamamen mali düzenlemeleri ihtiva eden sözkonusu hükümlerin Anayasa'nın 91. maddesine aykırı olduğu ve iptali gerektiği açıkça anlaşılmaktadır.

2- 663 sayılı KHK'nin 'sözleşmeli uzman çalıştırılması' başlıklı 45. maddesinde, Bakanlık ve bağlı kuruluşlarında özel bilgi ve ihtisas gerektiren nitelikli bir işin yapılması veya proje hazırlanması veya yürütülmesi için 657 sayılı Kanun ve diğer kanunların sözleşmeli personel çalıştırılması hakkındaki hükümlerine bağlı olmaksızın proje süresince ve her halde üç yıla kadar sözleşme ile yerli ve yabancı uzman çalıştırılabileceği hususu düzenlenmiş ve maddenin (2), (3) ve (4) numaralı fıkralarında da sözkonusu sözleşmeli uzman personelle ilgili kimi mali ve özlük haklarına yer verilmiştir.

6.4.2011 günlü, 6223 sayılı Yetki Kanunu'nun 1. maddesinin (1) numaralı fıkrasının (b) bendi, kamu kurum ve kuruluşlarında 'istihdam edilen' kamu görevlileriyle ilgili olarak, sayılan hususlarda düzenleme yapmak üzere KHK çıkarma yetkisi vermektedir. Oysa 663 sayılı KHK'nin anılan hükmünde 'istihdam edilen' kamu görevlileriyle ilgili değil, 'yabancı uzmanların' sözleşmeli olarak istihdam edilmesi ile ilgili konular yer almaktadır. Oysa yabancı uzman istihdamı ile ilgili olarak 6223 sayılı Yetki Kanunu'nda herhangi bir düzenleme yapma yetkisi verilmediği görülmektedir. Dolayısıyla bu konuda KHK ile bir düzenleme yapılabilmesi imkânı bulunmadığından; anılan hüküm Anayasa'nın 91. maddesine aykırı düşmektedir.

3- İçerik bakımından Anayasa'ya aykırılığı ileri sürülen 663 sayılı KHK'nin 'Sağlık Politikaları Kurulu' başlıklı 6. maddesinin (1) numaralı fıkrasında; Sağlık Politikaları Kurulunun, Bakanlığın sağlık sistemi yönetimi ve politika belirleme ile ilgili temel görevlerini yerine getirmek üzere görevlendirilen 11 üye ile müsteşar ve müsteşar yardımcısından meydana geldiği, (2) numaralı fıkrasında ise Kurul üyelerinin, en az dört yıllık yüksek okul mezunu ve sekiz yıl iş tecrübesi bulunanlar arasından Bakan tarafından görevlendirileceği, görev süresinin iki yıl olduğu, süresi sona eren üyelerin yeniden görevlendirilebileceği, Kurula müsteşar veya görevlendireceği yardımcılarında birinin başkanlık edeceği hüküm altına alınmıştır.

Anayasa'nın 56. maddesinde 'Devlet, herkesin hayatını, beden ve ruh sağlığı içinde sürdürmesini sağlamak; insan ve madde gücünde tasarruf ve verimi artırarak, işbirliğini gerçekleştirmek amacıyla sağlık kuruluşlarını tek elden planlayıp hizmet vermesini düzenler.' denilmektedir. Şüphesiz, Devlet'in 'sağlık politikaları' da sözkonusu Anayasal hükmün icrası cümlesinden olarak Sağlık Bakanlığına düşen bir görevdir. Bir kamu hizmeti olduğunda kuşku olmayan sağlık politikalarını belirleme görevinin, Bakan tarafından kamu görevlileri dışındaki kişiler arasından seçilecek kişilerin oluşturduğu bir Kurul eliyle gördürülmesi Anayasa'nın belirtilen 56. maddesi hükmü ile 128. maddesine açıkça aykırı düşmektedir.

4- İçerik bakımından Anayasa'ya aykırılığı ileri sürülen 663 sayılı KHK'nin 58. maddesinin (6) numaralı fıkrasının (e) bendi ile 657 sayılı Kanun'un EK-33. maddesindeki tablonun (a) sırasında

geçen 'Klinik Şefi, şef yardımcısı' ibareleri 'Eğitim görevlisi' şeklinde değiştirilmiş; 58. maddesinin (7) numaralı fıkrasının (a) bendiyle ise 7.5.1987 tarihli, 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun EK-1. maddesinin üçüncü fıkrası 'Eğitim ve araştırma hastanelerinde eğitim görevlilerinden biri hastane yöneticisi tarafından bir yıllık süre için ilgili birimin eğitim sorumlusu olarak görevlendirilir, idari sorumlusu ise aynı süreyle ilgili daldaki uzmanlar arasından seçilir. Birimin eğitim sorumlularına idari sorumluluk görevi de verilebilir.' şeklinde düzenlenmiştir.

Sözkonusu düzenlemelerle, Sağlık Bakanlığına Bağlı Eğitim ve Araştırma Hastanelerinde uzun yıllardır uygulanan 'Klinik Şefliği' ve ' Klinik Şef Yardımcılığı' uygulaması kaldırılarak, yerine 'Eğitim görevlisi' statüsü ihdas edilmiş; ayrıca 'Eğitim sorumlusu' adı altında bir başka statü öngörülmüştür.

Yine 663 sayılı KHK'nin Geçici 6. maddesi ile 'Bu maddenin yayımı tarihinde görevde bulunan klinik şefi ve klinik şef yardımcılarının görevleri bu maddenin yayımı tarihinde sona erer. Bunlar eğitim görevlisi kadrolarına kazanılmış hak aylık dereceleriyle atanmış sayılır.' şeklinde bir düzenleme yapılmıştır.

Belirtilen tüm bu maddeler birbiriyle bağlantılı olduğundan; birlikte incelenip değerlendirme yapılması gerekli bulunmaktadır.

Klinik Şefliği ve Klinik Şef Yardımcılığı statüleri, evvelce 7.5.1987 tarih ve 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 1. maddesini ile öngörülmüştü. Maddenin konuya ilişkin düzenlemesi şöyleydi:

" Sağlık Bakanlığı eğitim ve araştırma hastanelerinde tıpta uzmanlık eğitimi Klinik Şefi, Klinik Şef yardımcısı, ilgili dalda profesör ve doçent unvanına sahip kişiler tarafından verilir ve bu kişiler eğitim sorumlusu olarak nitelendirilir. Klinik Şefi, Klinik Şef yardımcısı, başasistan ve asistan kadrolarına açıktan atama izni alınmaksızın ilgili mevzuatı çerçevesinde atama yapılır. Klinik Şefi, Klinik Şef Yardımcısı ve başasistan kadrolarına atamalar, ilgili dalda uzman olan tabipler arasından Bakanlıkça yapılacak veya yaptırılacak yazılı ve sözlü mesleki sınav sonuçlarına göre yapılır. Bu sınavlara mesleki çalışma, bilimsel yayın ve yabancı dilde yeterliliği bulunanlar katılabilir. Yeterlilik kriterleri ile sınavlara ilişkin usul ve esaslar yönetmelik ile düzenlenir.

Profesör veya doçentlerden klinik şefi veya klinik şef yardımcısı kadrolarına atanmak isteyenler için mevcut toplam kadroların % 35'ini geçmemek üzere kadro ayrılabilir. İlgili uzmanlık alanlarında profesör veya doçentlik unvanını almış olanlar Bakanlıkça yapılacak ilanda belirtilen kadrolardan sadece birisine müracaat edebilirler. Müracaat eden adayların bilimsel çalışmalarını ve eğitimci niteliklerini değerlendirmek üzere Bakanlık tarafından, ilgili uzmanlık alanlarında üç profesör veya

klirik Őefi tespit edilir. Bu profes6r veya klinik Őefleri, adaylar hakkında m6talaalarını, 6ncelik sıralaması yaparak ayrı ayrı Bakanlıđı bildirirler. Bakanlık bu m6talaalara g6re atamaları yapar"

Belirtilen bu yasa h6km6 ile bu h6k6m esas alınarak 6ıkartılan d6zenleyici tasarruflarla 'Klinik Őefliđi' ve 'Klinik Őef Yardımcılıđı' unvanları, Sađlık Bakanlıđı eđitim ve araŐtırma hastanelerinde bir kariyer basamađı olarak 6ng6r6lm6Ő ve belli prosed6rdan ge6ilerek ulaŐılan bu stat6ler, ilgilileri bakımından terfien ulaŐılmıŐ bir makam olarak d6zenlenmiŐti. Bu unvanları alarak s6zkonusu kadrolara s6re kaydı olmaksızın atamaları yapılanların idarece stat6lerine son verilmesi s6zkonusu olmamakta, ilgililer aksi y6nde bir talepleri olmadık6a yaŐ hadlerine kadar 'Klinik Őefi' ya da 'Klinik Őef Yardımcısı' unvanlarını muhafaza etmekteydiler. S6zkonusu yasal d6zenlemelerle hem bu unvanlar (stat6ler) kaldırılarak yerine 'eđitim g6revlisi' unvanı getirilmekte, hem de evvelce bu stat6y6 kazananların hukuki durumlarına son verilerek yeni getirilen sisteme 'eđitim g6revlisi' olarak intibakları 6ng6r6lmektedir. B6ylelikle bu konumdaki hekimler 6alıŐtıkları kliniklerin ya da birimlerin y6neticisi olmaktan 6ıkarılmakta, klinik personeli 6zerindeki bir takım hak ve tasarruflarına son verilmekte, yeni sistemde evvelce 6mir konumunda oldukları klinik hekimleriyle aynı stat6ye indirgenmekte, dolayısıyla mevzuatın 6ng6rd6đ6 belli koŐulları sađlayarak bu makamlara atanan kiŐiler, bu d6zenlemelerle haiz oldukları stat6leri ve unvanları bir anda yetirerek diđer klinik hekimleriyle (eski maiyetleriyle) eŐit duruma getirilmektedirler.

Anayasa'nın 2. maddesinde, T6rkiye Cumhuriyeti'nin nitelikleri arasında sayılan Hukuk Devleti ilkesi, hukuk g6venliđinin ve adaletin sađlanmasına y6nelik hukuk anlayıŐını yansıtmakta, yasaların kamu yararı amacıyla 6ıkarılmasını zorunlu kılmaktadır. Hukuk g6venliđi ve adalet kavramları ile istikrar arasında sıkı bir bađ bulunmaktadır. Hukuk g6venliđi ve adalet, 6ađdaŐ kamu y6netimi anlayıŐında, istikrar olgusunun temelini oluŐurmaktadır. Hukuk g6venliđi, kamu g6revlileri y6n6nden 6nemli bir g6vencedir. 663 sayılı KHK deđiŐikliđinden 6nceki d6zenlemede, Klinik Őefleri ve klinik Őef yardımcılarının kendi talepleri hari6, belli koŐulları sađlayarak ve s6re kaydı olmaksızın atandıkları anılan g6revlerden (kadrolardan) yaŐ haddinden 6nce bu stat6lerinin sona erdirilemeyeceđi konusunda yasal bir g6venceye sahip oldukları anlaŐılmaktadır. Yasayla elde edilen bu stat6n6n klinik Őefleri ve klinik Őef yardımcıları i6in kazanılmıŐ hak olarak deđerlendirilmesi olanaklı olmasa da, stat6lerin devam edeceđi yolunda meŐru bir beklentiye sahip oldukları, bu beklentinin ise hukuki g6venlik, adalet ve belirlilik ilkeleri geređince korunması gerektiđinin kabul6 zorunludur. Nitekim Anayasa Mahkemesinin konuya iliŐkin i6tihatları da bu dođrultudadır. (Any.Mah.nin 16.7.2010 tarih ve E.2010/29, K.2010/90; 9.6.2011 tarih ve E.2008/31, K.2011/94 sayılı kararları)

Davanın somutunda da görüleceği üzere, dava konusu düzenlemelerle klinik şefleri ve klinik şef yardımcılarının mevcut bu haklı beklentileri hiç dikkate alınmadan statülerine son verildiği ve yeni öngörülen sistemde eğitim sorumlusu unvanıyla evvelce maiyetlerinde olan hekimlerle aynı konuma getirildikleri açık olduğundan; bu düzenlemenin Anayasa'nın 2. maddesine aykırı düştüğü ve iptali gerektiği değerlendirilmektedir.

Yukarıda açıklanan nedenlerle dört başlık altında incelenen hükümlerin iptaline karar verilmesi kanaatine ulaştığımızdan; aksi yöndeki çoğunluk kararına katılmıyoruz.

Üye - Serdar ÖZGÜLDÜR

Üye - Zehra Ayla PERKTAŞ

DEĞİŞİK GEREKÇE

6.4.2011 günlü, 6223 sayılı Yetki Kanunu'nun 1. maddesinin (1) numaralı fıkrasının (b) bendi 'Kamu kurum ve kuruluşlarında istihdam edilen memurlar, işçiler, sözleşmeli personel ile diğer kamu görevlilerinin çalışmalarında etkinliği arttırmak üzere, bunların atanma, nakil, görevlendirme, seçilme, terfi, yükselme, görevden alınma ve emekliye sevk edilme usul ve esaslarına' ilişkin konularda düzenlemelerde bulunmak üzere, Bakanlar Kuruluna Kanun Hükmünde Kararname çıkarma yetkisi vermektedir. 663 sayılı KHK'nin 44. maddesinin (2), (3) ve (4) numaralı fıkraları memuriyet statüsüne alınmaya ilişkin bir düzenleme niteliğindedir. Oysa yukarıda ifade edildiği üzere 6223 sayılı Yetki Kanunu'nun belirtilen hükümleri salt 'istihdam edilen' kamu görevlileri bakımından bir düzenleme yapılabilmesi konusunda yetki vermektedir. Diğer bir deyişle söz konusu kurallar Yetki kanunu kapsamı dışında kalmakta ve bu mahiyeti itibarıyla de Anayasa'nın 91. maddesine aykırı düşmektedir.

Açıklanan nedenle, anılan kuralların iptaline bu gerekçeyle katılıyoruz.

Üye: Serdar ÖZGÜLDÜR; Burhan ÜSTÜN

KARŞIOY YAZISI

1- Reddi hakim talebinin kötü niyetle yapıldığı gerekçesiyle DİSİPLİN PARA CEZASI UYGULANMASINA yer olmadığına dair KARŞIOY:

İptal davasını açan Parti tarafından Başkan Haşim KILIÇ'ın reddi talebinin kötü niyetle yapıldığına ve 6216 sayılı Kanun'un 60. maddesinin (5) numaralı fıkrası gereğince disiplin para cezası uygulanmasına ilişkin çoğunluk kararına aşağıdaki nedenlerle katılmıyorum:

6216 sayılı Kanun'un 60. maddesinin (5) numaralı fıkrasında 'Ret talebinin kötü niyetle yapıldığının anlaşılması ve esas yönünden kabul edilmemesi halinde, talepte bulunanların her birine Mahkemece beşyüz Türk Lirasından beşbin Türk Lirasına kadar disiplin para cezası verilir' denilmiş; (6) numaralı fıkrasında 'Bu Kanun anlamında disiplin para cezasından maksat, bireysel başvuru hakkını veya ret talebini açıkça kötüye kullandığı tespit edilen başvurucular aleyhine verilen ' para cezası' olduğu belirtilmiştir. Buna göre para cezası verilebilmesi için öncelikle talebin esastan reddedilmesi gerekli olmakla birlikte yeterli değildir. Talepte kötü niyet olup olmadığı talebin yerinde olup olmadığı hususundan bağımsız olarak ayrıca incelenecek, varlığı açıkça saptanmışsa kötü niyete ilişkin para cezasına hükmedilebilecektir.

Reddi hakim talep etme hakkı Anayasa'nın 36. maddesinde yer alan hak arama hürriyetinin ve adil yargılanma hakkının gereğince kullanılmasını güvence altına alan bir hukuk müessesesidir. Temel hakların kötüye kullanılması gerekçesi, çoğu kez hakkın özüne dokunacak nitelikte kısıtlayıcı düşüncelere yönelebildiğinden, ihtiyatla kullanılmalı ve ancak açık, nesnel koşulların oluşması halinde başvurulmalıdır. Bu nedenle reddi hakim talepleri yönünden de kötü niyetin varlığı açık, somut ve nesnel delillere dayanmalıdır. Talebin gerekçelerinin yetersiz olması, davacının daha önce de benzeri nitelikte, kabul edilmeyen taleplerde bulunması, davacının mahkemeye ve hakime karşı itimatsızlığının bilinmesi, tek başına kötü niyetin kanıtlarını oluşturamazlar.

Olayda davacının reddi hakim talebinde bulunmasının kendi açısından hassasiyet yaratan bazı beyan ve olgulara dayandığı, bu bağlamda:

- Başkan Haşim KILIÇ'ın aleni bir konuşmada kullandığı ifadeler siyaset alanına giren eleştirilerdir. İyi işleyen demokrasilerde yüksek yargı başkanlarının siyaset alanına yönelik, ifade özgürlüğü kapsamında da olsa, yorum veya değerlendirme yapmaları olağan değildir. Öte yandan, Anayasa'nın 150. maddesine göre iptal davası açma hakkı Cumhurbaşkanına, iktidar ve ana muhalefet partisi Meclis gruplarına ve TBMM üye tamsayısının en az beşte biri tutarındaki üyelere ait olup, bunlardan Cumhurbaşkanının dava açması uygulamasına uzun süredir rastlanmadığı, iktidar partisinin dava açtığına ise hiç görülmediği bilinmektedir. Bu durumda eleştirinin hedefinin ana muhalefet olduğu açıktır.

- WIKILEAKS belgeleri her ne kadar hukuki bir işleme veya karara esas alınabilecek nitelikte değillerse de bunlarda geçen anlatımların davalı partide menfi yönde sübjektif kanaat veya kuşku uyandırmaya elverişli oldukları

anlaşılmaktadır.

Başkan Haşim KILIÇ'ın derdest olan davada tarafsız hareket edemeyeceği yönünde somut bir ret nedeni bulunmamakla birlikte Sayın Başkan'dan kaynaklanan nedenlerle davacıda bir hassasiyet doğmuş olduğu, dosyadaki evraktan anlaşılmaktadır. Bu nedenle olayda açıkça kötü niyet bulunduğu söylenemez. Para cezasına hükmedilmemesi gerekir.

II- KHK Kurallarına İlişkin Karşioy Gerekçeleri:

A) KHK hükümlerinin 6223 sayılı Yetki Kanunu Kapsamında Olmamaları Yönünden:

KHK'nin 58. maddesinin (8) numaralı fıkrasının (b) bendinde yapılan değişiklikle 1219 sayılı Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanun'un 4. maddesinin birinci cümlesindeki 'Türk hekimlerinin' ibaresi genel olarak hekimlik mesleği ile ilgili bir düzenleme olup, Yetki Yasasının bakanlıklar, bağlı ve ilgili kuruluşlar, kamu kuruluşlarında istihdam edilen memurlar, işçiler, sözleşmeli personel ve diğer kamu görevlileriyle ilgili düzenleme yetkisi vermesi nedeniyle kural, yetki yasası kapsamında değildir.

58. maddenin (9) numaralı fıkrasıyla 6283 sayılı Hemşirelik Kanunu'nun 3. maddesi değiştirilmiş ve hemşirelik mesleğinin genel olarak icrası ile ilgili bir kural getirilmiştir. Bu değişiklik özel sağlık kurumlarında hemşirelik yapılmasına ilişkin koşul getirdiğinden, Yetki Yasasının kapsamı dışındadır.

B) KHK Hükümlerinin Anayasa'nın 91. Maddesine Aykırı Olmaları Yönünden:

1- KHK'nin 6. maddesinin (2) ve (3) numaralı fıkraları:

Sağlık Politikaları Kurulunun üye yapısını ve özlük haklarını düzenleyen iptal istemine konu kurallar, daha önce kamu hizmetinde bulunmayan kişilerin kamu hizmetine girmelerini öngörmektedir. Kamu hizmetine girme hakkı Anayasa'nın 70. maddesinde düzenlenmiş olup, 91. maddenin birinci fıkrasına göre KHK ile düzenlenmesi yasak olan alandaki temel haklardandır. Bu nedenle kurallar, Anayasa'nın 91. maddesine aykırıdır, iptalleri gerekir.

2- KHK'nin 23. maddesinin (7) numaralı fıkrasının (a) bendi:

Maddenin (7) numaralı fıkrasının (c) ve (ç) bentleri, Anayasa'nın 38. maddesi kapsamında değerlendirilmesi gereken sağlık meslek mensuplarının meslekten geçici men ve meslekten men

edilmesini gerektiren fiiller ile bunlara uygulanacak yaptırımlara ilişkin hükümler içerdiğinden, Anayasa'nın 91. maddesinin birinci fıkrasına aykırı oldukları gerekçesiyle iptal edilmişlerdir.

Aynı konuda cezaya ek olarak öngörülen yaptırımları içeren (a) bendi, ölüme veya vücut fonksiyon kaybına sebep olanlar yönünden, ceza mahkumiyeti olmaksızın müstakil olarak uygulanacak nitelikte değildir. Bu nedenle diğer bentlerle aynı gerekçeyle iptali gerekir.

3-KHK'nin 24. maddesi:

İptali istenen madde, sağlık mesleklerinin uygulanmasından dolayı zarara uğradığını iddia edenlerin dava açma süresi içerisinde bu madde kapsamında yapacakları maddi ve manevi tazminat başvurularının Bakanlık tarafından halledilmesi yöntemini belirlemektedir.

Anayasa'nın 36. maddesinde hak arama hürriyeti, 74. maddesinde dilekçe, bilgi edinme ve Kamu Denetçisine başvurma hakkı düzenlenmiştir.

Sağlık mesleklerinin uygulanmasından dolayı zarara uğrayan vatandaşların doğrudan dava açmak veya dava açmadan önce Anayasa'nın öngördüğü idari yollara başvurmak, sonuç alamadığı takdirde dava açmak konusunda geniş bir tercih özgürlüğü bulunmaktadır. Bu hakların kullanımının kanunla düzenleneceği Anayasa'da belirtildiğinden kanun koyucunun sağlık mesleklerinin uygulanmasından doğan ihtilaflarda yasa ile belli bir yöntem öngörmesi mümkündür. Ancak iptali istenen yasal düzenleme Anayasanın 36. ve 74. maddelerindeki haklara ve bunların kullanımına takaddüm eden ön hazırlık ve işlemlere bazı sınırlamalar getirdiğinden, kanun hükmünde kararname ile değil yasa ile gerçekleştirilmelidir. Zira 36. ve 74. maddelerdeki temel haklar, Anayasa'nın 91. maddesinin birinci fıkrası gereğince KHK ile düzenlenmesi yasak olan hak ve hürriyetlerdendir. Kuralın bu nedenle iptali gerekir.

4- KHK'nin 32. maddesinin (2), (4) ve (5) numaralı fıkraları:

İptali istenen (2) numaralı fıkrada genel sekreter, idari ve mali hizmetler başkanları, hastane yöneticisi, müdür ve müdür yardımcısı olacak kişilerin; (4) numaralı fıkrada açıktan alınacak uzman ve büro görevlilerinin; (5) numaralı fıkrada ise kurum başkanları, başkanlar, hastane yöneticileri, başhekim ve müdürlerin işe alınış yöntem ve koşullarına ilişkin hükümler getirilmiştir.

Bahse konu görevler kamuda görev yapmayan kişiler yönünden Anayasa'nın 70. maddesindeki kamu hizmetine giriş hakkına taalluk etmektedir. Bu hak, Anayasa'nın 91. maddesine göre KHK'lerle düzenlenmesi yasak olan temel haklardan olup, kuralların iptali gerekir.

5- KHK'nin 33. maddesinin (1), (2), (3), (4) ve (6) numaralı fıkraları:

Maddenin (1), (2), (3), (4) ve (6) numaralı fıkralarında hakları düzenlenen personel, kamu hizmetine yeni giren kişileri de kapsamaktadır. Bunların kamu hizmetine girişinin dayanağı Anayasa'nın 70. maddesinde belirtilen temel hak olduğundan, bunlar hakkında KHK ile düzenleme yapılması mümkün değildir. Anayasal bakımdan yasak alan içinde yapılan ve anayasaya aykırı olan düzenlemelere dayanan mali hakların da Anayasal dayanağı bulunmamaktadır. Bu nedenle kurallar, Anayasa'nın 91. maddesine aykırıdır.

C) KHK Hükümlerinin İçerik Yönünden Anayasaya Aykırı Hükümleri:

1- 6. maddenin (1) ve (2) numaralı Fıkraları:

İptali istenen kurallar Sağlık Politikaları Kurulunun oluşumu, kurul üyelerinde aranacak nitelikler ve üyelerin görev süresine ilişkindir.

Sağlık sistemi ve politika belirleme ile ilgili temel görevleri ifa etmek üzere kurulan Sağlık Politikaları Kurulu üyelerinin, Anayasa'nın 128. maddesinde belirtilen devletin genel idare esaslarına göre yükümlü olduğu asli ve sürekli görevleri yürüten kamu görevlisi niteliğinde olduğunda kuşku bulunmamaktadır. Buna göre, Kurul üyelerinin sadece atanmaları değil, nitelikleri, görev ve yetkileri, hakları ve yükümlülükleri, aylık ve ödenekleri ile diğer özlük işlerinin kanunla düzenlenmesi gerekmektedir.

Anayasanın kanunla düzenlenmesini öngördüğü bir alanda sadece genel düzenlemelerin yapılarak geniş bir alanın idarenin takdirine bırakılması, anayasal anlamda kanunla düzenleme sayılmaz. İptali istenen kurallar yeterli açıklık ve belirliliği içermedikleri, geniş bir alanı idarenin takdirine bıraktıkları için kanunla düzenleme niteliğinde değildir. Bu nedenle Anayasa'nın 128. maddesine aykırı olan kuralların iptali gerekir.

2- 58. maddenin (6) numaralı fıkrasının (e) bendi ile (7) numaralı fıkrasının (a) bendi ve Geçici 6. maddesi:

İptali istenen kurullarla klinik şefi ve şef yardımcılarının görevleri sona erdirilerek, eğitim görevlisi haline getirilmişlerdir.

Kamu hizmetinde ve özellikle sağlık gibi temel bir alanda bilgi birikimi, deneyim, donanım ve liyakat kriterlerini gözetmeden yapılan düzenlemelerin, yasa koyucunun kamu görevlilerinin statüsünde, unvanlarında, görev ve yetkilerinde değişiklik yapmak konusundaki takdir hakkı ile açıklanması olanaklı değildir. İşin niteliği ve hizmetin gereği gibi kavramlar nesnel ve somut olup, yasa koyucunun gerekli yasal çerçeveyi belirlemeden idareye geniş bir hareket alanı bırakması, anayasaya uymaz. İdari görevlerle bilimsel ve mesleki yeterliliğin karıştırıldığı, sağlık konularında bilgisiz bir

yöneticinin sağlık alanında uzman yetiştirilmesinde görev alacak eğitimciyi belirleyebildiği düzenlemeler vatandaşın sağlık hakkını tehlikeye attığından Anayasa'nın 56. maddesine, kazanılmış hakları gözetmediğinden 2. maddesine ve yasa ile yeterli çerçeve çizilmediğinden 128. maddesine aykırıdır.

3- 58. maddenin (8) numaralı fıkrasının (a) bendi:

Kuralla, 1219 sayılı Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanun'un 4. maddesinin birinci cümlesinde değişiklik yapılarak, Türkiye'de hekimlik yapabilmek için Türk Üniversitelerinden diploma almış olmak şartı kaldırılmıştır. Fıkranın, Anayasaya aykırılığı Yeki Kanunu kapsamı dışında olması nedeniyle yukarıda ilgili bölümde açıklanan (b) bendi ile yabancıların Türkiye'de hekimlik yapabilmesi olanaklı hale geldiğinden, her iki kural birlikte değerlendirildiğinde, hangi ülke tıp fakültesinden diploma almış olursa olsun yabancıların Türkiye'de hekimlik yapabilmeleri yolunun açıldığı anlaşılmaktadır.

Anayasa'nın 5. maddesinde devletin temel amaç ve görevleri sayılmış, 56. maddesinde sağlık hakkı düzenlenmiştir.

Çağdaş ve insana saygılı ülkelerde sağlık hizmetinin, faşist rejimlerin insanı sadece devlete hizmet edebilmesi için iyi işlemesi gereken bir makine, sağlık hizmetini de makine bakımı olarak gören anlayışlarından farklı olarak, hasta-hekim diyalogu, güven, empati ve sosyal-kültürel uyum gibi boyutları da vardır. Bu nedenle, yabancı hekim ithali, sporcu veya mühendis ithalinden farklıdır. Kuşkusuz, yabancı ülkelerde her ırk ve dilden, çok iyi yetişmiş ve yetenekli hekimler de olabilir. Ancak yabancı hekimlerin diplomalarının akademik değeri, mesleki deneyim ve becerileri, toplumsal-kültürel konulardaki bilgi dereceleri gözetilmeden ve bu konularda tercih veya yeterlilik kriterleri getirilmeden yasa ile geniş bir serbesti tanınması, Anayasa'nın 5. ve 56. maddelerine ters düşer. Bu nedenle kuralın iptali gerekir.

Üye - Osman Alifeyyaz PAKSÜT

KARŞIOY GEREKÇESİ

11.10. 2011 günlü, 663 sayılı Kanun Hükmünde Kararname'nin; 6. maddesinin (2) ve (3) numaralı fıkraları, 23. maddesinin (7) numaralı fıkrasının (a) bendi, 32. maddesinin (2), (4) ve (5) numaralı fıkralarının incelenmesi;

Anayasa'nın 7. maddesinde, 'Yasama Yetkisi Türk Milleti adına Türkiye Büyük Millet Meclisindedir. Bu yetki devredilemez.' hükmü yer almıştır. Anayasa'nın 87. maddesinde ise, 'Bakanlar Kuruluna belli konularda kanun hükmünde kararname çıkarma yetkisi vermek' Türkiye Büyük Millet Meclisinin görev ve yetkileri arasında sayılmıştır.

Anayasa'nın 91. maddesinde 'Türkiye Büyük Millet Meclisi, Bakanlar Kuruluna kanun hükmünde kararname çıkarma yetkisi verebilir. Ancak sıkıyönetim ve olağanüstü haller saklı kalmak üzere, Anayasa'nın ikinci kısmının birinci ve ikinci bölümlerinde yer alan temel haklar, kişi hakları ve ödevleri ile dördüncü bölümünde yer alan siyasi haklar ve ödevler kanun hükmünde kararnamelerle düzenlenemez.' denilmektedir.

Yukarıya aynen alınan madde hükümlerinden yasama yetkisinin genel ve asli bir yetki olup devredilemeyeceği, kanun hükmünde kararname çıkarma yetkisinin ise kendine özgü istisnai bir yetki olduğu ve Anayasa'nın 91. maddesinde belirtilen sınırlar içinde kullanılabileceği anlaşılmaktadır.

Anayasa'nın 'siyasi haklar ve ödevler' başlıklı Dördüncü bölümünde yer alan 70. madde de ise 'Her Türk, kamu hizmetlerine girme hakkına sahiptir. Hizmete alınmada görevin gerektirdiği niteliklerden başka bir ayırım gözetilemez.' hükmü yer almıştır. Madde hükmü ile kamu hizmetlerine girme hakkı düzenlenirken, hizmete alınmada görevin gerektirdiği niteliklerden başka bir ayırım gözetilemeyeceği de belirtilmek suretiyle bu hakkın güvence altına alındığı açıktır.

Bu durumda 663 sayılı Kanun Hükmünde Kararname'nin Sağlık Politikaları Kurulunu düzenleyen 6. maddesinin (2) ve (3) numaralı fıkraları, Sağlık Meslekleri Kurulunu düzenleyen 23. maddesinin 7/a fıkrası ve Kamu Hastaneleri Birliği personelinin niteliği ve statüsünü düzenleyen 32. maddesinin (2), (4), ve (5) numaralı fıkraları, Anayasa'nın dördüncü bölümünde yer alan 70. maddede hüküm altına alınan 'kamu hizmetine girme hakkına' ilişkin olup, Anayasa'nın 91. maddesine göre Kanun Hükmünde Kararname ile düzenlenmesi mümkün olmayan yasak alan içindedir.

Açıklanan nedenlerle belirtilen kurallar, Anayasa'nın 7., 87. ve 91. maddelerine aykırı olduğu ve iptali gerektiği düşüncesiyle verilen karara katılmıyorum.

Üye - Zehra Ayla PERKTAŞ

KARŞI GÖRÜŞ

11.10.2011 günlü, 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin tümünün ve dava dilekçesinde gösterilen bazı maddelerinin Anayasa'ya aykırı olduğu gerekçesiyle iptali istenmiştir.

İptali istenen maddelerden birisi de KHK'nın 24. maddesidir. Dava dilekçesinde söz konusu hükmün, Anayasa'nın 2., 9., 36. ve 138. maddelerine aykırı olduğu ileri sürülmüştür.

Sağlık mesleklerinin icra edilmesi esnasında verilen zararların uzlaşma yoluyla tazmin edilmesine ilişkin 24. madde şöyledir:

'Uzlaştırma prosedürü

MADDE 24- (1) Sağlık mesleklerinin uygulanmasından dolayı zarara uğradığını iddia edenlerin dava açma süresi içerisinde bu madde kapsamında yapacakları maddî ve manevî tazminat başvuruları Bakanlık tarafından aşağıdaki şekilde uzlaşma yoluyla halledilir.

- a) Tazminat talebinde bulunan veya bunların birden fazla olması hâlinde aralarından seçecekleri bir temsilci,
- b) Zarar verdiği iddia olunan ilgili meslek mensubu veya bunların birden fazla olması hâlinde aralarından seçecekleri bir temsilci,
- c) Varsa ilgili meslek mensuplarının meslekî malî sorumluluk sigortasını yapan sigorta şirketinin temsilcisi veya bunların birden fazla olması hâlinde ise aralarından seçecekleri bir temsilci,

Bakanlık tarafından uzlaşmaya davet edilir. Tarafların uzlaşma yolunu kabul etmeleri hâlinde, üzerinde anlaşmış oldukları bir hukukçu uzlaştırıcı marifetiyle uzlaşma süreci başlatılır. Uzlaşma en fazla üç ayda sonuçlandırılır. Bu süre bilirkişi görüşleri alınmadığı hallerde tarafların kabulü ile altı aya kadar uzatılabilir. Uzlaşma müracaatı dava açma süresini durdurur. Uzlaşma sağlanamaması hâlinde taraflarca tanzim edilecek tutanak veya taraflardan birinin talebi üzerine Bakanlık tarafından taraflara tebliğ edilerek verilecek belge tarihinden itibaren dava açma süresi yeniden başlar. Uzlaşma sağlanırsa, uzlaşma konusunu, yerini, tarihini, yerine getirilmesi gereken hususları içeren uzlaşma tutanağı tanzim edilir. Bu tutanak 9/6/1932 tarihli ve 2004 sayılı İcra ve İflas Kanununun 38 inci maddesi anlamında ilâm niteliğindedir. Uzlaştırma masrafları ve arabulucu ücreti taraflarca karşılanır. Uzlaşma neticesinde belli bir bedel üzerinde uzlaşma sağlandığında bu bedel doğrudan sigortacı, sigortasının bulunmaması durumunda ilgili personel tarafından ödenir. Bakanlıkça bu madde kapsamında herhangi bir ödeme yapılmaz.

(2) Uzlaştırıcı, meslekî kusur bulunup bulunmadığı hususunda Yüksek Sağlık Şûrasının belirlediği bilirkişilerin; uğranıldığı iddia edilen zarar miktarının hesaplanmasında adlî yargı adalet komisyonları tarafından her yıl düzenlenecek olan listelerde yer alan bilirkişilerin görüşüne başvurabilir.'

Mahkememiz çoğunluk görüşünde, sağlık mesleklerinin uygulanmasından doğan zararın uzlaştırıcı aracılığı ile belirleneceği, bu yolun zorunlu olmadığı, belirlenen zararın varsa sigortacı, yoksa ilgili personel tarafından ödeneceği, Sağlık Bakanlığınca bu madde kapsamında herhangi bir ödeme yapılmamasının Anayasa'ya aykırı olmadığı sonucuna varılmıştır.

Ancak söz konusu kuralı Anayasa'nın 129. maddesinin beşinci fıkrası açısından da incelemek gerekmektedir.

Anayasa'nın 129. maddesinin beşinci fıkrasında: 'Memurlar ve kamu görevlilerinin yetkilerini kullanırken işledikleri kusurlardan doğan tazminat davaları, kendilerine rücu edilmek kaydıyla ve kanunun gösterdiği şekil ve şartlara uygun olarak, ancak idare aleyhine açılabilir.' hükmüne yer verilmiştir. Anayasa koyucu, bu hükümlerle, memurların görevleriyle ilgili olarak kusurlu davranışları ile zarar vermeleri halinde, doğrudan memura değil, idare aleyhine dava açılmasını emretmiş, ayrıca bu konuda oluşabilecek tereddütleri gidermek için "ancak idare aleyhine açılabilir." ifadesine yer vererek, bu konuda hiçbir istisnaya yer vermek istememiştir. Buna göre, memurun kusurlu davranışı nedeniyle zarara uğrayanlar, doğrudan idareye karşı dava açabilecek, memura karşı dava açılmayacak, idareye karşı açılan dava sonunda ilgili idare zarar görene tazminat ödemeye mahkûm edilirse, bunu tazmin edip daha sonra kusurlu memura rücu edebilecektir. Bu şekilde, bir taraftan, memurun kusurundan zarar görenler için, zararının tazmin edilmesi açısından, memura göre ödeme gücü çok daha yüksek idare muhatap olarak kabul edilerek onlara bir teminat oluşturulurken; diğer taraftan memurlar, açılan davalarla doğrudan karşı karşıya bırakılmayarak, onlara da bir teminat sağlanmakta, ciddi olmayan davalarla tedirgin edilmeleri engellenerek, görevlerini daha iyi yerine getirmeleri sağlanmaya çalışılmaktadır. Şu halde Anayasa m.129/5'te öngörülen sistemle, zarar görenle, zarar veren memur hem zararın belirlenmesi aşamasında, hem de ilamın icrası aşamasında karşı karşıya getirilmemektedir.

İptali istenilen kuralın birinci fıkrasında ise, genel mahkemelerde açılan davanın alternatifi olan uzlaşma yoluna başvurulurken, Anayasa m.129/5'de öngörülen sorumluluk sisteminin dışında farklı bir sistem getirilmekte, zarar veren memurla, zarar gören karşı karşıya getirilerek zararın miktarının belirlenmesi sağlanmakta, daha sonra da belirlenen zararı, sigorta varsa sigortacı, sigorta yoksa zarar veren memur bizzat kendisi ödeme yapmak zorunda bırakılmaktadır. Birinci fıkranın son cümlesinde

ise 'Bakanlıkça bu madde kapsamında herhangi bir ödeme yapılmaz.' denilerek bu husus pekiştirilmektedir. Bu süreçte Bakanlık, sadece uzlaşma sürecinin idare edilmesi görevini üstlenmiş olmaktadır.

Sağlık mesleklerinin icrası esnasında doğan zararların, uzlaşma yoluyla belirlenmesi halinde, uzlaşma yoluna başvurulmasının tarafların iradelerine dayanması, zarar görenle zarar veren memurun uzlaşma istememeleri halinde yahut süreç sonunda uzlaşma sağlanamaması halinde genel mahkemelerde dava yolunun açık olması, Anayasa m. 129/5 ile öngörülen sorumluluk sistemini tümüyle değiştirmeyi, hem zarar gören açısından, hem de zarar veren memur açısından getirilen teminatları kaldırmayı haklı kılmaz. Sağlık mesleklerinin icrası esnasında verilen zararın belirlenmesi için uzlaştırma yoluna başvurulabilir, bu yolla genel mahkemelerin iş yükü azaltılabilir, uyuşmazlığın daha kısa süre içinde ve uzlaşma yoluyla sonuçlanması sağlanabilir, bunda hem tarafların, hem de kamunun yararı vardır. Ancak, öngörülen sistemin Anayasa m. 129/5 ile kabul edilen sorumluluk sistemiyle de uyumlu olması gerekir.

Yukarıda belirtilen nedenlerle, 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 24. maddesinin birinci fıkrasının, Anayasa'nın 129. maddesinin beşinci fıkrasına aykırı olduğu ve iptali gerektiği kanaatinde olduğumdan, çoğunluk görüşüne katılmıyorum.

Üye - Erdal TERCAN

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2010/40

Karar Sayısı: 2012/8

Karar Günü: 19.1.2012

R.G. Tarih-Sayı: 06.03.2013-28579

İPTAL DAVASINI AÇAN: Anamuhalefet Partisi (Cumhuriyet Halk Partisi) TBMM Grubu adına Grup Başkanvekilleri Hakkı Suha OKAY, Kemal KILIÇDAROĞLU ve Kemal ANADOL

İPTAL DAVASININ KONUSU: 17.2.2010 günlü, 5952 sayılı Kamu Düzeni ve Güvenliği Müsteşarlığının Teşkilat ve Görevleri Hakkında Kanun'un;

1) 1. maddesinin, (1) numaralı fıkrasında yer alan "terörle mücadeleye ilişkin politika ve stratejileri geliştirmek ve bu konuda ilgili kurum ve kuruluşlar arasında koordinasyonu sağlamak üzere İçişleri Bakanlığına bağlı" bölümünün,

2) 2. maddesinin (1) numaralı fıkrasının (a) ve (d) bentlerinin,

3) 3. maddesinin,

4) 4. maddesinin (1) ve (2) numaralı fıkralarının,

5) 5. maddesinin;

a- (2) numaralı fıkrasında yer alan "Bakanın onayı ile özel ihtisas ve araştırma komisyonları"ibaresinin,

b- (3) numaralı fıkrasının,

6) 6. maddesinin;

a- (1) numaralı fıkrasında yer alan "Terörle" sözcüğünün,

b- (1) numaralı fıkrasının (a) ve (b) bentlerinin,

c- (1) numaralı fıkrasının (c) bendinde yer alan "veya yaptırmak' ibaresinin,

d- (1) numaralı fıkrasının (ç) bendinde yer alan 'Güvenlik kuruluşlarına" ve "ilgili kurumlara"ibarelerinin,

- e- (1) numaralı fıkrasının (f) bendinin,
- 7) 7. maddesinin (1) numaralı fıkrasında yer alan "Bakana" sözcüğünün,
- 8) 8. maddesinin,
- 9) 9. maddesinin (1) numaralı fıkrasının;
- a- (a) bendinin (1) numaralı alt bendinde yer alan "uygulanmasına yönelik eylem planları hazırlamak..."ibaresinin,
- b- (a) bendinin (2) numaralı alt bendinde yer alan 'Güvenlik kuruluşları" ibaresinin,
- c- (a) bendinin (3) numaralı alt bendinde yer alan 'Valilikler" sözcüğünün,
- d- (a) bendinin (4) numaralı alt bendinin,
- e- (b) bendinin (1) numaralı alt bendinde yer alan 'Veri, bilgi ve belgeleri toplamak, tasnif etmek," ibaresinin,
- f- (b) bendinin (2) numaralı alt bendinde yer alan "yaptırmak" sözcüğünün,
- g- (b) bendinin (4) numaralı alt bendinde yer alan "Terörle" sözcüğünün,
- 10) 10. maddesinin (1) numaralı fıkrasının;
- a- (b) bendinin (1) numaralı alt bendinin,
- b- (c) bendinin birinci cümlesinin "Bakan onayı ile en çok on Müsteşarlık Müşaviri pozisyon unvanıyla sözleşmeli personel çalıştırılabilir" bölümünün,
- c- (c) bendinin "Personelin sözleşme usul ve esasları Müsteşarlıkça tespit edilir ve bu Kanuna ekli (2) sayılı cetvelde belirlenen taban ve tavan ücretleri arasında kalmak üzere Müsteşarın teklifi ve Bakan onayı ile aylık brüt sözleşme ücreti ödenir. Ayrıca Müsteşarlıkta sözleşmeli personel olarak istihdam edilenler için belirlenen usul ve esaslar çerçevesinde ikramiye ve teşvik ikramiyesi ödenebilir. Bu statüde çalıştırılma, sözleşme bitiminde kamu kurum ve kuruluşlarında herhangi bir pozisyon, kadro veya statüde çalışma açısından kazanılmış hak teşkil etmez.' şeklindeki ikinci, üçüncü ve dördüncü cümlelerinin,
- 11) 13. maddesinin;
- a- (2) numaralı fıkrasının,
- b- (4) numaralı fıkrasının son cümlesinin,
- 12) 15. maddesinin (1) numaralı fıkrasının ikinci cümlesinin,

13) 16. maddesinin (1) numaralı fıkrasının ikinci cümlesinin,

14) 18. maddesinin;

a- (1) numaralı fıkrasının (a) ve (b) bentlerinin,

b- (3) numaralı fıkrasının (a) ve (b) bentlerinin,

c- (4) numaralı fıkrasının,

d- (5) numaralı fıkrasının,

Anayasa'nın 2., 5., 6., 7., 8., 11., 13., 20., 25., 95., 104., 113., 117., 123., 128., 138., 153., 159., 161. ve 162. maddelerine aykırılığı ileri sürülerek iptallerine ve yürürlüklerinin durdurulmasına karar verilmesi istemidir.

II- YASA METİNLERİ

A- İptali İstenen Yasa Kuralları

17.10.2010 günlü, 5952 sayılı Kanun'un iptali istenen sözcük, ibare, alt bent, bent, fıkra ve maddelerinin yer aldığı kurallar şöyledir:

'MADDE 1- (1) Bu Kanunun amacı; terörle mücadeleye ilişkin politika ve stratejileri geliştirmek ve bu konuda ilgili kurum ve kuruluşlar arasında koordinasyonu sağlamak üzere İçişleri Bakanlığına bağlı Kamu Düzeni ve Güvenliği Müsteşarlığının kurulması ile teşkilat, görev, yetki ve sorumluluklarına ilişkin esasları düzenlemektir.

MADDE 2- (1) Bu Kanunda geçen;

a) Bakan: İçişleri Bakanını,

b) Bakanlık: İçişleri Bakanlığını,

c) Kurul: Terörle Mücadele Koordinasyon Kurulunu,

ç) Müsteşar: Kamu Düzeni ve Güvenliği Müsteşarını,

d) Müsteşarlık: Kamu Düzeni ve Güvenliği Müsteşarlığını,

ifade eder.

MADDE 3- (1) Terörle mücadeleye ilişkin politika ve stratejileri geliştirmek ve bu konuda ilgili kurum ve kuruluşlar arasında koordinasyonu sağlamak üzere İçişleri Bakanlığına bağlı Kamu Düzeni ve Güvenliği Müsteşarlığı kurulmuştur.

MADDE 4- (1) Güvenlik kuruluşları ve ilgili kurumlar arasında terörle mücadele alanında gerekli koordinasyonu sağlamak, bu alandaki politika ve uygulamaları değerlendirmek amacıyla Terörle Mücadele Koordinasyon Kurulu kurulmuştur.

(2) Kurul, İçişleri Bakanının başkanlığında, Genelkurmay İkinci Başkanı, Jandarma Genel Komutanı, Milli İstihbarat Teşkilatı Müsteşarı, Adalet Bakanlığı Müsteşarı, İçişleri Bakanlığı Müsteşarı, Dışişleri Bakanlığı Müsteşarı, Kamu Düzeni ve Güvenliği Müsteşarı, Emniyet Genel Müdürü ve Sahil Güvenlik Komutanından oluşur. Gerekliğinde gündemle ilgili diğer kurum ve kuruluş temsilcileri de toplantıya davet edilebilir. Kurul İçişleri Bakanının daveti üzerine toplanır. Toplantı gündemi, Kurul üyelerinin görüşleri alınarak İçişleri Bakanı tarafından belirlenir. Kurulun sekreteryaya görevi Müsteşarlık tarafından yerine getirilir.

MADDE 5- (1) Müsteşarlık; Müsteşar, müsteşar yardımcıları ile ana hizmet, danışma ve yardımcı hizmet birimlerinden oluşur.

(2) Gerekli görüldüğünde görevleri ve hizmet süreleri belirtmek kaydıyla Müsteşarın teklifi ve Bakanın onayı ile özel ihtisas ve araştırma komisyonları kurulabilir.'

(3) Müsteşarlık teşkilatı ekli (1) sayılı cetvelde gösterilmiştir.

MADDE 6- (1) Terörle mücadele alanında;

- a) Politika ve stratejiler belirlenmesine yönelik çalışmalar yürütmek ve bu politika ve stratejilerin uygulamasını izlemek,
- b) Güvenlik kuruluşları ve istihbarat birimlerinden gelen stratejik istihbaratı değerlendirmek ve ilgili birimlerle paylaşmak,
- c) Gerekli araştırma, analiz ve değerlendirme çalışmaları yapmak veya yaptırmak,
- ç) Güvenlik kuruluşlarına ve ilgili kurumlara stratejik bilgi desteği sağlamak ve bunlar arasında koordinasyonu temin etmek,
- d) Kamuoyunu bilgilendirmek ve halkla iletişimi sağlamak,
- e) Uluslararası gelişmeleri Dışişleri Bakanlığı ve ilgili kurumlarla işbirliği içinde izlemek ve değerlendirmek,
- f) İnceleme ve denetleme yapmak ya da yaptırmak.

(2) Müsteşarlığın güvenlikle ilgili operasyonel bir görevi yoktur.'

MADDE 7- (1) Müsteşar, Müsteşarlığın en üst amiri olup, Müsteşarlığın görev ve hizmetlerinin mevzuata uygun olarak yürütülmesinden Bakana karşı sorumludur.

(2) Bu Kanunla belirlenen görevlerin ifasında Müsteşara yardımcı olmak üzere iki müsteşar yardımcısı görevlendirilir.

MADDE 8- (1) Terörle mücadele alanında oluşturulacak politika ve stratejiler ile alınacak tedbirlere esas olmak üzere, ilgili birimlerden stratejik istihbaratın alınması ve değerlendirilmesi amacıyla doğrudan Müsteşara bağlı İstihbarat Değerlendirme Merkezi oluşturulur. Bu çerçevede güvenlik kuruluşları ve istihbarat birimleri ile Dışişleri Bakanlığınca elde edilecek stratejik bilgi ve istihbarat bu merkezde değerlendirilir.

(2) Terörle mücadeleye yönelik strateji belirlemek amacıyla ihtiyaç duyulan istihbari bilgiler; Genelkurmay Başkanlığı, Dışişleri Bakanlığı, Milli İstihbarat Teşkilatı Müsteşarlığı, Jandarma Genel Komutanlığı, Emniyet Genel Müdürlüğü ve Sahil Güvenlik Komutanlığı tarafından Müsteşarlığa verilir. Bu bilgiler doğrultusunda yapılacak analiz ve değerlendirmeler ilgili birimlerle paylaşılır.

MADDE 9- (1) Müsteşarlığın ana hizmet birimleri ve görevleri şunlardır:

a) Planlama, Koordinasyon ve Sosyal Destek Daire Başkanlığı: Terörle mücadele politika ve stratejileri kapsamında;

- 1) Belirlenen politikaların uygulanmasına yönelik eylem planları hazırlamak ve uygulamayı izlemek,
- 2) Güvenlik kuruluşları arasında bilgi paylaşımını ve koordinasyonu sağlamak,
- 3) Valilikler arasında koordinasyonu sağlamak,
- 4) Belirlenen politikalar ile sosyo-ekonomik politikaların uyumlu bir şekilde yürütülmesi için ilgili kurumlar arasında koordinasyonu sağlamak,
- 5) Müsteşarlıkça verilecek diğer görevleri yapmak.

b) Araştırma-Geliştirme Daire Başkanlığı: Terörle mücadele alanında;

- 1) Veri, bilgi ve belgeleri toplamak, tasnif etmek, analiz ve değerlendirmeler yapmak,
- 2) Araştırma yapmak, yaptırmak ve bu alandaki bilimsel çalışmalarını desteklemek,
- 3) Toplantı, sempozyum, seminer, eğitim ve benzeri etkinlikler düzenlemek,
- 4) Terörle Mücadele Raporu hazırlamak,
- 5) Müsteşarlıkça verilecek diğer görevleri yapmak.

c) İletişim Daire Başkanlığı: Terörle mücadele politikaları kapsamında;

- 1) Kamuoyunu bilgilendirmek,
- 2) Toplum desteğinin sağlanmasına yönelik faaliyetleri yürütmek,
- 3) İlgili kamu kurum ve kuruluşları ile sivil toplum kuruluşlarının işbirliğini sağlamak,
- 4) Müsteşarlıkça verilecek diğer görevleri yapmak.

ç) Dış İlişkiler Daire Başkanlığı: Terörle mücadeleye ilişkin;

- 1) Yabancı devletlerdeki faaliyet ve gelişmeleri Dışişleri Bakanlığı ve ilgili diğer kurumlarla işbirliği içinde izlemek ve tedbirler geliştirmek,
- 2) Uluslararası gelişmeleri ve deneyimleri takip etmek ve uygulamaya kazandırmak,
- 3) İlgili uluslararası kurum ve kuruluşlarla işbirliği yapmak,
- 4) Müsteşarlıkça verilecek diğer görevleri yapmak.

MADDE 10- (1) Müsteşarlığın danışma birimleri ve görevleri şunlardır:

a) Strateji Geliştirme Daire Başkanlığı:

- 1) Ulusal kalkınma strateji ve politikaları ile yıllık program çerçevesinde Müsteşarlığın orta ve uzun vadeli kurumsal strateji ve politikalarını belirlemek üzere gerekli çalışmaları yapmak.
- 2) Müsteşarlığın görev alanına giren konularda performans ve kalite ölçütleri geliştirmek, izlemek, değerlendirmek, sürekli gelişim için önerilerde bulunmak.
- 3) Müsteşarlık bütçesini stratejik plana ve yıllık hedeflere göre hazırlamak ve Müsteşarlık faaliyetlerinin bunlara uygunluğunu izlemek ve değerlendirmek.
- 4) Müsteşarlığın iç denetime yönelik işlevinin etkinliğini ve verimliliğini artırmak için gerekli hazırlıkları yapmak.
- 5) Müsteşarlığın yıllık idari faaliyet raporunu hazırlamak.
- 6) Müsteşarlıkça verilecek diğer görevleri yapmak.

b) Hukuk Müşavirliği:

- 1) Terörle mücadele mevzuatını ve uygulamasını değerlendirmek, günün şartlarına göre geliştirmek.
- 2) Güvenlik ve terörle mücadele ile ilgili kanun, tüzük ve yönetmelik taslakları ile diğer hukuki konular hakkında görüş bildirmek.

3) Terörle mücadeleye ilişkin uluslararası mevzuatı takip etmek.

4) Müsteşarlıkça verilecek diğer görevleri yapmak.

c) Müsteşarlık Müşavirleri: Terörle mücadele alanında özel bilgi ve ihtisasından yararlanılmak üzere, 657 sayılı Devlet Memurları Kanunu ve diğer kanunların sözleşmeli personel çalıştırılması hakkındaki usul ve esaslara bağlı olmaksızın, Bakan onayı ile en çok on Müsteşarlık Müşaviri pozisyon unvanıyla sözleşmeli personel çalıştırılabilir. Personelin sözleşme usul ve esasları Müsteşarlıkça tespit edilir ve bu Kanuna ekli (2) sayılı cetvelde belirlenen taban ve tavan ücretleri arasında kalmak üzere Müsteşarın teklifi ve Bakan onayı ile aylık brüt sözleşme ücreti ödenir. Ayrıca Müsteşarlıkta sözleşmeli personel olarak istihdam edilenler için belirlenen usul ve esaslar çerçevesinde ikramiye ve teşvik ikramiyesi ödenebilir. Bu statüde çalıştırılma, sözleşme bitiminde kamu kurum ve kuruluşlarında herhangi bir pozisyon, kadro veya statüde çalışma açısından kazanılmış hak teşkil etmez.

MADDE 13- (1) Müsteşarlıkta; Müsteşar, Müsteşar Yardımcısı, I. Hukuk Müşaviri, Daire Başkanı, Hukuk Müşaviri, Uzman, Çözümleyici, Programcı, Mütercim, İstatistikçi, Mühendis, Sosyolog, Psikolog, Antropolog ve Veri Hazırlama ve Kontrol İşletmeni kadroları karşılık gösterilmek suretiyle, 657 sayılı Kanun ve diğer kanunların sözleşmeli personel çalıştırılması hakkındaki hükümlerine bağlı olmaksızın sözleşmeli personel çalıştırılabilir.

(2) Ayrıca özel uzmanlık isteyen konularda kadro karşılığı olmaksızın tam gün veya kısmi gün veya belli bir konu veya proje bazında, konu veya projenin süresi ile sınırlı olmak koşuluyla sözleşmeli personel ve yabancı uzman çalıştırılabilir. Bunlara ödenecek ücret Müsteşarın teklifi üzerine Bakan onayı ile belirlenir.

(3) Sözleşmeli olarak çalıştırılacak personel ve uzmanlara bu Kanuna ekli (2) sayılı cetvelde unvanlar itibarıyla yer alan taban ve tavan ücretleri arasında aylık brüt sözleşme ücreti ödenir. Sözleşmeli personel ve uzman çalıştırmaya ilişkin esaslar ve ödenecek ücret Müsteşarın teklifi üzerine Bakan onayı ile tespit edilir. Sözleşmeler Müsteşar tarafından imzalanır.

(4) Başbakanlık merkez teşkilatında sözleşmeli olarak çalıştırılan emsali personelin yararlandığı ücret artışlarından Müsteşarlıkta çalışan sözleşmeli personel de aynı usul ve esaslara göre aynen yararlandırılır. Söz konusu personele, çalıştıkları günlerle orantılı olarak (hastalık ve yıllık izinleri dahil) Ocak, Nisan, Temmuz ve Ekim aylarında birer aylık sözleşme ücreti tutarında ikramiye ödenir. Bunlardan üstün gayret ve çalışmaları sonucunda emsallerine göre başarılı çalışma yaptıkları tespit edilenlere Müsteşarın teklifi üzerine Bakan onayı ile Haziran ve Aralık aylarında birer aylık sözleşme

ücreti tutarına kadar teşvik ikramiyesi ödenebilir. Bu fıkranın uygulanmasına ilişkin usul ve esaslar ile söz konusu personele yapılacak diğer ödemeler Müsteşarın teklifi üzerine Bakan onayı ile tespit edilir.

MADDE 15- (1) Müsteşarlık, bu Kanunla belirlenen görevlerin ifasında bakanlıklar, kurum ve kuruluşlar ile işbirliği içerisinde çalışır. Bu kapsamda Müsteşarlık tarafından istenen her türlü bilgi ve belge talebi; ilgili bakanlık, kurum ve kuruluşlar tarafından gecikmeksizin yerine getirilir.

MADDE 16- (1) Müsteşarlık, 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununa tabi genel bütçeli bir idaredir. Bu Kanun kapsamında yürütülen ve gizlilik ihtiva eden işler için 5018 sayılı Kanunun 24 üncü maddesi esaslarına göre Müsteşarlık bütçesine ödenek konulur.

MADDE 18- (1) 657 sayılı Kanuna ekli;

a) (I) sayılı cetvelin 'VIII. Mülki İdare Amirliği Hizmetleri Sınıfı' bölümünün (a) bendine 'Müsteşar,' ibaresinden sonra gelmek üzere 'Kamu Düzeni ve Güvenliği Müsteşarı,'

b) (II) sayılı cetvelin '4. Başbakanlık ve Bakanlıklarda' bölümüne "Nüfus ve Vatandaşlık Müdürü," ibaresinden sonra gelmek üzere 'İl Sosyal Etüt ve Proje Müdürü,'

ibareleri eklenmiştir.

(2) 10/10/1984 tarihli ve 3056 sayılı Başbakanlık Teşkilatı Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabulü Hakkında Kanunun 12 nci maddesinin birinci fıkrasının (a) bendinde yer alan 've terörle mücadele' ibaresi yürürlükten kaldırılmış ve (b) bendinde yer alan ' , dış güvenlik ve terörle mücadeleyi' ibaresi 've dış güvenliği' şeklinde değiştirilmiştir.

(3) 14/2/1985 tarihli ve 3152 sayılı İçişleri Bakanlığı Teşkilat ve Görevleri Hakkında Kanunun;

a) 28 inci maddesine aşağıdaki fıkra eklenmiştir.

'Güvenlik politikaları ve sosyo-ekonomik politikaların uyumlu bir şekilde yürütülmesini sağlamak üzere, illerde İl Sosyal Etüt ve Proje Müdürlüğü kurulmuştur. Bu amaçla, ihtiyaç duyulan ilçelerde valiliğin teklifi ve Bakanlığın onayı ile büro kurulabilir. Valilik, kadro, yer ve unvanlarına bakılmaksızın ihtiyaç durumuna göre uzman, sözleşmeli personel ve memurları bu birimlerde görevlendirmeye yetkilidir.'

b) 29 uncu maddesinin birinci fıkrasına aşağıdaki bent eklenmiştir.

'd) Kamu Düzeni ve Güvenliği Müsteşarlığı.'

(4) 5018 sayılı Kanuna ekli (I) sayılı cetvele 33 üncü sırasından sonra gelmek üzere '34) Kamu Düzeni ve Güvenliği Müsteşarlığı' ibaresi eklenmiş ve diğer sıralar buna göre teselsül ettirilmiştir.

(5) 27/6/1989 tarihli ve 375 sayılı Kanun Hükmünde Kararnamenin ek 3 üncü maddesinin birinci fıkrasına 'Savunma Sanayii Müsteşarlığı,' ibaresinden sonra gelmek üzere 'Kamu Düzeni ve Güvenliği Müsteşarlığı,' ibaresi eklenmiştir.'

B- Dayanılan Anayasa Kuralları

Dava dilekçesinde, Anayasa'nın 2., 5., 6., 7., 8., 11., 13., 20., 25., 95., 104., 113., 117., 123., 128., 138., 153., 159., 161. ve 162. maddelerine dayanılmıştır.

III- İLK İNCELEME

Anayasa Mahkemesi İctüzüğü'nün 8. maddesi gereğince Haşim KILIÇ, Osman Alifeyyaz PAKSÜT, Fulya KANTARCIOĞLU, Ahmet AKYALÇIN, Mehmet ERTEN, Serdar ÖZGÜLDÜR, Şevket APALAK, Serruh KALELİ, Zehra Ayla PERKTAŞ, Engin YILDIRIM ve Nuri NECİPOĞLU'nun katılmalarıyla 8.6.2010 gününde yapılan ilk inceleme toplantısında;

1- 17.2.2010 günlü, 5952 sayılı Kamu Düzeni ve Güvenliği Müsteşarlığının Teşkilat ve Görevleri Hakkında Kanun'un 6. maddesinin (1) numaralı fıkrasının (a) bendine ilişkin dava dilekçesindeki noksanlığın verilen süre içerisinde giderilmemesi nedeniyle, 2949 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 27. maddesinin beşinci fıkrası uyarınca bu bent yönünden iptal davasının açılmamış sayılmasına,

2- 5952 sayılı Yasa'nın 6. maddesinin (1) numaralı fıkrasının (a) bendi dışındaki iptali istenen kurallar yönünden, dosyada eksiklik bulunmadığından işin esasının incelenmesine,

3- Yürürlüğü durdurma isteminin esas inceleme aşamasında karara bağlanmasına, oybirliğiyle karar verilmiştir.

IV- ESASIN İNCELENMESİ

Dava dilekçesi ve ekleri, Raportör Mustafa ÇAĞATAY tarafından hazırlanan işin esasına ilişkin rapor, iptali istenen Yasa kuralları, dayanılan Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

A- İptal Başvurusundan Sonra Yapılan Değişikliklerin İptal Konusu Kurallara Etkisi

1- 3.6.2011 günlü, 643 sayılı Kanun Hükmünde Kararname ile Yapılan Değişiklik

İptal başvurusundan sonra 8.6.2011 gün ve 27958 sayılı Resmi Gazete'de (mükerrer) yayımlanarak yürürlüğe giren 3.6.2011 günlü, 643 sayılı '3046 sayılı Kanun ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun Hükmünde Kararname'nin 2. maddesiyle 3046 sayılı Kanun'a 19/A maddesi eklenmiştir.

643 sayılı KHK ile yapılan değişiklikle; Bakanlık bağlı, ilgili ve ilişkili kuruluşları (10/12/2003 tarihli ve 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanununa ekli (III) sayılı cetvelde yer alan kurumlar dahil) Başbakanın teklifi ve Cumhurbaşkanının onayı ile, Başbakanlıkla veya diğer bakanlıklarla ilgilendirilebileceği, söz konusu kuruluşların özel kanunlarında bağlı, ilgili ve ilişkili olunan bakanlığa ya da bakana verilen yetki ve görevlerin ilgilendirilen bakanlık veya bakan tarafından kullanılacağı ve yerine getirileceği kurala bağlanmıştır.

Anılan KHK'nin verdiği yetkiye dayanılarak Başbakanlığın 7.7.2011 günlü, B.02.0.PPG.0.12-300-02/7062 sayılı teklifi ve Cumhurbaşkanlığının aynı gün ve B.01.0.KKB.01-08/D-1-507 sayılı onayıyla İçişlerine bağlı olarak kurulan Kamu Düzeni ve Güvenliği Müsteşarlığı, Başbakanlık'la ilgilendirilmiştir. Bu durumda;

Kanun'un 1. maddesinin, (1) numaralı fıkrasının "Terörle Mücadeleye İlişkin Politika ve Stratejileri Geliştirmek ve Bu Konuda İlgili Kurum ve Kuruluşlar Arasında Koordinasyonu Sağlamak Üzere İçişleri Bakanlığına Bağlı" bölümü,

Kanun'un 2. maddesinin (1) numaralı fıkrasının (a) bendi,

Kanun'un 3. maddesi,

Kanun'un 4. maddesinin (2) numaralı fıkrası,

Kanun'un 5. maddesinin (2) numaralı fıkrasındaki "Bakanın Onayı İle Özel İhtisas ve Araştırma Komisyonları" ibaresi,

Kanun'un 7. maddesinin (1) numaralı fıkrasındaki "Bakana" sözcüğü,

Kanun'un 10. maddesinin (1) numaralı fıkrasının (c) bendinin "Bakan onayı ile en çok on Müsteşarlık Müşaviri pozisyon unvanıyla sözleşmeli personel çalıştırılabilir. Personelin sözleşme usul ve esasları Müsteşarlıkça tespit edilir ve bu Kanuna ekli (2) sayılı cetvelde belirlenen taban ve tavan ücretleri arasında kalmak üzere Müsteşarın teklifi ve Bakan onayı ile aylık brüt sözleşme ücreti ödenir. Ayrıca Müsteşarlıkta sözleşmeli personel olarak istihdam edilenler için belirlenen usul ve esaslar çerçevesinde ikramiye ve teşvik ikramiyesi ödenebilir. Bu statüde çalıştırılma, sözleşme bitiminde

kamu kurum ve kuruluşlarında herhangi bir pozisyon, kadro veya statüde çalışma açısından kazanılmış hak teşkil etmez.' bölümü,

Kanun'un 13. maddesinin (2) numaralı fıkrası,

Kanun'un 18. maddesinin (3) numaralı fıkrasının (b) bendiyle 3152 sayılı Kanun'un 29. maddesinin birinci fıkrasına eklenen (d) bendi,

643 sayılı Kanun Hükmünde Kararname'nin 2. maddesi ile 3046 sayılı Kanun'a eklenen 19/A maddesinin verdiği yetkiyle Başbakanlığın 7.7.2011 günlü, B.02.0.PPG.0.12-300-02/7062 sayılı teklifi ile Cumhurbaşkanlığının aynı gün ve B.01.0.KKB.01-08/D-1-507 sayılı onayıyla yürürlükten kaldırıldığından, söz konusu madde, fıkra, bent, bölüm, ibare ve sözcüğe ilişkin konusu kalmayan iptal istemi hakkında karar verilmesine yer olmadığına karar verilmesi gerekir.

Fulya KANTARCIOĞLU, Osman Alifeyyaz PAKSÜT, Zehra Ayla PERKTAŞ ile Nuri NECİPOĞLU;

Kanun'un 1. maddesinin, (1) numaralı fıkrasındaki iptal konusu bölüm ile 3. maddesi için verilen karar verilmesine yer olmadığına kararına 'Sadece 'İçişleri Bakanlığına bağlı' ibaresi için karar verilmesine yer olmadığına karar verilmesi gerektiği',

Kanun'un 4. maddesinin (2) numaralı fıkrası için verilen karar verilmesine yer olmadığına kararına 'Sadece 'İçişleri Bakanının' ve 'İçişleri Bakanı' ibareleri yönünden karar verilmesine yer olmadığına karar verilmesi gerektiği',

Kanun'un 5. maddesinin (2) numaralı fıkrasındaki iptal konusu ibare ile 13. maddesinin (2) numaralı fıkrası için verilen karar verilmesine yer olmadığına kararına 'Sadece 'Bakanın' sözcüğü için karar verilmesine yer olmadığına karar verilmesi gerektiği',

Kanun'un 10. Maddesinin (1) numaralı fıkrasının (c) bendinin iptal konusu bölümü için verilen karar verilmesine yer olmadığına kararına 'Sadece bölümde yer alan 'Bakan' sözcüğü ile "ve bu Kanuna ekli (2) sayılı cetvelde belirlenen taban ve tavan ücretleri arasında kalmak üzere Müsteşarın teklifi ve Bakan onayı ile aylık brüt sözleşme ücreti ödenir. Ayrıca Müsteşarlıkta sözleşmeli personel olarak istihdam edilenler için belirlenen usul ve esaslar çerçevesinde ikramiye ve teşvik ikramiyesi ödenebilir. " ibaresi yönünden karar verilmesine yer olmadığına karar verilmesi gerektiği',

yönündeki gerekçeyle katılmamışlardır.

2- 11.10.2011 günlü, 666 sayılı Kanun Hükmünde Kararname ile Yapılan Değişiklik

Kanun'un 13. maddesinin (4) numaralı fıkrasının son cümlesi, 11.10.2011 günlü, 666 sayılı Kanun Hükmünde Kararname'nin 1. maddesiyle 375 sayılı Kanun Hükmünde Kararname'ye eklenen ek 12. maddenin (3) numaralı fıkrasının (n) bendiyle,

Kanun'un 18. maddesinin (5) numaralı fıkrasıyla 375 sayılı Kanun Hükmünde Kararname'nin Ek 3. maddesinin birinci fıkrasına 'Savunma Sanayi Müsteşarlığı,' ibaresinden sonra gelmek üzere eklenen 'Kamu Düzeni ve Güvenliği Müsteşarlığı,' ibaresi, 11.10.2011 günlü, 666 sayılı Kanun Hükmünde Kararname'nin 1. maddesiyle 375 sayılı Kanun Hükmünde Kararname'ye eklenen ek 12. maddenin (1) numaralı fıkrasının (m) bendiyle,

yürürlükten kaldırıldığından, söz konusu cümle ve ibareye ilişkin konusu kalmayan iptal istemi hakkında karar verilmesine yer olmadığına karar verilmesi gerekir.

3- 10.10.2011 günlü, 657 sayılı Kanun Hükmünde Kararname ile Yapılan Değişiklik

Kanun'un 18. maddesinin(1) numaralı fıkrasının (a) bendiyle 14.7.1965 günlü, 657 sayılı Devlet Memurları Kanunu'na ekli (I) sayılı cetvelin 'VIII. Mülki İdare Amirliği Hizmetleri Sınıfı' bölümünün (a) bendine 'Müsteşar,' ibaresinden sonra gelmek üzere eklenen 'Kamu Düzeni ve Güvenliği Müsteşarı,' ibaresi, 10.10.2011 günlü, 657 sayılı Kanun Hükmünde Kararname'nin 37. maddesiyle,

yürürlükten kaldırıldığından, söz konusu ibareye ilişkin konusu kalmayan iptal istemi hakkında karar verilmesine yer olmadığına karar verilmesi gerekir.

B- Kanun'un 2. Maddesinin (1) Numaralı Fıkrasının (d) Bendinin İncelenmesi

Dava dilekçesinde; Kanun'un 1. maddesinin (1) numaralı fıkrasında yer alan ibareye yönelik iptal istemindeki gerekçelerle kuralın Anayasa'nın 2., 6., 7., 8., 13., 95., 113. ve 123. maddelerine aykırı olduğu ileri sürülmüştür.

Dava dilekçesinde yollama yapılan kurala ilişkin gerekçede ise 3046 sayılı 'Bakanlıkların Kuruluş ve Görev Esasları Hakkında 174 sayılı Kanun Hükmünde Kararname ile 13.12.1983 gün ve 174 sayılı Bakanlıkların Kuruluş ve Görev Esasları Hakkında Kanun Hükmünde Kararnamenin Bazı Maddelerinin Kaldırılması ve Bazı Maddelerinin Değiştirilmesi Hakkında 202 sayılı Kanun Hükmünde Kararnamenin Değiştirilerek Kabulü Hakkında Kanun'un 16. maddesinin (d) bendinde yer alan 'Bir bakanlıkta birden fazla müsteşarlık kurulamaz' biçimindeki kural uyarınca İçişleri Bakanlığına bağlı ikinci bir müsteşarlık kurulamayacağı, 3046 sayılı Kanun'da müsteşarlıkların örgütlenmesinde öngörülmeleyen 'merkez', 'il müdürlüğü' ve 'büro' şeklindeki bir yapılanmanın mümkün olmadığı, yine 3046 sayılı Kanun uyarınca bağlı kuruluşların ancak genel müdürlük olarak örgütlenmelerinin zorunlu bulunduğu, kuralda geçen 'terör' kavramının tanımının yapılmaması ya

da ilgili mevzuata atıfta bulunulmadığı belirtilerek kuralın Anayasa'nın 2., 6., 7., 8., 13., 95., 113. ve 123. maddelerine aykırı olduğu ileri sürülmüştür.

İptali istenen kuralda, Kanun'da geçen 'Müsteşarlık' ibaresinin Kamu Düzeni ve Güvenliği Müsteşarlığını ifade ettiği belirtilmiştir. Kuralda, terör sözcüğüne yer verilmediği gibi Müsteşarlığın İçişleri Bakanlığına bağlı olduğuna ve Müsteşarlığın örgütlenme biçimine ilişkin hükümler de yer almamaktadır. Ayrıca, 3.6.2011 günlü, 643 sayılı Kanun Hükmünde Kararname'nin 2. maddesi ile 3046 sayılı Kanun'a eklenen 19/A maddesinin verdiği yetkiyle Başbakanlığın 7.7.2011 günlü, B.02.0.PPG.0.12-300-02/7062 sayılı teklifi ile Cumhurbaşkanlığının aynı gün ve B.01.0.KKB.01-08/D-1-507 sayılı onayıyla Kamu Düzeni ve Güvenliği Müsteşarlığı İçişleri Bakanlığına bağlı olmaktan çıkarılıp, Başbakanlıkla ilgilendirilmiştir.

Bir yasa kuralının başka bir yasa kuralı ile uyumlu olmaması onun iptal edilmesini gerektiren bir durum değildir. Anayasa Mahkemesi yasaların başka yasalara ya da daha alt düzeydeki diğer normlara uygunluğunu değil, yasaların Anayasa'ya uygunluğunu denetlemektedir.

Dava dilekçesinde ileri sürülen kurala ilişkin Anayasa'ya aykırılık gerekçelerinin bir kısmının kuralla ilgisinin bulunmaması, bir kısım gerekçelerin ise yukarıda belirtilen yasal değişikliklerle ortadan kalkması nedeniyle iptal isteminin reddine karar vermek gerekmiştir.

Açıklanan nedenlerle, iptali istenen kural, Anayasa'nın 2., 6., 7., 8., 13., 95., 113. ve 123. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

C- Kanun'un 4. Maddesinin (1) Numaralı Fıkrasının İncelenmesi

Dava dilekçesinde; iptali istenen kuralda geçen 'güvenlik kuruluşları' ve 'terör' kavramının tanımlarının yapılmaması nedeniyle, bu kavramların neyi işaret ettiği hususunun belirsiz olduğu, 'terör' kavramının tanımına yer verilmemiş olması veya ilgili mevzuata atıfta bulunulmamış olması karşısında idareye uygulamada 'terör' kapsamını belirleme yetkisinin dolaylı olarak verildiği, terör kavramının tanımının yapılmamasının kanunun uygulanmasında kişisel hak ve hürriyetlerin sınırlandırılmasına neden olabileceği, kurul başkanlığı ve buna bağlı olarak daire başkanlığı, şube müdürlüğü ve şeflik biçiminde bir yapılanmaya gidilmeksizin Terörle Mücadele Koordinasyon Kurulu adında bağımsız bir kurulun kurulmasının 3046 sayılı Kanun'a uygun bulunmadığı belirtilerek, iptali istenen kuralın Anayasa'nın 2., 6., 7., 8., 13., 95., 113. ve 123. maddelerine aykırı olduğu ileri sürülmüştür.

İptali istenen fıkrada Terörle Mücadele Koordinasyon Kurulunun kuruluş amacı belirtilmektedir. Buna göre adı geçen Kurul'un görevi, güvenlik kuruluşları ve ilgili kurumlar arasında terörle

mücadele konusunda gerekli koordinasyonu sağlamak ve bu alandaki politika ve uygulamaları değerlendirmektir. 3046 sayılı Kanun'un 39. maddesinde görevleri ve kuruluş biçimleri kanunlarında veya diğer kanunlarda gösterilmesi kaydıyla, gerektiğinde sürekli kurullar kurulabileceği belirtilmektedir. Kuralda öngörülen Terörle Mücadele Koordinasyon Kurulunun, 3046 sayılı Kanun'un 39. maddesi anlamında, istişari nitelikte bir kurul olduğu anlaşılmaktadır.

Anayasa'nın 2. maddesinde, Türkiye Cumhuriyeti'nin bir hukuk devleti olduğu belirtilmiştir. Hukuk devletinin temel ilkelerinden biri de 'belirlilik'tir. Bu ilkeye göre, yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olması, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi gereklidir. Belirlilik ilkesi, bireylerin hukuksal güvenliğinin sağlanması bakımından da önem arz etmektedir

Anayasa'nın 7. maddesinde 'Yasama yetkisi Türk Milleti adına Türkiye Büyük Millet Meclisi'nindir. Bu yetki devredilemez'; Anayasa'nın 8. maddesinde ise 'Yürütme yetkisi ve görevi, Cumhurbaşkanı ve Bakanlar Kurulu tarafından, Anayasaya ve kanunlara uygun olarak kullanılır ve yerine getirilir.' denilmektedir.

Anayasa'nın 113. maddesinde, Bakanlıkların kurulması, kaldırılması, görevleri, yetkileri ve teşkilatının kanunla düzenleneceği hükmü yer almaktadır.

Anayasa'nın 123. maddesinde ise 'İdare, kuruluş ve görevleriyle bir bütündür ve kanunla düzenlenir. İdarenin kuruluş ve görevleri, merkezden yönetim ve yerinden yönetim esaslarına dayanır. Kamu tüzelkişiliği, ancak kanunla veya kanunun açıkça verdiği yetkiye dayanılarak kurulur' denilmektedir.

Bir yasa kuralının başka bir yasa kuralı ile uyumlu olmaması onun iptal edilmesini gerektiren bir durum değildir. Anayasa Mahkemesi yasaların başka yasalara ya da daha alt düzeydeki diğer normlara uygunluğunu değil, yasaların Anayasa'ya uygunluğunu denetlemekte olduğundan, bu gerekçeye dayanan Anayasa'ya aykırılık savları yerinde değildir. Kaldı ki, Anayasa'nın 113. maddesinde bakanlıkların kurulması, kaldırılması, görevleri, yetkileri ve teşkilatının kanunla düzenleneceği belirtilmek suretiyle bu konuda yasama organına takdir yetkisi tanınmıştır. Yasama organının bu takdir yetkisini 3046 sayılı Kanun çerçevesinde ya da başka bir kanunla da kullanabileceği açıktır.

Anayasa'nın 123. maddesinde anlamını bulan idarenin bütünlüğü ilkesi, tek tip yapılanmayı gerektirmemektedir. Yasakoyucu, anayasal sınırlar içinde kalmak koşuluyla, merkezden yönetim ve yerinden yönetim esaslarına uygun olarak değişik yapılanmaya da gidebilir. Anayasa'nın 123.

maddesinde öngörülen idarenin yaptığı işlem ve eylemlerin kanuna dayalı olması zorunluluğu, yasama organı için geçerli değildir. Bir başka ifadeyle idarenin kanuniliği ilkesi, idare organına hitap etmektedir. Yasakoyucu, yasamanın asliliği ve genelliği ilkesinin bir gereği olarak, Anayasa'da düzenlenmeyen bir alanı doğrudan düzenleyebilir. Bu bağlamda, yasama organının daha önce çıkardığı 3046 sayılı Kanun'a göre işlem yapması gerektiği yönündeki düşüncenin idarenin kanuniliği ilkesiyle bir ilgisi bulunmamaktadır.

5952 sayılı Kanun'da 'terör' kavramının tanımına yer verilmemiştir. Terör kavramının tanımındaki belirsizlikten dolayı terörle mücadeleyi konu edinen uluslararası sözleşmelerde terörle ilgili bir tanıma yer verilmemiş, sadece terör eylemleri olarak nitelendirilebilecek suçlara ilişkin ayrıntılı bir liste yapılmış ise de Türk Hukukunda terör kavramının tanımının 12.4.1991 günlü, 3713 sayılı Terörle Mücadele Kanunu'nun 1. maddesinde yapılmıştır. 3713 sayılı Kanun'da yer alan terör tanımı, öğreti ve yargısal kararlarda da benimsenmiştir. Bu durumda, mevzuatta tanımı yapılmış, uygulamada yerleşmiş, uygulama ve öğretinin yardımıyla açıklık kazanmış 'terör' kavramının belirsiz olduğundan söz edilemez. Dolayısıyla, kavramın içeriğinin belirlenmesi konusunda yasama yetkisinin devri de söz konusu değildir.

Öte yandan, iptali istenen kuralda geçen 'güvenlik kuruluşları' ibaresinin Kanun'un genel gerekçesinde de belirtildiği üzere, iç güvenlik kuruluşları olan Jandarma Genel Komutanlığı, Emniyet Genel Müdürlüğü ve Sahil Güvenlik Komutanlığı, Genelkurmay Başkanlığı, Kara Kuvvetleri Komutanlığına bağlı bazı askeri birlikler ile Milli İstihbarat Teşkilatını ifade ettiği açık olduğundan, söz konusu ibarenin de belirsiz olduğu sonucu çıkarılamaz.

Açıklanan nedenlerle, iptali istenen kural, Anayasa'nın 2., 6., 7., 113. ve 123. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın Anayasa'nın 8., 13. ve 95. maddeleriyle ilgisi görülmemiştir.

D- Kanun'un 5. Maddesinin (3) Numaralı Fıkrasının İncelenmesi

Dava dilekçesinde; 5952 sayılı Kanun'un 1. maddesinin (1) numaralı fıkrasının birinci cümlesindeki ibareye ilişkin gerekçeler doğrultusunda, iptali istenen fıkranın Anayasa'nın 2., 6., 7., 8., 13., 95., 113. ve 123. maddelerine aykırı olduğu ileri sürülmüştür.

İptali istenen kuralda, Müsteşarlık teşkilatının kimlerden oluştuğunun Kanun'a eklenen (1) sayılı cetvelde gösterildiği ifade edilmektedir. Dava dilekçesinde, Kamu Düzeni ve Güvenliği Müsteşarlığının İçişleri Bakanlığına bağlı ayrı bir müsteşarlık olarak kurulmasının Anayasa'ya aykırı olduğunun iddia edilmesi üzerine, bu kabulün doğal sonucu olarak söz konusu müsteşarlığın alt

birimlerini düzenleyen kuralın da Anayasa'ya aykırılığı nedeniyle iptalinin istendiği anlaşılmaktadır. Ancak iptal başvurusunun yapılmasından sonra yürürlüğe giren 643 sayılı Kanun Hükmünde Kararname'nin verdiği yetkiye dayanılarak Başbakanlığın 7.7.2011 günlü, B.02.0.PPG.0.12-300-02/7062 sayılı teklifi ve Cumhurbaşkanlığının aynı gün ve B.01.0.KKB.01-08/D-1-507 sayılı onayıyla İçişlerine bağlı olarak kurulan Kamu Düzeni ve Güvenliği Müsteşarlığı, Başbakanlıkla ilgilendirilmiştir. Bu durumda, dava dilekçesinde iptali istenen kural için ileri sürülen Anayasa'ya aykırılık gerekçeleri ortadan kalkmıştır. Kuralın Anayasa'ya aykırı başka bir yönü de bulunamamıştır.

Açıklanan nedenlerle iptali istenen kural, Anayasa'nın 2., 6., 7., 8., 13., 95., 113. ve 123. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

E- Kanun'un 6. Maddesinin İncelenmesi

1- (1) Numaralı Fıkrasında Yer Alan "Terörle" Sözcüğünün İncelenmesi

Dava dilekçesinde; maddenin (1) numaralı fıkrasında yer alan 'terör' kavramının tanımına yer verilmemiş olması veya ilgili mevzuata atıfta bulunulmamış olması karşısında idareye uygulamada 'terör' kapsamını belirleme yetkisinin dolaylı olarak verildiği, terör kavramının tanımının yapılmamasının kanunun uygulanmasında kişisel hak ve hürriyetlerin sınırlandırılmasına neden olabileceği belirtilerek, iptali istenen sözcüğün Anayasa'nın 2., 7., 8. ve 13. maddelerine aykırı olduğu ileri sürülmüştür.

Kanun'un 4. maddesinin (1) numaralı fıkrasının incelendiği bölümde belirtilen Anayasa'nın 2. ve 7. maddelerine ilişkin gerekçelerle kuralda Anayasa'ya aykırı bir yön bulunmamaktadır. İptal isteminin reddi gerekir.

Kuralın Anayasa'nın 8. ve 13. maddeleriyle ilgisi görülmemiştir.

2- (1) Numaralı Fıkranın (b) Bendi ile (ç) Bendinde Yer Alan "Güvenlik kuruluşlarına" ve "İlgili kurumlara" İbarelerinin İncelenmesi

Dava dilekçesinde; Kanun'un 6. maddesinin (1) numaralı fıkrasının (b) bendi ile (ç) bendinde geçen 'güvenlik kuruluşları' ve 'ilgili kurumlar' ibarelerinin belirsiz olduğu ifade edilerek iptali istenen bent ve ibarelerin Anayasa'nın 2., 7., 8. ve 13. maddelerine aykırı olduğu ileri sürülmüştür.

İptali istenen ibarelerin yer aldığı kurallarda, Müsteşarlığın terörle mücadele alanında güvenlik kuruluşları ve istihbarat birimlerinden gelen stratejik istihbaratı değerlendirip, ilgili birimlerle

paylaşacağı, güvenlik kuruluşlarına ve ilgili kurumlara stratejik bilgi desteği sağlayacağı ve bunlar arasında koordinasyonu temin edeceği hükme bağlanmıştır.

Kanun'un 4. maddesinin (1) numaralı fıkrasının incelendiği bölümde belirtilen Anayasa'nın 2. ve 7. maddelerine ilişkin gerekçelerle kuralda Anayasa'ya aykırı bir yön bulunmamaktadır. İptal isteminin reddi gerekir.

Kanun'un 6. maddesinin (1) numaralı fıkrasının (ç) bendinde geçen 'ilgili kurumlar' ibaresinin maddenin bir bütün olarak yorumlandığında terörle mücadele alanında görev yapan ve güvenlik kuruluşları dışında kalan diğer kamu kurumlarını ifade ettiği açıkça anlaşılmaktadır. Terörle mücadele, çok boyutlu bir mücadeledir. Bu mücadelenin güvenlik boyutu yanında, sosyolojik, psikolojik, adli, idari, ekonomik, siyasi bir çok boyutu ya da nedeni bulunmakta ve dolayısıyla bir çok kamu kurumu da işin içine müdahil olabilmektedir. Keza ortaya çıkış nedenlerine bağlı olarak terörün farklı yansımaları bulunmaktadır. Bu anlamda, terörle mücadele alanında, bakanlıklardan bağımsız idari kurullara kadar pek çok kamu kurumu arasında işbirliği ya da koordinasyona ihtiyaç bulunması kaçınılmazdır. Kuralda söz konusu 'ilgili kurumlar'ın teker teker sayılmasına gerek bulunmamaktadır.

Açıklanan nedenlerle, Kanun'un 6. maddesinin (1) numaralı fıkrasının (ç) bendinde geçen "ilgili kurumlar" ibaresi, Anayasa'nın 2. ve 7. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralların Anayasa'nın 8. ve 13. maddeleriyle ilgisi görülmemiştir.

3- (1) Numaralı Fıkranın (c) Bendinde Yer Alan "veya yaptırmak" İbaresini ile (f) Bendinin İncelenmesi

Dava dilekçesinde; kuralla idareye muhatabı, yaptırımı ve sınırları belirsiz bir araştırma, analiz, değerlendirme, inceleme ve denetleme çalışmaları yapması veya yaptırabilmesine yetki verilmesinin Anayasa'nın 2., 7., 8. ve 13. maddelerine aykırı olduğu ileri sürülmüştür.

İptali istenen ibarenin de yer aldığı (c) bendindeki kuralla, Kamu Düzeni ve Güvenliği Müsteşarlığına, terörle mücadele alanında gerekli araştırma, analiz ve değerlendirme çalışmalarını bizzat yapabilme ya da kurum dışındaki kurum ya da kuruluşlar aracılığıyla yaptırabilme yetkisi, (f) bendinde ise Kamu Düzeni ve Güvenliği Müsteşarlığına, terörle mücadele alanında inceleme ve denetleme yapmak ya da yaptırmak görevi verilmektedir.

'Teröristle mücadele', esas itibarıyla güvenlik kuvvetlerinin yürüttüğü silahlı mücadeleyi, 'terörle mücadele' ise güvenlik tedbirleriyle birlikte toplumsal, ekonomik ve kültürel alanlarda devletin bütün kurumları ve sivil toplum kuruluşlarının topyekun mücadelesini ifade etmektedir. Bu

bağlamda, Kamu Düzeni ve Güvenliği Müsteşarlığına terörle mücadele alanında gerektiğinde konusunda uzman olan kişi, kurum veya kuruluşlardan yardım alabilme ya da inceleme ve denetleme yapabilme yetkisinin tanınması, Kurumun işlevlerini yerine getirmesi açısından bir gereklilik olarak ortaya çıkmaktadır.

İptali istenen her iki kuralda 'araştırma, analiz ve değerlendirme çalışmaları' ile 'inceleme ve denetleme' yapmak ya da yaptırmanın 'terörle mücadele' alanıyla ilgili ve sınırlı olarak yapılacağı hususu açıkça belirtildiğinden sınırsız bir yetki devrinden söz edilemez.

Açıklanan nedenlerle, Kanun'un 6. maddesinin (c) bendinde yer alan 'veya yaptırmak' ibaresi ile (f) bendi, Anayasa'nın 2., 7. ve 8. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralların Anayasa'nın 13. maddesiyle ilgisi görülmemiştir.

F- Kanun'un 8. Maddesinin İncelenmesi

Dava dilekçesinde; 3046 sayılı Kanun'un 16. maddesinin (d) bendinde yer alan 'Bir bakanlıkta birden fazla müsteşarlık kurulamaz' biçimindeki kural uyarınca İçişleri Bakanlığına bağlı ikinci bir müsteşarlık kurulamayacağı, aynı Kanun'un 15. maddesinde bakanlık merkez teşkilatının müsteşarlık, müsteşarlığa bağlı genel müdürlük, kurul veya daire başkanlığı, genel müdürlük veya kurul başkanlığına bağlı şube müdürlüğü şeklinde bir örgütlenmenin öngörüldüğü, iptali istenen kuralla öngörülen 'merkez' şeklinde bir yapının oluşturulmasının 3046 sayılı Kanun'a göre mümkün olmadığı, iptali istenen kuralda Mevzuat Hazırlama Usul ve Esasları Hakkında Yönetmelik hükümlerine göre tüm mevzuatın incelenerek yasalar arasında uyumun sağlanması gerektiği, kuralda geçen 'terör' kavramının tanımının yapılmadığı ya da ilgili mevzuata atıfta bulunulmadığı, öngörülen düzenlemenin idarenin kanuniliği ilkesine aykırı olduğu, ayrıca kuralın ikinci fıkrasıyla Genelkurmay Başkanlığı, Dışişleri Bakanlığı ve Milli İstihbarat Teşkilatı Müsteşarlığı tarafından Müsteşarlığa ihtiyaç duyulan istihbari bilgilerin verilmesinin buyurucu biçimde düzenlendiği ve herhangi bir sınırlama da getirilmediği belirtilerek kuralın Anayasa'nın 2., 7., 8., 13., 95., 104., 113. ve 123. maddelerine aykırı olduğu ileri sürülmüştür.

İptali istenen kuralda, müsteşara bağlı olarak kurulan İstihbarat Değerlendirme Merkezinin kuruluş amacı ve görevi ile ihtiyaç duyulan istihbari bilgilerin güvenlik kuruluşları, istihbarat birimleri ve Dışişleri Bakanlığınca Müsteşarlığa verilmesi hususları düzenlenmektedir. Kuralda ayrıca, istihbari bilgiler doğrultusunda Müsteşarlıkça yapılacak analiz ve değerlendirmelerin de ilgili birimlerle paylaşılacağı belirtilmektedir.

Kanun'un 4. maddesinin (1) numaralı fıkrasının incelendiği bölümde belirtilen gerekçelerle, iptali istenen kural, Anayasa'nın 2., 7., 113. ve 123. maddelerine aykırı değildir. İptal isteminin reddi gerekir. Kuralın Anayasa'nın 8., 13., 95. ve 104. maddeleriyle ilgisi görülmemiştir.

G- Kanun'un 9. Maddesinin (1) Numaralı Fıkrasının İncelenmesi

1- (a) Bendinin (1) Numaralı Alt Bendinde Yer Alan "uygulanmasına yönelik eylem planları hazırlamak" İbaresinin İncelenmesi

Dava dilekçesinde; Kanun'un 6. maddesinde müsteşarlığa verilen görevlerin sadece politika ve stratejilerin belirlenmesine yönelik çalışmalar yürütmek olduğu belirtilmişken, iptali istenen kuralla belirlenen politikaların uygulanmasına ilişkin eylem planları hazırlamanın da müsteşarlığın ana hizmet birimi olarak öngörülen Planlama, Koordinasyon ve Sosyal Destek Daire Başkanlığının görevleri arasında sayılmak suretiyle Kanun'un maddeleri arasında uyumsuzluğa yol açıldığı, ayrıca kuralla yürütme organına kaynağı Anayasa'da bulunmayan bir yetki verildiği belirtilerek, kuralın Anayasa'nın 2. ve 6. maddelerine aykırı olduğu ileri sürülmüştür.

İptali istenen kuralda, Kamu Düzeni ve Güvenliği Müsteşarlığının ana hizmet birimlerinden olan Planlama, Koordinasyon ve Sosyal Destek Daire Başkanlığının, terörle mücadele politika ve stratejileri kapsamında belirlenen politikaların uygulanmasına yönelik eylem planları hazırlamakla görevli olduğu belirtilmektedir.

Bir yasa kuralının başka bir yasa kuralı ile uyumlu olmaması onun iptal edilmesini gerektiren bir durum değildir. Anayasa Mahkemesi yasaların başka yasalara ya da daha alt düzeydeki diğer normlara uygunluğunu değil, yasaların Anayasa'ya uygunluğunu denetlemekte olduğundan, bu gerekçeye dayanan Anayasa'ya 2. maddesine aykırılık savı yerinde değildir. Kuralın Anayasa'ya aykırı başka bir yönü de bulunmamıştır.

Anayasa'nın 6. maddesinde egemenliğin, kayıtsız şartsız Millete ait olduğu, Türk Milletinin egemenliğini, Anayasa'nın koyduğu esaslara göre, yetkili organları eliyle kullanacağı, egemenliğin kullanılmasının, hiçbir surette hiçbir kişiye, zümreye veya sınıfa bırakılmayacağı ve hiçbir kimse veya organın kaynağını Anayasa'dan almayan bir Devlet yetkisi kullanamayacağı ifade edilmiştir.

Anayasa'da engelleyici bir hüküm bulunmaması durumunda yasakoyucunun genel düzenleme yapma yetkisine dayanarak kural koyması, kaynağını Anayasa'dan almayan bir yetkinin kullanılması anlamına gelmez. İptali istenen kuralla, Müsteşarlık bünyesinde ana hizmet birimi olarak düzenlenen Planlama, Koordinasyon ve Sosyal Destek Daire Başkanlığına, kurumun amaçları doğrultusunda belirlenen politikaların uygulanmasına yönelik eylem planları hazırlamak görevinin verilmesi,

Anayasa'da buna ilişkin engelleyici bir hüküm olmadığı gözetildiğinde, Anayasa'nın 6. maddesine aykırılık tan söz edilemez.

Açıklanan nedenlerle, iptali istenen ibare, Anayasa'nın 2. ve 6. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

2- (a) Bendinin (2) Numaralı Alt Bendinde Yer Alan 'Güvenlik kuruluşları' İbaresinin İncelenmesi

Dava dilekçesinde; 'güvenlik kuruluşları' ibaresinin neyi işaret ettiğinin belirsiz olduğu ve kuralın Anayasa'nın 2., 5., 7., 8., 13., 104. ve 123. maddelerine aykırı olduğu ileri sürülmüştür.

İptali istenen ibarenin de yer aldığı kuralda, Müsteşarlığın ana hizmet birimlerinden olan Planlama, Koordinasyon ve Sosyal Destek Daire Başkanlığının, terörle mücadele politika ve stratejileri kapsamında güvenlik kuruluşları arasında bilgi paylaşımını ve koordinasyonu sağlamakla görevli olduğu belirtilmektedir.

Kanun'un 4. maddesinin (1) numaralı fıkrasının incelendiği bölümde belirtilen Anayasa'nın 2. maddesine ilişkin gerekçelerle kuralda Anayasa'ya aykırı bir yön bulunmamaktadır. İptal isteminin reddi gerekir.

Kuralın Anayasa'nın 5., 7., 8., 13., 104. ve 123. maddeleriyle ilgisi görülmemiştir.

3- (a) Bendinin (3) Numaralı Alt Bendinde Yer Alan 'Valilikler' Sözcüğünün İncelenmesi

Dava dilekçesinde; kuralla ilgili mevzuatla uyum gözetilmeden valilikler arasında koordinasyon sağlanmasına ilişkin düzenleme yapılmasının Anayasa'nın 2. ve 104. maddelerine aykırı olduğu ileri sürülmüştür.

İptali istenen sözcüğün de yer aldığı kuralda, Müsteşarlığın ana hizmet birimlerinden olan Planlama, Koordinasyon ve Sosyal Destek Daire Başkanlığının, terörle mücadele politika ve stratejileri kapsamında valilikler arasında koordinasyonu sağlamakla görevli olduğu belirtilmektedir.

Bir yasa kuralının başka bir yasa kuralı ile uyumlu olmaması onun iptal edilmesini gerektiren bir durum değildir. Anayasa Mahkemesi yasaların başka yasalara ya da daha alt düzeydeki diğer normlara uygunluğunu değil, yasaların Anayasa'ya uygunluğunu denetlemekte olduğundan, bu gerekçeye dayanan Anayasa'ya 2. maddesine aykırılık savı yerinde değildir. Kuralın Anayasa'ya aykırı başka bir yönü de bulunamamıştır. İptal isteminin reddi gerekir.

Kuralın Anayasa'nın 104. maddesiyle ilgisi görülmemiştir.

4- (a) Bendinin (4) Numaralı Alt Bendinin İncelenmesi

Dava dilekçesinde; Kanun'un 6. maddesinde müsteşarlığa verilen görevlerin sadece politika ve stratejilerin belirlenmesine yönelik çalışmalar yürütmek olduğu belirtilmişken, iptali istenen kuralla belirlenen politikalar ile sosyo-ekonomik politikaların uyumlu bir şekilde yürütülmesi için ilgili kurumlar arasında koordinasyonu sağlamanın da müsteşarlığın ana hizmet birimi olarak öngörülen Planlama, Koordinasyon ve Sosyal Destek Daire Başkanlığının görevleri arasında sayılmak suretiyle Kanun'un maddeleri arasında uyumsuzluğa neden olduğu, ayrıca kuralda yer alan 'belirlenen politikalar' ve 'ilgili kurumlar' gibi müphem ve sınırları belli olmayan kavramlarla yürütme organına asli düzenleme yetkisi verildiği belirtilerek, kuralın Anayasa'nın 2. ve 7. maddelerine aykırı olduğu ileri sürülmüştür.

İptali istenen kuralda, Kamu Düzeni ve Güvenliği Müsteşarlığının ana hizmet birimlerinden olan Planlama, Koordinasyon ve Sosyal Destek Daire Başkanlığının, terörle mücadele politika ve stratejileri kapsamında belirlenen politikalar ile sosyo-ekonomik politikaların uyumlu bir şekilde yürütülmesi için ilgili kurumlar arasında koordinasyonu sağlamakla görevli olduğu belirtilmektedir.

Terörle mücadele alanında politikanın belirlenmesi Kamu Düzeni ve Güvenliği Müsteşarlığına ait bir görev olmayıp, Müsteşarlığın görevi politikaların belirlenmesine yönelik hazırlık çalışmaları yapmaktır. Kuralda, Planlama, Koordinasyon ve Sosyal Destek Daire Başkanlığına terörle mücadele alanında politika belirleme yetkisi verilmesi söz konusu değildir.

Kanun'un 6. maddesinin (1) numaralı fıkrasının (ç) bendinin incelendiği bölümde belirtilen gerekçelerle, iptali istenen kuralda geçen 'ilgili kurumlar' ibaresinin Anayasa'ya aykırı bir yönü bulunmamaktadır.

Açıklanan nedenlerle, iptali istenen kural, Anayasa'nın 2. ve 7. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

5- (b) Bendinin (1) Numaralı Alt Bendinde Yer Alan 'Veri, bilgi ve belgeleri toplamak, tasnif etmek,' İbaresinin İncelenmesi

Dava dilekçesinde; iptali istenen kuralla herhangi bir sınırlama getirilmeksizin Araştırma-Geliştirme Daire Başkanlığına 'veri, bilgi ve belgeleri toplamak, tasnif etmek' görevinin verildiği, 'veri, bilgi ve belgeleri toplama'nın her türlü kişisel verileri de kapsama alacağı, veri toplamanın sınırlarına yasal düzenleme getirilmeyerek kişilerin idareye karşı korumasız bırakıldığı belirtilerek, kuralın Anayasa'nın 13., 20. ve 25. maddelerine aykırı olduğu ileri sürülmüştür.

İptali istenen kuralda Kamu Düzeni ve Güvenliği Müsteşarlığının ana hizmet birimlerinden olan Araştırma-Geliştirme Daire Başkanlığının terörle mücadele alanında, veri, bilgi ve belgeleri toplayabileceği, tasnif edebileceği, analiz ve değerlendirmeler yapabileceği hükme bağlanmaktadır.

Anayasa'nın 20. maddesinde, herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı ifade edilmiştir. Maddede ayrıca kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hükmüne de yer verilmiştir.

Anayasa'nın 13. maddesinde, temel hak ve hürriyetlerin, özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği, bu sınırlamaların Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacağı belirtilmiştir.

İptali istenen kuralda geçen 'veri', 'bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done' anlamına gelmekte olup, bilimsel, istatistiki, ekonomik, kişisel bilgileri de içine alan bir kavramdır. Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Ancak söz konusu hak sınırsız değildir. Kişisel verilerin korunması hakkı, veri sahibinin mutlak ve sınırsız bir veri hakimiyetini mümkün kılmamaktadır. Nitekim Türkiye'nin imzaladığı ancak uygulama kanununun yürürlüğe konamaması nedeniyle taraf olmadığı 1981 tarihli ve 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Avrupa Konseyi Sözleşmesi'nin 9. maddesinde de devlet güvenliği, kamu güvenliği, devletin ekonomik menfaatlerinin korunması ve suçlarla mücadele edilmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması ile verilerin istatistiki veya bilimsel amaçlarla kullanılması durumlarında kişisel verilerin korunmasına sınırlamalar getirilebileceği öngörülmüştür. Bu nedenle, kişisel verilerin korunması temel hakkına kamu yararı nedenlerine dayalı olarak müdahale edilebilmesine olanak tanınmaktadır.

Terörle mücadele alanında strateji ve politikalar geliştirmekle görevli olan Kamu Düzeni ve Güvenliği Müsteşarlığının kendisine verilen görevleri yerine getirebilmesi için kişisel veriler de dahil olmak üzere bir takım bilgi ve belgelere ihtiyacının bulunması kaçınılmazdır. İptali istenen kuralda, veri ve bilgilerin terörle mücadele alanıyla sınırlı olacağı açıkça ifade edilmiştir. Kuralda kişisel verilerin

korunmasıyla ilgili olarak Anayasa'nın 20. maddesinde öngörülen güvencelere aykırı bir hüküm de yer almamaktadır. Türk Ceza Kanunu'nun kişisel verilerin korunmasına ilişkin cezai hükümleri, Müsteşarlık personeli için de geçerlidir. Bu nedenle, dava konusu kuralla Kamu Düzeni ve Güvenliği Müsteşarlığına terörle mücadele alanıyla sınırlı olmak üzere verilen veri ve bilgi toplama yetkisinin özel hayatın gizliliği kapsamında kişisel verilerin korunmasını isteme hakkına ölçsüz bir müdahale olduğu söylenemez. Ayrıca, söz konusu düzenlemenin kişisel verilerin korunmasını isteme hakkını aşırı derecede zorlaştıran ya da ortadan kaldıran, dolayısıyla hakkın özüne dokunan bir sınırlama olmadığı da açıktır.

Açıklanan nedenlerle, iptali istenen kural, Anayasa'nın 13. ve 20. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Fulya KANTARCIOĞLU, Mehmet ERTEN, Osman Alifeyyaz PAKSÜT, Zehra Ayla PERKTAŞ ile Engin YILDIRIM bu görüşe katılmamışlardır.

Kuralın Anayasa'nın 25. maddesiyle ilgisi görülmemiştir.

6- (b) Bendinin (2) Numaralı Alt Bendinde Yer Alan "yaptırmak" Sözcüğünün İncelenmesi

Dava dilekçesinde; iptali istenen kuralla Araştırma ' Geliştirme Daire Başkanlığına muhatabı, yaptırımı ve sınırları belirsiz bir araştırma yaptırmaya yetkisinin tanınmasının Anayasa'nın 2., 5. ve 13. maddelerine aykırı olduğu ileri sürülmüştür.

İptali istenen kuralda, Müsteşarlığın ana hizmet birimlerinden olan Araştırma ' Geliştirme Daire Başkanlığının, terörle mücadele alanında, araştırma yaptırabileceği hükme bağlanmaktadır. Kural, anılan Daire Başkanlığının Müsteşarlık dışındaki kurum, kuruluş veya uzmanlar aracılığıyla terörle mücadele alanında araştırmalar yaptırılabilmesine olanak tanımaktadır.

Kanun'un 6. maddesinin (1) numaralı fıkrasının (c) bendinde yer alan "veya yaptırmak" şeklindeki ibarenin incelendiği bölümde belirtilen gerekçelerle, iptali istenen sözcük, Anayasa'nın 2. ve 5. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın Anayasa'nın 13. maddesiyle ilgisi görülmemiştir.

7- (b) Bendinin (4) Numaralı Alt Bendinde Yer Alan "Terörle" Sözcüğünün İncelenmesi

Dava dilekçesinde; terör kavramının tanımsal karşılığına yer verilmemiş olması veya ilgili mevzuata atıfta bulunulmamış olması karşısında, idareye uygulamada 'terör' kapsamını belirleme yetkisini dolaylı olarak verdiği belirtilerek, iptali istenen ibarenin Anayasa'nın 2., 7. ve 13. maddelerine aykırı olduğu ileri sürülmüştür.

İptali istenen kuralda, Müsteşarlığın ana hizmet birimlerinden olan Araştırma ' Geliştirme Daire Başkanlığının, terörle mücadele alanında Terörle Mücadele Raporu hazırlamakla görevli olduğu hükme bağlanmaktadır.

Kanun'un 4. maddesinin (1) numaralı fıkrasının incelendiği bölümde belirtilen Anayasa'nın 2. ve 7. maddelerine ilişkin gerekçelerle kuralda Anayasa'ya aykırı bir yön bulunmamaktadır. İptal isteminin reddi gerekir.

Kuralın Anayasa'nın 13. maddesiyle ilgisi görülmemiştir.

H- Kanun'un 10. Maddesinin (1) Numaralı Fıkrasının (b) Bendinin (1) Numaralı Alt Bendinin İncelenmesi

Dava dilekçesinde; iptali istenen kuralla hukuk müşavirliğine yasama yetkisini kapsar biçimde mevzuatı günün şartlarına göre geliştirme görevinin verilmesinin Anayasa'nın 2., 6. ve 7. maddelerine aykırı olduğu ileri sürülmüştür.

Kuralla, Müsteşarlığın danışma birimi olarak kurulan Hukuk Müşavirliğine, terörle mücadele mevzuatını ve uygulamasını değerlendirmek ve günün şartlarına göre geliştirmek görevi verilmiştir.

Anayasa'nın 88. maddesinde kanun teklif etmeye Bakanlar Kurulu ve milletvekillerinin yetkili olduğu belirtilmiştir. Buna karşılık, kanun teklif ve tasarılarının Anayasa'nın 88. maddesi dışında kalan kişi veya kuruluşlar tarafından hazırlanmasına Anayasal bir engel bulunmamaktadır. Kuralla, Hukuk Müşavirliğine verilen görev, Müsteşarlığın görev alanına giren konularla ilgili mevzuatı takip etme, değerlendirme ve gerektiğinde taslak metinler hazırlamaktır. 3046 sayılı Kanun'un bakanlıkların danışma birimi olarak öngörülen hukuk müşavirliklerinin görevlerini düzenleyen 25. maddesinin birinci fıkrasının (d) ve (e) bentlerinde, hukuk müşavirliklerinin gerek bakanlık gerekse bakanlık kuruluşlarınca mevzuat (kanun, tüzük, yönetmelik vs.) teklifleri hazırlamalarının kendilerine bir görev olarak verildiği açıkça ifade edilmektedir. Mevzuat Hazırlama Usul ve Esasları Hakkında Yönetmeliğin 5. maddesinde de mevzuat taslaklarının konuyla ilgili kurum ve kuruluşların görevli birimleri (hukuk müşavirlikleri) tarafından hazırlanacağı hükmüne yer verilmiştir. Bu durumda, kuralla hukuk müşavirliğine taslak hazırlama görevinin verilmesinde Anayasa'ya aykırı bir yön bulunmamaktadır.

Açıklanan nedenlerle, iptali istenen kural, Anayasa'nın 2., 6. ve 7. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

I- Kanun'un 15. Maddesinin (1) Numaralı Fıkrasının İkinci Cümlesinin İncelenmesi

Dava dilekçesinde; iptali istenen kuralla herhangi bir sınırlama getirilmeksizin her türlü bilgi ve belge talebinin ilgili bakanlık, kurum ve kuruluşlar tarafından yerine getirilmesinin öngörüldüğü, bilgi ve belge ibarelerinin her türlü kişisel verileri de kapsama alacağı, veri toplamanın sınırlarına yasal düzenleme getirilmeyerek kişilerin idareye karşı korumasız hale getirildiği belirtilerek, kuralın Anayasa'nın 13., 20. ve 25. maddelerine aykırı olduğu ileri sürülmüştür.

Kuralda, Müsteşarlığın bu kanun çerçevesinde belirlenen terörle mücadeleye ilişkin politika ve stratejileri geliştirmek ve bu konuda ilgili kurum ve kuruluşlar arasında koordinasyonu sağlamak görevini yerine getirirken, bu kapsamda istediği her türlü bilgi ve belge talebinin ilgili bakanlık, kurum ve kuruluşlarca gecikmeksizin yerine getirileceği hükme bağlanmaktadır.

Kuralda geçen 'her türlü bilgi ve belge' ibaresinin, 5952 sayılı Kanun'un 9. maddesinin (1) numaralı fıkrasının (b) bendinin (2) numaralı alt bendinde yer alan 'Veri, bilgi ve belgeleri toplamak, tasnif etmek, analiz ve değerlendirmeler yapmak' biçimindeki hükümlerle birlikte değerlendirildiğinde ve kuralda 'veri' ibaresinin de geçmediği dikkate alındığında, 'kişisel veri' niteliğinde bulunmayan her türlü bilgi ve belgeyi kapsadığı anlaşılmaktadır.

Terörle mücadele alanında strateji ve politikalar geliştirmekle görevli olan Kamu Düzeni ve Güvenliği Müsteşarlığının da kendisine verilen görevleri yerine getirebilmesi için bazı bilgi ve belgelere ihtiyaç duyması kaçınılmazdır. İptali istenen kuralda, bilgi ve belgelerin Müsteşarlığa 5952 sayılı Kanun kapsamında verilen terörle mücadeleye ilişkin politika ve stratejileri geliştirmek ve bu konuda ilgili kurum ve kuruluşlar arasında koordinasyonu sağlamak göreviyle sınırlı olacağı açıkça ifade edilmiştir. Kuralda kişisel verilerin korunmasıyla ilgili olarak Anayasa'nın 20. maddesinde öngörülen güvencelere aykırı bir hüküm de yer almamaktadır.

Açıklanan nedenlerle, iptali istenen kural, Anayasa'nın 20. maddesine aykırı değildir. İptal isteminin reddi gerekir.

Kuralın Anayasa'nın 13. ve 25. maddeleriyle ilgisi görülmemiştir.

J- Kanun'un 16. Maddesinin (1) Numaralı Fıkrasının İkinci Cümlesinin İncelenmesi

Dava dilekçesinde; 5018 sayılı Kanun'un 24. maddesi uyarınca örtülü ödeneğin esasen Başbakanlık bütçesine konulduğu ve ancak istisnaen kanunlarla verilen istihbarat hizmetlerini yürüten diğer kamu idarelerinin de bütçelerine örtülü ödenek konulabildiği, Kamu Düzeni ve Güvenliği Müsteşarlığının ise istihbarat hizmetlerini yürüten bir kamu idaresi niteliğinde olmaması nedeniyle 5018 sayılı Kanun hükümleri dairesinde bütçesine örtülü ödenek konulamayacağı, ayrıca Anayasa'nın 161. ve 162. maddelerinde bütçelerin gerek hazırlanması gerekse TBMM'de kabul

edilmesi süreçlerinin şeffaf olmasının öngörüldüğünü oysa söz konusu düzenlemede, operasyonel yetkisi olmayan bir oluşuma örtülü ödenek ayrılması öngörülmek suretiyle şeffaflıktan uzak bir şekilde harcama yetkisi verildiği belirtilerek, kuralın Anayasa'nın 2., 161. ve 162. maddelerine aykırı olduğu ileri sürülmüştür.

Kanun'un 16. maddesinde Müsteşarlığın bütçesine ilişkin düzenleme yer almaktadır. Maddenin (1) numaralı fıkrasının birinci cümlesinde, Müsteşarlığın 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanunu'na tabi genel bütçeli bir idare olduğu belirtilmiştir. Aynı fıkranın iptali istenen ikinci cümlesinde ise 5952 sayılı Kanun kapsamında yürütülen ve gizlilik ihtiva eden işler için 5018 sayılı Kanun'un 24. maddesi esaslarına göre Müsteşarlık bütçesine ödenek konulacağı kurala bağlanmıştır.

Bir yasa kuralının başka bir yasa kuralı ile uyumlu olmaması onun iptal edilmesini gerektiren bir durum değildir. Anayasa Mahkemesi yasaların başka yasalara ya da daha alt düzeydeki diğer normlara uygunluğunu değil, yasaların Anayasa'ya uygunluğunu denetlemekte olduğundan, bu gerekçeye dayanan Anayasa'ya 2. maddesine aykırılık savı yerinde değildir. Kuralın Anayasa'ya aykırı başka bir yönü de bulunamamıştır. İptal isteminin reddi gerekir.

Kuralın Anayasa'nın 161. ve 162. maddeleriyle ilgisi görülmemiştir.

K- Kanun'un 18. Maddesinin İncelenmesi

1- (1) Numaralı Fıkranın (b) Bendi ile (3) Numaralı Fıkranın (a) Bendinin İncelenmesi

Dava dilekçesinde; iptali istenen kurullarla illerde İl Sosyal Etüt ve Proje Müdürlüğü, ihtiyaç duyulan ilçelerde ise bürolar kurulmasının 3046 sayılı Kanun'da öngörülmeyen bir teşkilatlanma biçimi olduğu, bu durumun aynı zamanda idarenin kanuniliği ilkesine aykırı olduğu, söz konusu birimlerde çalışacak personelin görev, yetki ve nitelikleri konusunda da herhangi bir düzenlemeye yer verilmediği belirtilerek, kurulların Anayasa'nın 2., 123. ve 128. maddelerine aykırılığı ileri sürülmüştür.

Kanun'un 18. maddesinin (1) numaralı fıkrasının iptali istenen (b) bendiyle 657 sayılı Kanun'a ekli (II) sayılı cetvelin '4. Başbakanlık ve Bakanlıklarda' bölümüne "Nüfus ve Vatandaşlık Müdürü," ibaresinden sonra gelmek üzere 'İl Sosyal Etüt ve Proje Müdürü,' ibaresi eklenmiştir. Söz konusu (II) sayılı cetvelde ise kadroları genel idare hizmetleri sınıfının birinci derecesinde bulunanların ek göstergeleri düzenlenmektedir.

Kanun'un 18. maddesinin (3) numaralı fıkrasının (a) bendiyle, 14.2.1985 günlü, 3152 sayılı İçişleri Bakanlığı Teşkilat ve Görevleri Hakkında Kanun'un İçişleri Bakanlığının taşra teşkilatını düzenleyen 28. maddesine eklenen fıkra ile, illerde İl Sosyal Etüt ve Proje Müdürlüğü kurulduğuna ilişkin hüküm

eklenmiş, ayrıca ihtiyaç duyulan ilçelerde valiliğin teklifi ve Bakanlığın onayı ile büro kurulabileceği, valiliğin kadro, yer ve unvanlarına bakılmaksızın ihtiyaç durumuna göre uzman, sözleşmeli personel ve memurları bu birimlerde görevlendirmeye yetkili olduğu kurala bağlanmıştır.

Anayasa'nın 128. maddesinde, Devletin, kamu iktisadi teşebbüsleri ve diğer kamu tüzelkişilerinin genel idare esaslarına göre yürütmekle yükümlü oldukları kamu hizmetlerinin gerektirdiği asli ve sürekli görevlerinin memurlar ve diğer kamu görevlileri eliyle yürütüleceği, bu kapsama giren personelin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülüklerinin de Kanunla düzenleneceği belirtilmiştir.

İptali istenen kuralla, illerde yeni ihdas edilen İl Sosyal Etüt ve Proje Müdürlüğünün acil eleman ihtiyacının karşılanması için Valilere özel olarak yetki verilmektedir. İptali istenen kural, Valinin genel görevlendirme yetkisinin özel olarak düzenlenmesinden başka bir anlam ifade etmemektedir. Kuralda geçen 'görevlendirme' nin mevcut olan uzman, sözleşmeli personel ve memurlar arasından yapılacağı açıktır. Bir başka ifadeyle söz konusu personel, 657 sayılı Kanun'un 4. maddesi kapsamında kalan ve halen kamuda çalışmakta olan personeldir. Bu durumda, atanmaları, görev ve yetkileri ile hak ve yükümlülükleri 657 sayılı Kanun'a tabi olan personelin Valiler tarafından İl Sosyal Etüt ve Proje Müdürlüğünde görevlendirilmesinde Anayasa'nın 128. maddesine aykırı bir yön bulunmamaktadır.

Kuralın 3046 sayılı Kanun'da öngörülmeleyen bir yapılanma öngördüğü ve idarenin kanuniliği ilkesine aykırı olduğu yönünde ileri sürülen Anayasa'ya aykırılık itirazları, Kanun'un 4. maddesinin (1) numaralı fıkrasının incelendiği bölümde belirtilen gerekçelerle, yerinde görülmemiştir.

Açıklanan nedenlerle, iptali istenen kurallar, Anayasa'nın 2., 123. ve 128. maddelerine aykırı değildir. İptal isteminin reddi gerekir.

2- (4) Numaralı Fıkranın İncelenmesi

Dava dilekçesinde; 3046 sayılı Kanun'un 16. maddesinin (d) bendinde yer alan 'Bir bakanlıkta birden fazla müsteşarlık kurulamaz' biçimindeki kural uyarınca İçişleri Bakanlığına bağlı ikinci bir Müsteşarlık kurulamayacağı belirtilerek, kuralın Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüştür.

İptali istenen kuralla 5018 sayılı Kanun'a ekli (I) sayılı cetvele 33. sırasından sonra gelmek üzere '34) Kamu Düzeni ve Güvenliği Müsteşarlığı' ibaresi eklenmiş ve diğer sıralar buna göre teselsül ettirilmiştir. 5018 sayılı Kanun'a ekli (I) sayılı cetvelde, genel bütçe kapsamındaki kamu idarelerinin isimleri bulunmaktadır.

3.6.2011 günlü, 643 sayılı Kanun Hükmünde Kararname'nin 2. maddesi ile 3046 sayılı Kanun'a eklenen 19/A maddesinin verdiği yetkiyle Başbakanlığın 7.7.2011 günlü, B.02.0.PPG.0.12-300-02/7062 sayılı teklifi ile Cumhurbaşkanlığının aynı gün ve B.01.0.KKB.01-08/D-1-507 sayılı onayıyla Kamu Düzeni ve Güvenliği Müsteşarlığı İçişleri Bakanlığına bağlı olmaktan çıkarılıp, Başbakanlıkla ilgilendirildiğinden, kurala ilişkin olarak ileri sürülen Anayasa'ya aykırılık gerekçesi ortadan kalkmıştır. Kaldı ki, bir yasa kuralının başka bir yasa kuralı ile uyumlu olmaması onun iptal edilmesini gerektiren bir durum değildir. Anayasa Mahkemesi yasaların başka yasalara ya da daha alt düzeydeki diğer normlara uygunluğunu değil, yasaların Anayasa'ya uygunluğunu denetlemekte olduğundan, bu gerekçeye dayanan Anayasa'ya 2. maddesine aykırılık savı yerinde değildir. Kuralın Anayasa'ya aykırı başka bir yönü de bulunamamıştır. İptal isteminin reddi gerekir.

Açıklanan nedenlerle, iptali istenen kural, Anayasa'nın 2. maddesine aykırı değildir. İptal isteminin reddi gerekir.

V- YÜRÜRLÜĞÜN DURDURULMASI İSTEMİ

17.2.2010 günlü, 5952 sayılı Kamu Düzeni ve Güvenliği Müsteşarlığının Teşkilat ve Görevleri Hakkında Kanun'un:

A- 1- 2. maddesinin (1) numaralı fıkrasının (d) bendine,

2- 4. maddesinin (1) numaralı fıkrasına,

3- 5. maddesinin (3) numaralı fıkrasına,

4- 6. maddesinin (1) numaralı fıkrasının;

a- Başında yer alan "Terörle" sözcüğüne,

b- (b) bendine,

c- (c) bendinde yer alan "veya yaptırmak" ibaresine,

d- (ç) bendinde yer alan "Güvenlik kuruluşlarına" ve "ilgili kurumlara" ibarelerine,

e- (f) bendine,

5- 8. maddesine,

6- 9. maddesinin (1) numaralı fıkrasının;

a- (a) bendinin (1) numaralı alt bendinde yer alan "uygulanmasına yönelik eylem planları hazırlamak" ibaresine,

b- (a) bendinin (2) numaralı alt bendinde yer alan "Güvenlik kuruluşları" ibaresine,

- c- (a) bendinin (3) numaralı alt bendinde yer alan "Valilikler " sözcüğüne,
- d- (a) bendinin (4) numaralı alt bendine,
- e- (b) bendinin (1) numaralı alt bendinde yer alan "Veri, bilgi ve belgeleri toplamak, tasnif etmek, " ibaresine,
- f- (b) bendinin (2) numaralı alt bendinde yer alan "yaptırmak " sözcüğüne,
- g- (b) bendinin (4) numaralı alt bendindeki "Terörle " sözcüğüne,
- 7- 10. maddesinin (1) numaralı fıkrasının (b) bendinin (1) numaralı alt bendine,
- 8- 15. maddesinin (1) numaralı fıkrasının ikinci cümlesine,
- 9- 16. maddesinin (1) numaralı fıkrasının ikinci cümlesine,
- 10- 18. maddesinin;
- a- (1) numaralı fıkrasının (b) bendiyle 657 Sayılı Kanun'a ekli (II) sayılı cetvelin '4. Başbakanlık ve Bakanlıklarda' bölümüne 'Nüfus ve Vatandaşlık Müdürü,' ibaresinden sonra gelmek üzere eklenen 'İl Sosyal Etüt ve Proje Müdürü,' ibaresine,
- b- (3) numaralı fıkrasının (a) bendiyle 14.2.1985 günlü, 3152 sayılı İçişleri Bakanlığı Teşkilat ve Görevleri Hakkında Kanun'un 28. maddesine eklenen fıkraya,
- c- (4) numaralı fıkrasına,
- yönelik iptal istemleri 19.1.2012 günlü, E. 2010/40, K. 2012/8 sayılı kararla reddedildiğinden, bu madde, fıkra, bent, alt bent, cümle, ibare ve sözcüklere ilişkin yürürlüğün durdurulması isteminin REDDİNE,
- B- 1- 1. maddesinin (1) numaralı fıkrasının " terörle mücadeleye ilişkin politika ve stratejileri geliştirmek ve bu konuda ilgili kurum ve kuruluşlar arasında koordinasyonu sağlamak üzere İçişleri Bakanlığına bağlı " bölümü,
- 2- 2. maddesinin (1) numaralı fıkrasının (a) bendi,
- 3- 3. maddesi,
- 4- 4. maddesinin (2) numaralı fıkrası,
- 5- 5. maddesinin (2) numaralı fıkrasında yer alan " Bakanın onayı ile özel ihtisas ve araştırma komisyonları " ibaresi,
- 6- 7. maddesinin (1) numaralı fıkrasında yer alan " Bakana " sözcüğü,

7- 10. maddesinin (1) numaralı fıkrasının (c) bendinin " Bakan onayı ile en çok on Müsteşarlık Müşaviri pozisyon unvanıyla sözleşmeli personel çalıştırılabilir. Personelin sözleşme usul ve esasları Müsteşarlıkça tespit edilir ve bu Kanuna ekli (2) sayılı cetvelde belirlenen taban ve tavan ücretleri arasında kalmak üzere Müsteşarın teklifi ve Bakan onayı ile aylık brüt sözleşme ücreti ödenir. Ayrıca Müsteşarlıkta sözleşmeli personel olarak istihdam edilenler için belirlenen usul ve esaslar çerçevesinde ikramiye ve teşvik ikramiyesi ödenebilir. Bu statüde çalıştırılma, sözleşme bitiminde kamu kurum ve kuruluşlarında herhangi bir pozisyon, kadro veya statüde çalışma açısından kazanılmış hak teşkil etmez.' bölümü,

8- 13. maddesinin;

a- (2) numaralı fıkrası,

b- (4) numaralı fıkrasının son cümlesi,

9- 18. maddesinin;

a- (1) numaralı fıkrasının (a) bendiyle 14.7.1965 günlü, 657 sayılı Devlet Memurları Kanunu'na ekli (I) sayılı cetvelin 'VIII. Mülki İdare Amirliği Hizmetleri Sınıfı' bölümünün (a) bendine 'Müsteşar,' ibaresinden sonra gelmek üzere eklenen 'Kamu Düzeni ve Güvenliği Müsteşarı,' ibaresi,

b- (3) numaralı fıkrasının (b) bendiyle 3152 sayılı Kanun'un 29. maddesinin birinci fıkrasına eklenen (d) bendi,

c- (5) numaralı fıkrasıyla 27.6.1989 günlü, 375 sayılı Kanun Hükmünde Kararname'nin Ek 3. maddesinin birinci fıkrasına 'Savunma Sanayi Müsteşarlığı,' ibaresinden sonra gelmek üzere eklenen 'Kamu Düzeni ve Güvenliği Müsteşarlığı,' ibaresi,

hakkında, 19.1.2012 günlü, E. 2010/40, K. 2012/8 sayılı kararlar ile karar verilmesine yer olmadığına karar verildiğinden, bu madde, fıkra, bent, bölüm, cümle, ibare ve sözcüklere ilişkin yürürlüğün durdurulması istemi hakkında KARAR VERİLMESİNE YER OLMADIĞINA,

19.1.2012 gününde OYBİRLİĞİYLE karar verilmiştir.

VI- SONUÇ

17.2.2010 günlü, 5952 sayılı Kamu Düzeni ve Güvenliği Müsteşarlığının Teşkilat ve Görevleri Hakkında Kanun'un:

1- 1. maddesinin (1) numaralı fıkrasının " terörle mücadeleye ilişkin politika ve stratejileri geliştirmek ve bu konuda ilgili kurum ve kuruluşlar arasında koordinasyonu sağlamak üzere İçişleri Bakanlığına bağlı " bölümünde yer alan '...İçişleri Bakanlığına bağlı " ibaresi, 3.6.2011 günlü, 643 sayılı Kanun

Hükmünde Kararname'nin 2. maddesi ile 3046 sayılı Kanun'a eklenen 19/A maddesinin verdiği yetkiyle Başbakanlığın 7.7.2011 günlü, B.02.0.PPG.0.12-300-02/7062 sayılı teklifi ile Cumhurbaşkanlığının aynı gün ve B.01.0.KKB.01-08/D-1-507 sayılı onayıyla yürürlükten kaldırıldığından, konusu kalmayan bu bölüme ilişkin iptal istemi hakkında KARAR VERİLMESİNE YER OLMADIĞINA, Fulya KANTARCIOĞLU, Osman Alifeyyaz PAKSÜT, Zehra Ayla PERKTAŞ ile Nuri NECİPOĞLU'nun 'Sadece 'İçişleri Bakanlığına bağlı' ibaresi için karar verilmesine yer olmadığına karar verilmesi gerektiği' yolundaki karşıoyları ve OYÇOKLUĞUYLA,

2- 2. maddesinin (1) numaralı fıkrasının;

a- (a) bendi, 3.6.2011 günlü, 643 sayılı Kanun Hükmünde Kararname'nin 2. maddesi ile 3046 sayılı Kanun'a eklenen 19/A maddesinin verdiği yetkiyle Başbakanlığın 7.7.2011 günlü, B.02.0.PPG.0.12-300-02/7062 sayılı teklifi ile Cumhurbaşkanlığının aynı gün ve B.01.0.KKB.01-08/D-1-507 sayılı onayıyla yürürlükten kaldırıldığından, bu bende ilişkin konusu kalmayan iptal istemi hakkında KARAR VERİLMESİNE YER OLMADIĞINA, OYBİRLİĞİYLE,

b- (d) bendinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

3- 3. maddesinin (1) numaralı fıkrasında yer alan "İçişleri Bakanlığına bağlı" ibaresi, 3.6.2011 günlü, 643 sayılı Kanun Hükmünde Kararname'nin 2. maddesi ile 3046 sayılı Kanun'a eklenen 19/A maddesinin verdiği yetkiyle Başbakanlığın 7.7.2011 günlü, B.02.0.PPG.0.12-300-02/7062 sayılı teklifi ile Cumhurbaşkanlığının aynı gün ve B.01.0.KKB.01-08/D-1-507 sayılı onayıyla yürürlükten kaldırıldığından, bu maddeye ilişkin konusu kalmayan iptal istemi hakkında KARAR VERİLMESİNE YER OLMADIĞINA, Fulya KANTARCIOĞLU, Osman Alifeyyaz PAKSÜT, Zehra Ayla PERKTAŞ ile Nuri NECİPOĞLU'nun 'Sadece 'İçişleri Bakanlığına bağlı' ibaresi için karar verilmesine yer olmadığına karar verilmesi gerektiği' yolundaki karşıoyları ve OYÇOKLUĞUYLA,

4- 4. maddesinin;

a- (1) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

b- (2) numaralı fıkrasının, birinci cümlesinde yer alan '...İçişleri Bakanının ', ikinci cümlesinde yer alan '...İçişleri Bakanının ' ve üçüncü cümlesinde yer alan '...İçişleri Bakanı ' ibareleri, 3.6.2011 günlü, 643 sayılı Kanun Hükmünde Kararname'nin 2. maddesi ile 3046 sayılı Kanun'a eklenen 19/A maddesinin verdiği yetkiyle Başbakanlığın 7.7.2011 günlü, B.02.0.PPG.0.12-300-02/7062 sayılı teklifi ile Cumhurbaşkanlığının aynı gün ve B.01.0.KKB.01-08/D-1-507 sayılı onayıyla yürürlükten kaldırıldığından, bu fıkraya ilişkin konusu kalmayan iptal istemi hakkında KARAR VERİLMESİNE

YER OLMADIĞINA, Fulya KANTARCIOĞLU, Osman Alifeyyaz PAKSÛT, Zehra Ayla PERKTAŞ ile Nuri NECİPOĞLU'nun 'Sadece 'İçişleri Bakanının' ve 'İçişleri Bakanı' ibareleri yönünden karar verilmesine yer olmadığına karar verilmesi gerektiği' yolundaki karşıoyları ve OYÇOKLUĞUYLA, 5- 5. maddesinin;

a- (2) numaralı fıkrasında yer alan " Bakanın onayı ile özel ihtisas ve araştırma komisyonları " ibaresindeki '... Bakanın...' sözcüğü, 3.6.2011 günlü, 643 sayılı Kanun Hükmünde Kararname'nin 2. maddesi ile 3046 sayılı Kanun'a eklenen 19/A maddesinin verdiği yetkiyle Başbakanlığın 7.7.2011 günlü, B.02.0.PPG.0.12-300-02/7062 sayılı teklifi ile Cumhurbaşkanlığının aynı gün ve B.01.0.KKB.01-08/D-1-507 sayılı onayıyla yürürlükten kaldırıldığından, bu ibareye ilişkin konusu kalmayan iptal istemi hakkında KARAR VERİLMESİNE YER OLMADIĞINA, Fulya KANTARCIOĞLU, Osman Alifeyyaz PAKSÛT, Zehra Ayla PERKTAŞ ile Nuri NECİPOĞLU'nun 'Sadece 'Bakanın' sözcüğü için karar verilmesine yer olmadığına karar verilmesi gerektiği' yolundaki karşıoyları ve OYÇOKLUĞUYLA,

b- (3) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

6- 6. maddesinin (1) numaralı fıkrasının;

a- Başında yer alan 'Terörle' sözcüğünün Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

b- (b) bendinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

c- (c) bendinde yer alan 'veya yaptırmak' ibaresinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

d- (ç) bendinde yer alan 'Güvenlik kuruluşlarına' ve 'ilgili kurumlara' ibarelerinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

e- (f) bendinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

7- 7. maddesinin (1) numaralı fıkrasında yer alan " Bakana " sözcüğü, 3.6.2011 günlü, 643 sayılı Kanun Hükmünde Kararname'nin 2. maddesi ile 3046 sayılı Kanun'a eklenen 19/A maddesinin verdiği yetkiyle Başbakanlığın 7.7.2011 günlü, B.02.0.PPG.0.12-300-02/7062 sayılı teklifi ile Cumhurbaşkanlığının aynı gün ve B.01.0.KKB.01-08/D-1-507 sayılı onayıyla yürürlükten kaldırıldığından, bu sözcüğe ilişkin konusu kalmayan iptal istemi hakkında KARAR VERİLMESİNE YER OLMADIĞINA, OYBİRLİĞİYLE,

8- 8. maddesinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

9- 9. maddesinin (1) numaralı fıkrasının;

a- (a) bendinin (1) numaralı alt bendinde yer alan "uygulanmasına yönelik eylem planları hazırlamak" ibaresinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

b- (a) bendinin (2) numaralı alt bendinde yer alan 'Güvenlik kuruluşları' ibaresinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

c- (a) bendinin (3) numaralı alt bendinde yer alan 'Valilikler' sözcüğünün Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

d- (a) bendinin (4) numaralı alt bendinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

e- (b) bendinin (1) numaralı alt bendinde yer alan 'Veri, bilgi ve belgeleri toplamak, tasnif etmek,' ibaresinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, Fulya KANTARCIOĞLU, Mehmet ERTEN, Osman Alifeyyaz PAKSÜT, Zehra Ayla PERKTAŞ ile Engin YILDIRIM'ın karşıoyları ve OYÇOKLUĞUYLA,

f- (b) bendinin (2) numaralı alt bendinde yer alan "yaptırmak" sözcüğünün Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

g- (b) bendinin (4) numaralı alt bendindeki 'Terörle' sözcüğünün Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

10- 10. maddesinin (1) numaralı fıkrasının;

a- (b) bendinin (1) numaralı alt bendinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

b- (c) bendinin "Bakan onayı ile en çok on Müsteşarlık Müşaviri pozisyon unvanıyla sözleşmeli personel çalıştırılabilir. Personelin sözleşme usul ve esasları Müsteşarlıkça tespit edilir ve bu Kanuna ekli (2) sayılı cetvelde belirlenen taban ve tavan ücretleri arasında kalmak üzere Müsteşarın teklifi ve Bakan onayı ile aylık brüt sözleşme ücreti ödenir. Ayrıca Müsteşarlıkta sözleşmeli personel olarak istihdam edilenler için belirlenen usul ve esaslar çerçevesinde ikramiye ve teşvik ikramiyesi ödenebilir. Bu statüde çalıştırılma, sözleşme bitiminde kamu kurum ve kuruluşlarında herhangi bir pozisyon, kadro veya statüde çalışma açısından kazanılmış hak teşkil etmez.' bölümünde yer alan 'Bakan' sözcüğü, 3.6.2011 günlü, 643 sayılı Kanun Hükmünde Kararname'nin 2. maddesi ile 3046

sayılı Kanun'a eklenen 19/A maddesinin verdiği yetkiyle Başbakanlığın 7.7.2011 günlü, B.02.0.PPG.0.12-300-02/7062 sayılı teklifi ile Cumhurbaşkanlığının aynı gün ve B.01.0.KKB.01-08/D-1-507 sayılı onayıyla; yine aynı bölümde yer alan "ve bu Kanuna ekli (2) sayılı cetvelde belirlenen taban ve tavan ücretleri arasında kalmak üzere Müsteşarın teklifi ve Bakan onayı ile aylık brüt sözleşme ücreti ödenir. Ayrıca Müsteşarlıkta sözleşmeli personel olarak istihdam edilenler için belirlenen usul ve esaslar çerçevesinde ikramiye ve teşvik ikramiyesi ödenebilir. " ibaresi de 11.10.2011 günlü, 666 sayılı Kanun Hükmünde Kararname'nin 1. maddesiyle 375 sayılı Kanun Hükmünde Kararname'ye eklenen ek 12. maddenin (3) numaralı fıkrasının (n) bendi ile yürürlükten kaldırıldığından, bu bölüme ilişkin konusu kalmayan iptal istemi hakkında KARAR VERİLMESİNE YER OLMADIĞINA, Fulya KANTARCIOĞLU, Osman Alifeyyaz PAKSÜT, Zehra Ayla PERKTAŞ ile Nuri NECİPOĞLU'nun 'Sadece bölümde yer alan 'Bakan' sözcüğü ile "ve bu Kanuna ekli (2) sayılı cetvelde belirlenen taban ve tavan ücretleri arasında kalmak üzere Müsteşarın teklifi ve Bakan onayı ile aylık brüt sözleşme ücreti ödenir. Ayrıca Müsteşarlıkta sözleşmeli personel olarak istihdam edilenler için belirlenen usul ve esaslar çerçevesinde ikramiye ve teşvik ikramiyesi ödenebilir. " ibaresi yönünden karar verilmesine yer olmadığına karar verilmesi gerektiği' yolundaki karşıoyları ve OYÇOKLUĞUYLA, 11- 13. maddesinin;

a- (2) numaralı fıkrasında yer alan 'Bakan" sözcüğü, 3.6.2011 günlü, 643 sayılı Kanun Hükmünde Kararname'nin 2. maddesi ile 3046 sayılı Kanun'a eklenen 19/A maddesinin verdiği yetkiyle Başbakanlığın 7.7.2011 günlü, B.02.0.PPG.0.12-300-02/7062 sayılı teklifi ile Cumhurbaşkanlığının aynı gün ve B.01.0.KKB.01-08/D-1-507 sayılı onayıyla yürürlükten kaldırıldığından, bu fıkraya ilişkin konusu kalmayan iptal istemi hakkında KARAR VERİLMESİNE YER OLMADIĞINA, Fulya KANTARCIOĞLU, Osman Alifeyyaz PAKSÜT, Zehra Ayla PERKTAŞ ile Nuri NECİPOĞLU'nun 'Sadece 'Bakan' sözcüğü için karar verilmesine yer olmadığına karar verilmesi gerektiği' yolundaki karşıoyları ve OYÇOKLUĞUYLA,

b- (4) numaralı fıkrasının son cümlesi, 11.10.2011 günlü, 666 sayılı Kanun Hükmünde Kararname'nin 1. maddesiyle 375 sayılı Kanun Hükmünde Kararname'ye eklenen ek 12. maddenin (3) numaralı fıkrasının (n) bendi ile yürürlükten kaldırıldığından, bu cümleye ilişkin konusu kalmayan iptal istemi hakkında KARAR VERİLMESİNE YER OLMADIĞINA, OYBİRLİĞİYLE,

12- 15. maddesinin (1) numaralı fıkrasının ikinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

13- 16. maddesinin (1) numaralı fıkrasının ikinci cümlesinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

14- 18. maddesinin;

a- (1) numaralı fıkrasının (a) bendiyle 14.7.1965 günlü, 657 sayılı Devlet Memurları Kanunu'na ekli (I) sayılı cetvelin 'VIII. Mülki İdare Amirliği Hizmetleri Sınıfı' bölümünün (a) bendine 'Müsteşar,' ibaresinden sonra gelmek üzere eklenen 'Kamu Düzeni ve Güvenliği Müsteşarı,' ibaresi, 10.10.2011 günlü, 657 sayılı Kanun Hükmünde Kararname'nin 37. maddesiyle yürürlükten kaldırıldığından, bu ibareye ilişkin konusu kalmayan iptal istemi hakkında KARAR VERİLMESİNE YER OLMADIĞINA, OYBİRLİĞİYLE,

b- (1) numaralı fıkrasının (b) bendiyle 657 Sayılı Kanun'a ekli (II) sayılı cetvelin '4. Başbakanlık ve Bakanlıklarda' bölümüne 'Nüfus ve Vatandaşlık Müdürü,' ibaresinden sonra gelmek üzere eklenen 'İl Sosyal Etüt ve Proje Müdürü,' ibaresinin Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

c- (3) numaralı fıkrasının (a) bendiyle 3152 sayılı İçişleri Bakanlığı Teşkilat ve Görevleri Hakkında Kanun'un 28. maddesine eklenen fıkranın Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

d- (3) numaralı fıkrasının (b) bendiyle 3152 sayılı Kanun'un 29. maddesinin birinci fıkrasına eklenen (d) bendi, 3.6.2011 günlü, 643 sayılı Kanun Hükmünde Kararname'nin 2. maddesi ile 3046 sayılı Kanun'a eklenen 19/A maddesinin verdiği yetkiyle Başbakanlığın 7.7.2011 günlü, B.02.0.PPG.0.12-300-02/7062 sayılı teklifi ile Cumhurbaşkanlığının aynı gün ve B.01.0.KKB.01-08/D-1-507 sayılı onayıyla yürürlükten kaldırıldığından, bu bende ilişkin konusu kalmayan iptal istemi hakkında KARAR VERİLMESİNE YER OLMADIĞINA, OYBİRLİĞİYLE,

e- (4) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve iptal isteminin REDDİNE, OYBİRLİĞİYLE,

f- (5) numaralı fıkrasıyla 375 sayılı Kanun Hükmünde Kararname'nin Ek 3. maddesinin birinci fıkrasına 'Savunma Sanayi Müsteşarlığı,' ibaresinden sonra gelmek üzere eklenen 'Kamu Düzeni ve Güvenliği Müsteşarlığı,' ibaresi, 11.10.2011 günlü, 666 sayılı Kanun Hükmünde Kararname'nin 1. maddesiyle 375 sayılı Kanun Hükmünde Kararname'ye eklenen ek 12. maddenin (1) numaralı fıkrasının (m) bendi ile yürürlükten kaldırıldığından, bu ibareye ilişkin konusu kalmayan iptal istemi hakkında KARAR VERİLMESİNE YER OLMADIĞINA, OYBİRLİĞİYLE,

19.1.2012 gününde karar verildi.

Başkan - Haşim KILIÇ

Başkanvekili - Serruh KALELİ

Başkanvekili - Alparslan ALTAN

Üye: Fulya KANTARCIOĞLU; Mehmet ERTEN; Osman Alifeyyaz PAKSÜT; Zehra Ayla PERKTAŞ; Recep KÖMÜRCÜ; Burhan ÜSTÜN; Engin YILDIRIM; Nuri NECİPOĞLU; Hicabi DURSUN; Celal Mümtaz AKINCI; Erdal TERCAN

KARŞIOY GEREKÇESİ

I- 3.6.2011 günlü, 643 sayılı ve 11.10.2011 günlü, 666 sayılı Kararnamelerin Etkilediği Kurallar Yönünden

17.2.2010 günlü, 5952 sayılı Kanun'un bazı maddelerinin iptali istemiyle 3.6.2010 tarihinde açılan davadan sonra, anılan Yasa'da 643 ve 666 sayılı KHK'lerin yürürlüğe girmesi sonucu yapılan değişikliklerin, ilgili oldukları dava konusu kuralların tümünü etkilediği gerekçesiyle bu maddeler hakkındaki incelemenin esasına girilmesine gerek görülmeverek 'karar verilmesine yer olmadığı' yolunda karar verilmiştir.

Anayasa Mahkemesi'ne yapılan iptal başvurularının konusunu oluşturan kuralların tümüyle yasal değişikliğe uğramaları halinde, iptal davalarının doğrudan soyut norm denetimine ilişkin oldukları da gözetildiğinde, söz konusu başvurular hakkında esastan karar verilmesinde, hukuki yarar bulunmamakta ise de yapılan değişikliğin, dava konusu kuralın bir bölümüne yönelik olması durumunda, kalan bölüm hakkında incelemenin sürdürülmesi gerekir. Aksi halde dava konusu kurallarda, daha sonraki yasal düzenlemelerle yapılacak en küçük değişiklikler o kuralların, iptal davası yoluyla Anayasal denetiminin engellenmesi sonucunu doğurur. Böyle bir sonucu, Anayasa yargısının amacı ve işleviyle bağdaştırmak olanaksızdır.

Açıklanan nedenlerle 5952 sayılı Yasa'nın, tümü değiştirilmeyerek sadece bazı bölüm, ibare ve sözcüklerinde değişiklik yapılan kurallarının, kalan bölümlerinin Anayasa'ya uygunluk denetiminin yapılarak esas hakkında karar verilmesi gerektiği düşüncesiyle çoğunluk görüşüne katılmıyorum.

II- Yasa'nın 9. Maddesinin (1) Numaralı Fıkrasının (b) Bendinin (1) Numaralı Alt Bendinin 'Veri, bilgi ve belgeleri toplamak, tasnif etmek' Bölümünün İncelenmesi

5952 sayılı Yasa'nın 9. maddesi ile Kamu Düzeni ve Güvenliği Müsteşarlığı'nın Araştırma-Geliştirme Daire Başkanlığı'na dava konusu kuralla terörle mücadele alanında 'veri, bilgi ve belgeleri toplamak, tasnif etmek görevi verilmiştir. Hiçbir ayırım ve sınırlama getirilmediğinden Kural'ın, kişilerin temel

hak ve özgürlük alanlarını da kapsayacak biçimde her türlü veri, bilgi ve belge toplamayı içerdiği açıktır.

Anayasa'nın 20. maddesinin ilk fıkrasında herkesin; özel hayatına saygı gösterilmesini isteme hakkına sahip olduğu özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş, son fıkrasında da Herkes, kendisiyle ilgili kişisel verilen korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir' denilerek kişisel verilerin korunması, özel hayatın gizliliğinin korunması kapsamında güvenceye kavuşturulmuştur.

Kişisel verilerin korunmasını isteme hakkına sağlanan Anayasal güvencenin yaşama geçirilebilmesi için, bu hakkı ilgilendiren yasal düzenlemelerin, açık, anlaşılabilir ve kişilerin söz konusu haklarını kullanabilmelerine elverişli olması gerekir. Ancak böyle bir düzenleme ile kişilerin özel hayatlarını ilgilendiren veri, bilgi ve belgelerin resmi makamların keyfi müdahalelerine karşı korunması olanaklı hale getirilebilir.

Dava konusu kural ile Kamu Düzeni ve Güvenliği Müsteşarlığının Araştırma-Geliştirme Daire Başkanlığı'na kapsamı ve koşulları belirlenmeksizin her türlü veri, bilgi ve belgeleri toplama görevi verilerek kişilerin özel hayatlarının gizliliğinin korunması kapsamında bulunan, kişisel verilerin korunmasını isteme hakları ihlâl edilmiştir.

Açıklanan nedenlerle Kural'ın Anayasa'nın 20. maddesine aykırı olduğu ve iptali gerektiği düşüncesiyle çoğunluk görüşüne katılmıyorum.

Üye - Fulya KANTARCIOĞLU

KARŞIOY GEREKÇESİ

Kamu Düzeni ve Güvenliği Müsteşarlığının Teşkilat ve Görevleri Hakkında Kanun'un 9. maddesinin (1) numaralı fıkrasının (b) bendinde, müsteşarlığın hizmet birimlerinden olan Araştırma Geliştirme Daire Başkanlığı'nın terörle mücadele alanındaki görevleri sayılırken, söz konusu (b) bendinin iptali istenilen (1) numaralı alt bendinde, veri, bilgi ve belgeleri toplamanın da bu görevler arasında olduğu ifade edilmiştir.

İptali istenen kuralda, açıklayıcı bir düzenleme bulunmadığı için, veri, bilgi ve belgeleri toplama olarak adlandırılan görevlendirme uyarınca, Araştırma Geliştirme Daire Başkanlığı'nın kişisel veri, bilgi ve belgeler dahil her türlü veri, bilgi ve belgeyi toplama yetkisinin bulunduğu duraksama bulunmamaktadır.

Anayasa'nın 20. maddesinde, herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkını kapsadığı ifade edilmiş, ayrıca, kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hükmüne de yer verilmiştir.

Araştırma Geliştirme Daire Başkanlığı, iptali istenilen kural uyarınca, temel hak ve özgürlüklere müdahale niteliğinde de olsa her türlü kişisel veri, bilgi ve belgeyi toplayabilecektir.

Anayasa'da yer alan güvenceye rağmen, iptale konu kuralla, veri, bilgi ve belgelerin toplanmasına her hangi bir sınırlama getirilmeyerek, temel hak ve özgürlüklere müdahale niteliğinde olanlar dâhil, her türlü kişisel veri, bilgi ve belgelerin toplanmasına imkân tanınmakta, böylece kişiler idareye karşı korunmasız hale getirilmektedir. Bu durum, Anayasa'nın 20.maddesinde öngörülen kişisel veri, bilgi ve belgelerin korunması hakkına aykırılık oluşturmaktadır.

Açıklanan nedenle kuralın iptali gerektiğinden, çoğunluk görüşüne katılmadım.

Üye - Mehmet ERTEN

KARŞIOY YAZISI

5952 sayılı Kanun'un 9. maddesinin (1) numaralı fıkrasının (b) bendinin (1) numaralı alt bendinde Müsteşarlığın, terörle mücadele alanında görevleri arasında 'veri, bilgi ve belgeleri toplamak, tasnif etmek' de yer almıştır.

Kişisel bilgi ve verilerin korunması, Anayasa'nın 'Özel hayatın gizliliği' kenar başlıklı 20. maddesinde düzenlenmiştir. Maddenin birinci fıkrasında herkesin, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiştir. Maddenin üçüncü fıkrasında herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu; bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve

amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı; kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği; kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir.

Anayasa'nın 13. maddesinde temel hak ve hürriyetlerin özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği; bu sınırlamaların Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamayacağı ifade edilmiştir.

İptali istenen kural, kişisel verilerin, bilgi ve belgelerin toplanmasına ve tasnif edilmesine olanak vermekte, veri, bilgi ve belgelerin kişisel veri ve bilgileri kapsamadığı yönünde bir güvence de içermemektedir.

Anayasa'nın 20. maddesinde özel hayatın gizliliğine milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması sebeplerine bağlı olarak hakim kararıyla sınırlanabileceği öngörülmüş ise de iptali istenen kural bu kapsama girmemektedir. Kişinin bu kural uyarınca fişlendiğinden haberdar olması, bunların silinmesini talep etmesi ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmesi de mümkün değildir. Bu nedenle kural, Anayasa'nın 20. maddesiyle güvence altına alınmak istenen temel hakka karşı yapılmış pervasız bir müdahaledir.

Anayasa'nın 20. maddesine aykırı olan kural, Anayasa'nın 2. maddesinde belirtilen hukuk devletine de ters düşmektedir. Bu nedenlerle iptali gerekir.

Üye - Osman Alifeyyaz PAKSÜT

KARŞIOY GEREKÇESİ

Dava 17.2.2010 günlü, 5952 sayılı Kamu Düzeni ve Güvenliği Müsteşarlığının Teşkilat Görevleri Hakkında Kanun'un bazı maddelerinde yer alan fıkra, bent, tümce, ibare ve sözcüklerin Anayasa'ya aykırılığı ileri sürülerek iptali istemiyle açılmıştır.

1- 1. maddenin (1) numaralı fıkrasının "İçişleri Bakanlığına" ibaresi; 3. maddenin (1) numaralı fıkrasında yer alan "İçişleri Bakanlığına bağlı" ibaresi; 4. maddenin (2) numaralı fıkrasının birinci, ikinci ve üçüncü cümlesinde yer alan "İçişleri Bakanının" ibareleri; 5. maddenin (2) numaralı fıkrasında; 10. maddenin (1) numaralı fıkrasının (c) bendinde ve 13. maddenin (2) numaralı fıkrasında yer alan "Bakanın" sözcüğü 3.6.2011 günlü 643 sayılı Kanun Hükmünde Kararname ile

kaldırıldığından bahisle sözü geçen kuralların iptali istemi hakkında karar verilmesine yer olmadığına karar verilmiştir.

Anayasa Mahkemesine yapılan iptal başvurularının konusunu oluşturan kuralların tümüyle yasal değişikliğe uğramaları halinde, söz konusu başvurular hakkında karar verilmesinde hukuki yarar bulunmamakta ise de, yapılan değişikliğin dava konusu tümce, ibare veya sözcüklere ilişkin olması durumunda incelemenin sürdürülerek istemle ilgili karar verilmesi gerekir. Aksi halde dava konusu kurallarda yapılacak en küçük ekleme ve çıkarma şeklindeki değişiklikler sonucunda bu kuralların anayasal denetimin dışında kalmasına sebep olacağından bu durum Anayasa yargısının amacıyla ve işleviyle bağdaşmaz.

Bu nedenle, 17.2.2010 günlü, 5952 sayılı Yasa'nın 1. maddesinin (1) numaralı fıkrasının, 3. maddesinin (1) numaralı fıkrasının, 4. maddesinin (2) numaralı fıkrasının, 5. maddesinin (2) numaralı fıkrasının, 10. maddesinin (1) numaralı fıkrasının (c) bendinin, 13. maddesinin (2) numaralı fıkrasının değiştirilmeyen ibare dışında kalan bölümüne ilişkin incelemenin sürdürülmesi gerektiğinden sözü geçen maddelerin iptal istemi hakkında karar verilmesine yer olmadığı yolundaki çoğunluk görüşüne katılmıyorum.

2- 9. maddenin (1) numaralı fıkrasının (b) bendinin (1) numaralı alt bendinde yer alan 'veri,bilgi ve belgeleri toplamak, tasnif etmek' ibaresinin incelenmesi;

Maddede; Kamu Düzeni ve Güvenliği Müsteşarlığının ana hizmet birimlerinden Araştırma ve Geliştirme Dairesi Başkanlığının terörle mücadelede görevlerinin neler olduğu düzenlenmekte olup, (1) numaralı alt bendinde ise 'veri, bilgi ve belgeleri toplamak tasnif etmek' ibaresi yer almaktadır.

Anayasa'nın 'özel hayatın gizliliği' başlıklı 20. maddesinde 'Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar.' denilmektedir. Maddede ayrıca kişisel verilerin ancak Kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hükmüne de yer verilmiştir. Bilindiği gibi; 'kişisel veri' kavramı, belirli veya kimliği belirlenebilir olmak şartıyla bir kişiye ait bütün bilgileri ifade etmektedir.

İptali istenilen kuralda ise herhangi bir sınırlama getirilmeden kişilere ait verilerin toplanması konusunda Kamu Düzeni ve Güvenliği Müsteşarlığına yetki verilmesi, kişileri idareye karşı

korunmasız duruma getirmekte olup, bu haliyle kural Anayasa'nın 20. maddesinde öngörülen, kişisel veri, bilgi ve belgelerin korunması hakkına aykırıdır.

Açıklanan nedenlerle 17.2.2010 günlü, 5952 sayılı Kanun'un 1. maddesinin (1) numaralı fıkrası, 3. maddesinin (1) numaralı fıkrası, 4. maddesinin (2) numaralı fıkrası, 5. maddesinin (2) numaralı fıkrası, 10. maddesinin (1) numaralı fıkrası (c) bendi, 13. maddesinin (2) numaralı fıkrası hakkında incelemenin sürdürülmesi ve esası hakkında karar verilmesi gerektiği, 9. maddenin (b) bendinin (1) numaralı fıkrasının (1) numaralı alt bendinde yer alan "veri, bilgi ve belgeleri toplamak, tasnif etmek" ibaresinin iptali gerektiği düşüncesi ile verilen karara katılmıyorum.

Üye - Zehra Ayla PERKTAŞ

KARŞI OY YAZISI

Geçici güvenlik için özgürlüğünü feda edenler,
ne özgürlüğü hak eder, ne de güvenliği.

Benjamin Franklin, 1755

5952 sayılı Kamu Düzeni ve Güvenliği Müsteşarlığının (KDGM) Teşkilat ve Görevleri Hakkında Kanun'un 9. maddesinin (1) numaralı fıkrasının (b) bendinin, (1) numaralı alt bendinde, Müsteşarlığın ana hizmet birimlerinden olan Araştırma-Geliştirme Daire Başkanlığının, 'terörle mücadele alanında; veri, bilgi ve belgeleri toplamak, tasnif etmek, analiz ve değerlendirmeler' yapmakla görevli olduğu hükmü yer almaktadır. Burada, 'veri, bilgi ve belgeleri toplamak, tasnif etmek', kısmının iptali istenmektedir.

Bu düzenlemede anayasal bir sorun görmeyen çoğunluk görüşüne katılmanın neden mümkün olmadığını üç bölümden oluşan karşı oy yazısıyla açıklamaya çalışacağız. İlk bölümde uluslararası sözleşmelerin ilgili hükümlerini ve mahkeme kararlarını, ikinci bölümde ise iptali istenilen kuralın anayasaya aykırı olduğu yönündeki iddiamızı temellendirebilmek için konuyla yakından ilgili olduğunu düşündüğümüz özgürlük ve güvenlik arasındaki ilişkiyi, iktisat teorisinden de yararlanarak kısaca inceleyeceğiz. Son bölümde ise, ilgili düzenlemenin Anayasa'nın hangi maddelerine aykırılık taşıdığını ilk iki bölümden hareketle ele alacağız.

Uluslar arası Hukuki Durum: Sözleşmeler ve Mahkeme Kararları

Türkiye'nin taraf olduğu Uluslararası Medeni ve Siyasi Haklar Sözleşmesi'nin 17. maddesinde, 'Hiç kimsenin özel hayatına, ailesine, evine ya da haberleşmesine keyfi ya da yasadışı olarak müdahale

edilemeyeceği' belirtilirken, Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) 8. maddesinin ilk fıkrasında da, 'Herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir', hükmü yer almaktadır. İkinci fıkrada ise, 'Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda, zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir' denmektedir. Bu düzenlemeyle Sözleşme'nin 8. maddesinin ilk fıkrasında tanınan hakların kullanılmasına, ikinci fıkrada belirtilen hususlarla sınırlı olmak kaydıyla kısıtlamalar getirilebilmektedir. İptali istenen kural açısından değerlendirildiğinde, devletin negatif yükümlülüğü, 8. maddeye aykırı olarak kişisel ve hassas verilerde dâhil olmak üzere her çeşit veri, bilgi ve belgeyi toplama, saklama, işleme ve üçüncü taraflarla paylaşma gibi müdahalelerden kaçınmasını ifade ederken, pozitif yükümlülüğü, özel yaşam hakkına saygıyı güvence altına almak için gerekli önlemleri almasına işaret etmektedir.

Konumuz açısından önemli olan bir sözleşmede, 1981 tarihli ve 108 sayılı, 'Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Avrupa Konseyi Sözleşmesidir*'. Bu Sözleşme'nin 2. maddesi, kişisel veriyi belirli veya belirlenebilir bir kişiye ait tüm bilgiler şeklinde tanımlamaktadır. Adalet Bakanlığı tarafından hazırlanan 'Kişisel Verilerin Korunması Kanun' tasarısında da bu tanım benimsenmiştir. Sözleşme'nin 5. maddesine göre, kişisel veriler açıkça belirlenmiş meşru amaçlar için, toplanma gerekçesiyle sınırlı olmak ve gerekli olan süreyi aşmamak şartlarıyla tutulabilir. 6. maddede ise, kişinin ırkı ve etnik kökeni, siyasi düşüncesi, dini veya benzer inançları, sağlık, cinsel hayat ve ceza mahkûmiyetleriyle ilgili verileri hassas veri olarak kabul edilerek, bunların toplanmasına ve işlenmesine ulusal mevzuatta koruyucu tedbirlerinin alınması şartıyla izin verilmektedir. Sözleşme'nin 9. maddesinde de, kamu güvenliğinin sağlanması, suçla mücadele edilmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin güvence altına alınması ile kişisel verilerin korunmasının sınırlanabileceği belirtilmiştir.

Avrupa Konseyince 2002'de kabul edilen, 'İnsan Hakları ve Terörle Mücadele Hakkında İlkeler', rehberinde de, devletin güvenlik birimleri bünyesinde herhangi bir yetkili merci tarafından kişisel veri ve bilgilerin toplanması ve incelenmesinin, yasayla yapılması, amacıyla orantılılık içermesi ve bağımsız bir makamın gözetimine tâbi olması şartıyla meşru olduğu ifade edilmiştir. Rehberde, 'Bir yandan, demokratik bir toplumun' kendisini korumak üzere birtakım önleyici ya da bastırıcı tedbirler alması gerekirken, öte yandan, kamu makamları'Avrupa İnsan Hakları Sözleşmesi ve diğer

enstrümanlarda belirlenmiş olan insan hakları ve temel özgürlükleri gözetmek konusunda yasal bir yükümlülük altındadır', ifadesi de yer almaktadır (Avrupa Konseyi 2002: 16).

Avrupa Konseyi Bakanlar Komitesi'nin, 'Emniyet Alanında Kişisel Verilerin Kullanılmasını' düzenleyen R(87)15 sayılı Tavsiye Kararına göre ise, verilerin polisiye amaçlarla toplanmasına ancak gerçek bir tehlikenin önlenmesi ya da belirli bir suçun engellenmesi için zorunlu olması durumunda başvurulması gerekmektedir. Kişinin bilgisi dışında kişiye ilişkin verilerin toplanması ve saklanması durumunda, bu veriler silinmediği takdirde, kişiye bu konuda bilgi verilmesi de bu ilke çerçevesinde istenmiştir (Atak 2010: 106).

AİHS kişisel verilerin korunması ile ilgili ayrı bir hüküm içermemekle birlikte, Avrupa İnsan Hakları Mahkemesi (AİHM), bu verilerin özel yaşam alanı içinde yer aldığını kabul ederek, konuyu 8. madde kapsamında incelemektedir. AİHM, özel hayatı, kişinin kendi hayatını istediği gibi yaşayabileceği bir iç alan ve bunun da ötesinde, başkalarıyla ilişki kurmak ve bu ilişkileri geliştirmek suretiyle özgür olarak kişiliğini oluşturmasını ve geliştirmesini sağlayan daha geniş bir alandan ibaret görmektedir.

Nitekim AİHM, Klass ve Diğerleri-Almanya (1978) davasında, bireyin özel hayatına ilişkin verilerin kamusal organlar tarafından toplanmasına, saklanmasına ve işlenmesine dayanak oluşturacak önemli ilkeleri belirlemiştir. Mahkeme bu davada, mektupların ve telgrafların okunmasına, telefon görüşmelerinin dinlenmesi ve kaydedilmesine olanak tanıyan bir yasanın Sözleşme'ye uygunluğunu incelemiştir. AİHM genel olarak gizli izleme yöntemlerine demokratik kurumların korunması için kesinlikle zorunlu olması durumunda başvurulabileceğini kabul etmiş, ancak bireyin 8. maddede güvence altına alınan hakkı kullanabilmesi ile demokratik bir toplumu koruma amacıyla gizli izlemenin yapılmasının gerekliliği arasında bir denge kurulması gerektiğini belirterek, 'Milli güvenliği korumak için oluşturulan bir gizli izleme sisteminin, demokrasiyi korumak adına demokrasiye zarar verebileceği, hatta demokrasiyi yok edebileceği riski dikkate alındığında, kötüye kullanmaya karşı teminatların gerekli olduğu konusunda bir tereddüt bulunmamaktadır', görüşünü dile getirmiştir (Klass ve Diğerleri-Almanya para. 42 ve 49). Bu kararda, Mahkeme, bireyin özel yaşamı kapsamındaki bilgilere ilişkin kamusal müdahaleleri, bireyi koruyucu uygun ve etkili garantiler içeren yasal düzenlemeler ve istismar ve kötü kullanıma karşı güvenceler bulunmadığı sürece Sözleşmenin 8. maddesinde belirtilen hakların bir ihlali olarak değerlendirmiştir (Klass ve Diğerleri-Almanya para. 50). Mahkeme, istihbarat örgütlerinin gizli izleme yoluyla bireylerin haklarına yönelik gerçekleştirdikleri müdahalelerin etkili bir denetime tabi olması gerektiğini, ulusal güvenlikten kaynaklanan ihtiyaçlara her durumda öncelik verilemeyeceğini, sınırsız önlemler alınmasına izin veren bir yasanın demokrasi için tehdit oluşturacağını ve Avrupa ülkelerinin casusluk

ve terörizmle mücadeleyi gerekçe göstererek uygun gördükleri her türlü tedbiri alamayacaklarını önemle vurgulamıştır.

AİHM, Leander-İsveç (1987) kararında ise, başvurucu hakkında güvenlik soruşturması yapılması suretiyle bilgi toplanmasının ve bunların doğruluğuna ilişkin olarak kendisine itiraz hakkı verilmemesinin, AİHS 8. madde birinci fıkrası kapsamında özel hayatın gizliliğine müdahale oluşturduğuna, ancak, bu müdahalenin aynı maddenin ikinci fıkrası gereğince milli güvenliği koruma meşru amacını gerçekleştirmek için taraf devletlere tanınan geniş takdir hakkı içinde olduğu sonucuna ulaşmıştır. Bununla birlikte, Mahkeme, verilerin toplanmasına olanak tanıyan düzenlemelerin makul denetim mekanizmaları öngörmek zorunda olduğunu, bunların da, hangi durumlarda verilerin toplanabileceği, ne kadar süre ile muhafaza edileceği ve imhasına ilişkin hususlara yer vermesi gerektiğini not etmiştir.

Amann v. İsviçre (2000) davasında bireyin özel yaşamına ilişkin bilgilerin kamu görevlileri tarafından saklanması özel yaşama bir müdahale oluşturduğunu kabul etmiştir. Yapılan müdahale yasaya dayanmakla birlikte, mevcut yasal düzenleme yeterli korumayı sağlamamaktadır. İlgili yasada savcılığın veri toplama, kaydetme ve saklama yetkisini kullanma şartları ve kapsamı belirtilmemekte, hangi bilgilerin saklanacağı ve nasıl bir yöntem izleneceği konusunda açıklık bulunmamaktadır (Amann- İsviçre para. 76 ve 80).

AİHM'nin Rotaru-Romanya (2000) kararı da konumuz açısından önem taşımaktadır. Bu davada, Romanya İstihbarat Örgütü'nün başvurucu hakkında tuttuğu gizli dosya ele alınmıştır. İlgili devlet, dosyada yer alan bilgilerin özel yaşama ilişkin olmadığını, kamusal alandaki faaliyetlerle ilgili olan bilgileri içerdiğini ileri sürmüştü de, Mahkeme, 108 sayılı Sözleşme'nin kişisel veri tanımına atıfla, bunu kabul etmemiştir. AİHM, terörle mücadelede özel yöntemlerin kullanılabilirliğini kabul ederek, istisnaî hallerde ve bir yasal düzenlemeye dayanmak şartıyla, demokratik bir toplumda milli güvenlik ve/veya asayişin bozulması ya da suçun önlenmesi gibi amaçlar dâhilinde veri toplanabileceğini kabul etmektedir (Rotaru-Romanya para. 57-58). AİHM, yetkili otoriteler tarafından kişinin kamusal hayatına ilişkin bilginin sistematik olarak toplandığı ve saklandığı durumları özel hayat kapsamında değerlendirerek, bunun kişinin çok uzak geçmişiyile ilgili bilgiler içermesi halinde dahi geçerli olduğunu ifade etmiştir. Mahkeme, yürürlükte olan yasanın milli güvenliği etkileyecek bilgilerin toplanmasına, kaydedilmesine ve gizli dosyalarda arşivlenmesine izin verdiğini saptamış ancak bu yasanın AİHS ile uyumlu olmadığını tespit etmiştir. AİHM, hangi koşullar altında, hangi amaçla, ne kadar süreyle kamu otoritelerinin özel hayatla ilgili bilgileri saklayacağı ve kullanacağını belirsizliğini, istismarlara karşı hiçbir önlem alınmamasını, kötüye kullanımı engellemeye yönelik

etkili denetim mekanizmalarının öngörülmemesini ve verilerin değerlendirilmesine ilişkin hukuki sınırlar çizilmemesini, AİHS'nin 8.maddesinin ihlali olarak görmüştür (Rotaru v.Romanya para.57 ve 59).

Mahkeme, Segerstedt-Wiber ve Diğerleri-İsveç (2006) davasında da kişisel verilerin kamu birimleri tarafından toplanması ve saklanması incelenmiştir. Başvurucular, kişisel verilerinin gizli polis biriminde saklanmasının ve bunların içeriği hakkında kendilerine bilgi verilmemesinin AİHS 8. maddeye aykırı olduğunu ileri sürmüşlerdir. AİHM saklanan bilgilerin özel hayata ait bilgiler olduğunu tespit etmiştir. Ancak, ilk başvuru bakımından, bu bilgilerin bir kısmının suçun önlenmesi amacı taşıması nedeniyle ihlal bulmamıştır. Aynı şekilde saklanan verilerin tamamının başvurularda açıklanmamasını da, ilgili yasanın buna izin verip, yeterli güvenceyi sağladığı gerekçesiyle 8. maddeye aykırı bulmamıştır. Buna karşılık Mahkeme, diğer başvurulardan, toplanan ve muhafaza edilen verilerin katıldıkları siyasi faaliyetler ilgili olması ve bu faaliyetlerin taraf devletin milli güvenliğini tehdit ettiğine dair yeterli kanıtın olmamasından hareketle, bu verilerin sürekli saklanmasının, Sözleşme'nin 8.maddesini ihlal ettiği sonucuna varmıştır (Segerstedt-Wiber ve Diğerleri-. İsveçpara.88-92)

AİHM'nin kararları kadar ulusal anayasa mahkemelerinin, özellikle de Almanya Federal Anayasa Mahkemesi'nin, konumuz bağlamında verdiği önemli bazı kararlardan da bahsetmek yerinde olacaktır.

Alman Mahkemesi 1983'de nüfus sayımıyla ilgili bir kararında, Alman Anayasasının insan onurunu teminat altına alan md. 1/1 ile bağlantılı olarak, md. 2/1'de düzenlenen kamu düzenini bozmama, genel ahlaka aykırı olmama ve kimseye zarar vermeme kaydıyla, bireylerin kişiliklerini istedikleri gibi geliştirebilme hakkı düzenlemesinden hareketle, kişisel veriler üzerinde kendi kaderini tayin temel hakkının varlığını kabul etmiştir. 'Enformasyonel özerklik' olarak tanımlanan bu hak, kişiliğin serbestçe geliştirilmesi hakkı ile insan onurundan kaynaklanan genel kişilik hakkının bir yansıması olarak, bireyin kendi hakkındaki bilgileri kontrol edebilme, kendisine ilişkin herhangi bir bilginin rızası olmaksızın açıklanmaması, yayılmaması, bu bilgilere başkalarının ulaşmaması, kişisel verilerin sınırsız toplanması, kaydedilmesi, kullanılması ve nakledilmesine karşı bireyin korunmasını içermektedir (Küzeci 2010: 67-8).

Federal Anayasa Mahkemesi, 2006'da önüne gelen bir bireysel başvuruda, 'enformasyonel özerkliğin' ihlal edildiği sonucuna ulaşmıştır. 24 yaşında Fas'lı bir öğrenci olan başvuru, El-Kaide yanlısı 'uyuyan hücreler' olup, olmadığını ortaya çıkarmak için 18-40 yaş arası tüm Müslüman erkek öğrencilerle ilgili veri toplanmasına olanak tanıyan Kuzey Ren Westphalia Eyaleti Polis Yasası'nın 31.

maddesinin Alman anayasasına aykırılığını iddia etmiştir. Bu uygulama sonucunda, yukarıdaki kişisel özellikleri taşıyan ve adı geçen eyalette ikamet eden 32 bin kişi ile ilgili toplam 5 milyon kayıt elde edilip, dosyalanmış sadece 8 kişi için ayrıntılı araştırma yapılmasına ihtiyaç duyulmuş ve sonuçta bunların hiçbiri aleyhine dava açılmamıştır (Young 2008: 338). Şüpheli olmayan ve demokratik toplum düzeni için herhangi bir tehlike arz etmeyen bu kişiler hakkında sırf belli dini, etnik ve yaş grupları içinde olmalarından dolayı bilgi toplanmış, yani bu insanlar, ülkemizdeki tabiriyle fişlenmiştir. Olayı inceleyen Mahkeme, Alman Anayasası'nın 1. maddesi ile birlikte değerlendirildiğinde 2. maddesinin ilk fıkrasının ihlal edildiği sonucuna varmıştır. Mahkeme kararında, 'Anayasanın, yasa koyucunun özgürlük ve güvenlik arasında makul bir denge bulmasını belirttiğine' dikkati çekerek bunun da 'her halükarda imkânsız olan mutlak bir güvenlik peşinde koşmayı dışladığını' belirtmiştir (Young 2008: 386). Mahkeme'ye göre, toplanan bilgiler ve veriler kişilik açısından önemsiz olsa bile, genel bir terör tehdidi karşısında polise verilen yetkinin çok geniş ve açık uçlu olması ve toplanan verilerin çapraz referans olarak başka amaçlar için kullanılabilme olasılığının varlığı, Alman Anayasa'sının yukarıda belirtilen fıkrasının ihlal edilmesi sonucunu doğurmaktadır. Alman Mahkemesi için varsayımsal temellerden hareketle, soyut ve genel bir tehlike terörle mücadele adı altında meşrulaştırılsa dahi, kişiler hakkında veri toplanmamalı ve kişisel veri elde etmek için veri madenciliği (data mining) ve benzeri faaliyetlere ancak ve ancak somut ve yakın belirli bir ciddi suç işlenmesi tehlikesi karşısından girilmesi meşru olacaktır (Schwartz 2011: 372).

Anayasa Mahkemesi de, Türkiye İstatistik Kanunuyla ilgili bir kararında (E: 2006/167 Esas, K:2008/86), istenecek bilgilerin kapsam ya da sınırlarının belirsizliğinin, bireyi İdareye karşı korumasız bıraktığını, bunun da Anayasa'nın özel hayatın gizliliğini koruyan hükümlerine aykırı olduğunu tespit etmiştir.

Şu ana kadar anlatılanlardan iki önemli sonuç ortaya çıkmaktadır. İlk olarak, Uluslararası Sözleşmeler ve Mahkeme kararlarına baktığımızda, terörle mücadelede, kişisel verilerin toplanması, saklanması ve işlenmesi yakın ve somut bir tehlike varsa meşru görülmektedir. İkinci sonuçta ise, ilgili yasal düzenlemelerin ucu açık ve belirsiz olmamasının önemi vurgulanmakta ve bu işin bağımsız, dışsal bir otorite tarafından denetlenmesi gerektiğinin altı ısrarla çizilmektedir.

Özgürlük-Güvenlik: Denge mi; İkilem mi'

KDGM'nin internet sayfasında, Müsteşarlığın, 'Özgürlük ve güvenlik dengesini daima gözetin' bir kurum olduğu vurgulanmaktadır. Oysa iptali istenen kural özgürlük-güvenlik dengesini gözetmemekte, tam tersine güvenliği özgürlüğe öncelemektedir. Güvenlik diğer tüm hakları ve özgürlükleri temellendiren bir tür meta-hak değildir (Michaelsen 2006: 14-5). Güvenlik ve özgürlük

arasında bir öncelik veya hiyerarşi yoktur. Bununla birlikte, bir an için olduğunu varsayalım. Böyle bir durumda özgürlük güvenlik temelli değil, güvenlik özgürlük temelli olmalıdır. Özgürlük-güvenlik dengesi azami etkinliği gerçekleştirecek bir güvenlik sağlamayabilir ama bu otoriter bir siyasi sistemden ziyade anayasal bir demokraside yaşamının bedeli olarak düşünülmelidir.

Şüphesiz ki, insan hayatını, malını, haklarını ve özgürlüğünü tehdit eden terör ile mücadele etmek devletin asli görevlerinden biridir. Ancak, bunun başarılı olabilmesi için uygulanacak politikaların, evrensel insan hakları ve hukuk devleti ilkelerine uygun olması, devletin demokratik sınırlar içinde kalarak, insan haklarına mümkün olduğunca asgari seviyede müdahaleyi gerektiren önlemleri tercih etmesi gerekmektedir. Terör örgütleri neredeyse hiçbir kural tanımadan her türlü faaliyetleri ve eylemleri gerçekleştirirken, demokratik ve insan haklarına saygılı olduğunu iddia eden devletler terör ile mücadelede hukuk ve demokrasi sınırları içinde kalmak mecburiyetindedirler. Bu bir zafiyet değil, demokrasinin ahlaki üstünlüğünün ve erdemliliğinin bir sonucu olarak değerlendirilmelidir.

Devletin terör eylemlerini tespit etme ve önlemeye dönük faaliyetlerinde, korumaya çalıştığı bireylerin haklarını ihlal etmeme ve bunları aşırı sınırlamama hususlarında özen göstermesi demokratik toplum düzeninin oluşturulması, korunması ve geliştirilmesi açısından hayati öneme sahiptir. Teröre karşı, devletin bireylerin başta yaşam hakkı olmak üzere çeşitli haklarını korumak pozitif yükümlülüğünün yanı sıra, negatif olarak da anayasal düzenin tanıdığı haklara saygı yükümlülüğü vardır. Burada açıklığa kavuşturulması gereken konu, temel hakları korumak adına bunlarla ilgili sınırlamaların derecesinin ne olacağıdır. Sorun, 'özgürlüğün güvenlikten daha çok veya daha az önemli olup olmadığından ziyade, belli bir güvenlik tedbirinin özgürlüğü, koruduğu güvenlikten daha az mı, daha çok mu zarar verip, vermediğinin belirlenmesidir' (Posner 2006: 31-2). Bir demokrasiyi otoriter bir siyasi, hukuki ve toplumsal düzenden ayıran en önemli hususlardan biri güvenliğin özgürlük ortamında sağlanabilmesidir.

Belli düzeylerde güvenlik ve özgürlük birbirine ikame edebileceği gibi tamamlayıcı olabilir. Güvenlik olmadan özgürlüğün bir anlamı olmadığı gibi, özgürlüğe yer vermeyen, onu kısıtlama eğilimi taşıyan bir güvenlik anlayışının da anlamı yoktur (Waldron 2003: 195). Güvenliğin olmadığı yerde kim kendini özgür his eder ne kadar doğruysa, özgürlüğün olmadığı yerde kim kendini güvende his edebilir de o kadar doğrudur. Demokrasilerde güvenlik ve özgürlük birbirini tamamlayıcı olup, taraflardan birinin kazanıp diğerinin kaybettiği sıfır toplamlı bir oyun değildir.

Güvenlik için hakların, özgürlüklerin kolayca kısıtlanması devlet gücünün artması sonucunu doğurmaktadır. Zaten güvenlik dediğimiz andan itibaren devleti adeta ayrıcalıklı kılan bir alana girdiğimizden, bir Leviathan yaratma tehlikesiyle karşı karşıya gelebiliriz. Bunun anlamı, John

Locke'nin, 'Hükümet Üzerine İkinci İncelemede' vurguladığı gibi, 'insanların sansar veya tilkilerden gelebilecek zararlara karşı kendilerini korumaktan kaçınacak, fakat aslanlar tarafından yutulmaktan memnun olacak kadar aptal olduklarını düşünmektir' (2010: 88-9). Bizi falanca veya filanca tehlikeden korumak için devletin aldığı her tedbiri meşru görmek, insanların tilkiler ve sansarlardan gelebilecek tehlikelere karşı korunayım derken aslanlar tarafından yutulmasına güvenlik adına razı olmak demektir.

Demokratik bir toplumda yasa koyucuların karşılaştıkları en önemli sorunlardan biri kamu güvenliğini sağlamak için alınacak tedbirlerle insan haklarının korunması ve geliştirilmesi arasındaki ilişkidir. Bu özgürlük-güvenlik ilişkisini, iktisat teorisinde yaygın olarak kullanılan Pareto Sınırı kavramıyla göstermeye çalışalım.

Kaynak: Vermeule, 2011: 2

Eksenlerin birinde özgürlük, diğerinde ise güvenlik gösterilmektedir. Eğrinin veya sınırın üzerinde güvenlikteki bir artış özgürlükte bir azalamaya neden olacaktır ve bunun tersi de doğrudur. Pareto Sınırı altında, mesela P noktasında, güvenlik ve özgürlük birbirinden taviz vermeden arttırılabilir. Sınırın ötesindeki politikalar kaynak yokluğundan veya siyaseten uygulanamaz olduğundan tercih edilemez ve yasa koyucunun toplam refahı arttıracak özgürlük ve güvenlik politikalarını takip etmesi beklenir. Güvenliğe ve özgürlüğe yönelik politikaların toplumsal refaha marjinal katkısının eşit olduğu nokta uygun politika seçimi olabilir. K-K* noktasının altında özgürlük politikalarının olmasına toplum, güvenlik ve toplam refah artsa bile izin vermeyebilir. Q'Q*' a doğru gittiğimizde ise güvenlikte bir artış olmadan özgürlük azalmakta ve aynı şekilde R-R*'ya doğru gittiğimizde özgürlük artmadan güvenlik azalmaktadır.

Güvenlik ve özgürlük bireysel refaha katkı yapan değerli mallar olup, bireyler açısından birbirleriyle karşılaştırılabilirler(Posner ve Vermeule 2007: 22). Başka bir deyişle, birini göz ardı ederek, diğerini maksimize edemeyiz. Güvenlik-özgürlük sınırında, güvenlikteki bir artış, özgürlükte bir azalma gerektirmekte olup, bunun tersi de doğrudur (Posner ve Vermeule 2007: 26). Pareto sınırı bir kere oluştuktan sonra değişmeyen bir sınır değildir. Güvenlikteki artış özgürlüklerdeki azalmaya değerse devlet güvenliği arttırır. Benzer şekilde, güvenlikteki azalma, özgürlük artışına değerse, güvenliği azaltarak Pareto sınırını değiştirebilir. Benzer şekilde, terörle mücadele eden bir kamu kurumu ve saldırı planlayan bir terörist örgüt arasındaki etkileşimi oyun teorisi bağlamında inceleyen bir çalışmada, özgürlüğü azaltıcı tedbirlerin terörizme karşı artan bir güvenlik sağlamadığı görülmüştür (Dragu 2011: 64).

Elbette, ilgili hukuki düzenlemeler çerçevesinde şüphe duyulan bir kişi hakkında veri toplanabilir. Ancak hiçbir şüphe olmadan geliştirilen ve tanımlanan profiller çerçevesinde veri toplanması sorunlu bir uygulamadır. Unutulmamalıdır ki, Kafka'nın 'Dava' romanının kahramanı K'nın başına gelen her bireyin başına da gelebilir. K'nın neden tutuklandığı ona bir türlü söylenmediği için kendisine yönelik iddiaları çürütme şansı hiç olmuyor. Her türlü veri, veri madenciliği yapmaya olanak tanıdığından, kendilerinden şüphelenilen bireylerin neden şüphelenildiğini asla öğrenememeleri ve bu şüpheyi giderici hiçbir şey yapamamaları sonucunu doğurabilir.

Büyük veri yığınları içerisinde gelecekle ilgili tahminde bulunmayı sağlayacak bağıntıların bilgisayar programı ve istatistiksel teknikler kullanarak aranması demek olan veri madenciliği, konumuz bağlamında, toplanan kişisel verilerin birleştirilerek şüpheli görülen belli özelliklerin ve davranış biçimlerinin bu temelden hareketle çözümlenmesini içermektedir. Bir suç işlenmesi olasılığı karşısında veri madenciliği ve profil oluşturulabilir ama bunun ağla yapılan balık avı gibi, 'ne çıkarsa bahtımıza' anlayışıyla yürütülmesi tehlikelidir (Solove 2011: 190-195).

Veri madenciliği ve hassas kişisel veriler esas alınarak profil oluşturma, idari bir kararla hiçbir suçu olmayan çok sayıda insan için özel hayatlarını içeren bilgi ve verilerin toplanması anlamına gelmektedir ve bunun demokratik bir toplumda kabul edilemeyeceğini Avrupa Konseyi İnsan Hakları Komiseri de 2008'de konuyla ilgili olarak yayınladığı bir raporda belirtmiştir (2008: 4). BM İnsan Hakları Konseyi, 'Terörle Mücadelede Temel Özgürlüklerin ve İnsan Haklarının Korunması ve Teşvik Edilmesi' özel raportörü de, terörizmle mücadelenin, mahremiyete, özel yaşamın gizliliğine otomatikman müdahaleyi meşrulaştıran bir koz olmadığını vurgulayarak, kötüye kullanma olasılığına karşı güvencelerin varlığını ve elde edilen veri ve bilginin kullanımının, saklanması ve paylaşımının sınırlarının belirli olması gerektiğinin altını çizmektedir. Raportör, özel yaşam ihlalinin seviyesi arttıkça ilgili kurumun karar verme mekanizmasında daha üst düzey yetkililerin onayının aranması, mahremiyet etki değerlendirmesi ile ilgili düzenlemelerin yapılmasını ve bütün bunları denetleyecek bağımsız bir makamın oluşturulmasını da önerileri arasında saymaktadır (Scheinin 2009).

Kamu güvenliğini tehdit edici faaliyetlere katılma olasılığının yüksek olduğu düşünülen bireylerle ve gruplar bunun ceremesini çoğunluğa göre çok daha fazla çekmektedir (Michaelsen 2005: 78). Genel olarak özgürlük bireysel bir hak olarak belirsiz ve soyut bir şey gibi algılanırken, güvenlik somut olarak can ve mal emniyetini akla getirmektedir. Bu nedenle de insanların çoğunluğu daha güvenli olmak veya öyle hissetmek için hak ve özgürlüklerinden fedakârlığa hazırdır. Bununla birlikte, özgürlüğü sınırlayan tedbirler ve özgürlüğün kısıtlanmasının getirdiği maliyetler dağıtımsal özelliğe

sahip olduğundan herkes bu durumdan aynı oranda etkilenmemektedir. Toplumdaki herkes özgürlüğünden azıcık fedakârlık edip, daha çok güvenlik içinde olmamaktadır (Waldron 2007: 503). Özellikle siyasi görüş, etnik, ırk, din, cinsiyet ve cinsel tercih olarak ötekileştirilen, azınlıkta kalan bireyler ve gruplar hakkında önyargılı bir şekilde profiller oluşturulabilir. İnsanlar güvenlik için haklarından ve özgürlüklerinden fedakârlık yaptıklarında aslında vazgeçtikleri kendilerinin değil, başkalarının, özellikle de ötekileştirilenlerin ve azınlıkların haklarıdır (Sottiaux 2008: 8).

Güvenlik politikası, hukuk devleti ve insan haklarına dayalı olmalıdır ve gerçek anlamda güvenliğin, ancak demokrasiyle sağlanabileceği unutulmamalıdır. Terörle mücadele sırasında demokrasiyi koruyayım derken onu zayıflatabilecek, hatta tahrip edebilecek önlemler alınmasından kaçınmak gerekir. Amaç aracı meşru kılsa da terörist ile terörle mücadele edenler arasındaki ahlaki ve hukuki ayırım azalır ve özgürlüğü daraltmanın uzun dönemli sonuçları kısa dönemde terörle mücadelenin getirdiği kazançları zayıflatabilir. Zaten, özgürlükten yapılacak fedakârlıkların etkin güvenlik sağlamadığı da bir gerçektir. Güvenliğin etkinliğini zayıflattığı düşünülen insan hak ve özgürlüklerin tamamen ortadan kaldırıldığı bir durumda bile mutlak bir güvenliği sağlamak mümkün değildir (Hein van Kempen 2013: 14). Demokratik bir devlette güvenlik önlemleri sadece güvenlik bürokrasisinin takdirine bırakılmayacak kadar önemlidir. Sağlıklı bir demokraside devlet, 'merak etmeyin, bana güvenin' diyerek, terörle mücadele için alınan tedbirlerin kişi hak ve özgürlüklerine olan etkisini göz ardı edemez.

Görüldüğü üzere özgürlük ve güvenlik arasındaki ilişki bir ikilemden ziyade dengeye dayanmaktadır. İptali istenen kuralda bu denge gözetilmeyerek, aşağıda ele alacağımız anayasal haklar ihlal edilmiştir.

13. Madde Yönünden

Anayasa'nın 13. maddesinde, temel hak ve özgürlüklerin özlerine dokunulmaksızın ölçülülük ilkesine uygun şekilde, yasayla sınırlandırılabilmesi belirtilmektedir. Ölçülülük ilkesi sınırlamada başvurulan aracın sınırlama amacını gerçekleştirmeye elverişli olmasını; bu aracın sınırlama amacı açısından gerekli olmasını ve araçla amacın ölçüsüz bir oran içinde bulunmamasını ifade eder. Burada kısıtlama için kullanılan araçla amaç arasında hak ve özgürlüğü en az sınırlayacak dengeli bir orantı aranmaktadır.

KDGM'nin terörle mücadele etmek için kişinin özel hayatını da içerecek şekilde, ona ait veri, bilgi ve belgeleri toplamasının, saklamasının ve işleminin o bireyin özel hayatına müdahale anlamına geldiği hususunda bir şüphe bulunmamaktadır. Toplanacak veri, bilgi ve belgelerin türü, içeriği, hangi insan gruplarını kapsayacağı, toplanmış veri, bilgi ve belgelerin ne kadar süre ile muhafaza

edileceği ölçülülük ve demokratik toplumda gereklilik testine göre değerlendirilmelidir. Burada sorulması gereken soru bu hak ihlalinin terörle mücadele alanında demokratik toplum gereklerine ve zorunluluklarına ne ölçüde uyup, uymadığıdır.

Bireylerin korunması ve güvenliklerinin sağlanması amacını taşıyan terörle mücadele, bu yönüyle insan haklarını korumaya katkı yaparken, bu mücadelede alınan bazı tedbirler bireylerin hak ve özgürlüklerinin sınırlandırılmasına neden olmaktadır. İptali istenen kural temel hakların sınırlandırılmasına ilişkin düzenlemelerden muaf düşünülemez. Veri, bilgi ve belge toplama demokratik bir toplumda milli güvenlik, kamu düzeni ve suçun önlenmesi gibi amaçlara ulaşmak için dahi olsa ölçülü olmalıdır.

Elverişlilik ölçütüne göre bir yasal düzenlemenin sınırlama amacı bakımından elverişli sayılması için bu düzenlemenin arzulan amaca katkı yapması gerekmektedir. Konumuz açısından bakıldığında, veri, bilgi ve belge toplanmasının terörle mücadele amacına hizmet ettiğini söyleyebiliriz. Gereklilik ise bir temel hakkı en az sınırlayan aracın seçilmesini gerektirmekle birlikte iptali istenen kuralın, hakkı en az sınırlayan yumuşak bir araç olduğunu söyleyemeyiz. Çünkü söz konusu kural çok geniş ve sınırsız bir çerçeveyi kapsayarak, terörle mücadele adına, bireyin her türlü eylemini kapsamı dâhilinde görmekte, ona devlet müdahalesine karşı nefes alacak bir alan bırakmamaktadır. Orantılılıkta aranan ise araç ve amacın birbirine karşı ölçüsüz bir oran içerisinde olmamasıdır. Terörle mücadele amacıyla sınırsız bir şekilde, herhangi bir bağımsız denetime tabi olmadan, neredeyse başıboş bir tarzda veri, bilgi ve belge toplanması ölçüsüz bir orantısızlık yaratmaktadır. Orantılılık, yetkililerin, makul, dikkatli ve iyi niyetli hareket etmelerini ve müdahaleyi haklı kılmak için ileri sürülen sebeplerin tatmin edici, gerekli ve yeterli olmasını da kapsar. Bireyin özel alanının tehlikeye girmesi, onun hakkında veri, bilgi ve belge toplanması kadar, kime, hangi amaçlarla bunların aktarılacağı konusunda denetim imkânını da kaybetmesinde yatmaktadır. Yasal olarak veri, bilgi ve belge toplayan, kamu kuruluşları amacı gerçekleştirmeye yetecek kadar veriyle kendilerini sınırlamalıdır. İtiraza konu olan ibarede bu hususta hiçbir güvenceye yer verilmemiş olması, düzenlemenin orantısız olduğunun bir göstergesidir.

Veri, bilgi ve belgelerin toplanması ve tasnif edilmesinin terörle mücadele alanıyla sınırlı olacağı belirtilmekle birlikte, bu alanının kapsamının belirsiz ve tanımlanamaz olması, devlete çok geniş ve ucu açık bir takdir hakkı bırakmaktadır. Ayrıca, bunun terörle mücadelede ne derece etkinlik sağlayacağı da şüphelidir. Amerikan Bilimler Akademisinin konuyla ilgili hazırladığı bir çalışmada, çok sayıda veri içeren çok büyük veri tabanlarından potansiyel teröristleri bulabilmenin matematiksel olarak ya hatalı pozitif (suçsuz insanları şüpheli olarak değerlendirmek) ya da hatalı negatif (gerçek

suçluları veya teröristleri tespit edememek) gibi sonuçlar doğurduğu belirtilmiştir (National Research Council 2008: 2-3). Mesela, dünyada uçakla günde yaklaşık olarak 2 milyon kişi seyahat etmektedir. Tüm bu kişiler arasında terörist profiline benzeyen ve hatalı pozitif çıkanların oranının %1 olduğunu varsayalım. Bunun anlamı 20 bin kişinin haksız yere terörist olma olasılığına karşı çeşitli sınırlayıcı muamelelere maruz kalmasıdır (Solove 2008: 353). Yakın tarihe bakmakta konumuz açısından aydınlatıcı olabilir. Örneğin, Doğu Alman Hükümeti nüfusunun dörtte biri ile ilgili veri, bilgi ve belge toplamasına rağmen, kendi sonunu öngörememişti. Çok sayıda veri ve bilgiyi etkili bir şekilde çözümleyebilmek, samanlıkta iğne aramaya benzemektedir. Çeşitli gerekçelerle aşırı veri toplanmasının, bu verileri toplayanların amaçlarına ne derece hizmet ettiği de kuşkuludur. Çünkü aşırı veri toplanması, veri kirliliğine yol açmakta ve amaca uygun verilerin bu veri çöplüğünden çıkarılması, ayıklanması ve çözümlenmesi zorlaşmaktadır.

Demokratik toplumda gereklilikten anlaşılması gereken başvurulan tedbirin demokratik toplumu açıklayan ilkelerle uyumlu olup, olmamasıdır. Bu ilkelerin değerini azaltan her uygulama demokratik toplum için gerekli değildir. Demokratik toplum, ayrıca hak ve özgürlüklere karşı gerçekleştirilen her müdahaleye karşı kişilere bir takım güvencelerin de sağlanmasını gerektirir. Oysa iptali istenen ibare, kötüye kullanım olasılığı karşısında engelleyici etkili ve yeterli tedbirlere yer vermemektedir. Örneğin, KDGM'nin Araştırma-Geliştirme Dairesinin bu son derece geniş yetkisini denetleyecek bağımsız bir makam yoktur.

İptali istenilen düzenlemenin temel amacının insanları ve toplumu teröre karşı korumak olduğu görülmektedir. Bu son derece meşru bir amaçtır ve bu açıdan anayasaya aykırılık iddia edilemez. Ancak, bu amaca ulaşmak için kullanılan yöntemin uygunluğu ise sorunludur. Hakkı sınırlayan düzenlemeyle, ilgili güvenlik kuruluşuna belirsiz ve ihtiyaç duyulandan çok daha geniş bir şekilde, sınırsız veri, bilgi ve belge toplama ve tasnif yetkisi verilmektedir. Veri, bilgi ve belgelerin toplanması sırasında kişinin temel hak ve özgürlük alanına zorunlu olmadıkça müdahale edilmemeli, terörle mücadele gibi meşru bir amaç için dahi yapılacaksa, müdahalenin sınırları iyi çizilmelidir.

17. ve 20. Maddeler Yönünden

Anayasa'nın 17. maddesi herkesin, yaşama, maddî ve manevî varlığını koruma ve geliştirme hakkına sahip olduğu hükmünü içermektedir. 'Özel hayatın gizliliği' başlığını taşıyan Anayasa'nın 20. maddesine göre de, 'Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları

doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir'.

Özel hayatın gizliliği ve bu kapsamda kişisel verilerin korunması konusu her şeyden önce insan onuruna saygı ve kişilik haklarına dayanmaktadır. Bu hak, kişinin saygınlığını ve kişiliğini serbestçe geliştirmesini mümkün kılan şeref ve haysiyet, özel yaşam ve sağlık gibi kişisel değerler üzerindeki çıkarlarını belirterek, bireye kişiliğini dilediği şekilde, serbestçe geliştirebileceği, kendisi ve sevdikleriyle bir arada olabileceği özerk bir yaşam alanına sahip olma şansı vermektedir. Bu alanda birey, maddi ve manevi kişiliğini geliştirmek ve başkaları tarafından bilinmesini istemediği hususların güvence altına alınmasını istemek hakkına sahiptir.

İptali istenen kural, KDGM'ye Anayasaya aykırı bir şekilde son derece geniş ve sınırsız bir yetki vererek, muazzam bir veri, bilgi ve belge toplama, saklama, işleme ve değiştirme gücü olan devlet karşısında bireyi kişi olarak yok saymakta, onu basit bir veri nesnesi haline dönüştürmektedir. Adı geçen kural, insanı hakkında veri toplanan basit bir veri nesnesi konumuna indirgemektedir. İnsan onuruna saygı, insanlara nesneymiş gibi davranmayı yasaklamaktadır. Alman Anayasa Mahkemesi de insanın devlet için basit bir nesne olarak görülmesinin insan onuruna aykırı olduğunu ve devletin insana bir eşya gibi yaklaşmamasının gerekliliğini vurgulamıştır (Şimşek 2008: 5).

Kişisel verilerin korunması kişinin maddi ve manevi varlığını geliştirmesine imkân tanıyarak, bireyin hayatını kendi özgür iradesiyle düzenlemesine katkı sağlamaktadır. Bireyin kişisel verileri üzerindeki hakkı yeteri kadar korunmazsa, kişiliğini serbestçe geliştirmesi zora gireceğinden, özgür iradeleriyle yaşamlarını biçimlendiren bireylerden oluşan demokratik bir toplum düzeninin ortaya çıkması ve korunması da güçleşecektir. Kişinin maddi ve manevi varlığını geliştirmesi, ancak ve ancak, faaliyetlerini özgürce gerçekleştirmesi ile mümkündür. Kişisel verilerin korunmasıyla, kişisel veri toplanması, saklanması ve işlenmesi sırasında bireyin hak ve özgürlüklerinin korunarak demokratik toplum düzeninin oluşmasına katkı yapmak hedeflenmektedir.

Bireyin özel hayatını, kendi tercihleri ile nasıl şekillendirdiği ilke olarak, bir başka kişinin veya devletin ilgi alanına girmemelidir. Yaşam ilişkilerine ait tüm kişisel verileri kapsamlı bir kayda tutulan ve özel yaşamının gizliliği adeta ortadan kalkan bireyin kişiliğini geliştirmesi mümkün değildir. Kişisel verilerin korunması hakkı ihlal edildiğinde bireyin diğer temel hak ve özgürlükleri kullanması zorlaşmaktadır. Kayıt altına alınan veya alındığını düşünen birey kendi özgür kişiliğinin gereği gibi değil, kendisinden istenilen veya beklenen davranış tarzıyla hareket edecektir. Bireyler çeşitli faaliyetlerinin devlet tarafından izleneceği endişesiyle bunları gerçekleştirmekten vazgeçebilirler. Aykırı hareket tarzlarının sürekli kayıt altına alındığını düşünen birey, örneğin

örgütlenme, toplantı ve düşünce özgürlüklerini kullanmama eğilimine girecektir. Eğer insanlar seyahat etmek, iletişimde bulunmak gibi belli eylemlerin hükümet tarafından yakından izleneceğini düşünürlerse, bu eylemleri gerçekleştirmekten kaçınabilirler ve yasal faaliyetlerinde kendi kendilerini sınırlama eğilimine girebilirler. Bu durum kişinin özerkliğini etkileyerek, yurttaşların özgür iradeleriyle kendi yaşamlarını belirleyebildikleri özgürlükçü demokratik esaslara dayanan bir toplum düzeninin oluşmasını engelleyecektir.

Teknolojideki gelişmeler nedeniyle çok çeşitli denetim, gözetleme ve izleme biçimleriyle bireyin özel hayatının gizliliğini muhafaza etmek gittikçe zorlaşmaktadır. Fransız filozofu Foucault'un deyişiyle 'panoptik bir gözetleme' hayatı kuşatmaktadır. Gözetlemenin esas alındığı panoptik yaşam biçimlerine doğru evrilen modern toplumlarda özel yaşama saygı hakkının ve bu hak kapsamında korunan en önemli hukuksal çıkarlardan olan mahremiyetin nasıl korunacağı önemli bir sorun olarak karşımıza çıkmaktadır. Bireyin, ahlaki ve toplumsal kişiliğinin gelişiminde ve diğer insanlarla olan ilişkilerini düzenlemede önemli bir kavram olan mahremiyetin ihlali insan onurunun ve kişiliğinin ihlali anlamına gelmektedir. Birey muazzam ve dehşet verici bir bilgi bankası veya veri tabanı içinde bir numaradan ibaret bir nesneye indirgenme riskiyle karşı karşıya kalmaktadır. Bu gücün sınırlandırılması, özel hayatın ve kişilik haklarının korunması bakımından büyük önem taşımaktadır.

Kişisel verilerin korunması, bir özgürlük sorunudur ve özel hayatın gizliliği, yalnız kalma hakkından kişinin kendisi hakkındaki veri ve bilgileri kontrol hakkını içerir bir şekle dönüşmüştür. Bireylere hayatlarını diledikleri gibi düzenleme fırsatı sunan bir alan yaratma imkânı tanıyan özel yaşamın gizliliği hakkı, kişinin özerk bir birey olması açısından son derece önemlidir. Bu hak, başkaları ve devlet tarafından ihlal edilmemesi, saygı gösterilmesi gereken bir çeşit onursal duvar yaratmaktadır. Bireyin özel yaşamının gizliliği hakkı ile devletin güvenlik sağlama görevi arasında çatışmada güvenlik her zaman öncelik taşıyacaksa özel hayatın gizliliği ve kişisel verilerin korunması haklarında söz etmenin çok fazla bir anlamı kalmamaktadır.

90. Madde Yönünden

Bu maddeye göre, 'Usulüne göre yürürlüğe konulmuş milletlerarası antlaşmalar kanun hükmündedir. Usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası andlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası andlaşma hükümleri esas alınır.' İptal konusu düzenleme, ilk bölümde de anlatıldığı üzere, Türkiye'nin taraf olduğu Uluslararası Medeni ve Siyasi Haklar Sözleşmesinin 17. maddesi ile Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesini ihlal ettiğinden, Anayasa'nın 90. maddesine de aykırıdır.

Sonuç

İptali istenen düzenleme, Anayasanın, temel hak ve hürriyetlerin demokratik toplum düzeninin gereklerine aykırı olarak sınırlanamayacağını belirten 13., herkesin maddi ve manevi kişiliğini geliştirme hakkına sahip olmasını güvence altına alan 17., özel hayatın gizliliğini ve kişisel verilerin korunmasını düzenleyen 20., ve temel hak ve özgürlüklere ilişkin milletlerarası antlaşma hükümlerini anayasal güvence altına alan 90. maddelerine aykırı olduğundan çoğunluk görüşüne muhalif kalmıştır.

Üye - Engin YILDIRIM

Kaynakça

Atak, Songül, (2010), 'Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler', Türkiye Barolar Birliği Dergisi, sayı 87, ss: 90-120.

Avrupa Konseyi, (2008), Protecting the Right to Privacy in the Fight against Terrorism, CommDH/IssuePaper(2008), [https://wcd.coe.int/com.instranet.InstraServlet?Index=no&command=com.instranet.](https://wcd.coe.int/com.instranet.InstraServlet?Index=no&command=com.instranet.CmdBlobGet&InstranetImage=1416463&SecMode=1&DocId=1426260&Usage=2)

erişim tarihi 15.11.2012

Avrupa Konseyi, (2002), İnsan Hakları ve Terörle Mücadele Hakkında İlkeler, http://www.jp.coe.int/upload/90_guidelineshumanrights_terrorism_tur.pdf, erişim tarihi 15.11.2012.

Dragu, Tiberiu, (2011), 'Is There a Tradeoff between Security and Liberty' Executive Bias, Privacy Protections and Terrorism Preventions', American Political Science Review, 105(1): 64-78.

Hein van Kempen, Piet (2013), 'Four Concepts of Security-A Human Rights Perspective', Human Rights Law Review, 13: 1-23.

Küzeci, Elif, (2010), Kişisel Verilerin Korunması, Ankara: Turhan Kitabevi.

Locke, John, (2010), Hükümet Üstüne İkinci Tez, çev. Aysel Doğan, İzmir: İlya Yayınevi.

Michaelson, Christopher, (2006), Balancing Civil Liberties against National Security: A Critique of Counterterrorism Rhetoric', University of New South Wales Law Journal, 29 (1): 1-21.

National Research Council (2008), Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment, Executive Summary http://www.nap.edu/catalog.php?record_id=12452, erişim tarihi, 19.11.2012.

Posner, Richard, (2006), *Not a Suicide Pact: The Constitution in a Time of National Emergency*, Oxford: Oxford University Press.

Posner, Eric A. ve Adrian, Vermeule (2007), *Terror in the Balance: Security, Liberty and the Courts*, New York: Oxford University Press.

Scheinin, Martin, (2009), *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, Human Rights Council, UN, <http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf>, erişim tarihi, 19.11.2012.

Schwartz, Paul, M (2011), 'Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the State and New Technology', *William and Mary Law Review*, 53: 351-387.

Solove, J. Daniel (2011), *Nothing to Hide: The False Tradeoff between Privacy and Security*, New Haven: Yale University Press.

Solove, J. Daniel, (2008), 'Data Mining and the Security-Liberty Debate', *The University of Chicago Law Review*, 75: 343-362.

Sottiaux, Stefan, (2008), *Terrorism and the Limitation of the Rights: The ECHR and the US Constitution*, Oxford: Hart Publishing.

Şimşek, Oğuz, (2008), *Anayasa Hukukunda Kişisel Verilerin Korunması*, İstanbul: Beta.

Vermeule, Adrian, (2011), 'Security and Liberty: Critiques of Tradeoff Thesis', *Harvard Law School Public Law and Legal Theory Working Paper Series*, paper no: 11-19 <http://ssrn.com/abstract=1888334> s. 2, erişim tarihi, 2.11.2012.

Waldron, Jeremy, (2007), 'Safety and Security', *Nebraska Law Review* 85(1): 455-507.

Waldron Jeremy, (2003), 'Security and Liberty: The Image of Balance', *The Journal of Political Philosophy*, 11 (2): 191-210.

Young, Raymond, (2008) 'Germany: Shooting Down Aircraft and Analysing Computer Data', *International Journal of Constitutional Law*, 6(2): 331-348.

MUHALEFET ŞERHİ

17.2.2010 günlü, 5952 sayılı Kamu Düzeni ve Güvenliği Müsteşarlığının Teşkilat ve Görevleri Hakkında Kanun'un:

1- 1. maddesinin (1) numaralı fıkrasının '... terörle mücadeleye ilişkin politika ve stratejileri geliştirmek ve bu konuda ilgili kurum ve kuruluşlar arasında koordinasyonu sağlamak üzere İçişleri Bakanlığına bağlı ...' bölümünde yer alan '... İçişleri Bakanlığına bağlı ...' ibaresi;

2- 3. maddesinin (1) numaralı fıkrasında yer alan '... İçişleri Bakanlığına bağlı ...' ibaresi;

3- 4. maddesinin (2) numaralı fıkrasının, birinci cümlesinde yer alan '... İçişleri Bakanının ...', ikinci cümlesinde yer alan '... İçişleri Bakanının ...' ve üçüncü cümlesinde yer alan '... İçişleri Bakanı ...' ibareleri;

4- 5. maddesinin (2) numaralı fıkrasında yer alan '... Bakanın onayı ile özel ihtisas ve araştırma komisyonları ...' ibaresindeki '... Bakanın ...' sözcüğü;

5- 10. maddesinin (1) numaralı fıkrasının (c) bendinin '... Bakan onayı ile en çok on Müsteşarlık Müşaviri pozisyon unvanıyla sözleşmeli personel çalıştırılabilir. Personelin sözleşme usul ve esasları Müsteşarlıkça tespit edilir ve bu Kanuna ekli (2) sayılı cetvelde belirlenen taban ve tavan ücretleri arasında kalmak üzere Müsteşarın teklifi ve Bakan onayı ile aylık brüt sözleşme ücreti ödenir. Ayrıca Müsteşarlıkta sözleşmeli personel olarak istihdam edilenler için belirlenen usul ve esaslar çerçevesinde ikramiye ve teşvik ikramiyesi ödenebilir. Bu statüde çalıştırılma, sözleşme bitiminde kamu kurum ve kuruluşlarında herhangi bir pozisyon, kadro veya statüde çalışma açısından kazanılmış hak teşkil etmez.' bölümünde yer alan 'Bakan ...' sözcüğü ile yine aynı bölümde yer alan '... ve bu Kanuna ekli (2) sayılı cetvelde belirlenen taban ve tavan ücretleri arasında kalmak üzere Müsteşarın teklifi ve Bakan onayı ile aylık brüt sözleşme ücreti ödenir. Ayrıca Müsteşarlıkta sözleşmeli personel olarak istihdam edilenler için belirlenen usul ve esaslar çerçevesinde ikramiye ve teşvik ikramiyesi ödenebilir. ...' ibaresi;

6- 13. maddesinin (2) numaralı fıkrasında yer alan 'Bakan ...' sözcüğünün;

643 ve 666 sayılı Kanun Hükmünde Kararnameler ile yürürlükten kaldırıldığından sözü geçen kuralların iptali istemi hakkında 'karar verilmesine yer olmadığına' karar verilmiştir.

Anayasa Mahkemesi'ne yapılan iptal başvurularının konusunu oluşturan kuralların tümüyle yasal değişikliğe uğramaları halinde, söz konusu başvurular hakkında karar verilmesinde hukuki yarar bulunmamaktadır. Ancak; yapılan değişikliğin dava konusu tümce, ibare veya sözcüklere ilişkin olması durumunda incelemenin sürdürülerek sonuca gidilmesi dolayısıyla istemle ilgili karar verilmesi gerekir. Aksi takdirde dava konusu kurallarda esasa müessir olmayacak şekilde yapılacak ekleme ve çıkarma şeklindeki değişiklikler anayasal denetimin dışında kalmasına neden olacağı, bu

durumun da Anayasa Yargısının amacı ve işlevine ters düşeceğinden çoğunluk görüşüne katılmıyorum.

Üye - Nuri NECİPOĞLU

* Türkiye, bu Sözleşmeyi imzalamakla birlikte, 'Kişisel Verilerin Korunması Hakkında Kanun', henüz yasalaşmadığından Sözleşme'nin ilgili hükmü gereğince taraf olmamıştır.

Anayasa Mahkemesi - 5429 sayılı Türkiye İstatistik Kanunu (2010/12)

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2010/12

Karar Sayısı: 2011/135

Karar Günü: 12.10.2011

R.G. Tarih-Sayı: 28.12.2011-28156

İTİRAZ YOLUNA BAŞVURANLAR:

1- Selçuk Sulh Ceza Mahkemesi (E.2010/12)

2- Eskişehir 5. Sulh Ceza Mahkemesi (E.2010/76)

İTİRAZIN KONUSU: 10.11.2005 günlü, 5429 sayılı Türkiye İstatistik Kanunu'nun;

1) 25.11.2008 günlü, 5813 sayılı Yasa'nın 1. maddesiyle yeniden düzenlenen 8. maddesinin,

2) 54. maddesinin ikinci fıkrasının,

Anayasa'nın Başlangıç'ı ile 2., 5., 10., 11., 12., 13., 17., 19., 20., 24. ve 25. maddelerine aykırılığı savıyla iptali istemidir.

I- OLAY

Türkiye İstatistik Kurumu Başkanlığının ilgili Bölge Müdürlükleri tarafından verilen idari para cezalarına karşı yapılan itirazları incelemekte olan Mahkemeler, itiraz konusu kuralların iptali için başvurmuşlardır.

III- YASA METİNLERİ

A- İtiraz Konusu Yasa Kuralları

10.11.2005 günlü, 5429 sayılı Kanun'un 25.11.2008 günlü, 5813 sayılı Kanun'un 1. maddesiyle yeniden düzenlenen 8. maddesi ile 54. maddenin itiraz konusu kuralı da içeren ikinci fıkrası şöyledir:

'MADDE 8.- İstatistikî birimler, ülkenin ekonomi, sosyal, demografi, kültür, çevre, bilim, teknoloji ve ihtiyaç duyulan diğer alanlardaki resmi istatistikleri üretmek üzere, Anayasa'da belirlenen temel haklar ve ödevler çerçevesinde, kendilerinden istenen veri veya bilgileri, Başkanlığın belirleyeceği şekil, süre ve standartlarda eksiksiz ve doğru olarak ücretsiz vermekle yükümlüdür.

MADDE 54.- '

Başkanlık veya kurum ve kuruluşlar tarafından Program kapsamında istenen bilgileri, geçerli bir mazereti olmaksızın belirlenen şekil ve sürede vermeyen veya eksik veya hatalı verenler, bir kereye mahsus olmak üzere uyarılarak yedi gün içerisinde bilgileri vermeleri veya eksik ve hataları gidermeleri istenir. Bu uyarıya rağmen, bilgileri hiç vermeyen veya talep edildiği hâlde eksikleri gidermeyen ve hataları düzeltmeyen gerçek kişiler veya özel hukuk tüzel kişilerinin organ ve temsilcileri hakkında, fiilin;

- a) Hanehalkı veya bireylerle yapılan araştırmalarda işlenmesi durumunda beşyüz Yeni Türk Lirası,
- b) Hane halkı veya bireyler dışında kalan diğer istatistikî birimlerle yapılan araştırmalarda işlenmesi durumunda binbeşyüz Yeni Türk Lirası,
- c) Sayımlarda işlenmesi durumunda ikibin Yeni Türk Lirası,

İdarî para cezası uygulanır.

"

B- Dayanılan Anayasa Kuralları

Başvuru kararlarında Anayasa'nın Başlangıç hükümleri ile 2., 5., 10., 11., 12., 13., 17., 19., 20., 24. ve 25. maddelerine dayanılmıştır.

IV- İLK İNCELEME

Anayasa Mahkemesi İçtüzüğü'nün 8. maddesi gereğince, E.2010/12 sayılı dosyanın 25.2.2010 gününde yapılan ilk inceleme toplantısında dosyada eksiklik bulunmadığından işin esasının incelenmesine OYBİRLİĞİYLE karar verilmiştir.

E.2010/76 sayılı dosyanın 22.9.2010 gününde yapılan ilk inceleme toplantısında öncelikle itiraz konusu 10.11.2005 günlü, 5429 sayılı Türkiye İstatistik Kanunu'nun 54. maddesinin ikinci fıkrasının davada uygulanacak kural niteliğinde olup olmadığı sorunu ele alınmıştır.

Anayasa'nın 152. ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 40. maddesine göre, bir davaya bakmakta olan mahkeme, o dava sebebiyle uygulanacak bir kanunun veya kanun hükmünde kararnamenin hükümlerini Anayasa'ya aykırı görürse veya taraflardan birinin ileri sürdüğü aykırılık savının ciddi olduğu kanısına varırsa, bu hükmün iptali için Anayasa Mahkemesi'ne başvurmaya yetkilidir. Ancak, bu kurallar uyarınca bir mahkemenin Anayasa Mahkemesi'ne başvurabilmesi için, elinde yöntemince açılmış ve mahkemenin görevine giren bir davanın bulunması ve iptali istenen kuralın o davada uygulanacak olması gerekir.

Uygulanacak yasa kuralları, bakılmakta olan davayı yürütmeye, uyuşmazlığı çözmeye, davayı sona erdirmeye veya kararın dayanağını oluşturmaya yarayacak kurallardır.

İtiraz konusu 54. maddenin ikinci fıkrasında Türkiye İstatistik Kurumu Başkanlığı veya kurum ve kuruluşlar tarafından program kapsamında istenen bilgileri, geçerli bir mazereti olmaksızın belirlenen şekil ve sürede vermeyen veya eksik veya hatalı verenlerin uyarılmalarına rağmen bilgileri vermemekte ya da eksikleri gidermemekte veya hataları düzeltmemekte ısrar etmeleri halinde idari para cezası uygulanması düzenlenmektedir. Söz konusu fıkrada bilgi verme yükümlülüğünü yerine getirmeyenlere uygulanacak idari para cezaları üç bent halinde düzenlenmiştir. Buna göre, (a) bendinde fiilin hane halkı veya bireylerle yapılan araştırmalarda, (b) bendinde hane halkı veya bireyler dışında kalan diğer istatistikî birimlerle yapılan araştırmalarda, (c) bendinde ise sayımlarda işlenmesi durumunda uygulanacak idari para cezaları öngörülmektedir.

İtiraz yoluna başvuran Mahkemenin bakmakta olduğu itiraza konu olan idari para cezası '2009 Hane Halkı Bütçe Anketi'nin uygulanması sırasında istenilen bilgilerin verilmemesi nedeniyle verilmiştir. 5429 sayılı Kanun'un 54. maddesinin ikinci fıkrasının (b) ve (c) bentlerinin itiraz başvurusunda bulunan Mahkeme'nin bakmakta olduğu davada uygulanma olanağı bulunmamaktadır. Bu nedenle (b) ve (c) bentlerine ilişkin başvurunun Mahkemenin yetkisizliği nedeniyle REDDİNE, itiraz başvurusunun diğer kısımları hakkında ise dosyada eksiklik bulunmadığından işin esasının incelenmesine OYBİRLİĞİYLE karar verilmiştir.

V- BİRLEŞTİRME KARARI

10.11.2005 günlü, 5429 sayılı Türkiye İstatistik Kanunu'nun 54. maddesinin ikinci fıkrasının (a) bendinin iptaline karar verilmesi istemiyle yapılan itiraz başvurusuna ilişkin E.2010/76 sayılı davanın, aralarındaki hukuki irtibat nedeniyle 2010/12 esas sayılı dava ile birleştirilmesine, esasının kapatılmasına, esas incelemenin 2010/12 esas sayılı dosya üzerinden yürütülmesine, 22.9.2010 gününde OYBİRLİĞİYLE karar verilmiştir.

VI- ESASIN İNCELENMESİ

Başvuru kararları ve ekleri, işin esasına ilişkin rapor, itiraz konusu kurallar, dayanılan Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

Başvuru kararlarında, 5429 sayılı Kanun'un 8. maddesinde yer alan, istatistikî birimlerin kendilerinden istenen veri veya bilgileri, Başkanlığın belirleyeceği şekil, süre ve standartlarda eksiksiz, doğru ve ücretsiz olarak vermekle yükümlü oldukları kuralı ile bu yükümlülüğe

uymayanların idari para cezasıyla cezalandırılacaklarına ilişkin 54. maddesinin ikinci fıkrasının (a) bendi hükmünün eşitlik ilkesi, temel hak ve hürriyetlerin niteliği, kişi hürriyeti ve güvenliği, özel hayatın gizliliği, düşünce ve kanaat hürriyetine ilişkin düzenlemelere aykırı olduğu; temel hak ve hürriyetlerin kanunla sınırlanabileceği ve bu sınırlamanın demokratik toplum düzeninin gereklerine aykırı olamayacağı, kişilerin her ne sebeple ve amaçla olursa olsun düşünce ve kanaatlerini açıklamaya zorlanması ve buna uymayanların idari yaptırımla karşı karşıya bırakılmasının hukuk devleti ilkesine aykırılık teşkil edeceği gerekçesiyle itiraz konusu kuralların, Anayasa'nın Başlangıç'ı ile 2., 5., 10., 11., 12., 13., 17., 19., 20., 24. ve 25. maddelerine aykırı olduğu ileri sürülmüştür.

5429 sayılı Kanun'un 8. maddesinde Türkiye İstatistik Kurumu Başkanlığı tarafından istenen veri veya bilgileri istatistikî birimlerin süresinde, eksiksiz, doğru ve ücretsiz olarak verme yükümlülüğü düzenlenmiştir. Kanun'un 2. maddesinin (h) bendine göre istatistikî birim, yapılan sayım veya örnekleme çalışmalarına konu olan, hakkında veri toplanacak gerçek ve tüzel kişiler ile kurum ve kuruluşları ifade etmektedir.

Türkiye İstatistik Kurumu ülkenin ekonomik, sosyal, kültürel ve demografik yapısına ilişkin resmi istatistikleri üretmekle sorumlu bir kuruluştur. İstatistik, verilerin toplanması, düzenlenmesi ve uygun yöntemlerle analiz edilerek sonuçların yorumlanması olarak tanımlanmaktadır. İstatistikten söz edebilmek için önce 'veri'ye ihtiyaç vardır. Veriler, araştırma yapılacak konu ile ilgili bilinen veya herhangi bir kaynaktan doğrudan ya da dolaylı olarak elde edilen bilgilerdir. Resmi istatistikler için ihtiyaç duyulan veriler ülkemizde iki yolla toplanmaktadır. Bunlardan ilki, kamu kurum ve kuruluşlarının görevleri gereği tuttıkları idari kayıtlardan verilerin derlenmesi, diğeri ise ihtiyaç duyulan konularda istatistikî birimler ile görüşülerek bilgi toplanmasını içeren sayım ve araştırmaların yapılmasıdır. Resmî istatistikler ulusal planların yapılması ve bu planlara dayalı politikaların oluşturulmasında kullanılan temel göstergeler olduğundan üretilen resmî istatistiklerin doğru, kaliteli, güvenilir, karşılaştırılabilir, güncel, tarafsız ve uluslararası standartlara uygun olması hayati önem taşımaktadır. Resmî istatistiklerin dayanağını oluşturan veri ve bilgilerin ilgililer tarafından doğru, eksiksiz ve zamanında verilmemesi halinde ihtiyaç duyulan doğru ve güvenilir istatistiklerin üretilmesi mümkün olamayacaktır.

İtiraz konusu 8. madde hükmüyle sayım ve örnekleme çalışmalarına konu olan istatistikî birimlere, ülkenin ekonomi, sosyal, demografi, kültür, çevre, bilim, teknoloji ve ihtiyaç duyulan diğer alanlardaki resmi istatistikleri üretmek üzere, Anayasa'da belirlenen temel haklar ve ödevler çerçevesinde, kendilerinden istenen veri veya bilgileri, Başkanlığın belirleyeceği şekil, süre ve

standartlarda eksiksiz ve doğru olarak ücretsiz verme yükümlülüğü getirilmiş, bu yükümlülüğe uymayanların da 54. maddenin ikinci fıkrasında gösterilen biçimde idarî para cezasıyla cezalandırılması öngörülmüştür.

Anayasa'nın 2. maddesinde belirtilen hukuk devleti, eylem ve işlemleri hukuka uygun, insan haklarına saygılı, bu hak ve özgürlükleri koruyup güçlendiren, her alanda adaletli bir hukuk düzeni kurup bunu geliştirerek sürdüren, Anayasa'ya aykırı durum ve tutumlardan kaçınan, Anayasa ve hukukun üstün kurallarıyla kendini bağlı sayan, yargı denetimine açık devlettir.

Anayasa'nın 10. maddesinde yer verilen eşitlik ilkesi de hukuksal durumları aynı olanlar için söz konusudur. Bu ilke ile eylemli değil, hukuksal eşitlik öngörülmüştür. Eşitlik ilkesinin amacı, aynı durumda bulunan kişilerin yasalar karşısında aynı işleme bağlı tutulmalarını sağlamak, ayırım yapılmasını ve ayrıcalık tanınmasını önlemektir. Bu ilkeyle, aynı durumda bulunan kimi kişi ve topluluklara ayrı kurallar uygulanarak yasa karşısında eşitliğin ihlali yasaklanmıştır. Yasa önünde eşitlik, herkesin her yönden aynı kurallara bağlı tutulacağı anlamına gelmez. Durumlarındaki özellikler, kimi kişiler ya da topluluklar için değişik kuralları ve uygulamaları gerektirebilir. Aynı hukuksal durumlar aynı, ayrı hukuksal durumlar farklı kurallara bağlı tutulursa Anayasa'da öngörülen eşitlik ilkesi zedelenmez.

İtiraz konusu kurallarla istatistiklerin kamu yararı için önemi dikkate alınarak bireylere mecburi ve ücretsiz kamusal bir külfet yüklenmiştir. Karşılaştırmalı hukukta da bazı ülkelerde bireylere istatistik amaçlı bilgi verme yükümlülüğü getirildiği görülmektedir. Modern bir devlette kamu hizmetlerinin planlanması ve kamu güvenliğinin sağlanabilmesi için bireylerin kendileriyle ilgili pek çok bilgiyi kamu otoritelerine verme yükümlülüğü bulunmaktadır. Bu bilgilerin istatistik amacıyla toplanmış olması bilgi toplamayı kendiliğinden Anayasa'ya aykırı hale getirmez.

5429 sayılı Kanun'un 8. maddesinin eski düzenlemesini Anayasa Mahkemesi 20.3.2008 tarih ve E.2006/167, K.2008/86 sayılı kararıyla, hiçbir sınırlama öngörmeksizin istatistikî birimlere istenilen bilgileri verme yükümlülüğü getirmesi nedeniyle Anayasa'nın 20. ve 25. maddelerine aykırı bularak iptal etmiştir. Bu iptal kararından sonra 5813 sayılı Kanun'la getirilen düzenleme ile 8. maddede bilgi verme yükümlülüğünün sınırı Anayasa'da belirlenen temel hakların ve ödevlerin ihlal edilmemesi olarak belirlenmiştir. Anayasa'nın 20. maddesinde herkesin özel hayatına ve aile yaşayışına saygı gösterilmesini isteme hakkına sahip olduğu; 24. maddesinde kimsenin dini inanç ve kanaatlerini açıklamaya zorlanamayacağı; 25. maddesinde de herkesin düşünce ve kanaat özgürlüğüne sahip olduğu, her ne sebep ve amaçla olursa olsun kimsenin düşünce ve kanaatlerini açıklamaya zorlanamayacağı hüküm altına alınmıştır. Bunlar gibi, Anayasanın diğer maddelerinde güvence

altına alınan hak ve ödevler gözetilerek bilgi talep edilebilecektir. İstenilen bilgilerin bu nitelikte olduğunu düşünen istatistikî birimler, nedenini açıklayarak bilgi vermekten kaçınabileceği gibi haklarında idari para cezası uygulanması halinde buna itiraz ederek istenilen bilginin temel haklarını ihlal edecek nitelikte olduğunu mahkemeler önünde de ileri sürebilirler.

5429 sayılı Kanun'un 54. maddesinin ikinci fıkrasında, istatistikî birimlerin kendilerinden istenen bilgileri geçerli bir mazereti olmaksızın belirlenen şekil ve sürede, eksiksiz ve hatasız olarak vermek zorunluluğuna uyulmaması idari para cezası yaptırımına bağlanmıştır. Bu durumda dava konusu iki hüküm birlikte değerlendirildiğinde bireylerin temel haklarının korunmasının idari ve adli makamların sorumluluğuna bırakıldığı görülmektedir. İdari makamlar bireyin temel haklarını ihlal edecek şekilde bilgi talep etmeme yükümlülüğündedirler. İdari makamların bu ödevini yerine getirmemesi halinde istatistikî birimler haklarını yargı makamları önünde arayabileceklerdir. Bu durumda itiraz konusu kurallarla bireyin hakları ile kamu yararı arasında makul bir denge kurulduğu ve bireylerin haklarına ölçsüz bir müdahaleye izin verilmediği anlaşıldığından Anayasanın 2. maddesindeki hukuk devleti ilkesine aykırılık görülmemiştir.

Diğer taraftan istatistik biliminin doğası gereği bilimsel yöntemlerle tespit edilen ilgili tüm kişi ve kurumlardan ayırım yapılmadan bilgi istenebileceğinden kuralın Anayasa'nın 10. maddesinde öngörülen eşitlik ilkesine aykırı olduğu söylenemez.

Açıklanan nedenlerle itiraz konusu kurallar Anayasa'nın 2., 10., 20., 24. ve 25. maddelerine aykırı değildir iptal isteminin reddi gerekir. Bu sonuca 8. madde açısından Osman Alifeyyaz PAKSÜT, Serruh KALELİ ve Erdal TERCAN; 54. maddenin ikinci fıkrasının (a) bendi açısından Osman Alifeyyaz PAKSÜT katılmamışlardır.

Konunun Anayasa'nın Başlangıcı ile 5., 11., 12., 13., 17. ve 19. maddeleriyle ilgisi görülmemiştir.

VII- SONUÇ

10.11.2005 günlü, 5429 sayılı Türkiye İstatistik Kanunu'nun;

1- 25.11.2008 günlü, 5813 sayılı Kanun'un 1. maddesiyle yeniden düzenlenen 8. maddesinin Anayasa'ya aykırı olmadığına ve itirazın REDDİNE, Osman Alifeyyaz PAKSÜT, Serruh KALELİ ile Erdal TERCAN'nın karşıoyları ve OYÇOKLUĞUYLA,

2- 54. maddesinin ikinci fıkrasının (a) bendinin Anayasa'ya aykırı olmadığına ve itirazın REDDİNE, Osman Alifeyyaz PAKSÜT'ün karşıoyu ve OYÇOKLUĞUYLA,

12.10.2011 gününde karar verildi.

Başkan - Haşim KILIÇ

Başkanvekili - Osman Alifeyyaz PAKSÜT

Başkanvekili -Serruh KALELİ

Üye: Fulya KANTARCIOĞLU; Mehmet ERTEN; Fettah OTO; Serdar ÖZGÜLDÜR; Recep KÖMÜRCÜ; Alparslan ALTAN; Burhan ÜSTÜN; Engin YILDIRIM; Nuri NECİPOĞLU; Hicabi DURSUN; Celal Mümtaz AKINCI; Erdal TERCAN

KARŞIOY YAZISI

İtiraz konusu 8. maddeyle, daha önce Anayasa Mahkemesi'nin E:2006/167, K:2008/86 sayılı kararıyla iptal edilen aynı mealdeki kural yeniden düzenlenmiş ve iptal gerekçesindeki hususları karşılamak amacıyla maddeye 'Anayasada belirtilen temel haklar ve ödevler çerçevesinde' ibaresi eklenerek, bilgi verme yükümlülüğüne bir sınır getirilmeye çalışılmıştır.

Buna göre vatandaşlar (istatistiki birimler) istenilen bilgilerin verilmesinin Anayasa'da belirtilen temel haklarını ihlal edeceği kanaatinde iseler bilgi vermeyebilecekler ve bundan dolayı haklarında idari para cezası uygulanmayacaktır.

Anayasa'nın 2. maddesinde hukuk devleti ilkesi belirtilmiştir. Hukuk devletinin temel unsurlarından olan hukuk güvenliği, kişilerin idarece sürekli yaptırım tehdidi altında tutulmalarına izin vermez.

İtiraz konusu kural, toplumsal ve özel hayatın tüm alanlarını kapsayabilecek bilgi istemlerinden hangilerinin Anayasada belirtilen temel hakları ihlal edeceğini, hangilerinin ise verilmek zorunda olduğunu bir yandan idarenin, diğer yandan vatandaşların yorumuna bırakarak bu konuda belirsizlik yaratmaktadır. Maddeye eklenen 'Anayasada belirtilen temel haklar ve ödevler çerçevesinde' ibaresi malumun ilanı ve abesle iştiğal dışında somut bir güvence getirmemekte, Anayasa Mahkemesi'nin önceki iptal kararında açıklanan sakıncaları gidermemektedir. Yasa bu konuda istatistiki bilgi talep edilemeyecek alanları ve bunlara taalluk eden konuları açıkça belirtmiş veya bu konuda Anayasaya paralel bir çerçeve çizmiş olmadığından, iptal istemine konu olan kural uygulamada çok sayıda para cezasına ve bundan kaynaklanan uyuşmazlıklara neden olabilecek, haksız uygulama sonucu para cezasına uğrayan vatandaşlar yok yere dava açmak, avukat tutmak, harç ödemek gibi külfetlere maruz kalacaklardır. Bunun, hukuk güvenliği ilkesiyle bağdaşmadığı açıktır. Çağdaş hukuk devleti, idarenin hatalı uygulamalarının telafisi için gereken çabayı ve bundan

doğacak külfeti vatandaşına yükleyen değil, böyle durumlara olabildiğince az sebebiyet veren devlettir.

Bu nedenlerle Anayasa'nın 2. maddesine aykırı olan kuralın iptali gerekmektedir.

Kuralın Anayasaya aykırılığı, bunun yaptırımını olarak 54. maddede öngörülen idari para cezasını da vatandaşlar yönünden Anayasa'ya aykırı hale getirdiğinden 54. maddenin ikinci fıkrasının (a) bendinin de iptali gerekir.

Başkanvekili - Osman Alifeyyaz PAKSÜT

KARŞIOY

Mahkememizin 5429 sayılı Türkiye İstatistik Kanunu'nun 8. ve 54. maddesinin ikinci fıkrasının b bendinin Anayasa'ya aykırılığı istemi üzerine vermiş bulunduğu 2006/167 Esas, 2008/86 Karar sayılı kararında;

'İstatistiki birimler, kendilerinden istenen veri veya bilgileri başkanlığın belirleyeceği şekil süre ve standartlarda eksiksiz ve doğru olarak ücretsiz vermekle yükümlüdür.' şeklindeki 8. madde düzenlemesini ve dolayısıyla buna ceza tanzim eden 54. maddenin ikinci fıkrasını Anayasa'ya aykırı bulup iptal ederken özetle ve kısaca; Madde de açıklayıcı bir düzenleme bulunmadığını, istenecek bilgilerin kapsam ya da sınırlarının belirsizliği ile, temel haklara ve özgürlüklere müdahale niteliği kapsamında olduğu anlaşıldığından özel yaşamın gizliliği ve düşünce kanaat açıklaması sonucu doğurabilecek bu belirsizliğin bireyin idareye karşı korumasız bırakması ile Anayasa'nın özel hayatın gizliliği ve düşünce ve kanaat özgürlüğünü koruyan hükümlerine aykırılığı nedeniyle iptal ettiği görülmektedir.

Aynı kural 25.11.2008 tarihinde bu kez istatistiki birimler ülkenin "ihtiyaç duyulan alanlardaki resmi istatistikleri üretmek üzere yeni alan belirterek ve de Anayasa'da belirtilen temel hak ve ödevler çerçevesinde kendilerinden istenen veri veya bilgileri" ücretsiz vermekle yükümlüdür diyerek yani sınırlama da yaparak Mahkemenin iptal kararına uygun bir düzenleme yapıldığı kanaati ile tekrar yasalaştırılmıştır.

Anayasa'nın 2. kısmını oluşturan temel hak ve ödevler, 2. bölümünde mahkemenin önceki iptal kararında değinip iptale esas aldığı özel hayatın gizliliği ve düşünce ve kanaat hürriyetini içerdiği gibi 3. bölümünde sosyal ve ekonomik hak ve ödevleri 4. bölümünde de siyasal hak ve ödevleri kapsama almaktadır.

İptali istenen kural da, önceki iptal edilen kurala 'Anayasa'da belirlenen temel haklar ve ödevler çerçevesinde' diye eklenen yeni ibarenin; bu hali ile, kurala bir sınırlama alanı mı yoksa genişleme alanı mı yarattığı anlaşılammıştır. Türk Dil Kurumu yayını Türkçe sözlük 2009 basımında 'çerçeve' kelimesi bir konunun bir düşünce alanının sınırları veya bu sınırlar içindeki alanı' ifade eder demektedir. O halde 8. madde kuralı, 'temel hak ve ödevler çerçevesinde' diyerek bu kapsama giren her konuda yani Anayasa'nın 12. ve 74. maddeleri dahil arasındaki her konuda, Türkiye İstatistik Kurumu'nca bilgi talep edebilme hakkını yaratıp cevap verme yükümlülük ve sınırlarını bu şekilde belirlediği söylenebilecektir.

Bu da hali ile iptali istenen yeni düzenlemeden, önceki iptal kararımıza esas, istenen bilgilerin temel hak ve özgürlüklere müdahale ve özel yaşamın gizliliği ve kanaat açıklaması zorunluluğuna neden OLMAYACAĞININ anlaşılması mümkün olmadığı gibi soruların bu kapsamda sunulmasına da olanak verdiğinin anlaşılması mümkün gözükmemektedir.

Bu lafzî yorum hataları getirebilecek belirsizlik içeren ve önceki iptal kararını adeta genişleten düzenlemeye ilişkin Mahkememiz çoğunluk görüşüne, bu yönüyle katılmak mümkün olmamıştır.

Kamu güvenliğinin sağlanması, kamu hizmetlerinin planlanması, doğru ve güvenilir istatistik bilgilerin üretilmesi ve bu sayede planlı kalkınmanın, sosyal, adil hukuk devletinin, maddi ve manevi varlığı gelişmiş toplum yaratılmasının sağlanması için devletin veri toplaması, bilgi edinilmesi kaçınılmazdır. Sorulana külfet gibi gelebilecek bu yükümlülükten herkesin istifade payının da olabileceği muhakkaktır.

Devleti bu görevini yaparken bireye nesne ya da araç gibi muamele etmemeli, Anayasa'nın 5. maddesi ile tanınan varlığını, manevi kişiliğini serbestçe ve sorumlu bir şekilde geliştirecek bir alan bırakmalı ve müdahil olmamalıdır.

Düzenlemenin açıkça sayılarak ilgili 'temel hak ve özgürlük alanlarını İHLAL ETMEKSİZİN istenilen veri ve bilgiler toplanır' demesi gerekeceği yerde, temel hak ve ödevler çerçevesinde soru sorar cevap alırım denebileceğinin anlaşılması metodolojik yorum hatası yaratacaktır. Yasal düzenlemelerde lafzî ve amaçsal yorumlar şüphe götürmeyecek netlikte birbirlerine yakın olup örtüşmelidir. Yasa'nın gerekçesinde de temel hakları ihlal etmeme kasdının anlaşılabilceğine ilişkin bilgiye ulaşılammıştır.

Mukayeseli hukuka baktığımızda devletlerin gerçek ya da tüzel kişilerden kamusal yarar içeriği ile bilgi almasına bir engel gözükmemekte, ancak alınacak bilginin öncelikli hangi amaçla alındığı konusunda bilgilendirme yapılması, bilgilerin işlenmesi ve kullanılması sırasında kişisel bilgilerin saklanması, transferi gibi konularda bireye tanınan rıza, yetki hakları ve doğal olarak AİHS'nin 8.

maddesinde yer alan özel ve aile hayatına saygı hakkının getirdiği güvenceninde bir koruma alanı yarattığı görülmektedir.

Kaldı ki Anayasamızın 5982 sayılı Yasa ile değişik 20. maddesi de kişisel verilerin korunmasını, silinmesini ve kişinin ancak AÇIK RIZASI ile işlenebileceğini ifade etmektedir. Bu düzenleme ile bir veri tablosuna işlenmesine izin vermediği bir cevabın sorusunun sorulabilirliği, sınırlama alanı dışında dahi olsa hukukiliği tartışılabilir durumdadır.

Türkiye İstatistik Kanunu 13. maddesi topladığı verinin gizli olabileceğini de kabul etmekte ama gizliliği, bireyin korunan özelinden değil, kendi perspektifinden bakarak bilginin istatistiksel sonuçlarına atıfta bulunarak yapmaktadır.

Gizli bilgilerin izinsiz, yetkisiz başkalarına ulaşması halinde olacaklar özel yaşamın korunması kapsamında değerlendirilemeyeceği gibi açık özgürlük ihlalleri yaratabilecektir.

Anayasamızın 3. bölümünde yer alan sosyal ve ekonomik hakların dahi nispeten günümüzde temel hak ve özgürlükler kapsamında değerlendirilmeye başladığı düşünüldüğünde, geniş bir yelpazede yer alan hak ve özgürlükler çerçevesinde denildiğinde hangi temel hakkın yasal bir sınırlama alanı içinde kaldığını belirlemek mümkün olmayabilecek neticede konu yargısal çözüm gerektirecek, birey karşılaştığı yaptırımı aşmak için hak aramaya zorlanacaktır. Kuralın anayasal doğruluk ilkelerine uygun olarak yasada yer alması gerekirken, ihlalin varlığı ya da yokluğunun denetimi mahkemelere yaptırılacaktır.

Özel ve aile hayatına müdahale kamu güvenliği ülkenin ekonomik refahı vb nedenlerle mümkün olacak ise de, bunun Anayasa'nın 13. maddesinde belirlenen sınırlar içinde olacağı tabiidir. Hak arama özgürlüğü bir temel hak olsa da, durup dururken soruya cevap vermeyen, eksik ya da hatalı verene suç işlemiş değerlendirmesi ile ceza verip kaldırmasının temini için yargı yoluna başvurmaya zorlamak, hukuk devleti ilkesi ile bağdaştırılmaz.

Kamu güvenliği ve planlı kalkınma verileri için istatistik bilgi ve veri toplamak amaçlandığında birey hakları ve kamu yararı arasında kurulacak bir dengenin varlığından söz edebilmek için, devlet önce gerekli bilgileri herkese açık, gizli olmayan özel ya da tüzel kişi kaynaklarından öğrenmeli ve edinilmesinde zorluk çekilen bazı hassas konularda da gönüllülük, rıza ya da ücret teklifi gibi usullerinin kullanılmasında anayasal engel bulunmamaktadır.

Kaldı ki, kamu yararı ve kamu düzeninin kurulması için ceza yargılamasında maddi gerçeğin bulunması yolunda tanığa kamusal görevi için ücret takdir edildiği de gözden uzak tutulmamalıdır.

İptali istenen kuralın, cevap verme ödevi yerine getirmeyenler yönünden muhatabı derhal ceza yaptırımını ile karşılamak yerine, öncelikle bireyin davranış düzenine ve iradesine izin verecek yapıda olup birey ile kamu yararı arasında denge kurmaması hukuk devleti ilkesine aykırılık içerir.

Kural ile, kamu gücü kullanarak amaca ulaşmada kullanılan yol, kamu düzeni için gerekli olsa da alternatifleri karşısında bu yolun EN ELVERİŞLİ yol olduğu söylenemeyeceği için kural Hukuk Devletinin belirlilik ilkesine tam uygunluk sağlamadığı, temel hak ve özgürlüklere orantısız müdahale içeriği taşıdığından Anayasa'nın 2. ve 20. maddesine aykırıdır.

Açıklanan nedenler ile çoğunluk görüşüne katılmamıştır.

Başkanvekili - Serruh KALELİ

Üye - Erdal TERCAN

ANAYASA MAHKEMESİ KARARI

Esas Sayısı: 2006/123

Karar Sayısı: 2009/43

Karar Günü: 5.3.2009

R.G. Tarih-Sayı: 02.06.2009-27246

İTİRAZ YOLUNA BAŞVURANLAR:

1- Genelkurmay Başkanlığı Askeri Mahkemesi (Esas Sayısı: 2006/123)

2- Karşıyaka 5. Asliye Ceza Mahkemesi (Esas Sayısı: 2006/132)

İTİRAZIN KONUSU: 26.9.2004 günlü, 5237 sayılı Türk Ceza Kanunu'nun 5377 sayılı Yasa'nın 27. maddesi ile değiştirilen 245 maddesinin (1) numaralı fıkrasının Anayasa'nın 2., 10. ve 11. maddelerine aykırılığı savıyla iptali istemidir

I- OLAY

İşlem sonrası hamili tarafından ATM cihazında unutulmuş banka kartını kullanarak kartın bağlı bulunduğu hesaptan para çektiği iddia olunan sanıkların, haksız olarak ele geçirdiği kredi kartını kullanmak suretiyle harcama yapan sanık hakkında açılan davalarda, itiraz konusu kuralın Anayasaya aykırı olduğu kanısına varan mahkemeler iptali için başvurmuşlardır.

III- YASA METİNLERİ

A- İtiraz Konusu Yasa Kuralı

5237 sayılı Türk Ceza Kanunu'nun 5377 sayılı Kanununun 27. maddesiyle değiştirilen 245. maddesinin (1) numaralı fıkrası şöyledir:

"(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır."

B- Dayanılan Anayasa Kuralları

Başvuru kararında Anayasa'nın 2., 10. ve 11. maddelerine dayanılmıştır.

IV- İLK İNCELEME

Anayasa Mahkemesi içtüzüğünün 8. maddesi gereğince yapılan ilk inceleme toplantılarında dosyalarda eksiklik bulunmadığından işin esasının incelenmesine karar verilmiştir.

V- BİRLEŞTİRME KARARI

26.9.2004 günlü, 5237 sayılı "Türk Ceza Kanunu"nun 5377 sayılı Yasa'nın 27. maddesi ile değiştirilen 245. maddesinin (1) numaralı fıkrasının iptali istemiyle yapılan itiraz başvurusuna ilişkin 2006/132 esas sayılı davanın, aralarındaki hukuki irtibat nedeniyle 2006/123 esas sayılı dava ile BİRLEŞTİRİLMESİNE, esasının kapatılmasına, esas incelemenin 2006/123 esas sayılı dosya üzerinden yürütülmesine, 27.9.2006 gününde OYBİRLİĞİYLE karar verilmiştir.

VI- ESASIN İNCELENMESİ

Başvuru kararları ve ekleri, işin esasına ilişkin rapor, itiraz konusu Yasa kuralı, dayanılan Anayasa kuralları ve bunların gerekçeleri ile diğer yasama belgeleri okunup incelendikten sonra gereği görüşülüp düşünüldü:

Başvuru kararlarında itiraz konusu kuralda öngörülen cezanın benzer nitelikteki suçların cezalarıyla kıyaslandığında fahiş olduğu, özellikle onlara uygulanabilecek etkin pişmanlık hükümlerinin fıkra açısından uygulanamamasının cezayı suçla orantısız hale getirdiği belirtilerek kuralın Anayasanın 2., 10. ve 11. maddelerine aykırı olduğu ileri sürülmüştür.

İtiraz konusu kuralla, başkasına ait bir banka veya kredi kartını her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimsenin, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlaması suç sayılmakta ve yaptırım olarak üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası öngörülmektedir. Fail hakkında hangi hallerde ceza verilmeyeceği, kuralın içinde yer aldığı maddenin dördüncü fıkrasında açıklanmakla birlikte, bunlar arasında etkin pişmanlığa ilişkin bir hüküm bulunmamaktadır. Başvuru tarihi itibarıyla, Türk Ceza Kanunu'nun 168. maddesindeki etkin pişmanlığa konu olabilecek suçlar arasında banka veya kredi kartlarının kötüye kullanılması suçları da yer almadığından, itiraz konusu kural uyarınca yargılanan sanığın cezasında etkin pişmanlık nedeniyle indirim yapılması mümkün olmamaktadır.

Anayasa'nın 2. maddesinde belirtilen hukuk devleti, insan haklarına dayanan, bu hak ve özgürlükleri koruyup güçlendiren, eylem ve işlemleri hukuka uygun olan, her alanda adaletli bir hukuk düzeni kurup bunu geliştirerek sürdüren, Anayasa'ya aykırı durum ve tutumlardan kaçınan, hukuku tüm devlet organlarına egemen kılan, Anayasa ve yasalarla kendini bağlı sayan, yargı denetimine açık,

Anayasa'nın ve yasaların üstünde yasakoyucunun da bozamayacağı temel hukuk ilkeleri bulunduğu bilincinde olan devlettir.

Anayasa'nın 10. maddesinde belirtilen eşitlik ilkesiyle, birbirinin aynı durumunda olanlara ayrı kuralların uygulanması, ayrıcalıklı kişi ve toplulukların yaratılması engellemektedir. Aynı durumda olanlar için farklı düzenleme eşitliğe aykırılık oluşturur. Anayasa'nın amaçladığı eşitlik, mutlak ve eylemli eşitlik değil hukuksal eşitliktir. Aynı hukuksal durumlar aynı, ayrı hukuksal durumlar ayrı kurallara bağlı tutulursa Anayasa'nın öngördüğü eşitlik ilkesi ihlal edilmiş olmaz. Kişisel nitelikleri ve durumları özdeş olanlar arasında, yasalara konulan kurallarla değişik uygulamalar yapılamaz.

Hukuk devletinde ceza siyasetinin gereği olarak yasakoyucu, Anayasanın ve ceza hukukunun temel ilkelerine bağlı kalmak koşuluyla, cezalandırmada güdülen amacı da gözeterek hangi eylemlerin suç sayılacağına, bunlara verilecek cezanın türü, miktarı, artırım ve indirim nedenleri ve oranları ile suçun takibine ve yargılama usulüne ilişkin koşullar öngörebilir.

Suç sayılan eylemler arasında benzerlikler olduğu gibi farklılıklar da bulunabilir. Kimi benzerliklere rağmen eylemin toplumda yarattığı infial, kişiler üzerinde oluşturduğu tehlike, işlenme oranındaki artış ve azalma gibi faktörlere bağlı olarak daha ağır cezayla yaptırıma bağlanması veya bu sonucu doğuracak biçimde indirim nedenlerine yer verilmemesi yasa koyucunun takdirindedir.

Banka ve kredi kartlarının hukuka aykırı olarak kullanılması suretiyle çıkar sağlayanlar hakkında üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası öngören kurala, Türk Ceza Kanunu'nun bilişim alanında suçlara ilişkin bölümünde yer verilmiştir. Bundan, kartın bağlı bulunduğu hesap sahibinin malvarlığı yanında kişisel verilerinin de hukuki koruma kapsamında olduğu anlaşılmaktadır. Bu durumda, kuralın salt malvarlığı aleyhine işlenen suçlara benzemesine rağmen, onlara uygulanan etkin pişmanlık hükümleri içermemesi nedeniyle eşitliğe aykırı olduğu sonucu çıkarılamaz. Cezayı hafifletici sebepler de ceza siyasetine bağlı olarak yasa koyucunun takdirindedir.

Kuralla korunmak istenen hukuki yarar, suçun niteliği ile öngörülen cezanın tür ve miktarı gözetildiğinde kuralda yer alan cezanın adaletsiz ve ölçüsüz olduğundan söz edilemez.

Açıklanan nedenlerle kural Anayasaya aykırı değildir. İtirazın reddi gerekir.

VII- SONUÇ

26.9.2004 günlü, 5237 sayılı Türk Ceza Kanunu'nun 245. maddesinin, 29.6.2005 günlü, 5377 sayılı Yasa'nın 27. maddesiyle değiştirilen (1) numaralı fıkrasının Anayasa'ya aykırı olmadığına ve itirazın REDDİNE, 5.3.2009 gününde OYBİRLİĞİYLE karar verildi.

Başkan - Haşim KILIÇ

Başkanvekili - Osman Alifeyyaz PAKSÜT

Üye: Sacit ADALI; Fulya KANTARCIOĞLU; Ahmet AKYALÇIN; Mehmet ERTEN; A. Necmi ÖZLER; Serdar ÖZGÜLDÜR; Şevket APALAK; Serruh KALELİ; Zehra Ayla PERKTAŞ

ANAYASA MAHKEMESİ BİREYSEL BAŞVURU KARARLARI

Bölüm İçeriği

- Ümit Eyüpoğlu Kararı (2018/6161)
- Alper Erarslan Kararı (2018/16857)
- Fırat Gerçek Kararı (2019/25604)
- Ümit Karaduman Kararı (2020/20874)
- H.Ö. Kararı (2019/20473)
- Samet Ayyıldız Kararı (2018/34548)
- Sebiha Kaya Kararı (2018/34124)
- Celal Oraj Altunörgü Kararı (2018/31036)
- Bestami Eroğlu Kararı (2018/23077)
- Ertan Erçıktı (3) Kararı (2018/14040)
- Ramazan Şahin Kararı (2018/11988)
- Kemal Karanfil Kararı (2017/24776)
- A.A.Y. Kararı (2016/13011)
- E.Ü. (B. No: 2016/13010)
- Arif Ali Cangı Kararı (2016/4060)
- Ali Çığır Kararı (2015/19298)
- C.K. (Unutulma Hakkı) Kararı (2014/19685)
- Asli Alp ve Şükrü Alp (Unutulma Hakkı) Kararı (2014/18260)
- Fahri Göncü (Unutulma Hakkı) Kararı (2014/17943)
- N.B.B. (2) (Unutulma Hakkı) Kararı (2014/17143)
- G.Y. (Unutulma Hakkı) Kararı (2014/16026)
- Turgut Duman Kararı (2014/15365)
- B.K. Kararı (2014/14189)
- Nurcan Belin Kararı (2014/14187)
- Fatih Saraman Kararı (2014/7256)
- Güzide Defne Samyeli Kararı (2014/4399)
- Asım Bayar ve Veysel Bayar (Unutulma Hakkı) Kararı (2014/4141)
- G.D. (2) (Unutulma Hakkı) Kararı (2014/1808)
- E.Ç.A. Kararı (2014/5671)

- N.B.B. (Unutulma Hakkı) Kararı (2013/5653)
- Ömür Kara ve Onursal Özbek Kararı (2013/4825)
- Bülent Kaya Kararı (2013/2941)

Anayasa Mahkemesi - Ümit Eyüpoğlu Kararı (2018/6161)

Ümit Eyüpoğlu, B. No: 2018/6161, 28/6/2022

Başvuru, başvurucunun kullandığı telefon hattı ile ilgili bilgilerin verilmesine yönelik talebinin reddedilmesi nedeniyle özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkı ile bağlantılı olarak etkili başvuru hakkının ihlal edildiği iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

İKİNCİ BÖLÜM

KARAR

ÜMİT EYÜPOĞLU BAŞVURUSU

(Başvuru Numarası: 2018/6161)

Karar Tarihi: 28/6/2022

R.G. Tarih ve Sayı: 20/12/2022 - 32049

İKİNCİ BÖLÜM

KARAR

Başkan: Kadir ÖZKAYA

Üyeler: Engin YILDIRIM, Rıdvan GÜLEÇ, Yıldız SEFERİNOĞLU, Kenan YAŞAR

Raportör: Berrak YILMAZ

Başvurucu: Ümit EYÜPOĞLU

I. BAŞVURUNUN KONUSU

1. Başvuru, başvurucunun kullandığı telefon hattı ile ilgili bilgilerin verilmesine yönelik talebinin reddedilmesi nedeniyle özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkı ile bağlantılı olarak etkili başvuru hakkının ihlal edildiği iddiasına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 19/2/2018 tarihinde yapılmıştır.

3. Komisyon, başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar vermiştir.

4. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına gönderilmiştir.

III. OLAY VE OLGULAR

5. Başvuru formu ve eklerinde ifade edildiği şekliyle olaylar özetle şöyledir:

6. Başvurucu; müşterisi olduğu A. İletişim Hizmetleri A.Ş.den (Şirket) kullandığı telefon hattına ait 2014-2015 yıllarının internet verilerini, log kayıtlarını, telefonunun IMEI bilgilerini, Hot Spot (açık Wi-Fi noktası) kullandığı tarih bilgisini istemiştir. Başvurucu ayrıca cep telefonu üzerinden internet kullandığında başka abonelerle ortak aldığı IP numaralarının bu ortak kullanımlardaki diğer abonelere ait telefonların kendisinin telefon numarasıyla aynı, tek IP numarası aldığı tarihlerdeki log kayıtlarına ilişkin veri bilgisinin kendisi ile paylaşılması talebinde bulunmuştur.

7. Başvurucu Şirket Müşteri Hizmetlerinden aranarak bu bilgilerin beş yıl boyunca kayıtlarında saklandığı için ancak mahkeme isterse bu bilgileri/verileri paylaşacaklarından bahisle söz konusu taleplerinin reddedildiğini belirtmiş; İstanbul Anadolu 1. Tüketici Mahkemesinde (Mahkeme) dava açmıştır. Dava dilekçesinde başvurucu; istediği bilgilerin özel hayatıyla ilgili olduğunu, kendisiyle paylaşılması gerektiğini, söz konusu işlem nedeniyle mağdur edildiğini belirterek anılan bilgilerin kendisine verilmesi ve manevi tazminat talebinde bulunmuştur.

8. Davaya cevap dilekçesinde; başvurunun çağrı detaylarını Şirketten çeşitli yollardan talep edebileceği ve talep tarihinden en fazla iki yıl öncesine kadar olan görüşme detaylarını öğrenebileceği belirtilmiştir. Ayrıca başvurucu aboneye gönderilen çağrı detaylarının görüştüğü numara, tarih, saat, süre ve her kullanımı için tabi olduğu ücret bilgilerini içerdiği, başvurunun talep ettiği diğer bilgilerin kişisel verilerin korunması ve tüketici mevzuatı çerçevesinde abone ile paylaşılması yükümlülüğünün bulunmadığı, başvuru tarafından tespit edilebilecek kendi kullanımına ilişkin bilgilerin paylaşılmamasının herhangi bir hak ihlaline sebep olmadığı ifade edilmiştir.

9. Cevap dilekçesinde ayrıca 28/10/2017 tarihli ve 30224 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Elektronik Haberleşme Sektörüne İlişkin Tüketici Hakları Yönetmeliği'nin (Yönetmelik) "Tüketici hakları" kenar başlıklı 5. maddesinin (e) bendi gereği abonelerin ayrıntılı fatura talep edebilme hakkı bulunduğu, fatura detaylarında kullanım miktarı, aranan numara, süre ve ücret detaylarının yer aldığı belirtilmiştir. Bu kapsamda olmayan bilgilerin verilmesini zorunlu kılan bir düzenlemenin mevzuatta bulunmadığı, Şirket nezdinde talep edilen bilgilerden sadece IMEI numarasına ulaşılabildiği fakat başvurunun hangi IP numarasını kullandığı, hangi web sitelerine

giriş yaptığı ve Wi-Fi bağlantı detaylarının tespit edilemediği ifade edilmiştir. Diğer taraftan dilekçede; Şirketin işlemediği/kayıtlarında tutmadığı verilere ilişkin bilgi verme imkânı/zorunluluğu olmadığı, abonelik sözleşmesi ile mevzuatta böyle bir yükümlülüğün öngörülmediği ve cihaz IMEI bilgisinin başvuruçunun da cihaz üzerinden sorgulayarak tespit edebileceği vurgulanmıştır.

10. Mahkeme 18/4/2017 tarihinde davanın reddine karar vermiştir. Kararın gerekçesinde; başvuruçunun özellikle 2014 yılı Ağustos ve Eylül ayları içinde üzerine kayıtlı telefon numarasına ait ortak IP bilgisi olup olmadığı ve Hot Spot işlemi yapılıp yapılmadığı, ortak IP verilmiş ise ilgili telefon numaralarının tespiti talebiyle dava açtığı belirtilmiştir. Kararda ayrıca davada tespiti talep edilen hususların bir hak ya da hukuki ilişkiden ziyade maddi verilere ilişkin olduğu vurgulanmıştır. Anılan verilerin 12/1/2011 tarihli ve 6100 sayılı Hukuk Muhakemeleri Kanunu'nun 106. maddesinde düzenlenen tespit davasının konusunu oluşturmadığı, dolayısıyla menfaatin varlığının ispatlanamadığı, zarar meydana gelmemesi nedeniyle de manevi tazminat koşullarının oluşmadığı ifade edilmiştir.

11. Başvuruçucu karara karşı yaptığı istinaf başvurusu üzerine İstanbul Bölge Adliye Mahkemesi 3. Hukuk Dairesi (Bölge Adliye Mahkemesi) 10/11/2017 tarihinde başvuruçunun istinaf talebini esastan reddetmiştir. Kararda başvuruçunun istediği bilgilerin mevzuat uyarınca paylaşmakla yükümlü olunan asgari bilgilerin dışında kaldığı belirtilmiştir. Söz konusu bilgilerin 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 8. maddesinde yazılı suçların faillerine ulaşmak için hâkim kararı ile adli mercilere verilebileceği vurgulanmıştır. Diğer taraftan kararda başvuruçunun tüketici mahkemesi nezdinde hukuken korunmaya değer güncel bir yararının bulunduğunu iddia ve ispat edememesi nedeniyle başvuruçunun talebinin 6100 sayılı Kanun'un 106. maddesinde düzenlenen tespit davası şartlarını taşımadığı, başvuruçunun talebinin bir hukuki ilişkinin varlığının tespitine değil maddi verilere ilişkin olduğu, bu hususun anılan Kanun'un 400. maddesi kapsamında delil tespiti talebi şeklinde ileri sürülebileceği belirtilmiştir. Ayrıca kararda dava dilekçesinde ileri sürülen iddia ve sebeplerin 11/1/2011 tarihli ve 6098 sayılı Türk Borçlar Kanunu ile 22/11/2001 tarihli ve 4721 sayılı Türk Medeni Kanunu'nda manevi tazminat için öngörülen kişilik haklarına ihlal şartını karşılamadığı değerlendirilmesine yer verilmiştir.

12. Nihai karar 20/1/2018 tarihinde başvuruçuya tebliğ edilmiştir.

IV. İLGİLİ HUKUK

A. Ulusal Hukuk

13. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Genel ilkeler" kenar başlıklı 4. maddesi şöyledir:

"(1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.

(2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

a) Hukuka ve dürüstlük kurallarına uygun olma.

b) Doğru ve gerektiğinde güncel olma.

c) Belirli, açık ve meşru amaçlar için işlenme.

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme."

14. 6698 sayılı Kanun'un "İlgili kişinin hakları" kenar başlıklı 11. maddesinin ilgili kısmı şöyledir:

"Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

a) Kişisel veri işlenip işlenmediğini öğrenme,

b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme

...haklarına sahiptir."

15. 28/5/2009 tarihli ve 27241 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği'nin "İşletmecilerin hak ve yükümlülükleri" kenar başlıklı 19. maddesinin (1) numaralı fıkrasının 11/6/2016 tarihli ve 29739 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren değişik (f) bendi şöyledir:

"Trafik bilgilerinin muhafaza edilmesi: Erişim sağlayıcı olan veya telefon hizmeti sunan işletmeci, taraflara ilişkin IP adresi, port aralığı, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı, kullanıcı sayısı ve abone kimlik bilgileri ile altyapısı üzerinden gerçekleşen görüşmelere ait trafik bilgilerini iki yıl süreyle; kullanıcı bilgilerini ise ilgili mevzuatta belirtilen zamanaşımı süresi boyunca muhafaza etmekle yükümlüdür."

16. 4/12/2020 tarihli ve 31324 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik'in (Yönetmelik) "Tanımlar ve kısaltmalar" kenar başlıklı 4. maddesinin ilgili kısmı şöyledir:

"(1) Bu Yönetmelikte geçen;

...

h) Konum verisi: Kamuya açık elektronik haberleşme hizmeti kullanıcısına ait bir cihazın coğrafi konumunu belirleyen ve elektronik haberleşme şebekesinde veya elektronik haberleşme hizmeti aracılığıyla işlenen belirli veriyi,

...

k) Trafik verisi: Bir elektronik haberleşme şebekesinde haberleşmenin iletimi veya bu haberleşmenin faturalandırılması amacıyla işlenen her türlü veriyi,... ifade eder."

17. Yönetmelik'in "Trafik ve konum verilerine ilişkin aydınlatma yükümlülüğü" kenar başlıklı 9. maddesi şöyledir:

"(1) 6698 sayılı Kanununun 10 uncu maddesi hükümleri saklı kalmak üzere, trafik ve konum verilerinin işlenebildiği hallerde işletmeciler, işlenebilecek trafik veya konum verisi türleri, işleme amacı ve süresi hakkında abonelere/kullanıcılara bilgi vermekle yükümlüdür."

18. Yönetmelik'in "Tüketici hakları" kenar başlıklı 5. maddesinin (1) numaralı fıkrasının (e) bendi şöyledir:

"e) Abonelerin ayrıntılı fatura talep edebilme hakkı,"

19. Yönetmelik'in "Şeffaflık ve bilgilendirme" kenar başlıklı 6. maddesinin (1) numaralı fıkrası şöyledir:

"(1) İşletmeciler, sundukları elektronik haberleşme hizmetlerine erişim ve bu hizmetlerin kullanımı ile ilgili olarak asgari aşağıdaki bilgiler olmak üzere, özellikle hizmetler arasında seçim yapılırken ve abonelik sözleşmesi kurulurken tüketicilerin karar vermelerinde etkili olabilecek hususlar ile dürüstlük kuralı gereğince bilgilendirilmelerinin gerekli olduğu her durumda talep olmaksızın tüketicileri bilgilendirmekle ve bu bilgilere kolayca ulaşılabilmesini sağlamakla yükümlüdür:

a) İşletmecinin adı, unvanı ve adresi,

b) Sunulacak hizmete ilişkin olarak; hizmetin tanımı ve kapsamı, hizmete erişim ve hizmetin kullanımı konusunda genel hüküm ve şartlar, hizmet için uygulanacak tarifeler ve varsa abonelik paketleri, tarifelerin içerdiği vergi türleri ile bu vergilerin tarifeler hesaplanırken tarifelere yansıtılma oranı, doğru tüketici algısının oluşması amacıyla tarifelerin yalnızca tüm vergiler dahil değeri, abonelik tesisi dolayısıyla alınacak diğer ücretler, tarife ücreti ile birlikte telsiz kullanım ücreti yansıtılacağına dair abonenin doğru değerlendirme yapabileceği açıklıkta bilgi,

c) Taahhütnamelere ilişkin şartlar, sunulan bakım/onarım hizmetlerine ilişkin genel bilgi ve standart sözleşme şartları ile geri ödeme şartları ve/veya işletmecinin kusurundan kaynaklanan nedenlerle sözleşmede belirtilen hizmet kalite seviyesinin sağlanamaması halinde zararın giderilmesine ilişkin bilgi,

ç) Tüketici şikâyetlerinin çözüm usul ve süreçlerine ilişkin bilgi..."

B. Uluslararası Hukuk

1. Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi

20. Birleşmiş Milletler Genel Kurulunun 10/12/1948 tarihli ve 217 (111) sayılı kararı ile kabul edilen İnsan Hakları Evrensel Beyannamesi'nin 12. maddesi şöyledir:

"Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfî karışmalara, şeref ve şöhretine karşı tecavüzlere mâruz kalamaz. Herkesin bu karışmalara ve tecavüzlere karşı kanun ile korunmağa hakkı vardır."

21. Birleşmiş Milletler Genel Kurulu tarafından kişisel verilerin korunması konusunda kabul edilen 14/12/1990 tarihli ve 45/95 sayılı "Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler" de şunlara yer verilmiştir:

"...

4- İlgili kişilerin erişmesi ilkesi: Kimlik kanıtı sunan herkes kendisiyle ilgili bilgilerin işlenip işlenmediğini bilme ve gereksiz bir gecikme veya masraf olmadan anlaşılır biçimde elde etme hakkına sahiptir. Ayrıca bu bilgilerin kanuna aykırı, gereksiz veya yanlış olması durumunda uygun düzeltmelerin yapılmasını veya silinmesini talep etme hakkına sahiptir. Devletler buna uygun bir çözüm yolu sağlamak durumundadır. Herhangi bir düzeltme maliyeti dosyadan sorumlu kişi tarafından karşılanmalıdır. Bu ilke hükümlerinin uyruk veya ikâmetine bakılmaksızın herkes için uygulanması arzu edilir.

..."

2. Avrupa Birliği Genel Veri Koruma Tüzüğü

22. 27/4/2016 tarihli ve 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nün "Tanımlar" kenar başlıklı 4. maddesinin ilgili kısmı şöyledir:

"Bu Tüzük'ün amaçları doğrultusunda, aşağıdaki tanımlar geçerlidir:

Kişisel veri, belirli veya belirlenebilir bir gerçek kişi hakkındaki her bilgiyi ifade eder (veri sahibi); belirlenebilir bir gerçek kişi ad, kimlik, yer bilgisi, online kimlik veya kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel ya da sosyal kimliği gibi belirleyici bir özelliikle doğrudan veya dolaylı olarak belirlenebilen kişidir.

İşleme, kişisel veri veya kişisel veri dizisinin otomatik veya başka bir şekilde toplanması, kaydedilmesi, organize edilmesi, yapılandırılması, depolanması, uyarlanması veya değiştirilmesi, geri alınması, kullanılması, iletim yoluyla açıklanması, yayılması veya erişilebilir hâle getirilmesi, sıralanması veya kombine edilmesi, sınırlandırılması, silinmesi veya yok edilmesi gibi yollarla herhangi bir işlem veya işlem dizisine tabi tutulması anlamına gelir."

23. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün "Kişisel verilerin işlenmesi ile ilgili ilkeler" kenar başlıklı 5. maddesinin ilgili kısmı şöyledir:

"Kişisel veri;

Veri sahibi ile ilgili olarak hukuka uygun, adil ve şeffaf bir biçimde işlenmelidir (hukuka uygunluk, adillik ve şeffaflık),

..."

3. Avrupa İnsan Hakları Sözleşmesi

24. Avrupa İnsan Hakları Sözleşmesi'nin (Sözleşme) "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesi şöyledir:

"(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."

4. Avrupa Konseyi Siber Suç Sözleşmesi

25. Türkiye Cumhuriyeti tarafından 10/11/2010 tarihinde imzalanan ve Türkiye Büyük Millet Meclisi tarafından onaylanması uygun bulunarak 2/5/2014 tarihinde yürürlüğe giren Avrupa Konseyi Siber Suç Sözleşmesi'nin "Depolanmış bilgisayar verilerine izinli şekilde veya bu verilerin halka açık olduğu durumlarda sınır ötesinden erişim sağlanması" kenar başlıklı 32. maddesi şöyledir:

"Bir taraf, diğer tarafın izni olmaksızın; a) Halkın serbest kullanımına sunulan (açık kaynaktan gelen) depolanmış bilgisayar verilerine bunların coğrafi konumuna bakılmaksızın erişilebilir; veya b) Kendi

ülkesindeki bir bilgisayar sistemi aracılığıyla, diğer tarafın ülkesindeki depolanmış bilgisayar verilerine, eğer bu taraf, söz konusu bilgisayar sistemi aracılığıyla veriyi ifşa etme yetkisini yasal olarak haiz bulunan kişinin yasal ve gönüllü onayını sağlayabilirse, söz konusu verilere erişebilir veya bunları temin edebilir."

5. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

26. 18/2/2016 tarihli ve 29628 sayılı Resmî Gazete'de yayımlanan 30/1/2016 tarihli ve 6669 sayılı Kanun'la uygun bulunan 28/1/1981 tarihli Avrupa Konseyi Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "Tanımlar" kenar başlıklı 2. maddesinin ilgili kısmı şöyledir:

"Bu Sözleşmenin amaçları bakımından:

a "Kişisel veriler": Kimliği belirli veya belirlenebilir bir gerçek kişi ("ilgili kişi") hakkındaki tüm bilgileri ifade eder.

...

c "Otomatik işlem" den, tamamen veya kısmen otomatik yöntemlerle gerçekleştirilen; verilerin kaydı, bu verilere mantıksal ve/ veya aritmetik işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya dağıtılması anlaşılır."

27. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "Verilerin niteliği" kenar başlıklı 5. maddesi şöyledir:

"Otomatik işleme konu olan kişisel veriler:

a. Adil biçimde ve yasal yoldan elde edilir ve işlenir;

b. Belli ve meşru amaçlar için kaydedilir ve bu amaçlara aykırı şekilde kullanılmaz;

c. Kaydedilme amaçlarına göre uygun ve yerinde olur ve aşırı olmaz;

d. Doğru bilgileri yansıtır ve gerektiğinde güncellenir;

e. Kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkan veren bir biçimde saklanır."

28. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "İstisnalar ve kısıtlamalar" kenar başlıklı 9. maddesinin ilgili kısmı şöyledir:

“2. Taraf devletin kanunlarında öngörölmüş olması ve demokratik bir toplumda aşğıdaki hususların sağlanması için gerekli bir önlem oluşturması halinde işbu Sözleşmenin 5, 6 ve 8. maddelerine istisna getirilebilir:

- a. Devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi;
- b. İlgili kişinin veya başkasının hak ve özgürlüklerinin korunması.”

6. Avrupa İnsan Hakları Mahkemesi İctihadı

29. Avrupa İnsan Hakları Mahkemesi (AİHM) içtihatlarında özel hayatın eksiksiz bir tanımı bulunmayan geniş bir kavram olduğunu belirtmektedir. Özel hayata saygı hakkı alt kategorisinde geçen özel hayat kavramını AİHM oldukça geniş yorumlamakta ve bu kavrama ilişkin tüketici bir tanım yapmaktan özellikle kaçınmaktadır (Koch/Almanya, B. No: 497/09, 19/7/2012, § 51). Bununla birlikte Sözleşme'nin denetim organlarının içtihatlarında bireyin kişiliğini serbestçe geliştirmesi ve gerçekleştirmesi ile kişisel bağımsızlık kavramlarının özel hayata saygı hakkının kapsamının belirlenmesinde temel alındığı anlaşılmıştır (Sidabras ve Džiautas/Litvanya, B. No: 55480/00, 59330/00, 27/7/2004, § 43; K.A. ve A.D./Belçika, B. No: 42758/98, 45558/99, 17/2/2005, § 83; Pretty/Birleşik Krallık, B. No: 2346/02, 29/4/2002, § 61; Christine Goodwin/Birleşik Krallık [BD], B. No: 28957/95, 11/7/2002, § 90).

30. AİHM'e göre devlet pozitif sorumluluğu kapsamında başvuruçuların kendilerini ilgilendiren herhangi bir bilgiye erişimini sağlayacak etkili ve erişilebilir bir usulü temin etmek zorundadır (Yonchev/Bulgaristan, B. No: 12504/09, 7/12/2017 § 53; K.H. ve diğerleri/Slovakya B. No: 32881/04, 28/4/2009 § 46). AİHM başvuruçunun İçişleri Bakanlığındaki personel dosyasına ve özellikle de değerlendirmelere erişim talebinin birtakım belgelerin gizli olduğu gerekçesiyle reddedilmesinin Sözleşme'nin 8. maddesini ihlal ettiğine karar vermiştir (Yonchev /Bulgaristan §§ 62, 63).

31. AİHM kişilerin kendileriyle ilgili tutulan tıbbi kayıtların fotokopilerini alamamalarını, davalı devletin başvuruçuların özel ve aile hayatına saygı hakkından etkili bir şekilde yararlanmalarını temin edecek pozitif yükümlülüklerini yerine getirmediği gerekçesiyle Sözleşme'nin 8. maddesini ihlal ettiğine karar vermiştir (K.H. ve diğerleri/Slovakya § 58).

V. İNCELEME VE GEREKÇE

32. Anayasa Mahkemesinin 28/6/2022 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları

33. Başvurucu; 2014-2015 yıllarında kullandığı adına kayıtlı telefon hattından internet kullanımına bağlı olarak hangi tarihlerde başka telefon numaralarıyla ortak tek IP numarası aldığına, bu ortak IP numaralarının ne olduğuna, hangi internet sitelerine girildiğine ve hangi programların kullanıldığına ilişkin veriler ile log kayıtlarına ilişkin belgelerin tamamının tarafına verilmesini Şirketten talep ettiğini ancak talebinin Şirket tarafından bu bilgilerin sadece mahkeme kararıyla verilebileceği söylenerek reddedildiğini belirtmiştir. Başvurucu; ayrıca Tüketici Mahkemesinde açtığı davanın reddedilmesi sonucunda kendisine ait kişisel verilere ulaşma, bu verilerin doğru olup olmadığını öğrenme, bu bilgilerde hata varsa düzeltme hakkını kullanmadığını ifade ederek kişisel verilerin korunması, özel hayata saygı hakkı, hak arama hürriyeti ve mülkiyet hakkının ihlal edildiğini ileri sürmüştür.

B. Değerlendirme

34. Anayasa'nın "Devletin temel amaç ve görevleri" kenar başlıklı 5. maddesi şöyledir:

"Cumhuriyeti ve demokrasiyi korumak, kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak; kişinin temel hak ve hürriyetlerini, sosyal hukuk devleti ve adalet ilkeleriyle bağdaşmayacak surette sınırlayan siyasal, ekonomik ve sosyal engelleri kaldırmaya, insanın maddî ve manevî varlığının gelişmesi için gerekli şartları hazırlamaya çalışmaktır."

35. Anayasa'nın "Özel hayatın gizliliği" kenar başlıklı 20. maddesinin birinci ve üçüncü fıkraları şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

...

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

36. Anayasa'nın "Temel hak ve hürriyetlerin korunması" kenar başlıklı 40. maddesi şöyledir:

"Anayasa ile tanınmış hak ve hürriyetleri ihlal edilen herkes, yetkili makama geciktirilmeden başvurma imkânının sağlanmasını isteme hakkına sahiptir.

Devlet, işlemlerinde, ilgili kişilerin hangi kanun yolları ve mercilere başvuracağını ve sürelerini belirtmek zorundadır.

Kişinin, resmî görevliler tarafından vâki haksız işlemler sonucu uğradığı zarar da, kanuna göre, Devletçe tazmin edilir. Devletin sorumlu olan ilgili görevliye rücu hakkı saklıdır."

37. Özel hayata saygı hakkı Anayasa'nın 20. maddesinde koruma altına alınmıştır. Devlet, kişilerin özel ve aile hayatına keyfî olarak müdahale etmemek ve üçüncü kişilerin haksız saldırılarını önlemekle yükümlüdür. Özel hayata saygı hakkı kapsamında korunan hukuksal çıkarlardan biri de bireyin mahremiyet hakkıdır. Ancak mahremiyet hakkı sadece yalnız kalma hakkından ibaret olmayıp bu hak, bireyin kendisiyle ilgili bilgileri kontrol edebilme hukuksal çıkarını da kapsamaktadır. Bireyin kendisine ilişkin herhangi bir bilginin rızası olmaksızın açıklanmaması, yayılmaması, bu bilgilere başkaları tarafından ulaşılabilmesi ve rızası hilafına kullanılmaması, kısaca bu bilgilerin mahrem kalması konusunda menfaati bulunmaktadır. Bu husus, bireyin kendisiyle ilgili bilgilerin geleceğini belirleme hakkına işaret etmektedir (Serap Tortuk, B. No: 2013/9660, 21/1/2015, §§ 31, 32). Özel hayata saygı hakkının kapsamında olan bireylerin kişisel verilerinin korunması hakkı Anayasa'nın 20. maddesinde açık olarak düzenlenmiştir (Nurcan Belin, B. No: 2014/14187, 10/1/2018, § 38).

38. Anayasa'nın 20. maddesinin üçüncü fıkrasında herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilmeyi, bu verilere erişmeyi, bunların düzeltilmesini veya silinmesini talep etmeyi ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı ifade edilmiştir. Maddede ayrıca kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır (AYM, E.2014/122, K.2015/123, 30/12/2015, §§ 19, 20; Nurcan Belin, § 45).

39. Anayasa Mahkemesi kararlarında da belirtildiği üzere kişisel veri -belirli veya kimliği belirlenebilir olmak şartıyla- bir kişiye ilişkin bütün bilgileri ifade etmekte olup bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi sadece kimliğini ortaya koyan bilgileri değil telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, öz geçmişi, fotoğrafı, görüntü ve ses kayıtları, parmak izleri, sağlık bilgileri, genetik bilgileri, IP adresi, e-posta adresi, alışveriş alışkanlıkları, hobileri, tercihleri, etkileşimde bulunduğu kişiler, grup üyelikleri, aile bilgileri gibi

kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır (AYM, E.2014/74, K.2014/201, 25/12/2014; E.2014/180, K.2015/30, 19/3/2015).

40. Öte yandan Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı yönünden inceleme yapılabilmesi için öncelikle anılan hak kapsamında korunması gerekli bir kişisel verinin olup olmadığı belirlenmelidir. Anayasa hükmünün lafzı, konuya ilişkin uluslararası belgeler ve karşılaştırmalı hukuk dikkate alındığında belirli veya belirlenebilir bir gerçek veya tüzel kişi hakkındaki her türlü bilgi kişisel veri olarak değerlendirilir. Ancak her dava ya da başvuruda Anayasa'nın 20. maddesinin üçüncü fıkrası anlamında bir kişisel veri bulunup bulunmadığı davanın ve başvurunun kendine özgü koşulları dikkate alınarak otonom olarak tespit edilir. Bir kişisel verinin bulunduğu tespit edildiğinde bu veriye yönelik her türlü sınırlama ve müdahale Anayasa'nın anılan hükmü kapsamındaki güvenceleri harekete geçirir (E.Ü., § 59).

41. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Somut olayda başvuru adına kayıtlı telefon hattına ait internet verileri, log kayıtları, telefonunun IMEI bilgileri, Hot Spot (açık Wi-Fi noktası) kullandığı tarihe ilişkin bilgiler belirli bir gerçek kişi hakkındaki bilgi kapsamında olduğu anlaşılınca bu bilgilere erişmenin, bunların düzeltilmesini veya silinmesini talep etmenin ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmenin özel hayata saygı hakkı kapsamında, kişisel verilerin korunmasını isteme hakkı yönünden incelenmesi gerektiği değerlendirilmiştir. Ayrıca başvuru cep telefonu üzerinden internet kullandığında aynı, ortak, tek IP numarası alan başka abonelere ait telefon numaraları ile log kayıtlarına ilişkin bilgiler de bu kişiler yönünden belirli bir gerçek kişi hakkındaki bilgi kapsamında olup bu bilgilere erişilememesi özel hayata saygı hakkı kapsamında, kişisel verilerin korunmasını isteme hakkı ile bağlantılı olarak etkili başvuru hakkının ihlal edildiği iddiaları çerçevesinde ele alınmıştır.

42. Somut olayda başvuru müşterisi olduğu şirkete karşı 2014-2015 yıllarında telefon hattında ortak IP bilgisi olup olmadığı ve Hot Spot işlemi yapılıp yapılmadığı bilgisi ile ortak IP verilmiş ise ilgili telefon numaraları bilgisinin tarafına verilmesi, ayrıca yapılan bu uygulama nedeniyle mağdur edildiğinden bahisle manevi tazminat istemiyle Tüketici Mahkemesinde açtığı dava; tespit davasının konusunu oluşturmadığı, menfaat şartının ispatlanamadığı, zarar meydana gelmemesi nedeniyle de manevi tazminat koşullarının oluşmadığı gerekçesiyle reddedilmiştir. Söz konusu sürece ilişkin olarak başvuru temel iddiası söz konusu kişisel verilerinin tarafına verilmesi ve tazminata hükmedilmesi talebiyle açtığı dava hakkında etkili, ciddi ve sonuç alabileceği şekilde bir çözüm

imkânı sunulmadığına ilişkindir. Bu kapsamda başvuru hakkının öncelikle Anayasa'nın 20. maddesinde düzenlenen kişinin kişisel verilerin korunması hakkıyla bağlantılı olarak Anayasa'nın 40. maddesinde güvence altına alınan etkili başvuru hakkı kapsamında değerlendirilmesi gerektiği kanaatine varılmıştır.

1. Kabul Edilebilirlik Yönünden

43. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan kişisel verilerin korunması hakkıyla bağlantılı olarak etkili başvuru hakkının ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

2. Esas Yönünden

a. Genel İlkeler

44. Anayasa'nın 5. maddesinde bireylerin temel hak ve özgürlüklerinin korunması için gerekli şartların hazırlanması, devletin temel amaç ve görevlerinden biri olarak sayılmaktadır. Anayasa ve Sözleşme'nin ortak koruma alanı kapsamında kalan temel hak ve hürriyetler, yalnızca kamusal gücün doğrudan uygulanmasıyla değil kimi zaman da özel hukuk kişileri arasındaki uyuşmazlıklara konu olacak şekilde üçüncü kişilerin müdahalelerine de konu olabilmektedir. Anayasa Mahkemesi birçok kararında uyuşmazlıkların özel hukuk kişileri arasında gerçekleştiği durumlarda başvuruları devletin pozitif yükümlülükleri bağlamında ele almıştır. Özel hayatın korunması kapsamında kişisel verilerin korunmasını isteme hakkı yönünden de devletin pozitif bir yükümlülük olarak yetki alanında bulunan tüm bireyleri gerek kamusal makamların ve diğer bireylerin gerekse kişinin kendisinin eylemlerinden kaynaklanabilecek risklere karşı koruma yükümlülüğü bulunmaktadır (Ömür Kara ve Onursal Özbek, B. No: 2013/4825, 24/3/2016, §§ 45, 46; E.Ü., § 65; Ali Çığır, B. No: 2015/19298, 8/5/2019, §§ 32, 33; Erol Kumcu, B. No: 2015/18988, 9/5/2019, §§ 32, 33; U. B., B. No: 2015/3175, 10/10/2019, §§ 33, 34).

45. Pozitif yükümlülükler özel hukuk kişilerinin birbirleri ile olan uyuşmazlıklarının çözümüne ilişkin yasal alt yapının oluşturulmasını, söz konusu uyuşmazlıkların adil yargılama gereklerine uygun ve usul yönünden güvenceleri haiz bir yargılama kapsamında incelenmesini ve bu yargılamaalarda temel haklara ilişkin anayasal güvencelerin gözetilip gözetilmediğinin denetlenmesini gerektirir (Ömür Kara ve Onursal Özbek, §§ 47-50).

46. Söz konusu yükümlülükler, kişilerin maddi ve manevi varlıklarının korunmasını ve devam eden müdahalelerin durdurulmasını sağlayabilmelidir. Ayrıca müdahalenin kaynağı olan işlemler, eylemler veya ihmaller konusunda kişilere etkili bir karşı çıkma ve oluşan zararların tazmin

edilebilmesi için telafi etme imkânı tanınmalıdır. Bu imkân ise ancak etkili bir başvuru yolunun mevcut olması ile mümkündür (benzer yöndeki değerlendirmeler için bkz. Meral Danış Beştaş (3), § 36).

47. Etkili başvuru hakkı; anayasal bir hakkının ihlal edildiğini ileri süren herkese, hakkın niteliğine uygun olarak iddialarını inceletebileceği makul, erişilebilir, ihlalin gerçekleşmesini veya sürmesini engellemeye ya da sonuçlarını ortadan kaldırmaya (yeterli giderim sağlama) elverişli idari ve yargısal yollara başvuruda bulunabilme imkânının sağlanması olarak tanımlanabilir (Y.T. [GK], B. No: 2016/22418, 30/5/2019, § 47; Meral Danış Beştaş (3), § 37).

b. İlkelerin Olaya Uygulanması

48. Anayasa'nın 20. maddesinin üçüncü fıkrasının birinci cümlesinde genel olarak herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu belirtilmiş, ikinci cümlesinde kişisel veriler bağlamında bazı özel güvenceler sayılmış, üçüncü cümlesinde kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği düzenlenmiş, dördüncü cümlesinde ise kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hüküm altına alınmıştır. Buna göre lafzı dikkate alındığında Anayasa'nın 20. maddesinin üçüncü fıkrasının kişisel verilerin korunmasını isteme hakkı kapsamında sadece işleme şeklindeki sınırlama ya da müdahalelere karşı değil kişisel verilere yönelik her türlü müdahale ve sınırlamalara karşı güvence getirdiği anlaşılmaktadır (E.Ü., § 63; Bestami Eroğlu, B. No:2018/23077, 17/9/2020, § 101).

49. Bunun yanında Anayasa'nın 20. maddesinin üçüncü fıkrasının ikinci cümlesinde kişisel verilerin korunmasını isteme hakkının, kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı belirtilmiştir.

50. Kişilerin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme ve bu verilere erişim hakkı veri işleminin şeffaflığı veya açıklığı ilkesinin bir uzantısıdır. Kişilerin kendisi hakkında hangi verilerin kim tarafından ne zaman ve hangi nedenle işlendiğini bilmesi bu verileri düzeltme, sildirme, engelleme gibi haklarını kullanmasını da mümkün kılmakta ve söz konusu anayasal güvencelerin hayata geçirilmesini sağlamaya yönelik tamamlayıcı bir özellik taşımaktadır.

51. Bu ilkeler ışığında demokratik bir toplumda kişisel verilerin işlenmesi süreci şeffaf bir şekilde gerçekleştirilmeli, bunun bir gereği olarak veri sahiplerine kişisel verilerine erişim imkânı tanınmalı ve bu imkânın kolayca kullanılması için gerekli tedbirler alınmalıdır.

52. Başvuru özetle başvurucunun adına kayıtlı telefon hattından internet kullanımına bağlı bazı kişisel verilerin verilmesi ile tazminat talebiyle tüketici mahkemesine açtığı davanın reddedilmesi

nedenleriyle bu verilere erişim, kontrol etme ve düzeltme hakkının elinden alınarak ihlal iddialarının dile getirebileceği etkili bir başvuru yolunun bulunmamasına, bir başka deyişle mevcut yargısal sistemin etkili şekilde işletilmemesine ilişkindir.

53. Kişisel verilerin korunması hakkına yönelik eylemler ya da ihmaller konusunda muhataplarınca dava açılması, itirazlarda bulunulması ve hukuka aykırılıkların tespit edilerek kaldırılması konusunda etkin bir hukuk yolunun varlığı büyük önem taşımaktadır. Devletin kişisel verilerin korunması hakkına müdahale edilmesini önleyecek, müdahale edildiği takdirde giderim sağlayacak etkili hukuki başvuru yollarını hayata geçirmesi ve bu yolları işlevsel kılmaması gerekir. Bu anlamda kişisel verilerin korunması hakkına müdahale teşkil ettiği ve kaldırılması gerektiği konusunda ileri sürülecek iddiaların esasının incelenmesine imkân sağlayan ve gerektiğinde uygun bir telafi yöntemi sunan etkili hukuk yollarının olması ilgililere etkili başvuru hakkının sağlanması bakımından bir gerekliliktir.

54. Kişisel verilerin korunmasını isteme hakkı çerçevesinde devlete yüklenen pozitif yükümlülükler, bu hakkın kapsamında kişilere tanınmış olan güvencelerden etkili bir şekilde yararlanılmayı temin etmek için devlete mevzuat oluşturma ve özellikle de güvencelere aykırılıkları yaptırıma bağlama yükümlülüğü vermektedir. Ayrıca Anayasa'nın 20. maddesinin üçüncü fıkrasının son cümlesinin "Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." şeklindeki hükmü uyarınca mevzuat oluşturma yükümlülüğü gereklerinin çerçevesi kanunla belirlenmelidir.

55. Bu çerçevede Anayasa'nın 20. maddesinde güvence altına alınan kişisel verilerin korunmasını isteme hakkına ilişkin güvenceler ile 6698 sayılı Kanun ve hukuk sistemimizde mevcut olan düzenlemelerin mevcut başvuruya konu uyumsuzlukta uygulanması yönünde bir engel olmadığı gözetildiğinde yasal altyapı oluşturmak bağlamında pozitif yükümlülüklerin yerine getirildiği söylenebilir (bkz. §§ 13-19). Ancak bir hukuk yolunun teorik olarak mevcut olması pozitif yükümlülüklerin yerine getirildiğini ifade edebilmek bakımından yeterli olmayıp ayrıca bu yolun etkili bir biçimde işletilmesi gerekir.

56. Somut olayda mahkemelerin çok dar bir yorumla söz konusu talepleri bir hak ya da hukuki ilişkiden ziyade maddi verilere ilişkin bulduğu ve tüketici mahkemesi nezdinde güncel bir yararın bulunmadığından menfaat şartı yokluğu nedeniyle davanın esasına girmeyerek reddettiği görülmüştür. Bu yorumun başvuru hakkının kişisel verilerine erişimini engellediği açıktır. Nitekim başvuru bu verilere erişme yönündeki talebi reddedildiği için bu davayı açmıştır. Yukarıda da değinildiği üzere kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme ve bu verilere erişme

hakkı Anayasa'nın 20. maddesinin üçüncü fıkrasında açıkça öngörölmüş olan güvencelerdir. Kişisel verilerin şeffaflığı ilkesi de bu güvencelerin sağlanmasını gerektirmektedir.

57. Bireysel başvuru bağlamında ikincilik ilkesinin bir gereği olarak hâkimin önündeki uyuşmazlıkları Anayasa'da yer alan temel hak ve hürriyetlere yönelik güvenceleri öncelikle dikkate alarak çözüme kavuşturması gerekir. Zira Anayasa'nın 11. maddesine göre Anayasa hükümleri, yasama, yürütme ve yargı organlarını, idare makamlarını ve diğer kuruluş ve kişileri bağlayan temel hukuk kurallarıdır. Anayasa'nın 138. maddesi de hâkimlerin Anayasa'ya, kanuna ve hukuka uygun olarak vicdani kanaatlerine göre hüküm vereceklerini düzenlemiştir. Dolayısıyla uyuşmazlığa uygulanacak kanun hükümlerinin ve diğer ikincil düzenlemelerin yoruma açık nitelikte olması durumunda hâkim tarafından Anayasa'da yer alan ilke ve güvenceler ışığında yorumlanması gerekir.

58. Yapılan yargılama sürecinde davanın esasının incelenmediği başvuruçunun kişisel verilerine erişme talebinin reddedilmesinde Anayasa'nın 20. maddesinde düzenlenen kişisel verilerin korunmasını isteme hakkının gerekliliklerine uygun bir sebep gösterilmediği, ayrıca böyle bir uygulamayı haklı kılabilecek ilgili ve yeterli bir gerekçenin de ortaya konulmadığı anlaşılmıştır. Bununla birlikte mahkemelerce gerek kişisel verilerin korunmasına ilişkin kanun hükümleri ve gerekse ilgili diğer mevzuat gözetilerek şirketin bu verilere erişim sağlaması yönünden ne gibi yükümlülükleri olduğu yargılama sürecinde hiç tartışılmamış, bu hususlar açıklığa kavuşturulmamıştır (bkz. §§ 13-19; konu hakkındaki uluslararası hukuk için bkz. §§ 20-31). Sonuç olarak mevcut başvuruda başvuruçunun anayasal güvencelerden yararlanabilmesini sağlayabilecek nitelikteki davada uyuşmazlığın esasının incelenmemesi teorik olarak mevcut olan etkili bir hukuk yolunun işlevsiz kalmasına yol açmıştır. Diğer bir deyişle bu hâliyle teorik düzeyde etkili görölebilecek bir dava yolu mahkemelerin söz konusu yorumu sebebiyle somut olayda başarı şansı sunma kapasitesini yitirmiştir.

59. Açıklanan gerekçelerle derece mahkemelerinin başvuruçunun kişisel verilerine erişebilmesi yönündeki talebinin esasının incelenmesini engelleyen yorumu sebebiyle özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkı ile bağlantılı etkili başvuru hakkının ihlal edildiğine karar verilmesi gerekir.

3. Giderim Yönünden

60. Başvuruçucu; ihlalin tespiti ve yargılamanın yenilenmesini, yargılamanın yenilenmesi yerinde görülmediği takdirde 1.102.700 TL maddi ve 300.000 TL manevi tazminat talebinde bulunmuştur.

61. Başvuruda tespit edilen hak ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmasında hukuki yarar bulunmaktadır. Bu kapsamda kararın gönderildiği yargı mercilerince yapılması gereken iş, yeniden yargılama işlemlerini başlatmak ve Anayasa Mahkemesini ihlal sonucuna ulaştıran nedenleri gideren, ihlal kararında belirtilen ilkelere uygun yeni bir karar vermektir (30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 50. maddesinin (2) numaralı fıkrasında düzenlenen bireysel başvuruya özgü yeniden yargılama kurumunun özelliklerine ilişkin kapsamlı açıklamalar için bkz. Mehmet Doğan [GK], B. No: 2014/8875, 7/6/2018, §§ 54-60; Aligül Alkaya ve diğerleri (2), B. No: 2016/12506, 7/11/2019, §§ 53-60, 66; Kadri Enis Berberoğlu (3) [GK], B. No: 2020/32949, 21/1/2021, §§ 93-100).

62. İhlalin ve sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmasının yeterli bir giderim sağlayacağı anlaşıldığından tazminat talebinin reddine karar verilmesi gerektiği sonucuna ulaşılmıştır.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkıyla bağlantılı etkili başvuru hakkının KABUL EDİLEBİLİR OLDUĞUNA,

B. Anayasa'nın 20. maddesinde yer alan özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkıyla bağlantılı etkili başvuru hakkının İHLAL EDİLDİĞİNE,

C. Kararın bir örneğinin kişisel verilerin korunmasını isteme hakkıyla bağlantılı etkili başvuru hakkının ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmak üzere İstanbul Anadolu 1. Tüketici Mahkemesine (E.2016/1953, K.2017/879) GÖNDERİLMESİNE,

D. Başvurucunun tazminat talebinin REDDİNE,

E. 294,70 TL harç ve 4.500 TL vekâlet ücretinden oluşan toplam 4.794,70 TL yargılama giderinin başvurucuya ÖDENMESİNE,

F. Kararın bir örneğinin Adalet Bakanlığına GÖNDERİLMESİNE 28/6/2022 tarihinde OYBİRLİĞİYLE karar verildi.

Anayasa Mahkemesi - Alper Erarşlan Kararı (2018/16857)

Alper Erarşlan [GK], B. No: 2018/16857, 29/9/2022

Başvuru, aleni olmayan bir konuşmanın hukuka aykırı şekilde kayıt altına alınmasına yönelik şikâyet üzerine yapılan soruşturma nın devlet in pozitif yükümlülüklerine uygun yürütülmemesi nedeniyle kişisel verilerin korunmasını isteme hakkının ihlal edildiđi iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

GENEL KURUL

KARAR

ALPER ERARŞLAN BAŞVURUSU

(Başvuru Numarası: 2018/16857)

Karar Tarihi: 29/9/2022

R.G. Tarih ve Sayı: 1/12/2022 - 32030

GENEL KURUL

KARAR

Başkan: Zühtü ARSLAN

Başkanvekili: Hasan Tahsin GÖKCAN

Başkanvekili: Kadir ÖZKAYA

Üyeler: Engin YILDIRIM, Hicabi DURSUN, Muammer TOPAL, M. Emin KUZ, Rıdvan GÜLEÇ, Recai AKYEL, Yıldız SEFERİNOĞLU, Selahaddin MENTEŞ, Basri BAĞCI, İrfan FİDAN, Kenan YAŞAR

Raportör: Fatih ALKAN

Başvurucu: Alper ERARŞLAN

Vekili: Av. Sabahattin GÜMAN

I. BAŞVURUNUN KONUSU

1. Başvuru, aleni olmayan bir konuşmanın hukuka aykırı şekilde kayıt altına alınmasına yönelik şikâyet üzerine yapılan soruşturmanın devletin pozitif yükümlülüklerine uygun yürütülmemesi nedeniyle kişisel verilerin korunmasını isteme hakkının ihlal edildiği iddiasına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 28/5/2018 tarihinde yapılmıştır. Komisyon başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar vermiştir.

3. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına gönderilmiştir.

4. İkinci Bölüm tarafından niteliği itibarıyla Genel Kurul tarafından karara bağlanması gerekli görüldüğünden başvurunun Anayasa Mahkemesi İçtüzüğü'nün (İçtüzük) 28. maddesinin (3) numaralı fıkrası uyarınca Genel Kurula sevkine karar verilmiştir.

III. OLAY VE OLGULAR

5. Başvuru formu ve eklerinde ifade edildiği şekliyle olaylar özetle şöyledir:

6. Başvurucu; borç ilişkisiyle ilgili konuşmasının planlı şekilde ve suç kastıyla hareket edilerek aleni olmayan bir ortamda kayıt altına alındığını ve bu kaydın şüpheli olarak bulunduğu bir ceza soruşturması dosyasına sunulduğunu belirterek kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçu kapsamında İstanbul Cumhuriyet Başsavcılığına (Başsavcılık) suç duyurusunda bulunmuştur. Başvurucu 3/1/2018 tarihli dilekçesinde, söz konusu konuşmanın rızasına aykırı şekilde M.R.A. tarafından kayda alındığını ileri sürerek anılan kişi hakkında kamu davası açılması talebinde bulunmuştur.

7. Başsavcılık, söz konusu ses kaydının başvuruçunun ve diğer bir kısım kişinin şüpheli olduğu bir soruşturmanın müştekisi durumundaki M.R.A. tarafından soruşturma dosyasına sunulduğunu tespit etmiş; ses kaydının başvuruçunun rızası ve bilgisi dışında kayda alındığı iddiasıyla ilgili olarak özel hayatın gizliliğini ihlal ve kişiler arasındaki konuşmaların kayda alınması suçları kapsamında soruşturma başlatmıştır.

8. Soruşturma neticesinde Başsavcılık, şüphelinin ses kayıtlarını sunarken başvuruçunun tarafından işlendiğini iddia ettiği suçlara ilişkin olarak delil sunma saikiyle hareket ettiği kanaatine ulaşmıştır. Başsavcılık; başvuruçunun özel hayat alanına dâhil olan ve özel hayatının gizliliğini ihlal eden bir hususun konuşulmadığını, söz konusu görüşmenin kayda alınmasında ve soruşturmaya delil olarak sunulmasında kasıt unsurunun oluşmadığını, bu yönde Yargıtay kararlarının bulunduğunu belirterek 8/2/2018 tarihinde kamu adına kovuşturmaya yer olmadığına karar vermiştir. Söz konusu

kararda ayrıca kaydın şüpheli M.R.A.nın başvurucuya olan borcunun ödenmesine ve sonraki süreçte başvurucunun yapmadığı birtakım iş ve işlemlere ilişkin ifadeler içerdiği de belirtilmiştir.

9. Karara karşı başvuru, sunduğu 19/3/2018 tarihli itiraz dilekçesinde; talep edilen delillerin toplanmadığını, ses kaydının aidiyetinin araştırılmadığını, ses kaydında kesinti ya da montaj olup olmadığına ilişkin tespit yapılmadığını, kendisinin ve ses kaydında isimleri geçen kişilerin ifadelerinin alınmadığını ileri sürmüştür. Ayrıca ses kaydının suç kastıyla hareket edilerek planlı şekilde alındığını ve verilen kararlar özel hayata saygı hakkının güvencelerinin yerine getirilmediğini iddia etmiştir.

10. İtiraz talebi İstanbul 3. Sulh Ceza Hâkimliğinin 27/3/2018 tarihli kararıyla reddedilmiştir. Kararda, Başsavcılığın verdiği kararın usule ve mevzuata uygun olduğu ifade edilmiştir.

11. Nihai karar 27/4/2018 tarihinde başvurucuya tebliğ edilmiştir.

IV. İLGİLİ HUKUK

A. Ulusal Hukuk

12. 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun "Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" kenar başlıklı 133. maddesi şöyledir:

"Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır.

Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adli para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur. "

13. 5237 sayılı Kanun'un "Özel hayatın gizliliğini ihlal" kenar başlıklı 134. maddesinin (1) numaralı fıkrası şöyledir:

"Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır"

14. Yargıtay 12. Ceza Dairesinin 27/4/2015 tarihli ve E.2014/23371, K.2015/6859 sayılı kararının ilgili kısmı şöyledir:

"... Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçundan: sanığın, haberleşme içeriğini kaydedip, bu kaydı içeren CD'yi, görülmekte olan dava dosyasına delil olarak vermesi biçimindeki eylemleri, TCK'nın 133/1. maddesinde düzenlenen kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçu kapsamında değerlendirilebilir ise de, sanığın konuşmanın tarafı olması nedeniyle atılı TCK'nın 133/1. maddesindeki kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçunun yasal unsurlarının oluşmadığı, eylemin TCK'nın 134. maddesinde düzenlenen özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilebileceği ancak, kişinin, bir daha kanıt elde etme olanağının bulunmadığı ve yetkili makamlara başvurma imkanının olmadığı ani gelişen durumlarda, örneğin; kendisine yada akrabalarına karşı işlenmekte olan (cinsel saldırı, hakaret, tehdit, iftira veya şantaj gibi) bir suç söz konusu olduğunda ya da kendisine veya aile birliğine yönelen, onurunu zedeleyen, haksız bir saldırıyı önlemek için, kaybolma olasılığı bulunan kanıtların kaybolmasını engelleyip, yetkili makamlara sunarak güvence altına almak amacıyla, saldırıyı gerçekleştiren tarafın bilgisi ve rızası dışında, özel hayata ait bilgileri okuma, konuşma ve haberleşme içeriklerini veya özel hayata ilişkin ses ve görüntüleri dinleme, izleme ya da kaydetme, kişisel verileri kaydetme, ele geçirme ve yayma eylemlerinin hukuka aykırı olduğunu kabul etmek mümkün olmadığı gibi, esasen bu hallerde, kişinin hukuka aykırı hareket ettiği bilinciyle hareket ettiğinden de söz edilemeyeceği gözetildiğinde, kayda alınan haberleşme ve konuşma içeriklerini, üçüncü kişi ya da kişilerle paylaştığına ilişkin hakkında bir iddia ileri sürülmeyen sanığın, katılanın sanık olarak yargılandığı ve akrabası olan mağdur İ.ye karşı cinsel taciz davasındaki mağdurenin iddiasını ispatlama amacını taşıyan eylemlerinde, hukuka aykırı hareket ettiği bilinciyle hareket etmediği anlaşılmalı, sanığın eylemlerinin anılan suçları da oluşturmayacağı gözetilerek atılı suçtan beraat kararı verilmesi gerektiği gözetilmeden yazılı şekilde mahkumiyet kararı verilmesi ...Kanuna aykırı olup ... hükmün ... bozulmasına ... karar verildi..."

15. Yargıtay 12. Ceza Dairesinin 7/6/2017 tarihli ve E.2016/4795, K.2017/4840 sayılı kararının ilgili kısmı şöyledir:

"... İki veya daha fazla kişinin, başkalarının bilmeyeceği ve sınırlı bir dinleyici çevresi dışına çıkmayacağı yönünde haklı bir inanç ve iradeyle hareket ederek, herhangi bir aracı vasıta olarak kullanmadan, yüz yüze gerçekleştirdikleri, ancak özel bir çaba gösterilerek duyulabilecek, aleni olmayan, söze dayalı, sesli düşünce açıklamalarının, konuşmanın tarafı olmayan kişi veya kişilerce, ilgisinin rızası olmaksızın, elverişli bir aletle (sesli bir açıklamayı kuvvetlendirerek veya naklederek

onu ses alanının dışına çıkartıp doğrudan doğruya algılanabilir hale getirmeye yarayan her türlü düzenekle) dinlenmesi veya akustik olarak tekrar dinlenebilmesi imkanını sağlayan bir aletle kaydedilmesinin TCK'nın 133/1. maddesinde; en az üç veya daha fazla kişinin, yüz yüze gerçekleştirdikleri, aleni olmayan, söze dayalı düşünce aktarımlarının, söyleşinin tarafı olan kişi veya kişilerce, ilgililerinin rızası olmaksızın, bir aletle kaydedilmesinin aynı Kanununun 133/2. maddesinde kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması başlığı altında suç olarak tanımlandığı, söyleşiden farklı olarak, iki kişi arasında da gerçekleşebilecek olan konuşmada, konuşan tarafların, aralarında geçen sözleri kaydetmesi, TCK'nın 133/1. maddesi kapsamında suç olarak tanımlanmamış olup, koşulları bulunduğu takdirde eylemin aynı Kanununun 134. maddesinde düzenlenen özel hayatın gizliliğini ihlal suçunu oluşturabileceği; elverişli bir aletle dinlenen veya kaydedilen konuşma veya söyleşiden elde edilen bilgiler sayesinde kendi veya üçüncü kişi lehine, maddi ya da manevi yarar, yani; fayda veya avantaj sağlanması; bu bilgilerin, menfaat karşılığı olsun ya da olmasın, ilgilisi dışındaki kişi veya kişilere verilmesi ya da diğer kişilerin dolaylı olarak bilgi edinmelerinin temin edilmesinin TCK'nın 133/3. maddesinde ayrıca suç olarak tanımlandığı, hükümden önce 05.07.2012 tarihli Resmi Gazete'de yayınlanarak yürürlüğe giren 6352 sayılı Yargı Hizmetlerinin Etkinleştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılması ve Basın Yayın Yoluyla İşlenen Suçlara İlişkin Dava ve Cezaların Ertelenmesi Hakkında Kanununun 80. maddesi ile TCK'nın 133/3. maddesinde yapılan değişiklikte kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verilerin hukuka aykırı olarak ifşa edilmesi eyleminin suç olarak düzenlendiği, Bu açıklamalar ışığında incelenen dosya kapsamına göre; sanığın, hakkında hükmün açıklanmasının geri bırakılması kararı verilen sanık M.yi azmettirip katılan ile yüzyüze yapmış olduğu konuşmayı kaydettirip, katılanın açmış olduğu İş Mahkemesindeki davaya delil olarak sunduğu iddia edilen olayda, iki kişinin yüzyüze yapmış olduğu konuşmaların kaydedilmesinin kanunda suç olarak tanımlanmadığı, şartları oluştuğu takdirde TCK 134. maddesinde düzenlenen özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilebileceği, ancak konuşma içeriklerinin incelenmesinde konuşmaların katılanın özel yaşam alanına dahil ve onun özel hayatının gizliliğini ihlal edecek bir husus konuşulmadığından, sanığın söz konusu konuşma içeriklerini devam eden İş Mahkemesindeki davaya delil olarak sunmasında hukuka aykırı hareket etme bilinciyle de hareket etmemesi nedeniyle, sanığın eyleminde, TCK'nın 134. maddesinde düzenlenen özel hayatın gizliliğini ihlal suçunun yasal unsurlarının da gerçekleşmediği gözetilmeden sanığın CMK'nın 223/2-a maddesi gereğince beraatine karar verilmesi gerekirken aynı kanununun 223/2-e maddesi gereğince beraatine karar verilmesi ... Kanuna aykırı olup ... hükmün düzeltilerek onanmasına ... karar verildi."

16. Yargıtay 12. Ceza Dairesinin 24/3/2021 tarihli ve E.2019/8984, K.2021/3089 sayılı kararının ilgili kısmı şöyledir:

".. Dosya kapsamına göre, iş arkadaşı ve komşusu olan katılan sanık Y. tarafından şahsına sürekli hakaret edildiğini iddia eden sanık T.nin, apartman merdiven boşluğunda karşılaştığı katılan sanık Y. ile aralarında geçen tartışmayı ve bu esnada katılan sanık Y. tarafından söylenen rencide edici sözleri gizlice cep telefonuna kaydedip, söz konusu ses kaydını, şikayet dilekçesindeki iddialarının delili olarak Cumhuriyet Başsavcılığına sunduğu olayda; ses kaydının çözümüne ilişkin 19.08.2015 tarihli bilirkişi raporu ile kolluk görevlilerince düzenlenen 14.01.2015 tarihli tutanak, dosyada mevcut diğer delillerle birlikte değerlendirildiğinde; şikayete konu kaydı, üçüncü kişi ya da kişilerle paylaştığına ve/veya çoğaltarak dağıttığına ilişkin hakkında bir iddia ileri sürülmeyen sanık T.nin, haksız bir saldırı altında ve başkaca şekilde ispatlanması mümkün olmayan bir hal içerisinde iken, kaybolma olasılığı bulunan delillerin muhafazasını sağlayıp katılan sanık Y.nin şahsına yönelik hakaret suçunu işlediğine dair iddialarını ispatlama amacını taşıyan eylemlerinde hukuka aykırı hareket ettiği bilinciyle davranmaması nedeniyle sanık T.nin CMK'nın 223/2-a maddesi gereğince beraatine karar verilmesi gerekirken, sanık T. hakkında aynı Kanun'un 223/2-d maddesi gereğince beraat hükmü kurulması, Kanuna aykırı olup ...hükmün düzeltilerek onanmasına ... karar verildi."

B. Uluslararası Hukuk

17. Avrupa İnsan Hakları Sözleşmesi'nin (Sözleşme) "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesi şöyledir:

"(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."

18. Avrupa İnsan Hakları Mahkemesi (AİHM) kişiler arası ilişkilerde Sözleşme'nin 8. maddesine uyulmasını güvence altına alacak tedbirlerin seçiminin ulusal makamların takdirinde olduğunu, bu konudaki yükümlülüğü yerine getirmenin niteliğinin özel hayata yönelik müdahaleye göre farklılık oluşturabileceğini ifade etmiştir. AİHM, devletlerin Sözleşme'nin 8. maddesi uyarınca uygun bir yasal koruma çerçevesi oluşturma ve uygulama yükümlülüğünün her zaman ceza hükümlerinin tatbik edilmesi anlamına gelmeyeceğini de vurgulamıştır (Söderman/İsveç [BD], B. No: 5786/08, 12/11/2013, § 79; M.P./Portekiz, B. No: 27516/14, 7/9/2021, §§ 40, 41). AİHM, eşlerin birbirlerinin

erişimine rıza gösterdiği bilgilerin hukuk davasında kullanılması suretiyle ifşa edildiği iddiasının incelendiği bir ceza davasının akabinde yapılan başvuruda, ifşa edildiği iddia edilen söz konusu bilgilerin ortak erişime açık olduğuna ve başvuranın özel hayatı üzerindeki etkilerinin sınırlı olduğuna vurgu yapmış; neticede bu bilgilerin hukuk davasında kullanılmasının cezai takibatı gerektirmediği yönünde ulaşılan sonucu özel hayata saygı hakkının öngördüğü pozitif yükümlülüklerin yerine getirilmediği anlamına gelmediğini belirterek sonuca ulaşmıştır (M.P./Portekiz, §§ 46-51).

V. İNCELEME VE GEREKÇE

19. Anayasa Mahkemesinin 29/9/2022 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları

20. Başvurucu;

i. Aleni olmayan bir konuşmasının şüpheli tarafından rızasına aykırı şekilde kayıt altına alınarak ifşa edildiğini, söz konusu ortamda kendisinden ve şüpheliden başka iki kişinin daha bulunduğunu, şüphelinin soruşturulması ve hakkında ceza davası açılması talebiyle suç duyurusunda bulunduğunu ancak Başsavcılık tarafından yapılan değerlendirmelerin hatalı olduğunu, ulaşılan sonucun hukuka uygun olarak nitelendirilemeyeceğini ileri sürmüştür.

ii. Ses kaydının yapıldığı tarihte iddia edildiği gibi bir suçun mevcut olmadığını, ses kaydının planlı şekilde ve suç kastıyla hareket edilerek alındığını, ses kaydının kişisel veri mahiyetinde olup olmadığını tartışılmadığını, Başsavcılığın atıf yaptığı Yargıtay kararının somut olaya uygun olmadığını ifade etmiştir.

iii. İfadesine başvurulmadığını, ses kaydının kime ait olduğunun araştırılmadığını, ses kaydındaki kesinti ve montaj hakkında inceleme yapılmadığını, ses kaydındaki kişilerin ve sesleri duyulan üçüncü kişilerin bilgisine başvurulmadığını, tüm bu nedenlerle etkili soruşturma yapma yükümlülüğünün yerine getirilmediğini belirterek adil yargılanma, özel hayata saygı, kişisel verilerin korunmasını isteme ve hak arama hürriyetinin ihlal edildiğini iddia etmiştir.

B. Değerlendirme

21. Anayasa'nın iddianın değerlendirilmesinde dayanak alınacak 20. maddesinin ilgili kısmı şöyledir:

"Herkes, özel hayatına ... saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ... gizliliğine dokunulamaz.

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

22. Anayasa'nın 5. maddesi şöyledir:

"Devletin temel amaç ve görevleri, ... Cumhuriyeti ve demokrasiyi korumak, kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak; kişinin temel hak ve hürriyetlerini, sosyal hukuk devleti ve adalet ilkeleriyle bağdaşmayacak surette sınırlayan siyasal, ekonomik ve sosyal engelleri kaldırmaya, insanın maddî ve manevî varlığının gelişmesi için gerekli şartları hazırlamaya çalışmaktır."

23. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Başvurucunun şikâyetlerinin özü, özel hayatına ve bu kapsamdaki kişisel nitelikteki birtakım verilerine yönelik saldırılara karşı devletin pozitif yükümlülüklerine uygun şekilde etkili bir ceza soruşturması yürütmediği iddiasıdır. Dolayısıyla başvurunun Anayasa'nın 20. maddesinde düzenlenen özel hayata saygı hakkının güvencelerinden olan kişisel verilerin korunmasını isteme hakkı kapsamında değerlendirilmesi gerektiği sonucuna ulaşılmıştır.

1. Kabul Edilebilirlik Yönünden

24. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan kişisel verilerin korunmasını isteme hakkının ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

2. Esas Yönünden

a. Genel İlkeler

25. Anayasa'nın 20. maddesinin birinci fıkrasında, herkesin özel hayatına saygı gösterilmesini isteme hakkına sahip olduğu düzenlenmiştir. Özel hayat, fiziksel ve ruhsal özerkliği de kapsamakta; bu hak bireyleri gerek kamusal makamların gerek özel hukuk kişilerinin fiziksel ve ruhsal bütünlüğe yönelik saldırılarına karşı korumaktadır (Halime Sare Aysal [GK], B. No: 2013/1789, 11/11/2015, § 48). Ayrıca Anayasa'nın 20. maddesinin üçüncü fıkrasında, herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkının olduğu ifade edilmektedir. Söz konusu anayasal güvence, Sözleşme'nin 8. maddesinde koruma altına alınan özel hayata saygı hakkına karşılık gelmektedir. Kişisel verilerin korunmasını isteme hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe

geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır (AYM, E.2014/122, K.2015/123, 30/12/2015, §§ 19-20).

26. Anayasa Mahkemesi kararlarında belirtildiği üzere kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır (AYM, E.2014/74, K.2014/201, 25/12/2014; E.2014/180, K.2015/30, 19/3/2015). Kişinin görüntüsünün yanında sesinin de kişisel veri mahiyetinde olduğu açıktır. Yine aleni olmayacak şekilde yapılan konuşmalar da kişinin özel hayat alanına dairdir. Dolayısıyla söz konusu değerlere karşı her türlü saldırı karşısında korunmayı talep etme hakkı, özel hayata saygı ile onun daha özel güvencelerinden olan kişisel verilerin korunmasını isteme hakkı kapsamındadır.

27. Anayasa'nın 20. maddesinin üçüncü fıkrasında, genel olarak kişisel verilerin korunmasını isteme hakkı ve bu kapsamdaki özel güvenceler sadece kamu makamlarının müdahalelerine karşı tanınmamıştır. Öte yandan Anayasa'nın 11. maddesinin birinci fıkrasında Anayasa hükümlerinin sadece yasama, yürütme ve yargı organlarını, idare makamlarını ve diğer kuruluşları değil kişileri de bağlayan temel hukuk kuralları olduğu hükmüne yer verilmiştir. Buna göre Anayasa'nın 20. maddesinin üçüncü fıkrası kapsamında kişisel veriler yönünden öngörülen güvenceleri özel kişiler de veri sahiplerine sağlamak zorundadır. Dolayısıyla veri sahiplerine kamu müdahaleleri bakımından sağlanması gereken güvenceler niteliğine uygun düştüğü ölçüde özel kişilerin yaptığı müdahaleler bakımından da geçerlidir. Anılan Anayasa hükümleri Anayasa'nın 5. maddesiyle birlikte ele alındığında devletin bu kapsamdaki pozitif yükümlülüğü, özel kişiler tarafından veri sahiplerinin kişisel verilerine Anayasa'daki güvencelere aykırı olarak müdahale edilmemesini sağlamaktır. Bunun için de kamu makamlarının ve özellikle yargısal makamların özel kişilerin müdahaleleriyle ilgili uyuşmazlıklarda veri sahibinin kişisel verilerine söz konusu güvencelere aykırı müdahalede bulunup bulunulmadığını gerektiği gibi incelemeleri ve bu incelemeyi uygun sonuçlara bağlamaları gerekir.

28. Pozitif yükümlülükler özel hukuk kişilerinin birbirleri ile olan uyuşmazlıklarının çözümüne ilişkin yasal altyapının oluşturulmasını, söz konusu uyuşmazlıkların adil yargılama gereklerine uygun ve usul yönünden güvenceleri haiz bir yargılama kapsamında incelenmesini ve bu yargılamalarda temel haklara ilişkin anayasal güvencelerin gözetilip gözetilmediğinin denetlenmesini gerektirir. Bu doğrultuda derece mahkemelerince söz konusu güvenceler gözardı edilmemeli, taraflar arasındaki çatışan çıkarlar adil biçimde dengelenmeli, kişilerin temel haklarına yönelik müdahalenin meşru amaca dayalı ve ölçülü olup olmadığı değerlendirilmeli, ulaşılan sonuç

hakkında hüküm kurulurken ilgili ve yeterli gerekçeler sunulmalıdır (Ömür Kara ve Onursal Özbek, B. No: 2013/4825, 24/3/2016, §§ 47-50).

29. Dolayısıyla Anayasa'nın 20. maddesinde güvence altına alınan hak kapsamında devletin -pozitif bir yükümlülük olarak- yetki alanında bulunan tüm bireylerin haklarını kamusal makamların yanı sıra diğer bireylerin eylemlerinden kaynaklanabilecek müdahalelere karşı yargısal tedbirler alma yükümlülüğü bulunmaktadır. Ancak bu yükümlülüğün yöntemi konusunda devletin geniş takdir yetkisinin bulunduğu açıktır (Erol Kumcu, B. No: 2015/18988, 9/5/2019, § 33; Ali Çığır, B. No: 2015/19298, 8/5/2019, § 33). Geniş takdir yetkisi kapsamında yerine getirilmesi beklenen söz konusu pozitif yükümlülük özellikle olayın kim tarafından nasıl gerçekleştirildiği konusunda aydınlatılmasını gerekli kılan durumların bulunması hâlinde etkili soruşturma yapılmasını da içerir. Her durumda soruşturmalar ya da yargılamalar neticesinde yargısal makamlarca ulaşılan sonuçların kişisel verilerin korunmasını isteme hakkının içerdiği güvenceleri koruyacak şekilde ilgili ve yeterli gerekçelerle açıklanması gerekir.

b. İlkelerin Olaya Uygulanması

30. Somut olayda başvuru, özel hayat alanında olduğunu ileri sürdüğü bir konuşmanın ve bu suretle sesinin rızası dışında kayıt altına alınarak kullanıldığını ileri sürmüştü; gerçeklerin ortaya çıkarılması ve ismini verdiği bir şüphelinin cezalandırılması talebiyle suç duyurusunda bulunmuştur. Bu durumda başlatılan soruşturmanın yukarıda ifade edilen kişisel verilerin korunmasını isteme hakkının içerdiği güvencelere uygun şekilde yürütülüp yürütülmediği ve neticesinde verilen kararın ilgili ve yeterli gerekçeler içerip içermediği irdelenmelidir.

31. Başvurucunun gizliliğinin korunacağı konusundaki haklı beklentisine dayalı olarak aleni olmayan bir ortamda diğer kişilerle yaptığı konuşmalarının onun rızasına aykırı şekilde kayıt altına alınmasının ve söz konusu ses içeriğinin yine onun rızasına aykırı olarak kullanılmasının özel hayatı kapsamında olan kişisel verilerine saldırı teşkil ettiği ve saldırının anılan hukuki değerler üzerindeki etkilerinin ağır olduğu açıktır.

32. 5237 sayılı Kanun başta olmak üzere mevcut yasal düzenlemelerde, özel hayat alanının parçası olan ve hukuken koruma altında olması gereken kişisel veriler gibi değerlere saldırı teşkil eden eylemler çeşitli tiplerde suç olarak kabul edilmiş ve yaptırımlara bağlanmıştır. Yine ilgili mevzuat kapsamında kişilik haklarına yönelik saldırıların sona erdirilmesi ve zararın tazmin edilmesi hususunda hukuk davaları açılabilir. Dolayısıyla somut olay özelinde kişisel verilerin korunmasını isteme hakkı bakımından yasal altyapının oluşturulduğu anlaşılmıştır. Ayrıca

başvuruya konu olan süreçte başvuruçunun şikâyeti üzerine Başsavcılık tarafından soruşturmaya derhâl başlandığı, bu kapsamda şüphelinin ifadesinin alındığı görülmüştür.

33. Öte yandan soruşturma neticesinde Başsavcılık tarafından yapılan değerlendirmede, şüphelinin delil sunma saikiyle hareket ettiği ve özel hayatın gizliliğini ihlal edecek bir hususun yer almadığı konuşmanın kayda alınmasında ve soruşturma dosyasına delil olarak sunulmasında suç kastının bulunmadığı ifade edilmiştir. Başsavcılık, söz konusu konuşmanın şüpheli M.R.A.nın başvuruçuya olan borcunun ödenmesi sürecine ve başvuruçudan yapılmadığı iddia edilen birtakım iş ve işlemlere ilişkin olduğunu belirtmiştir. Ayrıca delil sunma saikiyle hareket edilmesi durumunda suçun kast unsurunun oluşmayacağını, bu hususa ilişkin Yargıtay içtihadını da gözönüne aldığını ifade etmiştir.

34. Bununla birlikte Başsavcılık, başvuruçunun rızasına aykırı olarak elde edilen ve kullanılan ses kaydının alınma usulünün başvuruçunun temel haklarının korunması konusundaki haklı beklentisine aykırı olmadığına ilişkin olarak ikna edici bir yaklaşım ortaya koyamamıştır. Zira kovuşturmaya yer olmadığına dair verilen kararda, ses kaydını elde eden kişilerin meşru bir amacının bulunduğu ve suç kastının mevcut olmadığı ifade edilmiş ise de başvuruçunun rızasına aykırı şekilde gerçekleştirilen söz konusu eylemlerin onun kişisel verilerini ve özel hayat alanını ne suretle etkilediği hususunda herhangi bir değerlendirme yapılmamıştır.

35. Süreçte verilen kararlarda, özel hayat alanına ve kişisel verilere saldırı teşkil eden bazı eylemlerde belirli şartlarda hukuka uygunluk sebebinin bulunduğunu kabul eden bir Yargıtay kararına atıf yapılmıştır. Anılan Yargıtay kararında ortaya konulan şartların sınırlarının özel hayat alanını korumasız bırakmaya neden olacak şekilde belirsiz olduğu değerlendirilmektedir. Ayrıca mevcut başvuruya konu kararlarda söz konusu şartların somut olay özelinde ne şekilde gerçekleştiği dahi tartışılmamıştır. Yine başvuruçunun özel hayat alanı ile kişisel verilerine saldırı teşkil eden yöntemin ölçülü olup olmadığı ile amaçlananın farklı yöntemlerle elde edilip edilemeyeceği hususlarında açık ve anayasal güvenceleri dikkate alan bir değerlendirme de yapılmamıştır. Çatışan menfaatler arasında hangi tarafa üstünlük tanınacağı konusunda sınırları kesin olmayan ve uygulanması olaya göre değişebilen bir karara atıf yapılmakla yetinilmiş ve somut olay özelinde var olan çatışma hâlindeki menfaatlerin adil biçimde dengelenmesi çabasına girilmemiştir. Delil elde etme amacına kesin şekilde üstünlük veren bu türden bir yaklaşımın kategorik olarak böylesi saldırıların hukuk karşısında himaye edilmesine neden olacağı ve anayasal düzeyde teminat altında olan kişisel verileri ve özel hayat alanını korumasız bırakacağı değerlendirilmektedir.

36. Ayrıca verilen kararlarda, konuşmaların içeriğinin özel hayata ilişkin olup olmadığı bakımından değerlendirmeler yapılarak sonuca gidilmesi ve aleni olmayan konuşmaların Anayasa'nın 20. maddesinin koruma alanının tamamen dışında tutulduğu anlamına gelecek şekilde gerekçeler oluşturulması da anayasal güvencelerle bağdaşmamaktadır. Söz konusu yaklaşım aleni olmayan ortamda yapılan konuşmaları bütün hâlinde özel hayat alanının dışında bırakmaktadır. Bu hususlarla beraber ses kaydında kesinti ya da ekleme işlemlerinin yapılıp yapılmadığının tespit edilmesi konusunda başvurucunun taleplerinin karşılanmaması, ses kaydının planlı şekilde yapıldığı iddiasına ilişkin olarak ismi geçen ilgili diğer kişilerin bilgisine başvurulmaması soruşturmanın açıklığını temin etmemekte; soruşturma sürecinde başvurucunun usule ilişkin güvencelerden yeterli şekilde yararlandırılmadığını göstermektedir.

37. Açıklanan gerekçelerle somut başvuruya konu olan süreçte verilen kararların başvurucunun kişisel verilerin korunmasını isteme hakkının içerdiği güvenceleri koruyacak şekilde ilgili ve yeterli gerekçe içermediği değerlendirilmiştir. Sonuç olarak kamusal makamlarca üstlenilmesi gereken pozitif yükümlülüğün gerektirdiği şartların somut olayda yerine getirilmediği anlaşıldığından Anayasa'nın 20. maddesinde düzenlenen özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiği sonucuna varılmıştır.

3. Giderim Yönünden

38. Başvurucu, ihlalin tespiti ile yeniden soruşturma yapılmasına karar verilmesi talebinde bulunmuştur.

39. Başvuruda tespit edilen hak ihlalinin sonuçlarının ortadan kaldırılması için yeniden soruşturma yapılmasında hukuki yarar bulunmaktadır. Bu kapsamda kararın gönderildiği yargı mercilerince yapılması gereken iş, yeniden soruşturma işlemlerini başlatmak ve Anayasa Mahkemesini ihlal sonucuna ulaştıran nedenleri gideren, ihlal kararında belirtilen ilkelere uygun yeni bir karar vermektir (30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 50. maddesinin (2) numaralı fıkrasında düzenlenen bireysel başvuruya özgü yeniden yargılama kurumunun özelliklerine ilişkin kapsamlı açıklamalar ve benzer yöndeki kararlar için bkz. Mehmet Doğan [GK], B. No: 2014/8875, 7/6/2018, §§ 54-60; Aligül Alkaya ve diğerleri (2), B. No: 2016/12506, 7/11/2019, §§ 53-60, 66; Kadri Enis Berberoğlu (3) [GK], B. No: 2020/32949, 21/1/2021, §§ 93-100). Öte yandan belirtmek gerekir ki kişilerin sorumluluğuna ilişkin hukuki sorunların incelenmesi ve olaya konu eylemin suç tipinin mahiyetinin belirlenmesi ilgili yargı mercilerinin takdirindedir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Kişisel verilerin korunmasını isteme hakkının ihlal edildiğine ilişkin iddianın KABUL EDİLEBİLİR OLDUĞUNA,

B. Anayasa'nın 20. maddesinde güvence altına alınan kişisel verilerin korunmasını isteme hakkının İHLAL EDİLDİĞİNE,

C. Kararın bir örneğinin kişisel verilerin korunmasını isteme hakkına yönelik ihlalin sonuçlarının ortadan kaldırılması için yeniden soruşturma yapılmak üzere İstanbul Cumhuriyet Başsavcılığına (S.2017/145749; K.2018/11270) GÖNDERİLMESİNE,

D. 294,70 TL harç ve 9.900 TL vekâlet ücretinden oluşan toplam 10.194,70 TL yargılama giderinin başvurucuya ÖDENMESİNE,

E. Ödemenin kararın tebliğini takiben başvurucunun Hazine ve Maliye Bakanlığına başvuru tarihinden itibaren dört ay içinde yapılmasına, ödemede gecikme olması hâlinde bu sürenin sona erdiği tarihten ödeme tarihine kadar geçen süre için yasal FAİZ UYGULANMASINA,

F. Kararın bir örneğinin Adalet Bakanlığına GÖNDERİLMESİNE 29/9/2022 tarihinde OYBİRLİĞİYLE karar verildi.

Anayasa Mahkemesi - Fırat Gerçek Kararı (2019/25604)

Fırat Gerçek, B. No: 2019/25604, 21/9/2022

Başvuru, özel bir şirkette çalışan başvurucunun bir iş arkadaşı ile yaptığı cep telefonu yazışmalarının işveren tarafından incelenmesi ve bu yazışmalar gerekçe gösterilerek iş akdinin feshedilmesi nedeniyle özel hayata saygı hakkı ile haberleşme hürriyetinin ihlal edildiği iddialarına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

BİRİNCİ BÖLÜM

KARAR

FIRAT GERÇEK BAŞVURUSU

(Başvuru Numarası: 2019/25604)

Karar Tarihi: 21/9/2022

R.G. Tarih ve Sayı: 15/11/2022-32014

BİRİNCİ BÖLÜM

KARAR

Başkan: Hasan Tahsin GÖKCAN

Üyeler: Muammer TOPAL, Recai AKYEL, Yusuf Şevki HAKYEMEZ, İrfan FİDAN

Raportör: Ferhat YILDIZ

Başvurucu: Fırat GERÇEK

Vekili: Av. Nil Merve ÇELİKBAŞ ŞEKER

I. BAŞVURUNUN KONUSU

1. Başvuru, özel bir şirkette çalışan başvurucunun bir iş arkadaşı ile yaptığı cep telefonu yazışmalarının işveren tarafından incelenmesi ve bu yazışmalar gerekçe gösterilerek iş akdinin feshedilmesi nedeniyle özel hayata saygı hakkı ile haberleşme hürriyetinin ihlal edildiği iddialarına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 19/7/2019 tarihinde yapılmıştır. Komisyon başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar vermiştir.

3. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına gönderilmiştir.

III. OLAY VE OLGULAR

4. Başvuru formu ve eklerinde ifade edildiği ve Ulusal Yargı Ağı Bilişim Sistemi (UYAP) üzerinden tespit edilen şekliyle ilgili olaylar özetle şöyledir:

5. Özel bir şirket çalışanı olan başvurucunun iş sözleşmesi, işveren tarafından 31/10/2017 tarihinde feshedilmiştir. Aynı işyerinde çalışan Ö.Ç. isimli kişiye verilen cep telefonunun incelenmesi sonucunda elde edilen mesaj içerikleri feshin gerekçesi olarak bildirilmiştir.

6. Başvurucu 22/11/2017 tarihinde İstanbul Anadolu 7. İş Mahkemesinde (Mahkeme) işe iade istemiyle dava açmıştır. Dava dilekçesinde başvurucu; iş akdinin haksız olarak feshedildiğini, feshe dayanak yapılan mesajlaşma içeriklerinin bir suretinin fesih bildirimine eklenmediğini, yazışmaların hayal mahsulü olduğunu, şirketin verdiği telefon hatlarının çalışanların özel hayatlarında da kullanıldığını, bu yazışmaların kişisel veri olarak korunması gerektiğini ifade etmiştir.

7. Davalı şirket vekili davaya cevabında; işten ayrılan şirket çalışanı Ö.Ç. ye iş amacıyla tahsis edilen cep telefonunun müşterilerin iletişim bilgilerine ulaşmak için incelendiğini, başvurucu ile Ö.Ç. arasındaki mesajlaşmaların feshe dayanak yapılan içeriklerine ulaşıldığı vurgulanmıştır. Anılan mesaj içeriklerinde şirket çalışanları hakkında rahatsız edici, şirket çalışanlarının görev ve sorumluluklarını yerine getirmekten imtina ettiklerine dair hakaret içeren ifadeler olduğu belirtilmiştir.

8. Mahkeme 31/5/2018 tarihinde davanın reddine karar vermiştir. Kararın gerekçesinde; başvurucu ile Ö.Ç. arasındaki yazışmaların içeriklerine yer verilmiş olup bunların haklı fesih sebebi teşkil edebileceği, cep telefonunun işveren tarafından verilmesi nedeniyle anılan yazışmaların hukuka uygun olarak elde edildiğinin kabulünün gerekeceği vurgulanmıştır.

9. Başvurucu vekilinin anılan karara karşı yaptığı istinaf başvurusu, İstanbul Bölge Adliye Mahkemesi 30. Hukuk Dairesinin (Bölge Adliye Mahkemesi) 28/5/2019 tarihli kararıyla kabul edilmiş, mahkeme kararının kaldırılmasına ve davanın reddine kesin olarak karar verilmiştir. Kararın gerekçesinde; mesaj içeriklerinde kullanılan sözlerin işverenle çalışanlar arasında çalışma barışını bozabilecek ve iş ilişkisini olumsuz etkileyecek nitelikte olduğu, bu açıdan Mahkemece davanın

reddine karar verilmesinde bir isabetsizlik bulunmadığı ifade edilmiştir. Başvurucunun mesajlaştığı Ö.Ç.nin kullandığı cep telefonunun işverene ait olduğu, işverence düzenlenen "İletişim Araçları Politikası" başlıklı belgenin 5.2.4.1 maddesinde "şirkete ait iletişim araçları (bilgisayar, telefon, GSM hat ve diğer) sadece görev nedeniyle ve iş amaçlı olarak kullanılması gerektiği, özel amaçlı haberleşme ve işler için kullanılmaması gerektiği" hususlarının belirtildiği vurgulanmıştır. Bu durumda işverene ait cep telefonunu işverenin incelemesinin özel hayatın gizliliğinin ihlal edildiği ve bu delilin hukuka aykırı şekilde elde edildiği neticesi doğurmayacağı, personelin bu telefon ile özel amaçlı haberleşmesinin yasaklandığı belirtilmiştir. Ancak mahkeme kararında, geçerli nedenle iş akdinin feshedildiği kabul edilmesi gerekirken feshin haklı nedenle yapıldığı yönündeki gerekçenin hatalı olduğu ve bu hususun kamu düzenine aykırılık teşkil edeceği ifade edilmiştir.

10. Nihai karar 25/6/2019 tarihinde başvuru vekiline tebliğ edilmiştir.

IV. İLGİLİ HUKUK

11. İlgili hukuk için bkz. E.Ü. [GK], B. No: 2016/13010, 17/9/2020, §§ 22-51.

V. İNCELEME VE GEREKÇE

12. Anayasa Mahkemesinin 21/9/2022 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları

13. Başvurucu; iş akdinin haksız olarak feshedildiğini, feshe dayanak olan yazışmaların fesih bildirimine eklenmediğini, Ö.Ç. ile mesajlaşmadığını, aksinin kabulü hâlinde mesaj içeriklerinin hukuka aykırı olarak ele geçirildiğini ve kişisel veri niteliğinde olduğunu ileri sürerek özel hayata ve aile hayatına saygı hakkının ihlal edildiğini iddia etmiştir.

B. Değerlendirme

14. Anayasa'nın iddianın değerlendirilmesinde dayanak alınacak "Özel hayatın gizliliği" kenar başlıklı 20. maddesinin birinci ve üçüncü fıkrası şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

...

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de

kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

15. Anayasa'nın "Haberleşme hürriyeti" kenar başlıklı 22. maddesi şöyledir:

"Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.

İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir."

16. Özel hayata saygı hakkı Anayasa'nın 20. maddesinde koruma altına alınmıştır. Bu anlamda devlet, kişilerin özel ve aile hayatına keyfi olarak müdahale etmemek ve üçüncü kişilerin haksız saldırılarını önlemekle yükümlüdür (E.Ü., § 56). Ayrıca Anayasa'nın 22. maddesinde güvence altına alınan haberleşme hürriyeti, haberleşmenin yanında içeriği ve biçimi ne olursa olsun haberleşmenin içeriğinin gizliliğini de güvence altına almaktadır. Haberleşme bağlamında bireylerin karşılıklı ve toplu olarak sözlü, yazılı ve görsel iletişimlerine konu olan ifadelerinin gizliliğinin sağlanması ve haberleşmeye yönelik haksız müdahalelerde bulunulmaması gerekir (Yasemin Çongar ve diğerleri, B. No: 2013/7054, 6/1/2015, § 49; E.Ü., § 60).

17. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Somut olayda işverenin çalışanlara verdiği cep telefonundaki mesajlaşmaları denetlemesi ve içeriğini incelemesi sonucu elde ettiği bilgileri iş akdinin feshine dayanak yapması söz konusudur. Dolayısıyla başvurucağın iş arkadaşı ile cep telefonu üzerinden gerçekleştirdiği yazışmaların incelendiği ve içeriklerine ulaşıldığı gözetildiğinde başvurucağın özel hayata saygı hakkı ile haberleşme hürriyeti yönünden incelenmesi gerektiği değerlendirilmiştir.

1. Kabul Edilebilirlik Yönünden

18. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan özel hayata saygı hakkı ile haberleşme hürriyetinin ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

2. Esas Yönünden

a. Genel İlkeler

19. Anayasa ve Avrupa İnsan Hakları Sözleşmesi'nin ortak koruma alanı kapsamında kalan temel haklar, yalnızca kamusal gücün doğrudan uygulanmasıyla değil kimi zaman da özel hukuk kişileri arasındaki uyuşmazlıklara konu olacak şekilde üçüncü kişilerin müdahaleleriyle zedelenebilmektedir. Anayasa Mahkemesi özel hukuk kişileri arasındaki uyuşmazlıkların devletin pozitif yükümlülükleri kapsamında incelenebileceğini çeşitli kararlarında vurgulamıştır (Ömür Kara ve Onursal Özbek, B. No: 2013/4825, 24/3/2016, § 46; Ali Çığır, B. No: 2015/19298, 8/5/2019, §§ 32, 33; Erol Kumcu, B. No: 2015/18988, 9/5/2019, §§ 32, 33; U.B., B. No: 2015/3175, 10/10/2019, §§ 33, 34; E.Ü., § 65).

20. Pozitif yükümlülükler özel hukuk kişilerinin birbirleri ile olan uyuşmazlıklarının çözümüne ilişkin yasal altyapının oluşturulmasını, söz konusu uyuşmazlıkların adil yargılama gereklerine uygun ve usul yönünden güvenceleri haiz bir yargılama kapsamında incelenmesini, bu yargılamalarda temel haklara ilişkin anayasal güvencelerin gözetilip gözetilmediğinin denetlenmesini gerektirir. Bu doğrultuda derece mahkemelerince söz konusu güvenceler gözardı edilmemeli, işveren ve çalışanlar arasındaki çatışan çıkarlar adil biçimde dengelenmeli, başvuruların temel haklarına yönelik müdahalenin meşru amaca dayalı ve ölçülü olup olmadığı değerlendirilmeli, ulaşılan sonuç hakkında hüküm kurulurken ilgili ve yeterli gerekçeler sunulmalıdır (Ömür Kara ve Onursal Özbek, §§ 47-50; E.Ü., § 66).

21. Anayasa Mahkemesi daha önce iletişim araçlarının işveren tarafından denetlenmesi kapsamındaki uyuşmazlıklarda derece mahkemeleri tarafından devletin pozitif yükümlülükleri bağlamında çıkarların dengelenmesi ve müdahalenin ölçülülüğünün irdelenmesi kapsamında gözetilmesi gereken hususları genel olarak belirlemiş; buna göre somut olayın koşullarına göre iş sözleşmelerinde kısıtlayıcı ve zorlayıcı düzenlemelerin ne şekilde belirlendiği, tarafların bu düzenlemeler hakkında bilgilendirilip bilgilendirilmediği, çalışanların temel haklarına yönelik müdahalede bulunulmasına neden olan meşru amacın müdahale ile ölçülü olup olmadığı, sözleşmenin feshinin çalışanların eylem ya da eylemsizlikleri karşısında makul ve orantılı bir işlem olup olmadığı hususlarının uyuşmazlığın çözümünde gözetilmesi gerektiğini tespit etmiştir (Ömür Kara ve Onursal Özbek, § 50; E.Ü., § 67).

22. Yukarıda belirtilen hususlar gözetilerek işverenin işçinin iletişimini denetlemesi yetkisini özel hayata saygı hakkı ve haberleşme hürriyeti bağlamında devletin pozitif yükümlülükleri kapsamında irdelenmek gerekmektedir. Öncelikle somut olayda olduğu gibi teknolojik gelişmelerin imkânlarından

yararlanmak isteyen işverenlerin bilgisayar, internet, e-posta veya cep telefonu gibi iletişim araç ve gereçlerini çalışanın kullanıma sunması nedeniyle oluşan uyuşmazlıklarda işverenin menfaatleri ile işçinin temel hak ve özgürlükleri arasında bir dengeleme yapma gerekliliği doğmaktadır. Bu bağlamda işveren ile çalışan arasındaki ilişkinin iki taraf açısından da belirli hak ve yükümlülükler öngören ve esasen güven ilişkisi üzerine kurulu iş sözleşmesiyle şekillendiği unutulmamalıdır. Somut uyuşmazlığın ilgili olduğu iş hukukunun dinamik bir nitelik taşıdığı, ayrıca iş ilişkilerinin genel kurallardan farklı, kendine özgü bazı hukuki kurallar içerdiği de dikkate alınmalıdır (E.Ü., § 68).

23. Bu bağlamda işlerin etkin bir şekilde yürütülmesi ile bilgi akışının kontrolünü sağlamak, işçinin eylemlerine bağlı cezai ve hukuki sorumluluğa karşı korunmak, verimliliği ölçmek veya güvenlik endişeleri gibi haklı ve meşru görülebilecek nedenlerle işverenin yönetim yetkisi kapsamında kural olarak işçinin kullanımına sunduğu iletişim araçlarını denetleyebileceği ve kullanıma ilişkin sınırlamalar öngörebileceği söylenebilir. Ancak işverenin yönetim yetkisinin işyerinde işin yürütülmesi, işyerinin düzeninin ve güvenliğinin sağlanmasıyla sınırlı olduğu unutulmamalıdır. Bu bağlamda işverenin yetki ve haklarının sınırsız olmadığı, çalışana tanınan temel hak ve özgürlüklerin somut olayda haberleşme hürriyeti ve özel hayata saygı hakkının işyeri sınırları dâhilinde de korunduğu, aynı zamanda kısıtlayıcı ve uyulması zorunlu işyeri kurallarının çalışanların temel haklarının özünü zedeleyecek nitelikte olmaması gerektiği vurgulanmalıdır. Bu çerçevede işyerinde kullanıma sunulan iletişim araçlarının işverene ait olduğu gözetilerek sırf bu nedenle bile işverenin iletişim araçları üzerinde sınırsız ve mutlak bir gözetleme ve denetleme yetkisinin olduğunu kabul etmek, işçinin demokratik bir toplumda temel hak ve özgürlüklerine işyerinde de saygı gösterilmesi gerektiği yönündeki haklı beklentisiyle uyuşmayacaktır (E.Ü., § 69).

24. Nitekim Anayasa Mahkemesi benzer bir olaya ilişkin E.Ü. kararında derece mahkemelerince aşağıda belirtilen güvenceleri olayda hakka müdahale eden üçüncü kişinin sağlayıp sağlamadığının gereği gibi denetlenip denetlenmediğini incelemek gerektiğini vurgulamıştır (E.Ü., § 70):

i. İşverenin çalışanın kullanımına sunduğu iletişim araçlarının ve iletişim içeriklerini incelemesinin haklı olduğunu gösteren meşru gerekçeleri olup olmadığı denetlenmelidir. Bu durumda işverenin gerekçelerinin ifa edilen işin ve işyerinin özellikleri de gözetilerek meşru olup olmadığı irdelenmelidir. Bu denetlemede iletişim akışı ile iletişim içeriklerinin incelenmesi arasında ayırım yapılarak içeriklerin incelenmesi yönünden daha ciddi gerekçeler aranmalıdır.

ii. Demokratik bir toplumda iletişimin denetlenmesi ve kişisel verilerin işlenmesi süreci şeffaf bir şekilde gerçekleştirilmeli ve bunun bir gereği olarak da süreçle ilgili olarak çalışanlar işveren tarafından önceden bilgilendirilmelidir. Uluslararası hukuk ve karşılaştırmalı hukuk dikkate

alındığında bu bilgilendirmenin -somut olayın özelliklerine uygun düştüğü ölçüde- en azından iletişimin denetlenmesi ile kişisel verilerin işlenmesinin hukuki dayanağı ve amaçları, denetlemenin ve veri işlemenin kapsamı, verilerin saklanacağı süre, veri sahibinin hakları, denetlemenin ve işlemenin sonuçları ile verilerin muhtemel yararlanıcıları hususlarını kapsamaması gerekir. Ayrıca bildirimde iletişim araçlarının kullanımına ilişkin olarak işveren tarafından öngörülen sınırlamalara da yer verilmelidir. Bilgilendirmenin mutlaka belli şekilde yapılması şart olmayıp şeffaflığı sağlamak bakımından bireylere kişisel verilerin işlenmesine ve iletişimin denetlenmesine ilişkin süreçten yukarıda belirtilen kapsamda haberdar olma imkânı sağlayan uygun bir yöntem tercih edilebilir.

iii. Çalışanın temel hak ve hürriyetlerine işveren tarafından yapılan müdahale, ulaşılmak istenen amaç ile ilgili ve bu amacı gerçekleştirmeye elverişli olmalıdır. Ayrıca inceleme faaliyetiyle elde edilen verilerin işveren tarafından hedeflenen amaç doğrultusunda kullanılması gerekir.

iv. İşveren tarafından yapılan müdahalenin gerekli kabul edilebilmesi için aynı amaca daha hafif bir müdahale ile ulaşılabilecek şekilde mümkün olmamalı, müdahale ulaşılmak istenen amaç bakımından zorunlu olmalıdır. Çalışanın iletişiminin içeriğine girilmesi yerine daha az müdahale içeren yöntem ve tedbirlerin uygulanmasının mümkün olup olmadığı denetlenmelidir. Bu kapsamda işverenin ulaşmak istediği amaca çalışanın iletişimi incelenmeden de erişme imkânı olup olmadığı her bir vakianın somut özellikleri ışığında değerlendirilmelidir.

v. Müdahalenin orantılı kabul edilebilmesi için iletişimin denetlenmesi ile işlenecek veya herhangi bir şekilde yararlanılacak veriler, ulaşılmak istenen amaçla sınırlı olmalı; bu amacı aşacak şekilde sınırlama ya da müdahaleye izin verilmemelidir.

vi. Ayrıca iletişimin incelenmesinin muhatabı olan çalışan üzerindeki etkisi ve çalışan bakımından sonuçları gözönünde tutularak tarafların çatışan menfaat ve haklarının adil bir biçimde dengelenip dengelenmediğine bakılması gerekmektedir. Taraflardan birine şahsi olarak aşırı bir külfet yüklediğinin tespiti hâlinde devletin pozitif yükümlülüklerini yerine getirmediği sonucuna varılabilir.

b. İlkelerin Uygulanması

25. Başvurucu; cep telefonundaki yazışmalarının incelenmesinin özel hayat alanına ve haberleşme hürriyetine haksız bir müdahale oluşturmasına rağmen açtığı işe iade istemli davasında bu yönde bir tespit yapılmadığını, yazışmalarının işveren tarafından hukuka aykırı yöntemlerle elde edildiğini iddia etmiştir. Bu kapsamdaki iddiaların yukarıda belirtilen esaslar gözetilerek devletin pozitif yükümlülükleri bağlamında değerlendirilmesi gerekmektedir.

26. Öncelikle işverenin işçinin kullanımına sunulan iletişim araçlarını denetlemesine ilişkin olarak 4857 sayılı Kanun'da özel bir düzenleme olmadığı görülmüştür. Ancak Anayasa'nın 20. ve 22. maddelerinde yer bulan özel hayata saygı hakkına ve haberleşme hürriyetine ilişkin güvenceler ile hukuk sistemimizde mevcut olan düzenlemelerin iş hukuku uyumsuzluklarında uygulanması yönünde bir engel olmadığı gözetildiğinde yasal altyapı oluşturmak bağlamında pozitif yükümlülüklerin yerine getirilmiş olduğu söylenebilir (E.Ü., § 72).

27. Başvuru konusu olayda başvurucunun çalıştığı şirketten ayrılan Ö.Ç. isimli işçi, şirket tarafından kendisine verilen cep telefonunu işten ayrıldıktan bir süre sonra şirkete iade etmiştir. Anılan cep telefonunun Ö.Ç.'nin işle ilgili iletişimlerinin tespiti amacıyla incelendiği ve başvurucu ile Ö.Ç. arasındaki mesajlaşmalara erişildiği anlaşılmıştır. Bununla birlikte davalı şirket dilekçeleri ve yargı kararlarından başvurucu ile iş arkadaşı Ö.Ç. arasındaki mesajlaşmaların işveren ve çalışanları hakkında özel görüşler içerdiği, içeriğinde bazı küçük düşürücü ifadelerin bulunduğu hususunun tespit edildiği görülmüştür.

28. Somut olayda Bölge Adliye Mahkemesi kararında "İletişim Araçları Politikası" başlıklı, genel bir düzenleme içerdiği anlaşılan belgede işverene ait olup da işçiye verilen iletişim araçlarının iş amaçlı kullanılması gerektiğinin belirlendiğini vurgulamıştır. Ancak anılan belgede iletişim araçlarının inceleme ve denetleme yetkisini, kullanım sınırlarını ve bu sınırların aşılması durumuna bağlı yaptırımın açıkça düzenlenip düzenlenmediği ve anılan belgenin işçilere aydınlatma yükümlülüğü kapsamında bildirilip bildirilmediği hususlarının tartışılmadığı görülmüştür.

29. İstinaf merciinin gerekçelerinin başvurucuya özgü belge ve iletişim araçları üzerinden değil Ö.Ç. isimli işçi bağlamında Ö.Ç.'nin kullanımına sunulan telefon üzerinden ortaya konulduğu anlaşılmıştır. Bu durumda başvurucuya/işçilere, işveren tarafından teslim edilen iletişim araçlarının kullanım sınırları, işverenin anılan araçları inceleme/denetleme yetkisi ve amaca aykırı kullanılmasına bağlanan yaptırım hususunu da içerecek şekilde aydınlatma yükümlülüğünün yerine getirildiği, Mahkemenin de başvurucu özelinde bu yönde bir bilgilendirmenin yapılıp yapılmadığına dair bir araştırma yaptığı söylenemez. Bunun yanında işveren, Ö.Ç.'nin kullanımında olan telefonda amaçla uyumlu ve sınırlı bir inceleme yaptığını ortaya koyamamıştır. Zira işveren yargılama sürecinde müşteri iletişim bilgilerine ulaşmak adına telefonda inceleme yapıldığını savunsa da telefonda ele geçirilen ve feshe dayanak teşkil eden mesaj içerikleri bu durumu doğrulamamıştır.

30. Kaldı ki mesajlaşma programlarının kişisel olarak da kullanılabileceği gözetildiğinde bir başkasına ait olan cep telefonunun denetlenmesinin ve başvurucuya ait mesajların ele geçirilmesinin başvurucunun özel hayatının ve haberleşmesinin gizliğinin korunması konusundaki makul

beklentisine aykırı olduğu açıktır. Mahkemece de bir başkasına ait cep telefonunda yer alan yazışmaların ne suretle denetlendiğine, mesaj içeriklerinin feshe dayanak alınmasının gerekli olup olmadığına ve başvuruçunun özel hayatı ile haberleşmesine olan etkisine yönelik herhangi bir değerlendirme yapılmamıştır (benzer değerlendirmeler için bkz. Samet Ayyıldız, B. No: 2018/34548, 28/12/2021, §§ 36-46).

31. Nitekim Anayasa Mahkemesi başvuruya benzer olayları incelediği E.Ü. ve Samet Ayyıldız kararlarında, başvuruçuların kurumsal e-posta ve kişisel Whatsapp hesabı içeriklerinin işveren tarafından denetlenmesi ve bu yazışmalar gerekçe gösterilerek iş akdinin feshedilmesi şeklindeki müdahalelerde ihlal kararları vermiştir. Somut olayda da yukarıda belirtilen gerekçelerle anılan kararlardaki ilkelerden ayrılmayı gerektirir bir durum bulunmadığı sonucuna ulaşılmıştır.

32. Açıklanan gerekçelerle özel hukuk iş ilişkilerinden doğan uyuşmazlığı karara bağlayan derece mahkemeleri tarafından yukarıda belirtilen anayasal güvenceleri gözetilen özenli bir yargılama yapılarak pozitif yükümlülüklerin yerine getirilmediği anlaşıldığından başvuruçunun Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkı ile Anayasa'nın 22. maddesinde güvence altına alınan haberleşme hürriyetinin ihlal edildiğine karar verilmesi gerekir.

3. Giderim Yönünden

33. Başvuruçucu; ihlalin tespit edilmesini, yeniden yargılama yapılmasını ve 2.700,91 TL'lik yargılama masrafının maddi tazminat olarak ödenmesini talep etmiştir. Başvuruçucu manevi tazminat talebinde bulunmamıştır.

34. Tespit edilen ihlalin ve sonuçlarının ortadan kaldırılmasına ilişkin usul ve esaslar 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 50. maddesinde yer almaktadır.

35. Başvuruda tespit edilen hak ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmasında hukuki yarar bulunmaktadır. Bu kapsamda kararın gönderildiği yargı mercilerince yapılması gereken iş yeniden yargılama işlemlerini başlatmak ve Anayasa Mahkemesini ihlal sonucuna ulaştıran nedenleri gideren, ihlal kararında belirtilen ilkelere uygun yeni bir karar vermektir (6216 sayılı Kanun'un 50. maddesinin (2) numaralı fıkrasında düzenlenen bireysel başvuruya özgü yeniden yargılama kurumunun özelliklerine ilişkin kapsamlı açıklamalar için bkz. Mehmet Doğan [GK], B. No: 2014/8875, 7/6/2018, §§ 54-60; Aligül Alkaya ve diğerleri (2), B. No: 2016/12506, 7/11/2019, §§ 53-60, 66; Kadri Enis Berberoğlu (3) [GK], B. No: 2020/32949, 21/1/2021, §§ 93-100).

36. Anayasa Mahkemesinin maddi tazminata hükmedebilmesi için başvuruçunun uğradığını iddia ettiği maddi zarar ile tespit edilen ihlal arasında illiyet bağı bulunmalıdır. Başvuruçunun ödemek zorunda kaldığı yargılama giderlerini tazminat olarak talep etmesi nedeniyle maddi tazminat talebinin reddine karar verilmesi gerekir.

37. Dosyadaki belgelerden tespit edilen 364,60 TL harç ve 9.900 TL vekâlet ücretinden oluşan toplam 10.264,60 TL yargılama giderinin başvuruçuya ödenmesine karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Özel hayata saygı hakkı ile haberleşme hürriyetinin ihlal edildiğine ilişkin iddianın KABUL EDİLEBİLİR OLDUĞUNA,

B. Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkı ve Anayasa'nın 22. maddesinde güvence altına alınan haberleşme hürriyetinin İHLAL EDİLDİĞİNE,

C. Kararın bir örneğinin özel hayata saygı hakkı ile haberleşme hürriyetinin ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmak üzere İstanbul Anadolu 7. İş Mahkemesine (E.2017/1006, K.2018/246) GÖNDERİLMESİNE,

D. Başvuruçunun maddi tazminat talebinin REDDİNE,

E. 364,60 TL harç ve 9.900 TL vekâlet ücretinden oluşan toplam 10.264,60 TL yargılama giderinin başvuruçuya ÖDENMESİNE,

F. Ödemenin kararın tebliğini takiben başvuruçunun Hazine ve Maliye Bakanlığına başvuru tarihinden itibaren dört ay içinde yapılmasına, ödemede gecikme olması hâlinde bu sürenin sona erdiği tarihten ödeme tarihine kadar geçen süre için yasal FAİZ UYGULANMASINA,

G. Kararın bir örneğinin bilgi için İstanbul Bölge Adliye Mahkemesi 30. Hukuk Dairesine (E.2018/3120, K.2019/1263) GÖNDERİLMESİNE,

H. Kararın bir örneğinin Adalet Bakanlığına GÖNDERİLMESİNE 21/9/2022 tarihinde OYBİRLİĞİYLE karar verildi.

Anayasa Mahkemesi - Ümit Karaduman Kararı (2020/20874)

Ümit Karaduman, B. No: 2020/20874, 2/2/2022

Başvuru, tutuklu olan başvurucuya gelen veya başvurucu tarafından gönderilen mektupların Ulusal Yargı Ağı Bilişim Sistemi'ne kaydedilmesi nedeniyle özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ihlal edildiği iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

İKİNCİ BÖLÜM

KARAR

ÜMİT KARADUMAN BAŞVURUSU

(Başvuru Numarası: 2020/20874)

Karar Tarihi: 2/2/2022

R.G. Tarih ve Sayı: 7/4/2022-31802

İKİNCİ BÖLÜM

KARAR

Başkan: Kadir ÖZKAYA

Üyeler: Engin YILDIRIM, M. Emin KUZ, Rıdvan GÜLEÇ, Basri BAĞCI

Raportör: Ali KOZAN

Başvurucu: Ümit KARADUMAN

I. BAŞVURUNUN KONUSU

1. Başvuru, tutuklu olan başvurucuya gelen veya başvurucu tarafından gönderilen mektupların Ulusal Yargı Ağı Bilişim Sistemi'ne kaydedilmesi nedeniyle özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ihlal edildiği iddiasına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 1/7/2020 tarihinde yapılmıştır.
3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.
4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.
5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.
6. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık, görüşünü bildirmiştir.
7. Başvurucu, Bakanlık görüşüne karşı beyanda bulunmuştur.

III. OLAY VE OLGULAR

8. Başvuru formu ve eklerinde ifade edildiği şekliyle olaylar özetle şöyledir:
9. Başvurucu, silahlı terör örgütüne üye olma suçundan 13/2/2018 tarihinde tutuklanmıştır. Başvurucu hâlen Tekirdağ 1 No.lu T Tipi Kapalı Ceza İnfaz Kurumunda (İnfaz Kurumu) tutuklu olarak bulunmaktadır.
10. Ceza ve Tevkifleri Genel Müdürlüğünün 10/10/2016 tarihli Genelge'si (Genelge) ile infaz kurumunda bulunan hükümlü ve tutukluların resmî makamlara veya savunması için avukatına verdiği kapalı zarf içindeki mektup ve faksler hariç olmak üzere tüm mektup, faks ve dilekçelerinin taranmak suretiyle Ulusal Yargı Ağı Bilişim Sistemi'ne (UYAP) kaydedilmesi gerektiği ülke genelindeki infaz kurumlarına başsavcılıklar aracılığıyla iletilmiştir. İnfaz kurumları da Genelge içeriğine uygun uygulama başlatmıştır. Başvurucunun gönderdiği ve kendisine gelen mektuplar da anılan Genelge kapsamında UYAP'a kaydedilmiştir.
11. Başvurucu; gönderdiği ve kendisine gelen mektupların UYAP'a kaydedilmesi uygulamasının sonlandırılması ve kayıtların silinmesi talebiyle 27/2/2020 tarihinde Tekirdağ 2. İnfaz Hâkimliğine (İnfaz Hâkimliği) başvurmuştur. Başvurucu dilekçesinde; kendisine gelen ve gönderdiği mektupların kalıcı bir şekilde sisteme kaydedilmesinin yasal dayanağının olmadığını, bu uygulamaya son verilmesine ve kayıtların silinmesine dair taleplerine İnfaz Kurumu tarafından cevap verilmediğini vurgulayarak özel hayata saygı hakkı ile masumiyet karinesinin ihlal edildiğini ileri sürmüştür.
12. İnfaz Hâkimliği; Bakanlığın anılan yazısını ve Anayasa Mahkemesinin ilgili kararını hatırlattıktan sonra 13/12/2004 tarihli ve 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun'un 68.

maddesinin (2) numaralı fıkrasında hükümlü tarafından gönderilen ve kendisine gelen mektup, faks ve telgrafların mektup okuma komisyonu, komisyon bulunmaması hâlinde ise kurumun en üst amirince denetleneceğinin düzenlendiğini vurgulamıştır. Somut olayda anılan hükme göre işlem yapıldığını, bu uygulamanın Anayasa'ya aykırı bulunmadığını ifade etmiştir.

13. Başvurucunun anılan karara itirazı Tekirdağ 2. Ağır Ceza Mahkemesinin 4/6/2020 tarihli kararıyla reddedilmiştir.

14. Nihai karar, başvurucuya 15/6/2020 tarihinde tebliğ edilmiştir.

15. Başvurucu 1/7/2020 tarihinde bireysel başvuruda bulunmuştur.

16. Danıştay İdari Dava Daireleri Kurulu 14/9/2020 tarihli ve 2020/403 sayılı kararı ile anılan Genelge'nin yürütmesinin durdurulmasına karar vermiştir. Kararın ilgili kısmı şu şekildedir:

"5275 sayılı Kanun'da yer verilen her türlü ceza muhakemesi işlemlerinde Ulusal Yargı Ağı Bilişim Sistemi (UYAP) kullanılacağı kuralı ve ilgili diğer mevzuat hükümleri uyarınca, hükümlü ve tutukluların avukatlarına verdiği kapalı zarf içerisindeki mektup ve fakslar dışında kalan yazışmaların taranmak suretiyle UYAP sistemine kaydedilmesine imkân bulunmakla birlikte; bu kayıt işleminin sınırsız ve koşulsuz olduğunun kabulü mümkün değildir.

Söz konusu kayıt yetkisinin; 5275 sayılı Kanun ve Ceza İnfaz Kurumlarının Yönetimi ile Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Tüzük'te yer alan kurallar çerçevesinde verilen denetleme yetkisinin kapsam ve sınırları içinde ve bunu ihlal etmeyecek biçimde düzenlenmesi gerekmektedir.

Bu bağlamda, anılan Tüzük'te mektup okuma komisyonunun ne şekilde çalışacağı ayrıntılı bir şekilde belirlenmiş, hükümlü tarafından alınan ve gönderilen mektupların sakıncalı olup olmamasına göre farklı usuller getirilmiştir. Buna göre, fiziki ortamda sakıncalı olmayan mektupların ilgiliye teslim edilmesi hususu düzenlenirken, bir kopyasının muhafaza edilmesi öngörülmediği halde, dava konusu işlemle UYAP'a kaydedilecek evraklar hususunda bir istisna öngörülmediğinden, bu durum, herhangi bir sakınca içermeyen, tamamen özel nitelikte olan ve kişisel mahremiyet kapsamında bulunan mektupların dahi zaman ve nitelik sınırlaması olmaksızın elektronik ortama kaydedilmesi sonucunu doğuracaktır.

Bakanlığın yazısında tüm hükümlü ve tutukluların resmi makamlara veya savunması için avukatına verdiği kapalı zarf içindeki mektup ve fakslar hariç, diğer tüm faks ve dilekçelerin taranmak suretiyle UYAP sistemine kaydedilmesi gerektiği belirtildiğinden, tutuklu ve hükümlülerin yargısal süreçlerle hiçbir ilgisi olmayan kişisel verilerini de içerebilecek olan özel yazışmaları da sakıncalı olup olmadığına bakılmaksızın UYAP sistemine kaydedilecektir. Bu özel yazışmaların ne kadar süreyle

sistemde saklı tutulacağı, bunların üçüncü kişilerin erişimine ve kullanımına açılıp açılmayacağı, infaz kurumu tarafından hangi mercilerle paylaşılıp paylaşılamayacağı ve bunun nasıl olacağı hususlarında belirsizlik söz konusudur.

Bu itibarla, dava konusu işlemin hükümlü ve tutuklular tarafından herhangi bir sakınca içermeyen, tamamen özel nitelikte olan veya önleyici, koruyucu önlemler açısından herhangi bir değer taşımayan, kişisel mahremiyet kapsamında bulunan mektup ve belgelerin süresiz şekilde elektronik ortama kaydedilmesi sonucunu doğuracak olan ve ayrıca söz konusu mektup ve belgelerin kaydı, muhafazası, erişimi ve imhası hususunda herhangi bir sınır ve koşul getirmeyen dava konusu işlemin bu haliyle ve yönleriyle hukuka aykırı olduğu ve uygulanması halinde telafisi güç mağduriyetlere yol açabileceği sonucuna ulaşılmıştır."

IV. İLGİLİ HUKUK

A. Ulusal Hukuk

17. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Amaç" kenar başlıklı 1. maddesi şöyledir:

"Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir."

18. 6698 sayılı Kanun'un "Tanımlar" kenar başlıklı 3. maddesinin (1) numaralı fıkrasının ilgili kısmı şöyledir:

" ...

d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade eder."

19. 6698 sayılı Kanun'un "Kişisel verilerin işleme şartları" kenar başlıklı 5. maddesinin ilgili kısmı şöyledir:

" (1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

...

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

..."

20. 6698 sayılı Kanun'un "Özel nitelikli kişisel verilerin işleme şartları" kenar başlıklı 6. maddesinin ilgili kısmı şöyledir:

"(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

..."

21. 6698 sayılı Kanun'un "İstisnalar" kenar başlıklı 28. maddesinin ilgili kısmı şöyledir:

"(1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:

...

ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi".

22. 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu'nun "Elektronik işlemler" kenar başlıklı 38/A maddesinin ilgili kısmı şöyledir:

"(1) Her türlü ceza muhakemesi işlemlerinde Ulusal Yargı Ağı Bilişim Sistemi (UYAP) kullanılır. Bu işlemlere ilişkin her türlü veri, bilgi, belge ve karar, UYAP vasıtasıyla işlenir, kaydedilir ve saklanır.

...

(7) Zorunlu nedenlerle fiziki olarak düzenlenmiş belge veya kararlar, yetkili kişilerce taranarak UYAP'a aktarılır ve gerektiğinde ilgili birimlere elektronik ortamda gönderilir.

...

(9) Elektronik ortamda yapılan işlemlerde süre gün sonunda biter.

...

(11) Ceza muhakemesi işlemlerinin UYAP'ta yapılmasına dair usul ve esaslar, Adalet Bakanlığı tarafından çıkarılacak yönetmelikle düzenlenir."

23. Bakanlık Bilgi İşlem Dairesi Başkanlığının 10/11/2011 tarihli ve 124/1 sayılı Genelge'sinin ilgili kısmı şöyledir:

"UYAP Bilişim Sistemi kullanılarak soruşturma ve kovuşturma işlemleri ile diğer adlî ve idarî işlemlerin etkin, verimli, hızlı, düzenli, şeffaf ve usul ekonomisine uygun biçimde yürütülmesi amacıyla;

1- Her türlü işlem ve faaliyetin, UYAP üzerinden gerçekleştirilmesine imkân bulunmayan istisnai hâller saklı olmak koşuluyla, UYAP ortamında, zamanında, eksiksiz ve doğru bir biçimde gerçekleştirilmesi,

...

3- Tüm birimlerde her türlü veri girişinin eksiksiz ve doğru biçimde yapılması,

...

5- Zorunluluk sebebiyle haricen oluşturulan belgeler ile Sistem haricinde gelen belgelerin ekleriyle birlikte taranarak UYAP ortamına aktarılması,

...

15- Bilgi güvenliği, elektronik imza ve kişisel verilerin korunmasına ilişkin mevzuat hükümlerine azamî dikkat gösterilmesi, özellikle elektronik imza cihazı veya erişim kodu ile her türlü kullanıcı adı ve parolasının başkalarına verilmemesi ..."

24. 5275 sayılı Kanun'un "Hükümlünün mektup, faks ve telgrafları alma ve gönderme hakkı" kenar başlıklı 68. maddesinin başvuru tarihi itibarıyla yürürlükteki hâli şöyledir:

"(1)Hükümlü, bu maddede belirlenen kısıtlamalar dışında, kendisine gönderilen mektup, faks ve telgrafları alma ve ücretleri kendisince karşılanmak koşuluyla, gönderme hakkına sahiptir.

(2) Hükümlü tarafından gönderilen ve kendisine gelen mektup, faks ve telgraflar; mektup okuma komisyonu bulunan kurumlarda bu komisyon, olmayanlarda kurumun en üst amirince denetlenir.

(3) Kurumun asayiş ve güvenliğini tehlikeye düşüren, görevlileri hedef gösteren, terör ve çıkar amaçlı suç örgütü veya diğer suç örgütleri mensuplarının haberleşmelerine neden olan, kişi veya kuruluşları paniğe yöneltecek yalan ve yanlış bilgileri, tehdit ve hakareti içeren mektup, faks ve telgraflar hükümlüye verilmez. Hükümlü tarafından yazılmış ise gönderilmez.

(4) Hükümlü tarafından resmî makamlara veya savunması için avukatına gönderilen mektup, faks ve telgraflar denetime tâbi değildir."

25. 6/4/2006 tarihli ve 26131 sayılı Resmî Gazete'de yayımlanan Ceza İnfaz Kurumlarının Yönetimi ile Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Tüzük'ün (Tüzük) "Mektupların gönderilmesi ve gelen mektupların verilmesi" kenar başlıklı 122. maddesi şöyledir:

"(1) 91 inci maddeye göre mektup alma ve gönderme hakkı kapsamında hükümlüler tarafından yazılan mektup, faks ve telgraflar, zarfı kapatılmaksızın bu işle görevlendirilen ikinci müdür başkanlığında, idare memuru ve yüksek okul mezunu iki infaz ve koruma memuru tarafından oluşturulan mektup okuma komisyonuna iletilmek üzere güvenlik ve gözetim servisi personeline verilir. Yapılan incelemeden sonra gönderilmesinde sakınca görülmeyen mektuplar üzerine "görüldü" kaşesi vurulur, zarf içerisine konularak kapatılır ve postaneye teslim edilir.

(2) Resmî makamlara veya savunması için avukatına gönderilenler hakkında 91 inci maddenin dördüncü fıkrası hükmü uygulanır.

(3) Hükümlülere gönderilen ve açılıp incelendikten sonra verilmesinde sakınca olmadığı anlaşılan mektup, faks ve telgraflar zarfları ile birlikte verilir."

26. Tüzük'ün "Sakıncalı görülen mektuplar" kenar başlıklı 123. maddesi şöyledir:

"(1) Mektup okuma komisyonunca, mahalline gönderilmesi veya hükümlüye verilmesi sakıncalı görülen mektuplar, en geç yirmidört saat içinde disiplin kuruluna verilir. Mektubun disiplin kurulu tarafından kısmen veya tamamen sakıncalı görülmesi hâlinde, mektup aslı çizilmeden veya yok edilmeden şikâyet ve itiraz süresinin sonuna kadar muhafaza edilir. Mektubun kısmen sakıncalı görülmesi hâlinde, aslı idarede tutularak fotokopisinde sakıncalı görülen kısımlar okunmayacak şekilde çizilerek disiplin kurulu kararı ile birlikte ilgisine tebliğ edilir. Mektubun tamamının

sakıncalı görülmesi hâlinde, sadece disiplin kurulu kararı tebliğ edilir. Tebliğ tarihinden itibaren infaz hâkimliğine başvuru için gereken süre beklenir. Bu süre içinde infaz hâkimliğine başvurulmamış ise, disiplin kurulu kararı yerine getirilir. İnfaz hâkimliğine başvurulmuş ise, infaz hâkimliği kararının tebliğinden itibaren itiraz süresi beklenir. İnfaz hâkimliği kararına itiraz edilmemiş ise bu karara göre, itiraz edilmiş ise mahkemenin kararına göre işlem yapılır.

(2) Hükümlüye yapılacak tebligatta, tebliğ tarihinden itibaren onbeş gün içinde infaz hâkimliğine şikâyet hakkının kullanılmaması veya infaz hâkimliği kararına karşı tebliğ tarihinden itibaren bir hafta içinde ağır ceza mahkemesine itiraz edilmemesi hâlinde, disiplin kurulu kararının kesinleşerek mektubun sakıncalı görülen kısımlarının okunmayacak şekilde çizilerek verileceği veya tamamı sakıncalı görülen mektubun verilmeyeceği bildirilir.

(3) Kısmen veya tamamen sakıncalı görülen mektuplar, iç hukuk veya uluslararası hukuk yollarına başvuru yapılması durumunda kullanılmak üzere idarece saklanır."

27. 14/6/1930 tarihli ve 1721 sayılı Hapishane ve Tevkifhanelerin İdaresi Hakkında Kanun'un 2. maddesinin ilgili kısmı şöyledir:

"... E) Ceza evinin emniyeti bakımından mahkûmlara ait mektupların ve kendilerini ziyarete gelenlerle konuşmalarının ve hariçle muhaberelelerinin ne suretle tanzim ve kontrol edileceği,

...

hakkında bir nizamname tanzim olunur.

..."

28. 17/6/2021 tarihli ve 7328 sayılı Kanun'un 7. maddesiyle 5275 sayılı Kanun'un 68. maddesine eklenen (5) numaralı fıkra şöyledir:

"(5)Kamu düzeninin korunması ile kişi, toplum ve kurum güvenliğinin sağlanması veya suç işlenmesinin önlenmesi amacıyla terör suçları, örgüt kurmak, yönetmek veya örgüte üye olmak suçları ile örgüt faaliyeti kapsamında işlenen suçlardan mahkûm olan veya tehlikeli hâlde bulunan ya da dışarı ile iletişiminin kurum güvenliği açısından tehlikeli olabileceği değerlendirilen hükümlülere gelen veya bu hükümlüler tarafından gönderilen mektup, faks ve telgraflar dijital olarak kaydedilebilir veya fiziki olarak saklanabilir. Bunlar, amacı dışında kullanılamaz, kanunda açıkça belirtilen hâller dışında hiçbir kişi veya kurumla paylaşılamaz, herhangi bir soruşturma veya kovuşturmaya konu edilmemiş ise en geç bir yıl sonunda silinir veya imha edilir. Silme veya imha

işlemi Cumhuriyet savcısı tarafından denetlenir. Bu fıkra hükmü dördüncü fıkra bakımından uygulanmaz."

29. Adalet Bakanlığı Ceza ve Tevkifevleri Genel Müdürlüğünün 19/1/2021 tarihli Genelge'sinin ilgili kısmı şöyledir:

"1- Resmî makamlara veya savunması için avukatına gönderilenler hariç olmak üzere terör ve örgütlü suçlardan barındırılan hükümlü ve tutukluların göndermek istedikleri veya kendilerine gelen mektup/faksların, adli suçlardan hükümlü ve tutukluların ise sadece kısmen veya tamamen sakıncalı olduğu değerlendirilen, adli ve disiplin soruşturma konusu olacak mektup/faksların UYAP sistemine kayıt edilmesi,

2- Hükümlü/tutuklular tarafından gönderilen ve kendilerine gelen mektup/faksların sadece Mektup Okuma Komisyonunda görevli personel tarafından denetlenmesi, UYAP sisteminde kayıt altına alınan bu verilere belirtilen yetkili personel dışında kullanıcı personelin erişimine imkan verilmemesi için portal ve ekran yetkilendirmesi yapılması amacıyla Bilgi İşlem Genel Müdürlüğüne 3 gün içinde personel isim, sicil, ünvan ve görevlerinin bildirilmesi, ayrıca mevzuatta öngörülen hâller dışında verilerin başka kişi ve kurumlarla paylaşılması,

3- UYAP sistemine kaydedilen mektup/faksların adli suçlardan barındırılan hükümlü ve tutuklular için 3 yıl süreyle, terör ve örgütlü suçlardan barındırılan hükümlü ve tutuklular için 5 yıl süre ile muhafaza edilmesi ve belirtilen süreler sonunda silinmesi, ancak adli ve idari soruşturmaya konu edilen mektup/fakslar için mevzuatta öngörülen sürelerin saklı kalacağı..."

B. Uluslararası Hukuk

1. Uluslararası Mevzuat

30. Avrupa İnsan Hakları Sözleşmesi'nin (Sözleşme) "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesi şöyledir:

"1. Herkes özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesini isteme hakkına sahiptir.

2. Bu hakların kullanılmasına ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, suçun veya düzensizliğin önlenmesi, genel sağlık ve genel ahlakın korunması, başkalarının hak ve özgürlüklerinin korunması amacıyla, hukuka uygun olarak yapılan ve demokratik bir toplumda gerekli bulunan müdahaleler dışında, kamu makamları tarafından hiçbir müdahale yapılamaz."

31. Avrupa Konseyi bünyesinde hazırlanan 28/1/1981 tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin 2. maddesinin birinci fıkrasının (a) bendi şöyledir:

"Kişisel veriler: Kimliği belirli veya belirlenebilir bir gerçek kişi ('ilgili kişi') hakkındaki tüm bilgileri ifade eder."

32. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin 6. maddesinin ilgili kısmı şöyledir:

"İç hukukta uygun güvenceler sağlanmadıkça, ırksal kökeni, siyasi düşünceleri, dini veya diğer inançları ortaya koyan kişisel verileri ile sağlık veya cinsel hayatla ilgili kişisel veriler otomatik işleme tabi tutulamaz. Aynı şey ceza mahkumiyetiyle ilgili kişiler verileri için geçerlidir."

33. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin 9. maddesinin ilgili kısmı şöyledir:

"2. Taraf devletin kanunlarında öngörülmüş olması ve demokratik bir toplumda aşağıdaki hususların sağlanması için gerekli bir önlem oluşturması halinde iş bu sözleşmenin 5, 6, ve 8. maddelerine istisna getirilebilir:

a. Devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi ..."

34. Avrupa Konseyi Bakanlar Komitesinin Üye Devletlere Avrupa Cezaevleri Kuralları Hakkında REC (2006) 2 sayılı tavsiye kararının hükümlü ve tutukluların dış dünya ile ilişkilerine dair kısmı şöyledir:

"24. 1. Mahpusların mümkün olabilen sıklıkta mektup, telefon veya diğer iletişim vasıtalarıyla aileleriyle, başka kişilerle ve dışarıdaki kuruluşların temsilcileriyle haberleşmelerine ve bu kişilerin mahpusları ziyaret etmelerine izin verilmelidir.

24. 2 Devam etmekte olan bir ceza soruşturması, emniyet, güvenlik ve düzeninin muhafaza edilmesi, suç işlenmesinin önlenmesi ve suç mağdurunun korunması için gerekli görülmesi halinde, haberleşme ve ziyaretlere kısıtlamalar konabilir ve izlenebilir. Ancak adli bir merci tarafından konulan özel kısıtlamalar da dahil olmak üzere, bu tür kısıtlamalar yine de kabul edilebilir asgari bir iletişime izin vermelidir.

24.3. Ulusal hukuk, mahpuslarla iletişim kurması kısıtlanamayacak olan ulusal ve uluslararası kuruluşları belirlemelidir,

24.4. Ziyaretler için yapılan düzenlemeler, mahpuslara aile ilişkilerini mümkün olduğunca normal bir düzeyde sürdürmelerine ve geliştirmelerine izin verecek bir tarzda olmalıdır.

24.5. Cezaevi yetkilileri, dış dünyayla yeterli bir iletişim sürdürmelerinde mahpuslara yardım etmelidirler ve bunun için onlara uygun destek ve yardım sağlamalıdır."

2. Uluslararası İctihat

35. Avrupa İnsan Hakları Mahkemesi (AİHM) devletlerin millî güvenliğin korunması amacını gerçekleştirmede sahip oldukları takdir yetkisinin geniş olduğunu kabul etmektedir. AİHM, Sözleşme'ye taraf devletlerin millî güvenliği korumak için yetkili ulusal makamlara ilk olarak kişiler hakkında bilgi toplama ve halka açık olmayan siciller tutma, ikinci olarak millî güvenlik bakımından önemli kadrolarda çalışmak isteyen adayların bu işe uygunluğunu takdir ederken bu bilgiyi kullanma yetkisi veren kurallara sahip olmaları gerektiğinde kuşku bulunmadığını belirtmektedir (Leander/İsveç, B. No: 9248/81, 26/03/1987, § 59).

36. Bununla birlikte AİHM içtihadına göre kamu mercilerinin bir bireyin özel hayatıyla ilgili bilgileri toplaması, kaydetmesi, saklaması, özel hayata saygı hakkına müdahale oluşturur (Leander/İsviçre, § 48; Kopp/İsviçre, B. No: 23224/94, 25/3/1998, § 53; Amann/İsviçre [BD], B. No: 27798/95, 16/2/2000, § 69; Rotaru/Romanya [BD], B. No: 28341/95, 4/5/2000, §§ 43, 44, 46).

37. Kaydedilen bilgilerin daha sonra kullanılmış olup olmamasının bir önemi yoktur. Bununla birlikte kamu makamları tarafından muhafaza edilen kişisel nitelikli bilgilerin özel yaşam unsurlarından birini devreye sokup sokmadığını tespit etmek için bu bilgilerin hangi çerçevede alındığının ve muhafaza edildiğinin, verilerin türünün, kullanıldığı ve işlendiği şeklin, bunlardan çıkarılabilecek sonuçların dikkate alınması zaruridir (Leander/İsveç, § 48; Amann/İsviçre, § 69; S. ve Marper/Birleşik Krallık [BD], B. No: 30562/04, 30566/04, 4/12/2008, § 67).

38. AİHM kararlarına göre haberleşme özgürlüğüne yapılan müdahale öncelikle kanunla öngörülmelidir. Müdahalenin yasal dayanağını oluşturan mevzuatın ulaşılabilir, yeterince açık ve belirli bir eylemin gerektirdiği sonuçlar açısından öngörülebilir olması gerekir. İkinci olarak söz konusu sınırlandırma meşru bir amaca dayalı olmalı, bunun yanı sıra müdahale demokratik bir toplumda gerekli ve ölçülü olmalıdır (Silver ve diğerleri/Birleşik Krallık, B. No: 5947/72...25/3/1983, §§ 85-90; Klass ve diğerleri/Almanya, B. No: 5029/71, 6/10/1978, §§ 42-55; Campbell/Birleşik Krallık, B. No: 13590/88, 25/3/1992, § 34).

39. AİHM; haberleşme hürriyetine yapılan müdahaleleri incelediği kararlarda, öncelikle ceza infaz kurumlarında bulunan kimselerin yazışmalarının belirli ölçüde kontrolünün başlı başına

Sözleşme'nin ihlaline sebebiyet vermeyeceğini, keza ceza infaz kurumunun olağan ve makul gereksinimleri dikkate alınarak bir değerlendirmede bulunmanın gerekli olduğunu belirtmiştir (Mehmet Nuri Özen/Türkiye, B. No: 15672/08...11/1/2011, § 51; Silver ve diğerleri/Birleşik Krallık, § 98).

40. AİHM, her somut olayda kamu makamlarının bu değerlendirmeyi yaparken mektup gönderme ve almanın ceza infaz kurumlarında bulunan hükümlülerin ve tutukluların dış dünya ile tek bağlantısı olduğu gerçeğini gözönünde bulundurması gereğini belirtmektedir (Campbell/Birleşik Krallık, § 45).

V. İNCELEME VE GEREKÇE

41. Anayasa Mahkemesinin 2/2/2022 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Adli Yardım Talebi Yönünden

42. Başvurucu, bireysel başvuru harç ve masraflarını karşılama imkânlarının olmadığını belirterek adli yardım talebinde bulunmuştur.

43. Anayasa Mahkemesinin Mehmet Şerif Ay (B. No: 2012/1181, 17/9/2013) kararında belirtilen ilkeler dikkate alınarak geçimini önemli ölçüde güçleştirmeksizin yargılama giderlerini ödeme gücünden yoksun olduğu anlaşılan başvurusunun açıkça dayanaktan yoksun olmayan adli yardım talebinin kabulüne karar verilmesi gerekir.

B. Özel Hayata Saygı Hakkı ile Haberleşme Hürriyetinin İhlal Edildiğine İlişkin İddia

1. Başvurucunun İddiaları ve Bakanlık Görüşü

44. Başvurucu, tutuklu olarak bulunduğu İnfaz Kurumunda kendisine gönderilen ve kendisinin göndermek istediği mektupların tamamının meşru bir dayanağı olmadan taranmak suretiyle UYAP'a süresiz olarak kaydının yapılması nedeniyle özel hayata saygı hakkının ve masumiyet karinesinin ihlal edildiğini ileri sürmüştür. Olağanüstü hâl (OHAL) ilanını takiben getirilen uygulamanın OHAL kalkmasına rağmen devam ettirilmesinin de yasal dayanağının olmadığını ifade etmiştir. Ayrıca söz konusu uygulamanın kaldırılması amacıyla yaptığı şikâyetin yargı makamları tarafından gerekçesiz bir şekilde reddedildiğini, yargılamada savcının mütalaasının kendisine tebliğ edilmediğini ve İnfaz Hâkimliğinin uyuşmazlıkla ilgili bir hafta içinde karar verme yükümlülüğünü yerine getirmediğini vurgulayarak adil yargılanma hakkının ihlal edildiğini ifade etmiştir.

45. Bakanlık görüşünde;

i. Danıştay İdari Dava Daireleri Kurulunun 14/9/2020 tarihinde, mektupların UYAP'a kaydedilmesi işlemlerinin dayanağı olan 10/10/2016 tarihli Genelge'nin yürütmesinin durdurulmasına karar verdiği ve bu kararda tespit edilen eksiklikler gözetilerek Ceza ve Tevkifevleri Genel Müdürlüğü tarafından 19/1/2021 tarihli Genelge çıkarıldığı vurgulanmıştır.

ii. Bakanlığın yeni genelge merkezli değerlendirmesinde kişisel verilerin kayıt, muhafaza ve kullanımını içeren tedbirlerin kapsamını ve uygulanmasını düzenleyen ve özellikle süre, stoklama, kullanım, üçüncü kişilerin erişimi, verilerin gizliliği, bütünlüğü ve imhası konusundaki prosedürlere ilişkin olarak muhataplarının yetki aşımı ve keyfiliğe karşı yeteri kadar güvenceye sahip olmalarını sağlayacak açık ve detaylı kuralların belirlenmesinin kanunilik ilkesinin gereği olduğu hatırlatılmıştır. 5271 sayılı Kanun'un 38. maddesinde kişisel verilerin UYAP'a kaydedileceği hususu ilkesel olarak belirlenmekle birlikte ayrıntıların düzenleyici işlemlere bırakıldığı, 10/10/2016 ve 19/1/2021 tarihli Genelgeler ile de uygulamanın düzenlendiği vurgulanmıştır. Anılan Genelgelerde hangi mektup ve yazışmaların UYAP'a kaydedileceği, bunlara kimlerin erişebileceği ve ne kadar süre ile sistemde tutulabileceğinin belirtildiği gözetildiğinde yazışmaların UYAP'a kaydedilmesinin kanuni dayanağının mevcut olduğu ifade edilmiştir.

iii. Bununla birlikte somut başvuruda uygulanan tedbirin mahpuslara gönderilen veya mahpuslarca başkalarına gönderilen mektupların UYAP ortamına kaydedilmesinden ibaret olduğu, kişisel veri mahiyetindeki bu yazışmaların ceza infaz kurumunun yetkili personeli hariç herhangi bir üçüncü kişinin erişimine veya kullanımına açılmasının söz konusu olmadığı belirtilmiştir. UYAP'ta her kullanıcı kendisine tanınan yetki sınırları çerçevesinde erişim imkânına sahip olduğundan yetki verilenler dışında erişim sağlanmasının mümkün olmadığı eklenmiştir. Ayrıca bilgilere erişim yetkisi bulunan -çok sınırlı sayıdaki- kişilerin bunu kötüye kullanması veya kanunda öngörülen hâller dışında bu bilgileri başka kişi ve kurumlara vermesi ya da onların erişimine açık hâle getirmesi hâlinde bu kişilere yönelik uygulanacak idari, cezai ve hukuki müeyyidelerin kanunlarda öngörüldüğü değerlendirilmesine yer verilmiştir.

46. Başvurucu; Bakanlık görüşüne karşı beyanında iddialarını tekrarlamakla birlikte Bakanlığın başvuru konusu olayda uygulanan 2016 tarihli Genelge'nin hukuka aykırı olduğunu ikrar ettiğini, yeni genelgeye dayanarak geçmişteki hukuka aykırılıkla ilgili bir yorum yapmadığını belirtmiştir. Mektuplarının sakıncalı olup olmadığına bakılmaksızın UYAP'a kaydedilmesinin kanuni bir dayanağının olmadığını, sadece genelgeye dayandığını, kişisel verilerinin bu şekilde işlenmesinin keyfi kullanıma açık olduğunu belirterek özel hayata saygı hakkı ile haberleşme hürriyetinin ihlal edildiğini ileri sürmüştür.

2. Değerlendirme

47. Anayasa'nın 20. maddesinin ilgili kısmı şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

...

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

48. Anayasa'nın 22. maddesi şöyledir:

"Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.

İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir."

49. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Başvurucunun iddiasının temeli, başvurucuya gönderilen veya başvurucağın göndermek istediğı tüm mektupların İnfaz Kurumu idaresi tarafından UYAP'a kaydedilmesine ilişkindir. Bireyin kişisel verilerinin ve bu verilerin korunmasına dair menfaatinin özel yaşamı kapsamında olduğu açıktır. Haberleşme içeriklerinin ve biçimin, kaydı şeklinde gerçekleşen müdahalenin haberleşme hürriyetine yapılan müdahalenin özel bir şekli olduğu hususunda da tereddüt bulunmamaktadır. Dolayısıyla mahremiyet hakkı ve bu alanla ilgili bilgilerin gizliliğinin korunması ile haberleşmenin denetlenmesine ilişkin eldeki başvurunun Anayasa'nın 20. ve 22.

maddeleri çerçevesinde özel hayata saygı hakkı ve haberleşme hürriyeti yönünden ve birlikte incelenmesi gerektiği değerlendirilmiştir (Kemal Karanfil, B. No: 2017/24776, 24/5/2018, § 48).

a. Kabul Edilebilirlik Yönünden

50. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan özel hayata saygı hakkı kapsamında mahremiyetin ve kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

b. Esas Yönünden

i. Müdahalenin Varlığı

51. Anayasa Mahkemesi Kemal Karanfil kararında başvurucunun dış dünyayla iletişimini sağlayan yazışmaların bazı istisnalar haricinde kurum idaresi tarafından denetlenerek UYAP'a kaydedilmesinin, kişiye ait bilgileri içeren mektupların açılıp okunarak sistemde tutulmasının başvurucunun özel hayatına ve haberleşmesine müdahale oluşturduğunu kabul etmiştir (Kemal Karanfil, § 53).

ii. Müdahalenin İhlal Oluşturup Oluşturmadığı

52. Anayasa'nın 13. maddesi şöyledir:

"Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz."

53. Yukarıda belirlenen müdahale, Anayasa'nın 13. maddesinde belirtilen koşullara uygun olmadığı takdirde Anayasa'nın 20. ve 22. maddelerini ihlal edecektir. Bu sebeple sınırlamanın Anayasa'nın 13. maddesinde öngörülen ve somut başvuruya uygun düşen, kanun tarafından öngörülme, meşru amaç taşıma, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmama kriterlerine uygun olup olmadığının belirlenmesi gerekir (Halil Berk, B. No: 2017/8758, 21/3/2018, § 49; Süveyda Yarkin, B. No: 2017/39967, 11/12/2019, § 32; Şennur Acar, B. No: 2017/9370, 27/2/2020, § 34; R.G. [GK], B. No: 2017/31619, 23/7/2020, § 82). Bu bağlamda somut başvuruda öncelikle müdahalenin kanuni dayanağının bulunup bulunmadığı incelenmelidir. Bu incelemenin -ilgili mevzuatta süreç içinde değişiklikler yapılmış ise de (bkz. §§ 28, 29)- başvuruya konu olay tarihi itibarıyla geçerli olan mevzuat hükümleriyle sınırlı olarak yapılması uygun görülmüştür.

(1) Genel İlkeler

54. Anayasa uyarınca temel hak ve özgürlüklere getirilen sınırlamaların öncelikle kanunla öngörülmüş olması gerekir. Kanun ile sınırlama ölçütü veya kanunilik ilkesi Sözleşme'nin 8. maddesinde de bir sınırlama ve güvence ölçütü olarak yer almaktadır. Buna karşın Sözleşme'de yer alan kanunla öngörülmüş olma kavramı ile Anayasa'da yer alan kanunilik ilkesi tam olarak aynı değildir (Bülent Polat [GK], B. No: 2013/7666, 10/12/2015, § 73).

55. AİHM kanunda öngörülen koşulları, bir diğer ifadeyle hukukiliği geniş yorumlayarak istikrar kazanmış yargı kararlarına dayanan içtihat yoluyla geliştirilmiş ilkelerin de hukukilik şartını karşılayabildiğini kabul ederken (Malone/İngiltere, B. No: 8691/79, 2/8/1984, §§ 66-68; Sunday Times/Birleşik Krallık (No. 1), B. No: 6538/74, 26/4/1979, § 47) Anayasa, tüm sınırlandırmaların mutlaka kanun ile yapılacağını öngörerek Sözleşme'den daha geniş bir koruma sağlamıştır (Mehmet Akdoğan ve diğerleri, B. No: 2013/817, 19/12/2013, § 31; Bülent Polat § 75). Anayasa'nın temel hak ve hürriyetlerin sınırlandırılmasının ancak kanunla yapılacağına ilişkin 13. maddesi, bir kanun hükmü olmaksızın yürütme ve idarenin bir hak ve hürriyeti ilk elden düzenleyici işlemle sınırlamasına izin vermez (Tuğba Arslan [GK], B. No: 2014/256, 25/6/2014, § 87).

56. Anayasa'nın temel hak ve özgürlüklerin sınırlandırılması rejimini düzenleyen 13. maddesinde hak ve özgürlüklerin ancak kanunla sınırlanabileceği temel bir ilke olarak benimsenmiştir. Bunun yanında Anayasa'nın 20. maddesinin üçüncü fıkrasının üçüncü cümlesinde kişisel verilerin “ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla” işlenebileceği belirtilmiş, aynı fıkranın dördüncü cümlesinde ise kişisel verilerin korunmasına ilişkin esas ve usullerin “kanunla” düzenleneceği hüküm altına alınmıştır. Buna göre kişisel verilerin korunmasını isteme hakkına yapılan müdahalelerde dikkate alınacak öncelikli ölçüt, müdahalenin kanuna dayalı olmasıdır (Arif Ali Cangı [GK], B. No: 2016/4060, 17/9/2020 § 72).

57. Bununla birlikte temel hak ve hürriyetlerin sınırlandırılmasına ilişkin kanunların şeklen var olması yeterli değildir. Kanunilik ölçütü aynı zamanda maddi bir içeriği de gerektirmekte olup bu noktada kanunun niteliği önem kazanmaktadır. Kanunla sınırlama ölçütü sınırlamanın erişilebilirliğini, öngörülebilirliğini ve kesinliğini ifade etmekte; böylece uygulayıcının keyfî davranışlarının önüne geçtiği gibi kişinin hukuku bilmesine de yardımcı olmakta; bu yönüyle hukuk güvenliği teminatı sağlamaktadır (Halime Sare Aysal [GK], B. No: 2013/1789, 11/11/2015, § 62; Fatih Saraman [GK], B. No: 2014/7256, 27/2/2019, § 66; Turgut Duman, B. No: 2014/15365, 29/5/2019, § 66).

58. Kanunun bu gerekliliklere uygun olduğunun söylenebilmesi için yeterince ulaşılabilir olması, vatandaşların belirli bir olaya uygulanabilir nitelikteki hukuk kurallarının varlığı hakkında yeterli

bilgiye sahip olabilmesi, ayrıca ilgili normun keyfiliğe karşı uygun bir koruma sağlaması, yetkili makamlara verilen yetkinin genişliğini ve icra edilme biçimlerini yeterli bir netlikte tanımlaması gerekmektedir (Halime Sare Aysal, § 63; Fatih Saraman, § 67; Turgut Duman, § 68).

59. Hukukun kendisi -beraberinde getireceği idari pratiğin dışında- söz konusu işlemin meşru amacını da gözönünde tutarak keyfi müdahalelere karşı bireyi korumak için yetkili makamlara bırakılan takdir yetkisinin kapsamını yeterince açık bir şekilde göstermelidir. Hukuk sistemi vatandaşlara kamu makamlarına hangi koşullarda ve hangi sınırlar içinde müdahalelerde bulunma yetkisi verdiğini yeterince açık ifadelerle gösterecek nitelikte olmalı ve bu bağlamda ilgili müdahalenin muhataplarının müdahaleye zemin hazırlayan koşullar ile müdahalenin sonuçları açısından bir öngöründe bulunabilmeleri imkânı tanınmalıdır (Halime Sare Aysal, § 64; Fatih Saraman, § 68; Turgut Duman, § 69).

60. Bununla birlikte her ihtimale çözüm getiremeyecek olan yasal mevzuatın sağladığı koruma seviyesi büyük ölçüde ilgili metnin düzenlediği alan ve içeriğiyle birlikte muhataplarının niteliği ve sayısı ile yakından bağlantılıdır. Bu nedenle kuralın karmaşık olması ya da belirli ölçülerde soyut nitelik taşıması ve buna bağlı olarak hukuki yardım ile tam olarak anlaşılabilir hâle gelmesi tek başına hukuken öngörülebilirlik ilkesine aykırı görülemez. Bu kapsamda hak ya da özgürlüğe müdahale eden kural belirli ölçülerdeki takdir alanını elbette uygulayıcıya bırakabilir. Fakat bu takdir alanının sınırlarının da yeterli açıklıkta belirlenmesi ve kuralın asgari bir kesinlik içermesi zaruridir (Halime Sare Aysal, § 65; Fatih Saraman, § 69; Turgut Duman, § 70).

61. Bu kapsamda ilgili kanuni düzenlemenin söz konusu sınırlamaya ilişkin temel çerçeveyi ortaya koymakla birlikte özellikle uygulama koşulları ve usule ilişkin ayrıntıları düzenleyici işlemlere bırakması mümkündür. Ancak bu ihtimalde de söz konusu düzenleyici işlemin yine muhataplarınca ulaşılabilir olması ve içeriği hakkında ilgilileri yeterince aydınlatacak nitelik ve açıklıkta olması gerekmektedir (Halime Sare Aysal, § 66).

62. Somut başvuru açısından ise kişisel verilerin kayıt, muhafaza ve kullanımını içeren tedbirlerin kapsamını ve uygulanmasını düzenleyen ve özellikle süre, stoklama, kullanım, üçüncü kişilerin erişimi, verilerin gizliliği, bütünlüğü ve imhası konusundaki prosedürlere ilişkin olarak muhataplarının yetki aşımı ve keyfiliğe karşı yeteri kadar güvenceye sahip olmalarını sağlayacak açık ve detaylı kuralların belirlenmesinin söz konusu gerekliliklere temel oluşturduğu açıktır (Bülent Kaya [GK], B. No: 2013/2941, 11/5/2016, § 64).

63. Bu kapsamda ilgili sisteme bilgilerin girilmesi, müdahaleye temel oluşturan meşru amaçları taşıma şartına bağlı olmalı ve söz konusu yasal düzenleme, hangi bilgilerin kayıt altına alınabileceği,

hangi yetkililere iletilebileceđi, böyle bir iletimin hangi kořullarda mümkün olabileceđi ve bilginin ilgili makamlara iletilmesi hususunda izlenecek usul konusunda açık ve ayrıntılı hükümler içermelidir. Söz konusu sisteme ilişkin düzenleme; bilgi toplama, kaydetme ve bilgiyi ilgili makamlarla paylaşma veya sair şekilde kullanma konusunda yetkili makamlara tanıdığı takdir yetkisinin kullanılma tarzı ve alanı bakımından vatandaşlara yeterince öngörüde bulunma olanağı sağlamak durumundadır (Bülent Kaya, § 66).

(2) İlkelerin Olaya Uygulanması

64. Anayasa Mahkemesi Kemal Karanfil kararında başvuruya konu idari uygulamanın ve yargısal sürecin 5271 sayılı Kanun'un 38/A maddesi, 5275 sayılı Kanun'un 68. maddesi, Tüzük'ün 122. ve 123. maddeleri ile Bakanlığın 10/10/2016 tarihli Genelge'si temelinde yürütüldüğünü tespit ederek kanuni dayanağının mevcut olduğuna karar vermiştir (Kemal Karanfil, §§ 56-69).

65. Bununla birlikte yapılan incelemede tutuklu ve hükümlülerin yazışmalarının UYAP'a kaydedilmesi şeklindeki müdahalenin özel hayata saygı hakkı ile haberleşme hürriyetini ihlal etmediđi sonucuna varılmakla birlikte Anayasa Mahkemesince ulařılan sonucun mahpusların mektuplarının kaydı hususunda kamu makamlarına sınırsız yetki verildiđi biçiminde anlaşılamayacağı vurgulanmıştır. Ayrıca kararda belirtilen ve müdahalenin orantılı bulunmasında dayanak alınan kořulların fiilen sağlanmadığının veya mektupların kaydedilmesindeki meşru amacın ortadan kalktığıının tespit edilmesi hâlinde ihlal sonucuna ulařılmasının mümkün olduğu belirtilmiştir (Kemal Karanfil § 79).

66. Bu bağlamda anılan karardan sonra gelişen uygulama ve OHAL sürecinin sona erdiđi gözetildiđinde anılan müdahalenin yeniden değerlendirilmesi gerektiđi sonucuna ulařılmıştır. Mahpusların mektuplarının UYAP'a kaydedilmesinin uygulamanın 5271 sayılı Kanun'un 38/A maddesi, 5275 sayılı Kanun'un 68. maddesi, Tüzük'ün 122. ve 123. maddeleri ile Bakanlığın 10/10/2016 tarihli Genelgesine dayandıđı anlaşılmaktadır.

67. Öncelikle ceza infaz kurumlarında bulunan hükümlü ve tutukluların yaptıkları yazışmaların denetimi ile sınırlandırılmasının 5275 sayılı Kanun'un 68. maddesinde düzenlendiđi, anılan düzenlemeye dayalı Tüzük ile de denetlemenin usul ve sonuçlarının ayrıntılarına yer verildiđi görülmüştür (Ahmet Temiz, B. No: 2013/1822, 20/5/2015, §§ 37-46). Anılan düzenlemeler gözetildiđinde ceza infaz kurumuna mektupları denetleme yetkisi verildiđi, bu bağlamda sakıncalı görülmeyen mektupların muhatabına teslim edilmesi veya gönderilmesi, sakıncalı kabul edilenlerin ise infaz kurumunda muhafazasının gerektiđi anlaşılmaktadır.

68. Öte yandan 5271 sayılı Kanun'un 38/A maddesiyle de ceza muhakemesi işlemlerine ilişkin her türlü veri, bilgi, belge ve kararın UYAP vasıtasıyla işlenebileceği, kaydedilebileceği ve saklanabileceği düzenlenmiştir. Her iki kanun ve "İlgili Hukuk"ta belirtilen mevzuat birlikte değerlendirildiğinde infaz kurumuna tanınan denetim yetkisi kapsamında mahpusların yazışmalarının kural olarak UYAP'a kaydedilebilmesine olanak sağlayan yasal düzenlemenin mevcut olduğu söylenebilir. Bununla birlikte "Genel İlkeler"de belirtildiği üzere (bkz. §§ 57-63) temel hak ve hürriyetlerin sınırlandırılmasına ilişkin kanunların şeklen var olması yeterli değildir. Kanunilik ölçütü aynı zamanda maddi bir içeriği de gerektirmekte olup bu noktada kanunun niteliği önem kazanmaktadır.

69. Bu durumda mahpusların yazışmalarının özel hayata dair mahrem kalmasını istediği konular ile kişisel veri kapsamında kalacak bilgileri içerebileceği gözetildiğinde mahpusun temel hak ve özgürlüklerinin sınırlandırılmasını içeren kanunların konuyla ilgili temel esasları ve ilkeleri belirleyecek nitelikte olması gerektiği de vurgulanmalıdır. Bu kapsamda kanun veya ilgili kanuna dayanan mevzuatın özellikle yazışmaların sistematik olarak kaydedilmesinin kapsamına ve mektup ile içeriğindeki mahrem bilgiler ile kişisel verilerin muhafazasına ilişkin esasları belirlemesi beklenir. Bununla birlikte mahpusların yazışmalarının tutulma süresi, bu yazışmalara üçüncü kişilerin erişimi ile içeriğindeki verilerin kullanılması, imhası ve verilerin gizliliğinin sağlanması hususlarına ilişkin muhataplarının yetki aşımı ve keyfiliğe karşı yeteri kadar güvenceye sahip olmalarını sağlayacak açık ve detaylı kuralları içermesi gerekmektedir.

70. Somut olaydaki uygulamanın dayanağı olan Bakanlığın 10/10/2016 tarihli Genelge'si ile tüm hükümlü ve tutukluların resmî makamlara veya savunması için avukatına verdiği kapalı zarf içindeki mektup ve faksler hariç olmak üzere tüm faks ve yazışmaların taranmak suretiyle UYAP'a kaydedilmesi gerektiği düzenlenmiştir. Bu düzenlemenin mahpusun sakıncalı bulunmayan, kişisel nitelikteki bilgilerini de içeren ve yargısal süreçlerle ilgisi olmayan yazışmalarının UYAP'a kaydedilmesi suretiyle muhafaza edilmesine olanak sağlayarak mevzuatın mektubun sakıncalı olup olmamasına göre belirlediği usulden ayrılma sonucunu doğurduğu görülmüştür.

71. Bununla birlikte başvuru konusu uygulamayla mahkûmiyete konu suçun özelliği ya da tutuklu ile hükümlünün ceza hukuku bağlamındaki statülerine göre farklılık öngörülmeden, sakıncalı olup olmadığına bakılmaksızın tüm yazışmaların UYAP'a sistematik bir şekilde kaydedildiğinin altı çizilmelidir. Ayrıca mahpusun yazışmalarının ne kadar süreyle sistemde saklı tutulacağı, bunların üçüncü kişilerin erişimine ve kullanımına hangi şartlarda açılacağı, infaz kurumu tarafından hangi mercilerle paylaşılabilirliği ile kişisel verilerin ve mahremiyetin nasıl korunacağı hususlarında açık bir düzenlemenin mevcut olmadığı, uygulamada da anılan konular yönünden bir belirsizliğin

bulunduđu anlaşılmıřtır. Bu durumda mahpusun mahrem bilgileri ile kiřisel verilerinin kayıt, muhafaza ve kullanımını ieren tedbirlerin kapsamını, uygulanmasını, idarenin takdir yetkisinin sınırlarını dzenleyen, bununla birlikte muhataplarının yetki ařımı ile keyfiliđe karřı yeteri kadar gvenceye sahip olmalarını sađlayacak niteliđe ve aıklıđa sahip kuralların mevcut olmadığı sylenbilir. Bu aıklamalar erevesinde somut olayda zel hayata saygı hakkı ile haberleřme hrriyetine yapılan mdahalenin kanuni dayanađının olmadığı sonucuna varılmıřtır.

72. Aıklanan gerekelerle bařvurucunun Anayasa'nın 20. ve 22. maddelerinde gvence altına alınan mahremiyetin ve kiřisel verilerin korunmasını isteme bađlamında zel hayata saygı hakkı ile haberleřme hrriyetinin ihlal edildiđine karar verilmesi gerekir.

73. Yukarıda yer verilen tespitler uyarınca bařvuruya konu mdahalenin kanunilik kořulunu sađlamadıđı anlaşıldıđından sz konusu mdahale aısından diđer gvence ltlerine riayet edilip edilmediđinin ayrıca deđerlendirilmesine gerek grlmemiřtir.

C. 6216 Sayılı Kanun'un 50. Maddesi Ynnden

74. 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluđu ve Yargılama Usulleri Hakkında Kanun'un 50. maddesinin ilgili kısmı řoyledir:

“(1) Esas inceleme sonunda, bařvurucunun hakkının ihlal edildiđine ya da edilmediđine karar verilir. İhlal kararı verilmesi hlinde ihlalin ve sonularının ortadan kaldırılması iin yapılması gerekenlere hkmedilir...

(2) Tespit edilen ihlal bir mahkeme kararından kaynaklanmıřsa, ihlali ve sonularını ortadan kaldırmak iin yeniden yargılama yapmak zere dosya ilgili mahkemeye gnderilir. Yeniden yargılama yapılmasında hukuki yarar bulunmayan hllerde bařvurucu lehine tazminata hkmedilebilir veya genel mahkemelerde dava aılması yolu gsterilebilir. Yeniden yargılama yapmakla ykml mahkeme, Anayasa Mahkemesinin ihlal kararında aıkladıđı ihlali ve sonularını ortadan kaldıracak řekilde mmknse dosya zerinden karar verir.”

75. Bařvurucu; ihlalin tespit edilmesini, tm sonularıyla giderilmesini istemiř ve 200.000 TL manevi tazminat talebinde bulunmuřtur.

76. Anayasa Mahkemesinin Mehmet Dođan ([GK], B. No: 2014/8875, 7/6/2018) kararında ihlal sonucuna varıldıđında ihlalin nasıl ortadan kaldırılacađı hususunda genel ilkeler belirlenmiřtir. Anayasa Mahkemesi diđer bir kararında ise bu ilkelerle birlikte ihlal kararının yerine getirilmemesinin sonularına da deđermiř ve bu durumun ihlalin devamı anlamına geleceđi gibi ilgili

hakkın ikinci kez ihlal edilmesiyle sonuçlanacağına işaret etmiştir (Aligül Alkaya ve diğerleri (2), B. No: 2016/12506, 7/11/2019).

77. Bireysel başvuru kapsamında bir temel hakkın ihlal edildiğine karar verildiği takdirde ihlalin ve sonuçlarının ortadan kaldırıldığından söz edilebilmesi için temel kural, mümkün olduğunca eski hâle getirmenin yani ihlalden önceki duruma dönülmesinin sağlanmasıdır. Bunun için ise öncelikle ihlalin kaynağı belirlenerek devam eden ihlalin durdurulması, ihlale neden olan karar veya işlemin ve bunların yol açtığı sonuçların ortadan kaldırılması, varsa ihlalin sebep olduğu maddi ve manevi zararların giderilmesi, ayrıca bu bağlamda uygun görülen diğer tedbirlerin alınması gerekmektedir (Mehmet Doğan, §§ 55, 57).

78. İhlalin mahkeme kararından kaynaklandığı veya mahkemenin ihlali gideremediği durumlarda Anayasa Mahkemesi, 6216 sayılı Kanun'un 50. maddesinin (2) numaralı fıkrası ile Anayasa Mahkemesi İçtüzüğü'nün 79. maddesinin (1) numaralı fıkrasının (a) bendi uyarınca, ihlalin ve sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmak üzere kararın bir örneğinin ilgili mahkemeye gönderilmesine hükmeder. Anılan yasal düzenleme, usul hukukundaki benzer hukuki kurumlardan farklı olarak ihlali ortadan kaldırmak amacıyla yeniden yargılama sonucunu doğuran ve bireysel başvuruya özgülenen bir giderim yolunu öngörmektedir. Bu nedenle Anayasa Mahkemesi tarafından ihlal kararına bağlı olarak yeniden yargılama kararı verildiğinde usul hukukundaki yargılamanın yenilenmesi kurumundan farklı olarak ilgili mahkemenin yeniden yargılama sebebinin varlığını kabul hususunda herhangi bir takdir yetkisi bulunmamaktadır. Dolayısıyla böyle bir kararın kendisine ulaştığı mahkemenin yasal yükümlülüğü, ilgilinin talebini beklemeksizin Anayasa Mahkemesinin ihlal kararı nedeniyle yeniden yargılama kararı vererek devam eden ihlalin sonuçlarını gidermek üzere gereken işlemleri yerine getirmektir (Mehmet Doğan, §§ 58, 59; Aligül Alkaya ve diğerleri (2), §§ 57-59, 66, 67).

79. İncelenen başvuruda, müdahalenin sınırlarını ve usullerini gösteren kanuni dayanak olmaksızın yazışmaların idare tarafından kaydedilmesi nedeniyle özel hayata saygı hakkı ile haberleşme hürriyetinin ihlal edildiği sonucuna ulaşılmıştır. Dolayısıyla ihlalin idarenin işleminden kaynaklandığı anlaşılmaktadır. Bununla birlikte Mahkemeler de ihlali giderememiştir.

80. Bu durumda anılan ihlalin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmasında hukuki yarar bulunmaktadır. Yapılacak yeniden yargılama ise bireysel başvuruya özgü düzenleme içeren 6216 sayılı Kanun'un 50. maddesinin (2) numaralı fıkrasına göre ihlalin ve sonuçlarının ortadan kaldırılmasına yöneliktir. Bu kapsamda yapılması gereken iş, yeniden yargılama kararı verilerek Anayasa Mahkemesini ihlal sonucuna ulaştıran nedenleri gideren, ihlal kararında belirtilen ilkelere

uygun yeni bir karar verilmesinden ibarettir. Bu sebeple kararın bir örneğinin yeniden yargılama yapılmak üzere Mahkemesine gönderilmesine karar verilmesi gerekmektedir.

81. İhlalin ve sonuçlarının ortadan kaldırılması için yeniden yargılamanın yeterli bir giderim sağlayacağı anlaşıldığından tazminat talebinin reddine karar verilmesi gerektiği sonucuna ulaşılmıştır.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Başvurucunun adli yardım talebinin **KABULÜNE,**

B. Özel hayata saygı hakkı ve haberleşme hürriyetinin ihlal edildiğine ilişkin iddianın **KABUL EDİLEBİLİR OLDUĞUNA,**

C. Anayasa'nın 20. ve 22. maddelerinde güvence altına alınan özel hayata saygı hakkı ve haberleşme hürriyetinin **İHLAL EDİLDİĞİNE,**

D. Kararın bir örneğinin özel hayata saygı hakkının ve haberleşme hürriyetinin ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmak üzere Tekirdağ 2. İnfaz Hâkimliğine (E.2020/398, K.2020/642) **GÖNDERİLMESİNE,**

E. Başvurucunun tazminat talebinin **REDDİNE,**

F. Kararın bir örneğinin bilgi için Tekirdağ 1. Ağır Ceza Mahkemesine (E.2020/1034 D.iş) ve Adalet Bakanlığına **GÖNDERİLMESİNE** 2/2/2022 tarihinde **OYBİRLİĞİYLE** karar verildi.

Anayasa Mahkemesi - H.Ö. Kararı (2019/20473)

H.Ö., B. No: 2019/20473, 3/2/2022

Başvuru, kişisel verilerin hukuka aykırı şekilde ele geçirilmesine yönelik şikâyet hakkında etkili bir ceza soruşturması yapılmaması nedeniyle özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiği iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ ANAYASA MAHKEMESİ

BİRİNCİ BÖLÜM

KARAR

H.Ö. BAŞVURUSU

(Başvuru Numarası: 2019/20473)

Karar Tarihi: 3/2/2022

R.G. Tarih ve Sayı: 18/3/2022-31782

BİRİNCİ BÖLÜM

KARAR

GİZLİLİK TALEBİ KABUL

Başkan: Hasan Tahsin GÖKCAN

Üyeler: Hicabi DURSUN, Muammer TOPAL, Recai AKYEL, Selahaddin MENTEŞ

Raportör: Ali KOZAN

Başvurucu: H.Ö.

Vekili: Av. Mert APAYDIN

I. BAŞVURUNUN KONUSU

1. Başvuru, kişisel verilerin hukuka aykırı şekilde ele geçirilmesine yönelik şikâyet hakkında etkili bir ceza soruşturması yapılmaması nedeniyle özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiği iddiasına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 11/6/2019 tarihinde yapılmıştır.
3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.
4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.
5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.
6. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına gönderilmiştir.

III. OLAY VE OLGULAR

7. Başvuru formu ve eklerinde ifade edildiği şekliyle ve Ulusal Yargı Ağı Bilişim Sistemi (UYAP) aracılığıyla erişilen bilgi ve belgeler çerçevesinde ilgili olaylar özetle şöyledir:
8. Başvurucu ile eşi arasında devam eden boşanma davasında, başvurucunun eşi 19/12/2018 tarihinde mahkemeye beyan ve delil dilekçesi ibraz etmiştir. Anılan dilekçede başvurucunun eşi; başvurucunun dava ve cevaba cevap dilekçelerinde evlendikten sonra migren ataklarının arttığı, bu durumun da kendisinden (başvurucunun eşinden) kaynaklandığı yönünde iddialarının olduğunu, bu iddialarının aksini ispatlamak amacıyla yaptığı araştırma sonucunda başvurucunun evlenmeden önce de migren ve psikolojik rahatsızlığının olduğunu tespit ettiğini belirtmiştir. Bu bağlamda ilgili Afyonkarahisar Devlet Hastanesinin 2014 ve 2015 yıllarına ait raporları ve tedavi bilgileri gözetildiğinde başvurucu hakkında migren ve anksiyete bozukluğu tanısıyla reçete düzenlendiğini, daha sonra başvurucuya bipolar duygulanım bozukluğu teşhisi konulduğunun ve başvurucunun yatarak tedavi gördüğünün anlaşıldığını vurgulayan başvurucunun eşi 2013 ile 2018 tarihleri arasında düzenlenen tedavi evrakı ile ilaç reçetelerinin anılan Hastaneden temini için müzekkere yazılmasını talep etmiştir.
9. Başvurucu; hakkındaki hastane kayıtlarını eşinin ele geçirip delil olarak mahkemeye sunması nedeniyle görevi kötüye kullanma, özel hayatın gizliliğini ihlal, kişisel verilerin hukuka aykırı olarak ele geçirilmesi ve verilerin paylaşılması suçlarını işlediği iddiasıyla 20/12/2018 tarihinde eşinden şikâyetçi olmuştur. Şikâyet dilekçesinde başvurucu vekili; başvurucunun evlilik öncesi dönemine ait hastane kayıtları, tedavi gördüğü poliklinik numarası ve tedavi tarihi ile ilgili reçeteler ve tedavi bilgilerinin özel hayatın gizliliği ve kişisel verilerin korunması haklarına aykırı olarak başvurucunun eşi tarafından ele geçirilip mahkeme dosyasına sunulduğunu vurgulamıştır. Başvurucunun eşinin anılan ilde doktor olarak görev yaptığını, Hastane tarafından gizli tutulması gereken bilgilere yetkili

merci talebi olmadan, mesleki imtiyazlarını kullanarak ulaştığını belirtmiştir. Hasta ile doktor arasındaki bilgilerin gizliliğinin esas olduğunu, başvuruçunun eşinin doktor olmasının verdiği kolaylıktan yararlanıp mahkemenin ya da resmî bir kurumun talebi olmaksızın bu bilgilere ulaşmak suretiyle bilgileri menfaati için kullanmasının 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 136., 137. ve 257. maddeleri ile 1/8/1998 tarihli ve 23420 sayılı Resmî Gazete'de yayımlanan Hasta Hakları Yönetmeliği'nin (Yönetmelik) 23. maddesine aykırı olduğunu ifade etmiştir.

10. Ceza soruşturmasını yürüten Afyonkarahisar Cumhuriyet Başsavcılığı (Başsavcılık) tarafından 6/2/2019 tarihli müzekkereyle, ilgili hastaneden başvuruçunun tedavi bilgileri talep edilmiştir. Ayrıca bu bilgilere sorgulama yaparak ulaşan veya çıktı alan tüm kamu görevlilerinin isimleri, görevleri, sorgulamanın tarih ve zaman aralığı ile sisteme girerken kullanılan cihazların bilgisinin tespit edilerek ayrıntılı bir şekilde raporlandırılması istenmiştir. Kurumun 4/3/2019 tarihli cevabında, başvuruçunun yatarak tedavi gördüğüne dair kayıt bulunmadığı, ayakta tedavi gördüğü dönemlere ait raporların gönderildiği belirtilmiş; ayrıca Adli Kalem Biriminde görevli veri hazırlama kontrol işletmen memuru A.G. tarafından 19/2/2019-4/3/2019 tarihleri arasında cep telefonu ve bilgisayar üzerinden sorgulama ve çıktı alma işleminin yapıldığı bildirilmiştir.

11. Başsavcılık başvuruçunun eşinin ifadesini 17/1/2019 tarihinde almıştır. Başvuruçunun eşi ifadesinde; başvuruçunun boşanma ve ceza davalarında aleyhine beyanda bulunduğunu hatta migren şikâyetlerinin evlilik hayatında yaşadıklarından dolayı arttığını iddia ettiğini belirtmiştir. Bunun üzerine kendisinin de eşinin evlenmeden önceki rahatsızlığı hakkında bilgi sahibi olmak için hastaneye giderek hastane bilgisayarında araştırma yaptığını, araştırma sonucunda bazı rahatsızlıkları olduğunu gördüğünü ancak herhangi bir belge almadığını beyan etmiştir. Ayrıca başvuruçunun kişisel haklarını ihlal etme niyetinin olmadığını, yargılama esnasında kendini koruma maksadıyla hareket ettiğini, hasta hakları mahremiyetini ihlal etmediğini vurgulamıştır.

12. Bu süreçte başvuruçunun vekili 1/2/2019 tarihinde ek şikâyet dilekçesi vererek soruşturmanın genişletilmesi talebinde bulunmuştur. Anılan dilekçede; başvuruçunun eşinin ifadesinde hastaneye giderek hastane bilgisayarlarından müvekkilinin hastane kayıtlarını araştırdığını beyan ettiğini, bu yolla kişisel verileri ele geçirme ve yasma suçunu işlediğini açıkça ikrar ettiğini vurgulamıştır. Hastane bilgisayarlarında şifre olduğunu belirterek şüphelinin hastane kayıtlarına hangi bilgisayardan erişim sağladığı, bu bilgisayarın kimin kullanımında olduğu hususlarının araştırılarak şüpheliye suçun işlenmesinde yardım ve iştirakte bulunan diğer şüphelilerin tespitini talep etmiştir.

13. Başsavcılık 13/3/2019 tarihinde kovuşturmayaya yer olmadığına dair karar vermiştir. Kararın gerekçesinde; anılan Hastanenin cevap yazısı ile şüphelinin ifadeleri tekrarlandıktan sonra eşin diğer

eş hakkında birinci dereceden yakını olması nedeniyle kişisel ve sağlık bilgilerine ulaşma hakkının bulunduğu vurgulanmıştır. Bu nedenle şüphelinin eyleminin mahremiyetin ve özel hayatın ihlali olarak değerlendirilemeyeceği, aynı zamanda taraflar arasında devam eden dava kapsamında iddia ve delilleri sunmanın iddia ve savunma dokunulmazlığı kapsamında kaldığı, delil değerlendirmesinin yargılamayı yapan makama ait olduğu görüşüne yer verilmiştir.

14. Başvurucu vekili bu karara karşı yaptığı itirazında Başsavcılığın eksik inceleme ile karar verdiğini vurgulamıştır. Bu bağlamda şüphelinin hastane kayıtlarına bizzat bilgisayar kullanarak ulaştığını beyan ettiğini ancak bir memur tarafından sorgulama yapıldığının Hastane tarafından bildirildiği gözetildiğinde bir çelişkinin mevcut olduğunu belirtmiştir. Bu durumda çelişkiyi gidermek için ilgili memurun tanık olarak dinlenmesi ya da müştekinin beyanına itibar ediliyorsa görevli olmadığı hastanede kimin bilgisayarını ve şifresini kullanarak kayıtları incelediğinin tespit edilmesi gerektiğini ileri sürmüştür. Ayrıca mevzuatta hastane kayıtlarının gizliliğinin kişisel verilerin korunması kapsamında sıkı kurallara tabi olduğunu, mevzuatın sınırlı sayıda kişinin erişimine izin verdiğini, eşlerin ya da birinci dereceden yakınların bu kayıtlara ulaşacağına dair mevzuatta bir düzenleme olmadığını, bu durumun hukuka uygunluk nedeni olarak da düzenlenmediğini ifade etmiştir.

15. Karara karşı yapılan itiraz, Afyonkarahisar 1. Sulh Ceza Hâkimliğinin 10/5/2019 tarihli kararıyla reddedilmiştir. Kararda, Başsavcılık tarafından verilen kararın usule ve mevzuata uygun olduğu ifade edilmiştir.

16. Nihai karar 14/5/2019 tarihinde başvurucuya tebliğ edilmiştir.

17. Başvurucu 11/6/2019 tarihinde bireysel başvuruda bulunmuştur.

18. UYAP üzerinden yapılan inceleme neticesinde aile mahkemesinde görülen boşanma davasında, başvurucuya ait tedavi kayıtlarının ve raporlarının anılan Hastaneden celbedildiği, bu belgelerle başvurucunun başka bir devlet hastanesine sevkinin yapılarak akıl sağlığıyla ilgili rapor tanziminin sağlandığı, başvurucunun fiilî ve cezai ehliyetinin tam olduğuna yönelik rapor düzenlendiği görülmüştür. Mahkeme ayrıca asliye ceza mahkemeleriyle yaptığı yazışma neticesinde bir yargılamada eşinin başvurucuyu tehdit etme suçundan ceza aldığını, diğer bir yargılamada da eşe karşı yaralama suçundan başvurucu ile eşinin ceza aldığını ve bu mahkûmiyet kararlarının kesinleştiğini tespit etmiştir. Mahkeme tarafların boşanmalarına 10/3/2020 tarihinde karar vermiştir. Dava istinaf incelemesinde derdesttir. Anılan kararın gerekçesinde dava dosyasındaki deliller belirtilen ceza yargılamalarıyla birlikte değerlendirilmiş ve eşinin başvurucuya şiddet uyguladığı, başvurucuyu tehdit ettiği, yaşadığımız toplumun değer yargılarıyla bağdaşmayacak şekilde

kıskandıđı, bu kıskaçlık nedeniyle başvurucuya psikolojik şiddet uyguladıđı tespitlerine yer verilmiştir.

IV. İLGİLİ HUKUK

19. İlgili hukuk (ulusal mevzuat, yargı kararları, uluslararası düzenlemeler ve Avrupa İnsan Hakları Mahkemesi kararları) için bkz. E.Ü. [GK], B. No: 2016/1310, 17/9/2020, §§ 22-51; Bestami Erođlu [GK], B. No: 2018/23077, 17/9/2020, §§ 42-83.

20. 5237 sayılı Kanun'un "Özel hayatın gizliliđini ihlal" kenar başlıklı 134. maddesinin (1) numaralı fıkrası şöyledir:

"Kişilerin özel hayatının gizliliđini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliđin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır"

21. 5237 sayılı Kanun'un "Verileri hukuka aykırı olarak verme veya ele geçirme" kenar başlıklı 136. maddesi şöyledir:

"(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır."

22. 5237 sayılı Kanun'un "Nitelikli hâller" kenar başlıklı 137. maddesinin ilgili kısmı şöyledir:

"(1) Yukarıdaki maddelerde tanımlanan suçların;

...

b) Belli bir meslek ve sanatın sağladıđı kolaylıktan yararlanmak suretiyle,

İşlenmesi hâlinde, verilecek ceza yarı oranında artırılır. "

23. Yönetmelik'in "Kayıtları İnceleme" kenar başlıklı 16. maddesi şöyledir:

"Hasta, sağlık durumu ile ilgili bilgiler bulunan dosyayı ve kayıtları, doğrudan veya vekili veya kanuni temsilcisi vasıtası ile inceleyebilir ve bir suretini alabilir. Bu kayıtlar, sadece hastanın tedavisi ile doğrudan ilgili olanlar tarafından görülebilir."

24. Yönetmelik'in "Bilgilerin Gizli Tutulması" kenar başlıklı 23. maddesinin ilgili kısmı şöyledir:

"Sağlık hizmetinin verilmesi sebebiyle edinilen bilgiler, kanun ile müsaade edilen haller dışında, hiçbir şekilde açıklanamaz.

Kişinin rızasına dayansa bile, kişilik haklarından bütünüyle vazgeçilmesi, bu hakların başkalarına devri veya aşırı şekilde sınırlandırılması neticesini doğuran hallerde bilginin açıklanması, bunları açıklayanın hukuki sorumluluğunu kaldırmaz.

Hukuki ve ahlaki yönden geçerli ve haklı bir sebebe dayanmaksızın hastaya zarar verme ihtimali bulunan bilginin ifşa edilmesi, personelin ve diğer kimselerin hukuki ve cezai sorumluluğunu da gerektirir..."

25. 17/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu'nun "Bir suçun işlendiğini öğrenen Cumhuriyet savcısının görevi" kenar başlıklı 160. maddesi şöyledir:

"(1) Cumhuriyet savcısı, ihbar veya başka bir suretle bir suçun işlendiği izlenimini veren bir hâli öğrenir öğrenmez kamu davasını açmaya yer olup olmadığına karar vermek üzere hemen işin gerçeğini araştırmaya başlar.

(2) Cumhuriyet savcısı, maddî gerçeğin araştırılması ve adil bir yargılamanın yapılabilmesi için, emrindeki adli kolluk görevlileri marifetiyle, şüphelinin lehine ve aleyhine olan delilleri toplayarak muhafaza altına almakla ve şüphelinin haklarını korumakla yükümlüdür."

26. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Amaç" kenar başlıklı 1. maddesinin ilgili kısmı şöyledir:

"Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir."

27. 6698 sayılı Kanun'un "Özel nitelikli kişisel verilerin işlenmesi şartları" kenar başlıklı 6. Maddesi şöyledir:

"(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama

yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır."

28. 6698 sayılı Kanun'un "Kişisel verilerin aktarılması" kenar başlıklı 8. maddesinin ilgili kısmı şöyledir:

"(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz..."

29. 6698 sayılı Kanun'un "Veri güvenliğine ilişkin yükümlülükler" kenar başlıklı 12. maddesinin ilgili kısmı şöyledir:

"(1) Veri sorumlusu;

- a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
- c) Kişisel verilerin muhafazasını sağlamak,

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

...

(3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

...

(5) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir."

V. İNCELEME VE GEREKÇE

30. Anayasa Mahkemesinin 3/2/2022 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları

31. Başvurucu, evlilik dönemi öncesine ait hastane kayıtları ile sağlık bilgilerinin boşanma aşamasında olduğu eşi tarafından hukuka aykırı olarak ele geçirildiğini vurgulamıştır. Eşinin doktor

olarak görev yaptığını, görevinin ayrıcalığını kullanarak görev yapmadığı hastanenin kayıtlarına ulaştığını ve bu eylemi gerçekleştirdiğini soruşturma aşamasında ikrar ettiğini ancak Başsavcılığın mevzuata aykırı bir kararla kişisel veri olduğunda şüphe olmayan bilgilerin ele geçirilmesini hukuka uygun gördüğünü ifade etmiştir. Talebine rağmen başvurusunun bilgilere nasıl ve hangi bilgisayardan ve kimin yardımıyla erişim sağladığı yönünde Başsavcılığın araştırma yapmadığını belirtmiştir. Ayrıca Başsavcılığın eşlerin diğer eş hakkındaki bilgilere ulaşabileceği şeklindeki gerekçesinin Anayasa'nın 20. maddesi kapsamında korunamayacağı gibi mevzuatta da eşlere böyle bir hakkı tanıyan düzenlemenin mevcut olmadığını iddia etmiştir. Ayrıca mevzuatta sağlık kayıtlarını kimin ve hangi şartlarda inceleyebileceğinin açıkça belirlendiğini, eşinin ikrar ettiği eylemin suç olduğunun kesin olduğunu, rızası dışında ele geçirilen kişisel verilerinin boşanma davasında kullanılmasının eşinin eylemini hukuka uygun hâle getirmeyeceğini belirten başvurucu; adil yargılanma hakkı ile özel hayata saygı hakkı ve kişisel verilerin korunması hakkının ihlal edildiğini ileri sürmüştür. Başvurucu, isminin kamuya açık belgelerde gizlenmesi talebinde bulunmuştur.

B. Değerlendirme

32. Anayasa'nın iddianın değerlendirilmesinde dayanak alınacak "Özel hayatın gizliliği" kenar başlıklı 20. maddesinin birinci ve üçüncü fıkraları şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

...

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

33. Anayasa'nın 20. maddesinin üçüncü fıkrasında herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı ayrıca düzenlenmiş ve güvence altına alınmıştır. Söz konusu anayasal güvence, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde koruma altına alınan özel hayata saygı hakkına karşılık gelmektedir. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve

özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır (AYM, E.2014/122, K.2015/123, 30/12/2015, §§ 19, 20).

34. Anayasa Mahkemesi kararlarında da belirtildiği üzere kişisel veri -belirli veya kimliği belirlenebilir olmak şartıyla- bir kişiye ilişkin bütün bilgileri ifade etmekte olup bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi sadece kimliğini ortaya koyan bilgileri değil telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, öz geçmiş, resim, görüntü ve ses kayıtları, parmak izleri, sağlık bilgileri, genetik bilgiler, IP adresi, e-posta adresi, alışveriş alışkanlıkları, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır (AYM, E.2014/74, K.2014/201, 25/12/2014; E.2014/180, K.2015/30, 19/3/2015).

35. Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı yönünden inceleme yapılabilmesi için öncelikle anılan hak kapsamında korunması gereken bir kişisel verinin olup olmadığı belirlenmelidir. Anayasa hükmünün lafzı, konuya ilişkin uluslararası belgeler ve karşılaştırmalı hukuk dikkate alındığında belirli veya belirlenebilir bir gerçek veya tüzel kişi hakkındaki her türlü bilgi kişisel veri olarak değerlendirilir. Ancak her davada ya da başvuruda Anayasa'nın 20. maddesinin üçüncü fıkrası anlamında bir kişisel veri bulunup bulunmadığı, davanın ve başvurunun kendine özgü koşulları dikkate alınarak tespit edilir. Bir kişisel verinin bulunduğu tespit edildiğinde bu veriye yönelik her türlü sınırlama ve müdahale Anayasa'nın anılan hükmü kapsamındaki güvenceleri harekete geçirir (E.Ü., § 59; Bestami Eroğlu, § 102; Bülent Kaya [GK], B. No: 2013/2941, 11/5/2016, § 49; Fatih Saraman [GK], B. No: 2014/7256, 27/2/2019, § 57; AYM, E.2014/74, K.2014/201, 25/12/2014; E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2013/84, K.2014/183, 4/12/2014).

36. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Somut olayda başvuru kişinin sağlık durumuna ilişkin bilgilerin ve kişiye özel hastane kayıtlarının belirli bir gerçek kişi hakkındaki bilgi olarak kabul edilmesi gerektiği, bu bağlamda anılan bilgilerin ele geçirilmesinin, bunların kullanılmasının ve işlenmesini kişisel verilerin korunması hakkı kapsamında kaldığı anlaşılmıştır. Somut olayda başvuru kişinin şikâyetlerinin özünü; sağlık durumu ve tedavilerine ilişkin bilgilerin dolayısıyla kişisel nitelikteki birtakım verilerinin hukuka aykırı olarak ele geçirilmesine ilişkin suç duyurusunda etkili bir ceza soruşturması yürütülmediği iddiası oluşturmaktadır. Bu durumda başvurunun Anayasa'nın 20. maddesinin güvence altına alınan kişisel verilerin korunmasını isteme hakkı yönünden değerlendirilmesi gerektiği sonucuna ulaşılmıştır.

1. Kabul Edilebilirlik Yönünden

37. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkının ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

2. Esas Yönünden

a. Genel İlkeler

38. Anayasa'nın 20. maddesinin üçüncü fıkrasının birinci cümlesinde genel olarak herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu belirtilmiş, ikinci cümlesinde kişisel veriler bağlamında bazı özel güvenceler sayılmış, üçüncü cümlesinde kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği düzenlenmiş, dördüncü cümlesinde ise kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hüküm altına alınmıştır. Buna göre lafzı dikkate alındığında Anayasa'nın 20. maddesinin üçüncü fıkrasının kişisel verilerin korunmasını isteme hakkı kapsamında sadece işleme şeklindeki sınırlama ya da müdahalelere karşı değil, kişisel verilere yönelik her türlü müdahale ve sınırlamalara karşı güvence getirdiği anlaşılmaktadır (E.Ü., § 63; Bestami Eroğlu, § 101).

39. Yine Anayasa'nın 12. maddesine göre herkes kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlere sahiptir. Bu genel nitelikteki anayasal düzenleme ile bireylerin kişilik değerlerine yönelen ve zarar veren olumsuz tutum ve davranışlar dışlanmaktadır. Ayrıca Anayasa'nın 5. maddesinde bireylerin temel hak ve özgürlüklerinin korunması, maddi ve manevi varlıklarının geliştirilmesi için gerekli şartların hazırlanması devletin temel amaç ve görevlerinden biri olarak sayılmaktadır. Bu düzenlemeler ışığında devletin bireyin temel hak ve özgürlüklerine keyfi olarak müdahale etmemenin yanında üçüncü kişilerin saldırılarını önlemekle yükümlü kıldığı, bu bağlamda pozitif yükümlülüklerinin de bulunduğu söylenebilir. Uyuşmazlıkların özel hukuk kişileri arasında gerçekleştiği durumlarda da temel hak ve özgürlüklerin sağladığı güvencelerin yerine getirilip getirilmediği denetlenirken Anayasa'nın kamusal makamlara yüklediği sorumluluklardan doğrudan özel hukuk kişileri sorumlu tutulamayacağından taşıdığı koşulların özelliklerine göre bu tür başvuruların devletin pozitif yükümlülükleri bağlamında ele alınması gerekebilir. Dolayısıyla özel hayatın korunması kapsamında kişisel verilerin korunmasını isteme hakkı yönünden de devletin pozitif bir yükümlülük olarak yetki alanında bulunan tüm bireyleri gerek kamusal makamların ve diğer bireylerin gerekse kişinin kendisinin eylemlerinden kaynaklanabilecek risklere karşı koruma yükümlülüğü bulunmaktadır (E.Ü., § 65; Ömür Kara ve Onursal Özbek, B. No:

2013/4825, 24/3/2016, §§ 45, 46; Ali Çığır, B. No: 2015/19298, 8/5/2019, §§ 32, 33; Erol Kumcu, B. No: 2015/18988, 9/5/2019, §§ 32, 33; U.B., B. No: 2015/3175, 10/10/2019, §§ 33, 34).

40. Bu anlamda öncelikle devlet, uyuşmazlıkların çözümüne ilişkin etkili yargısal sistem kurma yükümlülüğünü yerine getirmelidir. Söz konusu pozitif yükümlülük; olayın meydana gelme şekli ile etkisi, ağırlığı ve sonuçları bakımından yapılacak değerlendirmelere ve olayın kim tarafından nasıl gerçekleştirildiği konusunda aydınlatılmasını gerekli kılan durumların bulunup bulunmadığına göre her durumda ceza soruşturması/yargılaması yapılmasını gerekli kılmaz. Nitekim yargısal sistem kurma yükümlülüğü -olayın koşullarına göre- hukuki ve idari yolların devlet tarafından oluşturulmasıyla da yerine getirilebilir. Bu bağlamda bazı durumlarda disiplin soruşturması ile de devletin aydınlatma yükümlülüğünü yerine getirmesi mümkün olabilir (Ali Çığır, § 34; Erol Kumcu, § 34).

41. Öte yandan yargısal sistem kurma yükümlülüğünün ceza soruşturması/yargılaması yapılmasını gerekli kılması, failer hakkında mutlaka ceza davası açılmasını ya da onların cezalandırılmasını zorunlu hâle getirmediği gibi başvuruçulara üçüncü tarafları bir suç nedeniyle yargılatma ya da cezalandırılmalarını talep etme hakkı da vermemektedir. Zira burada kastedilen sonuç yükümlülüğü değil uygun araçların kullanılması yükümlülüğüdür. Ancak her durumda söz konusu yargısal sistemlerin etkili şekilde işletilmesi ve soruşturmalar ya da yargılamalar neticesinde yargısal makamlarca ulaşılan tüm sonuçların temel hakların içerdiği güvenceleri koruyacak şekilde ilgili ve yeterli gerekçelerle açıklanması gerekir (Ali Çığır, § 35; Erol Kumcu, § 35).

42. Ek olarak ayrıca vurgulamak gerekir ki kişilerin cezai sorumluluğuna ilişkin hukuki sorunların incelenmesi, ceza soruşturması/kovuşturması sürecinin mahkûmiyet kararı ile sonuçlanması, bu hâlde takdir edilecek cezanın miktar ve mahiyetinin belirlenmesi Anayasa Mahkemesinin görev alanı içinde olmayıp bu husus esasen derece mahkemelerinin takdirindedir (Ali Çığır, § 36; Erol Kumcu, § 36).

b. İlkelerin Uygulanması

43. Öncelikle devletin pozitif yükümlülüğünün kişisel verilerin korunması kapsamında üçüncü kişilerin müdahalelerine karşı yasal altyapı oluşturulması yanında bu altyapının hakkın ihlaline etkili yargısal tepki vermeyi de içerdiği vurgulanmalıdır. Bu bağlamda devletin kişisel verilerin korunması kapsamında kişisel verilerin hukuka aykırı olarak ele geçirilmesine, işlenmesine ve açıklanmasına yönelik önleyici tedbirler alması ve benzer durumların bir daha yaşanmaması için bunu yapanlara karşı caydırıcı yargısal tepki göstermesi gerekir. Bu yargısal tepkinin adli ceza biçiminde olması zorunlu değildir. Ancak bu tür müdahalelerin kanunda suç olarak düzenlenmesi hâlinde ceza

soruşturması ve kovuşturmasının etkili bir biçimde yürütülmesinin sağlanması da devletin pozitif yükümlülüklerinin gereğidir (benzer değerlendirmeler için bkz. Ferhat Ölmez, B. No: 2018/20040, 10/3/2021, § 29; B.Y., B. No: 2018/30296, 7/9/2021, § 39).

44. Başvuru konusu olayda başvurucunun eşi, başvurucunun evlilik öncesi geçirdiği hastalıklara ilişkin bilgileri içeren hastane kayıt bilgilerine ulaşarak bu bilgileri boşanma davasında delil olarak sunmuştur. Başvurucunun gördüğü tedaviler ile sağlık durumuna ve geçirdiği hastalıklara ilişkin bilgilerin başvurucuya ilişkin kişisel veri niteliğinde olduğu, kişisel veri mahiyetindeki bilgilerin hukuka aykırı olarak ele geçirilmesinin ve açıklanmasının da mevzuatta suç olarak düzenlendiği açıktır. Ayrıca 6698 sayılı Kanun'un (bkz. §§ 27-29) işlenen kişisel verilerin aktarılmasının kişinin açık rızasının varlığına bağlı olduğu, 6. maddede özel nitelikli kişisel veri kapsamında sayılan sağlık bilgilerinin aynı maddede belirtilen istisnalar dışında kişinin açık rızası olmaksızın işlenmesinin yasak olduğunun düzenlendiği ve veri sorumlusuna da uhdesinde bulunan kişisel verilerin hukuka aykırı olarak erişilmesini önleyecek tedbirleri alma çerçevesinde yükümlülükler öngörüldüğü vurgulanmalıdır. Bununla birlikte Yönetmelik ile de hasta haklarına ilişkin ayrıca düzenleme yapılmış, bu kapsamda kişiye özel hastane kayıtlarının açıklanması ve işlenmesi sıkı şartlara bağlanmıştır (bkz. §§ 23,24). Bu durumda başvurucunun şikâyetlerine ilişkin ilgili mevzuat da gözetilerek etkili bir ceza soruşturması yapılması, bu bağlamda öncelikle olayın tüm yönleriyle açıklığa kavuşturularak ulaşılan sonucun olaya özgü gerekçelerle açıklanması gerektiği söylenebilir.

45. Bu hâlde bireysel başvuru kapsamında yapılacak değerlendirmede dikkate alınacak husus; belirtilen çerçeve içinde yeterli usule ilişkin güvencelerin sunulduğu bir cezai takibatın yürütülüp yürütülmediğine, soruşturmanın bağımsız, özenli, süratli, etkili şekilde yapılıp yapılmadığına ve ulaşılan sonuçların temel hakların içerdiği güvenceleri koruyacak şekilde ilgili ve yeterli gerekçelerle açıklanıp açıklanmadığına ilişkin olacaktır (Ali Çığır, § 38; Erol Kumcu, § 38).

46. Öncelikle somut başvuruya konu soruşturma sürecinde başvurucunun şikâyeti üzerine Başsavcılık tarafından soruşturmaya derhâl başlandığı ve bu kapsamda şüphelinin ifadesinin alındığı, iddialarla ilgili olarak devlet hastanesiyle yazışma yapıldığı ve boşanma davasının incelendiği görülmüştür. Başvurucunun şikâyeti doğrultusunda Başsavcılık tarafından yapılan değerlendirme neticesinde elde edilen bilgilerin anılan dava kapsamında kullanılmış olması ve ilgili mahkemenin bu bilgileri değerlendirmekte takdir yetkisi de gözetilerek bir değerlendirme yapıldığı anlaşılmıştır.

47. Öte yandan Başsavcılığa anılan Hastane tarafından verilen cevapta başvurucunun hastane kayıtlarına ilişkin sorgulama ve çıktı alma işlemlerini A.G. isimli memurun yaptığı bildirilmiştir. Bu

cevabi bilgi ile eşinin hastane kayıtlarını kendisinin ele geçirdiği yönündeki ikrarının çeliştiğini ileri süren başvuruçunun soruşturmanın genişletilmesi taleplerinin Başsavcılık tarafından karşılanmadığı görülmüştür. Bu bağlamda Başsavcılık tarafından eşle ilgili kişisel verilere diğer eşin erişme hakkının olduğu ön kabulüyle hareket edildiği, Başsavcılığın başvuruçunun eşinin ne zaman ve nasıl bu bilgilere ulaştığı, hastane kayıtlarına girmek için şifre gerekip gerekmediği gibi hususları araştırmadığı görülmüştür. Ayrıca başvuruçunun eşinin boşanma davasında 19/12/2018 tarihinde sunmuş olduğu dilekçesinde başvuruçuya ait kişisel verileri edindiği anlaşılmasına rağmen Başsavcılığın anılan tarih öncesini kapsayacak şekilde bir araştırma yapmadığı, A.G.nin ifadesini de almadığı gözetildiğinde soruşturmanın genişletilip gerekli inceleme yapılmayarak olayın tam aydınlatılmadığı anlaşılmıştır.

48. Ayrıca yargılama süreci gözetildiğinde başvuruçunun evlenmeden önceki tedavisiyle ilgili bilgileri eşine daha önce açıklamadığı, bununla birlikte kişisel veri mahiyetindeki bu bilgilerin eşî dâhil üçüncü kişilere verilmesi yönünde açık bir rızasının da olmadığı görülmüştür. Bu duruma rağmen Başsavcılık eşlerin diğer eş hakkında birinci dereceden yakını olması nedeniyle kişisel ve sağlık bilgilerine ulaşma hakkının bulunduğu, bu nedenle şüphelinin eyleminin mahremiyetin ve özel hayatın ihlali olarak değerlendirilemeyeceği şeklinde yasal dayanağı gösterilmeyen birtakım gerekçelerle sonuca ulaşmıştır. Bu gerekçenin keskin bir kabulden yola çıkılarak oluşturulduğu, istisnasız bir kural yaklaşımıyla ele alındığı, kişisel verilerin korunmasını isteme hakkı ve hasta hakları bakımından kişiyi korumasız bıraktığı, ayrıca benzer müdahaleler yönünden caydırıcılığı olmadığı açıktır. Açıklanan bu gerekçenin temel hakların içerdiği güvenceleri koruduğu ve bu yönüyle ilgili ve yeterli olduğu söylenemez.

49. Dolayısıyla olayın aydınlatılmasına yönelik esaslı iddiaların Başsavcılık tarafından araştırılmaması, bu suretle soruşturmanın derinleştirilmemesi ve yasal dayanağı gösterilmeyen gerekçelerle sonuca ulaşılması nedeniyle anayasal hakların güvence altına alınacak şekilde etkili ve özenli bir soruşturma yapıldığı söylenemeyecektir. Ayrıca gerek kovuşturmayaya yer olmadığına dair karar gerekse bu karara karşı yapılan itiraz neticesinde verilen karar incelendiğinde yargı mercilerince ulaşılan sonuçların kişisel verileri ve hasta haklarını koruyacak şekilde ilgili ve yeterli gerekçeler içermediği sabittir.

50. Sonuç olarak soruşturmanın etkili ve özenli şekilde yürütülmesi konusunda kamusal makamlarca üstlenilmesi gereken pozitif yükümlülüğün gerektirdiği şartların somut olayda yerine getirilmediği değerlendirildiğinden Anayasa'nın 20. maddesinde düzenlenen özel hayata saygı kapsamında kişisel verilerin korunmasını isteme hakkının ihlal edildiği sonucuna varılmıştır.

3. 6216 Sayılı Kanun'un 50. Maddesi Yönünden

51. 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 50. maddesinin ilgili kısmı şöyledir:

“(1) Esas inceleme sonunda, başvurunun hakkının ihlal edildiğine ya da edilmediğine karar verilir. İhlal kararı verilmesi hâlinde ihlalin ve sonuçlarının ortadan kaldırılması için yapılması gerekenlere hükmedilir...

(2) Tespit edilen ihlal bir mahkeme kararından kaynaklanmışsa, ihlali ve sonuçlarını ortadan kaldırmak için yeniden yargılama yapmak üzere dosya ilgili mahkemeye gönderilir. Yeniden yargılama yapılmasında hukuki yarar bulunmayan hâllerde başvuru lehine tazminata hükmedilebilir veya genel mahkemelerde dava açılması yolu gösterilebilir. Yeniden yargılama yapmakla yükümlü mahkeme, Anayasa Mahkemesinin ihlal kararında açıkladığı ihlali ve sonuçlarını ortadan kaldıracak şekilde mümkünse dosya üzerinden karar verir.”

52. Başvurucu; yeniden yargılanmaya ve 50.000 TL manevi tazminat ödenmesine karar verilmesi talebinde bulunmuştur.

53. Anayasa Mahkemesinin Mehmet Doğan ([GK], B. No: 2014/8875, 7/6/2018) kararında ihlal sonucuna varıldığında ihlalin nasıl ortadan kaldırılacağı hususunda genel ilkeler belirlenmiştir. Anayasa Mahkemesi diğer bir kararında ise bu ilkelerle birlikte ihlal kararının yerine getirilmemesinin sonuçlarına da değinmiş ve bu durumun ihlalin devamı anlamına geleceği gibi ilgili hakkın ikinci kez ihlal edilmesiyle sonuçlanacağına işaret etmiştir (Aligül Alkaya ve diğerleri (2), B. No: 2016/12506, 7/11/2019).

54. Bireysel başvuru kapsamında bir temel hakkın ihlal edildiğine karar verildiği takdirde ihlalin ve sonuçlarının ortadan kaldırıldığından söz edilebilmesi için temel kural, mümkün olduğunca eski hâle getirmenin yani ihlalden önceki duruma dönülmesinin sağlanmasıdır. Bunun için ise öncelikle ihlalin kaynağı belirlenerek devam eden ihlalin durdurulması, ihlale neden olan karar veya işlemin ve bunların yol açtığı sonuçların ortadan kaldırılması, varsa ihlalin sebep olduğu maddi ve manevi zararların giderilmesi, ayrıca bu bağlamda uygun görülen diğer tedbirlerin alınması gerekmektedir (Mehmet Doğan, §§ 55, 57).

55. İhlalin kovuşturmayaya yer olmadığı ya da daimî arama kararı gibi bazı nedenlerle soruşturmanın sonlandırılmasından kaynaklandığı durumlarda Anayasa Mahkemesi, 6216 sayılı Kanun'un 50. maddesinin (2) numaralı fıkrası ile Anayasa Mahkemesi İçtüzüğü'nün 79. maddesinin (1) numaralı fıkrasının (a) bendi uyarınca ihlalin ve sonuçlarının ortadan kaldırılması için yeniden soruşturma

yapılması için kararın bir örneğinin ilgili Cumhuriyet başsavcılığına gönderilmesine hükmeder. Anılan yasal düzenleme, usul hukukundaki benzer hukuki kurumlardan farklı olarak, ihlali ortadan kaldırmak amacıyla yeniden soruşturma yapılması sonucunu doğuran ve bireysel başvuruya özgülünen bir giderim yolunu öngörmektedir. Bu nedenle Anayasa Mahkemesi tarafından ihlal kararına bağlı olarak yeniden soruşturma yapılması kararı verildiğinde usul hukukundaki yargılamanın yenilenmesi kurumundan farklı olarak ilgili Cumhuriyet başsavcılığının yeniden soruşturma yapılması sebebinin varlığını kabul hususunda herhangi bir takdir yetkisi bulunmamaktadır. Dolayısıyla böyle bir kararın kendisine ulaştığı Cumhuriyet başsavcılığının yasal yükümlülüğü, ilgilinin talebini beklemeksizin Anayasa Mahkemesinin ihlal kararı nedeniyle yeniden soruşturma yapma kararı vererek devam eden ihlalin sonuçlarını gidermek üzere gereken işlemleri yerine getirmektir (benzer yöndeki kararlar için bkz. Mehmet Doğan, §§ 58, 59; Aligül Alkaya ve diğerleri (2), §§ 57-59, 66, 67).

56. İncelenen başvuruda başvuruya konu Başsavcılık soruşturmasında olayın aydınlatılmasına yönelik esaslı iddiaların Başsavcılık tarafından araştırılmaması, bu suretle soruşturmanın derinleştirilmemesi ve somut olaya uygun olmayan gerekçelerle sonuca ulaşılması nedeniyle özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkının ihlal edildiğine karar verilmiştir. Buna göre ihlalin soruşturma makamlarının işlemlerinden kaynaklandığı anlaşılmaktadır. Ayrıca itiraz mercii de ihlali giderememiştir.

57. Bu durumda kişisel verilerin korunmasını isteme hakkının ihlalinin sonuçlarının ortadan kaldırılması için yeniden soruşturma yapılmasında hukuki yarar bulunmaktadır. Yapılacak yeniden soruşturma ise bireysel başvuruya özgü düzenleme içeren 6216 sayılı Kanun'un 50. maddesinin (2) numaralı fıkrasına göre ihlalin ve sonuçlarının ortadan kaldırılmasına yöneliktir. Bu kapsamda Cumhuriyet başsavcılığının yapması gereken iş, önceki kovuşturmayaya yer olmadığına dair kararını kaldırmak ve akabinde ihlal kararında tespit edilen eksiklikleri giderecek şekilde yeni bir soruşturma yapmaktan ibarettir. Bu sebeple kararın bir örneğinin yeniden soruşturma yapılmak üzere Afyonkarahisar Cumhuriyet Başsavcılığına gönderilmesine karar verilmesi gerekir.

58. İhlalin ve sonuçlarının ortadan kaldırılması için yeniden soruşturmanın yeterli bir giderim sağlayacağı anlaşıldığından tazminat talebinin reddine karar verilmesi gerektiği sonucuna ulaşılmıştır.

59. Dosyadaki belgelerden tespit edilen 364,60 TL harç ve 4.500 TL vekâlet ücretinden oluşan toplam 4.864,60 TL yargılama giderinin başvurucuya ödenmesine karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Başvurucunun kamuya açık belgelerde kimliğinin gizli tutulması talebinin KABULÜNE,

B. Kişisel verilerin korunmasını isteme hakkının ihlal edildiğine ilişkin iddianın KABUL EDİLEBİLİR OLDUĞUNA,

C. Anayasa'nın 20. maddesinde güvence altına alınan kişisel verilerin korunmasını isteme hakkının İHLAL EDİLDİĞİNE,

D. Kararın bir örneğinin kişisel verilerin korunmasını isteme hakkının ihlalinin sonuçlarının ortadan kaldırılması için yeniden soruşturma yapılmak üzere Afyonkarahisar Cumhuriyet Başsavcılığına (Soruşturma No: 2019/193) GÖNDERİLMESİNE,

E. Başvurucunun tazminat talebinin REDDİNE,

F. 364,60 TL harç ve 4.500 TL vekâlet ücretinden oluşan toplam 4.864,60 TL yargılama giderinin başvurucuya ÖDENMESİNE,

G. Ödemenin, kararın tebliğini takiben başvurucunun Hazine ve Maliye Bakanlığına başvuru tarihinden itibaren dört ay içinde yapılmasına, ödemede gecikme olması hâlinde bu sürenin sona erdiği tarihten ödeme tarihine kadar geçen süre için yasal FAİZ UYGULANMASINA,

H. Kararın bir örneğinin bilgi için Afyonkarahisar 1. Sulh Ceza Hâkimliğine (2019/782 D.İş) GÖNDERİLMESİNE,

İ. Kararın bir örneğinin Adalet Bakanlığına GÖNDERİLMESİNE 3/2/2022 tarihinde OYBİRLİĞİYLE karar verildi.

Anayasa Mahkemesi - Samet Ayyıldız Kararı (2018/34548)

Samet Ayyıldız, B. No: 2018/34548, 28/12/2021

Başvuru, özel bir şirkette çalışan başvurucunun WhatsApp adlı mesajlaşma programını kullanarak yaptığı yazışmaların işveren tarafından incelenmesi ve bu yazışmalar gerekçe gösterilerek iş akdinin feshedilmesi nedeniyle özel hayata saygı hakkı ile haberleşme hürriyetinin ihlal edildiği iddialarına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

BİRİNCİ BÖLÜM

KARAR

SAMET AYYILDIZ BAŞVURUSU

(Başvuru Numarası: 2018/34548)

Karar Tarihi: 28/12/2021

R.G. Tarih ve Sayı: 11/2/2022-31747

BİRİNCİ BÖLÜM

KARAR

Başkan: Hasan Tahsin GÖKCAN

Üyeler: Hicabi DURSUN, Yusuf Şevki HAKYEMEZ, Selahaddin MENTEŞ, İrfan FİDAN

Raportör: Ferhat YILDIZ

Başvurucu: Samet AYYILDIZ

Vekili: Av. Öznur AYYILDIZ

I. BAŞVURUNUN KONUSU

1. Başvuru, özel bir şirkette çalışan başvurucunun WhatsApp adlı mesajlaşma programını kullanarak yaptığı yazışmaların işveren tarafından incelenmesi ve bu yazışmalar gerekçe gösterilerek iş akdinin feshedilmesi nedeniyle özel hayata saygı hakkı ile haberleşme hürriyetinin ihlal edildiği iddialarına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 22/11/2018 tarihinde yapılmıştır.
3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.
4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.
5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.
6. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık, görüşünü bildirmiştir.
7. Başvurucu, Bakanlık görüşüne karşı beyanda bulunmuştur.

III. OLAY VE OLGULAR

8. Başvuru formu ve eklerinde ifade edildiği ve Ulusal Yargı Ağı Bilişim Sistemi (UYAP) üzerinden tespit edilen şekliyle ilgili olaylar özetle şöyledir:
9. Özel bir şirket çalışanı olan ve 1/5/2015 tarihinden itibaren şirketin hizmet sağladığı Sağlık Bakanlığına bağlı bir devlet hastanesinde (kurum) bilgi işlem sorumlusu olarak görev yapan başvurucunun iş sözleşmesi 22/11/2017 tarihinde feshedilmiştir.
10. UYAP üzerinden edinilen bilgilere göre başvurucunun işveren şirket tarafından 16/11/2017 tarihli yazı ile gerçeğe aykırı beyanla izin almaya çalıştığı, mesajlaşma programı ile çalışma arkadaşları ile firma ve kurum yöneticilerine karşı iftira ve hakaret ettiği, çalışma arkadaşlarıyla birlikte örgütlü bir biçimde bilişim sistemini sekteye uğrattığı hususlarında savunması istenmiştir. Başvurucu, savunmasını 21/11/2017 tarihinde göndermiş ve 22/11/2017 tarihinde iş akdi bildirimsiz olarak feshedilmiştir.
11. Başvurucu 20/12/2017 tarihinde Ordu İş Mahkemesinde (Mahkeme) işe iade istemiyle dava açmıştır. Dava dilekçesinde başvurucu; iş akdinin haksız olarak feshedildiğini, feshe dayanak yapılan mesajlaşma programının çok yaygın olarak kullanıldığını, bu yazışmaların kişisel veri olarak korunması gerektiğini, bu konuşmaların elde edilmiş şeklinin muğlak olduğunu, konuşmaların hukuka aykırı delil niteliğinde olduğunu ifade etmiştir.

12. Davalı şirket vekili davaya cevabında; davanın yasal süresi içinde açılmadığını, feshin 10/6/2003 tarihli ve 4857 sayılı İş Kanunu'nun 25. maddesine göre yapıldığını, bu nedenle bildirimsiz ve

tazminatsız yapılabileceğini, ayrıca fesih bildirimının yapılmasını engellemek amacıyla başvuru sahibinin sürekli olarak rapor aldığı, fesih sebebi olan WhatsApp yazışmalarının görev başındayken kendisine tahsis edilen bilgisayarda gerçekleştirildiğini, başvuru sahibinin bilgisayarı açık bırakması sonucunda sorumlu olan amirin yazışmaları elde ettiğini vurgulamıştır. Dilekçede ayrıca feshe dayanak yazışmalarda ağır şekilde sövmeler, iftiralar ve tehditler bulunduğu, başvuru sahibinin sürekli rapor olarak iş akışını bozduğu, bu nedenlerle feshin haklı olduğu belirtilmiştir.

13. Davalı Sosyal Güvenlik Kurumu (SGK) vekili davaya cevabında; SGK ile başvuru sahibi arasında bir iş sözleşmesinin olmadığını, davalı şirketle aralarında ihale ilişkisinin bulunduğunu, başvuru sahibinin tüm özlük işlemlerinin davalı şirket tarafından yürütüldüğünü, bu nedenle kendilerine husumet yöneltilemeyeceğini, davanın öncelikle husumet yönünden reddi gerektiğini ifade etmiştir. Bunun yanında feshe dayanak olan yazışmaların hizmeti sekteye uğratmaya yönelik olduğu ve davanın reddi gerektiği vurgulanmıştır.

14. Mahkeme 31/5/2018 tarihinde davanın kabulüne, feshin geçersizliğine ve başvuru sahibinin işe iadesine karar vermiştir. Kararın gerekçesinde; fesih bildiriminin yazılı olarak yapılmadığı, bu nedenle şekil şartlarına uygun olmayan feshin geçersiz olduğu belirtilmiştir.

15. Davalıların vekillerinin anılan karara karşı yaptığı istinaf başvurusu Samsun Bölge Adliye Mahkemesi 8. Hukuk Dairesinin (Bölge Adliye Mahkemesi) 27/9/2018 tarihli kararıyla kabul edilmiş, mahkeme kararının kaldırılmasına ve davanın reddine kesin olarak karar verilmiştir. Kararın gerekçesinde; işverenin haklı nedenle derhâl fesih hakkını kullandığı, bu nedenle yazılı fesih şartı aranmadığı, başvuru sahibinin eylemleri nedeniyle yapılan feshin geçerli olduğu, feshe dayanak yapılan mesajlarda davalı şirket ve kurum yöneticilerine karşı küçük düşürücü, hakaret içeren yazışmaların bulunduğu ifade edilmiştir.

16. Nihai karar 14/11/2018 tarihinde başvuru sahibine tebliğ edilmiştir.

17. Başvuru sahibi 22/11/2018 tarihinde bireysel başvuru yapmıştır.

18. Öte yandan UYAP üzerinden yapılan incelemede başvuru sahibi ile benzer sebeple iş akdi feshedilen E.O.nun Mahkeme nezdinde açtığı dava kabul edilmiş ancak Samsun Bölge Adliye Mahkemesi 7. Hukuk Dairesinin 5/10/2018 tarihli kararıyla dosyanın esasını incelemeyen kaldırılmasına ve mahkemesine iadesine karar verilmiştir. Anılan karar üzerine Mahkemede yeniden yargılama yapılmış, konu ile ilgili maddi deliller toplanmış ve bu sefer davanın reddine karar verilmiştir. Bu karara karşı yapılan istinaf başvurusunun esasın reddi üzerine kararın kesinleştiği görülmüştür.

IV. İLGİLİ HUKUK

19. İlgili hukuk için bkz. E.Ü. [GK], B. No: 2016/13010, 17/9/2020, §§ 22-51.

V. İNCELEME VE GEREKÇE

20. Anayasa Mahkemesinin 28/12/2021 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları ve Bakanlık Görüşü

21. Başvurucu; iş akdinin haksız olarak feshedildiğini, WhatsApp mesajlaşma programının 3. kişilerin erişimine kapalı olduğunu, bu nedenle bu mesaj içeriklerinin hukuka aykırı delil niteliğinde bulunduğunu, çalışanların kendi aralarında iletişim grubu kurmalarının ve burada iletişim hâlinde olmalarının hukuka aykırı olmadığını iddia etmiştir. Savunması beklenmeden iş akdinin feshedildiğini, Mahkemece dosyanın esasına girilmeden feshin şekil şartlarından yoksun olduğundan bahisle davanın kabulüne karar verilmesine rağmen Bölge Adliye Mahkemesince deliller toplanmadan ve sadece davalı tarafın iddiaları dikkate alınarak karar verildiğini ileri sürmüştür. Diğer yandan başvurucu, kendisi ile aynı durumdaki diğer çalışanların davasında istinaf incelemesinde kararın bozulmasına hükmedildiğini ve ilk derece mahkemelerince esas incelemelerinin yapıldığını ifade etmiştir. Kendisi hakkında ise tanıklar dinlenmeden, deliller toplanmadan karar verilmesi nedeniyle adil yargılanma hakkının ihlal edildiğini, kişisel veri niteliğindeki mesajların delil olarak kullanılması nedeniyle özel hayatın gizliliği hakkının ihlal edildiğini iddia etmiştir.

22. Bakanlık görüşünde, başvurucunun kurum bilgisayarındaki WhatsApp isimli mesajlaşma programı aracılığıyla sistem üzerinden arkadaşları ile birlikte şirket ve kurum yöneticilerine karşı hakarete bulunduğu, çalışma arkadaşları ile birlikte örgütlü bir biçimde bilişim sistemini sekteye uğrattığı belirtilmiş; ahlak ve iyi niyet kurallarına uymayan bu davranışları nedeniyle iş ilişkisinin sürdürülemeyeceği gerekçeleri ile iş sözleşmesinin feshedildiğinin anlaşıldığı ifade edilmiştir. Görüşte ayrıca kamu makamları tarafından başvurucunun özel hayatına doğrudan bir müdahale gerçekleştirilmediği, bu nedenle devletin pozitif yükümlülükleri kapsamında inceleme yapılması gerektiği, bu kapsamda idari ve yargısal kararların ilgili ve yeterli gerekçe içerip içermediğinin, verilen kararlarda başvurucunun özel ve aile hayatına saygı hakkı ile onun ödev ve sorumlulukları arasında adil bir denge kurulup kurulmadığının takdirinin Anayasa Mahkemesinde olduğu vurgulanmıştır.

23. Bakanlık görüşüne karşı beyanında başvurucu vekili; karara dayanak gösterilen yazışmaların hukuka aykırı olarak ele geçirildiğini, delillerin mahkemece değerlendirilmeden karar verildiğini, bu

nedenlerle öncelikle yeniden yargılama yapılmasına, mümkün değilse tazminata hükmedilmesi gerektiğini belirtmiştir.

B. Değerlendirme

24. Anayasa'nın iddianın değerlendirilmesinde dayanak alınacak "Özel hayatın gizliliği" kenar başlıklı 20. maddesinin birinci ve üçüncü fıkrası şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

...

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

25. Anayasa'nın "Haberleşme hürriyeti" kenar başlıklı 22. maddesi şöyledir:

"Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.

İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir."

26. Özel hayata saygı hakkı Anayasa'nın 20. maddesinde koruma altına alınmıştır. Bu anlamda devlet, kişilerin özel ve aile hayatına keyfi olarak müdahale etmemek ve üçüncü kişilerin haksız saldırılarını önlemekle yükümlüdür (E.Ü., § 56). Ayrıca Anayasa'nın 22. maddesinde güvence altına alınan haberleşme hürriyeti, haberleşmenin yanında içeriği ve biçimi ne olursa olsun haberleşmenin içeriğinin gizliliğini de güvence altına almaktadır. Haberleşme bağlamında bireylerin karşılıklı ve toplu olarak sözlü, yazılı ve görsel iletişimlerine konu olan ifadelerinin gizliliğinin sağlanması ve

haberleşmeye yönelik haksız müdahalelerde bulunulmaması gerekir (Yasemin Çongar ve diğerleri, B. No: 2013/7054, 6/1/2015, § 49; E.Ü., § 60).

27. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Somut olayda işverenin başvurucağın işyeri bilgisayarını kullanarak yaptığı mesajlaşmalarını denetlemesi ve içeriğini incelemesi sonucu elde ettiği bilgileri iş ağıdının feshine dayanak yapması söz konusudur. Dolayısıyla başvurucağın iş arkadaşları ile WhatsApp adlı program üzerinden gerçekleştirdiği yazışmalarının incelendiği ve içeriklerine ulaşıldığı gözetildiğinde başvurucağın özel hayata saygı hakkı ile haberleşme hürriyeti yönünden incelenmesi gerektiği değerlendirilmiştir.

1. Kabul Edilebilirlik Yönünden

28. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan özel hayata saygı hakkı ile haberleşme hürriyetinin ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

2. Esas Yönünden

a. Genel İlkeler

29. Anayasa ve Sözleşme'nin ortak koruma alanı kapsamında kalan temel haklar, yalnızca kamusal gücün doğrudan uygulanmasıyla değil kimi zaman da özel hukuk kişileri arasındaki uyuşmazlıklara konu olacak şekilde üçüncü kişilerin müdahaleleriyle zedelenebilmektedir. İlkinde söz konusu güvencelerin sağlanması adına kamusal makamlara yüklenen negatif ve pozitif tüm yükümlülüklerin doğrudan yerine getirilmesi konusunda tereddüt bulunmamakta ise de ikinci durumda devletin üçüncü kişilerin müdahalelerine karşı bireylere ne tür bir koruma imkânı sunması gerektiği ve hangi çerçevede yükümlülükler taşıdığı hususunda her olayın kendine özgü koşullarına göre değerlendirmelerde bulunulması gerekmektedir (Ömür Kara ve Onursal Özbek, B. No: 2013/4825, 24/3/2016, § 45; E.Ü., § 64).

30. Yine Anayasa'nın 12. maddesine göre herkes kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlere sahiptir. Bu genel nitelikteki anayasal düzenleme ile bireylerin kişilik değerlerine yönelen ve zarar veren olumsuz tutum ve davranışlar dışlanmaktadır. Ayrıca Anayasa'nın 5. maddesinde bireylerin temel hak ve özgürlüklerinin korunması, maddi ve manevi varlıklarının geliştirilmesi için gerekli şartların hazırlanması devletin temel amaç ve görevlerinden biri olarak sayılmaktadır. Bu düzenlemeler ışığında devletin bireyin temel hak ve özgürlüklerine

keyfi olarak müdahale etmemenin yanında üçüncü kişilerin saldırılarını önlemekle yükümlü kılındığı, bu bağlamda pozitif yükümlülüklerinin de bulunduğu söylenebilir. Uyuşmazlıkların özel hukuk kişileri arasında gerçekleştiği durumlarda da temel hak ve özgürlüklerin sağladığı güvencelerin yerine getirilip getirilmediği denetlenirken Anayasa'nın kamusal makamlara yüklediği sorumluluklardan doğrudan özel hukuk kişileri sorumlu tutulamayacağı için taşıdığı koşulların özelliklerine göre bu tür başvuruların devletin pozitif yükümlülükleri bağlamında ele alınması gerekebilir. Dolayısıyla özel hayata saygı hakkı ve haberleşme hürriyeti yönünden de devletin pozitif bir yükümlülük olarak yetki alanında bulunan tüm bireyleri gerek kamusal makamların ve diğer bireylerin gerekse kişinin kendisinin eylemlerinden kaynaklanabilecek risklere karşı koruma yükümlülüğü bulunmaktadır (Ömür Kara ve Onursal Özbek, § 46; Ali Çığır, B. No: 2015/19298, 8/5/2019, §§ 32, 33; Erol Kumcu, B. No: 2015/18988, 9/5/2019, §§ 32, 33; Ulvi Bacıoğlu, B. No: 2015/3175, 10/10/2019, §§ 33, 34; E.Ü., § 65).

31. Pozitif yükümlülükler özel hukuk kişilerinin birbirleri ile olan uyuşmazlıklarının çözümüne ilişkin yasal altyapının oluşturulmasını, söz konusu uyuşmazlıkların adil yargılama gereklerine uygun ve usul yönünden güvenceleri haiz bir yargılama kapsamında incelenmesini, bu yargılamalarda temel haklara ilişkin anayasal güvencelerin gözetilip gözetilmediğinin denetlenmesini gerektirir. Bu doğrultuda derece mahkemelerince söz konusu güvenceler gözardı edilmemeli, işveren ve çalışanlar arasındaki çatışan çıkarlar adil biçimde dengelenmeli, başvuruların temel haklarına yönelik müdahalenin meşru amaca dayalı ve ölçülü olup olmadığı değerlendirilmeli, ulaşılan sonuç hakkında hüküm kurulurken ilgili ve yeterli gerekçeler sunulmalıdır (Ömür Kara ve Onursal Özbek, §§ 47-50; E.Ü., § 66).

32. Anayasa Mahkemesi daha önce iletişim araçlarının işveren tarafından denetlenmesi kapsamındaki uyuşmazlıklarda derece mahkemeleri tarafından devletin pozitif yükümlülükleri bağlamında çıkarların dengelenmesi ve müdahalenin ölçülülüğünün irdelenmesi kapsamında gözetilmesi gereken hususları genel olarak belirlemiş; buna göre somut olayın koşullarına göre iş sözleşmelerinde kısıtlayıcı ve zorlayıcı düzenlemelerin ne şekilde belirlendiği, tarafların bu düzenlemeler hakkında bilgilendirilip bilgilendirilmediği, çalışanların temel haklarına yönelik müdahalede bulunulmasına neden olan meşru amacın müdahale ile ölçülü olup olmadığı, sözleşmenin feshinin çalışanların eylem ya da eylemsizlikleri karşısında makul ve orantılı bir işlem olup olmadığı hususlarının uyuşmazlığın çözümünde gözetilmesi gerektiğini tespit etmiştir (Ömür Kara ve Onursal Özbek, § 50; E.Ü., § 67).

33. Yukarıda belirtilen hususlar gözetilerek işverenin işçinin iletişimini denetlemesi yetkisini özel hayata saygı hakkı ve haberleşme hürriyeti bağlamında devletin pozitif yükümlülükleri kapsamında irdelemek gerekmektedir. Öncelikle somut olayda olduğu gibi teknolojik gelişmelerin imkânlarından yararlanmak isteyen işverenlerin bilgisayar, internet, e-posta gibi iletişim araç ve gereçlerini çalışanın kullanıma sunması nedeniyle oluşan uyuşmazlıklarda işverenin menfaatleri ile işçinin temel hak ve özgürlükleri arasında bir dengeleme yapma gerekliliği doğmaktadır. Bu bağlamda işveren ile çalışan arasındaki ilişkinin iki taraf açısından da belirli hak ve yükümlülükler öngören ve esasen güven ilişkisi üzerine kurulu iş sözleşmesiyle şekillendiği unutulmamalıdır. Somut uyuşmazlığın ilgili olduğu iş hukukunun dinamik bir niteliğinin olduğu, ayrıca iş ilişkilerinin genel kurallardan farklı, kendine özgü bazı hukuki kurallar içerdiği de dikkate alınmalıdır (E.Ü., § 68).

34. Bu bağlamda işlerin etkin bir şekilde yürütülmesi ile bilgi akışının kontrolünü sağlamak, işçinin eylemlerine bağlı cezai ve hukuki sorumluluğa karşı korunmak, verimliliği ölçmek veya güvenlik endişeleri gibi haklı ve meşru görülebilecek nedenlerle işverenin yönetim yetkisi kapsamında kural olarak işçinin kullanımına sunduğu iletişim araçlarını denetleyebileceği ve kullanıma ilişkin sınırlamalar öngörebileceği söylenebilir. Ancak işverenin yönetim yetkisinin işyerinde işin yürütülmesi, işyerinin düzeninin ve güvenliğinin sağlanmasıyla sınırlı olduğu unutulmamalıdır. Bu bağlamda işverenin yetki ve haklarının sınırsız olmadığı, çalışana tanınan temel hak ve özgürlüklerin somut olayda haberleşme hürriyeti ve özel hayata saygı hakkının işyeri sınırları dâhilinde de korunduğu, aynı zamanda kısıtlayıcı ve uyulması zorunlu işyeri kurallarının çalışanların temel haklarının özünü zedeleyecek nitelikte olmaması gerektiği vurgulanmalıdır. Bu çerçevede işyerinde kullanıma sunulan iletişim araçlarının işverene ait olduğu gözetilerek sırf bu nedenle bile işverenin iletişim araçları üzerinde sınırsız ve mutlak bir gözetleme ve denetleme yetkisinin olduğunu kabul etmek, işçinin demokratik bir toplumda temel hak ve özgürlüklerine işyerinde de saygı gösterilmesi gerektiği yönündeki haklı beklentisiyle uyuşmayacaktır (E.Ü., § 69).

35. Nitekim Anayasa Mahkemesi benzer bir somut olaya ilişkin bulunan E.Ü. kararında derece mahkemelerince aşağıda belirtilen güvencelerin somut olayda hakka müdahale eden üçüncü kişi tarafından sağlanıp sağlanmadığının gereği gibi denetleyip denetlemediğinin incelenmesi gerektiğini vurgulamıştır (E.Ü., § 70):

i. İşverenin çalışanın kullanımına sunduğu iletişim araçlarının ve iletişim içeriklerinin incelenmesinin haklı olduğunu gösteren meşru gerekçeleri olup olmadığı denetlenmelidir. Bu durumda işverenin gerekçelerinin ifa edilen işin ve işyerinin özellikleri de gözetilerek meşru olup olmadığı

irdelenmelidir. Bu denetlemede iletişim akışı ile iletişim içeriklerinin incelenmesi arasında ayırım yapılarak içeriklerin incelenmesi yönünden daha ciddi gerekçeler aranmalıdır.

ii. Demokratik bir toplumda iletişimin denetlenmesi ve kişisel verilerin işlenmesi süreci şeffaf bir şekilde gerçekleştirilmeli ve bunun bir gereği olarak da süreçle ilgili olarak çalışanlar işveren tarafından önceden bilgilendirilmelidir. Uluslararası hukuk ve karşılaştırmalı hukuk dikkate alındığında bu bilgilendirmenin -somut olayın özelliklerine uygun düştüğü ölçüde- en azından iletişimin denetlenmesi ile kişisel verilerin işlenmesinin hukuki dayanağı ve amaçları, denetlemenin ve veri işlemenin kapsamı, verilerin saklanacağı süre, veri sahibinin hakları, denetlemenin ve işlemenin sonuçları ile verilerin muhtemel yararlanıcıları hususlarını kapsamaması gerekir. Ayrıca bildirimde iletişim araçlarının kullanımına ilişkin olarak işveren tarafından öngörülen sınırlamalara da yer verilmelidir. Bilgilendirmenin mutlaka belli şekilde yapılması şart olmayıp şeffaflığı sağlamak bakımından bireylere, kişisel verilerin işlenmesine ve iletişimin denetlenmesine ilişkin süreçten yukarıda belirtilen kapsamda haberdar olma imkânı sağlayan uygun bir yöntem tercih edilebilir.

iii. Çalışanın temel hak ve hürriyetlerine işveren tarafından yapılan müdahale, ulaşılmak istenen amaç ile ilgili ve bu amacı gerçekleştirmeye elverişli olmalıdır. Ayrıca inceleme faaliyetiyle elde edilen verilerin işveren tarafından hedeflenen amaç doğrultusunda kullanılması gerekir.

iv. İşveren tarafından yapılan müdahalenin gerekli kabul edilebilmesi için aynı amaca daha hafif bir müdahale ile ulaşılabilecek olması mümkün olmamalı, müdahale ulaşılmak istenen amaç bakımından zorunlu olmalıdır. Çalışanın iletişiminin içeriğine girilmesi yerine daha az müdahale içeren yöntem ve tedbirlerin uygulanmasının mümkün olup olmadığı denetlenmelidir. Bu kapsamda işverenin ulaşmak istediği amaca çalışanın iletişimi incelenmeden de erişilme imkânı olup olmadığı her bir vakianın somut özellikleri ışığında değerlendirilmelidir.

v. Müdahalenin orantılı kabul edilebilmesi için ise iletişimin denetlenmesi ile işlenecek veya herhangi bir şekilde yararlanılacak veriler ulaşılmak istenen amaçla sınırlı olmalı, bu amacı aşacak şekilde sınırlama ya da müdahaleye izin verilmemelidir.

vi. Ayrıca iletişimin incelenmesinin muhatabı olan çalışan üzerindeki etkisi ve çalışan bakımından sonuçları gözönünde tutularak tarafların çatışan menfaat ve haklarının adil bir biçimde dengelenip dengelenmediğine bakılması gerekmektedir. Taraflardan birine şahsi olarak aşırı bir külfet yüklendiğinin tespiti hâlinde devletin pozitif yükümlülüklerini yerine getirmediği sonucuna varılabilir.

b. İlkelerin Uygulanması

36. Başvurucu; WhatsApp adlı mesajlaşma programındaki yazışmalarının incelenmesinin özel hayat alanına ve haberleşme hürriyetine haksız bir müdahale oluşturmasına rağmen açtığı işe iade istemli davasında bu yönde bir tespit yapılmadığını, yazışmalarının işveren tarafından hukuka aykırı yöntemlerle elde edildiğini iddia etmiştir. Bu kapsamdaki iddiaların yukarıda belirtilen esaslar gözetilerek devletin pozitif yükümlülükleri bağlamında değerlendirilmesi gerekmektedir.

37. Öncelikle işverenin işçinin kullanımına sunulan iletişim araçlarını denetlemesine ilişkin olarak 4857 sayılı Kanun'da özel bir düzenleme olmadığı görülmüştür. Ancak Anayasa'nın 20. ve 22. maddelerinde yer bulan özel hayata saygı hakkına ve haberleşme hürriyetine ilişkin güvenceler ile hukuk sistemimizde mevcut olan düzenlemelerin iş hukuku uyumsuzluklarında uygulanması yönünde bir engel olmadığı gözetildiğinde yasal altyapı oluşturmak bağlamında pozitif yükümlülüklerin yerine getirilmiş olduğu söylenebilir (E.Ü., § 72).

38. Başvuru konusu olayda başvurucu, bir özel şirket çalışanı olup 1/5/2015 tarihinden itibaren bu şirketin hizmet sağladığı Sağlık Bakanlığına bağlı bir devlet hastanesinde bilgi işlem sorumlusu olarak görev yapmaktadır. Kurum yöneticilerinden birinin başvurucuya görevi için tahsis edilmiş bilgisayardaki WhatsApp yazışmalarını bir şekilde görerek bu yazışmaların içeriklerini temin ettiği ve bunların dayanak yapılarak başvurucunun iş sözleşmesinin feshedildiği anlaşılmaktadır.

39. Başvuru konusu olayda işveren şirket vekili davaya cevap dilekçesinde, mesaj içeriklerinin başvurucunun bilgisayarını açık bırakması sonucunda sorumlu olan amiri tarafından elde edildiğini ifade etmiştir. Anılan mesajlaşma programının işyerinin işleyişiyle bir ilgisinin bulunmadığı, başvurucu ve arkadaşları tarafından özel mesajlaşmalar için oluşturulduğu anlaşılmaktadır. Yargı kararlarından ve taraf dilekçelerinden başvurucu ile iş arkadaşları arasındaki mesajlaşmaların işyeri ve çalışanları ile ilgili özel görüşlerini içerdiği, içeriğinde bazı küçük düşürücü ifadelerin bulunduğu görülmektedir.

40. Öncelikle işyerinde kullanıma tahsis edilen bilgisayar üzerinden yapılan iletişimin denetlenebileceğine ve iletişim araçlarının kullanım koşullarına ilişkin olarak önceden tam ve açık bir bilgilendirme yapılmadığı hâllerde temel hak ve özgürlüklerinin işyerinde de korunacağı yönündeki haklı beklentiyle çalışan kişinin işyeri bilgisayarı üzerinden kişisel yazışmalar yapabileceğinin işveren tarafından da öngörülebilecek bir durum olduğu vurgulanmalıdır. Buradan hareketle çalışana açık bir bilgilendirmenin yapılmadığı hâllerde hak ve özgürlüklerine bir müdahalede bulunulmayacağı hususunda çalışanların makul bir beklenti içinde olacaklarının kabul edilmesi, temel hak ve özgürlüklerin sağladığı güvencelerden yararlandırılması gerektiği söylenebilir.

41. Somut olayda işverenin işyeri bilgisayarını inceleme yetkisi ile kapsamını gösteren bir bildirim başvurusuna yapıldığına ilişkin bilgi ve belge sunmadığı hususları gözetildiğinde işveren tarafından işyerinde kullanıma tahsis edilen bilgisayar üzerinden yapılan iletişimin izlenebileceği ve denetlenebileceği yönünde açık bir bilgilendirme yapılmadığı anlaşılmaktadır. Öte yandan özel hayat alanına dâhil olan WhatsApp mesajlaşma içerikleri gerekçe gösterilerek başvuruçunun iş akdi feshedilmiştir. Ancak işveren, davalı taraf olarak yargılama sürecinde müdahalenin meşru görülebilecek nedenlerini ve dayanaklarını, başvuruçunun beklentilerinin gözetildiğini ve haklarının dikkate alındığını, ayrıca müdahale konusunda başvuruçunun bilgilendirildiğini ortaya koyamamıştır. Bu bağlamda yargılama sürecinde feshin temel sebebini oluşturan WhatsApp mesajlaşma programı ile iletişime veya işyeri bilgisayarlarında özel iletişime yönelik olarak böyle bir bilgilendirmenin yapıp yapılmadığı derece mahkemelerince tartışılmamış, başvuruçunun kendisi alenileştirmedeği hâlde onun rızası alınmadan ve önceden bir bilgilendirme yapılmadan mesaj içeriklerine hukuka aykırı olarak erişildiği yönündeki esaslı iddialarının karşılanmadığı anlaşılmıştır.

42. Kaldı ki somut olayda kişisel kullanıma ilişkin olduğu herkesçe ve işverence bilinen söz konusu programın denetlenmesinin başvuruçunun özel hayatının ve haberleşmesinin gizliğinin korunması konusundaki makul beklentisine aykırı olduğu açıktır. Mahkemece de anılan programın kişisel kullanıma özgü bir mesajlaşma programı olduğunun herkesçe bilinebilir bir durum olmasına rağmen bu tür bir programın içerisinde yer alan yazışmaların ne suretle denetlendiğine ve içeriklerinin feshe dayanak alındığı hususunun gerekli olup olmadığına ve başvuruçunun özel hayatı ile haberleşmesine olan etkisine yönelik herhangi bir değerlendirme yapılmamıştır.

43. Bunun yanında işveren başvuruçunun bilgisayarındaki özel mesajları hukuka uygun bir yöntemle elde ettiğine yönelik de sağlıklı bir açıklama yapamamıştır. Yargılama aşamasında davalı şirket vekilinin davaya cevap dilekçesinden feshe dayanak olan mesajlaşma içeriklerinin başvuruçunun bilgisayarını açık bırakması sonucunda sorumlu olan amiri tarafından elde edildiği anlaşılmıştır. Bu anlamda başvuruçunun bilgisayarında yer alan iletişiminin içeriğine erişilmesini zorunlu kılan bir durumun mevcut olduğunun işveren tarafından açıklanmadığı görülmüştür. Ancak aynı amaca ulaşılabilmesi bakımından tarafların şikâyet ve savunmalarının analizi, tanıkların dinlenilmesi, işyeri kayıtları ile yürütülen projelerin süreç ve sonuçlarının incelenmesi gibi araçlar da mevcut olduğu hâlde niçin mesaj içeriklerinin incelenmesinin zorunlu ve gerekli görüldüğü işveren tarafından açık bir şekilde ortaya konulmadığı gibi derece mahkemeleri tarafından da somut olay bu yönüyle tartışılmamıştır.

44. Öte yandan somut olayda işverenin yaptığı müdahalenin kapsamının tartışılması gerekir. Bu bağlamda işveren tarafından Mahkemeye sunulan başvurucunun yazışmaları ve yargılama süreci bir bütün hâlinde değerlendirildiğinde işverenin yazışma içeriklerine başvurucunun ve mesajlaştığı arkadaşlarının rızası hilafına erişim sağladığı ve bu içeriklerin de iş akdinin feshine dayanak yapıldığı görülmüştür.

45. Nitekim Anayasa Mahkemesi E.Ü. kararına konu başvurucunun kurumsal e-posta hesabı içeriğinin işveren tarafından incelenmesi ve bu yazışmalar gerekçe gösterilerek iş akdinin feshedilmesi şeklindeki benzer somut olayda da aynı sonuca ulaşmış ve ihlal kararı vermiştir. Başvurucunun kurumsal kullanım için değil kendi özel kullanımı amacıyla bilgisayarına kurduğu ve kullanarak arkadaşlarıyla özel mesajlaşmalar gerçekleştirdiği WhatsApp adlı mesajlaşma programındaki içeriklerin işveren tarafından bir şekilde elde edilerek iş akdinin feshine dayanak yapıldığı somut olayda da anılan karardaki ilkelerden ayrılmayı gerektirir bir durum bulunmadığı sonucuna ulaşılmıştır.

46. Açıklanan gerekçelerle özel hukuk iş ilişkilerinden doğan uyuşmazlığı karara bağlayan derece mahkemeleri tarafından yukarıda belirtilen anayasal güvenceleri gözeten özenli bir yargılama yapılarak pozitif yükümlülüklerin yerine getirilmediği anlaşıldığından başvurucunun Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkı ile Anayasa'nın 22. maddesinde güvence altına alınan haberleşme hürriyetinin ihlal edildiğine karar verilmesi gerekir.

3. 6216 Sayılı Kanun'un 50. Maddesi Yönünden

47. 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 50. maddesinin ilgili kısmı şöyledir:

“(1) Esas inceleme sonunda, başvurucunun hakkının ihlal edildiğine ya da edilmediğine karar verilir. İhlal kararı verilmesi hâlinde ihlalin ve sonuçlarının ortadan kaldırılması için yapılması gerekenlere hükmedilir. ...

(2) Tespit edilen ihlal bir mahkeme kararından kaynaklanmışsa, ihlali ve sonuçlarını ortadan kaldırmak için yeniden yargılama yapmak üzere dosya ilgili mahkemeye gönderilir. Yeniden yargılama yapılmasında hukuki yarar bulunmayan hâllerde başvurucu lehine tazminata hükmedilebilir veya genel mahkemelerde dava açılması yolu gösterilebilir. Yeniden yargılama yapmakla yükümlü mahkeme, Anayasa Mahkemesinin ihlal kararında açıkladığı ihlali ve sonuçlarını ortadan kaldıracak şekilde mümkünse dosya üzerinden karar verir.”

48. Başvurucu, ihlalin tespit edilmesini, yeniden yargılama yapılmasını istemiş; yeniden yargılama mümkün olmadığı takdirde kıdem ve ihbar tazminatları ile işsiz kaldığı sürelerin karşılığı olarak 50.000 TL maddi tazminat talebinde bulunmuştur. Başvurucunun manevi tazminat talebinde bulunmadığı anlaşılmaktadır.

49. Anayasa Mahkemesinin Mehmet Doğan ([GK] B. No: 2014/8875, 7/6/2018) kararında ihlal sonucuna varıldığında ihlalin nasıl ortadan kaldırılacağı hususunda genel ilkeler belirlenmiştir. Anayasa Mahkemesi diğer bir kararında ise bu ilkelerle birlikte ihlal kararının yerine getirilmemesinin sonuçlarına da değinmiş ve bu durumun ihlalin devamı anlamına geleceği gibi ilgili hakkın ikinci kez ihlal edilmesiyle sonuçlanacağına işaret etmiştir (Aligül Alkaya ve diğerleri (2), B. No: 2016/12506, 7/11/2019).

50. Bireysel başvuru kapsamında bir temel hakkın ihlal edildiğine karar verildiği takdirde ihlalin ve sonuçlarının ortadan kaldırıldığından söz edilebilmesi için temel kural mümkün olduğunca eski hâle getirmenin yani ihlalden önceki duruma dönülmesinin sağlanmasıdır. Bunun için ise öncelikle ihlalin kaynağı belirlenerek devam eden ihlalin durdurulması, ihlale neden olan karar veya işlemin ve bunların yol açtığı sonuçların ortadan kaldırılması, varsa ihlalin sebep olduğu maddi ve manevi zararların giderilmesi, ayrıca bu bağlamda uygun görülen diğer tedbirlerin alınması gerekmektedir (Mehmet Doğan, §§ 55, 57).

51. İhlalin mahkeme kararından kaynaklandığı veya mahkemenin ihlali gideremediği durumlarda Anayasa Mahkemesi 6216 sayılı Kanun'un 50. maddesinin (2) numaralı fıkrası ile Anayasa Mahkemesi İçtüzüğü'nün 79. maddesinin (1) numaralı fıkrasının (a) bendi uyarınca ihlalin ve sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmak üzere kararın bir örneğinin ilgili mahkemeye gönderilmesine hükmeder. Anılan yasal düzenleme, usul hukukundaki benzer hukuki kurumlardan farklı olarak ihlali ortadan kaldırmak amacıyla yeniden yargılama sonucunu doğuran ve bireysel başvuruya özgülünen bir giderim yolunu öngörmektedir. Bu nedenle Anayasa Mahkemesi tarafından ihlal kararına bağlı olarak yeniden yargılama kararı verildiğinde usul hukukundaki yargılamanın yenilenmesi kurumundan farklı olarak ilgili mahkemenin yeniden yargılama sebebinin varlığını kabul hususunda herhangi bir takdir yetkisi bulunmamaktadır. Dolayısıyla böyle bir kararın kendisine ulaştığı mahkemenin yasal yükümlülüğü, ilgilinin talebini beklemeksizin Anayasa Mahkemesinin ihlal kararı nedeniyle yeniden yargılama kararı vererek devam eden ihlalin sonuçlarını gidermek üzere gereken işlemleri yerine getirmektir (Mehmet Doğan, §§ 58, 59; Aligül Alkaya ve diğerleri (2), §§ 57-59, 66, 67).

52. İncelenen başvuruda özel hayata saygı hakkı ve haberleşme hürriyetiyle ilgili anayasal güvenceleri gözetilen bir yargılama yapılmaması nedeniyle anılan hak ve özgürlüğün ihlal edildiği sonucuna varılmıştır. Dolayısıyla ihlalin mahkeme kararından kaynaklandığı anlaşılmaktadır.

53. Bu durumda özel hayata saygı hakkı ile haberleşme hürriyetinin ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmasında hukuki yarar bulunmaktadır. Yapılacak yeniden yargılama ise bireysel başvuruya özgü düzenleme içeren 6216 sayılı Kanun'un 50. maddesinin (2) numaralı fıkrasına göre ihlalin ve sonuçlarının ortadan kaldırılmasına yöneliktir. Bu kapsamda yapılması gereken iş, yeniden yargılama kararı verilerek Anayasa Mahkemesini ihlal sonucuna ulaştırılan nedenleri gideren, ihlal kararında belirtilen ilkelere uygun yeni bir karar verilmesinden ibarettir. Bu sebeple kararın bir örneğinin yeniden yargılama yapılmak üzere ilgili mahkemeye gönderilmesine karar verilmesi gerekmektedir.

54. Anayasa Mahkemesinin maddi tazminata hükmedebilmesi için başvurucunun uğradığını iddia ettiği maddi zarar ile tespit edilen ihlal arasında illiyet bağı bulunmalıdır. Başvurucunun bu konuda herhangi bir belge sunmamış olması nedeniyle maddi tazminat talebinin reddine karar verilmesi gerekir.

55. Dosyadaki belgelerden tespit edilen 294,70 TL harç ve 4.500 TL vekâlet ücretinden oluşan toplam 4.794,70 TL yargılama giderinin başvurucuya ödenmesine karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Özel hayata saygı hakkı ile haberleşme hürriyetinin ihlal edildiğine ilişkin iddianın KABUL EDİLEBİLİR OLDUĞUNA,

B. Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkı ve Anayasa'nın 22. maddesinde güvence altına alınan haberleşme hürriyetinin İHLAL EDİLDİĞİNE,

C. Kararın bir örneğinin özel hayata saygı hakkı ile haberleşme hürriyetinin ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmak üzere Ordu İş Mahkemesine (E.2017/696, K.2018/346) GÖNDERİLMESİNE,

D. Başvurucunun maddi tazminat talebinin reddine,

E. 294,70 TL harç ve 4.500 TL vekâlet ücretinden oluşan toplam 4.794,70 TL yargılama giderinin başvurucuya ÖDENMESİNE,

F. Ödemenin, kararın tebliğini takiben başvurusunun Hazine ve Maliye Bakanlığına başvuru tarihinden itibaren dört ay içinde yapılmasına, ödemede gecikme olması hâlinde bu sürenin sona erdiği tarihten ödeme tarihine kadar geçen süre için yasal FAİZ UYGULANMASINA,

G. Kararın bir örneğinin bilgi için Samsun Bölge Adliye Mahkemesi 8. Hukuk Dairesine (E.2018/2034, K.2018/1350) GÖNDERİLMESİNE,

H. Kararın bir örneğinin Adalet Bakanlığına GÖNDERİLMESİNE 28/12/2021 tarihinde OYBİRLİĞİYLE karar verildi.

Anayasa Mahkemesi - Sebiha Kaya Kararı (2018/34124)

Sebiha Kaya [GK], B. No: 2018/34124, 20/5/2021

Başvuru, güvenlik soruşturması ve arşiv araştırmasının olumsuz sonuçlandığı gerekçesiyle memuriyete başlatılmama işlemine karşı açılan iptal davasında hukuka aykırı karar verilmesi nedeniyle adil yargılanma hakkının ihlal edildiği iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

GENEL KURUL

KARAR

SEBİHA KAYA BAŞVURUSU

(Başvuru Numarası: 2018/34124)

Karar Tarihi: 20/5/2021

R.G. Tarih ve Sayı: 5/8/2021-31559

GENEL KURUL

KARAR

Başkan: Zühtü ARSLAN

Başkanvekili: Hasan Tahsin GÖKCAN

Başkanvekili: Kadir ÖZKAYA

Üyeler: Engin YILDIRIM, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĞLU, Selahaddin MENTEŞ, Basri BAĞCI, İrfan FİDAN

Raportör: Ayhan KILIÇ

Başvurucu: Sebiha KAYA

Vekili: Av. Vural KAYA

I. BAŞVURUNUN KONUSU

1. Başvuru, güvenlik soruşturması ve arşiv araştırmasının olumsuz sonuçlandığı gerekçesiyle memuriyete başlatılmama işlemine karşı açılan iptal davasında hukuka aykırı karar verilmesi nedeniyle adil yargılanma hakkının ihlal edildiği iddiasına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 14/11/2018 tarihinde yapılmıştır.

3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.

4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.

5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.

6. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık, görüşünü bildirmiştir.

7. Başvurucu, Bakanlığın görüşüne karşı süresinde beyanda bulunmuştur.

8. Birinci Bölüm tarafından, niteliği itibarıyla Genel Kurul tarafından karara bağlanması gerekli görüldüğünden başvurunun Anayasa Mahkemesi İçtüzüğü'nün (İçtüzük) 28. maddesinin (3) numaralı fıkrası uyarınca Genel Kurula sevkine karar verilmiştir.

III. OLAY VE OLGULAR

9. Başvuru formu ve eklerinde ifade edildiği şekliyle ilgili olaylar özetle şöyledir:

10. Başvurucu 1988 doğumlu olup Ağrı'nın Doğubeyazıt ilçesinde ikamet etmektedir.

11. Başvurucu; Ölçme, Seçme ve Yerleştirme Merkezi Başkanlığı tarafından 2016/I döneminde yapılan Kamu Personeli Seçme Sınavı'na (KPSS) girmiştir. Bu sınav sonucu esas alınarak başvurucu, Elektrik Üretim Anonim Şirketi Genel Müdürlüğüne (Genel Müdürlük) bağlı Diyarbakır Karakaya HES İşletme Müdürlüğüne sözleşmeli memur olarak yerleştirilmiştir.

12. Genel Müdürlük 3/10/2016 tarihli ve 676 sayılı Olağanüstü Hâl Kapsamında Bazı Düzenlemeler Yapılması Hakkında Kanun Hükmünde Kararname'nin (676 sayılı KHK) 74. maddesiyle 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu'nun 48. maddesinin birinci fıkrasının (A) bendine eklenen (8) numaralı alt bent uyarınca başvurucu hakkında güvenlik soruşturması ve arşiv araştırması yaptırmıştır. Genel Müdürlük 18/7/2017 tarihli yazıyla güvenlik soruşturması ve arşiv

araştırmasının olumsuz sonuçlanması nedeniyle atamasının yapılmadığı hususunu başvurucuya bildirmiştir.

13. Başvurucu söz konusu idari işleme karşı 21/9/2017 tarihinde iptal davası açmıştır. Dava Ankara 10. İdare Mahkemesinde (Mahkeme) görülmüştür. Dava dilekçesinde, Anayasa'nın 10., 49. ve 70. maddelerinden söz edilmiş; başvurucunun atanmamasına dayanak gösterilen olguların açık bir biçimde ortaya konulmamasının hukuk devleti ilkesinin bir gereği olan belirlilik ilkesine aykırı olduğu vurgulanmıştır. Dilekçede, başvurucunun herhangi bir adli sicil kaydı bulunmadığı gibi bugüne kadar soruşturma dahi geçirmediği belirtilmiş; buna rağmen atanmamış olmasının hakkaniyete aykırı olduğu ileri sürülmüştür. Güvenlik soruşturması yapılması şartının Anayasa'nın 70. maddesinde belirtilen "görevin gerektirdiği niteliklerden" olmadığının savunulduğu dilekçede, başvurucunun yerleştirildiği kadronun güvenlik soruşturması ve arşiv araştırmasına tabi olmadığı ifade edilmiştir. Başvurucu ayrıca güvenlik soruşturmasının içeriğinden haberdar edilmediğinden de yakınmıştır.

14. Genel Müdürlüğün Mahkemeye sunduğu savunma dilekçesinde, başvurucu hakkında güvenlik soruşturması yapılmasının 676 sayılı KHK'nın 74. maddesiyle 657 sayılı Kanun'un 48. maddesinin birinci fıkrasının (A) bendine eklenen (8) numaralı alt bende dayandığı ve hukuka uygun olduğu belirtilmiştir. Savunma dilekçesinde, başvurucu hakkında yapılan güvenlik soruşturması neticesinde başvurucunun Kürt dili ile ilgili eğitim veren Kürt Dili Araştırma ve Geliştirme Derneği (KURDİ-DER/Derneğ) isimli derneği açtığı, söz konusu Dernekte öğretmenlik yaptığı ve kurs için öğrenci aradığının tespit edildiği ifade edilmiştir. Savunmada, KURDİ-DER'in 31/10/2016 tarihli ve 677 sayılı Olağanüstü Hâl Kanun Hükmünde Kararname (677 sayılı KHK) ile kapatıldığının altı çizilmiştir. Savunma dilekçesinde; başvurucunun babasının terör örgütüne üye olma suçundan yargılandığı ve yargılamasının devam ettiği, ayrıca anılan kişinin (başvurucunun babasının) taksirle yaralama olayında mağdur/şüpheli sıfatıyla ifadesinin alındığının tespit edildiği vurgulanmıştır. 12/4/2000 tarihli ve 24018 sayılı Resmî Gazete'de yayımlanan Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği'nin (Yönetmelik) 15. maddesine atıfta bulunan Genel Müdürlük, hakkındaki olumsuz istihbarat gözetilerek başvurucunun atamasının yapılmamasının hukuka uygun olduğunu savunmuştur.

15. Başvurucu, Genel Müdürlüğün savunmasına karşı cevaplarını Mahkemeye sunmuş; güvenlik soruşturması ve arşiv araştırmasında tespit edilen olguların gerçeği yansıtmadığını ileri sürmüştür. Başvurucu anılan Dernek dâhil hiçbir derneğe üyeliğinin bulunmadığını, bu hususun Valilik bünyesindeki Dernekler Müdürlüğünden sorularak teyit ettirilebileceğini belirtmiştir. KURDİ-DER'e

üyeliği olmamakla birlikte söz konusu Derneğin Kürt dilinin araştırılmasını ve öğretilmesini hedefleyen bir dernek olduğunu ve bu Dernekte eğitim vermenin kanunlara aykırılık taşımadığını ifade etmiştir. Babasının yargılanıyor olmasının kendisi aleyhine değerlendirilmesinin suç ve cezaların şahsiliği ilkesini zedelediğine değinmiştir. Danıştay'ın benzer olaylara özgü olarak bireyler lehine çokça kararının bulunduğu vurgulayan başvuru, hiçbir suç işlemediği ve soruşturma dahi geçirmediği hâlde güvenlik soruşturmasının olumsuz sonuçlanması gerekçe gösterilerek atanmaması yolunda tesis edilen işlemin kanuna ve Anayasa'ya aykırı olduğunu ileri sürmüştür.

16. Mahkeme 10/5/2018 tarihli kararla davayı reddetmiştir. Kararın gerekçesinde, 676 sayılı KHK'nın 74. maddesiyle 657 sayılı Kanun'un 48. maddesine eklenen alt bentten söz edilmiş ve buna göre "güvenlik soruşturması ve arşiv araştırması yapılmış olma"nın devlet memurluğuna alınmada genel bir şart hâline getirildiği ifade edilmiştir. Kararda, 26/10/1994 tarihli ve 4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun'a ve anılan Kanun'a dayanılarak çıkarılan Yönetmelik'in ilgili maddelerine yer verildikten sonra 22/7/2016 tarihli ve 667 sayılı Olağanüstü Hal Kapsamında Alınan Tedbirlere İlişkin Kanun Hükmünde Kararname'nin (667 sayılı KHK) amacı ile KHK'da düzenlenen tedbirlerin kapsamı ve mahiyeti dikkate alındığında söz konusu KHK'nın ve anılan KHK ile getirilen kamu görevinden ihraç tedbirinin arkasındaki gerekçelerin kamu hizmetine alınmada da dikkate alınması gerektiğinin altı çizilmiştir. Mahkeme sonuç olarak başvuruçunun güvenlik soruşturmasının olumsuz değerlendirilerek atamasının yapılmaması yolunda tesis edilen idari işlemde hukuka aykırılık bulunmadığı kanaatine varmıştır. Kararın gerekçesinin ilgili kısmı şöyledir:

"Dava dosyasının incelenmesinden, davacının Ölçme Seçme ve Yerleştirme Merkezi Başkanlığınca KPSS 2016/1 puanlarıyla Bazı Kamu Kurum ve Kuruluşlarının Kadro ve Pozisyonlarına yapılan 1. yerleştirme sonuçlarına göre, Diyarbakır ili, Karakaya HES İşletme Müdürlüğüne Sözleşmeli Memur olarak yerleştirildiği, hakkında yapılan inceleme ve araştırma sonucunda, kuruluşunda görev alarak öğretmenlik de yaptığı Kürdi-Der isimli derneğin, [kararın orijinalinde koyu yazılmıştır] 677 sayılı Olağanüstü Hal Kapsamında Bazı Tedbirler Alınması Hakkında Kanun Hükmü'nde Kararname'nin 3. maddesi hükümleri çerçevesinde, Terör örgütlerine veya Milli Güvenlik Kurulunca Devletin milli güvenliğine karşı faaliyette bulunduğu karar verilen yapı, oluşum veya gruplara aidiyet, iltisakı veya bunlarla irtibatı olan: ekli (6) sayılı listede yer alan dernekler arasında bulunduğu; 'Babası [N.K.nın] Ağrı Ağır Ceza Mahkemesince 2017/46 Esas Nolu dosyada 'Silahlı Terör Örgütüne Üye Olmak' suçuyla sanık sıfatıyla yargılamasının devam ettiği, 12.09.2011 tarihinde Ağrı Murat Şehit

Halis Çınar Polis Merkezi Amirliğinde 'Taksirli Yaralama' olayından şüpheli olarak işlem yapıldığı' şeklindeki bilgi notu üzerine, 13.06.2017 tarihli Komisyonu Kararı ile güvenlik soruşturması olumsuz değerlendirilerek atamasının yapılmaması üzerine bakılan davanın açıldığı anlaşılmıştır.

667 sayılı Kanun Hükmünde Kararnamenin amacı ile 4. maddesinde düzenlenen tedbirlerin kapsamı ve mahiyeti birlikte dikkate alındığında, anılan tedbirler vasıtasıyla başta FETÖ/PDY olmak üzere terör örgütlerine veya Milli Güvenlik Kurulu'nca devletin milli güvenliğine karşı faaliyette bulunduğu karar verilen yapı, oluşum veya gruplara üyeliği, mensubiyeti veya iltisakı yahut bunlarla irtibatı olduğu değerlendirilen kişilerin, kamu kurum ve kuruluşlarından çıkarılarak, Anayasa ile kurulan demokrasi düzeninin korunmak istendiği görülmekte olup çalışanlarını bu gerekçelerle çıkaran kamu idarelerinin aynı gerekçeleri ilk atamalarda da dikkate alması gerektiği açıktır.

Yine, 657 sayılı Devlet Memurları Kanunu'nun 48/A-8 maddesinde 'Güvenlik soruşturması ve/veya arşiv araştırması yapılmış olmak', Devlet memurluğuna alınmada aranılacak genel şartlar arasında sayılmış olup yukarıda ayrıntısına yer verilen bilgiler dikkate alındığında davacının güvenlik soruşturmasının olumsuz değerlendirilerek atanmaması yolundaki davalı idare takdirinde hukuka aykırılık bulunmamıştır."

17. Başvurucu, mahkeme kararına karşı istinaf yoluna başvurmuştur. İstinaf dilekçesinde ilk derece mahkemesinde ileri sürdüğü iddialarını tekrarlamıştır. İstinaf talebini inceleyen Ankara Bölge İdare Mahkemesi 1. Dava Dairesi 19/9/2018 tarihinde istemi reddetmiştir. Nihai karar 15/10/2018 tarihinde başvurucuya tebliğ edilmiştir.

18. Başvurucu 14/11/2018 tarihinde bireysel başvuruda bulunmuştur.

IV. İLGİLİ HUKUK

A. Ulusal Hukuk

1. Mevzuat Hükümleri

19. 657 sayılı Kanun'un 6. maddesinin birinci fıkrasının birinci cümlesi şöyledir:

"Devlet memurları, Türkiye Cumhuriyeti Anayasasına ve kanunlarına sadakatla bağlı kalmak ve milletin hizmetinde Türkiye Cumhuriyeti kanunlarını sadakatla uygulamak zorundadırlar"

20. 657 sayılı Kanun'un 48. maddesi şöyledir:

"Devlet memurluğuna alınacaklarda aşağıdaki genel ve özel şartlar aranır.

A) Genel şartlar:

1. Türk Vatandaşı olmak,
 2. Bu Kanununun 40 ncı maddesindeki yaş şartlarını taşımak,
 3. Bu Kanununun 41 nci maddesindeki öğrenim şartlarını taşımak,
 4. Kamu haklarından mahrum bulunmamak,
 5. Türk Ceza Kanununun 53 üncü maddesinde belirtilen süreler geçmiş olsa bile; kasten işlenen bir suçtan dolayı bir yıl veya daha fazla süreyle hapis cezasına ya da affa uğramış olsa bile devletin güvenliğine karşı suçlar, Anayasal düzene ve bu düzenin işleyişine karşı suçlar, (...) zimmet, irtikâp, rüşvet, hırsızlık, dolandırıcılık, sahtecilik, güveni kötüye kullanma, hileli iflas, ihaleye fesat karıştırma, edimin ifasına fesat karıştırma, suçtan kaynaklanan malvarlığı değerlerini aklama veya kaçakçılık suçlarından mahkûm olmamak.
 6. Askerlik durumu itibariyle;
 - a) Askerlikle ilgisi bulunmamak,
 - b) Askerlik çağına gelmemiş bulunmak,
 - c) Askerlik çağına gelmiş ise muvazzaf askerlik hizmetini yapmış yahut ertelenmiş veya yedek sınıfa geçirilmiş olmak,
 7. 53 üncü madde hükümleri saklı kalmak kaydı ile görevini devamlı yapmasına engel olabilecek (...) akıl hastalığı (...) bulunmamak.
 8. [Anayasa Mahkemesinin 24/7/2019 tarihli ve E.:2018/73; K.:2019/65 sayılı Kararı ile iptal edilmiştir]
B) Özel şartlar:
 1. Hizmet göreceği sınıf için 36 ve 41 nci maddelerde belirtilen öğretim ve eğitim kurumlarının birinden diploma almış olmak,
 2. Kurumların özel kanun veya diğer mevzuatında aranan şartları taşımak."
- 21.** 676 sayılı KHK'nın 74. maddesiyle 657 sayılı Kanun'un 48. maddesinin birinci fıkrasının (A) bendine eklenen ve Anayasa Mahkemesinin 24/7/2019 tarihli ve E.2018/73, K.2019/65 sayılı kararıyla iptal edilen (8) numaralı alt bent şöyledir:
- "Güvenlik soruşturması ve/veya arşiv araştırması yapılmış olmak."
- 22.** 677 sayılı KHK'nın 3. maddesinin (1) numaralı fıkrasının ilgili kısmı şöyledir:

"(1) Terör örgütlerine veya Milli Güvenlik Kurulunca Devletin milli güvenliğine karşı faaliyette bulunduğu karar verilen yapı, oluşum veya gruplara aidiyeti, iltisakı veya bunlarla irtibatı olan;

a) Ekli (6) sayılı listede yer alan dernekler,

...

Kapatılmıştır." [Ekli (6) sayılı listenin 115. sırasında 'Kürt Dili Araştırma ve Geliştirme Derneği' de yer almaktadır].

2. Anayasa Mahkemesi Kararı

23. Anayasa Mahkemesinin 24/7/2019 tarihli ve E.2018/73, K.2019/65 sayılı kararıyla ilgili kısmı şöyledir:

"163. Anayasa'nın 20. maddesinin birinci fıkrasında, herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş; üçüncü fıkrasında da 'Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir' denilerek kişisel verilerin korunması özel hayatın gizliliğinin korunması kapsamında güvenceye kavuşturulmuştur. Anayasa'nın 13. maddesinde de temel hak ve hürriyetlerin yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği ifade edilmiştir.

164. Anayasa'nın 128. maddesinin ikinci fıkrasında 'Memurların ve diğer kamu görevlilerinin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülükleri, aylık ve ödenekleri ve diğer özlük işleri kanunla düzenlenir. Ancak, malî ve sosyal haklara ilişkin toplu sözleşme hükümleri saklıdır' hükmüne yer verilerek memurlar ve diğer kamu görevlilerinin nitelikleri ve atanmalarına ilişkin hususların kanunla düzenleneceği belirtilmiştir.

165. Kanuni düzenleme ilkesi, düzenlenen alanda temel ilkelerin kanunla konulmasını ve çerçevenin kanunla çizilmesini ifade etmektedir. Bu ilke uyarınca kamu görevlilerinin nitelikleri ve atanmalarına ilişkin kuralların kanunda gösterilmesi, kuralın açık, anlaşılır ve sınırlarının belli olması gerekmektedir.

166. Kişisel verilerin korunmasını isteme hakkı, insan onurunun korunması ve bireyin kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır.

167. Anayasa'nın 20. maddesi uyarınca kişisel veriler ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir. Dolayısıyla kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvencenin yaşama geçirilebilmesi için bu hakkı ilgilendiren yasal düzenlemelerin açık, anlaşılabilir ve söz konusu hakkın kullanılabilmesine elverişli olması gerekir. Ancak böyle bir düzenleme ile kişilerin özel hayatlarını ilgilendiren veri, bilgi ve belgelerin resmî makamların keyfî müdahalelerine karşı korunması mümkün hâle gelebilir.

168. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3. maddesine göre kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Anayasa Mahkemesinin yerleşik kararlarında da belirtildiği üzere '...adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler...' kişisel veri olarak kabul edilmektedir (AYM, E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2014/74, K.2014/201, 25/12/2014; E.2014/180, K.2015/30, 19/3/2015; E.2015/32, K.2015/102, 12/11/2015).

169. Bu bağlamda güvenlik soruşturması ve arşiv araştırmasıyla elde edilen veriler kişisel veri niteliğindedir. Kuralla güvenlik soruşturması ve arşiv araştırması kapsamında kamu mercileri tarafından özel yaşamı ile ilgili sorular sorulması da dâhil olmak üzere bir bireyin özel hayatı, iş ve sosyal yaşamıyla ilgili bilgilerinin alınması, kaydedilmesi ve kullanılması özel hayata saygı hakkına sınırlama niteliğindedir.

170. Anayasa'nın 129. maddesinin birinci fıkrasında memurlar ve kamu görevlilerinin Anayasa ve kanunlara sadık kalarak faaliyette bulunma yükümlülükleri düzenlenmiştir. Belirtilen hususlar gözetilerek kamu görevlerine atanacak kişiler bakımından birtakım şartlar getirilmesi doğaldır. Bu şekilde aranan nitelikler kamu hizmetinin etkin ve sağlıklı bir biçimde yürütülmesi amacına yöneliktir. Dolayısıyla kamu görevine atanmadan önce kişilerin güvenlik soruşturması ve arşiv araştırmasının yapılmasını öngören kural kanun koyucunun takdir yetkisindedir. Ancak bu alanda düzenleme getiren kuralların kamu makamlarına hangi koşullarda ve hangi sınırlar içinde tedbirler

uygulama ve özel hayatın gizliliğine yönelik müdahalelerde bulunma yetkisi verildiğini yeterince açık olarak göstermesi ve olası kötüye kullanmalara karşı yeterli güvenceleri sağlaması gerekir.

171. Kuralda güvenlik soruşturması ve/veya arşiv araştırması yapılması memurluğa alımlarda genel şartlar arasında sayılmasına karşın güvenlik soruşturmasına ve arşiv araştırmasına konu edilecek bilgi ve belgelerin neler olduğuna, bu bilgilerin ne şekilde kullanılacağına, hangi mercilerin soruşturma ve araştırmayı yapacağına ilişkin herhangi bir düzenleme yapılmamıştır. Diğer bir ifadeyle güvenlik soruşturması ve arşiv araştırmasının yapılmasına ve elde edilecek verilen kullanılmasına ilişkin temel ilkeler belirlenmeksizin kuralla sadece güvenlik soruşturması ve arşiv araştırması yapılması devlet memurluğuna alımlarda aranacak şartlar arasında sayılmıştır.

172. Güvenlik soruşturması ve arşiv araştırması sonucunda devlet memurluğuna atanmada esas alınacak kişisel veri niteliğindeki bilgilerin alınmasına, kullanılmasına ve işlenmesine yönelik güvenceler ve temel ilkeler kanunla belirlenmeksizin bunların alınmasına ve kullanılmasına izin verilmesi Anayasa'nın 13., 20. ve 128. maddeleriyle bağdaşmamaktadır."

B. Uluslararası Hukuk

24. Avrupa İnsan Hakları Sözleşmesi'nin (Sözleşme) 6. maddesinin (1) numaralı fıkrasının ilgili kısmı şöyledir:

"Herkes davasının medeni hak ve yükümlülükleri ile ilgili uyuşmazlıklar[ın] ... esas konusunda karar verecek olan ... bir mahkeme tarafından ... görülmesini isteme hakkına sahiptir..."

25. Avrupa İnsan Hakları Mahkemesi (AİHM) adil yargılanma hakkının demokratik toplumda önemli bir yere sahip olduğunu vurgulamaktadır (Airey/İrlanda, B. No: 6289/73, 9/10/1979, § 24). AİHM'e göre hukuk devletinin temel ilkelerinden biri olan hukuki belirlilik Sözleşme'nin bütün maddelerinde mündemiçtir (Iordan Iordanov/Bulgaristan, B. No: 23530/02, 2/7/2009, § 47). Adil yargılanma hakkı hukukun kabul edilmiş evrensel ilkelerine uygun olarak yorumlanmalıdır. Bu bağlamda hakkın tesliminden kaçınma (denial of justice) yasağı bu ilkelerin başında gelmektedir (Golder/Birleşik Krallık, B. No: 4451/70, 21/2/1975, § 35).

26. AİHM iç hukukun yorumlanmasında öncelikli görevin ulusal otoritelere ait olduğunu vurgulamaktadır. AİHM'in görevi ulusal hukuk mercilerinin yorumlarının etkilerinin Sözleşme ile uyumlu olup olmadığını tespit etmekle sınırlıdır (Waite ve Kennedy/Almanya, B. No: 26083/94, 18/2/1999, § 54). AİHM kural olarak kendisinin ulusal mahkemelerin yerine geçerek değerlendirme yapma görevinin bulunmadığını, ulusal hukukun yorumlanmasına ilişkin sorunları çözümlenmenin öncelikli olarak ulusal otoritelerin -özellikle ulusal mahkemelerin- yetkisinde olduğunu ifade

etmektedir. AİHM bu sebeple ulusal mahkemelerin iç hukukun yorumuna ilişkin tartışmalarına karışmayacağını belirtmektedir. Ancak AİHM keyfiliğin bulunduğu, diğer bir ifadeyle ulusal mahkemelerin iç hukuku açıkça hatalı veya keyfî ya da adaleti hiçe sayacak şekilde uyguladıklarını gözlemlediği hâllerde bunu sorgulayabileceğine işaret etmektedir (Anđelković/Sırbistan, B. No: 1401/08, 9/4/2013, § 24).

V. İNCELEME VE GEREKÇE

27. Mahkemenin 20/5/2021 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları ve Bakanlık Görüşü

28. Başvurucu; atanmama gerekçesine dayanak olarak gösterilen KURDİ-DER'in açılışını yapma ve orada öğretmenlik yapma olgusunun gerçeği yansıtmadığının Valilik bünyesindeki Dernekler Müdürlüğünden teyit ettirilebileceğini ileri sürdüğü hâlde derece mahkemelerinin bu yönde bir araştırma yapmadığını belirtmiştir. Herhangi bir dernek üyeliğinin bulunmadığını ileri süren başvurucu; anılan Dernekle de bir organik bağının bulunmadığını, kolluk birimlerinin istihbari mahiyet taşıyan tespitlerinden öte bir bilginin mevcut olmadığını ifade etmiştir. Başvurucu ayrıca babasının fiillerinden kendisinin sorumlu tutulmasının suç ve cezaların kanuniliği ilkesi ile adil yargılanma hakkını ihlal ettiğini savunmuştur. Sonuç olarak istihbarata dayanılarak atamasının yapılmamasının çalışma hakkını ve kamu hizmetlerine girme hakkını zedelediğini iddia etmiştir.

29. Bakanlık görüş yazısında, başvurunun Anayasa'nın 36. maddesinde güvence altına alınan adil yargılanma hakkı kapsamında incelenmesi gerektiği ifade edilmiştir. Bakanlık 15 Temmuz 2016 tarihinde gerçekleşen darbe teşebbüsünden ve darbe teşebbüsünden sonraki gelişmelerden söz etmiştir. Darbe teşebbüsünü doğuran koşulların bertaraf edilmesi amacıyla olağanüstü hâl ilan edildiğine değinen Bakanlık 676 sayılı KHK'nın 74. maddesiyle 657 sayılı Kanun'un 48. maddesine eklenen hükümlerle güvenlik soruşturması ve/veya arşiv araştırması yapılmasının memurluğa alınmada genel bir şart hâline getirildiğini vurgulamıştır. Bakanlık söz konusu kuralın Anayasa Mahkemesinin 24/7/2019 tarihli ve E.2018/73, K.2019/65 sayılı kararı ile iptal edildiğini hatırlatmış, başvurucu hakkında yapılan güvenlik soruşturması ve arşiv araştırması ile konuya ilişkin diğer belgelerin ve görüşlerin ilgili kurumlardan istenmesinin Anayasa Mahkemesinin takdirinde olduğunu belirtmiştir.

30. Başvurucu, Bakanlık görüşüne karşı beyanında başvuru formundaki iddialarını tekrarlamış; ayrıca güvenlik soruşturması ve/veya arşiv araştırmasını devlet memurluğu için genel bir şart hâline getiren kuralın Anayasa Mahkemesince iptal edildiğini de anımsatmıştır.

B. Değerlendirme

31. Anayasa'nın "Hak arama hürriyeti" kenar başlıklı 36. maddesinin birinci fıkrası şöyledir:

"Herkes, meşru vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir."

32. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Bununla birlikte bireysel başvuru kapsamındaki hak ve özgürlüklerden hangisinin hangi nedenle ihlal edildiğine ve buna ilişkin gerekçelere dair açıklamalarda bulunarak hukuki iddialarını ortaya koymak başvurucuya düşer (benzer yöndeki karar için bkz. Veli Özdemir, B. No: 2013/276, 9/1/2014, §§ 19, 20; Ünal Yiğit, B. No: 2013/1075, 30/6/2014, §§ 18, 19; Sabah Yıldızı Radyo ve Televizyon Yayın İletişim Reklam Sanayi ve Ticaret Anonim Şirketi [GK], B. No: 2014/12727, 25/5/2017, § 19). Bir başka ifadeyle bireysel başvuru incelemesinde Anayasa Mahkemesi, kamu gücü eylem ve işlemleri ile mahkeme kararlarının Anayasa'ya uygunluğunun ve müdahale gerekçelerinin denetimini kendiliğinden yapmaz. Anayasa Mahkemesinin başvuru yerine geçerek ihlal iddialarını gerekçelendirme, olay ve olguları ortaya koyma, delil toplama görev ve yükümlülüğü bulunduğundan söz edilemez. Söz konusu yükümlülükler başvurucuya aittir (Cemal Günsel [GK], B. No: 2016/12900, 21/1/2021, §§ 24, 25). Başvurucu, yukarıda da belirtildiği gibi (bkz. § 28), başvuru formunda istihbarat raporuna dayalı olarak atamasının yapılmaması ve buna karşı açtığı davanın reddedilmesi nedeniyle adil yargılanma hakkının, çalışma hakkının ve kamu hizmetlerine girme hakkının ihlal edildiğini ileri sürmüştür. Başvurucu, özel hayata saygı hakkının veya bu hak kapsamında kişisel verilerin korunmasını isteme hakkının ihlal edildiğine ilişkin herhangi bir iddia ve açıklamada bulunmamıştır. Dolayısıyla başvuruda somut meselenin kamu görevinden çıkarılmaya ilişkin olmadığı da gözetilerek özel hayata saygı hakkı kapsamında ayrı bir inceleme yapılmamıştır. Diğer taraftan Anayasa Mahkemesinin yerleşik içtihadı (Serkan Acar, B. No: 2013/1613, 2/10/2013) uyarınca çalışma hakkı ve kamu görevine girme hakkı Anayasa ve Sözleşme ile Türkiye'nin taraf olduğu ek protokollerin ortak koruma alanına girmediğinden bu iddialar yönünden de değerlendirme yapılmasına gerek görülmemiştir. Tüm bu açıklamalar ışığında başvurunun yalnızca Anayasa'nın 36. maddesinde güvence altına alınan adil yargılanma hakkı kapsamında incelenmesi gerektiği sonucuna ulaşılmıştır.

1. Uygulanabilirlik Yönünden

33. Anayasa'nın 36. maddesinde güvence altına alınan adil yargılanma hakkı, suç isnadına bağlı yargılamaların yanında bir kimsenin medeni hak ve yükümlülüklerinin karara bağlanmasıyla ilgili

yargılamalarda da uygulanır. Anayasa'nın 36. maddesinin (1) numaralı fıkrasının medeni meselelerde uygulanabilmesi için ortada hukuk düzeni tarafından kişiye tanınmış veya en azından savunulabilir temeli bulunan bir hakkın bulunması gerekir. Ayrıca bu hakka ilişkin olarak ilgili kişinin menfaatini etkileyen bir uyuşmazlık mevcut olmalıdır. Öte yandan bu uyuşmazlık ihtilaf konusu hakkın tespiti ve bu haktan yararlanılması bakımından belirleyici bir nitelik arz etmelidir (Mehmet Güçlü ve Ramazan Erdem, B. No: 2015/7942, 28/5/2019, § 28).

34. Anayasa'nın 70. maddesi ile 657 sayılı Kanun'un 48. maddesi uyarınca her Türk vatandaşının kamu hizmetine girme hakkına sahip olduğu tartışmasızdır. Öte yandan Türk hukukunda devlet memurluğuna alınmamaya ilişkin işlemlerin dava konusu edilebilirliğine ilişkin bir tereddüt bulunmamaktadır. Somut olayda başvuru, kanunda öngörülen koşulları taşımadığı gerekçesiyle atamasının yapılmamasına ilişkin işleme karşı dava açmıştır. Başvurucunun devlet memurluğuna girme koşullarını taşıyıp taşımadığı hususu uyuşmazlığın esasını oluşturmaktadır. Bu yönüyle davanın başvuru konusunun memuriyete atanmaması yolundaki işlemin iptalini sağlama kapasitesi vardır. Bu durumda bireysel başvuru konusu davanın başvuru konusunun medeni hak ve yükümlülükleri yönünden belirleyici bir nitelik taşıdığı ve adil yargılanma hakkının tüm güvencelerinin bu davada uygulanması gerektiği sonucuna varılmıştır.

2. Kabul Edilebilirlik Yönünden

a. Genel İlkeler

35. Anayasa'nın 36. maddesinde güvence altına alınan adil yargılanma hakkı maddi adaleti değil şekli adaleti temin etmeye yönelik güvenceler içermektedir. Bu bakımdan adil yargılanma hakkı davanın taraflardan biri lehine sonuçlanmasını garanti etmemektedir. Adil yargılanma hakkı temel olarak yargılama sürecinin ve usulünün hakkaniyete uygun olarak yürütülmesini teminat altına almaktadır (M.B. [GK], B. No: 2018/37392, 23/7/2020, § 80).

36. Anayasa'nın 148. maddesinin dördüncü fıkrasında, kanun yolunda gözetilmesi gereken hususlara ilişkin şikâyetlerin bireysel başvuruda incelenemeyeceği belirtilmiştir. Bu kapsamda ilke olarak mahkemeler önünde dava konusu yapılmış maddi olay ve olguların kanıtlanması, delillerin değerlendirilmesi, hukuk kurallarının yorumlanması ve uygulanması ile uyuşmazlık konusunda varılan sonucun adil olup olmaması bireysel başvuru konusu olamaz. Ancak bireysel başvuru kapsamındaki hak ve özgürlüklere müdahale teşkil eden, bariz takdir hatası veya açık bir keyfîlik içeren tespit ve sonuçlar bu kapsamda değildir (konuya ilişkin birçok karar arasından bkz. Ahmet Sağlam, B. No: 2013/3351, 18/9/2013).

37. Ancak temel hak ve özgürlüklere müdahalenin söz konusu olduğu durumlarda derece mahkemelerinin takdir ve değerlendirmelerinin Anayasa'daki güvencelere etkisini nihai olarak değerlendirecek merci Anayasa Mahkemesidir. Bu itibarla Anayasa'da öngörülen güvenceler dikkate alınarak bireysel başvuru kapsamındaki temel hak ve özgürlüklerin ihlal edilip edilmediğine ilişkin herhangi bir inceleme kanun yolunda gözetilmesi gereken hususun incelenmesi olarak nitelendirilemez (Şahin Alpay (2) [GK], B. No: 2018/3007, 15/3/2018, § 53).

38. Diğer taraftan Anayasa Mahkemesi çok istisnai durumlarda temel hak ve özgürlüklerden biri ile doğrudan ilgili olmayan bir şikâyeti kanun yolunda gözetilmesi gereken hususlara ilişkin yasak kapsamına girmeden inceleyebilir. Açık bir keyfîlik nedeniyle yargılamanın hakkaniyetinin temelden sarsıldığı ve adil yargılama hakkı kapsamındaki usule ilişkin güvencelerin anlamsız hâle geldiği çok istisnai hâllerde, aslında yargılamanın sonucuna ilişkin olan bu durumun bizatihi kendisi usule ilişkin bir güvenceye dönüşmüş olur. Dolayısıyla Anayasa Mahkemesinin derece mahkemelerinin değerlendirmelerinin usule ilişkin güvenceleri anlamsız hâle getirip getirmediğini ve açık bir keyfîlik nedeniyle yargılamanın hakkaniyetinin temelden sarsılıp sarsılmadığını incelemesi yargılamanın sonucunu değerlendirdiği anlamına gelmez. Sonuç olarak Anayasa Mahkemesi derece mahkemelerinin delillerle ilgili değerlendirmelerine ancak açık bir keyfîlik ve adil yargılanma hakkı kapsamındaki usule ilişkin güvenceleri anlamsız hâle getiren bir uygulama varsa müdahale edebilecektir (Ferhat Kara [GK], B. No: 2018/15231, 4/6/2020, § 149; M.B., § 83).

39. Adil yargılanma hakkı, hukuk kuralının davanın başvuru lehine sonuçlanmasını temin eden yorumunun esas alınmasını güvence altına almamaktadır. Uyuşmazlığa uygulanacak hukuk kurallarının yorumlanması -yukarıda belirtildiği gibi- derece mahkemelerinin takdirindedir. Bununla birlikte derece mahkemelerinin hukuk kurallarını yorumlarken Anayasa'nın 2. maddesinde düzenlenen ve Cumhuriyet'in nitelikleri arasında sayılan hukuk devleti ilkesini gözönünde bulundurmaları gerekir. Esasen hukuk devleti ilkesi Anayasa'nın tüm maddelerinin yorumlanmasında dikkate alınması zorunlu olan bir ilkedir. Bu bağlamda Anayasa'nın 36. maddesinde güvence altına alınan adil yargılanma hakkının kapsam ve içeriğinin yorumlanmasında da hukuk devletinin gerekleri gözetilmelidir (M.B., § 84).

40. Bu noktada hukuk devletinin gereklerinden birini de hukuk güvenliği ilkesi oluşturmaktadır (AYM, E.2008/50, K.2010/84, 24/6/2010 ve E.2012/65, K.2012/128, 20/9/2012). Kişilerin hukuki güvenliğini sağlamayı amaçlayan hukuki güvenlik ilkesi; hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar. Belirlilik

ilkesi ise yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olmasını, ayrıca kamu otoritelerinin keyfî uygulamalarına karşı koruyucu önlem içermesini ifade etmektedir (AYM, E.2013/39, K.2013/65, 22/5/2013).

41. Başvurucuların medeni haklarıyla ilgili uyuşmazlıklarda uygulanan hukuk kurallarının açıkça keyfî veya hakkın tesliminden kaçınacak (adaleti hiçe sayacak) biçimde yorumlanması usule ilişkin güvenceleri anlamsız hâle getireceğinden adil yargılanma hakkının ihlal edildiğinden söz edilebilir. Zira bu hâlde, derece mahkemesinin yorumunun başvuru tarafından öngörülmesi mümkün olmayıp hukuk kurallarının öngörülemez biçimde yorumlanması hukuk devleti ilkesini örseler. Özellikle hak ve özgürlükleri kısıtlayıcı hükümlerin geniş yoruma tabi tutulması keyfîliğe ve bireylerin kendilerini hukuk karşısında güvensiz hissetmelerine yol açar (M.B., § 86).

42. Hakkaniyete uygun yargılanma hakkının unsurlarından biri de silahların eşitliği ve çelişmeli yargılama ilkeleridir. Silahların eşitliği ilkesi, davanın taraflarının usule ilişkin haklar bakımından aynı koşullara tabi tutulması ve taraflardan birinin diğerine göre daha zayıf bir duruma düşürülmeksizin iddia ve savunmalarını makul bir şekilde mahkeme önünde dile getirme fırsatına sahip olması anlamına gelir. Ceza davalarının yanı sıra medeni hak ve yükümlülüklerle ilgili uyuşmazlıklara ilişkin hukuk davaları ve idari davalarda da bu ilkeye uyulması gerekir (Yaşasın Aslan, B. No: 2013/1134, 16/5/2013, § 32). Silahların eşitliği ilkesinin tamamlayıcısı olan çelişmeli yargılama ilkesi, kural olarak bir hukuk ya da ceza davasında tüm taraflara, gösterilen kanıtlar ve sunulan görüşler hakkında bilgi sahibi olma ve bunlarla ilgili görüş bildirebilme imkânı vermektedir. Bu çerçevede başvuranların bilirkişi raporunun sonucuna itiraz edememesi ya da delillerle ilgili görüş bildirmelerine fırsat verilmemesi çelişmeli yargılama ilkesinin ihlali olarak değerlendirilebilmektedir (Hüseyin Sezen, B. No: 2013/1793, 18/9/2014, § 38).

b. İlkelerin Olaya Uygulanması

43. Somut olaydaki dava, başvuruçunun sözleşmeli memur olarak atanmamasına ilişkin işleme karşı açılmıştır. Davada çözüme kavuşturulması gereken temel mesele başvuruçunun memuriyete atanma koşullarını taşıyıp taşımadığıdır. Devlet memurluğuna atanmanın genel ve özel koşulları 657 sayılı Kanun'un 48. maddesinde düzenlenmiştir. Başvuruçunun 676 sayılı KHK'nın 74. maddesiyle 657 sayılı Kanun'un 48. maddesinin birinci fıkrasının (A) bendine eklenen (8) numaralı alt bent dışındaki şartları taşıdığına yönelik bir ihtilaf bulunmamaktadır. Tartışma konusu olan husus başvuruçunun bu bentteki şartı taşıyıp taşımadığıdır. Mahkeme başvuruçunun belirtilen alt bent ile getirilen şartı sağlayamadığını kabul etmiştir.

44. 657 sayılı Kanun'un 48. maddesine eklenen "Güvenlik soruşturması ve/veya arşiv araştırması yapılmış olmak" biçimindeki alt bendin başvuruçunun yerleştirildiği kadro da dâhil olmak üzere tüm devlet memurluğu kadrolarına atanabilmek için güvenlik soruşturması ve/veya arşiv araştırması yapılması şartı getirdiği açıktır. Bu sebeple sözleşmeli memur kadrosuna yerleştirilen başvuruçunun güvenlik soruşturması ve arşiv araştırmasına tabi tutulacağına öngörülebilir olduğundan kuşku duymayı gerektirecek bir neden bulunmamaktadır.

45. Anılan kuralın Anayasa Mahkemesinin 24/7/2019 tarihli ve E.2018/73, K.2019/65 sayılı kararıyla iptal edilmiş olması da bu neticeyi değiştirmemektedir. Anayasa Mahkemesinin iptal kararında özel hayata saygı hakkıyla sınırlı bir inceleme yapıldığı dikkatten kaçırılmamalıdır. Anayasa Mahkemesinin söz konusu kararında güvenlik soruşturması ve arşiv araştırması sonucu bireylerin kişisel verilerinin toplanmasının, işlenmesinin ve kullanılmasının kişisel verilerin korunmasını isteme hakkına müdahale teşkil ettiği kabul edilerek bu müdahaleye dayanak oluşturan kanunun hukuk devleti ilkesinin gerektirdiği kriterleri karşılayıp karşılamadığı irdelenmiştir. Anayasa Mahkemesi, güvenlik soruşturması ve arşiv araştırması neticesinde devlet memurluğuna atanmada esas alınacak kişisel veri niteliğindeki bilgilerin alınmasına, kullanılmasına ve işlenmesine yönelik güvenceler ve temel ilkeler kanunla belirlenmeksizin bunların alınmasına ve kullanılmasına izin verilmesinin Anayasa'nın 13., 20. ve 128. maddeleriyle bağdaşmadığı sonucuna ulaşmıştır.

46. 657 sayılı Kanun'un 48. maddesinin birinci fıkrasının (A) bendinin devlet memurluğuna girişte güvenlik soruşturması ve arşiv araştırması yapılması şartını getiren (8) numaralı alt bendinin kişisel verilerin korunması hakkı yönünden yeterli güvenceleri içermediği gerekçesiyle iptal edilmiş olmasının, yürürlükte bulunduğu dönemdeki uygulamalarına ilişkin olarak açılan davalarda bu kuralın dikkate alınmasının otomatik olarak adil yargılanma hakkını zedelediği söylenemez. Kuralın kişisel verilerin korunmasını isteme hakkının ihlalini teşkil etmesi adil yargılanma hakkını da ihlal ettiği biçiminde anlaşılabilir. Zira adil yargılanma hakkı uyumsuzlukta uygulanacak kuralın içeriği itibarıyla adil olmasını değil uygulanma şekli itibarıyla adil olmasını garanti etmektedir. Bu açıdan iptal edilen kuralın somut olaydaki uygulanma şeklinin adil yargılanma hakkını zedeleyip zedelediği irdelenmelidir.

47. Anayasa Mahkemesince iptal edilen kuralla, güvenlik soruşturması ve/veya arşiv araştırması yapılmasının memuriyete girişte genel bir şart hâline gelmiş olduğu açık ise de güvenlik soruşturmasının sonuçlarının ne anlama geleceği ve bunların atamaya yetkili makamın kararına tesirinin ne olacağı hususunda kanunda bir sarahat bulunmamaktadır. Bireysel başvuruya konu kararın gerekçesinden Mahkemenin 657 sayılı Kanun'un 48. maddesine eklenen alt bentteki şartı

güvenlik soruşturması ve/veya arşiv araştırmasının olumlu sonuçlanması biçiminde yorumladığı anlaşılmaktadır.

48. Uyuşmazlıkta uygulanacak hukuk kurallarının yorumlanmasında öncelikli yetkinin derece mahkemelerine ait olduğunun altı bir kez daha çizilmelidir. Anayasa Mahkemesinin kendi yorumunu derece mahkemelerinininkinin yerine kaim etmesi söz konusu olamaz. Bununla birlikte derece mahkemelerinin yorumlarının etkilerinin adil yargılanma hakkıyla çelişip çelişmediğini incelemek Anayasa Mahkemesinin görevindedir. Bu bakımdan bireysel başvuru kapsamında yapılacak değerlendirmede derece mahkemelerinin söz konusu fıkranın güvenlik soruşturmasının olumlu sonuçlanmasını gerektirdiği biçimindeki yorumu veri kabul edilecektir.

49. Güvenlik soruşturması ve arşiv araştırmasının olumlu sonuçlanması şartının aranmasının kuralı belli ölçüde muğlaklaştırdığı söylenebilir. Zira güvenlik soruşturmasının olumlu neticelenip neticelenmediği konusunda ulaşılabilecek sonucun atamaya yetkili konumda bulunan kişi veya kişilere bağlı olarak değişmesi riski bulunmaktadır. Bu da keyfî ve ayrımcı uygulamaların gelişmesine, dolayısıyla bireylerin devlete olan güvenlerinin zedelenmesine sebep olabilecektir. Bununla birlikte kuralların iyi uygulanmayabileceği hususunda oluşan şüphe tek başına kuralın öngörülemez olduğu sonucuna varılmasına haklılık kazandırmaz. Hukuk kurallarının muğlak ifadeler içermesi hukuk devletinde arzu edilir bir durum olmasa da modern devlette bundan kaçınılması ve kuralın kapsamına giren tüm durumların kazuistik bir yöntemle önceden düzenlenmesi imkânsızdır. Dolayısıyla kuralın somut olaydaki uygulanma biçimi, diğer ifadeyle Mahkemenin somut olayda kuralın kapsamını öngörülemez biçimde genişletip genişletmediği önemli hâle gelmektedir.

50. Mahkemenin başvurucu hakkında yapılan güvenlik soruşturmasını olumsuz olarak nitelerken başvurucunun PKK ile irtibatlı olduğu gerekçesiyle 677 sayılı KHK ile kapatılan KURDİ-DER isimli derneğin açılışında bulunduğu, söz konusu Dernekte öğretmenlik yaptığı ve Derneğe kursiyer topladığı, babası aleyhine örgüt üyeliği suçlamasıyla açılan ve derdest olan kamu davasının bulunduğu, ayrıca babasının basit yaralama olayı kapsamında mağdur/şüpheli sıfatıyla ifade verdiği tespitlerine dayandığı anlaşılmaktadır. Mahkeme ayrıca 667 sayılı KHK'nın ve anılan KHK ile getirilen kamu görevinden ihraç tedbirinin arkasındaki gerekçelerin kamu hizmetine alımda da dikkate alınması gerektiğine vurgu yapmıştır.

51. 15 Temmuz 2016 tarihinde gerçekleşen darbe girişiminden sonra ülkenin karşı karşıya kaldığı ve ulusal egemenliğe yönelen tehdidin bertaraf edilmesi amacıyla olağanüstü hâl ilan edilmiştir. Olağanüstü hâli doğuran tehdidin bertaraf edilmesi amacıyla bu dönemde kanun hükmünde kararname çıkarılmıştır. Bu kanun hükmünde kararname sonradan kanunlaşmıştır. Bu

kapsamda çıkarılan 676 sayılı KHK ile devlete sadakatten ziyade terör örgütlerine veya devletin millî güvenliğine karşı faaliyette bulunduğu Millî Güvenlik Kurulunca karar verilen yapı, oluşum veya gruplara sadakat gösterdiğine kanaat getirilen kamu görevlilerinin memuriyetten çıkarılmalarına ilişkin hükümler sevk edilmiştir. Mahkeme, söz konusu KHK'yla meslekten çıkarma tedbirinin getirilmesinin arkasındaki gerekçelerin memuriyete girişte de gözetilmesi gerektiğini ifade etmiştir.

52. Mahkemenin bu yorumunun keyfî olmadığı vurgulanmalıdır. Anayasa'ya ve 657 sayılı Kanun'a göre devlete sadakat yükümlülüğü devlet memurlarının temel ödevlerindedir. Bu sebeple bir kimse hakkında yapılan güvenlik soruşturması sonucunda bu kişinin devlete sadakatinden kuşku edilmesini haklı gösterecek ölçüde tespitlerin elde edilmesi hâlinde güvenlik soruşturmasının olumsuz olarak nitelenmesi makul karşılanabilir. Olağanüstü hâl ilan edilmesine neden olan olaylar ve olağanüstü hâl döneminde alınan tedbirlerin amacı gözetildiğinde bir kimsenin terör örgütleriyle bağlantısının bulunduğu tespit edilmesi durumunda bu kişinin devlete sadakatinden kuşku edilmesini gerektiren haklı nedenlerin var olduğu sonucuna ulaşılması keyfî bir yargı olmaz.

53. Buna karşılık kişinin devlete sadakat göstermeyeceğine yönelik kuşku kişisel değerlendirme ve kanaatlere değil somut ve maddi tespitlere dayanmalıdır. Bu çerçevede güvenlik soruşturması ve arşiv araştırması sonucu elde edilen verilerin somut olmaması hâlinde bunlara dayanılarak güvenlik soruşturmasının olumsuz olarak nitelenmesi keyfîliğe yol açabilir ve kuralın uygulanmasını öngörülebilir olmaktan çıkarabilir. Bu açıdan somut olayda başvuru hakkında yapılan tespitler gözetildiğinde yerleştiği sözleşmeli memur kadrosuna atamasının yapılmayacağına başvuru açısından öngörülebilir olup olmadığı ve kamu makamlarının yorumlarının keyfîlik taşıyıp taşımadığı değerlendirilmelidir.

54. Başvurucunun güvenlik soruşturmasının olumsuz olarak nitelendirilmesine yol açan tespitlerin bir kısmı başvurucunun şahsına değil babasına ilişkindir. İdarenin dayandığı olgulardan biri başvurucunun babasının basit yaralama olayı kapsamında kolluk birimlerine mağdur/şüpheli sıfatıyla ifade vermiş olması, diğeri ise yine başvurucunun babasının aleyhine örgüt üyeliği suçlamasıyla açılmış ve derdest olan bir kamu davasının bulunmasıdır. Hukuk devletinde bir kimsenin başkalarının fiillerinden sorumlu tutulması -kanunda öngörülen- çok istisnai hâller dışında kabul edilemez. Çağdaş hukuk sistemleri bireyin özerkliğini esas alarak ona haklar bahşetmekte ve sorumluluklar yüklemektedir. Bir kimsenin hukuken ve fiilen davranışlarını kontrol etme gücü ve yükümlülüğünü haiz olmadığı başka bir bireyin fiillerden dolayı kamu otoritelerinin yaptırımına maruz kalması bireysel özerklik düşüncesiyle bağdaşmamaktadır.

55. Bununla birlikte somut olayda Mahkemenin başvuruçunun babası ile ilgili olguya dayanmadığı görülmektedir. Mahkeme kararında başvuruçunun şahsıyla ilgili tespitler ön plana çıkarılarak değerlendirme yapılmıştır. Anayasa Mahkemesi başvuruçunun adil yargılanma hakkının ihlal edilip edilmediğini idarenin işlem tesis ederkenki gerekçesinden ziyade derece mahkemelerinin gerekçesi üzerinden gerçekleştirir. Olayda Mahkemenin başvuruçunun babasıyla ilgili olguyu gerekçesinin dışında tuttuğu gözetildiğinde bu olguya ilgili olarak Anayasa Mahkemesinin bir değerlendirme yapmasına gerek bulunmamaktadır.

56. Başvuruçunun güvenlik soruşturmasının olumsuz olarak değerlendirilmesine dayanak gösterilen diğer bir tespit ise KURDİ-DER isimli derneğin açılışında bulunması, bu Dernekte öğretmenlik yapması ve kursiyer toplamaya çalışmasıdır. Başvuruçunun bu iddiaya karşı itirazlarını ileri sürme imkânına kavuştuğu not edilmelidir. Bu bağlamda başvuruçunun, Dernek ile organik bir bağının bulunmadığını öne sürmüş ise de başvuruçunun Derneğin faaliyetlerine katıldığı tespitine yönelik açık bir itirazda bulunmadığı dikkate alınmalıdır.

57. Terör örgütü ile bağlantılı olduğu tespit edilen bir derneğin faaliyetlerine katılan bir kişinin anayasal düzene sadakati hususunda kamu makamlarında kuşku oluşması kabul edilebilir bir durumdur. Bu hâle uyan bir kimsenin memuriyete alınmamasının bu kişi açısından öngörülebilir olduğu söylenebilir. Öte yandan kamu makamlarının soyut bilgiler içeren bir istihbarat raporundan hareket etmediği gözlemlenmektedir. Aksine söz konusu raporda başvuruçunun Derneğin faaliyetlerine katıldığına ilişkin olarak somut tespitler yer almaktadır. Başvuruçunun karşı argümanları ileri sürme imkânına sahip olmasına rağmen bu tespite karşı bir itiraz öne sürmediği gözetildiğinde Mahkemenin başvuruçunun 677 sayılı KHK ile kapatılan bir derneğin faaliyetlerine katılmasını güvenlik soruşturmasının olumsuz sonuçlanması olarak yorumlamasında herhangi bir keyfilik veya bariz takdir hatası bulunmamaktadır.

58. Tüm bu hususlar gözetildiğinde başvuruçunun güvenlik soruşturmasının olumsuz olarak kabul edilmesinin keyfî ve temelsiz olmadığı, bu nedenle başvuruçunun iddialarının kanun yolu şikâyeti niteliğinde olduğu değerlendirilmiştir. Dolayısıyla başvuruçunun şikâyetinin açıkça dayanaktan yoksun olduğu kanaatine varılmıştır.

59. Açıklanan gerekçelerle başvuruçunun açıkça dayanaktan yoksun olması nedeniyle kabul edilemez olduğuna karar verilmesi gerekir.

Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, Hicabi DURSUN, Celal Mümtaz AKINCI, M. Emin KUZ ve Yusuf Şevki HAKYEMEZ bu görüşe katılmamışlardır.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Adil yargılanma hakkının ihlal edildiğine ilişkin iddianın açıkça dayanaktan yoksun olması nedeniyle KABUL EDİLEMEZ OLDUĞUNA Zühtü ARSLAN, Hasan Tahsin GÖKCAN, Engin YILDIRIM, Hicabi DURSUN, Celal Mümtaz AKINCI, M. Emin KUZ ve Yusuf Şevki HAKYEMEZ'in karşıoyu ve OYÇOKLUĞUYLA,

B. Yargılama giderlerinin başvuru üzerinde BIRAKILMASINA 20/5/2021 tarihinde karar verildi.

KARŞIOY GEREKÇESİ

1. Başvurucunun, hakkında yapılan güvenlik soruşturması ve arşiv araştırmasının olumsuz sonuçlanması nedeniyle memuriyete başlatılmamasının adil yargılanma hakkını ihlal ettiğine dair şikâyeti Mahkememiz çoğunluğu tarafından açıkça dayanaktan yoksun olduğu gerekçesiyle kabul edilemez bulunmuştur.

2. Başvurucu girdiği Kamu Personeli Seçme Sınavı (KPSS) ve -başvuru formunda belirtildiğine göre-kurumca yapılan mülakat sonucunda Elektrik Üretim Anonim Şirketi Genel Müdürlüğüne bağlı bir işletme müdürlüğüne sözleşmeli memur olarak yerleştirilmiş, ancak hakkında yapılan güvenlik soruşturması ve arşiv araştırmasının olumsuz sonuçlanması sebebiyle ataması yapılmamıştır.

3. Bu idari işleme karşı açılan dava idare mahkemesi tarafından reddedilmiştir. Başvurucunun istinaf talebinin bölge idare mahkemesi tarafından reddedilmesiyle de karar kesinleşmiştir.

4. Başvurucu hakkındaki dava dosyası incelendiğinde idare mahkemesinin ret kararını davalı idarenin beyanlarına dayandırdığı görülmektedir. Mahkeme, idare tarafından yapıldığı anlaşılan güvenlik soruşturması ve arşiv araştırmasıyla ilgili olarak düzenlenmiş olan bir "bilgi notu"nu hükme esas almıştır. Davacının atamasının yapılmamasına sebep olan bu istihbari "bilgi notu"nun içeriği mahkeme kararında şu şekilde ifade edilmiştir: "[Davacının] hakkında yapılan inceleme ve soruşturma sonucunda, kuruluşunda görev alarak öğretmenlik de yaptığı ... isimli derneğin, 677 sayılı Olağanüstü Hal Kapsamında Bazı Tedbirler Alınması Hakkında Kanun Hükmünde Kararname'nin 3. maddesi hükümleri çerçevesinde, Terör örgütlerine veya Milli Güvenlik Kurulunca Devletin milli güvenliğine karşı faaliyette bulunduğu karar verilen yapı, oluşum veya gruplara aidiyet, iltisak veya bunlarla irtibatlı olan ekli (6) sayılı listede yer alan dernekler arasında bulunduğu;

Babası ...'nın ... 'Silahlı Terör Örgütüne Üye Olmak' suçuyla sanık sıfatıyla yargılamasının devam ettiği, ...,Taksirli Yaralama olayından şüpheli olarak işlem yapıldığı..." (§16).

5. Görüldüğü üzere, Mahkemenin gerekçesi biri başvuruçunun kendisiyle, diğeri babasıyla ilgili iki bilgiye dayanmaktadır. Bu nedenle "Mahkemenin başvuruçunun babasıyla ilgili olguyu gerekçesinin dışında tuttuğu" yönündeki çoğunluk görüşüne(§ 55) katılma imkânı bulunmamaktadır. Belirtmek gerekir ki kararın hiçbir yerinde başvuruçunun sadece kendisiyle ilgili bilginin dikkate alındığı, babasının terör örgütüne üye olma suçundan yargılanmasına ve taksirli yaralama olayından dolayı hakkında işlem yapılmasına ilişkin bilgilerin davanın sonucuna etkili olmadığı ifade edilmemiştir. Mahkemenin başvuruçuyla ilgili olarak bir derneğin kuruluşunda görev alarak öğretmenlik yaptığına dair bilgiyi koyu (bold) yazmış olması, bu hususa vurgu yaptığını göstermekle birlikte bu durum -başvuruçunun kendisiyle ilgili bilgilerin devamında- babasıyla ilgili olarak Mahkemeye sunulan bilgilerin hiçbir şekilde hükme esas alınmadığı anlamına gelmemektedir.

6. Anayasa Mahkemesinin konuya ilişkin kararlarında belirttiği üzere, hakkaniyete uygun yargılanma hakkının en önemli unsurlarından biri gerekçeli karar hakkıdır. Gerekçenin ilgili ve yeterli olması, kişinin hakkında verilen hükmü anlaması ve bunlara karşı etkili şekilde itiraz veya temyiz yoluna başvurabilmesi bakımından oldukça önemlidir (bkz. Sencer Başat ve diğeri [GK], B. No: 2013/7800, 18/6/2014, § 34).

7. Gerekçeli karar hakkı, taraflardan birinin davanın sonucuna etkili olacak bir iddiasının makul şekilde karşılanmasını gerektirir. Anayasa Mahkemesinin vurguladığı üzere bir davada taraflarca öne sürülen iddia ve savunmalar davanın sonucunu değiştirecek mahiyetteyse, bunlara mahkemelerce makul bir cevap verilmelidir (Sencer Başat ve diğeri, § 35; Erdal Türkmen, B.No: 2016/2100, 4/4/2019, § 37). Makul gerekçelendirme "iddia ve savunmadan birinin diğeri üstün tutulma sebebinin ve bu kapsamda davanın taraflarınca gösterilen delillerden karara dayanak olarak alınanların mahkemelerce kabul edilme ve diğeri reddedilmesi hususunda, makul dayanakları olan bir bilgilendirmeyi sağlayacak ölçü ve özene sahip olması"nu gerektirmektedir (Sencer Başat ve diğeri, § 37).

8. Davanın sonucunu etkileyebilecek bir hususta mahkemenin ilgili ve yeterli bir cevap vermemesi yahut esaslı iddiaların cevapsız bırakılması halinde gerekçeli karar hakkı ihlal edilebilir (Sencer Başat ve diğeri, § 39). Avrupa İnsan Hakları Mahkemesi de temel hak ve özgürlüklerin etkili bir şekilde korunması için ulusal mahkemelerin tarafların dayanaklarını, iddialarını ve sundukları delilleri etkili bir şekilde inceleme görevi olduğunu vurgulamıştır (Dulaurans/Fransa, B.No: 34553/97, 21/3/2000, § 33; Kraska/İsveç, B.No: 13942/88, 19/4/1993, § 30).

9. Somut olayda başvuru, kuruluşunda görev aldığı söylenen derneğin kurucusu, üyesi ve öğretmeni olmadığını, bu durumun dernekle ilgili kayıtların incelenmesinden anlaşılacağı ileri sürmüştür. Başvurucuya göre aksi yöndeki bilgiler gerçeği yansıtmayan, somut bir veriye veya belgeye dayanmayan istihbari nitelikte bir yorumdan ibarettir. Bu durumda gerekçeli karar hakkı, sonuca etkili olacak bu önemli iddianın tartışılmasını, değerlendirilmesini ve davacının itirazının karşılanmasını zorunlu kılmaktadır. Buna karşılık bireysel başvuruya konu kararda bu husus değerlendirilmemiş, bunun yerine hiçbir açıklama yapılmadan idare tarafından sunulan “bilgi notu”nun doğru olduğu kabul edilmiştir.

10. Bunun yanı sıra anılan husus istinaf aşamasında da hiçbir şekilde değerlendirilmemiştir. Mahkemeler, idare tarafından sunulan bilgilerin doğruluğunu araştırmadan ve kararlarında tartışmadan sadece ilgili mevzuat hükümlerine atıf yapmak suretiyle kabul etmişlerdir. Halbuki istihbari bilgiler çoğu zaman teyide muhtaç verilerden oluşmaktadır ve bunun bir sonucu olarak da hatalı olabilirler. Somut olayda olduğu gibi yalnızca bu bilgilere dayalı olarak, bilgi notunda yer alan olgular araştırılmadan ve doğrulanmadan verilen yargısal kararlar, hakkaniyete uygun yargılanma hakkının ihlaline yol açabilir.

11. İdare mahkemelerinin sunulan istihbari bilgileri sorgulamadan kabul etmesi, uygulamada bu bilgilerin “otomatik sonuç doğurması” anlamına gelir. Halbuki Anayasa Mahkemesi yakın tarihli bir kararında istihbari bildirimlerin idari ve yargısal makamlarca sorgulanmadan esas alınmasının Anayasa’yla bağdaşmayacağını belirtmiştir. Anayasa Mahkemesine göre “güvenlik kurumlarınca yapılacak değerlendirmenin otomatik sonuç doğurması idarelere ve idari işlemi denetleyecek mahkemelere gerçek ve tüzel kişilerin terör örgütleriyle iltisakı yahut irtibatı bulunup bulunmadığı hususunda değerlendirme yapma yetkisinin verilmemesi, söz konusu bildirimlerin doğruluğunu denetleme ve gerçek duruma göre idari işlem tesis etme imkânını önemli ölçüde sınırlamaktadır” (AYM, E. 2018/90, K.2019/85, 14/11/2019, § 47).

12. Kamu makamlarının düzenlediği ancak içeriği tartışmalı olan bir belgenin yargılamada “otomatik” olarak doğru kabul edilmesi, bu belgeye taraflarca ileri sürülen diğer bilgi ve belgeler karşısında üstünlük tanınması anlamına gelir. Bu da hiç kuşkusuz davacıyı davalı idare karşısında dezavantajlı duruma düşürecektir. Bu bağlamda belirtmek gerekir ki sunulan belgelerin içeriği sorgulanmayacaksa ve buna yönelik itirazlar dikkate alınmayacaksa söz konusu belgeyi esas alan idari işlemlere karşı dava açmanın da anlamı kalmayacaktır.

13. Somut olayda idare mahkemesinin kamu makamlarınca hazırlanan belgeye üstünlük tanıyarak, adeta mutlak bir “gerçeklik karinesi” atfettiği anlaşılmaktadır. Halbuki, içeriğine itiraz edilen bir

belgede yer alan bilgilerin hükme esas alınırken incelenmesi, güvenilirliğinin ve doğruluğunun tespit edilmesi hakkaniyete uygun bir yargılamanın olmazsa olmaz şartıdır. Bunun yapılmamış olması veya yapıldığının gerekçede gösterilmemesi, davacıyı dezavantajlı duruma düşürdüğü için silahların eşitliği ilkesine aykırılık teşkil etmektedir.

14. Diğer taraftan önemle vurgulamak gerekir ki, Anayasa'nın 129. maddesinin birinci fıkrası uyarınca memurlar ve diğer kamu görevlilerinin Anayasa ve kanunlara sadakat yükümlülüğü bulunmaktadır. Terör örgütleriyle irtibatlı ve iltisaklı bir derneğin kuruluşunda yer alan ve faaliyetlerine katılan bir kişinin memuriyete kabul edilmemesi anlaşılabilir bir durumdur. Ancak ilgili kişinin irtibat ve iltisakının, istihbari bilgi notlarıyla yetinilmeden, teyit ve tespit edilmesi gerekir.

15. Bu bağlamda başvurunun faaliyetlerine katıldığı ileri sürülen ve 677 sayılı OHAL KHK'sı ile kapatılan derneğin terör örgütüyle nasıl bir irtibat ve iltisak içinde olduğuna dair herhangi bir açıklama mahkeme kararında bulunmamaktadır. Mahkemenin gerekçesinde başvurunun dernekle ilişkisi gösterilemediği gibi, söz konusu derneğin faaliyetlerinin terörle veya milli güvenliğe aykırı yapı veya oluşumlarla ilişkili olduğuna dair bir açıklamaya da yer verilmemiştir. Bu durum başvurucuyu yargılamada davalı tarafa nazaran dezavantajlı bir pozisyona düşürmüştür.

16. Öte yandan, başvurunun babasına ilişkin bilgilerin de memuriyete başlatmama işlemini hukuka uygun bulan yargı kararında kullanıldığı, ancak başvurunun kendisiyle ilgili olmayan bu bilgilerin idari işlemi neden ve nasıl haklılaştırdığı hususunun gerekçede yer almadığı görülmektedir. Mahkeme kararında bu konuda hiçbir değerlendirmenin yapılmaması, başvurunun sadece kendisiyle ilgili istihbari bilgilerden değil aynı zamanda babası hakkında sunulan bilgilerden dolayı da memuriyete atanmadığı kanaatinin oluşmasına yol açmaktadır.

17. Babalarının yaptıklarından dolayı evlatlarını sorumlu tutmak, insanı hür ve irade sahibi bir varlık olarak kabul etmemek demektir. Bu nedenle babaların işlediği suçun cezası evlatlara çektirilemez. Bu kadim bir ilkedir. Somut olayda derece mahkemelerinin kararlarında bu kadim ve evrensel ilkeye de uyulmadığı görülmektedir.

18. Açıklanan gerekçelerle, adil yargılanma hakkı kapsamında başvurunun gerekçeli karar hakkının ve silahların eşitliği ilkesinin ihlal edildiğini düşündüğümünden çoğunluğun kabul edilemezlik kararına katılmıyorum.

Başkan

Zühtü ARSLAN

KARŞIOY GEREKÇESİ

1. Başvuran ÖSYM Başkanlığı tarafından yapılan KPSS sınav sonucu esas alınarak EÜAŞ Genel Müdürlüğü'ne bağlı Karakaya HES İşletme Müdürlüğü'ne sözleşmeli memur olarak yerleştirilmiştir. Akabinde 676 sayılı Ohal Kararnamesinin 74. maddesiyle değişik 657 sayılı DMK 48/A-8. madde ve bendi uyarınca güvenlik soruşturması ve arşiv araştırması olumsuz sonuçlanması nedeniyle atamasının yapılmadığı bildirilmiş, başvurucunun açtığı iptal davası idare mahkemesi tarafından reddedilmiş, istinaf başvurusu de reddedilerek karar kesinleşmiştir.

2. İdare mahkemesi ret gerekçesinde idarenin işlemi tesis ederken dayanağı olan iki bilgi ve belgeye atıf yapmıştır. Bunlar başvuranın babası hakkında terör örgütü üyeliği isnadıyla soruşturma bulunması, başvuranın da Kararname ile kapatılan Kurdi-Der isimli dil derneğinin kuruculuğunu ve öğretmenliğini yaptığı yönündeki istihbari bilgidir. Bununla birlikte dosyada başvuranın söz konusu Dernekle irtibatı olduğuna veya görev aldığına ilişkin herhangi bir belge veya tanık anlatımı bulunmamaktadır. Bu nedenle konunun aslında Kararname ile kapatılan bir Derneğin üyesi veya yöneticisi olmakla bir ilgisi bulunmamaktadır. Olayda sakıncası nedeniyle kapatılan bir derneğin faaliyetlerine katıldığı iddiası dolayısıyla irtibat ve iltisakın tartışılması söz konusudur.

3. İdare mahkemesi kararı adil yargılanma hakkı yönünden iki nedenle sorunludur. İlkin adil yargılanma hakkının alt ilkesi olan silahların eşitliği ilkesi; davanın taraflarından birinin mahkeme tarafından daha üstün bir konumda tutulmamasını, her iki tarafın da iddialarını eşit bir biçimde mahkeme önünde sunma ve mahkemenin de bu delilleri tartışmasına imkan sağlamasını gerektirir. Buna karşın idarenin sunduğu belgelerden ilki, başvuranın babası hakkındaki soruşturma olup, bir kişinin akrabalarının davranışlarından sorumlu tutulamayacağı hususu hukuk devleti ilkesinin evrensel prensiplerindedir. Buna karşın bu bilgiye idare tarafından atfedilen hukuki değer, mahkeme gerekçesinde tekrarlanmakla (gerekçede buna itibar edilmediğinden söz edilmediği gözetildiğinde) mahkemece de kabul görmüştür. Babasına ilişkin soruşturma bilgisinin hukuka aykırı olarak aleyhine yorumlanmasına karşı başvuranın yapabileceği hiçbir savunma imkanı kalmamaktadır. Bu durum idarenin ve mahkemenin tutumu karşısında başvurunu savunmasız bırakmaktadır.

4. Hukuk devletinde adil bir yargılama yapıldığından söz edilebilmesi için bir tarafa yüklenen vakaların doğruluğuna ilişkin delillerin ortaya konulması ve ilgisine de bunun aksini ileri sürme imkanının tanınması gerekir. Başvuranın kendi faaliyetlerine ilişkin istihbari bilgide ise yer ve zaman gibi detayları içeren olgusal bir temele dayanılmaksızın soyut fiil atfı söz konusudur. Başvuran bu iddialara karşı başvuru formunda; herhangi bir dernek üyeliğinin veya bir dernekle organik bağının

bulunmadığını ve esasen aksi olsaydı belgeleriyle ortaya konulabileceği halde dosyaya böyle bir belgenin konulmadığını belirterek itiraz etmektedir. Başvuranın kabul etmediği bir vakıanın var olduğunu iddia eden tarafın bu iddiasını çeşitli delil araçlarıyla ispat etmesi gerekirken, idare mahkemesi idarenin dayandığı istihbarat notunu tekrarlamakla yetinip idarenin işleminin hukuka uygun bulunduğu sonucuna ulaşmıştır. Başvuranın ders verme veya diğer bir ilişkinin olmadığını savunmasına karşın, aksini gösteren herhangi bir delil ortaya konulmadığı halde bu iddianın gerçek olduğu sonucu çıkartılması, üstelik ulaşılan bu sonuca ilişkin mahkemece tek bir cümle gerekçenin de ortaya konulamaması, yargılanan davacı tarafın hukuken çaresiz bırakılması anlamına gelmektedir. İstihbari bir bilgide kişiye bir faaliyet-fiil isnat edilmesi o bilgiyi soyut olmaktan çıkarmamaktadır. Tarih, yer, faaliyete katılanlar, vb. denetlenebilir ve aksi kanıtlanabilir detayların bulunmadığı soyut bir fiil atfının gerekçesiz kabulü adil yargılanma hakkının güvenceleri bakımından büyük sorunlar içerir. Böyle bir durumda belki karine delilinden yararlanıldığı ileri sürülebilir. Hukuk yargılaması usulünde kimi zaman karinelere de yararlanılabilir. Fakat bunun için kişinin belirli bir durumda bulunduğuna ilişkin olgusal bir temel bulunmalıdır. Bununla birlikte olgusal temeline ilişkin herhangi bir kanıt sunulamayan ve kişinin de kabul etmediği bir vakaya ilişkin böyle bir bilgi notuna mutlak bir anlam yüklenmesi onu neredeyse aksi ispatlanamaz kesin delil derecesine yükseltmektedir. Bu durum ilk olarak silahların eşitliği ilkesi yönünden sorun oluşturur. Bu ilke uyarınca görünüşte davacıya delili tartışma ve görüşlerini sunma imkanı tanınmış ise de davacının ileri sürdüğü argümanlar karşısında hiçbir yorum yapılmaksızın söz konusu bilgi notuna mahkemece atfedilen değer karşısında, başvurana bir istihbarat notunun doğru olmadığını ispat etme imkanı tanınmamıştır. Bir delil veya emare hakkında ne söylenirse söylensin ilgisinin aksini ispat edemeyeceğinin belli olduğu bir muhakemede çelişmeli yargılama ilkesine uyulduğu söylenemez. Başka deyişle böyle bir durumda adil yargılanma hakkının alt güvencelerinden olan çelişmeli yargılama ilkesinin içi boşaltılmış, gerçek bir güvence sağlanamamış olur.

5. İkinci olarak mahkemenin davacının iddialarını karşılamadan ve idarenin işlemine dayanak yaptığı soyut bilgi notu hakkında hiçbir değerlendirme yapmadan, “yukarıda ayrıntısına yer verilen bilgiler dikkate alındığında ... davalı idare takdirinde hukuka aykırılık bulunmamıştır” şeklindeki ifadeyle davanın reddine karar verilmesi gerekçeli karar hakkını ihlal eder niteliktedir. Gerçekten idare mahkemesinin kararında dava konusu olayı yorumladığı tek bir cümleden ibaret olsa dahi bir gerekçenin olduğu tespit edilememektedir. Gerekçeli karar hakkı adil yargılanma hakkının en önemli güvenceleri içerisinde yer almaktadır. Bu durum karşısında gerekçeli karar hakkının ihlal edildiği açıktır.

6. Sonuç olarak ifade etmek gerekiyor ki başvuruya konu yargılama örneği ile insan haklarına saygılı bir hukuk devletinde kişilerin yargılama sürecinde mahkemelerin adil yargılanma hakkına ilişkin usul güvencelerine uygun hareket edileceği beklentilerini boşa çıkarılmakta, daha doğrusu bu güvencelerin hiçe sayılmasına yol açmaktadır. Belirtilen nedenlerle başvuranın adil yargılanma hakkının ihlal edildiği vicdani kanaatıyla karşıoy kullandım.

Başkanvekili

Hasan Tahsin GÖKCAN

KARŞIOY GEREKÇESİ

1. Kamu Personeli Seçme Sınavı (KPSS) sonucunda Elektrik Üretim Anonim Şirketi Genel Müdürlüğüne bağlı Diyarbakır Karakaya HES İşletme Müdürlüğünde sözleşmeli memur olarak işe yerleştirilen başvurusunun ilgili kurum tarafından yaptırılan güvenlik soruşturması ve arşiv araştırmasının olumsuz sonuçlanması üzerine ataması yapılmamıştır.

2. Söz konusu idari işleme karşı açılan davaya bakan Ankara 10. İdare Mahkemesi, başvurusunun güvenlik soruşturmasının olumsuz değerlendirilerek atamasının yapılmaması işleminin hukuka uygun olduğu sonucuna ulaşmıştır. Mahkemenin başvuru hakkında yapılan güvenlik soruşturmasını olumsuz olarak nitelerken başvurusunun PKK ile irtibatlı olduğu gerekçesiyle 677 sayılı KHK ile kapatılan KURDİ-DER isimli derneğin açılışında bulunduğu, söz konusu Dernekte öğretmenlik yaptığı ve kursiyer topladığı, babası aleyhine örgüt üyeliği suçlamasıyla açılan ve derdest olan kamu davasının bulunduğu, ayrıca babasının basit yaralama olayı kapsamında mağdur/şüpheli sıfatıyla ifade verdiği tespitlerine dayandığı anlaşılmaktadır. Mahkeme ayrıca 667 sayılı KHK'nın ve anılan KHK ile getirilen kamu görevinden ihraç tedbirinin arkasındaki gerekçelerin kamu hizmetine alımda da dikkate alınması gerektiğine vurgu yapmıştır.

3. Anayasa Mahkemesi, 7070 sayılı Olağanüstü Hal Kapsamında Bazı Düzenlemeler Yapılması Hakkında Kanun'un; 60. maddesiyle 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu'nun 48. maddesine eklenen hükümle güvenlik soruşturması ve/veya arşiv araştırması yapılmasının memurluğa alınmada genel bir şart hâline getiren kuralı Anayasa'nın 13., 20. ve 128. maddelerine aykırı görerek oyçokluğuyla (13'e 1) iptal etmiştir. AYM, bu kararda özel hayata saygı hakkıyla sınırlı bir inceleme yaparak, Anayasa'nın 129. maddesinin birinci fıkrası uyarınca memurlar ve kamu görevlilerinin Anayasa ve kanunlara sadık kalarak faaliyette bulunma yükümlülüğü altında olduğu, belirtilen hususlar gözetilerek kamu görevlerine atanacak kişiler bakımından birtakım şartlar

getirilmesi çerçevesinde kamu görevine atanmadan önce kişilerin güvenlik soruşturması ve arşiv araştırmasının yapılmasının kanun koyucunun takdir yetkisinde olduğunu belirtmiştir. Bununla birlikte, Mahkememiz kamu görevlilerinin nitelikleri ve atanmalarına ilişkin kurallarla kişisel verileri ilgilendiren yasal düzenlemelerin kanunda gösterilmesi, açık, anlaşılabilir ve sınırlarının belli olması gerektiğinin altını çizmiş ve incelenen kuralın güvenlik soruşturmasına ve arşiv araştırmasına konu edilecek bilgi ve belgelerin neler olduğuna, bu bilgilerin ne şekilde kullanılacağına, hangi mercilerin soruşturma ve araştırmayı yapacağına ilişkin herhangi bir düzenleme içermediği tespitinde bulunmuştur (E.2018/73, K.2019/65, 24/7/2019, §§ 165-166, 170-171).

4. Yakın tarihli bir başka kararda da Mahkememiz terör örgütlerine iltisaklı yahut bunlarla irtibatlı olduğu bildirilen gerçek ve tüzel kişilerin kamu ihalelerine katılamayacaklarını öngören kuralı Anayasa'nın 13. ve 48. maddelerine aykırı görerek oybirliğiyle iptal etmiştir. Kural, terör örgütleriyle iltisaklı yahut irtibatlı olma bakımından Emniyet Genel Müdürlüğü ve Millî İstihbarat Teşkilâtı tarafından bildirim yapılması hâlinde kişilerin otomatik olarak kamu ihalelerine katılamaması veya ihale dışı bırakılması sonucunu doğurmaktaydı. Bu bildirim kapsamındaki değerlendirmeye esas alınan olay ve olguların büyük bir olasılıkla istihbarî nitelikte olduğuna dikkat çeken Mahkememiz, bu nedenle "idarelerce tesis edilecek işlemlerle ilgili yargısal denetimin daha da önemli hâle geldiği" ne dikkat çekmiştir (E.2018/90, K.2019/85, 14/11/2019, §47).

5. Güvenlik birimlerince yapılan ve ceza soruşturmasına esas alınabilecek nitelikte bilgi ve belgelere dayanma zorunluluğu olmayan değerlendirmenin adeta otomatik sonuç doğurarak idarelerin bunun aksi yönde işlem yapmaktan kaçınma eğilimleri ve kendilerini istihbari değerlendirmeyle neredeyse bağlı hissetmeleri, bu bildirimlerin doğruluğunun ortaya konulabilmesi bakımından idari işlemi denetleyecek mahkemelerin yapacakları değerlendirmeyi yukarıda alıntıladığımız Anayasa Mahkemesi kararının da vurguladığı gibi çok önemli kılmaktadır. Güvenlik soruşturmasına ilişkin raporlarda yer alan bilgiler istihbari nitelik taşıdıklarından, hukuken geçerli başka bilgi ve belgelerle doğrulanmadıkça bu raporların tek başlarına hukuki delil gücünde kabul edilmeleri ve ilgililer aleyhine kullanılmaları hukuk devleti ilkesine aykırı olacaktır. Bu açıdan, AYM tarafından iptal edilen kuralın (bkz. § 4) somut başvurudaki uygulanma şeklinin adil yargılanma hakkını ihlal edip, etmediğinin incelenmesi gerekmektedir.

6. Çoğunluk, başvurucunun güvenlik soruşturmasının olumsuz olarak kabul edilmesinin keyfi ve temelsiz olmadığı, bu nedenle başvurucunun iddialarının kanun yolu şikâyeti niteliğinde olduğunu kabul ederek başvurucunun şikâyetinin açıkça dayanaktan yoksun olduğu kanaatiyle kabul edilemez bulmuştur. Çoğunluğa göre, derece mahkemesinin başvurucunun 677 sayılı KHK ile kapatılan bir

derneğin faaliyetlerine katılmasını güvenlik soruşturmasının olumsuz sonuçlanması olarak yorumlamasında herhangi bir keyfilik veya bariz takdir hatası bulunmamaktadır (§ 57).

7. Anayasa'nın 148. maddesinin dördüncü fıkrasında kanun yolunda gözetilmesi gereken hususlara ilişkin şikâyetlerin bireysel başvuruda incelenemeyeceği belirtilmiştir. Ancak temel hak ve özgürlüklere müdahalenin söz konusu olduğu durumlarda derece mahkemelerinin takdir ve değerlendirmelerinin Anayasa'daki güvencelere etkisini nihai olarak değerlendirecek merci Anayasa Mahkemesidir. Bu itibarla Anayasa'da öngörülen güvenceler dikkate alınarak bireysel başvuru kapsamındaki temel hak ve özgürlüklerin ihlal edilip edilmediğine ilişkin herhangi bir inceleme "kanun yolunda gözetilmesi gereken hususun incelenmesi" olarak nitelendirilemez (Şahin Alpay (2) [GK], B. No: 2018/3007, 15/3/2018, § 53, Ferhat Kara, B. No: 2018/15231, 4/6/2020, § 148).

8. Anayasa Mahkemesi istisnai durumlarda temel hak ve özgürlüklerden biri ile doğrudan ilgili olmayan bir şikâyeti kanun yolunda gözetilmesi gereken hususlara ilişkin yasak kapsamına girmeden inceleyebilir. Anayasa Mahkemesinin derece mahkemelerinin değerlendirmelerinin usule ilişkin güvenceleri anlamsız hâle getirip getirmediğini ve açık keyfilik nedeniyle yargılamanın hakkaniyetinin temelden sarsılıp sarsılmadığını incelemesi yargılamanın sonucunu değerlendirdiği anlamına gelmez. Anayasa Mahkemesi derece mahkemelerinin delillerle ilgili değerlendirmelerine ancak açıkça keyfî ve adil yargılanma hakkı kapsamındaki usule ilişkin güvenceleri anlamsız hâle getiren bir uygulama varsa müdahale edebilecektir (Ferhat Kara, B. No: 2018/15231, 4/6/2020, § 149). Belirtilen nedenlerle başvurunun kabul edilebilir olmasında herhangi bir sorun görmediğimden, esasa ilişkin incelememize geçebiliriz.

9. Anayasa'nın 36. maddesinde güvence altına alınan adil yargılanma hakkı temel olarak yargılama sürecinin ve usulünün hakkaniyete uygun olarak yürütülmesini teminat altına almaktadır (M.B. [GK], B. No: 2018/37392, 23/7/2020, § 80). Bu maddenin kapsam ve içeriğinin yorumlanmasında hukuk devleti ilkelerine göre hareket edilmesi gerekir (M.B., § 84). Bu bağlamda hukuk güvenliği ve belirliliği ilkeleri hukuk devletinin gereklerinden biri olarak dikkate alınmalıdır. Mahkememiz bir kararında hukuk güvenliği ilkesiyle ilgili olarak şu açıklamalarda bulunmuştur:

Kişilerin hukuki güvenliğini sağlamayı amaçlayan hukuki güvenlik ilkesi; hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar. Belirlilik ilkesi ise yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olmasını, ayrıca

kamu otoritelerinin keyfî uygulamalarına karşı koruyucu önlem içermesini ifade etmektedir (AYM, E.2013/39, K.2013/65, 22/5/2013).

10. Bireysel başvuruya konu ilk derece Mahkemesi kararından, 657 sayılı Kanun'un 48. maddesine eklenen alt bentteki şartı güvenlik soruşturması ve/veya arşiv araştırmasının olumlu sonuçlanması gerektiği şeklinde bir yorum çıkmaktadır. Kuralın başvuruçunun yerleştirildiği kadro da dâhil olmak üzere tüm devlet memurluğu kadrolarına atanabilmek için güvenlik soruşturması ve/veya arşiv araştırması yapılması şartını aradığı açık olmakla birlikte bunun olumlu sonuçlanması gerektiği hususunda kural bir ibare içermemektedir. Bu da kuralın uygulanmasıyla ilgili belli ölçüde bir belirsizliğe neden olmaktadır. Zira güvenlik soruşturmasının olumlu neticelenip neticelenmediği konusunda ulaşılabilecek sonucun atamaya yetkili konumda bulunan kişi veya kişilere bağlı olarak değişmesi riskinin olması keyfi ve ayrımcı uygulamaların ortaya çıkmasına neden olabilecektir.

11. Elbette, bir kimse hakkında yapılan güvenlik soruşturması sonucunda bu kişinin devlete sadakatinden kuşkulandırılmasını haklı gösterecek tespitlerin elde edilmesi hâlinde güvenlik soruşturmasının olumsuz olarak nitelenmesi makul görülebilir. Çünkü, Anayasa'ya ve 657 sayılı Kanun'a göre devlet memurları devlete sadakat yükümlülüğü altındadır. Burada önemli olan nokta kişinin devlete sadakat göstermeyeceğine yönelik şüphenin kişisel değerlendirme ve kanaatlere değil somut, nesnel ve maddi tespitlere dayalı olmasıdır. Bu yapılmadan güvenlik soruşturmasının olumsuz olarak nitelenmesi keyfiliğe yol açabilir ve kuralın uygulanmasını öngörülebilir olmaktan çıkarabilir. Bu açıdan somut olayda başvuruçunun hakkında yapılan tespitler gözetildiğinde yerleştiği sözleşmeli memur kadrosuna atamasının yapılmayacağına başvuruçunun açısından öngörülebilir olup olmadığı ve kamu makamlarının yorumlarının keyfilik taşıyıp taşımadığı değerlendirilmelidir.

12. İlk derece mahkemesinin kararı esas olarak güvenlik ve arşiv araştırması yapan yetkililerin idareye sunduğu bildirimlerin aynen tekrarından ibarettir. Başvuruçunun güvenlik soruşturmasının olumsuz olarak değerlendirilmesine dayanak gösterilen ana iddia başvuruçunun KURDİ-DER isimli derneğin açılışını yapması, bu Dernekte öğretmenlik yapması ve kursiyer toplamaya çalışmasıdır. Başvuruçunun ilgili olarak yapılan bu iddialar istihbarat çalışmasından elde edilmiş olup, bunlarla ilgili olarak istihbarat raporu dışında herhangi bir belgeye derece mahkemesi kararında yer verilmemiştir. Mahkemenin başvuruçunun istihbarat raporundan başka bir dayanağı bulunmayan bu iddialara karşı öne sürdüğü savları tartışmadan ve gerçekliği hususunda gerekli araştırma ve inceleme yapmadan bunları hükme esas almasının adil yargılanma hakkının unsurlarından olan silahların eşitliği ve çelişmeli yargılama ilkelerini zedeleyen önemli bir eksiklik olduğundan şüphe duyulmamalıdır.

13. Elbette, terör örgütü ile bağlantılı olduğu tespit edilen bir derneğin faaliyetlerine katılan bir kişinin anayasal düzene ve devlete sadakati hususunda kamu makamlarında kuşku oluşması gayet anlaşılabilir ve makul bir duruma işaret etmektedir. Bununla birlikte adı geçen derneğin terör örgütü ile bağlantılı olduğuna, başvuruçunun da derneğin bu yönünü bilerek faaliyetlerine katıldığına dair kanaat oluşturacak olguların derece mahkemesince ortaya konulması gerekirdi. Mahkeme sadece Derneğin 677 sayılı KHK ile kapatıldığını belirtmiş ve bu Dernekle ilgili başka bir değerlendirme ve araştırma yapmamıştır. Derneğin kapatıldığı 677 sayılı KHK'da da terör örgütleriyle bağlantısının bulunduğu gerekçesine yer verilmiş, bu Derneğe yönelik başka herhangi bir somut tespitle bulunulmamıştır. Başvuruçunun Dernek faaliyetlerinin örgütsel bir amaç kapsamında kalıp, kalmadığı da kararda tartışılmamıştır. Kaldı ki, Derneğin OHAL Komisyonu tarafından terör örgütüyle bağlantısının bulunmadığının tespit edilmesi durumunda yerel mahkemenin değerlendirmesi herhangi bir temelden yoksun kalmış olacaktır. Bütün bu hususlar, başvuruçuyu silahların eşitliği bağlamında idare karşısında dezavantajlı bir konuma itmiştir.

14. Hak ve özgürlükleri sınırlandıran hükümlerin kamu makamlarınca geniş yorumlanması bireyler açısından öngörülemez sonuçlar doğurabileceğinden hukuk devletine aykırılık teşkil etmenin yanında adil yargılanma hakkını da zarar verecektir. Derece mahkemelerinin, hak ve özgürlükleri sınırlayıcı kuralların kapsamının geniş yorumlanması hususunda büyük bir dikkat ve özen göstermesi gerekmektedir.

15. Her ne kadar Mahkememiz çoğunluğu somut olayda derece mahkemesinin başvuruçunun babasıyla ilgili olguyu "gerekçesinin dışında tuttuğu" görüşünü savunsa da buna katılmak mümkün değildir. Derece mahkemesinin kararında başvuruçunun babasıyla ilgili olarak basit yaralama olayı kapsamında kolluk birimlerine mağdur/şüpheli sıfatıyla ifade vermiş olması, aleyhine örgüt üyeliği suçlamasıyla açılmış ve derdest olan bir kamu davasının bulunması tespitlerine de yer verilmiştir. Halbuki, bir kimsenin başkalarının fiillerinden sorumlu tutulmasının çok istisnai hâller dışında kabul edilememesi en temel hukuk devleti ilkelerinden biridir. Somut olayımızda, derece mahkemesinin başvuruçunun güvenlik soruşturmasının olumsuz olduğu sonucuna ulaşırken babasının fiillerini de dikkate alması esas gerekçesini destekleyici bir işlev görmektedir. Başvuruçunun memur olabilme şartlarını taşıyıp taşımadığının tartışıldığı bu davada babasının fiillerinin de kendisi hakkındaki karara yansıtılması öngörülebilir olmayan bir duruma işaret etmektedir.

16. Derece mahkemesi güvenlik birimlerinin bildirimindeki hususlarla ilgili bir değerlendirmede bulunmadan, bunların doğruluğunu araştırmadan bildirimdeki tespitleri gerekçe olarak aynen kabul etmiştir. Örneğin, mahkemenin başvuruçunun kapatılan derneğin faaliyetlerine katıldığını kararında

somut olarak göstermesi gerekirdi. Kaldı ki Kürt dili ile ilgili çalışmalar yapan derneğin kapatılmadan önceki faaliyetlerinin yasal olmadığına dair herhangi bir tespit ve bilgi de bulunmamaktadır.

17. Başvurucunun babasının somut olayla ilgili olmayan fiillerine de derece mahkemesi, kararda gerekçe olarak yer vermiştir. Bu durum bile tek başına derece mahkemesinin kararının bildirimdeki istihbari tespitlerin tekrarından öte bir şey içermediğinin bir göstergesi sayılabilir. Bu durumda şu soruyu sormamız gayet anlaşılır, makul, meşru ve rasyonel olacaktır: Eğer derece mahkemesi, istihbari bilgiler için güvenlik ve arşiv araştırmasıyla ilgili bir değerlendirme yapmayacaksa, buradaki bilgilerin doğruluğunu araştırmayacaksa mahkemeye başvurmanın, yargı yoluna gitmenin ne anlamı olacaktır? İnsan haklarına saygılı anayasal demokratik bir hukuk devletinde yargı organları önlerine gelen konularda değerlendirme ve araştırma yapmaktan kaçınmamalıdır.

18. Açıklanan tüm bu hususlar dikkate alındığında Anayasa'nın 36. maddesinde güvence altına alınan adil yargılanma hakkı kapsamında hukuk kurallarının öngörülemes biçimde yorumlanması ve ilgili ve yeterli bir gerekçe olmaması nedenleriyle hakkaniyete uygun yargılanma hakkının ihlal edildiği sonucuna ulaştığımdan çoğunluk kararına katılmadım.

Üye

Engin YILDIRIM

KARŞIOY GEREKÇESİ

1. Başvurucu, güvenlik soruşturması ve arşiv araştırmasının olumsuz sonuçlandığı gerekçesiyle memuriyete başlatılmama işlemine karşı açılan iptal davasında hukuka aykırı karar verilmesi nedeniyle adil yargılanma hakkının ihlal edildiği iddiasıyla Anayasa Mahkemesine bireysel başvuruda bulunmuştur. Çoğunluk kararında derece mahkemelerince başvuruçunun güvenlik soruşturmasının olumsuz olarak kabul edilmesinin keyfi ve temelsiz olmadığı, bu nedenle başvuruçunun iddialarının kanun yolu şikâyeti niteliğinde olduğu değerlendirilmiş ve başvuruçunun adil yargılanma hakkının ihlal edildiğine ilişkin iddiasının açıkça dayanaktan yoksun olduğu kanaatine ulaşılmıştır.

2. Bireysel başvuruya konu uyuşmazlık, Ölçme, Seçme ve Yerleştirme Merkezi Başkanlığı tarafından 2016/I döneminde yapılan Kamu Personeli Seçme Sınavı sonucu esas alınarak Elektrik Üretim Anonim Şirketi Genel Müdürlüğüne bağlı Diyarbakır Karakaya HES İşletme Müdürlüğüne sözleşmeli memur olarak yerleştirilen başvuruçunun sözleşmeli memur olarak atanmamasına ilişkin işleme karşı açtığı iptal davasında ortaya çıkmıştır.

3. Burada Mahkememiz çoğunluk kararındaki sorunlu yönün daha net biçimde fark edilebilmesi için İdare Mahkemesi karar gerekçesindeki bazı hususların daha detaylı biçimde ifade edilmesi gerekmektedir.

4. İptal davasında çözüme kavuşturulması gereken temel mesele başvuruçunun memuriyete atanma şartlarını taşıyıp taşımadığı hususunda ortaya çıkmaktadır. Başvuruçunun devlet memurluğuna atanmanın genel ve özel şartlarının düzenlendiği 657 sayılı Kanun'un 48. maddesinde sayılan şartlardan "Güvenlik soruşturması ve/veya arşiv araştırması yapılmış olmak" şartını sağlamadığı ifade edilmiş ve Elektrik Üretim Anonim Şirketi Genel Müdürlüğüne bağlı Diyarbakır Karakaya HES İşletme Müdürlüğüne sözleşmeli memur olarak yerleştirilen başvuruçuyu ile ilgili olarak Genel Müdürlükçe yaptırılan güvenlik soruşturması ve arşiv araştırması olumsuz sonuçlandırılarak bu durum başvuruçuya bildirilmiştir.

5. Başvuruçuyu bu işleme karşı Ankara 10. İdare Mahkemesinde dava açmıştır. İdare Mahkemesi ise, davayı sonuçlandırdığı 10.05.2018 tarihli kararında ilk olarak "yapılan inceleme ve araştırma sonucunda kuruluşunda görev alarak öğretmenlik de yaptığı Kürdi-Der isimli derneğin, 677 sayılı Olağanüstü Hâl Kapsamında Bazı Tedbirler Alınması Hakkında Kanun Hükmünde Kararnamenin 3. Maddesi hükümleri çerçevesinde, Terör örgütlerine veya Milli Güvenlik Kurulunca Devletin milli güvenliğine karşı faaliyette bulunduğu karar verilen yapı, oluşum veya gruplara aidiyet, iltisakı veya bunlarla irtibatı olan ekli (6) sayılı listede yer alan dernekler arasında bulunduğu; 'Babası Nesim Kaya'nın Ağrı Ağır Ceza Mahkemesince 2017/46 Esas Nolu dosyada 'Silahlı Terör Örgütüne Üye Olmak' suçuyla sanık sıfatıyla yargılanmasının devam ettiği, 12.09.2011 tarihinde Ağrı Murat Şehit Halis Çınar Polis Merkezi Amirliğinde 'Taksirli Yaralama' olayından şüpheli olarak işlem yapıldığı" şeklindeki bilgi notuna yer verilerek bu bilgi notu üzerine 13.06.2017 tarihli Komisyon Kararı ile güvenlik soruşturmasının olumsuz değerlendirilerek atamasının yapılmaması üzerine bu davanın açıldığı ifade edilmiştir.

6. İdare Mahkemesi kararında somut bireysel işlemin konusu olan güvenlik soruşturmasındaki bilgi notunda başvuruçuyu ve babası ile ilgili yazılanlar hakkında hiçbir değerlendirme yapılmamış, ancak 667 sayılı Kanun Hükmünde Kararnamenin amacı ve kapsamı dikkate alınarak alınan tedbirler vasıtasıyla başta FETÖ/PDY olmak üzere terör örgütlerine veya Milli Güvenlik Kurulunca devletin milli güvenliğine karşı faaliyette bulunduğu karar verilen yapı, oluşum veya gruplara üyeliği, mensubiyeti veya iltisakı yahut bunlarla irtibatı olduğu değerlendirilen kişilerin kamu kurum ve kuruluşlarından çıkarılarak Anayasa ile kurulan demokrasi düzeninin korunmak istendiğinin

görülmekte olduğu ve bu gerekçelerle çıkarılan kamu idarelerinin aynı gerekçeleri ilk atamalarda da dikkate alması gerektiğinin açık olduğu ifade edilmiştir.

7. Hemen akabinde ise "Yine, 657 sayılı Devlet Memurları Kanunu'nun 48/A-8 maddesinde 'Güvenlik soruşturması ve/veya arşiv araştırması yapılmış olmak' Devlet memurluğuna alınmada aranılacak genel şartlar arasında sayılmış olup yukarıda ayrıntısına yer verilen bilgiler dikkate alındığında davacının güvenlik soruşturmasının olumsuz değerlendirilerek atanmaması yolundaki davalı idare takdirinde hukuka aykırılık bulunmamıştır." denilerek davanın oybirliği ile reddine karar verilmiştir.

8. Yapılan bireysel başvuru üzerine Anayasa Mahkemesi çoğunluğu ise derece mahkemesinin bu yorumunun keyfî olmadığını (§ 52), somut olayda Mahkemenin başvuruçunun babası ile ilgili olguya dayanmadığını ve başvuruçunun şahsıyla ilgili tespitler ön plana çıkarılarak değerlendirme yaptığını, olayda Mahkemenin başvuruçunun babasıyla ilgili olguyu gerekçesinin dışında tuttuğu gözetildiğinde bu olguya ilgili olarak Anayasa Mahkemesinin bir değerlendirme yapmasına gerek bulunmadığını (§ 55) belirtmiştir.

9. Öte yandan Anayasa Mahkemesi çoğunluk kararında başvuruçunun kendisi ile ilgili güvenlik soruşturmasında yer alan bilgilerle ilgili de şu şekilde bir değerlendirmeye yer vermiştir:

"Terör örgütü ile bağlantılı olduğu tespit edilen bir derneğin faaliyetlerine katılan bir kişinin anayasal düzene sadakati hususunda kamu makamlarında kuşku oluşması kabul edilebilir bir durumdur. Bu hâle uyan bir kimsenin memuriyete alınmamasının bu kişi açısından öngörülebilir olduğu söylenebilir. Öte yandan kamu makamlarının soyut bilgiler içeren bir istihbarat raporundan hareket etmediği gözlemlenmektedir. Aksine söz konusu raporda başvuruçunun Derneğin faaliyetlerine katıldığına ilişkin olarak somut tespitler yer almaktadır. Başvuruçunun karşı argümanları ileri sürme imkânına sahip olmasına rağmen bu tespite karşı bir itiraz öne sürmediği gözetildiğinde Mahkemenin başvuruçunun 677 sayılı KHK ile kapatılan bir derneğin faaliyetlerine katılmasını güvenlik soruşturmasının olumsuz sonuçlanması olarak yorumlamasında herhangi bir keyfîlik veya bariz takdir hatası bulunmamaktadır." (§ 57).

10. Anayasa Mahkemesi çoğunluğunun kararına katılmak mümkün değildir. Çoğunluk kararında başvuruçunun ilgili bilgi notundan hareketle tesis edilen idari işlemin hukuka uygunluğu noktasında ciddi sorunlar yer almakla birlikte yapılan bireysel başvuru incelemesinde bu aşamada bunların değerlendirilmesine gerek bulunmadığı, daha öncelikli biçimde değerlendirilmesi gereken başka hususların bulunduğu kanaatindeyiz. Zira burada öncelikle Mahkememiz çoğunluğunca güvenlik soruşturmasında yer alan bilgilerle ilgili yapılan yorumun en az iki yönden ciddi sorunlar taşıdığı ifade edilmelidir.

11. Birinci olarak, çoğunluk kararındaki ilk derece mahkemesinin başvurusunun babası ile ilgili olguya dayanmadığı, başvurusunun şahsıyla ilgili tespitleri ön plana çıkararak değerlendirme yaptığı kabulü doğru değildir. Zira yukarıda detaylı biçimde içeriği açıklanan Ankara 10. İdare Mahkemesi karar gerekçesinde, başvuru hakkındaki güvenlik soruşturmasında kendisi ve başvurusunun babası ile ilgili yer verilenler hiçbir ayırım yapılmaksızın, olduğu gibi doğru kabul edilerek kararda başvurusunun “güvenlik soruşturmasının olumsuz değerlendirilerek atanmaması yolundaki davalı idare takdirinde hukuka aykırılık bulunmamıştır.” şeklinde bir gerekçeye yer verilmiştir.

12. Oysa Anayasa Mahkemesi çoğunluğu ilk derece mahkemesinin birkaç kelimeyi kararında koyu (bold) yazmasını esas alarak şu değerlendirmeyi yapmaktadır:

“Bununla birlikte somut olayda Mahkemenin başvurusunun babası ile ilgili olguya dayanmadığı görülmektedir. Mahkeme kararında başvurusunun şahsıyla ilgili tespitler ön plana çıkarılarak değerlendirme yapılmıştır. Anayasa Mahkemesi başvurusunun adil yargılanma hakkının ihlal edilip edilmediğini idarenin işlem tesis ederkenki gerekçesinden ziyade derece mahkemelerinin gerekçesi üzerinden gerçekleştirir. Olayda Mahkemenin başvurusunun babasıyla ilgili olguyu gerekçesinin dışında tuttuğu gözetildiğinde bu olguya ilgili olarak Anayasa Mahkemesinin bir değerlendirme yapmasına gerek bulunmamaktadır.” (§ 55).

13. Bu yorumun doğru olmadığı kanaatindeyiz. Zira gerekçenin varlığından söz edilebilmesi için ilk derece mahkemesince başvurusunun örgütle iltisakını ortaya koyan somut verileri göstermesi gerekir. Somut olayda mahkeme bunu yapmamıştır. Ankara 10. İdare Mahkemesinin kararında yukarıda aynen yer verilen bilgi notu içerisinde sadece “kuruluşunda görev alarak öğretmenlik de yaptığı Kürdi-Der isimli derneğin” kısmı “koyu” biçimde yazılmış olup Mahkememiz çoğunluğu buradan hareketle “Mahkeme kararında başvurusunun şahsıyla ilgili tespitler önplana çıkarılarak değerlendirme yapıl”dığına ve “başvurusunun babasıyla ilgili olguyu gerekçesinin dışında tuttuğu gözetildiğinde bu olguya ilgili olarak Anayasa Mahkemesinin bir değerlendirme yapmasına gerek bulunma”dığına karar vermiştir. Bu biçimdeki bir yorumlamayla ilk derece mahkemesi kararında gerekçe bulunduğunu kabul etmenin ve yine bu yaklaşımla başvurusunun babası ile ilgili bilgi notunda yer alanlara ilk derece mahkemesince dayanılmadığını söyleyebilmenin hukuken mümkün olmadığı açıktır. Mahkememiz çoğunluk gerekçesinde bu kanaate nasıl ulaştığı tatminkar bir biçimde açıklanamamıştır.

14. Nitekim Mahkememiz çoğunluğunun yaptığı ayırımın aksine Ankara 10. İdare Mahkemesi hükme ulaşırken karar gerekçesinde başvuru ile ilgili bilgi notunda yer alan tüm bilgileri kapsayacak bir biçimde “yukarıda ayrıntısına yer verilen bilgiler dikkate alındığında davacının güvenlik

soruşturmasının olumsuz değerlendirilerek atanmaması yolundaki davalı idare takdirinde hukuka aykırılık bulunmamıştır.” gerekçesiyle iptal istemini reddetmiştir. Görüldüğü üzere ilk derece mahkemesinin karar gerekçesinde Mahkememiz çoğunluğunun ifade ettiği biçimde “ön plana çıkararak değerlendirme yapma” şeklinde bir yaklaşım mevcut değildir.

15. İkincisi ve daha sorunlu olanı ise çoğunluk kararının 57. paragrafında yer alan ve yukarıya aynen aldığımız gerekçede göze çarpmaktadır. Anayasa Mahkemesi çoğunluğu bu gerekçesi ile somut başvuruya konu olayla ilgili olarak, normalde açılan iptal davasında İdare Mahkemesinin yapması gereken değerlendirmeyi kendisi yapmıştır. Bu bağlamda Anayasa Mahkemesi terör örgütü ile bağlantılı olduğu tespit edilen bir derneğin faaliyetlerine katılan başvurucu ile ilgili olarak bu hâle uyan bir kimsenin memuriyete alınmamasının bu kişi açısından öngörülebilir olduğuna yer vermiş ve yine aynı paragrafta kamu makamlarının soyut bilgiler içeren bir istihbarat raporundan hareket etmediğini, söz konusu raporda başvurucunun Derneğin faaliyetlerine katıldığına ilişkin somut tespitlerin yer aldığını belirtmiştir.

16. Oysa bu biçimdeki bir değerlendirmeye ne ilk derece mahkemesi kararında ne de istinafin onama kararında rastlamak mümkündür. Derece mahkemelerinin kararlarında yer verilmeyen bir gerekçeyi kendi kararıyla “ikame ederek” başvurucunun güvenlik soruşturmasının olumsuz olarak kabul edilmesinin keyfi ve temelsiz olmadığı ve bu nedenle başvurucunun iddialarının kanun yolu şikâyeti niteliğinde olduğu değerlendirmesi yapmasının bireysel başvuru incelemelerinde Anayasa Mahkemesinin yetkisi dahilinde olmadığını ifade etmek gerekir.

17. Çoğunluk kararındaki bu yaklaşım bireysel başvuru bağlamında Anayasa Mahkemesinin ve derece mahkemelerinin konumu göz önünde tutulduğunda sorunludur. Anayasa Mahkemesi adil yargılama hakkı kapsamındaki bir ihlal iddiası söz konusu olduğunda bir davanın esası ile ilgili olarak delilleri ilk elden ele alıp değerlendirme yapmamalıdır. Bu durum bireysel başvurunun “ikincil” niteliği ile de bağdaşmaz.

18. İşte tam da bununla bağlantılı olarak vurgulamak gerekir ki, başvurucunun iddiaları ile ilgili olarak derece mahkemelerinin kararlarına bakıldığında somut başvurunun, kanun yolu şikayeti olarak görülmesi mümkün değildir. Zira esasında ilk derece mahkemesi kararı, güvenlik soruşturmasında yer verilen bilgi notundaki başvurucu ve babası ile ilgili olan iki bilginin doğru olup olmadığından ve memuriyete başlatılmama biçimindeki işleme dayanak kabul edilip edilmemesinden bağımsız olarak, yargısal anlamda bir gerekçe içermemesi yönü ile sorunludur. Bu nedenle de burada gerekçeli karar hakkı ihlali söz konusudur.

19. Zira somut başvuruya konu idari işlemin dayanağı olan güvenlik soruşturmasındaki bilgi notu ile ilgili olarak ilk derece mahkemesin karar gerekçesinde yapılmış olan hiçbir değerlendirme mevcut değildir. Ankara 10. İdare Mahkemesi kararında ilk olarak ilgili mevzuat aktarılmış, ardından başvurucu hakkındaki güvenlik soruşturmasında yer verilen bilgi notuna aynen yer verilmiş, akabinde ise güvenlik soruşturması bilgi notunda başvurucunun babası ve kendisi ile ilgili olarak yukarıda da aynen yer verdiğimiz (§ 5) istihbari bilgiye atıfla “yukarıda ayrıntısına yer verilen bilgiler dikkate alındığında davacının güvenlik soruşturmasının olumsuz değerlendirilerek atanmaması yolundaki davalı idare takdirinde hukuka aykırılık bulunmamıştır.” şeklindeki formül ve kalıptan oluşan bir ifade ile işlemin iptal istemi reddedilmiştir. Karardaki bu ifadenin bir gerekçe olarak kabulü mümkün değildir. Zira bu ifadelerle ilk derece mahkemesi esasında sadece içeriğine yer verdiği güvenlik soruşturmasına referansla başvurucunun atanmaması biçimindeki idari işlemin hukuka aykırı olmadığına değinmektedir.

20. Oysa bu davada idari yargı mercilerince davanın esasının incelenmesi kapsamında başvurucunun kendisi ve babası ile ilgili olarak güvenlik soruşturması bilgi notunda yer verilen istihbari nitelikteki bilgilerle ilgili hukuki değerlendirmenin yapılmış olması ve başvurucunun güvenlik soruşturmasında yer verilen bilgilerden hareketle kamu hizmetine kabul edilip edilmemesi noktasında bu hususların mutlaka hukuken değerlendirilmesi gerekmektedir. Bununla birlikte derece mahkemesi kararında bu konuda hiçbir gerekçeye yer verilmediği, adeta güvenlik soruşturmasındaki hususlar peşinen doğru kabul edilerek hükme esas alınıp iptal isteminin reddedildiği görülmektedir.

21. Böyle bir durumda aslında bireysel başvuruya konu mahkeme kararında bir gerekçe olmadığı gerçeği ortaya çıktığından, sadece bu kadarlık bir inceleme ile birlikte bile kolaylıkla bu başvuruda gerekçeli karar hakkının asgari gerekleri karşılanmamış olmasından hareketle başvurucunun adil yargılanma hakkının ihlal edildiğine karar verilmesi gerekmektedir.

22. Nitekim Anayasa Mahkemesinin yerleşik içtihadında da belirtildiği üzere gerekçeli karar hakkı kişilerin adil bir şekilde yargılanmalarını sağlamayı ve denetlemeyi amaçlamaktadır. Gerekçeli karar, tarafların muhakeme sırasında ileri sürdükleri iddialarının kurallara uygun biçimde incelenip incelenmediğini bilmeleri ve ayrıca demokratik bir toplumda, kendi adlarına verilen yargı kararlarının sebeplerini toplumun öğrenmesinin sağlanması için de gereklidir (Sencer Başat ve diğerleri [GK], B. No: 2013/7800, 18/6/2014, §§ 31, 34; Kemal Turan, B. No: 2018/18194, 25/2/2021, § 37; Başkent Doğalgaz Dağıtım Gyo A.Ş., B. No: 2019/28520, 31/12/2020, § 23).

23. Esasında bu başvuruya konu ilk derece mahkemesi kararında davanın esasını çözen, idare mahkemesinin güvenlik soruşturmasındaki bilgi notlarını irdeleyip bunların gerçekliği, olgusal dayanakları, bu bilgilerin tesis edilen red işlemine ulaşmadaki hukuki etkisi ve benzeri boyutları ile işin esası ile ilgili kendi değerlendirmesini ortaya koyan bir cümlelik bir gerekçeye dahi rastlanılamamaktadır. Dolayısıyla öncelikle burada asgari düzeyde bir gerekçe olmaması yönüyle adil yargılanma hakkının ihlal edildiği ifade edilmelidir.

24. Oysa gerekçeli karar hakkı bağlamında Mahkememiz içtihadında mahkemelerin ileri sürülen iddia ve savunmalara şeklen cevap vermiş olmalarının yeterli olmadığı, iddia ve savunmalara verilen cevapların dayanaksız olmaması, mantıklı ve tutarlı olması ve makul bir gerekçeye dayanması gerektiği hususları da fevkalade önem arz etmektedir.

25. Anayasa Mahkemesine göre;

“Makul gerekçe, davaya konu olay ve olguların mahkemece nasıl nitelendirildiğini, kurulan hükmün hangi nedenlere ve hukuksal düzenlemelere dayandırıldığını ortaya koyacak, olay ve olgular ile hüküm arasındaki bağlantıyı gösterecek nitelikte olmalıdır (...). Gerekçelendirme, davanın sonucuna etkili olay, olgu ve argümanları açıklamak yükümlülüğü olmakla birlikte, bu şekildeki gerekçelendirmenin mutlaka detaylı olması şart değildir. Ancak gerekçelendirmenin, iddia ve savunmadan birinin diğerine üstün tutulma sebebinin ve bu kapsamda davanın taraflarınca gösterilen delillerden karara dayanak olarak alınanların mahkemelerce kabul edilme ve diğerlerinin reddedilmesi hususunda, makul dayanakları olan bir bilgilendirmeyi sağlayacak ölçü ve özene sahip olması gerekmektedir.

Zira bir davada tarafların, hukuk düzenince hangi nedenle haklı veya haksız görüldüklerini anlayıp değerlendirebilmeleri için usulüne uygun şekilde oluşturulmuş, hükmün içerik ve kapsamı ile bu hükme varılırken mahkemenin neleri dikkate aldığı ya da almadığını gösteren, ifadeleri özenle seçilmiş ve kuşkuya yer vermeyecek açıklıktaki bir gerekçe bölümünün ve buna uyumlu hüküm fıkralarının bulunması ‘gerekçeli karar hakkı’ yönünden zorunludur.

Aksi bir tutumla, mahkemenin, davanın sonucuna etkili olduğunu kabul ettiği bir husus hakkında “ilgili ve yeterli bir yanıt” vermemesi veya yanıt verilmesini gerektiren usul veya esasa dair iddiaların cevapsız bırakılmış olması bir hak ihlaline neden olabilecektir.” (Sencer Başat ve diğerleri [GK], B. No: 2013/7800, 18/6/2014, §§ 37-39).

26. Somut bireysel başvuruya konu olayda ise İdare Mahkemesi istihbarat raporlarından gelen bilgiyi hiçbir sorgulama, yorumlama ve değerlendirmeye tabi tutmadan adeta mutlak biçimde doğru kabul

ederek ona referansla davayı reddederken aslında bir mahkemenin davanın esası ile ilgili olarak yapması gereken minimum bir incelemeyi bile yapmamıştır. Dolayısıyla burada aslında bir gerekçe bile söz konusu olmadığından gerekçenin “ilgili ve yeterli” olup olmadığının değerlendirilebileceği aşamaya bile geçmek mümkün gözükmemektedir.

27. Öte yandan derece mahkemelerince hiçbir yorumlamaya tabi tutulmaksızın güvenlik soruşturmasında yer verilenlere bu biçimde peşinen üstünlük tanınmasının hukuk devletinde yargının konumu ve insan hakları açısından fevkalade sorunlu bir yaklaşım ortaya çıkarmış olması ise ayrı ve ciddi bir sorundur.

28. Nitekim Anayasa Mahkemesi'nin yakın zamanda verdiği bir kararında terör örgütlerine iltisakı yahut bunlarla irtibatı olduğu Emniyet Genel Müdürlüğü tarafından bildirilen gerçek ve tüzel kişiler ile bu kapsamda olduğu Millî İstihbarat Teşkilatı Müsteşarlığı tarafından bildirilen yurt dışı bağlantılı gerçek ve tüzel kişilerin doğrudan veya dolaylı veya alt yüklenici olarak, kendileri veya başkaları adına hiçbir şekilde kamu ihalelerine katılamayacaklarını öngören kuralı iptal ettiğini hatırlatmak gerekir.

29. Bu kararda Anayasa Mahkemesi, terör örgütleri ile irtibat veya iltisakı tespit edilenlerin kamu ihalelerine katılmamasını öngören kuralın millî güvenlik amacı ile öngörüldüğü ve anayasal anlamda meşru bir amaç taşıdığına söylenebileceğini, bu amaca yönelik olarak kanun koyucu tarafından idari önlemler öngörülebileceğinin açık olduğunu ve bu çerçevede millî güvenliğin sağlanması amacıyla kuralda öngörülen sınırlamaların elverişli ve gerekli olmadığını söylenemeyeceğini belirtmesine rağmen (E. S.:2018/90, K. S.:2019/85, K. T.:14/11/2019, §§ 40-46) idarenin bu önlemler bakımından sınırsız bir yetkiye sahip olamayacağına işaret etmiş ve kuralın terör örgütleriyle iltisaklı yahut irtibatlı olma bakımından Emniyet Genel Müdürlüğü ve Millî İstihbarat Teşkilatı tarafından yapılan bildirim esas olarak kişilerin otomatik olarak kamu ihalelerine katılmaması veya ihale dışı bırakılması sonucunu doğurmasının da çalışma ve sözleşme hürriyetine ne derece ölçsüz bir müdahale olduğuna ilişkin şu gerekçeye yer vermiştir:

“Emniyet Genel Müdürlüğü ve Millî İstihbarat Teşkilatı tarafından yapılan bildirim kural olarak ceza soruşturmasına esas alınabilecek nitelikte bilgi ve belgelere dayanma zorunluluğu bulunmamaktadır. Diğer bir ifadeyle bu kapsamdaki değerlendirmeye esas alınan olay ve olguların istihbarî nitelikte olması kuvvetle muhtemeldir. Bu nedenle kamu ihalelerini gerçekleştiren idarelerce tesis edilecek işlemlerle ilgili yargısal denetim daha da önemli hâle gelmektedir. Ceza soruşturmasına esas alınabilecek nitelikte bilgi ve belgelere dayanma zorunluluğu olmayan güvenlik kurumlarınca yapılacak değerlendirmenin otomatik sonuç doğurması ile idarelere ve idari işlemi denetleyecek

mahkemelere gerçek ve tüzel kişilerin terör örgütleriyle iltisakı yahut irtibatı bulunup bulunmadığı hususunda değerlendirme yapma yetkisinin verilmemesi, söz konusu bildirimlerin doğruluğunu denetleme ve gerçek duruma göre idari işlem tesis etme imkânını önemli ölçüde sınırlamaktadır. Kanun'da anılan yetkinin kuralın getiriliş amacına uygun olarak kullanılmasını sağlayacak ve bu konudaki olası keyfilikleri önleyecek yasal güvencelere de yer verilmediği görülmektedir.

Belirli bir süreyle sınırlı olmayan ve kamu ihalelerini yapan idareler ile bu işlemleri denetleyecek mahkemelere kural olarak değerlendirme yapma imkânı vermeyen düzenlemenin yukarıda belirtilen sonuçları dikkate alındığında çalışma ve sözleşme hürriyetine yönelik orantısız bir sınırlama getirdiği sonucuna varılmıştır" (§§ 47-48).

30. Elbette ki güvenlik soruşturmasındaki bir istihbari raporu esas alan idari işlemle bir kişinin kamu hizmetine kabul edilmediği durumlarda bir idare mahkemesi istihbari raporda yer alan bilgiye binaen bu kişinin terör örgütü ile olan bağlantısını tespit ettiğinde anayasal düzene sadakat şartının sağlanmaması gerekçesine dayalı olarak tesis edilen idari işlemin iptali talebini reddetmelidir. Ancak somut başvuruda İdare Mahkemesi hiçbir şekilde başvuru ile ilgili güvenlik soruşturmasındaki bilgiler bağlamında bir değerlendirme yapmamıştır. Başka bir şekilde ifade etmek gerekirse İdare Mahkemesi bu istihbari bilgileri değerlendirme aşamasına bile geçememiştir. Oysa derece mahkemesinden bu başvuruda başvuruçunun OHAL KHK'si ile kapatılan Kürdi-Der'deki hangi eylemi ile terör faaliyetleri içerisinde olduğu hususu ile ilgili değerlendirme yapması ve yine başvuruçunun babasının durumunun -eğer hukuken mümkün görülebiliyorsa- kamu hizmetine giriş sürecinde başvuruçuyu nasıl etkilediğine ilişkin değerlendirmelere yer vermesi beklenirdi.

31. Dolayısıyla somut başvuru bağlamında ifade etmek gerekir ki uyuşmazlığın esasına ilişkin hususları hukuken hiçbir şekilde temellendirmeden, istihbari nitelikteki güvenlik soruşturmasında yer verilen kayıtlara referansla geçiştirerek derece mahkemeleri davayı sonuçlandırıyorlarsa aslında bu durumda fiziksel olarak bir gerekçe var gibi görünüyorsa da bu biçimdeki bir metnin hukuken gerekçe olarak kabulü mümkün değildir. Böyle bir durumda Anayasa'nın "Bütün mahkemelerin her türlü kararları gerekçeli olarak yazılır" (1982 Anayasası, madde: 141/3) şeklindeki hükmünün asgari gerekliliği dahi karşılanmamış olmaktadır.

32. Sonuç olarak; yukarıda sıralanan gerekçelerle, adil yargılanma hakkının ihlal edildiğine ilişkin iddianın açıkça dayanaktan yoksun olması nedeniyle başvurunun kabul edilemez olduğuna karar verilmesi gerektiği şeklindeki Mahkememiz çoğunluğunun ulaştığı kanaate, başvuruçunun gerekçeli karar hakkının ihlal edildiğine ilişkin iddiasının kabul edilebilir olduğuna ve Anayasa'nın 36.

maddesinde güvence altına alınan adil yargılanma hakkı kapsamında gerekçeli karar hakkının ihlal edildiğine karar verilmesi gerektiği gerekçesiyle katılmamaktayız.

Üye

Hicabi DURSUN

Üye

Celal Mümtaz AKINCI

Üye

Yusuf Şevki HAKYEMEZ

KARŞIOY GEREKÇESİ

Güvenlik soruşturması ve arşiv araştırmasının olumsuz sonuçlanması sebebiyle atamanın yapılmaması işleminin iptali için açılan davada adil yargılanma hakkının ihlal edildiği iddiasına ilişkin başvurunun açıkça dayanaktan yoksun olduğu gerekçesiyle kabul edilemez olduğuna karar verilmiştir.

Kararın gerekçesinde; adil yargılanma hakkına ilişkin genel ilkeler tekrarlandıktan sonra, işlemin dayanağı olan kanun hükmünün iptal edilmesinin, yürürlükte olduğu dönemdeki uygulamalarla ilgili olarak açılan davalarda dikkate alınmasından dolayı adil yargılanma hakkının zedelenmesi sonucunu doğurmayacağı, ayrıca bu hakkın uyuşmazlıkta uygulanacak kuralın içeriği itibariyle değil, uygulanma şekli bakımından adil olmasını teminat altına aldığı, anılan hükmün başvuruya konu kararın gerekçesinden anlaşılan yorumunun keyfi olmadığı, güvenlik soruşturmasında yapılan tespitlerin bir kısmı başvuruçunun babasıyla ilgili olsa da ilk derece mahkemesinin bu olgulara dayanmadığı, başvuruçunun kendisine ilişkin tespitlere karşı itirazlarını ileri sürme imkânını bulmasına rağmen bunların bir bölümüne açık bir itirazda bulunmadığının da dikkate alınması gerektiği, dolayısıyla başvuruçunun güvenlik soruşturmasının olumsuz olarak kabul edilmesinin keyfi ve temelsiz olmadığı, bu itibarla iddiaların kanun yolu şikâyeti niteliğinde olduğu belirtilerek açıkça dayanaktan yoksun olduğu sonucuna varılmıştır.

Kuşkusuz kamu görevine alınacak olanlar için güvenlik soruşturması ve arşiv araştırması yapılması mümkündür. Anayasaya ve kanunlara göre memurların ve diğer kamu görevlilerinin devlete sadakat yükümlülüğü bulunduğundan, bu statüye girmek isteyen kişiler hakkında da güvenlik soruşturması ve arşiv araştırması yapılmasında Anayasaya aykırılık bulunmamaktadır. Mahkememiz de hiçbir

kararında bunun aksine hükmetmemiş; 657 sayılı Kanununun 48. maddesinin birinci fıkrasının (A) bendinin memurluğa girişte güvenlik soruşturması ve arşiv araştırması yapılması şartını getiren (8) numaralı alt bendini kişisel verilerin korunması hakkı yönünden yeterli güvenceleri içermediği gerekçesiyle iptal ettiği (bendin Anayasaya aykırı olmadığı ve davanın reddedilmesi gerektiği yönünde karşıoy kullandığım) yakın tarihli kararında da bu hususun kanun koyucunun takdir yetkisinde olduğunu belirtmiştir (24/7/2019 tarihli ve E. 2018/73, K.2019/65 sayılı karar, § 170).

Kararda da vurgulandığı üzere, bu kapsamda ilgililerin devlete sadakat yükümlülüğüne uyacağından şüpheye düşülmesi hâlinde güvenlik soruşturmasının olumsuz sonuçlanması da keyfi bir değerlendirme olarak kabul edilemez. Dolayısıyla Mahkememiz çoğunluğunun kabul edilemezlik kararının gerekçesinde bu konuda yapılan değerlendirmeler isabetli olmakla birlikte, yine gerekçede belirtildiği üzere güvenlik soruşturmasında kişi ile ilgili olarak aktarılan kuşkuların kişisel değerlendirme ve kanaatlere değil, somut ve maddî tespitlere dayanması ve bu tespitlerin derece mahkemelerince incelenerek değerlendirilmesi gerektiğinden, çoğunluğun derece mahkemelerinin gerekçelerine ilişkin değerlendirmelerine ve ulaştığı sonuca katılmak mümkün değildir.

Bilindiği gibi yargılamanın adil bir şekilde gerçekleştirilmesini ve bunun denetlenmesini hedefleyen gerekçeli karar hakkı, yargılama sırasında ileri sürülen iddiaların gereği gibi incelenip incelenmediğinin görülmesi ve varılan sonucun sebeplerinin öğrenilmesi bakımından büyük önem taşımakta; ancak mahkeme kararlarının gerekçeli olma zorunluluğu, yargılama sırasında ileri sürülen her iddianın ayrıntılı bir şekilde karşılanması gerektiği şeklinde anlaşılacağından, bunun kapsamı davanın ve verilen kararın niteliğine göre değişebilmektedir (Sencer Başat ve diğerleri [GK], B. No: 2013/7800, 18/6/2014, §§ 31, 34; Mehmet Yavuz, B. No: 2013/2995, 20/2/2014. § 51).

Diğer taraftan, mahkemeler bütün iddiaları kararın gerekçesinde ayrıntılı olarak karşılamak zorunda olmasalar da, yargılama sırasında açık ve somut bir şekilde belirtilen iddia ve savunmaların davanın sonucunu değiştirebilecek nitelikte bulunması hâlinde bu hususların mahkemelerce makul bir gerekçe ile karşılanması ve ihtilafın çözümünde esas olacak bütün bu hususların incelenmiş olduğunun gerekçeli karardan anlaşılması gerekmektedir. Buna göre, davanın sonucuna etkili olduğu kabul edilen bir hususta ilgili ve yeterli bir cevap verilmemesi hak ihlaline sebep olabilecektir (Sencer Başat ve diğerleri, §§ 35, 39).

Makul, yani ilgili ve yeterli gerekçe ise; davaya konu olay ve olguların mahkemece nasıl nitelendirildiğini, kurulan hükmün hangi sebeplere ve hukukî düzenlemelere dayandırıldığını ortaya koyacak, olay ve olgular ile hüküm arasındaki bağlantıyı gösterecek nitelikte olmalıdır (İbrahim Ataş, B. No: 2013/1235, 18/6/2013, § 24).

İlk derece mahkemesinin kararında ilgili ve yeterli bir gerekçe bulunması hâlinde, kanun yolu incelemesi yapan mercii yargılamayı yapan mahkeme ile aynı sonuca ulaşarak bunu aynı gerekçeyi kullanmak suretiyle veya atfla kararına yansıtması gerekçeli karar hakkı bakımından yeterli bulunmakla birlikte (Yasemin Ekşi, B. No: 2013/5486, 4/12/2013, §§ 56, 57), ilk derece mahkemesinin kararında bu nitelikte bir gerekçe bulunmayan hâllerde başvurunun itirazlarının itiraz mercii tarafından gerekçeli bir şekilde karşılanması gerekir.

Somut olayda, KPSS sonucu esas alınarak bir kuruma yerleştirilen başvurucuya, güvenlik soruşturması ve arşiv araştırmasının olumsuz sonuçlanması sebebiyle atamasının yapılmadığı bildirmiş ve başvurunun bu işleme karşı açtığı iptal davası idare mahkemesince reddedilmiştir.

İlk derece mahkemesinin kararı incelendiğinde, davacının (başvurucunun) hakkında yapılan inceleme ve araştırma sonucunda, kuruluşunda görev alarak öğretmenlik de yaptığı bir derneğin ilgili KHK hükmüyle kapatılan dernekler arasında bulunduğu, babasının da silahlı terör örgütüne üye olma suçundan yargılamasının devam ettiği ve taksirli yaralamadan dolayı bir polis merkezinde babası hakkında işlem yapıldığı şeklindeki bilgi notu ile kanun ve KHK hükümlerinin aynen aktarılarak “Komisyon kararı ile güvenlik soruşturması olumsuz değerlendirilerek atamasının yapılmaması üzerine bakılan davanın açıldığı”nın belirtildiği, devamında da yine anılan mevzuat hükümleri ile 667 sayılı KHK'nın amacı ve mahiyeti dikkate alındığında davalı idarenin takdirinde hukuka aykırılık bulunmaması nedeniyle davanın reddine karar verildiği anlaşılmıştır.

Başka bir anlatımla, ilk derece mahkemesinin kararında, davacının, hakkındaki güvenlik soruşturması ve arşiv araştırmasında belirtilen hususların gerçeği yansıtmadığı yönündeki iddiaları incelenerek gerekçede karşılanmamış; sadece ilgili mevzuat hükümleri ile davacı hakkındaki bilgi notunun aktarılmasıyla yetinilerek, dava konusu işlemde hukuka aykırılık bulunmadığı sonucuna ulaşılmıştır.

İlk derece mahkemesinde ileri sürdüğü iddiaları tekrarlayarak istinaf yoluna müracaat eden başvurunun bu talebi de bölge idare mahkemesince “...İdare Mahkemesince verilen karar usul ve hukuka uygun olup kaldırılmasını gerektiren bir neden bulunmadığı...” denilerek reddedilmiş; böylece başvurunun itirazları kanun yolu mercii tarafından da gerekçeli bir şekilde karşılanmamıştır.

Mahkememiz çoğunluğunun kabul edilemezlik kararının gerekçesinde, başvurunun güvenlik soruşturmasında yapılan tespitlerin bir kısmına açık bir itirazda bulunmadığı belirtilmekte ise de, başvurunun olumsuz sonuçlanan güvenlik soruşturması ve arşiv araştırmasındaki tespitlerin hiçbirini kabul etmediği, dava ve istinaf dilekçeleri ile başvuru formunda bu tespitlerin tamamını

aktararak bunların doğru olmadığını savunduğu ve başvuru formunda özellikle “herhangi bir dernek üyeliği[nin] dahi bulunma[dığını]”, aksinin “belgeleriyle birlikte ortaya konulması”nın mümkün olacağını, ancak böyle bir şey olmadığı için istihbarî bilgiden öteye gidilemediğini, “buna rağmen idarî yargı mercilerince yeterli araştırma yapılmadan” iptal davasının reddedildiğini belirttiği görülmektedir.

Kaldı ki re’sen tahkik ilkesinin geçerli olduğu idarî yargılama usulünde -tarafarca yeterince ayrıntılı bir şekilde ifade edilemese bile- derece mahkemelerinin kararlarına esas alınan diğer hususlar gibi, somut olaydaki güvenlik soruşturması ve arşiv araştırması sonucunda hazırlanan bilgi notundaki açıklamaların doğru olup olmadığının belirlenmesine çalışılması, hiç olmazsa bu hususların incelenmiş olduğunun gerekçeli karardan anlaşılması gerekmektedir.

Somut olayda ise, davacının (başvurucunun) açık itirazlarına rağmen ilk derece mahkemesinin red gerekçesinde mevzuatın ve bilgi notunun bir değerlendirme yapılmadan aynen aktarılmasıyla yetinildiği ve Mahkememiz çoğunluğunun gerekçesinde belirtilenin aksine, başvurucunun babasıyla ilgili bilgilerin de -kendisiyle ilgili bilgiler gibi- bir değerlendirme yapılmadan aktarılacak davanın reddine gerekçe yapıldığı anlaşılmaktadır.

Sonuç olarak, somut olayla ilgili yargılamada başvurucunun davanın sonucuna etkili olabilecek iddialarının tartışılmadığı ve karşılanmadığı, kararda mevzuat hükümlerinin ve başvuru hakkındaki bilgi notunun aynen aktarılmasıyla yetinildiği, bu itibarla yukarıda belirtilen ilkelere uygun şekilde hükme ulaşılması için ilgili ve yeterli gerekçe bulunmadığı, istinaf incelemesinde de bu noksanlığın telafi edilmediği, bu sebeplerle Anayasanın 36. maddesinde teminat alınan adil yargılanma hakkı kapsamındaki gerekçeli karar hakkının ihlal edildiğine ilişkin başvurunun kabul edilebilir olduğuna karar verilerek esas incelemesi yapılması ve ihlal kararı verilmesi gerektiği düşüncesiyle çoğunluğun kabul edilemezlik kararına katılmıyorum.

Üye

M. Emin KUZ

Anayasa Mahkemesi - Celal Oraj Altunörgü Kararı (2018/31036)

Celal Oraj Altunörgü, B. No: 2018/31036, 12/1/2021

Başvuru, özel bir bankada çalışan başvuruçunun kurumsal e-posta hesabı içeriğinin işveren tarafından incelenmesi ve bu yazışmalar gerekçe gösterilerek iş akdinin feshedilmesi nedeniyle özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyetinin ihlal edildiği iddialarına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

BİRİNCİ BÖLÜM

KARAR

CELAL ORAJ ALTUNÖRGÜ BAŞVURUSU

(Başvuru Numarası: 2018/31036)

Karar Tarihi: 12/1/2021

R.G. Tarih ve Sayı: 5/2/2021-31386

BİRİNCİ BÖLÜM

KARAR

Başkan: Hasan Tahsin GÖKCAN

Üyeler: Hicabi DURSUN, Muammer TOPAL, Recai AKYEL, Yusuf Şevki HAKYEMEZ

Raportör: Ali KOZAN

Başvurucu: Celal Oraj ALTUNÖRGÜ

Vekili: Av. Galip UZUN

I. BAŞVURUNUN KONUSU

1. Başvuru, özel bir bankada çalışan başvuruçunun kurumsal e-posta hesabı içeriğinin işveren tarafından incelenmesi ve bu yazışmalar gerekçe gösterilerek iş akdinin feshedilmesi nedeniyle özel

hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyetinin ihlal edildiği iddialarına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 3/10/2018 tarihinde yapılmıştır.

3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.

4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.

5. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık görüş bildirmemiştir.

III. OLAY VE OLGULAR

6. Başvuru formu ve eklerinde ifade edildiği ve Ulusal Yargı Ağı Sistemi (UYAP) üzerinden yapılan incelemeyle elde edilen bilgi ve belgelere göre olaylar özetle şöyledir:

A. Uyuşmazlığın Arka Planı

7. Başvurucu, özel bir bankada 14/5/2007 tarihli belirsiz süreli iş sözleşmesi kapsamında müşteri ilişkileri yönetmeni olarak çalışmaktadır. İş Sözleşmesi'nin "Özenle çalışma" kenar başlıklı bölümünde özetle personelin görevini banka yönetmelikleri ve iç düzenlemeler ile yönetim yetkisi kapsamında verilen emir ve talimatlara bağlı olarak özen ve dikkatle yerine getireceği, personelin verimliliğinin bankanın yürürlükte olan performans kriterlerine göre belirleneceği düzenlenmiştir. Ayrıca İş Sözleşmesi'nde ayrıntıları belirtilen özenle çalışma yükümlülüklerine uyulmaması hâlinin 22/5/2003 tarihli ve 4857 İş Kanunu'nun 17. maddesi kapsamında geçerli neden olarak kabul edileceğinin personel tarafından kabul edildiği ifade edilmiştir.

8. İş Sözleşmesi'nin "Demirbaş ve elektronik posta kullanımı" kenar başlıklı 6. maddesinin (c) bendinde, personelin banka mülkiyetinde olan elektronik posta adresini (kurumsal e-posta) sadece iş amaçlı olarak kullanmakla yükümlü olduğu belirtilmiştir. Aynı maddenin (d) bendinde ise kurumsal e-postanın banka yönetimi tarafından haber verilmeksizin denetlenebileceği, personelin bu konuda itirazının olmayacağı ve talimatlara uyacağını kabul ettiği şeklinde düzenleme yapıldığı görülmüştür.

9. Başvurucunun, eşi üstüne kayıtlı bir işletmede çalıştığı iddiası üzerine müfettiş incelemesi yapılmış ve başvurucunun konuyla ilgili savunması alınmıştır. Müfettiş incelemesi sonucunda 7/4/2016 tarihli rapor düzenlenmiştir. Raporda; başvurucunun eşi adına 1/4/2014 tarihinde bir şirket kurulduğu,

başvurucunun bu şirketin muhasebecisine kurumsal e-posta üzerinden ödemelere ilişkin çeşitli belgeler gönderdiği, başvurucunun kurumsal e-posta üzerinden başka bankalarla anılan şirkete ilişkin kredi pazarlığı yaparak kredi başvurusunda bulunduğu, işyerinin stokunda bulunan ürünlerle ilgili bazı belgeleri kişisel e-posta hesabından kurumsal e-posta hesabına gönderdiği ve eşinin hesabının sıkça görüntülediği hususlarının tespit edildiği belirtilmiştir.

10. İnceleme raporunda başvurucunun 30/3/2016 tarihinde alınan savunması da değerlendirilmiştir. Başvurucu savunmasında; eşiyile açtıkları işyerini zarara uğramaması için kendi gözetiminde tuttuğunu, ödeme stokun takibi gibi işlerde eşine yardımcı olduğunu, bu durumun zaman zaman iş performansını biraz olsa da etkilediğini ifade etmiştir. Başvurucu ayrıca kurumsal e-posta kullanılarak yapılan yazışmaların nedeninin işyerine ait faaliyetlerin düzene sokulması ve işyeri banka faaliyetlerinin kontrolü olduğunu, bunu sağlamak için eşinin hesabını da sıkça kontrol ettiğini, amacının işyerini zarar etmeden devretmek olduğunu beyan etmiştir. Rapor sonucunda, mesai saatleri içinde performansı etkileyecek şekilde eşine ait işyerinin çeşitli işlemlerini takip ettiği hususlarının tespit edilmesi ve bu şekilde ticari faaliyette bulunduğu dair kanıt niteliği taşıyan beyanları birlikte gözetildiğinde başvurucunun banka çalışma ilkelerine aykırı olarak kendi namına ve hesabına ticari faaliyette bulunduğu kanaatine ulaşıldığı ifade edilmiştir.

11. Başvurucunun iş akdi 11/5/2016 tarihli yazılı bildirimle feshedilmiştir. Anılan bildirimde; başvurucunun göreviyle bağdaşmayacak ve banka kurallarına aykırı şekilde eşine ait işletme üzerinden mesai saatleri içinde ticari faaliyette bulunduğu, başvurucunun bu nedenle asli görevini ihmal ettiği, şube içinde olumsuzluklara sebebiyet verdiği hususlarının başvurucunun ikrarı ve müfettiş raporuyla tespit edildiği vurgulanmıştır. Görev ve sorumluluklarla bağdaşmayan, banka kurallarına aykırı bu davranışların kabul edilemeyeceği belirtilerek iş akdinin 4857 sayılı Kanununun 17. ve 18. maddeleri uyarınca feshedildiği ifade edilmiştir.

B. İşe İade Davası Süreci

12. Başvurucu, işveren aleyhine Amasya İş Mahkemesinde 8/6/2016 tarihinde işe iade istemli tespit davası açmıştır. Dava dilekçesinde başvurucu özetle feshin haksız olduğunu, işverenin daha önce de performans eksikliği gerekçesiyle kendisinden savunma aldığını ve iş akdinin tazminatsız feshedilmesi amacıyla bahane üretildiğini ileri sürmüştür. Başvurucu çalışma hayatı boyunca işverene sadakat yükümlülüğüne aykırı ve görevini olumsuz etkileyecek davranışının olmadığını vurgulamıştır. Başvurucu ayrıca yargılama sürecindeki beyanlarda, kurumsal e-posta hesabının işveren tarafından incelenmesinin özel hayatın gizliliğini ihlal ettiğini ve hukuka aykırı olması nedeniyle hükme esas alınmaması gerektiğini belirtmiştir.

13. İşveren davaya cevabında özetle müfettiş raporundaki tespitlere ve başvurucunun ikrar içeren savunmasına dayanarak başvurucunun mesai saatleri içinde eşine ait şirketin işlerini takip ettiğini, bu durumun başvurucunun performansında kayba neden olduğunu vurgulamıştır. Ayrıca iş sözleşmesi ve işyeri etik kurallarına göre başvurucunun başka bir işte çalışmayacağına dair düzenlemeler olduğu hatırlatıldıktan sonra başvurucunun davranışlarının İş Sözleşmesi'nde ayrıntılı bir şekilde belirtilen çalışanın yükümlülüklerine bu bağlamda özellikle özen yükümlülüğüne aykırı olduğu belirtilmiştir.

14. Yargılama sürecinde tarafların tanıkları dinlenmiştir. Başvurucunun tanıkları özetle başvurucunun başka bir yerde çalıştığı ve performans düşüklüğü yaşadığını görmediklerini ancak eşinin adına bir ayakkabı dükkânının mevcut olduğunu ifade etmişlerdir. Davalı tanıkları ise özetle başvurucunun mesai saatlerinde ticari faaliyetleri takip ettiğine birkaç kez şahit olduklarını, ayrıca son dört beş aydır performans düşüklüğü yaşadığını bildiklerini beyan etmişlerdir.

15. Mahkeme 27/12/2017 tarihinde davanın reddine karar vermiştir. Kararın gerekçesinde; tanık beyanları, başvurucunun savunması, dosyaya sunulan belgeler ile e-posta içerikleri değerlendirilerek eşine ait ticari işletmenin işlerini başvurucunun takip ettiğinin sabit olduğu, bu durumun başvuru tarafından da kabul edildiği belirtilmiştir. Ayrıca davacının e-posta kayıtlarından mesai saatleri içinde ticari faaliyet takibi amacıyla yazışmalar yaptığının anlaşıldığı ifade edilmiştir. Başvurucunun görevi dışında ticari faaliyet ile ilgilendiğini kabul ettiği, dosyaya sunulan kayıtların davacının mesai saatleri içinde ticari faaliyetine ilişkin iş ve işlemleri yaptığını doğruladığı ve bu durumun performansına olumsuz etki ettiğinin başvuru tarafından da beyan edildiği vurgulanmıştır. Başvurucunun özel işleri ile işini sektöre uğratabilecek kadar ilgilenmesinin İş Sözleşmesi'nin gereklerine aykırılık teşkil edeceği, doğruluk ve bağlılık kuralı gereği işçinin gelir getirici başkaca işlerle mesai saatleri içinde ilgilenmesi ile iş ilişkisinin sarsıldığı ve işverenden iş ilişkisini sürdürmesinin beklenemeyeceği belirtilerek feshin geçerli nedene dayandığı değerlendirilmesine yer verilmiştir.

16. Başvurucu vekili; ikrar içeren yazılı savunmasının baskı ile alındığını, ayrıca Avrupa İnsan Hakları Mahkemesinin (AİHM) işverenin e-posta incelemesini özel hayata saygı hakkının ihlali saydığını, müvekkilinin de e-postasının incelenmesinin bu kapsamda olduğunu belirterek istinaf başvurusu yapmıştır. Samsun Bölge Adliye Mahkemesi 7. Hukuk Dairesi 17/7/2018 tarihinde delillerin takdirinde isabetsizlik görülmediği ve davalı işverenin geçerli nedeni ispatladığının anlaşıldığı gerekçesiyle istinaf itirazlarının reddine kesin olmak üzere karar vermiştir.

17. Nihai karar 4/9/2018 tarihinde başvurucuya tebliğ edilmiştir.

18. Başvurucu 3/10/2018 tarihinde bireysel başvuruda bulunmuştur.

IV. İLGİLİ HUKUK

19. İlgili hukuk (ulusal mevzuat, uluslararası düzenlemeler ve AİHM kararları) için bkz. E.Ü. [GK], B. No: 2016/13010, 17/9/2020, §§ 22-51.

20. 4857 sayılı Kanunun "Feshin geçerli sebeplere dayandırılması" kenar başlıklı 18. maddesi şöyledir:

"Otuz veya daha fazla işçi çalıştıran işyerlerinde en az altı aylık kıdemi olan işçinin belirsiz süreli iş sözleşmesini fesheden işveren, işçinin yeterliliğinden veya davranışlarından ya da işletmenin, işyerinin veya işin gereklerinden kaynaklanan geçerli bir sebebe dayanmak zorundadır. (Ek cümle: 10/9/2014-6552/2 md.) Yer altı işlerinde çalışan işçilerde kıdem şartı aranmaz.

Altı aylık kıdem hesabında bu Kanunun 66 ncı maddesindeki süreler dikkate alınır.

Özellikle aşağıdaki hususlar fesih için geçerli bir sebep oluşturmaz:

- a) Sendika üyeliği veya çalışma saatleri dışında veya işverenin rızası ile çalışma saatleri içinde sendikal faaliyetlere katılmak.
- b) İşyeri sendika temsilciliği yapmak.
- c) Mevzuattan veya sözleşmeden doğan haklarını takip veya yükümlülüklerini yerine getirmek için işveren aleyhine idari veya adli makamlara başvurmak veya bu hususta başlatılmış sürece katılmak.
- d) Irk, renk, cinsiyet, medeni hal, aile yükümlülükleri, hamilelik, doğum, din, siyasi görüş ve benzeri nedenler.
- e) 74 üncü maddede öngörülen ve kadın işçilerin çalıştırılmasının yasak olduğu sürelerde işe gelmemek.
- f) Hastalık veya kaza nedeniyle 25 inci maddenin (I) numaralı bendinin (b) alt bendinde öngörülen bekleme süresinde işe geçici devamsızlık.

İşçinin altı aylık kıdemi, aynı işverenin bir veya değişik işyerlerinde geçen süreler birleştirilerek hesap edilir. İşverenin aynı işkolunda birden fazla işyerinin bulunması halinde, işyerinde çalışan işçi sayısı, bu işyerlerinde çalışan toplam işçi sayısına göre belirlenir."

V. İNCELEME VE GEREKÇE

21. Mahkemenin 12/1/2021 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları

22. Başvurucu; kurumsal e-posta hesapları ile gerçekleştirdiği yazışmaların bilgilendirme yapılmadan ve rızası alınmadan incelendiğini, bu yazışmalara dayanılarak performans düşüklüğü nedeniyle iş

akdinin haksız olarak feshedildiğini belirtmiştir. İş performansının her zaman üst düzeyde olduğunu, ayrıca yazılı savunmasının iş akdini sonlandırmak amacıyla banka müfettişlerinin baskısı ve psikolojik tacizi ile alındığını ileri sürmüştür. Eşinin işyeri ve kendisinin e-posta kayıtlarının iş akdinin feshini sağlamaya yönelik bahaneler olduğunu, Bankanın e-posta içeriklerini incelemesi ve Mahkemenin bu içerikleri hükme esas delil olarak kabul etmesi sonucu özel hayatına saygı hakkı ile haberleşme hürriyetinin ihlal edildiğini ileri sürmüştür.

B. Değerlendirme

23. Anayasa'nın iddianın değerlendirilmesinde dayanak alınacak "Özel hayatın gizliliği" kenar başlıklı 20. maddesinin birinci ve üçüncü fıkrası şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

...

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

24. Anayasa'nın "Haberleşme hürriyeti" kenar başlıklı 22. maddesi şöyledir:

"Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.

İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir."

25. Özel hayata saygı hakkı Anayasa'nın 20. maddesinde koruma altına alınmıştır. Devlet, kişilerin özel ve aile hayatına keyfî olarak müdahale etmemek ve üçüncü kişilerin haksız saldırılarını önlemekle yükümlüdür. Anayasa'nın 20. maddesinin üçüncü fıkrasında ise herkesin kendisiyle ilgili

kişisel verilerin korunmasını isteme hakkı ayrıca düzenlenmiş ve güvence altına alınmıştır. Söz konusu anayasal güvence, Sözleşme'nin 8. maddesinde koruma altına alınan özel hayata saygı hakkına karşılık gelmektedir. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır (AYM, E.2014/122, K.2015/123, 30/12/2015, §§ 19, 20).

26. Anayasa Mahkemesi kararlarında da belirtildiği üzere kişisel veri -belirli veya kimliği belirlenebilir olmak şartıyla- bir kişiye ilişkin bütün bilgileri ifade etmekte olup bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi sadece kimliğini ortaya koyan bilgileri değil telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, öz geçmişi, resmi, görüntü ve ses kayıtları, parmak izleri, sağlık bilgileri, genetik bilgileri, IP adresi, e-posta adresi, alışveriş alışkanlıkları, hobileri, tercihleri, etkileşimde bulunduğu kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır (AYM, E.2014/74, K.2014/201, 25/12/2014; E.2014/180, K.2015/30, 19/3/2015).

27. Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı yönünden inceleme yapılabilmesi için öncelikle anılan hak kapsamında korunması gereken bir kişisel verinin olup olmadığı belirlenmelidir. Anayasa hükmünün lafzı, konuya ilişkin uluslararası belgeler ve karşılaştırmalı hukuk dikkate alındığında belirli veya belirlenebilir bir gerçek veya tüzel kişi hakkındaki her türlü bilgi kişisel veri olarak değerlendirilir. Ancak her davada ya da başvuruda Anayasa'nın 20. maddesinin üçüncü fıkrası anlamında bir kişisel veri bulunup bulunmadığı, davanın ve başvurunun kendine özgü koşulları dikkate alınarak tespit edilir. Bir kişisel verinin bulunduğu tespit edildiğinde bu veriye yönelik her türlü sınırlama ve müdahale Anayasa'nın anılan hükmü kapsamındaki güvenceleri harekete geçirir (E.Ü., § 59).

28. Ayrıca Anayasa'nın 22. maddesinde güvence altına alınan haberleşme hürriyeti, haberleşmenin yanında içeriği ve biçimi ne olursa olsun haberleşmenin içeriğinin gizliliğini de güvence altına almaktadır. Haberleşme bağlamında bireylerin karşılıklı ve toplu olarak sözlü, yazılı ve görsel iletişimlerine konu olan ifadelerinin gizliliğinin sağlanması ve haberleşmeye yönelik haksız müdahalelerde bulunulmaması gerekir (Yasemin Çongar ve diğerleri, B. No: 2013/7054, 6/1/2015, § 49).

29. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Somut olayda işverenin başvuru sahibinin kurumsal e-posta hesabını kullanarak yaptığı

mesajlaşmalarını denetlemesi ve içeriğini geriye dönük olarak incelemesi sonucu elde ettiği bilgileri, iş akdinin feshine dayanak yapması söz konusudur. Bu durumla birlikte başvuruçunun e-posta bilgileri ve yazışmalarının belirli bir gerçek kişi hakkındaki bilgi kapsamında olduğu gözetildiğinde bu bilgilere erişilmesinin, bunların kullanılmasının ve işlenmesinin özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyeti yönünden incelenmesi gerektiği değerlendirilmiştir.

1. Kabul Edilebilirlik Yönünden

30. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

2. Esas Yönünden

a. Genel İlkeler

31. Anayasa'nın 12. ve 5. maddesindeki düzenlemeler ışığında devletin bireyin temel hak ve özgürlüklerine keyfi olarak müdahale etmemesinin yanında üçüncü kişilerin saldırılarını önlemekle yükümlü kılındığı, bu bağlamda pozitif yükümlülüklerinin de bulunduğu söylenebilir. Uyuşmazlıkların özel hukuk kişileri arasında gerçekleştiği durumlarda da temel hak ve özgürlüklerin sağladığı güvencelerin yerine getirilip getirilmediği denetlenirken Anayasa'nın kamusal makamlara yüklediği sorumluluklardan doğrudan özel hukuk kişileri sorumlu tutulamayacağı için taşıdığı koşulların özelliklerine göre bu tür başvuruların devletin pozitif yükümlülükleri bağlamında ele alınması gerekebilir.(Ömür Kara ve Onursal Özbek, B.No: 2013/4825, 24/3/2016, § 46; Ali Çığır, B. No: 2015/19298, 8/5/2019, §§ 32, 33; Erol Kumcu, B. No: 2015/18988, 9/5/2019, §§ 32, 33; U.B., B. No: 2015/3175, 10/10/2019, §§ 33, 34; E.Ü., § 65).

32. Pozitif yükümlülükler özel hukuk kişilerinin birbirleri ile olan uyuşmazlıklarının çözümüne ilişkin yasal altyapının oluşturulmasını, söz konusu uyuşmazlıkların adil yargılama gereklerine uygun ve usul yönünden güvenceleri haiz bir yargılama kapsamında incelenmesini ve bu yargılamalarda temel haklara ilişkin anayasal güvencelerin gözetilip gözetilmediğinin denetlenmesini gerektirir. Bu doğrultuda derece mahkemelerince söz konusu güvenceler gözardı edilmemeli, işveren ve çalışanlar arasındaki çatışan çıkarlar adil biçimde dengelenmeli, başvuruların temel haklarına yönelik müdahalenin meşru amaca dayalı ve ölçülü olup olmadığı değerlendirilmeli,

ulařılan sonuç hakkında hkm kurulurken ilgili ve yeterli gerekeler sunulmalıdır (mr Kara ve Onursal zbek, řř 47-50; E.., ř 66).

33. Yukarıda belirtilen hususlar gzetilerek iřverenin iřinin iletiřimini denetlemesi yetkisini kiřisel verilerin korunmasını isteme hakkı ve haberleřme hrriyeti baęlamında devletin pozitif ykmllkleri kapsamında irdellemek gerekmektedir. ncelikle teknolojik geliřmelerin imknlarından yararlanmak isteyen iřverenlerin bilgisayar, internet, e-posta gibi iletiřim ara ve gerelerini alıřanın kullanıma sunması nedeniyle oluřan uyuřmazlıklarda iřverenin menfaatleri ile iřinin temel hak ve zgrlkleri arasında bir dengeleme yapma gereklilięi doęmaktadır. Bu baęlamda iřveren ile alıřan arasındaki iliřkinin iki taraf aısından da belirli hak ve ykmllkler ngren ve esasen gven iliřkisi zerine kurulu iř szleřmesiyle řekillendięi unutulmamalıdır. Somut uyuřmazlıęın ilgili olduęu iř hukukunun dinamik bir nitelięinin olduęu, ayrıca iř iliřkilerinin genel kurallardan farklı, kendine zg bazı hukuki kurallar ierdięi de dikkate alınmalıdır (E.., ř 68).

34. Bu baęlamda iřlerin etkin bir řekilde yrtlmesi ile bilgi akıřının kontroln saęlamak, iřinin eylemlerine baęlı cezai ve hukuki sorumluluęa karřı korunmak, verimlilięi lmek veya gvenlik endiřeleri gibi haklı ve meřru grlebilecek nedenlerle iřverenin ynetim yetkisi kapsamında kural olarak iřinin kullanımına sunduęu iletiřim aralarını denetleyebileceęi ve kullanıma iliřkin sınırlamalar ngrebileceęi sylenebilir. Ancak iřverenin ynetim yetkisinin iřyerinde iřin yrtlmesi, iřyerinin dzeninin ve gvenlięinin saęlanmasıyla sınırlı olduęu unutulmamalıdır. Bu baęlamda iřverenin yetki ve haklarının sınırsız olmadıęı, alıřana tanınan temel hak ve zgrlklerin somut olayda haberleřme hrriyeti ve kiřisel verilerin korunmasını isteme hakkının iřyeri sınırları dhilinde de korunduęu, aynı zamanda kısıtlayıcı ve uyulması zorunlu iřyeri kurallarının alıřanların temel haklarının zn zedeleyecek nitelikte olmaması gerektięi vurgulanmalıdır. Bu erevede iřyerinde kullanıma sunulan iletiřim aralarının iřverene ait olduęu gzetilerek sırf bu nedenle bile iřverenin iletiřim araları zerinde sınırsız ve mutlak bir gzetleme ve denetleme yetkisinin olduęunu kabul etmek, iřinin demokratik bir toplumda temel hak ve zgrlklerine iřyerinde de saygı gsterilmesi gerektięi ynndeki haklı beklentisiyle uyuřmayacaktır (E.., ř 69).

35. Tm bu aıklamalar erevesinde devletin pozitif ykmllkleri kapsamında Anayasa Mahkemesinin zellikle derece mahkemelerinin -somut olayın kořullarına uygun dřtę lde-ařaęıda belirtilen gvencelerin somut olayda hakka mdahale eden cnc kiři tarafından saęlanıp saęlanmadıęını gereęi gibi denetleyip denetlemedięini incelemesi gerekir:

i. Iřverenin alıřanın kullanımına sunduęu iletiřim aralarının ve iletiřim ieriklerinin incelenmesinin haklı olduęunu gsteren meřru gerekeleri olup olmadıęı denetlenmelidir. Bu durumda iřverenin

gerekçelerinin ifa edilen işin ve işyerinin özellikleri de gözetilerek meşru olup olmadığı irdelenmelidir. Bu denetlemede iletişim akışı ile iletişim içeriklerinin incelenmesi arasında ayırım yapılarak içeriklerin incelenmesi yönünden daha ciddi gerekçeler aranmalıdır.

ii. Demokratik bir toplumda iletişimin denetlenmesi ve kişisel verilerin işlenmesi süreci şeffaf bir şekilde gerçekleştirilmeli ve bunun bir gereği olarak da süreçle ilgili olarak çalışanlar işveren tarafından önceden bilgilendirilmelidir. Uluslararası hukuk ve karşılaştırmalı hukuk dikkate alındığında bu bilgilendirmenin -somut olayın özelliklerine uygun düştüğü ölçüde- en azından iletişimin denetlenmesi ile kişisel verilerin işlenmesinin hukuki dayanağı ve amaçları, denetlemenin ve veri işlemenin kapsamı, verilerin saklanacağı süre, veri sahibinin hakları, denetlemenin ve işlemenin sonuçları ile verilerin muhtemel yararlanıcıları hususlarını kapsamaması gerekir. Ayrıca bildirimde iletişim araçlarının kullanımına ilişkin olarak işveren tarafından öngörülen sınırlamalara da yer verilmelidir. Bilgilendirmenin mutlaka belli şekilde yapılması şart olmayıp şeffaflığı sağlamak bakımından bireylere, kişisel verilerin işlenmesine ve iletişimin denetlenmesine ilişkin süreçten yukarıda belirtilen kapsamda haberdar olma imkânı sağlayan uygun bir yöntem tercih edilebilir.

iii. Çalışanın kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine işveren tarafından yapılan müdahale, ulaşılmak istenen amaç ile ilgili ve bu amacı gerçekleştirmeye elverişli olmalıdır. Ayrıca inceleme faaliyetiyle elde edilen verilerin işveren tarafından hedeflenen amaç doğrultusunda kullanılması gerekir.

iv. İşveren tarafından çalışanın kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine işveren tarafından yapılan müdahalenin gerekli kabul edilebilmesi için aynı amaca daha hafif bir müdahale ile ulaşılmaması mümkün olmamalı, müdahale ulaşılmak istenen amaç bakımından zorunlu olmalıdır. Çalışanın iletişiminin içeriğine girilmesi yerine onun kişisel verilerine daha az müdahale eden yöntem ve tedbirlerin uygulanmasının mümkün olup olmadığı denetlenmelidir. Bu kapsamda işverenin ulaşmak istediği amaca çalışanın iletişimi incelenmeden de erişilme imkânı olup olmadığı her bir vakıanın somut özellikleri ışığında değerlendirilmelidir.

v. İşveren tarafından başvuruçunun kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine yönelik müdahalenin orantılı kabul edilebilmesi için ise iletişimin denetlenmesi ile işlenecek veya herhangi bir şekilde yararlanılacak veriler ulaşılmak istenen amaçla sınırlı olmalı, bu amacı aşacak şekilde sınırlama ya da müdahaleye izin verilmemelidir.

vi. Ayrıca iletişimin incelenmesinin muhatabı olan çalışan üzerindeki etkisi ve çalışan bakımından sonuçları gözönünde tutularak tarafların çatışan menfaat ve haklarının adil bir biçimde dengelenip dengelenmediğine bakılması gerekmektedir. Taraflardan birine şahsi olarak aşırı bir külfet

yüklendiğinin tespiti hâlinde devletin pozitif yükümlülüklerini yerine getirmediği sonucuna varılabilir (E.Ü., § 70).

b. İlkelerin Uygulanması

36. Başvurucu; e-posta hesabının incelenmesinin özel hayat alanına ve haberleşme hürriyetine haksız bir müdahale oluşturmasına rağmen açtığı işe iade davasında bu yönde bir tespit yapılmadığını, mahkemelerce verilen kararlar nedeniyle söz konusu müdahalelerin meşru hâle getirildiğini iddia etmiştir. Bu kapsamdaki iddiaların yukarıda belirtilen esaslar gözetilerek değerlendirilmesi gerekmektedir.

37. Öncelikle işverenin işçinin kullanımına sunulan iletişim araçlarını denetlemesi ve çalışanın kişisel verilerinin işlemesine ilişkin olarak 4857 sayılı Kanun'da özel bir düzenleme olmadığı görülmüştür. Ancak Anayasa'nın 20. ve 22. maddelerinde yer bulan özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyetine ilişkin güvenceler ile 6698 sayılı Kanun ve hukuk sistemimizde mevcut olan genel düzenlemelerin iş hukuku uyumsuzluklarında uygulanması yönünde bir engel olmadığı anlaşılmıştır. Bu durumda yasal altyapı oluşturmak bağlamında pozitif yükümlülüklerin yerine getirilmiş olduğu söylenebilir (E.Ü., § 69).

38. Başvuru konusu olayda başvurucu, çok sayıda çalışanı istihdam eden özel bir bankanın çalışanıdır. Başvurucu adına tanımlanmış kurumsal e-posta hesabının mevcut olduğu ve başvurucunun kullanımına sunulan bu e-posta hesabının işveren tarafından incelendiği hususlarında başvuran ile işveren arasında bir ihtilaf olmadığı görülmüştür. Çok sayıda çalışanı olduğu ve kurumsal olarak finans hizmeti verdiği anlaşılan işverenin çalışanlarına kurumsal e-posta hesabı oluşturmak suretiyle kişisel verileri işlemesinin ve iletişim akışını denetim altında tutmasının işlerin etkin bir şekilde yürütülmesini sağlama amacına yönelik olduğu anlaşılmaktadır. Bu durumda kurumsal e-posta hesabının iletişim akışına ve içeriğine erişilecek şekilde kullanıma sunulmasının somut olayda işyerinin yönetimi bakımından meşru bir menfaat teşkil ettiği, ayrıca hedeflenen amacı sağlamaya elverişli bir yöntem olduğu söylenebilir.

39. Öte yandan e-posta hesabı üzerinden yapılan iletişimin denetlenebileceğine ve iletişim araçlarının kullanım koşullarına ilişkin olarak önceden tam ve açık bir bilgilendirme yapılmadığı hâllerde temel hak ve özgürlüklerinin işyerinde de korunacağı yönündeki haklı beklentiyle çalışan kişinin kurumsal e-posta üzerinden kişisel yazışmalar yapabileceğinin işveren tarafından da öngörülebilecek bir durum olduğu vurgulanmalıdır. Buradan hareketle çalışana açık bir bilgilendirmenin yapılmadığı hâllerde hak ve özgürlüklerine bir müdahalede bulunulmayacağı hususunda çalışanların makul bir

beklenti içinde olacaklarının kabul edilmesi, temel hak ve özgürlüklerin sağladığı güvencelerden yararlandırılması gerektiği söylenebilir (E.Ü., § 75).

40. Bununla birlikte açık bir bilgilendirme yapılması hâlinde işverenin kurumsal e-postayı incelemeden önce çalışanın ayrıca rızasını alması beklenemez. Bu bağlamda bilgilendirme sonrası işverenin denetleme yetkisine ilişkin bir itiraz şerh edilmediği sürece çalışanın rızasının mevcut olduğu ve aksi kanıtlanana kadar da bu rızanın geçerli olduğunun kabulü gerektiği vurgulanmalıdır.

41. Somut olayda başvuru bilgilendirme yapılmadan ve rızası olmadan kurumsal e-posta hesabının incelediğini ileri sürmüştür. Başvurucunun bağlı olduğu iş akdi incelendiğinde (bkz. §§ 7, 8) başvurucuya tahsis edilen kurumsal e-postanın sadece iş amaçlı olarak kullanılacağı ve kurumsal e-postanın banka yönetimi tarafından haber verilmeksizin denetlenebileceğinin, personelin bu konuda itirazının olmayacağı ve talimatlara uyacağı hususlarının düzenlendiği görülmüştür. Ayrıca iş sözleşmesinde çalışan için belirlenen yükümlülükler -kurumsal e-postanın amacına uygun kullanılması, performans düşüklüğü tespiti, başka işte çalışma yasağı- uyulmaması durumunda iş akdinin feshedilebileceğinin açıkça düzenlendiği anlaşılmaktadır.

42. Bu durumda işverenin iş sözleşmesinde, kurumsal e-postanın kullanımına ilişkin sınırları, e-postanın denetlenme usulü ve inceleme yetkisini, işçinin işini yürütürken ve e-postayı kullanırken uyması gereken yükümlülükleri ile belirlenen yükümlülükler uyulmaması durumunda 4857 sayılı Kanun çerçevesinde nasıl yaptırım uygulanacağını belirlediği söylenebilir. Bu durum gözetildiğinde başvurucunun kullanımına sunulan kurumsal e-postanın denetlenebileceği ve denetimin usulüne ilişkin önceden İş Sözleşmesi'yle açıkça bildirim yapıldığı, ayrıca İş Sözleşmesi'nde belirlenen denetleme usulü ve yetkisine başvurucunun İş Sözleşmesi'ni imzalayarak rıza gösterdiği kabul edilmelidir. Ayrıca başvurucunun bu rızanın geçerli olmadığına dair bir iddiası ya da açıklaması olmadığı görülmüştür.

43. Öte yandan somut olayda işverenin yaptığı müdahalenin kapsamının tartışılması gerekir. Bu bağlamda yargılama kapsamında başvurucunun işveren tarafından sunulan yazışmaları ve yargılama süreci bir bütün hâlinde değerlendirildiğinde işverenin başvurucunun başka bir işte çalıştığı iddiasını destekleyen mesajları incelediği ve iddiasını kanıtlamak amacıyla sadece yargı sürecinde kullandığı görülmüştür. Bu durumda işverenin inceleme amacı dâhilinde bir denetleme gerçekleştirdiği, inceleme sonucu elde edilen verileri amaca uygun kullandığı söylenebilir. Ayrıca işverenin kurumsal e-postayı inceleme amacına uygun olmayacak şekil ve kapsamda incelediği ve denetleme sonuçlarının amaca uygun kullanılmadığı yönünde başvurucunun bir iddiasının bulunmadığı vurgulanmalıdır.

44. Bununla birlikte yargılama süreci incelendiğinde; Mahkemenin sadece kurumsal e-postanın incelenmesi ile elde edilen bilgi ve belgelere değil tanık anlatımları, iş sözleşmesi, işyeri dosyası ve dosyaya sunulan diğer belgeleri de değerlendirerek bir sonuca ulaştığı, ilgili ve yeterli gerekçe sunduğu görülmüştür. Ayrıca bir vekille temsil edilen başvuruçunun yargılama sürecine etkin olarak katılımının sağlandığı anlaşılmaktadır.

45. Açıklanan gerekçelerle özel hukuk iş ilişkilerinden doğan uyuşmazlığı karara bağlayan derece mahkemeleri tarafından pozitif yükümlülüklerin yerine getirildiği anlaşıldığından başvuruçunun Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkı ile Anayasa'nın 22. maddesinde güvence altına alınan haberleşme hürriyetinin ihlal edilmediğine karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ihlal edildiğine ilişkin iddianın **KABUL EDİLEBİLİR OLDUĞUNA,**

B. Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkı ve Anayasa'nın 22. maddesinde güvence altına alınan haberleşme hürriyetinin **İHLAL EDİLMEDİĞİNE,**

C. Yargılama giderlerinin başvuruçucu üzerinde **BIRAKILMASINA,**

D. Kararın bir örneğinin Adalet Bakanlığına **GÖNDERİLMESİNE** 12/1/2021 tarihinde **OYBİRLİĞİYLE** karar verildi.

Anayasa Mahkemesi - Bestami Erođlu Kararı (2018/23077)

Bestami Erođlu [GK], B. No: 2018/23077, 17/9/2020

Başvuru, tutuklama tedbirinin hukuki olmaması nedeniyle kişi hürriyeti ve güvenliği hakkının, ByLock haberleşmesi ve kişisel verilerin yasal olmayan şekilde elde edilmesi nedeniyle özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ve geçmişteki ByLock kullanımı dolayısıyla cezalandırılma nedeniyle de suç ve cezaların kanuniliđi ilkesinin ihlal edildiđi iddialarına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

GENEL KURUL

KARAR

BESTAMİ EROĐLU BAŞVURUSU

(Başvuru Numarası: 2018/23077)

Karar Tarihi: 17/9/2020

R.G. Tarih ve Sayı: 13/10/2020-31273

GENEL KURUL

KARAR

Başkan: Zühtü ARSLAN

Başkanvekili: Hasan Tahsin GÖKCAN

Başkanvekili: Kadir ÖZKAYA

Üyeler: Serdar ÖZGÜLDÜR, Burhan ÜSTÜN, Engin YILDIRIM, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĐLU, Selahaddin MENTEŞ, Basri BAĞCI

Raportörler: Şermin BİRTANE, Ayhan KILIÇ

Başvurucu: Bestami EROĐLU

Vekili: Av. Metin POLAT

I. BAŞVURUNUN KONUSU

1. Başvuru; tutuklama tedbirinin hukuki olmaması nedeniyle kişi hürriyeti ve güvenliği hakkının, ByLock haberleşmesi ve kişisel verilerin yasal olmayan şekilde elde edilmesi nedeniyle özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ve geçmişteki ByLock kullanımı dolayısıyla cezalandırılma nedeniyle de suç ve cezaların kanuniliği ilkesinin ihlal edildiği iddialarına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 26/7/2018 tarihinde yapılmıştır.

3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.

4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.

5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.

6. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık görüş bildirmiştir.

7. Başvurucu, Bakanlık görüşüne karşı beyanda bulunmamıştır.

8. İkinci Bölüm tarafından 9/9/2020 tarihinde yapılan toplantıda, niteliği itibarıyla Genel Kurul tarafından karara bağlanması gerekli görüldüğünden başvurunun Anayasa Mahkemesi İçtüzüğü'nün (İçtüzük) 28. maddesinin (3) numaralı fıkrası uyarınca Genel Kurula sevkine karar verilmiştir.

III. OLAY VE OLGULAR

9. Başvuru formu ve eklerinde ifade edildiği şekliyle ilgili olaylar özetle şöyledir:

10. Başvurucu 1978 doğumlu olup inceleme tarihi itibarıyla Kayseri 1 No.lu T Tipi Kapalı Ceza İnfaz Kurumunda hükümlü olarak bulunmaktadır. Başvurucu, bireysel başvuruya konu olayların geçtiği tarihte öğretmen olarak görev yapmaktadır. Başvurucu, terör örgütleriyle veya Millî Güvenlik Kurulunca devletin millî güvenliğine karşı faaliyette bulunduğu karar verilen yapı, oluşum veya

gruplarla irtibatı olduğu gerekçesiyle 15/8/2016 tarihli ve 672 sayılı Olağanüstü Hal Kapsamında Alınan Tedbirlere İlişkin Kanun Hükmünde Kararname ile kamu görevinden çıkarılmıştır.

A. Genel Bilgiler

11. Türkiye 15 Temmuz 2016 tarihinde askerî bir darbe teşebbüsüyle karşı karşıya kalmış, bu nedenle 21/7/2016 tarihinde ülke genelinde olağanüstü hâl ilan edilmesine karar verilmiş ve olağanüstü hâl 19/7/2018 tarihinde -yeniden uzatılmayarak- son bulmuştur. Kamu makamları ve yargı organları -olgusal temellere dayanarak- bu teşebbüsün arkasında Fetullahçı Terör Örgütü/Paralel Devlet Yapılanmasının (FETÖ/PDY) olduğunu değerlendirmiştir (darbe teşebbüsü ve arkasındaki yapılanmaya ilişkin ayrıntılı bilgi için bkz. Aydın Yavuz ve diğerleri [GK], B. No: 2016/22169, 20/6/2017, §§ 12-25). Darbe teşebbüsü sırasında ve sonrasında ülke genelinde darbe girişimiyle bağlantılı ya da doğrudan darbe girişimiyle bağlantılı olmasa bile FETÖ/PDY'nin kamu kurumlarındaki örgütlenmesinin yanı sıra eğitim, sağlık, ticaret, sivil toplum ve medya gibi farklı alanlardaki yapılanmasına yönelik olarak Cumhuriyet başsavcılıkları tarafından soruşturmalar yürütülmüş; çok sayıda kişi hakkında gözaltı ve tutuklama tedbirleri uygulanmıştır (Aydın Yavuz ve diğerleri, § 51; Mehmet Hasan Altan (2) [GK], B. No: 2016/23672, 11/1/2018, § 12).

12. Yargı organları birçok kararda FETÖ/PDY'nin devletin anayasal kurumlarını ele geçirmeyi, sonrasında devleti, toplumu ve fertleri kendi ideolojisi doğrultusunda yeniden şekillendirmeyi, oligarşik özellikler taşıyan bir zümre eliyle ekonomiyi, toplumsal ve siyasi gücü yönetmeyi amaçlayan, bu doğrultuda mevcut idari sisteme paralel şekilde örgütlenen bir terör örgütü olduğunu kabul etmiştir. Yargı organları kararlarında ayrıca FETÖ/PDY'nin gizlilik, hücre tipi yapılanma, her kurumda örgütlenmiş olma, kendisine kutsallık atfetme, itaat ve teslimiyet temelinde hareket etme gibi birçok özelliğinin bulunduğunu, bu örgütün diğerlerine nazaran çok daha zor ve karmaşık bir yapı olduğunu ortaya koymuştur (FETÖ/PDY'nin genel özellikleri için bkz. Aydın Yavuz ve diğerleri, § 26; yargı organlarındaki örgütlenme biçimi için bkz. Selçuk Özdemir [GK], B. No: 2016/49158, 26/7/2017, § 22; Alparslan Altan [GK], B. No: 2016/15586, 11/1/2018, § 11).

13. Örgütlenme şekli olarak gizliliği esas alan FETÖ/PDY'nin üyelerine telkin ettiği yöntemler, istihbarata karşı koyma olarak nitelendirilebilecek düzeyde güvenlik önlemleridir. Bu bağlamda FETÖ/PDY'nin kurucusu ve lideri olan Fetullah Gülen'in örgüt mensuplarına "Hizmet bir namaz ise tedbir onun abdestidir. Tedbirsiz hizmet abdestsiz namaz gibidir." şeklinde talimat verdiği ifade edilmiştir. Gizliliği sağlamak üzere örgüt tarafından başvurulan yöntemler arasında -diğer pek çok terör örgütünde olduğu üzere- kod adı kullanmak da yer almaktadır. Soruşturma ve kovuşturma makamlarının tespitlerine göre FETÖ/PDY'nin deşifre olmamak için bir tedbir olarak iletişimde

başvurduğu temel yöntem yüz yüze görüşme, bunun mümkün olmadığı durumlarda ise kripto programlar üzerinden iletişimidir. Örgüt liderinin "Telefonla görüşme yapanlar hizmete ihanet etmiş olur." şeklindeki talimatı nedeniyle telefonla olağan usulde örgütsel görüşme yapılması yasaktır (bu konuda detaylı bilgi için bkz. Yargıtay 9. Ceza Dairesinin -ilk derece mahkemesi sıfatıyla- 28/3/2019 tarihli ve E.2018/12, K.2019/45 sayılı kararı). Bu nedenle örgütsel iletişimde kullanılmak üzere güçlü kriptolu programlar geliştirilmiştir (Ferhat Kara [GK], B. No: 2018/15231, 4/6/2020, § 22).

B. ByLock Programına İlişkin Açıklamalar

14. FETÖ/PDY'nin örgütsel haberleşme için oluşturduğu ve örgüt mensuplarınca kullanılan iletişim yöntemlerinden birinin ByLock uygulaması olduğu özellikle darbe teşebbüsünden sonra örgütle bağlantılı soruşturma ve kovuşturmalarda tespit edilmiştir (Ferhat Kara, § 23). ByLock haberleşme programıyla ilgili kavramsal açıklamalara, programın tespiti, adli makamlara ulaştırılması ve adli sürece, yüklenmesine ve iletişimde kullanılmasına, genel ve örgütsel özelliklerine, yaygın uygulamalardan ayrılan yönlerine, ByLock verilerinin niteliği, anlamlandırılması ve kişilerle eşleştirilmesine ilişkin arka plan bilgisinin detaylarına Ferhat Kara kararında yer verilmiştir (Ferhat Kara, §§ 23-67).

C. ByLock Programının Tespiti, Adli Makamlara Ulaştırılması ve Adli Süreç

15. Millî İstihbarat Teşkilatı (MİT) tarafından 1/1/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu'nun 4. ve 6. maddeleri uyarınca yürütülen çalışmalar kapsamında ana sunucusu yurt dışında bulunan ByLock (ByLock: Chat and Talk) adlı bir mobil uygulama ve bu uygulamanın iletişim kurduğu sunucular ayrıntılı teknik çalışmalara tabi tutulmuştur. MİT'e özgü teknik istihbarat usul, araç ve yöntemleri kullanılmak suretiyle yapılan bu çalışma sonucunda, FETÖ/PDY'nin kullandığı değerlendirilen bu programla ilgili olarak birtakım veriler elde edilmiştir (Ferhat Kara, § 25).

16. MİT, ByLock programıyla ilgili olarak temin edilen dijital verileri içeren sabit diski ve uygulamaya bağlantı sağlayan ByLock abone listesinin bulunduğu flash bellek ile düzenlediği ByLock Uygulaması Teknik Raporu'nu Ankara Cumhuriyet Başsavcılığına teslim etmiştir (Ferhat Kara, § 26)

17. Bunun akabinde Ankara Cumhuriyet Başsavcılığı, Ankara 4. Sulh Ceza Hâkimliğinden söz konusu (dijital) materyal üzerinde 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu'nun 134. maddesi uyarınca inceleme, kopyalama, çözümlene işlemi yapılmasına karar verilmesi talebinde bulunmuştur. İlgili yazıda; anılan madde gereğince bir adet Sony marka HD-B1 model, üzerinde BBW3DEK69121056 seri numaralı ve ön yüzünde 1173d7a09195cf0274ce24f0d69ede96 yazılı hard disk

ve bir adet Kingston marka data traveler, uç kısmında DTIG4/8GB 04570-700.A00LF5V 0S7455704 yazılı flash bellek üzerinde inceleme yapılmasına, iki kopya çıkarılmasına ve kopya üzerindeki kayıtların çözümlenerek metin hâline getirilmesine karar verilmesi istenmiştir (Ferhat Kara, § 27).

18. Ankara 4. Sulh Ceza Hâkimliği tarafından 5271 sayılı Kanun'un 134. maddesi uyarınca talep kabul edilmiş ve "dijital materyaller üzerinde inceleme yapılması, kopya çıkarılması ve kopya üzerinde bilirkişi incelemesi yapılarak metin haline getirilmesi için bir kopyasının Ankara Cumhuriyet Başsavcılığına gönderilmesine" karar verilmiştir. Anılan karar doğrultusunda görevlendirilen iki uzman bilirkişi tarafından hâkim huzurunda kamera kaydı da yapılmak suretiyle söz konusu hard disk ve flash bellek üzerinde imaj alma-kopyalama işlemi yapılmıştır (Ferhat Kara, § 28).

19. Ankara Cumhuriyet Başsavcılığınca Emniyet Genel Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığına (EGM-KOM Daire Başkanlığı) gönderilen bir yazıyla Ankara 4. Sulh Ceza Hâkimliğince verilen inceleme, kopyalama ve çözümleme kararına istinaden gerekli araştırma ve soruşturma işlemlerinin yapılması, ulaşılan tespitleri içerir bir rapor düzenlenmesi talimatı verilmiştir (Ferhat Kara, § 29).

20. EGM-KOM Daire Başkanlığınca teslim alınan verilerin (ByLock verilerini içeren hard disk ve abone listesinin bulunduğu flash bellek) incelenmesi ve rapor hazırlanması amacıyla EGM-KOM, Terörle Mücadele (TEM), İstihbarat ve Siber Suçlarla Mücadele Daire Başkanlıkları tarafından görevlendirilen personelden oluşan bir çalışma grubu oluşturulmuştur. Bu kapsamda ByLock verilerinin dışarı aktarılması için arayüz programı kullanılmış ve bu sayede ByLock verileri incelenmeye başlanmıştır (Ferhat Kara, § 30).

21. Bu arada Yargıtay 16. Ceza Dairesince yürütülen bir yargılamaya esas olmak üzere EGM-KOM Daire Başkanlığından ByLock'un teknik özelliklerine dair bilgi istenmiştir. EGM-KOM Daire Başkanlığı tarafından bir rapor hazırlanarak anılan Daireye gönderilmiştir. Söz konusu raporda; ByLock iletişim sisteminin mahiyeti ve diğer özellikleri hakkında ayrıntılı bilgiler verildikten sonra anılan uygulamadaki kullanıcı sayısı, arkadaş grubu, mesaj ve e-posta içeriklerine dair açıklamalarda bulunulmuştur (Ferhat Kara, § 31).

22. Sonraki süreçte Ankara Cumhuriyet Başsavcılığı tarafından ByLock IP adreslerine bağlandığı belirtilenlere ilişkin listede yer alan abonelerin ByLock IP adreslerine kaç defa bağlandığına dair raporlar (CGNAT verileri) Bilgi Teknolojileri ve İletişim Kurumundan (BTK) talep edilmiştir (Ferhat Kara, § 32).

23. Bu arada MİT tarafından detaylı çalışma yapılarak güncellenen abone listesinin yeni hâli tekrar Ankara Cumhuriyet Başsavcılığına gönderilmiştir. Başsavcılığın talebi üzerine Ankara 5. Sulh Ceza Hâkimliğince MİT tarafından gönderilen data traveler G4 marka, DTİG4/8GB 04570-760B00LF 5V 0S 7575458 seri numaralı TAIWAN ibaresi bulunan dijital materyal üzerinde 5271 sayılı Kanun'un 134. maddesi gereğince inceleme yapılmasına, kopya çıkarılmasına (imaj alma), bu kayıtların çözümlenerek metin hâline getirilmesine karar verilmiştir. Bu karar doğrultusunda söz konusu materyalin imaj alma (kopyalama) işlemi Cumhuriyet savcısı ve görevlendirilen iki adli bilişim görevlisinin huzurunda video kamera eşliğinde gerçekleştirilmiştir (Ferhat Kara, § 33).

24. Sonrasında Ankara Cumhuriyet Başsavcılığı tarafından abone listesi BTK'ya bildirilmiş ve ByLock sunucusuna bağlanan güncellenmiş numaraların abonelerine ait şahıs kimlik bilgilerinin tespiti için BTK'dan bilgi istenmiştir (Ferhat Kara, § 34).

25. Bağlantı yapılan GSM numaralarına ait abonelik bilgileri ve ADSL numaralarına ait abonelik bilgileri de farklı tarihlerde BTK'dan alınarak Ankara Cumhuriyet Başsavcılığına iletilmiştir. Devamında KOM Daire Başkanlığınca Ankara Cumhuriyet Başsavcılığından teslim alınan abonelik bilgilerinden yararlanılarak yeni "user ID_list" (kullanıcı listesi) tablosu oluşturulmuştur (Ferhat Kara, § 35).

26. Ankara Cumhuriyet Başsavcılığınca EGM-KOM Daire Başkanlığına verilen talimat üzerine BTK tarafından gönderilen 123.111 GSM numarasına ait CGNAT verilerinin (ByLock sunucusuna ait IP adreslerine hangi tarihte kaç defa bağlanıldığı bilgisi) -il Cumhuriyet başsavcılıklarına gönderilmek üzere- il KOM birimlerine dağıtılmasına başlanmıştır. VPN programı kullanılarak yapılan bağlantıların Türkiye IP'si almaması sebebiyle gerçekte ByLock kullanıcısı olan kişilerin VPN programı kullanarak ByLock sunucusunun IP'lerine yaptıkları bağlantılara dair CGNAT kayıtlarına erişilememiştir. CGNAT kayıtlarına ulaşılanlar, ByLock sunucusuna ait hedef IP'lerine Türkiye IP'lerinden VPN kullanmaksızın yapılan ya da Türkiye'den VPN ile bağlantı devam ederken VPN'nin devre dışı kalması sonucunda yeniden Türkiye IP'si alınması nedeniyle tespit edilebilen bağlantılara aittir (Ferhat Kara, § 36).

27. Bu arada internet üzerinde yayımlanan Morbeyin isimli adres ve uygulamaları kullananların arka plandaki kodlar vasıtasıyla doğrudan ByLock IP'sine bağlandıklarına ve ByLock dökümü bulunmayan (gerçekte ByLock kullanıcısı olmayan) bazı kişilerin haksız yere cezalandırıldığına dair kamuoyunda paylaşılan iddia ve haberlerle ilgili olarak Ankara Cumhuriyet Başsavcılığı tarafından soruşturma başlatılmış ve bu kapsamda Siber Suçlarla Mücadele Daire Başkanlığı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) ve BTK görevlilerinden oluşan inceleme grubu

oluşturulmuştur. Başsavcılığın yaptığı soruşturmada FETÖ/PDY'nin ileride delil olması ihtimaline karşı gerçek ByLock kullanıcılarının açığa çıkmasını önlemek, ilgisiz kişileri bu programa yönlendirmek ve bu suretle delilin güvenilirlik derecesini düşürmek amacıyla 2014 yılında Morbeyin isimli bir yazılım yaptırdığı, kullanıcının kible pusulası, namaz vakti, dua dinleme, Kur'an okuma ve çeşitli sözlük uygulamalarına girmesi hâlinde bu programın tesiriyle bilgisi ve iradesi dışında cihazının bir iki saniye kadar ByLock sunucusunun IP'lerine bağlandığının görüldüğü tespit edilmiştir. Bu konuda gerçekleştirilen detaylı inceleme neticesinde bağlantı ve veri parametreleri bakımından benzer özellikler taşıyan 11.480 GSM numarasının kullanıcısının iradeleri dışında ByLock sunucusu IP'lerine yönlendirilmiş olduğu belirlenmiştir. Bunlar listelerden çıkarılmıştır (Ferhat Kara, § 37).

D. Başvurucuya İlişkin Süreç

28. Kayseri Cumhuriyet Başsavcılığı (Başsavcılık) tarafından başvurucunun da aralarında bulunduğu Millî Eğitim Bakanlığı personeli hakkında FETÖ/PDY'ye üye olma suçunu işledikleri isnadıyla soruşturma başlatılmıştır.

29. Soruşturma kapsamında Başsavcılığın 5/9/2016 tarihli talebi üzerine Kayseri 3. Sulh Ceza Hâkimliğince 5271 sayılı Kanun'un 116., 127. ve 134. maddeleri uyarınca başvurucunun da aralarında bulunduğu şüphelilerin ikametgâhlarında 6/9/2016 tarihinde arama yapılmasına, bulunan cep telefonu, bilgisayar, hard disk, hafıza kartları, sim kartları vb. kayıt tutma özelliği bulunan her türlü dijital materyale el konulmasına, ele geçirilecek kayıtlardan kopya alınmasına, kayıtların çözümlenerek metin hâline getirilmesine karar verilmiştir.

30. Başvurucu, Kayseri 3. Sulh Ceza Hâkimliğinin 8/9/2016 tarihli kararı ile tutuklanmıştır.

31. Kayseri Cumhuriyet Başsavcılığının 26/10/2016 tarihli yazısıyla, 5271 sayılı Kanun'un 135. maddesi uyarınca başvurucunun da aralarında bulunduğu şüphelilerin telefon numaralarının 1/10/2013 ile 1/10/2016 tarihleri arasında iletişim kayıtları ve hangi baz istasyonlarından servis aldığına tespitine karar verilmesi talep edilmiştir. Kayseri 1. Sulh Ceza Hâkimliğinin 2/11/2016 tarihli kararı ile talep doğrultusunda karar verilmiştir.

32. Başsavcılık tarafından 27/12/2016 tarihli iddianame ile Kayseri 2. Ağır Ceza Mahkemesinde (Mahkeme) kamu davası açılmıştır. İddianamede FETÖ/PDY'ye ilişkin açıklamalara yer verildikten sonra başvurucunun durumu değerlendirilmiştir. İddianamede başvurucunun örgütün haberleşme aracı olan ByLock programının kullanıcısı olduğu tespitine yer verilmiştir. Söz konusu haberleşme programının örgüt üyesi olmayanlar tarafından kullanılmasının mümkün olmadığı vurgulandığı

iddianamede, başvuruçunun terör örgütüne üye olma suçunu işlediği kanaati ifade edilmiştir. İddianamede başvuruçunun ByLock isimli şifreli haberleşme programını adına kayıtlı 533....2 GSM numarası ile kullandığının tespit edildiği belirtilmiştir. İddianamede ayrıca başvuruçunun Bank Asyada hesabının bulunmasına, 22/7/2016 tarihli ve 667 sayılı Olağanüstü Hal Kapsamında Alınan Tedbirlere İlişkin Kanun Hükmünde Kararname ile kapatılan Aktif Eğitim-Sen isimli sendika ile Silopi Eğitimciler ve Girişimci İş Adamları Derneğinin üyesi olmasına ve başvuruçunun sohbet imamı olduğunu beyan eden O.D. isimli bir tanığın ifadesine dayanılmıştır.

33. Mahkeme başvuruçunun ByLock kullanıp kullanmadığı, kullanmış ise hangi telefon hattı ve IMEI numaralı telefonda kullandığı hususunda bilgi verilmesini KOM'dan ve Kayseri İl Emniyet Müdürlüğünden istemiştir. Kayseri Siber Suçlar İle Mücadele Şube Müdürlüğünce 18/2/2017 tarihinde başvuruçuya ait dijital materyallere dair inceleme raporu ve ekinde bir adet DVD mahkeme dosyasına sunulmuştur.

34. Kayseri İl Emniyet Müdürlüğü KOM Şube Müdürlüğünce 6/2/2017 tarihinde Yeni ByLock CBS Sorgu Sonucu Raporu sunulmuş ve başvuruçuya ait telefonun hat numarası ve IMEI numarası bilgilerine göre başvuruçunun telefonuna ByLock haberleşme programını yükleyerek (4397) ID kullanıcı numarasıyla kullandığının anlaşıldığı belirtilmiştir. Ayrıca Ankara Cumhuriyet Başsavcılığının 2016/180056 sayılı soruşturma dosyasından elde edilen bilgi kapsamında başvuruçuya ait ByLock kullanımını gösteren ByLock Tespit ve Değerlendirme Tutanağı sunulmuştur. Söz konusu tutanakta, başvuruçunun adına kayıtlı olan GSM hattı kullanılarak ByLock sunucusuna yapılan bağlantı sonucunda ByLock iletişim sistemi içinde oluşturulan verilere ilişkin bilgiler yer almaktadır. Buna göre ByLock Tespit ve Değerlendirme Tutanağı'nda; kullanıcı bilgilerinin yanı sıra kullanıma ilişkin istatistiksel verilere, kullanıcıyı ekleyenlerin ve kullanıcının eklediği kişilere, kullanıcının kurduğu ve katıldığı gruplar ile bunların kişi listesine, kullanıcıya bağlı kişi ve mail listesi ile yazışmalara, mail bilgisi ve arama kayıtları ile log tablolarına dair bilgiler bulunmaktadır.

35. Başvuruçunun hakkındaki yargılama iki celsede tamamlanmıştır. 9/3/2017 tarihli ilk duruşmada Mahkeme bir tanığı dinlemiştir. Tanık O.D. başvuruçunun sohbet imamı olduğunu, sohbetlerde Fetullah Gülen'in vaazlarını dinlediklerini beyan etmiştir. Başvuruçunun ise suçlamaları ve tanık beyanını kabul etmediğini, ByLock programını kullanmadığını, 7-8 yıldır aynı telefon hattını kullandığını, bu hatla ByLock programını ne zaman ne şekilde indirdiğini bilmediğini, HTS kayıtlarında inceleme yapıldığı takdirde ByLock kullanmadığının anlaşılacağını belirtmiştir.

Başvurucu müdafii; HTS kayıtları, IP çakışması, ByLock içeriklerini gösteren belgelerin getirtilmesini talep ettiğini belirtmiştir.

36. 14/3/2017 tarihinde yapılan ikinci duruşmada Mahkeme, başvurucunun silahlı terör örgütüne üye olma suçundan 7 yıl 6 ay hapis cezası ile cezalandırılmasına karar vermiştir. Kararın gerekçesinde hem FETÖ/PDY'nin kuruluşu, amaçları ve yapılanmasıyla ilgili hem de ByLock iletişim programına, bu programa dair verilerin hukuka uygun delil olduğuna ve programın örgütün kullanımına sunulmuş, örgütsel amaçlarla kullanılan bir program olduğuna dair açıklamalara yer verilmiştir. Başvurucunun sıradan bir vatandaşın temin edip kullanma imkânı olmayan ve sadece FETÖ/PDY mensuplarınca haberleşme amacıyla kullanıldığı bilinen ByLock isimli programını kullanmak, FETÖ/PDY ile irtibat ve iltisakı olması nedeniyle 667 sayılı KHK'yla kapatılan Aktif Eğitim Sen ile Silopi Eğitimciler ve Girişimci İş Adamları Derneğine üye olmak, FETÖ/PDY tarafından düzenlenen toplantılara katılmak, bu toplantılarda imamlık yapmak, Bank Asyaya gelirinin çok üzerinde para yatırarak Bank Asyayı desteklemek suretiyle örgütün hiyerarşik yapısına dâhil olduğu, böylelikle üzerine atılı terör örgütüne üye olma suçunu işlediği belirtilmiştir.

37. Başvurucu anılan karara karşı istinaf başvurusunda bulunmuştur. İstinaf dilekçesinde ceza normunun geçmişe yürütülmesi, telefona ByLock programının yüklenmiş olmasının suç kapsamında yorumlanması sebebiyle suç ve cezaların kanuniliği ilkesinin, ceza kanununun geniş yorumlanması sebebiyle de kıyas yasağının ihlal edildiğini ileri sürmüştür. Başvurucu, kanuni olmayan delillere dayanılarak suç isnat edilmesinin belirlilik ilkesine aykırı olduğunu, mahkûmiyet hükmünün varsayımına dayandığını belirtmiş; ByLock delilinin hukuka aykırı olarak elde edildiğini iddia etmiştir.

38. Ankara Bölge Adliye Mahkemesi 4. Ceza Dairesi (Bölge Adliye Mahkemesi) başvurucunun kullandığı GSM hattının ve bu hatlarda kullanılan IMEI numaralarının 1/1/2014-15/7/2016 tarihi aralığını kapsayacak şekilde HTS kayıtları ile 12/7/2014-15/7/2016 tarihi aralığını kapsayacak şekilde ByLock'un belirlenen IP numaralarına bağlantı yaptığı tarih, saat ve baz istasyonu gösterir HTS kayıtlarını BTK Başkanlığından ve başvurucunun kullandığı GSM hatları ile Bylock programı üzerinden yaptığı iletişim içeriklerinin tespitini Emniyet Genel Müdürlüğü KOM Daire Başkanlığından talep etmiştir. Bölge Adliye Mahkemesi başvurucunun GSM hattı ve bu hattın kullanıldığı cihazlarla ByLock programına erişime ilişkin olarak BTK Başkanlığı ve Emniyet Genel Müdürlüğü KOM Daire Başkanlığından getirtilen kayıtlar üzerinde adli bilişim konusunda uzman bilirkişiden rapor aldırmıştır. Adli bilişim uzmanınca hazırlanan 29/6/2017 tarihli bilirkişi raporunda, başvurucunun adına kayıtlı olan ve kullandığı 0533....2 numaralı GSM hattı ile 11/8/2014 ve 9/5/2015 tarihleri arasında 99 farklı günde ByLock sunucuları/sistemlerine ait 46.166.160.137, 46.166.164.176,

46.166.164.177 ve 46.166.164.181 No.lu IP numaraları ile iletişim kurduğu, belirtilen IP numarası üzerinden belirtilen tarih aralığında ByLock sistemine 119.451 kez erişim sağladığı belirtilmiştir.

39. Bölge Adliye Mahkemesi 19/10/2017 tarihinde istinaf istemini esastan reddetmiştir. Mahkeme kararında ByLock delilinin hukuka aykırı şekilde elde edildiğine ilişkin iddialar da değerlendirilmiştir. Kararda, Anayasa'nın 22. maddesinin son fıkrasında yer alan "İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir." hükmü uyarınca MİT'in istisna kurumlardan kabul edildiği, ayrıca ByLock delilinin elde edilmesinde MİT'in 2937 sayılı Kanun'un 6. maddesinin (d) ve (g) bentleri ile 4. maddesinin (i) bendi kapsamında verilen yetkileri kullandığının açık olduğu ifade edilmiştir. Kararda ByLock iletişim sisteminin FETÖ/PDY mensuplarının kullanmaları amacıyla oluşturulan ve münhasıran bu örgütün mensupları tarafından kullanılan bir ağ olduğu, bu nedenle örgüt talimatı ile bu ağa dâhil olunduğunun ve gizliliği sağlamak için haberleşme amacıyla kullanıldığının her türlü şüpheden uzak, kesin kanaate ulaştıracak teknik verilerle tespiti hâlinde kişinin örgütle bağlantısını gösteren delil sayılacağı belirtilmiştir. Bunun yanı sıra somut olayda sadece FETÖ/PDY mensuplarının kullanması amacıyla oluşturulan ve münhasıran bu suç örgüt mensupları tarafından kullanıldığı tespit edilen ByLock iletişim sistemine, bu özelliğini bilerek dâhil olan ve birçok kez kullanan başvurucunun inkâra dayanan savunmalarına itibar edilmeyerek dosya içinde bulunan diğer delillerle birlikte FETÖ/PDY'ye üye olduğu sonucuna ulaşan ilk derece mahkemesinin değerlendirmesinde isabetsizlik olmadığı belirtilmiştir.

40. Başvurucu temyiz başvurusunda bulunmuş, Yargıtay 16. Ceza Dairesi 4/6/2018 tarihinde Mahkemenin mahkûmiyet kararına yönelik istinaf istemini reddeden Bölge Adliye Mahkemesi kararını onamıştır. Nihai karar başvurucu müdafisine 25/7/2018 tarihinde tebliğ edilmiştir.

41. Başvurucu 26/7/2018 tarihinde bireysel başvuruda bulunmuştur.

IV. İLGİLİ HUKUK

A. Ulusal Hukuk

1. İlgili Mevzuat

42. 5271 sayılı Kanun'un "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" kenar başlıklı 134. maddesinin olay tarihinde yürürlükte bulunan hâli şöyledir:

"(1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde

arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

(4) Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır."

43. 5271 sayılı Kanun'un "İletişimin tespiti, dinlenmesi ve kayda alınması" kenar başlıklı 135. maddesinin olay tarihinde yürürlükte olan hâlinin ilgili kısmı şöyledir:

"(1) Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi (...) dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir. Cumhuriyet savcısı kararını derhâl hâkimin onayına sunar ve hâkim, kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde tedbir Cumhuriyet savcısı tarafından derhâl kaldırılır.

...

(8) Bu madde kapsamında dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesine ilişkin hükümler ancak aşağıda sayılan suçlarla ilgili olarak uygulanabilir:

...

16. (Ek: 2/12/2014-6572/42 md.) Anayasal Düzene ve Bu Düzenin İşleyişine Karşı Suçlar (madde 309, 311, 312, 313, 314, 315, 316),"

44. 5271 sayılı Kanun'un "Cumhuriyet savcısının görev ve yetkileri" kenar başlıklı 161. maddesinin ilgili kısmı şöyledir:

"(1) Cumhuriyet savcısı, doğrudan doğruya veya emrindeki adli kolluk görevlileri aracılığı ile her türlü araştırmayı yapabilir; yukarıdaki maddede yazılı sonuçlara varmak için bütün kamu görevlilerinden her türlü bilgiyi isteyebilir. ...

...

(4) Diğer kamu görevlileri de, yürütülmekte olan soruşturma kapsamında ihtiyaç duyulan bilgi ve belgeleri, talep eden Cumhuriyet savcısına vakit geçirmeksizin temin etmekle yükümlüdür."

45. 2937 sayılı Kanun'un 4. maddesinin olay tarihinde yürürlükte bulunan hâlinin ilgili kısmı şöyledir:

"Millî İstihbarat Teşkilatının görevleri şunlardır;

a) Türkiye Cumhuriyetinin ülkesi ve milleti ile bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, Anayasal düzenine ve milli gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkında milli güvenlik istihbaratını Devlet çapında oluşturmak ve bu istihbaratı Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile gerekli kuruluşlara ulaştırmak.

...

i) Dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak."

46. 2937 sayılı Kanun'un 6. maddesinin ilgili kısmı şöyledir:

"Millî İstihbarat Teşkilatı bu Kanun kapsamındaki görevlerini yerine getirirken aşağıdaki yetkileri kullanır:

a) Yerli ve yabancı her türlü kurum ve kuruluş, tüm örgüt veya oluşumlar ve kişilerle doğrudan ilişki kurabilir, uygun koordinasyon yöntemlerini uygulayabilir.

b) Kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu kapsamındaki kurum ve kuruluşlar ile diğer tüzel kişiler ve tüzel kişiliği bulunmayan kuruluşlardan bilgi, belge, veri ve kayıtları alabilir, bunlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim alt yapısından yararlanabilir ve bunlarla irtibat kurabilir. Bu kapsamda talepte bulunulanlar, kendi mevzuatlarındaki hükümleri gerekçe göstermek suretiyle talebin yerine getirilmesinden kaçınamazlar.

...

d) Görevlerini yerine getirirken gizli çalışma usul, prensip ve tekniklerini kullanabilir.

...

g) Telekomünikasyon kanallarından geçen dış istihbarat, millî savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplayabilir."

47. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Genel ilkeler" kenar başlıklı 4. maddesi şöyledir:

"(1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.

(2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

a) Hukuka ve dürüstlük kurallarına uygun olma.

b) Doğru ve gerektiğinde güncel olma.

c) Belirli, açık ve meşru amaçlar için işlenme.

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme."

48. 6698 sayılı Kanun'un "İstisnalar" kenar başlıklı 28. maddesinin (1) numaralı fıkrasının ilgili kısmı şöyledir:

"Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:

...

ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

..."

49. 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'nun BTK'nın görev ve yetkilerini düzenleyen "Kurumun görev ve yetkileri" kenar başlıklı 6. maddesinin birinci fıkrasının ilgili kısmı şöyledir:

"c) Abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak.

...

1) Elektronik haberleşmeyle ilgili olarak, işletmeciler, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden ihtiyaç duyacağı her türlü bilgi ve belgeyi almak ve gerekli kayıtları tutmak,

..."

50. 5809 sayılı Kanun'un "Kişisel verilerin işlenmesi ve gizliliğinin korunması" kenar başlıklı 51. maddesinin ilgili kısmı şöyledir:

"(1) Kişisel verilerin işlenmesinde; hukuka ve dürüstlük kurallarına uygun olması, doğru ve gerektiğinde güncel olması, belirli, açık ve meşru amaçlar için işlenmesi, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ile işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi ilkelerine uyulur.

(2) Elektronik haberleşmenin ve ilgili trafik verisinin gizliliği esas olup, ilgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi yasaktır.

(3) Elektronik haberleşme şebekeleri, haberleşmenin sağlanması dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla işletmeciler tarafından ancak ilgili abonelerin/kullanıcıların verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve açık rızalarının alınması kaydıyla kullanılabilir.

(4) İşletmeciler şebekelerinin, abonelerine/kullanıcılarına ait kişisel verilerin ve sundukları hizmetlerin güvenliğini sağlamak amacıyla uygun teknik ve idari tedbirleri alır.

(5) Bu Kanununun 49 uncu maddesi kapsamında veya kamu yararının sağlanması amacıyla Kurum tarafından işletmecilere getirilen yükümlülüklerin yerine getirilebilmesi için kişisel veriler işlenebilir.

...

(7) Trafik verileri; trafiğin yönetimi, arabağlantı, faturalama, usulsüzlük/dolandırıcılık tespitleri ve benzeri işlemleri gerçekleştirmek veya tüketici şikâyetleri ile arabağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü amacıyla sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla işlenir ve bu uzlaşmazlıkların çözüm süreci tamamlanıncaya kadar gizliliği ve bütünlüğü sağlanarak saklanır.

(8) İşletmeciler konum verilerinin işlenmesinde abonelere/kullanıcılara bu verilerin işlenmesini reddetme imkânı sağlar. İlgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde ancak acil yardım çağrıları ile 29/5/2009 tarihli ve 5902 sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanunda tanımlanan afet ve acil durum hâllerinde abonelerin/kullanıcıların açık rızası aranmaksızın konum verileri ve ilgili kişilerin kimlik bilgileri işletmeci tarafından yetkilendirilen kişilerle sınırlı olmak kaydıyla işlenebilir.

(9) Abone/kullanıcı şikâyetlerinin incelenmesi ve denetim faaliyetleri kapsamında trafik ve konum verileri ile kişisel veriler, belirtilen faaliyetlerle sınırlı olmak kaydıyla işlenebilir.

(10) Bu Kanun kapsamında sunulan hizmetlere ilişkin olarak;

a) Soruşturma, inceleme, denetleme veya uzlaşmazlığa konu olan kişisel veriler ilgili süreç tamamlanuncaya kadar,

b) Kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtları iki yıl,

c) Kişisel verilerin işlenmesine yönelik abonelerin/kullanıcıların rızalarını gösteren kayıtlar asgari olarak abonelik süresince saklanır. Veri kategorileri ile haberleşmenin yapıldığı tarihten itibaren bir yıldan az ve iki yıldan fazla olmamak üzere verilerin saklanma süreleri yönetmelikle belirlenir..."

51. 24/7/2012 tarihli ve 28363 sayılı Resmî Gazete'de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'in (Yönetmelik) "Kişisel verilerin işlenmesine ilişkin ilkeler" kenar başlıklı 4. maddesinin (1) numaralı fıkrası şöyledir:

"Kişisel verilerin;

a) Hukuka ve dürüstlük kurallarına uygun olarak işlenmesi,

b) İlgili kişinin rızasına dayalı olarak işlenmesi,

c) Elde edilme amacıyla bağlantılı, yeterli ve orantılı olması,

ç) Doğru olması ve gerektiğinde güncellenmesi,

d) İlgili kişilerin kimliklerini belirtecek biçimde ve kaydedildikleri veya yeniden işlenecekleri amaç için gerekli olan süre kadar muhafaza edilmesi esastır."

52. Yönetmelik'in "Haberleşmenin gizliliği" kenar başlıklı 7. maddesinin (1) numaralı fıkrası şöyledir:

"Elektronik haberleşme ve ilgili trafik verisinin gizliliği esas olup, ilgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve gözetimi yasaktır."

53. Yönetmelik'in "Trafik verisinin bildirilmesi" kenar başlıklı 10. Maddesi şöyledir:

"Trafik verisi, arabağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü, tüketici şikâyetlerinin değerlendirilmesi ve denetim faaliyetlerinin gerçekleştirilmesi amacıyla yazılı olarak talep edilmesi halinde kanunların yetkili kıldığı mercilere verilir."

54. Yönetmelik'in "İşletmecilerin veri saklama süreleri" kenar başlıklı 14. maddesinin (2) numaralı fıkrası şöyledir:

"Soruşturma, inceleme, denetleme veya uzlaşmazlığa konu olan kişisel veriler, ilgili süreç tamamlanuncaya kadar saklanır."

2. İlgili Yargı Kararları

55. Anayasa Mahkemesi 5809 sayılı Kanun'un 51. maddesinin (2) numaralı fıkrasında yer alan "...ilgili mevzuatın ve...", (6) numaralı fıkrasında yer alan "...ilgili mevzuat hükümleri saklı kalmak kaydıyla,..." ve (8) numaralı fıkrasının ikinci cümlesinde yer alan "...ilgili mevzuatın ve..." ibareleri ile (13) numaralı fıkrasının Anayasa'ya aykırılık iddiasını incelemiş; söz konusu düzenlemelerin Anayasa'nın kişisel verilerin korunmasını isteme hakkını güvence altına alan 20. maddesine aykırı olmadığına karar vermiştir (AYM E.2015/61, K.2016/172, 2/11/2016). Anayasa Mahkemesinin söz konusu kararının ilgili kısmı şöyledir:

"191. Anayasa'nın 20. maddesinin üçüncü fıkrasında, herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu; bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı belirtildikten sonra kişisel verilerin, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği, kişisel verilerin korunmasına ilişkin esas ve usullerin de kanunla düzenleneceği hüküm altına alınmıştır. Böylece kişisel verilerin korunması hakkı anayasal güvenceye bağlanmıştır.

192. Kişisel verilerin korunması hakkı, insan onurunun korunması ve kişiliğin serbestçe geliştirilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Anayasa'nın 20. maddesinin üçüncü fıkrası uyarınca kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Türkiye'nin taraf olduğu 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Avrupa Konseyi Sözleşmesi'nin 9. maddesinde de devlet güvenliği, kamu güvenliği, devletin ekonomik menfaatlerinin korunması ve suçlarla mücadele edilmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması ile verilerin istatistiki veya bilimsel amaçlarla kullanılması durumlarında

kişisel verilerin korunmasına sınırlamalar getirilebileceği öngörülmüştür. Ancak bu sınırlamalar, Anayasa'nın 13. maddesinde yer alan güvencelere aykırı olamaz. Anayasa'nın 13. maddesine göre temel hak ve özgürlüklere yönelik sınırlamalar, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacağı gibi hak ve özgürlüklerin özlerine de dokunamaz.

193. Kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvencenin yaşama geçirilebilmesi için, bu hakkı ilgilendiren yasal düzenlemelerin, açık, anlaşılabilir ve kişilerin söz konusu haklarını kullanabilmelerine elverişli olması gerekir. Ancak böyle bir düzenleme ile kişilerin özel hayatlarını ilgilendiren veri ve bilgilerin resmi makamların keyfi müdahalelerine karşı korunması olanaklı hâle getirilebilir.

194. Kanun'un 51. maddesinin (2) numaralı fıkrasında, elektronik haberleşmenin ve ilgili trafik verisinin gizliliğinin esas olduğu ifade edildikten sonra, dava konusu kuralla 'ilgili mevzuatın' öngördüğü durumlar istisna tutularak, haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi yasaklanmıştır. Böylece, kişisel verilerin işlenmesi kural olarak yasaklanmış olmakla beraber ilgili mevzuatın öngördüğü durumlarda haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi mümkün kılınmıştır.

195. Anayasa'nın 20. maddesinin üçüncü fıkrasında, kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin rızasıyla işlenebilmesine olanak tanınmış, Anayasa Mahkemesinin yukarıda anılan 9.4.2014 tarihli ve E.2013/122, K.2014/74 sayılı kararında da bu husus teyit edilerek kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceği ifade edilmiştir. Anayasa'nın 20. maddesinin açık hükmü ve Anayasa Mahkemesinin anılan kararı gözetildiğinde, kanunla bir belirleme ve sınırlama yapılmaksızın yürütmenin düzenleyici işlemleriyle haberleşmeye ilişkin kişisel verilerin işlenmesine anayasal açıdan olanak bulunmamaktadır. Bu bağlamda, elektronik haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesine olanak tanıyan kuralda yer alan 'ilgili mevzuat' ibaresiyle de kişisel verilerin işlenmesiyle ilgili düzenlemeler öngören diğer kanun hükümlerinin kastedildiği anlaşılmaktadır. Nitekim, kuralın gerekçesinde de Anayasa'nın 20. maddesi uyarınca kişisel verilerin işlenmesi konusunun kanunla düzenlenmesi gerektiğinden elektronik haberleşme sektöründe kişisel verilerin işlenmesi ve gizliliğine yönelik hususlara ilişkin olarak yeni bir kanun tasarısı hazırlandığı ifade edilmiştir. Ayrıca kişisel verilerin korunması konusunda çerçeve kanun niteliği taşıyan 6698 sayılı Kişisel Verilerin

Korunması Kanunu'nun 4. maddesinin (1) numaralı fıkrasında da, kişisel verilerin ancak kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği hüküm altına alınmıştır.

196. Dolayısıyla, kuralda yer alan 'ilgili mevzuat' kavramı, elektronik haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesiyle ilgili yasal düzenlemeleri ifade ettiğinden, dava konusu kuralda, kişisel verilerin korunmasına ilişkin usul ve esasların kanunla düzenlenmesini öngören Anayasa'nın 20. maddesine aykırı bir yön bulunmamaktadır.

197. Günümüzde, milli güvenlik, istihbarat, suçla mücadele gibi çok farklı nedenlerle kişisel verilerin işlenmesine ihtiyaç duyulabilmektedir. Ayrıca zaman içerisinde gelişen teknolojiyle birlikte bu konuda yeni kanuni düzenlemeler yapılması da gerekebilir. Bu nedenle, haberleşmeye ilişkin kişisel verilerin hangi durumlarda işlenebileceğinin kanunla tek tek sayılmak suretiyle belirlenmesi mümkün değildir. Dava konusu kuralda da genel bir belirleme yapılarak haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesinin yasak olduğu hüküm altına alındıktan sonra, elektronik haberleşmeye ilişkin kişisel verilerin işlenmesine olanak tanıyan ilgili kanun hükümleri saklı tutulmuştur.

198. Diğer taraftan, dava konusu kuralla, konuyla ilgili kanunlarda haberleşmeye ilişkin kişisel verilerin işlenmesine olanak tanınmakla birlikte bu konuda kanun koyucunun sınırsız bir takdir yetkisi bulunmamaktadır. Nitekim, 5809 sayılı Kanun'un 51. maddesinin (1) numaralı fıkrasında, kişisel verilerin işlenmesinde; hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işleme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uyulması gerektiği belirtilmiş, Kişisel Verilerin Korunması Kanunu'nun 4. maddesinde de, benzer ilkelere yer verilerek kişisel verilerin işlenmesinde gözetilmesi gereken hususlar ayrıntılı bir şekilde düzenlenmiştir. Dolayısıyla, dava konusu kuralın kişisel verilerin işlenmesi noktasında kanun koyucuya sınırsız bir takdir hakkı verdiği söylenemez.

199. Bu itibarla, ilgili kanunların öngördüğü durumlarda, haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesine olanak tanıyan kuralda belirsizlik bulunmadığı gibi, kişisel verilerin korunmasını isteme hakkının özüne dokunan ya da bu hakkı ölçüsüz şekilde sınırlandıran bir husus bulunmamaktadır.

200. Açıklanan nedenlerle kural, Anayasa'nın 2., 13. ve 20. maddelerine aykırı değildir. İptal talebinin reddi gerekir."

56. Yargıtay Ceza Genel Kurulunun 26/9/2017 tarihli ve E.2017/16.MD-956, K.2017/370 sayılı kararında ByLock iletişim sistemindeki veri tespitlerinin hangi koruma tedbiri kapsamında incelenmesi gerektiğine ilişkin olarak yapılan açıklamalar şöyledir:

"Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbiri, CMK'nun 134. maddesinde düzenlenmiştir. Bu koruma tedbiri, CMK'nun 116 ve 134. maddeleri arasında düzenlenen 'arama' ve 'elkoyma' koruma tedbirlerinin özel bir görünümünü oluşturmaktadır.

...

Bilgisayar kütüklerinin sadece hard disk şeklinde anlaşılması gerekir. Bilgisayar kütükleri, internet servis sağlayıcılarının internet erişimi sağladıkları kullanıcılara ait IP no'larını ve diğer erişim bilgilerini depoladıkları veri tabanlarını da ifade etmekte[dir] ...

Nitekim Adli ve Önleme Aramaları Yönetmeliğinin 'bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma' başlıklı 17. maddesinin yedekleme işlemi düzenleyen üçüncü fıkrası; yedekleme işleminin, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanacağını düzenlemiştir. Yönetmelikte yer alan "Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır" ibaresi ile olay yerindeki bilgisayarların yanı sıra uzak bilgisayar kütüklerine de erişim sağlanabilecektir.

...

... [İ]nternet ortamında gerçekleştirilen iletişime ilişkin kayıtlar, bilgisayar kütüğünde kayıt altına alındığından, bu iletişim kayıtları hakkında CMK'nun 134. maddesinin birinci fıkrası gereğince arama, kopyalama ve elkoyma koruma tedbirleri uygulanabilir..."

B. Uluslararası Hukuk

1. Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi

57. Birleşmiş Milletler Genel Kurulunun 10/12/1948 tarihli ve 217 (111) sayılı kararı ile kabul edilen İnsan Hakları Evrensel Beyannamesi'nin 12. maddesi şöyledir:

"Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfî karışmalara, şeref ve şöhretine karşı tecavüzlere mâruz kalamaz. Herkesin bu karışmalara ve tecavüzlere karşı kanun ile korunmağa hakkı vardır."

58. Birleşmiş Milletler Genel Kurulu tarafından kişisel verilerin korunması konusunda kabul edilen 14/12/1990 tarihli ve 45/95 sayılı “Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler”de şu temel ilkelere yer verilmiştir:

"1- İşlemenin hukuka uygun ve adil olması ilkesi: Kişilerin hakkındaki veriler hukuka aykırı veya adil olmayan şekilde toplanmamalı veya işlenmemelidir. Ayrıca Birleşmiş Milletler Şartı’ndaki ilkelere aykırı amaçlarla kullanılmamalıdır.

2- Doğruluk ilkesi: Kişisel verileri tutmakla sorumlu makamlar bu bilgilerin doğru tutulmasını güvence altına almalıdır.

3- Belirli ve meşru amaçlar için işleme ilkesi: Bir kaydın tutulması ve kullanımı meşru ve belirli bir amaca dayalı olmalıdır. Bütün kişisel veriler amaç ile ilgili ve onu gerçekleştirmeye elverişli olacak şekilde toplanmalı ve kaydedilmelidir. Bu kişisel verilerin hiçbiri, ilgili kişinin rızası dışında, belirtilenlerle uyuşmayan amaçlar için kullanılamaz veya ifşa edilemez. Kişisel verilen saklanma süresi, belirtilen amaçlara ulaşılmasını sağlayacak süreyi aşamaz.

4- İlgili kişilerin erişmesi ilkesi: Kimlik kanıtı sunan herkes kendisiyle ilgili bilgilerin işlenip işlenmediğini bilme ve gereksiz bir gecikme veya masraf olmadan anlaşılır biçimde elde etme hakkına sahiptir. Ayrıca bu bilgilerin kanuna aykırı, gereksiz veya yanlış olması durumunda uygun düzeltmelerin yapılmasını veya silinmesini talep etme hakkına sahiptir. Devletler buna uygun bir çözüm yolu sağlamak durumundadır. Herhangi bir düzeltme maliyeti dosyadan sorumlu kişi tarafından karşılanmalıdır. Bu ilke hükümlerinin uyruk veya ikâmetine bakılmaksızın herkes için uygulanması arzu edilir.

5- Ayrımcılığın önlenmesi ilkesi: (6) numaralı ilkede kısıtlı olarak öngörülen hâller söz konusu olduğunda ırk veya etnik köken, renk, cinsel yaşam, siyasi görüş, dini, felsefi ve diğer inançların yanı sıra dernek veya sendika üyeliği bilgileri de dahil olmak üzere kanuna aykırı veya keyfî olarak ayrımcılığa yol açabilmesi muhtemel veriler toplanmamalıdır.

6- Üstün amaçlar için istisna koyabilme ilkesi: Ulusal güvenlik, genel sağlık ve ahlakı korumak veya özellikle zulüm gören kişilerin ve diğerlerinin hak ve özgürlüklerinin korunması amacıyla (1) ila (4) numaralı ilkelere ayırılmak mümkün olabilir. Ancak bu tür istisnalar, sınırlarının açıkça belirlendiği ve uygun tedbirlerin ortaya konulduğu iç hukuk sistemine göre yürürlüğe konan bir kanun veya eşdeğer bir düzenlemede açıkça belirtilmiş olmalıdır.

7- Güvenlik ilkesi: Veri dosyaları, kaza ile kaybetme veya yok etme gibi doğal afetler, hileli verilerin yanlış kullanılması ya da bilgisayar virüsleri gibi insan odaklı tehlikelere karşı uygun tedbirlerle korunmalıdır.

8- Denetleme ve yaptırım ilkesi: Her ülkenin kanunu, yerel hukuk sistemine uygun olarak yukarıda belirtilen ilkelere uyulmasından sorumlu makamı belirler. Bu makam tarafsızlık, veri işleme ve oluşturmada sorumlu kişilere karşı bağımsızlık ve teknik yeterlilik teminatı sunmalıdır. Yukarıda belirtilen ilkeleri uygulayan ulusal kanun hükümlerinin ihlali durumunda cezai veya diğer idari yaptırımlar uygun bireysel çözümlerle birlikte öngörülmüş olmalıdır.

9- Sınır ötesi veri transferi ilkesi: Sınır ötesi bir veri akışı ile ilgili olarak iki veya daha fazla ülkenin mevzuatı mahremiyetin korunması için karşılaştırılabilir güvenceler sunduğu takdirde veri dolaşımı mümkün kılınabilir."

2. Avrupa Birliği Genel Veri Koruma Tüzüğü

59. 27/4/2016 tarihli ve 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nün "Tanımlar" kenar başlıklı 4. maddesinin ilgili kısmı şöyledir:

"Bu Tüzük'ün amaçları doğrultusunda, aşağıdaki tanımlar geçerlidir:

Kişisel veri, belirli veya belirlenebilir bir gerçek kişi hakkındaki her bilgiyi ifade eder (veri sahibi); belirlenebilir bir gerçek kişi ad, kimlik, yer bilgisi, online kimlik veya kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel ya da sosyal kimliği gibi belirleyici bir özelliklerle doğrudan veya dolaylı olarak belirlenebilen kişidir.

İşleme, kişisel veri veya kişisel veri dizisinin otomatik veya başka bir şekilde toplanması, kaydedilmesi, organize edilmesi, yapılandırılması, depolanması, uyarlanması veya değiştirilmesi, geri alınması, kullanılması, iletim yoluyla açıklanması, yayılması veya erişilebilir hâle getirilmesi, sıralanması veya kombine edilmesi, sınırlandırılması, silinmesi veya yok edilmesi gibi yollarla herhangi bir işlem veya işlem dizisine tabi tutulması anlamına gelir."

60. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün "Kişisel verilerin işlenmesi ile ilgili ilkeler" kenar başlıklı 5. maddesinin ilgili kısmı şöyledir:

"Kişisel veri;

Veri sahibi ile ilgili olarak hukuka uygun, adil ve şeffaf bir biçimde işlenmelidir (hukuka uygunluk, adillik ve şeffaflık),

Belirlenmiş, açık ve meşru amaçlar için toplanmış olmalı ve bu amaçlara uygun olmayan bir şekilde işlenmemelidir. Kamu yararı, bilimsel ve tarihsel amaçlar ya da arşivleme amacıyla yapılacak diğer işlemler madde 89/1 uyarınca başlangıç amaçlarıyla uyumsuz kabul edilmeyecektir (amaç sınırlaması)

Yeterli, ilgili ve işlendiği amaçlar için gerekli olanlarla sınırlı işlenmelidir (verilerin en az seviyeye indirilmesi)

Doğru ve gerektiğinde güncel tutulmalı; hatalı olan kişisel verinin işlenme amacına bakılmaksızın gecikmeden silinmesini veya düzeltilmesini sağlamak için makul her adım atılmalıdır (doğruluk).

İşlenme amacı için gerekenden daha uzun olmayan bir süre boyunca veri konularının tanımlanmasına izin veren bir formda tutulmalıdır. Kişisel veriler, veri sahibinin hak ve özgürlüklerini korumak için bu Tüzüğün öngördüğü uygun teknik ve yapısal tedbirler alınmak kaydıyla Tüzüğün 89/1. maddesi uyarınca sadece kamu yararına, bilimsel veya tarihi araştırma amaçlarına ya da istatistiki amaçlara yönelik olarak arşivleme amacıyla daha uzun bir süre saklanabilir (saklama süresinin sınırlandırılması).

Yetkisiz veya kanun dışı işlemeye ve kazara kayıp, imha ve hasara karşı uygun teknik veya yapısal tedbirler alınarak kişisel verilerin güvenli bir biçimde işlenmesi sağlanmalıdır (bütünlük ve gizlilik)."

61. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün "Kısıtlamalar" kenar başlıklı 23. maddesinin ilgili kısmı şöyledir:

"Veri sorumlusunun veya işleyenin tabi olduğu Birlik veya Üye Devlet hukuku, 12. ila 22. (bunlara karşılık geldiği sürece 5. madde) ve 34. maddelerdeki yükümlülükleri ve hakların kapsamını, temel hak ve özgürlüklerin özüne saygı gösterdiğinde ve demokratik bir toplumda korunmak için gerekli ve orantılı bir tedbir olduğu takdirde aşağıdaki hâllerde kanun yoluyla sınırlayabilir:

Ulusal güvenlik,

Savunma,

Kamu güvenliği,

Kamu güvenliğine yönelik tehditlerin önlenmesi de dahil olmak üzere suçların önlenmesi, soruşturulması, tespit edilmesi, kovuşturulması veya cezaların infazı,

Birliğin veya Üye Devletin genel olarak kamu yararına olan diğer önemli hedeflerin, özellikle para, bütçe, önemli bir vergilendirme, kamu sağlığı veya sosyal güvenlik dahil olmak üzere önemli bir ekonomik veya mali çıkar amacıyla,

Yargı bağımsızlığının ve yargısal işlemlerin (sürecin) korunması,

Regüle edilmiş meslekler için etik ihlallerin önlenmesi, tespiti, soruşturulması ve kovuşturulması,

(a) ila (e) ve (g) maddelerinde atıfta bulunulan hallerde resmi otoritenin kullanımına zaman zaman bağlı olsa bile izleme, inceleme veya düzenleyici işlevin yerine getirilmesi,

Veri sahibinin veya başkalarının hak ve özgürlüklerinin korunması,

Medeni hukuk hak ve alacaklarının icrası,

Özellikle 1. paragrafta atıfta bulunulan herhangi bir hukuki tedbir öngören kanun en azından uygun olduğu hâllerde şu belirli hükümleri içermelidir:

İşleme veya işleme kategorilerinin amaçları,

Kişisel veri kategorileri,

Tanınan kısıtlamaların boyutu,

Keyfi veya hukuk dışı erişimin ya da aktarımın önlenmesine dair güvenceler,

Sorumlunun veya sorumlu kategorilerinin belirlenmesi,

Depolama dönemleri ve işlemenin niteliği, kapsamı ve amaçları veya işleme kategorileri dikkate alınarak uygulanabilir güvenceler,

Veri sahibinin hakları ve özgürlüklerine getirilen riskler,

Veri sahibinin, amacına halel getirmediği sürece kısıtlama hakkında bilgilendirilmesi."

3. Avrupa İnsan Hakları Sözleşmesi

62. Avrupa İnsan Hakları Sözleşmesi'nin (Sözleşme) "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesinin ilgili kısmı şöyledir:

"(1) Herkes yazışmasına saygı gösterilmesi hakkına sahiptir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."

4. Avrupa Konseyi Siber Suç Sözleşmesi

63. Türkiye Cumhuriyeti tarafından 10/11/2010 tarihinde imzalanan ve Türkiye Büyük Millet Meclisi tarafından onaylanması uygun bulunarak 2/5/2014 tarihinde yürürlüğe giren Avrupa Konseyi Siber

Suç Sözleşmesi'nin "Depolanmış bilgisayar verilerine izinli şekilde veya bu verilerin halka açık olduğu durumlarda sınır ötesinden erişim sağlanması" kenar başlıklı 32. maddesi şöyledir:

"Bir taraf, diğer tarafın izni olmaksızın; a) Halkın serbest kullanımına sunulan (açık kaynaktan gelen) depolanmış bilgisayar verilerine bunların coğrafi konumuna bakılmaksızın erişilebilir; veya b) Kendi ülkesindeki bir bilgisayar sistemi aracılığıyla, diğer tarafın ülkesindeki depolanmış bilgisayar verilerine, eğer bu taraf, söz konusu bilgisayar sistemi aracılığıyla veriyi ifşa etme yetkisini yasal olarak haiz bulunan kişinin yasal ve gönüllü onayını sağlayabilirse, söz konusu verilere erişebilir veya bunları temin edebilir."

5. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

64. 18/2/2016 tarihli ve 29628 sayılı Resmî Gazete'de yayımlanan 30/1/2016 tarihli ve 6669 sayılı Kanun'la uygun bulunan 28/1/1981 tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "Tanımlar" kenar başlıklı 2. maddesinin ilgili kısmı şöyledir:

"Bu Sözleşmenin amaçları bakımından:

a "Kişisel veriler": Kimliği belirli veya belirlenebilir bir gerçek kişi ("ilgili kişi") hakkındaki tüm bilgileri ifade eder.

...

c "Otomatik işlem" den, tamamen veya kısmen otomatik yöntemlerle gerçekleştirilen; verilerin kaydı, bu verilere mantıksal ve/ veya aritmetik işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya dağıtılması anlaşılır."

65. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "Verilerin niteliği" kenar başlıklı 5. maddesi şöyledir:

"Otomatik işleme konu olan kişisel veriler:

- a. Adil biçimde ve yasal yoldan elde edilir ve işlenir;
- b. Belli ve meşru amaçlar için kaydedilir ve bu amaçlara aykırı şekilde kullanılmaz;
- c. Kaydedilme amaçlarına göre uygun ve yerinde olur ve aşırı olmaz;
- d. Doğru bilgileri yansıtır ve gerektiğinde güncellenir;
- e. Kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkan veren bir biçimde saklanır."

66. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "İstisnalar ve kısıtlamalar" kenar başlıklı 9. maddesinin ilgili kısmı şöyledir:

"2. Taraf devletin kanunlarında öngörülmüş olması ve demokratik bir toplumda aşağıdaki hususların sağlanması için gerekli bir önlem oluşturması halinde işbu Sözleşmenin 5, 6 ve 8. maddelerine istisna getirilebilir:

a. Devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi;

b. İlgili kişinin veya başkasının hak ve özgürlüklerinin korunması."

6. Avrupa İnsan Hakları Mahkemesi İçtihadı

a. Olağan Hukuk Yollarının Tüketilmesi Kuralı Yönünden

67. Avrupa İnsan Hakları Mahkemesi (AİHM) Hambardzumyan/Ermenistan (B. No: 43478/11, 5/12/2019) kararında ceza soruşturması kapsamında başvuru edilen gizli dinleme tedbirinin haberleşme hürriyetini ihlal ettiği iddiasının ceza yargılamasının sonuçlanmasından sonra bireysel başvuruya konu edilmesini başvuru süresi açısından tartışmıştır (Hambardzumyan/Ermenistan, §§ 39-55). Başvuruya konu olayda başvuru, bir ıslahevinin kadınlarla ilgili bölümünün başkan yardımcısı olarak çalışmakta iken ıslahevinde kalan bir mahkûmun başvuru eden kendisinden rüşvet istediği ihbarında bulunması üzerine başvuru edenin görüntülü ve sesli izleme altına alınmasına, telefonlarının dinlenmesine 3/2/2010 tarihinde hâkim tarafından karar verilmiştir. Bu suretle elde edilen delillere istinaden başvuru hakkında ceza davası açılmıştır. Başvuru edenin avukatı 12/5/2010 tarihinde 3/2/2010 tarihli karardan haberdar olmuştur. Başvuru eden gerek ceza mahkemesinde gerekse temyizde gizli dinleme ve izleme kararının hukuka aykırı olduğunu ileri sürmüş, derece mahkemeleri de başvuru edenin bu iddiasını esastan tartışmıştır. Başvuru eden 9/11/2010 tarihinde 9 yıl hapis cezasına mahkûm olmuş, ceza 28/4/2011 tarihinde kesinleşmiştir (Hambardzumyan/Ermenistan, §§ 5-22).

68. Başvuru eden ceza yargılamasının kesinleşmesinden sonra AİHM'e yaptığı bireysel başvuruda gizli izleme tedbiri sebebiyle Sözleşme'nin 8. maddesinin ihlal edildiğini öne sürmüştür (Hambardzumyan/Ermenistan, § 35). Hükûmet başvuru edenin tedbirden haberdar olduğu 12/5/2010 tarihinden itibaren altı ay içinde bireysel başvuruda bulunması gerektiği itirazında bulunmuş, ceza yargılamasında delilin hukuka aykırılığının ileri sürülmesinin 8. madde bağlamında etkili bir yol olamayacağını belirtmiştir (Hambardzumyan/Ermenistan, § 37). AİHM sadece etkili olan hukuk yollarının tüketilmesinin zorunlu olduğunu belirtmiş (Hambardzumyan/Ermenistan, § 40), etkili bir başvuru yolunun bulunmadığı veya var olan yolun etkisiz olduğu kanaatine varıldığı hâllerde

başvuru süresinin kural olarak şikâyet edilen fiilin/işlemin gerçekleştiği tarihten itibaren işlemeye başlayacağını ifade etmiştir (Hambardzumyan/Ermenistan, § 41).

69. AİHM başvurucunun suçluluğu hakkında karar veren mahkemenin Sözleşme'nin 8. maddesiyle ilgili şikâyet için etkili bir giderim sağlamaya muktedir olmadığını vurgulamıştır. AİHM'e göre ceza mahkemeleri delilin kabul edilebilirliğiyle ilgili sorunları incelemeye yetkili olsalar da başvurucunun özel hayatına ve haberleşmesine saygı hakkına yapılan müdahalenin kanuni dayanağının bulunup bulunmadığı ya da demokratik toplumda gerekli olup olmadığı şikâyetinin incelenmesi ceza mahkemelerinin yetki alanının dışındadır. Ayrıca bu mahkemeler bu şikâyetle ilgili olarak uygun giderim sağlama niteliğini de haiz değildir (Hambardzumyan/Ermenistan, § 43). Bu sebeple gizli izleme meselesinin başvurucu aleyhine açılan ceza davasının esasını inceleyen mahkemelerde ileri sürülmesi Sözleşme'nin 8. maddesiyle ilgili şikâyetler için etkili yol olarak görülemez (Hambardzumyan/Ermenistan, § 44).

70. Daha sonra AİHM etkili olmadığını tespit ettiği ceza davasından sonra başvuru yapılmış olmasının altı ay kuralıyla bağdaşıp bağdaşmadığını incelemiştir. AİHM başvurucunun gizli izleme kararından soruşturmanın son evrelerinde -dinleme sonucu elde edilen delillerin onun aleyhine olan suçlamanın dayanağı olarak gösterildiği iddianameden kısa bir süre sonra- dosyaya erişim imkânının sağlandığından haberdar olduğunun altını çizmiştir. AİHM olayın arka planı gözetildiğinde başvurucunun bu şikâyetini ceza mahkemesi önünde dile getirmesinin gayrimakul olmadığını kabul etmiştir. AİHM'e göre derece mahkemelerinin gerçekte başvurucunun bu şikâyetini incelemiş olması bu sonucu desteklemektedir. Derece mahkemeleri, izleme tedbirinin hukukiliği iddiasıyla ilgili olarak yaptıkları incelemede Sözleşme şikâyetinin esasıyla ilgili değerlendirmelerde bulunmuştur. Bu koşullarda başvurucu, şikâyetini -hatalı olarak- etkili olduğunu düşündüğü bir hukuk yolunda derece mahkemelerinin dikkatine sunmuş olması sebebiyle suçlanamaz (Hambardzumyan/Ermenistan, § 52).

71. AİHM sonuç olarak Sözleşme'nin kurduğu koruma mekanizmasının insan haklarını güvence altına alan ulusal hukuk sistemine nazaran ikincil nitelikte olduğu ilkesine saygı gösteren başvurucunun ihlalin ulusal hukuk sistemi içinde düzeltilmesi fırsatını derece mahkemelerine vermek için Sözleşme şikâyetini aleyhine yöneltilen suçlamayla ilgili olarak karar veren ceza mahkemesinde öne sürmüş olmasının mantıksız olmadığını vurgulamış ve hükûmetin süre aşımı itirazını reddetmiştir (Hambardzumyan/Ermenistan, §§ 53, 54).

b. Kişisel Verilerin Korunmasını İsteme Hakkı Yönünden

72. AİHM, devletlerin millî güvenliğin korunması amacını gerçekleştirmede sahip oldukları takdir yetkisinin geniş olduğunu kabul etmektedir. AİHM, Sözleşme'ye taraf devletlerin millî güvenliği korumak için yetkili ulusal makamlarına ilk olarak kişiler hakkında bilgi toplama ve halka açık olmayan siciller tutma, ikinci olarak millî güvenlik bakımından önemli kadrolarda çalışmak isteyen adayların bu işe uygunluğunu takdir ederken bu bilgiyi kullanma yetkisi veren kurallara sahip olmaları gerektiğinde kuşku bulunmadığını belirtmektedir (Leander/İsveç, B. No: 9248/81, 26/3/1987, § 59).

73. Bununla birlikte AİHM içtihadına göre kamu mercilerinin bir bireyin özel hayatıyla ilgili bilgileri toplaması, kaydetmesi, saklaması özel hayata saygı hakkına müdahale oluşturur (Leander/İsviçre, § 48; Kopp/İsviçre, B. No: 23224/94, 25/3/1998, § 53; Amann/İsviçre [BD], B. No: 27798/95, 16/2/2000, § 69; Rotaru/Romanya [BD], B. No: 28341/95, 4/5/2000, §§ 43, 44, 46).

74. AİHM'e göre bir kişinin özel yaşamına ilişkin verilerin kaydedilmesi ve saklanması kendi başına özel hayata saygı hakkı bakımından bir müdahale oluşturmaktadır. Bu müdahalenin tespiti için kaydedilen bilgilerin daha sonra kullanılmış olması gibi bir koşul da aranmamaktadır. Bununla birlikte kamu makamları tarafından muhafaza edilen kişisel verilerin Sözleşme'nin 8. maddesinde öngörülen unsurlardan birini devreye sokup sokmadığını tespit etmek için bu bilgilerin hangi çerçevede alındığının ve muhafaza edildiğinin, verilerin türünün, kullanıldığı ve işlendiği şeklin, bunlardan çıkarılabilecek sonuçların dikkate alınması zaruridir (S. ve Marper/Birleşik Krallık [BD], B. No: 30562/04, 30566/04, 4/12/2008, § 67).

75. AİHM'e göre kişisel verilerin korunması, Sözleşme'nin 8. maddesinde öngörülen özel hayata saygı hakkından kişinin yararlanması konusunda büyük öneme sahiptir. İç hukuk kişisel verilerin bu maddede öngörülen güvencelere uygun olmayan şekilde kullanımını engellemek için gerekli güvenceleri sağlamalıdır. Bu tür güvencelerin bulunmasının gerekliliği; otomatik işleme tabi tutulan kişisel verilerin korunması söz konusu olduğunda, özellikle de bu verilerin polis tarafından kullanılması hâlinde daha fazla hissedilmektedir. İç hukuk, bu verilerin saklanma amaçlarına uygun ve aşırıktan uzak olmalarını sağlamalı; verilerin kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde muhafaza edilmesini temin etmelidir. İç hukuk, aynı zamanda kişisel verilerin uygun olmayan şekillerde, keyfî ve yetki aşımı yapılarak kullanılmalarına karşı uygun güvenceler de içermelidir (S.ve Marper/Birleşik Krallık, § 103; M.M./Birleşik Krallık, B. No: 24029/07, 13/11/2012, § 195).

c. Haberleşme Hürriyeti Yönünden

76. AİHM kararlarında gizli tedbirlere ilişkin kanun hükümlerinin barındırması gereken asgari unsurlar sıralanmıştır. Bu kapsamda izleme kararı verilmesine yol açabilecek suçların niteliği, iletişimleri izlenecek kişi kategorisi, izleme sürelerinin sınırları, elde edilen verilerin incelenme, değerlendirilme ve saklanmalarına ilişkin esaslar, verilerin başkalarıyla paylaşılmasına ilişkin önlemler ve elde edilen verilerin ortadan kaldırılmasına ilişkin koşulların kanunda açık bir şekilde düzenlenmesi gereklidir (the Association for European Integration and Human Rights ve Ekimdzhev/Bulgaristan, B. No: 62540/00, 28/6/2007, §§ 76, 77).

77. AİHM somut olaya tam olarak benzemeyen ancak ortaya konulan ilkeler bakımından dikkate değer olan Weber ve Saravia/Almanya ((k.k.), B. No: 53934/00, 29/6/2006) kararında Almanya İstihbarat Teşkilatına mail, posta ve iletişime müdahale yetkisi tanıyan 1968 tarihli Kanun'da 1994 yılında yapılan değişikliği haberleşme hürriyeti yönünden incelemiştir. Söz konusu kanun stratejik izleme olarak tabir edilen yöntemlerle iletişimi kayıt altına alma ve bu yolla temin ettiği bilgileri yetkili makamlara aktarma yetkisini Alman İstihbarat Teşkilatına tanımaktadır. Anılan Kanun'a göre stratejik izlemenin amacı, Federal Almanya Cumhuriyeti'nin karşılaşılabileceği, ülkesine yönelik silahlı saldırı, uluslararası terörist saldırılar ile öteki bazı ağır suçlar gibi ciddi tehlikeleri tespit etmek ve önlemek için iletişimin tespiti ve dinlenmesi yoluyla bilgi toplamaktır. Belli bir kişinin iletişimine müdahale olarak tanımlanan bireysel izleme ise izlenen kişinin işlediğinden veya planladığından şüphelenilen belli ağır suçları önleme veya soruşturma hedefine yöneliktir (Weber ve Saravia/Almanya §§ 3-13).

78. Başvurucular söz konusu Kanun'un başka ülkelerin egemenliklerine yasa dışı olarak müdahale edilmesini öngörmesi sebebiyle kanunilik kriterini sağlamadığını ileri sürmüşlerdir. AİHM söz konusu Kanun'un uluslararası kablosuz iletişim şebekelerini izleme yetkisi verdiğini, bunun da sabit telefon hatlarını değil uydu ve radyo ağlarını etkilediğini belirtmiştir. AİHM'e göre yabancı ülkelerden emilen sinyaller Alman topraklarında yerleşik tesislerden izlenmekte ve toplanan veriler Almanya'da kullanılmaktadır. Bu çerçevede başvurucular, Alman otoritelerinin stratejik izleme yöntemini uygulamak suretiyle yabancı devletlerin uluslararası hukukla korunan toprak egemenliklerini ihlal edecek şekilde davrandıklarını gösteren delil ibraz etme yükümlülüklerini yerine getirememişlerdir (Weber ve Saravia/Almanya, § 88).

79. Başvurucular Kanun'un öngörülebilir olmadığından da şikâyet etmişlerdir. AİHM'e göre gizli dinleme tedbirinin kendine özgü bağlamındaki öngörülebilirlik, kişinin davranışlarını ayarlayabilmesi amacıyla otoritelerin onun iletişimine ne zaman müdahale edebileceğini öngörmesi gerektiği anlamına gelmemektedir. Ancak özellikle idari otoritelere tanınan yetkinin gizli bir şekilde

kullanıldığı hâllerde keyfîlik ihtimali bariz hâle gelmektedir. Bu yüzden özellikle kullanıma açık olan teknolojinin gün geçtikçe daha karmaşık hâle geldiği bu süreçte telefon konuşmalarını dinlemeye ilişkin kuralların açık olması önemlidir. Ulusal hukukun vatandaşların hangi durumlarda kamu otoritelerinin bu tedbiri uygulamaya yetkili olduğunu bilmelerine imkân sağlayacak ölçüde açık olması gerekir. Öte yandan kanun, yetkili otoritelere tanınan takdirin kapsamını ve keyfî müdahalelere karşı koruma sağlamak için nasıl uygulanacağını bireye yeterli açıklıkta göstermelidir (Weber ve Saravia/Almanya, §§ 93, 94).

80. AİHM, devletin gizli izleme tedbiri yoluyla ulusal güvenliğini sağlamadaki menfaati ile başvuruçuların özel hayatına saygı hakkına yapılan bu ciddi müdahale arasında denge kurulması bağlamında ulusal otoritelerin ne tür araçları seçecekleri hususunda nispeten geniş bir takdir yetkisine sahip olduklarına işaret etmiştir (Weber ve Saravia/Almanya, § 106).

81. AİHM elde edilen bilginin başka kurumlara verilmesine ve kullanılmasına ilişkin olarak ise Alman Anayasa Mahkemesinin iptal kararından sonra yapılan değişikliklerle bunların çok sıkı koşullara bağlandığını belirtmiş, özellikle söz konusu bilginin aktarılması için bunun zorunlu olması gerektiğine ve Alman Anayasa Mahkemesinin bu bilginin elde edilme amacı dışında kullanılmayacağına dair kararına işaret etmiştir (Weber ve Saravia/Almanya, §§ 121, 122). AİHM bu bilgilerin Anayasayı Koruma Ofisi ile diğer otoritelere aktarılması ve bunlar tarafından kullanılmasını da incelemiştir. AİHM izlenen kişiler aleyhine ceza soruşturması başlatılmasına imkân sağlamak amacıyla, öncesinde herhangi bir suç şüphesi olmaksızın uygulanan gizli izleme tedbiri ile elde edilen kişisel verilerin transferinin bu kişilerin haberleşmenin gizliliği hakkına yapılan nispeten ciddi bir müdahale olduğunu kabul etmiştir. Bununla birlikte AİHM, stratejik gözetleme yoluyla elde edilen bilginin transferinin sadece kanunda belirtilen ve nispeten ciddi mahiyet taşıyan suçların önlenmesi ve soruşturulması amacıyla sınırlı olduğunu not etmiştir. Ayrıca Alman Anayasa Mahkemesi, iptal kararıyla buna ilişkin güvenceleri sıkılaştırmıştır. Öte yandan bilginin aktarılması kararı, İstihbarat Teşkilatının transfer koşullarının oluşup oluşmadığını değerlendirme konusunda eğitimli olan personeli tarafından verilmektedir. Tüm bu koşulları gözetken AİHM, gözetlemenin konusu olan kişilerin haberleşmenin gizliliği hakkına yapılan müdahalenin gerek suç bakımından makul sınırlamalar getirilmiş olmasıyla gerekse kötüye kullanmaya karşı uygun denetim mekanizmalarının getirilmesiyle dengelendiği sonucuna ulaşmıştır (Weber ve Saravia/Almanya, §§ 125-129).

82. AİHM bilginin imha edilmesini de incelemiştir. AİHM kişisel verilerin kanunda öngörülen amaçlar çerçevesinde arşivlenmesine artık ihtiyaç kalmadığının anlaşıldığı anda imhasının ve imha koşullarının oluşup oluşmadığının görece kısa aralıklarla değerlendirilmesinin öngörülmesinin

haberleşmenin gizliliğine yapılan müdahalenin etkisinin kaçınılmaz seviyeye kadar azaltılmasında önemli bir unsur oluşturduğuna dikkat çekmiştir. AİHM ayrıca Federal Anayasa Mahkemesinin yargısal süreçler için hâlen ihtiyaç duyulan bilgilerin hemen imha edilemeyeceğine ve kanun kapsamında oluşturulan bağımsız komisyonun denetim yetkisinin imhası da dâhil olmak üzere bilginin kullanılmasına ilişkin bütün süreci kapsadığına karar verdiğine işaret etmiştir (Weber ve Saravia/Almanya, § 131).

83. AİHM devletin stratejik gözetleme yetkisinin kötüye kullanılmasına karşı etkili ve yeterli güvencelerin olduğu kanaatine varmış; somut olayda haberleşmenin gizliliğine ulusal güvenliğin sağlanması, suç işlenmesinin önlenmesi amaçlarıyla müdahale edilmesinin demokratik toplumda gereklilik kriterini karşıladığını belirtmiştir. AİHM sonuç olarak başvuruyu açıkça dayanaktan yoksun olması sebebiyle kabul edilemez bulmuştur (Weber ve Saravia/Almanya, §§ 137, 138).

V. İNCELEME VE GEREKÇE

84. Mahkemenin 17/9/2020 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Kişi Hürriyeti ve Güvenliği Hakkının İhlal Edildiğine İlişkin İddia

1. Başvurucunun İddiaları

85. Başvurucu, ByLock programını kullandığı gerekçesiyle tutuklanmasının Anayasa'nın 15. ve 19. maddelerine aykırı olduğunu belirterek kişi hürriyeti ve güvenliği hakkının ihlal edildiğini ileri sürmüştür.

2. Değerlendirme

86. 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 47. maddesinin (5) numaralı ve İçtüzük'ün 64. maddesinin (1) numaralı fıkraları uyarınca bireysel başvurunun başvuru yollarının tüketildiği, başvuru yolu öngörülmemişse ihlalin öğrenildiği tarihten itibaren otuz gün içinde yapılması gerekmektedir.

87. Bir suç isnadına bağlı olarak tutuklulukla ilgili şikâyetleri içeren bireysel başvurunun hükümlerle birlikte verilen tutukluluğun devamı kararı sonrasında yapılması hâlinde tutukluluğun devamı kararına itiraz edilmemiş ise kararın verildiğinin öğrenildiği tarihten itibaren, itiraz edilmiş ise itiraz merciince verilen kararın öğrenildiği tarihten itibaren otuz gün içinde yapılması gerekmektedir (Fırat İşgören, B. No: 2014/6425, 17/11/2016, § 34).

88. Somut olayda başvurucunun ilk derece mahkemesince hükümlerle -14/3/2017 tarihli mahkûmiyet kararıyla- birlikte verilen tutukluluğun devamı kararına itiraz ettiğine yönelik bir bilgi ve/veya belge

bulunmamaktadır. Bu nedenle başvurunun ilk derece mahkemesinin nihai kararının tefhimle öğrenildiği 14/3/2017 tarihinden itibaren otuz gün içinde yapılması gerekmektedir. Buna göre 26/7/2018 tarihinde yapılan bireysel başvuruda süre aşımı olduğu sonucuna varılmıştır.

89. Açıklanan gerekçelerle başvurunun bu kısmının süre aşımı nedeniyle kabul edilemez olduğuna karar verilmesi gerekir.

B. Özel Hayata Saygı Hakkı Kapsamında Kişisel Verilerin Korunmasını İsteme Hakkının ve Haberleşme Hürriyetinin İhlal Edildiğine İlişkin İddia

1. Başvurucunun İddiaları ve Bakanlık Görüşü

90. Başvurucu, haberleşme araçları ve içeriğinin gizli olması gerektiğini belirtmiş; ByLock haberleşmesinin 5271 sayılı Kanun'un 134. ve 135. maddelerine uyulmadan ele geçirildiğini, ByLock uygulamasının ele geçirilmesi ve kişisel verilerinin ortaya çıkarılışındaki hukuksuzluk nedeniyle kişisel verilerin korunmasını isteme hakkının ve haberleşmenin gizliliğinin ihlal edildiğini iddia etmiştir. Başvurucu bu nedenlerle özel hayata saygı ile kişisel verilerin korunmasını isteme hakları ve haberleşme hürriyetinin ihlal edildiğini ileri sürmüştür.

91. Bakanlık görüşünde; Yargıtay 16. Ceza Dairesinin (E.2015/3, K.2017/3; E.2017/1443, K.2017/4758 sayılı) ve Yargıtay Ceza Genel Kurulunun (E.2017/16.MD-956, K.2017/370 sayılı) kararları ile Anayasa Mahkemesinin Aydın Yavuz ve diğerleri kararındaki ByLock iletişim sistemine dair inceleme ve tespitlerin bulunduğu kısımlara yer verilmiştir. Bu kararlara atıfla ByLock iletişim sisteminin kullanımı sonucunda oluşan verilerin tespitinin 5271 sayılı Kanun'un 135. maddesinin birinci fıkrası veya 2937 sayılı Kanun'un 6. maddesinin ikinci fıkrası kapsamında olmayıp 5271 sayılı Kanun'un "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" kenar başlıklı 134. maddesinin birinci fıkrası kapsamında olduğu belirtilmiştir. Bu sebeple 2937 sayılı Kanun'un 4. maddesinin birinci fıkrasının (i) bendi ile 6. maddesinin birinci fıkrasının (d) ve (g) bentlerine uygun şekilde MİT tarafından elde edilen ByLock'a ilişkin dijital materyaller hakkında Ankara Cumhuriyet Başsavcılığının talebi üzerine 5271 sayılı Kanun'un 134. maddesi gereğince Ankara 4. Sulh Ceza Hâkimliği tarafından verilen "inceleme, kopyalama ve çözümleme" kararına istinaden bilgisayar ve bilgisayar kütüklerindeki iletilerin tespiti işleminde herhangi bir hukuka aykırılık bulunmadığı bildirilmiştir. Ayrıca kanuna uygun olarak elde edilen ByLock programına ilişkin verilerin analiz edilmesi neticesinde kullanıcı bilgilerine ulaşıldığı, çalışmanın başlangıcında herhangi bir şahıstan yola çıkılmadığı, diğer bir ifadeyle başlangıçta herhangi bir şahsın kişisel verileri üzerinde çalışma gerçekleştirilmediği belirtilmiştir.

2. Değerlendirme

a. Uygulanabilirlik Yönünden

92. Anayasa'nın iddianın değerlendirilmesinde dayanak alınacak "Özel hayatın gizliliği ve korunması" kenar başlıklı 20. maddesinin ilgili kısmı şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

...

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

93. Anayasa'nın 20. maddesinde 7/5/2010 tarihli ve 5982 sayılı Kanun ile yapılan değişikliğe ilişkin madde gerekçesi şöyledir:

"Anayasada kişisel verilerin korunmasına yönelik dolaylı hükümler bulunmakla birlikte yeterli değildir. Mukayeseli hukukta ve tarafı olduğumuz uluslararası belgelerde de kişisel verilerin korunması önemle vurgulanmaktadır. Maddeyle, herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı, anayasal bir hak olarak teminat altına alınmaktadır. Bu bağlamda, bireylerin kendilerini ilgilendiren kişisel veriler üzerinde hangi hak ve yetkilere sahip olduğu ve kişisel verilerin hangi hallerde işlenebileceği hükme bağlanırken, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği öngörülmektedir."

94. Anayasa'nın "Haberleşme hürriyeti" kenar başlıklı 22. maddesi şöyledir:

"Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.

İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir."

95. Anayasa'nın 22. maddesinde herkesin haberleşme hürriyetine sahip olduğu ve haberleşmenin gizliliğinin esas olduğu hüküm altına alınmıştır. Sözleşme'nin 8. maddesinde de herkesin haberleşmesine saygı gösterilmesini isteme hakkına sahip olduğu düzenlemesine yer verilmiştir (Yasemin Çongar ve diğerleri, B. No: 2013/7054, 6/1/2015, § 48).

96. Anayasa ve Sözleşme'nin ortak koruma alanı, haberleşme hürriyetinin yanı sıra içeriği ve biçimi ne olursa olsun haberleşmenin gizliliğini de güvence altına almaktadır. Posta, elektronik posta, telefon, faks ve internet aracılığıyla yapılan haberleşme faaliyetlerinin haberleşme hürriyeti ve haberleşmenin gizliliği kapsamında değerlendirilmesi gerekir. Haberleşme bağlamında bireylerin karşılıklı ve toplu olarak sözlü, yazılı ve görsel iletişimlerine konu olan ifadelerinin gizliliğinin sağlanması gerekir (Yasemin Çongar ve diğerleri, §§ 49, 50).

97. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16).

98. Başvurucu; ByLock programını kullanım bilgilerinin yasal olmayan şekilde elde edilmesi nedeniyle haberleşmenin gizliliğinin, haberleşme hürriyetinin ve kişisel verilerin korunmasını isteme hakkının ihlal edildiğini ileri sürmüştür. Bu iddianın incelenebilmesi için öncelikle ByLock programının bir haberleşme aracı olup olmadığı, dolayısıyla bu program üzerinden gerçekleştirilen iletişimlerin haberleşme hürriyeti kapsamında olup olmadığına açıklığa kavuşturulması gerekir.

99. Anayasa Mahkemesi ve Yargıtay kararlarında ByLock programının anlık mesajlaşma, e-posta gönderme, ekleme yoluyla kişi listesi oluşturma, grup içi mesajlaşma, sesli görüşme, görüntü veya belge gönderebilme özellikleri bulunduğu tespit edilmiştir. Yapısı ve yazılım mantığı itibarıyla kişiler arası anlık haberleşmeyi ve birtakım verilerin iletimini sağlayan bir yapıda olduğu açıklanmıştır. ByLock uygulamasına erişim sağlanabilmesi için online (çevrim içi) bağlantı gereklidir, uygulama çevrim dışı kullanımı desteklememektedir. Diğer bir ifadeyle kullanıcılar internet bağlantısını sağlayarak mesaj, mail ve veri aktarımı gerçekleştirebilmektedir (Yargıtay Ceza Genel Kurulunun 26/9/2017 tarihli ve E.2017/16.MD-956, K.2017/370 sayılı kararı; Ferhat Kara, §§ 42-54). Tüm bu özellikleri nedeniyle ByLock programının online haberleşme programı olduğu konusunda kuşku yoktur. Haberleşme hürriyetinin posta, elektronik posta, telefon, faks ve internet aracılığıyla yapılan haberleşme faaliyetlerini içerdiği dikkate alındığında ByLock haberleşme programı üzerinden

yapılan iletişimin de haberleşme hürriyeti kapsamında değerlendirilmesi gerektiği sonucuna ulaşılmıştır.

100. Anayasa'nın özel hayata saygı hakkını düzenleyen 20. maddesinin üçüncü fıkrasında; herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme, bu veriler hakkında bilgilendirilme, verilere erişme, bunların düzeltilmesini veya silinmesini talep etme, verilerin amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkına sahip olduğu, kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hükmüne yer verilerek anayasal sınırlar belirlenmiştir. Söz konusu Anayasa hükmünde kişilerin kendileri hakkındaki verilerin amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkına sahip olduğu özellikle vurgulanmıştır.

101. Anayasa'nın 20. maddesinin üçüncü fıkrasının birinci cümlesinde genel olarak herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu belirtilmiş, ikinci cümlesinde kişisel veriler bağlamındaki bazı özel güvenceler sayılmış, üçüncü cümlesinde kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği düzenlenmiş, dördüncü cümlesinde ise kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hüküm altına alınmıştır. Buna göre lafzı dikkate alındığında Anayasa'nın 20. maddesinin üçüncü fıkrasının kişisel verilerin korunmasını isteme hakkı kapsamında sadece işleme şeklindeki sınırlama ya da müdahalelere karşı değil kişisel verilere yönelik her türlü müdahale veya sınırlamalara karşı güvence getirdiği anlaşılmaktadır.

102. Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı yönünden inceleme yapılabilmesi için öncelikle anılan hak kapsamında korunması gereken bir kişisel verinin olup olmadığı belirlenmelidir. Anayasa hükmünün lafzı, konuya ilişkin uluslararası belgeler ve karşılaştırmalı hukuk dikkate alınarak Anayasa Mahkemesi tarafından kişisel veri kavramının -belirli veya kimliği belirlenebilir olmak şartıyla- bir gerçek veya tüzel kişiye ilişkin bütün bilgileri ifade ettiği kabul edilmiştir (AYM, E.2014/74, K.2014/201, 25/12/2014; E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2013/84, K.2014/183, 4/12/2014; E.2014/180, K.2015/30, 19/3/2015; Bülent Kaya [GK], B. No: 2013/2941, 11/5/2016, § 49; Fatih Saraman, [GK], B. No: 2014/7256, 27/2/2019, § 57).

103. Bununla birlikte bir başvuruda Anayasa'nın 20. maddesinin üçüncü fıkrası anlamında bir kişisel veri bulunup bulunmadığı davanın ve başvurunun kendine özgü koşulları dikkate alınarak otonom olarak tespit edilir. Bir kişisel verinin bulunduğu tespit edildiğinde bu veriye yönelik her türlü sınırlama ve müdahale Anayasa'nın anılan hükmü kapsamındaki güvenceleri harekete geçirir.

104. Anayasa Mahkemesinin Ferhat Kara kararında belirtildiği üzere suç isnadı altındaki kişilerin adli soruşturma ve kovuşturmalar kapsamında el konulan cihazlarında tespit edilen ByLock programına dair kurulum dosyası vs. dijital veriler dışında ByLock verileri esas olarak iki kaynağa dayanmaktadır. Bunlardan ilki MİT'in adli makamlara iletildiği ve adli makamların mahkeme kararlarıyla üzerinde inceleme yaptığı ByLock sunucusundan elde edilen verilerdir. İkincisi ise ByLock sunucusuna ait hedef IP'lere Türkiye'den hangi IP'lerden erişildiğine ilişkin olarak mahkeme kararıyla BTK'dan elde edilen CGNAT kayıtlarıdır (Ferhat Kara, § 58). Cumhuriyet Başsavcılıkları ve mahkemelerin talebi üzerine BTK, ByLock IP'sine bağlanan numaraların abonelerine ait şahıs kimlik bilgilerini tespit ederek Başsavcılık ve mahkemelere bildirmiştir (Ferhat Kara, §§ 32-38). Anayasa Mahkemesi kararlarında haberleşme trafik bilgisi kapsamında yer alan IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve abone kimlik bilgilerinin kişisel veri olduğu belirtilmiştir (AYM, E.2014/149, K.2014/151, 2/10/2014).

105. Bu durumda kişinin telefon ve internet kullanımı, bağlandığı IP adresleri bilgisi, gönderdiği mail, mesaj ve arama kayıt bilgilerinin, dolayısıyla ByLock haberleşme programını kullandığına ilişkin verilerin toplanmasının hem özel hayata saygı hakkının içinde yer alan kişisel verilerin korunmasını isteme hakkının hem de haberleşme hürriyetinin kapsamında olduğu sonucuna varılmıştır. Bu nedenle başvurucağın ByLock kullanımını tespit eden belgelerin yasal olmayan şekilde elde edildiği yönündeki iddiasının hem kişisel veriler hem de haberleşmeyle sıkı bağlantısı dikkate alınarak kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyeti kapsamında incelenmesi gerektiği değerlendirilmiştir.

b. Kabul Edilebilirlik Yönünden

106. Mevcut başvuruda öncelikle başvurunun süresi içinde yapılıp yapılmadığının incelenmesi gerekir.

107. 6216 sayılı Kanun'un 47. maddesinin (5) numaralı fıkrası ile İÇtüzük'ün 64. maddesinin (1) numaralı fıkrası uyarınca başvuru yollarının tüketildiği tarihten, başvuru yolu öngörülmemiş ise ihlalin öğrenildiği tarihten itibaren otuz gün içinde bireysel başvuruların yapılması gerekmektedir (Bilent Aktaş ve diğeri, B. No: 2014/19389, 7/12/2016, § 11). Buna göre Anayasa'da güvence altına alınmış temel hak ve özgürlüklerden Sözleşme kapsamındaki herhangi birinin ihlaline neden olduğu ileri sürülen işlem, eylem ya da ihmale ilişkin otuz günlük bireysel başvuru süresi; söz konusu işlem veya eylem için herhangi bir başvuru yolunun kanunlarda öngörülmüş olması hâlinde bu yolun tüketilmesinden sonra verilen nihai kararın öğrenilmesinden, buna karşılık söz konusu işlem veya

eyleme ilişkin olarak kanunlarda herhangi bir başvuru yolunun öngörülmemiş olması durumunda işlemin tesis edildiği ya da eylemin ika edildiği tarihten itibaren işlemeye başlayacaktır.

108. Bir başvuru yolunun tüketilmesi gereğinden söz edilebilmesi için bu hukuki yolun iddia edilen ihlalin sonuçlarını giderici, etkili ve başvuru açısından makul bir çabayla ulaşılabilir nitelikte olması ve sadece teoride kalmayıp fiilen de işlerliği olması gerekmektedir. İhlalin sonuçlarını düzeltici bir vasıf taşımayan veya aşırı ve olağan olmayan birtakım şekli koşulların öngörülmesi nedeniyle fiilen erişilebilir ve kullanılabilir olmaktan uzaklaşan başvuru yollarının tüketilmesi zorunluluğu bulunmamaktadır (Fatma Yıldırım, B. No: 2014/6577, 16/2/2017, § 39). Bununla birlikte soyut olarak makul bir başarı sunma kapasitesi bulunan bir yolun uygulamada başarıya ulaşmayacağına dair şüphe, o başvuru yolunun tüketilmemesini haklı kılmaz (Sait Orçan, B. No: 2016/29085, 19/7/2017, § 36).

109. Başvurucunun başvuru yollarının tüketilmesi noktasında kendisinden beklenebilecek her şeyi yerine getirip getirmediğinin başvurunun özellikleri dikkate alınarak incelenmesi gerekir (S.S.A., B. No: 2013/2355, 7/11/2013, §§ 27, 28). Ancak somut olayın koşulları itibarıyla başvuru yollarının tüketilmesinin yarar sağlamayacağını veya etkili olmadığını anlaşılması hâlinde anılan yollar tüketilmeden yapılan bir başvuru incelenebilir (Şehap Korkmaz, B. No: 2013/8975, 23/7/2014, § 33). Öte yandan başvuru yollarının tüketilmesi, çok katı olarak uygulanması gereken mutlak bir kural değildir. Teorik düzeyde var olan bir başvuru yolunun tüketilmesinin somut olayın koşullarında başvurucuya aşırı külfet yüklemesi hâlinde bu yolun tüketilmesinin gerekli olmadığına karar verilebilir (Rasul Kocatürk, B. No: 2016/8080, 26/12/2019, § 38).

110. Somut olayda başvurucunun ByLock haberleşme programını kullandığına ilişkin verilerin hukuka aykırı olarak elde edilmesi sebebiyle kişisel verilerin korunmasını isteme hakkının ve haberleşme hürriyetinin ihlal edildiği iddiası, başvuru aleyhine yürütülen ve ByLock programı üzerinden elde edilen verilerin delil olarak kullanıldığı ceza yargılamasında ileri sürülmüş; ceza yargılamasının sonuçlanmasından sonra 26/7/2018 tarihinde bireysel başvuruya konu edilmiştir. Başvurucu aleyhine yürütülen ceza yargılamasında ceza mahkemesi, ByLock kullanım bilgilerine ulaşılmasının ve buradan elde edilen verilerin kullanılmasının haberleşme hürriyeti ile kişisel verilerin korunmasını isteme hakkını ihlal edip etmediğine yönelik bir denetim yapmayacağı gibi herhangi bir ihlal bulunması hâlinde uygun giderim sağlama yetkisine de sahip değildir. Bu sebeple başvuru aleyhine yürütülen ceza yargılamasının ByLock haberleşme programına ilişkin bilgilerin elde edilmesi ve kullanılmasının kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyetini ihlal ettiği iddiası yönünden etkili bir başvuru yolu olarak kabul edilmesi zordur.

111. Buna karşılık ceza yargılamasının sözü edilen şikâyet yönünden etkisiz olması ceza yargılamasının sonuçlanmasından sonra yapılan bireysel başvurunun süresinde olmadığı hükmüne varılması için tek başına belirleyici bir unsur değildir. Bireysel başvuru süresine ilişkin olarak yorum yapılırken somut olayın tüm koşulları gözönünde bulundurulmalı ve başvurucuya aşırı külfet yüklenmemesine özen gösterilmelidir. Bu bakımdan kanunda öngörülen başvuru yolunun ihlali tespit etme ve uygun giderim sağlama kapasitesini haiz olup olmadığının tereddütü olduğu, başvurucunun söz konusu başvuru yolundan netice elde edebileceğine dair beklentiye sahip olmasını haklı kılan nedenlerin bulunduğu hâllerde ilgili mekanizmanın tüketilmesinden sonra yapılan başvuruların süresinde olduğu kabul edilebilir. Anayasal şikâyete ilişkin olarak etkililiği hususunda tereddüt bulunan bir başvuru yolu dışında başkaca bir mekanizmanın bulunmadığı hâllerde ilgilinin etkililiği hususunda tereddüt bulunan yolu tükettikten sonra bireysel başvuruda bulunması durumunda başvuru süresiyle ilgili olarak daha esnek davranılmasını haklılaştıran güçlü nedenler bulunmaktadır. Zira asıl olan, ihlalin Anayasa Mahkemesinden önce olağan başvuru yolları kullanılarak tespit edilmesi ve giderilmesidir. Diğer taraftan Anayasa'nın 40. maddesi Anayasa'da güvence altına alınan hak ve özgürlüklere ilişkin ihlalleri tespit edecek ve giderecek hukuksal mekanizmalar oluşturma yükümlülüğünü devlete yüklemektedir. İlgilinin ikincil bir fonksiyona sahip olan Anayasa Mahkemesine başvuru yolunu kullanmasından önce ihlal iddiasını olağan hukuk yollarında öne sürmesi, ihlalin tespiti ve giderilmesi fırsatını öncelikle olağan hukuk mekanizmalarına tanınması anlaşılabilir bir durumdur.

112. Türk hukukunda iletişimin denetlenmesi ve sonrasında ceza davası açılması durumunda iletişimin tespiti suretiyle yapılan müdahalenin haberleşme hürriyetini ihlal ettiğine yönelik iddiaları inceleyecek, varsa ihlali tespit edecek ve gerektiğinde uygun giderim sağlayacak -bireysel başvuru öncesinde tüketilmesi gerekli- bir hukuksal mekanizma bulunmamaktadır. Öte yandan başvurucu aleyhine yürütülen ceza yargılamasında mahkeme ByLock programı bilgilerinin elde edilmesinin ve kullanılmasının haberleşme hürriyetini ihlal edip etmediğini tespit etme yetkisine sahip değil ise de ByLock verilerinin hukuka uygun olarak elde edilip edilmediğini inceleme yetkisine sahiptir. Nitekim somut olayda derece mahkemeleri bu incelemeye kararlarında yer vermişlerdir. Mahkemenin ByLock verilerinin hukuka aykırı olarak elde edilmediği sonucuna ulaşması, haberleşme hürriyeti yönünden ayrı bir değerlendirme mahiyeti taşımasa bile haberleşme hürriyetine yapılan müdahalenin kanuna uygunluğuyla ilgili olarak bir değere sahip olacaktır. Haberleşme hürriyetinin ihlali iddiasıyla ilgili olarak başka bir yolun da bulunmadığı gözetildiğinde başvurucunun dolaylı da olsa haberleşme hürriyetine yapılan müdahalenin kanuniliğiyle ilgili değerlendirme yapılması niteliğini haiz olan

ceza yargılaması yolunu tükettikten sonra ve nihai kararın öğrenilmesinden itibaren otuz gün içinde yaptığı bireysel başvurunun süresinde olduğunun kabulü gerekir.

113. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ve haberleşme hürriyetinin ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

c. Esas Yönünden

i. Müdahalenin Varlığı

114. Somut olayda başvuru suçu işlemediğinden bahisle tüm yargılama süreci boyunca ByLock kullanıcısı olduğu iddiasını kabul etmemiş olsa da aleyhine başlatılan soruşturmanın temel dayanaklarından birini anılan iddia oluşturmaktadır. Başvurucuya yönelik suçlamada ByLock haberleşme programı üzerinden ele geçirilen veriler de esas alınmıştır. Başsavcılığın talebi üzerine Sulh Ceza Hâkimliği kararına dayalı olarak başvurunun ByLock haberleşme programını kullanmasına yönelik iletişim bilgileri tespit edilmiştir. Başvurucunun ByLock kullanıcı bilgileri ve yazışmaları ile log kayıtlarına erişildiği, bu bilginin analiz edilerek soruşturma ile kovuşturma makamlarınca tespit edildiği anlaşılmaktadır (bkz. §§ 28-40). Belirli bir gerçek kişi olan başvurucuya ait olduğu derece mahkemelerince tespit edilen bu elektronik bilgiler kişisel veri olarak kabul edilmelidir. Olayda kamu makamlarınca bu elektronik verilerin tespiti suretiyle kişisel verilerin toplanması, yargısal makamlara nakledilmesi suretiyle aktarılması ve analiz edilerek mahkûmiyete esas alınması suretiyle de kullanılması kişisel verilerin korunmasını isteme hakkına müdahale teşkil etmektedir. Öte yandan söz konusu veriler haberleşme kapsamında kaldığına göre bunlara erişilerek aktarılması ve kullanılması aynı zamanda haberleşmenin gizliliğine de müdahale niteliği taşımaktadır. Buna göre başvuru hakkında uygulanan söz konusu tedbirler özel hayata saygı hakkı içinde yer alan kişisel verilerin korunmasını isteme hakkına ve haberleşme hürriyetine yönelik bir müdahale oluşturmaktadır.

ii. Müdahalenin İhlal Oluşturup Oluşturmadığı

115. Anayasa'nın 13. maddesi şöyledir:

"Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz."

116. Yukarıda belirlenen müdahale, Anayasa'nın 13. maddesinde belirtilen koşullara uygun olmadığı takdirde Anayasa'nın 20. ve 22. maddelerini ihlal edecektir. Bu sebeple sınırlamanın Anayasa'nın 13. maddesinde öngörülen ve somut başvuruya uygun düşen, kanun tarafından öngörülme, meşru amaç taşıma, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmama kriterlerine uygun olup olmadığının belirlenmesi gerekir (Halil Berk, B. No: 2017/8758, 21/3/2018, § 49; Süveyda Yarkin, B. No: 2017/39967, 11/12/2019, § 32; Şennur Acar, B. No: 2017/9370, 27/2/2020, § 34).

117. Başvuru konusu şikâyetin özü, kişisel verilerin korunmasını isteme hakkına ve haberleşme hürriyetine yapılan müdahalenin kanuni dayanağının bulunup bulunmadığına ilişkindir. Bu nedenle öncelikle müdahalenin kanuni dayanağının incelenmesi gerekir.

(1) Kanunilik

(a) Genel İlkeler

118. Anayasa'nın temel hak ve özgürlüklerin sınırlandırılması rejimini düzenleyen 13. maddesinde hak ve özgürlüklerin "ancak kanunla" sınırlanabileceği temel bir ilke olarak benimsenmiştir. Bunun yanında Anayasa'nın 20. maddesinin üçüncü fıkrasının üçüncü cümlesinde kişisel verilerin "ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla" işlenebileceği belirtilmiş, aynı fıkranın dördüncü cümlesinde ise kişisel verilerin korunmasına ilişkin esas ve usullerin "kanunla" düzenleneceği hüküm altına alınmıştır. Aynı şekilde Anayasa'nın 22. maddesinin ikinci fıkrasında "kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça" haberleşmenin engellenemeyeceği ve gizliliğine dokunulamayacağı düzenlenmiştir. Buna göre kişisel verilerin korunmasını isteme hakkına ve haberleşme hürriyetine yapılan müdahalelerde dikkate alınacak öncelikli ölçüt, müdahalenin kanuna dayalı olmasıdır.

119. Müdahalenin kanuna dayalı olması öncelikle şekli manada bir kanunun varlığını zorunlu kılar. Kişisel verilerin korunmasını isteme hakkına ve haberleşme hürriyetine müdahale edilmesi ancak yasama organınca kanun adı altında çıkarılan düzenleyici işlemlerde müdahaleye imkân tanıyan bir hükmün bulunması şartına bağlıdır. Ayrıca bu çerçevede belirtmek gerekir ki kişisel verilerin korunmasını isteme hakkına işleme suretiyle yapılan müdahaleler ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla yapıldığı takdirde kanunilik koşulu sağlanmış kabul edilir.

120. Diğer taraftan Anayasa'nın 2. maddesinde yer alan hukuk devleti ilkesinin bir gereği olarak kanunun kalitesi de kanunilik koşulunun sağlanıp sağlanmadığının tespitinde önem arz etmektedir. Zira hukuki güvenlik ile belirlilik ilkeleri hukuk devletinin ön koşullarındandır. Kişilerin hukuki güvenliğini sağlamayı amaçlayan hukuki güvenlik ilkesi hukuk normlarının öngörülebilir olmasını,

bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar (AYM, E.2013/39, K.2013/65, 22/5/2013; AYM, E.2014/183, K.2015/122, 30/12/2015, § 5) Belirlilik ilkesi ise yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olmasını, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesini ifade etmektedir (AYM, E.2013/39, K.2013/65, 22/5/2013; AYM, E.2010/80, K.2011/178, 29/12/2011). Buna göre bir hukuk devletinde temel hak özgürlüklere müdahalenin kanuna dayalı olması için şekli anlamda bir kanunun varlığı yanında o kanunun metninin de bireylerin, davranışlarının sonucunu öngörebilmesine imkân verecek şekilde belirlilik taşıması gerekir. Diğer bir ifadeyle müdahaleye imkân veren kanun yeterince belirli ve öngörülebilir olmalıdır (benzer yöndeki karar için bkz. Halime Sare Aysal [GK], B. No: 2013/1789, 11/11/2015, § 62).

121. Öte yandan Anayasa Mahkemesi, Anayasa'da temel hak ve özgürlüklerin sınırlandırılması gibi münhasıran kanunla düzenlenmesi öngörülen konularda kanunun söz konusu meselenin temel esaslarını, ilkelerini ve çerçevesini belirlemiş olmasını gerektirdiğini ancak yasama organının meselenin temel kurallarını saptadıktan sonra uzmanlık ve idare tekniğine ilişkin hususları yürütmeye bırakmasının yasama yetkisinin devri olarak yorumlanamayacağını kabul etmiştir (AYM, E.2014/133, K.2014/165, 30/10/2014). Bu bağlamda temel hak ve özgürlüklerin sınırlandırılmasına yönelik kanuni düzenlemelerde kanun koyucu tarafından temel esaslar, ilkeler ve çerçeve belirlendikten sonra diğer ayrıntıların düzenleyici işlemler ile belirlenebileceği kabul edilmiştir (Mehmet Koray Eryaşa, B. No: 2013/6693, 16/4/2015, § 63).

(b) İlkelerin Olaya Uygulanması

122. Anayasa Mahkemesinin Ferhat Kara kararında belirtildiği üzere suç isnadı altındaki kişilerin adli soruşturma ve kovuşturmalar kapsamında el konulan cihazlarında tespit edilen ByLock programına dair kurulum dosyası vs. dijital veriler dışında ByLock verileri esas olarak iki kaynağa dayanmaktadır. Bunlardan ilki MİT'in adli makamlara iletildiği ve adli makamların mahkeme kararlarıyla üzerinde inceleme yaptığı ByLock sunucusundan elde edilen verilerdir. İkincisi ise ByLock sunucusuna ait hedef IP'lere Türkiye'den hangi IP'lerden erişildiğine ilişkin mahkeme kararıyla BTK'dan elde edilen CGNAT (ByLock sunucusuna ait IP adreslerine hangi tarihte kaç defa bağlanıldığı bilgisi) kayıtlarıdır (Ferhat Kara, § 58). BTK, ByLock IP'sine bağlanan numaraların abonelerine ait şahıs kimlik bilgilerini tespit ederek Başsavcılık ve mahkemelere bildirmiştir (Ferhat Kara, §§ 32-58). Bu nedenle somut olayda müdahalenin kanuni dayanağının olup olmadığının

incelenmesi ByLock sunucusundan elde edilen veriler açısından ve ByLock verilerinin adli makamlara ulaştırılmasından sonraki süreç açısından olmak üzere iki başlıkta yapılmıştır.

(i) ByLock Sunucusundan Elde Edilen Veriler Açısından

123. Demokratik toplumlarda temel hak ve özgürlüklerin korunması amacıyla terör örgütleri gibi son derece karmaşık yapılarla etkin bir şekilde mücadele edilmesi ve bu tür örgütleri gizli yöntemlerle takip etmek amacıyla istihbarat organlarına ve onların yöntemlerine ihtiyaç duyulması kaçınılmazdır. Dolayısıyla terör örgütlerinin çökertilmesi amacıyla gizlilik taşıyan istihbarat yöntemleri kullanılarak bu örgütlerle ilgili bilgilerin toplanması ve analiz edilmesi demokratik toplumlardaki önemli bir ihtiyaca karşılık gelmektedir. Zira istihbarat birimlerinin elde ettikleri bu bilgiler vasıtasıyla demokratik anayasal düzene yönelik tehditlerin tespit edilmesi ve bunlara karşı önlemler alınması söz konusu olabilir (Ferhat Kara, § 130).

124. FETÖ/PDY'nin örgütlenmesi ve faaliyetleri öteden beri toplumda tartışma konusu olmakla birlikte özellikle 2013 yılı sonrasında soruşturma mercileri ve devletin güvenlik birimleri bu yapılanmanın millî güvenlik üzerinde tehdit oluşturduğunu değerlendirmeye başlamıştır. Bu bağlamda bilhassa 17-25 Aralık soruşturmaları ve MİT tırlarının durdurulması, bu yapılanmanın faaliyetlerinin Hükûmeti devirmeyi amaçladığı yönünde soruşturma mercileri ve yargı organlarınca yapılan değerlendirmelerin temel dayanakları arasındadır. Yine bu yapılanmayla bağlantılı olduğu değerlendirilen yargı mensupları eliyle açılan/yürütülen birçok davanın da örgütün başta Türk Silahlı Kuvvetleri olmak üzere kamu kurumlarında ve sivil toplumun farklı alanlarında etkinliğini sağlama veya artırma gayesine yönelik olduğu çok sayıda soruşturma/kovuşturma belgesinde ifade edilmiştir. Bu süreçte kamu makamları da bir taraftan FETÖ/PDY'nin illegal yönünü ortaya koyan karar ve uygulamalarda bulunmuş, diğer taraftan yapılanmaya karşı bazı tedbirlere başvurmuştur (Ferhat Kara, § 131)

125. Devletin istihbarat organlarının FETÖ/PDY'nin ulusal güvenlik üzerinde oluşturduğu tehdidin yaklaşan bir tehlikeye dönüşmekte olduğunu değerlendirerek bu konuda istihbarat çalışmalarında bulunmuş olmasının hukukiliğinin veya yerindeliğinin takdiri Anayasa Mahkemesinin görevi olmadığı gibi eldeki bireysel başvurunun inceleme konusu da değildir. İlgili makamlardan gerekli önleyici tedbirleri almaları için terör tehdidinin fiilen gerçekleşmesini beklemeleri istenemez. Karmaşık yapısı ve uluslararası niteliğinin FETÖ/PDY ile ilgili olarak -darbe teşebbüsü öncesinde- istihbarat anlamında bazı çalışmalar yapılmasını zorunlu kıldığı anlaşılmaktadır. Nitekim 15 Temmuz darbe teşebbüsü millî güvenlik üzerinde FETÖ/PDY'den kaynaklanan tehdidin ne denli büyük olduğunu ve bunun -öncesinde alınan birtakım tedbirlere rağmen- ulusun varlığını ve

bütünlüğünü yok etmeye yönelik nasıl ağır bir tehlikeye dönüştüğünü göstermiştir (ayrıntılı açıklama ve değerlendirmeler için bkz. Aydın Yavuz ve diğerleri, §§ 12-25; 212-221; Ferhat Kara, § 132).

126. FETÖ/PDY'nin kamu kurum ve kuruluşlarındaki örgütlenmesinin, bunun yanı sıra başta eğitim ve din olmak üzere farklı sosyal, kültürel ve ekonomik alanlardaki faaliyetlerinin millî güvenlik üzerinde tehdit oluşturduğunun soruşturma mercileri ve devletin güvenlik birimlerince kabul edilmeye başlandığı süreçte MİT de kendi görev alanı çerçevesinde bu yapılanmanın faaliyetleriyle ilgili çalışmalarda bulunmuştur. Nitekim 2937 sayılı Kanun'un 4. maddesinin birinci fıkrasının (a) bendinde MİT'in Türkiye Cumhuriyeti'nin bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, anayasal düzenine ve millî gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkındaki millî güvenlik istihbaratını devlet çapında oluşturmak ve bu istihbaratı gerekli kuruluşlara ulaştırmakla yükümlü olduğu belirtilmiştir.

127. MİT tarafından yapılan çalışmalar kapsamında FETÖ/PDY mensuplarının örgütsel haberleşmelerinin sağlanması amacıyla geliştirildiği anlaşılan, ana sunucusu yurt dışında bulunan ByLock adlı mobil uygulama ve bu uygulamanın iletişim kurduğu sunucular olduğu tespit edilmiş; bunlar ayrıntılı teknik çalışmalara tabi tutulmuştur. Kendi görev alanı kapsamında MİT tarafından bu uygulamayla ilgili olarak yapılan çalışmalar adli soruşturma işlemi niteliğinde değildir. Zira 2937 sayılı Kanun'un 4. maddesinin birinci fıkrasının (i) bendinde MİT'in terörle mücadele konularında da her türlü teknik istihbarat usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplama, kaydetme, analiz etme, üretilen istihbaratı gerekli kuruluşlara ulaştırma görev ve yetkisine sahip olduğu düzenlenmiştir (Ferhat Kara, § 128).

128. 2937 sayılı Kanun'un 6. maddesinde; MİT'in bu görevlerini yerine getirirken gizli çalışma usul, prensip ve tekniklerini kullanabileceği, telekomünikasyon kanallarından geçen dış istihbarat, millî savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplayabileceği de hüküm altına alınmıştır. Dolayısıyla anılan Kanun'un ülkenin anayasal düzeninin korunması ve millî güvenliğin sağlanması amacı ile terör faaliyetlerinin eyleme dönüşmeden belirlenebilmesi için MİT'e ilgili kişi ve gruplar hakkında teknik yöntemlerle bilgi ve veri toplama, topladığı bu bilgileri analiz etme yetkisi verdiği görülmektedir.

129. 2937 sayılı Kanun'un 4. maddesinin birinci fıkrasının (a) bendinde MİT'in Türkiye Cumhuriyeti'nin bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, anayasal düzenine ve millî gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkındaki millî güvenlik istihbaratını devlet çapında oluşturmak ve bu istihbaratı gerekli

kuruluşlara ulařtırmakla yükümlü olduđu belirtilmiřtir. Aynı fıkranın (i) bendinde de terörle mücadele konularında da her türlü teknik istihbarat usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulařtırmak görev ve yetkisine sahip olduđu düzenlenmiřtir. MİT'in bu görevlerini yerine getirirken gizli çalışma usul, prensip ve tekniklerini kullanılabileceđi, telekomünikasyon kanallarından geöen dıř istihbarat, millî savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplayabileceđi aynı Kanun'un 6. maddesinde hüküm altına alınmıřtır. Anılan Kanun'un ülkenin anayasal düzeninin korunması ve ulusal güvenliđin sađlanması için terör faaliyetlerinin eyleme dönüşmeden belirlenebilmesi amacıyla MİT'e ilgili kiři ve gruplar hakkında teknik yöntemlerle bilgi ve veri toplama ve topladıđı bu bilgileri analiz etme yetkisi verildiđi görölmektedir. Bu bağlamda MİT'e 2937 sayılı Kanun'un 4. ve 6. maddeleri uyarınca yurt dıřında bulunan bilgisayar verilerini satın alma da dâhil olmak üzere terörle mücadele konusunda telekomünikasyon kanallarından terör suçlarıyla ilgili geöen bilgi, belge ve diđer tüm verileri her türlü teknik istihbarat yöntemlerini kullanmak suretiyle toplama, analiz etme ve bunları gerekli kuruluşlara ulařtırma yetkisi verilmiřtir. Buna göre ilgili düzenlemelerin yeterince açık, anlaşılabilir ve öngörülebilir olduđu, kanunilik ölçütünü karřıladıđı sonucuna varılmıřtır.

(ii) ByLock Verilerinin Adli Makamlara Ulařtırılmasından Sonraki Süreç Açısından

130. MİT tarafından ByLock iletiřim sistemine iliřkin dijital materyaller ve bu materyallere iliřkin düzenlenen teknik analiz raporunun Ankara Cumhuriyet Bařsavcılıđına iletilmesi üzerine bu ařamadan itibaren soruřturma iřlemleri 5271 sayılı Kanun'a göre yürütölmüřtür. Bu kapsamda söz konusu dijital materyaller üzerinde 5271 sayılı Kanun'un 134. maddesine göre inceleme, kopyalama, çözümleme iřlemi yapmak için Ankara Cumhuriyet Bařsavcılıđınca Ankara 4. Sulh Ceza Hâkimliđine talepte bulunulmuřtur. Anılan talep üzerine Ankara 4. Sulh Ceza Hâkimliđi "dijital materyaller üzerinde inceleme yapılması, kopya çıkarılması ve kopya üzerinde bilirkiři incelemesi yapıl[masına]" karar vermiřtir (Ferhat Kara, § 28).

131. Söz konusu mahkeme kararına dayalı olarak Ankara Cumhuriyet Bařsavcılıđı tarafından ByLock IP'sine bađlanan aboneliklere ait "ByLock abone listesi"nde yer alan abonelerin ByLock IP adreslerine kaç defa bađlandıđına dair raporlar (CGNAT verileri) BTK'dan talep edilmiřtir (Ferhat Kara, § 32). Bađlantı yapan GSM ve ADSL numaralarına ait abonelik bilgileri BTK tarafından Ankara Cumhuriyet Bařsavcılıđına iletilmiřtir. Ankara Cumhuriyet Bařsavcılıđından KOM Daire Bařkanlıđınca teslim alınan abonelik bilgileriyle "user ID_list" (kullanıcı listesi) tablosu oluşturulmuřtur (Ferhat Kara, § 35).

132. Yargıtay Ceza Genel Kurulunun 26/9/2017 tarihli ve E.2017/16.MD-956, K.2017/370 sayılı kararında da ByLock iletişim sistemindeki veri tespitlerinin 5271 sayılı Kanun'un 134. maddesi kapsamında kaldığı vurgulanmıştır (bkz. § 56). Anılan karara göre internet ortamında gerçekleştirilen iletişime ilişkin kayıtlar, bilgisayar kütüğünde kayıt altına alındığından bu iletişim kayıtları hakkında 5271 sayılı Kanun'un 134. maddesinin (1) numaralı fıkrası gereğince arama, kopyalama ve elkoyma koruma tedbirleri uygulanabilir. Yargıtaya göre 5271 sayılı Kanun'un 134. maddesindeki "bilgisayar kütükleri" ifadesi teknik anlamda sadece masaüstü ve dizüstü bilgisayarlarda bulunanları değil CD, DVD, flash disk, disket, hard disk vs. tüm çıkarılabilir bellekler, telefon vb. dijital tabanlı mobil cihazlar da dâhil olmak üzere herhangi bir bilgi işlem veya veri toplama araç ya da gerecinde bulunabilecek tüm dijital dosyaları kapsamaktadır.

133. Somut olayda Kayseri 3. Sulh Ceza Hâkimliğince 5271 sayılı Kanun'un 116., 127. ve 134. maddeleri uyarınca başvurunun ikametgâhında 6/9/2016 tarihinde arama yapılmasına, bulunan cep telefonu, bilgisayar, hard disk, hafıza kartları, sim kartları vb. kayıt tutma özelliği bulunan her türlü dijital materyallere el konulmasına, ele geçirilecek kayıtlardan kopya alınmasına, kayıtların çözümlenerek metin hâline getirilmesine karar verilmiştir. Kayseri 1. Sulh Ceza Hâkimliğinin 2/11/2016 tarihli kararı ile 5271 sayılı Kanun'un 135. maddesi uyarınca başvurunun telefon numarasının 1/10/2013 ile 1/10/2016 tarihleri arasında iletişim kayıtları ve hangi baz istasyonlarından servis aldığı tespitine karar verilmiştir. Ayrıca Kayseri İl Emniyet Müdürlüğü KOM Şube Müdürlüğüne 6/2/2017 tarihinde Yeni ByLock CBS Sorgu Sonucu Raporu sunulmuş ve başvurucuya ait telefonun hat numarası ve IMEI numarası bilgilerine göre başvurunun telefonuna ByLock haberleşme programını yükleyerek (4397) ID kullanıcı numarasıyla kullandığının anlaşıldığı belirtilmiştir. Aynı şekilde Ankara Cumhuriyet Başsavcılığının 2016/180056 sayılı soruşturma dosyasından elde edilen bilgi kapsamında başvurucuya ait ByLock kullanımını gösteren ByLock Tespit ve Değerlendirme Tutanağı sunulmuştur. Bölge Adliye Mahkemesi kararıyla da başvurunun kullandığı GSM hattının ve bu hatlarda kullanılan IMEI numaralarının HTS kayıtları ile ByLock'un belirlenen IP numaralarına bağlantı yaptığı tarih, saat ve baz istasyonu gösterir HTS kayıtları BTK'dan temin edilmiştir.

134. Buna göre başvurunun ByLock haberleşme programını kullanmasına yönelik iletişim bilgilerinin tespit edilmesi şeklindeki müdahalenin hâkim kararına dayalı olarak öncelikle 5271 sayılı Kanun'un 134. maddesi kapsamında dijital materyallere el konulması, ele geçirilecek kayıtlardan kopya alınması, kayıtların çözümlenerek metin hâline getirilmesi hükmü çerçevesinde, daha sonra aynı Kanun'un 135. maddesi uyarınca ve hâkim kararıyla başvurunun telefon numarasının iletişim

kayıtları ve hangi baz istasyonlarından servis aldığıın tespiti şeklinde gerçekleştirildiği anlaşılmaktadır. 5271 sayılı Kanun'un 134. ve 135. maddelerinde öngörülen arama, dijital verilere elkoyma, telefon kayıtlarının tespitine yönelik açık ve detaylı kurallar ortaya konmuş; kamu makamlarının değerlendirme yetkisinin kapsam ve sınırları net bir şekilde belirtilmiştir. Aynı şekilde uygulanan tedbirlerin hangi suçlar için verileceği ve süresi ile kayıtların saklanma ve imha edilme şartları belirlenmiştir. Ayrıca söz konusu tedbirlerin acil hâllerde dahi keyfiliğe karşı yeterli bir güvence sağlayacak şekilde hâkim onayına tabi tutulması öngörülmüştür. Buna göre müdahalenin dayanağı olan kanun hükümleri, hak ve özgürlüğe yöneltilen müdahalelerin sınırlarını yeterli açıklıkta ortaya koyan, erişilebilir ve öngörülebilir niteliktedir. Yapılan değerlendirmeler neticesinde 5271 sayılı Kanun'un anılan maddelerinin kanunilik ölçütünü karşıladığı sonucuna varılmıştır (benzer yöndeki değerlendirmeler için bkz. Mehmet Seyfi Oktay [GK], B. No: 2013/6367, 10/12/2015, § 53; Rıdvan Bayram, B. No: 2013/1171, 9/9/2015, § 43; C.E., B. No: 2016/436, 12/9/2019, § 49; Günay Dağ ve diğerleri, B. No: 2013/1631, 17/12/2015, § 136).

(2) Meşru Amaç

135. Anayasa'nın 13. maddesinde temel hak ve hürriyetlerin yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak sınırlandırılabilmesi hüküm altına alınmıştır. Ancak Anayasa'nın 20. maddesinin üçüncü fıkrasında kişisel verilerin korunmasını isteme hakkına yönelik sınırlama ve müdahaleler yönünden özel bir sınırlama sebebine yer verilmediği görülmektedir. Bununla birlikte Anayasa Mahkemesinin yerleşik içtihadına göre özel sınırlama nedeni öngörülmemiş hak ve özgürlüklerin de o hak ve özgürlüğün doğasından kaynaklanan bazı sınırları bulunmaktadır. Ayrıca Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevler, özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebilir (birçok karar arasından bkz. AYM, E.2014/177, K.2015/49, 14/5/2015).

136. Anayasa'nın 20. maddesinin üçüncü fıkrasındaki düzenlemelerden kişisel verilerin korunmasını isteme hakkına sınırlama getirilebileceği anlaşılmaktadır. Ancak fıkrada tüketici sayıda bir sebepler ya da meşru amaçlar listesine yer verilmemiştir. Kimliği belirli veya belirlenebilir bir gerçek kişi hakkındaki tüm bilgileri ifade eden kişisel veri kavramının kullanım alanlarının oldukça geniş olması nedeniyle her bir kullanım alanı yönünden farklı sınırlama sebeplerinin ya da meşru amaçların kabul edilmesi kaçınılmazdır. Bu durumda hangi alanda kişisel verilerin korunmasını isteme hakkına yönelik sınırlama getirildiği ya da müdahale edildiğine bağlı olarak sınırlama nedeni ya da meşru amaç değişebilir. Buna göre yapılacak incelemede kişisel verilerin korunmasını isteme hakkının bu hakkın doğasından kaynaklanan bazı sınırlarının bulunduğu dikkate alındığında her dosya ve

başvuru kapsamında işin doğasından kaynaklanan sınırlama sebebinin tespit edilmesi ve bunun meşru bir sebep olarak kabul edilip edilemeyeceğinin değerlendirilmesi gerekir. Öte yandan Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin de bu hakka sınır teşkil edebileceği kabul edilmelidir.

137. Türkiye Cumhuriyeti'ne yönelik terör faaliyetlerinin tespiti ve önlenmesi devletin temel ödevlerindedir. Bu açıdan terör örgütlerinin ve bunların faaliyetlerinin tespiti, bu suretle suç işlenmesinin önlenmesi amacıyla kişisel verilerin korunması hakkının sınırlandırılmasının meşru bir amaca dayandığı sonucuna ulaşılmaktadır.

138. Diğer taraftan Anayasa'nın 22. maddesinin ikinci fıkrasına göre millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak haberleşme hürriyeti sınırlandırılabilir. Somut olayda terör örgütüyle mücadele, suç işlenmesinin önlenmesi ve suç kanıtlarının elde edilmesi amacıyla yönelik olarak 5271 sayılı Kanun'un 134. ve 135. maddeleri uyarınca ve hâkim kararlarıyla başvurucunun ByLock haberleşme programını kullanmasına yönelik iletişim bilgileri tespit edilmiştir. Dolayısıyla müdahalenin Anayasa'nın 22. maddesinde gösterilen suç ve suçlularla mücadele bağlamında kamu düzeni ve güvenliğinin sağlanmasına yönelik meşru bir amaç taşıdığı anlaşılmaktadır.

(3) Demokratik Toplum Düzeninin Gereklere Uygunluk ve Ölçülülük

(a) Genel İlkeler

139. Temel hak ve özgürlüklere yönelik bir müdahalenin demokratik toplum düzeninin gereklere uygun kabul edilebilmesi için zorunlu bir toplumsal ihtiyacı karşılaması ve ölçülü olması gerekir. Açıktır ki bu başlık altındaki değerlendirme, sınırlamanın amacı ile bu amacı gerçekleştirmek üzere başvurulan araç arasındaki ilişki üzerinde temellenen ölçülülük ilkesinden bağımsız yapılamaz. Çünkü Anayasa'nın 13. maddesinde demokratik toplum düzeninin gereklere aykırı olmama ve ölçülülük ilkesine aykırı olmama biçiminde iki ayrı kritere yer verilmiş olmakla birlikte bu iki kriter bir bütünün parçaları olup aralarında sıkı bir ilişki vardır (Ferhat Üstündağ, B. No: 2014/15428, 17/7/2018, § 45).

140. Müdahaleyi oluşturan tedbirin zorunlu bir toplumsal ihtiyacı karşıladığının kabul edilebilmesi için amaca ulaşmaya elverişli olması, başvurulabilecek en son çare ve alınabilecek en hafif önlem olarak kendisini göstermesi gerekmektedir. Amaca ulaşmaya yardımcı olmayan veya ulaşılmak

istenen amaca nazaran bariz bir biçimde ağır olan bir müdahalenin zorunlu bir toplumsal ihtiyacı karşıladığı söylenemeyecektir (Ferhat Üstündağ, § 46).

141. Orantılılık ise sınırlamayla ulaşılmak istenen amaç ile başvuru sınırlama tedbiri arasında dengesizlik bulunmamasına işaret etmektedir. Diğer bir ifadeyle orantılılık, bireyin hakkı ile kamunun menfaatleri veya müdahalenin amacı başkalarının haklarını korumak ise diğer bireylerin hak ve menfaatleri arasında adil bir dengenin kurulmasına işaret etmektedir. Dengeleme sonucu müdahalede bulunulan hakkın sahibine terazinin diğer kefesinde bulunan kamu menfaati veya diğer bireylerin menfaatine nazaran açıkça orantısız bir külfet yüklendiğinin tespiti hâlinde orantılılık ilkesi yönünden bir sorunun varlığından söz edilebilir (Ferhat Üstündağ, § 46).

142. Bununla birlikte kişisel verilerin korunmasını isteme hakkına yönelik sınırlama ve müdahalelerin demokratik toplum düzeninin gereklerine uygun olabilmesi için zorunlu bir toplumsal ihtiyacı karşılaması yetmez. Zira Anayasa'nın 20. maddesinin üçüncü fıkrasının ikinci cümlesinde "Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar." denilerek kişisel verilerin korunmasını isteme hakkına yönelik sınırlamalar ya da müdahaleler bakımından bazı özel güvencelere de yer verilmiştir. Bunlar, kişisel verilerin korunmasını isteme hakkına yönelik sınırlama ya da müdahalelerin demokratik bir toplum düzeninin gereklerine uygun olabilmesi için Anayasa koyucu tarafından özel olarak belirlenmiş güvenceler mahiyetindedir.

143. Ayrıca Anayasa'nın 20. maddesinin üçüncü fıkrasının birinci cümlesinde "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir." denildikten sonra ikinci cümlesinde bu hakkın yukarıda belirtilen bazı özel güvenceleri de kapsadığı belirtilmiştir. İkinci cümlede geçen "...de kapsar" ibaresi birinci cümle ile birlikte değerlendirildiğinde Anayasa koyucunun iradesinin demokratik bir toplumda kişisel verilerin korunmasını isteme hakkı kapsamında tanınması gereken güvenceleri ikinci cümlede sayılanlarla sınırlı tutmak olmadığı anlaşılmaktadır. Nitekim uluslararası belgeler ve karşılaştırmalı hukuk metinleri incelendiğinde kişilere Anayasa'da sayılan güvencelerin tanınmasının yanında bazı durumlarda bu güvencelerin daha geniş olan bazı ilkelerin parçası olarak öngörüldüğü, bazı durumlarda Anayasa'daki özel güvencelerin detaylarının ortaya konulduğu, bazı durumlarda ise ilave bazı güvencelere yer verildiği görülmektedir (bkz. §§ 58-60). Anayasa değişikliğinin uluslararası belgelere ve karşılaştırmalı hukuk metinlerine atıf yapan gerekçesi (bkz. § 93), Anayasa'nın 20. maddesinin üçüncü fıkrasının birinci cümlesindeki kişisel verilerin korunmasını isteme hakkına ilişkin genel hüküm, ikinci cümlesinde güvencelerin tüketici şekilde sayılmamış

olması dikkate alındığında Anayasa'nın 13. maddesindeki sınırlama ölçütlerinden demokratik toplum düzeninin gereklerine uygunluk ölçütü kapsamında yorum yapılırken uluslararası belgelerde ve karşılaştırmalı hukuk metinlerinde yer alan ilkelerin de her başvurunun somut koşullarına uygun düştüğü ölçüde değerlendirmeye alınabileceği sonucuna ulaşılmaktadır.

144. Bu bakımdan kamu müdahalesine konu olan kişisel verinin niteliğine bağlı olarak aşağıdaki ek güvencelerin bir kısmının veya tamamının sağlanması gerekebilir:

i. Kişisel verilerin işlenmesi süreci şeffaf bir şekilde gerçekleştirilmeli ve bunun bir gereği olarak da süreçle ilgili olarak veri sahipleri önceden bilgilendirilmelidir. Bu bilgilendirmenin -somut olayın özelliklerine uygun düştüğü ölçüde- kişisel verilerin işlenmesinin hukuki dayanağı ve işlemenin amaçları, işlenecek verilerin kapsamı, verilerin saklanacağı süre, veri sahibinin hakları, işlemenin sonuçları ve verilerin muhtemel yararlanıcıları hususlarını kapsamaması gerekir. Bilgilendirmenin mutlaka belli şekilde yapılması şart olmayıp şeffaflığı sağlamak bakımından bireylere, kişisel verilerin işlenmesine ilişkin süreçten yukarıda belirtilen kapsamda haberdar olma imkânı sağlayan uygun bir yöntem tercih edilebilir.

ii. Kişisel verilerin işlenmesi süreci şeffaf bir şekilde gerçekleştirilmeli, bunun bir gereği olarak veri sahiplerine kişisel verilerine erişim imkânı tanınmalı ve bu imkânın kolayca kullanılması için gerekli tedbirler alınmalıdır.

iii. Kişisel veriler doğru ve güncel bir biçimde tutulmalı, yanlış olan, güncel olmayan ya da hukuka aykırı olarak tutulan kişisel verilerin gecikmeksizin düzeltilmesi veya silinmesi için gerekli tedbirler alınmalı, bu kapsamda kişilere talepte bulunma hakkı tanınmalıdır.

iv. Kişisel verilerin gizliliğinin sağlanması ve bu verilerin yetkisiz veya kanuna aykırı olarak işlenmemesi, kaybolmaması, imha edilmemesi ya da zarar görmemesi için uygun teknik ve yapısal tedbirler öngörülmesi; bu tedbirler etkili bir biçimde uygulanmalıdır.

v. Kişisel verilerin korunmasını isteme hakkına yönelik sınırlama ya da müdahalenin orantılı kabul edilebilmesi için kişisel veriler sınırlama ya da müdahale amacı için gerekenden daha uzun süre saklanmamalıdır.

vi. Kişisel verilerin korunmasını isteme hakkına yönelik sınırlamanın ya da müdahalenin orantılı kabul edilebilmesi için veri sahibine, menfaatlerini zedeleyen bir yöntem olan kişisel verilerden veri sahibi hakkında otomatik sonuçlar çıkarılması yöntemine kural olarak başvurulmamalıdır. İşin niteliğinin bu yöntemin uygulanmasını gerektirdiği durumlarda ise veri dezavantajlı durumunu

hafifletmek amacıyla söz konusu yönteme dayanmayan bir karar alınmasını talep etme hakkı gibi usule ilişkin güvenceler sağlanmalıdır.

vii. Kişisel verilerin korunmasını isteme hakkına yönelik sınırlamanın ya da müdahalenin orantılı kabul edilebilmesi için işlenecek veya herhangi bir şekilde yararlanılacak veriler ulaşılmak istenen amaçla sınırlı olmalı, bu amacı aşacak şekilde sınırlama ya da müdahaleye izin verilmemelidir. Ayrıca kişilere hakkın sağladığı güvencelerin ihlali hâlinde yargı yoluna başvurma imkânı tanınmalı ve yargılamanın adil bir şekilde yapılmasını temin için usule ilişkin güvenceler sağlanmalıdır.

viii. Din veya felsefi inanç, ırk veya etnik köken, cinsel yönelim, bazı örgütlenmelere üyelik, sağlık, genetik veriler, biyometrik veriler ve mahkûmiyet verileri gibi hassas kişisel verilerin söz konusu olduğu durumlarda kişisel verilerin korunmasını isteme hakkı kural olarak sınırlanmamalı ya da bu hakka müdahale edilmemelidir. Sınırlama ve müdahalenin zorunlu olduğu bazı istisnai hâllerde ise bunun kişiler üzerinde ortaya çıkaracağı sonuçların ağırlığı ve kişiler hakkında ayrımcı uygulamalara yol açma tehlikesi dikkate alınarak kişisel verilerin korunmasına ilişkin güvenceler daha katı uygulanmalıdır.

145. Millî güvenlik, kamu düzeni, devletin mali menfaatleri, suçların önlenmesi, ilgili kişinin veya başkalarının hak ve özgürlüklerinin korunması, istatistikî veya bilimsel araştırma gibi amaçlarla yapılan sınırlama ve müdahaleler bakımından kimi durumlarda işin niteliğinin zorunlu kılması hâlinde kişisel verilerin korunması hakkına yönelik sınırlama ve müdahaleler yönünden ortaya çıkan özel güvencelere istisna getirilebilir. Ancak bu durumda bile Anayasa'nın 13. maddesinde tüm temel hak ve özgürlükler yönünden öngörülmüş olan sınırlama ölçütlerinin asgari standartlarına uyulmalıdır. Diğer bir ifadeyle istisna hâlleri bulunsa bile sınırlama ve müdahale kanuna dayanmalı, sınırlama sebeplerini barındırmalı ya da meşru amaç takip etmeli, demokratik toplum düzeninin gereği olarak zorunlu bir toplumsal ihtiyacı karşılamalı ve ölçülü olmalıdır. Bu durumda anılan ölçütler özel güvenceler dikkate alınmaksızın yorumlanır. Bununla birlikte bir istisna hâlinin varlığı özel güvencelerin tamamının otomatik olarak ortadan kalkmasına neden olmaz. Böyle bir durumun varlığı hâlinde işin niteliği dikkate alınarak her bir özel güvence yönünden istisna getirilmesinin zorunlu olup olmadığı değerlendirilmelidir.

(b) İlkelerin Olaya Uygulanması

146. Başvurucunun kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine yönelik müdahalenin amacının FETÖ/PDY'nin ve faaliyetlerinin tespiti, bu suretle suç işlenmesinin önlenmesidir. ByLock haberleşme programı verilerinin elde edilmesi, tahlil edilmesi ve soruşturma makamlarına aktarılmasının, yine başvurucunun bu programı kullanıp kullanmadığının ortaya

konulması gayesiyle iletişim kayıtları ve hangi baz istasyonlarından servis aldığı tespit edilmesinin belirtilen amaca ulaşılması yönünden elverişli bir araç olduğu açıktır.

147. İkinci olarak müdahalenin zorunlu bir toplumsal ihtiyaca karşılık gelip gelmediği ve bu çerçevede başvurucaunun ByLock verilerinin elde edilmesinin, iletişim kayıtları ile baz hareketliliğinin temin edilmesinin son çare olarak başvuruca olan bir araç olup olmadığı incelenmelidir.

148. Günümüzde terör, tüm dünyada demokratik topluma ve bireylerin şiddetten arı bir ortamda yaşamını sürdürmesine yönelik en ciddi tehditlerin başında gelmektedir. Terör örgütleri çoğunlukla belli bir ülkenin coğrafi hudutlarıyla sınırlı olarak faaliyet göstermemekte, uluslararası mahiyeti bulunan bir küresel güvenlik sorunu olarak karşımıza çıkmaktadır. Kendine özgü yapısı ve gizlilik esasına dayanan çalışma yöntemi, sivil organizasyonları örgütsel amaçlarına ulaşabilmek amacıyla kullanmadaki maharetiyle FETÖ/PDY çok sayıda ülkede kendine alan açmayı başarmış ve faaliyetleri dünyanın her yanına yayılmış en organize ve tehlikeli terör örgütlerinden biridir. Bu sebeple örgütün millî güvenlik üzerinde oluşturduğu tehdit ve tehlikenin bertaraf edilebilmesi bakımından yalnızca ceza soruşturması bağlamında soruşturma makamlarına tanınan yetkilerle iktifa edilmesinin yeterli olmayacağı açıktır. Dolayısıyla örgütün faaliyetlerinin ve mensuplarının tespiti için gizlilik taşıyan istihbarat tekniklerine başvurulması kaçınılmaz hâle gelmiştir. Anayasa'nın 20. ve 22. maddeleri istihbarat yöntemleri kullanılmak suretiyle haberleşme hürriyeti ile kişisel verilerin korunmasını isteme hakkına müdahalede bulunulmasını yasaklamamaktadır. Hiçbir demokratik devlet, kendi varlığına yönelmiş tehditler karşısında hareketsiz kalmaz. Devletin demokratik toplum düzenini, anayasal nizamı ve meşru hükûmeti zorla ortadan kaldırmayı hedefleyen kişi ve yapılara karşı mücadele etme yetki ve görevinin bulunduğu tartışma götürmez bir gerçektir. Bu açıdan gizli istihbarat teknikleri kullanılmak suretiyle ByLock verilerine ulaşılmasının demokratik toplum düzeninin gereklerine aykırı olduğu söylenemez.

149. Nitekim örgütün faaliyetlerinin ve üyelerinin tespitinde ByLock sunucusundan elde edilen veriler oldukça önemli bir role sahip olmuştur. Örgütün birçok üst düzey yöneticisi ByLock verilerinin analizi neticesinde tespit edilebilmiştir. FETÖ/PDY'nin kendine özgü yapısı gözetildiğinde daha hafif bir aracın tercihiyle aynı sonucun elde edilmesinin mümkün olamayacağı da ortadadır. Şu hâlde istihbarat yöntemleri kullanılmak suretiyle ByLock sunucusunda bulunan verilerin elde edilmesinin ve bunların yargılama makamlarına aktarılmasının demokratik toplum düzeninin gereklerine uygun olma kriterini taşıdığı sonucuna ulaşılmaktadır.

150. Üçüncü olarak kişisel verilerin korunması hakkının mahiyetinden kaynaklanan özel güvencelerin sağlanıp sağlanmadığı incelenmelidir. Ancak öncelikle somut olayda kişisel verilerin

korunmasını isteme hakkına yönelik sınırlama ve müdahaleler yönünden ortaya çıkan özel güvencelere istisna getirilmesi gereken bir durumun bulunup bulunmadığı irdelenmelidir.

151. Anayasa'nın 13. maddesi ve 14. maddesinin birinci fıkrasında yer alan "Anayasada yer alan hak ve hürriyetlerden hiçbirisi, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmayı ve insan haklarına dayanan demokratik ve lâik Cumhuriyeti ortadan kaldırmayı amaçlayan faaliyetler biçiminde kullanılamaz." şeklindeki hüküm uyarınca demokratik devlet düzeni ve millî güvenliğin sağlanması, terörle mücadele amacıyla kişisel verilerin korunması hakkının özel güvencelerine istisna getirilmesi mümkündür. Nitekim konuyla ilgili uluslararası hukuk belgelerinde de millî güvenliğin korunması ve terörle mücadele amacıyla kişisel verilerin korunmasını isteme hakkının özel güvencelerine istisna getirilebileceği kabul edilmiştir (bkz. §§61, 66). 6698 sayılı Kanun'un "istisnalar" kenar başlıklı 28. maddesinde suçla mücadele ve millî güvenlik amacıyla kişisel verilerin önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi istisnalar arasında sayılmıştır (bkz. § 48).

152. Olayda başvurucunun kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine yönelik müdahalenin amacının millî güvenliğin sağlanması ve suç işlenmesinin önlenmesiyle yakından ilgili olduğu açıktır. Kamu makamları örgütün faaliyetlerinin ve mensuplarının tespiti ve örgütün varlığının kamu düzeni ve millî güvenlik üzerinde doğurduğu risklerin önlenmesi için yalnızca adli soruşturma yapmakla yetinilmesinin yetersiz kalacağı kanaatine ulaşmış, bu nedenle ceza soruşturması kapsamında bulunmayan birtakım gizli istihbarat tekniklerine başvurmuşlardır. Bu yönleme başvurulmasında, örgütün Türkiye Cumhuriyeti'nin egemenliğine yönelik olarak oluşturduğu ve 15 Temmuz 2016 tarihinde yaşanan darbe teşebbüsüyle görünür hâle gelen tehdidin büyüklüğünün etkili olduğu inkâr edilemez. Dolayısıyla somut olaydaki müdahalenin kişisel verilerin korunmasını isteme hakkı yönünden ortaya çıkan özel güvencelere istisna getirilmesini gerektiren türden olduğu açıktır.

153. Bununla birlikte bir istisna hâlinin varlığı özel güvencelerin tamamının otomatik olarak ortadan kalkmasını gerektirmez. Somut olayın özelliği gözetildiğinde (1) sınırlı olma, (2) uzun süre saklanmama, (3) veri sahibiyle ilgili olarak otomatik sonuç doğurmama ve (4) etkili yargısal denetim güvencelerinin sağlanması gerektiği değerlendirilmiştir. Bu durumda somut olayda bunların sağlanıp sağlanmadığı ele alınmalıdır.

154. ByLock verilerinin istihbarat tekniklerinin kullanılması suretiyle elde edilmesi suretiyle kişisel verilerin korunmasını isteme hakkına ve haberleşme hürriyetine yönelik olarak gerçekleşen müdahalenin örgütün faaliyetlerinin ve mensuplarının açığa çıkarılması ve örgütün çökertilmesi amacının ötesine geçtiğine dair bir bilgi bulunmamaktadır. Başvurucunun da bu verilerin amacı ile

sınırlı olarak kullanılmadığı yönünde bir şikâyeti bulunmamaktadır. ByLock haberleşme programından elde edilen veriler yalnızca bu örgüte üye olma suç isnadıyla yürütülen ceza yargılamasında kullanılmıştır. Dolayısıyla başvurucuya ait kişisel verilerin amacı dışında kullanılmadığı anlaşılmaktadır.

155. Başvurucunun ByLock haberleşme programını kullandığına ilişkin veriler ile BTK'dan temin edilen telefon ve internet kullanımı, bağlandığı IP adresleri bilgisi, gönderdiği mail, mesaj ve arama kayıt bilgilerinin yargılama süresince saklanması öngörülmektedir. Yargılamada delil olarak kullanılan kişisel verilerin yargılama süresince saklanması adil yargılanma hakkı bakımından gerekli olduğu açıktır. Başvurucunun da saklama süresine uyulmadığı yönünde hiçbir şikâyeti bulunmamaktadır. Dolayısıyla saklama süresinin gereğinden uzun olmadığı değerlendirilmiştir.

156. ByLock sunucusundan elde edilen veriler başvuru ile ilgili olarak otomatik sonuç doğurmamış; öncelikle kolluk birimlerince ardından da yargı mercilerince değerlendirilip analizi yapıldıktan sonra bu veriler, başvuru aleyhine soruşturma konusu edilmiştir. Son olarak başvuru, aleyhine yürütülen yargılamada bunlara yönelik itirazlarını derece mahkemeleri önünde dile getirebilmiş, derece mahkemeleri ise başvuru itirazlarını ayrıntılı olarak değerlendirmiş ve karşılamıştır. Dolayısıyla başvuru "Genel İlkeler" bölümünde değinilen kişisel verilerin korunmasını isteme hakkına yönelik özel güvenceler bakımından bir şikâyeti bulunmadığı gibi bu güvencelere yönelik herhangi bir eksiklik tespit edilmemiş, başvuru yargısal güvencelerden de yararlanabildiği kanaatine varılmıştır.

157. Açıklanan gerekçelerle Anayasa'nın 20. ve 22 maddelerinde güvence altına alınan özel hayata saygı hakkı içinde yer alan kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ihlal edilmediğine karar verilmesi gerekir.

C. Diğer İhlal İddiaları

158. Başvuru; ByLock programının kullanıldığı tarih itibarıyla bu programı kullanmanın suç olmadığını, sonradan suç olarak ilan edilmesinin işlendiği zaman suç olmayan bir fiile dayanılarak mahkûm olması anlamına geldiğini, bunun suç ve cezaların kanuniliği ilkesini ihlal ettiğini ileri sürmüştür.

159. Anayasa Mahkemesine başvuru konusu olaylarla ilgili delilleri sunmak suretiyle olaylar hakkındaki iddiaları temellendirmek ve dayanılan Anayasa hükmünün ihlal edildiği iddiasına dair açıklamalarda bulunarak hukuki iddialarını ortaya koymak başvurucuya düşer. Başvurucunun kamu gücünün işlem, eylem ya da ihmali nedeniyle ihlal edildiğini ileri sürdüğü hak ve özgürlük ile

dayanılan Anayasa hükümlerini, ihlal gerekçelerini, dayanılan deliller ile ihlale neden olduğu ileri sürülen işlem veya kararların neler olduğunu başvuru dilekçesinde belirtmesi şarttır. Başvuru dilekçesinde kamu gücünün ihlale neden olduğu iddia edilen işlem, eylem ya da ihmeline dair olayların tarih sırasına göre özeti yapılmalı; bireysel başvuru kapsamındaki hak ve özgürlüklerden hangisinin hangi nedenle ihlal edildiği ve buna ilişkin gerekçeler ve deliller açıklanmalıdır (Veli Özdemir, B. No: 2013/276, 9/1/2014, §§ 19, 20; Ünal Yiğit, B. No: 2013/1075, 30/6/2014, §§ 18, 19).

160. Başvurucunun ByLock kullanma fiilinden değil örgüt üyeliği suçundan mahkûm olduğu vurgulanmalıdır. Bu açıdan derece mahkemesinin ByLock kullanımını suç olarak nitelendirmesi söz konusu değildir. Derece mahkemesi, başvurucunun ByLock kullanmış olmasını örgüt üyeliği suçunu işlediğinin bir delili olarak kabul etmiştir. Bu sebeple başvurucunun suç ve cezaların kanuniliği ilkesinin ihlal edildiği iddiasının incelenebilir bir temeli bulunmamaktadır. Başvurucu suç ve cezaların kanuniliği ilkesinin anayasal koruma alanına temas eden başkaca bir iddia da öne sürmemiştir. Bu itibarla suç ve cezaların kanuniliği ilkesinin ihlal edildiğine ilişkin şikâyetin temellendirilemediği kanaatine varılmıştır.

161. Açıklanan gerekçelerle başvurunun bu kısmının açıkça dayanaktan yoksun olması nedeniyle kabul edilemez olduğuna karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. 1. Kişi hürriyeti ve güvenliği hakkının ihlal edildiğine ilişkin iddianın süre aşımı nedeniyle **KABUL EDİLEMEZ OLDUĞUNA,**

2. Özel hayata saygı hakkı içinde yer alan kişisel verilerin korunmasını isteme hakkının ve haberleşme hürriyetinin ihlal edildiğine ilişkin iddianın **KABUL EDİLEBİLİR OLDUĞUNA,**

3. Diğer ihlal iddialarının açıkça dayanaktan yoksun olması nedeniyle **KABUL EDİLEMEZ OLDUĞUNA,**

B. Anayasa'nın 20. maddesinde yer alan kişisel verilerin korunmasını isteme hakkının ve 22. maddesinde düzenlenen haberleşme hürriyetinin **İHLAL EDİLMEDİĞİNE,**

C. Yargılama giderlerinin başvurucu üzerinde **BIRAKILMASINA,**

D. Kararın bir örneğinin Adalet Bakanlığına **GÖNDERİLMESİNE 17/9/2020 tarihinde OYBİRLİĞİYLE** karar verildi.

Anayasa Mahkemesi - Ertan Erçikti (3) Kararı (2018/14040)

Ertan Erçikti (3), B. No: 2018/14040, 30/6/2021

Başvuru, internet trafik bilgilerinin mevzuatta belirlenen süreden fazla tutulması ve bu bilgilerin yargı makamına gönderilmesi nedeniyle özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkının ihlal edildiği iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

BİRİNCİ BÖLÜM

KARAR

ERTAN ERÇIKTI BAŞVURUSU (3)

(Başvuru Numarası: 2018/14040)

Karar Tarihi: 30/6/2021

R.G. Tarih ve Sayı: 24/8/2021-31578

BİRİNCİ BÖLÜM

KARAR

Başkan: Hasan Tahsin GÖKCAN

Üyeler: Hicabi DURSUN; Muammer TOPAL, Yusuf Şevki HAKYEMEZ, İrfan FİDAN

Raportör: Ali KOZAN

Başvurucu: Ertan ERÇIKTI

Vekili: Av. Serap BEDİR

I. BAŞVURUNUN KONUSU

1. Başvuru, internet trafik bilgilerinin mevzuatta belirlenen süreden fazla tutulması ve bu bilgilerin yargı makamına gönderilmesi nedeniyle özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkının ihlal edildiği iddiasına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 2/5/2018 tarihinde yapılmıştır.
3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.
4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.
5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.
6. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık, görüşünü bildirmiştir.
7. Başvurucu, Bakanlığın görüşüne karşı beyanda bulunmuştur.

III. OLAY VE OLGULAR

8. Başvuru formu ve eklerinde ifade edildiği şekliyle olaylar özetle şöyledir:
9. Eski emniyet müdürü olan başvurucu hakkında terör örgütüne üye olma suçundan yürütülen yargılamada İstanbul 14. Ağır Ceza Mahkemesi (Mahkeme) tarafından 3/11/2017 tarihinde mahkûmiyet kararı verilmiş olup istinaf incelemesinde olan karar kesinleşmemiştir. Anılan yargılamada Mahkeme, Bilgi Teknolojileri ve İletişim Kurumundan (Kurum/BTK) 4/5/2017 tarihinde başvurucunun cep telefonu numarasına ait internet trafik bilgilerini istemiştir. Kurum tarafından 2014-2015 tarih aralığına ait internet trafik bilgileri 4/7/2017 tarihinde Mahkemeye gönderilmiştir.
10. Başvurucu 10/10/2017 tarihli dilekçesi ile Kurum ve cep telefonu ile erişim sağlayan üç şirket (Şirketler) hakkında İstanbul Cumhuriyet Başsavcılığına (Başsavcılık) suç duyurusunda bulunmuştur. Başvurucu şikâyetinde; Mahkemenin talebi üzerine Kurumun gönderdiği internet trafik bilgilerinin 2014-2015 tarih aralığına ait olduğunu belirtmiştir. Mevzuata göre şirketlerin internet trafik bilgilerini en fazla bir yıl saklayabileceğini, gönderilen bilgilerin çoktan silinmiş olması gerektiğini ancak Kurumun yaklaşık üç yıl sonra bilgileri mahkemeye göndererek suç işlediğini iddia etmiştir. Trafik bilgisi adı altında temin edilen bilgilerin Anayasa ile teminat altına alınan ifade ve haberleşme hürriyeti ile kişisel verilerin korunmasını isteme hakkı gibi birçok temel hakla doğrudan ilgili olduğunu, bu bilgilerin Kurum tarafından gönderilmesinin mevzuata aykırılık teşkil ettiğini belirten başvurucu, şüphelilerin cezalandırılmasını talep etmiştir.

11. Başsavcılık; kişisel verileri hukuka aykırı olarak işleme, ele geçirme, yayma ve verileri yok etmeme suçlarından yaptığı soruşturma sonucunda 8/11/2017 tarihinde kovuşturma yapılmasına yer olmadığına karar vermiştir. Kararın gerekçesinde;

i. Başvurucu hakkında 2014 yılında soruşturmaya başlandığı ve bu kapsamda 2015 yılı içinde çeşitli zamanlarda soruşturma makamı tarafından başvurucuya ait bir kısım internet trafik bilgilerinin Kurumdan ve Şirketlerden temin edildiği belirtilmiştir. Yargılama aşamasında da bu bilgilerle bağlantılı olarak ByLock gibi yeni ortaya çıkan deliller çerçevesinde internet trafik bilgilerinin Kurumdan talep edildiği, dolayısıyla Mahkeme tarafından talep edilen bir kısım bilgilerin zaten daha önce soruşturma makamı tarafından temin edildiğinin anlaşıldığı ifade edilmiştir.

ii. Ayrıca mevzuat hükümleri uyarınca Şirketlerin trafik bilgisini bir yıl saklama yükümlülüğünün olduğu, Kurum için ise böyle bir yükümlülük ve süre belirlenmediği, Şirketlerin anılan süre sonunda bu bilgileri silmesine ya da yok etmesine ilişkin bir yükümlülük ve bir yaptırım öngörülmediği belirtilmiştir. Bu durumun Şirketlerin her zaman Kuruma talep ettiği bilgileri sağlamakla yükümlü olması, mevzuatta Şirketlere ve Kuruma verileri yok etme yükümlülüğü öngörülmemesi hususuyla birlikte değerlendirildiğinde atılı suçun yasal unsurlarının oluşmadığı ifade edilmiştir. Öte yandan şikâyete konu bilgilerin ve bu bağlamda delillerin hukuka uygun olup olmadığının da yargılamayı yapan mahkeme ve nihai olarak denetim yapan yüksek mahkemeler tarafından değerlendirilebileceği vurgulanmıştır.

12. Başvurucunun bu karara karşı yapmış olduğu itiraz, İstanbul 8. Sulh Ceza Hâkimliği tarafından 14/3/2018 tarihinde Başsavcılık kararının usul ve yasaya uygun olduğu gerekçesiyle reddedilmiştir.

13. Nihai karar, başvurucuya 2/4/2018 tarihinde tebliğ edilmiştir.

14. Başvurucu 2/5/2018 tarihinde bireysel başvuruda bulunmuştur.

15. Kurumun 14/7/2020 tarihli bilgilendirme yazısında; Kurumun 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemeleri Kanunu'nun 135. maddesi kapsamında adli amaçlı iletişimin tespit edilmesi, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasına yönelik işlemleri süresinde ve eksiksiz şekilde yerine getirmekle yükümlü olduğu, ilgili mevzuat kapsamında elde edilen verileri de ilgisine göre talep eden kurumlara, mahkemeye ve Cumhuriyet başsavcılıklarına iletmenin görevi kapsamında olduğu vurgulanmıştır. IP arasında bir iletişim olup olmadığı yönünde istenilen bilgilerin 5271 sayılı Kanun'un 135. maddesinde yer alan iletişimin tespiti kavramı içinde olduğu, kamu kurum ve kuruluşlarından gelen her türlü bilgi, belge ve kayıtların Kurum tarafından bilgi güvenliği kriterlerine uygun olarak arşivlenmesinin mevzuat gereği olduğu belirtilmiştir. İlgili

mevzuat hatırlatılarak elektronik haberleşme sektörüne ilişkin her türlü düzenleme, yetkilendirme ve denetlemeye ilişkin Telekomünikasyon İletişim Başkanlığının tüm yetkilerinin Kuruma devrildiği, telekomünikasyon yoluyla yapılan iletişime ait verilerin adli soruşturma ve kovuşturma kapsamında talep hâlinde ilgili dosyaya gönderilmek üzere saklanması bir zorunluluk olduğu, bu durumun özel hayata saygı hakkını ve haberleşme hürriyetini ihlal etmediği ifade edilmiştir.

IV. İLGİLİ HUKUK

A. İlgili Mevzuat

16. İlgili hukuk (ulusal mevzuat, yargı kararları, uluslararası düzenlemeler ve Avrupa İnsan Hakları Mahkemesi (AİHM) kararları) için bkz. E.Ü. [GK], B. No: 2016/1310, 17/9/2020, §§ 22-51; Bestami Eroğlu [GK], B. No: 2018/23077, 17/9/2020, §§ 42-83.

17. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Kapsam" kenar başlıklı 2. maddesi şöyledir:

"Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır."

18. 6698 sayılı Kanun'un "Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi" kenar başlıklı 7. maddesi şöyledir:

"(1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.

(2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır.

(3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir."

19. 6698 sayılı Kanun'un "İstisnalar" kenar başlıklı 28. maddesinin ilgili kısmı şöyledir:

" (1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:

...

ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi..."

20. 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'nun "Kurumun görev ve yetkileri" kenar başlıklı 6. maddesinin ilgili kısmı şöyledir:

"(1) Kurumun görev ve yetkileri şunlardır:

...

c) Abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak.

...

ı) Elektronik haberleşmeyle ilgili olarak, işletmeciler, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden ihtiyaç duyacağı her türlü bilgi ve belgeyi almak ve gerekli kayıtları tutmak, Bakanlık tarafından elektronik haberleşme sektörüne yönelik strateji ve politikaların belirlenmesinde ihtiyaç duyulanları, talebi üzerine Bakanlığa iletmek...."

21. 5809 sayılı Kanun'un "İşletmecilerin hak ve yükümlülükleri" kenar başlıklı 12. maddesinin ilgili kısmı şöyledir:

"(1) İşletmeci, Kurum düzenlemeleri ve yetkilendirmesinde öngörülen şartlara uygun olarak yetkilendirildiği kapsamdaki elektronik haberleşme hizmetini sunma hakkına sahiptir.

(2) Kurum, işletmecilere sektörün ihtiyaçları, uluslararası düzenlemeler, teknolojide meydana gelen gelişmeler gibi hususları gözeterek aşağıdaki hususlar başta olmak üzere, mevzuat doğrultusunda yükümlülükler getirebilir:

...

d) Kişisel veri ve gizliliğin korunması.

e) Tüketicinin korunması.

f) Kuruma bilgi ve belge verilmesi.

g) Kanunlarla yetkili kılınan ulusal kurumlarca yasal dinleme ve müdahalenin yapılmasına teknik olanak sağlanması.

...

(4) İşletmecilerin hak ve yükümlülükleri ile ilgili usul ve esaslar Kurumca belirlenir.

(5) İşletmeciler, elektronik haberleşme sistemleri üzerinden millî güvenlikle ve 5397 ve 5651 sayılı kanunlar ve ilgili diğer kanunlarda getirilen düzenlemelerle ilgili taleplerin karşılanmasına yönelik teknik alt yapıyı, elektronik haberleşme sistemini hizmete sunmadan önce kurmakla yükümlüdür. Halen elektronik haberleşme hizmeti sunan işletmeciler de; söz konusu teknik alt yapıyı, Kurum tarafından belirlenecek süre içerisinde aynı şartlarla ve tüm harcamaları kendilerine ait olmak üzere kurmakla yükümlüdürler."

22. 5809 sayılı Kanun'un "Kişisel verilerin işlenmesi ve gizliliğinin korunması" kenar başlıklı 51. maddesinin ilgili kısmı şöyledir:

"(1) Kişisel verilerin işlenmesinde; hukuka ve dürüstlük kurallarına uygun olması, doğru ve gerektiğinde güncel olması, belirli, açık ve meşru amaçlar için işlenmesi, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ile işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi ilkelerine uyulur.

(2) Elektronik haberleşmenin ve ilgili trafik verisinin gizliliği esas olup, ilgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi yasaktır.

...

(10) Bu Kanun kapsamında sunulan hizmetlere ilişkin olarak;

a) Soruşturma, inceleme, denetleme veya uzlaşmazlığa konu olan kişisel veriler ilgili süreç tamamlanıncaya kadar,

b) Kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtları iki yıl,

c) Kişisel verilerin işlenmesine yönelik abonelerin/kullanıcıların rızalarını gösteren kayıtlar asgari olarak abonelik süresince, saklanır. Veri kategorileri ile haberleşmenin yapıldığı tarihten itibaren bir yıldan az ve iki yıldan fazla olmamak üzere verilerin saklanma süreleri yönetmelikle belirlenir..."

23. 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un "Tanımlar" kenar başlıklı 2. maddesinin ilgili kısmı şöyledir:

"...

d) Erişim: Bir internet ortamına bağlanarak kullanım olanağı kazanılmasını,

e) Erişim sağlayıcı: Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri,

...

ı) Kurum: Bilgi Teknolojileri ve İletişim Kurumunu,

...

j) Trafik bilgisi: Taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini,

k) Veri: Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri...ifade eder"

24. 5651 sayılı Kanun'un "Erişim sağlayıcının yükümlülükleri" kenar başlıklı 6. maddesinin ilgili kısmı şöyledir:

"(1) Erişim sağlayıcı;

...

b) Sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla,

...

d) (Ek bent: 06/02/2014-6518 S.K./89. md) Kurumun talep ettiği bilgileri talep edilen şekilde Kuruma teslim etmekle ve Kurum tarafından bildirilen tedbirleri almakla, yükümlüdür..."

25. 30/11/2007 tarihli ve 26716 sayılı Resmî Gazete'de yayımlanan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik'in "Erişim sağlayıcının yükümlülükleri" kenar başlıklı 8. maddesinin ilgili kısmı şöyledir:

"...

b) Sağladığı hizmetlere ilişkin olarak, Başkanlığın Kanunla ve ilgili diğer mevzuatla verilen görevlerini yerine getirebilmesi için; erişim sağlayıcı trafik bilgisini bir yıl saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşturan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte muhafaza etmek ve gizliliğini temin etmekle, internet trafik izlemesinde Başkanlığa gerekli yardım ve desteği sağlamakla, faaliyet belgesinde yer alan Başkanlığın uygun gördüğü bilgileri talep edildiğinde bildirmekle ve ticari amaçla internet toplu kullanım sağlayıcılar için belirli bir IP bloğundan sabit IP adres planlaması yapmakla ve bu bloktan IP adresi vermekle...Yükümlüdür."

26. 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun "Kişisel verilerin kaydedilmesi" kenar başlıklı 135. maddesi şöyledir:

"(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.

(2) Kişisel verinin, kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır."

27. 5237 sayılı Kanun'un "Verileri hukuka aykırı olarak verme veya ele geçirme" kenar başlıklı 136. maddesi şöyledir:

"(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır."

28. 5237 sayılı Kanun'un "Verileri yok etmeme" kenar başlıklı 138. maddesi şöyledir:

"(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.

(2) (Ek fıkra: 21/02/2014-6526 S.K./5. md) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.

"

29. 6/1/1982 tarihli ve 2577 sayılı İdari Yargılama Usulü Kanunu'nun "İptal ve tam yargı davaları" kenar başlıklı 12. maddesinin ilgili kısmı şöyledir:

"İlgililer haklarını ihlal eden bir idari işlem dolayısıyla Danıştaya ve idare ve vergi mahkemelerine doğrudan doğruya tam yargı davası veya iptal ve tam yargı davalarını birlikte açabilecekleri gibi ilk önce iptal davası açarak bu davanın karara bağlanması üzerine, bu husustaki kararın veya kanun yollarına başvurulması halinde verilecek kararın tebliği veya bir işlemin icrası sebebiyle doğan zararlardan dolayı icra tarihinden itibaren dava süresi içinde tam yargı davası açabilirler..."

30. 11/1/2011 tarihli ve 6098 sayılı Türk Borçlar Kanunu'nun "Kişilik haklarının zedelenmesi" kenar başlıklı 58. maddesi şöyledir:

"Kişilik hakkının zedelenmesinden zarar gören, uğradığı manevi zarara karşılık manevi tazminat adı altında bir miktar para ödenmesini isteyebilir.

Hâkim, bu tazminatın ödenmesi yerine, diğer bir giderim biçimi kararlaştırabilir veya bu tazminata ekleyebilir; özellikle saldırıyı kınayan bir karar verebilir ve bu kararın yayımlanmasına hükmedebilir."

B. İlgili Yargı Kararları

31. Ankara 13. İdare Mahkemesinin 14/2/2020 tarihli ve E.2018/2355, K.2020/426 sayılı kararı şöyledir:

"Dava dosyasının incelenmesinden, 'Silahlı Terör Örgütüne Üye Olma' suçundan tutuklu bulunan davacının, aynı suçtan yargılandığı Ağır Ceza Mahkemesi'nin HTS kayıtlarının davalı idareden istenmesi üzerine anılan kayıtların Mahkemeye sunulduğu, bunun üzerine davacı tarafından HTS kayıtlarının süresinden fazla tutulmasında ve gönderilmesinde davalı idarenin hizmet kusuru bulunduğundan manevi tazminatın idareye başvuru tarihinden itibaren işleyecek yasal faiziyle birlikte tazmini istemiyle bakılan davanın açıldığı anlaşılmaktadır.

İdarenin hukuki sorumluluğundan söz edilebilmesi için ortada bir zararın bulunması ve bunun idareye yüklenebilen bir işlem veya eylemden doğması, başka bir deyişle zararlı idari faaliyet arasında uygun illiyet bağının bulunması gerektiği, idarenin sorumluluğu hizmet kusuru ve kusursuz sorumluluk ilkelerine dayandığı, ister hizmet kusuru, isterse kusursuz sorumluluk ilkelerine dayandırılınsın, idarenin tazmin borcunun doğabilmesi için bir zararın mevcudiyeti, zarara yol açan eylemin veya işlemin idareye yüklenebilir nitelikte olması ve zarar ile eylem veya işlem arasında illiyet bağının bulunması zorunlu kıldığı, bu şartlardan birinin yokluğu idarenin sorumluluğunu ortadan kaldıracaktır. Diğer bir ifadeyle, ortada bir zarar yoksa veya meydana gelen zararın idari eylem veya işlemle ilgisi bulunmuyorsa, idari faaliyet zararın gerçek nedenini, illiyetini teşkil etmiyorsa, arada illiyet bağı mevcut değilse veya zarara yol açan eylem veya işlem idareye yüklenebilir nitelikte değilse, idarenin sorumluluğu ortadan kalkmaktadır.

Uyuşmazlıkta, yukarıda aktarılmış mevzuat hükümlerinin dava konusu olayla birlikte değerlendirilmesinden, telekomünikasyon yoluyla yapılan iletişime ait verilerin adli soruşturma ve kovuşturmalarda Cumhuriyet Başsavcılıkları ile Mahkemeler tarafından istenilmesi halinde davalı idare tarafından bu taleplerin yerine getirilebilmesi için saklanması yasal zorunluluk olduğu anlaşılmaktadır.

Bu durumda, yasaların uygulanmasından kaynaklanan dava konusu olayda, davalı idareye atfedilebilecek bir hizmet kusurunun bulunmadığı, yine somut olayda davalı idarenin kusursuz sorumluluğuna da gidilemeyeceği anlaşıldığından, davacının manevi tazminat talebinin reddi

gerektiđi sonu ve kanaatine varılmıřtır." (Benzer gereke iin bkz. Ankara 23. İdare Mahkemesinin 3/10/2019 tarihli ve E.2018/741, K.2019/352 sayılı kararı).

32. Ankara 2. İdare Mahkemesinin 19/2/2019 tarihli ve E.2019/1169, K.2019/2537 sayılı kararı řoyledir:

"Uyuřmazlıkta, yukarıda yer verilen mevzuat hukmlerine gre, davalı kurumun, 5271 sayılı Ceza Muhakemesi Kanunu'nun 135. maddesi kapsamında, adli amalı iletiřimin tespit edilmesi, dinlenmesi, sinyal bilgilerin deđerlendirilmesi ve kayda alınmasına ynelik iřlemlerin eksiksiz ve herhangi bir aksamaya sebep vermeyecek řekilde yerine getirmekle ykml olduđu, faaliyet alanıyla ilgili kamu kurum ve kuruluřları ile iřletmecilerden gelen her trl bilgi, belge ve kayıtların bilgi gvenliđi kriterlerine uygun olarak arřivlenmesinin de davalı kurumun grevleri arasında bulunduđu, yine davalı kurumun kiřisel bilgilerin iřlenmesi ve gizliliđinin korunmasına iliřkin gerekli dzenlemeleri ve denetlemeleri yapmak ve elektronik haberleřme sektrne ynelik olarak, mill gvenlik, kamu dzeni veya kamu hizmetinin geređi gibi yrtlmesi amacıyla mevzuatın ngrdđ tedbirleri almak ile ykml olduđu, telekomnikasyon yoluyla yapılan iletiřime ait verilerin iletiřim operatrleri ve kamu kurumlarınca en fazla ne kadar sre saklanabileceđi noktasında ise; iřletmeciler (GSM operatrleri) tarafından, davalı kurumun denetleme faaliyeti kapsamında veya yargı mercileri tarafından yapılan soruřturma, kovuřturma, inceleme veya uyuřmazlıkla ilgili durumların bildirilmesi halinde, 5809 sayılı Kanun'da belirtilen iřlendikleri ama iin gerekli sre kadar muhafaza edilmesi ilkesi geređi telekomnikasyon yoluyla yapılan iletiřime ait her trl verinin iki yıllık sre ile bađlı kalınmaksızın saklanabilmesinin mmkn olduđu grlmřtr.

Olayda yukarıda yer verilen bilgiler ıřıđında, davalı kurumun denetim faaliyetlerini yerine getirme noktasında herhangi bir hizmet kusurunun bulunmadıđı aık olup, davacı hakkında Tekirdađ 2. Ađır Ceza Mahkemesince yrtlen ceza yargılamasında, iřletmeci (GSM operatr) tarafından CGNAT kayıtlarının hatalı olarak oluřturulduđuna dair herhangi bir tespit de bulunmadıđı, aksine davacının FET/PDY terr rgtnn rgt ii kriptolu haberleřme sistemi olarak kullanılan ByLock programına girdiđinin tespit edilmesi sonucunda mahkumiyetine hkmedildiđi dikkate alındıđında, olayda tazmini gereken herhangi bir zararın varlıđından sz edilemeyeceđi, bu itibarla, davalı kurumun, davacı tarafından uđranıldıđı ileri srlen manevi zararın tazmini noktasında sorumluluđunun bulunmadıđı anlařılmıřtır."

33. Ankara Blge İdare Mahkemesi 7. İdari Dava Dairesinin 25/6/2020 tarihli ve E.2020/753, K.2020/627 sayılı kararı řoyledir:

"Dava, davacı tarafından, belirli bir süre kullandığını belirttiği telefon hattıyla ilgili olarak tüm HTS, GSM kayıtları ve trafik verilerinin ilgili yasal hükümlere aykırı bir şekilde süresi dışında saklandığı, zamanında silinmediği dolayısıyla hizmet kusurunda bulunulduğundan bahisle maddi ve manevi tazminata hükmedilmesi istemiyle açılmıştır.

İdare Mahkemesince, uyuşmazlık konusu tazminat talebine esas olan ve silinmesi istenilen kayıtların; ceza hukukunda delil olarak kullanıldığı ve tespit niteliğinde olduğu, idari bir işlem niteliğinde olmadığı ve idari davaya konu edilemeyeceğinden buna bağlı olarak istenen tazminat talebinin de esasının incelenme olanağı bulunmadığı gerekçesiyle incelenmeksizin ret kararı verilmiştir.

Anayasanın 125. maddesinin 1. fıkrasında; idarenin her türlü eylem ve işlemlerine karşı yargı yolunun açık olduğu belirtildikten sonra son fıkrasında; idarenin kendi eylem ve işlemlerinden doğan zararı ödemekle yükümlü olduğu hükme bağlanmıştır.

2577 sayılı İdari Yargılama Usulü Kanunu'nun 2. maddesinde, idari dava türleri; idari işlemler hakkında yetki, şekil, sebep, konu ve maksat yönlerinden biri ile hukuka aykırı olduklarından dolayı açılan iptal davaları; idari işlem ve eylemlerden dolayı kişisel hakları doğrudan muhtel olanlar tarafından açılan tam yargı davaları ve kamu hizmetlerinden birinin yürütülmesi için yapılan her türlü idari sözleşmelerden dolayı açılan davalar olarak sayılmış, idari yargının idari eylem ve işlemlerin hukuka uygunluğunun denetimini yapmakla görevli olduğu kurala bağlanmıştır.

İdare Mahkemesince, tazminat talebine esas olan ve silinmesi istenilen kayıtların; ceza hukukunda delil olarak kullanıldığı ve tespit niteliğinde olduğu, idari bir işlem niteliğinde olmadığı ve idari davaya konu edilemeyeceği gerekçesiyle davanın incelenmeksizin reddine karar verilmişse de; davacı tarafından kişisel verilerinin yasal hükümlere aykırı olarak süresi dışında saklandığı, zamanında silinmemesinin hizmet kusuru oluşturduğu iddialarıyla görülmekte olan davanın açıldığı, dolayısıyla bu işlemler nedeniyle Anayasanın ilgili hükmü ve 2577 sayılı Kanun çerçevesinde tam yargı davası açılmasına engel bulunmadığı anlaşıldığından, İdare Mahkemesince işin esasının incelenerek bir karar verilmesi gerekirken, davanın incelenmeksizin reddi yolunda verilen kararda hukuki isabet bulunmamaktadır.

Açıklanan nedenlerle, istinaf başvurusunun kabulü ile istinaf başvurusuna konu idare mahkemesi kararının kaldırılmasına; dava dosyasının yeniden bir karar verilmek üzere mahkemesine gönderilmesine...oybirliğiyle karar verildi."

34. İstanbul Anadolu 7. Asliye Hukuk Mahkemesinin 15/10/2020 tarihli ve E.2017/454, K.2020/212 sayılı kararının ilgili kısmı şöyledir:

"Dava konusunun maddi ve manevi tazminat talebine yönelik olduğu, davacının, davalı (erişim sağlayıcı şirket) kurum tarafından kendisine ait olan bilgileri, yok etmeyerek özel hayatın gizliliğini ihlal ettiğini, bilgileri mahkeme ve savcılık ile paylaştığını, bu nedenle tutuklandığını, bundan ise davalının sorumlu olduğunu belirtmiş ise de; TBK'nın 49. maddesine göre, kusurlu ve hukuka aykırı bir fiille başkasına zarar veren, bu zararı gidermekle yükümlüdür. Aynı yasanın 58. maddesinde de 'Şahsiyet hakkı hukuka aykırı bir şekilde tecavüze uğrayan kişi, uğradığı manevi zarara karşılık manevi tazminat namıyla bir miktar para ödenmesini dava edebilir.' düzenlemesine yer verilmiştir.

Somut olayda davalının hukuka aykırı ve kusurlu bir eylemi bulunmadığı, buna göre sorumlu tutulmasının söz konusu olmadığı, sadece Ağır Ceza Mahkemesi tarafından istenen bilgileri gizli olarak mahkemeye gönderdiği anlaşıldığından davanın reddine dair aşağıdaki şekilde hüküm kurulması netice ve kanaatine varılmıştır."

C. Uluslararası Hukuk

35. Avrupa İnsan Hakları Sözleşmesi'nin (Sözleşme) "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesinin (1) numaralı fıkrası şöyledir:

"(1) Herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir."

36. Avrupa İnsan Hakları Mahkemesi (AİHM) Sözleşme'nin 13. maddesi uyarınca temel hak ve özgürlüklerin ulusal düzeyde korunması için etkili bir başvuru yolunun var olması gerektiğini belirtmektedir. AİHM'e göre Sözleşme'nin 13. maddesi yetkili ulusal makamlar tarafından Sözleşme kapsamına giren bir şikâyetin esasının incelenmesine izin veren ve uygun telafi yöntemi sunan bir iç hukuk yolunun sağlanmasını gerekli kılmaktadır. Ayrıca bu hukuk yolunun teoride olduğu kadar pratikte de etkili bir yol olması gerekmektedir (İlhan/Türkiye [BD], B. No: 22277/93, 27/6/2000, § 97; Kudla/Polonya [BD], B. No: 30210/96, 26/10/2000, § 157; Özpinar/Türkiye, B. No: 20999/04, 19/10/2010, § 82).

37. AİHM, ayrıca açık bir şekilde faydasız olmayan belirli bir hukuk yolunun başarı ihtimali hakkındaki şüphelerin tek başına, söz konusu hukuk yolundan faydalanmamanın geçerli bir nedeni olmadığını yinelemektedir (Akdıvar ve diğerleri/Türkiye, B. No: 21893/93, 16/9/1996, § 71; Van Oosterwijck/Belçika, B. No: 7654/76, 6/11/1980, § 37).

V. İNCELEME VE GEREKÇE

38. Mahkemenin 30/6/2021 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Adli Yardım Talebi Yönünden

39. Yargılama giderlerini karşılayacak gelirin olmadığı ifade eden başvuru adli yardım talebinde bulunmuştur.

40. Anayasa Mahkemesinin Mehmet Şerif Ay (B. No: 2012/1181, 17/9/2013, §§ 22-27) kararında belirtilen ilkeler dikkate alınarak geçimini önemli ölçüde güçleştirmeksizin yargılama giderlerini ödeme gücünden yoksun olduğu anlaşılan başvuruçunun açıkça dayanaktan yoksun olmayan adli yardım talebinin kabulüne karar verilmesi gerekir.

B. Özel Hayata Saygı Hakkının İhlal Edildiğine İlişkin İddia

1. Başvuruçunun İddiaları ve Bakanlık Görüşü

41. Başvuruçusu; Kurumun internet trafik bilgilerini kendi bünyesinde tutmadığını, soruşturma veya kovuşturma sürecinde talep hâlinde erişim sağlayıcı Şirketlerden temin ederek ilgili makama gönderdiğini, mevzuata göre erişim sağlayıcı Şirketlerin bu bilgileri en fazla iki yıl saklayabileceklerini belirtmiştir. Mahkemenin talebi üzerine kullandığı cep telefonu numarasına ilişkin 2014-2015 tarih aralığına ait internet trafik bilgilerini Kurumun 4/7/2017 tarihinde gönderdiğini, bu durumun ticari amaçla kurulmuş Şirketlerin ilgili mevzuatta belirtilen süreler geçmiş olsa bile hukuka aykırı olarak internet trafik bilgilerini tutmaya devam ettiklerini gösterdiğini iddia etmiştir. Kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceğini, kendisine ait verilerin depolanmasına ilişkin rızasının olmadığını, mevzuata göre Şirketlerin kişisel verileri süresiz olarak saklama yetkilerinin mevcut olmadığını vurgulamıştır. Asıl sorunun bu ülkenin insanlarına ait kişisel verilerin özel şirketlerce depolanmaya devam edilmesi olduğunu, bu nedenle bireysel başvuru amacının üçüncü kişilerin cezalandırılması olmadığını ve durum tespiti yapılmasına yönelik olduğunu, bu ciddi sorunun tazminat davasıyla da çözülmesinin beklenemeyeceğini ifade etmiştir. Konunun önemini gözetilen özenli bir soruşturma yapılmayarak yeterli gerekçe sunulmadan şikâyetinin reddedildiğini belirten başvuruçusu, özel hayata saygı ve kişisel verilerin korunmasını isteme hakkı ile adil yargılanma hakkının ihlal edildiğini ileri sürmüştür.

42. Bakanlık görüşünde; ilgili mevzuat hatırlatıldıktan sonra başvuruçunun şikâyetinin Başsavcılık tarafından ayrıntılı olarak incelendiği ve ihlal teşkil ettiği iddia olunan müdahalenin yasal dayanağının ortaya konulduğu ileri sürülmüştür. Başvuruçusu hakkındaki soruşturmaya 2014 yılında başlandığı ve bu kapsamda 2015 yılı içinde çeşitli zamanlarda soruşturma makamı tarafından başvuruçusuya ait bir kısım internet trafik bilgilerinin Kurumdan ve Şirketlerden talep ve temin edildiği belirtilmiştir. Yargılama aşamasında da mahkeme tarafından talep edilen bir kısım bilgilerin zaten daha önce soruşturma makamı tarafından temin edilen bilgilerin devamı mahiyetinde ve ByLock gibi yeni ortaya çıkan deliller çerçevesindeki bilgileri kapsadığı, dolayısıyla başvuruçusu hakkında

tutulmaya devam edilen verilerin daha önceden zaten BTK ve ilgili kurumlardan talep edilmiş veriler olduğunun açık olduğu vurgulanmıştır. Sonuç olarak başvuru hakkındaki kişisel verilerin hakkında yürütülen soruşturma ve kovuşturmanın bir gereği olarak mevzuatta belirtilen gerekçeler nedeniyle tutulmaya devam edildiği, bu hususun da yürütülen soruşturmada açıkça ortaya konulduğu gözetildiğinde kişisel verilerin korunması hakkına yönelik meşru olmayan bir müdahalenin bulunmadığı gerekçesiyle başvurunun açıkça dayanaktan yoksun olması nedeniyle reddedilmesi gerektiği ifade edilmiştir.

43. Bakanlık görüşüne karşı başvuru vekili beyanında; Bakanlık görüşünde atıfta bulunulan kanun maddelerinin başvuru hakkındaki internet verilerinin iki yıl geçtikten sonra mahkemeye gönderilemeyeceğini hüküm altına aldığını vurgulamıştır. Bakanlık görüşünde; başvurucuya konu internet trafik kayıtlarının 2014 yılındaki soruşturmada istendiği iddiasının gerçeği yansıtmadığını, 2014 yılında soruşturma savcısı tarafından yalnızca HTS (arama, arandı, mesaj aldı/attı) ve GPRS kayıtlarının talep edildiğini, kişinin ByLock sunucusuna kaç defa bağlantı yaptığını gösteren CGNAT bilgilerinin ülke çapında ByLock soruşturmalarının başladığı 15/7/2016 tarihinden sonra talep edildiğini belirtmiştir. Bu kapsamda başvurucuya ait anılan bilgilerin de ilk defa 2017 yılında mahkemeye gönderildiğini zira bu verilerin 2014 yılında zaten mevcut olmadığını iddia etmiştir. Bu veriler 2014 yılındaki taleplerin devamı niteliğinde olsaydı sonradan ortaya çıkan ve masa başında üretildiğini düşündüğü bu CGNAT verilerinin de 2014 yılında mahkemelere gelmesi gerektiğini, mevzuatta bu verilerin en fazla bir yıl tutulacağı emredici olarak düzenlenmiş olmasına rağmen imha edilmediğini vurgulamıştır.

2. Değerlendirme

44. Anayasa Mahkemesi, olayların başvurucular tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Şikâyetin özü, internet trafik bilgilerinin yasada belirtilen süreden fazla tutulmasına ve bu bilgilerin yargı makamlarına gönderilmesine yöneliktir. İnternet trafik bilgilerinin belirli bir gerçek kişi hakkındaki bilgi kapsamında olduğu gözetildiğinde bu bilgilere erişilmesinin, bunların kullanılmasının ve işlenmesinin özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkı yönünden değerlendirilmesi gerekmiştir.

45. Anayasa'nın 148. maddesinin üçüncü fıkrası ile 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 45. maddesinin (1) numaralı fıkrası gereği bireysel başvuru yoluyla Anayasa Mahkemesine başvurabilmek için olağan kanun yollarının tüketilmiş olması gerekir. Temel hak ve özgürlüklere saygı, devletin tüm organlarının

anayasal ödevi olup bu ödevin ihmal edilmesi nedeniyle ortaya çıkan hak ihlallerinin düzeltilmesi idari ve yargısal makamların görevidir. Bu nedenle temel hak ve özgürlüklerin ihlal edildiği iddialarının öncelikle derece mahkemeleri önünde ileri sürülmesi, bu makamlar tarafından değerlendirilmesi ve bir çözüme kavuşturulması esastır (Ayşe Zıraman ve Cennet Yeşilyurt, B. No: 2012/403, 26/3/2013, § 16).

46. Anayasa Mahkemesine bireysel başvuru, iddia edilen hak ihlallerinin derece mahkemelerince düzeltilmemesi hâlinde başvurulabilecek ikincil nitelikte bir başvuru yoludur. Bireysel başvuru yolunun ikincil niteliği gereği Anayasa Mahkemesine bireysel başvuruda bulunabilmek için öncelikle olağan kanun yollarının tüketilmesi zorunludur. Bu ilke uyarınca başvuru yolunun şikâyetini öncelikle ve süresinde yetkili idari ve yargısal mercilere usulüne uygun olarak iletmesi, bu konuda sahip olduğu bilgi ve kanıtlarını zamanında bu makamlara sunması, aynı zamanda bu süreçte dava ve başvurusunu takip etmek için gerekli özeni göstermiş olması gerekir (Ayşe Zıraman ve Cennet Yeşilyurt, § 17).

47. Tüketilmesi gereken başvuru yollarının ulaşılabilir olması yanında telafi kabiliyetini haiz olması ve tüketildiğinde başvuru yolunun şikâyetlerini gidermede makul başarı şansı tanınması gerekir. Dolayısıyla mevzuatta bu yollara yer verilmesi tek başına yeterli olmayıp uygulamada da etkili olduğunun gösterilmesi ya da en azından etkili olmadığı kanıtlanmamış olması gerekir (Ramazan Aras, B. No: 2012/239, 2/7/2013, § 29). Bununla birlikte soyut olarak makul bir başarı sunma kapasitesi bulunan bir başvuru yolunun uygulamada başarıya ulaşmayacağına dair şüphe, o başvuru yolunun tüketilmemesini haklı kılmaz. Özellikle sonradan oluşturulan ve henüz uygulaması olmayan başvuru yollarının bu kapsamda değerlendirilmesi gerekir (Ramazan Korkmaz, B. No: 2016/36550, 19/7/2017, § 33, Remziye Duman, B. No: 2016/25923, 20/7/2017, § 35).

48. Öte yandan bir ihlal iddiasına ilişkin olarak başvurulabilecek birden fazla etkili başvuru yolunun bulunması durumunda, kural olarak başvuru yolunun aynı amacı taşıyan başvuru yollarının tamamının tüketilmesi beklenemez (S.S.A., B. No: 2013/2355, 7/11/2013, § 30). Bununla birlikte tüketilen hukuk yolunun başvuru yolunun amacına uygun başarı şansı bulunan bir yol olması gerekir. Buradan hareketle somut olay bağlamında mevzuat incelendiğinde kişisel verilerin hukuka aykırı olarak paylaşılması ve verilerin kanunlarda belirtilen süre sonunda yok edilmemesi 5237 sayılı Kanun kapsamında suç olarak düzenlenmiştir. Diğer yandan kişisel veri kapsamındaki internet trafik bilgilerinin mevzuatta belirtilen süre sonunda yok edilmemesi ve hukuka aykırı şekilde kullanılmasının somut olayın koşullarına göre kişilik haklarına yönelik bir eylem olduğu kabul edilebilir. Bu durumdan kaynaklı olarak kişilik hakkının zedelenmesinden zarar gördüğünü iddia

edenlerin ilgili mevzuata göre tazminat yoluna başvurabilmesi mümkündür. Bu açıklamalar bağlamında kişisel verilerin korunmasını isteme hakkına ilişkin hem cezai müeyyide hem de tazminat yükümlülüğü öngörüldüğü dikkate alındığında somut başvuru yönünden öncelikle tüketilmesi gereken hukuk yolunun belirlenmesi gerekmektedir.

49. Anayasa Mahkemesi çeşitli kararlarında etkili bir yargısal sistem kurma yönündeki pozitif yükümlülüğün her olayda mutlaka ceza davası açılmasını gerektirmediğini vurgulamıştır. Bu bağlamda ceza yargılamasında objektif sorumluluğa yer verilmezken tazminat davalarında objektif sorumluluk ilkesinin uygulanması, aynı maddi vakıalar çerçevesinde tazminat yolunda daha düşük bir ispat standardı kullanılması, ceza hukukunda taksire dayalı sorumluluğun istisnai olmasına rağmen taksire dayalı tazminat sorumluluğu kapsamında giderim imkânının daha yüksek olması ve tazminat sorumluluğunda asıl gayenin oluşan zararın telafi edilmesi olduğu hususlarını gözeterek Anayasa Mahkemesi somut olayın koşullarına göre tazminat davalarının yüksek başarı şansı sunabilecek etkili bir yol olarak kabul edilebileceğine karar vermiştir (S.S.A., § 31; Yaprak Yüksek, B. No: 2013/9116, 14/10/2015, §§ 32-35; Adnan Oktar (3), B. No: 2013/1123, 2/10/2013, §§ 35, 36; Işıl Yaykır, B. No: 2013/2284, 15/4/2014, § 44; Ramazan Demir, B. No: 2014/16285, 22/3/2018, §§ 29-41; H.Ö., B. No: 2017/34332, 12/12/2018, §§ 35-43; Mustafa Kahraman, B. No: 2018/19096, 15/6/2021, §§ 30-33).

50. Bununla birlikte etkin bir ceza soruşturması ve kovuşturması yaparak kanunda suç sayılan eylem bağlamında failerin tespit edilmesi ve olayın aydınlatılması devletin pozitif yükümlülüğünün gereğidir. Ancak özellikle aydınlatma yükümlülüğü bağlamında failin belli olduğu ve suç duyurusuyla kişisel zararın giderilmesinin amaçlandığı durumlarda hukuki sorumluluğun ceza yargılamasına göre etkili bir hukuk yolu olduğu her somut olayın koşulları gözetilmek şartıyla söylenebilir. Öte yandan suç sayılan fiil için tazminat yükümlülüğü de öngörülmesi, hukuki sorumluluğun doğrudan etkili bir hukuk yolu olarak kabul edilebilmesi için yeterli değildir. Tazminat yolu aynı zamanda başvuru kişinin şikâyetleri açısından makul bir başarı şansı ve başvuru kişinin amacına uygun bir çözüm sağlayabilecek nitelikte olmalıdır. Bu bağlamda somut olay yönünden etkili olduğu kabul edilecek başvuru yolunun Anayasa'da öngörülmüş güvencelere aykırılık nedeniyle kişisel verilerin korunmasını isteme hakkının ihlal edildiğini özü itibarıyla tespit etme ve yeterli giderim sağlama imkânı sunan bir yol olması gerekmektedir.

51. Somut olayda başvuru kişinin, internet trafik bilgilerinin mevzuatta belirlenen süreden fazla tutulması ve bu bilgilerin ilgili Mahkemeye gönderilmesi eylemine ilişkin suç duyurusunda bulunduğu, yapılan soruşturma sonunda ise Başsavcılık tarafından kovuşturmaya yer olmadığına karar verildiği anlaşılmaktadır. Başvuru kişinin şikâyetine konu eylemlerin ve faillerinin belli olduğu

hususunda ihtilaf olmadığı gözetildiğinde başvuru konusunun suç duyurusuyla hak ihlalinin tespitini, kişisel zararının giderimini ve faillerin cezalandırmasını amaçladığı söylenebilir. Bununla birlikte şikâyet konusu fiilin erişim sağlayıcı Şirketler ile Kurumun kurumsal faaliyet niteliğindeki işlemlerinden kaynaklandığı anlaşılmaktadır. Bu durumda ceza yargılaması sonunda kasıtlı veya ihmali bir eylemi tespit edilmediği sürece Kurum ve Şirket çalışanlarının bireysel olarak ceza sorumluluğundan söz edilemeyeceği, kurumsal sorumluluğun da her hâlde ceza yargılamasına konu olamayacağı açıktır. Ayrıca başvuru konusunun Kurum ve Şirket çalışanların bireysel sorumluluğu olduğu yönünde başvuru formunda bir iddiası da bulunmamaktadır.

52. Öte yandan başvuru konusunun iddia ettiği kişisel zararlarının ceza yargılamasıyla gideriminin sağlanması da mümkün değildir. Yukarıda belirtilen mevzuat hükümleri (bkz. §§ 29, 30) birlikte değerlendirildiğinde başvuru konusunun maruz kaldığı eylemlerin hukuka aykırı olduğu ve kişisel verilerin korunmasını isteme hakkının ihlal edildiği iddiasına, dolayısıyla şikâyetin esasına ilişkin idare ve hukuk mahkemeleri tarafından araştırma yapılarak varsa bir hukuka aykırılığın ve hak ihlalinin tespit edilmesinin mümkün olduğu anlaşılmaktadır. Ayrıca hukuka aykırı bir eylemin tespiti hâlinde kişisel zararların tazmini amacıyla manevi tazminata hükmedilebileceği sabittir. Bunun yanında ceza yargılamasından farklı olarak tazminat yolunda hem bireysel hem de kurumsal sorumluluğa dayanılabileceği, genel hükümler çerçevesinde hâkimin tespit edilen hak ihlaline ilişkin tazminatın yanında ek giderim ve tedbire karar verilebileceği söylenebilir. Atıf yapılan yargı kararları (bkz. §§ 31-34) incelendiğinde ise başvuru konusunun iddialarıyla benzer iddiaların hem hukuk hem de idare mahkemeleri tarafından esasa girilerek ayrıntılı bir şekilde incelendiği, tarafların iddia ve savunmalarıyla yargılamaya etkin bir şekilde katılmalarının sağlandığı, ayrıca ilk derece mahkemelerinin kararlarının kanun yolu incelemelerine tabi olduğu görülmüştür. Bu tespitler bağlamında başvuru konusunun iddiaları yönünden hukuk ve idare mahkemeleri nezdinde etkin şekilde işleyen bir hukuk yolunun mevcut olduğu söylenebilir.

53. Açıklamalar ve yargı kararları birlikte değerlendirildiğinde somut olayda kişisel verilerin korunmasını isteme hakkının ihlalinin tespiti ile gideriminin sağlanması bağlamında, tazminat davalarının ceza yargılamasına göre başvuru konusunun amacına daha uygun ve makul bir başarı sunma kapasitesinin bulunduğu anlaşılmaktadır. Ayrıca başvuru konusunun da tazminat yolunun etkili bir hukuk yolu olmadığına ilişkin somut verilere dayanan bir iddiasının olmadığı görülmüştür. Bu durumda başvuru konusunun ihlal iddiaları dikkate alındığında ilk bakışta ulaşılabilir ve ihlal iddialarıyla ilgili başarı şansı sunma ve yeterli giderim sağlama kapasitesi olduğu görünen tazminat yolu

tüketilmeden yapılan başvurunun incelenmesinin bireysel başvurunun ikincil niteliği ile bağdaşmayacağı sonucuna varılmıştır.

54. Açıklanan gerekçelerle başvurunun başvuru yollarının tüketilmemesi nedeniyle kabul edilemez olduğuna karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Başvurucunun adli yardım talebinin **KABULÜNE**,

B. Özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkının ihlal edildiğine ilişkin iddianın başvuru yollarının tüketilmemesi nedeniyle **KABUL EDİLEMEZ OLDUĞUNA**,

C. 12/1/2011 tarihli ve 6100 sayılı Hukuk Muhakemeleri Kanunu'nun 339. maddesinin (2) numaralı fıkrası uyarınca tahsil edilmesi mağduriyetine neden olacağından adli yardım talebi kabul edilen başvurucunun yargılama giderlerini ödemekten **TAMAMEN MUAF TUTULMASINA**,

D. Kararın bir örneğinin Adalet Bakanlığına **GÖNDERİLMESİNE** 30/6/2021 tarihinde **OYBİRLİĞİYLE** karar verildi.

Anayasa Mahkemesi - Ramazan Şahin Kararı (2018/11988)

Ramazan Şahin [GK], B. No: 2018/11988, 10/3/2022

Başvuru, parmak izi kayıt sistemi ile mesai takibi yapılması nedeniyle özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiği iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

GENEL KURUL

KARAR

RAMAZAN ŞAHİN BAŞVURUSU

(Başvuru Numarası: 2018/11988)

Karar Tarihi: 10/3/2022

R.G. Tarih ve Sayı: 19/4/2022-31814

GENEL KURUL

KARAR

Başkan: Zühtü ARSLAN

Başkanvekili: Hasan Tahsin GÖKCAN

Başkanvekili: Kadir ÖZKAYA

Üyeler: Engin YILDIRIM, Hicabi DURSUN, Muammer TOPAL, M. Emin KUZ, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĞLU, Selahaddin MENTEŞ, Basri BAĞCI, İrfan FİDAN, Kenan YAŞAR

Raportör: Ali KOZAN

Başvurucu: Ramazan ŞAHİN

Vekili: Av. Nazan SAKALLI AKTAŞ

I. BAŞVURUNUN KONUSU

1. Başvuru, parmak izi kayıt sistemi ile mesai takibi yapılması nedeniyle özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiği iddiasına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 5/2/2018 tarihinde yapılmıştır.

3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.

4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.

5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.

6. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına gönderilmiştir.

7. İkinci Bölüm tarafından 7/10/2021 tarihinde yapılan toplantıda, niteliği itibarıyla başvurunun Genel Kurul tarafından karara bağlanması gerekli görüldüğünden Anayasa Mahkemesi İçtüzüğü'nün (İçtüzük) 28. maddesinin (3) numaralı fıkrası uyarınca Genel Kurula sevkine karar verilmiştir.

III. OLAY VE OLGULAR

8. Başvuru formu ve eklerinde ifade edildiği şekliyle ve Ulusal Yargı Ağı Bilişim Sistemi (UYAP) aracılığıyla erişilen bilgi ve belgeler çerçevesinde olaylar özetle şöyledir:

9. Başvurucu, Söke Belediye Başkanlığı (Kurum) bünyesinde devlet memuru olarak çalışmaktadır. İşyerinde parmak izi sistemi ile mesai takibine başlanması üzerine Kurum tarafından 13/4/2016 tarihinde başvurusunun parmak izi kaydedilmiştir. Başvurucu 15/4/2016 tarihli dilekçesiyle parmak izinin kaydedilmesine ve parmak izi sistemiyle mesai takibi yapılmasına itiraz ederek uygulamanın kaldırılmasını talep etmiştir. Başvurucu; anılan dilekçede, parmak izinin bireyin fiziksel olarak belirlenmesini sağlayan kişisel bilgi olarak kabul edilmesi nedeniyle özel hayatın gizliliği kapsamında kaldığını ve Anayasa'da ve uluslararası sözleşmelerde anılan hakkın korunduğunu vurgulamıştır.

10. Kurumun talebi reddetmesi üzerine başvuru 27/6/2016 tarihinde Aydın 1. İdare Mahkemesinde (Mahkeme) anılan idari işlemin iptali talebiyle dava açmıştır. Davalı Kurum savunmasında; Kurum çalışanlarının ve başvurusunun mesaiye devam yükümlülükleri olduğunu, personelin mesai giriş ve çıkışlarının takip edilmesi amacıyla kamera ve parmak izi kayıt cihazı konulduğunu belirtmiştir. Kamu hizmetinin devamlılığının sağlanması ve personelin verimliliğinin denetlenmesi amacıyla gelişen teknolojiyle birlikte çeşitli cihazların mesai takibinin kontrolünde kurumlar tarafından

kullanıldığı ifade edilmiştir. Ayrıca 3/7/2005 tarihli ve 5393 sayılı Belediye Kanunu'nun 38. maddesine göre belediye başkanının belediye teşkilatını sevk ve idare etme görevinin olduğu, uygulamanın kamu hizmetinin etkin yürütülmesine hizmet ettiği vurgulanarak çalışanın mesai saatlerine uyup uymadığının kontrolü amacıyla yapılan uygulamanın özel hayata saygı hakkını ihlal etmediği iddia edilmiştir.

11. Başvurucu vekili, Kurum savunmasına karşı cevabında 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu'nda memurların çalışma saatleri ile günlük çalışmaya başlayış ve çalışmanın bitiş saatlerinin tespitine yönelik düzenlemelere yer verildiği ancak kamu görevlilerinin mesaiye devam durumlarının kontrolü konusunda bir düzenlemenin mevzuatta olmadığını vurgulamıştır. İdarelerin, gelişen teknolojinin sunduğu olanakları kullanmaya başlamasının doğal olduğunu ancak kişisel verilerin kayıt altına alınması uygulamasının özel hayata saygı hakkına ilişkin anayasal güvencelere uygun olması gerektiğini belirtmiştir. Parmak izi okuma sistemiyle her insanda kendine özgü olduğu bilinen ve kişisel veri kapsamında kalan parmak izinin bir sisteme kaydedildiğini, bu sistemin çalışabilmesi için Kurum bünyesinde çalışan personelin parmak izlerinin bir yerde depolanması gerektiğini ifade etmiştir. Kayıt altına alınan ve depolanan verilerin ne şekilde kullanılacağı ya da bu kayıtların başka kişi ve kurumlarla paylaşılıp paylaşılmayacağı konusunda davalı Kurumun dahi bir garanti veremeyeceğini ileri sürmüştür. Ayrıca personelin parmak izi sistemi ile mesai kontrolünün yapılmasının özel hayatın gizliliği bağlamında değerlendirilmesi gerektiğini, başvurunun ve personelin anılan uygulama için rızalarının da alınmadığını vurgulamıştır.

12. Mahkeme 2/3/2017 tarihinde davanın kabulüyle idari işlemin iptaline karar vermiştir. Kararın gerekçesinde ilgili mevzuata atıf yapılarak personelin parmak izi tarama sistemi ile mesai kontrolünün yapılması durumunun özel hayata saygı hakkı kapsamında kişisel verilerin işlenmesi çerçevesinde değerlendirilmesi gerektiği vurgulanmıştır. 657 sayılı Kanun'da devlet memurlarının çalışma saatleri ile günlük çalışma saatlerinin başlayış ve bitişlerinin tespitine yönelik düzenlemelere yer verilmiş olmakla birlikte kamu görevlilerinin mesaiye devam durumlarının kontrolü konusunda ayrıntılı bir yasal düzenlemenin mevzuatta olmadığı, temel hakların kısıtlanabilmesi için yasal bir dayanağın bulunmasının anayasal bir zorunluluk, aynı zamanda da Avrupa İnsan Hakları Sözleşmesi'nin de (Sözleşme) temel ilkelerinden biri olduğu belirtilmiştir. Personelden kişisel veri alınması kapsamında olan parmak izi tarama sistemi ile mesai takibi uygulamasının -kamusal alanda da olsa özel hayatın gizliliği ilkesi kapsamında olması ve uygulamanın sınırlarını usul ile esaslarını

gösteren bir yasal dayanağın bulunmaması karşısında- temel haklar ve anayasal ilkelerle bağdaşmayan dava konusu işlemde hukuka uyarlık bulunmadığı değerlendirilmiştir.

13. Anılan karara karşı Kurum tarafından istinaf kanun yoluna başvurulmuştur. Kurum vekili ilgili dilekçesinde, birçok kurum tarafından kullanılan parmak izi sistemiyle mesai takibinin personelin mesaiye uyup uymadığını denetlemek amacıyla hizmet ettiğini ve özel hayata saygı hakkını ihlal etmediğini vurgulamıştır. Ayrıca parmak izinin kişiye özgü bilgi içerdiği için kartlı sistemle mesai takibinden daha güvenilir olduğunu ve kayıt altına alınan parmak izlerinin personel dosyasında muhafaza edildiğini, İnsan Kaynakları ve Eğitim Müdürlüğü tarafından dosyalandığını ve başka bir işlemde kullanılmadığını belirtmiştir. Başvurucu vekili istinaf başvurusuna cevabında önceki iddialarını tekrarlamakla birlikte kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceğini, uygulamanın kanuni dayanağının ve toplanan verilerin başka şekilde kullanılmayacağına dair güvencenin mevcut olmadığını ifade etmiştir.

14. İzmir Bölge İdare Mahkemesi 2. İdare Dava Dairesi 29/11/2017 tarihinde istinaf başvurusunun kabulü ile davanın reddine kesin olarak karar vermiştir. Kararın gerekçesinde; kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması amacıyla idarelerce teknolojik sistemlerin kullanılmaya başlanması kamu yararına ve hizmet gereklerine uygun olduğu belirtilmiştir. Başvurucunun mesaiye devam etme zorunluluğunun olduğu, idarenin de bunu kontrol ve denetim yükümlülüğünün bulunduğu gözetildiğinde parmak izi alınarak teknik cihazlarla mesai takibinin yapılmasında mevzuata aykırılık bulunmadığı değerlendirilmesine yer verilmiştir. Ayrıca kamu görevine girerek görev alanında hizmet gereklerine uygun olarak idarece konan kurallara uymakla yükümlü bulunan başvurucunun parmak izi alınarak teknik cihazlarla takibinin yapılmasının özel hayatın gizliliğinin ihlali olarak kabulüne olanak bulunmadığı gibi başvurucunun bu yöndeki iddiasına dayanak teşkil edecek somut bir kanıt da ortaya koymadığı belirtilmiştir.

15. Nihai karar, başvuru vekiline 5/1/2018 tarihinde tebliğ edilmiştir.

16. Başvurucu 5/2/2018 tarihinde bireysel başvuruda bulunmuştur.

IV. İLGİLİ HUKUK

A. İlgili Mevzuat

17. Genel olarak özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkıyla ilgili hukuk (ulusal mevzuat, uluslararası düzenlemeler ve Avrupa İnsan Hakları Mahkemesi kararları) için bkz. E.Ü. [GK], B. No: 2016/1310, 17/9/2020, §§ 22-51; Bestami Eroğlu [GK], B. No: 2018/23077, 17/9/2020, §§ 42-83, Arif Ali Cangı [GK], B. No: 2016/4060, 17/9/2020, §§ 21-50.

18. Ayrıca 657 sayılı Kanun'un "Çalışma saatleri" kenar başlıklı 99. maddesi şöyledir:

"Memurların haftalık çalışma süresi genel olarak 40 saattir.

Bu süre Cumartesi ve Pazar günleri tatil olmak üzere düzenlenir.

Ancak bu kanuna, özel kanunlara, Cumhurbaşkanlığı kararnamelerine veya bunlara dayanılarak çıkarılacak yönetmeliklerle, kurumların ve hizmetlerin özellikleri dikkate alınmak suretiyle farklı çalışma süreleri tespit olunabilir.

Cumhurbaşkanı, yurt dışı kuruluşlarda hizmetin gerektirdiği hallerde, hafta tatilini Cumartesi ve Pazardan başka günler olarak tespit edebilir."

19. 657 sayılı Kanun'un "Günlük çalışma saatlerinin tespiti" kenar başlıklı 100. maddesi şöyledir.

"Günlük çalışmanın başlama ve bitme saatleri ile öğle dinlenme süresi, bölgelerin ve hizmetin özelliklerine göre merkezde Cumhurbaşkanınca, illerde valiler tarafından tesbit olunur.

(Ek fıkra: 13/2/2011 - 6111/104 md.) Ancak engelliler için; engel durumu, hizmet gerekleri, iklim ve ulaşım şartları göz önünde bulundurulmak suretiyle günlük çalışmanın başlama ve bitiş saatleri ile öğle dinlenme süreleri merkezde üst yönetici, taşrada mülki amirlerce farklı belirlenebilir.

(Ek fıkra: 13/2/2011 - 6111/104 md.) Memurların yürüttükleri hizmetin özelliklerine göre, bu madde uyarınca tespit edilen çalışma saat ve süreleri ile görev yerlerine bağlı olmaksızın çalışabilmeleri mümkündür. Bu hususa ilişkin usûl ve esaslar, Cumhurbaşkanınca belirlenir."

20. 5393 sayılı Kanun'un "Belediye başkanının görev ve yetkileri" kenar başlıklı 38. maddesinin ilgili kısmı şöyledir.

"Belediye başkanının görev ve yetkileri şunlardır:

a) Belediye teşkilâtının en üst amiri olarak belediye teşkilâtını sevk ve idare etmek, belediyenin hak ve menfaatlerini korumak.

b) Belediyeyi stratejik plâna uygun olarak yönetmek, belediye idaresinin kurumsal stratejilerini oluşturmak, bu stratejilere uygun olarak bütçeyi, belediye faaliyetlerinin ve personelinin performans ölçütlerini hazırlamak ve uygulamak, izlemek ve değerlendirmek, bunlarla ilgili raporları meclise sunmak.

..."

21. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Tanımlar" kenar başlıklı 3. maddesinin ilgili kısmı şöyledir:

" (1) Bu Kanunun uygulanmasında;

a) Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,

...

d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

...ifade eder."

22. 6698 sayılı Kanun'un "Kişisel verilerin işleme şartları" kenar başlıklı 5. maddesi şöyledir:

"(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması."

23. 6698 sayılı Kanun'un "Özel nitelikli kişisel verilerin işleme şartları" kenar başlıklı 6. maddesi şöyledir:

"(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır."

24. 6698 sayılı Kanun'un "İstisnalar" kenar başlıklı 28. maddesi şöyledir:

"(1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:

a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklerle uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi.

b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.

c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.

ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

(2) Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili

kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri aşağıdaki hâllerde uygulanmaz:

- a) Kişisel veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.
- b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.
- c) Kişisel veri işleminin kanunun verdiği yetkiye dayanarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.
- ç) Kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması."

B. İlgili Yargı Kararı

25. Danıştay İdari Dava Daireleri Kurulunun 9/12/2015 tarihli ve E.2014/2242, K.2015/4991 sayılı kararı şöyledir:

"Kişisel verilerin korunması hakkı, kişinin insan onurunun korunması ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı ifade etmektedir. Bununla birlikte, sözkonusu hak mutlak ve sınırsız olmayıp, Anayasa'nın 13. ve 20. maddeleri gereğince belirli koşullarda, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmamak üzere yasayla sınırlanabilir. Bu bağlamda, kişisel verilerin sistematik biçimde kayıt altına alınabilmesi için verilerin korunmasına ilişkin esas ve usullerin yasayla düzenlenmesi zorunludur. Diğer bir deyişle, kişisel verilerin korunmasına ilişkin gerekli yasal düzenlemeye ve teknik olanaklara sahip olmayan bir idarenin, kişinin rızasını alsa dahi bu konudaki işleminin hukuka uygunluğundan söz etmek olanaklı olmayacaktır.

Bu çerçevede, idarelerce gelişen teknolojinin, kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması nedeniyle, kamu kesiminde kullanılmaya başlanması doğal olmakla birlikte, teknoloji kullanılarak kişisel verilerin kayıt altına alınması uygulamasının yukarıda belirtilen hükümlere uygun olması gerektiğinde kuşku bulunmamaktadır.

Yukarıda belirtildiği üzere, gerek Anayasa'da gerekse ülkemizin tarafı olduğu ve yine Anayasa'nın 90. maddesi uyarınca kanun hükmünde olan uluslararası sözleşmelerde, kişilerin özel hayatı ile aile hayatının ve kişisel verilerinin gizliliğine saygı gösterilmesi gerektiği ve bu gizliliğe müdahale edilemeyeceği açıkça hüküm altına alınmış olup, bu gizliliğe müdahalenin milli güvenlik, kamu

düzeni gibi zorunluluk arz eden durumlara münhasır olarak ve yasayla öngörölmek şartıyla mümkün olduđu anlaşılmaktadır.

Bu kapsamda, ilgililerden kişisel veri alınması niteliğinde olan 'parmak izi taraması'nın, 'özel hayatın gizliliği' ilkesi kapsamında bulunması karşısında 'uygulamanın sınırlarını, usul ve esaslarını' gösteren bir yasal dayanağının bulunmaması, toplanan verilerin ileride başka bir şekilde kullanılamayacağına dair bir güvencenin mevcut olmaması gözönüne alındığında, yukarıda belirtilen temel haklar ve Anayasal ilkeler ile uluslararası sözleşme kuralları ile bağdaşmayan dava konusu işlemlerde hukuka uyarlık bulunmadığı sonucuna varılmıştır. Açıklanan nedenlerle, davacının temyiz isteminin kabulüne..."

C. Kişisel Verileri Koruma Kurumu Kararları

26. Kişisel Verileri Koruma Kurulunun (Kurul) 1/12/2020 tarihli ve 2020/915 sayılı kararının ilgili kısmı şöyledir:

"Kurula intikal eden şikâyetle ilgili kişi tarafından veri sorumlusu bünyesinde 657 sayılı Devlet Memurları Kanunu kapsamında çalışan memur olduđu, veri sorumlusu bünyesinde personel giriş çıkışlarının takibi için parmak izi okuma cihazları ile kişisel verilerinin, her personel için parmak izi bilgilerinin alındığı ve sisteme tanıtıldığı, bu konudaki uygulama için kendisine ait olan parmak izi bilgilerinin veri sorumlusunun kayıt sisteminden, kağıt ortamından ve elektronik ortamdan silinmesi ve kendisine bilgi verilmesi talebiyle veri sorumlusuna başvuru yaptığı; kendisine verilen cevapta sistemlerinden bu bilgilerin silinemeyeceğinin beyan edildiği, parmak izi bilgilerinin onayı olmadan işlenemeyeceği ve resmi başvuru yapmasına rağmen verilerinin silinmesi isteğinin kabul edilmediği belirtilmiştir..."

Somut olayda ilgili kişinin veri sorumlusu tarafından kendisine ait olan parmak izi bilgilerinin hukuka aykırı olarak işlenmesine ilişkin şikâyeti ile ilgili veri sorumlusunun PDKS sistemi gereği personelden alınan parmak izlerinin salt mesai kontrollerinde kullanıldığı, parmak izi tanıma algoritmasının temel işlevinin parmak izinin çıkartılması ve karakterlerin eşleştirilmesi olduđu, parmak izinin çıkartılmasıyla kastedilenin parmak izinin temel karakteristik verilerinin şifrelenip karakteristik bir şablon haline getirilmesi olduđu, bir şablon haline getirilen parmak izinin daha sonra hiçbir şekilde görüntüsünün alınamadığı ve işlem yapılamadığı şeklindeki açıklamaları çerçevesinde veri sorumlusu bünyesinde çalışan personellerden işe giriş ve çıkışlarda parmak izlerinin kullanıldığının açıkça kabul edildiği, ilgili kişinin parmak izinin açık rızasına dayanılarak alınıp alınmadığı hususunun anlaşılamadığı; ancak işe giriş ve çıkışlarda söz konusu kişisel verisinin işlenmesinin devam etmesi noktasında ilgili kişinin onayı olmadan parmak izinin işlenemeyeceği

hususunda şikayeti bulunduğu dikkate alındığında ilgili kişinin parmak izi kullanılarak mesai kontrolü yapılması hususunda açık rızasının olmadığı kanaatine varıldığı,

Öte yandan veri sorumlusu tarafından mesai kontrolü için parmak izi, sicil numarası ve şifreli giriş, ıslak imzalı form yöntemlerinin kullanıldığı, covid-19 salgını sebebiyle halihazırda müdürlüklerde personel kontrolünün ıslak imzalama metodu ile sağlandığı, parmak izi sisteminin devre dışı olduğuna yönelik savunması dikkate alındığında işe giriş ve çıkış kontrollerinin biyometrik verileri işlemenin haricinde alternatif yollar ile sağlanabildiği, dolayısı ile üstün güvenlik önlemleri alınmasını gerektirecek bir durumun da olmadığı görüldüğü, bu kapsamda veri sorumlusu bünyesinde mesai kontrolü amaçlı giriş ve çıkışlar için parmak izi okutma sisteminin kurulmasının Kanunun 'Genel İlkeler' başlıklı 4 üncü maddesinin (ç) bendindeki ölçülülük ilkesine aykırı olduğu kanaatine varıldığı ve veri sorumlusunun söz konusu uygulamasının Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendine aykırılık teşkil ettiği..."

27. Kurulun 27/2/2020 tarihli ve 2020/167 sayılı kararının ilgili kısmı şöyledir:

"Spor salonu hizmeti sunan şirketin (veri sorumlusu), üyelerinin giriş-çıkış kontrolünde el okutma sistemine geçilmesi gibi biyometrik verileri içeren bazı özel nitelikli kişisel verileri işlemesi ve bu bilgilerin güvenli şekilde muhafaza edildiğinden şüphe duyulması üzerine ilgili kişilerce Kuruma intikal ettirilen şikâyetin incelenmesi neticesinde ...

Kanunun 'Genel İlkeler' başlıklı 4 üncü maddesinde de, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra, kişisel verilerin ancak hukuka ve dürüstlük kurallarına uygun şekilde, belirli, açık ve meşru amaçlar kapsamında, doğru ve gerektiğinde güncel olma şartıyla, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun işlenebileceğinin düzenlendiği,

Bu ilkelerden, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesinin, işlenen verilerin belirlenen amaçların gerçekleştirilebilmesine elverişli olması, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirdiği, sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik olarak veri işlenmesi yoluna gidilmemesi gerektiği,

Ölçülülük ilkesinin ise, veri işleme faaliyeti ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması, diğer bir ifadeyle veri işlemenin amacı gerçekleştirecek ölçüde olması anlamına geldiği, bu kapsamda, kişisel veri işleme faaliyetinin gerçekleşmesi için gerekli olmayan kişisel

verilerin toplanmaması ve/veya işlenmemesi gerektiği, veri sorumlusunun amacı çerçevesinde ölçülülük ilkesine uygun olarak ilgili kişiden minimum düzeyde bilgi talep etmesi, bunun dışındaki amaç için gerekli olmayan veri işlemeden kaçınması gerektiği, kişisel verilerin işlenmesinin ilgili kişinin iznine bağlı olarak gerçekleştirilse ve belirli bir amaca bağlı olsa bile açık rızanın, aşırı miktarda veri toplanmasını meşrulaştırmayacağı, buna göre kişisel verilerin yalnızca belirli amaçlar için ve gerektiği kadar toplanması, amacın gerektirdiği yerlerde kullanılması ve amaç için gerekli olandan uzun süre tutulmaması gerektiği, dikkate alındığında spor salonuna giriş için veri sorumlusu tarafından uygulanan 'el ve parmak izi taraması' sisteminin, üyelerin açık rızası olsa bile hizmetten faydalanmak için üyelere sunulmasının, kişisel verilerin işlenmesinde ölçülülük ilkesi ışığında ilgili kişilerden minimum düzeyde veri talep etme ilkesi ile uyumlu olmadığı değerlendirilmiştir..."

D. Avrupa İnsan Hakları Mahkemesi Kararı

28. Avrupa İnsan Hakları Mahkemesi (AİHM) parmak izlerini, biyolojik örnekleri ve genetik profilleri kişisel veri olarak nitelendirmiştir (S. ve Marper/Birleşik Krallık, B. No: 30562/04, 30566/04, 4/12/2008, §§ 97, 98). Söz konusu kararında AİHM, kişisel verilerin korunmasının Sözleşme'nin 8. maddesi kapsamında güvence altına alınan özel hayata saygı hakkının korunması konusunda büyük öneme sahip olduğunu vurgulamıştır. Mahkeme, kişisel verilerin kullanılmasının Sözleşme'nin 8. maddesinde yer alan güvencelere aykırılık teşkil etmesinin önüne geçilmesi amacıyla yeterli güvenceleri sağlayacak şekilde iç hukukta düzenlemeler yapılması gerektiğini belirtmiştir. AİHM, bu tür güvencelere olan ihtiyacın öneminin otomatik olarak işlenen kişisel verilerin korunmasının söz konusu olduğu durumlarda daha da arttığını ifade etmiştir. AİHM, ulusal düzenlemelerin bu verilerin saklanma amaçlarına uygun olması ve aşırı olmaması gerektiğini, verilerin saklanma amacının gerektirdiğinden daha uzun süre tutulmamasına olanak tanıyacak ve ilgili kişinin tespitini sağlayacak bir biçimde muhafaza edilmesini temin etmesi gerektiğini de belirtmiştir (S. ve Marper/Birleşik Krallık, § 103).

V. İNCELEME VE GEREKÇE

29. Anayasa Mahkemesinin 10/3/2022 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları

30. Başvurucu;

i. Temel hak ve hürriyetlerin Anayasa'da belirtilen nedenlerle sadece kanun ile sınırlandırılabilceğini vurgulayarak 657 sayılı Kanun'da memurların çalışma saatleri ile günlük çalışmaya başlayış ve bitiş

saatlerinin tespitine yönelik düzenlemelere yer verildiğini ancak kamu görevlilerinin mesaiye devam durumlarının kontrolü konusunda bir düzenlemenin mevzuatta bulunmadığını iddia etmiştir. Parmakların son eklemesinde ve uç kısımlarında bulunan izin her bireyde farklı olduğunu ve parmak izi okuma sisteminin okuyucu panele parmak bastırıldığında cihazın parmak izini kaydederek bir kod oluşturduğunu, dolayısıyla bu şekilde kişisel veri kapsamındaki bir bilginin işlendiğini belirtmiştir.

ii. Bu sistemin işleyebilmesi için çalışan personelin parmak izlerinin Kurum bünyesinde bir yerde depolanması gerektiğini, depolanan verilerin ne şekilde kullanılacağı ya da bu kayıtların başka kişiler ve kurumlarla paylaşılıp paylaşılmayacağı konusunda davalı Kurumun dahi bir garanti verebilmesinin mümkün olmadığını ifade etmiştir. Ayrıca uygulamanın kanuni dayanağı ve bu uygulamaya rızası olmamasına rağmen Mahkemenin hatalı bir değerlendirme ile iptal davasını reddettiğini ifade etmiş; özel hayata saygı, kişisel verilerin korunmasını isteme ve adil yargılanma hakları ile zorla çalıştırma yasağının ihlal edildiğini ileri sürmüştür.

B. Değerlendirme

31. Anayasa'nın iddianın değerlendirilmesinde dayanak alınacak "Özel hayatın gizliliği" kenar başlıklı 20. maddesinin birinci ve üçüncü fıkraları şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

...

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

32. Özel hayata saygı hakkı Anayasa'nın 20. maddesinde koruma altına alınmıştır. Devlet, kişilerin özel ve aile hayatına keyfî olarak müdahale etmemek ve üçüncü kişilerin haksız saldırılarını önlemekle yükümlüdür. Özel hayata saygı hakkı kapsamında korunan hukuksal çıkarılardan biri de bireyin mahremiyet hakkıdır. Ancak mahremiyet hakkı sadece yalnız kalma hakkından ibaret olmayıp bu hak, bireyin kendisiyle ilgili bilgileri kontrol edebilme hukuksal çıkarımı da kapsamaktadır. Bireyin kendisine ilişkin herhangi bir bilginin kendi rızası olmaksızın açıklanmaması, yayılmaması, bu bilgilere başkaları tarafından ulaşılamaması ve rızası hilafına kullanılmaması, kısaca bu bilgilerin mahrem kalması konusunda menfaati bulunmaktadır. Bu husus, bireyin

kendisiyle ilgili bilgilerin geleceğini belirleme hakkına işaret etmektedir (Serap Tortuk, B. No: 2013/9660, 21/1/2015, §§ 31, 32). Özel hayata saygı hakkının kapsamında olan bireylerin kişisel verilerinin korunması hakkı, Anayasa'nın 20. maddesinde açık olarak düzenlenmiştir (Nurcan Belin, B. No: 2014/14187, 10/1/2018, § 38).

33. Anayasa'nın 20. maddesinin üçüncü fıkrasında herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilmeyi, bu verilere erişmeyi, bunların düzeltilmesini veya silinmesini talep etmeyi ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı ifade edilmiştir. Maddede ayrıca kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır (AYM, E.2014/122, K.2015/123, 30/12/2015, §§ 19, 20; Nurcan Belin, § 45).

34. Anayasa Mahkemesi kararlarında da belirtildiği üzere kişisel veri -belirli veya kimliği belirlenebilir olmak şartıyla- bir kişiye ilişkin bütün bilgileri ifade etmekte olup bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi sadece kimliğini ortaya koyan bilgileri değil telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, öz geçmişi, resmi, görüntü ve ses kayıtları, parmak izleri, sağlık bilgileri, genetik bilgileri, IP adresi, e-posta adresi, alışveriş alışkanlıkları, hobileri, tercihleri, etkileşimde bulunduğu kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır (AYM, E.2014/74, K.2014/201, 25/12/2014; E.2014/180, K.2015/30, 19/3/2015).

35. Öte yandan Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı yönünden inceleme yapılabilmesi için öncelikle anılan hak kapsamında korunması gerekli bir kişisel verinin olup olmadığı belirlenmelidir. Anayasa hükmünün lafzı, konuya ilişkin uluslararası belgeler ve karşılaştırmalı hukuk dikkate alındığında belirli veya belirlenebilir bir gerçek veya tüzel kişi hakkındaki her türlü bilgi kişisel veri olarak değerlendirilir. Ancak her dava ya da başvuruda Anayasa'nın 20. maddesinin üçüncü fıkrası anlamında bir kişisel veri bulunup bulunmadığı davanın ve başvurunun kendine özgü koşulları dikkate alınarak otonom olarak tespit edilir. Bir kişisel verinin bulunduğu tespit edildiğinde bu veriye yönelik her türlü sınırlama ve müdahale Anayasa'nın anılan hükmü kapsamındaki güvenceleri harekete geçirir (E.Ü., § 59).

36. Ayrıca 6698 sayılı Kanun'un 6. maddesinde (bkz. § 22) özel nitelikli kişisel veriler tahdidî olarak sayılmak suretiyle işlenmesi genel nitelikli verilere göre daha sıkı koşullara bağlanmıştır. Anılan düzenlemeyle biyometrik veri de özel nitelikli kişisel veri olarak kabul edilmiştir. Biyometrik veri bir kişinin diğer şahıslardan ayrılmasını ve bizzat kişinin kimliğinin tanımlanmasını sağlayan, bu kişiye ait bir biyolojik veya davranışsal bilgi içermesi nedeniyle önemine binaen özel nitelikli kişisel veri olarak kabul edilmiştir. Parmak izinin de sadece o kişiye ait olan ve kişinin kimliğini doğrudan tanımlamaya yarayan fizyolojik bilgi içerdiği, bu bağlamda biyometrik veri olduğu açıktır.

37. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Somut olayda devlet memuru olarak çalışan başvuruçunun mesaiye devamını takip etmek amacıyla parmak izinin bir sisteme kaydedilmesi ve bu sistem aracılığıyla mesai takibinin yapılması söz konusudur. Parmak izinin her bireyde farklı olduğu ve kişinin biyolojik olarak teşhisine imkân verecek nitelikte kişiye özgü bilgi içerdiği gözetildiğinde biyometrik veri olduğu sabittir. Bu durumda başvuruçunun parmak izinin belirli bir gerçek kişi hakkındaki bilgi kapsamında olduğu dikkate alındığında bu bilgilere erişilmesinin, bunların kullanılmasının ve işlenmesinin özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkı yönünden incelenmesi gerektiği değerlendirilmiştir.

1. Kabul Edilebilirlik Yönünden

38. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

2. Esas Yönünden

a. Müdahalenin Varlığı

39. Somut olayda idarenin başvuruçunun parmak izini kaydederek parmak izi takip sistemi ile mesai takibinde kullandığı anlaşılmaktadır. Başvuruçuya ait parmak izinin kişisel veri olarak nitelendirilebileceğinde kuşku yoktur. Bu durumda söz konusu kişisel verilerin işlenmesinin Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkına bir müdahale oluşturduğu sonucuna varılmıştır.

b. Müdahalenin İhlal Oluşturup Oluşturmadığı

40. Anayasa'nın 13. maddesi şöyledir:

"Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz."

41. Yukarıda belirlenen müdahale, Anayasa'nın 13. maddesinde belirtilen koşullara uygun olmadığı takdirde Anayasa'nın 20. maddesini ihlal edecektir. Bu sebeple sınırlamanın Anayasa'nın 13. maddesinde öngörülen ve somut başvuruya uygun düşen, kanun tarafından öngörülme, meşru amaç taşıma, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmama kriterlerine uygun olup olmadığının belirlenmesi gerekir (Halil Berk, B. No: 2017/8758, 21/3/2018, § 49; Süveyda Yarkin, B. No: 2017/39967, 11/12/2019, § 32; Şennur Acar, B. No: 2017/9370, 27/2/2020, § 34; R.G. [GK], B. No: 2017/31619, 23/7/2020, § 82). Bu bağlamda somut başvuruda öncelikle müdahalenin kanuni dayanağının bulunup bulunmadığı incelenmelidir.

i. Genel İlkeler

42. Anayasa uyarınca, temel hak ve özgürlüklere getirilen sınırlamaların öncelikle kanunla öngörülmüş olması gerekir. Kanun ile sınırlama ölçütü veya kanunilik ilkesi Sözleşme'nin 8. maddesinde de bir sınırlama ve güvence ölçütü olarak yer almaktadır. Buna karşın Sözleşme'de yer alan kanunla öngörülmüş olma kavramı ile Anayasa'da yer alan kanunilik ilkesi tam olarak aynı değildir (Bülent Polat [GK], B. No: 2013/7666, 10/12/2015, § 73).

43. AİHM kanunda öngörülen koşulları, bir diğer ifadeyle hukukiliği geniş yorumlayarak istikrar kazanmış yargı kararlarına dayanan, içtihat yoluyla geliştirilmiş ilkelerin de hukukilik şartını karşılayabildiğini kabul ederken (Malone/Birleşik Krallık [GK], B. No: 8691/79, 2/8/1984, §§ 66-68; Sunday Times/Birleşik Krallık (No. 1) [GK], B. No: 6538/74, 26/4/1979, § 47) Anayasa, tüm sınırlandırmaların mutlaka kanun ile yapılacağını öngörerek Sözleşme'den daha geniş bir koruma sağlamıştır (Mehmet Akdoğan ve diğerleri, B. No: 2013/817, 19/12/2013, § 31; Bülent Polat § 75). Anayasa'nın temel hak ve hürriyetlerin sınırlandırılmasının ancak kanunla yapılacağına ilişkin 13. maddesi, bir kanun hükmü olmaksızın yürütme ve idarenin bir hak ve hürriyeti ilk elden düzenleyici işlemle sınırlamasına izin vermez (Tuğba Arslan [GK], B. No: 2014/256, 25/6/2014, § 87).

44. Anayasa'nın temel hak ve özgürlüklerin sınırlandırılması rejimini düzenleyen 13. maddesinde hak ve özgürlüklerin ancak kanunla sınırlanabileceği temel bir ilke olarak benimsenmiştir. Bunun yanında Anayasa'nın 20. maddesinin üçüncü fıkrasının üçüncü cümlesinde kişisel verilerin "ancak

kanunda öngörülen hallerde veya kişinin açık rızasıyla" işlenebileceği belirtilmiş, aynı fıkranın dördüncü cümlesinde ise kişisel verilerin korunmasına ilişkin esas ve usullerin "kanunla" düzenleneceği hüküm altına alınmıştır. Buna göre kişisel verilerin korunmasını isteme hakkına yapılan müdahalelerde dikkate alınacak öncelikli ölçüt, müdahalenin kanuna dayalı olmasıdır (Arif Ali Cangı, § 72).

45. Bununla birlikte temel hak ve hürriyetlerin sınırlandırılmasına ilişkin kanunların şeklen var olması yeterli değildir. Kanunilik ölçütü aynı zamanda maddi bir içeriği de gerektirmekte olup bu noktada kanunun niteliği önem kazanmaktadır. Kanunla sınırlama ölçütü sınırlamanın erişilebilirliğini, öngörülebilirliğini ve kesinliğini ifade etmekte; böylece uygulayıcının keyfi davranışlarının önüne geçtiği gibi kişinin hukuku bilmesine de yardımcı olmakta; bu yönüyle hukuk güvenliği teminatı sağlamaktadır (Halime Sare Aysal [GK], B. No: 2013/1789, 11/11/2015, § 62).

46. Kanunun bu gerekliliklere uygun olduğunun söylenebilmesi için yeterince ulaşılabilir olması, vatandaşların belirli bir olaya uygulanabilir nitelikteki hukuk kurallarının varlığı hakkında yeterli bilgiye sahip olabilmesi, ayrıca ilgili normun keyfiliğe karşı uygun bir koruma sağlaması, yetkili makamlara verilen yetkinin genişliğini ve icra edilme biçimlerini yeterli bir netlikte tanımlaması gerekmektedir (Halime Sare Aysal, § 63).

47. Hukukun kendisi -beraberinde getireceği idari pratiğin dışında- söz konusu işlemin meşru amacını da gözönünde tutarak keyfi müdahalelere karşı bireyi korumak için yetkili makamlara bırakılan takdir yetkisinin kapsamını yeterince açık bir şekilde göstermelidir. Hukuk sistemi vatandaşlara, kamu makamlarına hangi koşullarda ve hangi sınırlar içinde müdahalelerde bulunma yetkisi verdiğini yeterince açık ifadelerle gösterecek nitelikte olmalı ve bu bağlamda ilgili müdahalenin muhataplarının müdahaleye zemin hazırlayan koşullar ile müdahalenin sonuçları açısından bir öngörüde bulunabilmeleri imkânı tanınmalıdır (Halime Sare Aysal, § 64).

48. Bununla birlikte her ihtimale çözüm getiremeyecek olan yasal mevzuatın sağladığı koruma seviyesi büyük ölçüde ilgili metnin düzenlediği alan ve içeriğiyle birlikte muhataplarının niteliği ve sayısı ile yakından bağlantılıdır. Bu nedenle kuralın karmaşık olması ya da belirli ölçülerde soyutluk içermesi ve buna bağlı olarak hukuki yardım ile tam olarak anlaşılabilir hâle gelmesi tek başına hukuken öngörülebilirlik ilkesine aykırı görülemez. Bu kapsamda hak ya da özgürlüğe müdahale eden kural belirli ölçülerdeki takdir alanını elbette uygulayıcıya bırakabilir. Fakat bu takdir alanının sınırlarının da yeterli açıklıkta belirlenmesi ve kuralın asgari bir kesinlik içermesi zaruridir (Halime Sare Aysal, § 65).

49. Bu kapsamda ilgili kanuni düzenlemenin söz konusu sınırlamaya ilişkin temel çerçeveyi ortaya koymakla birlikte özellikle uygulama koşulları ve usule ilişkin ayrıntıları düzenleyici işlemlere bırakması mümkündür. Ancak bu ihtimalde de söz konusu düzenleyici işlemin yine muhataplarınca ulaşılabilir olması ve içeriği hakkında ilgilileri yeterince aydınlatacak nitelik ve açıklıkta olması gerekmektedir (Halime Sare Aysal, § 66).

ii. İlkelerin Olaya Uygulanması

50. Anayasa'nın 20. maddesine göre kişisel verilerin "ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla" işlenebileceği açıktır. 6698 sayılı Kanun ise kişisel verilerin işleme şartlarını verinin niteliğini esas alarak farklı kurallara bağlamıştır. Bu kapsamda anılan Kanun'un 5. maddesinin (1) numaralı fıkrasında genel nitelikli kişisel verilerin ilgili kişinin açık rızasıyla işlenebileceği kural olarak belirlenmiş, (2) numaralı fıkrasında ise bu kuralın istisnaları düzenlenmiştir.

51. 6698 sayılı Kanun'un 6. maddesinde ise kanun koyucu tahdidi olarak saydığı özel nitelikli kişisel verileri işlemeyi önemine binaen daha katı kurallara bağlamıştır. Bu düzenlemeye göre sağlık ve cinsel hayata ilişkin kişisel veriler dışındaki özel nitelikli veriler kişinin açık rızasının varlığı hâlinde işlenebilecektir. Bu kuralın tek istisnası ise kanunlarda öngörülmesi durumunda kişinin rızası aranmadan özel nitelikli kişisel verilerin işlenebilmesidir. Anayasa'nın 20. maddesinin üçüncü fıkrasının ve anılan Kanun'un düzenlemeleri dikkate alındığında, özel nitelikli kişisel veri kapsamındaki biyometrik verilerin kişinin açıkça rıza göstermesi durumunda veya Kanununun 6. maddesinin (3) numaralı fıkrasının ikinci cümlesindeki şartlarda ya da diğer bir kanunda açıkça öngörülmesi hâlinde rıza aranmadan işlenebileceği söylenebilir. Öte yandan anılan düzenlemede rıza aranmadan veri işleme nedenleri arasında kurum veya kuruluşların mesai düzeni yer almamaktadır. Bu açıklamalar çerçevesinde somut olayda belediye çalışanlarının özel nitelikli kişisel veri kapsamında kalan parmak izlerinin kaydedilebilmesi ve bu verilerin kullanılabilmesi için bu durumun ayrıca ve açıkça bir kanun ile düzenlenmesi veya çalışanların açık rızalarının varlığı gerekir.

52. Başvuru konusu olayda, Kurum tarafından personelin mesaiye uyup uymadığının parmak izi takip sistemi ile denetlendiği, bu kapsamda başvurucunun da parmak izinin kaydedilerek depolandığı anlaşılmıştır. Teknolojik gelişmelerin imkânlarından yararlanmak isteyen idarenin ve işverenlerin personelin verimliliğini artırmak, güvenliği sağlamak gibi amaçlara dayalı olarak mesai takibi ile işyerine giriş ve çıkış denetimlerini sağlayacak manyetik kimlik kartları, yüz ve iris tarama, parmak izi kayıt sistemi gibi yöntemler kullandıkları görülmektedir.

53. Bununla birlikte özellikle biyometrik verilerin kaydedilmesi yöntemiyle personel takip sistemi uygulanabilmesi için kanunlarda düzenlenmeyen hâllerde kişinin açık rızasının mevcut olması

gerektiği vurgulanmalıdır. Ayrıca çalışanın rızasına dayanılarak özel nitelikli verinin işlenmesi hâlinde de elbette öncelikle Anayasa'nın 13. maddesi bağlamında kanunilik ilkesinin karşılanması gerekir. Açık rızanın varlığından söz edilebilmesi için ise en azından işlenecek kişisel verinin kapsamı, amacı, sınırları ve sonuçları hakkında çalışanın önceden yeterli bir biçimde bilgilendirilmesi elzemdir. Bununla birlikte anılan yöntemlerin idarenin denetim ve yönetim yetkisi kapsamında, kural olarak meşru bir amacın varlığı, hak ve özgürlüklere daha az müdahale ile bu amacı gerçekleştirmeye elverişli başka bir yolun olmaması hâlinde ve amaçla sınırlı olmak üzere uygulanabileceği söylenebilir. Bu kapsamda kişisel verilerin işlenmesi ve paylaşılmasını içeren yöntemlerin işyerinde kullanılması hâlinde çalışanın hak ve özgürlüklerini koruyacak anayasal güvencelerin idare tarafından sağlanması gerektiği de hatırlatılmalıdır.

54. Öte yandan çalışanın kişisel verilerinin işlenmesine ilişkin rızasının olmaması durumunda ise ancak kanunlarda açıkça öngörülen hâllerde özel nitelikli kişisel veri işlenebilecektir. Bir başka deyişle çalışanın özel nitelikli kişisel verilerinin işlenmesinin esas ve usullerinin kanun ile düzenlendiği hâllerde rıza olmasa dahi ilgili kanun hükümleri uygulanabilecektir. Bununla birlikte kanunun çalışanın temel hak ve özgürlüklerinin sınırlandırılmasını içeren konuyla ilgili temel esasları ve ilkeleri belirleyecek nitelikte olması gerektiği de vurgulanmalıdır. Bu kapsamda kanun ve ilgili kanuna dayanan mevzuatın özellikle kişisel verilerin işlenmesinin kapsamına ve muhafazasına ilişkin esasları belirlemesi beklenir. Kanunun ayrıca tutulma süresi, üçüncü kişilerin erişimi ile verilerin kullanılması ve imhası konusundaki usullere ilişkin muhataplarının yetki aşımı ve keyfiliğe karşı yeteri kadar güvenceye sahip olmalarını sağlayacak açık ve detaylı kuralları içermesi gerekmektedir. Bunun yanında kanunla sınırlamanın elbette meşru bir amaca dayanması, demokratik toplum gereklerine uygun ve ölçülü olması gerektiği hatırlatılmalıdır.

55. Somut olayda başvuruçunun mesai takibi amacıyla parmak izinin Kurum tarafından kaydedilmesine, dolayısıyla kendisiyle ilgili özel nitelikli kişisel verinin işlenmesine rıza göstermediği hususunda bir ihtilaf yoktur. Ancak kişinin rızasının olmaması hâlinde kanunlarda açıkça öngörülmüş ise özel nitelikli kişisel veri işlenebilir. Bu durumda Anayasa'nın 20. maddesinde ve 6698 sayılı Kanun'un 6. maddesinde yer verilen "açık rıza" şartı bulunmadığına göre biyometrik veri kapsamındaki parmak izinin işlenerek mesai takibinde kullanılmasının bir kanun ile düzenlenip düzenlenmediği değerlendirilmelidir. Öncelikle anılan mevzuatta belirtilen kanunlarda açıkça öngörülmeyen, özel nitelikli verilerin işlenmesinin ve kullanılmasının -ilgili faaliyet alanına veya sektöre ilişkin- kanunlarda ayrıca ve açıkça düzenlenmiş olması kastedilmektedir. Bu bağlamda 6698 sayılı Kanun, belediye çalışanlarının parmak izlerini kaydetme ve parmak izi takip sistemiyle mesai

takip etme yetkisini veren, bu konuyu açıkça düzenleyen bir kanun değildir. Bu durumda idare ve derece mahkemelerinin gerekçelerinde dayandıkları 657 sayılı Kanun ile 5393 sayılı Kanun'un somut olaya uygun açık bir düzenleme barındırıp barındırmadıkları hususunun tartışılması gerekir.

56. Bu bağlamda anılan mevzuat incelendiğinde (bkz. §§ 18-20) 657 sayılı Kanun'da genel olarak devlet memurlarının çalışma saatleri ile günlük çalışma saatlerinin başlama ve bitme saatlerinin tespitine ilişkin düzenlemelerin mevcut olduğu ancak çalışanın mesaiye devam durumunun kontrolü ve bu amaçla özel nitelikli kişisel verilerin işlenmesine ilişkin açık bir düzenlemenin olmadığı görülmüştür. 5393 sayılı Kanun'da da belediye teşkilatını sevk ve idare etme yetkisinin belediye başkanına bırakıldığı ancak bu yetki kapsamında özel nitelikli kişisel verilerin işlenmesine yönelik bir düzenlemenin yapılmadığı anlaşılmıştır.

57. Bu tespitler ışığında anılan mevzuatta mesai takibi veya çalışanın denetimi amacıyla özel nitelikli kişisel verilerin işlenmesine, bu bağlamda biyometrik veri bazlı takip sistemlerinin kullanılmasına dair temel esasları ve ilkeleri belirleyen bir düzenlemenin olmadığı açıktır. Açıklamalar çerçevesinde başvurucunun özel nitelikli kişisel verilerin işlenmesine dair rızasının olmadığı, çalışanın mesaiye uyumunun kontrolünde biyometrik verilerin işlenmesinin ve kullanılmasının anılan kanunlar ile ayrıca ve açıkça öngörülmediği hususları dikkate alındığında başvuruya konu müdahalenin kanunilik şartını sağlamadığı sonucuna varılmıştır.

58. Başvuruya konu müdahalenin kanunilik şartını sağlamadığı anlaşıldığından söz konusu müdahale açısından diğer güvence ölçütlerine riayet edilip edilmediğinin ayrıca değerlendirilmesine gerek görülmemiştir.

59. Açıklanan gerekçelerle başvurucunun Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiğine karar verilmesi gerekir.

3. 6216 Sayılı Kanun'un 50. Maddesi Yönünden

60. 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 50. maddesinin ilgili kısmı şöyledir:

“(1) Esas inceleme sonunda, başvurucunun hakkının ihlal edildiğine ya da edilmediğine karar verilir. İhlal kararı verilmesi hâlinde ihlalin ve sonuçlarının ortadan kaldırılması için yapılması gerekenlere hükmedilir...

(2) Tespit edilen ihlal bir mahkeme kararından kaynaklanmışsa, ihlali ve sonuçlarını ortadan kaldırmak için yeniden yargılama yapmak üzere dosya ilgili mahkemeye gönderilir. Yeniden

yargılama yapılmasında hukuki yarar bulunmayan hâllerde başvuru lehine tazminata hükmedilebilir veya genel mahkemelerde dava açılması yolu gösterilebilir. Yeniden yargılama yapmakla yükümlü mahkeme, Anayasa Mahkemesinin ihlal kararında açıkladığı ihlali ve sonuçlarını ortadan kaldıracak şekilde mümkünse dosya üzerinden karar verir.”

61. Başvuru, ihlalin tespit edilmesini ve yeniden yargılama yapılmasını istemiş ve 10.000 TL manevi tazminat talebinde bulunmuştur.

62. Anayasa Mahkemesinin Mehmet Doğan ([GK], B. No: 2014/8875, 7/6/2018) kararında ihlal sonucuna varıldığında ihlalin nasıl ortadan kaldırılacağı hususunda genel ilkeler belirlenmiştir. Anayasa Mahkemesi diğer bir kararında ise bu ilkelerle birlikte ihlal kararının yerine getirilmemesinin sonuçlarına da değinmiş ve bu durumun ihlalin devamı anlamına geleceği gibi ilgili hakkın ikinci kez ihlal edilmesiyle sonuçlanacağına işaret etmiştir (Aligül Alkaya ve diğerleri (2), B. No: 2016/12506, 7/11/2019).

63. Bireysel başvuru kapsamında bir temel hakkın ihlal edildiğine karar verildiği takdirde ihlalin ve sonuçlarının ortadan kaldırıldığından söz edilebilmesi için temel kural, mümkün olduğunca eski hâle getirmenin yani ihlalden önceki duruma dönülmesinin sağlanmasıdır. Bunun için ise öncelikle ihlalin kaynağı belirlenerek devam eden ihlalin durdurulması, ihlale neden olan karar veya işlemin ve bunların yol açtığı sonuçların ortadan kaldırılması, varsa ihlalin sebep olduğu maddi ve manevi zararların giderilmesi, ayrıca bu bağlamda uygun görülen diğer tedbirlerin alınması gerekmektedir (Mehmet Doğan, §§ 55, 57).

64. İhlalin mahkeme kararından kaynaklandığı veya mahkemenin ihlali gideremediği durumlarda Anayasa Mahkemesi, 6216 sayılı Kanun'un 50. maddesinin (2) numaralı fıkrası ile İçtüzük'ün 79. maddesinin (1) numaralı fıkrasının (a) bendi uyarınca, ihlalin ve sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmak üzere kararın bir örneğinin ilgili mahkemeye gönderilmesine hükmeder. Anılan yasal düzenleme, usul hukukundaki benzer hukuki kurumlardan farklı olarak ihlali ortadan kaldırmak amacıyla yeniden yargılama sonucunu doğuran ve bireysel başvuruya özgülünen bir giderim yolunu öngörmektedir. Bu nedenle Anayasa Mahkemesi tarafından ihlal kararına bağlı olarak yeniden yargılama kararı verildiğinde usul hukukundaki yargılamanın yenilenmesi kurumundan farklı olarak ilgili mahkemenin yeniden yargılama sebebinin varlığını kabul hususunda herhangi bir takdir yetkisi bulunmamaktadır. Dolayısıyla böyle bir kararın kendisine ulaştığı mahkemenin yasal yükümlülüğü, ilgilinin talebini beklemeksizin Anayasa Mahkemesinin ihlal kararı nedeniyle yeniden yargılama kararı vererek devam eden ihlalin

sonuçlarını gidermek üzere gereken işlemleri yerine getirmektir (Mehmet Doğan, §§ 58, 59; Aligül Alkaya ve diğerleri (2), §§ 57-59, 66, 67).

65. İncelenen başvuruda, kanuni dayanağı olmaksızın özel nitelikli kişisel verilerin idare tarafından işlenmesi nedeniyle özel hayata saygı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiği sonucuna ulaşılmıştır. Dolayısıyla ihlalin idarenin işleminden kaynaklandığı anlaşılmaktadır. Bununla birlikte Mahkemeler de ihlali giderememiştir.

66. Bu durumda özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmasında hukuki yarar bulunmaktadır. Yapılacak yeniden yargılama ise bireysel başvuruya özgü düzenleme içeren 6216 sayılı Kanun'un 50. maddesinin (2) numaralı fıkrasına göre ihlalin ve sonuçlarının ortadan kaldırılmasına yöneliktir. Bu kapsamda yapılması gereken iş, yeniden yargılama kararı verilerek Anayasa Mahkemesini ihlal sonucuna ulaştıran nedenleri gideren, ihlal kararında belirtilen ilkelere uygun yeni bir karar verilmesinden ibarettir. Bu sebeple kararın bir örneğinin yeniden yargılama yapılmak üzere Aydın 1. İdare Mahkemesine gönderilmesine karar verilmesi gerekmektedir.

67. İhlalin ve sonuçlarının ortadan kaldırılması için yeniden yargılamanın yeterli bir giderim sağlayacağı anlaşıldığından tazminat talebinin reddine karar verilmesi gerektiği sonucuna ulaşılmıştır.

68. Dosyadaki belgelerden tespit edilen 294,70 TL harç ve 4.500 TL vekâlet ücretinden oluşan toplam 4.794,70 TL yargılama giderinin başvurucuya ödenmesine karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiğine ilişkin iddianın **KABUL EDİLEBİLİR OLDUĞUNA,**

B. Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının **İHLAL EDİLDİĞİNE,**

C. Kararın bir örneğinin kişisel verilerin korunmasını isteme hakkının ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmak üzere Aydın 1. İdare Mahkemesine (E.2016/1055, K.2017/221) **GÖNDERİLMESİNE,**

D. Tazminat talebinin **REDDİNE,**

E. 294,70 TL harç ve 4.500 TL vekâlet ücretinden oluşan toplam 4.794,70 TL yargılama giderinin başvurucuya ÖDENMESİNE,

F. Ödemenin, kararın tebliğini takiben başvurucunun Hazine ve Maliye Bakanlığına başvuru tarihinden itibaren dört ay içinde yapılmasına, ödemede gecikme olması hâlinde bu sürenin sona erdiği tarihten ödeme tarihine kadar geçen süre için yasal FAİZ UYGULANMASINA,

G. Kararın bir örneğinin bilgi için İzmir Bölge İdare Mahkemesi 2. İdare Dava Dairesine (E.2017/7571) ve Adalet Bakanlığına GÖNDERİLMESİNE 10/3/2022 tarihinde OYBİRLİĞİYLE karar verildi.

Anayasa Mahkemesi - Kemal Karanfil Kararı (2017/24776)

Kemal Karanfil, B. No: 2017/24776, 24/5/2018

Başvuru, tutuklu olan başvurucuya gelen veya başvurucu tarafından gönderilen mektupların Ulusal Yargı Ağı Bilişim Sistemi ne kaydedilmesi nedeniyle özel hayata saygı hakkı ve haberleşme hürriyetinin ihlal edildiği iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

İKİNCİ BÖLÜM

KARAR

KEMAL KARANFİL BAŞVURUSU

(Başvuru Numarası: 2017/24776)

Karar Tarihi: 24/5/2018

İKİNCİ BÖLÜM

KARAR

Başkan: Engin YILDIRIM

Üyeler: Osman Alifeyyaz PAKSÜT, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ

Raportör: Elif ÇELİKDEMİR ANKİTÇİ

Başvurucu: Kemal KARANFİL

I. BAŞVURUNUN KONUSU

1. Başvuru, tutuklu olan başvurucuya gelen veya başvurucu tarafından gönderilen mektupların Ulusal Yargı Ağı Bilişim Sistemi'ne kaydedilmesi nedeniyle özel hayata saygı hakkı ve haberleşme hürriyetinin ihlal edildiği iddiasına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 23/5/2017 tarihinde yapılmıştır.

3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.
4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.
5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.
6. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık görüşünü sunmuştur.

III. OLAY VE OLGULAR

7. Başvuru formu ve eklerinde ifade edildiği şekliyle olaylar özetle şöyledir:
8. Başvurucu, hâkim olarak görev yapmakta iken 15 Temmuz Darbe Teşebüsünün ardından Fethullahçı Terör Örgütü/Paralel Devlet Yapılanması (FETÖ/PDY) soruşturması kapsamında 20/7/2016 tarihinde tutuklanmıştır. Başvurucu hâlen Kocaeli 2 No.lu T Tipi Kapalı Ceza İnfaz Kurumunda (İnfaz Kurumu) tutuklu olarak bulunmaktadır.
9. Bakanlık Ceza ve Tevkifevleri Genel Müdürlüğünün 10/10/2016 tarihli yazısıyla, infaz kurumunda bulunan tüm hükümlü ve tutukluların resmî makamlara veya savunması için avukatına verdiği kapalı zarf içindeki mektup ve faksler hariç tüm mektup, faks ve dilekçelerinin taranmak suretiyle Ulusal Yargı Ağı Bilişim Sistemi'ne (UYAP) kaydedilmesi gerektiği ülke genelindeki tüm infaz kurumlarına başsavcılıklar aracılığıyla iletilmiştir.
10. Bakanlığın yazısı doğrultusunda başvurucuya gönderilen veya başvurucunun göndermek istediği mektuplar taranmak suretiyle UYAP sistemine kaydedilerek sakıncalı olup olmadıkları yönünden denetlenmektedir.
11. Başvurucu, mektupların UYAP sistemine kaydedilmesinin haberleşme hürriyeti ile özel ve aile hayatının gizliliği ilkesine aykırılık oluşturduğunu ileri sürerek Kocaeli İnfaz Hâkimliğine (Mahkeme) şikâyetle bulunmuştur.
12. Mahkeme 24/3/2017 tarihli kararıyla, infaz hâkimliklerinin yetkisinin infaz kurumlarındaki işlem ve eylemlerin kanun, tüzük, yönetmelik veya genelgelere uygunluğunu denetiminden ibaret olduğunu açıklamış; mevcut uygulamanın Bakanlığın 10/10/2016 tarihli yazısına dayandığını ve yazının hukuken genelge niteliğinde olduğunu belirterek şikâyetin reddine karar vermiştir.

13. Başvurucunun anılan karara itirazı, Kocaeli 2. Ağır Ceza Mahkemesinin 14/4/2017 tarihli kararıyla reddedilmiştir. Ret kararı başvurucuya 27/4/2017 tarihinde tebliğ edilmiştir.

14. Başvurucu 23/5/2017 tarihinde bireysel başvuruda bulunmuştur.

IV. İLGİLİ HUKUK

A. Ulusal Hukuk

15. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (1) numaralı maddesi şöyledir:

"Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir."

16. 6698 sayılı Kanun'un 3. maddesinin (1) numaralı fıkrasının ilgili kısmı şöyledir:

"d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade eder."

17. 6698 sayılı Kanun'un 5. maddesinin ilgili kısmı şöyledir:

" (1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

...

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

..."

18. 6698 sayılı Kanun'un 6. maddesinin ilgili kısmı şöyledir:

"(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir .

..."

19. 6698 sayılı Kanun'un 28. maddesinin ilgili kısmışöyledir:

"(1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:

...

ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi".

20. 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu'nun 38/A maddesinin ilgili kısımları şöyledir:

"(1) Her türlü ceza muhakemesi işlemlerinde Ulusal Yargı Ağı Bilişim Sistemi (UYAP) kullanılır. Bu işlemlere ilişkin her türlü veri, bilgi, belge ve karar, UYAP vasıtasıyla işlenir, kaydedilir ve saklanır.

...

(7) Zorunlu nedenlerle fiziki olarak düzenlenmiş belge veya kararlar, yetkili kişilerce taranarak UYAP'a aktarılır ve gerektiğinde ilgili birimlere elektronik ortamda gönderilir.

...

(9) Elektronik ortamda yapılan işlemlerde süre gün sonunda biter.

...

(11) Ceza muhakemesi işlemlerinin UYAP'ta yapılmasına dair usul ve esaslar, Adalet Bakanlığı tarafından çıkarılacak yönetmelikle düzenlenir."

21. Bakanlık Bilgi İşlem Dairesi Başkanlığının 10/11/2011 tarihli ve 124/1 sayılı Genelgesi'nin ilgili kısmı şöyledir:

"UYAP Bilişim Sistemi kullanılarak soruşturma ve kovuşturma işlemleri ile diğer adlî ve idarî işlemlerin etkin, verimli, hızlı, düzenli, şeffaf ve usul ekonomisine uygun biçimde yürütülmesi amacıyla;

1- Her türlü işlem ve faaliyetin, UYAP üzerinden gerçekleştirilmesine imkân bulunmayan istisnai hâller saklı olmak koşuluyla, UYAP ortamında, zamanında, eksiksiz ve doğru bir biçimde gerçekleştirilmesi,

...

3- Tüm birimlerde her türlü veri girişinin eksiksiz ve doğru biçimde yapılması,

...

5- Zorunluluk sebebiyle haricen oluşturulan belgeler ile Sistem haricinde gelen belgelerin ekleriyle birlikte taranarak UYAP ortamına aktarılması,

...

15- Bilgi güvenliği, elektronik imza ve kişisel verilerin korunmasına ilişkin mevzuat hükümlerine azamî dikkat gösterilmesi, özellikle elektronik imza cihazı veya erişim kodu ile her türlü kullanıcı adı ve parolasının başkalarına verilmemesi ..."

22. 13/12/2004 tarihli ve 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun'un 68. maddesi şöyledir:

"Hükümlü, bu maddede belirlenen kısıtlamalar dışında, kendisine gönderilen mektup, faks ve telgrafları alma ve ücretleri kendisince karşılanmak koşuluyla, gönderme hakkına sahiptir.

(2) Hükümlü tarafından gönderilen ve kendisine gelen mektup, faks ve telgraflar; mektup okuma komisyonu bulunan kurumlarda bu komisyon, olmayanlarda kurumun en üst amirince denetlenir.

(3) Kurumun asayiş ve güvenliğini tehlikeye düşüren, görevlileri hedef gösteren, terör ve çıkar amaçlı suç örgütü veya diğer suç örgütleri mensuplarının haberleşmelerine neden olan, kişi veya kuruluşları paniğe yöneltmek yalan ve yanlış bilgileri, tehdit ve hakareti içeren mektup, faks ve telgraflar hükümlüye verilmez. Hükümlü tarafından yazılmış ise gönderilmez.

(4) Hükümlü tarafından resmî makamlara veya savunması için avukatına gönderilen mektup, faks ve telgraflar denetime tâbi değildir."

23. 6/4/2006 tarihli ve 26131 sayılı Resmî Gazete'de yayımlanan Ceza İnfaz Kurumlarının Yönetimi ile Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Tüzük'ün (Tüzük) 122. maddesi şöyledir:

"(1) 91 inci maddeye göre mektup alma ve gönderme hakkı kapsamında hükümlüler tarafından yazılan mektup, faks ve telgraflar, zarfı kapatılmaksızın bu işle görevlendirilen ikinci müdür başkanlığında, idare memuru ve yüksek okul mezunu iki infaz ve koruma memuru tarafından oluşturulan mektup okuma komisyonuna iletilmek üzere güvenlik ve gözetim servisi personeline verilir. Yapılan incelemeden sonra gönderilmesinde sakınca görülmeyen mektuplar üzerine "görüldü" kaşesi vurulur, zarf içerisine konularak kapatılır ve postaneye teslim edilir.

(2) Resmî makamlara veya savunması için avukatına gönderilenler hakkında 91 inci maddenin dördüncü fıkrası hükmü uygulanır.

(3) Hükümlülere gönderilen ve açılıp incelendikten sonra verilmesinde sakınca olmadığı anlaşılan mektup, faks ve telgraflar zarfları ile birlikte verilir."

24. Tüzük'ün 123. maddesi şöyledir:

"(1) Mektup okuma komisyonunca, mahalline gönderilmesi veya hükümlüye verilmesi sakıncalı görülen mektuplar, en geç yirmidört saat içinde disiplin kuruluna verilir. Mektubun disiplin kurulu tarafından kısmen veya tamamen sakıncalı görülmesi hâlinde, mektup aslı çizilmeden veya yok edilmeden şikâyet ve itiraz süresinin sonuna kadar muhafaza edilir. Mektubun kısmen sakıncalı görülmesi hâlinde, aslı idarede tutularak fotokopisinde sakıncalı görülen kısımlar okunmayacak şekilde çizilerek disiplin kurulu kararı ile birlikte ilgisine tebliğ edilir. Mektubun tamamının sakıncalı görülmesi hâlinde, sadece disiplin kurulu kararı tebliğ edilir. Tebliğ tarihinden itibaren infaz hâkimliğine başvuru için gereken süre beklenir. Bu süre içinde infaz hâkimliğine başvurulmamış ise, disiplin kurulu kararı yerine getirilir. İnfaz hâkimliğine başvurulmuş ise, infaz hâkimliği kararının tebliğinden itibaren itiraz süresi beklenir. İnfaz hâkimliği kararına itiraz edilmemiş ise bu karara göre, itiraz edilmiş ise mahkemenin kararına göre işlem yapılır.

(2) Hükümlüye yapılacak tebligatta, tebliğ tarihinden itibaren onbeş gün içinde infaz hâkimliğine şikâyet hakkının kullanılmaması veya infaz hâkimliği kararına karşı tebliğ tarihinden itibaren bir hafta içinde ağır ceza mahkemesine itiraz edilmemesi hâlinde, disiplin kurulu kararının kesinleşerek mektubun sakıncalı görülen kısımlarının okunmayacak şekilde çizilerek verileceği veya tamamı sakıncalı görülen mektubun verilmeyeceği bildirilir.

(3) Kısmen veya tamamen sakıncalı görülen mektuplar, iç hukuk veya uluslararası hukuk yollarına başvuru yapılması durumunda kullanılmak üzere idarece saklanır."

25. 26/6/1930 tarihli ve 1721 sayılı Hapishane ve Tevkifhanelerin İdaresi Hakkında Kanun'un 2. maddesinin ilgili kısmı şöyledir:

"E) Ceza evinin emniyeti bakımından mahkümlara ait mektupların ve kendilerini ziyarete gelenlerle konuşmalarının ve hariçle muhaberetlerinin ne suretle tanzim ve kontrol edileceği,

...

hakkında bir nizamname tanzim olunur.

..."

B. Uluslararası Hukuk

1. Uluslararası Mevzuat

26. Avrupa İnsan Hakları Sözleşmesi'nin (Sözleşme) "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesi şöyledir:

"1. Herkes özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesini isteme hakkına sahiptir.

2. Bu hakların kullanılmasına ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, suçun veya düzensizliğin önlenmesi, genel sağlık ve genel ahlakın korunması, başkalarının hak ve özgürlüklerinin korunması amacıyla, hukuka uygun olarak yapılan ve demokratik bir toplumda gerekli bulunan müdahaleler dışında, kamu makamları tarafından hiçbir müdahale yapılamaz."

27. Avrupa Konseyi bünyesinde hazırlanan 28/1/1981 tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin 2. maddesinin birinci fıkrasının (a) bendi şöyledir:

"Kişisel veriler': Kimliği belirli veya belirlenebilir bir gerçek kişi ('ilgili kişi') hakkındaki tüm bilgileri ifade eder."

28. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin 6. maddesinin ilgili kısmı şöyledir:

"İç hukukta uygun güvenceler sağlanmadıkça, ırksal kökeni, siyasi düşünceleri, dini veya diğer inançları ortaya koyan kişisel verileri ile sağlık veya cinsel hayatla ilgili kişisel veriler otomatik işleme tabi tutulamaz. Aynı şey ceza mahkumiyetiyle ilgili kişiler verileri içinde geçerlidir."

29. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin 9. maddesinin ilgili kısmı şöyledir:

"2. Taraf devletin kanunlarında öngörülmüş olması ve demokratik bir toplumda aşağıdaki hususların sağlanması için gerekli bir önlem oluşturması halinde iş bu sözleşmenin 5, 6, ve 8. maddelerine istisna getirilebilir:

a. Devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi ..."

30. Avrupa Konseyi Bakanlar Komitesinin Üye Devletlere Avrupa Cezaevleri Kuralları Hakkında REC (2006) 2 Sayılı Tavsiye Kararı'nın hükümlü ve tutukluların dış dünya ile ilişkilerine dair kısmı şöyledir:

"24. 1. Mahpusların mümkün olabilen sıklıkta mektup, telefon veya diğer iletişim vasıtalarıyla aileleriyle, başka kişilerle ve dışarıdaki kuruluşların temsilcileriyle haberleşmelerine ve bu kişilerin mahpusları ziyaret etmelerine izin verilmelidir.

24. 2 Devam etmekte olan bir ceza soruşturması, emniyet, güvenlik ve düzeninin muhafaza edilmesi, suç işlenmesinin önlenmesi ve suç mağdurunun korunması için gerekli görülmesi halinde, haberleşme ve ziyaretlere kısıtlamalar konabilir ve izlenebilir. Ancak adli bir merci tarafından konulan özel kısıtlamalar da dahil olmak üzere, bu tür kısıtlamalar yine de kabul edilebilir asgari bir iletişime izin vermelidir.

24.3. Ulusal hukuk, mahpuslarla iletişim kurması kısıtlanamayacak olan ulusal ve uluslararası kuruluşları belirlemelidir,

24.4. Ziyaretler için yapılan düzenlemeler, mahpuslara aile ilişkilerini mümkün olduğunca normal bir düzeyde sürdürmelerine ve geliştirmelerine izin verecek bir tarzda olmalıdır.

24.5. Cezaevi yetkilileri, dış dünyayla yeterli bir iletişim sürdürmelerinde mahpuslara yardım etmelidirler ve bunun için onlara uygun destek ve yardım sağlamalıdır."

2. Uluslararası İçtihat

31. Avrupa İnsan Hakları Mahkemesi (AİHM), devletlerin millî güvenliğin korunması amacını gerçekleştirmede sahip oldukları takdir yetkisinin geniş olduğunu kabul etmektedir. AİHM, Sözleşme'ye taraf devletlerin millî güvenliği korumak için yetkili ulusal makamlarına ilk olarak kişiler hakkında bilgi toplama ve halka açık olmayan siciller tutma, ikinci olarak millî güvenlik bakımından önemli kadrolarda çalışmak isteyen adayların bu işe uygunluğunu takdir ederken bu bilgiyi kullanma

yetkisi veren kurallara sahip olmaları gerektiğinde kuşku bulunmadığını belirtmektedir (Leander/İsveç, B. No: 9248/81, 26/03/1987, § 59).

32. Bununla birlikte AİHM içtihadına göre kamu mercilerinin bir bireyin özel hayatıyla ilgili bilgileri toplaması, kaydetmesi, saklaması, özel hayata saygı hakkına müdahale oluşturur (Leander/İsviçre, § 48;Kopp/İsviçre, B. No: 23224/94, 25/3/1998, § 53;Amann/İsviçre [BD], B. No: 27798/95, 16/2/2000, § 69; Rotaru/Romanya [BD], B. No: 28341/95, 4/5/2000, §§ 43, 44,46).

33. Kaydedilen bilgilerin daha sonra kullanılmış olup olmamasının bir önemi yoktur. Bununla birlikte kamu makamları tarafından muhafaza edilen kişisel nitelikli bilgilerin özel yaşam unsurlarından birini devreye sokup sokmadığını tespit etmek için bu bilgilerin hangi çerçevede alındığının ve muhafaza edildiğinin, verilerin türünün, kullanıldığı ve işlendiği şeklin, bunlardan çıkarılabilecek sonuçların dikkate alınması zaruridir (Leander/İsveç, § 48; Amann/İsviçre, § 69; S. ve Marper/Birleşik Krallık [BD], B. No: 30562/04, 30566/04, 4/12/2008, § 67).

34. AİHM kararlarına göre haberleşme özgürlüğüne yapılan müdahale öncelikle kanunla öngörülmedir. Müdahalenin yasal dayanağını oluşturan mevzuatın ulaşılabilir, yeterince açık ve belirli bir eylemin gerektirdiği sonuçlar açısından öngörülebilir olması gerekir. İkinci olarak söz konusu sınırlandırma meşru bir amaca dayalı olmalı; bunun yanı sıra müdahale demokratik bir toplumda gerekli ve ölçülü olmalıdır (Silver ve diğerleri/Birleşik Krallık, B. No: 5947/72...25/3/1983, §§ 85-90; Klass ve diğerleri/Almanya, B. No: 5029/71, 6/10/1978, §§ 42-55; Campbell/Birleşik Krallık, B. No:13590/88, 25/3/1992, § 34).

35. AİHM; haberleşme hürriyetine yapılan müdahalelerin incelediği kararlarda, öncelikle ceza infaz kurumlarında bulunan kimselerin yazışmalarının belirli ölçüde kontrolünün başlı başına Sözleşme'nin ihlaline sebebiyet vermeyeceğini, keza ceza infaz kurumunun olağan ve makul gereksinimleri dikkate alınarak bir değerlendirmede bulunmanın gerekli olduğunu belirtmiştir (Mehmet Nuri Özen/Türkiye, B. No: 15672/08...11/1/2011, § 51; Silver ve diğerleri/Birleşik Krallık, § 98).

36. AİHM, her somut olayda kamu makamlarının bu değerlendirmeyi yaparken mektup gönderme ve almanın ceza infaz kurumlarında bulunan hükümlülerin ve tutukluların dış dünya ile tek bağlantısı olduğu gerçeğini gözönünde bulundurması gereğini belirtmektedir (Campbell/Birleşik Krallık,§ 45).

V. İNCELEME VE GEREKÇE

37. Mahkemenin 24/5/2018 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Adli Yardım Talebi Yönünden

38. Başvurucu, adli yardım talebinde bulunmuştur.

39. Anayasa Mahkemesinin Mehmet Şerif Ay (B. No: 2012/1181, 17/9/2013) kararında belirtilen ilkeler dikkate alınarak geçimini önemli ölçüde zor duruma düşürmeksizin yargılama giderlerini ödeme gücünden yoksun olduğu anlaşılan başvurusunun açıkça dayanaktan yoksun olmayan adli yardım talebinin kabulüne karar verilmesi gerekir.

B. Özel Hayata Saygı Hakkı ile Haberleşme Hürriyetinin İhlal Edildiğine İlişkin İddia

1. Başvurucunun İddiaları ve Bakanlık Görüşü

40. Başvurucu, tutuklu olarak bulunduğu İnfaz Kurumunda kendisine gönderilen veya kendisinin göndermek istediği mektupların tamamının taranmak suretiyle UYAP sistemine kaydının yapılması nedeniyle haberleşmenin gizliliği ilkesinin ihlal edildiğini ileri sürmüştür. Öte yandan bu uygulamanın özel yazışmalarının bir sistemde depolanıp saklanması sonucunu doğurduğu için özel hayatına saygı hakkının da ihlal ettiğini iddia etmiştir. Ayrıca söz konusu uygulamanın kaldırılması için İnfaz Hâkimliğine yaptığı şikâyetinin reddedildiğini, bu ret kararına karşı yaptığı itirazının da Ağır Ceza Mahkemesince gerekçesiz olarak reddediğini belirterek adil yargılanma hakkının ihlal edildiğini ifade etmiştir.

41. Bakanlık görüşünde, ceza infaz kurumunda bulunan mahpusların haberleşmelerinin denetlenebileceği ve bu kapsamda UYAP'a kaydedilebileceği belirtildikten sonra müdahalenin kamu düzeni ve kurum güvenliğini sağlamaya yönelik anayasal açıdan meşru bir amaca dayandığı ve güdülen meşru amaçla başvurusunun bireysel yararı arasında adil bir dengenin kurulmuş olması nedeniyle de ölçülü olduğu açıklanmıştır.

2. Değerlendirme

42. Anayasa'nın 20. maddesinin ilgili kısmı şöyledir:

“Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

...

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de

kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.”

43. Anayasa'nın 22. maddesi şöyledir:

"Herkes, haberleşme hürriyetinesahiptir. Haberleşmenin gizliliği esastır.

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.

İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir."

44. Özel hayata saygı hakkı kapsamında korunan hukuksal çıkarlardan biri, bireyin mahremiyet hakkıdır. Ancak mahremiyet hakkı sadece yalnız bırakılma hakkından ibaret olmayıp bu hak, bireyin kendisi hakkındaki bilgileri kontrol edebilme hukuksal çıkarını da kapsamaktadır. Bireyin kendisine ilişkin herhangi bir bilginin kendi rızası olmaksızın açıklanmaması, yayılmaması, bu bilgilere başkaları tarafından ulaşılamaması ve rızası hilafına kullanılamaması, kısaca bu bilgilerin mahrem kalması konusunda menfaati bulunmaktadır. Bu husus, bireyin kendisi hakkındaki bilgilerin geleceğini belirleme hakkına işaret etmektedir (Serap Tortuk, B. No: 2013/9660, 21/1/2015, § 32).

45. Anayasa Mahkemesi tarafından kişisel veri kavramının -belirli veya kimliği belirlenebilir olmak şartıyla- bir kişiye ilişkin bütün bilgileri ifade ettiği kabul edilmekte olup bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgilerin değil telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, öz geçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunduğu kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm verilerin kişisel veri kapsamında olduğu belirtilmektedir (AYM, E.2014/74, K.2014/201, 25/12/2014; E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2013/84, K.2014/183, 4/12/2014; E.2014/180, K.2015/30, 19/3/2015; Bülent Kaya [GK], B. No: 2013/2941, 11/5/2016, § 49).

46. Bu noktada Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi ile 6698 sayılı Kanun da önemli tespitler içermektedir. Belirtilen sözleşme ve Kanun'a göre

kişisel bilgi, belirli veya belirlenebilir bir kişiye ilişkin herhangi bir bilgi olarak tanımlanmakta ve söz konusu verilerin özel nitelikte olması gibi bir unsur aranmamaktadır. Dolayısıyla ceza infaz kurumlarında bulunan mahpusların yazdığı veya kendilerine hitaben yazılan mektupların UYAP sistemine taranması suretiyle kaydı sağlandığından sadece mektup içeriklerinin değil aynı zamanda mektuplardaki el yazısı, imza gibi mektubu yazanı belirlemeye yarayan her türlü bilgi kişisel veri sayılmaktadır.

47. Söz konusu haberleşme içeriklerinin ve biçiminin denetlenerek bir sisteme kaydedilmesi, bireyin mahremiyetine olduğu kadar aynı zamanda haberleşme hürriyetine de müdahale oluşturmaktadır.

48. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Başvurucunun iddiasının temeli, başvurucuya gönderilen veya başvurucunun göndermek istediği tüm mektupların İnfaz Kurumu idaresi tarafından UYAP sistemine kaydedilmesine ilişkindir. Bireyin kişisel verilerinin ve bu verilerin korunmasına dair menfaatinin özel yaşamı kapsamında olduğu açıktır. Haberleşme içeriklerinin ve biçiminin kaydı şeklinde gerçekleşen müdahalenin haberleşme hürriyetine yapılan müdahalenin özel bir biçimi olduğu hususunda da tereddüt bulunmamaktadır. Dolayısıyla mahremiyet hakkı ve bu alana ilişkin bilgilerin gizliliğinin korunması ile haberleşmenin denetlenmesine ilişkin eldeki başvurunun Anayasa'nın 20. ve 22. maddeleri çerçevesinde özel hayata saygı ve haberleşme hürriyeti yönünden ve birlikte incelenmesi gerektiği değerlendirilmiştir.

a. Kabul Edilebilirlik Yönünden

49. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan özel hayata saygı ve haberleşme hakkının ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

b. Esas Yönünden

i. Müdahalenin Varlığı

50. Kamu mercileri tarafından özel yaşamı ile ilgili sorular sorulması da dâhil olmak üzere bir bireyin özel hayatı, iş ve sosyal yaşamıyla ilgili bilgilerinin, parmak izinin, fotoğrafının, hücre ve DNA örneklerinin alınması, kaydedilmesi, saklanması ve kullanılması özel hayata saygı hakkına müdahale oluşturur (Bülent Kaya, § 51).

51. Kaydedilen bilgilerin daha sonra kullanılmış olup olmamasının bir önemi yoktur. Bununla birlikte kamu makamları tarafından muhafaza edilen kişisel nitelikli bilgilerin özel yaşam unsurlarından

birini devreye sokup sokmadığını tespit etmek için bu bilgilerin hangi çerçevede alındığının ve muhafaza edildiğinin, verilerin türünün, kullanıldığı ve işlendiği şeklin, bunlardan çıkarılabilecek sonuçların dikkate alınması zaruridir (Bülent Kaya, § 53).

52. Ceza infaz kurumunda bulunan mahpusların haberleşmelerinin denetlenmesi haberleşme hürriyetine müdahale teşkil etmektedir (Mehmet Koray Eryaşa, B. No: 2013/6693, 16/4/2015).

53. Başvurucu, infaz kurumunda tutuklu olarak bulunmaktadır. Başvurucunun dış dünyayla iletişimini sağlayan yazışmaları bazı istisnalar haricinde (bkz. § 9) kurum idaresi tarafından denetlenerek UYAP sistemine kaydedilmektedir. Kişiye ait bilgileri içeren mektupların açılıp okunarak sistemde tutulmasının başvurucunun özel hayatına ve haberleşmesine müdahale oluşturduğu şüphesizdir.

ii. Müdahalenin İhlal Oluşturup Oluşturmadığı

54. Anayasa'nın 13. maddesi şöyledir:

"Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz."

55. Yukarıda belirlenen müdahale, Anayasa'nın 13. maddesinde belirtilen koşullara uygun olmadığı takdirde Anayasa'nın 20. maddesini ihlal edecektir. Bu sebeple sınırlamanın Anayasa'nın 13. maddesinde öngörülen ve somut başvuruya uygun düşen, kanun tarafından öngörülme, meşru amaç taşıma, demokratik toplum düzeninin gereklerine uygunluk ve ölçülülük ilkesine aykırı olmama koşullarına uygun olup olmadığının belirlenmesi gerekir.

(1) Kanunilik

56. Hak ve özgürlüklerin kanunla sınırlanması ölçütü anayasa yargısında önemli bir yere sahiptir. Hak ya da özgürlüğe bir müdahale söz konusu olduğunda öncelikle tespiti gereken husus, müdahaleye yetki veren bir kanun hükmünün yani müdahalenin hukuki bir temelini mevcut olup olmadığıdır (Sevim Akat Eşki, B. No: 2013/2187, 19/12/2013, § 36).

57. Anayasa'nın 20. maddesi kapsamında yapılan bir müdahalenin yasallık şartını sağladığının kabulü için de müdahalenin kanuni bir dayanağının bulunması zorunludur. Bununla birlikte temel hak ve hürriyetlerin sınırlandırılmasına ilişkin kanunların şeklen var olması yeterli değildir. Yasallık ölçütü aynı zamanda maddi bir içeriği de gerektirmekte olup bu noktada kanunun niteliği önem

kazanmaktadır. Yasayla sınırlama ölçütü, sınırlamanın erişilebilirliğini, öngörülebilirliğini ve kesinliğini ifade etmekte, böylece uygulayıcının keyfî davranışlarının önüne geçtiği gibi kişinin hukuku bilmesine de yardımcı olmakta ve bu yönüyle hukuk güvenliği güvencesi sağlamaktadır (Halime Sare Aysal [GK], B. No: 2013/1789, 11/11/2015, § 62).

58. Kanunun bu gerekliliklere uygun olduğunun söylenebilmesi için yeterince ulaşılabilir olması, yani vatandaşların belirli bir olaya uygulanabilir nitelikteki hukuk kurallarının varlığı hakkında yeterli bilgiye sahip olabilmesi, ayrıca ilgili normun keyfiliğe karşı uygun bir koruma sağlaması, yetkili makamlara verilen yetkinin genişliğini ve icra edilme biçimlerini yeterli bir netlikte tanımlaması gerekmektedir (Halime Sare Aysal, § 63).

59. Somut başvuru açısından ise kişisel verilerin kayıt, muhafaza ve kullanımını içeren tedbirlerin kapsamını ve uygulanmasını düzenleyen ve özellikle süre, stoklama, kullanım, üçüncü kişilerin erişimi, verilerin gizliliği, bütünlüğü ve imhası konusundaki prosedürlere ilişkin olarak muhataplarının yetki aşımı ve keyfiliğe karşı yeteri kadar güvenceye sahip olmalarını sağlayacak açık ve detaylı kuralların belirlenmesinin söz konusu gerekliliklere temel oluşturduğu açıktır (Bülent Kaya, § 64).

60. Bu kapsamda ilgili sisteme bilgilerin girilmesi, müdahaleye temel oluşturan meşru amaçları taşıma şartına bağlı olmalı ve söz konusu yasal düzenleme, hangi bilgilerin kayıt altına alınabileceği, hangi yetkililere iletilebileceği, böyle bir iletimin hangi koşullarda mümkün olabileceği ve bilginin ilgili makamlara iletilmesi hususunda izlenecek usul konusunda açık ve ayrıntılı hükümler içermelidir. Söz konusu sisteme ilişkin düzenleme; bilgi toplama, kaydetme ve ilgili makamlarla paylaşma veya sair şekilde kullanma konusunda yetkili makamlara tanıdığı takdir yetkisinin kullanılma tarzı ve alanı bakımından vatandaşlara yeterince öngörülebilir bulunma olanağı sağlamak durumundadır (Bülent Kaya, § 66).

61. Öte yandan Anayasa Mahkemesi; Anayasa'da temel hak ve özgürlüklerin sınırlandırılması gibi münhasıran kanunla düzenlenmesi öngörülen konularda kanunun, söz konusu meselenin temel esaslarını, ilkelerini ve çerçevesini belirlemiş olmasını gerektirdiğini ancak yasama organının meselenin temel kurallarını saptadıktan sonra uzmanlık ve idare tekniğine ilişkin hususları yürütmeye bırakmasının yasama yetkisinin devri olarak yorumlanamayacağını kabul etmiştir (AYM, E.2014/133, K.2014/165, 30/10/2014). Bu bağlamda temel hak ve özgürlüklerin sınırlandırılmasına yönelik kanuni düzenlemelerde kanun koyucu tarafından temel esaslar, ilkeler ve çerçeve belirlendikten sonra diğer ayrıntıların düzenleyici işlemler ile belirlenebileceği kabul edilmiştir (Mehmet Koray Eryaşa, B. No: 2013/6693, 16/4/2015, § 63).

62. Başvuruya konu idari uygulama ve yargısal sürecin 5271 sayılı Kanun'un 38/A maddesi, 5275 sayılı Kanun'un sayılı 68. maddesi, Tüzük'ün 122. ve 123. maddeleri ile 3/5/1973 tarihli ve 1712 sayılı Kanun'un 2. maddesine dayanılarak Bakanlığın 10/10/2016 tarihli yazısı temelinde yürütüldüğü anlaşılmaktadır.

63. UYAP, 2008 yılından itibaren ülke genelindeki yargı birimleri tarafından tüm işlemlerde etkin biçimde kullanılan bir bilişim sistemidir. Hükümlü ve tutukluların bulunduğu ceza infaz kurumları da bu bakımdan önemli bir yere sahiptir. Hükümlü ve tutukluların tüm infaz işlemleri ile birlikte kurumda kalmalarından kaynaklanan talep ve şikâyetleri de idari ve yargısal işlemler olarak UYAP sistemi üzerinden yürütülmektedir.

64. Ceza infaz kurumlarında bulunan hükümlü veya tutukluların yaptıkları yazışmaların denetimi ve sınırlandırılmasının 5275 sayılı Kanun'un 68. maddesine dayandığı açıktır (Ahmet Temiz, B. No: 2013/1822, 20/5/2015, §§ 37-46). Uygulama, ancak ilgili yazışmanın incelenerek içeriğinin denetlenmesi sonucu mümkün olabilmektedir. Sakıncalı olarak değerlendirilen yazışmanın hakkındaki yargısal işlemlerin tamamlanması için gerekli süre sonuna kadar kurumca muhafaza edilmesi ise kanuni bir zorunluluktur.

65. Yargı birimleri tarafından gerçekleştirilen idari veya yargısal işlemlerde işlemle ilgili fiziki tüm evrakın işlem şeffaflığını sağlamak amacıyla UYAP sistemine kaydedildiği bilinmektedir. Bu evrak arasında belirli kişilere ait kişisel bilgilerin yer alması da işin doğası gereği mümkündür. Kişisel veri niteliğinde olan bu bilgilerin sisteme hangi kurallar çerçevesinde, hangi amaçla ve kimler tarafından kaydedileceği ve saklanacağı, bilgileri kaydeden yargı biriminin niteliğine göre ilgili kanunda düzenlenmektedir.

66. Ceza infaz kurumları da 5271 sayılı Kanun'un 38/A maddesi gereği UYAP sistemini kullanmaktadır. Maddeye göre kişisel verilerin UYAP sistemine kaydedileceği hususu ilkesel olarak belirlenmekle birlikte ayrıntıların düzenleyici işlemlere bırakıldığı anlaşılmaktadır. Bakanlığın bu yöndeki 10/10/2016 tarihli yazısı da derece mahkemelerince açıklandığı üzere genelge niteliğinde olup adı konulmamış bir düzenleyici işlemdir. Anılan genelgede denetime tabi olan tüm yazışmaların UYAP sistemine kaydedileceği açıkça belirtilmiştir.

67. Müdahalenin kanuni dayanağının mevcut olduğunu tespit edebilmek için ilgili kanunun yeterince ulaşılabilir olması gerekmektedir. Yukarıda belirtilen kanunların ulaşılabilir ve öngörülebilir olmasının yanı sıra Bakanlıkça bu husustaki genelgelerden konuyla birebir ilişkili olanların bizzat ilgililere de tebliğ edildiği gözönüne alındığında sınırlamanın öngörülebilir olduğu söylenebilmektedir.

68. Diğer taraftan 6698 sayılı Kanun gereğince kişisel verilerinin ilgilinin rızası dışında kaydedilememesi kural olarak kabul edilmiş ise de kamu güvenliği gibi bazı istisnai hâllerde kişinin rızası hilafına verilerin kaydedilebileceği belirtilmiştir. İnfaz kurumları da kamu güvenliği kapsamında infaz kurumunda güvenliğin sağlanması ve suç işlenmesinin önlenmesi amacıyla mahkumların yazışmalarını denetlerken yazışma hakkında birtakım idari ve yargısal işlemler yapılacağından ilgili yazışmanın diğer bilgiler gibi UYAP sistemine kaydedilmesi olağandır.

69. Bu bağlamda hükümlü ve tutukluların denetime tabi yazışmalarının diğer kişisel veriler gibi UYAP sistemine kaydedilmesi şeklindeki müdahalenin kanuni dayanağının mevcut olduğu anlaşılmaktadır.

(2) Meşru Amaç

70. İnfaz kurumlarının Anayasa'nın 22. maddesinin üçüncü fıkrası kapsamında kalan istisnai kamu kurumları olduğu kabul edilmekle birlikte bu istisna, anılan kurumlar tarafından hâkim kararı alınması şartı aranmaksızın haberleşme hürriyetine müdahale niteliğinde işlem tesis edilebileceği anlamına gelmektedir. Bununla birlikte bu kurumların haberleşme hürriyetine müdahale anlamındaki işlemlerinin meşru olabilmesi için mutlaka Anayasa'nın 22. maddesinin ikinci fıkrasında sayılan sınırlandırma sebeplerine dayalı olması gerekmektedir (Ahmet Temiz, § 50).

71. Somut başvuru açısından hükümlü veya tutuklulara ait mektupların UYAP sistemine kaydedilerek söz konusu mektuplarda yer alan bilgilerin suç işlenmesinin önlenmesi, İnfaz Kurumu güvenliğinin sağlanması kapsamında denetlendiği, dolayısıyla söz konusu uygulamanın Anayasa'nın haberleşme özgürlüğüne ilişkin 22. maddesinin ikinci fıkrası kapsamında kamu düzeni ve güvenliğinin temini şeklinde meşru bir amacının bulunduğu sonucuna ulaşılmaktadır.

(3) Demokratik Toplum Düzeninin Gereklerine Uygunluk ve Ölçülülük

(a) Genel İlkeler

72. Özel hayata saygı hakkının sınırlanması mümkün olmakla beraber Anayasa'nın 13. maddesi vasıtasıyla Anayasa'da yer alan tüm temel hak ve özgürlüklerin sınırlandırılması hususunda geçerli olan ilkeler, özel hayata saygı hakkının sınırlandırılmasında da gözönünde bulundurulmalıdır. Buna göre demokratik toplum düzeninin gerekleri gözetilmeli, sınırlamada öngörülen meşru amaç ile sınırlandırma aracı arasında orantısızlık bulunmamalı, sınırlandırmayla ulaşılabilecek genel yarar ile temel hak ve özgürlüğü sınırlandırılan bireyin kaybı arasında adil bir denge kurulmasına özen gösterilmelidir (Marcus Frank Cerny [GK], B. No: 2013/5126, 2/7/2015, § 73; Bülent Polat [GK], B. No: 2013/7666, 10/12/2015, §§ 104, 107; Serap Tortuk, §§ 44, 48).

73. Başvuru konusu olay bakımından yapılacak değerlendirmenin temel eksenini, müdahaleye neden olan idare ve derece mahkemelerinin kararlarında dayandıkları gerekçelerin özel hayata saygı hakkını kısıtlama bakımından demokratik bir toplumda gerekli ve ölçülülük ilkesine uygun olduğunun inandırıcı bir şekilde ortaya konulup konulmadığı olacaktır. Bu çerçevede bir müdahale, meşru amaçla orantılı bir müdahale olmalıdır. İkinci olarak müdahalenin haklılığı için kamu makamlarının gösterdikleri gerekçeler konuyla ilgili ve yeterli olmalıdır (Marcus Frank Cerny, § 83).

(b) İlkelerin Olaya Uygulanması

74. İnfaz kurumunda tutuklu veya hükümlü olanların yazışmaları, kural olarak denetime tabi olup denetim sürecinin sağlıklı işlemesi ve yeri geldiğinde yapılan müdahale nedeniyle bireylerin hak kayıplarının önüne geçilmesi amacıyla diğer tüm yargısal işlemlerde olduğu gibi UYAP sistemine işlenmektedir.

75. Ülkedeki terör suçlarına yönelik gelişmeler dikkate alındığında ceza infaz kurumlarında kapasitelerinin üstünde kişi bulunduğu bilinmektedir. Dolayısıyla infaz kurumlarının mevcudu ile personel sayısı dikkate alındığında tutuklu veya hükümlülerin yazışmalarının korunması ve denetlenmesi amacıyla ek tedbirlere başvurulması kaçınılmazdır. Bu doğrultudaki tedbirlerden biri olan yazışmaların UYAP sistemine kaydedilmesi suretiyle, denetimin tam anlamıyla gerçekleştirilebilmesinin yanı sıra yazışma metinlerine dair olası kayıpların önüne geçilerek bireylerin menfaatine de hizmet edilmesi amaçlanmaktadır.

76. Sisteme kaydedilen bilgiler arasında müdahaleye maruz kalan kişilerin -bu arada başvuru yapan- özel nitelikteki kişisel verilerinin bulunması mümkündür. Yazışmaların denetiminin amacının, öncelikle suç işlenmesinin önlenmesi ve ceza infaz kurumunun güvenliğinin sağlanması ve böylelikle kamu düzeninin korunması olduğu gözönüne alındığında denetimin bir parçası olan verilerin kaydı suretiyle bireyin mahremiyet hakkına yapılan müdahalenin toplum menfaati karşısında gerekli olmadığını söylemek mümkün görünmemektedir.

77. Öte yandan somut başvuruda uygulanan tedbirin mahpuslara gönderilen veya mahpuslarca başkalarına gönderilen mektupların UYAP ortamına kaydedilmesinden ibaret olduğu anlaşılmaktadır. Kişisel veri mahiyetindeki bu yazışmaların ceza infaz kurumunun yetkili personeli hariç herhangi bir üçüncü kişinin erişimine veya kullanımına açılması söz konusu değildir. Bu yazışmaların muhafazası hususunda yeterli düzenlemenin mevcut olduğu anlaşılmaktadır. Ayrıca bilgilere erişim yetkisi bulunan -çok sınırlı sayıdaki- yetkili kişilerin bunu kötüye kullanması veya kanunda öngörülen hâller dışında başka kişi ve kurumlara vermesi veya onların erişimine dahi açık hâle getirmesi hâlinde bunlara yönelik olarak uygulanacak idari, cezai ve hukuki müeyyideler

kanunlarda öngörülmektedir. Tüm bu hususlar gözetildiğinde mahpusların yazışmalarının UYAP sistemine kaydedilmesinden ibaret olan müdahalenin başvurucuya aşırı bir külfet yüklediği ve ceza infaz kurumunun güvenliğinin sağlanmasındaki kamu yararı ile başvurucunun haberleşme hürriyetinin ve kişisel verilerinin korunmasındaki bireysel yarar arasındaki makul dengenin gözetildiği sonucuna varılmaktadır.

78. Bununla birlikte Anayasa Mahkemesi kişisel veri mahiyetindeki mektupların UYAP ortamına kaydedilmesindeki hassasiyetin farkındadır. Anayasa Mahkemesi mektupların UYAP ortamına kaydedilmesi biçimindeki müdahaleyi yukarıda açıklanan koşulları gözeterek orantılı bulsa da bu durum mahpusların mektuplarının kaydı hususunda kamu makamlarına sınırsız yetki verildiği biçiminde anlaşılabilir. Anayasa Mahkemesince yukarıda belirtilen ve müdahalenin orantılı bulunmasında dayanak alınan koşulların fiilen sağlanmadığının veya mektupların kaydedilmesindeki meşru amacın ortadan kalktığına tespit edilmesi hâlinde ihlal sonucuna ulaşması mümkün ise de bu aşamada henüz bir hak ihlaline sebebiyet verilmediği kanaatine varılmaktadır.

79. Açıklanan gerekçelerle Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkının ve 22. maddesinde güvence altına alınan haberleşme hürriyetinin ihlal edilmediğine karar verilmesi gerekir.

Engin YILDIRIM bu görüşe katılmamıştır.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Adli yardım talebinin KABULÜNE OYBİRLİĞİYLE,

B. Özel hayata saygı hakkının ve haberleşme hürriyetinin ihlal edildiğine ilişkin iddianın KABUL EDİLEBİLİR OLDUĞUNA OYBİRLİĞİYLE,

C. Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkının ve 22. maddesinde güvence altına alınan haberleşme hürriyetinin İHLAL EDİLMEDİĞİNE Engin YILDIRIM'ın karşıoyu ve OYÇOKLUĞUYLA,

D. Kararın bir örneğinin Adalet Bakanlığına GÖNDERİLMESİNE,

E. 12/1/2011 tarihli ve 6100 sayılı Hukuk Muhakemeleri Kanunu'nun 339. maddesinin (2) numaralı fıkrası uyarınca tahsil edilmesi mağduriyetine neden olacağından başvurucunun yargılama giderlerini ödemekten TAMAMEN MUAF TUTULMASINA 24/5/2018 tarihinde karar verildi.

KARŞIOY GEREKÇESİ

1. Bir infaz kurumunda tutuklu bulunan başvuru, özel yazışmalarının ve mektuplarının UYAP sistemine kaydedilmesinden yakınmaktadır. İnfaz kurumlarında tutuklu ve hükümlülerin yazışmaları, kural olarak denetime tabidir. Başvurucunun şikayetine neden olan işlem Adalet Bakanlığının 10/10/2016 tarihli yazısından kaynaklanmaktadır. Bakanlık yazısında denetime tabi olan tüm yazışmaların UYAP sistemine kaydedileceği ifade edilmiştir.

2. Düzenleyici işlem anlamında bir genelge niteliğinde değerlendirilmesi mümkün olan Bakanlık yazısı kanuni temel olarak 5271 sayılı Kanun'un 38/A maddesi,5275 sayılı Kanun'un sayılı 68. maddesi, ilgili Tüzük'ün 122. ve 123. maddeleri ile 1712 sayılı Kanun'un 2. maddesine dayanmaktadır. Dolayısıyla başvuru özel hayata saygı hakkına yapılan müdahalenin kanuni dayanağının olmadığını söyleyemeyiz.

3. Hükümlü veya tutuklulara ait mektupların UYAP sistemine kaydı yapılarak söz konusu mektuplarda yer alan bilgilerin suç işlenmesinin önlenmesi kapsamında denetlendiği, dolayısıyla söz konusu uygulamanın kamu düzeni ve güvenliğini sağlamaya dönük meşru amacını taşıdığını kabul etmek gerekir.

4. Somut başvuruda müdahaleye neden olan idare ve derece mahkemelerinin kararlarında dayandıkları gerekçelerin özel hayata saygı hakkını kısıtlama bakımından demokratik bir toplumda gerekli ve ölçülülük ilkesine uygun olup, olmadığını değerlendirilmesi gerekmektedir.

5. Özel hayata saygı hakkının önemli unsurlarından biri olan mahremiyet hakkı kişinin kendisi hakkındaki bilgiler ve veriler üzerinde denetim ve söz sahibi olma hukuksal çıkarını da içermektedir. Kişinin kendisine ilişkin herhangi bir bilginin veya verinin rızası olmadan açıklanmaması, paylaşılmaması, bu bilgilere başkaları tarafından ulaşılamaması ve rızasına aykırı düşecek şekilde kullanılmaması gerekmektedir. Mahkememizin konuyla ilgili içtihadı da bu yöndedir (Serap Tortuk, B. No: 2013/9660, 21/1/2015).

6. Diğer taraftan 6693 sayılı Kanun kişinin kişisel verilerinin rızası dışında kaydedilememesini kural olarak benimsemekle birlikte kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesinin Kanunda sunulan güvencelerden yararlanılmasının istisnasını oluşturduğunu da hüküm altına almaktadır.

7. Özel hayata saygı hakkının sınırlanması mümkün olmakla beraber, Anayasa'nın 13. maddesi vasıtasıyla Anayasa'da yer alan tüm temel hak ve özgürlüklerin sınırlandırılması hususunda geçerli olan ilkeler, özel hayata saygı hakkının sınırlandırılmasında da gözönünde bulundurulmalıdır. Buna

göre demokratik toplum düzeninin gerekleri gözetilmeli, sınırlamada öngörülen meşru amaç ile sınırlandırma aracı arasında orantısızlık bulunmamalı, sınırlandırmayla ulaşılabilecek genel yarar ile temel hak ve özgürlüğü sınırlandırılan bireyin kaybı arasında adil bir denge kurulmasına özen gösterilmelidir (Marcus Frank Cerny [GK], B. No: 2013/5126, 2/7/2015, § 73; Serap Tortuk, §§ 44, 48).

8. Bakanlığın 10/10/2016 tarihli yazısında tüm hükümlü ve tutukluların resmi makamlara veya savunması için avukatına verdiği kapalı zarf içindeki mektup ve faks ve hariç diğer tüm faks ve dilekçelerin taranmak suretiyle UYAP sistemine kaydedilmesi gerektiği belirtilmektedir. Dolayısıyla tutuklu ve hükümlülerin yargısal süreçlerle hiçbir ilgisi olmayan kişisel verilerini de içerebilecek olan özel yazışmaları da sakıncalı olup, olmadığına bakılmaksızın UYAP sistemine kaydedilecektir. Bu özel yazışmaların ne kadar süreyle sistemde saklı tutulacağı, bunların üçüncü kişilerin erişimine ve kullanımına açılıp açılmayacağı, infaz kurumu tarafından hangi mercilerle paylaşılıp paylaşılamayacağı ve bunun nasıl olacağı hususlarında ciddi bir belirsizlik söz konusudur.

9. Kişisel verilerin kayıt, muhafaza ve kullanımını içeren tedbirlerin kapsamını ve uygulanmasını düzenleyen ve özellikle süre, stoklama, kullanım, üçüncü kişilerin erişimi, verilerin gizliliği, bütünlüğü ve imhası konusundaki prosedürlere ilişkin, muhataplarının yetki aşımı ve keyfilige karşı yeteri kadar güvenceye sahip olmalarını sağlayacak açık ve detaylı kuralların yokluğu somut başvuruya neden olan müdahalenin demokratik toplum düzeni açısından ölçülü olmadığı konusunda ciddi şüpheler uyandırmaktadır.

10. Çoğunluk görüşünde "...bilgilerin tespit edilen amaç dışında yararlanıldığına yahut başvurucunun özel yaşamı bakımından olumsuz sonuçlar doğurduğuna ilişkin somut olgulara dayalı herhangi bir delil başvurucu tarafından ortaya konulamamıştır. Kaldı ki yazışmalarda yer alan bilgilerin amacı dışında kullanılmayacağı ve bu doğrultuda üçüncü kişilere verilemeyeceği muhakkaktır" (bkz. § 70) düşüncesi savunularak UYAP sistemine yapılan kaydın başvurucuya aşırı külfet yüklediğinden orantılı olduğu sonucuna ulaşılmıştır.

11. Başvurucunun özel yazışmalarının hiçbir değerlendirmeye tabi tutulmadan otomatikman UYAP sistemine kaydedilmesi işleminin bireyin özel hayatı açısından ne gibi olumsuzluklara neden olduğunun somut olarak ortaya konulması imkânsız olmasa bile çok zordur. Bireyin sevdiği bir kimseye yazdığı çok özel ifadelerin başkaları tarafından okunma olasılığının varlığını düşünmesi, bu yazışmadaki ifadelerin, duyguların, belki de kişisel hassas verilerinin büyük bir veri seti içerisinde ucu açık bir şekilde tutulmasının bireye manevi anlamda kendi iç dünyasında aşırı bir külfet yüklediğini söylemek kolay değildir. Çoğunluk, kişinin yazışmalarında yer alan bilgilerin amaç dışında kullanılmayacağından ve bu yönde üçüncü kişilere verilmeyeceğinden haddinden fazla emin

görünmektedir. Thomas Jefferson'ın anayasacılıkla ilgili deyişini biraz deęiştirerek söylemek gerekirse, veri ve veri seti söz konusu olduğunda “insanlara hiçbir zaman güvenmemek ve onları kötülük yapmamaları için anayasanın zincirine bağlamak gerekir”.

12. Sonuç olarak, gerçekleştirilen müdahale demokratik toplum düzeni açısından acil ve baskılayıcı bir toplumsal ihtiyaca cevap vermemekte ve ulaşılmak istenen kamu düzeninin korunması amacı ile bireysel yarar arasında makul bir denge kurmayarak, bireye katlanmak zorunda olmadığı bir külfet getirmektedir.

13. Açıklanan gerekçelerle başvurucunun Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkının ihlal edildięi düşüncesiyle karara katılmıyorum.

Anayasa Mahkemesi - A.A.Y. Kararı (2016/13011)

A.A.Y., B. No: 2016/13011, 29/9/2020

Başvuru, özel bir şirkette çalışan başvurucunun kurumsal e-posta hesabı içeriğinin işveren tarafından incelenmesi ve bu yazışmalar gerekçe gösterilerek iş akdinin feshedilmesi nedeniyle özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyetinin ihlal edildiği iddialarına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

BİRİNCİ BÖLÜM

KARAR

A.A.Y. BAŞVURUSU

(Başvuru Numarası: 2016/13011)

Karar Tarihi: 29/9/2020

BİRİNCİ BÖLÜM

KARAR

GİZLİLİK TALEBİ KABUL

Başkan: Hasan Tahsin GÖKCAN

Üyeler: Serdar ÖZGÜLDÜR, Burhan ÜSTÜN, Muammer TOPAL, Selahaddin MENTEŞ

Raportör: Ali KOZAN

Başvurucu: A.A.Y.

Vekili: Av. Türker YÖNDEM

I. BAŞVURUNUN KONUSU

1. Başvuru, özel bir şirkette çalışan başvurucunun kurumsal e-posta hesabı içeriğinin işveren tarafından incelenmesi ve bu yazışmalar gerekçe gösterilerek iş akdinin feshedilmesi nedeniyle özel

hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyetinin ihlal edildiği iddialarına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 15/7/2016 tarihinde yapılmıştır.

3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.

4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.

5. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık görüş bildirmemiştir.

III. OLAY VE OLGULAR

6. Başvuru formu ve eklerinde ifade edildiği şekliyle olaylar özetle şöyledir:

A. Uyuşmazlığın Arka Planı

7. Başvurucu 4/1/2012 tarihinden bir Avukatlık Ortaklığında avukat olarak çalışmaya başlamıştır. Başvurucuya ortaklık ismiyle "av.tr." uzantılı kurumsal bir e-posta verilmiştir. Kurumsal e-posta bilgi, trafik ve içerikleri işverene ait sunucu üzerinde saklı tutulmaktadır. Başvurucu, beş kişilik bir ekipte ekip yöneticisi olarak görevlidir. İşyerinde 15/12/2014 tarihinde yaşanan tartışma sonrasında ekipte görevli üç kişi yönetime şikâyet dilekçeleri vermiştir. Dilekçelerde, bir buçuk yıldır ekip yöneticisi olan başvurucunun ekibin kıdemli üyesi olan E.Ü. ile iş ilişkisinde nesneliği kaybettiği, her olayda onu destekleyerek diğer ekip üyelerini zor durumda bıraktığı, E.Ü.nün diğer ekip üyelerine karşı kaba davranışlarının ekip içinde ciddi sıkıntılara yol açmasına rağmen başvurucunun olumsuzlukları gidermek için bir adım atmadığı, barışçıl çalışma ortamının kaybolduğu hususlarının dile getirildiği ifade edilmiştir.

8. Başvurucunun iş sözleşmesi 22/5/2003 tarihli ve 4857 sayılı İş Kanunu'nun 18. maddesine dayanılarak 16/1/2015 tarihinde işveren tarafından feshedilmiştir. Fesih bildiriminde; işyerinde Avukat E.Ü. ile başka bir çalışan arasında yaşanan sözlü tartışma sonrası başvurucu hakkında ekip arkadaşları tarafından verilen şikâyet dilekçelerindeki iddiaları araştırmak amacıyla inceleme başlatıldığı belirtilmiştir.

9. Fesih bildiriminde ayrıca yukarıda belirtilen şikâyet dilekçelerindeki suçlamaların sözlü iddialar niteliğinde olması nedeniyle somut olayın ve ekip üyeleri arasındaki ilişkilerin aydınlatılması

amacıyla işlerin sürekliliğinin sağlanması için kullanılan ve güvenlik gerekçeleriyle internet ortamında saklı tutulan -her an kontrol edilebileceği de bilinen- kurumsal e-posta yazışmalarının incelendiği ifade edilmiştir. İnceleme sonucu elde edilen mesajlarda E.Ü.nün başvuru ve iş arkadaşları hakkında ağır ithamlarda bulunduğu, hakaretamiz ifadeler kullandığı, başvuru rahatsız edecek ve psikolojik taciz sayılabilecek yazışmalar yaptığı, ekip yöneticisi olan başvuru da bu durumu kabullendiği, bu üsluba karşı caydırıcı adımlar atmayı reddettiği hususlarının tespit edildiği belirtilmiştir. Anılan inceleme ile başvuruyla yapılan mülakat ve başvurudan alınan yazılı savunma sonucunda, başvuru ekip yönetiminde nesnellik kaybettiği ve bu durumu bilerek düzeltmediği, diğer çalışanlar hakkında hasmane, tutarsız, ön yargılı davranışlar sergilediği hususlarının sabit olduğu bu durumun işyerindeki barışçıl çalışma ortamını bozacak nitelikte olduğu vurgulanarak, iş akdinin feshedildiği ve işçilik haklarının ödeneceği ifade edilmiştir.

10. İşverenin ilk derece mahkemesine sunduğu yazışma içerikleri incelendiğinde; başvuru ile E.Ü. arasında geçen ve genellikle birbirleriyle ve işyeri ile ilgili düşüncelerin açıklandığı yer yer karşılıklı tartışma şeklinde diyalogların mevcut olduğu görülmüştür. Ayrıca başvuru ve E.Ü.nün dışında, birlikte çalıştıkları başka bir avukatla yapılan yazışmalara da yer verilmiştir. Yazışmaların bir kısmı şu şekildedir: E.Ü.den başvuruya; "hayatımdan çık ve geri dönme senden bıktım", "annenle konuşacağım merak etme tüm rezilliklerini anlatacağım", "her şey ortaya çıkacak, kendi hırsların için neler yaptığını en yakınlarında bilsin", "senin yarattığın tipler bunlar ama adam ederim", "sana ıspatı olsun, kendisi bulamadığı için sevgilisi A.yı seferber etmiş...nasıl bir örgütlenme olduğunu gör", "adam kendisi benim belgelerime giremeyecek kadar aciz, kız arkadaşını sokuyor, şımarıklığın hadsizliğin dik boyutu". Başvuru cevaplarında: "Ben senin hayatında değilim, çok oldu çıkalı dönmek gibi bir niyetim de yok, beni böyle taciz ederek İ.E ile konuşturamazsın", "rezil sensin, buyur konuş, bana bir daha böyle mail atma", "benim üzerime bu kadar gelme, kendini kontrol etmeyi öğren", "seni bu grupta tutacağım seninle anlaşamadığım algısı yaratılmayacağı", "yoruldum maillerinden, aşırı derecede asabım bozuluyor, çalışmıyorum. Kimsenin kimseye bu tip bir tavır sergilemeye ve eziyet etmeye hakkı yok..."

B. İşe İade Davası Süreci

11. Başvuru, işveren aleyhine İstanbul 8. İş Mahkemesinde işe iade istemli tespit davası açmıştır. Dava dilekçesinde başvuru özetle; davalılar tarafından birlikte istihdam edildiğini, çalışmaya başladıktan on sekiz ay sonra çalışma performansı ve iş arkadaşlarıyla sosyal ilişkileri gözetilerek ekip yöneticisi olarak görevlendirildiğini belirtmiştir. Fesih sebebi olarak gösterilen ofiste iki ekip

arkadaşı arasında yaşanan sözlü tartışmanın tarafı olmadığını, tartışmaya müdahale ederek sonlandırdığını, yoğun ve stresli çalışma ortamında zaman zaman yaşanan bu tartışmaların fesih nedeni olamayacağını ifade etmiştir. Ayrıca fesih nedeni olarak gösterilen e-posta yazışmalarının ise o dönemdeki işlerin gerginliği ile söylenen, ekip arkadaşı ile yaptığı şahsi ve dışarıya yansımayan görüşmeler olduğunu, geriye dönük inceleme yapılacak olsa benzer e-postaların diğer çalışanlar arasında da geçtiğinin tespit edilebileceğini ifade ederek, iş akdinin feshinin kötü niyetli olduğunu, haklı bir gerekçeye dayanmadığını ileri sürmüştür.

12. İşveren davaya cevabında özetle; başvurucuyla aynı ekipte çalışan Avukat E.Ü. ile başka bir çalışan arasında işyerinde tartışma yaşanması sonrasında ekip arkadaşlarının başvurucu ve E.Ü. hakkında şikâyet dilekçeleri verdiklerini belirtmiştir. İddiaların araştırılması sırasında başvurucu ve diğer çalışanlar ile mülakat yapıldığını, başvurunun savunmasının alındığını; çalışma ekibinde yaşanan sıkıntıların temelinde olayların değil söylemlerin ve ispatı neredeyse imkânsız olan anlık hareketlerin bulunması nedeniyle başvurunun kurum e-posta hesabı üzerinden yaptığı yazışmaların incelendiği belirtilmiştir. Anılan incelemenin başvurucu ile diğer ekip üyeleri arasında geçen yazışmalar ile sınırlı tutulduğunu, inceleme sonucunda E.Ü.nün ekip yöneticisi olan başvurucuya yönelik tehdit ve taciz içerikli mesajları ile diğer çalışma arkadaşlarına yönelik hakaret içerikli mesajlarının tespit edildiği, bu şekilde yönetici olan başvurunun objektifliğini ve yönetim yetkisini kaybettiğinin anlaşıldığı vurgulanarak ilgili mesaj içerikleri dilekçede sunulmuştur. Ayrıca sözlü savunmanın gerçekleştirilmesine rağmen başvurucu ile ilgili iddiaların gerçek olup olmadığı yönünde somut veri olmaması nedeniyle e-postaların incelendiği, kurumsal e-posta olması nedeniyle başvurunun e-postasının işveren tarafından her zaman incelenebileceği ifade edilmiştir.

13. Mahkeme 20/8/2015 tarihinde davanın reddine karar vermiştir. Kararın gerekçesinde; tanık beyanları, dosyaya sunulan belgeler ile e-posta içerikleri değerlendirilerek başvurunun davalılar tarafından birlikte istihdam edildiğinin anlaşıldığı öte yandan iş akdinin feshine dayanak edilen olayların ve nedenlerin fesih bildiriminde açık bir şekilde gösterildiği belirtilmiştir. Bununla birlikte ekip lideri olarak çalışan başvurunun ekipte yaşanan tartışmalarda ekip arkadaşları arasında eşit mesafede durarak sorunların çözümü yönünde girişimde bulunmadığı, uzun süredir devam ettiği anlaşılabilir olaylara zamanında müdahale etmeyerek iş barışının bozulmasına neden olduğu hususlarının sabit olduğu vurgulanmıştır. Ayrıca işvereni hakkında eleştiri boyutunu aşacak nitelikte ifadelerle organik bağ bulunan diğer davalılara mesajlar gönderdiği belirtilerek anılan tutum ve davranışlar nedeniyle iş akdinin devamının işverenden beklenemeyeceği vurgulanarak geçerli nedene dayalı feshin yerinde olduğu sonucuna varılmıştır.

14. Başvurucu vekili tarafından anılan karar temyiz edilmiştir. Temyiz dilekçesinde, kişisel hesaplar üzerinden gerçekleştirilen yazışmalardan oluşan e-postaların fesih gerekçesi olarak gösterilmesiyle özel hayatın gizliliği hakkı ile haberleşme hürriyetinin ihlal edildiği, buna rağmen Mahkeme tarafından söz konusu mesajların delil olarak değerlendirildiği belirtilmiştir. Başvurucunun e-postasının şifreli olduğu ve işveren tarafından şifre kırılmadan inceleme yapılamayacağı, ayrıca işyerinde kurumsal e-posta yazışmalarının okunabileceğine veya incelenebileceğine dair yazılı bir kural olmadığı vurgulanmış ve e-posta içeriklerinin işveren tarafından okunamayacağı düşünülerek iki kişi arasında geçen kişisel yazışmalardan oluştuğu belirtilmiştir.

15. Temyiz nedenlerine karşı cevap dilekçesi sunan davalı işveren vekilince yazışmaların Şirket tarafından çalışanlar adına açılmış ve tüm hakları işverene ait olan e-posta hesapları üzerinden gerçekleştirildiği, bu e-posta adreslerinin herhangi bir şifresinin olmadığı ve bu iletişim adreslerinden yapılan tüm mesajların işverene ait sunucuda biriktirildiği ifade edilmiştir. Ayrıca Yargıtay içtihatlarına yer verilerek işverenin işçiye tahsis ettiği bilgisayar ve kurumsal e-posta adreslerini her zaman denetleyebileceği vurgulanarak feshin haklı nedenlere dayandığı iddiası yinelenmiştir.

16. Yargıtay 9. Hukuk Dairesi 12/5/2016 tarihli ilamıyla ilk derece mahkemesinin kararını, başvurucuyu davalıların birlikte istihdam ettiğine ilişkin kısmı gerekçeden çıkararak onamıştır.

17. Nihai karar 17/6/2016 tarihinde başvurucuya tebliğ edilmiştir.

18. Başvurucu 15/7/2016 tarihinde bireysel başvuruda bulunmuştur.

IV. İLGİLİ HUKUK

19. İlgili hukuk (ulusal mevzuat, uluslararası düzenlemeler ve Avrupa İnsan Hakları Mahkemesi kararları) için bkz. E.Ü. [GK], B. No: 2016/1310, 17/9/2020, §§ 22-51.

20. Ayrıca 22/5/2003 tarihli ve 4857 sayılı İş Kanunu'nun "Feshin geçerli sebeplere dayandırılması" kenar başlıklı 18. maddesi şöyledir:

"Otuz veya daha fazla işçi çalıştıran işyerlerinde en az altı aylık kıdemi olan işçinin belirsiz süreli iş sözleşmesini fesheden işveren, işçinin yeterliliğinden veya davranışlarından ya da işletmenin, işyerinin veya işin gereklerinden kaynaklanan geçerli bir sebebe dayanmak zorundadır. (Ek cümle: 10/9/2014-6552/2 md.) Yer altı işlerinde çalışan işçilerde kıdem şartı aranmaz.

Altı aylık kıdem hesabında bu Kanununun 66 ncı maddesindeki süreler dikkate alınır.

Özellikle aşağıdaki hususlar fesih için geçerli bir sebep oluşturmaz:

- a) Sendika üyeliği veya çalışma saatleri dışında veya işverenin rızası ile çalışma saatleri içinde sendikal faaliyetlere katılmak.
- b) İşyeri sendika temsilciliği yapmak.
- c) Mevzuattan veya sözleşmeden doğan haklarını takip veya yükümlülüklerini yerine getirmek için işveren aleyhine idari veya adli makamlara başvurmak veya bu hususta başlatılmış sürece katılmak.
- d) Irk, renk, cinsiyet, medeni hal, aile yükümlülükleri, hamilelik, doğum, din, siyasi görüş ve benzeri nedenler.
- e) 74 üncü maddede öngörülen ve kadın işçilerin çalıştırılmasının yasak olduğu sürelerde işe gelmemek.
- f) Hastalık veya kaza nedeniyle 25 inci maddenin (I) numaralı bendinin (b) alt bendinde öngörülen bekleme süresinde işe geçici devamsızlık.

İşçinin altı aylık kıdemi, aynı işverenin bir veya değişik işyerlerinde geçen süreler birleştirilerek hesap edilir. İşverenin aynı işkolunda birden fazla işyerinin bulunması halinde, işyerinde çalışan işçi sayısı, bu işyerlerinde çalışan toplam işçi sayısına göre belirlenir.

V. İNCELEME VE GEREKÇE

21. Mahkemenin 29/9/2020 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları

22. Başvurucu; kurumsal e-posta hesapları üzerinden gerçekleştirdiği kişisel yazışmaların işveren tarafından rızası olmaksızın incelendiğini, çalışanların e-postalarının incelenebileceğine, denetleneceğine dair yazılı ya da sözlü işyeri kuralının mevcut olmadığını, işverenin iş sözleşmesinin feshine gerekçe bulmak amacıyla tüm e-posta yazışmaları üzerinde inceleme yaptığını belirtmiştir. İşveren tarafından okunacağını beklemeden yazdığı ve inceleme anına kadar işverenin bilmediği kişisel yazışma niteliğindeki e-postalardaki ifadelerin fesih gerekçesi yapıldığını, işveren tarafından yazışmalarının alenileştirildiğini, açtıkları işe iade istemli tespit davasında da söz konusu yazışmaların delil olarak kabul edildiğini ifade etmiştir. Ayrıca, feshin haklı ya da geçerli bir sebebe dayanmadığını, Mahkemenin itirazlarını ve delillerini karşılayacak şekilde gerekçe sunmadığını belirterek, adil yargılanma ve özel hayata saygı hakkı ile haberleşme hürriyetinin ihlal edildiğini ileri sürmüştür. Başvurucu ayrıca meslek kariyerini gerekçe göstererek, kamuya açık belgelerde kimlik bilgilerinin gizli tutulmasını talep etmiştir.

B. Değerlendirme

23. Anayasa'nın iddianın değerlendirilmesinde dayanak alınacak "Özel hayatın gizliliği" kenar başlıklı 20. maddesinin birinci ve üçüncü fıkrası şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

...

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

24. Anayasa'nın "Haberleşme hürriyeti" kenar başlıklı 22. maddesi şöyledir:

"Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.

İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir."

25. Özel hayata saygı hakkı Anayasa'nın 20. maddesinde koruma altına alınmıştır. Devlet, kişilerin özel ve aile hayatına keyfî olarak müdahale etmemek ve üçüncü kişilerin haksız saldırılarını önlemekle yükümlüdür. Anayasa'nın 20. maddesinin üçüncü fıkrasında ise herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı ayrıca düzenlenmiş ve güvence altına alınmıştır. Söz konusu anayasal güvence, Sözleşme'nin 8. maddesinde koruma altına alınan özel hayata saygı hakkına karşılık gelmektedir. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır (AYM, E.2014/122, K.2015/123, 30/12/2015, §§ 19, 20).

26. Anayasa Mahkemesi kararlarında da belirtildiği üzere kişisel veri -belirli veya kimliği belirlenebilir olmak şartıyla- bir kişiye ilişkin bütün bilgileri ifade etmekte olup bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi sadece kimliğini ortaya koyan bilgileri değil telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, öz geçmişi, resim, görüntü ve ses kayıtları, parmak izleri, sağlık bilgileri, genetik bilgiler, IP adresi, e-posta adresi, alışveriş alışkanlıkları, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır (AYM, E.2014/74, K.2014/201, 25/12/2014; E.2014/180, K.2015/30, 19/3/2015).

27. Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı yönünden inceleme yapılabilmesi için öncelikle anılan hak kapsamında korunması gereken bir kişisel verinin olup olmadığı belirlenmelidir. Anayasa hükmünün lafzı, konuya ilişkin uluslararası belgeler ve karşılaştırmalı hukuk dikkate alındığında belirli veya belirlenebilir bir gerçek veya tüzel kişi hakkındaki her türlü bilgi kişisel veri olarak değerlendirilir. Ancak her davada ya da başvuruda Anayasa'nın 20. maddesinin üçüncü fıkrası anlamında bir kişisel veri bulunup bulunmadığı davanın ve başvurunun kendine özgü koşulları dikkate alınarak otonom olarak tespit edilir. Bir kişisel verinin bulunduğu tespit edildiğinde bu veriye yönelik her türlü sınırlama ve müdahale Anayasa'nın anılan hükmü kapsamındaki güvenceleri harekete geçirir (E.Ü. [GK], § 59).

28. Ayrıca Anayasa'nın 22. maddesinde güvence altına alınan haberleşme hürriyeti, haberleşmenin yanında içeriği ve biçimi ne olursa olsun haberleşmenin içeriğinin gizliliğini de güvence altına almaktadır. Haberleşme bağlamında bireylerin karşılıklı ve toplu olarak sözlü, yazılı ve görsel iletişimlerine konu olan ifadelerinin gizliliğinin sağlanması ve haberleşmeye yönelik haksız müdahalelerde bulunulmaması gerekir (Yasemin Çongar ve diğerleri, B. No: 2013/7054, 6/1/2015, § 49).

29. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Somut olayda işverenin başvuru sahibinin kurumsal e-posta hesabını kullanarak yaptığı mesajlaşmalarını denetlemesi ve içeriğinin geriye dönük olarak incelemesi sonucu elde ettiği bilgileri iş akdinin feshine dayanak yapması söz konusudur. Ayrıca e-posta bilgilerinin internet ortamında saklı tutulduğu, bu verilere erişildiği ve içeriğinin denetlenerek kullanıldığı dikkate alındığında veri işleminin söz konusu olduğu da söylenebilir. Bu durumla birlikte başvuru sahibinin e-posta bilgileri ve yazışmalarının belirli bir gerçek kişi hakkındaki bilgi kapsamında olduğu gözetildiğinde bu bilgilere erişilmesinin, bunların kullanılmasının ve işlenmesinin özel hayata saygı hakkı kapsamında kişisel

verilerin korunmasını isteme hakkı ve haberleşme hürriyeti yönünden incelenmesi gerektiği değerlendirilmiştir.

1. Kabul Edilebilirlik Yönünden

30. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

2. Esas Yönünden

a. Genel İlkeler

31. Anayasa'nın 20. maddesinin üçüncü fıkrasının birinci cümlesinde genel olarak herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu belirtilmiş, ikinci cümlesinde kişisel veriler bağlamında bazı özel güvenceler sayılmış, üçüncü cümlesinde kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği düzenlenmiş, dördüncü cümlesinde ise kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hüküm altına alınmıştır. Buna göre lafzı dikkate alındığında Anayasa'nın 20. maddesinin üçüncü fıkrasının kişisel verilerin korunmasını isteme hakkı kapsamında sadece işleme şeklindeki sınırlama ya da müdahalelere karşı değil kişisel verilere yönelik her türlü müdahale ve sınırlamalara karşı güvence getirdiği anlaşılmaktadır (E.Ü. [GK], § 63).

32. Öte yandan Anayasa ve Sözleşme'nin ortak koruma alanı kapsamında kalan temel haklar, yalnızca kamusal gücün doğrudan uygulanmasıyla değil kimi zaman da özel hukuk kişileri arasındaki uyuşmazlıklara konu olacak şekilde üçüncü kişilerin müdahaleleriyle zedelenebilmektedir. İlkinde söz konusu güvencelerin sağlanması adına kamusal makamlara yüklenen negatif ve pozitif tüm yükümlülüklerin doğrudan yerine getirilmesi konusunda tereddüt bulunmamakta ise de ikinci durumda devletin üçüncü kişilerin müdahalelerine karşı bireylere ne tür bir koruma imkânı sunması gerektiği ve hangi çerçevede yükümlülükler taşıdığı hususunda her olayın kendine özgü koşullarına göre değerlendirmelerde bulunulması gerekmektedir (Ömür Kara ve Onursal Özbek, B. No: 2013/4825, 24/3/2016, § 45).

33. Yine Anayasa'nın 12. ve 5. maddesindeki düzenlemeler ışığında devletin bireyin temel hak ve özgürlüklerine keyfi olarak müdahale etmemenin yanında üçüncü kişilerin saldırılarını önlemekle yükümlü kılındığı, bu bağlamda pozitif yükümlülüklerinin de bulunduğu söylenebilir. Uyuşmazlıkların özel hukuk kişileri arasında gerçekleştiği durumlarda da temel hak ve özgürlüklerin

sağladığı güvencelerin yerine getirilip getirilmediği denetlenirken Anayasa'nın kamusal makamlara yüklediği sorumluluklardan doğrudan özel hukuk kişileri sorumlu tutulamayacağı için taşıdığı koşulların özelliklerine göre bu tür başvuruların devletin pozitif yükümlülükleri bağlamında ele alınması gerekebilir. Dolayısıyla özel hayatın korunması kapsamında kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyeti yönünden de devletin pozitif bir yükümlülük olarak yetki alanında bulunan tüm bireyleri gerek kamusal makamların ve diğer bireylerin gerekse kişinin kendisinin eylemlerinden kaynaklanabilecek risklere karşı koruma yükümlülüğü bulunmaktadır (Ömür Kara ve Onursal Özbek, § 46; Ali Çığır, B. No: 2015/19298, 8/5/2019, §§ 32, 33; Erol Kumcu, B. No: 2015/18988, 9/5/2019, §§ 32, 33; U.B., B. No: 2015/3175, 10/10/2019, §§ 33, 34; E.Ü. [GK], § 65).

34. Pozitif yükümlülükler özel hukuk kişilerinin birbirleri ile olan uyuşmazlıklarının çözümüne ilişkin yasal altyapının oluşturulmasını, söz konusu uyuşmazlıkların adil yargılama gereklerine uygun ve usul yönünden güvenceleri haiz bir yargılama kapsamında incelenmesini ve bu yargılamalarda temel haklara ilişkin anayasal güvencelerin gözetilip gözetilmediğinin denetlenmesini gerektirir. Bu doğrultuda derece mahkemelerince söz konusu güvenceler gözardı edilmemeli, işveren ve çalışanlar arasındaki çatışan çıkarlar adil biçimde dengelenmeli, başvuruların temel haklarına yönelik müdahalenin meşru amaca dayalı ve ölçülü olup olmadığı değerlendirilmeli, ulaşılan sonuç hakkında hüküm kurulurken ilgili ve yeterli gerekçeler sunulmalıdır (Ömür Kara ve Onursal Özbek, §§ 47-50; E.Ü. [GK], § 66).

35. Anayasa Mahkemesi iletişim araçlarının işveren tarafından denetlenmesi kapsamındaki uyuşmazlıklarda derece mahkemeleri tarafından devletin pozitif yükümlülükleri bağlamında çıkarların dengelenmesi ve müdahalenin ölçülülüğünün irdelenmesi kapsamında gözetilmesi gereken hususları genel olarak belirlemiş; buna göre somut olayın koşullarına göre iş sözleşmelerinde kısıtlayıcı ve zorlayıcı düzenlemelerin ne şekilde belirlendiği, tarafların bu düzenlemeler hakkında bilgilendirilip bilgilendirilmediği, çalışanların temel haklarına yönelik müdahalede bulunulmasına neden olan meşru amacın müdahale ile ölçülü olup olmadığı, sözleşmenin feshinin çalışanların eylem ya da eylemsizlikleri karşısında makul ve orantılı bir işlem olup olmadığı hususlarının uyuşmazlığın çözümünde gözetilmesi gerektiğini tespit etmiştir (Ömür Kara ve Onursal Özbek, § 50).

36. Yukarıda belirtilen hususlar gözetilerek işverenin işçinin iletişimini denetlemesi yetkisini kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyeti bağlamında devletin pozitif yükümlülükleri kapsamında irdelenmek gerekmektedir. Öncelikle somut olayda olduğu gibi teknolojik gelişmelerin imkânlarından yararlanmak isteyen işverenlerin bilgisayar, internet, e-posta gibi iletişim araç ve gereçlerini çalışanın kullanıma sunması nedeniyle oluşan uyuşmazlıklarda

işverenin menfaatleri ile işçinin temel hak ve özgürlükleri arasında bir dengeleme yapma gerekliliği doğmaktadır. Bu bağlamda işveren ile çalışan arasındaki ilişkinin iki taraf açısından da belirli hak ve yükümlülükler öngören ve esasen güven ilişkisi üzerine kurulu iş sözleşmesiyle şekillendiği unutulmamalıdır. Somut uyuşmazlığın ilgili olduğu iş hukukunun dinamik bir niteliğinin olduğu, ayrıca iş ilişkilerinin genel kurallardan farklı, kendine özgü bazı hukuki kurallar içerdiği de dikkate alınmalıdır (E.Ü. [GK], § 68)

37. Bu bağlamda işlerin etkin bir şekilde yürütülmesi ile bilgi akışının kontrolünü sağlamak, işçinin eylemlerine bağlı cezai ve hukuki sorumluluğa karşı korunmak, verimliliği ölçmek veya güvenlik endişeleri gibi haklı ve meşru görülebilecek nedenlerle işverenin yönetim yetkisi kapsamında kural olarak işçinin kullanımına sunduğu iletişim araçlarını denetleyebileceği ve kullanıma ilişkin sınırlamalar öngörebileceği söylenebilir. Ancak işverenin yönetim yetkisinin işyerinde işin yürütülmesi, işyerinin düzeninin ve güvenliğinin sağlanmasıyla sınırlı olduğu unutulmamalıdır. Bu bağlamda işverenin yetki ve haklarının sınırsız olmadığı, çalışana tanınan temel hak ve özgürlüklerin somut olayda haberleşme hürriyeti ve kişisel verilerin korunmasını isteme hakkının işyeri sınırları dâhilinde de korunduğu, aynı zamanda kısıtlayıcı ve uyulması zorunlu işyeri kurallarının çalışanların temel haklarının özünü zedeleyecek nitelikte olmaması gerektiği vurgulanmalıdır. Bu çerçevede işyerinde kullanıma sunulan iletişim araçlarının işverene ait olduğu gözetilerek sırf bu nedenle bile işverenin iletişim araçları üzerinde sınırsız ve mutlak bir gözetleme ve denetleme yetkisinin olduğunu kabul etmek, işçinin demokratik bir toplumda temel hak ve özgürlüklerine işyerinde de saygı gösterilmesi gerektiği yönündeki haklı beklentisiyle uyuşmayacaktır (E.Ü. [GK], § 69).

38. Tüm bu açıklamalar çerçevesinde devletin pozitif yükümlülükleri kapsamında Anayasa Mahkemesinin özellikle derece mahkemelerinin -somut olayın koşullarına uygun düştüğü ölçüde- aşağıda belirtilen güvencelerin somut olayda hakka müdahale eden üçüncü kişi tarafından sağlanıp sağlanmadığını gereği gibi denetleyip denetlemediğini incelemesi gerekir:

i. İşverenin çalışanın kullanımına sunduğu iletişim araçlarının ve iletişim içeriklerinin incelenmesinin haklı olduğunu gösteren meşru gerekçeleri olup olmadığı denetlenmelidir. Bu durumda işverenin gerekçelerinin ifa edilen işin ve işyerinin özellikleri de gözetilerek meşru olup olmadığı irdelenmelidir. Bu denetlemede iletişim akışı ile iletişim içeriklerinin incelenmesi arasında ayırım yapılarak içeriklerin incelenmesi yönünden daha ciddi gerekçeler aranmalıdır.

ii. Demokratik bir toplumda iletişimin denetlenmesi ve kişisel verilerin işlenmesi süreci şeffaf bir şekilde gerçekleştirilmeli ve bunun bir gereği olarak da süreçle ilgili olarak çalışanlar işveren

tarafından önceden bilgilendirilmelidir. Uluslararası hukuk ve karşılaştırmalı hukuk dikkate alındığında bu bilgilendirmenin -somut olayın özelliklerine uygun düştüğü ölçüde- en azından iletişimin denetlenmesi ile kişisel verilerin işlenmesinin hukuki dayanağı ve amaçları, denetlemenin ve veri işlemenin kapsamı, verilerin saklanacağı süre, veri sahibinin hakları, denetlemenin ve işlemenin sonuçları ile verilerin muhtemel yararlanıcıları hususlarını kapsamaması gerekir. Ayrıca bildirimde iletişim araçlarının kullanımına ilişkin olarak işveren tarafından öngörülen sınırlamalara da yer verilmelidir. Bilgilendirmenin mutlaka belli şekilde yapılması şart olmayıp şeffaflığı sağlamak bakımından bireylere, kişisel verilerin işlenmesine ve iletişimin denetlenmesine ilişkin süreçten yukarıda belirtilen kapsamda haberdar olma imkânı sağlayan uygun bir yöntem tercih edilebilir.

iii. Çalışanın kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine işveren tarafından yapılan müdahale, ulaşılmak istenen amaç ile ilgili ve bu amacı gerçekleştirmeye elverişli olmalıdır. Ayrıca inceleme faaliyetiyle elde edilen verilerin işveren tarafından hedeflenen amaç doğrultusunda kullanılması gerekir.

iv. İşveren tarafından çalışanın kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine işveren tarafından yapılan müdahalenin gerekli kabul edilebilmesi için aynı amaca daha hafif bir müdahale ile ulaşılmak mümkün olmamalı, müdahale ulaşılmak istenen amaç bakımından zorunlu olmalıdır. Çalışanın iletişiminin içeriğine girilmesi yerine onun kişisel verilerine daha az müdahale eden yöntem ve tedbirlerin uygulanmasının mümkün olup olmadığı denetlenmelidir. Bu kapsamda işverenin ulaşmak istediği amaca çalışanın iletişimi incelenmeden de erişilme imkânı olup olmadığı her bir vakianın somut özellikleri ışığında değerlendirilmelidir.

v. İşveren tarafından başvurucunun kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine yönelik müdahalenin orantılı kabul edilebilmesi için ise iletişimin denetlenmesi ile işlenecek veya herhangi bir şekilde yararlanılacak veriler ulaşılmak istenen amaçla sınırlı olmalı, bu amacı aşacak şekilde sınırlama ya da müdahaleye izin verilmemelidir.

vi. Ayrıca iletişimin incelenmesinin muhatabı olan çalışan üzerindeki etkisi ve çalışan bakımından sonuçları gözönünde tutularak tarafların çatışan menfaat ve haklarının adil bir biçimde dengelenip dengelenmediğine bakılması gerekmektedir. Taraflardan birine şahsi olarak aşırı bir külfet yüklendiğinin tespiti hâlinde devletin pozitif yükümlülüklerini yerine getirmediği sonucuna varılabilir (E.Ü. [GK], § 70).

b. İlkelerin Uygulanması

39. Başvurucu; e-posta hesabının incelenmesinin özel hayat alanına ve haberleşme hürriyetine haksız bir müdahale oluşturmasına rağmen açtığı işe iade davasında bu yönde bir tespit yapılmadığını, yazışmalarının işveren tarafından alenileştirildiğini, mahkemelerce verilen kararlar nedeniyle söz konusu müdahalelerin meşru hâle getirildiğini iddia etmiştir. Bu kapsamdaki iddiaların, yukarıda belirtilen esaslar gözetilerek değerlendirilmesi gerekmektedir.

40. Öncelikle işverenin işçinin kullanımına sunulan iletişim araçlarını denetlemesi ve çalışanın kişisel verilerinin işlemesine ilişkin olarak 4857 sayılı Kanun'da özel bir düzenleme olmadığı görülmüştür. Ancak Anayasa'nın 20. ve 22. maddelerinde yer bulan özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyetine ilişkin güvenceler ile 6698 sayılı Kanun ve hukuk sistemimizde mevcut olan genel düzenlemelerin iş hukuku uyumsuzluklarında uygulanması yönünde bir engel olmadığı anlaşılmıştır. Bu durumda yasal altyapı oluşturmak bağlamında pozitif yükümlülüklerin yerine getirilmiş olduğu söylenebilir (E.Ü. [GK], § 69).

41. Başvuru konusu olayda başvurucu, çok sayıda çalışanı istihdam eden bir avukatlık ortaklığı bünyesinde avukat ve ekip yöneticisi olarak görev yapmaktadır. İşveren işyerinde yaşanan sorunlar ile ilgili yürütülen disiplin soruşturması kapsamında somut delil elde etmek amacıyla işlerin yürütülmesini kolaylaştırmak üzere oluşturulan ve çalışanın kullanımına sunulan kurumsal e-posta hesaplarının incelendiğini belirtmiştir. Başvurucu adına tanımlanmış kurumsal e-posta hesabının mevcut olduğu ve başvurucunun kullanımına sunulan bu e-posta hesabının işveren tarafından incelendiği hususlarında başvuran ile işveren arasında bir ihtilaf olmadığı görülmüştür. Çok sayıda çalışanı olduğu ve kurumsal olarak avukatlık hizmeti verdiği anlaşılan işverenin çalışanlarına kurumsal e-posta hesabı oluşturmak suretiyle kişisel verileri işlemesinin ve iletişim akışını denetim altında tutmasının işlerin etkin bir şekilde yürütülmesini sağlama amacına yönelik olduğu anlaşılmaktadır. Bu durumda kurumsal e-posta hesabının iletişim akışına ve içeriğine erişilecek şekilde kullanıma sunulmasının somut olayda işyerinin yönetimi bakımından meşru bir menfaat teşkil ettiği, ayrıca hedeflenen amacı sağlamaya elverişli bir yöntem olduğu söylenebilir (aynı yönde değerlendirmeler için bkz. E.Ü. [GK], § 73).

42. Öte yandan e-posta hesabı üzerinden yapılan iletişimin denetlenebileceğine ve iletişim araçlarının kullanım koşullarına ilişkin olarak önceden tam ve açık bir bilgilendirme yapılmadığı hâllerde temel hak ve özgürlüklerinin işyerinde de korunacağı yönündeki haklı beklentiyle çalışan kişinin kurumsal e-posta üzerinden kişisel yazışmalar yapabileceğinin işveren tarafından da öngörülebilecek bir durum olduğu vurgulanmalıdır. Buradan hareketle çalışana açık bir bilgilendirmenin yapılmadığı hâllerde hak ve özgürlüklerine bir müdahalede bulunulmayacağı hususunda çalışanların makul bir

beklenti içinde olacaklarının kabul edilmesi, temel hak ve özgürlüklerin sağladığı güvencelerden yararlandırılması gerektiği söylenebilir (E.Ü. [GK], § 75).

43. Somut olayda E.Ü. ile başvurucu arasında geçen ve başvurucu ya da E.Ü. tarafından alenileştirilmediği anlaşılan kişisel yazışmaların iş sözleşmesinin feshine dayanak oluşturduğu, İstanbul 8. İş Mahkemesinde yürütülen işe iade davasında da davanın reddine ilişkin kararın gerekçeleri arasında sayıldığı görülmüştür. Ancak başvurucunun iş sözleşmesinde işverenin kurumsal e-postayı inceleme yetkisi ile kapsamını gösteren bir düzenleme olmadığı sabittir. Bu durumla birlikte yargılama sürecinde işverenin kurumsal e-postayı inceleme yetkisi ile kapsamını gösteren bir bildirim başvurucuya yapıldığına ilişkin bilgi ve belge sunmadığı hususu da değerlendirildiğinde; işveren tarafından kurumsal e-posta hesabı üzerinden yapılan iletişimin izlenebileceği ve denetlenebileceği yönünde açık bir bilgilendirme yapılmadığı değerlendirilmektedir. Öte yandan e-posta iletişim içerikleri gerekçe gösterilerek başvurucunun iş akdi feshedilmiştir. Ancak işveren davalı taraf olarak yargılama sürecinde kişisel verilerin işlenmesinin hukuki dayanağı ve işlemenin amaçları, işlenecek verilerin kapsamı, verilerin saklanacağı süre, veri sahibinin hakları, işlemenin sonuçları ve verilerin muhtemel yararlanıcılarını gösterir bir bilgilendirme yapıldığını ortaya koyamamıştır. Bu bağlamda yargılama sürecinde feshin temel sebebinin oluşturduğu e-posta iletişimine yönelik olarak böyle bir bilgilendirmenin yapıp yapılmadığı derece mahkemelerince tartışılmamış, başvurucunun kendisi alenileştirmediği hâlde onun rızası alınmadan ve önceden bir bilgilendirme yapılmadan e-posta içeriklerine erişildiği yönündeki esaslı iddialarının karşılanmadığı anlaşılmıştır.

44. Ayrıca başvurucunun çalışma ekibindeki diğer üyelerin disiplin soruşturmasına dayanak oluşturan şikâyet dilekçelerinde yakındıkları hususlar gözetildiğinde (bkz. § 7) başvurucunun e-posta iletişiminin içeriğine erişilmesini zorunlu kılan bir durumun mevcut olduğunun işveren tarafından açıklanmadığı, fesih bildiriminde ise "iddiaların araştırılması ve ekip üyeleri arasındaki ilişkilerin anlaşılabilmesi" amaçlarının belirtilmesiyle yetinildiği görülmüştür. Ancak aynı amaca ulaşılabilmesi bakımından tarafların şikâyet ve savunmalarının analizi, tanıkların dinlenilmesi, işyeri kayıtları ile yürütülen projelerin süreç ve sonuçlarının incelenmesi gibi araçlar da mevcut olduğu hâlde niçin e-posta içeriklerinin incelenmesinin zorunlu ve gerekli görüldüğü işveren tarafından açık bir şekilde ortaya konulmadığı gibi derece mahkemeleri tarafından da somut olay bu yönüyle tartışılmamıştır.

45. Öte yandan somut olayda işverenin yaptığı müdahalenin kapsamının tartışılması gerekir. Bu bağlamda yargılama kapsamında işveren tarafından sunulan başvurucunun yazışmaları ve yargılama süreci bir bütün hâlinde değerlendirildiğinde işverenin yazışma içeriklerine E.Ü.nün ve

başvurucunun rızası hilafına erişim sağladığı, E.Ü. ile başvurucu arasında geçen yazışmalar dışında üçüncü kişilerle olan yazışmaların da incelendiği, ayrıca incelemeye dayanak gösterilen iddialarla sınırlı bir denetim yapılmayarak konu ile ilgili olup olmadığı belirsiz içeriklere de erişildiği ve bu içeriklerin de iş akdinin feshine dayanak yapıldığı görülmüştür. Dolayısıyla başvurucunun kişisel verisi kapsamında olan e-postaları ile ilgili olarak trafik bilgisi ile yetinilmediği gibi içeriklerine de kapsamı belirsiz olacak şekilde erişildiği ve bunların kullanıldığı anlaşılmıştır (Aynı yönde değerlendirmeler için bkz. E.Ü. [GK], §§ 76-79).

46. Açıklanan gerekçelerle özel hukuk iş ilişkilerinden doğan uyuşmazlığı karara bağlayan derece mahkemeleri tarafından yukarıda belirtilen anayasal güvenceleri gözeten özenli bir yargılama yapılarak pozitif yükümlülüklerin yerine getirilmediği anlaşıldığından başvurucunun Anayasa'nın 20. maddesinde güvence altına alınan kişisel verilerin korunmasını isteme hakkı ile Anayasa'nın 22. maddesinde güvence altına alınan haberleşme hürriyetinin ihlal edildiğine karar verilmesi gerekir.

3. 6216 Sayılı Kanun'un 50. Maddesi Yönünden

47. 30/11/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 50. maddesinin ilgili kısmı şöyledir:

“(1) Esas inceleme sonunda, başvurucunun hakkının ihlal edildiğine ya da edilmediğine karar verilir. İhlal kararı verilmesi hâlinde ihlalin ve sonuçlarının ortadan kaldırılması için yapılması gerekenlere hükmedilir...

(2) Tespit edilen ihlal bir mahkeme kararından kaynaklanmışsa, ihlali ve sonuçlarını ortadan kaldırmak için yeniden yargılama yapmak üzere dosya ilgili mahkemeye gönderilir. Yeniden yargılama yapılmasında hukuki yarar bulunmayan hâllerde başvurucu lehine tazminata hükmedilebilir veya genel mahkemelerde dava açılması yolu gösterilebilir. Yeniden yargılama yapmakla yükümlü mahkeme, Anayasa Mahkemesinin ihlal kararında açıkladığı ihlali ve sonuçlarını ortadan kaldıracak şekilde mümkünse dosya üzerinden karar verir.”

48. Başvurucu, ihlalin tespit edilmesini istemiş; 10.000 TL manevi tazminat ve zararların giderilmesi talebinde bulunmuştur.

49. Anayasa Mahkemesinin Mehmet Doğan kararında ihlal sonucuna varıldığında ihlalin nasıl ortadan kaldırılacağı hususunda genel ilkeler belirlenmiştir (B. No: 2014/8875, 7/6/2018, [GK]). Mahkeme diğer bir kararında ise bu ilkelerle birlikte ihlal kararının yerine getirilmemesinin sonuçlarına da değinmiş ve bu durumun ihlalin devamı anlamına geleceği gibi ilgili hakkın ikinci kez

ihlal edilmesiyle sonuçlanacağına da işaret etmiştir (Aligül Alkaya ve diğerleri (2), B. No: 2016/12506, 7/11/2019).

50. Bireysel başvuru kapsamında bir temel hakkın ihlal edildiğine karar verildiği takdirde ihlalin ve sonuçlarının ortadan kaldırıldığından söz edilebilmesi için temel kural mümkün olduğunca eski hâle getirmenin yani ihlalden önceki duruma dönülmesinin sağlanmasıdır. Bunun için ise öncelikle ihlalin kaynağı belirlenerek devam eden ihlalin durdurulması, ihlale neden olan karar veya işlemin ve bunların yol açtığı sonuçların ortadan kaldırılması, varsa ihlalin sebep olduğu maddi ve manevi zararların giderilmesi, ayrıca bu bağlamda uygun görülen diğer tedbirlerin alınması gerekmektedir (Mehmet Doğan, §§ 55, 57).

51. İhlalin mahkeme kararından kaynaklandığı veya mahkemenin ihlali gideremediği durumlarda Anayasa Mahkemesi, 6216 sayılı Kanun'un 50. maddesinin (2) numaralı fıkrası ile İçtüzük'ün 79. maddesinin (1) numaralı fıkrasının (a) bendi uyarınca, ihlalin ve sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmak üzere kararın bir örneğinin ilgili mahkemeye gönderilmesine hükmeder. Anılan yasal düzenleme, usul hukukundaki benzer hukuki kurumlardan farklı olarak, ihlali ortadan kaldırmak amacıyla yeniden yargılama sonucunu doğuran ve bireysel başvuruya özgülünen bir giderim yolunu öngörmektedir. Bu nedenle Anayasa Mahkemesi tarafından ihlal kararına bağlı olarak yeniden yargılama kararı verildiğinde, usul hukukundaki yargılamanın yenilenmesi kurumundan farklı olarak ilgili mahkemenin yeniden yargılama sebebinin varlığını kabul hususunda herhangi bir takdir yetkisi bulunmamaktadır. Dolayısıyla böyle bir karar kendisine ulaşan mahkemenin yasal yükümlülüğü, ilgilinin talebini beklemeksizin Anayasa Mahkemesinin ihlal kararı nedeniyle yeniden yargılama kararı vererek devam eden ihlalin sonuçlarını gidermek üzere gereken işlemleri yerine getirmektir (Mehmet Doğan, §§ 58-59; Aligül Alkaya ve diğerleri (2), §§ 57-59, 66-67).

52. İncelenen başvuruda kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyetiyle ilgili anayasal güvenceleri gözetilen bir yargılama yapılmaması nedeniyle anılan hak ve özgürlüğün ihlal edildiği sonucuna varılmıştır. Dolayısıyla ihlalin mahkeme kararından kaynaklandığı anlaşılmaktadır.

53. Bu durumda kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmasında hukuki yarar bulunmaktadır. Yapılacak yeniden yargılama ise bireysel başvuruya özgü düzenleme içeren 6216 sayılı Kanun'un 50. maddesinin (2) numaralı fıkrasına göre ihlalin ve sonuçlarının ortadan kaldırılmasına yöneliktir. Bu kapsamda yapılması gereken iş, yeniden yargılama kararı verilerek Anayasa Mahkemesini ihlal

sonucuna ulařtıran nedenleri gideren, ihlal kararında belirtilen ilkelere uygun yeni bir karar verilmesinden ibarettir. Bu sebeple kararın bir örneğinin yeniden yargılama yapılmak üzere ilgili mahkemeye gönderilmesine karar verilmesi gerekmektedir.

54. Öte yandan somut olayda ihlalin tespit edilmesinin başvuruçunun uğradığı zararların giderilmesi bakımından yetersiz kalacağı açıktır. Dolayısıyla eski hâle getirme kuralı çerçevesinde ihlalin bütün sonuçlarıyla ortadan kaldırılabilmesi için kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ihlali nedeniyle yalnızca ihlal tespitiyle giderilemeyecek olan manevi zararları karşılığında başvuruçuya net 8.000 TL manevi tazminat ödenmesine, tazminata ilişkin diğer taleplerin reddine karar verilmesi gerekir.

55. Dosyadaki belgelerden tespit edilen 239,50 TL harç ve 3.000 TL vekâlet ücretinden oluşan toplam 3.239,50 TL yargılama giderinin başvuruçuya ödenmesine karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Başvuruçunun kamuya açık belgelerde kimlik bilgilerinin gizli tutulmasına ilişkin talebinin **KABULÜNE,**

B. Kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ihlal edildiğine ilişkin iddianın **KABUL EDİLEBİLİR OLDUĞUNA,**

C. Anayasa'nın 20. maddesinde güvence altına alınan kişisel verilerin korunmasını isteme hakkı ve Anayasa'nın 22. maddesinde güvence altına alınan haberleşme hürriyetinin **İHLAL EDİLDİĞİNE,**

D. Kararın bir örneğinin kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmak üzere İstanbul 8. İş Mahkemesine (E.2015/104, K.2015/565) **GÖNDERİLMESİNE,**

E. Başvuruçuya net 8.000 TL manevi tazminat **ÖDENMESİNE,** tazminata ilişkin diğer taleplerin **REDDİNE,**

F. 239,50 TL harç ve 3.000 TL vekâlet ücretinden oluşan toplam 3.239,50 TL yargılama giderinin başvuruçuya **ÖDENMESİNE,**

G. Ödemelerin, kararın tebliğini takiben başvuruçunun Hazine ve Maliye Bakanlığına başvuru tarihinden itibaren dört ay içinde yapılmasına, ödemede gecikme olması hâlinde bu sürenin sona erdiği tarihten ödeme tarihine kadar geçen süre için yasal **FAİZ UYGULANMASINA,**

H. Kararın bir örneğinin bilgi için Yargıtay 9. Hukuk Dairesine **GÖNDERİLMESİNE,**

İ. Kararın bir örneğinin Adalet Bakanlığına GÖNDERİLMESİNE 29/9/2020 tarihinde OYBİRLİĞİYLE karar verildi.

Anayasa Mahkemesi - E.Ü. Kararı (2016/13010)

E.Ü. [GK], B. No: 2016/13010, 17/9/2020

Başvuru, özel bir şirkette çalışan başvurucunun kurumsal e-posta hesabı içeriğinin işveren tarafından incelenmesi ve bu yazışmalar gerekçe gösterilerek iş akdinin feshedilmesi nedeniyle özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyetinin ihlal edildiği iddialarına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

GENEL KURUL

KARAR

E.Ü. BAŞVURUSU

(Başvuru Numarası: 2016/13010)

Karar Tarihi: 17/9/2020

R.G. Tarih ve Sayı: 14/10/2020-31274

GENEL KURUL

KARAR

GİZLİLİK TALEBİ KABUL

Başkan: Zühtü ARSLAN

Başkanvekili: Hasan Tahsin GÖKCAN

Başkanvekili: Kadir ÖZKAYA

Üyeler: Serdar ÖZGÜLDÜR, Burhan ÜSTÜN, Engin YILDIRIM, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĞLU, Selahaddin MENTEŞ, Basri BAĞCI

Raportör: Ali KOZAN

Başvurucu: E.Ü.

Vekili: Av. Türker YÖNDEM

I. BAŞVURUNUN KONUSU

1. Başvuru, özel bir şirkette çalışan başvurucunun kurumsal e-posta hesabı içeriğinin işveren tarafından incelenmesi ve bu yazışmalar gerekçe gösterilerek iş akdinin feshedilmesi nedeniyle özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyetinin ihlal edildiği iddialarına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 15/7/2016 tarihinde yapılmıştır.

3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.

4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.

5. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık görüş bildirmemiştir.

6. İkinci Bölüm tarafından 23/10/2019 tarihinde yapılan toplantıda, niteliği itibarıyla başvurunun Genel Kurul tarafından karara bağlanması gerekli görüldüğünden Anayasa Mahkemesi İçtüzüğü'nün (İçtüzük) 28. maddesinin (3) numaralı fıkrası uyarınca Genel Kurula sevkine karar verilmiştir.

III. OLAY VE OLGULAR

7. Başvuru formu ve eklerinde ifade edildiği şekliyle olaylar özetle şöyledir:

A. Uyuşmazlığın Arka Planı

8. Başvurucu 14/11/2011 tarihinde E. Avukatlık Ortaklığında avukat olarak çalışmaya başlamıştır. Başvurucuya ortaklık ismiyle "av.tr." uzantılı kurumsal bir e-posta verilmiştir. Kurumsal e-posta bilgi, trafik ve içerikleri işverene ait sunucu üzerinde saklı tutulmaktadır.

9. Başvurucu, avukat A.A.Y.nin yöneticisi olduğu beş kişilik bir ekipte görevlidir. İşyerinde 15/12/2014 tarihinde yaşanan tartışma sonrasında ekipte görevli üç kişi yönetime şikâyet dilekçeleri vermiştir. Dilekçelerde, bir buçuk yıldır ekip yöneticisi olan A.A.Y.nin başvurucu ile ilişkisinde nesnelliği kaybettiği ve her olayda başvurucuyu destekleyip diğer ekip üyelerini zor durumda

bıraktığı belirtilmiştir. Bunun yanında başvurucunun ekip üyelerine kaba davrandığı ve ekipteki projelerin sağlıklı yürütülebilmesi için gerekli ortamın kaybolduğu ifade edilmiştir.

10. Başvurucu 26/12/2014 tarihinde verdiği dilekçe ile iddialara yanıt vermiş ve 9/1/2015 tarihinde işyerinde yönetim ile başvurucu arasında üç buçuk saat süren bir mülakat yapılmıştır.

11. Avukatlık Ortaklığınca 10/1/2015 tarihinde başvurucunun kurumsal e-posta yazışmaları incelenmeye alınmış ve inceleme 12/1/2015 tarihinde sona ermiştir. Yapılan inceleme sonucunda Ortaklık 14/1/2015 tarihinden itibaren geçerli olmak üzere başvurucunun iş akdini feshetmiştir. Noter aracılığıyla gönderilen 16/1/2015 tarihli fesih bildiriminde, iddiaların araştırılması amacıyla işlerin sürekliliğinin sağlanması için kullanılan, her an kontrol edilebileceği de bilinen ve güvenlik nedeniyle kurumsal internet ortamında saklı tutulan e-posta yazışmalarının incelendiği belirtilmiştir. Bu fesih bildiriminin ilgili kısmı şöyledir:

"...Yapılan inceleme sonucunda;

- üstünüz olan A.A.Y.yi tehditkar e-postalarla objektiflikten uzak, kendi lehinize tavır alması için zorladığınız,

- çalışma arkadaşlarınıza karşı hakeratamız, tehditkar ve yakışsız bir üslupla hitap ettiğiniz,

- devamlı ve gereksiz tartışmalara girerek ciddi geçimsizlik gösterdiğiniz,

- özellikle A.A.Y. ile olan iş ilişkinizde psikolojik taciz olarak nitelendirilebilecek bir tavır içine girdiğiniz anlaşılmıştır. Bu üslubunuz bir hukuk bürosunda asla kabul görmeyecek bir üslup olup bir avukata yakışan ve avukatlık meslek etiğiyle bağdaşan bir üslup da değildir. Bu e-posta içerikleri ayrıca ekip yöneticiniz A.A.Y. ile olan ilişkinizin de mülakatınızda verdiğiniz savunmanızın tam aksine profesyonellikten uzak bir ilişki olduğunu da kanıtlamaktadır.

Bütün bu davranışların karşılıklı güven temeline dayalı bir meslek olan avukatlık mesleğinde güven ilişkisinin derinden çökmesine yol açması nedeniyle iş ilişkiniz 14/1/2015 tarihinden itibaren geçerli olmak üzere İş Kanunu'nun 25. maddesinin II. fıkrası uyarınca haklı nedenle sona erdirilmiştir..."

12. İşverenin ilk derece mahkemesine sunduğu yazışma içerikleri incelendiğinde başvurucu ile A.A.Y. arasında geçen, genellikle birbirleriyle ve işyeri ile ilgili düşüncelerini yer yer tartışma şeklinde diyalogların yer aldığı görülmüştür. Ayrıca başvurucu ve A.A.Y.nin dışında birlikte çalıştıkları başka bir avukatla yapılan yazışmalara da yer verilmiştir. Yazışmaların bir kısmı şu şekildedir: Başvurucudan A.A.Y.ye "Hayatımdan çık ve geri dönme senden bıktım.", "Annenle konuşacağım merak etme tüm rezilliklerini anlatacağım.", "Her şey ortaya çıkacak, kendi hırsların için neler

yaptığını en yakınların da bilsin.", "Senin yarattığın tipler bunlar ama adam ederim.", "Sana ispatı olsun, kendisi bulamadığı için sevgilisi A.yı seferber etmiş...nasıl bir örgütlenme olduğunu gör.", "Adam kendisi benim belgelerime giremeyecek kadar aciz, kız arkadaşını sokuyor, şımarıklığın hadsizliğin dik boyutu."; A.A.Y. cevaplarında "Ben senin hayatında değilim, çok oldu çıkalı dönmek gibi bir niyetim de yok, beni böyle taciz ederek İ.E ile konuşturamazsın.", "Rezil sensin, buyur konuş, bana bir daha böyle mail atma.", "Benim üzerime bu kadar gelme, kendini kontrol etmeyi öğren.", "Seni bu grupta tutacağım seninle anlaşılamadığım algısı yarattırmayacağım.", "Yorulduğum maillerinden, aşırı derecede asabım bozuluyor, çalışmıyorum. Kimsenin kimseye bu tip bir tavır sergilemeye ve eziyet etmeye hakkı yok..."

B. İşe İade Davası Süreci

13. Başvurucu, işveren aleyhine İstanbul 8. İş Mahkemesinde işe iade istemli tespit davası açmıştır. Dava dilekçesinde başvurucu özetle davalılar E. Avukatlık Ortaklığı ve B.M. Danışmanlık Hizmetleri ile B.M. Ofis Yönetimi ve Hizmetleri Limitet Şirketi tarafından birlikte istihdam edildiğini, anılan şirketler bünyesinde yazılı olmayan belirsiz süreli iş sözleşmesi ile çalıştığını belirtmiştir. Fesih sebebi olarak gösterilen tartışmayı kendisinin başlatmadığını, tartışma sırasında karşılıklı hakaret olmadığını, ekip yöneticisinin araya girmesi ile tartışmanın sona erdiğini iddia etmiştir. Ayrıca fesih nedeni olarak gösterilen e-posta yazışmalarının o dönemdeki işlerin gerginliği ile söylenen, ekip yöneticisi ile yaptığı şahsi ve dışarıya yansımaya görüşmeler olduğunu, savunma davet çağrısında ve sözlü savunma mülakatında bu e-postalar ile ilgili soru sorulmadığını, geriye dönük inceleme yapılacak olsa benzer e-postaların diğer çalışanlar arasında da geçtiğinin tespit edilebileceğini ifade ederek iş akdinin feshinin kötü niyetli olduğunu, haklı bir gerekçeye dayanmadığını ileri sürmüştür.

14. İşveren cevabında, başvurucuyla aynı ekipte çalışan başka bir avukat arasında işyerinde tartışma yaşanması sonrasında ekip arkadaşlarının başvurucu ve ekip yöneticisi A.A.Y. hakkında şikâyet dilekçeleri verdiği, çalışma ekibinde yaşanan sıkıntıların temelinde olayların değil söylemlerin ve ispatı neredeyse imkânsız olan anlık hareketlerin olması nedeniyle ekip yöneticisi avukat A.A.Y.nin kullanımındaki kurum e-posta hesabının incelendiği belirtilmiştir. Cevapta; anılan incelemenin A.A.Y. ile diğer ekip üyeleri arasında geçen yazışmalar ile sınırlı tutulduğu, başvurunun ekip yöneticisine yönelik tehdit ve psikolojik taciz, diğer ekip arkadaşlarına yönelik ise hakaret içerikli mesajlarının tespit edildiği vurgulanarak ilgili mesaj içerikleri dilekçe ile sunulmuştur. Ayrıca başvurunun e-postasının incelenmesi neticesinde bu mesajların silindiğinin tespit edildiği, başvurucu ile sözlü savunma mülakatı gerçekleştirilmesine rağmen başvurucu ile ilgili iddiaların gerçek olup olmadığı yönünde somut veri olmaması nedeniyle e-postaların incelendiği, kurumsal e-

posta olması nedeniyle başvuruçunun e-postasının işveren tarafından her zaman incelenebileceği ifade edilmiştir.

15. İlk derece mahkemesi 20/8/2015 tarihinde davanın reddine karar vermiştir. Kararın gerekçesinde; birlikte istihdam şartlarının gerçekleştiği, öte yandan iş akdinin feshine dayanak teşkil eden olayların ve nedenlerin fesih bildiriminde açık bir şekilde gösterildiği, başvuruçunun ekipteki diğer çalışanlarla kavgaya varan tartışmalar yaşadığı, bu tartışma ve kavgaların davacının tutum ve davranışlarından kaynaklandığının anlaşıldığı belirtilmiştir. Aynı zamanda başvuruçunun görevi gereği işverenin işlerini yürütmesi için verilen ve işveren tarafından da ulaşılabilceğini bildiği mail adresini kullanmak suretiyle işverenin diğer çalışanlarına karşı hakarete varan sözler sarf ettiği vurgulanarak işçinin bir başka işçiye sataşmasının işveren açısından haklı fesih nedeni oluşturacağı ve işverence yapılan feshin yerinde olduğu sonucuna varılmıştır.

16. Anılan karar, başvuruçucu vekili tarafından bozma talebiyle temyiz edilmiştir. Temyiz dilekçesinde kişisel hesaplar üzerinden gerçekleştirilen yazışmalardan oluşan e-postaların fesih gerekçesi olarak gösterilmesiyle özel hayatın gizliliğinin ve haberleşme hürriyetinin ihlal edildiği, buna rağmen ilk derece mahkemesi tarafından söz konusu mesajların delil olarak değerlendirildiği belirtilmiştir. Ayrıca kurumsal e-postanın şifreli olduğu, işyerinde çalışanlara e-posta yazışmalarının okunabileceğine dair bildirim yapılmadığı ve bu konuda çalışanların rızasının alınmadığı, davalı işverenin de dava sırasında bu durumun aksine bir iddiasının olmadığı, sadece e-postaların okunabileceğinin bilinmesi gerektiğini iddia ettiği ifade edilmiştir. Söz konusu e-posta yazışmalarının iki kişi arasındaki özel yazışmalardan ibaret olduğu ve işveren tarafından okunana kadar dış dünyaya yansımadağı vurgulanmıştır.

17. Temyiz nedenlerine karşı cevap sunan işveren; yazışmaların şirket tarafından çalışanlar adına açılmış e-posta hesapları üzerinden gerçekleştirildiğini, bu e-posta adreslerinin herhangi bir şifresinin olmadığını, bu iletişim adreslerinden yapılan tüm mesajların işverene ait sunucuda depolandığını ifade etmiştir. Ayrıca karşı cevapta, Yargıtay içtihatlarına yer verilerek işverenin işçiye tahsis ettiği bilgisayar ve kurumsal e-posta adreslerini her zaman denetleyebileceği vurgulanarak feshin haklı nedenlere dayandığı iddiası yinelenmiştir.

18. Yargıtay 9. Hukuk Dairesi 12/5/2016 tarihli ilamıyla ilk derece mahkemesinin kararını, başvuruçuyu davalıların birlikte istihdam ettiğine ilişkin kısmı gerekçeden çıkarmak suretiyle onamıştır.

19. Nihai karar 17/6/2016 tarihinde başvuruçuya tebliğ edilmiştir.

20. Başvurucu 15/7/2016 tarihinde bireysel başvuruda bulunmuştur.

21. Ayrıca başvurucu vekili 7/2/2018 tarihli dilekçesiyle 24/6/2016 tarihinde onama kararının maddi hataya dayalı olarak verildiğini ileri sürerek kararın ortadan kaldırılması talebiyle yaptığı başvurusu üzerine Dairenin onama kararının gerekçesini değiştirdiğini bildirmiştir. Ulusal Yargı Ağı Bilişim Sistemi (UYAP) üzerinden yapılan incelemede anılan başvuru üzerine Dairenin 12/5/2016 tarihli kararın sehven yazıldığını kabul ederek vermiş olduğu 13/10/2016 tarihli kararında, derece mahkemesinin iş akdinin feshinin haklı nedenlere dayandığı yönündeki kabulünün doğru bir değerlendirme olmadığı belirtilmiştir. Daire kararında, başvuru davranışlarının haklı fesih aralığında olmadığı ancak verilen dilekçeler ve tanık anlatımları gözetildiğinde başvuru davranışlarının işyerinde huzursuzluğa yol açan ve çalışma barışını bozan nitelikte olduğu, bu nedenle feshin geçerli nedene dayandığı vurgulanmış; kararın onanmasına hükmedilmiştir.

IV. İLGİLİ HUKUK

A. Ulusal Hukuk

22. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Amaç" kenar başlıklı 1. maddesinin ilgili kısmı şöyledir:

"Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir."

23. 6698 sayılı Kanun'un "Kapsam" kenar başlıklı 2. maddesi şöyledir:

"Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır."

24. 6698 sayılı Kanun'un "Tanımlar" kenar başlıklı 3. maddesinin ilgili kısmı şöyledir:

" (1) Bu Kanunun uygulanmasında;

a) Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,

...

d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi,

depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,"

25. 6698 sayılı Kanun'un "Kişisel verilerin işleme şartları" kenar başlıklı 5. maddesi şöyledir:

" (1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması."

26. 6698 sayılı Kanun'un "Veri sorumlusunun aydınlatma yükümlülüğü" kenar başlıklı 10. maddesi şöyledir:

"(1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere;

a) Veri sorumlusunun ve varsa temsilcisinin kimliği,

b) Kişisel verilerin hangi amaçla işleneceği,

c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabilceği,

ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,

d) 11 inci maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür."

27. 6698 sayılı Kanun'un "İlgili kişinin hakları" kenar başlıklı 11. maddesi şöyledir:

"(1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

- a) Kişisel veri işlenip işlenmediğini öğrenme,
- b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- c) Kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
- e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
- f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir."

28. 22/5/2003 tarihli ve 4857 sayılı İş Kanunu'nun "İşverenin haklı nedenle derhal fesih hakkı" kenar başlıklı 25. maddesinin ilgili kısmı şöyledir:

"Süresi belirli olsun veya olmasın işveren, aşağıda yazılı hallerde iş sözleşmesini sürenin bitiminden önce veya bildirim süresini beklemeksizin feshedebilir:

...

II- Ahlak ve iyi niyet kurallarına uymayan haller ve benzerleri:

...

d) İşçinin işverene yahut onun ailesi üyelerinden birine yahut işverenin başka işçisine sataşması..."

29. 4/2/2011 tarihli ve 6098 sayılı Türk Borçlar Kanunu'nun "Özen ve sadakat borcu" kenar başlıklı 396. maddesinin ilgili kısmı şöyledir:

"İşçi, yüklendiği işi özenle yapmak ve işverenin haklı menfaatinin korunmasında sadakatle davranmak zorundadır.

İşçi, işverene ait makineleri, araç ve gereçleri, teknik sistemleri, tesisleri ve taşıtları usulüne uygun olarak kullanmak ve bunlarla birlikte işin görülmesi için kendisine teslim edilmiş olan malzemeye özen göstermekle yükümlüdür..."

30. 6098 sayılı Kanun'un "Düzenlemelere ve talimatlara uyma borcu" kenar başlıklı 399. maddesi şöyledir:

"İşveren, işin görülmesi ve işçilerin işyerindeki davranışlarıyla ilgili genel düzenlemeler yapabilir ve onlara özel talimat verebilir. İşçiler, bunlara dürüstlük kurallarının gerektirdiği ölçüde uymak zorundadırlar."

31. 6098 sayılı Kanun'un "İşçinin kişiliğinin korunması" kenar başlıklı 417. maddesi şöyledir:

"İşveren, hizmet ilişkisinde işçinin kişiliğini korumak ve saygı göstermek ve işyerinde dürüstlük ilkelerine uygun bir düzeni sağlamakla, özellikle işçilerin psikolojik ve cinsel tacize uğramamaları ve bu tür tacizlere uğramış olanların daha fazla zarar görmemeleri için gerekli önlemleri almakla yükümlüdür.

İşveren, işyerinde iş sağlığı ve güvenliğinin sağlanması için gerekli her türlü önlemi almak, araç ve gereçleri noksansız bulundurmak; işçiler de iş sağlığı ve güvenliği konusunda alınan her türlü önleme uymakla yükümlüdür.

İşverenin yukarıdaki hükümler dâhil, kanuna ve sözleşmeye aykırı davranışı nedeniyle işçinin ölümü, vücut bütünlüğünün zedelenmesi veya kişilik haklarının ihlaline bağlı zararların tazmini, sözleşmeye aykırılıktan doğan sorumluluk hükümlerine tabidir."

32. 6098 sayılı Kanun'un "Kişisel verilerin kullanılmasında" kenar başlıklı 419. maddesi şöyledir:

"İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir. Özel kanun hükümleri saklıdır."

B. Uluslararası Hukuk

1. Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi

33. Birleşmiş Milletler Genel Kurulunun 10/12/1948 tarihli ve 217 (111) sayılı kararı ile kabul edilen İnsan Hakları Evrensel Beyannamesi'nin 12. maddesi şöyledir:

"Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfî karışmalara, şeref ve şöhretine karşı tecavüzlere mâruz kalamaz. Herkesin bu karışmalara ve tecavüzlere karşı kanun ile korunmağa hakkı vardır."

34. Birleşmiş Milletler Genel Kurulu tarafından kişisel verilerin korunması konusunda kabul edilen 14/12/1990 tarihli ve 45/95 sayılı "Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler"de şu temel ilkelere yer verilmiştir:

"1- İşlemenin hukuka uygun ve adil olması ilkesi: Kişilerin hakkındaki veriler hukuka aykırı veya adil olmayan şekilde toplanmamalı veya işlenmemelidir. Ayrıca Birleşmiş Milletler Şartı'ndaki ilkelere aykırı amaçlarla kullanılmamalıdır.

2- Doğruluk ilkesi: Kişisel verileri tutmakla sorumlu makamlar bu bilgilerin doğru tutulmasını güvence altına almalıdır.

3- Belirli ve meşru amaçlar için işleme ilkesi: Bir kaydın tutulması ve kullanımı meşru ve belirli bir amaca dayalı olmalıdır. Bütün kişisel veriler amaç ile ilgili ve onu gerçekleştirmeye elverişli olacak şekilde toplanmalı ve kaydedilmelidir. Bu kişisel verilerin hiçbiri, ilgili kişinin rızası dışında, belirtilenlerle uyuşmayan amaçlar için kullanılamaz veya ifşa edilemez. Kişisel verilen saklanma süresi, belirtilen amaçlara ulaşılmasını sağlayacak süreyi aşamaz.

4- İlgili kişilerin erişmesi ilkesi: Kimlik kanıtı sunan herkes kendisiyle ilgili bilgilerin işlenip işlenmediğini bilme ve gereksiz bir gecikme veya masraf olmadan anlaşılır biçimde elde etme hakkına sahiptir. Ayrıca bu bilgilerin kanuna aykırı, gereksiz veya yanlış olması durumunda uygun düzeltmelerin yapılmasını veya silinmesini talep etme hakkına sahiptir. Devletler buna uygun bir çözüm yolu sağlamak durumundadır. Herhangi bir düzeltme maliyeti dosyadan sorumlu kişi tarafından karşılanmalıdır. Bu ilke hükümlerinin uyruk veya ikâmetine bakılmaksızın herkes için uygulanması arzu edilir.

5- Ayrımcılığın önlenmesi ilkesi: (6) numaralı ilkede kısıtlı olarak öngörülen hâller söz konusu olduğunda ırk veya etnik köken, renk, cinsel yaşam, siyasi görüş, dini, felsefi ve diğer inançların yanı sıra dernek veya sendika üyeliği bilgileri de dahil olmak üzere kanuna aykırı veya keyfi olarak ayrımcılığa yol açabilmesi muhtemel veriler toplanmamalıdır.

6- Üstün amaçlar için istisna koyabilme ilkesi: Ulusal güvenlik, genel sağlık ve ahlakı korumak veya özellikle zulüm gören kişilerin ve diğerlerinin hak ve özgürlüklerinin korunması amacıyla (1) ila (4) numaralı ilkelerden ayrılabilme mümkün olabilir. Ancak bu tür istisnalar, sınırlarının açıkça belirlendiği ve uygun tedbirlerin ortaya konulduğu iç hukuk sistemine göre yürürlüğe konan bir kanun veya eşdeğer bir düzenlemede açıkça belirtilmiş olmalıdır.

7- Güvenlik ilkesi: Veri dosyaları, kaza ile kaybetme veya yok etme gibi doğal afetler, hileli verilerin yanlış kullanılması ya da bilgisayar virüsleri gibi insan odaklı tehlikelere karşı uygun tedbirlerle korunmalıdır.

8- Denetleme ve yaptırım ilkesi: Her ülkenin kanunu, yerel hukuk sistemine uygun olarak yukarıda belirtilen ilkelere uyulmasından sorumlu makamı belirler. Bu makam tarafsızlık, veri işleme ve

oluşturmadan sorumlu kişilere karşı bağımsızlık ve teknik yeterlilik teminatı sunmalıdır. Yukarıda belirtilen ilkeleri uygulayan ulusal kanun hükümlerinin ihlali durumunda cezai veya diğer idari yaptırımlar uygun bireysel çözümlerle birlikte öngörülmüş olmalıdır.

9- Sınır ötesi veri transferi ilkesi: Sınır ötesi bir veri akışı ile ilgili olarak iki veya daha fazla ülkenin mevzuatı mahremiyetin korunması için karşılaştırılabilir güvenceler sunduğu takdirde veri dolaşımı mümkün kılınabilir."

2. Avrupa Birliği Genel Veri Koruma Tüzüğü

35. 27/4/2016 tarihli ve 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nün "Tanımlar" kenar başlıklı 4. maddesinin ilgili kısmı şöyledir:

"Bu Tüzük'ün amaçları doğrultusunda, aşağıdaki tanımlar geçerlidir:

Kişisel veri, belirli veya belirlenebilir bir gerçek kişi hakkındaki her bilgiyi ifade eder (veri sahibi); belirlenebilir bir gerçek kişi ad, kimlik, yer bilgisi, online kimlik veya kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel ya da sosyal kimliği gibi belirleyici bir özelliklerle doğrudan veya dolaylı olarak belirlenebilen kişidir.

İşleme, kişisel veri veya kişisel veri dizisinin otomatik veya başka bir şekilde toplanması, kaydedilmesi, organize edilmesi, yapılandırılması, depolanması, uyarlanması veya değiştirilmesi, geri alınması, kullanılması, iletim yoluyla açıklanması, yayılması veya erişilebilir hâle getirilmesi, sıralanması veya kombine edilmesi, sınırlandırılması, silinmesi veya yok edilmesi gibi yollarla herhangi bir işlem veya işlem dizisine tabi tutulması anlamına gelir."

36. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün "Kişisel verilerin işlenmesi ile ilgili ilkeler" kenar başlıklı 5. maddesinin ilgili kısmı şöyledir:

"Kişisel veri;

Veri sahibi ile ilgili olarak hukuka uygun, adil ve şeffaf bir biçimde işlenmelidir (hukuka uygunluk, adillik ve şeffaflık),

Belirlenmiş, açık ve meşru amaçlar için toplanmış olmalı ve bu amaçlara uygun olmayan bir şekilde işlenmemelidir. Kamu yararı, bilimsel ve tarihsel amaçlar ya da arşivleme amacıyla yapılacak diğer işlemler madde 89/1 uyarınca başlangıç amaçlarıyla uyumsuz kabul edilmeyecektir (amaç sınırlaması)

Yeterli, ilgili ve işlendiği amaçlar için gerekli olanlarla sınırlı işlenmelidir (verilerin en az seviyeye indirilmesi)

Dođru ve gerektiğinde gncel tutulmalı; hatalı olan kiřisel verinin iřlenme amacına bakılmaksızın gecikmeden silinmesini veya dzltilmesini sađlamak iin makul her adım atılmalıdır (dođruluk).

İřlenme amacı iin gerekenden daha uzun olmayan bir sre boyunca veri konularının tanımlanmasına izin veren bir formda tutulmalıdır. Kiřisel veriler, veri sahibinin hak ve zgrlklerini korumak iin bu Tzğn ngrdđ uygun teknik ve yapısal tedbirler alınmak kaydıyla Tzğn 89/1. maddesi uyarınca sadece kamu yararına, bilimsel veya tarihi arařtırma amalarına ya da istatistiki amalara ynelik olarak arřivleme amacıyla daha uzun bir sre saklanabilir (saklama sresinin sınırlandırılması).

Yetkisiz veya kanun dıřı iřlemeye ve kazara kayıp, imha ve hasara karřı uygun teknik veya yapısal tedbirler alınarak kiřisel verilerin gvenli bir biimde iřlenmesi sađlanmalıdır (btnlk ve gizlilik)."

37. Avrupa Birliđi Genel Veri Koruma Tzğ'nn "Kısıtlamalar" kenar bařlıklı 23. maddesinin ilgili kısmı řyledir:

"Veri sorumlusunun veya iřleyeninin tabi olduđu Birlik veya ye Devlet hukuku, 12. ila 22. (bunlara karřılık geldiđi srece 5. madde) ve 34. maddelerdeki ykmllkleri ve hakların kapsamını, temel hak ve zgrlklerin zne saygı gsterdiđinde ve demokratik bir toplumda korunmak iin gerekli ve orantılı bir tedbir olduđu takdirde ařađıdaki hllerde kanun yoluyla sınırlayabilir:

Ulusal gvenlik,

Savunma,

Kamu gvenliđi,

Kamu gvenliđine ynelik tehditlerin nlenmesi de dahil olmak zere suların nlenmesi, soruřturulması, tespit edilmesi, kovuřturulması veya cezaların infazı,

Birliđin veya ye Devletin genel olarak kamu yararına olan diđer nemli hedeflerin, zellikle para, bte, nemli bir vergilendirme, kamu sađlıđı veya sosyal gvenlik dahil olmak zere nemli bir ekonomik veya mali ıkar amacıyla,

Yargı bađımsızlıđının ve yargısal iřlemlerin (srecin) korunması,

Regle edilmiř meslekler iin etik ihlallerin nlenmesi, tespiti, soruřturulması ve kovuřturulması,

(a) ila (e) ve (g) maddelerinde atıfta bulunulan hllerde resmi otoritenin kullanımına zaman zaman bađlı olsa bile izleme, inceleme veya dzenleyici iřlevinin yerine getirilmesi,

Veri sahibinin veya bařkalarının hak ve zgrlklerinin korunması,

Medeni hukuk hak ve alacaklarının icrası,

Özellikle 1. paragrafta atıfta bulunulan herhangi bir hukuki tedbir öngören kanun en azından uygun olduğu hâllerde şu belirli hükümleri içermelidir:

İşleme veya işleme kategorilerinin amaçları,

Kişisel veri kategorileri,

Tanınan kısıtlamaların boyutu,

Keyfi veya hukuk dışı erişimin ya da aktarımın önlenmesine dair güvenceler,

Sorumlunun veya sorumlu kategorilerinin belirlenmesi,

Depolama dönemleri ve işlemenin niteliği, kapsamı ve amaçları veya işleme kategorileri dikkate alınarak uygulanabilir güvenceler,

Veri sahibinin hakları ve özgürlüklerine getirilen riskler,

Veri sahibinin, amacına halel getirmediği sürece kısıtlama hakkında bilgilendirilmesi."

3. Avrupa İnsan Hakları Sözleşmesi

38. Avrupa İnsan Hakları Sözleşmesi'nin (Sözleşme) "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesi şöyledir:

"(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."

4. Avrupa Konseyi Siber Suç Sözleşmesi

39. Türkiye Cumhuriyeti tarafından 10/11/2010 tarihinde imzalanan ve Türkiye Büyük Millet Meclisi tarafından onaylanması uygun bulunarak 2/5/2014 tarihinde yürürlüğe giren Avrupa Konseyi Siber Suç Sözleşmesi'nin "Depolanmış bilgisayar verilerine izinli şekilde veya bu verilerin halka açık olduğu durumlarda sınır ötesinden erişim sağlanması" kenar başlıklı 32. maddesi şöyledir:

"Bir taraf, diğer tarafın izni olmaksızın; a) Halkın serbest kullanımına sunulan (açık kaynaktan gelen) depolanmış bilgisayar verilerine bunların coğrafi konumuna bakılmaksızın erişilebilir; veya b) Kendi ülkesindeki bir bilgisayar sistemi aracılığıyla, diğer tarafın ülkesindeki depolanmış bilgisayar verilerine, eğer bu taraf, söz konusu bilgisayar sistemi aracılığıyla veriyi ifşa etme yetkisini yasal

olarak haiz bulunan kişinin yasal ve gönüllü onayını sağlayabilirse, söz konusu verilere erişebilir veya bunları temin edebilir."

5. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

40. 18/2/2016 tarihli ve 29628 sayılı Resmî Gazete'de yayımlanan 30/1/2016 tarihli ve 6669 sayılı Kanun'la uygun bulunan 28/1/1981 tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "Tanımlar" kenar başlıklı 2. maddesinin ilgili kısmı şöyledir:

"Bu Sözleşmenin amaçları bakımından:

a "Kişisel veriler": Kimliği belirli veya belirlenebilir bir gerçek kişi ("ilgili kişi") hakkındaki tüm bilgileri ifade eder.

...

c "Otomatik işlem"den, tamamen veya kısmen otomatik yöntemlerle gerçekleştirilen; verilerin kaydı, bu verilere mantıksal ve/ veya aritmetik işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya dağıtılması anlaşılır."

41. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "Verilerin Niteliği" kenar başlıklı 5. maddesi şöyledir:

"Otomatik işleme konu olan kişisel veriler:

- a. Adil biçimde ve yasal yoldan elde edilir ve işlenir;
- b. Belli ve meşru amaçlar için kaydedilir ve bu amaçlara aykırı şekilde kullanılmaz;
- c. Kaydedilme amaçlarına göre uygun ve yerinde olur ve aşırı olmaz;
- d. Doğru bilgileri yansıtır ve gerektiğinde güncellenir;
- e. Kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkan veren bir biçimde saklanır."

42. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "İstisnalar ve kısıtlamalar" kenar başlıklı 9. maddesinin ilgili kısmı şöyledir:

"2. Taraf devletin kanunlarında öngörülmüş olması ve demokratik bir toplumda aşağıdaki hususların sağlanması için gerekli bir önlem oluşturması halinde işbu Sözleşmenin 5, 6 ve 8. maddelerine istisna getirilebilir:

a. Devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi;

b. İlgili kişinin veya başkasının hak ve özgürlüklerinin korunması.”

6. Avrupa İnsan Hakları Mahkemesi İçtihadı

43. Avrupa İnsan Hakları Mahkemesi (AİHM) içtihatlarında özel hayatın eksiksiz bir tanımı bulunmayan geniş bir kavram olduğunu belirtmektedir. Özel hayata saygı hakkı alt kategorisinde geçen özel hayat kavramı AİHM tarafından oldukça geniş yorumlanmakta ve bu kavrama ilişkin tüketici bir tanım yapılmaktan özellikle kaçınılmaktadır (Koch/Almanya, B. No: 497/09, 19/7/2012, § 51). Bununla birlikte Sözleşme'nin denetim organlarının içtihatlarında bireyin kişiliğini serbestçe geliştirmesi ve gerçekleştirmesi ile kişisel bağımsızlık kavramlarının özel hayata saygı hakkının kapsamının belirlenmesinde temel alındığı anlaşılmaktadır (Sidabras ve Džiautas/Litvanya, B. No: 55480/00, 59330/00, 27/7/2004, § 43; K.A. ve A.D./Belçika, B. No: 42758/98, 45558/99, 17/2/2005, § 83; Pretty/Birleşik Krallık, B. No: 2346/02, 29/4/2002, § 61; Christine Goodwin/Birleşik Krallık [BD], B. No: 28957/95, 11/7/2002, § 90).

44. AİHM'e göre mesleki hayat özel hayat kavramı dışında tutulamaz. Özel hayat unsurları gerekçe gösterilerek mesleki hayata getirilen sınırlamalar, bireyin sosyal kimliğini etkilediği ölçüde Sözleşme'nin 8. maddesi kapsamına girebilmektedir. AİHM bireylerin genellikle iş yaşamında dış dünyayla ilişkiler kurduğunu hatırlatarak bireyin kimliğini oluşturmasının ve sosyalleşmesinin önemli bir aracı olan dış dünyayla ilişki kurma hakkının bireyin iş çevresini de kapsadığını, bu durumun serbest meslek bağlamında özellikle geçerli olduğunu ifade etmiştir (Niemitz/Almanya, B. No: 137/1088, 16/12/1992, § 29; Özpınar/Türkiye, B. No: 20999/04, 19/10/2010, § 45; Campagnano/İtalya, B. No: 77955/01, 23/3/2006, § 53).

45. Sözleşme'nin 8. maddesinde geçen yazışma teriminin mektup gibi geleneksel iletişim araçları yanında telefon, faks ve e-posta gibi yeni teknolojik araçlarla yapılan iletişimi de kapsadığını, özel hayata saygı hakkı ve bu hakkın bir görünümü olan haberleşme hürriyetinin işyerindeki iletişim bakımından da uygulanabilir nitelikte olduğunu tespit eden AİHM, özel hukuk iş ilişkilerinde Sözleşme'nin 8-11. maddelerinin ihlal edildiği iddiasıyla önüne gelen davalarda devletin pozitif yükümlülükleri bağlamında inceleme yapmakta ve anılan hakların ulusal mahkemelerce yeterli derecede korunup korunmadığını irdelemektedir (Palomo Sanchez ve diğerleri/İspanya [BD], B. No: 28955/06..., 12/9/2011, § 61, Bărbulescu/Romanya [BD], B. No: 61496/08, 5/9/2017, §§ 69-81).

46. AİHM Bărbulescu/Romanya kararında çalışanın iletişiminin işveren tarafından denetlenmesiyle ilgili ilkeleri belirlemiştir. İlgili kararın konusunu, bir işyerinde mühendis olarak çalışan başvurucunun işverenin talebiyle açtığı e-posta hesabının başvurucuya önceden haber verilmeden işveren tarafından denetlenmesi oluşturmaktadır. İşveren inceleme sonucunda başvurucuya, kurumsal e-posta üzerinden kardeşi ve nişanlısı ile mesajlaşmak suretiyle interneti işyeri iç düzenlemelerine aykırı olarak kişisel amaçla kullandığının tespit edildiğini bildirmiştir. İşveren, başvurucunun iş ahdini şirketin iç düzenlemelerinde yer alan "Şirket disiplini ile düzenini bozan ve özellikle, bilgisayarların, fotokopi makinelerinin, telefonların, teleks ve faks makinelerinin kişisel amaçlarla kullanılması kesinlikle yasaktır." düzenlemesine dayanarak feshetmiştir. Başvurucunun işe iade istemli davası da yerel mahkemelerce reddedilmiştir. AİHM inceleme sonucunda Sözleşme'nin 8. maddesinin ihlal edildiğine karar vermiştir.

47. AİHM, iş hukukunun dikkate alınması gereken kendisine özgü özellikleri olduğunu hatırlattıktan sonra çalışanın işyerinde özel hayatına ve yazışmasına saygı gösterilmesi hakkının kullanımı hususunda Avrupa'da bir mutabakat bulunmadığını gözeterek işverenin çalışanların işyerindeki mesleki nitelikte olmayan elektronik ortamdaki yazışmaları hakkında düzenlemeler yapabileceği koşulları belirleyen yasal bir çerçeve çizilmesi konusundaki gerekliliğin değerlendirilmesinde Sözleşmeciler devletlerin geniş bir takdir yetkisi olduğunu belirtmiştir. Bununla birlikte AİHM devletlerin anılan takdir yetkisinin sınırsız olmadığını, devletler tarafından işverence yazışmaların ve diğer iletişim türlerinin incelenmesi kapsamında alınan tedbirlerin kötüye kullanımı engellemek adına yeterli güvenceleri içermesi gerektiğini vurgulamıştır (Bărbulescu/Romanya, §§ 113-119)

48. AİHM Bărbulescu/Romanya kararında, iletişim alanındaki hızlı gelişmelere rağmen keyfilğe karşı orantılılık incelemesinin ve usule ilişkin güvencelerin varlığının zorunlu olduğunu belirterek çalışanın iletişiminin incelenmesi bağlamında devletin pozitif yükümlülüklerine ilişkin esasları tespit etmiştir. Bu bağlamda AİHM işverenin denetleme yöntemleri hakkında çalışana önceden açıkça bilgilendirilip bilgilendirilmediğinin ve yapılan incelemenin kapsamı ile iletişimin denetlenmesi yoluyla çalışanın mahremiyetine ne ölçüde müdahale edildiğinin gözetilmesi gerektiğini vurgulamıştır. Bu noktada AİHM iletişim akışının incelenmesi ile iletişimin içeriğinin incelenmesi arasında ayırım yaparak içerik incelemesine ayrı bir önem atfetmiş ve incelemenin süresi, inceleme sonucuna erişen kişi sayısı gibi hususların gözönünde tutulması gerektiğini belirtmiştir. AİHM'e göre işveren iletişimin incelenmesini haklı kılan meşru gerekçeleri ortaya koyabilmelidir. Ayrıca amaçlanan sonucun içerik incelemesi yapılmadan daha hafif bir müdahale teşkil eden yöntem ile elde etmenin mümkün olmaması gerekir. AİHM çalışana iletişimin denetlenmesi tedbiri karşısında yeterli

güvencelerin sağlanması ve inceleme sonucunda elde edilen verilerin hedeflenen amaç doğrultusunda kullanılması gerektiğini belirtmiştir. AİHM'e göre pozitif yükümlülükler dair bu ilkelerin her somut olayın özelliğine göre ne ölçüde uygulandığının yetkili yargı organı tarafından tespit edilmesi gerekir (Bărbulescu/Romanya, §§ 112, 123).

49. 18/2/2016 tarihli ve 29628 sayılı Resmî Gazete'de yayımlanan, 6669 sayılı Kanun'la uygun bulunan 28/1/1981 tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "Tarafların görevleri" kenar başlıklı 4. maddesinin birinci fıkrası şöyledir:

"Her Taraf, kendi iç hukukunda işbu bölümde yer alan verilerin korunmasına ilişkin temel ilkelere işlerlik kazandırmak amacıyla gerekli önlemleri alır."

50. Anılan sözleşmenin "Verilerin niteliği" kenar başlıklı 5. maddesi şöyledir:

"Otomatik işleme konu olan kişisel veriler:

- a. Adil biçimde ve yasal yoldan elde edilir ve işlenir;
- b. Belli ve meşru amaçlar için kaydedilir ve bu amaçlara aykırı kullanılamaz;
- c. Kaydedilme amaçlarına göre uygun ve yerinde olur ve aşırı olmaz;
- d. Doğru bilgileri yansıtır ve gerektiğinde güncellenir;
- e. Kaydedilme amaçlarını gerçekleştirmek için gerekli süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkân veren bir şekilde saklanır."

51. Anılan sözleşmenin "Yaptırımlar ve başvuru yolları" kenar başlıklı 10. maddesi şöyledir:

"Her bir Taraf, iş bu bölümde düzenlenen verilerin korunması hakkındaki temel ilkelere işlerlik sağlayan iç hukuk kurallarının ihlaliyle ilgili uygun yaptırımlar ve başvuru yolları getirmekle yükümlüdür."

V. İNCELEME VE GEREKÇE

52. Mahkemenin 17/9/2020 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları

53. Başvurucu; kurumsal e-posta hesapları üzerinden gerçekleştirdiği kişisel yazışmaların rızası olmaksızın işveren tarafından incelendiğini, çalışanların e-postalarının incelenebileceğine, denetleneceğine dair işyerinde yazılı ya da sözlü bir kuralın mevcut olmadığını, işverenin iş sözleşmesinin feshine gerekçe bulmak amacıyla böyle bir inceleme yaptığını belirtmiştir. Ekip lideri, A.A.Y.nin kurumsal e-posta hesabı üzerinden binlerce yazışmanın işveren tarafından incelendiğini,

bunların arasından işverenin okuyacağını düşünmeden yazdığı ve inceleme anına kadar işverenin bilmediği kişisel yazışma niteliğindeki e-posta içeriklerinin fesih gerekçesi yapıldığını, açtığı işe iade istemli tespit davasında da söz konusu yazışmaların delil olarak kabul edildiğini ifade etmiştir. Ayrıca feshin haklı ya da geçerli bir sebebe dayanmadığını, feshin sebebinin öğrenilmesinden itibaren altı iş günü içinde feshin yapılmadığını, derece mahkemesinin itirazlarını ve delillerini karşılayacak şekilde gerekçe sunmadığını belirterek adil yargılanma hakkı ile haberleşme hürriyeti ve özel hayata saygı hakkının ihlal edildiğini ileri sürmüştür. Başvurucu, ifa ettiği mesleğin özelliklerini gerekçe göstererek kamuya açık belgelerde kimlik bilgilerinin gizli tutulmasını talep etmiştir.

B. Değerlendirme

54. Anayasa'nın iddianın değerlendirilmesinde dayanak alınacak "Özel hayatın gizliliği" kenar başlıklı 20. maddesinin birinci ve üçüncü fıkrası şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

...

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

55. Anayasa'nın "Haberleşme hürriyeti" kenar başlıklı 22. maddesi şöyledir:

"Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.

İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir."

56. Özel hayata saygı hakkı Anayasa'nın 20. maddesinde koruma altına alınmıştır. Devlet, kişilerin özel ve aile hayatına keyfî olarak müdahale etmemek ve üçüncü kişilerin haksız saldırılarını önlemekle yükümlüdür.

57. Anayasa'nın 20. maddesinin üçüncü fıkrasında ise herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı ayrıca düzenlenmiş ve güvence altına alınmıştır. Söz konusu anayasal güvence, Sözleşme'nin 8. maddesinde koruma altına alınan özel hayata saygı hakkına karşılık gelmektedir. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır (AYM, E.2014/122, K.2015/123, 30/12/2015, §§ 19, 20).

58. Anayasa Mahkemesi kararlarında da belirtildiği üzere kişisel veri -belirli veya kimliği belirlenebilir olmak şartıyla- bir kişiye ilişkin bütün bilgileri ifade etmekte olup bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi sadece kimliğini ortaya koyan bilgileri değil telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, öz geçmiş, resim, görüntü ve ses kayıtları, parmak izleri, sağlık bilgileri, genetik bilgiler, IP adresi, e-posta adresi, alışveriş alışkanlıkları, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır (AYM, E.2014/74, K.2014/201, 25/12/2014; E.2014/180, K.2015/30, 19/3/2015).

59. Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı yönünden inceleme yapılabilmesi için öncelikle anılan hak kapsamında korunması gereken bir kişisel verinin olup olmadığı belirlenmelidir. Anayasa hükmünün lafzı, konuya ilişkin uluslararası belgeler ve karşılaştırmalı hukuk dikkate alındığında belirli veya belirlenebilir bir gerçek veya tüzel kişi hakkındaki her türlü bilgi kişisel veri olarak değerlendirilir. Ancak her davada ya da başvuruda Anayasa'nın 20. maddesinin üçüncü fıkrası anlamında bir kişisel veri bulunup bulunmadığı davanın ve başvurunun kendine özgü koşulları dikkate alınarak otonom olarak tespit edilir. Bir kişisel verinin bulunduğu tespit edildiğinde bu veriye yönelik her türlü sınırlama ve müdahale Anayasa'nın anılan hükmü kapsamındaki güvenceleri harekete geçirir.

60. Ayrıca Anayasa'nın 22. maddesinde güvence altına alınan haberleşme hürriyeti, haberleşmenin yanında içeriği ve biçimi ne olursa olsun haberleşmenin içeriğinin gizliliğini de güvence altına almaktadır. Haberleşme bağlamında bireylerin karşılıklı ve toplu olarak sözlü, yazılı ve görsel iletişimlerine konu olan ifadelerinin gizliliğinin sağlanması ve haberleşmeye yönelik haksız müdahalelerde bulunulmaması gerekir (Yasemin Çongar ve diğerleri, B. No: 2013/7054, 6/1/2015, § 49).

61. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Somut olayda işverenin başvurucaunun kurumsal e-posta hesabını kullanarak yaptığı mesajlaşmalarını denetlemesi ve içeriğinin geriye dönük olarak incelemesi sonucu elde ettiği bilgileri iş ahdinin feshine dayanak yapması söz konusudur. Ayrıca e-posta bilgilerinin internet ortamında saklı tutulduğu, bu verilere erişildiği ve içeriğinin denetlenerek kullanıldığı dikkate alındığında veri işleminin söz konusu olduğu da söylenebilir. Bu durumla birlikte başvurucaunun e-posta bilgileri ve yazışmalarının belirli bir gerçek kişi hakkındaki bilgi kapsamında olduğu gözetildiğinde bu bilgilere erişilmesinin, bunların kullanılmasının ve işlenmesinin özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyeti yönünden incelenmesi gerektiği değerlendirilmiştir.

1. Kabul Edilebilirlik Yönünden

62. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan kişisel verilerin korunması hakkı ile haberleşme hürriyetinin ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

2. Esas Yönünden

a. Genel İlkeler

63. Anayasa'nın 20. maddesinin üçüncü fıkrasının birinci cümlesinde genel olarak herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu belirtilmiş, ikinci cümlesinde kişisel veriler bağlamında bazı özel güvenceler sayılmış, üçüncü cümlesinde kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği düzenlenmiş, dördüncü cümlesinde ise kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hüküm altına alınmıştır. Buna göre lafzı dikkate alındığında Anayasa'nın 20. maddesinin üçüncü fıkrasının kişisel verilerin korunmasını isteme hakkı kapsamında sadece işleme şeklindeki sınırlama ya da müdahalelere karşı değil kişisel verilere yönelik her türlü müdahale ve sınırlamalara karşı güvence getirdiği anlaşılmaktadır.

64. Öte yandan Anayasa ve Sözleşme'nin ortak koruma alanı kapsamında kalan temel haklar, yalnızca kamusal gücün doğrudan uygulanmasıyla değil kimi zaman da özel hukuk kişileri arasındaki uyuşmazlıklara konu olacak şekilde üçüncü kişilerin müdahaleleriyle zedelenebilmektedir. İlkinde söz konusu güvencelerin sağlanması adına kamusal makamlara yüklenen negatif ve pozitif tüm yükümlülüklerin doğrudan yerine getirilmesi konusunda tereddüt bulunmamakta ise de ikinci

durumda devletin üçüncü kişilerin müdahalelerine karşı bireylere ne tür bir koruma imkânı sunması gerektiği ve hangi çerçevede yükümlülükler taşıdığı hususunda her olayın kendine özgü koşullarına göre değerlendirmelerde bulunulması gerekmektedir (Ömür Kara ve Onursal Özbek, B. No: 2013/4825, 24/3/2016, § 45).

65. Yine Anayasa'nın 12. maddesine göre herkes kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlere sahiptir. Bu genel nitelikteki anayasal düzenleme ile bireylerin kişilik değerlerine yönelen ve zarar veren olumsuz tutum ve davranışlar dışlanmaktadır. Ayrıca Anayasa'nın 5. maddesinde bireylerin temel hak ve özgürlüklerinin korunması, maddi ve manevi varlıklarının geliştirilmesi için gerekli şartların hazırlanması devletin temel amaç ve görevlerinden biri olarak sayılmaktadır. Bu düzenlemeler ışığında devletin bireyin temel hak ve özgürlüklerine keyfi olarak müdahale etmemenin yanında üçüncü kişilerin saldırılarını önlemekle yükümlü kılındığı, bu bağlamda pozitif yükümlülüklerinin de bulunduğu söylenebilir. Uyuşmazlıkların özel hukuk kişileri arasında gerçekleştiği durumlarda da temel hak ve özgürlüklerin sağladığı güvencelerin yerine getirilip getirilmediği denetlenirken Anayasa'nın kamusal makamlara yüklediği sorumluluklardan doğrudan özel hukuk kişileri sorumlu tutulamayacağı için taşıdığı koşulların özelliklerine göre bu tür başvuruların devletin pozitif yükümlülükleri bağlamında ele alınması gerekebilir. Dolayısıyla özel hayatın korunması kapsamında kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyeti yönünden de devletin pozitif bir yükümlülük olarak yetki alanında bulunan tüm bireyleri gerek kamusal makamların ve diğer bireylerin gerekse kişinin kendisinin eylemlerinden kaynaklanabilecek risklere karşı koruma yükümlülüğü bulunmaktadır (Ömür Kara ve Onursal Özbek, § 46; Ali Çığır, B. No: 2015/19298, 8/5/2019, §§ 32, 33; Erol Kumcu, B. No: 2015/18988, 9/5/2019, §§ 32, 33; U.B., B. No: 2015/3175, 10/10/2019, §§ 33, 34).

66. Pozitif yükümlülükler özel hukuk kişilerinin birbirleri ile olan uyuşmazlıklarının çözümüne ilişkin yasal altyapının oluşturulmasını, söz konusu uyuşmazlıkların adil yargılama gereklerine uygun ve usul yönünden güvenceleri haiz bir yargılama kapsamında incelenmesini ve bu yargılamalarda temel haklara ilişkin anayasal güvencelerin gözetilip gözetilmediğinin denetlenmesini gerektirir. Bu doğrultuda derece mahkemelerince söz konusu güvenceler gözardı edilmemeli, işveren ve çalışanlar arasındaki çatışan çıkarlar adil biçimde dengelenmeli, başvuruların temel haklarına yönelik müdahalenin meşru amaca dayalı ve ölçülü olup olmadığı değerlendirilmeli, ulaşılan sonuç hakkında hüküm kurulurken ilgili ve yeterli gerekçeler sunulmalıdır (Ömür Kara ve Onursal Özbek, §§ 47-50).

67. Anayasa Mahkemesi daha önce iletişim araçlarının işveren tarafından denetlenmesi kapsamındaki uyuşmazlıklarda derece mahkemeleri tarafından devletin pozitif yükümlülükleri bağlamında çıkarların dengelenmesi ve müdahalenin ölçülülüğünün irdelenmesi kapsamında gözetilmesi gereken hususları genel olarak belirlemiştir; buna göre somut olayın koşullarına göre iş sözleşmelerinde kısıtlayıcı ve zorlayıcı düzenlemelerin ne şekilde belirlendiği, tarafların bu düzenlemeler hakkında bilgilendirilip bilgilendirilmediği, çalışanların temel haklarına yönelik müdahalede bulunulmasına neden olan meşru amacın müdahale ile ölçülü olup olmadığı, sözleşmenin feshinin çalışanların eylem ya da eylemsizlikleri karşısında makul ve orantılı bir işlem olup olmadığı hususlarının uyuşmazlığın çözümünde gözetilmesi gerektiğini tespit etmiştir (Ömür Kara ve Onursal Özbek, § 50).

68. Yukarıda belirtilen hususlar gözetilerek işverenin işçinin iletişimini denetlemesi yetkisini kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyeti bağlamında devletin pozitif yükümlülükleri kapsamında irdelenmek gerekmektedir. Öncelikle somut olayda olduğu gibi teknolojik gelişmelerin imkânlarından yararlanmak isteyen işverenlerin bilgisayar, internet, e-posta gibi iletişim araç ve gereçlerini çalışanın kullanıma sunması nedeniyle oluşan uyuşmazlıklarda işverenin menfaatleri ile işçinin temel hak ve özgürlükleri arasında bir dengeleme yapma gerekliliği doğmaktadır. Bu bağlamda işveren ile çalışan arasındaki ilişkinin iki taraf açısından da belirli hak ve yükümlülükler öngören ve esasen güven ilişkisi üzerine kurulu iş sözleşmesiyle şekillendiği unutulmamalıdır. Somut uyuşmazlığın ilgili olduğu iş hukukunun dinamik bir niteliğinin olduğu, ayrıca iş ilişkilerinin genel kurallardan farklı, kendine özgü bazı hukuki kurallar içerdiği de dikkate alınmalıdır.

69. Bu bağlamda işlerin etkin bir şekilde yürütülmesi ile bilgi akışının kontrolünü sağlamak, işçinin eylemlerine bağlı cezai ve hukuki sorumluluğa karşı korunmak, verimliliği ölçmek veya güvenlik endişeleri gibi haklı ve meşru görülebilecek nedenlerle işverenin yönetim yetkisi kapsamında kural olarak işçinin kullanımına sunduğu iletişim araçlarını denetleyebileceği ve kullanıma ilişkin sınırlamalar öngörebileceği söylenebilir. Ancak işverenin yönetim yetkisinin işyerinde işin yürütülmesi, işyerinin düzeninin ve güvenliğinin sağlanmasıyla sınırlı olduğu unutulmamalıdır. Bu bağlamda işverenin yetki ve haklarının sınırsız olmadığı, çalışana tanınan temel hak ve özgürlüklerin somut olayda haberleşme hürriyeti ve kişisel verilerin korunmasını isteme hakkının işyeri sınırları dâhilinde de korunduğu, aynı zamanda kısıtlayıcı ve uyulması zorunlu işyeri kurallarının çalışanların temel haklarının özünü zedeleyecek nitelikte olmaması gerektiği vurgulanmalıdır. Bu çerçevede işyerinde kullanıma sunulan iletişim araçlarının işverene ait olduğu gözetilerek sırf bu

nedenle bile işverenin iletişim araçları üzerinde sınırsız ve mutlak bir gözetleme ve denetleme yetkisinin olduğunu kabul etmek, işçinin demokratik bir toplumda temel hak ve özgürlüklerine işyerinde de saygı gösterilmesi gerektiği yönündeki haklı beklentisiyle uyuşmayacaktır.

70. Tüm bu açıklamalar çerçevesinde devletin pozitif yükümlülükleri kapsamında Anayasa Mahkemesinin özellikle derece mahkemelerinin -somut olayın koşullarına uygun düştüğü ölçüde- aşağıda belirtilen güvencelerin somut olayda hakka müdahale eden üçüncü kişi tarafından sağlanıp sağlanmadığını gereği gibi denetleyip denetlemediğini incelemesi gerekir:

i. İşverenin çalışanın kullanımına sunduğu iletişim araçlarının ve iletişim içeriklerinin incelenmesinin haklı olduğunu gösteren meşru gerekçeleri olup olmadığı denetlenmelidir. Bu durumda işverenin gerekçelerinin ifa edilen işin ve işyerinin özellikleri de gözetilerek meşru olup olmadığı irdelenmelidir. Bu denetlemede iletişim akışı ile iletişim içeriklerinin incelenmesi arasında ayırım yapılarak içeriklerin incelenmesi yönünden daha ciddi gerekçeler aranmalıdır.

ii. Demokratik bir toplumda iletişimin denetlenmesi ve kişisel verilerin işlenmesi süreci şeffaf bir şekilde gerçekleştirilmeli ve bunun bir gereği olarak da süreçle ilgili olarak çalışanlar işveren tarafından önceden bilgilendirilmelidir. Uluslararası hukuk ve karşılaştırmalı hukuk dikkate alındığında bu bilgilendirmenin -somut olayın özelliklerine uygun düştüğü ölçüde- en azından iletişimin denetlenmesi ile kişisel verilerin işlenmesinin hukuki dayanağı ve amaçları, denetlemenin ve veri işlemenin kapsamı, verilerin saklanacağı süre, veri sahibinin hakları, denetlemenin ve işlemenin sonuçları ile verilerin muhtemel yararlanıcıları hususlarını kapsaması gerekir. Ayrıca bildirimde iletişim araçlarının kullanımına ilişkin olarak işveren tarafından öngörülen sınırlamalara da yer verilmelidir. Bilgilendirmenin mutlaka belli şekilde yapılması şart olmayıp şeffaflığı sağlamak bakımından bireylere, kişisel verilerin işlenmesine ve iletişimin denetlenmesine ilişkin süreçten yukarıda belirtilen kapsamda haberdar olma imkânı sağlayan uygun bir yöntem tercih edilebilir.

iii. Çalışanın kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine işveren tarafından yapılan müdahale, ulaşılmak istenen amaç ile ilgili ve bu amacı gerçekleştirmeye elverişli olmalıdır. Ayrıca inceleme faaliyetiyle elde edilen verilerin işveren tarafından hedeflenen amaç doğrultusunda kullanılması gerekir.

iv. İşveren tarafından çalışanın kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine işveren tarafından yapılan müdahalenin gerekli kabul edilebilmesi için aynı amaca daha hafif bir müdahale ile ulaşılmak mümkün olmamalı, müdahale ulaşılmak istenen amaç bakımından zorunlu olmalıdır. Çalışanın iletişiminin içeriğine girilmesi yerine onun kişisel verilerine daha az müdahale eden yöntem ve tedbirlerin uygulanmasının mümkün olup olmadığı denetlenmelidir. Bu

kapsamda işverenin ulaşmak istediği amaca çalışanın iletişimi incelenmeden de erişilme imkânı olup olmadığı her bir vakianın somut özellikleri ışığında değerlendirilmelidir.

v. İşveren tarafından başvurucunun kişisel verilerinin korunmasını isteme hakkına ve haberleşme hürriyetine yönelik müdahalenin orantılı kabul edilebilmesi için ise iletişimin denetlenmesi ile işlenecek veya herhangi bir şekilde yararlanılacak veriler ulaşılmak istenen amaçla sınırlı olmalı, bu amacı aşacak şekilde sınırlama ya da müdahaleye izin verilmemelidir.

vi. Ayrıca iletişimin incelenmesinin muhatabı olan çalışan üzerindeki etkisi ve çalışan bakımından sonuçları gözönünde tutularak tarafların çatışan menfaat ve haklarının adil bir biçimde dengelenip dengelenmediğine bakılması gerekmektedir. Taraflardan birine şahsi olarak aşırı bir külfet yüklediğinin tespiti hâlinde devletin pozitif yükümlülüklerini yerine getirmediği sonucuna varılabilir.

b. İlkelerin Uygulanması

71. Başvurucu; e-posta yazışmalarının incelenmesi özel hayat alanına ve haberleşme hürriyetine haksız bir müdahale oluşturmasına rağmen açtığı işe iade istemli davasında bu yönde bir tespit yapılmadığını, yazışmalarının işveren tarafından alenileştirildiğini, mahkemelerce verilen kararlar nedeniyle söz konusu müdahalelerin meşru hâle getirildiğini iddia etmiştir. Bu kapsamdaki iddiaların yukarıda belirtilen esaslar gözetilerek devletin pozitif yükümlülükleri bağlamında değerlendirilmesi gerekmektedir.

72. Öncelikle işverenin işçinin kullanımına sunulan iletişim araçlarını denetlemesi ve çalışanın kişisel verilerinin işlemesine ilişkin olarak 4857 sayılı Kanun'da özel bir düzenleme olmadığı görülmüştür. Ancak Anayasa'nın 20. ve 22. maddelerinde yer bulan özel hayata saygı ile kişisel verilerin korunmasını isteme hakları ve haberleşme hürriyetine ilişkin güvenceler ile 6698 sayılı Kanun ile hukuk sistemimizde mevcut olan genel düzenlemelerin (bkz. §§ 22-29) iş hukuku uyumsuzluklarında uygulanması yönünde bir engel olmadığı gözetildiğinde yasal altyapı oluşturmak bağlamında pozitif yükümlülüklerin yerine getirilmiş olduğu söylenebilir.

73. Başvuru konusu olayda başvurucu, çok sayıda çalışanı istihdam eden bir avukatlık ortaklığı bünyesinde avukat olarak görev yapmaktadır. İşveren işyerinde yaşanan sorunlar ile ilgili yürütülen disiplin soruşturması kapsamında somut delil elde etmek amacıyla işlerin yürütülmesini kolaylaştırmak üzere oluşturulan ve çalışanın kullanımına sunulan kurumsal e-posta hesaplarının incelendiğini belirtmiştir. Başvurucu adına tanımlanmış kurumsal e-posta hesabının mevcut olduğu ve başvurucunun kullanımına sunulan bu e-posta hesabının işveren tarafından incelendiği

hususlarında başvuran ile işveren arasında bir ihtilaf olmadığı görülmüştür. Çok sayıda çalışan olduğu ve kurumsal olarak avukatlık hizmeti verdiği anlaşılan işverenin çalışanlarına kurumsal e-posta hesabı oluşturmak suretiyle kişisel verileri işleminin ve iletişim akışını denetim altında tutmasının işlerin etkin bir şekilde yürütülmesini sağlama amacına yönelik olduğu anlaşılmaktadır. Bu durumda kurumsal e-posta hesabının iletişim akışına ve içeriğine erişilecek şekilde kullanıma sunulmasının somut olayda işyerinin yönetimi bakımından meşru bir menfaat teşkil ettiği, ayrıca hedeflenen amacı sağlamaya elverişli bir yöntem olduğu söylenebilir.

74. Başvuru konusu olayda işveren yargılama aşamasında, disiplin soruşturması sırasında yapılan incelemede başvurucunun e-posta hesabında mesajların silindiğinin tespit edilmesi üzerine ekip lideri A.A.Y.nin e-postasının incelenmesiyle başvurucunun iş akdinin feshine dayanak olan mesajlarının elde edildiğini beyan etmiştir. Başvurucu, işverenin tespit ettiği mesajların incelenen binlerce mail içinden seçilen, işveren tarafından okunmayacağı beklentisiyle yazılan kişisel yazışmalar olduğunu ileri sürmüştür. Mahkemeye işveren tarafından sunulan e-posta mesajlarının başvurucu ile ekip yöneticisi arasında geçen ve genel olarak birbirleriyle ve işyeri ile ilgili düşüncelerin açıklandığı, yer yer tartışma şeklindeki diyaloglardan oluştuğu anlaşılmaktadır.

75. Öncelikle e-posta hesabı üzerinden yapılan iletişimin denetlenebileceğine ve iletişim araçlarının kullanım koşullarına ilişkin olarak önceden tam ve açık bir bilgilendirme yapılmadığı hâllerde temel hak ve özgürlüklerinin işyerinde de korunacağı yönündeki haklı beklentiyle çalışan kişinin kurumsal e-posta üzerinden kişisel yazışmalar yapabileceğinin işveren tarafından da öngörülebilecek bir durum olduğu vurgulanmalıdır. Buradan hareketle çalışana açık bir bilgilendirmenin yapılmadığı hâllerde hak ve özgürlüklerine bir müdahalede bulunulmayacağı hususunda çalışanların makul bir beklenti içinde olacaklarının kabul edilmesi, temel hak ve özgürlüklerin sağladığı güvencelerden yararlandırılması gerektiği söylenebilir.

76. Somut olayda başvurucunun yazılı olmayan iş sözleşmesi kapsamında görev yaptığı, yargılama sürecinde işverenin kurumsal e-postayı inceleme yetkisi ile kapsamını gösteren bir bildirim başvurucuya yapıldığına ilişkin bilgi ve belge sunmadığı hususları gözetildiğinde işveren tarafından kurumsal e-posta hesabı üzerinden yapılan iletişimin izlenebileceği ve denetlenebileceği yönünde açık bir bilgilendirme yapılmadığı anlaşılmaktadır. Öte yandan e-posta iletişim içerikleri gerekçe gösterilerek başvurucunun iş akdi feshedilmiştir. Ancak işveren davalı taraf olarak yargılama sürecinde kişisel verilerin işlenmesinin hukuki dayanağı ve işlemin amaçları, işlenecek verilerin kapsamı, verilerin saklanacağı süre, veri sahibinin hakları, işlemin sonuçları ve verilerin muhtemel yararlanıcılarını gösterir bir bilgilendirme yapıldığını ortaya koyamamıştır. Bu bağlamda yargılama

sürecinde feshin temel sebebini oluşturan e-posta iletişimine yönelik olarak böyle bir bilgilendirmenin yapılıp yapılmadığı derece mahkemelerince tartışılmamış, başvuruçunun kendisi alenileştirmedeği hâlde onun rızası alınmadan ve önceden bir bilgilendirme yapılmadan e-posta içeriklerine erişildiği yönündeki esaslı iddialarının karşılanmadığı anlaşılmıştır.

77. Ayrıca başvuruçunun çalışma ekibindeki diğer üyelerin disiplin soruşturmasına dayanak oluşturan şikâyet dilekçelerinde yakındıkları hususlar gözetildiğinde (bkz. § 9) başvuruçunun e-posta iletişiminin içeriğine erişilmesini zorunlu kılan bir durumun mevcut olduğunun işveren tarafından açıklanmadığı, fesih bildiriminde ise "iddiaların araştırılması ve ekip üyeleri arasındaki ilişkilerin anlaşılabilmesi" amaçlarının belirtilmesiyle yetinildiği görülmüştür. Ancak aynı amaca ulaşılabilmesi bakımından tarafların şikâyet ve savunmalarının analizi, tanıkların dinlenilmesi, işyeri kayıtları ile yürütülen projelerin süreç ve sonuçlarının incelenmesi gibi araçlar da mevcut olduğu hâlde niçin e-posta içeriklerinin incelenmesinin zorunlu ve gerekli görüldüğü işveren tarafından açık bir şekilde ortaya konulmadığı gibi derece mahkemeleri tarafından da somut olay bu yönüyle tartışılmamıştır.

78. Öte yandan somut olayda işverenin yaptığı müdahalenin kapsamının tartışılması gerekir. Bu bağlamda yargılama kapsamında işveren tarafından sunulan başvuruçunun yazışmaları ve yargılama süreci bir bütün hâlinde değerlendirildiğinde işverenin yazışma içeriklerine A.A.Y.nin ve başvuruçunun rızası hilafına erişim sağladığı, A.A.Y. ile başvuruçunun arasında geçen yazışmalar dışında üçüncü kişilerle olan yazışmaların da incelendiği, ayrıca incelemeye dayanak gösterilen iddialarla sınırlı bir denetim yapılmayarak konu ile ilgili olup olmadığı belirsiz içeriklere de erişildiği ve bu içeriklerin de iş akdinin feshine dayanak yapıldığı görülmüştür. Dolayısıyla başvuruçunun kişisel verisi kapsamında olan e-postaları ile ilgili olarak trafik bilgisi ile yetinilmediği gibi içeriklerine de kapsamı belirsiz olacak şekilde erişildiği ve bunların kullanıldığı anlaşılmıştır.

79. Açıklanan gerekçelerle özel hukuk iş ilişkilerinden doğan uyuşmazlığı karara bağlayan derece mahkemeleri tarafından yukarıda belirtilen anayasal güvenceleri gözetilen özenli bir yargılama yapılarak pozitif yükümlülüklerin yerine getirilmediği anlaşıldığından başvuruçunun Anayasa'nın 20. maddesinde güvence altına alınan kişisel verilerin korunmasını isteme hakkı ile Anayasa'nın 22. maddesinde güvence altına alınan haberleşme hürriyetinin ihlal edildiğine karar verilmesi gerekir.

3. 6216 Sayılı Kanun'un 50. Maddesi Yönünden

80. 30/11/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 50. maddesinin ilgili kısmı şöyledir:

“(1) Esas inceleme sonunda, başvuru hakkının ihlal edildiğine ya da edilmediğine karar verilir. İhlal kararı verilmesi hâlinde ihlalin ve sonuçlarının ortadan kaldırılması için yapılması gerekenlere hükmedilir...

(2) Tespit edilen ihlal bir mahkeme kararından kaynaklanmışsa, ihlali ve sonuçlarını ortadan kaldırmak için yeniden yargılama yapmak üzere dosya ilgili mahkemeye gönderilir. Yeniden yargılama yapılmasında hukuki yarar bulunmayan hâllerde başvuru lehine tazminata hükmedilebilir veya genel mahkemelerde dava açılması yolu gösterilebilir. Yeniden yargılama yapmakla yükümlü mahkeme, Anayasa Mahkemesinin ihlal kararında açıkladığı ihlali ve sonuçlarını ortadan kaldıracak şekilde mümkünse dosya üzerinden karar verir.”

81. Başvuru, ihlalin tespit edilmesini istemiş; 10.000 TL manevi tazminat ve zararların giderilmesi talebinde bulunmuştur.

82. Anayasa Mahkemesinin Mehmet Doğan ([GK] B. No: 2014/8875, 7/6/2018) kararında ihlal sonucuna varıldığında ihlalin nasıl ortadan kaldırılacağı hususunda genel ilkeler belirlenmiştir. Anayasa Mahkemesi diğer bir kararında ise bu ilkelerle birlikte ihlal kararının yerine getirilmemesinin sonuçlarına da değinmiş ve bu durumun ihlalin devamı anlamına geleceği gibi ilgili hakkın ikinci kez ihlal edilmesiyle sonuçlanacağına işaret etmiştir (Aligül Alkaya ve diğerleri (2), B. No: 2016/12506, 7/11/2019).

83. Bireysel başvuru kapsamında bir temel hakkın ihlal edildiğine karar verildiği takdirde ihlalin ve sonuçlarının ortadan kaldırıldığından söz edilebilmesi için temel kural mümkün olduğunca eski hâle getirmenin yani ihlalden önceki duruma dönülmesinin sağlanmasıdır. Bunun için ise öncelikle ihlalin kaynağı belirlenerek devam eden ihlalin durdurulması, ihlale neden olan karar veya işlemin ve bunların yol açtığı sonuçların ortadan kaldırılması, varsa ihlalin sebep olduğu maddi ve manevi zararların giderilmesi, ayrıca bu bağlamda uygun görülen diğer tedbirlerin alınması gerekmektedir (Mehmet Doğan, §§ 55, 57).

84. İhlalin mahkeme kararından kaynaklandığı veya mahkemenin ihlali gideremediği durumlarda Anayasa Mahkemesi 6216 sayılı Kanun'un 50. maddesinin (2) numaralı fıkrası ile İçtüzük'ün 79. maddesinin (1) numaralı fıkrasının (a) bendi uyarınca, ihlalin ve sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmak üzere kararın bir örneğinin ilgili mahkemeye gönderilmesine hükmeder. Anılan yasal düzenleme, usul hukukundaki benzer hukuki kurumlardan farklı olarak ihlali ortadan kaldırmak amacıyla yeniden yargılama sonucunu doğuran ve bireysel başvuruya özgülünen bir giderim yolunu öngörmektedir. Bu nedenle Anayasa Mahkemesi tarafından ihlal kararına bağlı olarak yeniden yargılama kararı verildiğinde, usul hukukundaki yargılamanın

yenilenmesi kurumundan farklı olarak ilgili mahkemenin yeniden yargılama sebebinin varlığını kabul hususunda herhangi bir takdir yetkisi bulunmamaktadır. Dolayısıyla böyle bir kararın kendisine ulaştığı mahkemenin yasal yükümlülüğü, ilgilinin talebini beklemeksizin Anayasa Mahkemesinin ihlal kararı nedeniyle yeniden yargılama kararı vererek devam eden ihlalin sonuçlarını gidermek üzere gereken işlemleri yerine getirmektir (Mehmet Doğan, §§ 58, 59; Aligül Alkaya ve diğerleri (2), §§ 57-59, 66, 67).

85. İncelenen başvuruda kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyetiyle ilgili anayasal güvenceleri gözetilen bir yargılama yapılmaması nedeniyle anılan hak ve özgürlüğün ihlal edildiği sonucuna varılmıştır. Dolayısıyla ihlalin mahkeme kararından kaynaklandığı anlaşılmaktadır.

86. Bu durumda kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmasında hukuki yarar bulunmaktadır. Yapılacak yeniden yargılama ise bireysel başvuruya özgü düzenleme içeren 6216 sayılı Kanun'un 50. maddesinin (2) numaralı fıkrasına göre ihlalin ve sonuçlarının ortadan kaldırılmasına yöneliktir. Bu kapsamda yapılması gereken iş, yeniden yargılama kararı verilerek Anayasa Mahkemesini ihlal sonucuna ulaştıran nedenleri gideren, ihlal kararında belirtilen ilkelere uygun yeni bir karar verilmesinden ibarettir. Bu sebeple kararın bir örneğinin yeniden yargılama yapılmak üzere ilgili mahkemeye gönderilmesine karar verilmesi gerekmektedir.

87. Öte yandan somut olayda ihlalin tespit edilmesinin başvuruçunun uğradığı zararların giderilmesi bakımından yetersiz kalacağı açıktır. Dolayısıyla eski hâle getirme kuralı çerçevesinde ihlalin bütün sonuçlarıyla ortadan kaldırılabilmesi için kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ihlali nedeniyle yalnızca ihlal tespitiyle giderilemeyecek olan manevi zararları karşılığında başvuruçuya net 8.000 TL manevi tazminat ödenmesine, tazminata ilişkin diğer taleplerin reddine karar verilmesi gerekir.

88. Dosyadaki belgelerden tespit edilen 239,50 TL harç ve 3.000 TL vekâlet ücretinden oluşan toplam 3.239,50 TL yargılama giderinin başvuruçuya ödenmesine karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Başvuruçunun kamuya açık belgelerde kimlik bilgilerinin gizli tutulmasına ilişkin talebinin **KABULÜNE,**

- B.** Kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ihlal edildiğine ilişkin iddianın KABUL EDİLEBİLİR OLDUĞUNA,
- C.** Anayasa'nın 20. maddesinde güvence altına alınan kişisel verilerin korunmasını isteme hakkı ve Anayasa'nın 22. maddesinde güvence altına alınan haberleşme hürriyetinin İHLAL EDİLDİĞİNE,
- D.** Kararın bir örneğinin kişisel verilerin korunmasını isteme hakkı ile haberleşme hürriyetinin ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmak üzere İstanbul 8. İş Mahkemesine (E.2015/105, K.2015/566) GÖNDERİLMESİNE,
- E.** Başvurucuya net 8.000 TL manevi tazminat ÖDENMESİNE, tazminata ilişkin diğer taleplerin REDDİNE,
- F.** 239,50 TL harç ve 3.000 TL vekâlet ücretinden oluşan toplam 3.239,50 TL yargılama giderinin başvurucuya ÖDENMESİNE,
- G.** Ödemenin, kararın tebliğini takiben başvurucunun Hazine ve Maliye Bakanlığına başvuru tarihinden itibaren dört ay içinde yapılmasına, ödemede gecikme olması hâlinde bu sürenin sona erdiği tarihten ödeme tarihine kadar geçen süre için yasal FAİZ UYGULANMASINA,
- H.** Kararın bir örneğinin bilgi için Yargıtay 9. Hukuk Dairesine GÖNDERİLMESİNE,
- I.** Kararın bir örneğinin Adalet Bakanlığına GÖNDERİLMESİNE 17/9/2020 tarihinde OYBİRLİĞİYLE karar verildi.

Anayasa Mahkemesi - Arif Ali Cangı Kararı (2016/4060)

Arif Ali Cangı [GK], B. No: 2016/4060, 17/9/2020

Başvuru, yargılamanın uzun sürmesi nedeniyle makul sürede yargılanma hakkının, kişisel verinin idare tarafından üçüncü bir kişiye verilmesi nedeniyle de özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiği iddialarına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

GENEL KURUL

KARAR

ARİF ALİ CANGI BAŞVURUSU

(Başvuru Numarası: 2016/4060)

Karar Tarihi: 17/9/2020

R.G. Tarih ve Sayı: 14/10/2020-31274

GENEL KURUL

KARAR

Başkan:

Zühtü ARSLAN

Başkanvekili:

Hasan Tahsin GÖKCAN

Başkanvekili:

Kadir ÖZKAYA

Üyeler: Serdar ÖZGÜLDÜR, Burhan ÜSTÜN, Engin YILDIRIM, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĞLU, Selahaddin MENTEŞ, Basri BAĞCI

Raportör: Ali KOZAN

Başvurucu: Arif Ali CANGI

Vekili: Av. Nilgün TORTOP

I. BAŞVURUNUN KONUSU

1. Başvuru; yargılamanın uzun sürmesi nedeniyle makul sürede yargılanma hakkının, kişisel verinin idare tarafından üçüncü bir kişiye verilmesi nedeniyle de özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiği iddialarına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 24/2/2016 tarihinde yapılmıştır.

3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.

4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.

5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.

6. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık görüş bildirmemiştir.

7. İkinci Bölüm tarafından 27/11/2019 tarihinde yapılan toplantıda, niteliği itibarıyla başvurunun Genel Kurul tarafından karara bağlanması gerekli görüldüğünden Anayasa Mahkemesi İçtüzüğü'nün (İçtüzük) 28. maddesinin (3) numaralı fıkrası uyarınca Genel Kurula sevkine karar verilmiştir.

III. OLAY VE OLGULAR

8. Başvuru formu ve eklerinde ifade edildiği şekliyle olaylar özetle şöyledir:

A. Uyuşmazlığın Arka Planı

9. İzmir Barosuna kayıtlı olarak avukatlık görevini ifa eden başvurucu, kendi beyanına göre ağırlıklı olarak çevre hukuku ile ilgili davaları üstlenmekte; çevrenin ve kültürel değerlerin korunması için çalışmalar yapan Ege Çevre ve Kültür Platformu (EGEÇEP) isimli derneğin de başvuru konusu olay tarihinde sözcülüğünü yapmaktadır. Bergama Altın Madeni'nin de içinde bulunduğu alana ilişkin imar planının iptali istemiyle açılan davada başvurucu, davacı sıfatıyla taraftır. Bölgede altın çıkarma faaliyetinde bulunan ve anılan davaya müdahil olan Koza Altın İşletmeleri Anonim Şirketinin (Şirket)

avukatı İçişleri Bakanlığına 24/7/2006 tarihinde başvurarak 7/4/1969 tarihli ve 1136 sayılı Avukatlık Kanunu ile 24/10/2003 tarihli ve 4632 sayılı Bilgi Edinme Kanunu kapsamında yargısal süreçte kullanılmak üzere bilgi talebinde bulunmuştur. Başvuruda, Alman Vakıfları olarak bilinen kuruluşlar ile bazı kişilerin Bergama Ovacık Altın Madeni aleyhinde faaliyette bulunup bulunmadığı hususu sorulmuş; faaliyette bulunuyorlar ise bu kuruluşlar ile ilgili kişiler hakkındaki bilgi ve belgelerin verilmesi talep edilmiştir.

10. Bilgi talebinde bulunan avukatın vekilliğini yaptığı şirketin Koza İpek Grubu bünyesinde bir şirket olduğu görülmüştür. Koza İpek Grubu temel olarak İpek ailesinin en az bir ferdinin ortak olduğu veya yönetimi kontrolü altında bulundurduğu -2015 yılı sonu itibarıyla- yirmi sermaye şirketini, bir vakfı ve vakfa bağlı bir özel üniversiteyi ifade etmektedir. Koza İpek Grubu içinde yer alan şirketlerin ortaklık yapıları incelendiğinde holding yapılanmasına uygun olarak hâkim şirketin bağlı şirketlere iştirak etmesi yoluyla bir yapının oluşturulduğu ve bu yapı içinde yer alan şirketlerin altın madenciliğinden enerji, gıda, medya, bilişim, sigorta, tedarik, turizm, seyahat sektörüne kadar pek çok farklı alanda faaliyet gösterdiği anlaşılmaktadır. Ankara 5. Sulh Ceza Hâkimliği tarafından 26/10/2015 tarihinde ilgili Cumhuriyet başsavcılığının talebi üzerine şirketlerin Fetullahçı Terör Örgütü/Paralel Devlet Yapılanmasının (FETÖ/PDY) faaliyetleri kapsamında ve faaliyetlerine destek olacak şekilde kullanıldığı gerekçesiyle, Koza Grubuna ait şirketlere kayyum atanmıştır (Hamdi Akın İpek, B. No: 2015/17763, 24/5/2018, §§ 16-24).

11. İçişleri Bakanlığının şirket vekili avukatın talebine karşılık verdiği 10/8/2006 tarihli cevap şöyledir: "1136 sayılı Avukatlık ile 4982 sayılı Bilgi Edinme Hakkı kanunu kapsamında; Ülkemizde faaliyet gösteren ve genel olarak Alman Vakıfları olarak bilinen kuruluşlar ile bu kuruluşların ve bazı kişilerin Bergama Ovacık Altın Madeni aleyhinde faaliyette bulunup bulunmadıkları, faaliyette bulunuyorlar ise bu kuruluşlarla ilgili kişiler hakkında kayıtlarımızda bulunan bilgi ve belgelerin, yargı sürecinde kullanılmak üzere tarafınıza verilmesini içeren ilgili kayıtlı dilekçeniz incelenmiştir.

Bakanlığımıza daha önce de konu ile ilgili daha çeşitli iddialar intikal etmiş olup, bu iddialar üzerine Bakanlığımızca ilgili Teşkilatlar nezdinde yaptırılan inceleme neticesinde; Ovacık Beldesindeki altın madenin çıkarılmasını engellemeye yönelik tüm eylemleri [B.L.nin] organize ettiği, eylemlere şahısların katılması için her türlü maddi desteği sağladığı, Arif Ali CANGI, [O.K.], [C.N.], [E.İ.G.], [S.G.], [Ö.D.], [V.A.], isimli şahıslar ile irtibat içerisinde olduğu, bu şahısların özellikle kamuoyu oluşturmak için [B.L.ye] ait otelde kaldıkları tespit edilmiştir. Ayrıca dilekçede adı geçen şahıslardan [B.L.nin] Alman Yeşiller Partisinin kurucularından olup Ülkemizde, Uluslararası İnsan Hakları Örgütü (FLAN) adına faaliyet gösterdiği, FLAN'ın 1986'da kurulduğu, dilekçede adı geçen bazı

şahıslarla ilgili olarak çeşitli suçlardan işlem yapılarak adli makamlara tevdi edildikleri anlaşılmıştır. Konuya ilişkin bazı kamu görevlileri ile ilgili iddialar gereği için Adalet Bakanlığı'na intikal ettirilmiştir. Bilgilerinize rica ederim."

12. Başvurucu, Bugün gazetesinin 22/7/2006 tarihli nüshasında yayımlanan "Altın Yumurtlayan Köşe Yazarı Clup Orient'den Yazıyor" başlıklı yazısı nedeniyle köşe yazarına yönelik suç duyurusunda bulunmuştur. Köşe yazarı, İçişleri Bakanlığının şirket vekiline verdiği cevap yazısını Şişli Cumhuriyet Başsavcılığının ilgili soruşturma dosyasına ibraz etmiştir.

13. Bugün gazetesinin 22/7/2006 tarihli nüshasının beşinci sayfasında yayımlanan köşe yazısında Cumhuriyet gazetesi yazarı H.Ç.nin Fethullah Gülen ve Bergama Ovacık Altın Madenleriyle ilgili çalışmalarından dolayı takıntılarının olduğunu belirtildiği, devamında "Türkiye'den bir Türkten yana değil bir Almandan yana davranıyor. Alman ajanlığı ile yargılanmış kişilerin Ovacık'ta altının çıkartılmaması için yaptıkları çabaları övüyor. AKP'nin Türkiye'deki madenleri çıkartması ve bunu milli servete katması için yaptığı çabayı Türkiye'nin aleyhine bir faaliyetmiş gibi sunmaya çalışıyor....Yaa [H.Ç.] kimden yana olduğunu açıkla da biz de bilelim. Şimdi yazıda bahsettiğim Ovacık Altın Madeni işletilmesini engellemeye çalışan kişileri ele alalım." denildikten sonra "Ali Arif Cangı, [O.K.] gibi devlet aleyhine çete kurmak suçlamasıyla yargılanmış, fakat yabancı bir ülkenin dışişleri bakanının zamanın Türk dışişleri bakanını ziyaretinden sonra dava dosyaları delil yetersizliğinden kapatılmış olan şahıslar..." şeklinde ifadelere yer verildiği görülmektedir. Buna göre söz konusu yazıda doğrudan doğruya başvurusunun adına yer verilerek hakkındaki bir ceza soruşturması olduğundan ve bu soruşturmanın akıbetinden söz edilmektedir.

14. Başvurucu, soruşturma dosyasına ibraz edilen İçişleri Bakanlığının cevap yazısına dayanarak 14/5/2007 ve 6/7/2007 tarihlerinde İçişleri Bakanlığına bilgi edinme hakkı kapsamında başvurmuştur. Anılan başvurularda başvuru özetle Alman Vakıfları olarak bilinen vakıfların faaliyetleri, bu vakıflarla bağlantısı tespit edilen kişiler arasında yer alıp almadığı hususları ile kendisiyle ilgili yürütülen incelemeye ilişkin bilgi verilmesini talep etmiştir. İçişleri Bakanlığı 14/6/2007 ve 3/8/2007 tarihli cevap yazılarında özetle Alman Vakıfları olarak adlandırılan bir vakfa İçişleri Bakanlığı kayıtlarında rastlanmadığı, başvuru hakkında İçişleri Bakanlığı nezdinde yürütülen bir incelemenin de mevcut olmadığı bildirilmiştir.

B. Tam Yargı Davası Süreci

15. Başvurucu, İçişleri Bakanlığı tarafından şirket vekiline verilen cevapta kendisi hakkında gerçeği yansıtmayan bilgi ve tespitlerin bulunduğu, yazının üçüncü kişilere verilmesi nedeniyle kişilik haklarının zedelendiği iddialarıyla manevi tazminat ödenmesi talebinde bulunmuştur. Bu talebin

İçişleri Bakanlığı tarafından reddedilmesi üzerine 17/12/2007 tarihinde Ankara 7. İdare Mahkemesi nezdinde tam yargı davası açmıştır. Dava dilekçesinde başvuru; şirket vekiline idare tarafından verilen yazıda kendisi hakkında "Alman vakıfları ile ilgili", "Bergama Ovacık beldesindeki altın madeni çıkarılmasını önlemeye yönelik eylemlere katılan, bu konuda eylemleri organize eden kişilerle irtibat içinde olan", "kamuoyu oluşturmak amacıyla [B.L.nin] otelinde kalan", "çeşitli suçlardan işlem yapılarak adli makamlara tevdi edilen kişi" şeklinde gerçeğe aykırı ifadelerin yer aldığını, bu tespitlerin kayıtlara işlendiğini ve üçüncü kişilere verildiğini belirtmiştir. İdarenin hukuka aykırı eylemleri sonucu ulaştığı gerçek dışı tespitlerin üçüncü kişilere ve kamuoyuna yansması nedeniyle ön yargıları silmek için çaba göstermek zorunda kaldığını, onur, saygınlık, mesleki kariyer vb. kişilik haklarının ciddi şekilde zedelendiğini ifade etmiştir.

16. İdarenin davaya cevabında; ilgili yazının şirket vekilinin başvurusu üzerine 1136 sayılı Kanun ile 4632 sayılı Kanun kapsamında verildiği, talep edilen konularla ilgili ayrıntılara girilmediği, yazının genel bilgiler içerdiği belirtilmiştir. Ayrıca şahısların özel hayatının gizliliğinin korunması adına gerekli dikkat ve özenin gösterilerek bir cürüm atfında bulunulmamasına dikkat edildiği vurgulanmıştır.

17. Mahkeme 26/12/2008 tarihinde davanın reddine karar vermiştir. Kararın gerekçesinde; şirket vekili tarafından 1136 sayılı Kanun ve 4632 sayılı Kanun kapsamında şirketin haklarının savunulması amacıyla altın madeni aleyhine faaliyette bulunan, Alman Vakıfları olarak bilinen kuruluşlar ile kişiler hakkında bilgi ve belgeler talep edildiği, bu başvurudan daha önce gelen bir ihbar mektubunda belirtilen, başvurucağının da yer aldığı bazı şahıslar ile ilgili iddialar nedeniyle İzmir Emniyet Müdürlüğü tarafından suçların önlenmesi kapsamında yapılan inceleme ile elde edilen tespitlerin talep edene verildiği belirtilmiştir. Başvurucağının serbest avukatlık yaptığı, altın madeni işletmesi için kamu kurumlarınca tesis edilen işlemlere karşı açılan davalarda, çevrenin ve çevre sağlığının korunmasının sağlanması, yargı kararlarının yerine getirilmesinin takibi gibi iddialarla davacı veya davacı vekili sıfatıyla taraf olduğu ve kamuoyu oluşturulmasına yönelik faaliyetlerde bulunduğunun bilindiği vurgulanmıştır. Dava konusu yazı içeriğinde de başvurucağı yönünden kamuoyu tarafından da bilinen süreç dışında bir bilginin yer almadığı belirtilmiştir. Ayrıca anılan yazıdaki "Dilekçede yer alan bazı şahıslarla ilgili olarak çeşitli suçlardan işlem yapılarak adli makamlara tevdi edildikleri anlaşılmıştır." şeklindeki ibarenin genel nitelikli bir ifadeyi içerdiği, başvurucağının isminin belirtilerek bu kapsamda olduğuna dair bir bilginin yer almadığı ve başvurucağının suçluymuş gibi algılanmasına yol açabilecek bir ifadeye yer verilmediği vurgulanmıştır.

18. Anılan karar, Danıştay Onuncu Dairesinin 31/10/2013 tarihli kararıyla usul ve hukuka uygun olduğu gerekçesiyle onanmıştır. Başvurucunun karar düzeltme talebi de aynı Dairenin 22/12/2015 tarihli kararıyla reddedilmiştir.

19. Nihai karar başvurucuya 25/1/2016 tarihinde tebliğ edilmiştir.

20. Başvurucu 24/2/2016 tarihinde bireysel başvuruda bulunmuştur.

IV. İLGİLİ HUKUK

A. Ulusal Hukuk

21. 1136 sayılı Kanun'un "Avukatlığın mahiyeti" kenar başlıklı 1. maddesi şöyledir:

"Avukatlık, kamu hizmeti ve serbest bir meslektir.

Avukat, yargının kurucu unsurlarından olan bağımsız savunmayı serbestçe temsil eder."

22. 1136 sayılı Kanun'un "Avukatlığın amacı" kenar başlıklı 2. maddesi şöyledir:

"Avukatlığın amacı; hukuki münasebetlerin düzenlenmesini, her türlü hukuki mesele ve anlaşmazlıkların adalet ve hakkaniyete uygun olarak çözümlenmesini ve hukuk kurallarının tam olarak uygulanmasını her derecede yargı organları, hakemler, resmi ve özel kişi, kurul ve kurumlar nezdinde sağlamaktır.

Avukat bu amaçla hukuki bilgi ve tecrübelerini adalet hizmetine ve kişilerin yararlanmasına tahsis eder.

Yargı organları, emniyet makamları, diğer kamu kurum ve kuruluşları ile kamu iktisadi teşebbüsleri, özel ve kamuya ait bankalar, noterler, sigorta şirketleri ve vakıflar avukatlara görevlerinin yerine getirilmesinde yardımcı olmak zorundadır. Kanunlarındaki özel hükümler saklı kalmak kaydıyla, bu kurumlar avukatın gerek duyduğu bilgi ve belgeleri incelemesine sunmakla yükümlüdür. Bu belgelerden örnek alınması vekaletname ibrazına bağlıdır. Derdest davalarda müzekereler duruşma günü beklenmeksizin mahkemeden alınabilir."

23. 4982 sayılı Kanun'un "Bilgi edinme hakkı" kenar başlıklı 4. maddesinin ilgili kısmı şöyledir:

"Herkes bilgi edinme hakkına sahiptir."

24. 4982 sayılı Kanun'un "Bilgi verme yükümlülüğü" kenar başlıklı 5. maddesinin ilgili kısmı şöyledir:

"Kurum ve kuruluşlar, bu Kanunda yer alan istisnalar dışındaki her türlü bilgi veya belgeyi başvuranların yararlanmasına sunmak ve bilgi edinme başvurularını etkin, süratli ve doğru sonuçlandırmak üzere, gerekli idari ve teknik tedbirleri almakla yükümlüdürler."

25. 4982 sayılı Kanun'un "İstenilecek bilgi veya belgenin niteliği" kenar başlıklı 7. maddesi şöyledir:
"Bilgi edinme başvurusu, başvuru kurum ve kuruluşların ellerinde bulunan veya görevleri gereği bulunması gereken bilgi veya belgelere ilişkin olmalıdır.

Kurum ve kuruluşlar, ayrı veya özel bir çalışma, araştırma, inceleme ya da analiz neticesinde oluşturulabilecek türden bir bilgi veya belge için yapılacak başvurulara olumsuz cevap verebilirler.

İstenen bilgi veya belge, başvuru kurum ve kuruluştan başka bir yerde bulunuyorsa, başvuru dilekçesi bu kurum ve kuruluşa gönderilir ve durum ilgiliye yazılı olarak bildirilir."

26. 4982 sayılı Kanun'un "Başvuruların cevaplandırılması" kenar başlıklı 12. maddesi şöyledir:

"Kurum ve kuruluşlar, bilgi edinme başvurularıyla ilgili cevaplarını yazılı olarak veya elektronik ortamda başvuru sahibine bildirirler. Başvurunun reddedilmesi halinde bu kararın gerekçesi ve buna karşı başvuru yolları belirtilir."

27. 4982 sayılı Kanun'un "Özel hayatın gizliliği" kenar başlıklı 21. maddesi şöyledir:

"Kişinin izin verdiği haller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması halinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, mesleki ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır.

Kamu yararının gerektirdiği hallerde, kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir."

28. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Amaç" kenar başlıklı 1. maddesinin ilgili kısmı şöyledir:

"Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir."

29. 6698 sayılı Kanun'un "Kapsam" kenar başlıklı 2. maddesi şöyledir:

"Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır."

30. 6698 sayılı Kanun'un "Tanımlar" kenar başlıklı 3. maddesinin ilgili kısmı şöyledir:

" (1) Bu Kanunun uygulanmasında;

a) Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,

...

- d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
- e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,"

31. 6698 sayılı Kanun'un "Kişisel verilerin işleme şartları" kenar başlıklı 5. maddesi şöyledir:

" (1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması."

32. 6698 sayılı Kanun'un "İlgili kişinin hakları" kenar başlıklı 11. maddesi şöyledir:

"(1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

a) Kişisel veri işlenip işlenmediğini öğrenme,

b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

c) Kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,

ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

- d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
- e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
- f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir."

33. 12/10/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun "Verileri hukuka aykırı olarak verme veya ele geçirme" kenar başlıklı 136. maddesi şöyledir:

"(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır."

34. 6/1/1982 tarihli ve 2577 sayılı İdari Yargılama Usulü Kanunu'nun "İptal ve tam yargı davaları" kenar başlıklı 12. maddesinin ilgili kısmı şöyledir:

"İlgililer haklarını ihlal eden bir idari işlem dolayısıyla Danıştaya ve idare ve vergi mahkemelerine doğrudan doğruya tam yargı davası veya iptal ve tam yargı davalarını birlikte açabilecekleri gibi ilk önce iptal davası açarak bu davanın karara bağlanması üzerine, bu husustaki kararın veya kanun yollarına başvurulması halinde verilecek kararın tebliği veya bir işlemin icrası sebebiyle doğan zararlardan dolayı icra tarihinden itibaren dava süresi içinde tam yargı davası açabilirler..."

B. Uluslararası Hukuk

1. Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi

35. Birleşmiş Milletler Genel Kurulunun 10/12/1948 tarihli ve 217 (111) sayılı kararı ile kabul edilen İnsan Hakları Evrensel Beyannamesi'nin 12. maddesi şöyledir:

"Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfî karışmalara, şeref ve şöhretine karşı tecavüzlere mâruz kalmaz. Herkesin bu karışmalara ve tecavüzlere karşı kanun ile korunmağa hakkı vardır."

36. Birleşmiş Milletler Genel Kurulu tarafından kişisel verilerin korunması konusunda kabul edilen 14/12/1990 tarihli ve 45/95 sayılı “Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler”de şu temel ilkelere yer verilmiştir:

1- İşlemenin hukuka uygun ve adil olması ilkesi: Kişilerin hakkındaki veriler hukuka aykırı veya adil olmayan şekilde toplanmamalı veya işlenmemelidir. Ayrıca Birleşmiş Milletler Şartı’ndaki ilkelere aykırı amaçlarla kullanılmamalıdır.

2- Doğruluk ilkesi: Kişisel verileri tutmakla sorumlu makamlar bu bilgilerin doğru tutulmasını güvence altına almalıdır.

3- Belirli ve meşru amaçlar için işleme ilkesi: Bir kaydın tutulması ve kullanımı meşru ve belirli bir amaca dayalı olmalıdır. Bütün kişisel veriler amaç ile ilgili ve onu gerçekleştirmeye elverişli olacak şekilde toplanmalı ve kaydedilmelidir. Bu kişisel verilerin hiçbiri, ilgili kişinin rızası dışında, belirtilenlerle uyuşmayan amaçlar için kullanılamaz veya ifşa edilemez. Kişisel verilen saklanma süresi, belirtilen amaçlara ulaşılmasını sağlayacak süreyi aşamaz.

4- İlgili kişilerin erişmesi ilkesi: Kimlik kanıtı sunan herkes kendisiyle ilgili bilgilerin işlenip işlenmediğini bilme ve gereksiz bir gecikme veya masraf olmadan anlaşılır biçimde elde etme hakkına sahiptir. Ayrıca bu bilgilerin kanuna aykırı, gereksiz veya yanlış olması durumunda uygun düzeltmelerin yapılmasını veya silinmesini talep etme hakkına sahiptir. Devletler buna uygun bir çözüm yolu sağlamak durumundadır. Herhangi bir düzeltme maliyeti dosyadan sorumlu kişi tarafından karşılanmalıdır. Bu ilke hükümlerinin uyruk veya ikâmetine bakılmaksızın herkes için uygulanması arzu edilir.

5- Ayrımcılığın önlenmesi ilkesi: (6) numaralı ilkede kısıtlı olarak öngörülen hâller söz konusu olduğunda ırk veya etnik köken, renk, cinsel yaşam, siyasi görüş, dini, felsefi ve diğer inançların yanı sıra dernek veya sendika üyeliği bilgileri de dahil olmak üzere kanuna aykırı veya keyfî olarak ayrımcılığa yol açabilmesi muhtemel veriler toplanmamalıdır.

6- Üstün amaçlar için istisna koyabilme ilkesi: Ulusal güvenlik, genel sağlık ve ahlaki korumak veya özellikle zulüm gören kişilerin ve diğerlerinin hak ve özgürlüklerinin korunması amacıyla (1) ila (4) numaralı ilkelerden ayrılabilmek mümkün olabilir. Ancak bu tür istisnalar, sınırlarının açıkça belirlendiği ve uygun tedbirlerin ortaya konulduğu iç hukuk sistemine göre yürürlüğe konan bir kanun veya eşdeğer bir düzenlemede açıkça belirtilmiş olmalıdır.

7- Güvenlik ilkesi: Veri dosyaları, kaza ile kaybetme veya yok etme gibi doğal afetler, hileli verilerin yanlış kullanılması ya da bilgisayar virüsleri gibi insan odaklı tehlikelere karşı uygun tedbirlerle korunmalıdır.

8- Denetleme ve yaptırım ilkesi: Her ülkenin kanunu, yerel hukuk sistemine uygun olarak yukarıda belirtilen ilkelere uyulmasından sorumlu makamı belirler. Bu makam tarafsızlık, veri işleme ve oluşturmada sorumlu kişilere karşı bağımsızlık ve teknik yeterlilik teminatı sunmalıdır. Yukarıda belirtilen ilkeleri uygulayan ulusal kanun hükümlerinin ihlali durumunda cezai veya diğer idari yaptırımlar uygun bireysel çözümlerle birlikte öngörülmüş olmalıdır.

9- Sınır ötesi veri transferi ilkesi: Sınır ötesi bir veri akışı ile ilgili olarak iki veya daha fazla ülkenin mevzuatı mahremiyetin korunması için karşılaştırılabilir güvenceler sunduğu takdirde veri dolaşımı mümkün kılınabilir."

2. Avrupa Birliği Genel Veri Koruma Tüzüğü

37. 27/4/2016 tarihli ve 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nün "Tanımlar" kenar başlıklı 4. maddesinin ilgili kısmı şöyledir:

"Bu Tüzük'ün amaçları doğrultusunda, aşağıdaki tanımlar geçerlidir:

Kişisel veri, belirli veya belirlenebilir bir gerçek kişi hakkındaki her bilgiyi ifade eder (veri sahibi); belirlenebilir bir gerçek kişi ad, kimlik, yer bilgisi, online kimlik veya kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel ya da sosyal kimliği gibi belirleyici bir özelliklerle doğrudan veya dolaylı olarak belirlenebilen kişidir.

İşleme, kişisel veri veya kişisel veri dizisinin otomatik veya başka bir şekilde toplanması, kaydedilmesi, organize edilmesi, yapılandırılması, depolanması, uyarlanması veya değiştirilmesi, geri alınması, kullanılması, iletim yoluyla açıklanması, yayılması veya erişilebilir hâle getirilmesi, sıralanması veya kombine edilmesi, sınırlandırılması, silinmesi veya yok edilmesi gibi yollarla herhangi bir işlem veya işlem dizisine tabi tutulması anlamına gelir."

38. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün "Kişisel verilerin işlenmesi ile ilgili ilkeler" kenar başlıklı 5. maddesinin ilgili kısmı şöyledir:

"Kişisel veri;

Veri sahibi ile ilgili olarak hukuka uygun, adil ve şeffaf bir biçimde işlenmelidir (hukuka uygunluk, adillik ve şeffaflık),

Belirlenmiş, açık ve meşru amaçlar için toplanmış olmalı ve bu amaçlara uygun olmayan bir şekilde işlenmemelidir. Kamu yararı, bilimsel ve tarihsel amaçlar ya da arşivleme amacıyla yapılacak diğer işlemler madde 89/1 uyarınca başlangıç amaçlarıyla uyumsuz kabul edilmeyecektir (amaç sınırlaması)

Yeterli, ilgili ve işlendiği amaçlar için gerekli olanlarla sınırlı işlenmelidir (verilerin en az seviyeye indirilmesi)

Doğru ve gerektiğinde güncel tutulmalı; hatalı olan kişisel verinin işleme amacına bakılmaksızın gecikmeden silinmesini veya düzeltilmesini sağlamak için makul her adım atılmalıdır (doğruluk).

İşleme amacı için gerekenden daha uzun olmayan bir süre boyunca veri konularının tanımlanmasına izin veren bir formda tutulmalıdır. Kişisel veriler, veri sahibinin hak ve özgürlüklerini korumak için bu Tüzüğün öngördüğü uygun teknik ve yapısal tedbirler alınmak kaydıyla Tüzüğün 89/1. maddesi uyarınca sadece kamu yararına, bilimsel veya tarihi araştırma amaçlarına ya da istatistiki amaçlara yönelik olarak arşivleme amacıyla daha uzun bir süre saklanabilir (saklama süresinin sınırlandırılması).

Yetkisiz veya kanun dışı işlemeye ve kazara kayıp, imha ve hasara karşı uygun teknik veya yapısal tedbirler alınarak kişisel verilerin güvenli bir biçimde işlenmesi sağlanmalıdır (bütünlük ve gizlilik)."

39. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün "Kısıtlamalar" kenar başlıklı 23. maddesinin ilgili kısmı şöyledir:

"Veri sorumlusunun veya işleyeninin tabi olduğu Birlik veya Üye Devlet hukuku, 12. ila 22. (bunlara karşılık geldiği sürece 5. madde) ve 34. maddelerdeki yükümlülükleri ve hakların kapsamını, temel hak ve özgürlüklerin özüne saygı gösterdiğinde ve demokratik bir toplumda korunmak için gerekli ve orantılı bir tedbir olduğu takdirde aşağıdaki hâllerde kanun yoluyla sınırlayabilir:

Ulusal güvenlik,

Savunma,

Kamu güvenliği,

Kamu güvenliğine yönelik tehditlerin önlenmesi de dahil olmak üzere suçların önlenmesi, soruşturulması, tespit edilmesi, kovuşturulması veya cezaların infazı,

Birliğin veya Üye Devletin genel olarak kamu yararına olan diğer önemli hedeflerin, özellikle para, bütçe, önemli bir vergilendirme, kamu sağlığı veya sosyal güvenlik dahil olmak üzere önemli bir ekonomik veya mali çıkar amacıyla,

Yargı bağımsızlığının ve yargısal işlemlerin (sürecin) korunması,

Regüle edilmiş meslekler için etik ihlallerin önlenmesi, tespiti, soruşturulması ve kovuşturulması,

(a) ila (e) ve (g) maddelerinde atıfta bulunulan hallerde resmi otoritenin kullanımına zaman zaman bağlı olsa bile izleme, inceleme veya düzenleyici işlevin yerine getirilmesi,

Veri sahibinin veya başkalarının hak ve özgürlüklerinin korunması,

Medeni hukuk hak ve alacaklarının icrası,

Özellikle 1. paragrafta atıfta bulunulan herhangi bir hukuki tedbir öngören kanun en azından uygun olduğu hâllerde şu belirli hükümleri içermelidir:

İşleme veya işleme kategorilerinin amaçları,

Kişisel veri kategorileri,

Tanınan kısıtlamaların boyutu,

Keyfi veya hukuk dışı erişimin ya da aktarımın önlenmesine dair güvenceler,

Sorumlunun veya sorumlu kategorilerinin belirlenmesi,

Depolama dönemleri ve işlemenin niteliği, kapsamı ve amaçları veya işleme kategorileri dikkate alınarak uygulanabilir güvenceler,

Veri sahibinin hakları ve özgürlüklerine getirilen riskler,

Veri sahibinin, amacına hâle getirmediği sürece kısıtlama hakkında bilgilendirilmesi."

3. Avrupa İnsan Hakları Sözleşmesi

40. Avrupa İnsan Hakları Sözleşmesi'nin (Sözleşme) "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesi şöyledir:

“(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.”

4. Avrupa Konseyi Siber Suç Sözleşmesi

41. Türkiye Cumhuriyeti tarafından 10/11/2010 tarihinde imzalanan ve Türkiye Büyük Millet Meclisi tarafından onaylanması uygun bulunarak 2/5/2014 tarihinde yürürlüğe giren Avrupa Konseyi Siber

Suç Sözleşmesi'nin "Depolanmış bilgisayar verilerine izinli şekilde veya bu verilerin halka açık olduğu durumlarda sınır ötesinden erişim sağlanması" kenar başlıklı 32. maddesi şöyledir:

"Bir taraf, diğer tarafın izni olmaksızın; a) Halkın serbest kullanımına sunulan (açık kaynaktan gelen) depolanmış bilgisayar verilerine bunların coğrafi konumuna bakılmaksızın erişilebilir; veya b) Kendi ülkesindeki bir bilgisayar sistemi aracılığıyla, diğer tarafın ülkesindeki depolanmış bilgisayar verilerine, eğer bu taraf, söz konusu bilgisayar sistemi aracılığıyla veriyi ifşa etme yetkisini yasal olarak haiz bulunan kişinin yasal ve gönüllü onayını sağlayabilirse, söz konusu verilere erişebilir veya bunları temin edebilir."

5. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

42. 18/2/2016 tarihli ve 29628 sayılı Resmî Gazete'de yayımlanan 30/1/2016 tarihli ve 6669 sayılı Kanun'la uygun bulunan 28/1/1981 tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "Tanımlar" kenar başlıklı 2. maddesinin ilgili kısmı şöyledir:

"Bu Sözleşmenin amaçları bakımından:

a "Kişisel veriler": Kimliği belirli veya belirlenebilir bir gerçek kişi ("ilgili kişi") hakkındaki tüm bilgileri ifade eder.

...

c "Otomatik işlem" den, tamamen veya kısmen otomatik yöntemlerle gerçekleştirilen; verilerin kaydı, bu verilere mantıksal ve/ veya aritmetik işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya dağıtılması anlaşılır."

43. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "Verilerin niteliği" kenar başlıklı 5. maddesi şöyledir:

"Otomatik işleme konu olan kişisel veriler:

- a. Adil biçimde ve yasal yoldan elde edilir ve işlenir;
- b. Belli ve meşru amaçlar için kaydedilir ve bu amaçlara aykırı şekilde kullanılmaz;
- c. Kaydedilme amaçlarına göre uygun ve yerinde olur ve aşırı olmaz;
- d. Doğru bilgileri yansıtır ve gerektiğinde güncellenir;
- e. Kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkan veren bir biçimde saklanır."

44. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "İstisnalar ve kısıtlamalar" kenar başlıklı 9. maddesinin ilgili kısmı şöyledir:

"2. Taraf devletin kanunlarında öngörülmüş olması ve demokratik bir toplumda aşağıdaki hususların sağlanması için gerekli bir önlem oluşturması halinde işbu Sözleşmenin 5, 6 ve 8. maddelerine istisna getirilebilir:

a. Devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi;

b. İlgili kişinin veya başkasının hak ve özgürlüklerinin korunması."

6. Avrupa İnsan Hakları Mahkemesi İçtihadı

45. Avrupa İnsan Hakları Mahkemesi (AİHM) devletlerin millî güvenliğin korunması amacını gerçekleştirmede sahip oldukları takdir yetkisinin geniş olduğunu kabul etmektedir. AİHM, Sözleşme'ye taraf devletlerin millî güvenliği korumak için yetkili ulusal makamlarına ilk olarak kişiler hakkında bilgi toplama ve halka açık olmayan siciller tutma, ikinci olarak millî güvenlik bakımından önemli kadrolarda çalışmak isteyen adayların bu işe uygunluğunu takdir ederken bu bilgiyi kullanma yetkisi veren kurallara sahip olmaları gerektiğinde kuşku bulunmadığını belirtmektedir (Leander/İsveç, B. No: 9248/81, 26/3/1987, § 59).

46. Bununla birlikte AİHM içtihadına göre kamu mercilerinin bir bireyin özel hayatıyla ilgili bilgileri toplaması, kaydetmesi, saklaması özel hayata saygı hakkına müdahale oluşturur (Leander/İsviçre, § 48; Kopp/İsviçre, B. No: 23224/94, 25/3/1998, § 53; Amann/İsviçre [BD], B. No: 27798/95, 16/2/2000, § 69; Rotaru/Romanya [BD], B. No: 28341/95, 4/5/2000, §§ 43, 44, 46).

47. AİHM'e göre bir kişinin özel yaşamına ilişkin verilerin kaydedilmesi ve saklanması kendi başına özel hayata saygı hakkı bakımından bir müdahale oluşturmaktadır. Bu müdahalenin tespiti için kaydedilen bilgilerin daha sonra kullanılmış olması gibi bir koşul da aranmamaktadır. Bununla birlikte kamu makamları tarafından muhafaza edilen kişisel verilerin Sözleşme'nin 8. maddesinde öngörülen unsurlardan birini devreye sokup sokmadığını tespit etmek için bu bilgilerin hangi çerçevede alındığının ve muhafaza edildiğinin, verilerin türünün, kullanıldıkları ve işlendikleri şeklin, bunlardan çıkarılabilecek sonuçların dikkate alınması zaruridir (S. ve Marper/Birleşik Krallık [BD], B. No: 30562/04, 30566/04, 4/12/2008, § 67).

48. AİHM'e göre kişisel verilerin korunmasının Sözleşme'nin 8. maddesinde öngörülen özel hayata saygı hakkından kişinin yararlanması konusunda büyük önemi vardır. İç hukuk kişisel verilerin bu maddede öngörülen güvencelere uygun olmayan şekilde kullanımını engellemek için gerekli

güvenceleri sağlamalıdır. Bu tür güvencelerin bulunmasının gerekliliği; otomatik işleme tabi tutulan kişisel verilerin korunması söz konusu olduğunda, özellikle de bu verilerin polis tarafından kullanılması hâlinde daha fazla hissedilmektedir. İç hukuk, bu verilerin saklanma amaçlarına uygun ve aşırıktan uzak olmalarını sağlamalı ve verilerin kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde muhafaza edilmesini temin etmelidir. İç hukuk aynı zamanda kişisel verilerin uygun olmayan şekilde, keyfî ve yetki aşımı yapılarak kullanılmasına karşı uygun güvenceler de içermelidir (S. ve Marper/Birleşik Krallık, § 103; M.M./Birleşik Krallık, B. No: 24029/07, 13/11/2012, § 195).

49. Ayrıca AİHM, kişilerin suç kayıtlarının tutulması ve kullanılması hakkında konuyu düzenleyen ilgili kanunun niteliğine ayrı bir önem vermektedir. AİHM, suç kayıtlarının tutulması ve kullanılmasına dair kanunun niteliği bakımından -aynı telefon dinlemelerinde, gizli takipte ve gizli istihbarat toplamada dayanılan kanunlar yönünden olduğu gibi- keyfî müdahalelere karşı bireyi korumak amacıyla yüksek bir standart aramaktadır. AİHM'e göre suç kayıtlarının tutulması ve kullanılmasına dair kanun -telefon dinlemelerinde, gizli takipte, gizli istihbarat toplamada olduğu gibi- tedbirlerin kapsamını ve uygulanmasını düzenleyen ve özellikle süre, stoklama, kullanım, üçüncü kişilerin veriye erişimi, verilerin gizliliği ile bütünlüğünün korunmasına, bunların imhasına ilişkin prosedürlere dair ve kişilerin yetki aşımı ve keyfiliğe karşı yeteri kadar güvenceye sahip olmalarını sağlayacak açık ve detaylı hükümler içermelidir (S. ve Marper/Birleşik Krallık, § 99; M.M./Birleşik Krallık, § 195).

50. Başvuru konusu olaya benzer bir davada AİHM, başvurucunun zihinsel durumuna ve psikiyatrik tedavisine ilişkin bilgilerin davacı olduğu tazminat davasında toplanarak açıklanmasının onun özel hayatına saygı hakkına müdahale teşkil ettiğini kabul etmiş ve Sözleşme'nin 8. maddesinin müdahalenin kanuniliği ilkesi bakımından ihlal edildiğine karar vermiştir. Somut olayda başvurucu, hukuk fakültesi yöneticisi aleyhine akıl sağlığını sorgulayan sözleri nedeniyle tazminat davası açmıştır. Başvurucunun geçmişte maruz kaldığı bir zihinsel rahatsızlıkla ilgili bazı kanıtlar toplayan ve bunları tarafların ve kamunun katılımının sağlandığı bir duruşmada açıklayan mahkeme davayı reddetmiştir. İstinaf mahkemesi ilk derece mahkemesi kararını esastan onamış ancak ilk derece mahkemesini başvurucunun akıl sağlığıyla ilgili hassas bilgileri ifşa etme konusunda kusurlu bulmuştur. AİHM bu davada istinaf mahkemesinin ilk derece mahkemesini başvurucunun kişisel bilgileriyle ilgili yaklaşımının, psikiyatrik verilerin toplanması, saklanması, kullanılması ve yayılmasıyla ilgili hususları düzenleyen 1992 tarihli Veri Kanunu'na aykırı olduğuna dikkat çekmiştir. AİHM ayrıca mahkemece ifşa edilen hususların davanın sonucuna müessir olmadığını, bir

araştırma, soruşturma ya da yargılama için önemli bir bilgi olmadığından mahkemenin bilgi talebinin gereksiz olduğunu ve bu sebeple 2000 tarihli Psikiyatrik Tıbbi Yardım Kanunu'nun amaçları bakımından kanuni olmadığını ifade etmiştir (Panteleyenکو/Ukrayna, B. No: 11901/02, 29/6/2006, §§ 43-62).

V. İNCELEME VE GEREKÇE

51. Mahkemenin 17/9/2020 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Makul Sürede Yargılanma Hakkının İhlal Edildiğine İlişkin İddia

1. Başvurucunun İddiaları

52. Başvurucu 11/12/2007 tarihinde açtığı davanın 22/12/2015 tarihli karar düzeltme talebinin reddine dair karar ile sonuçlandığını, sekiz yılı aşan yargılama süresinin makul sayılamayacağını belirterek makul sürede yargılanma hakkının ihlal edildiğini ileri sürmüştür.

2. Değerlendirme

53. 31/7/2018 tarihli ve 30495 sayılı Resmî Gazete'de yayımlanan 25/7/2018 tarihli ve 7145 sayılı Kanun'un 20. maddesiyle 9/1/2013 tarihli ve 6384 sayılı Avrupa İnsan Hakları Mahkemesine Yapılmış Bazı Başvuruların Tazminat Ödenmek Suretiyle Çözümüne Dair Kanun'a geçici madde eklenmiştir.

54. 6384 sayılı Kanun'a eklenen geçici maddeye göre yargılamaların uzun sürmesi ve yargı kararlarının geç veya eksik icra edilmesi ya da icra edilmemesi şikâyetiyle Anayasa Mahkemesine yapılan ve bu maddenin yürürlüğe girdiği tarih itibarıyla Anayasa Mahkemesi önünde derdest olan bireysel başvuruların başvuru yollarının tüketilmemesi nedeniyle verilen kabul edilemezlik kararının tebliğinden itibaren üç ay içinde yapılacak müracaat üzerine Adalet Bakanlığı İnsan Hakları Tazminat Komisyonu Başkanlığı (Tazminat Komisyonu) tarafından incelenmesi öngörülmüştür.

55. Anayasa Mahkemesi Ferat Yüksel (B. No: 2014/13828, 12/9/2018) kararında yargılamaların makul sürede sonuçlandırılmadığı ya da yargı kararlarının geç veya eksik icra edildiği ya da hiç icra edilmediği iddiasıyla 31/7/2018 tarihinden önce gerçekleştirilen bireysel başvurulara ilişkin olarak Tazminat Komisyonuna başvuru imkânının getirilmesine ilişkin yolu ulaşılabilir olma, başarı şansı sunma ve yeterli giderim sağlama kapasitesinin bulunup bulunmadığı yönlerinden inceleyerek bu yolun etkililiğini tartışmıştır (Ferat Yüksel, § 26).

56. Ferat Yüksel kararında özetle anılan başvuru yolunun kişileri mali külfet altına sokmaması ve başvuruda kolaylık sağlama nedenleriyle ulaşılabilir olduğu, düzenleniş şekli itibarıyla ihlal iddialarına makul bir başarı şansı sunma kapasitesinden mahrum olmadığı ve tazminat ödenmesine

imkân tanınması ve/veya bu mümkün olmadığında başka türlü telafi olanakları sunması nedenleriyle potansiyel olarak yeterli giderim sağlama imkânına sahip olduğu hususunda değerlendirmelerde bulunulmuştur (Ferat Yüksel, §§ 27-34). Bu gerekçeler doğrultusunda Anayasa Mahkemesi, ilk bakışta ulaşılabilir olan ve ihlal iddialarıyla ilgili başarı şansı sunma ve yeterli giderim sağlama kapasitesi olduğu görülen Tazminat Komisyonuna başvuru yolu tüketilmeden yapılan başvurunun incelenmesinin bireysel başvurunun ikincil niteliği ile bağdaşmayacağı sonucuna vararak başvuru yollarının tüketilmemiş olması nedeniyle kabul edilemezlik kararı vermiştir (Ferat Yüksel, §§ 35, 36).

57. Mevcut başvurunun bu kısmı yönünden söz konusu karardan ayrılmayı gerektiren bir durum bulunmamaktadır. Açıklanan gerekçelerle başvurunun bu kısmının başvuru yollarının tüketilmemiş olması nedeniyle kabul edilemez olduğuna karar verilmesi gerekir.

B. Özel Hayata Saygı Hakkı Kapsamındaki Kişisel Verilerin Korunmasını İsteme Hakkının İhlal Edildiğine İlişkin İddia

1. Başvurucunun İddiaları

58. Başvurucu; İçişleri Bakanlığının düzenlediği yazının şikâyetçi olduğu köşe yazarıyla ilgili ceza soruşturması dosyasına sunulması dolayısıyla bu yazıdan haberdar olduğunu, yazının noter onayından geçirildikten sonra köşe yazarı tarafından ibraz edildiğini, ayrıca anılan kişi aleyhine açtığı manevi tazminat davasında davaya cevap dilekçesinde anılan belge içeriğinin tekrar kullanıldığını belirtmiştir. Sadece yargı makamlarınca istenebilecek kendisine ilişkin bilgilerin mevzuat tarafından öngörülen koşullar gözetilmeden İdarece şirket vekiline verildiğini, yazının başka kimler tarafından ve nasıl kullanılacağına belirsiz olduğunu iddia etmiştir. Anılan yazıya dayanılarak başka bir gazetede de "Çevreci Avukatlar Fişlendi" başlığıyla haber yapılmasından sonra Bugün gazetesinin de bu habere dayanarak tekrar konuyla ilgili haber yaptığını, İçişleri Bakanlığı yazısı nedeniyle kişilik haklarının zedelendiği hususu sabit olmasına rağmen Mahkemenin davasını reddettiğini ve Danıştay kararlarında gerekçe sunulmadığını ifade etmiştir. Bununla birlikte ilgili yazıda adı geçen kişilerden bahsedilirken bir suç örgütünün faaliyetleri izlenimi veren üslup kullanıldığını, kişisel verilerin ancak kanunda öngörülen hâllerde ve kişinin rızası ile işlenebileceğini, yabancı devlet ajanı gibi gösterildiğini, hakkında bir soruşturma olmadığı hâlde suçlu ilan edildiğini vurgulayan başvurucu, masumiyet karinesinin ve özel hayata saygı ile adil yargılanma haklarının ihlal edildiğini ileri sürmüştür.

2. Değerlendirme

59. Anayasa'nın iddianın değerlendirilmesinde dayanak alınacak "Özel hayatın gizliliği" kenar başlıklı 20. maddesinin birinci ve üçüncü fıkrası şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

...

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

60. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki tavsifi ile bağlı olmayıp olay ve olguların hukuki nitelendirmesini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, Ş 16). Başvurucunun şikâyetlerinin özünü, kişisel nitelikteki birtakım verilerinin idare tarafından üçüncü kişilere aktarıldığı iddiası oluşturmaktadır. Dolayısıyla aşağıda belirtilen ilkeler çerçevesinde başvurunun Anayasa'nın 20. maddesinin üçüncü fıkrasında düzenlenen özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkı yönünden değerlendirilmesi gerektiği sonucuna ulaşılmıştır.

a. Uygulanabilirlik Yönünden

61. Özel hayata saygı hakkı Anayasa'nın 20. maddesinde koruma altına alınmıştır. Devlet, kişilerin özel ve aile hayatına keyfî olarak müdahale etmemek ve üçüncü kişilerin haksız saldırılarını önlemekle yükümlüdür. Özel hayata saygı hakkı kapsamında korunan hukuksal çıkarlardan biri de bireyin mahremiyet hakkıdır. Ancak mahremiyet hakkı sadece yalnız kalma hakkından ibaret olmayıp bu hak, bireyin kendisiyle ilgili bilgileri kontrol edebilme hukuksal çıkarını da kapsamaktadır. Bireyin kendisine ilişkin herhangi bir bilginin kendi rızası olmaksızın açıklanmaması, yayılmaması, bu bilgilere başkaları tarafından ulaşılabilmesi ve rızası hilafına kullanılmaması, kısaca bu bilgilerin mahrem kalması konusunda menfaati bulunmaktadır. Bu husus, bireyin kendisiyle ilgili bilgilerin geleceğini belirleme hakkına işaret etmektedir (Serap Tortuk, B. No: 2013/9660, 21/1/2015, §§ 31, 32). Özel hayata saygı hakkının kapsamında olan bireylerin kişisel verilerinin korunması hakkı, Anayasa'nın 20. maddesinde açık olarak düzenlenmiştir (Nurcan Belin, B. No: 2014/14187, 10/1/2018, § 38).

62. Anayasa'nın 20. maddesinin üçüncü fıkrasında ise herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı ifade edilmiştir. Maddede ayrıca kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır (AYM, E.2014/122, K.2015/123, 30/12/2015, §§ 19, 20; Nurcan Belin, § 45).

63. Anayasa Mahkemesi kararlarında da belirtildiği üzere kişisel veri -belirli veya kimliği belirlenebilir olmak şartıyla- bir kişiye ilişkin bütün bilgileri ifade etmekte olup ad, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgilerin değil telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, öz geçmişi, resim, görüntü ve ses kayıtları, parmak izleri, sağlık bilgileri, genetik bilgiler, IP adresi, e-posta adresi, alışveriş alışkanlıkları, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm verilerin kişisel veri kapsamında olduğu belirtilmektedir (AYM, E.2014/74, K.2014/201, 25/12/2014; E.2014/180, K.2015/30, 19/3/2015; E.2017/180, K.2018/109, 6/12/2018, § 54).

64. Öte yandan Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı yönünden inceleme yapılabilmesi için öncelikle anılan hak kapsamında korunması gerekli bir kişisel verinin olup olmadığı belirlenmelidir. Anayasa hükmünün lafzı, konuya ilişkin uluslararası belgeler ve karşılaştırmalı hukuk dikkate alındığında belirli veya belirlenebilir bir gerçek veya tüzel kişi hakkındaki her türlü bilgi kişisel veri olarak değerlendirilir. Ancak her dava ya da başvuruda Anayasa'nın 20. maddesinin üçüncü fıkrası anlamında bir kişisel veri bulunup bulunmadığı davanın ve başvurunun kendine özgü koşulları dikkate alınarak otonom olarak tespit edilir. Bir kişisel verinin bulunduğu tespit edildiğinde bu veriye yönelik her türlü sınırlama ve müdahale Anayasa'nın anılan hükmü kapsamındaki güvenceleri harekete geçirir.

65. Somut olayda İçişleri Bakanlığının şirket avukatına verdiği cevap yazısında başvuruçunun hangi otelde kaldığına, irtibat hâlinde olduğu kişilerin isimlerine ve bu sosyal ilişkinin amacına dair bilgi verildiği görülmüştür. Ayrıca başvuruçuyla birlikte yazıda adı belirtilen kişiler kastedilerek "bazı şahıslarla ilgili olarak çeşitli suçlardan işlem yapılarak adli makamlara tevdi edildikleri" şeklinde bir yargı sürecinin varlığına ilişkin genel bilgi verilmiştir. İlgili yazı bir bütün hâlinde

değerlendirildiğinde başvuruçunun kaldığı otele, irtibat hâlinde olduğu kişilere ve sosyal ilişkileri ile bir yargılama sürecine ilişkin bilgilerin belirli bir gerçek kişiye ait bilgi niteliğinde olduğu dikkate alındığında kişisel veri olarak kabul edilmesi gerekir. Bu durumda kişisel veri niteliğindeki bu bilgilerin üçüncü kişi niteliğindeki şirketin avukatına verilmesi şeklinde gerçekleşen olayda, Anayasa'nın kişisel verilerin korunmasını isteme hakkına ilişkin 20. maddesinin üçüncü fıkrasının uygulanabilir olduğu sonucuna varılmıştır.

b. Kabul Edilebilirlik Yönünden

66. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

c. Esas Yönünden

i. Müdahalenin Varlığı

67. Somut olayda idare tarafından başvuruçunun kaldığı otel ve kimlerle irtibatlı olduğuna dair sosyal çevre bilgilerinin üçüncü bir kişiye yazı ile bildirildiği anlaşılmaktadır. Başvuruçuya ait bu bilgilerin belirlenebilir bir gerçek kişiye ait bilgi olduğu için kişisel veri olarak nitelendirilebileceğinde kuşku yoktur. Bu durumda söz konusu kişisel verilerin üçüncü bir kişi ile paylaşılmasının Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkına bir müdahale oluşturduğu sonucuna varılmıştır.

ii. Müdahalenin İhlal Oluşturup Oluşturmadığı

68. Anayasa'nın 13. maddesi şöyledir:

"Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz."

69. Yukarıda belirlenen müdahale, Anayasa'nın 13. maddesinde belirtilen koşullara uygun olmadığı takdirde Anayasa'nın 17. maddesini ihlal edecektir. Bu sebeple sınırlamanın Anayasa'nın 13. maddesinde öngörülen ve somut başvuruya uygun düşen, kanun tarafından öngörülme, meşru amaç taşıma, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmama kriterlerine

uygun olup olmadığının belirlenmesi gerekir (R.G. [GK], B. No: 2017/31619, 23/7/2020, § 82; Halil Berk, B. No: 2017/8758, 21/3/2018, § 49; Süveyda Yarkın, B. No: 2017/39967, 11/12/2019, § 32; Şennur Acar, B. No: 2017/9370, 27/2/2020, § 34). Bu bağlamda somut başvuruda öncelikle müdahalenin kanuni dayanağının bulunup bulunmadığı incelenmelidir.

(1) Kanunilik

70. Anayasa uyarınca temel hak ve özgürlüklere getirilen sınırlamaların öncelikle kanunla öngörülmüş olması gerekir. Kanun ile sınırlama ölçütü veya kanunilik ilkesi Sözleşme'nin 8. maddesinde de bir sınırlama ve güvence ölçütü olarak yer almaktadır. Buna karşın Sözleşme'de yer alan kanunla öngörülmüş olma kavramı ile Anayasa'da yer alan kanunilik ilkesi tam olarak aynı değildir (Bülent Polat [GK], B. No: 2013/7666, 10/12/2015, § 73).

71. AİHM kanunda öngörülen koşulları, bir diğer ifadeyle hukukiliği geniş yorumlayarak istikrar kazanmış yargı kararlarına dayanan içtihat yoluyla geliştirilmiş ilkelerin de hukukilik şartını karşılayabildiğini kabul ederken (Malone/İngiltere, B. No: 8691/79, 2/8/1984, §§ 66-68; Sunday Times/Birleşik Krallık (No. 1), B. No: 6538/74, 26/4/1979, § 47) Anayasa, tüm sınırlandırmaların mutlaka kanun ile yapılacağını öngörerek Sözleşme'den daha geniş bir koruma sağlamıştır (Mehmet Akdoğan ve diğerleri, B. No: 2013/817, 19/12/2013, § 31; Bülent Polat § 75). Anayasa'nın temel hak ve hürriyetlerin sınırlandırılmasının ancak kanunla yapılacağına ilişkin 13. maddesi, bir kanun hükmü olmaksızın yürütme ve idarenin bir hak ve hürriyeti ilk elden düzenleyici işlemle sınırlamasına izin vermez (Tuğba Arslan [GK], B. No: 2014/256, 25/6/2014, § 87).

72. Anayasa'nın temel hak ve özgürlüklerin sınırlandırılması rejimini düzenleyen 13. maddesinde hak ve özgürlüklerin ancak kanunla sınırlanabileceği temel bir ilke olarak benimsenmiştir. Bunun yanında Anayasa'nın 20. maddesinin üçüncü fıkrasının üçüncü cümlesinde kişisel verilerin "ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla" işlenebileceği belirtilmiş, aynı fıkranın dördüncü cümlesinde ise kişisel verilerin korunmasına ilişkin esas ve usullerin "kanunla" düzenleneceği hüküm altına alınmıştır. Buna göre kişisel verilerin korunmasını isteme hakkına yapılan müdahalelerde dikkate alınacak öncelikli ölçüt, müdahalenin kanuna dayalı olmasıdır.

73. Müdahalenin kanuna dayalı olması öncelikle şekli manada bir kanunun varlığını zorunlu kılar. Kişisel verilerin korunmasını isteme hakkına müdahale edilmesi ancak yasama organınca kanun adı altında çıkarılan düzenleyici işlemlerde müdahaleye imkân tanıyan bir hükmün bulunması şartına bağlıdır.

74. Diğer taraftan Anayasa'nın 2. maddesinde yer alan hukuk devleti ilkesinin bir gereği olarak kanunun kalitesi de kanunilik şartının sağlanıp sağlanmadığının tespitinde önem arz etmektedir. Zira hukuki güvenlik ile belirlilik ilkeleri hukuk devletinin ön koşullarındandır. Kişilerin hukuki güvenliğini sağlamayı amaçlayan hukuki güvenlik ilkesi hukuk normlarının öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerinde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar (AYM, E.2013/39, K.2013/65, 22/5/2013; AYM, E.2014/183, K.2015/122, 30/12/2015, § 5). Belirlilik ilkesi ise yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olmasını, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesini ifade etmektedir (AYM, E.2010/80, K.2011/178, 29/12/2011; AYM, E.2013/39, K.2013/65, 22/5/2013).

75. Buna göre bir hukuk devletinde temel hak özgürlüklere müdahalenin kanuna dayalı olması için şekli anlamda bir kanunun varlığı yanında o kanunun metninin de bireylerin davranışlarının sonucunu öngörebilmesine imkân verecek şekilde belirlilik taşıması gerekir. Diğer bir ifadeyle müdahaleye imkân veren kanun yeterince belirli ve öngörülebilir olmalıdır (benzer görüş için bkz. Halime Sare Aysal [GK], B. No: 2013/1789, 11/11/2015, § 62). Ayrıca belirtmek gerekir ki kişisel verilerin korunmasını isteme hakkına işleme suretiyle yapılan müdahalelerde ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla yapıldığı takdirde kanunilik şartı sağlanmış kabul edilir.

76. Somut olayda başvurucunun açık rızası olmadan kişisel verilerinin üçüncü bir kişiyle paylaşıldığı görülmektedir. Bu durumda Anayasa'nın 20. maddesinin üçüncü fıkrasının üçüncü cümlesinde yer verilen "açık rıza" şartı bulunmadığına göre idare ve derece mahkemelerinin gerekçelerinde dayandıkları 4982 sayılı Kanun ile 1136 sayılı Kanun'da öngörülen hâllerden birinin somut olayda olup olmadığının tartışılması gerekir.

77. Bu bağlamda 4982 sayılı Kanun irdelendiğinde anılan Kanun'un "Özel hayatın gizliliği" kenar başlıklı 21. maddesine göre (bkz. § 27) özel hayatın gizliliği kapsamında kalan ve açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, mesleki ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler bilgi edinme hakkı kapsamı dışındadır. Bu düzenlemenin tek istisnası kişiye önceden haber verilerek yazılı rızasının alınması şartıyla ve kamu yararının gerektirdiği hâllerin varlığı durumunda anılan bilgilerin açıklanabilmesidir.

78. Somut olayda başvurucunun kaldığı otele sosyal çevresi ve yargılama sürecine ilişkin kişisel veri niteliğindeki bilgilerin özel hayatın gizliliği kapsamında kaldığı ve açıklanması hâlinde avukatlık

yapan başvuruçunun Őeref ve itibarı ile mesleki deęerlerine haksız m¼dahale oluŐturabilecek bilgiler olduęu aıktır. Bu durumda 4982 sayılı Kanun'un anılan h¼km¼ karŐısında somut olayda başvuruçunun idare tarafından aıklanan kiŐisel verilerinin bilgi edinme hakkı kapsamında olmadıęı anlaŐılmaktadır. Bu durumla birlikte idare ve yargı makamlarının başvuruçuya ait bu bilgilerin aıklanmasında kamu yararı olduęunu ortaya koymadıkları ve başvuruçunun da kiŐisel verilerinin aıklanması y¼n¼nde aık rızasının olmadıęı hususları g¼zetildięinde 4982 sayılı Kanun h¼k¼mlerinin başvuruçunun kiŐisel verilerinin ¼ç¼nc¼ bir kiŐiyle paylaŐılmasına dair bir kanuni dayanak oluŐturmadıęı s¼ylenebilir.

79. Anayasa Mahkemesi itihadında belirtildięi ¼zere 1136 sayılı Kanun'un genel gerekçesinde avukatlık mesleęinin nitelikleri ve ¼nemi, bir kamu hizmeti olduęu, avukatın yargılama s¼reci iinde adaletin bulunup ortaya ıkarılmasında g¼rev aldıęı, kamu yararını koruduęu belirtilmiŐtir. Kanun'un 1. ve 2. maddelerinde avukatlıęın kamusal y¼n¼ aęır basan bir meslek olduęu vurgulanmıŐtır. Bilgi ve deneyimlerini ¼ncelikle adalet hizmetine vererek adalete ve hakkaniyete uygun ¼z¼mler iin hukuk kurallarının tam olarak uygulanmasında yargı organlarıyla yetkili kurul ve kurumlara yardımı g¼rev bilen avukatın yargı d¼zeni iindeki yeri hukuk devletinde ¼nemlidir. Hukuk devletinin olmazsa olmaz unsuru olan baęımsız yargı, yargının olmazsa olmaz unsuru olan savunma ile birlikte anlam kazanır. Savunma sav-savunma-karar ¼çgeninden oluŐan yargının vazgeilmez ¼gesidir. Adaletli bir yargılamanın varlıęı, ancak avukatın etkin katılımıyla saęlanabilir (AYM, E.2007/16, K.2009/147, 15/10/2009).

80. Bu baęlamda m¼dahaleye dayanak g¼sterilen 1136 sayılı Kanun'un "Avukatlıęın amacı" kenar baŐlıklı 2. maddesinin ¼ç¼nc¼ fıkrasında yer alan "Kanunlarındaki ¼zel h¼k¼mler saklı kalmak kaydıyla, bu kurumlar avukatın gerek duyduęu bilgi ve belgeleri incelemesine sunmakla y¼k¼ml¼d¼r." Őeklindeki d¼zenlemenin adaletli bir yargılamaya hizmet etme noktasında avukatın yargılamaya etkin katılımına kamu kurumlarınca destek verilmesi amacını taŐıdıęı s¼ylenebilir. Ancak anılan Kanun h¼km¼n¼n avukatların bilgi belge taleplerinin dava konusuyla ilgili olup olmadıęı idare tarafından tartıŐılmaksızın avukatların istedikleri her t¼rl¼ bilgi ve belgeye eriŐimlerinin saęlanması gerektięi Őeklindeki geniŐ yoruma m¼sait olmadıęı aıktır.

81. BaŐvuru konusu olayda başvuruçuya iliŐkin kiŐisel veri nitelięindeki bilgilerin ¼ç¼nc¼ kiŐiye verilme nedeni olan asıl dava bir imar planına y¼nelik iptal davasıdır. Avukatın sorduęu Alman Vakıfları olarak bilinen kuruluŐlar ile bazı kiŐilerin Bergama Ovacık Altın Madeni aleyhinde faaliyette bulunup bulunmadıkları hususu ve emniyetin cevap yazısında belirttięi başvuruçunun baŐka kimselerle olan irtibatına, hangi otelde kaldıęına dair bilgilerin ise imar planına karŐı aılan davanın

esasyla ilgili olduđu yargılama sürecinde ortaya konulamamıştır. Bunun da ötesinde başvuruçunun hangi otelde kaldığına, kimlerle irtibatlı olduđuna dair kişisel veri niteliğindeki bilgilerin hangi nedenle toplandıđı ve bunun kanuni dayanağı gösterilememiştir. Bununla birlikte başvuruçunun hakkında bir ceza soruşturması yürütüldüğüne dair bir bilgi olmadığı da gözetildiğinde ancak istihbari olarak toplandıđı kabul edilebilecek bu verilerin başvuruçunun açık rızası olmamasına rağmen üçüncü kişilerle paylaşılması yönündeki idari işlemin 4982 sayılı Kanun ile 1136 sayılı Kanun'da sayılan hâller kapsamında olmadığı, dolayısıyla başvuruçunun kişisel verilerinin üçüncü kişiyle paylaşılması şeklindeki müdahalenin kanuni dayanağının bulunmadığı anlaşılmıştır.

82. Öte yandan dava konusu olay bir yönüyle devletin kendi güvenliği için topladıđı kişisel verileri içeren ancak istihbari olduđu değerlendirilebilecek bilgilerin üçüncü kişiler yararına kullanılması olduđu gözetildiğinde, somut olayın ağırlığı ve önemi nedeniyle demokratik toplum düzeninin gereklerine uygunluğu bakımından kapsamlı bir değerlendirmeye tabi tutulması gerekmektedir.

(2) Meşru Amaç

83. Anayasa'nın 13. maddesinde temel hak ve hürriyetlerin yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağılı olarak sınırlandırılabilmesi hüküm altına alınmıştır. Ancak Anayasa'nın 20. maddesinin üçüncü fıkrasında kişisel verilerin korunmasını isteme hakkına yönelik sınırlama ve müdahaleler yönünden özel bir sınırlama sebebine yer verilmediği görülmektedir. Bununla birlikte Anayasa Mahkemesinin yerleşik içtihadına göre özel sınırlama nedeni öngörülmemiş hak ve özgürlüklerin de o hak ve özgürlüğün doğasından kaynaklanan bazı sınırları bulunmaktadır. Ayrıca Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevler özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebilir (birçok karar arasında bkz. AYM, E.2014/177, K.2015/49, 14/5/2015).

84. Bu bağlamda Anayasa'nın 20. maddesinin üçüncü fıkrasındaki düzenlemelerden kişisel verilerin korunmasını isteme hakkına yönelik sınırlama getirilebileceği anlaşılmaktadır. Ancak fıkrada sınırlayıcı nitelikte sebepler ya da meşru amaçlar listesine yer verilmiştir. Bu durumda hangi alanda kişisel verilerin korunmasını isteme hakkına yönelik sınırlama getirildiği ya da müdahale edildiğine bağılı olarak sınırlama nedeni ya da meşru amaç değişebilir. Buna göre yapılacak incelemede kişisel verilerin korunmasını isteme hakkının bu hakkın doğasından kaynaklanan bazı sınırların bulunduğu dikkate alındığında her dosya ve başvuru kapsamında işin doğasından kaynaklanan sınırlama sebebinin tespit edilmesi ve bunun meşru bir sebep olarak kabul edilip edilemeyeceğinin değerlendirilmesi gerekir. Öte yandan Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin de bu hakka sınır teşkil edebileceği kabul edilmelidir.

85. Bu açıklamalar çerçevesinde somut olayda başvurucunun kişisel verilerinin paylaşılmasının sadece özel hukuka ilişkin bir ihtilafta taraf olan üçüncü kişinin özel yararına hizmet ettiği söylenebilir. Bu durumda ilgili yargılamanın esasına ilişkin olduğu da ortaya konulamayan başvurucuya ait özel hayatın gizliliği kapsamında kalan kişisel bilgilerin üçüncü kişiye verilmesinde, dolayısıyla başvurucunun kişisel verilerin korunmasını isteme hakkına müdahalede bir meşru amacın varlığından söz edilemeyeceği açıktır.

(3) Demokratik Toplum Düzeninin Gereklere Uygunluk

(a) Genel İlkeler

86. Temel hak ve özgürlüklere yönelik bir müdahalenin demokratik toplum düzeninin gereklerine uygun kabul edilebilmesi için zorunlu bir toplumsal ihtiyacı karşılaması ve orantılı olması gerekir. Açıktır ki bu başlık altındaki değerlendirme, sınırlamanın amacı ile bu amacı gerçekleştirmek üzere başvuru araçları arasındaki ilişki üzerinde temellenen ölçülülük ilkesinden bağımsız yapılamaz. Çünkü Anayasa'nın 13. maddesinde demokratik toplum düzeninin gereklerine aykırı olmama ve ölçülülük ilkesine aykırı olmama biçiminde iki ayrı kritere yer verilmiş olmakla birlikte bu iki kriter bir bütünün parçaları olup aralarında sıkı bir ilişki vardır (Ferhat Üstündağ, B. No: 2014/15428, 17/7/2018, § 45).

87. Müdahaleyi oluşturan tedbirin zorunlu bir toplumsal ihtiyacı karşıladığının kabul edilebilmesi için amaca ulaşmaya elverişli olması, başvurulabilecek en son çare ve alınabilecek en hafif önlem olarak kendisini göstermesi gerekmektedir. Amaca ulaşmaya yardımcı olmayan veya ulaşılmak istenen amaca nazaran bariz bir biçimde ağır olan bir müdahalenin zorunlu bir toplumsal ihtiyacı karşıladığı söylenemeyecektir (Ferhat Üstündağ, § 46).

88. Orantılılık ise sınırlamayla ulaşılmak istenen amaç ile başvuru sınırlama tedbiri arasında dengesizlik bulunmamasına işaret etmektedir. Diğer bir ifadeyle orantılılık, bireyin hakkı ile kamunun menfaatleri veya müdahalenin amacı başkalarının haklarını korumak ise diğer bireylerin hak ve menfaatleri arasında adil bir dengenin kurulmasına işaret etmektedir. Dengeleme sonucu müdahalede bulunulan hakkın sahibine terazinin diğer kefesinde bulunan kamu menfaati veya diğer bireylerin menfaatine nazaran açıkça orantısız bir külfet yüklendiğinin tespiti hâlinde orantılılık ilkesi yönünden bir sorunun varlığından söz edilebilir (Ferhat Üstündağ, § 46).

89. Devletin özel hayatın gizliliğinin korunması bağlamında kişisel verilerin yetkisiz kişiler tarafından elde edilmesini veya kullanılmasını önleme, ayrıca bu verilerin ifşa edilmesini engelleme yükümlülüğü bulunmaktadır.

90. Anayasa'nın 12. maddesine göre herkes kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlere sahiptir. Bu genel nitelikteki anayasal düzenleme ile bireylerin kişilik değerlerine yönelen ve zarar veren olumsuz tutum ve davranışlar dışlanmaktadır. Ayrıca Anayasa'nın 5. maddesinde bireylerin temel hak ve özgürlüklerinin korunması, maddi ve manevi varlıklarının geliştirilmesi için gerekli şartların hazırlanması devletin temel amaç ve görevlerinden biri olarak sayılmaktadır. Bu düzenlemeler ışığında devletin bireyin kişisel verilerinin korunması hakkına keyfi olarak müdahale etmemenin yanında üçüncü kişilerin saldırılarını önlemekle yükümlü kılındığı anlaşılmaktadır (Erol Kumcu, B. No: 2015/18988, 9/5/2019, § 32).

(b) İlkelerin Olaya Uygulanması

91. Somut olayda başvuruçunun kişisel verilerinin imar planının iptali davasında taraf olan şirket vekilinin talebi üzerine yargılama sürecinde kullanılmak üzere paylaşıldığı anlaşılmaktadır. Bu kapsamda idarenin şirket vekiline verdiği yazının başvuruçunun hangi otelde kaldığına, irtibatı olduğu kişiler ile sosyal çevresine ilişkin bilgiler içerdiği gözetildiğinde bu bilgilerin imar planının hukuka uygunluğunun tartışıldığı bir yargılamanın esasına etki edebilecek nitelikte olduğu söylenemez. Ayrıca başvuruçunun açmış olduğu tam yargı davasında da kişisel verilerin imar planının iptali davası ile ilgisi ve kişisel verilerin paylaşılmasının söz konusu yargı süreci bağlamında gerekli olduğu tartışılmamıştır.

92. Öte yandan Anayasa Mahkemesi içtihadında belirtildiği üzere 4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Salâhiyet Kanunu, 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu gibi ilgili kuruluş kanunlarında görev ve yetki verilmiş polis teşkilatı ve Millî İstihbarat Teşkilatı gibi kamu kurum ve kuruluşları millî güvenliği, kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik olarak görev ve yetki verilen kamu kurum ve kuruluşlarıdır. Bu Kanunlarda söz konusu kamu kurum ve kuruluşlarının görev ve yetkileri ayrıntılı şekilde düzenlenmiş ve bu düzenlemelerde söz konusu görevlerin Türkiye Cumhuriyeti'nin ülkesi ve milleti ile bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, anayasal düzene ve millî gücünü meydana getiren bütün unsurlara karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkında millî güvenlik istihbaratını oluşturmak olduğu belirtilerek bu kamu kurum ve kuruluşları tarafından yürütülecek önleyici, koruyucu ve istihbari faaliyetler de düzenlenmiştir. Ayrıca söz konusu kurum ve kuruluşların yetki ve sorumlulukları ile bunlara aykırı davranılması hâlinde öngörülen cezai yaptırımlar ilgili kanunlarda ayrıntılı şekilde düzenlendiği gibi 5237 sayılı Kanun'un 136. maddesi uyarınca da kişisel verileri hukuka aykırı olarak başkasına vermek, yaymak veya ele geçirmek suç olarak düzenlenmiştir. Dolayısıyla elde edilecek bilgilerin amacı dışında kullanılmasını

önleyecek ve kişilerin özel hayatına dair bilgilerin ve kişisel verilerin ifşa edilmesini önleyecek yasal güvencelerin de bulunduğu görülmektedir (AYM, E. 2016/125, K. 2017/143, 28/9/2017, §§ 159, 160).

93. Ancak idarenin başvuru hakkında İçişleri Bakanlığı nezdinde yürütülen bir incelemenin de mevcut olmadığı yönünde verdiği bilgi (bkz. § 14) gözetildiğinde somut olayda başvurucuya ait kişisel verilerin hangi gerekçeyle ne gibi bir kapsamda toplandığının idare tarafından ortaya konulmadığı anlaşılmaktadır. Ayrıca tam yargı davasında derece mahkemeleri de söz konusu kişisel verilerin toplanması ve paylaşılmasının hangi zorunlu toplumsal ihtiyaca karşılık geldiğini ilgili ve yeterli bir gerekçe ile gösterememiştir. Bu durumla birlikte söz konusu kişisel verilerin kullanılmak istenen yargı sürecinin esasıyla ilgisi olmadığı gözönünde bulundurulduğunda, başvurucuya ait bu verilerin toplanmasının ve açık rızası olmamasına rağmen üçüncü bir kişiyle paylaşılmasının zorunlu bir toplumsal ihtiyaca karşılık geldiği ve demokratik toplum düzeninin gereklerine uygun olduğu söylenemez.

94. Açıklanan gerekçelerle başvuru hakkındaki Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiğine karar verilmesi gerekir.

C. 6216 Sayılı Kanun'un 50. Maddesi Yönünden

95. 30/11/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 50. maddesinin ilgili kısmı şöyledir:

“(1) Esas inceleme sonunda, başvuru hakkının ihlal edildiğine ya da edilmediğine karar verilir. İhlal kararı verilmesi hâlinde ihlalin ve sonuçlarının ortadan kaldırılması için yapılması gerekenlere hükmedilir...

(2) Tespit edilen ihlal bir mahkeme kararından kaynaklanmışsa, ihlali ve sonuçlarını ortadan kaldırmak için yeniden yargılama yapmak üzere dosya ilgili mahkemeye gönderilir. Yeniden yargılama yapılmasında hukuki yarar bulunmayan hâllerde başvuru lehine tazminata hükmedilebilir veya genel mahkemelerde dava açılması yolu gösterilebilir. Yeniden yargılama yapmakla yükümlü mahkeme, Anayasa Mahkemesinin ihlal kararında açıkladığı ihlali ve sonuçlarını ortadan kaldıracak şekilde mümkünse dosya üzerinden karar verir.”

96. Başvuru hakkındaki ihlalin tespit edilmesini istemiş ve 10.000 TL maddi, 25.000 TL manevi tazminat talebinde bulunmuştur.

97. Anayasa Mahkemesinin Mehmet Doğan ([GK], B. No: 2014/8875, 7/6/2018) kararında ihlal sonucuna varıldığında ihlalin nasıl ortadan kaldırılacağı hususunda genel ilkeler belirlenmiştir.

Anayasa Mahkemesi diđer bir kararında ise bu ilkelerle birlikte ihlal kararının yerine getirilmemesinin sonuçlarına da değinmiş ve bu durumun ihlalin devamı anlamına geleceđi gibi ilgili hakkın ikinci kez ihlal edilmesiyle sonuçlanacağına işaret etmiştir (Aligül Alkaya ve diđerleri (2), B. No: 2016/12506, 7/11/2019).

98. Bireysel başvuru kapsamında bir temel hakkın ihlal edildiđine karar verildiđi takdirde ihlalin ve sonuçlarının ortadan kaldırıldığından söz edilebilmesi için temel kural mümkün olduđunca eski hâle getirmenin yani ihlalden önceki duruma dönülmesinin sağlanmasıdır. Bunun için ise öncelikle ihlalin kaynađı belirlenerek devam eden ihlalin durdurulması, ihlale neden olan karar veya işlemin ve bunların yol açtığı sonuçların ortadan kaldırılması, varsa ihlalin sebep olduđu maddi ve manevi zararların giderilmesi, ayrıca bu bağlamda uygun görülen diđer tedbirlerin alınması gerekmektedir (Mehmet Dođan, §§ 55, 57).

99. İhlalin mahkeme kararından kaynaklandığı veya mahkemenin ihlali gideremediđi durumlarda Anayasa Mahkemesi, 6216 sayılı Kanun'un 50. maddesinin (2) numaralı fıkrası ile İçtüzük'ün 79. maddesinin (1) numaralı fıkrasının (a) bendi uyarınca, ihlalin ve sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmak üzere kararın bir örneđinin ilgili mahkemeye gönderilmesine hükmeder. Anılan yasal düzenleme, usul hukukundaki benzer hukuki kurumlardan farklı olarak ihlali ortadan kaldırmak amacıyla yeniden yargılama sonucunu doğuran ve bireysel başvuruya özgülenen bir giderim yolunu öngörmektedir. Bu nedenle Anayasa Mahkemesi tarafından ihlal kararına bađlı olarak yeniden yargılama kararı verildiđinde usul hukukundaki yargılamanın yenilenmesi kurumundan farklı olarak ilgili mahkemenin yeniden yargılama sebebinin varlığını kabul hususunda herhangi bir takdir yetkisi bulunmamaktadır. Dolayısıyla böyle bir kararın kendisine ulaştığı mahkemenin yasal yükümlülüđü, ilgilinin talebini beklemeksizin Anayasa Mahkemesinin ihlal kararı nedeniyle yeniden yargılama kararı vererek devam eden ihlalin sonuçlarını gidermek üzere gereken işlemleri yerine getirmektir (Mehmet Dođan, §§ 58, 59; Aligül Alkaya ve diđerleri (2), §§ 57-59, 66, 67).

100. İncelenen başvuruda, kişisel verilerin idare tarafından üçüncü kişiye verilmesi nedeniyle özel hayata saygı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiđi sonucuna ulaşılmıştır. Dolayısıyla ihlalin idarenin işleminden kaynaklandığı anlaşılmaktadır. Bununla birlikte Mahkeme de ihlali giderememiştir.

101. Bu durumda özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmasında hukuki yarar bulunmaktadır. Yapılacak yeniden yargılama ise bireysel başvuruya özgü düzenleme içeren 6216

sayılı Kanun'un 50. maddesinin (2) numaralı fıkrasına göre ihlalin ve sonuçlarının ortadan kaldırılmasına yöneliktir. Bu kapsamda yapılması gereken iş, yeniden yargılama kararı verilerek Anayasa Mahkemesini ihlal sonucuna ulaştıran nedenleri gideren, ihlal kararında belirtilen ilkelere uygun yeni bir karar verilmesinden ibarettir. Bu sebeple kararın bir örneğinin yeniden yargılama yapılmak üzere Ankara 7. İdare Mahkemesine gönderilmesine karar verilmesi gerekmektedir.

102. İhlalin ve sonuçlarının ortadan kaldırılması için yeniden yargılamanın yeterli bir giderim sağlayacağı anlaşıldığından tazminat talebinin reddine karar verilmesi gerektiği sonucuna ulaşılmıştır.

103. Dosyadaki belgelerden tespit edilen 239,50 TL harç ve 3.000 TL vekâlet ücretinden oluşan toplam 3.239,50 TL yargılama giderinin başvurucuya ödenmesine karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. 1. Makul sürede yargılanma hakkının ihlal edildiğine ilişkin iddianın başvuru yollarının tüketilmemesi nedeniyle **KABUL EDİLEMEZ OLDUĞUNA,**

2. Özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiğine ilişkin iddianın **KABUL EDİLEBİLİR OLDUĞUNA,**

B. Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme hakkının **İHLAL EDİLDİĞİNE,**

C. Kararın bir örneğinin kişisel verilerin korunmasını isteme hakkının ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmak üzere Ankara 7. İdare Mahkemesine (E.2007/1516, K.2008/2337) **GÖNDERİLMESİNE,**

D. Tazminat talebinin **REDDİNE,**

E. 239,50 TL harç ve 3.000 TL vekâlet ücretinden oluşan toplam 3.239,50 TL yargılama giderinin başvurucuya **ÖDENMESİNE,**

F. Ödemenin, kararın tebliğini takiben başvurucunun Hazine ve Maliye Bakanlığına başvuru tarihinden itibaren dört ay içinde yapılmasına, ödemede gecikme olması hâlinde bu sürenin sona erdiği tarihten ödeme tarihine kadar geçen süre için yasal **FAİZ UYGULANMASINA,**

G. Kararın bir örneğinin bilgi için Danıştay Onuncu Daireye (E.2014/2080) ve Adalet Bakanlığına **GÖNDERİLMESİNE** 17/9/2020 tarihinde **OYBİRLİĞİYLE** karar verildi.

Anayasa Mahkemesi - Ali ığır Kararı (2015/19298)

Ali ığır, B. No: 2015/19298, 8/5/2019

Başvuru, kişisel verilerin hukuka aykırı şekilde kaydedildiğine yönelik şikâyet hakkında etkili bir ceza soruşturması yapılmaması nedeniyle kişisel verilerin korunması hakkının ihlal edildiği iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

BİRİNCİ BÖLÜM

KARAR

ALİ IĞIR BAŞVURUSU

(Başvuru Numarası: 2015/19298)

Karar Tarihi: 8/5/2019

BİRİNCİ BÖLÜM

KARAR

Başkan: Hasan Tahsin GÖKCAN

Üyeler: Burhan ÜSTÜN, Hicabi DURSUN, Kadir ÖZKAYA, Yusuf Şevki HAKYEMEZ

Raportör Yrd.: Fatih ALKAN

Başvurucu: Ali IĞIR

I. BAŞVURUNUN KONUSU

1. Başvuru, kişisel verilerin hukuka aykırı şekilde kaydedildiğine yönelik şikâyet hakkında etkili bir ceza soruşturması yapılmaması nedeniyle kişisel verilerin korunması hakkının ihlal edildiği iddiasına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 9/12/2015 tarihinde yapılmıştır.

3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.

4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.

5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.

6. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık görüş bildirmemiştir.

III. OLAY VE OLGULAR

7. Başvuru formu ve eklerinde ifade edildiği şekliyle olaylar özetle şöyledir:

8. Başvurucu, 2014 yılı itibarıyla Kırşehir Emniyet Müdürlüğünde şube müdürü olarak görev yapmaktadır.

9. 16/6/2014 tarihinde, bazı haber sitelerinde "Kırşehir'de polisleri alevi, problemlili, alkol alır diye fişlemişler" başlıklı haberler yayımlanmıştır. Haberde, İstihbarat Şube Müdürlüğünde görevli bir başkomiser tarafından tutulduğu ileri sürülen bir ajandadan bahsedilmiş ve söz konusu ajandada bulunduğu belirtilen yazılara ilişkin görseller paylaşarak başvurucu ile birlikte birçok emniyet mensubunun fişlendiği iddia edilmiştir. Haber içeriğinde verilen görsellerde başvurucunun isminin karşısına "- (eksi), geliş farklı" ibaresinin yazıldığı görülmektedir.

10. Başvurucu, anılan dönemde İstihbarat Şube Müdürlüğünde görevli tek bir başkomiser olduğunu belirterek başkomiser K.Y. ve fişlemeyi gerçekleştiren kişiler hakkında Kırşehir Cumhuriyet Başsavcılığına (Başsavcılık) 2/7/2014 tarihinde suç duyurusunda bulunmuştur. Başvurucu; söz konusu fişlemeler nedeniyle görev yerinin değiştirildiğini, bunun neticesinde "Emniyette paralel temizlik" başlığı altında haberler yapıldığını, kendisinin ve atama işlemlerine tabi tutulan diğer personelin zan altında bırakıldığını ve aşağılandığını iddia etmiştir. Hakkında tutulan söz konusu yasa dışı notlar nedeniyle çevresine izahatta bulunamadığını, insanların kendisinden uzaklaşmaya çalıştığını ve işyerindeki olumsuz tutumun psikolojik taciz boyutuna ulaştığını ileri sürmüştür. Başvurucu, tazminata ilişkin haklarını saklı tutarak delillerin toplanmasını, olayın aydınlatılmasını ve şüpheli ya da şüphelilerin cezalandırılmalarını talep etmiştir.

11. Başsavcılık tarafından kişisel verileri hukuka aykırı olarak ele geçirme veya yayma, hukuka aykırı olarak kişisel verileri kaydetme ve ayrımcılık suçları kapsamında yürütülen soruşturmada; haber içeriklerinde kullanılan görseller, yazı ve imza incelemesinde kullanılmak üzere ilgili yerlerden talep edilmiş ve ajandanın çalındığı iddiasıyla ilgili olarak yürütülen adli soruşturma ile şüpheli hakkında

açılan idari soruşturma kapsamında elde edilen deliller dosyaya eklenmiştir. Ayrıca 2/7/2014 tarihinde başvuruçunun ve 3/6/2015 tarihinde şüpheli K.Y.nin ifadeleri alınmıştır.

12. Şüpheli K.Y. ifadesinde; görevi gereğince aldığı duyumları not ettiği bir ajandasının bulunduğunu, ajandada yer alan notların sahada yapılan istihbarat faaliyetleri kapsamında elde edildiğini ve teyide muhtaç ham bilgilerden ibaret olduğunu ileri sürmüştür. Elde edilen bilgileri ancak teyit ettikten ve devletin güvenliğini tehdit edecek durumların oluştuğuna kanaat getirdikten sonra kıymetlendirerek ilgili birimlere ulaştırdığını vurgulamış ve soruşturmaya konu olan notları herhangi bir yere iletmediğini belirtmiştir. K.Y.; istihbarat şube müdürlüğüne vekâlet ettiği dönemde arkadaşının vefat etmesi üzerine üç gün izin aldığını, izin için ayrılmadan önce ajandasını çekmeceye koyup kilitletiğini ve anahtarını da masasının üzerinde bulunan kalemiğe bıraktığını, döndüğünde herhangi bir şüphe duymadığı için ajandasının yerinde olup olmadığını özellikle kontrol etmediğini, basında çıkan haberler üzerine ajandasının çalındığı konusunda bilgi sahibi olduğunu ifade etmiştir. Hırsızlık olayıyla ilgili olarak şikâyeti üzerine başlatılan adli soruşturmada kamera kayıtlarının yetersiz olması nedeniyle bir sonuç alınamadığını dile getiren K.Y.; kimseyi fişlemediğini, söz konusu notların herkesin not edebileceği türden bilgilerden oluştuğunu, hatta ajandasında kendi arkadaşlarının da isimlerinin bulunduğunu, hırsızlık olayı olmadığı takdirde bu bilgilerden kimsenin haberinin olmayacağını ve yapılan atama işlemlerinde de ajandada bulunan birçok kişinin görev yerinde herhangi bir değişiklik olmadığını belirtmiştir. Ayrıca açılan idari soruşturma neticesinde hakkında ceza verilmesine yer olmadığına karar verildiğini ve amlandığını ifade eden K.Y.; yayımlanan görsellerde kendisine ait olmayan el yazısıyla yazılmış isim listelerinin de bulunduğunu, birtakım eklemelerin yapıldığını ve bu durumun Kayseri Polis Kriminal Laboratuvarında yapılan el yazısı karşılaştırmalarıyla ortaya konulduğunu ileri sürmüştür.

13. Başsavcılık, 31/8/2015 tarihinde şüpheli K.Y. hakkında kovuşturmaya yer olmadığına karar vermiştir. Karar gerekçesinde; haber sitelerinde yayımlanan ve şüpheli K.Y. tarafından bir kısmının doğru olduğu kabul edilen görsellerin asıllarının elde edilemediği, şüpheliye ait ajandanın herhangi bir resmî belge niteliği taşımadığı, içerdiği notların da gerçek ve resmî olmadığı, bu hususların sabit olduğu, ayrıca ajandanın şüphelinin istek ve iradesi ile bir başkasına verildiğine ilişkin bir delilin de bulunmadığı belirtilmiştir. Kararda, şüpheli tarafından ikrar edilen sayfaların olması nedeniyle ayrıca ekleme yapıp yapılmadığı hususunun soruşturmanın sıhhati açısından bir önem arz etmediği dile getirilmiştir. Somut olayda şüpheli tarafından tutulan ve müştekiler tarafından doğruluğu reddedilen notların kişisel veri olarak nitelendirilmesinin mümkün olmadığı, notlarda yer alan bilgilerin bir sisteme kayıtlı olmaması nedeniyle hukuka aykırı olarak ele geçirilmiş bilgiler olarak

kabul edilemeyeceği ifade edilmiştir. Ayrıca kararda, ayrımcılık suçunun unsurlarının oluşmadığı ve başvuru ile birlikte diğer müştekiler hakkında yapılan görev değişikliklerinin hukuka aykırı olduğuna ilişkin iddialar hakkında Başsavcılıkça yapılacak bir işlemin bulunmadığı belirtilmiştir.

14. Karara karşı yapılan itiraz Kırşehir Sulh Ceza Hâkimliğinin 22/10/2015 tarihli kararıyla reddedilmiştir. Kararda, Başsavcılık tarafından verilen kararın usule ve mevzuata uygun olduğu ifade edilmiştir.

15. Nihai karar 10/11/2015 tarihinde başvurucuya tebliğ edilmiştir.

16. Başvurucu 9/12/2015 tarihinde bireysel başvuruda bulunmuştur.

IV. İLGİLİ HUKUK

17. 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun "Kişisel verilerin kaydedilmesi " kenar başlıklı 135. maddesi şöyledir:

"Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.

Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır."

18. 5237 sayılı Kanun'un "Verileri hukuka aykırı olarak verme veya ele geçirme" kenar başlıklı 136. maddesi şöyledir:

"(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır."

19. 5237 sayılı Kanun'un "Nefret ve ayrımcılık" kenar başlıklı 122. maddesi şöyledir:

"(1) Dil, ırk, milliyet, renk, cinsiyet, engellilik, siyasi düşünce, felsefi inanç, din veya mezhep farklılığından kaynaklanan nefret nedeniyle;

a) Bir kişiye kamuya arz edilmiş olan bir taşınır veya taşınmaz malın satılmasını, devrini veya kiraya verilmesini,

b) Bir kişinin kamuya arz edilmiş belli bir hizmetten yararlanmasını,

c) Bir kişinin işe alınmasını,

d) Bir kişinin olağan bir ekonomik etkinlikte bulunmasını,

engelleyen kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır."

20. 22/11/2001 tarihli ve 4721 sayılı Türk Medeni Kanunu'nun 24. maddesi şöyledir:

"Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir.

Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır."

21. 4721 sayılı Kanun'un 25. maddesinin birinci ve ikinci fıkraları şöyledir:

"Davacı, hâkimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir.

Davacı bunlarla birlikte, düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabilir."

22. 11/1/2011 tarihli ve 6098 sayılı Türk Borçlar Kanunu'nun 49. maddesinin birinci fıkrası şöyledir:

"Kusurlu ve hukuka aykırı bir fiille başkasına zarar veren, bu zararı gidermekle yükümlüdür."

23. 6098 sayılı Kanun'un 58. maddesi şöyledir:

"Kişilik hakkının zedelenmesinden zarar gören, uğradığı manevi zarara karşılık manevi tazminat adı altında bir miktar para ödenmesini isteyebilir.

Hâkim, bu tazminatın ödenmesi yerine, diğer bir giderim biçimi kararlaştırabilir veya bu tazminata ekleyebilir; özellikle saldırıyı kınayan bir karar verebilir ve bu kararın yayımlanmasına hükmedebilir."

24. 6/1/1982 tarihli ve 2577 sayılı İdari Yargılama Usulü Kanunu'nun "İptal ve tam yargı davaları" kenar başlıklı 12. maddesinin ilgili kısmı şöyledir:

"İlgililer haklarını ihlal eden bir idari işlem dolayısıyla Danıştaya ve idare ve vergi mahkemelerine doğrudan doğruya tam yargı davası veya iptal ve tam yargı davalarını birlikte açabilecekleri gibi ilk önce iptal davası açarak bu davanın karara bağlanması üzerine, bu husustaki kararın veya kanun yollarına başvurulması halinde verilecek kararın tebliği veya bir işlemin icrası sebebiyle doğan zararlardan dolayı icra tarihinden itibaren dava süresi içinde tam yargı davası açabilirler. ..."

25. 2577 sayılı Kanun'un "Doğrudan doğruya tam yargı davası açılması" kenar başlıklı 13. maddesinin (1) numaralı fıkrası şöyledir:

"İdari eylemlerden hakları ihlal edilmiş olanların idari dava açmadan önce, bu eylemleri yazılı bildirim üzerine veya başka suretle öğrendikleri tarihten itibaren bir yıl ve her halde eylem tarihinden itibaren beş yıl içinde ilgili idareye başvurarak haklarının yerine getirilmesini istemeleri gereklidir. Bu isteklerin kısmen veya tamamen reddi halinde, bu konudaki işlemin tebliğini izleyen günden itibaren veya istek hakkında altmış gün içinde cevap verilmediği takdirde bu sürenin bittiği tarihten itibaren, dava süresi içinde dava açılabilir."

V. İNCELEME VE GEREKÇE

26. Mahkemenin 8/5/2019 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları

27. Başvurucu; haber sitelerinde yayımlanan görsellerde yer alan listelerle uyumlu olacak şekilde atama işlemleri yapıldığını, bu doğrultuda kendisinin de görev yerinin değiştirildiğini, bu işlemlere dayanak olan fişlemeyi yapan failerin bulunması ve gerçeklerin ortaya çıkarılması amacıyla suç duyurusunda bulunduğunu belirtmiştir. Söz konusu soruşturma kapsamında haber kaynağının araştırılması ve İstihbarat Şube Müdürlüğü'nün kamera kayıtlarının incelenmesi dışında bir işlem yapılmadığını, şüpheliden yazı örneklerinin alınarak inceleme yapılması yönündeki talebinin yerine getirilmediğini iddia etmiştir. Başvurucu; etkili bir ceza soruşturması yürütülmediğini, yasa dışı fişleme kayıtlarına dayanılarak gerçekleştirilen işlemler nedeniyle itibarının zarar gördüğünü ve kamunun imkanlarından mahrum bırakıldığını ileri sürmüştür. Yaşanan süreçte kendisinin ve ailesinin psikolojisinin olumsuz şekilde etkilendiğini, eşinin ilaç kullanmaya başladığını, sosyal çevresi tarafından dışlandığını belirten başvurucu; özel hayata saygı hakkının, kötü muamele yasağının, hak arama hürriyetinin, adil yargılanma hakkının, kişisel verilerin korunması hakkının ve ayrımcılık yasağının ihlal edildiğini iddia etmiştir.

B. Değerlendirme

28. İddianın değerlendirilmesinde dayanak alınacak Anayasa'nın 20. maddesinin üçüncü fıkrası şöyledir:

"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

29. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Başvurucunun şikâyetlerinin özünü; kişisel nitelikteki birtakım verilerine yönelik saldırılara karşı etkili bir ceza soruşturması yürütülmediği iddiası oluşturmaktadır. Dolayısıyla başvurunun Anayasa'nın 20. maddesinin üçüncü fıkrasında düzenlenen kişisel verilerin korunması hakkı kapsamında değerlendirilmesi gerektiği sonucuna ulaşılmıştır.

30. Anayasa'nın 20. maddesinin üçüncü fıkrasında, herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkının olduğu ifade edilmektedir. Söz konusu anayasal güvence, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde koruma altına alınan özel hayata saygı hakkına karşılık gelmektedir. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır (AYM, E.2014/122, K. 2015/123, 30/12/2015, §§ 19-20).

31. Devletin, kişisel verilerin korunması hakkına saygı gösterme yükümlülüğü, öncelikle kamu otoritelerinin öngörülen güvencelere aykırı şekilde bu hakka müdahale etmemelerini gerektirir.

32. Anayasa'nın 20. maddesinde düzenlenen kişisel verilerin korunması hakkı, kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsamaktadır. Maddede ayrıca kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir. Yine Anayasa'nın 12. maddesine göre herkes kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlere sahiptir. Bu genel nitelikteki anayasal düzenleme ile bireylerin kişilik değerlerine yönelen ve zarar veren olumsuz tutum ve davranışlar dışlanmaktadır. Ayrıca Anayasa'nın 5. maddesinde, bireylerin temel hak ve özgürlüklerinin korunması, maddi ve manevi varlıklarının geliştirilmesi için gerekli şartların hazırlanması devletin temel amaç ve görevlerinden biri olarak sayılmaktadır. Bu düzenlemeler ışığında devletin, bireyin kişisel verilerinin korunması hakkına keyfi olarak müdahale etmemenin yanında üçüncü kişilerin saldırılarını önlemekle yükümlü kıldığı, bu bağlamda pozitif yükümlülüklerinin de bulunduğu söylenebilir.

33. Dolayısıyla Anayasa'nın 20. maddesinin üçüncü fıkrasında düzenlenen hak kapsamında devletin, pozitif bir yükümlülük olarak yetki alanında bulunan tüm bireylerin kişisel verilerin korunması hakkını gerek kamusal makamların gerek diğer bireylerin gerekse kişinin kendisinin eylemlerinden kaynaklanabilecek risklere karşı koruma yükümlülüğü bulunmaktadır.

34. Bu anlamda öncelikle devlet, uyuşmazlıkların çözümüne ilişkin etkili yargısal sistem kurma yükümlülüğünü yerine getirmelidir. Söz konusu pozitif yükümlülük; olayın meydana gelme şekli ile etkisi, ağırlığı ve sonuçları bakımından yapılacak değerlendirmelere ve olayın kim tarafından nasıl gerçekleştirildiği konusunda aydınlatılmasını gerekli kılan durumların bulunup bulunmadığına göre her durumda ceza soruşturması/yargılaması yapılmasını gerekli kılmaz. Nitekim yargısal sistem kurma yükümlülüğü, -olayın koşullarına göre- hukuki ve idari yolların devlet tarafından oluşturulmasıyla da yerine getirilebilir. Bu bağlamda bazı durumlarda disiplin soruşturması ile dahi devletin aydınlatma yükümlülüğünün yerine getirilmesi mümkün olabilir.

35. Öte yandan yargısal sistem kurma yükümlülüğünün ceza soruşturması/yargılaması yapılmasını gerekli kılması, failer hakkında mutlaka ceza davası açılmasını ya da onların cezalandırılmasını zorunlu hâle getirmediği gibi başvuruçulara üçüncü tarafları bir suç nedeniyle yargılatma ya da cezalandırılmalarını talep etme hakkı da vermemektedir. Zira burada kastedilen sonuç yükümlülüğü değil uygun araçların kullanılması yükümlülüğüdür. Ancak her durumda söz konusu yargısal sistemlerin etkili şekilde işletilmesi ve soruşturmalar ya da yargılamalar neticesinde yargısal makamlarca ulaşılan tüm sonuçların temel hakların içerdiği güvenceleri koruyacak şekilde ilgili ve yeterli gerekçelerle açıklanması gerekir.

36. Ek olarak ayrıca vurgulamak gerekir ki kişilerin cezai sorumluluğuna ilişkin hukuki sorunların incelenmesi, ceza soruşturması/kovuşturması sürecinin mahkûmiyet kararı ile sonuçlanması ve bu hâlde takdir edilecek cezanın miktar ve mahiyetinin belirlenmesi Anayasa Mahkemesinin görev alanı içinde olmayıp bu husus esasen derece mahkemelerinin takdirindedir.

37. Somut olayda başvuruçuyu; hakkında tutulan ve önceden bilgi sahibi olmadığı birtakım notların haber sitelerinde yayımlandığını, yasa dışı şekilde tutulan bu notlara dayanılarak hakkında işlemler yapıldığını ileri sürmüş, sorumluların bulunması ve gerçeklerin ortaya çıkarılması amacıyla suç duyurusunda bulunduğunu beyan etmiştir. Olayın özellikleri dikkate alındığında; her ne kadar bir şüpheli olsa da söz konusu notların kim tarafından nasıl bir yetki kapsamında ve hangi amaçla tutulduğu konularında kamusal makamların devreye girmeleri ve olayı tüm yönleriyle aydınlatmaları gerektiği değerlendirilmektedir. Ayrıca, olayın meydana gelme şekli ile ağırlığı da göz önüne alındığında devletin etkili yargısal sistem kurma yükümlülüğünün -somut olay özelinde- bir ceza soruşturması yapılmasını gerekli kıldığı kanaatine varılmıştır.

38. Bu durumda bireysel başvuru kapsamında yapılacak değerlendirmede dikkate alınacak husus; belirtilen çerçeve içerisinde yeterli usule ilişkin güvencelerin sunulduğu bir cezai takibatın yürütülüp yürütülmediğine, soruşturmanın bağımsız, özenli, süratli, etkili şekilde yapılıp yapılmadığına ve

ulařılan sonuçların temel hakların ierdiđi gvenceleri koruyacak řekilde ilgili ve yeterli gerekerle aıklanıp aıklanmadıđına iliřkin olacaktır.

39. Bařvuruya konu olay hakkında Bařsavcılık tarafından yapılan ceza soruřturmasında, ncelikle bařvurucunun ifadesinin alındıđı ve řikyetlerinin dinlendiđi anlařılmaktadır. Akabinde, haber ieriđinde İstihbarat řube Mdrlđnde grevli bir bařkomiser olarak belirtilen K.Y.nin ifadesine bařvurulduđu grlmektedir. Ayrıca ilgili haber ieriklerinde kullanılan grsellerin, yazı ve imza incelemesinde kullanılmak zere haberi yapan yayın řirketinden istendiđi anlařılmaktadır. Yine řpheli hakkında bařlatılan idari tahkikat srecinde ve ajandanın alındıđı iddiasıyla ilgili olarak yrtlen adli soruřturmada elde edilen bařta kamera kaydı olmak zere delillerin incelendiđi, ajandanın řpheli K.Y. tarafından bir bařkasına verilip verilmediđi hususunda arařtırmalar yapıldıđı ve tespitlerde bulunulduđu grlmektedir.

40. Soruřturma neticesinde verilen 31/8/2015 tarihli kararda, bahse konu haberlerin ieriđindeki grsellerde yer alan ve bařvurucunun isminin de bulunduđu notların kim tarafından tutulduđu ve nasıl elde edildiđi konusunda aıklamada bulunulduđu grlmektedir. Ayrıca sz konusu notların niteliđine, hangi amala tutulduđuna ve notları tuttuđunu ikrar eden řphelinin grevi dikkate alınarak bu tr bir eylemin su oluřturup oluřturmadıđı konusunda deđerlendirmeler yapıldıđı anlařılmaktadır. Sz konusu ceza soruřturması bir btn olarak deđerlendirildiđinde, bařvurucu tarafından ileri srlen gereklerin ve sorumluların belirlenmesi talebinin yerine getirildiđi, ulařılan sonucun ilgili ve yeterli gerekerle aıklandıđı ve soruřturmanın etkili bir řekilde yapılmadıđı tespitinde bulunmayı gerektiren bir nedenin olmadıđı kanaatine varılmıřtır.

41. te yandan bařvuruya konu olayın Bařsavcılık tarafından yrtlen soruřturma vasıtasıyla aydınlatıldıđı dikkate alındıđında; bařvurucunun kiřilik haklarına saldırı mahiyetindeki sz konusu iddialarının ayrıca adli ve idari yargı dzenindeki mahkemelerce deđerlendirilebileceđi, bu dođrultuda ilgili mevzuat kapsamında kiřilik haklarına ynelen saldırıların sona erdirilmesi ve zararın tazmin edilmesi hususunda hukuk davası ile tam yargı davası aılabileceđi konusunda bir tereddt yoktur. Dolayısıyla bařvurucunun anılan yollara bařvurarak iddialarını ileri srebilmesi ve zararlarını tazmin edebilmesi de mmkndr.

42. Sonu olarak etkili yargısal sistem kurma ykmllđnn ceza soruřturması/yargılaması yapılmasını gerekli kılmasının sorumlular hakkında mutlaka ceza davası aılmasını ya da onların cezalandırılmasını zorunlu hle getirmediđi konusunda ortaya konulan ilke gz nne alındıđında; somut bařvuruda kamusal makamlarca stlenilmesi gereken pozitif ykmllđn gerektirdiđi

řartların gerisinde kalınmadığı ve açık bir ihlalin bulunmadığı deęerlendirildięinden bařvurunun açıkça dayanaktan yoksun olması nedeniyle kabul edilemez olduęuna karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Kişisel verilerin korunması hakkının ihlal edildięine ilişkin iddianın açıkça dayanaktan yoksun olması nedeniyle **KABUL EDİLEMEZ OLDUĞUNA,**

B. Yargılama giderlerinin bařvurucu üzerinde **BIRAKILMASINA 8/5/2019 tarihinde OYBİRLİĞİYLE** karar verildi.

Anayasa Mahkemesi - C.K. (Unutulma Hakkı) Kararı (2014/19685)

C.K. [GK], B. No: 2014/19685, 15/3/2018

Başvuru, isim yazılarak yapılan araştırmada arama motorlarında listelenen ve internet haber arşivlerinde yer alan bazı haberler ile ilgili içeriğe erişimin engellenmesi yönündeki taleplerin reddedilmesi nedeniyle şeref ve itibarın korunması hakkının ihlal edildiği iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

GENEL KURUL

KARAR

C.K. BAŞVURUSU

(Başvuru Numarası: 2014/19685)

Karar Tarihi: 15/3/2018

R.G. Tarih ve Sayı: 17/5/2018 - 30424

GENEL KURUL

KARAR

GİZLİLİK TALEBİ KABUL

Başkan: Zühtü ARSLAN

Başkanvekili: Burhan ÜSTÜN

Başkanvekili: Engin YILDIRIM

Üyeler: Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Rıdvan GÜLEÇ, Yusuf Şevki HAKYEMEZ

Raportör Yrd.: Derya ATAKUL

Başvurucu: C.K.

Vekili: Av. Müşerref SEKO

I. BAŞVURUNUN KONUSU

1. Başvuru, isim yazılarak yapılan araştırmada arama motorlarında listelenen ve internet haber arşivlerinde yer alan bazı haberler ile ilgili içeriğe erişimin engellenmesi yönündeki taleplerin reddedilmesi nedeniyle şeref ve itibarın korunması hakkının ihlal edildiği iddiasına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 12/12/2014 tarihinde yapılmıştır.

3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.

4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.

5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.

6. Birinci Bölüm tarafından 24/1/2018 tarihinde yapılan toplantıda, niteliği itibarıyla başvurunun Genel Kurul tarafından karara bağlanması gerekli görülmüş ve Anayasa Mahkemesi İçtüzüğü'nün 28. maddesinin (3) numaralı fıkrası uyarınca Genel Kurula sevkine karar verilmiştir.

III. OLAY VE OLGULAR

7. Başvuru formu ve eklerinde ifade edildiği şekliyle olaylar özetle şöyledir:

8. Başvurucu, olayların olduğu tarihten bu yana mankenlik ajansı sahibidir ve kendisi de eski bir mankendir. Başvurucunun sinema ve tiyatro alanında da çalışmaları bulunmaktadır.

9. 2001 yılında Türkiye Yüz Güzeli seçilmiş ve başvurucunun sahibi olduğu mankenlik ajansına bağlı olarak çalışan bir manken, 2004 yılında aşırı dozda uyuşturucudan hayatını kaybetmiştir.

10. Türkiye Yüz Güzeli seçilmesinin ardından tanınmışlık düzeyi oldukça artan mankenin ölüm nedeni ülke gündeminde geniş yer bulmuş, olay tarihi ve sonrasında birçok gazetede ve internet haber sitesinde konuyla ilgili haberler yapılmıştır. Haberlerde olayın oluş şekli, mankene uyuşturucuyu temin eden zanlılar, olaya ilişkin savcılık soruşturması ile ilgili bilgiler yer almaktadır.

11. Yine bu konuyla ilgili olarak başvurucunun bireysel başvuru konusu yaptığı haberlerden birinde yargılamayı yapan mahkeme tarafından mankenin çalıştığı ajansın sahibi olarak başvurucunun da tanık olarak dinlendiği bilgisi aktarılmıştır. Bir diğer haberde, ölen mankenin basına verdiği son röportajda içinde bulunduğu durumun sorumlusu olarak başvurucuyu gösterdiğinin öğrenilmesi

üzerine başvuruçunun adli makamlar tarafından uzun süre sorgulandıđı belirtilmiştir. Haberlerde, ölen mankenin başvuruçunun asistanı ile de ilişkisi olduđu ve ortak arkadaşları olan bir transseksüel ile hep birlikte para karşılığında cinsel ilişkiye girdikleri iddialarına yer verilmiştir. Haberlerde ayrıca yine kamuoyunda tanınmış bir kişi olan başvuruçunun eşinin de yıllar önce aşırı dozda uyuşturucudan öldüğü bildirilmiştir.

12. Başvuruçucu; yaşanan olaylarla bir ilgisi olmadığı hâlde arama motorlarına ismi yazıldığında hem ölen manken ile hem de ölen eşi ile ilgili haberlerin listelendiğini, bu haberler nedeniyle şeref ve itibarının zedelendiğini ileri sürerek internet içeriklerine erişimin engellenmesi talebinde bulunmuştur.

13. İstanbul 2. Sulh Ceza Hâkimliği 30/9/2014 tarihinde dava konusu haberlerin başvuruçunun kişilik haklarına saldırı niteliğinde ve incitici mahiyette olmadığı, ayrıca haber içerikleri dikkate alındığında talebin kabulü hâlinde haber alma ve haber verme hürriyetinin sınırlandırılacağı gerekçesiyle erişimin engellenmesi talebinin reddine karar vermiştir.

14. Başvuruçunun anılan karara itirazı İstanbul 3. Sulh Ceza Hâkimliğince 16/10/2014 tarihinde reddedilmiştir.

15. Karar, başvuruçuya 11/11/2014 tarihinde tebliğ edilmiştir. Başvuruçucu 11/12/2014 tarihinde bireysel başvuruda bulunmuştur.

IV. İLGİLİ HUKUK

A. Ulusal Hukuk

16. 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un "İçeriğın yayından çıkarılması ve erişimin engellenmesi" kenar başlıklı 9. maddesinin ilgili kısmı şöyledir:

"(1) İnternet ortamında yapılan yayın içeriğı nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğın yayından çıkarılmasını isteyebileceğı gibi doğrudan sulh ceza hâkimine başvurarak içeriğın erişimin engellenmesini de isteyebilir.

(2) İnternet ortamında yapılan yayın içeriğı nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişilerin talepleri, içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılır.

(3) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talepleri doğrultusunda hâkim bu maddede belirtilen kapsamda erişimin engellenmesine karar verebilir.

(4) Hâkim, bu madde kapsamında vereceği erişimin engellenmesi kararlarını esas olarak, yalnızca kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verir. Zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemez. Ancak, hâkim URL adresi belirtilerek içeriğe erişimin engellenmesi yöntemiyle ihlalin engellenemeyeceğine kanaat getirmesi hâlinde, gerekçesini de belirtmek kaydıyla, internet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilir.

(5) Hâkimin bu madde kapsamında verdiği erişimin engellenmesi kararları doğrudan Birliğe gönderilir.

(6) Hâkim bu madde kapsamında yapılan başvuruyu en geç yirmi dört saat içinde duruşma yapmaksızın karara bağlar. Bu karara karşı 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir.

(7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

(8) Birlik tarafından erişim sağlayıcıya gönderilen içeriğe erişimin engellenmesi kararının gereği derhâl, en geç dört saat içinde erişim sağlayıcı tarafından yerine getirilir.

(9) Bu madde kapsamında hâkimin verdiği erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının (...) başka internet adreslerinde de yayınlanması durumunda ilgili kişi tarafından Birliğe müracaat edilmesi hâlinde mevcut karar bu adresler için de uygulanır.

(10) Sulh ceza hâkiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişi, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır."

B. Uluslararası Hukuk

17. Somut olayla ilgili uluslararası hukuk kuralları için Anayasa Mahkemesinin Ali Kızılcık (B. No: 2014/5552, 26/10/2017, §§ 22-29) kararına bakılabilir.

V. İNCELEME VE GEREKÇE

18. Mahkemenin 15/3/2018 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları

19. Başvurucu; sahibi olduğu mankenlik ajansında çalışan bir mankenin aşırı dozda uyuşturucudan ölmesi olayıyla ilgili medyada sayısız haber yapıldığını, bu haberlerde kendisi ile ilgili bilgilere de yer verildiğini ifade etmiştir. Başvurucu; yaşanan olaylarla bir ilgisi olmadığı hâlde arama motorlarına ismi yazıldığında hem ölen manken ile hem de kendisinin ölen eşi ile ilgili haberlerin listelendiğini, bu haberler nedeniyle şeref ve itibarının zedelendiğini iddia etmiştir. İnternet içeriklerine erişimin engellenmesi talebinin Mahkemece reddedilmesi ve bunun sonucunda söz konusu haber ve yazıların internet ortamında yer almaya devam etmesi nedeniyle özel hayatın gizliliği, şeref ve itibarın korunması ile adil yargılanma haklarının ihlal edildiğini ileri sürmüştür.

B. Değerlendirme

20. Anayasa'nın iddianın değerlendirilmesinde dayanak alınacak "Kişinin dokunulmazlığı, maddi ve manevi varlığı" kenar başlıklı 17. maddesi ile "Düşünceyi açıklama ve yayma hürriyeti" kenar başlıklı 26. maddesi ve "Basın hürriyeti" kenar başlıklı 28. maddesinin ilgili kısımları şöyledir:

“(17) Herkes, yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkına sahiptir.

...

(26) Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet resmi makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Bu fıkra hükmü, radyo, televizyon, sinema veya benzeri yollarla yapılan yayımların izin sistemine bağlanmasına engel değildir.

Bu hürriyetlerin kullanılması, millî güvenlik, kamu düzeni, kamu güvenliği, Cumhuriyetin temel nitelikleri ve Devletin ülkesi ve milleti ile bölünmez bütünlüğünün korunması, suçların önlenmesi, suçluların cezalandırılması, Devlet sırrı olarak usulünce belirtilmiş bilgilerin açıklanmaması, başkalarının şöhret veya haklarının, özel ve aile hayatlarının yahut kanunun öngördüğü meslek sırlarının korunması veya yargılama görevinin gereğine uygun olarak yerine getirilmesi amaçlarıyla sınırlanabilir.

...

Düşünceyi açıklama ve yayma hürriyetinin kullanılmasında uygulanacak şekil, şart ve usuller kanunla düzenlenir.

(28) “Basın hürdür, sansür edilemez...

...

Devlet, basın ve haber alma hürriyetlerini sağlayacak tedbirleri alır.

Basın hürriyetinin sınırlanmasında, Anayasanın 26 ve 27 nci maddeleri hükümleri uygulanır.

...”

21. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Başvurucu, hakkında yayımlanan haberlerin internet ortamında yer almaya devam etmesi nedeniyle kişilik haklarının zedelendiğinden şikâyet etmektedir. Başvurucunun bu şikâyeti şeref ve itibarın korunması hakkı kapsamında incelenmiştir.

Hasan Tahsin GÖKCAN farklı gerekçeyle bu görüşe katılmıştır.

1. Genel İlkeler

a. Kişinin Manevi Varlığını Koruma ve Geliştirme Hakkı

22. Bireyin kişisel şeref ve itibarı, Anayasa'nın 17. maddesinde yer alan "manevi varlık" kapsamında yer almaktadır. Devlet, bireyin manevi varlığının bir parçası olan kişisel şeref ve itibara keyfî olarak müdahale etmemek ve üçüncü kişilerin saldırılarını önlemekle yükümlüdür (Adnan Oktar (2), B. No: 2013/1123, 2/10/2013, § 33). Başka bir deyişle kişisel itibarın korunması hakkı Anayasa'nın 17. maddesinin birinci fıkrasının koruması altındadır (Kadir Sağdıç [GK], B. No: 2013/6617, 8/4/2015, § 36; İlhan Cihaner (2), B. No: 2013/5574, 30/6/2014, § 42).

23. Anayasa'nın 17. maddesinin birinci fıkrasının olaya uygulanabilmesi için kişinin itibarına yapılan saldırının belli bir ağırlık düzeyine erişmiş olması ve kişinin itibarına saygı gösterilmesini isteme hakkından başvuru kişinin kişisel olarak yararlanmasını güçleştirecek şekilde yapılmış olması gerekir (Kadir Sağdıç, § 39; İlhan Cihaner (2), §§ 45, 46; benzer yöndeki AİHM kararı için bkz. Mater/Türkiye, B. No: 54997/08, 16/7/2013, § 52).

24. Anayasa Mahkemesi; N.B.B. (B. No: 2013/5653, 3/3/2016, § 37) kararında internet ortamının sağladığı ulaşılabilirlik, yaygınlık, haber ve fikirlerin depolanmasındaki ve muhafazasındaki kolaylık dikkate alındığında yayımlandığı tarihte belirli ağırlık eşiğini aşmayan veya kişinin kendi eylemlerinden kaynaklanan haber ve yazıların internet ortamında uzun süre erişilebilir kalması hâlinde kişilerin şeref ve itibarının zedelenebileceğini belirtmiş ve bu durumu unutulma hakkı kapsamında incelemiştir.

b. İfade Özgürlüğü ve İnternetin Rolü

25. Anayasa'nın "Düşünceyi açıklama ve yayma hürriyeti" kenar başlıklı 26. maddesine göre herkes düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve

yayma hakkına sahiptir. Bu hürriyet, resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Anılan maddede ifade özgürlüğünün kullanımında başvurulabilecek araçlar “söz, yazı, resim veya başka yollar” olarak ifade edilmiş ve “başka yollar” ifadesiyle her türlü ifade aracının anayasal koruma altında olduğu gösterilmiştir (Emin Aydın, B. No: 2013/2602, 23/1/2014, § 43).

26. İnternet haberciliğinin -basının temel işlevini yerine getirdiği sürece- basınözgürlüğü kapsamında değerlendirilmesi gerekir (Medya Gündem Dijital Yayıncılık Ticaret A.Ş. [GK], B. No: 2013/2623, 11/11/2015, §§ 36-42; Önder Balıkçı, B. No: 2014/6009, 15/2/2017, § 39; Orhan Pala, B. No: 2014/2983, 15/2/2017, § 45). Basın yönünden düşünce ve kanaat açıklama özgürlüğü kapsamında değerlendirilen internet özgürlüğü, internete erişenler yönünden ise Anayasa tarafından korunan ve ifade özgürlüğünün özünde yer alan haber veya fikir almak özgürlüğü olarak mütalaa edilmektedir.

27. Ulaşılabilirliği, haber ve fikirlerin saklanma süresi ve kapasitesi ile hacimce büyük haber ve fikirleri iletme imkânı gözetildiğinde internet, halkın haber almasının ve bilgilerin iletilmesinin gelişiminde önemli bir role sahiptir. İnternet, herhangi bir sınırlama gözetmeksizin herkesin haber ve fikirlere ulaşması ile fikirlerini yayması noktasında çok önemli bir imkân sağlamaktadır. Bu durum ifade özgürlüğü açısından da çok geniş bir alan yaratmaktadır (Medya Gündem Dijital Yayıncılık Ticaret A.Ş., § 34).

28. Dolayısıyla internet sitelerine veya internet sitelerinde yer alan haberlere erişimin engellenmesi biçiminde getirilen her türlü kısıtlama, bilgi alma ve verme özgürlüğüne müdahale niteliğindedir. Basın özgürlüğünün kamuoyuna çeşitli fikir ve tutumların iletilmesi, bunlara ilişkin bir kanaat oluşturması için en iyi araçlardan birini sağladığı bilinmektedir (İlhan Cihaner (2), § 63).

2. 5651 Sayılı Kanun'un 9. Maddesine Dayanan Erişimin Engellenmesi Kararı Hakkında Bazı Tespitler

29. Anayasa Mahkemesi, Ali Kızık kararında 5651 sayılı Kanun ile getirilen içeriğin yayından çıkarılması ve yayına erişimin engellenmesi kararlarına yönelik usulü ayrıntılı bir şekilde incelemiştir (bkz. §§ 55-63). Mahkemeye göre bu usul, kanun koyucunun internet ortamında işlenen suçlarla mücadelenin daha etkin yapılabilmesi, özel hayatın ve kişilik haklarının hızlı ve etkili bir şekilde korunması ihtiyacı nedeniyle öngördüğü özel ve hızlı sonuç alınabilecek bir koruma tedbiri kararıdır, dolayısıyla istisnai bir yoldur (Ali Kızık, § 55).

30. Kişilik haklarına saldırı nedeniyle erişimin engellenmesi yolunun istisnai bir yol kabul edilmesinin sebebi bu yolun ifade ve basın özgürlükleri önünde orantısız bir mühadale oluşturması ihtimalidir.

31. 5651 sayılı Kanun'da öngörülen erişimin engellenmesi yolu çekişmesiz bir yargı yolu olduğundan, başka bir deyişle karşı taraf bulunmadığından karardan etkilenecek basın organının temsilcileri ile sorumlu kişiler silahların eşitliği ilkesinden faydalanamamakta; talepte bulunanın iddialarına karşı delil sunmak da dâhil olmak üzere savunmalarını ortaya koymak için makul ve kabul edilebilir olanaklara sahip olamamaktadır. Özet olarak hâkim kararını dosya üzerinden, delil toplamaksızın, sınırlı bir inceleme ile yani talepte bulunanın sunduğu bilgi ve belgelere göre vermekte; bu yargılamada karşı tarafın görüşleri alınamamaktadır (Ali Kıdık, §§ 60-62).

32. Dahası 5651 sayılı Kanun'un 9. maddesinde internet erişiminin engellenmesi kararından sonra failer hakkında adli soruşturma açılıp açılmayacağı belirsizdir. Kişilik haklarına müdahale nedeniyle soruşturma açıldığı takdirde soruşturma veya kovuşturmanın sonucuna göre yargı mercileri, erişimin engellenmesi tedbirinin akıbeti hakkında bir karar verebilir. Buna karşılık bir soruşturma açılmadığı takdirde erişimin engellenmesine ilişkin söz konusu tedbir, internet kullanıcılarını engellenen içeriğe belirsiz bir süreyle erişmekten alıkoyacaktır (Ali Kıdık, § 59).

33. Bu sebeplerle başvuruya konu internet yayınına erişimin engellenmesi tedbirinin alınmasının haklılığı, ancak bir görüşte haklılık veya "ilk bakışta" (prima facia) haklılık olarak nitelendirilebilir. Anayasa Mahkemesi, bu usulün ancak internet yayınının kişilik haklarını apaçık bir şekilde ihlal ettiğinin daha ilk bakışta anlaşıldığı durumlarda işletilebileceğini belirtmiştir. Bir kimsenin çıplak resimlerinin veya video görüntülerinin yayımlanması gibi kişilik haklarının ihlal edildiğinin daha ileri bir inceleme yapılmaya gerek olmaksızın ilk bakışta anlaşılabilirliği hâllerde 5651 sayılı Kanun'un 9. maddesinde öngörülmüş olan istisnai usul işletilebilir. Böyle durumlarda "ilk bakışta ihlal doktrini" internet ortamında yapılan yayınlara karşı kişilik haklarının hızlı bir şekilde korunması ihtiyacıyla ifade hürriyeti arasında adil bir denge sağlayacaktır (Ali Kıdık, §§ 62, 63).

3. Şeref ve İtibara Yapılan Müdahalelerde Başvurulabilecek Diğer Hukuki Yollar

34. Yukarıdaki değerlendirmeler dikkate alındığında internet içeriğine erişimin engellenmesi taleplerinin zorunlu durumlarda kabul edilmesi gerektiği ortadadır. Bununla birlikte internet üzerinden yapılan yayınlara ulaşılmasının kolaylığı gözetildiğinde başvurucular açısından yayın içeriği bakımından toplumda sürekli olarak bir ön yargının ve özel hayata müdahalenin oluşması söz konusu olabilir.

35. Bu tür durumlarda üçüncü kişilerce kişilik haklarına yapılan müdahaleler için ülkemizde hem cezai hem de hukuki koruma yolları öngörülmüştür. Kişilik haklarına internet ortamında yapılan bir yayınlara saldırıda bulunulan kişi tarafından, özel hukuk davaları yoluyla örneğin 22/11/2001 tarihli ve 4721 sayılı Türk Medeni Kanunu'nun 24. ve 25. maddelerine dayanılarak müdahalenin önlenmesi,

durdurulması veya devam eden müdahaleye son verilmesi, müdahalenin hukuka aykırılığının saptanması, mahkemenin alacağı kararın veya cevap ve düzeltme metninin yayımlanması ya da üçüncü kişilere bildirilmesi istenebilir; maddi veya manevi tazminat davaları açılabilir. Gecikmesinde sakınca bulunan ve ciddi bir zararın doğacağı anlaşılan hâllerde tehlike veya zararın önlenmesi için hâkimden gereken tedbirlere karar vermesi istenebilir. Bu kapsamda talep edildiği takdirde 4/2/2011 tarihli ve 6100 sayılı Hukuk Muhakemeleri Kanunu'nun 389. ve devamı maddeleri uyarınca gecikmesinde sakınca bulunan ya da gecikmesi durumunda önemli zarar oluşacağı hâllerde tehlike veya zararı önlemek için ihtiyati tedbir kararı verilebilir. Bunlardan başka basın yoluyla kişilik haklarına müdahalede bulunulan kişi, açıklamalarından dolayı sebepsiz yere zenginleşen kişi aleyhine sebepsiz zenginleşme davası açabilir veya yayın nedeniyle elde ettiği kazancın vekâletsiz iş görme hükümlerine göre kendisine ödenmesini isteyebilir (Ali Kızık, § 64).

36. İnternet yolu ile kişilik haklarına yönelik bir saldırı ceza kanunlarına göre suç oluşturuyor ise müşteki yalnızca veya aynı zamanda failin cezalandırılmasını da isteyebilir, bu durumda ceza soruşturması ve kovuşturması için Cumhuriyet savcılığına da başvurabilir. Zaten suç, şikâyete tabi olmayan suçlardan ise Cumhuriyet savcısının resen soruşturma başlatması kanuni bir zorunluluktur. Bir ceza kovuşturması açıldığı takdirde 4/12/2014 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu'nun 223. maddesinin (6) numaralı fıkrasına göre hâkim mahkûmiyet kararı verdiği takdirde güvenlik tedbirlerine de hükmedebileceği için internet erişiminin engellenmesi tedbiri hakkında da bir karar verilmiş olacaktır (Ali Kızık, § 65).

37. Anayasa Mahkemesi 5651 sayılı Kanun'un 9. maddesine göre ortada ilk bakışta ihlal bulunmadığı gerekçesiyle istediği korumayı elde edemeyen kişinin de kişilik haklarının korunması için genel hukuk yoluna her hâlde başvurabileceği, sulh ceza hâkiminin ilk bakışta ihlalin olduğuna veya olmadığına karar vermesinin uyuşmazlığın tümüyle çözümlendiği anlamına gelmeyeceği sonucuna varmıştır. Bu tür kararların hiçbir zaman normal bir dava için maddi anlamda kesin hüküm teşkil etmeyeceğini ifade eden Anayasa Mahkemesi, genel mahkemelerde görülen davalarda erişimin engellenmesi talebinin kabul edilebilmesi için ihlal iddiasının ispatlanması gerekeceğini belirtmiştir (Ali Kızık, §§ 66, 67).

4. Genel İlkelerin Somut Olaya Uygulanması

38. Somut olayda başvurucunun şikâyetine konu olan yayınlar internet haber arşivlerinde yer alan bazı haberlerdir. Haberler 2001 yılında güzellik yarışmasında derece almış bir mankenin hızlı yükselişini ve 2004 yılındaki dramatik ölümünü konu almaktadır. Bu olay ülke gündemini uzun süre meşgul etmiş, olay tarihinden sonra konuyla ilgili sayısız haber yapılmıştır. Haberler, mesleğinde

umut vadeden bir geleceğe sahip olabilecek bir gencin uyuşturucu ile tanıştıktan sonra yaşamının seyirindeki değişiklik ile kısa sürede ölümle sonuçlanan yaşamı hakkında bilgi vermektedir. Verilen bilginin bir kısmı ölen manken tarafından tutulan günlüğe dayanırken bir kısmı olaya ilişkin ceza yargılamasına dayanmaktadır. Haberlerde, ölen mankenin bağlı olduğu mankenlik ajansının sahibi ve toplumda tanınmış bir kişi olan başvuruçunun ismi açık olarak yazılmış ve başvuruçunun hakkında bazı bilgilere de yer verilmiştir. Bu bilgiler; ölüm olayına ilişkin soruşturmada başvuruçunun önce tanık, sonra şüpheli sıfatıyla dinlenmesi, ölen mankenin başvuruçunun asistanı ile arasındaki ilişki, yine kamuoyunda tanınmış bir kişi olan başvuruçunun eşinin de aşırı dozda uyuşturucudan ölmüş olması hakkındadır.

39. Başvuruçunun; arama motorlarına ismi yazılarak yapılan aramada hem ölen manken ile hem de ölen eşi ile ilgili haberlerin çıktığını, bu haberler nedeniyle şeref ve itibarının zedelendiğini ileri sürerek internet içeriklerine erişimin engellenmesi talebinde bulunmuştur. İstanbul 2. Sulh Ceza Hâkimliği, başvuruçunun şeref ve itibarının korunması ile kamu yararı bağlamında yaptığı değerlendirme neticesinde söz konusu yayınların basın özgürlüğü kapsamında kaldığını belirterek talebin reddine karar vermiştir. Başvuruçunun anılan karara itirazı da reddedilmiştir.

40. Çelişmesiz bir dava sonucunda yayın içeriğine erişimin engellenmesi kararı verilebilmesinin ancak hukuka aykırılığın ve kişilik haklarına müdahalenin ilk bakışta anlaşılacak kadar belirgin olduğu ve zararın süratle giderilmesinin zaruri olduğu hâllerde mümkün olduğu hatırlanmalıdır (bkz. § 31). Bu yolun amacı; internet faaliyetleri ile kişilik hakları arasında gerekli hassas dengenin kurulmasını sağlamak, kişi ve kuruluşlara haksız zarar veren, onlar hakkında gerçek dışı bilgiler yayan ve şeref ve itibarlarını ihlal eden internet kullanımına karşı bireylerin haklarını korumaktır. O hâlde bu yol, basın özgürlüğünün ve basın mensuplarının haber verme ve eleştiri haklarının özüne dokunmayacak ve aynı zamanda hak sahibinin çıkarlarını koruyacak şekilde kullanılmalıdır.

41. Başvuruçunun internetten kaldırılmasını talep ettiği haberler 2004 yılına aittir. Başvuruçunun 2014 yılında erişimin engellenmesi talebinde bulunmuştur. Başvuruçunun kişisel verilerin işleme amacının dışında kullanıldığına yönelik bir şikâyeti de bulunmamaktadır. Dolayısıyla başvuruçunun, şeref ve itibarına yapılan müdahalenin çelişmeli bir yargılama yapılmadan, gecikmeksizin ve süratle bertaraf edilmesi ihtiyacını ortaya koyabilmiş değildir. Haber içeriklerinin incelenmesinden de içeriğe erişimin engellenmesi tedbirinin uygulanmasını gerektirecek ağırlıkta bir durum bulunmadığı görülmektedir.

42. Dahası başvuruçunun, açacağı çelişmeli bir hukuk davasında internet yayını kaldırma veya hazırlayacağı bir metni yayınlama imkânına da sahiptir. Dolayısıyla somut davada olduğu gibi

hukuka aykırılığın ve gerçek dışılığın çok belirgin olduğu ve zararın süratle giderilmesinin zaruri olduğu hâller dışında diğer ceza veya hukuk yollarının daha yüksek başarı şansı sunabilecek, kullanılabilir ve etkili başvuru yolları olduğu anlaşılmaktadır.

43. Yukarıda yer verilen tespitler çerçevesinde başvurucunun ortaya çıktığını iddia ettiği zararın giderimi için uyuşmazlığın esasına dair ve somut başvuru açısından koşullara göre sulh ceza hâkimliklerinin görevinde bulunan içeriğin yayından çıkarılması dışındaki daha etkili diğer koruma yollarına başvurmadığı anlaşıldığından Anayasa Mahkemesine bireysel başvuruda bulunabilmek için tüm başvuru yollarının tüketilmesi koşulunun yerine getirildiği söylenemez.

44. Açıklanan gerekçelerle başvurunun başvuru yollarının tüketilmemesi nedeniyle kabul edilemez olduğuna karar verilmesi gerekir.

Hicabi DURSUN ve Muammer TOPAL bu görüşe katılmamışlardır.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Kamuya açık belgelerde başvurucunun kimliğinin gizli tutulması talebinin KABULÜNE OYBİRLİĞİYLE,

B. Başvurunun başvuru yollarının tüketilmemesi nedeniyle KABUL EDİLEMEZ OLDUĞUNA Hicabi DURSUN ve Muammer TOPAL'ın karşıoyu ve OYÇOKLUĞUYLA,

C. Yargılama giderlerinin başvurucu üzerinde BIRAKILMASINA 15/3/2018 tarihinde karar verildi.

KARŞIOY GEREKÇESİ

Başvuru, isim yazılarak yapılan araştırmada arama motorlarında listelenen ve internet haber arşivlerinde yer alan bazı haberler ile ilgili içeriğe erişimin engellenmesi yönündeki taleplerin reddedilmesi nedeniyle şeref ve itibarın korunması hakkının ihlal edildiği iddiasına ilişkindir.

Başvurucu; sahibi olduğu mankenlik ajansında çalışan bir mankenin aşırı dozda uyuşturucudan ölmesi olayıyla ilgili medyada sayısız haber yapıldığını, bu haberlerde kendisi ile ilgili bilgilere de yer verildiğini ifade etmiştir. Başvurucu; yaşanan olaylarla bir ilgisi olmadığı halde arama motorlarına ismi yazıldığında hem ölen manken ile hem de kendisinin ölen eşi ile ilgili haberlerin listelendiğini, bu haberler nedeniyle şeref ve itibarının zedelendiğini iddia etmiştir. İnternet içeriklerine erişimin engellenmesi talebinin mahkemece reddedilmesi ve bunun sonucunda söz

konusu haber ve yazıların internet ortamında yer almaya devam etmesi nedeniyle özel hayatın gizliliği, şeref ve itibarın korunması ile adil yargılanma haklarının ihlal edildiğini ileri sürmüştür.

Somut olayda başvuru; arama motorlarına ismi yazılarak yapılan aramada hem ölen manken ile hem de ölen eşi ile ilgili haberlerin çıktığını, bu haberler nedeniyle şeref ve itibarının zedelendiğini ileri sürerek internet içeriklerine erişimin engellenmesi talebinde bulunmuştur. İstanbul 2. Sulh Ceza Hakimliği, başvuru sahibinin şeref ve itibarının korunması ile kamu yararı bağlamında yaptığı değerlendirme neticesinde söz konusu yayınların basın özgürlüğü kapsamında kaldığını belirterek talebin reddine karar vermiştir. Başvuru sahibinin anılan karara itirazı da reddedilmiştir. Diğer yollara başvurulmamıştır.

Unutulma hakkı Anayasa'mızda açıkça düzenlenmemiş olmakla birlikte Anayasa'nın "Devletin temel amaç ve ödevleri" başlığı altında düzenlenen 5. Maddesinde "insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak" ifadesi ile devlete pozitif bir yükümlülük yüklenmiştir. Bu yükümlülük bağlamında Anayasa'nın 17.maddesinde düzenlenen kişinin manevi bütünlüğü bağlamında şeref ve itibarının korunması hakkı ve Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı ile birlikte düşünüldüğünde, devletin bireye geçmişte yaşadıklarının başkaları tarafından öğrenilmesi engellenerek "yeni bir sayfa açma" olanağı verme hususunda bir sorumluluğu olduğu açıktır. Özellikle kişisel verilerin korunması hakkı kapsamında kişisel verilerin silinmesini talep edebilme hakkı, kişilerin geçmişlerinde yaşadıkları olumsuzlukların unutulmasına imkan tanımayı kapsamaktadır. Dolayısıyla Anayasa'da açıkça düzenlenmeyen unutulma hakkı, internet vasıtasıyla ulaşılması kolay olan ve dijital hafızada bulunan haberlere erişimin engellenmesi için Anayasa'nın 5., 17. ve 20. maddelerinin doğal bir sonucu olarak karşımıza çıkmaktadır. Diğer taraftan unutulma hakkının kabul edilmemesi, internet vasıtasıyla kolayca ulaşılabilir ve uzun süre muhafaza edilebilir kişisel veriler nedeniyle başkaları tarafından kişiler hakkında ön yargı oluşturabilmesi nedeniyle manevi varlığının geliştirilmesi için gerekli onurlu bir yaşam sürdürmesine ve manevi bağımsızlığına müdahaleyi sürekli kılmaktadır (N.B.B., B. No: 2013/5653, 3/3/2016, § 47).

Bireyin kişisel şeref ve itibarı, Anayasa'nın 17. maddesinde yer alan "manevi varlık" kapsamında yer almaktadır. Devlet, bireyin manevi varlığının bir parçası olan kişisel şeref ve itibara keyfi olarak müdahale etmemek ve üçüncü kişilerin saldırılarını önlemekle yükümlüdür (Adnan Oktar (2), B. No: 2013/1123, 2/10/2013, § 33). Kamusal bir tartışma bağlamında ve yayımlanan yazılar nedeniyle eleştirilmiş olsa bile bir kişinin itibarı, kimliğinin ve manevi bütünlüğünün bir parçasını oluşturur

(Pfeifer/Avusturya, § 35) ve Anayasa'nın 17. maddesinin birinci fıkrasının koruması altındadır (Kadir Sağdıç, § 38; İlhan Çihaner (2), § 44).

AİHM de kişisel şeref ve itibara yapılan müdahaleleri Avrupa İnsan Hakları Sözleşmesi'nin "özel ve aile yaşamına, konuta ve haberleşmeye saygı hakkı" kenar başlıklı 8. maddesi kapsamında değerlendirmektedir. AİHM'e göre kişisel itibarın korunması hakkı, Sözleşme'nin 8. maddesi tarafından korunan özel yaşama saygı hakkının bir parçasıdır (Pfeifer/Avusturya, B.No: 12556/03, 15/11/2007 § 35;Axel SpringerAGIAİmanyada, B.No: 39954/08 7/2/2012, § 83).

Unutulma hakkı internet ortamında bir haberin, uzun süredir kolayca ulaşılabilir olması nedeniyle kişinin şeref ve itibarını zedeleyen bir hâle dönüşmesi durumunda karşımıza çıkmaktadır. Bu hakkın amacı, internetin yaygınlaşması ve sağladığı imkanlar nedeniyle ifade ve basın özgürlükleri ile kişilerin manevi varlığının geliştirilmesi hakkı arasında gerekli hassas dengenin kurulmasını sağlamaktır. O hâlde bu yol, internet ortamında haber arşivini koruma altına alan basın özgürlüğünün ve halkın haber ve fikirlere ulaşma özgürlüğünün özüne dokunmayacak ve aynı zamanda hak sahibinin çıkarlarını koruyacak şekilde kullanılmalıdır (N.B.B., § 70).

Anayasa'nın 148. maddesinin dördüncü fıkrası ile 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 45. maddesinin (2) numaralı fıkrasında, bireysel başvuruda bulunulmadan önce ihlal iddiasının dayanağı olan işlem, eylem ya da ihmâl için kanunda öngörülmüş olan idari ve yargısal başvuru yollarının tamamının tüketilmiş olması gerektiği belirtilmiştir. Temel hak ihlallerini öncelikle derece mahkemelerinin gidermekle yükümlü olması, kanun yollarının tüketilmesi koşulunu zorunlu kılar (Necati Gündüz ve Recep Gündüz, B. No: 2012/1027, 12/2/2013, §§ 19, 20).

Ancak belirtilen hükümlerde yer verilen olağan başvuru yolları ibaresinin, başvuru yollarının şikayetleri açısından makul bir başarı şansı sunabilecek ve bir çözüm sağlayabilecek nitelikte, kullanılabilir ve etkili başvuru yolları olarak anlaşılması gerekmektedir. Ayrıca başvuru yollarının tüketme kuralı ne mutlak ne de şekli olarak uygulanabilir bir kural olup bu kurala riayetinin denetlenmesinde münferit başvurunun koşullarının dikkate alınması esastır. Bu anlamda hukuk sisteminde yalnızca birtakım başvuru yollarının varlığının değil aynı zamanda bunların uygulanma şartları ile başvuru yollarının kişisel koşullarının gerçekçi bir biçimde ele alınması gerekmektedir. Bu nedenle başvuru yollarının tüketilmesi noktasında kendilerinden beklenebilecek her şeyi yerine getirip getirmediği incelenirken başvurunun özellikleri dikkate alınmalıdır (S.S.A., B. No: 2013/2355, 7/11/2013, § 28).

O hâlde somut başvuruda devletin pozitif yükümlülüğünün, sulh ceza mahkemelerinin yetkisinde bulunan internet içeriklerine erişimin engellenmesini gerekli kılıp kılmadığı değerlendirilmelidir. Başka bir deyişle sulh ceza mahkemeleri nezdinde bulunan içeriğin yayından çıkarılması ve erişimin engellenmesi yolunun şeref ve itibar hakkının korunmadığı yönündeki şikayetler açısından makul bir başarı şansı sunabilecek ve bir çözüm sağlayabilecek nitelikte kullanılabilir ve etkili bir başvuru yolu olup olmadığı tespit edilmelidir.

Hukuk sistemimizde internet içeriğinin yayından çıkarılmasının, başvurudaki gibi sulh ceza hakimliklerine başvurmak suretiyle veya hukuk mahkemelerinde açılacak dava yolu ile gerçekleştirilmesi mümkündür (Ahmet Oğuz Çinko ve Erkan Çelik [GK], B. No: 2013/6237, 2/7/2015). Ancak somut başvuruda, arama motorlarına ismi yazılarak yapılan aramada hem ölen manken hem de ölen eşi ile ilgili haberlerin çıktığı, haber arşivleri üzerinden olayca ulaşılabildiği; bu şekilde başvurucunun şeref ve itibarını koruma bakımından müdahalenin çok uzun süredir devam ettiği gözetilerek; başvurucunun şeref ve itibar hakkının ve kişisel verilerinin korunmasının, bu yayının bir an önce kaldırılması ile sağlanacağı değerlendirildiğinde, sulh ceza hakimliğine başvuru yolunun somut olayın koşulları açısından etkili bir yol olduğu kabul edilmelidir. Nitekim hukuk mahkemelerinde çekişmeli bir yargılama yolunun, somut olaydaki şeref ve itibarın korunması hakkına yönelik uzun süredir devam eden müdahalenin gecikmeksizin ve süratle bertaraf edilmesi ihtiyacını karşılayabileceği söylenemez (Türkiye İş Adamları ve Sanayiciler Konfederasyonu, B. No: 2014/8691,6/10/2015, § 22; N.B.B., § 27).

Başvurucunun manevi varlığına internet haberleri yoluyla (bkz. § 11) yapılan müdahalenin, önceki kararımızdaki başvurucuya aynı yolla yapılan müdahaleden (N.B.B., § 9) daha hafif olduğu değerlendirilemez. Anayasa Mahkemesi sözü edilen kararında, internet ortamının sağladığı ulaşılabilirlik, yaygınlık, haber ve fikirlerin depolanmasındaki ve muhafazasındaki kolaylık dikkate alındığında, yayımlandığı tarihte belirli ağırlık eşiğini aşmayan veya kişinin kendi eylemlerinden kaynaklanan haber ve yazıların internet ortamında uzun süre erişilebilir kalması halinde kişilerin şeref ve itibarının zedelenebileceğini belirtmiş ve bu durumu unutulma hakkı kapsamında incelemiştir. O halde internet ortamında uzun süre erişilebilir durumda kalan ve manevi varlığın daha fazla örselendiği bu olayda da önceki kararımızdan ayrılmayı gerektiren bir durum bulunmamaktadır.

Başvurucunun arama motorlarında listelenen ve internet haber arşivlerinde yer alan bazı haberler ile ilgili içeriğe erişimin engellenmesi yönündeki taleplerinin reddedilmesi nedeniyle kişilik haklarının zarar gördüğüne ve Anayasa'nın 17. maddesinin ihlal edildiğine ilişkin şikayetleri açıkça dayanaktan

yoksun değildir. İstanbul 2. Sulh Ceza Hakimliğinin kararına itiraz edilmek suretiyle başvuru yolları da tüketilmiş durumdadır. Ayrıca başka bir kabul edilemezlik nedeni de bulunmadığından başvurunun kabul edilebilir olduğuna karar verilmesi gerekir.

Açıklanan nedenlerle çoğunluğun kararına katılmıyoruz.

Üye

Hicabi DURSUN

Üye

Muammer TOPAL

ÖZEL HAYAT HAKKI VE KAPSAMI KONUSUNDA FARKLI GEREKÇE

1. Başvuranın 2004 yılında meydana gelen bir olayla ilgili olarak internet arama motorlarında halen ismi geçtiği için haber içeriğine erişimin engellenmesi isteminin reddedilmesi nedeniyle şeref ve itibar hakkının ihlal edildiğine ilişkin başvurusu Mahkeme çoğunluğu tarafından Anayasa'nın 17/1. maddesinde düzenlenen "maddi ve manevi varlığını koruma ve geliştirme hakkı" çerçevesinde incelenmiştir. Kararda ulaşılan kabul edilemezlik sonucuna ve gerekçesine iştirak etmekle birlikte, aşağıda açıklanan gerekçelerle konunun incelendiği anayasal dayanak konusunda farklı düşünmekteyim.

2. Öncelikle, Anayasa'nın 148/3. maddesi uyarınca, Mahkememizin konu bakımından yetkisine girebilmesi için, bireysel başvuruya konu hakkın AİHS veya Türkiye'nin taraf olduğu ek protokollerden birine girmesi gerekmektedir. Bu nedenle bireysel başvuruya konu hakkın Sözleşme kapsamına girip girmediğinin belirlenmesi gerekmektedir. Mahkememiz kararında başvurunun Anayasa'nın 17/1. maddesi kapsamına girdiği belirtilmiş, fakat Sözleşmeyle ortak konuyu tespit bakımından hangi hakka ilişkin olduğundan söz edilmemiştir (bkz. par. 20-23).

3. AİHS'nin 8. maddesinde özel hayata saygı hakkı düzenlenmiştir. Kişinin iyi bir itibara sahip olma hakkı, nam, şeref, şöhret, isim, resim vb. manevi varlıkları ile 'fiziksel ve zihinsel/ruhsal bütünlüğü' üzerindeki hakları Sözleşmenin 8. maddesi çerçevesinde özel hayata saygı hakkı içerisinde değerlendirilmektedir. (özellikle itibar, şeref, şöhret hakkı yönünden bkz. AİHM Chauvy/Fransa, par. 70; Abeberry/Fransa; Leempoel ve S.A. Ed. Cine Revue/Belçika, par. 67; Minelli/İsviçre, No: 14991/02; A./Norveç, No: 28070/06, par. 64; Osman Doğru-Atilla Nalbant, AİHS Açıklama ve Önemli Kararlar, Ankara 2013, s. 41) İfade özgürlüğü yönünden yapılan başvurularda da muhatabın Sözleşmenin 8.

maddesi kapsamındaki şöhreti ve onurunun korunması meşru müdahale nedeni olarak kabul edilmekte ve hakların dengelenmesi açısından değerlendirilmektedir (Shabanov ve Tren/Rusya, 2006, par. 46; Hachette Filipachi Associes/Fransa, 2007, par. 43; DJ. Harris/M.O'Boyle/E.P. Bates/C.M. Buckley, Avrupa İnsan Hakları Sözleşmesi Hukuku, 2013, s. 493).

4. Bilindiği üzere özel hayata saygı ve gizliliğinin korunması hakkı Anayasa'nın 20/1. maddesinde düzenlenmektedir. Özel hayata saygı hakkının kapsamında bulunduğu şüphe olmayan kişinin itibar, nam, şöhret ve şerefi üzerindeki haklarının da anılan 20/1. madde içerisinde değerlendirilmesi gerektiği açıktır.

5. Buna karşın heyetimiz çoğunluğunun konunun 17/1. madde kapsamında incelenmesi gerektiğine ilişkin bu yaklaşımı, Anayasa'nın 20. maddesinde düzenlenen özel hayata saygı hakkının kapsamını daralttığı gibi, temel kişilik haklarının tümünün kendinden neşet ettiği "varlığını koruma ve geliştirme hakkını" içeren 17/1. maddedeki genel nitelikli kişilik hakkını özel hayatın spesifik bir alanına hapsedmektedir.

6. Çoğunluğun dayandığı Anayasa'nın 17/1. maddesinde; "Herkes, yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkına sahiptir" denilmektedir. Madde gerekçesinde bu fıkra hakkında; "Kişinin sahip olduğu hak ve hürriyetler bu maddeden itibaren önem dereceleri göz önünde tutularak belirlenmiştir. Bu madde ile yaşama, maddi ve manevi varlığın bütünlüğü ve bunun geliştirilmesi hakkı korunmaktadır." izahatı yapılmıştır. Gerekçedeki açıklamadan, bu fıkra ile birbirini tamamlayan iki ayrı hakkın düzenlendiği anlaşılmaktadır. Diğer taraftan aynı maddenin 2. fıkrasında vücut bütünlüğünün dokunulmazlığı hakkı, 3. fıkrasında ise işkence ve kötü muamele yasakları yer almaktadır.

7. Kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı öyle anaç bir haktır ki, Anayasa'da özel olarak sayılan bütün temel hakların ondan doğduğu, onun türevi olduğu söylenebilir. Anayasa'da düzenlenen temel hakları hatırlayalım; zorla çalıştırma yasağı (m.18), kişi hürriyeti ve güvenliği (m.19), konut dokunulmazlığı (m.21), haberleşme hürriyeti (m.22), yerleşme ve seyahat hürriyeti (m.23), din ve vicdan hürriyeti (m.24), düşünce ve kanaat hürriyeti (m.25), düşünceyi açıklama ve yayma hürriyeti (m.26), bilim ve sanat hürriyeti (m.27), basın hürriyeti (m.28), dernek kurma hürriyeti (m.33), toplantı ve gösteri yürüyüşü düzenleme hakkı (m.34), mülkiyet hakkı (m.35), hak arama hürriyeti ve adil yargılanma hakkı (m.36), ailenin korunması ve çocuk hakları (m.41), eğitim ve öğrenim hakkı (m.42), çalışma ve dinlenme hakları (m.49, 50), sendika kurma hakkı (m.51), ücrette adalet hakkı (m.55), sağlık ve çevre hakkı (m.56), seçme, seçilme ve siyasi faaliyet hakkı (m.67),

dilekçe ve bilgi edinme hakkı (m.74). Düşüncemize göre kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı, yukarıda sayılan hakların her birinin içinde yer almaktadır.

8. Bu durumda Anayasa'nın 17/1. maddesinde düzenlenen hakkın anayasal niteliğinin belirlenmesi gerekmektedir. Doktrinde Gören, 17/1. maddedeki hakkın hiyerarşik olarak temel teşkil ettiğini ve bu hakkın kişiye 'genel nitelikte bir eylem özgürlüğü' tanıyan sübjektif bir kamu hakkı niteliğinde olduğunu ifade etmiştir. Yazar ayrıca bütün temel hakların bu hakkın sonuçları olduğunu belirtmektedir (Prof. Dr. Zafer Gören, Anayasa Hukuku, Ankara 2006, s. 412, 413). Diğer bazı yazarlarca da benimsenen bu nitelenmenin Anayasa'nın sistemi açısından oldukça yerinde olduğu düşünülmelidir. Sağlam ise, Federal Alman Anayasasının 2/1. maddesinde de düzenlenen kişiliğini geliştirme hakkının düzenlenmesinin amacının, insan yaşamının Anayasa'da öngörülen diğer temel haklar dışında kalan bölümünü de kapsayarak, eksiksiz bir temel hak güvencesini temin etmek olduğuna dikkat çekmektedir. Sağlam'ın işaret ettiği üzere kişiliği geliştirme hakkı ile diğer temel haklar arasında özel-genel hüküm ilişkisi bulunduğundan, bir insan eylemi Anayasa'daki temel haklardan birinin geçerlik alanına girmekteyse yalnızca özel nitelikli olan temel hak uygulanır. Dolayısıyla kişiliği geliştirme hakkı, diğer temel haklarla düzenlenmemiş olan tüm hakları kapsayan 'genel bir fiil özgürlüğü' niteliğindedir (Doç. Dr. Fazıl Sağlam, Temel Hakların Sınırlanması ve Özü, AÜSBFY Ankara 1982, s. 42).

9. Doktrinde diğer bazı yazarlar da Anayasa'daki maddi ve manevi varlığını koruma ve geliştirme hakkının genel fiil özgürlüğü niteliğinde olduğu ve Anayasa'da sayılan temel haklar ile arasında özel-genel hüküm ilişkisi bulunduğu görüşünü paylaşmaktadırlar (bkz. Doç. Dr. Ali Tarık Gümüş, "Türk Anayasasında Kişinin Maddi ve Manevi Varlığını Koruma ve Geliştirme Hakkı", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Cilt 13, Sayı 2, Yıl 2005, s. 149; Dr. Oğuz Şimşek, Anayasa Hukukunda İnsan Onuru Kavramı ve Korunması, Basılmamış Doktora Tezi, İzmir 1999, s. 55) Bu yazarlardan Gümüş, madde gerekçesinde 17. maddeden itibaren hak ve hürriyetlerin önem derecesine göre sıralandığına ilişkin açıklama ile kastedilen hususun, varlığını koruma ve geliştirme hakkının temel haklardan biri ve en önemlisi olduğu değil, bu hakkın diğer haklara kaynaklık ettiğini izah anlamına geldiğini ifade etmektedir (agm. s. 153).

10. Daha önce belirtildiği gibi kişinin maddi ve manevi kişilik değerleri içerisinde olan şeref, itibar, isim, resim, vücudu, vb. hakları Anayasa'nın 20. maddesinde düzenlenen özel hayata saygı ve gizliliğinin korunması hakkı kapsamındadır. Belirtilen kişilik değerlerine yönelik bir saldırıya karşı korunma hakkı ile bu değerlerini geliştirmeye yönelik hakları da anılan hakkın içerisindedir. Başka

bir ifadeyle, bireyin kişiliğini (maddi-manevi varlığını) koruma ve geliştirme hakkı özel hayattan ayrılamaz niteliktedir.

11. Diğer taraftan, konut dokunulmazlığına, haberleşmeye, yerleşme ve seyahat özgürlüğüne, düşünce açıklama veya bilim sanat yapma ve yayma özgürlüğüne karşı yapılacak müdahaleler de özünde kişiliğini koruma ve geliştirme hakkının ihlali mahiyetinde olmakla birlikte, Anayasa'da özel olarak düzenlenmesi dolayısıyla 21. ila 27. maddeler kapsamında incelenmesi gerekmektedir. Bölüm çoğunluğunun dayandığı görüşün bu konulara yansıtılması durumunda, belirtilen hakların da 17/1. madde üzerinden incelenmesi gerekecek, böylece Anayasada özel olarak düzenlenen ilgili temel hakların alanı daraltılırken, genel kapsamlı olan kişiliği koruma-geliştirme hakkı, amacı dışında ve anayasal sistematığe aykırı biçimde kullanılmış ve genişletilmiş olacaktır.

12. Sonuç olarak, Anayasa'nın 20. maddesinde özel olarak düzenlenen özel hayata saygı hakkı, maddi ve manevi varlığa (ve bu arada şeref ve itibara) yönelik müdahaleleri de kapsamaktadır. Anayasa'nın 17/1. maddesindeki "maddi ve manevi varlığı koruma ve geliştirme hakkı" özel hayat hakkını değil, tüm temel hakların özünü ve ideal formunu düzenlemektedir. Anayasa'nın, kişinin maddi-manevi varlığına farklı bağlamlarda yer veren 5, 12, 15/2 ve 17/1,2. maddeleri, ilgili özel/temel hak bağlamında yalnızca destek norm olarak değerlendirilmelidir. Ne var ki başvuru konusu olay ölçü norm olan 20. madde üzerinden incelenmesi gerekirken, Anayasa'nın genel nitelikli 17/1. maddesi çerçevesinde değerlendirilmiştir.

Belirtilen nedenlerle "başvuru yollarının tüketilmemesi nedeniyle kabul edilemez olduğu" şeklindeki karar sonucuna, konunun Anayasa'nın 20/1. maddesinde düzenlenen özel hayata saygı hakkı kapsamında incelenmesi gerektiği yolundaki farklı gerekçeyle katılmış bulunmaktayım.

Hasan Tahsin GÖKCAN

Anayasa Mahkemesi - Asli Alp ve Şükrü Alp (Unutulma Hakkı) Kararı (2014/18260)

Asli Alp ve Şükrü Alp, B. No: 2014/18260, 4/10/2017

Başvuru, internet haber arşivlerinde erişilebilir durumda olan haber ile ilgili içeriğin yayından kaldırılması yönündeki talebin reddedilmesi nedeniyle şeref ve itibarın korunması hakkının ihlal edildiği iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

İKİNCİ BÖLÜM

KARAR

ASLİ ALP VE ŞÜKRÜ ALP BAŞVURUSU

(Başvuru Numarası: 2014/18260)

Karar Tarihi: 4/10/2017

İKİNCİ BÖLÜM

KARAR

Başkan: Engin YILDIRIM

Üyeler: Serdar ÖZGÜLDÜR, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ

Raportör Yrd.: Derya ATAKUL

Başvurucular: 1. Asli ALP; 2. Şükrü ALP

Vekili: Av. Sevil ARACI BEK

I. BAŞVURUNUN KONUSU

1. Başvuru, internet haber arşivlerinde erişilebilir durumda olan haber ile ilgili içeriğin yayından kaldırılması yönündeki talebin reddedilmesi nedeniyle şeref ve itibarın korunması hakkının ihlal edildiği iddiasına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 20/11/2014 tarihinde yapılmıştır.

3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.

4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.

5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.

III. OLAY VE OLGULAR

6. Başvuru formu ve eklerinde ifade edildiği şekliyle olaylar özetle şöyledir:

7. Millî Eğitim Bakanlığına (MEB) bağlı bir eğitim kurumunda öğretmen olarak çalışan bir kişi 8/9/2009 tarihinde başvurucuların ikâmetgahında ölü olarak bulunmuştur.

8. Kahramanmaraş Cumhuriyet Başsavcılığının 27/10/2009 tarihli iddianamesiyle, olay tarihinde MEB'e bağlı bir eğitim kurumunda öğretmen olan başvurucu Asli Alp hakkında kasten adam öldürmeye yardım; eşi başvurucu Şükrü Alp hakkında kasten adam öldürme suçlarından kamu davası açılmıştır. Kahramanmaraş 2. Ağır Ceza Mahkemesi 20/9/2011 tarihinde başvurucu Asli Alp'in cezalandırılmasına yeter derecede kesin, inandırıcı ve her türlü şüpheden uzak delil elde edilemediğinden müsnet suçtan beraatine, başvurucu Şükrü Alp'in üzerine atılı suçu işlediği sabit olduğundan on yıl hapis cezası ile cezalandırılmasına karar verilmiştir. Karar Yargıtay 1. Ceza Dairesinin 12/11/2012 tarihli ilamı ile onanmıştır.

9. Bir öğretmenin ölümüyle sonuçlanan olaydan sonra bazı internet haber siteleri ile birkaç gazetenin İnternet sayfasında başvurucuların sanık sıfatıyla yargılandıkları ceza yargılamasına yönelik haberler yapılmıştır. Yapılan haberlerde "Yasak aşk cinayetine 10 yıl hapis", "Birçok kez cinsel ilişkiye girdim", "Yasak aşk cinayetinin zanlıları hakim karşısında", "Öğretmenin katili sevgilisinin eşi çıktı", "Cinsel ilişkiye girdim, dost hayatı yaşamadık" gibi başlıklar kullanılmış; haber içeriklerinde başvurucuların ceza yargılaması esnasında alınan savunmalarına, yargılama sürecine ve sonucuna ilişkin bilgilere yer verilmiştir.

10. Başvurucular; geçmişte yaşanan bu olayın izlerini silerek yeni bir hayat kurmak istediklerini, haberlerin güncelliğini yitirdiğini ancak yayınlanmaya devam edilmesi nedeniyle kişilik haklarının zedelendiğini ileri sürerek 15/9/2014 tarihinde haber içeriklerine erişimin engellenmesi talebinde bulunmuşlardır. Adana 5. Sulh Ceza Hâkimliği 16/9/2014 tarihli kararı ile erişimin engellenmesi talebinin reddine karar vermiştir. Hâkimlik; gerekçeli kararında, bahse konu haberlerin yayımlanmasında kamu yararı bulunduğunu, topluma mal olan kişilerle siyasal ve idari yaşam içinde

yer alan kişilerin hayatlarının toplumu ilgilendirdiğini, okuyucunun ilgisini çekebilmek amacıyla haberi ilginç biçime getirmenin basın hakkı ve görevi olduğunu belirtmiştir. Hâkimlik, yapılan yayınların haber niteliğinde olduğuna, yayınların içeriği bütüncül olarak değerlendirildiğinde hukuka uygunluk sınırları içinde ve basın özgürlüğü kapsamında kaldığına karar vermiştir.

11. Başvurucuların anılan karara itirazı Adana 1. Sulh Ceza Hâkimliğinin 13/10/2014 tarihli kararı ile reddedilmiştir.

12. Karar başvuruculara 22/10/2014 tarihinde tebliğ edilmiştir. Başvurucular 20/11/2014 tarihinde bireysel başvuruda bulunmuşlardır.

IV. İLGİLİ HUKUK

13. Anayasa Mahkemesinin 3/3/2016 tarihli ve 2013/5653 numaralı N.B.B. Kararı.

V. İNCELEME VE GEREKÇE

14. Mahkemenin 4/10/2017 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucuların İddiaları

15. Başvurucular, bazı internet haber siteleri ile birkaç gazetenin internet sayfasında bir kişinin ölümüyle sonuçlanan olay ve bu olay nedeniyle sanık sıfatıyla yargılandıkları davaya ilişkin haberler yapıldığını belirtmişlerdir. Başvuruculardan Asli Alp, öğretmen olarak çalışmaya devam ettiğini ve hakkında yayımlanmaya devam eden haberlerin eğitim camiası ve sosyal yaşam içinde kendisini rencide ettiğini; başvuruculardan Şükrü Alp kasten adam öldürme suçundan çekmekte olduğu cezanın bitmek üzere olduğunu ve yakın zamanda tahliye edileceğini ifade etmiştir. Başvurucular; ortak bir çocukları olduğunu, geçmişte yaşanan bu acı olayın izlerini silerek yeni bir hayat kurmak istediklerini, internet içeriklerine erişimin engellenmesi taleplerinin mahkemece reddedildiğini, haberlerin internet ortamında yer almaya devam etmesi nedeniyle özel hayatın gizliliği, şeref ve itibarın korunması ile adil yargılanma haklarının ihlal edildiğini ileri sürmüşlerdir.

B. Değerlendirme

16. Anayasa Mahkemesi, olayların başvurucular tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Başvurucular, haklarında yayımlanan haberlerin internet ortamında yer almaya devam etmesi nedeniyle kişilik haklarının zedelendiğinden şikâyet etmektedirler. Başvurucuların bu şikâyeti şeref ve itibarın korunması hakkı kapsamında incelenmiştir.

17. Bireyin kişisel şeref ve itibarı, Anayasa'nın 17. maddesinde yer alan "manevi varlık" kapsamında yer almaktadır. Devletin, bireyin manevi varlığının bir parçası olan kişisel şeref ve itibara keyfi olarak müdahale etmemek şeklinde negatif yükümlülüğü ve üçüncü kişilerin saldırılarını önlemek şeklinde pozitif yükümlülüğü bulunmaktadır (Adnan Oktar (3), B. No: 2013/1123, 2/10/2013, § 33). Şeref ve itibarı etkileyen saldırılar veya basın ve yayın yolu ile yapılan yayınlara karşı bireyin korunmaması hâlinde Anayasa'nın 17. maddesinin birinci fıkrası ihlal edilmiş olabilir (Kadir Sağdıç [GK], B. No: 2013/6617, 8/4/2015, § 36; İlhan Cihaner (2), B. No: 2013/5574, 30/6/2014, § 42).

18. Anayasa'nın "Düşünceyi açıklama ve yayma hürriyeti" kenar başlıklı 26. maddesine göre herkes düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Anılan maddede ifade özgürlüğünün kullanımında başvurulabilecek araçlar "söz, yazı, resim veya başka yollar" olarak ifade edilmiş ve "başka yollar" ifadesiyle her türlü ifade aracının anayasal koruma altında olduğu gösterilmiştir (Emin Aydın, B. No: 2013/2602, 23/1/2014, § 43).

19. Haber ve fikirlerin iletilmesinde ve alınmasında önemli bir işlev gören internet, Anayasa'nın 26. maddesinde düzenlenen ifade özgürlüğünün güvencesi altındadır. Nitekim Anayasa Mahkemesi, internet erişimine yönelik bir müdahalenin ifade özgürlüğü kapsamında incelenmesi gerektiğini kabul etmiştir (Yaman Akdeniz ve diğerleri, B. No: 2014/3986, 2/4/2014; Youtube LLC Corporation Service Company ve diğerleri [GK], B. No: 2014/4705, 29/5/2014).

20. Anayasa Mahkemesi birçok kararında ifade özgürlüğünün sadece düşünce ve fikirleri yayma özgürlüğünü değil haber ve fikirlere ulaşma özgürlüğünü de kapsadığını vurgulamıştır (Emin Aydın, § 40; Kamuran Reşit Bekir [GK], B. No: 2013/3614, 8/4/2015, § 34). İnternet üzerinde arşiv oluşturma, aktüalitenin ve haberlerin saklanmasına ve erişilebilirliğine büyük ölçüde hizmet etmektedir. Bu nitelikteki arşivler özellikle doğrudan halkın erişimine açık ve genelde ücretsiz olmaları nedeniyle tarih eğitimi ve araştırma faaliyetleri için kaynak sunmaktadır. Öte yandan demokratik bir toplumda basının ilk işlevi olan "gözetleyici" rolünün bir sonucu da arşivlerin halkın erişimine sunulmasıdır. Bu nedenle internette tutulan arşivlerin ifade ve basın özgürlükleri kapsamında olduğu açıktır. Dolayısıyla internette yayınlanan ve gazetecilik faaliyeti kapsamında kabul edilen bir haber arşivinin yayından kaldırılması basın özgürlüğüne yönelik bir müdahale teşkil edebilir (N.B.B., B. No: 2013/5653, 3/3/2016, § 61).

21. İfade özgürlüğü ile onu tamamlayan ve ifade özgürlüğünün kullanılmasını sağlayan basın özgürlüğü, Anayasa'da yer alan temel hak ve özgürlükleri sınırlama rejimine tabidir. Anayasa'nın 26.,

27. ve 28. maddelerinde sayılan sınırlandırmalardan biri, "başkalarının şöhret veya haklarının, özel veya aile hayatlarının" korunmasıdır (Kadir Sağdıç, § 55; İlhan Cihaner (2), § 62). Öte yandan "başkalarının şöhret veya haklarının, özel veya aile hayatlarının" korunması bağlamında şeref ve itibarın korunması hakkının etki alanını genişletmenin ifade ve basın özgürlüklerinin ihlali sonucunu doğurabileceği hatırdta tutulmalıdır.

22. Bu sebeple Anayasa'nın 17. maddesinin birinci fıkrasında koruma altına alınan şeref ve itibarın korunmasını isteme hakkı ile başvuruya konu internet haber arşivlerinin Anayasa'nın 28. maddesinde güvence altına alınan basın özgürlüğü ve bu özgürlükle bağlantılı olarak Anayasa'nın 26. maddesinde güvence altına alınan ifade özgürlüğü arasında Anayasa Mahkemesi içtihadında ortaya konulan kriterlere uygun şekilde bir denge kurulması gerekmektedir. İnternet ortamının sağladığı ulaşılabilirlik, yaygınlık, haber ve fikirlerin depolanmasındaki ve muhafazasındaki kolaylık dikkate alındığında yayımlandığı tarihte belirli ağırlık eşiğini aşmayan veya kişinin kendi eylemlerinden kaynaklanan haberlerin internet ortamında uzun süre erişilebilir kalması kişilerin şeref ve itibarını zedeleyebilir (N.B.B., § 37).

23. Anayasa Mahkemesi 3/3/2016 tarihli ve 2013/5653 numaralı N.B.B. başvurusunda internetin etkin olarak kullanılmasıyla beraber ifade ve basın özgürlükleri ile şeref ve itibarın korunması arasındaki dengenin ilki lehine bozulduğunu, bu dengenin tekrar kurulabilmesinin şeref ve itibar yönünden bireylerin unutulma hakkının kabul edilmesi ile mümkün olabileceğini belirtmiştir (N.B.B., § 46).

24. Anayasa Mahkemesi bahsi geçen başvuruda unutulma hakkının anayasal dayanaklarına yer vererek devletin bireye geçmişte yaşadıklarının başkaları tarafından öğrenilmesi engellenerek "yeni bir sayfa açma" olanağı verme hususunda bir sorumluluğu olduğunu, dolayısıyla unutulma hakkının kişilerin manevi varlıklarını geliştirmelerine bir fırsat vermek açısından devletin pozitif yükümlülüğünün bir sonucu olduğunu ortaya koymuştur (N.B.B., §§ 47-49).

25. Bununla birlikte Mahkeme, unutulma hakkının internet üzerindeki her türlü haber veya yazı yönünden uygulanmasını beklemenin mümkün olmadığını; özellikle basın özgürlüğü temelinde gazete arşivinin araştırmacılar, hukukçular veya tarihçiler için önem taşıyan veriler olduğunu belirtmiştir. Unutulma hakkı, internet ortamında haber arşivini koruma altına alan basın özgürlüğünün ve halkın haber ve fikirlere ulaşma özgürlüğünün özüne dokunmayacak ve aynı zamanda hak sahibinin çıkarlarını koruyacak şekilde kullanılmalıdır. Mahkeme, internet ortamındaki bir haber veya yazının unutulma hakkı kapsamında internette çıkarılabilmesi için yayının içeriği, yayında kaldığı süre, güncelliğini yitirme, tarihsel bir veri olarak kabul edilememe, kamu yararına katkısı (toplumsal açıdan haberin değeri, haberin geleceğe ışık tutan niteliği) haber veya yazıya konu

kişinin siyasetçi veya ünlü olup olmadığı, haber veya yazının konusu, bu bağlamda haber ya da yazının olgusal gerçekler veya değer yargısı içerip içermediği, halkın ilgili veriye yönelik ilgisi gibi hususların somut olay açısından incelenmesi gerekliliğini ortaya koymuştur (N.B.B., § 50).

26. Somut olayda başvurucuların şikâyetine konu olan haberler, olay tarihi olan 8/9/2009 tarihinden sonra yayınlanmış ve arşiv niteliğindedir. Haberlerin konusu o tarihte işlenen bir cinayete ilişkindir. Haber içerikleri incelendiğinde cinayet sebebi olarak meslektaş olan maktul ile failin eşi arasındaki yasak aşk ilişkisinin gösterildiği, haber başlıklarında maktul ile failin eşi arasındaki ilişkiyi ön plana çıkaracak ifadelerin kullanıldığı görülmektedir. Haberlerde, ölüm olayına ilişkin ayrıntıların ise sanıklar ile görgü tanıklarının soruşturma ve kovuşturma aşamalarındaki ifadelerinden yola çıkılarak aktarıldığı tespit edilmiştir. Haberlerin başlıkları ile içerikleri incelendiğinde amacın kamuoyunun ilgisine matuf, MEB'e bağlı eğitim kurumlarında çalışan iki öğretmenden birinin, kadın öğretmenin eşi tarafından öldürülmesi olayı hakkında kamuoyunu bilgilendirmek olduğu görülmektedir. Başvurucular, bu haberlerin gerçeğe aykırı veya uydurma haberler olduğunu ileri sürmemişlerdir. Derece mahkemelerince de başvurucuların savunmaları, tanık beyanları, iletişim tespit tutanakları, bilirkişi raporları ve tüm dosya kapsamı incelenerek başvurucu Şükrü Alp'in kasten adam öldürme suçundan on yıl hapis cezası ile cezalandırılmasına, başvurucu Asli Alp'in cezalandırılmasına yeter derecede kesin, inandırıcı ve her türlü şüpheden uzak delil elde edilemediğinden müsnet suçtan beraatine karar verilmiştir.

27. Başvurucular, kendileri hakkında yayımlanan haberlerden beş yıl sonra 15/9/2014 tarihinde haber içeriklerine erişimin engellenmesi talebiyle Adana 5. Sulh Ceza Hâkimliğine başvuruda bulunmuşlardır. Hâkimlik, başvurucuların şeref ve itibarının korunması ile kamu yararı bağlamında yaptığı değerlendirme neticesinde söz konusu yayınların basın özgürlüğü kapsamında kaldığını belirterek (bkz. § 10), 16/9/2014 tarihli kararı ile talebin reddine karar vermiştir. Başvurucuların anılan karara itirazı da Adana 1. Sulh Ceza Hâkimliğinin 13/10/2014 tarihli kararı ile reddedilmiştir.

28. Başvuru tarihi itibarıyla söz konusu haberlerin yayın tarihi üzerinden 5 yıl 3 aylık bir süre geçmiştir. Başvurucu Şükrü Alp'in Sulh Ceza Hâkimliğinden erişimin engellenmesi talebinde bulunduğu, sonrasında da Anayasa Mahkemesine bireysel başvuru yaptığı bu süre içerisinde anılan suça ilişkin cezasının infaz edilmekte olduğu da tespit edilmiştir. Haberlerin yayın tarihi üzerinden geçen süre ile haklarında haber yapılan kişilerin kimlikleri de dikkate alındığında haberin güncelliğini ve kamuoyu ilgisini yitirdiği söylenemez. Bu bağlamda haberin konusu, içeriği ve ilk yayın tarihi üzerinden geçen süre gözönünde bulundurulduğunda toplumsal açıdan haber ve yazıların arşivde kolaylıkla ulaşılabilir kılınması için gerekli haber ve bilgilendirme değerinin devam

ettiđi, bu bağlamda unutulma hakkı kapsamında değeriendirilmeyi zorunlu kılacak şartların oluşmadığı belirlenmiştir. Sonuç olarak ifade ve basın özgürlükleri ile birlikte halkın haber alma ve bilgiye ulaşma hakkı birlikte değeriendirildiğinde başvuru konusu olayda, ifade ve basın özgürlükleri ile kişinin manevi bütünlüğünün korunması hakkı arasında adil bir dengenin kurulduğu, derece mahkemesinin takdir yetkisine müdahale etmeyi gerekli kılacak bir durumun bulunmadığı sonucuna ulaşılmıştır.

29. Açıklanan nedenlerle başvurunun diđer kabul edilebilirlik koşulları yönünden incelenmeksizin açıkça dayanaktan yoksun olması nedeniyle kabul edilemez olduğuna karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Şeref ve itibarın korunması hakkının ihlal edildiğine ilişkin iddianın açıkça dayanaktan yoksun olması nedeniyle **KABUL EDİLEMEZ OLDUĞUNA,**

B. Yargılama giderlerinin başvurucular üzerinde bırakılmasına 4/10/2017 tarihinde **OYBİRLİĞİYLE** karar verildi.

Anayasa Mahkemesi - Fahri Gnc (Unutulma Hakkı) Kararı (2014/17943)

Fahri Gnc, B. No: 2014/17943, 5/10/2017

Başvuru, bir gazetenin İnternet haber arşivinde erişilebilir durumda olan haber ile ilgili içeriğın yayından kaldırılması yönündeki talebin reddedilmesinin şeref ve itibarın korunması hakkını ihlal ettiğı iddiasına ilişkindir.

TRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

BİRİNCİ BLM

KARAR

FAHRİ GNC BAŞVURUSU

(Başvuru Numarası: 2014/17943)

Karar Tarihi: 5/10/2017

BİRİNCİ BLM

KARAR

Başkan: Burhan STN

yeler: Serruh KALELİ, Hicabi DURSUN, Hasan Tahsin GKCAN, Yusuf Şevki HAKYEMEZ

Raportr Yrd.: Derya ATAKUL

Başvurucu: Fahri GNC

Vekili: Av. Banu GNC

I. BAŞVURUNUN KONUSU

1. Başvuru, bir gazetenin İnternet haber arşivinde erişilebilir durumda olan haber ile ilgili içeriğın yayından kaldırılması yönündeki talebin reddedilmesinin şeref ve itibarın korunması hakkını ihlal ettiğı iddiasına ilişkindir.

II. BAŞVURU SRECİ

2. Başvuru 6/11/2014 tarihinde yapılmıştır.

3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.
4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.
5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.
6. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık görüş sunmamıştır.

III. OLAY VE OLGULAR

7. Başvuru formu ve eklerinde ifade edildiği şekliyle olaylar özetle şöyledir:
8. Ulusal ölçekte yayımlanan Hürriyet gazetesinin İnternet arşivi sayfalarında 18/12/2003 tarihinde "Yargıtay'dan polise gözaltı uyarısı" başlıklı bir haber yayımlanmıştır. Haber şöyledir:

"Gözaltına almada, Anayasa, Avrupa İnsan Hakları Sözleşmesi, Ceza Muhakemeleri Usulü Kanunu (CMUK) hükümlerine uyulmasını isteyen Yargıtay, ceza soruşturma ve kovuşturmalarında temel ilkenin kişi hürriyetlerine müdahale edilmeden başvurulabilecek bir yöntem var iken hürriyeti daraltan yöntemlere başvurulmaması olduğuna işaret etti.

Yargıtay, bir kişiyi 20 saat gözaltına aldıktan sonra ifadesini dahi almadan serbest bırakan sanık polisin 'hürriyeti tahdit' suçunu işlediğine karar verdi.

Yargıtay 4. Ceza Dairesi, gözaltına almada uyulması gereken ilkeleri, Şişli 5. Asliye Ceza Mahkemesi'nce verilen bir kararın temyiz incelemesini yaparken belirledi.

Şişli 5. Asliye Ceza Mahkemesi, sanıklar Fahri G. ile Asayiş Büro Amiri A. B.'ye "iftira", "bireylere kötü davranma" ve "hürriyeti tahdit" suçlarından beraatına karar verdi.

Yargıtay 4. Ceza Dairesi, sanık Fahri G.'ye "iftira", A. B.'ye "bireylere kötü davranmadan" verilen beraat kararını usul ve yasaya uygun bularak onadı.

Ancak, daire sanık A. B.'ye "hürriyeti tahditten" verilen beraat kararını yasaya aykırı bularak oy birliği ile bozdu. Yargıtay 4. Ceza Dairesi'nin bozma kararında, gözaltına almada uyulacak ilkeler sayıldı.

Anayasa, Polis Vazife ve Selahiyet Yasası, Avrupa İnsan Hakları Sözleşmesi ve Yakalama, Gözaltına Alma ve İfade Alma Yönetmeliği'nin ilgili maddeleri uyarınca suç kovuşturmasıyla ilgili olarak yönteminde verilen yargıç kararı dışında kişilerin yakalanıp gözaltına alınmalarının ancak suç üstü

durumunda veya işlendiği bilinen bir suça ilişkin soruşturma veya kovuşturma sırasında olarak bulunduğu belirtilen kararda, şöyle denildi:

"Kolluk görevlileri ise bu ikinci durumda yalnızca gecikmesinde sakınca bulunan durumlarda yakalama yetkisini kullanabilir. Diğer taraftan belirtilen hukuki düzenlemelerin gereği olarak ceza soruşturma ve kovuşturmalarında temel ilke, kişi hürriyetlerine müdahale edilmeden başvurulabilecek bir yöntem var iken hürriyeti daraltan yöntemlere başvurulmaması ilkesidir."

Gözaltına almada bu ilkeler ışığında temyize konu olayın da irdelendiği kararda, herhangi bir suçla ilgili suç üstü durumu veya suça teşkil eden belirli bir olayla ilgili ceza soruşturması bulunmamasına karşın, salt kimliği belirsiz bir kişinin 16 Mayıs 2000'de telefonla, yakınlarının kimlik ve adreslerini vererek, "Şişli ilçesindeki market ve işyerlerindeki hırsızlık suçlarını bu kişiler işliyorlar" şeklindeki soyut ihbar üzerine bu kişilerin gözaltına alındığı kaydedildi. Kararda, şöyle devam edildi:

"Kimlik ve adresleri aynı tarihli tutanakla tespit edilen bu kişiler hakkında arşiv ve benzeri araştırmalar yapılmaksızın asayiş büro amiri sanığın talimatı doğrultusunda harekete geçilerek 3 saat sonra yakınların gözaltına alınması, cumhuriyet savcısına hırsızlığa karıştığı iddia edilen kişilerin yakalandığı yolunda bilgi verilip peşi sıra bu kişilerin 'herhangi bir suçla' ilgilerinin olup olmadığı yönünde araştırma yapılarak, 20 saat gözaltında kalan yakınların ertesi gün saat 13.30'da bir kanıt bulunmadığı gerekçesiyle ifadeleri dahi alınmadan ve soruşturma evrakı fezlekeye bağlanarak cumhuriyet savcılığına sunulmaksızın serbest bırakılması biçimindeki eylemin Türk Ceza Kanunu'nun 181/1 (hürriyeti tahdit) maddesine uyan suçu oluşturduğu gözetilmeden, kanıtları yanlış değerlendiren yetersiz gerekçeyle beraat hükmü kurulması yasaya aykırıdır."

Yargıtay 4. Ceza Dairesi'nin bozma kararından sonra sanık Ata Bozkır yerel mahkemede yeniden yargılanacak. Yerel mahkeme, beraat kararında direnir ve hüküm yeniden temyiz edilirse son sözü Yargıtay Ceza Genel Kurulu söyleyecek."

9. Başvurucu; iş adamı olduğunu ve uzun süredir inşaat, akaryakıt ve gemicilik sektöründe faaliyette bulunduğunu, anılan haberin iş ve aile hayatında maddi ve manevi kayıplara yol açtığını, şeref ve itibarının zedelendiğini belirterek 21/8/2014 tarihinde söz konusu habere erişimin engellenmesi talebinde bulunmuştur.

10. Bakırköy 5. Sulh Ceza Hâkimliği 21/8/2014 tarihli kararı ile yazı içeriğinde başvurucunun kişilik haklarına saldırı teşkil edebilecek bir ifade olmadığı, yazının kamuoyunu bilgilendirme amacı taşıdığı ve basın özgürlüğü sınırları içinde kaldığı gerekçesiyle talebin reddine karar vermiştir.

11. Başvurucunun anılan karara itirazı Bakırköy 1. Sulh Ceza Hâkimliğinin 22/9/2014 tarihli kararı ile reddedilmiştir.

12. Karar başvurucuya 21/10/2014 tarihinde tebliğ edilmiştir. Başvurucu 6/11/2014 tarihinde bireysel başvuruda bulunmuştur.

IV. İLGİLİ HUKUK

13. Anayasa Mahkemesinin 3/3/2016 tarihli ve 2013/5653 numaralı N.B.B. kararı.

V. İNCELEME VE GEREKÇE

14. Mahkemenin 5/10/2017 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları

15. Başvurucu, Hürriyet gazetesinin İnternet arşivi sayfalarında 18/12/2003 tarihinde Yargıtay'dan polise gözaltı uyarısı başlıklı bir haber yayımlandığını belirtmiştir. Başvurucu anılan haberde, hakkında yapılan ceza yargılaması sonucunda iftira suçundan beraat kararı verildiği ve hükmün Yargıtay 4. Ceza Dairesi tarafından onandığı bilgisine yer verildiğini ifade etmiştir. Başvurucu; ilgili yayın kuruluşunun İnternet sitesinin arşiv bölümünde hakkındaki haberin yer almaya devam ettiğini, haber içeriğinin yayından kaldırılması yönündeki talebinin yargısal makamlar tarafından reddedildiğini belirterek Anayasa'nın 17. ve 20. maddelerinde tanımlanan haklarının ihlal edildiğini ileri sürmüştür.

B. Değerlendirme

16. Anayasa Mahkemesi, olayların başvurucu tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Başvurucu, hakkında yayımlanan habere bahsi geçen gazetenin İnternet sitesindeki haber arşivi üzerinden hâlen kolayca ulaşılabilmesi ve bu arşiv haberin İnternet'ten çıkarılması talebinin reddedilmesi nedeniyle kişilik haklarının zarar gördüğünüden şikâyet etmektedir. Başvurucunun bu şikâyeti şeref ve itibarın korunması hakkı kapsamında incelenmiştir.

17. Bireyin kişisel şeref ve itibarı, Anayasa'nın 17. maddesinde yer alan "manevi varlık" kapsamında yer almaktadır. Devletin, bireyin manevi varlığının bir parçası olan kişisel şeref ve itibara keyfî olarak müdahale etmemek şeklinde negatif yükümlülüğü ve üçüncü kişilerin saldırılarını önlemek şeklinde pozitif yükümlülüğü bulunmaktadır (Adnan Oktar (3), B. No: 2013/1123, 2/10/2013, § 33). Şeref ve itibarı etkileyen saldırılar veya basın ve yayın yolu ile yapılan yayınlara karşı bireyin korunmaması

hâlinde Anayasa'nın 17. maddesinin birinci fıkrası ihlal edilmiş olabilir (Kadir Sağdıç [GK], B. No: 2013/6617, 8/4/2015, § 36; İlhan Cihaner (2), B. No: 2013/5574, 30/6/2014, § 42).

18. Anayasa'nın "Düşünceyi açıklama ve yayma hürriyeti" kenar başlıklı 26. maddesine göre herkes düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Anılan maddede ifade özgürlüğünün kullanımında başvurulabilecek araçlar "söz, yazı, resim veya başka yollar" olarak ifade edilmiş ve "başka yollar" ifadesiyle her türlü ifade aracının anayasal koruma altında olduğu gösterilmiştir (Emin Aydın [GK], B. No: 2013/2602, 23/1/2014, § 43).

19. Haber ve fikirlerin iletilmesinde ve alınmasında önemli bir işlev gören İnternet, Anayasa'nın 26. maddesinde düzenlenen ifade özgürlüğünün güvencesi altındadır. Nitekim Anayasa Mahkemesi, İnternet erişimine yönelik bir müdahalenin ifade özgürlüğü kapsamında incelenmesi gerektiğini kabul etmiştir (Yaman Akdeniz ve diğerleri, B. No: 2014/3986, 2/4/2014; Youtube LLC Corporation Service Company ve diğerleri [GK], B. No: 2014/4705, 29/5/2014).

20. Diğer taraftan Anayasa Mahkemesi birçok kararında ifade özgürlüğünün sadece düşünce ve fikirleri yayma özgürlüğünü değil haber ve fikirlere ulaşma özgürlüğünü de kapsadığını vurgulamıştır (Emin Aydın, B. No: 2013/2602, 23/1/2014, § 40; Kamuran Reşit Bekir [GK], B. No: 2013/3614, 8/4/2015, § 34). Bu bağlamda haber ve fikirlerin yayılmasını ve bunlara kamunun ulaşmasını kolaylaştıran İnternet'in toplum hayatındaki önemli rolü yadsınamaz. İnternet üzerinde arşiv oluşturma, aktüalitenin ve haberlerin saklanmasına ve erişilebilirliğine büyük ölçüde hizmet etmektedir. Bu nitelikteki arşivler özellikle doğrudan halkın erişimine açık ve genelde ücretsiz olmaları nedeniyle tarih eğitimi ve araştırma faaliyetleri için kaynak sunmaktadır. Öte yandan demokratik bir toplumda basın ilk işlevi olan "gözetleyici" rolünün bir sonucu da arşivlerin halkın erişimine sunulmasıdır. Bu nedenle İnternet'te tutulan arşivlerin, ifade ve basın özgürlükleri kapsamında olduğu açıktır. Dolayısıyla İnternet'te yayımlanan ve gazetecilik faaliyeti kapsamında kabul edilen bir haber arşivinin yayından kaldırılması basın özgürlüğüne yönelik bir müdahale teşkil edebilir (N.B.B., B. No: 2013/5653, 3/3/2016, § 61).

21. İfade özgürlüğü ile onu tamamlayan ve ifade özgürlüğünün kullanılmasını sağlayan basın özgürlüğü, Anayasa'da yer alan temel hak ve özgürlükleri sınırlama rejimine tabidir. Anayasa'nın 26., 27. ve 28. maddelerinde sayılan sınırlandırmalardan biri, "başkalarının şöhret veya haklarının, özel veya aile hayatlarının" korunmasıdır (Kadir Sağdıç, § 55; İlhan Cihaner (2), § 62). Öte yandan "başkalarının şöhret veya haklarının, özel veya aile hayatlarının" korunması bağlamında şeref ve

itibarın korunması hakkının etki alanını genişletmenin ifade ve basın özgürlüklerinin ihlali sonucunu doğurabileceği hatırd tutulmalıdır.

22. Bu sebeple Anayasa'nın 17. maddesinin birinci fıkrasında koruma altına alınan şeref ve itibarın korunmasını isteme hakkı ile başvuruya konu İnternet haber arşivinin Anayasa'nın 28. maddesinde güvence altına alınan basın özgürlüğü ve bu özgürlükle bağlantılı olarak Anayasa'nın 26. maddesinde güvence altına alınan ifade özgürlüğü arasında Anayasa Mahkemesi içtihadında ortaya konulan kriterlere uygun şekilde bir denge kurulması gerekmektedir. İnternet ortamının sağladığı ulaşılabilirlik, yaygınlık, haber ve fikirlerin depolanmasındaki ve muhafazasındaki kolaylık dikkate alındığında yayımlandığı tarihte belirli ağırlık eşiğini aşmayan veya kişinin kendi eylemlerinden kaynaklanan haberlerin İnternet ortamında uzun süre erişilebilir kalması kişilerin şeref ve itibarını zedeleyebilir (N.B.B., § 37).

23. Anayasa Mahkemesi, 3/3/2016 tarihli ve 2013/5653 numaralı N.B.B. başvurusunda İnternet'in etkin olarak kullanılmasıyla beraber ifade ve basın özgürlükleri ile şeref ve itibarın korunması arasındaki dengenin ilki lehine bozulduğunu, bu dengenin tekrar kurulabilmesinin şeref ve itibar yönünden bireylerin unutulma hakkının kabul edilmesi ile mümkün olabileceğini belirtmiştir (N.B.B., § 46).

24. Anayasa Mahkemesi, bahsi geçen başvuruda unutulma hakkının Anayasal dayanaklarına yer vererek devletin bireye geçmişte yaşadıklarının başkaları tarafından öğrenilmesi engellenerek “yeni bir sayfa açma” olanağı verme hususunda bir sorumluluğu olduğunu, dolayısıyla unutulma hakkının kişilerin manevi varlıklarını geliştirmelerine bir fırsat vermek açısından devletin pozitif yükümlülüğünün bir sonucu olduğunu ortaya koymuştur (N.B.B., §§ 47-49).

25. Bununla birlikte Mahkeme, unutulma hakkının İnternet üzerindeki her türlü haber veya yazı yönünden uygulanmasını beklemenin mümkün olmadığını, özellikle basın özgürlüğü temelinde gazete arşivinin araştırmacılar, hukukçular veya tarihçiler için önem taşıyan veriler olduğunu belirtmiştir. Unutulma hakkı, İnternet ortamında haber arşivini koruma altına alan basın özgürlüğünün ve halkın haber ve fikirlere ulaşma özgürlüğünün özüne dokunmayacak ve aynı zamanda hak sahibinin çıkarlarını koruyacak şekilde kullanılmalıdır. Mahkeme, İnternet ortamındaki bir haber veya yazının unutulma hakkı kapsamında İnternet'ten çıkarılabilmesi için yayının içeriği, yayında kaldığı süre, güncelliğini yitirme, tarihsel bir veri olarak kabul edilememe, kamu yararına katkısı (toplumsal açıdan haberin değeri, haberin geleceğe ışık tutan niteliği) haber veya yazıya konu kişinin siyasetçi veya ünlü olup olmadığı, haber veya yazının konusu, bu bağlamda haber ya da yazının olgusal gerçekler veya değer yargısı içerip içermediği, halkın ilgili veriye yönelik ilgisi gibi hususların somut olay açısından incelenmesi gerekliliğini ortaya koymuştur (N.B.B., § 50).

26. Somut olayda başvuru konusundaki şikâyetine konu olan haber 18/12/2003 tarihinde yayımlanmış ve arşiv niteliğindedir. Haber genel olarak gözaltı koruma tedbirinin uygulanması esnasında kolluk görevlileri tarafından uyulması gereken ilkeler hakkındadır. Habere göre Yargıtay ilgili ceza dairesi, temyize konu bir olayı irdelerken bu ilkelerden yararlanmış, gözaltı nedeni bulunmadığı halde bir kişinin yirmi saat gözaltında tutulduktan sonra ifadesi dahi alınmadan serbest bırakılmasının hürriyeti tahdit suçunu oluşturacağı gerekçesiyle ilk derece mahkemesinin kolluk görevlisi hakkındaki beraat kararını bozmuştur. Haberde, Yargıtayın kişi hürriyetine müdahale edilmeden başvurulabilecek bir koruma tedbiri var ise kolluk görevlileri tarafından hürriyeti daraltan yöntemlere başvurulmaması gerektiği yönündeki kanaati aktarılmaktadır. Yargıtay'dan polise gözaltı uyarısı başlığının kullanıldığı haberde, ilk derece mahkemesinde yapılan yargılamada sanıklar arasında yer alan başvuru konusundaki iftira suçundan yargılanarak beraat ettiği, Yargıtay tarafından başvuru hakkında verilen beraat kararının onandığı bilgisine de yer verilmiştir. Bu haberin gerçeğe aykırı olduğu ileri sürülmemiştir.

27. Başvuru, şeref ve itibarının zedelendiğini belirterek 21/8/2014 tarihinde söz konusu habere erişimin engellenmesi talebinde bulunmuştur. Bakırköy 5. Sulh Ceza Hâkimliği, başvuru konusundaki şeref ve itibarının korunması ile kamu yararı bağlamında yaptığı değerlendirme neticesinde söz konusu yayının basın özgürlüğü kapsamında kaldığını belirterek (bkz. § 10) 21/8/2014 tarihli kararı ile talebin reddine karar vermiştir. Başvuru konusundaki anılan karara itirazı da Bakırköy 1. Sulh Ceza Hâkimliğinin 22/9/2014 tarihli kararı ile reddedilmiştir.

28. Bahsi geçen haberin başlığı ile içeriği incelendiğinde amacın, kamuoyunun ilgisine matuf, polisin gözaltı tedbirini uygularken uyması gereken ilkelere yönelik Yargıtay yaklaşımını somut dava kapsamında aktarmak ve kamuoyunu bilgilendirmek olduğu görülmektedir. Her ne kadar haberin yapıldığı tarih ile haber içeriğine erişimin engellenmesi talebinde bulunulduğu tarih arasında on bir yıla yakın süre bulursa da haberin kişi özgürlüğü ve güvenliği hakkına ilişkin bir sorun hakkında temyiz merciinin yaklaşımını ortaya koyması bakımından güncelliğini ve kamuoyunun ilgisini yitirdiği söylenemez. Haberde, somut davaya ilişkin bilgilere yer verilirken sanık sıfatıyla yer alması sebebiyle başvuru hakkında ilk derece mahkemesi ile Yargıtay ilgili ceza dairesinin verdiği beraat ve onama kararlarına da değinilmiştir. Bununla birlikte yukarıda yer verilen tespitler ışığında haberin doğrudan başvuru konusundaki şahsını hedef alır nitelikte bir haber olmadığı da açıktır. Kaldı ki haberde, başvuru hakkında değer yargısı olarak nitelendirilebilecek herhangi bir ifadeye de yer verilmemiş, yalnızca beraat ve onama kararları aktarılmıştır. Bu bakımdan başvuru hakkında menfi olarak nitelendirilebilecek bir bilgiye yer verilmediği de görülmektedir. Diğer taraftan İnternet haber

arşivindeki bireysel başvuru konusu linke tıklanıldığında ilgili gazete tarafından haberin yayımlanmaya devam ettiđi ancak başvuru sahibinin soyadının sadece baş harfe yer verecek şekilde kısaltılarak haberi ulaşılabilir kılan kişisel verilerin silindiđi de tespit edilmiştir.

29. Tüm bu tespitler ışığında haberin arşivde kolaylıkla ulaşılabilir kılınması için gerekli haber değerinin devam ettiđi, bu bağlamda unutulma hakkı kapsamında değerlendirilmeyi zorunlu kılacak şartların oluşmadığı belirlenmiştir. Sonuç olarak ifade ve basın özgürlükleri ile birlikte halkın haber alma ve bilgiye ulaşma hakkı birlikte değerlendirildiğinde başvuru konusu olayda ifade ve basın özgürlükleri ile kişinin manevi bütünlüğünün korunması hakkı arasında adil bir dengenin kurulduğu, derece mahkemesinin takdir yetkisine müdahale etmeyi gerekli kılacak bir durumun bulunmadığı sonucuna ulaşılmıştır.

30. Açıklanan nedenlerle başvurunun diğer kabul edilebilirlik koşulları yönünden incelenmeksizin açıkça dayanaktan yoksun olması nedeniyle kabul edilemez olduğuna karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Başvurunun açıkça dayanaktan yoksun olması nedeniyle **KABUL EDİLEMEZ OLDUĞUNA,**

B. Yargılama giderlerinin başvuru üzerinde bırakılmasına 5/10/2017 tarihinde **OYBİRLİĞİYLE** karar verildi.

Anayasa Mahkemesi - N.B.B. (2) (Unutulma Hakkı) Kararı (2014/17143)

N.B.B. (2) [GK], B. No: 2014/17143, 1/3/2017

Başvuru, bir gazetenin İnternet haber arşivinde erişilebilir durumda olan haber ve yayınlar ile ilgili içeriğin yayından kaldırılması yönündeki talebin reddedilmesinin şeref ve itibarın korunması hakkını ihlal ettiği iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

GENEL KURUL

KARAR

N.B.B. BAŞVURUSU (2)

(Başvuru Numarası: 2014/17143)

Karar Tarihi: 1/3/2017

R.G. Tarih ve Sayı: 22/3/2017 - 30015

GENEL KURUL

KARAR

GİZLİLİK TALEBİ KABUL

Başkan: Zühtü ARSLAN

Başkanvekili: Burhan ÜSTÜN

Başkanvekili: Engin YILDIRIM

Üyeler: Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ, Nuri NECİPOĞLU, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ

Raportör: Murat ŞEN

Başvurucu: N. B. B.

Vekili:

Av. Ahmet Volkan MEMİŐ

I. BAŐVURUNUN KONUSU

1. BaŐvuru, bir gazetenin İnternet haber arŐivinde eriŐilebilir durumda olan haber ve yayınlar ile ilgili iŐeriŐin yayından kaldırılması yÖnündeki talebin reddedilmesinin Őeref ve itibarın korunması hakkını ihlal ettiĐi iddiasına iliŐkindir.

II. BAŐVURU SÜRECİ

2. BaŐvuru 17/10/2014 tarihinde BakırkÖy 2. Sulh Ceza HâkimliĐi vasıtasıyla yapılmıŐtır. BaŐvuru formu ve belgelerinin idari yÖnden yapılan ön incelemesi neticesinde baŐvurunun Komisyona sunulmasına engel teŐkil edecek bir eksikliĐinin bulunmadıĐı tespit edilmiŐtir.

3. Birinci Bölümün Üçüncü Komisyonunca baŐvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiŐtir.

4. Birinci Bölüm tarafından 11/1/2017 tarihinde yapılan toplantıda baŐvurunun niteliĐi itibarıyla Genel Kurul tarafından karara baĐlanması gerekli görüldüĐünden Anayasa Mahkemesi İŐtüzüĐü'nün (İŐtüzük) 28. maddesinin (3) numaralı fıkrası uyarınca Genel Kurula sevkine karar verilmiŐtir.

III. OLAY VE OLGULAR

A. Olaylar

5. BaŐvuru formu ve eklerinde ifade edildiĐi Őekliyle olaylar özetle Őöyledir:

6. Ulusal ölçekte yayımlanan bir gazetenin İnternet arŐivi sayfalarında, baŐvurucu hakkında uyuyturuocu kullandıĐı iddiası ile yürütölen bir ceza kovuyturması neticesinde adli para cezasına hükmedilen olaya iliŐkin olarak 1999 yılında bir haber yayımlanmıŐtır.

7. BaŐvurucu, ilgili basın kuruluşunun İnternet sayfasının arŐiv bölümünde hakkındaki haberlerin yayımına devam ettiĐini belirterek 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İŐlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 9/A maddesi gereĐince İnternet yayınının kaldırılması iŐin 11/7/2014 tarihinde (kapatılan) BakırkÖy 5. Sulh Ceza Mahkemesine baŐvurmuŐtur.

8. Anılan Mahkeme, 11/7/2014 tarihli ve 2014/848 DeĐiŐik İŐ sayılı kararı ile talebin reddine karar vermiŐtir.

9. Başvurucunun anılan karara karşı yaptığı itiraz, Bakırköy 5. Sulh Ceza Hâkimliğinin 21/8/2014 tarihli ve 2014/716 Değişik İş sayılı kararlarıyla reddedilmiştir.

10. Karar17/9/2014 tarihinde başvuru vekiline tebliğ edilmiştir.

11. Başvurucu17/10/2014 tarihinde bireysel başvuruda bulunmuştur.

B. İlgili Hukuk

12. 6/2/2014 tarihli ve 6518 sayılı Kanun ile değişik 5651 sayılı Kanun'un 9. ve 9/A maddeleri,19/6/2004 tarihli ve 5187 sayılı Basın Kanunu'nun 3. maddesi.

13. Yargıtay Hukuk Genel Kurulunun 17/6/2015 tarihli ve E.2014/4-56, K.2015/1679 sayılı kararının ilgili kısmı şöyledir:

"...Unutulma hakkına gelince; unutulma hakkı ve bununla ilişkili olan gerektiği ölçüde ve en kısa süreliğine kişisel verilerin depolanması veya tutulması konuları, aslında kişisel verilerin korunması hakkının çatısını oluşturmaktadır. Her iki hakkın temelinde bireyin kişisel verileri üzerinde serbestçe tasarruf edebilmesini, geçmişin engeline takılmaksızın geleceğe yönelik plan yapabilmesini, kişisel verilerin kişi aleyhine kullanılmasının engellenmesini sağlamak yatmaktadır. Unutulma hakkı ile geçmişinde kendi iradesi ile veya üçüncü kişinin neden olduğu bir olay nedeni ile kişinin geleceğinin olumsuz bir şekilde etkilenmesinin engellenmesi sağlanmaktadır. Bireyin geçmişinde yaşadığı olumsuz etkilerden kurtularak geleceğini şekillendirebilmesi bireyin yararına olduğu gibi toplumun kalitesinin gelişmişlik seviyesinin yükselmesine etkisi de tartışılmazdır.

Unutulma hakkı; üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerin silinmesini ve yayılmasının önlenmesini isteme hakkı olarak ifade edilebilir.

..."

IV. İNCELEME VE GEREKÇE

14. Mahkemenin 1/3/2017 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları

15. Başvurucu; hakkında yapılan ceza yargılaması sonucunda adli para cezası ödemeye mahkûm edildiği olay ile ilgili olarak bir basın yayın organının İnternet sitesinde1999 yılında haber ve yayınlar yapıldığını, ilgili yayın kuruluşunun İnternet sitesinin arşiv bölümlerinde hakkındaki haber ve yayının yer almaya devam ettiğini, yayına erişimin engellenmesi talebinin reddedildiğini belirterek

Anayasa'nın 12., 17., 20., 25., 26., 27. ve 32.maddelerinde tanımlanan haklarının ihlal edildiğini iddia etmiştir.

B. Değerlendirme

16. Başvurucu; gerçeğe aykırı veya uydurma haber olduğunu ileri sürmediği 1999 yılında hakkında yapılan bir yargılamaya ilişkin haberin hâlen arşivde yer alması ve İnternet üzerinden habere kolayca ulaşılabilir olması nedenleriyle özel ve iş hayatının olumsuz etkilendiğini, itibarının zedelendiğini iddia etmiştir. Başvurucu, bu iddialarını 22/7/2013 tarihli ve 2013/5653 numaralı bireysel başvurusunda da dile getirmiştir. Anayasa Mahkemesi, anılan başvuruyu 3/3/2016 tarihinde Anayasa'nın 17. maddesinin birinci fıkrasında güvence altına alınan şeref ve itibarın korunması hakkının ihlal edildiğine karar vererek sonuçlandırmıştır (N.B.B. [GK], B. No: 2013/5653, 3/3/2016).

17. Başvurucu, ihlal kararı ile sonuçlanan başvurusunda incelenen bu başvuruya konu olaya ilişkin olarak sadece 1999 tarihinde yapılan habere değil 1998 yılında yapılan habere ilişkin de şeref ve itibarının zedelendiğini de ileri sürmüştür. İki başvuruda İnternet arşivinde haber içeriğini yayımlayan basın kuruluşları ve erişimin engellenmesi talep edilen derece mahkemeleri farklıdır. Öte yandan her iki başvuru açısından İnternet arşivindeki haberin içeriği, başvurusunun 1998 ve 1999 yıllarında uyuşturucu kullandığı iddiası ile yürütülen aynı ceza kovuşturması neticesinde adli para cezası almasına neden olan olaya ilişkindir. Ayrıca her iki başvuruda da şikâyetler aynı şekilde kaleme alınmış aynı hususları kapsamaktadır. Başvurucu 3/3/2016 tarihli ve 2013/5653 numaralı başvurudan farklı olarak mevcut başvuruda herhangi bir iddia ileri sürmemiştir.

18. Dolayısıyla mevcut başvurunun, Anayasa Mahkemesinin 3/3/2016 tarihli ve 2013/5653 numaralı kararının içeriğinden farklı bir yönü bulunmamaktadır. Başvurular arasındaki tek fark aynı haberin farklı gazetelerin İnternet arşivlerinde yayımlanmasıdır.

19. İçtüzük'ün 80. maddesinin (1) numaralı fıkrasının (ç) bendi şöyledir:

“(1) Bölümler ya da Komisyonlarca yargılamanın her aşamasında aşağıdaki hâllerde düşme kararı verilebilir:

...

ç) Bölümler ya da Komisyonlarca saptanan herhangi bir başka gerekçeden ötürü, başvurunun incelenmesinin sürdürülmesini haklı kılan bir neden görülmemesi.”

20. Yukarıda belirtildiği gibi başvurusunun aynı içerikli şikâyetlerine ilişkin olarak Anayasa Mahkemesi 3/3/2016 tarihinde, başvurusunun Anayasa'nın 17. maddesinin birinci fıkrasında güvence

altına alınan şeref ve itibarın korunması hakkının ihlal edildiğine karar vermiştir. Her ne kadar mevcut başvuruda, başvuru farklı bir gazetenin İnternet arşivindeki habere ilişkin olarak farklı bir mahkemeden içeriğe erişimin engellenmesini talep etmiş ise de şikâyete konu haber içeriği aynıdır. Bununla birlikte başvuru anılan kararda ileri sürdüğü aynı yöndeki iddialarına ilişkin olarak Bakırköy 5. Sulh Ceza Mahkemesi, Anayasa Mahkemesinin ihlal kararından önce talebin reddine karar vermiştir. Bu karara rağmen, Anayasa Mahkemesinin anılan kararını referans alarak başvuru yetkili yargı mercilerinden tekrar içeriğe erişimin engellenmesini talep edebileceğinde herhangi bir tereddüt bulunmamaktadır. Bu itibarla başvurunun incelenmesinin sürdürülmesini haklı kılan bir neden kalmadığı anlaşılmıştır.

21. Bu nedenlerle başvurunun diğer kabul edilebilirlik koşulları yönünden incelenmeksizin düşmesine karar verilmesi gerektiği sonucuna ulaşılmıştır.

V. HÜKÜM

Açıklanan gerekçelerle;

A. Kamuya açık belgelerde başvuru kimliğinin gizli tutulması talebinin **KABULÜNE**,

B. Başvurunun incelenmesinin sürdürülmesini haklı kılan bir nedenin kalmamış olması nedeniyle **DÜŞMESİNE**,

C. Yargılama giderlerinin başvuru üzerinde **BIRAKILMASINA** 1/3/2017 tarihinde **OYBİRLİĞİYLE** karar verildi.

Anayasa Mahkemesi - G.Y. (Unutulma Hakkı) Kararı (2014/16026)

G.Y., B. No: 2014/16026, 5/10/2017

Başvuru, bazı İnternet siteleri ile bir sosyal medya hesabında belediye üst düzey çalışanı hakkında yapılan haber ve yorumlara erişimin engellenmesi talebinin Mahkemece kabul edilmemesi ve bu haber ile yorumların İnternet ortamında yer almaya devam etmesi nedenleriyle şeref ve itibarın korunması hakkının ihlal edildiği iddialarına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

BİRİNCİ BÖLÜM

KARAR

G.Y. BAŞVURUSU

(Başvuru Numarası: 2014/16026)

Karar Tarihi: 5/10/2017

BİRİNCİ BÖLÜM

KARAR

Başkan: Burhan ÜSTÜN

Üyeler: Serruh KALELİ, Hicabi DURSUN, Hasan Tahsin GÖKCAN, Yusuf Şevki HAKYEMEZ

Raportör Yrd.: Derya ATAKUL

Başvurucu: G.Y.

Vekili: Av. Zeynep Sedef ÖZDOĞAN

I. BAŞVURUNUN KONUSU

1. Başvuru, bazı İnternet siteleri ile bir sosyal medya hesabında belediye üst düzey çalışanı hakkında yapılan haber ve yorumlara erişimin engellenmesi talebinin Mahkemece kabul edilmemesi ve bu haber ile yorumların İnternet ortamında yer almaya devam etmesi nedenleriyle şeref ve itibarın korunması hakkının ihlal edildiği iddialarına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 1/10/2014 tarihinde yapılmıştır.
3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.
4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.
5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.
6. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık görüş sunmamıştır.

III. OLAY VE OLGULAR

7. Başvuru formu ve eklerinde ifade edildiği şekliyle olaylar özetle şöyledir:
8. Başvurucu 1/10/2014 tarihli bireysel başvuru formunda 2008 yılında İzmir Büyükşehir Belediyesi işletmesi Grand Plazada işe başladığını, aynı yıl Belediyenin halkla ilişkiler birimine geçtiğini belirtmiştir. Başvuru formunda başvurusunun İzmir Büyükşehir Belediyesinin tanıtım, iletişim, halkla ilişkiler işlerini yürüten İz Enerji ve Ünibel Şirketlerinde çalıştığı; İzmir Büyükşehir Belediye Başkanı'nun sosyal medya hesaplarının kullanılmasında görev aldığı belirtilmiştir. Formda başvurusunun 2010 yılında Cumhuriyet Halk Partisi (CHP) Buca ilçe başkan yardımcısı seçildiği, daha sonra da Konak belediye başkan adayının seçim çalışmalarında aktif görev üstlendiği bilgilerine yer verilmiştir.
9. Gazeteci S.G., kendisine ait blogspot İnternet sitesinde 28/6/2010 tarihinde Dede Zora Giriyor başlıklı bir yazı paylaşmıştır. Anılan yazının başvurusu ile ilgili kısmı şöyledir:

"NOT 2: Grand Plaza eski Genel Müdürü, şimdilerin İzbelkom Genel Müdürü M. D.'nin örgütlenmesi de dikkatimizi çekiyor. Öncelikle arkeolog oğlu büyükşehirde işe başlamış. Kayınbiraderi V. S. ile kayınbiraderinin eşi G. Seyhan da Grand Plaza'da. Arkadaşının kızı S. N. ile S. N.'nin eşi E. N. de Grand Plaza'da. Yakın arkadaşı Personel Müdürü H. G.... H. G.'nin eşi A. G. ise Grand Plaza'da halkla ilişkiler şefi... Ekmek fabrikası açılmadan üç ay önce işe alınan yine arkadaşının oğlu L. Bey de Ekmek Fabrikası Personel Müdürlüğü'ne getirilmiş. M. D.'nin oğlunun yakın arkadaşları da Grand Plaza'da iş bulmuş, çalışıyorlar. Tabii bu ilişkileri en iyi anlatacak olan isim İşletmelerden

Sorumlu Genel Müdür Yardımcısı H. B.. H. B.'nin oğlu da büyükşehir çalışanı... Belediye değil, aile şirketi gibi..."

10. www.gaze-temiz.com isimli İnternet haber sitesinde Gazeteci S.G. tarafından kaleme alınan; 20/5/2013 tarihinde "Büyük Şehrin Yeni Yıldızı", 24/5/2013 tarihinde G. Hanım Dava Açabilir, 25/5/2013 tarihinde Sabuktay G.'yi Savunuyor ve 26/5/2013 tarihinde Kocaoğlu Yemeklere Şap Koydursun başlıklı haberler yayımlanmıştır. Anılan haberlerden ikisinin başvuru ile ilgili kısımları şöyledir:

"Büyük Şehrin Yeni Yıldızı"

"Hikayenin başında bu kez G.Y. var.Bu isim yabancı geldi mi size..."

Aslında M. D.'nin kayınbiraderinin eski eşi. V. S.'nin... Grand Plaza'da garson iken tanışıp evlenmiş V. S., G.Y. ile... O evlilikte halkla ilişkiler birimine geçmiş.

Bir ay sonra da çift ayrılma kararı almış.

Genç hanım bu kez İZENERJİ eski Genel Müdürü A. S. S.'nin asistanı olarak karşımıza çıkıyor. A. S. S.'nin Ünibel Genel Müdürü olması ile birlikte lise mezunu bu kızımız başarılarından ötürü Ünibel'in medya ve internet müdürü olur."

"Kocaoğlu Yemeklere Şap Koydursun"

"Çok merak ediyordum, son operasyonlar ile Aziz Kocaoğlu'nun çok güvendiği genel sekreter yardımcısı S. B. neden İZSU'ya yine Aziz Kocaoğlu'nun Manisa'dan büyük ümitlerle transfer ettiği Kültür ve Sosyal İşler Dairesi Başkanı M. Ö. neden APİKAM'a gitti diye.

Büyükşehir üst düzeyinin yaptığı Avrupa seyahatleri geldi önüme.

Demek ki Kocaoğlu, S. B. ile M. Ö.'nün aynı çatı altında olmalarını istememiş.

İşte tam burada yukarıdaki başlığı okuyun.

Kültür müdürü V. Ç. ... Tabii ki her müdürün bir sekreteri vardır. O da G. A. ...

Başlığa dönünüz...

Sonra Ünibel'in önemli şahsiyeti G.Y.i tanıdık.

Yine başlığa dönünüz...

Kendini genel sekreter olarak tanıtan ancak göreve yeniden dönerken üçlü kararname gereği İçişleri Bakanlığı'ndan imza almaya gerek görmeyen P.Ş.G. olanlardan haberdar mı? ..."

11. Gazeteci S.G. 14/2/2014 tarihinde Facebook hesabında "Bak şimdi bu haber neden geldi aklıma?" şeklinde bir not yazmış ve yazının altına, yukarıda yer verilen "Büyük Şehrin Yeni Yıldızı" başlıklı haber linkini eklemiştir. Yine anılan gazeteci Facebook hesabında başvurucu ile ilgili olarak "Durum vahim... G.y. konak adayı sema hanımın danışmanı olmuş." şeklinde bir not paylaşmıştır.

12. Başvurucu; söz konusu haber ve yazıların gerçeği yansıtmadığını, iftira ve hakaret içeren sözler nedeniyle kişilik haklarına saldırı niteliği taşıdığını, bu nedenle şeref ve itibarının zedelendiğini ileri sürerek İnternet içeriklerine erişimin engellenmesi talebinde bulunmuştur. İzmir 2. Sulh Ceza Hâkimliği 20/8/2014 tarihli kararı ile erişimin engellenmesi talebinin reddine karar vermiştir. Hâkimlik, gerekçeli kararında bir yazının haber niteliğinin bulunması için taşınması gereken unsurları (gerçeklik, güncellik, kamu yararı, biçim ile konu arasında fikri bağ) sıralamış, dava konusu yazıların bu unsurları taşıdığını, yazılar arasında konu bütünlüğünün olduğunu ve yayımlanmalarında kamu yararı bulunduğunu belirtmiştir.

13. Başvurucunun anılan karara itirazı İzmir 3. Sulh Ceza Hâkimliğinin 27/8/2014 tarihli kararı ile reddedilmiştir.

14. Karar başvurucuya 1/9/2014 tarihinde tebliğ edilmiştir. Başvurucu 1/10/2014 tarihinde bireysel başvuruda bulunmuştur.

IV. İLGİLİ HUKUK

15. Anayasa Mahkemesinin 3/3/2016 tarihli ve 2013/5653 numaralı N.B.B. Kararı.

V. İNCELEME VE GEREKÇE

16. Mahkemenin 5/10/2017 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları

17. Başvurucu, bir gazeteci tarafından kendisi hakkında www.gaze-temiz.com isimli İnternet haber sitesinde yayımlanan haberler ile bu gazetecinin blogspot İnternet sitesinde ve Facebook hesabında paylaştığı yazıların gerçeği yansıtmadığını, iftira ve hakaret içeren sözler nedeniyle kişilik haklarına saldırı niteliği taşıdığını iddia etmiştir. Başvurucu, İnternet içeriklerine erişimin engellenmesi talebinin mahkemece reddedilmesi ile bu haber ve yazıların İnternet ortamında yer almaya devam etmesi nedeniyle özel hayatın gizliliği, şeref ve itibarın korunması ile adil yargılanma haklarının ihlal edildiğini ileri sürmüştür.

B. Değerlendirme

18. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağılı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Başvurucu, hakkında yayımlanan haber ve yazıların İnternet ortamında yer almaya devam etmesi nedeniyle kişilik haklarının zedelendiğinden şikâyet etmektedir. Başvurucunun bu şikâyeti şeref ve itibarın korunması hakkı kapsamında incelenmiştir.

19. Bireyin kişisel şeref ve itibarı, Anayasa'nın 17. maddesinde yer alan "manevi varlık" kapsamında yer almaktadır. Devletin, bireyin manevi varlığının bir parçası olan kişisel şeref ve itibara keyfî olarak müdahale etmemek şeklinde negatif yükümlülüğü ve üçüncü kişilerin saldırılarını önlemek şeklinde pozitif yükümlülüğü bulunmaktadır (Adnan Oktar (3), B. No: 2013/1123, 2/10/2013, § 33). Şeref ve itibarı etkileyen saldırılar veya basın ve yayın yolu ile yapılan yayınlara karşı bireyin korunmaması hâlinde Anayasa'nın 17. maddesinin birinci fıkrası ihlal edilmiş olabilir (Kadir Sağdıç [GK], B. No: 2013/6617, 8/4/2015, § 36; İlhan Cihaner (2), B. No: 2013/5574, 30/6/2014, § 42).

20. Anayasa'nın "Düşünceyi açıklama ve yayma hürriyeti" kenar başlıklı 26. maddesine göre herkes düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Anılan maddede ifade özgürlüğünün kullanımında başvurulabilecek araçlar "söz, yazı, resim veya başka yollar" olarak ifade edilmiş ve "başka yollar" ifadesiyle her türlü ifade aracının anayasal koruma altında olduğu gösterilmiştir (Emin Aydın, B. No: 2013/2602, 23/1/2014, § 43).

21. Haber ve fikirlerin iletilmesinde ve alınmasında önemli bir işlev gören İnternet, Anayasa'nın 26. maddesinde düzenlenen ifade özgürlüğünün güvencesi altındadır. Nitekim Anayasa Mahkemesi İnternet erişimine yönelik bir müdahalenin ifade özgürlüğü kapsamında incelenmesi gerektiğini kabul etmiştir (Yaman Akdeniz ve diğeri, B. No: 2014/3986, 2/4/2014; Youtube LLC Corporation Service Company ve diğeri [GK], B. No: 2014/4705, 29/5/2014). Bu itibarla bir blogspot İnternet sitesinde ve Facebook gibi sosyal medya hesaplarında paylaşılan fikirlerin de ifade özgürlüğü kapsamında değerlendirileceği açıktır.

22. Anayasa Mahkemesi birçok kararında ifade özgürlüğünün sadece düşünce ve fikirleri yayma özgürlüğünü değil haber ve fikirlere ulaşma özgürlüğünü de kapsadığını vurgulamıştır (Emin Aydın, § 40; Kamuran Reşit Bekir [GK], B. No: 2013/3614, 8/4/2015, § 34). İnternet üzerinde arşiv oluşturma, aktüalitenin ve haberlerin saklanmasına ve erişilebilirliğine büyük ölçüde hizmet etmektedir. Bu nitelikteki arşivler özellikle doğrudan halkın erişimine açık ve genelde ücretsiz olmaları nedeniyle tarih eğitimi ve araştırma faaliyetleri için kaynak sunmaktadır. Öte yandan demokratik bir toplumda

basının ilk işlevi olan "gözetleyici" rolünün bir sonucu da arşivlerin halkın erişimine sunulmasıdır. Bu nedenle İnternet'te tutulan arşivlerin, ifade ve basın özgürlükleri kapsamında olduğu açıktır. Dolayısıyla İnternet'te yayımlanan ve gazetecilik faaliyeti kapsamında kabul edilen bir haber arşivinin yayından kaldırılması basın özgürlüğüne yönelik bir müdahale teşkil edebilir (N.B.B., B. No: 2013/5653, 3/3/2016, § 61).

23. Başvuru konusu olayda başvuru hakkında yapılan haberler www.gaze-temiz.com isimli İnternet sitesinde yayımlanmıştır. Bahsi geçen İnternet sitesi ağırlıklı olarak İzmir ili ve bağlı ilçelerine ilişkin siyasi, ekonomik ve güncel konularda haber yapan bir sitedir. Bu bağlamda geleneksel gazeteciliğe yakınlığı ile "gözetleyicilik" görevini yerine getirdiği değerlendirilebilir. Dolayısıyla anılan haber arşivi sitesinin basın özgürlüğü kapsamında değerlendirilmesi mümkündür.

24. İfade özgürlüğü ile onu tamamlayan ve ifade özgürlüğünün kullanılmasını sağlayan basın özgürlüğü, Anayasa'da yer alan temel hak ve özgürlükleri sınırlama rejimine tabidir. Anayasa'nın 26., 27. ve 28. maddelerinde sayılan sınırlandırmalardan biri, "başkalarının şöhret veya haklarının, özel veya aile hayatlarının" korunmasıdır (Kadir Sağdıç, § 55; İlhan Cihaner (2), § 62). Öte yandan "başkalarının şöhret veya haklarının, özel veya aile hayatlarının" korunması bağlamında şeref ve itibarın korunması hakkının etki alanını genişletmenin ifade ve basın özgürlüklerinin ihlali sonucunu doğurabileceği hatırlanmalıdır.

25. Bu sebeple Anayasa'nın 17. maddesinin birinci fıkrasında koruma altına alınan şeref ve itibarın korunmasını isteme hakkı ile başvuruya konu blogspot İnternet sitesi ve sosyal medya hesabının Anayasa'nın 26. maddesinde güvence altına alınan ifade özgürlüğü ile İnternet haber arşivinin Anayasa'nın 28. maddesinde güvence altına alınan basın özgürlüğü ve bu özgürlükle bağlantılı olarak Anayasa'nın 26. maddesinde güvence altına alınan ifade özgürlüğü arasında Anayasa Mahkemesi içtihadında ortaya konulan kriterlere uygun şekilde bir denge kurulması gerekmektedir. İnternet ortamının sağladığı ulaşılabilirlik, yaygınlık, haber ve fikirlerin depolanmasındaki ve muhafazasındaki kolaylık dikkate alındığında yayımlandığı tarihte belirli ağırlık eşiğini aşmayan veya kişinin kendi eylemlerinden kaynaklanan haber ve yazıların İnternet ortamında uzun süre erişilebilir kalması kişilerin şeref ve itibarını zedeleyebilir (N.B.B., § 37).

26. Anayasa Mahkemesi, 3/3/2016 tarihli ve 2013/5653 numaralı N.B.B. başvurusunda İnternet'in etkin olarak kullanmasıyla beraber ifade ve basın özgürlükleri ile şeref ve itibarın korunması arasındaki dengenin ilki lehine bozulduğunu, bu dengenin tekrar kurulabilmesinin şeref ve itibar yönünden bireylerin unutulma hakkının kabul edilmesi ile mümkün olabileceğini belirtmiştir (N.B.B., § 46).

27. Anayasa Mahkemesi, bahsi geçen başvuruda unutulma hakkının Anayasal dayanaklarına yer vererek devletin bireye geçmişte yaşadıklarının başkaları tarafından öğrenilmesi engellenerek “yeni bir sayfa açma” olanağı verme hususunda bir sorumluluğu olduğunu, dolayısıyla unutulma hakkının kişilerin manevi varlıklarını geliştirmelerine bir fırsat vermek açısından devletin pozitif yükümlülüğünün bir sonucu olduğunu ortaya koymuştur (N.B.B., §§ 47-49).

28. Bununla birlikte Mahkeme, unutulma hakkının İnternet üzerindeki her türlü haber veya yazı yönünden uygulanmasını beklemenin mümkün olmadığını, özellikle basın özgürlüğü temelinde gazete arşivinin araştırmacılar, hukukçular veya tarihçiler için önem taşıyan veriler olduğunu belirtmiştir. Unutulma hakkı, İnternet ortamında haber arşivini koruma altına alan basın özgürlüğünün ve halkın haber ve fikirlere ulaşma özgürlüğünün özüne dokunmayacak ve aynı zamanda hak sahibinin çıkarlarını koruyacak şekilde kullanılmalıdır. Mahkeme, İnternet ortamındaki bir haber veya yazının unutulma hakkı kapsamında İnternet'ten çıkarılabilmesi için yayının içeriği, yayında kaldığı süre, güncelliğini yitirme, tarihsel bir veri olarak kabul edilememe, kamu yararına katkısı (toplumsal açıdan haberin değeri, haberin geleceğe ışık tutan niteliği) haber veya yazıya konu kişinin siyasetçi veya ünlü olup olmadığı, haber veya yazının konusu, bu bağlamda haber ya da yazının olgusal gerçekler veya değer yargısı içerip içermediği, halkın ilgili veriye yönelik ilgisi gibi hususların somut olay açısından incelenmesi gerekliliğini ortaya koymuştur (N.B.B., § 50).

29. Somut olayda başvurucunun şikâyetine konu olan haber ve yazılar 28/6/2010 ile 14/2/2014 tarihleri arasında yayımlanmış ve arşiv niteliğindedir. Haber ve yazılar genel olarak başvurucunun İzmir Büyükşehir Belediyesi bünyesinde aldığı görevler ve siyasi yaşamı ile bağlantılıdır. Söz konusu haber ve yazılarda; Belediye bünyesindeki şirketlerde yürüttüğü idari görevlerin ardından 2010 yılında CHP Buca ilçe başkan yardımcısı seçilmiş, başkan yardımcılığı görevinin sonrasında da aktif olarak siyasi yaşamın içinde bulunmuş olan başvurucuya ilişkin eleştirel nitelikte ifadeler yer almaktadır. Haberlerin başlıkları ile içerikleri incelendiğinde amacın kamuoyunun ilgisine matuf, CHP Buca ilçe başkan yardımcılığı görevini icra etmiş ve haber ile yazıların yayımlandığı dönemde aktif olarak siyasi yaşamın içinde bulunan başvurucu hakkında kamuoyunu bilgilendirmek olduğu görülmektedir.

30. Başvurucu, kendisi hakkında yayımlanan ilk yazıdan 4 yıl 1 ay, son yazıdan da 6 ay sonra 19/8/2014 tarihinde haber ve yazı içeriklerine erişimin engellenmesi talebiyle İzmir 2. Sulh Ceza Hâkimliğine başvuruda bulunmuştur. Hâkimlik, başvurucunun şeref ve itibarının korunması ile kamu yararı bağlamında yaptığı değerlendirme neticesinde söz konusu yayınların basın özgürlüğü kapsamında kaldığını belirterek (bkz. § 12) 20/8/2014 tarihli kararı ile talebin reddine karar vermiştir.

Başvurucunun anılan karara itirazı da İzmir 3. Sulh Ceza Hâkimliğinin 27/8/2014 tarihli kararı ile reddedilmiştir.

31. Başvuru tarihi itibarıyla söz konusu haber ve yazılardan ilkinin yayın tarihi olan 28/6/2010 tarihi üzerinden 4 yıl 3 ay, son yazının yayın tarihi olan 14/2/2014 tarihi üzerinden ise 7 aylık bir süre geçmiştir. Bu süreler ile hakkında haber yapılan kişinin kimliği de dikkate alındığında haberin güncelliğini ve kamuoyu ilgisini yitirdiği söylenemez. Bu bağlamda haberin konusu, içeriği ve ilk yayın tarihi üzerinden geçen süre gözönünde bulundurulduğunda toplumsal açıdan, haber ve yazıların arşivde kolaylıkla ulaşılabilir kılınması için gerekli haber ve bilgilendirme değerinin devam ettiği, bu bağlamda unutulma hakkı kapsamında değerlendirilmeyi zorunlu kılacak şartların oluşmadığı belirlenmiştir. Sonuç olarak ifade ve basın özgürlükleri ile birlikte halkın haber alma ve bilgiye ulaşma hakkı birlikte değerlendirildiğinde başvuru konusu olayda ifade ve basın özgürlükleri ile kişinin manevi bütünlüğünün korunması hakkı arasında adil bir dengenin kurulduğu, derece mahkemesinin takdir yetkisine müdahale etmeyi gerekli kılacak bir durumun bulunmadığı sonucuna ulaşılmıştır.

32. Açıklanan nedenlerle başvurunun diğer kabul edilebilirlik koşulları yönünden incelenmeksizin açıkça dayanaktan yoksun olması nedeniyle kabul edilemez olduğuna karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Şeref ve itibarın korunması hakkının ihlal edildiğine ilişkin iddianın açıkça dayanaktan yoksun olması nedeniyle **KABUL EDİLEMEZ OLDUĞUNA,**

B. Yargılama giderlerinin başvuru üzerinde **BIRAKILMASINA 5/10/2017 tarihinde OYBİRLİĞİYLE** karar verildi.

Anayasa Mahkemesi - Turgut Duman Kararı (2014/15365)

Turgut Duman, B. No: 2014/15365, 29/5/2019

Başvuru, kanunen verilmemesi gereken kişisel verinin idari makamlara açıklanması ve güvenlik soruşturmasına esas alınması nedeniyle özel hayata saygı hakkının; idare mahkemesince verilen kararda ceza soruşturmasına konu suçun işlendiği yönünde ifadeler bulunması nedeniyle masumiyet karinesinin ihlal edildiği iddialarına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

BİRİNCİ BÖLÜM

KARAR

TURGUT DUMAN BAŞVURUSU

(Başvuru Numarası: 2014/15365)

Karar Tarihi: 29/5/2019

BİRİNCİ BÖLÜM

KARAR

Başkan: Hasan Tahsin GÖKCAN

Üyeler: Burhan ÜSTÜN, Hicabi DURSUN, Kadir ÖZKAYA, Yusuf Şevki HAKYEMEZ

Raportör: Şermin BİRTANE

Başvurucu: Turgut DUMAN

Vekili: Av. Barış YAVUZ

I. BAŞVURUNUN KONUSU

1. Başvuru, kanunen verilmemesi gereken kişisel verinin idari makamlara açıklanması ve güvenlik soruşturmasına esas alınması nedeniyle özel hayata saygı hakkının; idare mahkemesince verilen kararda ceza soruşturmasına konu suçun işlendiği yönünde ifadeler bulunması nedeniyle masumiyet karinesinin ihlal edildiği iddialarına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 19/9/2014 tarihinde yapılmıştır.
3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.
4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.
5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.
6. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık görüşünü bildirmiştir.
7. Başvurucu, Bakanlığın görüşüne karşı süresinde beyanda bulunmuştur.

III. OLAY VE OLGULAR

8. Başvuru formu ve eklerinde ifade edildiği şekliyle olaylar özetle şöyledir:
9. 25/5/1981 doğumlu olan başvurucu, 28/12/1999 tarihinde Devrimci Halk Kurtuluş Partisi-Cephesi (DHKP-C) terör örgütüne yardım suçunu işlediği isnadına bağlı olarak gözaltına alınmış ve hakkında Adana 1. Devlet Güvenlik Mahkemesinde kamu davası açılmıştır. Söz konusu kovuşturma kapsamında 4/1/2000 tarihinde tutuklanan başvurucu yaklaşık bir yıl üç ay sonra 10/4/2001 tarihinde serbest bırakılmış ve yargılanmasına tutuksuz olarak devam edilmiştir. Yargılama sonucunda; Adana 1. Devlet Güvenlik Mahkemesinin 4/12/2001 tarihli kararıyla fiilin örgüte yardım ve yataklık türünde olduğu, süre itibarıyla koşulları oluştuğundan 21/12/2000 tarihli ve 4616 sayılı 23 Nisan 1999 Tarihine Kadar İşlenen Suçlardan Dolayı Şartla Salıverilmeye, Dava ve Cezaların Ertelenmesine Dair Kanun'un 1. maddesinin birinci fıkrasının dördüncü bendi gereğince davanın kesin hükme bağlanmasının ertelenmesine hükmedilmiştir. Adana 6. Ağır Ceza Mahkemesinin 2/4/2007 tarihli kararı ile de başvurucunun beş yıllık deneme süresi içinde başka suç işlemediği gerekçesiyle kamu davasının ortadan kaldırılmasına karar verilmiştir.
10. Ayrıca başvurucunun İçişleri Bakanlığına müracaatı üzerine 18/5/2007 tarihli yazıyla hakkındaki Genel Bilgi Toplama (GBT) kaydının iptal edildiği bildirilmiştir.
11. 16/3/2012 tarihinde Bakanlık tarafından verilen izne istinaden sözleşmeli ceza infaz kurumu şoförlüğü alımı için Hatay Adalet Komisyonu (Komisyon) Başkanlığı tarafından sınav yapılmıştır. Sınavla altı kişinin işe alınması planlanmıştır.

12. Başvurucunun söz konusu sınav dolayısıyla Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğünden temin ettiği 6/7/2012 tarihli adli sicil kaydı ve adli sicil arşiv kaydı belgesinde adli sicil ve arşiv kaydının bulunmadığı belirtilmiştir.

13. Komisyon Başkanlığınca yapılan yazılı ve sözlü sınavlar sonucunda başvuru 3. sırada başarılı olmuştur. Sözleşmeli ceza infaz kurumu şoförlüğüne yerleştirilmesi düşünülen başvuru hakkında, Komisyon Başkanlığınca güvenlik soruşturması işlemlerine başlanmıştır.

14. Hatay Valiliği İl Emniyet Müdürlüğü tarafından Komisyon Başkanlığına hitaben yazılan 8/5/2012 tarihli yazıda, başvuru hakkında istenen güvenlik soruşturması ve arşiv araştırması sonucunda yasadışı silahlı DHKP-C örgütüne yardım suçu ile ilgili Adana 1. Devlet Güvenlik Mahkemesince verilen 4/12/2001 tarihli kararın gönderildiği bildirilmiştir. Söz konusu yazı ekinde 4/12/2001 tarihli kararın tamamının değil sanık isimlerinin bulunduğu 1., 2., 3. ve 4. sayfalarının ve hüküm fıkrasının yer aldığı 15., 16. ve 17. sayfalarının gönderildiği görülmekte olup bu kısımlarda başvuru hakkında hangi eylemleri işlediği konusunda bilgi bulunmamaktadır.

15. Komisyon Başkanlığının 21/5/2012 tarihli kararı ile başvuru hakkında yargılamaya konu eyleminin niteliği dikkate alınarak istihdam edilmesinin uygun olmadığına karar verilmiş ve bu karar başvuru hakkında bildirilmiştir.

16. Bunun üzerine başvuru tarafından Bakanlık ve Komisyon Başkanlığı aleyhine atama işleminin yapılmaması nedeniyle Hatay İdare Mahkemesi nezdinde iptal davası açılmıştır.

17. Başvuru ayrıca Türkiye Büyük Millet Meclisi (TBMM) İnsan Haklarını İnceleme Komisyonuna (İnceleme Komisyonu) müracaatta bulunmuştur. İnceleme Komisyonunun 16/7/2013 tarihli yazısında; davanın ortadan kaldırılmasına, adli sicil, arşiv ve emniyet kayıtlarının silinmesine rağmen başvuru hakkında ilk yargı kararına dair bilgilerinin Hatay İl Emniyet Müdürlüğü tarafından paylaşılmasının hukuka aykırı olduğu görüşü bildirilmiştir.

18. Başvuru Hatay İdare Mahkemesine (Mahkeme) verdiği 24/7/2013 tarihli dilekçesinde İnceleme Komisyonunun görüş yazısını da sunmak suretiyle silinmiş suç kayıtlarının Hatay İl Emniyet Müdürlüğü tarafından paylaşılmasının hukuka aykırı olduğunu belirtmiştir. Başvuru Mahkemeye sunduğu 10/10/2012 tarihli dilekçesinde, GBT kayıtlarının silinmiş ve yargı kararıyla davanın ortadan kaldırılmış olmasının yok sayıldığını, hakkında herhangi bir mahkûmiyet içermeyen sicilin ne zamana kadar saklanacağını, bunun süresiz olarak saklanmasının mümkün olmadığını ifade etmiş ve Anayasa'nın 41. ve 70. maddelerinde yer alan temel haklarının ihlal edildiğini ileri sürmüştür.

Başvurucu aynı yöndeki iddialarını yürütmenin durdurulmasının reddi kararına itiraz ve temyiz dilekçelerinde de tekrar etmiştir.

19. Mahkeme 7/3/2013 tarihli kararıyla davayı reddetmiştir. Kararda, ceza infaz kurumları ile tutukevlerinde çalıştırılacak personel hakkında güvenlik soruşturması ve arşiv araştırması yapılmasının zorunlu olduğu, idarenin atama yapıp yapmamak konusunda takdir yetkisinin bulunduğu ifade edilmiştir. Kararda; ceza yargılamasında davanın kesin hükme bağlanmasının ertelenmesine karar verildiği, bu kararın başvurusunun üzerine atılı suçu işlemediği anlamına gelmeyeceği, hakkında verilmiş bir beraat kararı da bulunmadığı belirtilmiştir. Bu durumda başvurusunun atanmak istediği görevin önem ve özelliği ile güvenlik soruşturmasında elde edilen bilgiler gözetildiğinde, başvurusunun atanmamasına ilişkin işlemde hukuka aykırılık bulunmadığı gerekçesine yer verilmiştir. Kararın gerekçesinin ilgili kısmı şöyledir:

“Bu durumda, davacının, üzerine atılı eyleminden dolayı hakkında yapılan yargılamada davanın kesin hükme bağlanmasının ertelenmesine karar verildiği, bu kararın davacının üzerine atılı suçu işlemediği anlamına gelmeyeceği, davacının üzerine atılı suçu işlemediği yönünde verilmiş bir beraat kararı da bulunmadığı, kaldı ki, güvenlik soruşturmasında elde edilen bilgiler ve davacının atanmak istediği görevin nitelikleri ve hassasiyeti göz önüne alındığında, atama yapıp yapmamak konusunda idarenin takdir yetkisinin olduğu ve bu yetkinin kamu yararı ve hizmet gerekleri gözetilerek kullanıldığı anlaşıldığından davacının istihdam edilmesinin uygun görülmediğine ilişkin dava konusu işlemde hukuka aykırılık bulunmamıştır.”

20. Başvurusunun temyiz istemi Danıştay Onikinci Dairesinin 19/9/2013 tarihli kararıyla reddedilerek hüküm onanmıştır.

21. Karar düzeltme istemi ise aynı Dairenin 16/5/2014 tarihli kararıyla reddedilmiştir. Anılan karar 22/8/2014 tarihinde başvurucuya tebliğ edilmiştir.

22. Başvurucu 19/9/2014 tarihinde bireysel başvuruda bulunmuştur.

23. Bunun yanı sıra Anayasa Mahkemesince Hatay Valiliği İl Emniyet Müdürlüğünden başvuru hakkındaki Adana 1. Devlet Güvenlik Mahkemesinin 4/12/2001 tarihli kararının nasıl ve nereden tespit edildiği sorulmuştur. Hatay Valiliği İl Emniyet Müdürlüğü tarafından verilen 11/4/2018 tarihinde kayda alınan cevapta; başvurusunun yargılanmış olduğunun kayıtlarının tetkikinden anlaşıldığı, bunun üzerine Adana İl Emniyet Müdürlüğü ile yapılan yazışma sonucunda söz konusu Mahkeme kararının temin edildiği bildirilmiştir.

24. Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğünün 25/6/2018 tarihli yazısında; 4616 sayılı Kanun'a göre verilmiş erteleme kararlarının kesinleşmiş mahkûmiyet hükmü niteliğinde bulunmadığı, bu nedenle bir sicil kaydı olmadığı, bilgi mahiyetinde kayda alındığı belirtilmiştir. 4616 sayılı Kanun'a göre verilmiş erteleme kararlarının 25/5/2005 tarihli ve 5352 sayılı Adli Sicil Kanunu'nun 6. maddesi uyarınca sadece soruşturma ve kovuşturma kapsamında mahkeme, hâkim, askerî hâkim, Cumhuriyet başsavcılığı veya askerî savcılık tarafından istenmesi hâlinde verilmek üzere sicil kayıtlarından ayrı bir yerde sistemde tutulduğu bildirilmiştir. Söz konusu yazıda ayrıca 4616 sayılı Kanun'a göre verilmiş erteleme kararlarının kamu görevlerine yapılacak atamalar dolayısıyla güvenlik soruşturması kapsamında ilgili kamu kurumlarına verilemeyeceği ifade edilmiştir.

IV. İLGİLİ HUKUK

A. Ulusal Hukuk

1. İlgili Mevzuat

25. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Özel nitelikli kişisel verilerin işleme şartları" kenar başlıklı 6. maddesinin ilgili kısımları şöyledir:

“(1)Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3)Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir....”

26. 6698 sayılı Kanun'un "İstisnalar" kenar başlıklı 28. maddesinin birinci fıkrasının (ç) ve (d) bentleri şöyledir:

“ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi...”

27. 4616 sayılı Kanun'un olay tarihinde yürürlükte olan hâliyle 1. maddesinin birinci fıkrasının dördüncü bendi şöyledir:

“23 Nisan 1999 tarihine kadar işlenmiş ve ilgili kanun maddesinde öngörülen şahsî hürriyeti bağlayıcı cezanın üst sınırı on yılı geçmeyen suçlardan dolayı haklarında henüz takibata geçilmemiş veya hazırlık soruşturmasına girişilmiş olmakla beraber dava açılmamış veya son soruşturma aşamasına geçilmiş olmakla beraber henüz hüküm verilmemiş veya verilen hüküm kesinleşmemiş ise, davanın açılması veya kesin hükme bağlanması ertelenir; varsa tutukluluk halinin kaldırılmasına karar verilir. Bu suçlarla ilgili dosya ve deliller, bu bentte öngörülen sürelerin sonuna kadar muhafaza edilir.

Erteleme konusu suç kabahat ise bir yıl, cürüm ise beş yıl içinde bu kabahat veya cürüm ile aynı cins veya daha ağır şahsî hürriyeti bağlayıcı cezayı gerektiren bir suç işlendiğinde, erteleme konusu suçtan dolayı da dava açılır veya daha önce açılmış bulunan davaya devam edilerek hüküm verilir. Öngörülen süreler, erteleme konusu kabahat veya cürüm ile aynı cins veya daha ağır şahsî hürriyeti bağlayıcı cezayı gerektiren bir suç işlenmeksizin geçirildiğinde, ertelemeden yararlanan hakkında kamu davası açılmaz, açılmış olan davanın ortadan kaldırılmasına karar verilir.”

28. 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu'nun 48. maddesinin ilgili kısımları şöyledir:

"Devlet memurluğuna alınacaklarda aşağıdaki genel ve özel şartlar aranır.

A) Genel şartlar:

Türk Ceza Kanununun 53 üncü maddesinde belirtilen süreler geçmiş olsa bile; kasten işlenen bir suçtan dolayı bir yıl veya daha fazla süreyle hapis cezasına ya da affa uğramış olsa bile devletin güvenliğine karşı suçlar, Anayasal düzene ve bu düzenin işleyişine karşı suçlar, (...) zimmet, irtikâp, rüşvet, hırsızlık, dolandırıcılık, sahtecilik, güveni kötüye kullanma, hileli iflas, ihaleye fesat karıştırma, edimin ifasına fesat karıştırma, suçtan kaynaklanan malvarlığı değerlerini aklama veya kaçakçılık suçlarından mahkûm olmamak.

...

B) Özel şartlar:

...

2. Kurumların özel kanun veya diğer mevzuatında aranan şartları taşımak."

29. 10/7/2003 tarihli ve 25164 sayılı Resmî Gazete'de yayımlanan Adalet Bakanlığı Memur Sınav, Atama ve Nakil Yönetmeliği'nin "Özel şartlar" kenar başlıklı 6. maddesinin ilgili kısımları şöyledir:

"18) Ceza infaz kurumları ve tutukevleri ile denetimli serbestlik müdürlüklerinde görev alacak bütün unvanlardaki personel için ayrıca aranacak şartlar;

...

b) Güvenlik soruşturması olumlu olmak,"

30. 26/10/1994 tarihli ve 4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun'un 1. maddesi şöyledir:

"Güvenlik Soruşturması ve Arşiv Araştırması; kamu kurum ve kuruluşlarında, yetkili olmayan kişilerin bilgi sahibi olmaları halinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile askeri, emniyet ve istihbarat teşkilatlarında çalıştırılacak kamu personeli ve ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında yapılır.

Devletin güvenliğini, ulusun varlığını ve bütünlüğünü iç ve dış menfaatlerinin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeler ile gizlilik dereceli kamu personeli ile meslek gruplarının tespiti, birim ve kısımların tanımlarının yapılması, güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak merciler ve üst kademe yöneticilerinin kimler olduğu Bakanlar Kurulu Kararı ile yürürlüğe konulacak yönetmelik ile düzenlenir."

31. 12/4/2000 tarihli ve 24018 sayılı Resmî Gazete'de yayımlanan Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği'nin (Yönetmelik) "Kapsam" kenar başlıklı 2. maddesi şöyledir:

"Bu Yönetmelik; yetkili olmayan kişilerin bilgi sahibi olmaları halinde Devletin güvenliğinin, iç ve dış menfaatlerinin, ulusal varlığın ve bütünlüğün zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeleri, bunların toplanmasını ve işlemini yürüten bakanlıklar ile kamu kurum ve kuruluşlarının ilgili birim ve kısımlarının belirlenmesini, Türk Silahlı Kuvvetlerinde, emniyet ve istihbarat teşkilatlarında, ceza infaz kurumları ve tutukevlerinde çalışacak personeli, ayrıca bakanlıklar ile kamu kurum ve kuruluşlarının yurtdışı teşkilatlarında sürekli görevlendirilecek bütün personel için yapılacak güvenlik soruşturması ve arşiv araştırmasının esas ve usullerini, bunu yapacak mercileri, hakkında güvenlik soruşturması ve arşiv araştırması yapılacak gizlilik dereceli yerlerde çalışan kamu personeli ile meslek grupları ve üst kademe yöneticilerini kapsar."

32. Yönetmelik'in "Güvenlik soruşturması ve arşiv araştırması yapacak makamlar" kenar başlıklı 7. maddesi şöyledir:

"Güvenlik soruşturması ve arşiv araştırması, Milli İstihbarat Teşkilatı Müsteşarlığı, Emniyet Genel Müdürlüğü ve mahalli mülki idare amirlikleri tarafından yapılır.

İçişleri Bakanlığı Kaçakçılık İstihbarat Harekat ve Bilgi Toplama Dairesi Başkanlığı'ndaki bilgi kayıtları ile Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü'ndeki adli sicil kaydı, talepleri üzerine, güvenlik soruşturması ve arşiv araştırmasını yapacak makamlar ile Türk Silahlı Kuvvetlerinin ilgili birimlerine verilir."

33. Yönetmelik'in "Hakkında güvenlik soruşturması ve arşiv araştırması yapılacak personel" kenar başlıklı 8. maddesinin birinci ve ikinci fıkraları şöyledir:

"Güvenlik soruşturması ve arşiv araştırması; gizlilik dereceli birim ve kısımlar ile askeri, emniyet, istihbarat teşkilatlarında ve ceza infaz kurumları ve tutukevlerinde çalıştırılacak personel hakkında yapılır.

Emniyet Genel Müdürlüğü ve mahalli mülki idare amirlikleri, güvenlik soruşturması ve arşiv araştırmasını; bakanlıklar, kamu kurum ve kuruluşlarının gizlilik dereceli birim ve kısımları ile yurtdışı teşkilatında ve askeri, emniyet, istihbarat teşkilatlarında ve ceza infaz kurumu ve tutukevlerinde çalıştırılacak personel hakkında yapar."

34. Yönetmelik'in "Güvenlik soruşturması ve arşiv araştırmasında araştırılacak hususlar" kenar başlıklı 11. maddesi şöyledir:

"Güvenlik soruşturması ve arşiv araştırmasında kişinin içinde bulunduğu ortam da dikkate alınarak:

a) Kimlik kontrolü, kimlik kayıtlarının doğruluk derecesi, uyrukluđu, geçmişte yabancı bir devletin uyrukluđuna girip girmediđi,

b) Kolluk kuvvetleri tarafından halen aranıp aranmadıđı, kolluk kuvvetlerinin ve istihbarat ünitelerinin arşivlerinde bilgiler bulunup bulunmadıđı, adli sicil kaydının ve hakkında bir tahdidin olup olmadıđı,

c) Yıkıcı faaliyetlerde bulunup bulunmadıđı ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanuna ve Atatürk ilke ve inkılaplarına aykırı davranıp davranmadıđı.

d) Şeref ve haysiyetini ihlal edecek ve görevine yansıyacak şekilde kumara, uyuşturucuya, içkiye, paraya ve aşırı bir şekilde menfaatine düşkün olup olmadıđı, ahlak ve adaba aykırı davranıp davranmadıđı,

e) Yabancılarla, özellikle hasım ve hasım olması muhtemel Devlet mensupları ve temsilcileriyle ilgili derecesinin iç yüzü ve nedeni,

f) Sır saklama yeteneđinin olup olmadıđı,

araştırılır."

35. Yönetmelik'in "Güvenlik soruşturması ve arşiv araştırmasında izlenecek yöntem" kenar başlıklı 12. maddesi şöyledir:

"Bu Yönetmelik kapsamına giren bakanlıklar ile kamu kurum ve kuruluşlarınca yaptırılacak güvenlik soruşturması ve arşiv araştırmasında aşağıdaki yöntem izlenir:

a) Güvenlik soruşturması ve arşiv araştırması formundaki sorular nüfus kayıtlarında yapılan tashih ve değişiklikler belirtilmek ve isimler açıkca yazılmak suretiyle cevaplandırılır ve nüfus cüzdanı örneği noksansız olarak doldurularak istek yazısı ekinde soruşturmayı yapan makama bildirilir.

b) Hakkında güvenlik soruşturması ve arşiv araştırması yapılması istenilen kişiler için kurum ve kuruluşunca Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğünden sağlanan adli sicil kaydıyla ekteki formdan bir örneği kişinin nüfusa kayıtlı olduğu il valiliğine, bir örneği ikamet ettiği il valiliğine, bir örneği Emniyet Genel Müdürlüğüne, bir örneği de ilgisine göre Milli İstihbarat Teşkilatı Müsteşarlığına gönderilir. Bir örneği de istekte bulunan kurum ve kuruluşun dosyasında saklanır. Türk Silahlı Kuvvetlerince yaptırılacak arşiv araştırmalarında forma adli sicil kaydının eklenmesi zorunlu değildir.

c) Güvenlik soruşturması ve arşiv araştırması yapılması isteminin ilgili makama ulaşmasından itibaren arşiv araştırması sonuçları en geç 30 gün, güvenlik soruşturması sonuçları en geç 60 gün içinde cevaplandırılır. Soruşturma ve araştırma sonucunu içeren bilgi ve belgeler ilgilinin güvenlik makamlarındaki dosyasında asgari 'gizli' gizlilik derecesinde saklanır.

d) Güvenlik soruşturması ve arşiv araştırmasını isteyen makama, kişi hakkında karar vermeye yeterli bilgiler aktarılır.

e) Güvenlik soruşturması ve arşiv araştırmasının nasıl ve ne şekilde yapılacağı, soruşturma ve araştırma yapmaya yetkili makamların görev talimatları ile belirlenir.

f) Mahalli mülki idare amirliklerince yapılmış olan güvenlik soruşturması ve arşiv araştırmasında olumsuz durumu saptananların evrakın bir örneği dosya açılmak üzere Emniyet Genel Müdürlüğüne gönderilir.

g) Güvenlik soruşturması ve arşiv araştırmasında olumsuz durumu saptananlarla ilgili bilgiler Milli İstihbarat Teşkilatı Müsteşarlığı ve Emniyet Genel Müdürlüğüne karşılıklı olarak birbirlerine aktarılır.

..."

36. 5352 sayılı Kanun'un 6. maddesi şöyledir:

“Kamu davasının açılmasının ertelenmesine ve hükmün açıklanmasının geri bırakılmasına ilişkin kararlar, ancak bir soruşturma veya kovuşturmayla bağlantılı olarak mahkeme, hâkim, askerî hâkim, Cumhuriyet Başsavcılığı veya askerî savcılık tarafından istenmesi halinde verilmek üzere kaydedilir.”

37. Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü tarafından çıkarılan 17/12/2007 tarihli ve "4616 Sayılı Kanun'a İlişkin Erteleme Kararları" konulu Genelge'nin ilgili kısmı şöyledir:

“...4616 sayılı Kanuna göre verilmiş erteleme kararları kesinleşmiş mahkûmiyet hükmü niteliğinde bulunmadığı nedenle bir sabıka kaydı olmayıp, bilgi mahiyetinde kayda alınıp, sadece soruşturma ve kovuşturma kapsamında mahkeme, hâkim, askeri hâkim, Cumhuriyet başsavcılığı veya askeri savcılık tarafından istenmesi halinde verilmek üzere sabıka kayıtlarından ayrı bir yerde tutulmaktadır. Bu kayıtları tutan Genel Müdürlüğümüzün kayıtlara ilişkin davaların dava zamanaşımı süresi içerisinde zanlının başka bir suç işleyip işlemediğini tespit etme imkânı bulunmadığı gibi, erteleme kararı veren merciin 4616 sayılı Kanununun 1/4. maddesinde belirtilen şartların gerçekleşmesi halinde, ertelemeden yararlanan hakkında kamu davasının açılmamasına karar verilmesi ve kesinleşmesini takiben Genel Müdürlüğümüze gönderilmesi halinde bu bilgilerin kayıtlarımızdan çıkarılabileceği izahtan varestedir.”

38. Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü tarafından çıkarılan 1/1/2006 tarihli ve 56 sayılı Genelge'nin ilgili kısımları şöyledir:

“... ”

2) 23 Nisan 1999 tarihine kadar işlenmiş suçlardan dolayı ...sanıklar hakkında öngörülen ...kesin hükme bağlanmasının ertelenmesi'kararlarına dayalı olarak düzenlenecek tali karar fişlerinde ;...ertelemenin 4616 sayılı Kanun hükümlerine dayandığının (14) numaralı sütunda mutlaka belirtilmesi...bu şekilde tanzim edilen tali karar fişlerinin üç gün içerisinde Adli Sicil ve İstatistik Genel Müdürlüğüne gönderilmesi

...

4) Adli sicil müdürlükleri veya şefliklerince, 4616 sayılı Kanun uyarınca verilen erteleme kararlarına dair adli sicil bilgilerinin sadece soruşturma ve kovuşturma konusu olan işler nedeniyle Cumhuriyet Başsavcılıkları ve mahkemelerce istenildiğinde verilmesi gerektiğinin bilinmesi.

...konularında gereken dikkat ve özenin gösterilmesini rica ederim. ”

39. Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğünün 25/6/2018 tarihli yazısının ilgili kısımları şöyledir:

"Açıklanan nedenlerle; 5352 sayılı Adli Sicil Kanununun 6 ncı maddesinde ve söz konusu Genelgede 4616 sayılı Kanuna göre verilmiş erteleme kararlarının kesinleşmiş mahkûmiyet hükmü niteliğinde bulunmadığından bir sicil kaydı olmadığı, bilgi mahiyetinde kayda alınıp, sadece soruşturma ve kovuşturma kapsamında mahkeme, hâkim, askeri hâkim, Cumhuriyet başsavcılığı veya askeri savcılık tarafından istenmesi hâlinde verilmek üzere sicil kayıtlarından ayrı bir yerde, mahsus sistemde tutulmakta olup, kamu görevlerine yapılacak atamalar dolayısıyla güvenlik soruşturması kapsamında ilgili kamu kurumlarına verilmemesi gerektiği,

Genel Müdürlüğümüzce yapılan değerlendirme sonucunda, konuya ilişkin olarak ilgili mevzuat hükmü uygulamanın yukarıda zikredildiği şekilde olduğu hususunu,

Bilgilerinize arz ederim."

2. 4616 sayılı Kanun'la Düzenlenen Ertelemenin Hukuki Niteliği ile İlgili Yargı Kararları

40. Anayasa Mahkemesi 4616 sayılı Kanun'un 1. maddesinin birinci fıkrasının dördüncü bendini eşitlik ilkesine aykırı bularak iptal etmiştir. Anayasa Mahkemesinin söz konusu kararında af, şartla salıverilme ve erteleme kavramlarının hukuki nitelikleri açıklanmıştır. Anayasa Mahkemesinin 18/7/2001 tarihli ve E.2001/4, K.2001/332 sayılı kararının ilgili kısımları şöyledir:

"...Erteleme, (tecil) işlediği suçtan dolayı mahkûm edilen suçluya ait cezanın infazının belirli bir süre ile geri bırakılması ve suçlu bu süre içinde yeniden bir suç işlemediği takdirde suçun ya işlenmemiş veya hükümlülüğünün gerçekleşmemiş ya da cezanın çekilmiş sayılmasıdır.

...

Türk Hukukunda cezanın ertelenmesi, hükümlüye bir deneme süresi tanıyarak cezanın yerine getirilmesini bu sürenin sonuna bırakan, bu süreyi suç işlemeden geçiren hükümlünün mahkûmiyetini 'vaki olmamış' sayan bir olanaktır.

...

Erteleme cezanın infazını geri bırakan kanuni bir sebep, bir bakıma ise şartlı bir af diğer yönden de şartlı bir hükümlülük niteliğindedir. Bu durumda 'ertelemenin' Ceza Hukukundaki diğer müesseselerle kıyaslanmasından onun 'müstakil', 'sui generis(kendine özgü)' bir yapıya sahip olduğu sonucuna varılmaktadır."

41. Danıştay Birinci Dairesinin 18/4/2001 tarihli ve E.2001/33, K.2001/47 sayılı kararının ilgili kısımları şöyledir:

“İstem, 23 Nisan 1999TarihineKadarİşlenenSuçlardanDolayıŞartla Salıverilmeye, Dava ve Cezaların Ertelenmesine Dair 4616 sayılı Kanun’dan yararlananların657sayılıDevletMemurları Kanununa göre Devlet memurluğuna alınıp alınamayacakları, bunlardan memur olanların memurluğuna son verilip verilemeyeceği ve 4616 sayılı Kanun kapsamına giren bir suçtan dolayı haklarında takibata geçilen veya dava açılan memurların isnad edilen suçu işlemediğini belirterek dava açılmasını ya da açılan davaya devam edilerek hüküm verilmesini ilgili mercilerden isteyip isteyemeyecekleri, memur olmaya engel hüküm verilmesi halinde memurluğun sona ermesinin mümkün olup olmadığı hususlarında düşülen duraksamanın giderilmesine ilişkindir.

...İstem karara bağlanabilmesi için öncelikle 657 sayılı Kanunun 48 inci maddesinin (A) bendinin 5 inci fıkrasında yer alan 'hükümlü bulunmamak' ibaresinin anlam ve niteliğinin açıklığa kavuşturulması gerekmektedir. ...Yargı yerlerinin yerleşik kararlarında 657sayılıKanunun48inci maddesinin(A)bendinin5incifıkrasındaöngörülen'hükümlübulunmamak' ibaresi, yargı yerinin son kararı üzerine kanun yollarına başvurulmaması veya başvurulmuş ise bu yolların tüketilmesi sonucu kesinleşmiş bir hükme dayalı ceza mahkumiyetinin olmaması gerektiği biçiminde değerlendirilmekte ve uygulama da bu doğrultuda bulunmaktadır.

Açıklanan nedenlerle;

1- 657 sayılı Kanunun 48 inci maddesinin (A) bendinin 5 inci fıkrasında sayılan suçlar dışında ve 6 aydan fazla hapis veya ağır hapis cezası gerektiren ve cezanın üst sınırı on yılı geçmeyen bir suç işlediği öne sürülen Devlet memurlarından, 4616 sayılı Kanun gereğince haklarında takibata geçilmemiş veya hazırlık soruşturmasına girilmiş olmakla beraber dava açılmamış veya son soruşturma aşamasına geçilmiş olmakla birlikte henüz hüküm verilmemiş veya verilenhükümkesinleşmemişolanların,657 sayılı Kanunun 48 inci maddesinde belirtilen Devlet memuru olmaya engel sayılan bir cezadan dolayı haklarında kesinleşmiş mahkumiyet kararının bulunmaması nedeniyle memuriyet görevlerine son verilemeyeceği...

Sonuçlarına ulaşılmıştır.”

B. Uluslararası Hukuk

1. Uluslararası Belgeler

42. 18/2/2016 tarihli ve 29628 sayılı Resmî Gazete'de yayımlanan 6669 sayılı Kanun'la uygun bulunan 28/1/1981 tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "Özel veri kategorileri" kenar başlıklı 6. maddesi şöyledir:

"İç hukukta uygun güvenceler sağlanmadıkça, ırksal kökeni, siyasi düşünceleri, dini veya diğer inançları ortaya koyan kişisel veriler ile sağlık veya cinsel hayatla ilgili kişisel veriler, otomatik işleme tabi tutulmaz. Aynı durum ceza mahkumiyetiyle ilgili kişisel veriler için de geçerlidir."

2. Avrupa İnsan Hakları Sözleşmesi ve Avrupa İnsan Hakları Mahkemesi İçtihadı

43. Avrupa İnsan Hakları Sözleşmesi'nin (Sözleşme) "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesi şöyledir:

"(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."

44. Avrupa İnsan Hakları Mahkemesi (AİHM), devletlerin millî güvenliğin korunması amacını gerçekleştirmede sahip oldukları takdir yetkisinin geniş olduğunu kabul etmektedir. AİHM, Sözleşme'ye taraf devletlerin millî güvenliği korumak için yetkili ulusal makamlarına ilk olarak kişiler hakkında bilgi toplama ve halka açık olmayan siciller tutma, ikinci olarak millî güvenlik bakımından önemli kadrolarda çalışmak isteyen adayların bu işe uygunluğunu takdir ederken bu bilgiyi kullanma yetkisi veren kurallara sahip olmaları gerektiğinde kuşku bulunmadığını belirtmektedir (Leander/İsveç, B. No: 9248/81, 26/03/1987, § 59).

45. Bununla birlikte AİHM içtihadına göre kamu mercilerinin bir bireyin özel hayatıyla ilgili bilgileri toplaması, kaydetmesi, saklaması, özel hayata saygı hakkına müdahale oluşturur (Leander/İsveç, § 48; Kopp/İsveç, B. No: 23224/94, 25/3/1998, § 53; Amann/İsveç [BD], B. No: 27798/95, 16/2/2000, § 69; Rotaru/Romanya [BD], B. No: 28341/95, 4/5/2000, §§43, 44, 46).

46. AİHM'e göre bir kişinin özel yaşamına ilişkin verilerin kaydedilmesi ve saklanması, kendi başına özel hayata saygı hakkı bakımından bir müdahale oluşturmaktadır. Bu müdahalenin tespiti için kaydedilen bilgilerin daha sonra kullanılmış olması gibi bir koşul da aranmamaktadır. Bununla birlikte kamu makamları tarafından muhafaza edilen kişisel verilerin, Sözleşme'nin 8. maddesinde öngörülen unsurlardan birini devreye sokup sokmadığını tespit etmek için bu bilgilerin hangi çerçevede alındıklarının ve muhafaza edildiklerinin, verilerin türünün, kullanıldıkları ve işlendikleri

şeklin ve bunlardan çıkarılabilecek sonuçların dikkate alınması zaruridir (S. ve Marper/Birleşik Krallık [BD], B. No: 30562/04, 30566/04, 4/12/2008, § 67).

47. AİHM'e göre kişisel verilerin korunması, Sözleşme'nin 8. maddesinde öngörülen özel hayata saygı hakkından kişinin yararlanması konusunda büyük öneme sahiptir. İç hukuk kişisel verilerin bu maddede öngörülen güvencelere uygun olmayan şekilde kullanımını engellemek için gerekli güvenceleri sağlamalıdır. Bu tür güvencelerin bulunmasının gerekliliği, otomatik işleme tabi tutulan kişisel verilerin korunması söz konusu olduğunda özellikle de bu verilerin polis tarafından kullanılması hâlinde daha fazla hissedilmektedir. İç hukuk, bu verilerin saklanma amaçlarına uygun ve aşırıktan uzak olmalarını sağlamalı ve verilerin kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde muhafaza edilmesini temin etmelidir. İç hukuk, aynı zamanda, kişisel verilerin uygun olmayan şekillerde, keyfî ve yetki aşımı yapılarak kullanılmalarına karşı uygun güvenceler de içermelidir (S.ve Marper/Birleşik Krallık, § 103; M.M./Birleşik Krallık, B. No: 24029/07, 13/11/2012, § 195).

48. Ayrıca AİHM, kişilerin suç kayıtlarının tutulması ve kullanılması hakkında konuyu düzenleyen ilgili kanunun niteliğine ayrı bir önem vermektedir. AİHM, suç kayıtlarının tutulması ve kullanılmasına dair kanunun niteliği bakımından aynı telefon dinlemelerinde, gizli takipte ve gizli istihbarat toplamada dayanılan kanunlar yönünden olduğu gibi keyfî müdahalelere karşı bireyi korumak amacıyla yüksek bir standart aramaktadır. AİHM'e göre suç kayıtlarının tutulması ve kullanılmasına dair kanun, tıpkı telefon dinlemelerinde, gizli takipte ve gizli istihbarat toplamada olduğu gibi, tedbirlerin kapsamını ve uygulanmasını düzenleyen ve özellikle, süre, stoklama, kullanım, üçüncü kişilerin veriye erişimi, verilerin gizliliği ve bütünlüğünün korunmasına ve bunların imhasına ilişkin prosedürlere dair ve kişilerin, yetki aşımı ve keyfiliğe karşı yeteri kadar güvenceye sahip olmalarını sağlayacak açık ve detaylı hükümler içermelidir (S. ve Marper/Birleşik Krallık, § 99; M.M./Birleşik Krallık, § 195).

V. İNCELEME VE GEREKÇE

49. Mahkemenin 29/5/2019 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Özel Hayata Saygı Hakkının İhlal Edildiğine İlişkin İddia

1. Başvurucunun İddiaları ve Bakanlık Görüşü

50. Başvurucu; hakkında mahkûmiyet kararı bulunmadığını, Adana 1. Devlet Güvenlik Mahkemesince davanın kesin hükme bağlanmasının ertelenmesine hükmedildiğini, Adana 6. Ağır Ceza Mahkemesinin 2/4/2007 tarihli kararı ile de beş yıllık deneme süresi içinde başka suç işlemediği

gerekçesiyle kamu davasının ortadan kaldırılmasına karar verildiğini belirtmiştir. Başvurucu; GBT kayıtlarının, adli sicil ve arşiv kayıtlarının silindiğinin kendisine bildirilmesine rağmen kişisel veri olan söz konusu bilgilerin tekrar ortaya çıkarıldığını ve ceza infaz kurumuna şoför olarak atanmasının engellendiğini ve böylelikle özel hayatın gizliliğinin ihlal edildiğini ifade etmiştir. Bu nedenlerle başvurucu özel hayata saygı hakkının ihlal edildiğini ileri sürmüştür.

51. Bakanlık görüşünde; 4045 sayılı Kanun'un 1. maddesi doğrultusunda güvenlik soruşturması ve arşiv araştırması yapıldığı, anılan Kanun'un 1. maddesinin ikinci fıkrasına dayanılarak yürürlüğe konan Yönetmelik'te güvenlik soruşturması ve arşiv araştırmasının nasıl yapılacağı belirlendiği, bu çerçevede müdahalenin hukukilik unsurunu taşıdığı belirtilmiştir. Diğer taraftan atanmak istenen görevin nitelikleri ve hassasiyeti dikkate alındığında güvenlik araştırması yapılması konusunda meşru amacın olduğu, bu uygulamanın demokratik toplum gereklerine aykırı bir yönünün bulunmadığı ifade edilmiştir.

52. Bakanlık görüşüne karşı verilen cevapta, başvuru dilekçesinde yer alan hususlar tekrar edilmiştir.

2. Değerlendirme

53. Anayasa'nın 20. maddesinin ilgili kısımları şöyledir:

“Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

...

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.”

54. Özel hayata saygı hakkı kapsamında korunan hukuki menfaatlerden biri de bireyin mahremiyet hakkıdır. Mahremiyet hakkı bireyin kendisi hakkındaki bilgileri kontrol edebilme hukuksal çıkarını da kapsamaktadır. Kendisine ilişkin herhangi bir bilginin rızası olmaksızın açıklanmaması, yayılmaması, bu bilgilere başkaları tarafından ulaşılamaması ve rızası hilafına kullanılmaması, kısaca bu bilgilerin mahrem kalması konusunda bireyin menfaati bulunmaktadır. Bu husus, bireyin kendisi hakkındaki bilgilerin geleceğini belirleme hakkına işaret etmektedir (Serap Tortuk, B. No: 2013/9660, 21/1/2015, § 32).

55. Anayasa'nın özel hayata saygı hakkını düzenleyen 20. maddesinin üçüncü fıkrasında, herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme, bu veriler hakkında bilgilendirilme, verilere erişme, bunların düzeltilmesini veya silinmesini talep etme, verilerin amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkına sahip olduğu, kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hükmüne yer verilerek anayasal sınırlar belirlenmiştir.

56. Söz konusu Anayasa hükmünde kişilerin kendileri hakkındaki verilerin amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkına sahip olduğu özellikle vurgulanmıştır.

57. Anayasa Mahkemesi tarafından kişisel veri kavramının -belirli veya kimliği belirlenebilir olmak şartıyla- bir kişiye ilişkin bütün bilgileri ifade ettiği kabul edilmektedir (AYM, E.2014/74, K.2014/201, 25/12/2014; E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2013/84, K.2014/183, 4/12/2014; E.2014/180, K.2015/30, 19/3/2015; Bülent Kaya [GK], B. No: 2013/2941, 11/5/2016, § 49).

58. Bu bağlamda ceza mahkûmiyeti ile ilgili verilerin kişisel veri olduğu açıktır. Başvurunun temelinde başvuru hakkında verilen erteleme kararının kamu makamlarına verilmesi yani kişisel verisinin açıklanması hususu bulunmaktadır. Kişisel verilerin tutulması, saklanması veya aktarılmasının ise Anayasa'nın 20. maddesi bağlamında kişilerin özel hayatına saygı hakkı kapsamında incelenmesi gerektiği kuşkusuzdur. Bu nedenle başvurunun Anayasa'nın 20. maddesinde yer alan özel hayata saygı hakkı kapsamında değerlendirilmesi gerekmektedir (Fatih Saraman [GK], B. No: 2014/7256, 27/2/2019, § 57).

a. Kabul Edilebilirlik Yönünden

59. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan özel hayata saygı hakkının ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

b. Esas Yönünden

i. Müdahalenin Varlığı

60. Kamu mercileri tarafından özel yaşamı ile ilgili sorular sorulması da dâhil olmak üzere bir bireyin özel hayatı, iş ve sosyal yaşamıyla ilgili bilgilerinin alınması, kaydedilmesi, saklanması ve kullanılması özel hayata saygı hakkına müdahale oluşturur (Bülent Kaya § 51; Güzide Defne Samyeli, B. No: 2014/4399, 21/9/2016, § 67).

61. Somut olayda başvuruçunun devlet güvenlik mahkemesinde yargılanması sonucu verilen davanın kesin hükme bağlanmasının ertelenmesine dair kararın Hatay Valiliği İl Emniyet Müdürlüğü tarafından Komisyon Başkanlığına verildiği ve bu Mahkeme kararı dikkate alınarak başvuruçunun sözleşmeli ceza infaz kurumu şoförlüğüne atamasının yapılmadığı anlaşılmaktadır.

62. Resmî makamlar tarafından muhafaza edilmekte olan başvuruçunun hakkında yürütülen ceza yargılamasına dair bilgilerin özel hayata saygı hakkı anlamında kişisel veri olduğu açıktır (Fatih Saraman § 61). Söz konusu kişisel verilerin muhafaza edilmesi ve güvenlik soruşturmasında kullanılmasının, Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkına bir müdahale oluşturduğu sonucuna varılmıştır.

ii. Müdahalenin İhlal Oluşturup Oluşturmadığı

63. Anayasa'nın 13. maddesi şöyledir:

"Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz."

64. Yukarıda anılan müdahalenin ihlal oluşturup oluşturmadığının Anayasa'nın 13. maddesinde öngörülen ve somut başvuruya uygun düşen, kanunlar tarafından öngörülme, Anayasa'nın ilgili maddesinde belirtilen nedenlere dayanma, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmama koşulları yönünden incelenmesi gerekir. Bu bağlamda somut başvuruda öncelikle müdahalenin kanuni dayanağının bulunup bulunmadığı incelenmelidir.

(1) Genel İlkeler

65. Anayasa uyarınca temel hak ve özgürlüklere getirilen sınırlamaların öncelikle kanunla öngörülmüş olması gerekmektedir. Kanun ile sınırlama ölçütü veya kanunilik ilkesi Sözleşme'nin 8. maddesinde de bir sınırlama ve güvence ölçütü olarak yer almaktadır. Buna karşın Sözleşme'de yer alan kanunla öngörülmüş olma kavramı ile Anayasa'da yer alan kanunilik ilkesi tam olarak aynı değildir (Bülent Polat, B. No: 2013/7666,10/12/2015, § 73).

66. AİHM, kanunda öngörülen koşulları, bir diğer ifadeyle hukukiliği geniş yorumlayarak istikrar kazanmış yargı kararlarına dayanan içtihat yoluyla geliştirilmiş ilkelerin de hukukilik şartını karşılayabildiğini kabul ederken (Malone/İngiltere [BD], B. No: 8691/79, 2/8/1984, §§ 66-68; Sunday Times/Birleşik Krallık (No. 1) [BD], B. No: 6538/74, 26/04/1979, § 47) Anayasa, tüm sınırlandırmaların

mutlaka kanun ile yapılacağını öngörerek Sözleşme'den daha geniş bir koruma sağlamıştır (Mehmet Akdoğan ve diğerleri, B. No: 2013/817, 19/12/2013, § 31; Bülent Polat § 75).

67. Bununla birlikte temel hak ve hürriyetlerin sınırlandırılmasına ilişkin kanunların şeklen var olması yeterli değildir. Kanunilik ölçütü aynı zamanda maddi bir içeriği de gerektirmekte olup bu noktada kanunun niteliği önem kazanmaktadır. Kanunla sınırlama ölçütü sınırlamanın erişilebilirliğini, öngörülebilirliğini ve kesinliğini ifade etmekte; böylece uygulayıcının keyfî davranışlarının önüne geçtiği gibi kişinin hukuku bilmesine de yardımcı olmakta; bu yönüyle hukuk güvenliği teminatı sağlamaktadır (Halime Sare Aysal [GK], B. No: 2013/1789, 11/11/2015, § 62).

68. Kanunun bu gerekliliklere uygun olduğunun söylenebilmesi için yeterince ulaşılabilir olması, vatandaşların belirli bir olaya uygulanabilir nitelikteki hukuk kurallarının varlığı hakkında yeterli bilgiye sahip olabilmesi, ayrıca ilgili normun keyfiliğe karşı uygun bir koruma sağlaması, yetkili makamlara verilen yetkinin genişliğini ve icra edilme biçimlerini yeterli bir netlikte tanımlaması gerekmektedir (Halime Sare Aysal, § 63).

69. Hukukun kendisi -beraberinde getireceği idari pratiğin dışında- söz konusu işlemin meşru amacını da gözönünde tutarak keyfî müdahalelere karşı bireyi korumak için yetkili makamlara bırakılan takdir yetkisinin kapsamını yeterince açık bir şekilde göstermelidir. Hukuk sistemi vatandaşlara, kamu makamlarına hangi koşullarda ve hangi sınırlar içinde müdahalelerde bulunma yetkisi verdiğini yeterince açık ifadelerle gösterecek nitelikte olmalı ve bu bağlamda ilgili müdahalenin muhataplarının müdahaleye zemin hazırlayan koşullar ile müdahalenin sonuçları açısından bir öngörüde bulunabilmeleri imkânı tanınmalıdır (Halime Sare Aysal, § 64).

70. Bununla birlikte her ihtimale çözüm getiremeyecek olan yasal mevzuatın sağladığı koruma seviyesi büyük ölçüde ilgili metnin düzenlediği alan ve içeriğiyle birlikte muhataplarının niteliği ve sayısı ile yakından bağlantılıdır. Bu nedenle kuralın karmaşık olması ya da belirli ölçülerde soyutluk içermesi ve buna bağlı olarak hukuki yardım ile tam olarak anlaşılabilir hâle gelmesi tek başına hukuken öngörülebilirlik ilkesine aykırı görülemez. Bu kapsamda hak ya da özgürlüğe müdahale eden kural belirli ölçülerdeki takdir alanını elbette uygulayıcıya bırakabilir. Fakat bu takdir alanının sınırlarının da yeterli açıklıkta belirlenmesi ve kuralın asgari bir kesinlik içermesi zaruridir (Halime Sare Aysal, § 65).

71. Bu kapsamda ilgili kanuni düzenlemenin söz konusu sınırlamaya ilişkin temel çerçeveyi ortaya koymakla birlikte özellikle uygulama koşulları ve usule ilişkin ayrıntıları düzenleyici işlemlere bırakması mümkündür. Ancak bu ihtimalde de söz konusu düzenleyici işlemin yine muhataplarınca

ulařılabilir olması ve içerięi hakkında ilgilileri yeterince aydınlatacak nitelik ve açıklıkta olması gerekmektedir (Halime Sare Aysal, § 66).

(2) İlkelerin Olaya Uygulanması

72. Belirli kamu görevlerinde çalıştırılacak personel hakkında uygulanan güvenlik soruşturması ve arşiv araştırmasının kanuni dayanaęı 4045 sayılı Kanun'dur (bkz. § 30).

73. 4045 sayılı Kanun'da güvenlik soruşturması ve arşiv araştırmasının kamu kurum ve kuruluşlarında yetkili olmayan kişilerin bilgi sahibi olmaları hâlinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceęi veya tehlikeye düşebileceęi bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile askerî teşkilatlarda, emniyet ve istihbarat teşkilatlarında çalıştırılacak kamu personeli, ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında yapılacaęı düzenlenmiştir.

74. Ancak 657 sayılı Kanun'un 48. maddesine 3/10/2016 tarihli ve 29872 sayılı Resmî Gazete'de yayımlanan 676 sayılı Olaęanüstü Hal Kapsamında Bazı Düzenlemeler Yapılması Hakkında Kanun Hükmünde Kararname (KHK) ve bu KHK'nın uygun bulunmasına dair 7070 sayılı Kanun ile devlet memurluęuna alınacaklarda aranan genel şartlar arasına "Güvenlik soruşturması ve/veya arşiv araştırması yapılmıř olmak" şartı eklenmiştir. Dolayısıyla daha önce sadece 4045 sayılı Kanun'da sayılan belirli görevler yönünden güvenlik soruşturması yapılacaęı öngörölmüş iken söz konusu deęişiklik sonrasında artık tüm kamu görevleri yönünden güvenlik soruşturması ve arşiv araştırması yapılmasının öngörüldüęü anlaşılmaktadır.

75. Bununla birlikte eldeki başvuruda başvurucu yönünden müdahale teşkil eden işlemin tesis edildięi tarihte mevcut olan yasal düzenlemelerin esas alınması bir zorunluluk olup Anayasa Mahkemesinin olay tarihinden sonra kabul edilmiş 657 sayılı Kanun'un 48. maddesine getirilen düzenlemeyi somut olayın incelenmesi bakımından dikkate alması mümkün bulunmamaktadır.

76. 4045 sayılı Kanun'da güvenlik soruşturması ve arşiv araştırması konusunda sadece bir maddeye yer verilerek hangi kamu görevleri bakımından güvenlik soruşturması yaptırılacaęı düzenlenmiş, bunun dışındaki tüm düzenlemelerin bir yönetmelikle yapılacaęı belirtilmiştir.

77. Bu doęrultuda Yönetmelik çıkarılmıştır. Söz konusu Yönetmelik'in 4. maddesinde güvenlik soruşturması "kişinin kolluk kuvvetleri tarafından halen aranıp aranmadıęının, kolluk kuvvetleri ve istihbarat ünitelerinde iliřięi ile adli sicil kaydının ve hakkında herhangi bir tahdit olup olmadıęının, yıkıcı ve bölücü faaliyetlerde bulunup bulunmadıęının, ahlaki durumunun, yabancılar ile ilgisinin ve sır saklama yeteneęinin mevcut kayıtlardan ve yerinden araştırılmak suretiyle saptanması ve

değerlendirilmesi" şeklinde tanımlanmıştır. Arşiv araştırması ise kişinin kolluk kuvvetleri tarafından hâlen aranıp aranmadığının, kolluk kuvvetleri ve istihbarat ünitelerinde ilişkisi ile adli sicil kaydının ve hakkında herhangi bir tahdit olup olmadığının mevcut kayıtlardan saptanması olarak belirtilmiştir.

78. Yönetmelik'in 7. maddesi uyarınca güvenlik soruşturması ve arşiv araştırması yapacak makamlar Millî İstihbarat Teşkilatı Müsteşarlığı, Emniyet Genel Müdürlüğü ve mahalli mülki idare amirlikleridir.

79. Yönetmelik'in 11. maddesinde; güvenlik soruşturması ve arşiv araştırmasında kişinin içinde bulunduğu ortam da dikkate alınarak kimlik kontrolü, kimlik kayıtlarının doğruluk derecesi, uyrukluğı, geçmişte yabancı bir devletin uyrukluğuna girip girmediğı, kolluk kuvvetleri tarafından hâlen aranıp aranmadığı, kolluk kuvvetlerinin ve istihbarat ünitelerinin arşivlerinde bilgiler bulunup bulunmadığı, adli sicil kaydının ve hakkında bir tahdidin olup olmadığı, yıkıcı faaliyetlerde bulunup bulunmadığı, 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'a ve Atatürk ilke ve inkılaplarına aykırı davranıp davranmadığı, şeref ve haysiyetini ihlal edecek ve görevine yansiyacak şekilde kumara, uyuşturucuya, içkiye, paraya ve aşırı bir şekilde menfaatine düşkün olup olmadığı, ahlak ve adaba aykırı davranıp davranmadığı, yabancılarla, özellikle hasım ve hasım olması muhtemel devlet mensupları ve temsilcileriyle olan ilgi derecesinin iç yüzü ve nedeni, sır saklama yeteneğinin olup olmadığı hususlarının araştırılacağı belirtilmiştir.

80. Yönetmelik'in 12. maddesinde güvenlik soruşturması ve arşiv araştırmasının nasıl ve ne şekilde yapılacağına soruşturma ve araştırma yapmaya yetkili makamların görev talimatları ile belirleneceğı düzenlenmiştir.

81. Ayrıca anılan maddede soruşturma ve araştırma sonucunu içeren bilgi ve belgelerin ilgilinin güvenlik makamlarındaki dosyasında asgari "gizli" gizlilik derecesinde saklanacağı, güvenlik soruşturması ve arşiv araştırmasında olumsuz durumu saptananlarla ilgili bilgilerin Millî İstihbarat Teşkilatı Müsteşarlığı ve Emniyet Genel Müdürlüğüne karşılıklı olarak birbirlerine aktarılacağı düzenlenmiştir.

82. Anayasa'nın 129. maddesinin birinci fıkrasında memurlar ve kamu görevlilerinin Anayasa ve kanunlara sadık kalarak faaliyette bulunma yükümlülükleri düzenlenmiştir. Ayrıca 657 sayılı Kanun'da bu sadakat yükümlülüğünün yanı sıra kamu görevlilerine tarafsızlık ve devlete bağlılık yükümlülükleri de getirilmiştir.

83. Kamu görevlilerinin sadakat, tarafsızlık ve devlete bağlılık yükümlülüğü çerçevesinde devleti temsil eden ve millî güvenlik bakımından hassasiyet içeren bazı kamu görevlerine atanacak kişiler bakımından daha sıkı nitelikler aranması ve birtakım sınırlamaların getirilmesi doğaldır. Bu şekilde aranan nitelikler ve kanunlarda öngörülen kısıtlamalar, kamu hizmetinin etkin ve sağlıklı bir biçimde yürütülmesi amacıyla yöneliktir. Dolayısıyla idarenin millî güvenlik açısından önem arz eden kadrolara atanacak kişilerin tabi olacağı güvenlik soruşturması ve arşiv araştırması konusunda kanunla temel çerçeveyi ortaya koyan kurallar getirmesi elbette mümkündür. Bu çerçevenin kanunla belirlenmesinden sonra uygulama koşulları ve usule ilişkin ayrıntılar düzenleyici işlemlerle belirlenebilir. Üstelik millî güvenlik ile ilgili alanlarda çalışacak personelin seçimi ve kontrolü bakımından konuyu düzenleyen kanunda aranacak öngörülebilirlik koşulunun diğer alanlardakilere göre daha esnek olacağı da söylenebilir. Ancak yine de bu alanda düzenleme getiren kanun ile diğer alt mevzuatın kişilere, kamu makamlarına hangi koşullarda ve hangi sınırlar içinde bu tür gizli tedbirler uygulama ve potansiyel olarak özel hayatın gizliliğine yönelik müdahalelerde bulunma yetkisi verildiğini yeterince açık olarak gösterecek ve olası kötüye kullanmalara karşı yeterli güvence sağlayacak şekilde kaleme alınmış olması gerekir (Fatih Saraman, § 82).

84. 4045 sayılı Kanun'un güvenlik soruşturmasına ve arşiv araştırmasına konu edilecek bilgi ve belgelerin neler olduğu, bu bilgilerin nerelerden elde edileceği ve ne suretle ve ne kadar süre ile saklanacağı, kişilerin söz konusu bilgilere itiraz etme olanağı olup olmadığı, bilgilerin bir müddet sonra silinmesinin mümkün olup olmadığı veya silinmesine dair izlenecek usulün ne olduğu, gizlilik dereceli kamu personeli ile meslek gruplarının tespiti, güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak mercilerin kimler olduğu ile ilgili hiçbir düzenleme içermediği görülmektedir. Bunun yanı sıra kanunlarda, kesinleşmiş ceza mahkûmiyetlerine dair ilk olarak akla gelmesi ve uygulanması gereken kanun olan 5352 sayılı Kanun'a atıf içeren bir düzenlemenin bulunmadığı, bireyleri keyfiliğe karşı koruyucu hiçbir hükme yer verilmediği anlaşılmaktadır. Aynı şekilde Yönetmelik'te de elde edilen bilgilerin saklanma süreleri, bilgilerin bir müddet sonra silinmesinin mümkün olup olmadığı veya silinmesine dair izlenecek usulün ne olduğu, kişilerin söz konusu bilgilere itiraz etme olanağı olup olmadığı hususlarını düzenlemediği, bireylerin özel hayatına saygı hakkının güvencelerini sağlayacak hükümlerden yoksun olduğu anlaşılmaktadır (Fatih Saraman, § 83).

85. Bunun yanı sıra 4045 sayılı Kanun'da kişilerin geçmiş ceza mahkûmiyetlerine ilişkin kayıtlar bakımından hangi suçların kamu görevine girmeye engel olduğu, kişilerin onsekiz yaşından önce işledikleri suçlara dair kayıtların güvenlik soruşturmasının olumsuz sonuçlanmasına sebep olup

olmayacağı konularında hiç bir belirleme, suçlar arasında herhangi bir ayırım ve derecelendirme yapılmamış olduğu anlaşılmaktadır. Aynı şekilde 4616 sayılı Kanun uyarınca kesinleşmiş mahkûmiyet niteliğinde sayılmayan kamu davasının açılmasının ertelenmesine ve hükmün açıklanmasının geri bırakılmasına ilişkin kararların da güvenlik soruşturmasının olumsuz sonuçlanmasının bir sebebi olup olmayacağı hususunda hiç bir düzenlemeye yer verilmediği görülmektedir (Fatih Saraman, § 87).

86. 4045 sayılı Kanun sadece hangi kamu görevleri bakımından güvenlik soruşturması yaptırılacağını düzenlemiş, bunun dışındaki tüm düzenlemeleri ise bir Yönetmelik'e bırakmıştır. İlgili Yönetmelik hükümlerine bakıldığında Yönetmelik'te güvenlik soruşturması ve arşiv araştırmasının nasıl ve ne şekilde yapılacağı konusunda hiçbir düzenleme içermediği, bu konunun soruşturma ve araştırma yapmaya yetkili makamların görev talimatlarına bırakılmış olduğu görülmektedir. Yetkili makamların görev talimatlarının neler olduğunun -bu talimatların yayımlanarak genelin bilgisine sunulmamış olması ve idare tarafından istenen her durumda değiştirilebileceği dikkate alındığında- bireyler tarafından önceden bilinmesi ve öngörülmesi mümkün değildir (Fatih Saraman, § 88).

87. Üstelik Yönetmelik'te soruşturma ve araştırma sonucunu içeren bilgi ve belgelerin ilgilinin güvenlik makamlarındaki dosyasında süresiz olarak saklanacağı, güvenlik soruşturması ve arşiv araştırmasında olumsuz durumu saptananlarla ilgili bilgilerin Millî İstihbarat Teşkilatı Müsteşarlığı ve Emniyet Genel Müdürlüğüne karşılıklı olarak birbirlerine aktarılacağı hükümlerine yer verilmiş olup kişilerin söz konusu bilgilere itiraz etme olanağı bulunmadığı gibi bilgilerin bir müddet sonra silinmesine de imkân verilmediği görülmektedir. Bu durumda güvenlik soruşturması ve arşiv araştırmasının objektif, öngörülebilir ve önceden belirlenebilir güvencelere ve usullere tabi kılınmış olmadığı, tamamen yetkili makamların talimatlarına bağlı olarak yapıldığı, bu hâliyle de keyfiliğe açık bir durum yaratmakta olduğu anlaşılmaktadır (Fatih Saraman, § 89).

88. Bu saptamalar ışığında 4045 sayılı Kanun'un temel hak ve özgürlüklerin sınırlandırılmasını içeren konuyla ilgili temel esasları, ilkeleri ve çerçeveyi belirlemiş olduğundan söz etmek mümkün değildir. Kanun'un ve ilgili Yönetmelik'in kişisel verilerin kayıt, muhafaza ve kullanımını içeren tedbirlerin kapsamını ve uygulanmasını düzenleyen ve özellikle süre, stoklama, kullanım, üçüncü kişilerin erişimi, verilerin gizliliği, bütünlüğü ve imhası konusundaki usullere ilişkin, muhataplarının yetki aşımı ve keyfiliğe karşı yeteri kadar güvenceye sahip olmalarını sağlayacak açık ve detaylı kuralları içermediği tespit edilmektedir. Buna göre başvuruya konu müdahalenin dayanağı olan düzenlemenin kanunilik şartını sağlamadığı sonucuna varılmaktadır (Fatih Saraman, § 90).

89. Öte yandan 5352 sayılı Kanun'un 6. maddesinde kamu davasının açılmasının ertelenmesine ve hükmün açıklanmasının geri bırakılmasına ilişkin kararların ancak bir soruşturma veya kovuşturmayla bağlantılı olarak mahkeme, hâkim, askerî hâkim, Cumhuriyet başsavcılığı veya askerî savcılık tarafından istenmesi hâlinde verileceği düzenlenmiştir. Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğünün 25/6/2018 tarihli yazısında anılan Kanun hükmü ve ilgili genelgeler uyarınca 4616 sayılı Kanun'a göre verilmiş erteleme kararlarının kamu görevlerine yapılacak atamalar dolayısıyla güvenlik soruşturması kapsamında ilgili kamu kurumlarına verilemeyeceği ifade edilmiştir. Buna göre Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü uygulamasının da bu yönde olduğu anlaşılmaktadır (bkz. §§ 37-39).

90. Buna göre somut olayda başvurucunun yazılı ve sözlü sınavı kazandığının ilan edilmiş olduğu, 4616 sayılı Kanun'a göre verilmiş ve daha sonra 2/4/2007 tarihli yargı kararı ile ortadan kaldırılmış olan erteleme kararının 5352 sayılı Kanun'un 6. maddesinin birincifıkrasında yer alan hükme açıkça aykırı şekilde idari makamlara verilmiş olduğu dikkate alındığında özel hayata saygı hakkına yönelik müdahalenin bu yönüyle de kanuni dayanaktan yoksun olduğu anlaşılmaktadır.

91. Yukarıda yer verilen tespitler uyarınca başvuruya konu müdahalenin Anayasa'da yer alan kanunilik şartına uygun olmadığı anlaşıldığından söz konusu müdahale açısından diğer güvence ölçütlerine riayet edilip edilmediğinin ayrıca değerlendirilmesine gerek görülmemiştir.

92. Açıklanan gerekçelerle başvurucunun Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkının ihlal edildiğine karar verilmesi gerekir.

B. Masumiyet Karinesinin İhlal Edildiğine İlişkin İddia

1. Başvurucunun İddiaları ve Bakanlık Görüşü

93. Başvurucu, idare mahkemesinin kararında "...davanın kesin hükme bağlanmasının ertelenmesine karar verildiği, bu kararın davacının üzerine atılı suçu işlemediği anlamına gelmeyeceği, davacının üzerine atılı suçu işlemediği yönünde verilmiş bir beraat kararı da bulunmadığı,..." gerekçesine yer verildiğini, karardaki bu ifadelerin masumiyet karinesinin ihlali niteliğinde olduğunu, sanki suçluymuş gibi bir algı oluşturduğunu ileri sürmüştür.

94. Bakanlık görüşünde masumiyet karinesi yönünden başvurucuya bir suç isnad edilmediğinin değerlendirildiği bildirilmiştir.

95. Bakanlık görüşüne karşı verilen cevapta, başvuru dilekçesinde yer alan hususlar tekrar edilmiştir.

2. Değerlendirme

96. Anayasa'nın "Hak arama hürriyeti" kenar başlıklı 36. maddesinin birinci fıkrası şöyledir:

"Herkes, meşru vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahiptir."

97. Anayasa'nın 38. maddesinin dördüncü fıkrası şöyledir:

"Suçluluğu hükmen sabit oluncaya kadar, kimse suçlu sayılamaz."

98. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Somut olayda başvuru sahibinin şikâyetlerinin masumiyet karinesi yönünden incelenmesi gerektiği değerlendirilmiştir.

a. Kabul Edilebilirlik Yönünden

99. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan masumiyet karinesinin ihlal edildiğine ilişkin başvurunun kabul edilebilir olduğuna karar verilmesi gerekir.

b. Esas Yönünden

i. Genel İlkeler

100. Masumiyet karinesi, Anayasa'nın 38. maddesinin dördüncü fıkrasında "Suçluluğu hükmen sabit oluncaya kadar, kimse suçlu sayılamaz." şeklinde düzenlenmiştir. Anayasa'nın 36. maddesinde ise herkesin iddia ve savunma ile adil yargılanma hakkına sahip olduğu belirtilmektedir. Anılan maddeye adil yargılanma ibaresinin eklenmesine ilişkin gerekçede, Türkiye'nin taraf olduğu uluslararası sözleşmelerde de güvence altına alınan adil yargılama hakkının madde metnine dâhil edildiği vurgulanmıştır. Nitekim Sözleşme'nin 6. maddesinin (2) numaralı fıkrasında, kendisine bir suç isnat edilen herkesin suçluluğu yasal olarak sabit oluncaya kadar suçsuz sayılacağı düzenlenmiştir. Bu itibarla masumiyet karinesi, Anayasa'nın 36. maddesinde güvence altına alınan adil yargılanma hakkının bir unsuru olmakla beraber suçluluğu hükmen sabit oluncaya kadar kimsenin suçlu sayılmayacağına dair 38. maddesinin dördüncü fıkrasında ayrıca düzenlenmiştir (Fameka İnş. Plastik San ve Tic. Ltd. Şirketi, B. No: 2014/3905, 19/04/2017, § 27).

101. Masumiyet karinesi, hakkında suç isnadı bulunan bir kişinin adil bir yargılama sonunda suçlu olduğuna dair kesin hüküm tesis edilene kadar masum sayılması gerektiğini ifade etmekte ve hukuk devleti ilkesinin de bir gereğini oluşturmaktadır (AYM, E.2013/133, K.2013/169, 26/12/2013). Anılan karene, kişinin suç işlediğine dair kesinleşmiş bir yargı kararı olmadan suçlu olarak kabul

edilmemesini güvence altına almaktadır. Ayrıca hiç kimse suçluluğu hükmen sabit oluncaya kadar yargılama makamları ve kamu otoriteleri tarafından suçlu olarak nitelendirilemez ve suçlu muamelesine tabi tutulamaz (Kürşat Eyol, B. No: 2012/665, 13/6/2013, § 26).

102. Adil yargılanma hakkının bir unsuru olan masumiyet karinesinin sağladığı güvencenin iki yönü bulunmaktadır.

103. Güvencenin ilk yönü; kişi hakkındaki ceza yargılaması sonuçlanıncaya kadar geçen, bir başka ifadeyle kişinin ceza gerektiren bir suçla itham edildiği (suç isnadı altında olduğu) sürece ilişkin olup suçlu olduğuna dair hüküm tesis edilene kadar kişinin suçluluğu ve eylemleri hakkında erken açıklamalarda bulunulmasını yasaklar. Güvencenin bu yönünün kapsamı sadece ceza yargılamasını yürüten mahkemeye sınırlı değildir. Güvence aynı zamanda diğer tüm idari ve adli makamların da işlem ve kararlarında, suçluluğu hükmen sabit oluncaya kadar kişinin suçlu olduğu yönünde ima ya da açıklamalarda bulunmamasını gerekli kılar. Dolayısıyla sadece suç isnadına konu ceza yargılaması kapsamında değil ceza yargılaması ile eş zamanlı olarak yürütülen diğer hukuki süreç ve yargılamalarda da (idari, hukuk, disiplin gibi) masumiyet karinesinin ihlali söz konusu olabilir (Galip Şahin, B. No: 2015/6075, 11/6/2018, § 39).

104. Güvencenin ikinci yönü ise ceza yargılaması sonucunda mahkûmiyet dışında bir hüküm kurulduğunda devreye girer ve daha sonraki yargılamalarda ceza gerektiren suçla ilgili olarak kişinin masumiyetinden şüphe duyulmamasını, kamu makamlarının toplum nezdinde kişinin suçlu olduğu izlenimini uyandıracak işlem ve uygulamalardan kaçınmasını gerektirir (Galip Şahin, § 40).

105. Ceza muhakemesiyle eş zamanlı olarak yürütülen, bir başka ifadeyle kişinin henüz suç isnadı altında olduğu, ceza makamları tarafından hakkında herhangi bir hüküm kurulmadığı süreçte devam eden disiplin soruşturma ve yargılamalarında masumiyet karinesi bakımından önemli olan husus; kamu makamlarının işlem ya da kararlarında belirttikleri gerekçeler veya kullandıkları dil nedeniyle bireye cezai sorumluluk yüklememeleri, ceza mahkemeleri tarafından henüz suçlu bulunmamış bireyin masumiyeti üzerine gölge düşürülmesine sebebiyet vermemeleridir (Galip Şahin, § 47).

106. Bununla birlikte ceza yargılamasına konu maddi olay ve olguların disiplin hukuku esasları çerçevesinde diğer kamu makamlarınca (idari/adli) ayrıca değerlendirilmesi ve bu değerlendirme sonucunda ulaşılabilecek kanaate göre işlem/karar tesis edilmesi mümkündür. Bu bağlamda disiplin işlem ve yargılamalarında ceza yargılamasında elde edilen bir delile dayanılması ya da kişi hakkında yapılan ceza yargılamasına bir olgu olarak atıf yapılmış olması tek başına masumiyet karinesinin sağladığı güvencelere aykırılık teşkil etmez. Ancak adli ve idari makamların kendi görev sınırlarını aşarak kişiyi suçlu ilan etmesi veya bu bağlamda birtakım çıkarımlarda bulunması masumiyet

karinesinin ihlaline yol açabilir. Masumiyet karinesi kapsamındaki güvencelerin sağlanıp sağlanmadığının tespiti yapılırken ise kararın gerekçesinin bir bütün olarak değerlendirilmesi gerekir (Galip Şahin, § 48).

107. Masumiyet karinesinin ihlal edilip edilmediği değerlendirilirken özellikle hukuk ve idari yargılama bakımından üzerinde durulması gereken önemli hususlardan biri, yargılamayı yapan makamın ilgili kişiye suç isnat edip etmediği ve ceza yargılaması kararını sorgulayıp sorgulamadığıdır. Kamu otoriteleri veya görevlileri tarafından hakkında soruşturma veya kovuşturma yürütülen kişiyle ilgili olarak yargılama süreci bir mahkûmiyet hükmüyle kesinlik kazanmadan suçluluğa dair herhangi bir kanaat ifade edilmiş olması ya da ceza yargılaması mahkûmiyet dışında bir kararla sona ermesine rağmen sona ermeye ilişkin kararda sanığın suçlu olabileceğinin ifade edilmiş olması durumunda masumiyet karinesinin ihlali söz konusu olabilecektir. Bu kapsamda karar vericilerin kullandıkları dil kritik önem taşır (Mustafa Akın, B. No: 2013/2696, 9/9/2015, §§ 38, 39).

108. Anayasa Mahkemesi, Münür İcer (B. No: 2012/584, 12/3/2015, §§ 31- 33) kararında, başvuruya konu idari yargı mercii kararının gerekçesinde yer alan ifadelerde, suçluluğu ilgili mahkeme kararıyla sabit olmayan ve zamanaşımı nedeniyle hakkında açılan ceza davası ortadan kaldırılan başvurucunun anılan eylemleri işlediği ve suçlu olduğu inancının yansıtıldığı gerekçesiyle başvurucunun masumiyet karinesinin ihlal edildiğine karar vermiştir. Dolayısıyla mahkeme kararlarında, resmî yazılarda veya kamu görevlilerinin ifadelerinde sarf edilen söz veya ifadeler nedeniyle kişiler hakkındaki masumiyet karinesinin ihlal edilmemesi için kullanılan ifadelerde seçilecek kelimelere azami dikkat edilmesi gerekir (Ömer Aybar, B. No: 2013/6974, 14/4/2016, § 30).

ii. İlkelerin Olaya Uygulanması

109. Somut olayda başvuru hakkındaki ceza yargılaması sonucunda 4616 sayılı Kanun'un 1. maddesinin birinci fıkrasının dördüncü bendi gereğince davanın kesin hükme bağlanmasının ertelenmesine hükmedilmiş ve daha sonra başvurucunun beş yıllık deneme süresi içinde başka suç işlemediği gerekçesiyle kamu davasının ortadan kaldırılmasına karar verilmiştir.

110. Başvurucunun sözleşmeli ceza infaz kurumu şoförlüğüne atamasının yapılmaması işlemine karşı açılan davada İdare Mahkemesi kamu görevine atamama işleminin hukuka uygun olduğu sonucuna ulaşırken başvurucunun durumunu ceza yargılamasında verilen kararı esas almıştır.

111. İdare Mahkemesi kararının gerekçesinde "...davanın kesin hükme bağlanmasının ertelenmesine karar verildiği, bu kararın davacının üzerine atılı suçu işlemediği anlamına gelmeyeceği, davacının

üzerine atılı suçu işlemediği yönünde verilmiş bir beraat kararı da bulunmadığı,...” ifadeleri yer almaktadır. Söz konusu ifadelerle başvuru konusuna konu suçu işlediği izlenimi verilmiştir. Bu çerçevede başvuruya konu kararın gerekçesinde yer alan söz konusu ifadeyle suçluluğu ilgili Mahkeme kararıyla sabit olmayan ve 4616 sayılı Kanun uyarınca hakkında açılan ceza davası ortadan kaldırılan başvuru konusuna konu suçu işlemediği yönünde inancının yansıtıldığı görülmektedir. Üstelik İdare Mahkemesi kararında daha sonra yargı kararıyla kamu davasının ortadan kaldırılmasına hükmedilmiş olması hususuna da yer verilmemiştir. Karardaki özellikle “davacının üzerine atılı suçu işlemediği anlamına gelmeyeceği, davacının üzerine atılı suçu işlemediği yönünde verilmiş bir beraat kararı da bulunmadığı” ifadelerinin masumiyet karinesi ile bağdaştırılması söylenemez.

112. Yukarıdaki açıklamalar çerçevesinde İdare Mahkemesince hakkında herhangi bir mahkûmiyet kararı bulunmayan başvuru konusuna konu eylemleri işlediğinin sabit olduğu varsayımına dayanılarak karar verildiği anlaşıldığından başvuru konusuna Anayasa'nın 36. ve 38. maddelerinde güvence altına alınan masumiyet karinesinin ihlal edildiğine karar verilmesi gerekir.

C. 6216 Sayılı Kanun'un 50. Maddesi Yönünden

113. 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 50. maddesinin (1) ve (2) numaralı fıkraları şöyledir:

“(1) Esas inceleme sonunda, başvuru konusunun hakkının ihlal edildiğine ya da edilmediğine karar verilir. İhlal kararı verilmesi hâlinde ihlalin ve sonuçlarının ortadan kaldırılması için yapılması gerekenlere hükmedilir. ...

(2) Tespit edilen ihlal bir mahkeme kararından kaynaklanmışsa, ihlali ve sonuçlarını ortadan kaldırmak için yeniden yargılama yapmak üzere dosya ilgili mahkemeye gönderilir. Yeniden yargılama yapılmasında hukuki yarar bulunmayan hâllerde başvuru konusuna lehine tazminata hükmedilebilir veya genel mahkemelerde dava açılması yolu gösterilebilir. Yeniden yargılama yapmakla yükümlü mahkeme, Anayasa Mahkemesinin ihlal kararında açıkladığı ihlali ve sonuçlarını ortadan kaldıracak şekilde mümkünse dosya üzerinden karar verir.”

114. Anayasa Mahkemesinin Mehmet Doğan ([GK], B. No: 2014/8875, 7/6/2018) kararında, Anayasa Mahkemesince bir temel hakkın ihlal edildiği sonucuna varıldığında ihlalin ve sonuçlarının nasıl ortadan kaldırılacağına belirlenmesi hususunda genel ilkelere yer verilmiştir (Mehmet Doğan, §§ 57-60).

115. İhlalin ve sonuçlarının ortadan kaldırılması için yapılması gerekenlere hükmedilmeden önce ihlalin kaynağının belirlenmesi gerekir. Buna göre ihlal; idari eylem ve işlemler, yargısal işlemler veya

yasama işlemlerinden kaynaklanabilir. İhlalin kaynağının belirlenmesi uygun giderim yolunun belirlenebilmesi bakımından önem taşımaktadır (Mehmet Doğan, § 57).

116. İhlalin mahkeme kararından kaynaklandığı durumlarda 6216 sayılı Kanun'un 50. maddesinin (2) numaralı fıkrası ile Anayasa Mahkemesi İçtüzüğü'nün 79. maddesinin (1) numaralı fıkrasının (a) bendi uyarınca kural olarak ihlali ve sonuçlarını ortadan kaldırmak için yeniden yargılama yapılmak üzere kararın bir örneğinin ilgili mahkemeye gönderilmesine hükmedilir (Mehmet Doğan, § 58).

117. Buna göre Anayasa Mahkemesince ihlalin tespit edildiği hâllerde yargılamanın yenilenmesinin gerekliliği hususundaki takdir derece mahkemelerine değil ihlalin varlığını tespit eden Anayasa Mahkemesine bırakılmıştır. Derece mahkemeleri ise Anayasa Mahkemesinin ihlal kararında belirttiği doğrultuda ihlalin sonuçlarını gidermek üzere gereken işlemleri yapmakla yükümlüdür (Mehmet Doğan, § 59).

118. Başvurucu ihlalin tespiti ile 900.000 TL maddi, 300.000 TL manevi tazminat talebinde bulunmuştur.

119. Mevcut başvuruda ceza yargılamasına dair bilgilerin idari makamlara açıklanması şeklindeki müdahalenin dayanağı olan 4045 sayılı Kanun'un Anayasa'da yer alan kanunilik güvencesine uygun olmaması nedeniyle Anayasa'nın 20. maddesinde düzenlenen özel hayata saygı hakkının ihlal edildiği sonucuna varılmıştır. Ayrıca İdare Mahkemesi kararında kullanılan ifadelerin masumiyet karinesini ihlal ettiği sonucuna varmıştır. Dolayısıyla somut başvuruda ihlalin mahkeme kararından kaynaklandığı anlaşılmaktadır.

120. Bu durumda özel hayata saygı hakkının ve masumiyet karinesinin ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmasında hukuki yarar bulunmaktadır. Buna göre yapılacak yeniden yargılama ise 6216 sayılı Kanun'un 50. maddesinin (2) numaralı fıkrasına göre ihlalin ve sonuçlarının ortadan kaldırılmasına yöneliktir. Bu kapsamda derece mahkemelerince yapılması gereken iş, öncelikle ihlale yol açan mahkeme kararının ortadan kaldırılması ve nihayet ihlal sonucuna uygun yeni bir karar verilmesinden ibarettir. Bu sebeple kararın bir örneğinin yeniden yargılama yapılmak üzere Hatay İdare Mahkemesine gönderilmesine karar verilmesi gerekir (Fatih Saraman, § 101).

121. Yeniden yargılama yapılmak üzere dosyanın yetkili yargı merciine gönderilmesine karar verilmesinin ihlal iddiası açısından yeterli bir giderim oluşturduğu anlaşıldığından başvurucunun tazminat taleplerinin reddine karar verilmesi gerekir.

122. Dosyadaki belgelerden tespit edilen 206,10 TL harç ve 2.475 TL vekâlet ücretinden oluşan toplam 2.681,10 TL yargılama giderinin başvurucuya ödenmesine karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. 1. Özel hayata saygı hakkının ihlal edildiğine ilişkin iddianın KABUL EDİLEBİLİR OLDUĞUNA,

2. Masumiyet karinesi ilkesinin ihlal edildiğine ilişkin iddianın KABUL EDİLEBİLİR OLDUĞUNA,

B. 1. Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkının İHLAL EDİLDİĞİNE,

2. Anayasa'nın 36. ve 38. maddesinin dördüncü fıkrasında hüküm altına alınan masumiyet karinesinin İHLAL EDİLDİĞİNE,

C. Kararın bir örneğinin özel hayata saygı hakkının ve masumiyet karinesinin ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmak üzere Hatay İdare Mahkemesine (7/3/2013 tarihli ve E.2012/1285, K.2013/429 sayılı kararlar ile ilgilidir.) GÖNDERİLMESİNE,

D. Başvurucunun tazminat taleplerinin REDDİNE,

E. 206,10 TL harç ve 2.475 TL vekâlet ücretinden oluşan toplam 2.681,10 TL yargılama giderinin BAŞVUCUYA ÖDENMESİNE,

F. Ödemelerin, kararın tebliğini takiben başvurucunun Hazine ve Maliye Bakanlığına başvuru tarihinden itibaren dört ay içinde yapılmasına, ödemede gecikme olması hâlinde bu sürenin sona erdiği tarihten ödeme tarihine kadar geçen süre için yasal FAİZ UYGULANMASINA,

G. Kararın bir örneğinin Adalet Bakanlığına GÖNDERİLMESİNE 29/5/2019 tarihinde OYBİRLİĞİYLE karar verildi.

Anayasa Mahkemesi - B.K. Kararı (2014/14189)

B.K., B. No: 2014/14189, 25/10/2017

Başvuru, hatalı tedavi uygulanması nedeniyle maddi ve manevi varlığın korunması ve geliştirilmesi hakkının; operasyonu gerçekleştiren doktor aleyhine açılan tazminat davasında duruşmaların gizli yapılması yönündeki talebin reddi nedeniyle özel hayatın gizliliği hakkının ve davanın makul sürede sonuçlandırılmaması nedenleriyle adil yargılanma hakkının ihlal edildiği iddialarına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

BİRİNCİ BÖLÜM

KARAR

B. K. BAŞVURUSU

(Başvuru Numarası: 2014/14189)

Karar Tarihi: 25/10/2017

R.G. Tarih ve Sayı: 16/11/2017-30242

BİRİNCİ BÖLÜM

KARAR

GİZLİLİK TALEBİ KABUL

Başkan: Burhan ÜSTÜN

Üyeler: Serruh KALELİ, Hicabi DURSUN, Hasan Tahsin GÖKCAN, Rıdvan GÜLEÇ

Raportör: Şermin BİRTANE

Başvurucu: B. K.

Vekili: Av. Hilal ÇALKIN

I. BAŞVURUNUN KONUSU

1. Başvuru, hatalı tedavi uygulanması nedeniyle maddi ve manevi varlığın korunması ve geliştirilmesi hakkının; operasyonu gerçekleştiren doktor aleyhine açılan tazminat davasında

duruşmaların gizli yapılması yönündeki talebin reddi nedeniyle özel hayatın gizliliği hakkının ve davanın makul sürede sonuçlandırılmaması nedenleriyle adil yargılanma hakkının ihlal edildiği iddialarına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 27/8/2014 tarihinde yapılmıştır.

3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.

4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.

5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.

6. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık görüş sunmamıştır.

III. OLAY VE OLGULAR

7. Başvuru formu ve eklerinde ifade edildiği şekliyle olaylar özetle şöyledir:

8. Başvurucu 17/4/2009 tarihinde meme küçültme operasyonu geçirmiştir.

9. Başvurucu; bu operasyon neticesinde sağ memesini ve meme ucunu yitirdiğini, sol memesinin biçimsiz hâl aldığını, bu durumun oluşmasında operasyonu gerçekleştiren doktorun kusurunun bulunduğunu ileri sürerek ilgili doktor hakkında İzmir Cumhuriyet Başsavcılığına suç duyurusunda bulunmuştur.

A. Ceza Davasına İlişkin Süreç

10. Doktor hakkında İzmir 7. Sulh Ceza Mahkemesinde kamu davası açılmıştır. Mahkemece Adli Tıp Kurumundan bilirkişi raporu alınmıştır. Adli Tıp Kurumu 3. Adli Tıp İhtisas Kurulunun 1/8/2012 tarihli raporunda; başvurusunun ameliyat nedeniyle hayati tehlike geçirmediği, yaralanmanın basit tıbbi müdahale ile giderilemeyeceği, uzuv zaafı veya uzuv tatalinin söz konusu olmadığı belirtilmiştir. Raporda ayrıca ameliyat sonrası gelişen kısmi doku nekrozu ve yara açılmasının bu tür plastik cerrahi ameliyatlarında komplikasyon olarak kabul edilebileceği, kişinin mevcut durumunun daha iyi hâle getirilebilmesi için rekonstrüktif müdahalelerin gerektiği, ameliyat sırasında tıbbi uygulama hatasına dair deliller olmasa da meydana gelen sonucun kabul edilebilir olmadığı ifade edilmiştir.

11. İzmir 7. Sulh Ceza Mahkemesinin 14/1/2013 tarihli kararıyla sanık doktorun beraatine hükmedilmiştir.
12. Başvurucunun temyizi üzerine karar; Yargıtay 12. Ceza Dairesinin 29/5/2014 tarihli ilamıyla, sanığın tıbbi açıdan kusurlu olup olmadığı, meydana gelen sonuç ile tıbbi müdahale arasında illiyet bağı bulunup bulunmadığının kuşkuya yer vermeyecek şekilde saptanması için Yüksek Sağlık Şurasından rapor alınması gerektiği gerekçesiyle bozulmuştur.
13. Bireysel başvuru dilekçesinde dosyanın temyiz incelemesi nedeniyle Yargıtayda derdest durumda olduğu ifade edilmişse de Yargıtayın bozma kararı üzerine dosyanın yerel mahkemeye gönderildiği anlaşılmıştır. Dosya, İzmir 7. Sulh Ceza Mahkemesinin kapatılmış olması nedeniyle İzmir 28. Asliye Ceza Mahkemesinin 2014/372 sayılı esasına kaydedilmiştir.
14. Mahkeme tarafından Sağlık Bakanlığı Yüksek Sağlık Şura Başkanlığından bilirkişi raporu alınmıştır. Yüksek Sağlık Şura Başkanlığının 17/4/2015 tarihli raporunda, estetik olarak uygulanan meme küçültme ameliyatında meydana gelen deformasyonun komplikasyon olduğu ve komplikasyon yönetiminin yerinde olduğu belirtilmiştir. Raporda; tıp terminolojisi yönünden, komplikasyonun hastanın ya da doktorun elinde olmadan gelişen, istenmeyen, öngörülebilir fakat önlenemeyen gelişmeler anlamına geldiği, dolayısıyla hekimin eylemi ile meydana gelen olay arasında illiyet bağı kurulamayacağından ameliyatı gerçekleştiren doktora tıbbi kusur atfedilemeyeceği ifade edilmiştir. Bununla birlikte raporda, hasta dosyasında operasyon öncesinde hastanın bilgilendirilmesine dair onam belgesinin bulunmamasının önemli bir eksiklik olduğu bildirilmiştir.
15. İzmir 28. Asliye Ceza Mahkemesinin 13/7/2015 tarihli kararıyla, meydana gelen deformasyonun tıbbi komplikasyondan kaynaklandığı, hekime tıbbi kusur atfedilemeyeceği gerekçesiyle sanığın beraatine karar verilmiştir.
16. Anılan karar, Yargıtay 12. Ceza Dairesinin 31/1/2017 tarihli kararıyla bozulmuştur. Yargıtay bozma ilamında, ameliyatı yapan doktor sanığın başvurusunun ikinci kez meme ameliyatı olacağını bilmesine rağmen önceki ameliyata dair belgeleri getirtmediği ve ameliyatın riskleri hakkında başvurucağı bilgilendirmediği, bu nedenle kusurlu olduğu, 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 252. maddesinin ikinci fıkrası uyarınca mahkûmiyetine karar verilmesi gerekirken beraatine karar verilmesinin kanuna aykırı olduğu gerekçesine yer verilmiştir.
17. Bozma kararı üzerine dosya, İzmir 28. Asliye Ceza Mahkemesinin 2017/236 sayılı esasına kaydedilmiş olup yerel mahkeme aşamasında derdest durumdadır.

B. Tazminat Davasına İlişkin Süreç

18. Başvurucu aynı zamanda maddi ve manevi zararlarının giderilmesi için söz konusu doktor aleyhine 19/7/2010 tarihinde İzmir 4. Asliye Hukuk Mahkemesinde tazminat davası açmıştır. Dava dilekçesinde özel hayata saygı hakkının ihlalini teşkil edebilecek fotoğraflar gibi bilgi ve belgeler hakkında gizlilik kararı verilmesi talep edilmiştir.

19. İzmir 4. Asliye Hukuk Mahkemesinin 2010/347 Esas sayısına kaydedilen dosyanın 26/10/2010 tarihli tensip duruşmasında başvurusunun "gizlilik talebi ile ilgili karar verilmesine yer olmadığına" karar verilmiştir.

20. İzmir 4. Asliye Hukuk Mahkemesinin 26/4/2012 tarihli duruşmasında, İzmir 7. Sulh Ceza Mahkemesinde görülmekte olan ceza davası sonucunda verilecek kararın beklenmesine karar verilmiştir. Mahkemenin 10/9/2012 tarihli duruşmasında ise belirtilen ceza davası sonucunda verilecek kararın kesinleşmesinin beklenmesine; 12/1/2011 tarihli ve 6100 sayılı Hukuk Muhakemeleri Kanun'unun 165. maddesi uyarınca, söz konusu karar kesinleşinceye kadar dosyanın askıya alınmasına karar verilmiştir. Dosya yerel mahkeme aşamasında derdest durumdadır.

21. Başvurucu 27/8/2014 tarihinde bireysel başvuruda bulunmuştur.

IV. İLGİLİ HUKUK

A. İlgili Mevzuat

22. 6100 sayılı Kanun'un "Aleniyet ilkesi" kenar başlıklı 28. maddesi şöyledir:

“(1) Duruşma ve kararların bildirilmesi alenidir.

(2) Duruşmaların bir kısmının veya tamamının gizli olarak yapılmasına ancak genel ahlâkın veya kamu güvenliğinin kesin olarak gerekli kıldığı hâllerde, taraflardan birinin talebi üzerine yahut resen mahkemece karar verilebilir.

(3) Tarafların gizlilik talebi ön sorunlar hakkındaki hükümler çerçevesinde gizli duruşmada incelenir ve karara bağlanır. Hâkim, bu kararının gerekçelerini, esas hakkındaki kararı ile birlikte açıklar.

(4) Hâkim, gizli yargılama işlemleri sırasında hazır bulunanları o yargılamayla ilgili edindikleri bilgileri açıklamamaları hususunda uyarır ve 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun gizliliğin ihlaline ilişkin hükmünün uygulanacağını ihtar ederek bu hususu tutanağa geçirir.”

23. 6100 sayılı Kanun'un 28. maddesinin gerekçesinin ilgili kısmı şöyledir:

“...

Bazı hâllerde, temel haklardan olan “yargılamanın alenî yapılması” ilkesinin Anayasamız ve Avrupa İnsan Hakları sözleşmesinin yukarıda açıklanan ölçüleri içinde sınırlandırılması zorunlu olmaktadır. Maddenin ikinci fıkrasında, bu hâller, mümkün olduğu kadar somutlaştırılmaya çalışılmıştır.

Üçüncü fıkrada, gizlilik kararının verilebilmesi için araştırmanın da gizli duruşmada yapılacağı ve gizlilik kararı gerekçesinin hemen değil de esas hakkındaki kararlar birlikte açıklanması uygun bulunmuştur. Zira yargılamanın her noktasında karara ulaşmak için bir araştırma yapılması, tarafların diyeceklerinin sorulması, bu konuda delillerin toplanıp incelenmesi zorunludur. Bu zorunluluğu yerine getirirken dahi gizliliğin amacını yok edecek açıklamaların alenen yapılması uygun olmayabilir. Doğaldır ki Anayasamızın 141 inci maddesinin üçüncü fıkrasında ifade olunduğu üzere, gizlilik kararının da gerekçesi gösterilmelidir. Yine gizliliğin amacını korumak için bu gerekçenin açıklanmasının da davanın sonuna tehir edilmesi uygun bulunmuştur.

...”

24. 6100 sayılı Kanun’un “Ön sorunun ileri sürülmesi” kenar başlıklı 163. maddesi şöyledir:

“Yargılama sırasında, davaya ilişkin bir ön sorun ortaya çıkarsa, ilgili taraf, bunu dilekçe vermek suretiyle yahut duruşma sırasında sözlü olarak ileri sürebilir.”

25. 6100 sayılı Kanun’un “Ön sorunun incelenmesi” kenar başlıklı 164. maddesi şöyledir:

“(1) Hâkim, taraflardan birinin ileri sürdüğü ön sorunu incelemeye değer bulursa, belirleyeceği süre içinde, varsa delilleriyle birlikte cevabını bildirmesi için diğer tarafa tefhim veya tebliğ eder.

(2) Ön sorun hakkında iki taraf arasında uyuşmazlık varsa, hâkim gerekirse tarafları davet edip dinledikten sonra kararını verir.

(3) Hâkim, ön sorun hakkındaki kararını taraflara tefhim veya tebliğ eder.”

26. 6100 sayılı Kanun’un 158. maddesi şöyledir:

“(1) Tutanakların tamamı veya bir kısmının örnekleri, talep hâlinde taraflara veya fer’î müdahile verilir. ...

(2) Tutanağın eki niteliğinde bulunan ve gizlilik kararı kapsamında kalan belgelerin örneği ancak hâkimin izni ile verilebilir.”

27. 6100 sayılı Kanun’un “Dosyanın taraflar ve ilgililerce incelenmesi” kenar başlıklı 161. maddesi şöyledir:

“(1) Zabıt kâtibinin gözetimi altında taraflar veya fer’î müdahil, dava dosyasını inceleyebilir. Dava ile ilgili olanlar da bunu ispatlamak kaydı ve hâkimin izniyle dosyayı inceleyebilir.

(2) Gizli olarak saklanmasına karar verilen belge ve tutanakların incelenebilmesi hâkimin açık iznine bağlıdır.”

28. 6100 sayılı Kanun’un "Kayıt ve yayın yasağı" kenar başlıklı 153. maddesi şöyledir:

“(1) Duruşma sırasında fotoğraf çekilemez ve hiçbir şekilde ses ve görüntü kaydı yapılamaz. Ancak, dava dosyasında saklı kalmak kaydıyla, yargılamanın zorunlu kıldığı hâllerde, mahkemece çekim yapılabilir ve kayıt alınabilir. Bu şekilde yapılan çekim ve kayıtlar ile kişilik haklarını ilgilendiren konuları içeren dava dosyası içindeki her türlü belge ve tutanak, mahkemenin ve ilgili kişilerin açık izni olmadıkça hiçbir yerde yayımlanamaz.

(2) Duruşma sırasında bu yasağa aykırı davranan kişi hakkında 151 inci madde hükmü uygulanır.

(3) Kayıt ve yayın yasağına aykırı davranan kişi hakkında, ayrıca Türk Ceza Kanununun 286 ncı maddesi hükümleri uygulanır.”

29. 6100 sayılı Kanun’un "Devletin sorumluluğu ve rücu" kenar başlıklı 46. maddesi şöyledir:

“(1) Hâkimlerin yargılama faaliyetinden dolayı aşağıdaki sebeplere dayanılarak Devlet aleyhine tazminat davası açılabilir:

a) Kayırma veya taraf tutma yahut taraflardan birine olan kin veya düşmanlık sebebiyle hukuka aykırı bir hüküm veya karar verilmiş olması.

b) Sağlanan veya vaat edilen bir menfaat sebebiyle kanuna aykırı bir hüküm veya karar verilmiş olması.

c) Farklı bir anlam yüklenemeyecek kadar açık ve kesin bir kanun hükmüne aykırı karar veya hüküm verilmiş olması.

ç) Duruşma tutanağında mevcut olmayan bir sebebe dayanılarak hüküm verilmiş olması.

d) Duruşma tutanakları ile hüküm veya kararların değiştirilmiş yahut tahrif edilmiş veya söylenmeyen bir sözün hüküm ya da karara etkili olacak şekilde söylenmiş gibi gösterilmiş ve buna dayanılarak hüküm verilmiş olması.

e) Hakkın yerine getirilmesinden kaçınılmış olması.

(2) Tazminat davasının açılması, hâkime karşı bir ceza soruşturmasının yapılması yahut mahkûmiyet şartına bağlanamaz.

(3) Devlet, ödediği tazminat nedeniyle, sorumlu hâkime ödeme tarihinden itibaren bir yıl içinde rücu eder.”

30. 6100 sayılı Kanun’un "Davaların açılacağı mahkeme" kenar başlıklı 47. maddesi şöyledir:

“Devlet aleyhine açılan tazminat davası, ilk derece ve bölge adliye mahkemesi hâkimlerinin fiil ve kararlarından dolayı, Yargıtay ilgili hukuk dairesinde; Yargıtay Başkan ve üyeleri ile kanunen onlarla aynı konumda olanların fiil ve kararlarından dolayı Yargıtay Dördüncü Hukuk Dairesinde ilk derece mahkemesi sıfatıyla görülür.

Dava, bu dairenin Başkan ve üyelerinin fiil ve kararlarından dolayı ise yargılama Yargıtay Üçüncü Hukuk Dairesinde yapılır. Verilen kararların temyiz incelemesi Hukuk Genel Kurulunca yapılır. Temyiz incelemesine, kararı veren başkan ile üyeler katılamaz.

(2) Devletin sorumlu hâkime karşı açacağı rücu davası, tazminat davasını karara bağlamış olan mahkemede görülür.”

31. 6100 sayılı Kanun’un "Dava dilekçesi ve davanın ihbarı" kenar başlıklı 48. maddesi şöyledir:

“(1) Tazminat davası dilekçesinde hangi sorumluluk sebebine dayanıldığı ve delilleri açıkça belirtilir; varsa belgeler de eklenir.

(2) Mahkeme, açılan tazminat davasını, ilgili hâkime resen ihbar eder.”

32. 6100 sayılı Kanun’un "Davanın reddi hâlinde verilecek ceza" kenar başlıklı 49. maddesi şöyledir:

"Dava esastan reddedilirse davacı, beşyüz Türk Lirasından beşbin Türk Lirasına kadar disiplin para cezasına mahkûm edilir.”

33. 6100 sayılı Kanun’un "Bekletici sorun" kenar başlıklı 165. maddesinin birinci fıkrası şöyledir:

“Bir davada hüküm verilebilmesi, başka bir davaya, idari makamın tespitine yahut dava konusuyla ilgili bir hukuki ilişkinin mevcut olup olmadığına kısmen veya tamamen bağlı ise mahkemece o davanın sonuçlanmasına veya idari makamın kararına kadar yargılama bekletilebilir.”

B. İlgili Yargı Kararları

34. Yargıtay İçtihatları Birleştirme Hukuk Genel Kurulunun 17/4/2014 tarihli ve 28975 sayılı Resmî Gazete’de yayımlanan 21/2/2014 tarihli ve E.2013/1, K.2014/1 sayılı kararının "Ara kararların temyiz kabiliyeti" kenar başlıklı kısmı şöyledir:

“Usul kanunumuz sadece nihai kararların temyiz edilebileceklerini kabul ettiğinden (5236 s.K. ile yeniden düzenlenmeden önceki HUMK m.427/1; 6100 sayılı HMK m.341/(1) ve m.361/1) ara kararları

tek başlarına temyiz edilemez. Yargılamayı sona erdirip mahkemenin dosyadan el çekmesini gerektirmediği (nihai karar olmadığı) için tek başlarına temyiz edilemeyen ara kararları ancak, bir nihai karar olan hüküm ile birlikte temyiz edilebilir.”

V. İNCELEME VE GEREKÇE

35. Mahkemenin 25/10/2017 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Kişinin Maddi ve Manevi Varlığını Koruma Hakkının İhlal Edildiğine İlişkin İddia

36. Başvurucu; hukuk yargılaması sürecinde bilirkişi görüşü alınması yönündeki taleplerinin karşılanmadığını, ceza davasının sonucunun bekletici mesele yapıldığını, dolayısıyla talepleri hakkında hiçbir inceleme yapılmadığını, bu nedenle kusur ve tazmin sorumluluğunun niteliği ve kapsamının belirlenmesi konusunda kendisine davasını ispatlama olanağı sağlanmadığını belirtmiştir. Ayrıca operasyonu gerçekleştiren uzmanın kusurunun belirlenebilmesi için dava süreci boyunca yaklaşık beş yıl estetik operasyon geçirmemesine rağmen fiziksel ve psikolojik sağlığını korumak ve yapılacak ameliyatların başarı şansını -gecikmeyi artırarak- daha fazla zedelememek için 15/2/2014 ve 17/6/2014 tarihlerinde iki kez düzeltme ameliyatı yaptırmak zorunda kaldığını bildirmiştir. Başvurucu, bu nedenlerle Anayasa'nın 17. maddesinde tanımlanan haklarının ihlal edildiğini ileri sürmüştür. Başvurucu ayrıca kimliğinin kamuya açık belgelerde gizli tutulmasını talep etmiştir.

37. İddianın değerlendirilmesinde dayanak alınacak Anayasa'nın 17. maddesinin birinci fıkrası şöyledir:

“Herkes, yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkına sahiptir.”

38. Anayasa Mahkemesi, ameliyat sonrası göğüslerde meydana gelen deformasyon şikâyeti (Melahat Sönmez, B. No: 2013/7528, 9/9/2015) ile parmağın sakat kaldığı tıbbi bir müdahaleyle ilgili olan şikâyeti (Ahmet Sevim, B. No: 2013/474, 9/9/2015) Anayasa'nın 17. maddesinin birinci fıkrasında düzenlenen kişinin maddi ve manevi varlığını koruma hakkı kapsamında ele almıştır. Anılan kararlar doğrultusunda somut olayda başvurucunun geçirdiği ameliyat sonrasında göğüs bölgesinde oluşan deformasyon üzerine açtığı tazminat davasında taleplerinin karşılanmamış olduğu yönündeki şikâyetinin Anayasa'nın 17. maddesinin birinci fıkrasında düzenlenen kişinin maddi ve manevi varlığını koruma hakkı kapsamında incelenmesi gerekmektedir.

39. Tıbbi ihmalle ilgili olarak yalnızca ceza muhakemesi yoluna başvurulmuş olması, kural olarak bireysel başvuruda bulunabilmek için şart olan etkili tüm başvuru yollarının tüketilmesi koşulunun yerine getirildiği anlamına gelmemektedir. Buna göre yaşam hakkının veya fiziksel bütünlüğün

ihlaline kasten sebebiyet verilmemiş ise "etkili bir yargısal sistem kurma" yönündeki pozitif yükümlülük her olayda mutlaka ceza davası açılmasını gerektirmez. Bu ilke, tıbbi ihmal sonucu meydana geldiği ileri sürülen ölüm olayları ile maddi ve manevi varlığa verilen zarar hâlleri için de geçerlidir. Bu durumlarda mağdurlara hukuki, idari hatta disiplinle ilgili hukuk yollarının açık olması yeterli olabilir (Serpil Kerimoğlu ve diğerleri, B. No: 2012/752, 17/9/2013, § 59; Nail Artuç, B. No: 2013/2839, 3/4/2014, § 37; Sabri Oğurlu, B. No: 2013/6005, 7/7/2015, § 42; Mahmut Sancar, B. No: 2013/3583, 7/7/2015, § 36).

40. Bu şekilde bir kabul, bu tür olaylarda yürütülen ceza soruşturmalarının Anayasa Mahkemesi tarafından değerlendirilmeyeceği anlamına gelmemektedir. Ancak ilke olarak tıbbi ihmellere ilişkin şikâyetler konusunda temel başvuru yolu, hukuki sorumluluğu tespit adına takip edilecek olan hukuki veya idari tazminat davası yoludur (Nail Artuç, § 38; Seyfi Yayla ve diğerleri, B. No: 2013/829, 11/12/2014 § 51; Turgay Çamlı, B. No: 2012/1266, 17/9/2014, § 48; Sabri Oğurlu, § 43; Mahmut Sancar, § 37).

41. Bireysel başvuru yolunun ikincil niteliği gereği Anayasa Mahkemesine başvuruda bulunabilmek için öncelikle olağan kanun yollarının tüketilmesi zorunludur. Somut olayda ihlale neden olduğu ileri sürülen tıbbi müdahale nedeniyle başvuru, ceza yargılamasının yanı sıra İzmir4. Asliye Hukuk Mahkemesinde tazminat davası açmıştır. Ancak bu başvuru yolu tüketilmeden bireysel başvuruda bulunulmuştur.

42. Açıklanan nedenlerle başvurunun bu kısmının diğer kabul edilebilirlik koşulları yönünden incelenmeksizin başvuru yollarının tüketilmemesi nedeniyle kabul edilemez olduğuna karar verilmesi gerekir.

B. Hukuk Davasında Yargılamanın Üçüncü Kişilere Kapalı Yapılması Talebinin Reddi Nedeniyle Özel Hayatın Gizliliği Hakkının İhlal Edildiğine İlişkin İddia

1. Başvurucunun İddiaları

43. Başvurucu; hukuk davasında, operasyon sonrasında vücudunda meydana gelen bozulmayı göstermek amacıyla belden üstünü gösteren ameliyat öncesi ve sonrası fotoğrafları delil olarak dava dosyasına sunduğunu, bunların mahrem nitelikte olması nedeniyle gizlilik talebinde bulunduğunu ancak mahkemenin bu talebi reddettiğini belirtmiştir. Başvurucu bu nedenle Anayasa'nın 20., 36. ve 141. maddelerinde tanımlanan haklarının ihlal edildiğini ileri sürmüştür; 33.200 TL maddi ve 395.000 TL manevi tazminat ödenmesine karar verilmesini talep etmiştir.

2. Değerlendirme

44. Anayasa'nın 20. maddesinin birinci ve üçüncü fıkraları şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

...

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

45. Anayasa'nın 141. maddesinin birinci fıkrası şöyledir:

"Mahkemelerde duruşmalar herkese açıktır. Duruşmaların bir kısmının veya tamamının kapalı yapılmasına ancak genel ahlâkın veya kamu güvenliğinin kesin olarak gerekli kıldığı hallerde karar verilebilir."

a. Kabul Edilebilirlik Yönünden

46. Anayasa Mahkemesine bireysel başvuru, ikincil nitelikte bir hukuk yoludur. Temel hak ve özgürlüklerin ihlal edildiği iddialarının öncelikle derece mahkemelerinde ve olağan kanun yolları ile çözüme kavuşturulması esastır. Bireysel başvuru yoluna, iddia edilen hak ihlallerinin bu olağan denetim mekanizması çerçevesinde giderilememesi durumunda başvurulabilir (Bayram Gök, B. No: 2012/946, 26/3/2013, §§ 16-20).

47. Başvuru yollarının tüketilmesi gereğinden söz edilebilmesi için öncelikle hukuk sisteminde, hakkının ihlal edildiğini iddia eden kişinin başvurabileceği idari veya yargısal bir hukuki yolun öngörülmüş olması gerekmektedir. Ayrıca bu hukuki yolun iddia edilen ihlalin sonuçlarını giderici, etkili ve başvuru açısından makul bir çabayla ulaşılabilir nitelikte olması ve sadece kâğıt üzerinde kalmayıp fiilen de işlerliğe sahip bulunması gerekmektedir. Olmayan bir hukuki yolun tüketilmesi başvurucudan beklenemeyeceği gibi hukuken veya fiilen etkili bulunmayan, ihlalin sonuçlarını düzeltici bir vasıf taşımayan veya ölçülü olmayan birtakım şekli koşulların öngörülmesi nedeniyle fiilen erişilebilir ve kullanılabilir olmaktan uzaklaşan başvuru yollarının tüketilmesi zorunluluğu bulunmamaktadır (Fatma Yıldırım, B. No: 2014/6577, 16/2/2017, § 39).

48. Başvurucu, İzmir 4. Asliye Hukuk Mahkemesinde tazminat davası açmıştır. Dava dilekçesinde, özel hayatın gizliliği hakkının ihlalini teşkil edebilecek, fotoğraflar gibi bilgi ve belgeler hakkında

gizlilik kararı verilmesi talep edilmiştir. İzmir 4. Asliye Hukuk Mahkemesinin E.2010/347 sayılı dosyasının 26/10/2010 tarihli tensip duruşmasında başvuruçunun "gizlilik talebi ile ilgili karar verilmesine yer olmadığına" karar verilmiştir.

49. İzmir 4. Asliye Hukuk Mahkemesinin gizlilik talebinin bu şekilde reddine dair söz konusu kararı ara kararı niteliğinde olup bu kararların ancak hükümle birlikte istinaf veya temyiz kanun yolunda incelenmesi mümkündür. Dolayısıyla esas hakkındaki karar verilmeden önceki aşamada söz konusu ara kararına karşı gidilebilecek, ilk derece mahkemesinin bu ara kararını denetleyerek hukuka aykırılığı tespit edecek ve gerekiyorsa Mahkemenin verdiği ara kararını kaldıracak etkili ama aynı zamanda pratik olarak da yeterince belirgin bir idari veya yargısal başvuru yolu bulunmamaktadır (Tuğba Arslan [GK], B. No: 2014/256, 25/6/2014, § 42).

50. Ayrıca bu ara kararının hükümle birlikte temyiz veya istinaf yolunda denetlenmesi de başvuruçunun şikâyetini gidermede yeterli ve etkili bir çözüm sunmamaktadır. Medeni yargılama, özel hukuk kişileri arasındaki uyuşmazlıkların görüldüğü yargılama türüdür. İlk derece mahkemesinin taraflardan birinin gizlilik talebini reddetmesi durumunda Anayasa'yla kamu makamlarına yüklenmiş olan bireyin mahremiyetine saygı gösterilmesi ödevinin yerine getirilip getirilmediği tartışması ortaya çıkmaktadır. Ancak medeni usul hukukunda öngörülen istinaf ve temyiz kanun yolları, özel hayatın gizliliği hakkı bakımından hüküm verilmesine kadar geçecek sürede ortaya çıkabilecek ihlalleri engelleyemediği gibi, bir zarar meydana gelmesi hâlinde bu zararın telafisine imkân veren tazminat gibi bir giderim sunacak şekilde de tasarlanmamıştır.

51. Bunun yanı sıra istinaf veya temyiz yolunda taraflardan birinin gizlilik talebinin reddedilmiş olması nedeniyle bozma kararı verilmesi ve bu suretle yargılamanın yeniden ve gizli şekilde yapılması da oldukça zayıf bir ihtimaldir. Zira hukukumuzda mahkemelerin resen dikkate alması gereken medeni usul hukuku kurallarına aykırı karar vermesi mutlak bozma sebebi sayılmakta, mutlak bozma sebepleri dışında kalan medeni usul hukuku kurallarına aykırılıklar ise nispi bozma sebepleri olarak adlandırılmaktadır. Nispi bozma sebepleri kapsamındaki medeni usul hukuku kurallarına aykırılık, ancak mahkemenin vermiş olduğu hükmü etkileyecek nitelikte ise bozma sebebi olarak kabul edilmektedir. Aleniyet ilkesine ilişkin kurallara aykırılıklar da nispi bozma sebepleri arasında görülmektedir. Dolayısıyla bir tarafın yargılamanın gizli yapılmasına ilişkin talebi reddedilmiş ve aleni yargılamaya devam edilmiş ise bu durum sonuca mutlak etkili bir usul yanlışlığı olarak kabul edilmemektedir.

52. Buna göre temyiz veya istinaf kanun yollarının başvuru kanunlarının gizlilik talebinin reddi yönündeki ara kararına karşı ilk derece mahkemesinde yargılama devam ederken gidilebilecek, tüketilmesi zorunlu kanun yolları olmadığı sonucuna varılmıştır.

53. Açıklanan nedenlerle başvuru kanunlarının gizlilik talebinin reddi yönündeki ara kararını ortadan kaldıracak ve ihlali derhâl giderecek nitelikte bir telafi imkânı sunan başvuru yolu bulunmadığından başvuru yolunun tüketilmesi koşulunun sağlandığı sonucuna ulaşılmıştır.

54. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan özel hayatın gizliliği hakkının ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

b. Esas Yönünden

55. Başvurucu, İzmir 4. Asliye Hukuk Mahkemesinde tazminat davası açmıştır. Dava dilekçesinde özel hayata saygı hakkının ihlalini teşkil edebilecek fotoğraflar gibi bilgi ve belgeler hakkında gizlilik kararı verilmesi talep edilmiştir.

56. İzmir 4. Asliye Hukuk Mahkemesinin E.2010/347 sayılı dosyasının 26/10/2010 tarihli tensip duruşmasında başvuru kanunlarının "gizlilik talebi ile ilgili karar verilmesine yer olmadığına" karar verilmiştir.

57. Anayasa Mahkemesinin daha önceki kararlarında da belirtildiği üzere kişisel veri -belirli veya kimliği belirlenebilir olmak şartıyla- bir kişiye ilişkin bütün bilgileri ifade eder (AYM, E.2014/74, K.2014/201, 25/12/2014; E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2013/84, K.2014/183, 4/12/2014; E.2014/180, K.2015/30, 19/3/2015). Kişilerin sağlık durumlarına dair bilgiler de kişisel veri niteliğindedir (T.A.A., B. No: 2014/19081, 1/2/2017, § 103).

58. Anayasa'nın 20. maddesi esas itibarıyla bireyi kamu makamlarının keyfî müdahalesine karşı korumakla birlikte devletin sadece böyle bir müdahalede bulunmaktan kaçınması şeklindeki negatif yükümlülüğün yanı sıra özel hayata ve aile hayatına etkili bir şekilde saygı gösterilmesi bakımından pozitif yükümlülükleri de kapsamına almaktadır. Bu yükümlülükler, bireylerin kendi aralarındaki ilişkiler alanında olsa dahi özel hayata saygıyı sağlamayı hedefleyen tedbirlerin alınmasını zorunlu kılar (Adnan Oktar (3), B. No: 2013/1123, 2/10/2013, § 32; Marcus Frank Cerny [GK], B. No: 2013/5126, 2/7/2015, § 36).

59. Başvuru konusu olayda olduğu gibi kişiler arasındaki özel hukuk ilişkilerinde kamusal makamların yükümlülükleri, bireylerin temel hak ve özgürlüklerine üçüncü kişilerin müdahalesinin önlenmesi için gerekli önlemlerin alınması ve mahkemelerce korunma sağlanmasıdır. Kamusal

makamlarca gerekli yapısal önlemler alınmış olursa da uyuşmazlık konusu davayı yürüten mahkemelerce verilen kararlarda üçüncü kişilerin müdahalelerine karşı bireylere korunma imkânı sağlanmadığı durumlarda bu yükümlülükler gereği gibi yerine getirilmemiş olacaktır. Bu, kamusal makam olan mahkemeler aracılığıyla bireylerin hak ve özgürlüklerinin korunmasız bırakıldığı anlamına gelecektir (Ömür Kara ve Onursal Özbek, B. No: 2013/4825 , 24/3/2016, § 49).

60. Medeni usul yargılamasında aleniyet, duruşmaların ve esas hakkındaki kararın bildirilmesinin herkese açık olarak yürütülmesini ifade etmektedir. Yargılamaların aleni yapılması ilkesi adil yargılanma hakkı kapsamında korunmaktadır. Yargılamanın aleniliği ilkesinin amacı, adli mekanizmanın işleyişini kamu denetimine açarak yargılama faaliyetinin saydamlığını güvence altına almak ve yargılamada keyfiliği önlemektir. Bu yönüyle anılan ilke, hukuk devletinin en önemli gerçekleştirme araçlarından birini oluşturur (Nevruz Bozkurt, B. No: 2013/664, 17/9/2013, § 32).

61. Bununla birlikte somut olayda olduğu gibi özel hayatın gizliliği hakkı bağlamında özellikle hassasiyet arz eden kişisel verilerin korunmasının gözetilmesi gereken durumlarda yargı makamlarının gerekli tedbirleri alması ödevi bulunmaktadır. Bu doğrultuda derece mahkemelerince yargılamanın aleni yürütülmesinde var olan kamusal menfaat ile başvurucunun mahremiyetinin korunması menfaati arasında adil bir denge kurulmalı ve ulaşılan sonuç hakkında hüküm kurulurken ilgili ve yeterli gerekçeler sunulmalıdır.

62. Somut olayda başvuru; İzmir 4. Asliye Hukuk Mahkemesinin 2010/347 esasına kayıtlı dava dosyasına göğüs bölgesini gösteren, ameliyat öncesi ve sonrası fotoğraflarını sunmuştur. Bu fotoğraflarda başvurucunun yüzü görünmemektedir ancak dava dosyasında başvurucunun kimliğini ortaya koyan bilgilerin mevcut olduğu dikkate alındığında söz konusu fotoğrafların -kimliği belirli veya belirlenebilir gerçek kişiye ilişkin veri- kişisel veri niteliğinde olduğuna kuşku yoktur.

63. Olayda; kadın olan başvurucunun vücudunun göğüs bölgesine ilişkin fotoğraflarını ve sağlık bilgilerini içeren dava dosyasının gizli kalmasını istemesi, yargılamanın kamuya ve dolayısıyla üçüncü kişilere açık olarak görülmesinden ve mahrem bilgilerinin ifşa edilmesinden kaygı duyması özel hayatın gizliliği hakkına ilişkin makul ve savunulabilir nitelikte bir taleptir.

64. Bunun yanı sıra başvurucunun talebi yaklaşık yedi sene önce 26/10/2010 tarihinde yapılan tensip duruşmasında karara bağlanmış, gerekçesi açıklanmadan kabul edilmemiştir ve dava derdesttir. Dolayısıyla başvuru çok uzun bir süre mahrem fotoğraflarının üçüncü kişilerce görülebileceği tehlikesine maruz bırakılmıştır. Bu bakımdan başvurucunun mahrem fotoğraflarına erişimin kısıtlanması hakkında özel hayatına ilişkin korunmaya değer önemli bir menfaatinin bulunduğu tartışmasızdır.

65. Yargı mercilerinin tarafların iddia ve taleplerini değerlendirmede takdir yetkileri olduğu açık olmakla birlikte kişilerin mahremiyeti, dolayısıyla özel hayatı üzerinde önemli etkiler doğurabilecek konulara ilişkin taleplerin reddi durumunda bunun gerekçelerinin ayrıntılı şekilde kararda gösterilmesi, hakkaniyete uygun bir yargılamanın gereğidir.

66. 6100 sayılı Kanun'un 28. maddesinin üçüncü fıkrasında tarafların gizlilik talebi hakkındaki kararın gerekçelerinin esas hakkındaki kararla birlikte açıklanacağı hükmü yer almaktadır. Ancak maddenin gerekçesinde de belirtildiği üzere bu düzenleme, gizliliğe karar verilmesi durumunda gizliliğin amacını yok edecek açıklamaların alenen yapılmasının önlenmesi için getirilmiştir. Anayasa'nın 141. maddesinin üçüncü fıkrasında da "Bütün mahkemelerin her türlü kararları gerekçeli olarak yazılır." denilerek mahkemelere her türlü kararlarını gerekçeli yazma yükümlülüğü yüklenmiştir.

67. Anayasa'nın üstünlüğü ve bağlayıcılığı dikkate alınarak 6100 sayılı Kanun'un 28. maddesinin üçüncü fıkrasında yer alan, tarafların gizlilik talebi hakkındaki kararın gerekçelerinin esas hakkındaki karar ile birlikte açıklanacağı düzenlemesinin bu konudaki ara kararların tamamen gerekçesiz olacağı şeklinde yorumlanması kabul edilemez. İlk derece mahkemesinin gizlilik talepleri hakkındaki ara kararını gizliliğin amacını yok edecek açıklamalardan kaçınarak ama mutlaka gerekçeli olarak vermesi gereklidir. Üstelik bu şekildeki ara kararların denetlenmesine yönelik etkili olağan kanun yolu bulunmadığı dikkate alındığında bu kararların gerekçeli olmasının önemi daha da artmaktadır. Zira tarafların muhakeme sırasında ileri sürdükleri iddialarının kurallara uygun biçimde incelenip incelenmediğini bilmeleri ve ayrıca demokratik bir toplumda, kendi adlarına verilen yargı kararlarının sebeplerini öğrenmelerinin sağlanması ancak gerekçe ile mümkündür.

68. İzmir 4. Asliye Hukuk Mahkemesince 26/10/2010 tarihli ara kararı ile gizlilik talebi reddedilmiştir ancak bu kararda hiçbir gerekçe bulunmamakta olup hangi somut nedenlere bağlı olarak gizlilik kararı verilmediği açıklanmamıştır. Bir başka ifadeyle delil mahiyetinde dosyaya sunulan ve kişisel veri oluşturan bir fotoğraf hakkında gizlilik kararı verilmesinin "aleniyet ilkesi"ni neden ihlal edeceğinin gerekçesi ortaya konmamıştır. Bu bağlamda söz konusu kararların konuyla ilgili ve yeterli gerekçe içermediği kabul edilmelidir. Buna görederece mahkemesi kararı bu yönde tatmin edici gerekçe içermediği ve yedi yıldan bu yana derdest olan davada çok uzun bir süre başvurusunun korunmaya çalıştığı riskle yüz yüze bırakılmış olması dikkate alındığında bireysel yarar ile kamu yararı arasında adil dengeyi sağlayacak bir önlem alınmadığı sonucuna ulaşılmıştır.

69. Açıklanan nedenlerle Anayasa'nın 20. maddesinde yer alan özel hayatın gizliliği hakkının ihlal edildiğine karar verilmesi gerekir.

C. Adil Yargılanma Hakkının İhlal Edildiğine İlişkin İddia

1. Başvurucunun İddiaları

70. Başvurucu; katılan sıfatıyla yer aldığı ceza yargılaması sürecinde eksik inceleme yapıldığını, delillerin yanlış değerlendirildiğini, yargılamanın makul sürede sonuçlandırılmadığını, ayrıca hukuk yargılamasının da makul sürede sonuçlandırılmadığını belirterek Anayasa'nın 36. maddesinde tanımlanan adil yargılanma hakkının ihlal edildiğini ileri sürmüştür.

2. Değerlendirme

a. Ceza Yargılamasında Adil Yargılanma Hakkının İhlal Edildiğine İlişkin İddia

71. 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 45. maddesinin (1) numaralı fıkrasına göre bireysel başvurunun incelenmesi için kamu gücü tarafından ihlal edildiği iddia edilen hakkın Anayasa'da güvence altına alınmış olmasının yanı sıra Avrupa İnsan Hakları Sözleşmesi (Sözleşme) ve Türkiye'nin taraf olduğu Sözleşme'ye ek protokoller kapsamına da girmesi gerekir. Anayasa ve Sözleşme'nin ortak koruma alanı dışında kalan hak ihlali iddiasını içeren başvurular bireysel başvurunun kapsamında değildir (Onurhan Solmaz, B. No: 2012/1049, 26/3/2013, § 18).

72. Sözleşme'nin 6. maddesinde adil yargılanmaya ilişkin hak ve ilkelerin "medeni hak ve yükümlülükler ile ilgili uyumsuzlukların ve bir suç isnadı"nın esasının karara bağlanması esnasında geçerli olduğu belirtilerek hakkın kapsamı bu konularla sınırlandırılmıştır. Dolayısıyla bahsedilen hâller dışında kalan adil yargılanma hakkının ihlali iddiasına dayanan başvurular, Anayasa ve Sözleşme kapsamı dışında kalacağından bireysel başvuruya konu olamaz. Bir ceza davasında üçüncü kişilerin cezalandırılmasını talep eden mağdur, suçtan zarar gören, şikâyetçi veya katılan sıfatını haiz kişiler Sözleşme'nin 6. maddesinin koruma alanı dışında kalmaktadır (Onurhan Solmaz, §§ 23, 24).

73. Somut olayda başvurucunun katılan sıfatıyla yer aldığı ceza yargılaması süreciyle ilgili şikâyetlerinin üçüncü kişilerin cezalandırılmasına yönelik olduğu, dolayısıyla adil yargılanma hakkı kapsamına girmediği anlaşılmaktadır.

74. Açıklanan nedenlerle başvurunun bu kısmının diğer kabul edilebilirlik koşulları yönünden incelenmeksizin konu bakımından yetkisizlik nedeniyle kabul edilemez olduğuna karar verilmesi gerekir.

b. Hukuk Yargılamasında Makul Sürede Yargılanma Hakkının İhlal Edildiğine İlişkin İddia

i. Kabul Edilebilirlik Yönünden

75. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan makul sürede yargılanma hakkının ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

ii. Esas Yönünden

76. Medeni hak ve yükümlülüklerle ilgili uyuşmazlıklara ilişkin yargılamanın süresi tespit edilirken sürenin başlangıç tarihi olarak davanın ikame edildiği tarih; sürenin sona erdiği tarih olarak -çoğu zaman icra aşamasını da kapsayacak şekilde- yargılamanın sona erdiği tarih, yargılaması devam eden davalar yönünden ise Anayasa Mahkemesinin makul sürede yargılanma hakkının ihlal edildiğine ilişkin şikâyetle ilgili kararını verdiği tarih esas alınır (Güher Ergun ve diğerleri, B. No: 2012/13, 2/7/2013, §§ 50, 52).

77. Medeni hak ve yükümlülüklerle ilgili uyuşmazlıklara ilişkin yargılama süresinin makul olup olmadığı değerlendirilirken yargılamanın karmaşıklığı ve kaç dereceli olduğu, tarafların ve ilgili makamların yargılama sürecindeki tutumu ve başvuruçunun yargılamanın süratle sonuçlandırılmasındaki menfaatinin niteliği gibi hususlar dikkate alınır (Güher Ergun ve diğerleri, §§ 41-45).

78. Hukuk ve ceza davalarının konuları, tarafları ve amaçları farklı olduğundan ceza mahkemesi kararları hukuk davaları için kural olarak kesin hüküm oluşturmaz. Haksız fiil nedeniyle açılan tazminat davalarını çözmek bütünüyle hukuk hâkiminin görevi içindedir. Bir "bekletici sorun" iddiası karşısında kalan hâkimin görevi dışındaki bu iddianın mutlaka görevli mahkemede çözülmesini bekleme yükümlülüğü yoktur. Kendisi de birçok durumda ileri sürülen hususu karara bağlayabilir. Kaldı ki hukuk hâkimi, ceza mahkemesinin mahkûmiyet kararıyla bağlı ise de maddi olayı tespit etmeyen beraat kararı hukuk hâkimini bağlamaz. Bu yüzden hukuk hâkimi, topladığı deliller doğrultusunda karar verebilir. Ceza mahkemesinin delilleri tespit ve takdiri ile hukuk mahkemesinin delilleri tespit ve takdirinin farklı olmasının bir sonucu olarak bir olayda sebep-sonuç bağı bulunmadığına dair ceza mahkemesi kararı dahi hukuk hâkimini bağlamayabilir. Bu nedenle hukuk mahkemeleri ceza davasının sonucunu beklemek için yargılamayı uzun bir süre ertelemek zorunda değildir (Tevfik Yıldırım, B. No: 2013/4701, 23/1/2014, § 58).

79. Somut olayda İzmir 4. Asliye Hukuk Mahkemesinde 19/7/2010 tarihinde tazminat davası açılmış, Mahkemenin 26/4/2012 tarihli duruşmasında İzmir 7. Sulh Ceza Mahkemesinde görülmekte olan ceza davası sonucunda verilecek kararın beklenmesine karar verilmiştir. Mahkemenin 10/9/2012 tarihli duruşmasında ise belirtilen ceza davası sonucunda verilecek kararın kesinleşmesinin beklenmesine ve 6100 sayılı Kanun'un 165. maddesi uyarınca söz konusu karar kesinleşinceye kadar dosyanın

askıya alınmasına karar verildiği, dosyanın yerel mahkeme aşamasında derdest durumda olduğu anlaşılmıştır.

80. Belirtilen ceza davası sonucunun beklenmesi noktasındaki takdir ilgili usul hükümleri uyarınca derece mahkemelerine aittir. Ancak ilk derece mahkemesince yargılamanın uzunluğuna neden olan en önemli unsurun ceza mahkemesinde devam eden davanın bekletici mesele yapılarak yaklaşık 7 yıl (6 yıl 10 ay 11 gün) süreyle ceza davasında verilecek kararın beklenmesi olduğu anlaşılmaktadır. Buna göre İzmir 4. Asliye Hukuk Mahkemesinde 19/7/2010 tarihinde açılan, yaklaşık yedi yıl süren ve sonuçlanmadığı anlaşılan davada yargılama süresinin makul olmadığı sonucuna varılmıştır.

81. Açıklanan nedenlerle Anayasa'nın 36. maddesinde güvence altına alınan makul sürede yargılanma hakkının ihlal edildiğine karar verilmesi gerekir.

D. 6216 Sayılı Kanun'un 50. Maddesi Yönünden

82. 6216 sayılı Kanun'un 50. maddesinin (1) ve (2) numaralı fıkraları şöyledir:

“(1) Esas inceleme sonunda, başvurunun hakkının ihlal edildiğine ya da edilmediğine karar verilir. İhlal kararı verilmesi hâlinde ihlalin ve sonuçlarının ortadan kaldırılması için yapılması gerekenlere hükmedilir...

(2) Tespit edilen ihlal bir mahkeme kararından kaynaklanmışsa, ihlali ve sonuçlarını ortadan kaldırmak için yeniden yargılama yapmak üzere dosya ilgili mahkemeye gönderilir. Yeniden yargılama yapılmasında hukuki yarar bulunmayan hâllerde başvuru lehine tazminata hükmedilebilir veya genel mahkemelerde dava açılması yolu gösterilebilir. Yeniden yargılama yapmakla yükümlü mahkeme, Anayasa Mahkemesinin ihlal kararında açıkladığı ihlali ve sonuçlarını ortadan kaldıracak şekilde mümkünse dosya üzerinden karar verir.”

83. Başvurucu 33.200 TL maddi ve 395.000 TL manevi tazminat ödenmesine karar verilmesini talep etmiştir.

84. Mevcut başvuruda, hukuk davasında yargılamanın üçüncü kişilere kapalı yapılması talebinin reddi nedeniyle özel hayatın gizliliği hakkının ihlal edildiği sonucuna varılmıştır.

85. Özel hayatın gizliliği hakkının ihlali nedeniyle yalnızca ihlal tespitiyle giderilemeyecek olan manevi zararları karşılığında başvurucuya takdiren net 8.000 TL manevi tazminat ödenmesine karar verilmesi gerekir. Ayrıca söz konusu tazminat davasının İzmir 4. Asliye Hukuk Mahkemesinde derdest olduğu dikkate alınarak özel hayatın gizliliği hakkının ihlalinin geleceğe dönük sonuçlarının

ortadan kaldırılması için kararın bir örneğinin İzmir 4. Asliye Hukuk Mahkemesine gönderilmesine karar verilmesi gerekir.

86. Bunun yanı sıra başvurucunun açtığı tazminat davası, makul olmayan bir süre olan yaklaşık yedi yıldır devam etmektedir. Dolayısıyla başvurucuya yalnızca ihlal tespitiyle giderilemeyecek olan manevi zararı karşılığında takdiren 9.600 TL manevi tazminat ödenmesine karar verilmesi gerekir.

87. Başvurucu maddi tazminat talep etmiş olmakla birlikte başvurucunun açtığı tazminat davası yerel mahkeme aşamasında derdest durumdadır. Başvurucunun maddi zararlarının tespitine ilişkin yargılama süreci devam ettiğinden bu aşamada maddi tazminat koşullarının Anayasa Mahkemesince incelenmesi mümkün değildir. Bu nedenle maddi tazminat isteminin reddi gerekir.

88. Dosyadaki belgelerden tespit edilen 206,10 TL harç ve 1.800 TL vekâlet ücretinden oluşan toplam 2.006,10 TL yargılama giderinin başvurucuya ödenmesine karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Kamuya açık belgelerde başvurucunun kimliğinin gizli tutulması talebinin **KABULÜNE,**

B. 1. Kişinin maddi ve manevi varlığını koruma hakkının ihlal edildiğine ilişkin iddianın başvuru yollarının tüketilmemesi nedeniyle **KABUL EDİLEMEZ OLDUĞUNA,**

2. Ceza davası sürecinde adil yargılanma hakkının ihlal edildiğine ilişkin iddianın konu bakımından yetkisizlik nedeniyle **KABUL EDİLEMEZ OLDUĞUNA,**

3. Tazminat davasında yargılamanın üçüncü kişilere kapalı yapılması talebinin reddi nedeniyle özel hayatın gizliliği hakkının ihlal edildiğine ilişkin iddianın **KABUL EDİLEBİLİR OLDUĞUNA,**

4. Tazminat davası sürecinde makul sürede yargılanma hakkının ihlal edildiğine ilişkin iddianın **KABUL EDİLEBİLİR OLDUĞUNA,**

C. 1. Anayasa'nın 20. maddesinde güvence altına alınan özel hayatın gizliliği hakkının **İHLAL EDİLDİĞİNE,**

2. Anayasa'nın 36. maddesinde güvence altına alınan makul sürede yargılanma hakkının **İHLAL EDİLDİĞİNE,**

D. Tazminat davasının İzmir 4. Asliye Hukuk Mahkemesinde derdest olduğu dikkate alınarak özel hayatın gizliliği hakkının ihlalinin geleceğe dönük sonuçlarının ortadan kaldırılması için kararın bir örneğinin İzmir 4. Asliye Hukuk Mahkemesine **GÖNDERİLMESİNE,**

- E. 1.** Özel hayatın gizliliđi hakkının ihlali nedeniyle yalnızca ihlal tespitiyle giderilemeyecek olan manevi zararları karşılığında başvurucuya net 8.000 TL manevi tazminat ÖDENMESİNE,
2. Yargılama faaliyetinin uzunluđu sebebiyle başvurucuya net 9.600 TL manevi tazminat ÖDENMESİNE,
3. Tazminata ilişkin diđer taleplerin REDDİNE,
- F.** 206,10 TL harç ve 1.800 TL vekâlet ücretinden oluşan toplam 2.006,10 TL yargılama giderinin BAŞVURUCUYA ÖDENMESİNE,
- G.** Ödemelerin, kararın tebliđini takiben başvurucunun Maliye Bakanlıđına başvuru tarihinden itibaren dört ay içinde yapılmasına, ödemede gecikme olması hâlinde bu sürenin sona erdiđi tarihten ödeme tarihine kadar geçen süre için yasal FAİZ UYGULANMASINA,
- H.** Kararın bir örneğinin Adalet Bakanlıđına GÖNDERİLMESİNE 25/10/2017 tarihinde OYBİRLİĞİYLE karar verildi.

Anayasa Mahkemesi - Nurcan Belin Kararı (2014/14187)

Nurcan Belin, B. No: 2014/14187, 10/1/2018

Başvuru, mesleki sicil notlarının gizli ve kişiye özel bir yazıyla başvurucuya bildirilmesine karar verilmesine karşın bu belgelerin kurumdaki diğer çalışanlarca görülmesine imkân verecek şekilde işleme alınması nedeniyle özel hayata saygı hakkının ihlal edildiği iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

BİRİNCİ BÖLÜM

KARAR

NURCAN BELİN BAŞVURUSU

(Başvuru Numarası: 2014/14187)

Karar Tarihi: 10/1/2018

BİRİNCİ BÖLÜM

KARAR

Başkan: Burhan ÜSTÜN

Üyeler: Nuri NECİPOĞLU, Kadir ÖZKAYA, Rıdvan GÜLEÇ, Yusuf Şevki HAKYEMEZ

Raportör: Özgür DUMAN

Başvurucu: Nurcan BELİN

I. BAŞVURUNUN KONUSU

1. Başvuru, mesleki sicil notlarının "gizli" ve "kişiye özel" bir yazıyla başvurucuya bildirilmesine karar verilmesine karşın bu belgelerin kurumdaki diğer çalışanlarca görülmesine imkân verecek şekilde işleme alınması nedeniyle özel hayata saygı hakkının ihlal edildiği iddiasına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 29/8/2014 tarihinde yapılmıştır.

3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.
4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.
5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.
6. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık görüş sunmamıştır.

III. OLAY VE OLGULAR

7. Başvuru formu ve eklerinde ifade edildiği şekliyle ilgili olaylar özetle şöyledir:
8. Başvurucu Millî Savunma Bakanlığı (MSB) Sağlık Dairesi Başkanlığında sivil memur olarak görev yapmaktadır.
9. Başvurucu 1/8/2012 tarihinde MSB'ye başvurarak 2003 yılından 2010 yılına kadar olan döneme ait hakkında düzenlenmiş bulunan sicil raporlarının tarafına bildirilmesini talep etmiştir. MSB, hâlen görevde olan personelin sicil bilgilerinin açıklanamayacağı gerekçesiyle 8/8/2012 tarihinde başvurucunun talebini reddetmiştir.
10. Başvurucu, bu işleme karşı 23/8/2012 tarihinde Bilgi Edinme Değerlendirme Kuruluna (Kurul) itirazda bulunmuştur. Kurul 1/11/2012 tarihinde itirazı kabul ederek başvurucunun sicil raporlarının "gizli" ve "kişiyeye özel" yazı ile başvurucunun erişimine sunulmasına karar vermiştir. Kurul, çağdaş kamu yönetiminin yerleşik ülke uygulamalarında kamu görevlileri için düzenlenen sicil raporu benzeri dosyaların üçüncü kişilere karşı gizli tutulduğunu ancak dosyanın ilgisine karşı ise açık olduğunun görüldüğünü belirtmiştir. Kurul 9/10/2003 tarihli ve 4982 sayılı Bilgi Edinme Hakkı Kanunu'nun 15. maddesine atıfta bulunmuş ve bu Kanun hükümlerine göre kurum ve kuruluşların kendi personeli hakkındaki bilgi ve belgeleri üçüncü kişilere karşı gizli tutması gerektiğini ancak bu bilgi ve belgelerin başvurucunun çalışma hayatını ve meslek onurunu etkileyecek nitelikte olmaları durumunda kişiyeye açık olması gerektiğini vurgulamıştır. Kurula göre, talebe konu sicil notlarının başvurucunun çalışma hayatını ve meslek onurunu etkileyecek bir nitelik taşıdığı kuşkusuzdur.
11. MSB Personel Dairesi Başkanlığının 21/11/2012 tarihli yazısı ile Kurul kararının gereği doğrultusunda başvurucuya yazı yoluyla cevap verilmesi hususu Sağlık İşleri Dairesi Başkanlığına bildirilmiştir. Bu yazıya sadece "gizli" kaşesi vurulmuş ve gizlilik derecesi numarası verilmiştir. Bu

belge, MSB Sağlık İşleri Dairesi Başkanlığında görevli İdari Şube Müdürü tarafından 23/11/2012 tarihinde açılarak havalesi yapılmak üzere daire başkanına sunulmuştur. Evrak başvurucaya teslim edilmek üzere Plan ve Yönetim Şube Müdürüne teslim edilmiştir. Başvurucunun da amiri olan bu kişi tarafından başvurucaya ait sicil raporlarının bulunduğu söz konusu yazı kapalı zarf içinde olmadan başvurucaya tebliğ edilmiştir.

12. Başvurucu, gizli kalması gereken bilgilerinin yetkisiz kişilerce görülmek suretiyle kişilik haklarının saldırıya uğradığını belirterek 18/1/2013 tarihinde Askeri Yüksek İdare Mahkemesinde (AYİM) manevi tazminat davası açmıştır. Başvurucu, bu davada MSB aleyhine 50.000 TL manevi tazminata hükmedilmesi talebinde bulunmuştur.

13. AYİM Başsavcılığının 21/5/2013 tarihli görüş yazısında, başvurucaya talebine konu sicil notlarının "gizli" gizlilik derecesiyle ancak "kişiyeye özel" tasnifi yapılmaksızın postaya verildiği belirtilmiştir. Görüş yazısında, bu yüzden evrakın ulaştığı her aşamada evrak memurlarınca açılarak kaydının yapılıp numara verilmesi suretiyle ilgili birime ulaştırıldığı tespitine yer verilmiştir. Başsavcılık, başvurucaya "kişiyeye özel" sicil bilgilerinin içinde yer aldığı zarfın sadece başvuruca tarafından açılacak şekilde tebligata çıkarılması gerektiği hâlde bunun yapılmayarak evrakın başkalarına öğrenilmesine yol açıldığını vurgulamıştır. Başsavcılığa göre bu işlem nedeniyle kişisel hakları ihlal edildiğinden başvurucaya manevi tazminat talebi kabul edilmelidir.

14. AYİM İkinci Dairesi (Daire) 15/1/2014 tarihinde oyçokluğuyla davanın reddine karar vermiştir. Kararın gerekçesinde, başvurucaya bilgi edinme talebi üzerine sicil notlarının Türk Silahlı Kuvvetleri (TSK) Karargâh Hizmetleri Yönergesi'nin üçüncü bölümündeki düzenlemelere uygun olarak verildiği belirtilmiştir. Daireye göre başvurucaya sicil notlarına ilişkin evrakın İdari Şube Müdürü tarafından açılarak Daire Başkanı'na arz edilerek başvurucaya teslim edilmek üzere Plan ve Yönetim Şube Müdürü'ne teslim edilmesi yönergeye uygundur. Daire, gizli ibareli evrakın Yönerge gereği görmesi gereken kişiler dışında başka bir kimse tarafından görülmediğini vurgulamıştır. Daire bu gerekçeyle başvurucaya manevi olarak bir zarara uğramadığını kabul etmiştir. Kararda yer alan karşıoy yazısında ise davalı idarece bu sicillerin gizli ve kişiyeye özel tasnifi yapılmaksızın postaya verildiği ve evrakın ulaştığı her aşamada evrak memurlarınca açılıp kaydının yapılarak ilgili birime ulaştırıldığı belirtilmiştir. Bu yazıda, başvurucaya kişiyeye özel sicil bilgilerinin içinde yer aldığı zarfın sadece başvuruca tarafından açılacak şekilde tebligata çıkarılması gerektiği hâlde iletilen makamlarca açılarak kaydının yapıldığı vurgulanmıştır. Karşıoy yazısına göre sadece davacı tarafından görülmesi gereken evraka başvuruca dışındaki kişilerce vâkıf olduğundan başvurucaya kişilik hakları ihlal edilmiştir.

15. Başvurucu, karar düzeltme talebinde bulunmuştur. Karar düzeltme talebi üzerine AYİM Başsavcılığının 8/5/2014 tarihli görüş yazısında, Kurul kararı uyarınca gizli ve kişiye özel bir yazı ile başvurucuya tebliğ edilmesi gereken evraka başvuru dışındaki kişilerin de vâkif olduğu belirtilmiştir. Görüş yazısında, bu durumun evraka "kişiye özel" kaşesi vurulmamasından kaynaklandığı ifade edilmiştir. AYİM Başsavcılığı, karar düzeltme isteminin kabulü gerektiği yönünde görüş bildirmiştir. Başvurucunun karar düzeltme istemi Dairenin 18/6/2014 tarihli kararı ile oyçokluğuyla kabul edilmiştir. Bununla birlikte Daire; başvuru ile ilam harçları yönünden itirazı kabul ederek bu hususlarda yeniden karar vermiştir. Kararın gerekçesinde, talep edilen sicil notlarının başvurucuya verilmesi işleminin Yönerge'ye uygun olarak yapıldığı belirtilmiştir. Daireye göre; başvuru evrakı, Yönerge gereği görmesi gerekenler dışında hiç kimse tarafından görülmemiştir. Daire, bu gerekçeyle başvuru herhangi bir zarara uğramadığını belirterek manevi tazminat koşullarının oluşmadığı sonucuna varmıştır.

16. Nihai karar, başvurucuya 1/8/2014 tarihinde tebliğ edilmiştir.

17. Başvurucu 29/8/2014 tarihinde bireysel başvuruda bulunmuştur.

IV. İLGİLİ HUKUK

A. Ulusal Hukuk

18. 4982 sayılı Kanun'un 5. maddesinin birinci fıkrası şöyledir:

"Kurum ve kuruluşlar, bu Kanunda yer alan istisnalar dışındaki her türlü bilgi veya belgeyi başvuranların yararlanmasına sunmak ve bilgi edinme başvurularını etkin, süratli ve doğru sonuçlandırmak üzere, gerekli idarî ve teknik tedbirleri almakla yükümlüdürler."

19. 4982 sayılı Kanun'un 10. maddesinin birinci fıkrası şöyledir:

"Kurum ve kuruluşlar, başvuru sahibine istenen belgenin onaylı bir kopyasını verirler."

20. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3. maddesinin (1) numaralı fıkrasının ilgili kısmı şöyledir:

"d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi, ... ifade eder. "

21. 6698 sayılı Kanun'un 8. maddesi şöyledir:

"(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz.

(2) Kişisel veriler;

a) 5 inci maddenin ikinci fıkrasında,

b) Yeterli önlemler alınmak kaydıyla, 6 ncı maddenin üçüncü fıkrasında,

belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir..."

22. 27/7/1967 tarihli ve 926 sayılı Türk Silâhlı Kuvvetleri Personel Kanunu'nun 1. maddesinin ikinci fıkrası şöyledir:

"Türk Silâhlı Kuvvetlerinde görevli diğer asker ve sivil kişiler kendi özel kanunlarına tabidirler."

23. 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu'nun 13/2/2011 tarihli ve 6111 sayılı Kanun'un 117. maddesi ile kaldırılan 110., 111. ve 113. maddeleri şöyledir:

"Sicil dosyası

Madde 110 - Her Devlet memurunun bir sicil dosyası bulunur, Sicil amirleri tarafından düzenlenecek sicil raporları ile varsa müfettişler tarafından verilen denetleme raporları ve memurların mal beyannameleri sicil dosyalarına konulur.

Özlük ve sicil dosyasının önemi

Madde 111 - Devlet memurlarının ehliyetlerinin tespitinde, kademe ilerlemelerinde, derece yükselmelerinde, emekliye çıkarma veya hizmetle ilişkilerinin kesilmesinde özlük ve sicil dosyaları başlıca dayanaktır.

Sicil raporlarında belirtilecek hususlar

Madde 113 - Sicil amirleri, belli zamanlarda düzenleyecekleri sicil raporlarında, memurların liyakat derecesini not esasına göre kıymetlendirerek tespit ederler."

24. 4/1/1980 tarihli ve 16859 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Türk Silahlı Kuvvetlerinde Görevli Sivil Memurlara Sicil Raporu Vermeye Yetkili Amirler Yönetmeliği'nin 8. maddesi şöyledir:

"Silahlı Kuvvetlerde görevli memurların sicil dosyaları, bağlı oldukları kuruluşun Personel Daire Başkanlığı Sivil Memurlar Şube Müdürlüklerinde (Jandarma Genel Komutanlığı Personel Başkanlığında) muhafaza edilir. Sicil Dosyalarını saklamakla görevli memurlara ait sicil dosyaları bunların amirleri tarafından korunur."

25. Bu Yönetmelik'in 9. maddesi şöyledir:

"Sivil Memurların ehliyetlerinin tesbitinde, kademe ilerlemelerinde, derece yükselmelerinde, emekli edilme veya hizmetle ilişkilerinin kesilmesinde özlük ve sicil dosyaları başlıca dayanaktır."

26. Anılan Yönetmelik 15/7/2011 tarihli ve 27995 sayılı Resmî Gazete'de yayımlanan Türk Silahlı Kuvvetlerinde Görevli Sivil Memurlara Sicil Raporu Vermeye Yetkili Amirler Yönetmeliğinin Yürürlükten Kaldırılmasına Dair Yönetmelik ile yürürlükten kaldırılmıştır.

27. 15/4/2011 tarihli ve 27906 sayılı Resmî Gazete'de yayımlanan 2 Seri No.lu Kamu Personeli Genel Tebliği'nin (B) bendinin (1) numaralı alt bendi şöyledir:

"6111 sayılı Kanunla 657 sayılı Devlet Memurları Kanunundaki sicile ilişkin düzenlemeler yürürlükten kaldırıldığından 2011 yılından başlamak üzere Devlet memurları için sicil raporu doldurulmayacaktır. Geçmiş yıllara ait sicil raporlarının, 1/1/2011 tarihinden başlamak üzere beşinci yılın sonuna kadar muhafaza edilmesi gerekmektedir. 657 sayılı Kanun dışındaki kanunlarda yer alan sicil ve değerlendirmeye ilişkin hükümlerde bir değişiklik yapılmadığından bu hükümlerin uygulanmasına devam edilecektir. Diğer kanunların sicil konusunda 657 sayılı Kanuna atıf yapan hükümlerinin uygulama imkanı kalmadığından bu hükümler uyarınca işlem yapılmaması gerekmektedir.

..."

28. Bu Tebliğ'in (D) bendinin (9) numaralı alt bendi şöyledir:

"Özlük dosyalarının tutulması ve muhafazasında özel hayatın gizliliği ilkesine riayet edilir. Özlük dosyası içeriği hakkında soruşturma ve kovuşturmaya yetkili merciler dışındakilere açıklama yapılamaz, bilgi verilemez. Ayrıca kişinin rızası olmaksızın özlük dosyasındaki bilgiler ve kayıtlar esas alınarak kişi hakkında yayında bulunulamaz."

29. 2/2/2015 tarihli ve 29255 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik'in 27. maddesinin (6) numaralı fıkrası şöyledir:

"'KİŞİYE ÖZEL' ibaresi taşıyan zarf veya belgeler açılmadan ilgiliye teslim edilmek üzere alınır. 'KİŞİYE ÖZEL' ibaresi taşıyan belge üzerinde yalnızca ilgili kişi tasarruf hakkına sahiptir ve ilgilinin talebi olmadan kayda alınamaz."

30. Danıştay İkinci Dairesinin 15/2/2013 tarihli ve E.2008/3328, K.2013/791 sayılı kararının ilgili kısmı şöyledir:

"... 657 sayılı Devlet Memurları Kanunu'nun uyuşmazlık tarihi itibarıyla yürürlükte olan hükümleri uyarınca her yıl düzenlenen sicil raporları; Devlet memurlarının o yıl içerisinde genel durum ve davranışları bakımından olumlu ve olumsuz niteliklerini, kusur ve eksikliklerini, liyakat durumunu

gösteren ve sicil amirlerince not esasına göre düzenlenen belgeler olup, sicil raporlarında bulunan sorular gözönüne alındığında, Devlet memurunun o yıl içerisinde disipline riayeti, sorumluluk duygusu, verimlilik ve çalışkanlığı, görevine bağlılığı, iş heyecanı, mesleki bilgisi, tarafsızlığı, iş arkadaşlarına, amirlerine ve iş sahiplerine karşı tutumu gibi konulara ilişkin olduğu görülmektedir.

Buna göre, sicil raporlarının düzenlenmesi ve olumsuz sicil alanlara getirilen müeyyidelerle sağlanmak istenen amacın, üretimi teşvik priminde güdülen amaç gibi, kamu personelinin daha etkin ve verimli çalışmasını sağlayarak kamu hizmetinin en verimli şekilde yerine getirilmesi olduğu anlaşıl[maktadır]..."

B. Uluslararası Hukuk

31. Avrupa İnsan Hakları Sözleşmesi'nin (Sözleşme) "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesi şöyledir:

“(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.”

32. Avrupa İnsan Hakları Mahkemesi (AİHM), kişisel verilerin korunmasının Sözleşme'nin 8. maddesi kapsamında güvence altına alınan özel hayat ve aile hayatına saygı hakkını bir kişinin kullanması konusunda büyük öneme sahip olduğunu belirtmektedir (S ve Marper/Birleşik Krallık [BD], B. No: 30562/04-30566/04, 4/12/2008, § 103). Leander/İsveç (B. No: 9248/81, 26/3/1987) kararında, başvurucunun bazı mesleki ve sendikal faaliyetlerinin gizli kayıtlarının tutulmasının özel hayatına ilişkin olduğu, bunun yanında söz konusu bilgilerin saklanması ve ifşa edilmesinin özel hayata saygı hakkına bir müdahale teşkil ettiği kabul edilmiştir (Leander/İsveç, § 48). Sõro/Estonya (B. No: 22588/08, 3/9/2015) kararında gizli serviste şoför olarak çalışmış olan başvurucunun mesleki bilgilerinin gazetede yayımlanmasının özel hayata müdahale teşkil ettiği kabul edilmiştir (Sõro/Estonya, § 56). Bu başvuruda AİHM, müdahalenin gözetilen amaçla orantısız olduğu gerekçesiyle Sözleşme'nin 8. maddesinin ihlal edildiğine karar vermiştir (Sõro/Estonya, §§ 56-64).

V. İNCELEME VE GEREKÇE

33. Mahkemenin 10/1/2018 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları

34. Başvurucu, bilgi edinme hakkı çerçevesinde Kurul tarafından mesleki sicil notlarının kendisine "gizli" ve "kişiyeye özel" olarak verilmesine karar verildiğini ifade etmiştir. Başvurucu, mesleki yaşamı ve onurunu etkileyecek nitelikteki belgelerin gizlilik kurallarına uygun olarak kendisine verilmesi gerektiğini öne sürmüştür. Başvurucu, ancak kendisi tarafından öğrenilmesi gereken söz konusu evraka kendisi dışındaki kişiler tarafından da vâkıf olunduğunu belirtmiştir. Başvurucu, bu sebeplerle özel hayata saygı hakkının ihlal edildiğini ileri sürmüştür.

B. Değerlendirme

35. İddianın değerlendirilmesine dayanak alınacak Anayasa'nın 20. maddesi şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

...

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

36. Anayasa'nın 5. maddesinin ilgili kısmı şöyledir:

"Devletin temel amaç ve görevleri, ... Cumhuriyeti ve demokrasiyi korumak, kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak; kişinin temel hak ve hürriyetlerini, sosyal hukuk devleti ve adalet ilkeleriyle bağdaşmayacak surette sınırlayan siyasal, ekonomik ve sosyal engelleri kaldırmaya, insanın maddî ve manevî varlığının gelişmesi için gerekli şartları hazırlamaya çalışmaktır."

1. Uygulanabilirlik Yönünden

37. Özel hayata saygı hakkı kapsamında korunan hukuksal çıkarılardan biri de bireyin mahremiyet hakkıdır. Ancak mahremiyet hakkı sadece yalnız kalma hakkından ibaret olmayıp bu hak, bireyin kendisi hakkındaki bilgileri kontrol edebilme hukuksal çıkarını da kapsamaktadır. Bireyin; kendisine ilişkin herhangi bir bilginin kendi rızası olmaksızın açıklanmaması, yayılmaması, bu bilgilere başkaları tarafından ulaşılamaması ve rızası hilafına kullanılamaması, kısaca bu bilgilerin mahrem kalması konusunda menfaati bulunmaktadır. Bu husus, bireyin kendisi hakkındaki bilgilerin geleceğini belirleme hakkına işaret etmektedir (Serap Tortuk, B. No: 2013/9660, 21/1/2015, §§ 31-32).

Özel hayata saygı hakkının kapsamında olan bireylerin kişisel verilerinin korunması hakkı, Anayasa'nın 20. maddesinde açık olarak düzenlenmiştir.

38. Anayasa Mahkemesi kararlarında da belirtildiği üzere kişisel veri -belirli veya kimliği belirlenebilir olmak şartıyla- bir kişiye ait bütün bilgileri ifade etmekte olup adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgilerin değil telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, öz geçmiş, resim, görüntü ve ses kayıtları, parmak izleri, sağlık bilgileri, genetik bilgiler, IP adresi, e-posta adresi, alışveriş alışkanlıkları, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm verilerdir (AYM, E.2014/74, K.2014/201, 25/12/2014; E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2013/84, K.2014/183, 4/12/2014; E.2014/180, K.2015/30, 19/3/2015; Bülent Kaya [GK], B. No: 2013/2941, 11/5/2016, § 49).

39. Bunun yanı sıra özel hayata saygı hakkı, ilişki kurmak ve geliştirmek üzere çevresinde bulunanlarla temas kurma hakkını da içermektedir. Kişilerin mesleki hayatı özel hayatıyla iç içedir, bu yüzden mesleki hayat çerçevesinde yürütülen faaliyetlerin "özel hayat" kavramı dışında tutulması mümkün değildir (Bülent Polat [GK], B. No: 2013/7666, 10/12/2015, §62; Ata Türkeri, B. No: 2013/6057, 16/12/2015, § 31).

40. Somut olayda MSB Sağlık Dairesi Başkanlığında sivil memur olarak görev yapan başvurucu hakkında sicil amirleri tarafından düzenlenen sicil raporlarının başvurucunun mesleki faaliyetlerine ilişkin olduğu kuşkusuzdur. Danıştay; sicil raporlarının devlet memurlarının o yıl içindeki genel durum ve davranışları bakımından olumlu ve olumsuz niteliklerini, kusur ve eksikliklerini, liyakat durumunu gösteren ve sicil amirlerince not esasına göre düzenlenen belgeler olduğunu tespit etmiştir. Buna göre sicil raporlarında; devlet memurunun dönem içinde disipline riyeti, sorumluluk duygusu, verimlilik ve çalışkanlığı, görevine bağlılığı, iş heyecanı, mesleki bilgisi, tarafsızlığı, iş arkadaşlarına, amirlerine ve iş sahiplerine karşı tutumu gibi konular yer almaktadır (bkz. § 30).

41. Başvurucunun mesleki faaliyetlerinin değerlendirildiği sicil raporlarının belirtilen önemi, taşıdığı mahiyet ve içeriği sebebiyle kişisel veri niteliğinde olduğu tartışma konusu değildir. Kişisel verilerin tutulması, saklanması veya aktarılmasının ise Anayasa'nın 20. maddesi bağlamında kişilerin özel hayatına saygı hakkı kapsamında incelenmesi gerektiği kuşkusuzdur.

2. Kabul Edilebilirlik Yönünden

42. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir nedeni de bulunmadığı anlaşılan özel hayata saygı hakkının ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

3. Esas Yönünden

a. Genel İlkeler

43. Özel hayata saygı hakkına ilişkin negatif ve pozitif yükümlülükleri kesin sınırlarla birbirinden ayırmak mümkün olmayıp her ikisinde de uygulanacak ilkeler benzerdir (N.Ö., B. No: 2014/19725, 19/11/2015, § 53).

44. Anayasa'nın 20. maddesi esas itibarıyla bireyi kamu makamlarının keyfî müdahalesine karşı korumakla birlikte, devletin sadece böyle bir müdahalede bulunmaktan kaçınmasını gerektirmemekte, belirtilen negatif yükümlülüğün yanı sıra özel ve aile yaşamına etkili bir şekilde saygı gösterilmesi noktasındaki pozitif yükümlülükleri de kapsamına almaktadır. Anayasa'nın 20. maddesi, "Devletin temel amaç ve görevleri" kenar başlıklı 5. maddedeki genel yükümlülükle birlikte ele alındığında, belirtilen pozitif yükümlülüklerle işaret etmektedir (Mehmet Arif Kılınç, B. No: 2013/1656, 16/7/2014, § 27; Marcus Frank Cerny [GK], B. No: 2013/5126, 2/7/2015, § 36).

45. Anayasa'nın 20. maddesinin üçüncü fıkrasında ise herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı ifade edilmiştir. Maddede ayrıca kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır (AYM, E.2014/122, K. 2015/123, 30/12/2015, §§ 19-20).

46. Devletin özel hayatın gizliliğinin korunması bağlamında kişisel verilerin yetkisiz kişiler tarafından elde edilmesini veya kullanılmasını önleme ve ayrıca bu verilerin ifşa edilmesini engelleme yükümlülükleri bulunmaktadır. Kamu makamlarınca belirtilen koruma yükümlülüğüne uyulmaması sonucu kişisel verilerin ilgisiz kişilerce öğrenilmesi bireyin özel hayatına saygı hakkının ihlaline yol açar.

b. İlkelerin Olaya Uygulanması

47. Başvuruya konu belgeler, 2003 yılından 2010 yılına kadar olan dönemde başvuru hakkında verilen sicil raporlarıdır. İdare, bilgi edinme hakkı çerçevesinde Kurul kararı gereği bu belgelere başvuru hakkına erişimine izin vermiştir. Yukarıda da değinildiği üzere başvuru hakkında öznel ve nesnel bazı değerlendirmeleri içeren söz konusu raporlardaki bilgiler aynı zamanda kişisel verilerdir (bkz. § 40).

48. Başvurucunun bu verilere erişim talebi idarece reddedilmiş ancak bilgi edinme hakkı çerçevesinde yapılan itiraz neticesinde Kurul, söz konusu sicil raporlarının "gizli" ve "kişiyeye özel" olarak başvuru hakkına verilmesine karar vermiştir. Böylelikle başvuru hakkının belirtilen kişisel verilerine erişiminin engellenmesi yönündeki mağduriyeti giderilmiştir. Bununla birlikte idarece gizlilik derecesi verilen bu sicil raporları "kişiyeye özel" kaydı düşülmediği için bütün aşamalardan -kapalı bir zarf içinde olmaksızın- geçerek başvuru hakkına tebliğ edilmiştir. Bu sebeple AYİM Başsavcılığı tarafından da tespit edildiği üzere "kişiyeye özel" olarak gönderilmeyen sicil raporlarına tebliğ aşamasına kadar geçen sürede başvuru hakkındaki kişilerin de vâkıf olabildikleri anlaşılmaktadır (bkz. §§ 13, 15).

49. Başvuru konusu olayda başvuru hakkının kişisel verileri kapsamındaki mesleki sicil raporlarına erişimi sağlanmış ancak başvuru hakkı bu verilerin kişiyeye özel olarak gönderilmemesinden şikâyetçi olmuştur. Gerçekten de derece mahkemesi, başvuru hakkına ait sicil raporlarının "kişiyeye özel" kaydı olmadan gönderildiğini tespit etmiştir. Hâlbuki bu sicil raporlarının başvuru hakkına verilmesine ilişkin Kurul kararında, evrakın "kişiyeye özel" olarak teslim edilmesi gerektiği belirtilmiş olup resmî yazışma kurallarına ilişkin mevzuatta da bu evrakın nasıl teslim edileceği düzenlenmiştir (bkz. § 29). Bununla birlikte başvuru hakkının özel hayatına yapılan bu müdahaleye ilişkin olarak manevi tazminat istemiyle açtığı davada AYİM, evrakın TSK Karargâh Hizmetleri Yönergesi doğrultusunda yalnızca ilgili kişilerce öğrenildiği gerekçesiyle davanın reddine karar vermiştir.

50. Kamu hizmetlerinin etkin bir şekilde görülebilmesi için kamu personelinin faaliyetlerinin değerlendirildiği sicil raporlarının düzenlenmesi, tutulması ve muhafaza edilmesi kamu yararı bakımından gerekli görülebilir. Bununla birlikte kamu makamlarından çalışanların mesleki faaliyetlerine ilişkin söz konusu bilgilerin tutulması ve saklanması sırasında Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkının korunmasına ilişkin gerekliliklere uygun hareket etmeleri beklenir. Bu bağlamda kamu görevlilerinin haklarında düzenlenen mesleki sicil raporlarının tutulması ve saklanması sırasında gizliliğe riayet edilmesi, bu verilere ilgisiz kişilerin erişiminin engellenmesi gerekmektedir.

51. Kişisel verilerin korunması hususunda Anayasa'nın 20. maddesindeki gereklilikleri sağlamaya yönelik bazı düzenlemelerin mevcut olduğu görülmektedir. Bu kapsamda 4982 sayılı Kanun'un ilgili hükümleri uyarınca bilgi edinme hakkı çerçevesinde kişisel verilere erişimin kolaylaştırılması sağlanmıştır. Nitekim başvuru da bu sayede mesleki faaliyetlerine ilişkin tutulan sicil raporlarına erişebilmiştir. Diğer taraftan 6698 sayılı Kanun ile kişisel verilerin kişilerin açık rızası olmaksızın aktarılamayacağı hüküm altına alınmıştır. Ayrıca Türk Silahlı Kuvvetlerinde Görevli Sivil Memurlara Sicil Raporu Vermeye Yetkili Amirler Yönetmeliği'nin 8. maddesinde, Silahlı Kuvvetlerde görevli memurların sicil dosyalarının bağlı oldukları kuruluşun Personel Daire Başkanlığı Sivil Memurlar Şube Müdürlüklerinde muhafaza edileceği düzenlenmiştir. Nihayet 2 Seri No.lu Kamu Personeli Genel Tebliği'nin (D) bendinin (9) numaralı alt bendinde, özlük dosyalarının tutulması ve muhafazasında özel hayatın gizliliği ilkesine riayet edileceği düzenlenmiştir.

52. Somut olayda ise başvuru kişinin mesleki hayatına ilişkin önemli bilgileri içeren sicil raporlarının sicil dosyalarının muhafaza edildiği Personel Dairesi Başkanlığından başvuru kişinin görev yaptığı Sağlık İşleri Dairesi Başkanlığına "kişiyeye özel" evrak tasnifi yapılmadan gönderildiği anlaşılmaktadır. Her ne kadar AYİM kararında, yalnızca yönergede belirtilen kişilerce evrakın öğrenildiği gerekçesine dayanılmış ise de kişiyeye özel olarak gönderilmediği için bu evrakın başvurucuya tebliğ edildiği ana kadar bütün aşamalarda ilgili olmayan kişilerce de öğrenilebilmesinin mümkün kılındığı açıktır.

53. Bunun yanında başvuru kişinin bilgilerinin yalnız kamuya açık olmaması değil aynı zamanda kurum içinde de mümkün olduğunca gizli tutulması önem taşımaktadır. Nitekim söz konusu evrakın tutulmasına ilişkin kurallar gözetildiğinde ilgili olmayan personelin başvuru kişiyle aynı birimde görev yapsa dahi bu evrakı öğrenmesine lüzum da bulunmamaktadır. Kaldı ki resmî yazışma kurallarına göre, bu gibi belgelerin gizlilik kuralları çerçevesinde başvurucuya teslim edilebilmesi kolaylıkla mümkün görülmektedir. Ayrıca aynı düzenlemede "kişiyeye özel" ibaresi taşıyan belge üzerinde yalnızca ilgili kişinin tasarruf hakkına sahip olduğu da belirtilmiştir (bkz. § 29). Bu bağlamda Personel Dairesi Başkanlığınca "kişiyeye özel" kaydı düşülerek gönderilmesi durumunda sicil raporlarının kapalı bir zarf içinde başvurucuya tebliğ edilebileceği dikkate alınmalıdır. Buna karşın dosya kapsamına göre, sicil raporlarının başvurucuya kişiyeye özel olarak gönderilmediği ve kapalı bir zarf içinde tebliğ edilmediği açıkça ortadadır.

54. Sonuç olarak başvuru kişinin mesleki faaliyetlerine ilişkin önemli bilgileri içeren sicil raporlarının başkalarına öğrenilebilmesinin mümkün kılındığı anlaşıldığından somut olayda devletin özel hayata saygı hakkı kapsamında kişisel verilerin korunmasına ilişkin pozitif yükümlülüklerinin yerine getirilmediği anlaşılmaktadır.

55. Açıklanan nedenlerle Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkının ihlal edildiğine karar verilmesi gerekir.

C. 6216 Sayılı Kanun'un 50. Maddesi Yönünden

56. 30/3/2011 tarihli ve 6216 sayılı Kanun'un 50. maddesinin (1) ve (2) numaralı fıkraları şöyledir:

“(1) Esas inceleme sonunda, başvuru hakkının ihlal edildiğine ya da edilmediğine karar verilir. İhlal kararı verilmesi hâlinde ihlalin ve sonuçlarının ortadan kaldırılması için yapılması gerekenlere hükmedilir...

(2) Tespit edilen ihlal bir mahkeme kararından kaynaklanmışsa, ihlali ve sonuçlarını ortadan kaldırmak için yeniden yargılama yapmak üzere dosya ilgili mahkemeye gönderilir. Yeniden yargılama yapılmasında hukuki yarar bulunmayan hâllerde başvuru lehine tazminata hükmedilebilir veya genel mahkemelerde dava açılması yolu gösterilebilir. Yeniden yargılama yapmakla yükümlü mahkeme, Anayasa Mahkemesinin ihlal kararında açıkladığı ihlali ve sonuçlarını ortadan kaldıracak şekilde mümkünse dosya üzerinden karar verir.”

57. Başvuru, yeniden yargılama ve manevi tazminat talebinde bulunmuştur.

58. Somut olayda özel hayata saygı hakkının ihlal edildiği sonucuna varılmıştır.

59. Özel hayata saygı hakkının ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmasında hukuki yarar bulunduğundan kararın bir örneğinin yeniden yargılama yapılmak üzere AYİM İkinci Dairesine (Anayasa'nın 21/1/2017 tarihli ve 6771 sayılı Kanun ile getirilen geçici 21. maddesinin birinci fıkrasının(E) bendi uyarınca Askeri Yüksek İdare Mahkemesi kaldırılmış olduğundan anılan bendin (b) alt bendi gereğince belirlenecek görevli ve yetkili idare mahkemesine) gönderilmesine karar verilmesi gerekir.

60. Yeniden yargılama yapılmak üzere dosyanın yetkili yargı merciine gönderilmesine karar verilmesinin ihlal sonucu açısından yeterli bir giderim sağladığı anlaşıldığından başvuru tazminat taleplerinin reddine karar verilmesi gerekir.

61. Dosyadaki belgelerden tespit edilen 206,10 TL harçtan oluşan yargılama giderinin başvurucuya ödenmesine karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Başvurunun KABUL EDİLEBİLİR OLDUĞUNA,

B. Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkının İHLAL EDİLDİĞİNE,

C. Kararın bir örneğinin özel hayata saygı hakkının ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmak üzere Askeri Yüksek İdare Mahkemesi İkinci Dairesine (Anılan Dairenin 18/6/2014 tarihli ve E.2014/1084, K.2014/1007 sayılı kararına ait dava dosyası ile ilgilidir.) (Anayasa'nın 21/1/2017 tarihli ve 6771 sayılı Kanun ile getirilen geçici 21. maddesinin birinci fıkrasının (E) bendi uyarınca Askeri Yüksek İdare Mahkemesi kaldırılmış olduğundan anılan bendin (b) alt bendi gereğince belirlenecek görevli ve yetkili idare mahkemesine) GÖNDERİLMESİNE,

D. Başvurucunun tazminat taleplerinin REDDİNE,

E. 206,10 TL harçtan oluşan yargılama giderinin BAŞVURUCUYA ÖDENMESİNE,

F. Ödemenin kararın tebliğini takiben başvurucunun Maliye Bakanlığına başvuru tarihinden itibaren dört ay içinde yapılmasına, ödemede gecikme olması hâlinde bu sürenin sona erdiği tarihten ödeme tarihine kadar geçen süre için yasal FAİZ UYGULANMASINA,

G. Kararın bir örneğinin Adalet Bakanlığına GÖNDERİLMESİNE 10/1/2018 tarihinde OYBİRLİĞİYLE karar verildi.

Anayasa Mahkemesi - Fatih Saraman Kararı (2014/7256)

Fatih Saraman [GK], B. No: 2014/7256, 27/2/2019

Başvuru, kanunen verilmemesi gereken kişisel verinin idari makamlara açıklanması ve güvenlik soruşturmasına esas alınması nedeniyle özel hayata saygı hakkının ihlal edildiği iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

GENEL KURUL

KARAR

FATİH SARAMAN BAŞVURUSU

(Başvuru Numarası: 2014/7256)

Karar Tarihi: 27/2/2019

R.G. Tarih ve Sayı: 27/3/2019 - 30727

GENEL KURUL

KARAR

Başkan:

Zühtü ARSLAN

Başkanvekili: Burhan ÜSTÜN

Başkanvekili: Engin YILDIRIM

Üyeler: Serdar ÖZGÜLDÜR, Serruh KALELİ, Recep KÖMÜRCÜ, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ, Yıldız SEFERİNOĞLU

Raportörler: Şermin BİRTANE; Hikmet Murat AKKAYA

Başvurucu: Fatih SARAMAN

Vekili: Av. Mustafa BALABAN

I. BAŞVURUNUN KONUSU

1. Başvuru, kanunen verilmemesi gereken kişisel verinin idari makamlara açıklanması ve güvenlik soruşturmasına esas alınması nedeniyle özel hayata saygı hakkının ihlal edildiği iddiasına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 21/5/2014 tarihinde yapılmıştır.

3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.

4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.

5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.

6. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık görüşünü bildirmiştir.

7. Başvurucu, Bakanlık görüşüne karşı beyanda bulunmamıştır.

8. İkinci Bölüm tarafından 8/11/2017 tarihinde yapılan toplantıda, niteliği itibarıyla Genel Kurul tarafından karara bağlanması gerekli görüldüğünden başvurunun Anayasa Mahkemesi İçtüzüğü'nün 28. Maddesinin (3) numaralı fıkrası uyarınca Genel Kurula sevkine karar verilmiştir.

III. OLAY VE OLGULAR

9. Başvuru formu ve eklerinde ifade edildiği şekliyle olaylar özetle şöyledir:

10. Başvurucu 19/11/1983 tarihinde doğmuştur. Adana 4. Asliye Ceza Mahkemesinin 13/3/2002 tarihli kararı ile başvurucunun hırsızlık suçu nedeniyle 5 ay hapis cezası ile cezalandırılmasına hükmedilmiş, hapis cezası ağır para cezasına çevrilmiş ve ceza ertelenmiştir. Başvurucunun suçu işlediği tarihte on sekiz yaşından küçük olduğu anlaşılmaktadır.

11. Adalet Bakanlığı Ceza ve Tevkifevleri (CTE) Genel Müdürlüğünün 10/6/2009 tarihli yazısıyla Kocaeli 1 ve 2 No'lu F Tipi Kapalı Ceza İnfaz Kurumları ile Kocaeli 1 ve 2 No'lu T Tipi Kapalı Ceza İnfaz Kurumlarına sözleşmeli infaz ve koruma memurluğu alımı için sınav yapılmıştır. Sınavla 501 kişinin işe alınması planlanmıştır.

12. Atama yapılmak üzere verilen sınav izni ile Kocaeli Adli Yargı İlk Derece Mahkemesi Adalet Komisyonu (Komisyon) Başkanlığı tarafından yapılan yazılı ve sözlü sınavlar sonucunda başvuru nihai başarı listesininin 300. Sırasında yer almaktadır. İnfaz ve koruma memurluğuna yerleştirilmesi

düşünülen başvurucu hakkında Komisyon Başkanlığınca güvenlik soruşturması işlemlerine başlanmıştır.

13. Adana Valiliği Emniyet Müdürlüğü tarafından Komisyon Başkanlığına hitaben yazılan 10/9/2009 tarihli yazıda, başvurucu hakkında istenen güvenlik soruşturması ve arşiv araştırması sonucunda hırsızlık suçundan işlem yapıldığının tespit edildiği bildirilmiş ve yazı ekinde Adana 4. Asliye Ceza Mahkemesinin 13/3/2002 tarihli kararı gönderilmiştir.

14. Komisyon Başkanlığı tarafından CTE Genel Müdürlüğüne gönderilen 9/10/2009 tarihli yazıda, hırsızlık suçu nedeniyle başvurucunun devlet memurluğuna atanacaklarda aranan şartları taşımadığı belirtilerek sözleşmeli infaz ve koruma memuru olarak istihdam edilmesinin uygun olmayacağı görüşü bildirilmiştir.

15. Başvurucu 7/12/2009 tarihli Bilgi Edinme Başvuru Formu ile hakkında yapılan güvenlik soruşturmasının sonucunun kendisine iletilmesini talep etmiştir.

16. CTE Genel Müdürlüğünün 16/12/2009 tarihli cevabında, başvurucunun 10/7/2003 tarihli ve 25164 sayılı Resmî Gazete’de yayımlanan Adalet Bakanlığı Memur Sınav, Atama ve Nakil Yönetmeliği’nin “Özel şartlar” kenar başlıklı 6. Maddesinin (5) numaralı bendinin (d) alt bendinde öngörülen “güvenlik soruşturması olumlu olmak” şartını taşıması nedeniyle atamasının yapılmadığı bildirilmiştir.

17. Bunun üzerine başvurucu tarafından 4/2/2010 tarihinde, atama işleminin yapılmaması nedeniyle Ankara 4. İdare Mahkemesinde iptal davası açılmıştır.

18. Mahkeme 14/12/2010 tarihli kararıyla davayı reddetmiştir. Kararda ceza infaz kurumları ile tutukevlerinde çalıştırılacak personel hakkında güvenlik soruşturması ve arşiv araştırması yapılmasının zorunlu olduğu, ceza infaz kurumu infaz ve koruma memurluğu görevinin önem ve özelliği gözetildiğinde hırsızlık suçundan mahkûm olması nedeniyle güvenlik soruşturması sonucu olumsuz olan başvurucunun atanmamasına ilişkin işlemde hukuka aykırılık bulunmadığı belirtilmiştir.

19. Başvurucunun temyiz istemi Danıştay Onikinci Dairesinin 10/12/2013 tarihli kararıyla reddedilerek hüküm onanmıştır.

20. Anılan karar 21/4/2014 tarihinde başvurucuya tebliğ edilmiştir.

21. Başvurucu 21/5/2014 tarihinde bireysel başvuruda bulunmuştur.

22. Başvurucu, bireysel başvuru yaptıktan sonra Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğünden temin ettiği 23/11/2017 tarihli adli sicil kaydı ile adli sicil arşiv kaydı sorgulaması sonuçlarını Anayasa Mahkemesine sunmuştur. Söz konusu belgelerde, belgelerin verileceği yer olarak kurum türü kısmına resmî kurumlara, belgenin konu kısmına ise devlet memurluğu için olduğu yazılmış; başvurucaunun adli sicil ve arşiv kaydının bulunmadığı belirtilmiştir.

23. Ayrıca İçişleri Bakanlığı Kaçakçılık, İstihbarat, Harekat ve Bilgi Toplama Dairesi Başkanlığı tarafından gönderilen 16/11/2017 tarihli yazıda başvuruca hakkında genel bilgi toplama (GBT) kaydı bulunmadığı bildirilmiştir.

24. Bunun yanı sıra Anayasa Mahkemesince Adana İl Emniyet Müdürlüğünden Adana 4. Asliye Ceza Mahkemesinin 13/3/2002 tarihli, başvuruca hakkındaki kararının nasıl ve nereden tespit edildiği sorulmuştur. Adana Valiliği Emniyet Müdürlüğünün 2/5/2018 tarihinde kayda alınan cevabında, kayıtlarının tetkikinden başvuruca hakkında hırsızlık suçu nedeniyle hazırlık tahkikatı yapılmış olduğunun anlaşıldığı, bunun üzerine Adana Cumhuriyet Başsavcılığı ile yapılan yazışma sonucunda söz konusu mahkeme kararının temin edildiği bildirilmiştir.

25. Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğünün 11/6/2018 tarihli yazısında 25/5/2005 tarihli ve 5352 sayılı Adli Sicil Kanunu'nun 10. Maddesinin üçüncü fıkrası hükmü dikkate alındığında on sekiz yaşından küçükken işlenen suçlara dair kayıtların kamu görevlerine yapılacak atamalar dolayısıyla güvenlik soruşturması kapsamında ilgili kamu kurumlarına verilemeyeceği bildirilmiştir.

IV. İLGİLİ HUKUK

A. Ulusal Hukuk

26. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Özel nitelikli kişisel verilerin işleme şartları" kenar başlıklı 6. Maddesinin ilgili kısmı şöyledir:

"(1)Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir..."

27. 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu'nun 48. Maddesinin ilgili kısmı şöyledir:

"Devlet memurluğuna alınacaklarda aşağıdaki genel ve özel şartlar aranır.

G) Genel şartlar:

Türk Ceza Kanununun 53 üncü maddesinde belirtilen süreler geçmiş olsa bile; kasten işlenen bir suçtan dolayı bir yıl veya daha fazla süreyle hapis cezasına ya da affa uğramış olsa bile ... hırsızlık, ... suçlarından mahkûm olmamak.

...

8. (Ek: 3/10/2016 - KHK-676/74 md.; Aynen kabul: ½/2018-7070/60 md.) Güvenlik soruşturması ve/veya arşiv araştırması yapılmış olmak.

B) Özel şartlar:

...

2. Kurumların özel kanun veya diğer mevzuatında aranan şartları taşımak.”

28. Adalet Bakanlığı Memur Sınav, Atama ve Nakil Yönetmeliği'nin “Özel şartlar” kenar başlıklı 6. Maddesinin ilgili kısmı şöyledir:

“Genel şartların yanında, atama yapılacak kadroların niteliğine göre aşağıdaki şartlar aranır:

...

5) Koruma güvenlik görevlisi ile infaz ve koruma memuru kadrolarına atanabilmek için;

...

d) Güvenlik soruşturması olumlu olmak”

29. 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 53. Maddesinin ilgili kısmı şöyledir:

“(1) Kişi, kasten işlemiş olduğu suçtan dolayı hapis cezasına mahkûmiyetin kanuni sonucu olarak;

G) Sürekli, süreli veya geçici bir kamu görevinin üstlenilmesinden; ... atamaya veya seçime tabi bütün memuriyet ve hizmetlerde istihdam edilmekten,

...

Yoksun bırakılır.

...

(4) ... fiili işlediği sırada onsekiz yaşını doldurmamış olan kişiler hakkında birinci fıkra hükmü uygulanmaz.”

30. 25/5/2005 tarihli ve 5352 sayılı Adli Sicil Kanunu'nun “Amaç ve kapsam” kenar başlıklı 1. Maddesi şöyledir:

“Bu Kanun, kesinleşmiş ceza ve güvenlik tedbirlerine mahkûmiyete ilişkin bilgilerin otomatik işleme tâbi bir sistem kullanılarak toplanmasına, sınıflandırılmasına, değerlendirilmesine, muhafaza edilmesine ve gerektiğinde en seri ve sağlıklı biçimde ilgililere bildirilmesine dair usul ve esasları belirler.”

31. 5352 sayılı Kanun’un “Arşiv bilgilerinin istenmesi” kenar başlıklı 10. Maddesinin (3) numaralı fıkrası şöyledir:

“Onsekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebilir.”

32. 7/9/2005 tarihli ve 25929 sayılı Resmî Gazete’de yayımlanan Adli Sicil Yönetmeliği’nin 12. Maddesinin dördüncü fıkrası şöyledir:

“Onsekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere mahkeme, hâkim veya savcılıklarca istenebilir.”

33. Adli Sicil Yönetmeliği’nin “Adlî sicil bilgilerinin sınırlı olarak verilebileceği haller” kenar başlıklı 14. Maddesinin birinci fıkrası şöyledir:

“Onsekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere mahkeme, hâkim veya savcılıklara talep halinde verilir.”

34. Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü tarafından çıkarılan 1/1/2006 tarihli ve 55 sayılı Genelge’nin ilgili kısmı şöyledir:

“Adlî sicil kayıtlarının şahsi başvurularda ilgilisi dışındaki kişilere verilmemesi gerektiği hususunda, Genel Müdürlüğümüzde düzenlenen hizmet içi eğitim kurslarında üzerinde önemle durulmasına ve tüm uyarılara rağmen konuya gereken özen ve hassasiyet gösterilmeyerek, ilgilisi dışındaki şahıslara adlî sicil kaydı verilmek suretiyle yer yer şikayetlere sebebiyet verildiği müşahede olunmuştur.

...

Bu itibarla;

G) Haklarında mahkemelerce mülga 2253 sayılı Kanunun 12 nci veya mülga 765 sayılı Kanunun 55 inci maddeleri ile 5237 sayılı TCK’nun 31 inci maddesi uygulanan onsekiz yaşından küçükler hakkında adlî sicil ve arşiv kayıtlarının; ancak, soruşturma ve kovuşturma kapsamında değerlendirilmek üzere mahkeme, hâkim veya savcılıklarca istenildiği takdirde verilmesi hususunda

gereken tüm tedbirlerin alınması, konu ile ilgili olarak adlî sicil görevlilerinin bilgilendirilerek uyarılması

..."

35. 26/10/1994 tarihli ve 4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun'un 1. Maddesi şöyledir:

"Güvenlik Soruşturması ve Arşiv Araştırması; kamu kurum ve kuruluşlarında, yetkili olmayan kişilerin bilgi sahibi olmaları halinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile askeri, emniyet ve istihbarat teşkilatlarında çalıştırılacak kamu personeli ve ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında yapılır.

Devletin güvenliğini, ulusun varlığını ve bütünlüğünü iç ve dış menfaatlerinin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeler ile gizlilik dereceli kamu personeli ile meslek gruplarının tespiti, birim ve kısımların tanımlarının yapılması, güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak merciler ve üst kademe yöneticilerinin kimler olduğu Bakanlar Kurulu Kararı ile yürürlüğe konulacak yönetmelik ile düzenlenir."

36. 12/4/2000 tarihli ve 24018 sayılı Resmî Gazete'de yayımlanan Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği'nin (Yönetmelik) "Güvenlik soruşturması ve arşiv araştırması yapacak makamlar" kenar başlıklı 7. Maddesi şöyledir:

"Güvenlik soruşturması ve arşiv araştırması, Milli İstihbarat Teşkilatı Müsteşarlığı, Emniyet Genel Müdürlüğü ve mahalli mülki idare amirlikleri tarafından yapılır.

İçişleri Bakanlığı Kaçakçılık İstihbarat Harekat ve Bilgi Toplama Dairesi Başkanlığı'ndaki bilgi kayıtları ile Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü'ndeki adli sicil kaydı, talepleri üzerine, güvenlik soruşturması ve arşiv araştırmasını yapacak makamlar ile Türk Silahlı Kuvvetlerinin ilgili birimlerine verilir."

37. Yönetmeliğin "Hakkında güvenlik soruşturması ve arşiv araştırması yapılacak personel" kenar başlıklı 8. Maddesinin birinci ve ikinci fıkraları şöyledir:

"Güvenlik soruşturması ve arşiv araştırması; gizlilik dereceli birim ve kısımlar ile askeri, emniyet, istihbarat teşkilatlarında ve ceza infaz kurumları ve tutukevlerinde çalıştırılacak personel hakkında yapılır.

Emniyet Genel Müdürlüğü ve mahalli mülki idare amirlikleri, güvenlik soruşturması ve arşiv araştırmasını; bakanlıklar, kamu kurum ve kuruluşlarının gizlilik dereceli birim ve kısımları ile yurtdışı teşkilatında ve askeri, emniyet, istihbarat teşkilatlarında ve ceza infaz kurumu ve tutukevlerinde çalıştırılacak personel hakkında yapar.”

38. Yönetmeliğin “Güvenlik soruşturması ve arşiv araştırmasında araştırılacak hususlar” kenar başlıklı 11. Maddesi şöyledir:

“Güvenlik soruşturması ve arşiv araştırmasında kişinin içinde bulunduğu ortam da dikkate alınarak:

a) Kimlik kontrolü, kimlik kayıtlarının doğruluk derecesi, uyrukluđu, geçmişte yabancı bir devletin uyrukluđuna girip girmediđi,

b) Kolluk kuvvetleri tarafından halen aranıp aranmadıđı, kolluk kuvvetlerinin ve istihbarat ünitelerinin arşivlerinde bilgiler bulunup bulunmadıđı, adli sicil kaydının ve hakkında bir tahdidin olup olmadıđı,

c) Yıkıcı faaliyetlerde bulunup bulunmadıđı ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanuna ve Atatürk ilke ve inkılaplarına aykırı davranıp davranmadıđı.

d) Şeref ve haysiyetini ihlal edecek ve görevine yansıyacak şekilde kumara, uyuşturucuya, içkiye, paraya ve aşırı bir şekilde menfaatine düşkün olup olmadıđı, ahlak ve adaba aykırı davranıp davranmadıđı,

e) Yabancılarla, özellikle hasım ve hasım olması muhtemel Devlet mensupları ve temsilcileriyle ilgili derecesinin iç yüzü ve nedeni,

f) Sır saklama yeteneđinin olup olmadıđı,

araştırılır.”

39. Devlet Personel Başkanlığının 26/8/2013 tarihli ve 13899 sayılı, üniversitede araştırma görevlisi olarak çalışan, adli sicil kaydı bulunmayan ancak küçük yaşta işlediđi suçlardan dolayı 3 yıl 1 ay 15 gün ve 1 yıl 10 ay 15 gün hapis cezası ile tecziye edilen personelin 657 sayılı Kanun’un 48. Maddesinin birinci fıkrasının (A) bendinin (5) numaralı alt bendi çerçevesinde görevine devam edip edemeyeceđi hususunda verdiđi görüşün ilgili kısmı şöyledir:

“25/5/2005 tarihli ve 5352 sayılı Adli Sicil Kanununun 10 uncu maddesinde; ...Onsekiz yaşından küçüklerle ilgili adli sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebilir.”
Hükmüne yer verilmek suretiyle, kamu kurumlarının özel kanunlarda gösterilen hallerde (657 sayılı

Kanunun 48/A-5 maddesi gereği) ilgililerin adli sicil arşiv bilgilerini isteyebileceği, ancak suçun işlendiği tarihte 18 yaşından küçük olanlarla ilgili adli sicil ve arşiv kayıtlarını sadece soruşturma ve kovuşturma kapsamında Cumhuriyet başsavcılıkları, hâkim veya mahkemelerin isteyebileceği, bunun dışındaki resmi veya özel kuruluşların 18 yaşından küçüklerle ilgili adli sicil ve arşiv kayıtlarını istemesinin ve bunlara istinaden işlem tesis etmesinin mümkün olmadığı belirtilmiş; bir başka anlatımla kamu kurumları açısından 18 yaşından küçüklerle ilgili adli sicil ve arşiv kayıtları bir bakıma hükmen yok sayılmıştır. Bu kapsamda, söz konusu mahkumiyetin 657 sayılı Kanunun 48/A-5 maddesi kapsamında memuriyete engel teşkil etmesi mümkün bulunmamaktadır...”

40. Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğünün 11/6/2018 tarihli yazısının ilgili kısmı şöyledir:

“...Adli Sicil Yönetmeliğinin ‘Adlî sicil bilgilerinin sınırlı olarak verilebileceği haller’ kenar başlıklı 14 üncü maddesinin birinci fıkrasında; ‘Onsekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere mahkeme, hâkim veya savcılıklara talep halinde verilir.’ Genel Müdürlüğümüz tarafından çıkarılan 1/1/2006 tarihli ve 55 sayılı Genelgenin ilgili kısmında; ‘Adlî sicil kayıtlarının şahsi başvurularda ilgilisi dışındaki kişilere verilmemesi gerektiği hususunda, Genel Müdürlüğümüzde düzenlenen hizmet içi eğitim kurslarında üzerinde önemle durulmasına ve tüm uyarılara rağmen konuya gereken özen ve hassasiyet gösterilmeyerek, ilgilisi dışındaki şahıslara adlî sicil kaydı verilmek suretiyle yer yer şikayetlere sebebiyet verildiği müşahede olunmuştur’ ...denilmektedir...”

Bu itibarla; ...on sekiz yaşından küçükken işlenen suçlara dair kayıtların kamu görevlerine yapılacak atamalar dolayısıyla güvenlik soruşturması kapsamında ilgili kamu kurumlarına verilemeyeceği hususunu bilgilerinize arz ederim.”

B. Uluslararası Hukuk

1. Uluslararası Belgeler

41. 18/2/2016 tarihli ve 29628 sayılı Resmî Gazete’de yayımlanan, 30/1/2016 tarihli ve 6669 sayılı Kanun’la uygun bulunan 28/1/1981 tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi’nin “Özel veri kategorileri” kenar başlıklı 6. Maddesi şöyledir:

“İç hukukta uygun güvenceler sağlanmadıkça, ırksal kökeni, siyasi düşünceleri, dini veya diğer inançları ortaya koyan kişisel veriler ile sağlık veya cinsel hayatla ilgili kişisel veriler otomatik işleme tabi tutulmaz. Aynı durum ceza mahkumiyetiyle ilgili kişisel veriler için de geçerlidir.”

42. Birleşmiş Milletler Genel Kurulu tarafından 20/11/1989 tarihinde kabul edilen ve Türkiye tarafından imzalanarak 9/12/1994 tarihli ve 4058 sayılı Kanun'la uygun bulunan Çocuk Haklarına Dair Sözleşme'nin 3. Maddesinin birinci fıkrası şöyledir:

"Kamusal ya da özel sosyal yardım kuruluşları, mahkemeler, idari makamlar veya yasama organları tarafından yapılan ve çocukları ilgilendiren bütün faaliyetlerde, çocuğun yararı temel düşüncedir."

2. Avrupa İnsan Hakları Sözleşmesi ve Avrupa İnsan Hakları Mahkemesi İçtihadı

43. Avrupa İnsan Hakları Sözleşmesi'nin (Sözleşme) "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. Maddesi şöyledir:

"(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."

44. Avrupa İnsan Hakları Mahkemesi (AİHM), devletlerin millî güvenliğin korunması amacını gerçekleştirmede sahip oldukları takdir yetkisinin geniş olduğunu kabul etmektedir. AİHM, Sözleşme'ye taraf devletlerin millî güvenliği korumak için yetkili ulusal makamlarına ilk olarak kişiler hakkında bilgi toplama ve halka açık olmayan siciller tutma, ikinci olarak millî güvenlik bakımından önemli kadrolarda çalışmak isteyen adayların bu işe uygunluğunu takdir ederken bu bilgiyi kullanma yetkisi veren kurallara sahip olmaları gerektiğinde kuşku bulunmadığını belirtmektedir (Leander/İsveç, B. No: 9248/81, 26/03/1987, § 59).

45. Bununla birlikte AİHM içtihadına göre kamu mercilerinin bir bireyin özel hayatıyla ilgili bilgileri toplaması, kaydetmesi, saklaması özel hayata saygı hakkına müdahale oluşturur (Leander/İsveç, § 48; Kopp/İsviçre, B. No: 23224/94, 25/3/1998, § 53; Amann/İsviçre [BD], B. No: 27798/95, 16/2/2000, § 69; Rotaru/Romanya [BD], B. No: 28341/95, 4/5/2000, §§43, 44, 46).

46. AİHM'e göre bir kişinin özel yaşamına ilişkin verilerin kaydedilmesi ve saklanması, kendi başına özel hayata saygı hakkı bakımından bir müdahale oluşturmaktadır. Bu müdahalenin tespiti için kaydedilen bilgilerin daha sonra kullanılmış olması gibi bir koşul da aranmamaktadır. Bununla birlikte kamu makamları tarafından muhafaza edilen kişisel verilerin Sözleşme'nin 8. Maddesinde öngörülen unsurlardan birini devreye sokup sokmadığını tespit etmek için bu bilgilerin hangi çerçevede alındığının ve muhafaza edildiğinin, verilerin türünün, kullanıldığı ve işlendiği şeklin,

bunlardan çıkarılabilecek sonuçların dikkate alınması zaruridir (S.ve Marper/Birleşik Krallık [BD], B. No: 30562/04, 30566/04, 4/12/2008, § 67).

47. AİHM'e göre kişisel verilerin korunması, kişinin Sözleşme'nin 8. Maddesinde öngörülen özel hayata saygı hakkından yararlanması konusunda büyük öneme sahiptir. İç hukuk, kişisel verilerin bu maddede öngörülen güvencelere uygun olmayan şekilde kullanımını engellemek için gerekli güvenceleri sağlamalıdır. Bu tür güvencelerin bulunmasının gerekliliği, otomatik işleme tabi tutulan kişisel verilerin korunması söz konusu olduğunda özellikle de bu verilerin polis tarafından kullanılması hâlinde daha fazla hissedilmektedir. İç hukuk, bu verilerin saklanma amaçlarına uygun ve aşırıktan uzak olmasını sağlamalı; verilerin kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde muhafaza edilmesini temin etmelidir. İç hukuk, aynı zamanda kişisel verilerin uygun olmayan şekillerde, keyfi ve yetki aşımı yapılarak kullanılmasına karşı uygun güvenceler de içermelidir (S.ve Marper/Birleşik Krallık, § 103; M.M./Birleşik Krallık, B. No: 24029/07,13/11/2012, § 195).

48. Ayrıca AİHM, kişilerin suç kayıtlarının tutulması ve kullanılması hakkında konuyu düzenleyen ilgili kanunun niteliğine ayrı bir önem vermektedir. AİHM, suç kayıtlarının tutulması ve kullanılmasına dair kanunun niteliği bakımından aynı telefon dinlemelerinde, gizli takipte ve gizli istihbarat toplamada dayanan kanunlar yönünden olduğu gibi keyfi müdahalelere karşı bireyi korumak amacıyla yüksek bir standart aramaktadır. AİHM'e göre suç kayıtlarının tutulması ve kullanılmasına dair kanun; tıpkı telefon dinlemelerinde, gizli takipte ve gizli istihbarat toplamada olduğu gibi tedbirlerin kapsamını ve uygulanmasını düzenleyen, özellikle süre, stoklama, kullanım, üçüncü kişilerin veriye erişimi, verilerin gizliliği ve bütünlüğünün korunmasına, bunların imhasına ilişkin prosedürlere dair ve kişilerin yetki aşımı ve keyfilığe karşı yeteri kadar güvenceye sahip olmalarını sağlayacak, açık ve detaylı hükümler içermelidir (S.ve Marper/Birleşik Krallık, § 99; M.M./Birleşik Krallık, § 195).

V. İNCELEME VE GEREKÇE

49. Mahkemenin 27/2/2019 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları ve Bakanlık Görüşü

50. Başvurucu, on sekiz yaşını doldurmayanların küçük olmalarından dolayı bazı hatalar yapabileceğinin kanun koyucu tarafından öngörüldüğünü ve bu hataların onların gelecekteki yaşamlarını etkilememesi için 5352 sayılı Kanun'un 10. Maddesinin üçüncü fıkrasında yer alan düzenlemenin getirildiğini belirtmiştir. Başvurucu, idarenin 5352 sayılı Kanun'un 10. Maddesinin

üçüncü fıkrasındaki düzenlemeye aykırı olarak on sekiz yaşından küçükken işlediği suçun kayıtlarına ulaştığını ve böylelikle özel hayatın gizliliğinin ihlal edildiğini, devlet memuru olarak çalışma hakkının da elinden alındığını ifade etmiştir. Bu nedenlerle başvuru özel hayata saygı ve çalışma haklarının ihlal edildiğini ileri sürmüştür.

51. Bakanlık görüşünde; başvurunun esası yönünden yapılan değerlendirmede 4045 sayılı Kanun'un 1. Maddesi doğrultusunda güvenlik soruşturması ve arşiv araştırması yapıldığı, anılan Kanun'un 1. Maddesinin ikinci fıkrasına dayanılarak yürürlüğe konan Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği'nde güvenlik soruşturması ve arşiv araştırmasının nasıl yapılacağı belirlendiği, bu çerçevede müdahalenin hukukilik unsurunu taşıdığı belirtilmiştir. Diğer taraftan atanmak istenen görevin nitelikleri ve hassasiyeti dikkate alındığında güvenlik araştırması yapılması konusunda meşru amacın olduğu, bu uygulamanın demokratik toplum gereklerine aykırı bir yönünün bulunmadığı ifade edilmiştir.

52. Başvuru, Bakanlık görüşüne karşı beyanda bulunmamıştır.

B. Değerlendirme

53. Anayasa'nın 20. Maddesinin ilgili kısmı şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

...

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

54. Özel hayata saygı hakkı kapsamında korunan hukuki menfaatlerden biri de bireyin mahremiyet hakkıdır. Mahremiyet hakkı bireyin kendisi hakkındaki bilgileri kontrol edebilme hukuksal çıkarını da kapsamaktadır. Kendisine ilişkin herhangi bir bilginin rızası olmaksızın açıklanmaması, yayılmaması, bu bilgilere başkaları tarafından ulaşılamaması ve rızası hilafına kullanılmaması, kısaca bu bilgilerin mahrem kalması konusunda bireyin menfaati bulunmaktadır. Bu husus, bireyin kendisi hakkındaki bilgilerin geleceğini belirleme hakkına işaret etmektedir (Serap Tortuk, B. No: 2013/9660, 21/1/2015, § 32).

55. Anayasa'nın özel hayata saygı hakkını düzenleyen 20. Maddesinin üçüncü fıkrasında, herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme, bu veriler hakkında bilgilendirilme, verilere erişme, bunların düzeltilmesini veya silinmesini talep etme, verilerin amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkına sahip olduğu, kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hükmüne yer verilerek anayasal sınırlar belirlenmiştir.

56. Söz konusu Anayasa hükmünde kişilerin kendileri hakkındaki verilerin amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkına sahip olduğu özellikle vurgulanmıştır.

57. Anayasa Mahkemesi tarafından kişisel veri kavramının -belirli veya kimliği belirlenebilir olmak şartıyla- bir kişiye ilişkin bütün bilgileri ifade ettiği kabul edilmektedir (AYM, E.2014/74, K.2014/201, 25/12/2014; E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2013/84, K.2014/183, 4/12/2014; E.2014/180, K.2015/30, 19/3/2015; Bülent Kaya [GK], B. No. 2013/2941, 11/5/2016, § 49). Bu bağlamda ceza mahkûmiyeti ile ilgili verilerin kişisel veri olduğu açıktır. Başvurucu devlet memuru olarak atanmadığını belirterek çalışma hakkının da ihlal edildiğini ileri sürmüştü de atama işleminin yapılmamasının temelinde başvurucunun on sekiz yaşından önce işlediği suça ait kaydın kamu makamlarına verilmesi yani kişisel verisinin açıklanması hususu bulunmaktadır. Kişisel verilerin tutulması, saklanması veya aktarılmasının ise Anayasa'nın 20. Maddesi bağlamında kişilerin özel hayatına saygı hakkı kapsamında incelenmesi gerektiği kuşkusuzdur. Bu nedenle başvurunun Anayasa'nın 20. Maddesinde yer alan özel hayata saygı hakkı kapsamında değerlendirilmesi gerekmektedir.

1. Kabul Edilebilirlik Yönünden

58. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan özel hayata saygı hakkının ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

2. Esas Yönünden

a. Müdahalenin Varlığı

59. Kamu mercileri tarafından özel yaşamı ile ilgili sorular sorulması da dâhil olmak üzere bir bireyin özel hayatı, iş ve sosyal yaşamıyla ilgili bilgilerinin alınması, kaydedilmesi, saklanması ve kullanılması özel hayata saygı hakkına müdahale oluşturur (Bülent Kaya [GK], B. No: 2013/2941, 11/5/2016, § 51; Güzide Defne Samyeli, B. No: 2014/4399, 21/9/2016, § 67).

60. Somut olayda başvuruçunun on sekiz yaşından küçükken işlediği suçun kayıtlarının Adana Valiliği Emniyet Müdürlüğü tarafından Komisyon Başkanlığına verildiği, bu kaydın dikkate alınmak suretiyle güvenlik soruşturmasının olumsuz sonuçlandığı, başvuruçunun sözleşmeli infaz ve koruma memurluğuna atamasının yapılmadığı anlaşılmaktadır.

61. Resmî makamlar tarafından muhafaza edilmekte olan, başvuruçunun hakkında yürütülen ceza yargılamasına dair bilgilerin özel hayata saygı hakkı anlamında kişisel nitelikli veriler olduğu açıktır. Söz konusu kişisel verinin kamu kurumlarıyla paylaşılması ve güvenlik soruşturmalarında kullanılmasının Anayasa'nın 20. Maddesinde güvence altına alınan özel hayata saygı hakkına bir müdahale oluşturduğu sonucuna varılmıştır.

b. Müdahalenin İhlal Oluşturup Oluşturmadığı

62. Anayasa'nın 13. Maddesi şöyledir:

“Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.”

63. Yukarıda anılan müdahalenin ihlal oluşturup oluşturmadığının Anayasa'nın 13. Maddesinde öngörülen ve somut başvuruya uygun düşen, kanunlar tarafından öngörülme, Anayasa'nın ilgili maddesinde belirtilen nedenlere dayanma, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmama koşulları yönünden incelenmesi gerekir. Bu bağlamda somut başvuruda öncelikle müdahalenin kanuni dayanağının bulunup bulunmadığı incelenmelidir.

i. Genel İlkeler

64. Anayasa uyarınca temel hak ve özgürlüklere getirilen sınırlamaların öncelikle kanunla öngörülmüş olması gerekmektedir. Kanun ile sınırlama ölçütü veya kanunilik ilkesi Sözleşme'nin 8. Maddesinde de bir sınırlama ve güvence ölçütü olarak yer almaktadır. Buna karşın Sözleşme'de yer alan kanunla öngörülmüş olma kavramı ile Anayasa'da yer alan kanunilik ilkesi tam olarak aynı değildir (Bülent Polat, § 73).

65. AİHM, kanunda öngörülen koşulları, bir diğer ifadeyle hukukiliği geniş yorumlayarak istikrar kazanmış yargı kararlarına dayanan içtihat yoluyla geliştirilmiş ilkelerin de hukukilik şartını karşılayabildiğini kabul ederken (bkz. Malone/İngiltere, B. No: 8691/79, 2/8/1984, §§ 66-68; Sunday Times/Birleşik Krallık (No. 1), B. No: 6538/74, 26/04/1979, § 47) Anayasa, tüm sınırlandırmaların

mutlaka kanun ile yapılacağını öngörerek Sözleşme'den daha geniş bir koruma sağlamıştır (Mehmet Akdoğan ve diğerleri, B. No: 2013/817, 19/12/2013, § 31; Bülent Polat § 75).

66. Bununla birlikte temel hak ve hürriyetlerin sınırlandırılmasına ilişkin kanunların şeklen var olması yeterli değildir. Kanunilik ölçütü aynı zamanda maddi bir içeriği de gerektirmekte olup bu noktada kanunun niteliği önem kazanmaktadır. Kanunla sınırlama ölçütü sınırlamanın erişilebilirliğini, öngörülebilirliğini ve kesinliğini ifade etmekte; böylece uygulayıcının keyfî davranışlarının önüne geçtiği gibi kişinin hukuku bilmesine de yardımcı olmakta; bu yönüyle hukuk güvenliği teminatı sağlamaktadır (Halime Sare Aysal [GK], B. No: 2013/1789, 11/11/2015, § 62).

67. Kanunun bu gerekliliklere uygun olduğunun söylenebilmesi için yeterince ulaşılabilir olması, vatandaşların belirli bir olaya uygulanabilir nitelikteki hukuk kurallarının varlığı hakkında yeterli bilgiye sahip olabilmesi, ayrıca ilgili normun keyfiliğe karşı uygun bir koruma sağlaması, yetkili makamlara verilen yetkinin genişliğini ve icra edilme biçimlerini yeterli bir netlikte tanımlaması gerekmektedir (Halime Sare Aysal, § 63).

68. Hukukun kendisi -beraberinde getireceği idari pratiğin dışında- söz konusu işlemin meşru amacını da gözönünde tutarak keyfî müdahalelere karşı bireyi korumak için yetkili makamlara bırakılan takdir yetkisinin kapsamını yeterince açık bir şekilde göstermelidir. Hukuk sistemi vatandaşlara, kamu makamlarına hangi koşullarda ve hangi sınırlar içinde müdahalelerde bulunma yetkisi verdiğini yeterince açık ifadelerle gösterecek nitelikte olmalı ve bu bağlamda ilgili müdahalenin muhataplarının müdahaleye zemin hazırlayan koşullar ile müdahalenin sonuçları açısından bir öngörüde bulunabilmeleri imkânı tanınmalıdır (Halime Sare Aysal, § 64).

69. Bununla birlikte her ihtimale çözüm getiremeyecek olan yasal mevzuatın sağladığı koruma seviyesi büyük ölçüde ilgili metnin düzenlediği alan ve içeriğiyle birlikte muhataplarının niteliği ve sayısı ile yakından bağlantılıdır. Bu nedenle kuralın karmaşık olması ya da belirli ölçülerde soyutluk içermesi ve buna bağlı olarak hukuki yardım ile tam olarak anlaşılabilir hâle gelmesi tek başına hukuken öngörülebilirlik ilkesine aykırı görülemez. Bu kapsamda hak ya da özgürlüğe müdahale eden kural belirli ölçülerdeki takdir alanını elbette uygulayıcıya bırakabilir. Fakat bu takdir alanının sınırlarının da yeterli açıklıkta belirlenmesi ve kuralın asgari bir kesinlik içermesi zaruridir (Halime Sare Aysal, § 65).

70. Bu kapsamda ilgili kanuni düzenlemenin söz konusu sınırlamaya ilişkin temel çerçeveyi ortaya koymakla birlikte özellikle uygulama koşulları ve usule ilişkin ayrıntıları düzenleyici işlemlere bırakması mümkündür. Ancak bu ihtimalde de söz konusu düzenleyici işlemin yine muhataplarınca

ulařılabilir olması ve içerięi hakkında ilgilileri yeterince aydınlatacak nitelik ve açıklıkta olması gerekmektedir (Halime Sare Aysal, § 66).

ii. İlkelerin Olaya Uygulanması

71. Belirli kamu görevlerinde çalıştırılacak personel hakkında uygulanan güvenlik soruşturması ve arşiv araştırmasının kanuni dayanaęı 4045 sayılı Kanun'dur (bkz. § 35).

72. 4045 sayılı Kanun'da güvenlik soruşturması ve arşiv araştırmasının kamu kurum ve kuruluşlarında yetkili olmayan kişilerin bilgi sahibi olmaları hâlinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceęi veya tehlikeye düşebileceęi bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile askerî teşkilatlarda, emniyet ve istihbarat teşkilatlarında çalıştırılacak kamu personeli, ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında yapılacaęı düzenlenmiştir.

73. Ancak 657 sayılı Kanun'un 48. Maddesine, 3/10/2016 tarihinde 676 sayılı Olaęanüstü Hal Kapsamında Bazı Düzenlemeler Yapılması Hakkında Kanun Hükmünde Kararname (KHK) ve bu KHK'nın uygun bulunmasına dair 7070 sayılı Kanun ile devlet memurluęuna alınacaklarda aranan genel şartlar arasına "Güvenlik soruşturması ve/veya arşiv araştırması yapılmıř olmak" şartı eklenmiştir. Dolayısıyla daha önce sadece 4045 sayılı Kanun'da sayılan belirli görevler yönünden güvenlik soruşturması yapılacaęı öngörölmüş iken söz konusu deęişiklik sonrasında artık tüm kamu görevleri yönünden güvenlik soruşturması ve arşiv araştırması yapılacaęı anlaşılmaktadır.

74. Bununla birlikte eldeki başvuru yönünden müdahale teşkil eden başvurucu hakkındaki işlemin tesis edildięi tarihte mevcut olan yasal düzenlemelerin esas alınması bir zorunluluk olup Anayasa Mahkemesinin olay tarihinden sonra kabul edilmiş 657 sayılı Kanun'un 48. Maddesine getirilen düzenlemeyi somut olayın incelenmesi bakımından dikkate alması mümkün bulunmamaktadır.

75. 4045 sayılı Kanun'da güvenlik soruşturması ve arşiv araştırması konusunda sadece bir maddeye yer verilerek hangi kamu görevleri bakımından güvenlik soruşturması yaptırılacaęı düzenlenmiş, bunun dışındaki tüm düzenlemelerin bir yönetmelikle yapılacaęı belirtilmiştir.

76. Bu doęrultuda Güvenlik Soruşturması ve Arşiv Araştırması Yönetmelięi çıkarılmıştır. Söz konusu Yönetmelięin 4. Maddesinde güvenlik soruşturması "kişinin kolluk kuvvetleri tarafından halen aranıp aranmadığının, kolluk kuvvetleri ve istihbarat ünitelerinde iliřięi ile adli sicil kaydının ve hakkında herhangi bir tahdit olup olmadığının, yıkıcı ve bölücü faaliyetlerde bulunup bulunmadığının, ahlaki durumunun, yabancılar ile ilgisinin ve sır saklama yeteneęinin mevcut kayıtlardan ve yerinden araştırılmak suretiyle saptanması ve deęerlendirilmesi" şeklinde

tanımlanmıştır. Arşiv araştırması ise kişinin kolluk kuvvetleri tarafından hâlen aranıp aranmadığının, kolluk kuvvetleri ve istihbarat ünitelerinde ilişiği ile adli sicil kaydının ve hakkında herhangi bir tahdit olup olmadığının mevcut kayıtlardan saptanması olarak belirtilmiştir.

77. Yönetmeliğin 7. Maddesi uyarınca güvenlik soruşturması ve arşiv araştırması yapacak makamlar Millî İstihbarat Teşkilatı Müsteşarlığı, Emniyet Genel Müdürlüğü ve mahalli mülki idare amirlikleridir.

78. Yönetmeliğin 11. Maddesinde; güvenlik soruşturması ve arşiv araştırmasında kişinin içinde bulunduğu ortam da dikkate alınarak kimlik kontrolü, kimlik kayıtlarının doğruluk derecesi, uyrukluğ, geçmişte yabancı bir devletin uyrukluğuna girip girmediği, kolluk kuvvetleri tarafından hâlen aranıp aranmadığı, kolluk kuvvetlerinin ve istihbarat ünitelerinin arşivlerinde bilgiler bulunup bulunmadığı, adli sicil kaydının ve hakkında bir tahdidin olup olmadığı, yıkıcı faaliyetlerde bulunup bulunmadığı, 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'a ve Atatürk ilke ve inkılaplarına aykırı davranıp davranmadığı, şeref ve haysiyetini ihlal edecek ve görevine yansiyacak şekilde kumara, uyuşturucuya, içkiye, paraya ve aşırı bir şekilde menfaatine düşkün olup olmadığı, ahlak ve adaba aykırı davranıp davranmadığı, yabancılarla, özellikle hasım ve hasım olması muhtemel devlet mensupları ve temsilcileriyle olan ilgi derecesinin iç yüzü ve nedeni, sır saklama yeteneğinin olup olmadığı hususlarının araştırılacağı belirtilmiştir.

79. Yönetmeliğin 12. Maddesinde güvenlik soruşturması ve arşiv araştırmasının nasıl ve ne şekilde yapılacağına soruşturma ve araştırma yapmaya yetkili makamların görev talimatları ile belirleneceği düzenlenmiştir.

80. Ayrıca anılan maddede soruşturma ve araştırma sonucunu içeren bilgi ve belgelerin ilgilinin güvenlik makamlarındaki dosyasında asgari "gizli" gizlilik derecesinde saklanacağı, güvenlik soruşturması ve arşiv araştırmasında olumsuz durumu saptananlarla ilgili bilgilerin Millî İstihbarat Teşkilatı Müsteşarlığı ve Emniyet Genel Müdürlüğüne karşılıklı olarak birbirlerine aktarılacağı düzenlenmiştir.

81. Anayasa'nın 129. Maddesinin birinci fıkrasında memurlar ve kamu görevlilerinin Anayasa ve kanunlara sadık kalarak faaliyette bulunma yükümlülükleri düzenlenmiştir. Ayrıca 657 sayılı Kanun'da bu sadakat yükümlülüğünün yanı sıra kamu görevlilerine tarafsızlık ve devlete bağlılık yükümlülükleri de getirilmiştir.

82. Kamu görevlilerinin sadakat, tarafsızlık ve devlete bağlılık yükümlülüğü çerçevesinde devleti temsil eden ve millî güvenlik bakımından hassasiyet içeren bazı kamu görevlerine atanacak kişiler

bakımından daha sıkı nitelikler aranması ve birtakım sınırlamaların getirilmesi doğaldır. Bu şekilde aranan nitelikler ve kanunlarda öngörülen kısıtlamalar, kamu hizmetinin etkin ve sağlıklı bir biçimde yürütülmesi amacıyla yöneliktir. Dolayısıyla idarenin millî güvenlik açısından önem arz eden kadrolara atanacak kişilerin tabi olacağı güvenlik soruşturması ve arşiv araştırması konusunda kanunla temel çerçeveyi ortaya koyan kurallar getirmesi elbette mümkündür. Bu çerçevenin kanunla belirlenmesinden sonra uygulama koşulları ve usule ilişkin ayrıntılar düzenleyici işlemlerle belirlenebilir. Üstelik millî güvenlik ile ilgili alanlarda çalışacak personelin seçimi ve kontrolü bakımından konuyu düzenleyen kanunda aranacak öngörülebilirlik koşulunun diğer alanlardakilere göre daha esnek olacağı da söylenebilir. Ancak yine de bu alanda düzenleme getiren kanun ile diğer alt mevzuatın kişilere, kamu makamlarına hangi koşullarda ve hangi sınırlar içinde bu tür gizli tedbirler uygulama ve potansiyel olarak özel hayatın gizliliğine yönelik müdahalelerde bulunma yetkisi verildiğini yeterince açık olarak gösterecek ve olası kötüye kullanmalara karşı yeterli güvence sağlayacak şekilde kaleme alınmış olması gerekir.

83. 4045 sayılı Kanun'un güvenlik soruşturmasına ve arşiv araştırmasına konu edilecek bilgi ve belgelerin neler olduğu, bu bilgilerin nerelerden elde edileceği ve ne suretle ve ne kadar süre ile saklanacağı, kişilerin söz konusu bilgilere itiraz etme olanağı olup olmadığı, bilgilerin bir müddet sonra silinmesinin mümkün olup olmadığı veya silinmesine dair izlenecek usulün ne olduğu, gizlilik dereceli kamu personeli ile meslek gruplarının tespiti, güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak mercilerin kimler olduğu ile ilgili hiçbir düzenleme içermediği görülmektedir. Bunun yanı sıra kanunlarda, kesinleşmiş ceza mahkûmiyetlerine dair ilk olarak akla gelmesi ve uygulanması gereken kanun olan 5352 sayılı Kanun'a atıf içeren bir düzenlemenin bulunmadığı, bireyleri keyfiliğe karşı koruyucu hiçbir hükme yer verilmediği anlaşılmaktadır. Aynı şekilde Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği'nin de elde edilen bilgilerin saklanma süreleri, bilgilerin bir müddet sonra silinmesinin mümkün olup olmadığı veya silinmesine dair izlenecek usulün ne olduğu, kişilerin söz konusu bilgilere itiraz etme olanağı olup olmadığı hususlarını düzenlemediği, bireylerin özel hayatına saygı hakkının güvencelerini sağlayacak hükümlerden yoksun olduğu anlaşılmaktadır.

84. Anayasa'nın 10., 41., 58., 61. Ve 141. Maddelerinde; devletin çocukların korunması, topluma kazandırılması ve yargılanmalarının özel kurallara tabi tutulması konularında gerekli tedbirleri alacağı, teşkilat ve tesisleri kuracağı belirtilmek suretiyle bazı pozitif yükümlülükler öngörülmüştür.

85. Devletin çocukların korunması ile ilgili bahsedilen pozitif yükümlülükleri kapsamında hukukumuzda bazı kanuni düzenlemelere de yer verildiği görülmektedir. Bunlardan biri çocukların

işledikleri bir suç nedeniyle kamu görevlerinden sürekli olarak yasaklanamayacakları ilkesidir. 5237 sayılı Kanun'un 53. Maddesinde, kasten işlediği bir suçtan dolayı hapis cezasına mahkûm olmuş ve fiili işlediği sırada on sekiz yaşını doldurmamış olanların sürekli bir kamu görevini üstlenmekten mahrum bırakılmayacakları ifade edilmiştir (bkz. § 29).

86. Aynı şekilde 5352 sayılı Kanun'un 10. Maddesinde on sekiz yaşından küçüklerle ilgili adli sicil ve arşiv kayıtlarının ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebileceği düzenlenmiştir. Buna göre kişilerin on sekiz yaşından küçükken işlediği herhangi bir suça ait kayıtların idari makamlara bildirilmesi hukuken mümkün değildir. "İlgili Hukuk" kısmında belirtildiği üzere Devlet Personel Başkanlığı görüşünün ve Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü uygulamasının da bu yönde olduğu anlaşılmaktadır (bkz. §§ 39, 40).

87. Buna karşılık 4045 sayılı Kanun'da kişilerin geçmiş ceza mahkûmiyetlerine ilişkin kayıtlar bakımından hangi suçların kamu görevine girmeye engel olduğu, kişilerin on sekiz yaşından önce işlediği suçlara dair kayıtların güvenlik soruşturmasının olumsuz sonuçlanmasına sebep olup olmayacağı konusunda hiçbir belirleme, suçlar arasında herhangi bir ayırım ve derecelendirme yapılmamıştır. Aynı şekilde 21/12/2000 tarihli ve 4616 sayılı 23 Nisan 1999 Tarihine Kadar İşlenen Suçlardan Dolayı Şartla Salıverilmeye, Dava ve Cezaların Ertelenmesine Dair Kanun uyarınca kesinleşmiş mahkûmiyet niteliğinde sayılmayan kamu davasının açılmasının ertelenmesine ve hükmün açıklanmasının geri bırakılmasına ilişkin kararların da güvenlik soruşturmasının olumsuz sonuçlanmasının bir sebebi olup olmayacağı hususunda hiçbir düzenlemeye yer verilmediği görülmektedir.

88. 4045 sayılı Kanun sadece hangi kamu görevleri bakımından güvenlik soruşturması yaptırılacağını düzenlemiş, bunun dışındaki tüm düzenlemeleri ise bir yönetmeliğe bırakmıştır. İlgili Yönetmelik hükümlerine bakıldığında Yönetmeliğin de güvenlik soruşturması ve arşiv araştırmasının nasıl ve ne şekilde yapılacağı konusunda hiçbir düzenleme içermediği, bu konunun soruşturma ve araştırma yapmaya yetkili makamların görev talimatlarına bırakılmış olduğu görülmektedir. Yetkili makamların görev talimatlarının neler olduğunun -bu talimatların yayımlanarak genelin bilgisine sunulmamış olması ve idare tarafından istenen her durumda değiştirilebileceği dikkate alındığında- bireyler tarafından önceden bilinmesi ve öngörülmesi mümkün değildir.

89. Üstelik Yönetmelik'te soruşturma ve araştırma sonucunu içeren bilgi ve belgelerin ilgilinin güvenlik makamlarındaki dosyasında süresiz olarak saklanacağı, güvenlik soruşturması ve arşiv araştırmasında olumsuz durumu saptananlarla ilgili bilgilerin Millî İstihbarat Teşkilatı Müsteşarlığı

ve Emniyet Genel Müdürlüğüne karşılıklı olarak birbirlerine aktarılacağı hükümlerine yer verilmiş olup kişilerin söz konusu bilgilere itiraz etme olanağı bulunmadığı gibi bilgilerin bir müddet sonra silinmesine de imkân verilmediği görülmektedir. Bu durumda güvenlik soruşturması ve arşiv araştırmasının objektif, öngörülebilir ve önceden belirlenebilir güvenceye ve usullere tabi kılınmış olmadığı, tamamen yetkili makamların talimatlarına bağlı olarak yapıldığı, bu hâliyle de keyfiliğe açık bir durum yaratmakta olduğu anlaşılmaktadır.

90. Bu saptamalar ışığında 4045 sayılı Kanun'un temel hak ve özgürlüklerin sınırlandırılmasını içeren konuyla ilgili temel esasları, ilkeleri ve çerçeveyi belirlemiş olduğundan söz etmek mümkün değildir. Kanun'un ve ilgili Yönetmeliğin kişisel verilerin kayıt, muhafaza ve kullanımını içeren tedbirlerin kapsamını ve uygulanmasını düzenleyen ve özellikle, süre, stoklama, kullanım, üçüncü kişilerin erişimi, verilerin gizliliği, bütünlüğü ve imhası konusundaki usullere ilişkin, muhataplarının yetki aşımı ve keyfiliğe karşı yeteri kadar güvenceye sahip olmalarını sağlayacak açık ve detaylı kuralları içermediği tespit edilmektedir. Buna göre başvuruya konu müdahalenin dayanağı olan düzenlemenin kanunilik şartını sağlamadığı sonucuna varılmaktadır.

91. Öte yandan somut olayda başvurucunun yazılı ve sözlü sınavı kazandığının ilan edilmiş olduğu, on sekiz yaşından küçükken işlediği suça ilişkin kaydın 5352 sayılı Kanun'un 10. Maddesinin (3) numaralı fıkrasında yer alan hükme açıkça aykırı şekilde idari makamlara verilmiş olduğu dikkate alındığında özel hayata saygı hakkına yönelik müdahalenin bu yönüyle de kanuni dayanaktan yoksun olduğu anlaşılmaktadır.

92. Yukarıda yer verilen tespitler uyarınca başvuruya konu müdahalenin kanunilik şartını sağlamadığı anlaşıldığından söz konusu müdahale açısından diğer güvence ölçütlerine riayet edilip edilmediğinin ayrıca değerlendirilmesine gerek görülmemiştir.

93. Açıklanan gerekçelerle başvurucunun Anayasa'nın 20. Maddesinde güvence altına alınan özel hayata saygı hakkının ihlal edildiğine karar verilmesi gerekir.

M. Emin KUZ bu sonuca farklı gerekçeyle katılmıştır.

3. 6216 Sayılı Kanun'un 50. Maddesi Yönünden

94. 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 50. Maddesinin (1) ve (2) numaralı fıkraları şöyledir:

“(1)Esas inceleme sonunda, başvurucunun hakkının ihlal edildiğine ya da edilmediğine karar verilir. İhlal kararı verilmesi hâlinde ihlalin ve sonuçlarının ortadan kaldırılması için yapılması gerekenlere hükmedilir...

(2) Tespit edilen ihlal bir mahkeme kararından kaynaklanmışsa, ihlali ve sonuçlarını ortadan kaldırmak için yeniden yargılama yapmak üzere dosya ilgili mahkemeye gönderilir. Yeniden yargılama yapılmasında hukuki yarar bulunmayan hâllerde başvuru lehine tazminata hükmedilebilir veya genel mahkemelerde dava açılması yolu gösterilebilir. Yeniden yargılama yapmakla yükümlü mahkeme, Anayasa Mahkemesinin ihlal kararında açıkladığı ihlali ve sonuçlarını ortadan kaldıracak şekilde mümkünse dosya üzerinden karar verir.”

95. Başvurucu, ihlalin tespiti ile 50.000 TL maddi, 50.000 TL manevi tazminat talebinde bulunmuştur.

96. Anayasa Mahkemesinin Mehmet Doğan ([GK], B. No: 2014/8875, 7/6/2018) kararında, ihlal sonucuna varıldığında ihlalin ortadan nasıl kaldırılacağı hususunda genel ilkeler belirlenmiştir.

97. İhlalin ve sonuçlarının ortadan kaldırılması için yapılması gerekenlere hükmedilmeden önce ihlalin kaynağının belirlenmesi gerekir. Buna göre ihlal; idari eylem ve işlemler, yargısal işlemler veya yasama işlemlerinden kaynaklanabilir. İhlalin kaynağının belirlenmesi uygun giderim yolunun belirlenebilmesi bakımından önem taşımaktadır (Mehmet Doğan, § 57).

98. İhlalin mahkeme kararından kaynaklandığı durumlarda 6216 sayılı Kanun’un 50. Maddesinin (2) numaralı fıkrası ile Anayasa Mahkemesi İçtüzüğü’nün 79. Maddesinin (1) numaralı fıkrasının (a) bendi uyarınca kural olarak ihlali ve sonuçlarını ortadan kaldırmak için yeniden yargılama yapılmak üzere kararın bir örneğinin ilgili mahkemeye gönderilmesine hükmedilir (Mehmet Doğan, § 58).

99. Buna göre Anayasa Mahkemesince ihlalin tespit edildiği hâllerde yargılamanın yenilenmesinin gerekliliği hususundaki takdir derece mahkemelerine değil ihlalin varlığını tespit eden Anayasa Mahkemesine bırakılmıştır. Derece mahkemeleri ise Anayasa Mahkemesinin ihlal kararında belirttiği doğrultuda ihlalin sonuçlarını gidermek üzere gereken işlemleri yapmakla yükümlüdür (Mehmet Doğan, § 59).

100. Mevcut başvuruda başvuru hakkında onsekiz yaşından küçükken yürütülen ceza yargılamasına dair bilgilerin idari makamlara açıklanması şeklindeki müdahalenin kanunilik şartını sağlamaması nedeniyle Anayasa’nın 20. Maddesinde düzenlenen özel hayata saygı hakkının ihlal edildiği sonucuna varılmıştır.

101. Bu nedenle ihlalin idarenin işleminden kaynaklandığı anlaşılmaktadır. Bununla birlikte işlemin iptali istemiyle açılan davanın reddedilmesi ve dolayısıyla davada ihlalin giderilememesi nedeniyle ihlalin aynı zamanda mahkeme kararından da kaynaklandığı görülmektedir. Bu durumda özel hayata saygı hakkının ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmasında hukuki yarar bulunmaktadır. Buna göre yapılacak yeniden yargılama ise 6216 sayılı

Kanun'un 50. Maddesinin (2) numaralı fıkrasına göre ihlalin ve sonuçlarının ortadan kaldırılmasına yöneliktir. Bu kapsamda derece mahkemelerince yapılması gereken iş, öncelikle ihlale yol açan mahkeme kararının ortadan kaldırılması ve nihayet ihlal sonucuna uygun yeni bir karar verilmesinden ibarettir. Bu sebeple kararın bir örneğinin yeniden yargılama yapılmak üzere Ankara 4. İdare Mahkemesine gönderilmesine karar verilmesi gerekir.

M. Emin KUZ bu sonuca katılmamıştır.

102. Yeniden yargılama yapılmak üzere dosyanın yetkili yargı merciine gönderilmesine karar verilmesinin ihlal iddiası açısından yeterli bir giderim oluşturduğu anlaşıldığından başvurucunun tazminat taleplerinin reddine karar verilmesi gerekir.

103. Dosyadaki belgelerden tespit edilen 206,10 TL harç ve 2.475 TL vekâlet ücretinden oluşan toplam 2.681,10 TL yargılama giderinin başvurucuya ödenmesine karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Özel hayata saygı hakkının ihlal edildiğine ilişkin iddianın **KABUL EDİLEBİLİR OLDUĞUNA OYBİRLİĞİYLE,**

B. Anayasa'nın 20. Maddesinde güvence altına alınan özel hayata saygı hakkının **İHLAL EDİLDİĞİNE OYBİRLİĞİYLE,**

C. Kararın bir örneğinin özel hayata saygı hakkının ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmak üzere Ankara 4. İdare Mahkemesine (14/12/2010 tarihli ve E.2010/208, K.2010/2068 sayılı kararlar ile ilgilidir) **GÖNDERİLMESİNE M. Emin KUZ'un karşıoyu ve OYÇOKLUĞUYLA,**

D. Başvurucunun tazminat taleplerinin **REDDİNE,**

E. 206,10 TL harç ve 2.475 TL vekâlet ücretinden oluşan toplam 2.681,10 TL yargılama giderinin **BAŞVURUCUYA ÖDENMESİNE,**

F. Ödemelerin, kararın tebliğini takiben başvurucunun Hazine ve Maliye Bakanlığına başvuru tarihinden itibaren dört ay içinde yapılmasına, ödemede gecikme olması hâlinde bu sürenin sona erdiği tarihten ödeme tarihine kadar geçen süre için yasal **FAİZ UYGULANMASINA,**

G. Kararın bir örneğinin Adalet Bakanlığına **GÖNDERİLMESİNE 27/2/2019 tarihinde karar verildi.**

FARKLI GEREKÇE VE KARŞIOY GEREKÇESİ

Güvenlik soruşturmasının olumlu neticelenmemesi sebebiyle infaz ve koruma memurluğuna atama yapılmamasına ilişkin işlemin özel hayata saygı ve çalışma haklarını ihlal ettiği iddialarına yönelik başvuruda özel hayata saygı hakkının ihlal edildiğine ve ihlalin giderilmesi için yeniden yargılama yapılmasına karar verilmiştir.

Oybirliği ile verilen ihlal kararına katılmakla birlikte başvuruya konu müdahalenin kanunîlik şartını sağlamadığı görüşüne farklı gerekçeyle katılıyorum. İhlalin giderilmesi için yeniden yargılama yapılması kararına ise katılmıyorum.

1. Farklı Gerekçe

Kararda ihlal sonucuna varılırken kanunîlik açısından Mahkememiz ve AİHM tarafından kabul edilen ilkelerin de tekrarlanmasına rağmen, 4045 sayılı Kanunda güvenlik soruşturması ve arşiv araştırması konusunda sadece bir maddeye yer verilerek hangi kamu görevleri bakımından güvenlik soruşturması yaptırılacağı düzenlendiği, bunun dışındaki tüm düzenlemelerin bir yönetmelikle yapılacağı belirtildiği, bu doğrultuda çıkarılan yönetmelikte konu ile ilgili düzenlemelere yer verildiği, ancak 4045 sayılı Kanunun temel hak ve özgürlüklerin sınırlandırılmasına ilişkin temel esasları, ilkeleri ve çerçeveyi belirlemiş olduğundan söz edilemeyeceği, ayrıca anılan Kanunun ve ilgili Yönetmeliğin kişisel verilerin kayıt, muhafaza ve kullanımına yönelik tedbirlerin kapsamını ve uygulanmasını düzenleyen açık ve detaylı kuralları içermediği ifade edilmiştir.

Bilindiği gibi, temel hak ve hürriyetlere bir müdahale söz konusu olduğunda, müdahaleye yetki veren bir kanun hükmünün olup olmadığının tespit edilmesi gerekmektedir. Anayasanın 20. maddesi kapsamındaki bir müdahalenin kanunîlik şartını sağladığının kabul edilebilmesi için de müdahalenin kanunî bir dayanağının olması zorunludur.

Kararın genel ilkelere ilişkin paragraflarında, Sözleşmede yer alan “kanunla öngörülmüş olma” şartı ile Anayasada yer alan “kanunîlik ilkesi”nin aynı olmadığı, AİHM’in hukukîliği geniş yorumlayarak yasama tasarrufları dışındaki mevzuatın ve istikrar kazanmış yargı kararlarına dayanan ilkelerin de hukukîlik şartını karşılayabildiğini kabul etmesine karşılık, bu konuda Anayasanın Sözleşmeden daha geniş bir koruma sağladığı belirtilmektedir (§§ 64-65).

Bununla birlikte, kararın yukarıda aktarılan paragraflarında atıf yapılan ilke kararlarımızda, belirlilik ilkesinin yalnızca yasal belirliliği değil, daha geniş anlamda hukukî belirliliği ifade ettiği; erişilebilir, bilinebilir ve öngörülebilir olma gibi şartların karşılanması hâlinde kanunların yanında yürütmenin düzenleyici işlemleriyle ve yargısal içtihatlarla da hukukî belirliliğin sağlanabileceği ve aslolanın

muhtemel muhataplarının mevcut şartlar altında belirli bir işlemin ne tür sonuçlar doğurabileceğini öngörmelerini mümkün kılacak bir normun varlığı olduğu belirtilerek, genel ifadelerle idarenin görevlerini sayan kanun hükümleri, daha ayrıntılı düzenlemeler içeren yönetmelik ve yönerge (hatta emir) şeklindeki düzenleyici işlemlerle birlikte değerlendirilmek suretiyle başvurusunun özel hayata saygı hakkına yapılan müdahalenin dayanağı olan düzenlemelerin “kanunîlik” ölçütünü karşıladığı sonucuna varıldığı da bilinmektedir (Bülent Polat [GK], B. No: 2013/7666, 10/12/2015, §§ 82-98).

Yukarıda atıf yapılan ve özel hayata saygı hakkının ihlal edilmediği sonucuna varılan bireysel başvuruda kanunîlik açısından belirlenen bu genel ilkeler, ihlal sonucuna varılan birçok başvuruda da tekrarlanarak, müdahalenin kanunîliği açısından sorun bulunmamış, ancak müdahalenin ölçüsüz olduğu gerekçesiyle özel hayata saygı hakkının ihlal edildiğine karar verilmiştir (örn. olarak bkz. Tevfik Türkmen [GK], B. No: 2013/9704, 3/3/2016, §§ 62-64; Adem Yüksel [GK], B. No: 2013/9045, 1/6/2016, §§ 67-70).

Aynı şekilde, başvuru hakkındaki ceza yargılamasına ilişkin bilginin Genel Bilgi Toplama (GBT) sistemine kaydedilmesi ve ilgili kaydın silinmemesi nedeniyle özel hayata saygı hakkının ihlal edildiği iddiasıyla yapılan başvurularda da 3152 sayılı Kanunun, ilgili birimin görevlerini düzenleyen 13. maddesi ile 2557 sayılı Kanunun, polisin istihbarat amacıyla bilgi toplayıp değerlendirmesini ve yetkili mercilere ulaştırmasını öngören ek 7. maddesi de, buna dayanılarak yürürlüğe konulan Yönerge hükümleri ile birlikte değerlendirilerek, söz konusu düzenlemelerin başvuruya konu müdahalenin kanuni dayanağını oluşturduğuna ve müdahalenin kanunîlik şartını sağladığına hükmedilmiştir (örn. olarak bkz. Bülent Kaya [GK], B. No: 2013/2941, 11/5/2016, §§ 71-78; E.Ç.A. [GK], B. No: 2014/5671, 7/6/2018, § 48).

İncelenen başvuruya konu somut olayda, sözleşmeli infaz ve koruma memurluğu sınavında başarılı olduğu açıklanan başvurusunun ataması güvenlik soruşturması sonucunun olumsuz olması nedeniyle yapılmamıştır.

657 sayılı Devlet Memurları Kanununun 48. maddesinde Devlet memurluğuna alınacaklarda aranan genel şartlar arasında affa uğramış olsa bile hırsızlık suçundan mahkûm olmama şartı sayılmış; kurumların özel kanun veya mevzuatında aranan şartları taşımak da özel şartlar arasında öngörülmüştür. İlgili Yönetmelikte de infaz ve koruma memuru olarak atanabilmek için genel şartların yanında diğer özel şartlarla birlikte “güvenlik soruşturması olumlu olma” şartı aranmıştır.

Anılan mevzuatta öngörülen şartların bulunup bulunmadığının belirlenmesi bakımından yapılacak güvenlik soruşturmalarına ilişkin 4045 sayılı Kanunun 1. maddesinde, hakkında güvenlik soruşturması yapılacak personel arasında ceza infaz kurumları ve tutukevlerinde çalışacak personel

de sayılarak Kanunda belirtilen hususlara ilişkin usul ve esasların Bakanlar Kurulu kararıyla yürürlüğe konulacak yönetmelikle düzenleneceği hükme bağlanmıştır.

Resmî Gazetede yayımlanarak yürürlüğe giren ve ilgilileri tarafından erişilebilir, bilinebilir ve öngörülebilir olma şartlarını taşıdığına kuşku bulunmayan mezkûr Yönetmelikte ise güvenlik soruşturması yapacak makamlar, hakkında güvenlik soruşturması yapılacak personel, güvenlik soruşturmasında araştırılacak hususlar ve konuya ilişkin diğer usul ve esaslar ayrıntılı olarak düzenlenmiştir.

Dolayısıyla, 657 ve 4045 sayılı Kanunlar ile bunlara dayanılarak çıkarılan Yönetmeliklerin, hukukun keyfi bir şekilde uygulanması riskini ortadan kaldıracak açıklıkta hükümler içerdiği ve başvuru açısından ulaşılabilir ve öngörülebilir olduğu, bu sebeple söz konusu düzenlemelerin “kanunîlik” ölçütünü karşıladığı açıktır.

Kuşkusuz söz konusu güvencelere mevzuatta yer verilmemesi gibi yer verildiği hâlde uygulanmaması veya etkisizleştirilmesi de anayasal hakları ihlal eder.

Çoğunluğun ihlal gerekçesinde 4045 sayılı Kanunun konuyla ilgili temel esasları, ilkeleri ve çerçeveyi belirlemediği, Kanunun ve ilgili Yönetmeliğin açık ve detaylı kuralları içermediği, bu durumda güvenlik soruşturmasının objektif, öngörülebilir ve belirlenebilir güvencelere bağlanmadığı ve tamamen yetkili makamların talimatına bağlı olarak yapıldığı, bu hâliyle de keyfiliğe açık bir durum doğurduğu belirtilmekte ise de, bu tespitlerin isabetli olmadığı düşüncesiyle ve müdahalenin dayanağını oluşturan mezkûr düzenlemelerin değil müdahaleyi oluşturan (ve kararın 1. paragrafında da belirtilen) “kanunen verilmemesi gereken kişisel verinin idarî makamlara açıklanması ve güvenlik soruşturmasına esas alınması” nedeniyle, yani müdahalenin dayanağını oluşturan düzenlemelerin değil, anılan müdahalenin kanunîlik şartını sağlamadığı gerekçesiyle “kanunîlik” bakımından ihlal sonucuna katılıyorum.

Başka bir anlatımla, Anayasanın 20. maddesinin son fıkrasında kişisel verilerin ancak kanunlarda öngörülen hâllerde ilgili kişinin açık rızası alınmaksızın işlenebileceğinin belirtilmesine ve 5237 sayılı Kanunun 53. maddesinin (4) numaralı fıkrasında kişinin kasten işlediği bir suçtan dolayı hapis cezasına mahkûmiyetin kanunî sonucu olarak memur olarak görevlendirilemeyeceğine dair (1) numaralı fıkrasının, fiili işlediği sırada onsekiz yaşını doldurmamış olan kişiler hakkında uygulanmayacağı; 5352 sayılı Kanunun 10. maddesinin (3) numaralı fıkrasında da “onsekiz yaşından küçüklerle ilgili adli sicil ve arşiv kayıtlarının ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere mahkeme, hâkim veya savcılıklara” verilebileceğinin öngörülmesine rağmen, mezkûr kişisel verinin idareye verilmesi ve güvenlik soruşturmasına esas alınmasından dolayı

başvuruya konu müdahalenin kanunîlik şartını sağlamadığını düşünüyor ve bu nedenle, özel hayata saygı hakkının ihlal edildiği sonucuna farklı gerekçeyle katılıyorum.

2. Karşıoy Gerekçesi

Yukarıdaki gerekçelerle, başvurucunun Anayasanın 20. maddesinde teminat altına alınan özel hayata saygı hakkının ihlal edildiği kararına katılmakla birlikte, ihlalin giderilmesi için yeniden yargılama yapılmasına ilişkin çoğunluk görüşüne katılmıyorum.

Mahkememizin Mehmet Doğan kararında belirlenen ve bu kararda da tekrarlanan genel ilkelere göre, bireysel başvuru kapsamında bir temel hakkın veya hürriyetin ihlal edildiğine karar verildiği takdirde ihlalin ve sonuçlarının ortadan kaldırılması için esas olarak eski hâle getirmeyi, başka bir ifadeyle ihlalden önceki duruma dönülmesini sağlayacak bir giderim yolunun da belirlenmesi gerekir. Ancak bu genel ilkelerin somut olayda ihlalin giderilmesi bakımından yeniden yargılama yapılması yerine başvurucuya manevî tazminat ödenmesini gerektirdiğini düşünüyorum.

Bilindiği gibi, kamu hizmetine girme hakkı, Anayasanın 70. maddesinde düzenlenmiş olmakla birlikte Sözleşme kapsamında korunan bir hak değildir. Anayasa ve Sözleşmenin ortak koruma alanı dışında kalan hak ihlali iddialarını içeren başvurular bireysel başvurunun konusu dışında kaldığından, Mahkememiz kamu hizmetine girme hakkının ihlal edildiğine ilişkin bireysel başvuruların -Anayasa ve Sözleşmenin ortak koruma alanı dışında kaldığı gerekçesiyle- konu bakımından yetkisizlik nedeniyle kabul edilemez olduğuna karar vermektedir.

Somut olayda, başvuru formunda başvurucunun çalışma ve özel hayatın gizliliği haklarının ihlal edildiği ileri sürüldüğünden, başvurucunun iddialarının Anayasanın 20. maddesinde güvence altına alınan özel hayata saygı hakkı kapsamında incelenmesi ve bu hak bakımından ihlal sonucuna varılması isabetli olmakla birlikte, yeniden yargılama yapılmasına hükmedilmesi yukarıda belirtilen ilkelerle bağdaşmamakta ve ortak koruma alanında yer almayan, bireysel başvurunun konusu dışında kalan kamu hizmetine girme hakkının da yeniden yargılama ile tanınması sonucunu doğuracak bir değerlendirme olarak görünmektedir.

Başka bir anlatımla, Mahkememizin bugüne kadar verdiği kararlarda belirlenen ilkelere göre, kamu hizmetine girme hakkının bireysel başvurunun konusu dışında kalmasına ve sadece bireysel başvuru kapsamındaki bir hakkın ihlal edildiğine karar verildiği takdirde ihlalden önceki duruma dönülmesini sağlayacak bir giderim yolunun belirlenmesinin gerekmesine rağmen, bireysel başvurunun konusu dışında kalan kamu hizmetine girme hakkının tanınması ihtimalini doğuracak şekilde yeniden yargılama yapılmasına karar verilmiştir.

Yukarıda farklı gerekçe kısmında örnek olarak belirtilen, TSK'dan iliřiđi kesilen ok sayıda bařvurucu ile ilgili benzer ihlal kararlarında zel hayata sayđı hakkının ihlal edilmesi sebebiyle yeniden yargılama yapılmasına hkmedilmiş olmakla birlikte, anılan kararlarda bařvurucuların kamu hizmeti yapmakta iken zel hayata sayđı hakkının ihlal edilmesi suretiyle grevlerinden ıkarılan kiřiler olmaları sebebiyle anılan kararlarda varılan yeniden yargılama yapılması ynndeki giderim yolu, bu bařvurudan farklı olarak bireysel bařvurunun konusu dıřında kalan kamu hizmetine girme hakkının tanınması sonucunu dođurmamıřtır.

Bu sebeplerle, bařvurucunun zel hayata sayđı hakkının ihlal edilmesinden dolayı yeniden yargılama yapılmasının isabetli olmadığı ve uygun giderim yolu olarak manev tazminata hkmedilmesi gerektiđi dřncesiyle, ođunluđun kararının bu kısmına katılmıyorum.

ye

M. Emin KUZ

Anayasa Mahkemesi - Güzide Defne Samyeli Kararı (2014/4399)

Güzide Defne Samyeli, B. No: 2014/4399, 21/9/2016

Başvuru, Türkiye İstatistik Kurumu TÜİK) tarafından gerçekleştirilen Hanehalkı Bütçe Anketi ne geçerli bir mazeret olmaksızın ankete katılmadığı gerekçesiyle hakkında idari para cezası uygulanması nedeniyle özel hayata saygı hakkının ihlal edildiği iddialarına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

BİRİNCİ BÖLÜM

KARAR

GÜZİDE DEFNE SAMYELİ BAŞVURUSU

(Başvuru Numarası: 2014/4399)

Karar Tarihi: 21/9/2016

BİRİNCİ BÖLÜM

KARAR

Başkan: Burhan ÜSTÜN

Üyeler: Hicabi DURSUN, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Rıdvan GÜLEÇ

Raportör: Şermin BİRTANE

Başvurucu: Güzide Defne SAMYELİ

Vekili: Av. Ayşegül ANDIÇ

I. BAŞVURUNUN KONUSU

1. Başvuru, Türkiye İstatistik Kurumu (TÜİK) tarafından gerçekleştirilen Hanehalkı Bütçe Anketi'ne geçerli bir mazeret olmaksızın ankete katılmadığı gerekçesiyle hakkında idari para cezası uygulanması nedeniyle özel hayata saygı hakkının ihlal edildiği iddialarına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 21/3/2014 tarihinde İstanbul 28. Sulh Ceza Mahkemesi vasıtasıyla yapılmıştır. Başvuru formu ve eklerinin idari yönden yapılan ön incelemesi neticesinde başvurunun Komisyona sunulmasına engel teşkil edecek bir eksikliğin bulunmadığı tespit edilmiştir.
3. Birinci Bölüm Birinci Komisyonunca 27/2/2015 tarihinde, başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.
4. Bölüm tarafından 14/05/2015 tarihinde, başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.
5. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık görüşünü 14/7/2015 tarihinde Anayasa Mahkemesine sunmuştur.
6. Bakanlık tarafından Anayasa Mahkemesine sunulan görüş 17/8/2015 tarihinde başvurucuya tebliğ edilmiştir. Başvurucu, Bakanlığın görüşüne karşı beyanlarını süresi içinde ibraz etmemiştir.

III. OLAY VE OLGULAR

A. Olaylar

7. Başvuru formu ve eklerinde ifade edildiği şekliyle ilgili olaylar özetle şöyledir:
8. TÜİK tarafından Türkiye'deki hanelerin harcamalarının nasıl şekillendiğini tespit etmek amacıyla gerçekleştirilen "2013 yılı Hanehalkı Bütçe Anketi" kapsamında başvurunun adresi örnek hane olarak seçilmiş; araştırmanın uygulanma aralığı 1/10/2013 ve 31/10/2013 tarihleri olarak belirlenmiş ve TÜİK İstanbul Bölge Müdürlüğüne, yapılacak çalışma hakkında bilgi içeren 6/9/2013 tarihli yazı başvurunun adresine gönderilmiştir.
9. Bireysel başvuru dosyasına sunulan Hanehalkı Bütçe Anketi'nde, ailedeki aynı gelir elde eden kişilerin ad ve soyadları, edinilen aynı gelirin kaynağı, aynı gelirin elde edilme sıklığının, haneye gelen hediye ve yardımlar ile haneden başka hanelere yapılan yardımlar ve verilen hediyelerin belirtilmesi, anket ayı boyunca yapılan tüm harcamaların marka, ölçü, miktar, alışverişin yapıldığı yer gibi detaylarının bir ay süreyle günlük harcama kayıt defterine kaydedilerek listelenmesinin istendiği anlaşılmıştır. Ayrıca söz konusu bir aylık sürede ortalama sekiz defa anket yapılan kişinin evinin anketörler tarafından ziyaret edilerek harcama kayıt defterinin kontrol edileceği belirtilmektedir.
10. 27/9/2013 ile 8/10/2013 tarihleri arasında TÜİK anketörleri başvuruyla telefonda iletişime geçmişler, ayrıca üç kez evini ziyaret etmişlerdir. Başvurunun ankete katılmak istemediğini belirtmesi üzerine İstanbul Bölge Müdürlüğü tarafından 8/10/2013 tarihli cevapsızlık tutanağı düzenlenmiştir. Başvurucuya 21/10/2013 tarihinde tebliğ edilen söz konusu tutanakta, yazının

tebliğinden itibaren yedi gün içinde ankete cevap verilmemesi durumunda 10/11/2005 tarihli ve 5429 sayılı Türkiye İstatistik Kanunu'nun 54. maddesi uyarınca 923 TL idari para cezası uygulanacağı ihtarına yer verilmiştir.

11. Başvurucu, İstanbul Bölge Müdürlüğüne verdiği 24/10/2013 tarihli dilekçesinde işi nedeniyle sürekli medyada yer alan bir sanatçı olarak yoğun iş temposuna sahip olduğu ve sürekli televizyon çekimleri ve iki çocuğunun bakımı ile uğraştığından bahisle ankete katılmasının mümkün olmadığını belirterek mazeretinin dikkate alınmasını ve anketin cevaplandırılmasından muaf tutulmasını talep etmiştir.

12. Bu dilekçe üzerine İstanbul Bölge Müdürlüğü'nün 25/10/2013 tarihli yazısıyla başvurucuya 5429 sayılı Kanun uyarınca vereceği bilgilerin gizliliğinin ve güvenliğinin yasal güvenceye kavuşturulduğu, söz konusu anketi 31/10/2013 tarihine kadar cevaplamadığı takdirde hakkında idari para cezası uygulanacağı bildirilmiştir.

13. Başvurucuya Hanehalkı Bütçe Anketi çalışmalarına katılmaması nedeniyle 7/11/2013 tarihli işlemle 5429 sayılı Kanun'un 54. maddesi gereğince 923 TL idari para cezası verilmiştir. Başvurucu, bu cezayı 21/11/2013 tarihinde ödemiştir.

14. Başvurucu 26/11/2013 tarihinde söz konusu anket çalışmasında, ekonomik durumu hakkında bir ay süreyle ayrıntılı bilgi vermesinin istenmesi ve anketörlerin ev ziyaretleri nedenleriyle özel hayatın gizliliğinin ihlal edildiğini belirterek anılan idari para cezasının iptali için İstanbul 28. Sulh Ceza Mahkemesine başvurmuştur.

15. İstanbul 28. Sulh Ceza Mahkemesi 5/2/2014 tarihli ve 2013/602 Değişik İş sayılı ilamında "...itirazcıya hane halkı bütçe anketi yapılacağı hususunda ihtarlat yapılmasına rağmen uyarıya aykırı hareket ettiği, bu haliyle eyleminin 5429 sayılı Kanun'un 54. Maddesinin ikinci fıkrasına aykırılık teşkil ettiği, idari para cezasına yönelik itiraz sebeplerinin yerinde olmadığı..." gerekçesiyle itirazın reddine kesin olarak karar vermiştir.

16. Anılan karar başvurucu vekiline 20/2/2014 tarihinde tebliğ edilmiş olup başvurucu 21/3/2014 tarihinde bireysel başvuruda bulunmuştur.

B. TÜİK Anketi Hakkında Açıklamalar

17. TÜİK'in İnternet sitesinde yayımlanmış olan 2013 yılı Hanehalkı Bütçe Anketi Mikro Veri Seti'nde (Bu belge hakkında detaylı bilgi "İlgili Hukuk" kısmında yer almaktadır.) anketin 1 Ocak 2013-31 Aralık 2013 tarihleri arasında bir yıl süre ile kentsel ve kırsal kesimden (Kentsel yerler, nüfusu 20.001 ve daha fazla olan yerleşim yerleri; kırsal yerler, nüfusu 20.000 ve daha az olan yerleşim yerleridir.)

her ay deęişen aylık toplam 1.104 örnek hane halkına uygulandıęı, hane halkı gelirlerine ve tüketim harcamalarına ilişkin bilgilerin hane halkı fertleriyle yapılan birebir görüřmeler ve hane halkının bir ay boyunca yaptıęı günlük harcamaları tuttuęu kayıt defterleri yoluyla derlendięi, her anketörün her ay ortalama altı örnek hane halkını anket ayı öncesi bir kez, 1. ve 2. haftalarda ikiřer kez, 3. ve 4. haftalarda bir kez ve anket ayı bitiminde de bir kez olmak üzere her bir hane halkını ayda ortalama sekiz defa ziyaret ederek tüketim harcamaları ve son ziyarette gelir bilgilerini kayıt ettięi belirtilmiřtir. Bunun yanı sıra anket ayı öncesinde örnek hane halkına yapılan ilk ziyarette, hane halkı ile tanışma saęlandıktan sonra hane halkının sosyoekonomik durumuna ait bilgilerin alındıęı, harcama kayıt defterinin nasıl doldurulacaęının açıklandıęı, anket ayı içinde yapılan ziyaretler sırasında örnek hanenin anket ayında yaptıęı gıda, giyim, saęlık, ulařtırma, haberleřme, eęitim, kültür, eęlence, konut, ev eřyası vb. gibi tüketim harcamalarının hane halkına bırakılan kayıt defterinden kayıtlama ve görüřme yöntemleri ile toplandıęı, anket ayı bitiminde yapılan son görüřmede ise hane halkı fertlerinin anket ayı içindeki istihdam durumu, iktisadi faaliyeti, mesleęi, iřteki durumu, son bir yıl içinde elde ettięi gelir bilgilerinin derlendięi bildirilmiřtir.

18. Ankette kullanılan soru kâğıdında on iki harcama grubunda (gıda ve alkolsüz içecekler, alkollü içecekler, sigara ve tütün, giyim ve ayakkabı, konut, su, elektrik, gaz ve dięer yakıtlar , mobilya, ev aletleri ve ev bakım hizmetleri, saęlık, ulařtırma, haberleřme, eęlence ve kültür, eęitim hizmetleri, lokanta, yemek hizmetleri ve oteller, çeřitli mal ve hizmetler) yapılan harcamaların "mal ve hizmetin adı, tanımı, ölçü birimi, miktarı, toplam deęer, alışveriřin yapıldıęı yer" belirtilmek üzere kaydedilmesinin istendięi ifade edilmiřtir.

19. Anılan veri setinde, örnek hane halkının belirlenmesinde Ulusal Adres Veri Tabanı'nın (UAVT) kullanıldıęı, bu veri tabanında kentsel yerlerden ve belediye teřkilatı olan kırsal yerlerden ve köylerden yerleřim yerinin büyüklüęüne orantılı olasılıkla bloklar belirlendięi ve her bloktan hane halklarının örnekleme yoluyla seçildięi belirtilmiřtir. Buna göre hane halkı bütçe anketinin örnekleme birimi hane halkıdır. Örnek haneler, tabakalı iki aşamalı küme örnekleme yöntemi kullanılarak seçilmektedir. İlk aşama örnekleme birimi olan blokların seçiminde kullanılan örnekleme çerçevesi, UAVT'dir. UAVT kullanılarak öncelikle Türkiye genelinde her biri 100 hane içeren bloklar oluřturulmaktadır. Oluřturulan bu bloklardan arařtırma tasarımına ve ölçülmek istenen deęiřkene baęlı olarak hesaplanan örnek blok sayısı kadar blok tesadüfi olarak seçilmektedir. İkinci aşamada ise her bloktan örnek hane halkları sistematik olarak seçilmektedir.

20. Anketten ařaęıda gösterilen temel olarak üç ana grup deęiřken elde edildięi belirtilmiřtir.

a) Hane Halkı Sosyoekonomik Durum Değişkenleri: Oturulan konutun tipi, mülkiyet durumu, ısıtma sistemi, konut kolaylıkları, sahip olunan eşyalar ve ulaştırma araçları vb.

b) Tüketim Harcaması Değişkenleri: Alt harcama grubu ve yapılan tüketim harcaması değeri.

c) Fertlere İlişkin Değişkenler: Yaş grubu, cinsiyet, öğrenim durumu, medeni durum, istihdam durumu (meslek, iktisadi faaliyet, işteki durum) değişkenleri, son on iki ay faaliyet ve faaliyet dışı kullanılabilir gelirler.

21. Söz konusu belgede "Amaç" başlığı altında, Hanehalkı Bütçe Anketi'nden elde edilen verilerin; tüketici fiyat endekslerinde (TÜFE) kullanılacak maddelerin seçimi ve temel yıl ağırlıklarının elde edilmesi, hanelerin tüketim kalıplarında zaman içinde meydana gelen değişikliklerin izlenmesi, millî gelir hesaplamalarında özel nihai tüketim harcamaları tahminlerine yardımcı olacak verilerin derlenmesi, yoksulluk sınırının belirlenmesi, asgari ücret tespit çalışmaları vb. diğer sosyoekonomik analizler için kullanılacağı ifade edilmiştir.

C. İlgili Hukuk

22. TÜİK'in İnternet sitesinde yayımlanmış olan 2013 yılı Hanehalkı Bütçe Anketi Mikro Veri Seti'nde yer alan tanım ve kavramlar şöyledir:

"Hanehalkı: Aralarında akrabalık bağı bulunsun veya bulunmasın aynı konutta veya aynı konutun bir bölümünde yaşayan, temel ihtiyaçlarını birlikte karşılayan, hanehalkı hizmet ve yönetimine iştirak eden bir veya birden fazla kişiden oluşan topluluktur.

Hanehalkı ferdi: hanehalkını meydana getiren topluluğun her bir üyesidir. Bununla birlikte askerde, hapiste olanlar ve huzurevlerinde kalan yaşlılar ve üniversite yurdunda kalan öğrenciler, hanede kalış süresi ne olursa olsun misafirler ve hane halkından evlenme, askere gitme, çalışmaya gitme gibi sebeplerle kesin olarak ayrılanlar hane halkı ferdi olarak kapsamamaktadır.

Hanehalkı sorumlusu: Hanehalkının kazanç ve masraflarından sorumlu olan, kısaca hanehalkını bilfiil yöneten kişidir. Burada ölçü yalnız gelir getirmek değil, hanehalkı adına hukuki, sosyal ve iktisadi tasarruflarda bulunabilmektir. Hanede hiç değilse bir noktada diğer fertlerden daha üstün ve aktif bir rol oynayan fert, hanehalkı sorumlusu olarak tanımlanmıştır.

Referans fert: Hanede en yüksek gelir elde eden fert, referans fert olarak tanımlanmıştır.

Hanehalkı Günlük Harcama Kayıt Defteri: Hanehalkının anket ayı süresince yapacağı tüm harcamaların, hane tarafından unutulmadan kaydedilmesini sağlamak amacıyla hazırlanmıştır.

Günlükler, anket ayı öncesinde hanehalkına yapılan ziyarette haneye tanıtılmakta, nasıl doldurulacağı anketör tarafından anlatılarak hanede bırakılmaktadır. Hanehalkının gerek satın alarak yaptığı harcamalar, gerekse kendi üretimlerinden tükettiği maddeler, çalışan hanehalkı fertlerinin işyerinde üretilen ya da satılan mal ya da hizmetlerden haneye getirdikleri ile haneye başka hane ya da kuruluşlardan verilen hediye ve yardımlar; hanehalkı sorumlusu veya hanehalkında yaşayan yetişkin bir fert tarafından bir ay boyunca günlüklere kaydedilmektedir.”

23. 2013 yılı Hanehalkı Bütçe Anketi'nin amacı şöyle ifade edilmiştir:

“Amaç: Gelişen ve sürekli değişen bir sosyo-ekonomik yapı içinde bulunan ülkemizde, bireylerin ve bunların oluşturduğu hanehalkının tüketim harcamalarını, gelir düzeylerini, sosyo-ekonomik kesimler ve bölgelere göre ortaya çıkaran çalışmalar “Hanehalkı Bütçe Anketleri” dir.

Hanehalkı bütçe anketinden elde edilen tüketim harcamaları bilgileri ile; tüketici fiyat endekslerinde kullanılacak maddelerin seçimi ve temel yıl ağırlıklarının elde edilmesi, hanelerin tüketim kalıplarında zaman içinde meydana gelen değişikliklerin izlenmesi, milli gelir hesaplamalarında özel nihai tüketim harcamaları tahminlerine yardımcı olacak verilerin derlenmesi, yoksulluk sınırının belirlenmesi, asgari ücret tespit çalışmaları vb. diğer sosyo-ekonomik analizler için gerekli verilerin elde edilmesi amaçlanmaktadır.”

24. 5429 sayılı Kanun'un "Amaç" kenar başlıklı 1. maddesi şöyledir:

“Bu Kanunun amacı; resmî istatistiklerin üretimine ve organizasyonuna ilişkin temel ilkeleri ve standartları belirlemek; ülkenin ihtiyaç duyduğu alanlarda veri ve bilgilerin derlenmesini, değerlendirilmesini, gerekli istatistiklerin üretilmesini, yayımlanmasını, dağıtımını ve Resmî İstatistik Programında istatistik sürecine dâhil kurum ve kuruluşlar arasında koordinasyonu sağlamak üzere, Türkiye İstatistik Kurumunun kuruluş, görev ve yetkilerine ilişkin esasları düzenlemektir.”

25. 5429 sayılı Kanun'un "Tanımlar" kenar başlıklı 2. maddesi şöyledir:

“Bu Kanunun uygulanmasında;

...

e) Kurum ve kuruluşlar: Başbakanlık ve bakanlıklar ile bunların bağlı, ilgili ve ilişkili kuruluşlarını, mahallî idareler ve bunların bağlı ve ilgili kuruluşları ile birlik ve şirketlerini, Türkiye Cumhuriyet Merkez Bankası, İstanbul Menkul Kıymetler Borsası ve üniversiteler de dâhil olmak üzere, tüzel

kişiliği haiz enstitü, teşebbüs, teşekkül, birlik, döner sermaye, fon ve sair adlarla kurulmuş olan diğer kurum ve kuruluşlar ile kamu kurumu niteliğindeki meslek kuruluşlarını,

f) Program: Resmî İstatistik Programını,

g) Resmî istatistik: Türkiye İstatistik Kurumu veya Programda yer alan konularda istatistik üretecek kurum ve kuruluşlar tarafından derlenen verilerin, kitle özelliklerini ortaya koymak amacıyla işlenmesi ile elde edilen bilgiyi,

h) İstatistikî birim: Yapılan sayım veya örnekleme çalışmalarına konu olan, hakkında veri toplanacak gerçek ve tüzel kişiler ile kurum ve kuruluşları,

i) Kitle: Sayım veya örnekleme konu olan istatistikî birim veya alt birimlerin tamamını,

j) Sayım: Kitle özelliklerini ortaya koymak üzere ilgili tüm istatistikî birimlerden veri derlenmesini,

k) Örnekleme: Kitleyi oluşturan istatistikî birimler arasından kitleyi temsil etmek üzere belli sayıda birimin seçilmesi işlemini,

l) Ulusal kayıt sistemi: Kurum ve kuruluşların idarî işlemlerini yürütmek amacıyla kayıt altına aldıkları bilgilerin standartlaştırılarak tanımlanmış tek bir numara vasıtasıyla ulusal düzeyde ilgili diğer kurum ve kuruluşların kayıtları ile konuşabilirliğinin sağlandığı veri tabanı sistemini,

m) Alan çalışması: İstatistik çalışmalarıyla ilgili her türlü veriyi derlemek üzere istatistikî birim ile görüşülmesi, bilgilerin anket formuna aktarılması ve bu formların Başkanlığa teslimine kadar geçen sürede yapılan çalışmaları,

n) Veri: Anket veya idarî kayıtlar yoluyla elde edilen nicel ve/veya nitel istatistikî bilgileri,

o) Bireysel veri: Hakkında bilgi toplanan istatistikî birimlerin, özellikleri ile birlikte tanımlandığı veriyi,

p) Doğrudan tanınma: Bir istatistikî birimin kimliğinin adı, adresi veya resmen verilmiş ve genel olarak bilinen bir kimlik numarası ile ortaya çıkarılmasını,

r) Dolaylı tanınma: Bir istatistikî birimin kimliğinin, doğrudan tanımlamada yer almayan diğer özelliklerinden faydalanılarak ortaya çıkarılmasını,

s) Gizli veri: İstatistik birimin doğrudan veya dolaylı bir şekilde özellikleri ile birlikte tanınabilmesine ve bu şekilde bireysel bilgilerin açığa çıkarılmasına imkân sağlayan bireysel veya tablo hâlinde saklı tutulan veriyi,

t) İstatistik amaçlı kullanım: İstatistik birimlerden toplanan verilerin sadece istatistikî tabloların oluşturulması ve istatistikî analizlerin yapılması için kullanımını,

u) Dağıtım: Kullanılan şekil ve araçlara bakılmaksızın, istatistikî bilgilerin kullanıcılara sunulmasını, ifade eder.”

26. 5429 sayılı Kanun’un "İlkeler" kenar başlıklı 4. maddesi şöyledir:

“Resmî istatistiklerin kalitesinin geliştirilmesi için Program kapsamında üretilen istatistikler, güvenilirlik, tutarlılık, tarafsızlık, istatistikî gizlilik, güncellik ve şeffaflık ilkelerine göre hazırlanır ve uygulanır.

Resmî istatistiklerin gerçekleri yansıtmasının sağlanması, tüm kullanıcılara tarafsız ve eş zamanlı olarak sunulması, gizlilik ilkesine riayet edilmesi, kamuoyunun bilgi edinme hakkının gözetilmesi temel esaslardır.

Resmî istatistiklerin kalitesinin ve ilkelere uygunluğunun değerlendirilebilmesi için gerekli tüm bilgiler ve resmî istatistik üretiminde kullanılan yöntemler kamuoyuna açıklanır....”

27. 5429 sayılı Kanun’un "Cevap verme yükümlülüğü ve sınırları" kenar başlıklı 8. maddesi şöyledir:

“(İptal: Anayasa Mahkemesi’nin 20/3/2008 tarihli ve E: 2006/167, K: 2008/86 sayılı Kararı ile; Yeniden Düzenleme: 25/11/2008-5813/1 md.) İstatistikî birimler, ülkenin ekonomi, sosyal, demografi, kültür, çevre, bilim, teknoloji ve ihtiyaç duyulan diğer alanlardaki resmi istatistikleri üretmek üzere, Anayasa’da belirlenen temel haklar ve ödevler çerçevesinde, kendilerinden istenen veri veya bilgileri, Başkanlığın belirleyeceği şekil, süre ve standartlarda eksiksiz ve doğru olarak ücretsiz vermekle yükümlüdür....”

28. 5429 sayılı Kanun’un "Gizli veriler" kenar başlıklı 13. maddesi şöyledir:

“Gizli verilere yalnızca resmî istatistik üretiminde görev alanlar, görevlerini yerine getirebilmek için ihtiyaç duydukları ölçüde erişebilirler.

Bireysel verinin toplulaştırılması ile oluşturulan veri tablosunun herhangi bir hücresindeki istatistikî birim sayısının üçten az olması veya birim sayısı üç ve daha fazla olduğu hâlde bir veya iki istatistikî birimin hakim durumda olması hâlinde ilgili hücredeki veri gizli kabul edilir.

Resmî istatistiklerin üretilmesi için toplanan, işlenen ve saklanan verilerden gizli olanları, idarî, adli ve askerî hiçbir organ, makam, merci veya kişiye verilemez, istatistik amacı dışında kullanılamaz ve ispat aracı olamaz. Bu bilgileri derleyen ve değerlendiren memurlar ve diğer görevliler de bu yasağa

uymak zorundadır. Bu yükümlülük, görevlilerin görevlerinden ayrılmalarından sonra da devam eder.

Resmî istatistik üreten kurum ve kuruluşların yetkilileri tarafından, gizli verilerin hukuka aykırı erişimine, açıklanmasına veya kullanımına karşı her türlü önlem alınır.

Herkese açık kaynaklardan elde edilen veri veya bilgiler gizli kabul edilmez.

İstatistikî birimin, kendisine ait gizli verilerin açıklanmasına yazılı onay vermesi hâlinde, veri gizliliği ortadan kalkar.

Gizli veriler, ancak doğrudan veya dolaylı tanımlamaya yol açmayacak şekilde diğer bilgilerle birleştirilerek yayımlanabilir.

(Ek fıkra: 25/11/2008-5813/2 md.) Dış ticaret istatistiklerinde dolaylı tanınma ile gizlilik kapsamına giren veriler için bu gizlilik hükümleri, istatistikî birimin kendisine ait verinin gizlenmesini talep eden yazılı başvurusu halinde uygulanır.

Veri gizliliği ve güvenliğine ilişkin usûl ve esaslar, ulusal ve uluslararası ilkeler doğrultusunda, ilgili kurum ve kuruluşların görüşleri alınarak çıkarılacak yönetmelikle düzenlenir.”

29. 5429 sayılı Kanun’un "Bireysel verilerin kullanımı" kenar başlıklı 14. maddesi şöyledir:

“Bireysel veriler, istatistikî birimlerin doğrudan veya dolaylı olarak tanınmasına yol açacak bölümleri gizlendikten sonra, münferit birimlere atıfta bulunmayan bilimsel amaçlı araştırmalarda kullanılması kaydı ve Başkanlığın yazılı izniyle verilebilir. Bireysel verileri kullanma hakkı elde edenler, bu verileri üçüncü şahıslara veremezler.”

30. 5429 sayılı Kanun’un "İstatistikî birimlerin hakları" kenar başlıklı 15. maddesi şöyledir:

“Resmî istatistiklerin üretimi için veri veya bilgi talep edilen istatistikî birimler, sayımın veya araştırmanın amacı, kapsamı, istatistikî verinin gizliliğinin sağlanması için alınan önlemler ve hakları ile ilgili konularda 4982 sayılı Bilgi Edinme Hakkı Kanunu çerçevesinde, bilgi edinme, kendilerine ait gizli verinin izinsiz açıklanması durumunda da maddi ve manevi her türlü zararının tazmin edilmesini isteme hakkına sahiptir.

Kendilerine ait gizli verilerin açıklanması nedeniyle açılan davalarda Başkanlık veya diğer kurum ve kuruluşlar aleyhine tazminata hükmedilmesi durumunda, bu hususta kusuru olan memur ve diğer görevlilere genel hükümlere göre rücu edilir.”

31. 5429 sayılı Kanun’un "Yöneticilerin sorumlulukları" kenar başlıklı 50. maddesi şöyledir:

“Başkanlığın her kademedeki yöneticileri, görevlerini mevzuata, stratejik plân ve programlara, performans ölçütlerine ve hizmet kalite standartlarına uygun olarak yürütmekten üst kademelere karşı sorumludur.”

32. 5429 sayılı Kanun’un “Uluslararası işbirliği” kenar başlıklı 51. maddesi şöyledir:

“Başkanlık, istatistikî bilgilerin en gelişmiş yöntemlerle elde edilmesi, veri ve yayın değişimi, eğitim, ortak proje geliştirme ve uygulama konularında diğer ülkelerin benzer kuruluşları, uluslararası ve uluslararası kuruluşların ilgili birimleri ile genel hükümler çerçevesinde ilişkiler kurabilir ve işbirliği yapabilir.”

33. 5429 sayılı Kanun’un 53. maddesi şöyledir:

“Bu Kanunun 13 üncü maddesinde yazılı yasaklara aykırı hareket eden kamu görevlileri, 5237 sayılı Türk Ceza Kanununun 258 inci maddesine göre cezalandırılır.

Bu Kanunun 6 ncı maddesinin üçüncü fıkrası ve 14 üncü maddesinde belirtilen yükümlülüklere uymayan gerçek kişilerle özel hukuk tüzel kişilerinin organ ve temsilcilerine adlî para cezası verilir.”

34. 5429 sayılı Kanun’un 54. maddesinin ikinci fıkrası şöyledir:

“Başkanlık veya kurum ve kuruluşlar tarafından Program kapsamında istenen bilgileri, geçerli bir mazereti olmaksızın belirlenen şekil ve sürede vermeyen veya eksik veya hatalı verenler, bir kereye mahsus olmak üzere uyarılarak yedi gün içerisinde bilgileri vermeleri veya eksik ve hataları gidermeleri istenir. Bu uyarıya rağmen, bilgileri hiç vermeyen veya talep edildiği hâlde eksikleri gidermeyen ve hataları düzeltmeyen gerçek kişiler veya özel hukuk tüzel kişilerinin organ ve temsilcileri hakkında, fiilin;

a) Hanehalkı veya bireylerle yapılan araştırmalarda işlenmesi durumunda beşyüz Yeni Türk Lirası,

...

İdarî para cezası uygulanır.”

35. 20/6/2006 tarihli ve 26204 sayılı Resmî Gazete’de yayımlanan Resmî İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkında Yönetmelik’in (Yönetmelik) “Amaç” kenar başlıklı 1. maddesi şöyledir:

“Bu Yönetmeliğin amacı, resmî istatistiklerde veri gizliliğine ve gizli verinin güvenliğinin sağlanmasına ilişkin usul ve esasları düzenlemektir.”

36. Anılan Yönetmelik’in “Tanımlar” kenar başlıklı 4. maddesi şöyledir:

“1) Bu Yönetmelikte geçen;

- a) Başkanlık: Türkiye İstatistik Kurumu Başkanlığını,
- b) Bireysel Veri: Hakkında bilgi toplanan istatistikî birimlerin özellikleri ile birlikte tanımlandığı veriyi,
- c) Doğrudan Tanınma: Bir istatistikî birimin kimliğinin; adı, adresi veya resmen verilmiş ve genel olarak bilinen bir kimlik numarası ile ortaya çıkarılmasını,
- ç) Dolaylı Tanınma: Bir istatistikî birimin kimliğinin, doğrudan tanımlamada yer almayan diğer özelliklerinden faydalanılarak ortaya çıkarılmasını,
- d) Gizli Veri: İstatistikî birimin doğrudan veya dolaylı bir şekilde sahip olduğu özellikleri ile birlikte tanınabilmesine ve bu şekilde bireysel bilgilerin açığa çıkarılmasına imkân sağlayan bireysel veya tablo hâlinde saklı tutulan veriyi,
- e) İstatistik Amaçlı Kullanım: İstatistikî birimlerden toplanan verilerin sadece istatistikî tabloların oluşturulması ve istatistikî analizlerin yapılması için kullanımını,
- f) İstatistikî Birim: Yapılan sayım veya örnekleme çalışmalarına konu olan, hakkında veri toplanacak gerçek ve tüzel kişiler ile kurum ve kuruluşları,
- g) (Değişik:RG-27/10/2010-27742) İş Kayıtları Sistemi: Gayrisafi yurtiçi hasılaya katkısı bulunan, ülke sınırları içerisinde tüm ekonomik faaliyetleri gösteren ve idarî kayıtlarda yer alan tüm işletmeleri ve onlara ilişkin kimlik, tabakalama ve demografik ilişki gibi değişkenleri içeren sistemi,
- ğ) Kanun: 10/11/2005 tarihli ve 5429 sayılı Türkiye İstatistik Kanununu,
- h) Kurum/Kuruluş: Program kapsamında istatistik üreten kurumları/kuruluşları,
- ı) Program: Resmî İstatistik Programını,
- i) Resmî İstatistik: Kurumda veya Programda yer alan konularda istatistik üretecek kurum ve kuruluşlar tarafından derlenen verilerin, kitle özelliklerini ortaya koymak amacıyla işlenmesi ile elde edilen bilgiyi,
- j) Veri: Anket veya idarî kayıtlar yoluyla elde edilen nicel ve/veya nitel istatistikî bilgileri, ifade eder.”

37. Söz konusu Yönetmelik'in “Gizli verinin istisnaları” kenar başlıklı 5. maddesi şöyledir:

“ (1) Resmî istatistik çalışmaları kapsamında kullanılan;

a) Herkese açık kaynaklardan elde edilen veriler ile iş kayıtları sistemi kapsamında bulunan istatistikî birimlerin bu nitelikteki unvan, faaliyet ve adres bilgileri,

b) İstatistikî birimin, bizzat kendisi veya açıkça yetkili kıldığı vekili ya da yetkili kanuni temsilcisinin yazılı onayı ile açıklanmasına izin verdiği sadece kendisine ait bireysel veriler,

gizli veri niteliğinde değerlendirilmez.

(2) (Değişik:RG-27/10/2010-27742) İdarî kayıtların resmî istatistik üretim sürecine dâhil olması hâlinde, bu Yönetmelikte belirtilen gizlilik hükümleri, sadece bu kayıtları tutan kurum ve kuruluşlardan yalnızca istatistik üretmek amacıyla idarî kayıtları olarak kullanan kurum/kuruluşlar için uygulanır. İdarî kayıtların paylaşımında ise bu kayıtları tutan kurum/kuruluşlar kendi mevzuatındaki hükümlere tâbidir.

(3) (Ek:RG-27/10/2010-27742) Dış ticaret istatistiklerinde dolaylı tanınma ile gizlilik kapsamına giren veriler için gizlilik hükümleri, istatistikî birimin kendisine ait verinin gizlenmesini talep eden yazılı başvurusu halinde uygulanır. ”

38. Yönetmelik'in "Tablolaştırılmış veride gizlilik" kenar başlıklı 6. maddesi şöyledir:

“(1) Bireysel veriler, çeşitli özelliklerine göre gruplandırılmaları yoluyla tablolaştırılarak kullanıma açılabilir.

(2) Bireysel verilerin toplulaştırılması ile oluşturulan tablonun herhangi bir hücresindeki bilginin ait olduğu;

a) İstatistikî birim sayısının üçten az olması,

b) İstatistikî birim sayısı üç ve daha fazla olduğu hâlde herhangi bir birime ait bilginin o hücredeki toplam bilginin yüzde sekseninden, iki birime ait bilginin o hücredeki toplam bilginin yüzde doksanından fazlasını oluşturması, durumunda ilgili hücredeki veri gizli kabul edilir.

(3) Gizli verilerin bulunduğu hücre, ancak gizli veriler ortaya çıkmayacak şekilde başka hücre veya hücrelerle birleştirildikten sonra açıklanabilir.”

39. Yönetmelik'in "Gizli verinin korunması" kenar başlıklı 7. maddesi şöyledir:... şöyledir:

“Kurumların/kuruluşların yetkilileri, Programda belirtilen resmî istatistik çalışmalarının, gizli verilerin açıklanmasına imkân vermeyecek şekilde yürütülmesini sağlar, bu verilerin istatistikî amaç dışında kullanılmaması için her türlü önlemi alır ve istatistik üretiminin her aşamasındaki gizli verinin bulunduğu ortama yetkisiz kimselerin fiziksel veya elektronik yollarla erişiminin engellenmesi için gerek duyulan güvenlik sistemlerini belirler ve kullanır.”

40. Yönetmelik'in "Görevlilerin tespiti" kenar başlıklı 8. maddesi şöyledir:

"(1) Gizli verilere yalnızca resmî istatistik üretiminde görev alanlar, görevlerini yerine getirebilmek için ihtiyaç duydukları ölçüde erişebilir.

(2) Kurumlar/kuruluşlar, sorumlulukları altındaki veri derleme, işleme ve saklama çalışmalarını kimlerin yürüteceğini belirleyerek bu görevlilerin hangi ayrıntıdaki veriye ulaşabileceklerini, hangi tarihlerde yetkili olduklarını açık olarak tanımlar ve istatistik üretim sürecinin her aşamasındaki görev değişikliklerinin düzenli olarak kaydını tutar."

41. Yönetmelik'in "Gizli/bireysel verinin paylaşım sınırı" kenar başlıklı 9. maddesi şöyledir:

"(1) Resmî istatistiklerin üretilmesi için veri toplayan ve işleyen görevliler ile toplanan veriden üretilen istatistikleri saklamakla görevli personel, gizli/bireysel veri ile gizli/bireysel veriye ulaşılmasını sağlayacak toplulaştırılmış veriyi istatistik üretim sürecinde görevlendirilenler dışında hiçbir organ, makam, merci veya kişiye veremezler.

(2) Resmî istatistik üretim ve dağıtım sürecindeki görevlilerin bu yükümlülüğü, görevlerinden ayrılmalarından sonra da devam eder.

(3) Gizli veriler idarî, adlî ve askerî hiçbir organ, makam, merci veya kişiye verilemez, istatistik amacı dışında kullanılamaz ve ispat aracı olamaz. "

42. Yönetmelik'in "Bireysel verinin bilimsel amaçlı kullanılması" kenar başlıklı 10. maddesi şöyledir:

"(1) Başkanlık tarafından derlenen ve saklanan bireysel veriler, verinin niteliğine göre, ancak istatistikî birimlerin doğrudan tanınmasına yol açacak bölümleri gizlendikten sonra, veri güvenliğine ilişkin önlemlerin alındığı çalışma ortamında veya doğrudan ve/veya dolaylı tanınmasına yol açacak bölümleri gizlendikten sonra elektronik ortamda, münferit birimlere atıfta bulunmayan bilimsel amaçlı araştırmalarda kullanılması kaydı ve Başkanlığın yazılı izni ile araştırmacıların kullanımına açılabilir. Kullanıcıların çalışma ortamında yaptıkları analizlerin sonuçları, istatistikî birimin dolaylı olarak tanınmasına yol açacak bölümleri gizlendikten sonra verilir.

(2) Birden fazla kurum/kuruluş tarafından ortaklaşa gerçekleştirilen çalışmalarda taraflar arasında imzalanan protokolde aksi belirtilmediği sürece, derlenen bireysel verilerin birinci fıkrada belirtilen esaslara uygun olarak kullanımı ve dağıtımı Başkanlık tarafından gerçekleştirilir. İdarî kayıtların kullanımında ise idarî kaydı tutan kurum/kuruluşların yazılı izni alınır.

(3) Bireysel verileri kullanma hakkını elde edenler, bu hakkı üçüncü şahıslara devredemezler ve elde ettikleri verileri hiçbir kişi veya kuruluşa veremezler. Bu hükümlere uymayanlar hakkında 5429 sayılı Kanunun 53 üncü maddesinde belirtilen ceza hükümleri uygulanır. ”

43. Yönetmelik'in "Gizliliği sağlama taahhüdü" kenar başlıklı 11. maddesi şöyledir:

"Resmî istatistiklerin üretim sürecinin her aşamasında görevlendirilen personele, Kanunda ve bu Yönetmelikte öngörülen gizlilik ilkelerini içeren bir eğitim verilir. Ayrıca, bu personelden Ek-1'de yer alan "Gizlilik Taahhüt Belgesi" alınır. ”

44. Yönetmelik'in "Bilgi taleplerinin karşılanması" kenar başlıklı 12. maddesi şöyledir:

"Kurumlar/kuruluşlar, resmî istatistik çalışmaları kapsamında veri derledikleri istatistikî birimlerin, istatistikî verinin gizliliğinin sağlanması için alınan önlemler ve hakları ile ilgili konularda bilgi taleplerini karşılamakla yükümlüdür."

45. Yönetmelik'in "İstatistikî birimlerin hakları" kenar başlıklı 13. maddesi şöyledir:

"İstatistikî birimler, kendilerine ait gizli verinin izinsiz açıklanması durumunda uğradıkları maddi ve manevi her türlü zararın tazminini isteyebilir. Bu amaçla açılan davalarda Başkanlık veya diğer kurumlar/kuruluşlar aleyhine tazminata hükmedilmesi durumunda, bu hususta kusuru olan memur ve diğer görevlilere genel hükümlere göre rücu edilir."

46. 30/3/2005 tarihli ve 5326 sayılı Kabahatler Kanunu'nun 27. maddesinin (1) numaralı fıkrası şöyledir:

"İdarî para cezası ve mülkiyetin kamuya geçirilmesine ilişkin idarî yaptırım kararına karşı, kararın tebliği veya tefhimi tarihinden itibaren en geç onbeş gün içinde, sulh ceza mahkemesine başvurulabilir. Bu süre içinde başvurunun yapılmamış olması halinde idarî yaptırım kararı kesinleşir."

47. 5326 sayılı Kanun'un 28. maddesinin (10) numaralı fıkrası şöyledir:

"Üçbin Türk Lirası dahil idarî para cezalarına karşı başvuru üzerine verilen kararlar kesindir."

48. Türkiye Büyük Millet Meclisi tarafından 30/1/2016 tarihli ve 6669 sayılı Kanun'la uygun bulunan 28/1/1981 tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "Tanımlar" başlıklı 2. maddesinin birinci fıkrasının (a) bendi şöyledir:

"Bu Sözleşmenin amaçları bakımından:

(a) Kişisel Veriler: Kimliği belirli veya belirlenebilir bir kişi hakkındaki tüm bilgileri ifade eder."

49. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "Verilerin niteliği" başlıklı 5. maddesinin birinci fıkrasının (a) bendi şöyledir:

"Otomatik bilgi işleme konu teşkil eden kişisel nitelikteki veriler:

(a) Meşru ve yasal yoldan elde edilmeli ve işleme tâbi tutulmalıdır;

(b) Belli ve meşru amaçlar için kaydedilmeli ve bu amaca aykırı şekilde kullanılmamalıdır;

(c) Uygun ve elverişli olmalı ve kaydedildikleri amaca göre aşırı olmamalıdır;

(d) Doğru ve icabında güncel olmalıdır;

(e) İlgili kişilerin kimliklerini belirtecek bir biçim altında ve kaydedildikleri nihai amaç için gerekli görülen süreyi aşmayacak bir süre için muhafaza edilmelidir."

50. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "İstisnalar ve kısıtlamalar" kenar başlıklı 9. maddesi şöyledir:

" 1. İşbu maddede belirtilen şuur dışındaki, Sözleşmenin 5, 6 ve 8. maddeleri hükümlerine hiçbir istisna getirilemez.

2. Taraf devletin kanunlarında öngörülmüş olması ve demokratik bir toplumda aşağıdaki hususların sağlanması için gerekli bir önlem oluşturması halinde işbu Sözleşmenin 5, 6 ve 8. maddelerine istisna getirilebilir:

a. Devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi;

b. İlgili kişinin veya başkasının hak ve özgürlüklerinin korunması.

3. İlgili kişilerin özel yaşamlarına tecavüz tehlikesi bulunmadığının açık olduğu durumlarda, 8. maddenin b, c ve d fıkralarında düzenlenen haklar istatistikî veya bilimsel amaçlar için kullanılan kişisel veri dosyaları bakımından kanunla kısıtlanabilir."

51. 5429 sayılı Kanun'un 8. maddesinde yer alan "İstatistikî birimler, kendilerinden istenen veri veya bilgileri, Başkanlığın belirleyeceği şekil, süre ve standartlarda eksiksiz ve doğru olarak ücretsiz vermekle yükümlüdür." hükmü ile 54. maddesinin ikinci fıkrasının (b) bendinin iptali istenmiştir. Anayasa Mahkemesi Genel Kurulunun 20/3/2008 tarihli ve E.2006/167, K.2008/865 sayılı kararıyla, Anayasa'nın 20. ve 25. maddelerinde yer alan güvencelere rağmen itiraza konu 8. madde hükmü bilgi toplama, saklama, işleme ve değiştirme tekeli olan idareye ve diğer kişilere karşı kişilerin korumasız

bırakıldığı, veri toplamanın sınırlarına yasal düzenlemede yer verilmediği, bu nedenle Anayasa'nın 20. ve 25. maddelerine aykırı olduğu gerekçesiyle iptal edilmiştir.

52. Bu iptal kararından sonra anılan hükümler 25/11/2008 tarihli ve 5813 sayılı Kanun'la yeniden düzenlenmiş, 5429 sayılı Kanun'un yeniden düzenlenen 8. maddesi ile 54. maddesinin ikinci fıkrasının (a) bendinde yer alan "Hanehalkı veya bireylerle yapılan araştırmalarda işlenmesi durumunda beşyüz Yeni Türk Lirası," ibaresinin, Anayasa'nın 20. maddesine aykırılığı iddiasıyla iptali istenmiştir. Anayasa Mahkemesi Genel Kurulunun 12/10/2011 tarihli ve E.2010/12, K.2011/135 sayılı kararıyla iptal istemi reddedilmiştir. Kararın gerekçesinin ilgili kısmı şöyledir:

"İtiraz konusu kurullarla istatistiklerin kamu yararı için önemi dikkate alınarak bireylere mecburi ve ücretsiz kamusal bir külfet yüklenmiştir. Karşılaştırmalı hukukta da bazı ülkelerde bireylere istatistik amaçlı bilgi verme yükümlülüğü getirildiği görülmektedir. Modern bir devlette kamu hizmetlerinin planlanması ve kamu güvenliğinin sağlanabilmesi için bireylerin kendileriyle ilgili pek çok bilgiyi kamu otoritelerine verme yükümlülüğü bulunmaktadır. Bu bilgilerin istatistik amacıyla toplanmış olması bilgi toplamayı kendiliğinden Anayasa'ya aykırı hale getirmez.

5429 sayılı Kanun'un 8. maddesinin eski düzenlemesini Anayasa Mahkemesi 20.3.2008 tarih ve E.2006/167, K.2008/86 sayılı kararıyla, hiçbir sınırlama öngörmeksizin istatistikî birimlere istenilen bilgileri verme yükümlülüğü getirmesi nedeniyle Anayasa'nın 20. ve 25. maddelerine aykırı olarak iptal etmiştir. Bu iptal kararından sonra 5813 sayılı Kanun'la getirilen düzenleme ile 8. maddede bilgi verme yükümlülüğünün sınırı Anayasa'da belirlenen temel hakların ve ödevlerin ihlal edilmemesi olarak belirlenmiştir. Anayasa'nın 20. maddesinde herkesin özel hayatına ve aile yaşayışına saygı gösterilmesini isteme hakkına sahip olduğu; 24. maddesinde kimsenin dini inanç ve kanaatlerini açıklamaya zorlanamayacağı; 25. maddesinde de herkesin düşünce ve kanaat özgürlüğüne sahip olduğu, her ne sebep ve amaçla olursa olsun kimsenin düşünce ve kanaatlerini açıklamaya zorlanamayacağı hüküm altına alınmıştır. Bunlar gibi, Anayasanın diğer maddelerinde güvence altına alınan hak ve ödevler gözetilerek bilgi talep edilebilecektir. İstenilen bilgilerin bu nitelikte olduğunu düşünen istatistikî birimler, nedenini açıklayarak bilgi vermekten kaçınabileceği gibi haklarında idari para cezası uygulanması halinde buna itiraz ederek istenilen bilginin temel haklarını ihlal edecek nitelikte olduğunu mahkemeler önünde de ileri sürebilirler.

5429 sayılı Kanun'un 54. maddesinin ikinci fıkrasında, istatistikî birimlerin kendilerinden istenen bilgileri geçerli bir mazereti olmaksızın belirlenen şekil ve sürede, eksiksiz ve hatasız olarak vermek zorunluluğuna uyulmaması idari para cezası yaptırımına bağlanmıştır. Bu durumda dava konusu iki hüküm birlikte değerlendirildiğinde bireylerin temel haklarının korunmasının idari ve adli

makamların sorumluluğuna bırakıldığı görülmektedir. İdari makamlar bireyin temel haklarını ihlal edecek şekilde bilgi talep etmeme yükümlülüğündedirler. İdari makamların bu ödevini yerine getirmemesi halinde istatistikî birimler haklarını yargı makamları önünde arayabileceklerdir. Bu durumda itiraz konusu kurullarla bireyin hakları ile kamu yararı arasında makul bir denge kurulduğu ve bireylerin haklarına ölçsüz bir müdahaleye izin verilmediği anlaşıldığından Anayasanın 2. maddesindeki hukuk devleti ilkesine aykırılık görülmemiştir. ”

IV. İNCELEME VE GEREKÇE

53. Mahkemenin 21/9/2016 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları

54. Başvurucu, TÜİK yetkileri tarafından gerçekleştirilen Hanehalkı Bütçe Anketi çalışmalarında konutunun istatistikî birim olarak seçildiğini, kendisinin fiilî imkânsızlıklar nedeniyle anket çalışmasına katılmaktan muaf tutulması talebinin reddedildiğini, söz konusu anket çalışması kapsamında günlük olarak alışveriş yaparken hangi markaları tercih ettiği, düzenli aylık harcamaları, taksit ve borç ödemeleri ve bunun gibi özel hayatının gizliliğine müdahale niteliğindeki soruları cevaplandırmaya karşı çıkararak anket çalışmasına katılmadığını, bu nedenle idari para cezasıyla cezalandırıldığını, TÜİK tarafından ankete katılmasının zorunlu tutulması sebebiyle Anayasa'nın 20. maddesinde tanımlanan özel hayata saygı hakkı ile 25. maddesinde düzenlenen düşünce ve kanaat hürriyetinin ihlal edildiğini ileri sürmüştü; ihlalin tespiti talebinde bulunmuştur.

B. Değerlendirme

55. Yukarıda belirtildiği üzere başvurucunun katılması istenen söz konusu ankette, ailedeki aynı gelir elde eden kişilerin ad ve soyadları, elde edilen aynı gelirin kaynağı, aynı gelirin elde edilme sıklığının, haneye gelen hediye ve yardımlar ile haneden başka hanelere yapılan yardımlar ve verilen hediyelerin belirtilmesi, bir ay boyunca yapılan tüm harcamaların marka, ölçü, miktar, alışverişin yapıldığı yer gibi detaylarının bir ay süreyle listelenmesinin istendiği, herhangi bir konuda kişisel düşünce ve kanaatlerine dair soruların bulunmadığı anlaşılmıştır. Bu nedenle başvurucunun iddiaları Anayasa'nın 20. maddesi kapsamında incelenmiştir.

1. Kabul Edilebilirlik Yönünden

56. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan özel hayata saygı hakkının ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

2. Esas Yönünden

57. Başvurucu, özel hayata saygı hakkının ihlal edildiğini ileri sürmüştür.

58. Bakanlık görüşünde, toplumun menfaatleri ile bireyin menfaatlerinin çatıştığı durumlarda adil denge gözetilirken devletin takdir alanının varlığının kabulü gerektiği, somut olayda kişiden bir ay boyunca yaptığı tüm harcamaların listesini yapmasını istemenin demokratik toplumda gerekli olup olmadığı konusunda takdirin Anayasa Mahkemesine ait olduğu belirtilmiştir.

59. Başvurucu, Bakanlık görüşüne verdiği cevapta önceki iddialarını tekrar etmiştir.

i. Genel İlkeler

60. Anayasa'nın "Özel hayatın gizliliği" kenar başlıklı 20. maddesi şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

61. Özel hayat kavramı eksiksiz bir tanımı bulunmayan geniş bir kavramdır. Bu kapsamda korunan hukuki değer esasen kişisel bağımsızlık olup bu koruma bir taraftan herkesin istenmeyen bütün müdahalelerden uzak kendine özel bir ortamda yaşama hakkına sahip olduğuna işaret etse de diğer taraftan özel hayat kavramının herkesin kişisel yaşamını istediği şekilde sürdürme ve dış dünyayı bu çemberden ayrı tutma kavramına indirgenemeyeceği açıktır. Bu açıdan Anayasa'nın 20. maddesi özel bir sosyal hayat sürdürmeyi güvence altına almaktadır (Serap Tortuk, B. No: 2013/9660, 21/1/2015, Ş 31).

62. Özel hayata saygı hakkı kapsamında korunan hukuksal çıkarlardan biri de bireyin mahremiyet hakkıdır. Ancak mahremiyet hakkı sadece yalnız bırakılma hakkından ibaret olmayıp bu hak, bireyin kendisi hakkındaki bilgileri kontrol edebilme hukuksal çıkarını da kapsamaktadır. Bireyin kendisine ilişkin herhangi bir bilginin kendi rızası olmaksızın açıklanmaması, yayılmaması, bu bilgilere başkaları tarafından ulaşılamaması ve rızası hilafına kullanılmaması, kısaca bu bilgilerin mahrem kalması konusunda menfaati bulunmaktadır (Serap Tortuk, § 32). Bu husus, ilk defa Federal Almanya Anayasa Mahkemesinin Nüfus Sayımı Kanunu kararında ifade edilen "bireyin kendisi hakkındaki bilgilerin geleceğini belirleme hakkı"na işaret etmektedir (Federal Almanya Anayasa Mahkemesi, Nüfus Sayımı Kanunu kararı, BVerfGE, 65, 1 - Volkszählung, 15/12/1983; Küzeci, Elif, İnsan Hakları Yıllığı, Cilt 32, 2014, s. 53-75; AYM, E. 2010/40, K. 2012/8, 19/1/2012; E. 1986/24, K. 1987/8, 31/3/1987).

63. Anayasa'nın 20. maddesinde herkesin, özel hayatına saygı gösterilmesi hakkına sahip olduğu ve özel hayatın gizliliğine dokunulamayacağı belirtilmektedir. Kamu makamlarının özel hayata saygı hakkına keyfi bir şekilde müdahale etmelerinin önlenmesi, Anayasa'nın 20. ve Avrupa İnsan Hakları Sözleşmesi'nin (Sözleşme) 8. maddesi ile sağlanan güvenceler kapsamında yer almaktadır. Özel hayata saygı hakkının kapsamında olan bireylerin kişisel verilerinin korunması hakkı, Anayasa'nın 20. maddesinde açık olarak düzenlenmiştir.

64. Anayasa Mahkemesi kararlarında da belirtildiği üzere kişisel veri -belirli veya kimliği belirlenebilir olmak şartıyla- bir kişiye ilişkin bütün bilgileri ifade etmekte olup ad, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgilerin değil telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, öz geçmiş, resim, görüntü ve ses kayıtları, parmak izleri, sağlık bilgileri, genetik bilgiler, IP adresi, e-posta adresi, alışveriş alışkanlıkları, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm verilerdir (AYM, E.2014/74, K.2014/201, 25/12/2014; E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2013/84, K.2014/183, 4/12/2014; E.2014/180, K.2015/30, 19/3/2015; Bülent Kaya [GK], B. No: 2013/2941, 11/5/2016, § 49).

65. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin 2. maddesinde de kişisel bilgi, belirli veya belirlenebilir bir kişiye ilişkin herhangi bir bilgi olarak tanımlanmaktadır.

ii. Genel İlkelerin Somut Olaya Uygulanması

a. Müdahalenin Varlığı

66. Somut olayda başvuru; kendisinin ve aile bireylerinin adları, adresi, maddi durumları, gelirlerinin kaynağı, aylık harcamaları, mal ve hizmet tercihleri konusunda detaylı bilgiler vermesini gerektiren ankete katılmayı reddetmesi nedeniyle idari para cezasıyla karşılaşmıştır. Kamu makamlarının başvuruyla ilgili öğrenmek istediği söz konusu kişisel bilgilerin, kimliği belirlenmiş ya da belirlenebilecek kişilerle ilgili olmasından dolayı özel hayata saygı hakkı kapsamında kişisel nitelikli veriler olduğu anlaşılmaktadır.

67. Kamu mercileri tarafından özel yaşamı ile ilgili sorular sorulması da dahil olmak üzere, bir bireyin özel hayatı, iş ve sosyal yaşamıyla ilgili bilgilerinin, parmak izinin, fotoğrafının, hücre ve DNA örneklerinin alınması, kaydedilmesi, saklanması ve kullanılması özel hayata saygı hakkına müdahale oluşturur (Bülent Kaya, § 51). (Benzer yöndeki AİHM kararları için bkz. Leander/ İsviçre, B. No: 9248/81, 26/3/1987, § 48; Kopp/İsviçre, B. No: 23224/94, 25/3/1998, § 53; Amann/İsviçre [BD], B. No: 27798/95, 16/2/2000, § 69; Rotaru/Romanya [BD], B. No: 28341/95, 4/5/2000, §§ 43, 44, 46).

68. Kaydedilen bilgilerin daha sonra kullanılmış olup olmamasının bir önemi yoktur. Bununla birlikte kamu makamları tarafından muhafaza edilen kişisel nitelikli bilgilerin özel yaşam unsurlarından birini devreye sokup sokmadığını tespit etmek için bu bilgilerin hangi çerçevede alındıklarının ve muhafaza edildiklerinin, verilerin türünün, kullanıldıkları ve işlendikleri şekli, bunlardan çıkarılabilecek sonuçların dikkate alınması zaruridir (Bülent Kaya, § 53).

69. Somut olayda kamu makamları tarafından başvuru; adı, adresi, gelir kaynakları, tüketim alışkanlıkları ve ekonomik durumuna yönelik kişisel verileri vermeye zorlanması, bilgileri vermemesi üzerine hakkında idari para cezası uygulanması suretiyle Anayasa'nın 20. maddesinde güvence altına alınmış özel hayata saygı hakkına müdahalede bulunulduğu anlaşılmaktadır.

b. Müdahalenin İhlal Oluşturup Oluşturmadığı

70. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Avrupa Konseyi Sözleşmesi'nin 9. maddesinde devlet güvenliği, kamu güvenliği, devletin ekonomik menfaatlerinin korunması ve suçlarla mücadele edilmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması ile verilerin istatistiki veya bilimsel amaçlarla kullanılması gibi durumlarda kişisel verilerin korunmasına sınırlamalar getirilebileceği öngörülmüştür.

71. Anayasa'nın 20. maddesinin ikinci fıkrasında, çeşitli nedenlerle özel hayata saygı hakkına sınırlamalar getirilebileceği belirtilerek bu hakkın mutlak olmadığı kabul edilmiştir (Serap Tortuk, § 38).

72. Anayasa'nın 20. maddesinin üçüncü fıkrasında ise herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme, bu veriler hakkında bilgilendirilme, verilere erişme, bunların düzeltilmesini veya silinmesini talep etme, verilerin amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkına sahip olduğu, kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hükmüne yer verilerek anayasal sınırlar belirtilmiştir.

73. Anayasa'nın "Temel hak ve hürriyetlerin sınırlanması" kenar başlıklı 13. maddesi şöyledir:

"Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz."

74. Belirtilen Anayasa hükmü, hak ve özgürlükleri sınırlama ve güvence rejimi bakımından temel öneme sahip olup Anayasa'da yer alan bütün hak ve özgürlüklerin yasa koyucu tarafından hangi ölçütler gözönünde bulundurularak sınırlandırılabilceğini ortaya koymaktadır. Anayasanın bütünselliği ilkesi çerçevesinde Anayasa kurallarının bir arada ve hukukun genel kuralları gözönünde tutularak uygulanması zorunlu olduğundan belirtilen düzenlemede yer alan başta kanun ile sınırlama kaydı olmak üzere tüm güvence ölçütlerinin, Anayasa'nın 20. maddesinde yer verilen hakların kapsamının belirlenmesinde de gözetilmesi gerektiği açıktır (Sevim Akat Eşki, B. No: 2013/2187, 19/12/2013, § 35).

75. Dolayısıyla özel hayata saygı hakkına yapıldığı iddia edilen müdahalelerin incelemesinde kanunilik ve müdahaleyi haklı kılan sebeplerin var olup olmadığı her somut olayın kendi koşulları içinde değerlendirilmelidir.

i. Kanunilik

76. Hak ve özgürlüklerin kanunla sınırlanması ölçütü Anayasa yargısında önemli bir yere sahiptir. Hak ya da özgürlüğe bir müdahale söz konusu olduğunda öncelikle tespiti gereken husus, müdahaleye yetki veren bir kanun hükmünün yani müdahalenin hukuki bir temelini mevcut olup olmadığıdır (Sevim Akat Eşki, § 36).

77. Somut olayda başvuru idari para cezasıyla tecziyesinin dayanağı 5429 sayılı Kanun'un 8. ve 54. maddeleridir. Söz konusu 8. maddede, yapılan sayım veya örnekleme çalışmalarına konu olan hakkında veri toplanacak gerçek ve tüzel kişiler ile kurum ve kuruluşların (istatistiki birim) Anayasa'da belirlenen temel haklar ve ödevler çerçevesinde kendilerinden istenen veri veya bilgileri,

Başkanlığın belirleyeceği şekil, süre ve standartlarda eksiksiz ve doğru olarak ücretsiz vermekle yükümlü oldukları düzenlenmiştir.

78. Kanun'un 54. maddesinde istenen bilgileri, geçerli bir mazereti olmaksızın belirlenen şekil ve sürede vermeyen veya eksik veya hatalı verenlerin, bir kereye mahsus olmak üzere uyarılarak yedi gün içerisinde bilgileri vermeleri veya eksik ve hataları gidermelerinin isteneceği, bu uyarıya rağmen bilgileri hiç vermeyen veya talep edildiği hâlde eksikleri gidermeyen ve hataları düzeltmeyenler hakkında idari para cezası uygulanacağı düzenlenmiştir.

79. 5429 sayılı Kanun'da ülkenin ekonomi, sosyal, demografi, kültür, çevre, bilim, teknoloji ve ihtiyaç duyulan diğer alanlardaki resmî istatistikleri üretmek üzere Anayasa'da belirlenen temel haklar ve ödevler çerçevesinde kişilerden bilgi isteneceği, bu bilgilerin toplanma, kaydedilme ve saklanma esas ve usulleri detaylı olarak düzenlenmiştir. Anılan Kanun'da söz konusu bilgilerin güvenilirlik, tutarlılık, tarafsızlık, istatistiki gizlilik, güncellik ve şeffaflık ilkelerine göre hazırlanacağı, resmî istatistiklerin gerçekleri yansıtmasının sağlanması, tüm kullanıcılara tarafsız ve eş zamanlı olarak sunulması, gizlilik ilkesine riayet edilmesinin esas olduğu düzenlenmiştir. Kişilerden elde edilen istatistiki bilgilerin kimlere, hangi koşullarda verilebileceği, bilgilerin gizliliği, gizliliğin ihlali durumunda yargı yolunun açık olduğu ve kurumun tazminat yükümlülüğü gibi konularda ayrıntılı düzenlemelere yer verilmiştir. Anılan hükümlerle elde edilecek bilgilerin amacı dışında kullanılmasını önleyecek ve kişilerin özel hayatına dair bilgilerin ve kişisel verilerin ifşa edilmesini önleyecek yasal güvencenin sağlandığı görülmektedir.

80. Bu kapsamda somut olayda başvurusunun özel hayatına saygı hakkına yapılan müdahalenin kanuni bir dayanağının mevcut olduğu anlaşılmaktadır. Anılan Kanun hükümlerinin yeterli açıklıkta hükümler içerdiği, başvuru açısından yeterli derecede ulaşılabilir ve öngörülebilir olduğu kanaatine varılmıştır. Bu durumda söz konusu düzenlemelerin "kanunilik" ölçütünü karşıladığı sonucuna varılmıştır.

ii. Meşru Amaç

81. 5429 sayılı Kanun'un 1. ve 8. maddeleri, müdahalenin amacını belirlemede yol gösterici niteliktedir. "Amaç" kenar başlıklı 1. maddede yer alan düzenlemede ülkenin ihtiyaç duyduğu alanlarda veri ve bilgilerin derlenmesi, değerlendirilmesi, gerekli istatistiklerin üretilmesi amacıyla yer verilmiş; Kanun'un 8. maddesinde de ülkenin ekonomi, sosyal, demografi, kültür, çevre, bilim, teknoloji ve ihtiyaç duyulan diğer alanlardaki resmî istatistikleri üretmek üzere Anayasa'da belirlenen temel haklar ve ödevler çerçevesinde kişilerden bilgi isteneceği düzenlenmiştir.

82. Söz konusu düzenlemeler, kamu düzeni, ülkenin ekonomik refahı amaçlarına yöneliktir. Bu kapsamda somut müdahalenin temelini oluşturan kanuni düzenlemelerin Anayasa'nın 20. maddesi ve Sözleşme'nin 8. maddesi çerçevesinde meşru bir amaca dayalı olduğu sonucuna varılmıştır.

iii. Demokratik Bir Toplumda Gerekli Olma ve Ölçülülük

83. Kişisel verilerin korunması, kişisel bilgileri sınırsız şekilde toplayabilen ve kullanabilen günümüz bilişim teknolojileri karşısında savunmasız ve zayıf hâle gelen bireyin korunmasını amaçlamakta olup Anayasa Mahkemesi kararlarında belirtildiği gibi kişisel verilerin korunması hakkı, insan onuru ve kişiliğin serbestçe geliştirilmesi hakkına dayanmaktadır (AYM,E.2014/122, K. 2015/123, 30/12/2015, § 20).

84. Kişisel verilerin korunması kişinin maddi ve manevi varlığını geliştirmesine imkân tanıyarak bireyin hayatını kendi özgür iradesiyle düzenlemesine katkı sağlamaktadır. Bireyin kişisel verileri üzerindeki hakkı yeteri kadar korunmazsa kişiliğini serbestçe geliştirmesi zora gireceğinden özgür iradeleriyle yaşamlarını biçimlendiren bireylerden oluşan demokratik bir toplum düzeninin ortaya çıkması ve korunması da güçleşecektir. Kişinin maddi ve manevi varlığını geliştirmesi ancak ve ancak faaliyetlerini özgürce gerçekleştirmesi ile mümkündür. Kişisel verilerin korunmasıyla, kişisel veri toplanması, saklanması ve işlenmesi sırasında bireyin hak ve özgürlüklerinin korunarak demokratik toplum düzeninin oluşmasına katkı yapmak hedeflenmektedir (Federal Almanya Anayasa Mahkemesi, Nüfus Sayımı Kanunu kararı, BVerfGE, 65, 1 - Volkszählung, 15/12/1983)

85. Kural olarak bireyin özel hayatını kendi tercihleri ile nasıl şekillendirdiği, bir başka kişinin veya devletin ilgi alanına girmemelidir. Yaşam ilişkilerine ait tüm kişisel verilerinin kapsamlı bir kaydı tutulan ve özel yaşamının gizliliği adeta ortadan kalkan bireyin kişiliğini geliştirmesi mümkün değildir. Kişisel verilerin korunması hakkı ihlal edildiğinde bireyin diğer temel hak ve özgürlükleri kullanması zorlaşmaktadır. Kayıt altına alınan veya alındığını düşünen birey kendi özgür kişiliğinin gereği gibi değil kendisinden istenilen veya beklenen davranış tarzıyla hareket edecektir. Bireyler çeşitli faaliyetlerinin devlet tarafından izleneceği endişesiyle bunları gerçekleştirmekten vazgeçebilirler. Aykırı hareket tarzlarının sürekli kayıt altına alındığını düşünen birey, örneğin örgütlenme, toplantı ve düşünce özgürlüklerini kullanmama eğilimine girecektir. Eğer insanlar seyahat etmek, iletişimde bulunmak gibi belli eylemlerin hükümet tarafından yakından izleneceğini düşünürlerse, bu eylemleri gerçekleştirmekten kaçınabilirler ve yasal faaliyetlerinde kendi kendilerini sınırlama eğilimine girebilirler. Bu durum kişinin özerkliğini etkileyerek yurttaşların özgür iradeleriyle kendi yaşamlarını belirleyebildikleri özgürlükçü demokratik esaslara dayanan bir

toplum düzeninin oluşmasını engelleyecektir (Federal Almanya Anayasa Mahkemesi, Nüfus Sayımı Kanunu kararı, BVerfGE, 65, 1 - Volkszählung, 15/12/1983).

86. Kişisel verilerin korunmasına yönelik uluslararası sözleşmelerle kişisel verilerin korunması ve bireyin kendisi hakkındaki bilgilerin geleceğini belirleme hakkı kapsamında gerekli olan temel ilkelere bu amaçla düzenlenen kanunlarda bulunması zorunlu olan hususlar belirlenmiştir. Buna göre kişisel veriler, Kanun'la açıklanan hallerle sınırlı olarak ve belirli amaçlar için toplanmalı, yalnızca bu amaçlar doğrultusunda kullanılmalı ve verilerin gelecekte başka amaçlar için kullanılması önlenmelidir. Bireylere kurum ve kuruluşlarca kendileri hakkında bilgi toplandığı konusunda bilgilendirilme, bunun yanında söz konusu bilgilere erişme, yanlış bilgileri düzeltme, hukuka aykırı şekilde işlenmiş olanları sildirme hakları tanınmalıdır. Bildirim, düzeltme veya silme talebinin yerine getirilmemesi hâlinde etkili bir başvuru yolundan yararlanma imkânı verilmelidir. Çeşitli kurum ve kuruluşlar tarafından kişisel verileri hukuka uygun olarak kayıt altında tutulan kişilerin, bu verilerin daha sonra üçüncü kişilerle paylaşılması konusunda rızalarının alınması sağlanmalıdır (bkz. § 47; Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi).

87. Anayasa'nın 20. maddesinde kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hükmü bulunmasına rağmen anılan maddenin çıkarılmasını öngördüğü kanun başvuruya konu işlemin tesis edildiği tarihte çıkarılmamış olup söz konusu Kanun 24/3/2016 tarihinde kabul edilmiştir (24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu). Bu nedenle anılan Kanun hükümlerinin başvuru konusu dosya bakımından dikkate alınması mümkün değildir. Bununla birlikte somut olayda müdahalenin 5429 sayılı Türkiye İstatistik Kanunu'na dayandığı ve anılan Kanun'un "kanunilik" ölçütünü karşıladığı yukarıda ortaya konulmuştur.

88. Öte yandan sosyal devletin gereği olarak ekonomik ve sosyal gelişmenin sürekliliğini sağlamak için bu alanlara yönelik kapsamlı, doğru ve güncel bilgilerin elde edilmesine ihtiyaç vardır. Bu konuda istatistik bilim dalından faydalanmak objektif ve rasyonel sonuçlara ulaşılmasında çok önemli ve etkilidir. Bu nedenle modern devletler istatistik çalışmalarına önem vermekte ve bu çalışmaların sonuçlarından yararlanmaktadır.

89. 5429 sayılı Kanun'un Anayasa Mahkemesinin iptal kararının ardından yeniden düzenlenmiş olan 8. maddesinde, bireylere kendilerinden istenilen bilgileri vermek yükümlülüğü getirilmekle birlikte, bilgi verme yükümlülüğünün sınırı Anayasa'da belirlenen temel hakların ve ödevlerin ihlal edilmemesi olarak belirlenmiştir. Bu çerçevede Anayasa Mahkemesi Genel Kurulunun 12/10/2011 tarihli ve E.2010/12, K.2011/135 sayılı kararının gerekçesinde de belirtildiği üzere istenilen bilgilerin

Anayasa'da güvence altına alınan temel hak ve özgürlüklere -somut olayda özel hayata saygı hakkına- müdahale niteliğinde olduğunu düşünen bireyler (istatistiki birimler) nedenini açıklayarak bilgi vermekten kaçınabilirler.

90. Bireyin temel haklarına yapılan müdahale ile bu müdahaleyle güdülen meşru amaç arasında bir orantı bulunması zorunludur. Anayasa'nın 13. maddesinde bu orantının değerlendirilmesi noktasında dikkate alınmak üzere demokratik toplumda gereklilik, hakkın özü ve ölçülülük unsurlarına riayet edilmesi şeklinde üç ayrı güvence ölçütüne daha yer verilmiştir (Marcus Frank Cerny [GK], B. No: 2013/5126, 2/7/2015, § 70).

91. Avrupa İnsan Hakları Mahkemesi (AİHM) içtihatlarında ifade edilen demokratik toplumda zorunluluk kavramı, müdahale teşkil eden eylemin acil bir toplumsal ihtiyaçtan kaynaklanması ve takip edilen meşru amaç bakımından orantılı olması unsurlarını içermektedir. Bir müdahalenin orantılı olduğunun kabul edilebilmesi için söz konusu temel hakka daha az zarar verebilecek ancak aynı zamanda güdülen amacı da yerine getirebilecek nitelikte olan yöntemin tercih edilmiş olması gerekmektedir (Nada/İsviçre, B. No: 10593/08, 12/9/2012, § 183; Silver ve diğerleri/Birleşik Krallık, B. No: 5947/72, 25/3/1983, § 97).

92. Hakkın özü, dokunulduğunda söz konusu temel hak ve özgürlüğü anlamsız kılan asli çekirdeği ifade etmekte olup bu yönüyle her temel hak açısından kişiye dokunulmaz asgari bir alan güvencesi sağlamaktadır. Bu çerçevede hakkın kullanılmasını önemli ölçüde güçleştiren, hakkı kullanılamaz hâle getiren veya ortadan kaldıran sınırlamaların, hakkın özüne dokunduğu kabul edilmelidir. Özel hayata saygı hakkı bağlamında da bu hakkın ortadan kaldırılması, kullanılamaz hâle getirilmesi veya kullanılmasının aşırı derecede güçleştirilmesi sonucunu doğuran müdahalelerin bu hakkın özünü zedeleyeceği açıktır. Ölçülülük ilkesinin amacı da temel hak ve özgürlüklerin gereğinden fazla sınırlandırılmasının önlenmesidir. Anayasa Mahkemesi kararları uyarınca ölçülülük ilkesi, sınırlama için kullanılan aracın sınırlama amacını gerçekleştirmeye uygun olmasını ifade eden elverişlilik, sınırlayıcı önlemin sınırlama amacına ulaşmak bakımından zorunlu olmasına işaret eden zorunluluk ve araçla amacın orantsız bir ölçü içinde bulunmaması ile sınırlamanın ölçüsüz bir yükümlülük getirmemesini ifade eden oranlılık unsurlarını içermektedir (AYM, E.2012/100, K.2013/84, 4/7/2013; Marcus Frank Cerny, § 72).

93. Belirtilen ölçütlere riayetle bir sınırlandırma yapıp yapılmadığının tespiti için müdahale teşkil eden önlemin temelini oluşturan meşru amaç karşısında, bireye düşen fedakârlığın ağırlığının gözönünde bulundurulması ve gözetilen toplumun genel yararının gerekleri ile bireyin temel hakkının korunması arasında adil bir dengenin kurulup kurulmadığının belirlenmesi zorunludur.

Anayasa'nın 13. maddesi vasıtasıyla Anayasa'da yer alan tüm temel hak ve özgürlüklerin sınırlandırılması hususunda geçerli olan bu denge, özel hayata saygı hakkının sınırlandırılmasında da gözönünde bulundurulmalıdır (Marcus Frank Cerny, § 73).

94. Başvuru konusu olay bakımından yapılacak değerlendirmenin temel eksenini, müdahaleye neden olan idare ve derece mahkemelerinin kararlarında dayandıkları gerekçelerin özel hayata saygı hakkını kısıtlama bakımından "demokratik bir toplumda gerekli" ve "ölçülülük ilkesi"ne uygun olduğunun inandırıcı bir şekilde ortaya konup konamadığı olacaktır. Bu çerçevede bir müdahale, meşru amaçla orantılı bir müdahale olmalıdır. İkinci olarak müdahalenin haklılığı için kamu makamlarının gösterdikleri gerekçeler konuyla ilgili ve yeterli olmalıdır (Marcus Frank Cerny, § 83).

95. Somut olayda başvuru, idarenin 8/10/2013 tarihli yazısıyla ankete katılmaması hâlinde idari para cezasıyla cezalandırılacağı yönünde ihtar edilmiştir. Başvuru 24/10/2013 tarihinde mazeret dilekçesi vererek anket çalışmasına katılmak istemediğini belirtmiş, idare 25/10/2013 tarihli yazısıyla başvuru talebini zımnen reddederek idari para cezasına dair ihtarını yinelemiştir. Tanınan süre içinde söz konusu ankete cevap vermemesi üzerine başvuru 7/11/2013 tarihli işleme idari para cezasıyla tecziye edilmiştir. Başvurucunun anılan işleme itirazı, İstanbul 28. Sulh Ceza Mahkemesince cezanın mevzuata uygun olduğu gerekçesiyle reddedilmiştir.

96. Toplumun tüketim harcamaları ile ekonomik düzeyinin belirlenmesi ve tespit edilen veriler ışığında devletin kamu güvenliği ve planlı kalkınma hususlarında ihtiyaç duyulan tedbirleri alması için hane halklarına yönelik anket yapılması demokratik bir toplumda gerekli olarak görülebilir.

97. Belli bir toplumda yaşayan kişilerin o toplumun ihtiyaçlarını karşılayacak bazı ödevlerle sorumlu tutulabilmesi olağandır. Bireylerin birlikte yaşamanın gerektirdiği bazı ödevlere katılmaları gerekebilir. Somut olayda başvuru kamu yararına olarak bazı verilerin toplanması konusunda ankete katılım ödevi ile sorumlu tutulmuştur. Ankette özel hayata ilişkin bilgiler istenilmekle birlikte Kurum başvurucuya bu bilgilerin gizliliği konusunda gerekli yasal güvencelerin sağlandığını bildirmiştir. Başvuru bunun aksini ileri sürmemektedir. Bu hususlar dikkate alındığında ankete katılımın zorunlu tutulmasının demokratik bir toplumda gerekli olmadığı söylenemez.

98. Bunun yanı sıra başvuru, sanatçı olması nedeniyle iş yoğunluğunu ve iki çocuğuna bakmasını gerekçe göstererek ankete katılımın kendisine ağır külfet getirdiğini, anketörlerin ev ziyareti nedeniyle özel hayatın gizliliğinin ihlal edildiğini ileri sürmektedir. Anketörlerle toplamda sekiz görüşme yapılması ve tüketim harcamalarına ilişkin kayıt tutma zorunluluğu bulunmakla birlikte anket bir ay ile sınırlıdır. Toplumda sınırlı sayıda kişinin hayatlarında belki de bir defa katlanacakları böyle bir yükümlülüğün bireylere başlı başına aşırı külfet yüklediği söylenemez. Diğer taraftan

ankette toplumun farklı katmanlarındaki kişilerin gelir ve harcama durumlarına ilişkin bilgilere ihtiyaç duyulmaktadır. Başvurucunun mazeretleri içinde bulunduğu toplum katmanında başka herhangi bir kişinin de dile getirebileceği mazeretlerdir. Bunların kabul edilmesi hâlinde başvurucunun içinde bulunduğu toplum katmanından herhangi bir kişiyle anket çalışması yapılması neredeyse imkânsız olacaktır. Önemli ekonomik verilere temel olan anket çalışmalarının kamu gücünün belli bir zorlaması olmadan yapılabilmesi oldukça zordur.

99. Son olarak uygulanan yaptırım, başvurucunun ekonomik ve sosyal durumu dikkate alındığında oldukça düşük miktarda bir idari para cezasıdır. Dolayısıyla müdahalenin ölçülü olduğu sonucuna varılmıştır.

100. Açıklanan nedenlerle Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkının edilmediğine karar verilmesi gerekir.

V. HÜKÜM

Açıklanan gerekçelerle;

- A.** Özel hayata saygı hakkının ihlal edildiğine ilişkin iddianın **KABUL EDİLEBİLİR OLDUĞUNA,**
- B.** Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkının **İHLAL EDİLMEDİĞİNE,**
- C.** Yargılama giderlerinin başvurucu üzerinde **BIRAKILMASINA,**
- D.** Kararın bir örneğinin Adalet Bakanlığına **GÖNDERİLMESİNE 21/9/2016 tarihinde OYBİRLİĞİYLE** karar verildi.

Anayasa Mahkemesi - Asım Bayar ve Veysel Bayar (Unutulma Hakkı) Kararı (2014/4141)

Asım Bayar ve Veysel Bayar, B. No: 2014/4141, 4/10/2017

Başvuru, ulusal ölçekte yayın yapan bir gazetenin İnternet haber arşivinde erişilebilir durumda olan haber ile ilgili içeriğe erişimin engellenmesi yönündeki taleplerin reddedilmesi nedeniyle şeref ve itibarın korunması hakkının ihlal edildiği iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

İKİNCİ BÖLÜM

KARAR

ASIM BAYAR VE VEYSEL BAYAR BAŞVURUSU

(Başvuru Numarası: 2014/4141)

Karar Tarihi: 4/10/2017

İKİNCİ BÖLÜM

KARAR

Başkan: Engin YILDIRIM

Üyeler: Serdar ÖZGÜLDÜR, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ

Raportör Yrd.: Derya ATAKUL

Başvurucular: 1. Asım BAYAR; 2. Veysel BAYAR

Vekili: Av. Ali Fuat YILDIZ

I. BAŞVURUNUN KONUSU

1. Başvuru, ulusal ölçekte yayın yapan bir gazetenin İnternet haber arşivinde erişilebilir durumda olan haber ile ilgili içeriğe erişimin engellenmesi yönündeki taleplerin reddedilmesi nedeniyle şeref ve itibarın korunması hakkının ihlal edildiği iddiasına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 20/3/2014 tarihinde yapılmıştır.

3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.

4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.

5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.

III. OLAY VE OLGULAR

6. Başvuru formu ve eklerinde ifade edildiği şekliyle ilgili olaylar özetle şöyledir:

7. Ulusal ölçekte yayımlanan Hürriyet gazetesinin İnternet arşivi sayfasında 16/2/2007 tarihinde başvuru hakkında "Mimar ile Mühendis Yumruk Yumruğa" başlıklı bir haber yayımlanmıştır. Haber içeriğinde, haberin yayımlandığı dönemde Kayseri ilinin Melikgazi ilçesinde Belediye Meclisi Adalet ve Kalkınma Partisi (AK Parti) Başkan Vekili olan Mimar Veysel Bayar ile Doğru Yol Partisi (DYP) İlçe Yönetim Kurulu Üyesi Makine Mühendisi Y.Ç. arasında iş ilişkisinden kaynaklanan tartışmanın büyüyerek kavgaya dönüştüğüne, başvuru Veysel Bayar ile kardeşi başvuru Asım Bayar'ın polis merkezinde ifadelerinin alındığına ve olayla ilgili soruşturmanın sürdüğüne ilişkin ifadeler yer almaktadır.

8. Başvurucular; bahsi geçen haberin yayımlandığı tarihin üzerinden yaklaşık yedi yıla yakın zaman geçtiğini, haberin güncelliğini yitirdiğini ancak İnternet arşivinde yer almaya devam etmesi nedeniyle şeref ve itibarlarının zedelendiğini ileri sürerek 22/1/2014 tarihinde söz konusu habere erişimin engellenmesi talebinde bulunmuşlardır.

9. (Kapatılan) Kayseri 5. Sulh Ceza Mahkemesi 23/1/2014 tarihli kararı ile erişimin engellenmesi talebinin reddine karar vermiştir. Anılan kararın gerekçesi şöyledir:

"www.hurriyet.com.tr adresinde 16/02/2007 tarihinde "mimar ile mühendis yumruk yumruğa" başlıklı haberin yayından kaldırılmasını istemiş iseler de; haber içeriğinde istem sahiplerini küçük düşürücü bir anlatımın olmadığı, haberin gerçeğe aykırılığının da iddia edilmediği, 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da güncelliğini yitirmiş haberlerin internet yayımından kaldırılmasına dair bir düzenlemenin bulunmadığı, böylece şartları oluşmadığından yerinde görülmeyen talebin reddine dair aşağıda yazılı olduğu şekilde karar verilmiştir."

10. Başvurucuların anılan karara itirazı Kayseri 3. Asliye Ceza Mahkemesinin 7/2/2014 tarihli kararı ile "itiraza konu yayının haber içerikli olduğu, kamuyu bilgilendirme niteliği taşıdığı ve haberde adı geçen kişilerin haklarının ihlaline dair ibareler olmadığı" gerekçesiyle reddedilmiştir.

11. Karar başvuruculara 18/2/2014 tarihinde tebliğ edilmiştir. Başvurucular 20/3/2014 tarihinde bireysel başvuruda bulunmuşlardır.

IV. İLGİLİ HUKUK

12. Anayasa Mahkemesinin 3/3/2016 tarihli ve 2013/5653 numaralı N.B.B. Kararı.

V. İNCELEME VE GEREKÇE

13. Mahkemenin 4/10/2017 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucuların İddiaları

14. Başvurucular; Hürriyet gazetesinin İnternet arşivi sayfalarında 16/2/2007 tarihinde Makine Mühendisi Y.Ç. ile aralarında iş ilişkisinden kaynaklanan tartışmanın büyüyerek kavgaya dönüştüğüne, polis merkezinde ifadelerinin alındığına ve olayla ilgili soruşturmanın sürdüğüne ilişkin bir haber yayımlandığını, haberin ilk yayımlandığı tarihin üzerinden yedi yıldan fazla zaman geçtiğini, haberin güncelliğini yitirmiş olmasına rağmen İnternet arşivinde yer almaya devam ettiğini, habere erişimin engellenmesi yönündeki taleplerinin yargısal makamlar tarafından reddedildiğini belirterek Anayasa'nın 5., 17., 32. ve 40. maddelerinde tanımlanan haklarının ihlal edildiğini ileri sürmüşlerdir.

B. Değerlendirme

15. Anayasa Mahkemesi, olayların başvurucular tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Başvurucular, haklarında yayımlanan habere, bahsi geçen gazetenin İnternet sitesindeki haber arşivi üzerinden hâlen kolayca ulaşılabilmesi ve bu arşiv haberin İnternet'ten çıkarılması taleplerinin reddedilmesi nedeniyle kişilik haklarının zarar gördüğünden şikâyet etmektedir. Başvurucuların bu şikâyeti şeref ve itibarın korunması hakkı kapsamında incelenmiştir.

16. Bireyin kişisel şeref ve itibarı, Anayasa'nın 17. maddesinde yer alan "manevi varlık" kapsamında yer almaktadır. Devletin, bireyin manevi varlığının bir parçası olan kişisel şeref ve itibara keyfi olarak müdahale etmemek şeklinde negatif yükümlülüğü ve üçüncü kişilerin saldırılarını önlemek şeklinde pozitif yükümlülüğü bulunmaktadır (Adnan Oktar (3), B. No: 2013/1123, 2/10/2013, § 33). Şeref ve itibarı etkileyen saldırılar veya basın ve yayın yolu ile yapılan yayınlara karşı bireyin korunmaması

hâlinde Anayasa'nın 17. maddesinin birinci fıkrası ihlal edilmiş olabilir (Kadir Sağdıç [GK], B. No: 2013/6617, 8/4/2015, § 36; İlhan Cihaner (2), B. No: 2013/5574, 30/6/2014, § 42).

17. Anayasa'nın "Düşünceyi açıklama ve yayma hürriyeti" kenar başlıklı 26. maddesine göre herkes düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Anılan maddede ifade özgürlüğünün kullanımında başvurulabilecek araçlar "söz, yazı, resim veya başka yollar" olarak ifade edilmiş ve "başka yollar" ifadesiyle her türlü ifade aracının anayasal koruma altında olduğu gösterilmiştir (Emin Aydın [GK], B. No: 2013/2602, 23/1/2014, § 43).

18. Haber ve fikirlerin iletilmesinde ve alınmasında önemli bir işlev gören İnternet, Anayasa'nın 26. maddesinde düzenlenen ifade özgürlüğünün güvencesi altındadır. Nitekim Anayasa Mahkemesi İnternet erişimine yönelik bir müdahalenin ifade özgürlüğü kapsamında incelenmesi gerektiğini kabul etmiştir (Yaman Akdeniz ve diğerleri, B. No: 2014/3986, 2/4/2014; Youtube Llc Corporation Service Company ve diğerleri [GK], B. No: 2014/4705, 29/5/2014).

19. Anayasa Mahkemesi birçok kararında ifade özgürlüğünün sadece düşünce ve fikirleri yayma özgürlüğünü değil haber ve fikirlere ulaşma özgürlüğünü de kapsadığını vurgulamıştır (Emin Aydın, § 40; Kamuran Reşit Bekir [GK], B. No: 2013/3614, 8/4/2015, § 34). İnternet üzerinde arşiv oluşturma, aktüalitenin ve haberlerin saklanması ve erişilebilirliğine büyük ölçüde hizmet etmektedir. Bu nitelikteki arşivler özellikle doğrudan halkın erişimine açık ve genelde ücretsiz olmaları nedeniyle tarih eğitimi ve araştırma faaliyetleri için kaynak sunmaktadır. Öte yandan demokratik bir toplumda basın ilk işlevi olan "gözetleyici" rolünün bir sonucu da arşivlerin halkın erişimine sunulmasıdır (N.B.B., B. No: 2013/5653, 3/3/2016, § 61). Bu nedenle İnternet'te tutulan arşivlerin, ifade ve basın özgürlükleri kapsamında olduğu açıktır. Dolayısıyla İnternet'te yayımlanan ve gazetecilik faaliyeti kapsamında kabul edilen bir haber arşivinin yayından kaldırılması basın özgürlüğüne yönelik bir müdahale teşkil edebilir.

20. İfade özgürlüğü ile onu tamamlayan ve ifade özgürlüğünün kullanılmasını sağlayan basın özgürlüğü, Anayasa'da yer alan temel hak ve özgürlükleri sınırlama rejimine tabidir. Anayasa'nın 26., 27. ve 28. maddelerinde sayılan sınırlandırmalardan biri, "başkalarının şöhret veya haklarının, özel veya aile hayatlarının" korunmasıdır (Kadir Sağdıç, § 55; İlhan Cihaner (2), § 62). Öte yandan "başkalarının şöhret veya haklarının, özel veya aile hayatlarının" korunması bağlamında şeref ve itibarın korunması hakkının etki alanını genişletmenin ifade ve basın özgürlüklerinin ihlali sonucunu doğurabileceği hatırdta tutulmalıdır.

21. Bu sebeple Anayasa'nın 17. maddesinin birinci fıkrasında koruma altına alınan şeref ve itibarın korunmasını isteme hakkı ile başvuruya konu İnternet haber arşivlerinin Anayasa'nın 28. maddesinde güvence altına alınan basın özgürlüğü ve bu özgürlükle bağlantılı olarak Anayasa'nın 26. maddesinde güvence altına alınan ifade özgürlüğü arasında Anayasa Mahkemesi içtihadında ortaya konulan kriterlere uygun şekilde bir denge kurulması gerekmektedir. İnternet ortamının sağladığı ulaşılabilirlik, yaygınlık, haber ve fikirlerin depolanmasındaki ve muhafazasındaki kolaylık dikkate alındığında yayımlandığı tarihte belirli ağırlık eşiğini aşmayan veya kişinin kendi eylemlerinden kaynaklanan haberlerin İnternet ortamında uzun süre erişilebilir kalması kişilerin şeref ve itibarını zedeleyebilir (N.B.B., § 37).

22. Anayasa Mahkemesi 3/3/2016 tarihli ve 2013/5653 numaralı N.B.B. başvurusunda İnternet'in etkin olarak kullanmasıyla beraber ifade ve basın özgürlükleri ile şeref ve itibarın korunması arasındaki dengenin ilki lehine bozulduğunu, bu dengenin tekrar kurulabilmesinin şeref ve itibar yönünden bireylerin unutulma hakkının kabul edilmesi ile mümkün olabileceğini belirtmiştir (N.B.B., § 46).

23. Mahkeme bahsi geçen başvuruda unutulma hakkının anayasal dayanaklarına yer vererek devletin bireye geçmişte yaşadıklarının başkaları tarafından öğrenilmesi engellenerek “yeni bir sayfa açma” olanağı verme hususunda bir sorumluluğu olduğunu, dolayısıyla unutulma hakkının kişilerin manevi varlıklarını geliştirmelerine bir fırsat vermek açısından devletin pozitif yükümlülüğünün bir sonucu olduğunu ortaya koymuştur (N.B.B., §§ 47-49).

24. Bununla birlikte Mahkeme; unutulma hakkının İnternet üzerindeki her türlü haber veya yazı yönünden uygulanmasını beklemenin mümkün olmadığını, özellikle basın özgürlüğü temelinde gazete arşivinin araştırmacılar, hukukçular veya tarihçiler için önem taşıyan veriler olduğunu belirtmiştir. Unutulma hakkı, İnternet ortamında haber arşivini koruma altına alan basın özgürlüğünün ve halkın haber ve fikirlere ulaşma özgürlüğünün özüne dokunmayacak ve aynı zamanda hak sahibinin çıkarlarını koruyacak şekilde kullanılmalıdır. Mahkeme, İnternet ortamındaki bir haber veya yazının unutulma hakkı kapsamında İnternet'ten çıkarılabilmesi için yayının içeriği, yayında kaldığı süre, güncelliğini yitirme, tarihsel bir veri olarak kabul edilememe, kamu yararına katkısı (toplumsal açıdan haberin değeri, haberin geleceğe ışık tutan niteliği), haber veya yazıya konu kişinin siyasetçi veya ünlü olup olmadığı, haber veya yazının konusu, bu bağlamda haber ya da yazının olgusal gerçekler veya değer yargısı içerip içermediği, halkın ilgili veriye yönelik ilgisi gibi hususların somut olay açısından incelenmesi gerekliliğini ortaya koymuştur (N.B.B., § 50).

25. Somut olayda başvuru sahiplerinin şikâyetine konu olan haber 16/2/2007 tarihinde yayımlanmış ve arşiv niteliğindedir. Haber, Kayseri ilinin Melikgazi ilçesinde Belediye Meclisi AK Parti Başkan Vekili

olan Mimar Veysel Bayar ve kardeşi Asım Bayar ile DYP İlçe Yönetim Kurulu Üyesi Makine Mühendisi Y.Ç. arasındaki iş ilişkisinden kaynaklanan tartışma ve bu tartışmanın kavgaya dönüşmesi ile olayın adli makamlara intikal etmesi hakkındadır. Bu haberin gerçeğe aykırı olduğu ileri sürülmemiştir. Haberin başlığı ile içeriği incelendiğinde amacın, kamuoyunun ilgisine matuf, haberin yayımlandığı dönemde aynı zamanda siyasi kimliğe sahip başvuru Mimar Veysel Bayar ve kardeşi başvuru Asım Bayar ile yine siyasi kimliğe sahip Makine Mühendisi Y.Ç. arasında iş ilişkisi nedeniyle ortaya çıkan ihtilafa ve akabinde yaşananlara yönelik haber yapmak ve kamuoyunu bilgilendirmek olduğu görülmektedir.

26. Başvurucular, haberin yayımlandığı 16/2/2007 tarihinden 6 yıl 11 ay sonra 22/11/2014 tarihinde haber içeriklerine erişimin engellenmesi talebiyle (kapatılan) Kayseri 5. Sulh Ceza Mahkemesine başvuruda bulunmuşlardır. Mahkeme 23/1/2014 tarihli kararı ile haber içeriğinde istem sahiplerini küçük düşürücü bir anlatım olmadığı, haberin gerçeğe aykırılığının da iddia edilmediği, 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da güncelliğini yitirmiş haberlerin İnternet yayınından kaldırılmasına dair bir düzenlemenin bulunmadığı gerekçesiyle talebi reddetmiştir. Başvurucuların anılan karara itirazı da Kayseri 3. Asliye Ceza Mahkemesinin 7/2/2014 tarihli kararı ile yayının haber değeri olduğu ve kamuoyunu bilgilendirme niteliği taşıdığı ve haberde adı geçen kişilerin haklarının ihlaline dair ibareler bulunmadığı gerekçesiyle reddedilmiştir. Başvurucular, ret kararı üzerine 21/3/2014 tarihinde Anayasa Mahkemesine bireysel başvuruda bulunmuşlardır. Bireysel başvurunun yapıldığı tarihte, haberin ilk yayımlandığı tarih üzerinden 7 yıl 1 aylık sürenin geçtiği anlaşılmaktadır.

27. Yukarıda yer verilen süreler ile hakkında haber yapılan kişilerin kimlikleri de dikkate alındığında haberin güncelliğini ve kamuoyu ilgisini yitirdiği söylenemez. Bu bağlamda haberin konusu, içeriği ve ilk yayın tarihi üzerinden geçen süre gözönünde bulundurulduğunda haberin arşivde kolaylıkla ulaşılabilir kılınması için gerekli haber değerinin toplumsal açıdan devam ettiği, bu bağlamda unutulma hakkı kapsamında değerlendirilmeyi zorunlu kılacak şartların oluşmadığı belirlenmiştir. Öte yandan bireysel başvurunun karara bağlandığı tarih itibarıyla şikâyet konusu haberin başvuruçulara ve haberde adı geçen diğer şahıslara ilişkin kişisel veriler gizlenmiş olarak yayımlanmaya devam edildiği de tespit edilmiştir.

28. Sonuç olarak ifade ve basın özgürlükleri ile birlikte halkın haber alma ve bilgiye ulaşma hakkı birlikte değerlendirildiğinde başvuru konusu olayda, ifade ve basın özgürlükleri ile kişinin manevi

bütünlüğünün korunması hakkı arasında adil bir dengenin kurulduğu, derece mahkemesinin takdir yetkisine müdahale etmeyi gerekli kılacak bir durumun bulunmadığı sonucuna ulaşılmıştır.

29. Açıklanan nedenlerle başvurunun diğer kabul edilebilirlik koşulları yönünden incelenmeksizin açıkça dayanaktan yoksun olması nedeniyle kabul edilemez olduğuna karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Başvurunun açıkça dayanaktan yoksun olması nedeniyle **KABUL EDİLEMEZ OLDUĞUNA,**

B. Yargılama giderlerinin başvuruçular üzerinde bırakılmasına 4/10/2017 tarihinde **OYBİRLİĞİYLE** karar verildi.

Anayasa Mahkemesi - G.D. (2) (Unutulma Hakkı) Kararı (2014/1808)

G.D. (2), B. No: 2014/1808, 4/10/2017

Başvuru, ulusal ölçekte yayın yapan iki gazetenin internet haber arşivlerinde erişilebilir durumda olan haberler ile ilgili içeriğe erişimin engellenmesi yönündeki taleplerin reddedilmesi nedeniyle şeref ve itibarın korunması hakkının ihlal edildiği iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

İKİNCİ BÖLÜM

KARAR

G. D. BAŞVURUSU (2)

(Başvuru Numarası: 2014/1808)

Karar Tarihi: 4/10/2017

İKİNCİ BÖLÜM

KARAR

GİZLİLİK TALEBİ KABUL

Başkan: Engin YILDIRIM

Üyeler: Serdar ÖZGÜLDÜR, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ

Raportör Yrd.: Derya ATAKUL

Başvurucu: G. D.

Vekili: Av. Erdal Fatih ÇANAKÇI

I. BAŞVURUNUN KONUSU

1. Başvuru, ulusal ölçekte yayın yapan iki gazetenin internet haber arşivlerinde erişilebilir durumda olan haberler ile ilgili içeriğe erişimin engellenmesi yönündeki taleplerin reddedilmesi nedeniyle şeref ve itibarın korunması hakkının ihlal edildiği iddiasına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 11/2/2014 tarihinde yapılmıştır.
3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.
4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.
5. Başvurucu tarafından yapılan 2014/1808 ve 2014/1812 numaralı başvurular, aralarında konu yönünden hukuki irtibat bulunduğu anlaşıldığından birleştirilmiş; incelemeye 2014/1808 numaralı bireysel başvuru dosyası üzerinden devam edilmiştir.
6. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.
7. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık, görüşünü bildirmiştir.
8. Başvurucu, Bakanlığın görüşüne karşı süresinde beyanda bulunmuştur.

III. OLAY VE OLGULAR

9. Başvuru formu ve eklerinde ifade edildiği şekliyle olaylar özetle şöyledir:
10. Ulusal ölçekte yayımlanan Milliyet ve Radikal gazetelerinin İnternet arşivi sayfalarında 25/5/2009 tarihinde, eski Esenyurt Belediye Başkanı hakkında yürütülen ceza yargılamasına yönelik haberler yer almıştır. Haber içeriklerinde Başkanın aile fertlerinin de aynı davada yargılandığına, Başkanın kardeşi olan başvurucunun yargılamayı yürüten mahkeme tarafından suç örgütüne üye olma suçundan on ay hapis cezası ile cezalandırılmasına karar verildiğine ilişkin ifadeler yer almaktadır.
11. Başvurucu; haberlerde bahsi geçen mahkeme kararının Yargıtay 5. Ceza Dairesi tarafından bozulduğunu, bozma üzerine yapılan yargılama sonucunda hakkında açılan davanın ortadan kaldırılmasına karar verildiğini, herhangi bir suçtan hakkında mahkûmiyet hükmü bulunmadığını ancak bu haber nedeniyle şeref ve itibarının zedelendiğini ileri sürerek 1/10/2013 tarihinde söz konusu haberlere erişimin engellenmesi talebinde bulunmuştur.
12. Büyükçekmece 3. Sulh Ceza Mahkemesi 18/11/2013 tarihli kararları ile erişimin engellenmesi taleplerinin reddine karar vermiştir. Anılan kararların gerekçesi şöyledir:
"Bilindiği gibi Anayasal güvence altında bulunan (Anayasa 28. Madde) basın hürriyetinin yine yasalarca korunan kişilik haklarına yeğ tutulabilmesi için bu hürriyetin (haber verme, yorum ve eleştiri hürriyetinin) öğretide ve uygulamada tartışmasız benimsenen;

a-Gerçeklik,

b-Güncellik,

c-Kamu yararı ve toplumsal ilgi,

d-Konu ile ifade arasında düşünsel bağ kuralları çerçevesinde kullanılması gerekir. Ne var ki olay, doğru, güncel ve kamu yararı bulunsa bile şekle de aykırı olmamalı, haber ve eleştirinin veriliş, yazılış biçimi, kişilik hakkını zedeleyecek üslup ve tarzda olmamalıdır. Yani öze biçim arasında uygun bir denge bulunmalıdır.

Haber verme hakkı bu sınırlar içerisinde kaldığı sürece hukuka uygundur. Haber anılan temel kurallardan birine ters düşerse kamu yararı, kişisel hak dengesi bozulur, kullanılan bu hakkın hukuka uygunluğundan söz edilemez. Başka bir deyişle bu kurallardan herhangi birinin ihlali halinde saldırıya uğrayan kişisel hak korumaya değer bir üstünlük kazanır. Gerçeklikten kasıt ise somut gerçeklik değil, olayın verildiği andaki (haber dayanağı olan beyan ve belgelere göre) belirli biçimine uygunluk olarak anlaşılmalıdır.

...

İstanbul 9. Ağır Ceza Mahkemesinin 25/5/2009 günlü kararı ile itiraz eden G. D. hakkında suç işlemek için kurulan örgüte üye olma suçundan mahkumiyetine karar verildiği (ileride Yargıtay tarafından kararın bozulmasına ve İstanbul 9. Ağır Ceza Mahkemesinin 4/9/2012 tarihli ilamı ile G.D. hakkında açılan kamu davasının 765 sayılı TCK'nın 102/4 ve 104/2 maddeleri gereğince zaman aşımı nedeniyle ortadan kaldırılmasına karar verilmesine karşın), yukarıda uzantıları belirtilen internet sitelerinde haber yayın tarihlerinin 25/5/2009 tarihi olduğu anlaşılınca, muterizle ilgili haberin yayınlanma biçim ve içeriği itibariyle basın özgürlüğü ile kişi hak ve özgürlüğünün de dengeli gözetilmesi sonucunda yukarıda ayrıntısı ile belirtilen "gerçeklik, güncellik, kamu yararı ve toplumsal ilgi, konu ile ifade arasında düşünsel bağ kuralları çerçevesinde kullanılması" kurallarına aykırı olmadığı, haber tarihi itibarı ile ortada kesinleşmemiş dahi olsa mahkeme kararı ile verilmiş bir mahkumiyet kararı olduğu maddi gerçeğinin gözardı edilemeyeceği izahtan varestedir. Bu çerçevede, yayının yukarıda ayrıntısı belirtilen basın özgürlüğü sınırları içerisinde kalan bir yayın olduğu, kişilik haklarına bir saldırının bulunmadığı kanaatine varılmakla muteriz vekilinin talebine ilişkin reddine yönelik hüküm tesis edilmiştir."

13. Başvurucunun anılan kararlara itirazı Büyükçekmece 6. Asliye Ceza Mahkemesinin 18/11/2013 ve 26/12/2013 tarihli kararları ile reddedilmiştir.

14. Kararlar başvuruca 14/1/2014 tarihinde tebliğ edilmiştir. Başvurucu 11/2/2014 tarihinde bireysel başvuruda bulunmuştur.

IV. İLGİLİ HUKUK

15. Anayasa Mahkemesinin 3/3/2016 tarihli ve 2013/5653 numaralı N.B.B. kararı.

V. İNCELEME VE GEREKÇE

16. Mahkemenin 4/10/2017 tarihinde yapmış olduđu toplantıda başvuru incelenip gereği düşünöldü:

A. Başvurucunun İddiaları ve Bakanlık Görüşü

17. Başvurucu: Milliyet ve Radikal gazetelerinin İnternet arşivi sayfalarında 25/5/2009 tarihinde, suç örgütüne üye olma suçundan on ay hapis cezası ile cezalandırıldığına ilişkin haberler yayımlandığını, haberlerde sözü edilen mahkeme kararının Yargıtay 5. Ceza Dairesi tarafından bozulduğunu, bozma üzerine yapılan yargılama sonucunda davanın ortadan kaldırılmasına karar verildiğini, herhangi bir suçtan hakkında mahkûmiyet hükmü bulunmadığı hâlde ilgili yayın kuruluşlarının İnternet sitelerinin arşiv bölümlerinde hapis cezası ile cezalandırıldığına ilişkin haberlerin yer almaya devam ettiğini, toplumda suç işlemiş biri olarak göröldüğünü, haberlere erişimin engellenmesi yönündeki taleplerinin yargısal makamlar tarafından reddedilmesi nedeniyle Anayasa'nın 17. ve 38.maddelerinde tanımlanan haklarının ihlal edildiğini ileri sürmüş ve kamuya açık belgelerde kimliğinin gizli tutulması talebinde bulunmuştur.

18. Bakanlık görüşünde, şeref ve itibarın korunması hakkı ile ifade ve basın özgürlükleri arasında adil bir denge gözetilmesi gerekliliği ifade edilmiştir. Bakanlık, başvuru konusu haberin yapıldığı tarih itibarıyla güncel ve görünür gerçekliğe uygun olduğunu, ancak aradan geçen zaman dikkate alındığında çatışan haklar arasında tekrar değerlendirme yapılması gerekebileceğini belirtmiştir.

19. Başvurucu, Bakanlık görüşüne karşı beyanında önceki iddialarını tekrarlamıştır.

B. Değerlendirme

1. Gizlilik Talebi Yönünden

20. Başvuruya konu olayın niteliğinin başvurucaunun itibarını zedeleyebileceği dikkate alınarak gizlilik talebinin kabulüne karar verilmesi gerekir.

2. Kabul Edilebilirlik Yönünden

21. Anayasa Mahkemesi, olayların başvuruca tarafından yapılan hukuki nitelendirmesi ile bağılı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969,

18/9/2013, § 16). Başvurucu, hakkında yayımlanan haberlere, bahsi geçen gazetelerin İnternet sitelerindeki haber arşivleri üzerinden hâlen kolayca ulaşılabilmesi ve bu arşiv haberlerin İnternet'ten çıkarılması taleplerinin reddedilmesi nedeniyle kişilik haklarının zarar gördüğünden şikâyet etmektedir. Başvurucunun bu şikâyeti şeref ve itibarın korunması hakkı kapsamında incelenmiştir.

22. Bireyin kişisel şeref ve itibarı, Anayasa'nın 17. maddesinde yer alan "manevi varlık" kapsamında yer almaktadır. Devletin, bireyin manevi varlığının bir parçası olan kişisel şeref ve itibara keyfî olarak müdahale etmemek şeklinde negatif yükümlülüğü ve üçüncü kişilerin saldırılarını önlemek şeklinde pozitif yükümlülüğü bulunmaktadır (Adnan Oktar (3), B. No: 2013/1123, 2/10/2013, § 33). Şeref ve itibarı etkileyen saldırılar veya basın ve yayın yolu ile yapılan yayınlara karşı bireyin korunmaması hâlinde Anayasa'nın 17. maddesinin birinci fıkrası ihlal edilmiş olabilir (Kadir Sağdıç [GK], B. No: 2013/6617, 8/4/2015, § 36; İlhan Cihaner (2), B. No: 2013/5574, 30/6/2014, § 42).

23. Anayasa'nın "Düşünceyi açıklama ve yayma hürriyeti" kenar başlıklı 26. maddesine göre herkes düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Anılan maddede ifade özgürlüğünün kullanımında başvurulabilecek araçlar "söz, yazı, resim veya başka yollar" olarak ifade edilmiş ve "başka yollar" ifadesiyle her türlü ifade aracının anayasal koruma altında olduğu gösterilmiştir (Emin Aydın [GK], B. No: 2013/2602, 23/1/2014, § 43).

24. Haber ve fikirlerin iletilmesinde ve alınmasında önemli bir işlev gören İnternet, Anayasa'nın 26. maddesinde düzenlenen ifade özgürlüğünün güvencesi altındadır. Nitekim Anayasa Mahkemesi İnternet erişimine yönelik bir müdahalenin ifade özgürlüğü kapsamında incelenmesi gerektiğini kabul etmiştir (Yaman Akdeniz ve diğerleri, B. No: 2014/3986, 2/4/2014; Youtube LLC Corporation Service Company ve diğerleri [GK], B. No: 2014/4705, 29/5/2014).

25. Anayasa Mahkemesi birçok kararında ifade özgürlüğünün sadece düşünce ve fikirleri yayma özgürlüğünü değil haber ve fikirlere ulaşma özgürlüğünü de kapsadığını vurgulamıştır (Emin Aydın, § 40; Kamuran Reşit Bekir [GK], B. No: 2013/3614, 8/4/2015, § 34). İnternet üzerinde arşiv oluşturma, aktüalitenin ve haberlerin saklanmasına ve erişilebilirliğine büyük ölçüde hizmet etmektedir. Bu nitelikteki arşivler özellikle doğrudan halkın erişimine açık ve genelde ücretsiz olmaları nedeniyle tarih eğitimi ve araştırma faaliyetleri için kaynak sunmaktadır. Öte yandan demokratik bir toplumda basının ilk işlevi olan "gözetleyici" rolünün bir sonucu da arşivlerin halkın erişimine sunulmasıdır (N.B.B., B. No: 2013/5653, 3/3/2016, § 61). Bu nedenle İnternet'te tutulan arşivlerin, ifade ve basın özgürlükleri kapsamında olduğu açıktır. Dolayısıyla İnternet'te yayımlanan ve gazetecilik faaliyeti

kapsamında kabul edilen bir haber arşivinin yayından kaldırılması basın özgürlüğüne yönelik bir müdahale teşkil edebilir.

26. İfade özgürlüğü ile onu tamamlayan ve ifade özgürlüğünün kullanılmasını sağlayan basın özgürlüğü, Anayasa'da yer alan temel hak ve özgürlükleri sınırlama rejimine tabidir. Anayasa'nın 26., 27. ve 28. maddelerinde sayılan sınırlandırmalardan biri, "başkalarının şöhret veya haklarının, özel veya aile hayatları"nın korunmasıdır (Kadir Sağdıç, § 55; İlhan Cihaner (2), § 62). Öte yandan "başkalarının şöhret veya haklarının, özel veya aile hayatları"nın korunması bağlamında şeref ve itibarın korunması hakkının etki alanını genişletmenin ifade ve basın özgürlüklerinin ihlali sonucunu doğurabileceği hatırd tutulmalıdır.

27. Bu sebeple Anayasa'nın 17. maddesinin birinci fıkrasında koruma altına alınan şeref ve itibarın korunmasını isteme hakkı ile başvuruya konu İnternet haber arşivlerinin Anayasa'nın 28. maddesinde güvence altına alınan basın özgürlüğü ve bu özgürlükle bağlantılı olarak Anayasa'nın 26. maddesinde güvence altına alınan ifade özgürlüğü arasında Anayasa Mahkemesi içtihadında ortaya konulan kriterlere uygun şekilde bir denge kurulması gerekmektedir. İnternet ortamının sağladığı ulaşılabilirlik, yaygınlık, haber ve fikirlerin depolanmasındaki ve muhafazasındaki kolaylık dikkate alındığında yayımlandığı tarihte belirli ağırlık eşiğini aşmayan veya kişinin kendi eylemlerinden kaynaklanan haberlerin İnternet ortamında uzun süre erişilebilir kalması kişilerin şeref ve itibarını zedeleyebilir (N.B.B., § 37).

28. Anayasa Mahkemesi 3/3/2016 tarihli ve 2013/5653 numaralı N.B.B. başvurusunda İnternet'in etkin olarak kullanmasıyla beraber ifade ve basın özgürlükleri ile şeref ve itibarın korunması arasındaki dengenin ilki lehine bozulduğunu, bu dengenin tekrar kurulabilmesinin şeref ve itibar yönünden bireylerin unutulma hakkının kabul edilmesi ile mümkün olabileceğini belirtmiştir (N.B.B., § 46).

29. Mahkeme bahsi geçen başvuruda unutulma hakkının anayasal dayanaklarına yer vererek devletin bireye geçmişte yaşadıklarının başkaları tarafından öğrenilmesi engellenerek "yeni bir sayfa açma" olanağı verme hususunda bir sorumluluğu olduğunu, dolayısıyla unutulma hakkının kişilerin manevi varlıklarını geliştirmelerine bir fırsat vermek açısından devletin pozitif yükümlülüğünün bir sonucu olduğunu ortaya koymuştur (N.B.B., §§ 47-49).

30. Bununla birlikte Mahkeme, unutulma hakkının İnternet üzerindeki her türlü haber veya yazı yönünden uygulanmasını beklemenin mümkün olmadığını, özellikle basın özgürlüğü temelinde gazete arşivinin araştırmacılar, hukukçular veya tarihçiler için önem taşıyan veriler olduğunu belirtmiştir. Unutulma hakkı, İnternet ortamında haber arşivini koruma altına alan basın özgürlüğünün ve halkın haber ve fikirlere ulaşma özgürlüğünün özüne dokunmayacak ve aynı

zamanda hak sahibinin çıkarlarını koruyacak şekilde kullanılmalıdır. Mahkeme, İnternet ortamındaki bir haber veya yazının unutulma hakkı kapsamında İnternet'ten çıkarılabilmesi için yayının içeriği, yayında kaldığı süre, güncelliğini yitirme, tarihsel bir veri olarak kabul edilememe, kamu yararına katkısı (toplumsal açıdan haberin değeri, haberin geleceğe ışık tutan niteliği) haber veya yazıya konu kişinin siyasetçi veya ünlü olup olmadığı, haber veya yazının konusu, bu bağlamda haber ya da yazının olgusal gerçekler veya değer yargısı içerip içermediği, halkın ilgili veriye yönelik ilgisi gibi hususların somut olay açısından incelenmesi gerekliliğini ortaya koymuştur (N.B.B., § 50).

31. Somut olayda başvuru konusundaki şikâyetine konu olan haberler 25/5/2009 tarihinde yayımlanmış ve arşiv niteliğindedir. Haberler, eski Esenyurt Belediye Başkanının belediye başkanlığı yaptığı dönemde belediyedeki yolsuzluk iddiaları üzerine kendisi ve başvuru konusundaki aralarında bulunduğu aile fertleri hakkında "suç işlemek amacıyla örgüt kurma, suç örgütüne üye olma, özel evrakta sahtecilik ve ihaleye fesat karıştırma" suçlarından açılan kamu davası hakkındadır. Bu haberlerin gerçeğe aykırı olduğu ileri sürülmemiştir. Bahsi geçen haberlerde Belediye Başkanı ile başvuru konusundaki aralarında bulunduğu aile fertleri hakkında Başsavcılık tarafından hazırlanan iddianame ve bu kapsamda ilk derece mahkemesi tarafından yapılan yargılama sonucunda 25/5/2009 tarihinde verilen mahkûmiyet kararı aktarılmıştır. Haberlerin başlıkları ile içerikleri incelendiğinde amacın, kamuoyunun ilgisine matuf, Esenyurt Belediye Başkanlığı görevini icra etmiş bir siyasetçi ile başvuru konusundaki aralarında bulunduğu aile fertleri hakkında belediye başkanlığı döneminde yapıldığı iddia edilen fiillere yönelik olarak yapılan soruşturma ve kovuşturma hakkında haber yapmak ve kamuoyunu bilgilendirmek olduğu görülmektedir.

32. Başvuru hakkında suç örgütüne üye olma suçundan verilen ceza Yargıtay 5. Ceza Dairesi tarafından bozulmuş, bozmaya uyularak yapılan yargılamada ilk derece mahkemesince 4/9/2012 tarihinde, başvuru hakkında açılan kamu davasının zamanaşımı nedeniyle ortadan kaldırılmasına karar verilmiştir. Başvuru, haberlerin yayımlandığı 25/5/2009 tarihinden 4 yıl 4 ay ve ilk derece mahkemesinin 4/9/2012 tarihli kamu davasının zamanaşımı nedeniyle ortadan kaldırılması kararından bir yıl sonra 1/10/2013 tarihinde haber içeriklerine erişimin engellenmesi talebiyle Büyükçekmece 3. Sulh Ceza Mahkemesine başvuruda bulunmuştur.

33. Büyükçekmece 3. Sulh Ceza Mahkemesi, başvuru hakkında açılan kamu davasının zamanaşımı nedeniyle ortadan kaldırılmasına ilişkin kararı gözönünde bulundurmuş olmakla birlikte haberlerin "gerçeklik, güncellik, kamu yararı ve toplumsal ilgi, konu ile ifade arasında düşünsel bağ kuralları çerçevesinde kullanılması" kurallarına aykırı olmadığını, haber tarihi itibarı ile ortada kesinleşmemiş dahi olsa mahkeme kararı ile verilmiş bir mahkûmiyet hükmü bulunduğunu, bu bağlamda haberlerin

basın özgürlüğü sınırları içerisinde kalan yayınlar olduğunu ve kişilik haklarına bir saldırının bulunmadığını belirterek haber içeriklerine erişimin engellenmesi talebini reddetmiştir.

34. Haberin konusu, eski Esenyurt Belediye Başkanının belediye başkanlığı yaptığı dönemde belediyedeki yolsuzluk iddiaları üzerine kendisi ve aile fertleri hakkında başlatılan soruşturma ve devamındaki yargılama sürecine ilişkindir. Başvuru tarihi itibarıyla söz konusu haberin yayın tarihi olan 25/5/2009 tarihi üzerinden 4 yıl 8 aylık bir süre geçmiştir. Yine başvuru hakkındaki davanın zamanaşımı nedeniyle ortadan kaldırılmasına ilişkin 4/9/2012 tarihli karar ile haber içeriklerine erişimin engellenmesi talebiyle Sulh Ceza Mahkemesine yapılan başvuru arasında bir yıllık süre bulunmaktadır. Başvurucu, davanın ortadan kaldırılmasına ilişkin verilen karar üzerinden 1 yıl 5 ay geçtikten sonra da Anayasa Mahkemesine bireysel başvuruda bulunmuştur. Bu süreler ile hakkında haber yapılan kişilerin kimlikleri de dikkate alındığında haberin güncelliğini ve kamuoyu ilgisini yitirdiği söylenemez. Bu bağlamda haberin konusu, içeriği, ilk yayın tarihi üzerinden geçen süre ile ceza yargılamasının nihai olarak karara bağlandığı tarih gözönünde bulundurulduğunda toplumsal açıdan haberin arşivde kolaylıkla ulaşılabilir kılınması için gerekli haber değerinin devam ettiği, bu bağlamda unutulma hakkı kapsamında değerlendirilmeyi zorunlu kılacak şartların oluşmadığı belirlenmiştir. Sonuç olarak ifade ve basın özgürlüğü ile halkın haber alma ve bilgiye ulaşma hakkı birlikte değerlendirildiğinde başvuru konusu olayda, ifade ve basın özgürlükleri ile kişinin manevi bütünlüğünün korunması hakkı arasında adil bir dengenin kurulduğu, derece mahkemesinin takdir yetkisine müdahale etmeyi gerekli kılacak bir durumun bulunmadığı sonucuna ulaşılmıştır.

35. Açıklanan nedenlerle başvurunun diğer kabul edilebilirlik koşulları yönünden incelenmeksizin açıkça dayanaktan yoksun olması nedeniyle kabul edilemez olduğuna karar verilmesi gerekir.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Başvurucunun kamuya açık belgelerde kimliğinin gizli tutulması talebinin **KABULÜNE**,

B. Başvurunun açıkça dayanaktan yoksun olması nedeniyle **KABUL EDİLEMEZ OLDUĞUNA**,

C. Yargılama giderlerinin başvuru üzerinde bırakılmasına 4/10/2017 tarihinde **OYBİRLİĞİYLE** karar verildi.

Anayasa Mahkemesi - E.Ç.A. Kararı (2014/5671)

E.Ç.A. [GK], B. No: 2014/5671, 7/6/2018

Başvuru, hırsızlık suçlarına ilişkin bilgilerin adli sicil arşiv kaydında tutulması ve Genel Bilgi Toplama Sistemi'ne kaydedilmesi nedeniyle özel hayatın gizliliği hakkının ihlal edildiği iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

GENEL KURUL

KARAR

E.Ç.A. BAŞVURUSU

(Başvuru Numarası: 2014/5671)

Karar Tarihi: 7/6/2018

R.G. Tarih ve Sayı: 24/7/2018-30488

GENEL KURUL

KARAR

GİZLİLİK TALEBİ KABUL

Başkan: Zühtü ARSLAN

Başkanvekili: Burhan ÜSTÜN

Başkanvekili: Engin YILDIRIM

Üyeler: Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Muammer TOPAL, M. Emin KUZ, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Rıdvan GÜLEÇ, Recai AKYEL, Yusuf Şevki HAKYEMEZ

Raportörler: Şermin BİRTANE; Hikmet Murat AKKAYA

Başvurucu: E.Ç.A.

Vekili: Av. Fatih Mehmet AKTAŞ

I. BAŞVURUNUN KONUSU

1. Başvuru, hırsızlık suçlarına ilişkin bilgilerin adli sicil arşiv kaydında tutulması ve Genel Bilgi Toplama Sistemi'ne kaydedilmesi nedeniyle özel hayatın gizliliği hakkının ihlal edildiği iddiasına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 17/4/2014 tarihinde yapılmıştır.

3. Başvuru, başvuru formu ve eklerinin idari yönden yapılan ön incelemesinden sonra Komisyona sunulmuştur.

4. Komisyonca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.

5. Bölüm Başkanı tarafından başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.

6. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık, görüşünü bildirmiştir.

7. Başvurucu, Bakanlığın görüşüne karşı süresinde beyanda bulunmuştur.

8. İkinci Bölüm tarafından 6/12/2017 tarihinde yapılan toplantıda, niteliği itibarıyla Genel Kurul tarafından karara bağlanması gerekli görüldüğünden başvurunun Anayasa Mahkemesi İçtüzüğü'nün 28. maddesinin (3) numaralı fıkrası uyarınca Genel Kurula sevkine karar verilmiştir.

III. OLAY VE OLGULAR

9. Başvuru formu ve eklerinde ifade edildiği şekliyle olaylar özetle şöyledir:

10. Başvurucu 6/10/1971 tarihinde doğmuştur. Başvurucu, esnaf olup bakkal dükkânı işletmektedir.

11. Başvurucu 9/10/1989, 10/10/1989 ve 19/10/1989 tarihlerinde işlediği üç ayrı fiilden dolayı 1/3/1926 tarihli ve 765 sayılı mülga Türk Ceza Kanunu'nun ilgili hükümlerine göre hırsızlık suçu kapsamında İzmir 8. Asliye Ceza Mahkemesinin 27/3/1990 tarihli kararıyla ağır para cezaları ile cezalandırılmış ve başvurucunun cezaları ertelenmiştir.

12. Başvurucunun adli sicil kaydının silinmesi talebiyle yaptığı başvuru üzerine İzmir 8. Asliye Ceza Mahkemesi 9/4/1996 tarihli kararıyla tecilli cezanın işlenmemiş sayılarak adli sicil kayıtlarından silinmesine karar vermiştir.

13. Başvurucu 30/6/2006 tarihinde Genel Bilgi Toplama (GBT) Sistemi'nde bulunan kaydının silinmesi talebiyle Emniyet Genel Müdürlüğüne müracaat etmiştir.

14. Başvurucunun dilekçesi idarenin ilgili birimleri tarafından başvuru hakkındaki adli sicil kaydının düzenlendiği İzmir İl Emniyet Müdürlüğüne iletilmiştir. İzmir İl Emniyet Müdürlüğü'nün 8/8/2006 tarihli yazısıyla Bilgi Toplama Yönergesi (Yönerge) gereğince başvuru hakkındaki bilgi formlarının iptal edilemeyeceği belirtilmiştir. Bu yazı başvurucuya 26/7/2006 tarihinde tebliğ edilmiştir.

15. Başvurucu, GBT sisteminde bulunan kaydının silinmesi amacıyla İçişleri Bakanlığı aleyhine Ankara 9. İdare Mahkemesinde iptal davası açmıştır.

16. Mahkeme, 11/4/2008 tarihli kararıyla davayı reddetmiştir. Mahkeme kararında İçişleri Bakanlığı Kaçakçılık İstihbarat, Harekat ve Bilgi Toplama Dairesi (KİHBİ) Başkanlığınca çıkarılan 29/3/2005 tarihli Yönerge'de yer alan hükümlere yer verilmiştir. Kararda; kamu güvenliğinin ve suç ve suçluyla mücadelenin etkin şekilde sağlanması amacıyla Yönerge ile bazı suç tiplerinden hüküm giyenler hakkında GBT sistem kaydının nasıl tutulacağına düzenlendiği, Yönerge'nin 9. maddesinin (b) bendinde hırsızlık suçunun da bu suç türleri arasında gösterildiği belirtilmiştir. Bu nedenle hırsızlık suçundan cezalandırılan başvuru hakkında tutulan GBT sisteminden kaydının silinmesi için yapılan başvurunun reddine ilişkin işlemin hukuka aykırı olmadığı ifade edilmiştir.

17. Başvurucunun temyiz istemi Danıştay Onuncu Dairesinin 23/5/2012 tarihli kararıyla reddedilerek hüküm onanmıştır.

18. Başvurucunun karar düzeltme istemi aynı Dairenin 12/2/2014 tarihli kararıyla reddedilmiştir.

19. Nihai karar, başvurucuya 2/4/2014 tarihinde tebliğ edilmiştir.

20. Başvurucu 17/4/2014 tarihinde bireysel başvuruda bulunmuştur.

21. KİHBİ Başkanlığı tarafından Anayasa Mahkemesinin 2013/2941 sayılı bireysel başvuru dosyasına gönderilen 11/6/2015 tarihli ve 1962 sayılı yazıda Yönerge'nin dayanakları ve uygulama alanı ile ilgili bilgilere yer verilmiştir.

22. Söz konusu yazıda Yönerge'nin 14/2/1985 tarihli ve 3152 sayılı İçişleri Bakanlığı Teşkilat ve Görevleri Hakkında Kanun'un 13. maddesinin birinci fıkrasının (c) bendi ve 33. maddesi, 4/7/1934 tarihli ve 2559 sayılı Pasif Vazife ve Salâhiyet Kanunu'nun ek 7. maddesi ile 17/12/1983 tarihli Jandarma Teşkilatı Görev ve Yetkileri Yönetmeliği'nin 42. maddesinin birinci fıkrasının (f) bendine dayanılarak hazırlandığı ve söz konusu Yönerge'nin "hizmete özel" dereceli olması nedeniyle kamuya açık olmadığı belirtilmiştir. Ayrıca Yönerge'de 4/6/2007 tarihli İçişleri Bakanlığı onayı ile değişiklikler yapıldığı bildirilmiştir.

23. Yazı içeriğinde GBT sistemine kaydı yapılan bilgilerin kolluk kuvvetlerine suç ve suçlarla mücadele çalışmalarında istihbarat kaynağı olarak idarenin vatandaşlarla ilgili yürüttüğü iş ve işlemlerde (silah ruhsatı, sürücü belgesi ve pasaport işlemleri, kamu hizmetlerinden men cezalarının takibi) kullanıldığı bildirilmiştir. Bunun yanı sıra GBT sistemindeki bilgilerin 26/10/1994 tarihli ve 4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ile Kamu Görevine Alınmayanların Haklarının Geri Verilmesinde ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun ile Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği gereği, bakanlıklar ile kamu kurum ve kuruluşlarının gizlilik dereceli birim ve kısımları ile yurt dışı teşkilatlarında, askerî, emniyet, istihbarat teşkilatlarında, ceza infaz kurumu ve tutukevlerinde çalıştıracakları personelin güvenlik soruşturması ve arşiv araştırması işlemleri için kullanıldığı ifade edilmiştir.

24. Bunun yanı sıra söz konusu yazıda ilgili programın esas olarak İçişleri Bakanlığına bağlı kolluk birimlerince kullanılmakla birlikte Başbakanlık ve Maliye Bakanlığı bünyesinde bulunan birimler ile yapılan protokoller gereği bilgi paylaşımı yapıldığı da belirtilmiştir.

IV. İLGİLİ HUKUK

A. Ulusal Hukuk

25. Mevcut başvurunun değerlendirilmesi sırasında gözönünde bulundurulanan GBT Sistemi'nde kayıt tutulmasına dair ulusal hukuk kaynakları için bkz. Bülent Kaya [GK], B. No: 2013/2941, 11/5/2016, §§ 20-28.

26. 25/5/2005 tarihli ve 5352 sayılı Adli Sicil Kanunu'nun "Adlî sicil ve arşiv bilgilerinin silinmesi" kenar başlıklı 12. maddesi şöyledir:

"(Değişik: 5/4/2012-6290/2 md.) Arşiv bilgileri;

a) İlgilinin ölümü üzerine,

b) Anayasanın 76 ncı maddesi ile Türk Ceza Kanunu dışındaki kanunlarda bir hak yoksunluğuna neden olan mahkûmiyetler bakımından kaydın arşive alınma koşullarının oluştuğu tarihten itibaren;

1. Yasaklanmış hakların geri verilmesi kararı alınması koşuluyla onbeş yıl geçmesiyle,

2. Yasaklanmış hakların geri verilmesi kararı alınması koşulu aranmaksızın otuz yıl geçmesiyle,

c) Diğer mahkûmiyetler bakımından kaydın arşive alınma koşullarının oluştuğu tarihten itibaren beş yıl geçmesiyle tamamen silinir.

(2) Fiilin kanunla suç olmaktan çıkarılması halinde, bu suçtan mahkûmiyete ilişkin adlî sicil ve arşiv kayıtları, talep aranmaksızın tamamen silinir.

(3) Kanun yararına bozma veya yargılamanın yenilenmesi sonucunda verilen beraat veya ceza verilmesine yer olmadığı kararının kesinleşmesi halinde, önceki mahkûmiyet kararına ilişkin adlî sicil ve arşiv kaydı tamamen silinir..."

B. Uluslararası Hukuk

1. Uluslararası Belgeler

27. Mevcut başvurunun değerlendirilmesi sırasında gözönünde bulundurulmuş GBT sisteminde kayıt tutulmasına dair uluslararası hukuk kaynakları için bkz. Bülent Kaya, §§ 29-34.

2. Avrupa İnsan Hakları Sözleşmesi ve Avrupa İnsan Hakları Mahkemesi İçtihadı

28. Avrupa İnsan Hakları Sözleşmesi'nin (Sözleşme) "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesi şöyledir:

"(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."

29. Avrupa İnsan Hakları Mahkemesi (AİHM) içtihadına göre bir kişinin özel yaşamına ilişkin verilerin kaydedilmesi ve saklanması, kendi başına özel hayata saygı hakkı bakımından bir müdahale oluşturmaktadır. Bu müdahalenin tespiti için kaydedilen bilgilerin daha sonra kullanılmış olması gibi bir koşul da aranmamaktadır. Bununla birlikte kamu makamları tarafından muhafaza edilen kişisel nitelikteki bilgilerin özel yaşam unsurlarından birini devreye sokup sokmadığını tespit etmek için bu bilgilerin hangi çerçevede alındıklarının ve muhafaza edildiklerinin, verilerin türünün, kullanıldıkları ve işlendikleri şekli ve bunlardan çıkarılabilecek sonuçların dikkate alınması zaruridir (S. ve Marper/Birleşik Krallık [BD], B. No: 30562/04, 30566/04, 4/12/2008, § 67).

V. İNCELEME VE GEREKÇE

30. Mahkemenin 7/6/2018 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Adli Sicil Arşiv Kaydının Tutulması Nedeniyle Özel Hayata Saygı Hakkının İhlal Edildiğine İlişkin İddia

31. Başvurucu; yirmi yıldan beri ticaretle uğraştığını, adli sicil belgelerinde arşiv kayıtlarına yer verilmesi nedeniyle tüm resmî işlemlerde ve esnaf odası faaliyetlerinde kendisine adli sicil kaydı silinmemiş gibi muamele yapıldığını belirtmektedir. Başvurucu ayrıca arşiv kaydının silinmemesi nedeniyle çeşitli imkânlardan yararlanamadığını, bu durumun kendisine sınırlama getirdiğini belirterek özel hayata saygı hakkının ihlal edildiğini ileri sürmüştür.

32. Bakanlık görüşünde, adli sicil arşiv kaydının tutulmasıyla ilgili değerlendirme yapılmamıştır.

33. Bireysel başvuru yolunun ikincil niteliği gereği Anayasa Mahkemesine başvuruda bulunabilmek için öncelikle olağan kanun yollarının tüketilmesi zorunludur. Başvurucunun bireysel başvuru konusu şikâyetini öncelikle ve süresinde yetkili idari ve yargısal mercilere usulüne uygun olarak iletmesi, bu konuda sahip olduğu bilgi ve delilleri zamanında bu makamlara sunması, bu süreçte dava ve başvurusunu takip etmek için gerekli özeni göstermiş olması gerekir (İsmail Buğra İşlek, B. No: 2013/1177, 26/3/2013, § 17).

34. Başvurucunun açtığı davanın konusu ile bu başlık altında yer verilen şikâyetkonusu aynı nitelikte değildir. Açılan davanın konusu "GBT sisteminden kaydının silinmesi talebinin reddi" işlemi, şikâyet edilen husus ise adli sicil arşiv kaydının silinmemesidir. Başvurucu, derece mahkemesi önünde ileri sürmediği iddiaları Anayasa Mahkemesi önünde ileri sürmüştür. Bu sebeple başvurucunun 5352 sayılı Kanun kapsamındaki taleplerini öncelikle Adli Sicil ve İstatistik Genel Müdürlüğüne iletmesi gerekir.

35. Buna göre somut olayda başvurucunun adli sicil arşiv kaydının tutulmasıyla ilgili olarak hukuk sisteminde mevcut idari ve yargısal yolları tüketmeksizin bireysel başvuruda bulunduğu anlaşılmaktadır.

36. Açıklanan gerekçelerle başvurunun bu kısmının diğer kabul edilebilirlik koşulları yönünden incelenmeksizin başvuru yollarının tüketilmemesi nedeniyle kabul edilemez olduğuna karar verilmesi gerekir.

B. GBT Kaydı Nedeniyle Özel Hayata Saygı Hakkının İhlal Edildiğine İlişkin İddia

1. Başvurucunun İddiaları ve Bakanlık Görüşü

37. Başvurucu; hakkında uzun yıllar önce yürütülen ceza yargılamasına ilişkin bilginin GBT sistemine kaydedildiğini, polis kontrollerinde kendisine karşı tutumun değiştiğini, aile bireylerinin yanında küçük düştüğünü, ilgili kaydın silinmesi hususunda idareye yaptığı başvuru ile bu hususta açtığı davanın reddedildiğini belirterek Anayasa'nın 20. maddesinde tanımlanan özel hayata saygı hakkının ihlal edildiğini iddia etmiştir.

38. Bakanlık görüşünde; benzer başvurularda AİHM tarafından, kişinin rızası olmaksızın hakkında kişisel veri toplanması, saklanması ve kullanılması hususunun Sözleşme'nin 8. maddesi bağlamında değerlendirildiği ifade edilmiştir. Müdahalenin demokratik toplum düzeninde zorunlu bir toplumsal ihtiyaçtan kaynaklanıp kaynaklanmadığı değerlendirilirken gözönünde bulundurmak üzere AİHM önüne benzer ihlal iddialarıyla yansıyan dava ve karar örneklerine yer verilmiştir.

39. Başvurucu, Bakanlık görüşüne karşı beyanında başvuru formunda belirttiği hususları tekrar etmiştir.

2. Değerlendirme

40. Anayasa'nın "Özel hayatın gizliliği" kenar başlıklı 20. maddesinin ilgili kısmı şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

...

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

41. Özel hayata saygı hakkı kapsamında korunan hukuksal çıkarılardan biri de bireyin mahremiyet hakkıdır. Mahremiyet hakkı yalnız kalma hakkının yanında bireyin kendisi hakkındaki bilgileri kontrol edebilme hukuksal çıkarını da kapsamaktadır. Bireyin kendisine ilişkin herhangi bir bilginin kendi rızası olmaksızın açıklanmaması, yayılmaması, bu bilgilere başkaları tarafından ulaşılamaması ve rızası hilafına kullanılmaması, kısaca bu bilgilerin mahrem kalması konusunda menfaati bulunmaktadır. Bu husus, bireyin kendisi hakkındaki bilgilerin geleceğini belirleme hakkına işaret etmektedir (Serap Tortuk, B. No: 2013/9660, 21/1/2015, § 32).

42. Anayasa Mahkemesi tarafından kişisel veri kavramının belirli veya kimliği belirlenebilir olmak şartıyla bir kişiye ilişkin bütün bilgileri ifade ettiği kabul edilmekte olup bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgilerin değil telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, öz geçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm verilerin kişisel veri kapsamında olduğu belirtilmektedir (AYM, E.2014/74,

K.2014/201, 25/12/2014; E.2013/122, K.2014/74, 9/4/2014; E.2014/149, K.2014/151, 2/10/2014; E.2013/84, K.2014/183, 4/12/2014; E.2014/180, K.2015/30, 19/3/2015; Bülent Kaya § 49).

43. Bu noktada Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi de önemli tespitler içermektedir. Belirtilen sözleşmenin 2. maddesinde kişisel bilgi, belirli veya belirlenebilir gerçek bir kişiye ilişkin herhangi bir bilgi olarak tanımlanmakta ve söz konusu verilerin özel nitelikte olması gibi bir unsur aranmamaktadır.

44. Başvuruya konu olayda 1989 yılında işlenen suçlar sebebiyle 1990 yılındaki ceza yargılamasına ilişkin başvurucu hakkındaki verilerin GBT Sistemi'ne kaydedildiği görüldüğünden başvurucuyla ilgili olarak resmî makamların muhafaza ettikleri söz konusu kişisel bilgilerin özel hayata saygı hakkı anlamında kişisel veri olduğu anlaşılmaktadır. Bu kapsamda başvurucunun şikâyetinin özel hayata saygı hakkı çerçevesinde ele alınması gerekmektedir.

a. Kabul Edilebilirlik Yönünden

45. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan özel hayata saygı hakkının ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

b. Esas Yönünden

i. Müdahalenin Varlığı

46. Somut başvuruda, başvurucu hakkında hırsızlık suçu nedeniyle 27/3/1990 tarihinde verilen ceza mahkûmiyetine dair bilgilerin GBT Sistemi'ne kaydedilerek muhafaza edildiği ve bu sistemdeki kayıtların yapılan güvenlik taramalarında kullanılabilecek nitelikte olduğu dikkate alındığında (bkz. §§ 23,24) söz konusu kişisel verilerin ilgili sistemde tutulmasının Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkına bir müdahale oluşturduğu anlaşılmaktadır.

ii. Müdahalenin İhlal Oluşturup Oluşturmadığı

47. Anayasa'nın 13. maddesi şöyledir:

"Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz."

48. Belirtilen Anayasa hükmü, hak ve özgürlükleri sınırlama ve güvence rejimi bakımından temel öneme sahip olup Anayasa'da yer alan bütün hak ve özgürlüklerin yasa koyucu tarafından hangi

ölçütler gözönünde bulundurularak sınırlandırılabilceğini ortaya koymaktadır. Anayasa'nın bütünselliği ilkesi çerçevesinde Anayasa kurallarının bir arada ve hukukun genel kuralları gözönünde tutularak uygulanması zorunlu olduğundan belirtilen düzenlemede yer alan başta kanunla sınırlama kaydı olmak üzere tüm güvence ölçütlerinin Anayasa'nın 20. maddesinde yer verilen hakkın kapsamının belirlenmesinde de gözetilmesi gerektiği açıktır (Sevim Akat Eşki, B. No:2013/2187, 19/12/2013, § 35).

(1) Kanunilik

49. Anayasa Mahkemesi Genel Kurulu tarafından GBT sisteminin kanuni dayanakları konusunda Bülent Kaya kararında inceleme yapılmış ve konuyla ilgili mevzuatın "kanunla sınırlama" ölçütünü karşıladığı sonucuna varılmıştır. Mevcut başvuruda anılan karardaki tespitlerden ayrılmayı gerektiren bir yön bulunmamaktadır (Bülent Kaya, §§ 71-78).

(2) Meşru Amaç

50. GBT Sistemi'ne terör, kaçakçılık, devlet güvenliğine karşı işlenen suçlar ve yüz kızartıcı suçların sanıkları ile ilgili dava bilgileri kaydedilmekte olup bu uygulamanın suç ve suçlularla mücadele bağlamında kamu düzeni ve güvenliğinin sağlanmasına yönelik meşru bir amaç taşıdığı anlaşılmaktadır.

(3) Demokratik Toplum Düzeninde Gerekli Olma ve Ölçülülük

(a) Genel İlkeler

51. Özel hayata saygı hakkının sınırlanması mümkün olup Anayasa'nın 13. maddesi vasıtasıyla Anayasa'da yer alan tüm temel hak ve özgürlüklerin sınırlandırılması hususunda geçerli olan ilkeler, özel hayata saygı hakkının sınırlandırılmasında da gözönünde bulundurulmalıdır. Buna göre demokratik toplum düzeninin gereklerine uygunluk gözetilmeli, sınırlamada öngörülen meşru amaç ile sınırlandırma aracı arasında orantısızlık bulunmamalı, sınırlandırmayla ulaşılabilecek genel yarar ile temel hak ve özgürlüğü sınırlandırılan bireyin kaybı arasında adil bir denge kurulmasına özen gösterilmelidir (Marcus Frank Cerny [GK], B. No: 2013/5126, 2/7/2015, § 73; Bülent Polat [GK], B. No: 2013/7666, 10/12/2015, §§ 104, 107; Serap Tortuk, §§ 44, 48).

52. Başvuru konusu olay bakımından yapılacak değerlendirmenin temel ekseni, müdahaleye neden olan idare ve derece mahkemelerinin kararlarında dayandıkları gerekçelerin özel hayata saygı hakkını kısıtlama bakımından "demokratik toplum düzeninin gereklerine" ve "ölçülülük ilkesi"ne uygun olduğunun inandırıcı bir şekilde ortaya konulup konulmadığı olacaktır. Bu çerçevede bir

müdahale, meşru amaçla orantılı olmalıdır. İkinci olarak müdahalenin haklılığı için kamu makamlarının gösterdiği gerekçeler konuyla ilgili ve yeterli olmalıdır (Marcus Frank Cerny, § 83).

(b) İlkelerin Olaya Uygulanması

53. Somut olayda başvuruçunun ceza mahkûmiyetine esas olan hırsızlık suçunun Yönerge'nin 9. maddesinin (b) fıkrasında yer alan suçlar arasında olduğu görülmektedir. Bu verilerin polis ve idari merciler tarafından kullanılmasının gizlilik kurallarına tabi olduğu, açık şekilde belirlenmiş durumlarla sınırlı tutulduğu, ilgili bilgilerin toplanma, paylaşım, kullanım ve silinmesine ilişkin hususların ayrıntılı olarak düzenlendiği anlaşılmaktadır.

54. Bunun yanı sıra 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 17. maddesinde kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140. maddeleri hükümlerinin uygulanacağı hükme bağlanmıştır. 5237 sayılı Kanun'un 136. maddesi uyarınca da kişisel verileri hukuka aykırı olarak başkasına vermek, yaymak veya ele geçirmek suç olarak düzenlenmiştir. Dolayısıyla elde edilen bilgilerin amacı dışında kullanılmasını önleyecek ve kişilerin özel hayatına dair bilgilerin ve kişisel verilerin ifşa edilmesini önleyecek yasal güvencenin mevcut olduğu görülmektedir.

55. Ayrıca somut olayda söz konusu verilerin toplanması, muhafazası ve kullanımı hususunda tespit edilen amaç dışında yararlanıldığına yahut özel yaşamı ve çalışma hayatı bakımından olumsuz sonuçlar doğurduğuna ilişkin somut olgulara dayalı herhangi bir delil başvuruçunun tarafından ortaya konulamamıştır. Bu nedenlerle başvuruya konu müdahalenin demokratik toplumda gerekli ve ölçülü olmadığı söylenemez.

56. Açıklanan gerekçelerle Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkının ihlal edilmediğine karar verilmesi gerekir.

Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Muammer TOPAL, Hasan Tahsin GÖKCAN ve Yusuf Şevki HAKYEMEZ bu görüşe katılmamışlardır.

VI. HÜKÜM

Açıklanan gerekçelerle;

A. Kamuya açık belgelerde başvuruçunun kimliğinin gizli tutulması talebinin **KABULÜNE OYBİRLİĞİYLE**,

B. 1. Adli sicil arşiv kaydı nedeniyle özel hayata saygı hakkının ihlal edildiğine ilişkin iddianın başvuru yollarının tüketilmemesi nedeniyle **KABUL EDİLEMEZ OLDUĞUNA OYBİRLİĞİYLE**,

2. Özel hayata saygı hakkının ihlal edildiğine ilişkin iddianın KABUL EDİLEBİLİR OLDUĞUNA OYBİRLİĞİYLE,

C. Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkının İHLAL EDİLMEDİĞİNE Engin YILDIRIM, Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Muammer TOPAL, Hasan Tahsin GÖKCAN ve Yusuf Şevki HAKYEMEZ'in karşıoyu ve OYÇOKLUĞUYLA,

D. Yargılama giderlerinin başvuru üzerinde BIRAKILMASINA,

E. Kararın bir örneğinin Adalet Bakanlığına GÖNDERİLMESİNE 7/6/2018 tarihinde karar verildi.

KARŞIOY GEREKÇESİ

2013/2941 numaralı bireysel başvuruya ilgili karşıoyumda belirttiğim gerekçelerle, başvuru Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkının ihlal edildiği düşüncesiyle çoğunluk kararına katılmadım.

Başkanvekili

Engin YILDIRIM

KARŞI OY GEREKÇESİ

Başvurucunun 9.4.1996 tarihinde 765 sayılı (halen mülga) Türk Ceza Kanununun (TCK) ilgili hükümlerince üç ayrı hırsızlık suçundan mahkûm olduğu, bu cezaların ağır para cezalarına çevrildiği ve ertelendiği, aynı kanunun 95 nci maddesindeki "...Cürüm ile mahkûm olan kimse hüküm tarihinden itibaren beş sene içinde işlediği diğer bir cürümden dolayı evvelce verilen ceza cinsinden bir cezaya yahut hapis veya ağır hapis cezasına mahkûm olmazsa, cezası tecil edilmiş olan mahkûmiyeti esasen vaki olmamış sayılır..." hükmü uyarınca, başvuru talebi üzerine 9.4.1996 tarihinde ilgili mahkemece "tecilli cezanın işlenmemiş sayılarak adli sicil kayıtlarından silinmesine" karar verildiği, buna rağmen İçişleri Bakanlığınca çıkartılan Bilgi Toplama Yönergesi'nin (Yönerge) ilgili hükümlerine dayanılarak, başvuru "esasen vaki olmamış" sayılan bu mahkûmiyetinin Emniyet Genel Müdürlüğü Bilgi Toplama Sistemi'ne (GBT) kaydedildiği, bireysel başvuru tarihinde ve halen bu durumun anılan sistemde varlığını devam ettirdiği ve başvuru emniyet mensuplarınca her bilgi sorgulamasında karşısına çıktığı ve anılan Yönergenin ilgili hükümleri gereğince "hırsızlık" suçundan sisteme giren her bilginin (verinin) "beraat, ceza verilmesine yer

olmadığı, davanın düşmesi veya dava zaman aşımı nedeniyle davanın ortadan kaldırılmasına “karar verilmedikçe sistemden çıkışının (silinmesinin) mümkün olmadığı, diğer bir deyişle başvuru hakkındaki, anılan kaydın onun ölümüne kadar sistemde muhafaza edileceği, başvurucağının da, sürekli karşısına çıkan ve özel hayatına bir müdahale olarak değerlendirdiği bu durum nedeniyle sözkonusu bireysel başvuruyu yaptığı anlaşılmaktadır.

Anılan Yönerge “Gizli” gizlilik dereceli olup, bilmesi gerekenler (uygulayıcılar) dışındaki üçüncü kişilerin erişimine kapalıdır. Yine Yönergenin dayanağı olarak gösterilen 3152 Sayılı Kanunun 13/1-c ve 33. maddeleri ile 2559 sayılı Kanunun EK-7. maddelerinde, Yönergedeki düzenlemeye dayanak teşkil edebilecek bir hüküm bulunmamaktadır. Yani işaret edilen yasa hükümlerinin, anılan düzenlemeyi haklı kılabilecek bir “çerçeve getirdiği” nin kabulü mümkün değildir. Dolayısıyla, Yönergenin dayanakları olarak gösterilen kanunlarda “yakalansalar dahi bazı suçları işlemiş olan kişiler” (Yönerge Md. 9/b) hakkında GBT bilgi kaydı tutulacağına ilişkin herhangi bir yetkinin verilmemiş olduğu, bunun doğal sonucu olarak da idarenin temel hak ve hürriyetlere sınırlama getiren düzenlemeleri Anayasanın 13. maddesine uygun olmayan biçimde, herhangi bir kanuni dayanağı olmaksızın ilk elden düzenleyici tasarrufla (Yönergeyle) getirdiği anlaşılmaktadır. Somut olayda da başvurucağının hakkında hırsızlık suçundan verilen ve “esasen vaki olmamış sayılan” ceza mahkûmiyetine dair bilgilerin GBT sistemine kaydedilerek muhafaza edilmesi ve davacının ölümüne kadar sistemde kalmaya devam edecek oluşu şeklinde gerçekleşen “özel hayata saygı hakkına yönelik müdahalenin” kanunilik şartını sağlamadığı görülmektedir.

Öte yandan, açık kanun hükmü uyarınca “esasen vaki olmamış”, yani artık hukuk alanında mevcudiyetinden söz edilemeyecek bir kişisel verinin, anılan Yönerge uyarınca “varmış gibi” kabul edilmesi aynı zamanda “ölçülülük” ilkesini de ihlâl etmektedir. Esasen vaki olmamış bir mahkûmiyet nedeniyle hâlâ beraat, düşme vb. şeklinde yargı kararı beklemek aynı zamanda Anayasanın 2. maddesinde ifadesini bulan Hukuk Devleti ilkesi ile de bağdaşmamaktadır. Dolayısıyla ilgili düzenlemenin ölçülülük ilkesiyle de uyum halinde olmadığı açıktır.

Genel güvenlik, suçla mücadele ve önleyici kolluk hizmetleri gibi demokratik toplum düzeninde gereklilik ölçütleri ile uyumlu kabul edilebilecek gerekçelerin de, somut başvuruda anılan düzenlemeyi haklı kılabilecek bir yönü yoktur. Çünkü, esasen vaki olmamış kabul edilen bir mahkûmiyet hükmünün Emniyet veri tabanında başvurucağının ölüm tarihine kadar saklanması fiili olgusu, başlıca hedefi kişilerin hak ve özgürlüklerden en geniş biçimde yararlanmalarını sağlamak olan demokratik hukuk devleti kavramı ile bağdaştırılamaz. Dolayısıyla böyle bir düzenlemeyi demokratik toplum düzeni bakımından “gerekli” olarak kabul etmek mümkün değildir.

Diğer taraftan, Avrupa İnsan Hakları Mahkemesi'nin (AİHM) ilgili kararları incelendiğinde de, bu şekildeki düzenlemeler bakımından ihlâl kararları verildiği görülmektedir. AİHM, Shimovolos/Rusya Davasında (No. 30194/09, 21.6.2011), bir insan hakları aktivistinin gizli bir güvenlik izleme veri tabanına kaydedilmesi ve hareketlerinin takip edilmesi ile ilgili olarak başvuranın adının kaydedildiği veri tabanının, yayınlanmamış ve halka açık olmayan bir bakanlık emri üzerine oluşturulmuş olmasından bahisle, insanların bu veri tabanına niçin kaydedildiğini, bu veri tabanında ne tür bilgilerin ne kadar süre tutulduğunu, kaydın nasıl yapıldığı, nasıl kullanıldığı ve kimin bu kayıtları kontrol ettiğinin bilinmesinin mümkün olmadığı gerekçeleriyle Sözleşmenin 8. maddesinin ihlâl edildiğine hükmetmiştir. Yine AİHM Brunet/Fransa kararında (B.No: 21010/10, 18.9.2014), bizdeki GBT'ye benzer şekilde Fransa'daki STIC sistemi tartışılmış ve başvurunun bu bilgilerin sistemden silinmesini isteme hakkının olmadığına vurgu yapılarak, sonuçta özel hayata saygı hakkının ihlâl edildiğine karar vermiştir. Aynı doğrultudaki bir başka karar Dimitrov-Kazakov /Bulgaristan kararıdır. (B.No: 11379/03,10.2.2011). AİHM bu başvuruda, cinsel saldırı suçundan mahkûm olan başvurunun adının kayıtlarda yer alması olayında, etkili bir hukuk yolunun bulunmamasını ölçsüz bir müdahale olarak kabul etmiştir.

Yukarıda açıklanan nedenlerle, başvurunun Anayasanın 20. maddesinde güvence altına alınan özel hayata saygı hakkının ihlâl edildiğine karar verilmesi gerektiği kanaatine vardığımızdan, çoğunluğun aksi yöndeki kararına katılmıyoruz.

Üye

Serdar ÖZGÜLDÜR

Üye

Serruh KALELİ

KARŞIOY GEREKÇESİ

1. Başvuru, başvuru hakkında 1990 yılında verilen ve adli sicilden de silinmiş olan ceza mahkumiyetinin, GBT sistemine kaydedilerek halen muhafaza edilmesinin özel hayata saygı hakkını ihlâl ettiği iddiasına ilişkindir.
2. GBT sistemine kayıtlı bilgiler esas itibariyle kolluk kuvvetleri tarafından suç ve suçlularla mücadele çalışmalarında istihbarat kaynağı olarak kullanılmaktadır. Bunun yanı sıra, idarenin vatandaşlarla ilgili yürüttüğü iş ve işlemlerde GBT bilgilerinden yararlanıldığı, kamu kurum ve kuruluşlarının yurt

dışı veya gizlilik dereceli birimlerinde çalıştırılacak personelin güvenlik soruşturması ve arşiv araştırması amacıyla kullanıldığı bilinmektedir. Bu konuda mevzuatta farklı ve dağınık hükümler yer aldığı görülmektedir.

3. GBT ile ilgili mevzuatta, özel hayata ilişkin ve hassas nitelikli bu bilgilerin saklanma süresine, hangi şartlarda silinebileceğine veya bunların “bilmesi gereken” ilkesi gereğince kimler tarafından incelenebileceğine ilişkin açık ve öngörülebilir düzenlemeler bulunmadığı; aksine, uygulamada bu bilgilerin kişinin hayatının sonuna kadar saklandığı ve yaptığı kamu hizmeti nedeniyle “bilmesi gereken” görevliler dışında da çok geniş bir kesimin tetkikine açık olduğu, demokratik bir toplumda başta terör olmak üzere suçla ve suçlulukla mücadele, kamu güvenliği ve kamu düzeni için zorunlu olmakla birlikte, GBT sisteminin uygulamada ölçüsüzce genişletildiği anlaşılmaktadır. Örneğin, başvuru konusu olayda olduğu gibi, trafik veya genel bir asayiş kontrolü yapan kolluk kuvvetlerinin, kişilerle ilgili varsa arama, yakalama, devam eden soruşturma veya kovuşturma, sahip olduğu veya geri alınmış olabilecek ehliyet, silah ruhsatı, pasaport, yurda giriş-çıkış ve benzeri bilgilere derhal erişebilmeleri ne kadar gerekli ve ölçülü ise, her trafik polisinin GBT bilgilerine baktığı kişinin - başvuruda olduğu gibi- 25 yıl önce para cezasına mahkum olduğu, adli sicilden çıkarılmış bir hırsızlık olayını bilmesi aynı derecede gereksiz ve ölçüsüzdür.

4. Bu nedenlerle, Anayasanın 13. maddesinin emrettiği anlamda “kanunilik” şartını karşılamayan, fiilen silinemeyen ve kişiye karşı hangi amaçla kim tarafından kullanılacağı bilinemeyen bir arşive dönüşen GBT uygulaması nedeniyle, başvurucunun temel haklarının ihlal edildiğini kabul etmek gerekir.

Üye

Osman Alifeyyaz PAKSÜT

Üye

Muammer TOPAL

KARŞIOY GEREKÇESİ

1. Başvuruya konu olaylar şöyledir : Başvurucu 1989 yılı Ekim ayında işlediği üç hırsızlık suçu nedeniyle ceza mahkemesi tarafından 1990 yılında adli para cezası ile cezalandırılmış ve cezası ertelenmiştir. İzmir 8. Asliye Ceza Mahkemesi 9.4.1996 tarihli kararıyla tecilli cezanın işlenmemiş sayılarak adli sicil kayıtlarından silinmesine karar vermiştir. Başvurucunun 2006 yılında Emniyet

Genel Müdürlüğüne yaptığı Genel Bilgi Toplama (GBT) kayıtlarının silinmesi istemi, Bilgi Toplama Yönergesi gerekçe gösterilerek reddedilmiş, bu işlemin iptali için açtığı dava da idare mahkemesince reddedilerek, karar Danıştay 10. Dairesince onanmıştır.

2. Başvurunun, GBT kaydı nedeniyle özel hayata saygı hakkının ihlal edildiği iddiasına ilişkin bölümünde başvuru; mahkumiyetine ilişkin adli sicil kaydı silinmesine karşın GBT kaydının silinmemesi nedeniyle polis kontrollerinde bu konunun gündeme geldiğini, polisin kendisine tutumunun değiştiğini ve ailesi yanında küçük düştüğünü, bu durumun özel hayata saygı hakkını ihlal ettiğini ileri sürmektedir.

3. Başvurucunun geçmiş mahkumiyetine ilişkin bilgilerin tüm güvenlik taramalarında kullanılabilir otomatik bir ortam oluşturan GBT kaydında tutulması, Anayasanın 20. maddesinde düzenlenen özel hayatına saygı hakkına müdahale teşkil etmektedir. Bu müdahalenin ihlal oluşturup oluşturmadığı meselesi, kanuni temeli ile meşru amacının varlığına ve demokratik bir toplumda gerekli ve ölçülü olup olmadığına bağlı bulunmaktadır.

4. Bilindiği üzere kanuni temel ölçütü bakımından AİHS hukukundaki otonom anlamından farklı olarak Anayasamızda temel hakların sınırlanmasıyla ilgili düzenlemelerin iç hukukumuzdaki anlamıyla 'kanun'a dayanması zorunludur (AY m. 13, 20/3). Böylece kişi hakları güvence altına alınmakta ve idarenin yetkisi kanunla sınırlandırılmaktadır. Temel hakların sınırlandırılmasının kanun'a dayanması zorunluluğu; sınırlamanın kapsamı ve sınırının parlamento tarafından belirlenmesini öngörmekle, demokratik bir rejimde oluşumu ve karar alma süreci boyutuyla parlamentonun insan haklarının korunması konusundaki işlevinin bir gereği olarak görülmesinden kaynaklanmaktadır. Yürütme elbette, sınırlama hükümleri ve çerçevesi kanunda belirlenmek kaydıyla temel haklar alanında da düzenleyici işlemler yapabilir. Fakat Anayasadaki güvence sistemi bakımından temel haklara ilişkin olarak kanunda öngörülmemen bir sınırlamanın düzenleyici işlemlerle yapılması söz konusu olamaz. Aksi durum, temel haklara ilişkin Anayasal güvenceleri işlevsiz bırakacağı gibi pozitif temeli bulunmayan düzenlemelerin hukuki sonuç doğurmasına da cevaz verilemez. Anayasa Mahkemesinin bir kararında belirtildiği gibi, "bir hukuk devletinde kaynağını anayasadan almayan bir düzenlemenin hukuk alanında varlığını sürdürmesi düşünülemez." (AYM 11.06.2003, E.2001/346, K.2003/63).

5. Soruşturma ve kovuşturma sürecinde suç işlediği iddia edilen kişiler hakkındaki kolluk işlemleri ve adli işlemler Ceza Muhakemesi Kanunu ve kolluğun görevleriyle ilgili kanunlar çerçevesinde yürütülmektedir. Örneğin yakalama kararının ilgili kolluk birimlerinde kayda girmesi, mahkumiyet veya beraat kararının yargılayan ve kanun yolu denetimi yapan mahkemelerin kayıt ve karar

arşivlerinde yer alması bu süreçle bağlantılıdır. Mahkemelerin arşivlerinde yer alan kararlar kanunda belirtilen nedenler dışında kamu kurumlarına da kapalıdır. Mahkumiyet kararlarının genel bilgi sistemine kaydedilmesi ise 5352 Sayılı Adli Sicil Kanununda düzenlenmiştir. Anılan kanun hükümlerinde kaydın süresi, yararlanacak kurumlar, bilgi güvenliğinin korunması, kaydın silinmesi koşulları, vb. güvenceler sağlanıp, Resmi Gazetede yayımlandığı için kişilerin erişimine de açık bulunması dolayısıyla kanunilik bakımından gerekli anayasal güvenceler temin edilmiş durumdadır. Buna karşın ceza soruşturma veya kovuşturmasının herhangi bir şekilde sonuçlandığı durumda, kişinin soruşturma-kovuşturma sürecine veya sonucuna ilişkin bilgilerin adli sicil dışında genel ya da lokal bir bilgi arşivine kaydedilmesini öngören bir kanun hükmü bulunmamaktadır.

6. Kolluğun Genel Bilgi Toplama kaydının dayanağı, İçişleri Bakanlığı Emniyet Genel Müdürlüğü Kaçakçılık ve İstihbarat Daire Başkanlığı tarafından çıkartılan 29.3.2005 tarihli Yönergede gösterilmektedir. Yönerge uyarınca, herhangi bir suç nedeniyle yakalama kaydı bulunanlar, kayıp şahıslar, belli hakları kullanmaktan yoksun bırakılanlar ve 9/b maddesinde sayılan bazı suçları işleyenler hakkında bilgi formu düzenlenmektedir (m.7). Yönergenin 16. maddesine (16/b-4) göre, 9/b maddesinde belirtilen (hırsızlık dahil) suçları işleyenler hakkında düzenlenen bilgi formları, kişilerin ölümlerine kadar silinmemektedir. Yönergenin 1. maddesinde açıklandığı üzere suçla ve suçlulukla mücadele görevine ilişkin olarak böyle bir bilgi kaydı düzenlenmesinin meşru amacının bulunduğu ileri sürülebilir. Fakat müdahalenin ihlal oluşturmaması için Yönergenin kanuni dayanağının bulunması, başka bir anlatımla temel hakka ilişkin sınırlamanın kanuna dayanması gerekmektedir.

7. Anayasanın 13. maddesinde temel hakların sınırlandırılmasına ilişkin düzenlemelerin münhasıran (ancak) kanunla yapılabileceği ifade edilmiş, 20/3. maddesinde de kişisel verilerle ilgili düzenlemelerin kanunla yapılması gerektiği belirtilmiştir. Aynı maddeye göre kişisel verilerle ilgilihak kişilere; verilerin korunmasını isteme, bilgilendirme, verilere erişme, düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar.Yine kişisel veriler ancak kanunla öngörülen hallerde veya kişinin açık rızasıyla işlenebilir, korunmasıyla ilgili esas ve usuller kanunla düzenlenir. Mahkememiz kararlarında müstakar biçimde belirtildiği üzere, hukuk devleti ilkesinin alt unsuru olan hukuki güvenlik ilkesi gereği hukuk kuralları belirli ve öngörülebilir olmalıdır. Yasal düzenlemeye dayanması, erişilebilir, bilinebilir ve öngörülebilir olmaları kaydıyla mahkeme içtihatları ve yürütmenin düzenleyici işlemleri ile de hukuki belirlilik sağlanabilir. Fakat tali düzenleyici işlemler ve yargı kararlarının belirliliği sağladığının söylenebilmesi için sınırlamaya ilişkin temel unsurların kanunda açık ve kesin bir biçimde belirlenmiş ve erişilebilir olması zorunludur. Ne var ki Yönerge ilk olarak erişilebilirlik

testinden geçememektedir. Bakanlık yazısında 'hizmete özel' dereceli olduğu belirtilen Yönerge Resmi Gazetede yayımlanmadığından kişilerin düzenlemeye erişimi ve kuralları öngörmeleri de mümkün bulunmamaktadır. Buna karşın konunun her boyutuyla değerlendirilebilmesi için, sınırlamanın kanuni dayanağının varlığı sorununu ayrıca incelemeye gerek duymaktayız.

8. İçişleri Bakanlığı'nın 11.6.2015 tarih ve 1962 sayılı Yazısında Yönergenin kanuni dayanağı olarak; Bakanlığın kuruluşuna ilişkin 3152 Sayılı Kanunun 13/1-c ve 33. maddeleri ile 2559 sayılı PVSK'nın ek 7. maddesi, gösterilmiştir. Kaçakçılık İstihbarat, Harekat ve Bilgi Toplama Dairesi Başkanlığının görevlerini düzenleyen 3152 sayılı Kanunun 13/1-c maddesinde verilen yetki; "c) Suç işleyip ele geçmeyen kişilerin, çalınan veya kaybedilen motorlu taşıtların, ateşli silahların, kimliği ispata yarayan her türlü belgelerin kayıtlarını tutarak güvenlik kuvvetlerine bildirmek, görevli kuruluşlarla ilgili koordinasyon sağlamak." hususlarını kapsamaktadır. Görüldüğü üzere maddedeki yetki suç işleyip ele geçirilemeyen kimseler hakkında bilgi kaydı tutulmasıyla sınırlıdır. 3152 sayılı Kanunun 33. maddesinde ise İçişleri Bakanlığının düzenleme yapma yetkisi; "Bakanlık, kanunla yerine getirmekle yükümlü oldukları hizmetleri; tüzük, yönetmelik, tebliğ, genelge ve diğer idari metinlerle düzenlemekle görevli ve yetkilidir." şeklinde ifade edilmiştir. Belirtilen düzenleme yetkisinin kullanılabilmesi için, kanunda açık bir yetkinin varlığına ihtiyaç olduğu açıktır. Dolayısıyla da bu hükümlerin Yönergeye kanuni dayanak olarak kabulü mümkün değildir.

9. Yönergeye dayanak olarak gösterilen 2559 sayılı Kanunun ek 7. maddesi ise şöyledir: "Polis, ... emniyet ve asayişini sağlamak üzere ülke seviyesinde istihbarat faaliyetlerinde bulunur, bu amaçla bilgi toplar, değerlendirir, yetkili mercilere veya kullanma alanına ulaştırır." Bu hüküm, gerek diğer kanunlarda ve gerekse bu kanunda polise verilen yetkiler çerçevesinde bilgi toplamayı kapsamaktadır. Diğer kanunlarda verilen yetkinin sınırı yukarıda belirtilmişti. Ek 7. maddede ise emniyet ve asayişin sağlanması için istihbarat yapılması ve bilgi toplanması düzenlenmektedir. Ayrıca kişilerin temel haklarıyla ilgili Anayasal ilkeler ile diğer kanun hükümleri de sözü edilen düzenleme yetkisinin sınırını oluşturmaktadır. Görüleceği üzere anılan hükümde temel hakların sınırlanmasıyla ilgili olarak idareye herhangi bir yetki verilmiş değildir.

10. Yukarıda belirtildiği üzere kişilerin mahkumiyetlerine ilişkin bilgilerin genel otomatik bilgi sistemine kaydedilmesi Adli Sicil Kanununda düzenlenmektedir. Bu kanun uyarınca hak yoksunluğuna neden olan kayıtlar dahi, yasaklanmış hakların geri alınması kararı verilmesi durumunda 15 yıl, böyle bir karar alınmamışsa 30 yıl, diğer mahkumiyet kayıtları ise infaz veya arşive alınma tarihinden itibaren 5 yıl sonra arşiv kaydından silinmektedir. Buna karşılık Yönerge ile düzenlenen GBT sisteminde kişiler hakkında herhangi bir güvence sağlanmadan süresiz (kalan

ömürle sınırlı) bir kayıt sistemi öngörülmüştür. GBT kaydındaki bilgilerin özellikle yapılan güvenlik taramaları ve güvenlik soruşturmalarında kullanıldığı anlaşılmaktadır (AYM B. No: 2013/2941, 11/5/2016, par. 88). Nitekim Anayasa Mahkemesi Adli Sicil Kanununun, arşiv bilgilerinin silinmesiyle ilgili 12. maddesinin 1. fıkrasını iptal ederken, söz konusu kuralda hak kısıtlamaları sona ermesine karşın arşiv kaydının 80 yıl süreyle veya kişinin ölümüne kadar sürdürülmesinin, Anayasadaki hukuk devleti ilkesine (m.2) ve kişinin maddi ve manevi varlığını koruma ve geliştirme hakkına (m.5, 17/1) aykırı olduğunu ifade etmiştir (bkz. AYM 2008/44 E.-2011/21 K., 20.1.2011; RG. : 14.04.2011-27905). Bu iptalden sonra yasama organı 12. maddeyi mevcut şekliyle yeniden düzenlemiştir.

11. Konuyla ilgili kanunlarda kişiler hakkındaki kesinleşmiş suç kayıtlarının dahi ancak belirli koşullarda ve belirli sürelerle otomatik bilgi sistemine kaydedilebileceği düzenlenmişken adli sicil sisteminden bağımsız şekilde, kolluk tarafından kanuna dayanmayan ve vatandaşlarca ulaşılabilir olmayan tali düzenlemelerle ayrı ve otomatik bir kayıt sistemi oluşturulması, müdahalenin kanuniliği yönünden Anayasanın 13. ve 20/3. maddelerine aykırıdır. Kanuni temeli olmayan bir müdahalenin hak ihlaline yol açacağı da açıktır.

12. Diğer taraftan, kanuni dayanağının bulunduğu kabul edilmesi durumunda dahi müdahalenin demokratik toplumda gerekli ve ölçülü olduğu söylenemez. Suçla ve suçlulukla mücadele ve bazı kamu görevlerinin gerektirdiği etik ilkelere bağlılık yönünden belirli bir süreyle adli sicil kayıtlarının merkezi arşiv sisteminde tutulmasında kamu yararı görülmektedir. Bu amaçla Adli Sicil Kanunu düzenlenmiş ve gerekli anayasal güvenceler öngörülmüştür. Ele geçirilemeyen suç zanlılarının veya cezasının infazı için aranan kimselerin kolluk tarafından merkezi kayıt sistemine kaydedilmesinin de kamu yararına yönelik ve gerekli olduğu söylenebilir. Buna karşılık yakalanarak işlemleri veya infazı tamamlanmış kişilere yönelik mahkumiyet kayıtlarının bir kısım suçlar bakımından merkezi bir sistemde ve ömür boyu sürecek şekilde (Yönerge, m.16/b-4) tutulmasının demokratik bir toplumda gerekli ve ölçülü olduğu kabul edilemez. Böyle bir uygulama, kişilerin devlet tarafından ömür boyunca izlendiği anlamına gelmektedir. Suç işleyen kişilerin potansiyel olarak ömür boyu suç işleyeceği varsayılarak izlemeye tabi tutulması hukuk devleti ilkesiyle ve Anayasanın 38. maddesinde ifade edilen masum sayılma hakkıyla bağdaşmaz.

Belirtilen nedenlerle, başvuranın özel hayatına saygı ve gizliliğinin korunması hakkının ihlal edildiği düşüncesiyle oy kullanmış bulunmaktayız.

Üye

Hasan Tahsin GÖKCAN

Üye

Yusuf Şevki HAKYEMEZ

Anayasa Mahkemesi - N.B.B. (Unutulma Hakkı) Kararı (2013/5653)

N.B.B. [GK], B. No: 2013/5653, 3/3/2016

Başvuru, bir gazetenin İnternet haber arşivinde erişilebilir durumda olan haber ve yayınlar ile ilgili içeriğin yayından kaldırılması yönündeki talebin reddedilmesinin şeref ve itibarın korunması hakkını ihlal ettiği iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

GENEL KURUL

KARAR

N.B.B. BAŞVURUSU

(Başvuru Numarası: 2013/5653)

Karar Tarihi: 3/3/2016

R.G. Tarih ve Sayı: 24/8/2016-29811

GENEL KURUL

KARAR

GİZLİLİK TALEBİ KABUL

Başkan: Zühtü ARSLAN

Başkanvekili: Burhan ÜSTÜN

Başkanvekili: Engin YILDIRIM

Üyeler: Serdar ÖZGÜLDÜR, Serruh KALELİ, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ, Alparslan ALTAN, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Erdal TERCAN, Muammer TOPAL, M. Emin KUZ, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Rıdvan GÜLEÇ

Raportör: Murat ŞEN

Başvurucu: N.B.B

Vekili: Av. Ahmet Volkan MEMİŞ

I. BAŞVURUNUN KONUSU

1. Başvuru, bir gazetenin İnternet haber arşivinde erişilebilir durumda olan haber veyayınlar ile ilgili içeriğin yayından kaldırılması yönündeki talebin reddedilmesinin şeref ve itibarın korunması hakkını ihlal ettiği iddiasına ilişkindir.

II.BAŞVURU SÜRECİ

2. Başvuru 22/7/2013 tarihinde İstanbul 26. Sulh Ceza Mahkemesi vasıtasıyla yapılmıştır. Başvuru formu ve eklerinin idari yönden yapılan ön incelemesi neticesinde başvurunun Komisyona sunulmasına engel teşkil edecek bir eksikliğinin bulunmadığı tespit edilmiştir.

3. İkinci Bölümün Birinci Komisyonunca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.

4. Bölüm Başkanı tarafından 11/7/2014 tarihinde, başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.

5. Başvuru belgelerinin bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık görüşünü 14/8/2014 tarihinde Anayasa Mahkemesine sunmuştur.

6. Bakanlık tarafından Anayasa Mahkemesine sunulan görüş 1/9/2014 tarihinde başvurucuya tebliğ edilmiştir. Başvurucu, Bakanlık görüşüne karşı beyanda bulunmamıştır.

7. İkinci Bölümün 3/2/2016 tarihinde yaptığı toplantıda başvurunun niteliği itibarıyla Genel Kurul tarafından karara bağlanması gerekli görüldüğünden Anayasa Mahkemesi İçtüzüğü'nün 28. maddesinin (3) numaralı fıkrası uyarınca dosyanın Genel Kurula sevkine karar verilmiştir.

III. OLAY VE OLGULAR

A. Olaylar

8. Başvuru formu ve eklerinde ifade edildiği şekliyle ilgili olaylar özetle şöyledir:

9. Ulusal ölçekte yayımlanan bir gazetenin İnternet arşivi sayfalarında, başvurucu hakkında uyuşturucu kullandığı iddiası ile yürütülen bir ceza kovuşturması neticesinde adli para cezasına hükmedilen olaya ilişkin olarak 1998 yılında iki, 1999 yılında bir olmak üzere toplam üç haber başlığı yayımlanmıştır.

10. Başvurucu, ilgili basın kuruluşunun İnternet sayfasının arşiv bölümünde hakkındaki haberlerin yayınına devam ettiğini belirterek 2/4/2013 tarihinde ilgili basın kuruluşuna İnternet yayınının kaldırılması hakkında ihtarname göndermiştir. Bu ihtarname 3/4/2013 tarihinde tebliğ edilmiştir.

İhtarnamenin içeriğinde sitede yayımlanan haberlerin başvuruçunun şeref ve haysiyetini zedelediği, özel hayatına ilişkin mahremiyetini ortadan kaldırdığı, topluma mal olmuş ünlü bir kişi olmamasına rağmen başta aile yaşamı olmak üzere iş ve sosyal hayatını olumsuz etkilediği ileri sürülmüştür.

11. 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 9. maddesinin (1) numaralı fıkrası gereğince ilgili siteniniki gün içinde anılan haber içeriklerini kaldırmaması üzerine başvuruçunun, içeriklerin yayından kaldırılması talebiyle ilgili basın kuruluşu aleyhine 18/4/2013 tarihinde (kapatılan) İstanbul 36. Sulh Ceza Mahkemesine başvurmuştur.

12. (Kapatılan) İstanbul 36. Sulh Ceza Mahkemesi 22/4/2013 tarihli ve 2013/314 Değişik İş sayılı kararı ile talebin kabulüne karar vermiştir. Mahkemenin gerekçesi şöyledir:

"Yazı içeriğine yönelik yapılan incelemede, 1998 yılında gerçekleşen bir olay nedeniyle kamuoyuna yansıtılan bir haber niteliğinde olduğu anlaşılmış olup, basının görevi genel olarak kamu yararı ve toplumsal ilgi taşıyan, gerçek ve güncel haberlere ilişkin bilgi vermek, düşünceye sevk etmek, eleştiri yorum ve uyarılarda bulunmak olarak tanımlandığında talebe konu yazının güncelliğini yitirdiği, haber değerinin bulunmadığı, gündemde kalmasında kamu yararı bulunmadığı ve bu haliyle muhatabının özel hayatına ilişkin incitici ve örseleyici bir bilgi niteliğinde olduğu ve her isteyen kolaylıkla özel hayata erişme olanağı sağlaması bakımından kişilik haklarının ihlal edilmesi sonucunu doğurduğu gözetilerek, yazı içeriğinin yayından çıkarılması talebinin kabulü gerektiği değerlendirilmiştir."

13. Anılan karara karşı yapılan itiraz, İstanbul 2. Asliye Ceza Mahkemesinin 28/5/2013 tarihli ve 2013/235 Değişik İş sayılı kararlarıyla kabul edilerek (kapatılan) İstanbul 36. Sulh Ceza Mahkemesinin kararının kaldırılmasına hükmedilmiştir. Mahkemenin gerekçesi şöyledir:

"Talep konusu ... ve ... isimli sitelerde yayımlanan ... başlıklı haberlerde içeriğin yayından çıkarılması talebinde bulunanın şeref ve haysiyetini ihlal edici bir içerik bulunmadığı gibi arşiv niteliğindeki haberin yayınlandığı tarihte görünür gerçekliğe uygun olduğu, yazıda talepte bulunanı rahatsız edici (kanaat ve olgu biçiminde) görüşler olsa da olguların daha sonra yanlış çıkması halinde dahi hak ihlal etme kastı bulunmayan gazetecinin bundan sorumlu tutulmayacağı, talepte bulunanın kişilik haklarına saldırı niteliğinde söz ve cümlelerin kullanılmadığı anlaşılmalı itirazın kabulüne..."

14. Karar21/6/2013 tarihinde başvuruçunun vekiline tebliğ edilmiştir.

15. Başvuruçunun22/7/2013 tarihinde bireysel başvuruda bulunmuştur.

B. İlgili Hukuk

16. 6/2/2014 tarihli ve 6518 sayılı Kanun ile değiştirilmeden önce başvuru tarihinde yürürlükte olan 5651 sayılı Kanun'un "İçeriğin yayından çıkarılması ve cevap hakkı" kenar başlıklı 9. maddesi şöyledir:

"(1) İçerik nedeniyle hakları ihlâl edildiğini iddia eden kişi, içerik sağlayıcısına, buna ulaşamaması halinde yer sağlayıcısına başvurarak kendisine ilişkin içeriğin yayından çıkarılmasını ve yayındaki kapsamından fazla olmamak üzere hazırladığı cevabı bir hafta süreyle internet ortamında yayımlanmasını isteyebilir. İçerik veya yer sağlayıcı kendisine ulaştığı tarihten itibaren iki gün içinde, talebi yerine getirir. Bu süre zarfında talep yerine getirilmediği takdirde reddedilmiş sayılır.

(2) Talebin reddedilmiş sayılması halinde, kişi onbeş gün içinde yerleşim yeri sulh ceza mahkemesine başvurarak, içeriğin yayından çıkarılmasına ve yayındaki kapsamından fazla olmamak üzere hazırladığı cevabın bir hafta süreyle internet ortamında yayımlanmasına karar verilmesini isteyebilir. Sulh ceza hâkimi bu talebi üç gün içinde duruşma yapmaksızın karara bağlar. Sulh ceza hâkiminin kararına karşı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir.

(3) Sulh ceza hâkiminin kesinleşen kararının, birinci fıkraya göre yapılan başvuruyu yerine getirmeyen içerik veya yer sağlayıcısına tebliğinden itibaren iki gün içinde içerik yayından çıkarılarak hazırlanan cevabın yayımlanmasına başlanır.

(4) Sulh ceza hâkiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır. İçerik veya yer sağlayıcının tüzel kişi olması halinde, bu fıkra hükmü yayın sorumlusu hakkında uygulanır."

17. 5651 sayılı Kanun'un 6518 sayılı Kanun ile değiştirilen 9. maddesi şöyledir:

"(1) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğe erişimin engellenmesini de isteyebilir.

(2) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişilerin talepleri, içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılır.

(3) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talepleri doğrultusunda hâkim bu maddede belirtilen kapsamda erişimin engellenmesine karar verebilir.

(4) Hâkim, bu madde kapsamında vereceği erişimin engellenmesi kararlarını esas olarak, yalnızca kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verir. Zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemez. Ancak, hâkim URL adresi belirtilerek içeriğe erişimin engellenmesi yöntemiyle ihlalin engellenemeyeceğine kanaat getirmesi hâlinde, gerekçesini de belirtmek kaydıyla, internet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilir.

(5) Hâkimin bu madde kapsamında verdiği erişimin engellenmesi kararları doğrudan Birliğe gönderilir.

(6) Hâkim bu madde kapsamında yapılan başvuruyu en geç yirmi dört saat içinde duruşma yapmaksızın karara bağlar. Bu karara karşı 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir.

(7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

(8) Birlik tarafından erişim sağlayıcıya gönderilen içeriğe erişimin engellenmesi kararının gereği derhâl, en geç dört saat içinde erişim sağlayıcı tarafından yerine getirilir.

(9) Bu madde kapsamında hâkimin verdiği erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının veya aynı mahiyetteki yayınların başka internet adreslerinde de yayınlanması durumunda ilgili kişi tarafından Birliğe müracaat edilmesi hâlinde mevcut karar bu adresler için de uygulanır.

(10) Sulh ceza hâkiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişi, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır."

18. 19/6/2004 tarihli ve 5187 sayılı Basın Kanunu'nun 3. maddesi şöyledir:

"Basın özgürdür. Bu özgürlük; bilgi edinme, yayma, eleştirme, yorumlama ve eser yaratma haklarını içerir.

Basın özgürlüğünün kullanılması ancak demokratik bir toplumun gereklerine uygun olarak; başkalarının şöhret ve haklarının, toplum sağlığının ve ahlakının, milli güvenlik, kamu düzeni, kamu güvenliği ve toprak bütünlüğünün korunması, Devlet sırlarının açıklanmasının veya suç işlenmesinin önlenmesi, yargı gücünün otorite ve tarafsızlığının sağlanması amacıyla sınırlanabilir."

19. Yargıtay Hukuk Genel Kurulunun 17/6/2015 tarihli ve E.2014/4-56, K.2015/1679 sayılı kararının ilgili kısmı şöyledir :

"...Unutulma hakkına gelince; unutulma hakkı ve bununla ilişkili olan gerektiği ölçüde ve en kısa süreliğine kişisel verilerin depolanması veya tutulması konuları, aslında kişisel verilerin korunması hakkının çatısını oluşturmaktadır. Her iki hakkın temelinde bireyin kişisel verileri üzerinde serbestçe tasarruf edebilmesini, geçmişin engeline takılmaksızın geleceğe yönelik plan yapabilmesini, kişisel verilerin kişi aleyhine kullanılmasının engellenmesini sağlamak yatmaktadır. Unutulma hakkı ile geçmişinde kendi iradesi ile veya üçüncü kişinin neden olduğu bir olay nedeni ile kişinin geleceğinin olumsuz bir şekilde etkilenmesinin engellenmesi sağlanmaktadır. Bireyin geçmişinde yaşadığı olumsuz etkilerden kurtularak geleceğini şekillendirebilmesi bireyin yararına olduğu gibi toplumun kalitesinin gelişmişlik seviyesinin yükselmesine etkisi de tartışılmazdır.

Unutulma hakkı; üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerin silinmesini ve yayılmasının önlenmesini isteme hakkı olarak ifade edilebilir.

..."

IV. İNCELEME VE GEREKÇE

20. Mahkemenin 3/3/2016 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları

21. Başvurucu, hakkında yapılan ceza yargılaması sonucunda adli para cezası ödemeye mahkûm edildiği olay ile ilgili olarak bir basın yayın organının İnternet sitesinde 1998 ve 1999 yıllarında haber ve yayınlar yapıldığını, ilgili yayın kuruluşunun İnternet sitesinin arşiv bölümlerinde hakkındaki haber ve yayınların yer almaya devam ettiğini, yayınların kaldırılması yönündeki talebinin kabul edilmesine rağmen itiraz merciince içeriğin yayından kaldırılması talebinin kabulüne dair kararın kaldırılmasına hükmedildiğini, belirtilen İnternet sitelerinde yer almaya devam eden haber içeriğinin yayından kaldırılması yönündeki taleplerinin yargısal makamlar tarafından reddedilmesi nedeniyle Anayasa'nın 12., 17., 20., 25., 26., 27. ve 32.maddelerinde tanımlanan haklarının ihlal edildiğini iddia etmiştir.

B. Değerlendirme

1. Kabul Edilebilirlik Yönünden

22. Başvurucu, anılan şikâyetleri bağlamında Anayasa'nın 12., 17., 20., 25., 26., 27. ve 32. maddelerinde tanımlanan haklarının ihlal edildiğini iddia etmiş ise de başvurusunun iddialarının mahiyeti dikkate alındığında "Esas Yönünden" başlığı altında açıklanan gerekçelerle Anayasa'nın 20. maddesinin üçüncü fıkrası ile bağlantılı olarak Anayasa'nın 17. maddesinin birinci fıkrası kapsamında değerlendirilmesi uygun görülmüştür.

23. Somut olayda başvuru, şeref ve itibarına yönelik müdahale nedeniyle yalnızca Sulh Ceza Mahkemesine başvurarak İnternet sitesinde yayınlanan içeriklerin kaldırılması talebinde bulunmuş, diğer yollara başvurmamıştır.

24. Anayasa'nın 148. maddesinin dördüncü fıkrası ile 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 45. maddesinin (2) numaralı fıkrasında, bireysel başvuruda bulunulmadan önce ihlal iddiasının dayanağı olan işlem, eylem ya da ihmal için kanunda öngörülmüş olan idari ve yargısal başvuru yollarının tamamının tüketilmiş olması gerektiği belirtilmiştir. Temel hak ihlallerini öncelikle derece mahkemelerinin gidermekle yükümlü olması, kanun yollarının tüketilmesi koşulunu zorunlu kılar (Necati Gündüz ve Recep Gündüz, B. No: 2012/1027, 12/2/2013, §§ 19, 20).

25. Ancak belirtilen hükümlerde yer verilen olağan başvuru yolları ibaresinin, başvuru yollarının şikâyetleri açısından makul bir başarı şansı sunabilecek ve bir çözüm sağlayabilecek nitelikte, kullanılabilir ve etkili başvuru yolları olarak anlaşılması gerekmektedir. Ayrıca başvuru yollarının tüketme kuralı ne mutlak ne de şeklî olarak uygulanabilir bir kural olup bu kurala riayet denetlenmesinde münferit başvurunun koşullarının dikkate alınması esastır. Bu anlamda hukuk sisteminde yalnızca birtakım başvuru yollarının varlığının değil aynı zamanda bunların uygulanma şartları ile başvuru yollarının kişisel koşullarının gerçekçi bir biçimde ele alınması gerekmektedir. Bu nedenle başvuru yollarının tüketilmesi noktasında kendilerinden beklenebilecek her şeyi yerine getirip getirmediği incelenirken başvurunun özellikleri dikkate alınmalıdır (S.S.A., B. No: 2013/2355, 7/11/2013, § 28).

26. O hâlde somut başvuruda devletin pozitif yükümlülüğünün, sulh ceza mahkemelerinin yetkisinde bulunan İnternet içeriğinin yayından çıkarılmasını gerekli kılıp kılmadığı değerlendirilmelidir. Başka bir deyişle sulh ceza mahkemeleri nezdinde bulunan içeriğin yayından çıkarılması ve erişimin engellenmesi yolunun başvuruya konu haber arşivi nedeniyle şeref ve itibar hakkının korunmadığı yönündeki şikâyetler açısından makul bir başarı şansı sunabilecek ve bir çözüm sağlayabilecek nitelikte kullanılabilir ve etkili bir başvuru yolu olup olmadığı tespit edilmelidir.

27. Hukuk sistemimizde İnternet içeriğinin yayından çıkarılmasının, başvurudaki gibi sulh ceza hâkimliklerine başvurmak suretiyle veya hukuk mahkemelerinde açılacak dava yolu ile gerçekleştirilmesi mümkündür (Ahmet Oğuz Çinko ve Erkan Çelik [GK], B. No:2013/6237, 2/7/2015). Ancak somut başvuruda, İnternet'ten kaldırılması istenen haberlerin çok uzun süredir yayımlandığı ve İnternet sitesindeki haber arşivi üzerinden kolayca ulaşılabilirdiği ve bu şekilde başvuru sahibinin şeref ve itibarını koruma bakımından müdahalenin çok uzun süredir devam ettiği gözetilerek ve başvuru sahibinin şeref ve itibar hakkının korunması ve kişisel verilerin korunması bu yayının bir an önce kaldırılması ile sağlanacağı değerlendirildiğinde sulh ceza hâkimliğine başvuru yolunun somut olayın koşulları açısından etkili bir yol olduğu kabul edilmelidir. Nitekim hukuk mahkemelerinde çekişmeli bir yargılama yolunun, somut olaydaki şeref ve itibarın korunması hakkına yönelik uzun süredir devam eden müdahalenin gecikmeksizin ve süratle bertaraf edilmesi ihtiyacını karşılayabileceği söylenemez (Türkiye İş Adamları ve Sanayiciler Konfederasyonu, B. No: 2014/8691, 6/10/2015, § 22).

28. Başvuru sahibinin hakkında yayımlanan haberlere hâlen bir gazetenin İnternet sitesindeki haber arşivi üzerinden kolayca ulaşılabilmesi ve bu arşiv haberin İnternet'ten çıkarılması talebinin reddedilmesi nedeniyle kişilik haklarının zarar gördüğüne ve Anayasa'nın 17. maddesinin ihlal edildiğine ilişkin şikâyetleri açıkça dayanaktan yoksun değildir. Ayrıca başka bir kabul edilemezlik nedeni de bulunmadığı için başvurunun bu şikâyetlere ilişkin kısmının kabul edilebilir olduğuna karar verilmesi gerekir.

2. Esas Yönünden

29. Başvurucu gerçeğe aykırı veya uydurma haber olduğunu ileri sürmediği 1998 ve 1999 yılında hakkında yürütülmüş soruşturmalara ilişkin haberlerin hâlen arşivde yer alması ve İnternet üzerinden kolayca ulaşılabilir olması nedeniyle özel ve iş hayatının olumsuz etkilendiğini ve itibarının zedelendiğini iddia etmiştir.

30. Bakanlık görüş yazısında, Avrupa İnsan Hakları Mahkemesinin (AİHM) özel yaşama saygı hakkı kapsamındaki içtihadına atfen ilgili içtihadta benimsenen ilkelerin başvurunun değerlendirilmesinde gözönünde bulundurulması gerektiği ifade edilmiştir.

a. Genel İlkeler

i. Kişinin Manevi Varlığını Koruma ve Geliştirme Hakkı

31. Başvuru sahibinin iddialarının temelinde 1998 ve 1999 yıllarında hakkında çıkan haberlere hâlen İnternet ortamında ulaşılabilmesinin şeref ve itibarını zedelediği şikâyeti yer almaktadır. Bu

bağlamda başvuru, geçmişte hakkında yapılan haber içeriğinin yayından çıkartılmasını talep etmiş ve nihayetinde talep reddedilmiştir.

32. Anayasa'nın 17. maddesinin birinci fıkrası şöyledir:

“Herkes, yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkına sahiptir.”

33. Bireyin kişisel şeref ve itibarı, Anayasa'nın 17. maddesinde yer alan "manevi varlık" kapsamında yer almaktadır. Devlet, bireyin manevi varlığının bir parçası olan kişisel şeref ve itibara keyfî olarak müdahale etmemek ve üçüncü kişilerin saldırılarını önlemekle yükümlüdür (Adnan Oktar (2), B. No: 2013/1123, 2/10/2013, § 33). Başka bir deyişle kişisel itibarın korunması hakkı Anayasa'nın 17. maddesinin birinci fıkrasının koruması altındadır (Kadir Sağdıç [GK], B. No: 2013/6617, 8/4/2015, § 36; İlhan Cihaner (2), B. No: 2013/5574, 30/6/2014, § 42).

34. AİHM, kişisel şeref ve itibara yapılan müdahaleleri Avrupa İnsan Hakları Sözleşmesi'nin (Sözleşme) "özel ve aile yaşamına, konuta ve haberleşmeye saygı hakkı" kenar başlıklı 8. maddesi kapsamında değerlendirmektedir. AİHM'e göre kişisel itibarın korunması hakkı, Sözleşme'nin 8. maddesi tarafından korunan özel yaşama saygı hakkının bir parçasıdır (Pfeifer/Avusturya, B. No: 12556/03, 15/11/2007 § 35; Axel Springer AG/ Almanya, B. No: 39954/08, 7/2/2012, § 83). Aynı şekilde gazete makalesinde hakaret içerdiği iddia edilen beyanlara karşı bir kimsenin itibarının korunması hakkı (White/İsveç, B. No: 42435/02, 19/12/2006, § 19) ile eleştirel bir gazete makalesine karşı kişinin korunmadığı iddiası da (Minelli/İsviçre (k.k.), B. No: 14991/02, 14/06/2005) özel yaşam kapsamında görülmüştür.

35. Kamusal bir tartışma bağlamında ve yayımlanan yazılar nedeniyle eleştirilmiş olsa bile bir kişinin itibarı, kimliğinin ve manevi bütünlüğünün bir parçasını oluşturur (Pfeifer/Avusturya, § 35) ve Anayasa'nın 17. maddesinin birinci fıkrasının koruması altındadır (Kadir Sağdıç, § 38; İlhan Cihaner (2), § 44).

36. Öte yandan Anayasa'nın 17. maddesinin birinci fıkrasının olaya uygulanabilmesi için kişinin itibarına yapılan saldırının belli bir ağırlık düzeyine erişmiş olması ve kişinin itibarına saygı gösterilmesini isteme hakkından başvuruçunun kişisel olarak yararlanmasını güçleştirecek şekilde yapılmış olması gerekir. Ayrıca öngörülebilir şekilde, şeref ve itibarın kendi eylemleri sonucunda zedelenmesi hâlinde kişinin Anayasa'nın 17. maddesinin getirdiği korumadan yararlanması söz konusu olamaz (Kadir Sağdıç, § 39; İlhan Cihaner (2), §§ 45, 46; benzer yöndeki AİHM kararı için bkz. Mater/Türkiye, B. No: 54997/08, 16/7/2013, § 52).

37. Yukarıda belirtilen şekilde şeref ve itibara yönelik bir müdahalenin Anayasa'nın 17. maddesinin birinci fıkrası kapsamında incelenebilmesi için gerekli olan belirli bir ağırlık eşliğini aşması ve müdahalenin öngörülebilir şekilde kişinin kendi eylemleri sonucu ortaya çıkmaması ön koşulları İnternet üzerinden uzun süredir devam eden yayınlar açısından farklı değerlendirilmelidir. İnternet ortamının sağladığı ulaşılabilirlik, yaygınlık, haber ve fikirlerin depolanmasındaki ve muhafazasındaki kolaylık dikkate alındığında yayımlandığı tarihte belirli ağırlık eşliğini aşmayan veya kişinin kendi eylemlerinden kaynaklanan haberlerin İnternet ortamında uzun süre erişebilir kalması kişilerin şeref ve itibarını zedeleyebilir.

38. Haberlerin İnternet ortamında yayınlanmasının kişisel verilerin korunması hakkı ile ilişkisi bulunmaktadır. Nitekim İnternet ortamına aktarılırken ve kişi ile haber arasında bağlantı kurulurken teknik olarak kişiye ait verilerin İnternet ortamına işlenmesi gerekmektedir. Kişisel verilerin işlenmesi 5651 sayılı Kanun kapsamında İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler olarak tanımlanan içerik sağlayıcısı tarafından yapılmaktadır. Bu bağlamda içerik sağlayıcılar, kişisel verileri İnternet ortamına aktaran ve böylelikle gazete arşivi üzerinden kişiler hakkındaki haberleri ulaşılabilir kılan kişilerdir. Şeref ve itibarın korunması hakkı ile kişisel veriler arasındaki bu ilişki İnternet ortamında şeref ve itibara yönelik saldırıların, kişisel verilerin korunması hakkı ile bağlantılı olarak değerlendirilmesini gerektirmektedir.

39. Anayasa'nın "Özel hayatın gizliliği" kenar başlıklı 20. maddesinin birinci ve üçüncü fıkraları şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

...

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

40. Anayasa'nın 20. maddesinde özel hayata saygı hakkı düzenlenmiştir. Özel hayat geniş bir kavram olup kapsayıcı bir tanımının yapılması oldukça zordur (Serap Tortuk, B. No: 2013/9660, 21/1/2015, Ş 31) Bununla beraber özel hayata saygı hakkı, kişinin maddi ve manevi bütünlüğü, fiziksel ve sosyal

kimliği, bireyin ismi, cinsel yönelimi, cinsel yaşamı gibi unsurları korumaktadır (Ahmet Acartürk, B. No: 2013/2084, 15/10/2015, § 46). Kişisel bilgiler ve veriler, kişisel gelişim, aile hayatı vb. konular da bu hakkın içinde yer almaktadır.

41. Öte yandan Anayasa'nın 20. maddesinin üçüncü fıkrasında herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı ifade edilmiştir. Maddede ayrıca kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir. Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla bir kişiye ilişkin bütün bilgileri ifade etmektedir. Kişisel verilerin korunması hakkı, kişinin onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır (AYM, E.2013/122, K.2014/74, 9/4/2014). Öte yandan kişisel verilerin korunması hakkı sadece kişisel verilerin işlenmesi sırasında değil bu veriler işlendikten sonra da düzeltilmesini veya silinmesini talep etme hakkını içermektedir. Bu hak, sadece kamu otoritesini kullanarak işlenen kişisel verileri değil gerçek ve tüzel kişiler tarafından işlenen verileri de kapsamaktadır.

42. Dolayısıyla ifade ve basın özgürlüğü kapsamında (bkz. §§ 56-64) İnternet ortamında yayınlanan bir haberin, Anayasa'nın 17. maddesinin birinci fıkrasında düzenlenen "kişinin manevi varlığının korunması ve geliştirilmesi hakkı" kapsamında kabul edilmesinin yanı sıra, kişinin kimliği ile bağlantı kurularak (Sevim Akat Eşki, B. No. 2013/2187, 19/12/2013, §§ 30,31; AYM, E.2011/34, K.2012/48, 30/3/2012; AYM, E.2009/85, K.2011/49, 10/3/2011) kişisel bir verinin alenileştirilmesi Anayasa'nın 20. maddesinin üçüncü fıkrasının dikkate alınmasını zorunlu kılmaktadır. Bu bağlamda anılan düzenlemenin sadece kamu otoritelerine yönelik olmadığı gerçek ve tüzel kişileri de bağladığı dikkate alınmalıdır. Somut olaydaki gibi kişisel bir veri olan kimlik bilgilerinin İnternet ortamında kamu otoritesi dışındaki gerçek ve tüzel kişiler tarafından yayınlanması, depolanması, muhafaza edilmesi ve kullanılması da anılan düzenlemeler kapsamında değerlendirilmelidir.

43. Anayasa'nın 20. maddesinin üçüncü fıkrasında kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızası ile işlenebileceği belirtilmiştir. Kişisel verilerin işlenmesi çok geniş bir çerçevede kişisel verilerin açıklanması, kaydedilmesi, aktarılması, elde edilebilir hâle getirilmesi, depolanması, muhafaza edilmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi kapsamaktadır. Dolayısıyla İnternet ortamında yayınlanan bir haberi ulaşılabilir kılan her türlü

kişisel verilerin işlenmesi de bu kapsamda değerlendirilmelidir. Her ne kadar kişisel verilerin ancak kanunla veya kişinin açık rızası ile işlenebileceği belirtilmiş ise de Anayasa'da tanımlanan ifade ve basın özgürlükleri kapsamında yapılan bir haberin anılan sınırların istisnası olacağı açıktır. Bu bağlamda temel mesele bireyin geçmişte haber yapılmış ve gerçeğe aykırılığı ileri sürülmemiş davranışlarının artık hatırlanmasının engellenmesidir. Zira ifade ve basın özgürlüğü kapsamında İnternet ortamına yüklenen haber ve fikirler çoğu kez kişisel verilerin de kullanılmasını ve işlenmesini beraberinde getirir. Başka bir ifade ile İnternet ortamındaki ilgili haber arşivlerindeki kişisel verilere veya habere erişimin engellenerek kişilerin yaptıklarının unutulmasının sağlanmasıdır.

44. Haber ve fikirleri iletmedeki hızı ve bunları saklama süresi ve kapasitesi gözetildiğinde İnternet, geleneksel iletişim araçlarından farklı, küresel olarak bilgiye erişim ve iletişim aracıdır. Dünya çapında milyonlarca kullanıcıya hizmet eden merkezi olmayan bu elektronik iletişim ağı, temel hak ve özgürlüklerin kullanımında farklı bir boyut getirmiştir. Temel hak ve özgürlüklerin kullanımında sağladığı imkânlar aynı zamanda temel hak ve özgürlüklere yönelik farklı müdahale yolları ortaya çıkarmıştır. Özellikle bireylerin özel hayatlarına ve manevi bütünlüklerine yönelik olarak çok ciddi müdahale alanları ortaya çıkmıştır. Bu nedenle geleneksel medyadan farklı olarak İnternet, ortaya çıkardığı riskler açısından farklı bir bakış açısı ile değerlendirilmelidir. Bu bağlamda ilgili hak ve özgürlükler açısından koruma ve ilerleme sağlayabilmek için kaçınılmaz olarak teknolojik gelişmeleri de dikkate alacak farklı bir yaklaşım belirlenmelidir.

45. İnternet'in yaygınlaşmasından önce kişilerin geçmişlerine ilişkin özel yaşamları zaman içinde kaybolmaktaydı. Bununla birlikte bireylerin geçmişlerinde yaşadıklarına ilişkin herhangi bir kayıt tutulmuşsa da bu kayıtlara ulaşılmasının zorluğu kişilerin geçmişlerinde yaptıkları hatalardan bağımsız olarak yaşamlarını sürdürmelerine imkân tanımaktaydı. Ancak günümüzde basit bir İnternet araştırması, bireylerin geçmişte yaptıkları ve hatırlamak ve/veya hatırlanılmasını istemedikleri hatalarını kolayca ortaya koymaktadır. Bu bağlamda İnternet ortamı, arşivde kalmış ve sadece araştırmacıların veya meraklıların özel çabası ile tespit edilebilecek haberleri kolaylıkla ulaşılabilir hâle getirmiştir. Haber arşivlerine erişimin kolaylaşması kişiler hakkında yapılan haberin unutulmasına fırsat vermeyen bir sanal ortam meydana getirmiştir. Bu durum İnternet'in yaygınlığı ile birlikte değerlendirildiğinde bireylerin geçmişte yaptıkları ve hatırlanmasını istemedikleri hususların sürekli olarak kişilerin karşısına çıkması ihtimalini kuvvetlendirmiştir.

46. İnternet'in yaygın kullanımı ile ortaya çıkan bu durum basının İnternet'i etkin olarak kullanmasıyla beraber ifade ve basın özgürlükleri ile şeref ve itibarın korunması arasındaki dengeyi ilkinin lehine bozmuştur. İfade ve basın özgürlüğü ile şeref ve itibarın korunması hakkı, eşit düzeyde

koruma gerektiren temel hak ve özgürlüklerdir. Bu nedenle bozulan dengenin her iki temel hak arasında tekrar kurulması zorunluluk olmuştur. İnternet haberciliği ile birlikte unutulmanın zor olduğu günümüzde anılan dengenin tekrar kurulabilmesi şeref ve itibar yönünden bireylerin unutulma hakkının kabul edilmesi ile mümkün olabilir. Bu bağlamda unutulma hakkı adil dengenin kurulması için vazgeçilmez niteliktedir (Avrupa Birliği Adalet Divanı, Google Spain SL, Google Inc/İspanya Kişisel Verilerin Korunması Kurumu, Mario Costeja Gonzales, C-131/12, 13/5/2014).

47. Unutulma hakkı Anayasa'mızda açıkça düzenlenmemiştir. Bununla birlikte Anayasa'nın "Devletin temel amaç ve ödevleri" başlığı altında düzenlenen 5. maddesinde "insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak" ifadesi ile devlete pozitif bir yükümlülük yüklenmiştir. Bu yükümlülük bağlamında Anayasa'nın 17. maddesinde düzenlenen kişinin manevi bütünlüğü bağlamında şeref ve itibarının korunması hakkı ve Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı ile birlikte düşünüldüğünde, devletin bireye geçmişte yaşadıklarının başkaları tarafından öğrenilmesi engellenerek "yeni bir sayfa açma" olanağı verme hususunda bir sorumluluğu olduğu açıktır. Özellikle kişisel verilerin korunması hakkı kapsamında kişisel verilerin silinmesini talep edebilme hakkı, kişilerin geçmişlerinde yaşadıkları olumsuzlukların unutulmasına imkân tanımayı kapsamaktadır. Dolayısıyla Anayasa'da açıkça düzenlenmeyen unutulma hakkı, İnternet vasıtasıyla ulaşılması kolay olan ve dijital hafızada bulunan haberlere erişiminin engellenmesi için Anayasa'nın 5., 17. ve 20. maddelerinin doğal bir sonucu olarak karşımıza çıkmaktadır. Diğer taraftan unutulma hakkının kabul edilmemesi, İnternet vasıtasıyla kolayca ulaşılabilir ve uzun süre muhafaza edilebilir kişisel veriler nedeniyle başkaları tarafından kişiler hakkında ön yargı oluşturabilmesi nedeniyle manevi varlığının geliştirilmesi için gerekli onurlu bir yaşam sürdürmesine ve manevi bağımsızlığına müdahaleyi sürekli kılmaktadır.

48. Anayasa Mahkemesinin ifade ve basın özgürlükleri ile şeref ve itibarın korunması hakkı arasındaki dengelemeye ilişkin kararlarında Anayasa'nın 17. maddesinin birinci fıkrası temelinde değerlendirme yaptığı gözetilerek unutulma hakkına ilişkin iddiaların İnternet ortamındaki haberlerin kişisel veriler ile arasındaki ilişki dikkate alınarak Anayasa'nın 17. maddesinin birinci fıkrası kapsamında inceleme yapılması gerekmektedir.

49. Öte yandan inceleme konusu olan başvuruya benzer diğer başvurularda devletin bir eylemi söz konusu olmayıp yargı mercilerince başvurucuların kişisel itibarlarına sağlanan korumanın yetersiz olduğu iddia edilmektedir. Anayasa'nın 17. maddesi esas olarak kamu görevlilerinin keyfi müdahalelerine karşı bireyi korumayı amaçlasa da söz konusu madde sadece devletin bu tür

müdahalelerde bulunmasından kaçınmasını sağlamayı amaçlamamaktadır. Anayasa'nın 17. maddesinin birinci fıkrasında mündemiç negatif yükümlülüğe, Anayasa'nın 5. maddesi dikkate alınarak bireyin maddi ve manevi varlığına etkin bir saygının sağlanması için gerekli pozitif yükümlülükler eklenebilir. Bu yükümlülükler, kişilerin birbirleri ile olan ilişkilerini de kapsayacak şekilde kişisel itibarının korunmasını isteme hakkına saygının güvence altına alınması amacıyla birtakım tedbirler alınmasını gerektirebilir (Ahmet Çinko ve Erkan Çelik [GK], B. No: 2013/6237, 3/7/2015, § 39). Bu tedbirlere, kişisel itibarın üçüncü kişilerin müdahalelerine karşı korunması hususunda da başvurulabilir (Kadir Sağdıç, § 40; İlhan Cihaner (2), § 47). Dolayısıyla unutulma hakkı kişilerin manevi varlıklarını geliştirmelerine bir fırsat vermek açısından devletin pozitif yükümlülüğünün bir sonucudur.

50. Unutulma hakkının İnternet gazete arşivlerindeki her türlü haber yönünden uygulanmasını beklemek mümkün değildir. Nitekim özellikle basın özgürlüğü temelinde gazete arşivinin araştırmacılar, hukukçular veya tarihçiler için önem taşıyan veriler olduğu açıktır. Bu durumda bir İnternet haberinin unutulma hakkı kapsamında İnternet'ten çıkarılabilmesi için yayının içeriği, yayında kaldığı süre, güncelliğini yitirme, tarihsel bir veri olarak kabul edilememe, kamu yararına katkısı (toplumsal açıdan haberin değeri, haberin geleceğe ışık tutan niteliği) habere konu kişinin siyasetçi veya ünlü olup olmadığı, haber veya makalenin konusu, bu bağlamda haberin olgusal gerçekler ya da değer yargısı içerip içermediği, halkın ilgili veriye yönelik ilgisi gibi hususların her somut olay açısından incelenmesi gerekmektedir.

51. Yapılacak değerlendirme sonucunda unutulmayı etkin kılacak farklı yöntemler benimsenebilir. 5651 sayılı Kanun'un 6518 sayılı Kanun ile değiştirilen 9. maddesinde erişimin engellenmesinin kapsamının kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL vb.) içeriğe erişimin engellenmesi yöntemiyle verileceği ve zorunlu olmadıkça İnternet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemeyeceği belirtilmiştir.

52. Bu bağlamda unutulma hakkı bağlamında ifade ve basın özgürlükleri ile şeref ve itibarın korunması hakkı arasındaki dengenin sağlanması açısından 5651 sayılı Kanun kapsamında yukarıda belirtilen önlemler alınabilir (bkz. § 51). Ancak alınacak tedbirlerin Anayasa'nın 13. maddesi gereğince ölçülülük kriteri esas alınarak yapılması gereklidir. Nitekim kişinin şeref ve itibarına yönelik müdahaleleri unutulma hakkı gereğince engellemek için arşivde arama yapmaya imkân tanıyan haber ile kişi arasında ilişki kuran kişisel verilerin silinmesi, haberin anonim hâle getirilmesi, haber içeriğinin bir kısmına erişimin engellenmesi gibi birçok yöntem benimsenebilir. Bu bağlamda yargının görevinin, İnternet ortamının sağladığı kolaylıkla zamanla kişilerin itibarına yönelik

müdahale oluşturan haberleri tamamen ortadan kaldırarak geçmişte meydana gelmiş olayların yeniden yazılmasını sağlamak olmadığı dikkate alınmalıdır. İnternet haber arşivinin bir bütün olarak basın özgürlüğünün korunması altında olduğu unutulmamalıdır.

ii. Düşünceyi Açıklama ve Yayma Özgürlüğü ile Basın Özgürlüğü

53. Başvuru konusu olayda İnternet üzerinden yayınlanan haber arşivinin başvuru ile ilgili kısmının yayından kaldırılması talebinin reddedilmesi söz konusudur.

54. Anayasa'nın "Düşünceyi açıklama ve yayma hürriyeti" kenar başlıklı 26. maddesi şöyledir:

"Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet resmi makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Bu fıkra hükmü, radyo, televizyon, sinema veya benzeri yollarla yapılan yayımların izin sistemine bağlanmasına engel değildir.

Bu hürriyetlerin kullanılması, millî güvenlik, kamu düzeni, kamu güvenliği, Cumhuriyetin temel nitelikleri ve Devletin ülkesi ve milleti ile bölünmez bütünlüğünün korunması, suçların önlenmesi, suçluların cezalandırılması, Devlet sırrı olarak usulünce belirtilmiş bilgilerin açıklanmaması, başkalarının şöhret veya haklarının, özel ve aile hayatlarının yahut kanunun öngördüğü meslek sırlarının korunması veya yargılama görevinin gereğine uygun olarak yerine getirilmesi amaçlarıyla sınırlanabilir.

Haber ve düşünceleri yayma araçlarının kullanılmasına ilişkin düzenleyici hükümler, bunların yayımını engellemek kaydıyla, düşünceyi açıklama ve yayma hürriyetinin sınırlanması sayılmaz.

Düşünceyi açıklama ve yayma hürriyetinin kullanılmasında uygulanacak şekil, şart ve usuller kanunla düzenlenir."

55. Anayasa'nın "Basın hürriyeti" kenar başlıklı 28. maddesinin ilgili fıkraları şöyledir:

"Basın hürdür, sansür edilemez. Basımevi kurmak izin alma ve malî teminat yatırma şartına bağlanamaz.

...

Devlet, basın ve haber alma hürriyetlerini sağlayacak tedbirleri alır.

Basın hürriyetinin sınırlanmasında, Anayasanın 26 ve 27 nci maddeleri hükümleri uygulanır.

..."

56. Haber ve fikirlerin iletilmesinde ve alınmasında önemli bir işlev gören İnternet, Anayasa'nın 26. maddesinde düzenlenen ifade özgürlüğünün güvencesi altındadır. Nitekim Anayasa Mahkemesi İnternet erişimine yönelik bir müdahalenin ifade özgürlüğü kapsamında incelenmesi gerektiğini kabul etmiştir (Yaman Akdeniz ve diğerleri, B. No: 2014/3986, 2/4/2014; Youtube Llc Corporation Service Company ve diğerleri [GK], B. No: 2014/4705, 29/5/2014). Öte yandan İnternet üzerinden her türlü haber ve görüşlerin iletilmesinin Anayasa'nın 28 ila 32. maddelerinde güvence altına alınan basın özgürlüğü kapsamında olduğunun kabulü mümkün değildir.

57. Ulaşılabilirliği, haber ve fikirlerin saklanma süresi ve kapasitesi ile hacimce büyük haber ve fikirleri iletme imkânı gözetildiğinde İnternet, halkın haber almasının ve bilgilerin iletilmesinin gelişiminde önemli bir role sahiptir. İnternet, herhangi bir sınırlama gözetmeksizin herkesin haber ve fikirlere ulaşması ile fikirlerini yayması noktasında çok önemli bir imkân sağlamaktadır. Bu durum ifade özgürlüğü açısından da çok geniş bir alan yaratmaktadır (Medya Gündem Dijital Yayıncılık Ticaret A.Ş. [GK], B. No:2013/2623, 11/11/2015, § 34).

58. İnternet'teki bu geniş faaliyet alanı çerçevesinde, yayımlanan haber ve fikirlerin Anayasa'nın 28. maddesinde güvence altına alınan basın özgürlüğü kapsamında değerlendirilip değerlendirilemeyeceği, her somut olay açısından ayrıca incelenmelidir. Bu kapsamda Anayasa'nın 28. maddesi ve devamı maddelerinde tanımlanan basın özgürlüğü her ne kadar temel olarak basılı kitle iletişim araçları çerçevesinde tanımlanmış ise de İnternet'te önemli bir yer işgal eden İnternet haberciliğinin, basının temel işlevi olan "gözetleyicilik" görevini yerine getirdiği sürece basın özgürlüğü kapsamında değerlendirilebilmesi mümkündür (Medya Gündem Dijital Yayıncılık Ticaret A.Ş. , § 36).

59. Başvuru konusu olayda başvurucu hakkında haberleri İnternet'te yayımlayan şirketin ülkemizde bilinen ve ulusal ölçekte yayımlanan bir gazetenin İnternet yayını olması ve bu bağlamda geleneksel gazeteciliğe yakınlığı ile "gözetleyicilik" görevini yerine getirdiği değerlendirilebilir. Dolayısıyla anılan haber arşivi sitelerinin basın özgürlüğü kapsamında değerlendirilmesi mümkündür.

60. Öte yandan belirlenmesi gereken bir diğer husus, haber arşivinin basın özgürlüğünün korumasından yararlanıp yararlanmayacağıdır.

61. Anayasa Mahkemesi birçok kararında ifade özgürlüğünün sadece düşünce ve fikirleri yayma özgürlüğünü değil haber ve fikirlere ulaşma özgürlüğünü de kapsadığını vurgulamıştır (Emin Aydın, B. No: 2013/2602, 23/1/2014, § 40; Kamuran Reşit Bekir [GK], B. No: 2013/3614, 8/4/2015, § 34). Bu bağlamda haber ve fikirlerin yayılmasını ve bunlara kamunun ulaşmasını kolaylaştıran İnternet'in toplum hayatındaki önemli rolü yadsınamaz. İnternet üzerinde arşiv oluşturma, aktüalitenin ve

haberlerin saklanmasına ve erişilebilirliğine büyük ölçüde hizmet etmektedir. Bu nitelikteki arşivler özellikle doğrudan halkın erişimine açık ve genelde ücretsiz olmaları nedeniyle tarih eğitimi ve araştırma faaliyetleri için kaynak sunmaktadır. Öte yandan demokratik bir toplumda basın ilk işlevi olan "gözetleyici" rolünün bir sonucu da arşivlerin halkın erişimine sunulmasıdır (Wegrzynowski ve Smolczewski/Polonya, B. No: 33846/07, 16/7/2013, § 59; Times Newspapers Ltd/Birleşik Krallık (No. 1 ve 2), B. No: 3002/03 23676/03, 10/3/2009, §§ 27, 45). Bu nedenle İnternet'te tutulan arşivlerin, ifade ve basın özgürlükleri kapsamında olduğu açıktır. Dolayısıyla İnternet'te yayımlanan ve gazetecilik faaliyeti kapsamında kabul edilen bir haber arşivinin yayından kaldırılması basın özgürlüğüne yönelik bir müdahale teşkil eder.

62. Demokrasilerde devletin eylem ve işlemlerinin, adli ve idari yetkililerin olduğu kadar basın ve aynı zamanda kamuoyunun da denetimi altında bulunması gerekmektedir. Yazılı, işitsel ve görsel basın; kamu gücünü kullanan organların siyasi kararlarını, eylemlerini ve ihmallerini sıkı bir denetime tabi tutarak ve vatandaşların karar alma süreçlerine katılımını kolaylaştırarak demokrasinin sağlıklı bir şekilde işlemlenmesini ve bireylerin kendilerini gerçekleştirmelerini güvence altına almaktadır (Kadir Sağdıç, § 50). Bu sebeple basın özgürlüğü, herkes için geçerli ve yaşamsal öneme sahip bir özgürlüktür (AYM, E.1997/19, K.1997/66, 23/10/1997).

63. AİHM, birçok kez demokratik bir toplumda basının oynadığı temel rolün altını çizmiştir. Her ne kadar başkalarının şöhret ve haklarının korunmasıyla ilgili olarak bazı sınırları aşmaması gerekse de basının, görev ve sorumluluklarının bilincinde olarak kamu yararını ilgilendiren her konuyu iletme görevi vardır. Basının böyle konularda bilgi ve fikir yaymadan ibaret olan görevine kamunun bu fikir ve bilgileri alma hakkı eklenir. AİHM'e göre bu görevi olmasaydı basın, vazgeçilmez "gözetleyicilik" işlevini yerine getiremezdi (Bladet Tromso ve Stensaas/Norveç [BD], B. No: 21980/93, 20/5/1999, §§ 59, 62; Pedersen ve Baadsgaard/Danimarka [BD], B. No: 49017/99, 17/12/2004, § 71).

64. İfade özgürlüğü ile onu tamamlayan ve ifade özgürlüğünün kullanılmasını sağlayan basın özgürlüğü, Anayasa'da yer alan temel hak ve özgürlükleri sınırlama rejimine tabidir. Anayasa'nın 28. maddesinin dördüncü fıkrasında basın özgürlüğünün sınırlanmasında 26. ve 27. madde hükümlerinin uygulanacağı belirtilmiştir. Böylece basın özgürlüğü, ifade özgürlüğü ile ilgili genel hüküm niteliğindeki 26. madde ile sanatsal ve akademik ifadelerle ilgili 27. maddedeki sınırlama rejimine tabi tutulmuştur. Basın özgürlüğüne yönelik diğer sınırlamalar ise 28. maddenin beşinci ve izleyen fıkralarında yer almıştır. Basının, Anayasa'nın 26., 27. ve 28. maddelerinde sayılan sınırlandırmalardan biri olan "başkalarının şöhret veya haklarının, özel veya aile hayatlarının" korunması için konmuş olan sınırlandırmalara uyması gerekir (Kadir Sağdıç, § 55; İlhan Cihaner (2),

§ 62). Bu itibarla "başkalarının şöhret veya haklarının, özel veya aile hayatlarının" korunması bağlamında şeref ve itibarın korunması hakkının etki alanını genişletmenin ifade ve basın özgürlüklerinin ihlali sonucunu doğurabileceği hatırd tutulmalıdır.

65. Öte yandan başkalarının şöhret ve haklarının korunmasıyla ilgili olarak bazı sınırların aşılmaması gerekse de basının, görev ve sorumluluklarının bilincinde olarak kamu yararını ilgilendiren her konuyu iletme görevi olduğu, onun bu tür konularda bilgi ve fikir yaymadan ibaret olan görevine kamunun bu fikir ve bilgileri alma hakkının eklendiği hatırd tutulmalıdır (Kadir Sağdıç, § 51)

66. Bu sebeple Anayasa'nın 17. maddesinin birinci fıkrasında koruma altına alınan şeref ve itibarın korunmasını isteme hakkı ile başvuruya konu İnternet haber arşivinin Anayasa'nın 28. maddesinde güvence altına alınan basın özgürlüğü ve bu özgürlükle bağlantılı olarak Anayasa'nın 26. maddesinde güvence altına alınan ifade özgürlüğü arasında Anayasa Mahkemesi içtihadında ortaya konulan kriterlere uygun şekilde bir denge kurulması gerekmektedir. Ancak geçmişteki olayların arşivlenmiş olması hâlinde çatışan haklar arasındaki dengelemenin güncel olaylara ilişkin yapılan haberlerden daha farklı yorumlanması makul kabul edilmelidir. Bu bağlamda, basının yayımladığı haberlerin gerçekliğine ilişkin olarak sorumluluk bilinci ile hareket etmesi (Kadir Sağdıç, §§ 53, 54; İlhan Cihaner (2), §§ 60, 61) gerekliliği, güncel haberlere nazaran doğası itibarıyla eskiyen ve yayımlanması ivedilik ve zorunluluk arz etmeyen geçmişe ilişkin haberler bakımından daha katı görünmektedir. Ancak yapılacak dengelemede haber arşivinin de Anayasa'nın 26. ve 28. maddeleri bağlamında güvence altına alındığı gözönünde tutulmalıdır.

b. Genel İlkelerin Somut Olaya Uygulanması

67. Başvuru konusu olayda, şikâyete konu haberler 1998 ve 1999 yılında başvuru hakkında yürütülen ceza yargılamasına ilişkindir. Başvuru bu haberlerin gerçeğe aykırı veya uydurma haber olduğunu ileri sürmemiştir. Başvuru haberlerin hâlen arşivde yer alması ve İnternet üzerinden kolayca ulaşılabilir olması nedeniyle özel ve iş hayatının olumsuz etkilendiğini ve itibarının zedelendiğini belirtmiştir. Başvurucunun şikâyeti İstanbul (kapatılan) 36. Sulh Ceza Mahkemesi tarafından kabul görse de itirazı inceleyen İstanbul 2. Asliye Ceza Mahkemesi itirazı kabul ederek İnternet yayınının kaldırılmasını uygun görmemiştir.

68. İstanbul (kapatılan) 36. Sulh Ceza Mahkemesi, 1998 yılında gerçekleşen bir olay nedeniyle başvuru hakkında haber yapıldığı ancak haberin güncelliğini yitirdiği ve haber değerinin kalmadığı, haberin gündemde kalmasında kamu yararı bulunmadığı ve bu hâliyle başvuru özel hayatına ilişkin incitici bir bilgi niteliğinde olduğu gerekçesiyle yazı içeriğinin yayından çıkartılmasına karar vermiştir (§ 13). Anılan karara itirazı değerlendiren İstanbul 2. Asliye Ceza

Mahkemesi talep konusu arşivin başvuru konusunun şeref ve haysiyetini ihlal edici bir içerik içermediği gibi yayınlandığı tarihte görünür gerçekliğe uygun arşiv niteliğindeki bir haberin olduğu ve başvuru konusunun kişilik haklarına saldırı niteliğinde söz ve cümlelerin kullanılmadığı gerekçesiyle itirazın kabulüne karar vermiştir (§ 14).

69. Mevcut olayda başvuru konusunun, haberlerin hâlen İnternet'te yer alması nedeniyle müdahale edilen şeref ve itibar hakkı ile içeriğin yayından çıkarılması hâlinde müdahale edilecek olan ifade ve basın özgürlükleri arasında adil bir denge kurulması gerekmektedir. Bu dengenin değerlendirilmesinde somut olay açısından gözönünde bulundurulması gereken önemli bir husus şeref ve itibarın korunması hakkı ve unutulma hakkı karşısında sadece ifade ve basın özgürlüklerinin değil ayrıca kişilerin haber ve fikirlere ulaşma özgürlüğünün de olduğudur. Anayasa Mahkemesi anılan hak ve özgürlükler arasında adil bir denge kurulup kurulmadığı hususundaki değerlendirmesini temel olarak yetkili yargı mercilerinin ortaya koyduğu gerekçe üzerinden yapmaktadır.

70. Yukarıda da belirtildiği üzere unutulma hakkı İnternet ortamında bir haberin uzun süredir kolayca ulaşılabilir olması nedeniyle kişinin şeref ve itibarını zedeleyen bir hâle dönüşmesi şeklinde karşımıza çıkmaktadır. Bu hakkın amacı, İnternet'in yaygınlaşması ve sağladığı imkânlar nedeniyle ifade ve basın özgürlükleri ile kişilerin manevi varlığının geliştirilmesi hakkı arasında gerekli hassas dengenin kurulmasını sağlamaktır. O hâlde bu yol, İnternet ortamında haber arşivini koruma altına alan basın özgürlüğünün ve halkın haber ve fikirlere ulaşma özgürlüğünün özüne dokunmayacak ve aynı zamanda hak sahibinin çıkarlarını koruyacak şekilde kullanılmalıdır.

71. Somut olayda, başvuru konusunun şikâyetine konu olan haberler 1998 ve 1999 yıllarında yayımlanmış ve arşiv niteliğindedir. Gazete arşivi niteliğinde olan haberler açısından arşivin sadece dijital alanda tutulmadığı ve içerik sağlayıcı tarafından saklanabileceği açıktır. Özellikle ölçülülük ilkesi temelinde yapılacak bir değerlendirme ile İnternet ortamında haberi ulaşılabilir kılan kişisel verilerin silinerek erişimin engellenmesi gibi yöntemler gözetildiğinde (bkz. § 52) İnternet ortamındaki arşiv niteliğindeki haberin tamamen silinmeden sonuca ulaşılabilmesi mümkündür. Bu bağlamda bilimsel araştırmalar açısından dijital haber arşivinin tamamen silinerek geçmişteki olayların yeniden yazılması sonucunu doğuracak basın özgürlüğüne yönelik ciddi müdahalelerin ortaya çıkması önlenebilir.

72. Başvuru hakkında İnternet ortamındaki arşivde muhafaza edilen ve kolaylıkla ulaşılabilir kılınan haberler 1998 ve 1999 yılındaki ceza yargılamasına ilişkindir. Bu haberlerin gerçeğe aykırı olduğu ileri sürülmemiştir. Haberler başvuru konusunun uyuşturucu kullanırken yakalanması ve daha sonrasında yargılanması hakkındadır. Bu bağlamda haberin konusunun, haberin arşivde kolaylıkla

ulařılabilir kılınması için gerekli toplumsal açıdan haber değeri devam ettiđi veya haberin geleceđe ışık tutacak nitelikte bir haber olduđu söylenemez.

73. Başvuru tarihi itibarıyla söz konusu haberin yaklaşık on dört yıl önceki bir olaya ilişkin olduđu ve böylelikle güncelliđini yitirdiđi açıktır. Haberın içeriđi açısından uyuşturuıcı kullanımı ile ilgili bir haberin tarihi, istatistiksel veya bilimsel amaçlarla İnternet ortamında kolaylıkla ulařılabilirliđinin sađlanması zorunlu olduđu da söylenemez. Bu bağlamda kamu yararı bakımından siyasi veya medyatik bir kişiliđe sahip olmayan başvuruıcı hakkında İnternet ortamında yayınlanan haberlerin kolaylıkla ulařılabilirliđinin başvuruıcunun itibarını zedelediđi açıktır.

74. Sonuç olarak başvuruıcı hakkında yapılan haberler unutulma hakkı kapsamında değerlendirilmesi gereken haberlerdir. İnternet ortamının sađladıđı kolaylıklar gözetildiğinde başvuruıcunun şeref ve itibarının korunması için anılan habere erişimin engellenmesi gerekmektedir. Bu bağlamda erişiminin engellenmesine yönelik talebin reddedilmesiyle ifade ve basın özgürlükleri ile kişinin manevi bütünlüđünün korunması hakkı arasında adil bir denge kurulduđu söylenemez.

75. Açıklanan gerekçelerle başvuruıcunun şeref ve itibarını koruma hakkının ihlal edildiđi sonucuna varılmıştır.

3. 6216 Sayılı Kanun'un 50. Maddesi Yönünden

76. 6216 sayılı Kanun'un 50. maddesinin (1) ve (2) numaralı fıkraları şöyledir:

"1) Esas inceleme sonunda, başvuruıcunun hakkının ihlal edildiđine ya da edilmediđine karar verilir. İhlal kararı verilmesi hâlinde ihlalin ve sonuçlarının ortadan kaldırılması için yapılması gerekenlere hükmedilir...

2) Tespit edilen ihlal bir mahkeme kararından kaynaklanmışsa, ihlali ve sonuçlarını ortadan kaldırmak için yeniden yargılama yapmak üzere dosya ilgili mahkemeye gönderilir. Yeniden yargılama yapılmasında hukuki yarar bulunmayan hâllerde başvuruıcı lehine tazminata hükmedilebilir veya genel mahkemelerde dava açılması yolu gösterilebilir. Yeniden yargılama yapmakla yükümlü mahkeme, Anayasa Mahkemesinin ihlal kararında açıkladıđı ihlali ve sonuçlarını ortadan kaldıracak şekilde mümkünse dosya üzerinden karar verir."

77. Başvuruıcı, tazminat talebinde bulunmamış, ihlalin ortadan kaldırılmasını talep etmiştir.

78. Başvuruıcunun şeref ve itibarın korunması hakkının ihlal edildiđi sonucuna varılmıştır.

79. İhlalin ortadan kaldırılması için kararın bir örneğinin (kapatılan) İstanbul 36. Sulh Ceza Mahkemesi yerine görevlendirilen sulh ceza hâkimliğine gönderilmek üzere İstanbul Cumhuriyet Başsavcılığına gönderilmesine karar verilmesi gerekir.

80. Dosyadaki belgelerden tespit edilen 198,35 TL başvuru harcının ve 1.800 TL vekâlet ücretinin başvurucaya ödenmesine karar verilmesi gerekir.

V. HÜKÜM

Açıklanan gerekçelerle;

A. Kamuya açık belgelerde başvurucaunun kimliğinin gizli tutulması talebinin KABULÜNE,

B. Şeref ve itibarın korunması hakkının ihlal edildiğine ilişkin iddianın KABUL EDİLEBİLİR OLDUĞUNA,

C. Anayasa'nın 17. maddesinin birinci fıkrasında güvence altına alınan şeref ve itibarın korunması hakkının İHLAL EDİLDİĞİNE,

D. Kararın bir örneğinin şeref ve itibarın korunması hakkının ihlalinin sonuçlarının ortadan kaldırılması için yeniden yargılama yapılmak üzere (kapatılan) İstanbul36. Sulh Ceza Mahkemesi yerine görevlendirilen sulh ceza hâkimliğine gönderilmek üzere İstanbul Cumhuriyet Başsavcılığına GÖNDERİLMESİNE,

E. 198,35 TL harç ve 1.800 TL vekâlet ücretinden oluşan toplam 1998,35 TL yargılama giderinin BAŞVURUCUYA ÖDENMESİNE,

F. Ödemenin, kararın tebliğini takiben başvurucaunun Maliye Bakanlığına başvuru tarihinden itibaren dört ay içinde yapılmasına, ödemede gecikme olması hâlinde bu sürenin sona erdiği tarihten ödeme tarihine kadar geçen süre için yasal FAİZ UYGULANMASINA,

G. Kararın bir örneğinin Adalet Bakanlığına GÖNDERİLMESİNE

3/3/2016 tarihinde OYBİRLİĞİYLE karar verildi.

Anayasa Mahkemesi - Ömür Kara ve Onursal Özbek Kararı (2013/4825)

Ömür Kara ve Onursal Özbek, B. No: 2013/4825, 24/3/2016

Başvuru, özel bir şirket bünyesinde çalışan başvurucuların mahremiyete ilişkin yazışmalar içeren kurumsal e-posta hesaplarının işveren tarafından incelenmesi ve bu yazışmaların işe iade davasında delil olarak kullanılması nedenleriyle özel hayata saygı ve haberleşmenin gizliliği haklarının ihlal edildiği iddialarına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

İKİNCİ BÖLÜM

KARAR

ÖMÜR KARA VE ONURSAL ÖZBEK BAŞVURUSU

(Başvuru Numarası: 2013/4825)

Karar Tarihi: 24/3/2016

RG Tarih ve Sayı:10/5/2016 - 29708

İKİNCİ BÖLÜM

KARAR

Başkan: Engin YILDIRIM

Üyeler: Serdar ÖZGÜLDÜR, Osman Alifeyyaz PAKSÜT, Recep KÖMÜRCÜ, Alparslan ALTAN

Raportör Yrd: Fatih ALKAN

Başvurucular: 1. Ömür KARA; 2. Onursal ÖZBEK

Vekili: Av. Zeliha Tuyan ÇAĞLAR

I. BAŞVURUNUN KONUSU

1. Başvuru, özel bir şirket bünyesinde çalışan başvurucuların mahremiyete ilişkin yazışmalar içeren kurumsal e-posta hesaplarının işveren tarafından incelenmesi ve bu yazışmaların işe iade davasında delil olarak kullanılması nedenleriyle özel hayata saygı ve haberleşmenin gizliliği haklarının ihlal edildiği iddialarına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 27/6/2013 tarihinde Bakırköy 8. İş Mahkemesi vasıtasıyla yapılmıştır. Başvuru formu ve eklerinin idari yönden yapılan ön incelemesi neticesinde başvurunun Komisyona sunulmasına engel teşkil edecek bir eksikliğin bulunmadığı tespit edilmiştir.
3. İkinci Bölüm Üçüncü Komisyonunca başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.
4. Bölüm tarafından 18/2/2014 tarihinde, başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.
5. Konu bakımından irtibat nedeniyle 2013/5442 numaralı başvurunun 2013/4825 numaralı başvuru üzerinde birleştirilmesine ve incelemenin bu dosya üzerinden yapılmasına karar verilmiştir.
6. Başvuru belgelerinin bir örneği 2013/5442 numaralı başvuru dosyası üzerinden bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık, görüşünü 21/4/2014 tarihinde Anayasa Mahkemesine sunmuştur.
7. Bakanlık tarafından Anayasa Mahkemesine sunulan görüş 29/4/2014 tarihinde başvuruculara tebliğ edilmiştir. Başvurucular, Bakanlığın görüşüne karşı beyanlarını 14/5/2014 tarihinde ibraz etmiştir.

III. OLAY VE OLGULAR

A. Olaylar

8. Başvuru formu ve eklerinde ifade edildiği şekliyle ilgili olaylar özetle şöyledir:
9. Birinci başvurucu 1/3/2010 tarihinde imzaladığı iş sözleşmesi ile, ikinci başvurucu 11/4/2011 tarihinde imzaladığı iş sözleşmesi ile işveren T. Ticaret A.Ş. (Şirket) bünyesinde işçi statüsünde çalışmaya başlamıştır.
10. Anılan iş sözleşmelerinin “Özel Şartlar” başlıklı bölümünde “13.8. Personel, işyerinde yürürlükte olan tüm Yönetmelik, İç Tüzük, Prosedür ve talimatlara uymakla yükümlüdür.”, “13.23. İşyerinde uyulması gereken kurallara ilişkin iç tüzük, yönetmelik, oryantasyon kitapçığı, hükümler ve seyahat yönetmeliği, talimatlar, prosedürler, iş bu iş akdinin ayrılmaz eki ve parçasıdır.” şeklinde ifadelerle yer verilerek yönetmelik ile diğer düzenlemeler iş sözleşmelerinin bir parçası olarak belirlenmiş ve bu düzenlemelere uygun davranmak konusunda başvurucular ve işveren karşılıklı taahhüt altına girmişlerdir.
11. Bu kapsamda Şirket Temel Yönetmeliği'nin “İşyerleri içerisinde, temel ahlaki kurallara uyulması ve yanlış anlaşılacak davranış ve ilişkilerden kaçınılması” başlıklı 20. maddesinde yer alan “Eşit veya

ast/üst pozisyonlarda çalışan personel, hem eşitleri hem de üst veya astları ile karşılıklı saygıya dayanan mesafeli ve profesyonel bir ilişki kurmalı, özel yaşamlarını, birbirlerine açacak kadar samimi olmaktan kaçınılmalı, özel dostluklarını tercihen şirket dışındaki arkadaşları ile oluşturmalı” şeklindeki düzenleme, anılan iş sözleşmelerinin bir parçası kabul edilerek her iki başvurucu tarafından imzalanmıştır. Yine iş sözleşmelerinin devamı olarak kabul edilen Bilgi Güvenliği Taahhütnamesi’nin 2. maddesinde yer alan “Şirket tarafından çalışanlara iş için tahsis edilmiş olan bilgisayar, e-posta, internet kullanımı, telefon, USB memory, CD-writer, iletişim programı ve diğer IT kaynaklarını ve iletişim araçlarını zaruri ihtiyaçları aşan ölçüde kişisel amaçlı, kabul edilemez maksatlı, eğlence niyetli, genel ahlaka, örf ve adetlere aykırı şekilde kullanılmayacağı” şeklindeki taahhüt ile 6. maddesinde yer alan “Yetkili şirket yöneticileri tarafından çalışanlara herhangi bir haber verilmeksizin ve uyarıda bulunulmaksızın; kullandıkları IT ve iletişim kaynaklarının her zaman takip altında tutulabileceği, yaptıkları yazışmaların ve iletişim kayıtlarının yedeklenebileceği, raporlanabileceği, gerekli durumlarda detay bazlı incelenebileceği, el konulabileceğini ve kullanım sınırlaması getirilebileceği” şeklindeki taahhütleri içeren düzenlemeler de başvurucular tarafından imzalanmıştır.

12. 14/5/2012 tarihinde işveren Şirketin yöneticilerinin başvurucularla yaptıkları görüşmede, ikinci başvurucunun eşinin Şirket üst yöneticisini ziyaret ederek başvurucular arasında duygusal bir ilişki bulunduğunu belirttiği ve buna kanıt olarak başvuruculara ait e-posta yazışmalarının bir suretini Şirket yönetimine verdiği dile getirilmiştir. Ayrıca bu nedenle işverenin artık başvurucularla çalışmak istemediği, istifa edebilecekleri ya da karşılıklı anlaşma yoluna gidilebileceği, aksi takdirde iş sözleşmelerinin işveren tarafından feshedileceği ifade edilmiştir. Başvurucular, duygusal ilişki yaşadıkları iddiasını reddetmişler ve iş sözleşmelerinin feshini gerektirecek bir neden bulunmadığını belirtmişlerdir. Anılan görüşme sonrasında iş yerinde kullanım amaçlı olarak başvuruculara tahsis edilen bilgisayarlar işveren tarafından kapatılmıştır. Ayrıca aynı gün talepleri üzerine başvuruculara yıllık izin verilmiştir.

13. Başvurucuların iş sözleşmeleri 22/5/2003 tarihli ve 4857 sayılı İş Kanunu’nun 25. maddesinde yer alan “Ahlak ve iyiniyet kurallarına uymayan haller ve benzerleri” başlıklı (II) numaralı bendi gereğince 21/5/2012 tarihinde işveren tarafından feshedilmiştir.

14. Başvurucular; ikinci başvurucu ile eşi arasında boşanma davasının devam ettiğini, haklarında dile getirilen beyanların bir iftiradan ibaret olduğunu, özel hayatlarının gizliliği ve haberleşme hürriyetleri yok sayılarak kişisel e-posta hesaplarının incelendiğini, ve bu hesaplardan elde edilen yazışmaların içerikleri üzerinden ulaşılan “evlilik dışı ilişki yaşadıkları” şeklindeki varsayım gerekçe

gösterilerek iş sözleşmelerinin haksız yere feshedildiğini ileri sürerek 20/6/2012 tarihinde işveren şirket aleyhine işe iade istemli tespit davası açmışlardır.

15. Söz konusu davalar Bakırköy 12. İş Mahkemesinin 2012/279 ve 2012/280 Esas sıralarına kaydedilmiştir.

16. Davalı işveren tarafından sunulan cevap dilekçesinde, başvuruçuların iş sözleşmelerinin yalnızca ikinci başvuruçunun eşinin tek taraflı beyanları üzerine feshedilmediği, başvuruçuların özel hayat alanlarının dışında kalan ve Şirketin işleyişini ilgilendiren iddiaların araştırılması için başvuruçuların kullanımına tahsis edilen ancak mülkiyeti Şirkete ait olan bilgisayarların sınırlı şekilde incelendiği, iddiaları destekleyen ve iş sözleşmelerinin devamını çekilmez kılan hususların bulunduğu, iddiaları doğrulayacak şekilde başvuruçuların karşılıklı olarak e-posta hesapları üzerinden yazışmalarının tespit edildiği, bu yazışmaların müstehcenlik unsurları taşıdığı, tüm bu hususların iş sözleşmesi ile iş sözleşmesinin parçası olan Şirket içindeki diğer düzenlemelere aykırılıklar oluşturduğu belirtilmiş ve söz konu yazışmaların içerikleri Mahkemeye delil olarak sunulmuştur.

17. 2012/279 Esas sıra sayılı davada, davalı Şirket çalışanları tarafından Mahkeme huzurunda tanık sıfatıyla verilen ifadelerin ilgili kısımları şöyledir:

“... ben 2005 yılından bu yana davalı işyerinde çalışmaktayım, ben Uluslararası mağazacılık insan kaynakları direktörü olarak davalı işyerinde çalışmaktayım, davacı firmanın avukatıydı. fesih öncesinde 3-4 ay öncesinde davacı ve Ömür Hanım aralarında yakınlık olduğu konusunda birkaç duyum aldım, aralarındaki ilişkinin profesyonelliğin ötesinde yorumlandığını gördüm, bu konuda davacı ve Ömür Hanımı bilgilendirdim, onlarda böyle bir ilişkinin olmadığını söylediler, davacı Ömür Kara'nın çalıştığı bölüm kapanmadı, grup içerisinde organizasyonda değişiklik oldu, bu değişikli Onursal Özbek'i ilgilendirdi, V. bey ile Onursal Özbek in eşi İ.Özbek bu konuda görüşmüş bunu bana yönetim kurulu başkanı V. Bey söyledi, bilgi işlem vasıtasıyla davacının e-mailini özel amaçlı kullanıp kullanmadığı konusunda araştırma yaptık, gerçekten de belirtilen e-mailler bilgisayar kayıtlarında mevcuttur, ... davacı ile Ömür hanım arasında iş ilişkisinden farklı bir ilişki olduğuna dair diğer birimlerde çalışan kişilerden işyerinde bu kadar uzun mola nasıl yapılabiliyor. Hep aynı 2 kişinin işyerinde dikkat çekici şekilde her molada sürekli birlikte olmalarının dikkat çektiği hususunda bana bilgi verildi. Ben kendileri ile görüştüğümde reddettiler. Buna ilişkin olarak genel müdürümüzün de bana uyarısı olmuştur. Bu durumun dışında davacının işyerindeki performansı veya çalışmasına ilişkin herhangi bir olumsuzluk bana iletilmedi. İşyerinde davacının evli olması sebebiyle bize bu konuyu bilmeniz gerekir şeklinde uyarılar gelmişti. Davacı vekilinin talebi üzerine

soruldu: davacı ile Ömür hanım arasındaki diyalogun liseli aşıklar şeklinde benzetme ile bana iletilmişti dedi.”

“... ben 2003 yılından bu yana davalı işyerinde çalışmaktayım,ben Uluslararası genişleme direktörü olarak davalı işyerinde çalışmaktayım,davacı firmanın avukatıydı. davacı ve Ömür Hanım mesai saatlerinin arasında mola zamanlarında normal mesai arkadaşlarından daha fazla vakit geçirmekte idiler,davacının işi aksatacak şekilde mesai saatleri içerisinde davranışlarına tanık olmadım.”

“Ben ekim 2011 ayı ile ocak 2013 ayı arasında davalı işyerinde personel ve özlük işleri müdürü olarak çalıştım, benim işyerine karşı açılmış herhangi bir davam yoktur. Davacı firmanın avukatıydı. Bildiğim kadarıyla şu an davacının çalıştığı bölüm faaliyet göstermemektedir,ben sadece fesih sürecinde yer aldım bunun dışında tam bilgim yoktur,fesih öncesinde feshe, daha sonra ek olarak sunulan e-mail yazışmaları ve diğer belgeler nedeniyle davacı ve Ömür Hanımın iş akdi feshedildi.”

“Onursal Özbek benim eski eşim olur, işyerinden ortak arkadaşlarımla davacı ile eşim arasında yakınlık olduğunu duydum, ayrıca birbirlerine göndermiş oldukları e-mailleri gördüm, bunun üzerine yönetim kurulu başkanı V. Bey ile görüştüm,diğer yönetici ve avukatlarıyla görüşüp durumu değerlendireceğini söyledi, benim gerekçelerimle hareket etmeyeceğini söyledi, gerekli araştırma yapıldıktan sonra işlem yapılacağını söyledi,daha sonra dan iş akitlerinin feshedildiğini öğrendim, evliliğin bitmesinebuneden olmuştur iki tarafla da görüşmeme rağmen sonuç alamadım dedi.”

“Ağustos 2011 ve temmuz 2012 tarihleri arasında davalı işyerinde Uluslar arası finansal kiralama ve sözleşme uzmanı olarak çalıştım. davacı firmanın avukatıydı. Davacı ile Ömür Hanım arasında yakınlık konusunda herhangi bir bilgim yoktur,davacının çalıştığı bölüm kapatılmadı, Onursal Özbek bana Ömür Kara ile beraberliği nedeniyle iş akdinin feshedildiğini, eşinin e-maillerini kırıp e-mailleri V. beye gösterdiğini söyledi, bir daha işyerinde çalışmak istemediğini söyledi, her zaman dikkat çekecek şekilde Ömür Kara ile beraberliği yoktu, herkese karşı sıcak davranmaktadır, ben hiçbirfarklılık görmedim, davacı hakkında daha önce fesih konusunda araştırma yapıp yapılmadığını bilmiyorum..”

18. 2012/280 Esas Sıra sayılı davada verilen tanık ifadeleri de aynı doğrultudadır.

19. Birinci başvuru açısından Bakırköy 12. İş Mahkemesinin 8/2/2013 tarihli ve E.2012/280, K.2013/76 sayılı kararı ile; ikinci başvuru açısından Bakırköy 12. İş Mahkemesinin 7/3/2013 tarihli ve E.2012/279, K.2013/129 sayılı kararı ile davaların reddine karar verilmiştir.

20. 8/2/2013 tarihli kararın gerekçesi şöyledir:

“... Davacının hizmet cetveli, işyeri özlük dosyası dosyaya celb edilmiştir.

Dava ile ilgili olarak davacı ve davalı tanıklarının beyanları alınmıştır.

Dosyanın incelenmesinden; davacının iş akdinin 4857 sayılı Kanununun 25/2. maddesi gereğince feshedildiği, davacı ile Onursal Özbek arasındaki e-maillerin dosyaya ibraz edildiği, şirketin kendisine tahsis edilen e-mail adresinden mesai saatleri içerisinde özel amaçlı olarak e-mail gönderilmesi ve kabul edilmesinin doğruluk ve bağlılıkla bağdaşmayan eylem niteliğinde olduğu, davacı ve Onursal Özbek arasındaki yakınlaşma nedeniyle, aynı zamanda Onursal Özbek in eşinin işyerine gelip şikayetçi olması nedeniyle de şirket açısından iş akdinin devamının imkansız hale geldiği nazara alınarak davanın reddine karar vermek gerekmiştir”.

21. 7/3/2013 tarihli kararın gerekçesi ise şöyledir:

“... Mahkememizce davacının hizmet cetveli, işyeri özlük dosyası getirtilip incelenmiş, davacı ve davalı tanıkları dinlenmiştir. Davalı tarafından sunulan, şirketçe tahsis edilmiş e-mail adresinden yapılan yazışmaların içeriği davacı tarafından kabul edilmiştir.

Tüm dosya kapsamı, e-mail yazışmaları, tanıkların beyanları birlikte değerlendirildiğinde; evli olan davacının işyerinde bir bayan işçi ile gönül ilişkisine girmesi sonrası, davacı eşinin işyerine geldiği ve durumu yöneticilere iletmediği, bu nedenle işyerinde olumsuzluklar yaşandığı ve bu olumsuzlukların davacının davranışından kaynaklandığı, işverenin zor durumda kaldığı ve işveren açısından iş ilişkisinin sürdürülmesi olanağı kalmadığı anlaşıldığından davanın reddine karar vermek gerekli ve uygun görülmüştür.”

22. Kişisel hesaplar üzerinden gerçekleştirilen yazışmalardan oluşan e-postaların fesih gerekçesi olarak gösterilmesiyle özel hayatın gizliliğinin ihlal edildiği, buna rağmen söz konusu delil içeriklerinin Mahkemece değerlendirildiği ve yalnızca bu hukuka aykırı deliller esas alınarak hüküm kurulduğu, performans ve verimliliğe ilişkin tanık ifadelerinin dikkate alınmadığı, özel hayat alanına yönelen haksız müdahalenin Mahkemece benimsendiği, işe iade davalarının kabulü gerekirken şartları oluşmadığı hâlde reddedildiği ileri sürülmüş ve söz konusu kararlar bozma talebiyle başvuru sahiplerinin vekilince temyiz edilmiştir.

23. Temyiz nedenlerine karşı cevap dilekçesi sunan davalı işveren vekilince, yazışmaların Şirket tarafından çalışanlar adına açılmış e-posta hesapları üzerinden gerçekleştirildiği, bu hesapların yalnızca iş amaçlı kullanılması yönünde başvuru sahiplerine gerekli uyarıların yapıldığı, buna rağmen yazışmaların içeriğinde adap ve ahlaka aykırı unsurlar içeren yazılar ve resimler bulunduğu, lehe tanık ifadeleri ve tüm bu saptamalar dikkate alındığında birinci başvuru ile fesih sürecinde evli olan ikinci başvuru arasında duygusal bir ilişkinin bulunduğu, bu nedenlerle davacıların iş

sözleşmelerinin devamının çekilmez hâle geldiği ileri sürülmüş ve söz konusu kararların onanması talep edilmiştir.

24. Temyiz incelemesi neticesinde delillerin takdirinde isabetsizlik bulunmadığı gerekçesiyle birinci başvuru açısından Yargıtay 22. Hukuk Dairesinin 30/4/2013 tarihli ve E.2013/6232, K.2013/9082 sayılı ilamı ile; ikinci başvuru açısından yine Dairenin 16/5/2013 tarihli ve E.2013/9419, K.2013/11237 sayılı ilamı ile kararlar onanarak kesinleşmiştir.

25. 30/4/2013 tarihli nihai karar 29/5/2013 tarihinde başvuruların vekiline tebliğ edilmiş ve 27/6/2013 tarihinde bireysel başvuru yapılmıştır.

B. İlgili Hukuk

26. 4857 sayılı Kanun'un "İşverenin haklı nedenle derhal fesih hakkı" kenar başlıklı 25. maddesinin ilgili kısımları şöyledir:

"Süresi belirli olsun veya olmasın işveren, aşağıda yazılı hallerde iş sözleşmesini sürenin bitiminden önce veya bildirim süresini beklemeksizin feshedebilir:

...

II- Ahlak ve iyi niyet kurallarına uymayan haller ve benzerleri:

...

b) İşçinin, işveren yahut bunların aile üyelerinden birinin şeref ve namusuna dokunacak sözler sarfetmesi veya davranışlarda bulunması, yahut işveren hakkında şeref ve haysiyet kırıcı asılsız ihbar ve isnadlarda bulunması.

c) İşçinin işverenin başka bir işçisine cinsel tacizde bulunması.

d) İşçinin işverene yahut onun ailesi üyelerinden birine yahut işverenin başka işçisine sataşması, işyerine sarhoş yahut uyuşturucu madde almış olarak gelmesi ya da işyerinde bu maddeleri kullanması.

e) İşçinin, işverenin güvenini kötüye kullanmak, hırsızlık yapmak, işverenin meslek sırlarını ortaya atmak gibi doğruluk ve bağlılığa uymayan davranışlarda bulunması.

...

h) İşçinin yapmakla ödevli bulunduğu görevleri kendisine hatırlatıldığı halde yapmamakta ısrar etmesi.

...

III- Zorlayıcı sebepler:

İşçiyi işyerinde bir haftadan fazla süre ile çalışmaktan alıkoyan zorlayıcı bir sebebin ortaya çıkması.

..."

27. Başvurucular tarafından imzalanan iş sözleşmelerinin "Özel Şartlar" başlıklı bölümünde yer alan ilgili düzenleme şöyledir:

"13.8. Personel, işyerinde yürürlükte olan tüm Yönetmelik, İç Tüzük, Prosedür ve talimatlara uymakla yükümlüdür.

...

13. 23. İşyerinde uyulması gereken kurallara ilişkin iç tüzük, yönetmelik, oryantasyon kitapçığı, hükümler ve seyahat yönetmeliği, talimatlar, prosedürler, iş bu iş akdinin ayrılmaz eki ve parçasıdır."

28. Şirket Temel Yönetmeliği'nin "İşyerleri içerisinde, temel ahlaki kurallara uyulması ve yanlış anlaşılacak davranış ve ilişkilerden kaçınılması" başlıklı 20. maddesi şöyledir:

"Eşit veya ast/üst pozisyonlarda çalışan personel, hem eşitleri hem de üst veya astları ile karşılıklı saygıya dayanan mesafeli ve profesyonel bir ilişki kurmalı, özel yaşamlarını, birbirlerine açacak kadar samimi olmaktan kaçınılmalı, özel dostluklarını tercihen şirket dışındaki arkadaşları ile oluşturmalı. (Eşitler veya ast/üst arasındaki aşırı samimiyet, duygusallığı öne çıkarıp, profesyonellikten uzaklaştıracağı için günlük iş ilişkilerinde, performans değerlendirmede ve ileride oluşabilecek terfi sonrası otorite kurmada, zaafılara neden olabilecektir.)"

29. Başvurucular tarafından imzalanan Bilgi Güvenliği Taahhütnamesi'nin ilgili kısımları şöyledir:

"Çalışanı olduğum Şirketin faaliyetleri kapsamında;

...

2. Şirket tarafından şahsıma iş için tahsis edilmiş olan bilgisayar, e-posta, internet kullanımı, telefon, USB memory, CD-writer, iletişim programı ve diğer IT kaynaklarını ve iletişim araçlarını zaruri ihtiyaçları aşan ölçüde kişisel amaçlı, kabul edilemez maksatlı (örn: yasal olmayan kopyalama, iş yürütme, iş araştırma, izinsiz yazılım kurulumu, kullanımı v.b.), eğlence niyetli(örn: çevrimiçi topluluklara, sohbet odalarına, forumlara katılım, toplu e-mail gönderimi, müzik sitelerine giriş v.b.), genel ahlaka, örf ve adetlere aykırı şekilde (örn: cinsel içerikli materyallere erişim, taciz, kumar, bahis amaçlı) kullanmayacağımı,

...

6. Yetkili şirket yöneticileri tarafından şahsıma herhangi bir haber verilmeksizin ve uyarıda bulunulmaksızın; kullandığım IT ve iletişim kaynaklarının her zaman takip altında tutulabileceğini, yaptığım yazışmaların ve iletişim kayıtlarının yedeklenebileceğini, raporlanabileceğini, gerekli durumlarda detay bazlı incelenebileceğini, el konulabileceğini ve kullanım sınırlaması getirilebileceğini,

... kabul ve taahhüt ediyorum. ... iş bu taahhütname tarafımdan okunarak imzalanmıştır.”

IV. İNCELEME VE GEREKÇE

30. Mahkemenin 24/3/2016 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları

31. Başvurucular; kişisel e-posta hesapları üzerinden gerçekleştirdikleri yazışmaların içeriklerine işveren tarafından rızaları olmaksızın ulaşıldığını, bu içerikler dikkate alınarak devamının çekilmez hâle geldiği gerekçesiyle iş sözleşmelerinin feshedildiğini, açtıkları işe iade istemli tespit davasında söz konusu yazışmaların delil olarak kabul edildiğini, elde ediliş biçimleri dikkate alınmaksızın e-posta içeriklerini inceleyip değerlendiren Mahkemece feshin hukuka uygun olduğuna karar verildiğini, ikinci başvurucunun eski eşinin tanık sıfatıyla Mahkeme huzurunda dinlenmesi ile söz konusu davanın özel hayatlarının detayları üzerinden devam eden bir davaya büründüğünü, Mahkeme tarafından özel hayatlarına ilişkin yazışmaların bu şekilde alenileştirildiğini, üçüncü kişiler tarafından özel hayat alanlarına yapılan haksız müdahale karşısında Mahkemece bir korunma sağlanmadığını ve dava sürecinde dile getirdikleri düşüncelerin sorgulandığını belirterek Anayasa'nın 20., 22. ve 25. maddelerinde tanımlanan haklarının ihlal edildiğini iddia etmişlerdir.

B. Değerlendirme

32. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16).

33. Bakanlık görüş yazısında, delillerin takdirine ilişkin şikâyetlerin yargılamanın adil olup olmadığının değerlendirilmesinden ibaret olduğu, bu nedenle adil yargılanma hakkı bağlamında incelenmesi gerektiği, buna ilişkin görüşlerin benzer nitelikteki şikâyetlerin bulunduğu başvurularda sunulduğu belirtilmiştir. Ayrıca davalı işverenin davranışları yönünden yapılan değerlendirmede, davalı Şirket aleyhine tazminat davası açılabileceği ve ilgili kişiler hakkında suç duyurusunda bulunulabileceği dikkate alınarak başvuru yollarının tüketilip tüketilmediği açısından inceleme yapılması gerektiği, özel yazışmaların davalarda kullanılması yönünden yapılan değerlendirmede

ise özel hayatın kapsamı ile fesih işlemi arasındaki ilişkinin incelenmesi ve özel hayata saygı hakkının kamusal makamlara tedbirler alma yükümlülüğü yükleyip yüklemediği açısından inceleme yapılması gerektiği ifade edilmiş; Avrupa İnsan Hakları Mahkemesi (AİHM) önüne benzer ihlal iddialarıyla yansıyan dava ve karar örneklerine yer verilmiştir.

34. Başvurucular tarafından Bakanlık görüşüne karşı verilen beyanda, ihlal iddialarının yargılamanın adil olup olmadığı hususuna değil, özel hayata saygı hakkına ve haberleşmenin gizliliğine ilişkin olduğu belirtilmiş ve başvuru dilekçelerindeki görüş ve talepler tekrar edilmiştir.

35. Söz konusu iddiaların özünün, başvurucuların özel hayat alanlarına üçüncü kişilerin yaptığı müdahalelere karşı Mahkemeler tarafından bir koruma sağlanmaması ve kişisel yazışmaların Mahkemelerce delil olarak kabul edilip alenileştirilmesi hususunda olduğu anlaşıldığından incelemenin delillerin değerlendirilmesinin adil olup olmadığı yönünden değil, iddiaların özüne uygun olarak özel hayata saygı hakkı ile haberleşmenin gizliliği hakkı yönünden yapılması gerektiği değerlendirilmiştir.

1. Kabul Edilebilirlik Yönünden

36. Başvurucular tarafından açılan işe iade davalarının gerekçesi, iş sözleşmelerinin feshedilmesine dayanak olarak gösterilen kurumsal e-posta hesaplarının incelenmesiyle elde edilen yazışmalar nedeniyle özel hayata saygı hakkı ile haberleşme hürriyetlerinin ihlal edilmesi, bunun da fesih işlemlerini hükümsüz kılmasıdır. Dolayısıyla haberleşmelerin denetlenmesi şeklindeki işverenin müdahalesine ilişkin şikâyetlerin Derece Mahkemeleri önünde dile getirildiği sonucuna ulaşılmaktadır.

37. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan özel hayata saygı hakkı ile haberleşmenin gizliliği hakkının ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna karar verilmesi gerekir.

2. Esas Yönünden

38. Başvurucular esas olarak üçüncü kişilerin müdahalesi karşısında özel hayat alanlarının Mahkemelerce korunmadığını ve kişisel yazışmalarının Mahkemelerce delil olarak kabul edilip alenileştirildiğini, bu nedenle Anayasa'nın 20. ve 22. maddelerinde tanımlanan haklarının ihlal edildiğini ileri sürmüşlerdir.

39. Anayasa'nın 148. maddesinin üçüncü fıkrası ile 6216 sayılı Kanun'un 45. maddesinin (1) numaralı fıkrası hükümlerine göre Anayasa Mahkemesine yapılan bir bireysel başvurunun esasının incelenebilmesi için kamu gücü tarafından müdahale edildiği iddia edilen hakkın, Anayasa'da

güvence altına alınmış olmasının yanı sıra Sözleşme ve Türkiye'nin taraf olduğu ek protokollerinin kapsamına girmesi gerekir. Bir başka ifadeyle Anayasa ve Sözleşme'nin ortak koruma alanı dışında kalan bir hak ihlali iddiasını içeren başvurunun kabul edilebilir olduğuna karar verilmesi mümkün değildir (Onurhan Solmaz, B. No: 2012/1049, 26/3/2013, § 18).

40. Anayasa'nın "Özel hayatın gizliliği" kenar başlıklı 20. maddesinin birinci fıkrası şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz."

41. Anayasa'nın "Haberleşme hürriyeti" kenar başlıklı 22. maddesi şöyledir:

"Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.

İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir."

42. Sözleşme'nin "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesi şöyledir:

"(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlâkın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."

43. Özel hayata saygı hakkı Anayasa'nın 20. maddesinde koruma altına alınmıştır. Devlet, kişilerin özel ve aile hayatına keyfî olarak müdahale etmemek ve üçüncü kişilerin haksız saldırılarını önlemekle yükümlüdür. Özel hayat geniş bir kavram olup bu kavramın kapsayıcı bir tanımının yapılması oldukça zordur. Bununla beraber bu kavram; kişinin maddi ve manevi bütünlüğü, fiziksel ve sosyal kimliği, bireyin ismi, cinsel yönelimi, cinsel yaşamı gibi unsurları korumaktadır. Kişisel bilgiler ve veriler, kişisel gelişim, aile hayatı vb. konular da bu hakkın içinde yer almaktadır (Bülent Polat [GK], B. No: 2013/7666, 10/12/2015, § 61). Ayrıca Anayasa'nın 20. ve 22. maddelerinde yer alan

güvencelerin amacı gözetildiğinde somut olayda olduğu gibi iş yerlerinden gerçekleştirilen kişisel telefon görüşmelerinin ve internet kullanımının izlenmesiyle elde edilmiş veriler de benzer şekilde bu hak kapsamında incelenmektedir (Benzer yöndeki AİHM kararı için bkz. Barbulescu/Romanya, B. No: 61496/08, 12/1/2016, § 36).

44. Özel hayat kavramı, özel bir sosyal hayat sürdürmeyi yani kişinin sosyal kimliğini geliştirme hakkı anlamında bir “özel hayatı” güvence altına almaktadır. Bu yönü ile birlikte değerlendirildiğinde bahsi geçen hak, ilişki kurmak ve geliştirmek üzere çevresinde bulunanlarla temas kurma hakkını da içermektedir. AİHM içtihatlarında da mesleki hayat çerçevesinde yürütülen faaliyetlerin “özel hayat” kavramı dışında tutulamayacağı belirtilmektedir. Mesleki hayata getirilen sınırlamalar, bireyin sosyal kimliğini yakınlarında bulunan insanlarla olan ilişkilerini geliştirme şeklinde yansıttığı ölçüde Sözleşme’nin 8. maddesi kapsamına girebilmektedir. Bu noktada belirtmek gerekir ki insanların büyük çoğunluğu, dış dünya ile olan ilişkilerini geliştirme olanaklarını daha çok mesleki hayatları çerçevesinde yürüttükleri faaliyet kapsamında elde etmektedir (Bülent Polat, § 62; Özpınar/Türkiye, B. No: 20999/04, 19/10/2010, § 45; Niemietz/Almanya, B. No: 13710/88, 16/12/1992, § 29).

a. Genel İlkeler

45. Anayasa ve Sözleşme’nin ortak koruma alanı kapsamında kalan temel haklar, yalnızca kamusal gücün doğrudan uygulanmasıyla değil; kimi zamanda özel hukuk kişileri arasındaki uyuşmazlıklara konu olacak şekilde üçüncü kişilerin müdahaleleriyle zedelenebilmektedir. İlkinde söz konusu güvencelerin sağlanması adına kamusal makamlara yüklenen negatif ve pozitif tüm yükümlülüklerin doğrudan yerine getirilmesi konusunda tereddüt bulunmamakta ise de ikinci durumda devletin üçüncü kişilerin müdahalelerine karşı bireylere ne tür bir koruma imkânı sunması gerektiği ve hangi çerçevede yükümlülükler taşıdığı hususunda her olayın kendine özgü koşullarına göre değerlendirmelerde bulunulması gerekmektedir.

46. Anayasa’nın 11. maddesine göre Anayasa hükümleri; yasama, yürütme ve yargı organları ile idare makamlarının yanı sıra diğer kuruluş ve kişileri de bağlayan temel hukuk kurallarıdır. Buna göre Anayasa’da tanınan hak ve özgürlükler tüm bireyler bakımından güvence altındadır. Yine Anayasa’nın 5. maddesinde sayılan devletin temel amaç ve görevlerinin kapsamı ile temel hak ve hürriyetlerin niteliklerine yönelik Anayasa’nın 12. maddesinde yer alan vurgu da bu koruma alanını pekiştirmektedir. Söz konusu hak ve özgürlüklerin etkili şekilde korunması amacıyla özel hukuk kişileri arasındaki uyuşmazlıklardan dahi kaynaklansa kamusal makamlar belirli durumlarda pozitif yükümlülükler altına girebilir. Uyuşmazlıkların özel hukuk kişileri arasında gerçekleştiği

durumlarda temel hak ve özgürlüklerin sağladığı güvencelerin yerine getirilip getirilmediği denetlenirken Anayasa'nın kamusal makamlara yüklediği sorumluluklardan doğrudan özel hukuk kişileri sorumlu tutulamayacağından taşıdığı koşulların özelliklerine göre bu tür başvuruların devletin pozitif yükümlülükleri bağlamında ele alınması gerekebilir (Barbulescu/Romanya, § 53).

47. Bu yükümlülükler özel hukuk kişilerinin birbirleri ile olan uyuşmazlıklarının çözümüne ilişkin yasal alt yapının oluşturulmasını, söz konusu uyuşmazlıkların adil yargılama gereklerine uygun ve usul yönünden güvenceleri haiz bir yargılama kapsamında incelenmesini ve bu yargılamalarda temel haklara ilişkin anayasal güvencelerin gözetilip gözetilmediğinin denetlenmesini gerektirir. Bu gereklilikler üçüncü kişilerin, bireylerin hak ve özgürlüklerine yaptığı haksız müdahalelere karşı kamusal makamlar tarafından müsamaha gösterilmemesi zorunluluğundan kaynaklanır. Zira derece mahkemeleri, özel hukuk ilişkisi kapsamındaki uyuşmazlıkların çözümlenmesinde bağlayıcı kararlar vererek güvencelerin korunup korunmamasında rol almaktadır. Bu noktada uyuşmazlıkların yargısal makamlar önüne taşınması ve hakkaniyete uygun bir yargılama yapılarak çözümlenmesi, kamusal makamların pozitif yükümlülüklerinin bir parçasını oluşturur.

48. AİHM de devletin doğrudan müdahalesinden kaynaklanmasa da bu tür uyuşmazlıklarla ilgili olarak devletlerin sorumluluğunun devam edebileceğini, kamusal makamlardan gelebilecek keyfi uygulamalardan başka Sözleşme'deki haklara etkili şekilde koruma sağlanabilmesi için özel hukuk kişileri arasındaki ilişkilerde de makul ve uygun önlemler almak suretiyle devletlerin müdahale etme yükümlülüğü taşıyabileceğini ifade etmektedir (Sorensen ve Rasmussen/Danimarka [BD], B. No: 52562/99, 52620/99, 11/1/2006, § 57; Palomo Sanchez ve diğerleri/İspanya [BD], B. No: 28955/06, ..., 12/9/2011, § 59).

49. Başvuru konusu olayda olduğu gibi kamu gücünü kullanan aktörler dışında kalan kişiler arasındaki özel hukuk ilişkilerinde kamusal makamların yükümlülükleri; bireylerin temel hak ve özgürlüklerine, bu başvuru açısından özel hayata saygı hakkı ile haberleşmenin gizliliği hakkına üçüncü kişilerin müdahalesinin önlenmesi için gerekli önlemlerin alınması ve mahkemelerce korunma sağlanmasıdır. Kamusal makamlarca gerekli yapısal önlemler alınmış olursa da uyuşmazlık konusu davayı yürüten mahkemelerce verilen kararlarda üçüncü kişilerin müdahalelerine karşı bireylere korunma imkânı sağlanmadığı durumlarda bu yükümlülükler gereği gibi yerine getirilmemiş olacaktır. Bu, kamusal makam olan mahkemeler aracılığıyla bireylerin hak ve özgürlüklerinin korunmasız bırakıldığı anlamına gelecektir.

50. Bu doğrultuda, özel hukuk iş ilişkisi kapsamında çalışan bireylerin Anayasa ile güvence altına alınan haklarına yönelik müdahale iddiası içeren uyuşmazlıklarının karara bağlandığı davalarda

derece mahkemelerince söz konusu güvenceler göz ardı edilmemeli, işveren ve çalışanlar arasındaki çatışan çıkarlar adil biçimde dengelenmeli, başvuruculara tahsis edilmiş kurumsal e-posta hesaplarının incelenmesi şeklindeki müdahalenin işverenin meşru amacıyla ölçülü olup olmadığı değerlendirilmeli ve ulaşılan sonuç hakkında hüküm kurulurken ilgili ve yeterli gerekçeler sunulmalıdır.

51. Derece mahkemeleri tarafından tarafların çıkarları dengelenirken ve müdahalenin ölçülülüğü irdelenirken iş sözleşmelerinde kısıtlayıcı ve zorlayıcı düzenlemelerin ne şekilde belirlendiği, tarafların bu düzenlemeler hakkında bilgilendirilip bilgilendirilmediği, çalışanların temel haklarına yönelik müdahalede bulunulmasına neden olan meşru amacın müdahale ile ölçülü olup olmadığı, başvuruya konu olayda olduğu gibi sözleşmenin feshinin çalışanların eylem ya da eylemsizlikleri karşısında makul ve orantılı bir işlem olup olmadığı somut olayın koşullarına göre ele alınmalıdır. Ayrıca yargılamalar sırasında gerçekleştirilen işlemlerin ve neticede verilen kararın gerekçesinin bizatihi özel hayat alanına ilişkin bir müdahale oluşturmaması için derece mahkemelerince gereken özen gösterilmelidir.

52. AİHM de özel hukuk iş ilişkilerinde Sözleşmenin 8-11. maddelerinin ihlal edildiği iddiasıyla önüne gelen davalarda, taraf devletlerin anılan maddelerdeki güvencelerden kaynaklanan pozitif yükümlülüklerini yerine getirip getirmediğini incelemekte ve işten çıkarılan başvurucuların söz konusu güvencelerinin özel hukuk iş ilişkileri çerçevesinde ulusal mahkemelerce yeterli derecede korunup korunmadığını irdellemektedir (Palomo Sanchez ve diğerleri/İspanya, § 61).

53. AİHM'e göre Sözleşme'nin 8-11. maddelerinde yer alan haklara ilişkin olan özel hukuk uyuşmazlıklarında bireylerin çıkarlarıyla toplumun çatışan çıkarları arasında ulusal mahkemelerce adil bir denge kurulması gerekir. (Köpke/Almanya, B. No: 420/07, 5/10/2010; Palomo Sanchez ve diğerleri/İspanya, § 62; Eweida ve diğerleri/Birleşik Krallık, B. No: 48420/10, ..., 15/1/2013, § 84). Ayrıca güvence altındaki söz konusu haklara özel hukuk iş ilişkisi kapsamında yapılan müdahalelerin meşru amaçla ölçülü olup olmadığı ile ulusal mahkemelerce verilen kararlarda sunulan gerekçelerin ilgili ve yeterli olup olmadığı tespit edilmelidir (Palomo Sanchez ve diğerleri/İspanya, § 63).

54. Karşılıklı menfaatler gözetilerek özel hukuk kişileri tarafından imzalanan iş sözleşmeleri gereğince taraflar, doğal olarak birtakım sorumluluklar altına girmekte, çalışma saatleri içinde bazı kısıtlayıcı kurallara uyacaklarını taahhüt etmekte ve sözleşmeye aykırılık hâlinde ne tür yaptırımlarla karşı karşıya kalacakları hususunda bilgi sahibi olmaktadır. Bu noktada iş yerindeki huzur ve güvenin devamından elde edilecek yararlar gözetilerek işveren tarafından çalışma saatleri içinde

çalışanların bazı haklarının kısıtlanabilmesi ve belirlenen çalışma düzeninin gerçekleştirilmesi için çalışanların bazı kurallara uymak zorunda bırakılmaları mümkün olabilmektedir. Ancak bu tür kısıtlayıcı ve belirlenen özel kurallara uyulmasını zorlayıcı nitelikteki hususların çalışanların temel haklarının özünü zedeleyici nitelikte olmaması, imza altına alınan iş sözleşmelerinde bu hususların açık bir şekilde yer alması ve çalışanların bu hususlarda bilgilendirilmesi gerekir. Bilgilendirmelerin ve gerekli uyarıların yapılmadığı durumlarda çalışanlar, temel hak ve özgürlüklerine keyfî bir müdahalede bulunulmayacağı hususunda makul bir beklenti içinde olacaklarından sözleşme şartlarını genellikle belirleyici konumda olan işverenler tarafından çalışanlara yönelecek bu tür müdahalelerin kabul görmesi söz konusu olmayacaktır.

55. Çatışan çıkarların belirlenmesi, doğru dengenin kurulması ve müdahalelerin işverenin meşru amacıyla ölçülü olup olmadığının tespiti öncelikle derece mahkemelerinin yetki ve sorumluluk alanındadır. Olayın tüm tarafları ile doğrudan temas hâlinde bulunan derece mahkemelerinin olayın koşullarını değerlendirmek açısından daha avantajlı konumda bulunduğu da tartışmasızdır. Anayasa Mahkemesinin rolü ise bu kuralların yorumunun Anayasa'ya uygun olup olmadığını belirlemekle sınırlıdır. Bu nedenle Anayasa Mahkemesi, derece mahkemeleri tarafından izlenen usulü denetleme ve özellikle mahkemelerin tarafların sınırlanan hak ve özgürlüklerine yönelik müdahalelerin hukukiliğini yorumlayıp uygularken Anayasa'nın 20. ve 22. maddesindeki güvenceleri gözetip gözetmediğini belirleme yetkisine sahiptir. Bu kapsamda Anayasa Mahkemesinin görevi, sözleşmelerin fesih nedeninin oluşup oluşmadığını değerlendirmek ve bunların uygulanması hususunda derece mahkemelerinin yerini almak olmayıp kamusal makamların takdir hakları kapsamında aldıkları kararları, özel hayata saygı hakkı ile haberleşme hürriyeti bağlamındaki güvenceler açısından değerlendirmektir.

56. Bu doğrultuda AİHM de ulusal mahkemeler tarafından izlenen usulü denetleme ve özellikle ulusal mahkemelerin mevzuat hükümlerini yorumlayıp uygularken Sözleşme'deki ve özellikle 8. maddedeki güvenceleri gözetip gözetmediğini belirleme yetkisine sahip olduğunu vurgulamakta; yaptığı denetime temel aldığı önemli bir ilke olan ikincillik ilkesi gereği, ulusal mahkemelerin mevzuat hükümlerinin yorumlanmasına ilişkin takdirini değerlendirmeye tabi tutmamakta; ancak ulusal mahkemeler tarafından ulaşılan sonucun Sözleşme'nin 8. maddesinde öngörülen standartlara uygun bir denge sağlayıp sağlamadığını ve ulaşılan sonucun bu yönüyle özel hayata saygı hakkının ihlali anlamına gelip gelmediğini incelemektedir (Petrenco/Moldova, B. No: 20928/05, 30/6/2010, § 54; Palomo Sanchez ve diğerleri/İspanya, § 55).

b. Genel İlkelerin Uygulanması

57. Somut olaydaki uyuşmazlığın özel hukuk kişileri arasında gerçekleşmesi nedeniyle temel hak ve özgürlüklerin sağladığı güvencelerin yerine getirilmediği iddiasını içeren başvurunun devletin pozitif yükümlülükleri bağlamında ele alınması gerekir (bkz. § 46).

58. Belirtildiği üzere özel hayata saygı hakkı kapsamında ele alınabilecek olan negatif ve pozitif yükümlülüklerin sınırının ve pozitif yükümlülüklerin hangi durumda olumlu edimde bulunulmasını zorunlu kıldığı kesin çizgilerle belirlenmesi mümkün olmayıp bu yükümlülüklerin olaydan olaya farklılaşması olasıdır (bkz. §§45, 46).

59. Başvurucular, e-posta hesaplarının incelenmesinin özel hayat alanlarına ve haberleşme hürriyetlerine haksız bir müdahale oluşturmasına rağmen feshin haksız olduğunun tespit edilerek geçersiz sayılması ve işe iadelerinin sağlanması talebiyle açtıkları işe iade davalarında bu yönde bir tespit yapılmadığını, aksine Mahkemelerce verilen kararlar nedeniyle söz konusu müdahalelerin meşru hâle getirildiğini ve yazışmalarının alenileştirildiğini iddia etmişlerdir. Bu kapsamdaki iddiaların, müdahalelerin nedeni olarak gösterilen olayların gerçekleştiği sürecin özellikleri incelenerek ve derece mahkemelerince gerçekleştirilen yargılamalarda yukarıda belirlenen ilkelere (bkz. §§ 50, 51, 54) uygun şekilde hareket edilip edilmediği dikkate alınarak değerlendirilmesi gerekir.

60. Başvuru konusu olayda işe iade davalarını yürüten Bakırköy 12. İş Mahkemesinin 31/1/2013 tarihli birinci oturumunda, ikinci başvurucunun eski eşi dâhil yedi tanık dinlenmiş; tanık ifadelerinin genelinde başvurucular arasındaki ilişkinin boyutu ve yakınlığı hakkında tanıkların gözlemlerine yer verilmiştir. Ayrıca farklı birimlerde çalışan başvurucuların arkadaşlıklarının verimlilik ve performanslarına olan yansıması ile genel olarak iş ortamına olan etkisi de tanık ifadelerinde dile getirilmiştir. Buna göre fesih tarihinde başvurucular ile aynı Şirket bünyesinde birlikte çalışan diğer tanıkların beyanlarında başvurucuların performans ve verimliliklerine ilişkin olumsuz değerlendirmelerin bulunmadığı görülmüş, bazı tanıklar ise başvurucuların birbirlerine yakın davrandıkları konusunda birtakım duyular aldıklarını ancak arkadaşlık ilişkisinin ötesindeki bir ilişkinin varlığından haberdar olmadıklarını dile getirmişlerdir (bkz. § 17).

61. Tarafların yargılama sürecinde dile getirdikleri beyanlar ile tanıkların ifadeleri incelendiğinde, ikinci başvurucunun eski eşi tarafından işverene sunulan başvuruculara ait yazışmaların kişisel e-posta hesapları üzerinden mi yoksa kurumsal e-posta hesapları üzerinden mi gerçekleştirildiği hususu tespit edilememekle birlikte başvurucuların iş sözleşmelerinin feshedildiği tarihte işveren Şirket bünyesinde insan kaynakları direktörü olarak çalışan tanığın mahkeme huzurunda dile getirdiği “..Bilgi işlem vasıtasıyla davacının e-maillini özel amaçlı kullanıp kullanmadığı konusunda araştırma yaptık, gerçekten de belirtilen e-mailler bilgisayar kayıtlarında mevcuttur.” şeklindeki

beyanları ile işverenin Derece Mahkemelerine sunduğu dilekçelerdeki kabul beyanları dikkate alındığında, söz konusu yazışmaların içerikleri ile ikinci başvurucunun eski eşinin beyanları üzerinden durumdan haberdar olan işveren tarafından yazışmaların doğruluğunun teyit edilmesi amacıyla bilgi işlem sisteminden ulaşılabilen başvurucuların kurumsal e-posta hesaplarının incelendiği anlaşılmaktadır.

62. Yargılamaya konu dava dosyalarından, başvurucuların karşılıklı olarak gerçekleştirdikleri yazışmaların dava dışı üçüncü kişi tarafından davalı Şirketin yetkili kişi ya da organlarının bilgisine sunulduğu, bundan sonra kurumsal e-posta hesapları üzerinden işveren tarafından inceleme yapıldığı, elde edilen yazışmalarda yer alan unsurların iş sözleşmelerine aykırı olduğundan yola çıkılarak farklı gerekçelerin de eklenmesiyle sözleşmelerin feshedildiği, davalı Şirket tarafından söz konusu yazışmaların liste hâlinde ilk Derece Mahkemelerine delil olarak sunulduğu, delilleri inceleyen ve tanıkları dinleyen Mahkemelerce oluşturulan karar gerekçelerinde söz konusu yazışmaların içeriklerine ilişkin olarak herhangi bir detaya yer verilmediği ve işveren açısından iş ilişkilerinin sürdürülmesi olanağının kalmadığı şeklinde değerlendirme yapılarak davaların reddedildiği görülmektedir.

63. Başvuru konusu olayda, işverenin belirlediği kurallar çerçevesinde iş yerinde huzur ve disiplinin devamından elde edeceği faydalar ile başvurucuların özel hayatlarına saygı hakları ve haberleşmelerinin gizliliği arasında var olan bir çatışma hâlimden söz edilebilir. Ancak Anayasa Mahkemesinin görevi, özel hukuk kişileri arasındaki söz konusu uyuşmazlık hakkında doğrudan değerlendirmelerde bulunmak değildir. Anayasa Mahkemesinin rolü, uyuşmazlığın çözümünde tarafları bağlayıcı kararlar alan derece mahkemeleri tarafından izlenen usulü denetlemek ve tarafların sınırlanan hak ve özgürlüklerine yönelik müdahalelerin hukukiliğini yorumlayıp uygularken Anayasa'nın 20. ve 22. maddelerindeki güvencelerin derece mahkemelerince gözetilip gözetilmediğini belirlemektir.

64. Başvurucular ve işveren tarafından imzalanan iş sözleşmelerinde yer alan hükümler gereğince başvurucuların iş yerinde uyulması gereken kurallara ilişkin yürürlükte olan İç Tüzük'ü, Temel Yönetmelik'i, oryantasyon kitapçığını, Seyahat Yönetmeliği'ni, talimatları ve prosedürleri ilgili sözleşmelerin ayrılmaz eki ve parçası olarak kabul ettikleri ve tüm bu düzenlemelere uymakla kendilerini yükümlü kıldıkları görülmektedir.

65. İşverenlerin keyfî ve sınırsız bir şekilde çalışanların özel hayat alanlarına ve haberleşme hürriyetlerine yönelik müdahalelerde bulunabilmelerine izin veren düzenlemelerin, Anayasa'nın 11. ve 12. maddeleri kapsamında kabul görmesi mümkün olmamakla birlikte anayasal hak ve

özgürlüklerin sağladığı güvencelere, kanunlara, uluslararası sözleşmelere aykırı olmayacak şekilde işletmenin ticari gerekliliklerine ve disiplin anlayışına göre belirlenen kuralların açık bir şekilde yer aldığı düzenlemelerin bulunduğu ve bu düzenlemeler konusunda çalışanların önceden bilgilendirilip uyarıldığı durumlarda, kapsamı belirli şekilde çalışanların özellikle çalışma saatleri içinde birtakım haklarının kısıtlanması ve kuralların dışına çıkılmamaya zorlanması amacıyla tedbirler alınması makul görülebilir. Bu doğrultuda bir bilgilendirmenin ve uyarının yapılmadığı durumlarda, hak ve özgürlüklerine bir müdahalede bulunulmayacağı hususunda çalışanların makul bir beklenti taşıyacaklarının kabul edilmesi ve söz konusu hak ve özgürlüklerin sağladığı güvencelerden yararlandırılması gerekmektedir.

66. Bu kapsamda yapılan incelemede iş sözleşmelerinin parçası olarak kabul edilen İş Yeri Temel Yönetmeliği'nin, Bilgi Güvenliği Taahhütnamesi'nin, temel yönetim ilkeleri ve temel davranış kurallarının yer aldığı düzenlemenin, ticari alışveriş yapılan firma ilişkilerine yönelik etik kuralların yer aldığı düzenlemenin, İş Yeri Seyahat Yönetmeliği'nin, İş Yeri Disiplin Yönetmeliği'nin, İş Yeri Personel Yönetmeliği'nin ve İş Yeri Kıyafet Yönetmeliği'nin iş sözleşmesiyle birlikte başvurucular tarafından her bir sayfasının ayrı ayrı imzalandığı ve böylece iş yerinde huzur ve disiplinin sağlanması amacıyla işveren tarafından hazırlanmış kuralları ve kısıtlamaları içeren tüm genel düzenlemeler hakkında başvurucuların yeterli biçimde bilgilendirildiği anlaşılmaktadır.

67. Özellikle Bilgi Güvenliği Taahhütnamesi'yle başvurucuların, Şirket tarafından kendilerine iş için tahsis edilmiş olan bilgisayar, e-posta, internet kullanımı, telefon, iletişim programı, diğer IT kaynaklarını ve iletişim araçlarını zaruri ihtiyaçları aşan ölçüde kişisel amaçlı, eğlence niyetli, genel ahlaka, örf ve adetlere aykırı şekilde kullanmayacakları hususunda işverenlerine karşı taahhüt altına girdikleri; ayrıca Şirket yöneticileri tarafından başvuruculara haber verilmeksizin ve uyarıda bulunulmaksızın kullandıkları IT ve iletişim kaynaklarının her zaman takip altında tutulabileceği, yapılan yazışmaların ve iletişim kayıtlarının yedeklenebileceği, raporlanabileceği, gerekli durumlarda detaylı olarak incelenebileceği, el konulabileceği ve kullanım sınırlaması getirilebileceği hususunda da kabul beyanında buldukları ve taahhüt verdikleri görülmektedir.

68. İş sözleşmelerinin parçası olan düzenlemeler ile şirket kaynaklarının, bilgisayarların, kurumsal e-posta hesaplarının kişisel amaçlar doğrultusunda kullanımı kesin şekilde yasaklanmış; gerektiğinde yazışmaların ve iletişim kayıtlarının takip edilebileceği ve incelenebileceği hususunda başvuruculara gerekli uyarılar ve bilgilendirmeler yapılmıştır. Bunun yanında, kurumsal olmadığı sürece kişisel hesapların ve kişisel iletişim vasıtalarının mesai saatleri içerisinde kullanılma imkânı olmasına ve buna ilişkin bir engel bulunmamasına rağmen, yapılan işin gerekleriyle ilgisi olmayan yazışmaların

iş sözleşmelerine aykırı biçimde mesai saatleri içerisinde kurumsal hesaplar üzerinden gerçekleştirildiği anlaşılmaktadır. Bu nedenlerle başvurucuların kurumsal e-posta hesapları üzerinden gerçekleştirdikleri kişisel yazışmaların korunması konusunda makul bir beklenti içinde oldukları sonucuna ulaşamaz.

69. Ayrıca işveren, başvurucuların kurumsal e-posta hesaplarını incelemiş; bunu da ikinci başvurucunun eski eşi tarafından Şirket yönetimine sunulan e-posta yazışmaları hakkında bilgi sahibi olduktan sonra başvurucuların Şirket düzenlemelerine aykırı davranışlarının bulunduğu şeklindeki iddianın doğruluğunu teyit etme inancıyla gerçekleştirmiştir. Bu yöndeki tespit ile birlikte 4857 sayılı Kanun hükümleri ve iş sözleşmelerinde yer alan düzenlemeler dikkate alındığında kurumsal e-posta hesaplarının kişisel amaçlarla ve Temel Yönetmelik'e uygun kullanıp kullanmadığını doğrulamak amacıyla başvurucuların yazışmalarını inceleyen işverenin meşru bir amaç taşıdığı ve işveren tarafından gerçekleştirilen müdahalenin söz konusu meşru amaçla ölçülü olduğu, bu hususların Derece Mahkemelerince verilen kararların gerekçelerinde dikkate alındığı kanaatine ulaşılmıştır.

70. Başvuruya konu edilen yargılama süreçleri incelendiğinde öncelikle başvurucuların Derece Mahkemeleri önünde delillerini sundukları, iddiada bulunma ve savunma haklarını herhangi bir engellemeyle karşı karşıya kalmadan kullandıkları görülmektedir. Ayrıca söz konusu yazışmaların çalışma saatleri içinde kişisel amaçlar doğrultusunda kullanıldığı, iş yeri düzenine ilişkin olarak belirlenen düzenlemeler hakkında başvurucuların bilgilendirildikleri ve uyarıldıkları, bu durumu ispat edecek şekilde imzalarının alındığı, sözleşmelere aykırı davranışların bulunduğu hususunda oluşan inanç doğrultusunda önceden belirlenmiş müdahale sınırlarına riayet edilerek işveren tarafından kurumsal e-posta hesaplarının denetlendiği, bunun dışında işveren tarafından başvuruculara ait diğer verilere ulaşıp inceleme yapıldığına dair herhangi bir bilginin bulunmadığı anlaşılmaktadır. Yargılamalarda, başvuruculara ait hizmet cetveli ile iş yeri özlük dosyalarının Derece Mahkemeleri tarafından celp edilerek incelendiği, karar gerekçelerinde kurumsal e-posta yazışmalarının içeriklerine yer verilmediği, dava konusuyla sınırlı bir şekilde değerlendirme yapıldığı, başvurucuların doğruluk ve bağlılıkla bağdaşmayan eylemleri nedeniyle iş yerinde olumsuzlukların yaşandığı ve bu durumun işveren açısından sözleşmelerin sürdürülmesi imkânını ortadan kaldırdığının kararlarda vurgulandığı, başvurucuların eylemlerinin 4857 sayılı Kanun'un yanı sıra iş sözleşmelerine ve iş yerinin iç düzenlemelerine aykırılıklar oluşturduğu, bu nedenlerle sözleşmelerin feshedilmesinde hukuka aykırı bir durumun bulunmadığı şeklinde kararlar verilmiştir. Ayrıca ikinci başvurucunun eski eşinin tanık sıfatıyla alınan ifadesinin işverenin iddialarının doğruluğunun anlaşılabilmesi amacıyla Mahkemece sorulan ve mahremiyet içermeyen sorulara

verilen cevaplardan oluştuğu, yargılama süreçlerinde ve oluşturulan karar gerekçelerinde başvurucuların özel hayat alanlarını alenileştiren ve haberleşmelerinin gizliliğini ortadan kaldıran herhangi bir unsura yer verilmediği anlaşılmaktadır.

71. Derece Mahkemelerince verilen kararlarda, başvurucuların makul bir beklentisinin bulunmadığı hususunun dikkate alınarak başvurucular ile işveren arasında çatışan çıkarların dengelendiği, işveren tarafından başvuruculara tahsis edilmiş kurumsal e-posta hesaplarının incelenmesi şeklindeki müdahalenin Şirket içi düzenlemeler gereğince işverenin meşru amacıyla ölçülü olup olmadığı hususunda değerlendirmelerin yapıldığı, sözleşmelerin feshinin başvurucuların eylemleri karşısında makul ve orantılı bir işlem olup olmadığının gözetildiği ve tüm bu hususlara dayanılarak davaların reddine ilişkin ilgili ve yeterli gerekçeler sunulduğu, ayrıca başvurucular arasındaki yazışmalara ait içeriklerin gerek yargılamaya ilişkin işlemlerde gerekse karar gerekçesinde alenileştirilmediği sonucuna ulaşılmıştır.

72. Açıklanan nedenlerle özel hukuk iş ilişkilerinden doğan uyuşmazlıkları karara bağlayan Derece Mahkemelerince ilgili ve yeterli gerekçeler oluşturularak anayasal güvencelerin korunması açısından pozitif yükümlülüklerin yerine getirildiği ve yargılama süreçlerde gerçekleştirilen işlemlerde yazışmaların içeriklerinin alenileştirilmediği anlaşıldığından başvurucuların Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkı ile Anayasa'nın 22. maddesinde güvence altına alınan haberleşmenin gizliliği hakkının ihlal edilmediğine karar verilmesi gerekir.

V. HÜKÜM

Açıklanan gerekçelerle;

A. Özel hayata saygı hakkının ve haberleşmenin gizliliği hakkının ihlal edildiğine ilişkin iddianın **KABUL EDİLEBİLİR OLDUĞUNA,**

B. Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkının ve Anayasa'nın 22. maddesinde güvence altına alınan haberleşmenin gizliliği hakkının **İHLAL EDİLMEDİĞİNE,**

C. Başvurucular tarafından yapılan yargılama giderlerinin üzerlerinde **BIRAKILMASINA**

24/3/2016 tarihinde OYBİRLİĞİYLE karar verildi.

Anayasa Mahkemesi - Bülent Kaya Kararı (2013/2941)

Bülent Kaya [GK], B. No: 2013/2941, 11/5/2016

Başvuru, başvuru hakkındaki derdest ceza yargılamasına ilişkin bilginin Genel Bilgi Toplama (GBT) sistemine kaydedilmesi ve ilgili kaydın silinmesi hususunda idareye yapılan başvuru ile bu hususta açılan davanın reddedilmesi nedeniyle özel hayatın gizliliği hakkının ihlal edildiği iddiasına ilişkindir.

TÜRKİYE CUMHURİYETİ

ANAYASA MAHKEMESİ

GENEL KURUL

KARAR

BÜLENT KAYA BAŞVURUSU

(Başvuru Numarası: 2013/2941)

Karar Tarihi: 11/5/2016

R.G. Tarih ve Sayı: 26/8/2016-29813

GENEL KURUL

KARAR

Başkan: Zühtü ARSLAN

Başkanvekili : Burhan ÜSTÜN

Başkanvekili: Engin YILDIRIM

Üyeler: Serdar ÖZGÜLDÜR, Serruh KALELİ, Recep KÖMÜRCÜ, Alparslan ALTAN, Nuri NECİPOĞLU, Hicabi DURSUN, Celal Mümtaz AKINCI, Erdal TERCAN, Muammer TOPAL, M. Emin KUZ, Hasan Tahsin GÖKCAN, Kadir ÖZKAYA, Rıdvan GÜLEÇ

Raportör: Şebnem NEBİOĞLU ÖNER

Başvurucu: Bülent KAYA

Vekili: Av. Duygu DEMİREL

I. BAŞVURUNUN KONUSU

1. Başvuru, başvurucu hakkındaki derdest ceza yargılamasına ilişkin bilginin Genel Bilgi Toplama (GBT) sistemine kaydedilmesi ve ilgili kaydın silinmesi hususunda idareye yapılan başvuru ile bu hususta açılan davanın reddedilmesi nedeniyle özel hayatın gizliliği hakkının ihlal edildiği iddiasına ilişkindir.

II. BAŞVURU SÜRECİ

2. Başvuru 8/5/2013 tarihinde Anayasa Mahkemesine doğrudan yapılmıştır. Başvuru formu ve eklerinin idari yönden yapılan ön incelemesi neticesinde başvurunun Komisyona sunulmasına engel teşkil edecek bir eksikliğin bulunmadığı tespit edilmiştir.

3. Birinci Bölüm İkinci Komisyonunca 11/11/2013 tarihinde, başvurunun kabul edilebilirlik incelemesinin Bölüm tarafından yapılmasına karar verilmiştir.

4. Bölüm tarafından 4/12/2013 tarihli toplantıda, başvurunun kabul edilebilirlik ve esas incelemesinin birlikte yapılmasına karar verilmiştir.

5. Başvurunun bir örneği bilgi için Adalet Bakanlığına (Bakanlık) gönderilmiştir. Bakanlık, görüşünü 4/2/2014 tarihinde Anayasa Mahkemesine sunmuştur.

6. Bakanlık tarafından Anayasa Mahkemesine sunulan görüş 12/2/2014 tarihinde başvurucuya tebliğ edilmiştir. Başvurucu, Bakanlık görüşüne karşı beyanda bulunmamıştır.

7. İkinci Bölüm tarafından 20/4/2016 tarihinde, başvurunun niteliği itibarıyla Genel Kurul tarafından karara bağlanması gerekli görüldüğünden Anayasa Mahkemesi İçtüzüğü'nün 28. maddesinin (3) numaralı fıkrası uyarınca Genel Kurula sevkine karar verilmiştir.

III. OLAY VE OLGULAR

A. Olaylar

8. Başvuru formu ve eklerinde ifade edildiği şekliyle ilgili olaylar özetle şöyledir.

9. Başvurucu hakkında 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu'nun 7. maddesine muhalefet iddiasıyla iddianame tanzim edilmiş olup Van 4. Ağır Ceza Mahkemesince müsnet suçun 1/3/1926 tarihli ve 765 sayılı Türk Ceza Kanunu'nun 312. maddesinin ikinci fıkrası kapsamında değerlendirildiği gerekçesiyle Mahkemenin 29/9/2004 tarihli ve E.2004/122, K.2004/116 sayılı görevsizlik kararı ile dosya Van Asliye Ceza Mahkemesine iletilmiştir.

10. Van 2. Asliye Ceza Mahkemesinin 15/2/2007 tarihli ve E.2004/596, K.2007/41 sayılı kararı ile başvurucu ve diğer sanıklar hakkındaki yargılamanın 3713 sayılı Kanun'un 7. maddesi kapsamında

yapılması kanaatiyle görevsizlik kararı verilmekle dosyanın Van Ağır Ceza Mahkemesine gönderilmesine karar verilmiştir.

11. Van 4. Ağır Ceza Mahkemesinin 12/4/2007 tarihli ve E.2007/159, K.2007/161 sayılı görevsizlik kararı ile, yargılamanın 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 215. ve 216. maddeleri kapsamında yapılması gerektiği kanaatiyle görevsizlik kararı verilmekle, dosya olumsuz görev uyuşmazlığının çözümü için Yargıtay 5. Ceza Dairesine gönderilmiştir.

12. Yargıtay 5. Ceza Dairesinin 10/10/2007 tarihli ve E.2007/9615, K.2007/7544 sayılı kararı ile Van 4. Ağır Ceza Mahkemesinin 12/4/2007 tarihli görevsizlik kararının kaldırılması sonucunda Van 4. Ağır Ceza Mahkemesinin 17/3/2008 tarihli ve E.2004/596, K.2007/333 sayılı kararı ile başvurusunun 5237 sayılı Kanun'un 215. maddesi uyarınca cezalandırılmasına karar verilmiş ve karar temyiz edilmeksizin 20/5/2008 tarihinde kesinleşmiştir.

13. Belirtilen yargısal süreç devam ederken Van Devlet Güvenlik Mahkemesi Cumhuriyet Başsavcılığının 16/10/2003 tarihli yazısı ile başvuru hakkında bölücü terör örgütüne yardım ve yataklık etmek suçu kapsamında soruşturma yapılmasının istenilmesi üzerine Van Emniyet Müdürlüğüne, İçişleri Bakanlığı Kaçakçılık, İstihbarat, Harekat ve Bilgi Toplama Daire Başkanlığı Bilgi Toplama Yönergesi (Bilgi Toplama Yönergesi) uyarınca başvurucuya ait (Örnek No.1) Bilgi Formu tanzim edilerek GBT sistemi kapsamında tasnife alınmıştır.

14. Başvurusunun 24/11/2005 tarihli dilekçe ile GBT sisteminde yer alan şahsına ait bilgilerin silinmesi talebiyle idareye yaptığı başvuru, hakkındaki yargılamanın ilgili Yönerge'nin 9. maddesinin (b) fıkrasında belirtilen suçlara ilişkin olduğu ve başvuru hakkındaki söz konusu kaydın, ilgili davanın beraat veya dava zamanaşımı nedeniyle ortadan kaldırılması hâlinde iptalinin mümkün olduğu belirtilerek reddedilmiştir.

15. Başvurucu tarafından 6/1/2006 tarihinde idarenin red işleminin iptali istemiyle açılan dava, Ankara 1. İdare Mahkemesinin 22/3/2007 tarihli ve E.2006/44, K.2007/683 sayılı kararı ile reddedilmiş ve ret gerekçesi olarak 14/2/1985 tarihli ve 3152 sayılı İçişleri Bakanlığı Teşkilat ve Görevleri Hakkında Kanun'un 13. maddesinin birinci fıkrasının (c) bendi, 4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Selahiyeti Kanunu'nun Ek 7. maddesi ve Bilgi Toplama Yönergesi'nin 9. maddesinde yer alan düzenlemelere değinilmiş; davacı tarafından 3713 sayılı Kanun'un 7. maddesine muhalefet suçundan ceza davası açıldığı, ancak Van 4. Ağır Ceza Mahkemesinin 29/9/2004 tarihli kararı ile suç vasfının değişerek olay tarihinde yürürlükte olan 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 312. maddesinin 2. fıkrasında yer alan suç kapsamında yargılama yapılması gerektiği gerekçesiyle görevsizlik kararı verildiği belirtilmiştir. Gerekçede ayrıca, bu suçun ilgili Yönerge'nin 9. maddesi

kapsamında yer almadığı ileri sürülmekte ise de aynı nitelikteki suçun yürürlükteki 5237 sayılı Kanun'un 216. maddesinde yer aldığı ve Yönerge'nin belirtilen maddesinde bu suç türüne de yer verildiği anlaşıldığından, anılan iddiada yerindelik görülmediği belirtilerek 2559 sayılı Kanun'un Ek 7. maddesine dayanılarak çıkarılan Yönerge'nin 9. maddesinin (b) fıkrası uyarınca, anılan maddede belirtilen suç türleri için bilgi kaydı tutulmasına ilişkin işlemde hukuka aykırılık görülmediği ifade edilmiştir.

16. Başvurucunun temyiz talebi üzerine İlk Derece Mahkemesi kararı Danıştay Onuncu Dairesinin 7/6/2011 tarihli ve E.2007/8796, K.2011/2135 sayılı kararı ile onanmıştır.

17. Karar düzeltme talebi, Danıştay Onuncu Dairesinin 7/6/2013 tarihli ve E.2011/10693, K.2013/730 sayılı kararı ile reddedilmiş; ret kararı 8/4/2013 tarihinde başvuru vekiline tebliğ edilmiştir.

18. 8/5/2013 tarihinde bireysel başvuruda bulunulmuştur.

19. İçişleri Bakanlığı Kaçakçılık İstihbarat, Harekat ve Bilgi Toplama Dairesi Başkanlığının Anayasa Mahkemesine hitaben gönderdiği 11/6/2015 tarihli ve 1962 sayılı yazıda; Bilgi Toplama Yönergesi'nin, 3152 sayılı Kanun'un 13. maddesinin birinci fıkrasının (c) bendi ve 33. maddesi, 2559 sayılı Kanun'un Ek 7. maddesi ile 17/12/1983 tarihli Jandarma Teşkilatı Görev ve Yetkileri Yönetmeliği'nin 42. maddesinin birinci fıkrasının (f) bendine dayanılarak hazırlandığı ve söz konusu Yönerge'nin "hizmete özel" dereceli olması nedeniyle kamuya açık olmadığı belirtilmiştir. Yazı içeriğinde ayrıca, GBT sistemine kaydı yapılan bilgilerin, kolluk kuvvetlerine suç ve suçlularla mücadele çalışmalarında istihbarat kaynağı olarak, idarenin vatandaşlarla ilgili yürüttüğü iş ve işlemlerde (silah ruhsatı, sürücü belgesi ve pasaport verilmesi, kamu hizmetlerinden men cezalarının takibi) kullanıldığı, bunun yanı sıra 26/10/1994 tarihli ve 4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli İle Kamu Görevine Alınmayanların Haklarının Geri Verilmesinde ve 1402 Numaralı Sıkıyönetim Kanunu'nda Değişiklik Yapılmasına İlişkin Kanun ile Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği gereği, bakanlıklar ile kamu kurum ve kuruluşlarının gizlilik dereceli birim ve kısımları ile yurtdışı teşkilatlarında ve askeri, emniyet, istihbarat teşkilatlarında ve ceza infaz kurumu ve tutuk evlerinde çalıştıracakları personelin güvenlik soruşturması ve arşiv araştırması işlemleri için kullanıldığı ifade edilmiştir. İlgili program esas olarak İçişleri Bakanlığına bağlı kolluk birimlerince kullanılmakla birlikte, ayrıca Başbakanlık ve Maliye Bakanlığı bünyesinde bulunan birimler ile yapılan protokoller gereği bilgi paylaşımı yapıldığı belirtilmiştir.

B. İlgili Hukuk

20. 3152 sayılı Kanun'un 13. maddesinin birinci fıkrasının (c) bendi şöyledir:

"Kaçakçılık İstihbarat, Harekat ve Bilgi Toplama Dairesi Başkanlığının görevleri şunlardır:

...

c) Suç işleyip ele geçmeyen kişilerin, çalınan veya kaybedilen motorlu taşıtların, ateşli silahların, kimliği ispata yarayan her türlü belgelerin kayıtlarını tutarak güvenlik kuvvetlerine bildirmek, görevli kuruluşlarla ilgili kuvvetleri arasında koordinasyon sağlamak."

21. 3152 sayılı Kanun'un 33. maddesi şöyledir:

"Bakanlık, kanunla yerine getirmekle yükümlü oldukları hizmetleri; tüzük, yönetmelik, tebliğ, genelge ve diğer idari metinlerle düzenlemekle görevli ve yetkilidir."

22. 2559 sayılı Kanun'un Ek 7. maddesi şöyledir:

"Polis, Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayişini sağlamak üzere, ülke seviyesinde istihbarat faaliyetlerinde bulunur, bu amaçla bilgi toplar, değerlendirir, yetkili mercilere veya kullanma alanına ulaştırır. Devletin diğer istihbarat kuruluşlarıyla işbirliği yapar."

23. Jandarma Teşkilatı Görev ve Yetkileri Yönetmeliği'nin 42. maddesinin birinci fıkrasının (e) ve (f) bentleri şöyledir:

"Jandarma;emniyetveasayişisağlamak,kamudüzeninikorumaklayükümlüolup,bu görevlerini iki şekilde yürütür.

...

(e) Eski hükümlülerin, sabıkalı ya da şüpheli ve serserilerin, iş ve ilişkilerini araştırır. Belirli zaman aralıklarıyla çevrelerinde gizlice soruşturur ve elde ettiği bilgileri kayıtlara geçirerek; toplumun emniyet ve asayişini yönünden, gerekli önlemleri alır. Bu gibilerin suç işlemesini önler. Jandarmanın bu konuya ilişkin görevleri bir yönergede gösterilir.

(f) Suç faili olarak aranan kişilerin, izlenmesi ve ele geçirilmesi amacıyla gerekli teşkilatı kurar, kayıtlarını tutar, diğer kamu kurum ve kuruluşlarıyla işbirliği sağlar. Bu konuyla ilgili ayrıntılar, bir yönergeyle düzenlenir."

24. Bilgi Toplama Yönergesi'nin "Tanımlar" başlıklı 4. maddesinin ilgili kısmı şöyledir:

"Form iptali: Yönerge'nin 9/b maddesine girmeyen suçlardan açılan bilgi formlarının şahısların yakalanmaları halinde tasniften çıkarılarak imha edilmesi, 9/b maddesine giren suçlar için açılan bilgi

formlarının ise iptal koşulları oluştuğunda tasniften çıkarılarak iptal evrakı ekinde arşive alınması işlemidir. İptaller bilgi toplama birimleri tarafından re'sen veya söz konusu şahıs veya vekilinin yazılı müracaatı üzerine Yönerge'de belirlenen usül ve esaslara göre yapılır.”

25. Bilgi Toplama Yönergesi'nin "Şahıslar, hakkında bilgi formu düzenlenmesi halleri ve yapılacak işlemler" başlıklı 7. maddesinin ilgili kısmı şöyledir:

“...

Şahıslar, hakkında aşağıdaki hallerde bilgi formu açılarak programa veri girişi yapılır.

a) Şahıslar hakkında

Bu Yönerge'nin birinci maddesinde bilgi kayıtlarının hangi amaçla tutulacağı açıklanmıştır. Bu sebeple;

1) Adli makamlarca gönderilen yakalama emri ve yokluğunda tutuklama kararı ile arananlara bilgi formu düzenlenir.

2) Bu Yönerge'nin 9/b maddesinde sayılan suçları işleyenler, yakalanmış olsalar da haklarında bilgi formu düzenlenir.

...”

26. Bilgi Toplama Yönergesi'nin "Sanıkların yakalanması halinde dahi bilgi formu düzenlenecek suç türleri ve bunlar hakkında yapılacak işlemler" başlıklı 9. maddesinin ilgili kısımları şöyledir:

“a) Bu maddenin (b) fıkrasında belirtilen suçları işlemiş ve yakalanmış olan sanıklar için suç türüne uygun bilgi formu doldurulur. Bilgi Toplama Programına veri girişi yapıldığında "YAKALANDI" seçeneği işaretlenir ve bilgi formunun ortasına "YAKALANDI" kaşesi basılır. Bilgi Toplama Programının "SUÇ DETAY BİLGİLERİ" sayfasındaki bölüme ve ilçe güvenlik kuvvetinde ve emniyet şube müdürlüklerinde kalan bilgi formuna soruşturma evrakının Cumhuriyet Başsavcılığına gönderiliş tarih ve numarası yazılır.

b) Sanığı yakalanmış olsa dahi hakkında bilgi formu açılacak suç türleri.

...

14- 3713 Satılı Terörle Mücadele Kanunu kapsamına giren suçlar

...”

27. Bilgi Toplama Yönergesi'nin "Suç işleyip yakalanmayanalar ile yakalansalar dahi Yönerge'nin 9/b maddesinde sayılan suçları işleyenler hakkında yapılacak işlemler" başlıklı 10. maddesinin ilgili kısmı şöyledir:

"b) Güvenlik kuvvetlerinin kendi sorumluluk alanında el koydukları olaylarda; suç işleyen şahsın bilgisayar sorgulamasını yapar, geçmişte işledikleri suç kayıtları varsa tespit eder, soruşturma evrakına yazar.

...

2) Şüpheli/sanık yakalanmışsa (İşlediği suç 9/b maddesinde olanlar);

...

(b) Şüpheli hakkında Cumhuriyet Başsavcılığınca iddianame hazırlanıp mahkemece iddianamenin kabulünden sonra mahkemenin "Esas" sayısı alınmak suretiyle şahıs bilgi formu açılarak, Bilgi Toplama Programına girişi, programda "Hakkında İşlem Yapılacaklar" ibaresiyle şüphelinin kaydı mevcutsa kayıt üzerinde düzeltme işlemi yapılır."

28. Bilgi Toplama Yönergesi'nin "Şahıslar hakkında açılmış olan bilgi formlarının iptal edilmesi" başlıklı 16. maddesinin (b) fıkrası şöyledir:

"b) Yönerge'nin 9/b maddesi kapsamına giren suçlara ait bilgi formlarının iptali;

Bu Yönerge'nin 9/b maddesinin bentlerinde yazılı suç sayılan fiilleri işleyenler hakkında adli makamlarca, beraat, ceza verilmesine yer olmadığı, davanın düşmesi veya dava zaman aşımı nedeniyle davanın ortadan kaldırılmasına karar verilmiş ve kararın kesinleşmiş olması halinde bilgi formları iptal edilir."

29. Avrupa Konseyi bünyesinde hazırlanan 28/1/1981 tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "Tanımlar" başlıklı 2. maddesinin birinci fıkrasının (a) bendi şöyledir:

"Bu Sözleşmenin amaçları bakımından:

(a) Kişisel Veriler: Kimliği belirli veya belirlenebilir bir kişi hakkındaki tüm bilgileri ifade eder."

30. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "Verilerin niteliği" başlıklı 5. maddesinin birinci fıkrasının (a) bendi şöyledir:

"Otomatik bilgi işleme konu teşkil eden kişisel nitelikteki veriler:

(a) Meşru ve yasal yoldan elde edilmeli ve işleme tâbi tutulmalıdır;

- (b) Belli ve meşru amaçlar için kaydedilmeli ve bu amaca aykırı şekilde kullanılmamalıdır;
- (c) Uygun ve elverişli olmalı ve kaydedildikleri amaca göre aşırı olmamalıdır;
- (d) Doğru ve icabında güncel olmalıdır;
- (e) İlgili kişilerin kimliklerini belirtecek bir biçim altında ve kaydedildikleri nihai amaç için gerekli görülen süreyi aşmayacak bir süre için muhafaza edilmelidir.”

31. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin “Verilerin güvenliği” başlıklı 7. maddesinin birinci fıkrasının (a) bendi şöyledir:

“Otomatik fişiyelere kaydedilen kişisel nitelikteki verileri korumak için, bunların kazaen veya izinsiz olarak imhasına veya zayi olmasına veya bunların elde edilmesine, değiştirilmesine veya izinsiz olarak dağıtılmasına karşı uygun güvenlik önlemleri alınması zorunludur.”

32. Avrupa Konseyi Parlamenterler Meclisinin emniyet birimleri tarafından kişisel nitelikteki verilerin kullanılmasını düzenlemeye yönelik R(87)15 sayılı Tavsiye Kararının “Verilerin toplanması” başlıklı 2 nolu prensibi şöyledir:

“Kişisel nitelikteki verilerin, emniyet birimlerince kullanılmak üzere toplanması, somut bir tehlikenin ya da belli bir suçun cezalandırılmasıyla sınırlandırılmalıdır. Bu maddeye yapılacak her istisna, özel bir yasal mevzuatla öngörülmelidir.”

33. Belirtilen Tavsiye Kararının “Verilerin kaydedilmesi” başlıklı 3 nolu prensibi şöyledir:

“Kişisel nitelikteki verilerin, emniyet birimlerince kullanılmak üzere, kaydedilmesi, sadece, gerçek verileri kapsamalı ve polislerin, iç hukuk çerçevesinde ve uluslar arası hukuktan doğan yükümlülükleri çerçevesinde, yasal görevlerini yerine getirmeleri için gereken verileri sağlamalıdır.”

34. Belirtilen Tavsiye Kararının “Verilerin saklanma süresi ve güncellenmeleri” başlıklı 7 No.lu prensibi şöyledir:

“Emniyet tarafından kullanılacak kişisel nitelikteki verilerin, kaydedildikleri amaçlar için gerekli olmamaları halinde, silinmeleri için gerekli tedbirler alınmalıdır.

Bu amaçla, özellikle, aşağıdaki kriterler dikkate alınmalıdır: verileri, belli bir durum için yapılan soruşturma ışığında saklama gerekliliği; kesin bir kararın verilmesi ve özellikle de beraat; hakların iadesi, zamanaşımı; af; ilgili kişinin yaşı; özel kategorideki veriler.”

IV. İNCELEME VE GEREKÇE

35. Mahkemenin 11/5/2016 tarihinde yapmış olduğu toplantıda başvuru incelenip gereği düşünüldü:

A. Başvurucunun İddiaları

36. Başvurucu; aranan şahıslardan olmamasına rağmen hakkında yürütülen derdest ceza yargılamasına ilişkin bilginin GBT sistemine kaydedildiğini, belirtilen kaydın silinmesi hususunda idareye yaptığı başvurunun ve bu hususta açtığı davanın, ilgili mevzuat hükümlerinin doğru şekilde yorumlanmaması nedeniyle reddedildiğini, belirtilen uygulamaya temel alınan Bilgi Toplama Yönergesi'nin dayandığı Kanun ile kolluk görevlilerine verilen yetkinin amacına aykırı şekilde genişletilerek, idarenin düzenleyici işlem yapma yetkisinin aşıldığını ve yasal dayanaktan yoksun idari bir pratik oluşturulduğunu, yargılandığı suçun Bilgi Toplama Yönergesi'nin 9. maddesinin (b) fıkrasında yer alan suçlar arasında olmadığını, belirtilen bilgilerin ne kadar süreyle saklı tutulacağını ve silinip silinmeyeceğinin belirsiz olduğunu, ayrıca derdest yargılama bilgisinin mahkumiyet kaydı gibi işlem görmesi nedeniyle yargı kararı olmaksızın suçlu olarak addedildiğini belirterek Anayasa'nın 20. maddesinde tanımlanan özel hayatın gizliliği hakkının ve 38. maddesinde tanımlanan masumiyet karinesinin ihlal edildiğini iddia etmiştir.

B. Değerlendirme

37. Anayasa Mahkemesi, olayların başvuru tarafından yapılan hukuki nitelendirmesi ile bağlı olmayıp olay ve olguların hukuki tavsifini kendisi takdir eder (Tahir Canan, B. No: 2012/969, 18/9/2013, § 16). Başvurucu tarafından Anayasa'nın 20. ve 38. maddelerinde tanımlanan haklarının ihlal edildiği iddia edilmiş olmakla beraber, ihlal iddialarının mahiyeti gereği, başvurunun özel hayatın gizliliği hakkı kapsamında incelenmesi uygun görülmüştür.

1. Kabul Edilebilirlik Yönünden

38. Açıkça dayanaktan yoksun olmadığı ve kabul edilemezliğine karar verilmesini gerektirecek başka bir neden de bulunmadığı anlaşılan başvurunun kabul edilebilir olduğuna karar verilmesi gerekir.

2. Esas Yönünden

39. Başvurucu, hakkında yürütülen derdest ceza yargılamasına ilişkin bilginin GBT sistemine kaydedildiğini ve ilgili kaydın silinmesi hususunda idareye yaptığı başvuru ile bu hususta açtığı davanın reddedildiğini belirterek Anayasa'nın 20. maddesinde tanımlanan özel hayatın gizliliği hakkının ihlal edildiğini iddia etmiştir.

40. Bakanlık görüş yazısında benzer başvurularda Avrupa İnsan Hakları Mahkemesi (AİHM) tarafından, kişinin rızası olmaksızın hakkında kişisel veri toplanması, saklanması ve kullanılması hususunun Avrupa İnsan Hakları Sözleşmesi'nin (Sözleşme) 8. maddesi bağlamında değerlendirildiği, bu kapsamda yapılan faaliyetlerin 8. maddenin gereklerine uygun olabilmesi için,

belirtilen konuda kamu makamlarına yetki veren mevzuatın, söz konusu bilgilerin toplanma, saklanma ve kullanılma amaç ve usulleri konusunda yeterince açık düzenlemeler içermesi gerektiği, somut başvuru açısından başvurucunun yargılandığı suça ait derdest dava bilgilerinin GBT sistemine kayıt yapılmasına ilişkin yönerge kapsamında bulunup bulunmadığının tespitinin önemli olduğu belirtilerek, AİHM önüne benzer ihlal iddialarıyla yansıyan dava ve karar örneklerine yer verilmiştir.

a. Genel İlkeler

41. Anayasa'nın 148. maddesinin üçüncü fıkrası ile 30/11/2011 tarih ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 45. maddesinin (1) numaralı fıkrası hükümlerine göre Anayasa Mahkemesine yapılan bir bireysel başvurunun esasının incelenebilmesi için, kamu gücü tarafından müdahale edildiği iddia edilen hakkın Anayasa'da güvence altına alınmış olmasının yanı sıra Sözleşme ve Türkiye'nin taraf olduğu ek protokollerinin kapsamına da girmesi gerekir. Bir başka ifadeyle Anayasa ve Sözleşme'nin ortak koruma alanı dışında kalan bir hak ihlali iddiasını içeren başvurunun kabul edilebilir olduğuna karar verilmesi mümkün değildir (Onurhan Solmaz, B. No: 2012/1049, 26/3/2013, § 18).

42. Anayasa'nın "Özel hayatın gizliliği" kenar başlıklı 20. maddesi şöyledir:

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

43. Sözleşme'nin "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesi şöyledir:

"(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.”

44. Özel hayat kavramı eksiksiz bir tanımı bulunmayan geniş bir kavramdır. Bu kapsamda korunan hukuki değer esasen kişisel bağımsızlık olup, bu koruma bir taraftan herkesin istenmeyen bütün müdahalelerden uzak kendine özel bir ortamda yaşama hakkına sahip olduğuna işaret etse de, özel hayat kavramının herkesin kişisel yaşamını istediği şekilde sürdürme ve dış dünyayı bu çemberden ayrı tutma kavramına indirgenemeyeceği açıktır. Bu açıdan Anayasa'nın 20. maddesi özel bir sosyal hayat sürdürmeyi güvence altına almaktadır (Serap Tortuk, B. No: 2013/9660, 21/1/2015, § 31).

45. Özel yaşama saygı hakkı kapsamında korunan hukuksal çıkarlardan biri de bireyin mahremiyet hakkıdır. Ancak mahremiyet hakkı sadece yalnız bırakılma hakkından ibaret olmayıp, bu hak bireyin kendisi hakkındaki bilgileri kontrol edebilme hukuksal çıkarını da kapsamaktadır. Bireyin kendisine ilişkin herhangi bir bilginin; kendi rızası olmaksızın açıklanmaması, yayılmaması, bu bilgilere başkaları tarafından ulaşılamaması ve rızası hilafına kullanılamaması kısaca bu bilgilerin mahrem kalması konusunda menfaati bulunmaktadır. Bu husus, bireyin kendisi hakkındaki bilgilerin geleceğini belirleme hakkına işaret etmektedir (Serap Tortuk, § 32).

46. Özel yaşama saygı hakkı alt kategorisinde geçen “özel yaşam” kavramı AİHM tarafından da oldukça geniş yorumlanmakta ve bu kavrama ilişkin tüketici bir tanım yapmaktan özellikle kaçınılmaktadır. Bununla birlikte Sözleşme'nin denetim organlarının içtihatlarında “bireyin kişiliğini geliştirmesi ve gerçekleştirilmesi” kavramının, özel yaşama saygı hakkının kapsamının belirlenmesinde temel alındığı anlaşılmaktadır. Özel yaşamın korunması hakkının sadece mahremiyet hakkına indirgenemeyeceği gerçeği karşısında, kişiliğin serbestçe geliştirilmesiyle uyumlu birçok hukuksal çıkar bu hakkın kapsamına dâhil edilmiştir. Bu bağlamda, kişinin kendi hakkındaki bilgileri kontrol edebilme hukuksal çıkarının da özel hayata saygı hakkı kapsamındaki konununun tespit edilmesi gerekmektedir (Koch/Almanya, B. No: 497/09, 19/7/2012, § 51).

47. Bireyin kendisi hakkındaki bilgiyi kontrol edebilme hakkının konusunu oluşturan “bilgi” kavramının ne anlama geldiğinin, başka bir ifade ile özel hayatın korunması hakkının güvence kapsamında yer alan bilgilerin ne olduğunun tespiti önemlidir.

48. Anayasa'nın 20. maddesinde, herkesin özel hayatına saygı gösterilmesi hakkına sahip olduğu ve özel hayatın gizliliğine dokunulamayacağı belirtilmekte olup, bu düzenlemede yer verilen özel hayatın gizliliği hakkı, Sözleşme'nin 8. maddesi çerçevesinde özel yaşama saygı hakkı kapsamında

güvence altına alınan hakka karşılık gelmektedir. Bireyin kişisel verilerinin ve bu verilerin korunmasına dair hukuksal menfaatinin de özel yaşamı kapsamında olduğu açıktır. Mahremiyet hakkı ve bu alana ilişkin bilgilerin gizliliğinin korunması Anayasa Mahkemesi tarafından da, Anayasa'nın 20. maddesi kapsamında değerlendirilmektedir.

49. Anayasa Mahkemesi tarafından kişisel veri kavramının, belirli veya kimliği belirlenebilir olmak şartıyla bir kişiye ilişkin bütün bilgileri ifade ettiği kabul edilmekte olup bu bağlamda ad, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgilerin değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm verilerin kişisel veri kapsamında olduğu belirtilmektedir (AYM, E.2013/122, K.2014/74, 9/4/2014).

50. Bu noktada Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi de önemli tespitler içermektedir. Belirtilen Sözleşme'nin 2. maddesinde kişisel bilgi, belirli veya belirlenebilir bir kişiye ilişkin herhangi bir bilgi olarak tanımlanmakta ve söz konusu verilerin özel nitelikte olması gibi bir unsur aranmamaktadır.

51. AİHM de bilgiyi kontrol edebilme hakkı bağlamında ele aldığı birçok başvuruda, yukarıda değinilen Sözleşme hükümlerine gönderme yapmakta ve bu bağlamda AİHM içtihadında da, kişiye özel yaşamı ile ilgili sorular sorulması da dahil olmakla üzere, iş ve sosyal yaşamı ile ilgili bilgilerin, parmak izinin, fotoğrafının, hücre ve DNA örneklerinin alınması, kaydedilmesi, saklanması ve kullanılmasının, enformasyonel özerklik bağlamında değerlendirmeye tabi tutulduğu görülmektedir (Leander/İsveç, B. No: 9248/81, 26/3/1987, § 48; Rotaru/Romanya [B.D.], B. No: 28341/95, 4/5/2000, § 46; S. ve Marper/Birleşik Krallık, B. No: 30562/04 ve 30566/04, 4/12/2008, §§ 66, 67).

52. Özel hayat kavramı, bir bireyin fiziksel ve sosyal kimliğine dair birçok unsuru kapsayabilir. Bu kapsamda cinsel kimliğin belirlenmesi; isim, cinsel eğilim ve cinsel yaşam gibi unsurlar özel hayat kapsamına girdiği gibi bu kavram diğer kişisel kimlik belirleme ve bir aileye bağlanma yöntemlerini de kapsar. Bunun yanı sıra kişinin sağlığına ilişkin bilgiler de özel yaşamının önemli bir parçasını oluşturur (Mikulić/Hırvatistan, B. No: 53176/99, 7/2/2002, § 53; S. ve Marper/Birleşik Krallık, § 66).

53. Bir kişinin özel yaşamına ilişkin verilerin kaydedilmesi, özel hayata saygı hakkı anlamında bir müdahale oluşturmaktadır. Kaydedilen bilgilerin, daha sonra kullanılmış olup olmamasının bir önemi yoktur. Bununla birlikte kamu makamları tarafından muhafaza edilen kişisel nitelikli bilgilerin, özel yaşam unsurlarından birini devreye sokup sokmadığını tespit etmek için bu bilgilerin

hangi çerçevede alındıklarının ve muhafaza edildiklerinin, verilerin türünün, kullanıldıkları ve işlendikleri şeklin ve bunlardan çıkarılabilecek sonuçların dikkate alınması zaruridir (Leander/İsveç, § 48; Amann/İsviçre [B.D.], B. No: 27798/95, 16/2/2000, § 69).

b. İlkelerin Olaya Uygulanması

i. Müdahalenin Varlığı

54. Başvuruya konu olayda, başvuru hakkındaki derdest ceza yargılaması bağlamındaki verilerin GBT sistemine kaydedildiği görülmekle, başvuruyla ilgili olarak resmi makamların muhafaza ettikleri söz konusu kişisel bilgilerin, özel hayata saygı hakkı anlamında kişisel nitelikli veriler olduğu, zira kimliği belirlenmiş ya da belirlenebilecek kişilerle ilgili olduğu anlaşılmaktadır. Bu kapsamda GBT sisteminde yer alan söz konusu bilgilerin, başvuruyla ilgili olduğu tartışmasızdır.

55. Somut başvuruda, başvuru hakkında yürütülen bir ceza yargılaması ile bağlantılı olarak hakkındaki derdest dava bilgisinin bilgi toplama sistemine kaydedildiği ve bu sistemdeki kayıtların özellikle yapılan güvenlik taramaları ve güvenlik soruşturmalarında kullanılabilecek nitelikte olduğu görülmekle (bkz. § 19), söz konusu kişisel verilerin ilgili sistemde tutulması ve belirtilen şekillerde kullanılmasının, Anayasa'nın 20. maddesinde güvence altına alınan özel hayatın gizliliği hakkına bir müdahale oluşturduğu açıktır.

ii. Müdahalenin İhlal Oluşturup Oluşturmadığı

56. Özel hayatın gizliliği hakkı bağlamında kişisel veriler, Anayasa'nın 20. maddesinde ayrı bir fıkra olarak düzenlenmiş olup madde gerekçesinde karşılaştırmalı hukuk ve uluslararası belgelere işaret edilerek özel hayata saygı hakkı bağlamında kişisel verilerin korunmasının önemine değinilmiştir. Belirtilen düzenlemede özel sınırlama sebepleri öngörülmemiş olmakla birlikte yasa ile düzenleme hükmüne yer verilmiş ve kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızası ile işlenebileceği belirtilmiştir.

57. Bu bağlamda Anayasa'nın 20. maddesinde özel hayatın gizliliği hakkı açısından, bu hakkın tüm boyutlarına ilişkin olmadığı anlaşılan birtakım sınırlama sebeplerine yer verilmiş olmakla beraber özel sınırlama nedeni öngörülmemiş olan hakların dahi hakkın doğasından kaynaklanan bazı sınırları bulunmakta ayrıca Anayasa'nın diğer maddelerinde yer alan kurallara dayanılarak da bu hakların sınırlanması mümkün olabilmektedir. Bu noktada Anayasa'nın 13. maddesinde yer alan güvence ölçütleri işlevsel niteliği haizdir (Sevim Akat Eşki, B. No: 2013/2187, 19/12/2013, § 33).

58. Anayasa'nın "Temel hak ve hürriyetlerin sınırlanması" kenar başlıklı 13. maddesi şöyledir:

“Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.”

59. Belirtilen Anayasa hükmü, hak ve özgürlükleri sınırlama ve güvence rejimi bakımından temel öneme sahip olup, Anayasa'da yer alan bütün hak ve özgürlüklerin yasa koyucu tarafından hangi ölçütler gözönünde bulundurularak sınırlandırılabilceğini ortaya koymaktadır. Anayasa'nın bütünselliği ilkesi çerçevesinde Anayasa kurallarının bir arada ve hukukun genel kuralları gözönünde tutularak uygulanması zorunlu olduğundan belirtilen düzenlemede yer alan başta kanunla sınırlama kaydı olmak üzere tüm güvence ölçütlerinin, Anayasa'nın 20. maddesinde yer verilen hakkın kapsamının belirlenmesinde de gözetilmesi gerektiği açıktır (Sevim Akat Eşki, § 35).

Kanunilik

60. Hak ve özgürlüklerin kanunla sınırlanması ölçütü anayasa yargısında önemli bir yere sahiptir. Hak ya da özgürlüğe bir müdahale söz konusu olduğunda öncelikle tespiti gereken husus, müdahaleye yetki veren bir kanun hükmünün, yani müdahalenin hukuki bir temelini mevcut olup olmadığıdır (Sevim Akat Eşki, § 36).

61. Sözleşme'nin lafzı ve AİHM içtihadı uyarınca da Sözleşme'nin 8. maddesi kapsamında yapılacak bir müdahalenin meşruluğu, öncelikle söz konusu müdahalenin yasa uyarınca gerçekleştirilmesine bağlı tutulmuş olup, müdahalenin hukukilik unsurunu taşımadığının tespiti halinde, Sözleşme'nin 8. maddesinin (2) numaralı fıkrasında yer alan diğer güvence ölçütleri tetkik edilmeksizin, müdahalenin ilgili maddeye aykırı olduğu sonucuna ulaşılmaktadır (Fadeyeva/Rusya, B. No: 55723/00, 9/6/2005, § 95; Bykov/Rusya, B. No: 4378/02, 10/3/2009, § 82).

62. Anayasa'nın 20. maddesi kapsamında yapılan bir müdahalenin yasallık şartını sağladığının kabulü için de müdahalenin kanuni bir dayanağının bulunması zorunludur. Bununla birlikte temel hak ve hürriyetlerin sınırlandırılmasına ilişkin kanunların şeklen var olması yeterli değildir. Yasallık ölçütü aynı zamanda maddi bir içeriği de gerektirmekte olup bu noktada yasanın niteliği önem kazanmaktadır. Yasayla sınırlama ölçütü, sınırlamanın erişilebilirliğini, öngörülebilirliğini ve kesinliğini ifade etmekte böylece uygulayıcının keyfî davranışlarının önüne geçtiği gibi kişinin hukuku bilmesine de yardımcı olmakta bu yönüyle hukuk güvenliği güvencesi sağlamaktadır (Halime Sare Aysal, B. No: 2013/1789, 11/11/2015, § 62).

63. Kanunun, bu gerekliliklere uygun olduğunun söylenebilmesi için yeterince ulaşılabilir olması yani vatandaşların belirli bir olaya uygulanabilir nitelikteki hukuk kurallarının varlığı hakkında yeterli bilgiye sahip olabilmesi, ayrıca ilgili normun keyfiliğe karşı uygun bir koruma sağlaması, yeterli bir netlikte yetkili makamlara verilen yetkinin genişliğini ve icra edilme biçimlerini tanımlaması gerekmektedir (Halime Sare Aysal, § 63; Benzer yöndeki AİHM kararları için bkz. Silver ve diğerleri/Birleşik Krallık, B. No: 5947/72..., 25/3/1983, § 86-88; Malone/Birleşik Krallık, B. No: 8691/79, 2/8/1984, § 66-68; Rotaru/Romanya, § 55).

64. Somut başvuru açısından ise söz konusu gerekliliklere, kişisel verilerin kayıt, muhafaza ve kullanımını içeren tedbirlerin kapsamını ve uygulanmasını düzenleyen ve özellikle süre, stoklama, kullanım, üçüncü kişilerin erişimi, verilerin gizliliği, bütünlüğü ve imhası konusundaki prosedürlere ilişkin, muhataplarının yetki aşımı ve keyfiliğe karşı yeteri kadar güvenceye sahip olmalarını sağlayacak açık ve detaylı kuralların belirlenmesinin temel oluşturduğu açıktır.

65. Hukukun kendisi, beraberinde getireceği idari pratiğin dışında, yetkili makamlara bırakılan takdir yetkisinin kapsamını, söz konusu işlemin meşru amacını da gözönünde tutarak keyfi müdahalelere karşı bireyi korumak için yeterince açık bir şekilde göstermelidir. Hukuk sistemi vatandaşlara, kamu makamlarına hangi koşullarda ve hangi sınırlar içinde kişisel verileri konu alan ve potansiyel olarak özel yaşama karşı tehlike oluşturabilecek müdahalelerde bulunma yetkisi verdiğini, yeterince açık ifadelerle gösterecek nitelikte olmalıdır (Halime Sare Aysal, § 64).

66. Bu kapsamda ilgili sisteme bilgilerin girilmesi, müdahaleye temel oluşturan meşru amaçları taşıma şartına bağlı olmalı ve söz konusu yasal düzenleme, hangi bilgilerin kayıt altına alınabileceği, hangi yetkililere iletilebileceği, böyle bir iletimin hangi koşullarda mümkün olabileceği ve bilginin ilgili makamlara iletilmesi hususunda izlenecek usul konusunda açık ve ayrıntılı hükümler içermelidir. Söz konusu sisteme ilişkin düzenleme; bilgi toplama, kaydetme ve ilgili makamlarla paylaşma veya sair şekilde kullanma konusunda, yetkili makamlara tanıdığı takdir yetkisinin kullanılma tarzı ve alanı bakımından vatandaşlara yeterince öngörüde bulunma olanağı sağlamak durumundadır.

67. Anayasa Mahkemesi idareye keyfi uygulamalara meydan verebilecek çok geniş bir takdir yetkisi tanınmasını birçok kararında Anayasa'ya aykırı görmüştür. Mahkemenin gerek Anayasa'nın 13. maddesindeki yasallık ilkesini yorumlayan kararlarında gerek 7. maddedeki yasama yetkisinin devredilmezliği ilkesini yorumlayan kararlarında gerekse 2. madde kapsamında hukuk devleti ilkesini ele alan kararlarında bunu görmek mümkündür. Söz konusu kararlarda Mahkeme, kanunun şeklen var olmasını yeterli görmemekte kanunun niteliğini de araştırmakta ve bu bağlamda bir

sınırlamanın nerede başlayıp nerede bittiğinin belirtilmemesi durumunda, amacı aşan, demokratik toplum düzeninin gerekleriyle bağdaşmayan, içeriğinin takdiri yönetime bırakılmış sakıncalı sınırlamalar getirilmiş olacağı; içeriğinin belirlenmesi yönetimin görüşüne bırakılan sınırlamanın yasa ile konulduğundan söz edilemeyeceği; hukuk devletinin hukuk güvenliği ilkesinin belirliliği de gerektirdiği ve belirlilik ilkesinin, ilgili yükümlülüğün hem kişiler hem de idare yönünden belirli ve kesin olmasını, yasa kuralının, ilgili kişilerin mevcut şartlar altında belirli bir işlemin ne tür sonuçlar doğurabileceğini makul bir düzeyde öngörmelerini mümkün kılacak şekilde düzenlenmesini gerektirdiği ve yasa koyucunun temel ilkeleri koymadan, genel çerçeveyi çizmeden yürütmeye yetki vermemesi, sınırsız ve belirsiz bir alanı yönetimin düzenlemesine bırakmaması gerektiği belirtilmektedir (E.1984/14, K.1985/7, 13.06.1985; E.1987/16, K.1988/8, 19.04.1988; E.2010/7, K.2011/172, 22.12.2011).

68. Sözleşme organları da birçok kez ve özellikle ceza davaları kapsamında, resmî makamlar tarafından kişisel nitelikli verilerin depolanması, muhafaza edilmesi ve kullanılmasıyla ilgili sorunlara eğilmiş ve bu kapsamda yapılan değerlendirmelerde, uygulayıcıya sınırları belirsiz müdahale yetkisi veren hukuki düzenlemelerin hukuk devleti ilkesiyle de çatıştığı vurgulanarak keyfi müdahaleleri önlemek için hukuk kuralının verdiği yetkinin amacını ve kullanım biçimini yeterli açıklıkta belirtmiş olması zorunluluğuna işaret edilmiştir (Al Nashif/Bulgaristan, B. No: 50963/99, 20/6/2002, §§ 119-124).

69. Bununla birlikte her ihtimale çözüm getiremeyecek olan yasal mevzuatın gereken koruma seviyesi, büyük ölçüde ilgili metnin düzenlediği alan ve içeriğiyle birlikte muhataplarının niteliği ve sayısı ile yakından bağlantılıdır. Bu nedenle kuralın karmaşık olması ya da belirli ölçülerde soyutluk içermesi ve bu nedenle hukuki yardım ile tam olarak anlaşılabilir hale gelmesi, tek başına hukuken öngörülebilirlik ilkesine aykırı görülemez. Bu kapsamda hak ya da özgürlüğe müdahale eden kural belirli ölçülerdeki takdir alanını elbette uygulayıcıya sunabilir. Fakat bu takdir alanının sınırlarının da yeterli açıklıkta belirlenmesi ve kuralın asgari bir kesinlik içermesi zaruridir (Halime Sare Aysal, § 65).

70. Bu kapsamda ilgili kanuni düzenlemenin, söz konusu sınırlamaya ilişkin temel çerçeveyi ortaya koymakla birlikte özellikle uygulama koşulları ve prosedürel ayrıntıları düzenleyici işlemlere bırakması mümkündür. Ancak bu ihtimalde de söz konusu düzenleyici işlemin, yine muhataplarınca ulaşılabilir olması ve içeriği hakkında ilgilileri yeterince aydınlatacak nitelik ve açıklıkta olması gerekmektedir (Halime Sare Aysal, § 66).

71. Başvuruya konu idari uygulama ve yargısal sürecin, 3152 sayılı Kanun'un 13. maddesinin birinci fıkrasının (c) bendi, 2559 sayılı Kanun'un Ek 7. maddesi ve Bilgi Toplama Yönergesi'nin 9. maddesi temelinde yürütüldüğü anlaşılmaktadır.

72. İlgili idari ve yargısal kararlarda söz konusu uygulamanın yasal temeli olarak gösterilen 2559 sayılı Kanun'un 7. maddesine dayanılarak hazırlandığı belirtilen Yönerge'nin 9. maddesinin (a) fıkrasında, maddenin (b) fıkrasında belirtilen suçları işlemiş ve yakalanmış olan sanıklar için de suç türüne uygun bilgi formu doldurulacağı ve yakalandığı kaydı düşülmek suretiyle sistemde muhafaza edileceği ifade edilmektedir. Yönerge'nin 10. maddesinin (b) fıkrasında, güvenlik kuvvetlerinin kendi sorumluluk alanında el koydukları olaylarda; suç işleyen şahsın bilgisayar sorgulamasını yapacağı, geçmişte işledikleri suç kayıtları varsa tespit edeceği ve soruşturma evrakına yazacağı; aynı maddenin (b) fıkrasının (2) numaralı bendinin (b) alt bendinde ise şüpheli hakkında Cumhuriyet Başsavcılığınca iddianame hazırlanıp mahkemece iddianamenin kabulünden sonra mahkemenin "Esas" sayısı alınmak suretiyle şahıs bilgi formu açılarak Bilgi Toplama Programına girişinin, programda "Hakkında İşlem Yapılacaklar" ibaresiyle şüphelinin kaydı mevcutsa kayıt üzerinde düzeltme işlemi yapılacağı belirtilmektedir. Kayıtların silinmesi hususunda ise 16. maddenin (b) fıkrasında, Yönerge'nin 9. maddesinin (b) fıkrasında yazılı suç sayılan fiilleri işleyenler hakkında adli makamlarca, beraat, ceza verilmesine yer olmadığı, davanın düşmesi veya dava zaman aşımı nedeniyle davanın ortadan kaldırılmasına karar verilmiş ve kararın kesinleşmiş olması halinde bilgi formlarının iptal edileceği belirtilmekle birlikte Yönerge'nin 4. maddesinde, Yönerge'nin 9. maddesinin (b) fıkrası kapsamına girmeyen suçlardan açılan bilgi formlarının şahısların yakalanmaları halinde tasniften çıkarılarak imha edileceği, 9. maddesinin (b) fıkrası kapsamına giren suçlar için açılan bilgi formlarının ise iptal koşulları oluştuğunda tasniften çıkarılarak iptal evrakı ekinde arşive alınacağı düzenlenmektedir.

73. İlgili Yönerge uyarınca genel bilgi toplama sisteminde kaydı tutulacak unsurlar, kişileri, bazı belgeleri ve araçları kapsamaktadır. Hakkında bilgi tutulacak kişilerin ise, Yönerge'nin amacını düzenleyen 1. maddesi uyarınca suç işlemesi sebebiyle aranmasına karar verilen, kaybolan, yakalansalar dahi bazı suçları işlemiş olan ve kamu haklarından yararlanmaları konusunda sınırlama getirilen kişiler olduğu anlaşılmaktadır.

74. Yönerge'nin 7. maddesi ve 9. maddesinin (a) fıkrası hükümlerine göre hakkında arama kararı bulunmadığı veya yakalanmış olduğu hâlde belirli bazı suçlardan dolayı yargılanan kişiler hakkında da genel bilgi toplama programına bilgi kaydedilebilmektedir. Bu suçların hangileri olduğu, Yönerge'nin 9. maddesinin (b) fıkrasında gösterilmektedir.

75. Yönerge'nin hangi normlara dayalı olarak düzenlendiği "Kanuni dayanak" başlıklı 3. maddesinde açıklanmıştır. Buna göre söz konusu Yönerge, 3152 sayılı Kanun'un 13. maddesinin birinci fıkrasının (c) bendi ve 33. maddesi, 2559 sayılı Kanun'un Ek 7. maddesi ile Jandarma Teşkilatı Görev ve Yetkileri Yönetmeliği'nin 42. maddesinin birinci fıkrasının (e) ve (f) bendine dayanılarak hazırlanmıştır.

76. 3152 sayılı Kanun'un 13. maddesinin birinci fıkrasının (c) bendi, İçişleri Bakanlığı Kaçakçılık İstihbarat, Harekât ve Bilgi Toplama Dairesi Başkanlığının görevlerini düzenlemekte ve suç işleyip ele geçmeyen kişilerin, çalınan veya kaybedilen motorlu taşıtların, ateşli silahların, kimliği ispata yarayan her türlü belgelerin kayıtlarını tutarak güvenlik kuvvetlerine bildirmek, görevli kuruluşlarla ilgili kuvvetleri arasında koordinasyon sağlamak görevini, ilgili birimin görevleri arasında saymaktadır. Bu yönüyle kişilere ilişkin kayıtların tutulmasına ilişkin yetkinin, suç işleyip ele geçmeyen kişiler ile sınırlı olarak öngörüldüğü anlaşılmaktadır. Bu kapsamda ilgili Yönergeye dayanak olarak gösterilen belirtilen kanun maddesinin, Yönerge'nin "yakalansalar dahi bazı suçları işlemiş olan kişiler" hakkında kayıt tutulacağı şeklindeki düzenlemesini ve bu yöndeki uygulamayı temellendirmediği anlaşılmaktadır. 3152 sayılı Kanun'un 33. maddesinin ise yerine getirmekle yükümlü olduğu hizmetleri idari metinlerle düzenleme konusunda İçişleri Bakanlığını yetkilendirdiği anlaşılmaktadır.

77. Bununla birlikte Yönerge'nin dayanakları arasında gösterilen 2559 sayılı Kanun'un Ek 7. maddesinde, polisin devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri alacağı, emniyet ve asayişini sağlamak üzere ülke seviyesinde istihbarat faaliyetlerinde bulunacağı, bu amaçla bilgi toplayacağı, değerlendireceği, yetkili mercilere veya kullanma alanına ulaştıracağı, devletin diğer istihbarat kuruluşlarıyla işbirliği yapacağı düzenlemesine yer verildiği görülmektedir. Bu kapsamda, istihbarat faaliyetlerinde bulunma, bu amaçla bilgi toplama, değerlendirme, yetkili mercilere veya kullanma alanına ulaştırma şeklindeki yetkilere yer veren söz konusu düzenlemenin, başvuruya konu müdahalenin kanuni dayanağını oluşturduğunu anlaşılmaktadır (bkz. Bülent Polat, B. No: 2013/7666, 10/12/2015, § 87).

78. İlgili idari ve yargısal kararlara temel alınan söz konusu düzenleme göz önünde bulundurulduğunda, başvuruya konu müdahalenin kanunilik şartını sağladığı anlaşılmaktadır.

Meşru Amaç

79. Somut başvuru açısından, belirli suçlar kapsamında yargılanan kişiler hakkındaki derdest dava bilgilerinin GBT sistemine kaydı yapılarak, söz konusu bilgilerin özellikle yapılan güvenlik taramaları ve güvenlik soruşturmasında kullanıldığı (bkz. § 19), bu kapsamda söz konusu uygulamanın kamu düzeni ve güvenliğinin temini şeklindeki meşrutemelleri içerdiği anlaşılmaktadır.

Demokratik Toplum Düzeninde Gerekli Olma ve Ölçülülük

80. Kanuni dayanağı bulunan ve meşru amaç taşıyan müdahalenin ihlal teşkil etmemesi için Anayasa'nın 13. maddesinde yer verilen demokratik toplum düzeninde gereklilik, hakkın özüne dokunmama ve ölçülülük şeklindeki güvence ölçütlerine uygun olması gerekir.

81. Çağdaş demokrasiler, temel hak ve özgürlüklerin en geniş ölçüde sağlanıp güvence altına alındığı rejimlerdir. Temel hak ve özgürlüklerin özüne dokunup onları büyük ölçüde kısıtlayan veya tümüyle kullanılamaz hâle getiren sınırlamaların demokratik toplum düzeninin gerekleriyle de bağdaştığı kabul edilemez. Demokratik hukuk devletinin amacı, kişilerin hak ve özgürlüklerden en geniş biçimde yararlanmalarını sağlamak olduğundan yasal düzenlemelerde insanı öne çıkaran bir yaklaşımın esas alınması gerekir. Bu nedenle getirilen sınırlamaların yalnız ölçüsü değil; koşulları, nedeni, yöntemi ve kısıtlamaya karşı öngörülen kanun yolları gibi unsurların tamamı demokratik toplum düzeni kavramı içinde değerlendirilmelidir (Serap Tortuk, § 46; Murat Atılğan, B. No: 2013/9047, 7/5/2015, § 37; Marcus Frank Cerny, (GK), B. No: 2013/5126, 2/7/2015, § 71).

82. Hakkın özü, dokunulduğunda söz konusu temel hak ve özgürlüğü anlamsız kılan asli çekirdeği ifade etmektedir. Bu yönüyle her temel hak açısından kişiye dokunulmaz asgari bir alan güvencesi sağlamaktadır. Bu çerçevede, hakkın kullanılmasını önemli ölçüde güçleştiren, hakkı kullanılamaz hâle getiren veya ortadan kaldıran sınırlamaların, hakkın özüne dokunduğu kabul edilmelidir. Özel hayata saygı hakkı bağlamında da bu hakkın ortadan kaldırılması, kullanılamaz hâle getirilmesi veya kullanılmasının aşırı derecede güçleştirilmesi sonucunu doğuran müdahalelerin, bu hakkın özünü zedeleyeceği açıktır. Ölçülülük ilkesinin amacı da temel hak ve özgürlüklerin gereğinden fazla sınırlanmasının önlenmesidir. Anayasa Mahkemesi kararları uyarınca ölçülülük ilkesi, sınırlama için kullanılan aracın sınırlama amacını gerçekleştirmeye uygun olmasını ifade eden elverişlilik, sınırlayıcı önlemin sınırlama amacına ulaşmak bakımından zorunlu olmasına işaret eden zorunluluk ve araçla amacın orantısız bir ölçü içinde bulunmaması ile sınırlamanın ölçüsüz bir yükümlülük getirmemesi anlamına gelen orantılılık unsurlarını içermektedir (Serap Tortuk, § 47, Murat Atılğan, § 38; Marcus Frank Cerny, § 72).

83. Anayasa'nın 13. maddesi vasıtasıyla Anayasa'da yer alan tüm temel hak ve özgürlüklerin sınırlanması hususunda geçerli olan bu denge, özel hayatın gizliliği hakkının sınırlanmasında da gözönünde bulundurulmalıdır. Özel hayatın gizliliği hakkının sınırlanması mümkün olmakla beraber, sınırlamada öngörülen meşru amaç ile sınırlama aracı arasında orantısızlık bulunmamalı, sınırlama ile ulaşılabilecek yarar ile temel hak ve özgürlüğü sınırlanan bireyin kaybı arasında adil bir denge kurulmasına özen gösterilmelidir. Bu noktada, belirtilen ölçütlere riayetle bir sınırlama yapıp

yapılmadığının tespiti için müdahale teşkil ettiği ve özel hayatın gizliliğini ihlal ettiği iddia edilen önlemin temelini oluşturan meşru amaç karşısında, bireye düşen fedakârlığın ağırlığının gözönünde bulundurulması ve söz konusu menfaatler arasında adil bir denge kurulup kurulmadığının belirlenmesi gerekmektedir (Serap Tortuk, § 48, Murat Atılğan, § 39; Marcus Frank Cerny, § 73).

84. Bu alandaki belirleyici mesele; ilgili bireyin ve kamu düzeninin yarışan menfaatleri arasında, kamusal makamların bu konuda kendilerine tanınan takdir alanı içinde adil bir denge kurup kurmadıklarıdır. Özellikle kişisel veriler gibi özel yaşamın en hassas yönlerinin etkilendiği durumlarda, bu dengelemenin titizlikle yapılması ve takdirin gerekçelerinin ilgili kararlara açıkça yansıtılması zaruri olup, başvuruya konu idari ve yargısal uygulamanın yukarıda belirtilen meşru temellere dayandığı açık olmakla birlikte, başvurucunun özel hayatın gizliliği hakkına müdahale teşkil ettiği anlaşılan sınırlamanın belirtilen hakkın özüne dokunarak, onu anlamsız kılacak ölçüde olmaması gerekmektedir.

85. Kamusal makamların izlenen meşru amaçlar bağlamında bir hakkın sınırlandırılması sürecinde takdir yetkisi bulunmakla birlikte, belirtilen takdir yetkisi, her bir vaka özelinde ayrı bir kapsama sahiptir. Güvence altına alınan hakkın veya hukuksal yararın niteliği ve bunun birey bakımından önemi gibi unsurlara bağlı olarak bu yetkinin kapsamı daralmakta veya genişlemekte, yükümlülüklerin türü ve kapsamı her bir olay özelinde farklı değerlendirme yapılmasını gerektirmektedir.

86. Özel hayatın gizliliği hakkına müdahale teşkil eden uygulamaların değerlendirilmesinde de, ilgili idari ve yargısal makamların takdirlerinin gerekçelerini, ilgililerin yargı yoluna müracaat imkânını da etkili şekilde kullanabilmelerini sağlayacak surette ayrıntılı olarak ortaya koymaları gerekmektedir. Söz konusu işlemin bir temel hak üzerinde etki gösterdiği durumlarda, söz konusu tedbirin demokratik bir toplumda gerekli olduğunun ve alınan tedbir ile icra tarzının gözetilen meşru amaç ile orantılı olduğunun ortaya konulması şarttır.

87. Anayasa Mahkemesinin bu noktadaki görevi, kişisel verilerin belirli kamusal amaçlarla tutulması, işlenmesi ve kullanılması hususunun ne şekilde düzenlenmesi gerektiği hususunda bir yargıda bulunmak ve derece mahkemelerinin yerine geçerek ilgili mevzuat hükümlerinin yorumunun bizzat tespiti olmayıp, ilgili anayasal normlar bağlamında, kamusal makamların kendilerine tanınmış olan takdir yetkileri çerçevesinde hareket edip etmediklerinin denetlenmesidir. Anayasa Mahkemesi, derece mahkemelerinin söz konusu mevzuat hükümlerini yorumlayıp uygularken özel hayatın gizliliğine ilişkin bireysel menfaat ve söz konusu sınırlama ile gözetilen kamusal menfaat arasında kurulması gereken dengeyi tespit etmek suretiyle Anayasa'nın 20. maddesindeki güvenceleri

koruyup korumadıklarını belirleme yetkisine sahiptir. Bu nedenle derece mahkemelerince varılan sonucun Anayasa'nın 20.maddesine uygun olup olmadığının, söz konusu uygulamanın özel hayatın gizliliği hakkına yönelik orantılı bir müdahale oluşturup oluşturmadığının karara bağlanması gerekmektedir.

88. Somut başvuru açısından, belirli suçlar nedeniyle hakkında kamu davası açılmış olan şahıslar hakkındaki derdest dava bilgilerinin GBT sistemine kaydının yapıldığı, kamu düzeni ve güvenliğinin temini şeklindeki meşrutemelleri içerdiği anlaşılan uygulama kapsamında söz konusu bilgilerin özellikle yapılan güvenlik taramaları ve güvenlik soruşturmalarında kullanıldığı (bkz. § 19), ilgili bilgilerin toplanma, paylaşım, kullanım ve silinmesine ilişkin hususların ayrıntılı olarak düzenlendiği anlaşılmaktadır.

89. Başvurucunun, yargılandığı suçun Yönerge'nin 9. maddesinin (b) fıkrasında yer alan suçlar arasında olmaması nedeniyle müdahalenin meşru olmadığı yönündeki iddiasında ilgili derece mahkemesince değerlendirildiği, bu suçun ilgili Yönerge'nin 9. maddesi kapsamında yer almadığı ileri sürülmekte ise de aynı nitelikteki suçun yürürlükteki 5237 sayılı Kanun'un 216. maddesinde yer aldığı ve Yönerge'nin belirtilen maddesinde bu suç türüne de yer verildiğinin anlaşıldığının ifade edildiği, bu kapsamda, derece mahkemelerinin söz konusu mevzuat hükümlerini ve maddi olayı yorumlayış şeklinde bir takdir hatasının söz konusu olmadığı görülmektedir.

90. Bunun yanı sıra başvuru tarafından, söz konusu verilerden, toplama, muhafaza ve kullanım hususunda tespit edilen amaç dışında yararlanıldığına ilişkin herhangi bir iddiada da bulunulmadığı anlaşılmaktadır.

91. Yukarıda yer verilen tespitler kapsamında, başvuruya konu müdahalenin demokratik toplumda gerekli ve ölçülü olmadığı söylenemez.

Engin YILDIRIM, Serruh KALELİ, Alparslan ALTAN, Erdal TERCAN ve Hasan Tahsin GÖKCAN bu görüşe katılmamıştır.

V. HÜKÜM

Açıklanan gerekçelerle;

A. Özel hayatın gizliliği hakkının ihlal edildiğine ilişkin iddianın KABUL EDİLEBİLİR OLDUĞUNA OYBİRLİĞİYLE,

B. Anayasa'nın 20. maddesinde güvence altına alınan özel hayatın gizliliği hakkının İHLAL EDİLMEDİĞİNE Engin YILDIRIM, Serruh KALELİ, Alparslan ALTAN, Erdal TERCAN ve Hasan Tahsin GÖKCAN'ın karşıoyları ve OYÇOKLUĞUYLA,

C. Yargılama giderlerinin başvuru üzerinde bırakılmasına OYBİRLİĞİYLE,

D. Kararın bir örneğinin Adalet Bakanlığına GÖNDERİLMESİNE OYBİRLİĞİYLE,

11/5/2016 tarihinde karar verildi.

KARŞIOY GEREKÇESİ

1. Başvurucu, hakkında yürütülen bir ceza yargılaması ile bağlantılı olarak hakkındaki derdest dava bilgisinin Genel Bilgi Toplama (GBT) sistemine kaydedildiği ve bu sistemdeki kayıtların yapılan güvenlik taramaları ve adli işlemlerde kullanılacak nitelikte olduğunu ve bu kişisel verilerin ilgili sistemde tutulması ve belirtilen şekillerde kullanılmasının Anayasa'nın 20. maddesinde güvence altına alınan özel hayatın gizliliği hakkının ihlal edildiğini iddia etmiştir.

2. Hak ya da özgürlüğe bir müdahale olduğunda öncelikle tespiti gereken husus, müdahaleye yetki veren bir kanun hükmünün, yani müdahalenin hukuki bir temelini olup olmadığıdır. Anayasa'nın 20. maddesi kapsamında yapılan bir müdahalenin kanuni bir dayanağının olması zorunludur. İlgili düzenlemede özel sınırlama sebepleri öngörülmemiş olmakla birlikte yasa ile düzenleme hükmüne yer verilmiş ve kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızası ile işlenebileceği belirtilmiştir.

3. Avrupa İnsan Hakları Sözleşmesi (AİHS) kişisel verilerin korunması ile ilgili ayrı bir hüküm içermemekle birlikte, Avrupa İnsan Hakları Mahkemesi (AİHM), bu verilerin özel yaşam alanı içinde yer aldığını kabul ederek, konuyu Sözleşmenin 8. maddesi kapsamında incelemektedir. AİHM, özel hayatı, kişinin kendi hayatını istediği gibi yaşayabileceği bir iç alan ve bunun da ötesinde, başkalarıyla ilişki kurmak ve bu ilişkileri geliştirmek suretiyle özgür olarak kişiliğini oluşturmasını ve geliştirmesini sağlayan daha geniş bir alandan ibaret görmektedir.

4. Bir müdahale hukukilik unsurunu taşıyorsa AİHS 8 (2) fıkrasında yer alan diğer güvence ölçütlerine geçilmeden müdahalenin ilgili maddeye aykırı olduğu sonucuna varılabilmektedir (Fadeyeva/Rusya B. No: 55723/00, 9/6/2005, § 95).

5. Kanunla sınırlama ölçütü, sınırlamanın erişilebilirliğini, öngörülebilirliğini ve kesinliğini ifade etmekte; böylece uygulayıcının keyfi davranışlarının önüne geçtiği gibi kişinin hukuku bilmesine de

yardımcı olmakta, bu yönüyle hukuk güvenliği teminatı sağlamaktadır (Halime Sare Aysal B. No: 2013/1789, 11/11/2015, § 62). Hukuk düzeni bireylere, kamu makamlarına hangi koşullarda ve hangi sınırlar içinde özel yaşama karşı tehlike oluşturabilecek müdahalelerde bulunma yetkisi verdiğini, yeterince açık ifadelerle gösterecek nitelikte olmalı ve bu bağlamda ilgili müdahalenin muhataplarının müdahaleye zemin hazırlayan koşullar ile müdahalenin sonuçları açısından bir öngöründe bulunabilmeleri imkânı tanınmalıdır (§ 64).

6. Kanunun, yeterince ulaşılabilir olması yani vatandaşların belirli bir olaya uygulanabilir nitelikteki hukuk kurallarının varlığı hakkında yeterli bilgiye sahip olabilmesi, ayrıca ilgili normun keyfiliğe karşı uygun bir koruma sağlaması, yetkili makamlara verilen yetkinin genişliğini ve icra edilme biçimlerini yeterli bir netlikte tanımlaması gerekmektedir (Benzer yöndeki AİHM kararları için bkz. Silver ve diğerleri/Birleşik Krallık, B. No: 5947/72, 25/3/1983, §§ 86-88; Malone/Birleşik Krallık, B. No: 8691/79, 2/8/1984, §§ 66-68; Rotaru/Romanya [BD], B. No: 28341/95, 4/5/2000, § 55, Amann/İsviçre B.D. B.No: 27798/95, 16/2/2000 § 76 ve § 80).

7. Bununla birlikte her ihtimale çözüm getiremeyecek olan yasal mevzuatın sağladığı koruma seviyesi büyük ölçüde ilgili metnin düzenlediği alan ve içeriğiyle birlikte muhataplarının niteliği ve sayısı ile yakından bağlantılıdır. Bu nedenle kuralın karmaşık olması ya da belirli ölçülerde soyutluk içermesi ve buna bağlı olarak hukuki yardım ile tam olarak anlaşılabilir hâle gelmesi tek başına hukuken öngörülebilirlik ilkesine aykırı görülemez. Bu kapsamda hak ya da özgürlüğe müdahale eden kural belirli ölçülerdeki takdir alanını elbette uygulayıcıya bırakabilir. Fakat bu takdir alanının sınırlarının da yeterli açıklıkta belirlenmesi ve kuralın asgari bir kesinlik içermesi zaruridir.

8. Bu kapsamda ilgili kanuni düzenlemenin, söz konusu sınırlamaya ilişkin temel çerçeveyi ortaya koymakla birlikte özellikle uygulama koşulları ve usule ilişkin ayrıntıları düzenleyici işlemlere bırakması mümkündür. Ancak bu ihtimalde de söz konusu düzenleyici işlemin, yine muhataplarınca ulaşılabilir olması ve içeriği hakkında ilgilileri yeterince aydınlatacak nitelik ve açıklıkta olması gerekmektedir.

9. Somut başvuru açısından söz konusu gerekliliklere kişisel verilerin kayıt, muhafaza ve kullanımını içeren tedbirlerin kapsamını ve uygulanmasını düzenleyen ve özellikle süre, stoklama, kullanım, üçüncü kişilerin erişimi, verilerin gizliliği bütünlüğü ve imhası konusunda prosedürlere ilişkin muhataplarının yetki aşımı ve keyfiliğe karşı yeteri kadar güvenceye sahip olmalarını sağlayacak açık ve detaylı kuralın belirlenmesinin temel oluşturduğu açıktır.

10. Başvuruya konu idari uygulama ve yargısal sürecin hukuki dayanağını 3152 sayılı Kanunun 13. maddesinin birinci fıkrasının (c) bendi, 2559 sayılı Kanun'un Ek 7. maddesi ve Bilgi Toplama Yönergesinin 9. maddesi oluşturmaktadır.

11. 2559 sayılı Kanun'un Ek 7. maddesine dayanılarak hazırlandığı belirtilen Yönergenin 9 maddesinin (a) fıkrasında, (b) fıkrasında belirtilen suçları işlemiş ve yakalanmış olan sanıklar ile bazı suçlardan dolayı yargılanan kişiler için de suç türüne uygun bilgi formu doldurulacağı ve yakalandı kaydı düşmek suretiyle sistemde muhafaza edileceği belirtilmiştir.

12. İlgili kanunlar hangi kişilere ait ne tür bilgilerin, hangi şartlarda toplanabileceği, ne surette kullanılabilceği ve ne kadar süreyle saklanabileceğine dair bir açıklık ve belirlilik içermemektedir.

13. Hangi kişilere ait ne tür bilgilerin hangi şartlarda toplanabileceği, hangi amaçlarla ne şekilde kullanılabilceği ve ne kadar süreyle saklanabileceği hususunda ayrıntılı düzenlemeler içeren Yönerge hizmete özeldir ve kamuya açık değildir. Yönergenin yayınlanmamış olduğu dikkate alındığında söz konusu düzenlemenin kişilerin belirli bir olaya uygulanabilir nitelikteki hukuk kurallarının varlığı hakkında yeterli bilgiye sahip olmasını sağlayacak surette ulaşılabilir olma niteliği taşımadığı anlaşılmaktadır.

14. Öngörülebilirlik ve belirlilik unsurlarının değerlendirmesi bakımından ilgili düzenleme, bir hakka dönük yapılan müdahalelerin incelenmesinde ilk aşama olan kanunilik testini geçememektedir.

15. Sonuç olarak, başvuru kişinin kişisel verilerinin GBT sisteminde tutulmasının herkese açık, öngörülebilir ve belirlilik unsurlarını içeren kanuni bir dayanağı olmadığından, Anayasanın 20. maddesinde güvence altına alınan özel hayatın gizliliği hakkının ihlal edildiği kanaatine varılmıştır.

Başkanvekili

Engin YILDIRIM

KARŞIOY GEREKÇESİ

1. Başvuru, aranan kişilerden olmamasına rağmen başvuru hakkındaki derdest ceza yargılamasına ilişkin bilginin Genel Bilgi Toplama (GBT) sistemine kaydedilmesi ve ilgili kaydın silinmesi hususunda idareye yapılan başvuru ile bu hususta açılan davanın mevzuata aykırı olarak reddedilmesi nedeniyle özel hayatın gizliliği hakkının ihlali iddiasına ilişkindir.

2. Çoğunluk kararıyla, belirli suçlar nedeniyle hakkında kamu davası açılmış olan şahıslar hakkındaki derdest dava bilgilerinin GBT sistemine kaydının yapılması uygulamasının kamu düzeni ve

güvenliğinin temini şeklindeki meşru temelleri içerdiği, uygulama kapsamında söz konusu bilgilerin özellikle yapılan güvenlik taramaları ve güvenlik soruşturmalarında kullanıldığı, ilgili bilgilerin toplanma, paylaşım, kullanım ve silinmesine ilişkin hususların ayrıntılı olarak düzenlendiği; başvurucunun, yargılandığı suçun Yönerge'nin 9. maddesinin (b) fıkrasında yer alan suçlar arasında olmaması nedeniyle müdahalenin meşru olmadığı yönündeki iddiasının ilgili derece mahkemesince değerlendirildiği, bu suçun ilgili Yönerge'nin 9. maddesi kapsamında yer almadığı ileri sürülmekte ise de, aynı nitelikteki suçun yürürlükteki 5237 sayılı Kanun'un 216. maddesinde yer aldığı ve Yönerge'nin belirtilen maddesinde bu suç türüne de yer verildiğinin anlaşıldığının ifade edildiği, bu kapsamda, derece mahkemelerinin söz konusu mevzuat hükümlerini ve maddi olayı yorumlayış şeklinde bir takdir hatasının söz konusu olmadığı, bunun yanı sıra başvuru tarafından, söz konusu verilerden, toplama, muhafaza ve kullanım hususunda tespit edilen amaç dışında yararlanıldığına ilişkin herhangi bir iddiada da bulunulmadığı belirtilerek özel hayatın gizliliği hakkının ihlal edilmediği sonucuna varılmıştır.

3. Başvurucu hakkında 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu'nun 7. maddesine muhalefet iddiasıyla iddianame tanzim edilmiş olup, Van 4. Ağır Ceza Mahkemesinin 17/3/2008 tarihli ve E.2004/596, K.2007/333 sayılı kararı ile, başvurucunun 5237 sayılı Kanun'un 215. maddesi uyarınca cezalandırılmasına karar verilmiş ve karar temyiz edilmeksizin 20/5/2008 tarihinde kesinleşmiştir.

4. Belirtilen yargısal süreç devam ederken, Van Devlet Güvenlik Mahkemesi Cumhuriyet Başsavcılığının 16/10/2003 tarihli yazısı ile, başvuru hakkında bölücü terör örgütüne yardım ve yataklık etmek suçu kapsamında soruşturma yapılmasının istenilmesi üzerine, Van Emniyet Müdürlüğüne, İçişleri Bakanlığı Kaçakçılık, İstihbarat, Harekat ve Bilgi Toplama Daire Başkanlığı Bilgi Toplama Yönergesi (Bilgi Toplama Yönergesi) uyarınca başvurucuya ait Örnek No 1 Bilgi Formu tanzim edilerek GBT sistemi kapsamında tasnife alınmıştır.

5. Başvurucunun 24/11/2005 tarihli dilekçe ile, GBT sisteminde yer alan şahsına ait bilgilerin silinmesi talebiyle idareye yaptığı başvuru, hakkındaki yargılamanın ilgili Yönerge'nin 9. maddesinin (b) fıkrasında belirtilen suçlara ilişkin olduğu ve başvuru hakkındaki söz konusu kaydın, ilgili davanın beraat veya dava zamanaşımı nedeniyle ortadan kaldırılması halinde iptalinin mümkün olduğu belirtilerek reddedilmiştir.

6. Başvurucu tarafından 6/1/2006 tarihinde idarenin red işleminin iptali istemiyle açılan dava, Ankara 1. İdare Mahkemesinin 22/3/2007 tarihli ve E.2006/44, K.2007/683 sayılı kararı ile reddedilmiş ve ret gerekçesi olarak; 14/2/1985 tarihli ve 3152 sayılı İçişleri Bakanlığı Teşkilat ve Görevleri Hakkında

Kanun'un 13. maddesinin birinci fıkrasının (c) bendi, 4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Selahiyeti Kanunu'nun Ek 7. maddesi ve Bilgi Toplama Yönergesi'nin 9. maddesinde yer alan düzenlemelere değinilmiş, davacı tarafından 3713 sayılı Kanun'un 7/2 maddesine muhalefet suçundan ceza davası açıldığı, ancak Van 4. Ağır Ceza Mahkemesinin 29/9/2004 tarihli kararı ile suç vasfının değışerek olay tarihinde yürürlükte olan Türk Ceza Kanunu'nun 312. maddesinin 2. fıkrasında yer alan suç kapsamında yargılama yapılması gerektiği gerekçesiyle görevsizlik kararı verildiği ve bu suçun ilgili Yönerge'nin 9. maddesi kapsamında yer almadığı ileri sürülmekte ise de, aynı nitelikteki suçun yürürlükteki Türk Ceza Kanunu'nun 216. maddesinde yer aldığı ve Yönerge'nin belirtilen maddesinde bu suç türüne de yer verildiği anlaşıldığından, anılan iddiada yerindelik görülmediği belirtilerek, 2559 sayılı Kanun'un Ek 7. maddesine dayanılarak çıkarılan Yönerge'nin 9. maddesinin (b) fıkrası uyarınca, anılan maddede belirtilen suç türleri için bilgi kaydı tutulmasına ilişkin işlemde hukuka aykırılık görülmediği ifade edilmiştir.

7. Başvurucu, aranan şahıslardan olmamasına rağmen hakkında yürütülen derdest ceza yargılamasına ilişkin bilginin GBT sistemine kaydedildiğini, belirtilen kaydın silinmesi hususunda idareye yaptığı başvurunun ve bu hususta açtığı davanın, ilgili mevzuat hükümlerinin doğru şekilde yorumlanmaması nedeniyle reddedildiğini, belirtilen uygulamaya temel alınan Bilgi Toplama Yönergesinin dayandığı Kanun ile kolluk görevlilerine verilen yetkinin amacına aykırı şekilde genişletilerek, idarenin düzenleyici işlem yapma yetkisinin aşıldığını ve yasal dayanaktan yoksun idari bir pratik oluşturulduğunu, yargılandığı suçun Bilgi Toplama Yönergesinin 9. maddesinin (b) fıkrasında yer alan suçlar arasında olmadığını, belirtilen bilgilerin ne kadar süreyle saklı tutulacağını ve silinip silinmeyeceğinin belirsiz olduğunu, ayrıca derdest yargılama bilgisinin mahkumiyet kaydı gibi işlem görmesi nedeniyle yargı kararı olmaksızın suçlu olarak addedildiğini belirterek, Anayasa'nın 20. maddesinde tanımlanan özel hayatın gizliliği hakkının ve 38. maddesinde tanımlanan masumiyet karinesinin ihlal edildiğini iddia etmiş, başvurucunun iddiaları Anayasa'nın 20. maddesinde tanımlanan özel hayatın gizliliği hakkı kapsamında incelenmiştir.

8. Çoğunluk gerekçesinde kanunilik başlığı altındaki 71 ila 78. paragraflarda da ifade edildiği üzere, Anayasa'nın 20. maddesinde, herkesin özel hayatına saygı gösterilmesi hakkına sahip olduğu ve özel hayatın gizliliğine dokunulamayacağı belirtilmektedir. Bireyin kişisel verilerinin ve bu verilerin korunmasına dair hukuksal menfaatinin de özel yaşamı kapsamında olduğu açıktır.

9. Mahremiyet hakkı ve bu alana ilişkin bilgilerin gizliliğinin korunması Anayasa Mahkemesi tarafından da, Anayasa'nın 20. maddesi kapsamında değerlendirilmektedir. Buna göre, özel yaşama saygı hakkı kapsamında korunan hukuksal çıkarlardan biri de bireyin mahremiyet hakkıdır. Ancak

mahremiyet hakkı sadece yalnız bırakılma hakkından ibaret olmayıp, bu hak bireyin kendisi hakkındaki bilgileri kontrol edebilme hukuksal çıkarını da kapsamaktadır. Bireyin kendisine ilişkin herhangi bir bilginin, kendi rızası olmaksızın açıklanmaması, yayılmaması, bu bilgilere başkaları tarafından ulaşılamaması ve rızası hilafına kullanılamaması, kısaca bu bilgilerin mahrem kalması konusunda menfaati bulunmaktadır. Bu husus, bireyin kendisi hakkındaki bilgilerin geleceğini belirleme hakkına işaret etmektedir (AYM, E. 2009/1, K. 2011/82, K.T. 18/5/2011; E. 1986/24, K. 1987/7, K.T. 31/3/1987).

10. Bireyin kendisi hakkındaki bilgiyi kontrol edebilme hakkının konusunu oluşturan “bilgi” kavramının ne anlama geldiğinin, başka bir ifade ile özel hayatın korunması hakkının güvence kapsamında yer alan bilgilerin ne olduğunun tespiti önemlidir.

11. Başvuruya konu olayda, başvuru hakkındaki derdest ceza yargılaması bağlamındaki verilerin GBT sistemine kaydedildiği görülmekle, başvuruyla ilgili olarak resmi makamların muhafaza ettikleri söz konusu kişisel bilgilerin, özel hayata saygı hakkı anlamında kişisel nitelikli veriler olduğu, zira kimliği belirlenmiş ya da belirlenebilecek kişilerle ilgili olduğu anlaşılmaktadır. Bu kapsamda GBT sisteminde yer alan söz konusu bilgilerin, başvuruyla ilgili olduğu tartışmasızdır.

12. Bir kişinin, özel yaşamına ilişkin verilerin kaydedilmesi, özel hayata saygı hakkı anlamında bir müdahale oluşturmaktadır. Kaydedilen bilgilerin, daha sonra kullanılmış olup olmamasının bir önemi yoktur. Başvuruya konu olayda da başvuru hakkında yürütülen bir ceza yargılaması ile bağlantılı olarak hakkındaki derdest dava bilgisinin bilgi toplama sistemine kaydedildiği ve bu sistemdeki kayıtların yapılan güvenlik taramaları ve adli işlemlerde kullanılacak nitelikte olduğu görülmekle, söz konusu kişisel verilerin ilgili sistemde tutulması ve belirtilen şekillerde kullanılmasının, Anayasa'nın 20. maddesinde güvence altına alınan özel hayatın gizliliği hakkına bir müdahale oluşturduğu açıktır. Zira Anayasada kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızası ile işlenebileceği belirtilmiştir.

13. Anayasa'nın “Temel hak ve hürriyetlerin sınırlanması” kenar başlıklı 13. maddesinde temel hak ve hürriyetlerin, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği, bu sınırlamaların, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacağı belirtilmiştir.

14. Hak ve özgürlüklerin kanunla sınırlanması ölçütü anayasa yargısında önemli bir yere sahiptir. Hak ya da özgürlüğe bir müdahale söz konusu olduğunda öncelikle tespiti gereken husus,

müdahaleye yetki veren bir kanun hükmünün, yani müdahalenin hukuki bir temelini mevcut olup olmadığıdır (Sevim Akat Eşki, § 36).

15. Sözleşme'nin lafzı ve AİHM içtihadı uyarınca da, Sözleşme'nin 8. maddesi kapsamında yapılacak bir müdahalenin meşruluğu, öncelikle söz konusu müdahalenin yasa uyarınca gerçekleştirilmesine bağlı tutulmuş olup, müdahalenin hukukîlik unsurunu taşımadığının tespiti halinde, Sözleşmenin 8. maddesinin (2) numaralı fıkrasında yer alan diğer güvence ölçütleri tetkik edilmeksizin, müdahalenin ilgili maddeye aykırı olduğu sonucuna ulaşılmaktadır (Bkz. Fadeyeva/Rusya, B. No: 55723/00, 9/6/2005, § 95; Bykov/Rusya, B. No: 4378/02, 10/3/2009, §82).

16. Anayasa'nın 20. maddesi kapsamında yapılan bir müdahalenin yasallık şartını sağladığının kabulü için de, müdahalenin kanuni bir dayanağının bulunması zorunludur. Bununla birlikte, temel hak ve hürriyetlerin sınırlandırılmasına ilişkin kanunların şeklen var olması yeterli değildir. Yasallık ölçütü aynı zamanda maddi bir içeriği de gerektirmekte olup, bu noktada yasanın niteliği önem kazanmaktadır. Yasayla sınırlama ölçütü, sınırlamanın erişilebilirliğini, öngörülebilirliğini ve kesinliğini ifade etmekte, böylece uygulayıcının keyfi davranışlarının önüne geçtiği gibi kişinin hukuku bilmesine de yardımcı olmakta, bu yönüyle hukuk güvenliği güvencesi sağlamaktadır (Halime Sare Aysal, B.No. 2013/1789, 11/11/2015, § 62).

17. Kanunun, bu gerekliliklere uygun olduğunun söylenebilmesi için, yeterince ulaşılabilir olması, yani vatandaşların belirli bir olaya uygulanabilir nitelikteki hukuk kurallarının varlığı hakkında yeterli bilgiye sahip olabilmesi, ayrıca ilgili normun keyfiliğe karşı uygun bir koruma sağlaması, yeterli bir netlikte, yetkili makamlara verilen yetkinin genişliğini ve icra edilme biçimlerini tanımlaması gerekmektedir (Halime Sare Aysal, § 63; Benzer yöndeki AİHM kararları için bkz. Silver ve Diğerleri/Birleşik Krallık, B.No: 5947/72, 25/3/1983, § 86-88; Malone/Birleşik Krallık, 2/8/1984, § 66-68; Rotaru/Romanya, § 55).

18. Somut başvuru açısından ise, söz konusu gerekliliklere, kişisel verilerin kayıt, muhafaza ve kullanımını içeren tedbirlerin kapsamını ve uygulanmasını düzenleyen ve özellikle, süre, stoklama, kullanım, üçüncü kişilerin erişimi, verilerin gizliliği, bütünlüğü ve imhası konusundaki prosedürlere ilişkin, muhataplarının yetki aşımı ve keyfiliğe karşı yeteri kadar güvenceye sahip olmalarını sağlayacak açık ve detaylı kuralların belirlenmesinin temel oluşturduğu açıktır.

19. Kanunun kendisi, beraberinde getireceği idari pratiğin dışında, yetkili makamlara bırakılan takdir yetkisinin kapsamını, söz konusu işlemin meşru amacını da göz önünde tutarak, keyfi müdahalelere karşı bireyi korumak için yeterince açık bir şekilde göstermelidir. Hukuk sistemi vatandaşlara, kamu makamlarına hangi koşullarda ve hangi sınırlar içinde kişisel verileri konu alan ve potansiyel olarak

özel yaşama karşı tehlike oluşturabilecek müdahalelerde bulunma yetkisi verdiğini, yeterince açık ifadelerle gösterecek nitelikte olmalıdır (Halime Sare Aysal,§ 64).

20. Bu kapsamda ilgili sisteme bilgilerin girilmesi, müdahaleye temel oluşturan meşru amaçları taşıma şartına bağlı olmalı ve söz konusu yasal düzenleme, hangi bilgilerin kayıt altına alınabileceği, hangi yetkililere iletilebileceği, böyle bir iletimin hangi koşullarda mümkün olabileceği ve bilginin ilgili makamlara iletilmesi hususunda izlenecek usul konusunda açık ve ayrıntılı hükümler içermelidir. Söz konusu sisteme ilişkin düzenleme, bilgi toplama, kaydetme ve ilgili makamlarla paylaşma veya sair şekilde kullanma konusunda, yetkili makamlara tanıdığı takdir yetkisinin kullanılma tarzı ve alanı bakımından, vatandaşlara yeterince öngörülebilir bulunma olanağı sağlamak durumundadır.

21. Anayasa Mahkemesi idareye keyfi uygulamalara meydan verebilecek çok geniş bir takdir yetkisi tanınmasını birçok kararında Anayasaya aykırı görmüştür. Bu kararlarda Mahkeme, kanunun şeklen var olmasını yeterli görmemekte, kanunun niteliğini de araştırmakta ve bu bağlamda, bir sınırlamanın nerede başlayıp nerede bittiğinin belirtilmemesi durumunda, amacı aşan, demokratik toplum düzeninin gerekleriyle bağdaşmayan, içeriğinin takdiri yönetime bırakılmış sakıncalı sınırlamalar getirilmiş olacağı; içeriğinin belirlenmesi yönetimin görüşüne bırakılan sınırlamanın yasa ile konulduğundan söz edilemeyeceği; hukuk devletinin hukuk güvenliği ilkesinin belirliliği de gerektirdiği ve belirlilik ilkesinin, ilgili yükümlülüğün hem kişiler hem de idare yönünden belirli ve kesin olmasını, yasa kuralının, ilgili kişilerin mevcut şartlar altında belirli bir işlemin ne tür sonuçlar doğurabileceğini makul bir düzeyde öngörmelerini mümkün kılacak şekilde düzenlenmesini gerektirdiği ve yasa koyucunun temel ilkeleri koymadan, genel çerçeveyi çizmeden yürütmeye yetki vermemesi, sınırsız ve belirsiz bir alanı yönetimin düzenlemesine bırakmaması gerektiği belirtilmektedir (E. 1984/14, K. 1985/7, K.T. 13.06.1985; E. 1987/16, K. 1988/8, K.T. 19.04.1988; E. 2010/7, K. 2011/172, K.T. 22.12.2011).

22. AİHM kararlarında da özellikle ceza davaları kapsamında, resmi makamlar tarafından kişisel nitelikli verilerin depolanması, muhafaza edilmesi ve kullanılmasıyla ilgili sorunlara eğilmiş ve bu kapsamda yapılan değerlendirmelerde, uygulayıcıya sınırları belirsiz müdahale yetkisi veren hukuki düzenlemelerin hukuk devleti ilkesiyle de çatıştığı vurgulanarak, keyfi müdahaleleri önlemek için hukuk kuralının verdiği yetkinin amacını ve kullanım biçimini yeterli açıklıkta belirtmiş olması zorunluluğuna işaret edilmiştir (Al Nashif/Bulgaristan, B. No:50963/99, 20/6/2002, §§ 119-124).

23. Bununla birlikte, her ihtimale çözüm getiremeyecek olan yasal mevzuatın gereken koruma seviyesi, büyük ölçüde, ilgili metnin düzenlediği alan ve içeriğiyle birlikte, muhataplarının niteliği ve

sayısıyla yakından bağlantılıdır. Bu nedenle, kuralın karmaşık olması ya da belirli ölçülerde soyutluk içermesi ve bu nedenle hukuki yardım ile tam olarak anlaşılabilir hale gelmesi, tek başına hukuken öngörülebilirlik ilkesine aykırı görülemez. Bu kapsamda hak ya da özgürlüğe müdahale eden kural belirli ölçülerdeki takdir alanını elbette uygulayıcıya sunabilir. Fakat bu takdir alanının sınırlarının da yeterli açıklıkta belirlenmesi ve kuralın asgari bir kesinlik içermesi zaruridir (Halime Sare Aysal, § 65).

24. Bu kapsamda ilgili kanuni düzenlemenin, söz konusu sınırlamaya ilişkin temel çerçeveyi ortaya koymakla birlikte, özellikle uygulama koşulları ve prosedürel ayrıntıları düzenleyici işlemlere bırakması mümkündür. Ancak bu ihtimalde de söz konusu düzenleyici işlemin, yine muhataplarınca ulaşılabilir olması ve içeriği hakkında ilgilileri yeterince aydınlatacak nitelik ve açıklıkta olması gerekmektedir (Halime Sare Aysal, § 66).

25. Başvuruya konu idari uygulama ve yargısal sürecin, 3152 sayılı Kanun'un 13. maddesinin birinci fıkrasının (c) bendi, 2559 sayılı Kanun'un Ek 7. maddesi ve Bilgi Toplama Yönergesi'nin 9. maddesi temelinde yürütüldüğü anlaşılmaktadır.

26. İlgili idari ve yargısal kararlarda söz konusu uygulamanın yasal temeli olarak gösterilen 2559 sayılı Kanun'un 7. maddesine dayanılarak hazırlandığı belirtilen Yönerge'nin 9. maddesinin (a) fıkrasında, maddenin (b) fıkrasında belirtilen suçları işlemiş ve yakalanmış olan sanıklar için de suç türüne uygun bilgi formu doldurulacağı ve yakalandığı kaydı düşülmek suretiyle sistemde muhafaza edileceği ifade edilmektedir. Yönerge'nin 10. maddesinin (b) fıkrasında, güvenlik kuvvetlerinin kendi sorumluluk alanında el koydukları olaylarda; suç işleyen şahsın bilgisayar sorgulamasını yapacağı, geçmişte işledikleri suç kayıtları varsa tespit edeceği ve soruşturma evrakına yazacağı; aynı maddenin (b) fıkrasının (2) numaralı bendinin (b) alt bendinde ise, şüpheli hakkında Cumhuriyet Başsavcılığınca iddianame hazırlanıp mahkemece iddianamenin kabulünden sonra mahkemenin "Esas" sayısı alınmak suretiyle şahıs bilgi formu açılarak, Bilgi Toplama Programına girişinin, programda "Hakkında İşlem Yapılacaklar" ibaresiyle şüphelinin kaydı mevcutsa kayıt üzerinde düzeltme işlemi yapılacağı belirtilmektedir. Kayıtların silinmesi hususunda ise 16. maddenin (b) fıkrasında, Yönerge'nin 9. maddesinin (b) fıkrasında yazılı suç sayılan fiilleri işleyenler hakkında adli makamlarca, beraat, ceza verilmesine yer olmadığı, davanın düşmesi veya dava zaman aşımı nedeniyle davanın ortadan kaldırılmasına karar verilmiş ve kararın kesinleşmiş olması halinde bilgi formlarının iptal edileceği belirtilmekle birlikte, Yönerge'nin 4. maddesinde, Yönerge'nin 9. maddesinin (b) fıkrası kapsamına girmeyen suçlardan açılan bilgi formlarının şahısların yakalanmaları halinde tasniften çıkarılarak imha edileceği, 9. maddesinin (b) fıkrası kapsamına giren

suçlar için açılan bilgi formlarının ise iptal koşulları oluştuğunda tasniften çıkarılarak iptal evrakı ekinde arşive alınacağı düzenlenmektedir.

27. Söz konusu düzenlemeler karşısında, hakkında belirli suçlardan ceza kovuşturması devam eden kişilere ait dava bilgilerinin ilgili sisteme kaydının yapılacağı, belirli amaçlarla kullanılacağı, söz konusu yargılamanın beraat, ceza verilmesine yer olmadığı, davanın düşmesi veya davanın ortadan kaldırılması kararlarıyla sonuçlanması durumunda bilgi formlarının tasniften çıkarılarak iptal edileceği, ancak ilgili kayıtların iptal evrakı ekinde arşivde muhafaza edilmeye devam edileceği anlaşılmaktadır.

28. İlgili Yönerge uyarınca genel bilgi toplama sisteminde kaydı tutulacak unsurlar, kişileri, bazı belgeleri ve araçları kapsamaktadır. Hakkında bilgi tutulacak kişilerin ise, Yönerge'nin amacını düzenleyen 1. maddesi uyarınca, suç işlemesi sebebiyle aranmasına karar verilen, kaybolan, yakalansalar dahi bazı suçları işlemiş olan ve kamu haklarından yararlanmaları konusunda sınırlama getirilen kişiler olduğu anlaşılmaktadır.

29. Yönerge'nin 7. maddesi ve 9. maddesinin (a) fıkrası hükümlerine göre; hakkında arama kararı bulunmadığı veya yakalanmış olduğu halde belirli bazı suçlardan dolayı yargılanan kişiler hakkında da genel bilgi toplama programına bilgi kaydedilebilmektedir. Bu suçların hangileri olduğu, Yönerge'nin 9. maddesinin (b) fıkrasında gösterilmektedir.

30. Yönerge'nin hangi normlara dayalı olarak düzenlendiği, "Kanuni dayanak" başlıklı 3. maddesinde açıklanmıştır. Buna göre söz konusu Yönerge, 3152 sayılı Kanun'un 13. maddesinin birinci fıkrasının (c) bendi ve 33. maddesi, 2559 sayılı Kanun'un Ek 7. maddesi ile Jandarma Teşkilatı Görev ve Yetkileri Yönetmeliği'nin 42. maddesinin birinci fıkrasının (e) ve (f) bendine dayanılarak hazırlanmıştır.

31. 3152 sayılı Kanun'un 13. maddesinin birinci fıkrasının (c) bendi, İçişleri Bakanlığı Kaçakçılık İstihbarat, Harekât ve Bilgi Toplama Dairesi Başkanlığının görevlerini düzenlemekte ve suç işleyip ele geçmeyen kişilerin, çalınan veya kaybedilen motorlu taşıtların, ateşli silahların, kimliği ispata yarayan her türlü belgelerin kayıtlarını tutarak güvenlik kuvvetlerine bildirmek, görevli kuruluşlarla ilgili kuvvetleri arasında koordinasyon sağlamak görevini, ilgili birimin görevleri arasında saymaktadır. Bu yönüyle, kişilere ilişkin kayıtların tutulmasına ilişkin yetkinin, suç işleyip ele geçmeyen kişiler ile sınırlı olarak öngörüldüğü anlaşılmaktadır. Bu kapsamda, ilgili Yönergeye dayanak olarak gösterilen mezkur kanun maddesinin, Yönergenin "yakalansalar dahi bazı suçları işlemiş olan kişiler" hakkında kayıt tutulacağı şeklindeki düzenlemesini ve bu yöndeki uygulamayı temellendirmediği görülmektedir. 3152 sayılı Kanun'un 33. maddesinin ise, yerine getirmekle

yükümlü olduğu hizmetleri idari metinlerle düzenleme konusunda İçişleri Bakanlığını yetkilendirdiği anlaşılmaktadır.

32. Yönergenin dayanakları arasında gösterilen ve Çoğunluk tarafından müdahalenin kanuni dayanağı olarak kabul edilen 2559 sayılı Kanun'un 7. maddesinde ise, polisin Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri alacağı, emniyet ve asayişini sağlamak üzere, ülke seviyesinde istihbarat faaliyetlerinde bulunacağı, bu amaçla bilgi toplayacağı, değerlendireceği, yetkili mercilere veya kullanma alanına ulaştıracağı, Devletin diğer istihbarat kuruluşlarıyla işbirliği yapacağı düzenlemesine yer verildiği, bu kapsamda genel nitelikte istihbarat yapma yetki ve görevini düzenlediği anlaşılmaktadır. Her bir normun, hiyerarşik olarak üstünde bulunan normlara uygun olması, yerleşmiş bir hukuk kuralıdır. Yönetmelik altı diğer düzenlemeler gibi yönergeler de, öncelikle kanunların uygulanmasında idareye yol göstermek üzere çıkarılır. Bu itibarla bir yönerge, ilgili Kanun hükmünün belirlediği çerçevede kalmak ve dayandığı sınırları aşmamak zorundadır. Bu kapsamda, 2559 sayılı Kanun'un 7. maddesinde yer alan düzenlemenin, belirli suçlardan yargılanan kişiler hakkındaki derdest dava bilgilerinin depolanması ve kullanılması şeklindeki başvuru konusu uygulamaya mesnet olduğu kabul edilse dahi, düzenlemenin hangi kişilere ait ne tür bilgilerin hangi koşullarda toplanabileceği, söz konusu bilgilerin hangi amaçlarla, ne surette kullanılabilmesi ve ne kadar süreyle saklanabileceğine dair bir belirleme içermediği görülmektedir. Bu nedenle sözkonusu düzenlemenin bu haliyle başvuruya konu müdahalenin kanuni temelini oluşturduğu söylenemez. Yönergenin dayanakları arasında gösterilen bir diğer düzenleme olan Jandarma Teşkilatı Görev ve Yetkileri Yönetmeliği'nin 42. maddesinin birinci fıkrasının (e) ve (f) bendi açısından da aynı değerlendirmeler geçerlidir.

33. Yukarıda yer verilen ilgili düzenlemelerin, söz konusu sınırlamaya ilişkin temel çerçeveyi ortaya koyarak, uygulama koşulları ve prosedürel ayrıntıları düzenleyici işlemlere bırakması mümkün olmakla birlikte, bu ihtimalde de ilgili alt mevzuatın, yine muhataplarınca ulaşılabilir olması ve içeriği hakkında ilgilileri yeterince aydınlatacak nitelik ve açıklıkta olması zorunludur. Öngörülebilirlik, belirlilik unsurlarının değerlendirilebilmesi açısından da, ilgili düzenlemenin öncelikle muhataplarınca ulaşılabilir nitelikte olması gerektiği tartışmasızdır.

34. Bundan başka ayrıca, konuyla bağlantılı olarak şu hususun da belirtilmesi gerekir: İçişleri Bakanlığı Kaçakçılık İstihbarat, Harekat ve Bilgi Toplama Dairesi Başkanlığının Anayasa Mahkemesine hitaben gönderdiği 11/6/2015 tarihli ve 1962 sayılı yazıda; Bilgi Toplama Yönergesinin, 3152 sayılı Kanun'un 13. maddesinin birinci fıkrasının (c) bendi ve 33. maddesi, 2559 sayılı Kanun'un

Ek 7 maddesi ve Jandarma Teşkilatı Görev ve Yetkileri Yönetmeliği'nin 42. maddesinin birinci fıkrasının (f) bendine dayanılarak hazırlandığı, ancak söz konusu Yönergenin "hizmete özel" dereceli olması nedeniyle kamuya açık olmadığı belirtilmiştir. Bu kapsamda, belirtilen yazı ekinde gönderilen ve başvuruya konu uygulamaya temel oluşturan Yönerge'nin, hangi kişilere ait ne tür bilgilerin hangi koşullarda toplanabileceği, söz konusu bilgilerin hangi amaçlarla, ne surette kullanılabilmesi ve ne kadar süreyle saklanabileceğine dair ayrıntılı düzenlemeler içerdiği görülmekle birlikte, ilgili Yönerge'nin yayınlanmamış olduğu nazara alındığında, söz konusu düzenlemenin kişilerin belirli bir olaya uygulanabilir nitelikteki hukuk kurallarının varlığı hakkında yeterli bilgiye sahip olabilmesini sağlayacak surette ulaşılabilir olma niteliğini taşımadığı anlaşılmaktadır.

35. Bu bağlamda başvurucunun, söz konusu uygulamanın yasal temeli olmadığı ve idari düzenlemelerle bir sınırlama öngörüldüğü noktasındaki itirazlarının ve yargılandığı suçun Yönerge'nin 9. maddesinin (b) fıkrasında yer alan suçlar arasında olmaması nedeniyle müdahalenin meşru olmadığı yönündeki iddiasının da yargı mercilerince dikkate alınmadığı anlaşılmaktadır.

36. İlgili yargı kararlarına temel alınan Yönerge'nin, ulaşılabilirlik unsurunu da taşımadığı görülmekle, başvuruya konu müdahalenin bu açıdan da kanunilik şartını sağlamadığı anlaşılmaktadır.

37. Açıklanan nedenlerle, başvurucunun Anayasa'nın 20. maddesinde güvence altına alınan özel hayatın gizliliği hakkının ihlal edildiğine karar verilmesi gerektiğini düşündüğümüzden, çoğunluğun aksi yönündeki kararına katılmadık.

Üye

Serruh KALELİ

Üye

Alparslan ALTAN

Üye

Erdal TERCAN

KARŞIOY GEREKÇESİ

Başvurucu hakkında, yargılandığı suçla ilgili olarak Van Emniyet Müdürlüğü tarafından, Bilgi Toplama Yönergesi kapsamında bilgi formu düzenlenmiştir. Başvurucunun GBT sisteminde şahsiyle

ilgili kaydın silinmesi talebi idare tarafından kabul edilmemiş, bu işleme karşı idare mahkemesinde açtığı iptal davası da reddedilmiş ve karar kanun yolu süreci sonunda da onanarak kesinleşmiştir. Başvurucu, kanuna aykırı bu uygulama nedeniyle özel hayatının gizliliğinin ihlal edildiğini ve masumiyet karinesinden yararlanma hakkının ihlal edildiğini ileri sürmektedir.

Kişiler hakkında bir suçu işlediğine veya bir suç şüphesiyle arandığına ilişkin kayıt tutulması, kişisel veri niteliğinde bulunmaktadır. Anayasa'nın 20/3. maddesi uyarınca;

“Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak, kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.”

Görüldüğü üzere kişisel veriler Anayasada özel hayatın gizliliği kapsamında ele alınmış ve hukuken bu verilerin kaydedilmesinin gerektiği hallerde de özel hayatın korunması amacıyla bazı güvencelerin sağlanması gerektiği ifade edilmiştir. Bu anlamda, kişisel verilerin toplanması ve kayda alınması işlemleri ancak kanunla düzenlenmeli ve bu düzenlemelerin de Anayasada belirtilen güvenceleri temin etmesi gerekmektedir.

3152 sayılı Kanun'un 13. maddesinde yer alan, suç işleyip ele geçmeyen kişilerle ilgili kayıt tutma yetkisinin somut olaya ilişkin olarak kanuni temel olamayacağı hususu çoğunluk gerekçesinde de kabul edilmektedir. Çoğunluk kararında kanuni dayanak olarak gösterilen 2559 sayılı Kanun'un Ek 7. maddesi hükmü de Anayasa'nın 20/3. maddesinde belirtilen güvenceleri kapsamadığı gibi, bu hususların kanun niteliğinde olmayan tali mevzuatla ilk kez düzenlenerek uygulanması da hukuka uygun bulunmamaktadır. Sözü edilen kanun hükmünde kimler hakkında hangi durumda ne tür bilgilerin kaydedileceği, bunların ne maksatla kullanılacağı, kayıtların ne kadar süreyle saklanabileceği gibi hususlar yer almamaktadır. 2559 sayılı Kanun'un Ek 7. maddesinde bahsi geçen “emniyet ve asayiş sağlamaya üzere ülke seviyesinde istihbarat faaliyetlerinde bulunmak” ibaresi ise önleyici kolluğun alması gereken tedbirler kapsamındaki istihbarat yetkisiyle ilgili olup, belirli bir kişiyle ilgili olarak işlenmiş bir suç kaydının (kişisel verinin) bu kapsamda değerlendirilmesi mümkün görülmemektedir. Bu şekliyle anılan kanun hükümlerinin Anayasa'nın 20/3 ve 13. maddelerine aykırı bulunduğu anlaşılmaktadır.

Diğer taraftan, kanunun açıkça yetki vermediği durumda bir kişi hakkındaki suç isnadının adli kayıtlardan ve yargılama süreçlerinden bağımsız olarak kamu makamlarının kayıtlarında süresiz bir

veri olarak tutulmasının Anayasa'nın 38. maddesinde düzenlenen masumiyet karinesini de ihlal edebileceđi ve başvurunun bu yönden de incelenmesi gerektiđi düşünölmelidir.

Açıklanan nedenlerle, başvurucunun kişisel hakkına yapılan müdahalenin kanuna uygun olmaması nedeniyle özel hayatın gizliliđinin ihlal edildiđi görüşünde olduğumdan, ihlal bulunmadığı yönündeki çoğunluk görüşüne iştirak edememekteyim.

Üye

Hasan Tahsin GÖKCAN

YARGITAY KARARLARI

Bölüm İçeriği

- Yargıtay Kararı - Ceza Genel Kurulu (E. 2015/708)
- Yargıtay Kararı - Ceza Genel Kurulu (E. 2012/1510)
- Yargıtay Kararı - Hukuk Genel Kurulu (E. 2017/1340)
- Yargıtay Kararı - Hukuk Genel Kurulu (E. 2014/56)
- Yargıtay Kararı - 19. Ceza Dairesi (E. 2017/3325)
- Yargıtay Kararı - 19. Ceza Dairesi (E. 2017/6127)
- Yargıtay Kararı - 19. Ceza Dairesi (E. 2017/6532)
- Yargıtay Kararı - 19. Ceza Dairesi (E. 2018/3318)
- Yargıtay Kararı - 19. Ceza Dairesi (E. 2019/28161)
- Yargıtay Kararı - 19. Ceza Dairesi (E. 2020/4751)
- Yargıtay Kararı - 17. Ceza Dairesi (E. 2016/10020)
- Yargıtay Kararı - 17. Ceza Dairesi (E. 2016/9901)
- Yargıtay Kararı - 17. Ceza Dairesi (E. 2015/22839)
- Yargıtay Kararı - 17. Ceza Dairesi (E. 2015/18421)
- Yargıtay Kararı - 12. Ceza Dairesi (E. 2020/974)
- Yargıtay Kararı - 12. Ceza Dairesi (E. 2019/4369)
- Yargıtay Kararı - 12. Ceza Dairesi (E. 2017/2960)
- Yargıtay Kararı - 12. Ceza Dairesi (E. 2015/13758)
- Yargıtay Kararı - 12. Ceza Dairesi (E. 2015/13582)
- Yargıtay Kararı - 12. Ceza Dairesi (E. 2013/9043)
- Yargıtay Kararı - 12. Ceza Dairesi (E. 2014/607)
- Yargıtay Kararı - 7. Ceza Dairesi (E. 2021/21566)
- Yargıtay Kararı - 6. Ceza Dairesi (E. 2021/10682)
- Yargıtay Kararı - Hukuk Genel Kurulu (E. 2014/56)
- Yargıtay Kararı - 22. Hukuk Dairesi (E. 2017/21857)
- Yargıtay Kararı - 20. Hukuk Dairesi (E. 2017/2277)
- Yargıtay Kararı - 14. Hukuk Dairesi (E. 2016/2792)
- Yargıtay Kararı - 9. Hukuk Dairesi (E. 2014/37215)
- Yargıtay Kararı - Ceza Genel Kurulu (E. 2015/708)

- Yargıtay Kararı - Ceza Genel Kurulu (E. 2012/1510)
- Yargıtay Kararı - Hukuk Genel Kurulu (E. 2017/1340)
- Yargıtay Kararı - Hukuk Genel Kurulu (E. 2014/56)
- Yargıtay Kararı - 19. Ceza Dairesi (E. 2017/3325)
- Yargıtay Kararı - 19. Ceza Dairesi (E. 2017/6127)
- Yargıtay Kararı - 19. Ceza Dairesi (E. 2017/6532)
- Yargıtay Kararı - 19. Ceza Dairesi (E. 2018/3318)
- Yargıtay Kararı - 19. Ceza Dairesi (E. 2019/28161)
- Yargıtay Kararı - 19. Ceza Dairesi (E. 2020/4751)
- Yargıtay Kararı - 17. Ceza Dairesi (E. 2016/10020)
- Yargıtay Kararı - 17. Ceza Dairesi (E. 2016/9901)
- Yargıtay Kararı - 17. Ceza Dairesi (E. 2015/22839)
- Yargıtay Kararı - 17. Ceza Dairesi (E. 2015/18421)
- Yargıtay Kararı - 12. Ceza Dairesi (E. 2020/974)
- Yargıtay Kararı - 12. Ceza Dairesi (E. 2019/4369)
- Yargıtay Kararı - 12. Ceza Dairesi (E. 2017/2960)
- Yargıtay Kararı - 12. Ceza Dairesi (E. 2015/13758)
- Yargıtay Kararı - 12. Ceza Dairesi (E. 2015/13582)
- Yargıtay Kararı - 12. Ceza Dairesi (E. 2013/9043)
- Yargıtay Kararı - 12. Ceza Dairesi (E. 2014/607)
- Yargıtay Kararı - 7. Ceza Dairesi (E. 2021/21566)
- Yargıtay Kararı - 6. Ceza Dairesi (E. 2021/10682)
- Yargıtay Kararı - Hukuk Genel Kurulu (E. 2014/56)
- Yargıtay Kararı - 22. Hukuk Dairesi (E. 2017/21857)
- Yargıtay Kararı - 20. Hukuk Dairesi (E. 2017/2277)
- Yargıtay Kararı - 14. Hukuk Dairesi (E. 2016/2792)
- Yargıtay Kararı - 9. Hukuk Dairesi (E. 2014/37215)

Yargıtay Kararı - Ceza Genel Kurulu (E. 2015/708)

Yargıtay CGK., E. 2015/708 K. 2019/414 T. 9.5.2019

Esas No.: 2015/708

Karar No.: 2019/414

Karar Tarihi: 09.05.2019

Kararı Veren

Yargıtay Dairesi: 12. Ceza Dairesi

Mahkemesi: Asliye Ceza

Sayısı: 714-321

Sanık ... hakkında hakaret suçundan cezalandırılması istemiyle açılan kamu davasında yapılan yargılama sırasında, Sakarya 4. Sulh Ceza Mahkemesince 01.11.2012 tarih ve 755-920 sayı ile, sanığın hakaret olarak vasıflandırılan eyleminin özel hayatın gizliliğini ihlal suçunu oluşturabileceği gerekçesiyle görevsizlik kararı verilmesi üzerine, dosyanın gönderildiği Sakarya 4. Asliye Ceza Mahkemesince 10.04.2013 tarih ve 714-321 sayı ile, sanığın eyleminin özel hayatın gizliliğini ihlal suçunu oluşturduğu kabul edilerek TCK'nın 134/1, 43/1 ve 53. maddeleri uyarınca 1 yıl 8 ay hapis cezası ile cezalandırılmasına ve hak yoksunluğuna karar verilmiştir.

Hükmün sanık ve müdafisi tarafından temyiz edilmesi üzerine dosyayı inceleyen Yargıtay 12. Ceza Dairesince 09.02.2015 tarih ve 15359-2143 sayı ile;

“Sanık hakkında düzenlenen 22.10.2012 tarihli iddianamedeki anlatıma ve iddianame yerine geçen Sakarya 4. Sulh Ceza Mahkemesinin 01.11.2012 tarihli görevsizlik kararının içeriğine göre; sanık ...'ın, mağdur ...'nın kendisinden ayrılıp bir başkasıyla evlenmesine tepki olarak, mağdurun diz kapağı ile başının arasının görüntülendiği resimlerinin üzerine, onun adı ve kızlık soyadı ile evlendikten sonra edindiği soyadı ve telefon numarasını yazıp mağdurun iç çamaşırlarına ve geceliğine zımbaladığı bu resimleri, mağdurun oturduğu muhitteki binaların duvarlarına astığı ve sokaklara bıraktığı olayda, Mağdurun özel yaşam alanı kapsamında bulunan iç çamaşırlarının ve geceliğinin afişe edilmesinin TCK'nın 134/1-1. maddesindeki özel hayatın gizliliğini ihlal, mağdura ait özel resimlerin ifşa edilmesinin aynı Kanun'un 134/2-1. maddesindeki özel hayatın gizliliğini ihlal, mağdurun kişisel veri niteliğindeki kimlik bilgileri ve telefon numarasının rızasına aykırı şekilde yayılmasının TCK'nın

136/1. maddesindeki verileri hukuka aykırı olarak verme veya ele geçirme, bu suretle mağdurun onur, şeref ve saygınlığının alenen rencide edilmesinin aynı Kanun'un 125/1-4. maddesindeki hakaret suçlarını oluşturacağı; ancak, bir fiil ile birden fazla farklı suçun oluşmasına neden olan sanığın, TCK'nın 44/1. maddesi gereğince, en ağır cezayı gerektiren TCK'nın 134/2-1. maddesindeki özel hayatın gizliliğini ihlal suçundan cezalandırılması, mağdurun resimlerini bir suç işleme kararının icrası kapsamında birden fazla defa ifşa eden sanığa hükmedilen cezada TCK'nın 43/1. maddesi gereğince artırım yapılması, diğer suçlardan ise hüküm kurulmasına yer olmadığına karar verilmesi gerekirken, mağdurun özel yaşam alanı kapsamındaki eşyasıyla beraber mağdurun özel hayatına ilişkin görüntülerinin ifşa edildiği kabul edildiği hâlde, fikri içtima hükmü nazara alınmaksızın yasal ve yeterli olmayan gerekçelerle sanık hakkında TCK'nın 134/1-1. maddesindeki özel hayatın gizliliğini ihlal suçundan mahkûmiyet hükmü kurularak sanığa eksik ceza tayin edilmesi," isabetsizliğinden CMUK'nın 326/son maddesi uyarınca ceza miktarı itibarıyla sanığın kazanılmış hakkı saklı kalmak kaydıyla bozulmasına karar verilmiştir.

Yargıtay Cumhuriyet Başsavcılığı ise 20.04.2015 tarih ve 158622 sayı ile;

"Sanık ...'nin, katılan ...'nın bırakmış olduğu iç çamaşırlarını ve resimlerini alarak bir şekilde Camili Mahallesiindeki bir kısım binaların kapılarına ve duvarlarına asmak yahut astırmak şeklinde kabul edilen eylemlerinin TCK'nın 125/1, 134/1, 134/2 ve 43. maddelerinde yazılı suçları oluşturduğu, ancak sanık, öç almak ve katılanı toplum nezdinde küçük düşürmek amacıyla hareket etmiş olup kastının birden fazla suça yönelik olduğu görülmemektedir. Sanık, tek suç işleme kastıyla hareket edip birden fazla icrai harekette bulunarak suçu işlemektedir. Bu suçlara yönelik icrai hareketlerin birbiriyle örtüşmesi söz konusudur. Bu itibarla TCK'nın 125/1, 134/1, 134/2 ve 43. maddelerinde yazılı suçların ortak icrai hareketlerle gerçekleştiği kabul edilerek sanık hakkında TCK'nın 44. maddesinde düzenlenen fikri içtima hükmü uyarınca en ağır cezayı gerektiren TCK'nın 134/2. maddesi gereğince mahkûmiyet hükmü kurulması gerekmektedir.

Ancak sanık ...'nin, katılan ...'in özel hayatının gizliliğini ihlal etmesi dışında ayrıca TCK'nın 136/1. maddesinde yazılı kişisel veri niteliğinde bulunan kimlik bilgilerinin ve telefon numarasının, rızasına aykırı olarak yayılmasını sağlamak amacıyla gerçekleştirdiği eyleminde, katılana yönelik tek suç işleme kastıyla hareket etmemiş, katılanın kimlik bilgileri ile telefon numarasını elde eden üçüncü kişilerin katılanı rahatsız etmesi ve katılanın cinsel taciz ve saldırıya maruz kalması amacıyla hareket etmiştir.

TCK'nın 136/1. maddesinde yazılı suçun icrai hareketleri, önceki bölümde açıklanan özel hayatın gizliliğini ihlal ve hakaret suçlarından farklı olup sanık, katılanın kimlik bilgilerinin ve telefon

numarasının temin edilmesi suretiyle katılan ...'nin aşağılanması ve küçük düşürülmesinin yanında, üçüncü kişiler tarafından rahatsız edilmesi ve cinsel yönden taciz edilmesi kastıyla hareket etmiştir.

Sanığın gerçekleştirdiği özel hayatın gizliliğini ihlal suçu ile kişisel verileri açıklama ve yayma suçunun icrai eylemlerinin birbirlerinden farklı olması durumunda bile aynı sonuca yönelmiş tek suç işleme kararıyla işlenmesi hâlinde, icrai hareketlerin birbiriyle örtüştüğü kabul edilmekte ve işlenen birden fazla suçla ilgili TCK'nın 44. maddesi uygulanmaktadır.

Ancak sanık ...'in gerçekleştirdiği tüm icrai eylemler göz önüne alındığında, sanığın tek suç işleme kastı bulunmamaktadır. Sanık, katılana yönelik özel hayatın gizliliğini ihlal ve hakaret suçlarında katılanı küçük düşürme amacıyla hareket ederek suçu işlemekte, diğer yandan farklı icrai hareketlerle, katılanın kimlik bilgilerinin ve telefon numarasının temin edilmesi suretiyle katılanın aşağılanması ve küçük düşürülmesinin yanında, üçüncü kişiler tarafından rahatsız edilmesi ve cinsel yönden taciz edilmesi kastıyla hareket etmektedir.

Maddi olayda birden fazla suç işleme kararı bulunduğundan, sanık hakkında TCK'nın 134/2 ve 43/1. maddelerinin yanında, ayrıca TCK'nın 136/1. maddesinde yazılı bulunan verileri hukuka aykırı olarak verme veya ele geçirme suçu oluşmaktadır. Bu suçla ilgili olarak TCK'nın 44. maddesinde yazılı fikri içtima kuralları uygulanmamalıdır.

Bu itibarla, sanık ...'nin, katılan ...'nin evde bırakmış olduğu iç çamaşırlarını ve resimlerini alarak Camili Mahallesiindeki bir kısım binaların kapılarına ve duvarlarına asmak yahut astırmak şeklindeki eylemlerinin, TCK'nın 125/1, 134/1, 134/2 ve 43. maddeleri kapsamında bulunduğu ve bu eylemleri hakkında TCK'nın 44. maddesi uyarınca en ağır cezayı gerektiren TCK'nın 134/2 ve 43. maddeleri uyarınca mahkûmiyetine karar verilmesi gerektiği,

Diğer yandan, sanık ...'nin, katılan ...'in kişisel veri niteliğinde bulunan kimlik bilgilerinin ve telefon numarasının rızasına aykırı olarak yayılmasını sağlama eyleminde, sanığın tek suç işleme kastıyla hareket etmediği, sanığın, kimlik bilgileri ile telefon numarasını elde eden kimsenin katılanı rahatsız etmesi ve cinsel taciz ve saldırıya maruz kalmasını sağlamak amacıyla hareket ettiği ve sanığın eyleminin TCK'nın 136/1. maddesinde yazılı verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğu,

Sanık hakkında TCK'nın 136/1. maddesi gereğince atılı suçtan ayrıca hüküm kurulması gerektiği gözetilmeden bu suçla ilgili TCK'nın 44. maddesinde düzenlenen fikri içtima hükümlerinin uygulanması gerektiği ileri sürülerek sanık hakkında yalnızca TCK'nın 134/2 ve 43. maddeleri

uyarınca hüküm kurulması hukuka aykırılık oluşturmaktadır." görüşüyle itiraz kanun yoluna başvurmuştur.

CMK'nın 308. maddesi uyarınca inceleme yapan Yargıtay 12. Ceza Dairesince 29.06.2015 tarih ve 9412-12049 sayı ile; itiraz nedenlerinin yerinde görülmediğinden bahisle Yargıtay Birinci Başkanlığına gönderilen dosya, Ceza Genel Kurulunca değerlendirilmiş ve açıklanan gerekçelerle karara bağlanmıştır.

TÜRK MİLLETİ ADINA

CEZA GENEL KURULU KARARI

Sanık hakkında tehdit suçundan kurulan mahkûmiyet hükmü Özel Dairece onanmak suretiyle kesinleşmiş olup itirazın kapsamına göre inceleme, özel hayatın gizliliğini ihlal suçundan kurulan mahkûmiyet hükmü ile sınırlı olarak yapılmıştır.

Özel Daire ile Yargıtay Cumhuriyet Başsavcılığı arasında oluşan ve Ceza Genel Kurulunca çözümlenmesi gereken uyuşmazlık; sanığın, katılanın diz kapağı ile başı arasındaki kısmının görüntülediği fotoğrafların üzerine, adı ve kızlık soyadı ile evlendikten sonra edindiği soyadı ve telefon numarasını yazarak katılanın iç çamaşırlarına ve geceliğine zımbalayıp katılanın oturduğu bina ile başka binalara ve sokaklara bırakması şeklinde gerçekleşen ve Özel Dairece eylemin TCK'nın 134/1, 134/2, 136/1 ve 125/1-4. maddelerindeki suçları oluşturduğu kabul edilen olayda; sanığın, TCK'nın 44. maddesi uyarınca en ağır cezayı gerektiren TCK'nın 134/2 ve 43. maddeleri uyarınca mı yoksa TCK'nın 134/2 ve 43. maddeleri ile birlikte ayrıca 136/1. maddesi uyarınca mı cezalandırılması gerektiğinin belirlenmesine ilişkindir.

İncelenen dosya kapsamından;

Katılanın, diz kapağı ile başı arasındaki kısmının görüntülediği fotoğrafların üzerine adı ve kızlık soyadı ile evlendikten sonra edindiği soyadı ve telefon numarasının yazılarak iç çamaşırlarına ve geceliklerine zımbalanıp oturduğu bina ile başka binalara ve sokaklara bırakıldığı yönünde şikâyette bulunarak söz konusu eşyayı kolluk görevlilerine teslim etmesi üzerine soruşturmanın başladığı,

Kolluk görevlilerince tutulan 24.07.2012 tarihli tutanakta; katılan tarafından teslim edilen iki poşet içerisindeki iç çamaşırları ve geceliklerin üzerinde damga teli ile tutturulmuş diz kapağı ile başı arasındaki kısmının görüntülediği fotoğrafların bulunduğu ve fotoğrafların üzerinde de "Selma KARAKULLUKÇU 0534 512 yeni soyad KOTAN" ibarelerinin olduğu bilgilerine yer verildiği,

Katılan ...'ın; sanık ile 7 yıl kadar birlikte yaşadıkdan sonra yaklaşık 1 yıl önce ayrıldıklarını, 5 ay önce bir başkasıyla evlendiğini ve Adapazarı'nda ikamet ettiğini, 10.07.2012 tarihinde saat 07.00 sıralarında aynı binada oturduğu ...'nun elinde çeşitli renklerde iç çamaşırları ve geceliklerle gelerek "Bu çamaşırların üzerinde senin fotoğrafların takılı ve üzerinde de ismin ve numaran yazılı, bunları binanın giriş kapısında buldum." dediğini, çamaşırlara baktığında sanık ile birlikte yaşarken kullandığı çamaşırlar olduğunu, fotoğrafların da kendisine ait olduğunu gördüğünü, aynı gün saat 22.00 sıralarında Hülya'nın kendisine, üzerinde fotoğraflarının takılı olduğu çamaşırlardan binanın yanındaki parkta da olduğunu söylemesi üzerine parka gittiğinde, üzerinde fotoğrafları bulunan gecelik ve iç çamaşırının parktaki kamelyada asılı olduğunu gördüğünü, yaptığı araştırma sonucunda bu işi sanığın yaptığını, iç çamaşırları ile fotoğraflarını Sakarya ili ve ilçelerindeki muhtelif sokaklara da bıraktığını, ayrıca etrafta çıplak vaziyette çekilmiş fotoğraflarını internette yayınlayacağı şeklinde konuştuğunu öğrendiğini, dayısı olan ...'e de sanığın "Selma'nın iç çamaşırlarını ben serdim, hatta daha fazla pislikler yapacağım" dediğini, sanıktan şikâyetçi olduğunu beyan ettiği,

Tanık ...'nun; 10.07.2012 tarihinde saat 06.50 sıralarında işe gitmek üzere ikametinden çıktığı esnada, komşusu olan katılanın fotoğraflarının zımbalandığı iç çamaşırlarının evinin kapısının koluna, binanın kapısına ve duvarlarına asılmış olduğunu gördüğünü, bunun üzerine çamaşırları ve fotoğrafları toplayıp katılana götürdüğünü, aynı şekilde katılanın fotoğraflarının zımbalandığı iç çamaşırlarını sokakta, bir arabanın üzerinde ve parkta da gördüğünü anlattığı,

Tanık ...'in; Hendek ilçesinde ikamet ettiğini, yeğeni olan katılan ile sanığın daha önce birlikte yaşadıklarını, yaklaşık iki hafta önce ikametinin yan tarafındaki bahçe duvarının demirlerinde iç çamaşırları asılı olduğunu ve üzerinde de katılanın fotoğrafının bulunduğunu gördüğünü, bunun üzerine sanığı arayıp "Kapının önüne iç çamaşırı asılmış, bunu sen mi yaptın." diye sorduğunu, sanığın da "Evet, ben yaptım. Selma bana çok çektirdi, ben de ona çektireceğim." şeklinde cevap verip telefonu kapattığını, sanığın başka yerlere de bu şekilde iç çamaşırı ve fotoğraf koyduğunu söylediği, Hakkında ek kovuşturmayaya yer olmadığına karar verilen ...'in; yaklaşık bir ay önce sanıkla kahvehanede sohbet ederken sanığa "Selma ile evlenmiyor musunuz" diye sorduğunu, sanığın "Yok, Selma beni bırakıp gitti." şeklinde cevap verdiğini, sanığa "Yapma, eşindir, tekrar bir araya gelin." demesi üzerine sanığın "Yok, o beni rezil etti, ben de onun evde bulunan iç çamaşırlarını evinin bulunduğu yere ve duraklara asacağım." dediğini, yaklaşık bir hafta sonra da sanığın katılanın iç çamaşırlarını duraklara ve evinin çevresine astığını duyduğunu ifade ettiği,

Sanık ...'nin suçlamaları kabul etmediği,

Anlaşılmıştır.

Anayasamızın "Özel hayatın gizliliği" başlıklı 20. maddesinin birinci fıkrası; "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz." şeklinde olup maddeye 13.05.2010 tarihli Resmî Gazete'de yayımlanarak yürürlüğe giren 5982 sayılı Kanun'un 2. maddesiyle; "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." biçimindeki üçüncü fıkra eklenmiştir.

Avrupa İnsan Hakları Sözleşmesi'nin "Özel ve aile hayatına saygı hakkı" başlıklı 8. maddesinde de; "1- Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

2- Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir." hükmü bulunmaktadır.

Bu genel açıklamalardan sonra uyuşmazlığın çözümü açısından 5237 sayılı TCK'nın "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" bölümünde düzenlenen "özel hayatın gizliliğini ihlal" ve "verileri hukuka aykırı olarak verme veya ele geçirme" suçları üzerinde durulmalıdır.

5237 sayılı TCK'nın 139. maddesi uyarınca soruşturulması ve kovuşturulması şikâyete bağlı bir suç olarak öngörülen özel hayatın gizliliğini ihlal suçunun düzenlendiği TCK'nın 134. maddesi;

"(1) Kişilerin özel hayatının gizliliğini ihlal eden kimse, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi hâlinde, cezanın alt sınırı bir yıldan az olamaz.

(2) Kişilerin özel hayatına ilişkin görüntü veya sesleri ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Fiilin basın ve yayın yoluyla işlenmesi halinde, ceza yarı oranında artırılır." şeklinde iken, suç tarihinden önce 05.07.2012 tarihli Resmî Gazete'de yayımlanarak yürürlüğe giren 6352 sayılı Kanun'un 81. maddesiyle; maddenin birinci fıkrasında yer alan "altı aydan iki yıla kadar hapis veya adli para" ibaresi "bir yıldan üç yıla kadar hapis" ve "cezanın alt sınırı bir yıldan az olamaz" ibaresi "verilecek ceza bir kat artırılır" şeklinde, ikinci fıkrası da "Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse, iki yıldan beş yıla kadar hapis cezası

ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması hâlinde de aynı cezaya hükmolunur." biçiminde değiştirilmiştir.

5237 sayılı TCK'nın 134. maddesinde düzenlenen suç ile korunan hukuki yarar; özel hayatın gizliliği ve korunması hakkıdır. Kişilerin özel hayatlarının gizliliğinin korunmasını isteme hakları olması nedeniyle bu suçun işlenmesi sonucu özel hayatlarının gizliliği ihlal edilmiş olmaktadır. Ancak suçun oluşabilmesi için bu ihlalin hukuka aykırı olarak yapılması zorunludur.

Maddenin birinci fıkrasında tanımlanan suçu oluşturan fiil, kişilerin özel hayatının gizliliğinin ihlalidir. Gizliliğin ne şekilde ihlal edildiğinin suçun temel şekli bakımından bir önemi olmayıp bu yönüyle serbest hareketli bir suçtur. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi ise suçun aynı fıkranın ikinci cümlesinde düzenlenen nitelikli hâlini oluşturacaktır.

Maddenin ikinci fıkrasında, kişilerin özel hayatına ilişkin görüntü veya seslerin hukuka aykırı olarak ifşa edilmesi ayrı bir suç olarak düzenlenmiştir. Madde metninde yer alan "ifşa" kelimesi, Türk Dil Kurumu Türkçe Sözlüğünde; "gizli bir şeyi açığa çıkarma, yayma" olarak tanımlanmıştır. Özel hayata ilişkin her hususun değil, yalnızca görüntü veya seslerin ifşa edilmesi bu fıkradaki suçun oluşumuna sebebiyet verecektir. Bu görüntü veya sesler, hukuka uygun bir şekilde kayda alınmış olabileceği gibi birinci fıkrada tanımlanan suçun işlenmesi suretiyle de elde edilmiş olabilir. Özel hayata ilişkin bu kayıtların, taksirle ya da tamamen hukuka uygun elde edilmiş olsa dahi, bilerek, isteyerek ve ilgisinin bilgisi ve rızası dışında ifşa edilmesi, bu bağlamda içeriğini öğrenme yetkisi bulunmayan kişi veya kişilerin bilgisine sunulması maddenin ikinci fıkrasında düzenlenen suçu oluşturacaktır. İfşanın kabulü için, görüntü veya sesin ilgili olduğu kişinin anlaşılması, en azından anlaşılabilir olması ya da açıklanması gerekmektedir. Bu fıkradaki suçun oluşumu için ifşanın hukuka aykırı olması gerekmektedir.

Bu suçlar ancak kasten işlenebilen suçlardan olup suçun oluşumu için saik aranmaz.

Uyuşmazlık konusuyla ilgili TCK'nın "Verileri hukuka aykırı olarak verme veya ele geçirme" başlıklı 136. maddesi ise; "Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır." şeklinde iken, suç tarihinden sonra 06.03.2014 tarihli Resmî Gazete'de yayımlanarak yürürlüğe giren 6526 sayılı Kanun'un 4. maddesiyle suçun cezasının alt sınırı "iki yıla" çıkartılmıştır.

TCK'nun 136. maddesinde düzenlenen suç ile korunan hukuki yarar, genel olarak kişilerin özel hayatı ve hayatın gizli alanı, özelde ise kişisel verilerdir. Bu düzenlemeler ile tüm kişisel veriler koruma altına alındığından kişisel verilerin mutlaka gizli olması zorunlu değildir. Gizli olmayan ve herkes

tarafından bilinen kişisel veriler de hukuka aykırı eylemlere karşı korunmalıdır. Zira kişisel verilerin korunmasına ilişkin suçlarda korunan hukuki değer "sır" olmayıp, verinin ilgilisi olan kişinin kişilik haklarıdır.(Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayınevi, Ankara, 2014, 4. bası, s.579, 588-593)

Suçun konusu, kişisel verilerdir. Suç tarihi itibarıyla yürürlükte olan Kanunlarda, suçun konusunu oluşturan kişisel veriden ne anlaşılması gerektiğine ilişkin bir tanım yer almayıp TCK'nın 135. maddesinin gerekçesinde; "Gerçek kişiyle ilgili her türlü bilgi, kişisel veri olarak kabul edilmelidir. Söz konusu suç tanımında kişisel verilerin bilgisayar ortamında veya kağıt üzerinde kayda alınması arasında bir ayırım gözetilmemiştir." denilmiştir.

Suç tarihinde sonra 07.04.2016 tarihli Resmî Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Tanımlar" başlıklı 3. maddesinin birinci fıkrasının (d) bendinde "Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi...ifade eder." şeklinde tanım yapılmış, maddenin gerekçesinde ise; "Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Bu bağlamda sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgiler de kişisel veridir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm hâlleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilmek üzere özellikleri nedeniyle kişisel verilerdir." açıklamasına yer verilmiştir.

28.01.1981 tarihli ve 108 nolu Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Uluslararası Sözleşme'nin 2/a maddesinde ise; "Kişisel nitelikteki veriler; kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm bilgileri ifade eder." denilmiş, 1995 tarihinde yürürlüğe giren Avrupa Topluluğu Veri Koruma Yönergesi'nin 2. maddesinde de kişisel veri; "doğrudan doğruya ya da dolaylı olarak bir gerçek kişi ile ilintili olabilecek ve onu belirlenebilir kılacak her türlü bilgi" olarak belirtilmiştir.

Kişilerin, sadece insan olması ve toplumdaki yeri, bazı değerleri kişisel veri hâline getirmektedir. Örneğin; kişinin adı, adresi, kimlik bilgileri, medeni durumu vb... Bunun yanında teknolojik

gelişmeler nedeniyle gittikçe karmaşıklaşan toplum hayatındaki bir takım bilgiler de kişisel veri hâline gelmiştir. Örneğin; vatandaşlık numarası, banka hesap numarası, telefon numarası, elektronik posta adresi ve şifresi vb... Dolayısıyla farklı gruplandırmalar bulunmakla birlikte kişisel verilerin iki başlık altında toplanması mümkündür. Birinci grupta; insanın varoluşundan kaynaklanan kişiliğine ait bilgiler, ikinci grupta ise; teknolojinin gelişmesiyle insanın modern toplumda yer alması nedeniyle kendisine verilen ya da çeşitli hizmetlere ulaşmasında kullanılan bilgiler yer almaktadır. Ancak her iki grupta yer alan bilgilerin de kişisel veri olarak hukuk düzenindeki değeri ve korunmaları açısından bir fark bulunmamaktadır. (Murat Volkan Dülger, s.577)

TCK'nın 136. maddesindeki "verileri hukuka aykırı olarak verme veya ele geçirme" suçu, seçimlik hareketli bir suç olarak düzenlenmiştir. Hukuka aykırı olarak kişisel verilerin başkasına verilmesi, kişisel verilerin yayılması ve kişisel verilerin ele geçirilmesi şeklindeki seçimlik hareketlerin birinin gerçekleştirilmesiyle suç işlenmiş olacaktır.

"Kişisel verileri bir başkasına verme" seçimlik hareketinde, maddede geçen "başkası" gerçek bir kişi olabileceği gibi tüzel kişi de olabilecek, veriler bu kişilere elden, posta ya da internet üzerinden elektronik posta ile vb. şekillerde verilebilecektir. Türk Dil Kurumu Büyük Türkçe Sözlüğünde "vermek"; "üzerinde, elinde veya yakınında olan bir şeyi birisine erdirtmek, iletmek, düşünce veya bilgi anlatan şeyleri başkalarına iletmek, bildirmek" şeklinde açıklanmıştır. Bu seçimlik harekette verilerin hukuka uygun ya da aykırı yöntemle elde edilmiş olmasının önemi bulunmamakta olup önemli olan husus verme eyleminin hukuka aykırı olmasıdır.

"Kişisel verileri yayma" seçimlik hareketi de çeşitli şekillerde gerçekleştirilebilecektir; internet üzerindeki bir web sitesinde kişisel verileri yayınlamak, birçok kişiye elektronik posta ile ya da telefonda kısa mesajla göndermek, yazılı ya da görsel medyada yayınlamak gibi... Türk Dil Kurumu Büyük Türkçe Sözlüğünde "yaymak"; "birçok kimseye duyurmak, çevreye dağılmasına sebep olmak" olarak açıklanmıştır.

"Kişisel verilerin ele geçirilmesi" seçimlik hareketi ise kişisel verilerin kayıtlı olduğu belgelerin alınması ya da kayıtlı olduğu bilişim sisteminden ele geçirilmesi vb... şekillerde gerçekleştirilebilecektir. Ele geçirme fiili, başkasının hâkimiyeti altında bulunan bir kişisel verinin, failin hâkimiyeti altına girmesi ile gerçekleşmiş olacaktır.

Bu suçta herhangi bir neticenin gerçekleşmesi aranmadığından maddede sayılan seçimlik hareketlerin yapılmasıyla suç oluşacaktır. Bu açıdan TCK'nın 136. maddesindeki "verileri hukuka aykırı olarak verme veya ele geçirme" soyut bir tehlike suçudur.

Bu maddede düzenlenen suç genel kastla işlenen bir suç olup suçun oluşumu için saik aranmaz.

Uyuşmazlıkla ilgili olarak ele alınması gereken diğer suç olan hakaret, 5237 sayılı TCK'nın 125. maddesinde;

“(1) Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran kişi, üç aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Mağdurun gıyabında hakaretin cezalandırılabilmesi için fiilin en az üç kişiyle ihtilâl ederek işlenmesi gerekir.

(2) Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi hâlinde, yukarıdaki fıkrada belirtilen cezaya hükmolunur.

(3) Hakaret suçunun;

a) Kamu görevlisine karşı görevinden dolayı,

b) Dinî, siyasi, sosyal, felsefi inanç, düşünce ve kanaatlerini açıklamasından, değiştirmesinden, yaymaya çalışmasından, mensup olduğu dinin emir ve yasaklarına uygun davranmasından dolayı,

c) Kişinin mensup bulunduğu dine göre kutsal sayılan değerlerden bahisle,

İşlenmesi hâlinde, cezanın alt sınırı bir yıldan az olamaz.

(4) Hakaretin alenen işlenmesi halinde ceza altıda biri oranında artırılır.

(5) Kurul hâlinde çalışan kamu görevlilerine görevlerinden dolayı hakaret edilmesi hâlinde suç, kurulu oluşturan üyelere karşı işlenmiş sayılır. Ancak, bu durumda zincirleme suça ilişkin madde hükümleri uygulanır.” şeklinde düzenlenmiştir.

Maddenin birinci fıkrasında hakaret suçunun temel şekli, üçüncü ve dördüncü fıkralarında ise nitelikli hâlleri düzenlenmiş, madde gerekçesinde de; “Hakaret fiillerinin cezalandırılmasıyla korunan hukuki değer, kişilerin şeref, haysiyet ve namusu, toplum içindeki itibarı, diğer fertler nezdindeki saygınlığıdır.” açıklaması yapılmıştır. Buna göre, suçun konusu kişilerin onur, şeref ve saygınlığı olup somut bir fiil veya olgu isnat etme ya da sövme suretiyle kişilerin onur, şeref ve saygınlığına saldırma eylemi hakaret suçunu oluşturacaktır.

Ceza Genel Kurulunun birçok kararında da belirtildiği üzere; 5237 sayılı TCK'da, 765 sayılı Kanun'daki hakaret ve sövme suçu ayrımı kaldırılmıştır. Hakaret fiillerinin cezalandırılmasıyla korunan hukuki değer, kişilerin şeref, haysiyet ve namusu, toplum içindeki itibarı, diğer fertler nezdindeki saygınlığı olduğundan, bu suçun oluşabilmesi için, davranışın kişiyi küçük düşürmeye matuf olarak gerçekleştirilmesi gerekmektedir. Somut bir fiil ya da olgu isnat etmek veya sövmek

şeklindeki seçimlik hareketlerden biri ile gerçekleştirilen eylem, bireyin onur, şeref ve saygınlığını rencide edebilecek nitelikte ise hakaret suçu oluşacaktır.

Son olarak uyuşmazlığın çözümü açısından fikri içtima üzerinde durulmalıdır.

5237 sayılı TCK'nın hazırlanmasında "kaç fiil varsa o kadar suç, kaç suç varsa o kadar ceza vardır" ilkesi esas alınmış, dolayısıyla da gerçek içtima kuralı benimsenmiştir. Nitekim Adalet Komisyonu raporunda bu husus; "Ceza hukukunun temel kurallarından birisi, 'kaç fiil varsa o kadar suç, kaç suç varsa o kadar ceza vardır.' şeklinde ifade edilmektedir. Bunun istisnaları, suçların içtimai bölümünde belirlenmiştir. Bu istisnalar dışında, işlenen her bir suçla ilgili olarak ayrı ayrı cezaya hükmedilecektir. Böylece verilen her bir ceza, bağımsızlığını koruyacaktır." şeklinde ifade edilmiştir. Bu kuralın istisnaları ise, 5237 sayılı TCK'nın "suçların içtimai" bölümünde, 42 (bileşik suç), 43 (zincirleme suç) ve 44. (fikri içtima) maddelerinde düzenlenmiştir.

765 sayılı TCK'da, aynı neviden fikri içtima ile farklı neviden fikri içtima tek madde hâlinde ve Kanun'un 79. maddesinde düzenlenmiş iken, 5237 sayılı TCK'da bu iki hâl birbirinden ayrılarak, aynı neviden fikri içtima, zincirleme suçun düzenlendiği 43. maddenin ikinci fıkrasında, farklı neviden fikri içtima ise Kanun'un 44. maddesinde düzenlenmiştir.

Farklı neviden fikri içtima 5237 sayılı Kanun'un 44. maddesinde; "İşlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır." şeklinde düzenlenmiş olup hükmün uygulanabilmesi için işlenen bir fiille birden fazla farklı suçun oluşması gerekmektedir.

Kanun koyucu, işlediği bir fiille birden fazla farklı suçu işleyen failin, fiilin tek olması nedeniyle en ağır ceza ile cezalandırılmasını yeterli görmüş, bu şekilde "non bis in idem" kuralı gereğince bir fiilden dolayı kişinin birden fazla cezalandırılmasının da önüne geçilmesini amaçlamış, "erime sistemini" benimsemek suretiyle, bu suçlardan en ağırının cezasının verilmesi ile yetinilmesini tercih etmiştir.

Bu bağlamda, "tek fiil" veya "bir fiil"den ne anlaşılması gerektiğinin de değerlendirilmesi gerekmektedir. Doğal anlamda gerçekleştirilen her bedensel eylem ayrı bir hareketi oluşturmakta ise de, hukuki anlamda hareketin tek olması ile ifade edilmek istenen husus, doğal anlamda birden fazla hareket bulunsa dahi, bu hareketlerin, hukuki nedenlerden dolayı değerlendirmede birlik oluşturması suretiyle tek hareket olarak kabulüdür. Diğer bir anlatımla, doğal anlamda fiilin tek olduğu her hâlde hukuki anlamda da fiilin tek olduğu söylenebilirse de, doğal anlamda fiilin çok olduğu her hâlde hukuki anlamda da fiilin çok olduğu her zaman söylenemeyecektir. Bazen bir

hareketler kümesi, hukuki açıdan tek bir fiil olarak kabul edilecektir. Bu hâlde suç tipinin birden fazla hareketle ihlal edilebilir olması hareketin hukuken tekliğini etkilemeyecek, doğal hareketler hukuken tek kabul edilecektir. Fikri içtimada da, fiil ya da hareketin tekliği, doğal anlamda değil hukuki anlamda tek olmayı ifade etmektedir. Bir kısım suçların işlenmesi sırasında doğal olarak birden fazla hareket yapılmakta ise de, ortaya konulan bu davranışlar suçun kanuni tanımında yer alan hukuksal anlamdaki "tek bir fiili" oluşturmaktadır. Nitekim öğretide de benzer nitelikte görüşler ileri sürülmüştür. (Mahmut Koca - İlhan Üzülmez, Türk Ceza Hukuku Genel Hükümler, Seçkin Yayınevi, 9. Bası, Ankara, 2016, s.492 vd., Hamide Zafer, Ceza Hukuku Genel Hükümler, Beta Yayıncılık, 3. Bası, İstanbul, 2013, s. 462 vd., Mehmet Emin Artuk - Ahmet Gökçen - Caner Yenidünya, Ceza Hukuku Genel Hükümler, Adalet Yayınevi, 7. Bası, Ankara, 2013, s.653 vb.)

5237 sayılı TCK'nın genel hükümleri arasında yer alan fikri içtima kuralları, şartlarının bulunması hâlinde kural olarak her suç için uygulanabilir ise de, kanun koyucunun açıkça istisna öngördüğü hâllerde bu kuralın uygulanma ihtimali bulunmamaktadır. Nitekim TCK'nın 212. maddesinde, sahte resmî veya özel belgenin bir başka suçun işlenmesi sırasında kullanılması hâlinde, hem sahtecilik hem de ilgili suçtan dolayı ayrı ayrı cezaya hükmolunacağı belirtilerek, açıkça fikri içtima hükümlerinin uygulanması engellenmiştir.

Bu anlatımlara göre, farklı neviden fikri içtimanın şartları, hareket ya da fiilin hukuki anlamda tek olması, tek fiille birden fazla farklı suçun işlenmiş olması, işlenen suçlarla ilgili kanunda açıkça fikri içtima hükümlerinin uygulanmasının engellenmemiş olması şeklinde belirlenebilecektir.

Görüldüğü gibi, kanuni istisnalar dışında, hukuki anlamda tek bir fiille birden fazla farklı suçun işlenmesi hâlinde, bu suçlardan en ağır cezayı gerektirenin cezasına hükmolunması kanun gereğidir.

Bu açıklamalar ışığında uyuşmazlık konusu değerlendirildiğinde;

TCK'nın 44. maddesinde düzenlenen farklı neviden fikri içtima hükmünün uygulanması için hukuki anlamda tek olan bir fiille birden fazla farklı suçun oluşması ve işlenen suçlarla ilgili kanunda açıkça fikri içtima hükmünün uygulanmasının engellenmemiş olması gerekmekte olup anılan maddenin uygulanma şartları arasında "tek suç işleme kastı" koşulunun bulunmadığı, bu itibarla sanığın uzun süre birlikte yaşadığı katılanın kendisinden ayrıldıktan kısa bir süre sonra bir başkasıyla evlenmesine tepki olarak katılanın diz kapağı ile başı arasındaki kısmının görüntülendiği fotoğrafların üzerine, adı ve kızlık soyadı ile evlendikten sonra edindiği soyadı ve telefon numarasını yazarak katılanın iç çamaşırlarına ve geceliğine zımbalayıp katılanın oturduğu bina ile Adapazarı ve Hendek ilçelerindeki bir kısım binalara ve sokaklara bıraktığı olayda; sanığın, katılanın özel yaşam alanı kapsamında bulunan iç çamaşırlarını ve geceliğini ifşa etmesinin TCK'nın 134. maddesinin birinci fıkrasının birinci

cümlesindeki özel hayatın gizliliğini ihlal suçunu, katılanın özel hayatına ilişkin fotoğrafları hukuka aykırı şekilde ifşa etmesinin TCK'nın 134. maddesinin ikinci fıkrasının birinci cümlesindeki özel hayatın gizliliğini ihlal suçunu, katılanın kişisel veri niteliğindeki ad, soyad ve cep telefonu numarasını hukuka aykırı şekilde yaymasının TCK'nın 136. maddesindeki verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğu, sanığın gerçekleştirdiği bu eylemlerin, aynı zamanda katılanın onur, şeref ve saygınlığını rencide edebilecek nitelikte olması nedeniyle TCK'nın 125. maddesinin birinci ve dördüncü fıkralar uyarınca alenen hakaret suçunun da olduğu, ancak sanığın, üzerinde katılanın kişisel veri niteliğindeki bilgileri bulunan özel hayatına ilişkin fotoğraflarını, katılanın özel yaşam alanı kapsamında kalan eşyasının üzerine zımbaladıktan sonra bunları yayma suretiyle açığa çıkarmaktan ibaret ve hukuki anlamda tek olan fiili ile birden fazla suç olduğundan hakkında TCK'nın 44. maddesi uygulanmak suretiyle oluşan suçlardan en ağır cezayı gerektiren TCK'nın 134. maddesinin ikinci fıkrası uyarınca ceza tayin edilmesi ve katılanın özel hayatına ilişkin fotoğrafları bir suç işleme kararının icrası kapsamında değişik zamanlarda ve değişik yerlerde birden fazla ifşa etmesi nedeniyle hükmolunacak cezada TCK'nın 43. maddesi uyarınca artırım yapılması gerekmektedir.

Bu itibarla, Özel Dairenin bozma kararı isabetli olup haklı nedene dayanmayan Yargıtay Cumhuriyet Başsavcılığı itirazının reddine karar verilmelidir.

Öte yandan, farklı neviden fikri içtima koşullarının oluşması nedeniyle faile tek bir ceza verilmesi, ancak hükümde fikri içtima ilişkisi içinde bulunan suçlardan her birinin ayrı ayrı gösterilmesi gerekir ise de ortada tek bir fiil bulunması nedeniyle sanık hakkında bu suçlardan cezası en ağır olan TCK'nın 134. maddesinin ikinci fıkrasından hüküm kurulmasıyla yetinilmeli, ayrıca diğer suçlardan hüküm kurulmasına yer olmadığına şeklinde karar verilmemelidir.

Ceza Genel Kurulu Üyeleri ..., ... ve ...; "Sanık hakkında TCK'nın 136. maddesinde düzenlenen 'Verileri hukuka aykırı olarak verme veya ele geçirme' suçundan açılmış bir kamu davası bulunmadığı" görüşüyle itirazın değişik gerekçe ile reddi yönünde oy kullanmışlar,

Çoğunluk görüşüne katılmayan Ceza Genel Kurulu Üyesi ...; "Sanığın, özel hayatın gizliliğini ihlal, verileri hukuka aykırı olarak verme veya ele geçirme ve hakaret suçlarını oluşturan eylemlerinden dolayı ayrı ayrı cezalandırılması gerektiği, TCK'nın 44. maddesinde düzenlenen fikri içtima hükmünün uygulanma koşullarının bulunmadığı" düşüncesiyle itirazın değişik gerekçe ile kabulü yönünde,

Üç Ceza Genel Kurulu Üyesi de; "İtirazın kabulüne karar verilmesi gerektiği" yönünde karşı oy kullanmışlardır.

SONUÇ:

Açıklanan nedenlerle;

1- Yargıtay Cumhuriyet Başsavcılığı itirazının REDDİNE,

2- Dosyanın, mahalline gönderilmek üzere Yargıtay Cumhuriyet Başsavcılığına TEVDİ EDİLMESİNE, 09.05.2019 tarihinde yapılan müzakerede oy çokluğuyla karar verildi.

Yargıtay Kararı - Ceza Genel Kurulu (E. 2012/1510)

Yargıtay CGK., E. 2012/1510 K. 2014/331 T. 17.6.2014

Esas No.: 2012/1510

Karar No.: 2014/331

Karar Tarihi: 17.06.2014

Kararı veren

Yargıtay Dairesi: 12. Ceza Dairesi

Mahkemesi: BİLECİK Asliye Ceza

Günü: 03.07.2007

Sayısı: 154-232

Özel hayatın gizliliğini ihlal suçundan sanık B.G.'ün 5237 sayılı TCK'nun 134/2, 62 ve 52. maddeleri uyarınca 6.000 Lira adli para cezası ile cezalandırılmasına ilişkin, Bilecik Asliye Ceza Mahkemesince verilen 03.07.2007 gün ve 154-232 sayılı hükmün katılan vekili ve sanık müdafii tarafından temyiz edilmesi üzerine dosyayı inceleyen Yargıtay 12. Ceza Dairesince 15.05.2012 gün ve 20072-12126 sayı ile;

"...Köşe yazarı olarak çalışan katılanın, sanığın genel yayın yönetmenliğini yaptığı gazetede yazdığı köşesinde kullanılan fotoğrafının, katılanın rızası olmadan arkadaşlık sitesine konulması eyleminin, TCK'nın 136. maddesinde düzenlenen, kişisel verileri hukuka aykırı olarak yayma suçunu oluşturacağı, hukuki durumunun buna göre tayin ve takdiri gerektiği gözetilmeden, suç vasfında yanılığa düşülerek, yazılı şekilde karar verilmesi" isabetsizliğinden oyçokluğuyla bozulmasına karar verilmiş,

Daire Üyeleri M.A.ve A.Y.;

"Sanık hakkında TCK'nın 134. maddesi gereğince özel hayatın gizliliğini ihlalden kamu davası açılmış olup sanığın aynı madde gereğince mahkumiyetine dair hüküm, dairemizce eylemin verileri hukuka aykırı olarak yayma suçundan hüküm kurulması gerektiği gerekçesiyle bozulmuştur. Eylemin basın yoluyla hakaret olarak değerlendirilmesi gerektiğini düşündüğümüzden sayın çoğunluğun görüşüne katılmıyoruz.

1- Katılanın 'Son Nokta' isimli gazetede yazdığı köşe yazısı için verdiği resim, sanık tarafından M.Bilişim Hizmetlerine ait 'www.istanbul.net' isimli sosyal ağ platformu olarak hizmet veren sitede 'belkiba' rumuzuyla yayınlanmış, evli ve iki çocuklu olan katılan için bekar, aradığı cinsiyet erkek 24-29 yaşlarında, aradığı ilişki arkadaşlık ve sitede sorulan birçok soruya cevap şeklinde kendisini tanıtan ve aradığı kişide bulunmasını istediği özellikler yazılmıştır.

2- Profil 14.10.2006 tarihi saat 16.31 de oluşturulduğu ve 16.10.2006 tarihi saat 16.28 de ise yayından kaldırıldığı ve yapılan araştırmada sanığın e-postası üzerinden oluşturulduğu sübuta ermiştir.

3- Sanığın eyleminin TCK'nın 136. maddesindeki verileri hukuka aykırı olarak verme olarak değerlendirilmesi yapıldığında;

Türk Ceza Kanunu'nun 135. maddesinde kişisel verilerin hukuka aykırı olarak kaydedilmesi ve 136. maddesinde ise verileri hukuka aykırı olarak verme, yayma ve ele geçirme suçları düzenlenmiştir. Bugüne kadar kişisel verilerin neler olduğuna dair kanunun çıkarılmaması nedeniyle TCK'ndaki 135 ve 136. maddelerindeki hukuka aykırılığın hangi hallerde oluştuğuna ilişkin başvurulabilecek kapsayıcı bir kaynak ya da norm olmaması nedeniyle bu iki madde eksik norm sayılırlar. Belki zamanın ihtiyaçlarına cevap verecek 'Kişisel Verilerin Korunması Kanunu' Meclisten geçtiğinde bu 'çerçeve düzenleme' tamamlanmış olacaktır. Bununla beraber adı geçen ceza maddeleri yürürlükte olduğundan uygulanması sırasında çok dikkatli olunması gerekir. Doktrinde birçok tanım ve kapsam belirlemesi yapılmaktadır. Bu bilimsel görüşlerden hareketle kişisel verilerin hangileri olabileceğini belirlemek gerekir. Şu da bir gerçek ki bu verilerin tamamının da ceza normları ile korunması gerektiği düşünülmemelidir. Bu tasnifin esasını genel yaşam mahremiyetinden hareketle özel hayatın gizli alanını korumayı amaçlayan ve sağlayan bilgiler olarak anlamak gerekir.

Bilimsel görüşlerden hareketle kişisel verilerin neler olabileceğini şu başlıkları altında sınıflandırabiliriz.

a- Yaşam şekline ilişkin kişisel veriler: Kişilerin üçüncü kişiler tarafından ayırimcılığa uğramaması ve haysiyetinin korunmasıyla ilişkili olarak, dini inançları, cinsel tercihleri, etnik kökeni, suç geçmişi, politik eğilimleri ve kişisel özel aktivitelere ilişkin bilgiler bu bağlamda sayılabilecektir.

b- Ekonomik ve finansal kişisel veriler: Suçlular tarafından suistimale ve kimlik hırsızlığına hedef olmamak için kişinin mali varlığı, sahip olduğu hisse ve hesaplar, borçları, yaptığı alışverişler, kredi kartlarına ilişkin veriler. Ayrıca sayılan bu bilgiler ile kişinin nerede ve kimlerle bulunduğu, sağlık bilgilerine ilişkin bilgiler de ortaya çıkarılabileceğinden ve varlık bilgisinin toplumsal açıdan da özel sayılmasından dolayı önemi artmaktadır.

c- Bilişim alanına ilişkin kişisel veriler: e-postaların bizzat adresleri veya şifreleri, internet ortamında paylaşılan kişisel veriler mahrem olarak değerlendirilebilir. Bunun önemi şu bakımdan artmaktadır. İnternette gezinti yapan kişi birçok kişisel bilgileri paylaşmakta, bu bilgiler kayıt altına alınmakta, yine internet erişimine ilişkin iz kayıtlarının hizmet sağlayıcı ve sunucu sahipleri tarafından tutulabiliyor olması nedenleriyle artmaktadır.

d- Sağlıkla ilgili kişisel veriler: Sağlık verileri kişilerin iş güvenliğini, toplum içindeki statüsünü ve sigorta kapsamını etkileyen hassas bilgilerdir. Ayrıca sağlık verileri kişilerin sosyal yaşantısı ve psikolojik durumları hakkında bilgi edinilmesine neden olabilir. Biyometrik (Kişinin kendine özgü fiziksel veya biyolojik niteliklerine dayalı olarak insanların kimliğini tespit için dijital teknolojiden faydalanma bilimi) veriler de kişisel veriler arasındadır.

e- Politik kişisel veriler: Toplum içinde yaşayan kişilerin siyasi tercihleri toplum katmanları arasında bilinme halinde ayrımcılığa maruz kalma ihtimali bulunduğundan bu bilgilerde kişisel veridir.

4- Anayasanın 38/3 ve Türk Ceza Kanununun 2. maddesi suçta ve cezada kanunilik ilkesini düzenlemektedir. TCK'nın 2. maddesi 'Kanunun açıkça suç saymadığı bir fiil için kimseye ceza verilemez' hükmünü içermektedir. Madde metninden de açıkça anlaşıldığı gibi fiilin kanunda suç olarak gösterilmesi yetmez, bunun açık bir biçimde belirlenebilir olması gerekir. Suçların ve cezaların kanunda önceden açık ve anlaşılır bir şekilde düzenlenmesi gerekir ki, insanlar neyin suç olduğunu önceden kolayca bilebilsin ve davranışlarını buna göre ayarlayabilsinler.

5- Yukarıda açıklanan kişisel veri açıklamalarına bakıldığında sanığın eyleminin bu kapsamda değerlendirilemeyeceği, amacın katılanı toplum nazarında küçük düşürmeye ve ahlaksız göstermeye yönelik olduğu dikkate alındığında eylem TCK'nın 125/1, 2 ve 4. maddesi kapsamında hakaret suçunu oluşturmaktadır.

Aksine bir uygulamanın kabulü halinde paylaşım sitelerinde her gün onbinlerce kişisel sayfa ve profil oluşturanların eylemleri resen takip edilen suç haline gelir ki bütün yargı mesaisini buna harcarsa bile işin altından kalkamaz. Kaldı ki bu sayfaların oluşturulması dünyanın her ülkesinden yapılmakta, kimin yaptığı da çoğu zaman tespit edilememektedir.

6- Sonuç olarak eylem hakaret suçunu oluşturmakta ve katılanlar FSEK'nun ek 4. maddesinde öngörülen prosedür çerçevesinde haklarına tecavüzün durdurulmasını veya 5651 sayılı 'İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 9. maddesi gereğince içerik sağlayıcıya başvurarak sayfanın

kaldırılmasını isteyebileceklerdir. Nitekim dava konusu olayda da sanık oluşturduğu profili 48 saat sonra kaldırmıştır.

Tüm açıkladığımız bu nedenlerden dolayı çoğunluğun 2 numaralı bozma düşüncesine katılmıyoruz” görüşüyle karşıoy kullanmışlardır.

Yargıtay Cumhuriyet Başsavcılığı ise 28.08.2012 gün ve 39110 sayı ile;

“Sanık Belkis Gümüş hakkında 12. Ceza Dairesince Son Nokta Gazetesinde, köşe yazarı olarak çalışan katılanın, sanığın genel yayın yönetmenliğini yaptığı gazetede yazdığı köşesinde kullanılan fotoğrafının, katılanın rızası olmadan arkadaşlık sitesine konulması eyleminin, TCK’nın 136. maddesinde düzenlenen, kişisel verileri hukuka aykırı olarak yayma suçunu oluşturacağı, hukuki durumunun buna göre tayin ve takdiri gerektiği şeklinde yer olan bozma kararının hukuka aykırı nitelikte olduğu ve eylemin kişiyi tahkir edici, incitici ve şeref ve itibarını zedeleyici nitelikte olup basın yoluyla hakaret suçunu oluşturduğu kabul edilmelidir.

Bu itibarla sanık Belkis Gümüş hakkında verilen bozma kararının itirazen kaldırılarak sanığın eyleminin 5237 sayılı TCK'nun 125/1-2, 125/4 maddesinde yazılı basın yoluyla hakaret suçunu oluşturduğu gözönüne alınarak hükmün bu nedenlerle bozulmasına karar verilmesi gerekmektedir..." görüşüyle itiraz kanun yoluna başvurmuştur.

5271 sayılı CMK'nun 308. maddesi uyarınca inceleme yapan Yargıtay 12. Ceza Dairesince 19.11.2012 gün ve 27129-24456 sayı ile; itiraz nedenlerinin yerinde görülmediğinden bahisle Yargıtay Birinci Başkanlığına gönderilen dosya, Ceza Genel Kurulunca değerlendirilmiş ve açıklanan gerekçelerle karara bağlanmıştır.

Sanığın özel hayatın gizliliğini ihlal suçundan cezalandırılmasına karar verilen somut olayda, Özel Daire çoğunluğu ile Yargıtay Cumhuriyet Başsavcılığı arasında oluşan ve Ceza Genel Kurulunca çözümlenmesi gereken uyuşmazlık; sanığın genel yayın yönetmenliğini yaptığı gazetede köşe yazarı olarak çalışan katılanın, yazdığı köşesinde kullanılan fotoğrafın, katılanın rızası olmadan internetteki bir arkadaşlık sitesine erkek arkadaş aradığı şeklindeki bilgilerle birlikte konulması eyleminin, kişisel verileri hukuka aykırı olarak yayma suçunu mu yoksa hakaret suçunu mu oluşturduğunun belirlenmesine ilişkindir.

Ancak yapılan müzakerede bir kısım Genel Kurul Üyeleri tarafından, iddianamede hakaret suçunu oluşturabilecek bir anlatımın bulunmadığının ileri sürülmesi üzerine bu hususun Yargıtay İç Yönetmeliğinin 27. maddesi uyarınca öncelikle değerlendirilmesi gerekmiştir.

İddianamede hakaret suçunu oluşturabilecek bir anlatım olup olmadığı, başka bir ifadeyle hakaret suçundan açılan bir davanın bulunup bulunmadığı:

İncelenen dosya kapsamından;

Söke Cumhuriyet Başsavcılığınca sanık hakkında; "Şüpheli İbrahim'in Son Nokta isimli yerel gazetenin sahibi, şüpheli Belkıs'ın aynı gazetede genel yayın yönetmeni olduğu, müşteki Emine'nin de olay tarihinde aynı gazetede editör olarak çalıştığı, Belkıs'ın gazeteye ait dijital fotoğraf makinesiyle, gazetede ki köşesine koymak amacıyla müştekinin fotoğrafını çekerek kendi bilgisayarına attığı, ancak daha sonra bu fotoğrafı www.istanbul.net isimli bir özel arkadaşlık internet sitesine 14.10.2006 tarihinde verdiği, ertesi gün müştekinin bir akrabasının söz konusu sitede kendisinin resmini görerek haber verdiği, bunun üzerine Belkıs'ın, cep telefonundan müştekiye mesaj atarak özür dilediği ve bu işi İbrahim ile birlikte yaptıklarını dolaylı olarak söylediği, 16.10.2006 tarihinde şüpheli Belkıs'ın 'belkiba' rumuzlu üyeliğini sildiği dolayısıyla müştekinin resminin de bu tarihte silindiği, her iki şüphelinin evli bir kadın olan müştekiye ait resmi iki gün süreyle özel arkadaşlık hizmeti veren bir web sitesinde yayınlamak suretiyle özel hayatın gizliliğini ihlal suçunu işledikleri" açıklamasına yer verilen iddianame ile kamu davası açılırken, sevk maddelerinin "5237 sayılı TCK'nun 134/2 ve 53" olarak gösterildiği ve suçun özel hayatın gizliliğini ihlal olarak adlandırıldığı, yerel mahkemece bu suçtan mahkumiyet hükmü kurulduğu anlaşılmaktadır.

Ceza muhakemesi hukukumuzda mahkemelerce bir yargılama faaliyetinin yapılabilmesi ve hüküm kurulabilmesi için, yargılamaya konu edilecek eylemle ilgili, usulüne uygun olarak açılmış bir ceza davası bulunması gerekmektedir. 5271 sayılı Ceza Muhakemesi Kanununun 170/1. maddesi uyarınca ceza davası, dava açan belge niteliğindeki icra ceza mahkemesine verilen şikâyet dilekçesi, son soruşturmanın açılması kararı gibi istisnai hükümler dışında, kural olarak Cumhuriyet savcısı tarafından düzenlenecek bir iddianame ile açılır. Belirtilen kanunun 170. maddesinin 4. fıkrasında da; "İddianamede, yüklenen suçu oluşturan olaylar, mevcut delillerle ilişkilendirilerek açıklanır" düzenlemesine yer verilmiştir.

CMK'nun 225. maddesi uyarınca da; "Hüküm, ancak iddianamede unsurları gösterilen suça ilişkin fiil ve faili hakkında verilir. Mahkeme, fiilin nitelendirilmesinde iddia ve savunmalarla bağlı değildir". Bu düzenleme gereğince hangi fail ve fiili hakkında dava açılmış ise, ancak o fail ve fiili hakkında yargılama yapılarak hüküm verilebilecektir.

Anılan kanuni düzenlemelere göre, iddianamede açıklanan ve suç oluşturduğu iddia olunan eylemin dışına çıkılması, dolayısıyla davaya konu edilmeyen fiil veya olaydan dolayı yargılama yapılması ve açılmayan davadan hüküm kurulması kanuna açıkça aykırılık oluşturacaktır. Öğretide "davasız

yargılama olmaz" ve "yargılamanın sınırlılığı" olarak ifade edilen bu ilke uyarınca hâkim, ancak hakkında dava açılmış bir fiil ve kişi ile ilgili yargılama yapabilecek ve önüne getirilen somut uyuşmazlığı hukuki çözüme kavuşturacaktır.

Diğer taraftan CMK'nun 226. maddesinde ise; "Sanık, suçun hukukî niteliğinin değişmesinden önce haber verilip de savunmasını yapabilecek bir hâlde bulundurulmadıkça, iddianamede kanunî unsurları gösterilen suçun değindiği kanun hükmünden başkasıyla mahkûm edilemez.

Cezanın artırılmasını veya cezaya ek olarak güvenlik tedbirlerinin uygulanmasını gerektirecek hâller, ilk defa duruşma sırasında ortaya çıktığında aynı hüküm uygulanır.

Ek savunma verilmesini gerektiren hâllerde istem üzerine sanığa ek savunmasını hazırlaması için süre verilir.

Yukarıdaki fıkralarda yazılı bildirimler, varsa müdafie yapılır. Müdafii sanığa tanınan haklardan onun gibi yararlanır" hükmü getirilmiştir.

Soruşturma aşamasında elde ettiği delillerden ulaştığı sonuca göre iddianameyi hazırlamakla görevli iddia makamı, düzenlenen iddianame ile CMK'nun 225/1. maddesi uyarınca kovuşturma aşamasının sınırlarını belirlemektedir. Bu bakımdan iddianamede, yüklenen suçun unsurlarını oluşturan fiil/fiillerin nelerden ibaret olduğunun hiçbir tereddüte yer bırakmayacak biçimde açıklanması zorunludur. Böylelikle sanık; iddianameden üzerine atılı suçun ne olduğunu hiçbir şüpheye yer vermeyecek şekilde anlamalı, buna göre savunmasını yapabilmeli ve delillerini sunabilmelidir. CMK'nun 226. maddesindeki düzenlemeyle iddianamede anlatılan eylem değişmemiş olduğundan, kanun koyucu o eylemin hukuki niteliğinde değişiklik olmasını "yargılamanın sınırlılığı" ilkesine aykırı görmemiş, bu gibi hallerde sanığa ek savunma hakkı verilerek değişen suç niteliğine göre bir hüküm kurulmasına imkan sağlamıştır. Bu düzenlemenin bir sonucu olarak mahkeme, eylemin hangi suçu oluşturacağına ilişkin nitelendirmede iddia ve savunmayla bağlı değildir. Örneğin, iddianamede kasten öldürmeye teşebbüs olarak nitelendirilen eylemin kasten yaralama suçunu oluşturacağı görüşünde olan mahkemece, sanığa ek savunma hakkı da verilmek suretiyle bahse konu suçtan hüküm kurulabilecektir. İddianamede anlatılan ve kapsamı belirlenen olayın dışında bir fail ve fiilin yargılanması söz konusu olduğunda ise, suç duyurusunda bulunulması ve iddianame ile dava açılması halinde gerekli görülürse her iki iddianame ile açılan davaların birleştirilmesi yoluna gidilebilecektir.

Nitekim, Ceza Genel Kurulunun 18.02.2014 gün ve 274-78 ile 16.04.2013 gün ve 1307-151 sayılı kararları başta olmak üzere birçok kararında da aynı sonuca ulaşılmıştır.

Bu açıklamalar ışığında uyumsuzluk konusu değerlendirildiğinde;

Bilecik Cumhuriyet Başsavcılığınca düzenlenen iddianamede yargılamaya konu edilen olayın açıklanmasından sonra sanığın eyleminin özel hayatın gizliliğini ihlal suçu olarak vasıflandırılıp TCK'nun 134/2. maddesi uyarınca cezalandırılması talebiyle kamu davası açılan olayda, CMK'nun 225. maddesine göre hükmün iddianamede unsurları gösterilen suça ilişkin fiil ve faili hakkında verileceği ve mahkemenin, fiilin nitelendirilmesinde iddia ve savunmalarla bağlı olmadığı da gözönüne alındığında, iddianamedeki anlatımın gerek TCK'nun 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak yayma, gerekse aynı kanununun 125. maddesinde düzenlenen hakaret suçlarını da oluşturabilecek şekilde yapıldığı kabul edilmelidir.

Önsorunun çözümlenmesinden sonra sanığın genel yayın yönetmenliğini yaptığı gazetede köşe yazarı olarak çalışan katılanın, yazdığı köşesinde kullanılan fotoğrafın, katılanın rızası olmadan internetteki bir arkadaşlık sitesine erkek arkadaş aradığı şeklindeki bilgilerle birlikte konulması eyleminin kişisel verileri hukuka aykırı olarak yayma suçunu mu, yoksa hakaret suçunu mu oluşturduğunun belirlenmesine gelince;

İncelenen dosya kapsamından;

Sanığın Bilecik ilinde yayınlanmakta olan "Son Nokta" isimli yerel gazetenin genel yayın yönetmeni olduğu, katılanın ise aynı gazetede köşe yazarlığı yaptığı, sanığın gazeteye ait dijital fotoğraf makinesiyle gazetede köşesine koymak amacıyla katılanın fotoğrafını çekerek bilgisayara kaydettiği, katılanın gazetede köşe yazılarında bu fotoğrafını kullandığı, sanığın bilgisayarda kayıtlı olan bu fotoğrafı daha sonra internetteki özel bir arkadaşlık sitesine 14.10.2006 tarihinde kimlik, adres ve telefon bilgilerini vermeksizin "belkiba" rumuzunu kullanarak koyduğu, katılanın 24-29 yaş arasında erkek arkadaş aradığı bilgisinin yazıldığı, ertesi gün bir yakınının söz konusu sitede kendisinin resmini görerek haber vermesi üzerine katılanın olaydan haberdar olduğu, olayın ortaya çıkması üzerine sanığın cep telefonundan katılana kısa mesaj göndererek özür dilediği, 16.10.2006 tarihinde sanığın "belkiba" rumuzlu üyeliği sildiği, katılanın sanıktan şikayetçi olduğu anlaşılmaktadır.

Anayasamızın "Özel hayatın gizliliği" başlıklı 20. maddesinin birinci fıkrası; "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz" şeklinde olup, maddeye 13.05.2010 gün ve 27580 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren 5982 sayılı Kanununun 2. maddesiyle; "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları

doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir" biçimindeki üçüncü fıkra eklenmiştir.

Avrupa İnsan Hakları Sözleşmesinin "Özel ve aile hayatına saygı hakkı" başlıklı 8. maddesinde de; "1-Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

2-Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir" hükmü bulunmaktadır.

5237 sayılı TCK'nun "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" bölümünde "Kişisel verilerin kaydedilmesi" başlıklı 135. maddesi; "(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.

(2) Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır",

"Verileri hukuka aykırı olarak verme veya ele geçirme" başlıklı 136. maddesi ise; "(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır" şeklinde düzenlenmiş, 21.02.2014 gün ve 6526 sayılı Kanunla da 135. maddesinin birinci fıkrasındaki suçun cezasının alt sınırı "bir yıla", 136. maddesindeki suçun cezanın alt sınırı ise "iki yıla" çıkartılmıştır.

Bu maddelerde geçen ve suçun konusunu oluşturan kişisel veriden ne anlaşılması gerektiğine ilişkin yürürlükte bulunan kanunlarda bir tanım yer almamaktadır. Bununla birlikte TCK'nun 135. maddesinin gerekçesinde; "Gerçek kişiyle ilgili her türlü bilgi, kişisel veri olarak kabul edilmelidir. Söz konusu suç tanımında kişisel verilerin bilgisayar ortamında veya kağıt üzerinde kayda alınması arasında bir ayırım gözetilmemiştir" denilmiş, Anayasamızın 20/3. maddesi uyarınca çıkarılması gereken ancak henüz kanunlaşmamış olan Kişisel Verilerin Korunması Kanun Tasarısının 3. maddesinde ise; "Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ...ifade eder" şeklinde tanım yapılmış, taslak maddenin gerekçesinde ise; "Kişisel veriler, sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin aklî, psikolojik, fizikî, kültürel, ekonomik, sosyal ve sair özelliklerine ilişkin

verilerdir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilecek özellikleri nedeniyle kişisel verilerdir" açıklamasına yer verilmiştir.

24.07.2012 gün ve 28363 sayılı Resmi Gazetede yayımlanan ve bu tarihten 6 ay sonra yürürlüğe giren Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkındaki Yönetmeliğin 3/1-h maddesinde kişisel veri; "belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler" olarak tanımlanmıştır.

28.01.1981 tarihli ve 108 nolu Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Uluslararası Sözleşme'nin 2/a maddesinde ise; "Kişisel nitelikteki veriler; kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm bilgileri ifade eder" denilmiş, 1995 tarihinde yürürlüğe giren Avrupa Topluluğu Veri Koruma Yönergesinin 2. maddesinde de kişisel veri; "doğrudan doğruya ya da dolaylı olarak bir gerçek kişi ile ilintili olabilecek ve onu belirlenebilir kılacak her türlü bilgi" olarak belirtilmiştir.

Öğretide de kişisel verilere ilişkin; "Bireyin şahsi, mesleki ve ailevi özelliklerini gösteren, o bireyi diğer bireylerden ayırmaya ve niteliklerini ortaya koymaya elverişli hertürlü bilgiyi ifade eder" (Ersan Şen, Türk Ceza Kanunu Yorumu, Vedat Kitapçılık, İstanbul, 2006, s.601), "Bir kişinin adı ve soyadı, yaşı, cinsiyeti, doğum yeri, dini, TC kimlik numarası, cinsel hayatı, cep telefonu numarası, medeni durumu, ailesi, işi, geliri, borçları, adresi, geçirdiği hastalıklar, özel zevkleri ve buna benzer bilgileri" (Volkan Sırabaşı, İnternet ve Radyo- Televizyon Aracılığıyla Kişilik Haklarına Tecavüz, Adalet Yayınevi, Ankara, 2007, 2. Bası, s.195) şeklinde tanımlar yapılmıştır.

Kişilerin, sadece insan olması ve toplumdaki yeri, bazı değerleri kişisel veri haline getirmektedir, örneğin; kişinin adı, adresi, kimlik bilgileri, medeni durumu vb... Bunun yanında teknolojik gelişmeler nedeniyle gittikçe karmaşıklaşan toplum hayatındaki bir takım bilgiler de kişisel veri haline gelmiştir, örneğin; vatandaşlık numarası, banka hesap numarası, telefon numarası, elektronik posta adresi ve şifresi vb... Dolayısıyla farklı gruplandırmalar bulunmakla birlikte kişisel verilerin iki başlık altında toplanması mümkündür. Birinci grupta; insanın varoluşundan kaynaklanan kişiliğine ait bilgiler, ikinci grupta ise; teknolojinin gelişmesiyle insanın modern toplumda yer alması nedeniyle

kendisine verilen ya da çeşitli hizmetlere ulaşmasında kullanılan bilgiler yer almaktadır. Ancak her iki grupta yer alan bilgilerin de kişisel veri olarak hukuk düzenindeki değeri ve korunmaları açısından bir fark bulunmamaktadır. (Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayınevi, Ankara, 2014, 4. bası, s.577)

TCK'nun 136. maddesinde tıpkı 135. maddesinde olduğu gibi korunan hukuki değer genel olarak kişilerin özel hayatı ve hayatın gizli alanı, özeldense kişisel verilerdir. Bu düzenlemeler ile tüm kişisel veriler koruma altına alındığından kişisel verilerin mutlaka gizli olması zorunlu değildir. Gizli olmayan ve herkes tarafından bilinen kişisel veriler de hukuka aykırı eylemlere karşı korunmalıdır. Zira kişisel verilerin korunmasına ilişkin suçlarda korunan hukuki değer "sır" olmayıp, verinin ilgilisi olan kişinin kişilik haklarıdır.(Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayınevi, Ankara, 2014, 4. bası, s.579, 588-593)

TCK'nun 136. maddesindeki "verileri hukuka aykırı olarak verme veya ele geçirme" suçu, seçimlik hareketli bir suç olarak düzenlenmiştir. Hukuka aykırı olarak kişisel verilerin başkasına verilmesi, kişisel verilerin yayılması ve kişisel verilerin ele geçirilmesi şeklindeki seçimlik hareketlerin birinin gerçekleştirilmesiyle suç işlenmiş olacaktır.

"Kişisel verileri bir başkasına verme" seçimlik hareketinde, maddede geçen "başkası" gerçek bir kişi olabileceği gibi tüzel kişi de olabilecek, veriler bu kişilere elden, posta ya da internet üzerinden elektronik posta ile vb. şekillerde verilebilecektir. Türk Dil Kurumu Büyük Türkçe Sözlüğünde "vermek"; "üzerinde, elinde veya yakınında olan bir şeyi birisine erdirtmek, iletmek, düşünce veya bilgi anlatan şeyleri başkalarına iletmek, bildirmek" şeklinde açıklanmıştır. Bu seçimlik harekette verilerin hukuka uygun ya da aykırı yöntemle elde edilmiş olmasının önemi bulunmamakta olup, önemli olan husus verme eyleminin hukuka aykırı olmasıdır.

"Kişisel verileri yayma" seçimlik hareketi de çeşitli şekillerde gerçekleştirilebilecektir; internet üzerindeki bir web sitesinde kişisel verileri yayınlamak, birçok kişiye elektronik posta ile ya da telefondan kısa mesajla göndermek, yazılı ya da görsel medyada yayınlamak gibi... Türk Dil Kurumu Büyük Türkçe Sözlüğünde "yaymak"; "birçok kimseye duyurmak, çevreye dağılmasına sebep olmak" olarak açıklanmıştır.

"Kişisel verilerin ele geçirilmesi" seçimlik hareketi ise; kişisel verilerin kayıtlı olduğu belgelerin alınması ya da kayıtlı olduğu bilişim sisteminden ele geçirilmesi vb... şekillerde gerçekleştirilebilecektir. Ele geçirme fiili, başkasının hakimiyeti altında bulunan bir kişisel verinin, failin hakimiyeti altına girmesi ile gerçekleşmiş olacaktır.

Bu suçta herhangi bir neticenin gerçekleşmesi aranmadığından maddede sayılan seçimlik hareketlerin yapılmasıyla suç oluşacaktır. Bu açıdan TCK'nun 136. maddesindeki "verileri hukuka aykırı olarak verme veya ele geçirme" soyut bir tehlike suçudur.

Uyuşmazlığın çözümlenmesi açısından, kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçundaki hukuka uygunluk nedenleri üzerinde de durulmalıdır.

5237 sayılı TCK'nun esas aldığı ve suçun bir haksızlık olarak tanımlandığı suç teorisinde suçun unsurları; maddi unsurlar, manevi unsurlar ve hukuka aykırılık unsuru olmak üzere üç başlık altında toplanmaktadır.

Uyuşmazlıkla yakından ilgili olan hukuka aykırılık, suçu oluşturan haksızlığın niteliği olup hukuka aykırılık ile kastedilen husus fiilin hukuk sistemiyle çatışması ve hukuk sistemine aykırı olmasıdır. 5237 sayılı Kanunda bazı suç tanımlarında "hukuka aykırı olarak", "hukuka aykırı başka bir davranışla", "hukuka aykırı diğer davranışlarla", "hukuka aykırı yolla", "hukuka aykırı yollarla" gibi ifadeler yer verilmiştir. Bu ifadelerin geçtiği suçlarda failin, işlediği fiilin hukuka aykırı olduğunu bilmesi, yani bu konuda doğrudan kastla hareket etmesi gerekmektedir.

5237 sayılı TCK'nda hukuka uygunluk sebepleri;

a- Kanunun hükmünü yerine getirme (m.24/1)

b- Meşru savunma (m.25/1)

c- İlgilinin rızası (m.26/2)

d- Hakkın kullanılması (m.26/1)

Olarak kabul edilmiştir.

Sayılan hukuka uygunluk nedenlerinden konumuzla ilgili olan kanunun hükmünü yerine getirme, ilgilinin rızası ve hakkın kullanılması hususlarının ayrıntılı olarak ele alınmasında fayda bulunmaktadır. Nitekim TCK'nun 135. maddesinin gerekçesinde; "Bu suçun oluşabilmesi için, kişisel verilerin hukuka aykırı bir şekilde kayda alınması gerekir. Kişinin rızası ile kendisiyle ilgili bilgilerin kayda alınmasının suç oluşturmayacağı muhakkaktır. Belirli nitelikteki kişisel verilerin kayda alınması kanun hükmünün gereği olarak yapılmaktadır. Bu bakımdan, çeşitli kamu kurumlarında verilen kamu hizmetinin gereği olarak kişilerle ilgili bazı bilgiler, ilgili kanun hükümlerine istinaden kayda alınmaktadırlar. Bu durumlarda, söz konusu suç oluşmayacaktır" denilmektedir.

TCK'nun 24. maddesinin birinci fıkrasındaki; "Kanunun hükmünü yerine getiren kimseye ceza verilmez" şeklindeki düzenleme ile kanunla verilen görevin yerine getirilmesi bir hukuka uygunluk

nedeni olarak öngörülmüştür. Maddede geçen kanun kelimesinden pozitif hukuk metinleri yani yazılı hukuk kuralları anlaşılmalıdır. Kanun hükmünün yerine getirilmesinde, belirli konularda kişiye verilen yetki aynı zamanda o kişinin görevidir. Bu nedenle sözü edilen hukuka uygunluk nedenini görevin ifası kapsamında değerlendirmek gerekir. Zira bir davranışın hukuka uygun olup olmadığını belirlerken yerine getirilen görevin mahiyeti gözönünde bulundurulmalıdır. Kanunun hükmünü yerine getirme çoğunlukla kamu görevlilerine ait olmakla birlikte bu görevin kamu görevlisi olmayan kişilere de verilmesi mümkündür. Örneğin; kolluk görevlilerinin dışında CMK'nun 90/1. maddesinde yazılı şartlar gerçekleştiğinde herkesin yakalama yetkisi bulunmaktadır. (İzzet Özgenç, Türk Ceza Hukuku Genel Hükümler, 9. bası, Ankara, 2013, s. 301-302; Mahmut Koca-İlhan Üzülmöz, Türk Ceza Hukuku Genel Hükümler, 6. bası, Ankara, 2013, s. 261-263)

Yazılı hukuk kuralları tarafından açıkça verilmiş bir yetki olmadığı sürece, kişisel verilerin kaydedilmesinde hukuka uygunluktan bahsedilemeyecek ve bu fiil suç teşkil edecektir.

Bir diğer hukuka uygunluk nedeni olan ilgilinin rızası, 5237 sayılı TCK'nun "Hakkın kullanılması ve ilgilinin rızası" başlıklı 26/2. maddesinde; "Kişinin üzerinde mutlak surette tasarruf edebileceği bir hakkına ilişkin olmak üzere, açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez" şeklindeki düzenleme ile hüküm altına alınmıştır. Sözü edilen hukuka uygunluk nedeninin doğabilmesi, rızanın kişinin üzerinde mutlak surette tasarruf edebileceği bir hakka ilişkin olmasına ve kişinin bu hakla ilgili olarak rıza açıklama ehliyetinin bulunmasına bağlıdır. Yine rızanın bir hukuka uygunluk nedeni olabilmesi için fiilin işlenmesinden önce ve en geç işlendiği sırada mevcut olması gerekir. Fiilin işlendiği sırada olmayıp sonradan ortaya çıkan rıza bir hukuka uygunluk nedeni değildir. (İzzet Özgenç, Türk Ceza Hukuku Genel Hükümler, 9. bası, Ankara, 2013, s. 285 vd.; Mahmut Koca-İlhan Üzülmöz, Türk Ceza Hukuku Genel Hükümler, 6. bası, Ankara, 2013, s. 252 vd.)

Konumuzla ilgili son hukuka uygunluk nedeni olan hakkın kullanılmasına gelince; basın hürriyeti Anayasamızın 28. maddesinde; "Basın hürdür, sansür edilemez. Basımevi kurmak izin alma ve mali teminat yatırma şartına bağlanamaz.

Devlet, basın ve haber alma hürriyetlerini sağlayacak tedbirleri alır.

Basın hürriyetinin sınırlanmasında, Anayasanın 26 ve 27 nci maddeleri hükümleri uygulanır..." şeklinde düzenlenmiş, maddenin atf yaptığı "Düşünceyi açıklama ve yayma hürriyeti" başlıklı 26. maddede; "Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet resmi makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Bu fıkra hükmü, radyo, televizyon, sinema veya benzeri yollarla yapılan yayımların izin sistemine bağlanmasına engel değildir.

Bu hürriyetlerin kullanılması, millî güvenlik, kamu düzeni, kamu güvenliği, Cumhuriyetin temel nitelikleri ve Devletin ülkesi ve milleti ile bölünmez bütünlüğünün korunması, suçların önlenmesi, suçluların cezalandırılması, Devlet sırrı olarak usulünce belirtilmiş bilgilerin açıklanmaması, başkalarının şöhret veya haklarının, özel ve aile hayatlarının yahut kanunun öngördüğü meslek sırlarının korunması veya yargılama görevinin gereğine uygun olarak yerine getirilmesi amaçlarıyla sınırlanabilir.

Haber ve düşünceleri yayma araçlarının kullanılmasına ilişkin düzenleyici hükümler, bunların yayımını engellemek kaydıyla, düşünceyi açıklama ve yayma hürriyetinin sınırlanması sayılmaz.

Düşünceyi açıklama ve yayma hürriyetinin kullanılmasında uygulanacak şekil, şart ve usuller kanunla düzenlenir" hükmüne yer verilmiş,

Avrupa İnsan Hakları Sözleşmesinin "İfade özgürlüğü" başlıklı 10. maddesinde de;

"1-Herkes ifade özgürlüğü hakkına sahiptir. Bu hak, kamu makamlarının müdahalesi olmaksızın ve ülke sınırları gözetilmeksizin, kanaat özgürlüğünü ve haber ve görüş alma ve de verme özgürlüğünü de kapsar. Bu madde, Devletlerin radyo, televizyon ve sinema işletmelerini bir izin rejimine tabi tutmalarına engel değildir.

2- Görev ve sorumluluklar da yükleyen bu özgürlüklerin kullanılması, yasayla öngörülen ve demokratik bir toplumda ulusal güvenliğin, toprak bütünlüğünün veya kamu güvenliğinin korunması, kamu düzeninin sağlanması ve suç işlenmesinin önlenmesi, sağlığın veya ahlakın, başkalarının şöhret ve haklarının korunması, gizli bilgilerin yayılmasının önlenmesi veya yargı erkinin yetki ve tarafsızlığının güvence altına alınması için gerekli olan bazı formaliteler, koşullar, sınırlamalar veya yaptırımlara tabi tutulabilir" denilmiştir.

Basın özgürlüğü, 26.06.2004 gün ve 25504 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren 5187 sayılı Basın Kanununun 3. maddesinde; "Basın özgürdür. Bu özgürlük; bilgi edinme, yayma, eleştirme, yorumlama ve eser yaratma haklarını içerir.

Basın özgürlüğünün kullanılması ancak demokratik bir toplumun gereklerine uygun olarak; başkalarının şöhret ve haklarının, toplum sağlığının ve ahlâkının, millî güvenlik, kamu düzeni, kamu güvenliği ve toprak bütünlüğünün korunması, Devlet sırlarının açıklanmasının veya suç işlenmesinin önlenmesi, yargı gücünün otorite ve tarafsızlığının sağlanması amacıyla sınırlanabilir" şeklinde düzenleme altına alınmış ve sınırları çizilmek istenilmiştir.

Ceza Genel Kurulunun 20.03.2007 gün ve 65-70 sayılı kararında da belirtildiği gibi; geneli ilgilendiren ya da ilgilendirmesi gereken tüm olaylar hakkında, halkı objektif ve gerçekleri yansıtacak biçimde

aydınlatmak, çeşitli sorunlar üzerinde kamuoyunu düşünmeye çağırarak tartışmalar açmak, onu toplumsal ve siyasal oluşumlar üzerinde doğru ve gerçeğe uygun bilgilerle donatmak, yöneticileri eleştirmek, uyararak ve bu yöntemlerle denetlemek, ayrıca içinde yaşadığı toplumun ve tüm insanlığın sorunları konusunda bireyi bilinçlendirmek durumunda olan basına, bu ödevlerini yerine getirirken ihtiyaç duyacağı bir kısım haklar da tanınmıştır. Bunlar; bilgi edinme, yayma, eleştirme, yorumlama ve eser ortaya koyma haklarıdır.

Temelini Avrupa İnsan Hakları Sözleşmesinin 10. maddesi ile Anayasa'nın 28. vd. maddelerinden alan ve 5187 sayılı Basın Kanununun 3. maddesinde düzenlenen basın özgürlüğü ve bu kapsamda bilgi edinme, yayma, eleştirme, yorumlama ve eser ortaya koyma hakkı, TCK'nun 25. maddenin birinci fıkrasında; "Hakkını kullanan kimseye ceza verilmez" düzenlemesi kapsamında bir hukuka uygunluk nedenidir. Ancak habere ulaşma, haberi yorumlama ve eleştirme ile haberi kamuya ulaştırmayı kapsayan bu hakkın hukuka uygunluk nedeni olarak kabul edilebilmesi için; haberin gerçek ve güncel olması, haberin kamuyu ilgilendirmesi yani kamuoyunun haberi öğrenmekte menfaatinin bulunması ve haber ile haberin veriliş şeklinin uyumlu olması gereklidir. (Hamide Zafer, Ceza Hukuku Genel Hükümler, Beta Yayınevi, İstanbul, 2013, 3. bası, s.323; Nur Centel, Hamide Zafer, Özlem Çakmut, Türk Ceza Hukukuna Giriş, Beta Yayınevi, İstanbul, 2010, 6. bası, s.336-338; Hakan Hakeri, Ceza Hukuku Genel Hükümler, Adalet Yayınevi, Ankara, 2011, 12. bası, s.279-282). Nitekim Ceza Genel Kurulunun 24.02.1998 gün ve 386-52 sayılı kararında da aynı hususlara vurgu yapılmıştır.

Uyuşmazlıkla ilgili olarak ele alınması gereken diğer suç olan hakaret, 5237 sayılı TCK'nun 125. maddesinde; "(1) Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran kişi, üç aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Mağdurun gıyabında hakaretin cezalandırılabilmesi için fiilin en az üç kişiyle ihtilâl ederek işlenmesi gerekir.

(2) Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi hâlinde, yukarıdaki fıkra da belirtilen cezaya hükmolunur.

(3) Hakaret suçunun;

a) Kamu görevlisine karşı görevinden dolayı,

b) Dinî, siyasî, sosyal, felsefi inanç, düşünce ve kanaatlerini açıklamasından, değiştirmesinden, yaymaya çalışmasından, mensup olduğu dinin emir ve yasaklarına uygun davranmasından dolayı,

c) Kişinin mensup bulunduğu dine göre kutsal sayılan değerlerden bahisle,

İşlenmesi hâlinde, cezanın alt sınırı bir yıldan az olamaz.

(4) Hakaretin alenen işlenmesi halinde ceza altıda biri oranında artırılır.

(5) Kurul hâlinde çalışan kamu görevlilerine görevlerinden dolayı hakaret edilmesi hâlinde suç, kurulu oluşturan üyelere karşı işlenmiş sayılır. Ancak, bu durumda zincirleme suça ilişkin madde hükümleri uygulanır" şeklinde düzenlenmiştir.

Maddenin birinci fıkrasında hakaret suçunun temel şekli, üçüncü ve dördüncü fıkralarında ise nitelikli halleri düzenlenmiş, madde gerekçesinde de; "Hakaret fiillerinin cezalandırılmasıyla korunan hukuki değer, kişilerin şeref, haysiyet ve namusu, toplum içindeki itibarı, diğer fertler nezdindeki saygınlığıdır" açıklaması yapılmıştır. Buna göre, suçun konusu kişilerin onur, şeref ve saygınlığı olup, somut bir fiil veya olgu isnat etme ya da sövme suretiyle kişilerin onur, şeref ve saygınlığına saldırma eylemi hakaret suçunu oluşturacaktır.

Ceza Genel Kurulunun 27.10.2009 gün ve 196-248 ile 14.10.2008 gün ve 170-220 sayılı kararlarında da belirtildiği üzere; 5237 sayılı TCK'nda, 765 sayılı Kanundaki hakaret ve sövme suçu ayrımı kaldırılmıştır. Hakaret fiillerinin cezalandırılmasıyla korunan hukuki değer, kişilerin şeref, haysiyet ve namusu, toplum içindeki itibarı, diğer fertler nezdindeki saygınlığı olduğundan, bu suçun oluşabilmesi için, davranışın kişiyi küçük düşürmeye matuf olarak gerçekleştirilmesi gerekmektedir. Somut bir fiil ya da olgu isnat etmek veya sövmek şeklindeki seçimlik hareketlerden biri ile gerçekleştirilen eylem, bireyin onur, şeref ve saygınlığını rencide edebilecek nitelikte ise hakaret suçu oluşacaktır.

Son olarak uyuşmazlığın çözümü açısından fikri içtima üzerinde de durulmalıdır.

5237 sayılı TCK'nun hazırlanmasında "kaç fiil varsa o kadar suç, kaç suç varsa o kadar ceza vardır" ilkesi esas alınmış, dolayısıyla da gerçek içtima kuralı benimsenmiştir. Nitekim Adalet Komisyonu raporunda bu husus; "Ceza hukukunun temel kurallarından birisi, 'kaç fiil varsa o kadar suç, kaç suç varsa o kadar ceza vardır' şeklinde ifade edilmektedir. Bunun istisnaları, suçların içtimaı bölümünde belirlenmiştir. Bu istisnalar dışında, işlenen her bir suçla ilgili olarak ayrı ayrı cezaya hükmedilecektir. Böylece verilen her bir ceza, bağımsızlığını koruyacaktır" şeklinde ifade edilmiştir (TBMM Adalet Komisyonu'nun 03.08.2004 gün ve 1/593-60 sayılı Raporu). Bu kuralın istisnaları ise, 5237 sayılı TCK'nun "suçların içtimaı" bölümünde, 42 (bileşik suç), 43 (zincirleme suç) ve 44. (fikri içtima) maddelerinde düzenlenmiştir.

765 sayılı TCK'nda, aynı nev'iden fikri içtima ile farklı nev'iden fikri içtima tek madde halinde ve kanunun 79. maddesinde düzenlenmiş iken, 5237 sayılı TCK'nda bu iki hal birbirinden ayrılarak, aynı

nev'iden fikri içtima, zincirleme suçun düzenlendiği 43. maddenin 2. fıkrasında, farklı nev'iden fikri içtima ise kanunun 44. maddesinde düzenlenmiştir.

Farklı neviden fikri içtima 5237 sayılı Kanunun 44. maddesinde; "İşlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır" şeklinde düzenlenmiş olup, hükmün uygulanabilmesi için işlenen bir fiille birden fazla farklı suçun oluşması gerekmektedir.

Kanun koyucu, işlediği bir fiille birden fazla farklı suçu işleyen failin, fiilin tek olması nedeniyle en ağır ceza ile cezalandırılmasını yeterli görmüş, bu şekilde "non bis in idem" kuralı gereğince bir fiilden dolayı kişinin birden fazla cezalandırılmasının da önüne geçilmesini amaçlamış, "erime sistemini" benimsemek suretiyle, bu suçlardan en ağırının cezasının verilmesi ile yetinilmesini tercih etmiştir.

Bu bağlamda, "tek fiil" veya "bir fiil"den ne anlaşılması gerektiğinin de değerlendirilmesi gerekmektedir. Doğal anlamda gerçekleştirilen her bedeni hareket ayrı bir hareketi oluşturmakta ise de, hukuki anlamda hareketin tek olması ile ifade edilmek istenen husus, doğal anlamda birden fazla hareket bulursa dahi, bu hareketlerin, hukuki nedenlerden dolayı değerlendirmede birlik oluşturması suretiyle tek hareket kabulüdür. Fikri içtimada da, fiil ya da hareketin tek olması, doğal anlamda değil hukuksal anlamda tekliği ifade etmektedir. Bir kısım suçların işlenmesi sırasında doğal olarak birden fazla hareket yapılmakta ise de, ortaya konulan bu davranışlar suçun kanuni tanımında yer alan hukuki anlamdaki "tek bir fiili" oluşturmaktadır. (Mahmut Koca-İlhan Üzülmöz, Türk Ceza Hukuku Genel Hükümler, 6. Bası, Ankara, 2013, s.484 ve 495)

5237 sayılı TCK'nun genel hükümleri arasında yer alan fikri içtima kuralları, şartlarının bulunması halinde kural olarak her suç için uygulanabilir ise de, kanun koyucunun açıkça istisna öngördüğü hallerde bu kuralın uygulanma ihtimali bulunmamaktadır. Nitekim TCK'nun 212. maddesinde, sahte resmi veya özel belgenin bir başka suçun işlenmesi sırasında kullanılması halinde, hem sahtecilik hem de ilgili suçtan dolayı ayrı ayrı cezaya hükmolunacağı belirtilerek, açıkça fikri içtima hükümlerinin uygulanması engellenmiştir.

Görüldüğü gibi, kanuni istisnalar dışında, hukuki anlamda tek bir fiille birden fazla farklı suçun işlenmesi halinde, bu suçlardan en ağır cezayı gerektirenin cezasına hükmolunması kanun gereği olup, suçların olası kastla veya doğrudan kastla işlenmiş olması da varılan bu sonucu değiştirmeyecektir.

Bu açıklamalar ışığında uyuşmazlık konusu değerlendirildiğinde;

TCK'nun 135 ve 136. maddelerindeki kişisel verilerin korunmasına ilişkin düzenlemelerde sadece sır niteliğinde kişisel verilerin korunacağına ilişkin bir hükmün bulunmaması ve aksine 135. maddenin gerekçesinde gerçek kişiyle ilgili her türlü bilginin kişisel veri olarak kabul edilmesi gerektiğinin belirtilmesi karşısında, her türlü kişisel verinin hukuka aykırı olarak başkasına verilmesi, yayılması ve ele geçirilmesi fiillerinin kanunun 136. maddesindeki suç oluşturduğu kabul edilmelidir. Bu kapsamda somut olayda, sanığın genel yayın yönetmenliğini yaptığı gazetede köşe yazarı olarak çalışan katılanın yazdığı köşesinde kullanılan fotoğrafın, hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle sanık tarafından internetteki özel bir arkadaşlık sitesine kimlik, adres ve telefon bilgileri verilmeksizin ve erkek arkadaşı aradığı açıklamasıyla konulması eylemi, TCK'nun 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak yayma suçunu oluşturmaktadır.

Bununla birlikte sanığın eylemi, aynı zamanda katılanın onur, şeref ve saygınlığını rencide edebilecek nitelikte olması nedeniyle TCK'nun 125. maddesinin birinci ve dördüncü fıkrası uyarınca alenen hakaret suçunu da oluşturmaktadır.

Bu nedenle hukuki anlamda tek fiil sayılması gereken eylem ile hem TCK'nun 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak yayma suçu, hem de aynı kanunun 125/1-4 maddesinde düzenlenen alenen hakaret suçu olduğundan, sanık hakkında 5237 sayılı TCK'nun 44. maddesinde farklı neviden fikri içtima hükümlerinin uygulanması ve oluşan suçlardan en ağır cezayı gerektiren kişisel verileri hukuka aykırı olarak yayma suçundan sanığa ceza tayin edilmesi gerekmektedir.

Bu itibarla, sanığın eyleminin TCK'nun 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak yayma suçunu oluşturacağını kabul eden Özel Daire çoğunluğunun kararı, sonucu itibarıyla isabetli olduğundan itirazın reddine karar verilmelidir.

Eylemin nitelendirilmesine ilişkin uyuşmazlık yönünden çoğunluk görüşüne katılmayan Genel Kurul Üyesi D. Kahveci, M. Albayrak, M. Sarıçam, S. Sönmez ve M. Simavlı; "Sanık hakkında TCK'nun 134. maddesi gereğince özel hayatın gizliliğini ihlal suçundan kamu davası açılmış, sanığın aynı madde gereğince mahkûmiyetine dair hüküm, 12. Ceza Dairesince eylemin kişisel verileri hukuka aykırı olarak yayma suçundan (TCK m.136) hüküm kurulması gerektiği gerekçesiyle bozulmuş olup Yargıtay Cumhuriyet Başsavcılığının eylemin basın yoluyla hakaret olarak değerlendirilmesi gerektiğine dair itirazı reddeden Ceza Genel Kurulunun çoğunluk görüşlerine aşağıdaki gerekçelerle katılmıyoruz.

İtiraz gerekçelerimiz; Türk Ceza Kanunu'nda kişisel verilerle ilgili bir tanım ve sınırlandırmanın yapılmaması nedeniyle kişisel verilerle ilgili maddeler suçta ve cezada kanunilik ilkesini ihlal ettiğinden Anayasa'ya aykırı oldukları, bu itirazın ciddi bulunmaması nedeniyle kişisel veri tanımının sınırlarının Yüksek Ceza Genel Kurulu kararıyla çizilmesi gerektiği ve son olarak ta eylemin basın yoluyla hakaret suçunu oluşturacağı ana başlıklarında olacaktır.

Bunlar;

1-Yürürlükteki mevzuatta kişisel veri tanımının yapılmadığı gözetildiğinde kişisel verilerle ilgili suçların düzenlendiği TCK'nın 135 ve 136. maddeleri suçta ve cezada kanunilik ve belirlilik (açıklık) ilkesine uymadığından Anayasa'ya aykırıdır. Kişisel verilerle ilgili suç düzenlemeleri ilk olarak 01 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı TCK'nın 135, 136 ve 138. maddeleri ile ceza mevzuatımıza girmiştir. TCK'nın 135. maddesinde kişisel verilerin kaydedilmesi, 136. maddesinde verileri hukuka aykırı olarak verme veya ele geçirme ve 138. maddesinde ise verileri yok etmeme suçu düzenlenmiştir.

Bu maddelerin hiçbirisinde kişisel veri ile ilgili hiçbir tanım bulunmamaktadır. Tanım yapılmamasının iki yönü bulunmaktadır. Bunlardan biri faydası diğeri ise zararının olmasıdır.

Tanım yapılmamasının faydası teknolojik ve sosyal gelişmelerin sonucu ortaya çıkan bilgilerin kanunlarda değişiklik yapılmadan kişisel veri kavramı içerisine alınması, zararı ise suçun konusunu oluşturan kişisel veri kavramının çok geniş yorumlanması sonucu suçta ve cezada kanunilik ilkesini ihlal edecek uygulamaların ortaya çıkmasıdır.

Kişisel verilerin kaydedilmesinin düzenlendiği 135.Maddenin gerekçesinde "Suçun konusu kişisel verilerdir. Gerçek kişiyle ilgili her türlü bilgi, kişisel veri olarak kabul edilmelidir." şeklinde bir açıklama bulunmaktadır.

Peki, kişiyle ilgili her türlü bilgiler nelerdir. Bunların bir kısmını sıralayacak olursak:

Kişinin; Türkiye Cumhuriyeti kimlik numarası, adı, soyadı, doğum tarihi, doğum yeri, nüfusa kayıtlı olunan yer (İl, İlçe, mahalle veya köy), anne ve baba adı, medeni hali (Evli, bekâr, boşanmış), nüfusa kayıtlı olduğu cilt ve aile sıra no, kan grubu, evlenme tarihi, boşanma tarihi ve mahkeme kararı bilgileri, adı-soyadı veya diğer kayıt düzeltmeleri, vatandaşlıktan çıkarılma bilgileri, evlatlık ilişkisi, adresi, dini, bitirilen okullar (ilk-orta-yüksek), hastalıkları, hastalıkları ile ilgili tahlil sonuçları (DNA bilgileri), mali durumu (servet, aldığı ücretler), ahlaki eğilimleri, zaafları, çevre ile ilişkileri, hatıra, anı ve günlükle ilgili defterindeki bilgileri, siyasi görüşü (oy verdiği partiler, üye olduğu dernekler), alışkanlıkları, sevdiği kitaplar veya gazeteler, alışveriş eğilimleri, vergi numarası, e posta adresi ve

şifresi, banka bilgileri, bilgisayarının IP numarası, emeklilik ve kurum sicil numarası, aldığı ödüller, parmak izi, avuç içi izleri, mektupları, yazıları, kitapları, telefon numaraları, mesajları, fiziki kimliği (boy, kilo, engellilik durumu, ten rengi, göz rengi, saç rengi ve şekli, sesi, genel görünüm, ayak ve beden numarası) ve çok daha fazla bilgi kişisel veri kapsamında değerlendirilebilecektir.

Acaba bu kadar bilgilerden hangilerinin kaydı veri olarak kabul edilip kayda alınması (TCK, m.135) ve hukuka aykırı olarak verme veya ele geçirme suçu olarak (TCK, 136) kabul edilip üst sınırı 4 yıla kadar hapis cezası ile bu suçları işleyenler cezalandırılacaktır. Bilgilerden de anlaşılacağı gibi, bunların büyük bir çoğunluğu herkes tarafından bilinmektedir. O halde herkes tarafından maruf ve meşhur olan kişiyle ilgili bir bilgiyi kaydetmenin, birisine vermenin veya yaymanın suç olarak cezalandırılması nasıl olacaktır. İşte burada karşımıza bu suçları işleyenler bakımından yukarıda tanım yapılmamasının zararı olan suçta ve cezada kanunilik ve belirlilik ilkesinin ihlali çıkmaktadır. (Veli Özer Özbek, Mehmet Nihat Kambur, Koray Doğan, Pınar Bacaksız, İlker Tepe, Türk Ceza Hukuku, Özel Hükümler, 2.B, Ankara 2011, s.517)

Anayasa Mahkemesi suçta ve cezada kanunilik ve belirlilik ilkesine bağlı kalınmasının gerekliliğine kararlarında vurgular yapmaktadır.

Anayasa'nın 38. maddesinin ilk fıkrasında, 'Kimse, ... kanunun suç saymadığı bir fiilden dolayı cezalandırılmaz' denilerek 'suçun yasallığı', üçüncü fıkrasında da 'ceza ve ceza yerine geçen güvenlik tedbirleri ancak kanunla konulur' denilerek, 'cezanın yasallığı' ilkesi getirilmiştir. Anayasa'da öngörülen suçta ve cezada yasallık ilkesi, insan hak ve özgürlüklerini esas alan bir anlayışın öne çıktığı günümüzde, ceza hukukunun da temel ilkelerinden birini oluşturmaktadır. Anayasa'nın 38. maddesine paralel olarak Türk Ceza Kanunu'nun 2. maddesinde yer alan 'suçta ve cezada kanunilik' ilkesi uyarınca, hangi eylemlerin yasaklandığı ve bu yasak eylemlere verilecek cezaların hiçbir kuşkuya yer bırakmayacak biçimde yasada gösterilmesi, kuralın açık, anlaşılır ve sınırlarının belli olması gerekmektedir. Kişilerin yasak eylemleri önceden bilmeleri düşüncesine dayanan bu ilkeyle temel hak ve özgürlüklerin güvence altına alınması amaçlanmaktadır.

Anayasa'nın 2. maddesinde yer alan hukuk devletinin temel ilkelerinden biri 'belirliliktir. Bu ilkeye göre, yasal düzenlemelerin hem kişiler hem de idare yönünden herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olması, ayrıca kamu otoritelerinin keyfi uygulamalarına karşı koruyucu önlem içermesi de gereklidir. Belirlilik ilkesi, hukuksal güvenlikle bağlantılı olup birey hangi somut eylem ve olguya hangi hukuksal yaptırımın veya sonucun bağlandığını, bunların idareye hangi müdahale yetkisini doğurduğunu bilmelidir. Birey ancak bu durumda kendisine düşen yükümlülükleri öngörebilir ve davranışlarını belirler.

Hukuk güvenliği, normların öngörülebilir olmasını, bireylerin tüm eylem ve işlemlerinde devlete güven duyabilmesini, devletin de yasal düzenlemelerde bu güven duygusunu zedeleyici yöntemlerden kaçınmasını gerekli kılar. (Anayasa Mahkemesinin, 7.7.2011/69-116 sayılı kararından)

Bilimsel görüşlere baktığımızda da belirlilik ilkesinin önemli ve vazgeçilmez bir ilke olduğu kabul edilmiştir.

Kanun koyucunun yükümlülüğü, hangi fiillerin suç teşkil ettiğini belirlemekle sona ermemektedir. Kanun koyucu, suç olarak öngördüğü fiili açıkça tanımlamalıdır. Zira kanunun açıkça suç saymadığı bir fiil için kimseye ceza verilemez ve güvenlik tedbiri uygulanamaz (m. 2/1).

Bu hüküm, aynı zamanda, yargıca yönelik bir emir de içermektedir. Şayet bir kimse tarafından gerçekleştirilen davranış, kanunda açıkça suç olarak tanımlanmamışsa, böyle bir fiilden dolayı o kimsenin cezalandırılması mümkün değildir. Dolayısıyla belirlilik ilkesi, kıyas yasağını da kapsamına almaktadır. Yapılan davranış, toplum düzeninin devamı bakımından ne kadar katlanılmaz olursa olsun, şayet kanunda suç olarak açıkça tarif edilmemişse, böyle bir davranışta bulunan kişinin cezalandırılması düşünülemez. Aksi takdirde, hâkim, kuvvetler ayrılığı ilkesini ihlâl ederek, kendisini kanun koyucu konumuna getirmiş olur. Bu ise, Anayasaya açık aykırılık oluşturur (AY m. 4).

Suçları tespit eden kanun hükümlerinin tanımları belirli olmalı, yani açık ve seçik nitelik göstermeli, farklı anlamlara gelen, belirsiz ve çok kapsamlı terimler kullanılmamalıdır. Suç teşkil eden fiillerin ve bunlara öngörülen yaptırımların yasada açıkça tanımlanması, vatandaş bakımından önemli bir güvence oluşturmaktadır. İnsanlar, hangi davranışların suç olduğunu bilmek suretiyle, bunların dışında kalan davranışlarda bulunma özgürlüğüne sahip olmaktadır. Bu anlamda, ceza kanunları hem özgürlüğün sınırını, hem de güvencesini teşkil etmektedir. Ancak ceza kanunları, soyut-genel normları içerdiği için, bu kanunlar bir davranışın cezalandırılabilirliğini somut olay bakımından belirlemezler. TCK'nın 2. maddesi, kişilere davranışlarının yönünü açıkça belirlemeye izin veren ve onların özgürlük alanını devletin önceden kestirilemeyen müdahalelerine karşı güvence altına alan normların yasal olarak tespitini istemektedir. Böylece belirlilik ilkesi, bastırıcı müdahalelerin maddi koşullarıyla ilgilenmektedir. Belirlilik ilkesi, ceza sorumluluğunu doğuran veya suçu nitelikli hale getiren unsurlar bakımından da söz konusudur.. (Mahmut Koca, İlhan Üzülmöz, Türk Ceza Kanunu Genel Hükümler, 6.Baskı, Ankara 2013, s.51)

Avrupa İnsan Hakları Mahkemesi de verdiği birçok kararında belirlilik ilkesinin suç içeren hükümlerde bulunmasını aramıştır.

'Suçta ve cezada kanunilik' ilkesi Anayasanın 38. maddesinde düzenlenen ve artık bir iç hukuk kuralı haline gelen ve Anayasanın 90/son maddesi uyarınca Anayasa'ya aykırılığı dahi ileri sürülemeyen İnsan Hakları Avrupa Sözleşmesi'nin 7. maddesinde düzenlenen pozitif bir ilkedir. Avrupa İnsan Hakları Mahkemesi Kararlarına baktığımızda konuya önemle vurgu yapıldığını görmekteyiz.

Örnek kararlar

a- Suçta ve cezada kanunilik ilkesi gereği, vatandaşların öncelikle ceza yaptırımını taşıyan hukuk kurallarının varlığı hakkında yeterli bilgiye sahip olabilmeleri ve ayrıca vatandaşların davranışlarını yönlendirebilmelerine olanak vermek için, ceza yaptırımını taşıyan kuralların herkesçe anlaşılacak bir biçimde açık ve net olarak düzenlenmiş olması gerekir. (İnsan Hakları Avrupa Mahkemesi; Sunday Times/Birleşik Krallık Kararı; 6.11.1980/6538/74)

b- Avrupa İnsan Hakları Mahkemesi, kanunun açık ve ulaşılabilir olmasını aramaktadır. Bir kararında 'Bir devlette var olan hükümlerin ihlalinin, bir çalışana karşı ceza kovuşturmasını haklı kılabilmesi için bu hükümlerin, bu kişi tarafından uymakla yükümlü olduğu kuralları belirleyebilmesi açısından açık ve anlaşılabilir olması gerekir' (ATAD, 23 Kasım 1999, Arblade ve Leloup Kararı, C.369/96 ve 376/96, Zikreden MANACOR-DA, 115, Avrupa Birliği Ceza Hukukunun Esasları, Ümit Kocasakal, İstanbul 2004, s. 157)

c- İlk olarak; uygulanacak olan hukuk, yeterince erişilebilir olmalıdır, başka bir anlatımla, vatandaşlar belirli bir olaya uygulanabilir nitelikteki hukuk kurallarının varlığı hakkında yeterli bilgiye sahip olabilmelidirler.

İkinci olarak, vatandaşların davranışlarını düzenlemelerine olanak vermek için yeterli açıklıkta düzenlenmemiş bir norm, hukuk kuralı olarak kabul edilemez. Vatandaşlar belirli bir eylemin gerektirdiği sonuçları, durumun makul saydığı ölçüde ve eğer gerekiyorsa uygun bir danışmayla önceden görebilmelidir. (Osman Doğru, Atilla Nalbant, İnsan Hakları Avrupa Sözleşmesi, Açıklama ve Önemli Kararlar, Ankara 2013, s.269)

İşte veri tanımının yapılmaması nedeniyle suçta ve cezada kanunilik ve açıklık ilkesi gereği veri ile ilgili suç düzenlemeleri Anayasaya aykırıdır. Bu hususun mahalli mahkemece, temyiz incelemesi yapan ceza dairesince hükmün Anayasaya aykırı olduğu ve iptali gerekçesiyle Anayasa Mahkemesine götürülmesi yerinde olurdu. Bu aşamada Anayasa'ya aykırılık iddiası ciddi bulunarak konunun Anayasa Mahkemesinin önüne getirilmesi gerekirdi.

2- Anayasaya aykırılığı ciddi bulmayan Ceza Genel Kurulu kişisel verilerin neler olması gerektiğine dair sınırları çizmesi gerekirdi.

TCK'nun m.135. gerekçesinde 'Söz konusu suç tanımında kişisel verilerin bilgisayar ortamında veya kâğıt üzerinde kayda alınması arasında bir ayırım gözetilmemiştir. Bu bakımdan, söz konusu suç tanımı ile Avrupa Konseyi bünyesinde hazırlanan Türkiye'nin de 28 Ocak 1981 tarihinde imzalamakla taraf olduğu Kişisel Nitelikteki Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme'nin ilgili hükümlerine geçerlilik tanınmıştır.'

Türkiye adı geçen sözleşmeyi imzalamakla beraber, Sözleşmenin 4. maddesi gereğince sözleşmenin yürürlüğe girmesi için iç hukukta düzenleme yapılmasını öngören hükmü yerine getirilmediğinden sözleşme henüz Türkiye'de yürürlüğe girmemiştir. Türkiye Cumhuriyeti bu hükümden hareketle ancak 2013 yılında Kişisel Verilerin Korunması Kanun Tasarısını TBMM sunmuş, ancak tasarı henüz kanunlaşmamıştır.

Bu durumda kişisel veri tanımını 1981 Tarihli Sözleşme, TCK'nun 135. madde gerekçesi ve kanunlaşmayı bekleyen Tasarıdan yararlanarak yapmamız gerekir.

Kişisel veriyi; adı geçen Sözleşmenin 2. maddesi 'Belirli veya belirlenebilir bir bireyle bağlantılandırılabilen tüm bilgiler' TCK'nun 135. maddesinin gerekçesi 'Gerçek kişiyle ilgili her türlü bilgi' Kişisel Verilerin Korunması Kanun Tasarısı madde 3 ise; 'Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler' olarak tanımlamaktadır. Görüldüğü gibi yukarıda 100'e yakın sayıda sıraladığımız kişilerle ilgili bilgiler kişisel veri kapsamında değerlendirilebilecektir. Bu sayılan kişisel verilerin hukuki yollarla korunması kabul edilebilir. Ancak bu verilerin her birinin kaydını suç kabul edip üst sınırı kişisel verileri kayıta 3 yıl, verileri verme veya yaymada 4 yıl hapis ve resen kovuşturulan bir suç haline getirdiğimizde de karşımıza 'Suç işleyen kişi hakkında işlenen fiilin ağırlığıyla orantılı ceza ve güvenlik tedbirine hükmolunur' (TCK, m.3/1) hükmünün açıkça ihlali ve takibi mümkün olmayan bir suç alanı ortaya çıkar. Şu iki örnek karşılaştırıldığında oransızlığın ne kadar büyük olduğu daha iyi anlaşılacaktır. Şöyle ki: Kişinin, evlenme tarihi veya kaç çocuğunun olduğu veya bir fotoğrafı veri kabul edilip bunu yayan için 4 yıl hapis cezası öngören (TCK, m.136) bir ceza davası ile bir kişinin kollarını ve bacaklarını kıran kişi için öngörülen en yüksek 4 yıl 6 aylık hapis cezası (TCK, 86/1,3) karşılaştırıldığında, oransızlığın ne kadar büyük olduğu ve zarar verici uygulamaya dönüşecek bir düzenlemenin bulunduğu apaçık ortadadır.

İşte suç içeren bu hükümlerdeki belirsizliği, suçla orantılı ceza uygulanmasının gerekliliği ilkesini taşımadığını gören bilim adamları suç olarak kabul edilebilecek kişisel verilerin kaydının sadece TCK'nın 135/2.maddesindeki bilgilerin (Kişilerin, siyasî, felsefi veya dinî görüşler, ırkî kökenler, ahlâkî eğilimler, cinsel yaşamları, sağlık durumları veya sendikal bağlantılarına ilişkin bilgiler) veri olarak kabul edilebileceği, bunların dışındaki bilgilerin suç kapsamında değerlendirilemeyeceği

yönünde bilimsel görüşler ileri sürmüşlerdir. (Zeki Hafızoğulları, Muharrem Özen, Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar, Ankara Barosu Dergisi, Yıl 67, sayı 4, 2009, s.9)

Nelerin kişisel veri olduğunu belirlemede kişilerin özel hassasiyetinin korunması, kişisel verilerin korunması açısından bilinçli bir toplumda gerekli değil, hatta zararlıdır. Zira kişisel verilerin gerektiği şekilde korunduğu bir toplumda kişilerin özel hassasiyetlerinin korunması, kavramın gereğinden daha geniş anlaşılması, dolayısıyla korumanın imkânsız hale gelmesi riskini doğurur. Ayrıca, kavramın sınırlarının çok geniş kabul edilmesi, bir noktadan sonra bu sınırların belirsizleşmesine ve kavramın anlamını yitirmesine yol açar ki bu durumda kişiler önceden sahip oldukları güvenceden bile yoksun kalırlar. Buna karşın, Türkiye gibi kişisel verilerin korunması bilincinin henüz gelişmediği ülkelerde kişilerin özel hassasiyetlerinin korunması zorunludur. Çünkü bu tip toplumlarda özel hassasiyetin korunmaması, neredeyse kişisel verinin korunmasını isteyen ve istemeyen kişiler arasındaki dengeyi kurmanın en kolay yollarından biriye, verilerin işlenmesine yaptırım uygulamak, ancak bu yaptırımın uygulanmasını şikâyet şartının gerçekleşmesine bağlamaktır. (Hale Akdağ, Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Ankara 2014, s.9)

Herkes tarafından bilinen veya kolaylıkla bilinmesi mümkün verileri bu kapsamda kabul etmek, maddenin kapsamının dayanılmaz ölçüde genişletmek anlamına geleceğinden 'kişisel veri' kavramını bu anlamda dar yorumlamakta zorunluluk vardır. (Hakan Hakeri, Tıp Hukuku, Ankara, 5.Bası, 2012, s.755)

Kişisel verilerin ceza hukuku anlamında suç konusu olabilmeleri, hassas kişisel bilgiler (veriler) hariç, şu şekilde bir sınırlamaya tabi tutarak suçta ve cezada kanunilik ve belirlilik ilkesine uymayan hükmü kısmen adaletli bir uygulamaya sokabiliriz. O da suç düzenlemelerinin yer aldığı bölüm başlığından hareketle özel hayata ve hayatın gizli alanına ait olup, kişinin başkaları ile paylaşmadığı ve alenileştirmedeği kişisel bilgiler olarak anlamak gerekir.

Buna göre kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, dernek, vakıf ya da sendika üyeliği, sağlığı veya cinsel hayatı ile ilgili verilerinin kaydı, bir başkasına verilmesi veya ele geçirilmesi bunlar hassas veriler oldukları için mutlak olarak cezai yaptırımlarla alanına alınması gereken kişisel verilerdir.

Buna göre kişilerle ilgilin bilginin; ilgili kişi tarafından alenileştirilmemiş, üçüncü kişilerle paylaşılmamış, bilinmesinin kişinin yaşam şekline, ekonomik ve finansal ve bilişim alanına zarar verme ihtimali bulunan bilgiler olması halinde kişisel verilerle ilgili suçların konusunu oluşturmalı.

Bunun dışında kalan kişilerle ilgili diğer bilgiler ise ancak kullanılış amacına göre hakaret, dolandırıcılık gibi suçların konusu olmalı ve hukuki ve idari yollarla korunmalıdır.

Ceza hukukunun konusu olabilecek kişisel verilerin sınırları bu şekildi çizilmiş olsaydı, fotoğrafın bu kapsamda kişisel veri olarak değerlendirilemeyeceği ortaya çıkmış olacaktı.

3- Dava konusu olayda, TCK'nın 136. maddesi anlamında bir yayma söz konusu değildir.

Katılanın fotoğrafının internette arkadaşlık sitesine konmasında, yukarıda açıklanan eksikliklerin biran için olmadığını düşünsek bile eylem TCK'nun 136. maddesi kapsamında kişisel verileri hukuka aykırı olarak yayma suçunu oluşturmamaktadır. Katılan köşe yazarı olarak çalıştığı 'Son Nokta' gazetesine verdiği ve gazetede her yazısı ile birlikte kullanılan fotoğrafı, gazeteden ayrılması üzerine aynı fotoğrafın www.istanbul.net sitesine konması ve katılanın bir yakınının haber vermesi üzerine yapılan soruşturma sonunda resmin sanıklar tarafından siteye konduğu anlaşılmıştır. Katılanın durumu sanıklara bildirmesi üzerine sitede 48 saat kalan fotoğraf ve işaretlenen bilgiler kaldırılmıştır. Görüldüğü gibi su üzerine yazı yazma gibi bir şey.

Siteyi, incelediğimizde 2005 yılında kurulduğu, İstanbul'a özel arkadaşlık sitesi olduğu, semt bazında arkadaş bulmaya imkân verdiği ve inceleme tarihi itibariyle 3.860.935 üyesinin bulunduğu anlaşılıyor.

Suç tarihi itibariyle oluşturulan sayfaya baktığımızda katılanla ilgili olduğu izlenimini veren bilgiler, rumuz; Belkiba, kadın, balık burcu, 24 yaşında, Kadıköy Bağdat Caddesinde oturur, aradığı cinsiyete erkek (24-29 yaş aralığında), aradığı ilişki arkadaşlık, göz rengi kahverengi, saç kumral, eğitimi lisansüstü, mesleği öğretim görevlisi, konuştuğu dil Almanca, İngilizce, yalnız yaşıyor, çocuksuz sigara az içiyor, içki içmiyor bilgileri ile yaşam tarzına, aradığı kişiye dair özellikler ve katılanla ilgili olarak beğenenlerin işaretlemesi için seçenek kutucuklar bulunuyor.

Tüm bu bilgilerden evli, iki çocuklu olan katılana ait doğru olan sadece fotoğrafın ona ait olmasıdır. Bunun dışında katılana ait olduğu söylenebilecek hiçbir gerçek bilgi yoktur. Eğer resim olmazsa katılanla ilişkisini tespit etmekte mümkün değildir.

Katılana ait kişisel veri olarak kabul edilen fotoğrafın buraya konması, katılanın kişisel verisini yayma olarak değerlendirmek mümkün değil, çünkü katılan resmini gazete köşesine koymakla zaten yaymış oldu. Kaldı ki. alışlagelen uygulamaya göre de gazetede fıkra yazarlığı yapan kişilerin internet sitesinde de resimleri yayınlamaktadır. Halen kanunlaşmayı bekleyen Kişisel Verileri Koruma Kanun tasarısının 5. maddesi, ilgili kişinin kendisi tarafından alenileştirilmiş bilginin ilgili kişinin açık rızası aranmaksızın işlenebileceğini kabul etmiştir.

Yine ilgili kişinin, her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim (TCK'nın 6/1-9) okyanusuna bıraktığı bir kişisel verisinin hangi okyanus, deniz, göl, gölet ve bataklığa gireceğine artık engel olamaz. Bu aşamada ortaya çıkan başka suçların araştırılması gerekir.

Katılanın resminin sadece gazete köşesine yayınlanmasına rızası vardı, dolayısıyla bu gibi yerlerde rızası yoktur, o nedenle kişisel verileri yayma suçu oluşur düşüncesi de ileri sürülemez. Bu suçlarda ilgilinin rızası önemli değildir (TCK, m.26/2), suç soruşturması ve kovuşturması şikâyete tabi olmadığından mağdurun üzerinde tasarrufta bulunabileceği bir hakkın var olduğu söylenemez. Bu suçlar bakımından bireyin değil, kamunun menfaatlerinin ağır bastığı kabul edilmiştir. Dolayısıyla bu suç bakımından ilgilinin rızası hukuka uygunluk sebebi değildir. (Veli Özer Özbek, Mehmet Nihat Kambur, Koray Doğan, Pınar Bacaksız, İlker Tepe, Türk Ceza Hukuku, Özel Hükümler, 2.B,Ankara 2011, s.521)

Fotoğrafın herhangi bir internet sitesine konması, kaldı ki bütün basın yayın organlarında haber ve yorum, eleştiri, tenkit, hakaret vb gibi tüm yazılarda hakkında yazı yazılan kişinin fotoğrafı kullanılmaktadır. Katılan şu aşamada şöyle bir beyanda bulunsa, 'Resmim internete arkadaşlık sitesine kondu, ancak 48 saat sonra kaldırılmış, hem fotoğrafımın konulmasından hemde benim bekâr biri olarak gösterilip erkek arkadaş aradığım yazıları dolayısıyla şikâyetçi değilim' beyanı karşısında bu kovuşturmayı kamu adına takip ettirmede kamu menfaatlerinin ağır bastığı hangi durum vardır? Veyahut 'adı geçen internet sitesinde yaklaşık bine yakın içindi bahar, kış, ay, güneş kelimeleri geçen rumuzlu bütün fotoğraflar sahiplerinin rızası dışında konulmuştur', şeklinde bir ihbar yapılsa, fotoğraf veri kabul edildiğinde bunu Cumhuriyet savcısının re'sen araştırması, sahte resim ve bunları koyanları tespit etmesi sonucunu doğurmaz mı?

Özetle, herhangi bir özellik arz etmeyen, yanında kişiyi belirleyen başka bir bilginin bulunmadığı (TC Kimlik No, Telefon numarası, e-posta adresi) bir fotoğrafın, umuma sunulmuş olması nedeniyle başka bir sitede yayınlanmasının kişisel verileri yayma suçunun konusunu oluşturmayacağı, sadece katılanın bekâr, erkek arkadaş arayan bir bayan olarak gösterilip küçük düşürdüğünden eylem TCK'nın 125/1-4. maddesi kapsamında hakaret suçunu oluşturur. Nasıl ki aynı bilgiler ve resim sokak duvarlarına ve ilan panolarına yapıştırılsa hakaret suçu oluşacak idiye burada da aynı suç oluşur. (Benzer kararlar, 4.CD, 6.6.2012/20400-13691; 12.CD, 10.6.2013/9656-15773; 12.CD, 25.11.2013/33007-26689, 12.CD, 26.5.2014/25334-12705) Hakaret suçundan da açılmış bir dava bulunduğundan eylemin bu kapsamda değerlendirilmesi gerektiğini düşündüğümüzden sayın çoğunluğun itirazın reddine dair görüşüne katılmıyoruz" düşüncesiyle,

Çoğunluk görüşüne katılmayan Ceza Genel Kurul Başkanı ve dört Genel Kurul Üyesi de; benzer düşüncelerle itirazın kabulü gerektiği yönünde karşı oy kullanmışlardır.

Açıklanan nedenlerle, 1- Yargıtay Cumhuriyet Başsavcılığı itirazının REDDİNE,2- Dosyanın, mahalline gönderilmek üzere Yargıtay Cumhuriyet Başsavcılığına TEVDİİNE, 10.06.2014 günü yapılan ilk müzakerede önsoruna ilişkin olarak gerekli çoğunluk sağlanamadığından, 17.06.2014 günü yapılan ikinci müzakerede oybirliğiyle, esasa ilişkin uyuşmazlık yönünden ise 17.06.2014 günü yapılan ilk müzakerede oyçokluğuyla karar verildi.

Yargıtay Kararı - Hukuk Genel Kurulu (E. 2017/1340)

Yargıtay HGK., E. 2017/1340 K. 2018/1622 T. 6.11.2018

Esas No.: 2017/1340

Karar No.: 2018/1622

Karar tarihi: 06.11.2018

MAHKEMESİ: Asliye Hukuk Mahkemesi

Taraflar arasındaki "manevi tazminat" davasından dolayı yapılan yargılama sonunda, Bakırköy 9. Asliye Hukuk Mahkemesince davalı ... yönünden davanın dava şartı noksanlığı nedeniyle usulden reddine, davalılar ... ve Nuri Aykon Gazetecilik Ltd.Şti. yönünden davanın kısmen kabulüne dair verilen 23.11.2012 tarihli ve 2010/345 E., 2012/570 K. sayılı kararın davalılar vekili tarafından temyiz edilmesi üzerine, Yargıtay 4. Hukuk Dairesinin 18.12.2013 tarihli ve 2013/2039 E., 2013/20094 K. sayılı kararı ile,

"...1-)Davalıların davacılarından ...'e yönelik temyiz itirazları yönünden;

Dava, basın yoluyla kişilik haklarının ihlaline dayalı manevi tazminat istemine ilişkindir. Mahkemece, davanın kısmen kabulüne karar verilmiş; hüküm, davalılar tarafından temyiz edilmiştir.

Davacılar, dava konusu "Generallerin Yahudi Damatları" başlığı ile yapılan haberde kişilik haklarının ihlal edildiğini, davacılarından ...'e ait pasaportun fotoğraf ve kimlik bilgilerinin bulunduğu sayfalarına burada yer alan her türlü bilgi okunacak şekilde yer verilip kişisel verilerin kullanılarak suç işlendiğini belirterek manevi tazminata hükmedilmesini istemişlerdir.

Dosya kapsamından dava konusu haberde davacılarından ...'in yahudi kökenli İspanyol vatandaşı olduğu idda edilmiş; anılan davacının açık kimlik bilgileri ve fotoğrafına yer verilmemiştir. Ceza davasında da, davacı ...'e yönelik kişisel verileri hukuka aykırı yaymak ve kişisel verilerin kaydedilmesi suçlarından davalılardan ... hakkında beraat kararı verilmiştir. Şu durumda, fotoğrafına yer verilmeyen, açık kimlik bilgileri habere konu edilmeyen sadece vatandaşlık ve dini inancına yönelik iddiaların dile getirildiği haber nedeniyle davacılarından ... yönünden manevi tazminatın koşulları oluşmadığından anılan davacı yönünden davanın reddine karar vermek gerekir. Mahkemece bu husus gözetilmeksizin yanılığa dayalı gerekçe ile anılan davacı yönünden de istemin bir bölümünün kabulüne karar verilmiş olması doğru görülmemiş ve bozmayı gerektirmiştir.

2-)Dosyadaki yazılara, kararın dayandığı kanıtlarla yasaya uygun gerektirici nedenlere, özellikle delillerin değerlendirilmesinde bir isabetsizlik görülmemesine göre davalıların davacılarından ...'e yönelik aşağıdaki bendin kapsamı dışında kalan temyiz itirazları reddedilmelidir.

3-)Davalıların davacılarından ...'e yönelik diğer temyiz itirazlarına gelince;

Kişilik hakları hukuka aykırı olarak saldırıya uğrayan kimse manevi tazminat ödetilmesini isteyebilir. Yargıç, manevi tazminatın tutarını belirlerken, saldırı oluşturan eylem ve olayın özelliği yanında tarafların kusur oranını, sıfatını, işgal ettikleri makamı ve diğer sosyal ve ekonomik durumlarını da dikkate almalıdır. Tutarın belirlenmesinde her olaya göre değişebilecek özel durum ve koşulların bulunacağı da gözetilerek takdir hakkını etkileyecek nedenleri karar yerinde nesnel (objektif) olarak göstermelidir. Çünkü yasanın takdir hakkı verdiği durumlarda yargıcın, hukuk ve adalete uygun (hak ve nasfette) karar vereceği Medeni Yasa'nın 4. maddesinde belirtilmiştir. Takdir edilecek bu para, zarara uğrayanda manevi huzuru doğurmayı gerçekleştirecek tazminata benzer bir işlevi (fonksiyonu) olan özgün bir nitelik taşır. Bir ceza olmadığı gibi malvarlığı hukukuna ilişkin bir zararın karşılanmasını da amaç edinmemiştir. O halde bu tazminatın sınırı onun amacına göre belirlenmelidir. Takdir edilecek tutar, var olan durumda elde edilmek istenilen doyum (tatmin) duygusunun etkisine ulaşmak için gerekli olan kadar olmalıdır.

Davaya konu olayda; haberin veriliş biçimi, kullanılan ifadeler ve yukarıdaki ilkeler gözetildiğinde, davacılarından ... yararına hükmedilen manevi tazminat miktarı fazladır. Davacı yararına daha alt düzeyde manevi tazminata hükmedilmek üzere karar bozulmalıdır...."

gereğesiyle oy çokluğuyla bozularak dosya yerine geri çevrilmekle yeniden yapılan yargılama sonunda mahkemece önceki kararda direnilmiştir.

HUKUK GENEL KURULU KARARI

Hukuk Genel Kurulunca incelenerek direnme kararının süresinde temyiz edildiği anlaşıldıktan ve dosyadaki belgeler okunduktan sonra gereği görüldü:

Dava, basın yoluyla kişilik haklarına saldırı nedeniyle manevi tazminat istemine ilişkindir.

Davacılar vekili; davalı gazetenin 29.06.2010 tarihli nüshasının birinci ve sekizinci sayfalarında davalı ... tarafından hazırlanan haberde "Generallerin Yahudi Damatları" ana başlığı altında "Bazı üst düzey komutanların siyonistlerce kutsal kabul edilen Ağlama Duvarı'ndaki görüntülerinin ortaya çıkmasının ardından şimdi de bazı üst düzey generallerin damatlarının Yahudi olduğu bilgisine ulaşıldı" şeklinde bir habere yer verildiğini, bu haber kapsamında müvekkillerinden ...'e ait pasaportun fotoğraf ve kimlik bilgilerinin bulunduğu sayfalarına her türlü bilgi okunacak şekilde yer

verildiğini ve çeşitli kişisel verileri kullanılarak suç işlendiğini, diğer müvekkilinin İspanyol asıllı olduğu doğru olmasına rağmen ne kendisi ne de ailesinin birinin Yahudi asıllı olmadığını, basın özgürlüğünün sınırsız olmadığını, haber verme kisvesi altında müvekkillerinin kişilik haklarına saldırıda bulunulduğunu, kamu yararı dışında hiçbir kişisel çıkarın hukuka aykırı şekilde elde edilmiş kişisel verilerin sunulmasına neden olmayacağını, haber niteliği taşımayan müvekkillerine ait kişisel verilerin salt sansasyon yaratmak için bir araç olarak kullanıldığını, müvekkillerinin bireysel anlamda bu tarz bir haberde yer almalarına yol açabilecek herhangi bir konum ve statüleri bulunmadığını, hukuka aykırı olarak ve rızaları dışında elde edilen kişisel verilerin kullanılmasında kamuyu bilgilendirme amacı bulunmadığını, özel hayatları bakımından buna katlanmak zorunda olmadıklarını, dini görüşlerine ve ırki kökenlerine vurgulamalar yapılarak toplumun belli bir kesiminin hedefi hâline getirildiklerini ileri sürerek her bir müvekkili için ayrı ayrı 20.000,00TL olmak üzere toplam 40.000,00TL manevi tazminatın 29.06.2010 tarihinden itibaren işleyecek yasal faizi ile birlikte davalılardan müştereken ve müteselsilen tahsiline, karar özetinin basın organları tarafından yayınlanmasına karar verilmesini talep etmiştir.

Davalılar vekili; müvekkili ...'nın sorumlu müdür olması sebebiyle bu davalı yönünden davanın pasif husumet nedeniyle reddi gerektiğini, gazetenin yayıncısı durumundaki tüzel kişinin de tazminat sorumluluğunun bulunmadığını, haberin gerçek olduğunu, davacı ...'nın yayın tarihinde Türk Silahlı Kuvvetlerinde en üst kademeye gelmiş ismi ilerdeki Genelkurmay Başkan adayları arasında geçen Birinci Ordu Komutanı Orgeneral Hasan İğsız'ın öz kızı olduğunu, örnek gösterilen diğer üst rütbeli askerlerin yakınları ile birlikte Orgeneral Hasan İğsız'ın kızının yabancı bir kimse ile evli olduğunun inkâr edilmediğini, TSK Personelinin yabancı ile evlenmesinin izne bağlı olup davacı TSK personeli olmadığından bu kurala uyma yükümlüğünün bulunmadığını ancak babasının TSK'daki konumunun bu olayı dikkat çekici yaptığını ve toplumsal ilgi uyandırdığını, haberde davacıların durumunun örnek olarak gösterildiğini ve evlenme kayıtları esas alınarak hazırlandığını, özel şöhretin kaybının kamusal bir gerçeğin kaybından daha az zarar verici olduğunu, dava konusu haberin eleştiri hakkının kullanılmasından ibaret olup davacıların kişilik haklarına saldırı teşkil etmediğini, istenilen tazminat miktarının fahiş olduğunu belirterek davanın reddini savunmuştur.

Mahkemece; Anadolu'da Vakit Gazetesi'nin 29.06.2010 tarihli nüshasında "Generallerin Yahudi Damatları" başlığı ile verilen haberin devamında davacılarından'nın Birinci Ordu Komutanı Orgeneral Hasan İğsız'ın kızı olduğu, İspanya Yahudilerinden biriyle evli olup evlendikten sonra Matos Martin soyismini alan'nın kocasının İspanya uyruklu ve Yahudi asıllı ... olduğu şeklinde haber içeriğinin devam ettiği ve davacı ...'nın nüfus cüzdanı örneğinin tüm bilgiler okunacak şekilde

fotoğrafi ile birlikte yayınlandığı, davacıların kamuoyunun ilgisini çekecek ve bireysel anlamda bu tarz bir haberde yer almalarına yol açabilecek herhangi bir konum ve statülerinin bulunmadığı, haberde davacıların özel hayat kapsamında kalan birtakım kişisel verileri ile dini görüşleri ve ırki kökenlerine ait yapılan belirtmelerin kamuoyunun hiçbir şekilde ilgisini çekmediği ve haber niteliği taşımadığı, bu kapsamda özel hayat kapsamındaki tüm bu verilerin açıklanmasının davacıların kişilik haklarına saldırı niteliğinde olduğu gerekçesiyle davalı ... hakkındaki davanın dava şartı noksanlığı nedeniyle usulden reddine, davalılar ... ve Nuri Aykon Gazetecilik Ltd.Şti. hakkındaki davanın kısmen kabulü ile her bir davacı için ayrı ayrı 8.000,00'er TL manevi tazminatın yayın tarihinden itibaren yasal faiziyle birlikte müştereken ve müteselsilen davalılardan tahsiline karar verilmiştir.

Davalılar vekilinin temyizi üzerine karar Özel Dairece yukarıda açıklanan gerekçelerle oy çokluğuyla bozulmuştur.

Yerel Mahkemece önceki gerekçeler tekrar edilerek ve haberin içinde davacı ...'in Yahudi olduğunun pek çok kez vurgulandığı ve yine davacının doğum yeri, doğum tarihi ve baba isminin de açıkça yazıldığı, kimlik bilgilerinin paylaşıldığı, davacı ...'un da özellikle bir İspanyol Yahudisiyle evli olduğu vurgulanarak nüfus cüzdan örneğinin fotokopisinin basıldığı fotoğrafının da yer aldığı, her ne kadar bozma ilamında davacı ...'e yönelik olarak haberde sadece vatandaşlık ve dini inancına yönelik iddiaların dile getirildiği belirtilmiş ise de haber içeriğinde bu davacının kişisel verilerinin de hukuka aykırı olarak habere konu edildiği, dini inancının özellikle birden fazla vurgulandığı, haberin basın özgürlüğü içinde ve haber verme kıstası çerçevesinde verildiğinin kabul edilemeyeceği, kişinin Anayasaca güvence altına alınan din ve vicdan hürriyetinin de ihlal edildiği, bu bakımdan davacı ... yönünden manevi tazminatın koşullarının oluşmadığı yönündeki gerekçeye katılmanın mümkün olmadığı, davacı ... yönünden ise haberin bütünlüğü, yazının içeriği ve söz konusu gazetede habere pek çok kişinin ulaşması, ayrıca haberin yayınlandığı dönem itibariyle ülkenin bulunduğu durum, ekonomik koşullar ve paranın satın alma gücü dikkate alındığında kişisel verileri hukuka aykırı olarak ele geçirilip yayınlanan davacı ... için takdir olunan 8.000,00TL manevi tazminatın uygun olduğu, diğer davacı için de özellikle dinsel inancının haber içeriğinde birden çok kez özellikle vurgulanması, Türkiye'nin içinde bulunduğu siyasi iklim, halkın Yahudilere bakış açısı ve bu insanların hedef olarak alınabilme ihtimalleri dikkate alındığında da bu davacı için takdir olunan 8.000,00TL tazminatın uygun olduğu gerekçesiyle direnme kararı verilmiştir.

Direnme kararı, davalılar vekili tarafından temyiz edilmiştir.

Hukuk Genel Kurulu önüne gelen uyuşmazlık,

1- Dava konusu haberde davacılar... 'in kişisel verilerine hukuka aykırı olarak yer verilip verilmediği, haber içeriğindeki ifadelerin kişilik haklarına saldırı teşkil edip etmediği, buradan varılacak sonuca göre davacı ... yararına manevi tazminata hükmedilmesinin gerekip gerekmediği,

2- Davaya konu haberin içeriği ve kullanılan ifadeler nedeniyle davacı ... yararına takdir edilen manevi tazminat miktarının fazla olup olmadığı,

noktalarında toplanmaktadır.

Hukuk Genel Kurulunda yapılan görüşmeler sırasında işin esasının incelenmesinden önce, temyize konu kararın, ilk hükmün gerekçesinde yer almayan yeni bir olguya dayalı yeni bir hüküm niteliğinde olup olmadığı, dolayısıyla temyiz incelemesinin Hukuk Genel Kurulunca mı, yoksa Özel Dairece mi yapılması gerektiği hususu ön sorun olarak değerlendirilmiştir.

Bilindiği üzere; direnme kararının varlığından söz edilebilmesi için, mahkeme bozmadan esinlenerek yeni herhangi bir delil toplamadan önceki deliller çerçevesinde karar vermeli; gerekçesini önceki kararına göre genişletebilirse de değiştirmemelidir (6217 sayılı Kanununun 30. maddesi ile 6100 sayılı Hukuk Muhakemeleri Kanununa eklenen "Geçici madde 3" atfıyla uygulanmakta olan 1086 sayılı Hukuk Usulü Muhakemeleri Kanununun 429. maddesi).

Eş söyleyişle; mahkemenin yeni bir delile dayanarak veya bozmadan esinlenerek gerekçesini değiştirerek veya daha önce üzerinde durmadığı bir hususu bozmada işaret olunan şekilde değerlendirerek karar vermiş olması hâlinde, direnme kararının varlığından söz edilemez.

Somut olayda ise, yerel mahkeme direnme kararında, ilk kararındaki gerekçelerine ilave olarak "...haberinde davacı ...'in Yahudi olduğunun birden fazla kez vurgulandığı, bu davacının da doğum yeri, doğum tarihi ve baba ismi gibi nüfus kimlik bilgileri ile vatandaşlığı ve dini inancına yönelik kişisel verilerinin de hukuka aykırı olarak habere konu edildiği, kişinin Anayasaca güvence altına alınan din ve vicdan hürriyetinin de ihlal edildiği..." gerekçesine de dayanmıştır.

Bu gerekçe yukarıda açıklanan ilkeler çerçevesinde değerlendirilmiş; temyize konu kararın yeni bir hüküm değil, eski gerekçenin yasal sınırlarda genişletilmesi kapsamında kabul edilerek, direnme niteliğinde olduğuna karar verilmiş, ön sorun oy birliğiyle aşılarak işin esasının incelenmesine geçilmiştir.

İşin esasının incelenmesine gelince:

I- Davalılar vekilinin davacı ...'e yönelik temyizi yönünden;

Uyuşmazlığın çözümü açısından öncelikle konuyla ilgili yasal düzenlemelerin irdelenmesinde yarar vardır.

Manevi zarar, kişilik değerlerinde oluşan objektif eksilmedir. Duyulan acı, çekilen ızdırap manevi zarar değil, onun görüntüsü olarak ortaya çıkabilir. Acı ve elemnin manevi zarar olarak nitelendirilmesi sonucu, tüzel kişileri ve bilinçsizleri; öte yandan, acılarını içlerinde gizleyenleri tazminat isteme haklarından yoksun bırakmamak için yasalar manevi tazminat verilebilecek bazı olguları özel olarak düzenlemiştir.

Bunlar kişilik değerlerinin zedelenmesi (TMK m.24), isme saldırı (TMK m.26), nişan bozulması (TMK m.121), evlenmenin butlanı (TMK m.158/2), boşanma (TMK m.174/2) bedensel zarar ve ölüme neden olma (818 sayılı BK m.47) durumlarından biri ile kişilik haklarının zedelenmesi (818 sayılı BK m.49-6098 sayılı TBK m. 58) olarak sıralanabilir.

4721 sayılı TMK'nın 24. maddesi ile 818 sayılı BK'nın 49. maddesi diğer yasal düzenlemelere nazaran daha kapsamlıdır.

4721 sayılı Türk Medeni Kanunu'nun (TMK) 24. maddesinde;

“Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hakimden, saldırıda bulunanlara karşı korunmasını isteyebilir.

Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar yada kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.”

Dava konusu yayının yapıldığı ve davanın açıldığı tarihte yürürlükte bulunan 818 sayılı Borçlar Kanununun (BK) 49. maddesinde ise;

“Şahsiyet hakkı hukuka aykırı bir şekilde tecavüze uğrayan kişi, uğradığı manevi zarara karşılık manevi tazminat namıyla bir miktar para ödenmesini dava edebilir.

Hakim, manevi tazminatın miktarını tayin ederken, tarafların sıfatını, işgal ettikleri makamı ve diğer sosyal ve ekonomik durumlarını da dikkate alır.

Hakim, bu tazminatın ödenmesi yerine, diğer bir tazmin sureti ikame veya ilave edebileceği gibi tecavüzü kınayan bir karar vermekle yetinebilir ve bu kararın basın yolu ile ilanına da hükmedebilir.”

hükümleri yer almaktadır.

TMK'nın 24 ve BK'nın 49. maddelerinde belirlenen kişisel haklar, bedensel ve ruhsal tamlık ve yaşam ile nesep gibi insanın, insan olmasından güç alan varlıklar ya da kişinin adı, onuru ve sır alanı gibi dolaylı varlıklar olarak iki kesimlidir.

Görüldüğü üzere BK'nın 49. maddesi gereğince kişisel hakları zarara uğrayanların manevi tazminat isteme hakları vardır.

Bu genel açıklamalardan sonra uluslararası metinlerde ifade özgürlüğünün nasıl yer aldığına da incelenmesinde yarar bulunmaktadır:

2709 sayılı Türkiye Cumhuriyeti Anayasasının 90. maddesinin son fıkrası; "Usulüne göre yürürlüğe konulmuş milletlerarası andlaşmalar kanun hükmündedir. Bunlar hakkında Anayasaya aykırılık iddiası ile Anayasa Mahkemesine başvurulamaz. Usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası andlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası andlaşma hükümleri esas alınır." hükmünü içermektedir. Bu durumda, mahkemelerce önlerine gelen uyuşmazlıklarda usulüne göre yürürlüğe konulmuş milletlerarası andlaşmalar ile iç hukukun birlikte yorumlanması ve uygulanması gerekmektedir.

Hâl böyle olunca, Türkiye'nin taraf olduğu Avrupa İnsan Hakları Sözleşmesi'nde (AİHS) konunun nasıl düzenlendiğinin ve Sözleşme'nin uygulanmasını sağlayan Avrupa İnsan Hakları Mahkemesi (AİHM) kararlarının incelenmesi yerinde olacaktır.

Avrupa İnsan Hakları Sözleşmesi'nin "İfade Özgürlüğü" başlıklı 10. maddesinin birinci fıkrası; "Herkes ifade özgürlüğü hakkına sahiptir. Bu hak, kamu makamlarının müdahalesi olmaksızın ve ülke sınırları gözetilmeksizin, kanaat özgürlüğünü ve haber ve görüş alma ve de verme özgürlüğünü de kapsar. Bu madde, devletlerin radyo, televizyon ve sinema işletmelerini bir izin rejimine tabi tutmalarına engel değildir." hükmünü içermekte olup hangi hâllerde ifade özgürlüğünün sınırlandırılabilceği de aynı maddenin ikinci fıkrasında düzenlenmiştir.

İfade özgürlüğü demokratik bir toplumun en önemli temellerinden birisi olup, toplumsal ilerlemenin ve her bireyin gelişiminin başlıca koşullarından birini teşkil etmektedir. AİHS'nin 10. maddesinin ikinci fıkrası saklı kalmak koşuluyla, ifade özgürlüğü yalnızca iyi karşılanan ya da zararsız veya önemsiz olduğu düşünülen değil, aynı zamanda kırııcı, hoş karşılanmayan ya da kaygı uyandıran "bilgiler" ya da "düşünceler" için de geçerlidir. Bunlar, çoğulculuğun, hoşgörünün ve açık fikirliliğin gerekleri olup, bunlar olmaksızın "demokratik toplum" olmaz (Handyside, parag. 49, başvuru no: 5493/72, 07.12.1976). AİHS'nin 10. maddesinde benimsenen ifade özgürlüğü bu şekilde olmakla

birlikte, yine de dar bir yorum gerektiren istisnalar içermektedir ve bu hakkı kısıtlama ihtiyacının ikna edici bir biçimde ortaya konması gerekmektedir (Pakdemirli/Türkiye kararı, başvuru no: 35839/97, 22 Şubat 2005).

İfade özgürlüğü geniş bir şekilde yorumlanmakta ise de, sınırsız olmadığı da Sözleşme'nin 10. maddesinin ikinci fıkrasında belirtilmiştir. Burada çözülmesi gereken temel sorun ifade özgürlüğü ile kişilik haklarına yönelik saldırı arasındaki sınırın hangi ölçütlere göre saptanacağıdır.

AİHM önüne gelen uyuşmazlıklarda yapılan müdahalenin ifade özgürlüğünü ihlal edip etmediğini aşağıdaki kriterleri uygulayarak tespit etmektedir:

1. Müdahalelerin yasayla öngörülmesi:

AİHM, Sözleşme'nin 10. maddesinin ikinci fıkrasında yer alan "yasayla öngörülme" ifadesinin, ilk olarak, itiraz konusunun iç hukukta bir dayanağı olması gerektiğini hatırlatır. Ancak söz konusu ifade hukuki normların ilgili kişinin erişiminde olmasını, sonuçlarının öngörülebilmesini ve hukukun üstünlüğü ilkesine uygun olmasını gerektiren kanun niteliğine de atıfta bulunmaktadır (Association Ekin/Fransa, başvuru no: 39288/98; Ürper ve diğerleri/Türkiye kararı, başvuru no: 14526/07, 14747/07, 15022/07, 15737/07, 36137/07, 47245/07, 50371/07, 50372/07 ve 54637/07, 20 Ekim 2009).

2. Müdahalelerin meşru bir amaç izleyip izlemediği konusu:

Sözleşme'nin 10/2. maddesine göre, "... bu özgürlüklerin kullanılması, demokratik bir toplumda ulusal güvenliğin, toprak bütünlüğünün veya kamu güvenliğinin korunması, kamu düzeninin sağlanması ve suç işlenmesinin önlenmesi, sağlığın veya ahlâkın, başkalarının şöhret ve haklarının korunması, gizli bilgilerin yayılmasının önlenmesi veya yargı erkinin yetki ve tarafsızlığının güvence altına alınması için gerekli olan bazı formaliteler, koşullar, sınırlamalar veya yaptırımlara tabi tutulabilir."

Görüldüğü üzere yasayla düzenlemek şartıyla ve "başkalarının şöhret ve haklarının korunması" amacıyla ifade özgürlüğünün sınırlandırılabilmesi kabul edilmekte olup sınırlama haklı olsa bile, bu kez sınırlamanın orantınlığı gündeme gelecektir (bkz. sınırlamanın orantısızlığı konusunda Pakdemirli/Türkiye kararı). Kişilik hakkının korunması ile ifade özgürlüğü arasındaki dengeyi iyi sağlamak gerekmektedir. Özellikle siyasetçilerin ve devlet görevlilerinin kişilik hakları ve şöhretleri söz konusu olduğunda bu dengede ifade özgürlüğünün ağır bastığı konusunda kuşku yoktur. Diğer bir deyişle, terazide bir yanda siyasetçilerin ve devlet görevlilerinin "kişilik hakları", diğer yanda "ifade özgürlüğü" bulunduğu durumlarda, tercihin daha çok ifade özgürlüğünden yana kullanıldığı

söylenbilir (Dođru, O., Nalbant, A; İnsan Hakları Avrupa Sözleşmesi Açıklama ve Önemli Kararlar, C. 2, Ankara 2013, s. 232).

3. Müdahalelerin demokratik bir toplumda gerekli olup olmadığı konusu:

AİHM, ifade özgürlüğünün, demokratik bir toplumun temel yapılarından birini oluşturduğu ve toplumun gelişimi ve bireyin kendini gerçekleştirmesinin temel koşullarından biri olduğunu hatırlatır (Lingens/Avusturya, başvuru no: 9815/82, 08 Temmuz 1986). İfade özgürlüğü istisnalara tabi olsa da, bu istisnalar dar bir biçimde yorumlanmalı ve sınırlama nedeni ikna edici bir biçimde ortaya konmalıdır (Observer ve Guardian/Birleşik Krallık, A Serisi no: 216, başvuru no: 13585/88, 26.11.1991).

Nitekim aynı ilkeler Hukuk Genel Kurulunun 25.04.2018 tarihli ve 2017/4-1320 E., 2018/986 K.; 30.05.2018 tarihli ve 2017/4-1470 E., 2018/1144 K. sayılı kararlarında da benimsenmiştir.

Basın özgürlüğü ise ifade özgürlüğünün en önemli unsurlarından birisidir. AİHM basın ile ilgili kararlarında ifade özgürlüğünün demokratik bir toplumun esaslı temellerinden birisini oluşturduğuna değinildikten sonra basına tanınması gereken güvencelerin özel bir öneme sahip bulunduğu belirtilmektedir. Basın ve diğer medya organlarının ifade özgürlüğü kamuoyuna yöneticilerin görüş ve davranışlarını tanıtmak ve yargılamak için en iyi araçlardan birisini sunmaktadır. Basına siyasal arenada ve kamunun ilgilendiği diğer alanlarda tartışma konusu olan bilgi ve görüşleri iletme görevi düşer. Basının bu görevi, kamuoyunun da bilgi ve görüşleri alma hakkı ile tanımlanır (Handyside/Birleşik Krallık, 7 Aralık 1976, Başvuru No: 5493/72, 49, Centro Europa 7 S.R.L. And Dı Stefano/İtalya, Başvuru No: 38433/09, 131).

O hâlde basın özgürlüğü bir yönüyle halkı ilgilendiren haber ve görüşleri iletme özgürlüğüdür, diğer yönüyle de halkın bu bilgi ve görüşleri alma hakkıdır. Mahkeme'ye göre basın ancak bu şekilde, kamuoyunun bilgi edinme hakkı bakımından yaşamsal önemi bulunan "halkın gözcülüğü" ya da "bekçisi" görevi yapabilir. Basın özgürlüğü söz konusu olduğunda, ulusal makamlara tanınan takdir yetkisi demokratik bir toplumun yararı dikkate alınarak sınırlandırılır (Éditions Plon/Fransa, Başvuru No: 58148/00, 44; Bladet Tromsø And Stensaas/Norveç, Başvuru No: 21980/93, 59).

Burada şu hususun da ifade edilmesi gerekir ki, Sözleşme'nin 10. maddesi sadece ifade edilen haber ve fikirlerin içeriğini değil, fakat aynı zamanda bunların nakledilme biçimlerini de korur. (Oberschlick/Avusturya, Başvuru No: 20834/92, 57). AİHM'nin yerleşik içtihadına göre; gazetecilik özgürlüğü ve mesleği, belirli ölçüde abartma, hatta kışkırtma unsurunu da içerir (Prager And Oberschlick/Avusturya, Başvuru No: 15974/90, 38).

Basının “başkalarının itibarını korumak” gibi çizilmiş sınırları aşmaması gerekmele birlikte kamunun menfaatinin bulunduğu diğer alanlarda olduğu gibi, siyasi meselelerde de haber ve fikirleri iletme yine basına düşen bir görevdir. Sadece basının bu tür haber ve fikirleri iletme görevi yoktur, halkın da bunları edinme hakkı da vardır (Sunday Times/Birleşik Krallık, parag. 30, başvuru no: 6538/74, 26.04.1979).

Basın özgürlüğünün iç hukukumuzda nasıl yer aldığı konusuna gelince;

1982 Anayasasının “Basın Hürriyeti” başlıklı 28. maddesi ile 5187 sayılı Basın Kanununun 3. maddesi basın özgürlüğünü düzenlemiş ve bunun sınırlarını göstermiştir.

5187 sayılı Kanunun 3. maddesinde;

“Basın özgürdür. Bu özgürlük; bilgi edinme, yayma, eleştirme, yorumlama ve eser yaratma haklarını içerir.

Basın özgürlüğünün kullanılması ancak demokratik bir toplumun gereklerine uygun olarak; başkalarının şöhret ve haklarının, toplum sağlığının ve ahlâkının, millî güvenlik, kamu düzeni, kamu güvenliği ve toprak bütünlüğünün korunması, Devlet sırlarının açıklanmasının veya suç işlenmesinin önlenmesi, yargı gücünün otorite ve tarafsızlığının sağlanması amacıyla sınırlanabilir.”

hükmü yer almaktadır.

Bu hükümden de anlaşılacağı üzere; basın özgürlüğü, kişinin dünyada ve özellikle içinde yaşadığı toplumda meydana gelen ve toplumu ilgilendiren olay ve olgular hakkında bilgi sahibi olmasını sağlamayı amaçlar.

Bunun gereği olarak basın, haber toplamak, fikir ve kanaatleri izleyerek bunları çözümlmek, yorumlamak, eleştirmek ve sonuçta kamuoyunu ilgilendiren konularda doğru ve gerçeğe uygun haber vermek hakkına sahip ve bununla görevlidir. Eş söyleyişle denetim, uyarma, eleştiri ve gerçekleri açıklama, basının doğal görevleridir.

Yine basın özgürlüğü ile bağlantılı kavramlar olarak; Anayasa da düşünce ve kanaat (m. 25); düşünceyi açıklama ve yayma hürriyeti (m. 26) ayrıntılı şekilde düzenlenmiştir. Demokratik yaşamın gelişmesinde, ulusal birliğin sağlanmasında, kamuoyunun sağlıklı bir biçimde oluşmasında, sosyal ve siyasal ilerlemede basının çok önemli bir fonksiyonunun bulunduğu açık ve kuşkuşuzdandır.

Doğaldır ki basının bu ayrıcalıklı konumu ve hukuk düzeninin kendisine tanıdığı özgürlük, tüm özgürlükler gibi yine hukuk düzenince çizilen sınırlara tabidir. Basın, yaptığı yayımlarda gerek Anayasanın “Temel Hak ve Özgürlükler” bölümünde yer alan ve gerekse de MK'nın 24 ve 25.

maddelerinde ve ayrıca özel yasalarda güvence altına alınmış olan, kişilik haklarına saygı göstermek, bunlara saldırı niteliği taşıyabilecek tutum ve davranışlardan kaçınmak zorundadır.

Bu cümleden olarak basın, belirli bir kişinin fikrini tartışmak zorunda kaldığı durumlarda bile, objektif bilgi vermekle ve eleştirmekle yetinmeli, olayları tahrif etmek veya kuşkuları yaymak gibi hukukun izin vermeyeceği yollara başvurmamalıdır. Özellikle de hakaret niteliğinde ya da yersiz, onur kırıcı söz ve deyimlerin kullanılmasından kaçınmalıdır.

Basının kamu görevi yapmasında göz önünde tutulan amaçla, kişilik haklarına verilen zarar arasında açık bir oransızlık varsa, yayımın hukuka aykırı olduğu kabul edilmelidir. Objektiflikten ayrılmak, haber sınırını aşmak, genişletici ve yanlış yorumlarda bulunmak, gerçek dışı haber vermek, yersiz şekilde onur kırıcı sözler kullanmak, dürüstlük kurallarına aykırı davranmak, kişisel nedenlerle salt sansasyon için yayım yapmak hukuka aykırıdır.

Bu açıklamalardan sonra, denilebilir ki, basın özgürlüğünün kişilik haklarına üstün tutulabilmesi için haberin gerçeğe uygun olması, gerçeğe uygun yayımın haber niteliği taşıması, gerçeğe uygun haberlerin verilmesinde nesnel (objektif) ölçütlere uyulması, haberin veriliş biçimi yönünden özle biçim arasında ölçülülük bulunması gerekir. Bir yayımın hukuka uygun olduğunun kabul edilebilmesi ancak açıklanan bütün bu koşulların birlikte varlığı halinde mümkündür. Yapılan bir yayım bu temel ilkelerden herhangi birine ters düşüyorsa hukuka aykırılık unsuru gerçekleşmiş olacaktır (Yargıtay Hukuk Genel Kurulunun 05.06.2015 tarihli ve 2014/4-33 E., 2015/1504 K., 08.05.2013 tarihli ve 2012/4-1162 E., 2013/631 K.sayılı kararları).

Önemle vurgulanmalıdır ki yayımlanmasında kamu yararı bulunan, gerçek ve güncel bir haberin veya eleştirinin, özle biçim arasında denge kurulmak suretiyle verildiği durumlarda manevi tazminat sorumluluğunun temel ögesi olan "hukuka aykırılık" gerçekleşmeyeceğinden basının sorumluluğu da söz konusu olamaz.

Basın objektif sınırlar içinde kalmak suretiyle olay ve konu ile ilgili olan, görünen, bilinen her şeyi araştırma, inceleme ve olayları o anda belirlenen biçimi ile değerlendirme, yayma ve yayınlama yetki ve sorumluluğuna sahip olmakla birlikte, haberin verilişi sırasında özle biçim arasındaki dengenin bozulmaması gerekir.

Öte yandan haberde gerekli, yararlı ve ilgili olmayan nitelermeler ve yorumlar yapıldığı, haberin içeriğine uygun düşmeyen, tahrik edici, kamuoyunda husumet ve kuşku yaratıcı, güveni zedeleyici bir üslubun kullanıldığı durumlarda, özle biçim arasındaki denge bozulmuş sayılır. Bu da hukuka aykırılığın varlığını kabule imkan sağlar.

Diğer bir anlatımla basın, olayları izleme, araştırma, değerlendirme, yayma ve böylece kişileri bilgilendirme, öğretme, aydınlatma, yönlendirme yetki ve sorumluluğuna sahiptir. Bunun içindir ki basının yaptığı yayından dolayı hukuka aykırılık teşkil edecek olan eylemi, genel olaylardaki hukuka aykırı olan eylemden farklılıklar taşır. İşte bu farklılık ve ayırık durum gözetilerek yapılan yayının hukuka aykırılık veya uygunluk sınırı belirlenmelidir. Basın dışı bir olaydaki davranış biçiminin hukuka aykırılık oluşturduğunun kabul edildiği durumlarda, basın yoluyla yapılan bir yayındaki olay hukuka aykırılık oluşturmayabilir. İşte basının bu nedenle ayrı bir konumu bulunmaktadır.

Ne var ki, basının bu ayrıcalık taşıyan konumu ve özgürlüğü, tüm özgürlüklerde olduğu gibi sınırsız değildir. Bundan dolayıdır ki, yayınlarında kişilik haklarına saygı göstermesi ve gerek Anayasanın Temel Haklar ve Ödevler bölümünde yer alan ve gerekse 4721 sayılı Türk Medeni Kanununun (TMK) 24 ve 25. maddelerinde ve yine özel yasalarda güvence altına alınmış bulunan kişilik haklarına saldırıda bulunmaması yasal bir zorunluluk ve hukuki gerekliliktir.

Yine, basının manevi tazminat sorumluluğunun doğması 818 sayılı Borçlar Kanununun 49. (6098 sayılı Türk Borçlar Kanunu m. 58) maddesindeki koşulların gerçekleşmiş olmasına bağlıdır.

Bütün bunların yanı sıra eldeki uyuşmazlığın çözümünde özel hayata saygı hakkının ve kişisel veri kavramının da değerlendirilmesi gerekmektedir.

Avrupa İnsan Hakları Sözleşmesinin özel hayatın ve aile hayatının korunmasına ilişkin 8. maddesi;

“1. Herkes özel hayatına, aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, .dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir.”

2709 sayılı Türkiye Cumhuriyeti Anayasasının ilgili maddesi ise;

“A. Özel hayatın gizliliği

Madde 20- Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz (Üçüncü cümle mülga: 3/10/2001-4709/5 md.).

...

(Ek fıkra: 07/05/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp

kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.”

şeklindedir.

Nitekim dava tarihinden sonra 07.04.2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanununun 3/1-(d) maddesinde tanımlandığı şekliyle kişisel veri, “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi” ifade eder şeklinde tanımlanmıştır.

Avrupa Birliği'nin 95/46/EC sayılı Bireylerin Kişisel Verilerinin İşlenmesi ve Serbestçe Dolaşımı Karşısında Korunmasına İlişkin Direktif'in 2/a maddesinde ve Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair 108 sayılı Avrupa Konseyi Sözleşmesi'nin 2(a) maddesinde benzer tanımlama yer almaktadır.

Avrupa İnsan Hakları Sözleşmesinde kişisel verilerle ilgili açık bir düzenleme bulunmamakla birlikte AİHM konuyla ilgili kararlarında kişisel veri kavramının içeriğini doldurmuştur. Kişisel verilerin sınırlı bir şekilde sayılması mümkün değil ise de, bireyin kimliğini ortaya çıkartan, bir kişiyi belirli kılan ve karakterize eden kişinin kimlik, ekonomik ve dijital bilgileri, tabiiyeti, kanaatleri, ırk, siyasî düşünce, felsefî inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık bilgileri, fotoğrafları, parmak izi, sağlık verileri, telefon mesajları, telefon rehberi, sosyal paylaşım sitelerinde yazdığı veya paylaştığı yazılar, fotoğraf, ses veya görüntü kayıtları kişisel veri olarak kabul edilebilir.

6698 sayılı Kişisel Verilerin Korunması Kanununun “Özel nitelikli kişisel verilerin işlenme şartları” başlıklı 6. maddesinin 1. fıkrasında “Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri”nin özel nitelikli kişisel veri olduğu düzenlenmiş, aynı maddenin 2. fıkrasında ise “Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.” hükmüne yer verilmiştir.

Önümüze gelen sorunun temelinde kişisel verilerin ve dolayısıyla özel hayatın korunması ile basın özgürlüğünün birbiri karşısındaki sınırlarının belirlenmesi yatmaktadır. Sorunun çözümünde dikkat edilmesi gereken husus ise, basın özgürlüğü ile bireyin özel hayatı kapsamında kalan kişisel verilerinin korunmasını isteme hakkı arasında adil bir dengenin kurulması gerekliliğidir. Bu adil

dengenin tespiti için yayınlanan haberin kamu yararı içeren tartışmalara bir katkısının olup olmadığının değerlendirilmesi gerekmektedir (Alkaya/Türkiye, Başvuru No: 42811/06).

Kişisel verilerin korunması temel hak ve özgürlükler ile yakından ilişkilidir. Çünkü kişisel verilerin açıklanması öncelikle özel hayatın gizliliğini ihlal edilebileceği gibi başka bir takım bağlantılı hakları da zarara uğratabilir.

Son yıllarda özellikle bilişim ve iletişim teknolojilerinin çok hızlı gelişmesi, kişisel verilerin daha da kolay toplanmasına, işlenmesine, paylaşılmasına ve depolanmasına imkân sağlamıştır. Bu durum kişisel verilerin korunması kavramının önemini her geçen gün daha da artırmaktadır. Kişisel verilerin korunması hakkının temel amacı, bireyin özel yaşamının gizliliğinin güvence altına alınması yoluyla kişiyi korumaktır. Bilgi toplumunda giderek önemli bir konu hâline gelen kişisel verilerin korunması hakkı, bireyin demokratik bir hukuk devletinde özgür iradesiyle kendi yaşamını bizzat düzenleyebilmesinin bir gereği olarak karşımıza çıkmaktadır. Diğer taraftan bireyin kişiliğini serbestçe geliştirmesi, kişiliğinin korunması ve özgür bireylerden oluşan bir toplum düzeninin oluşturulması, ancak bireyin kişisel verilerine ilişkin hakkının korunmasıyla mümkündür.

Avrupa İnsan Hakları Sözleşmesinin (AİHS) 8. maddesinde yer alan özel yaşama saygı hakkı kapsamında korunan "mahremiyet hakkı", bireyin kendisi hakkındaki bilgileri kontrol edebilmesi şeklindeki hukuki çıkarlarını da içermektedir. Zira bireyin kendisine ait herhangi bir bilginin, kendi rızası olmaksızın açıklanmaması, yayılmaması ve bu bilgilere başkalarının ulaşamaması kısacası kişisel verilerinin mahrem kalması konusunda hukuki menfaati bulunmaktadır (Arslan Öncü, G., Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması, Beta Yayınları, İstanbul 2011, s.182).

Kişisel verilerin korunmasının sağlanması ile birlikte özel hayatının gizliliği korunmuş olacaktır.

Nitekim aynı ilkeler Hukuk Genel Kurulunun 17.06.2015 tarihli ve 2014/4-56 E., 2015/1679 K. sayılı kararında da benimsenmiştir.

Tüm bu açıklamalar ve yasal düzenlemeler ışığında somut olay incelendiğinde; dava konusu Anadolu'da Vakit Gazetesinin 29.06.2010 tarihli nüshasının birinci ve sekizinci sayfalarında yer alan "Generallerin Yahudi Damatları" başlıklı haberin alt başlığında "Bazı üst düzey komutanların siyonistlerce kutsal kabul edilen Ağlama Duvarı'ndaki görüntülerinin ortaya çıkmasının ardından şimdi de bazı üst düzey generallerin damatlarının yahudi olduğu bilgisine ulaşıldı" ifadelerine yer verildiği, haber içeriğinde ise davacılar hakkında, "Birinci Ordu Komutanı Org. Hasan İğsız'ın tek kızı olan'nın bir İspanya Yahudisiyle evli olduğu tespit edildi. Tek oğlu olan Hüseyin Hakan'ın ... olduğu anlaşılan Org. Hasan İğsız'ın kızı, Eduardo isimli bir Yahudi ile evli. Evlendikten sonra

Matos Martin soy ismini alan'nın kocası İspanya uyruklu ve Yahudi asıllı 1972 Cacades doğumlu ..., İspanya Yahudilerinden Adolfa Matos Martin'in oğlu." ifadelerinin kullanıldığı anlaşılmaktadır.

Yukarıda belirtilen açıklamalar dikkate alındığında, haber içeriğinde davacı ...'in rızası dışında yer verilen doğum yeri, doğum tarihi ve baba ismi, vatandaşlık durumu ve dini inancı kişisel veri niteliğindedir.

Avrupa Birliği Adalet Divanı'nın "Google Kararı"nda açıkladığı gibi ilgili verinin kamu hayatında oynadığı önemli rol ve halkın ilgili veriye yönelik yoğun ilgisi şeklinde, üstün bir kamu yararını ortaya koyan özel sebepler bulunmadığına göre gazete haberinde kişisel veriler açık bir şekilde yer almamalıdır.

Bu durumda dava konusu haberin yukarıda vurgulanan AİHM içtihatları karşısında basın özgürlüğü kapsamında kalmadığı, davacı ...'in kişisel verilerine rızası dışında yer verilerek davacının özel hayatının gizliliğinin ihlal edildiği, davacının kişilik haklarına saldırı niteliği taşıdığı kabul edilmelidir.

Hukuk Genel Kurulunda yapılan görüşmeler sırasında, haberde kullanılan ifadelerin nefret söylemi olarak değerlendirilemeyeceği, kamunun bilgilendirilmesi anlamında konunun haber değeri bulunduğu, davalı ... hakkında davacı ...'e yönelik kişisel verileri hukuka aykırı yaymak ve kişisel verilerin kaydedilmesi suçlarından beraat kararı verildiği, haberin bu davacının kişilik haklarına saldırı teşkil etmediği, bu nedenle direnme kararının bozulması gerektiği görüşü ileri sürülmüş ise de, bu görüş Kurul çoğunluğu tarafından benimsenmemiştir.

O hâlde, davacı ...'in kişisel verilerinin hukuka aykırı olarak habere konu edildiğini, dini inancının birden çok kez vurgulandığını, haberin basın özgürlüğü sınırları içinde kalmadığını, özel hayatı ile din ve vicdan hürriyetinin ihlal edildiğini, davacı ... yönünden manevi tazminat koşullarının gerçekleştiğini kabul eden direnme kararı yerindedir.

Ne var ki, Özel Dairece tazminat miktarı yönünden bir inceleme yapılmadığından bu yöne ilişkin temyiz itirazlarının incelenmesi için dosyanın Özel Daireye gönderilmesi gerekir.

II- Davalılar vekilinin davacı ...'e yönelik temyizi yönünden;

BK'nın 49. (6098 sayılı TBK m. 58) maddesi gereğince kişilik hakları hukuka aykırı olarak saldırıya uğrayan kimse manevi tazminata hükmedilmesini isteyebilirse de; hâkimin özel hâlleri göz önünde tutarak manevi zarar adı ile hak sahibine verilmesine karar vereceği para tutarı adalete uygun olmalıdır. Hâkim manevi tazminatın miktarını tayin ederken saldırı teşkil eden eylem ve olayın

özelliği yanında tarafların kusur oranını, sıfatını, işgal ettikleri makamı ve diğer sosyal ve ekonomik durumlarını da dikkate almalıdır.

22.06.1966 tarihli ve 1966/7 E., 1966/7 K. sayılı İçtihadı Birleştirme Kararının gerekçesinde takdir olunacak manevi tazminatın tutarını etkileyecek özel durum ve koşullar açıkça gösterilmiştir. Miktarın belirlenmesinde her olaya göre değişebilecek özel hâl ve şartların bulunacağı gözetilerek hâkim, bu konuda takdir hakkını kullanırken ona etkili olan nedenleri de karar yerinde objektif ölçülere göre isabetli bir biçimde göstermelidir. Çünkü kanunun takdir hakkı verdiği hususlarda hâkimin hukuka ve hakkaniyete göre hüküm vereceği Türk Medeni Kanununun 4. maddesinde belirtilmiştir. Hükmedilecek bu tutar, zarara uğrayanda manevi huzuru doğurmayı gerçekleştirecek tazminata benzer bir fonksiyonu olan özgün bir nitelik taşır. Manevi tazminat bir ceza olmadığı gibi mal varlığı hukukuna ilişkin bir zararın karşılanmasını da amaç edinmemiştir. O halde bu tazminatın sınırı onun amacına göre belirlenmelidir. Takdir edilecek miktar, mevcut durumda elde edilmek istenilen tatmin duygusunun etkisine ulaşmak için gerekli olan kadar olmalıdır.

Ayrıca, AİHM kararlarında da ifade özgürlüğüne getirilecek sınırlamanın; kanuni olması, meşru amaca dayanması ve demokratik toplumda gerekli olmasının yanı sıra orantılı olması gerektiği belirtilmiştir. İfade özgürlüğünün esas, sınırlamanın ise istisna olması nedeniyle getirilecek sınırlama (somut olayda tazminat miktarı) kişilik haklarına yapılan saldırı ile orantılı olmalıdır. Aksi hâlde sınırlama, AİHS'in 10. maddesine aykırılık teşkil edecektir (AİHM 35839/97 Başvuru numaralı Pakdemirli/Türkiye kararı).

Somut olayda, dava konusu haberde yer alan ve yukarıda belirtilen ifadelerin yanı sıra, haber kapsamında davacı ...'e ait pasaportun fotoğraf ve kimlik bilgilerinin bulunduğu sayfalarının görsel olarak kullanıldığı, bu görselde davacı ...'in kimlik bilgilerinin açık bir şekilde görüldüğü anlaşılmakta olup, haberin bir bütün hâlinde değerlendirilmesinde davacı ...'in kişilik haklarına saldırı teşkil ettiği hususunda yerel mahkeme ile Özel Daire arasında herhangi bir uyuşmazlık bulunmamaktadır.

Ancak davacı ... lehine hükmedilen manevi tazminat miktarına bakıldığında olay tarihi, haberin veriliş biçimi, kullanılan ifadeler ve tarafların ekonomik ve sosyal durumları dikkate alındığında, hükmedilen manevi tazminatın fazla olduğu kanaatine varılmıştır.

Hâl böyle olunca tarafların karşılıklı iddia ve savunmalarına, dosyadaki tutanak ve kanıtlara, bozma kararında açıklanan gerektirici nedenlere göre, Hukuk Genel Kurulunca da benimsenen Özel Daire bozma kararına ... yönünden uyulmak gerekirken, önceki kararda direnilmesi usul ve yasaya aykırıdır.

Bu nedenle davacı ... yönünden direnme kararı bozulmalıdır.

SONUÇ: Yukarıda (I) numaralı bentte açıklanan nedenlerle davacı ... yönünden direnme kararı uygun olup davalılar vekilinin hükmedilen tazminat miktarına yönelik temyiz itirazlarının incelenmesi için dosyanın 4. HUKUK DAİRESİNE GÖNDERİLMESİNE, oy çokluğuyla,

(II) numaralı bentte açıklanan nedenlerle davalılar vekilinin davacı ...'e yönelik temyiz itirazlarının kabulü ile direnme kararının Özel Daire bozma kararında gösterilen nedenlerden dolayı BOZULMASINA, istek hâlinde temyiz peşin harcının yatırana iadesine, oy birliğiyle,

06.11.2018 tarihinde karar düzeltme yolu kapalı olmak üzere kesin olarak karar verildi.

Yargıtay Kararı - Hukuk Genel Kurulu (E. 2014/56)

HGK., E. 2014/56 K. 2015/1679 T. 17.6.2015

Esas No.: 2014/56

Karar No.: 2015/1679

Karar Tarihi: 17.06.2015

Taraflar arasındaki “manevi tazminat” davasından dolayı yapılan yargılama sonunda; İzmir 3. Asliye Hukuk Mahkemesince davanın kısmen kabulüne dair verilen 11.04.2011 gün ve 2010/399 E. 2011/172 K. sayılı kararın incelenmesi taraflar vekili tarafından istenilmesi üzerine, Yargıtay 4. Hukuk Dairesinin 08.11.2012 gün ve 2011/7193 E. 2012/16450 K. sayılı ilamıyla;

“...Dava, haksız fiil nedeni ile manevi tazminat istemine ilişkindir. Yerel mahkemece istemin bir bölümü kabul edilmiş; karar, taraflarca temyiz olunmuştur

Davacı vekili, müvekkilinin cinsel taciz suçundan şikayetçi olduğu ceza davasının yapılan yargılaması sonucunda, mahkeme ilamının temyizi sonrasında Yargıtay'ca verilen kararın davalılara ait Yorumlu-Uygulamalı Türk Ceza Kanunu adlı altı ciltlik eserde müvekkilinin ve diğer kişilerin isimlerinin açıkça yazılmak suretiyle yayınlandığını, bu durumun kişilik haklarına saldırı oluşturduğunu, belirterek davalıların manevi tazminatla sorumlu tutulmalarını talep etmiştir.

Davalılar vekili, söz konusu kitapların bilimsel eser niteliğinde olduğu, Avrupa İnsan Hakları Mahkemesi kararlarında davaların davacıların ismiyle adlandırıldığı, kitabın geniş kitlelere hitap etmediği, ceza hakimleri, savcılar ve ceza avukatlarınca okunduğu, kitapta isim belirtmenin hukuka aykırı olmadığını belirterek davanın reddini talep etmiştir.

Mahkemece, adı geçen eserde davacı ve diğer kişilerin isimlerinin kodlanmadan açıkça yazıldığı, söz konusu olayların anlatımında açıkça isim belirtmenin kitap içeriğine bir fayda sağlamadığı gibi, davacının isminin geçtiği olayın hassasiyeti ve Türk toplum yapısı da göz önünde tutulduğunda, yurt çapında dağıtımı ve satışı yapılan bir kitapta, bu tür bir olayla davacının adının açıkça belirtilmesinin davacının kişilik haklarını zedelediği, çevresine karşı davacıyı zor duruma düşürdüğü gerekçesi ile davanın kısmen kabulüne karar verilmiştir.

Bilimsel bilgi, taşıdığı özellikler dolayısıyla fikir üretiminin en yüce değer ve biçimi olma niteliğine haizdir ve herşeyden önce, insanlığın gerçekliğe ulaşması bakımından önemli bir araç sayılır. Bu durum, bilimsel bilgi ve onu üreten araştırmacının geniş bir özgürlük alanında bulunmasını

gerektirir. Bilimi serbestçe öğrenme, araştırma, yayma ve öğretme haklarını içeren bilim özgürlüğü Anayasada kişisel haklar arasında (madde 27) düzenlenmiştir. Anılan madde de herkesin bilim ve sanatı serbestçe öğrenme ve öğretme, açıklama ve yayma ve bu konularda araştırma yapma hakkına sahip olduğu belirtilmektedir. Keza, AB Temel Haklar Bildirgesinin 13. maddesinde "sanat ve bilimsel araştırma kısıtlamaya tabi olmamalıdır. Akademik özgürlüğe saygı gösterilmelidir" ibaresine yer verilmiştir. Bu bağlamda bilimsel özgürlük, bilimsel bir etkinlikte bulunan veya böyle bir faaliyette bulunmak isteyen tüm bireylere tanınmış ve bu bireylerin kişiliğine sıkı sıkıya bağlı kalmış, öznel temel haktır.

Taşıdığı önem dolayısıyla insan hakları belgelerine giren bilim özgürlüğü, araştırma özgürlüğünü, araştırma için zorunlu araçlara ve ortama sahip olma hakkını ve bilimsel üretme özgürlüğü veya bilgilendirme ve yayın hakkını içerir. Bu çerçevede bilim adamı bilimsel metotlarını kullanarak araştırma yapma hakkına ve bu araştırmanın sonuçlarını yayma hakkına sahip olacak, kural olarak bu konularda dış bir engelle karşılaşmayacaktır. Hatta bu konularda karşılaşacağı maddi ve manevi engeller devlet tarafından ortadan kaldırılacaktır.

Düşünce özgürlüğünün bir alt kategorisi olan fakat, üretilmesindeki özel çabanın ya da emeğin doğal sonucu olarak, sıradan düşünceye göre daha sistematik ve derin sayılması gereken bilimsel eserler, kural olarak ancak kendi ilkeleri çerçevesinde sınır tanır ve istisnaen ancak insan yaşamına yönelen bir tehlike olasılığında kısıtlanabilirler. Bunun ötesine geçilerek yapılan sınırlamalar, toplumun bilimsel düşüncelerle buluşmasını önleyebilecek ve dolayısıyla gerçekliğe ulaşılmasını engelleyebilecektir. Bu bakımdan bilimsel özgürlük hukuki rejim ve yaptırım açısından diğer entelektüel özgürlüklere göre daha mutlak bir özgürlük rejiminden yararlanmasını gerektirir. Fakat tüm özgürlüklerde olduğu gibi bilimsel özgürlük de sınırsız değildir. Bilim özgürlüğü ile kişilerin, kişilik değerlerinin karşı karşıya geldiği durumlarda somut olaydaki olgular itibariyle koruma altına alınmış bulunan bu iki değerden birinin diğerine üstün tutulması gerekecektir.

Davaya konu olayda; bilimsel araştırma özgürlüğü kapsamında, aleniyet kazanmış ve kamu malı haline gelmiş Yargıtay ilamı, tarafların isimleri kodlanmadan davalıların yazmış oldukları Yorumlu-Uygulamalı Türk Ceza Kanunu adlı altı ciltlik bilimsel çalışma ürünü olan kitapta yayınlanmıştır. Adı geçen eserin bilimsel nitelikli bir çalışma olduğu, kamuya açık hale gelen Yargıtay kararının bilimsel çalışma ürünü olan kitapta olduğu gibi yer almasından dolayı yukarıda anlatılan ilkeler gereği davalıların sorumlu tutulamayacağı, çatışan yararlar dengesinin davacı aleyhine bozulmadığı, bu olayın davacının kişilik haklarına saldırı teşkil etmeyeceği gözetilerek davanın tümünden reddine karar

verilmesi gerekirken, yazılı biçimde karar verilmiş olması usul ve yasaya uygun düşmediğinden kararın bozulması gerekmiştir...”

gerekçesiyle bozularak dosya yerine geri çevrilmekle, yeniden yapılan yargılama sonunda; mahkemece önceki kararda direnilmiştir.

TEMYİZ EDEN: Davalılar vekili

HUKUK GENEL KURULU KARARI

Hukuk Genel Kurulunca incelenerek direnme kararının süresinde temyiz edildiği anlaşıldıktan ve dosyadaki kağıtlar okunduktan sonra gereği görüldü:

Dava, kişilik hakkına saldırı nedenine dayalı tazminat istemine ilişkindir.

Davacı K1 vekili 16/08/2010 harç tarihli dava dilekçesinde özetle; “müvekkilinin 14/11/2003 tarihinden beri İzmir Adliyesinde savcılık zabıt katibi olarak görev yaptığını, 18/07/2005 ile 11/04/2006 tarihleri arasında o dönem İzmir C. Başsavcı vekili olarak görev yapan K2 ile çalışmak için görevlendirildiğini ancak başladıktan sonra 8 ay boyunca Başsavcı vekilinin sözlü ve fiziksel taciziyle karşı karşıya kaldığını, fiziksel tacizin başlaması ve bu durumun çekilmez hale gelmesi nedeniyle davacının şikayette bulunduğunu, ailesinin ve çevresinin duymaması için çaba sarf ettiğini, K2 hakkında soruşturma açıldığını ve cezalandırıldığını, sanığın Başsavcı vekili olması nedeni ile olayların o dönem için basında yer aldığını, davacının bu olayları unutmaya başladığı bir dönemde Yargıtay 4. Ceza Dairesi Başkanı ve tetkik hakimleri olan davalıların Nisan 2010 tarihinde yorumlu-uygulamalı Türk Ceza Kanunu adlı altı ciltlik eser yayınladıklarını, örnek Yargıtay kararlarının başladığı 3262 nolu sayfa ve devamındaki sayfalarda davacının başına gelen olayların, tüm aktörlerin isimlerinin açıkça yazılmak suretiyle ve olayın tamamının açık bir şekilde anlatıldığını, davacı tarafından bu durumun öğrenilmesiyle davacının tekrar psikolojik bunalıma girdiğini, bütün kötü olayları tekrar yaşamak zorunda kaldığını, adliyede çalışması nedeniyle bu olayın davacının çevresinde, savcı ve avukatlar tarafından duyulduğunu, müvekkilinin zor da olsa saklayabildiği bir olayın kamuoyuna duyurulduğunu, iffetinin tartışılır hale geldiğini, bir genç kızın hayalleri ve geleceğinin kararmış olduğunu, eserin bir defa yararlanılacak bir eser olmadığını, uzun yıllar boyunca yaygın kitlelerce okunacak nitelikte bulunduğunu belirterek tüm bu nedenlerle davacının isminin geçtiği söz konusu ciltlerin toplatılmasını, 50.000,00-TL manevi tazminatın davalılardan tahsiline karar verilmesini istemiştir.

Davalılar K3., K4, K5 ve F1 Basın Yayın ve Dağıtım San. Ve Tic. Ltd. Şti. vekili 11.10.2010 havale tarihli cevap dilekçesinde özetle; “ Söz konusu kitapların bilimsel eser niteliğinde olduğunu, bilimsel eser

niteliğinde olan kitaplarda fail ve mağdur adının olmasının hukuka aykırı olmadığını, ceza hukukundaki kitaplarının kaynağının yargısal kararlar olduğunu, geniş kitlelere hitap etmediğini, ceza hakimleri, savcılar ve ceza avukatlarınca okunduğunu, kitapta isim belirtmenin hukuka aykırı olmadığını, eserde adı geçen kişilerle ilgili vakıalar daha önce yargı konusu olduğu için ilgili mahkemelerin bulunduğu yerlerdeki kişiler tarafından duyulup öğrenildiğini, bu nedenle sözü edilen vakıaların ilk defa dava konusu eserde gündeme getirilmediğini, AİHM kararlarının ve Anayasa Mahkemesi kararlarının da isimler çıkarılmadan yayınlandığını, 2011 yılının başından itibaren UYAP sisteminde bulunan kararlardaki kişisel veriler rumuzlanmadan hakim ve savcının kullanımına açıldığını, dava konusu kararın son bölümünde rumuzlama yapılmış ise de ilk bölümünde yapılmamasının dizgi hatası olduğunu, olayın üzerine adliyeye gelen müfettişin yaptığı soruşturma sırasında tüm adliyenin olayı öğrendiğini ve olayın basına da yansımalarını, yine davacının ileri sürdüğü hususların daha sonra düzeltilmiş ve düzeltilmiş bir nüshasının davacı vekilini sunulduğunu bu nedenle kitabın toplatılmasına gerek olmadığını istenen tazminatın fahiş olduğunu savunarak” davanın reddine karar verilmesini talep etmiştir.

Mahkemece, davanın kısmen kabulüne dair verilen kararın taraflarca temyiz edilmesi üzerine yukarıda başlık bölümünde yazılan Yargıtay ilamı ile bozulmuş, karar düzeltme istemi oyçokluğu ile reddedilmiş, mahkemece önceki gerekçeler tekrar edilerek direnilmiş; hükmü davalılar vekili temyize getirmiştir.

Hukuk Genel Kurulu önüne gelen uyuşmazlık; davalılar K3., K6 ve K5 tarafından yayına hazırlanan ve davalılardan F1 Basın Yay. Dağıtım San ve Tic. Ltd. Şti tarafından basılan eserde yer alan kararda, davalının isminin rumuzlanmadan ve rızası alınmadan açık bir şekilde yazılmasının kişilik hakkında saldırı oluşturup oluşturmayacağı noktasında toplanmaktadır.

İşin esasına girilmeden önce davacıya ait 13.01.2014 tarihli dilekçenin temyiz harcının tahsil edilip edilmediğinin belirlenmesi için dosyanın mahkemesine geri çevrilmesinin gerekip gerekmediği ön sorun olarak tartışılmış, şu sonuca varılmıştır:

Davacı vekiline gerekçeli karar 09.12.2013 tarihinde tebliğ edilmiştir. 15 günlük yasal temyiz süresi geçtikten sonra davacı vekili tarafından mahkemeye verilmiş bir dilekçe olmamasına rağmen 25.12.2013 (Çarşamba) tarihinde yazı işleri müdürü tarafından davacıdan temyiz harcı tahsil edilmesi için müzekkere yazılmıştır. Ancak temyiz harcının tahsiline dair tahsilât makbuzu dosya içinde bulunmamaktadır. Bir diğer deyişle süresi içinde harcı yatırılmış davacıya ait bir temyiz dilekçesi dosya içinde bulunmamaktadır. Davalılara ait temyiz dilekçesi ise 30.12.2013 tarihinde davacı vekiline tebliğ edilmiştir. 10 günlük yasal karşı temyiz süresi 09.01.2014 (Perşembe) sona erdikten

sonra davacı vekili (dilekçe tarihi: 13.01.2014 pazartesi havale tarihi 13.01.2014) temyize cevap dilekçesi vermiş direnme kararının onanmasını; az olan miktar yönünden dosyanın incelenmek üzere Yargıtay 4. Hukuk Dairesine gönderilmesi istenilmiştir. Bu nedenle davacının hem asıl hem de karşı temyiz süresini geçirdikten sonra verdiği dilekçe nedeni ile dosyanın geri çevrilmesine gerek olmadığı oybirliği ile kabul edilmiştir.

İşin esasına gelince; uyuşmazlığın çözümünde etkili yasal mevzuata bakılacak olursa;

Avrupa İnsan Hakları Sözleşmesinin ilgili maddeleri;

Özel ve aile hayatına saygı hakkı

1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.
2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.

şeklindedir.

Türkiye Cumhuriyeti Anayasası'nın ilgili maddeleri;

"IX. Bilim ve sanat hürriyeti

Madde 27 - Herkes, bilim ve sanatı serbestçe öğrenme ve öğretme, açıklama, yayma ve bu alanlarda her türlü araştırma hakkına sahiptir.

..."

"A. Özel hayatın gizliliği

Madde 20 - Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. (Üçüncü cümle mülga: 3/10/2001-4709/5 md.)

...

(Ek fıkra: 7/5/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

şeklindedir.

Türk Medeni Kanunu'nun ilgili maddeleri;

"II. Saldırıya karşı

1. İlke

Madde 24- Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir.

Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır."

şeklindedir.

Önümüze gelen sorunun temelinde unutulma hakkı ve bunun sonucu olan kişisel verilerin ve kişilik hakkının korunması ile bilim ve sanat hürriyetinin birbiri karşısında sınırlarının belirlenmesi yatmaktadır. Sorunun çözümünde dikkat edilmesi gereken husus, bilim ve sanat özgürlüğü ile bireyin temel hakları arasında adil bir dengenin kurulmasıdır.

Kişisel veri belli veya belirlenebilir olan gerçek veya tüzel bir kişiye ilişkin her türlü bilgiyi ifade eder. Avrupa Birliği'nin 95/46/EC sayılı Bireylerin Kişisel Verilerinin İşlenmesi ve Serbestçe Dolaşımı Karşısında Korunmasına İlişkin Direktif'in 2/a ve Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair 108 sayılı Avrupa Konseyi Sözleşmesi'nin 2(a) maddelerinde benzer tanımlama yer almaktadır.

Kişisel verilerin korunması insan haklarıyla yakından ilişkilidir. Çünkü kişisel verilerin açıklanması öncelikle özel hayatın gizliliğini ihlal edilebileceği gibi bir takım diğer bağlantılı hakları da zarar görebilir.

AİHS'de kişisel verilerle ilgili bir hüküm yoktur. Ancak mahkeme konuyla ilgili kararlarında kişisel veri içeriğini doldurmuştur. Hemen ifade edilmesi gerekir ki kişisel verinin sayısal olarak sınırlandırılması mümkün değildir. Ancak içtihatlar ve akademik yayınlar dikkate alındığında bireyin kimliğini ortaya çıkartan, bir kişiyi belirli kılan ve karakterize eden kişinin kimlik, ekonomik ve dijital bilgileri, tabiiyeti, kanaatleri, ırk, siyasî düşünce, felsefi inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık bilgileri, fotoğrafları, parmak izi, sağlık verileri, telefon mesajları, telefon rehberi, sosyal paylaşım sitelerinde yazdığı veya paylaştığı yazı, fotoğraf, ses veya görüntü kayıtları kişisel verileri olarak kabul edilebilir.

Kişisel verilerin korunması, çağımızda, insan hakları kavramı ve korunması bilincinin gittikçe gelişmesine paralel olarak önemini artırmaktadır. Kişisel verilerin korunması hakkının temel amacı, bireyin özel yaşamının gizliliğinin güvence altına alınması yoluyla kişiyi korumaktır. Bilgi toplumunda giderek oldukça önemli bir konu haline gelen kişisel verilerin korunması hakkı, bireyin, demokratik bir hukuk devletinde özgür iradesiyle kendi yaşamını bizzat düzenleyebilmesinin bir gereği olarak karşımıza çıkmaktadır. Diğer taraftan bireyin kişiliğini serbestçe geliştirmesi, kişiliğinin korunması ve özgür bireylerden oluşan bir toplum düzeninin oluşturulması, ancak bireyin kişisel verilerine ilişkin hakkının korunmasıyla mümkündür. Bu hak yukarıda ifade edildiği üzere TC Anayasası'nın 20/2 maddesinde açık bir şekilde düzenlenmiştir.

Unutulma hakkına gelince; unutulma hakkı ve bununla ilişkili olan gerektiği ölçüde ve en kısa süreliğine kişisel verilerin depolanması veya tutulması konuları, aslında kişisel verilerin korunması hakkının çatısını oluşturmaktadır. Her iki hakkın temelinde bireyin kişisel verileri üzerinde serbestçe tasarruf edebilmesini, geçmişin engeline takılmaksızın geleceğe yönelik plan yapabilmesini, kişisel verilerin kişi aleyhine kullanılmasının engellenmesini sağlamak yatmaktadır. Unutulma hakkı ile geçmişinde kendi iradesi ile veya üçüncü kişinin neden olduğu bir olay nedeni ile kişinin geleceğinin olumsuz bir şekilde etkilenmesinin engellenmesi sağlanmaktadır. Bireyin geçmişinde yaşadığı olumsuz etkilerden kurtularak geleceğini şekillendirebilmesi bireyin yararına olduğu gibi toplumun kalitesinin gelişmişlik seviyesinin yükselmesine etkisi de tartışılmazdır.

Unutulma hakkı; üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerin silinmesini ve yayılmasının önlenmesini isteme hakkı olarak ifade edilebilir.

Bu hak bir yandan kişiye "geçmişini kontrol etme", "belirli hususların geçmişinden silinmesini ve hatırlanmaması isteme hakkı" sağladığı gibi, diğer yandan muhataplarına kişi hakkındaki bir kısım bilgilerin üçüncü kişilerin kullanmamasını veya üçüncü kişilerin hatırlanmamasına yönelik önlenmeleri alma yükümlülüğü yükler. Bu hakkın; bireylerin fotoğraf, internet günlüğü gibi kendileri hakkındaki içerikleri silmek için üçüncü şahısları zorlamayı içermesinin yanında geçmişteki cezalarına ilişkin bilgilerin veya haklarında olumsuz yorumlara neden olabilecek bilgi ve fotoğraflarının kaldırılmasını isteme hakkını tanıdığı kabul edilmektedir. Diğer taraftan bu hak, bireyin geçmişindeki belirli yönlerinin mümkün olmayacak biçimde hatırlanmaması için önlemler alınmasını gerektirmektedir.

Avrupa İnsan Hakları Sözleşmesi (AİHS)'nin 8. maddesinde yer alan özel yaşama saygı hakkı altında korunan "mahremiyet hakkı"nın, bireyin kendisi hakkındaki bilgileri kontrol edebilmesi şeklindeki

hukuki çıkarlarını da içerdiği ifade edilmektedir. Zira bireyin kendisine ait herhangi bir bilginin, kendi rızası olmaksızın açıklanmaması, yayılmaması ve bu bilgilere başkalarının ulaşmaması kısacası kişisel verilerinin mahrem kalması konusunda hukuki menfaati bulunmaktadır. (Gülay Arslan Öncü, Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması, Beta Yayınları, İstanbul 2011, s.182)

Kişiyi unutulma hakkının sağlanması ile birlikte özel hayatının gizliliği korunmuş olacaktır.

Somut olaya bu kapsamda bakıldığında; davacı, kamu görevinin veya hizmet ilişkisinin sağladığı nüfuzu kötüye kullanarak, müteselsilen cinsel saldırı suçunun mağdurudur. 2006 yılında gerçekleşen eylem tarihinde davacı bekâr olup maruz kaldığı eylem geleceği açısından etkilidir. Yapılan yargılama sonunda kamu görevlisi olan sanık ceza almıştır. Temyiz istemi üzerine yapılan inceleme sonunda ise hüküm 2009 yılında onanmıştır. Mağdur davacı gerek hazırlık gerekse de yargılama sırasında cinsel saldırının nasıl gerçekleştiğini açık bir şekilde anlatmış, bu anlatımlar doğal olarak karar metnine geçirilmiştir. Karar mağdur ve sanığın ismi rumuzlanmadan 2010 yılı nisan ayında yayınlanan kitapta yer almıştır.

Hemen ifade edilmelidir ki; davacının rızası dışında bir kitapta geçen ismi kişisel veri niteliğindedir.

Ayrıca şunun da ifade edilmesi gereklidir ki; unutulma hakkı tanımlarına bakıldığında her ne kadar dijital veriler için düzenlenmiş ise de, bu hakkın özellikleri ve bu hakkın insan haklarıyla arasındaki ilişkisi dikkate alındığında; yalnızca dijital ortamdaki kişisel veriler için değil, kamunun kolayca ulaşabileceği yerde tutulan kişisel verilere yönelik olarak da kabul edilmesi gerektiği açıktır.

Davacı, geçmişte yaşadığı kötü bir olayın toplum hafızasından silinmesini istemektedir. Unutulma hakkı ile geçmişindeki yaşanan talihsiz bir olayın unutulmasıyla geleceğini serbestçe şekillendirmek, diğer bir deyişle hayatında, yeni bir sayfa açma olanağı istemektedir. Kaldı ki, davacı da yargılama sırasında verdiği dilekçelerinde bu istem üzerinde ısrarla durmuştur. Davacı unutulma hakkı ile özel hayatına ilişkin kişisel verilerinin üçüncü kişiler tarafından bilinmemesini, aradan geçen süre nedeniyle toplum hafızasından silinmesini istemektedir.

Bu bağlamda değerlendirildiğinde; 4 yıl önce gerçekleşen bir olayın mağduru olan kişinin adının açık bir şekilde yazılarak kitapta yer alması halinde unutulma hakkının bunun sonucunda da davacının özel hayatının gizliliğinin ihlal edildiği kabul edilmelidir. Avrupa Birliği Adalet Divanı'nın "Google Kararı"nda açıkladığı gibi ilgili verinin kamu hayatında oynadığı önemli rol ve halkın ilgili veriye yönelik yoğun ilgisi şeklinde, üstün bir kamu yararını ortaya koyan özel sebepler bulunmadığına göre bilimsel esere alınan kararda kişisel veriler açık bir şekilde yer almamalıdır.

Görüşmeler sırasında azınlıkta kalan üyeler mahkeme kararlarında yer alan isimlerin rumuzlanmasına gerek olmadığını, yargılamanın istisnalar haricinde açık bir şekilde yapıldığını hükmün alenen tefhim edildiğini, bu nedenle özel hayatın gizliliğinin ihlal edilmediğini savunmuşlar ise bu görüş “sorunun mahkeme kararlarında isimlerin rumuzlanmadan yer alması değil, kararların kitaba alınması sırasında rumuzlanması gerekip gerekmediği sorunu olduğu” gerekçesi ile kurul çoğunluğu tarafından kabul edilmemiştir.

O halde davacının isminin rumuzlanmadan kitapta yer almasının unutulma hakkını ve bunun neticesinde özel hayatın gizliliğini ihlal ettiği dikkate alındığında davacı lehine manevi tazminat koşullarının gerçekleştiğinin kabulü zorunludur.

Ne var ki, Özel Dairece tazminat miktarı yönünden inceleme yapılmadığından bu yöne ilişkin temyiz itirazlarının incelenmesi için dosyanın Özel Daireye gönderilmesi gerekir.

Yukarıda yazılı gerekçelerle yerel mahkemenin direnme kararı yerinde bulunduğundan tazminat miktarı yönünden mahkemenin kurduğu hükme yönelik temyiz itirazlarının incelenmesi için dosyanın 4. Hukuk Dairesine gönderilmesine, 17.06.2015 gününde oyçokluğu ile karar verildi.

Yargıtay Kararı - 19. Ceza Dairesi (E. 2017/3325)

Yargıtay 19. CD., E. 2017/3325 K. 2018/11147 T. 31.10.2018

Esas No.: 2017/3325

Karar No.: 2018/11147

Karar Tarihi: 31.10.2018

MAHKEMESİ: Ağır Ceza Mahkemesi

SUÇ: 5411 Sayılı Kanuna Aykırılık

HÜKÜM: Beraat

Yerel Mahkemece verilen hüküm temyiz edilmekle; başvurunun süresi, kararın niteliği ve suç tarihine göre dosya incelendi, gereği görüşülüp düşünüldü:

Temyiz isteğinin reddi nedenleri bulunmadığından işin esasına geçildi.

Vicdani kanının oluştuğu duruşma sürecini yansıtan tutanaklar, belgeler ve gerekçe içeriğine göre yapılan incelemede;

Eyleme ve yükletilen suça yönelik katılan vekilinin temyiz nedenleri yerinde görülmediğinden tebliğnameye uygun olarak, TEMYİZ DAVASININ ESASTAN REDDİYLE HÜKMÜN ONANMASINA, 31/10/2018 tarihinde oy birliğiyle ve Üye ...'ün değişik gerekçesi ile karar verildi.

DEĞİŞİK GEREKÇE

Sayın Çoğunluk ile aramızdaki uyuşmazlık sanığın katılan banka tarafından görevi sebebiyle öğrendiği banka sırrı niteliğindeki bilgileri şahsi e posta adresine göndermesinin TCK'nin 135/1. maddesindeki kişisel verileri hukuka aykırı olarak kaydetme suçunu oluşturup oluşturmayacağı ve bu bağlamda söz edilen fiilin iddianame ile kamu davasına konu edilip edilmediğinin belirlenmesine ilişkindir.

1. Sanığın fiilinin kişisel verilerin korunması suçunu oluşturup oluşturmayacağı irdelenmesi

Somut uyuşmazlığın maddi konusunu oluşturan kişisel verilerin korunmasının ne denli önem taşıdığı vurgulanmasında ihtilafın çözümlenmesi bakımından yarar bulunmaktadır. Bu bağlamda öncelikle 1 Ekim 1985 tarihinde yürürlüğe giren "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" dikkat çekmektedir. Türkiye Cumhuriyeti Devleti, 28 Ocak 1981 tarihinde bu Sözleşmeyi imzalayan ilk ülkelerden birisi olmuş; bu Sözleşme, 17 Mart 2016

tarikh ve 29656 sayılı Resmi Gazete’de yayımlanarak iç hukuka dahil edilmiştir.. Anılan Sözleşmenin temel amacının; “her Üye Ülkede, uyruğu veya ikametgahı ne olursa olsun gerçek kişilerin, temel hak ve özgürlüklerini ve özellikle kendilerini ilgilendiren kişisel nitelikteki verilerin otomatik yollarla işleme tabi tutulması karşısında özel yaşam haklarını güvence altına almak” olduğu yerinde olarak ifade edilmektedir. Ayrıca kişisel verilerin korunmasına ilişkin uluslararası düzeyde, OECD’nin “Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri” (23 Eylül 1980) ve Birleşmiş Milletler’in “Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri” (14 Aralık 1990) temel uluslararası düzenlemeler olarak bulunmaktadır (https://www.kvkk.gov.tr/Icerik/4183/Kisisel_Verilerin-Korunmasi-Alaninda-Uluslararası_ve-Ulusal-Duzenlemeler). Türkiye Cumhuriyeti Anayasası’nın “Özel Hayatın Gizliliği” başlıklı 20. maddesi hükmüne eklenen üçüncü fıkra ile kişisel verilerin anayasal koruma altına alınması ise, bu konuda temel normatif çerçeveyi oluşturmaktadır. Anayasamızın 20/3. maddesine göre “Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.” Bununla birlikte Türk Medeni Kanunu’nun kişilik haklarının korunmasını düzenleyen 23. ve 24. maddesi hükümleri uyarınca da kişisel veriler korunmaktadır. Konuya ceza hukuku koruması bağlamında bakıldığında ise, 5237 sayılı Türk Ceza Kanunu’nun “Kişisel Verilerin Kaydedilmesi” başlıklı 135. maddesinde “kişisel verilerin hukuka aykırı olarak kaydedilmesi” 136. maddesinde ise “kişisel verileri hukuka aykırı olarak yayma veya ele geçirme” fiilleri suç olarak tanımlanmıştır. Nihayet 6698 sayılı Kişisel Verilerin Korunması Kanunu da 7 Nisan 2016 tarih ve 29677 sayılı Resmi Gazete’de yayımlanarak yürürlüğe girmiştir.

Kişisel Verilerin Korunması Kanunu’nda “Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder” şeklinde tanımlanarak kanuni koruma altına alınmıştır (6698/md. 3/1-c). Kişinin kendi nefesine ait her çeşit bilginin “kişisel veri” oluşturacağı kuşkusuzdur (Hafizoğulları, Zeki/ Özen, Muharrem: Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar, Ankara 2010, s. 269). Türk Ceza Kanunu kişisel veri kavramını tanımlamamış ise de hem Uluslararası metinlerde ve ilgili Kanunda hem de doktrinde “gerçek kişiye ait her türlü bilginin kişisel veri olarak kabul edileceği” hususunda ittifak bulunmaktadır. Bu suçların hukuki konusu ise özel hayatın gizliliği ve bu hakkın yeni gelişen bir parçasını oluşturan ve Anayasa’da yer verilmiş olan kişisel verilerin korunmasıdır (Akdağ, Hale: Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması: Ankara 2013, s. 39). Anılan suç bir tehlike suçu olup; suçun tamamlanması için bir zararın ortaya

çıkması da aranmamaktadır. Kişisel verilerin korunması suçuyla kişilerin manevi rahatlığının da güvenceye alınması amaçlanmaktadır (Akdağ, s. 98). Kısacası, modern toplumda “özel hayat” kavramının kapsamı “kişisel verilerin korunması ihtiyacı” karşısında daha bir derinlik ve özel mânâ kazanmıştır. Gerçekten, gelişen teknoloji karşısında kişisel verilerin hızla depolanabileceği, iletilebileceği vb. faaliyetler düşünüldüğünde bu alandaki koruma ihtiyacının önemi ortadadır. Bu anlamda kişisel verilerin korunmasının modern ve global dünyadaki hayatıyeti gözetilerek bu alanın ceza hukuku normları ile korunmasına da ihtiyaç duyulmuştur. Kişisel verilerin korunmasına ilişkin ceza normlarıyla kişilerin manevi varlıklarını geliştirebilecekleri bir iklim yaratılmasını engelleyebilecek fiillerin ceza hukuku araçlarıyla dahi olsa muhakkak surette önlenmesi amaçlanmıştır. Bu suç tipi ile nihayetinde bireylerin özel hayatlarının gizliliğinin korunması; dolayısıyla demokratik toplumun güçlendirilmesine katkı sağlanması hedeflenmektedir.

Somut uyuşmazlıkta sanığın işlediği iddia olunan fiil “sanığın katılan banka tarafından görevi sebebiyle kendisine tevdi edilen bilgisayarında kayıtlı olup içeriğinde müşterilere ait mali analiz bilgileri ve kredi kartı analiz dokümanı gibi bilgileri kendisine ait elektronik posta adresine göndermekten” ibarettir. Sanık bu hadiseden çok kısa bir süre sonra ise bankadaki işinden istifa etmiştir. Gerçek kişilere ait mali analiz bilgileri ile kredi kartı analiz bilgilerinin kişiden sadır olduğu bu itibarla kişisel veri niteliği taşıdığı kuşkusuzdur. Bu itibarla sanığın bu verileri özel elektronik posta adresine göndermek şeklindeki hareketinin TCK'nin 135/1. maddesindeki kişisel verilerin hukuka aykırı şekilde kaydedilmesi (depolanması) fiilini oluşturabileceği kanaatindeyiz.

2- Söz edilen fiilin iddianame ile kamu davasına konu edilip edilmediğinin belirlenmesi

Bilindiği üzere ceza muhakemesinin temel ilkelerinden birisi “davasız yargılama olmaz” ilkesidir. Bu ilke Ceza Muhakemesi Kanunu'nun (CMK) 225/1. maddesinde “Hüküm, ancak iddianamede unsurları gösterilen suça ilişkin fiil ve faili hakkında verilir” şeklinde ifade edilmiştir. Bu bağlamda somut uyuşmazlığa dönüldüğünde sanık hakkında dava konusu edilen fiil “müşteki bankada görev yaptığı sırada sıfat ve görevi sebebiyle öğrendiği banka sırrı niteliğindeki bilgileri şahsi e-posta adresine gönderdiği; daha sonra müştekinin bankadan istifa ederek ayrıldığı...” şeklinde ifade edilmiştir. İddianamede yer verilen (kısaca) “banka sırrı niteliğindeki bilgileri e-posta adresine gönderme” fiilinin kişisel verileri kaydetme olarak değerlendirilmesi güç gözükmemektedir. Banka sırrı olarak nitelendirilen bilgilerden söz eden iddianamede hiçbir şekilde “kişisel veri, kişisel bilgi, müşteri bilgisi” vb. şekilde kişisel veriye işaret edebilecek bir anlatımdan söz edilmemiştir. Aslında söz edilmek istenen şeyin müşterilere ait bilgiler dolayısıyla kişisel veriler olduğu kuşkusuzdur. Ancak bilinmektedir ki Yargıtay'ın yerleşik içtihatlarına göre “iddianamede bir fiil anlatılır iken başka

bir şeyden söz edilmiş olması o fiilden dava açılmış sayılması için yeterli kabul edilemez” Kuşkusuz, iddianamede sanığa yüklenen fiil açık, şüpheye yer bırakmayacak ve doğrudan bir anlatımla ifade edilmelidir. Bu ilke, sanığın isnadı öğrenme hakkının zorunlu bir gereğidir. İsnadı bilemeyen sanığın elinden savunma hakkının da alınacağı şüphesizdir.

Açıklanan gerekçelerle sanık hakkında kişisel verileri hukuka aykırı olarak kaydetme suçundan iddianame ile usulüne uygun şekilde açılmış bir kamu davası bulunmamaktadır. Bu itibarla, her ne kadar sanığın fiili kişisel verileri hukuka aykırı olarak kaydetme suçunu oluşturmakta ise de bu suçtan sanık hakkında iddianame ile usulüne uygun şekilde açılmış bir kamu davası bulunmadığı kanaatimle hükmün onanması gerektiği yolundaki Sayın Çoğunluğun düşüncesine değişik gerekçeyle katılıyorum.

Yargıtay Kararı - 19. Ceza Dairesi (E. 2017/6127)

Yargıtay 19. CD., E. 2017/6127 K. 2018/11148 T. 31.10.2018

Esas No.: 2017/6127

Karar No.: 2018/11148

Karar Tarihi: 31.10.2018

MAHKEMESİ: Ağır Ceza Mahkemesi

SUÇ: 5411 Sayılı Kanuna Aykırılık

HÜKÜM: Beraat

Yerel Mahkemece verilen hüküm temyiz edilmekle; başvurunun süresi, kararın niteliği ve suç tarihine göre dosya incelendi, gereği görüşülüp düşünüldü:

Temyiz isteğinin reddi nedenleri bulunmadığından işin esasına geçildi.

Gerekçeli karar başlığında katılanın müşteki olarak gösterilmesi mahallinde giderilebilir nitelikte bir hata olarak kabul edilmiştir.

Vicdani kanının oluştuğu duruşma sürecini yansıtan tutanaklar, belgeler ve gerekçe içeriğine göre yapılan incelemede;

Eyleme ve yükletilen suça yönelik katılan vekilinin temyiz nedenleri yerinde görülmediğinden tebliğnameye uygun olarak, TEMYİZ DAVASININ ESASTAN REDDİYLE HÜKMÜN ONANMASINA, 31/10/2018 tarihinde oy çokluğuyla karar verildi.

KARŞI OY

Sayın Çoğunluk ile aramızdaki uyuşmazlık sanığın katılan banka tarafından görevi sebebiyle kendisine tevdi edilen bilgisayarında kayıtlı olup içeriğinde müşterilere ait mali analiz bilgileri ve kredi değerlendirme formları gibi bilgileri kendi bilgisayarına kaydetmesinin TCK'nın 135. maddesindeki kişisel verileri hukuka aykırı olarak kaydetme suçunu oluşturup oluşturmayacağıının belirlenmesine ilişkindir.

Somut uyuşmazlığın maddi konusunu oluşturan kişisel verilerin korunmasının ne denli, önem taşıdığıının vurgulanmasında ihtilafın çözümlenmesi bakımından yarar, bulunmaktadır. Bu bağlamda öncelikle 1 Ekim 1985 tarihinde yürürlüğe giren "Kişisel, Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi", dikkat çekmektedir. Türkiye Cumhuriyeti

Devleti, 28 Ocak 1981 tarihinde bu Sözleşmeyi, imzalayan ilk ülkelerden birisi olmuş; bu Sözleşme, 17 Mart 2016 tarih ve 29656 sayılı, Resmi Gazete’de yayımlanarak iç hukuka dahil edilmiştir. Anılan Sözleşmenin temel, amacının; “her Üye Ülkede, uyruğu veya ikametgâhı ne olursa olsun gerçek kişilerin, temel, hak ve özgürlüklerini ve özellikle kendilerini ilgilendiren kişisel nitelikteki verilerin otomatik, yollarla işleme tabi tutulması karşısında özel yaşam haklarını güvence altına almak”, olduğu yerinde olarak ifade edilmektedir. Ayrıca kişisel verilerin korunmasına ilişkin uluslararası düzeyde, OECD’nin “Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri” (23 Eylül 1980) ve Birleşmiş Milletler’in “Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri” (14 Aralık 1990) temel uluslararası düzenlemeler olarak bulunmaktadır ([https://www.kvkk.gov.tr /Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararası-ve-Ulusal-Düzenlemeler](https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararası-ve-Ulusal-Düzenlemeler)). Türkiye Cumhuriyeti Anayasası’nın “Özel Hayatın Gizliliği” başlıklı 20. maddesi hükmüne eklenen üçüncü fıkra ile kişisel verilerin anayasal koruma altına alınması ise, bu konuda temel normatif çerçeveyi oluşturmaktadır. Anayasamızın 20/3. maddesine göre “Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.” Bununla birlikte Türk Medeni Kanunu’nun kişilik haklarının korunmasını düzenleyen 23. ve 24. maddesi hükümleri uyarınca da kişisel veriler korunmaktadır. Konuya ceza hukuku koruması bağlamında bakıldığında ise, 5237 sayılı Türk Ceza Kanunu’nun “Kişisel Verilerin Kaydedilmesi” başlıklı 135. maddesinde “kişisel verilerin hukuka aykırı olarak kaydedilmesi” 136. maddesinde ise “kişisel verileri hukuka aykırı olarak yayma veya ele geçirme” fiilleri suç olarak tanımlanmıştır. Nihayet 6698 sayılı Kişisel Verilerin Korunması Kanunu da 7 Nisan 2016 tarih ve 29677 sayılı Resmi Gazete’de yayımlanarak yürürlüğe girmiştir.

Kişisel Verilerin Korunması Kanunu’nda “Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder” şeklinde tanımlanarak kanuni koruma altına alınmıştır (6698/md. 3/1-c). Kişinin kendi nefesine ait her çeşit bilginin “kişisel veri” oluşturacağı kuşkusuzdur (Hafızoğulları, Zeki/ Özen, Muharrem: Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar, Ankara 2010, s. 269). Türk Ceza Kanunu kişisel veri kavramını tanımlamamış ise de hem Uluslararası metinlerde ve ilgili Kanunda hem de doktrinde “gerçek kişiye ait her türlü bilginin kişisel veri olarak kabul edileceği” hususunda ittifak bulunmaktadır. Bu suçların hukuki konusu ise özel hayatın gizliliği ve bu hakkın yeni gelişen bir parçasını oluşturan ve Anayasa’da yer verilmiş olan kişisel verilerin korunmasıdır (Akdağ, Hale: Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması:

Ankara 2013, s. 39). Anılan suç bir tehlike suçu olup; suçun tamamlanması için bir zararın ortaya çıkması da aranmamaktadır. Kişisel verilerin korunması suçuyla kişilerin manevi rahatlığının da güvenceye alınması amaçlanmaktadır (Akdağ, s. 98). Kısacası, modern toplumda “özel hayat” kavramının kapsamı “kişisel verilerin korunması ihtiyacı” karşısında daha bir derinlik ve özel mânâ kazanmıştır. Gerçekten, gelişen teknoloji karşısında kişisel verilerin hızla depolanabileceği, iletilebileceği vb. faaliyetler düşünüldüğünde bu alandaki koruma ihtiyacının önemi ortadadır. Bu anlamda kişisel verilerin korunmasının modern ve global dünyadaki hayatiyeti gözetilerek bu alanın ceza hukuku normları ile korunmasına da ihtiyaç duyulmuştur. Kişisel verilerin korunmasına ilişkin ceza normlarıyla kişilerin manevi varlıklarını geliştirebilecekleri bir iklim yaratılmasını engelleyebilecek fiillerin ceza hukuku araçlarıyla dahi olsa muhakkak surette önlenmesi amaçlanmıştır. Bu suç tipi ile nihayetinde bireylerin özel hayatlarının gizliliğinin korunması; dolayısıyla demokratik toplumun güçlendirilmesine katkı sağlanması hedeflenmektedir.

Somut uyuşmazlıkta dava konusu edilen fiil “sanığın katılan banka tarafından görevi sebebiyle kendisine tevdi edilen bilgisayarında kayıtlı olup içeriğinde müşterilere ait mali analiz bilgileri ve kredi değerlendirme formları gibi bilgileri kendisi veya yeni işyerine ait elektronik posta adresinden kendi adresine göndermekten” ibarettir. Sanık bu hadiseden çok kısa bir süre sonra ise bankadaki işinden istifa etmiştir. Gerçek kişilere ait mali analiz bilgileri ile kredi değerlendirme bilgilerinin kişiden sadır olduğu bu itibarla kişisel veri niteliği taşıdığı ve kuşkusuzdur. Bu itibarla sanığın bu verileri özel elektronik posta adresine göndermek şeklindeki hareketinin TCK’nin 135/1. maddesindeki kişisel verilerin hukuka aykırı şekilde kaydedilmesi (depolanması) fiilini oluşturacağı kanaatindeyiz.

Sanık hakkında 5411 sayılı Kanununun 159/1. maddesinin 1. cümlesi gereğince cezalandırılması istemiyle kamu davası açılmış ise de iddianame anlatımında “müşteri bilgilerinin gönderilmesi” “mali analiz bilgileri ve kredi değerlendirme formları gibi sırların gönderilmesi” hareketlerinden söz edilmektedir. İddianamede doğrudan “kişisel veri” kavramına yer verilmemiştir. Ancak hukuki nitelendirme farklılığı sebebiyle iddianamede “sır” ve “bilgi” olarak tanımlanan verilerin “kişisel veri” olarak nitelendirilmemiş olduğundan dolayısıyla kişisel verilerin hukuka aykırı olarak kaydedilmesi suçundan açılmış bir dava bulunmadığından söz edilemeyecektir. Sonuç olarak anılan gerekçelerle sanığın dava konusu edilen fiilinin TCK’nin 135/1. maddesindeki suçu oluşturacağı düşüncesiyle Sayın Çoğunluğun beraat hükmünün onanması yönündeki görüşüne katılmıyorum.

Yargıtay Kararı - 19. Ceza Dairesi (E. 2017/6532)

Yargıtay 19. CD., E. 2017/6532 K. 2018/11149 T. 31.10.2018

Esas No.: 2017/6532

Karar No.: 2018/11149

Karar Tarihi: 31.10.2018

MAHKEMESİ: Ağır Ceza Mahkemesi

SUÇ: 5411 Sayılı Kanuna Aykırılık

HÜKÜM: Beraat

Yerel Mahkemece verilen hüküm temyiz edilmekle; başvurunun süresi, kararın niteliği ve suç tarihine göre dosya incelendi, gereği görüşülüp düşünüldü:

Temyiz isteğinin reddi nedenleri bulunmadığından işin esasına geçildi.

Vicdani kanının oluştuğu duruşma sürecini yansıtan tutanaklar, belgeler ve gerekçe içeriğine göre yapılan incelemede;

Eyleme ve yükletilen suça yönelik katılan vekilinin temyiz nedenleri yerinde görülmediğinden tebliğnameye uygun olarak, TEMYİZ DAVASININ ESASTAN REDDİYLE HÜKMÜN ONANMASINA, 31/10/2018 tarihinde oyçokluğuyla karar verildi.

KARŞI OY

Sayın Çoğunluk ile aramızdaki uyuşmazlık sanığın katılan banka tarafından görevi sebebiyle kendisine tevdi edilen bilgisayarında kayıtlı olup içeriğinde müşterilere ait ticari sır ve müşteri sırrı niteliğinde olan bilgileri kendi kişisel e posta adresine göndermesinin TCK'nın 135. maddesindeki kişisel verileri hukuka aykırı olarak kaydetme suçunu oluşturup oluşturmayacağına belirlenmesine ilişkindir.

Somut uyuşmazlığın maddi konusunu oluşturan kişisel verilerin korunmasının ne denli, önem taşıdığına vurgulanmasında ihtilafın çözümlenmesi bakımından yarar, bulunmaktadır. Bu bağlamda öncelikle 1 Ekim 1985 tarihinde yürürlüğe giren "Kişisel, Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi", dikkat çekmektedir. Türkiye Cumhuriyeti Devleti, 28 Ocak 1981 tarihinde bu Sözleşmeyi, imzalayan ilk ülkelerden birisi olmuş; bu Sözleşme, 17 Mart 2016 tarih ve 29656 sayılı, Resmi Gazete'de yayımlanarak iç hukuka dahil edilmiştir. Anılan

Sözleşmenin temel, amacının; “her Üye Ülkede, uyruğu veya ikametgâhı ne olursa olsun gerçek kişilerin, temel, hak ve özgürlüklerini ve özellikle kendilerini ilgilendiren kişisel nitelikteki verilerin otomatik, yollarla işleme tabi tutulması karşısında özel yaşam haklarını güvence altına almak”, olduğu yerinde olarak ifade edilmektedir. Ayrıca kişisel verilerin korunmasına ilişkin, uluslararası düzeyde, OECD’nin “Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi, Akışına İlişkin Rehber İlkeleri” (23 Eylül 1980) ve Birleşmiş Milletler’in “Bilgisayarla İşlenen, Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri” (14 Aralık 1990) temel uluslararası düzenlemeler olarak bulunmaktadır (<https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararası-ve-Ulusal-Duzenlemeler>). Türkiye Cumhuriyeti Anayasası’nın “Özel Hayatın Gizliliği” başlıklı 20. maddesi hükmüne eklenen üçüncü fıkra ile kişisel verilerin anayasal koruma altına alınması ise, bu konuda temel normatif çerçeveyi oluşturmaktadır. Anayasamızın 20/3. maddesine göre “Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.” Bununla birlikte Türk Medeni Kanunu’nun kişilik haklarının korunmasını düzenleyen 23. ve 24. maddesi hükümleri uyarınca da kişisel veriler korunmaktadır. Konuya ceza hukuku koruması bağlamında bakıldığında ise, 5237 sayılı Türk Ceza Kanunu’nun “Kişisel Verilerin Kaydedilmesi” başlıklı 135. maddesinde “kişisel verilerin hukuka aykırı olarak kaydedilmesi” 136. maddesinde ise “kişisel verileri hukuka aykırı olarak yayma veya ele geçirme” fiilleri suç olarak tanımlanmıştır. Nihayet 6698 sayılı Kişisel Verilerin Korunması Kanunu da 7 Nisan 2016 tarih ve 29677 sayılı Resmi Gazete’de yayımlanarak yürürlüğe girmiştir.

Kişisel Verilerin Korunması Kanunu’nda “Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder” şeklinde tanımlanarak kanuni koruma altına alınmıştır (6698/md. 3/1-c). Kişinin kendi nefesine ait her çeşit bilginin “kişisel veri” oluşturacağı kuşkusuzdur (Hafizoğulları, Zeki/ Özen, Muharrem: Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar, Ankara 2010, s. 269). Türk Ceza Kanunu kişisel veri kavramını tanımlamamış ise de hem Uluslararası metinlerde ve ilgili Kanunda hem de doktrinde “gerçek kişiye ait her türlü bilginin kişisel veri olarak kabul edileceği” hususunda ittifak bulunmaktadır. Bu suçların hukuki konusu ise özel hayatın gizliliği ve bu hakkın yeni gelişen bir parçasını oluşturan ve Anayasa’da yer verilmiş olan kişisel verilerin korunmasıdır (Akdağ, Hale: Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması: Ankara 2013, s. 39). Anılan suç bir tehlike suçu olup; suçun tamamlanması için bir zararın ortaya çıkması da aranmamaktadır. Kişisel verilerin korunması suçuyla kişilerin manevi rahatlığının da

güvenceye alınması amaçlanmaktadır (Akdağ, s. 98). Kısacası, modern toplumda “özel hayat” kavramının kapsamı “kişisel verilerin korunması ihtiyacı” karşısında daha bir derinlik ve özel mânâ kazanmıştır. Gerçekten, gelişen teknoloji karşısında kişisel verilerin hızla depolanabileceği, iletilebileceği vb. faaliyetler düşünüldüğünde bu alandaki koruma ihtiyacının önemi ortadadır. Bu anlamda kişisel verilerin korunmasının modern ve global dünyadaki hayatiyeti gözetilerek bu alanın ceza hukuku normları ile korunmasına da ihtiyaç duyulmuştur. Kişisel verilerin korunmasına ilişkin ceza normlarıyla kişilerin manevi varlıklarını geliştirebilecekleri bir iklim yaratılmasını engelleyebilecek fiillerin ceza hukuku araçlarıyla dahi olsa muhakkak surette önlenmesi amaçlanmıştır. Bu suç tipi ile nihayetinde bireylerin özel hayatlarının gizliliğinin korunması; dolayısıyla demokratik toplumun güçlendirilmesine katkı sağlanması hedeflenmektedir.

Somut uyuşmazlıkta dava konusu edilen fiil “sanığın katılan banka tarafından görevi sebebiyle kendisine tevdi edilen bilgisayarında kayıtlı olup içeriğinde müşterilere ait ticari sır ve müşteri sırrı niteliğinde olan bilgileri kendi kişisel e posta adresine göndermekten” ibarettir. Gerçek kişilere ait ticari sır ve müşteri sırrı niteliğinde olan mali bilgilerin kişiden sadır olduğu bu itibarla kişisel veri niteliği taşıdığı ve kuşkusuzdur. Bu itibarla sanığın bu verileri özel-kişisel elektronik posta adresine göndermek şeklindeki hareketinin TCK’nin 135/1. maddesindeki kişisel verilerin hukuka aykırı şekilde kaydedilmesi (depolanması) fiilini oluşturacağı kanaatindeyiz.

Sanık hakkında 5411 sayılı Kanununun 159/1. maddesinin 1. cümlesi gereğince cezalandırılması istemiyle kamu davası açılmış ise de iddianame anlatımında “...müşterilere ait ticari sır ve müşteri sırrı niteliğinde olan bilgileri kendi kişisel e posta adresine gönderme” hareketinden söz edilmektedir. İddianamede doğrudan “kişisel veri” kavramına yer verilmemiştir. Ancak hukuki nitelendirme farklılığı sebebiyle iddianamede “müşteri bilgisi” olarak tanımlanan verilerin “kişisel veri” olarak nitelendirilmemiş olduğundan dolayısıyla kişisel verilerin hukuka aykırı olarak kaydedilmesi suçundan açılmış bir dava bulunmadığından söz edilemeyecektir. Sonuç olarak anılan gerekçelerle sanığın dava konusu edilen fiilinin TCK’nın 135/1. maddesindeki suçu oluşturacağı düşüncesiyle Sayın Çoğunluğun beraat hükmünün onanması yönündeki görüşüne katılamıyorum.

Yargıtay Kararı - 19. Ceza Dairesi (E. 2018/3318)

Yargıtay 19. CD., E. 2018/3318 K. 2018/9281 T. 24.9.2018

Esas No.: 2018/3318

Karar No.: 2018/9281

Karar Tarihi: 24.09.2018

Http://www.....gazetesi.com isimli internet sitesinde "Kooperatifte Skandal İddialar" başlıklı yayımlanan içerik nedeniyle ilgilisi ...'in kişilik haklarına ağır saldırı yapıldığından bahisle 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun uyarınca vaki erişimin engellenmesi isteminin reddine dair Eskişehir 2. Sulh Ceza Hâkimliğinin 30/01/2018 tarihli ve 2018/690 değişik iş sayılı kararına karşı yapılan itirazın reddine ilişkin Eskişehir 1. Sulh Ceza Hâkimliğinin 09/02/2018 tarihli ve 2018/822 değişik iş sayılı kararı aleyhine, Adalet Bakanlığı'nın 09/05/2018 gün ve 5349 sayılı kanun yararına bozma istemini içeren yazısı ekindeki dava dosyası, Yargıtay Cumhuriyet Başsavcılığının 16/05/2018 gün ve KYB. 2018 / 41336 sayılı ihbarnamesi ile dairemize gönderilmekle okundu.

Anılan ihbarnamede;

Dosya kapsamına göre, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu'nun 9/1. maddesinde "İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğe erişimin engellenmesini de isteyebilir." ve anılan maddenin 3. fıkrasında "İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talepleri doğrultusunda hâkim bu maddede belirtilen kapsamda erişimin engellenmesine karar verebilir." şeklindeki düzenlemeler karşısında, söz konusu internet sitesinde yapılan haber içeriğinde paylaşılan talep edene ait telefon numarası, iş yeri ve ev adresleri ile imzasının kişisel veri niteliğinde olup, bu verilerin talep edenin rızası olmadan yayımlanmasının ilgisinin kişilik haklarını zedeler mahiyette olduğunun anlaşılması karşısında itirazın kabulü yerine yazılı şekilde reddine karar verilmesinde isabet görülmediği, gerekçesiyle 5271 sayılı Ceza Muhakemesi Kanununun 309. maddesi uyarınca anılan kararın kanun yararına bozulması isteminde bulunulmakla,

Gereği görüştülüp düşünöldü:

5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"un "içeriğın yayından çıkarılması ve erişimin engellenmesi" başlıklı 9. maddesi;

"(1) İnternet ortamında yapılan yayın içeriğı nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğın yayından çıkarılmasını isteyebileceğı gibi doğrudan sulh ceza hâkimine başvurarak içeriğı erişimin engellenmesini de isteyebilir.

(2) İnternet ortamında yapılan yayın içeriğı nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişilerin talepleri, içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılır.

(3) İnternet ortamında yapılan yayın içeriğı nedeniyle kişilik hakları ihlal edilenlerin talepleri doğrultusunda hâkim bu maddede belirtilen kapsamda erişimin engellenmesine karar verebilir.

(4) Hâkim, bu madde kapsamında vereceğı erişimin engellenmesi kararlarını esas olarak, yalnızca kişilik hakkının ihlalinin gerçekleştiğı yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğı erişimin engellenmesi yöntemiyle verir. Zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemez. Ancak, hâkim URL adresi belirtilerek içeriğı erişimin engellenmesi yöntemiyle ihlalin engellenemeyeceğine kanaat getirmesi hâlinde, gerekçesini de belirtmek kaydıyla, internet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilir.

(5) Hâkimin bu madde kapsamında verdiğı erişimin engellenmesi kararları doğrudan Birliğe gönderilir.

(6) Hâkim bu madde kapsamında yapılan başvuruyu en geç yirmi dört saat içinde duruşma yapmaksızın karara bağlar. Bu karara karşı 04/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir.

(7) Erişimin engellenmesine konu içeriğın yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

(8) Birlik tarafından erişim sağlayıcıya gönderilen içeriğı erişimin engellenmesi kararının gereğı derhâl, en geç dört saat içinde erişim sağlayıcı tarafından yerine getirilir.

(9) Bu madde kapsamında hâkimin verdiği erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının başka internet adreslerinde de yayınlanması durumunda ilgili kişi tarafından Birliğe müracaat edilmesi hâlinde mevcut karar bu adresler için de uygulanır.

(10) Sulh ceza hâkiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişi, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır." hükümlerini amirdir.

Buna göre erişimin engellenmesi tedbirinin uygulanma şartları;

- İnternet ortamında yapılan bir yayın olması,

- Yapılan yayının içeriğinin, gerçek ve tüzel kişiler ile kurum ve kuruluşların "kişilik haklarını" ihlal eder mahiyette olmasıdır.

Başvuruya konu somut uyuşmazlıkta; başvuran kişinin, Eskişehir'de faaliyet gösteren bir esnaf odası başkanının oğlu olduğu, yerel bir gazete yazarının, internet sitesi üzerinden köşe yazısı mahiyetinde yaptığı bir haberle, başvuranın babasının başkanı olduğu oda hakkında yolsuzluk ve iltimas iddialarını dile getirdiği sırada, oda başkanının ve ailesinin çok sayıda ve miktarda kredileri kullandıkları ancak geri ödemediklerini iddia ettiği, haberin sonunda başvuran kişi tarafından kullanılan kredinin başvuru belgesinin bir fotokopisinde oda başkanının oğlu olan başvurucunun adı, soyadı, kimlik, adres ve telefon bilgilerinin bulunduğu görülmektedir.

5651 sayılı Kanun'un 9. maddesinde aranan şartlara bakılacak olursa, yapılan haberin "internet ortamında yapılan bir yayın" olduğu hususu tartışmasızdır.

Ancak, yapılan yayının içeriğinin, habere konu edilen gerçek kişinin kişilik haklarını ihlal eder mahiyette olup olmadığının tespiti için, öncelikle kişilik hakkı, kişisel veri, ifade ve basın özgürlüğü kavramlarının, ulusal ve uluslararası mevzuat ile yargı kararları kapsamında kısaca açıklanmasında fayda bulunmaktadır.

I- KİŞİLİK HAKLARI VE KİŞİSEL VERİ KAVRAMLARI

A-) KİŞİLİK HAKLARI; Özel hukukta kişinin doğumuyla birlikte kazandığı ve üzerine kişisel gelişimiyle birlikte her geçen gün yeni değerler kattığı kişiliğinin, maddi ve manevi bütünlüğünün, isminin, mesleki kariyerinin, ailesinin ve hatta sosyal çevresinin kişi

üzerinde oluşturduğu, kısacası kendini gerçekleştirme yolunda elde ettiği tüm kazanımlarının ve menfaatlerinin, hukuk düzeni tarafından koruma altına alınan yönüdür. Medeni hukuk kapsamında kişilik hakları, kategorik anlamda mutlak haklar içinde yer alan, her zaman varolan, zamanla

tükenmeyen, herkese karşı ileri sürülebilen, çoğu zaman kişiye sıkı sıkıya bağlı ve devredilemeyen haklardandır.

4721 sayılı Türk Medeni Kanun'un "Hak ehliyeti" başlıklı 8. maddesi;

"Her insanın hak ehliyeti vardır. Buna göre bütün insanlar, hukuk düzeninin sınırları içinde, haklara ve borçlara ehil olmada eşittirler." genel kuralıyla tüm bireylerin Adalet önünde eşit hak ehliyetlerine sahip olduğunu anlatmaktadır.

Adı geçen Kanun'un "Kişiliğin korunması" üst başlığında yer alan 24. maddesi;

"Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir. Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da Kanun'un verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır." maddesiyle, herhangi bir hukuka uygunluk sebebi olmaksızın kişilik hakkına karşı yapılan her saldırının hukuka aykırı olduğunu ve bu saldırıya uğrayan kimsenin hakimden bu özel kanun maddesine göre de korunma isteyebileceğini düzenlemektedir.

Kişilik haklarına dair yukarıdaki düzenlemeler, kişinin bu temel hakkını sınırlayabilen durumları, "kişinin rızası, daha üstün nitelikte özel veya kamusal yarar veya kanunun verdiği yetkisinin kullanılması" olarak sınırlandırmış, bu durumlar haricinde kişinin sahip olduğu kişilik haklarına karşı her tür saldırının mutlak suretle "hukuka aykırı" olduğunu belirtmiştir.

B-) KİŞİSEL VERİ; 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3. maddesinde "...Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi..." şeklinde tanımlanmıştır.

6698 sayılı Kanun'un ilgili madde gerekçesinde; "...Kişisel veriler, sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin aklı, psikolojik, fizikî, kültürel, ekonomik, sosyal ve sair özelliklerine ilişkin verilerdir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilecek özellikleri nedeniyle kişisel verilerdir" açıklamasına yer verilmiştir.

Avrupa İnsan Hakları Sözleşmesi'nin "Özel ve aile hayatına saygı hakkı" başlıklı 8. maddesinde;

"1-Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

2-Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin kanunla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir" hükmü bulunmaktadır.

28.01.1981 tarihli ve 108 nolu Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Uluslararası Sözleşme'nin 2/a maddesinde;

"Kişisel nitelikteki veriler; kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm bilgileri ifade eder" denilmiş, 1995 tarihinde yürürlüğe giren Avrupa Topluluğu Veri Koruma Yönergesinin 2. maddesinde de kişisel veri; "doğrudan doğruya ya da dolaylı olarak bir gerçek kişi ile ilintili olabilecek ve onu belirlenebilir kılacak her türlü bilgi" olarak belirtilmiştir.

T.C. Anayasası'nın "Özel hayatın gizliliği" başlıklı 20. maddesi;

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz...

...(Ek fıkra: 7/5/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükümlerini amirdir.

Öğretide de kişisel verilere ilişkin; "Bireyin şahsi, mesleki ve ailevi özelliklerini gösteren, o bireyi diğer bireylerden ayırmaya ve niteliklerini ortaya koymaya elverişli hertürlü bilgiyi ifade eder" (Ersan Şen, Türk Ceza Kanunu Yorumu, Vedat Kitapçılık, İstanbul, 2006, s.601), "Bir kişinin adı ve soyadı, yaşı, cinsiyeti, doğum yeri, dini, TC kimlik numarası, cinsel hayatı, cep telefonu numarası, medeni durumu, ailesi, işi, geliri, borçları, adresi, geçirdiği hastalıklar, özel zevkleri ve buna benzer bilgileri" (Volkan Sırabaşı, İnternet ve Radyo- Televizyon Aracılığıyla Kişilik Haklarına Tecavüz, Adalet Yayınevi, Ankara, 2007, 2. Baskı, s.195) şeklinde tanımlar yapılmıştır.

Yargıtay Ceza Genel Kurulu'nun 17.06.2014 tarihli, 2012/12-1510 E. 2014/331 K. Sayılı kararında;

"...Kişilerin, sadece insan olması ve toplumdaki yeri, bazı değerleri kişisel veri haline getirmektedir, örneğin; kişinin adı, adresi, kimlik bilgileri, medeni durumu vb... Bunun yanında teknolojik gelişmeler nedeniyle gittikçe karmaşıklaşan toplum hayatındaki bir takım bilgiler de kişisel veri haline gelmiştir, örneğin; vatandaşlık numarası, banka hesap numarası, telefon numarası, elektronik posta adresi ve şifresi vb... dolayısıyla farklı gruplandırmalar bulunmakla birlikte kişisel verilerin iki başlık altında toplanması mümkündür. Birinci grupta; insanın varoluşundan kaynaklanan kişiliğine ait bilgiler, ikinci grupta ise; teknolojinin gelişmesiyle insanın modern toplumda yer alması nedeniyle kendisine verilen ya da çeşitli hizmetlere ulaşmasında kullanılan bilgiler yer almaktadır. Ancak her iki grupta yer alan bilgilerin de kişisel veri olarak hukuk düzenindeki değeri ve korunmaları açısından bir fark bulunmamaktadır. (Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayınevi, Ankara, 2014, 4. baskı, s.577)

TCK'nın 136. maddesinde tıpkı 135. maddesinde olduğu gibi korunan hukuki değer genel olarak kişilerin özel hayatı ve hayatın gizli alanı, özeldir ise kişisel verilerdir. Bu düzenlemeler ile tüm kişisel veriler koruma altına alındığından kişisel verilerin mutlaka gizli olması zorunlu değildir. Gizli olmayan ve herkes tarafından bilinen kişisel veriler de hukuka aykırı eylemlere karşı korunmalıdır. Zira kişisel verilerin korunmasına ilişkin suçlarda korunan hukuki değer "sır" olmayıp, verinin ilgilisi olan kişinin kişilik haklarıdır.(Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayınevi, Ankara, 2014, 4. baskı, s.579, 588-593)...

...Bu açıklamalar ışığında uyumsuzluk konusu değerlendirildiğinde; TCK'nın 135 ve 136. maddelerindeki kişisel verilerin korunmasına ilişkin düzenlemelerde sadece sır niteliğinde kişisel verilerin korunacağına ilişkin bir hükmün bulunmaması ve aksine 135. maddenin gerekçesinde gerçek kişiyle ilgili her türlü bilginin kişisel veri olarak kabul edilmesi gerektiğinin belirtilmesi karşısında, her türlü kişisel verinin hukuka aykırı olarak başkasına verilmesi, yayılması ve ele geçirilmesi fiillerinin kanunun 136. maddesindeki suçu oluşturduğu kabul edilmelidir.

Bu kapsamda somut olayda, sanığın genel yayın yönetmenliğini yaptığı gazetede köşe yazarı olarak çalışan katılanın yazdığı köşesinde kullanılan fotoğrafın, hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle sanık tarafından internetteki özel bir arkadaşlık sitesine kimlik, adres ve telefon bilgileri verilmeksizin ve erkek arkadaşı aradığı açıklamasıyla konulması eylemi, TCK'nın 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak yayma suçunu oluşturmaktadır...."

Şeklindeki gerekçeyle, sanığın, mağdurun zaten onu tanıyan herkesçe bilinen ve kolaylıkla ulaşılabilen fotoğrafını, altında mağdurun erkek aradığını belirterek rızası dışında bir arkadaşlık

sitesinde yayınlaması eyleminin, hukuka aykırı bir eylem olduğu ayrıca TCK'nın 136. maddesinde belirtilen suçu oluşturduğuna tereddüt bulunmadığı tespiti yapılmıştır.

Keza Yargıtay Hukuk Genel Kurulu'nun 17.06.2015 tarihli, 2014/4-56 E. ve 2015/1679 K. sayılı kararında da;

"...Avrupa İnsan Hakları Sözleşmesi (AİHS)'nin 8. maddesinde yer alan özel yaşama saygı hakkı altında korunan "mahremiyet hakkı"nın, bireyin kendisi hakkındaki bilgileri kontrol edebilmesi şeklindeki hukuki çıkarlarını da içerdiği ifade edilmektedir. Zira bireyin kendisine ait herhangi bir bilginin, kendi rızası olmaksızın açıklanmaması, yayılmaması ve bu bilgilere başkalarının ulaşamaması kısacası kişisel verilerinin mahrem kalması konusunda hukuki menfaati bulunmaktadır. (Gülay Arslan Öncü, Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması, Beta Yayınları, İstanbul 2011, s.182)...

Kişiyi unutulma hakkının sağlanması ile birlikte özel hayatının gizliliği korunmuş olacaktır.

Somut olaya bu kapsamda bakıldığında; davacı, kamu görevinin veya hizmet ilişkisinin sağladığı nüfuzu kötüye kullanarak, müteselsilen cinsel saldırı suçunun mağdurudur. 2006 yılında gerçekleşen eylem tarihinde davacı bekâr olup maruz kaldığı eylem geleceği açısından etkilidir. Yapılan yargılama sonunda kamu görevlisi olan sanık ceza almıştır. Temyiz istemi üzerine yapılan inceleme sonunda ise hüküm 2009 yılında onanmıştır. Mağdur davacı gerek hazırlık gerekse de yargılama sırasında cinsel saldırının nasıl gerçekleştiğini açık bir şekilde anlatmış, bu anlatımlar doğal olarak karar metnine geçirilmiştir. Karar mağdur ve sanığın ismi rumuzlanmadan 2010 yılı nisan ayında yayınlanan kitapta yer almıştır.

Hemen ifade edilmelidir ki; davacının rızası dışında bir kitapta geçen ismi kişisel veri niteliğindedir.

Ayrıca şunun da ifade edilmesi gereklidir ki; unutulma hakkı tanımlarına bakıldığında her ne kadar dijital veriler için düzenlenmiş ise de, bu hakkın özellikleri ve bu hakkın insan haklarıyla arasındaki ilişkisi dikkate alındığında; yalnızca dijital ortamdaki kişisel veriler için değil, kamunun kolayca ulaşabileceği yerde tutulan kişisel verilere yönelik olarak da kabul edilmesi gerektiği açıktır.

Davacı, geçmişte yaşadığı kötü bir olayın toplum hafızasından silinmesini istemektedir. Unutulma hakkı ile geçmişindeki yaşanan talihsiz bir olayın unutulması

../..

geleceğini serbestçe şekillendirmek, diğer bir deyişle hayatında, yeni bir sayfa açma olanağı istemektedir. Kaldı ki, davacı da yargılama sırasında verdiği dilekçelerinde bu istem üzerinde ısrarla

durmuştur. Davacı unutulma hakkı ile özel hayatına ilişkin kişisel verilerinin üçüncü kişiler tarafından bilinmemesini, aradan geçen süre nedeniyle toplum hafızasından silinmesini istemektedir.

4 yıl önce gerçekleşen bir olayın mağduru olan kişinin adının açık bir şekilde yazılarak kitapta yer alması halinde unutulma hakkının bunun sonucunda da davacının özel hayatının gizliliğinin ihlal edildiği kabul edilmelidir. Avrupa Birliği Adalet Divanı'nın "Google Kararı"nda açıkladığı gibi ilgili verinin kamu hayatında oynadığı önemli rol ve halkın ilgili veriye yönelik yoğun ilgisi şeklinde, üstün bir kamu yararını ortaya koyan özel sebepler bulunmadığına göre bilimsel esere alınan kararda kişisel veriler açık bir şekilde yer almamalıdır..."

Şeklindeki gerekçeyle, başvuran ve cinsel saldırı suçu mağduru olan davacının isminin; her ne kadar okuyucuların somut olaydaki ismine değil gerçekleşen somut eyleme daha çok dikkat ettiği bilirse de, bilimsel ve eğitim amaçlı bir kitapta anlatılan örnek olay içeriğinde rumuzlanmadan bulunmasının, özel hayatın gizliliğini ve bu kapsamda unutulma hakkını ihlal eder mahiyette hukuka aykırı bir eylem olduğundan manevi tazminat koşullarının gerçekleştiğinin kabulüne karar verilmiştir.

II- İFADE VE BASIN ÖZGÜRLÜĞÜ

A-) İfade özgürlüğü; insanın özgürce bilgi ve düşünce sahibi olabilme, zihninde oluşturduğu düşünce ve kanaatlerinden ötürü kınanmama, bunları meşru şekil ve yöntemlerle dışa vurma imkan ve özgürlüğüdür. İfadenin, genellikle dış dünyayı gören, duyan, yorumlamaya ve algılamaya çalışan bir kişi veya toplum gibi gerçek bir muhatapı, bazen de cansız varlıklar veya bizzat kendisi gibi muhatapları vardır. İfadeye anlam veren onun muhatabıdır.

B-) Basın Özgürlüğü; ifade özgürlüğünün ayrılmaz bir parçası olmak üzere, insanların bilgiye ulaşma ve fikir elde edebilme yönündeki en önemli araçlardan olan basın, yazılı, görsel veya işitsel araçlarla sunduğu ve kamu hizmetini gerçekleştirme yolunda sahip olduğu özgürlüktür. Basın, geniş imkanları olan bir organizasyon olması, ona bireylere nazaran daha büyük bir muhatap sayısı (kitle) sağlamaktadır. Bu nedenle basının ifade özgürlüğünü kullanırken muhatapı üzerinde yarattığı etkinin boyutları da düşünülerek yaptığı işe bir kamu hizmeti ayrıcalığı tanınmış, bu ayrıcalıkla birlikte bahsedilen güvenilirliği, yapılan işten doğan sorumluluğun da büyük olmasını beraberinde getirmiştir.

Şüphesiz ifade ve basın özgürlüğü de diğer temel hak ve özgürlüklerde olduğu gibi sınırsız değildir. İfade ve Basın Özgürlüğünün sınırlanması, başta AİHS'nin 10/2. maddesi olmak üzere uluslararası ve ulusal mevzuatta düzenleme altına alınmıştır.

Avrupa İnsan Hakları Sözleşmesi'nin "ifade özgürlüğü" başlıklı 10. maddesinde;

"1- Herkes ifade özgürlüğü hakkına sahiptir. Bu hak, kamu makamlarının müdahalesi olmaksızın ve ülke sınırları gözetilmeksizin, kanaat özgürlüğünü ve haber ve görüş alma ve de verme özgürlüğünü de kapsar. Bu madde, devletlerin radyo, televizyon ve sinema işletmelerini bir izin rejimine tabi tutmalarına engel değildir.

2- Görev ve sorumluluklar da yükleyen bu özgürlüklerin kullanılması, Kanunla öngörülen ve demokratik bir toplumda ulusal güvenliğin, toprak bütünlüğünün veya kamu güvenliğinin korunması, kamu düzeninin sağlanması ve suç işlenmesinin önlenmesi, sağlığın veya ahlakın, başkalarının şöhret ve haklarının korunması, gizli bilgilerin yayılmasının önlenmesi veya yargı erkinin yetki ve tarafsızlığının güvence altına alınması için gerekli olan bazı formaliteler, koşullar, sınırlamalar veya yaptırımlara tabi tutulabilir."

İnsan Hakları Avrupa Mahkemesi ulusal makamların bu takdir yetkisini sözleşmenin 10. maddesiyle bağdaşır şekilde kullanıp kullanmadıklarını önüne gelen davalar aracılığıyla denetlemektedir. O halde, ulusal makamlar, ifade özgürlüğünün sınırlanması ile ilgili takdir yetkilerini kullanırken;

- Sınırlamanın kanunda öngörülüp öngörülmediği, açıkça tanımlanıp tanımlanmadığı,
- Sınırlamanın AİHS'nin 10/2. maddesinde yazılı veya Kanunda öngörülen meşru amaçlara uygun olup olmadığı,
- Sınırlamanın çağdaş demokratik toplumun gereklerine uygun olup olmadığı,
- Sınırlamada aşırıya gidilmemesi (orantılı ve ölçülü olunması), hususlarını gözetmek zorundadırlar.

Meşru amaç deyiminden; genellikle sözleşmenin 10/2. maddesinde yazılı kamu güvenliği, toplumsal ahlak ve ülkelerin yasalarında mevcut sair durumlar kastedilmektedir.

Çağdaş demokratik toplumun gerekleri tanımı ile anlatılmaya çalışılan ise; topluma sunulan, sınırlanmaması, kınanmaması, özgür bırakılması gereken ifadenin veya haberin; toplumun ilgisini çeken, güncel ve kamunun yararını güden bir tartışmayı içermesi ile halkı kin ve düşmanığa sevketmemesi, şiddete teşvik etmemesi, nefret veya ayrımcılık içermemesi, suçu ve suçluyu övmemesi, terör veya ayrılıkçı hareketleri övmemesi, meşrulaştırıp yüceltmemesi, başkalarının kişilik haklarını, onur, şeref ve saygınlığını, hakaret, sövme veya benzer yollarla zedelememesi gibi gerekliliklerdir.

Her ne kadar doktrinde bu konuda üye devletlerin aynı ölçüleri benimsemeleri gerektiği savunulmakta ise de değer yargıları ülkeden ülkeye değişmektedir. Çağdaş ülkelerin çoğunda; iftira,

onur, şeref ve saygınlığı zedeleyici söz ve beyanlar, müstehcen içerikli söz, yazı, resim ve açıklamalar, savaş kışkırtıcılığı, hukuk düzenini cebir yoluyla değiştirmeye yönelik, nefret, ayrımcılık, düşmanlık ve şiddet yaratmaya yönelik olan ifadeler düşünce özgürlüğü kapsamında değerlendirilmemekte, suç sayılmak suretiyle cezalandırılmaktadırlar.

T.C. Anayasası'nın 13. maddesine göre, temel hak ve hürriyetler;

- Özlerine dokunulmaksızın

- Yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak

- Ancak kanunla sınırlanabilir.

- Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.

Ancak olağanüstü hal, sıkıyönetim veya savaş halinde dahi kişilerin sert çekirdek hakları olan; yaşama hakkına, maddi ve manevi varlığının bütünlüğüne dokunulamaz, kimse din, vicdan, düşünce ve kanaatlerini açıklamaya zorlanamaz ve bunlardan dolayı suçlanamaz, suç ve cezalar geçmişe yürütülemez, suçluluğu mahkeme kararı ile saptanıncaya kadar kimse suçlu sayılamaz.

T.C. Anayasası'nın "Düşünce ve kanaat hürriyeti başlıklı" 25. maddesinde;

"Herkes, düşünce ve kanaat hürriyetine sahiptir.

Her ne sebep ve amaçla olursa olsun kimse, düşünce ve kanaatlerini açıklamaya zorlanamaz; düşünce ve kanaatleri sebebiyle kınanamaz ve suçlanamaz.",

T.C. Anayasası'nın "Düşünceyi açıklama ve yayma hürriyeti" başlıklı 26. maddesinde;

"Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Bu fıkra hükmü, radyo, televizyon, sinema veya benzeri yollarla yapılan yayımların izin sistemine bağlanmasına engel değildir.

Bu hürriyetlerin kullanılması, millî güvenlik, kamu düzeni, kamu güvenliği, Cumhuriyetin temel nitelikleri ve Devletin ülkesi ve milleti ile bölünmez bütünlüğünün korunması, suçların önlenmesi, suçluların cezalandırılması, Devlet sırrı olarak usulünce belirtilmiş bilgilerin açıklanmaması, başkalarının şöhret veya haklarının, özel ve aile hayatlarının yahut kanunun öngördüğü meslek sırlarının korunması veya yargılama görevinin gereğine uygun olarak yerine getirilmesi amaçlarıyla sınırlanabilir.

Haber ve düşünceleri yayma araçlarının kullanılmasına ilişkin düzenleyici hükümler, bunların yayımını engellemek kaydıyla, düşüncüyü açıklama ve yayma hürriyetinin sınırlanması sayılmaz.

Düşüncüyü açıklama ve yayma hürriyetinin kullanılmasında uygulanacak şekil, şart ve usuller kanunla düzenlenir."

T.C. Anayasası'nın "Basın hürriyeti" başlıklı 28. maddesinde;

"Basın hürdür, sansür edilemez. Basımevi kurmak izin alma ve malî teminat yatırma şartına bağlanamaz.

Devlet, basın ve haber alma hürriyetlerini sağlayacak tedbirleri alır.

Basın hürriyetinin sınırlanmasında, Anayasanın 26 ve 27 nci maddeleri hükümleri uygulanır..." şeklinde ifade ve basın özgürlüğü kavramlarının içeriği, kapsamı, sınırları ve kullanılması düzenleme altına alınmıştır.

Anayasa Mahkemesi Genel Kurulunun 03.03.2016 tarihli 2013/5653 başvuru sayılı dosyasında almış olduğu kararda da atıfta bulunduğu üzere;

"...Anayasa Mahkemesi birçok kararında ifade özgürlüğünün sadece düşünce ve fikirleri yayma özgürlüğünü değil haber ve fikirlere ulaşma özgürlüğünü de kapsadığını vurgulamıştır (Emin Aydın, B. No: 2013/2602, 23/1/2014, § 40; Kamuran Reşit Bekir [GK], B. No: 2013/3614, 8/4/2015, § 34). Bu bağlamda haber ve fikirlerin yayılmasını ve bunlara kamunun ulaşmasını kolaylaştıran İnternet'in toplum hayatındaki önemli rolü yadsınamaz. İnternet üzerinde arşiv oluşturma, aktüalitenin ve haberlerin saklanmasına ve erişilebilirliğine büyük ölçüde hizmet etmektedir. Bu nitelikteki arşivler özellikle doğrudan halkın erişimine açık ve genelde ücretsiz olmaları nedeniyle tarih eğitimi ve araştırma faaliyetleri için kaynak sunmaktadır. Öte yandan demokratik bir toplumda basının ilk işlevi olan "gözetleyici" rolünün bir sonucu da arşivlerin halkın erişimine sunulmasıdır (Wegrzynowski ve Smolczewski/Polonya, B. No: 33846/07, 16/7/2013, § 59; Times Newspapers Ltd/Birleşik Krallık (No. 1 ve 2), B. No: 3002/03 23676/03, 10/3/2009, §§ 27, 45). Bu nedenle İnternet'te tutulan arşivlerin, ifade ve basın özgürlükleri kapsamında olduğu açıktır. Dolayısıyla İnternet'te yayımlanan ve gazetecilik faaliyeti kapsamında kabul edilen bir haber arşivinin yayından kaldırılması basın özgürlüğüne yönelik bir müdahale teşkil eder.

Demokrasilerde devletin eylem ve işlemlerinin, adli ve idari yetkililerin olduğu kadar basının ve aynı zamanda kamuoyunun da denetimi altında bulunması gerekmektedir. Yazılı, işitsel ve görsel basın; kamu gücünü kullanan organların siyasi kararlarını, eylemlerini ve ihmallerini sıkı bir denetime tabi tutarak ve vatandaşların karar alma süreçlerine katılımını kolaylaştırarak demokrasinin sağlıklı bir

şekilde işlemlerini ve bireylerin kendilerini gerçekleştirmelerini güvence altına almaktadır (Kadir Sağdıç, § 50). Bu sebeple basın özgürlüğü, herkes için geçerli ve yaşamsal öneme sahip bir özgürlüktür (AYM, E.1997/19, K.1997/66, 23/10/1997).

AİHM, birçok kez demokratik bir toplumda basının oynadığı temel rolün altını çizmiştir. Her ne kadar başkalarının şöhret ve haklarının korunmasıyla ilgili olarak bazı sınırları aşmaması gerekse de basının, görev ve sorumluluklarının bilincinde olarak kamu yararını ilgilendiren her konuyu iletme görevi vardır. Basının böyle konularda bilgi ve fikir yaymadan ibaret olan görevine kamunun bu fikir ve bilgileri alma hakkı eklenir. AİHM'e

göre bu görevi olmasaydı basın, vazgeçilmez "gözetleyicilik" işlevini yerine getiremezdi (Bladet Tromso ve Stensaas/Norveç [BD], B. No: 21980/93, 20/5/1999, §§ 59, 62; Pedersen ve Baadsgaard/Danimarka [BD], B. No: 49017/99, 17/12/2004, § 71).

İfade özgürlüğü ile onu tamamlayan ve ifade özgürlüğünün kullanılmasını sağlayan basın özgürlüğü, Anayasa'da yer alan temel hak ve özgürlükleri sınırlama rejimine tabidir. Anayasa'nın 28. maddesinin dördüncü fıkrasında basın özgürlüğünün sınırlanmasında 26. ve 27. madde hükümlerinin uygulanacağı belirtilmiştir. Böylece basın özgürlüğü, ifade özgürlüğü ile ilgili genel hüküm niteliğindeki 26. madde ile sanatsal ve akademik ifadelerle ilgili 27. maddedeki sınırlama rejimine tabi tutulmuştur. Basın özgürlüğüne yönelik diğer sınırlamalar ise 28. maddenin beşinci ve izleyen fıkralarında yer almıştır. Basının, Anayasa'nın 26., 27. ve 28. maddelerinde sayılan sınırlandırmalardan biri olan "başkalarının şöhret veya haklarının, özel veya aile hayatlarının" korunması için konmuş olan sınırlandırmalara uyması gerekir (Kadir Sağdıç, § 55; İlhan Cihaner (2), § 62). Bu itibarla "başkalarının şöhret veya haklarının, özel veya aile hayatlarının" korunması bağlamında şeref ve itibarın korunması hakkının etki alanını genişletmenin ifade ve basın özgürlüklerinin ihlali sonucunu doğurabileceği hatırd tutulmalıdır.

Öte yandan başkalarının şöhret ve haklarının korunmasıyla ilgili olarak bazı sınırların aşılmaması gerekse de basının, görev ve sorumluluklarının bilincinde olarak kamu yararını ilgilendiren her konuyu iletme görevi olduğu, onun bu tür konularda bilgi ve fikir yaymadan ibaret olan görevine kamunun bu fikir ve bilgileri alma hakkının eklendiği hatırd tutulmalıdır (Kadir Sağdıç, § 51)

Bu sebeple Anayasa'nın 17. maddesinin birinci fıkrasında koruma altına alınan şeref ve itibarın korunmasını isteme hakkı ile başvuruya konu İnternet haber arşivinin Anayasa'nın 28. maddesinde güvence altına alınan basın özgürlüğü ve bu özgürlükle bağlantılı olarak Anayasa'nın 26. maddesinde güvence altına alınan ifade özgürlüğü arasında Anayasa Mahkemesi içtihadında ortaya konulan kriterlere uygun şekilde bir denge kurulması gerekmektedir. Ancak geçmişteki olayların arşivlenmiş

olması hâlinde çatışan haklar arasındaki dengelemenin güncel olaylara ilişkin yapılan haberlerden daha farklı yorumlanması makul kabul edilmelidir. Bu bağlamda, basının yayımladığı haberlerin gerçekliğine ilişkin olarak sorumluluk bilinci ile hareket etmesi (Kadir Sağdıç, §§ 53, 54; İlhan Cihaner (2), §§ 60, 61) gerekliliği, güncel haberlere nazaran doğası itibarıyla eskiyen ve yayımlanması ivedilik ve zorunluluk arz etmeyen geçmişe ilişkin haberler bakımından daha katı görünmektedir. Ancak yapılacak dengelemede haber arşivinin de Anayasa'nın 26. ve 28. maddeleri bağlamında güvence altına alındığı gözönünde tutulmalıdır...."

Yargıtay Ceza Genel Kurulunun 13.02.2007 tarihli, 2007/7-28 E. - 2007/34 K. sayılı kararında;

"Demokratik toplumlar, temel hak ve özgürlüklere dayanan toplumlardır. Bu tür toplumlarda Devletin görevi, temel hak ve özgürlükleri korumak ve geliştirmektir. Temel hak ve özgürlükler arasında düşünce ve kanaati açıklama özgürlüğünün önemli bir yeri bulunmaktadır. Bu özgürlüğün kullanılabilmesinin en önemli yollarından birisi de basındır.

Geneli ilgilendiren ya da ilgilendirmesi gereken tüm olaylar hakkında, halkı objektif ve gerçekleri yansıtabilecek biçimde aydınlatmak, çeşitli sorunlar üzerinde kamuoyunu düşünmeye çağırarak tartışmalar açmak, onu toplumsal ve siyasal oluşumlar üzerinde doğru ve gerçeğe uygun bilgilerle donatmak, yöneticileri eleştirmek, uyarmak ve bu yöntemlerle denetlemek, ayrıca içinde yaşadığı toplumun ve tüm insanlığın sorunları konusunda bireyi bilinçlendirmek durumunda olan basına, bu ödevlerini yerine getirirken ihtiyaç duyacağı bir kısım haklar da tanınmıştır. Bunlar; bilgi edinme, yayma, eleştirme, yorumlama ve eser yaratma haklarıdır.

Temelini Anayasa'nın 28. vd. maddelerinden alan ve 5187 sayılı Basın Kanunu'nun 3. maddesinde düzenlenen bu haklar, basın yoluyla işlenen suçlarda, hukuka uygunluk nedenlerini oluşturur. Bilgiyi yayma, eleştirme ve yorumlama haklarının kabulü için, açıklama, eleştiri veya değer yargısı biçimindeki bilginin gerçek ve güncel olması, açıklanmasında kamunun ilgi ve yararının bulunması, açıklanış şekli ile konusu arasında düşünsel bir bağ bulunması, açıklamada "küçültücü" sözlerin kullanılmaması gerekir."

Haber verme hakkının hukuka uygun bir biçimde kullanılabilmesi için gereken ölçütler dört başlık altında toplanmaktadır.

Bunlar;

- 1- Haber gerçek olmalı,
- 2- Haber güncel olmalı,

3- Haberin verilmesinde kamu yararı bulunmalı,

4- Haberin veriliş biçimi ile özü arasında düşünsel bir bağ bulunmalıdır.

Bu unsurlar eleştiri hakkı yönünden de geçerlidir. Yani eleştirinin olabilmesi için, yazının gerçek olgulara dayanması, güncel bulunması ve bu haberin verilmesinde kamu yararı bulunması koşullarına bağlıdır..." şeklinde gözetilmesi gereken temel kriterlerden bahsedilmiştir.

Yargıtay Ceza Genel Kurulu'nun 20.03.2007 gün ve 65-70 sayılı kararında da belirtildiği gibi; geneli ilgilendiren ya da ilgilendirmesi gereken tüm olaylar hakkında, halkı objektif ve gerçekleri yansıtacak biçimde aydınlatmak, çeşitli sorunlar üzerinde kamuoyunu düşünmeye çağırarak tartışmalar açmak, onu toplumsal ve siyasal oluşumlar üzerinde doğru ve gerçeğe uygun bilgilerle donatmak, yöneticileri eleştirmek, uyarmak ve bu yöntemlerle denetlemek, ayrıca içinde yaşadığı toplumun ve tüm insanlığın sorunları konusunda bireyi bilinçlendirmek durumunda olan basına, bu ödevlerini yerine getirirken ihtiyaç duyacağı bir kısım haklar da tanınmıştır. Bunlar; bilgi edinme, yayma, eleştirme, yorumlama ve eser ortaya koyma haklarıdır.

Temelini Avrupa İnsan Hakları Sözleşmesinin 10. maddesi ile Anayasa'nın 28. vd. maddelerinden alan ve 5187 sayılı Basın Kanununun 3. maddesinde düzenlenen basın özgürlüğü ve bu kapsamda bilgi edinme, yayma, eleştirme, yorumlama ve eser ortaya koyma hakkı, TCK'nın 25. maddesinin birinci fıkrasında; "Hakkını kullanan kimseye ceza verilmez" düzenlemesi kapsamında bir hukuka uygunluk nedenidir. Ancak habere ulaşma, haberi yorumlama ve eleştirme ile haberi kamuya ulaştırmayı kapsayan bu hakkın hukuka uygunluk nedeni olarak kabul edilebilmesi için; haberin gerçek ve güncel olması, haberin kamuyu ilgilendirmesi yani kamuoyunun haberi öğrenmekte menfaatinin bulunması ve haber ile haberin veriliş şeklinin uyumlu olması gereklidir. (Hamide Zafer, Ceza Hukuku Genel Hükümler, Beta Yayınevi, İstanbul, 2013, 3. bası, s.323; Nur Centel, Hamide Zafer, Özlem Çakmut, Türk Ceza Hukukuna Giriş, Beta Yayınevi, İstanbul, 2010, 6. basım, s.336-338; Hakan Hakeri, Ceza Hukuku Genel Hükümler, Adalet Yayınevi, Ankara, 2011, 12. basım, s.279-282). Nitekim Ceza Genel Kurulunun 24.02.1998 gün ve 386-52 sayılı kararında da aynı hususlara vurgu yapılmıştır.

III- DEĞERLENDİRME VE SONUÇ

Uyuşmazlığa konu somut olay, yukarıda yapılan açıklamalar, genel ilkeler ve emsal içtihatlarla birlikte değerlendirildiğinde;

Yerel bir gazetenin internet sitesinde verilen haberin bir kişinin şeref ve haysiyetine, kişiliğine saldırı amacından daha ziyade oda yönetimi hakkında bir yolsuzluk iddiasını ortaya koyduğu, haberin

sonunda yer alan fotoğrafın, iddiaların içinde yer alan oda başkanının oğlunun odaya yaptığı kredi başvurusu belgesi olduğu, açıklanması zorunlu olmayan bu belgenin, haberin çarpıcılığını, etkileyciliğini ve doğruluğunu artırmak maksadıyla haberin

kaynağını oluşturan bir delil mahiyetinde yazının sonuna yapıştırıldığı, böylece kredi başvuru belgesi içinde yer alan başvuranın kimlik, adres ve diğer iletişim bilgilerinin de üzeri çizilmeden, kapatılmadan haberi okuyan tüm ilgililere açıklandığı, bu yönüyle eylemin haberin muhataplarını tanımayan kişilere yönelik olarak kişisel verilerin korunmasına dair cezai ve hukuki mevzuata aykırı olabileceği, ancak bu değerlendirmeyi yapma hak ve yetkisinin bu hususta açılacak kamu davasına bakmakla görevli ve yetkili mahkemenin olduğu değerlendirilmiştir.

Başvuranın kimlik bilgilerinin, bir yolsuzluk iddiasıyla ilgili haberin altında yer alan kredi başvuru belgesi fotoğrafı aracılığıyla açıklanması eyleminin, ifade ve basın özgürlüğü kapsamında kalması, ayrıca URL adresinde yer alan haberin teknik olarak yazı ve fotoğraftan oluşan bir bütün halinde ve aynı sayfada yer alması karşısında; 5651 sayılı Kanun'un 9. maddesi kapsamında, haberde derhal ortadan kaldırılmasını ve erişimin engellenmesini gerektirir mahiyette acilen giderilmesi gereken bir kişilik hakkı ihlali olmadığından, başvuranın internet yayının içeriğine ve sayfanın tümüne erişimin engellenmesi yönündeki talebinin reddi gerektiği anlaşılmakla,

Yargıtay Cumhuriyet Başsavcılığının kanun yararına bozma istemine dayanan ihbarname içeriği, yukarıda belirtilen sebeplerle yerinde görülmediğinden REDDİNE, 24/09/2018 tarihinde oybirliğiyle karar verildi.

Yargıtay Kararı - 19. Ceza Dairesi (E. 2019/28161)

19. CD., E. 2019/28161 K. 2020/13552 T. 2.11.2020

Esas No.: 2019/28161

Karar No.: 2020/13552

Karar Tarihi: 02.11.2020

http://youtu.be/t_kZaSuaVQM uzantılı internet sitesinde yayımlanan video nedeniyle kişilik haklarına saldırıda bulunulduğunu iddia eden ilgisi ...tarafından yapılan erişimin engellenmesi talebinin reddine dair Çanakkale Sulh Ceza Hâkimliğinin 27/11/2018 tarihli ve 2018/4576değişik iş sayılı kararına karşı yapılan itirazın reddine ilişkin mercii Burhaniye Sulh Ceza Hâkimliğinin 14/12/2018 tarihli ve 2018/3053 değişik iş sayılı kararı aleyhine, Adalet Bakanlığı'nun 29.03.2019 gün ve 2019 - 891 sayılı kanun yararına bozma istemini içeren yazısı ekindeki dava dosyası, Yargıtay Cumhuriyet Başsavcılığının 08.04.2019 gün ve KYB. 2019/35859 sayılı ihbarnamesi ile dairemize gönderilmekle okundu.

Anılan ihbarnamede;

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu'nun 9/1. maddesinde "İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğe erişimin engellenmesini de isteyebilir." ve anılan maddenin 3. fıkrasında "İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talepleri doğrultusunda hâkim bu maddede belirtilen kapsamda erişimin engellenmesine karar verebilir." şeklindeki düzenlemeler karşısında, itiraz merciince erişimin engellenmesi talep edilen videoda talepte bulunanın kişilik haklarını ihlâl edici mahiyette olmadığı ve eleştiri mahiyetinde bulunduğundan bahisle itirazın reddine ilişkin karar verilmiş ise de;

Benzer bir olayla ilgili olarak Yargıtay 19. Ceza Dairesinin 10/12/2018 tarihli ve 2018/7735 esas, 2018/13080 karar sayılı ilâmında; "...Yargıtay Hukuk Genel Kurulunun 17/6/2015 tarihli ve E.2014/4-56, K.2015/1679 sayılı kararının ilgili kısmı şöyledir : "...Unutulma hakkına gelince; unutulma hakkı ve bununla ilişkili olan gerektiği ölçüde ve en kısa süreliğine kişisel verilerin depolanması veya

tutulması konuları, aslında kişisel verilerin korunması hakkının çatısını oluşturmaktadır. Her iki hakkın temelinde bireyin kişisel verileri üzerinde serbestçe tasarruf edebilmesini, geçmişin engeline takılmaksızın geleceğe yönelik plan yapabilmesini, kişisel verilerin kişi aleyhine kullanılmasının engellenmesini sağlamak yatmaktadır. Unutulma hakkı ile geçmişinde kendi iradesi ile veya üçüncü kişinin neden olduğu bir olay nedeni ile kişinin geleceğinin olumsuz bir şekilde etkilenmesinin engellenmesi sağlanmaktadır. Bireyin geçmişinde yaşadığı olumsuz etkilerden kurtularak geleceğini şekillendirebilmesi bireyin yararına olduğu gibi toplumun kalitesinin gelişmişlik seviyesinin yükselmesine etkisi de tartışılmazdır. Unutulma hakkı; üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerin silinmesini ve yayılmasının önlenmesini isteme hakkı olarak ifade edilebilir..." ... Yukarıda yapılan açıklamalar ve genel ilkeler bağlamında somut olay değerlendirildiğinde; başvuruya konu haberlerin ilk kez yayınlandıkları tarihte, herhangi bir eleştiri veya yorum yapılmaksızın internet üzerinde yorumsuz biçimde yayınlanmalarının, olay tarihinde kişilik haklarına karşı bir saldırı veya ihlal içermediği, bu hâliyle ifade ve basın özgürlüğü kapsamında değerlendirilebileceği, başvuranların beraat etmeleri sonucu, aradan geçen dokuz yıl sonra, haberin "güncellik" değerini yitirdiği, dolayısıyla haberin o tarihte "gerçeklik ve doğruluk" kriterlerini karşılamasının artık bir önemi kalmadığı, habere konu olan yargılama sürecinin tüm aşamalarıyla sona ermesiyle birlikte, habere konu olan kişiler için haksızlık içeren durumun, toplum tarafından öğrenilmesinin, geçmişte gerçeklik ve doğruluk payı varmış gibi ifşa edilmesi anlamına gelebileceği, dolayısıyla adı geçen habere istenildiği zaman ulaşılmasının, toplum açısından yanlış algılamaya yol açabileceği, başvuranların beraatle sonuçlanan bir yargı sürecinde gözaltına alınması ve tutuklanması süreçlerine dair haberin basının arşivinde bulunmasının, haberin kamu yararı için gelecekte hatırlanması veya istatistiki açıdan değerlendirilmeye alınması gibi işlevi de taşımadığı, dolayısıyla haberin yayında kalmasının, toplumun ilerlemesi, gelişmesi için bir katkı sağlamayacağı gibi, kamu yararına toplum hafızasında yer etmesi gibi bir etkisi de olmadığı, haberin içeriğini oluşturan kişilerin; toplumu temsil ve topluma hizmet etme gayesiyle seçilmiş veya atanmış siyasilerden olmadığı gibi, topluma kendini anlatma ve toplumu aydınlatma gayesiyle eser veren sanatçılardan veya aydınlardan da olmaması nedeniyle, suç geçmişlerine dair bilgilerin kamuyu ilgilendirmediği, ayrıca bu bilgilerin sadece devletin belirli organlarınca kayıt altında tutulabileceğinin, başvuranların isimlerinin ad ve soyadı şeklinde açıkça yazılması suretiyle "örgüt, fuhuş ve insan ticareti" gibi kelimelerin yanında anılmaya devam etmesinin, şeref ve haysiyetlerine karşı bir eylem olduğu gibi, bu nedenle gözaltına alındıkları bilgisinin arşivlenmesinin kişisel verilerin izinsiz olarak işlenmesi ve yayınlanması anlamına geleceği, yukarıda yer alan

değerlendirmeler karşısında, başvuruların istememesine rağmen, geçmişlerinde yer eden olumsuz tecrübelerle dair haberlere, toplum tarafından istenen her anda kolaylıkla ulaşılmasının başvuruların kişilik haklarını zedelediği, sonuç ve kanaatine varıldığından ..." şeklindeki açıklamalar nazara alındığında,

Dosya kapsamına göre, başvuru sahibinin talep konusu videonun yayınlandığı 01/08/2013 tarihinde ve halen Çanakkale Hasan Ali Yücel Anadolu Lisesinde Türk Dili ve Edebiyatı öğretmeni olarak görev yapmakta olduğu, bahse konu videonun yayınlanmasından itibaren beş yılı aşkın bir süre geçmiş ve halen ulaşılabilir olmasının, başvuru sahibinin mesleki haysiyetini zedeleyici nitelikte olduğu, video içeriğinin eleştiri sınırını aştığı ve başvuranın istememesine rağmen, geçmişinde yer eden olumsuz tecrübelerle dair habere, toplum tarafından istenen her anda kolaylıkla ulaşılmasının başvuranın kişilik hakkını zedelediği anlaşılmalı, itirazın kabulü yerine yazılı şekilde reddine karar verilmesinde isabet görülmediği gerekçesiyle 5271 sayılı Ceza Muhakemesi Kanununun 309. maddesi uyarınca anılan kararın kanun yararına bozulması isteminde bulunulmakla,

Gereği görüşülüp düşünüldü:

5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"un "içeriğin yayından çıkarılması ve erişimin engellenmesi" başlıklı 9. maddesinin uygulanma şartları;

- İnternet ortamında yapılan bir yayın olması,

- Yapılan yayın içeriği nedeniyle, gerçek ve tüzel kişiler ile kurum ve kuruluşların "kişilik haklarının" ihlal edilmesidir.

İnternet içeriğine erişimin engellenmesi tedbiri, başvuranın kişilik haklarını ihlal ettiği mahkeme kararıyla tespit edilen bir internet yayınına toplumun erişiminin derhal engellenmesi amacıyla düzenlenmiş bir tedbirdir. Erişimin engellenmesi tedbirinin uygulanması için yayının içeriğinde kişilik hakkına yönelik bir suç unsuru bulunması şartı aranmadığı gibi yayın içeriğinde bir suç işlenmişse dahi yürütülecek ceza muhakemesinin sonucu beklenmeksizin erişimin engellenmesi tedbirine bir koruma tedbiri olarak hükmedilebilecektir. Erişimin engellenmesine konu edilen ve başvuranın kişilik hakkını ihlal ettiği tespit edilen internet yayınının "bir an önce" internet ortamından kaldırılması, gerek kişilik haklarının gerekse kamu düzeninin korunması açısından elzemdir. Ancak verilecek kararlarda ifade ve basın özgürlüğünün zedelenmemesi de gözetilmesi gereken bir diğer husustur.

Kişilik Hakları; özel hukukta kişinin doğumla birlikte kazandığı ve üzerine kişisel gelişimiyle birlikte her geçen gün yeni değerler kattığı kişiliğinin, maddi ve manevi bütünlüğünün, isminin, mesleki kariyerinin, ailesinin ve hatta sosyal çevresinin kişi üzerinde oluşturduğu, kısacası kendini gerçekleştirme yolunda elde ettiği tüm kazanımlarının ve menfaatlerinin, hukuk düzeni tarafından koruma altına alınan yönüdür. Kişilik hakları, haklar kategorisinde yer alan mutlak haklar başlığı altında, kişiye sıkı sıkıya bağlı ve devredilemeyen, parayla satın alınamayacak bir takım değerleri koruduğu için malvarlığına ilişkin değil, şahısvarlığına ilişkin haklardandır.

4721 sayılı Türk Medeni Kanun'un "Kişiliğin korunması" üst başlığında yer alan 24. maddesi;

"Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir. Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da Kanun'un verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır." hükümleriyle, herhangi bir hukuka uygunluk sebebi olmaksızın kişilik hakkına karşı yapılan her saldırının hukuka aykırı olduğunu ve bu saldırıya uğrayan kimsenin hakimden bu özel kanun maddesine göre de korunma isteyebileceğini düzenlemektedir.

Kişilik haklarına dair yukarıdaki düzenlemeler, kişinin bu temel hakkını sınırlayabilen durumları, "kişinin rızası, daha üstün nitelikte özel veya kamusal yarar veya kanunun verdiği yetkisinin kullanılması" olarak sınırlandırmış, bu durumlar haricinde kişinin sahip olduğu kişilik haklarına karşı her tür saldırının mutlak suretle "hukuka aykırı" olduğunu belirtmiştir. İfade ve basın özgürlüğü de şüphesiz bir hukuka uygunluk nedeni olarak kabul edilmektedir.

İfade özgürlüğü; insanın dilediği zaman, koşul ve şekilde, herhangi bir baskı, sınırlama veya zorlama olmaksızın;

- Bilgi, haber, mesaj ve yorumlara erişebilme,
- Elde ettiği bilgiyi özgürce yorumlama, düşünebilme ve fikir sahibi olma,
- Sahip olduğu düşünce ve kanaatini baskı altında kalmadan açıklayabilme, iletme ve yayma imkanının bulunmasıdır.

İfade özgürlüğü, AİHS'nin 10. maddesinde, T.C. Anayasası'nın 25 ve 26. maddelerinde düzenlenmiş bir temel hak ve özgürlüktür. Ancak diğer temel hak ve özgürlüklerde olduğu gibi ifade özgürlüğünün de bir kapsamı ve sınırları vardır.

Yukarıda anlatılan genel ilkelerin kanun yararına bozmaya konu somut uyuşmazlık açısından değerlendirilmesine gelince;

Başvuran öğretmenin, erişime engellenmesini istediği video, youtube adlı sosyal paylaşım sitesinde Esat Kurnaz (sanal) adlı bir kişi tarafından 10.08.2013 tarihinde paylaşılan videodur. Paylaşım içeriğinde, Hasan Ali Yücel Lisesi'nde görev yapan başvuran öğretmenin, sınıf içinde ders yapmaya çalışırken kayda alındığı anlaşılmaktadır. Videoyu çeken cep telefonu, sınıftaki bir öğrenciye aittir ve çekimin öğrencilerin sıralarından ayakta çekildiği görülmektedir. Öğretmen iki erkek öğrenciyi tahtaya kaldırmış ve diğer öğrencilere ders anlatmaya çalışmakta, ancak sınıfta büyük bir gürültü ve herkesin kendi halinde birden fazla diyaloga girdiği görülmektedir. Videonun başlığı "Bu nasıl edebiyat öğretmeni"dir. Başvuranın dilekçesinde, 5 yıl önce bir öğrenci tarafından çekilen ancak internet üzerinde herkesin erişimine kim tarafından sunulduğu bilinmeyen bu videoyu artık unutmak istediğini, yeni okulu ve yeni sınıfındaki görevine, geçmişi ile ilgili bu video olmadan devam etmeyi amaçladığını belirterek erişimin engellenmesini talep ettiği görülmektedir.

Başvuranın talebi ve itirazı, ilgili Sulh Ceza Hakimliklerince, başvuruya konu yorumları yapan kişilerin ve içerikleri yayınlayan sitenin savunma yapabilme imkanı olmadığından bahisle konuyla doğrudan ilgisi olmayan ve "basın özgürlüğünü" anlatan bir Anayasa Mahkemesi kararına atıfla reddedilmiş ise de;

Başvuranın, oluşturulmasında bilgisi ve rızası olup olmadığı anlaşılamayan video kaydının, esasen başvuranın kişilik haklarını ihlalinden ziyade, bir okulda sadece öğrenciler ile öğretmen arasında yapılan ders sırasında, kamu hizmetini yerine getirmeye çalışan bir öğretmen ve sınıftaki tüm öğrencileri konu edinmesi bakımından kişisel verilerin işlenmesi olarak görülmesi mümkündür. Öte yandan kamu hizmetinin görülmesi sırasında ilgili idarenin bilgisi ve onayı alınmaksızın çekilen ve internet paylaşım sitelerinde dolaşan video nedeniyle bir soruşturma yapılıp yapılmadığı da dosya kapsamından anlaşılamamaktadır. Bu nedenle video içeriğinde bulunan görüntülerinin internet ortamında yer almasının "Kişisel Verilerin Korunması" ve "Unutulma Hakkı" kapsamında değerlendirilmesi gerekecektir.

Kişisel Veri; 07.04.2016 tarihinde yürürlüğe giren Kişisel Verilerin Korunması Kanunu'nun 3. Maddesinde "...Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi..." şeklinde tanımlanmıştır.

6698 sayılı Kanun'un ilgili madde gerekçesinde; "...Kişisel veriler, sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin aklî, psikolojik, fizikî, kültürel, ekonomik, sosyal ve sair özelliklerine ilişkin verilerdir. Bir kişinin belirli

veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabileme özellikleri nedeniyle kişisel verilerdir" açıklamasına yer verilmiştir.

Öğretide de kişisel verilere ilişkin; "Bireyin şahsi, mesleki ve ailevi özelliklerini gösteren, o bireyi diğer bireylerden ayırmaya ve niteliklerini ortaya koymaya elverişli hertürlü bilgiyi ifade eder" (Ersan Şen, Türk Ceza Kanunu Yorumu, Vedat Kitapçılık, İstanbul, 2006, s.601), "Bir kişinin adı ve soyadı, yaşı, cinsiyeti, doğum yeri, dini, TC kimlik numarası, cinsel hayatı, cep telefonu numarası, medeni durumu, ailesi, işi, geliri, borçları, adresi, geçirdiği hastalıklar, özel zevkleri ve buna benzer bilgileri" (Volkan Sırabaşı, İnternet ve Radyo- Televizyon Aracılığıyla Kişilik Haklarına Tecavüz, Adalet Yayınevi, Ankara, 2007, 2. Bası, s.195) şeklinde tanımlar yapılmıştır.

Yargıtay Ceza Genel Kurulu'nun 17.06.2014 tarihli, 2012/12-1510 E. 2014/331 K. sayılı kararında;

"...Kişilerin, sadece insan olması ve toplumdaki yeri, bazı değerleri kişisel veri haline getirmektedir, örneğin; kişinin adı, adresi, kimlik bilgileri, medeni durumu vb... Bunun yanında teknolojik gelişmeler nedeniyle gittikçe karmaşıklaşan toplum hayatındaki bir takım bilgiler de kişisel veri haline gelmiştir, örneğin; vatandaşlık numarası, banka hesap numarası, telefon numarası, elektronik posta adresi ve şifresi vb... Dolayısıyla farklı gruplandırmalar bulunmakla birlikte kişisel verilerin iki başlık altında toplanması mümkündür. Birinci grupta; insanın varoluşundan kaynaklanan kişiliğine ait bilgiler, ikinci grupta ise; teknolojinin gelişmesiyle insanın modern toplumda yer alması nedeniyle kendisine verilen ya da çeşitli hizmetlere ulaşmasında kullanılan bilgiler yer almaktadır. Ancak her iki grupta yer alan bilgilerin de kişisel veri olarak hukuk düzenindeki değeri ve korunmaları açısından bir fark bulunmamaktadır. (Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayınevi, Ankara, 2014, 4. bası, s.577)

TCK'nun 136. maddesinde tıpkı 135. maddesinde olduğu gibi korunan hukuki değer genel olarak kişilerin özel hayatı ve hayatın gizli alanı, özelde ise kişisel verilerdir. Bu düzenlemeler ile tüm kişisel veriler koruma altına alındığından kişisel verilerin mutlaka gizli olması zorunlu değildir. Gizli olmayan ve herkes tarafından bilinen kişisel veriler de hukuka aykırı eylemlere karşı korunmalıdır. Zira kişisel verilerin korunmasına ilişkin suçlarda korunan hukuki değer "sır" olmayıp, verinin ilgisi

olan kişinin kişilik haklarıdır.(Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayınevi, Ankara, 2014, 4. bası, s.579, 588-593)...

...Bu açıklamalar ışığında uyumsuzluk konusu değerlendirildiğinde; TCK'nun 135 ve 136. maddelerindeki kişisel verilerin korunmasına ilişkin düzenlemelerde sadece sır niteliğinde kişisel verilerin korunacağına ilişkin bir hükmün bulunmaması ve aksine 135. maddenin gerekçesinde gerçek kişiyle ilgili her türlü bilginin kişisel veri olarak kabul edilmesi gerektiğinin belirtilmesi karşısında, her türlü kişisel verinin hukuka aykırı olarak başkasına verilmesi, yayılması ve ele geçirilmesi fiillerinin kanunun 136. maddesindeki suçu oluşturduğu kabul edilmelidir.

Bu kapsamda somut olayda, sanığın genel yayın yönetmenliğini yaptığı gazetede köşe yazarı olarak çalışan katılanın yazdığı köşesinde kullanılan fotoğrafın, hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle sanık tarafından internetteki özel bir arkadaşlık sitesine kimlik, adres ve telefon bilgileri verilmeksizin ve erkek arkadaşı aradığı açıklamasıyla konulması eylemi, TCK'nun 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak yayma suçunu oluşturmaktadır...."

Şeklindeki gerekçeyle, sanığın, mağdurun zaten onu tanıyan herkesçe bilinen ve kolaylıkla ulaşılabilen fotoğrafını, altında mağdurun erkek aradığını belirterek rızası dışında bir arkadaşlık sitesinde yayınlaması eyleminin, hukuka aykırı bir eylem olduğu ayrıca TCK'nun 136. maddesinde belirtilen suçu oluşturduğuna tereddüt bulunmadığı tespiti yapılmıştır.

Keza Yargıtay Hukuk Genel Kurulu'nun 17.06.2015 tarihli, 2014/4-56 E. Ve 2015/1679 K. Sayılı kararında da;

"...Avrupa İnsan Hakları Sözleşmesi (AİHS)'nin 8. maddesinde yer alan özel yaşama saygı hakkı altında korunan "mahremiyet hakkı"nın, bireyin kendisi hakkındaki bilgileri kontrol edebilmesi şeklindeki hukuki çıkarlarını da içerdiği ifade edilmektedir. Zira bireyin kendisine ait herhangi bir bilginin, kendi rızası olmaksızın açıklanmaması, yayılmaması ve bu bilgilere başkalarının ulaşamaması kısacası kişisel verilerinin mahrem kalması konusunda hukuki menfaati bulunmaktadır. (Gülay Arslan Öncü, Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması, Beta Yayınları, İstanbul 2011, s.182)...

Kişiyi unutulma hakkının sağlanması ile birlikte özel hayatının gizliliği korunmuş olacaktır.

Somut olaya bu kapsamda bakıldığında; davacı, kamu görevinin veya hizmet ilişkisinin sağladığı nüfuzu kötüye kullanarak, müteselsilen cinsel saldırı suçunun mağdurudur. 2006 yılında gerçekleşen eylem tarihinde davacı bekâr olup maruz kaldığı eylem geleceği açısından etkilidir. Yapılan

yargılama sonunda kamu görevlisi olan sanık ceza almıştır. Temyiz istemi üzerine yapılan inceleme sonunda ise hüküm 2009 yılında onanmıştır. Mağdur davacı gerek hazırlık gerekse de yargılama sırasında cinsel saldırının nasıl gerçekleştiğini açık bir şekilde anlatmış, bu anlatımlar doğal olarak karar metnine geçirilmiştir. Karar mağdur ve sanığın ismi rumuzlanmadan 2010 yılı nisan ayında yayınlanan kitapta yer almıştır.

Hemen ifade edilmelidir ki; davacının rızası dışında bir kitapta geçen ismi kişisel veri niteliğindedir.

Ayrıca şunun da ifade edilmesi gereklidir ki; unutulma hakkı tanımlarına bakıldığında her ne kadar dijital veriler için düzenlenmiş ise de, bu hakkın özellikleri ve bu hakkın insan haklarıyla arasındaki ilişkisi dikkate alındığında; yalnızca dijital ortamdaki kişisel veriler için değil, kamunun kolayca ulaşabileceği yerde tutulan kişisel verilere yönelik olarak da kabul edilmesi gerektiği açıktır.

Davacı, geçmişte yaşadığı kötü bir olayın toplum hafızasından silinmesini istemektedir. Unutulma hakkı ile geçmişindeki yaşanan talihsiz bir olayın unutulması geleceğini serbestçe şekillendirmek, diğer bir deyişle hayatında, yeni bir sayfa açma olanağı istemektedir. Kaldı ki, davacı da yargılama sırasında verdiği dilekçelerinde bu istem üzerinde ısrarla durmuştur. Davacı unutulma hakkı ile özel hayatına ilişkin kişisel verilerinin üçüncü kişiler tarafından bilinmemesini, aradan geçen süre nedeniyle toplum hafızasından silinmesini istemektedir.

4 yıl önce gerçekleşen bir olayın mağduru olan kişinin adının açık bir şekilde yazılarak kitapta yer alması halinde unutulma hakkının bunun sonucunda da davacının özel hayatının gizliliğinin ihlal edildiği kabul edilmelidir. Avrupa Birliği Adalet Divanı'nın "Google Kararı"nda açıkladığı gibi ilgili verinin kamu hayatında oynadığı önemli rol ve halkın ilgili veriye yönelik yoğun ilgisi şeklinde, üstün bir kamu yararını ortaya koyan özel sebepler bulunmadığına göre bilimsel esere alınan kararda kişisel veriler açık bir şekilde yer almamalıdır..."

Şeklindeki gerekçeyle, başvuran ve cinsel saldırı suçu mağduru olan davacının isminin; her ne kadar okuyucuların somut olaydaki ismine değil gerçekleşen somut eyleme daha çok dikkat ettiği bilirse de, bilimsel ve eğitim amaçlı bir kitapta anlatılan örnek olay içeriğinde rumuzlanmadan bulunmasının, özel hayatın gizliliğini ve bu kapsamda unutulma hakkını ihlal eder mahiyette hukuka aykırı bir eylem olduğundan manevi tazminat koşullarının gerçekleştiğinin kabulüne karar verilmiştir.

Dairemizin, başta 2016/15510 E. 2017/5325 K. sayılı kararında ve pek çok emsal kararında da gerekçeleri belirtildiği üzere;

Unutulma Hakkı; insanlar hakkında, basında, yazılı, görsel/işitsel medya veya internet medyasında, kısacası kitle iletişim araçları üzerinde; kişilerin geçmişine dair kişisel verilerine, kişiler hakkında geçmişte hukuka uygun yollar ve gerekçelerle (tam anlamıyla eksiksiz ve doğru olarak sunulsa dahi) paylaşılmış bilgi, haber veya yorumlara, isteyen herkesçe her an ulaşılabilir olmasının engellenmesi yönünde hukuken korunan menfaat olarak adlandırılabilir.

Yargı organlarının; internet arşivinde kişilerin şeref ve saygınlığına yönelen, kişilerin özel hayatı ve kişisel verilerinin kamu yararına katkı sağlamayacak şekilde işlendiği görülen, güncelliğini yitiren, her an toplumun erişimine açık halde bulunan ve tarihsel bir veri olarak da kabul edilemeyeceği anlaşılan yayınlar hakkında; makul, haklı ve ispatlanabilir taleplerde bulunulması halinde, ifade ve basın özgürlüğünün özüne hâlel getirmemek şartıyla, "kişisel verilerin korunması" ve "unutulma hakkı" kapsamında "erişime engellenmesi" yönünde kararlar verebileceği değerlendirilmektedir.

Bu durumda bir İnternet yayınının "unutulma hakkı" kapsamında İnternet ortamından çıkarılabilmesi için;

- yayının içeriği,
- yayında kaldığı süre,
- güncelliğini yitirme,
- tarihsel bir veri olarak kabul edilememe,
- kamu yararına katkısı (toplumsal açıdan haberin değeri, haberin geleceğe ışık tutan niteliği)
- habere konu kişinin siyasetçi veya ünlü olup olmadığı,
- haber veya makalenin konusu, bu bağlamda haberin olgusal gerçekler ya da değer yargısı içerip içermediği,
- halkın paylaşılan veriye yönelik ilgisi gibi hususların her somut olay açısından birlikte değerlendirmeye tabi tutularak ayrıntılı şekilde incelenmesi gerekmektedir.

Yukarıda ayrıntılarıyla izah edildiği üzere;

Kanun yararına bozmaya konu karar ve başvuru sırasında, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun henüz yürürlükte olmadığı, ancak kişisel verilerin hukuken korunması ve unutulma hakkı kavramlarının yukarıda atıf yapılan değişik yargı kararlarına konu olduğu bilinmektedir. İnsanların isim, resim veya görüntü gibi vücut bütünlüklerine dair kişisel verilerinin, internet ortamında kişilerin rızası olmaksızın paylaşılması, hukuka aykırılık, hatta bazı durumlarda suç da oluşturabilmektedir. Başvuranın görüntülerinin internet üzerindeki bir sosyal paylaşım sitesinde

rızası olmadığı halde başkaları tarafından paylaşılmasının; kişisel verilerin korunmasına dair kurallara ve unutulma hakkına aykırılık teşkil edeceği değerlendirilmiştir.

Bu nedenlerle, ilgili Sulh Ceza Hakimliklerince, başvuru hakkında kişisel verilerin korunması ve unutulma hakkı çerçevesinde değerlendirme yapılması ve sonuç itibarıyla başvuranın görüntüsünün izni olmaksızın 5 yılı aşkın bir süredir yayınlandığı video paylaşımının (ifade veya basın özgürlüğü kapsamında kalsa dahi) kişisel verilerin korunması ve unutulma hakkı çerçevesinde erişimin engellenmesine dair olumlu yönde bir karar verilmesi gerekirken;

Ortada herhangi bir basın organizasyonu veya basın faaliyeti bulunmadığı göz ardı edilerek, Anayasa Mahkemesinin basın özgürlüğü ve erişimin engellenmesi kararı verilmesi istenen bir basın kuruluşunun savunmalarına dair emsal kararından hareketle, başvurunun reddine karar verildiği anlaşılmakla,

Yargıtay Cumhuriyet Başsavcılığının kanun yararına bozma istemine dayanan ihbarname içeriği yerinde görüldüğünden, Burhaniye Sulh Ceza Hâkimliğinin 14/12/2018 tarihli ve 2018/3053 değişik iş sayılı kararının 5271 sayılı CMK'nın 309/4-d maddesi uyarınca BOZULMASINA, bozma sebebine göre işin esasını çözen bir karar alınması ve yerel mahkemece yapılacak başka bir işlem bulunmaması nedenleriyle;

http://youtu.be/t_kZaSuaVQM uzantılı internet sitesinde yayımlanan video yayınına yönelik verilen erişimin engellenmesi talebinin reddine dair, başvuran tarafından yapılan itirazın kabulüne, adı geçen URL adreslerinde yukarıda adı geçen köşe yazısına ERİŞİMİN ENGELLENMESİNE, kararın gereğinin; 5651 sayılı Kanun'un 9. vd. maddeleri gereği "Erişim Sağlayıcıları Birliği" tarafından yerine getirilmesi için karardan bir suretin adı geçen Birliğe gönderilmesine, 02.11.2020 tarihinde oy birliğiyle karar verildi.

Yargıtay Kararı - 19. Ceza Dairesi (E. 2020/4751)

Yargıtay 19. CD., E. 2020/4751 K. 2021/1235 T. 8.2.2021

Esas No.: 2020/4751

Karar No.: 2021/1235

Karar Tarihi: 08.02.2021

<https://ilerihaber.org/içerik/11-108331.html>, [Bhttps://www.birgün.net/haber/283235](https://www.birgün.net/haber/283235) ve <https://www.krttv.com.tr/gündem-h24257.html> uzantılı internet sitelerinde yayınlanan haberlerin içeriğine ilgilisi ... vekili tarafından yapılan erişimin engellenmesi talebinin reddine dair Ankara 3. Sulh Ceza Hâkimliğinin 15/01/2020 tarihli ve 2020/689 değişik iş sayılı kararına yönelik itirazın reddine ilişkin mercii Ankara 4. Sulh Ceza Hâkimliğinin 21/01/2020 tarihli ve 2020/742 değişik iş sayılı kararı aleyhine, Adalet Bakanlığı'nın 04.08.2020 gün ve 2020 - 7443 sayılı kanun yararına bozma istemini içeren yazısı ve ekindeki dava dosyası, Yargıtay Cumhuriyet Başsavcılığının 15.09.2020 gün ve KYB. 2020/73747 sayılı ihbarnamesi dairemize gönderilmekle okundu.

Anılan ihbarnamede;

Dosya kapsamına göre, talepte bulunan hakkında kadına karşı şiddet olaylarına karıştığına, cinsel taciz, hakaret, özel hayatın gizliliğini ihlal ve kişisel verilerin kaydedilmesi suçlarından yapılan kovuşturmayla ilişkin olarak yukarıda belirtilen internet sitelerinde yapılan haber ve paylaşımlar sebebiyle ilgilisi vekili tarafından erişimin engellenmesi talebinde bulunulması üzerine, mahkemesince erişimin çekişmeli bir dava yoluna başvurmada gecikmesinin ve süratle ortadan kaldırılması ihtiyacını ortaya koymadığından ve söz konusu talebin çekişmesiz dava yoluyla uygulanmasını gerektirecek ağırlık ve nitelikte olmamasından bahisle talebin reddine karar verilmiş ise de; anılan haber içeriğindeki olaya ilişkin olarak yapılan yargılama neticesinde ...'nun cinsel taciz, özel hayatın gizliliğini ihlal ve kişisel verilerin kaydedilmesi suçlarından beraatine, hakaret suçundan mahkumiyetine dair verilen İstanbul Anadolu 42. Ağır Ceza Mahkemesinin 19/02/2016 tarihli ve 2015/354 esas, 2016/96 sayılı kararın, Yargıtay 12. Ceza Dairesinin 16/01/2019 tarihli ve 2018/7118 esas, 2019/629 sayılı kararı ile onanarak kesinleşmiş bulunduğu,

Benzer bir olayla ilgili olarak Yargıtay 19. Ceza Dairesinin 05/06/2017 tarihli ve 2016/15510 esas, 2017/5325 karar sayılı ilâmında yer alan, "Yargıtay Hukuk Genel Kurulunun 17/6/2015 tarihli ve E.2014/4-56, K.2015/1679 sayılı kararının ilgili kısmı şöyledir: "...Unutulma hakkına gelince; unutulma

hakkı ve bununla ilişkili olan gerektiği ölçüde ve en kısa süreliğine kişisel verilerin depolanması veya tutulması konuları, aslında kişisel verilerin korunması hakkının çatısını oluşturmaktadır. Her iki hakkın temelinde bireyin kişisel verileri üzerinde serbestçe tasarruf edebilmesini, geçmişin engeline takılmaksızın geleceğe yönelik plan yapabilmesini, kişisel verilerin kişi aleyhine kullanılmasının engellenmesini sağlamak yatmaktadır. Unutulma hakkı ile geçmişinde kendi iradesi ile veya üçüncü kişinin neden olduğu bir olay nedeni ile kişinin geleceğinin olumsuz bir şekilde etkilenmesinin engellenmesi sağlanmaktadır. Bireyin geçmişinde yaşadığı olumsuz etkilerden kurtularak geleceğini şekillendirebilmesi bireyin yararına olduğu gibi toplumun kalitesinin gelişmişlik seviyesinin yükselmesine etkisi de tartışılmazdır. Unutulma hakkı; üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerin silinmesini ve yayılmasının önlenmesini isteme hakkı olarak ifade edilebilir..." Yukarıda yapılan açıklamalar ve genel ilkeler bağlamında somut olay değerlendirildiğinde; başvuruya konu haberlerin ilk kez yayınlandıkları tarihte, herhangi bir eleştiri veya yorum yapılmaksızın internet üzerinde yorumsuz biçimde yayınlanmalarının, olay tarihinde kişilik haklarına karşı bir saldırı veya ihlal içermediği, bu hâliyle ifade ve basın özgürlüğü kapsamında değerlendirilebileceği, başvuranların beraat etmeleri sonucu, aradan geçen dokuz yıl sonra, haberin "güncellik" değerini yitirdiği, dolayısıyla haberin o tarihte "gerçeklik ve doğruluk" kriterlerini karşılamaının artık bir önemi kalmadığı, habere konu olan yargılama sürecinin tüm aşamalarıyla sona ermesiyle birlikte, habere konu olan kişiler için haksızlık içeren durumun, toplum tarafından öğrenilmesinin, geçmişte gerçeklik ve doğruluk payı varmış gibi ifşa edilmesi anlamına gelebileceği, dolayısıyla adı geçen habere istenildiği zaman ulaşılmasının, toplum açısından yanlış algılamaya yol açabileceği, başvuranların beraatle sonuçlanan bir yargı sürecinde gözaltına alınması ve tutuklanması süreçlerine dair haberin basının arşivinde bulunmasının, haberin kamu yararı için gelecekte hatırlanması veya istatistiki açıdan değerlendirilmeye alınması gibi işlevi de taşımadığı, dolayısıyla haberin yayında kalmasının, toplumun ilerlemesi, gelişmesi için bir katkı sağlamayacağı gibi, kamu yararına toplum hafızasında yer etmesi gibi bir etkisi de olmadığı, haberin içeriğini oluşturan kişilerin; toplumu temsil ve topluma hizmet etme gayesiyle seçilmiş veya atanmış siyasilerden olmadığı gibi, topluma kendini anlatma ve toplumu aydınlatma gayesiyle eser veren sanatçılardan veya aydınlardan da olmaması nedeniyle, suç geçmişlerine dair bilgilerin kamuyu ilgilendirmediği, ayrıca bu bilgilerin sadece devletin belirli organlarınca kayıt altında tutulabileceğinin, başvuranların isimlerinin ad ve soyadı şeklinde açıkça yazılması suretiyle "örgüt, fuhuş ve insan ticareti" gibi kelimelerin yanında anılmaya devam etmesinin, şeref ve haysiyetlerine karşı bir eylem olduğu gibi, bu nedenle gözaltına alındıkları bilgisinin arşivlenmesinin kişisel

verilerin izinsiz olarak işlenmesi ve yayınlanması anlamına geleceği, yukarıda yer alan değerlendirmeler karşısında, başvuranların istememesine rağmen, geçmişlerinde yer eden olumsuz tecrübelerle dair haberlere, toplum tarafından istenen her anda kolaylıkla ulaşılmamasının başvuranların kişilik haklarını zedelediği, sonuç ve kanaatine varıldığından ..." şeklindeki açıklamalar da nazara alındığında, ilgili haber içeriğinde yer alan haberin basın özgürlüğü kapsamında değerlendirilemeyeceği, başvurucunun unutulma hakkının bulunduğu, anılan haber ve paylaşımlarla ilgili yapılan yargılama neticesinde de beraat kararı verildiği, haberin güncellik değerini kaybettiği, bu nedenle haber içeriğinin ve paylaşımların kişilik haklarını zedelediği anlaşılmalı, itirazın kabulü yerine yazılı şekilde reddine karar verilmesinde isabet görülmediği gerekçesiyle 5271 sayılı Ceza Muhakemesi Kanununun 309. maddesi uyarınca anılan kararın kanun yararına bozulması isteminde bulunulmakla,

Gereği görüşülüp düşünüldü:

Kanun yararına bozmaya konu edilen karara konu uyuşmazlığın çözümü için öncelikle incelemenin kapsamı ve sınırlarının belirlenmesi, bu kapsamda kişilik hakları, ifade ve basın özgürlüğü, kişisel veriler bağlamında unutulma hakkı ve 5651 sayılı Kanun'un 9. maddesi uyarınca kişilik haklarının ihlali sebebiyle erişimin engellenmesi tedbirinin uygulanma şartlarının açıklanması ile somut uyuşmazlığın bu yönlerden hukuki boyutlarıyla değerlendirilmesi gerekmektedir.

A-) İNCELEMENİN KAPSAMI VE SINIRI

Yargıtay Cumhuriyet Başsavcılığınca kanun yararına bozulması istenen karar; başvuranın erişime engellenmesini istediği toplamda (53) adet URL sitesinde yapılan haber içeriğine dair yapılan başvurunun reddine dair karara yönelik itirazın reddi (merci) kararıdır. Ancak, kanun yararına bozma talebine konu edilen internet yayınları; başvuranın dilekçesinde belirttiği ve fakat dosya içerisinde tamamı bulunmayan (53) adet URL adresinden sadece (3)'ünde (<https://ilerihaber.org/içerik/11-108331.html>, <https://www.birgün.net/haber/283235> ve <https://www.krttv.com.tr/gündem-h24257.html> uzantılı URL adresleri) yer alan haberlerdir. Bu nedenle, Dairemizce yapılacak incelemenin sınırı; başvuran ve kanun yararına bozma talep eden kişi hakkında, sadece "<https://ilerihaber.org/içerik/11-108331.html>, <https://www.Birgün.net/haber/283235> ve <https://www.krttv.com.tr/gündem-h24257.html>" uzantılı (3) internet sitesinde yapılan haber içeriklerindeki bilgi ve paylaşımlardır. Dolayısıyla bozulması istenen kararın sadece bu haberler yönünden hukuka uygun olup olmadığı değerlendirilecektir.

Yargıtay Cumhuriyet Başsavcılığının kanun yararına bozma ihbarnamesinde; başvuran hakkında yukarıda adı geçen (3) adet internet sitesinde yer alan haberlerin "basın özgürlüğü" kapsamında

değerlendirilemeyeceği, böyle olduğu kabul edilse dahi, başvuranın geçmişine yönelik ceza yargılamasında, hakaret suçundan mahkumiyetine, diğer suçlardan ise beraatine karar verilmiş olması nedeniyle, haberin "unutulma hakkı" kapsamında artık güncelliğini yitirdiği, dolayısıyla bu adreslerdeki yayın içeriklerinin kişilik haklarını zedeler mahiyette olduğu gerekçesiyle erişimin engellenmesine karar verilmesi gerektiği ileri sürülmektedir. Bu nedenle, Dairemizce yapılacak incelemenin kapsamı;

a- İnternet yayını yoluyla yapılan haber içeriğinin kişilik haklarını ihlal edip etmediğinin, ifade ve basın özgürlüğü kapsamında kalıp kalmadığının,

b- Habere konu edilen başvuranın geçmişinde var olan yargılama sürecinin kişisel verilerin korunması bağlamında unutulma hakkı çerçevesinde kalıp kalmadığının,

c- Somut uyuşmazlıkta, yukarıda açıkça yazılı URL adreslerinde başvuran hakkında internet üzerinden yapılan yayın içeriklerine erişimin engellenmesine karar verilmesi için gerekli şartların var olup olmadığının araştırılmasıdır.

B-) BAŞVURUYA KONU SOMUT UYUŞMAZLIK VE BAŞVURU SÜRECİ

Başvuran hakkında, yukarıda URL adresi yazılı olan üç değişik internet haber sitesinde 08.01.2020 tarihinde yayınlanan; "Uluslararası Hukuk Kurultayı'na Abdülhamit Gül ve Mehmet Uçum davet edildi. Ankara Barosuna 'bu yanıştan dönün' çağrısı" ve "Avukatlardan Ankara Barosuna tepki; Hukuk Kurultayı'nda Saray temsilcisi konuşamaz" başlıklı haber içeriklerinde;

Ankara Barosu'nun 2020 yılında düzenlediği 11. Uluslararası Hukuk Kurultayı'nda konuşmacı olarak davet edilen bakan ve hukuk danışmanının yanı sıra (başvuran) ...'nin da konuşmacı olarak davet edildiğine, ancak bu durumun iki hukukçu sivil toplum örgütü tarafından kınandığına, yapılan açıklamaları aktarmak suretiyle yer verilmiştir. Haberde, Ankara Barosu Çağdaş Avukatlar Derneği tarafından yapılan açıklamadaki;

"...hukukun yerini keyfiliğin aldığı böylesine bir dönemde, tüm bu sürecin birinci elden kurucu ve sembolik isimlerinden olan kişilerin baro çatısı altında düzenlenen böylesi bir Kurultay'ın açılış konuşmasını yapmasını kabul edilemez buluyoruz.

Yine aynı Kurultay'da daha önce bir kadın meslektaşımıza yönelik cinsel taciz, özel hayatın gizliliğini ihlal, kişisel verilerin hukuka aykırı yayılması ve hakaret suçlarından cezalandırılmış, farklı platformlarda özellikle kadın avukatlara yönelik saldırılarına tanık olunan ... isimli kişinin sunum yapacak olmasını da kabul edilemez buluyoruz. Kadına yönelik şiddetin bizzat faili konumundaki bir kişiye İnsan Hakları ana temalı bir kurultayda yer verilmesinin bir amacı olamaz. Ne söylendiği

kadar kimlerle birlikte yan yana durulduğunun da aynı derecede önemli olduğu akıldan çıkarılmamalıdır..." ifadeleriyle,

Demokrasi İçin Hukukçular platformunun Ankara Barosu'na yazdığı yazıda yer alan;

"...Ankara Barosu'nu bu önemli kurultaya gölge düşürecek söz konusu isimleri açılış konuşması programından çıkarmaya davet ediyoruz...

..., özellikle kadına yönelik şiddet başta olmak üzere, pekçok kişisel hak ihlali ile tanınan bir kişi olduğundan Kurultay programında tebliğ sunumcusu olarak yer almasının vahim bir hata olduğuna dikkat çekmek istiyoruz.

..., 2015 yılında Avukatlar Sendikası yöneticisi kadın meslektaşımıza yönelik olarak, hukukçulardan oluşan bir Facebook grubunda, sendika ilanıyla ilgili olarak 'güzelmiş bu sendika, bekar ve niyeti ciddi arkadaşlar behemehal üye olsun diyorum; üyelik şartlarınızı açıklar mısınız, bekar avukatlara kota var mı' şeklindeki cinsel taciz içeren sözler sarf etmiştir. Yine meslektaşımızın kişisel sayfasındaki çeşitli fotoğraflarını izinsiz olarak ve sosyal taciz amacıyla bir sosyal paylaşım sitesine koymuş; bu saldırıları nedeniyle İstanbul 5. Aile Mahkemesinden 6284 s. yasa kapsamında tedbir kararı uygulanmış ve ayrıca İstanbul Anadolu 42. Asliye Ceza Mahkemesi tarafından mahkumiyet kararı verilmiştir. Bu taciz ve kişisel haklara saldırı içeren uygulamalar çeşitli gazete haberlerine konu olmuş; yargı sendikaları, hukuk kurumları ve bazı sendikal örgütler tarafından 24.03.2015 tarihli basın açıklamasıyla da kınanmıştır.

Ayrıca, ilgili kişinin bu ve benzer hareketleri nedeniyle YÖK disiplin kurulu tarafından disiplin cezası uygulandığı, yine kadına ve çocuğa yönelik şiddetle ilgili vahim isnatlarla devam eden yargılamalarının bulunduğu, Av. Sedef ÜNAL tarafından baronuza bildirilmiştir.

Kurultay konuşmacılarının bir kısmının Kurultay Yönergesi uyarınca, "kör hakem" yöntemi ile belirlenmesi gerekçesiyle, bu kişinin programda yer alması kabul edilemez. Bu yaklaşımın, şiddet faili erkeğin kravat takarak mahkemede iyi hal indirimi almasından farkı var mıdır? Anayasal ve yasal görevi itibarıyla de insan hak ve özgürlükleri için mücadele etmesi gereken Baroların, bir kadına şiddet failini sunumcu olarak yüceltmesi etik olarak kabul edilemez. Aynı saatlerde Muammer Aksoy salonundaki 'toplumsal cinsiyet ve temel haklar' başlıklı oturumla açıkça çelişkiye düşen Ankara Barosunu ve bilim kurulunu, korumak ve uygulanmasını sağlamakla yükümlü olduğu İstanbul Sözleşmesi ve 6284 s. yasanın da gereği olarak, kadına yönelik şiddet faili bu kişiyi Kurultay Programından çıkarmaya davet ediyoruz." şeklindeki ifadelerin tamamı haberde aynen aktarılmıştır.

Başvuran vekili, 15.01.2020 tarihli dilekçesinde (özetle); müvekkilinin halen bir devlet üniversitesinde ana bilim dalı başkanı öğretim üyesi olarak görev yaptığını, 2020 yılı Ankara Barosu Uluslararası Hukuk Kurultayı'na konuşmacı olarak davet edildiğini, ancak bir takım aşırı sol ideolojiye sahip örgütlerle LGBT birlikleri tarafından kendisi hakkında sanal ortamda karalama kampanyası başlatıldığını, internette müvekkili hakkında yer alan taciz, kişisel verilerin izinsiz kaydedilmesi veya hakaret yönündeki haberlerin tümünün yalan ve kötüniyetli paylaşımlar olduğunu, müvekkilinin uydurma ve iftira nitelikli tüm dosyalardan beraat ettiğini ve bunların Yargıtay tarafından da onandığını belirterek, kişilik haklarını ihlal eden boyuttaki (53) adet değişik URL adresinde yer alan yayınlara erişimin engellenmesini talep etmiştir.

Ankara 3. Sulh Ceza Hakimliğince 15.01.2020 tarihinde verilen kararda; internet haber sitelerinde başvuran hakkında yapılan yayınların kişilik haklarını ihlal edip etmediğinin tespiti için 5651 sayılı Kanun'da yer alan 24 saatlik karar verme süresi içinde, haberlerde yer alan bilgilerin doğru olup olmadığının veya kişilik haklarını ihlal edip etmediğinin araştırılması amacıyla bilgi ve belgelere ulaşılmasının imkansız olduğu, öte yandan internetteki yayınları erişime engellenmesi talep edilen tarafların da çekişmeli yargı ilkesinin bir sonucu olarak savunma hakkı yönünden dinlenilmesi gerektiği, aksi halde gözetilmesi gereken dengenin bozulacağı, kişilik haklarına saldırının veya hukuka aykırılığın ancak ilk bakışta anlaşılacak kadar belirgin olması halinde talebin kabulüne karar verilebileceği, nitekim Anayasa Mahkemesinin 2014/5552 sayılı başvuru hakkında verdiği 26.10.2017 tarihli kararında da bu hususa işaret edildiğinden bahisle; talebe konu haberlerin, ilk bakışta çekişmesiz bir dava yoluyla erişimin engellenmesi talebi uygulanmasını gerektirecek nitelikte ağır ve kişilik haklarını ihlal edici nitelikte olmadığı görülmekle talebin reddine karar verilmiştir.

Başvuran tarafından sunulan itiraz dilekçesinde (özetle), erişime engellenmesi talep edilen internet yayınlarında kişilik haklarının açıkça ihlal edildiği, verilen kararın kopyala - yapıştır şeklinde oluşturulan ve gerekçesiz bir karar olduğu, haberlerin gerçek dışı ve mesnetsiz olduğu, bazı sosyal paylaşım sitelerinde bu karalama kampanyasının hakaret ve sövme mahiyetinde suçlara dönüştüğü ve 5651 sayılı Kanun'un 9. maddesinin acele bir şekilde uygulanmasının gerektiği, atıfta bulunulan Anayasa Mahkemesinin kararının bir bireysel başvuru kararı olduğu emsal mahiyetinde somut olaya uygulanamayacağı ve beraat kararı onanmamış olsa bile bu kez de unutulma hakkı gereği yayınların erişime engellenmesi gerekeceği dile getirilerek kararın kaldırılması istenmiştir.

İtiraz üzerine karar veren Ankara 4. Sulh Ceza Hakimliğinin 21.01.2020 tarihli kararında ise; verilen kararın gerekçesinde hukuka aykırılık bulunmadığından itirazın reddine karar verildiği görülmektedir.

C-) İNCELEME VE DEĞERLENDİRME

1-) Kişilik Hakları ile İfade ve Basın Özgürlüğüne Yönelik İncelemede;

Suç tarihinde yürürlükte bulunan 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"un "içeriğin yayından çıkarılması ve erişimin engellenmesi" başlıklı 9. maddesinin uygulanma şartları;

- İnternet ortamında yapılan bir yayın olması,

- Yapılan yayın içeriği nedeniyle, gerçek ve tüzel kişiler ile kurum ve kuruluşların "kişilik haklarının" ihlal edilmesidir.

Dairemizin 02.11.2020 tarihli, 2019/29863 E. 2020/13554 K. sayılı kararında da belirtildiği üzere;

"5651 sayılı Kanun'un 9. maddesinde; kişilik hakkı ihlal edilenlerin "erişimin engellenmesi" taleplerini içerik veya yer sağlayıcısından yada bu hususta karar almaya görevli ve yetkili Sulh Ceza Hakimliğinden doğrudan isteyebileceği, bu hususta verilecek kararların mahkemece erişim sağlayıcıları birliğine gönderilerek derhal yerine getirilmesi, erişimin engellenmesine konu içeriğin yayından kaldırılması halinde hakim kararlarının da kendiliğinden ortadan kalkacağı ve kararların yerine getirilmemesi halinde uygulanacak ceza yaptırımları düzenlenmektedir.

İnternet içeriğine erişimin engellenmesi tedbiri, başvuranın kişilik haklarını ihlal ettiği mahkeme kararıyla tespit edilen bir internet yayınına toplumun erişiminin derhal engellenmesi amacıyla düzenlenmiş bir tedbirdir. Erişimin engellenmesi tedbirinin uygulanması için yayının içeriğinde kişilik hakkına yönelen bir suç unsuru bulunması şartı aranmadığı gibi yayın içeriğinde bir suç işlenmişse dahi yürütülecek ceza muhakemesinin sonucu beklenmeksizin erişimin engellenmesi tedbirine bir koruma tedbiri olarak hükmedilebilecektir. Erişimin engellenmesine konu edilen ve başvuranın kişilik hakkını ihlal ettiği tespit edilen internet yayınının "bir an önce" internet ortamından kaldırılması, gerek kişilik haklarının gerekse kamu düzeninin korunması açısından elzemdir. Ancak verilecek kararlarda ifade ve basın özgürlüğünün zedelenmemesi de gözetilmesi gereken bir diğer husustur.

Kişilik Hakları; özel hukukta kişinin doğumla birlikte kazandığı ve üzerine kişisel gelişimiyle birlikte her geçen gün yeni değerler kattığı kişiliğinin, maddi ve manevi bütünlüğünün, isminin, mesleki kariyerinin, ailesinin ve hatta sosyal çevresinin kişi üzerinde oluşturduğu, kısacası kendini gerçekleştirme yolunda elde ettiği tüm kazanımlarının ve menfaatlerinin, hukuk düzeni tarafından koruma altına alınan yönüdür. Medeni hukuk kapsamında kişilik hakları, kategorik anlamda mutlak

haklar içinde yer alan, her zaman varolan, zamanla tükenmeyen, herkese karşı ileri sürülebilen, çoğu zaman kişiye sıkı sıkıya bağlı ve devredilemeyen haklardandır.

İfade özgürlüğü; insanın dilediği şekil, zaman ve koşulda, herhangi bir baskı, sınırlama veya zorlama altında kalmadan bilgi ve fikir sahibi olma, özgürce düşünme, düşüncelerini baskı altında kalmadan açıklama, muhatabına iletme ve yayma imkanının elinde bulunmasıdır.

O halde ifade özgürlüğünün temel unsurları;

- Bilgiye, yorum ve değerlendirmelere, mesaj veya habere özgürce erişebilme,
- Herhangi bir sınırlama, baskı veya yönlendirme olmaksızın özgürce kanaat ve fikir sahibi olma,
- Sahip olunan düşünce ve kanaati özgürce açıklayabilme ve yayma imkanının bulunması olarak sayılabilir.

Basın Özgürlüğü; ifade özgürlüğünün ayrılmaz bir parçası olmak üzere, insanların bilgiye ulaşma ve fikir elde edebilme yönündeki en önemli araçlardan olan basın, yazılı, görsel veya işitsel araçlarla sunduğu ve kamu hizmetini gerçekleştirme yolunda sahip olduğu özgürlüktür. Basın özgürlüğü; basının, başkalarından gelebilecek her türlü müdahaleye ve baskıya karşı sırf toplumu aydınlatmak amacıyla gerçekleştirdiği faaliyetleri sırasında öngörülemeyen bir takım olumsuz durumlarla karşılaşma veya haksız bir yaptırımla cezalandırılma endişesi duymadan, özgürce görevini yerine getirebilmesi demektir.

Hemen her temel hak ve özgürlük için olduğu gibi ifade özgürlüğünün de sınırlanması açısından genel bir takım kriterlerin her somut olayda ayrı ayrı gerçekleşip gerçekleşmediğinin tespit edilmesi gerekmektedir. Bir temel hak ve özgürlüğün sınırlandırılması için gözetilmesi gereken kriterler;

- Sınırlamanın kanunla yapılması (yasal bir dayanağı olması),
- Sınırlamanın meşru bir amaca hizmet etmesi (AİHS'de veya iç hukukta yer alan sınırlama sebeplerinin varlığı),
- Sınırlamanın demokratik toplum gereklerine uygun olması (demokratik ve bilinçli bir toplumda yapılacak sınırlamanın normal görülmesi ve saygıyla karşılanması)
- Sınırlamanın ölçülü olmasıdır.

Meşru amaç deyiminden; genellikle sözleşmenin 10/2. maddesinde yazılı kamu güvenliği, toplumsal ahlak ve ülkelerin yasalarında mevcut sair durumlar kastedilmektedir.

Çağdaş demokratik toplumun gerekleri tanımı ile anlatılmaya çalışılan ise; topluma sunulan, sınırlanmaması, kınanmaması, özgür bırakılması gereken ifadenin veya haberin; toplumun ilgisini çeken, güncel ve kamunun yararını güden bir tartışmayı içermesi ile halkı kin ve düşmanığa sevketmemesi, şiddete teşvik etmemesi, nefret veya ayrımcılık içermemesi, suçu ve suçluyu övmemesi, terör veya ayrılıkçı hareketleri övmemesi, meşrulaştırıp yüceltmemesi, başkalarının kişilik haklarını, onur, şeref ve saygınlığını, hakaret, sövme veya benzer yollarla zedelememesi gibi gerekliliklerdir. Her ne kadar doktrinde bu konuda üye devletlerin aynı ölçüleri benimsemeleri gerektiği kabul edilmekte ise de; değer yargıları ülkeden ülkeye değişmektedir. Çağdaş ülkelerin çoğunda; iftira, onur, şeref ve saygınlığı zedeleyici söz ve beyanlar, müstehcen içerikli söz, yazı, resim ve açıklamalar, savaş kışkırtıcılığı, hukuk düzenini cebir yoluyla değiştirmeye yönelen, nefret, ayrımcılık, düşmanlık ve şiddet yaratmaya yönelik olan ifadeler düşünce özgürlüğü kapsamında değerlendirilmemekte, suç sayılmak suretiyle cezalandırılmaktadırlar.

Temel hak ve özgürlükler arasında düşünce ve kanaat açıklama özgürlüğünün önemli bir yeri bulunmaktadır. Bu özgürlüğün kullanılabilmesinin en önemli ve etkin yollarından birisi basındır. Basın özgürlüğü; bilgi edinme, yayma, eleştirme, yorumlama ve eser yaratma haklarını içerir. Düşünceyi açıklama ve basın özgürlüğü, onu kullananlar açısından olduğu kadar gerçekleri öğrenmek özgürlüğüne sahip kişi ve kitleler açısından da temel hak niteliğindedir (Centro Europa 7 S.R.L. ve Di Stefano, § 131). Böylelikle, basın özgürlüğü bir yönüyle halkı ilgilendiren haber ve görüşleri iletme özgürlüğüdür, diğer yönüyle ise bu özgürlük, halkın bu bilgi ve görüşleri alma hakkıdır. Bu şekilde basın kamuoyunun bilgi edinme hakkı bakımından birincil derecede önemi bulunan “halkın gözcülüğü” ya da “kamunun (kamu düzeninin) bekçisi” görevini yapabilir.

Çoğunlukçu, özgürlükçü, demokratik toplumlarda, düşünceyi açıklama özgürlüğü; sadece genel kabul gören ve zararsız veya önemsiz sayılan düşünceler yönünden değil, aynı zamanda halkın bir kısmı tarafından benimsenmeyen kural dışı, hatta rahatsız edici, endişe verici, sarsıcı düşünceler için de geçerlidir.

Toplumun ve insanlığın sorunları konusunda bireyi bilinçlendirmek, doğru ve gerçeğe uygun bilgiler ile donatmak, yaşanan sorun, olay ve oluşumlar hakkında kamuoyunu nesnel bir biçimde aydınlatmak, düşünmeye yönlendirici tartışmalar açmak, yöneticileri eleştirmek, uyarmak ve bu suretle denetlemek durumunda olan basının sahip olduğu hakkı hukuka uygun bir biçimde kullandığının kabulü için; açıklama, eleştiri ve değer yargısı biçimindeki bilginin gerçek ve güncel olması, açıklanmasında kamunun ilgi ve yararının bulunması, açıklanış şekli ile konusu arasında düşünsel bağ bulunması, açıklamada küçültücü sözlerin kullanılmaması gerekmektedir. Ancak,

basın özgürlüğünün bir dereceye kadar abartma hatta kışkırtmaya başvurma hakkını da içerdiği unutulmamalıdır.

Basın ve diğer medya organlarının ifade özgürlüğü, kamuoyuna yöneticilerin görüş ve davranışlarını tanıtmak ve yargılamak için en iyi araçlardan birisini sunmaktadır. Şüphesiz ifade özgürlüğünü kullanan kişilerin (gazeteciler vb...) bu özgürlüğü kullanırken “görev ve sorumlulukları” da vardır. Sözleşme'nin 10. maddesinin gazetecilere tanıdığı güvence, gazetecilerin gazeteci deontolojisine saygı içinde “doğru ve güvenilir” bilgiler sunmaları anlamında iyi niyetle hareket etmeleri koşuluna bağlıdır (Goodwin, § 39; Mc Vicar, § 83-86; Colombani, § 65).

Basın özgürlüğü ile kişilik değerlerinin karşı karşıya geldiği durumlarda; hukuk düzeninin çatışan iki değeri aynı zamanda koruma altına alması düşünülemez. Bu iki değerden birinin diğerine üstün tutulması gerektiği, bunun sonucunda da, daha az üstün olan yararın daha çok üstün tutulması gereken yarar karşısında o olayda ve o an için korumasız kalmasının mümkün olduğu kabul edilebilecektir. Bunun için temel ölçüt kamu yararıdır. Gerek yazılı ve gerekse görsel basın bu işlevini yerine getirirken, özellikle yayının gerçek olmasını, kamu yararı bulunmasını, toplumsal ilginin varlığını, konunun güncelliğini gözetmeli, haberi verirken öze biçim arasındaki dengeyi de korumalıdır. Yine basın, objektif sınırlar içinde kalmak suretiyle yayın yapmalıdır. O anda ve görünürde var olup da sonradan gerçek olmadığı anlaşılan olayların yayınından da basın sorumlu tutulmamalıdır.

AİHS'nin 10. maddesinde bir temel hak ve özgürlük olarak kabul edilen ifade özgürlüğünün de sınırsız olmadığı, objektif olarak belirlenmiş istisnai durumlarda sınırlanabileceği öngörülmüştür. AİHS'nin 10/2. maddesinde yer alan ifade özgürlüğünün sınırlama sebepleri;

- Ulusal güvenliğin, toprak bütünlüğünün veya kamu güvenliğinin korunması,
- Kamu düzeninin sağlanması ve suç işlenmesinin engellenmesi,
- Sağlığın veya ahlakın, başkalarının şöhret ve haklarının korunması,
- Gizli bilgilerin yayılmasının önlenmesi veya yargı erkinin yetki ve tarafsızlığının güvence altına alınması, olarak sayılmıştır.

Kanun yararına bozmaya konu uyumsuzluk bakımından; sınırlanması istenen ifadenin başkalarının şöhret ve haklarını ihlal etmeyecek derecede saygıdeğer olması gerektiği, aksi halde sınırlandırılmasının kaçınılmaz olduğu değerlendirilmektedir.

AIHM, Axel Springer & Almanya kararında, ifade özgürlüğü ile kişilerin özel hayatlarının korunması ve mahremiyet hakkının karşı karşıya geldiği durumlarda, sınırlamanın sözleşmeye uygun olup olmadığının tespiti bakımından aşağıdaki kriterlerin birlikte değerlendirilmesi gerektiğini öngörmektedir;

- İfadenin genel kamu yararını güden bir tartışmaya katkıda bulunması,
- İfadede sözü edilen kişinin tanınmışlık derecesi ve aktarılan konu,
- İfadede adı geçen kişinin daha önceki davranışları,
- İfadeye konu olan bilgiyi elde etmek için kullanılan yöntem,
- İfadede aktarılan bilginin doğruluğu, içeriği, biçimi ve etkileri,
- İfadenin sınırlanması için uygulanan yaptırımın türü, miktarı, ölçülü şekilde kullanılıp kullanılmadığı.

Basın yoluyla işlenen suçlar nedeniyle görülen davalarda göz önünde bulundurulması gereken "basın özgürlüğü" kavramının içeriği ve hukuka uygunluk nedenlerine dair Yargıtay Ceza Genel Kurulunun 13.02.2007 tarihli, 2007/7-28 E. - 2007/34 K. sayılı kararında;

"...Demokratik toplumlar, temel hak ve özgürlüklere dayanan toplumlardır. Bu tür toplumlarda Devletin görevi, temel hak ve özgürlükleri korumak ve geliştirmektir. Temel hak ve özgürlükler arasında düşünce ve kanaati açıklama özgürlüğünün önemli bir yeri bulunmaktadır. Bu özgürlüğün kullanılabilmesinin en önemli yollarından birisi de basındır.

Geneli ilgilendiren ya da ilgilendirmesi gereken tüm olaylar hakkında, halkı objektif ve gerçekleri yansıtabilecek biçimde aydınlatmak, çeşitli sorunlar üzerinde kamuoyunu düşünmeye çağırarak tartışmalar açmak, onu toplumsal ve siyasal oluşumlar üzerinde doğru ve gerçeğe uygun bilgilerle donatmak, yöneticileri eleştirmek, uyarmak ve bu yöntemlerle denetlemek, ayrıca içinde yaşadığı toplumun ve tüm insanlığın sorunları konusunda bireyi bilinçlendirmek durumunda olan basına, bu ödevlerini yerine getirirken ihtiyaç duyacağı bir kısım haklar da tanınmıştır. Bunlar; bilgi edinme, yayma, eleştirme, yorumlama ve eser yaratma haklarıdır.

Temelini Anayasa'nın 28. vd. maddelerinden alan ve 5187 sayılı Basın Yasasının 3. maddesinde düzenlenen bu haklar, basın yoluyla işlenen suçlarda, hukuka uygunluk nedenlerini oluşturur. Bilgiyi yayma, eleştirme ve yorumlama haklarının kabulü için, açıklama, eleştiri veya değer yargısı biçimindeki bilginin gerçek ve güncel olması, açıklanmasında kamunun ilgi ve yararının bulunması,

açıklanış şekli ile konusu arasında düşünsel bir bağ bulunması, açıklamada "küçültücü" sözlerin kullanılmaması gerekir...

...Haber verme hakkının hukuka uygun bir biçimde kullanılabilmesi için gereken ölçütler dört başlık altında toplanmaktadır.

Bunlar;

- 1- Haber gerçek olmalı,
- 2- Haber güncel olmalı,
- 3- Haberin verilmesinde kamu yararı bulunmalı,
- 4- Haberin veriliş biçimi ile özü arasında düşünsel bir bağ bulunmalıdır.

Bu unsurlar eleştiri hakkı yönünden de geçerlidir. Yani eleştirinin olabilmesi için, yazının gerçek olgulara dayanması, güncel bulunması ve bu haberin verilmesinde kamu yararı bulunması koşullarına bağlıdır..." şeklinde gözetilmesi gereken temel kriterlerden bahsedilmiştir.

Yukarıdaki açıklamalar çerçevesinde kanun yararına bozmaya konu somut uyuşmazlığın "ifade ve basın özgürlüğü" yönünden değerlendirilmesine gelince;

Değişik internet sitelerinde, Ankara Barosu'nun düzenlediği 11. Uluslararası Hukuk Kurultayı'nı konu edinen 08.01.2020 tarihli haberlerde;

- Haberin başlığında ve genelinde, adı geçen Kurultay'a konuşmacı olarak davet edilen isimlere ilişkin yorum, eleştiri ve sivil toplum kuruluşlarının açıklamalarına yer verildiği, dolayısıyla haberin genel kamu yararını güden tartışmaya katkı sunmayı amaçladığı,

- Haberde adı geçen başvuranın, ceza hukuku alanında önemli bir hukukçu olduğu, Kurultay'a konuşmacı ve bir kamu görevlisi olarak katılacağına aktarıldığı, habere konu kişinin habere ilgi gösteren kitlece tanınmış olduğu ve konuşma yapacağı konu (devlet suçluluğu, insan hakları ve ceza hukuku) ile çelişecek şekilde, hakkında açılan bir ceza davasında mahkumiyet aldığına dolaylı bir anlatımla kamuya iletildiği,

- Başvuranın habere konu kurultaydan önce meslektaşı olan bir avukata karşı sarf ettiği ifadeler ve yaptığı internet paylaşımları nedeniyle mahkumiyetine karar verildiği,

- İnternet üzerinde herkesin erişimine açık bulunan haber sitelerinde verilen bilgiyi elde etmek için kullanılan yöntemin, çok hızlı, etkili ve kolay bir habere ulaşma yöntemi olduğu, haberin yayımlandığı tarihin (08.01.2020) ise; başvuran konuşmacının davet edildiği Kurultay tarihinden (9-

12 Ocak 2020) hemen önce ve konuşmanın yapılmasından iki gün önce olduğu, dolayısıyla haberin zamanlamasının da gözetilen kamu yararı amacına yönelik olduğu,

- Başvuranın, bir avukat meslektaşına karşı internet üzerinde yaptığı paylaşımları nedeniyle açılan kamu davasında; hakaret suçundan adli para cezasına mahkum edildiği; cinsel taciz, özel hayatın gizliliğini ihlal ve kişisel verileri hukuka aykırı olarak kaydetmek suçlarından beraatine hükmedildiği, Yargıtay 12. Ceza Dairesinin 16.01.2019 tarihli kararıyla bu hükümlerin onandığı, ancak Yargıtay Cumhuriyet Başsavcılığınca yapılan itiraz üzerine, 12. Ceza Dairesinin 23.12.2019 tarihli, 2019/5024 E. 2019/12115 K. sayılı kararıyla "özel hayatın gizliliğini ihlal ve kişisel verilerin kaydedilmesi suçundan" verilen beraat - onama kararının kaldırılarak, başvuran hakkında özel hayatın gizliliğini ihlal ile kişisel verilerin hukuka aykırı olarak kaydedilmesi suçundan açılan kamu davasının bir bütün halinde "verileri hukuka aykırı olarak verme veya ele geçirme" suçunu oluşturduğu gerekçesiyle mahkumiyetine karar verilmesi gerekirken beraatine karar verildiğinden bahisle kararın bozulmasına karar verildiği, haberde tamamıyla gerçek dışı bilgilere yer verilmediği, atılı suçlamalardan cinsel taciz iddiası hakkında ise; haberin başvuran hakkında kamu davası açıldığına dair olgusal bir (somut) temeli olduğu, bu bilginin hukukçulardan oluşan sivil toplum örgütlerinin açıklamalarına dayanarak aynen aktarıldığı, dolayısıyla basın organının dayanağını göstererek toplumu bilgilendirmeye çalıştığı, gerçekleri bir dereceye kadar abartma hatta kışkırtma yoluna başvurarak duyurması sırasında; temelsiz, maksatlı veya kötüniyetli bir şekilde olayları çarpıttığına dair emare bulunmadığı,

- Başvuranın kişilik haklarını ihlal ettiği iddiasıyla erişimin engellenmesini istediği haberde, başvuranın geçmişine dair yer alan ifadelerin, haberin tümünü değil, sadece %30'a yakın bir kısmını oluşturduğu, dolayısıyla ifadenin sınırlanması için kullanılan haberin tümünün erişime engellenmesi yönündeki talebin ve istenen tedbirin kabulünün, ifadenin miktarı ve tedbirin ölçülülüğü bakımından da ağır olacağı,

- Sonuç olarak; Ankara Barosu Uluslararası Hukuk Kurultayı'nda konuşmacılardan duyulan rahatsızlığın dile getirildiği sivil toplum örgütlerinin açıklamalarına dair yapılan haberlerin; o tarihte güncelliğini koruyan, gerçek bilgilere dayalı, eleştiri ve yorum içeren ifadelerden oluştuğu, haberin veriliş biçimi ile özü arasında düşünsel bağın koparılmadığı, doğrudan ve sadece başvuranın kişilik haklarını hedef almayı amaçlamadığı, başvuran hakkında kamuoyunun ilgisini ve genel kamu yararını güden bir tartışmaya katkı sunduğu değerlendirilmekle, basın özgürlüğünün sınırları içinde kaldığı kanaatine varılmıştır.

2-) Kişisel Verilerin Korunması ve Unutulma Hakkına Yönelik İncelemede;

T.C. Anayasasının "Özel hayatın gizliliği ve korunması" başlık ve "Özel hayatın gizliliği" alt başlıklı 20. maddesi;

"... Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.

(Ek fıkra: 7/5/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir..." hükmünü içermektedir.

Dairemizin 02.11.2020 tarihli, 2019/28161 E. 2020/13552 K. sayılı kararında da belirtildiği üzere;

Kişisel Veri; 07.04.2016 tarihinde yürürlüğe giren Kişisel Verilerin Korunması Kanunu'nun 3. maddesinde "...Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi..." şeklinde tanımlanmıştır.

6698 sayılı Kanun'un ilgili madde gerekçesinde; "...Kişisel veriler, sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin aklî, psikolojik, fizikî, kültürel, ekonomik, sosyal ve sair özelliklerine ilişkin verilerdir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi

veriler dolaylı da olsa kişiyi belirlenebilir kılabılme özellikleri nedeniyle kişisel verilerdir" açıklamasına yer verilmiştir.

Öğretide de kişisel veri kavramı; "...Bireyin şahsi, mesleki ve ailevi özelliklerini gösteren, o bireyi diğer bireylerden ayırmaya ve niteliklerini ortaya koymaya elverişli hertürlü bilgiyi ifade eder..."(Ersan Şen, Türk Ceza Kanunu Yorumu, Vedat Kitapçılık, İstanbul, 2006, s.601), "...Bir kişinin adı ve soyadı, yaşı, cinsiyeti, doğum yeri, dini, TC kimlik numarası, cinsel hayatı, cep telefonu numarası, medeni durumu, ailesi, işi, geliri, borçları, adresi, geçirdiği hastalıklar, özel zevkleri ve buna benzer bilgileridir..." (Volkan Sırabaşı, İnternet ve Radyo- Televizyon Aracılığıyla Kişilik Haklarına Tecavüz, Adalet Yayınevi, Ankara, 2007, 2. Bası, s.195) şeklinde tanımlar yapılmıştır.

Dairemizin, başta 2016/15510 E. 2017/5325 K. sayılı kararında ve pek çok emsal kararında da gerekçeleri belirtildiği üzere;

Unutulma hakkı, Anayasa'mızda veya Kanunlarda açıkça düzenlenmiş bir hak değildir. Bununla birlikte Anayasa'nın "Devletin temel amaç ve ödevleri" başlığı altında düzenlenen 5. maddesinde "insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak" ifadesi ile devlete pozitif bir yükümlülük yüklenmiştir. Bu yükümlülük bağlamında Anayasa'nın 17. maddesinde düzenlenen kişinin manevi bütünlüğü kapsamında değerlendirilen şeref ve itibarının korunması hakkı ve Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı ile birlikte düşünüldüğünde, devletin; bireye -geçmişte yaşadıklarının başkaları tarafından öğrenilmesinin engellenerek "yeni bir sayfa açma" olanağı vermesi- yönünde bir sorumluluğu olduğu açıktır. Özellikle kişisel verilerin korunması hakkı kapsamında kişisel verilerin silinmesini talep edebilme hakkı, kişilerin geçmişlerinde yaşadıkları olumsuzlukların unutulmasına imkân tanımayı kapsamaktadır. Dolayısıyla Anayasa'da açıkça düzenlenmeyen unutulma hakkı, İnternet vasıtasıyla ulaşılması kolay olan ve dijital hafızada bulunan haberlere erişiminin engellenmesi için Anayasa'nın 5., 17. ve 20. maddelerinin doğal bir sonucu olarak karşımıza çıkmaktadır. Diğer taraftan unutulma hakkının kabul edilmemesi, İnternet vasıtasıyla kolayca ulaşılabilir ve uzun süre muhafaza edilebilir kişisel veriler nedeniyle başkaları tarafından kişiler hakkında ön yargı oluşturabilmesine yol açması nedeniyle, kişinin manevi varlığının geliştirilmesi için gerekli olan onurlu bir yaşam sürdürmesine ve manevi bağımsızlığına müdahaleyi sürekli kılabilecektir.

Yargıtay Ceza Genel Kurulu'nun 17.06.2014 tarihli, 2012/12-1510 E. 2014/331 K. sayılı kararında "kişisel veri" kavramı;

"...Kişilerin, sadece insan olması ve toplumdaki yeri, bazı değerleri kişisel veri haline getirmektedir, örneğin; kişinin adı, adresi, kimlik bilgileri, medeni durumu vb... Bunun yanında teknolojik gelişmeler nedeniyle gittikçe karmaşıklaşan toplum hayatındaki bir takım bilgiler de kişisel veri haline gelmiştir, örneğin; vatandaşlık numarası, banka hesap numarası, telefon numarası, elektronik posta adresi ve şifresi vb... Dolayısıyla farklı gruplandırmalar bulunmakla birlikte kişisel verilerin iki başlık altında toplanması mümkündür. Birinci grupta; insanın varoluşundan kaynaklanan kişiliğine ait bilgiler, ikinci grupta ise; teknolojinin gelişmesiyle insanın modern toplumda yer alması nedeniyle kendisine verilen ya da çeşitli hizmetlere ulaşmasında kullanılan bilgiler yer almaktadır. Ancak her iki grupta yer alan bilgilerin de kişisel veri olarak hukuk düzenindeki değeri ve korunmaları açısından bir fark bulunmamaktadır.(Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayınevi, Ankara, 2014, 4. bası, s.577)

TCK'nin 136. maddesinde tıpkı 135. maddesinde olduğu gibi korunan hukuki değer genel olarak kişilerin özel hayatı ve hayatın gizli alanı, özelde ise kişisel verilerdir. Bu düzenlemeler ile tüm kişisel veriler koruma altına alındığından kişisel verilerin mutlaka gizli olması zorunlu değildir. Gizli olmayan ve herkes tarafından bilinen kişisel veriler de hukuka aykırı eylemlere karşı korunmalıdır. Zira kişisel verilerin korunmasına ilişkin suçlarda korunan hukuki değer "sır" olmayıp, verinin ilgilisi olan kişinin kişilik haklarıdır.(Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayınevi, Ankara, 2014, 4. bası, s.579, 588-593)..." ifadeleriyle kabul edilmiştir.

Yargıtay Hukuk Genel Kurulunun 17/6/2015 tarihli ve E.2014/4-56, K.2015/1679 sayılı kararında ise;

"...Unutulma hakkı ve bununla ilişkili olan gerektiği ölçüde ve en kısa süreliğine kişisel verilerin depolanması veya tutulması konuları, aslında kişisel verilerin korunması hakkının çatısını oluşturmaktadır. Her iki hakkın temelinde bireyin kişisel verileri üzerinde serbestçe tasarruf edebilmesini, geçmişin engeline takılmaksızın geleceğe yönelik plan yapabilmesini, kişisel verilerin kişi aleyhine kullanılmasının engellenmesini sağlamak yatmaktadır. Unutulma hakkı ile geçmişinde kendi iradesi ile veya üçüncü kişinin neden olduğu bir olay nedeni ile kişinin geleceğinin olumsuz bir şekilde etkilenmesinin engellenmesi sağlanmaktadır. Bireyin geçmişinde yaşadığı olumsuz etkilerden kurtularak geleceğini şekillendirebilmesi bireyin yararına olduğu gibi toplumun kalitesinin gelişmişlik seviyesinin yükselmesine etkisi de tartışılmazdır.

Unutulma hakkı; üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerin silinmesini ve yayılmasının önlenmesini isteme hakkı olarak ifade edilebilir..." şeklinde unutulma hakkının kapsamı ve önemi belirtilmiştir.

Anayasa Mahkemesinin ifade ve basın özgürlüğü ile şeref ve itibarın korunması hakkı arasındaki dengelenmesine dair emsal kararlarında; "...Anayasa'nın 17. maddesinin birinci fıkrası temelinde değerlendirme yaptığı gözetilerek unutulma hakkına ilişkin iddiaların İnternet ortamındaki haberlerin kişisel veriler ile arasındaki ilişki dikkate alınarak Anayasa'nın 17. maddesinin birinci fıkrası kapsamında inceleme yapılması gerekmektedir. Anayasa'nın 17. maddesi esas olarak kamu görevlilerinin keyfî müdahalelerine karşı bireyi korumayı amaçlasa da söz konusu madde sadece devletin bu tür müdahalelerde bulunmasından kaçınmasını sağlamayı amaçlamamaktadır. Anayasa'nın 17. maddesinin birinci fıkrasında mündemiç negatif yükümlülüğe, Anayasa'nın 5. maddesi dikkate alınarak bireyin maddi ve manevi varlığına etkin bir saygının sağlanması için gerekli pozitif yükümlülükler eklenebilir. Bu yükümlülükler, kişilerin birbirleri ile olan ilişkilerini de kapsayacak şekilde kişisel itibarının korunmasını isteme hakkına saygının güvence altına alınması amacıyla birtakım tedbirler alınmasını gerektirebilir (Ahmet Çinko ve Erkan Çelik [GK], B. No: 2013/6237, 3/7/2015, § 39). Bu tedbirlere, kişisel itibarın üçüncü kişilerin müdahalelerine karşı korunması hususunda da başvurulabilir.(Kadir Sağdıç, § 40; İlhan Cihaner (2), § 47)..." ifadeleriyle, unutulma hakkı kişilerin manevi varlıklarını geliştirmelerine bir fırsat vermek açısından devletin pozitif yükümlülüğünün bir sonucu olarak kabul edilmiştir.

Anayasa Mahkemesi Genel Kurulunun 2013/5653 bireysel başvuru üzerine 03.03.2016 tarihinde verdiği kararda;

"...Haber ve fikirleri iletmedeki hızı ve bunları saklama süresi ve kapasitesi gözetildiğinde İnternet, geleneksel iletişim araçlarından farklı, küresel olarak bilgiye erişim ve iletişim aracıdır. Dünya çapında milyonlarca kullanıcıya hizmet eden merkezi olmayan bu elektronik iletişim ağı, temel hak ve özgürlüklerin kullanımında farklı bir boyut getirmiştir. Temel hak ve özgürlüklerin kullanımında sağladığı imkânlar aynı zamanda temel hak ve özgürlüklere yönelik farklı müdahale yolları ortaya çıkarmıştır. Özellikle bireylerin özel hayatlarına ve manevi bütünlüklerine yönelik olarak çok ciddi müdahale alanları ortaya çıkmıştır. Bu nedenle geleneksel medyadan farklı olarak İnternet, ortaya çıkardığı riskler açısından farklı bir bakış açısı ile değerlendirilmelidir. Bu bağlamda ilgili hak ve özgürlükler açısından koruma ve ilerleme sağlayabilmek için kaçınılmaz olarak teknolojik gelişmeleri de dikkate alacak farklı bir yaklaşım belirlenmelidir.

İnternet'in yaygınlaşmasından önce kişilerin geçmişlerine ilişkin özel yaşamları zaman içinde kaybolmaktaydı. Bununla birlikte bireylerin geçmişlerinde yaşadıklarına ilişkin herhangi bir kayıt tutulmuşsa da bu kayıtlara ulaşılmasının zorluğu kişilerin geçmişlerinde yaptıkları hatalardan bağımsız olarak yaşamlarını sürdürmelerine imkân tanımaktaydı. Ancak günümüzde basit bir

İnternet araştırması, bireylerin geçmişte yaptıkları ve hatırlamak ve/veya hatırlanılmasını istemedikleri hatalarını kolayca ortaya koymaktadır. Bu bağlamda İnternet ortamı, arşivde kalmış ve sadece araştırmacıların veya meraklıların özel çabası ile tespit edilebilecek haberleri kolaylıkla ulaşılabilir hâle getirmiştir. Haber arşivlerine erişimin kolaylaşması kişiler hakkında yapılan haberin unutulmasına fırsat vermeyen bir sanal ortam meydana getirmiştir. Bu durum İnternet'in yaygınlığı ile birlikte değerlendirildiğinde bireylerin geçmişte yaptıkları ve hatırlanmasını istemedikleri hususların sürekli olarak kişilerin karşısına çıkması ihtimalini kuvvetlendirmiştir.

İnternet'in yaygın kullanımı ile ortaya çıkan bu durum basının İnternet'i etkin olarak kullanmasıyla beraber ifade ve basın özgürlükleri ile şeref ve itibarın korunması arasındaki dengeyi ilkinin lehine bozmuştur. İfade ve basın özgürlüğü ile şeref ve itibarın korunması hakkı, eşit düzeyde koruma gerektiren temel hak ve özgürlüklerdir. Bu nedenle bozulan dengenin her iki temel hak arasında tekrar kurulması zorunluluk olmuştur. İnternet haberciliği ile birlikte unutulmanın zor olduğu günümüzde anılan dengenin tekrar kurulabilmesi şeref ve itibar yönünden bireylerin unutulma hakkının kabul edilmesi ile mümkün olabilir. Bu bağlamda unutulma hakkı adil dengenin kurulması için vazgeçilmez niteliktedir (Avrupa Birliği Adalet Divanı, Google Spain SL, Google Inc/İspanya Kişisel Verilerin Korunması Kurumu, Mario Costeja Gonzales, C-131/12, 13/5/2014)...

...Unutulma hakkının İnternet gazete arşivlerindeki her türlü haber yönünden uygulanmasını beklemek mümkün değildir. Nitekim özellikle basın özgürlüğü temelinde gazete arşivinin araştırmacılar, hukukçular veya tarihçiler için önem taşıyan veriler olduğu açıktır. Bu durumda bir İnternet haberinin unutulma hakkı kapsamında İnternet'ten çıkarılabilmesi için;

- yayının içeriği,
- yayında kaldığı süre,
- güncelliğini yitirme,
- tarihsel bir veri olarak kabul edilememe,
- kamu yararına katkısı (toplumsal açıdan haberin değeri, haberin geleceğe ışık tutan niteliği)
- habere konu kişinin siyasetçi veya ünlü olup olmadığı,
- haber veya makalenin konusu, bu bağlamda haberin olgusal gerçekler ya da değer yargısı içerip içermediği, halkın ilgili veriye yönelik ilgisi gibi hususların her somut olay açısından incelenmesi gerekmektedir.

Yapılacak değerlendirme sonucunda unutulmayı etkin kılacak farklı yöntemler benimsenebilir. 5651 sayılı Kanun'un 6518 sayılı Kanun ile değiştirilen 9. maddesinde erişimin engellenmesinin kapsamının kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL vb.) içeriğe erişimin engellenmesi yöntemiyle verileceği ve zorunlu olmadıkça İnternet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemeyeceği belirtilmiştir...

...Bu bağlamda unutulma hakkı çerçevesinde, ifade ve basın özgürlükleri ile şeref ve itibarın korunması hakkı arasındaki dengenin sağlanması açısından 5651 sayılı Kanun kapsamında yukarıda belirtilen önlemler alınabilir (bkz. § 51). Ancak alınacak tedbirlerin Anayasa'nın 13. maddesi gereğince ölçülülük kriteri esas alınarak yapılması gereklidir. Nitekim kişinin şeref ve itibarına yönelik müdahaleleri unutulma hakkı gereğince engellemek için arşivde arama yapmaya imkân tanıyan haber ile kişi arasında ilişki kuran kişisel verilerin silinmesi, haberin anonim hâle getirilmesi, haber içeriğinin bir kısmına erişimin engellenmesi gibi birçok yöntem benimsenebilir. Bu bağlamda yargının görevinin, İnternet ortamının sağladığı kolaylıkla zamanla kişilerin itibarına yönelik müdahale oluşturan haberleri tamamen ortadan kaldırarak geçmişte meydana gelmiş olayların yeniden yazılmasını sağlamak olmadığı dikkate alınmalıdır. İnternet haber arşivinin bir bütün olarak basın özgürlüğünün korunması altında olduğu unutulmamalıdır..."

şeklindeki ifadelerle unutulma hakkının kullanılmasında gözetilmesi gereken kriterler anlatılmıştır.

Yukarıdaki açıklamalar çerçevesinde, kanun yararına bozmaya konu somut uyuşmazlığın "unutulma hakkı" özelinde değerlendirilmesine gelince;

Değişik internet sitelerinde, Ankara Barosu'nun düzenlediği 11. Uluslararası Hukuk Kurultayı'nı konu edinen ve başvuranın özel hayatına dair bilgileri içeren 08.01.2020 tarihli haberlerde;

- Yayının içeriğinin %30'una yakın bir kısmında başvuranın ismi ve geçmişine dair bilgilerin yer aldığı,

- Haberin, Kurultay'ın yapılacağı tarihlere çok kısa bir süre kala ve başvurudan bir ay önce yapıldığı, bu sırada haberin yapıldığı tarihlerde; başvuranın habere konu kamu davasında, bir suçtan (hakaret) mahkumiyet hükmünün kesinleştirildiği, iki suçtan (özel hayatın gizliliğini ihlal ve kişisel verilerin hukuka aykırı olarak kaydedilmesi) verilen beraat hükümlerinin ise Yargıtay tarafından bozulmasına karar verildiği, habere konu edilen cinsel taciz suçundan kurulan beraatin ise kesinleştirildiği, dolayısıyla başvuranın habere konu edilen yargılama sürecinin kısmen devam ettiği,

- Haberin başvuran hakkında açılan kamu davasına yönelik ifadeler içerdiği ve haberin yapıldığı sırada da başvuru sırasında da güncelliğini koruduğu,

- Haberin kamu görevlisi olan başvuranın şahsi durumuna dair bilgiler içermesi yönüyle tarihsel bir veri olarak kabul edilemeyeceği, ancak Uluslararası Hukuk Kurultayı'nda konuşmacı olarak yer alması yönüyle tarihsel bir veri olarak kabul edileceği,
- Haberin geleceğe yönelik etkisi olduğu, dolayısıyla kamu yararına katkı sunduğu,
- Haberin konusu içinde kişisel verileri paylaşılan başvuranın bir kamu görevlisi olarak kamuya mal olan önemli bir kişi konumunda bulunduğu,
- Toplumun habere yönelik ilgisinin halen bulunduğu, öte yandan başvuran hakkında kamuya açıklanan kişisel verilerin olgusal gerçekliklere (hakkında kamu davası açıldığına dair bilgilere) dayandığı ve sivil toplum örgütlerinin değer yargılarını (Başvuranın Uluslararası Hukuk Kurultayı'nda konuşmacı olarak bulunmasının kabul edilemez olduğu) içerdiği,
- Sonuç olarak, yukarıdaki şartlar bir bütün olarak değerlendirildiğinde; başvuranın geçmişte bir başka avukatla arasında var olan hukuki sürecin halen devam ettiği ve güncelliğini koruduğu, bu uyuşmazlık devam ederken başvuruçunun Ankara Barosunca düzenlenen Uluslararası Hukuk Kurultayı'nda konuşmacı olarak bulunmasının kamunun ilgisini çekecek ölçüde meşgul etmesinin haber konusu yapıldığı, haberde başvuranın kişisel verilerinin haberin konusu ile ilgili olarak ele alındığı, bu bağlamda habere konu edilen kişinin haberle ilgisi olmayan başkaca (konuyla ilgisiz) kişisel verilerinin paylaşılmadığı, paylaşılan kişisel verilerin haberin yapılması için gerekli ve yeterli ölçüde olduğu, dolayısıyla hukuka uygunluk sınırları içinde kaldığı değerlendirilmiştir.

Uyuşmazlığa konu 08.01.2020 tarihli internet yayınlarında yer alan haberlerin, başvuranın kişisel verilerini ve geçmişine dair bilgileri, uzun bir süre boyunca, başvuranın kişilik haklarını ihlal edici boyutta hukuka aykırı olarak internet üzerinde yayınlanmadığı ve unutulma hakkı çerçevesinde erişimin engellenmesi kararı verebilmek için gerekli şartların oluşmadığı anlaşılmakla,

Yargıtay Cumhuriyet Başsavcılığının kanun yararına bozma istemine dayanan ihbarname içeriği, yukarıda yazılı gerekçelerle yerinde görülmediğinden kanun yararına bozma talebinin REDDİNE, 08.02.2021 tarihinde oy birliğiyle karar verildi.

Yargıtay Kararı - 17. Ceza Dairesi (E. 2016/10020)

Yargıtay 17. CD., E. 2016/10020 K. 2016/11226 T. 1.11.2016

Esas No.: 2016/10020

Karar No.: 2016/11226

Karar Tarihi: 01.11.2016

MAHKEMESİ: Çocuk Mahkemesi

SUÇ: Hırsızlık, konut dokunulmazlığını ihlal, mala zarar verme

HÜKÜM: Mahkumiyet, temyiz talebinin reddine

Yerel mahkemece verilen hüküm temyiz edilmekle, başvurunun süresi ve kararın niteliği ile suç tarihine göre dosya görüşüldü:

26/05/2016 tarihli "mala zarar verme suçu yönünden temyiz isteminin reddine" ilişkin ek kararın suça sürüklenen çocuğa tebliğine ilişkin evraka dosya arasında rastlanmamış ise de; anılan ek kararın suça sürüklenen çocuğa tebliği için ... Nolu Kapalı Ceza İnfaz Kurumu'na 30/05/2016 tarihinde müzekkere yazılmış olması ve suça sürüklenen çocuğun 03/06/2016 tarihinde temyiz talebinde bulunmuş olması karşısında, temyiz talebinin süresinde olduğu değerlendirilerek; 26.05.2016 tarih 2016/70-2016/604 sayılı "mala zarar verme suçu yönünden temyiz reddine" ilişkin karar ve 27.04.2016 tarih 2016/70-2016/604 sayılı hırsızlık ve konut dokunulmazlığı suçlarından kurulan hükümlere yönelik temyiz incelemesinde;yapılan incelemede;

Dosya ve duruşma tutanakları içeriğine, toplanıp karar yerinde incelenerek tartışılan hukuken geçerli ve elverişli kanıtlara, gerekçeye ve hakimin takdirine göre suça sürüklenen çocuk ... ve velisinin temyiz nedeni yerinde görülmemiş olduğundan reddiyle, 26/05/2016 tarih, 2016/70 Esas ve 2016/604 Karar sayılı temyiz isteminin reddine dair ve 27.04.2016 tarih 2016/70-2016/604 sayılı hırsızlık ve konut dokunulmazlığı suçlarından kurulan usul ve kanuna uygun bulunan hükümlerin tebliğnameye uygun olarak ONANMASINA, 01.11.2016 tarihinde oyçokluğu ile karar verildi.

(MUHALİF)

07/5/2010 tarih ve 5982 sayılı Yasa'nın 2. maddesi ile değişik 2709 sayılı Türkiye Cumhuriyeti Anayasası'nın 20/3 ncü maddesinde "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere

erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmünü taşımaktadır.

5982 sayılı Yasa'nın 2. maddesinin gerekçesinde "Anayasada kişisel verilerin korunmasına yönelik dolaylı hükümler bulunmakla birlikte yeterli değildir. Mukayeseli hukukta ve tarafı olduğumuz uluslararası belgelerde de kişisel verilerin korunması önemle vurgulanmaktadır. Maddeyle, herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı, anayasal bir hak olarak teminat altına alınmaktadır. Bu bağlamda, bireylerin kendilerini ilgilendiren kişisel veriler üzerinde hangi hak ve yetkilere sahip olduğu ve kişisel verilerin hangi hallerde işlenebileceği hükme bağlanırken, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği öngörülmektedir" denilmektedir.

Türkiye Cumhuriyeti Anayasası'nın 20/3ncü maddesindeki hükümden, kişisel verilerin korunmasının Devlet açısından yerine getirilmesi gereken bir yükümlülük, yönetilenler açısından da bir isteme hakkı olduğu, konunun temel haklara bakan ciheti itibariyle; kişisel verilerin kaydı, ya kişinin kendi rızasıyla veya kanuni bir yükümlülüğün yerine getirilmesi için alınması ve depolanması gerektiği, bunun dışında bir şekilde kişisel veri toplanamayacağı, bu hakkın Devlet tarafından kullanılabilmesi için mutlaka kanuni düzenleme yapılması gerektiği anlaşılmaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanun'unun 6/1'nci maddesinde özel nitelikli kişisel veriyi "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir." şeklinde tarif ettikten sonra, 28/1 nci maddesinde bu Kanun hükümlerinin kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi ve soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi halinde uygulanmayacağını hükme bağlamıştır.

DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı, 2007 yılında Türkiye Büyük Millet Meclisi Başkanlığı'na sunulmuş ise de kanunlaşmamıştır. Tasarının 8 nci maddesinde "DNA profillerinden yararlanma yetkisi" başlığı altında "(1) Banka bünyesinde kayıtlı olan DNA profillerinden ancak, bir soruşturma, kovuşturma veya özel hukuk uyuşmazlığında gerçeğin ortaya

çıkarılabilmesi veya kimlik tespiti amacıyla yararlanılabilir. Mahkeme, hâkim veya Cumhuriyet savcısı, bir kişiye ilişkin DNA profilleriyle sisteme kayıtlı olan DNA profillerinin karşılaştırılmasını Bankadan isteyebilir. (2) Banka, bu Kanunda belirtilen esaslar çerçevesinde analizleri yapılmak suretiyle sisteme kaydedilen her yeni DNA profilini, sisteme kayıtlı olan DNA profilleri ile karşılaştırarak ortaya çıkan eşleşmeleri, en son incelemeyi isteyen mercie rapor hâlinde gönderir. Bu karşılaştırma sonucunda yapılmakta olan soruşturma, kovuşturma veya özel hukuk uyumsuzluğu ile ilgisi olmayan ancak, diğer bir suçun işlendiği şüphesini uyandıracak bir eşleştirme elde edilirse; bu eşleştirme sonucu muhafaza altına alınır ve durum Cumhuriyet savcılığına derhal bildirilir." hükmünü taşımaktaydı.

5271 sayılı CMK'nun 80/1-birinci cümlesinde ise "75, 76 ve 78'inci madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz" denilmektedir.

5237 sayılı TCK'nun 135 ve devamı maddelerinde kişisel verilerin kaydedilmesi suçu düzenlenmiş, 138/2 nci maddesinde ise "Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması halinde verilecek cezanın bir kat artırılacağı" hüküm altına alınmıştır.

Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmeliğin 14/1. maddesinde " Bu Yönetmelik hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz;

dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez." ve 14/3. maddesinde ise "Bilirkişi tarafından yapılan analizler sonucu elde edilen bulgularla ilgili makama gönderilir; bulgular üzerinden moleküler genetik analizler için izole edilen DNA örnekleri bilirkişi tarafından rapor hazırlandıktan sonra imha edilir ve bu husus raporda açıkça belirtilir." hükümlerine amirdir. Gerek Kanunlarımızda ve gerekse Yönetmelik hükümlerinde adli soruşturma nedeniyle alınan örnekler üzerinde yapılan inceleme sonuçlarının bir sisteme kaydedileceğine ilişkin bir hüküm bulunmamaktadır.

Yine Yönetmeliğin 13/3 ncü maddesinde "Yapılacak incelemeler için resmen atanan veya bilirkişilikle yükümlü olan ya da soruşturma veya kovuşturmayı yürüten makama mensup olmayan veya bu makamın soruşturma veya kovuşturmayı yürüten dairesinden teşkilât yapısı itibarıyla ve objektif olarak ayrı bir birimine mensup olan görevliler, bilirkişi olarak görevlendirilebilirler. Bu kişiler, teknik ve teşkilât bakımından uygun tedbirlerle yasak moleküler genetik incelemelerin yapılmasını ve yetkisiz üçüncü kişilerin bilgi edinmesini önlemekle yükümlüdürler. İncelenecek bulgu, bilirkişiye

ilgilinin adı ve soyadı, adresi, doğum tarihi bildirilmeksizin verilir." hükmünü amirdir. Bu hükmün, Yönetmeliğin 14/1-3'ncü maddeleri ile birlikte yorumlanmasından, incelenecek bulgunun bilirkişiye ilgilinin adı ve soyadı, adresi, doğum tarihi bildirilmeksizin verilmesi karşısında zaten bilirkişi tarafından bir sisteme kaydının fiilen imkansız olmasının sağlanmasının amaçlandığı açıkça anlaşılmaktadır.

Avrupa İnsan Hakları Mahkemesi'nin 4 Aralık 2008 tarih, 30562/04 ve 30566/04 başvuru numaralı S. ve Marper-Birleşik Krallık Davası kararında kişisel verilerin kaydı ve muhafazasının şartları ayrıntıları ile tartışılmış, yine Anayasa Mahkemesinin 12/11/2015 tarih ve 2015/32 Esas, 2015/102 Karar sayılı kararında ise 5237 sayılı TCK'nun 136/1 nci maddesinin Türkiye Cumhuriyeti Anayasası'na aykırılığı bağlamında kişisel verilerin kayda alınması ve kullanılması konusu tartışılmıştır.

Suçta sürüklenen çocuk tüm aşamalarda atılı suçları işlemediğini, suçsuz olduğunu savunmuştur. Suça sürüklenen çocuk temyiz dilekçesinde de; vücudundan DNA analizi için örnek alınmadığını, olay mahallinde bulunan çorap üzerinden elde edilen epitel hücrelerin kendisine ait olmadığını, karşılaştırma yapıldığı bildirilen bilginin ait olduğu materyalinde kendisine ait olmadığını beyan etmiştir.

Bu itibarla, suça sürüklenen çocuğun 24/01/2011 tarihinde işlediği başka bir suç nedeniyle hukuka uygun olarak alınıp alınmadığı dahi tespit edilmemiş vücut örnekleri üzerinde yapılan çalışma sonucu elde edilen genotip özelliklerin hukuka aykırı olarak bir sisteme kaydedildiği ve yargılama konusu olayımızda olay mahallinde bulunan çorap üzerinden alınan epitel hücreler üzerinde genotip incelemesi yapılarak sisteme yüklenen sonuçlarla karşılaştırılıp suça sürüklenen çocuğa ait olduğunun tespit edilmesinin 5271 sayılı CMK'nun 217/2 nci maddesinde öngörülen "Yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir." hükmüne açıkça aykırı olduğu sabittir.

Her ne kadar Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmeliğin 17. maddesine göre, mahkumiyet kararı verilmesi halinde bu Yönetmeliğin 15 nci maddesinin birinci ve ikinci fıkraları uyarınca elde edilen veriler (fotoğrafı, iris görüntüsü, beden ölçüleri, diş izi, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak eşkal bilgileri, kulak, dudak gibi organların bıraktığı kimlik tespitine yarayabilecek vücut izleri ile sesi ve görüntüleri) kolluk tarafından, üçüncü fıkrasında belirtilen diş izleri ise bu işlemi yapan sağlık kuruluşu tarafından arşivleneceği belirtilmiş ise de bu bilgilerin fizik kimliğinin tespiti ile ilgili olup, DNA verilerini içermediği açıktır. Kaldı ki, fizik kimliğin tespitine ilişkin verilerin arşivlenebilmesinin ön koşulu da kişi hakkında mahkumiyet kararı verilmesidir. Yönetmeliğin bu

hükmü, DNA verilerinin arşivlenmesine kesinlikle izin veren bir hüküm değildir ve Türkiye Cumhuriyeti Anayasası'nın 20/3ncü maddesi hükmü nazara alındığında bu şekilde yorumlanması da mümkün değildir.

Yukarıda izah ettiğim Türkiye Cumhuriyeti Anayasası ve Kanunlarımızdaki hükümler çerçevesinde, yasak delil niteliğindeki bilirkişi raporu haricinde suça sürüklenen çoğun atılı suçları işlediğine dair mahkumiyetini gerektirir kesin ve inandırıcı delilin yargılama dosyası arasında bulunmadığından beraatına karar verilmesi ve dolayısıyla ilk derece mahkemesinin hırsızlık ve konut dokunulmazlığını ihlal suçlarından kurduğu hükümlerin bozulması gerektiği kanaatinde olduğumdan, sayın çoğunluğun onama kararına katılmıyorum. 04.11.2016

Yargıtay Kararı - 17. Ceza Dairesi (E. 2016/9901)

Yargıtay 17. CD., E. 2016/9901 K. 2016/11870 T. 16.11.2016

Esas No.: 2016/9901

Karar No.: 2016/11870

Karar Tarihi: 16.11.2016

MAHKEMESİ: Asliye Ceza Mahkemesi

SUÇ: Hırsızlık, konut dokunulmazlığını ihlal

HÜKÜM: Mahkumiyet

Yerel mahkemece verilen hüküm temyiz edilmekle, başvurunun süresi ve kararın niteliği ile suç tarihine göre dosya görüşüldü:

1)Sanığın, konut dokunulmazlığının ihlali suçundan kurulan hükme yönelik temyiz itirazlarının incelenmesinde;

Hak yoksunluklarına hükmedilirken yanılıklı hüküm kurulmuş ise de, mahkumiyetin kanuni sonucu olarak infaz evresinde resen ve doğru olarak, TCK'nın 53. maddesinin 1 ila 3. fıkralarında öngörüldüğü biçimde uygulanması mümkün görüldüğünden bozma nedeni yapılmamıştır.

Dosya ve duruşma tutanakları içeriğine, toplanıp karar yerinde incelenerek tartışılan hukuken geçerli ve elverişli kanıtlara, gerekçeye ve hakimin takdirine göre sanık ...'ın temyiz nedenleri yerinde görülmemiş olduğundan reddiyle, usul ve kanuna uygun bulunan hükmün tebliğnameye aykırı olarak ONANMASINA,

2)Sanığın, hırsızlık suçundan kurulan hükme yönelik temyiz itirazlarının incelenmesinde;

1-TCK'nın 142/2-h maddesinde düzenlenen hırsızlık suçunun alt sınırının 5 yıl olması karşısında, sanığın istinabe suretiyle sorguya çekilemeyeceği gözetilmeden, savunma hakkı kısıtlanarak hüküm kurulması suretiyle CMK'nın 196/2. maddesine aykırı davranılması,

Bozmayı gerektirmiş, sanık ...'ın temyiz sebepleri bu itibarla yerinde görülmüş olduğundan hükmün açıklanan nedenlerle sair yönleri incelenmeksizin tebliğnameye uygun olarak BOZULMASINA, 16.11.2016 tarihinde hırsızlık suçundan oybirliği, konut dokunulmazlığını ihlal suçundan oyçokluğu ile karar verildi.

MUHALEFET ŞERHİ

07/5/2010 tarih ve 5982 sayılı Yasa'nın 2. maddesi ile deęişik 2709 sayılı Türkiye Cumhuriyeti Anayasası'nın 20/3 ncü maddesinde "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve

amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmünü taşımaktadır.

5982 sayılı Yasa'nın 2. maddesinin gerekçesinde "Anayasada kişisel verilerin korunmasına yönelik dolaylı hükümler bulunmakla birlikte yeterli değildir. Mukayeseli hukukta ve tarafı olduğumuz uluslararası belgelerde de kişisel verilerin korunması önemle vurgulanmaktadır. Maddeyle, herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı, anayasal bir hak olarak teminat altına alınmaktadır. Bu bağlamda, bireylerin kendilerini ilgilendiren kişisel veriler üzerinde hangi hak ve yetkilere sahip olduğu ve kişisel verilerin hangi hallerde işlenebileceği hükme bağlanırken, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği öngörülmektedir" denilmektedir.

Türkiye Cumhuriyeti Anayasası'nın 20/3 ncü maddesindeki hükümden, kişisel verilerin korunmasının Devlet açısından yerine getirilmesi gereken bir yükümlülük, yönetilenler açısından da bir isteme hakkı olduğu, konunun temel haklara bakan ciheti itibariyle; kişisel verilerin kaydı, ya kişinin kendi rızasıyla veya kanuni bir yükümlülüğün yerine getirilmesi için alınması ve depolanması gerektiği, bunun dışında bir şekilde kişisel veri toplanamayacağı, bu hakkın Devlet tarafından kullanılabilmesi için mutlaka kanuni düzenleme yapılması gerektiği anlaşılmaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanun'unun 6/1 nci maddesinde özel nitelikli kişisel veriyi "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir." şeklinde tarif ettikten sonra, 28/1 nci maddesinde bu Kanun hükümlerinin kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi ve soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi halinde uygulanmayacağını hükme bağlamıştır.

DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı, 2007 yılında Türkiye Büyük Millet Meclisi Başkanlığına sunulmuş ise de kanunlaşmamıştır. Tasarının 8 nci maddesinde "DNA profillerinden yararlanma yetkisi" başlığı altında "(1) Banka bünyesinde kayıtlı olan DNA profillerinden ancak, bir soruşturma, kovuşturma veya özel hukuk uyuşmazlığında gerçeğin ortaya çıkarılabilmesi veya kimlik tespiti amacıyla yararlanılabilir. Mahkeme, hâkim veya Cumhuriyet Savcısı, bir kişiye ilişkin DNA profilleriyle sisteme kayıtlı olan DNA profillerinin karşılaştırılmasını Bankadan isteyebilir. (2) Banka, bu Kanunda belirtilen esaslar çerçevesinde analizleri yapılmak suretiyle sisteme kaydedilen her yeni DNA profilini, sisteme kayıtlı olan DNA profilleri ile karşılaştırarak ortaya çıkan eşleşmeleri, en son incelemeyi isteyen mercie rapor hâlinde gönderir. Bu karşılaştırma sonucunda yapılmakta olan soruşturma, kovuşturma veya özel hukuk uyuşmazlığı ile ilgisi olmayan ancak, diğer bir suçun işlendiği şüphesini uyandıracak bir eşleştirme elde edilirse; bu eşleştirme sonucu muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhal bildirilir." hükmünü taşımaktaydı.

5271 sayılı CMK'nın 80/1-birinci cümlesinde ise "75, 76 ve 78'inci madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz" denilmektedir.

5237 sayılı TCK'nın 135 ve devamı maddelerinde kişisel verilerin kaydedilmesi suçu düzenlenmiş, 138/2 nci maddesinde ise "Suçun konusunun Ceza Muhakemesi Kanun'u hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması halinde verilecek cezanın bir kat artırılacağı" hüküm altına alınmıştır.

Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmeliğin 14/1. maddesinde " Bu Yönetmelik hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez." ve

14/3. maddesinde ise "Bilirkişi tarafından yapılan analizler sonucu elde edilen bulgular ilgili makama gönderilir; bulgular üzerinden moleküler genetik analizler için izole edilen DNA örnekleri bilirkişi tarafından rapor hazırlandıktan sonra imha edilir ve bu husus raporda açıkça belirtilir." hükümlerine amirdir. Gerek Kanunlarımızda ve gerekse Yönetmelik hükümlerinde adli soruşturma nedeniyle alınan örnekler üzerinde yapılan inceleme sonuçlarının bir sisteme kaydedileceğine ilişkin bir hüküm bulunmamaktadır.

Yine Yönetmeliğin 13/3 ncü maddesinde "Yapılacak incelemeler için resmen atanan veya bilirkişilikle yükümlü olan ya da soruşturma veya kovuşturmayı yürüten makama mensup olmayan veya bu

makamın soruşturma veya kovuşturmayı yürüten dairesinden teşkilât yapısı itibarıyla ve objektif olarak ayrı bir birimine mensup olan görevliler, bilirkişi olarak görevlendirilebilirler. Bu kişiler, teknik ve teşkilât bakımından uygun tedbirlerle yasak moleküler genetik incelemelerin yapılmasını ve yetkisiz üçüncü kişilerin bilgi edinmesini önlemekle yükümlüdürler. İncelenecek bulgu, bilirkişiye ilgilinin adı ve soyadı, adresi, doğum tarihi bildirilmeksizin verilir." hükmünü amirdir. Bu hükmün, Yönetmeliğin 14/1-3 ncü maddeleri ile birlikte yorumlanmasından, incelenecek bulgunun bilirkişiye ilgilinin adı ve soyadı, adresi, doğum tarihi bildirilmeksizin verilmesi karşısında zaten bilirkişi tarafından bir sisteme kaydının fiilen imkansız olmasının sağlanmasının amaçlandığı açıkça anlaşılmaktadır.

Sanık ... tüm aşamalarda atılı suçları işlemediğini, suçsuz olduğunu savunmuştur.

Bu itibarla, sanık ...'ın 15/10/2014 tarihinde işlediği iddia olunan başka bir suç nedeniyle hukuka uygun olarak alınıp alınmadığı dahi tespit edilmemiş vücut örnekleri üzerinde yapılan çalışma sonucu elde edilen genotip özelliklerin hukuka aykırı olarak bir sisteme kaydedildiği ve yargılama konusu olayımızda olay mahallinde bulunan sigara izmariti üzerinden alınan epitel hücreler üzerinde genotip incelemesi yapılarak sisteme yüklenen sonuçlarla karşılaştırılıp sanığa ait olduğunun tespit edilmesinin 5271 sayılı CMK'nın 217/2 nci maddesinde öngörülen "Yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir." hükmüne açıkça aykırı olduğu sabittir.

Yukarıda izah ettiğim Türkiye Cumhuriyeti Anayasası ve Kanunlarımızdaki hükümler çerçevesinde, yasak delil niteliğindeki bilirkişi raporu haricinde sanığın atılı konut dokunulmazlığının ihlali suçunu işlediğine dair mahkumiyetini gerektirir kesin ve inandırıcı delilin yargılama dosyası arasında bulunmadığından beraatına karar verilmesi ve dolayısı ile ilk derece mahkemesinin konut dokunulmazlığını ihlal suçundan kurduğu hükmün bozulması gerektiği kanaatinde olduğumdan, sayın çoğunluğun onama kararına katılmıyorum. 17/11/2016

...

Yargıtay Üyesi

Yargıtay Kararı - 17. Ceza Dairesi (E. 2015/22839)

Yargıtay 17. CD., E. 2015/22839 K. 2017/2999 T. 14.3.2017

Esas No.: 2015/22839

Karar No.: 2017/2999

Karar Tarihi: 14.03.2017

MAHKEMESİ: Asliye Ceza Mahkemesi

SUÇLAR: Hırsızlık, konut dokunulmazlığının ihlali

HÜKÜM: Mahkumiyet

Yerel mahkemece verilen hükümler temyiz edilmekle, başvurunun süresi ve kararların niteliği ile suç tarihine göre dosya görüşüldü:

Anayasa Mahkemesi'nin hükümden sonra 24/11/2015 gün ve 29542 sayılı Resmi Gazete'de yayımlanan 08/10/2015 tarih, 2014/140 Esas ve 2015/85 sayılı kararı ile TCK'nın 53. maddesinin (1) numaralı fıkrasının (b) bendine yönelik olarak vermiş olduğu iptal kararlarının da kapsam ve içerik itibarıyla infaz aşamasında mahallinde gözetilebileceğinden bozma nedeni yapılmamıştır.

Dosya ve duruşma tutanakları içeriğine, toplanıp karar yerinde incelenerek tartışılan hukuken geçerli ve elverişli kanıtlara, gerekçeye ve hâkimin takdirine göre, sanık ...'ın temyiz nedenleri yerinde görülmemiş olduğundan reddiyle, usûl ve kanuna uygun bulunan hükümlerin, tebliğnameye uygun olarak ONANMASINA, 14.03.2017 tarihinde oyçokluğu ile karar verildi.

MUHALEFET ŞERHİ

07/05/2010 tarih ve 5982 sayılı Yasa'nın 2. maddesi ile değişik 2709 sayılı Türkiye Cumhuriyeti Anayasası'nın 20/3. maddesinde "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmünü taşımaktadır.

5982 sayılı Yasa'nın 2. maddesinin gerekçesinde "Anayasada kişisel verilerin korunmasına yönelik dolaylı hükümler bulunmakla birlikte yeterli değildir. Mukayeseli hukukta ve tarafı olduğumuz

uluslararası belgelerde de kişisel verilerin korunması önemle vurgulanmaktadır. Maddeyle, herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı, anayasal bir hak olarak teminat altına alınmaktadır. Bu bağlamda, bireylerin kendilerini ilgilendiren kişisel veriler üzerinde hangi hak ve yetkilere sahip olduğu ve kişisel verilerin hangi hallerde işlenebileceği hükme bağlanırken, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği öngörülmektedir" denilmektedir.

Türkiye Cumhuriyeti Anayasası'nın 20/3. maddesindeki hükümden, kişisel verilerin korunmasının Devlet açısından yerine getirilmesi gereken bir yükümlülük, yönetilenler açısından da bir isteme hakkı olduğu, konunun temel haklara bakan ciheti itibariyle; kişisel verilerin kaydı, ya kişinin kendi rızasıyla veya kanuni bir yükümlülüğün yerine getirilmesi için alınması ve depolanması gerektiği, bunun dışında bir şekilde kişisel veri toplanamayacağı, bu hakkın Devlet tarafından kullanılabilmesi için, mutlaka kanuni düzenleme yapılması gerektiği anlaşılmaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanun'u 6/1. maddesinde özel nitelikli kişisel veriyi "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir." şeklinde tarif ettikten sonra, 28/1. maddesinde bu Kanun hükümlerinin kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi ve soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi halinde uygulanmayacağını hükme bağlamıştır.

DNA verileri ve Türkiye Milli DNA Veri Bankası Kanun Tasarısı, 2007 yılında Türkiye Büyük Millet Meclisi Başkanlığına sunulmuş ise de kanunlaşmamıştır. Tasarının 8. maddesinde "DNA profillerinden yararlanma yetkisi" başlığı altında "(1) Banka bünyesinde kayıtlı olan DNA profillerinden ancak, bir soruşturma, kovuşturma veya özel hukuk uyuşmazlığında gerçeğin ortaya çıkarılabilmesi veya kimlik tespiti amacıyla yararlanılabilir. Mahkeme, hâkim veya Cumhuriyet savcısı, bir kişiye ilişkin DNA profilleriyle sisteme kayıtlı olan DNA profillerinin karşılaştırılmasını bankadan istenebilir. (2) Banka, bu Kanunda belirtilen esaslar çerçevesinde analizleri yapılmak suretiyle sisteme ve kaydedilen her yeni DNA profilini, sisteme kayıtlı olan DNA profilleri ile karşılaştırarak onaya çıkan eşleşmeleri, en son incelemeyi isteyen mercie rapor hâlinde gönderir. Bu karşılaştırma sonucunda yapılmakta olan soruşturma, kovuşturma veya özel hukuk uyuşmazlığı de

ilgisi olmayan ancak, diğere bir suçun işlendiğı şüphesini uyandıracak bir eşleştirme elde edilirse; bu eşleştirme sonucu muhafaza altına alınır ve durum Cumhuriyet savcılığına derhal bildirilir." hükmünü taşımaktaydı.

5271 sayılı CMK'nın 20/1-birinci cümlesinde ise "75, 76 ve 78. madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz" denilmektedir.

5237 sayılı TCK'nın 135 ve devamı maddelerinde kişisel verilerin kaydedilmesi suçu düzenlenmiş, 138/2. maddesinde ise "Suçun konusunun Ceza Muhakemesi Kanun'u hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması halinde verilecek cezanın bir kat artırılacağı" hüküm altına alınmıştır.

Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmeliğin 14/1. maddesinde " Bu Yönetmelik hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez." ve 14/3. maddesinde ise "Bilirkişi tarafından yapılan analizler sonucu elde edilen bulgular ilgili makama gönderilir; bulgular üzerinden moleküler genetik analizler için izole edilen DNA

örnekleri bilirkişi tarafından rapor hazırlandıktan sonra imha edilir ve bu husus raporda açıkça belirtilir." hükümlerine amirdir. Gerek Kanunlarımızda ve gerekse Yönetmelik hükümlerinde adli soruşturma nedeniyle alınan örnekler üzerinde yapılan inceleme sonuçlarının bir sisteme kaydedileceğine ilişkin bir hüküm bulunmamaktadır.

Yine Yönetmeliğin 13/3. maddesinde "Yapılacak incelemeler için resmen atanan veya bilirkişilikle yükümlü olan ya da soruşturma veya kovuşturmayı yürüten makama mensup olmayan veya bu makamın soruşturma veya kovuşturmayı yürüten dairesinden teşkilât yapısı itibarıyla ve objektif olarak ayrı bir birimine mensup olan görevliler, bilirkişi olarak görevlendirilebilirler. Bu kişiler, teknik ve teşkilât bakımından uygun tedbirlerle yasak moleküler genetik incelemelerin yapılmasını ve yetkisiz üçüncü kişilerin bilgi edinmesini önlemekle yükümlüdürler. İncelenecek bulgu, bilirkişiyeye ilgilinin adı ve soyadı, adresi, doğum tarihi bildirilmeksizin verilir." hükmünü amirdir. Bu hükmün, Yönetmeliğin 14/1-3. maddeleri ile birlikte yorumlanmasından, incelenecek bulgunun bilirkişiyeye ilgilinin adı ve soyadı, adresi, doğum tarihi bildirilmeksizin verilmesi karşısında zaten bilirkişi tarafından bir sisteme kaydının fiilen imkansız olmasının sağlanmasının amaçlandığı açıkça anlaşılmaktadır.

Sanık tüm aşamalarda atılı suçları işlemediğini, suçsuz olduğunu savunmuştur. Sanık, katılana ait evin balkonunun altında bulunan şapkanın kendisine ait olduğunu, ancak olay mahalline nasıl konulduğunu bilmediğini beyan etmiştir.

Bu itibarla sanığın daha önce işlediği başka bir suç nedeniyle hukuka uygun olarak alınıp alınmadığı dahi tespit edilmemiş vücut örnekleri üzerinde yapılan çalışma sonucu elde edilen genotip özelliklerin hukuka aykırı olarak bir sisteme kaydedildiği ve yargılama konusu olayımızda olay mahallinde bulunan şapka üzerinden alınan materyal üzerinde genotip incelemesi yapılarak sisteme yüklenen sonuçlarla karşılaştırılıp sanığa ait olduğunun tespit edilmesinin 5271 sayılı CMK'nın 217/2. maddesinde öngörülen "Yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir." hükmüne açıkça aykırı olduğu sabittir.

Yukarıda izah ettiğim Türkiye Cumhuriyeti Anayasası ve Kanunlarımızdaki hükümler çerçevesinde, yasak delil niteliğindeki bilirkişi raporu haricinde sanığın atılı suçları işlediğine dair mahkumiyetini gerektirir kesin ve inandırıcı delilin yargılama dosyası arasında bulunmadığından beraatine karar verilmesi ve dolayısı ile ilk derece mahkemesinin hırsızlık ve konut dokunulmazlığını ihlal suçlarından kurduğu hükümlerin bozulması gerektiği kanaatinde olduğumdan, sayın çoğunluğun onama kararına katılmıyorum. 14.03.2017

Yargıtay Kararı - 17. Ceza Dairesi (E. 2015/18421)

Yargıtay 17. CD., E. 2015/18421 K. 2016/11783 T. 14.11.2016

Esas No.: 2015/18421

Karar No.: 2016/11783

Karar Tarihi: 14.11.2016

MAHKEMESİ: Asliye Ceza Mahkemesi

SUÇ: Hırsızlık, mala zarar verme

HÜKÜM: Mahkumiyet

Yerel mahkemece verilen hüküm temyiz edilmekle, başvurunun süresi ve kararın niteliği ile suç tarihine göre dosya görüşüldü:

1-Sanık hakkında mala zarar verme suçundan kurulan hükmün temyiz incelemesinde;

Mala zarar verme suçundan doğrudan hükmolunan adli para cezasının miktar ve türüne göre; 14.04.2011 tarihinde yürürlüğe giren 6217 sayılı Yasa'nın 26. maddesi ile 5320 Sayılı Ceza Muhakemesi Kanunu'nun Yürürlük ve Uygulama Şekli Hakkındaki Kanun'a eklenen geçici 2. maddesi gereğince doğrudan hükmolunan 3.000,00 TL dahil adli para cezasına mahkumiyet hükümlerinin temyizi mümkün olmadığından, sanık ...'nin temyiz isteminin 1412 sayılı CMUK'nun 317. maddesi uyarınca REDDİNE,

2-Sanık hakkında hırsızlık suçundan kurulan hükmün temyiz incelemesinde;

Hırsızlık suçuna konu eşyanın önem ve değeri, meydana gelen zararın ağırlığı dikkate alınarak 5237 sayılı TCK'nın 61. maddesi uyarınca temel ceza belirlenirken alt sınırdan hüküm kurulması ile sanık hakkında, Gaziantep 8. Asliye Ceza Mahkemesi'nin 2008/667-1231 E-K. sayılı kararıyla izinsiz hint keneviri ekmek suçundan verilen ve 17.01.2013 tarihinde kesinleşen tekerrüre esas eski hükümlülüğü bulunduğu ve koşulları olduğu halde 5237 sayılı TCK'nın 58. maddesinin uygulanmaması hususları, karşı temyiz olmadığından bozma nedeni yapılmamıştır.

Hak yoksunluklarına hükmedilirken yanılıklı hüküm kurulmuş ise de, mahkumiyetin kanuni sonucu olarak infaz evresinde resen ve doğru olarak, TCK'nın 53. maddesinin 1 ila 3. fıkralarında öngörüldüğü biçimde uygulanması mümkün görüldüğünden ve Anayasa Mahkemesi'nin hükümden sonra 24/11/2015 gün ve 29542 sayılı Resmi Gazete'de yayımlanan 08/10/2015 tarih,

2014/140 Esas ve 2015/85 Karar sayılı kararı ile TCK'nın 53. maddesinin (1) numaralı fıkrasının (b) bendine yönelik olarak vermiş olduğu iptal kararlarının da kapsam ve içerik itibariyle infaz aşamasında mahallinde gözetilebileceğinden, bozma nedeni yapılmamıştır.

Dosya ve duruşma tutanakları içeriğine, toplanıp karar yerinde incelenerek tartışılan hukuken geçerli ve elverişli kanıtlara, gerekçeye ve hakimın takdirine göre sanık ...'nın temyiz nedeni yerinde görülmemiş olduğundan reddiyle usul ve kanuna uygun bulunan hükmün tebliğnameye uygun olarak ONANMASINA, 14.11.2016 gününde oyçokluğu ile karar verildi.

MUHALEFET ŞERHİ

07/5/2010 tarih ve 5982 sayılı Yasa'nın 2. maddesi ile değişik 2709 sayılı Türkiye Cumhuriyeti Anayasası'nın 20/3 ncü maddesinde "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmünü taşımaktadır.

5982 sayılı Yasa'nın 2. maddesinin gerekçesinde "Anayasa da kişisel verilerin korunmasına yönelik dolaylı hükümler bulunmakla birlikte yeterli değildir. Mukayeseli hukukta ve tarafı olduğumuz uluslararası belgelerde de kişisel verilerin korunması önemle vurgulanmaktadır. Maddeyle, herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı, anayasal bir hak olarak teminat altına alınmaktadır. Bu bağlamda, bireylerin kendilerini ilgilendiren kişisel veriler üzerinde hangi hak ve yetkilere sahip olduğu ve kişisel verilerin hangi hallerde işlenebileceği hükme bağlanırken, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği öngörülmektedir" denilmektedir.

Türkiye Cumhuriyet Anayasası'nın 20/3 ncü maddesindeki hükümden, kişisel verilerin korunmasının Devlet açısından yerine getirilmesi gereken bir yükümlülük, yönetilenler açısından da bir isteme hakkı olduğu, konunun temel haklara bakan ciheti itibariyle; kişisel verilerin kaydı, ya kişinin kendi rızasıyla veya kanuni bir yükümlülüğün yerine getirilmesi için alınması ve depolanması gerektiği, bunun dışında bir şekilde kişisel veri toplanamayacağı, bu hakkın Devlet tarafından kullanılabilmesi için mutlaka kanuni düzenleme yapılması gerektiği anlaşılmaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanun'u 6/1 nci maddesinde özel nitelikli kişisel veriyi "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık

ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir." şeklinde tarif ettikten sonra, 28/1 nci maddesinde bu Kanun hükümlerinin kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbarî faaliyetler kapsamında işlenmesi ve soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi halinde uygulanmayacağını hükme bağlamıştır.

DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı, 2007 yılında Türkiye Büyük Millet Meclisi Başkanlığına sunulmuş ise de kanunlaşmamıştır. Tasarının 8 nci maddesinde "DNA profillerinden yararlanma yetkisi" başlığı altında "(1) Banka bünyesinde kayıtlı olan DNA profillerinden ancak, bir soruşturma, kovuşturma veya özel hukuk uyuşmazlığında gerçeğin ortaya çıkarılabilmesi veya kimlik tespiti amacıyla yararlanılabilir. Mahkeme, hâkim veya Cumhuriyet savcısı, bir kişiye ilişkin DNA profilleriyle sisteme kayıtlı olan DNA profillerinin karşılaştırılmasını Bankadan isteyebilir. (2) Banka, bu Kanunda belirtilen

esaslar çerçevesinde analizleri yapılmak suretiyle sisteme kaydedilen her yeni DNA profilini, sisteme kayıtlıdan DNA profilleri ile karşılaştırarak ortaya çıkan eşleşmeleri, en son incelemeyi isteyen mercie rapor hâlinde gönderir. Bu karşılaştırma sonucunda yapılmakta olan soruşturma, kovuşturma veya özel hukuk uyuşmazlığı ile ilgisi olmayan ancak, diğer bir suçun işlendiği şüphesini uyandıracak bir eşleştirme elde edilirse; bu eşleştirme sonucu muhafaza altına alınır ve durum Cumhuriyet savcılığına derhal bildirilir." hükmünü taşımaktaydı.

5271 sayılı CMK'nın 80/1-birinci cümlesinde ise "75, 76 ve 78'inci madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup başka bir amaçla kullanılamaz" denilmektedir.

5237 sayılı TCK'nın 135 ve devamı maddelerinde kişisel verilerin kaydedilmesi suçu düzenlenmiş, 138/2 nci maddesinde ise "Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması halinde verilecek cezanın bir kat artırılacağı" hüküm altına alınmıştır.

Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmeliğin 14/1. maddesinde " Bu Yönetmelik hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez." ve 14/3. maddesinde ise

"Bilirkişi tarafından yapılan analizler sonucu elde edilen bulgular ilgili makama gönderilir; bulgular üzerinden moleküler genetik analizler için izole edilen DNA örnekleri bilirkişi tarafından rapor hazırlandıktan sonra imha edilir ve bu husus raporda açıkça belirtilir." hükümlerine amirdir. Gerek Kanunlarımızda ve gerekse Yönetmelik hükümlerinde adli soruşturma nedeniyle alınan örnekler üzerinde yapılan inceleme sonuçlarının bir sisteme kaydedileceğine ilişkin bir hüküm bulunmamaktadır.

Yine Yönetmeliğin 13/3 ncü maddesinde "Yapılacak incelemeler için resmen atanan veya bilirkişilikle yükümlü olan ya da soruşturma veya kovuşturmayı yürüten makama mensup olmayan veya bu makamın soruşturma veya kovuşturmayı yürüten dairesinden teşkilât yapısı itibarıyla ve objektif olarak ayrı bir birimine mensup olan görevliler, bilirkişi olarak görevlendirilebilirler. Bu kişiler, teknik ve teşkilât bakımından uygun tedbirlerle yasak moleküler genetik incelemelerin yapılmasını ve yetkisiz üçüncü kişilerin bilgi edinmesini önlemekle yükümlüdürler. İncelenecek bulgu, bilirkişiye ilgilinin adı ve soyadı, adresi, doğum tarihi bildirilmeksizin verilir." hükmünü amirdir. Bu hükmün, Yönetmeliğin 14/1-3 ncü maddeleri ile birlikte yorumlanmasından, incelenecek bulgunun bilirkişiye ilgilinin adı ve soyadı, adresi, doğum tarihi bildirilmeksizin verilmesi karşısında zaten bilirkişi tarafından bir sisteme kaydının fiilen imkansız olmasının sağlanmasının amaçlandığı açıkça anlaşılmaktadır.

Sanık tüm aşamalarda atılı suçu işlemediğini, hırsızlık suçu yapılan araçta bulunan kolonya şişesi üzerindeki kanın burada nasıl bulunduğu anlam veremediğini, suçsuz olduğunu savunmuştur. Dosya arasında moleküler genetik inceleme sonucu hazırlanan rapor dışında, sanığın atılı suçu işlediğine dair başka bir delil de mevcut değildir.

Bu itibarla, ... İl Jandarma Komutanlığı'nın 02/03/2012 ve ... Emniyet Müdürlüğü'nün 03/05/2012 tarihli yazılarına istinaden alınan kan örnekleri üzerinde yapılan çalışmalar neticesinde oluşturulan ve hukuka uygun olarak alınıp alınmadığı dahi tespit edilmemiş sanığa ait vücut örnekleri üzerinde yapılan çalışma sonucu elde edilen genotip özelliklerin hukuka aykırı olarak bir sisteme kaydedildiği ve yargılama konusu olayımızda olay mahallinde bulunan kolonya şişesi üzerinden alınan kan örnekleri üzerinde genotip incelemesi yapılarak sisteme yüklenen sonuçlarla karşılaştırılıp sanığa ait olduğunun tespit edilmesinin 5271 sayılı CMK'nun 217/2nci maddesinde öngörülen "Yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir." hükmüne açıkça aykırı olduğu sabittir.

Yukarıda izah ettiğim Türkiye Cumhuriyeti Anayasası ve Kanunlarımızdaki hükümler çerçevesinde, yasak delil niteliğindeki bilirkişi raporu haricinde sanığın atılı suçu işlediğine dair mahkumiyetini

gerektirir kesin ve inandırıcı delilin yargılama dosyası arasında bulunmadığından beraatına karar verilmesi ve dolayısı ile ilk derece mahkemesinin hırsızlık suçundan kurduğu hükmün bozulması gerektiği kanaatinde olduğumdan, sayın çoğunluğun onama kararına katılmıyorum. 14.11.2016

Yargıtay Kararı - 12. Ceza Dairesi (E. 2020/974)

Yargıtay 12. Ceza Dairesi. E. 2020/974 K. 2021/3641 T. 14.4.2021

Esas No.: 2020/974

Karar No. 2021/3641

Karar tarihi: 14.04.2021

Mahkemesi: Asliye Ceza Mahkemesi

Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçundan sanığın beraatine ilişkin hüküm, katılan tarafından temyiz edilmekle, dosya incelenerek gereği düşünüldü:

Yapılan yargılamaya, incelenen dosya kapsamına göre, katılanın sanık hakkında mahkumiyet kararı verilmemesinin isabetsiz olduğuna ilişkin sair temyiz itirazlarının reddine, ancak;

Şikayet dilekçesi, sanık hakkında düzenlenen iddianame ve dosya kapsamına göre, resmi nikahlı eşi olan tanık Havagül'ün sadakatinden kuşkulanan ve aldatıldığını düşünen sanık ...'ın, eşine ait cep telefonuna gizlice yüklediği casus program aracılığıyla eşi ile eşinin kardeşi olan katılan ...'ın yaptığı telefon görüşmelerini kayıt altına alması nedeniyle TCK'nın 133/1. maddesindeki kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçunu işlediğinin iddia edildiği olayda;

Ses kayıtlarının çözümüne ilişkin 26.05.2014 tarihli bilirkişi raporu, dosyada mevcut diğer delillerle birlikte değerlendirildiğinde; katılan ... ile katılanın ablası olan tanık Havagül arasındaki görüşmelerin yüz yüze değil, telefon aracılığıyla gerçekleşmesinden dolayı iddianamede kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçu olarak nitelendirilen eylemin, iddianame anlatımı gözetilerek, TCK'nın 132. maddesindeki haberleşmenin gizliliğini ihlal suçu kapsamında değerlendirilebileceği; ancak, katılanın tarafı olduğu haberleşme içeriklerini, üçüncü kişi ya da kişilerle paylaştığı ve/veya çoğaltarak dağıttığına ilişkin hakkında bir iddia ileri sürülmeyen sanığın, kendisine ve aile birliğine yönelik, onurunu zedeleyen, haksız bir saldırı altında ve başkaca şekilde ispatlanması mümkün olmayan bir hal içerisinde iken, kaybolma olasılığı bulunan delillerin muhafazasını sağlayıp, boşanma davasına sunarak, aile içi geçimsizliğin kaynağının, katılanın ablasının yani eşinin güven sarsıcı ve olumsuz davranışları olduğunu ispatlama amacını taşıyan eylemlerinde, hukuka aykırı hareket ettiği bilinciyle davranmaması nedeniyle sanık hakkında CMK'nın 223/2-a maddesi gereğince beraat kararı verilmesi gerekirken, aynı Kanununun 223/2-c maddesi gereğince beraat hükmü kurulması,

Kanuna aykırı olup, katılanın temyiz itirazları bu itibarla yerinde görüldüğünden, hükmün bu nedenle 5320 sayılı Kanun'un 8. maddesi uyarınca halen uygulanmakta olan 1412 sayılı CMUK'un 321. maddesi gereğince BOZULMASINA; ancak, yeniden yargılama gerektirmeyen bu konuda, aynı Kanunun 322. maddesi gereğince karar verilmesi mümkün bulunduğundan, aynı maddenin verdiği yetkiye istinaden; hüküm fıkrasının ilk paragrafının "İddianamede TCK'nın 133. maddesindeki kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçu olarak nitelendirilen eylemin, iddianame anlatımı ve dosya kapsamı gözetilerek, TCK'nın 132. maddesindeki haberleşmenin gizliliğini ihlal suçu kapsamında değerlendirilebileceği; ancak, yapılan yargılama sonunda, sanığa yüklenen fiilin kanunda suç olarak tanımlanmamış olduğu anlaşıldığından, sanığın, CMK'nın 223/2-a maddesi gereğince beraatine," olarak değiştirilmesi suretiyle, sair yönleri usul ve kanuna uygun bulunan hükmün DÜZELTİLEREK ONANMASINA, 14.04.2021 tarihinde oybirliğiyle karar verildi.

Yargıtay Kararı - 12. Ceza Dairesi (E. 2019/4369)

Yargıtay 12. Ceza Dairesi 2019/4369 E. 2019/8633 K.

Esas No: 2019/4369

Karar No: 2019/8633

Mahkemesi: Asliye Ceza Mahkemesi

Suç: Özel hayatın gizliliğini ihlal

Hüküm: TCK'nın 134/1-1, 134/1-2, 43/1, 62/2, 53. maddeleri gereğince mahkûmiyet

Özel hayatın gizliliğini ihlal suçundan sanığın mahkumiyetine ilişkin hüküm, mahalli Cumhuriyet savcısı ve sanık tarafından temyiz edilmekle, dosya incelenerek gereği düşünüldü:

Bozma ilamına uyularak yapılan yargılamaya, toplanıp karar yerinde gösterilen delillere, mahkemenin kovuşturma sonuçlarına uygun olarak oluşan kanaat ve takdirine, incelenen dosya kapsamına göre, mahalli Cumhuriyet savcısının ve sanığın sair temyiz itirazlarının reddine, ancak;

İncelenen dosyada; katılan ...'nın 07.05.2013 tarihli şikayeti üzerine başlatılan adli soruşturma sonunda düzenlenen 30.05.2013 tarihli iddianamede, "...Müşteki ve şüphelinin resmi evli oldukları, evli oldukları ve ayrı yaşadıkları, şüpheli eşinin kaldığı eve çocuklarını görmeye gittiğinde 25/02/2013 - 11/01/2013 - 28/12/2012 ve 14/12/2012 tarihlerinde müştekinin evine gittiğinde cep telefonuna konuşmalarla ve evin görüntüleriyle ilgili kayıt aldığı..." ve bu şekilde sanık ...'in TCK'nın 134/1. madde ve fıkrasındaki özel hayatın gizliliğini ihlal suçunu işlediğinin iddia edildiği,

Yapılan yargılama sonunda, "...Sanığın müşteki ile resmi evli oldukları ancak ayrı yaşadıkları, olay günü sanığın müştekinin ayrı yaşadığı ikametine çocuklarını görmeye gittiğinde cep telefonu ile gizlice müştekinin özel hayatını ilgilendiren konuşmalarını ve evinin görüntülerini kayıt ederek bunları müşteki ile aralarında devam eden boşanma davasında delil olarak sunduğu, bu eylemlerini aynı kasıt altında birden fazla gerçekleştirdiği, bu şekilde müştekinin özel hayatının gizliliğini ihlal etmek suçunu işlediği..." kabulüne dayalı olarak sanık hakkında zincirleme şekilde özel hayatın gizliliğini ihlal suçundan mahkumiyet kararı verildiği,

Yerel mahkemenin 10.07.2014 tarihli mahkumiyet hükmünün, mahalli Cumhuriyet savcısı ve katılan tarafından temyiz edilmesi üzerine, Dairemizin 08.02.2017 tarihli ilamı ile diğerlerinin yanı sıra, "...Şikayete konu kayıtları içeren CD'lerin taraflar arasındaki boşanma davasının görüldüğü Ankara 9. Aile Mahkemesinin 2012/1002 Esas sayılı dosyasına sunulduğu anlaşılacakla, anılan mahkemeden

CD'ler istenip incelenerek ve söz konusu mahkemeye sunulan 27.03.2013 tarihli 25 sayfalık bilirkişi raporunun tamamının onaylı örneği dosyaya konularak, gerektiğinde yeniden alınacak bilirkişi raporu ve beyanlarla; çekimin mağdurun bilgisi ve rızası dışında yapılıp yapılmadığı, kaydedilen konuşmaların hangi tarihte, nerede ve kimler arasında geçtiği, kayda alınan konuşmaların özel bir gayret gösterilmeksizin başkaları tarafından da duyulabilen aleni konuşmalar olup olmadığı, mağdurun özel yaşam alanına ilişkin ve özel hayatının gizliliğini ihlal edecek nitelikte bir görüntünün ve/veya konuşmanın kaydedilip kaydedilmediği hususları açıklığa kavuşturulup, toplanan tüm deliller birlikte değerlendirilerek, sanığın hukuki durumunun takdir ve tayini gerektiği gözetilmeksizin, mağdur tarafından bir kısmı dosyaya sunulan onaysız fotokopiden ibaret 27.03.2013 tarihli bilirkişi raporu hükme esas alınıp, eksik incelemeye ve yetersiz gerekçelere dayalı olarak sanık hakkında zincirleme şekilde özel hayatın gizliliğini ihlal suçundan dolayı mahkumiyet kararı verilmesi..." nedenine dayalı olarak hükmün bozulduğu,

Sanık tarafından aile mahkemesine sunulan 2 adet CD'nin çözümüne ilişkin Dairemizin bozma ilamından sonra tamamı temin edilerek dosya içerisine konulan 27.03.2013 tarihli bilirkişi raporunda ve mahkemece yeniden alınan 25.10.2018 tarihli bilirkişi raporunda; "Şahin ... 14-12-2012, 28-12-2012, 11-01-2013, 25-12-2013 çocukları almaya gidiş kaydedilen görüntüler alamadığının kanıtıdır" ve "Hülya ... hakaret ve çocukları vermeyişi kaynana hakaret" olarak isimlendirilen 2 adet CD'de toplam 18 adet video kaydının tespit edildiği, iddianamede yazılı dava konusu edilen videolardan;

NorRec_11-01-2013 adını taşıyan ve 14.05.2009 tarihinde kaydedilen 5 dakika 8 saniyelik videoda, sanıkla arkadaşı olan tanık Osman'ın araçtan inip katılan ...'nın ziline bastıkları, sanığın diafondan seslendiği oğluna gelmesini istediği, çocuğun ısrara rağmen gelmek istemediğini söylemesinin ardından bir süre bina önünde bekledikten sonra kaydın sonlandığı, kayıta katılanın olmadığı,

NorRec_14-12-2012 adını taşıyan ve 17.04.2009 tarihinde kaydedilen 10 dakika 41 saniyelik videoda, sanıkla arkadaşı olan tanık Osman'ın katılan ...'nın kapısını çalıp, kapının açılmasının ardından sanığın çocuklarını almaya geldiğini söylediği, katılan ... tarafından, mahkemece yılın çift haftalarına tekabül eden günlerde çocuklarla babası arasındaki şahsi ilişki kurulduğunu beyanla olumsuz yanıt verilmesi üzerine başlayan tartışma esnasında katılan ...'nın tanık Osman'ı içeri davet ederek aile içi geçimsizliğin nedenlerinin sanığın olumsuz tutum ve davranışları olduğuna dair açıklamalarda bulunduğu, daha sonra sanık, tanık Osman, katılan ... ve katılan ...'nin annesinin konuştukları, karşılıklı konuşulması ve apartman boşluğunda yankı yapması nedeniyle konuşmalardan bir kısmının anlaşılamadığı,

NorRec-_25-01-2013 adını taşıyan ve 28.05.2019 tarihinde kaydedilen 3 dakika 29 saniyelik videoda, dış mekanda bina önünde çekim yapıldığı, çok az ses kaydı olmakla beraber parazitten dolayı konuşma içeriğinin anlaşılamadığı,

NorRec-_28-12-2012 adını taşıyan ve 30.04.2009 tarihinde kaydedilen 5 dakika 13 saniyelik videoda, sanıkla arkadaşı olan tanık Osman'ın katılan ...'nın evine gelip zile bastıkları, ardından çocukların verilip verilmeyeceği konusunda tartışma başladığı, çocuğun babasına gelmek istemediğini söylediği, konuşmalara katılan ...'nın annesi ve babasının da dahil olduğu, karşılıklı konuşulması ve apartman boşluğunda yankı yapması nedeniyle konuşmalardan bir kısmının anlaşılamadığı, katılan ...'nın bir ara "Cep telefonuyla iyi kaydet, iyi kaydet" dediği,

Dosyada mevcut Ankara 9. Aile Mahkemesinin 10.06.2013 tarihli, 2012/1002 esas, 2013/758 karar sayılı ilamı ve nüfus kayıt örneklerine göre, sanıkla katılanın 29.09.1998 tarihinde evlendikleri, 15.06.2000 tarihinde doğan Berk ve 23.06.2004 tarihinde doğan Belgin isimli müşterek iki çocukları olduğu, sanığın 2006 yılında açtığı boşanma davasının reddedildiği, tarafların 2006 yılından beri fiilen ayrı yaşadıkları, katılan tarafından 26.07.2012 tarihinde boşanma davası açıldığı, sanık tarafından çekimlerin katılanın henüz boşanma davası açmadığı ve tarafların fiilen ayrı oldukları dönemde yapıldığı, sanıkla katılanın 18.03.2014 tarihinde boşandıkları,

Katılanın, 20.03.2018 tarihli duruşmada, "... suça konu çekimler benim bilğim ve rızam dışında yapılmıştır, olay tarihinde Osman ... ile birlikte Şahin ... benim çocuklarımla birlikte kaldığım evime gelmişlerdi, benimle konuştukları sırada ... telefonla çekim yaptığını son anda fark ettim, bu çekimi benim oturduğum apartmanın daire kapısının önünde yapmışlardır, yani, çekimler apartmanın içinde, apartman koridorunda, daire kapımın önünde olmuştur... Boşanma sürecinde Aile Mahkemesine ibraz ettikleri görüşme kayıtlarının tamamı benim kapımın önünde yapılan çekimlere ilişkindir, bu konuşmalar benim sanık ve Osman ... adlı kişi ile ve oğlum Berk ... arasında geçen konuşmalardır, zaten kapıyı da oğlum Berk ... açmıştı, aramızda geçen konuşmaların istediği kısımlarını kayda alıyorlar istemediği kısımlarını da telefonun düğmesine basıyorlardı, bunu da son anda fark ettim, zaten karşı dairede de annem ve babam oturmaktadır..." biçiminde beyanda bulunduğu,

Sanığın; çocuklarını görmek istediğinde katılanın her defasında çeşitli bahanelerle buna engel olduğunu, kendisine iftiralar atıldığını, hakaret edildiğini, bu durumu delillendirmek amacıyla kayıt yaptığını, kayıtları sadece aile mahkemesinde delil olarak kullandığını, kayıtlardan katılanın bilgisinin bulunduğunu ifade ederek suçlamaları kabul etmediği, 28.08.2008 tarihinde açıp, feragat etmesi nedeniyle 08.06.2009 tarihinde reddedilen Ankara 7. Aile Mahkemesinin 2008/1035 esasına

kayıtlı ortak çocuklarla kişisel ilişki düzenlenmesine ilişkin dava dosyasındaki 10.04.2009 tarihli psikososyal değerlendirme raporunun fotokopisi ile Ankara 11. İcra Müdürlüğü'nün çocuk teslim zaptına ilişkin belge örneklerini savunmalarını desteklemek için sunduğu, uzman klinik psikolog ve sosyal hizmet uzmanı imzalı 10.04.2009 tarihli psikososyal değerlendirme raporunda, "...Yapılan görüşmeler, gözlemler ve dosya içindeki bilgiler bir arada değerlendirildiğinde, yaşanan sürece, eşlerin anlatımlarına ve müşterek çocukların durumuna bakıldığında; eşler arasındaki temel uyuşmazlığın, temel çatışmanın; Şahin Bey ve Hülya Hanım'ın ayrılmalarından sonra, Hülya Hanım'ın eşine yönelik bitmemiş duygularını çocukları üzerinden yaşayarak, eşinin çocukları görme isteminde, çocukların kendisinde olmasını bir 'güç' olarak görüp çocukların babaya gitmesi konusunda olumsuz düşünce ve duygularını çocuklarına yansıtarak onları etkilemesi ve örselemesi, çocuklarını babaya gitme konusunda teşvik etmek yerine sürekli eşi ve ailesinden şikayet etmesi, böylelikle çocuklarının korku yaşamasına da sebep olması, sürekli 'ben Şahin'in gelip çocuklarını görmesini, ilgilenmesini, mutlu çocuklar yetiştirmeyi istiyorum' demesine karşın, söylemlerini destekleyecek olan tutum, düşünce, duygu ve davranışlarının hep ters yönde olması, şahsi ilişki saatlerini bilmesine rağmen, kimi zaman babanın geleceği gün evde olmayıp kimi zaman kapıyı açmayarak 'aktif engelleyici tutumlar' ortaya koyarken, kimi zaman da 'dedesine gitmesinler', 'dersleri etkileniyor' gibi sözler ve çocuklarını gitmeye teşvik etmeyen tavırlarıyla 'pasif engelleyici tutumlar' sergilemesi olduğu düşünülmektedir... Hülya Hanım'ın, çocuklarının, Şahin Bey ile görüşmelerinde engelleyici tavrı devam ettirdiği takdirde, velayet hakkının gözden geçirilmesinin uygun olacağı düşünülmektedir..." ibarelerinin yer aldığı anlaşılmaktadır.

Özel hayat; kişinin sadece gözlerden uzakta, başkalarıyla paylaşmadığı, kapalı kapılar ardında, dört duvar arasındaki yaşantısı ve mahremiyetinden ibaret değil, herkesin bilmediği veya bilmemesi gereken, istenildiğinde başka kişilere açıklanabilen, tamamen kişiye özel hayat olayları ve bilgilerin tamamını içerir. Bu nedenle, kamuya açık alanda bulunulması, bu alandaki her görüntü veya sesin dinlenilmesine, izlenilmesine, kaydedilmesine, sürekli ve izinsiz olarak elde bulundurulmasına rıza gösterildiği anlamına gelmez. Kamuya açık alanda bulunulduğunda dahi, "kalabalığın içinde dikkat çekmezlik, tanınmazlık, bilinmezlik" prensibi geçerli olup, kamuya açık alandaki kişinin, gün içerisinde yapıkları, gittiği yerler, kiminle niçin, nasıl, nerede ve ne zaman görüştüğü gibi hususları tespit etmek amacıyla sürekli denetim ve gözetim altına alınması sonucu elde edilmiş bilgileri ya da onun başkalarınca görülmesi ve bilinmesini istemeyeceği, özel yaşam alanına girdiğinde şüphe bulunmayan faaliyetleri özel hayat kavramı kapsamına dahildir; ancak, süreklilik içermeyen ve özel yaşam alanına dahil olmayan olay ve bilgiler ise bu kapsamda değerlendirilemez. Sonuç olarak, bir olay ya da bilginin, özel hayat kapsamına girip girmediği belirlenirken, kişinin toplum içindeki

konumu, mesleği, görevi, kamuoyu tarafından tanınıp tanınmadığı, dışa yansıyan davranışları, rıza ve öngörülerini, içinde bulunduğu fiziki çevrenin özellikleri, sosyal ilişkileri, müdahalenin derecesi gibi ölçütler göz önüne alınmalıdır.

Kişiyeye bağlı ve onun kişisel gelişimiyle ilgili olan özel hayatın gizliliği hakkı, evlilikle tamamen ortadan kalkmaz. Tarafların evli olmaları ve aynı konutu paylaşmalarından dolayı birbirlerinin kişisel eşyalarına ve özel yaşam alanına giren hususlara kolayca ulaşabilme imkanına sahip bulunmaları, eşlerin hiçbir sınır olmaksızın birbirlerini sürekli gözetleyebileceği ve denetleyebileceği şeklinde yorumlanamaz. Ancak, kişinin, bir daha kanıt elde etme olanağının bulunmadığı ve yetkili makamlara başvurma imkanının olmadığı ani gelişen durumlarda, örneğin; kendisine karşı işlenmekte olan (cinsel saldırı, hakaret, tehdit, iftira veya şantaj gibi) bir suç söz konusu olduğunda ya da kendisine veya aile birliğine yönelen, onurunu zedeleyen, haksız bir saldırıyı önlemek için, kaybolma olasılığı bulunan kanıtların kaybolmasını engelleyip, yetkili makamlara sunarak güvence altına almak amacıyla, saldırıyı gerçekleştiren tarafın bilgisi ve rızası dışında, özel hayata ait bilgileri okuma, konuşma ve haberleşme içeriklerini veya özel hayata ilişkin ses ve görüntüleri dinleme, izleme ya da kaydetme, kişisel verileri kaydetme, ele geçirme ve yayma eylemlerinin hukuka aykırı olduğunu kabul etmek mümkün olmadığı gibi, esasen bu hallerde, kişinin hukuka aykırı hareket ettiği bilinciyle davrandığından da söz edilemez.

Bu açıklamalar ve incelenen dosya kapsamına göre; iddianamede yazılı dava konusu edilen videolardan NorRec_14-12-2012 adını taşıyan ve 17.04.2009 tarihinde kaydedilen 10 dakika 41 saniyelik video ile NorRec_28-12-2012 adını taşıyan ve 30.04.2009 tarihinde kaydedilen 5 dakika 13 saniyelik videodan katılanın çekim anında bilgisi bulunmasına rağmen TCK'nın 73/1. madde ve fıkrasında öngörülen 6 aylık sürede şikayette bulunmadığı gibi, kayıtların yapıldığı yer, çekim şekli ve ayrıntıları bilirkişi raporlarında yer alan içeriklerine göre, çözümü yapılan videolarda, katılanın sürekli denetim ve gözetim altına alınması sonucu elde edilmiş özel hayatının gizliliğini ihlale yol açacak herhangi bir konuşmasının ve görüntüsünün de kaydedilmediği; ayrıca, şikayete konu kayıtları, üçüncü kişi ya da kişilerle paylaştığı ve/veya çoğaltarak dağıttığına ilişkin hakkında bir iddia ileri sürülmeyen sanığın, çekim tarihlerine ve içeriklerine nazaran, çocuklarıyla görüşmesinin katılan tarafından engellendiğine dair iddialarını ispatlama amacını taşıyan eylemlerinde, hukuka aykırı hareket ettiği bilinciyle davrandığı da kabul edilemeyeceğinden, sanığa yüklenen özel hayatın gizliliğini ihlal suçundan sanığın CMK'nın 223/2-a madde, fıkra ve bendi gereğince beraatine karar verilmesi gerekirken, yasal ve yeterli olmayan gerekçelerle sanık hakkında zincirleme şekilde özel hayatın gizliliğini ihlal suçundan dolayı mahkumiyet kararı verilmesi,

2- Kabul ve uygulamaya göre de:

TCK'nın 134. maddesinin 1. fıkrasının 1. cümlesinde, kişilerin özel hayatının gizliliği ihlal edildiği takdirde, altı aydan iki yıla kadar hapis veya adli para cezası, aynı madde ve fıkranın ikinci cümlesinde, gizliliğin görüntü veya seslerin kaydedilmesi suretiyle gerçekleşmesi halinde, bir yıldan iki yıla kadar hapis veya adli para cezası öngörülmüş iken, suç tarihinden sonra, 05.07.2012 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren 6352 sayılı Yargı Hizmetlerinin Etkinleştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılması ve Basın Yayın Yoluyla İşlenen Suçlara İlişkin Dava ve Cezaların Ertelenmesi Hakkında Kanun'un 81. maddesi ile yapılan değişiklikle TCK'nın 134. maddesinin 1. fıkrasının 1. cümlesindeki ceza miktarı bir yıldan üç yıla kadar hapis cezası olarak belirlenmiş, aynı madde ve fıkranın ikinci cümlesi gereğince, gizliliğin görüntü veya seslerin kaydedilmesi suretiyle gerçekleşmesi halinde verilecek cezanın bir kat artırılacağı düzenlenmiş olup, TCK'nın 7/2. madde ve fıkrası gereğince, suçun işlendiği zamandaki kanun ile sonradan yürürlüğe giren kanunun ilgili tüm hükümlerinin somut olaya ayrı ayrı uygulanması ve her iki kanuna göre hükmedilecek sonuç cezalar belirlendikten sonra sanığın lehine olan kanunun tespiti ile lehe kanunun bir bütün halinde uygulanması ve bu durumun kararın gerekçesine yansıtılması suretiyle hüküm kurulması gerektiği gözetilmeden, dava konusu edilen çekimlerin 2009 yılında yapıldığı belirlenmesine rağmen sanığın lehine olan düzenleme tespit edilmeksizin, 6352 sayılı Kanunun 81. maddesi ile yapılan değişiklikten sonraki TCK'nın 134/1. madde ve fıkrası uyarınca yazılı şekilde hüküm kurulması,

Kanuna aykırı olup, mahalli Cumhuriyet savcısının ve sanığın temyiz itirazları bu itibarla yerinde görüldüğünden, hükmün bu nedenlerle 5320 sayılı Kanunun 8. maddesi uyarınca halen uygulanmakta olan 1412 sayılı CMUK'un 321. maddesi gereğince isteme aykırı olarak BOZULMASINA, 11.09.2019 tarihinde oybirliğiyle karar verildi.

Yargıtay Kararı - 12. Ceza Dairesi (E. 2017/2960)

Yargıtay 12. CD. 2017/2960 E., 2018/1541 K.

Esas No.: 2017/2960

Karar No.: 2018/1541

Mahkemesi: Asliye Ceza Mahkemesi

Suçlar: Verileri hukuka aykırı olarak verme veya ele geçirme, Tehdit

Hüküm: Verileri hukuka aykırı olarak verme veya ele geçirme suçundan beraat, tehdit suçundan TCK'nın 106/1-2. cümle, 62/1, 52, CMK'nın 231/5. maddeleri gereğince mahkumiyet

Verileri hukuka aykırı olarak verme veya ele geçirme suçundan sanığın beraatine ilişkin hüküm ile tehdit suçundan hükmün açıklanmasının geri bırakılmasına ilişkin karar, katılan vekili tarafından temyiz edilmekle, dosya incelenerek gereği düşünüldü:

1- Tehdit suçundan kurulan hükmün açıklanmasının geri bırakılmasına ilişkin karara yönelik temyiz isteminin incelenmesinde:

Hükmün açıklanmasının geri bırakılması kararının 5271 sayılı CMK'nın 231/12. maddesi uyarınca itiraz kanun yoluna tabi bulunduğu, aynı Kanununun 264. maddesi uyarınca kabul edilebilir bir başvuruda mercide yanılmanın başvuranın hakkını ortadan kaldırmayacağı nazara alınarak, katılan vekilinin temyiz isteminin, itiraz mahiyetinde değerlendirilmesi suretiyle CMK'nın 264/2. maddesi uyarınca gereği merciince yapılmak üzere dosyanın incelenmeksizin mahkemesine iadesinin temini için Yargıtay Cumhuriyet Başsavcılığına TEVDİİNE,

2- Verileri hukuka aykırı olarak verme veya ele geçirme suçundan kurulan hükme yönelik temyiz isteminin incelenmesinde:

TCK'nın 136/1. maddesinde belirli veya belirlenebilir bir kişiye ait her türlü bilginin, başkasına verilmesi, yayılması ya da ele geçirilmesi "Verileri hukuka aykırı olarak verme veya ele geçirme" başlığı altında suç olarak tanımlanmıştır.

Verileri hukuka aykırı olarak verme veya ele geçirme suçunun maddi konusunu oluşturan "kişisel veri" kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı nüfus bilgileri (T.C. kimlik numarası, adı, soyadı,

doğum yeri ve tarihi, anne ve baba adı gibi), adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir.

Ayrıntıları Yargıtay Ceza Genel Kurulunun 17.06.2014 tarihli, 2012/1510 esas, 2014/331 sayılı kararında da vurgulandığı üzere; TCK'nın 135 ve 136. maddelerindeki kişisel verilerin korunmasına ilişkin düzenlemelerde sadece sır niteliğinde kişisel verilerin korunacağına ilişkin bir hükmün bulunmaması ve aksine 135. maddenin gerekçesinde gerçek kişiyle ilgili her türlü bilginin kişisel veri olarak kabul edilmesi gerektiğinin belirtilmesi karşısında, her türlü kişisel verinin hukuka aykırı olarak başkasına verilmesi, yayılması ve ele geçirilmesi fiilleri TCK'nın 136. maddesindeki verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturur. Bu nedenle herkes tarafından bilinen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olan kişisel bilgiler de, yasal anlamda "kişisel veri" olarak kabul edilmektedir. Ancak, verileri hukuka aykırı olarak verme veya ele geçirme suçunun uygulama alanının amaçlanandan fazla genişletilerek, uygulamada belirsizlik ve hemen her eylemin suç oluşturması gibi olumsuz sonuçların doğmaması için, somut olayın özellikleri dikkate alınarak titizlikle değerlendirme yapılması, olayda herhangi bir hukuk dalı tarafından kabul edilebilecek bir hukuka uygunluk nedeni veya bu kapsamda nazara alınabilecek bir hususun bulunup bulunmadığının saptanması ve sanığın eylemiyle hukuka aykırı hareket ettiğini bildiği ya da bilebilecek durumda olduğunun da tespit edilmesi gerekir.

TCK'nın 136/1. maddesinin, "Bu madde hükmü ile hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek, bağımsız bir suç olarak tanımlanmıştır." şeklindeki gerekçesinden de anlaşılacağı üzere, kişisel verilerin, "verildiği", "yayıldığı" veya "ele geçirildiği"nin kabul edilebilmesi için, kişisel verilerin kaydedilmiş halde bulunması, kaydedilmiş haliyle başkalarına verilmesi, yayılması ya da ele geçirilmesi gerekir.

Bu noktada belirtmek gerekir ki, kişisel verilerin, üzerinde yazılı olduğu belgenin bulunduğu yerden alınması ya da kaydedilmiş haliyle başka bir nesne üzerine taşınarak (örneğin; yazının başka bir kağıt, defter vb. nesne üzerine geçirilmesi, taşınabilir belleğe veya CD'ye aktarılması gibi işlemlerle) sabitlenmesi, böylece istenildiğinde tekrar kullanılabilmesi olanağını sağlayan her türlü faaliyet, kişisel verileri "ele geçirme" kapsamında değerlendirilebilir ise de, kişisel verilerin kaydedilmeden

önce öğrenilmesi, hafızada tutulan kişisel verilerin başkalarına açıklanması, kişisel verilere salt duyu organları aracılığıyla vakıf olunması, ancak TCK'nın 134/1. maddesinin 1. cümlesinde düzenlenen özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilebilir.

Bu açıklamalar ışığında incelenen dosya kapsamına ve ikrar içeren savunmaya göre; sanığın, bir dönem internet üzerinden tanışıp arkadaş olduğu katılanın daha önce kendi facebook hesabında paylaştığı resimleri, katılan ile tartışmaları nedeniyle katılan adına açtığı sahte facebook hesabından katılanın rızası dışında yayınladığı iddia edilen olayda, katılanın gündelik kıyafetler ile kamuya açık alanda çekilmiş ve kişisel veri niteliğindeki resimlerini daha önce kendi facebook hesabında yayımlamasının bu resimlerin kişisel veri olma özelliğini değiştirmeyeceği gibi üçüncü kişilere katılanın rızası dışında yayınlama hakkı da tanımayacağı gözetilmeden sanık hakkında verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyetine karar verilmesi gerekirken delillerin takdirinde yanılığa düşülerek yazılı şekilde sanığın beraatine karar verilmesi,

Kanuna aykırı olup, katılan vekilinin temyiz itirazları bu itibarla yerinde görüldüğünden, hükmün bu nedenle 5320 sayılı Kanununun 8. maddesi uyarınca halen uygulanmakta olan 1412 sayılı CMUK'un 321. maddesi gereğince isteme uygun olarak BOZULMASINA, 14.02.2018 tarihinde oybirliğiyle karar verildi.

Yargıtay Kararı - 12. Ceza Dairesi (E. 2015/13758)

Yargıtay 12. CD., E. 2015/13758 K. 2017/2514 T. 29.3.2017

Esas No.: 2015/13758

Karar No.: 2017/2514

Karar tarihi: 29.03.2017

Mahkemesi: Asliye Ceza Mahkemesi

Suç: Verileri hukuka aykırı olarak verme veya ele geçirme

Hüküm: Beraat

Verileri hukuka aykırı olarak verme veya ele geçirme suçundan sanıkların beraatine ilişkin hüküm, katılan tarafından temyiz edilmekle, dosya incelenerek gereği düşünüldü:

Yapılan yargılama sonunda, yüklenen fiilin kanunda suç olarak tanımlanmamış olduğu gerekçeleri gösterilerek mahkemece kabul ve takdir kılınmış olduğundan, katılanın, sanıkların subut bulan eylemlerine, cezalandırılmalarına ilişkin temyiz itirazlarının reddiyle, beraate ilişkin hükmün isteme uygun olarak ONANMASINA, 29.03.2017 tarihinde oyçokluğuyla karar verildi.

KARŞI OY

07/04/2016 tarihli Resmi Gazete de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanununun 3/1-(d). maddesinde kişisel veri, kimliği belirli ve belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmıştır. Kişilerin, sadece insan olması ve toplumdaki yeri; bazı değerleri kişisel veri haline getirmektedir. Kişinin adı, adresi, kimlik bilgileri, medeni durumu gibi özellikleri kişisel veri kapsamındadır. Bunun yanında teknolojik gelişmeler nedeniyle gittikçe karmaşıklaşan toplum hayatındaki bir takım bilgiler de kişisel veri haline gelmiştir. Örneğin, vatandaşlık numarası, banka hesap numarası, telefon numarası, elektronik posta adresi ve şifresi gibi kişisel bilgiler. Dolayısıyla farklı gruplandırmalar bulunmakla birlikte kişisel verilerin iki başlık altında toplanması mümkündür. Birinci grupta, insanın varoluşundan kaynaklanan kişiliğine ait bilgiler, ikinci grupta ise; teknolojinin gelişmesiyle insanın modern toplumda yer alması nedeniyle kendisine verilen ya da çeşitli hizmetlere ulaşmasında kullanılan bilgiler yer almaktadır. Ancak her iki grupta yer alan bilgilerin de kişisel veri olarak hukuk düzenindeki değeri ve korunmaları açısından bir fark bulunmamaktadır.

TCK'nın 136. maddesindeki “verileri hukuka aykırı olarak verme veya ele geçirme” suçu, seçimlik hareketli bir suç olarak nitelenmiştir. Hukuka aykırı olarak kişisel verilerin başkasına verilmesi, kişisel verilerin yayılması ve kişisel verilerin ele geçirilmesi şeklindeki seçimlik hareketlerinden birinin gerçekleştirilmesi ile suç işlenmiş olacaktır. “Kişisel verileri bir başkasına verme” seçimlik hareketinde, maddede geçen “başkası” gerçek bir kişi olabileceği gibi tüzel kişide olabilecek, veriler bu kişilere elden, posta ya da internet üzerinden elektronik posta ile vb. şekillerde verilebilecektir. Türk Dil Kurumu Büyük Türkçe Sözlüğünde “vermek”; “üzerinde, elinde veya yakınında olan bir şeyi birisine eriştirmek, iletmek, düşünce veya bilgi anlatan şeyleri başkalarına iletme, bildirmek” şeklinde açıklanmıştır. Bu seçimlik harekette verilerin hukuka uygun ya da aykırı yöntemle elde edilmiş olmasının önemi bulunmamakta olup, önemli olan husus verme eyleminin hukuka aykırı olmasıdır.

Bu açıklamalar ışığında uyuşmazlık konusu değerlendirildiğinde;

Türkiye Görme Engelliler Derneği Mersin Şubesi üyesi olan katılanın, kişisel veri niteliğinde bulunan kimlik bilgilerinin, katılan rızası dışında başkalarına öğrenilmesine neden olacak şekilde bir siyasal partiye verilerek bilgisi dışında üye yapılması hususları birlikte değerlendirildiğinde, sanıkların eylemi TCK'nın 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak yayma suçunu oluşturduğunun gözetilmemesi karşısında sayın çoğunluğun görüşüne katılmıyoruz.

Yargıtay Kararı - 12. Ceza Dairesi (E. 2015/13582)

Sosyal medya sitesinde mağdurların rızalarına aykırı şekilde fotoğraf paylaşılmasının verileri hukuka aykırı olarak verme veya ele geçirme suçu oluşturacağına ilişkin Yargıtay kararı

Yargıtay 12. CD., E. 2015/13582 K. 2017/3109 T. 12.4.2017

Esas No.: 2015/13582

Karar No.: 2017/3109

Karar Tarihi: 12.04.2017

Mahkemesi: Asliye Ceza Mahkemesi

Suç: Özel hayatın gizliliğini ihlal

Hükümler: Beraat

Özel hayatın gizliliğini ihlal suçundan sanığın beraatine ilişkin hükümler, mahalli Cumhuriyet savcısı tarafından temyiz edilmekle, dosya incelenerek gereği düşünüldü:

Mahalli Cumhuriyet savcısının sair temyiz itirazlarının reddine, ancak;

Sanık ...'ın, öz kızı olan mağdur ... ile diğer mağdur ... evlendikten sonra, her iki mağdurla aralarında başlayan husumetten dolayı mağdurlara tepki olarak, facebook adlı sosyal paylaşım sitesinde kendi ismini kullanarak açtığı hesap üzerinden, mağdur ...'nin bekarken çektiği ve diğer mağdur ...'ın temin ettiği resimlerini, onların uyarılarını dikkate almaksızın, rızalarına aykırı şekilde paylaştığı iddiasına konu olayda,

Mağdurların günlük kıyafetleriyle poz vermiş şekilde çektikleri resimleri, mağdurların başkaları tarafından görülmesini ve bilinmesini istemeyecekleri özel yaşam alanlarına ilişkin görüntüler olarak kabul edilemeyeceğinden, mağdurların kişisel veri niteliğindeki resimlerini, hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle facebook hesabı üzerinden yayımlayan sanığın eylemlerinin, TCK'nın 136/1. madde ve fıkrasında tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı gözetilmeden, eylemler salt özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilip, yasal ve yeterli olmayan yazılı gerekçelerle sanık hakkında beraat hükümleri kurulması,

Kanuna aykırı olup, mahalli Cumhuriyet savcısının temyiz itirazları bu itibarla yerinde görüldüğünden, hükümlerin bu nedenle 5320 sayılı Kanunun 8. maddesi uyarınca halen uygulanmakta olan 1412 sayılı CMUK'un 321. maddesi gereğince isteme aykırı olarak BOZULMASINA, 12.04.2017 tarihinde oybirliğiyle karar verildi.

Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -
Yargıtay Kararı -

Yargıtay Kararı - 12. Ceza Dairesi (E. 2013/9043)

Kişisel veri kavramından hangi bilgilerin anlaşılması gerektiğine ilişkin Yargıtay kararı

Yargıtay 12. CD., E. 2013/9043 K. 2014/151 T. 13.1.2014

Esas No.: 2013/9043

Karar No.: 2014/151

Karar Tarihi: 13.01.2014

Tebliğname No: 12 - 2012/61319

Mahkemesi: İzmir 2. Asliye Ceza Mahkemesi

Karar Tarihi: 28.11.2011

Numarası: 2011/210 - 2011/687

Kişisel verileri, hukuka aykırı olarak ele geçirmek veya yaymak suçundan sanığın beraatine ilişkin hüküm, katılan tarafından temyiz edilmekle, dosya incelenerek gereği düşünüldü:

Belirli veya belirlenebilir bir kişiye ait her türlü bilginin, başkasına verilmesi, yayılması ya da ele geçirilmesi, TCK'nın 136/1. maddesinde "Verileri hukuka aykırı olarak verme veya ele geçirme" başlığı altında suç olarak tanımlanmış olup, eylemin; kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle gerçekleşmesi hali, aynı Kanununun 137. maddesinde cezada artırım nedeni olarak öngörülmüştür.

Verileri hukuka aykırı olarak verme veya ele geçirme suçunun maddi konusunu oluşturan "kişisel veri" kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı nüfus bilgileri (T.C. kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi), adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir; ancak, herkes tarafından bilinen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olan kişisel bilgiler, yasal anlamda "kişisel

veri" olarak değerlendirilemez, aksinin kabulü; anılan maddenin uygulama alanının amaçlanandan fazla genişletilerek, uygulamada belirsizlik ve hemen her eylemin suç oluşturması gibi olumsuz sonuçlar doğurur, bu nedenle, bir kişisel bilginin, açıklanan anlamda "kişisel veri" kabul edilip edilmeyeceğine karar verilirken, somut olayın özellikleri dikkate alınarak titizlikle değerlendirme yapılması, sanığın eylemiyle hukuka aykırı hareket ettiğini bildiği ya da bilebilecek durumda olduğunun da ayrıca tespit edilmesi gerekir.

Bu açıklamalar ışığında, yapılan yargılamaya, toplanıp karar yerinde gösterilen delillere, mahkemenin kovuşturma sonuçlarına uygun olarak oluşan kanaat ve takdirine, incelenen dosya kapsamına göre;

1- Katılanın, 17.08.2010 tarihinde, bilgisi ve rızası dışında, adına bir arkadaşlık sitesinde üyelik işlemleri yapılarak profil oluşturulan sitede, "benherbaharaşıkolum" adı ile oluşturulan profile katılana ait cep telefonu numarasının yazıldığı ve bu profil üzerinden tanımadığı kişilerin kendisini telefonundan arayarak arkadaşlık isteğinde buldukları iddiasını içeren şikayet dilekçesi üzerine başlatılan adli soruşturma kapsamında, arkadaşlık sitesinin sahibi olan şirketten gelen yazı içeriğine göre, katılanın kişisel bilgilerinin yer aldığı profilin 17.08.2010 tarihinde oluşturulup siteye üye yapıldığı, bu işlemin ise "88.240.143.129" IP numaralı bilgisayar üzerinden gerçekleştirildiği, katılanın durumu öğrenip üyelik işlemini iptal ettirmesi üzerine başka IP numaralarını içeren bilgisayarlar tarafından da üye bilgilerine girilmeye çalışıldığının bildirildiği, konuyla ilgili olarak, Türk Telekomünikasyon A.Ş.'den gelen yazıda ise, üyelik işlemleri için kullanılan ve üyelik iptal edildikten sonra profile ulaşmaya çalışan bilgisayarlara ait IP numaralarının, sanığa ait "0.232.339.74.24" telefon numaralı ADSL hattı üzerinden internet erişiminin gerçekleştirildiğinin bildirildiği, ayrıca sanığın eşi olan tanık Semra Altun'un, dosya içerisine de getirilen ve takipsizlik kararı ile sonuçlanan başka bir soruşturma dosyasında, katılan ile şüpheli şahıs arasında doğan ihtilafta tanık olarak ifade verdiği, verdiği ifadesinde katılan ve ailesi hakkında ayrıntılı bilgilere de sahip olduğu anlaşıldığı halde, delillerin takdirinde hataya düşülerek, sanığın atılı suçtan mahkumiyeti yerine yazılı şekilde beraatine karar verilmesi kanuna aykırı,

2- Hükümden sonra 05.07.2012 tarihli Resmi Gazete'de yayınlanarak yürürlüğe giren 6352 sayılı Yargı Hizmetlerinin Etkinleştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılması ve Basın Yayın Yoluyla İşlenen Suçlara İlişkin Dava ve Cezaların Ertelenmesi Hakkında Kanununun Geçici 1. maddesinin, "31/12/2011 tarihine kadar, basın ve yayın yoluyla ya da sair düşünce ve kanaat açıklama yöntemleriyle işlenmiş olup; temel şekli itibarıyla adlî para cezasını ya da üst sınırı beş yıldan fazla olmayan hapis cezasını gerektiren bir suçtan dolayı; a) Soruşturma evresinde, 4/12/2004 tarihli ve 5271

sayılı Ceza Muhakemesi Kanununun 171 inci maddesindeki şartlar aranmaksızın kamu davasının açılmasının ertelenmesine, b) Kovuşturma evresinde, kovuşturmanın ertelenmesine, c) Kesinleşmiş olan mahkûmiyet hükmünün infazının ertelenmesine, karar verilir.” hükmü gereğince, TCK'nın 7/2. maddesi uyarınca, sanığın hukuki durumunun yeniden tayin ve takdirinde zorunluluk bulunması, Bozmayı gerektirmiş olup, katılanın temyiz itirazları bu itibarla yerinde görüldüğünden, hükmün bu sebeplerden dolayı 5320 sayılı Kanunun 8. maddesi uyarınca halen uygulanmakta olan 1412 sayılı CMUK'un 321. maddesi gereğince isteme uygun olarak BOZULMASINA, 13.01.2014 tarihinde oybirliğiyle karar verildi.

Yargıtay Kararı - 12. Ceza Dairesi (E. 2014/607)

Kişisel veri niteliğindeki telefon numarasının rıza dışında paylaşılması verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı hakkında Yargıtay kararı

Yargıtay 12. CD., E. 2014/607 K. 2014/16665 T. 7.7.2014

12. CD., E. 2014/607 K. 2014/16665 T. 7.7.2014

Esas No.: 2014/607

Karar No.: 2014/16665

Karar Tarihi: 07.07.2014

Tebliğname No: 12 - 2013/133761

Mahkemesi: Giresun 2. Asliye Ceza Mahkemesi

Tarihi: 22.02.2013

Numarası: 2012/351-2013/111

Suç: Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme

Verileri hukuka aykırı olarak verme veya ele geçirme suçundan sanıkların beraatlerine ilişkin hükümler, katılan vekili tarafından temyiz edilmekle, dosya incelenerek gereği düşünüldü:

Belirli veya belirlenebilir bir kişiye ait her türlü bilginin, başkasına verilmesi, yayılması ya da ele geçirilmesi, TCK'nın 136/1. maddesinde "Verileri hukuka aykırı olarak verme veya ele geçirme" başlığı altında suç olarak tanımlanmış olup, eylemin; kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle gerçekleşmesi hali, aynı Kanununun 137. maddesinde cezada artırım nedeni olarak öngörülmüştür.

Verileri hukuka aykırı olarak verme veya ele geçirme suçunun maddi konusunu oluşturan "kişisel veri" kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı nüfus bilgileri (T.C. kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi), adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya

belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir. Herkes tarafından bilinen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olan kişisel bilgiler de, yasal anlamda “kişisel veri” olarak kabul edilmekte ise de, anılan maddenin uygulama alanının amaçlanandan fazla genişletilerek, uygulamada belirsizlik ve hemen her eylemin suç oluşturması gibi olumsuz sonuçların doğmaması için, maddenin uygulamasında, somut olayın özellikleri dikkate alınarak titizlikle değerlendirme yapılması, olayda herhangi bir hukuk dalı tarafından kabul edilebilecek bir hukuka uygunluk nedeni veya bu kapsamda nazara alınabilecek bir hususun bulunup bulunmadığının saptanması ve sanığın eylemiyle hukuka aykırı hareket ettiğini bildiği ya da bilebilecek durumda olduğunun da ayrıca tespit edilmesi gerekir.

TCK'nın 136/1. maddesinin, “Bu madde hükmü ile hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek, bağımsız bir suç olarak tanımlanmıştır.” şeklindeki gerekçesinden de anlaşılacağı üzere, kişisel verilerin, “verildiği”, “yayıldığı” veya “ele geçirildiği”nin kabul edilebilmesi için, kişisel verilerin kaydedilmiş halde bulunması, kaydedilmiş haliyle başkalarına verilmesi, yayılması ya da ele geçirilmesi gerekir. Kişisel verilerin kaydedilmeden önce öğrenilmesi, hafızada tutulan kişisel verilerin başkalarına açıklanması, kişisel verilere salt duyu organları aracılığıyla vakıf olunması, ancak TCK'nın 134/1. maddesinin 1. cümlesinde düzenlenen özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilebilir.

Bu açıklamalar ışığında somut olay incelendiğinde, sanık Turgut'un, ayrıldığı kız arkadaşı olan şikayetçinin, kendisinde kayıtlı olan kişisel veri niteliğindeki telefon numarasını, şikayetçinin rızası dışında diğer sanık Onur'a verdiği olayda; şikayetçinin telefon numarasını hukuka aykırı olarak yayan sanık Turgut ile telefon numarasını hukuka aykırı olarak ele geçiren sanık Onur'un eyleminin, TCK'nın 136/1. maddesine uyan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı gözetilmeden, ayrı ayrı mahkumiyetleri yerine, “telefon numarası vermek şeklinde gerçekleşen eylemin kişisel verilerin ele geçirilmesi ve yayılması olarak değerlendirilemeyeceği” biçimindeki isabetsiz gerekçeyle beraatlerine karar verilmesi,

Kanuna aykırı olup, katılan vekilinin temyiz itirazları bu itibarla yerinde görüldüğünden, hükmün bu sebepten dolayı 5320 sayılı Kanununun 8. maddesi uyarınca halen uygulanmakta olan 1412 sayılı CMUK'un 321. maddesi gereğince isteme aykırı olarak BOZULMASINA, 07.07.2014 tarihinde oyçokluğuyla karar verildi.

KARŞI OY YAZISI:

Sanık Turgut'un, kendisinde kayıtlı katılana ait telefon numarasını diğer sanık Onur'a vermesi şeklinde gerçekleşen olayda, mahalli mahkemenin kişisel verileri verme ve ele geçirme suçunun oluşmadığına dair beraat kararı, dairesimiz çoğunluğunca eylem TCK'nun 136/1. maddesi kapsamında kişisel verileri hukuka aykırı olarak verme ve ele geçirme olarak değerlendirilip hüküm bozulmuştur. Biz aşağıdaki gerekçelerle bozma içeren düşünceye katılmıyoruz.

İtiraz gerekçelerimiz; Türk Ceza Kanunu'nda kişisel verilerle ilgili bir tanım ve sınırlandırmanın yapılmaması nedeniyle kişisel verilerle ilgili maddeler suçta ve cezada kanunilik ilkesini ihlal ettiğinden Anayasa'ya aykırı oldukları, tanım yapılmamasının sınırlarını suçta ve cezada kanunilik ve belirlilik ilkesi nazara alınarak belirlenmesi ve son olarak ta eylemin özel kanunlardaki düzenlemeler nazara alınarak çözümlenmesi ve bu haliyle ceza hukuku alanında değerlendirilemeyeceği başlıklarında olacaktır.

Bunlar;

1-Yürürlükteki mevzuatta kişisel veri tanımının yapılmadığı gözetildiğinde kişisel verilerle ilgili suçların düzenlendiği TCK'nın 135 ve 136. maddeleri suçta ve cezada kanunilik ve belirlilik (açıklık) ilkesine uymadığından Anayasa'ya aykırıdır. Kişisel verilerle ilgili suç düzenlemeleri ilk olarak 01 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı TCK'nın 135, 136 ve 138. maddeleri ile ceza mevzuatımıza girmiştir. TCK'nın 135. maddesinde kişisel verilerin kaydedilmesi, 136. maddesinde verileri hukuka aykırı olarak verme veya ele geçirme, 138. maddesinde ise verileri yok etmeme suçları düzenlenmiştir.

Kişisel verilerin kaydedilmesinin düzenlendiği 135. maddenin gerekçesinde "Suçun konusu kişisel verilerdir. Gerçek kişiyle ilgili her türlü bilgi, kişisel veri olarak kabul edilmelidir." şeklinde bir açıklama bulunmaktadır.

Peki, kişiyle ilgili her türlü bilgiler nelerdir. Bunların bir kısmını sıralayacak olursak:

Kişinin; Türkiye Cumhuriyeti kimlik numarası, adı, soyadı, doğum tarihi, doğum yeri, nüfusa kayıtlı olunan yer (İl, İlçe, mahalle veya köy), anne ve baba adı, medeni hali (Evli, bekâr, boşanmış), nüfusa kayıtlı olduğu cilt ve aile sıra no, kan grubu, evlenme tarihi, boşanma tarihi ve mahkeme kararı bilgileri, adı-soyadı veya diğer kayıt düzeltmeleri, vatandaşlıktan çıkarılma bilgileri, evlatlık ilişkisi, adresi, dini, bitirilen okullar (ilk-orta-yüksek), hastalıkları, hastalıkları ile ilgili tahlil sonuçları (DNA bilgileri), mali durumu (servet, aldığı ücretler), ahlaki eğilimleri, zaafı, çevre ile ilişkileri, hatıra, anı ve günlükle ilgili defterindeki bilgileri, siyasi görüşü (oy verdiği partiler, üye olduğu dernekler), alışkanlıkları, sevdiği kitaplar veya gazeteler, alışveriş eğilimleri, vergi numarası, e posta adresi ve

şifresi, banka bilgileri, bilgisayarının IP numarası, emeklilik ve kurum sicil numarası, aldığı ödüller, parmak izi, avuç içi izleri, mektupları, yazıları, kitapları, telefon numaraları, mesajları, fiziki kimliği (boy, kilo, engellilik durumu, ten rengi, göz rengi, saç rengi ve şekli, sesi, genel görünüm, ayak ve beden numarası) ve çok daha fazla bilgi kişisel veri kapsamında değerlendirilebilecektir.

Acaba bu kadar bilgilerden hangilerinin kaydı veri olarak kabul edilip kayda alınması (TCK, m.135) ve hukuka aykırı olarak verme veya ele geçirme suçu olarak (TCK, 136) kabul edilip üst sınırı 4 yıla kadar hapis cezası ile bu suçları işleyenler cezalandırılacaktır. Bilgilerden de anlaşılacağı gibi, bunların büyük bir çoğunluğu herkes tarafından bilinmektedir. O halde herkes tarafından maruf ve meşhur olan kişiyle ilgili bir bilgiyi kaydetmenin, birisine vermenin veya yaymanın suç olarak cezalandırılması nasıl olacaktır. İşte burada karşımıza bu suçları işleyenler bakımından tanım yapılmamasının zararı olan suçta ve cezada kanunilik ve belirlilik ilkesinin ihlali çıkmaktadır. (Veli Özer Özbek, Mehmet Nihat Kambur, Koray Doğan, Pınar Bacaksız, İlker Tepe, Türk Ceza Hukuku, Özel Hükümler, 2.B, Ankara 2011, s.517)

Anayasa Mahkemesi suçta ve cezada kanunilik ve belirlilik ilkesine bağlı kalınmasının gerekliliğine kararlarında vurgular yapmaktadır. (Anayasa Mahkemesinin, 7.7.2011/69-116 sayılı kararı)

Bilimsel görüşlere baktığımızda da belirlilik ilkesinin önemli ve vazgeçilmez bir ilke olduğu kabul edilmektedir. (Mahmut Koca, İlhan Üzülmöz, Türk Ceza Kanunu Genel Hükümler, 6.Baskı, Ankara 2013, s.51)

Avrupa İnsan Hakları Mahkemesi de verdiği birçok kararında belirlilik ilkesinin suç içeren hükümlerde bulunmasını aramıştır. (İnsan Hakları Avrupa Mahkemesi; Sunday Times/Birleşik Krallık Kararı; 6.11.1980/6538/74; ATAD, 23 Kasım 1999, Arblade ve Leloup Kararı, C.369/96 ve 376/96, Zikreden MANACOR-DA, 115, Avrupa Birliği Ceza Hukukunun Esasları, Ümit Kocasakal, İstanbul 2004, s. 157; Osman Doğru, Atilla Nalbant, İnsan Hakları Avrupa Sözleşmesi, Açıklama ve Önemli Kararlar, Ankara 2013, s.269)

İşte veri tanımının yapılmaması nedeniyle suçta ve cezada kanunilik ve açıklık ilkesi gereği veri ile ilgili suç düzenlemeleri Anayasaya aykırıdır. Bu hususun mahalli mahkemece, temyiz incelemesi yapan dairemizce de Anayasaya aykırı olduğu ve iptali gerekçesiyle Anayasa Mahkemesine götürülmesi gerekirdi.

2-Ceza hukuku uygulamasında kişisel veri kavramının sınırlarının çizilmesi gerekir.

Suç içeren bu hükümlerdeki belirsizliği, suçla orantılı ceza uygulanmasının gerekliliği ilkesini taşımadığını gören bilim adamları suç olarak kabul edilebilecek kişisel verilerin kaydının sadece

TCK'nın 135/2. maddesindeki bilgilerin (Kişilerin, siyasi, felsefi veya dinî görüşler, ırkî kökenler, ahlâkî eğilimler, cinsel yaşamları, sağlık durumları veya sendikal bağlantılarına ilişkin bilgiler) veri olarak kabul edilebileceği, bunların dışındaki bilgilerin suç kapsamında değerlendirilemeyeceği yönünde bilimsel görüşler ileri sürmüşlerdir. (Zeki Hafızoğulları, Muharrem Özen, Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar, Ankara Barosu Dergisi, Yıl 67, sayı 4, 2009, s.9)

Herkes tarafından bilinen veya kolaylıkla bilinmesi mümkün verileri bu kapsamda kabul etmek, maddenin kapsamının dayanılmaz ölçüde genişletmek anlamına geleceğinden "kişisel veri" kavramını bu anlamda dar yorumlamakta zorunluluk vardır. (Hakan Hakeri, Tıp Hukuku, Ankara, 5.B, 2012, s.755)

Kişisel verilerin ceza hukuku anlamında suç konusu olabilmeleri, hassas kişisel bilgiler (veriler) hariç, şu şekilde bir sınırlamaya tabi tutarak suçta ve cezada kanunilik ve belirlilik ilkesine uymayan hükmü kısmen adaletli bir uygulamaya sokabiliriz. O da suç düzenlemelerinin yer aldığı bölüm başlığından hareketle özel hayata ve hayatın gizli alanına ait olup, kişinin başkaları ile paylaşmadığı ve alenileştirmedeği kişisel bilgiler olarak anlamak gerekir.

Buna göre kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, dernek, vakıf ya da sendika üyeliği, sağlığı veya cinsel hayatı ile ilgili verilerinin kaydı, bir başkasına verilmesi veya ele geçirilmesi bunlar hassas veriler oldukları için mutlak olarak cezai yaptırımlarla korunmaları gereken kişisel verilerdir.

Bu kapsamda kişilerle ilgili bilginin; ilgili kişi tarafından alenileştirilmemiş, üçüncü kişilerle paylaşılmamış, bilinmesinin kişinin yaşam şekline, ekonomik ve finansal ve bilişim alanına zarar verme ihtimali bulunan bilgiler olması halinde kişisel verilerle ilgili suçların konusunu oluşturmalı. Bunun dışında kalan kişilerle ilgili diğer bilgiler ise ancak kullanım amacına göre hakaret, dolandırıcılık gibi suçların konusu olmalı ve hukuki ve idari yollarla korunmalıdır.

Ceza hukukunun konusu olabilecek kişisel verilerin sınırları bu şekilde çizilmiş olsaydı, telefon numarasının bu kapsamda yani kişisel veri olarak değerlendirilemeyeceği anlaşılacaktı.

3-Dava konusu olayda, TCK'nın 136. maddesi anlamında kişisel veriyi verme veya ele geçirme söz konusu değildir.

Katılan daha önce telefon numarasını rızasıyla sanık Turgut'a vermiştir. Halen kanunlaşmayı bekleyen Kişisel Verileri Koruma Kanun tasarısının 5. maddesi, ilgili kişinin kendisi tarafından alenileştirilmiş bilginin ilgili kişinin açık rızası aranmaksızın işlenebileceğini kabul etmiştir. Bir

eylemin suç olarak kabul edilip cezalandırılabilmesi için o eylemin toplumda en azından haksızlık oluşturduğu veya hoş karşılanmadığına dair bir kanının bulunması gerekir.

Telefon numarasının verilmesi veya alınmasını yasaklayan açık bir düzenleme bulunmayan bir alanda yorumla suç oluşturulmaktadır. Birisine telefon numarası vermenin ve almanın suç olduğunu kabul ile eylem kamu adına soruşturulan bir suç olarak karşımıza çıkmaktadır. Bu suçlarda ilgilinin rızası önemli değildir (TCK, m.26/2), suç soruşturması ve kovuşturması şikâyete tabi olmadığından mağdurun üzerinde tasarrufta bulunabileceği bir hakkın var olduğu söylenemez. Bu suçlar bakımından bireyin değil, kamunun menfaatlerinin ağır bastığı kabul edilmiştir. Dolayısıyla bu suç bakımından ilgilinin rızası hukuka uygunluk sebebi değildir. (Veli Özer Özbek, Mehmet Nihat Kambur, Koray Doğan, Pınar Bacaksız, İlker Tepe, Türk Ceza Hukuku, Özel Hükümler, 2.B,Ankara 2011, s.521)

Katılan şu aşamada şöyle bir beyanda bulunsa, “telefonumun verilmesi veya ele geçirilmesi nedeniyle yapılan kovuşturma nedeniyle şikayetçi değilim ” beyanı karşısında bu kovuşturmayı kamu adına takip ettirmede kamu menfaatlerinin ağır bastığı hangi durum vardır?

Tüm açıkladığımız bu nedenlerden dolayı mahalli mahkemenin beraat kararının yerinde olduğunu düşündüğümüzden sayın çoğunluğun telefon numarasını alma veya vermeyi TCK 136. madde kapsamında suç olarak değerlendiren görüşüne katılmıyoruz.

Yargıtay Kararı - 7. Ceza Dairesi (E. 2021/21566)

Yargıtay 7. CD., E. 2021/21566 K. 2021/13832 T. 12.10.2021

Esas No.: 2021/21566

Karar No.: 2021/13832

Karar Tarihi: 12.10.2021

5253 sayılı Dernekler Kanunu'nun 32/d maddesine muhalefet etmekten kabahatli ... hakkında ... Kaymakamlığının 07/08/2020 tarihli ve 63485207-450-E.3042 sayılı idarî para cezası karar tutanağı ile uygulanan 1.586,19 Türk lirası idarî para cezasına karşı yapılan başvurunun reddine ilişkin Sulh Ceza Hâkimliğinin 07/10/2020 tarihli ve 2020/3257 değişik iş sayılı kararı aleyhine Yüksek Adalet Bakanlığından verilen 03.05.2021 tarihli kanun yararına bozma istemini içeren dava dosyası Yargıtay Cumhuriyet Başsavcılığının 01.07.2021 tarihli ve KYB. 2021-70336 sayılı ihbarnamesi ile daireye verilmekle okundu.

Mezkür ihbarnamede;

Dosya kapsamına göre, dernek gelirlerinin tahsilinde kullanılan alındı belgelerinin üzerinde ödenti veya bağışta bulunan gerçek kişilerin T.C. kimlik numaralarının ve tüzel kişilerin vergi numaralarının yazılmadığından bahisle idarî para cezası uygulanmasına karar verildiği anlaşılmakta ise de;

1- 5253 sayılı Kanun'un 17. maddesinde yer alan "Derneklerin iş ve işlemlerinde, bu Kanun ve 4721 sayılı Türk Medenî Kanunu ile bunlara dayanılarak çıkarılan yönetmeliklerin hükümlerine aykırılık tespit edilmesi halinde, konusu suç teşkil etmeyen hata ve noksanlıkların mülkî idare amirinin yazılı istemi üzerine, ilgili dernek tarafından otuz gün içerisinde giderilmesi zorunludur." şeklindeki düzenleme uyarınca, eksiklikler bakımından ilgili derneğe hata ve noksanlıkların giderilmesi için belirtilen süre verilmesine rağmen hata ve eksikliğin giderilmemesi halinde idari yaptırım kararı verilebileceği, inceleme konusu dosyada kabahate konu eksiklik ile ilgili mülkî idare amirinin bu şekilde bir bildirimini olmadığı,

2- 5253 sayılı Kanun'un 32/d maddesinde "Derneğe ait tutulması gereken defter veya kayıtları tutmayan veya tasdiksiz defter tutan dernek yöneticileri üç aydan bir yıla kadar hapis veya adli para cezası ile cezalandırılır. Bu defter ve kayıtların usulüne uygun tutulmaması halinde dernek yöneticilerine ve defterleri tutmakla sorumlu kişilere beşyüz Türk Lirası idarî para cezası verilir. Adına yetki belgesi düzenlenmediği halde gelir toplayanlar ile bilerek bu şekilde gelir toplanmasına

izin veren yönetim kurulu üyelerine bin Türk Lirası idarî para cezası verilir" ve Dernekler Yönetmeliğinin 45. maddesinde yer alan "Alındı belgeleri, sabit boyalı sert veya sivri uçlu tükenmez kalemle okunaklı bir biçimde silintisiz ve kazıntısız olarak doldurulur. " şeklinde yer alan düzenlemelere nazaran, gerçek kişilerin T.C. kimlik numaralarının, tüzel kişilerin de vergi numaralarının alındı belgesinde yer almasının zorunlu olduğuna dair bir hüküm bulunmadığı gibi yer almamasının da yaptırıma bağlanmadığı; alındı belgesinde doldurulması gereken kısımlara dair açık bir düzenlemeye yer verilmediği, sadece alındı belgesinin şeklen nasıl doldurulacağına ilişkin yönetime dair açıklamaya yer verildiği, ayrıca bağışçı olan ve dernek kayıtlarında kişisel bilgileri sınırlı bir şekilde bulunan şahıslara ilişkin özel bilgi mahiyetindeki T.C. kimlik ve vergi numaralarına ulaşılmasının hayatın olağan akışına da uygun olmadığı, gözetilmeden başvurunun kabulü yerine yazılı şekilde reddine karar verilmesinde isabet görülmemiş ve 5271 sayılı Ceza Muhakemesi Kanununun 309. maddesi uyarınca anılan kararın bozulması lüzumu kanun yararına bozmaya atfen ihbar olunmuş bulunmakla Türk Milleti adına gereği görüşülüp düşünüldü;

1- 5253 sayılı Kanun'un "Gelir ve giderlerde usul ile dernek defterleri" başlıklı 11. maddesinin ilgili kısımları şöyledir; "Dernek gelirleri alındı belgesi ile toplanır ve giderler harcama belgesi ile yapılır... Alındı belgelerinin şekli, bastırılması, onaylanması ve kullanılması ile dernek gelirlerinin toplanmasında kullanılacak yetki belgesine ilişkin hususlar yönetmelikte düzenlenir",

2- 5253 sayılı Kanun'un 32/d maddesinde yeralan; "... Bu defter ve kayıtların usulüne uygun tutulmaması halinde dernek yöneticilerine ve defterleri tutmakla sorumlu kişilere beşyüz Türk Lirası idarî para cezası verilir...",

3- Dernekler Yönetmeliğinin "alındı belgelerinin kullanımına" ilişkin 45. maddesi ise; "Alındı belgeleri, sabit boyalı sert veya sivri uçlu tükenmez kalemle okunaklı bir biçimde silintisiz ve kazıntısız olarak doldurulur... (Ek fıkra:RG-9/7/2020-31180) Bu Yönetmelikte öngörülen alındı ve harcama belgeleri; Yönetmelik ekindeki örneklerinde gösterilen belgelerdeki tüm bilgilerin eksiksiz doldurulması ve ilgili kişilerce imzalanması suretiyle düzenlenir" şeklindedir.

5253 sayılı Dernekler Kanunu'nun 11. maddesinde "...Alındı belgelerinin şekli, bastırılması, onaylanması ve kullanılması ile dernek gelirlerinin toplanmasında kullanılacak yetki belgesine ilişkin hususlar yönetmelikte düzenlenir" ve Dernekler Yönetmeliğinin 45. maddesinde yeralan "... (EkFıkra:RG 9/7/2020-31180) Bu Yönetmelikte öngörülen alındı ve harcama belgeleri; yönetmelik ekindeki örneklerinde gösterilen belgelerdeki tüm bilgilerin eksiksiz doldurulması ve ilgili kişilerce imzalanması suretiyle düzenlenir." şeklindeki düzenlemeler ile Dernekler Yönetmeliğinin ekinde yer alan örnek belge (EK-17)'de "Dernek gelirleri alındı belgesinde T.C. kimlik numarası, adı-soyadı, cep

tel/e-posta adresine ilişkin verilerin" eksiksiz doldurulmasının zorunlu kılınması hususları birlikte değerlendirildiğinde dernek gelirleri alındı belgelerinde bulunan tüm bölümlerin dernek yetkilileri tarafından eksiksiz doldurulması gerektiği anlaşılmakta ise de;

T.C. Anayasası'nın "Özel hayatın gizliliği" başlıklı 20. maddesinde yer alan“(Ek fıkra: 7/5/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.” hükmü uyarınca yasa koyucu tarafından çıkarılan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3. maddesinde "... Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi..." şeklinde tanımlanmıştır. 6698 sayılı Kişisel Verilerin Korunması Kanunu'na göre, gerçek kişilerin T.C. kimlik numaralarının kişisel veri olduğu, kişisel verilerin ise ilgilinin açık rızası alınmadan işlenmesinin yasaklandığı görülmektedir.

Bu kapsamda, 5253 sayılı Dernekler Kanunu'nun 11. maddesinde, dernek gelirlerinin toplanmasında kullanılacak alındı belgesine bağışçıya ait kişisel verilerin eklenmesinin öngörülmediği, Kanun'un bildirim tabi tutmadığı kişilerin yönetmelik değişikliği ile açık rıza alınmadan TC. kimlik numarasını bildirim tabi tutulamayacağı yönüyle Kanun Yararına Bozma talebinde bulunup bulunmayacağı hususunda dosyanın Adalet Bakanlığı'na gönderilmek üzere Yargıtay Cumhuriyet Başsavcılığı'na TEVDİİNE, 12.10.2021 tarihinde oy birliğiyle karar verildi.

Yargıtay Kararı - 6. Ceza Dairesi (E. 2021/10682)

Yargıtay 6. Ceza Dairesi (E. 2021/10682)

Esas No.: 2021/10682

Karar No.: 2022/5430

MAHKEMESİ: Asliye Ceza Mahkemesi

SUÇ: Nitelikli hırsızlık

HÜKÜM: Beraat

Mahalli mahkemece verilen hüküm temyiz edilmekle dosya incelenerek, gereği düşünüldü:

... Anadolu Cumhuriyet Başsavcılığının 15.10.2014 günlü iddianamesi uyarınca ve özetle; sanık ...'nın 15.08.2014 tarihinden dört ay önce, temizlik şirketi aracılığıyla katılan mağdur ...'un evinde ücreti mukabili günlük temizlik ve ev işleri yapmak üzere işe başladığı, ilk iki ay sorunsuz çalıştığı, ancak sonraki iki ay içerisinde ise, değişik tarihlerde evde bulunan ziynet eşyası ve paraların bir kısmını çaldığı, eşya ve paralarının eksildiğini farkedene ve durumdan şüphelenen katılan mağdurun 14.08.2014 tarihinde evin içerisine iki adet güvenlik kamerası monte ettirdiği, kamera görüntülerine göre 15.08.2022 tarihinde de; eve gelen sanığın bir yandan temizlik yaparken, diğer yandan evde çalacak bir şeyler aradığı, bu bağlamda yatak odasında şifoniyerin içinde bulunan cüzdanı alıp içine baktığı içinin boş olduğunu görünce yerine koyduğu, kısa bir süre sonra da güvenlik kameralarını farketdiği, bu suretle sanığın suç tarihlerinde zincirleme biçimde nitelikli hırsızlık suçunu işlediği, kamera kayıtları çözüm tutanağı ve bilirkişi raporu başta olmak üzere, katılan mağdurun iddiası, diğer beyan ve tutanaklar ile tüm soruşturma evrakı kapsamında anlaşıldığından bahisle, 5237 sayılı TCK'nın 142/2-h ve 43. maddesinden cezalandırılması iddiasıyla iş bu kamu davası açılmıştır.

İlk Derece Mahkemesinin 26.04.2016 günlü kararıyla, suçu sübuta ermediğinden bahisle delil yetersizliği gerekçesiyle sanığın beraatine karar verilmiş, bu karar katılan vekili tarafından ve süresinde temyiz edilmiştir.

Yargıtay Cumhuriyet Başsavcılığı, kararın onanması gerektiği görüşündedir.

Karar tarihi itibarıyla bölge adliye mahkemeleri henüz faaliyete geçmediğinden 5320 sayılı Kanun'un 8. maddesi uyarınca, bu kararın doğrudan temyize tabi olduğu ve 1412 sayılı CMUK'nun temyize ilişkin hükümlerine göre temyiz incelemesinin yapılması gerektiği değerlendirilmiştir.

Katılan mağdurun evinde hırsızlık yapıldığı şüphesi üzerine güvenlik ve tedbir amacıyla evine kamera sistemi kurdurması ve sanığın hırsızlığa teşebbüs eylemindeki tek delilin kamera görüntüsü olması nedeniyle, bu delilin, hukuka uygun yahut aykırı olup olmadığı ön sorun olarak incelenmiştir.

Ceza yargılamasında özgürlük ve güvenlikten biri diğerine tercih edilmemiştir. Diğer bir anlatımla ceza yargılamasının temel amacı, kişisel hak ve özgürlüklere saygı ile toplumsal düzenin sağlanması arasında bir denge kurarak maddi gerçeğin ortaya çıkarılmasıdır. Maddi gerçeğin ortaya çıkarılması ise; delil ya da delillerin toplanması ile mümkün olur. Bu itibarla ceza yargılamasında bir yandan 'delil serbestliği' ilkesi benimsenmiş, diğer yandan delillerin hukuka uygun yöntemlerle elde edilmesinin zorunlu olduğu kabul edilmiştir.

Öncelikle belirtmek gerekir ki, Anayasanın 38/6, 5271 sayılı CMK'nın 206/2-a, 217/2, 230/1-b ve 289/1-i bendinin âmir hükümleri uyarınca, hukuka aykırı yöntemlerle elde edilen deliller hükme esas alınamaz.

Ancak, güvenlik ve toplumsal düzenin sağlanması amacıyla kamuya açık alanlarda kurulan "mobese" görüntüleriyle özel kişi ya da kuruluşların ev ya da iş yerlerinde, yaşama hakkı ile mülkiyet hakkı başta olmak üzere kendi hak ve menfaatlerini korumak amacıyla kurdukları kamera görüntülerinin gerektiğinde ceza yargılamasında hukuka uygun delil olarak kabul edilmesi gerekir.

Nitekim, Yargıtay 13. Ceza Dairesinin, 26.03.2012 günlü, 2011/7180 Esas ve 2012/8523 Karar sayılı kararına konu olan olayda, ... Üniversitesinde bulunan ... fakülte binasının yalnızca öğretim üyesi olan mağdur tarafından kullanılan odasına bıraktığı çantasından zaman zaman hırsızlık yapıldığını fakülte yönetimine bildirdiği, yönetim tarafından katılan mağdurun odasına güvenlik kamerası monte edildiği, bir müddet sonra bu kameranın tespit ettiği görüntülerden hırsızlık suçunu işleyen sanığa ulaşılan olayda, sözü edilen güvenlik kamerası görüntüleri hukuka uygun delil olarak kabul edilmiştir.

Zira Anayasanın 36/1 ve TCK'nın 26/1. maddeleri uyarınca herkes gibi mağdurun da hak arama özgürlüğü vardır. Hakkın kullanılması, bir hukuka uygunluk nedenidir.

Somut olayda sanık 13. Ceza Dairesinin sözü edilen kararında olduğu gibi gizlice kayda alınmış olmakla birlikte, kendi konutunda ve/veya özel hayatında değil, mağdurun konutunda görüntülenmiştir. Diğer bir anlatımla katılan mağdurun da hak arama özgürlüğü, bu bağlamda mağdurun aleyhine işlenen suçtan dolayı adli makamlara sunulmak üzere delil oluşturma hakkı mevcuttur.

Bu açıklamalar ışığında katılan mağdurun, özetle kendi can ve mal güvenliğini koruma amacıyla kurduđu kamera sistemine ait görüntülerin, hukuka uygun yöntemlerle elde edilen bir delil olduğunun kabul edilmesi gerektiđi sonucuna ulařılmıştır.

Sübut konusuna gelince; sanık ...'nın, katılan mağdur ...'un evinde temizlikçi olarak çalıştığı, katılan mağdurun evinde bulunan ziynet eşyası ve cüzdanında bulunan paranın eksildiğini fark etmesi üzerine güvenlik ve tedbir amaçlı alenen görünebilecek şekilde evine kamera sistemi kurduđu, 15.08.2014 günü sanığın yine temizlik için katılan mağdurun evine geldiđi, dosya içerisinde mevcut kamera görüntüsü ve buna ilişkin inceleme tutanađına göre sanığın, yatak odasına girerek çekmece içerisinde bulunan siyah cüzdanı alıp içine baktıktan sonra çekmeceye geri bıraktığı, şifonyer ve çekmece üzerinde herhangi bir temizleme işlemi yapmadan şifonyerin yanından ayrıldığının tespit edildiđi,

Buna karşılık iki ay öncesine kadar giden hırsızlık fiillerinin de sanık tarafından işlendiđi konusunda kuvvetli bir suç şüphesi mevcut ise de, sanığın baştan itibaren bütün suçlamaları kabul etmemesi ve bu fiillere ilişkin başkaca bir delil edilememesi karşısında, sanığın önceki fiillerinin deđil, yalnızca 15.08.2014 tarihinde işlediđi nitelikli hırsızlığa teşebbüs fiilinin sübuta erdiđi kabul edilmelidir.

Açıklanan nedenlerle;

Dosya ve duruşma tutanakları içeriđine, toplanıp karar yerinde incelenerek tartışılan hukuken geçerli ve elverişli kanıtlara, gerekçeye ve hâkimin takdirine göre; suçun sanık tarafından işlendiđini kabulde usul ve yasaya aykırılık bulunmadığı anlaşılmış, diđer temyiz itirazları da yerinde görülmemiştir.

Ancak;

Sanığın üzerine atılı TCK'nın 142/2-h ve 35. maddelerinde düzenlenen nitelikli hırsızlığa teşebbüs suçunun sübut bulduđu gözetilmeden delillerin takdirinde yanılıđıya düşölerek yazılı şekilde beraat hükmü kurulması,

Bozmayı gerektirmiş, katılan ... vekilinin temyiz itirazı bu bakımdan yerinde görölmüş olduğundan hükmün açıklanan nedenlerle 1412 sayılı CMUK'nun 321. maddesi uyarınca, tebliđnameye aykırı olarak BOZULMASINA, 11.04.2022 tarihinde oy birliđi ile karar verildi.

Yargıtay Kararı - Hukuk Genel Kurulu (E. 2014/56)

Unutulma hakkına ilişkin Yargıtay hukuk genel kurul kararı

HGK., E. 2014/56 K. 2015/1679 T. 17.6.2015

Esas No.: 2014/56

Karar No.: 2015/1679

Karar Tarihi: 17.06.2015

Taraflar arasındaki “manevi tazminat” davasından dolayı yapılan yargılama sonunda; İzmir 3. Asliye Hukuk Mahkemesince davanın kısmen kabulüne dair verilen 11.04.2011 gün ve 2010/399 E. 2011/172 K. sayılı kararın incelenmesi taraflar vekili tarafından istenilmesi üzerine, Yargıtay 4. Hukuk Dairesinin 08.11.2012 gün ve 2011/7193 E. 2012/16450 K. sayılı ilamıyla;

“...Dava, haksız fiil nedeni ile manevi tazminat istemine ilişkindir. Yerel mahkemece istemin bir bölümü kabul edilmiş; karar, taraflarca temyiz olunmuştur

Davacı vekili, müvekkilinin cinsel taciz suçundan şikayetçi olduğu ceza davasının yapılan yargılaması sonucunda, mahkeme ilamının temyizi sonrasında Yargıtay'ca verilen kararın davalılara ait Yorumlu-Uygulamalı Türk Ceza Kanunu adlı altı ciltlik eserde müvekkilinin ve diğer kişilerin isimlerinin açıkça yazılmak suretiyle yayımlandığını, bu durumun kişilik haklarına saldırı oluşturduğunu, belirterek davalıların manevi tazminatla sorumlu tutulmalarını talep etmiştir.

Davalılar vekili, söz konusu kitapların bilimsel eser niteliğinde olduğu, Avrupa İnsan Hakları Mahkemesi kararlarında davaların davacıların ismiyle adlandırıldığı, kitabın geniş kitlelere hitap etmediği, ceza hakimleri, savcılar ve ceza avukatlarınca okunduğu, kitapta isim belirtmenin hukuka aykırı olmadığını belirterek davanın reddini talep etmiştir.

Mahkemece, adı geçen eserde davacı ve diğer kişilerin isimlerinin kodlanmadan açıkça yazıldığı, söz konusu olayların anlatımında açıkça isim belirtmenin kitap içeriğine bir fayda sağlamadığı gibi, davacının isminin geçtiği olayın hassasiyeti ve Türk toplum yapısı da göz önünde tutulduğunda, yurt çapında dağıtımı ve satışı yapılan bir kitapta, bu tür bir olayla davacının adının açıkça belirtilmesinin davacının kişilik haklarını zedelediği, çevresine karşı davacıyı zor duruma düşürdüğü gerekçesi ile davanın kısmen kabulüne karar verilmiştir.

Bilimsel bilgi, taşıdığı özellikler dolayısıyla fikir üretiminin en yüce değer ve biçimi olma niteliğine haizdir ve herşeyden önce, insanlığın gerçekliğe ulaşması bakımından önemli bir araç sayılır. Bu durum, bilimsel bilgi ve onu üreten araştırmacının geniş bir özgürlük alanında bulunmasını gerektirir. Bilimi serbestçe öğrenme, araştırma, yayma ve öğretme haklarını içeren bilim özgürlüğü Anayasada kişisel haklar arasında (madde 27) düzenlenmiştir. Anılan madde de herkesin bilim ve sanatı serbestçe öğrenme ve öğretme, açıklama ve yayma ve bu konularda araştırma yapma hakkına sahip olduğu belirtilmektedir. Keza, AB Temel Haklar Bildirgesinin 13. maddesinde "sanat ve bilimsel araştırma kısıtlamaya tabi olmamalıdır. Akademik özgürlüğe saygı gösterilmelidir" ibaresine yer verilmiştir. Bu bağlamda bilimsel özgürlük, bilimsel bir etkinlikte bulunan veya böyle bir faaliyette bulunmak isteyen tüm bireylere tanınmış ve bu bireylerin kişiliğine sıkı sıkıya bağlı kalmış, öznel temel haklardır.

Taşıdığı önem dolayısıyla insan hakları belgelerine giren bilim özgürlüğü, araştırma özgürlüğünü, araştırma için zorunlu araçlara ve ortama sahip olma hakkını ve bilimsel üretme özgürlüğü veya bilgilendirme ve yayın hakkını içerir. Bu çerçevede bilim adamı bilimsel metotlarını kullanarak araştırma yapma hakkına ve bu araştırmanın sonuçlarını yayma hakkına sahip olacak, kural olarak bu konularda dış bir engelle karşılaşmayacaktır. Hatta bu konularda karşılaşacağı maddi ve manevi engeller devlet tarafından ortadan kaldırılacaktır.

Düşünce özgürlüğünün bir alt kategorisi olan fakat, üretilmesindeki özel çabanın ya da emeğin doğal sonucu olarak, sıradan düşünceye göre daha sistematik ve derin sayılması gereken bilimsel eserler, kural olarak ancak kendi ilkeleri çerçevesinde sınır tanırlar ve istisnaen ancak insan yaşamına yönelik bir tehlike olasılığında kısıtlanabilirler. Bunun ötesine geçilerek yapılan sınırlamalar, toplumun bilimsel düşüncelerle buluşmasını önleyebilecek ve dolayısıyla gerçekliğe ulaşılmasını engelleyebilecektir. Bu bakımdan bilimsel özgürlük hukuki rejim ve yaptırım açısından diğer entelektüel özgürlüklere göre daha mutlak bir özgürlük rejiminden yararlanmasını gerektirir. Fakat tüm özgürlüklerde olduğu gibi bilimsel özgürlük de sınırsız değildir. Bilim özgürlüğü ile kişilerin, kişilik değerlerinin karşı karşıya geldiği durumlarda somut olaydaki olgular itibarıyla koruma altına alınmış bulunan bu iki değerden birinin diğerine üstün tutulması gerekecektir.

Davaya konu olayda; bilimsel araştırma özgürlüğü kapsamında, aleniyet kazanmış ve kamu malı haline gelmiş Yargıtay ilamı, tarafların isimleri kodlanmadan davalıların yazmış oldukları Yorumlu-Uygulamalı Türk Ceza Kanunu adlı altı ciltlik bilimsel çalışma ürünü olan kitapta yayınlanmıştır. Adı geçen eserin bilimsel nitelikli bir çalışma olduğu, kamuya açık hale gelen Yargıtay kararının bilimsel çalışma ürünü olan kitapta olduğu gibi yer almasından dolayı yukarıda anlatılan ilkeler gereği

davalıların sorumlu tutulamayacağı, çatışan yararlar dengesinin davacı aleyhine bozulmadığı, bu olayın davacının kişilik haklarına saldırı teşkil etmeyeceği gözetilerek davanın tümünden reddine karar verilmesi gerekirken, yazılı biçimde karar verilmiş olması usul ve yasaya uygun düşmediğinden kararın bozulması gerekmiştir...”

gerekçesiyle bozularak dosya yerine geri çevrilmekle, yeniden yapılan yargılama sonunda; mahkemece önceki kararda direnilmiştir.

TEMYİZ EDEN: Davalılar vekili

HUKUK GENEL KURULU KARARI

Hukuk Genel Kurulunca incelenerek direnme kararının süresinde temyiz edildiği anlaşıldıktan ve dosyadaki kağıtlar okunduktan sonra gereği görüldü:

Dava, kişilik hakkına saldırı nedenine dayalı tazminat istemine ilişkindir.

Davacı K1 vekili 16/08/2010 harç tarihli dava dilekçesinde özetle; “müvekkilinin 14/11/2003 tarihinden beri İzmir Adliyesinde savcılık zabıt katibi olarak görev yaptığını, 18/07/2005 ile 11/04/2006 tarihleri arasında o dönem İzmir C. Başsavcı vekili olarak görev yapan K2 ile çalışmak için görevlendirildiğini ancak başladıktan sonra 8 ay boyunca Başsavcı vekilinin sözlü ve fiziksel taciziyle karşı karşıya kaldığını, fiziksel tacizin başlaması ve bu durumun çekilmez hale gelmesi nedeniyle davacının şikayette bulunduğunu, ailesinin ve çevresinin duymaması için çaba sarf ettiğini, K2 hakkında soruşturma açıldığını ve cezalandırıldığını, sanığın Başsavcı vekili olması nedeni ile olayların o dönem için basında yer aldığını, davacının bu olayları unutmaya başladığı bir dönemde Yargıtay 4. Ceza Dairesi Başkanı ve tetkik hakimleri olan davalıların Nisan 2010 tarihinde yorumlu-uygulamalı Türk Ceza Kanunu adlı altı ciltlik eser yayınladıklarını, örnek Yargıtay kararlarının başladığı 3262 nolu sayfa ve devamındaki sayfalarda davacının başına gelen olayların, tüm aktörlerin isimlerinin açıkça yazılmak suretiyle ve olayın tamamının açık bir şekilde anlatıldığını, davacı tarafından bu durumun öğrenilmesiyle davacının tekrar psikolojik bunalıma girdiğini, bütün kötü olayları tekrar yaşamak zorunda kaldığını, adliyede çalışması nedeniyle bu olayın davacının çevresinde, savcı ve avukatlar tarafından duyulduğunu, müvekkilinin zor da olsa saklayabildiği bir olayın kamuoyuna duyurulduğunu, iffetinin tartışılır hale geldiğini, bir genç kızın hayalleri ve geleceğinin kararmış olduğunu, eserin bir defa yararlanılacak bir eser olmadığını, uzun yıllar boyunca yaygın kitlelerce okunacak nitelikte bulunduğunu belirterek tüm bu nedenlerle davacının isminin geçtiği söz konusu ciltlerin toplatılmasını, 50.000,00-TL manevi tazminatın davalılardan tahsiline karar verilmesini istemiştir.

Davalılar K3., K4, K5 ve F1 Basın Yayın ve Dağıtım San. Ve Tic. Ltd. Şti. vekili 11.10.2010 havale tarihli cevap dilekçesinde özetle; “ Söz konusu kitapların bilimsel eser niteliğinde olduğunu, bilimsel eser niteliğinde olan kitaplarda fail ve mağdur adının olmasının hukuka aykırı olmadığını, ceza hukukundaki kitaplarının kaynağının yargısal kararlar olduğunu, geniş kitlelere hitap etmediğini, ceza hakimleri, savcılar ve ceza avukatlarınca okunduğunu, kitapta isim belirtmenin hukuka aykırı olmadığını, eserde adı geçen kişilerle ilgili vakıalar daha önce yargı konusu olduğu için ilgili mahkemelerin bulunduğu yerlerdeki kişiler tarafından duyulup öğrenildiğini, bu nedenle sözü edilen vakıaların ilk defa dava konusu eserde gündeme getirilmediğini, AİHM kararlarının ve Anayasa Mahkemesi kararlarının da isimler çıkarılmadan yayınlandığını, 2011 yılının başından itibaren UYAP sisteminde bulunan kararlardaki kişisel veriler rumuzlanmadan hakim ve savcının kullanımına açıldığını, dava konusu kararın son bölümünde rumuzlama yapılmış ise de ilk bölümünde yapılmamasının dizgi hatası olduğunu, olayın üzerine adliyeye gelen müfettişin yaptığı soruşturma sırasında tüm adliyenin olayı öğrendiğini ve olayın basına da yansıdığını, yine davacının ileri sürdüğü hususların daha sonra düzeltilindiğini ve düzeltilmiş bir nüshasının davacı vekilini sunulduğunu bu nedenle kitabın toplatılmasına gerek olmadığını istenen tazminatın fahiş olduğunu savunarak” davanın reddine karar verilmesini talep etmiştir.

Mahkemece, davanın kısmen kabulüne dair verilen kararın taraflarca temyiz edilmesi üzerine yukarıda başlık bölümünde yazılan Yargıtay ilamı ile bozulmuş, karar düzeltme istemi oyçokluğu ile reddedilmiş, mahkemece önceki gerekçeler tekrar edilerek direnilmiş; hükmü davalılar vekili temyize getirmiştir.

Hukuk Genel Kurulu önüne gelen uyuşmazlık; davalılar K3., K6 ve K5 tarafından yayına hazırlanan ve davalılardan F1 Basın Yay. Dağıtım San ve Tic. Ltd. Şti tarafından basılan eserde yer alan kararda, davalının isminin rumuzlanmadan ve rızası alınmadan açık bir şekilde yazılmasının kişilik hakkında saldırı oluşturup oluşturmayacağı noktasında toplanmaktadır.

İşin esasına girilmeden önce davacıya ait 13.01.2014 tarihli dilekçenin temyiz harcının tahsil edilip edilmediğinin belirlenmesi için dosyanın mahkemesine geri çevrilmesinin gerekip gerekmediği ön sorun olarak tartışılmış, şu sonuca varılmıştır:

Davacı vekiline gerekçeli karar 09.12.2013 tarihinde tebliğ edilmiştir. 15 günlük yasal temyiz süresi geçtikten sonra davacı vekili tarafından mahkemeye verilmiş bir dilekçe olmamasına rağmen 25.12.2013 (Çarşamba) tarihinde yazı işleri müdürü tarafından davacıdan temyiz harcı tahsil edilmesi için müzekkere yazılmıştır. Ancak temyiz harcının tahsiline dair tahsilât makbuzu dosya içinde bulunmamaktadır. Bir diğer deyişle süresi içinde harcı yatırılmış davacıya ait bir temyiz dilekçesi

dosya içinde bulunmamaktadır. Davalılara ait temyiz dilekçesi ise 30.12.2013 tarihinde davacı vekiline tebliğ edilmiştir. 10 günlük yasal karşı temyiz süresi 09.01.2014 (Perşembe) sona erdikten sonra davacı vekili (dilekçe tarihi: 13.01.2014 pazartesi havale tarihi 13.01.2014) temyize cevap dilekçesi vermiş direnme kararının onanmasını; az olan miktar yönünden dosyanın incelenmek üzere Yargıtay 4. Hukuk Dairesine gönderilmesi istenilmiştir. Bu nedenle davacının hem asıl hem de karşı temyiz süresini geçirdikten sonra verdiği dilekçe nedeni ile dosyanın geri çevrilmesine gerek olmadığı oybirliği ile kabul edilmiştir.

İşin esasına gelince; uyuşmazlığın çözümünde etkili yasal mevzuata bakılacak olursa;

Avrupa İnsan Hakları Sözleşmesinin ilgili maddeleri;

Özel ve aile hayatına saygı hakkı

1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.
2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.

şeklindedir.

Türkiye Cumhuriyeti Anayasası'nın ilgili maddeleri;

"IX. Bilim ve sanat hürriyeti

Madde 27 - Herkes, bilim ve sanatı serbestçe öğrenme ve öğretme, açıklama, yayma ve bu alanlarda her türlü araştırma hakkına sahiptir.

..."

"A. Özel hayatın gizliliği

Madde 20 - Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. (Üçüncü cümle mülga: 3/10/2001-4709/5 md.)

...

(Ek fıkra: 7/5/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya

kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.”

şeklindedir.

Türk Medeni Kanunu'nun ilgili maddeleri;

“II. Saldırıya karşı

1. İlke

Madde 24- Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir.

Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.”

şeklindedir.

Önümüze gelen sorunun temelinde unutulma hakkı ve bunun sonucu olan kişisel verilerin ve kişilik hakkının korunması ile bilim ve sanat hürriyetinin birbiri karşısında sınırlarının belirlenmesi yatmaktadır. Sorunun çözümünde dikkat edilmesi gereken husus, bilim ve sanat özgürlüğü ile bireyin temel hakları arasında adil bir dengenin kurulmasıdır.

Kişisel veri belli veya belirlenebilir olan gerçek veya tüzel bir kişiye ilişkin her türlü bilgiyi ifade eder. Avrupa Birliği'nin 95/46/EC sayılı Bireylerin Kişisel Verilerinin İşlenmesi ve Serbestçe Dolaşımı Karşısında Korunmasına İlişkin Direktif'in 2/a ve Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair 108 sayılı Avrupa Konseyi Sözleşmesi'nin 2(a) maddelerinde benzer tanımlama yer almaktadır.

Kişisel verilerin korunması insan haklarıyla yakından ilişkilidir. Çünkü kişisel verilerin açıklanması öncelikle özel hayatın gizliliğini ihlal edilebileceği gibi bir takım diğer bağlantılı hakları da zarar görebilir.

AİHS'de kişisel verilerle ilgili bir hüküm yoktur. Ancak mahkeme konuyla ilgili kararlarında kişisel veri içeriğini doldurmuştur. Hemen ifade edilmesi gerekir ki kişisel verinin sayısal olarak sınırlandırılması mümkün değildir. Ancak içtihatlar ve akademik yayınlar dikkate alındığında bireyin kimliğini ortaya çıkartan, bir kişiyi belirli kılan ve karakterize eden kişinin kimlik, ekonomik ve dijital bilgileri, tabiiyeti, kanaatleri, ırk, siyasî düşünce, felsefî inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık bilgileri, fotoğrafları, parmak izi, sağlık verileri,

telefon mesajları, telefon rehberi, sosyal paylaşım sitelerinde yazdığı veya paylaştığı yazı, fotoğraf, ses veya görüntü kayıtları kişisel verileri olarak kabul edilebilir.

Kişisel verilerin korunması, çağımızda, insan hakları kavramı ve korunması bilincinin gittikçe gelişmesine paralel olarak önemini artırmaktadır. Kişisel verilerin korunması hakkının temel amacı, bireyin özel yaşamının gizliliğinin güvence altına alınması yoluyla kişiyi korumaktır. Bilgi toplumunda giderek oldukça önemli bir konu haline gelen kişisel verilerin korunması hakkı, bireyin, demokratik bir hukuk devletinde özgür iradesiyle kendi yaşamını bizzat düzenleyebilmesinin bir gereği olarak karşımıza çıkmaktadır. Diğer taraftan bireyin kişiliğini serbestçe geliştirmesi, kişiliğinin korunması ve özgür bireylerden oluşan bir toplum düzeninin oluşturulması, ancak bireyin kişisel verilerine ilişkin hakkının korunmasıyla mümkündür. Bu hak yukarıda ifade edildiği üzere TC Anayasası'nın 20/2 maddesinde açık bir şekilde düzenlenmiştir.

Unutulma hakkına gelince; unutulma hakkı ve bununla ilişkili olan gerektiği ölçüde ve en kısa süreliğine kişisel verilerin depolanması veya tutulması konuları, aslında kişisel verilerin korunması hakkının çatısını oluşturmaktadır. Her iki hakkın temelinde bireyin kişisel verileri üzerinde serbestçe tasarruf edebilmesini, geçmişin engeline takılmaksızın geleceğe yönelik plan yapabilmesini, kişisel verilerin kişi aleyhine kullanılmasının engellenmesini sağlamak yatmaktadır. Unutulma hakkı ile geçmişinde kendi iradesi ile veya üçüncü kişinin neden olduğu bir olay nedeni ile kişinin geleceğinin olumsuz bir şekilde etkilenmesinin engellenmesi sağlanmaktadır. Bireyin geçmişinde yaşadığı olumsuz etkilerden kurtularak geleceğini şekillendirebilmesi bireyin yararına olduğu gibi toplumun kalitesinin gelişmişlik seviyesinin yükselmesine etkisi de tartışılmazdır.

Unutulma hakkı; üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerin silinmesini ve yayılmasının önlenmesini isteme hakkı olarak ifade edilebilir.

Bu hak bir yandan kişiye "geçmişini kontrol etme", "belirli hususların geçmişinden silinmesini ve hatırlanmamasını isteme hakkı" sağladığı gibi, diğer yandan muhataplarına kişi hakkındaki bir kısım bilgilerin üçüncü kişilerin kullanmamasını veya üçüncü kişilerin hatırlanmamasına yönelik önlenmeleri alma yükümlülüğü yükler. Bu hakkın; bireylerin fotoğraf, internet günlüğü gibi kendileri hakkındaki içerikleri silmek için üçüncü şahısları zorlamayı içermesinin yanında geçmişteki cezalarına ilişkin bilgilerin veya haklarında olumsuz yorumlara neden olabilecek bilgi ve fotoğraflarının kaldırılmasını isteme hakkını tanıdığı kabul edilmektedir. Diğer taraftan bu hak, bireyin geçmişindeki belirli yönlerinin mümkün olmayacak biçimde hatırlanmaması için önlemler alınmasını gerektirmektedir.

Avrupa İnsan Hakları Sözleşmesi (AİHS)'nin 8. maddesinde yer alan özel yaşama saygı hakkı altında korunan "mahremiyet hakkı"nın, bireyin kendisi hakkındaki bilgileri kontrol edebilmesi şeklindeki hukuki çıkarlarını da içerdiği ifade edilmektedir. Zira bireyin kendisine ait herhangi bir bilginin, kendi rızası olmaksızın açıklanmaması, yayılmaması ve bu bilgilere başkalarının ulaşmaması kısacası kişisel verilerinin mahrem kalması konusunda hukuki menfaati bulunmaktadır. (Gülay Arslan Öncü, Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması, Beta Yayınları, İstanbul 2011, s.182)

Kişiyi unutulma hakkının sağlanması ile birlikte özel hayatının gizliliği korunmuş olacaktır.

Somut olaya bu kapsamda bakıldığında; davacı, kamu görevinin veya hizmet ilişkisinin sağladığı nüfuzu kötüye kullanarak, müteselsilen cinsel saldırı suçunun mağdurudur. 2006 yılında gerçekleşen eylem tarihinde davacı bekâr olup maruz kaldığı eylem geleceği açısından etkilidir. Yapılan yargılama sonunda kamu görevlisi olan sanık ceza almıştır. Temyiz istemi üzerine yapılan inceleme sonunda ise hüküm 2009 yılında onanmıştır. Mağdur davacı gerek hazırlık gerekse de yargılama sırasında cinsel saldırının nasıl gerçekleştiğini açık bir şekilde anlatmış, bu anlatımlar doğal olarak karar metnine geçirilmiştir. Karar mağdur ve sanığın ismi rumuzlanmadan 2010 yılı nisan ayında yayımlanan kitapta yer almıştır.

Hemen ifade edilmelidir ki; davacının rızası dışında bir kitapta geçen ismi kişisel veri niteliğindedir.

Ayrıca şunun da ifade edilmesi gereklidir ki; unutulma hakkı tanımlarına bakıldığında her ne kadar dijital veriler için düzenlenmiş ise de, bu hakkın özellikleri ve bu hakkın insan haklarıyla arasındaki ilişkisi dikkate alındığında; yalnızca dijital ortamdaki kişisel veriler için değil, kamunun kolayca ulaşabileceği yerde tutulan kişisel verilere yönelik olarak da kabul edilmesi gerektiği açıktır.

Davacı, geçmişte yaşadığı kötü bir olayın toplum hafızasından silinmesini istemektedir. Unutulma hakkı ile geçmişindeki yaşanan talihsiz bir olayın unutulması geleceğini serbestçe şekillendirmek, diğer bir deyişle hayatında, yeni bir sayfa açma olanağı istemektedir. Kaldı ki, davacı da yargılama sırasında verdiği dilekçelerinde bu istem üzerinde ısrarla durmuştur. Davacı unutulma hakkı ile özel hayatına ilişkin kişisel verilerinin üçüncü kişiler tarafından bilinmemesini, aradan geçen süre nedeniyle toplum hafızasından silinmesini istemektedir.

Bu bağlamda değerlendirildiğinde; 4 yıl önce gerçekleşen bir olayın mağduru olan kişinin adının açık bir şekilde yazılarak kitapta yer alması halinde unutulma hakkının bunun sonucunda da davacının özel hayatının gizliliğinin ihlal edildiği kabul edilmelidir. Avrupa Birliği Adalet Divanı'nın "Google Kararı"nda açıkladığı gibi ilgili verinin kamu hayatında oynadığı önemli rol ve halkın ilgili veriye

yönelik yoğun ilgisi şeklinde, üstün bir kamu yararını ortaya koyan özel sebepler bulunmadığına göre bilimsel esere alınan kararda kişisel veriler açık bir şekilde yer almamalıdır.

Görüşmeler sırasında azınlıkta kalan üyeler mahkeme kararlarında yer alan isimlerin rumuzlanmasına gerek olmadığını, yargılamanın istisnalar haricinde açık bir şekilde yapıldığını hükmün alenen tefhim edildiğini, bu nedenle özel hayatın gizliliğinin ihlal edilmediğini savunmuşlar ise bu görüş “sorunun mahkeme kararlarında isimlerin rumuzlanmadan yer alması değil, kararların kitaba alınması sırasında rumuzlanması gerekip gerekmediği sorunu olduğu” gerekçesi ile kurul çoğunluğu tarafından kabul edilmemiştir.

O halde davacının isminin rumuzlanmadan kitapta yer almasının unutulma hakkını ve bunun neticesinde özel hayatın gizliliğini ihlal ettiği dikkate alındığında davacı lehine manevi tazminat koşullarının gerçekleştiğinin kabulü zorunludur.

Ne var ki, Özel Dairece tazminat miktarı yönünden inceleme yapılmadığından bu yöne ilişkin temyiz itirazlarının incelenmesi için dosyanın Özel Daireye gönderilmesi gerekir.

Yukarıda yazılı gerekçelerle yerel mahkemenin direnme kararı yerinde bulunduğundan tazminat miktarı yönünden mahkemenin kurduğu hükme yönelik temyiz itirazlarının incelenmesi için dosyanın 4. Hukuk Dairesine gönderilmesine, 17.06.2015 gününde oyçokluğu ile karar verildi.

Yargıtay 22. Hukuk Dairesi 2017/21857 E. , 2019/9884 K.

Esas No.: 2017/21857

Karar No.: 2019/9884

MAHKEMESİ: İş Mahkemesi

DAVA TÜRÜ: İTİRAZIN İPTALİ

Taraflar arasında görülen dava sonucunda verilen kararın, temyizen incelenmesi davacı vekili tarafından istenilmekle, temyiz talebinin süresinde olduğu anlaşıldı. Dava dosyası için Tetkik Hakimi ... tarafından düzenlenen rapor dinlendikten sonra dosya incelendi, gereği konuşulup düşünüldü:

YARGITAY KARARI

Davacı İsteminin Özeti:

Davacı vekili, davacının davalıya ait işyerinde mühendis olarak çalıştığını, iş sözleşmesinin davalı işveren tarafından haklı bir neden olmadan feshedildiğini, dört haftalık ihbar tazminatı tutarının ödenmemesi sebebiyle ilamsız icra takibi başlatıldığını, davalı işverenin haksız ve hukuka aykırı olarak takibe itiraz ettiğini ileri sürerek itirazın iptaline karar verilmesini, davalı işverenin icra inkar tazminatı ödemeye mahkum edilmesini talep etmiştir.

Davalı Cevabının Özeti:

Davalı vekili, davacının 18.02.2013/15.11.2014 tarihleri arasında satış ve pazarlama yöneticisi olarak çalıştığını, davacının iş sözleşmesinin başında işi yapma konusunda kendisinde olmayan bu şartları varmış gibi göstererek işvereni yanılttığını, şirkete ve müşterilere ait özel bilgilerin korunmasının esas olduğunu, davacının buna rağmen web sitelerinde alış veriş yaptığını, kariyer sitelerine iş başvuruları yaptığını, sosyal medya üzerinden rakip firmalar ile görüştüğünü, kendisine bir iki kez sözlü uyarı yapıldı ise de davranışlarının devam etmesi üzerine, güvenlik amacı ile bilgisayarının takibe alındığını, davacıya ait USB belleğin şirket aracı içinde araç yıkama firması tarafından bulunduğunu, USB'nin kontrolünde içinde şirkete ait dışarı çıkmaması gereken bilgilerin ve davacıya ait şahsi bilgilerin bulunduğu tespit edildiğini, davacının danışman firmalara, iş arkadaşlarına, şirketi kötüleyecek şekilde ifadeler kullanarak işinden memnun olmadığını söylediğini, iş sözleşmesinin

4857 sayılı İş Kanunu'nun 25/II maddesine göre haklı sebeple feshedildiğini savunarak davanın reddine karar verilmesini talep etmiştir.

Mahkeme Kararının Özeti:

Mahkemece, toplanan deliller ve bilirkişi raporu doğrultusunda davanın reddine karar verilmiştir.

Temyiz Başvurusu:

Kararı, davacı vekili temyiz etmiştir.

Gerekçe:

Taraflar arasında iş sözleşmesinin işverence feshinin haklı sebebe dayanıp dayanmadığı uyuşmazlık konusudur.

6098 sayılı Türk Borçlar Kanunu'nun 417. maddesine göre, işveren, hizmet ilişkisinde işçinin kişiliğini korumak ve saygı göstermek ve işyerinde dürüstlük ilkelerine uygun bir düzeni sağlamakla yükümlüdür. Kanununun 419. maddesine göre ise; "işveren işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir. Özel kanun hükümleri saklıdır."

Somut uyuşmazlıkta, davacı iş sözleşmesinin işverence haklı bir sebep olmadan feshedildiğini ileri sürmüş, davalı işveren ise hem davacının iş bilgisayarındaki takip programından hem de davacının araç yıkama sırasında araçta unuttuğu Usb bellekten, şirketle aralarındaki gizlilik sözleşmesine aykırı olarak sosyal medya ve alışveriş sitelerine girdiği, mesajlarında şirketi kötülediği ve headhunterlar ile görüşme yaptığı, şirkete ait iş sırrı niteliğindeki gizli bilgileri şirket dışına çıkartması yasal olmasına rağmen çıkardığı, 25/2 (a) hükmüne aykırı olarak işvereni yanılttığının anlaşıldığını, iş sözleşmesinin 25/2 maddesine göre haklı sebeple feshedildiğini savunmuştur. Mahkemece bilişim uzmanı ve hukukçu bilirkişiden alınan raporlar doğrultusunda iş sözleşmesinin 25/II (a) ve (e) bentlerine göre haklı sebeple feshedildiği sonucuna varılmıştır.

Dosya kapsamına göre, davacının iş sözleşmesi 15/11/2014 tarihli fesih bildirimini ile "gizlilik ve tarafsızlık sözleşmesine aykırı olarak, iş haricindeki web sitelerine sürekli erişimde bulunmak, gizlilik ve tarafsızlık sözleşmesine aykırı olarak, gizlilik içeren bilgileri şirket dışına yazılı olarak çıkarmak, her gün kısa süreli de olsa iş amaçlı bilgisayardan, internet üzerinden alışveriş ve kariyer sitelerine girmek, bir yıl içinde 6 kez yarım saat, 6 kez de 1 saatin üzerinde internette zaman geçirmek, bu sebeple iş görme edimini layıkı ile yerine getirmemek, şirket kaynaklarını verimsiz ve amaç dışı kullanmak, mesai saatlerine uymamak, iş disiplinini bozmak ve yanıltıcı beyanda bulunmak" sebebiyle feshedilmiştir. Davacı ile işveren arasında imzalanan gizlilik sözleşmesinde, davacının

şirkete ait bilgileri ve belgeleri sözlü veya yazılı olarak işyeri dışına çıkaramayacağı, müşteri bilgilerini gizli tutacağı, internet kullanımında şirketin güvenliği açısından iş haricindeki web sitelerine erişim ve yetkisiz dosya indiriminin yasak olduğu, anlık mesajlaşma servisleri ortak paylaşım siteleri vb hizmetlerin kullanımında ilgili şirket personelinin bilgilendirileceği düzenlenmiştir.

Somut uyuşmazlıkta davacının şirkete ait gizli bilgileri şirket dışına çıkardığını, bu hususun davacıya ait usb cihazının bulunması ile ortaya çıktığını savunmuş ise de, yargılama sırasında dinlenen davacı ve davalı tanıkları davacının zaman zaman işini evden de yürütebildiğini ve bilgisayarının da diz üstü bilgisayar olduğunu ifade etmiştir. Davalı taraf, davacının işyeri dışına çıkarmaması gereken iş sırrı niteliğindeki bilgileri işyeri dışına çıkardığına dair somut bir delil sunmamıştır. Diğer taraftan, dosya kapsamına göre davacının çalışma süresi içinde kariyer sitelerine girdiği, sohbet sitelerinde zaman geçirdiği, bir başka arkadaşını işverenine bazı bilgileri vermemesi konusunda yönlendirdiği, şirketin araç vermemesi üzerine işvereni kötülediği, fuarlara katılmama konusunda çeşitli bahaneler ürettiği, iş sözleşmesinin başlangıcında kendisinde bulunması gereken vasıflar konusunda hatalı bilgi verdiği sabit ise de, davalı işverenin bu bilgileri işçinin bilgisayarına yerleştirdiği özel bir takip programı ile elde ettiği anlaşılmaktadır. Davacı taraf, gerek haberleşme ve iletişiminin kayda alınması gerekse kaybolan USB'ye usulsüz olarak el konulduğu iddiası ile davalı işveren hakkında suç duyurusunda bulunduğunu belirterek, devam eden hazırlık soruşturmasının numarasını bildirmiştir. Davalı işveren ise işçinin bu izlemeden haberdar olduğu veya izlemenin yapılacağı konusunda bilgilendirilmediğine dair somut bir delil sunmamıştır. Şu halde davacı işçinin, bilgisayarında bulunan klavye yakalayıcısı adı verilen programdan haberinin olmadığı, işverence bu konuda bilgilendirilmediği, davacının rızası hilafına tüm kayıtların özel yahut işe ilişkin bilgi ayrımı olmadan işverence günlük olarak elde edildiğinin anlaşılması karşısında, elde edilen bu bilgilerin fesih sebebi olarak ileri sürülemeyeceği değerlendirilmelidir. İşverenin yönetim hakkının bir sonucu olarak işçiyi elektronik ortamda izlemesi ve takip etmesi her zaman mümkündür. Ancak bunun için işçinin bu izleme hakkında bilgilendirilmiş olması şarttır. İşçinin

izlendiğine dair bilgilendirilmemesi veya gizlice izlenmesi, bu izleme neticesinde elde edilen veriler, iş sözleşmesinin işçi tarafından ihlal edildiğini açıkça ortaya koysa dahi, hukuka aykırı olarak kabul edilmelidir. Hal böyle iken, somut olayda işverence gizlice izleme neticesinde elde edilen bilgilerin haklı fesih sebebi olarak ileri sürülmesinin mümkün olmadığı kabul edilmelidir. Mahkemece feshin haklı bir sebebe dayanmadığı ve davacının ihbar tazminatına hak kazandığı sonucuna varılması

gerekirken, yazılı gerekçe ile davanın reddine karar verilmesi hatalı olup, kararın bu sebeple bozulması gerekmiştir.

Sonuç: Temyiz olunan hükmün yukarıda açıklanan sebeplerden BOZULMASINA, peşin alınan temyiz harcının istek halinde ilgiliye iadesine, 07.05.2019 tarihinde oybirliği ile karar verildi.

Yargıtay Kararı - 20.Hukuk Dairesi (E. 2017/2277)

20. Hukuk Dairesi 2017/2277 E., 2018/7965 K.

Esas No.: 2017/2277

Karar No.: 2018/7965

Mahkemesi: Sulh Hukuk Mahkemesi

Taraflar arasındaki davanın yapılan duruşması sonunda kurulan hükmün Yargıtayca incelenmesi davacı-karşı davalı vekili tarafından istenilmekle, süresinde olduğu anlaşılan temyiz dilekçesinin kabulüne karar verildikten sonra dosya incelendi, gereği düşünüldü:

KARAR

Davacı-karşı davalı vekili, davacının anataşınmazda kat maliki olduğunu, davalı apartman yönetimi tarafından bina içerisine ve dışarısına güvenlik kameraları takıldığını, davacının bu hususta esas itibari ile bir itirazı bulunmadığını, zira davacının da daha öncesinden binada güvenlik önlemlerinin yeterli olmamasından dolayı kendi konutu için güvenlik kamerası taktırdığını, dava konusu olan kaldırılması istenen kameraların müvekkilin evinin giriş kapısı karşısına takılan ve yalnızca müvekkilin konutunu gören kamera ile davacının evinin balkonunu gören kamera olduğunu, güvenlik amacı ile olmayan, yalnızca davacının evinin giriş kapısını gören, davacının mahremiyetini ihlal eden bu kameranın takılması konusunda usulüne uygun alınmış bir kat malikleri kurul kararı da bulunmadığını, bu kameralardan alınan görüntülerin nerede saklandığı, kim tarafından izlendiği gibi soruların davacıda ciddi huzursuzluğa sebebiyet verdiğini beyan ederek; davanın kabulü ile apartman yönetimi tarafından bina içerisine ve dışarısına taktırılan güvenlik kameralarından sadece davacının evinin girişi ve balkonunu gören kameraların kaldırılmasına karar verilmesini ve daha sonraki aşamalarda karşı davanın reddini talep etmiştir.

Davalı-karşı davacı vekili cevap ve karşı dava dilekçesinde; davacıve apartman sakinleri arasında gerek hukuk davalarıyla, gerekse de ceza davalarıyla gündeme gelen birçok ihtilaf çıktığını, 07.06.2015 tarihli kat malikleri kurulu kararıyla gerek kurmuş oldukları kamera sisteminin kaldırılması gerekse de vermiş oldukları tüm rahatsızlıkları sona erdirmeleri için davacılara ihtar çekilmesinin karar altına alındığını, söz konusu kameraların görüntü açılarının birbirlerini tamamlayacak şekilde konuşlandırıldığını, yani kameralardan birinin kasıtlı/kendiliğinden kayıt

yapamaması/yapamayacak hale getirilmesi, bir kameranın görüntü açısının yetmemesi veya bir şekilde görüntü açısının içinde olmasına rağmen amaca hizmet edecek yeterlilikte görüntünün aktarılamaması sebebiyle doğabilecek muhtemel sorunlara karşı tedbiren birden fazla olacak şekilde kamera yerleştirildiğini, davacı-karşı davalı tarafın apartmanın giriş katında oturduğunu, kameranın giriş katında oturan davacının dairesinin girişini ve balkonun bir kısmını görmesi, apartmanın giriş görüntüsünün kayıt altına alınması için, işin doğası gereği, yani fiziken zorunlu olan bir durum olduğunu, eğer dava konusu kameranın yeri değiştirilecek/kaldırılacak olursa apartmanın güvenliğini sağlama hususunun yerine getirilemeyeceğini, kat maliklerinin, 15.12.2011 tarihli kurul kararıyla güvenlik önlemleri için gerekli tedbirlerin alınması konusunda karar aldığını, ilgili kararda apartman yönetimine yetki verildiğini, davacı-karşı davalı tarafın söz konusu toplantıya katılmadığını ve olumsuz oy kullanmadığını, sözkonusu kamera kayıtların yaklaşık 20 günlük periyotlarla kendi kendini sildiğini, eski kayıtların saklanması gibi bir uygulamanın söz konusu olmadığını, kayıt cihazının apartmanın ortak alanında bir panoda kilit altında olduğunu, iddia edildiği gibi her daim takip söz konusu olmayıp ancak bir sıkıntı olduğunda talep halinde apartman sakinleri yöneticiyle birlikte görüntüleri izleyebildiğini, davacı/karşı davalının kendi inisiyatifiyle, apartman yönetiminin ve kat maliklerinin tüm karşı çıkmalarına rağmen, apartmanın içine ve dışına kamera sistemi kurdurduğunu, davacı/karşı davalının kat malikleri kurulu kararı olmadan ana gayrimenkule kendiliğinden, 7/24 saat esasına göre gerçek zamanlı, evindeki televizyon ekranından herkesi izleyebildiği kamera sistemi kurdurmasının hukuka ve hakkaniyete aykırı olduğunu, bina içine kurdurulan kameranın ise, duman dedektörü görünümlü gizli kamera olduğunu ve tavana monteli bu kameranın apartmana gelen misafirleri izlendiklerini anlayamayacağı şekilde dizayn edildiği için her şeyden önce kişi hak ve özgürlüklerine aykırı bir eylem teşekkül ettiğini belirterek asıl davanın reddini, karşı davanın kabulü ile davacı/karşı davalının kurdurduğu kamera sisteminin kaldırılmasını talep etmiştir.

Mahkemece; davanın kısmen kabulüne,

Apartmanı yönetimince tesis edilen ve 15/04/2016 tarihli bilirkişi raporu 7. sayfasının alt kısmında gösterilen şekilde 3 ve 7 numaralı kameraların "alınabilecekleri konuma getirilmesi suretiyle " uyuşmazlığın giderilmesine, bu iş için yönetime 2 hafta süre verilmesine, kameraların tamamen kaldırılması talebinin reddine,

2-Karşı davanın kısmen kabulüne,

Apartmanı 6 nolu bağımsız bölüme ait olan ve 15/04/2016 tarihli bilirkişi raporunda gösterilen 1 ve 3 nolu kameraların iptali ile kaldırılmasına, eski hale iade için davacıya 2 hafta süre verilmesine, 2 nolu

kameranın ise sadece 6 nolu bağımsız bölüm apartman giriş tarafında kalan balkonun içini yukarıdan aşağı doğru göreceğ şekilde sabit olarak konumlandırılmasına, bu iş için davacıya 2 hafta süre verilmesine karar verilmiş, hüküm davacı/ karşı davalı vekili tarafından temyiz edilmiştir.

Dava, Kat Mülkiyeti Kanunu uyarınca projeye aykırı yapıldığı bildirilen imalatların (ortak alanlara kurulan kameraların kaldırılması) eski hale getirilmesi, müdahalenin önlenmesi istemine ilişkindir.

Mahkemece davanın kısmen kabulü, müdahalenin önlenmesi ve eski hale getirilme yönünde hüküm kurulmuş ise de yapılan inceleme ve araştırma hüküm kurmaya, kurulan hüküm de infaz etmeye elverişli değildir. Buna göre;

1- Mahkemece yerinde yapılan inceleme sonucu düzenlenen bilirkişi raporu içeriğinden ortak alana kamera ünitesinin yerleştirildiği anlaşılmaktadır. 634 sayılı Kat Mülkiyeti Kanununun 19. maddesinin ikinci fıkrasına göre, kat maliklerinden biri bütün kat maliklerinin beşte dördünün rızası olmadıkça anataşınmazın ortak yerlerinde onarım, tesis ve değişiklik yaptıramaz. Kanunun bu hükmü dikkate alınarak, hem asıl davaya hem de karşı davaya konu edilen kameralara ilişkin olarak, karar defterleri de incelendikten sonra alınan kat malikleri kurulu kararlarında kat maliklerinin beşte dördünün rızasının olup olmadığı değerlendirilmeksizin, kurulan hükümde kameraların sadece yer ve açılarının değiştirilmesi yönünde hüküm kurulması doğru görülmemiştir.

2- 6100 sayılı Hukuk Muhakemeleri Kanununun 297/2. maddesi; "Hükmün sonuç kısmında, gerekçeye ait herhangi bir söz tekrar edilmeksizin, taleplerden her biri hakkında verilen hükümle, taraflara yüklenen borç ve tanınan hakların, sıra numarası altında; açık, şüphe ve tereddüt uyandırmayacak şekilde gösterilmesi gereklidir." hükmünü amir olup, hüküm fıkrasının tarafların taleplerini karşılayacak, infazda tereddüt yaratmayacak şekilde, açık ve maddeler halinde oluşturulması gerekir. Buna göre;

Asıl davaya yönelik kurulan hüküm fıkrasının 1 nolu bendinde; "15/04/2016 tarihli bilirkişi raporunun 7. sayfasının alt kısmında gösterilen şekilde 3 ve 7 numaralı kameraların alınabilecekleri konuma getirilmesi suretiyle" şeklindeki genel ve soyut ifadelerle, bilirkişi raporunun eki olan "kamera açılındırmalarına ilişkin kroki" de dikkate alınmaksızın sadece bilirkişi raporuna atıf yapılması ile yetinilmesi, kaç numaralı kameranın nereye göreceği ve açılındırılmasının nasıl olacağı somut olarak belirtilmeksizin, her bir kamera yönünden duraksamaya yol açmayacak şekilde infaza elverişli hüküm kurulmaması, yukarıda anılan 297. maddesi hükmüne aykırı olup, hüküm fıkrasının açık, şeffaf, uygulanabilir ve gerekçe ile uyumlu olma, talepleri tek tek karşılama ilkesine aykırı, infazda tereddüt yaratacak ve duraksamaya yol açacak nitelikte olması nedeniyle bozma nedenidir.

SONUÇ: Yukarıda açıklanan nedenlerle; davacı-karşı davalı vekilinin temyiz itirazlarının kabulü ile hükmün BOZULMASINA, temyiz harcının istek halinde iadesine 06/12/2018 günü oy birliği ile karar verildi.

Yargıtay Kararı - 14. Hukuk Dairesi (E. 2016/2792)

Yargıtay 14. Hukuk Dairesi 2016/2792 E. 2018/6717 K.

14. Hukuk Dairesi

Esas No: 2016/2792

Karar No: 2018/6717 K.

MAHKEMESİ: Asliye Hukuk Mahkemesi

Davacılar vekili tarafından, davalı aleyhine 04.09.2013 gününde verilen dilekçe ile komşuluk hukukundan kaynaklanan elatmanın önlenmesi ve kal talebi üzerine yapılan duruşma sonunda; davanın kabulüne dair verilen 17.07.2014 günlü hükmün Yargıtayca incelenmesi davalı ... tarafından istenilmekle süresinde olduğu anlaşılan temyiz dilekçesinin kabulüne karar verildikten sonra dosya ve içerisindeki bütün kağıtlar incelenerek gereği düşünüldü:

KARAR

Dava, elatmanın önlenmesi ve kal isteğine ilişkindir.

Davacılar vekili; müvekkileri ile davalının aynı binada müvekkillerinin alt katta davalın üst katta oturduğu davalının evin girişine avlusuna, merdiven kısmına ve balkonuna kamera koyduğu kameraların müvekkillerinin evin giriş kapısı ve pencerelerine yöneltilerek kayıt işlemi yapıldığı özel hayatın gizliliğinin ihlal edildiğini belirterek elatmanın önlenmesine ve kameraların kal'ine karar verilmesini talep etmiştir.

Davalı, kameraları güvenlik için taktırdığını, davanın reddini talep etmiştir.

Mahkemece; davanın kabulüne ve müdahalenin önlenmesine, bilirkişi raporunda yerleri belirtilen 2, 3, 4, 5 nolu kameraların kal'ine karar verilmiştir.

Hükmü, davalı vekili temyiz etmiştir.

1- Yapılan yargılamaya, toplanan delillere ve dosya içeriğine göre aşağıdaki bendin kapsamı dışında kalan temyiz itirazları yerinde görülmemiş, reddi gerekmiştir.

2- Hükmün 2. bendinde; bu kameraların (2, 3, 4 ve 5 no'lu) kararın kesinleşmesinden itibaren 1 haftalık kesin süre de davalı tarafça kal'i ne, aksi halde masrafı davalı taraftan alınmak sureti ile davacılar tarafından kaldırılmasına, şeklinde hüküm kurulması doğru görülmemiş ise de; belirtilen bu husus kararın bozulmasını ve yeniden yargılama yapılmasını gerektirmediğinden HUMK'nun

438/7. maddesi uyarınca hüküm sonucunun aşağıdaki şekilde düzeltilerek onanmasına karar vermek gerekmiştir.

SONUÇ: Yukarıda (1) numaralı bentte açıklanan nedenlerle davalı vekilinin temyiz itirazlarının reddine, (2) numaralı bent uyarınca hüküm fıkrasının 2. bendindeki "aksi halde masrafı davalı taraftan alınmak sureti ile davacılar tarafından kaldırılmasına" şeklindeki kısmın hüküm fıkrasından çıkarılmasına hükmün HUMK'nun 438/7. maddesi gereğince DEĞİŞTİRİLMİŞ ve DÜZELTİLMİŞ bu şekliyle ONANMASINA, peşin yatırılan harcın istek halinde yatırana iadesine, kararın tebliğinden itibaren 15 gün içinde karar düzeltme yolu açık olmak üzere, 15.10.2018 tarihinde oybirliği ile karar verildi.

Yargıtay Kararı - 9. Hukuk Dairesi (E. 2014/37215)

İşyeri özlük dosyasının yeni işverene gönderilmesinin manevi tazminat sebebi olduğuna ilişkin Yargıtay kararı

Yargıtay 9. HD., E. 2014/37215 K. 2016/9418 T. 14.4.2016

Esas No.: 2014/37215

Karar No.: 2016/9418

Karar Tarihi: 14.04.2016

MAHKEMESİ: İŞ MAHKEMESİ

DAVA: Davacı, manevi tazminatın ödetilmesine karar verilmesini istemiştir.

Yerel mahkemece, davanın reddine karar verilmiştir.

Hüküm süresi içinde davacı avukatı tarafından temyiz edilmiş olmakla, dava dosyası için Tetkik Hakimi tarafından düzenlenen rapor dinlendikten sonra dosya incelendi, gereği konuşulup düşünüldü:

YARGITAY KARARI

A) Davacı İsteminin Özeti:

Davacı vekili; müvekkilinin 30.07.2012-18.9.2013 tarihleri arasında davalı işyerinde çalıştığını, müvekkilinin iş akdinin 18.9.2013 tarihinde işveren ile imzalanan protokol çerçevesinde sona erdiğini, aradan birkaç ay geçtikten sonra tarihinde müvekkilinin özlük dosyasının tamamının müvekkilinin halen çalıştığı teftiş kuruluna gönderildiğini, bu göndermenin müvekkilinin iş hayatına ve kariyerine zarar vermek için yapıldığını, müvekkilinin davalı işyerinden sağlık sebepleri nedeni ile ayrıldığını, müvekkilinin özlük dosyasının halen çalıştığı işyerine gönderilmesinin müvekkilinin kişilik haklarına ve manevi değerlerine zarar verdiğini, bunun neticesinde müvekkilinin halen çalıştığı işyerinin müvekkiline olumsuz baktığını, müvekkilinin psikolojik olarak yıpratıldığını iddia ederek manevi tazminatın davalıdan tahsilini talep etmiştir.

B) Davalı Cevabının Özeti:

Davalılar vekili, manevi tazminatı için gerekli şartların oluşmadığını, müvekkilinin kusurlu bir eyleminin olmadığını, davacının kişilik haklarının zedelenmediğini, davacının somut deliller

sunmadığını, müvekkilinin hukuka aykırı eyleminin olmadığını, müvekkilinin davacının yeni girdiği iş yeri ile yapılan şifahi görüşme sonucunda şahsi sicil dosyasının gönderildiğini, davacının ...'nin değil, işçisi olduğunu, davanın ...'ye yöneltilmesinin anlamının bulunmadığını savunarak açılan davanın reddini talep etmiştir.

C) Yerel Mahkeme Kararının Özeti:

Mahkemece, manevi tazminat oluşabilmesi için davacının kişilik haklarının zedelenmesi gerektiği, davacının kişilik haklarının zedelendiğini kanıtlamak için tanık dinlettiği, tanıkların davacının manevi zarara uğradığı konusunda beyanlarının olmadığı, gönderilen evraklar nedeniyle yeni işyerinde herhangi bir problem yaşamadığı, işinden uzaklaştırılmadığı, çalıştığı pozisyonun değiştirilmediği bu nedenle mahkemece davacının kişilik haklarının zedelenmediği kanaatine varıldığı gerekçesiyle davanın reddine karar verilmiştir.

D) Temyiz:

Kararı davacı vekili temyiz etmiştir.

E) Gerekçe:

Taraflar arasındaki uyuşmazlık, davacının önceki işverenin işyeri özlük dosyasını yeni işverene göndermesi nedeniyle davacının manevi tazminata hak kazanıp kazanmadığı noktasında toplanmaktadır.

İşçi özlük dosyası konusunda düzenleme 4857 sayılı İş Kanunu'nun 75. maddesinde yer almaktadır. Düzenlemeye göre "İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır.

İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür."

Davacı 18.09.2013 tarihinde davalı bünyesinden ayrıldıktan kısa bir süre sonra dava dışı bünyesinde çalışmaya başlamıştır. Davacı burada çalışmaya devam ederken davacının önceki işyerine ait içerisinde iş sözleşmesi, özel yazışmaların, davacının bir kısım senede bağlı tutarları eski işyerine ödeyeceğine dair taahhüdünü içeren işten ayrılma dilekçesinin ve ödeme dekontlarının bulunduğu özlük dosyası yeni işverene gönderilmiştir.

Davacı davalının iş hayatını baskı altına almaya olumsuz etkilemeye hakkı olmadığını, çalışma hakkını sekteye uğratma kariyerini olumsuz etkileme amacıyla hareket edildiğini, bu nedenle psikolojik olarak üzüntü yaşadığını, manevi yönden yıprandığını belirterek manevi tazminat talep etmiştir.

Davalı yargılama sırasında söz konusu şahsi sicil dosyasının işverence istendiğini bu nedenle gönderildiğini belirtmişse de, davalı bu yönde bir delil sunmamış olup insan kaynakları müdürü olan davalı tanığı da dosyayı kendiliğinden gönderdiğini beyan etmiştir.

İşyeri şahsi sicil dosyası içerisinde özel yazışma olarak, davacının eski işverenine gönderdiği elektronik posta yazışmaları bulunmaktadır. Söz konusu yazışmalarda davacı sağlık sorunları nedeniyle ayrılmak istediğini bir süre çalışmayacağını eşinin sağlık sorunları ilgileneceğini bu süreden sonra her şey yolunda giderse güvendiği birileriyle çalışma hayatına dönebileceğini belirtmektedir.

Yargılama sırasında dinlenen davacı tanığı ... özetle, davacının şu an çalıştığı genel müdürü olduğunu, davacı işe başladıktan sonra davalı şirketin sahibi davalı ... Zülfikar'ın kendisini aradığını, davacı ile sorunlu ayrıldıklarını, ayrılma sürecinin sorunlu olduğunu, davacının kendilerine doğruları söyleyemeyeceğini dikkat edilmesi gereken bir insan olduğunu söylediğini, bu konuşmadan bir ay sonra davacının önceki işyeri şahsi sicil dosyasının kendilerine gönderildiğini, davacıyı kötüleyen bir husus olmadığını, söz konusu belgelerin patrona kadar gittiğini davacının arkasında durmasa iş sözleşmesinin feshedileceğini ancak davacıyı tanıdığı için iş sözleşmesinin feshedilmediğini beyan etmiştir.

Somut olay, yargılama sırasında dinlenen tanıklar ve sunulan deliller değerlendirildiğinde, içerisinde özel yazışmaların, davacının bir kısım senede bağlı tutarları eski işyerine ödeyeceğine dair taahhüdünü içeren işten ayrılma dilekçesi ve ödeme dekontlarının olduğu işyeri özlük dosyasının yeni çalıştığı işverenine gönderilmesi eyleminin davacıyı rahatsız etme, onu doğruları söylemeyen bir kişi olarak gösterme amacı taşıdığı, bu olay sonrası davacının iş sözleşmesinin feshinin gündeme geldiği ancak buna engel olunduğu, yaşanan olay nedeniyle davacının manevi yönden etkileneceği açık olup bu nedenle manevi tazminata hak kazandığının kabulü gerekirken reddi hatalıdır.

F) Sonuç:

Temyiz olunan kararın, yukarıda yazılı nedenden dolayı BOZULMASINA, peşin alınan temyiz harcının istek halinde ilgiliye iadesine 14.04.2016 tarihinde oybirliğiyle karar verildi.

DANIŐTAY KARARLARI

Bölüm İçeriđi

- DanıŐtay İDDK. (E. 2020/1455)
- DanıŐtay İDDK. (E. 2020/1454)
- DanıŐtay İDDK. (E. 2020/1038)
- DanıŐtay İDDK. (E. 2020/937)
- DanıŐtay İDDK. (E. 2019/3003)
- DanıŐtay İDDK. (E. 2019/2983)
- DanıŐtay İDDK.(E. 2019/2549)
- DanıŐtay İDDK. (E. 2019/2425)
- DanıŐtay İDDK. (E. 2019/2273)
- DanıŐtay İDDK. (E. 2019/2365)
- DanıŐtay İDDK. (E. 2019/2278)
- DanıŐtay İDDK. (E. 2018/4437)
- DanıŐtay İDDK (E. 2014/2242)
- DanıŐtay 10. Daire (E. 2020/4379)
- DanıŐtay 2. Daire (E. 2020/847)
- DanıŐtay 10. Daire (E. 2019/10118)
- DanıŐtay 12. Daire (E. 2019/7364)
- DanıŐtay 12. Daire (E. 2019/7283)
- DanıŐtay 10. Daire (E. 2019/7114)
- DanıŐtay 10. Daire (E. 2019/7092)
- DanıŐtay 10. Daire (E. 2019/7049)
- DanıŐtay 12. Daire (E. 2019/5658)
- DanıŐtay 15. Daire (E. 2018/1490)
- DanıŐtay 12. Daire (E. 2019/1428)
- DanıŐtay 10. Daire (E. 2018/3449)
- DanıŐtay 13. Daire (E. 2018/2910)
- DanıŐtay 15. Daire (E. 2018/844)
- DanıŐtay 15. Daire (E. 2018/530)
- DanıŐtay 15. Daire (E. 2018/251)

- Danıřtay 8. Daire (E. 2017/7307)
- Danıřtay 10. Daire (E. 2017/4211)
- Danıřtay 8. Daire (E. 2017/1388)
- Danıřtay 10. Daire (E. 2017/1141)
- Danıřtay 11. Daire (E. 2017/816)
- Danıřtay 15. Daire (E. 2016/10500)
- Danıřtay 15. Daire (E. 2016/10488)
- Danıřtay 8. Daire (E. 2016/3355)
- Danıřtay 8. Daire (E. 2016/3316)
- Danıřtay 8. Daire (E. 2016/2727)
- Danıřtay 15. Daire (E. 2015/6279)
- Danıřtay 10. Daire (E. 2015/5219)
- Danıřtay 10. Daire (E. 2015/3902)
- Danıřtay 15. Daire (E. 2015/3035)
- Danıřtay 10. Daire (E. 2015/2995)
- Danıřtay 10. Daire (E. 2015/2787)
- Danıřtay 10. Daire (E. 2015/2696)

Danıştay Kararı - İDDK. (E. 2020/1455)

Danıştay Kararı - İDDK., E. 2020/1455 K. 2021/733 T. 8.4.2021

T.C. DANIŞTAY İDARİ DAVA DAİRELERİ KURULU

Esas No: 2020/1455

Karar No: 2021/733

TEMYİZ EDEN (DAVALI): ... Bakanlığı

VEKİLİ: Hukuk Müşaviri ...

KARŞI TARAF (DAVACI): ... Eğitim Merkezi Ltd. Şti.

VEKİLİ: Av. ...

İSTEMİN KONUSU: Danıştay Sekizinci Dairesinin 26/11/2019 tarih ve E:2019/4434, K:2019/10746 sayılı kararının temyizen incelenerek bozulması istenilmektedir.

YARGILAMA SÜRECİ:

Dava konusu istem: 18/05/2012 tarih ve 28296 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Milli Eğitim Bakanlığı Özel Eğitim Kurumları Yönetmeliği'nin 3. maddesinin 1. fıkrasının (e) bendinin, 16. maddesinin 3. fıkrasının, 19. maddesinin 1. fıkrasının, 20. maddesinin 1. fıkrasının, 22. maddesinin 2. fıkrasının, 25. maddesinin 2., 3. ve 4. fıkralarının, 29. maddesinin 1. fıkrasının (f) bendinin, 31. maddesinin 1. ve 4. fıkralarının iptali istenilmiştir.

Daire kararının özeti: Danıştay Sekizinci Dairesinin 26/11/2019 tarih ve E:2019/4434, K:2019/10746 sayılı kararıyla; davanın reddine yönelik Dairelerinin ... tarih ve E:..., K:... sayılı kararının, dava konusu Yönetmeliğin 25. maddesinin 3. ve 4. fıkralarına yönelik kısımlarının Danıştay İdari Dava Daireleri Kurulunun 19/12/2018 tarih ve E:2015/432, K:2018/503 sayılı kararıyla bozulması üzerine söz konusu bozma kararına uyularak;

Anayasa'nın "Özel hayatın gizliliği" başlıklı 20. maddesinde, herkesin, özel hayatına ve aile hayatına saygı gösterilmesini isteme ve kendisiyle ilgili kişisel verilerin korunmasının isteme hakkına sahip olduğu; bu hakkın; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı; kişisel verilerin, ancak kanunda öngörülen hallerde veya

kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmek suretiyle, kişisel verilerin korunmasının, özel hayatın gizliliğinin korunması kapsamında güvenceye bağlandığı;

Öte yandan, Avrupa İnsan Hakları Sözleşmesi'nin "Özel Hayatın ve Aile Hayatının Korunması" başlıklı 8. maddesinde, herkesin özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahip olduğu, bu hakkın kullanılmasına bir kamu makamının müdahalesinin, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabileceğinin kurala bağlandığı; Birleşmiş Milletler Medeni ve Siyasal Haklar Sözleşmesi'nin "Mahremiyet Hakkı" başlıklı 17. maddesinde ise, hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemeyeceği; onuru veya itibarının hukuka aykırı saldırılara maruz bırakılmayacağı, herkesin bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahip olduğunun belirtildiği;

652 Sayılı Milli Eğitim Bakanlığı Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 36. maddesinin 1. fıkrasında, Bakanlığın, görev, yetki ve sorumluluk alanına giren ve önceden kanunla izin verilen konularda idari düzenlemeler yapabileceğinin hüküm altına alındığı,

Dava konusu Yönetmeliğin 25. maddesinin 3. fıkrasında, kurumlarca engelli bireylerin ders devam takiplerinin, ders başlangıcından önce ve ders bitiminde engelli birey modülünde yer alan kimlik doğrulama sistemi ile yapılacağı; 4. fıkrasında, kurumlarca; eğitim personelinin ders devam takibinin ise giriş ve çıkışlarda engelli birey modülünde yer alan kimlik doğrulama sistemi ile yapılacağı kurallarına yer verildiği;

İdarelerce, gelişen teknolojinin kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması amacıyla, kamu kesiminde kullanılmaya başlanması mümkün olmakla birlikte, teknoloji kullanılarak kişisel verilerin kayıt altına alınması uygulamasının, ilgili Anayasal düzenleme uyarınca belirli bir yasal çerçeve içine oturtulması, konuya ilişkin usul ve esasların yasa hükmü ile tespit edilmesi ve yine Anayasa'daki ve Türkiye'nin taraf olduğu uluslararası andlaşmalardaki temel hak ve özgürlüklere ilişkin hükümlere uygun olması gerektiği;

24/03/2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 6. maddesi ve 652 sayılı Kanun Hükmünde Kararname'nin 43. maddesine 02/12/2016 tarihinde eklenen 3. fıkrasıyla 01/09/2017 tarihinden itibaren biyometrik kimlik doğrulama sistemi uygulamasına cevaz verilmiş ise de, belirtilen Kanun Hükmünde Kararname hükümlerinin (yürürlüğe giriş tarihi 694 sayılı KHK'nın 183.

maddesiyle 01/09/2018 olarak deęiştirildięinden) henüz yürürlüęe girmemiş olduęu ve 6698 sayılı Kanun'un koruyucu ve bilgilendirici hükümlerinin davaya konu kuralın tesisinden sonra yürürlüęe girdięi ve belli kořullarda kişisel verilere erişime izin verildięi gözetildięinde, işlemler tarihi itibarıyla Yönetmeliğin dava konusu ilgili hükümlerini hukuka uygun hale getirmeyeceęi;

Kişisel verilerin işlenmesine ilişkin olarak davaya konu düzenlemenin tesis edildięi tarihte, Anayasa'nın 20. maddesi hükmü çerçevesinde yürürlüęe konulmuş yasal bir düzenleme bulunmadıęı gibi, kişisel verilerin alınması, depolanması ve işlenmesi konusunda işlemler tesis etme yönünden davalı idareye yetki veren bir yasanın da mevcut olmadığı;

Bu bağlamda, Anayasa hükümleri ve Türkiye'nin taraf olduęu uluslararası andlaşmalar uyarınca güvence altına alınan ve kanunla düzenlenmesi gereken kişisel verilerin işlenmesine ilişkin olarak uygulamanın sınırlarını, kişisel verinin nasıl depolanıp, kullanılacağını tespit eden; usul ve esaslarını gösteren dava konusu düzenlemeden önce yürürlüęe konulmuş dayanak bir yasal düzenleme olmaması nedeniyle, dava konusu Yönetmeliğin 25. maddesinin 3. ve 4. fıkralarında hukuka uyarlık bulunmadıęı gerekçesiyle dava konusu düzenlemelerin iptaline karar verilmiştir.

TEMYİZ EDENİN İDDİALARI: Davalı idare tarafından, dava konusu Yönetmelik hükümleri mevzuatta öngörülen usul ve esaslar doğrultusunda hukuka uygun bir şekilde tesis edildięi halde farklı bir yorumla deęerlendirme yapılarak oluşturulan gerekçe ile verilen Daire kararında hukuki isabet bulunmadıęından, kararın bozulması gerektięi ileri sürülmektedir.

KARŐI TARAFIN SAVUNMASI: Davacı tarafından, Danıştay Sekizinci Dairesince verilen kararın usul ve hukuka uygun bulunduęu ve temyiz dilekçesinde öne sürülen nedenlerin, kararın bozulmasını gerektirecek nitelikte olmadığı belirtilerek temyiz isteminin reddi gerektięi savunulmaktadır.

DANIŐTAY TETKİK HÂKİMİ ...'UN DÜŐÜNCESİ: Temyiz isteminin reddi ile Daire kararının onanması gerektięi düşünölmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay İdari Dava Daireleri Kurulunca, Tetkik Hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereęi görüőüldü:

HUKUKİ DEęERLENDİRME:

2577 sayılı İdari Yargılama Usulü Kanunu'nun 49. maddesinin ikinci fıkrasında, Danıştay dava dairelerinin nihai kararlarının temyizen incelenerek bozulmasının;

"a) Görev ve yetki dışında bir işe bakılmış olması,

b) Hukuka aykırı karar verilmesi,

c)Usul hükümlerinin uygulanmasında kararı etkileyebilecek nitelikte hata veya eksikliklerin bulunması" sebeplerinden birinin varlığı hâlinde mümkün olduğu belirtilmiş; dördüncü fıkrasında, "Danıştayın ilk derece mahkemesi olarak baktığı davaların temyizen incelenmesinde bu madde ile ısrar hariç 50. madde hükümleri kıyasen uygulanır." denilmiş; 50. maddesinin dördüncü fıkrasında ise Danıştayın bozma kararına uyulduğu takdirde, bu kararın temyiz incelemesinin, bozma kararına uygunlukla sınırlı olarak yapılacağı hükme bağlanmıştır.

Danıştay Sekizinci Dairesinin temyize konu kararı; Danıştay İdari Dava Daireleri Kurulunun 19/12/2018 tarih ve E:2015/432, K:2018/503 sayılı kısmen bozma kararında belirtilen gerekçeler göz önüne alınarak verilmiş bir karar olduğundan, usul ve hukuka uygun bulunmakta ve bozulmasını gerektirecek bir hukuka aykırılık taşımamaktadır.

KARAR SONUCU:

Açıklanan nedenlerle;

1. Davalı idarenin temyiz isteminin reddine,

2. Dava konusu düzenlemenin yukarıda özetlenen gerekçeyle iptaline ilişkin Danıştay Sekizinci Dairesinin temyize konu 26/11/2019 tarih ve E:2019/4434, K:2019/10746 sayılı kararının ONANMASINA,

3.Bu kararın tebliğ tarihini izleyen günden itibaren 15 (onbeş) gün içinde karar düzeltme yolu açık olmak üzere, 08/04/2021 tarihinde oyçokluğu ile karar verildi.

KARŞI OY

X- Daire kararında, kişisel verilerin işlenmesine ilişkin olarak davaya konu düzenlemenin tesis edildiği tarihte, Anayasa'nın 20. maddesi hükmü çerçevesinde yürürlüğe konulmuş yasal bir düzenleme bulunmadığı gibi, kişisel verilerin alınması, depolanması ve işlenmesi konusunda işlem tesis etme yönünden davalı idareye yetki veren bir yasanın da mevcut olmadığı; 24/03/2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 6. maddesi ve 652 sayılı Kanun Hükmünde Kararname'nin 43. maddesine 02/12/2016 tarihinde eklenen 3. fıkrasıyla 01/09/2017 tarihinden itibaren biyometrik kimlik doğrulama sistemi uygulamasına cevaz verilmiş ise de, belirtilen Kanun Hükmünde Kararname hükümlerinin (yürürlüğe giriş tarihi 694 sayılı KHK'nın 183. maddesiyle

01/09/2018 olarak deęiştirildięinden) henüz yürürlüğe girmemiş olduęu ve 6698 sayılı Kanun'un koruyucu ve bilgilendirici hükümlerinin davaya konu kuralın tesisinden sonra yürürlüğe girdięi ve belli koşullarda kişisel verilere erişime izin verildięi gözetildięinde, işlem tarihi itibarıyla Yönetmeliğin dava konusu ilgili hükümlerini hukuka uygun hale getirmeyeceęi gerekçesiyle dava konusu Yönetmeliğin 25. maddesinin 3. ve 4. fıkralarının iptaline karar verilmiştir.

Ancak, karar tarihinden önce, kişisel verilerin işlenmesinde başta özel hayatın gizlilięi olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek amacıyla hazırlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu 07/04/2016 tarih ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiş, 652 sayılı Kanun Hükmünde Kararname'nin 43. maddesine 02/12/2016 tarihinde eklenen 3. fıkra ile 01/09/2018 tarihinden itibaren biyometrik kimlik doğrulama sistemi uygulamasına cevaz verilmiştir.

Düzenleyici işlemlerin hukuka uygunluk denetimi yapılırken, bireysel işlemlerden farklı olarak "işlemin tesis edildięi tarih itibarıyla deęerlendirilmesi" genel ilkesi yerine, düzenleyici işlemlerin "karar tarihi itibarıyla" deęerlendirilmesi gerekmektedir. Zira, düzenleyici işlemlerde, işlemin yürürlüğe konulduęu tarihte üst hukuk normlarına aykırılık bulunsa/bulunmasa da zaman içinde üst hukuk normlarında yapılan düzenlemeler ya da üst hukuk normlarına ilişkin olarak Anayasa Mahkemesi ve idari yargı mercilerince verilen kararlar nedeniyle dava konusu edilen düzenleyici işlemler, yasal dayanaktan yoksun kalabileceęi gibi, sonradan yasal dayanaęa da kavuşabilir.

Belirtilen nedenlerle, karar tarihi itibarıyla dava konusu Yönetmeliğin 25. maddesinin 3. ve 4. fıkralarının kanuni dayanaęının bulunduęu ve üst hukuk normlarına aykırılık taşımadıęı sonucuna varıldıęından, davanın reddine karar verilmesi gerekirken, 652 sayılı Kanun Hükmünde Kararname'nin 43. maddesinin karar tarihi itibarıyla son hali göz önünde bulundurulmaksızın verilen iptal kararının bozulması gerektięi oyuyla, karara katılmıyorum.

Danıştay Kararı - İDDK., E. 2020/1454 K. 2021/732 T. 8.4.2021

T.C. DANIŞTAY İDARİ DAVA DAİRELERİ KURULU

Esas No: 2020/1454

Karar No: 2021/732

TEMYİZ EDEN (DAVALI): ... Bakanlığı

VEKİLİ: Hukuk Müşaviri ...

KARŞI TARAF (DAVACI): ... Derneği

VEKİLİ: Av. ...

İSTEMİN KONUSU: Danıştay Sekizinci Dairesinin 26/11/2019 tarih ve E:2019/4435, K:2019/10747 sayılı kararının temyizen incelenerek bozulması istenilmektedir.

YARGILAMA SÜRECİ:

Dava konusu istem: 18/05/2012 tarih ve 28296 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Milli Eğitim Bakanlığı Özel Eğitim Kurumları Yönetmeliği'nin 3. maddesinin 1. fıkrasının (e) bendinin, 16. maddesinin 3. fıkrasının, 19. maddesinin 1. fıkrasının, 20. maddesinin 1. fıkrasının, 22. maddesinin 2. fıkrasının, 25. maddesinin 2., 3. ve 4. fıkralarının, 29. maddesinin birinci fıkrasının (f) bendinin, 31. maddesinin 1. ve 4. fıkralarının iptali istenilmiştir.

Daire kararının özeti: Danıştay Sekizinci Dairesinin 26/11/2019 tarih ve E:2019/4435, K:2019/10747 sayılı kararıyla; davanın reddine yönelik Dairelerinin 22/10/2014 tarih ve E:2012/10387, K:2014/7306 sayılı kararının, dava konusu Yönetmeliğin 25. maddesinin 3. ve 4. fıkralarına yönelik kısımlarının Danıştay İdari Dava Daireleri Kurulunun 19/12/2018 tarih ve E:2015/426, K:2018/504 sayılı kararıyla bozulması üzerine söz konusu bozma kararına uyularak;

Anayasa'nın "Özel hayatın gizliliği" başlıklı 20. maddesinde, herkesin, özel hayatına ve aile hayatına saygı gösterilmesini isteme ve kendisiyle ilgili kişisel verilerin korunmasının isteme hakkına sahip olduğu; bu hakkın; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı; kişisel verilerin, ancak kanunda öngörülen hallerde veya

kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmek suretiyle, kişisel verilerin korunmasının, özel hayatın gizliliğinin korunması kapsamında güvenceye bağlandığı;

Öte yandan, Avrupa İnsan Hakları Sözleşmesi'nin "Özel Hayatın ve Aile Hayatının Korunması" başlıklı 8. maddesinde, herkesin özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahip olduğu, bu hakkın kullanılmasına bir kamu makamının müdahalesinin, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabileceğinin kurala bağlandığı; Birleşmiş Milletler Medeni ve Siyasal Haklar Sözleşmesi'nin "Mahremiyet Hakkı" başlıklı 17. maddesinde ise, hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemeyeceği; onuru veya itibarının hukuka aykırı saldırılara maruz bırakılmayacağı, herkesin bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahip olduğunun belirtildiği;

652 Sayılı Milli Eğitim Bakanlığı Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 36. maddesinin 1. fıkrasında, Bakanlığın, görev, yetki ve sorumluluk alanına giren ve önceden kanunla izin verilen konularda idari düzenlemeler yapabileceğinin hüküm altına alındığı;

Dava konusu Yönetmeliğin 25. maddesinin 3. fıkrasında, kurumlarca engelli bireylerin ders devam takiplerinin, ders başlangıcından önce ve ders bitiminde engelli birey modülünde yer alan kimlik doğrulama sistemi ile yapılacağı; 4. fıkrasında, kurumlarca; eğitim personelinin ders devam takibinin ise giriş ve çıkışlarda engelli birey modülünde yer alan kimlik doğrulama sistemi ile yapılacağı kurallarına yer verildiği;

İdarelerce, gelişen teknolojinin kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması amacıyla, kamu kesiminde kullanılmaya başlanması mümkün olmakla birlikte, teknoloji kullanılarak kişisel verilerin kayıt altına alınması uygulamasının, ilgili Anayasal düzenleme uyarınca belirli bir yasal çerçeve içine oturtulması, konuya ilişkin usul ve esasların yasa hükmü ile tespit edilmesi ve yine Anayasa'daki ve Türkiye'nin taraf olduğu uluslararası andlaşmalardaki temel hak ve özgürlüklere ilişkin hükümlere uygun olması gerektiği;

24/03/2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 6. maddesi ve 652 sayılı Kanun Hükmünde Kararname'nin 43. maddesine 02/12/2016 tarihinde eklenen 3. fıkrasıyla 01/09/2017 tarihinden itibaren biyometrik kimlik doğrulama sistemi uygulamasına cevaz verilmiş ise de, belirtilen Kanun Hükmünde Kararname hükümlerinin (yürürlüğe giriş tarihi 694 sayılı KHK'nın 183.

maddesiyle 01/09/2018 olarak deęiştirildięinden) henüz yürürlüęe girmemiş olduęu ve 6698 sayılı Kanun'un koruyucu ve bilgilendirici hükümlerinin davaya konu kuralın tesisinden sonra yürürlüęe girdięi ve belli kořullarda kişisel verilere erişime izin verildięi gözetildięinde, işlemler tarihi itibarıyla Yönetmeliğin dava konusu ilgili hükümlerini hukuka uygun hale getirmeyeceęi;

Kişisel verilerin işlenmesine ilişkin olarak davaya konu düzenlemenin tesis edildięi tarihte, Anayasa'nın 20. maddesi hükmü çerçevesinde yürürlüęe konulmuş yasal bir düzenleme bulunmadıęı gibi, kişisel verilerin alınması, depolanması ve işlenmesi konusunda işlemler tesis etme yönünden davalı idareye yetki veren bir yasanın da mevcut olmadığı;

Bu bağlamda, Anayasa hükümleri ve Türkiye'nin taraf olduęu uluslararası andlaşmalar uyarınca güvence altına alınan ve kanunla düzenlenmesi gereken kişisel verilerin işlenmesine ilişkin olarak uygulamanın sınırlarını, kişisel verinin nasıl depolanıp, kullanılacağını tespit eden; usul ve esaslarını gösteren dava konusu düzenlemeden önce yürürlüęe konulmuş dayanak bir yasal düzenleme olmaması nedeniyle, dava konusu Yönetmeliğin 25. maddesinin 3. ve 4. fıkralarında hukuka uyarlık bulunmadıęı gerekçesiyle dava konusu düzenlemelerin iptaline karar verilmiştir.

TEMYİZ EDENİN İDDİALARI: Davalı idare tarafından, kamu yararı ve hizmet gereęi tesis edilen düzenlemenin iptaline ilişkin Daire kararı ile dayanan gerekçede hukuki isabet bulunmadıęından, kararın bozulması gerektięi ileri sürülmektedir.

KARŞI TARAFIN SAVUNMASI: Davacı tarafından, Danıştay Sekizinci Dairesince verilen kararın usul ve hukuka uygun bulunduęu ve temyiz dilekçesinde öne sürülen nedenlerin, kararın bozulmasını gerektirecek nitelikte olmadığı belirtilerek temyiz isteminin reddi gerektięi savunulmaktadır.

DANIŞTAY TETKİK HÂKİMİ ...'UN DÜŞÜNCESİ: Temyiz isteminin reddi ile Daire kararının onanması gerektięi düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay İdari Dava Daireleri Kurulunca, Tetkik Hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereęi görüldü:

HUKUKİ DEĞERLENDİRME:

2577 sayılı İdari Yargılama Usulü Kanunu'nun 49. maddesinin ikinci fıkrasında, Danıştay dava dairelerinin nihai kararlarının temyizen incelenerek bozulmasının;

"a) Görev ve yetki dışında bir işe bakılmış olması,

b) Hukuka aykırı karar verilmesi,

c)Usul hükümlerinin uygulanmasında kararı etkileyebilecek nitelikte hata veya eksikliklerin bulunması" sebeplerinden birinin varlığı hâlinde mümkün olduğu belirtilmiş; dördüncü fıkrasında, "Danıştayın ilk derece mahkemesi olarak baktığı davaların temyizen incelenmesinde bu madde ile ısrar hariç 50. madde hükümleri kıyasen uygulanır." denilmiş; 50. maddesinin dördüncü fıkrasında ise Danıştayın bozma kararına uyulduğu takdirde, bu kararın temyiz incelemesinin, bozma kararına uygunlukla sınırlı olarak yapılacağı hükme bağlanmıştır.

Danıştay Sekizinci Dairesinin temyize konu kararı; Danıştay İdari Dava Daireleri Kurulunun 19/12/2018 tarih ve E:2015/426, K:2018/504 sayılı kısmen bozma kararında belirtilen gerekçeler göz önüne alınarak verilmiş bir karar olduğundan, usul ve hukuka uygun bulunmakta ve bozulmasını gerektirecek bir hukuka aykırılık taşımamaktadır.

KARAR SONUCU:

Açıklanan nedenlerle;

1. Davalı idarenin temyiz isteminin reddine,
2. Dava konusu düzenlemenin yukarıda özetlenen gerekçeyle iptaline ilişkin Danıştay Sekizinci Dairesinin temyize konu 26/11/2019 tarih ve E:2019/4435, K:2019/10747 sayılı kararının ONANMASINA,
- 3.Bu kararın tebliğ tarihini izleyen günden itibaren 15 (onbeş) gün içinde karar düzeltme yolu açık olmak üzere, 08/04/2021 tarihinde oyçokluğu ile karar verildi.

KARŞI OY

X- Daire kararında, kişisel verilerin işlenmesine ilişkin olarak davaya konu düzenlemenin tesis edildiği tarihte, Anayasa'nın 20. maddesi hükmü çerçevesinde yürürlüğe konulmuş yasal bir düzenleme bulunmadığı gibi, kişisel verilerin alınması, depolanması ve işlenmesi konusunda işlem tesis etme yönünden davalı idareye yetki veren bir yasanın da mevcut olmadığı; 24/03/2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 6. maddesi ve 652 sayılı Kanun Hükmünde Kararname'nin 43. maddesine 02/12/2016 tarihinde eklenen 3. fıkrasıyla 01/09/2017 tarihinden itibaren biyometrik kimlik doğrulama sistemi uygulamasına cevaz verilmiş ise de, belirtilen Kanun Hükmünde Kararname hükümlerinin (yürürlüğe giriş tarihi 694 sayılı KHK'nın 183. maddesiyle 01/09/2018 olarak değiştirildiğinden) henüz yürürlüğe girmemiş olduğu ve 6698 sayılı Kanun'un

koruyucu ve bilgilendirici hükümlerinin davaya konu kuralın tesisinden sonra yürürlüğe girdiği ve belli koşullarda kişisel verilere erişime izin verildiği gözetildiğinde, işlem tarihi itibarıyla Yönetmeliğin dava konusu ilgili hükümlerini hukuka uygun hale getirmeyeceği gerekçesiyle dava konusu Yönetmeliğin 25. maddesinin 3. ve 4. fıkralarının iptaline karar verilmiştir.

Ancak, karar tarihinden önce, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek amacıyla hazırlanan 6698 sayılı Kanun 07/04/2016 tarih ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiş, 652 sayılı Kanun Hükmünde Kararname'nin 43. maddesine 02/12/2016 tarihinde eklenen 3. fıkra ile 01/09/2018 tarihinden itibaren biyometrik kimlik doğrulama sistemi uygulamasına cevaz verilmiştir.

Düzenleyici işlemlerin hukuka uygunluk denetimi yapılırken, bireysel işlemlerden farklı olarak "işlemin tesis edildiği tarih itibarıyla değerlendirilmesi" genel ilkesi yerine, düzenleyici işlemlerin "karar tarihi itibarıyla" değerlendirilmesi gerekmektedir. Zira, düzenleyici işlemlerde, işlemin yürürlüğe konulduğu tarihte üst hukuk normlarına aykırılık bulunsa/bulunmasa da zaman içinde üst hukuk normlarında yapılan düzenlemeler ya da üst hukuk normlarına ilişkin olarak Anayasa Mahkemesi ve idari yargı mercilerince verilen kararlar nedeniyle dava konusu edilen düzenleyici işlemler, yasal dayanaktan yoksun kalabileceği gibi, sonradan yasal dayanağa da kavuşabilir.

Belirtilen nedenlerle, karar tarihi itibarıyla dava konusu Yönetmeliğin 25. maddesinin 3. ve 4. fıkralarının kanuni dayanağının bulunduğu ve üst hukuk normlarına aykırılık taşımadığı sonucuna varıldığından, davanın reddine karar verilmesi gerekirken, 652 sayılı Kanun Hükmünde Kararname'nin 43. maddesinin karar tarihi itibarıyla son hali göz önünde bulundurulmaksızın verilen iptal kararının bozulması gerektiği oyuyla, karara katılmıyorum.

Danıştay Kararı - İDDK., E. 2020/1038 K. 2021/735 T. 8.4.2021

T.C. DANIŞTAY İDARİ DAVA DAİRELERİ KURULU

Esas No: 2020/1038

Karar No: 2021/735

TEMYİZ EDEN (DAVALI): ... Bakanlığı

VEKİLİ: Av. ...

KARŞI TARAF (DAVACI): ... Eğitim Kurumları Derneği

VEKİLİ: Av. ...

İSTEMİN KONUSU: Danıştay Sekizinci Dairesinin 09/10/2019 tarih ve E:2014/11070, K:2019/8510 sayılı kararının temyizen incelenerek bozulması istenilmektedir.

YARGILAMA SÜRECİ:

Dava konusu istem: Milli Eğitim Bakanlığı Özel Öğretim Kurumları Genel Müdürlüğünün 23/09/2014 tarih ve 4145908 sayılı onayı ile işleme konulan "Özel Eğitim ve Rehabilitasyon Merkezlerinde Kullanılan Sayısallaştırılmış Kimlik Bilgisi Doğrulama Sisteminin Uygulama Usul ve Esasları"nın 5. maddesinin 3. fıkrasının iptali istenilmiştir.

Daire kararının özeti: Danıştay Sekizinci Dairesinin 09/10/2019 tarih ve E:2014/11070, K:2019/8510 sayılı kararıyla;

Davalı İdarenin usule ilişkin iddası yerinde görülmemiş,

Esas yönünden;

Anayasa'nın "Özel hayatın gizliliği" başlıklı 20. maddesinde, herkesin, özel hayatına ve aile hayatına saygı gösterilmesini isteme ve kendisiyle ilgili kişisel verilerin korunmasının isteme hakkına sahip olduğu; bu hakkın; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı; kişisel verilerin, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla

düzenleneceği belirtilmek suretiyle, kişisel verilerin korunmasının, özel hayatın gizliliğinin korunması kapsamında güvenceye bağlandığı;

Öte yandan, Avrupa İnsan Hakları Sözleşmesi'nin "Özel Hayatın ve Aile Hayatının Korunması" başlıklı 8. maddesinde, herkesin özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahip olduğu, bu hakkın kullanılmasına bir kamu makamının müdahalesinin, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabileceğinin kurala bağlandığı; Birleşmiş Milletler Medeni ve Siyasal Haklar Sözleşmesi'nin "Mahremiyet Hakkı" başlıklı 17. maddesinde ise, hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemeyeceği; onuru veya itibarının hukuka aykırı saldırılara maruz bırakılmayacağı, herkesin bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahip olduğunun belirtildiği;

652 Sayılı Milli Eğitim Bakanlığı Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 36. maddesinin 1. fıkrasında, Bakanlığın, görev, yetki ve sorumluluk alanına giren ve önceden kanunla izin verilen konularda idari düzenlemeler yapabileceğinin hüküm altına alındığı;

18/05/2012 tarih ve 28296 sayılı Resmi Gazete'de yayımlanan Milli Eğitim Bakanlığı Özel Eğitim Kurumları Yönetmeliği'nin dava konusu işlemin tesis edildiği tarihteki haliyle "Günlük çalışma saatleri ve devam devamsızlık takibi" başlıklı 25. maddesinin 3. fıkrasında, kurumlarca engelli bireylerin ders devam takiplerinin, ders başlangıcından önce ve ders bitiminde engelli birey modülünde yer alan kimlik doğrulama sistemi ile yapılacağı; 4. fıkrasında, kurumlarca; eğitim personelinin ders devam takibinin ise giriş ve çıkışlarda engelli birey modülünde yer alan kimlik doğrulama sistemi ile yapılacağı; 5. fıkrasında da, kimlik doğrulama sisteminin uygulanması ile sistemi kullanamayacak durumda olan engelli birey ve eğitim personelinin ders devam takibinin Bakanlıkça belirlenecek usul ve esaslara göre yapılacağı ve engelli birey ve eğitim personelinin kimlik doğrulama sistemine tanıtılmalarının ise rehberlik araştırma merkezlerince yapılacağı kurallarına yer verildiği;

Milli Eğitim Bakanlığı Özel Öğretim Kurumları Genel Müdürlüğü'nün 05/06/2014 tarih ve 2296439 sayılı işlemi ile özel eğitim ve rehabilitasyon merkezlerinde eğitim alan engelli bireyler ile eğitim personelinin ders devam takiplerine ilişkin kimlik doğrulama sisteminin avuç içi damar izi yöntemiyle yapılmasına karar verildiği;

Milli Eğitim Bakanlığınca getirilen yukarıda bahsedilen kimlik doğrulama sisteminin avuç içi damar izi yöntemini uygulamak için Özel Eğitim Kurumları Genel Müdürlüğü'nün 23/09/2014 tarih ve 4145908 sayılı onayı ile "Özel Eğitim ve Rehabilitasyon Merkezlerinde Kullanılan Sayısallaştırılmış Kimlik Bilgisi Doğrulama Sisteminin Uygulama Usul ve Esasları"nın işleme konulduğu;

Avuç içi damar tanıma teknolojisinin, avuç içinde bulunan kan damarlarının her insanda farklı olmasından yola çıkılarak oluşturulmuş bir biyometrik kimlik doğrulama sistemi olup anılan sistemin tamamen kişiye özel biyometrik bilgileri içerdiği ve kişinin özel hayatına ilişkin kişisel bir veri olduğu hususunda kuşku bulunmadığı;

Anayasa Mahkemesinin kişisel veri kavramının tanımlandığı 25/12/2014 tarih ve E:2014/74, K:2014/201 sayılı kararında; kişisel veri kavramının, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade ettiği; bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamında olduğunun belirtildiği;

İdarelerce gelişen teknolojinin kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması amacıyla, kamu kesiminde kullanılmaya başlanması mümkün olmakla birlikte, teknoloji kullanılarak kişisel verilerin kayıt altına alınması uygulamasının; ilgili Anayasal düzenleme uyarınca belirli bir yasal çerçeve içine oturtulması, konuya ilişkin usul ve esasların yasa hükmü ile tespit edilmesi ve yine Anayasa'daki ve Türkiye'nin taraf olduğu uluslararası andlaşmalardaki temel hak ve özgürlüklere ilişkin hükümlere uygun olması gerektiğinin kuşkusuz olduğu;

Kişisel verilerin işlenmesine ilişkin olarak davaya konu düzenlemenin tesis olunduğu tarihte, Anayasa'nın 20. maddesi hükmü çerçevesinde yürürlüğe konulmuş yasal bir düzenleme bulunmadığı gibi, kişisel verilerin alınması, depolanması ve işlenmesi konusunda işlem tesis etme yönünden davalı idareye yetki veren bir kanuni düzenlemenin de mevcut olmadığı;

Her ne kadar 24/03/2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 6. maddesi ve 652 sayılı Kanun Hükmünde Kararname'nin 43. maddesine 02/12/2016 gününde eklenen 3. fıkrası ile 01/09/2018 tarihinden itibaren biyometrik kimlik doğrulama sistemi uygulamasına cevaz verilmiş ise de; belirtilen Kanun Hükmünde Kararname hükümlerinin dava konusu işlemin tesis edildiği tarihte yürürlükte olmadığı ve 6698 sayılı Kanun'un koruyucu ve bilgilendirici hükümlerinin davaya konusu işlemin tesisinden sonra yürürlüğe girdiği ve belli koşullarda kişisel verilere erişime izin verildiği

gözetildiğinde, işlem tarihi itibarıyla değerlendirilen dava konusu düzenlemenin bütün yönleri ile hukuka uygun hale gelmeyeceği;

Bu durumda, Anayasa hükümleri ve Türkiye'nin taraf olduğu uluslararası andlaşmalar uyarınca güvence altına alınan ve kanunla düzenlenmesi gereken kişisel verilerin işlenmesine ilişkin olarak uygulamanın sınırlarını, kişisel verinin nasıl depolanıp, kullanılacağını tespit eden; usul ve esaslarını gösteren bir yasal düzenleme olmadan çıkarılan Yönetmelik hükmü doğrultusunda tesis edilen işlemde hukuka uyarlık bulunmadığı;

Dava konusu düzenlemenin dayanağı olan, özel eğitim ve rehabilitasyon merkezlerinde eğitim alan engelli bireyler ile eğitim personelinin ders devam takiplerine ilişkin kimlik doğrulama sisteminin avuç iç damar izi yöntemiyle yapılmasına ilişkin Milli Eğitim Bakanlığı Özel Öğretim Kurumları Genel Müdürlüğünün 05/06/2014 tarih ve 2296439 sayılı işleminin Dairelerinin 20/03/2019 tarih ve E:2014/5926 K:2019/2018 sayılı kararı ile ve Özel Eğitim Kurumları Yönetmeliği'nin 25. maddesinin 3. ve 4. fıkralarının ise 14/06/2017 tarih ve E:2012/6447, K:2017/5293 sayılı kararı ile iptaline karar verildiği; 05/07/2018 tarih ve 30469 sayılı Resmi Gazete'de yayımlanan Özel Eğitim Kurumları Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmeliğin 16. maddesi ile de anılan Yönetmeliğin 25. maddesinin 3. ve 4. fıkralarının yürürlükten kaldırıldığı gerekçesiyle, dava konusu düzenlemenin iptaline karar verilmiştir.

TEMYİZ EDENİN İDDİALARI: Davalı idare tarafından, 652 sayılı Milli Eğitim Bakanlığı Teşkilat ve Görevleri Hakkında KHK'nın 36. maddesinde, Bakanlığın görev, yetki ve sorumluluk alanına giren ve önceden kanunla düzenlenmiş konularda idari düzenleme yapabilme yetkisi bulunduğundan dava konusu işlemin yasal dayanağı bulunduğu, Yönetmelik hükmünün uygulamaya geçirilmesi amacıyla hazırlanan düzenlemede hukuka ve mevzuata aykırılık bulunmadığı; düzenleme ile engelli bireylerin eğitimlerini eğitim verme şartlarını taşıyan personelden eksiksiz bir şekilde almalarını sağlamak suretiyle engelli bireylerin eğitim haklarının korunması ve engelli bireyler üzerinden haksız kazanç elde edilmesinin önüne geçilmesinin amaçlandığı ileri sürülmektedir.

KARŞI TARAFIN SAVUNMASI: Davacı tarafından, savunma verilmemiştir.

DANIŞTAY TETKİK HÂKİMİ ...'UN DÜŞÜNCESİ: Temyiz isteminin reddi ile Daire kararının onanması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay İdari Dava Daireleri Kurulunca, Tetkik Hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereği görüldü:

HUKUKİ DEĞERLENDİRME:

Danıştay dava dairelerinin nihai kararlarının temyizen incelenerek bozulması, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 49. maddesinde yer alan;

"a) Görev ve yetki dışında bir işe bakılmış olması,

b) Hukuka aykırı karar verilmesi,

c)Usul hükümlerinin uygulanmasında kararı etkileyebilecek nitelikte hata veya eksikliklerin bulunması" sebeplerinden birinin varlığı hâlinde mümkündür.

Temyizen incelenen karar usul ve hukuka uygun olup, temyiz dilekçesinde ileri sürülen iddialar kararın bozulmasını gerektirecek nitelikte görülmemiştir.

KARAR SONUCU:

Açıklanan nedenlerle;

1. Davalı idarenin temyiz isteminin reddine,

2.Dava konusu düzenlemenin yukarıda özetlenen gerekçeyle iptaline ilişkin Danıştay Sekizinci Dairesinin temyize konu 09/10/2019 tarih ve E:2014/11070, K:2019/8510 sayılı kararının ONANMASINA,

3.Kesin olarak, 08/04/2021 tarihinde oyçokluğu ile karar verildi.

KARŞI OY

X-Daire kararında, kişisel verilerin işlenmesine ilişkin olarak davaya konu düzenlemenin tesis edildiği tarihte, Anayasa'nın 20. maddesi hükmü çerçevesinde yürürlüğe konulmuş yasal bir düzenleme bulunmadığı gibi, kişisel verilerin alınması, depolanması ve işlenmesi konusunda işlem tesis etme yönünden davalı idareye yetki veren bir yasanın da mevcut olmadığı; 24/03/2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 6. maddesi ve 652 sayılı Kanun Hükmünde Kararname'nin 43. maddesine 02/12/2016 tarihinde eklenen 3. fıkrasıyla 01/09/2017 tarihinden itibaren biyometrik kimlik doğrulama sistemi uygulamasına cevaz verilmiş ise de, belirtilen Kanun Hükmünde Kararname hükümlerinin (yürürlüğe giriş tarihi 694 sayılı KHK'nın 183. maddesiyle 01/09/2018 olarak değiştirildiğinden) henüz yürürlüğe girmemiş olduğu ve 6698 sayılı Kanun'un koruyucu ve bilgilendirici hükümlerinin davaya konu kuralın tesisinden sonra yürürlüğe girdiği ve belli koşullarda kişisel verilere erişime izin verildiği gözetildiğinde, işlem tarihi itibarıyla

değerlendirilen dava konusu düzenlemeyi bütün yönleri ile hukuka uygun hale getirmeyeceği gerekçesiyle dava konusu Milli Eğitim Bakanlığı Özel Öğretim Kurumları Genel Müdürlüğü işleminin iptaline karar verilmiştir.

Ancak, karar tarihinden önce, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek amacıyla hazırlanan 6698 sayılı Kanun 07/04/2016 tarih ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiş, 652 sayılı Kanun Hükmünde Kararname'nin 43. maddesine 02/12/2016 tarihinde eklenen 3. fıkra ile 01/09/2018 tarihinden itibaren biyometrik kimlik doğrulama sistemi uygulamasına cevaz verilmiştir.

Düzenleyici işlemlerin hukuka uygunluk denetimi yapılırken, bireysel işlemlerden farklı olarak "işlemin tesis edildiği tarih itibarıyla değerlendirilmesi" genel ilkesi yerine, düzenleyici işlemlerin "karar tarihi itibarıyla" değerlendirilmesi gerekmektedir. Zira, düzenleyici işlemlerde, işlemin yürürlüğe konulduğu tarihte üst hukuk normlarına aykırılık bulunsa/bulunmasa da zaman içinde üst hukuk normlarında yapılan düzenlemeler ya da üst hukuk normlarına ilişkin olarak Anayasa Mahkemesi ve idari yargı mercilerince verilen kararlar nedeniyle dava konusu edilen düzenleyici işlemler, yasal dayanaktan yoksun kalabileceği gibi, sonradan yasal dayanağa da kavuşabilir.

Belirtilen nedenlerle, karar tarihi itibarıyla Milli Eğitim Bakanlığı Özel Eğitim Kurumları Yönetmeliği'nin 25. maddesinin 3. ve 4. fıkralarının kanuni dayanağının bulunduğu ve üst hukuk normlarına aykırılık taşımadığı anlaşıldığından, bu hükümler uyarınca tesis edilen Milli Eğitim Bakanlığı Özel Öğretim Kurumları Genel Müdürlüğü işleminde de hukuka aykırılık bulunmadığından, davanın reddine karar verilmesi gerekirken, 652 sayılı Kanun Hükmünde Kararname'nin 43. maddesinin karar tarihi itibarıyla son hali göz önünde bulundurulmaksızın verilen iptal kararının bozulması gerektiği oyuyla, karara katılmıyorum.

Danıştay Kararı - İDDK. (E. 2020/937)

Danıştay Kararı - İDDK., E. 2020/937 K. 2020/2778 T. 30.11.2020

T.C. DANIŞTAY İDARİ DAVA DAİRELERİ KURULU

Esas No: 2020/937

Karar No: 2020/2778

TEMYİZ EDEN (DAVALILAR): 1- ...

VEKİLİ: Hukuk Müşaviri ...

2- ... Bakanlığı

VEKİLİ: Av. ...

KARŞI TARAF (Davacı): ...

İSTEMİN KONUSU: Danıştay Onuncu Dairesinin 30/05/2019 tarih ve E:2014/5529, K:2019/4587 sayılı kararının iptale ilişkin kısmının temyizen incelenerek bozulması istenilmektedir.

YARGILAMA SÜRECİ:

Dava konusu istem: 22/12/2012 tarih ve 28505 sayılı Resmi Gazete'de yayımlanan ... tarih ve ... sayılı Bakanlar Kurulu kararı ile yürürlüğe konulan Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanunun Uygulanmasına İlişkin Yönetmeliğin 6., 11. ve 21. maddelerinin iptali istenilmiştir.

Daire kararının özeti: Danıştay Onuncu Dairesinin 30/05/2019 tarih ve E:2014/5529, K:2019/4587 sayılı kararıyla;

Dava konusu Yönetmeliğin dayanağını teşkil eden eden 6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun'un 5. maddesinin 4. fıkrasının ikinci, üçüncü, dördüncü ve beşinci cümleleri ile 11. fıkrasının itiraz yoluyla iptali için yapılan başvuru üzerine verilen Anayasa Mahkemesinin 12/11/2015 tarih ve E:2014/196, K:2015/103 sayılı kararına dayanılarak;

Yönetmeliğin 6. maddesinin incelenmesi:

Yönetmeliğin "Merkezi spor güvenlik biriminin görev, yetki ve sorumlulukları" başlıklı 6. maddesinde; "(1) Merkezi spor güvenlik biriminin görev, yetki ve sorumlulukları şunlardır:

a) Spor güvenlik birimleri arasında koordinasyonu sağlamak.

- b) Seyirden yasaklanma tedbirlerine ilişkin bilgilerin kaydedildiği elektronik bilgi bankasını oluşturmak.
- c) Federasyonlar bünyesinde oluşturulan merkezi veri tabanına spor güvenlik birimlerinin erişimini sağlamak.
- ç) Elektronik bilgi bankasında yer alan seyirden yasaklanma tedbirine ilişkin bilgileri, spor kulüpleri ve ilgili federasyonların erişiminin sağlanması amacıyla Spor Genel Müdürlüğü Türkiye Futbol Federasyonu ve spor güvenlik birimlerinin elektronik ortamda erişimine açmak.
- d) Haklarında seyirden yasaklanma tedbiri bulunanlara ilişkin bilgileri, gerektiğinde yurtdışında yapılacak müsabakalardan önce müsabakanın yapılacağı ülkenin yetkili mercilerine bildirmek.
- e) Yurtdışında yapılacak olan uluslararası müsabakalarda mücadele edecek spor kulüpleri ile milli takım ve bunların taraftarlarının güvenliği konusunda koordinasyonu sağlamak üzere ilgili müsabaka için spor kulübünün bulunduğu ilin spor güvenlik biriminden bir ve kendi biriminden bir olmak üzere en az iki personeli görevlendirmek.
- f) Gerektiğinde yurtdışında müsabakalara katılacak spor kulübünün kulüp güvenlik sorumlusu ve taraftardan sorumlu kulüp temsilcisi ile güvenlik organizasyonu konusunda toplantılar yapmak; il spor güvenlik birimi ve kendi personelinden görevlendirilen en az iki personele ilgili spor kulübü kulüp güvenlik sorumlusu ve taraftardan sorumlu kulüp temsilcisi ile birlikte müsabakadan önce yurtdışındaki müsabaka alanını incelettirmek, rakip spor kulübü yetkilileri ve diğer ülke genel kolluk görevlileri ile irtibat kurmalarını ve güvenlik toplantısı yapmalarını sağlamak ve alınan kararların müsabaka gününe kadar ilgili mercilerle birlikte uygulanmasını denetlemek.
- g) Yurtdışındaki uluslararası müsabakalarda güvenlik organizasyonu için görevlendirilen genel kolluk görevlilerinin müsabaka gününden bir gün önce ilgili ülkeye intikalini ve güvenlik toplantısına katılmasını temin etmek, diğer ülke genel kolluk görevlileri ve spor kulübü temsilcileriyle irtibat kurarak müsabakanın güvenliği ile ilgili koordinasyonu sağlamak.
- ğ) Ülkemizde yapılacak olan uluslararası müsabakalarda ilgili genel kolluk biriminden en az bir personelin görevlendirilmesini ve görevlendirilen personelin müsabaka güvenlik amiri ve spor kulübünün güvenlik sorumlusu ile irtibatını sağlamak, misafir seyircinin müsabakayı güvenli biçimde izlemesini ve haklarında seyirden yasaklanma tedbiri alınmış yurtdışından gelen kişilerin spor alanlarına sokulmaması için gerekli tedbirleri aldirmek.
- h) Spor güvenlik birimlerine ve müsabaka güvenlik amirlerine ulusal ve Uluslararası gelişmeler konusunda ilgili mercilerle birlikte eğitim verilmesini sağlamak.

ı) Kanuna göre ceza almış kişilerle ilgili istatistiki verilerin tutulmasını sağlamak.

ı) Diğer ülkelerin genel kolluk teşkilatı ile spor güvenliği konusunda işbirliği yapmak ve bu konuda yurtiçi ve yurtdışında yapılan toplantılara katılmak."

düzenlemesine yer verildiği,

Yönetmeliğin dayanağını oluşturan 6222 sayılı Kanun'un tanımlara ilişkin 3. maddesinin birinci fıkrasının (d) bendinde "merkezi spor güvenlik birimi"nin Emniyet Genel Müdürlüğü bünyesinde kurulan ilgili birimi ifade ettiği, (ğ) bendinde ise "spor güvenlik birimi"nin sorumluluk alanlarına göre il ve ilçe emniyet müdürlükleri veya jandarma komutanlıkları tarafından kurulan ilgili birimi ifade ettiğinin hükme bağlandığı, Kanun'un 4. maddesinde il ve ilçe spor güvenlik kurullarının oluşturulmasının, 5. maddesinde genel olarak spor alanlarının güvenlik ve düzenine ilişkin tedbirlerin, 6. maddesinde saha güvenliğine ilişkin konuların, 7. maddesinde müsabakaların güvenliğine ilişkin konuların, 10. maddesinde seyir güvenliğinin sağlanması konusunun, 12. maddesinde spor alanlarına sokulması yasak maddelere ilişkin hususların, 13. maddesinde spor alanlarına yasak madde sokulması ve müsabaka düzeninin bozulması konusunun, 15. maddesinde spor alanlarına usulsüz seyirci girişi ile ilgili hükümlerin, 18. maddesinde seyirden yasaklanma güvenlik tedbirine dair esasların düzenlendiği, 18. maddenin dördüncü fıkrasında "Koruma tedbiri olarak uygulanan ve güvenlik tedbiri olarak hükmedilen spor müsabakalarını seyirden yasaklama tedbirine ilişkin bilgiler Emniyet Genel Müdürlüğü bünyesinde tutulan bu amaca özgü elektronik bilgi bankasına derhal kaydedilir. Bu bilgi bankasına spor kulüplerinin ve federasyonların erişimi sağlanır. Yasaklanan kişilere ilişkin bilgiler, ilgili spor kulüplerine ve yurt dışında yapılacak müsabaka öncesinde müsabakanın yapılacağı ülkenin yetkili mercilerine bildirilir." hükmüne yer verildiği, Yönetmeliğin 6. maddesi incelendiğinde, maddenin 6222 sayılı Kanun'un anılan hükümlerinin uygulamaya geçirilmesi kapsamında ve anılan hükümler çerçevesinde düzenlendiğinin görüldüğü,

Bu durumda, Yönetmeliğin 6. maddesinin, 6222 sayılı Kanun'un 3., 4., 5., 6., 7., 10., 12., 13., 15. ve 18. maddesinde yer alan hükümler çerçevesinde düzenlendiği, söz konusu Yönetmelik maddesinde dayanağı Kanuna ve üst hukuk normlarına aykırılık bulunmadığı,

Yönetmeliğin 11. maddesinin 1. fıkrasının (a) bendinin incelenmesi:

Yönetmeliğin "Federasyonların görev, yetki ve sorumlulukları" başlıklı 11. maddesinin 1. fıkrasında, "Federasyonların görev, yetki ve sorumlulukları şunlardır:" ibaresine yer verildikten sonra (a) bendinde "Milli müsabakalarda, spor müsabakasına seyirci olarak girecek kişilerin kontrolünü

yaptırmak, haklarında seyirden yasaklanma tedbiri bulunanların spor alanlarına girişlerini engellemek ve tespit edilenleri genel kolluk kuvvetlerine bildirmek." hükmüne yer verildiği,

Yönetmeliğin 11. maddesinin 1. fıkrasının (a) bendi ile federasyonlara verilen "milli müsabakalarda, spor müsabakasına seyirci olarak girecek kişilerin kontrolünü yaptırmak", şeklinde ifade edilen görev, yetki ve sorumluluğun, Yönetmeliğin dayanağını oluşturan 6222 sayılı Kanun'un 5. maddesinin 4. fıkrasında yer alan "... Spor müsabakalarına, kişi ancak adına düzenlenen elektronik kart ile izleyici olarak girebilir. Spor müsabakasına izleyici olarak girecek kişilerin kontrolünü ev sahibi kulüp yapmakla yükümlüdür. Bu yükümlülük ev sahibi olmayan müsabakalarda, müsabakaya katılan her iki kulüp; milli müsabakalarda ise, ilgili federasyon tarafından yerine getirilir." hükmüne dayandığı, "haklarında seyirden yasaklanma tedbiri bulunanların spor alanlarına girişlerini engellemek ve tespit edilenleri genel kolluk kuvvetlerine bildirmek." şeklinde ifade edilen görev, yetki ve sorumlulukların ise anılan Kanun'un 18 ve 22. maddelerinde düzenlenen "seyirden yasaklanma" güvenlik tedbirinin hayata geçirilmesi kapsamında düzenlendiği; bu nedenle söz konusu Yönetmelik hükmünde dayanağı Kanuna ve üst hukuk normlarına aykırılık bulunmadığı,

Yönetmeliğin 11. maddesinin birinci fıkrasının (b) bendinin (1) numaralı alt bendinin incelenmesi:

Yönetmeliğin "Federasyonların görev, yetki ve sorumlulukları" başlıklı 11. maddesinin 1. fıkrasında, "Federasyonların görev, yetki ve sorumlulukları şunlardır:" ibaresine yer verildikten sonra (b) bendinin (1) numaralı alt bendinde "Bilet organizasyonu ve seyircilerin müsabaka alanlarına giriş ve çıkışına ilişkin kontrol ve denetimi gerçekleştirmek ve bu amaçla bünyesinde merkezi kontrol sistemi oluşturmak ve kurulacak sistemi kulüplerin hizmetine sunmak." hükmünün düzenlendiği,

Yönetmeliğin 11. maddesinin (b) bendinin (1) numaralı alt bendi ile Federasyonlara verilen "bilet organizasyonu ve seyircilerin müsabaka alanlarına giriş ve çıkışına ilişkin kontrol ve denetimi gerçekleştirmek", "bu amaçla bünyesinde merkezi kontrol sistemi oluşturmak" ve "kurulacak sistemi kulüplerin hizmetine sunmak" şeklinde ifade edilen görev, yetki ve sorumlulukların, Yönetmeliğin dayanağını oluşturan 6222 sayılı Kanun'un 5. maddesinin 11. fıkrasının (a) bendinde yer alan "Bilet organizasyonu ve seyircilerin müsabaka alanlarına giriş ve çıkışına ilişkin kontrol ve denetim yetkisi federasyonlara ait olup federasyonlar bu amaçla bünyelerinde merkezi kontrol sistemi oluşturur." hükmünün tekrarı niteliğinde olduğu,

6222 sayılı Kanun'un 5. maddesinde, spor alanlarının güvenlik ve düzeni için başta ev sahibi olmak üzere spor kulüplerinin yerine getirmesi gereken yükümlülükler, alınacak güvenlik tedbirleri, elektronik kart ve bilet uygulaması ve bunların gerçekleştirilme usullerinin düzenlendiği;

“Devlet, her yaştaki Türk vatandaşlarının beden ve ruh sađlığını geliřtirecek tedbirleri alır, sporun kitlelere yayılmasını teřvik eder.” kuralını ieren Anayasa'nın 59. maddesinin gerekesinde “Sporun geliřtirilmesi sadece fiilen spor yapanlara deđil, seyirciler iin de eđitici ve sađlık kurallarına uygun bir ortamda yařamaya sevk edici etkileri sebebiyle Devlete ele alınması iin bir bařka sebeptir.” ifadelerine yer verildiđi,

Bu durumda, Yönetmeliđin 11. maddesinin (b) bendinin (1) numaralı alt bendinin, Anayasa'nın 59. maddesinin öngördüđu yükümlölük kapsamında, sportif faaliyetlerde gerekleřen řiddetin toplum üzerinde oluřturduđu tehlike ve sportif faaliyetlerde iřlenen suçlardaki artış dikkate alınarak düzenlenen 6222 sayılı Kanun'un 5. maddesinin 11. fıkrasının (a) bendinde yer alan hükümlere paralel olarak düzenlendiđi, bu nedenle söz konusu Yönetmelik hükmünde dayanađı Kanuna ve üst hukuk normlarına aykırılık bulunmadıđı,

Yönetmeliđin 11. maddesinin 1. fıkrasının (b) bendinin (2) numaralı alt bendinin incelenmesi:

Yönetmeliđin "Federasyonların görev, yetki ve sorumlulukları" bařlıklı 11. maddesinin 1. fıkrasında, "Federasyonların görev, yetki ve sorumlulukları řunlardır:" ibaresine yer verildikten sonra (b) bendinin (2) numaralı alt bendinde "Elektronik kart oluřturmak amacıyla alınacak kiřisel bilgileri merkezi veri tabanında tutmak ve bu veri tabanını Maliye Bakanlıđı ve İiřleri Bakanlıđının eriřimine aık tutmak ve veri tabanları arasındaki eriřimi sađlamak." hükmüne yer verildiđi,

Yönetmeliđin 11. maddesinin (b) bendinin (2) numaralı alt bendi incelendiđinde, Federasyonlara verilen “elektronik kart oluřturmak amacıyla alınacak kiřisel bilgileri merkezi veri tabanında tutmak”, “bu veri tabanını Maliye Bakanlıđı ve İiřleri Bakanlıđının eriřimine aık tutmak” ve “veri tabanları arasındaki eriřimi sađlamak” řeklinde ifade edilen görev, yetki ve sorumlulukların, Yönetmeliđin dayanađını oluřturan 6222 sayılı Kanun'un 5. maddesinin 11. fıkrasının (a) bendinde yer alan “Elektronik kart oluřturulmak amacıyla alınacak kiřisel bilgiler federasyon bünyesinde oluřturulan merkezi veri tabanında tutulur. Bu veri tabanı Maliye Bakanlıđı ve İiřleri Bakanlıđı eriřimine aıktır.” hükmüne paralel olarak düzenlendiđi,

Anayasa Mahkemesinin yukarıda belirtilen kararıyla 6222 sayılı Kanun'un 5. maddesinin 11. fıkrasının (a) bendinde yer alan düzenlemeye yönelik olarak Anayasa aykırılık itirazının reddedildiđi,

Bu durumda, Yönetmeliđin 11. maddesinin 1. fıkrasının (b) bendinin (2) numaralı alt bendinin, 6222 sayılı Kanun'un 5. maddesinin 11. fıkrasının (a) bendinde yer alan hükümlere paralel olarak düzenlendiđi, bu nedenle söz konusu Yönetmelik hükmünde dayanađı Kanuna ve üst hukuk normlarına aykırılık bulunmadıđı,

Yönetmeliğin 11. maddesinin 1. fıkrasının (b) bendinin (3) numaralı alt bendinin incelenmesi:

Yönetmeliğin "Federasyonların görev, yetki ve sorumlulukları" başlıklı 11. maddesinin 1. fıkrasında, "Federasyonların görev, yetki ve sorumlulukları şunlardır:" ibaresine yer verildikten sonra (b) bendinin (3) numaralı alt bendinde "Sistem üzerinden merkezi satışları gerçekleştirmek, kart bilgilerinin kulüpler adına reklam ve pazarlamasını yapmak, haklarında seyirden yasaklanma tedbiri bulunanlara bilet satışı yapılmaması için her türlü tedbiri almak." hükmüne yer verildiği,

Yönetmeliğin 11. maddesinin 1. fıkrasının (b) bendinin (3) numaralı alt bendi incelendiğinde, Federasyonlara verilen "sistem üzerinden merkezi satışları gerçekleştirmek" ve "kart bilgilerinin kulüpler adına reklam ve pazarlamasını yapmak" şeklinde ifade edilen görev, yetki ve sorumlulukların, Yönetmeliğin dayanağını oluşturan 6222 sayılı Kanun'un 5. maddesinin 11. fıkrasının (b) ve (c) bentlerinde yer alan "Elektronik kart ile elektronik kart kapsamında satışı gerçekleştirilecek biletlerin basım, satış ve dağıtımına ilişkin yerel uygulamalar kulüpler tarafından, sistem üzerinden merkezi satışları ise ilgili federasyonlar tarafından gerçekleştirilir." ve "Elektronik kart bilgilerinin kulüpler adına reklam ve pazarlamasında ilgili federasyonlar yetkilidir..." hükümleri kapsamında, "haklarında seyirden yasaklanma tedbiri bulunanlara bilet satışı yapılmaması için her türlü tedbiri almak" şeklinde ifade edilen görev, yetki ve sorumluluğun ise 6222 sayılı Kanun'un 18. ve 22. maddelerinde düzenlenen "seyirden yasaklanma" güvenlik tedbirinin hayata geçirilmesi kapsamında düzenlendiği,

Yönetmeliğin 11. maddesinin 1. fıkrasının (b) bendinin (3) numaralı alt bendinde yer alan "Sistem üzerinden merkezi satışları gerçekleştirmek" ibaresinin incelenmesi:

Yönetmeliğin 11. maddesinin 1. fıkrasının (b) bendinin (3) numaralı alt bendinde, federasyonlara görev, yetki ve sorumluluk olarak düzenlenen "Sistem üzerinden merkezi satışları gerçekleştirmek" ibaresi ile getirilen düzenlemenin 6222 sayılı Kanun'un 5. maddesinin 11. fıkrasının (b) bendine dayanılarak hazırlandığı,

Anayasa Mahkemesinin yukarıda deyinilen kararında da belirtildiği üzere, anılan hükmün kamu düzeni ve güvenliği açısından büyük önem arz eden sporda şiddetin önlenmesi için alınan tedbirler kapsamında düzenlendiği ve sistem üzerinden merkezi bilet satışının, dayanak 6222 sayılı Kanun'un gerekçesinde de bahsedildiği üzere kamu düzenini korumak, toplumun, refah, huzur ve mutluluğunu etkileyen sporda şiddetin önlenmesini sağlamak, dolayısıyla kişilerin can ve mal güvenliğini de korumak amacıyla düzenlendiği; bu sistemde bilet satışlarının sadece elektronik kart üzerinden yapılabileceği ve spor müsabakasına kişinin ancak adına düzenlenmiş elektronik kart ile girebileceği, bilet organizasyonun, seyircilerin müsabakalara giriş ve çıkış kontrolleri ilgili

federasyonlarca gerçekleştirileceđi, belirtilen kart ve biletlerin basım, satıř ve dađıtımına iliřkin yerel uygulamaların kulüplerce, sistem üzerinden merkezi satıřların ise ilgili federasyonlarca yapılacađı, uygulama ile harici bilet satıřı ya da taraftar gruplarına toplu bilet temininin mümkün olmayacađı, bir kiřinin ancak kendi adına düzenlenmiř kart ile müsabakalara girebileceđinden yasaklanan kiřilerin başkasına ait bilet ile müsabakalara girmelerinin engellenebileceđi, elektronik kart ve bilet uygulaması ile bu kapsamda biletlerin basımı, satıřı ve dađıtımlarına iliřkin olarak kulüplere verilen görevler ve biletlerin merkezi satıřları ile bilet organizasyonu ve seyircilerin müsabaka alanlarına giriř ve çıkıřlarının kontrol ve denetimi federasyonlara verilen görevlerin, geliřen, büyüyen, çeřitlenen ve çođalan, zamanında ve etkin tedbir alınmadıđı takdirde engellenmesi daha da güçleřecek olan sporda řiddet sorununu çözmeye ve sporseverlerin kurallara uymalarını sađlama amacı için gerekli ve elveriřli olmadıđının söylenemeyeceđi, sportif müsabakaları izleyecek olanların faaliyetlerini engelleyecek, sınırlayacak nitelikte bir uygulama olmayan, günümüz teknolojisine uygun olarak bilet yüklenmesini ve denetimini kolaylařtıran, tüm spor müsabakalarında aynı kuralların uygulanması sonucu bütünlüğü sađlayan, içerisinde güvenlik amaçlı sınırlı sayıda bilgi barındıran elektronik kart uygulamasının getirilmesi ile daha önce kullanılan basılı bilet kullanılarak gerçekleştirilen uygulama arasında ulařılmak istenen amaç bakımından bir orantısızlık olduđundan da söz edilemeyeceđi ve Yönetmeliđin 11. maddesinin (b) bendinin (3) numaralı alt bendinde yer alan "Sistem üzerinden merkezi satıřları gerçekleřtirmek" ibaresinin, 6222 sayılı Kanun'un 5. maddesinin 11. fıkrasının (b) bendinde yer alan hükümlere paralel olarak düzenlendiđi anlařılmakta olup, dayanađı Kanuna ve üst hukuk normlarına aykırılık bulunmadıđı,

Yönetmeliđin 11. maddesinin 1. fıkrasının (b) bendinin (3) numaralı alt bendinde yer alan "kart bilgilerinin kulüpler adına reklam ve pazarlamasını yapmak," ibaresinin incelenmesi:

Yönetmeliđin 11. maddesinin 1. fıkrasının (b) bendinin (3) numaralı alt bendinde, federasyonlara görev, yetki ve sorumluluk olarak düzenlenen "kart bilgilerinin kulüpler adına reklam ve pazarlamasını yapmak" ibaresi ile getirilen düzenlemenin 6222 sayılı Kanun'un 5. maddesinin 11. fıkrasının (c) bendinin birinci cümlesine dayanılarak hazırlandıđı,

Anılan cümlede "Elektronik kart bilgilerinin kulüpler adına reklam ve pazarlamasında ilgili federasyonlar yetkilidir." kuralına yer verildiđi, Anayasa Mahkemesinin 12/11/2015 tarih ve E:2014/196, K:2015/103 sayılı kararıyla; "söz konusu yetkinin federasyona verilmesi suretiyle özel hayatın ve kiřisel verilerin korunması haklarına getirilen sınırlandırmanın sportif faaliyetlerde yařanan řiddeti önleme amacını gerçekleřtirmeye elveriřli olmadıđı, belirtilen amaç için gerekli ve

elverişli olmayan kuralın ölçülülük ilkesine uygun olmadığı" gerekçesiyle anılan cümlelerin Anayasa'nın 13. ve 20. maddelerine aykırı olduğuna hükmedilerek iptal edildiği,

Bu durumda, dayanağı olan 6222 sayılı Kanun'un 5. maddesinin 11. fıkrasının (c) bendinin birinci cümlesinin Anayasa Mahkemesinin 12/11/2015 tarih ve E:2014/196, K:2015/103 sayılı kararı ile iptal edilmiş olması karşısında, Anayasaya aykırılığı sabit olan kanuni düzenlemeye dayanılarak tesis edilen dava konusu, Yönetmeliğin 11. maddesinin birinci fıkrasının (b) bendinin (3) numaralı alt bendinde yer alan "kart bilgilerinin kulüpler adına reklam ve pazarlamasını yapmak," ibaresinde hukuka uyarlık bulunmadığı ve iptal edilmesi gerektiği sonucuna varıldığı,

Yönetmeliğin 11. maddesinin 1. fıkrasının (b) bendinin (3) numaralı alt bendinde yer alan "haklarında seyirden yasaklanma tedbiri bulunanlara bilet satışı yapılmaması için her türlü tedbiri almak" ibaresinin incelenmesi:

Yönetmeliğin 11. maddesinin 1. fıkrasının (b) bendinin (3) numaralı alt bendinde, federasyonlara görev, yetki ve sorumluluk olarak düzenlenen "haklarında seyirden yasaklanma tedbiri bulunanlara bilet satışı yapılmaması için her türlü tedbiri almak" ibaresi ile getirilen düzenlemenin 6222 sayılı Kanun'un 18. ve 22. maddelerinde düzenlenen "seyirden yasaklanma" güvenlik tedbirinin hayata geçirilmesi kapsamında düzenlendiği,

6222 sayılı Kanun'un (karar tarihi itibarıyla yürürlükte olan haliyle) "Seyirden yasaklama" başlıklı 18. maddesinde "seyirden yasaklanma" güvenlik tedbirinin verilme esaslarının düzenlendiği,

Anılan maddenin 3. fıkrasında, madde kapsamına giren suçlardan dolayı soruşturma başlatılması halinde şüpheli hakkında spor müsabakalarını seyirden yasaklama tedbirinin derhal uygulamaya konulacağı, 4. fıkrasında koruma tedbiri olarak uygulanan ve güvenlik tedbiri olarak hükmedilen spor müsabakalarını seyirden yasaklama tedbirine ilişkin bilgilerin Emniyet Genel Müdürlüğü bünyesinde tutulan bu amaca özgü elektronik bilgi bankasına derhal kaydedileceği, bu bilgi bankasına spor kulüplerinin ve federasyonların erişiminin sağlanacağı, yasaklanan kişilere ilişkin bilgilerin, ilgili spor kulüplerine ve yurt dışında yapılacak müsabaka öncesinde müsabakanın yapılacağı ülkenin yetkili mercilerine bildirileceği, 6. fıkrasında kamu davasının açılmasının ertelenmesine, hükmün açıklanmasının geri bırakılmasına, hapis cezası yerine seçenek yaptırım olarak tedbire veya hapis cezasının ertelenmesine karar verilmesi halinde, kararın kesinleştiği tarihten itibaren, önödeme halinde ise, önödemede bulunduğu tarihten itibaren, bir yıl süreyle spor müsabakalarını seyirden yasaklama tedbirinin uygulanmasına devam edileceği hususlarının hükme bağlandığı; "Şiddete neden olabilecek açıklamalar" başlıklı 22. maddesinde ise; "(1) Sporda şiddeti teşvik edecek şekilde basın ve yayın yoluyla açıklamada bulunan kişilere, fiilleri suç oluşturmadığı

takdirde, beşbin Türk Lirasından ellibin Türk Lirasına kadar idari para cezası verilir. ... (3) Birinci fıkra kapsamına giren fiilleri işleyen kişiler, ayrıca idari tedbir olarak spor müsabakalarını seyirden yasaklanır. Bu yasak, kararın verildiği tarihten itibaren üç ay süreyle uygulanır. Koruma tedbiri olarak yasak kararının uygulanmasına ilişkin esas ve usuller, bu tedbir bakımından da uygulanır. Ancak 18 inci maddenin sekizinci fıkrası hükmü bu kişiler bakımından uygulanmaz..." kuralına yer verildiği,

Anılan Kanun hükümlerinin incelenmesinden, kanun koyucunun spor müsabakalarını seyirden yasaklama kararını, sporda şiddetin önlenmesi, kamu düzeninin ve güvenliğinin sağlanması, bireylerin can ve mal güvenliğinin temin edilmesi kapsamında bir güvenlik tedbiri olarak düzenlediği, Kanun'un 18. maddesinin 4. fıkrasında düzenlenen "Koruma tedbiri olarak uygulanan ve güvenlik tedbiri olarak hükmedilen spor müsabakalarını seyirden yasaklama tedbirine ilişkin bilgiler Emniyet Genel Müdürlüğü bünyesinde tutulan bu amaca özgü elektronik bilgi bankasına derhal kaydedilir. Bu bilgi bankasına spor kulüplerinin ve federasyonların erişimi sağlanır." kuralının uygulanması kapsamında Yönetmeliğin 11. maddesinin 1. fıkrasının (b) bendinin (3) numaralı alt bendinde "haklarında seyirden yasaklanma tedbiri bulunanlara bilet satışı yapılmaması için her türlü tedbiri almak" ibaresi ile de Kanun'un 18. ve 22. maddeleri kapsamında federasyonlara görev, yetki ve sorumluluk verildiğinin anlaşıldığı,

Bu durumda, Yönetmeliğin 11. maddesinin 1. fıkrasının (b) bendinin (3) numaralı alt bendinde yer alan "haklarında seyirden yasaklanma tedbiri bulunanlara bilet satışı yapılmaması için her türlü tedbiri almak" ibaresinde dayanağı Kanuna ve üst hukuk normlarına aykırılık bulunmadığı,

Yönetmeliğin 11. maddesinin 1. fıkrasının (c) ila (p) bentlerinin incelenmesi:

Yönetmeliğin 11. maddesinin 1. fıkrasının (c) ila (p) bentleri incelendiğinde, (ç) bendinde yer alan "Kanun hükümlerine göre hakkında güvenlik tedbiri olarak spor müsabakalarını seyirden yasaklanma kararı verilen kişilerin yasak süresince federasyon yönetiminde yer almamasını ve spor müsabakalarında hakem, temsilci veya gözlemci olarak görev almamasını sağlamak" şeklindeki görev, yetki ve sorumlulukların 6222 sayılı Kanun'un 18. maddesinin 10. fıkrasında yer alan "Bu Kanun hükümlerine göre hakkında güvenlik tedbiri olarak spor müsabakalarını seyirden yasaklanma kararı verilen kişi, yasak süresince spor kulüplerinde ve federasyonlarda ve taraftar derneklerinde yönetici olamaz; spor müsabakalarında hakem, temsilci veya gözlemci olarak görev yapamaz." hükmü kapsamında; (e) bendinde yer alan "biletsiz seyirci girişini önleyici tedbirler aldırarak ve denetlemek" şeklindeki görev, yetki ve sorumlulukların 6222 sayılı Kanun'un 5/3-ç maddesinde yer alan "Müsabaka alanlarına kapasitenin üzerinde veya biletsiz seyirci alınamaz." hükmü kapsamında,

diğer bentlerde düzenlenen görev, yetki ve sorumlulukların ise 6222 sayılı Kanun'un 4. maddesinde düzenlenen "il ve ilçe spor güvenlik kurullarının oluşturulması", 5. maddesinde düzenlenen "genel olarak spor alanlarının güvenlik ve düzenine ilişkin alınacak tedbirler", 6. maddesinde düzenlenen "saha güvenliğine ilişkin konular", 7. maddesinde düzenlenen "müsabakaların güvenliğine ilişkin konular", 10. maddesinde düzenlenen "seyir güvenliğinin sağlanması konusu", 12. maddesinde düzenlenen "spor alanlarına sokulması yasak maddelere ilişkin hususlar", 13. maddesinde düzenlenen "spor alanlarına yasak madde sokulması ve müsabaka düzeninin bozulması konusu", 15. maddesinde düzenlenen "spor alanlarına usulsüz seyirci girişi ile ilgili hükümler" ile 18. maddesinde düzenlenen "seyirden yasaklanma güvenlik tedbirine dair esaslar" çerçevesinde, 6222 sayılı Kanun'un anılan hükümlerinin uygulamaya geçirilmesi kapsamında düzenlendiği,

Bu durumda, Yönetmeliğin 11. maddesinin 1. fıkrasının (c) ila (p) bentlerinin, 6222 sayılı Kanun'un 4., 5., 6., 7., 10., 12., 13., 15. ve 18. maddesinde yer alan hükümler çerçevesinde düzenlendiği, bu nedenle Yönetmeliğin anılan bentlerinde Yönetmeliğin dayanağı Kanuna ve üst hukuk normlarına aykırılık bulunmadığı,

Yönetmeliğin 21. maddesinin 3. fıkrasının (a) bendinin ikinci cümlesinin incelenmesi:

Yönetmeliğin "Biletlerin basılması ve satışa sunulması" başlıklı 21. maddesinin 3. fıkrasının (a) bendinin birinci cümlesinde "Elektronik kart üzerinde kişilerin adı, soyadı, Türkiye Cumhuriyeti kimlik numarası ve fotoğrafının bulunması zorunludur." kuralına yer verildiği, anılan hükümden sonra gelen ikinci cümlede ise "Elektronik kart üzerinde bulunacak diğer bilgileri belirleme yetkisi ilgili federasyona aittir." kuralının düzenlendiği,

6222 sayılı Kanun'un 5. maddesinin 4. fıkrasında "Spor müsabakalarının yapıldığı alanlara girişi sağlayacak biletler, elektronik sistem üzerinden oluşturulur. Bilet satın almak isteyen kişilerle ilgili olarak, üzerinde adı, soyadı, Türkiye Cumhuriyeti kimlik numarası ve fotoğrafı olan bir elektronik kart oluşturulur. Kişinin yabancı olması halinde kart üzerinde Türkiye Cumhuriyeti kimlik numarası yerine uyruğu olduğu devletin adı ile Türkiye'ye giriş yaptığı pasaportun seri numarası kaydedilir." kuralına yer verildiği, Yönetmeliğin 21. maddesinin 3. fıkrasının (a) bendinin ikinci cümlesinde dayanağı Kanun'un 5. maddesinin dördüncü fıkrasında düzenlenmiş olan elektronik kart üzerinde bulunması gereken bilgileri aşacak şekilde ve hukuki belirlilikten uzak bir biçimde "Elektronik kart üzerinde bulunacak diğer bilgileri belirleme yetkisi ilgili federasyona aittir." şeklindeki ikinci cümlede Yönetmeliğin dayanağı olan 6222 sayılı Kanun'un 5. maddesinin dördüncü fıkrası hükmüne uyarlık bulunmadığı ve anılan ikinci cümlenin iptal edilmesi gerektiği sonucuna varıldığı,

Yönetmeliğin 21. maddesinin 3. fıkrasının (c) bendinin incelenmesi:

Yönetmeliğin “Biletlerin basılması ve satışa sunulması” başlıklı 21. maddesinin 3. fıkrasında “Elektronik kart uygulaması ile ilgili olarak aşağıda yer alan usul ve esaslara uyulur:” ibaresinden sonra gelmek üzere (c) bendinde “c) Kulüpler, kişisel bilgilerin kullanılmasına ilişkin olarak seyircilerden elektronik ortamda veya yazılı muvafakatlerini alırlar. Muvafakatin içeriğinde kişisel bilgiler ile bağlı bulunan federasyon ve kulüplere ilişkin bilgilerin bulunmasının yanısıra bu bilgilerin Kanunda belirtilen görev ve yetkilerini yerine getirmesi amacıyla, federasyonun sponsorları ve anlaşma yaptığı kurumların reklam ve diğer hizmetleri için kullanılabileceği ve saklanabileceği hususları yer alır.” kuralına yer verildiği,

Anayasanın “Özel hayatın gizliliği” başlıklı 20. maddesinin 3. fıkrasında “Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.” hükmüne, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Kişisel verilerin işleme şartları" başlıklı 5. maddesinde;

“1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.” kuralına, “Özel nitelikli kişisel verilerin işleme şartları” başlıklı 6. maddesinde ise; “(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı,

dini, mezhebi veya diğler inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliđi, sađlıđı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır." kuralına yer verildiđi,

Diğler taraftan, dava konusu Yönetmeliđin dayanađı olan 6222 sayılı Kanun'un 5. maddesinin 11. fıkrasının (c) bendinde yer alan "Elektronik kart bilgilerinin kulüpler adına reklam ve pazarlamasında ilgili federasyonlar yetkilidir." şeklindeki birinci cümlenin Anayasa Mahkemesinin 12/11/2015 tarih ve E:2014/196, K:2015/103 sayılı kararı ile iptal edilmiş olması karşısında, Anayasa'ya aykırılıđı sabit olan kanuni düzenlemeye dayanılarak tesis edilen dava konusu, Yönetmeliđin 21. maddesinin 3. fıkrasının (c) bendinde yer alan "federasyonun sponsorları ve anlaşma yaptıđı kurumların reklam ve diğler hizmetleri için" ibaresinde hukuka uyarlık bulunmadıđı ve iptal edilmesi gerektiđi sonucuna varıldıđı,

Yönetmeliđin 21. maddesinin 3. fıkrasının (ç) bendinin incelenmesi:

Yönetmeliđin "Biletlerin basılması ve satıřa sunulması" bařlıklı 21. maddesinin 3. fıkrasında "Elektronik kart uygulaması ile ilgili olarak ařađıda yer alan usul ve esaslara uyulur:" ibaresinden sonra gelmek üzere (ç) bendinde "(ç) Elektronik kart bilgilerinin kulüpler adına reklam ve pazarlamasında ilgili federasyonlar yetkilidir. Merkezi pazarlama ve bilet satıřından elde edilecek gelirler kulüplere aittir. Federasyon ya da yetki verdiđi üçüncü kişiler nezdinde oluşacak bu gelirler kamu kurum ve kuruluşlarına ilişkin alacaklar hariç olmak üzere hacedilemez, devir ve temlik edilemez. Federasyonlar bu fıkra kapsamında belirtilen yetkilerini kısmen veya tamamen üçüncü kişilere devredebilir." kuralına yer verildiđi,

Anılan bendin birinci cümlesi yönünden:

Anılan bendin birinci cümlesinde "Elektronik kart bilgilerinin kulüpler adına reklam ve pazarlamasında ilgili federasyonlar yetkilidir." kuralı yer almakta olup, anılan kuralın Yönetmeliđin dayanađı olan 6222 sayılı Kanun'un 5. maddesinin 11. fıkrasının (c) bendinin birinci cümlesinin tekrarı mahiyetinde olduđu,

Bu durumda, dayanađı olan 6222 sayılı Kanununun 5/11-c. maddesinin birinci cümlesinin Anayasa Mahkemesinin 12/11/2015 tarih ve E:2014/196, K:2015/103 sayılı Kararı ile iptal edilmiş olması karşısında, Anayasaya aykırılıđı sabit olan kanuni düzenlemeye dayanılarak tesis edilen dava konusu

Yönetmeliğin 21. maddesinin 3. fıkrasının (ç) bendinin birinci cümlesinde hukuka uyarlık bulunmadığı ve iptal edilmesi gerektiği sonucuna varıldığı,

Anılan bendin dördüncü cümlesi yönünden:

Yönetmeliğin 21. maddesinin üçüncü fıkrasının (ç) bendinin dördüncü cümlesinde “Federasyonlar bu fıkra kapsamında belirtilen yetkilerini kısmen veya tamamen üçüncü kişilere devredebilir.” kuralına yer verildiği, anılan kuralın Yönetmeliğin dayanağı olan 6222 sayılı Kanun'un 5. maddesinin 11. fıkrasının (c) bendinin üçüncü cümlesinin tekrarı mahiyetinde olduğu,

Anayasa Mahkemesinin 12/11/2015 tarih ve E:2014/196, K:2015/103 sayılı kararında, 6222 sayılı Kanun'un 5. maddesinin 11. fıkrasının (c) bendinin üçüncü cümlesine yönelik olarak;

"- Kanunun 5. maddesinin onbirinci fıkrasının (c) bendinin itiraz konusu üçüncü cümlesi, federasyonların fıkra kapsamındaki yetkilerini kısmen ya da tamamen üçüncü kişilere devredebileceğini öngördüğü, üçüncü kişilere kısmen ya da tamamen devredilebilecek yetkilerin; “bilet organizasyonu ve seyircilerin müsabaka alanlarına giriş ve çıkışına ilişkin kontrolü ve denetimi yapmak ile bu amaçla merkezi kontrol sistemi oluşturulması”, “elektronik kart oluşturmak amacıyla alınan kişisel bilgilerin merkezi veri tabanında tutulması”, “elektronik kart ve elektronik kart kapsamında satışı gerçekleştirilecek biletlerin basım, satış ve dağıtımına ilişkin sistem üzerinden merkezi satışlar gerçekleştirilmesi” ve “elektronik kart bilgilerinin kulüpler adına reklam ve pazarlanması” olduğu,

- Kuralda devredilmesi öngörülen “bilet organizasyonu” ve “seyircilerin müsabaka alanlarına giriş ve çıkışına ilişkin kontrol ve denetim yetkisi” ile “bu amaçla merkezi kontrol sistemi oluşturma” ve “elektronik kart ve elektronik kart kapsamında satışı gerçekleştirilecek biletlerin basım, satış ve dağıtımına ilişkin sistem üzerinden merkezi satışlar gerçekleştirme” yetkisinin, Devletin, kamu iktisadî teşebbüslerinin ve diğer kamu tüzelkişilerinin genel idare esaslarına göre yürütmekle yükümlü oldukları kamu hizmetlerinden olmadığı, bu nedenle belirtilen bu görevlerin özel hukuk tüzel kişilerin yerine getirilmesinin mümkün olduğu, spor federasyonlarının da özel hukuk hükümlerine tabi bağımsız nitelikte kuruluşlar olduğu, dolayısıyla tamamen özel hukuk alanında kalan, genel idare esaslarına göre yürütülmesi zorunlu olan kamu hizmetlerinin gerektirdiği asli ve sürekli görev niteliği taşımayan görevlerin idarece yerine getirilme zorunluluğu olmadığı gibi bizatihi federasyonlar eliyle yürütülmesinin de gerekmediği, söz konusu yetkilerin devrinin, Devlete verilen yükümlülükleri öngören Anayasanın 59. maddesine aykırılık oluşturmadığı gibi özel hayatın ve kişisel verilerin korunması hakkını engelleyecek bir nitelik de taşımadığı, bu nedenle kuralın

belirtilen görev dolayısıyla federasyonlara tanınan yetkinin devredilebilmesine olanak sağlamasında Anayasaya aykırılık bulunmadığı,

- Elektronik kart bilgilerinin kulüpler adına reklam ve pazarlanması yetkisinin ilgili federasyonlara verilmesini öngören onbirinci numaralı fıkranın (c) bendinin birinci cümlesi Anayasaya aykırı bulunarak iptal edildiğinden, belirtilen bu yetkinin üçüncü kişilere devrinin Anayasaya uygunluğunun ayrıca incelenmesine gerek görülmediği,

- Öte yandan üçüncü kişilere devredilebilecek yetkiler arasında elektronik kart oluşturmak amacıyla alınan kişisel bilgileri merkezi veri tabanında tutmanın da bulunduğu, bu yetki uyarınca sportif faaliyetleri izlemek isteyenlerin kişisel verilerin bulunduğu veri tabanının ilgili federasyon tarafından üçüncü kişilere devredilebileceği, üstelik bu işlem için kişisel veri sahibi ilgilinin veri paylaşımına rızasının bulunması koşulunun da aranmadığı, ayrıca kişisel veri tabanının devri sonrasında kime, hangi amaçlarla aktarılacağı konusunda da denetim imkânı öngörülmediği, diğer anlatımla kuralın, kötüye kullanım olasılığını engelleyici etkili ve yeterli tedbirlere de yer vermediği, bu durumun kuralı, öngörülme amacının ötesinde kişisel bilgilerin gizliliğinin keyfi şekilde ihlal edilmesi sonucunu doğurabilecek bir araca dönüştürdüğü,

- İptali istenilen düzenlemenin temel amacının sporda şiddeti önlemek ve bu şekilde kamu düzeni ve güvenliğini korumak olduğunun görüldüğü, bu meşru amaç için öngörülen düzenleme uyarınca gerçekleştirilen veri tabanının üçüncü kişilere devrinin özel hayatın ve kişisel verilerin korunması hakkını sınırlandırdığının açık olduğu, ancak kişisel verilerin üçüncü kişilere devri sonucu gerçekleşecek bu sınırlandırmanın elektronik kart ve bilet uygulaması ile gerçekleştirilmek istenilen sporda şiddetin önlenmesine hiçbir katkısının bulunmadığı, hakkı sınırlayan düzenlemeyle, ilgili federasyona, ihtiyaç duyulandan çok daha geniş bir yetki verildiği, bu durumun sınırlama aracıyla sınırlama amacı arasında bulunması gereken makul dengeyi bozmakta, özel hayatın ve kişisel verilerin korunmasını isteme haklarına kuralda belirtilen sınırlama amacı dışında ölçüsüz bir şekilde müdahale edilebilmesine imkân tanımakta olduğu, itiraz konusu kuralla, özel hayatın gizliliğine ve kişisel verilerin korunması hakkına sınırlama getirilirken sınırlama aracının sınırlama amacına uygun ve orantılı olarak kullanılmasını temin edecek güvencelere yer verilmemesinin demokratik toplum düzeninde gerekli olmayan ölçüsüz bir sınırlama niteliğinde olduğu,"

Yönünde belirlemelerde bulunularak, itiraz konusu kuralın, 11. fıkranın (a) bendinin ikinci cümlesi yönünden Anayasa'nın 13., 20. ve 59. maddelerine aykırı olduğu ve kuralın bu cümle ile federasyona verilen yetkinin üçüncü kişilere devri yönünden iptaline; kuralın, 11. fıkranın (a) bendinin ikinci cümlesi dışındaki hükümler yönünden ise Anayasa'nın 13., 20. ve 59. maddelerine aykırı olmadığı ve

belirtilen hükümlerle federasyonlara verilen yetkilerin üçüncü kişilere devri yönünden iptal talebinin reddine hükmedildiği,

Bu durumda, dayanağı ve aynı hükmü içeren 6222 sayılı Kanun'un 5/11-c. maddesinin üçüncü cümlesinin, Anayasa Mahkemesinin 12/11/2015 tarih ve E:2014/196, K:2015/103 sayılı kararıyla 6222 sayılı Kanun'un 5. maddesinin 11. fıkrasının (a) bendinin ikinci cümlesi yönünden Anayasa'nın 13., 20. ve 59. maddelerine aykırı bulunması ve kuralın bu cümle ile federasyona verilen yetkinin üçüncü kişilere devri yönünden iptal edilmiş olması karşısında, Anayasa'ya aykırılığı sabit olan kanuni düzenlemeye dayanılarak tesis edilen dava konusu Yönetmeliğin 21. maddesinin 3. fıkrasının (ç) bendinin dördüncü cümlesinin "elektronik kart oluşturulmak amacıyla alınacak kişisel bilgilerin merkezi veri tabanında tutulması" yetkisinin "üçüncü kişilere devri yönünden" iptal edilmesi gerektiği,

6222 sayılı Kanun'un 5. maddesinin 11. fıkrasının (a) bendinin ikinci cümlesi dışındaki hükümler yönünden Anayasa'nın 13., 20. ve 59. maddelerine aykırı olmadığı ve belirtilen hükümlerle federasyonlara verilen yetkilerin üçüncü kişilere devri yönünden iptal talebinin reddedilmiş olması karşısında, diğer yetkilerin devri bakımından dayanağı Kanuna ve üst hukuk normlarına aykırılık bulunmadığı sonucuna varıldığı,

Yönetmeliğin 21. maddesinin diğer hükümlerinin incelenmesi:

Yönetmeliğin 21. maddesinin 3. fıkrasının (a), (c) ve (ç) bentleri dışında kalan hükümleri incelendiğinde, anılan hükümlerin genel olarak biletlerin, basımı, satışı ve müsabakaların yapılacağı spor alanlarına girişlere ilişkin hükümleri içerdiği ve anılan hükümlerin Yönetmeliğin dayanağı olan 6222 sayılı Kanun'un konuya ilişkin kurallarının uygulamaya geçirilmesi kapsamında düzenlendiğinin görüldüğü,

Bu durumda, Yönetmeliğin 21. maddesinin 3. fıkrasının (a), (c) ve (ç) bentleri dışında kalan hükümlerinde dayanağı Kanuna ve üst hukuk normlarına aykırılık bulunmadığı gerekçeleriyle,

Dava konusu Yönetmeliğin 11. maddesinin 1. fıkrasının (b) bendinin (3) numaralı alt bendinde yer alan "kart bilgilerinin kulüpler adına reklamını ve pazarlamasını yapmak" ibaresinin,

21. maddesinin 3. fıkrasının (a) bendinin ikinci cümlesinin,

21. maddesinin 3. fıkrasının (c) bendinde yer alan "federasyonun sponsorları ve anlaşma yaptığı kurumların reklam ve diğer hizmetleri için" ibaresinin,

21. maddesinin 3. fıkrasının (ç) bendinin birinci cümlesinin,

21. maddesinin 3. fıkrasının (ç) bendinin dördüncü cümlesinin "elektronik kart oluşturmak amacıyla alınacak kişisel bilgilerin merkezi veri tabanında tutulması" yetkisinin "üçüncü kişilere devri" yönünden iptaline,

Dava konusu Yönetmeliğin iptali istenen diğer hükümleri yönünden davanın reddine karar verilmiştir.

TEMYİZ EDENİN İDDİALARI: Davalı idarelerden Cumhurbaşkanlığı tarafından, iptal edilen hükümlerin kişisel verilerin yönetimine ilişkin hususları içerdiği, Daire kararında kişisel verilerin korunması ve yönetiminin yanlış değerlendirildiği, dava konusu Yönetmeliğin seyahat için bilet almaktan farkı bulunmayan sportif faaliyete katılmaya yönelik kişisel veri yönetiminin nasıl yapılacağını tarif ettiği, konunun kişisel verinin işlenmesinden ziyade korunması bağlamında ele alınmasının daha isabetli olacağı, Anayasa'nın 124. maddesi ile 6222 sayılı Kanun'un 24. maddesi kapsamında yürürlüğe konulan dava konusu Yönetmeliğin üst mevzuata aykırılık içermediği belirtilerek, Daire kararının iptale ilişkin kısımlarının bozulması gerektiği ileri sürülmektedir.

Davalı idarelerden Gençlik ve Spor Bakanlığı tarafından ise, Dairece süre ve ehliyetle ilişkin itirazların yeterince karşılanmadığı, temyize konu kararda dayanak olarak alınan Anayasa Mahkemesi kararı üzerine 6222 sayılı Kanun'da değişiklikler yapılarak uygulamada yaşanan sorunların giderildiği, bu haliyle davanın konusuz kaldığı, spor müsabakalarında meydana gelen şiddet olaylarının daha etkin bir biçimde önlenmesi açısından 5149 sayılı Spor Müsabakalarında Şiddet ve Düzensizliğin Önlenmesine Dair Kanun'un yerine 6222 sayılı Kanun'un yürürlüğe konulduğu, anılan Kanun'un sporda şiddetin önlenmesi bakımından Cumhuriyet Savcılıkları ile Emniyet Genel Müdürlüğüne aktif görevler yüklediği, bu çerçevede ilgililerin katılımı ile gerçekleştirilen Sporda Şiddetin Önlenmesi Çalıştayında elektronik bilet uygulamasının yerinde olduğu hususunun vurgulandığı, dava konusu Yönetmeliğin iptali talep edilen hükümlerinin 6222 sayılı Kanun'da aynen yer aldığı, özel hayatın gizliliği kapsamında korunan kişisel verilerin en temel insan haklarından birini teşkil ettiği, bununla birlikte elektronik bilet uygulaması ile Türkiye Futbol Federasyonuna tanınan yetkilerin kişisel verilerin gizliliğini ihlal ettiği yönündeki iddiaya itibar edilemeyeceği, dava konusu düzenleme ile kişisel verilerin denetlenmesi noktasında Türkiye Futbol Federasyonuna herhangi bir yetki tanınmadığı, kart bilgilerinin kulüpler adına reklam ve pazarlanması yetkisinin federasyona verilmesi bakımından da kişisel verilerin ihlalinden söz edilemeyeceği, nitekim Anayasa'nın 20. maddesinin 3. fıkrasında kişisel verilerin kişinin açık rızasıyla işlenebileceği hükmüne yer verildiği, dava konusu Yönetmeliğin 21. maddesinin 3. fıkrasının (c) bendi uyarınca kişisel verilerin kullanımı konusunda kişilerden muvafakat alındığı, bu halde kart bilgilerinin kulüpler adına pazarlanmasına

yönelik hükmün hukuka aykırılığında bahsedilemeyeceği, Kanun'da yazılı bulunan unsurlar haricinde elektronik kart üzerinde hangi verilerin yer alacağı yetkisinin her spor dalına göre ilgili federasyonlara bırakılmasının hukuka aykırı olmadığı, bu hükmün kart üzerinde mutlak surette kanunda sayılan verilerin dışındaki kişisel verilerin yer alacağı anlamına gelmeyeceği, federasyonlara yönelik amblem ve sembollerin yer almasını öngören bir düzenleme niteliğinde olduğu, bu haliyle kişisel verilerin gizliliğini ihlal edici bir yönünün bulunmadığı, Anayasa'nın 124. maddesi ile 6222 sayılı Kanun'un 24. maddesi kapsamında yürürlüğe konulan dava konusu Yönetmeliğin üst mevzuata aykırılık içermediği belirtilerek, Daire kararının iptale ilişkin kısımlarının bozulması gerektiği ileri sürülmektedir.

KARŞI TARAFIN SAVUNMASI: Davacı tarafından, savunma verilmemiştir.

DANIŞTAY TETKİK HÂKİMİ ... DÜŞÜNCE: Temyiz istemlerinin reddi ile Daire kararının onanması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay İdari Dava Daireleri Kurulunca, Tetkik Hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereği görüldü:

HUKUKİ DEĞERLENDİRME:

Danıştay dava dairelerinin nihai kararlarının temyizen incelenerek bozulması, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 49. maddesinde yer alan;

"a) Görev ve yetki dışında bir işe bakılmış olması,

b) Hukuka aykırı karar verilmesi,

c)Usul hükümlerinin uygulanmasında kararı etkileyebilecek nitelikte hata veya eksikliklerin bulunması" sebeplerinden birinin varlığı hâlinde mümkündür.

Temyizen incelenen kararın iptale ilişkin kısımları usul ve hukuka uygun olup, temyiz dilekçelerinde ileri sürülen iddialar kararın bu kısımlarının bozulmasını gerektirecek nitelikte görülmemiştir.

KARAR SONUCU:

Açıklanan nedenlerle;

1. Davalı idarelerin temyiz istemlerinin reddine,

2. Danıştay Onuncu Dairesinin temyize konu 30/05/2019 tarih ve E:2014/5529, K:2019/4587 sayılı kararının iptale ilişkin kısımlarının ONANMASINA,

3. Kesin olarak, 30/11/2020 tarihinde Daire kararının dava konusu Yönetmeliğin 21. maddesinin 3. fıkrasının (a) bendinin ikinci cümlesinin iptaline yönelik kısmı yönünden oyçokluğu, iptale ilişkin diğer kısımları yönünden ise oybirliği ile karar verildi.

KARŞI OY

X- Temyizen incelenen Daire kararında, dava konusu Yönetmeliğin 21. maddesinin 3. fıkrasının (a) bendinin ikinci cümlesinde yer alan "Elektronik kart üzerinde bulunacak diğer bilgileri belirleme yetkisi ilgili federasyona aittir." hükmünün, 6222 sayılı Kanun'un 5. maddesinin 4. fıkrasında düzenlenmiş olan elektronik kart üzerinde bulunması gereken bilgileri aşacak şekilde ve hukuki belirlilikten uzak bir biçimde düzenlendiği gerekçesiyle iptaline karar verilmiştir.

Davalı idarelerden Gençlik ve Spor Bakanlığının dosyaya sunduğu savunmada, anılan hükmün kart üzerinde mutlak surette kanunda sayılanların dışındaki kişisel verilerin yer alacağı anlamına gelmediği, federasyonlara yönelik amblem veya sembol gibi bilgilerin elektronik karta işlenmesi amacıyla yapılan bir düzenleme olduğu ileri sürülmektedir.

Anayasa'nın 124. maddesinde, kanunların uygulanmasını sağlamak üzere ve kanunlara aykırı olmamak kaydıyla yönetmelikler çıkartılabileceği öngörülmektedir. Bahse konu Anayasal hüküm, idareye türev düzenleme ihdas etme yetkisi vermektedir. Esasında bu yetki, genel ve soyut nitelikte hükümler ihtiva eden kanunların detaylandırılması amacını taşımaktadır. Bu çerçevede, kanunda öngörülmeyen bazı hususların yine kanuna aykırı olmamak kaydıyla yönetmeliklerde düzenlenmesi mümkün olabilmektedir.

Uyuşmazlıkta, davalı idarenin savunması gözetildiğinde, dava konusu Yönetmeliğin 21. maddesinin 3. fıkrasının (a) bendinin ikinci cümlesinde yer alan ve Daire kararında iptaline hükmedilen düzenlemenin farklı spor dallarına ilişkin amblem ve sembolleri içerecek şekilde elektronik kartın tasarımında federasyonlara yetki tanımaya yönelik olduğu, bu haliyle 6222 sayılı Kanun'un 5. maddesinin 4. fıkrasında yer alan "Bilet satın almak isteyen kişilerle ilgili olarak, üzerinde adı, soyadı, Türkiye Cumhuriyeti kimlik numarası ve fotoğrafı olan bir elektronik kart oluşturulur." şeklindeki hükmün detaylandırılması ve uygulanmasını sağlama amacını taşıdığı anlaşılmakta olup, anılan düzenlemede hukuka ve üst normlara aykırı bir yön bulunmadığı sonucuna ulaşılmıştır.

Bu itibarla, Daire kararının dava konusu Yönetmeliğin 21. maddesinin 3. fıkrasının (a) bendinin ikinci cümlesinin iptaline ilişkin kısmının bozulması gerektiği oyuyla, karara katılmıyoruz.

Danıştay Kararı - İDDK., E. 2019/3003 K. 2020/2056 T. 4.11.2020

T.C. DANIŞTAY İDARİ DAVA DAİRELERİ KURULU

TEMYİZ EDEN (DAVACI): ...

VEKİLİ: Av. ...

KARŞI TARAF (DAVALI): ... Birliği (...)

VEKİLİ: Av. ...

İSTEMİN KONUSU: Danıştay Sekizinci Dairesinin 25/02/2019 tarih ve E:2015/11124, K:2019/1305 sayılı kararının temyizen incelenerek bozulması istenilmektedir.

YARGILAMA SÜRECİ:

Dava konusu istem: Serbest muhasebeci mali müşavir olan davacı tarafından, 13/12/2013 tarih ve 28850 sayılı Resmi Gazete'de yayımlanan "Haksız Rekabetle Mücadele Yazılımının Meslek Mensuplarınca Kullanılması Hakkında Mecburi Meslek Kararı" başlıklı düzenlemenin 1, 3, 5, 6, 7, 8, 9 ve 10. maddelerinin iptali istenilmiştir.

Daire kararının özeti: Danıştay Sekizinci Dairesinin 25/02/2019 tarih ve E:2015/11124, K:2019/1305 sayılı kararıyla;

Meslek mensupları arasında güveni hakim kılmak üzere meslek disiplini ve ahlakını korumak maksadı ile kanunla kurulan kamu tüzel kişilikleri olan meslek kuruluşlarının; üyelerinin menfaatlerini korumak, üyelerin mükellefleri ile olan ilişkilerinde dürüstlüğü ve güveni hakim kılmakla yükümlü olduğu,

Bu çerçevede, F1 tarafından hazırlanan Haksız Rekabetle Mücadele Yazılımının Meslek Mensuplarınca Kullanılması Hakkında Mecburi Meslek Kararının "Amaç" başlıklı 1. maddesinde, "Bu mecburi meslek kararı; yazılı hizmet sözleşmesi düzenlemeden iş kabul edilmemesi, ücret tarifesine uyulması ve bunun sonucunda ücretsiz veya tarifenin altında iş görülmesinin önüne geçilmesi, sözleşmeden dolayı ücret borcu olan müşteriye bu edimini yerine getirmeden bir başka meslek mensubu tarafından iş yapılmasının engellenmesi, stajyerlerin ve bürolarda bağımlı çalışan meslek mensuplarının işten ayrılması halinde daha önce çalıştığı büronun müşterilerine iki yıl geçmedikçe

hizmet vermeme yasağına uyup uymadıklarının izlenmesi ve bu yöndeki aykırı uygulamaları sonlandıracak önlemlerin alınması amacıyla hazırlanmıştır." ifadelerine yer verildiği,

Dava konusu kararın amacının, Anayasa ve Yasa uyarınca kendisine verilen görev kapsamında konuyla ilgili meslek kuruluşu olan F1 tarafından sözleşme düzenlenmesi zorunlu konularda sözleşmesiz iş yapılıp yapılmadığını, asgari ücret tarifesine uyulup uyulmadığını kontrol etmek, bir müşteriye birden fazla meslek mensubunun hizmet vermesinin önüne geçmek olduğu,

Öte yandan, dava konusu meslek kararının 8. maddesinin (a) bendinde meslek mensubunun, "Mevcut müşterileri ile dönem sonunda yenilediği sözleşmeleri, dönem sonundan itibaren iki ay içerisinde" hazırlanan yazılım üzerinden bağlı oldukları odaya bildirmek zorunda olduğu kuralı getirildiği; burada yer alan zorunluluğun, sözleşme serbestisi çerçevesinde müşteriler ile dönem sonunda yenilenen sözleşmeleri kapsadığı; sözü edilen kuralın, meslek mensuplarını mükelleflerle her yıl yeniden sözleşme imzalamaya zorlayan bir nitelikte olmadığı kabulü gerektiği,

Bu durumda, söz konusu yazılım ile asıl amacın; sözleşme düzenlenmesi zorunlu konularda sözleşmesiz iş yapılıp yapılmadığını, asgari ücret tarifesine uyulup uyulmadığını kontrol etmek, bir müşteriye birden fazla meslek mensubunun hizmet vermesinin önüne geçmek suretiyle haksız rekabetle mücadele etmek olduğu anlaşıldığından, dava konusu kuralın, meslek kuruluşlarına, Anayasa ve 3568 sayılı Yasa ile verilen yükümlülükleri aşan bir yönü bulunmadığı gerekçesiyle, davanın reddine karar verilmiştir.

TEMYİZ EDENİN İDDİALARI: Davacı tarafından, dava konusu kararın 6698 sayılı Kişisel Verilerin Korunması Kanunu'na aykırı olduğu; mükelleflerin mağduriyetine sebep olabilecek nitelikte olduğu; her yıl sözleşmenin yenilenmesinin Borçlar Kanunu'na aykırı olduğu, sözleşme feshedilmedikçe kendiliğinden belirsiz süreli sözleşmeye döneceği; burada amacın damga vergisi almak olduğu; davalı idarenin, bu düzenleme ile iş sahibi ile sözleşmesini fesheden meslek mensuplarının, aynı iş sahibi ile sözleşme imzalamak isteyen meslek mensubuna sistem üzerinden onay verme yükümlülüğü getirdiği fakat bunun kanuni bir dayanağı olmadığı, hem de meslek mensupları tarafından kötüye kullanılarak iş sahiplerinin mağduriyetine yol açıldığı; davalı idare tarafından yayınlanan 2016/3 sayılı Genelge ile, sistemin kötüye kullanılmaya başladığının kabul edildiği; onay sistemi ve sözleşmelerin her yıl yenilenmesinin uygulamada sorunlar yarattığı belirtilerek dava konusu kararın iptal edildiği; F1 tarafından yayımlanan bu kuralların meslek mensuplarına ve diğer tüm kişilere zarar verdiği; dava açmak zorunda kaldıkları ve açılan bu davalar sonucunda haksız yere yargılama gideri ve vekalet ücreti ödemek zorunda kaldıkları ileri sürülmektedir.

KARŞI TARAFIN SAVUNMASI: Davalı idare tarafından, Danıştay Sekizinci Dairesince verilen kararın usul ve hukuka uygun bulunduğu ve temyiz dilekçesinde öne sürülen nedenlerin, kararın bozulmasını gerektirecek nitelikte olmadığı belirtilerek temyiz isteminin reddi gerektiği savunulmaktadır.

DANIŞTAY TETKİK HÂKİMİ ...'IN DÜŞÜNCESİ: Temyiz isteminin reddi ile Daire kararının onanması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay İdari Dava Daireleri Kurulunca, Tetkik Hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereği görüldü:

HUKUKİ DEĞERLENDİRME:

Danıştay dava dairelerinin nihai kararlarının temyizen incelenerek bozulması, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 49. maddesinde yer alan;

"a) Görev ve yetki dışında bir işe bakılmış olması,

b) Hukuka aykırı karar verilmesi,

c) Usul hükümlerinin uygulanmasında kararı etkileyebilecek nitelikte hata veya eksikliklerin bulunması" sebeplerinden birinin varlığı hâlinde mümkündür.

Temyizen incelenen karar usul ve hukuka uygun olup, temyiz dilekçesinde ileri sürülen iddialar kararın bozulmasını gerektirecek nitelikte görülmemiştir.

KARAR SONUCU:

Açıklanan nedenlerle;

1. Davacının temyiz isteminin reddine,
2. Davanın yukarıda özetlenen gerekçeyle reddine ilişkin Danıştay Sekizinci Dairesinin temyize konu 25/02/2019 tarih ve E:2015/11124, K:2019/1305 sayılı kararının ONANMASINA,
3. Kesin olarak, 04/11/2020 tarihinde oybirliği ile karar verildi.

Danıştay Kararı - İDDK., E. 2019/2983 K. 2020/2462 T. 19.11.2020

İSTEMİN KONUSU: Danıştay Onüçüncü Dairesinin 30/04/2019 tarih ve E:2015/2587, K:2019/1430 sayılı kararının aleyhlerine olan kısımlarının temyizden incelenerek bozulması taraflarca karşılıklı olarak istenilmektedir.

YARGILAMA SÜRECİ:

Dava konusu istem: 28/03/2015 tarih ve 29309 sayılı Resmî Gazete'de yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına İlişkin Yönetmeliğin 22. maddesiyle Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin iptali istenilmiştir.

Daire kararının özeti: Danıştay Onüçüncü Dairesinin 30/04/2019 tarih ve E:2015/2587, K:2019/1430 sayılı kararıyla;

Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'nin "Serbest tüketici veri tabanı" başlıklı 30/B maddesinde;

"(1) Serbest tüketicilere ilişkin uzlaştırmaya esas veriş-çekiş birimlerine ait tedarikçi değiştirme süreçlerinde kullanılmak üzere TEİAŞ ve dağıtım lisansı sahibi tüzel kişiler hizmet sundukları ve sayaçlarını okumakla yükümlü oldukları serbest tüketicilerin aşağıda yer alan bilgilerini PYS üzerinde tanımlanacak veri tabanına eklemek ve güncel tutmakla yükümlüdür:

- a) Serbest tüketicinin adı veya unvanı,
- b) Tüketim noktasının PYS'ye kayıt için gerekli kayıt kodu,
- c) Tüketim noktasının içerisinde bulunduğu il ve ilçe bilgisi,
- ç) Tüketim noktasının açık adresi.

(2) Piyasa İşletmecisi ilgili veri tabanına tedarikçilerin erişimini sağlamakla yükümlüdür. Bu madde kapsamında edinilen bilgiler lisansta belirtilen faaliyetler dışında kullanılamaz ve ticarete konu edilemez.

(3) TEİAŞ ve dağıtım lisansı sahibi tüzel kişiler birinci fıkranın (b) bendinde yer alan kayıt kodunun nasıl oluşturulduğuna ilişkin açıklamayı PYS üzerinde serbest tüketici kayıt ekranında yayımlar.

(4) PYS, 30/A maddesi kapsamındaki kayıt girişleri sırasında yeni tedarikçi olmak isteyen piyasa katılımcısının sayaç kaydı için giriş yaptığı kodun birinci fıkranın (b) bendi çerçevesinde oluşturulan veri tabanında olup olmadığını kontrol eder. Veri tabanında yer alan kodlarla eşleşmeyen girişlere izin verilmez.

(5) TEİAŞ ve dağıtım lisansı sahibi tüzel kişilerin veri tabanına ilişkin yükümlülüklerini yerine getirmemesi nedeni ile serbest tüketicinin yeni tedarikçisinin portföyüne geçişinin engellendiğinin tespiti halinde PYS üzerinden gerekli düzeltme yapılır ve Kanunun 16 ncı maddesi uyarınca yaptırım uygulanır." düzenlemesine yer verildiği;

Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 1. fıkrası yönünden;

Dava konusu edilen Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'nin "Serbest tüketici veri tabanı" başlıklı 30/B maddesi uyarınca, TEİAŞ ve dağıtım lisansı sahibi tüzel kişilerin hizmet sundukları ve sayaçlarını okumakla yükümlü oldukları serbest tüketicilerin adı veya unvanını, tüketim noktasının PYS'ye kayıt için gerekli kayıt kodunu, tüketim noktasının içerisinde bulunduğu il ve ilçe bilgisini ve tüketim noktasının açık adresini PYS üzerinde tanımlanacak veri tabanına eklemeleri ve güncel tutmaları, piyasa işletmecisinin de ilgili veri tabanına tedarikçilerin erişimini sağlaması gerektiği; bu düzenlemenin serbest tüketicilere ilişkin uzlaştırmaya esas veriş-çekiş birimlerine ait tedarikçi değiştirme süreçlerinde uygulanacağı;

Dava konusu düzenlemenin serbest tüketicilerin tedarikçi seçme ve değiştirme süreçlerine yönelik olduğu, bu süreçlerde serbest tüketiciler ve yeni tedarikçiler açısından meydana gelen olumsuzlukların giderilmesinin amaçlandığı; ayrıca, tedarikçiler açısından "abone no", "sayaç no" gibi takip numaralarına standart getirilmesinin öngörüldüğü;

Belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgilerin kişisel veri olarak tanımlandığı; kişisel veriyi, adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler olarak değerlendirmek gerektiği; kişinin belirli olması, kişisel veri ile başka hiçbir işleme ya da yoruma gerek kalmaksızın kişinin kimliğinin ortaya çıkarılabiliyor olması iken, kişinin belirlenebilir olmasının veri ile kişinin ilişkilendirilmesi suretiyle kişinin tanımlanabilmesi olduğu;

Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamadığı; bilişim teknolojilerindeki gelişmeler sonucunda, geleneksel yöntemlerle ulaşılmaması mümkün olmayan çok sayıda verinin toplanabilmesi; daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması; verilere erişim ve veri transferinin kolaylaşması; kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde meydana gelen risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenlerin, günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kıldığı;

Bu bağlamda, Anayasa'nın 20. maddesinin üçüncü fıkrasının son cümlesinde, "Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilerek kişisel verilerin korunması hakkının anayasal güvenceye bağlandığı, bu verilerin kamu makamlarının keyfi müdahalelerine karşı koruma altına alındığı ve işlenmesi ancak kişinin açık rızası veya kanunda öngörülen hâllerde mümkün kılındığı;

Dava konusu Yönetmeliğin 30/B maddesinin 1. fıkrasının (a) bendi ile kişisel veri olan serbest tüketicilerin adı veya unvanının, PYS üzerinde tanımlanacak veri tabanına ekleneceği, piyasa işletmecisinin veri tabanına tedarikçilerin erişimini sağlayacağını düzenlendiği;

Anayasa'nın 20. maddesinin 3. fıkrasına aykırı olarak, dava konusu düzenlemeyle kişiyi belirlenebilir kılan kişisel veri niteliğinde olan serbest tüketicilerin adları veya unvanlarının tedarikçilerin erişimine açık olan veri tabanına eklenmesinde hukuka uygunluk bulunmadığı;

Yönetmeliğin dava konusu maddesinin birinci fıkrasında yer alan diğer kısımlarında talep edilen bilgilerin tüketim noktasına ilişkin veriler olduğu; bu verilerin, kişinin ad ve unvanı olmaksızın kişinin belirlenebilmesine yeterli olabilecek veriler olmadığı; dolayısıyla, kişisel veri olarak kabul edilemeyecek veriler olduğu, tüketiciler değişebilecekken tüketim noktalarına ilişkin verilerin sabit olduğu da dikkate alındığında, Yönetmeliğin 30/B maddesinin 1. fıkrasının diğer kısımlarında hukuka aykırılık bulunmadığı;

Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 2. fıkrasının yönünden;

28/05/2016 tarih ve 29725 Sayılı Resmî Gazete'de Yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmeliğin 6. maddesi ile dava konusu "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 2. fıkrasında yer alan "Piyasa İşletmecisi ilgili veri tabanına tedarikçilerin erişimini sağlamakla yükümlüdür. Bu madde kapsamında edinilen bilgiler lisansta belirtilen faaliyetler dışında kullanılamaz ve ticarete konu edilemez." düzenlemesinin; "Tedarikçiler, tedarikçi değiştirme ve mali uzlaştırma süreçlerinde kullanılmak üzere tüketicilerine ilişkin, a) Serbest tüketicinin adı veya unvanı, b) Gerçek kişiler için T.C. kimlik numarası, tüzel kişiler için vergi kimlik numarası, bilgilerini PYS üzerinde tanımlanacak veri tabanına eklemek ve güncel tutmakla yükümlüdür. Piyasa İşletmecisi bu bilgileri veri tutarlılığının kontrolü amacı ile kullanır ve kişisel verilerin korunmasını sağlayacak önlemleri alır. Tedarikçilerin söz konusu yükümlülüklerini yerine getirmediklerinin tespiti halinde Kanununun 16 ncı maddesi uyarınca yaptırım uygulanır." şeklinde değiştirildiği ve davanın konusuz kaldığı anlaşıldığından, Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 2. fıkrası açısından uyumsuzluğun esası hakkında karar verilmesine gerek bulunmadığı;

Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 3., 4. ve 5. fıkraları yönünden;

Dava konusu edilen Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'nin "Serbest tüketici veri tabanı" başlıklı 30/B maddesinin 3. ve 4. fıkralarında Piyasa Yönetim Sisteminin (PYS) öngörülen şekilde çalışmasının sağlanmasına ilişkin birtakım düzenlemelere yer verildiği, bu düzenlemelerin, PYS'nin kullanımına ilişkin olduğu;

Yönetmeliğin 30/B maddesinin 5. fıkrasında ise, veri tabanına ilişkin yükümlülüklerin yerine getirilmemesi nedeniyle serbest tüketicinin yeni tedarikçisinin portföyüne geçişinin engellendiğinin tespiti hâlinde gerekli düzeltmelerin yapılacağı ve 6446 sayılı Kanun'a göre yaptırım uygulanacağını öngörüldüğü, Yönetmelik'te düzenlenen yükümlülüklerin yerine getirilmemesi hâlinde uygulanacak yaptırımlara ilişkin, Kanun hükmüne atıf yapıldığı; bu itibarla, Yönetmeliğin 30/B maddesinin 3., 4. ve 5. fıkrasında hukuka aykırılık bulunmadığı gerekçesiyle;

Dava konusu 28/03/2015 tarih ve 29309 sayılı Resmî Gazete'de yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına İlişkin Yönetmeliğin 22. maddesiyle, Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin birinci fıkrasının (a) bendinin iptaline, ikinci fıkrasının iptali istemi hakkında karar verilmesine yer olmadığına; maddenin diğer kısımları yönünden ise davanın reddine karar verilmiştir.

TEMYİZ EDENLERİN İDDİALARI:

Davacı tarafından, dava konusu Yönetmeliğin 30/B maddesinin 1. fıkrasının (ç) bendinin Anayasa'nın 20. maddesinin 3. fıkrasına aykırı olduğu ileri sürülmektedir.

Davalı idare tarafından, iptal edilen düzenlemenin karar tarihinden önce yürürlükten kaldırılmış olması nedeniyle karar verilmesine yer olmadığına karar verilmesi gerektiği ileri sürülmektedir.

KARŞI TARAFIN SAVUNMALARI:

Davacı tarafından, Danıştay Onüçüncü Dairesince verilen kararın iptale ilişkin kısmının usul ve hukuka uygun bulunduğu ve temyiz dilekçesinde öne sürülen nedenlerin, kararın bu kısmının bozulmasını gerektirecek nitelikte olmadığı belirtilerek temyiz isteminin reddi gerektiği savunulmaktadır.

Davalı idare tarafından, savunma verilmemiştir.

DANIŞTAY TETKİK HÂKİMİ K1'NUN DÜŞÜNCESİ: Temyiz istemlerinin reddi ile Daire kararının onanması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay İdari Dava Daireleri Kurulunca, Tetkik Hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereği görüldü:

HUKUKİ DEĞERLENDİRME:

Danıştay dava dairelerinin nihai kararlarının temyizen incelenerek bozulması, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 49. maddesinde yer alan;

- "a) Görev ve yetki dışında bir işe bakılmış olması,
- b) Hukuka aykırı karar verilmesi,
- c) Usul hükümlerinin uygulanmasında kararı etkileyebilecek nitelikte hata veya eksikliklerin bulunması" sebeplerinden birinin varlığı hâlinde mümkündür.

Temyizen incelenen karar usul ve hukuka uygun olup, temyiz dilekçelerinde ileri sürülen iddialar kararın bozulmasını gerektirecek nitelikte görülmemiştir.

KARAR SONUCU:

Açıklanan nedenlerle;

1. Tarafların temyiz istemlerinin reddine,

2. Yukarıda özetlenen gerekçeyle dava konusu düzenlemenin kısmen iptali, kısmen dava hakkında karar verilmesine yer olmadığı, kısmen davanın reddi yolundaki Danıştay Onüçüncü Dairesinin temyize konu 30/04/2019 tarih ve E:2015/2587, K:2019/1430 sayılı kararının temyize konu iptale ve davanın reddine yönelik kısımlarının ONANMASINA,

3. Kesin olarak, 19/11/2020 tarihinde oyçokluğu ile karar verildi.

KARŞIOY

X-Dava konusu Yönetmelik'in iptal edilen 30/B maddesinin birinci fıkrasının (a) bendi, 28/05/2016 tarih ve 29725 sayılı Resmî Gazete'de yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmeliğin 6. maddesi ile yürürlükten kaldırılmıştır.

Dava konusu edilen düzenlemenin yürürlükten kaldırılmış olması ve eski düzenlemeye dayalı olarak tesis edilmiş bir uygulama işleminin dava konusu edilmemiş olması karşısında davanın konusu kalmamıştır.

Açıklanan nedenle, temyize konu kısma ilişkin olarak Danıştay Onüçüncü Dairesince konusu kalmayan dava hakkında karar verilmesine yer olmadığına karar verilmesi gerektiği oyuyla, karara katılmıyoruz.

KARŞIOY

XX-Dava, 28/03/2015 tarih ve 29309 sayılı Resmî Gazete'de yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına İlişkin Yönetmeliğin 22. maddesiyle Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin iptali istemiyle açılmıştır.

Temyize konu kararda, Anayasa'nın 20. maddesinin 3. fıkrasına aykırı olarak, dava konusu düzenlemeyle kişiyi belirlenebilir kılan kişisel veri niteliğinde olan serbest tüketicilerin adları veya unvanlarının tedarikçilerin erişimine açık olan veri tabanına eklenmesinde hukuka uygunluk bulunmadığı gerekçesiyle, uyuşmazlık konusu 30/B maddesinin birinci fıkrasının (a) bendinin iptaline karar verilmiştir.

07/04/2016 tarih ve 29677 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanun ile kişisel verilerin işlenmesinde uyulacak usul ve esaslar düzenlenmiş olduğundan, dava devam ederken yürürlüğe giren bu yasal düzenleme dikkate alınarak

uyuşmazlıđın çözüme kavuşturulması gerektiđi oyuyla, Daire kararının temyize konu edilen iptale ilişkin kısmının onanmasına dair karara katılmıyorum.

Danıştay Kararı - İDDK.(E. 2019/2549)

Danıştay Kararı - İDDK., E. 2019/2549 K. 2020/716 T. 12.3.2020

KARAR DÜZELTME

İSTEMİNDE BULUNAN (DAVACI): K1

VEKİLİ: Av. K2

KARŞI TARAF (DAVALI): Hazine ve Maliye Bakanlığı

VEKİLİ: Haz. Av. K3

İSTEMİN KONUSU: Danıştay İdari Dava Daireleri Kurulunca verilen; Ankara 15. İdare Mahkemesinin 29/12/2016 tarih ve E:2016/5377, K:2016/5987 sayılı ısrar kararının onanmasına ilişkin 20/02/2019 tarih ve E:2017/686, K:2019/687 sayılı karara karşı, davacı karar düzeltme isteminde bulunmaktadır.

YARGILAMA SÜRECİ:

Dava konusu istem: Vergi müfettiş yardımcılığı yazılı ve sözlü sınavını başarı ile tamamlayan davacı tarafından, Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği'nin 15. maddesi uyarınca atamasının yapılmamasına ilişkin 15/04/2014 tarih ve 8744 sayılı işlemin iptali istenilmiştir.

İlk Derece Mahkemesi kararının özeti: Ankara 15. İdare Mahkemesinin 21/11/2014 tarih ve E:2014/814, K:2014/1576 sayılı kararıyla;

Davacının Pozantı Asliye Ceza Mahkemesinin 10/02/2011 tarih ve E:2009/55, K:2011/20 sayılı kararıyla, "Devletin Egemenlik Alametlerini Alenen Aşağılama" suçundan cezalandırıldığı, takdiri indirim nedenleri gözetilerek cezasının 10 aya indirildiği, yeniden suç işlemeyeceği kanaatine varılarak hükmün açıklanmasının geriye bırakılmasına karar verildiği, daha sonra davacı hakkında basit yaralama suçu nedeniyle iddianame düzenlendiği, Pozantı Asliye Ceza Mahkemesinin E:2013/108 sayılı dosyası üzerinden yargılamanın devam ettiği gerekçesi ile atamasının yapılmadığı, Türk Ceza Kanunu'nun 300/1. maddesinde düzenlenen "Devletin Egemenlik Alametlerini Alenen Aşağılama" suçunun niteliğine bakıldığında işlenen suçun, davacının gizlilik dereceli bir birimde ve unvanda çalışmasına engel nitelik ve ağırlıkta bulunduğu ve kamusal nitelikte bir suç olduğu sonucuna varıldığı, bu nedenle davacının Güvenlik Soruşturması ve Arşiv Araştırması

Yönetmeliği'nin 15. maddesi uyarınca vergi müfettiş yardımcılığına atamasının yapılmamasına ilişkin dava konusu işlemde hukuka ve mevzuat hükümlerine aykırılık bulunmadığı gerekçesiyle davanın reddine karar verilmiştir.

Daire kararının özeti: Danıştay Onaltıncı Dairesinin 21/06/2016 tarih ve E:2015/27351, K:2016/5444 sayılı kararıyla;

Güvenlik soruşturması ve arşiv araştırmasının, hakkında soruşturma yapılan kişinin mevzuatta belirtildiği gibi "yasadışı siyasi, yıkıcı, bölücü ideolojik görüş, eylem içinde" olup olmadığını tespit etmek amacıyla yapıldığı,

Olayda her ne kadar İdare Mahkemesince işlenen suçun niteliği ve ağırlığı gözetilerek bir değerlendirme yapılmış ise de; davacının "Devletin Egemenlik Alametlerini Alenen Aşağılama" suçundan yargılandığı davada, Pozantı Asliye Ceza Mahkemesinin 10/02/2011 tarih ve E:2009/55, K:2011/20 sayılı kararıyla 1 yıl hapis cezasıyla cezalandırıldığı, takdiri indirim nedenleri gözetilerek cezasının 10 aya indirildiği ve yeniden suç işlemeyeceği kanaatine varıldığından hükmün açıklanması geri bırakılarak 5 yıl denetim süresine tabi tutulduğu, denetim süresi sonunda ise Pozantı Asliye Ceza Mahkemesinin 06/04/2016 tarihinde aldığı ek karar ile;"sanığın denetiminin başladığı 10/03/2011 tarihinden itibaren 5 yıl içinde kasıtlı bir suç işlemediği, hakkında derdest bir soruşturmanın da bulunmadığı belirtilerek açıklanması geri bırakılan hükmün ortadan kaldırılmasına ve 5271 sayılı Ceza Muhakemesi Kanununun 231/10 maddesi uyarınca sanık hakkındaki kamu davasının düşürülmesine" karar verildiği;

Öte yandan davacı hakkında basit yaralama suçundan açılan ceza davasının da Pozantı Asliye Ceza Mahkemesinin 22/04/2014 tarih ve E:2013/108, K:2014/109 sayılı kararı ile şikayetten vazgeçilmesi nedeniyle düşürüldüğü tespiti yapılarak, 09/04/2014 tarih ve K:2013/08 sayılı Değerlendirme Komisyonu kararının dayanağını oluşturan her iki ceza yargılaması neticesinde de davacı hakkında herhangi bir mahkumiyet hükmü kurulmadığı;

Bu durumda; memuriyete alınmasına engel bir mahkumiyet hükmünün bulunduğu söz etme olanağı kalmayan, güvenlik ve arşiv araştırması sonucu elde edilen bilgilerin "olumlu" olarak değerlendirilmesine engel nitelikte bir durumunun da bulunmadığı anlaşılan davacının, Vergi Müfettiş Yardımcılığı kadrosuna atamasının yapılmamasına ilişkin dava konusu işlemde hukuka uyarlık, aksi yöndeki İdare Mahkemesi kararında ise hukuki isabet görülmediği gerekçesiyle Ankara 15. İdare Mahkemesinin 21/11/2014 tarih ve E:2014/814, K:2014/1576 sayılı kararının bozulmasına karar verilmiştir.

İlk Derece Mahkemesi ısrar kararının özeti: Ankara 15. İdare Mahkemesinin 29/12/2016 tarih ve E:2016/5377, K:2016/5987 sayılı kararıyla; davanın reddi yolundaki ilk kararda ısrar edilmiştir.

Danıştay İdari Dava Daireleri Kurulu kararının özeti: Davacının temyiz başvurusu üzerine, Danıştay İdari Dava Daireleri Kurulunun 20/02/2019 tarih ve E:2017/686, K:2019/687 sayılı kararıyla temyize konu ısrar kararı hukuk ve usule uygun bulunmuş ve kararın onanmasına karar verilmiştir.

KARAR DÜZELTME TALEP EDENİN İDDİALARI: Davacı tarafından, Ceza Muhakemesi Kanunu'nun 231/5. maddesinde; hükmün açıklanmasının geri bırakılmasının, kurulan hükmün sanık hakkında hukuki sonuç doğurmamasını ifade edeceğinin düzenlendiği, ayrıca denetim süresi içerisinde bir suç işlememesi sebebi ile hakkında açılan kamu davasının da düşürüldüğü, sonuç olarak hakkında memuriyete engel bir mahkumiyet hükmü bulunmadığı ve Mahkemece verilen kararın hukuka aykırı olduğu ileri sürülmektedir.

KARŞI TARAFIN SAVUNMASI: Davalı idare tarafından, düzeltilmesi istenen kararın usul ve yasaya uygun olduğu, ileri sürülen nedenlerin 2577 sayılı İdari Yargılama Usulü Kanunu'nun 54. maddesine uymadığı, bu nedenle istemin reddi gerektiği savunulmaktadır.

DANIŞTAY TETKİK HAKİMİ K4'NUNDÜŞÜNCESİ: İstemin kabulü gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay İdari Dava Daireleri Kurulunca, davacının karar düzeltme dilekçesinde öne sürdüğü hususlar, 2577 sayılı İdari Yargılama Usulü Kanunu'nun Geçici 8. maddesi uyarınca uygulanmasına devam edilen 3622 sayılı Kanun ile değişik 54. maddesi hükmüne uygun bulunduğundan, karar düzeltme isteminin kabulü ile Danıştay İdari Dava Daireleri Kurulunun 20/02/2019 tarih ve E:2017/686, K:2019/687 sayılı kararı kaldırılarak, Ankara 15. İdare Mahkemesinin 29/12/2016 tarih ve E:2016/5377, K:2016/5987 sayılı ısrar kararına yönelik davacının temyiz istemi yeniden incelendi, gereği görüldü:

İNCELEME VE GEREKÇE:

MADDİ OLAY:

12-21 Ağustos 2013 tarihleri arasında başvurusu yapılan vergi müfettiş yardımcılığı sınavının yazılı ve sözlü bölümlerini başarı ile tamamlayan davacı hakkında, "Devletin Egemenlik Alametlerini Alenen Aşağılama" suçunu işlediği isnadıyla açılan kamu davasında, Pozantı Asliye Ceza Mahkemesinin E:2009/55, K:2011/20 sayılı kararıyla; Türk Ceza Kanunu'nun 300/1. maddesi uyarınca eylemi sabit görülerek takdiren 1 yıl hapis cezasıyla cezalandırılmasına, takdiri indirim nedenleri

gözetilerek cezasının 10 aya indirilmesine ve hükmün açıklanmasının geri bırakılmasına karar verildiği tespit edilmiş ve bu nedenle davacının "Güvenlik soruşturması sonucu olumlu olmak" şartını taşımadığı gerekçesiyle ataması yapılmamıştır.

Bunun üzerine, anılan işlemin iptali istemiyle temyizden bakılan dava açılmıştır.

İLGİLİ MEVZUAT:

24/03/2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Özel Nitelikli Kişisel Verilerin İşlenme Şartları" kenar başlıklı 6. maddesinde; (1)Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, ... ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. (2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır. (3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir..."; "İstisnalar" kenar başlıklı 28. maddesinin birinci fıkrasında, " Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz: ... ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi. d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi..." kurallarına yer verilmiştir.

5352 sayılı Adli Sicil Kanunu'nun 6. maddesinde, "Kamu davasının açılmasının ertelenmesine ve hükmün açıklanmasının geri bırakılmasına ilişkin kararlar, ancak bir soruşturma veya kovuşturmayla bağlantılı olarak mahkeme, hâkim, askerî hâkim, Cumhuriyet Başsavcılığı veya askerî savcılık tarafından istenmesi halinde verilmek üzere kaydedilir." hükmü yer almaktadır.

657 sayılı Devlet Memurları Kanunu'nun 48. maddesinde, Devlet memurluğuna alınacaklarda aranılan genel ve özel şartlar belirtilerek, özel şartlar arasında kurumların özel kanun ve diğer mevzuatında aranan şartları taşımak gerektiği hüküm altına alınmıştır.

Maliye Bakanlığı Personeli Hakkında Yapılacak Güvenlik Soruşturması ve Arşiv Araştırması Yönergesi'nin "Kapsam" başlıklı 2.maddesinde,"Bu yönerge; Maliye Bakanlığı merkez ve taşra teşkilatında görevli bulunan personel ile ilk defa, yeniden veya kurumlararası naklen atanacaklardan gizlilik dereceli birim, kısım ve görevlerde çalıştırılması düşünülenler ile, yurtdışı teşkilatında sürekli görevlendirilecek bütün personelin güvenlik soruşturması ve arşiv araştırmasına ilişkin usul ve esasları kapsar."; "Gizlilik Dereceli Birim, Kısım ve Görevler" başlıklı 6. maddesinde,"a) Merkez teşkilatında; 1- Müsteşarlık ve Müsteşar Yardımcılığı makamlarının özel büroları, ana hizmet

birimlerinin denetim birimi başkanlıkları, özel büroları ile personel şubesi müdürlükleri, danışma ve denetim birimlerinin ve yardımcı birimlerin özel büroları ile personel şubesi müdürlükleri, 2- Teftiş Kurulu Başkanlığı, Hesap Uzmanları Kurulu Başkanlığı, Mali Suçları Araştırma Kurulu Başkanlığı, Personel Genel Müdürlüğü, Savunma Sekreterliği ve Özel Kalem Müdürlüğü, b) Taşra teşkilatında; Defterdarlık, Gelirler Bölge Müdürlüğü ve İşletme Bölge Müdürlüğü bünyesindeki denetmenler büroları, özel bürolar ile personel birimleri, c) Yurtdışı teşkilatında; Maliye Müşavirlikleri ile Maliye Ataşelikleri. B- Gizlilik dereceli görevleri yürüten personel: a) Unvanına bakılmaksızın yukarıda (A) bendinde sayılan yerlerde görevlendirilen personel, b) Görevli olduğu yer dikkate alınmaksızın, Bakanlık merkez ve taşra teşkilatında çalışan müdür ve daha üst düzeydeki personel, koruma ve güvenlik görevlileri ile kozmik evrak personeli, c) Kontrolörler ve Stajyer kontrolörler, d) Hazine avukatları, e) Özel Yönetmeliği bulunan merkez teşkilatı uzmanları ile denetmenler ve bunların yardımcıları. f) Birim amirince (Merkez ve döner sermaye teşkilatında Genel Müdür, Başkan veya Müstakil Daire Başkanı, taşra teşkilatında Defterdar veya Bölge Müdürü) hakkında Güvenlik Soruşturması ve Arşiv Araştırması yaptırılması uygun görülen personel" kurallarına yer verilmiştir.

4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ve Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun'un 1. maddesinin dava konusu işlem tarihi itibarıyla yürürlükte bulunan halinde; "Güvenlik Soruşturması ve Arşiv Araştırması; ... askeri, emniyet ve istihbarat teşkilatlarında çalıştırılacak kamu personeli ve ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında yapılır. Devletin güvenliğini, ulusun varlığını ve bütünlüğünü iç ve dış menfaatlerinin zarar görebileceği ve tehlikeye düşebileceği bilgi ve belgeler ile gizlilik dereceli kamu personeli ile meslek gruplarının tespiti birim ve kısımlarının tanımlarının yapılması güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak merciler ve üst kademe yöneticilerinin kimler olduğu Bakanlar Kurulu kararı ile yürürlüğe konulacak yönetmelik ile düzenlenir." hükmü bulunmaktadır.

12/04/2000 tarih ve 24018 sayılı Resmî Gazete'de yayımlanan Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği'nin (Yönetmelik) "Kapsam" kenar başlıklı 2. maddesinde, "Bu Yönetmelik; yetkili olmayan kişilerin bilgi sahibi olmaları halinde Devletin güvenliğinin, iç ve dış menfaatlerinin, ulusal varlığın ve bütünlüğün zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeleri, bunların toplanmasını ve işlemini yürüten bakanlıklar ile kamu kurum ve kuruluşlarının ilgili birim ve kısımlarının belirlenmesini, Türk Silahlı Kuvvetlerinde, emniyet ve istihbarat teşkilatlarında, ceza infaz kurumları ve tutukevlerinde çalışacak personeli, ayrıca bakanlıklar ile kamu kurum ve

kuruluşlarının yurtdışı teşkilatlarında sürekli görevlendirilecek bütün personel için yapılacak güvenlik soruşturması ve arşiv araştırmasının esas ve usullerini, bunu yapacak mercileri, hakkında güvenlik soruşturması ve arşiv araştırması yapılacak gizlilik dereceli yerlerde çalışan kamu personeli ile meslek grupları ve üst kademe yöneticilerini kapsar.";"Güvenlik Soruşturması ve Arşiv Araştırması Yapacak Makamlar" kenar başlıklı 7. maddesinde, "Güvenlik soruşturması ve arşiv araştırması, Milli İstihbarat Teşkilatı Müsteşarlığı, Emniyet Genel Müdürlüğü ve mahalli mülki idare amirlikleri tarafından yapılır. İçişleri Bakanlığı Kaçakçılık İstihbarat Harekat ve Bilgi Toplama Dairesi Başkanlığı'ndaki bilgi kayıtları ile Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü'ndeki adli sicil kaydı, talepleri üzerine, güvenlik soruşturması ve arşiv araştırmasını yapacak makamlar ile Türk Silahlı Kuvvetlerinin ilgili birimlerine verilir.";"Hakkında Güvenlik Soruşturması ve Arşiv Araştırması Yapılacak Personel" kenar başlıklı 8. maddesinde,"Güvenlik soruşturması ve arşiv araştırması; gizlilik dereceli birim ve kısımlar ile askeri, emniyet, istihbarat teşkilatlarında ve ceza infaz kurumları ve tutukevlerinde çalıştırılacak personel hakkında yapılır. Emniyet Genel Müdürlüğü ve mahalli mülki idare amirlikleri, güvenlik soruşturması ve arşiv araştırmasını; bakanlıklar, kamu kurum ve kuruluşlarının gizlilik dereceli birim ve kısımları ile yurtdışı teşkilatında ve askeri, emniyet, istihbarat teşkilatlarında ve ceza infaz kurumu ve tutukevlerinde çalıştırılacak personel hakkında yapar."

kurallarına yer verilmiştir.

Aynı Yönetmeliğin 'Güvenlik Soruşturması ve Arşiv Araştırmasında Araştırılacak Hususlar' başlıklı 11. maddesinde,

"Güvenlik soruşturması ve arşiv araştırmasında kişinin içinde bulunduğu ortam da dikkate alınarak;

- a) Kimlik kontrolü, kimlik kayıtlarının doğruluk derecesi, uyrukluđu, geçmişte yabancı bir devletin uyrukluđuna girip girmediđi,
- b) Kolluk kuvvetleri tarafından halen aranıp aranmadıđı, kolluk kuvvetlerinin ve istihbarat ünitelerinin arşivlerinde bilgiler bulunup bulunmadıđı, adli sicil kaydının ve hakkında bir tahdidin olup olmadıđı,
- c) Yıkıcı faaliyetlerde bulunup bulunmadıđı ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanuna ve Atatürk ilke ve inkılaplarına aykırı davranıp davranmadıđı,
- d) Şeref ve haysiyetini ihlal edecek ve görevine yansıyacak şekilde kumara, uyuşturucuya, içkiye, paraya ve aşırı bir şekilde menfaatine düşkün olup olmadıđı, ahlak ve adaba aykırı davranıp davranmadıđı,

e) Yabancılarla, özellikle hasım ve hasım olması muhtemel Devlet mensupları ve temsilcileriyle ilgi derecesinin iç yüzü ve nedeni,

f) Sır saklama yeteneğinin olup olmadığı,

araştırılır.";

'Güvenlik Soruşturması ve Arşiv Araştırmasında İzlenecek Yöntem' başlıklı 12. maddesinde de,

" ...

c) Güvenlik soruşturması ve arşiv araştırması yapılması isteminin ilgili makama ulaşmasından itibaren arşiv araştırması sonuçları en geç 30 gün, güvenlik soruşturması sonuçları en geç 60 gün içinde cevaplandırılır. Soruşturma ve araştırma sonucunu içeren bilgi ve belgeler ilgilinin güvenlik makamlarındaki dosyasında asgari 'gizli' gizlilik derecesinde saklanır.

d) Güvenlik soruşturması ve arşiv araştırmasını isteyen makama, kişi hakkında karar vermeye yeterli bilgiler aktarılır.

e) Güvenlik soruşturması ve arşiv araştırmasının nasıl ve ne şekilde yapılacağı, soruşturma ve araştırma yapmaya yetkili makamların görev talimatları ile belirlenir.

f) Mahalli mülki idare amirliklerince yapılmış olan güvenlik soruşturması ve arşiv araştırmasında olumsuz durumu saptananların evrakının bir örneği dosya açılmak üzere Emniyet Genel Müdürlüğüne gönderilir.

g) Güvenlik soruşturması ve arşiv araştırmasında olumsuz durumu saptananlarla ilgili bilgiler Milli İstihbarat Teşkilatı Müsteşarlığı ve Emniyet Genel Müdürlüğüne karşılıklı olarak birbirlerine aktarılır.

.

.. " kuralları yer almıştır.

HUKUKİ DEĞERLENDİRME

Somut olayda davacının işlediği iddia edilen fiillere istinaden yapılan yargılama neticesinde verilen hükmün açıklanmasının geri bırakılmasına ilişkin kararların kayıtlarının Adana Valiliği İl Emniyet Müdürlüğü tarafından davalı idareye verildiği ve bu kayıtlar dikkate alınmak suretiyle davacının güvenlik soruşturmasının olumsuz sonuçlandırıldığı anlaşılmaktadır.

Belirli kamu görevlerinde çalıştırılacak personel hakkında uygulanan güvenlik soruşturması ve arşiv araştırmasının kanuni dayanağı 4045 sayılı Kanun'dur. 4045 sayılı Kanun'un dava konusu işlem tarihi

itibarıyla yürürlükte bulunan halinde, güvenlik soruşturması ve arşiv araştırmasının; kamu kurum ve kuruluşlarında yetkili olmayan kişilerin bilgi sahibi olmaları hâlinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile askerî teşkilatlarda, emniyet ve istihbarat teşkilatlarında çalıştırılacak kamu personeli, ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında yapılacağı düzenlenmiştir.

Kamu görevlilerinin sadakat, tarafsızlık ve devlete bağlılık yükümlülüğü çerçevesinde devleti temsil eden ve millî güvenlik bakımından hassasiyet içeren bazı kamu görevlerine atanacak kişiler bakımından daha sıkı nitelikler aranması ve birtakım sınırlamaların getirilmesi doğaldır. Bu şekilde aranan nitelikler ve kanunlarda öngörülen kısıtlamalar, kamu hizmetinin etkin ve sağlıklı bir biçimde yürütülmesi amacına yöneliktir.

Dolayısıyla idarenin millî güvenlik açısından önem arz eden kadrolara atanacak kişilerin tabi olacağı güvenlik soruşturması ve arşiv araştırması konusunda kanunla temel çerçeveyi ortaya koyan kurallar getirmesi mümkündür.

Ancak, bu alanda yapılan düzenlemelerin diğer kanuni düzenlemelerle çelişmemesi ve diğer düzenlemelerde gözetilen amaçları ortadan kaldırır nitelikte de olmaması gerekmektedir.

Bu bağlamda, yukarıda metnine yer verilen 4045 sayılı Kanun'un 1. maddesinin işlem tarihindeki hali incelendiğinde; maddede, kişilerin geçmiş ceza mahkûmiyetlerine ilişkin kayıtlar bakımından hangi suçların kamu görevine girmeye engel olacağı konusunda hiçbir belirleme yapılmadığı, suçlar arasında herhangi bir ayırım ve derecelendirme öngörülmediği, aynı şekilde hükmün açıklanmasının geri bırakılmasına konu kararların güvenlik soruşturması veya arşiv araştırmasının olumsuz sonuçlandırılmasının bir sebebi olup olmayacağı hususunda herhangi bir düzenlemeye yer verilmediği anlaşılmaktadır.

Nitekim, Anayasa Mahkemesinin 29/05/2019 tarih ve 2014/15365 başvuru numaralı "K5" kararında, özetle; işleme dayanak olan 4045 sayılı Kanun hükümlerinin temel hakkın kısıtlanması bakımından yeterli güvenceye sahip olmaması ve kanunilik ilkesine aykırı bulunması sebebiyle ve ayrıca 5352 sayılı Kanun'un 6. maddesinde kamu davasının açılmasının ertelenmesine ve hükmün açıklanmasının geri bırakılmasına ilişkin kararların ancak bir soruşturma veya kovuşturmayla bağlantılı olarak mahkeme, hâkim, askerî hâkim, Cumhuriyet başsavcılığı veya askerî savcılık tarafından istenmesi hâlinde verileceği düzenlenmesine rağmen bu hükme aykırı şekilde yapılan güvenlik soruşturması ve arşiv araştırmasının özel hayata saygı hakkını ihlal ettiği belirtilmiştir.

Yine anılan kararda Anayasa Mahkemesi, İdare Mahkemesince davanın kesin hükme bağlanmasının ertelenmesine ilişkin karara dayanılarak hakkında herhangi bir mahkûmiyet kararı bulunmayan başvuruçunun ceza yargılamasına konu eylemleri işlediğinin sabit olduğu varsayımına dayanılarak karar verildiğinin anlaşıldığından bahisle başvuruçunun Anayasa'nın 36. ve 38. maddelerinde güvence altına alınan masumiyet karinesinin de ihlal edildiği sonucuna ulaşmıştır.

Bu durumda, 5352 sayılı Kanun'un 6. maddesine aykırı şekilde elde edilen bilgi ve belgelere dayalı olarak yapılan arşiv araştırması üzerine tesis edilen dava konusu işlemde hukuka uyarlık, İdare Mahkemesinin davanın reddine yönelik ısrar kararında ise hukuki isabet bulunmamaktadır.

KARAR SONUCU:

Açıklanan nedenlerle;

- 1.Davacının temyiz isteminin kabulüne;
- 2.Davanın yukarıda özetlenen gerekçeyle reddine ilişkin Ankara 15. İdare Mahkemesinin 29/12/2016 tarih ve E:2016/5377, K:2016/5987 sayılı ısrar kararının BOZULMASINA,
3. Yeniden bir karar verilmek üzere dosyanın anılan İdare Mahkemesine gönderilmesine,
- 4.12/03/2020 tarihinde oybirliği ile karar verildi.

Danıştay Kararı - İDDK. (E. 2019/2425)

Danıştay Kararı - İDDK., E. 2019/2425 K. 2020/715 T. 12.3.2020

İSTEMİN KONUSU: Danıştay İdari Dava Daireleri Kurulunca verilen; Ankara 4. İdare Mahkemesinin 18/10/2017 tarih ve E:2017/2115, K:2017/3031 sayılı ısrar kararının onanmasına ilişkin 18/02/2019 tarih ve E:2017/3749, K:2019/617sayılı karara karşı, davacı karar düzeltme isteminde bulunmaktadır.

YARGILAMA SÜRECİ:

Dava konusu istem: Gelir uzman yardımcısı olarak görev yapan ve vergi müfettiş yardımcılığı yazılı ve sözlü sınavında başarılı olan davacının, Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği'nin 15. maddesi uyarınca atamasının uygun görülmediğine dair 09/04/2014 tarih ve 2014/23 sayılı Maliye Bakanlığı Değerlendirme Komisyonu Başkanlığı işlemine dayalı olarak atamasının yapılmamasına ilişkin 27/06/2014 tarih ve 11895534/110/1-7 sayılı davalı idare işleminin iptali istenilmiştir.

İlk Derece Mahkemesi kararının özeti: Ankara 4. İdare Mahkemesinin 14/05/2015 tarih ve E:2014/1541, K:2015/738 sayılı kararıyla; davacı hakkında yapılan yargılama sonucu suçlu bulunarak cezaya hükmedildiği, kamu haklarının kullanımından yoksun bırakıldığı, hükmün açıklanmasının geri bırakılarak, beş yıl süreyle denetimli serbestlik kararının verildiği dikkate alındığında, davacının davalı idare bünyesindeki gizlilik dereceli bir birimde çalışacak olması nedeniyle hakkında bir tahdit olduğunun kabulüyle tesis edilen dava konusu işlemde hukuka aykırılık bulunmadığı gerekçesiyle davanın reddine karar verilmiştir.

Daire kararının özeti: Danıştay İkinci Dairesinin 13/02/2017 tarih ve E:2016/4384, K:2017/928 sayılı kararıyla; davacı hakkında açılan dava sonucunda, şantaj suçu ile ilgili olarak hükmün açıklanmasının geri bırakılması kararı verildiğinden, ilgili mevzuat hükümleri uyarınca söz konusu hükmün davacı hakkında bir hukuki sonuç doğurmadığı açık olup; Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği'nin 15. maddesi uyarınca davacının vergi müfettiş yardımcısı olarak atanmamasına ilişkin dava konusu işlemde hukuka uyarlık bulunmamakta olup, bu nedenle davanın reddi yolundaki Mahkeme kararında hukuki isabet görülmediği gerekçesiyle Ankara 4. İdare Mahkemesinin 14/05/2015 tarih ve E:2014/1541, K:2015/738 sayılı kararının bozulmasına karar verilmiştir.

İlk Derece Mahkemesi ısrar kararının özeti: Ankara 4. İdare Mahkemesinin 18/10/2017 tarih ve E:2017/2115, K:2017/3031 sayılı kararıyla; davanın reddi yolundaki ilk kararda ısrar edilmiştir.

Danıştay İdari Dava Daireleri Kurulu kararının özeti: Davacının temyiz başvurusu üzerine Danıştay İdari Dava Daireleri Kurulunun 18/02/2019 tarih ve E:2017/3749, K:2019/617 sayılı kararıyla; temyize konu ısrar kararı hukuk ve usule uygun bulunmuş ve kararın onanmasına karar verilmiştir.

KARAR DÜZELTME TALEP EDENİN İDDİALARI: Davacı tarafından, hakkında açılan kamu davası sonucu verilen hükmün açıklanmasının geri bırakılmasının, anılan hükmün hukuki sonuç doğurmamasını ifade ettiği, dolayısıyla arşiv araştırmasının olumlu olduğu, ayrıca vergi müfettiş yardımcısı olarak görev yapacağı birimin gizlilik dereceli birimler arasında sayılmadığı ileri sürülmektedir.

KARŞI TARAFIN SAVUNMASI: Davalı idare tarafından, düzeltilmesi istenen kararın usul ve yasaya uygun olduğu, ileri sürülen nedenlerin 2577 sayılı İdari Yargılama Usulü Kanunu'nun 54. maddesine uymadığı, bu nedenle istemin reddi gerektiği savunulmaktadır.

DANIŞTAY TETKİK HAKİMİ K1'İN DÜŞÜNCESİ: Olayda, davacının güvenlik soruşturmasının olumsuz sonuçlandığından bahisle idarece vergi müfettiş yardımcılığına ataması yapılmamış ise de, bu tespite esas olan bilgi ve belgeler, 4045 sayılı Kanun çerçevesinde yapılan güvenlik soruşturması sonucunda idareye verildiğinden, 4045 sayılı Kanun'un 1. maddesi olaya uygulanacak hukuk kuralı niteliğindedir.

Anılan Kanun hükmü bakımından, Anayasa Mahkemesinin 27/02/2019 tarih ve 2014/7256 başvuru numaralı "K3" ve 29/05/2019 tarih ve 2014/15365 başvuru numaralı "K2" kararlarında:

"Öncelikle belirtilmesi gerekir ki, temel hak ve hürriyetlerin sınırlandırılmasına ilişkin kanunların şeklen var olması yeterli değildir. Kanunilik ölçütü aynı zamanda maddi bir içeriği de gerektirmekte olup bu noktada kanunun niteliği önem kazanmaktadır. Kanunla sınırlama ölçütü sınırlamanın erişilebilirliğini, öngörülebilirliğini ve kesinliğini ifade etmekte; böylece uygulayıcının keyfi davranışlarının önüne geçtiği gibi kişinin hukuku bilmesine de yardımcı olmakta; bu yönüyle hukuk güvenliği teminatı sağlamaktadır.

Kanunun bu gerekliliklere uygun olduğunun söylenebilmesi için, ilgili normun keyfiliğe karşı uygun bir koruma sağlaması, yetkili makamlara verilen yetkinin genişliğini ve icra edilme biçimlerini yeterli bir netlikte tanımlaması gerekmektedir.

Bununla birlikte, ilgili kanuni düzenlemenin söz konusu sınırlamaya ilişkin temel çerçeveyi ortaya koymakla birlikte özellikle uygulama koşulları ve usule ilişkin ayrıntıları düzenleyici işlemlere

bırakması mümkündür. Ancak bu ihtimalde de söz konusu düzenleyici işlemin yine muhataplarınca ulaşılabilir olması ve içeriği hakkında ilgilileri yeterince aydınlatacak nitelik ve açıklıkta olması gerekmektedir.

Belirli kamu görevlerinde çalıştırılacak personel hakkında uygulanan güvenlik soruşturması ve arşiv araştırmasının kanuni dayanağı 4045 sayılı Kanun'dur. 4045 sayılı Kanun'da güvenlik soruşturması ve arşiv araştırmasının kamu kurum ve kuruluşlarında yetkili olmayan kişilerin bilgi sahibi olmaları hâlinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile askerî teşkilatlarda, emniyet ve istihbarat teşkilatlarında çalıştırılacak kamu personeli, ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında yapılacak düzenlenmiştir.

Kamu görevlilerinin sadakat, tarafsızlık ve devlete bağlılık yükümlülüğü çerçevesinde devleti temsil eden ve millî güvenlik bakımından hassasiyet içeren bazı kamu görevlerine atanacak kişiler bakımından daha sıkı nitelikler aranması ve birtakım sınırlamaların getirilmesi doğaldır. Bu şekilde aranan nitelikler ve kanunlarda öngörülen kısıtlamalar, kamu hizmetinin etkin ve sağlıklı bir biçimde yürütülmesi amacına yöneliktir.

Dolayısıyla idarenin millî güvenlik açısından önem arz eden kadrolara atanacak kişilerin tabi olacağı güvenlik soruşturması ve arşiv araştırması konusunda kanunla temel çerçeveyi ortaya koyan kurallar getirmesi elbette mümkündür. Bu çerçevenin kanunla belirlenmesinden sonra uygulama koşulları ve usule ilişkin ayrıntılar düzenleyici işlemlerle belirlenebilir. Üstelik millî güvenlik ile ilgili alanlarda çalışacak personelin seçimi ve kontrolü bakımından konuyu düzenleyen kanunda aranacak öngörülebilirlik koşulunun diğer alanlardakilere göre daha esnek olacağı da söylenebilir. Ancak yine de bu alanda düzenleme getiren kanun ile diğer alt mevzuatın kişilere, kamu makamlarına hangi koşullarda ve hangi sınırlar içinde bu tür gizli tedbirler uygulama ve potansiyel olarak özel hayatın gizliliğine yönelik müdahalelerde bulunma yetkisi verildiğini yeterince açık olarak gösterecek ve olası kötüye kullanmalara karşı yeterli güvence sağlayacak şekilde kaleme alınmış olması gerekir.

4045 sayılı Kanun'un güvenlik soruşturmasına ve arşiv araştırmasına konu edilecek bilgi ve belgelerin neler olduğu, bu bilgilerin nerelerden elde edileceği ve ne suretle ve ne kadar süre ile saklanacağı, kişilerin söz konusu bilgilere itiraz etme olanağı olup olmadığı, bilgilerin bir müddet sonra silinmesinin mümkün olup olmadığı veya silinmesine dair izlenecek usulün ne olduğu, gizlilik dereceli kamu personeli ile meslek gruplarının tespiti, güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak mercilerin kimler olduğu ile ilgili hiçbir düzenleme getirmediği görülmektedir. Bunun yanı sıra kanunlarda, kesinleşmiş ceza mahkumiyetlerine dair ilk

olarak akla gelmesi ve uygulanması gereken kanun olan 5352 sayılı Kanun'a atıf içeren bir düzenlemenin bulunmadığı, bireyleri keyfiliğe karşı koruyucu hiçbir hükme yer verilmediği anlaşılmaktadır. Aynı şekilde Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği'nin de elde edilen bilgilerin saklanma süreleri, bilgilerin bir müddet sonra silinmesinin mümkün olup olmadığı veya silinmesine dair izlenecek usulün ne olduğu, kişilerin söz konusu bilgilere itiraz etme olanağı olup olmadığı hususlarını düzenlemediği, bireylerin özel hayatına saygı hakkının güvencelerini sağlayacak hükümlerden yoksun olduğu anlaşılmaktadır."

ifadelerine yer verilmek suretiyle, güvenlik soruşturması ve arşiv araştırması yapılmasının özel hayata saygı hakkına müdahale teşkil ettiği, temel ve hak ve özgürlükler bakımından sınırlama yapılırken kanunilik ilkesine riayet edilmesi gerektiği, bu konunun kanuni dayanağı olan 4045 sayılı Kanun'un 1. maddesinin temel hakkı kısıtlama konusunda kanunilik kriteri bakımından gerekli şartları taşımadığı ortaya konulmaktadır.

Bu durumda, Anayasa Mahkemesinin anılan kararları uyarınca idarelerce yapılacak tüm güvenlik soruşturmaları ve arşiv araştırmaları bakımından temel hak ihlali gündeme gelecektir ki bu durumun uygulama bakımından çok ciddi sorunlar doğuracağı tabiidir.

Açıklanan nedenle, Anayasa'nın 152. maddesi uyarınca 4045 sayılı Kanun'un 1. maddesinin iptali için Anayasa Mahkemesine başvurulması ve başvuru üzerine verilecek karara göre karar düzeltme istemi hakkında karar verilmesi gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay İdari Dava Daireleri Kurulunca, davacının karar düzeltme dilekçesinde öne sürdüğü hususlar, 2577 sayılı İdari Yargılama Usulü Kanunu'nun Geçici 8. maddesi uyarınca uygulanmasına devam edilen 3622 sayılı Kanun ile değişik 54. maddesi hükmüne uygun bulunduğundan, karar düzeltme isteminin kabulü ile Danıştay İdari Dava Daireleri Kurulunca verilen 18/02/2019 tarih ve E:2017/3749, K:2019/617 sayılı onama kararı kaldırılarak, Ankara 4. İdare Mahkemesinin 18/10/2017 tarih ve E:2017/2115, K:2017/3031 sayılı ısrarkararına yönelik davacının temyiz istemi yeniden incelendi, gereği görüldü:

İNCELEME VE GEREKÇE:

MADDİ OLAY:

Davacının vergi müfettiş yardımcılığı yazılı ve sözlü sınavında başarılı olması üzerine, hakkında yapılan arşiv araştırması ve güvenlik soruşturması sonucunda; hakkında şantaj ve hakaret suçlarını işlediği isnadıyla dava açılmış, Kars 1. Asliye Ceza Mahkemesinin 09/12/2010 tarih ve E:2010/299,

K:2010/425 sayılı kararıyla; şantaj suçundan 10 ay hapis, 4 gün adli para cezası karşılığı 80,00-TL para cezası ile cezalandırılmasına ve hükmün açıklanmasının geri bırakılmasına karar verilmesi nedeniyle, Maliye Bakanlığı Değerlendirme Komisyonu Başkanlığının 09/04/2014 tarih ve 2014/23 sayılı kararıyla; davacının atamasının yapılmasının uygun görülmediğine ilişkin kararına Maliye Bakanı tarafından Olur verilmesi üzerine, davacının atamasının yapılmamasına ilişkin dava konusu işlem tesis edilmiştir.

Bunun üzerine, anılan işlemin iptali istemiyle temyizden incelenen dava açılmıştır.

İLGİLİ MEVZUAT:

24/03/2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Özel Nitelikli Kişisel Verilerin İşlenme Şartları" kenar başlıklı 6. maddesinde, (1)Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, ... ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. (2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır. (3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir..."; "İstisnalar" kenar başlıklı 28. maddesinin birinci fıkrasında, " Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz: ... ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi. d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi..." kurallarına yer verilmiştir.

5352 sayılı Adli Sicil Kanunu'nun 6. maddesinde, "Kamu davasının açılmasının ertelenmesine ve hükmün açıklanmasının geri bırakılmasına ilişkin kararlar, ancak bir soruşturma veya kovuşturmayla bağlantılı olarak mahkeme, hâkim, askerî hâkim, Cumhuriyet Başsavcılığı veya askerî savcılık tarafından istenmesi halinde verilmek üzere kaydedilir." hükmü yer almaktadır.

657 sayılı Devlet Memurları Kanunu'nun 48. maddesinde, Devlet memurluğuna alınacaklarda aranılan genel ve özel şartlar belirtilerek, özel şartlar arasında kurumların özel kanun ve diğer mevzuatında aranan şartları taşımak gerektiği hüküm altına alınmıştır.

Maliye Bakanlığı Personeli Hakkında Yapılacak Güvenlik Soruşturması ve Arşiv Araştırması Yönergesi'nin "Kapsam" başlıklı 2.maddesinde;"Bu yönerge; Maliye Bakanlığı merkez ve taşra teşkilatında görevli bulunan personel ile ilk defa, yeniden veya kurumlararası naklen atanacaklardan gizlilik dereceli birim, kısım ve görevlerde çalıştırılması düşünülenler ile, yurtdışı teşkilatında sürekli

görevlendirilecek bütün personelin güvenlik soruşturması ve arşiv araştırmasına ilişkin usul ve esasları kapsar."; "Gizlilik Dereceli Birim, Kısım ve Görevler" başlıklı 6. maddesinde; "a) Merkez teşkilatında; 1- Müsteşarlık ve Müsteşar Yardımcılığı makamlarının özel büroları, ana hizmet birimlerinin denetim birimi başkanlıkları, özel büroları ile personel şubesi müdürlükleri, danışma ve denetim birimlerinin ve yardımcı birimlerin özel büroları ile personel şubesi müdürlükleri, 2- Teftiş Kurulu Başkanlığı, Hesap Uzmanları Kurulu Başkanlığı, Mali Suçları Araştırma Kurulu Başkanlığı, Personel Genel Müdürlüğü, Savunma Sekreterliği ve Özel Kalem Müdürlüğü, b) Taşra teşkilatında; Defterdarlık, Gelirler Bölge Müdürlüğü ve İşletme Bölge Müdürlüğü bünyesindeki denetmenler büroları, özel bürolar ile personel birimleri, c) Yurtdışı teşkilatında; Maliye Müşavirlikleri ile Maliye Ataşelikleri. B- Gizlilik dereceli görevleri yürüten personel: a) Unvanına bakılmaksızın yukarıda (A) bendinde sayılan yerlerde görevlendirilen personel, b) Görevli olduğu yer dikkate alınmaksızın, Bakanlık merkez ve taşra teşkilatında çalışan müdür ve daha üst düzeydeki personel, koruma ve güvenlik görevlileri ile kozmik evrak personeli, c) Kontrolörler ve Stajyer kontrolörler, d) Hazine avukatları, e) Özel Yönetmeliği bulunan merkez teşkilatı uzmanları ile denetmenler ve bunların yardımcıları. f) Birim amirince (Merkez ve döner sermaye teşkilatında Genel Müdür, Başkan veya Müstakil Daire Başkanı, taşra teşkilatında Defterdar veya Bölge Müdürü) hakkında Güvenlik Soruşturması ve Arşiv Araştırması yaptırılması uygun görülen personel" kurallarına yer verilmiştir.

4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ve Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun'un 1. maddesinin dava konusu işlem tarihi itibarıyla yürürlükte bulunan halinde, "Güvenlik Soruşturması ve Arşiv Araştırması; ... askeri, emniyet ve istihbarat teşkilatlarında çalıştırılacak kamu personeli ve ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında yapılır. Devletin güvenliğini, ulusun varlığını ve bütünlüğünü iç ve dış menfaatlerinin zarar görebileceği ve tehlikeye düşebileceği bilgi ve belgeler ile gizlilik dereceli kamu personeli ile meslek gruplarının tespiti birim ve kısımlarının tanımlarının yapılması güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak merciler ve üst kademe yöneticilerinin kimler olduğu Bakanlar Kurulu kararı ile yürürlüğe konulacak yönetmelik ile düzenlenir." hükmü bulunmaktadır.

12/04/2000 tarih ve 24018 sayılı Resmî Gazete'de yayımlanan Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği'nin (Yönetmelik) "Kapsam" kenar başlıklı 2. maddesinde, "Bu Yönetmelik; yetkili olmayan kişilerin bilgi sahibi olmaları halinde Devletin güvenliğinin, iç ve dış menfaatlerinin, ulusal varlığın ve bütünlüğün zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeleri,

bunların toplanmasını ve işlemini yürüten bakanlıklar ile kamu kurum ve kuruluşlarının ilgili birim ve kısımlarının belirlenmesini, Türk Silahlı Kuvvetlerinde, emniyet ve istihbarat teşkilatlarında, ceza infaz kurumları ve tutukevlerinde çalışacak personeli, ayrıca bakanlıklar ile kamu kurum ve kuruluşlarının yurtdışı teşkilatlarında sürekli görevlendirilecek bütün personel için yapılacak güvenlik soruşturması ve arşiv araştırmasının esas ve usullerini, bunu yapacak mercileri, hakkında güvenlik soruşturması ve arşiv araştırması yapılacak gizlilik dereceli yerlerde çalışan kamu personeli ile meslek grupları ve üst kademe yöneticilerini kapsar." ; "Güvenlik Soruşturması ve Arşiv Araştırması Yapılacak Makamlar" kenar başlıklı 7. maddesinde, "Güvenlik soruşturması ve arşiv araştırması, Milli İstihbarat Teşkilatı Müsteşarlığı, Emniyet Genel Müdürlüğü ve mahalli mülki idare amirlikleri tarafından yapılır. İçişleri Bakanlığı Kaçakçılık İstihbarat Harekat ve Bilgi Toplama Dairesi Başkanlığı'ndaki bilgi kayıtları ile Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü'ndeki adli sicil kaydı, talepleri üzerine, güvenlik soruşturması ve arşiv araştırmasını yapacak makamlar ile Türk Silahlı Kuvvetlerinin ilgili birimlerine verilir." ; "Hakkında Güvenlik Soruşturması ve Arşiv Araştırması Yapılacak Personel" kenar başlıklı 8. maddesinde, "Güvenlik soruşturması ve arşiv araştırması; gizlilik dereceli birim ve kısımlar ile askeri, emniyet, istihbarat teşkilatlarında ve ceza infaz kurumları ve tutukevlerinde çalıştırılacak personel hakkında yapılır. Emniyet Genel Müdürlüğü ve mahalli mülki idare amirlikleri, güvenlik soruşturması ve arşiv araştırmasını; bakanlıklar, kamu kurum ve kuruluşlarının gizlilik dereceli birim ve kısımları ile yurtdışı teşkilatında ve askeri, emniyet, istihbarat teşkilatlarında ve ceza infaz kurumu ve tutukevlerinde çalıştırılacak personel hakkında yapar."

kurallarına yer verilmiştir.

Aynı Yönetmeliğin 'Güvenlik Soruşturması ve Arşiv Araştırmasında Araştırılacak Hususlar' başlıklı 11. maddesinde,

"Güvenlik soruşturması ve arşiv araştırmasında kişinin içinde bulunduğu ortam da dikkate alınarak;

- a) Kimlik kontrolü, kimlik kayıtlarının doğruluk derecesi, uyrukluğ, geçmişte yabancı bir devletin uyrukluğuna girip girmediği,
- b) Kolluk kuvvetleri tarafından halen aranıp aranmadığı, kolluk kuvvetlerinin ve istihbarat ünitelerinin arşivlerinde bilgiler bulunup bulunmadığı, adli sicil kaydının ve hakkında bir tahdidin olup olmadığı,
- c) Yıkıcı faaliyetlerde bulunup bulunmadığı ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanuna ve Atatürk ilke ve inkılaplarına aykırı davranıp davranmadığı,

d) Şeref ve haysiyetini ihlal edecek ve görevine yansıyacak şekilde kumara, uyuşturucuya, içkiye, paraya ve aşırı bir şekilde menfaatine düşkün olup olmadığı, ahlak ve adaba aykırı davranış davranmadığı,

e) Yabancılarla, özellikle hasım ve hasım olması muhtemel Devlet mensupları ve temsilcileriyle ilgili derecesinin iç yüzü ve nedeni,

f) Sır saklama yeteneğinin olup olmadığı,

araştırılır.";

'Güvenlik Soruşturması ve Arşiv Araştırmasında İzlenecek Yöntem' başlıklı 12. maddesinde de,

" ...

c) Güvenlik soruşturması ve arşiv araştırması yapılması isteminin ilgili makama ulaşmasından itibaren arşiv araştırması sonuçları en geç 30 gün, güvenlik soruşturması sonuçları en geç 60 gün içinde cevaplandırılır. Soruşturma ve araştırma sonucunu içeren bilgi ve belgeler ilgilinin güvenlik makamlarındaki dosyasında asgari 'gizli' gizlilik derecesinde saklanır.

d) Güvenlik soruşturması ve arşiv araştırmasını isteyen makama, kişi hakkında karar vermeye yeterli bilgiler aktarılır.

e) Güvenlik soruşturması ve arşiv araştırmasının nasıl ve ne şekilde yapılacağı, soruşturma ve araştırma yapmaya yetkili makamların görev talimatları ile belirlenir.

f) Mahalli mülki idare amirliklerince yapılmış olan güvenlik soruşturması ve arşiv araştırmasında olumsuz durumu saptananların evrakının bir örneği dosya açılmak üzere Emniyet Genel Müdürlüğüne gönderilir.

g) Güvenlik soruşturması ve arşiv araştırmasında olumsuz durumu saptananlarla ilgili bilgiler Milli İstihbarat Teşkilatı Müsteşarlığı ve Emniyet Genel Müdürlüğüne karşılıklı olarak birbirlerine aktarılır.

.. " kuralları düzenlenmiştir.

HUKUKİ DEĞERLENDİRME

Somut olayda davacının işlediği iddia edilen fiillere istinaden yapılan yargılama neticesinde verilen hükmün açıklanmasının geri bırakılmasına ilişkin kararların kayıtlarının İstanbul Valiliği İl Emniyet

Müdürlüğü tarafından davalı idareye verildiği ve bu kayıtlar dikkate alınmak suretiyle davacının güvenlik soruşturmasının olumsuz sonuçlandırıldığı anlaşılmaktadır.

Belirli kamu görevlerinde çalıştırılacak personel hakkında uygulanan güvenlik soruşturması ve arşiv araştırmasının kanuni dayanağı 4045 sayılı Kanun'dur. 4045 sayılı Kanun'un dava konusu işlem tarihi itibarıyla yürürlükte bulunan halinde, güvenlik soruşturması ve arşiv araştırmasının; kamu kurum ve kuruluşlarında yetkili olmayan kişilerin bilgi sahibi olmaları hâlinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile askerî

teşkilatlarda, emniyet ve istihbarat teşkilatlarında çalıştırılacak kamu personeli, ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında yapılacağı düzenlenmiştir.

Kamu görevlilerinin sadakat, tarafsızlık ve devlete bağlılık yükümlülüğü çerçevesinde devleti temsil eden ve millî güvenlik bakımından hassasiyet içeren bazı kamu görevlerine atanacak kişiler bakımından daha sıkı nitelikler aranması ve birtakım sınırlamaların getirilmesi doğaldır. Bu şekilde aranan nitelikler ve kanunlarda öngörülen kısıtlamalar, kamu hizmetinin etkin ve sağlıklı bir biçimde yürütülmesi amacına yöneliktir.

Dolayısıyla idarenin millî güvenlik açısından önem arz eden kadrolara atanacak kişilerin tabi olacağı güvenlik soruşturması ve arşiv araştırması konusunda kanunla temel çerçeveyi ortaya koyan kurallar getirmesi mümkündür.

Ancak, bu alanda yapılan düzenlemelerin diğer kanuni düzenlemelerle çelişmemesi ve diğer düzenlemelerde gözetilen amaçları ortadan kaldırır nitelikte de olmaması gerekmektedir.

Bu bağlamda, yukarıda metnine yer verilen 4045 sayılı Kanun'un 1. maddesinin işlem tarihindeki hali incelendiğinde; maddede, kişilerin geçmiş ceza mahkûmiyetlerine ilişkin kayıtlar bakımından hangi suçların kamu görevine girmeye engel olacağı konusunda hiçbir belirleme yapılmadığı, suçlar arasında herhangi bir ayırım ve derecelendirme öngörülmediği, aynı şekilde hükmün açıklanmasının geri bırakılmasına konu kararların güvenlik soruşturması veya arşiv araştırmasının olumsuz sonuçlandırılmasının bir sebebi olup olmayacağı hususunda herhangi bir düzenlemeye yer verilmediği anlaşılmaktadır.

Nitekim, Anayasa Mahkemesinin 29/05/2019 tarih ve 2014/15365 başvuru numaralı "K2" kararında, özetle; işleme dayanak olan 4045 sayılı Kanun hükümlerinin temel hakkın kısıtlanması bakımından yeterli güvenceye sahip olmaması ve kanunilik ilkesine aykırı bulunması sebebiyle ve ayrıca 5352 sayılı Kanun'un 6. maddesinde kamu davasının açılmasının ertelenmesine ve hükmün

açıklanmasının geri bırakılmasına ilişkin kararların; ancak, bir soruşturma veya kovuşturmayla bağlantılı olarak mahkeme, hâkim, askerî hâkim, Cumhuriyet başsavcılığı veya askerî savcılık tarafından istenmesi hâlinde verileceği düzenlenmesine rağmen bu hükme aykırı şekilde yapılan güvenlik soruşturması ve arşiv araştırmasının özel hayata saygı hakkını ihlal ettiği belirtilmiştir.

Yine anılan kararda Anayasa Mahkemesi, İdare Mahkemesince davanın kesin hükme bağlanmasının ertelenmesine ilişkin karara dayanılarak hakkında herhangi bir mahkûmiyet kararı bulunmayan başvuruçunun ceza yargılamasına konu eylemleri işlediğinin sabit olduğu varsayımına dayanılarak karar verildiğinin anlaşıldığından bahisle başvuruçunun Anayasa'nın 36. ve 38. maddelerinde güvence altına alınan masumiyet karinesinin de ihlal edildiği sonucuna ulaşmıştır.

Bu durumda, 5352 sayılı Kanun'un 6. maddesine aykırı şekilde elde edilen bilgi ve belgelere dayalı olarak yapılan arşiv araştırması üzerine tesis edilen dava konusu işlemde hukuka uyarlık, İdare Mahkemesinin davanın reddine yönelik ısrar kararında ise hukuki isabet bulunmamaktadır.

KARAR SONUCU:

Açıklanan nedenlerle;

- 1.Davacının temyiz isteminin kabulüne;
- 2.Davanın yukarıda özetlenen gerekçeyle reddine ilişkin Ankara 4. İdare Mahkemesinin 18/10/2017 tarih ve E:2017/2115, K:2017/3031 sayılı ısrar kararının BOZULMASINA,
3. Yeniden bir karar verilmek üzere dosyanın anılan İdare Mahkemesine gönderilmesine,
- 4.12/03/2020 tarihinde oybirliği ile karar verildi.

Danıştay Kararı - İDDK. (E. 2019/2273)

Danıştay Kararı - İDDK., E. 2019/2273 K. 2021/778 T. 15.4.2021

T.C. DANIŞTAY İDARİ DAVA DAİRELERİ KURULU

Esas No: 2019/2273

Karar No: 2021/778

TEMYİZ EDENLER: 1- (DAVALI): ... Kurumu

VEKİLİ: Av. ...

2- (DAVACI): ... Elektrik Dağıtım A.Ş.

VEKİLİ: Av. ...

İSTEMİN KONUSU: Danıştay Onüçüncü Dairesinin 30/04/2019 tarih ve E:2015/2769, K:2019/1432 sayılı kararının aleyhlerine olan kısımlarının temyizen incelenerek bozulması taraflarca karşılıklı olarak istenilmektedir.

YARGILAMA SÜRECİ:

Dava konusu istem: 28/03/2015 tarih ve 29309 sayılı Resmî Gazete'de yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına İlişkin Yönetmeliğin 22. maddesiyle Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin iptali istenilmiştir.

Daire kararının özeti: Danıştay Onüçüncü Dairesinin 30/04/2019 tarih ve E:2015/2769, K:2019/1432 sayılı kararıyla;

Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'nin "Serbest tüketici veri tabanı" başlıklı 30/B maddesinde;

"(1) Serbest tüketicilere ilişkin uzlaştırmaya esas veriş-çekiş birimlerine ait tedarikçi değiştirme süreçlerinde kullanılmak üzere TEİAŞ ve dağıtım lisansı sahibi tüzel kişiler hizmet sundukları ve sayaçlarını okumakla yükümlü oldukları serbest tüketicilerin aşağıda yer alan bilgilerini PYS üzerinde tanımlanacak veri tabanına eklemek ve güncel tutmakla yükümlüdür:

a) Serbest tüketicinin adı veya unvanı,

- b) Tüketim noktasının PYS'ye kayıt için gerekli kayıt kodu,
- c) Tüketim noktasının içerisinde bulunduğu il ve ilçe bilgisi,
- ç) Tüketim noktasının açık adresi.

(2) Piyasa İşletmecisi ilgili veri tabanına tedarikçilerin erişimini sağlamakla yükümlüdür. Bu madde kapsamında edinilen bilgiler lisansta belirtilen faaliyetler dışında kullanılamaz ve ticarete konu edilemez.

(3) TEİAŞ ve dağıtım lisansı sahibi tüzel kişiler birinci fıkranın (b) bendinde yer alan kayıt kodunun nasıl oluşturulduğuna ilişkin açıklamayı PYS üzerinde serbest tüketici kayıt ekranında yayımlar.

(4) PYS, 30/A maddesi kapsamındaki kayıt girişleri sırasında yeni tedarikçi olmak isteyen piyasa katılımcısının sayaç kaydı için giriş yaptığı kodun birinci fıkranın (b) bendi çerçevesinde oluşturulan veri tabanında olup olmadığını kontrol eder. Veri tabanında yer alan kodlarla eşleşmeyen girişlere izin verilmez.

(5) TEİAŞ ve dağıtım lisansı sahibi tüzel kişilerin veri tabanına ilişkin yükümlülüklerini yerine getirmemesi nedeni ile serbest tüketicinin yeni tedarikçisinin portföyüne geçişinin engellendiğinin tespiti halinde PYS üzerinden gerekli düzeltme yapılır ve Kanununun 16 ncı maddesi uyarınca yaptırım uygulanır." düzenlemesine yer verildiği;

Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 1. fıkrası yönünden;

Dava konusu edilen Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'nin "Serbest tüketici veri tabanı" başlıklı 30/B maddesi uyarınca, TEİAŞ ve dağıtım lisansı sahibi tüzel kişilerin hizmet sundukları ve sayaçlarını okumakla yükümlü oldukları serbest tüketicilerin adı veya unvanını, tüketim noktasının PYS'ye kayıt için gerekli kayıt kodunu, tüketim noktasının içerisinde bulunduğu il ve ilçe bilgisini ve tüketim noktasının açık adresini PYS üzerinde tanımlanacak veri tabanına eklemeleri ve güncel tutmaları, piyasa işletmecisinin de ilgili veri tabanına tedarikçilerin erişimini sağlaması gerektiği; bu düzenlemenin serbest tüketicilere ilişkin uzlaştırmaya esas veri-çekiş birimlerine ait tedarikçi değiştirme süreçlerinde uygulanacağı;

Dava konusu düzenlemenin serbest tüketicilerin tedarikçi seçme ve değiştirme süreçlerine yönelik olduğu, bu süreçlerde serbest tüketiciler ve yeni tedarikçiler açısından meydana gelen olumsuzlukların giderilmesinin amaçlandığı; ayrıca, tedarikçiler açısından "abone no", "sayaç no" gibi takip numaralarına standart getirilmesinin öngörüldüğü;

Belirli veya kimliđi belirlenebilir olmak şartıyla, bir kiřiye iliřkin bütn bilgilerin kiřiisel veri olarak tanımlandığı; kiřiisel veriyi, adı, soyadı, dođum tarihi ve dođum yeri gibi bireyin sadece kimliđini ortaya koyan bilgiler deđil; telefon numarası, motorlu tařıt plakası, sosyal güvenlik numarası, pasaport numarası, zgeçmiř, resim, grnt ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileřimde bulunulan kiřiler, grup yelikleri, aile bilgileri gibi kiřiye dođrudan veya dolaylı olarak belirlenebilir kılan tm veriler olarak deđerlendirmek gerektiđi; kiřinin belirli olması, kiřiisel veri ile bařka hiřbir iřleme ya da yoruma gerek kalmaksızın kiřinin kimliđinin ortaya çıkarılabiliyor olması iken, kiřinin belirlenebilir olmasının veri ile kiřinin iliřkilendirilmesi suretiyle kiřinin tanımlanabilmesi olduđu;

Kiřiisel verilerin korunması hakkının, kiřinin insan onurunun korunmasının ve kiřiliđini serbestçe geliřtirebilmesi hakkının zel bir biřimi olarak, bireyin hak ve zgrlklerini kiřiisel verilerin iřlenmesi sırasında korumayı amaçlamadıđı; biliřim teknolojilerindeki geliřmeler sonucunda, geleneksel yntemlerle ulařılması mmkn olmayan çok sayıda verinin toplanabilmesi; daha nce birbirinden iliřkisiz řekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri eřleřtirme ve veri madenciliđi gibi ileri teknolojik imknlarla analize tabi tutulmak suretiyle, veriden yeni veriler retme kapasitesinin artması; verilere eriřim ve veri transferinin kolaylařması; kiřiisel verilerin ticari iřletmeler iřin kıymetli bir varlık niteliđi kazanması neticesinde meydana gelen risklerin daha yaygın ve nemli boyutlara ulařması ve terr ve suç rgtlerinin kiřiisel verileri ele geçirme ynndeki faaliyetlerinin artması gibi etkenlerin, gnmzde kiřiisel verilerin en st seviyede korunmasını zorunlu kıldığı;

Bu bađlamda, Anayasa'nın 20. maddesinin çnc fıkrasının son cmlesinde, "Kiřiisel verilerin korunmasına iliřkin esas ve usuller kanunla dzenlenir." hkmne yer verilerek kiřiisel verilerin korunması hakkının anayasal gvenceye bađlandıđı, bu verilerin kamu makamlarının keyfi mdahalelerine karřı koruma altına alındığı ve iřlenmesi ancak kiřinin ađık rızası veya kanunda ngrlen hllerde mmkn kılındığı;

Dava konusu Ynetmeliđin 30/B maddesinin 1. fıkrasının (a) bendi ile kiřiisel veri olan serbest tketicilerin adı veya unvanının, PYS zerinde tanımlanacak veri tabanına ekleneceđi, piyasa iřletmecisinin veri tabanına tedarikçilerin eriřimini sađlayacađının dzenlendiđi;

Anayasa'nın 20. maddesinin 3. fıkrasına aykırı olarak, dava konusu dzenlemeyle kiřiye belirlenebilir kılan kiřiisel veri niteliđinde olan serbest tketicilerin adları veya unvanlarının tedarikçilerin eriřimine ađık olan veri tabanına eklenmesinde hukuka uygunluk bulunmadığı;

Yönetmeliğin dava konusu maddesinin birinci fıkrasında yer alan diğer kısımlarında talep edilen bilgilerin tüketim noktasına ilişkin veriler olduğu; bu verilerin, kişinin ad ve unvanı olmaksızın kişinin belirlenebilmesine yeterli olabilecek veriler olmadığı; dolayısıyla, kişisel veri olarak kabul edilemeyecek veriler olduğu, tüketiciler değişebilecekken tüketim noktalarına ilişkin verilerin sabit olduğu da dikkate alındığında, Yönetmeliğin 30/B maddesinin 1. fıkrasının diğer kısımlarında hukuka aykırılık bulunmadığı;

Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 2. fıkrasının yönünden;

28/05/2016 tarih ve 29725 Sayılı Resmî Gazete'de Yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmeliğin 6. maddesi ile dava konusu "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 2. fıkrasında yer alan "Piyasa İşletmecisi ilgili veri tabanına tedarikçilerin erişimini sağlamakla yükümlüdür. Bu madde kapsamında edinilen bilgiler lisansta belirtilen faaliyetler dışında kullanılamaz ve ticarete konu edilemez." düzenlemesinin; "Tedarikçiler, tedarikçi değiştirme ve mali uzlaştırma süreçlerinde kullanılmak üzere tüketicilerine ilişkin, a) Serbest tüketicinin adı veya unvanı, b) Gerçek kişiler için T.C. kimlik numarası, tüzel kişiler için vergi kimlik numarası, bilgilerini PYS üzerinde tanımlanacak veri tabanına eklemek ve güncel tutmakla yükümlüdür. Piyasa İşletmecisi bu bilgileri veri tutarlılığının kontrolü amacı ile kullanır ve kişisel verilerin korunmasını sağlayacak önlemleri alır. Tedarikçilerin söz konusu yükümlülüklerini yerine getirmediklerinin tespiti halinde Kanununun 16 ncı maddesi uyarınca yaptırım uygulanır." şeklinde değiştirildiği ve davanın konusuz kaldığı anlaşıldığından, Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 2. fıkrası açısından uyumsuzluğun esası hakkında karar verilmesine gerek bulunmadığı;

Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 3., 4. ve 5. fıkraları yönünden;

Dava konusu edilen Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'nin "Serbest tüketici veri tabanı" başlıklı 30/B maddesinin 3. ve 4. fıkralarında Piyasa Yönetim Sisteminin (PYS) öngörülen şekilde çalışmasının sağlanmasına ilişkin birtakım düzenlemelere yer verildiği, bu düzenlemelerin, PYS'nin kullanımına ilişkin olduğu;

Yönetmeliğin 30/B maddesinin 5. fıkrasında ise, veri tabanına ilişkin yükümlülüklerin yerine getirilmemesi nedeniyle serbest tüketicinin yeni tedarikçisinin portföyüne geçişinin engellendiğinin tespiti hâlinde gerekli düzeltmelerin yapılacağı ve 6446 sayılı Kanun'a göre yaptırım uygulanacağını öngörüldüğü, Yönetmelik'te düzenlenen yükümlülüklerin yerine getirilmemesi hâlinde uygulanacak

yaptırımlara ilişkin, Kanun hükmüne atıf yapıldığı; bu itibarla, Yönetmeliğin 30/B maddesinin 3., 4. ve 5. fıkralarında hukuka aykırılık bulunmadığı gerekçesiyle;

Dava konusu 28/03/2015 tarih ve 29309 sayılı Resmî Gazete'de yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına İlişkin Yönetmeliğin 22. maddesiyle, Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 1. fıkrasının (a) bendinin iptaline, 2. fıkrasının iptali istemi hakkında karar verilmesine yer olmadığına; maddenin diğer kısımları yönünden ise davanın reddine karar verilmiştir.

TEMYİZ EDENLERİN İDDİALARI:

Davacı tarafından, dava konusu Yönetmeliğin 30/B maddesinin tamamının hukuka aykırı olduğu ileri sürülmektedir.

Davalı idare tarafından, iptal edilen düzenlemenin karar tarihinden önce yürürlükten kaldırılmış olması nedeniyle karar verilmesine yer olmadığına karar verilmesi gerektiği ileri sürülmektedir.

KARŞI TARAFIN SAVUNMALARI:

Davacı tarafından, Danıştay Onüçüncü Dairesince verilen kararın iptale ilişkin kısmının usul ve hukuka uygun bulunduğu ve temyiz dilekçesinde öne sürülen nedenlerin, kararın bu kısmının bozulmasını gerektirecek nitelikte olmadığı belirtilerek temyiz isteminin reddi gerektiği savunulmaktadır.

Davalı idare tarafından, savunma verilmemiştir.

DANIŞTAY TETKİK HÂKİMİ ...'NUN DÜŞÜNCESİ: Temyiz istemlerinin reddi ile Daire kararının temyize konu kısımlarının onanması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay İdari Dava Daireleri Kurulunca, Tetkik Hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereği görüldü:

HUKUKİ DEĞERLENDİRME:

Danıştay dava dairelerinin nihai kararlarının temyizen incelenerek bozulması, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 49. maddesinde yer alan;

"a) Görev ve yetki dışında bir işe bakılmış olması,

b) Hukuka aykırı karar verilmesi,

c) Usul hükümlerinin uygulanmasında kararı etkileyebilecek nitelikte hata veya eksikliklerin bulunması" sebeplerinden birinin varlığı hâlinde mümkündür.

Temyizen incelenen kararın davanın reddine ve iptale yönelik kısımları usul ve hukuka uygun olup, temyiz dilekçelerinde ileri sürülen iddialar kararın temyize konu bu kısımlarının bozulmasını gerektirecek nitelikte görülmemiştir.

KARAR SONUCU:

Açıklanan nedenlerle;

1. Tarafların temyiz istemlerinin reddine,
2. Yukarıda özetlenen gerekçeyle dava konusu düzenlemenin kısmen iptali, kısmen dava hakkında karar verilmesine yer olmadığı, kısmen davanın reddi yolundaki Danıştay Onüçüncü Dairesinin temyize konu 30/04/2019 tarih ve E:2015/2769, K:2019/1432 sayılı kararının temyize konu iptale ve davanın reddine yönelik kısımlarının ONANMASINA,
3. Kesin olarak, 15/04/2021 tarihinde, davacının temyiz istemi yönünden oybirliği, davalı idarenin temyiz istemi yönünden oyçokluğu ile karar verildi.

KARŞI OY

X- Dava konusu Yönetmelik'in iptal edilen 30/B maddesinin 1. fıkrasının (a) bendi, 28/05/2016 tarih ve 29725 sayılı Resmî Gazete'de yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmeliğin 6. maddesi ile yürürlükten kaldırılmıştır.

Dava konusu edilen düzenlemenin yürürlükten kaldırılmış olması ve eski düzenlemeye dayalı olarak tesis edilmiş bir uygulama işleminin dava konusu edilmemiş olması karşısında bu kısım yönünden davanın konusu kalmamıştır.

Açıklanan nedenle, bu kısma ilişkin olarak Danıştay Onüçüncü Dairesince konusu kalmayan dava hakkında karar verilmesine yer olmadığına karar verilmesi gerektiğinden, davalı idarenin temyiz isteminin kabulü ve Daire kararının iptale yönelik kısmının bozulması gerektiği oyuyla karara bu kısım yönünden katılmıyorum.

KARŞI OY

XX- Dava, 28/03/2015 tarih ve 29309 sayılı Resmî Gazete'de yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına İlişkin Yönetmeliğin 22. maddesiyle Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin iptali istemiyle açılmıştır.

Temyize konu kararda, Anayasa'nın 20. maddesinin 3. fıkrasına aykırı olarak, dava konusu düzenlemeyle kişiyi belirlenebilir kılan kişisel veri niteliğinde olan serbest tüketicilerin adları veya unvanlarının tedarikçilerin erişimine açık olan veri tabanına eklenmesinde hukuka uygunluk bulunmadığı gerekçesiyle, uyuşmazlık konusu 30/B maddesinin 1. fıkrasının (a) bendinin iptaline karar verilmiştir.

07/04/2016 tarih ve 29677 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanun ile kişisel verilerin işlenmesinde uyulacak usul ve esaslar düzenlenmiş olduğundan, dava devam ederken yürürlüğe giren bu yasal düzenleme dikkate alınarak uyuşmazlığın çözüme kavuşturulması gerektiği oyuyla, çoğunluk kararının Daire kararının iptale yönelik kısmının onanmasına ilişkin kısmına katılmıyorum.

Danıştay Kararı - İDDK. (E. 2019/2365)

Danıştay Kararı - İDDK., E. 2019/2365 K. 2020/2461 T. 19.11.2020

İSTEMİN KONUSU: Danıştay Onüçüncü Dairesinin 30/04/2019 tarih ve E:2015/2532, K:2019/1429 sayılı kararının iptale yönelik kısmının temyizden incelenerek bozulması istenilmektedir.

YARGILAMA SÜRECİ:

Dava konusu istem: 28/03/2015 tarih ve 29309 sayılı Resmî Gazete'de yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına İlişkin Yönetmeliğin 22. maddesiyle Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin iptali istenilmiştir.

Daire kararının özeti: Danıştay Onüçüncü Dairesinin 30/04/2019 tarih ve E:2015/2532, K:2019/1429 sayılı kararıyla;

Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'nin "Serbest tüketici veri tabanı" başlıklı 30/B maddesinde;

"(1) Serbest tüketicilere ilişkin uzlaştırmaya esas veriş-çekiş birimlerine ait tedarikçi değiştirme süreçlerinde kullanılmak üzere TEİAŞ ve dağıtım lisansı sahibi tüzel kişiler hizmet sundukları ve sayaçlarını okumakla yükümlü oldukları serbest tüketicilerin aşağıda yer alan bilgilerini PYS üzerinde tanımlanacak veri tabanına eklemek ve güncel tutmakla yükümlüdür:

- a) Serbest tüketicinin adı veya unvanı,
- b) Tüketim noktasının PYS'ye kayıt için gerekli kayıt kodu,
- c) Tüketim noktasının içerisinde bulunduğu il ve ilçe bilgisi,
- ç) Tüketim noktasının açık adresi.

(2) Piyasa İşletmecisi ilgili veri tabanına tedarikçilerin erişimini sağlamakla yükümlüdür. Bu madde kapsamında edinilen bilgiler lisansta belirtilen faaliyetler dışında kullanılamaz ve ticarete konu edilemez.

(3) TEİAŞ ve dağıtım lisansı sahibi tüzel kişiler birinci fıkranın (b) bendinde yer alan kayıt kodunun nasıl oluşturulduğuna ilişkin açıklamayı PYS üzerinde serbest tüketici kayıt ekranında yayımlar.

(4) PYS, 30/A maddesi kapsamındaki kayıt girişleri sırasında yeni tedarikçi olmak isteyen piyasa katılımcısının sayaç kaydı için giriş yaptığı kodun birinci fıkranın (b) bendi çerçevesinde oluşturulan veri tabanında olup olmadığını kontrol eder. Veri tabanında yer alan kodlarla eşleşmeyen girişlere izin verilmez.

(5) TEİAŞ ve dağıtım lisansı sahibi tüzel kişilerin veri tabanına ilişkin yükümlülüklerini yerine getirmemesi nedeni ile serbest tüketicinin yeni tedarikçisinin portföyüne geçişinin engellendiğinin tespiti halinde PYS üzerinden gerekli düzeltme yapılır ve Kanunun 16 ncı maddesi uyarınca yaptırım uygulanır." düzenlemesine yer verildiği;

Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 1. fıkrası yönünden;

Dava konusu edilen Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'nin "Serbest tüketici veri tabanı" başlıklı 30/B maddesi uyarınca, TEİAŞ ve dağıtım lisansı sahibi tüzel kişilerin hizmet sundukları ve sayaçlarını okumakla yükümlü oldukları serbest tüketicilerin adı veya unvanını, tüketim noktasının PYS'ye kayıt için gerekli kayıt kodunu, tüketim noktasının içerisinde bulunduğu il ve ilçe bilgisini ve tüketim noktasının açık adresini PYS üzerinde tanımlanacak veri tabanına eklemeleri ve güncel tutmaları, piyasa işletmecisinin de ilgili veri tabanına tedarikçilerin erişimini sağlaması gerektiği; bu düzenlemenin serbest tüketicilere ilişkin uzlaştırmaya esas veri-çekiş birimlerine ait tedarikçi değiştirme süreçlerinde uygulanacağı;

Dava konusu düzenlemenin serbest tüketicilerin tedarikçi seçme ve değiştirme süreçlerine yönelik olduğu, bu süreçlerde serbest tüketiciler ve yeni tedarikçiler açısından meydana gelen olumsuzlukların giderilmesinin amaçlandığı; ayrıca, tedarikçiler açısından "abone no", "sayaç no" gibi takip numaralarına standart getirilmesinin öngörüldüğü;

Belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgilerin kişisel veri olarak tanımlandığı; kişisel veriyi, adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler olarak değerlendirmek gerektiği; kişinin belirli olması, kişisel veri ile başka hiçbir işleme ya da yoruma gerek kalmaksızın kişinin kimliğinin ortaya çıkarılabiliyor olması iken, kişinin belirlenebilir olmasının veri ile kişinin ilişkilendirilmesi suretiyle kişinin tanımlanabilmesi olduğu;

Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamadığı; bilişim teknolojilerindeki gelişmeler sonucunda, geleneksel yöntemlerle ulaşılmaması mümkün olmayan çok sayıda verinin toplanabilmesi; daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması; verilere erişim ve veri transferinin kolaylaşması; kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde meydana gelen risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenlerin, günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kıldığı;

Bu bağlamda, Anayasa'nın 20. maddesinin üçüncü fıkrasının son cümlesinde, "Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilerek kişisel verilerin korunması hakkının anayasal güvenceye bağlandığı, bu verilerin kamu makamlarının keyfi müdahalelerine karşı koruma altına alındığı ve işlenmesi ancak kişinin açık rızası veya kanunda öngörülen hâllerde mümkün kılındığı;

Dava konusu Yönetmeliğin 30/B maddesinin 1. fıkrasının (a) bendi ile kişisel veri olan serbest tüketicilerin adı veya unvanının, PYS üzerinde tanımlanacak veri tabanına ekleneceği, piyasa işletmecisinin veri tabanına tedarikçilerin erişimini sağlayacağını düzenlendiği;

Anayasa'nın 20. maddesinin 3. fıkrasına aykırı olarak, dava konusu düzenlemeyle kişiyi belirlenebilir kılan kişisel veri niteliğinde olan serbest tüketicilerin adları veya unvanlarının tedarikçilerin erişimine açık olan veri tabanına eklenmesinde hukuka uygunluk bulunmadığı;

Yönetmeliğin dava konusu maddesinin birinci fıkrasında yer alan diğer kısımlarında talep edilen bilgilerin tüketim noktasına ilişkin veriler olduğu; bu verilerin, kişinin ad ve unvanı olmaksızın kişinin belirlenebilmesine yeterli olabilecek veriler olmadığı; dolayısıyla, kişisel veri olarak kabul edilemeyecek veriler olduğu, tüketiciler değişebilecekken tüketim noktalarına ilişkin verilerin sabit olduğu da dikkate alındığında, Yönetmeliğin 30/B maddesinin 1. fıkrasının diğer kısımlarında hukuka aykırılık bulunmadığı;

Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 2. fıkrası yönünden;

28/05/2016 tarih ve 29725 Sayılı Resmî Gazete'de Yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmeliğin 6. maddesi ile dava konusu "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 2. fıkrasında yer alan "Piyasa İşletmecisi ilgili veri tabanına tedarikçilerin erişimini sağlamakla yükümlüdür. Bu madde kapsamında edinilen bilgiler lisansta belirtilen faaliyetler dışında kullanılamaz ve ticarete konu edilemez." düzenlemesinin; "Tedarikçiler, tedarikçi değiştirme ve mali uzlaştırma süreçlerinde kullanılmak üzere tüketicilerine ilişkin, a) Serbest tüketicinin adı veya unvanı, b) Gerçek kişiler için T.C. kimlik numarası, tüzel kişiler için vergi kimlik numarası, bilgilerini PYS üzerinde tanımlanacak veri tabanına eklemek ve güncel tutmakla yükümlüdür. Piyasa İşletmecisi bu bilgileri veri tutarlılığının kontrolü amacı ile kullanır ve kişisel verilerin korunmasını sağlayacak önlemleri alır. Tedarikçilerin söz konusu yükümlülüklerini yerine getirmediklerinin tespiti halinde Kanununun 16 ncı maddesi uyarınca yaptırım uygulanır." şeklinde değiştirildiği ve davanın konusuz kaldığı anlaşıldığından, Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 2. fıkrası açısından uyumsuzluğun esası hakkında karar verilmesine gerek bulunmadığı;

Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 3., 4. ve 5. fıkraları yönünden;

Dava konusu edilen Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'nin "Serbest tüketici veri tabanı" başlıklı 30/B maddesinin 3. ve 4. fıkralarında Piyasa Yönetim Sisteminin (PYS) öngörülen şekilde çalışmasının sağlanmasına ilişkin birtakım düzenlemelere yer verildiği, bu düzenlemelerin, PYS'nin kullanımına ilişkin olduğu;

Yönetmeliğin 30/B maddesinin 5. fıkrasında ise, veri tabanına ilişkin yükümlülüklerin yerine getirilmemesi nedeniyle serbest tüketicinin yeni tedarikçisinin portföyüne geçişinin engellendiğinin tespiti hâlinde gerekli düzeltmelerin yapılacağı ve 6446 sayılı Kanun'a göre yaptırım uygulanacağını öngörüldüğü, Yönetmelik'te düzenlenen yükümlülüklerin yerine getirilmemesi hâlinde uygulanacak yaptırımlara ilişkin, Kanun hükmüne atıf yapıldığı; bu itibarla, Yönetmeliğin 30/B maddesinin 3., 4. ve 5. fıkrasında hukuka aykırılık bulunmadığı gerekçesiyle;

Dava konusu 28/03/2015 tarih ve 29309 sayılı Resmî Gazete'de yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına İlişkin Yönetmeliğin 22. maddesiyle, Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin birinci fıkrasının (a) bendinin iptaline, ikinci fıkrasının iptali istemi hakkında karar verilmesine yer olmadığına; maddenin diğer kısımları yönünden ise davanın reddine karar verilmiştir.

TEMYİZ EDENİN İDDİALARI: Davalı idare tarafından, iptal edilen düzenlemenin karar tarihinden önce yürürlükten kaldırılmış olması nedeniyle karar verilmesine yer olmadığına karar verilmesi gerektiği ileri sürülmektedir.

KARŞI TARAFIN SAVUNMASI: Davacı tarafından, savunma verilmemiştir.

DANIŞTAY TETKİK HÂKİMİ K1'NUN DÜŞÜNCESİ: Temyiz isteminin reddi ile Daire kararının temyize konu kısmının onanması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay İdari Dava Daireleri Kurulunca, Tetkik Hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereği görüldü:

HUKUKİ DEĞERLENDİRME:

Danıştay dava dairelerinin nihai kararlarının temyizen incelenerek bozulması, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 49. maddesinde yer alan;

"a) Görev ve yetki dışında bir işe bakılmış olması,

b) Hukuka aykırı karar verilmesi,

c) Usul hükümlerinin uygulanmasında kararı etkileyebilecek nitelikte hata veya eksikliklerin bulunması" sebeplerinden birinin varlığı hâlinde mümkündür.

Temyizen incelenen kararın dava konusu düzenlemenin iptaline ilişkin kısmı usul ve hukuka uygun olup, temyiz dilekçesinde ileri sürülen iddialar kararın temyize konu bu kısmının bozulmasını gerektirecek nitelikte görülmemiştir.

KARAR SONUCU:

Açıklanan nedenlerle;

1. Davalı idarenin temyiz isteminin reddine,
2. Yukarıda özetlenen gerekçeyle dava konusu düzenlemenin kısmen iptali, kısmen dava hakkında karar verilmesine yer olmadığına, kısmen davanın reddi yolunda verilen Danıştay Onüçüncü Dairesinin 30/04/2019 tarih ve E:2015/2532, K:2019/1429 sayılı kararının temyize konu iptale ilişkin kısmının ONANMASINA,
3. Kesin olarak, 19/11/2020 tarihinde oyçokluğu ile karar verildi.

KARŞIOY

X-Dava konusu Yönetmelik'in iptal edilen 30/B maddesinin birinci fıkrasının (a) bendi, 28/05/2016 tarih ve 29725 sayılı Resmî Gazete'de yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmeliğin 6. maddesi ile yürürlükten kaldırılmıştır.

Dava konusu edilen düzenlemenin yürürlükten kaldırılmış olması ve eski düzenlemeye dayalı olarak tesis edilmiş bir uygulama işleminin dava konusu edilmemiş olması karşısında davanın konusu kalmamıştır.

Açıklanan nedenle, temyize konu kısma ilişkin olarak Danıştay Onüçüncü Dairesince konusu kalmayan dava hakkında karar verilmesine yer olmadığına karar verilmesi gerektiği oyuyla, karara katılmıyoruz.

KARŞIOY

XX-Dava, 28/03/2015 tarih ve 29309 sayılı Resmî Gazete'de yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına İlişkin Yönetmeliğin 22. maddesiyle Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin iptali istemiyle açılmıştır.

Temyize konu kararda, Anayasa'nın 20. maddesinin 3. fıkrasına aykırı olarak, dava konusu düzenlemeyle kişiyi belirlenebilir kılan kişisel veri niteliğinde olan serbest tüketicilerin adları veya unvanlarının tedarikçilerin erişimine açık olan veri tabanına eklenmesinde hukuka uygunluk bulunmadığı gerekçesiyle, uyuşmazlık konusu 30/B maddesinin birinci fıkrasının (a) bendinin iptaline karar verilmiştir.

07/04/2016 tarih ve 29677 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanun ile kişisel verilerin işlenmesinde uyulacak usul ve esaslar düzenlenmiş olduğundan, dava devam ederken yürürlüğe giren bu yasal düzenleme dikkate alınarak uyuşmazlığın çözüme kavuşturulması gerektiği oyuyla, Daire kararının temyize konu edilen iptale ilişkin kısmının onanmasına dair karara katılmıyorum.

Danıştay Kararı - İDDK. (E. 2019/2278)

Danıştay Kararı - İDDK., E. 2019/2278 K. 2020/2460 T. 19.11.2020

İSTEMİN KONUSU: Danıştay Onüçüncü Dairesinin 30/04/2019 tarih ve E:2015/2767, K:2019/1431 sayılı kararının iptale yönelik kısmının temyizden incelenerek bozulması istenilmektedir.

YARGILAMA SÜRECİ:

Dava konusu istem: 28/03/2015 tarih ve 29309 sayılı Resmî Gazete'de yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına İlişkin Yönetmeliğin 22. maddesiyle Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin iptali istenilmiştir.

Daire kararının özeti: Danıştay Onüçüncü Dairesinin 30/04/2019 tarih ve E:2015/2767, K:2019/1431 sayılı kararıyla;

Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'nin "Serbest tüketici veri tabanı" başlıklı 30/B maddesinde;

"(1) Serbest tüketicilere ilişkin uzlaştırmaya esas veriş-çekiş birimlerine ait tedarikçi değiştirme süreçlerinde kullanılmak üzere TEİAŞ ve dağıtım lisansı sahibi tüzel kişiler hizmet sundukları ve sayaçlarını okumakla yükümlü oldukları serbest tüketicilerin aşağıda yer alan bilgilerini PYS üzerinde tanımlanacak veri tabanına eklemek ve güncel tutmakla yükümlüdür:

- a) Serbest tüketicinin adı veya unvanı,
- b) Tüketim noktasının PYS'ye kayıt için gerekli kayıt kodu,
- c) Tüketim noktasının içerisinde bulunduğu il ve ilçe bilgisi,
- ç) Tüketim noktasının açık adresi.

(2) Piyasa İşletmecisi ilgili veri tabanına tedarikçilerin erişimini sağlamakla yükümlüdür. Bu madde kapsamında edinilen bilgiler lisansta belirtilen faaliyetler dışında kullanılamaz ve ticarete konu edilemez.

(3) TEİAŞ ve dağıtım lisansı sahibi tüzel kişiler birinci fıkranın (b) bendinde yer alan kayıt kodunun nasıl oluşturulduğuna ilişkin açıklamayı PYS üzerinde serbest tüketici kayıt ekranında yayımlar.

(4) PYS, 30/A maddesi kapsamındaki kayıt girişleri sırasında yeni tedarikçi olmak isteyen piyasa katılımcısının sayaç kaydı için giriş yaptığı kodun birinci fıkranın (b) bendi çerçevesinde oluşturulan veri tabanında olup olmadığını kontrol eder. Veri tabanında yer alan kodlarla eşleşmeyen girişlere izin verilmez.

(5) TEİAŞ ve dağıtım lisansı sahibi tüzel kişilerin veri tabanına ilişkin yükümlülüklerini yerine getirmemesi nedeni ile serbest tüketicinin yeni tedarikçisinin portföyüne geçişinin engellendiğinin tespiti halinde PYS üzerinden gerekli düzeltme yapılır ve Kanunun 16 ncı maddesi uyarınca yaptırım uygulanır." düzenlemesine yer verildiği;

Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 1. fıkrası yönünden;

Dava konusu edilen Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'nin "Serbest tüketici veri tabanı" başlıklı 30/B maddesi uyarınca, TEİAŞ ve dağıtım lisansı sahibi tüzel kişilerin hizmet sundukları ve sayaçlarını okumakla yükümlü oldukları serbest tüketicilerin adı veya unvanını, tüketim noktasının PYS'ye kayıt için gerekli kayıt kodunu, tüketim noktasının içerisinde bulunduğu il ve ilçe bilgisini ve tüketim noktasının açık adresini PYS üzerinde tanımlanacak veri tabanına eklemeleri ve güncel tutmaları, piyasa işletmecisinin de ilgili veri tabanına tedarikçilerin erişimini sağlaması gerektiği; bu düzenlemenin serbest tüketicilere ilişkin uzlaştırmaya esas veriş-çekiş birimlerine ait tedarikçi değiştirme süreçlerinde uygulanacağı;

Dava konusu düzenlemenin serbest tüketicilerin tedarikçi seçme ve değiştirme süreçlerine yönelik olduğu, bu süreçlerde serbest tüketiciler ve yeni tedarikçiler açısından meydana gelen olumsuzlukların giderilmesinin amaçlandığı; ayrıca, tedarikçiler açısından "abone no", "sayaç no" gibi takip numaralarına standart getirilmesinin öngörüldüğü;

Belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgilerin kişisel veri olarak tanımlandığı; kişisel veriyi, adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler olarak değerlendirmek gerektiği; kişinin belirli olması, kişisel veri ile başka hiçbir işleme ya da yoruma gerek kalmaksızın kişinin kimliğinin ortaya çıkarılabiliyor olması iken, kişinin belirlenebilir olmasının veri ile kişinin ilişkilendirilmesi suretiyle kişinin tanımlanabilmesi olduğu;

Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamadığı; bilişim teknolojilerindeki gelişmeler sonucunda, geleneksel yöntemlerle ulaşılmaması mümkün olmayan çok sayıda verinin toplanabilmesi; daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması; verilere erişim ve veri transferinin kolaylaşması; kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde meydana gelen risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenlerin, günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kıldığı;

Bu bağlamda, Anayasa'nın 20. maddesinin üçüncü fıkrasının son cümlesinde, "Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilerek kişisel verilerin korunması hakkının anayasal güvenceye bağlandığı, bu verilerin kamu makamlarının keyfi müdahalelerine karşı koruma altına alındığı ve işlenmesi ancak kişinin açık rızası veya kanunda öngörülen hâllerde mümkün kılındığı;

Dava konusu Yönetmeliğin 30/B maddesinin 1. fıkrasının (a) bendi ile kişisel veri olan serbest tüketicilerin adı veya unvanının, PYS üzerinde tanımlanacak veri tabanına ekleneceği, piyasa işletmecisinin veri tabanına tedarikçilerin erişimini sağlayacağını düzenlendiği;

Anayasa'nın 20. maddesinin 3. fıkrasına aykırı olarak, dava konusu düzenlemeyle kişiyi belirlenebilir kılan kişisel veri niteliğinde olan serbest tüketicilerin adları veya unvanlarının tedarikçilerin erişimine açık olan veri tabanına eklenmesinde hukuka uygunluk bulunmadığı;

Yönetmeliğin dava konusu maddesinin birinci fıkrasında yer alan diğer kısımlarında talep edilen bilgilerin tüketim noktasına ilişkin veriler olduğu; bu verilerin, kişinin ad ve unvanı olmaksızın kişinin belirlenebilmesine yeterli olabilecek veriler olmadığı; dolayısıyla, kişisel veri olarak kabul edilemeyecek veriler olduğu, tüketiciler değişebilecekken tüketim noktalarına ilişkin verilerin sabit olduğu da dikkate alındığında, Yönetmeliğin 30/B maddesinin 1. fıkrasının diğer kısımlarında hukuka aykırılık bulunmadığı;

Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 2. fıkrası yönünden;

28/05/2016 tarih ve 29725 Sayılı Resmî Gazete'de Yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmeliğin 6. maddesi ile dava konusu "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 2. fıkrasında yer alan "Piyasa İşletmecisi ilgili veri tabanına tedarikçilerin erişimini sağlamakla yükümlüdür. Bu madde kapsamında edinilen bilgiler lisansta belirtilen faaliyetler dışında kullanılamaz ve ticarete konu edilemez." düzenlemesinin; "Tedarikçiler, tedarikçi değiştirme ve mali uzlaştırma süreçlerinde kullanılmak üzere tüketicilerine ilişkin, a) Serbest tüketicinin adı veya unvanı, b) Gerçek kişiler için T.C. kimlik numarası, tüzel kişiler için vergi kimlik numarası, bilgilerini PYS üzerinde tanımlanacak veri tabanına eklemek ve güncel tutmakla yükümlüdür. Piyasa İşletmecisi bu bilgileri veri tutarlılığının kontrolü amacı ile kullanır ve kişisel verilerin korunmasını sağlayacak önlemleri alır. Tedarikçilerin söz konusu yükümlülüklerini yerine getirmediklerinin tespiti halinde Kanununun 16 ncı maddesi uyarınca yaptırım uygulanır." şeklinde değiştirildiği ve davanın konusuz kaldığı anlaşıldığından, Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 2. fıkrası açısından uyumsuzluğun esası hakkında karar verilmesine gerek bulunmadığı;

Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin 3., 4. ve 5. fıkraları yönünden;

Dava konusu edilen Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinin "Serbest tüketici veri tabanı" başlıklı 30/B maddesinin 3. ve 4. fıkralarında Piyasa Yönetim Sisteminin (PYS) öngörülen şekilde çalışmasının sağlanmasına ilişkin birtakım düzenlemelere yer verildiği, bu düzenlemelerin, PYS'nin kullanımına ilişkin olduğu;

Yönetmeliğin 30/B maddesinin 5. fıkrasında ise, veri tabanına ilişkin yükümlülüklerin yerine getirilmemesi nedeniyle serbest tüketicinin yeni tedarikçisinin portföyüne geçişinin engellendiğinin tespiti hâlinde gerekli düzeltmelerin yapılacağı ve 6446 sayılı Kanun'a göre yaptırım uygulanacağını öngörüldüğü, Yönetmelik'te düzenlenen yükümlülüklerin yerine getirilmemesi hâlinde uygulanacak yaptırımlara ilişkin, Kanun hükmüne atıf yapıldığı; bu itibarla, Yönetmeliğin 30/B maddesinin 3., 4. ve 5. fıkrasında hukuka aykırılık bulunmadığı gerekçesiyle;

Dava konusu 28/03/2015 tarih ve 29309 sayılı Resmî Gazete'de yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına İlişkin Yönetmeliğin 22. maddesiyle, Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin birinci fıkrasının (a) bendinin iptaline, ikinci fıkrasının iptali istemi hakkında karar verilmesine yer olmadığına; maddenin diğer kısımları yönünden ise davanın reddine karar verilmiştir.

TEMYİZ EDENİN İDDİALARI: Davalı idare tarafından, iptal edilen düzenlemenin karar tarihinden önce yürürlükten kaldırılmış olması nedeniyle karar verilmesine yer olmadığına karar verilmesi gerektiği ileri sürülmektedir.

KARŞI TARAFIN SAVUNMASI: Davacı tarafından, savunma verilmemiştir.

DANIŞTAY TETKİK HÂKİMİ K1'NUN DÜŞÜNCESİ: Temyiz isteminin reddi ile Daire kararının temyize konu kısmının onanması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay İdari Dava Daireleri Kurulunca, Tetkik Hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereği görüldü:

HUKUKİ DEĞERLENDİRME:

Danıştay dava dairelerinin nihai kararlarının temyizen incelenerek bozulması, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 49. maddesinde yer alan;

"a) Görev ve yetki dışında bir işe bakılmış olması,

b) Hukuka aykırı karar verilmesi,

c) Usul hükümlerinin uygulanmasında kararı etkileyebilecek nitelikte hata veya eksikliklerin bulunması" sebeplerinden birinin varlığı hâlinde mümkündür.

Temyizen incelenen kararın dava konusu düzenlemenin iptaline ilişkin kısmı usul ve hukuka uygun olup, temyiz dilekçesinde ileri sürülen iddialar kararın temyize konu bu kısmının bozulmasını gerektirecek nitelikte görülmemiştir.

KARAR SONUCU:

Açıklanan nedenlerle;

1. Davalı idarenin temyiz isteminin reddine,
2. Yukarıda özetlenen gerekçeyle dava konusu düzenlemenin kısmen iptali, kısmen dava hakkında karar verilmesine yer olmadığı, kısmen davanın reddi yolunda verilen Danıştay Onüçüncü Dairesinin 30/04/2019 tarih ve E:2015/2767, K:2019/1431 sayılı kararının temyize konu iptale ilişkin kısmının ONANMASINA,
3. Kesin olarak, 19/11/2020 tarihinde oyçokluğu ile karar verildi.

KARŞIOY

X-Dava konusu Yönetmelik'in iptal edilen 30/B maddesinin birinci fıkrasının (a) bendi, 28/05/2016 tarih ve 29725 sayılı Resmî Gazete'de yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmeliğin 6. maddesi ile yürürlükten kaldırılmıştır.

Dava konusu edilen düzenlemenin yürürlükten kaldırılmış olması ve eski düzenlemeye dayalı olarak tesis edilmiş bir uygulama işleminin dava konusu edilmemiş olması karşısında davanın konusu kalmamıştır.

Açıklanan nedenle, temyize konu kısma ilişkin olarak Danıştay Onüçüncü Dairesince konusu kalmayan dava hakkında karar verilmesine yer olmadığına karar verilmesi gerektiği oyuyla, karara katılmıyoruz.

KARŞIOY

XX- Dava, 28/03/2015 tarih ve 29309 sayılı Resmî Gazete'de yayımlanan Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliğinde Değişiklik Yapılmasına İlişkin Yönetmeliğin 22. maddesiyle Elektrik Piyasası Dengeleme ve Uzlaştırma Yönetmeliği'ne eklenen "Serbest Tüketici Veri Tabanı" başlıklı 30/B maddesinin iptali istemiyle açılmıştır.

Temyize konu kararda, Anayasa'nın 20. maddesinin 3. fıkrasına aykırı olarak, dava konusu düzenlemeyle kişiyi belirlenebilir kılan kişisel veri niteliğinde olan serbest tüketicilerin adları veya unvanlarının tedarikçilerin erişimine açık olan veri tabanına eklenmesinde hukuka uygunluk bulunmadığı gerekçesiyle, uyuşmazlık konusu 30/B maddesinin birinci fıkrasının (a) bendinin iptaline karar verilmiştir.

07/04/2016 tarih ve 29677 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanun ile kişisel verilerin işlenmesinde uyulacak usul ve esaslar düzenlenmiş olduğundan, dava devam ederken yürürlüğe giren bu yasal düzenleme dikkate alınarak uyuşmazlığın çözüme kavuşturulması gerektiği oyuyla, Daire kararının temyize konu edilen iptale ilişkin kısmının onanmasına dair karara katılmıyorum.

Danıştay Kararı - İDDK., E. 2018/4437 K. 2020/788 T. 4.5.2020

İSTEMİN KONUSU: Danıştay Onbeşinci Dairesinin 21/03/2018 tarih ve E:2014/10178, K:2018/2789 sayılı kararının aleyhlerine olan kısımlarının temyizden incelenerek bozulması taraflarca karşılıklı olarak istenilmektedir.

YARGILAMA SÜRECİ:

Dava konusu istem:27/10/2014 tarih ve 29158 sayılı Resmî Gazete'de yayımlanan Geleneksel ve Tamamlayıcı Tıp Uygulamaları Yönetmeliği'nin ekleriyle birlikte tamamının iptali istenilmiştir.

Daire kararının özeti: Danıştay Onbeşinci Dairesinin 21/03/2018 tarih ve E:2014/10178, K:2018/2789sayılı kararıyla;

663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 8. maddesinin 1. fıkrasının (c) bendinde,"Kamu ve özel hukuk tüzel kişileri ile gerçek kişilere ait sağlık kurum ve kuruluşlarına izin vermek ve ruhsatlandırmak, bu izin ve ruhsatları gerektiğinde süreli veya süresiz iptal etmek.", (ğ) bendinde,"Geleneksel, tamamlayıcı ve alternatif tıp uygulamaları ile ilgili düzenleme yapmak ve sağlık beyanı ile yapılacak her türlü uygulamalara izin vermek ve denetlemek, düzenleme ve izinlere aykırı faaliyetleri ve tanıtımları durdurmak.", (o) bendinde, "İlgili kuruluşlarla işbirliği yaparak sağlık mesleklerinin standartlarını belirlemek, eğitim müfredatlarının kanıta dayalı olarak güncellenmesini ve geliştirilmesini sağlamak, sağlık meslek mensuplarının sertifikasyonu ile ilgili işleri yapmak veya yaptırmak."görevlerinin Sağlık Bakanlığı Sağlık Hizmetleri Genel Müdürlüğü'nün görevleri arasında sayıldığı ve aynı Kanun Hükmünde Kararname'nin 40. maddesinde de; Bakanlık ve bağlı kuruluşların görev, yetki ve sorumluluk alanına giren ve önceden kanunla düzenlenmiş konularda idarî düzenlemeler yapabilecekleri hükmüne yer verildiği,

1219 sayılı Kanun'un Ek 13. maddesinde, tabipler ve dış tabipleri dışındaki sağlık meslek mensuplarının, hastalıklarla ilgili doğrudan teşhiste bulunarak tedavi planlayamayacağı ve reçete yazamayacağı; tabiplerce veya tabiplerin yönlendirmesiyle ilgili sağlık meslek mensubu tarafından uygulanmak şartıyla insan sağlığına yönelik geleneksel/tamamlayıcı tedavi yöntemlerinin

alanlarının, tanımlarının, şartlarının ve uygulama usul ve esaslarının Sağlık Bakanlığınca çıkarılacak yönetmelikle düzenleneceği hükmünün yer aldığı,

Anılan Kanun hükmümlerine istinaden hazırlanan Geleneksel ve Tamamlayıcı Tıp Uygulamaları Yönetmeliği'nin 27/10/2014 tarih ve 29158 sayılı Resmi Gazete'de yayımlanarak yürürlüğe konulduğu,

Dava konusu Yönetmeliğin, 4. maddesinin 1. fıkrasında; Bakanlık, Bilim Komisyonu, Genel Müdürlük, Müdürlük, sağlık kuruluşu, sertifikalı tabip, sertifikalı diş tabibi, uygulama, uygulama merkezi ve ünite tanımlarının yapıldığı,

Yönetmeliğin 5. maddesinde;Yönetmelik'te öngörülen uygulamalar, uygulamaları yapacak kişiler, ünite ve uygulama merkezlerinin standartları ile ilgili görüş vermek üzere, Bakanlıkça Geleneksel ve Tamamlayıcı Tıp Uygulamaları Bilim Komisyonunun oluşturulacağı kuralına yer verildiği ve bilim komisyonunun kimlerden teşekkül edeceği, çalışma usulü ve görevlerinin ise Yönetmeliğin 6. ve 7. maddelerinde düzenlendiği,

Davacı tarafından, dava konusu düzenlemede bahsolunan uygulamaların tıp biliminin ışığı altında disipline edilebilmesi için bilimsel bir komisyonun oluşturularak ve söz konusu komisyonun görüşleri doğrultusunda işlemlerin yürütülmesi gerektiği, bu bağlamda, bilimsel bir kuruldan bahsedebilmek için belirli ölçütler üzerinden seçilen ve konu ile ilgili çalışması olan, özerk bir kurulun varlığından söz etmenin lazım geldiği, ancak, Yönetmelik'te yer alan komisyonun nitelik ve yeterlilik açısından bilimsel yapı ve özerkliğe sahip olmadığı ileri sürülerek düzenlemenin iptalinin istenildiği, davalı idare tarafından ise Bilimsel Komisyon üyelerinin, modern tıp içerisindeki her disiplinde özellikle akademik titri olan ve kendi alanında bilimsel çalışmalarda aktif olarak görev yapan öğretim üyelerinden seçildiği, ihtiyaç duyulan konularda çalışma yapmak üzere alt komisyonlar kurulmasının öngörüldüğü, dolayısıyla anılan komisyonun nitelik ve yeterlilik bakımından bilimsel vasfı haiz olduğunun savunulduğu,

Dava konusu Yönetmelik hükümleri bir bütün olarak değerlendirildiğinde, geleneksel ve tamamlayıcı tıp uygulamaları, bu uygulamaları yapacak kişiler, ünite ve uygulama merkezlerinin standartları ile ilgili görüş vermek üzere oluşturulan Geleneksel ve Tamamlayıcı Tıp Uygulamaları Bilim Komisyonunun, ilgili alanlarda bilimsel çalışması bulunan üniversite öğretim üyesi veya Türkiye Kamu Hastaneleri Kurumuna bağlı eğitim ve araştırma hastanelerinde uzmanlık eğitimi verme yetkisine sahip tabipler arasından seçilecek üç üye, eczacılık fakültelerinin farmakognozi alanından bir üye, tıp fakültelerinin farmakoloji alanından bir üye, sertifikalı iki tabip üye, öğretim üyesi veya eğitim görevlisi tıbbi onkoloji uzmanı bir üye, tıbbi etik veya tıp tarihi ve deontoloji alanlarında

uzmanlık veya doktora eğitimi almış bir üyeden teşekkül ettiği ve bu yönüyle bilimsel niteliği haiz olduğu anlaşıldığından, anılan düzenlemede hukuka aykırılık bulunmadığı,

Öte yandan davacı tarafından, mevzuat taslak çalışma ve toplantılarına Birlik ve tıpta uzmanlık derneklerinin çağrılmamasının hukuka aykırı olduğu, dava konusu düzenlemenin oluşturuluş yönteminin, tıp biliminin gerektirdiği çalışmalar yapılmadan hazırlanmış olması, temel hak ve özgürlükleri ihlal etmesi sebebiyle kamu yararı gerçekleştirmekten uzak olduğu, söz konusu Yönetmeliğin, hekimlik mesleğini, bilimsel tıbbın gelişimini, toplumun sağlık hakkını ve sağlık hizmetine erişim hakkını ciddi bir biçimde etkileyeceği, Anayasa'nın 135. maddesi uyarınca kamu kurumu niteliğinde meslek kuruluşu olan Birliğin mesleğin menfaatini ve toplumun yararını gözetme yükümlülüğü karşısında görüşünün alınmasının gerekli olduğu, idarenin düzenleme yaparken, Dünya Sağlık Örgütü'nün konu hakkında yayımladığı 2014-2023 stratejisini, Avrupa Birliği ülkelerinden 12 ülkeden 16 enstitünün yer aldığı "Cambrella Projesi" raporlarını, Amerikan Ulusal Sağlık Enstitüsü çalışmalarını dikkate aldığını belirttiği; ancak bahsolunan çalışmaların tamamlanmamış çalışmalar olduğu, başka ülkelerde konuyla ilgili mevzuatın bulunmasının bu uygulamaların bilimsel açıdan etkin ve güvenilir olduğunu göstermediği, geleneksel ve tamamlayıcı tıp yöntemlerinin etkilerinin ortaya konulmadığı, uygulamaların zararlı olup olmadığı hususunun bilinmediği, yeni uygulamaların bir bilimsel araştırma ürünü olması gerektiği, kanıta dayalı araştırma yapılması gerekirken dava konusu Yönetmelikte yer alan uygulamalar için böyle bir araştırmanın söz konusu olmadığı, dolayısıyla bilimsel süreçten geçmeyen uygulamaların insan bedeni üzerinde yapılmasının Türk Ceza Kanunu'na göre suç teşkil edeceği ileri sürülerek düzenlemenin iptalinin istenildiği,

Davalı idarenin savunmasından, dava konusu düzenleme öncesinde Dünya Sağlık Örgütü'nün bu konuda belirlediği hedefin benimsenerek Avrupa Birliği ülkelerindeki geleneksel, tamamlayıcı ve alternatif tıp uygulamalarının yasal durumunun incelendiği, Yönetmelik taslağının internet ortamında paylaşılarak toplumun tüm sağlık paydaşlarının ve ilgililerin görüş ve önerilerine açıldığı, meslek kuruluşlarına da görüş bildirme imkanı tanındığı ve gelen geri bildirimlerin ve cevapların, belirli uluslararası kuruluşlar ve Yükseköğretim Kuruluna bağlı üniversite rektörleri, tıp fakültesi ve eczacılık fakültesi dekanları, kamuya bağlı taşra sağlık kuruluşları yöneticileri, Avrupa ve Asya'da bu konu ile ilgili hekimler tarafından değerlendirilmesi sonucunda düzenlemenin tamamlandığı, Türkiye'de geleneksel ve tamamlayıcı tıp uygulamalarının yaygınlık ve kullanım oranlarını ölçüm amaçlı olarak 7 bölge ve 14 şehirde, Hacettepe Üniversitesi Etik Kurulunun onayı ile yaptırılan anket çalışmasının sonuçlarına göre geleneksel ve tamamlayıcı tıp uygulamalarının genel kullanım

oranının %60 olduđu, bu kullanım oranları içerisinde uygulayıcıların %79,5'lik kısmının sağlık çalışanı olmadığı ve uygulamaların %75,9'unun ev ortamında yapıldığının tespit edildiđi, bu sonuçların, ehil olmayan kişiler tarafından denetimsiz bir şekilde yapılan uygulamaların önüne geçilip ivedilikle hukukî düzenlemelerin yapılması gerekliliđini ortaya koyduđu, dolayısıyla Yönetmeliđin kötü uygulamaları ve suiistimali önlemeye yönelik olduđu ve hazırlanmasında kamu yararının ön plana alındığı, uzman olmayan kişilerce ilaç tanıtımı yapıldığı ve çeşitli şekillerde satışların gerçekleştirildiđi, halk sağlığının ciddi bir risk ve tehlike altında olduđu, modern tıbbın dışındaki yöntemler olarak tarif edilebilecek tıp uygulamalarının yapılmasına olanak tanınırken her türlü bilimsel çalışma ve kanıta dayalıliđın göz önünde bulundurulduđu, Yönetmelik çalışmaları dahilinde mevcut bilimsel veri tabanlarından uygulama dalları ile ilgili bilimsel literatür taraması yapıldığı, Yönetmelik'te yayımlanmış veya yayımlanması gerektiđi düşünölen tüm uygulamaların bilimin süzgecinden geçirildikten sonra Bakanlıkça deđerlendirilebileceđi, 6519 sayılı Türkiye Sağlık Enstitöleri Başkanlığı Kurulması ve Bazı Kanun ve Kanun Hükmünde Kararnamelerde Deđişiklik Yapılmasına Dair Kanun'da yer alan 6 enstitüden bir tanesinin de Geleneksel ve Tamamlayıcı Tıp Uygulamaları Enstitüsü olduđu, bilimsel çalışmaların bu Enstitü, eğitim ve araştırma hastaneleri ve üniversiteler tarafından yürütöldüđü, geleneksel ve tamamlayıcı tıp uygulamalarının temel vasfının 'tamamlayıcı' olduđu, insan üzerinde deney çalışması olarak nitelendirilemeyeceđi, uygulamaların insan hayatının ve sağlığının korunmasını güvence altına alan üst hukuk normlarının tamamına bađlı kalmak ve bu normlara uygun olmak kaydıyla uygulandıđı, modern tıbbın yerine deđil onu destekleyici olarak kullanıldıđı anlaşıldığından dava konusu düzenlemede bu yönüyle hukuka aykırılık bulunmadığı,

Yönetmeliđin 8. maddesinde, Yönetmelik kapsamındaki uygulamalarla ilgili bir takım genel esasların belirlendiđi, bahse konu düzenlemenin incelenmesinden; uygulamaların, bu Yönetmelik'te belirlenen alanlarla sınırlı olduđu, Bilim Komisyonunun uygulamaların bilimsel kanıtlarını inceleyerek kişilere uygulanıp uygulanmayacağı ve uygun görölenlerden hangilerinin ünite veya uygulama merkezinde uygulanabileceđi hususunda Bakanlığa görüş vereceđi, Yönetmelik ekinde bulunmayan uygulamalara yönelik araştırmaların, 13/04/2013 tarih ve 28617 sayılı Resmî Gazete'de yayımlanan İlaç ve Biyolojik Ürünlerin Klinik Araştırmaları Hakkında Yönetmelik hükümlerine tabi olduđu, uygulamaların, hastalığın standart tedavisinin yerine geçecek ve devam eden tedaviyi aksatacak şekilde yapılamayacağı ve bu hususun bireylere açık bir şekilde anlatılacağı ve onaylanmış rıza formunda belirtileceđi, tabip ve dış tabibi olmayan uygulama alanında temel eğitimi bulunan sağlık meslek mensuplarının ise, sertifikalı tabip ve dış tabiplerinin gözetimi ve denetimi altında

uygulamalara katılacağı hususunun açıkça hüküm altına alındığı anlaşıldığından, anılan hükümde kamu yararı ve hukuka aykırılık görülmediği,

Yönetmeliğin 9. maddesinde, uygulamaların, Bakanlıkça yetkilendirilmiş ünite ile uygulama merkezlerinde ve ilgili alanda “uygulama sertifikası” bulunan tabip ve sadece diş hekimliği alanında olmak üzere diş tabibi tarafından yapılabileceği, uygulama alanında temel eğitimi bulunan sağlık meslek mensuplarının da merkez ve ünitelerde sertifikalı tabiplere uygulamada yardımcı olabileceği, diş hekimliği uygulama ve araştırma merkezlerinde, diş hastanelerinde ve ağız ve diş sağlığı merkezleri ile diş polikliniklerinde sadece diş hekimliği alanında uygulama yapılabileceğinin hüküm altına alındığı,

1219 sayılı Kanun’un Ek 13. maddesinde, tabipler ve diş tabipleri dışındaki sağlık meslek mensuplarının, hastalıklarla ilgili doğrudan teşhiste bulunarak tedavi planlayamayacağı ve reçete yazamayacağı kuralının yer aldığı, buna göre, sağlık meslek mensuplarının, geleneksel ve tamamlayıcı tıp uygulamaları alanında eğitim almak ve sertifikalarını onaylatmak şartıyla hekim yönlendirmesi ve onlarla birlikte bu uygulamaları yapmaları mümkün olabileceğinden dava konusu düzenlemede bu yönüyle hukuka aykırılık bulunmadığı,

Yönetmeliğin 10. maddesinde; uygulama merkezi ve ünitelerin çalışma usul ve esaslarına ilişkin kuralların düzenlendiği, maddenin 2. fıkrasında, Kültür ve Turizm Bakanlığında belgeli konaklama tesislerinde, tesiste konaklayan ve sadece akut tedavisi tamamlanmış kişilere uygulanmak kaydıyla Bakanlıkça uygun görülen uygulamalara yönelik birimin, planlama kapsamında kurulabileceği kuralına yer verildiği,

Davacı tarafından, ilgili mevzuatın yalnız hekimlere tanıdığı özel sağlık kuruluşu açma hakkının, turistik amaçlı kurulmuş konaklama tesislerine de tanındığı, hekim olmayan kişilerin ayakta teşhis ve tedavi hizmeti vermek üzere yetkilendirilmesinin 1219 sayılı Kanun'a ve Anayasa'ya aykırı olduğu iddia edilerek düzenlemenin iptali istenildiği,

Davalı idarenin savunmasından, anılan hükme göre sağlık kuruluşlarının kendi kadro ve kapasitelerini kullanarak konaklama tesislerinde ünite açabileceği ve sadece üniteye yapılabilecek uygulamaları yapacağı, bu uygulamanın amacının, mevcut durumda zaten fiilen var olan bir durumu hukukî düzenlemeye kavuşturarak disipline etmek böylece halk sağlığını korumak ve suistimallerin önüne geçilmesini temin ederek bu alanda da denetim sağlamak olduğunun anlaşıldığı, bu bağlamda, konaklama tesislerinde akut tedavisi tamamlanmış hastalara yönelik olarak yapılacak geleneksel ve tamamlayıcı tıp uygulamalarının, tıp biliminin ışığı altında disiplin altına alınmış olarak Yönetmelik'tebelirlenen çalışma usul ve esasları çerçevesinde yürütüleceğinin muhakkak olduğu,

Buna göre, sađlık kurum ve kuruluřlarının lke genelinde eřit, kaliteli ve verimli hizmet sunacak Őekilde planlanmasını koordine etmekle ve kamu ve zel btn sađlık kurum ve kuruluřlarının kurulması ve iřletilmesinde kaynak israfı ve atıl kapasiteye yol aılmaksızın kaliteli hizmet arzı ve verimliliđini esas almakla ykml davalı idare tarafından, sađlık turizmi kapsamında yurt dıřından veya yurt iinden gelerek konaklama tesislerinde konaklayan akut tedavisi tamamlanmıř kiřilere ynelik olarak geleneksel ve tamamlayıcı tıp uygulamalarının yapıldığı birim kurulmasına izin verilmesine ynelik dzenlemede, kamu yararı ve hizmet gereklerine, dayanađı mevzuat hkmlerine aykırılık bulunmadığı,

Anılan maddenin 3. fıkrasında,hastaya ve uygulamalara iliřkin verilerin elektronik ortamda talep edilmesi halinde, kiřisel sađlık verilerinin mahremiyeti gzetilerek, Bakanlıđa gnderilmesinin zorunlu olduđu kuralının yer aldıđı, Anayasa'nın 20. maddesinin nc fıkrasının son cmlesinde, "Kiřisel verilerin korunmasına iliřkin esas ve usuller kanunla dzenlenir."hkmne yer verilerek kiřisel verilerin korunması hakkı anayasal gvenceye bađlandıđı ve bu Őekilde kamu makamlarının keyfi mdahalelerine karřı koruma altına alındığı,

Davacı tarafından, kiřisel verilerin iřleyiři ile ilgili olarak, usul ve esasların kanunla belirlenmesinin anayasal bir zorunluluk olduđu, dava konusu Ynetmeliđin dayanađı olan 663 sayılı Kanun Hkmnde Kararname'nin 47. maddesinin birinci, ikinci ve nc fıkralarının, Anayasa Mahkemesi'nin 04/12/2014 tarih ve E:2013/114, K:2014/184 sayılı kararı ile iptal edildiđi, bylece dava konusu Ynetmelik hkmnn dayanađının ortadan kalktığı, Bakanlıđın kiřinin yazılı onayı olmaksızın kiřisel verileri ve sađlık kayıtlarını toplama yetkisinin bulunmadığı, dzenlemenin st hukuk normlarına aykırı olduđu ileri srlerek iptalinin istenildiđi,

Anayasa'nın 20. maddesine 5982 sayılı Kanun'un 2. maddesi ile eklenen fıkrada, "Herkes, kendisiyle ilgili kiřisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kiřinin kendisiyle ilgili kiřisel veriler hakkında bilgilendirilme, bu verilere eriřme, bunların dzeltilmesini veya silinmesini talep etme ve amaları dođrultusunda kullanılıp kullanılmadıđını đrenmeyi de kapsar. Kiřisel veriler, ancak kanunda ngrlen hallerde veya kiřinin aık rızasıyla iřlenebilir. Kiřisel verilerin korunmasına iliřkin esas ve usuller kanunla dzenlenir." hkmne yer verildiđi,

Anayasa'nın bu hkmnde kiřisel verilerin korunmasını isteme hakkının neleri kapsadıđı hususunun zellikle vurgulanmıř olması karřısında, hassas veri kabul edilen kiřisel sađlık verilerinin toplanması ve iřlenmesinin kapsamı, kořulları ve bu verilerin korunmasına iliřkin usul ve esasları iermeyen yasal dzenlemelerin, Anayasa'nın 20. maddesinde ngrlen kiřisel verilerin korunmasına iliřkin

usul ve esasların ancak kanunla düzenlenebileceğine ilişkin güvenceyi sağlamaktan uzak olduğu sonucuna ulaşıldığı,

Bu kapsamda, dava konusu Yönetmelik kuralının dayanağı olan 663 sayılı Kanun Hükmünde Kararname'nin 47. maddesinin 1. ve 3. fıkralarının Anayasa Mahkemesi'nin 14/02/2013 tarih ve E:2011/150, K:2013/30 sayılı kararı ile iptal edilmesinin ardından 02/08/2013 tarih ve 28726 sayılı Resmî Gazete'de yayımlanan 6495 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un 73. maddesinin (h) bendinin üçüncü alt bendi ile 663 sayılı Kanun Hükmünde Kararname'nin Anayasa Mahkemesince iptal edilen hükümlerinin yeniden düzenlendiği, bu kez de anılan hükmün Anayasa Mahkemesi'nin 04/12/2014 tarih ve E:2013/114, K:2014/184 sayılı kararıyla dava konusu kuralla sadece demokratik toplum düzeni yönünden zorunlu olan sınırlamalar değil, özel hayatın ve kişisel verilerin korunması haklarına yapılabilecek her türlü sınırlamaya izin verilmesi, bir başka ifade ile kuralda anılan haklara sınırlama getirilirken sınırlama aracının sınırlama amacına uygun ve orantılı olarak kullanılmasını temin edecek güvenceleere yer verilmemesinin ölçülülük ilkelerine aykırı düştüğü gerekçesiyle iptal edildiği,

Son durumda ise, 07/04/2016 tarih ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30. maddesi ile 663 sayılı Kanun Hükmünde Kararname'nin 47. maddesinin yeniden düzenlendiği,

Bununla birlikte anılan Kanun'un 30. maddesi ile 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 3. maddesinin (f) bendinin de, "Herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi maksadıyla, Sağlık Bakanlığı ve bağlı kuruluşlarınca gerekli kayıt ve bildirim sistemi kurulur. Bu sistem, e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabilir. Bu amaçla, Sağlık Bakanlığınca, bağlı kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemi kurulabilir." şeklinde değiştirildiği,

Her ne kadar 663 sayılı Kanun Hükmünde Kararname'nin 47. maddesi ve 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 3. maddesinin (f) bendi yeniden düzenlemiş ise de sonradan yürürlüğe giren yasal düzenlemelerin önceden yürürlüğe giren Yönetmeliğin dayanağı olamayacağını açık olduğu, bu durumda yasal dayanaktan yoksun hale gelen davakonusu düzenlemede hukuka uyarlık bulunmadığı,

Yönetmeliğin 13. maddesinde, Yönetmelik kapsamındaki sertifikalı eğitimlerin, 04/02/2014 tarih ve 28903 sayılı Resmî Gazete'de yayımlanan Sağlık Bakanlığı Sertifikalı Eğitim Yönetmeliği kapsamında, Bakanlıkça eğitim vermek üzere yetkilendirilmiş merkezler tarafından verileceğinin düzenlendiği,

Sağlık Bakanlığınca tescil edilecek sertifikalara ilişkin usul ve esasları düzenlemek amacıyla hazırlanan Sağlık Bakanlığı Sertifikalı Eğitim Yönetmeliği'nin 5. maddesine göre, her bir eğitim alanı için kurulan bilimsel komisyona, sertifikalı eğitimin süresi, müfredatı, merkezin niteliği, program sorumlusunu, eğitici ve programa katılacak katılımcıların niteliklerini, eğitim materyallerini, eğitim sonunda uygulanacak sınavların usul ve esaslarını, sertifikanın geçerlilik süresi ve yenilenmesi ile eğitim programının denetim usul ve esaslarına ilişkin standartları belirleme yetkisinin verildiği, maddenin devamında ise belirlenen standartların Bakanlığın internet sayfasında yayımlanacağını düzenlendiği,

Diğer taraftan, 663 sayılı Kanun Hükmünde Kararname'nin 22. maddesinde, tıpta uzmanlık eğitimi ve uzman insan gücü ile ilgili görüşler vermek hususunda Tıpta Uzmanlık Kurulunun yetkili kılındığı, 26/04/2014 tarih ve 28983 sayılı Resmî Gazete'de yayımlanan Tıpta ve Dış Hekimliğinde Uzmanlık Eğitimi Yönetmeliği'nin 5. maddesinin 1. fıkrasının (j) bendine göre, sertifikaları Bakanlıkça tescil edilecek olan ve uzmanlara yönelik olan sertifikalı eğitim programları ile ilgili olarak verilecek görüşün Kurulun görevleri arasında yer aldığı,

Davacı tarafından, söz konusu düzenlemede, Yönetmelik ekinde sayılan işlemler için sertifika alınması zorunlu kılınmışken Tıpta Uzmanlık Kurulunun görüşüne başvurulmadığı, uygulamaların sertifikalı hekim tarafından yapılacağı belirtilmekle beraber hekimlerin uzman hekim mi yoksa pratisyen hekim mi olduğu hususunun belirlenmediği, uzmanlık ayrımlarına gidilmediği, eğitim sürelerinin açıkça belirlenmediği, hastalık tanısının ne zaman kim tarafından konulacağını, hastanın ne zaman ve kim tarafından bu uygulamalara yönlendirileceğinin açık ve net olarak gösterilmediği, bu yönüyle düzenlemenin üst hukuk normlarına, usule ve hukuka aykırı olduğu, hekimler yönünden ise, uzmanlık eğitimi sırasında edindikleri bilgi, beceri ve deneyimin yeterli sayılmayarak sertifika alınmaya zorlandığı, uzmanlık gerektiren işlerin de uzman olmayan hekimlerce yapılmasına olanak tanındığı, bu yönüyle düzenlemenin hukuka aykırı olduğunun iddia edildiği,

Dosyanın incelenmesinden ve davalı idarenin savunmasından; Tıpta Uzmanlık Kurulunca yayımlanan tıpta ve dış hekimliğinde uzmanlık çekirdek eğitim müfredatlarının incelendiği, geleneksel ve tamamlayıcı tıp uygulamaları kapsamındaki sertifikalı eğitim programlarının, klasik tıp ve tıpta uzmanlık eğitimiyle ilgisi olmayan tamamlayıcı ve destekleyici nitelikte uygulamalara ilişkin olduğu, eğitim ve uygulama için tabip olmanın gerekli ve yeterli şart olduğu, dolayısıyla ortada münhasıran "uzman hekimlere" yönelik olarak düzenlenmesi plânlanan veya Tıpta ve Dış Hekimliğinde Uzmanlık Eğitimi Yönetmeliği kapsamında uzman hekimlik temelinde yükselmesi gereken bir eğitim mevcut olmadığından Tıpta Uzmanlık Kurulundan görüş alınmasını zorunlu kılan

bir durumun bulunmadığı, dava konusu Yönetmeliğin Ek-3 numaralı ekinde yapılabilecek uygulamaların tanımı, uygulama yapmaya yetkili personel, uygulanabileceği durumların, ünite ve uygulama merkezi ayrımı ile sıralı sayı ile belirlendiği, uygulama yapılamayacak durumların da yine sayma metodu ile belirlendiği, böylece yanlış uygulamaların, istismarın ve sömürünün önüne geçilmek istendiği ve uygulamaların eğitimli tabip ve alanları ile ilgili dış tabipleri tarafından uygulanacağını ortaya koyulduğu, uygulamaların, daha önce belli bir hastalık için tanı almış ve modern tıp ile tedavi olan hastalara, hastayı takip eden doktorunun bilgisi dâhilinde yapılabildiği, anılan uygulamaların, hekimlere uyguladıkları tedavileri çeşitlendirme ve hastayı daha kısa sürede ve daha etkin olarak tedavi etmeye yardımcı olan uygulamalar olduğu, konvansiyonel tıbbın yerine ikame edilmeye çalışılmadığı, söz konusu düzenleme ile uluslararası standartlara uygun, asıl işi eğitim ve araştırma olan sağlık kurumlarında hekim ve hekim gözetiminde sağlık meslek mensubuna uygulama yetkisi verilmek istendiği, anılan Yönetmeliğin 1219 sayılı Kanun'un Ek-13. maddesinin amir hükmü gereği hazırlandığı anlaşıldığından, dava konusu düzenlemede, üst hukuk normlarına ve hukuka aykırılık bulunmadığı gerekçesiyle,

27/10/2014 tarih ve 29158 sayılı Resmî Gazete'de yayımlanan Geleneksel ve Tamamlayıcı Tıp Uygulamaları Yönetmeliği'nin 10. maddesinin 3. fıkrasının 2. cümlesinin iptaline, diğer maddeler bakımından ise davanın reddine karar verilmiştir.

TEMYİZ EDENLERİN İDDİALARI:

Davacı tarafından, dava konusu Yönetmeliğin tıp biliminin gerektirdiği çalışmalar yapılmadan hazırlandığı, hazırlık aşamasında geleneksel ve alternatif tıp alanında başka ülke ve kuruluşların uygulama ve çalışmalarının incelenmiş olmasının düzenlemeye bilimsel bir nitelik kazandırmayacağı, söz konusu çalışmaların henüz tamamlanmamış çalışmalar olduğu, taslak çalışmalarına Birlik ve tıpta uzmanlık derneklerinin çağrılmamış olmasının hukuka aykırı olduğu, uygulamaların etkilerinin ortaya konulmadığı, bilimsel bir süreçten hazırlanan düzenlemelerin kamu yararına ve hukuka aykırı olduğu, Yönetmelik kapsamındaki kimi alanların Tıpta Uzmanlık Eğitimi çekirdek eğitim müfredatı içinde yer aldığı, bu nedenle dava konusu düzenlemenin hazırlanması sürecinde Tıpta Uzmanlık Kurulunun görüşünün alınmamış olmasının hukuka aykırı olduğu, tıpta uzmanlık eğitimi ile edinilen bilgi, beceri ve deneyimin, sertifikalı eğitim yolu ile kişilere kazandırılmak istendiği, Yönetmelik'te eğitim standartları, eğitici ve eğitim kurumlarının özelliklerine ilişkin hususların düzenlenmediği, hastaların hangi koşullarda geleneksel ve tamamlayıcı tıp uygulamalarına yönlendirileceğinin belirsiz olduğu, Ek-3'te yer alan uygulamaların bilimselliğinin kanıtlanmadığı, uygulama alanlarının istismara açık olduğu ve bu konuda davalı

idarece etkin bir denetim mekanizmasının oluşturulmadığı, Bilim Komisyonunda görevli hekimlerin uygulamaların tamamı hakkında bilgi sahibi olmalarının mümkün olmadığı, Ek-3'te sayılan uygulamaların endikasyonlarının birden fazla uzmanlık alanının çalışma konusuna girdiği, Bilim Komisyonunda meslek kuruluşları ve tıpta uzmanlık derneklerinden temsilcilerin katılımının sağlanmamasının eksiklik olduğu, oluşturulan alt komisyonlarda hekim olmayan kişilerin de yer aldığı, bu durumun komisyonun bilimsel bir özellik taşımadığının göstergesi olduğu, kanunen yalnızca hekimlere ait olan sağlık kuruluşu açma hakkının Yönetmelik ile konaklama tesislerine de verildiği, hekim olmayan gerçek ve tüzel kişilerin ayakta teşhis ve tedavi hizmeti vermek üzere yetkilendirilmesinin açıkça hukuka aykırı olduğu, 5510 sayılı Kanun'un 64. maddesinde geleneksel, tamamlayıcı ve alternatif tıp uygulamalarına ilişkin finansmanların Sosyal Güvenlik Kurumu tarafından karşılanmayacağına açıkça belirtildiği, söz konusu uygulamaların hastalıkların tedavisinde etkili ve yararlı olduğu kanıtlanmış ise Kurumca finanse edilmesi gerektiği, ancak söz konusu uygulamaların ücretlerinin vatandaşlar tarafından karşılandığı ve bunun da sağlık hizmetine erişimi engellediği ileri sürülmektedir.

Davalı idare tarafından, 07/04/2016 tarih ve 29677 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30. maddesi ile 663 sayılı Kanun Hükmünde Kararname'nin 47. maddesinin yeniden düzenlendiği, dava devam ederken yürürlüğe giren ve dava konusu Yönetmeliğin 10. maddesinin 3. fıkrasının dayanağını oluşturan bu yasal düzenleme dikkate alınarak uyuşmazlığın çözüme kavuşturulması gerektiği belirtilerek, Daire kararının anılan düzenlemenin iptali yolundaki kısmının bozulması gerektiği ileri sürülmektedir.

KARŞI TARAFIN SAVUNMALARI:

Davacı tarafından, Danıştay Onbeşinci Dairesince verilen kararın iptale yönelik kısmının usul ve hukuka uygun bulunduğu ve davalı tarafın temyiz dilekçesinde öne sürülen nedenlerin, kararın bu kısmının bozulmasını gerektirecek nitelikte olmadığı belirtilerek temyiz isteminin reddi gerektiği savunulmaktadır.

Davalı idare tarafından, Danıştay Onbeşinci Dairesince verilen kararın davanın reddine ilişkin kısmının usul ve hukuka uygun bulunduğu ve davacı tarafın temyiz dilekçesinde öne sürülen nedenlerin, kararın bu kısmının bozulmasını gerektirecek nitelikte olmadığı belirtilerek temyiz isteminin reddi gerektiği savunulmaktadır.

DANIŞTAY TETKİK HÂKİMİ K1'NİN DÜŞÜNCESİ: Temyiz istemlerinin reddi ile Daire kararının onanması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay İdari Dava Daireleri Kurulunca, Tetkik Hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereği görüldü:

HUKUKİ DEĞERLENDİRME:

Dava, 27/10/2014 tarih ve 29158 sayılı Resmî Gazete'de yayımlanan Geleneksel ve Tamamlayıcı Tıp Uygulamaları Yönetmeliği'nin ekleriyle birlikte tamamının iptali istemiyle açılmış olmakla birlikte, Kurulumuzca temyiz incelemesi, tarafların temyiz dilekçelerinde ileri sürülen iddialarla sınırlı olarak yapılmıştır.

Danıştay dava dairelerinin nihai kararlarının temyizen incelenerek bozulması, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 49. maddesinde yer alan;

"a) Görev ve yetki dışında bir işe bakılmış olması,

b) Hukuka aykırı karar verilmesi,

c)Usul hükümlerinin uygulanmasında kararı etkileyebilecek nitelikte hata veya eksikliklerin bulunması" sebeplerinden birinin varlığı hâlinde mümkündür.

Temyizen incelenen karar usul ve hukuka uygun olup, temyiz dilekçelerinde ileri sürülen iddialar kararın bozulmasını gerektirecek nitelikte görülmemiştir.

Diğer yandan, davacı tarafından 5510 sayılı Kanun'un 64. maddesi uyarınca geleneksel, tamamlayıcı, alternatif tıp uygulamalarının finansmanının Sosyal Güvenlik Kurumu tarafından karşılanmadığı, söz konusu uygulama ücretlerinin uygulamadan yararlanan vatandaşlarca karşılandığı, bunun ise sağlık hizmetine erişim hakkını engellediği ileri sürülmüş ve dava dilekçesinde bu yöndeki iddialar ile Yönetmeliğin 11. maddesi ile Ek-3. bölümünün iptalinin istenilmesine rağmen Daire tarafından bu iddialar değerlendirilmeden esas hakkında karar verildiği, eksik değerlendirme ve gerekçeyle verilen Daire kararının bu nedenle bozulması gerektiği ileri sürülmekte ise de; anılan uygulamaların finansmanının sağlanması hususunun davalı idarenin görev ve yetkisi dışında kaldığı, konunun sosyal güvenlik sisteminin finansal kapasitesi ile ilgili olduğu ve geri ödeme sistemine ilişkin bu uygulamanın yasal bir düzenleme ile kurala bağlandığı anlaşıldığından, Daire kararının bu kısma yönelik davacı iddiaları, bozma sebebi olarak görülmemiştir.

Ayrıca, davalı idare tarafından 07/04/2016 tarih ve 29677 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30. maddesi ile 663 sayılı Kanun Hükmünde Kararname'nin 47. maddesinin yeniden düzenlendiği, dava devam ederken yürürlüğe

giren ve dava konusu Yönetmeliğin 10. maddesinin 3. fıkrasının dayanağını oluşturan bu yasal düzenleme dikkate alınarak uyuşmazlığın çözüme kavuşturulması gerekirken, anılan düzenlemenin iptali yolunda verilen Daire kararının bozulması gerektiği ileri sürülmekte ise de, sonradan yapılan kanun değişikliğine istinaden davalı idarece her zaman konuya ilişkin düzenleme yapılması mümkün olduğundan, davalı tarafın bu kısma ilişkin temyiz iddialarına itibar edilmemiştir.

KARAR SONUCU:

Açıklanan nedenlerle;

1. Tarafların temyiz istemlerinin reddine,
2. Yukarıda özetlenen gerekçeyle kısmen davanın reddi, kısmen dava konusu düzenlemenin iptali yolundaki Danıştay Onbeşinci Dairesinin temyize konu 21/03/2018 tarih ve E:2014/10178, K:2018/2789 sayılı kararının ONANMASINA,
3. Kesin olarak, 04/05/2020 tarihinde oybirliği ile karar verildi.

Danıştay Kararı - İDDK (E. 2014/2242)

Danıştay Kararı - İDDK, E. 2014/2242 K. 2015/4991 T. 9.12.2015

T.C. DANIŞTAY İDARİ DAVA DAİRELERİ KURULU

Esas No: 2014/2242

Karar No: 2015/4991

Temyiz Eden (Davacı):

Vekili:

Karşı Taraf (Davacı):

Vekili:

İstemin Özeti: Konya 1. İdare Mahkemesinin 13/03/2014 günlü, E:2014/224, K:2014/256 sayılı ısrar kararının temyizen incelenerek bozulması, davacı tarafından istenilmektedir.

Savunmanın Özeti: Temyiz isteminin reddedilmesi gerektiği savunulmaktadır.

Danıştay Tetkik Hakimi:

Düşüncesi: Temyiz isteminin kabulü ile ısrar kararının Danıştay Beşinci Daire kararı doğrultusunda bozulması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Hüküm veren Danıştay İdari Dava Daireleri Kurulunca dosya incelendi, gereği görüşüldü:

Dava; davacı Sendika tarafından, Konya Eğitim ve Araştırma Hastanesinde parmak izi sistemiyle yürütülen mesai takibi uygulamasının sonlandırılması istemiyle 06/02/2012 tarihli dilekçe ile yapılan başvurunun reddine ilişkin 22/02/2012 günlü, 3259 sayılı Konya Eğitim ve Araştırma Hastanesi Başhekimliği işleminin iptali istemiyle açılmıştır.

Konya 1. İdare Mahkemesince; çalışma saatlerine uyma mecburiyeti bulunduğu tartışmasız olan kamu görevlilerinin mesaiye riayet edip etmediklerini izlemekle yükümlü olan davalı idarece, daha önce denenip verim alınamayan kart okutma yönteminden vazgeçilerek öteden beri uygulanmakta olan imza sistemiyle birlikte, kurum çalışanlarının mesaiye devamlarının takibi için en uygun ve elverişli yöntem olarak belirlenen ve bu sistemi seçme hususunda personele herhangi bir zorunluluk

da getirilmeyen parmak tarama yöntemiyle mesai takibine geçilmesinde hukuka ve mevzuata aykırılık bulunmadığı gerekçesiyle, davanın reddine karar verilmiştir.

Anılan karar, Danıştay Beşinci Dairesinin 10/12/2013 günlü, E:2013/5342, K:2013/9525 sayılı kararıyla; personelden kişisel veri alınması kapsamında olan "parmak izi tarama sistemi" ile mesai takibi uygulamasının, kamusal alanda da olsa "özel hayatın gizliliği" ilkesi kapsamında bulunduğu anlaşılması karşısında; uygulamanın sınırlarını usul ve esaslarını gösteren bir yasal dayanağının bulunmaması, toplanan verilerin ileride başka bir şekilde kullanılmayacağına dair bir güvencenin mevcut olmaması gözönüne alındığında, temel haklar ve Anayasal ilkelerle bağdaşmayan dava konusu işlemlerde hukuka aykırılık bulunmadığı gerekçesiyle bozulmuş ise de; İdare Mahkemesi, bozma kararına uymayarak, davanın reddi yolundaki ilk kararında ısrar etmiştir.

Davacı, Konya 1. İdare Mahkemesinin 13/03/2014 günlü, E:2014/224, K:2014/256 sayılı ısrar kararını temyiz etmekte ve bozulmasını istemektedir.

Dosyanın incelenmesinden, Konya Eğitim ve Araştırma Hastanesi'nde sadece imza yöntemiyle mesai takibi yapılmakta iken, önce kart okutma yöntemiyle mesai takibi yapılmasının denendiği, ancak bu yöntemlerin uygulanmasında güçlük yaşanması üzerine, imza yöntemiyle birlikte parmak tarama yönteminin uygulanmasına başlandığı, davacı Sendika tarafından bu yöntemin sonuçlandırılması konusunda yapılan başvurunun reddedilmesi üzerine bakılmakta olan davanın açıldığı anlaşılmaktadır.

Anayasa'nın 2. maddesinde belirtilen hukuk devleti; insan haklarına dayanan, bu hak ve özgürlükleri koruyup güçlendiren, eylem ve işlemleri hukuka uygun olan, her alanda adaletli bir hukuk düzeni kurup bunu geliştirerek sürdüren, Anayasa'ya aykırı durum ve tutumlardan kaçınan, hukuku tüm devlet organlarına egemen kılan, Anayasa ve yasalarla kendini bağlı sayan, yargı denetimine açık olan devlettir.

Anayasanın "Temel hak ve hürriyetlerin niteliği" başlıklı 12. maddesinde; "Herkes, kişiliğine bağlı, dokunulmaz, devredilemez, vazgeçilmez temel hak ve hürriyetlere sahiptir.

Temel hak ve hürriyetler, kişinin topluma, ailesine ve diğer kişilere karşı ödev ve sorumluluklarının da ihtiva eder." hükmüne yer verilmiş, "Temel hak ve hürriyetlerin sınırlanması" başlıklı değişik 13. maddesinde; temel hak ve hürriyetlerin, özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak yasayla sınırlanabileceği, bu sınırlamaların, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olmayacağı belirtilmiştir.

Anayasa'nın "Özel hayatın gizliliği" başlıklı değişik 20. maddesinde ise, "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.

....

Herkes, kendisiyle ilgili kişisel verilerin korunmasının isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." denilmek suretiyle, kişisel verilerin korunması, özel hayatın gizliliğinin korunması kapsamında güvenceye bağlanmıştır.

Öte yandan, Avrupa İnsan Hakları Sözleşmesinin "Özel Hayatın ve Aile Hayatının Korunması" başlıklı 8. maddesinde, herkesin özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahip olduğu, bu hakkın kullanılmasına bir kamu makamının müdahalesinin, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabileceği kurala bağlanmış; Birleşmiş Milletler Medeni ve Siyasal Haklar Sözleşmesinin "Mahremiyet Hakkı" başlıklı 17. maddesinde de, hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemeyeceği; onuru veya itibarının hukuka aykırı saldırılara maruz bırakılmayacağı, herkesin bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahip olduğu belirtilmiştir.

Kişisel verilerin korunması hakkı, kişinin insan onurunun korunması ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı ifade etmektedir. Bununla birlikte, sözkonusu hak mutlak ve sınırsız olmayıp, Anayasa'nın 13. ve 20. maddeleri gereğince belirli koşullarda, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmamak üzere yasayla sınırlanabilir. Bu bağlamda, kişisel verilerin sistematik biçimde kayıt altına alınabilmesi için verilerin korunmasına ilişkin esas ve usullerin yasayla düzenlenmesi zorunludur. Diğer bir deyişle, kişisel verilerin korunmasına ilişkin gerekli yasal düzenlemeye ve teknik olanaklara sahip olmayan bir idarenin, kişinin rızasını alsa dahi bu konudaki işleminin hukuka uygunluğundan söz etmek olanaklı olmayacaktır.

Bu çerçevede, idarelerce gelişen teknolojinin, kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması nedeniyle, kamu kesiminde kullanılmaya başlanması doğal olmakla

birlikte, teknoloji kullanılarak kişisel verilerin kayıt altına alınması uygulamasının yukarıda belirtilen hükümlere uygun olması gerektiğinde kuşku bulunmamaktadır.

Yukarıda belirtildiği üzere, gerek Anayasa'da gerekse ülkemizin tarafı olduğu ve yine Anayasa'nın 90. maddesi uyarınca kanun hükmünde olan uluslararası sözleşmelerde, kişilerin özel hayatı ile aile hayatının ve kişisel verilerinin gizliliğine saygı gösterilmesi gerektiği ve bu gizliliğe müdahale edilemeyeceği açıkça hüküm altına alınmış olup, bu gizliliğe müdahalenin milli güvenlik, kamu düzeni gibi zorunluluk arz eden durumlara münhasır olarak ve yasayla öngörülmek şartıyla mümkün olduğu anlaşılmaktadır.

Bu kapsamda, ilgililerden kişisel veri alınması niteliğinde olan "parmak izi taraması"nın, "özel hayatın gizliliği" ilkesi kapsamında bulunması karşısında "uygulamanın sınırlarını, usul ve esaslarını" gösteren bir yasal dayanağının bulunmaması, toplanan verilerin ileride başka bir şekilde kullanılmayacağına dair bir güvencenin mevcut olmaması gözönüne alındığında, yukarıda belirtilen temel haklar ve Anayasal ilkeler ile uluslararası sözleşme kuralları ile bağdaşmayan dava konusu işlemde hukuka uyarlık bulunmadığı sonucuna varılmıştır.

Açıklanan nedenlerle, davacının temyiz isteminin kabulüne, Konya 1. İdare Mahkemesince verilen 13/03/2014 günlü, E:2014/224, K:2014/256 sayılı ısrar kararının BOZULMASINA, dosyanın anılan İdare Mahkemesine gönderilmesine, kararın tebliğ tarihini izleyen 15 (onbeş) gün içinde karar düzeltme yolu açık olmak üzere, 09/12/2015 tarihinde oyçokluğu ile karar verildi.

KARŞI OY

X- Temyiz edilen kararla ilgili dosyanın incelenmesinden, Konya 1. İdare Mahkemesinin 13/03/2014 günlü, E:2014/224, K:2014/256 sayılı kararının usul ve hukuka uygun bulunduğu, dilekçede ileri sürülen temyiz nedenlerinin kararın bozulmasını gerektirecek nitelikte olmadığı anlaşıldığından, davacının temyiz isteminin reddi ile ısrar kararının onanması gerektiği oyuyla, karara katılmıyoruz.

Danıştay Kararı - 10. Daire (E. 2020/4379)

Danıştay Kararı - 10. D., E. 2020/4379 K. 2020/3834 T. 14.10.2020

T.C. DANIŞTAY ONUNCU DAİRE

Esas No: 2020/4379

Karar No: 2020/3834

DAVACI: ...

VEKİLİ: Av. ...

DAVALI: ... Kurumu / ...

DAVANIN ÖZETİ: Davacı tarafından, ... tarih ve ... sayılı Bilgi Teknolojileri ve İletişim Kurulu kararı ile onaylanan "Posta Gönderilerine İlişkin Güvenlik Tedbirlerine Yönelik Usul ve Esaslar"ın 4. maddesinin 2. fıkrasının kaldırılması istemiyle Bilgi Teknolojileri ve İletişim Kurumuna yapılan başvurunun zımnen reddine dair işlemin iptali istenilmektedir.

DANIŞTAY TETKİK HAKİMİ: ...

DÜŞÜNCESİ: Davanın süre aşımı nedeniyle reddine karar verilmesi gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay Onuncu Dairesince, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 14. maddesi uyarınca hazırlanan Tetkik Hakiminin raporu ve sözlü açıklamaları dinlendikten sonra, davacının yürütmenin durdurulması istemi hakkında bir karar verilmeksizin gereği görüldü:

2577 sayılı İdari Yargılama Usulü Kanunu'nun "Dava açma süresi" "başlıklı 7. maddesinde, özel kanunlarında ayrı süre gösterilmeyen hallerde Danıştayda ve idare mahkemelerinde dava açma süresinin altmış gün olduğu, bu sürelerin idari uyuşmazlıklarda yazılı bildirim yapıldığı tarihi izleyen günden itibaren, ilanı gereken düzenleyici işlemlerde ise ilan tarihini izleyen günden itibaren başlayacağı, ancak düzenleyici işlemlerin uygulanması üzerine ilgililerin, düzenleyici işlem veya uygulanan işlem yahut her ikisi aleyhine birden dava açabilecekleri; 14. maddesinin 3. fıkrasının (e) bendinde, dava dilekçesinin süre aşımı yönünden inceleneceği; 15. maddesinin 1. fıkrasının (b) bendinde ise, süre aşımı olan durumlarda davanın süre aşımı nedeniyle reddine karar verileceği hüküm altına alınmıştır.

Dava dosyasının incelenmesinden; ... barkod numaralı gönderinin Posta ve Telgraf Teşkilatı Anonim Şirketine (PTT) ait ... ili, ... ilçesinde bulunan şubeden davacı tarafından teslim alınmak üzere başvurulduğunda davacıdan vatandaşlık numarası ibrazının talep edildiği, davacının bu işleme rıza göstermemesi üzerine gönderinin kendisine teslim edilmediği, bunun üzerine PTT'ye yapılan 16/05/2019 tarihli başvuru ile söz konusu gönderinin vatandaşlık numarası ibrazı ve ücret istenmeden tarafına tesliminin yapılması, Bilgi Teknolojileri ve İletişim Kurumu (BTK) ile de iletişime geçilerek anılan Kuruma ait ... tarih ve ... sayılı karardaki "T.C. Kimlik numarası" ibaresinin karardan çıkartılması için girişimde bulunulması ve talep edilen vatandaşlık numarasının gizliliğinin nasıl sağlandığı ve ne sürede silindiği hakkında tarafına bilgi verilmesinin istendiği; anılan başvuru neticesinde PTT tarafından tesis edilen ... tarih ve ... sayılı işlemle, davacıya söz konusu gönderinin vatandaşlık numarası ibraz edilmeksizin tesliminin mevzuat gereği mümkün olmadığı, BTK'nın söz konusu kararıyla ilgili olarak talep ve şikayetlerin ilgili kuruma yapılacak başvuru ile takip edilebileceğinin bildirildiği; bu süreçle eş zamanlı olarak davacı tarafından 17/05/2019 tarihinde Kişisel Verileri Koruma Kurumuna da aynı taleplerle başvuru yapıldığı ve başvuru neticesinde Kişisel Verileri Koruma Kurumunca tesis edilen 11/11/2019 tarih ve 11670 sayılı işlemle, davacıdan posta gönderisi teslimi esnasında vatandaşlık numarası ibrazı istenmesinin 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 5. maddesinin 2. fıkrasının (ç) bendinde düzenlenen "veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olma hali" kapsamında kaldığından bahisle talebe konu uygulamanın Kanun'a aykırı olmadığına ve BTK düzenlemesine karşı yapılan itiraz ile ilgili olarak Kanun'a uygunluk hususunun yetkide ve usulde paralellik ilkesi gereği yetkili kurumun BTK olması sebebiyle ilgili kurumla istişare edilmesine karar verildiği; davacının 20/01/2020 tarihli dilekçe ile ... tarih ve ... sayılı Bilgi Teknolojileri ve İletişim Kurulu kararı ile onaylanan Posta Gönderilerine İlişkin Güvenlik Tedbirlerine Yönelik Usul ve Esasların 4. maddesinin 2. fıkrasının kaldırılmasını talep ettiği, bu talebin altmış günlük süre içerisinde cevap verilmemek suretiyle zımmen reddi üzerine ise 07/05/2020 kayıt tarihli dilekçe ile ... İdare Mahkemesi nezdinde bakılmakta olan davanın açıldığı; Mahkemenin ... tarih ve E:..., K:... sayılı kararıyla dava görev yönünden reddedilerek dosyanın Danıştaya gönderilmesine karar verildiği; Danıştay Onüçüncü Dairesinde esas alan dava dosyasının 22/07/2020 tarih ve E:2020/1948, K:2020/1946 sayılı kararlarla Dairemize gönderildiği anlaşılmaktadır.

2577 sayılı Kanun'un idari yargı yerinde dava açma sürelerine ilişkin yukarıda aktarılan hükümleri ve yerleşik Danıştay kararlarına göre, düzenleyici işlemlere karşı dava açma süresinin, şayet bu düzenleme ilanı gereken bir düzenleyici işlem değil ise, söz konusu düzenlemenin ilgililerce öğrenilmesini takip eden günden itibaren altmış gün olduğu; öte yandan, bahsi geçen düzenlemenin

uygulanmasına yönelik bir işlem tesis edilmesi halinde, uygulama işlemine dayanak olan düzenleyici işleme karşı dava açma süresinin yeniden canlanacağı ve bu sürenin de uygulama işleminin tebliğini takip eden günden itibaren altmış gün olmakla birlikte, bahsi geçen düzenleyici işlem ile uygulama işleminden menfaati etkilenenlerin, seçimlik olarak; düzenleyici işleme, uygulama işlemine yahut her iki işleme birden yasal süre içerisinde dava açmaları mümkün olup, davanın yalnızca uygulama işlemine karşı açılması halinde, idari yargı düzeni içerisinde davaya bakmakla görevli ilk derece yargı yerinin idare mahkemesi olduğu, düzenleyici işleme yahut her iki işleme karşı dava açıldığı hallerde ise, düzenleyici işlemin 2575 sayılı Kanun'un 24. maddesinde tanımlandığı gibi, ülke çapında uygulanacak bir düzenleme olması halinde, davaya ilk derece yargı yeri olarak Danıştayca bakılacağı açıktır.

Bakılan davanın düzenleyici işlemin uygulanması üzerine, uygulama işlemine karşı açılan dava niteliğinde olmadığı; davacı tarafından, adına gelen gönderinin PTT ilgili şubesinden alınmak istendiği esnada, kendisinden vatandaşlık numarası ibrazının istendiği, davacı tarafından bu talebin reddi üzerine teslimatın gerçekleşmediği, bu olayın gerçekleştiği tarihin dava dilekçesi ve eklerinde bildirilmediği; ancak, davacı tarafından bu olay üzerine, ... ve ... tarihlerinde PTT ve Kişisel Verileri Koruma Kuruluna dava konusu edilen ... tarih ve ... sayılı Bilgi Teknolojileri ve İletişim Kurulu kararı ile onaylanan Posta Gönderilerine İlişkin Güvenlik Tedbirlerine Yönelik Usul ve Esasların 4. maddesinin 2. fıkrasının hukuka aykırılığı ile ilgili olarak başvurularda bulunulduğu; bu başvurulardan istediği neticeyi elde edememesi üzerine ise 20/01/2020 tarihinde anılan düzenlemenin kaldırılması istemiyle davalı BTK'ya başvuruda bulunulduğu ve talebin zımnen reddi üzerine bakılan davanın açıldığı; olayda aktarıldığı üzere, ... barkod numaralı gönderinin dava konusu edilen düzenleme nedeniyle davacıya vatandaşlık numarası ibraz edilmeksizin tesliminin yapılmadığı tarihin (dava dilekçesinde olay tarihi net olarak belirlenememesi nedeniyle) en geç PTT'ye başvuru tarihi olan 16/05/2019 tarihi olarak nitelenebileceği ve bu tarihin dava konusu edilen düzenlemenin davacıya uygulandığı tarih olduğu görülmektedir.

Bu durumda; ... tarih ve ... sayılı Bilgi Teknolojileri ve İletişim Kurulu kararı ile onaylanan Posta Gönderilerine İlişkin Güvenlik Tedbirlerine Yönelik Usul ve Esasların 4. maddesinin 2. fıkrasının davacıya 16/05/2019 tarihinde uygulanması üzerine, bu tarihi takip eden günden itibaren dava açma süresinin işlemeye başladığı; davacının işlemeye başlayan altmış günlük dava açma süresi (15/07/2019 tarihinin resmi talil olması sebebiyle) 16/07/2019 tarihinde dolduktan sonra 22/01/2020 tarihinde davalı idareye, dava konusu edilen düzenlemenin kaldırılması istemi ile yapılan başvurunun zımnen reddinin uygulama işlemi niteliğinde bir işlem olmadığından, dolmuş olan dava

açma süresinin bu başvuru neticesinde canlanmayacağı görüldüğünden, bakılan davanın süre aşımı nedeniyle esasının incelenmesine hukuki olanak bulunmamaktadır.

Açıklanan nedenlerle, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 14. maddesinin üçüncü fıkrasının (e) bendi ve 15. maddesinin birinci fıkrasının (b) bendi uyarınca davanın süre aşımı nedeniyle REDDİNE, aşağıda dökümü yapılan ... TL yargılama giderinin davacı üzerinde bırakılmasına, kullanılmayan ... TL yürütmenin durdurulması harcının istemi halinde, ile posta ücreti avansından artan miktarın ise kararın kesinleşmesi üzerine istemi halinde davacıya iadesine, bu karara karşı tebliğ tarihini izleyen otuz (30) gün içerisinde Danıştay İdari Dava Daireleri Kuruluna temyiz yolu açık olmak üzere, 14/10/2020 tarihinde oy birliğiyle karar verildi.

Danıştay Kararı - 2. Daire (E. 2020/847)

Danıştay Kararı - 2. D., E. 2020/847 K. 2020/3028 T. 20.10.2020

İSTEMİN KONUSU: Ankara 5.İdare Mahkemesince verilen 14/01/2020günlü, E:2020/12, K:2020/64sayılı kararın, dilekçede yazılı nedenlerle 2577 sayılı İdari Yargılama Usulü Kanunu'nun 49. maddesi uyarınca temyizen incelenerek bozulması isteminden ibarettir.

YARGILAMA SÜRECİ:

Dava Konusu İstem: Dava; Bursa Büyükşehir Belediye Başkanlığında Mali Hizmetler Uzman Yardımcısı olarak görev yapmakta iken, Maliye Bakanlığı Vergi Denetim Kurulu Başkanlığı'nca 11 - 12 Mayıs 2013 tarihlerinde yazılı, 30 Temmuz - 02 Ağustos 2013 tarihleri arasında sözlü bölümü yapılan vergi müfettiş yardımcılığı giriş sınavında başarılı olan davacının, Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği 15. maddesine istinaden,Vergi Müfettiş Yardımcılığı'na atamasının gerçekleştirilmesi talebiyle yaptığı başvurunun zımnen reddine ilişkin işlemin iptali istemiyle açılmıştır.

İlk Derece Mahkemesi Kararının Özeti : Danıştay İkinci Dairesinin 03/01/2019 günlü E:2016/11854, K:2019/57 sayılı bozma kararına uyularak verilen Ankara5.İdareMahkemesinin temyize konu kararıyla; Maliye Bakanlığı Personeli Hakkında Yapılacak Güvenlik Soruşturması ve Arşiv Araştırması Yönergesi'ne göre, davacının görev yapacağı Vergi Denetim Kurulu Başkanlığı'nın gizlilik dereceli birimlerden ve atanacağı vergi müfettiş yardımcısı kadro unvanının da gizlilik dereceli görevlerden olduğu; hakkında açılan dava sonucunda, "Bıçak veya Diğer Aletleri İzinsiz Olarak Satma, Satın Alma, Taşıma veya Bulundurma" ve "Hakaret, Basit Yaralama ve Kamu Malına Zarar Verme" suçlarından hükmün açıklanmasının geri bırakılmasına karar verildiği, 5271 sayılı Ceza Muhakemesi Kanunu'nun ilgili hükümleri uyarınca hükmün açıklanmasının geri bırakılmasına ilişkin kararların davacı hakkında hukuki sonuç doğurmadığının açık olduğu, buna göre, davacının fiillerinin niteliği gereği gizlilik dereceli birimlerde görev yapmak açısından tehlike arz edip etmeyeceğinin irdelenmesi mümkün olmakla birlikte, Maliye Bakanlığı Değerlendirme Komisyonu'nun 27/12/2013 gün ve 2013-9 sayılı kararında sadece anılan mahkumiyet hükümleri yönünden değerlendirme yapılarak bir sonuca ulaşıldığı ve dava konusu işlemin bu komisyon kararına dayalı olarak tesis edildiği anlaşıldığından, Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği'nin 15. maddesi uyarınca davacının vergi müfettiş yardımcısı olarak atamasının

yapılmamasına ilişkin işlemde hukuka uyarlık bulunmadığı gerekçesiyle dava konusu işlem iptal edilmiştir.

TEMYİZ EDENİN İDDİALARI: Davalı idare tarafından; stratejik öneme sahip bir birimde çalışacak olması nedeniyle hakkında güvenlik ve arşiv araştırması yapılan davacının, "Bıçak veya Diğer Aletleri İzinsiz Olarak Satma, Satın Alma, Taşıma veya Bulundurma" ve "Hakaret, Basit Yaralama ve Kamu Malına Zarar Verme" suçlarını işlediği yapılan yargılamalarla da sabit görülen fiilleri nedeniyle denetimli serbestlik kararı verildiği, bu nedenle, Maliye Bakanlığı Değerlendirme Komisyonununun 27/12/2013 günlü kararı ile vergi müfettiş yardımcısı kadrosuna atanmasının uygun görülmediği, dava konusu işlemin hukuka ve mevzuata uygun olduğu ileri sürülerek, mahkeme kararının bozulması istenilmektedir.

KARŞI TARAFIN CEVABI: Davacı tarafından; daha önce işlediği çeşitli suçlar sebebiyle atamasının gerçekleştirilmediği belirtilmişse de, davalı idarenin işbu savunmasının kötüniyetli olduğu, 4045 sayılı Kanun ve Yönetmelik hükümlerinin bir arada değerlendirilmesinden; kamu kurum ve kuruluşlarının, devletin güvenliği, ulusal bütünlük ve ülkenin iç ve dış menfaatleri ile alakalı gizli bilgi veya belgelerin bulunduğu birimlerinde görev yapacak personel hakkında güvenlik soruşturması ve arşiv araştırması yapılması ve bu kapsamda ilgili kişi hakkında elde edilen bilgilerin olumsuz çıkması halinde, o kişinin söz konusu birimlerde görev yapmasının sakınca doğurup doğurmayacağına bu amaçla oluşturulacak komisyon tarafından değerlendirilmesi gerektiği, bahsi geçen düzenlemelerin amacından da açıkça anlaşıldığı üzere kişi hakkındaki her türlü mahkumiyetin söz konusu birimlerde görev yapmasına engel teşkil etmeyeceği, kişi hakkında elde edilen bilgilerin, niteliği gereği gizlilik dereceli birimlerde görev yapmak açısından tehlike arz edip etmeyeceği yönünden irdelenmesi gerektiği, açılan dava sonucunda verilen "hükmün açıklanmasının geri bırakılması" kararlarının hakkında hukuki sonuç doğurmadığı, idarenin işleminin hukuka aykırı olduğu, ilk derece mahkemesi kararının onanması gerektiği yolundadır.

DANIŞTAY TETKİK HAKİMİ: K1

DÜŞÜNCE: Temyiz isteminin reddi ile usul ve yasaya uygun olan İdare Mahkemesi kararının onanması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay İkinci Dairesince, Tetkik Hakiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereği görüldü:

MADDİ OLAY:

Davacının vergi müfettiş yardımcılığı yazılı ve sözlü sınavlarında başarılı olması üzerine, hakkında yapılan arşiv araştırması ve güvenlik soruşturması sonucunda; Eskişehir 3. Sulh Ceza Mahkemesi'nin 20/03/2008 tarihli ve E:2007/545, K:2008/270 sayılı kararıyla "Bıçak veya Diğer Aletleri İzinsiz Olarak Satma, Satın Alma, Taşıma veya Bulundurma" suçuyla ilgili olarak yapılan yargılaması sonucunda 5136 sayılı Kanuna muhalefet suçunu işlediği sabit görülerek 5 ay hapis ve 375,00 TL adli para cezası ile cezalandırılmasına karar verildiği, bu kararın Yargıtay 8. Ceza Dairesi'nin 01/06/2010 tarihli ve E:2010/4865, K:2010/7765 sayılı kararı ile bozulması üzerine Eskişehir 3. Sulh Ceza Mahkemesi'nin 03/03/2011 tarihli ve E:2010/628, K:2011/214 sayılı kararıyla, davacının bozma kararı uyarınca sabit olan suçundan yargılanmasına ve hakkında 5271 sayılı Ceza Muhakemesi Kanunu'nun 231/5. maddesi gereğince hükmün açıklanmasının geri bırakılmasına ve denetimli serbestlik tedbirine hükmolünmesine karar verildiği ve bu kararın da 18/03/2011 tarihinde kesinleştiği; yine davacının daha önce, "Hakaret, Basit Yaralama ve Kamu Malına Zarar Verme" suçlarından dolayı yapılan yargılaması sonucunda da, Eskişehir 1. Asliye Ceza Mahkemesi'nin 06/05/2008 tarihli ve E:2007/482, K:2008/265 sayılı kararı ile "Yaralama" suçundan 150 gün adli para cezası, "Hakaret" suçundan 11 ay 20 gün hapis cezası, "Kamu Malına Zarar Verme" suçundan da 5 ay hapis cezası ile cezalandırıldığı ve bu cezalara yönelik davacı hakkında 5271 sayılı Ceza Muhakemesi Kanunu'nun 231/5-8. maddeleri gereğince hükmün açıklanmasının geri bırakılmasına ve 5 yıl süre ile denetimli serbestlik tedbirine hükmolünmesi nedeniyle, Maliye Bakanlığı Değerlendirme Komisyonu Başkanlığının 27/12/2013 gün ve 2013-9 sayılı kararıyla; davacının atamasının uygun görülmediğine ilişkin kararına Maliye Bakanı tarafından Olur verilmesi üzerine, davacının atamasının yapılmamasına ilişkin tesis edilen dava konusu işlemin iptali istemiyle temyizden incelenen dava açılmıştır.

İLGİLİ MEVZUAT:

24/03/2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Özel Nitelikli Kişisel Verilerin İşlenme Şartları" kenar başlıklı 6. maddesinde, (1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, ... ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. (2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır. (3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir..."; "İstisnalar" kenar başlıklı 28. maddesinin birinci fıkrasında, " Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz: ... ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi, d) Kişisel

verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi..." kurallarına yer verilmiştir.

5352 sayılı Adli Sicil Kanunu'nun 6. maddesinde, "Kamu davasının açılmasının ertelenmesine ve hükmün açıklanmasının geri bırakılmasına ilişkin kararlar, ancak bir soruşturma veya kovuşturmayla bağlantılı olarak mahkeme, hâkim, askerî hâkim, Cumhuriyet Başsavcılığı veya askerî savcılık tarafından istenmesi halinde verilmek üzere kaydedilir." hükmü yer almaktadır.

657 sayılı Devlet Memurları Kanunu'nun 48. maddesinde, Devlet memurluğuna alınacaklarda aranılan genel ve özel şartlar belirtilerek, özel şartlar arasında kurumların özel kanun ve diğer mevzuatında aranan şartları taşımak gerektiği hüküm altına alınmıştır.

Maliye Bakanlığı Personeli Hakkında Yapılacak Güvenlik Soruşturması ve Arşiv Araştırması Yönergesi'nin "Kapsam" başlıklı 2. maddesinde;"Bu yönerge; Maliye Bakanlığı merkez ve taşra teşkilatında görevli bulunan personel ile ilk defa, yeniden veya kurumlararası naklen atanacaklardan gizlilik dereceli birim, kısım ve görevlerde çalıştırılması düşünülenler ile yurtdışı teşkilatında sürekli görevlendirilecek bütün personelin güvenlik soruşturması ve arşiv araştırmasına ilişkin usul ve esasları kapsar."; "Gizlilik Dereceli Birim, Kısım ve Görevler" başlıklı 6. maddesinde;"a) Merkez teşkilatında; 1- Müsteşarlık ve Müsteşar Yardımcılığı makamlarının özel büroları, ana hizmet birimlerinin denetim birimi başkanlıkları, özel büroları ile personel şubesi müdürlükleri, danışma ve denetim birimlerinin ve yardımcı birimlerin özel büroları ile personel şubesi müdürlükleri, 2- Teftiş Kurulu Başkanlığı, Hesap Uzmanları Kurulu Başkanlığı, Mali Suçları Araştırma Kurulu Başkanlığı, Personel Genel Müdürlüğü, Savunma Sekreterliği ve Özel Kalem Müdürlüğü, b) Taşra teşkilatında; Defterdarlık, Gelirler Bölge Müdürlüğü ve İşletme Bölge Müdürlüğü bünyesindeki denetmenler büroları, özel bürolar ile personel birimleri, c) Yurtdışı teşkilatında; Maliye Müşavirlikleri ile Maliye Ataşelikleri. B- Gizlilik dereceli görevleri yürüten personel: a) Unvanına bakılmaksızın yukarıda (A) bendinde sayılan yerlerde görevlendirilen personel, b) Görevli olduğu yer dikkate alınmaksızın, Bakanlık merkez ve taşra teşkilatında çalışan müdür ve daha üst düzeydeki personel, koruma ve güvenlik görevlileri ile kozmik evrak personeli, c) Kontrolörler ve Stajyer kontrolörler, d) Hazine avukatları, e) Özel Yönetmeliği bulunan merkez teşkilatı uzmanları ile denetmenler ve bunların yardımcıları, f) Birim amirince (Merkez ve döner sermaye teşkilatında Genel Müdür, Başkan veya Müstakil Daire Başkanı, taşra teşkilatında Defterdar veya Bölge Müdürü) hakkında Güvenlik Soruşturması ve Arşiv Araştırması yaptırılması uygun görülen personel" kurallarına yer verilmiştir.

4045 sayılı Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli ve Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim

Kanununda Değişiklik Yapılmasına İlişkin Kanun'un 1. maddesinin dava konusu işlem tarihi itibarıyla yürürlükte bulunan halinde, "Güvenlik Soruşturması ve Arşiv Araştırması; ... askeri, emniyet ve istihbarat teşkilatlarında çalıştırılacak kamu personeli ve ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında yapılır. Devletin güvenliğini, ulusun varlığını ve bütünlüğünü iç ve dış menfaatlerinin zarar görebileceği ve tehlikeye düşebileceği bilgi ve belgeler ile gizlilik dereceli kamu personeli ile meslek gruplarının tespiti birim ve kısımlarının tanımlarının yapılması güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak merciler ve üst kademe yöneticilerinin kimler olduğu Bakanlar Kurulu kararı ile yürürlüğe konulacak yönetmelik ile düzenlenir." hükmü bulunmaktadır.

12/04/2000 tarih ve 24018 sayılı Resmî Gazete'de yayımlanan Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği'nin (Yönetmelik) "Kapsam" kenar başlıklı 2. maddesinde, "Bu Yönetmelik; yetkili olmayan kişilerin bilgi sahibi olmaları halinde Devletin güvenliğinin, iç ve dış menfaatlerinin, ulusal varlığın ve bütünlüğün zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeleri, bunların toplanmasını ve işlemini yürüten bakanlıklar ile kamu kurum ve kuruluşlarının ilgili birim ve kısımlarının belirlenmesini, Türk Silahlı Kuvvetlerinde, emniyet ve istihbarat teşkilatlarında, ceza infaz kurumları ve tutukevlerinde çalışacak personeli, ayrıca bakanlıklar ile kamu kurum ve kuruluşlarının yurtdışı teşkilatlarında sürekli görevlendirilecek bütün personel için yapılacak güvenlik soruşturması ve arşiv araştırmasının esas ve usullerini, bunu yapacak mercileri, hakkında güvenlik soruşturması ve arşiv araştırması yapılacak gizlilik dereceli yerlerde çalışan kamu personeli ile meslek grupları ve üst kademe yöneticilerini kapsar."; "Güvenlik Soruşturması ve Arşiv Araştırması Yapacak Makamlar" kenar başlıklı 7. maddesinde, "Güvenlik soruşturması ve arşiv araştırması, Milli İstihbarat Teşkilatı Müsteşarlığı, Emniyet Genel Müdürlüğü ve mahalli mülki idare amirlikleri tarafından yapılır. İçişleri Bakanlığı Kaçakçılık İstihbarat Harekat ve Bilgi Toplama Dairesi Başkanlığı'ndaki bilgi kayıtları ile Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü'ndeki adli sicil kaydı, talepleri üzerine, güvenlik soruşturması ve arşiv araştırmasını yapacak makamlar ile Türk Silahlı Kuvvetlerinin ilgili birimlerine verilir.;"Hakkında Güvenlik Soruşturması ve Arşiv Araştırması Yapılacak Personel" kenar başlıklı 8. maddesinde,"Güvenlik soruşturması ve arşiv araştırması; gizlilik dereceli birim ve kısımlar ile askeri, emniyet, istihbarat teşkilatlarında ve ceza infaz kurumları ve tutukevlerinde çalıştırılacak personel hakkında yapılır. Emniyet Genel Müdürlüğü ve mahalli mülki idare amirlikleri, güvenlik soruşturması ve arşiv araştırmasını; bakanlıklar, kamu kurum ve kuruluşlarının gizlilik dereceli birim ve kısımları ile yurtdışı teşkilatında ve askeri, emniyet, istihbarat teşkilatlarında ve ceza infaz kurumu ve tutukevlerinde çalıştırılacak personel hakkında yapar."

kurallarına yer verilmiştir.

Aynı Yönetmeliğin 'Güvenlik Soruşturması ve Arşiv Araştırmasında Araştırılacak Hususlar' başlıklı 11. maddesinde,

"Güvenlik soruşturması ve arşiv araştırmasında kişinin içinde bulunduğu ortam da dikkate alınarak;

a) Kimlik kontrolü, kimlik kayıtlarının doğruluk derecesi, uyrukluđu, geçmişte yabancı bir devletin uyrukluđuna girip girmediđi,

b) Kolluk kuvvetleri tarafından halen aranıp aranmadıđı, kolluk kuvvetlerinin ve istihbarat ünitelerinin arşivlerinde bilgiler bulunup bulunmadıđı, adli sicil kaydının ve hakkında bir tahdidin olup olmadıđı,

c) Yıkıcı faaliyetlerde bulunup bulunmadıđı ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanuna ve Atatürk ilke ve inkılaplarına aykırı davranıp davranmadıđı,

d) Şeref ve haysiyetini ihlal edecek ve görevine yansıyacak şekilde kumara, uyuşturucuya, içkiye, paraya ve aşırı bir şekilde menfaatine düşkün olup olmadıđı, ahlak ve adaba aykırı davranıp davranmadıđı,

e) Yabancılarla, özellikle hasım ve hasım olması muhtemel Devlet mensupları ve temsilcileriyle ilgi derecesinin iç yüzü ve nedeni,

f) Sır saklama yeteneđinin olup olmadıđı,

araştırılır.";

'Güvenlik Soruşturması ve Arşiv Araştırmasında İzlenecek Yöntem' başlıklı 12. maddesinde de,

" ...

c) Güvenlik soruşturması ve arşiv araştırması yapılması isteminin ilgili makama ulaşmasından itibaren arşiv araştırması sonuçları en geç 30 gün, güvenlik soruşturması sonuçları en geç 60 gün içinde cevaplandırılır. Soruşturma ve araştırma sonucunu içeren bilgi ve belgeler ilgilinin güvenlik makamlarındaki dosyasında asgari 'gizli' gizlilik derecesinde saklanır.

d) Güvenlik soruşturması ve arşiv araştırmasını isteyen makama, kişi hakkında karar vermeye yeterli bilgiler aktarılır.

e) Güvenlik soruşturması ve arşiv araştırmasının nasıl ve ne şekilde yapılacağı, soruşturma ve araştırma yapmaya yetkili makamların görev talimatları ile belirlenir.

f) Mahalli mülki idare amirliklerince yapılmış olan güvenlik soruşturması ve arşiv araştırmasında olumsuz durumu saptananların evrakının bir örneği dosya açılmak üzere Emniyet Genel Müdürlüğüne gönderilir.

g) Güvenlik soruşturması ve arşiv araştırmasında olumsuz durumu saptananlarla ilgili bilgiler Milli İstihbarat Teşkilatı Müsteşarlığı ve Emniyet Genel Müdürlüğüne karşılıklı olarak birbirlerine aktarılır.

.. " kuralları düzenlenmiştir.

HUKUKİ DEĞERLENDİRME:

Somut olayda, davacının işlediği iddia edilen fiillere istinaden yapılan yargılama neticesinde verilen hükmün açıklanmasının geri bırakılmasına ilişkin kararların kayıtlarının Bursa Valiliği İl Emniyet Müdürlüğü tarafından davalı idareye verildiği ve bu kayıtlar dikkate alınmak suretiyle davacının güvenlik soruşturmasının olumsuz sonuçlandırıldığı anlaşılmaktadır.

Belirli kamu görevlerinde çalıştırılacak personel hakkında uygulanan güvenlik soruşturması ve arşiv araştırmasının kanuni dayanağı 4045 sayılı Kanun'dur. 4045 sayılı Kanun'un dava konusu işlem tarihi itibarıyla yürürlükte bulunan halinde, güvenlik soruşturması ve arşiv araştırmasının; kamu kurum ve kuruluşlarında yetkili olmayan kişilerin bilgi sahibi olmaları hâlinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile askerî teşkilatlarda, emniyet ve istihbarat teşkilatlarında çalıştırılacak kamu personeli, ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında yapılacağı düzenlenmiştir.

Kamu görevlilerinin sadakat, tarafsızlık ve devlete bağlılık yükümlülüğü çerçevesinde devleti temsil eden ve millî güvenlik bakımından hassasiyet içeren bazı kamu görevlerine atanacak kişiler bakımından daha sıkı nitelikler aranması ve birtakım sınırlamaların getirilmesi doğaldır. Bu şekilde aranan nitelikler ve kanunlarda öngörülen kısıtlamalar, kamu hizmetinin etkin ve sağlıklı bir biçimde yürütülmesi amacına yöneliktir.

Dolayısıyla idarenin millî güvenlik açısından önem arz eden kadrolara atanacak kişilerin tabi olacağı güvenlik soruşturması ve arşiv araştırması konusunda kanunla temel çerçeveyi ortaya koyan kurallar getirmesi mümkündür.

Ancak, bu alanda yapılan düzenlemelerin diğerkanuni düzenlemelerle çelişmemesi ve diğerdüzenlemelerde gözetilen amaçları ortadan kaldırır nitelikte de olmaması gerekmektedir.

Bu bağlamda, yukarıda metnine yer verilen 4045 sayılı Kanun'un 1. maddesinin işlem tarihindeki hali incelendiğinde; maddede, kişilerin geçmiş ceza mahkûmiyetlerine ilişkin kayıtlar bakımından hangi suçların kamu görevine girmeye engel olacağı konusunda hiçbir belirleme yapılmadığı, suçlar arasında herhangi bir ayırım ve derecelendirme öngörülmediği, aynı şekilde hükmün açıklanmasının geri bırakılmasına konu kararların güvenlik soruşturması veya arşiv araştırmasının olumsuz sonuçlandırılmasının bir sebebi olup olmayacağı hususunda herhangi bir düzenlemeye yer verilmediği anlaşılmaktadır.

Nitekim, Anayasa Mahkemesinin 29/05/2019 tarih ve 2014/15365 başvuru numaralı "Turgut Duman" kararında, özetle; işleme dayanak olan 4045 sayılı Kanun hükümlerinin temel hakkın kısıtlanması bakımından yeterli güvenceye sahip olmaması ve kanunilik ilkesine aykırı bulunması sebebiyle ve ayrıca 5352 sayılı Kanun'un 6. maddesinde kamu davasının açılmasının ertelenmesine ve hükmün açıklanmasının geri bırakılmasına ilişkin kararların; ancak, bir soruşturma veya kovuşturmayla bağlantılı olarak mahkeme, hâkim, askerî hâkim, Cumhuriyet başsavcılığı veya askerî savcılık tarafından istenmesi hâlinde verileceği düzenlenmesine rağmen bu hükme aykırı şekilde yapılan güvenlik soruşturması ve arşiv araştırmasının özel hayata saygı hakkını ihlal ettiği belirtilmiştir.

Yine anılan kararda Anayasa Mahkemesi, İdare Mahkemesince davanın kesin hükme bağlanmasının ertelenmesine ilişkin karara dayanılarak hakkında herhangi bir mahkûmiyet kararı bulunmayan başvuruçunun ceza yargılamasına konu eylemleri işlediğinin sabit olduğu varsayımına dayanılarak karar verildiğinin anlaşıldığından bahisle başvuruçunun Anayasa'nın 36. ve 38. maddelerinde güvence altına alınan masumiyet karinesinin de ihlal edildiği sonucuna ulaşmıştır.

Bu durumda, 5352 sayılı Kanun'un 6. maddesine aykırı şekilde elde edilen bilgi ve belgelere dayalı olarak yapılan arşiv araştırması üzerine tesis edilen dava konusu işlemde hukuka uyarlık, İdare Mahkemesi'nce verilen iptal kararında ise hüküm fıkrası itibarıyla hukuki isabetsizlik bulunmamaktadır.

Nitekim İdari Dava Daireleri Kurulunu'nun 12/03/2020 günlü, E:2019/2425, K:2020/715 sayılı kararı da bu yöndedir.

KARAR SONUCU:

Açıklanan nedenlerle;

1. DAVALI İDARENİN TEMYİZ İSTEMİNİN REDDİNE,

2. Ankara 5. İdare Mahkemesince verilen 14/01/2020günlü, E:2020/12, K:2020/64sayılı kararın YUKARIDA BELİRTİLEN GEREKÇE İLEONANMASINA,
3. Temyiz giderlerinin istemde bulunan davalı idare üzerinde bırakılmasına,
4. Dosyanın Mahkemesine gönderilmesine,
5. 2577 sayılı Kanun'un (Geçici 8. maddesi uyarınca uygulanmasına devam edilen) 54. maddesinin 1. fıkrası uyarınca bu kararın tebliğ tarihini izleyen günden itibaren (15) onbeşgün içinde Danıştay'da karar düzeltme yolu açık olmak üzere, 20/10/2020tarihinde oybirliğiyle karar verildi.

Danıştay Kararı - 10. Daire (E. 2019/10118)

Danıştay Kararı - 10. D., E. 2019/10118 K. 2021/43 T. 11.1.2021

T.C. DANIŞTAY ONUNCU DAİRE

Esas No: 2019/10118

Karar No: 2021/43

TEMYİZ EDEN (DAVACI): ... Sendikası

VEKİLLERİ: Av. ... - Av. ...

KARŞI TARAF (DAVALILAR): 1- ... Büyükşehir Belediye Başkanlığı

VEKİLİ: Av. ...

2-... Genel Müdürlüğü

VEKİLİ: Av. ...

İSTEMİN_KONUSU: ... İdare Mahkemesinin ... tarih ve E: ..., K: ... sayılı davanın reddi yolundaki kararının temyizden incelenerek bozulması istenilmektedir.

YARGILAMA SÜRECİ:

Dava konusu istem: Davacı Sendika tarafından, EGO Genel Müdürlüğü bünyesindeki kamu çalışanlarının faaliyet gösterdiği servislerde uygulanan kameralı takip sistemine son verilmesi istemiyle yapılan başvurunun reddine ilişkin ... tarih ve ... sayılı işlemin iptali istenilmektedir.

İlk Derece Mahkemesi kararının özeti: ... İdare Mahkemesinin ... tarih ve E: ..., K: ... sayılı kararıyla; kamu hizmeti görevini yerine getiren memur ve diğer kamu görevlilerinin kamuya sunulan bu faaliyeti ifa ettikleri ve bu hizmetin yürütüldüğü binaların kamuya açık olup bu yerlerde kamu hizmetine özgü olarak çalışma yapıldığı, kamu hizmetinin sunulduğu yerler ve hizmeti gören memur ve kamu görevlilerinin bu hizmeti vermekle yükümlü idarelerin gözetimi ve denetimi altında olduğu, idarelerin hizmet binalarında, kamu hizmeti ve yararına yönelik olarak gerekli gördükleri önlemleri almakla yetkili ve görevli oldukları, somut olayda kamu görevlilerince kamuya yönelik olarak kamu hizmeti verilen açık ofis sistemine sahip EGO Genel Müdürlüğü'nün hizmet binasının çalışma ortamının denetim ve güvenliğini sağlamaya yönelik olarak salonun tamamına hakim olacak şekilde kamera sistemi kurulmasında, sözü edilen hizmeti vermekle yükümlü davalı idarenin kamu yararı

ve hizmet gerekleri doğrultusunda hareket ettiği sonucuna varıldığından dava konusu işlemlerde hukuka aykırılık bulunmadığı gerekçesiyle davanın reddine karar verilmiştir.

TEMYİZ EDENİN İDDİALARI: Davacı tarafından, özel hayatın sadece konuttan ibaret olmayıp hiç beklenmedik zamanda ortaya çıkan ve süreklilik arz eden bir süreç olduğu, çalışma hayatının da özel hayat kapsamında değerlendirilmesi gerektiği, iş yerinin güvenliğini sağlama amacını aşır doğrudan çalışan memurların kendisinin ve diğer memurlarla ya da iş sahipleriyle ilişkisinin ve kamu hizmetlerinin görülmesi sırasında yaptığı her türlü haberleşmenin gözlenmesinin açıkça hukuka aykırı olduğu, bu nedenle Mahkeme kararının bozulması gerektiği ileri sürülmektedir.

KARŞI TARAFIN SAVUNMALARI: Davalı EGO Genel Müdürlüğü tarafından, haksız ve hukuki dayanağı bulunmayan temyiz isteminin reddi gerektiği savunulmaktadır. Diğer davalı Ankara Büyükşehir Belediye Başkanlığı tarafından savunma verilmemiştir.

DANIŞTAY TETKİK HÂKİMİ: ...

DÜŞÜNCE: Temyiz isteminin kabulü ile Mahkeme kararının bozulması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay Onuncu Dairesince, Danıştay Sekizinci Dairesinin 09/05/2019 tarihli gönderme kararı ile Dairemize gönderilen dava dosyasında tetkik hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereği görüldü:

İNCELEME VE GEREKÇE:

MADDİ OLAY:

Davacı sendika tarafından, EGO Genel Müdürlüğü nezdinde çalışan personelin şikayetleri üzerine bazı müdürlüklerde çalışanların kamera ile takibi şeklinde uygulama başlatıldığı öğrenildiği, bu uygulamanın giriş, çıkış, koridor, bahçe gibi yerlerin güvenlik açısından doğal yaşamı koruyacak şekilde izlenmesi bir gereklilik olarak görülebilir ise de binanın tüm oda, birim ve bölümlerinin kamera ile takip edilmesinin Anayasal normlara ve İnsan Hakları Avrupa Sözleşmesinin 8. maddesine aykırı bulunduğu bahisle kamera ile takip uygulamasından vazgeçilmesi istemiyle 28/04/2011 tarihli dilekçeyle başvuruda bulunulduğu, davalılardan Ankara Büyükşehir Belediyesinin ... tarih ve ... sayılı işlemleriyle başvuru ile ilgili yapılacak herhangi bir işlem olmadığından istemin reddine karar verilmesi üzerine dava konusu işlemin iptali istemiyle bakılmakta olan davanın açıldığı görülmektedir.

İLGİLİ MEVZUAT:

Türkiye Cumhuriyeti Anayasası'nın 2. maddesinde belirtilen hukuk devleti, insan haklarına dayalı ve adaletli bir hukuk düzeni kurup bunu geliştiren, temel hak ve özgürlüklerin kullanılması ve korunmasından ödün vermeyen, her türlü eylem ve işleminin hukuka uygun olduğu, hukuku devletin bütün organlarına ve kurumlarına egemen kılan, kendi koyduğu kurallarla kendisini bağlı sayan ve bu durumun yargı makamları tarafından denetlenmesini olmazsa olmaz gören devlettir.

Anayasa'nın "Devletin temel amaç ve görevleri" başlıklı 5. maddesinde, "Devletin temel amaç ve görevleri, Türk milletinin bağımsızlığını ve bütünlüğünü, ülkenin bölünmezliğini, Cumhuriyeti ve demokrasiyi korumak, kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak; kişinin temel hak ve hürriyetlerini, sosyal hukuk devleti ve adalet ilkeleriyle bağdaşmayacak surette sınırlayan siyasal, ekonomik ve sosyal engelleri kaldırmaya, insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmaktır." hükmüne, "Temel hak ve hürriyetlerin niteliği" başlıklı 12. maddesinde, "Herkes, kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlere sahiptir. Temel hak ve hürriyetler, kişinin topluma, ailesine ve diğer kişilere karşı ödev ve sorumluluklarını da ihtiva eder" hükmüne, ve "Temel hak ve hürriyetlerin sınırlanması" başlıklı 13. maddesinde, "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz." hükmüne yer verilmiştir.

Yine, "Özel Hayatın Gizliliği" başlıklı 20. maddesinde "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kağıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakim onayına sunulur. Hakim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar." hükmü bulunmaktadır.

Avrupa İnsan Hakları Sözleşmesinin "Özel Hayatın ve Aile Hayatının Korunması" başlıklı 8. maddesinde, herkesin özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahip olduğu, bu hakkın kullanılmasına bir kamu makamının müdahalesinin, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik

refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabileceği kurala bağlanmış; Birleşmiş Milletler Medeni ve Siyasal Haklar Sözleşmesi'nin "Mahremiyet Hakkı" başlıklı 17. maddesinde de, hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemeyeceği; onuru veya itibarının hukuka aykırı saldırılara maruz bırakılmayacağı, herkesin bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahip olduğu belirtilmiştir.

Türk Ceza Kanunu'nun "Özel hayatın gizliliğini ihlal" başlıklı 134. maddesinde "Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.", "Kişisel verilerin kaydedilmesi" başlıklı 135. maddesinde ise "Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir." hükümleri yer almaktadır.

Ceza Muhakemesi Kanunu'nun "İletişimin tespiti, dinlenmesi ve kayda alınması" başlıklı 135. maddesinde, bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişiminin dinlenebileceği ve kayda alınabileceği; "Teknik araçlarla izleme" başlıklı 140. maddesinde ise, maddede belirtilen suçların işlendiği hususunda somut delillere dayanan kuvvetli şüphe sebepleri bulunması ve başka suretle delil elde edilememesi hâlinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyerinin teknik araçlarla izlenebileceği, ses veya görüntü kaydının alınabileceği, teknik araçlarla izlemeye hâkim, gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından karar verilebileceği hükümleri bulunmaktadır.

HUKUKİ DEĞERLENDİRME:

Davacı tarafından, yapılan uygulamanın ve tesis edilen işlemin özel hayatın gizliliğini ihlal ettiği ve bu nedenle hukuka aykırı olduğu ileri sürülerek İdare Mahkemesi kararının temyizden incelenerek bozulması istenilmektedir.

Davacının temyiz gerekçesi olarak özel hayatın gizliliği ve mahremiyet hakkını ileri sürmüş olması dikkate alındığında, davanın incelenmesinde öncelikle özel hayat kavramının mahkeme kararları da dikkate alınarak Anayasal ve yasal açıdan değerlendirilmesi ve bu hakkın sınırlarını da ortaya koyacak şekilde çerçevesinin çizilmesi gerekmektedir.

Anayasa Mahkemesinin özel hayatın gizliliği ve mahremiyet hakkını dikkate alarak vermiş olduğu Başvuru No:2014/12591, Başvuru No:2014/11218, Başvuru No:2016/431 kararlarında şu tespitler yer almıştır:

Özel hayat kavramı eksiksiz bir tanımı bulunmayan geniş bir kavramdır. Bu kapsamda korunan hukuki değer esasen kişisel bağımsızlıktır. Özel hayata saygı hakkının kapsamının belirlenmesinde "bireyin kişiliğini geliştirmesi ve gerçekleştirilmesi" kavramı temel alınmaktadır. Anılan hak, herkesin istenmeyen bütün müdahalelerden uzak kendine özel bir ortamda yaşama hakkına sahip olduğuna işaret etmekle birlikte, kişiliğin serbestçe geliştirilmesiyle uyumlu birçok hukuki menfaati de içermektedir.(Serap Tortuk, B. No: 2013/9660, 21/1/2015, §§ 31-36; Bülent Polat [GK], B. No: 2013/7666, 10/12/2015, §§ 61-63; Tefik Türkmen [GK], B. No: 2013/9704, 3/3/2016, §§ 50-52; Ata Türkeri, B. No: 2013/6057, 16/12/2015, §§ 30-32).

Özel hayata saygı hakkı kapsamında korunan hukuksal çıkarlardan biri de bireyin mahremiyet hakkıdır. Özel hayata saygı hakkı, ilişki kurmak ve geliştirmek üzere çevresinde bulunanlarla temas kurma hakkını da içermektedir. Kişilerin mesleki hayatı özel hayatlarıyla sıkı bir irtibat içindedir. Özel hayata dair hususlar kişinin mesleği ile ilgili tasarruflara esas alınmışsa özel hayata saygı hakkı gündeme gelecektir. (Bülent Polat, § 62; Ata Türkeri, § 31)

Gelişen teknolojinin, kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması amacıyla, kamu kesiminde kullanılmaya başlanması doğaldır. Ancak; teknoloji kullanılarak kişisel görüntülerin kayıt altına alınmasında özel hayatın gizliliği ve kişilerin mahremiyet hakkı da dikkate alınarak uygulama yapılması gerektiğinde kuşku ve duraksamaya yer bulunmamaktadır.

Buna ek olarak, kamu çalışanlarının faaliyet yürüttüğü servislerde, çalışanların çalışma alanlarını ve dolayısıyla çalışanları görecektir şekilde yerleştirilen, güvenlik ve suçun önlenmesi gibi nedenlerle uygulandığı ileri sürülen kameralı takip sistemleri kullanılarak kişisel görüntülerin alınması, temel hak ve hürriyetler içerisinde sayılan özel hayatın gizliliği ilkesi kapsamında özel hayata müdahale olarak ele alınmalı, bu müdahalenin hukuka uygunluğunun değerlendirmesi ise kanunilik, ölçülülük gibi anayasal kavramlar yanında Avrupa İnsan Hakları Mahkemesi kararları ve Anayasa Mahkemesi kararları dikkate alınarak yapılmalıdır.

Yukarıda anılan müdahale, Anayasa'nın 13. maddesinde belirtilen koşulları yerine getirmediği müddetçe aynı zamanda Anayasa'nın 20. maddesinin ihlalini de teşkil edecektir.

Anayasamızın 13. maddesi "Temel hak ve hürriyetler, ... yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, ... demokratik toplum düzeninin... gereklerine ve ölçülülük ilkesine aykırı olamaz. " şeklindedir.

Bu sebeple müdahalenin ihlal oluşturup oluşturmadığının belirlenmesinde, Anayasa'nın 13. maddesinde öngörülen ve somut başvuruya uygun düşen kanunlar tarafından öngörülme, Anayasa'nın ilgili maddesinde belirtilen nedenlere dayanma, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmama koşulları yönünden inceleme yapılması gerekir.

Anayasa'nın 13. maddesi, temel hak ve özgürlüklerin sınırlandırılmasını, ilgili hak ve özgürlüğe ilişkin Anayasa maddesinde gösterilen özel sınırlandırma sebeplerinin bulunmasına bağlı kılmıştır. Bununla birlikte Anayasa Mahkemesinin kararlarına göre, özel sınırlama nedeni öngörülmemiş olan hakların dahi, hakkın doğasından kaynaklanan bazı sınırları bulunmaktadır. Ayrıca Anayasa'nın diğer maddelerinde yer alan kurallara dayanılarak da bu hakların sınırlanması mümkün olabilmektedir. Buna göre, Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebileceği kabul edilmektedir (AYM, E.2014/87, K.2015/112).

Anayasa'nın 20. maddesinin 1. fıkrası yönünden özel sınırlama nedeni düzenlenmemiştir. Maddenin 2. fıkrasında, birtakım sınırlama sebeplerine yer verilmiş olmakla beraber bu sebepler sadece arama ve elkoyma tedbirlerine yöneliktir. Dolayısıyla bu sebeplerin özel hayata saygı hakkının tüm boyutları yönünden uygulanması mümkün görünmemektedir.

Bu durumda, Anayasa'nın diğer maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin somut olay bakımından sınırlandırma sebebi olarak kabul edilip edilemeyeceği araştırılmalıdır.

Anayasa'nın 5. maddesinde, "Devletin temel amaç ve görevleri, Türk Milletinin bağımsızlığını ve bütünlüğünü, ülkenin bölünmezliğini, Cumhuriyeti ve demokrasiyi korumak, kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak; kişinin temel hak ve hürriyetlerini, sosyal hukuk devleti ve adalet ilkeleriyle bağdaşmayacak surette sınırlayan siyasal, ekonomik ve sosyal engelleri kaldırmaya, insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmaktır. " denilmektedir. Buna göre kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak devletin temel amaç ve görevlerindedir.

Kişinin ve toplumun refah, huzur ve mutluluğunu sağlamanın ön koşulu milli güvenlik ve kamu düzeninin tesisidir. Milli güvenlik ve kamu düzeninin sağlanmadığı bir ortamda, hak ve

özgürlüklerden gereği gibi yararlanılması, kişinin maddi ve manevi varlığını geliştirmesi mümkün değildir. Devletin hak ve özgürlükleri koruma ödevinin yanında, milli güvenliği ve kamu düzenini sağlama görevi de bulunmaktadır.

Yukarıda ifade edilen sınırlama nedenleri de dikkate alındığında uyuşmazlığın sağlıklı çözümü için; sınırlandırmanın, "demokratik toplum düzeninin gereklerinden olması" ve "ölçülülük ilkesine uygun olması"nın ne anlama geldiğinin de ortaya konması gerekmektedir.

"Demokratik toplum düzeninin gereklerinden olma, bir sınırlamanın demokratik bir toplumda zorlayıcı bir toplumsal ihtiyacın karşılanması amacına yönelik olmasını ifade etmektedir. Buna göre sınırlayıcı tedbir, bir toplumsal ihtiyacı karşılamıyorsa ya da başvurulabilecek son çare niteliğinde değilse demokratik toplum düzeninin gereklerine uygun bir tedbir olarak değerlendirilemez. (AYM, E.2015/96, K.2016/9, 10/2/2016 § 13; ifade özgürlüğü bağlamında Bekir Coşkun [GK], B. No: 2014/12151, 4/6/2015, § 51; özel hayatın gizliliği hakkı bağlamında Ata Türkeri, § 44; İ.F.A., B. No: 2013/8564, 17/2/2016, § 62).

Bu kapsamda kamu makamlarının faaliyetin niteliği ve sınırlamanın amacına göre değişen geniş bir takdir yetkisinin bulunması doğaldır. Ancak özel hayatın gizliliği hakkının mahremiyet hakkı gibi en gizli yönleri söz konusu olduğunda kamu makamlarının takdir yetkisi daha dardır ve bu alanlara yönelik müdahalelerin haklı olduğunun kabul edilebilmesi için kamu makamlarınca özellikle ciddi gerekçelerin gösterilmesi gerekir. (Ata Türkeri, § 47).

Kamu makamlarının özel hayata müdahaleleriyle ilgili olarak, müdahaleye yol açan karar alma sürecinde de keyfi davranmadıklarını kanıtlamaları gereklidir. Ancak bu halde de sınırlandırmanın ölçülülük ilkesine uygun olması gereklidir. (Ata Türkeri, § 48).

Anayasa Mahkemesi kararları uyarınca ölçülülük ilkesi, sınırlayıcı önlemin öngörülen amaç için zorunlu ve amaca ulaşmaya elverişli olmasını ayrıca amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder. Ölçülülük ilkesinin amacı da temel hak ve özgürlüklerin gereğinden fazla sınırlandırılmasının önlenmesidir (AYM, E.2015/102, K.2016/151, 7/9/2016, § 22; E.2012/100, K.2013/84, 4/7/2013; Marcus Frank Cerny, B. No: 2013/5126, 2/7/2015, § 72).

Kamu makamlarının özel hayata saygı hakkına keyfi bir şekilde müdahale etmelerinin önlenmesi, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi ile sağlanan güvenceler kapsamında yer almaktadır. Avrupa İnsan Hakları Mahkemesi (AİHM), devletin özel hayata saygı hakkı kapsamında bulunan bir menfaate müdahale ettiğini tespit ettiğinde, 8. maddenin 2. fıkrasında belirtilen koşulları incelemektedir. Buna göre kamu makamlarının müdahalesinin yasal bir dayanağı olup olmadığı,

anılan fıkrada yer alan meşru amaçlara dayalı olup olmadığı, demokratik bir toplumda gerekli ve öngörülen amaçla orantılı olup olmadığı araştırılmaktadır. (AİHM Dudgeon/Birleşik Krallık, § 43; Olsson/İsveç No.1, B. No: 10465/83, 24/3/1988, § 59)

Ayrıca, AİHM kararlarına göre Sözleşme'nin 8. maddesi açıkça usul şartları içermemekle birlikte anılan maddeyle güvence altına alınan haklardan etkili bir şekilde yararlanılabilmesi için müdahaleyi doğuran karar alma sürecinin bu maddeyle korunan hak ve özgürlüklere gerekli saygıyı sağlayacak nitelikte ve adil olması gerekir. Bu şekildeki bir süreç başvuruçunun 8. maddedeki haklarını -deliller ve kanıtlanma konuları dahil- adil şartlarda savunabileceği usule ilişkin etkili güvencelerden yararlandırılmasını gerektirir. AİHM'e göre bu şekildeki güvencelerin amacı 8. maddede yer alan haklara keyfi şekilde müdahalede bulunulmasını önlemek, müdahalenin gerekçelendirilmesini sağlamaktır (AİHM Ciubotaru/Moldova, B. No: 27138/04, 27/4/2010, § 51; T.P. ve K.M./Birleşik Krallık, B. No: 28945/95, 10/5/2001, § 72).

Avrupa İnsan Hakları Mahkemesi' ne göre gerek negatif yükümlülükler gerekse pozitif yükümlülükler bakımından söz konusu usule ilişkin etkili güvencelerin sunulması gerekmektedir. (Benzer yöndeki AİHM kararı için bkz. Hokkanen/Finlandiya, B.No: 19823/92, 23/9/1994, §§ 55-58; Glaser/Birleşik Krallık, B. No: 32346/96, 19/9/2000, §§ 63-66; Bajrami/Arnavutluk, B. No: 35853/04, 12/12/2006, §§ 50-55; Abdulaziz, Cabales ve Balkandali/Birleşik Krallık, B. No: 9214/80, 28/5/1985, § 67).

Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesi'nin "Mahremiyet Hakkı" başlıklı 17. maddesinde de, hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemeyeceği; onuru veya itibarının hukuka aykırı saldırılara maruz bırakılmayacağına, herkesin bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahip olduğu belirtilmiştir.

Avrupa İnsan Hakları Mahkemesinin Antovic ve Mirkovic v. Sırbistan ve Karadağ (Başvuru No. 70838/13) kararında, çalıştıkları anfi alanlarına demirbaş ve öğrenciler de dahil kişi güvenliğinin sağlanması amacıyla kamera sistemi kurulan iki profesörün özel hayatlarının gizliliğinin ihlal edildiğine karar verilmiştir. Kararda özellikle Avrupa İnsan Hakları Mahkemesinin daha öncede benzer konularda vermiş olduğu kararlara atıfta bulunularak bazı tespitlere de yer verilmiştir.

Bu tespitler arasında özellikle kişilerin iş yerinde ve çalışma ortamında yani kamusal bir alanda bulunsa da, özel hayatın profesyonel aktiviteler ve dış dünya ile ilişkileri de kapsayan ve Avrupa İnsan Hakları Mahkemesinin "sosyal özel hayat" olarak adlandırdığı bir alanı da kapsadığı ve bu alanın da korunması gerektiği, kamera sistemleri ile kişilerin sosyal özel hayatlarının izlenmesinin

"ciddi bir müdahale" olarak kabul edilmesi gerektiği, kişilerin güvenliği veya işverenin hakları başka yollarla korunamıyorsa ancak son çare olarak kamera sistemlerinin kişilerin çalışma alanlarını görece şekilde kurulmasının kabul edilebilir olacağı tespitlerine yer verilmiştir. Yine Avrupa İnsan Hakları Mahkemesinin Lopez Ribalba ve Ötekiler v. İspanya (Başvuru No. 1874/13) kararında da işverenin başka yollarla korunabilecek haklarını kamera sistemi yoluyla korumasının son çare olduğu, bu durumda bile kamera sistemleri ile ilgili olarak bildirimde bulunması ve usulleri belirlemesi gerektiği vurgulanmıştır.

Yine yukarıda yer verilen kararlardan, farklı güvenlik önlemleri yoluyla korunabilecek haklar veya önlenebilecek olaylara yönelik olarak kamera sistemleri kurulmaması gerekeceği ve çalışanların doğrudan çalışma alanlarını görüntüleme şeklinde kişilerin özel hayatına müdahale anlamına gelen bu sistemlerin bu durumlarda kullanılmaması gerekeceği, aksinin ölçülülük ilkesine aykırı olacağı sonucuna ulaşılmaktadır.

Avrupa İnsan Hakları Mahkemesi kararlarında yukarıda ifade edilen Antovic ve Mirkovic v. Sırbistan ve Karadağ (Başvuru No. 70838/13) kararında da yer aldığı gibi kamera sistemleri ile ilgili olarak belli başlı şartların ortaya konulması gerektiği de ifade edilmiştir. Bunlar özellikle uygulamanın kanuni bir dayanağının olması, sınırlı bir izleme olması ve kötüye kullanmaya karşı garantilerin olması gerektiğidir.

Türk Ceza Kanunu'nun 134. ve 135. maddeleri ile Ceza Muhakemesi Kanunu'nun 135. maddesindeki düzenlemeler, suça yönelik kuvvetli şüphe halinde bile en son çare olarak ses ve görüntü kaydına başvurulması gerektiğini ortaya koymaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanunu, 07/04/2016 tarih ve 29677 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Dava konusu işlem tarihinde yürürlükte bulunmamakla beraber konunun önemine binaen, dava konusu edilen kamera sistemleri ile ilgili belli başlı düzenlemelere de yer vermiştir. Kanunla, neden bu sisteme ihtiyaç duyulduğunun ortaya konulması, sistemden kimin veya kimlerin yasal olarak sorumlu olduğunun belirlenmesi, sisteminin maksada uygun olup olmadığının ortaya konulması, özel hayatın gizliliğinin ihlal edilip edilmediğini kimin kontrol edeceğinin ve görüntülere kimin ulaşımı olacağına belirlenmesi ve bu hususların kayıt altına alınması, kayıtların güvenliğinin ve gizliliğinin sağlanması, güvenlik prosedürleri hazırlanması, kameralarla gözlemlenen bölgelerin girişinde ve içerideki uygun yerlerde bölgenin kamera sistemleri tarafından gözetlendiği ve kayıt altına alındığının belirtilmesi gerektiği, sistemin kuruluş maksadıyla bağdaşmayan görüntülerin gereğinden uzun süre saklanmaması, kişilerin özel hayatının gizliliğinin

sağlanması yönünde beklentisinin olabileceği, görüntülerin yetkili kişiler haricinde hiç kimse tarafından izlenememesi için alınacak önlemler gibi bir çok konuda düzenleme getirilmiştir.

Tüm bu açıklamalar ışığında dava konusu işlem incelendiğinde, Avrupa İnsan Hakları Mahkemesi kararları da dikkate alındığında hakların korunması başka şekilde sağlanamıyorsa kamera sistemlerinin çalışanların çalışma alanlarını görecektir şekilde kurulmasının mümkün olduğu ancak bunun bir son çare olarak değerlendirildiği ve bu düzenlemenin içeriğini ayrıntılı olarak ortaya koyan özel bir düzenleyici işlem olması gerektiği, kamera sistemlerinin çalışma alanlarını çekmesinin özel hayatın gizliliğini ihlal ettiği, sınırlı bir izleme sağlayacak şekilde güvenlik amacıyla giriş ve çıkışları izlemek üzere veya vatandaşlara da açık olan ortak alanlar ve iş sahiplerinin de giriş çıkışına açık, yoğun bir alışveriş trafiği olan alanlarda kurulabileceği ancak bu kameraların da çalışanların iş yapış şekillerini denetlemek veya sürekli olarak belli kişileri çekecek şekilde kurulmaması gerektiği, güvenlik amacıyla kurulmuş olmaları gerektiği ve bu nedenle amaca hizmet eder şekilde konumlandırılması gerektiği anlaşılmaktadır.

Yine kamera sistemlerinin zorunlu güvenlik amacı ile ve başka bir yolla bu güvenlik amacı sağlanamıyorsa kurulabilmesi mümkün olsa da, yukarıda yer verilen açıklamalar ışığında uygulamanın usul ve esaslarını gösteren kanuni dayanağının bulunması, açık ve anlaşılabilir olması ve ilgililerin bu konudaki hakları ve kamera sistemi ile ilgili olarak bilgilendirilmiş olması gerektiği, toplanan görüntülerle ilgili güvencelerin sağlanması gerektiği, dava konusu işlemin bu haliyle sınırları belirlenmemiş, kanuni dayanağı olmayan, uygulamaya dair usul ve esaslar ile güvenceleri düzenlenmemiş bir sistemle yürütüldüğü ve bu haliyle kamu yararına yönelik olduğunu kabul etmeye imkan olmadığı; Anayasal bir ilke olan ölçülülük ilkesine aykırılık teşkil ettiği ve mahremiyet hakkını ihlal ettiği anlaşılmakta olup, kişilik haklarına aykırı şekilde kamu görevlilerinin tüm faaliyetlerinin izlenmesine imkan tanıyan uygulamada isabet bulunmamaktadır.

Kameralı takip sistemi ile kurumca amaçlanan kamu yararı arasında orantılılık bulunmadığından uygulama ölçülülük ilkesine de aykırılık teşkil etmektedir. Anayasa'nın 13. maddesinde, temel hak ve hürriyetlerin ancak kanunla sınırlanabileceği, değişik 20/3. maddesinde de, kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceğinin belirtildiği, ancak konuyla ilgili dava konusu işlemin gerçekleştirildiği aşamada kanuni bir düzenlemenin yapılmadığı anlaşılmaktadır.

İdarelerin teknolojik gelişmelerden de yararlanarak kamu çalışanlarının faaliyet yürüttüğü alanda güvenlik ve suçun önlenmesi amacıyla kameralı takip sistemi uygulaması, güvenlik amacı ile giriş ve çıkışlar gibi alanlar dışında kameraların çalışanların çalışma odalarını ve servisleri çekecek şekilde

yerleştirildiği durumlarda, kamusal alanda da olsa "özel hayatın gizliliği" ilkesi kapsamında bulunduğu Avrupa İnsan Hakları Mahkemesi kararları ve Dairemizin daha önceki tarihli kararlarından anlaşılmaktadır. Yine uygulamanın sınırlarını, usul ve esaslarını gösteren bir kanuni dayanağın bulunması, toplanan görüntülerin ileride başka bir şekilde kullanılamayacağına dair bir güvencenin mevcut olması gerektiği de anlaşılmaktadır.

İdarenin güvenlik ve kamu yararını sağlama ihtiyacı ve çalışanların özel hayatın gizliliği gibi haklarının karşı karşıya geldiği bu gibi uyuşmazlıklarda, olayın dosyaya özel olarak ele alınması ve değerlendirilmesi gerektiği açıktır.

Uyuşmazlığın bu davaya özgü hali değerlendirildiğinde; İdare Mahkemesi'nce, ... tarihli ara kararı ile davalı idareden EGO Genel Müdürlüğü binasında yer alan tüm kameraların hangi birimlerde ve birimler haricinde nerelerde yer aldığı bildirilmesinin ve söz konusu kameralara ilişkin kamera kayıt örneklerinin görüntülerini içeren CD'nin istenildiği, davalı idare tarafından daha önce Dairemizin E:2019/12230 sayılı dosyasında mevcut kamera görüntülerinin incelenmesinden, yerleştirilen kameraların bina ve koridor çevresini görüntülemeye, çevre güvenliğine ve binaya yönelik tehlikelerin tespitine yönelik olduğu belirtilmiş olmasına rağmen; davalı idarenin ara kararına verdiği cevap yazısı ekindeki kamera listesi ve CD içeriğinde yer alan kamera görüntülerinde ise, bunların masalarda ve bankolarda çalışan personeli doğrudan gören ve izleyen şekilde olduğu, kamera sisteminin yerleştirildiği konum ve çektiği alan dikkate alındığında, iş yerinin güvenliğini sağlama amacını aşarak, doğrudan çalışan memurun kendisinin, diğer memurlarla ya da iş sahipleriyle ilişkisinin ve kamu hizmetinin görülmesi sırasında yaptığı her türlü haberleşmesinin, çalışma alanı ve masasının gözlemlendiği kamera takip sistemi kurulmasının özel hayatın gizliliğini ihlal ettiği anlaşılmakta olup; uygulamanın sınırlarını, usul ve esaslarını gösteren bir kanuni dayanağın bulunmaması, toplanan görüntülerin ileride başka bir şekilde kullanılamayacağına dair bir güvencenin mevcut olmaması ve bu haliyle yukarıda belirtilen temel haklar ve Anayasal ilkelerle bağdaşmaması nedeniyle dava konusu işlemin iptaline karar verilmesi gerekirken davanın reddi yolunda verilen mahkeme kararının hukuka aykırı olduğu sonucuna varılmıştır.

KARAR SONUCU:

Açıklanan nedenlerle;

1. Davacının temyiz isteminin kabulüne,
2. Davanın reddine ilişkin temyize konu ... İdare Mahkemesinin ... tarih ve E: ..., K: ... sayılı kararının BOZULMASINA,

3. Yeniden bir karar verilmek üzere dosyanın anılan Mahkemeye gönderilmesine,
4. 2577 sayılı Kanun'un (Geçici 8. maddesi uyarınca uygulanmasına devam edilen) 54. maddesinin birinci fıkrası uyarınca bu kararın tebliğ tarihini izleyen günden itibaren 15 (on beş) gün içinde karar düzeltme yolu açık olmak üzere, 11/01/2021 tarihinde oybirliğiyle karar verildi.

Danıştay Kararı - 12. Daire (E. 2019/7364)

Danıştay Kararı - 12. D., E. 2019/7364 K. 2020/3108 T. 30.9.2020

T.C. DANIŞTAY ONİKİNCİ DAİRE

Esas No: 2019/7364

Karar No: 2020/3108

TEMYİZ EDEN (DAVACI): ...

VEKİLİ: Av. ...

KARŞI TARAF (DAVALI): ... Bakanlığı / ...

VEKİLİ: Av. ...

İSTEMİN KONUSU: ... Bölge İdare Mahkemesi ... İdari Dava Dairesinin ... tarih ve E:..., K:... sayılı kararının temyizen incelenerek bozulması istenilmektedir.

YARGILAMA SÜRECİ:

Dava konusu istem: ...Terörizmle Mücadele Eğitim ve Tatbikat Merkezi Komutanlığında uzman erbaş kursiyeri olan davacı tarafından, güvenlik soruşturmasının olumsuz sonuçlandığından bahisle sözleşmesinin feshedilmesine ilişkin 09.11.2018 tarih ve MRK.Ş.:17217803-1930-2586020-18 sayılı işleminin iptali ile mahrum kaldığı parasal hakların geriye dönük yasal faiziyle birlikte ödenmesine karar verilmesi istenilmiştir.

İlk Derece Mahkemesi kararının özeti: ... İdare Mahkemesince verilen ... tarih ve E:..., K:... sayılı kararda; dava konusu olayda, davacı hakkında "Kullanmak İçin Uyuşturucu ve Uyarıcı Madde Kabul Etmek veya Bulundurmak" suçundan suça sürüklenen çocuk sıfatıyla yapılan yargulamada ... Asliye Ceza Mahkemesi'nin ... tarih ve E:..., K:... sayılı kararıyla "... çocuğun uyuşturucu madde kullandığı ve hakkında verilen tedavi ve denetimli serbestlik kurallarına uymadığı anlaşılmakla neticeten 1 Yıl 1 Ay 10 Gün hapis cezasıyla cezalandırılmasına, Hükmün Açıklanmasının Geri Bırakılmasına ve 3 Yıllık Denetim Süresi Belirlenmesine..." karar verildiği, söz konusu kararın itiraz başvurusunun da reddedilerek 24.12.2015 tarihinde kesinleştiğinin görüldüğü, bu durumda, idarenin yapısı ve icra ettiği faaliyetin niteliği gereği askeri personele ilişkin özel durumları değerlendirilmek suretiyle davacı hakkındaki güvenlik soruşturması ve arşiv araştırması sonucu elde edilen istihbari bilgide

belirtilen, kullanmak için uyuşturucu ve uyarıcı madde kabul etmek veya bulundurmak suçunun vasıf ve mahiyeti de dikkate alındığında bu durumun askerlik göreviyle bağdaşmayacak nitelikte olduğu sonucuna varıldığından davacının güvenlik soruşturmasının olumsuz sonuçlanması nedeniyle sözleşmesinin feshedilmesine ilişkin dava konusu işlemde hukuka aykırılık bulunmadığı gerekçesiyle davanın reddine karar verilmiştir.

Bölge İdare Mahkemesi kararının özeti: ... Bölge İdare Mahkemesi ... İdari Dava Dairesince; istinaf başvurusuna konu ...İdare Mahkemesi kararının hukuka ve usule uygun olduğu ve davacı tarafından ileri sürülen iddiaların söz konusu kararın kaldırılmasını sağlayacak nitelikte görülmediği gerekçesiyle 2577 sayılı İdari Yargılama Usulü Kanunu'nun 45. maddesinin üçüncü fıkrası uyarınca istinaf başvurusunun reddine karar verilmiştir.

TEMYİZ EDENİN İDDİALARI: Davacı tarafından, dava konusu işlemin hukuka aykırı olduğu, mahkumiyet kararının bulunmadığı, Bölge İdare Mahkemesi kararının bozulması gerektiği ileri sürülmektedir.

KARŞI TARAFIN SAVUNMASI: Davalı idare tarafından, dava konusu işlemin hukuka uygun olduğu, idare tarafından takdir hakkının mevzuata uygun olarak kamu yararı gözetilerek en uygun adaydan yana kullanıldığı belirtilerek istemin reddi gerektiği savunulmuştur.

DANIŞTAY TETKİK HÂKİMİ: ...

DÜŞÜNCE: Temyiz isteminin kabulü ile Bölge İdare Mahkemesi kararının bozulması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay Onikinci Dairesince, Tetkik Hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra, dosya tekemmül ettiğinden yürütmenin durdurulması istemi hakkında ayrıca bir karar verilmeksizin işin gereği görüldü.

İNCELEME VE GEREKÇE:

MADDİ OLAY:

Dosyanın incelenmesinden; ... Terörizmle Mücadele Eğitim ve Tatbikat Merkez Komutanlığında uzman erbaş olan davacı hakkında yapılan güvenlik soruşturması ve arşiv araştırması neticesinde elde edilen "...Kullanmak İçin Uyuşturucu ve Uyarıcı Madde Kabul Etmek veya Bulundurmak suçundan 1 yıl 1 ay 10 gün hapis, HAGB, 3 yıl denetimli serbestlik..." yönündeki bilgi notuna istinaden güvenlik soruşturmasının olumsuz sonuçlandırıldığı, güvenlik soruşturmasının olumsuz

sonuçlandığı gerekçesiyle sözleşmesi feshedilerek ilişkisinin kesilmesi üzerine de bakılan davanın açıldığı anlaşılmaktadır.

İLGİLİ MEVZUAT:

Anayasa'nın "Özel hayatın gizliliği" başlıklı 20. maddesinin birinci fıkrasında;

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz" hükmüne, üçüncü fıkrasında; "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilmiştir.

Avrupa İnsan Hakları Sözleşmesinin "Özel ve aile hayatına saygı hakkı" başlıklı 8. maddesinde de;

"(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir," hükmü yer almaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 6. maddesinde;

"(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü yer almaktadır.

5352 sayılı Adli Sicil Kanunu'nun 10. maddesinin üçüncü fıkrasında, "Onsekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebilir. " hükmü yer almaktadır.

07/09//2005 tarihli ve 25929 sayılı Resmi Gazete'de yayımlanan Adli Sicil Yönetmeliği'nin 12. maddesinin dördüncü fıkrasında, "Onsekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere mahkeme, hâkim veya savcılıklarca istenebilir." hükmü ile 14. maddesinin birinci fıkrasında, "Onsekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere mahkeme, hâkim veya savcılıklara talep halinde verilir." hükmü yer almaktadır.

HUKUKİ DEĞERLENDİRME:

Anayasa Mahkemesi'nin 27/02/2019 tarihli ve 2014/7256 Başvuru no'lu kararında özetle;

"..Somut olayda başvurucunun on sekiz yaşından küçükken işlediği suçun kayıtlarının ... Valiligi Emniyet Müdürlüğü tarafından Komisyon Başkanlığına verildiği, bu kaydın dikkate alınmak suretiyle güvenlik soruşturmasının olumsuz sonuçlandığı, başvurucunun sözleşmeli infaz ve koruma memurluğuna atamasının yapılmadığı anlaşılmaktadır.

Resmi makamlar tarafından muhafaza edilmekte olan, başvurucu hakkında yürütülen ceza yargılamasına dair bilgilerin özel hayata saygı hakkı anlamında kişisel nitelikli veriler olduğu açıktır. Söz konusu kişisel verinin kamu kurumlarıyla paylaşılması ve güvenlik soruşturmalarında kullanılmasının Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkına bir müdahale oluşturduğu sonucuna varılmıştır...

...Öte yandan somut olayda başvurucunun yazılı ve sözlü sınavı kazandığının ilan edilmiş olduğu, on sekiz yaşından küçükken işlediği suça ilişkin kaydın 5352 sayılı Kanun'un 10. maddesinin (3) numaralı fıkrasında yer alan hükme açıkça aykırı şekilde idari makamlara verilmiş olduğu dikkate alındığında özel hayata saygı hakkına yönelik müdahalenin bu yönüyle de kanuni dayanaktan yoksun olduğu anlaşılmaktadır..." değerlendirmelerine yer verilmiştir.

Dosya içerisinde yer alan bilgi ve belgeler ile Anayasa Mahkemesi kararı doğrultusunda dava konusu olay incelendiğinde, 13/05/1997 doğumlu olan ve hakkındaki ceza mahkûmiyetine konu suçu işlediği 05/12/2014 tarihinde on sekiz yaşından küçük olan davacının, on sekiz yaşından küçükken işlediği bu suça ilişkin kayıtların Valilik tarafından ... Bakanlığı' na verilmesi üzerine, ilgili kurum tarafından bu

kaydın dikkate alınması suretiyle davacı hakkındaki güvenlik soruşturmasının olumsuz sonuçlandığı görülmüştür.

Bu durumda, davacının adli sicil kaydında görünmeyen, on sekiz yaşından küçükken işlediği suça ilişkin kaydın, yukarıda yazılı Kanun ve Yönetmelik hükümleri uyarınca, ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebileceği açık olduğundan, kişisel veri niteliğinde olan bu kaydın, güvenlik soruşturması kapsamında ilgili kamu kurumuna verilmesi ve güvenlik soruşturmasında kullanılması hukuka aykırı olduğundan, hukuka aykırı şekilde idari makamlara verilen bu kaydın değerlendirilmesi suretiyle güvenlik soruşturmasının olumsuz sonuçlandırılması, Anayasa'nın 20. maddesi ve Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi uyarınca "özel hayata saygı hakkının" ihlâli sonucunu doğurmaktadır.

Bu itibarla, davacının on sekiz yaşından küçükken işlediği suça ilişkin kayda dayanılarak güvenlik soruşturmasının olumsuz sonuçlanması suretiyle sözleşmenin feshedilmesine ilişkin dava konusu işlemde hukuka uyarlık, davanın reddine ilişkin İdare Mahkemesi kararına karşı yapılan istinaf başvurusunun reddi yönündeki Bölge İdare Mahkemesi kararında hukuki isabet görülmemiştir.

KARAR SONUCU:

Açıklanan nedenlerle;

1. 2577 sayılı Kanun'un 49. maddesine uygun bulunan davacının temyiz isteminin kabulüne,
2. Davanın yukarıda özetlenen gerekçeyle reddine ilişkin ... İdare Mahkemesi kararına karşı yapılan istinaf başvurusunun reddi yolundaki temyize konu ... Bölge İdare Mahkemesi ... İdari Dava Dairesinin ... tarih ve E:..., K:... sayılı kararının BOZULMASINA,
3. Davacının adli yardım talebi kabul edildiğinden temyiz aşamasında yapılan posta giderinin davalı idareden tahsili için mahkemesince müzekkere yazılmasına,
4. Yeniden bir karar verilmek üzere dosyanın ... Bölge İdare Mahkemesi ... İdari Dava Dairesine gönderilmesine, (karar düzeltme yolu kapalı olmak üzere) 30/09/2020 tarihinde oybirliğiyle karar verildi.

Danıştay Kararı - 12. Daire (E. 2019/7283)

Danıştay Kararı - 12. D., E. 2019/7283 K. 2020/3109 T. 30.9.2020

TEMYİZEDEN(DAVACI): K1

VEKİLİ: Av. K2

KARŞITARAF(DAVALI): Milli Savunma Bakanlığı / ANKARA

VEKİLİ: Av. K3

İSTEMİN KONUSU: Konya Bölge İdare Mahkemesi 4. İdari Dava Dairesince verilen 16/10/2019 tarihli, E:2019/1237, K:2019/994 sayılı kararının temyizden incelenerek bozulması istenilmektedir.

YARGILAMA SÜRECİ:

Dava konusu istem: Isparta Terörle Mücadele Eğitim ve Tatbikat Merkez Komutanlığı'nda sözleşmeli uzman erbaş kursiyeri olarak eğitim görmekte olan davacı tarafından, güvenlik soruşturmasının olumsuz sonuçlandığından bahisle sözleşmesinin feshedilmesine ilişkin 09.01.2019 tarih ve MRK.Ş.17217803-1930-62803-18 sayılı işlemin iptali istenilmiştir.

İlk Derece Mahkemesi kararının özeti:Isparta İdare Mahkemesince verilen 30/05/2019 tarih ve E:2019/47, K:2019/747 sayılı kararda; bakılan uyuşmazlıkta, davacı hakkında "Kamu Kurum ve Kuruluşlarında Bulunan Eşya Hakkında Hırsızlık" suçundan yapılan ceza yargılaması neticesinde Çekerek Asliye Ceza Mahkemesinin 04.05.2016 tarih ve E:2014/61, K:2016/154 sayılı kararıyla "4 ay 13 gün hapis cezası ile cezalandırılmasına, hapis cezası adli para cezasına çevrilerek 133 gün adli para cezası ile cezalandırılmasına (2660 TL adli para cezası), hükmün açıklanmasının geri bırakılmasına ve 3 yıl denetimli serbestlik tedbirine tabi tutulmasına" karar verildiği, kararın 27.06.2016 tarihinde kesinleştiği, davacının mahkum olduğu suçun, yukarıda yer verilen 3269 sayılı Uzman Erbaş Kanunu'nun 12. ve Yönetmeliğin 6. maddelerinde sayılan suçlardan olduğu anlaşıldığından davacının uzman erbaş sözleşmesinin feshedilmesine ilişkin dava konusu işlemde hukuka aykırılık bulunmadığı gerekisiyle davanın reddine karar verilmiştir.

Bölge İdare Mahkemesi kararının özeti: Konya Bölge İdare Mahkemesi 4. İdari Dava Dairesince; istinaf başvurusuna konu Isparta İdare Mahkemesi kararı hukuka ve usule uygun olduğundan, istinaf isteminin, incelemeye konu Isparta İdare Mahkemesi'nin 30/05/2019 tarih ve E:2019/47, K:2019/747 sayılı kararının 2.sayfasının 3.parağrafının son cümlesinde yer alan "...mahkum olduğu

suçun..." ifadesinin çıkarılarak bahse konu ifadenin; "...sabit görülen fiilin,..." şeklinde düzeltilerek reddine karar verilmiştir.

TEMYİZ EDENİN İDDİALARI: Davacı tarafından, sözleşmenin feshedilmesi ne gerekçe olan suçun on sekiz yaşından küçükken işlendiği ve Anayasa Mahkemesi kararlarına göre sözleşmenin feshine gerekçe olamayacağı bu nedenle dava konusu işlemin hukuka aykırı olduğu , Bölge İdare Mahkemesi kararının bozulması gerektiği ileri sürülmektedir.

KARŞI TARAFIN SAVUNMASI: Davalı idare tarafından, dava konusu işlemin hukuka uygun olduğu belirtilerek istemin reddi gerektiği savunulmuştur.

DANIŞTAY TETKİK HÂKİMİ: K4

DÜŞÜNCESİ: Temyiz isteminin reddi ile usul ve yasaya uygun olan Bölge Mahkemesi kararının onanması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay Onikinci Dairesince, Tetkik Hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra, dosya tekemmül ettiğinden yürütmenin durdurulması istemi hakkında ayrıca bir karar verilmeksizin işin gereği görüşüldü.

İNCELEME VE GEREKÇE:

MADDİ OLAY:

Dava dosyasının incelenmesinden; davacının Isparta Terörizmle Mücadele Eğitim ve Tatbikat Merkezi Komutanlığında uzman erbaş olarak eğitim görmekte iken hakkında yapılan güvenlik soruşturması ve arşiv araştırması neticesinde elde edilen "Kamu kurum ve kuruluşlarındaki eşya hakkında hırsızlık suçundan 133 gün adli para cezası (2660 TL) HAGB, 3 yıl denetimli serbestlik" şeklindeki bilgi notuna istinaden Aday Değerlendirme Kurulu kararıyla güvenlik soruşturmasının olumsuz sonuçlandırılması nedeniyle 09.01.2019 tarihli işlemle sözleşmesinin feshedilmesi üzerine bakılan davanın açıldığı anlaşılmaktadır.

Davacı hakkında verilen ceza mahkemesi kararından sonra üç yıllık denetim süresinin dolması üzerine davacı tarafından 02.07.2019 havale tarihli dilekçe ile yapılan başvuru üzerine Çekerek Asliye Ceza Mahkemesi'nin 1610.2019 tarihli ve E:2019/127, K:2019/154 sayılı kararı ile davanın düşmesine karar verilmiştir.

İLGİLİ MEVZUAT:

Anayasa'nın "Özel hayatın gizliliği" başlıklı 20. maddesinin birinci fıkrasında;

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz" hükmüne, üçüncü fıkrasında; "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilmiştir.

Avrupa İnsan Hakları Sözleşmesinin "Özel ve aile hayatına saygı hakkı" başlıklı 8. maddesinde de;

"(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir," hükmü yer almaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 6. maddesinde;

"(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü yer almaktadır.

5352 sayılı Adli Sicil Kanunu'nun 10. maddesinin üçüncü fıkrasında, "Onsekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebilir. " hükmü yer almaktadır.

07/09//2005 tarihli ve 25929 sayılı Resmi Gazete'de yayımlanan Adli Sicil Yönetmeliği'nin 12. maddesinin dördüncü fıkrasında, "Onsekiz yaşından küçüklerle ilgili adli sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere mahkeme, hâkim veya savcılıklarca istenebilir." hükmü ile 14. maddesinin birinci fıkrasında, "Onsekiz yaşından küçüklerle ilgili adli sicil ve arşiv kayıtları ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere mahkeme, hâkim veya savcılıklara talep halinde verilir." hükmü yer almaktadır.

HUKUKİ DEĞERLENDİRME:

Anayasa Mahkemesi'nin 27/02/2019 tarihli ve 2014/7256 Başvuru no'lu kararında özetle;

"..Somut olayda başvurucunun on sekiz yaşından küçükken işlediği suçun kayıtlarının Adana Valiliği Emniyet Müdürlüğü tarafından Komisyon Başkanlığına verildiği, bu kaydın dikkate alınmak suretiyle güvenlik soruşturmasının olumsuz sonuçlandığı, başvurucunun sözleşmeli infaz ve koruma memurluğuna atamasının yapılmadığı anlaşılmaktadır.

Resmi makamlar tarafından muhafaza edilmekte olan, başvurucu hakkında yürütülen ceza yargılamasına dair bilgilerin özel hayata saygı hakkı anlamında kişisel nitelikli veriler olduğu açıktır. Söz konusu kişisel verinin kamu kurumlarıyla paylaşılması ve güvenlik soruşturmalarında kullanılmasının Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkına bir müdahale oluşturduğu sonucuna varılmıştır...

Öte yandan somut olayda başvurucunun yazılı ve sözlü sınavı kazandığının ilan edilmiş olduğu, on sekiz yaşından küçükken işlediği suça ilişkin kaydın 5352 sayılı Kanun'un 10. maddesinin (3) numaralı fıkrasında yer alan hükme açıkça aykırı şekilde idari makamlara verilmiş olduğu dikkate alındığında özel hayata saygı hakkına yönelik müdahalenin bu yönüyle de kanuni dayanaktan yoksun olduğu anlaşılmaktadır..." değerlendirmelerine yer verilmiştir.

Dosya içerisinde yer alan bilgi ve belgeler ile Anayasa Mahkemesi kararı doğrultusunda dava konusu olay incelendiğinde, 03/08/1998 doğumlu olan ve hakkındaki ceza mahkûmiyetine konu suçu işlediği 15/11/2013 tarihinde on sekiz yaşından küçük olan davacının, on sekiz yaşından küçükken işlediği bu suça ilişkin kayıtların Valilik tarafından Milli Savunma Bakanlığı'na verilmesi üzerine, ilgili kurum tarafından bu kaydın dikkate alınması suretiyle davacı hakkındaki güvenlik soruşturmasının olumsuz sonuçlandığı görülmüştür.

Bu durumda, davacının adli sicil kaydında görünmeyen, on sekiz yaşından küçükken işlediği suça ilişkin kaydın, yukarıda yazılı Kanun ve Yönetmelik hükümleri uyarınca, ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya

mahkemelerce istenebileceđi açık olduđundan, kiřisel veri niteliđinde olan bu kaydın, güvenlik soruřturması kapsamında ilgili kamu kurumuna verilmesi ve güvenlik soruřturmasında kullanılması hukuka aykırı olduđundan, hukuka aykırı řekilde idari makamlara verilen bu kaydın deđerlendirilmesi suretiyle güvenlik soruřturmasının olumsuz sonulandırılması, Anayasa'nın 20. maddesi ve Avrupa İnsan Hakları Szleşmesi'nin 8. maddesi uyarınca "zel hayata saygı hakkının" ihlli sonucunu dođurmaktadır.

Bu itibarla, davacının on sekiz yařından kken iřlediđi sua iliřkin kayda dayanılarak güvenlik soruřturmasının olumsuz sonulanması suretiyle szleşmenin feshedilmesine iliřkin dava konusu iřlemdede hukuka uyarlık, davanın reddine iliřkin İdare Mahkemesi kararına karřı yapılan istinaf bařvurusunun reddi ynndeki Blge İdare Mahkemesi kararında hukuki isabet grlmemiřtir.

KARAR SONUCU:

Aıklanan nedenlerle;

1. 2577 sayılı Kanun'un 49. maddesine uygun bulunan davacının temyiz isteminin kabulne,
2. Davanın yukarıda zetlenen gerekeyle reddine iliřkin Isparta İdare Mahkemesi kararına karřı yapılan istinaf bařvurusunun reddi yolundaki temyize konu Konya Blge İdare Mahkemesi 4. İdari Dava Dairesince verilen 16/10/2019 tarihli, E:2019/1237, K:2019/994 sayılı kararının BOZULMASINA,
3. Kullanılmayan 89,60.-TL yrtmeyi durdurma harcının istemi hlinde davacıya iadesine,
4. Yeniden bir karar verilmek zere dosyanın Konya Blge İdare Mahkemesi 4. İdari Dava Dairesine gnderilmesine, (karar dzeltme yolu kapalı olmak zere) 30/09/2020 tarihinde oybirliđiyle karar verildi.

Danıştay Kararı - 10. Daire (E. 2019/7114)

Danıştay Kararı - 10. D., E. 2019/7114 K. 2020/7147 T. 29.12.2020

T.C. DANIŞTAY ONUNCU DAİRE

Esas No: 2019/7114

Karar No: 2020/7147

DAVACI: ... Birliği

VEKİLLERİ: Av. ..., Av. ...

DAVALI: ... Bakanlığı

VEKİLLERİ: Hukuk Müşaviri Av. ...

Hukuk Müşaviri Av. ...

DAVANIN KONUSU: Davacı tarafından, 12/12/2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 3. maddesi ile değiştirilen asıl Yönetmeliğin 19. maddesinin 3. fıkrasının; 4. maddesi ile değiştirilen 27. maddesinin 8. fıkrasının; 5. maddesi ile değiştirilen ek 1. maddesinin 16. fıkrasının; 5. maddesi ile ek 1. maddesine eklenen 18. fıkrasının; 8. maddesi ile değiştirilen EK-9'daki 1 sayılı Liste ve 2 sayılı Listenin iptali istenilmektedir.

DAVACININ İDDİALARI:

Dava konusu Yönetmeliğin 3. maddesi ile değiştirilen asıl Yönetmeliğin 19. maddesinin 3. fıkrası bakımından; yan dal uzmanı olan hekimlerin, sahip oldukları uzmanlık diplomalarına dayalı olarak özel hastanelerde mesleklerini icra etme olanaklarının yasal dayanağı olmaksızın sınırlandırıldığı, Bakanlığın konuyu hangi kriterlere göre değerlendireceği, bu değerlendirmeyi ne kadar süre içerisinde yapacağı hususlarına yer verilmediğinden hekimler yönünden yaratılan belirsizlik ve keyfi uygulamaların önünün açıldığı, özel sağlık kuruluşlarında çalışacak yan dal unvanına sahip bir hekimin çalışma izninin, kamudaki yan dal uzmanlığına sahip eğitici ihtiyacının bulunmaması koşuluna bağlı kılındığı, oysa yasalar ile atama usulü özel olarak belirlenmiş eğitici kadrolarına, kamu ile bağı bulunmayan hekimlerin doğrudan atanmasının söz konusu olmadığı, kişiler eğitici olmak istemezlerse zorla kamusal eğitim kadrolarına atanmalarının söz konusu olamayacağı,

akademik kadrolar için aranan tek niteliğin de yan dal uzmanlığı olmadığı, Kanunda tanınan hekimlik yetkisini normlar hiyerarşisine aykırı biçimde ortadan kaldıran, hukuki güvenlik ilkesini, hekimlerin maddi ve manevi varlığını geliştirme hakkını, bilim ve sanatı serbestçe öğrenme hakkını ve çalışma hak ve özgürlüğünün özünü zedeleyen düzenlemede hukuka uyarlık bulunmadığı;

4. maddesi ile değiştirilen asıl Yönetmeliğin 27. maddesinin 8. fıkrası bakımından; 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesi üzerine hastanın rızası dahi aranmaksızın ve sınırsız biçimde sağlık verilerinin toplanması anlamına gelen dava konusu düzenlemenin tesis edildiği, 6698 sayılı Kanun'un uygulanabilmesi için gereken kurum ve kurullar oluşturulmadan, bu kurul tarafından belirlenmesi gereken önlemler tanımlanmadan, veri sorumlusu sicili oluşturulmadan alana ilişkin düzenleme yapılmasının hukuka aykırı olduğu, dava konusu düzenlemede "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Sözleşme"de yer verilen istisnalardan hiçbirine yer verilmediği, sağlık politikalarına yön vermek için sağlık hizmeti verilerinin kişisel bilgilerden arınmış bir şekilde anonim hale getirilip toplanabileceği, dava konusu değişikliğin uygulamayı göstermekten uzak olduğu;

5. maddesi ile değiştirilen asıl Yönetmeliğin ek 1. maddesinin 16. fıkrası bakımından; bazı koşullarda hekimin diğer bir ilde çalışmasının söz konusu olabileceği ancak, bu hakkın koşullarının daima güncel olarak değerlendirilmesi ve düzenlenmesi gerektiği, Yönetmeliğin ise bu içerikten yoksun olduğu, söz konusu değişikliğin yeni bir hekim istihdamı yerine işverenin bir çok sorumluluktan kurtulması için ticari kaygılara dayalı olarak yapıldığı, birden çok ilde çalışmanın hekimin esas görevinin yanı sıra diğer ek görevlerinde de veriminin azalmasına ve mesleki uygulama sorunlarına yol açacağı, hekimin hastalarını takip edebilmesinin ve hastanın da hekime ulaşmasının zorlaşacağı;

5. maddesi ile asıl Yönetmeliğin ek 1. maddesine eklenen 18. fıkrası bakımından; değişikliğin özel sağlık kuruluşlarında çalışan tabip/uzman tabiplerin başka bir özel hastanede çalışmasını nöbetle sınırlandırdığı, özel sağlık kuruluşunda nöbet tutabilmek için bir sağlık kuruluşunda çalışıyor olmanın zorunlu hale getirildiği, özel hastanelerde çalışanların nöbet dışında başka bir sağlık kuruluşunda çalışabilmesinin kurumsal sözleşmeye bağlı kılındığı, 1219 sayılı Kanun'un 12. maddesinde tanınan hakkın nöbetle sınırlanmasının mümkün olmadığı, düzenlemenin Yönetmeliğin ek 1. maddesinin 2. fıkrasında yer alan hüküm ile de çeliştiği, bu hükmü örtülü bir biçimde yürürlükten kaldırdığı, maddede ayrıca özel hastane kadrosunda çalışan tabibin başka bir özel hastane ya da tıp merkezinde kısmi zamanlı çalışabilmesi için kurumsal sözleşme yapılmasının ve çalışacak hekimin muvafakat vermesinin gerekliliğinin düzenlendiği, söz konusu düzenleme ile hekimin iradesinin yok sayıldığı, bu şekilde çalışmanın işverenin iradesine bağlı kılındığı, özel

hastane sahibinin zincir hastane veya anlaşmalı olduğu bir başka sağlık kuruluşu ile anlaşarak hekimin ikinci bir yerde çalışmasını zorunlu kılacağı, işten atılma tehdidi karşısında hekimin muvafakat vermemesinin olanaklı olmadığı, planlama amacıyla yapılan bu düzenlemenin bu amaca değil ticari kaygılara hizmet edeceği, parçalı istihdamına karar verilen hekimin mesai sonrası nöbet tutmak zorunda bırakılmasının angarya yasağının ihlali anlamına geldiği, bunun toplum sağlığını da tehdit edeceği;

8. maddesi ile değiştirilen asıl Yönetmeliğin eki EK-9'daki 1 sayılı Liste ve 2 sayılı Liste bakımından; tıbbın dinamik bir alan olduğu, sürekli değişim ve gelişim gösteren bu alanda yapılabilecek olan işlemlerin sayma yoluyla belirlenmesinin olanaklı olmadığı, yapılabilecek işlemleri sayma yoluyla gösteren düzenlemenin genel, sürekli ve soyut olamayacağı, bu haliyle çalışma hakkını ve sağlık hizmetlerine ulaşım hakkını sınırlayan bir metin olduğu, düzenlemenin hukuki güvenlik ve belirlilik ilkelerine dolayısıyla hukuk devleti ilkesine aykırı olduğu, düzenleme yapılırken uzmanlık deneklerinden ve meslek örgütlerinden görüş alınmadığı, düzenlenmenin bilimsel bir çalışmaya dayanmadığı,

iddia edilerek anılan düzenlemelerin iptali istenilmektedir.

DAVALININ SAVUNMASI:

Dava konusu Yönetmeliğin 3. maddesi ile değiştirilen asıl Yönetmeliğin 19. maddesinin 3. fıkrası bakımından; dava konusu değişiklik ile Planlama İstihdam Komisyonu ibaresinin madde metninden çıkarıldığı, yapılan değişikliğin bundan ibaret olduğu, düzenlemenin amacının, yan dal insan kaynağının ülkemizde oldukça kısıtlı olması, yan dal uzmanlığı konusunda önceliğin yan dala ilişkin uzmanlık eğitimine verilmesinin gerekmesi ve yan dal uzmanlık eğitiminin kaliteli bir şekilde verilebilmesi için yeterli uzman kaynağının eğitim kurumlarında mutlaka sağlanması gerekliliği nedeniyle yan dal uzmanlık eğitiminin sürdürülebilirliğinin sağlanması olduğu, yan dal ve ana dalın birlikte çalışmasının ihtiyaç ve zorunluluk olduğu, hizmet gereği kamu hastaneleri ve üniversite hastanelerinde ana dal ve yan dal uzman kaynağının korunması gerektiği, düzenlemenin eğitim kurumlarında yan dal uzman insan gücünü korumak için yapıldığı, bu eğitim kurumlarının yan dal uzman ihtiyacı karşılandığında yan dal uzmanlarının özel sektörde ana dalda çalışabilecekleri, örneğin ülke ve ilde eğitici ihtiyacı bulunmayan algoloji gibi yan dallarda anadal uzmanlık kadrolarında çalışmasına izin verildiği, düzenlemenin kamu yararı amacı güttüğü;

4. maddesi ile değiştirilen asıl Yönetmeliğin 27. maddesinin 8. fıkrası bakımından; kanunkoyucu tarafından, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyenlerin yükümlülükleri ile uyacakları usul ve

esasları belirlemek üzere 6698 sayılı Kanun'un yürürlüğe girdiği, bu Kanun'la 663 sayılı Kanun Hükmünde Kararnamenin 47. maddesinin yeniden düzenlendiği, bu düzenlemelerin Anayasa Mahkemesince Anayasa'ya uygun bulunduğu, Anayasa'ya uygun bulunan bir Kanun hükmünün uygulanacağını gösteren Yönetmelik hükmünün uygulanmasının yargı kararı ile engellenemeyeceği, dava konusu düzenlemenin 6698 sayılı Kanun'a yapılan atıftan ibaret olduğu, kişisel verilere yönelik yeni bir hüküm ihtiva etmediği, davacının iddia ettiğinin aksine hükmün yayımlandığı tarihte Kişisel Verileri Koruma Kurulunun oluşturulduğu, Kurul tarafından bu alana ilişkin önlemlerin belirlendiği;

5. maddesi ile değiştirilen asıl Yönetmeliğin ek 1. maddesinin 16. fıkrası bakımından; düzenleme ile özel sağlık kuruluşlarında meslek icrasının aynı il içerisinde sınırlandırılmayarak hekimlerin iller arasında çalışmalarına izin verildiği, hükmün hekimlerin aleyhine değil lehine olduğu, düzenlemenin 1219 sayılı Kanun'un 12. maddesi hükmüne aykırı olmadığı, nitekim tabiplerin birden fazla sağlık kuruluşunda çalışmasına yönelik Yönetmelikte süre ve yer yönünden öngörülen kısıtlamaların 1219 sayılı Kanun'un 12. maddesine aykırı bulunarak Danıştayca iptal edildiği;

5. maddesi ile asıl Yönetmeliğin ek 1. maddesine eklenen 18. fıkrası bakımından; maddede nöbet ve kurumsal sözleşmeye ilişkin düzenleme yapıldığı, özel sağlık kuruluşlarında çalışan tabip ve uzman tabiplerin başka bir özel hastanede çalışmasının sadece nöbetle sınırlandırılmadığı, Yönetmeliğin ek 1. maddesinin 2. fıkrası ile bulunduğu ilde birden fazla özel sağlık kuruluşunda çalışabilmelerine, ek 1. maddenin 16. fıkrası kapsamında da iller arası çalışmalarına izin verildiği, bunların yanı sıra nöbet tutarak çalışmanın da hekimlerin lehine bir düzenleme olarak Yönetmeliğe eklendiği, ayrıca hüküm ile hekimlerin tıp merkezlerinde planlama kapsamında kadrolu çalışmaları halinde kurumsal sözleşme yaparak diğer özel sağlık kuruluşlarında çalışabileceğinin belirtildiği, hekimlerin çalışmasına yönelik herhangi bir kısıtlama getirilmediği, tüm tıp merkezlerinin sabitlenen kadroları doğrultusunda kadrolu çalışma halinde sözleşmeli çalışmanın da söz konusu olabileceğinin kurala bağlandığı, kurumsal sözleşmenin maksadının planlama kapsamındaki kısıtlı tabip insan gücünün özel sektör içinde kullanılabilmesi ve böylece sağlık hizmeti sunumunda verimin, ulaşılabilirliğin ve kalitenin artması olduğu, bu çalışmanın hekimin bilgisi ve isteği dışında olmadığı, kurumsal sözleşme ve hekimin muvafakati şartının getirildiği, hükümde hekimlerin çalışma şartlarını zorlaştıran ya da ağırlaştıran bir düzenleme bulunmadığı, düzenlemenin kamu hizmeti gerekleri gözetilerek yapıldığı;

8. maddesi ile değiştirilen asıl Yönetmeliğin eki EK-9'daki 1 sayılı Liste ve 2 sayılı Liste bakımından; tıp merkezlerinde yapılabilecek ve yapılamayacak işlemler listesinin, ilgili cerrahi uzmanlık dallarından hekimlerin katılımıyla toplanan komisyon tarafından, Sağlık Uygulama Tebliği ekinde

yer alan Ek-2/C ve Ek-2/B Listeleri ve Yönetmeliğin 23. maddesi hükmü baz alınarak belirlendiği, önceki düzenlemede de listenin sayma yoluyla belirlendiği ve bu düzenlemenin Danıştay incelemesinden geçerek hukuka uygun bulunduğu, listenin her bir uzmanlık dalından uzmanlar tarafından ayrı ayrı ve tıp merkezinin standartları esas alınarak belirlendiği, listenin sayma yoluyla belirlenmesinin belirlilik ilkesine uygun olduğu, konunun muhatapları için bilinebilir ve öngörülebilir olması gerektiği

ileri sürülerek davanın reddi gerektiği savunulmaktadır.

DANIŞTAY TETKİK HAKİMİ:...

DÜŞÜNCEİ: Dava konusu düzenlemelerin kamu yararı ve hizmet gerekleri ile hukuka uygun olduğu, davanın reddi gerektiği düşünülmektedir.

DANIŞTAY SAVCISI:...

DÜŞÜNCEİ: 12/12/2017 tarih ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 3. maddesi ile değiştirilen asıl Yönetmeliğin 19. maddesinin 3. fıkrasının, anılan Yönetmeliğin 4. maddesi ile değiştirilen asıl Yönetmeliğin 27. maddesinin 8. fıkrasının; 5. maddesi ile değiştirilen asıl Yönetmeliğin Ek-1. maddesinin 16. fıkrasının; 5. maddesi ile asıl Yönetmeliğe eklenen Ek-1. maddesinin 18. fıkrasının ve 8. maddesi ile değiştirilen asıl Yönetmeliğin ekinde yer alan EK-9'daki 1 sayılı Liste ve 2 sayılı Listenin iptali istenilmektedir.

3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 1. maddesinde; kanunun amacının, sağlık hizmetleri ile ilgili temel esasları belirlemek olduğu, 2. maddesinde; Milli Savunma Bakanlığı hariç bütün kamu kurum ve kuruluşları ile özel hukuk tüzelkişileri ve gerçek kişileri kapsadığı, 3. maddesinin (a) bendinde; sağlık kurum ve kuruluşlarının yurt sathında eşit, kaliteli ve verimli hizmet sunacak şekilde Sağlık ve Sosyal Yardım Bakanlığınca, diğer ilgili bakanlıkların da görüşü alınarak plânlanacağı, koordine edileceği, mali yönden destekleneceği ve geliştirileceği, (c) bendinde; bütün sağlık kurum ve kuruluşları ile sağlık personelinin ülke sathında dengeli dağılımı ve yaygınlaştırılmasının esas olduğu, sağlık kurum ve kuruluşlarının kurulması ve işletilmesinin bu esas içerisinde Sağlık ve Sosyal Yardım Bakanlığınca düzenleneceği, (e) bendinde; tesis edilecek eğitim, denetim, değerlendirme ve oto kontrol sistemi ile sağlık kuruluşlarının tespit edilen standart ve esaslar içinde hizmet vermesinin sağlanacağı, (f) bendinde; herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi amacıyla, Sağlık Bakanlığı ve bağlı kuruluşlarınca gerekli kayıt ve bildirim sisteminin kurulacağı, bu sistemin, e-

Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabileceği, bu amaçla, Sağlık Bakanlığınca, bağlı kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemi kurulabileceği, 9. maddesinin (c) bendinde; bütün kamu ve özel sağlık kuruluşlarının tesis, hizmet, personel, kıstaslarını belirlemeye, sağlık kurum ve kuruluşlarını sınıflandırmaya ve sınıflarının değiştirilmesine, sağlık kuruluşlarının amaca uygun olarak teşkilatlanmalarına, sağlık hizmet zinciri oluşturulmasına, hizmet içi eğitim usul ve esasları ile sağlık kurum ve kuruluşlarının koordineli çalışma ve hizmet standartlarının tespiti ve denetimi ile bu Kanunla ilgili diğer hususların Sağlık ve Sosyal Yardım Bakanlığınca çıkarılacak yönetmelikle tespit edileceği belirlenmiştir.

663 sayılı -dava konusu işlemlerin tesis edildiği tarihteki adıyla- Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin yine dava konusu işlemlerin tesis edildiği tarihte yürürlükte olan haliyle 8. maddesinin birinci fıkrasının (j) bendinde; ilgili mevzuat çerçevesinde kişisel verilen korunmasına ve veri mahremiyetinin sağlanmasına yönelik düzenleme yapmak Sağlık Hizmetleri Genel Müdürlüğü'nün görevleri arasında sayılmış, 40. maddesinde ise; Bakanlık ve bağlı kuruluşların görev, yetki ve sorumluluk alanına giren ve önceden kanunla düzenlenmiş konularda idarî düzenlemeler yapabilecekleri hükmüne yer verilmiştir.

Anılan mevzuat hükümlerine dayanılarak, kaynak israfı ve atıl kapasiteye yol açılmaksızın ülke düzeyinde dengeli, verimli ve kaliteli sağlık hizmeti sunulmasını sağlamak üzere ayakta teşhis ve tedavi yapılan özel sağlık kuruluşlarının yapılandırılmaları, ruhsatlandırma işlemleri, faaliyetleri ve faaliyetlerine son verilmesi, denetimleri ve diğer hususlar ile ilgili usûl ve esasları düzenlemek amacıyla Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelik 15/02/2008 tarihli ve 26788 sayılı Resmî Gazete'de yayımlanmıştır.

12/12/2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik ile asıl Yönetmeliğin bazı maddelerinde değişiklik yapılmıştır.

Dosyanın incelenmesinden, dava konusu Yönetmeliğin 3. maddesi ile değiştirilen asıl Yönetmeliğin 19. maddesinin 3. fıkrasına ilişkin olarak; dava konusu değişiklik ile Planlama İstihdam Komisyonu ibaresinin madde metninden çıkarıldığı, yapılan değişikliğin bundan ibaret olduğu, düzenlemenin amacının, yan dal insan kaynağının ülkemizde oldukça kısıtlı olması, yan dal uzmanlığı konusunda önceliğin yan dala ilişkin uzmanlık eğitime verilmesinin gerekmesi ve yan dal uzmanlık eğitiminin kaliteli bir şekilde verilebilmesi için yeterli uzman kaynağının eğitim kurumlarında mutlaka sağlanması gerekliliği nedeniyle yan dal uzmanlık eğitiminin sürdürülebilirliğinin sağlanması olduğu, yan dal ve ana dalın birlikte çalışmasının ihtiyaç ve zorunluluk olduğu, hizmet gereği kamu

hastaneleri ve üniversite hastanelerinde ana dal ve yan dal uzman kaynağının korunması gerektiği, düzenlemenin eğitim kurumlarında yan dal uzman insan gücünü korumak için yapıldığı, bu eğitim kurumlarının yan dal uzman ihtiyacı karşılandığında yan dal uzmanlarının özel sektörde ana dalda çalışabilecekleri, örneğin ülke ve ilde eğitici ihtiyacı bulunmayan algoloji gibi yan dallarda anadal uzmanlık kadrolarında çalışılmasına izin verildiği,

Dava konusu Yönetmeliğin 5. maddesi ile değiştirilen asıl Yönetmeliğin Ek-1. maddesinin 16. fıkrasına ilişkin olarak; düzenleme ile özel sağlık kuruluşlarında meslek icrasının aynı il içerisinde sınırlandırılmayarak hekimlerin iller arasında çalışmalarına izin verildiği, hükmün hekimlerin aleyhine değil lehine olduğu, düzenlemenin 1219 sayılı Kanun'un 12. maddesi hükmüne aykırı olmadığı,

Dava konusu Yönetmeliğin 5. maddesi ile asıl Yönetmeliğe eklenen Ek-1. maddesinin 18. fıkrasına ilişkin olarak; maddede nöbet ve kurumsal sözleşmeye ilişkin düzenleme yapıldığı, özel sağlık kuruluşlarında çalışan tabip ve uzman tabiplerin başka bir özel hastanede çalışmasının sadece nöbetle sınırlandırılmadığı, Yönetmeliğin Ek 1. maddesinin 2. fıkrası ile bulunduğu ilde birden fazla özel sağlık kuruluşunda çalışabilmelerine, Ek 1. maddenin 16. fıkrası kapsamında da iller arası çalışmalarına izin verildiği, bunların yanı sıra nöbet tutarak çalışmanın da hekimlerin lehine bir düzenleme olarak Yönetmeliğe eklendiği, ayrıca hüküm ile hekimlerin tıp merkezlerinde planlama kapsamında kadrolu çalışmaları halinde kurumsal sözleşme yaparak diğer özel sağlık kuruluşlarında çalışabileceğinin belirtildiği, hekimlerin çalışmasına yönelik herhangi bir kısıtlama getirilmediği, tüm tıp merkezlerinin sabitlenen kadroları doğrultusunda kadrolu çalışma halinde sözleşmeli çalışmanın da söz konusu olabileceğinin kurala bağlandığı, kurumsal sözleşmenin maksadının planlama kapsamındaki kısıtlı tabip insan gücünün özel sektör içinde kullanılabilmesi ve böylece sağlık hizmeti sunumunda verimin, ulaşılabilirliğin ve kalitenin artması olduğu, bu çalışmanın hekimin bilgisi ve isteği dışında olmadığı, kurumsal sözleşme ve hekimin muvafakati şartının getirildiği, hükümde hekimlerin çalışma şartlarını zorlaştıran ya da ağırlaştırıcı bir düzenleme bulunmadığı,

Dava konusu Yönetmeliğin 8. maddesi ile değiştirilen asıl Yönetmeliğin ekinde yer alan EK-9'daki 1 sayılı Liste ve 2 sayılı Liste'ye ilişkin olarak; tıp merkezlerinde yapılabilecek ve yapılamayacak işlemler listesinin, ilgili cerrahi uzmanlık dallarından hekimlerin katılımıyla toplanan komisyon tarafından, Sağlık Uygulama Tebliği ekinde yer alan Ek-2/C ve Ek-2/B Listeleri ve Yönetmeliğin 23. maddesi hükmü baz alınarak belirlendiği, önceki düzenlemede de listenin sayma yoluyla belirlendiği ve bu düzenlemenin Danıştay incelemesinden geçerek hukuka uygun bulunduğu, listenin her bir uzmanlık dalından uzmanlar tarafından ayrı ayrı ve tıp merkezinin standartları esas alınarak

belirlendiği, listenin sayma yoluyla belirlenmesinin belirlilik ilkesine uygun olduğu, anlaşılacakla dava konusu bu düzenlemelerde dayanağı mevzuata ve amaçlarına aykırılık bulunmadığı sonucuna varılmıştır.

15/02/2008 tarihli ve 26788 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmeliğin 27. maddesinin 8. fıkrasında; "Sağlık kuruluşları, istenecek tıbbi kayıtları, belirlenen formata uygun şekilde ve belirli aralıklarla Bakanlığa gönderir." hükmü yer almakta iken; dava konusu değişiklik ile, "Sağlık kuruluşları tarafından kayıt altına alınan kişisel sağlık verileri, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununa uygun bir şekilde işlenir ve Bakanlıkça belirlenen usul ve esaslara uygun bir şekilde merkezi sağlık veri sistemine aktarılır. Bakanlık tarafından kurulan kayıt ve bildirim sistemine ve Bakanlıkça yapılacak diğer iş ve işlemlere esas olmak üzere, istenilen bilgi ve belgelerin Bakanlığa gönderilmesi zorunludur." şeklinde yeniden düzenlenmiştir.

Anılan değişiklik ile sağlık kuruluşları tarafından kayıt altına alınan kişisel sağlık verilerinin, 6698 sayılı Kişisel Verilerin Korunması Kanununa uygun bir şekilde işleneceği ve Bakanlıkça belirlenen usul ve esaslara uygun bir şekilde merkezi sağlık veri sistemine aktarılacağı kuralına yer verilmiştir.

07/04/2016 tarih ve 29677 sayılı Resmî Gazete'de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu, Türkiye Büyük Millet Meclisi'ne sunulan genel gerekçesinden de anlaşılacağı üzere, kişisel verilerin korunması konusunun pek çok sektörü ve kamu ya da özel kurumu ilgilendirmesi nedeniyle bir "çerçeve kanun" olarak hazırlanmıştır.

Ayrıca 2010 yılında Anayasa'nın 20. maddesinde yapılan düzenlemeyle kişisel verilerin korunması temel bir insan hakkı olarak güvence altına alınmış ve konuya ilişkin usul ve esasların kanunla düzenleneceği öngörülmüştür.

Bu bağlamda, 6698 sayılı Kanunun 21. maddesi hükümlerine göre oluşturulan Kişisel Verileri Koruma Kurulu'nun görev ve yetkileri, aynı Kanun'un 22. maddesiyle belirlenmiştir. 22. maddenin 1. fıkrasının (h) bendinde "Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek" hükmüne yer verilmiştir.

Anılan Kanun'un, "Özel nitelikli kişisel verilerin işleme şartları" başlıklı 6. maddesinin 1. fıkrasında, dava konusu Yönetmelikle düzenlenen, sağlık verilerinin de özel nitelikli kişisel veri olduğu belirtilmiş; maddenin 4. fıkrasında, "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü getirilmiştir.

Buna göre, anılan Kanun hükümleri çerçevesinde, dava konusu düzenleme tesis edildiğinde özel nitelikli kişisel veri olarak kabul edilen sağlık verilerinin işlenmesinde alınması gerekli olan önlemlerin Kişisel Verileri Koruma Kurulu tarafından belirlenmediği ve Kanun'un 22. maddesinin 1. fıkrasının (h) bendine göre diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında Kurul görüşü alınmadan dava konusu düzenlemenin tesis edildiği görülmekte olup, bu yönüyle dava konusu Yönetmelik hükmünde hukuka uygunluk bulunmamaktadır.

Bu durumda, 6698 sayılı Kişisel Verilerin Korunması Kanunu'na göre sağlık gibi özel nitelikli verilerin işlenmesinde uyulacak önlemleri belirlemekle yetkili olan Kişisel Verileri Koruma Kurulu tarafından bu alana ilişkin yeterli önlemler belirlenmeden ve mevzuat taslağı hakkında Kurul görüşü alınmadan tesis olunan dava konusu düzenlemede hukuka uyarlık bulunmamaktadır.

Açıklanan nedenle, 12/12/2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 4. maddesi ile değiştirilen asıl Yönetmeliğin 27. maddesinin 8. fıkrasının iptaline, 12/12/2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 3. maddesi ile değiştirilen asıl Yönetmeliğin 19. maddesinin 3. fıkrasının, 5. maddesi ile değiştirilen asıl Yönetmeliğin Ek-1. maddesinin 16. fıkrasının, 5. maddesi ile asıl Yönetmeliğe eklenen Ek-1. maddesinin 18. fıkrasının, 8. maddesi ile değiştirilen asıl Yönetmeliğin ekinde yer alan EK-9'daki 1 sayılı Liste ve 2 sayılı Listenin iptali isteminin reddine karar verilmesi gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay Onuncu Dairesince, duruşma için önceden taraflara bildirilen 29/12/2020 tarihinde davacıyı temsilen Av. ...'nın ve Av. ...'in, davalı ... Bakanlığını temsilen Hukuk Müşaviri Av. ...'un geldiği, Danıştay Savcısının hazır olduğu görülmekle açık duruşmaya başlandı. Taraflara usulüne uygun olarak söz verilerek dinlendikten ve Danıştay Savcısının düşüncesi alındıktan sonra taraflara son kez söz verilip, duruşma tamamlandı. Tetkik hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereği görüldü:

MADDİ OLAY VE HUKUKİ SÜREÇ:

Dava, 12/12/2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 3. maddesi ile değiştirilen asıl Yönetmeliğin 19. maddesinin 3. fıkrasının; 4. maddesi ile değiştirilen 27.

maddesinin 8. fıkrasının; 5. maddesi ile deęiştirilen ek 1. maddesinin 16. fıkrasının; 5. maddesi ile ek 1. maddesine eklenen 18. fıkrasının; 8. maddesi ile deęiştirilen EK-9'daki 1 sayılı Liste ve 2 sayılı Listenin iptali istemiyle açılmıştır.

İNCELEME VE GEREKÇE:

İlgili Mevzuat:

Anayasanın 56. maddesinin birinci fıkrasında, herkesin, sağlıklı ve dengeli bir çevrede yaşama hakkına sahip olduğu; üçüncü fıkrasında, Devletin, herkesin hayatını, beden ve ruh sağlığı içinde sürdürmesini sağlamak; insan ve madde gücünde tasarruf ve verimi artırarak, işbirliğini gerçekleştirmek amacıyla sağlık kuruluşlarını tek elden planlayıp hizmet vermesini düzenleyeceği; dördüncü fıkrasında da, Devletin, bu görevini kamu ve özel kesimlerdeki sağlık ve sosyal kurumlarından yararlanarak, onları denetleyerek yerine getireceęi hükmüne yer verilmiştir.

3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 1. maddesinde; Kanununun amacının, sağlık hizmetleri ile ilgili temel esasları belirlemek olduğu, 2. maddesinde; Milli Savunma Bakanlığı hariç bütün kamu kurum ve kuruluşları ile özel hukuk tüzelkişileri ve gerçek kişileri kapsadığı, 3. maddesinin (a) bendinde; sağlık kurum ve kuruluşlarının yurt sathında eşit, kaliteli ve verimli hizmet sunacak şekilde Sağlık ve Sosyal Yardım Bakanlığınca, diğer ilgili bakanlıkların da görüşü alınarak plânlanacağı, koordine edileceęi, mali yönden destekleneceęi ve geliştirileceęi, (c) bendinde; bütün sağlık kurum ve kuruluşları ile sağlık personelinin ülke sathında dengeli dağılımı ve yaygınlaştırılmasının esas olduğu, sağlık kurum ve kuruluşlarının kurulması ve işletilmesinin bu esas içerisinde Sağlık ve Sosyal Yardım Bakanlığınca düzenleneceęi, (e) bendinde; tesis edilecek eğitim, denetim, değerlendirme ve oto kontrol sistemi ile sağlık kuruluşlarının tespit edilen standart ve esaslar içinde hizmet vermesinin sağlanacağı, (f) bendinde; herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi maksadıyla, Sağlık Bakanlığı ve baęlı kuruluşlarınca gerekli kayıt ve bildirim sisteminin kurulacağı, bu sistemin, e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabileceęi, bu amaçla, Sağlık Bakanlığınca, baęlı kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemi kurulabileceęi, 9. maddesinin (c) bendinde; bütün kamu ve özel sağlık kuruluşlarının tesis, hizmet, personel, kıstaslarını belirlemeye, sağlık kurum ve kuruluşlarını sınıflandırmaya ve sınıflarının deęiştirilmesine, sağlık kuruluşlarının amaca uygun olarak teşkilatlanmalarına, sağlık hizmet zinciri oluşturulmasına, hizmet içi eğitim usul ve esasları ile sağlık kurum ve kuruluşlarının koordineli çalışma ve hizmet standartlarının tespiti ve denetimi ile bu Kanunla ilgili diğer hususların Sağlık ve Sosyal Yardım Bakanlığınca çıkarılacak yönetmelikle tespit edileceęi belirlenmiştir.

663 sayılı -dava konusu işlemlerin tesis edildiği tarihteki adıyla- Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin yine dava konusu işlemlerin tesis edildiği tarihte yürürlükte olan haliyle 8. maddesinin birinci fıkrasının (j) bendinde; ilgili mevzuat çerçevesinde kişisel verilen korunmasına ve veri mahremiyetinin sağlanmasına yönelik düzenleme yapmak Sağlık Hizmetleri Genel Müdürlüğü'nün görevleri arasında sayılmış, 40. maddesinde ise; Bakanlık ve bağlı kuruluşların görev, yetki ve sorumluluk alanına giren ve önceden kanunla düzenlenmiş konularda idarî düzenlemeler yapabilecekleri hükmüne yer verilmiştir.

Anılan mevzuat hükümlerine dayanılarak, kaynak israfı ve atıl kapasiteye yol açılmaksızın ülke düzeyinde dengeli, verimli ve kaliteli sağlık hizmeti sunulmasını sağlamak üzere ayakta teşhis ve tedavi yapılan özel sağlık kuruluşlarının yapılandırılmaları, ruhsatlandırma işlemleri, faaliyetleri ve faaliyetlerine son verilmesi, denetimleri ve diğer hususlar ile ilgili usûl ve esasları düzenlemek amacıyla Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelik 15/02/2008 tarihli ve 26788 sayılı Resmî Gazete'de yayımlanmıştır.

12/12/2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik ile asıl Yönetmeliğin bazı maddelerinde değişiklik yapılmıştır.

Dava konusu maddelerin incelenmesi:

1) Dava konusu Yönetmeliğin 3. maddesi ile değiştirilen asıl Yönetmeliğin 19. maddesinin 3. fıkrasının incelenmesi:

15/02/2008 tarih ve 26788 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmeliğin 9. maddesiyle, sağlık kurum ve kuruluşları ile bunlara ait sağlık insan gücü, tıbbi hizmet birimleri ve nitelikleri ile teknoloji yoğunluklu tıbbi cihaz dağılımı alanlarında kamu ve özel sektörü kapsayacak şekilde planlama yapılması öngörülmüştür. Bakanlığın planlama yapmaya yetkili olduğu hususu yerleşik yargı kararlarıyla hukuka uygun bulunmuştur.

Anılan Yönetmeliğin 19. maddesinin 3. fıkrasında;

"(Değişik:RG-14/2/2012-28204) Sağlık kuruluşu kadrosuna, ayrılanın yerine aynı uzmanlık dalında tabip başlatılabilir. (Değişik cümle:RG-30/1/2015-29252) Yan dal uzmanlığı bulunanlar, her bir yan dal uzmanlık alanında ülkedeki ve ildeki eğitim kurumlarında tıpta uzmanlık eğitimini sağlayacak şekilde Bakanlıkça belirlenen sayıda yan dal uzmanı bulunması koşuluyla ve Planlama ve İstihdam Komisyonunun uygun görüşü ile o ildeki ana dal uzmanlık kadrolarında; tıpta uzmanlık eğitimi

verilmeyen illerde ise Planlama ve İstihdam Komisyonunca belirlenecek kriterlere ve bu komisyon tarafından verilecek uygun görüşe göre o ildeki ana dal uzmanlık kadrolarında başlatılabilir. Bunun dışında kuruluşa yeni başlayacak tabip ve diğer sağlık personeli için, öncelikle mesul müdür tarafından çalışma belgesi düzenlenerek müdürlüğe onaylatılır ve çalışma belgesi onaylandığı tarihten itibaren personel sağlık kuruluşunda çalışabilir.” hükmü yer almakta iken;

12/12/2017 tarihli ve 30268 sayılı Resmî Gazete’de yayımlanan dava konusu Yönetmeliğin 3. maddesi ile anılan fıkra,

“Sağlık kuruluşu kadrosuna, ayrılanın yerine aynı uzmanlık dalında tabip başlatılabilir ancak yan dal uzmanlığı bulunanlar Bakanlığın uygun görüşü ile ana dalda başlatılabilir. Bakanlık yan dal değerlendirmesini her bir yan dal uzmanlık alanında, ülkedeki ve ildeki eğitim kurumlarının tıpta uzmanlık eğitimini sağlayacak şekilde yan dal uzmanı bulunup bulunmadığı çerçevesinde yapar. Başlatılacak personel için mesul müdür tarafından personel çalışma belgesi düzenlenerek müdürlüğe en geç beş iş günü içinde onaylatılır. Ayrılanın yerine başlayış dışındaki her türlü personel başlayışlarında ise, öncelikle mesul müdür tarafından çalışma belgesi düzenlenerek müdürlüğe onaylatılır ve çalışma belgesi onaylandığı tarihten itibaren personel sağlık kuruluşunda çalışabilir.” şeklinde değiştirilmiştir.

Bu değişikliğin Özel Hastaneler Yönetmeliğinin ek 6. maddesine göre oluşturulan ve planlama yapmakla görevli olan Planlama İstihdam Komisyonunun anılan Yönetmelikte 25/08/2016 tarihinde yapılan değişiklik ile yürürlükten kaldırılması üzerine yapıldığı, böylece planlama yapılırken Planlama İstihdam Komisyonunun görüşünü alma şartının dava konusu düzenlemeden de çıkarıldığı, yan dal uzmanlığı bulunanların sağlık kuruluşu kadrosunda ana dallarında başlatılabilmelerinin Bakanlığın uygun görüşünü alma şartına bağlandığı ve ayrıca planlama yapılırken tıpta uzmanlık eğitimi veren ve vermeyen iller ayrımından vazgeçildiği anlaşılmaktadır. Sağlık hizmetinin ülke geneline eşit ve kaliteli şekilde sunumundan birinci derece sorumlu olan idare tarafından yan dal uzmanlık eğitiminin sürdürülebilirliğinin sağlanması, özel sağlık kuruluşlarında bulunan ana dal uzman hekim kadrolarına yan dalı olan uzman hekimlerin başlatılmasına plansız bir şekilde izin verilerek kamuda ve üniversitede görev yapan mevcut yan dal uzmanlarının tümünün özelde çalışmak için ayrılma riskinin önüne geçilmesi amacıyla yapıldığı anlaşılan düzenlemede kamu yararı ve hizmet gereklerine aykırılık bulunmamaktadır.

2) Dava konusu Yönetmeliğin 4. maddesi ile değiştirilen asıl Yönetmeliğin 27. maddesinin 8. fıkrasının incelenmesi:

15/02/2008 tarihli ve 26788 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmeliğin 27. maddesinin 8. fıkrasında; "Sağlık kuruluşları, istenecek tıbbi kayıtları, belirlenen formata uygun şekilde ve belirli aralıklarla Bakanlığa gönderir." hükmü yer almakta iken; anılan fıkra dava konusu değişiklik ile, "Sağlık kuruluşları tarafından kayıt altına alınan kişisel sağlık verileri, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununa uygun bir şekilde işlenir ve Bakanlıkça belirlenen usul ve esaslara uygun bir şekilde merkezi sağlık veri sistemine aktarılır. Bakanlık tarafından kurulan kayıt ve bildirim sistemine ve Bakanlıkça yapılacak diğer iş ve işlemlere esas olmak üzere, istenilen bilgi ve belgelerin Bakanlığa gönderilmesi zorunludur." şeklinde yeniden düzenlenmiştir.

Anılan değişiklik ile sağlık kuruluşları tarafından kayıt altına alınan kişisel sağlık verilerinin, 6698 sayılı Kişisel Verilerin Korunması Kanunu'na uygun bir şekilde işleneceği ve Bakanlıkça belirlenen usul ve esaslara uygun bir şekilde merkezi sağlık veri sistemine aktarılacağı kuralına yer verilmiştir.

07/04/2016 tarih ve 29677 sayılı Resmî Gazete'de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu, Türkiye Büyük Millet Meclisi'ne sunulan genel gerekçesinden de anlaşılacağı üzere, kişisel verilerin korunması konusunun pek çok sektörü ve kamu ya da özel kurumu ilgilendirmesi nedeniyle bir "çerçeve kanun" olarak hazırlanmıştır.

Bu Kanun'a neden ihtiyaç duyulduğunu açıklayan genel gerekçede, Türk Ceza Kanunu'nun 135. ve devamı maddelerinde kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa edilmesi fiillerinin suç olarak düzenlendiği ve yaptırıma bağlandığı, ancak kişisel verilerin işlenmesine yönelik özel bir kanun bulunmaması sebebiyle, bu fiillerin ne zaman hukuka aykırı ne zaman hukuka uygun olduğunun belirlenmesinde tereddütler yaşandığı vurgulanmaktadır.

Ayrıca 2010 yılında Anayasa'nın 20. maddesinde yapılan düzenlemeyle kişisel verilerin korunması temel bir insan hakkı olarak güvence altına alınmış ve konuya ilişkin usul ve esasların kanunla düzenleneceği öngörülmüştür.

Genel gerekçede, kişisel verilerin korunmasına yönelik bir kanunî düzenleme olmamasının uluslararası ilişkiler açısından da sorunlar yarattığı, EUROPOL, EUROJUST gibi Avrupa kurumları ile ilişkilerin sekteye uğradığı, sağlık kuruluşlarınca tutulan kişisel verilerin güvenliğinin sağlanmasında yeterli yasal önlem olmamasının Avrupa İnsan Hakları Mahkemesince özel hayatın gizliliğine müdahale olarak kabul edildiği ve bu nedenle ihlal kararları verildiği belirtilmektedir. Yine genel gerekçede, bu Kanunun Türkiye'nin Avrupa Birliği'ne üyelik süreci açısından da önemine dikkat çekilmekte, Türkiye'nin, Avrupa Konseyi tarafından tüm üye ülkelerde kişisel verilerin aynı standartlarda korunması ve sınır ötesi veri akışı ilkelerinin belirlenmesi amacıyla hazırlanan 108 sayılı

"Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"ne de 1981 yılından itibaren taraf olduğu ifade edilmektedir.

Bütün bu hususlardan anlaşılacağı üzere 6698 sayılı Kanun, kişisel verilerin korunması konusunda önemli bir yasal boşluğu doldurmak amacıyla kabul edilen çerçeve niteliğinde bir yasal düzenlemedir. Genel gerekçede yer verilen şu tespit Kanun ile oluşturulan Kişisel Verileri Koruma Kurulunun genel kontrol ve denetleme işlevlerine dikkat çekmesi bakımından önemlidir: "Ülkemizde kişisel verilerin işlenmesi sürecini kontrol edecek ve denetleyecek bir kurum bulunmamaktadır. Bunun bir sonucu olarak halen kişisel veriler yeterli düzenleme ve denetime tabi olmaksızın, birçok kişi veya kurum tarafından kullanılabilmekte ve bu durum bazı hak ihlallerinin yaşanmasına sebep olabilmektedir."

Bu bağlamda, 6698 sayılı Kanun'un 21. maddesi hükümlerine göre oluşturulan Kişisel Verileri Koruma Kurulunun görev ve yetkileri, aynı Kanun'un 22. maddesiyle belirlenmiştir. 22. maddenin 1. fıkrasının (h) bendinde "Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek" hükmüne yer verilmiştir.

Anılan Kanun'un, "Özel nitelikli kişisel verilerin işleme şartları" başlıklı 6. maddesinin 1. fıkrasında, dava konusu Yönetmelikle düzenlenen, sağlık verilerinin de özel nitelikli kişisel veri olduğu belirtilmiş; maddenin 4. fıkrasında, "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü getirilmiştir.

Anılan Kanun hükümleri çerçevesinde, 03/07/2018 tarihli ara kararı ile davalı idareden, kişisel verilere ilişkin dava konusu düzenleme yapılırken Kişisel Verileri Koruma Kurulunun görüşünün alınıp alınmadığı sorulmuş, davalı idare ara kararı cevabında, Kişisel Sağlık Verilerinin Korunması ve Mahremiyetinin Sağlanması Hakkında Yönetmelik için Kişisel Verileri Koruma Kurumundan görüş sorulduğu, 6698 sayılı Kanun'un 22. maddesinin birinci fıkrasının (h) bendi uyarınca tesis edilen Kurul kararı doğrultusunda Bakanlıklarına görüş bildirildiği, dava konusu düzenlemenin de bu görüş doğrultusunda yapıldığı yönünde açıklamada bulunmuştur.

Ara kararı cevabı ekinde yer alan evraktan, 20/10/2016 tarihli ve 29863 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verilerinin Korunması ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'te değişiklik yapılması düşünüldüğünden bahisle bu değişikliklere ilişkin olarak Kişisel Verileri Koruma Kurulundan görüş istendiği ve Kurulun da bu değişikliklere yönelik davalı idareye görüş verdiği, bu görüşün dava konusu düzenlemeye yönelik verilmiş bir görüş olmadığı anlaşılmaktadır.

Buna göre, anılan Kanun hükümleri çerçevesinde, dava konusu düzenleme tesis edildiğinde özel nitelikli kişisel veri olarak kabul edilen sağlık verilerinin işlenmesinde alınması gerekli olan önlemlerin Kişisel Verileri Koruma Kurulu tarafından belirlenmediği ve Kanun'un 22. maddesinin 1. fıkrasının (h) bendine göre diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında Kurul görüşü alınmadan dava konusu düzenlemenin tesis edildiği görülmektedir.

Bu durumda, 6698 sayılı Kişisel Verilerin Korunması Kanunu'na göre sağlık gibi özel nitelikli verilerin işlenmesinde uyulacak önlemleri belirlemekle yetkili olan Kişisel Verileri Koruma Kurulu tarafından bu alana ilişkin yeterli önlemler belirlenmeden ve mevzuat taslağı hakkında Kurul görüşü alınmadan tesis olunan dava konusu düzenlemede hukuka uyarlık bulunmamaktadır.

3) Dava konusu Yönetmeliğin 5. maddesi ile değiştirilen asıl Yönetmeliğin ek 1. maddesinin 16. fıkrasının incelenmesi:

15/02/2008 tarihli ve 26788 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmeliğin ek 1. maddesinde, sağlık kuruluşlarının kalite ve verimliliğini artırmak amacıyla izin verilebilecek hususlar düzenlenmiştir.

Ek 1. maddenin 21/03/2014 tarihli Yönetmelik ile değişik 16. fıkrasında; "A ve B tipi tıp merkezinde kadrolu olarak çalışan tabipler, başka ildeki özel hastane ile A ve B tipi tıp merkezlerinde kadro dışı geçici çalışabilir. Bu durumda kadro dışı geçici çalışılan ildeki Müdürlükçe tabip adına EK-4/a'da yer alan 'Çalışma Belgesi' düzenlenir." hükmü yer almakta iken; anılan fıkra 12/12/2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan dava konusu Yönetmeliğin 5. maddesi ile; "Tıp merkezlerinde çalışan tabiplerin, başka bir ildeki özel hastanede veya tıp merkezinde hizmet vermek istemeleri halinde;

- a) Hizmet verilecek hastanenin/tıp Merkezinin tıbbi ve fiziki şartları ile personel özelliklerinin uygun olması,
- b) Tedavi edilen hastaların sonraki bakım ve destek hizmetlerinin aksatılmaması,
- c) Kadrolu çalıştıkları tıp merkezi ve hizmet sunacakları hastane/tıp merkezi ile olan sözleşmelerinde bu durumun açıkça belirtilmesi,

zorunludur. Bu durumda hizmet sunacakları hastane/tıp Merkezinin bulunduğu ildeki Müdürlükçe tabip adına EK-4/a'da yer alan 'Çalışma Belgesi' düzenlenir." şeklinde değiştirilmiştir.

Söz konusu deęişiklik ile, tıp merkezinde çalışan tabiplerin aynı zamanda başka ildeki tıp merkezleri veya özel hastanelerde çalışabilme şartları yeniden düzenlenmiştir.

Davacı tarafından, bazı koşullarda hekimin dięer bir ilde çalışmasının söz konusu olabileceęi, ancak, bu hakkın koşullarının daima güncel olarak deęerlendirilmesi ve düzenlenmesi gerektięi, Yönetmelięin ise bu içerikten yoksun olduęu, birden çok ilde çalışmanın hekimin esas görevinin yanı sıra dięer ek görevlerinde de veriminin azalmasına ve mesleki uygulama sorunlarına yol açacaęı, hekimin hastalarını takip edebilmesinin ve hastanın da hekime ulaşmasının zorlaşacaęı iddia edilerek anılan düzenlemenin iptali istenilmektedir.

1219 sayılı Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanun'un 12. maddesinde -dava konusu işlemin tesis edildięi tarihte yürürlükte olan haliyle-; "Sanatını icra etmek üzere bir mahalde kayıtlı olan herhangi bir tabibin bizzat dükkan ve mağaza açmak suretiyle her türlü ticaret yapması memnudur.

(Deęişik ikinci fıkra: 21/1/2010-5947/7 md.; Deęişik: 2/1/2014-6514/21 md.) Tabipler, diş tabipleri ve tıpta uzmanlık mevzuatına göre uzman olanlar; 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanununun 28 inci maddesi, 27/7/1967 tarihli ve 926 sayılı Türk Silâhlı Kuvvetleri Personel Kanununun ek 27 nci maddesi, 4/11/1981 tarihli ve 2547 sayılı Yükseköğretim Kanununun 36 ncı maddesi ile 17/11/1983 tarihli ve 2955 sayılı Gülhane Askeri Tıp Akademisi Kanununun 32 nci maddesi saklı kalmak kaydıyla, aşağıdaki sağlık kurum ve kuruluşlarında mesleklerini icra edebilir:

- a) Kamu kurum ve kuruluşları.
- b) Sosyal Güvenlik Kurumu ve kamu kurumları ile sözleşmeli çalışan özel sağlık kurum ve kuruluşları, Sosyal Güvenlik Kurumu ve kamu kurumları ile sözleşmeli çalışan vakıf üniversiteleri.
- c) Sosyal Güvenlik Kurumu ve kamu kurumları ile sözleşmesi bulunmayan özel sağlık kurum ve kuruluşları, Sosyal Güvenlik Kurumu ve kamu kurumları ile sözleşmesi bulunmayan vakıf üniversiteleri, serbest meslek icrası.

(Deęişik üçüncü fıkra: 21/1/2010-5947/7 md.) Tabipler, diş tabipleri ve tıpta uzmanlık mevzuatına göre uzman olanlar, ikinci fıkranın her bir bendi kapsamında olmak kaydıyla birden fazla sağlık kurum ve kuruluşunda çalışabilir. Bu maddenin uygulanması bakımından Sosyal Güvenlik Kurumunca branş bazında sözleşme yapılan özel sağlık kurum ve kuruluşları ile vakıf üniversiteleri yalnızca sözleşme yaptıkları branşlarda (b) bendi kapsamında kabul edilir. Mesleğini serbest olarak icra edenler, hizmet bedeli hasta tarafından karşılanmak ve Sosyal Güvenlik Kurumundan talep edilmemek kaydıyla, (b) bendi kapsamında sayılan sağlık kuruluşlarında da hastalarının teşhis ve

tedavisini yapabilir. (Değişik dördüncü cümle: 2/1/2014-6514/21 md.) Kamu kurum ve kuruluşlarında çalışan ve yöneticilik görevi bulunmayan tabipler ile aile hekimleri, kurum ve kuruluşlarındaki çalışma saatleri dışında ve kurumlarının izniyle aylık otuz saati geçmemek üzere iş yeri hekimliği yapabilir. Döner sermayeli sağlık kuruluşları ise kurumsal olarak işyeri hekimliği hizmeti verebilir. (Ek cümle: 2/1/2014-6514/21 md.) Tabipler, iş yeri hekimliği eğitimi alma ve iş yeri hekimliği belgesine sahip olma şartı aranmaksızın 10'dan az işçi çalıştıran az tehlikeli iş yerlerinin iş yeri hekimliği görevini yapabilirler. Bu maddenin uygulamasına ve işyeri hekimliğine ilişkin esaslar Sağlık Bakanlığınca belirlenir." hükmü yer almakta olup, bu hüküm uyarınca, tabip, diş tabibi ve tıpta uzmanlık mevzuatına göre uzman olanların, anılan maddenin ikinci fıkrasının her bir bendi kapsamında olmak kaydıyla, birden fazla sağlık kurum ve kuruluşunda çalışabilme hakkına sahip oldukları açıktır.

Dava konusu düzenleme ile, özel sağlık kuruluşlarının kaliteli ve verimli hizmet verebilmesi için planlamadan istisna olarak, maddede belirtilen koşulları sağlamaları şartıyla tabiplerin çalıştıkları il dışında başka bir ilde de mesleklerini icra etmelerine imkan sağlandığı, birden fazla yerde ve ilde çalışmanın tabiplerin ihtiyarına bırakıldığı; bu yönüyle düzenlemenin 1219 sayılı Kanun'a, hizmet gereklerine ve kamu yararına uygun olduğu anlaşıldığından, iptali istenilen maddede hukuka aykırılık görülmemiştir.

4) Dava konusu Yönetmeliğin 5. maddesi ile asıl Yönetmeliğin ek 1. maddesine eklenen 18. fıkrasının incelenmesi:

12/12/2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan dava konusu Yönetmeliğin 5. maddesi ile asıl Yönetmeliğin ek 1. maddesine eklenen 18. fıkrada; "Özel Sağlık Kuruluşlarında çalışan tabip/uzman tabipler, 1219 sayılı Kanununun 12 nci maddesine uygun olmak kaydıyla, çalıştıkları sağlık kuruluşundaki çalışma saatleri dışında bir özel hastanenin acil servis, klinik servis ve ünitelerinde nöbet tutabilir. Bu tabiplerin nöbet listesi aylık olarak düzenlenir ve Müdürlükçe onaylanır. Özel sağlık kuruluşunun kadrosunda çalışan tabip ve uzman tabipler, kadrolu çalıştıkları özel sağlık kuruluşunun çalışma saatleri dışında 1219 sayılı Kanununun 12 nci maddesine uygun olmak kaydıyla kurumsal sözleşme yapılarak diğer özel hastane veya özel sağlık kuruluşunda çalıştırılabilir. Ancak, bu durumda tabip ve uzman tabiplerin muvafakatinin alınması zorunludur. Sözleşme Müdürlüğe bildirilir ve ilgili tabip ve uzman tabiplere çalışma belgesi düzenlenir. Özel sağlık kuruluşunun kadrosunda çalışan sözleşmeye konu tabip ve uzman tabiplerin kadrodan ayrılımları halinde sözleşme sona erer." hükmü yer almaktadır.

Düzenleme ile, kadrolu çalışmanın istisnalarına bir yenisinin eklendiği, bir özel hastanede kadrolu çalışan tabibe, kurumsal sözleşme yapılarak, kadro şartı aranmaksızın başka sağlık kuruluşlarında çalışma imkânı sağlandığı, bu şekilde çalışmanın hekimin muvafakati şartına bağlandığı, ayrıca tabiplere çalıştıkları sağlık kuruluşundaki çalışma saatleri dışında bir özel hastanenin acil servis, klinik servis ve ünitelerinde nöbet tutabilme imkânı getirildiği, böylece planlama kapsamındaki kısıtlı tabip insan gücünün kaliteli ve verimli kullanılabilmesinin amaçlandığı anlaşılmalı anılan düzenlemede kamu yararı ve hizmet gerekleri ile hukuka aykırılık görülmemiştir.

5) Dava konusu Yönetmeliğin 8. maddesi ile değiştirilen asıl Yönetmeliğin eki EK-9'daki 1 sayılı Liste ve 2 sayılı Listenin incelenmesi:

12/12/2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan dava konusu Yönetmeliğin 8. maddesi ile, Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmeliğin eki EK-9 da yer alan "Tıp Merkezlerinde Gerçekleştirilebilecek Cerrahi Müdahaleler Listesi" güncellenmiş, "Sağlık Uygulama Tebliği A, B ve C Grubu Olup Ayakta Teşhis ve Tedavi Merkezlerinde Yapılabilecek İşlemler Listesi (Liste-1)" ve "Sağlık Uygulama Tebliği D ve E Grubu Olup Ayakta Teşhis ve Tedavi Merkezlerinde Yapılamayacak İşlemler Listesi (Liste-2)" adıyla iki ayrı liste yayımlanmıştır.

Dava konusu Ek-9 sayılı liste, önce 01/10/2019 tarihli ve 30905 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 23. maddesi ile daha sonra da 10/10/2019 tarihli ve 30914 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 1. maddesi ile değiştirilerek yeniden düzenlenmiştir.

Bu durumda; dava açıldıktan sonra dava konusu düzenleme değiştirilerek yeni bir düzenlemeye gidilmesi nedeniyle davanın konusuz kaldığı görüldüğünden, bu düzenlemeye ilişkin olarak davanın esası hakkında karar verilmesine yer bulunmamaktadır.

KARAR SONUCU:

Açıklanan nedenlerle;

1. 12/12/2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 4. maddesi ile değiştirilen asıl Yönetmeliğin 27. maddesinin 8. fıkrasının İPTALİNE oyçokluğuyla,

2. Anılan Yönetmeliğin; 3. maddesi ile değiştirilen asıl Yönetmeliğin 19. maddesinin 3. fıkrası, 5. maddesi ile değiştirilen asıl Yönetmeliğin ek 1. maddesinin 16. fıkrası; 5. maddesi ile asıl Yönetmeliğin ek 1. maddesine eklenen 18. fıkrası yönünden DAVANIN REDDİNE oybirliğiyle,
3. Anılan Yönetmeliğin 8. maddesi ile değiştirilen asıl Yönetmeliğin eki EK-9'daki 1 sayılı Liste ve 2 sayılı Liste yönünden KARAR VERİLMESİNE YER OLMADIĞINA oybirliğiyle,
4. Dava kısmen iptal, kısmen ret, kısmen karar verilmesine yer olmadığına şeklinde sonuçlandığından aşağıda dökümü yapılan ... TL yargılama giderinin ... TL'sinin davacı üzerinde bırakılmasına, ... TL'sinin davalı idareden alınarak davacıya verilmesine,
5. Karar tarihinde yürürlükte bulunan Avukatlık Asgari Ücret Tarifesi uyarınca duruşmalı işler için belirlenen ... TL avukatlık ücretinin davalı idareden alınarak davacıya, ... TL avukatlık ücretinin davacıdan alınarak davalı idareye verilmesine,
6. Posta gideri avansından artan tutarın kararın kesinleşmesinden sonra davacıya iadesine,
7. Bu kararın tebliğ tarihini izleyen 30 (otuz) gün içerisinde, Danıştay İdari Dava Daireleri Kuruluna temyiz yolu açık olmak üzere, 29/12/2020 tarihinde karar verildi.

KARŞI OY

(X) :

07/04/2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 21. maddesi hükümlerine göre oluşturulan Kişisel Verileri Koruma Kurulu'nun görev ve yetkileri, aynı Kanun'un 22. maddesiyle belirlenmiştir.

Mezkûr Kanun'un 22. maddenin 1. fıkrasının (h) bendinde "Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek" hükmüne yer verilmiş olup, söz konusu hükümden diğer kurum ve kuruluşlarca hazırlanacak mevzuat taslakları hakkında Kuruldan görüş alınmasının zorunlu olduğu anlamı çıkarılamaz.

Ayrıca, anılan Kanun'un 6. maddesinin 4. fıkrasında, "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü yer almaktadır. Bu hükme göre Kurul tarafından yeterli önlemlerin belirlenmemesinin diğer kurum ve kuruluşlarca düzenleyici işlem yapılmasına engel teşkil edeceği düşünülemez. Anılan hükme göre kurum ve kuruluşların, mevzuat taslaklarını hazırlarken, Kurul tarafından belirlenmiş önlemler varsa bunları dikkate alacakları konusunda kuşku yoktur. Ancak maddede sözü geçen önlemler Kurul tarafından

bir kereye mahsus kararlařtırılıp daha sonra deęiřtirilemeyecek önlemler deęildir. Kurul her zaman, belirledięi önlemleri deęiřtirebilir, uluslararası geliřmelere, zamanın gereklerine vs. göre yenilerini ekleyebilir. Kiřisel verileri iřleyenlerin, Kurul tarafından herhangi bir zamanda belirlenen önlemleri her zaman alacaęı açıktır.

Açıklanan nedenlerle, dava konusu düzenlemede bu yönüyle hukuka aykırılık bulunmadıęından dava konusu Yönetmelięin 4. maddesi ile deęiřtirilen asıl Yönetmelięin 27. maddesinin 8. fıkrası yönünden de davanın reddine karar verilmesi gerektięi oyuyla bu madde yönünden aksi yöndeki çoęunluk kararına katılmıyoruz.

Danıştay Kararı - 10. Daire (E. 2019/7092)

Danıştay Kararı - 10. D., E. 2019/7092 K. 2021/1182 T. 16.3.2021

T.C. DANIŞTAY ONUNCU DAİRE

Esas No: 2019/7092

Karar No: 2021/1182

DAVACI: ... Sendikası

VEKİLİ: Av. ...

DAVALILAR: 1- ... Bakanlığı / ...

VEKİLLERİ: Av. ...

Huk. Müş. ...

2- ... Kurumu / ...

VEKİLİ: Av. ...

DAVANIN KONUSU: 20/10/2016 tarihli ve 29863 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin 5. maddesinin 5. fıkrası ile 14. maddesinin iptali istenilmektedir.

DAVACININ İDDİALARI: Davacı tarafından; eczacıların hem elden satışlarda hem de Sosyal Güvenlik Kurumu'na yapılan satışlarda İlaç Takip Sistemine bildirimde buldukları, ilaçları hastaya sistemden onay aldıktan sonra teslim ettikleri, eczacıların reçete karşılığında İlaç Takip Sistemi ile bağlantılı eczane programları kullandıkları, bu programlar vasıtasıyla reçete kayıt defterlerinin elektronik ortamda tutulma imkânının bulunduğu, söz konusu programlar ve eczanelerin iç işleyişi sebebiyle eczanelerde kişisel sağlık verilerinin kaydedildiği, Eczacılar ve Eczaneler Hakkında Yönetmeliğin "Eczane defter ve kayıtları" başlıklı 45. maddesinin 1. fıkrasında "Eczanede satışı yapılan tüm ilaçlar elektronik ortamda kaydedilir. Bu kayıtlar denetimlerde istenilmesi hâlinde sunulmak üzere saklanır." hükmünün bulunduğu, Yönetmeliğin 5. maddesinin 5. fıkrası ile kişisel sağlık verilerinin mahremiyeti sağlanmaya çalışılırken, eczacıların özel mevzuatları ile çelişen ve uygulanması fiilen imkânsız bir yükümlülük altına sokuldukları, Yönetmeliğin 14. maddesi ile eczacıların davalı Bakanlıkça verilen yetki belgesine sahip ve Bakanlıkça belirlenen standartlar ile

uyumlu yazılımları kullanmak zorunda bırakıldığı, eczacıların halen kullandıkları piyasada mevcut programların bu özellikleri taşımadığı, bu durumun eczacıların sağlık hizmeti sunumunu aksatacağı iddia edilerek dava konusu düzenlemelerin iptali istenilmektedir.

DAVALILARIN SAVUNMALARI:

... Bakanlığı tarafından; dava konusu maddelerin hizmet gereklerine ve hukuka uygun olduğu, serbest eczane sahibi eczacıların, kişisel sağlık verisi işliyor olmaları sebebiyle Yönetmelik hükümlerine tabi olmakla birlikte, Yönetmeliğin sağlık hizmeti sunucuları için öngörülen hükümlerine tabi olmadıkları, serbest eczane sahibi eczacıların, Yönetmelik uyarınca sağlık hizmeti sunucusu olarak değerlendirilmediği, buradaki karışıklığın, Sosyal Güvenlik Kurumu mevzuatından kaynaklandığı, anılan kurum tarafından çıkartılan Sosyal Güvenlik Kurumu Sağlık Uygulama Tebliği'nin "Sağlık hizmeti sunucuları" başlıklı ve 1.4 numaralı maddesinde, 6197 sayılı Eczacılar ve Eczaneler Hakkında Kanun kapsamında serbest faaliyet gösteren ve birinci basamak sağlık kuruluşu olan eczanelerin, sağlık hizmeti sunucuları arasında zikredildiği, Yönetmelikte kullanılan sağlık hizmeti sunucusu ile ifade edilmek istenenin, Sağlık Bakanlığı ve bağlı kuruluşları bünyesinde faaliyet gösteren ve birinci, ikinci ve üçüncü basamakta sağlık hizmeti sunmakta olan bütün sağlık tesisleri olduğu, dolayısıyla 5. maddesinin 5. fıkrasının iptalini talep etmekte davacı tarafın menfaatinin bulunmadığı, davanın evleviyetle bu hüküm bakımından usulden de reddinin gerektiği; Yönetmelikte Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü tarafından geliştirilen Ulusal Sağlık Sisteminden, merkezi sağlık veri sistemi olarak bahsedildiği, Yönetmeliğin 14. maddesi uyarınca sağlık hizmeti sunucularının, merkezi sağlık veri sistemine, Bakanlıkça belirlenen standartlara uygun bir şekilde veri aktarımı yapmalarının gerektiği, bununla birlikte serbest eczane sahibi eczacılardan, Ulusal Sağlık Sistemine veri gönderimi yapmalarının talep edilmediği, madde metninde yer alan "...Bakanlıkça belirlenen standartlara uygun..." ifadesi ile atıf yapılan düzenlemenin, Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü'nün 2015/17 sayılı Genelgesi olduğu, bu Genelgede Hastane Bilgi Yönetim Sistemi ve Sağlık Bilgi Yönetim Sistemine ilişkin düzenlemelerin yer aldığı; serbest eczane sahibi eczacıların kullandığı veya kullanabilecekleri yazılımlardan bahsedilmediği, Genelgede bahsedilen, tüm sağlık tesislerinde kullanılan sağlık uygulama yazılımlarını üreten kamu ve özel kurum ve kuruluşlarının kayıt ve tescil işlemlerini düzenlemek için Bakanlık bünyesinde oluşturulan Kayıt Tescil Sisteminde eczanelerin kullandıkları yazılımların tescil edilmediği ve eczanelerde kullanılacak yazılımlar için böyle bir tescil şartı aranmadığı, davacı tarafından iddia edildiği üzere eczacıların, Bakanlıkça verilen yetki belgesine

sahip ve Bakanlıkça belirlenen standartlar ile uyumlu yazılımlar kullanmak zorunda bırakılmadıkları belirtilerek davanın reddi gerektiği savunulmaktadır.

... Kurumu tarafından; 12/01/2017 tarihinde, 6698 sayılı Kanun'un 21. maddesi hükümlerine göre seçilen Kişisel Verileri Koruma Kurulu üyelerinin Yargıtay 1. Başkanlık Kurulu huzurunda yemin ettikleri, 30/01/2017 tarihinde Başkan ve 2. Başkanın seçildiği, Kurum tarafından halihazırda başta hizmet birimlerinin çalışma usul ve esaslarını belirleyen teşkilat yönetmeliğinin hazırlanması ile diğer mevzuat hazırlıkları, idari ve teknik çalışmalarının yürütüldüğü, Sağlık Bakanlığı tarafından çıkarılan dava konusu yönetmeliğin hazırlanma sürecinde Kurumun dahlinin bulunmadığı, işbu davada taraf sıfatını haiz olmadıkları, Anayasa'nın 20. maddesinin üçüncü fıkrasındaki, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenlenmesi hükmünün, bu alanın yalnızca kanunla düzenleneceği anlamına gelmediği savunulmaktadır.

DANIŞTAY TETKİK HAKİMİ: ...

DÜŞÜNCESİ: Dava konusu Yönetmeliğin 21/06/2019 tarih ve 30808 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Kişisel Sağlık Verileri Hakkında Yönetmeliğin 23. maddesi ile yürürlükten kaldırıldığı görüldüğünden konusuz kalan dava hakkında karar verilmesine yer olmadığına karar verilmesi gerektiği düşünülmektedir.

DANIŞTAY SAVCISI: ...

DÜŞÜNCESİ: Dava; 20.10.2016 tarihli ve 29863 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin, 5. maddesinin 5. fıkrası ile 14. maddesinin iptali istemiyle açılmıştır.

Kişisel verilerin korunması konusunda yasal boşluğu doldurmak amacıyla kabul edilen çerçeve niteliğinde bir yasal düzenleme olan 07.04.2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanununun 21. maddesi hükümlerine göre oluşturulan Kişisel Verileri Koruma Kurulu'nun görev ve yetkileri, aynı Kanun'un 22. maddesiyle belirlenmiştir. 22. maddenin 1. fıkrasının (h) bendinde "Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek" hükmüne yer verilmiştir.

Anılan Kanun'un, "Özel nitelikli kişisel verilerin işleme şartları" başlıklı 6. maddesinin 1. fıkrasında, dava konusu Yönetmelikle düzenlenen, sağlık verilerinin de özel nitelikli kişisel veri olduğu belirtilmiş; maddenin 4. fıkrasında, "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü getirilmiştir.

6698 sayılı Kanunun Geçici 1. maddesi hükmü uyarınca, Kanunun 21. maddesine göre oluşturulacak Kişisel Verileri Koruma Kurulu'nun Kanunun Resmi Gazete'de yayımlandığı 7/4/2016 tarihinden itibaren altı ay içinde üyelerinin seçiminin tamamlanması gerekmekte iken, bu yasal gerekliliğin ancak 30.01.2017 tarihinde yerine getirilebildiği anlaşılmaktadır.

Dosyanın incelenmesinden, dava konusu Yönetmeliğin Resmî Gazete'de yayımlandığı tarih olan 20.10.2016'da Kişisel Verileri Koruma Kurulu'nun henüz oluşturulmadığı, dolayısıyla 6698 sayılı Kanun'un 6. maddesinin 4. fıkrasında belirtilen yeterli önlemlerin Kurul tarafından belirlenmediği ve Kanun'un 22. maddesinin 1. fıkrasının (h) bendine göre diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında Kurul görüşü alınmadan dava konusu düzenlemenin tesis edildiği görülmekte olup; Kişisel Verileri Koruma Kurulu'nun kontrol ve denetiminden geçirilmeksizin hazırlanan ve dava konusu düzenlemede bu nedenle mevzuata ve hukuka uygunluk bulunmadığı sonucuna ulaşılmıştır.

Açıklanan nedenlerle, 20.10.2016 tarihli ve 29863 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin, 5. maddesinin 5. fıkrası ile 14. maddesinin iptali yolunda karar verilmesi gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay Onuncu Dairesince, tetkik hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereği görüldü:

Davacı Sendika üyesi eczacıların işlettiği eczaneler birinci basamak sağlık hizmeti sunucusu olduklarından davalı idarelerden Sağlık Bakanlığının menfaate yönelik usul itirazı yerinde görülmemekle ve Kişisel Verileri Koruma Kurumunun husumete yönelik usul itirazı da yerinde görülmemekle işin esasına geçildi.

İNCELEME VE GEREKÇE:

Dava, 20/10/2016 tarihli ve 29863 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin 5. maddesinin 5. fıkrası ile 14. maddesinin iptali istemiyle açılmıştır.

Anılan Yönetmelik 21/06/2019 tarih ve 30808 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Kişisel Sağlık Verileri Hakkında Yönetmeliğin 23. maddesi ile yürürlükten kaldırılmıştır.

Bu durumda; dava konusu düzenlemenin yürürlükten kaldırılmış olması karşısında, konusu kalmayan davanın esası hakkında karar verilmesine yer bulunmadığı sonucuna ulaşılmıştır.

KARAR SONUCU:

Açıklanan nedenlerle;

1. Konusu kalmayan dava hakkında karar verilmesine yer olmadığına,
2. Davalı idare tarafından davanın açılmasına sebebiyet verilmiş olması nedeniyle kararın verildiği tarihte yürürlükte olan Avukatlık Asgari Ücret Tarifesine göre belirlenen ... TL avukatlık ücretinin ve aşağıda dökümü yapılan toplam ... TL yargılama giderinin davalı idarelerden alınarak davacıya verilmesine,
3. Posta giderleri avansından artan tutarın kararın kesinleşmesinden sonra davacıya iadesine,
4. Bu karara karşı tebliğ tarihini izleyen otuz (30) gün içinde Danıştay İdari Dava Daireleri Kurulu nezdinde temyiz yolu açık olmak üzere, 16/03/2021 tarihinde oy çokluğuyla karar verildi.

KARŞI OY

(X) :

İptal davaları, idarenin hukuka aykırı işleminden dolayı bu işlemlerin iptali için menfaatleri ihlâl edilenler tarafından açılan davalardır. Bireysel ve düzenleyici işlemlerin iptali istemiyle açılan davalarda, davanın konusuz kaldığından bahisle karar verilmesine yer olmadığına yönünde karar verilebilmesi için davacının bu dava ile ulaşmak istediği sonuca veya sağlamak istediği yarara ulaşmış olması gerekmektedir.

İdari işlemler, idare tarafından geri alınarak, ilk yapıldıkları andan itibaren tüm etki ve sonuçları ile ortadan kaldırılmadıkları ve davacılar bu şekilde amaçlarına ulaşamadıkları sürece dava açma sebepleri devam etmektedir.

Dava konusu edilmiş bulunan bir düzenlemenin yargısal denetimi tamamlanmadan idare tarafından değiştirilmesi ya da yürürlükten kaldırılması işlemin kaldırıldığı tarihe kadar hüküm ifade etmesini etkilemeyip, gelecekte yaratacağı etkiler açısından önem taşır. Bu durumunda, bu işlemler tesis edildiği tarih ile değiştirildiği ya da yürürlükten kaldırıldığı tarih arasındaki dönemde uygulanmaya böylece hukuki etki ve sonuçlarını doğurmaya devam ettiklerinden menfaat ilgisi de devam etmektedir. Bu tür durumlarda, davanın konusuz kaldığından bahisle, "karar verilmesine yer olmadığına" yönünde karar verilmesi, bu gibi işlemlerin yargısal denetiminin yapılamaması sonucunu doğuracaktır.

İptal davaları ile, idari işlemlerin hukuka uygun olup olmadığının tespiti ve böylece hukukun üstünlüğünün, dolayısıyla idarenin hukuka bağlılığının sağlanması amaçlandığına göre, işlemin tesis edildiği tarih bakımından gerçekleştirilecek olan yargısal denetimle, eğer varsa değiştirilen ya da yürürlükten kaldırılan düzenlemenin neden olduğu hukuka aykırı sonuçların giderilmesi böylece bu amacın gerçekleştirilmesi sağlanacaktır.

20/10/2016 tarihli ve 29863 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren dava konusu Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik yargısal denetimi tamamlanmadan, 21/06/2019 tarih ve 30808 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Kişisel Sağlık Verileri Hakkında Yönetmeliğin 23. maddesi ile yürürlükten kaldırılmıştır. Buna göre, dava konusu düzenleme yürürlükte olduğu 20/10/2016-21/06/2019 tarihleri arasında hüküm ifade ettiğinden, eğer varsa bu düzenlemenin neden olduğu hukuka aykırı sonuçların giderilmesi için tesis edildiği tarih itibarıyla hukuka uygunluk denetiminin yapılması ve davanın esastan karara bağlanması gerekmektedir.

Öte yandan, iş bu davada iptali istenilen düzenlemelere benzer şekilde, sağlık hizmeti sunucularının merkezi sağlık veri sistemine veri aktarımına yönelik düzenlemelere yeni Yönetmelikte de yer verildiği ve dava konusu düzenlemelerin ileride doğuracağı hukuksal etkilerin de giderilmediği görüldüğünden, davacının menfaat ihlalinin bu açıdan da devam ettiği anlaşılmakta olup, davanın bu sebeplerle de esastan karara bağlanması gerekmektedir.

Bu durumda; yargısal denetimden amaç "hukuka uygunluk" denetimi olduğuna ve yargısal denetim işlemin kurulduğu tarih bakımından gerçekleştiğine göre, yürürlükte kaldığı süre içerisinde uygulandığında kuşku bulunmayan ve yeni Yönetmelikle de uygulanmasına devam edilen düzenlemelerin iptali istemiyle açılan iş bu davada, esastan yargılama yapılarak bir karar verilmesi gerektiğinden, dava konusu düzenlemelerin yürürlükten kaldırıldığı ve davanın konusuz kaldığından bahisle karar verilmesine yer olmadığı yönünde verilen Daire kararına katılmıyorum.

Danıştay Kararı - 10. Daire (E. 2019/7049)

Danıştay Kararı - 10. D., E. 2019/7049 K. 2020/7089 T. 29.12.2020

T.C. DANIŞTAY ONUNCU DAİRE

Esas No: 2019/7049

Karar No: 2020/7089

DAVACI: ... Birliği

VEKİLLERİ: Av. ..., Av. ...

DAVALI: ... Bakanlığı

VEKİLLERİ: Hukuk Müşaviri Av. ...

Hukuk Müşaviri Av. ...

DAVANIN KONUSU: Davacı tarafından, 22/03/2017 tarih ve 30015 sayılı Resmî Gazete'de yayımlanan Özel Hastaneler Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmeliğin 26. maddesi ile asıl Yönetmeliğin 49. maddesinin 1. fıkrasına eklenen, "merkezi tıbbi arşivin hastane bünyesinde bulunması zorunlu değildir." ibaresinin, 26. maddesi ile değiştirilen 49. maddesinin 4. fıkrasının, 36. maddesi ile değiştirilen ek 5. maddesinin 1. fıkrasının (e) bendinin (5) numaralı alt bendinin, 37. maddesi ile değiştirilen ek 8. maddesinin iptali istenilmektedir.

DAVACININ İDDİALARI:

Dava konusu Yönetmeliğin 26. maddesi ile asıl Yönetmeliğin 49. maddesinin 1. fıkrasına eklenen, "merkezi tıbbi arşivin hastane bünyesinde bulunması zorunlu değildir." ibaresi bakımından; tıbbi arşivin hastane bünyesinden çıkarılmasının sağlık hakkının özüne aykırı olduğu, arşiv kaydının hastaya verilen tıbbi bakımın değerlendirilmesinde kullanılabilecek önemli bir kaynak teşkil ettiği, dosyaların çabuk ve kolay bulunması, derhal hazır bulundurulması gerekliliği ile örtüşmediği, arşiv standartları belirlenmeyerek hasta haklarının açıkça ihlal edildiği,

26. maddesi ile değiştirilen 49. maddesinin 4. fıkrası bakımından; 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda sağlık gibi özel nitelikli verilerin işlenmesinde uyulacak önlemleri belirlemekle yetkili olan Kişisel Verileri Koruma Kurulu oluşturulmadan alana ilişkin düzenleme yapıldığı, sağlık verilerinin rıza alınmaksızın işlenebileceği istisnai hallerin, ülkemizce usulüne

uygun olarak onaylanarak yürürlüğe giren 108 sayılı “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Sözleşme”ye aykırı biçimde geniş tutulduğu, özel hayatın korunması ilkesinin özünün zedelendiği, Sözleşmenin 9. maddesinin 2. fıkrasında sağlık verilerinin işlenmeme yasağına sadece “devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi ile ilgili kişinin veya başkasının hak ve özgürlüklerinin korunması” halinde istisna getirilebileceği, ancak bu istisnaların da kanunla düzenlenmesinin ve demokratik bir toplumda zorunlu olmasının ön koşul olduğu, maddenin 1. fıkrasına göre ise sayılan bu haller dışında devletlerin başka istisnai halleri düzenleyemeyeceği, sağlık verisi sahibinin Anayasa ve 108 nolu Sözleşme ile güvence altına alınan haklarının yönetmelikle ortadan kaldırıldığı;

36. maddesi ile değiştirilen ek 5. maddesinin 1. fıkrasının (e) bendinin (5) numaralı alt bendi bakımından; düzenleme ile, çalışma hakkının kısıtlandığı, bu durumun üst hukuk normlarına ve yargı kararlarına aykırı olduğu, özel sağlık kuruluşlarında çalışan tabip/uzman tabiplerin özel hastanelerde sadece nöbet tutabilecekleri, özel hastanede kadrolu çalışan tabiplerin nöbet dışında bir başka sağlık kuruluşunda çalışabilmesinin kurumsal sözleşmeye bağlı kılındığı, nöbet biçimindeki kadro dışı geçici çalışmanın özel hastanede kadrolu çalışma zorunluluğu şartına tabi tutulmasının hukuka ve yargı kararlarına aykırı olduğu, tabiplerin çalışma saatleri dışında sadece nöbet tutabilmelerinin 1219 sayılı Kanun'a aykırılık teşkil ettiği, özel hastane kadrosunda çalışan tabibin başka bir özel hastane ya da tıp merkezinde kısmi zamanlı çalışabilmesi için kurumsal sözleşme yapılmasının ve çalışacak hekimin muvafakat vermesinin gerekliliğinin düzenlendiği, söz konusu düzenleme ile hekimin iradesinin yok sayıldığı, işletme sahibinin baskın olacağı, işten atılma tehdidi karşısında hekimin muvafakat vermemesinin ihtimal dahilinde olmadığı;

37. maddesi ile değiştirilen ek 8. maddesi bakımından; anılan hükümde, vakıf üniversiteleri ile işbirliği yapan özel hastanelere planlamadan istisna olarak, sadece üniversiteden görevlendirilmiş doçent ve profesör unvanlı öğretim üyelerine mahsus olmak ve sadece işbirliği yapılan hastanede çalışmak üzere asgari öğretim üyesi standartları açısından Yükseköğretim Kurulunun görüşü ve Bakanlık kadro planlamaları dikkate alınarak Bakanlıkça uzmanlık dalı ilavesi ve ek kadro tahsisi yapılabileceği düzenlemesine yer verildiği, dayanak 3359 sayılı Kanun'un ek 15. maddesinde ifade edilen amacın yeterli kapasite ve eğitim alt yapısı olmayan tıp fakültelerinin eğitiminin sağlanması olduğu, ancak, düzenlemede böyle bir kriterin yer almadığı, öğretim üyesinin özel hastanede çalıştırılmasının amaç haline getirildiği, üniversite hastanelerinin kamu hizmeti yönünün ağır bastığı, özel hastanelerin ise sırf kâr amaçlı işletmeler olduğu, dolayısıyla hükmün amaç ve konu yönlerinden hukuka aykırı olduğu;

iddia edilerek anılan düzenlemelerin iptali istenilmektedir.

DAVALININ SAVUNMASI:

Dava konusu Yönetmeliğin 26. maddesi ile asıl Yönetmeliğin 49. maddesinin 1. fıkrasına eklenen, "merkezi tıbbi arşivin hastane bünyesinde bulunması zorunlu değildir." ibaresi bakımından; merkezi tıbbi arşivin mutlaka hastane bünyesinde oluşturulan bir alanda saklanması zorunlu olmadığı, MEB Tıbbi Arşivleme Dokümanının bu konuda mutlak zorunluluk getirmediği ve yine Devlet Arşiv Hizmetleri Yönetmeliğinde de sadece arşiv hizmetlerinin yürütülmesi konusunun düzenlendiği, arşivin bulunacağı bina bakımından bir düzenlemeye gidilmediği, bu hususta önemli olan hususun, hasta kayıtlarının düzgün ve düzenli tutulması, ulaşılabilir olması, uygun şartlarda muhafaza edilmesi olduğu, dolayısıyla düzenlemenin hizmet gereklerine ve hukuka uygun olduğu;

26. maddesi ile değiştirilen 49. maddesinin 4. fıkrası bakımından; kişisel sağlık verilerinin işlenmesine ilişkin usûl ve esasların 6698 sayılı Kişisel Verilerin Korunması Kanuna istinaden düzenlendiği, dolayısıyla 6698 sayılı Kanun'un 6. maddesinin 3. fıkrasında öngörülen "kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi sağlık hizmetleri ile finansmanının planlanması ve yönetimi" amaçları ile kişisel verilerin işlenmesinin, davacı tarafından iddia edildiği gibi uluslararası sözleşme hükümlerine ve Anayasa'ya aykırılık teşkil etmediği;

36. maddesi ile değiştirilen ek 5. maddesinin 1. fıkrasının (e) bendinin (5) numaralı alt bendi bakımından; dava konusu hükmün 1219 sayılı Kanun'un 12. maddesine paralellik arzettiği, yargı kararının gerekçesine uygun olduğu, özel hastanede çalışmak için başka bir özel hastane veya özel sağlık kuruluşunda "kadrolu" olmak şartının getirilmediği, "sağlık kuruluşundaki çalışma saatleri dışında" ifadesine yer verildiği, özel sağlık kuruluşlarında çalışan tabiplerin mesai saatleri sonunda nöbet sistemiyle çalışabilmelerine imkan verildiği, kurumsal sözleşme getirilmesinin maksadının, planlama kapsamında kısıtlı tabip insan gücünün özel sektör içerisinde kullanılabilmesi ve böylece sağlık hizmeti sunumunda verimin, ulaşılabilirliğin ve kalitenin sağlanması olduğu;

37. maddesi ile değiştirilen ek 8. maddesi bakımından; 3359 sayılı Kanun'un ek 15. maddesine istinaden ve bu maddeye paralel şekilde getirilen bu hüküm ile bünyesinde tıp ve/veya diş hekimliği fakültesi bulunan vakıf üniversitelerinin, Sağlık Bakanlığı ve Yükseköğretim Kurulunun uygun görmesi üzerine özel hastanelerle işbirliği yapabilmelerine imkan tanındığı, dava konusu düzenlemede maksadın, davacı tarafın iddia ettiği gibi öğretim üyelerinin özel hastanelerde çalıştırılmasına imkan sağlamak değil, vakıf üniversitelerinin "uygulama hastanesi" ihtiyacını karşılamak olduğu, dolayısıyla hükmün hizmet gerekleri ve kamu yararına uygun olduğu;

ileri sürülerek davanın reddi gerektiği savunulmaktadır.

DANIŞTAY TETKİK HAKİMİ: ...

DÜŞÜNCEİ: Dava konusu düzenlemelerin kamu yararı ve hizmet gerekleri ile hukuka uygun olduğu, davanın reddi gerektiği düşünülmektedir.

DANIŞTAY SAVCISI: ...

DÜŞÜNCEİ: Dava; 22/03/2017 tarihli, 30015 sayılı Resmi Gazetede yayımlanan "Özel Hastaneler Yönetmeliğinde Değişiklik Yapılması Hakkında Yönetmelik" in 26. maddesi ile asıl Yönetmeliğin 49. maddesinin 1. fıkrasına eklenen, "merkezi tıbbi arşivin hastane bünyesinde bulunması zorunlu değildir." ibaresinin, 49. maddesinin 4. fıkrasının, aynı Yönetmeliğin Ek 5. maddesinin 1. fıkrasının (e) bendinin (5) numaralı alt bendinin ve Ek 8. maddesinin iptali istemiyle açılmıştır.

3359 Sayılı Sağlık Hizmetleri Temel Kanununun 3. maddesinin c) fıkrasında: "Bütün sağlık kurum ve kuruluşları ile sağlık personelinin ülke sathında dengeli dağılımı ve yaygınlaştırılması esastır. Sağlık kurum ve kuruluşlarının kurulması ve işletilmesi bu esas içerisinde Sağlık ve Sosyal Yardım Bakanlığınca düzenlenir. Bu düzenleme ilgili Bakanlığın görüşü alınarak yapılır. Gerek görüldüğünde özel sağlık kuruluşlarının her türlü ücret tarifeleri sağlık ve Sosyal Yardım Bakanlığınca onaylanır. Kamu kurum ve kuruluşlarına ait sağlık kuruluşları veya sağlık işletmelerinde verilen her türlü hizmetin fiyatları Sağlık ve Sosyal Yardım Bakanlığınca tespit ve ilan edilir.", 9. maddesinin (c) fıkrasında: "Bütün kamu ve özel sağlık kuruluşlarının tesis, hizmet, personel, kıstaslarını belirlemeye, sağlık kurum ve kuruluşlarını sınıflandırmaya ve sınıflarının değiştirilmesine, sağlık kuruluşlarının amaca uygun olarak teşkilatlanmalarına, sağlık hizmet zinciri oluşturulmasına, hizmet içi eğitim usul ve esasları ile sağlık kurum ve kuruluşlarının koordineli çalışma ve hizmet standartlarının tespiti ve denetimi ile bu Kanunla ilgili diğer hususlar Sağlık ve Sosyal Yardım Bakanlığınca, çıkarılacak yönetmelikle tespit edilir." kuralları yer almış, 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 40. maddesinde ise: "Bakanlık ve bağlı kuruluşlar görev, yetki ve sorumluluk alanına giren ve önceden kanunla düzenlenmiş konularda idarî düzenlemeler yapabilir." kurala bağlanmıştır.

Uyuşmazlık 49. maddenin 1. fıkrasına eklenen "merkezi tıbbi arşivin hastanesi bünyesinde bulunması zorunlu değildir." ibaresi yönünden ele alındığında;

Dava dilekçesinde; tıbbi arşivin hastane bünyesinden çıkarılmasının sağlık hakkının özüne aykırı olduğu, dosyanın çabuk ve kolay bulunması, derhal hazır bulundurulması gerekliliğiyle örtüşmediği,

arşive ilişkin hiçbir standardı düzenlemeyerek hasta haklarını açık şekilde ihlal ettiği, hekim açısından nitelikli bir sağlık hizmetinin sunumunu güçleştirdiği ileri sürülmektedir.

Davalı idarenin savunmasında; Yönetmeliğin 49. maddesiyle özel hastanelerde hasta kayıtlarının saklanması, bu konuda arşiv oluşturulması konusunda kesin zorunluluk getirildiği, 50. maddeyle tıbbî kayıtların muhafazası için "dijital arşiv" in oluşturulmasının mümkün olduğu, Devlet Arşivleri Yönetmeliğinde sadece arşiv hizmetlerinin yürütülmesi konusunun düzenlendiği, arşivin bulunacağı bina bakımından düzenlemeye gidilmediği, arşivin hastane binası dışında olup olmamasının sağlık haklarını ihlal edebilecek, sağlık hizmetlerinin niteliğini güçleştirecek boyutunun olmadığı savunulmaktadır.

Yönetmeliğin 49. maddenin 1. fıkrasının iptali istenmeyen kısımları ile 50. maddesi birlikte ele alındığında; özel hastanelerde tıbbî ve idarî işlemlere ilişkin kayıtların, düzenlenen ve kullanılan belgeleri tasnif ve muhafazaya uygun bir merkezî tıbbî arşiv kurulmasının zorunlu olduğu, Yönetmelikte belirtilmiş her türlü kayıt işlemi, bilgisayar ortamında ve/veya ihtiyaca göre yazılı kayıt sistemi ile tutulabileceği, kayıtların bilgisayar ortamında saklanması, değiştirilmesi ve silinmesinin önlenmesi, gizliliğin ihlal edilmemesi amacıyla fizikî, manyetik veya elektronik müdahalelere ve olası suistimallere karşı gerekli idarî ve teknik tedbirlerin alınması ve periyodik olarak denetlenmesinden mesul müdürün sorumlu olduğu, mevcut yedekleme sisteminde günlük, haftalık, aylık ve yıllık olmak üzere verilerin yedekleneceği, güvenli dijital hasta kaydına geçilmeyen hastanelerde bilgisayar ortamında kayıt tutulması, yazılı kayıt sisteminin gereklerini ortadan kaldırmayacağına ilişkin getirilen yükümlülükler karşısında, merkezi tıbbî arşivin hastane bünyesinde bulunmasına ilişkin zorunluluk getirilmemesinde, arşiv hizmetlerinin sunumuna ilişkin değişen teknik nitelik de göz önünde tutulduğunda hukuka aykırılığından söz edilemez.

Uyuşmazlık 49. maddenin 4. fıkrası ele alındığında;

27/03/2002 tarihli, 24708 sayılı Resmi Gazetede yayımlanan Özel Hastaneler Yönetmeliğinin 49. maddesinin 4. fıkrasında, "Kanunun 3 üncü maddesi uyarınca Bakanlık tarafından kurulacak kayıt ve bildirim sistemine ve Bakanlıkça yapılacak diğer iş ve işlemlere esas olmak üzere, istenilen bilgi ve belgelerin Bakanlığa gönderilmesi zorunludur." kuralının, dava konusu değişiklik ile anılan fıkra "Özel hastaneler tarafından kayıt altına alınan kişisel sağlık verileri, 6698 sayılı Kişisel Verilerin Korunması Kanununa uygun bir şekilde işlenir ve Bakanlıkça belirlenen usul ve esaslara uygun bir şekilde merkezi sağlık veri sistemine aktarılır. Bakanlık tarafından kurulan kayıt ve bildirim sistemine ve Bakanlıkça yapılacak diğer iş ve işlemlere esas olmak üzere, istenilen bilgi ve belgelerin Bakanlığa gönderilmesi zorunludur." şeklinde yeniden düzenlenmiştir.

Danıştay Onbeşinci Dairesinin 31/10/2017 tarihli, E:2017/1071 sayılı kararıyla dava edilen kuralın yürütmesinin durdurulmasından sonra 31/05/2019 tarihli, 30790 sayılı Resmi Gazetede yayımlanan Yönetmelikle değişikliğe gidilmiş anılan fıkra “Özel hastaneler tarafından kayıt altına alınan kişisel sağlık verileri, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ikincil düzenlemelere uygun bir şekilde Bakanlıkça belirlenen usul ve esaslar çerçevesinde merkezi sağlık veri sistemine aktarılır ve işlenir. Bakanlık tarafından kurulan kayıt ve bildirim sistemine ve Bakanlıkça yapılacak diğer iş ve işlemlere esas olmak üzere, istenilen bilgi ve belgelerin Bakanlığa gönderilmesi zorunludur.” şeklinde düzenlenmiştir.

Sağlık Bakanlığı tarafından kişisel sağlık verisi işleyen özel hukuk gerçek ve tüzel kişileri ile kamu hukuku tüzel kişilerinin, Sağlık Bakanlığı tarafından yürütülmekte olan süreç ve uygulamalara ilişkin faaliyetlerini kapsayan Kişisel Sağlık Verileri Hakkında Yönetmelik 21.06.2019 tarihli, 30808 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiş ve Danıştay Onbeşinci Dairesinin 06/07/2017 tarihli, E:2016/10500 sayılı kararıyla yürütmesi durdurulan 20/10/2016 tarihli ve 29863 sayılı Resmi Gazetede yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik de yürürlükten kaldırılmıştır.

Aktarılan bu hukuk durum göz önünde tutulduğunda; 6698 sayılı Kişisel Verilerin Korunması Kanunu hükümleri kapsamında, Sağlık Bakanlığının merkez ve taşra teşkilatı birimleri ile bunlara bağlı olarak faaliyet göstermekte olan sağlık hizmeti sunucuları ile bağlı ve ilgili kuruluşları tarafından yürütülen süreç ve uygulamalarda uyulacak usul ve esasların düzenlenmesi, dava konusu kuralın da anılan Yönetmelikle bağlantılı kurularak değiştiğinin görülmesi karşısında davanın bu kısmı konusuz hale gelmiştir.

Uyuşmazlık Ek 5. maddesinin 1. fıkrasının (e) bendinin (5) numaralı alt bendi yönünden ele alındığında;

Özel hastanenin kalite ve verimliliğini arttırmak amacıyla izin verilebilecek hususlar başlıklı Ek-5. maddesinin iptali istenile 1/e-5 numaralı alt bendinde: “Özel Sağlık Kuruluşlarında çalışan tabip/uzman tabipler, 1219 sayılı Kanunun 12 nci maddesine uygun olmak kaydıyla, çalıştıkları sağlık kuruluşundaki çalışma saatleri dışında başka bir özel hastanenin acil servis, klinik servis ve ünitelerinde nöbet tutabilir. Bu tabiplerin nöbet listesi aylık olarak düzenlenir ve Müdürlükçe onaylanır. Özel hastane kadrosunda çalışan tabip ve uzman tabipler, hastanedeki çalışma saatleri dışında 1219 sayılı Kanunun 12 nci maddesine uygun olmak kaydıyla kurumsal sözleşme yapılarak diğer özel hastane veya tıp merkezlerinde çalıştırılabilir. Ancak, bu durumda tabip ve uzman tabiplerin muvafakatının alınması zorunludur. Sözleşme Müdürlüğe bildirilir ve ilgili tabip ve uzman

tabiplere çalışma belgesi düzenlenir. Özel hastanenin kadrosunda çalışan sözleşmeye konu tabip ve uzman tabiplerin kadrodan ayrılmaları halinde sözleşme sona erer.” kuralı yer almaktayken 28/09/2019 tarihli, 30902 sayılı Resmi Gazetede yayımlanan Yönetmelikle dava konusu bentte değişikliğe gidilmiştir.

Buna göre dava konusu bent “Özel Sağlık Kuruluşlarında çalışan tabip/uzman tabipler, 1219 sayılı Kanunun 12 nci maddesine uygun olmak kaydıyla, çalıştıkları sağlık kuruluşundaki çalışma saatleri dışında başka bir özel hastanenin acil servis, klinik servis ve ünitelerinde nöbet tutabilir. Bu tabiplerin nöbet listesi aylık olarak düzenlenir ve Müdürlükçe onaylanır. Muayenehaneler hariç planlama kapsamındaki özel sağlık kuruluşlarında çalışan tabip ve diş tabipleri, Bakanlığın istihdam planlamaları gereğince, 1219 sayılı Kanunun 12 nci maddesine uygun olmak kaydıyla kadrolu çalıştığı özel sağlık kuruluşu dışında planlama kapsamındaki iki özel sağlık kuruluşunda daha çalışabilir. Bu kuruluşlardan bir tanesi kadrolu çalıştığı il dışındaki planlama kapsamındaki bir özel sağlık kuruluşu da olabilir.” şeklinde düzenlenmiştir.

Dava dilekçesinde, özel sağlık kuruluşlarında çalışan tabip/uzman tabiplerin başka hastanede sadece nöbet tutabileceği, özel sağlık kuruluşunda sadece nöbet tutabilmek için bir başka sağlık kuruluşunda çalışıyor olmanın zorunlu hale getirildiği, özel hastanede kadrolu çalışanların nöbet dışında bir başka sağlık kuruluşunda çalışabilmesinin kurumsal sözleşmeye bağlı kılındığı ileri sürülerek iptalinin istenildiği, dava konusu düzenlemede davanın görümü sırasında yapılan değişiklik ile iddia edilen hususlara yönelik olarak değişiklik yapıldığı, bu haliyle davanın konusuz kaldığı görülmüştür.

Uyuşmazlık Ek-8. madde yönünden ele alındığında;

Vakıf üniversiteleri ile özel hastaneler başlıklı Ek-8. maddenin dava konusu edilen şeklinde: “Vakıf üniversiteleri ile işbirliği yapan özel hastanelere planlamadan istisna olarak, sadece üniversiteden görevlendirilmiş doçent ve profesör unvanlı öğretim üyelerine mahsus olmak ve sadece işbirliği yapılan hastanede çalışmak üzere asgari öğretim üyesi standartları açısından Yükseköğretim Kurulunun görüşü ve Bakanlık kadro planlamaları dikkate alınarak Bakanlıkça uzmanlık dalı ilavesi ve ek kadro tahsisi yapılabilir. Bu hastanelere uzmanlık dallarının gerektirdiği tıbbi hizmet birimleri ve teknoloji yoğunluklu tıbbi cihazlar kurdurulabilir. Özel hastaneye tahsis edilen bu kadrolar ve uzmanlık dalları ile tıbbi hizmet birimleri ve teknoloji yoğunluklu tıbbi cihazlar, işbirliğinin sona ermesi halinde hastane hekim kadrosu ve faaliyet izin belgesinden düşülür.” kuralı yer almaktaydı.

Yönetmeliğin uyuşmazlığa konu maddesi 31/05/2019 tarihli, 30790 sayılı Resmi Gazetede yayımlanan Yönetmelik değişikliği sonucunda başlığı ile birlikte beş fıkradan oluşacak şekilde yeniden

düzenlenmiş, ayrıca 2. fıkrası da 28/9/2019 tarihli, 30902 sayılı Resmi Gazetede yayımlanan Yönetmelikle yeniden değiştirilmiştir.

Dava dilekçesinde; tıp fakültesi bulunan vakıf üniversitelerinin açtığı hastanelerin uygulama ve araştırma merkezi statüsünde olduğu, bu hastanelerin birer yükseköğretim kurumu olduğu, eğitimin bir parçası olarak sağlık hizmeti sunmasının zorunlu olduğu, kanundaki şartın yönetmeliğe yansıtılmadığı, eğitim amacı ilgisiz olduğu, özel hastanelerin hekim açığını düzenleme amacı taşıdığı ileri sürüldüğü, Yönetmelik değişikliğiyle hem vakıf üniversitesilerine ait hastaneler hem de vakıf üniversiteleri ile özel hastane işbirliği konusu birlikte ele alınarak yeniden düzenlenmiştir.

Bu haliyle dava konusu Ek-8. madde yönünden de dava konusuz kalmıştır.

Açıklanan nedenlerle, Yönetmeliğin 49. maddesinin 1. fıkrasında iptali istenen ibare yönünden davanın reddi, dava konusu edilen diğer maddeler yönünden ise karar verilmesine yer olmadığına karar verilmesi gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay Onuncu Dairesince, duruşma için önceden taraflara bildirilen 29/12/2020 tarihinde davacıyı temsilen Av. ...'nın ve Av. ...'in, davalı Sağlık Bakanlığını temsilen Hukuk Müşaviri Av. ...'un geldiği, Danıştay Savcısının hazır olduğu görülmekle açık duruşmaya başlandı. Taraflara usulüne uygun olarak söz verilerek dinlendikten ve Danıştay Savcısının düşüncesi alındıktan sonra taraflara son kez söz verilip, duruşma tamamlandı. Tetkik hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereği görüldü:

MADDİ OLAY VE HUKUKİ SÜREÇ:

Dava, 22/03/2017 tarih ve 30015 sayılı Resmî Gazete'de yayımlanan Özel Hastaneler Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmeliğin 26. maddesi ile asıl Yönetmeliğin 49. maddesinin 1. fıkrasına eklenen, "merkezi tıbbi arşivin hastane bünyesinde bulunması zorunlu değildir." ibaresinin, 26. maddesi ile değiştirilen 49. maddesinin 4. fıkrasının, 36. maddesi ile değiştirilen ek 5. maddesinin 1. fıkrasının (e) bendinin (5) numaralı alt bendinin, 37. maddesi ile değiştirilen ek 8. maddesinin iptali istemiyle açılmıştır.

İNCELEME VE GEREKÇE:

İlgili Mevzuat:

Anayasanın 56. maddesinin 1. fıkrasında, herkesin, sağlıklı ve dengeli bir çevrede yaşama hakkına sahip olduğu; üçüncü fıkrasında, Devletin, herkesin hayatını, beden ve ruh sağlığı içinde

sürdürmesini sağlamak; insan ve madde gücünde tasarruf ve verimi artırarak, işbirliğini gerçekleştirmek amacıyla sağlık kuruluşlarını tek elden planlayıp hizmet vermesini düzenleyeceği; 4. fıkrasında da, Devletin, bu görevini kamu ve özel kesimlerdeki sağlık ve sosyal kurumlarından yararlanarak, onları denetleyerek yerine getireceği hükmüne yer verilmiştir.

3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 1. maddesinde; Kanununun amacının, sağlık hizmetleri ile ilgili temel esasları belirlemek olduğu, 2. maddesinde; Milli Savunma Bakanlığı hariç bütün kamu kurum ve kuruluşları ile özel hukuk tüzelkişileri ve gerçek kişileri kapsadığı, 3. maddesinin (a) bendinde; sağlık kurum ve kuruluşlarının yurt sathında eşit, kaliteli ve verimli hizmet sunacak şekilde Sağlık ve Sosyal Yardım Bakanlığınca, diğer ilgili bakanlıkların da görüşü alınarak plânlanacağı, koordine edileceği, mali yönden destekleneceği ve geliştirileceği, (c) bendinde; bütün sağlık kurum ve kuruluşları ile sağlık personelinin ülke sathında dengeli dağılımı ve yaygınlaştırılmasının esas olduğu, sağlık kurum ve kuruluşlarının kurulması ve işletilmesinin bu esas içerisinde Sağlık ve Sosyal Yardım Bakanlığınca düzenleneceği, (e) bendinde; tesis edilecek eğitim, denetim, değerlendirme ve oto kontrol sistemi ile sağlık kuruluşlarının tespit edilen standart ve esaslar içinde hizmet vermesinin sağlanacağı, (f) bendinde; herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi maksadıyla, Sağlık Bakanlığı ve bağlı kuruluşlarınca gerekli kayıt ve bildirim sisteminin kurulacağı, bu sistemin, e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabileceği, bu amaçla, Sağlık Bakanlığınca, bağlı kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemi kurulabileceği, 9. maddesinin (c) bendinde; bütün kamu ve özel sağlık kuruluşlarının tesis, hizmet, personel, kıstaslarını belirlemeye, sağlık kurum ve kuruluşlarını sınıflandırmaya ve sınıflarının değiştirilmesine, sağlık kuruluşlarının amaca uygun olarak teşkilatlanmalarına, sağlık hizmet zinciri oluşturulmasına, hizmet içi eğitim usul ve esasları ile sağlık kurum ve kuruluşlarının koordineli çalışma ve hizmet standartlarının tespiti ve denetimi ile bu Kanunla ilgili diğer hususların Sağlık ve Sosyal Yardım Bakanlığınca çıkarılacak yönetmelikle tespit edileceği belirlenmiştir.

Anılan Kanun'un ek 15. maddesinde de, "Tıp ve/veya diş hekimliği fakültesi bulunan ancak sağlık uygulama ve araştırma merkezi bulunmayan veya sağlık uygulama ve araştırma merkezinde yeterli kapasite ve eğitim altyapısı bulunmayan vakıf üniversiteleri; tıp ve diş hekimliğinde lisans eğitimi, tıp, diş hekimliği ve eczacılıkta uzmanlık eğitimi ile araştırma faaliyetleri için yeterli kapasite ve eğitim altyapısı bulunan özel hastaneler ile bütçeleri ayrı olmak şartıyla işbirliği yapabilir. İlgili üniversite ve özel hastanenin yetkili makamları arasında işbirliği protokolü imzalanır ve Sağlık Bakanlığı ve Yükseköğretim Kurulunun onayıyla uygulamaya konulur.

İşbirliği yapılan özel hastane, üniversite için sağlık uygulama ve araştırma merkezi kabul edilir. Burada fiilen görev yapacak olan üniversite öğretim elemanları, ilgili dekan ve hastane yöneticisinin talebi üzerine rektör tarafından görevlendirilir. Görevlendirilen üniversite personeline kendi mevzuatı uygulanır. İşbirliği yapılan özel hastane, öğretim üyelerinin faaliyetleri ve üniversitenin eğitim ve araştırma işlevleri dışında kendi mevzuatına tabi olmaya devam eder.

Bu maddenin uygulanmasına ilişkin usul ve esaslar Yükseköğretim Kurulunun görüşü alınarak Sağlık Bakanlığı tarafından belirlenir." hükmü yer almaktadır.

663 sayılı -dava konusu işlemlerin tesis edildiği tarihteki adıyla- Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin yine dava konusu işlemlerin tesis edildiği tarihte yürürlükte olan haliyle 40. maddesinde ise; Bakanlık ve bağlı kuruluşların görev, yetki ve sorumluluk alanına giren ve önceden kanunla düzenlenmiş konularda idarî düzenlemeler yapabilecekleri hükmüne yer verilmiştir.

Yukarıda yer verilen mevzuat hükümlerine dayanılarak, etkin, verimli ve kaliteli sağlık hizmeti sunulmasını sağlamak üzere, bütün özel hastanelerin tesis, hizmet ve personel standartlarının tespit edilmesine, sınıflandırılmasına, sınıflarının değiştirilmesine, amaca uygun olarak teşkilatlandırılmasına ve bunların açılmalarına, faaliyetlerine, kapanmalarına ve denetlenmelerine ilişkin usûl ve esasları düzenlemek amacıyla hazırlanan Özel Hastaneler Yönetmeliği 27/03/2002 tarih ve 24708 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiş, bilahare 22/03/2017 tarihli ve 30015 sayılı Resmî Gazete'de yayımlanan değişiklik ile dava konusu düzenlemelere yer verilmiştir.

Dava konusu maddelerin incelenmesi:

1) Dava konusu Yönetmeliğin 26. maddesi ile asıl Yönetmeliğin 49. maddesinin 1. fıkrasına eklenen, "merkezi tıbbi arşivin hastane bünyesinde bulunması zorunlu değildir." ibaresinin incelenmesi:

Özel Hastaneler Yönetmeliğinin 49. Maddesinin 1. fıkrasında; "Özel hastanelerde, muayene, teşhis ve tedavi amacıyla başvuran hasta, yaralı, acil ve adlî vakalar ile ilgili olarak yapılan tıbbî ve idarî işlemlere ilişkin kayıtların, düzenlenen ve kullanılan belgelerin toplanması ve bunların müteakip başvurular ile denetim ve adlî mercilerce her istenildiğinde hazır bulundurulması amacıyla tasnif ve muhafazaya uygun bir merkezî tıbbî arşiv kurulması zorunludur." hükmü yer almakta iken; 22/3/2017 tarih ve 30015 sayılı Resmî Gazete'de yayımlanan Özel Hastaneler Yönetmeliğinde Değişiklik Yapılması Hakkında Yönetmeliğin 26. maddesi ile 49. maddesinin 1. fıkrasına; "Merkezi tıbbi arşivin hastane bünyesinde bulunması zorunlu değildir." cümlesi eklenmiştir.

Davacı tarafından, tıbbi arşivin hastane bünyesinden çıkarılmasının sağlık hakkının özüne aykırı olduğu, arşiv kaydının hastaya verilen tıbbi bakımın değerlendirilmesinde kullanılabilecek önemli bir kaynak teşkil ettiği, dosyaların çabuk ve kolay bulunması, derhal hazır bulundurulması gerekliliği ile örtüşmediği, arşiv standartları belirlenmeyerek hasta haklarının açıkça ihlal edildiği iddia edilerek anılan düzenlemenin iptali istenilmektedir.

Tıbbi kayıtların arşivlenmesi ile, tıbbi kayıtların toplanmasının, düzenlenmesinin, kaybının engellenmesinin, denetim, bilimsel çalışmalar, istatistiksel değerlendirmeler, adli mercilerce istenmesi, hastaların diğer müracaatları gibi durumlar için hazır bulundurulmasının amaçlandığı, önemli olan hususun merkezi tıbbi arşivin bu amaca hizmet etmesi ve ulaşılabilir olması durumu olduğu gözönünde bulundurulduğunda, merkezi tıbbi arşivin özel hastane bünyesinde bulunmasını zorunlu kılmayan dava konusu düzenlemede hizmet gereklerine ve hukuka aykırılık görülmemiştir.

2) Dava konusu Yönetmeliğin 26. maddesi ile değiştirilen 49. maddesinin 4. fıkrasının incelenmesi:

27/03/2002 tarih ve 24708 sayılı Resmî Gazete'de yayımlanan Özel Hastaneler Yönetmeliği'nin 49. maddesinin 4. fıkrasında, "Kanunun 3 üncü maddesi uyarınca Bakanlık tarafından kurulacak kayıt ve bildirim sistemine ve Bakanlıkça yapılacak diğer iş ve işlemlere esas olmak üzere, istenilen bilgi ve belgelerin Bakanlığa gönderilmesi zorunludur." hükmü yer almakta iken; dava konusu değişiklik ile anılan fıkra "Özel hastaneler tarafından kayıt altına alınan kişisel sağlık verileri, 6698 sayılı Kişisel Verilerin Korunması Kanununa uygun bir şekilde işlenir ve Bakanlıkça belirlenen usul ve esaslara uygun bir şekilde merkezi sağlık veri sistemine aktarılır. Bakanlık tarafından kurulan kayıt ve bildirim sistemine ve Bakanlıkça yapılacak diğer iş ve işlemlere esas olmak üzere, istenilen bilgi ve belgelerin Bakanlığa gönderilmesi zorunludur." şeklinde yeniden düzenlenmiştir.

Anılan değişiklik ile sağlık kuruluşları tarafından kayıt altına alınan kişisel sağlık verilerinin, 6698 sayılı Kişisel Verilerin Korunması Kanunu'na uygun bir şekilde işleneceği ve Bakanlıkça belirlenen usul ve esaslara uygun bir şekilde merkezi sağlık veri sistemine aktarılacağı kuralına yer verilmiştir.

07/04/2016 tarih ve 29677 sayılı Resmî Gazete'de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu, Türkiye Büyük Millet Meclisi'ne sunulan genel gerekçesinden de anlaşılacağı üzere, kişisel verilerin korunması konusunun pek çok sektörü ve kamu ya da özel kurumu ilgilendirmesi nedeniyle bir "çerçeve kanun" olarak hazırlanmıştır.

Bu Kanun'a duyulan ihtiyacı açıklayan genel gerekçede, Türk Ceza Kanunu'nun 135. ve devamı maddelerinde kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa edilmesi fiillerinin suç olarak düzenlendiği ve yaptırıma bağlandığı, ancak kişisel verilerin işlenmesine yönelik

özel bir kanun bulunmaması sebebiyle, bu fiillerin ne zaman hukuka aykırı ne zaman hukuka uygun olduğunun belirlenmesinde tereddütler yaşandığı vurgulanmaktadır.

Ayrıca 2010 yılında Anayasa'nın 20. maddesinde yapılan düzenlemeyle kişisel verilerin korunması temel bir insan hakkı olarak güvence altına alınmış ve konuya ilişkin usul ve esasların kanunla düzenleneceği öngörülmüştür.

Genel gerekçede, kişisel verilerin korunmasına yönelik bir kanunî düzenleme olmamasının uluslararası ilişkiler açısından da sorunlar yarattığı, EUROPOL, EUROJUST gibi Avrupa kurumları ile ilişkilerin sekteye uğradığı, sağlık kuruluşlarınca tutulan kişisel verilerin güvenliğinin sağlanmasında yeterli yasal önlem olmamasının Avrupa İnsan Hakları Mahkemesince özel hayatın gizliliğine müdahale olarak kabul edildiği ve bu nedenle ihlal kararları verildiği belirtilmektedir. Yine genel gerekçede, bu Kanunun Türkiye'nin Avrupa Birliği'ne üyelik süreci açısından da önemine dikkat çekilmekte, Türkiye'nin, Avrupa Konseyi tarafından tüm üye ülkelerde kişisel verilerin aynı standartlarda korunması ve sınır ötesi veri akışı ilkelerinin belirlenmesi amacıyla hazırlanan 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"ne de 1981 yılından itibaren taraf olduğu ifade edilmektedir.

Bütün bu hususlardan anlaşılacağı üzere 6698 sayılı Kanun, kişisel verilerin korunması konusunda önemli bir yasal boşluğu doldurmak amacıyla kabul edilen çerçeve niteliğinde bir yasal düzenlemedir. Genel gerekçede yer verilen şu tespit Kanun ile oluşturulan Kişisel Verileri Koruma Kurulunun genel kontrol ve denetleme işlevlerine dikkat çekmesi bakımından önemlidir: "Ülkemizde kişisel verilerin işlenmesi sürecini kontrol edecek ve denetleyecek bir kurum bulunmamaktadır. Bunun bir sonucu olarak halen kişisel veriler yeterli düzenleme ve denetime tabi olmaksızın, birçok kişi veya kurum tarafından kullanılabilmekte ve bu durum bazı hak ihlallerinin yaşanmasına sebep olabilmektedir."

Bu bağlamda, 6698 sayılı Kanun'un 21. maddesi hükümlerine göre oluşturulan Kişisel Verileri Koruma Kurulunun görev ve yetkileri, aynı Kanun'un 22. maddesiyle belirlenmiştir. 22. maddenin 1. fıkrasının (h) bendinde "Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek" hükmüne yer verilmiştir.

Anılan Kanun'un, "Özel nitelikli kişisel verilerin işlenme şartları" başlıklı 6. maddesinin 1. fıkrasında, dava konusu Yönetmelikle düzenlenen, sağlık verilerinin de özel nitelikli kişisel veri olduğu belirtilmiş; maddenin 4. fıkrasında, "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü getirilmiştir.

Dava dosyasının incelenmesinden, anılan Kanun hükümleri çerçevesinde, dava konusu düzenleme tesis edildiğinde özel nitelikli kişisel veri olarak kabul edilen sağlık verilerinin işlenmesinde alınması gerekli olan önlemlerin Kişisel Verileri Koruma Kurulu tarafından belirlenmediği ve Kanun'un 22. maddesinin 1. fıkrasının (h) bendine göre diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında Kurul görüşü alınmadan dava konusu düzenlemenin tesis edildiği görülmektedir.

Bu durumda, 6698 sayılı Kişisel Verilerin Korunması Kanunu'na göre sağlık gibi özel nitelikli verilerin işlenmesinde uyulacak önlemleri belirlemekle yetkili olan Kişisel Verileri Koruma Kurulu tarafından bu alana ilişkin yeterli önlemler belirlenmeden ve mevzuat taslağı hakkında Kurul görüşü alınmadan tesis olunan dava konusu düzenlemede hukuka uyarlık bulunmamaktadır.

3) Dava konusu Yönetmeliğin 36. maddesi ile değiştirilen ek 5. maddesinin 1. fıkrasının (e) bendinin (5) numaralı alt bendinin incelenmesi:

Dava konusu Yönetmeliğin 36. maddesi ile asıl Yönetmeliğin ek 5. maddesinin 1. fıkrasının (e) bendinin (5) numaralı alt bendi; "Özel Sağlık Kuruluşlarında çalışan tabip/uzman tabipler, 1219 sayılı Kanununun 12 nci maddesine uygun olmak kaydıyla, çalıştıkları sağlık kuruluşundaki çalışma saatleri dışında başka bir özel hastanenin acil servis, klinik servis ve ünitelerinde nöbet tutabilir. Bu tabiplerin nöbet listesi aylık olarak düzenlenir ve Müdürlükçe onaylanır. Özel hastane kadrosunda çalışan tabip ve uzman tabipler, hastanedeki çalışma saatleri dışında 1219 sayılı Kanununun 12 nci maddesine uygun olmak kaydıyla kurumsal sözleşme yapılarak diğer özel hastane veya tıp merkezlerinde çalıştırılabilir. Ancak, bu durumda tabip ve uzman tabiplerin muvafakatinin alınması zorunludur. Sözleşme Müdürlüğe bildirilir ve ilgili tabip ve uzman tabiplere çalışma belgesi düzenlenir. Özel hastanenin kadrosunda çalışan sözleşmeye konu tabip ve uzman tabiplerin kadrodan ayrılmaları halinde sözleşme sona erer." şeklinde değiştirilmiştir.

Düzenleme ile, kadrolu çalışmanın istisnalarına bir yenisinin eklendiği, bir özel hastanede kadrolu çalışan tabibe, kurumsal sözleşme yapılarak, kadro şartı aranmaksızın başka sağlık kuruluşlarında çalışma imkânı sağlandığı, bu şekilde çalışmanın hekimin muvafakati şartına bağlandığı, ayrıca tabiplere çalıştıkları sağlık kuruluşundaki çalışma saatleri dışında bir özel hastanenin acil servis, klinik servis ve ünitelerinde nöbet tutabilme imkânı getirildiği, böylece planlama kapsamındaki kısıtlı tabip insan gücünün kaliteli ve verimli kullanılabilmesinin amaçlandığı anlaşılmakla anılan düzenlemede kamu yararı ve hizmet gerekleri ile hukuka aykırılık görülmemiştir.

4) Dava konusu Yönetmeliğin 37. maddesi ile değiştirilen ek 8. maddesinin incelenmesi:

Dava konusu Yönetmeliğin 37. maddesi ile asıl Yönetmeliğin ek 8. maddesi değiştirilmiş ve maddede; “Vakıf üniversiteleri ile işbirliği yapan özel hastanelere planlamadan istisna olarak, sadece üniversiteden görevlendirilmiş doçent ve profesör unvanlı öğretim üyelerine mahsus olmak ve sadece işbirliği yapılan hastanede çalışmak üzere asgari öğretim üyesi standartları açısından Yükseköğretim Kurulunun görüşü ve Bakanlık kadro planlamaları dikkate alınarak Bakanlıkça uzmanlık dalı ilavesi ve ek kadro tahsisi yapılabilir. Bu hastanelere uzmanlık dallarının gerektirdiği tıbbi hizmet birimleri ve teknoloji yoğunluklu tıbbi cihazlar kurdurulabilir. Özel hastaneye tahsis edilen bu kadrolar ve uzmanlık dalları ile tıbbi hizmet birimleri ve teknoloji yoğunluklu tıbbi cihazlar, işbirliğinin sona ermesi halinde hastane hekim kadrosu ve faaliyet izin belgesinden düşülür.” hükmüne yer verilmiştir.

Anılan madde, önce 31/05/2019 tarihli ve 30790 sayılı Resmî Gazete'de yayımlanan Özel Hastaneler Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmeliğin 10. maddesi ile başlığı ile birlikte aşağıdaki şekilde değiştirilmiştir.

“Vakıf üniversitelerine ait hastaneler ve vakıf üniversiteleri ile özel hastane işbirliği

EK MADDE 8 - Vakıf üniversitelerine ait hastaneler ilgili mevzuattan kaynaklanan muafiyetleri saklı kalmak kaydıyla bu Yönetmelikte öngörülen planlama, ön izin ve ruhsatlandırma şartları ile sağlık insan gücü kriterlerine, bina, fizik yapı, tesis, tıbbi donanım ve hizmet standartlarına uyar.

Vakıf üniversitelerine ait hastanelerin ruhsatları üniversitenin adıyla düzenlenir ve hastane yalnızca üniversite tarafından işletilir. Hastane ruhsatında yazılı isim dışında isim kullanılamaz. Laboratuvar ve görüntüleme hizmetleri dışında tüm tıbbi hizmet birimlerinin ruhsat sahibi üniversite tarafından işletilmesi zorunludur. İşletme hakkının kısmen veya tamamen gerçek veya tüzel kişilere hiçbir şekilde devri mümkün değildir. Bu maddenin yürürlüğü girdiği tarihten önce Bakanlıkça vakıf üniversitelerine verilmiş hastane ön izinleri bir kereye mahsus olmak üzere ön izne esas projelerindeki kapasiteleriyle sınırlı olmak ve 68 inci maddede öngörülen sürelerde ruhsatname alınmak kaydıyla devredilebilir.

Tıp ve diş hekimliğinde lisans eğitimi, tıp, diş hekimliği ve eczacılıkta uzmanlık eğitimi ile araştırma faaliyetleri için yeterli kapasite ve eğitim altyapısı bulunan özel hastaneler; tıp ve/veya diş hekimliği fakültesi bulunan ancak hastanesi bulunmayan veya hastanesinde yeterli kapasite ve eğitim altyapısı bulunmayan vakıf üniversiteleri ile bütçeleri ayrı olmak şartıyla işbirliği yapabilir.

Vakıf üniversiteleri ile işbirliği yapan özel hastanelere üniversiteden görevlendirilecek doçent ve profesör unvanlı öğretim üyeleri için hastanenin ruhsatında kayıtlı mevcut uzman hekim kadroları

kullanılmak zorundadır. Hastane uzman hekim kadrosunun YÖK tarafından belirlenen asgari eğitim standardı için yetersiz olması halinde hastane, kendi kadrosunda bulunan başka bir uzmanlık dalı kadrosunu Bakanlık ile becayiş yoluyla değiştirerek asgari eğitim standardını sağlayabilir. İşbirliği protokolü kapsamında hastaneye planlamadan istisna uzman hekim kadrosu, tıbbi hizmet birimi ile teknoloji yoğunluklu tıbbi cihaz verilmez. Bu fıkranın yürürlüğe girdiği tarihten önce vakıf üniversitesi ile işbirliği protokolü bulunan hastanelere Bakanlıkça planlamadan istisna olarak verilmiş bulunan uzman hekim kadroları ve uzmanlık dallarının gerektirdiği tıbbi hizmet birimleri ile teknoloji yoğunluklu tıbbi cihazlar protokol süresinin bitiş tarihinde herhangi bir işleme gerek kalmaksızın iptal edilmiş sayılır. Ancak, protokolün bitmesine iki yıldan az süre kalmış hastanelerin iptal işlemleri bu Yönetmeliğin yayımlandığı tarihten itibaren ikinci yılın sonunda uygulanır.

Vakıf üniversiteleri kadrolarında bulunan öğretim üyesi tabip, diş tabibi ve tıpta uzmanlık mevzuatına göre uzman olanlar tıp fakültesi/diş hekimliği fakültesinin bulunduğu il dışındaki özel hastanelerde çalışamaz. Bu fıkranın hükümlerine aykırı olarak çalışan öğretim üyelerinin görevlendirmeleri 31/12/2019 tarihinde sonlandırılır.”

Ardından anılan maddenin ikinci fıkrası 28/09/2019 tarihli ve 30902 sayılı Resmî Gazete'de yayımlanan Yönetmeliğin 6. maddesi ile; "Vakıf üniversitelerine ait hastanelerin ruhsatları üniversitenin adıyla düzenlenir ve hastane yalnızca üniversite tarafından işletilir. Hastane ruhsatında yazılı isim dışında isim kullanılamaz. Laboratuvar ve görüntüleme hizmetleri dışında tüm tıbbi hizmet birimlerinin ruhsat sahibi üniversite tarafından işletilmesi zorunlu olup, işletme hakkının kısmen veya tamamen gerçek veya tüzel kişilere hiçbir şekilde devri mümkün değildir. Bakanlıkça vakıf üniversite hastanelerine/ek birimlerine verilen ön izinler, faal en az bir hastanesi olması kaydıyla ön izin alındığı ilden, planlama ilkeleri çerçevesinde sağlık hizmeti sunulması için öngörülen asgari nüfus ve/veya ilde verilmesi hedeflenen sağlık hizmetleri ile uzman tabip dağılımı yönünden daha az yoğunluklu diğer bir ile taşınmak şartı ve Bakanlık onayı ile bir kereye mahsus devredilebilir. En az bir faal hastanesi olan vakıf üniversiteleri, faal diğer hastanelerini/ek birimleri veya askıda olan hastanelerini/ek birimlerini aynı ilde veya planlama ilkeleri çerçevesinde sağlık hizmeti sunulması için öngörülen asgari nüfus ve/veya ilde verilmesi hedeflenen sağlık hizmetleri ile uzman tabip dağılımı yönünden daha az yoğunluklu diğer bir ile taşınmak şartı ve Bakanlık onayı ile bir kereye mahsus olmak kaydıyla devredebilir.” şeklinde değiştirilmiştir.

Bu durumda; dava açıldıktan sonra dava konusu düzenleme değiştirilerek yeni bir düzenlemeye gidilmesi nedeniyle davanın konusuz kaldığı görüldüğünden, bu düzenlemeye ilişkin olarak davanın esası hakkında karar verilmesine yer bulunmamaktadır.

KARAR SONUCU:

Açıklanan nedenlerle;

1. 22/03/2017 tarih ve 30015 sayılı Resmî Gazete'de yayımlanan Özel Hastaneler Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmeliğin 26. maddesi ile değiştirilen asıl Yönetmeliğin 49. maddesinin 4. fıkrasının İPTALİNE oyçokluğuyla,
2. Anılan Yönetmeliğin 26. maddesi ile asıl Yönetmeliğin 49. maddesinin 1. fıkrasına eklenen, "merkezi tıbbi arşivin hastane bünyesinde bulunması zorunlu değildir." ibaresi ve 36. maddesi ile değiştirilen asıl Yönetmeliğin ek 5. maddesinin 1. fıkrasının (e) bendinin (5) numaralı alt bendi yönünden DAVANIN REDDİNE oybirliğiyle,
3. Anılan Yönetmeliğin 37. maddesi ile değiştirilen asıl Yönetmeliğin ek 8. maddesi yönünden KARAR VERİLMESİNE YER OLMADIĞINA oybirliğiyle,
4. Dava kısmen iptal, kısmen ret, kısmen karar verilmesine yer olmadığına şeklinde sonuçlandırıldığından aşağıda dökümü yapılan ... TL yargılama giderinin ... TL'sinin davacı üzerinde bırakılmasına, ... TL'sinin davalı idareden alınarak davacıya verilmesine,
5. Karar tarihinde yürürlükte bulunan Avukatlık Asgari Ücret Tarifesi uyarınca duruşmalı işler için belirlenen ... TL avukatlık ücretinin davalı idareden alınarak davacıya, ... TL avukatlık ücretinin davacıdan alınarak davalı idareye verilmesine,
6. Posta gideri avansından artan tutarın kararın kesinleşmesinden sonra davacıya iadesine,
7. Bu kararın tebliğ tarihini izleyen 30 (otuz) gün içerisinde, Danıştay İdari Dava Daireleri Kuruluna temyiz yolu açık olmak üzere, 29/12/2020 tarihinde karar verildi.

KARŞI OY

(X) :

07/04/2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 21. maddesi hükümlerine göre oluşturulan Kişisel Verileri Koruma Kurulu'nun görev ve yetkileri, aynı Kanun'un 22. maddesiyle belirlenmiştir.

Mezkûr Kanun'un 22. maddenin 1. fıkrasının (h) bendinde "Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek" hükmüne yer

verilmiş olup, söz konusu hükümden diğer kurum ve kuruluşlarca hazırlanacak mevzuat taslakları hakkında Kuruldan görüş alınmasının zorunlu olduğu anlamı çıkarılamaz.

Ayrıca, anılan Kanun'un 6. maddesinin 4. fıkrasında, "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü yer almaktadır. Bu hükme göre Kurul tarafından yeterli önlemlerin belirlenmemesinin diğer kurum ve kuruluşlarca düzenleyici işlem yapılmasına engel teşkil edeceği düşünülemez. Anılan hükme göre kurum ve kuruluşların, mevzuat taslaklarını hazırlarken, Kurul tarafından belirlenmiş önlemler varsa bunları dikkate alacakları konusunda kuşku yoktur. Ancak maddede sözü geçen önlemler Kurul tarafından bir kereye mahsus kararlaştırılıp daha sonra değiştirilemeyecek önlemler değildir. Kurul her zaman, belirlediği önlemleri değiştirebilir, uluslararası gelişmelere, zamanın gereklerine vs. göre yenilerini ekleyebilir. Kişisel verileri işleyenlerin, Kurul tarafından herhangi bir zamanda belirlenen önlemleri her zaman dikkate alacağı açıktır.

Açıklanan nedenlerle, dava konusu düzenlemede bu yönüyle hukuka aykırılık bulunmadığından dava konusu Yönetmeliğin 26. maddesi ile değiştirilen asıl Yönetmeliğin 49. maddesinin 4. fıkrası yönünden de davanın reddine karar verilmesi gerektiği oyuyla bu madde yönünden aksi yöndeki çoğunluk kararına katılmıyoruz.

Danıştay Kararı - 12. Daire (E. 2019/5658)

Danıştay Kararı - 12. D., E. 2019/5658 K. 2020/3136 T. 12.10.2020

T.C. DANIŞTAY ONİKİNCİ DAİRE

Esas No: 2019/5658

Karar No: 2020/3136

TEMYİZ EDEN (DAVACI): ...

VEKİLLERİ: ...

KARŞI TARAF (DAVALI): Kayseri Valiliği / KAYSERİ

VEKİLİ: ...

İSTEMİN KONUSU: ... Bölge İdare Mahkemesi ... İdari Dava Dairesinin ... tarih ve E:..., K:... sayılı kararının temyizen incelenerek bozulması istenilmektedir.

YARGILAMA SÜRECİ:

Dava konusu istem: ... İli, ... İlçesi ... İmam Hatip Ortaokulu'nda hizmetli olarak görev yapan davacı tarafından; taklit anahtarla kilit açmak suretiyle hırsızlık suçundan dolayı 2 yıl 3 ay hapis cezası aldığı ve bu kararın Yargıtayca onanarak kesinleşmesi üzerine ... Cumhuriyet Savcılığınca ... tarihli ve ... sayılı dosyası ile cezasının infaz edildiği, bu nedenle 657 sayılı Devlet Memurları Kanunu'nun 48/A-5 ve 98/b maddeleri gereği Devlet memuru olma sıfatını kaybettiğinin anlaşıldığından bahisle Devlet memurluğundan çıkarılmasına ilişkin Valilik Makamı'nın ... tarihli ve E... sayılı işleminin iptaline karar verilmesi istenilmiştir.

İlk Derece Mahkemesi kararının özeti: ... İdare Mahkemesince verilen ... tarih ve E:..., K:... sayılı kararda; 657 sayılı Kanunun anılan 48/A-5 maddesinde devlet memuru olabilmek için yüz kızartıcı suçlardan mahkum olmamak koşulu arandığından, 5237 sayılı Türk Ceza Kanununun 53/4 maddesi yüz kızartıcı bir suçtan dolayı mahkumiyet kararı almış kişiler yönünden devlet memuru olabilmek koşullarını sağlama bakımından bir hak doğurmadığı,(Dan.İDDK. E.2007/2368-K.2011/1214), (Dan.12.D.E.2015/3412-K.2015/4807), diğer taraftan, halihazırda kamu görevlisi olanlar bakımından; yine 657 sayılı Kanun'un 98/b maddesinde, devlet memurlarının memurluğa alınma şartlarından herhangi birini taşımadığının sonradan anlaşılması veya memurlukları sırasında bu şartlardan herhangi

birinin kaybedilmesinin memuriyetten çıkarmayı gerektiren bir sebep olarak yer almakta ve personelin kamu görevinden çıkarılacağı düzenlendiği, bu durumda, davacının mahkumiyetine karar verilen "Taklit Anahtarla Kilit Açmak Suretiyle Hırsızlık" suçundan 2 yıl 3 ay hapis cezası ile mahkumiyetin 657 sayılı Kanun'un 48/A-5. maddesinde yer alan "Türk Ceza Kanununun 53. maddesinde belirtilen süreler geçmiş olsa bile". "Affa uğramış olsa bile" ifadeleri nedeniyle davacı lehine bir hak doğurmayacağı göz önüne alındığında, davacının 657 sayılı Kanun'un 48/A-5. maddesinde öngörülen şartları taşımadığı ve Devlet memuru olarak istihdamının mümkün olmadığı anlaşıldığından, davacının devlet memurluğundan çıkarılmasına ilişkin dava konusu işlemde hukuka aykırılık bulunmadığı, diğer taraftan davacı vekilince davacının durumu ile alakalı Maarif müfettişlerince yapılan inceleme bir disiplin soruşturması olarak değerlendirilerek müvekkilinin savunmasının alınmadığı, bu suretle savunma hakkının kısıtlandığı iddiasında bulunmuş ise de, yapılan incelemenin 657 sayılı Kanun'un 125. maddesi kapsamında bir disiplin soruşturması olmadığı, 657 sayılı Kanun'un 48/A-5 ve 98/b maddeleri kapsamında yapılan bir inceleme ve değerlendirme olduğu görüldüğünden bu iddiaya itibar edilmediği, nitekim; Danıştay Onikinci Dairesinin 30.03.2017 tarih ve E:2016/8129, 2017/1088 sayılı kararında bu yönde olduğu gerekçeleriyle davanın reddine karar verilmiştir.

Bölge İdare Mahkemesi kararının özeti: ... Bölge İdare Mahkemesi ... İdari Dava Dairesince; istinaf başvurusuna konu İdare Mahkemesi kararının hukuka ve usule uygun olduğu ve davacı tarafından ileri sürülen iddiaların söz konusu kararın kaldırılmasını gerektirecek nitelikte görülmediği gerekçesiyle 2577 sayılı İdari Yargılama Usulü Kanunu'nun 45. maddesinin üçüncü fıkrası uyarınca istinaf başvurusunun reddine karar verilmiştir.

TEMYİZ EDENİN İDDİALARI: Davacı tarafından, Anayasa Mahkemesi'nin 27/02/2019 tarihli ve 2014/7256 Başvuru numaralı kararında davacı ile aynı durumda olan başvurusunun 18 yaşından önce işlemiş olduğu yüz kızartıcı suç sebebiyle memuriyetten çıkartılamayacağına, özel hayatın gizliliği hakkının ihlaline karar verildiği, henüz yaşamın ciddiyetini kavrayamadığı 14 yaşında iken ve Çocuk Esirgeme Kurumu yurdunda kalırken karıştığı suç fiilinin sonuçlarını hesap edemeyeceği açık olduğu, tüm hayatı boyunca etkileneceği, TCK'nın 53/4 maddesinde 18 yaşını doldurmamış olanlar hakkında TCK'nın 53/1 maddesinin uygulanmayacağı belirtilmiştir, 657 sayılı Devlet Memurları Kanunu'nda bu durumun aksini belirtir özel düzenleme bulunmadığı, bu nedenle 18 yaşından küçük iken işlenen suçla ilgili memuriyetten çıkarılma kararının verilemeyeceği ileri sürülmektedir.

KARŞI TARAFIN SAVUNMASI: Davalı idare tarafından, davacının ... Çocuk Mahkemesinin ... tarihli ve E:..., K:... sayılı kararı ile taklit anahtarla kilit açmak suretiyle hırsızlık suçundan dolayı 2 yıl

3 ay hapis ceza aldığı, ... Ceza Dairesinin ... tarihli ve E:..., K:... sayılı kararı ile yerel mahkeme kararının onandığı, bunun üzerine davacı hakkında idari soruşturma başlatıldığı, inceleme sonucunda 657 sayılı Devlet Memurları Kanunu'nun 48/A-5 ve 98/b maddeleri gereği Devlet memuru olma sıfatını kaybettiğinin anlaşıldığından bahisle Devlet memurluğundan çıkarılması teklif edildiği ve davacı hakkında 657 sayılı Devlet Memurları Kanunu'nun 48/A-5 ve 98/b maddeleri uyarınca Devlet memurluğundan çıkarılmasına ilişkin işlemin tesis edildiği, dava konusu işlemin mevzuata uygun olduğu belirtilerek istemin reddi gerektiği savunulmuştur.

DANIŞTAY TETKİK HÂKİMİ: ...

DÜŞÜNCEİ: Dava; ... ili, ... ilçesi, ... İmam Hatip Ortaokulu'nda hizmetli olarak görev yapan davacının, 657 sayılı Devlet Memurları Kanunu'nun 48/A-5 ve 98/b maddeleri uyarınca Devlet memurluğundan çıkarılmasına ilişkin ... tarihli ve E/... sayılı işlemin iptali istemiyle açılmıştır.

Dosyanın incelenmesinden, 19/11/1997 doğumlu olan davacının, 29/08/2012 tarihinde işlemiş olduğu "taklit anahtarla kilit açmak suretiyle hırsızlık" suçundan ... Çocuk Mahkemesi'nin ... tarih ve E:..., K:... sayılı kararı ile 2 yıl 3 ay hapis cezası ile cezalandırılmasına karar verildiği, bu kararın ... Ceza Dairesi'nin ... tarih ve E:..., K:... sayılı kararı ile onanması üzerine 27/08/2018 tarihinde tutuklandığı anlaşılmaktadır. Bunun üzerine İl Milli Eğitim Müdürlüğü tarafından davacı hakkında başlatılan idari soruşturma neticesinde davacının Devlet memuru olma vasfını kaybettiği değerlendirilerek 657 sayılı Devlet Memurları Kanunu'nun 48/A-5 ve 98/b maddeleri uyarınca Devlet memurluğundan çıkarılmasına karar verildiği, bakılan davanın bu işlemin iptali istemiyle açıldığı anlaşılmıştır.

Anayasa'nın "Özel hayatın gizliliği" başlıklı 20. maddesinin birinci fıkrasında;

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz" hükmüne, üçüncü fıkrasında; "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilmiştir.

Avrupa İnsan Hakları Sözleşmesinin "Özel ve aile hayatına saygı hakkı" başlıklı 8. maddesinde de;

"(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı,

düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir," hükmü yer almaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 6. maddesinde;

"(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü yer almaktadır.

657 sayılı Devlet Memurları Kanunu'nun, Devlet memurluğuna alınma şartlarının düzenlendiği 48. maddesinin, birinci fıkrasının (A) bendinin 5 numaralı alt bendinde; "Türk Ceza Kanunu'nun 53'üncü maddesinde belirtilen süreler geçmiş olsa bile; kasten işlenen bir suçtan dolayı bir yıl veya daha fazla süreyle hapis cezasına ya da affa uğramış olsa bile devletin güvenliğine karşı suçlar, Anayasal düzene ve bu düzenin işleyişine karşı suçlar, devlet sırlarına karşı suçlar ve casusluk, zimmet, irtikâp, rüşvet, hırsızlık, dolandırıcılık, sahtecilik, güveni kötüye kullanma, hileli iflas, ihaleye fesat karıştırma, edimin ifasına fesat karıştırma, suçtan kaynaklanan malvarlığı değerlerini aklama veya kaçakçılık suçlarından mahkum olmamak" hükmüne yer verilmiştir.

5237 sayılı Türk Ceza Kanunu'nun "Güvenlik Tedbirleri, Belli Hakları Kullanmaktan Yoksun Bırakılma" başlıklı 53. maddesinde "Kişi, kasten işlemiş olduğu suçtan dolayı hapis cezasına mahkûmiyetin kanuni sonucu olarak; sürekli, süreli veya geçici bir kamu görevinin üstlenilmesinden; bu kapsamda, Türkiye Büyük Millet Meclisi üyeliğinden veya Devlet, il, belediye, köy veya bunların denetim ve gözetimi altında bulunan kurum ve kuruluşlarca verilen, atamaya veya seçime tâbi bütün memuriyet ve hizmetlerde istihdam edilmekten ... yoksun bırakılır. (2) Kişi, işlemiş bulunduğu suç dolayısıyla mahkûm olduğu hapis cezasının infazı tamamlanuncaya kadar bu hakları kullanamaz. (4)

Kısa süreli hapis cezası ertelenmiş veya fiili işlediği sırada on sekiz yaşını doldurmamış olan kişiler hakkında birinci fıkra hükmü uygulanmaz. " hükmüne yer verilmiştir.

5352 sayılı Adli Sicil Kanunu'nun 10.maddesinin üçüncü fıkrasında, "Onsekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebilir. " hükmü yer almaktadır.

07/09//2005 tarihli ve 25929 sayılı Resmi Gazete'de yayımlanan Adli Sicil Yönetmeliği'nin 12. maddesinin dördüncü fıkrasında, "Onsekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere mahkeme, hâkim veya savcılıklarca istenebilir." hükmü ile 14. maddesinin birinci fıkrasında, "Onsekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere mahkeme, hâkim veya savcılıklara talep halinde verilir." hükmü yer almaktadır.

Anayasa Mahkemesi'nin 27/02/2019 tarihli ve 2014/7256 Başvuru no'lu kararında özetle;

"..Somut olayda başvurucunun on sekiz yaşından küçükken işlediği suçun kayıtlarının ... Valiligi Emniyet Müdürlüğü tarafından Komisyon Başkanlığına verildiği, bu kaydın dikkate alınmak suretiyle güvenlik soruşturmasının olumsuz sonuçlandığı, başvurucunun sözleşmeli infaz ve koruma memurluğuna atamasının yapılmadığı anlaşılmaktadır.

Resmi makamlar tarafından muhafaza edilmekte olan, başvurucu hakkında yürütülen ceza yargılamasına dair bilgilerin özel hayata saygı hakkı anlamında kişisel nitelikli veriler olduğu açıktır. Söz konusu kişisel verinin kamu kurumlarıyla paylaşılması ve güvenlik soruşturmalarında kullanılmasının Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkına bir müdahale oluşturduğu sonucuna varılmıştır...

Öte yandan somut olayda başvurucunun yazılı ve sözlü sınavı kazandığının ilan edilmiş olduğu, on sekiz yaşından küçükken işlediği suça ilişkin kaydın 5352 sayılı Kanun'un 10. maddesinin (3) numaralı fıkrasında yer alan hükme açıkça aykırı şekilde idari makamlara verilmiş olduğu dikkate alındığında özel hayata saygı hakkına yönelik müdahalenin bu yönüyle de kanuni dayanaktan yoksun olduğu anlaşılmaktadır..." değerlendirmelerine yer verilmiştir.

Dosya içerisinde yer alan bilgi ve belgeler ile Anayasa Mahkemesi kararı doğrultusunda dava konusu olay incelendiğinde, 19/11/1997 doğumlu olan ve hakkındaki ceza mahkûmiyetine konu suçu işlediği 29/08/2012 tarihinde on sekiz yaşından küçük olan davacının, on sekiz yaşından küçükken işlediği bu suçun dikkate alınması suretiyle memuriyet görevine son verildiği, davacının 28/09/2020 tarihinde

UYAP üzerinden adli sicil ve arşiv kaydının sorgulaması sonucunda ise adli sicil kaydı ve adli sicil arşiv kaydının bulunmadığının yazılı olduğu görülmüştür.

Bu durumda, davacının adli sicil kaydında görünmeyen, on sekiz yaşından küçükken işlediği suça ilişkin kaydın, yukarıda yazılı Kanun ve Yönetmelik hükümleri uyarınca, ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebileceği, kişisel veri niteliğinde olduğu, kamu görevlerine yapılacak atamalar dolayısıyla ilgili kamu kurumuna verilemeyeceği açık olduğundan, söz konusu mahkûmiyetin 657 sayılı Kanun'un 48/A-5 maddesi kapsamında memuriyetine engel teşkil etmesi de mümkün değildir.

Bu itibarla, davacının on sekiz yaşından küçükken işlediği suça ilişkin mahkûmiyeti nedeniyle devlet memuru olma vasfını kaybettiğinden bahisle görevine son verilmesine ilişkin dava konusu işlemde hukuka uyarlık görülmediğinden, davanın reddi yönündeki ... İdare Mahkemesi kararına karşı yapılan istinaf başvurusunun reddi yolundaki temyize konu Bölge İdare Mahkemesi kararında hukuki isabet bulunmadığından Bölge İdare Mahkemesi kararının bozulması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay Onikinci Dairesince, Tetkik Hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereği görüldü:

HUKUKİ DEĞERLENDİRME:

Bölge idare mahkemelerinin nihai kararlarının temyizen bozulması, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 49. maddesinde yer alan sebeplerden birinin varlığı hâlinde mümkündür.

Anayasa Mahkemesi'nin 27/02/2019 tarihli ve 2014/7256 Başvuru no'lu kararında özetle; 5352 sayılı Adli Sicil Kanunu'nun 10. maddesinin üçüncü fıkrasında, on sekiz yaşından küçüklerle ilgili adli sicil ve arşiv kayıtlarının ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebileceğinin düzenlendiği, buna göre kişilerin on sekiz yaşından küçükken işlediği herhangi bir suça ait kayıtların idari makamlara bildirilmesinin hukuken mümkün olmadığı, somut olayda başvurusunun on sekiz yaşından küçükken işlediği suçun kayıtlarının ... Valiligi Emniyet Müdürlüğü tarafından Komisyon Başkanlığına verildiği, bu kaydın dikkate alınmak suretiyle güvenlik soruşturmasının olumsuz sonuçlandığı, başvurusunun sözleşmeli infaz ve koruma memurluğuna atamasının yapılmadığının anlaşıldığı, resmi makamlar tarafından muhafaza edilmekte olan, başvuru hakkında yürütülen ceza yargılamasına dair bilgilerin özel hayata saygı hakkı anlamında kişisel nitelikli veriler olduğu,

söz konusu kişisel verinin kamu kurumlarıyla paylaşılması ve güvenlik soruşturmalarında kullanılmasının Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkına bir müdahale oluşturduğu sonucuna varıldığı, öte yandan somut olayda başvuruçunun yazılı ve sözlü sınavı kazandığının ilan edilmiş olduğu, on sekiz yaşından küçükken işlediği suça ilişkin kaydın 5352 sayılı Kanun'un 10. maddesinin (3) numaralı fıkrasında yer alan hükme açıkça aykırı şekilde idari makamlara verilmiş olduğu dikkate alındığında özel hayata saygı hakkına yönelik müdahalenin bu yönüyle de kanuni dayanaktan yoksun olduğunun anlaşıldığı değerlendirilmelerine yer verilmiştir.

Uyuşmazlık konusu olayda ise davacının halihazırda 657 sayılı Devlet Memurları Kanunu'na tabi "Devlet memuru" statüsünde iken, hakkında hırsızlık suçundan 2 yıl 3 ay hapis cezasının kesinleştiği ve bu cezanın infaz edilmesi üzerine, 657 sayılı Devlet Memurları Kanunu'nun 48/A-5 ve 98/b maddeleri uyarınca Devlet memuru olma sıfatını kaybettiğinin anlaşıldığından bahisle Devlet memurluğundan çıkarılmasına ilişkin Valilik Makamı'nın 05/10/2018 tarihli ve E.18445001 sayılı işlemin tesis edildiği anlaşılmaktadır.

Dolayısıyla, uyuşmazlığın, 18 yaşından küçüklere ilişkin adli sici kayıtlarının, yetkisiz birimlere verilmesinden kaynaklanan ve Anayasa Mahkemesince "ihlal" kararı verilen uyuşmazlıklarla ilgisinin olmadığı sonucuna varıldığından, davacının bu yöndeki iddiası yerinde görülmemiştir.

Temyizen incelenen karar usul ve hukuka uygun olup, dilekçede ileri sürülen temyiz nedenleri kararın bozulmasını gerektirecek nitelikte görülmemiştir.

KARAR SONUCU:

Açıklanan nedenlerle;

1. Davacının temyiz isteminin reddine,
2. Davanın yukarıda özetlenen gerekçeyle reddine ilişkin İdare Mahkemesi kararına karşı yapılan istinaf başvurusunun reddi yolundaki temyize konu ... Bölge İdare Mahkemesi ... İdari Dava Dairesinin ... tarih ve E:..., K:... sayılı kararının yukarıda belirtilen açıklama ile birlikte ONANMASINA,
3. Temyiz giderlerinin istemde bulunan üzerinde bırakılmasına,
4. 2577 sayılı İdari Yargılama Usulü Kanunu'nun 50. maddesi uyarınca, bu onama kararının taraflara tebliğini ve bir örneğinin de ... Bölge İdare Mahkemesi ... İdari Dava Dairesine gönderilmesini teminen dosyanın ... İdare Mahkemesine gönderilmesine, 12/10/2020 tarihinde kesin olarak oybirliğiyle karar verildi.

Danıştay Kararı - 15. Daire (E. 2018/1490)

Danıştay Kararı - 15. D., E. 2018/1490 K. YD T. 8.5.2018

Dava konusu düzenlemenin üst normlara ve hukuka uygun olduğu, yürütmenin durdurulması isteminin ve davanın reddi gerektiği savunulmaktadır. Danıştay Tetkik Hakimi: Düşüncesi: Yürütmenin durdurulması isteminin kabulü gerektiği düşünülmektedir. TÜRK MİLLETİ ADINA Karar veren Danıştay Onbeşinci Dairesince davalı idarelerin birinci savunmaları alındıktan sonra incelenmesine karar verilen yürütmenin durdurulması istemi, savunmaların verildiği görülmüş olmakla incelenerek işin gereği görüldü: Dava, 24/11/2017 tarih ve 30250 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin tamamı ile anılan Yönetmelikle değiştirilen 20/10/2016 tarih ve 29863 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin; 5. maddesinin sekizinci fıkrasının, 7. maddesinin birinci fıkrasının, 8. maddesinin birinci fıkrasının yürütmesinin durdurulması ve iptali istemiyle açılmıştır.

T.C. DANIŞTAY ONBEŞİNCİ DAİRE

Esas No: 2018/1490

Davacılar ve Yürütmenin Durdurulmasını İsteyenler: 1-

2-

Vekili:

Davalılar: 1-

Vekilleri: Av.

2-

Vekili:

İstemin Özeti: 24/11/2017 tarih ve 30250 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin tamamı ile anılan Yönetmelikle değiştirilen 20/10/2016 tarih ve 29863 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında

Yönetmeliğin; 5. maddesinin sekizinci fıkrasının, 7. maddesinin birinci fıkrasının, 8. maddesinin birinci fıkrasının iptali ve yürütmesinin durdurulması istenilmektedir.

Savunmaların Özeti: Dava konusu düzenlemenin üst normlara ve hukuka uygun olduğu, yürütmenin durdurulması isteminin ve davanın reddi gerektiği savunulmaktadır.

Danıştay Tetkik Hakimi:

Düşüncesi: Yürütmenin durdurulması isteminin kabulü gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay Onbeşinci Dairesince davalı idarelerin birinci savunmaları alındıktan sonra incelenmesine karar verilen yürütmenin durdurulması istemi, savunmaların verildiği görülmüş olmakla incelenerek işin gereği görüldü:

Dava, 24/11/2017 tarih ve 30250 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin tamamı ile anılan Yönetmelikle değiştirilen 20/10/2016 tarih ve 29863 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin; 5. maddesinin sekizinci fıkrasının, 7. maddesinin birinci fıkrasının, 8. maddesinin birinci fıkrasının yürütmesinin durdurulması ve iptali istemiyle açılmıştır.

Davacılar tarafından, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin 20/10/2016 tarihinde yürürlüğe girdiği, Danıştay tarafından, Kişisel Verileri Koruma Kurulu'nun görüşü alınmadan çıkartılmış olan Yönetmeliğin tamamının yürütmesi durdurulduğu, Danıştay kararları ile Yönetmeliğin yürütmesinin durdurulmasından sonra Bakanlığın, dava konusu Yönetmelik ile asıl Yönetmeliğin bir takım maddelerinde değişiklikler yaptığı, dolayısıyla dava konusu Yönetmeliğin, esasen halen yürütmesi durdurulmuş olan bir yönetmelikte yapılan kısmi değişikliklere ilişkin olduğu, ortada yürütmesi durdurulmuş bir Yönetmelik olduğuna göre böyle bir değişikliğin yapılmasının, hukuk sistemimizde geçerli bulunmayan bir Yönetmelik üzerinde değişiklik olması sebebiyle uygulanamaz nitelikte olduğu, dava konusu Yönetmeliğin bir bütün olarak hukuka aykırı olduğu,

Kişisel Verileri Koruma Kurulu tarafından, sağlık verilerinin işlenmesinde alınacak önlemler belirlenmeden böyle bir yönetmelikle verilerin işlenmesinin hukuka aykırı olduğu, Kişisel Verileri Koruma Kurulunca henüz yaklaşık bir yıllık sürede çeşitli yayınlarla birlikte üç ayrı yönetmeliğin yayımlandığı, ancak, Kurul tarafından, özel nitelikli kişisel verilerin işlenebilmesi için şart olan önlemlere ilişkin bir belirlemede bulunulmadığı, insanların sağlık ve cinsel yaşamlarına ilişkin en

mahrem ve yaşam boyu deęiştirilmesi mümkün olmayan bilgilerini içeren veri kümesini oluşturan özel nitelikli kişisel verilerin Kurul tarafından belirlenen yeterli önlemlerin alınması şartı yerine getirilmeden işlenmesine olanak sağlayan dava konusu Yönetmeliğin bir bütün olarak hukuka aykırı olduğu,

Saęlık kurum ve kuruluşlarının, nın ve bütün tarafların verileri işlerken 6698 sayılı Kişisel Verilerin Korunması Kanununun 4. maddesindeki ilkelere uyma zorunluluęu olduğu, bu bağlamda, verilerin işlenmesinde özellikle "İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü, olma" ölçütüne uygun davranılması, bütün verilerin gönderilmesinin istenmesi yerine, toplanacak verilerin amaçla bağlantılı, sınırlı ve ölçülü olarak belirlenmesi gerektiğinin tartışmasız olduğu, saęlık verilerinin tamamının istenmesinin meşru amaçla açıklanamayacağı,

Yönetmeliğin 5. maddesinin sekizinci fıkrasına göre saęlık hizmeti sunucularının, Kanunun emredici hükümleri ile Kurul ve Bakanlık tarafından belirlenen usul ve esaslara uygun bir şekilde kişisel saęlık verilerini merkezi saęlık veri sistemine aktaracağı, bu düzenlemenin, saęlık verilerinin merkezi saęlık veri sistemine aktarılmasında Kanunun emredici hükümleri ile Kurul tarafından belirlenen usul ve esasların da dikkate alınacağını belirtmesi bakımından önceki kurala göre daha uygun olmakla birlikte kuralın özüne ilişkin hukuka aykırılığın devam etmekte olduğu, 7. maddenin birinci fıkrası ile 8. maddenin birinci fıkrasının ortak noktasının; kişisel saęlık verilerinin, hiçbir ayırım yapılmadan tarafından oluşturulan merkezi saęlık veri sistemine aktarılması zorunluluęu ve Bakanlığın da bu verileri dięer kamu kurum ve kuruluşlarına aktarabileceğine ilişkin olduğu, saęlık hizmet sunucularına getirilen bu zorunluluğun kapsamını belirlemeye/sınırlamaya yarar hiçbir hükmün Yönetmelikte bulunmadığı, saęlık hizmet sunucularının kayıt yapma süresinin, bu kaydın standardının ne olduğunun belirlenmediği gibi hangi alt düzenleyici işlemlerle, hangi birim tarafından bu belirlemenin yapılacağını da belirtilmediği, buna karşın, Yönetmelikte, belirsiz yükümlülüğün ihlali halinde uygulanacak yaptırıma yer verildiği, bu haliyle Yönetmelikte, uyulması gereken ölçüyü değil, ama sınırsız ve ölçüsüz veri paylaşılması yükümlülüğüne uyulmaması halindeki yaptırımı belirlemekle yetinildiği,

Dava konusu Yönetmelikte, saęlık hizmeti sunumunda görevli kişilerin, ilgili kişinin saęlık verilerini ancak verilecek olan saęlık hizmetinin gereği ile sınırlı olmak kaydıyla işleyebileceğinin belirtildiği, ancak, saęlık hizmeti sunucularına getirilen bu sınırlamanın, bütün kaynaklardan gelen özel nitelikli kişisel verilerin toplandığı merkezi sisteme idarenin erişmesi bakımından söz konusu edilmediği gibi verilerin merkezi sisteme anonimleştirilerek gönderilmesinin de düzenlenmediği, saęlık hizmet sunucularına Bakanlıkça belirlenen standartlarda yazılım kullanma zorunluluęu getirildiği, bu

yazılımları yapacak şirketlerin de Yönetmelik kapsamına alındığı; ancak, uyulması gereken standartların ne olduğu ve bunun kim ya da kimler tarafından belirleneceğine dair hükme Yönetmelikte yer verilmediği, yine sağlık hizmet sunucularına, kendilerine başvuran kişilere ait hangi verilerin, nasıl bir işleme tabi tutularak merkezi sisteme gönderileceğine dair kuralın da belirtilmediği, sağlık hizmet sunucularına getirilen aktarım zorunluluğu ile kişisel veri sahibine karşı sır saklama yükümlülükleri arasında bir denge kurulmadığı, bütün ülkenin sağlık verisinin, herhangi bir anonimleştirme yapılmadan bir merkezi sistemde tutulmasının yaratacağı sakıncanın açık olduğu, Yönetmeliğin kişisel verilerin sınırsız olarak merkezi sisteme aktarılmasına dair 5/8, 7/1 ve 8/1. maddesinin temel hakkın özüne zarar veren, amaçla uygun olmayan bir müdahale niteliğinde olduğu,

Kişisel sağlık verilerinin işlenmesini istisna değil, kural olarak belirleyen düzenlemenin hukuka aykırı olduğu, kişisel sağlık verilerinin işlenmesine olanak veren istisnaların sadece 108 sayılı Sözleşmenin 9. maddesinde sayılan haller olduğu, Sözleşmenin 25. maddesine göre taraf devletlerin bunları değiştirme takdirinin olmadığı, dolayısıyla burada belirlenen çerçeve ve amaç dışında kişisel sağlık verilerinin işlenmesinin açık kural ihlali olduğu, bu verilerin işlenemeyeceği, dava konusu Yönetmelikte, iç hukukta düzenlenmesi zorunlu sayılan hususların hiçbirinin düzenlenmediği, bu alanlara dair, açık, net, anlaşılabilir, çerçevesi belirli, uygulamaya yol gösterecek nitelikte bir düzenleyici işlem yapılmadığı, Yönetmeliğin 7. maddesinin birinci fıkrası ile 8. maddesinin birinci fıkrasındaki "sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla" ve "ilgilinin açık rızası aranmaksızın işlenebilir" ibarelerinin, yapılan değişiklik ile ilgili Kanun maddelerine atıf yapılmak suretiyle gizlendiği, ancak bu gizlemenin, 108 sayılı Sözleşmenin 6 ve 9. maddelerinde belirlenen açık yasağın ihlalini ortadan kaldırmadığı ileri sürerek düzenlemenin yürütmesinin durdurulması ve iptali istenilmektedir.

Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek amacıyla düzenlenen 24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu, Türkiye Büyük Millet Meclisi'ne sunulan genel gerekçesinden de anlaşılacağı üzere, kişisel verilerin korunması konusunun pek çok sektörü ve kamu ya da özel pek çok kurumu ilgilendirmesi nedeniyle bir "çerçeve kanun" olarak hazırlanmıştır.

Bu Kanuna neden ihtiyaç duyulduğunu açıklayan genel gerekçede, Türk Ceza Kanunu'nun 135 ve devamı maddelerinde kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa edilmesi fiillerinin suç olarak düzenlendiği ve yaptırıma bağlandığı, ancak kişisel verilerin

işlenmesine yönelik özel bir kanun bulunmaması sebebiyle, bu fiillerin ne zaman hukuka aykırı ne zaman hukuka uygun olduğunun belirlenmesinde tereddütler yaşandığı vurgulanmaktadır. Ayrıca 2010 yılında Anayasa'nın 20. maddesinde yapılan düzenlemeyle kişisel verilerin korunması temel bir insan hakkı olarak güvence altına alınmış ve konuya ilişkin usul ve esasların kanunla düzenleneceği öngörülmüştür.

Genel gerekçede, kişisel verilerin korunmasına yönelik bir kanuni düzenleme olmamasının uluslararası ilişkiler açısından da sorunlar yarattığı, EUROPOL, EUROJUST gibi Avrupa kurumları ile ilişkilerin sekteye uğradığı, sağlık kuruluşlarınca tutulan kişisel verilerin güvenliğinin sağlanmasında yeterli yasal önlem olmamasının Avrupa İnsan Hakları Mahkemesince özel hayatın gizliliğine müdahale olarak kabul edildiği ve bu nedenle ihlal kararları verildiği belirtilmektedir. Yine genel gerekçede, bu Kanunun Türkiye'nin Avrupa Birliği'ne üyelik süreci açısından da önemine dikkat çekilmekte, Türkiye'nin, Avrupa Konseyi tarafından tüm üye ülkelerde kişisel verilerin aynı standartlarda korunması ve sınır ötesi veri akışı ilkelerinin belirlenmesi amacıyla hazırlanan 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"ne de 1981 yılından itibaren taraf olduğu ifade edilmektedir.

Bütün bu hususlardan anlaşılacağı üzere 6698 sayılı Kanun, kişisel verilerin korunması konusunda önemli bir yasal boşluğu doldurmak amacıyla kabul edilen çerçeve niteliğinde bir yasal düzenlemedir. Genel gerekçede yer verilen şu tespit Kanun ile oluşturulan Kişisel Verileri Koruma Kurulu'nun genel kontrol ve denetleme işlevlerine dikkat çekmesi bakımından önemlidir: "Ülkemizde kişisel verilerin işlenmesi sürecini kontrol edecek ve denetleyecek bir kurum bulunmamaktadır. Bunun bir sonucu olarak halen kişisel veriler yeterli düzenleme ve denetime tabi olmaksızın, birçok kişi veya kurum tarafından kullanılabilmekte ve bu durum bazı hak ihlallerinin yaşanmasına sebep olabilmektedir."

6698 sayılı Kanununun 21. maddesi hükümlerine göre oluşturulan Kişisel Verileri Koruma Kurulu'nun görev ve yetkileri, aynı Kanun'un 22. maddesiyle belirlenmiştir. 22. maddenin birinci fıkrasının (h) bendinde "Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek" hükmüne yer verilmiştir.

Anılan Kanun'un, "Özel nitelikli kişisel verilerin işleme şartları" başlıklı 6. maddesinin birinci fıkrasında, dava konusu Yönetmelikle düzenlenen, sağlık verilerinin de özel nitelikli kişisel veri olduğu belirtilmiş; maddenin dördüncü fıkrasında, "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü getirilmiştir.

Dava dosyasının incelenmesinden; mülga 11/10/2011 tarihli ve 663 sayılı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 8. maddesinin birinci fıkrasının (j) bendi ile 47. maddesi ve 07/05/1987 tarihli ve 3359 sayılı Sağlık Hizmetleri Temel Kanununun 3. maddesinin birinci fıkrasının (f) bendine dayanılarak hazırlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'in 20/10/2016 tarih ve 29863 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girdiği ve anılan Yönetmelik ile; kişisel verilerin korunması ve veri mahremiyetinin sağlanmasına, kişisel sağlık verilerini toplama, işleme, aktarma, bu verilere erişim için kurulacak sisteme, kişisel sağlık verisi kaydı tutulan sistemlerin güvenliği ve denetimi ile sağlık hizmeti sunumundaki personel hareketlerinin Bakanlığa bildirilmesine ilişkin işlemlerde uyulacak usul ve esasların düzenlendiği,

Anılan Yönetmeliğin tamamının ve muhtelif maddelerinin iptali istemiyle davacılar tarafından açılan davada, Dairemizin 06/07/2017 tarihli ve E:2016/10500 sayılı kararı ile Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin tamamının yürütmesinin durdurulmasına karar verildiği,

Söz konusu Karar gerekçesinde ise, "dava konusu Yönetmeliğin Resmî Gazete'de yayımlandığı tarih olan 20/10/2016'da Kişisel Verileri Koruma Kurulu'nun henüz oluşturulmadığı, dolayısıyla 6698 sayılı Kanun'un 6. maddesinin dördüncü fıkrasında belirtilen yeterli önlemlerin Kurul tarafından belirlenmediği ve Kanun'un 22. maddesinin birinci fıkrasının (h) bendine göre diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında Kurul görüşü alınmadan dava konusu düzenlemenin tesis edildiği, Kanun'un genel gerekçesi ve Kanun hükümlerine göre, Kişisel Verileri Koruma Kurulu'nun kişisel verilerin korunması konusunda genel nitelikte bir kontrol ve denetim yetkisine sahip olduğu, diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hükümler içeren mevzuat taslakları hakkında Kişisel Verileri Koruma Kurulu'ndan görüş alınmasının şart olduğu, Kişisel Verileri Koruma Kurulu'nun kontrol ve denetiminden geçirilmeksizin hazırlanan ve 20/10/2016 tarihinde Resmî Gazete'de yayımlanarak yürürlüğe giren dava konusu düzenlemede bu nedenle mevzuata ve hukuka uygunluk bulunmadığı" tespitlerine yer verildiği.

Ancak anılan kararının ardından davalı tarafından Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik ile hakkında yürütmenin durdurulması kararı verilen esas Yönetmeliğin muhtelif maddelerinde değişiklik yapılarak 24/11/2017 tarih ve 30250 sayılı Resmî Gazete'de yayımlandığı ve görülmekte olan davanın açıldığı anlaşılmaktadır.

Anayasanın 138. maddesinin son fıkrasında "Yasama ve yürütme organları ile idare, mahkeme kararlarına uymak zorundadır; bu organlar ve İdare, mahkeme kararlarını hiçbir suretle değiştirilemez ve bunların yerine getirilmesini geciktiremez" kuralı yer almaktadır.

Öte yandan, 2577 sayılı İdari Yargılama Usulü Kanununun 28. maddesinde; "Danıştay, bölge idare mahkemeleri, idare ve vergi mahkemelerinin esasa ve yürütmenin durdurulmasına ilişkin kararlarının icaplarına göre idare, gecikmeksizin işlem tesis etmeye veya eylemde bulunmaya mecburdur. Bu süre hiçbir şekilde kararın idareye tebliğinden başlayarak otuz günü geçemez. Ancak, haciz veya ihtiyati haciz uygulamaları ile ilgili davalarda verilen kararlar hakkında, bu kararların kesinleşmesinden sonra idarece işlem tesis edilir." kuralına yer verilmiştir.

Bir düzenleyici işlemin iptaline karşı dava açılması durumunda yargı organlarınca düzenleyici işlemin ilgili maddesinin yürütülmesinin durdurulması ve iptali yolunda verdiği kararlar sonucunda oluşan hukuksal boşluk nedeniyle o alanın yeniden düzenlenmesi ve hukuk devletinin gereği olarak idari yargı merciiilerince verilen kararların, fiili ve hukuki imkânsızlık dışında gecikmeksizin yerine getirilmesi gerekmektedir. Aksine bir davranışın, yasama ve yürütme organları ile idarenin mahkeme kararlarına uymak zorunda oldukları yolundaki Anayasanın 138. maddesine aykırı olacağı açıktır. Böylece idarenin, uygulanmasında maddi ve hukuki imkânsızlık bulunanlar dışında yargı kararlarını "aynen" ve "gecikmeksizin" uygulamaktan başka bir seçeneği bulunmamaktadır. Başka bir deyişle, yargı kararlarının uygulanması bakımından idare "bağlı yetki" içerisinde bulunmaktadır.

Davalı idare savunmasında; 6698 sayılı Kanun uyarınca Kişisel Verileri Koruma Kurulu üyelerinin ancak 2017 yılının Ocak ayında belirlenebildiği ve bu nedenle Esas Yönetmelik hakkında Kurul görüşünün alınmasının mümkün olmadığı, Kişisel Verileri Koruma Kurulu üyelerinin belirlenmesini müteakip görüşmelere başlandığı, Yönetmelik hakkında Kurul üyelerinden şifahi görüşlerin alındığı, toplantılarda dile getirilen görüşler çerçevesinde Yönetmeliğin revize edilmesine yönelik çalışmalara başlanıldığı, hazırlanan Esas Yönetmelikte değişiklik yapmak üzere hazırlanan Yönetmelik Taslağının Kişisel Verileri Koruma Kuruluna gönderildiği ve görüşünün alındığı, Kurul görüşü çerçevesinde revize edilen Taslağın Kurula ikinci kez gönderildiği ve görüşlerin tamamının Taslağa yansıtıldığı ve Esas Yönetmelik'te gerekli değişikliklerin yapıldığı, Esas Yönetmelik hakkında açılan davada henüz yürütmenin durdurulması kararı verilmeden önce kararda gerekçe gösterilen "Kurul'dan görüş alınmamış olması" eksikliğini giderilmesine yönelik çalışmalara başlanmış olduğu, yürütmenin durdurulması kararının verildiği 06/07/2017 tarihinden önce Kurul görüşü alındığı, dolayısı ile yürütmenin durdurulması kararı henüz verilmeden, gecikmeksizin işlem tesis edildiği ve yürütmenin durdurulması kararının gereğinin yerine getirildiği, eksik bulunan hususun

tamamlanmış olduđu iddia edilmekte ise de, Dairemizce verilen yürütmenin durdurulması kararı üzerine Kişisel Verileri Koruma Kurulundan görüş alınarak oluşturulduđu iddia edilen yeni bir Yönetmeliğin Resmî Gazete'de yayımlanmadığı, hakkında yürütmenin durdurulması kararı verilen Esas Yönetmelikte yapılan kısmi deęişiklik metninin yayımlandığı görölmektedir.

Buna göre, bir düzenlemenin tamamının yürütülmesinin durdurulması veya iptal edilmesi üzerine, bu kararın gereğini yerine getirecek yeni bir düzenleme yürürlüğe konulmadığı sürece, önceki düzenlemede kısmi deęişiklikler yapılmak suretiyle hukuka aykırılığı saptanmış olan düzenlemenin canlandırılması hukuken mümkün deęildir. Zira düzenlemenin tamamının yürütülmesinin durdurulması veya iptali üzerine bu düzenlemede kısmen deęişikliğe gidilmesi durumunda, deęiştirilmeyen hükümlerin hukuken sakat olacağı da açıktır.

Bu durumda, Anayasada ve 2577 sayılı Kanun'da yer alan emredici kurallar karşısında, idarenin, yürütmenin durdurulması kararının gereğini yerine getirecek şekilde düzenleme yapması gerekirken, maddi ve hukuki koşullara göre uygulanabilir nitelikte olan bir yargı kararını aynen ve gecikmeksizin uygulamaktan kaçınarak, hakkında yürütmenin durdurulması kararı verilen Yönetmelikte kısmi deęişiklikler yapılarak yürürlüğe konulmasında hukuka uygunluk bulunmamaktadır.

Açıklanan nedenlerle, olayda 2577 sayılı İdari Yargılama Usulü Kanunu'nun 4001 sayılı Yasa ile deęişik 27. maddesinin ikinci fıkrasında sayılan koşullar gerçekleşmiş olduğundan yürütmenin durdurulması isteminin kabulüne, 24/11/2017 tarih ve 30250 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Deęişiklik Yapılmasına Dair Yönetmeliğin yürütülmesinin durdurulmasına, bu kararın tebliğini izleyen günden itibaren yedi gün içinde İdari Dava Daireleri Kurulu'na itiraz yolu açık olmak üzere 09/10/2018 tarihinde oybirliğiyle karar verildi.

Başkan

Üye

Üye

Üye

Üye

Danıştay Kararı - 12. Daire (E. 2019/1428)

Danıştay Kararı - 12. D., E. 2019/1428 K. 2020/3658 T. 11.11.2020

T.C. DANIŞTAY ONİKİNCİ DAİRE

Esas No: 2019/1428

Karar No: 2020/3658

KARAR DÜZELTME İSTEMİNDE BULUNAN (DAVALI): ... Bakanlığı / ...

VEKİLİ: Av. ...

DİĞER DAVALI: ... Başkanlığı / ...

KARŞI TARAF (DAVACI): ...

VEKİLİ: Av. ...

İSTEMİN KONUSU: ... İdare Mahkemesinin ... tarih ve E:..., K:... sayılı kararının onanmasına dair Danıştay Onikinci Dairesinin 14/11/2018 tarih ve E:2016/3765, K:2018/5226 sayılı kararının; 2577 sayılı İdari Yargılama Usulü Kanunu'nun Geçici 8. maddesi uyarınca uygulanmasına devam edilen 3622 sayılı Kanun ile değişik 54. maddesi uyarınca düzeltilmesi istenilmektedir.

YARGILAMA SÜRECİ:

Dava konusu istem: Dava, Edirne Açık Ceza İnfaz Kurumu'nda infaz ve koruma memuru öğrencisi olan davacı tarafından, hakkında yapılan güvenlik soruşturması neticesinde infaz ve koruma memuru olarak atanmasının uygun görülmemesine ilişkin Edirne Adli Yargı İlk Derece Mahkemesi Adalet Komisyonu Başkanlığı'nın ... tarih ve ... sayılı işlemi ile öğrenciliğe geçici kabulüne dair 15.01.2013 tarihli Bakanlık Olur'unun iptaline ilişkin Adalet Bakanlığı Ceza ve Tevkifevleri Genel Müdürlüğü'nün ... tarih ve ... sayılı işleminin iptali istemiyle açılmıştır.

İlk Derece Mahkemesi kararının özeti: İdare Mahkemesince, davacının basit yaralama suçundan dolayı almış olduğu hükmün açıklanmasının geri bırakılması kararına konu olan eylemin, olayın özelliği ve fiilin niteliği göz önüne alındığında, davacı hakkındaki güvenlik soruşturmasının olumsuz sonuçlanmasına neden olacak nitelikte bulunmadığı gerekçesiyle dava konusu işlemin iptaline karar verilmiştir.

Daire kararının özeti: Davalının temyiz başvurusu üzerine Danıştay Onikinci Dairesince, temyize konu karar hukuk ve usule uygun bulunmuş ve kararın onanmasına karar verilmiştir.

KARAR DÜZELTME TALEP EDENİN İDDİALARI: Davalı tarafından, davacı hakkında yapılan güvenlik soruşturması sonucu elde edilen bilgiler ve davacının atanmak istediği görevin nitelikleri ve hassasiyeti dikkate alındığında, davacının atanıp atanmaması hususunda idarenin takdir yetkisine sahip olduğu, davacı hakkında tesis edilen işlemde hukuka aykırılık bulunmadığı ileri sürülerek Danıştay Onikinci Dairesince verilen kararın düzeltilmesi istenilmektedir.

KARŞI TARAFIN SAVUNMASI: Savunma verilmemiştir.

DANIŞTAY TETKİK HÂKİMİ: ...

DÜŞÜNCESİ: Karar düzeltme isteminin reddi gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay Onikinci Dairesince, Tetkik Hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereği görüldü:

Kararın düzeltilmesi dilekçesinde ileri sürülen nedenler, 2577 sayılı Kanun'un Geçici 8. maddesi uyarınca uygulanmasına devam edilen 3622 sayılı Kanun ile değişik 54. maddesi hükmüne uygun bulunduğundan, karar düzeltme isteminin kabulü ile Danıştay Onikinci Dairesinin 14/11/2018 tarih ve E:2016/3765, K:2018/5226 sayılı kararı kaldırılarak uyumsuzluk yeniden incelendi:

İNCELEME VE GEREKÇE:

MADDİ OLAY:

Dava dosyasının incelenmesinden, Bakırköy Adli Yargı İlk Derece Mahkemesi Adalet Komisyonu tarafından Edirne Merkez Ceza İnfaz Kurumlarında çalıştırılmak üzere 127 adet infaz ve koruma öğrenciliği alımı için sınav yapıldığı ve davacının da bu sınavda başarılı olduğu, Edirne Adli Yargı İlk Derece Mahkemesi Adalet Komisyonu Başkanlığı'nın ... tarih ve ... sayılı kararı ile 127 erkek adayın infaz ve koruma memurluğu öğrenciliğine geçici kabul edilmesine ilişkin kararın Adalet Bakanlığı'na gönderildiği, 15.01.2013 tarihli Bakanlık Olur'u ile davacının da aralarında bulunduğu 127 adet infaz ve koruma memuru öğrencisinin geçici öğrenciliğe kabul edilmesine onay verildiği, davacının eğitimi devam ederken Muş Valiliği İl Emniyet Müdürlüğü tarafından gönderilen güvenlik soruşturması ve arşiv araştırması cevabında, "davacı hakkında ... Sulh Ceza Mahkemesi'nin ... tarih ve ... Esas, ... sayılı kararı ile basit yaralama suçundan 75 birim gün karşılığı toplam 1500-TL adli para cezası ile cezalandırılmasına, hükmün açıklanmasının geri bırakılmasına ve 3 yıl süre ile

denetimli serbestlik tedbirine tabi tutulmasına karar verildiği," nin bildirildiği, bunun üzerine Edirne Adli Yargı İlk Derece Mahkemesi Adalet Komisyonu Başkanlığı tarafından davacının güvenlik soruşturmasının olumsuz olarak değerlendirildiği ve Adalet Bakanlığı Ceza ve Tevkif Evleri Genel Müdürlüğü'nün işlemi ile davacının öğrenciliğe geçici kabulüne dair 15.01.2013 tarihli Bakanlık Olur'unun kendisiyle ilgili kısmının iptal edildiği anlaşılmaktadır.

İLGİLİ MEVZUAT:

Anayasa'nın "Özel hayatın gizliliği" başlıklı 20. maddesinin birinci fıkrasında;

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz" hükmüne, üçüncü fıkrasında; "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilmiştir.

Avrupa İnsan Hakları Sözleşmesinin "Özel ve aile hayatına saygı hakkı" başlıklı 8. maddesinde de;

"(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir," hükmü yer almaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 6. maddesinde;

"(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama

yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü yer almaktadır.

657 sayılı Devlet Memurları Kanunu'nun 48. maddesinde devlet memurluğuna alınmaya ilişkin genel ve özel şartlar düzenlenmiş; B/2 bendinde "Kurumların özel kanun veya diğer mevzuatında aranan şartları taşımak" özel şartlar arasında sayılmıştır.

5352 sayılı Adli Sicil Kanunu'nun 10. maddesinin üçüncü fıkrasında, "Onsekiz yaşından küçüklerle ilgili adli sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebilir. " hükmü yer almaktadır.

07/09//2005 tarihli ve 25929 sayılı Resmi Gazete'de yayımlanan Adli Sicil Yönetmeliği'nin 12. maddesinin dördüncü fıkrasında, "Onsekiz yaşından küçüklerle ilgili adli sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere mahkeme, hâkim veya savcılıklarca istenebilir." hükmü ile 14. maddesinin birinci fıkrasında, "Onsekiz yaşından küçüklerle ilgili adli sicil ve arşiv kayıtları ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere mahkeme, hâkim veya savcılıklara talep halinde verilir." hükmü yer almaktadır.

HUKUKİ DEĞERLENDİRME:

Anayasa Mahkemesi'nin 27/02/2019 tarihli ve 2014/7256 Başvuru no'lu kararında özetle;

"..Somut olayda başvuruçunun on sekiz yaşından küçükken işlediği suçun kayıtlarının Adana Valiliği Emniyet Müdürlüğü tarafından Komisyon Başkanlığına verildiği, bu kaydın dikkate alınmak suretiyle güvenlik soruşturmasının olumsuz sonuçlandığı, başvuruçunun sözleşmeli infaz ve koruma memurluğuna atamasının yapılmadığı anlaşılmaktadır.

Resmi makamlar tarafından muhafaza edilmekte olan, başvuruçunun hakkında yürütülen ceza yargılamasına dair bilgilerin özel hayata saygı hakkı anlamında kişisel nitelikli veriler olduğu açıktır. Söz konusu kişisel verinin kamu kurumlarıyla paylaşılması ve güvenlik soruşturmalarında kullanılmasının Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkına bir müdahale oluşturduğu sonucuna varılmıştır...

Öte yandan somut olayda başvuruçunun yazılı ve sözlü sınavı kazandığının ilan edilmiş olduğu, on sekiz yaşından küçükken işlediği suça ilişkin kaydın 5352 sayılı Kanun'un 10. maddesinin (3) numaralı fıkrasında yer alan hükme açıkça aykırı şekilde idari makamlara verilmiş olduğu dikkate

alındığında özel hayata saygı hakkına yönelik müdahalenin bu yönüyle de kanuni dayanaktan yoksun olduğu anlaşılmaktadır..." değerlendirmelerine yer verilmiştir.

Dosya içerisinde yer alan bilgi ve belgeler ile Anayasa Mahkemesi kararı doğrultusunda dava konusu olay incelendiğinde, ... doğumlu olan ve hakkındaki ceza mahkûmiyetine konu suçu işlediği 05.05.2010 tarihinde on sekiz yaşından küçük olan davacının, on sekiz yaşından küçükken işlediği bu suça ilişkin kayıtların Muş Valiliği İl Emniyet Müdürlüğü tarafından Edirne Adli Yargı İlk Derece Mahkemesi Adalet Komisyonu Başkanlığına verilmesi üzerine, ilgili kurum tarafından bu kaydın dikkate alınması suretiyle davacı hakkındaki güvenlik soruşturmasının olumsuz sonuçlandığı görülmektedir.

Bu durumda, davacının adli sicil kaydında görünmeyen, on sekiz yaşından küçükken işlediği suça ilişkin kaydın, yukarıda yazılı Kanun ve Yönetmelik hükümleri uyarınca, ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebileceği açık olduğundan, kişisel veri niteliğinde olan bu kaydın, güvenlik soruşturması kapsamında ilgili kamu kurumuna verilmesi ve güvenlik soruşturmasında kullanılması hukuka aykırı olduğundan, hukuka aykırı şekilde idari makamlara verilen bu kaydın değerlendirilmesi suretiyle güvenlik soruşturmasının olumsuz sonuçlandırılması, Anayasa'nın 20. maddesi ve Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi uyarınca "özel hayata saygı hakkının" ihlâli sonucunu doğurmaktadır.

Bu itibarla, davacının on sekiz yaşından küçükken işlediği suça ilişkin kayda dayanılarak güvenlik soruşturmasının olumsuz sonuçlanması suretiyle öğrencilikten ilişkisinin kesilmesine ilişkin dava konusu işlemde hukuka uyarlık bulunmadığından, temyize konu İdare Mahkemesi kararı sonucu itibarıyla hukuka uygun bulunmuştur.

KARAR SONUCU:

Açıklanan nedenlerle;

1. Davalı idarenin temyiz isteminin reddine,
2. Dava konusu işlemin iptaline ilişkin ... İdare Mahkemesinin ... tarih ve E:..., K:... sayılı kararının yukarıda belirtilen gerekçe ile SONUCU İTİBARIYLA ONANMASINA,
3. Davalı idare tarafından karar düzeltme aşamasında yapılan ... TL yargılama giderinin üzerine bırakılmasına, 11/11/2020 tarihinde oyçokluğuyla karar verildi.

(X)

KARŐI OY

Davalı idarenin karar dűzeltme isteminin reddi gerektiđi oyuyla Daire kararına katılmıyorum.

Danıştay Kararı - 10. Daire (E. 2018/3449)

Danıştay Kararı - 10. D., E. 2018/3449 K. 2021/1714 T. 8.4.2021

T.C. DANIŞTAY ONUNCU DAİRE

Esas No: 2018/3449

Karar No: 2021/1714

DAVACI: ... Barosu Başkanlığı

VEKİLLERİ: Av. ..., Av. ...

DAVALI: ... Bakanlığı

VEKİLLERİ: Av. ..., Av. ...

DAVANIN KONUSU: 02/06/2018 tarih ve 30439 sayılı Resmi Gazete'de yayımlanan Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu Yönetmeliği'nin 5. maddesinin 1. fıkrasının, 24. maddesinin 2. fıkrasının ve 25. maddesinin 2. fıkrasının iptali istenilmektedir.

DAVACININ İDDİALARI:

02/06/2018 tarih ve 30439 sayılı Resmi Gazete'de yayımlanan Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu Yönetmeliği'nin (kararın devamında HUAKY olarak kısaltılacaktır.) 5. maddesinin 1. fıkrasında, "Taraflar, arabulucuya başvurmak, süreci devam ettirmek, sonuçlandırmak veya bu süreçten vazgeçmek konusunda tamamen serbest olup, öncelikle uyuşmazlığı arabuluculuk yoluyla sonuçlandırma konusunda anlaşılır. Taraflar, bu sürecin içine zorla dâhil edilemeyecekleri gibi her aşamada uyuşmazlığı arabuluculuk yoluyla çözmekten de vazgeçebilirler. Ancak dava şartı olarak arabuluculuğa ilişkin özel hükümler saklıdır." kuralının yer aldığı, bu düzenlemenin yasaya aykırı olduğu, zira maddenin son cümlesinde 7036 sayılı Kanun'un 3. maddesi ile getirilen dava şartı olarak arabuluculuğa ilişkin özel hükümlerin saklı tutulduğu, bu haliyle düzenlemenin arabuluculuğun özüyle uyuşmadığı, arabuluculuğu iradi olmaktan çıkardığı, kendi içerisinde çelişki oluşturduğu; yine HUAKY'nin 24. maddesinin 2. fıkrasında yer alan, "Başvuran taraf, kendisine ve elinde bulunması hâlinde karşı tarafa ait her türlü iletişim bilgisini adliye arabuluculuk bürosuna verir." düzenlemesinin 6698 sayılı Kişisel Verilerin Korunması Kanunu'na (KVKK) aykırı olduğu, zira 6698 sayılı KVKK'nın 5. maddesinde, "Kişisel veriler ilgili kişinin açıkça rızası olmaksızın

işlenemez.", 8. maddesinde de "Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz." hükümlerinin düzenlendiği, 8. maddenin 3. fıkrasında bu hükmün istisnalarının sayıldığı ve ilgili Kanun maddesinde "Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır." hükmünün düzenlendiği, dolayısıyla kişisel verilerin aktarılması konusunda sadece kanunlarla istisnai hükümlerin konulabileceği, bu hususun bir yönetmelik maddesiyle düzenlenmesinin 6698 sayılı KVKK'nın 8. maddesine ve normlar hiyerarşisine aykırılık oluşturduğu; yine HUAKY'nin 25. maddesinin 2. fıkrasında yer alan, " Arabulucu adliye arabuluculuk bürosu tarafından görevlendirildikten sonra ilk önce başvuran taraftan başlamak üzere asiller ile ön görüşme yapar, başvurucudan ve diğer taraftan uyuşmazlığın esasını öğrenir." düzenlemesinin bu şekilde emredici nitelikte olmasının ve arabulucunun ilk önce asille görüşecek olmasının Anayasa'ya ve 1136 sayılı Avukatlık Kanunu'na aykırı olduğu, zira Anayasa'nın 36. maddesine göre, herkesin, meşru vasıta ve yollardan faydalanmak suretiyle yargı mercileri önünde davacı veya davalı olarak iddia ve savunma ile adil yargılanma hakkına sahip olduğu, ancak daha iyi savunulmak ve hakkını aramak için kendisini vekille temsil ettiren bir kişinin tayin ettiği vekilini aradan çıkararak, yalnızca asille ön görüşme zorunluluğunun Anayasa'nın 36. maddesinde düzenlenen hak arama hürriyeti ile Avrupa İnsan Hakları Sözleşmesi'nin 6. maddesinde güvence altına alınan adil yargılanma hakkının bileşenlerinden olan etkin savunma hakkını ihlal ettiği, 1136 sayılı Avukatlık Kanunu'nun 1. maddesinin 2. fıkrasında, "Avukat, yargının kurucu unsurlarından olan bağımsız savunmayı serbestçe temsil eder." hükmünün düzenlendiği, arabulucunun bağımsız savunmayı temsil eden avukatı ön görüşme sürecinin dışında bırakarak yalnızca asille görüşmesinin, bağımsız savunmayı serbestçe temsili engelleyen bir düzenleme olduğu, aynı zamanda, Avukatlık Kanunu'nun 2. maddesinin 1. fıkrasında, "Avukatlığın amacı; hukuki münasebetlerin düzenlenmesini, her türlü hukuki mesele ve anlaşmazlıkların adalet ve hakkaniyet uygun olarak çözümlenmesini ve hukuk kurallarının tam olarak uygulanmasını her derecede yargı organları, hakemler, resmi ve özel kişi, kurul ve kurumlar nezdinde sağlamaktır." hükmünün düzenlendiği ve Yönetmeliğin dava konusu edilen anılan hükmünün avukatlığın belirtilen amacının gerçekleştirilmesi önünde bir engel olduğu, arabuluculuk sürecinin başında, arabulucunun, kendisini vekille temsil ettiren asille doğrudan görüşecek olmasının, avukatın arabuluculuk sürecinden dışlanması anlamına geldiği, kaldı ki Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu'nda arabulucunun ilk başta asille görüşmesi yönünde herhangi bir hüküm bulunmadığı, kanunda olmayan bir düzenlemenin yönetmelikle getirilmesinin Anayasa'ya ve normlar hiyerarşisine aykırı olduğu ileri sürülmektedir.

DAVALININ SAVUNMASI: HUAKY'nin 5. maddesinin 1. fıkrasında yer alan "Ancak dava şartı olarak arabuluculuğa ilişkin özel hükümler saklıdır." hükmünün arabuluculuğun özülüyle uyuşmadığı

ve arabuluculuğun iradiliği ilkesine aykırı olduğundan bahisle iptali istenilmişse de, Kanuna, bireysel veya toplu iş sözleşmesine dayanan işçi ve işveren alacağı ve tazminatı ile işe iade taleplerinde dava açmadan önce arabulucuya başvurulmuş olmasını dava şartı haline getiren 12/10/2017 tarih ve 7036 sayılı İş Mahkemeleri Kanunu'nun 25/10/2017 tarih ve 30221 sayılı Resmi Gazete'de yayımlandığı ve dava şartı olarak arabuluculuğa ilişkin hükümlerinin de 01/01/2018 tarihinde yürürlüğe girdiği, bu nedenle 7036 sayılı Kanun'da yer bulan dava şartı olarak arabuluculuğa ilişkin hükümleri saklı tutan iptale konu yönetmelik hükmünün kanuna aykırılığından söz edilemeyeceği, 7036 sayılı İş Mahkemeleri Kanunu'nun 3. maddesinin 1. fıkrasında, Kanuna, bireysel veya toplu iş sözleşmesine dayanan işçi veya işveren alacağı ve tazminatı ile işe iade talebiyle açılan davalarda, arabulucuya başvurulmuş olmasının dava şartı olduğu düzenlendikten sonra, 2. fıkrasında davacının arabuluculuk faaliyeti sonunda anlaşmaya varılamadığına ilişkin son tutanağın aslını veya arabulucu tarafından onaylanmış bir örneğini dava dilekçesine eklemek zorunda olduğunun hükme bağlandığı, anlaşılacağı üzere arabuluculuk sürecinin devam ettirilmesi ve sona erdirilmesinin tamamen tarafların tasarrufuna bırakılan iradi bir süreç olduğu, 7036 sayılı Kanun'un genel gerekçesinde belirtilen yararlar da dikkate alınarak, sadece arabuluculuk sürecinin başlatılması bakımından iradilikten vazgeçildiği ve taraflara arabuluculuk sürecinin avantajları hakkında bilgi sahibi olma ve bunlardan yararlanma olanağının getirildiği, 7036 sayılı Kanun'un genel gerekçesinde belirtildiği üzere, İş Mahkemelerinin görev alanına giren uyuşmazlıkların yapısının tarafların konuyu müzakere ederek anlaşmaları suretiyle sonuçlandırılmasına uygun olduğu, arabuluculuğun dava şartı haline getirilmesinin iş uyuşmazlıklarının kısa süre içinde ve daha az masrafla çözülmesine yardımcı olacağı ve böylece adil yargılanma hakkının bir unsuru olan makul sürede yargılanma ilkesine riayet edilebileceği, ayrıca bu yöntemin maddi ya da şekli başka bir uyuşmazlığın doğmasını engellemek suretiyle uyuşmazlığı temelinden sonlandırması ve sosyal barışa katkı sağlamasının beklendiği, bununla birlikte arabuluculuk müzakerelerinin gizli olduğu dikkate alındığında her iki tarafın sırlarını korumaya elverişli bu yöntemle tarafların uyuşmazlığı sona erdirme imkanına da kavuşmakta olduğu, bu bakımdan anılan hükmün arabuluculuğun özüne, iradilik ilkesine ve kanuna aykırı olmadığı; HUAKY'nin 24. maddesinin 2. fıkrasında yer alan, " Başvuran taraf, kendisine ve elinde bulunması hâlinde karşı tarafa ait her türlü iletişim bilgisini adliye arabuluculuk bürosuna verir." hükmünün 6698 sayılı Kişisel Verilerin Korunması Kanunu'na (KVKK) aykırı olduğundan bahisle iptali istenilmişse de, 6698 sayılı KVKK'nın "Kişisel verilerin aktarılması" kenar başlıklı 8. maddesinde, kişisel verilerin ilgili kişinin açık rızası olmaksızın aktarılamayacağı belirtildikten sonra, kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğunun belirtildiği, 7036 sayılı İş Mahkemeleri Kanunu'nun 3. maddesinin 7. fıkrasında, " Başvuran taraf,

kendisine ve elinde bulunması halinde karşı tarafa ait her türlü iletişim bilgisini arabuluculuk bürosuna verir." hükmünün yer aldığı, açık kanun hükmüne dayanan ve onun bir tekrarı niteliğinde olan iptale konu yönetmelik hükmünün de 6698 sayılı KVKK'nın 8. maddesinin istisnasını oluşturduğu, normlar hiyerarşisine aykırılık bulunmadığı, kaldı ki bu çerçevede başvuruvercinun verdiği bilgilerin herhangi bir dava açılırken dava dilekçelerinde istenilen bilgilerden fazlası olmadığı, arabuluculuk sürecinin yürütülebilmesi için bu asgari bilgiye ihtiyaç duyulacağına izahattan varestede olduğu, iptal isteminin yerinde olmadığı; HUAKY'nin 25. maddesinin 2. fıkrasında yer alan, "Arabulucu adliye arabuluculuk bürosu tarafından görevlendirildikten sonra ilk önce başvuran taraftan başlamak üzere asiller ile ön görüşme yapar, başvuruvercinun ve diğer taraftan uyuşmazlığın esasını öğrenir." hükmünün Anayasa'nın 36. maddesine ve 1136 sayılı Avukatlık Kanunu'na aykırılık teşkil ettiğinden bahisle iptali istenilmişse de; arabuluculuk sürecinin bir yargılama faaliyeti değil, tarafların menfaatinin ön planda olduğu barışçıl bir uyuşmazlık çözüm, müzakere yöntemi olduğu, dava şartı olarak arabuluculukta tarafların dava açmadan önce arabulucuya başvurusunun zorunlu olduğu, ancak tarafların serbest iradeleriyle yürütülen arabuluculuk görüşmelerinde anlaşma zorunluluğunun bulunmadığı, arabuluculuk sürecinde anlaşamaması halinde tarafların dava açarak mahkeme huzurunda haklarını aramalarının mümkün olduğu, bu nedenle hak arama hürriyetinin ihlal edildiğinden bahsetmenin mümkün olmadığı, HUAKY'nin 25. maddesinin 2. fıkrasında yer alan, "Arabulucu adliye arabuluculuk bürosu tarafından görevlendirildikten sonra ilk önce başvuran taraftan başlamak üzere asiller ile ön görüşme yapar, başvuruvercinun ve diğer taraftan uyuşmazlığın esasını öğrenir." kuralının arabuluculuk sürecinin özüne uygun olduğu, zira uyuşmazlığın çözümü bağlamında gerçek çıkar ve gereksinimlerinin neler olduğunu en iyi tarafların bileceği, söz konusu düzenlemenin devamında yer alan "Arabulucu asilleri, arabuluculuğun esasları, süreci ve sonuçları hakkında aydınlatıp, arabuluculuk yoluyla uyuşmazlığın çözümünün ekonomik, sosyal ve psikolojik faydalarının olduğunu hatırlatarak onları bilgilendirir." kuralının da 6325 sayılı Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu'nun "Tarafların aydınlatılması" kenar başlıklı 11. maddesinde yer alan hükmün yönetmelikteki karşılığı olduğu, ayrıca hak temelinden ziyade menfaat temelli olan arabuluculuk süreçlerinde, kendilerini avukat ile temsil ettiren tarafların, gerçek çıkar ve gereksinimlerinin ön plana çıkması konusunda avukatları tarafından yeteri kadar bilgilendirilmedikleri arabulucu tarafından tespit edildiğinde, arabulucunun mevzuatın kendisine yüklediği eşitlik, adillik ve bilgilendirme yükümlülüğü çerçevesinde hareket etmesi ve gerekli bilgilendirmeleri yapmasının arabuluculuk faaliyetinin gereği olduğu, HUAKY'de dava dilekçesinde iddia edildiği gibi, 'kişinin tayin ettiği vekilini aradan çıkararak, yalnızca asille görüşme zorunluluğu' benzeri bir hüküm bulunmadığı, tam aksine arabuluculuk mevzuatının, arabuluculuk sürecinde

tarafların avukatları ile sürece katılımını destekleyici ve teşvik edici bir çok düzenleme barındırdığı, örneğin iptale konu yönetmelik maddesinin 2. fıkrasının son cümlesinde, arabulucunun asilleri ilk oturuma varsa vekilleri ile birlikte davet etmesi gerektiğinin açıkça düzenlendiği, yine 7036 sayılı Kanunla 6325 sayılı Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu'na 18. maddenin 4. fıkrası olarak "Taraflar ve avukatları ile arabulucunun birlikte imzaladıkları anlaşma belgesi, icra edilebilirlik şerhi aranmaksızın ilam niteliğinde belge sayılır." hükmünün eklendiği, böylece taraflara, avukatları ile birlikte katıldıkları arabuluculuk süreçlerinde, arabuluculuk anlaşma belgelerini mahkemece icra edilebilirlik şerhi verdirmeden ilam niteliğinde belge haline getirme olanağının tanındığı, bu sayede arabuluculuk sürecine tarafların avukatla katılımının teşvik edildiği, bu halde ortaya konulan mevzuat hükümleri uyarınca, arabuluculuk mevzuatının, dava dilekçesinde iddia edildiği gibi "avukatlığın amacının gerçekleşmesini engelleyen, avukatın arabuluculuk sürecinden dışlanması anlamına gelen, vekille temsil ilkesine ve dolayısıyla Anayasa ile güvence altına alınan adil yargılanma ilkesine aykırılık teşkil eden" bir hükmünün bulunmadığı savunulmaktadır.

DANIŞTAY TETKİK HAKİMİ: ...

DÜŞÜNCESİ: 02/06/2018 tarih ve 30439 sayılı Resmi Gazete'de yayımlanan Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu Yönetmeliği'nin 5. maddesinin 1. fıkrası ile 24. maddesinin 2. fıkrasının iptali istemi yönünden davanın reddi; anılan Yönetmeliğin 25. maddesinin 2. fıkrasının iptali istemi yönünden, dava konusu edilen düzenlemenin iptali gerektiği düşünülmektedir.

DANIŞTAY SAVCISI: ...

DÜŞÜNCESİ: Dava, 02/06/2018 tarih ve 30439 sayılı Resmi Gazete'de yayımlanan Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu Yönetmeliği'nin 5/1, 24/2 ve 25/2 maddelerinin; dava şartı olarak arabuluculuğa ilişkin özel hükümlerin saklı tutulduğu düzenlemesinin arabuluculuğun iradi olmasıyla bağdaşmadığı, kişisel verilerin korunması kanununa aykırılık içerdiği, yine emredici nitelikte arabulucunun kimle görüşeceğinin belirtilmesinin hak arama hürriyeti ve etkin savunma hakkının ihlali olduğu, vekille temsil edilen asille doğrudan görüşülmesinin bağımsız savunmanın serbestçe temsilinin engellenmesi ve savunmayı temsil eden avukatın arabuluculuk sürecinden dışlanması anlamına geldiği ve adil yargılanma ilkesinin ihlal edildiği, Kanunda ilk önce asil görüşülmesi konusunda bir hüküm bulunmadığı ileri sürülerek, iptali istemiyle açılmıştır.

Hukuk uyuşmazlıklarının arabuluculuk yoluyla çözümlenmesinde uygulanacak usul ve esasları düzenlemek amacıyla 6325 sayılı Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu yayımlanmıştır. 1. maddesi (2). fıkrasında, Bu Kanun, yabancılik unsuru taşıyanlar da dâhil olmak üzere, ancak tarafların üzerinde serbestçe tasarruf edebilecekleri iş veya işlemlerden doğan özel hukuk

uyuşmazlıklarının çözümlenmesinde uygulanır. Şu kadar ki, aile içi şiddet iddiasını içeren uyuşmazlıklar arabuluculuğa elverişli değildir." hükmüne yer verilmiş, Arabuluculuğa İlişkin Temel İlkelerin düzenlendiği bölümde bulunan 3. maddesinde "İradi olma ve eşitlik" ilkesi yer almıştır. Anılan 3. maddesinde; "(1)Taraflar, arabulucuya başvurmak, serbesttirler. (Ek cümle:6/12/2018-7155/22 md.) Şu kadar ki dava şartı olarak arabuluculuğa ilişkin 18/A maddesi hükmü saklıdır. (2)Taraflar, gerek arabulucuya başvururken gerekse tüm süreç boyunca eşit haklara sahiptirler." hükmü, "Gizlilik" başlıklı ilke, 4. maddesinde düzenlenmiş, "(1)Taraflarca aksi kararlaştırılmadıkça arabulucu, arabuluculuk faaliyeti çerçevesinde kendisine sunulan veya diğer bir şekilde elde ettiği bilgi ve belgeler ile diğer kayıtları gizli tutmakla yükümlüdür. (2) Aksi kararlaştırılmadıkça taraflar ve görüşmelere katılan diğer kişiler de bu konudaki gizliliğe uymak zorundadırlar." hükmüne, "Beyan veya belgelerin kullanılmaması" ilkesi 5. maddesinde; "(1) Taraflar, arabulucu veya arabuluculuğa katılanlar da dâhil üçüncü bir kişi, uyuşmazlıkla ilgili olarak hukuk davası açıldığında yahut tahkim yoluna başvurulduğunda, aşağıdaki beyan veya belgeleri delil olarak ileri süremez ve bunlar hakkında tanıklık yapamaz: a) Taraflarca yapılan arabuluculuk daveti veya bir tarafın arabuluculuk faaliyetine katılma isteği. b) Uyuşmazlığın arabuluculuk yolu ile sona erdirilmesi için taraflarca ileri sürülen görüşler ve teklifler. c) Arabuluculuk faaliyeti esnasında, taraflarca ileri sürülen öneriler veya herhangi bir vakıa veya iddianın kabulü. ç) Sadece arabuluculuk faaliyeti dolayısıyla hazırlanan belgeler. (2) Birinci fıkra hükmü, beyan veya belgenin şekline bakılmaksızın uygulanır. (3) Birinci fıkrada belirtilen bilgilerin açıklanması mahkeme, hakem veya herhangi bir idari makam tarafından istenemez. Bu beyan veya belgeler, birinci fıkrada öngörülenin aksine, delil olarak sunulmuş olsa dahi hükme esas alınmaz. Ancak, söz konusu bilgiler bir kanun hükmü tarafından emredildiği veya arabuluculuk süreci sonunda varılan anlaşmanın uygulanması ve icrası için gerekli olduğu ölçüde açıklanabilir. (4) Yukarıdaki fıkralar, arabuluculuğun konusuyla ilgili olup olmadığına bakılmaksızın, hukuk davası ve tahkimde uygulanır. (5) Birinci fıkrada belirtilen sınırlamalar saklı kalmak koşuluyla, hukuk davası ve tahkimde ileri sürülebilen deliller, sadece arabuluculukta sunulmaları sebebiyle kabul edilemeyecek deliller haline gelmez." hükmü getirilmiştir.

"Taraflarla görüşme ve iletişim kurulması" başlıklı 8. maddesinde, "(1) Arabulucu, tarafların her biri ile ayrı ayrı veya birlikte görüşebilir ve iletişim kurabilir. (...)" hükmü yer almıştır.

Kanuna daha sonra 6/12/2018 tarih ve 7155 sayılı Kanununun 23 maddesiyle eklenen "Dava şartı olarak arabuluculuk" başlıklı 18/A maddesinde, "(1) İlgili kanunlarda arabulucuya başvurulmuş olması dava şartı olarak kabul edilmiş ise arabuluculuk sürecine aşağıdaki hükümler uygulanır. (2) Davacı, arabuluculuk faaliyeti sonunda anlaşmaya varılamadığına ilişkin son tutanağın aslını veya arabulucu

tarafından onaylanmış bir örneğini dava dilekçesine eklemek zorundadır. Bu zorunluluğa uyulmaması hâlinde mahkemece davacıya, son tutanağın bir haftalık kesin süre içinde mahkemeye sunulması gerektiği, aksi takdirde davanın usulden reddedileceği ihtarını içeren davetiye gönderilir. İhtarın gereği yerine getirilmez ise dava dilekçesi karşı tarafa tebliğe çıkarılmaksızın davanın usulden reddine karar verilir. Arabulucuya başvurulmadan dava açıldığının anlaşılması hâlinde herhangi bir işlem yapılmaksızın davanın, dava şartı yokluğu sebebiyle usulden reddine karar verilir.(...)" hükme bağlanmıştır.

6325 sayılı Kanunun verdiği yetkiye dayanılmak suretiyle yayımlanmış olan Hukuk Uyuşmazlıklarında Arabuluculuk Yönetmeliğinin, "İradi olma ve eşitlik" başlıklı 5. maddesinde, "(1) Taraflar, arabulucuya başvurmak, süreci devam ettirmek, sonuçlandırmak veya bu süreçten vazgeçmek konusunda tamamen serbest olup, öncelikle uyuşmazlığı arabuluculuk yoluyla sonuçlandırma konusunda anlaşılırlar. Taraflar, bu sürecin içine zorla dâhil edilemeyecekleri gibi her aşamada uyuşmazlığı arabuluculuk yoluyla çözmekten de vazgeçebilirler. Ancak dava şartı olarak arabuluculuğa ilişkin özel hükümler saklıdır. (2) Taraflar, gerek arabulucuya başvururken gerekse süreç boyunca eşit haklara sahiptirler. Taraflardan biri arabuluculuk sürecinin dışında bırakılamayacağı gibi söz hakkı da diğerine göre kısıtlanamaz." kuralı getirilmiştir.

Dava konusu Yönetmeliğin Resmi Gazete'de yayımlandığı tarih itibariyle, dayanağını oluşturan Yasa hükmü ile tarafların, arabulucuya başvurmak, süreci devam ettirmek, sonuçlandırmak veya bu süreçten vazgeçmek konusunda serbest oldukları belirtilmiş ve istisna tutulan bir durumdan bahsedilmemiş, ancak dava konusu Yönetmeliğin 5. maddesinin 1. fıkrasında, arabuluculuğun dava şartı olması halinde özel hükümleri saklı tutan kuralına, yasada yer almadığı halde yönetmelikte yer verilmiştir. Bu davanın da açıldığı tarihten sonra 6325 sayılı Yasanın 3. maddesine; 6/12/2018 tarih ve 7155 sayılı Kanunun 22 maddesiyle, "Şu kadar ki dava şartı olarak arabuluculuğa ilişkin 18/A maddesi hükmü saklıdır." cümlesi eklenmiş ve 18/A maddesinde, ilgili kanunlarda arabulucuya başvurulmuş olmasının dava şartı olarak kabul edilmesi halinde, arabuluculuk sürecinde uygulanacak usul açıklanmıştır.

Bu durumda, dava şartı olarak arabuluculuğun öngörülebileceği istisnai durumun ilk defa yönetmelikte düzenlendiği, daha sonra yasal dayanağının oluşturulduğu görüldüğünden, davanın açıldığı tarih itibariyle idari işlemlerin hukukilik denetiminin yapılması gereği dikkate alındığında, Yönetmeliğin 5. maddesinin 1. fıkrasında yer alan "Ancak dava şartı olarak arabuluculuğa ilişkin özel hükümler saklıdır." cümlesinde hukuka uyarlık bulunmamıştır.

Dava konusu düzenlemenin 24/2. maddesine yönelik olarak; Yönetmeliğin, "Dava şartı olarak arabuluculukta arabulucunun görevlendirilmesi" başlıklı 24. maddesinde, "(1) Arabulucu, adli yargı ilk derece mahkemesi adalet komisyonu başkanlıklarına bildirilen listeden adliye arabuluculuk bürosu tarafından puanlama yöntemiyle belirlenir. Ancak tarafların listede yer alan herhangi bir arabulucu üzerinde başvuru sırasında anlaşmaları hâlinde taraflar veya tarafların imzasını taşıyan bir tutanakla beraber üzerinde anlaşılan arabulucu, durumu adliye arabuluculuk bürosuna bildirdiğinde bu arabulucu görevlendirilir. Dava şartı olan arabuluculuk ile ilgili uyuşmazlıklarda liste dışında bir arabulucu görevlendirilemez. (2) Başvuran taraf, kendisine ve elinde bulunması hâlinde karşı tarafa ait her türlü iletişim bilgisini adliye arabuluculuk bürosuna verir. Adliye arabuluculuk bürosu, tarafların resmi kayıtlarda yer alan iletişim bilgilerini araştırmaya da yetkilidir. İlgili kurum ve kuruluşlar, uyuşmazlık konusuyla sınırlı olmak üzere adliye arabuluculuk bürosu tarafından talep edilen iletişim bilgilerini vermekle yükümlüdür.(...)" kuralı yer almıştır.

6325 sayılı Yasaya 6/12/2018 tarih ve 7155 sayılı Kanunun 23 maddesiyle eklenen 18/A maddesinin 6. fıkrasında, "Başvuran taraf, kendisine ve elinde bulunması hâlinde karşı tarafa ait her türlü iletişim bilgisini arabuluculuk bürosuna verir. Büro, tarafların resmî kayıtlarda yer alan iletişim bilgilerini araştırmaya da yetkilidir. İlgili kurum ve kuruluşlar, büro tarafından talep edilen bilgi ve belgeleri vermekle yükümlüdür.", 7. fıkrasında, "Taraflara ait iletişim bilgileri, görevlendirilen arabulucuya büro tarafından verilir. Arabulucu bu iletişim bilgilerini esas alır, ihtiyaç duyduğunda kendiliğinden araştırma da yapabilir. Elindeki bilgiler itibarıyla her türlü iletişim vasıtasını kullanarak görevlendirme konusunda tarafları bilgilendirir ve ilk toplantıya davet eder. Bilgilendirme ve davete ilişkin işlemlerini belgeye bağlar." hükmü getirilmiştir. Yönetmeliğin yayımı tarihinde söz konusu hükmün Yasada yer almadığı görülmektedir. Yönetmelik hükmü ile Yasada yer almadığı halde ilgili kurum ve kuruluşlara, uyuşmazlık konusuyla sınırlı olmak üzere adliye arabuluculuk bürosu tarafından talep edilen iletişim bilgilerini vermek yükümlülüğü getirilmiştir.

Yine 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanunda, Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi kişisel veri olarak tanımlanmıştır. Kişisel verilerin işlenmesi için kişilerin açık rızası aranmış, bazı şartların varlığı halinde kişilerin açık rızası aranmadan da kişisel verilerin işlenebilmesi mümkün kılınmıştır. Özel nitelikte kişisel verilerin neler olduğu sayılmak suretiyle belirlenmiş, işlenmesi ve aktarılması ilgilinin açık rızasına tabi kılınmış olmakla birlikte, işlenmesini sağlayan istisnai koşullar belirlenmiş, kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler de saklı tutulmuştur.

Bu durumda, Yasadan alınmayan bir yetkinin kullanılarak, kurum ve kuruluşlara, Yönetmelik kuralı ile mecburiyet getirilmesinde, "Yasaların Geriye Yürümezliği" ilkesi uyarınca yürürlük tarihinden sonraki olay, işlem ve eylemlere uygulanmak üzere çıkarılmaları ve yürürlüğe giren yasaların geçmişe ve kesin nitelik kazanmış hukuksal durumlara etkili olamaması "Kazanılmış Hakların Korunması" ilkesi gereği olduğundan, anılan Kanunda sonradan yapılan düzenlemenin geçmişe yürütülemeyeceği ve bu yönetmeliğin yürürlüğe girdiği tarihten itibaren işlemlere dayanak oluşturacağı gözönüne alındığında, Yönetmeliğin 24/2. maddesi hükmünde hukuka uyarlık bulunmamıştır.

Yönetmeliğin 25/2. maddesi hükmüne gelince, "Dava şartı olarak arabuluculukta arabuluculuk faaliyeti" başlıklı 25. maddesinde, "(1) Arabuluculuk görüşmelerine taraflar bizzat, kanuni temsilcileri veya avukatları, idareler ise oluşturacakları komisyon aracılığıyla katılabilirler. İşverenin adi veya resmi yazılı belgeyle yetkilendirdiği çalışanı da görüşmelerde işvereni temsil edebilir ve son tutanağı imzalayabilir. (2) Arabulucu adliye arabuluculuk bürosu tarafından görevlendirildikten sonra ilk önce başvuran taraftan başlamak üzere asiller ile ön görüşme yapar, başvurucudan ve diğer taraftan uyuşmazlığın esasını öğrenir. Arabulucu asilleri, arabuluculuğun esasları, süreci ve sonuçları hakkında aydınlatıp, arabuluculuk yoluyla uyuşmazlığın çözümünün ekonomik, sosyal ve psikolojik faydalarının olduğunu hatırlatarak onları bilgilendirir. Asilleri ilk oturuma varsa vekilleri ile birlikte davet eder.(...)"

kuralına yer verilmiştir.

6325 sayılı Kanunda, hukuk uyuşmazlıklarının arabuluculuk yoluyla çözümlenmesinde, bu yola başvuranlar, taraf ve karşı taraf olarak nitelendirilmiştir. Arabulucunun, tarafların her biri ile ayrı ayrı veya birlikte görüşebileceği ve iletişim kurabileceği hükmü de bunu ortaya koymaktadır. Bu itibarla arabulucunun muhatap olacağı, başvuru taraftır. Başvurucuyu şahıs olarak adlandırmamıştır. Dolayısıyla bizzat başvuranın kendisi ya da yanında vekilinin olmasında bir sakınca görülmemiştir. Hukuki münasabetlerin düzenlenmesini, her türlü hukuki mesele ve anlaşmazlıkların adalet ve hakkaniyete uygun olarak çözümlenmesini ve hukuk kurallarının tam olarak uygulanmasını her derecede yargı organları, hakemler, resmi ve özel kişi, kurul ve kurumlar nezdinde sağlamak Avukatlık Kanununun amacı ise, hukuki bilgi ve tecrübelerini adalet hizmetine ve kişilerin yararlanmasına sunmakla görevli olan avukatların varlığı ya da avukatın dışında tutulduğu yalnızca başvuranın şahsı(asil) ile belli aşamalarda görüşmeye imkan veren bir hükmü bulunmamaktadır. Bu nedenle Yönetmeliğin bu maddesinde Yasayla getirilmeyen bir ön koşul ile asille ilk görüşmenin yapılacağı düzenlenmesi, Yasayı aşar nitelikte bulunmaktadır.

Kaldı ki, 6325 sayılı Kanununun 15/6. maddesine 12/10/2017 tarihinde, "arabuluculuk müzakerelerine taraflar bizzat, kanuni temsilcileri veya avukatları aracılığıyla katılabilirler, uyuşmazlığın çözümüne katkı sağlayabilecek uzman kişiler de müzakerelerde hazır bulundurulabilir." yönünde açıklayıcı bir hüküm getirilmiş olmakla, müzakerelerin, bizzat ya da kanuni temsilcileri ve avukatları aracılığıyla yapılmasına cevaz verilmiş, arabulucu tarafından yapılacak ilk görüşmenin de bizzat asille yapılabileceği yönündeki bir sınırlamanın yasal dayanağının bulunmadığı ortaya konulmuş olmakta, yine Yasada, dava açılmadan önce arabulucuya başvuru hâlinde, ilk toplantıya davet edilenlerin taraflar olarak ifade edilmesi, vekil aracılığı ile temsil edileceklerde etkin savunma hakkının bir gereği olarak, taraf ifadesinin vekili de kapsadığı, bizzat başvurunu yani asili ifade etmediği anlaşılmaktadır. Dolayısıyla Yönetmeliğin 25/2. maddesi hükmünde yer alan bu sınırlayıcı, mecburiyet getiren ifadenin, dayanağı Yasanın amacı ve kapsamı ile bağdaşmadığı sonucuna varılmıştır.

Açıklanan nedenlerle, dava konusu Yönetmeliğin 5/1, 24/2 ve 25/2. maddelerinin iptali gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay Onuncu Dairesince, duruşma için önceden taraflara bildirilen 08/04/2021 tarihinde davacıyı temsilen gelen olmadığı, davalı Adalet Bakanlığı'nı temsilen Av. ...'ün geldiği, Danıştay Savcısının hazır olduğu görülmekle açık duruşmaya başlandı. Hazır bulunan davalı idare vekiline usulüne uygun olarak söz verilerek dinlendikten ve Danıştay Savcısının düşüncesi alındıktan sonra davalı vekiline son kez söz verilip duruşma tamamlandı. Tetkik Hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereği görüşüldü:

MADDİ OLAY:

Davacı tarafından, 02/06/2018 tarih ve 30439 sayılı Resmi Gazete'de yayımlanan Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu Yönetmeliği'nin 5. maddesinin 1. fıkrasının, 24. maddesinin 2. fıkrasının ve 25. maddesinin 2. fıkrasının iptali istemiyle bakılmakta olan dava açılmıştır.

İNCELEME VE GEREKÇE:

ESAS YÖNÜNDEN:

İlgili Mevzuat:

22/06/2012 tarih ve 28331 sayılı Resmî Gazete'de yayımlanan 6325 sayılı Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu'nun 1. maddesinde, "(1) Bu Kanunun amacı, hukuk uyuşmazlıklarının

arabuluculuk yoluyla çözümlenmesinde uygulanacak usul ve esasları düzenlemektir. (2) Bu Kanun, yabancılık unsuru taşıyanlar da dâhil olmak üzere, ancak tarafların üzerinde serbestçe tasarruf edebilecekleri iş veya işlemlerden doğan özel hukuk uyuşmazlıklarının çözümlenmesinde uygulanır. Şu kadar ki, aile içi şiddet iddiasını içeren uyuşmazlıklar arabuluculuğa elverişli değildir."; 3. maddesinde, "(1) Taraflar, arabulucuya başvurmak, süreci devam ettirmek, sonuçlandırmak veya bu süreçten vazgeçmek konusunda serbesttirler. (Ek cümle:6/12/2018-7155/22 md.) Şu kadar ki dava şartı olarak arabuluculuğa ilişkin 18/A maddesi hükmü saklıdır. (2) Taraflar, gerek arabulucuya başvururken gerekse tüm süreç boyunca eşit haklara sahiptirler."; 4. maddesinde, "(1) Taraflarca aksi kararlaştırılmadıkça arabulucu, arabuluculuk faaliyeti çerçevesinde kendisine sunulan veya diğer bir şekilde elde ettiği bilgi ve belgeler ile diğer kayıtları gizli tutmakla yükümlüdür. (2) Aksi kararlaştırılmadıkça taraflar ve görüşmelere katılan diğer kişiler de bu konudaki gizliliğe uymak zorundadırlar."; 8. maddesinde, "(1) Arabulucu, tarafların her biri ile ayrı ayrı veya birlikte görüşebilir ve iletişim kurabilir."; 15. maddesinde, "(1) Arabulucu, seçildikten sonra tarafları en kısa sürede ilk toplantıya davet eder. (2) Taraflar, emredici hukuk kurallarına aykırı olmamak kaydıyla arabuluculuk usulünü serbestçe kararlaştırabilirler. (3) Taraflarca kararlaştırılmamışsa arabulucu; uyuşmazlığın niteliğini, tarafların isteklerini ve uyuşmazlığın hızlı bir şekilde çözümlenmesi için gereken usul ve esasları göz önüne alarak arabuluculuk faaliyetini yürütür. (4) Niteliği gereği yargısal bir yetkinin kullanımı olarak sadece hâkim tarafından yapılabilecek işlemler arabulucu tarafından yapılamaz. (5) Dava açıldıktan sonra tarafların birlikte arabulucuya başvuracaklarını beyan etmeleri hâlinde yargılama, mahkemece üç ayı geçmemek üzere ertelenir. Bu süre, tarafların birlikte başvurusu üzerine üç aya kadar uzatılabilir. (6) (Değişik: 12/10/2017-7036/22 md.) Arabuluculuk müzakerelerine taraflar bizzat, kanuni temsilcileri veya avukatları aracılığıyla katılabilirler. Uyuşmazlığın çözümüne katkı sağlayabilecek uzman kişiler de müzakerelerde hazır bulundurulabilir. (7) (Ek: 12/10/2017-7036/22 md.) Tarafların çözüm üretemediklerinin ortaya çıkması hâlinde arabulucu bir çözüm önerisinde bulunabilir. (8) (Ek: 12/10/2017-7036/22 md.) Arabuluculuk müzakerelerinde idareyi, üst yönetici tarafından belirlenen iki üye ile hukuk birimi amiri veya onun belirleyeceği bir avukat ya da hukuk müşavirinden oluşan komisyon temsil eder. Komisyon, arabuluculuk müzakereleri sonunda gerekçeli bir rapor düzenler ve beş yıl boyunca saklar. (9) (Ek: 12/10/2017-7036/22 md.) Komisyon üyelerinin arabuluculuk faaliyeti kapsamında yaptıkları işler ve aldıkları kararlar sebebiyle açılacak tazminat davaları, ancak Devlet aleyhine açılabilir. Devlet ödediği tazminattan dolayı görevinin gereklerine aykırı hareket etmek suretiyle görevini kötüye kullanan üyelere ödeme tarihinden itibaren bir yıl içinde rücu eder. (10) (Ek: 12/10/2017-7036/22 md.) Bu maddenin uygulanmasına ilişkin usul ve esaslar Bakanlıkça yürürlüğe konulan yönetmelikle

düzenlenir."; 6/12/2018 tarih ve 7155 sayılı Kanun'un 23. maddesiyle eklenen 18/A maddesinin ilgili fıkralarında, "(1) İlgili kanunlarda arabulucuya başvurulmuş olması dava şartı olarak kabul edilmiş ise arabuluculuk sürecine aşağıdaki hükümler uygulanır. (2) Davacı, arabuluculuk faaliyeti sonunda anlaşmaya varılamadığına ilişkin son tutanağın aslını veya arabulucu tarafından onaylanmış bir örneğini dava dilekçesine eklemek zorundadır. Bu zorunluluğa uyulmaması hâlinde mahkemece davacıya, son tutanağın bir haftalık kesin süre içinde mahkemeye sunulması gerektiği, aksi takdirde davanın usulden reddedileceği ihtarını içeren davetiye gönderilir. İhtarın gereği yerine getirilmez ise dava dilekçesi karşı tarafa tebliğe çıkarılmaksızın davanın usulden reddine karar verilir. Arabulucuya başvurulmadan dava açıldığının anlaşılması hâlinde herhangi bir işlem yapılmaksızın davanın, dava şartı yokluğu sebebiyle usulden reddine karar verilir. (...) (6) Başvuran taraf, kendisine ve elinde bulunması hâlinde karşı tarafa ait her türlü iletişim bilgisini arabuluculuk bürosuna verir. Büro, tarafların resmî kayıtlarda yer alan iletişim bilgilerini araştırmaya da yetkilidir. İlgili kurum ve kuruluşlar, büro tarafından talep edilen bilgi ve belgeleri vermekle yükümlüdür. (7) Taraflara ait iletişim bilgileri, görevlendirilen arabulucuya büro tarafından verilir. Arabulucu bu iletişim bilgilerini esas alır, ihtiyaç duyduğunda kendiliğinden araştırma da yapabilir. Elindeki bilgiler itibarıyla her türlü iletişim vasıtasını kullanarak görevlendirme konusunda tarafları bilgilendirir ve ilk toplantıya davet eder. Bilgilendirme ve davete ilişkin işlemlerini belgeye bağlar. (...) (19) İlgili kanunlarda dava şartı olarak arabuluculuğa ilişkin kabul edilen özel hükümler saklıdır. (20) Bu bölümde hüküm bulunmayan hâllerde niteliğine uygun düştüğü ölçüde bu Kanunun diğer hükümleri uygulanır." hükümleri yer almaktadır.

25/10/2017 tarih ve 30221 sayılı Resmî Gazete'de yayımlanan İş Mahkemeleri Kanunu'nun "Dava şartı olarak arabuluculuk" kenar başlıklı ve 01/01/2018 yürürlük tarihli 3. maddesinin ilgili fıkralarında, "(1) Kanuna, bireysel veya toplu iş sözleşmesine dayanan işçi veya işveren alacağı ve tazminatı ile işe iade talebiyle açılan davalarda, arabulucuya başvurulmuş olması dava şartıdır. (2) Davacı, arabuluculuk faaliyeti sonunda anlaşmaya varılamadığına ilişkin son tutanağın aslını veya arabulucu tarafından onaylanmış bir örneğini dava dilekçesine eklemek zorundadır. Bu zorunluluğa uyulmaması hâlinde mahkemece davacıya, son tutanağın bir haftalık kesin süre içinde mahkemeye sunulması gerektiği, aksi takdirde davanın usulden reddedileceği ihtarını içeren davetiye gönderilir. İhtarın gereği yerine getirilmez ise dava dilekçesi karşı tarafa tebliğe çıkarılmaksızın davanın usulden reddine karar verilir. Arabulucuya başvurulmadan dava açıldığının anlaşılması hâlinde herhangi bir işlem yapılmaksızın davanın, dava şartı yokluğu sebebiyle usulden reddine karar verilir. (3) İş kazası veya meslek hastalığından kaynaklanan maddi ve manevi tazminat ile bunlarla ilgili tespit, itiraz ve rücu davaları hakkında birinci fıkra hükmü uygulanmaz. (...) (7) Başvuran taraf, kendisine ve elinde

bulunması hâlinde karşı tarafa ait her türlü iletişim bilgisini arabuluculuk bürosuna verir. Büro, tarafların resmi kayıtlarda yer alan iletişim bilgilerini araştırmaya da yetkilidir. İlgili kurum ve kuruluşlar, büro tarafından talep edilen bilgi ve belgeleri vermekle yükümlüdür. (8) Taraflara ait iletişim bilgileri, görevlendirilen arabulucuya büro tarafından verilir. Arabulucu bu iletişim bilgilerini esas alır, ihtiyaç duyduğunda kendiliğinden araştırma da yapabilir. Elindeki bilgiler itibarıyla her türlü iletişim vasıtasını kullanarak görevlendirme konusunda tarafları bilgilendirir ve ilk toplantıya davet eder. Bilgilendirme ve davete ilişkin işlemlerini belgeye bağlar. (...) (21) Bu maddede hüküm bulunmayan hâllerde niteliğine uygun düştüğü ölçüde 7/6/2012 tarihli ve 6325 sayılı Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu hükümleri uygulanır. (22) Arabuluculuğa başvuru usulü, arabulucunun görevlendirilmesi ve arabuluculuk görüşmelerine ilişkin diğer hususlar Adalet Bakanlığınca yürürlüğe konulan yönetmelikle belirlenir." hükümleri düzenlenmiştir.

02/06/2018 tarih ve 30439 sayılı Resmi Gazete'de yayımlanan Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu Yönetmeliği'nin 3. maddesinde, "1) Bu Yönetmelik, 7/6/2012 tarihli ve 6325 sayılı Hukuk Uyuşmazlıklarında Arabuluculuk Kanununun 15 inci maddesinin onuncu fıkrası, 19 uncu maddesinin ikinci fıkrası, 22 nci maddesi, 31 inci maddesinin sekizinci fıkrası, 36 ncı maddesi ile 12/10/2017 tarihli ve 7036 sayılı İş Mahkemeleri Kanununun 3 üncü maddesinin yirmi ikinci fıkrasına dayanılarak hazırlanmıştır." 5. maddesinde, "(1) Taraflar, arabulucuya başvurmak, süreci devam ettirmek, sonuçlandırmak veya bu süreçten vazgeçmek konusunda tamamen serbest olup, öncelikle uyuşmazlığı arabuluculuk yoluyla sonuçlandırma konusunda anlaşılır. Taraflar, bu sürecin içine zorla dâhil edilemeyecekleri gibi her aşamada uyuşmazlığı arabuluculuk yoluyla çözmekten de vazgeçebilirler. Ancak dava şartı olarak arabuluculuğa ilişkin özel hükümler saklıdır. (2) Taraflar, gerek arabulucuya başvururken gerekse süreç boyunca eşit haklara sahiptirler. Taraflardan biri arabuluculuk sürecinin dışında bırakılmayacağı gibi söz hakkı da diğerine göre kısıtlanamaz."; 24. maddesinde, "(1) Arabulucu, adli yargı ilk derece mahkemesi adalet komisyonu başkanlıklarına bildirilen listeden adliye arabuluculuk bürosu tarafından puanlama yöntemiyle belirlenir. Ancak tarafların listede yer alan herhangi bir arabulucu üzerinde başvuru sırasında anlaşmaları hâlinde taraflar veya tarafların imzasını taşıyan bir tutanakla beraber üzerinde anlaşılan arabulucu, durumu adliye arabuluculuk bürosuna bildirdiğinde bu arabulucu görevlendirilir. Dava şartı olan arabuluculuk ile ilgili uyuşmazlıklarda liste dışında bir arabulucu görevlendirilemez. (2) Başvuran taraf, kendisine ve elinde bulunması hâlinde karşı tarafa ait her türlü iletişim bilgisini adliye arabuluculuk bürosuna verir. Adliye arabuluculuk bürosu, tarafların resmi kayıtlarda yer alan iletişim bilgilerini araştırmaya da yetkilidir. İlgili kurum ve kuruluşlar, uyuşmazlık konusuyla sınırlı olmak üzere adliye arabuluculuk bürosu tarafından talep edilen iletişim bilgilerini vermekle

yükümlüdür. (3) Taraflara ait iletişim bilgileri, görevlendirilen arabulucuya adliye arabuluculuk bürosu tarafından verilir. Arabulucu bu iletişim bilgilerini esas alır, ihtiyaç duyduğunda kendiliğinden araştırma da yapabilir. Elindeki bilgiler itibarıyla her türlü iletişim vasıtasını kullanarak görevlendirme konusunda tarafları bilgilendirir ve ilk toplantıya tarafları ve varsa avukatlarını birlikte davet eder. Bilgilendirme ve davete ilişkin işlemlerini belgeye bağlar. Arabulucu taraflara ulaşamaması hâlinde, ulaşmak için hangi yolları denediğini ve hangi sebeplerle ulaşamadığını son tutanakta belirtir."; 25. maddesinin ilgili fıkralarında, "(1) Arabuluculuk görüşmelerine taraflar bizzat, kanuni temsilcileri veya avukatları, idareler ise oluşturacakları komisyon aracılığıyla katılabilirler. İşverenin adi veya resmi yazılı belgeyle yetkilendirdiği çalışanı da görüşmelerde işvereni temsil edebilir ve son tutanağı imzalayabilir. (2) Arabulucu adliye arabuluculuk bürosu tarafından görevlendirildikten sonra ilk önce başvuran taraftan başlamak üzere asiller ile ön görüşme yapar, başvuruca dan ve diğer taraftan uyuşmazlığın esasını öğrenir. Arabulucu asilleri, arabuluculuğun esasları, süreci ve sonuçları hakkında aydınlatıp, arabuluculuk yoluyla uyuşmazlığın çözümünün ekonomik, sosyal ve psikolojik faydalarının olduğunu hatırlatarak onları bilgilendirir. Asilleri ilk oturuma varsa vekilleri ile birlikte davet eder. (3) Arabulucu ilk oturum davetini yaparken toplantı tarihi ve yerinin belirlenmesi konusunda taraflar ile iletişim kurar. Taraflarla yaptığı görüşme sonucunda bir mutabakat sağlanamazsa toplantı tarihini ve yerini kendisi belirler." kuralları yer almıştır.

Dava Konusu Yönetmeliğin 5. maddesinin 1. fıkrasının incelenmesi:

Dava konusu 02/06/2018 tarih ve 30439 sayılı Resmi Gazete'de yayımlanan Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu Yönetmeliği'nin 5. maddesinin 1. fıkrasında "(1) Taraflar, arabulucuya başvurmak, süreci devam ettirmek, sonuçlandırmak veya bu süreçten vazgeçmek konusunda tamamen serbest olup, öncelikle uyuşmazlığı arabuluculuk yoluyla sonuçlandırma konusunda anlaşılırlar. Taraflar, bu sürecin içine zorla dâhil edilemeyecekleri gibi her aşamada uyuşmazlığı arabuluculuk yoluyla çözmekten de vazgeçebilirler. Ancak dava şartı olarak arabuluculuğa ilişkin özel hükümler saklıdır." kuralları düzenlenmiştir. Davacı tarafından, fıkranın son cümlesinde yer alan "Ancak dava şartı olarak arabuluculuğa ilişkin özel hükümler saklıdır." hükmünün fıkra ile çelişki yarattığı, arabuluculuğu iradi olmaktan çıkarttığı, Kanun'a aykırı olduğu iddia edilerek fıkranın iptali istenilmişse de, söz konusu Yönetmeliğin 3. maddesinde, Yönetmeliğin 6325 sayılı Hukuk Uyuşmazlıklarında Arabuluculuk Kanununun 15 inci maddesinin onuncu fıkrası, 19 uncu maddesinin ikinci fıkrası, 22 nci maddesi, 31 inci maddesinin sekizinci fıkrası, 36 ncı maddesi ile 12/10/2017 tarih ve 7036 sayılı İş Mahkemeleri Kanununun 3 üncü maddesinin yirmi ikinci fıkrasına

dayanılarak hazırlandığının düzenlendiği, anılan 7036 sayılı İş Mahkemeleri Kanunu'nun 3. maddesinde dava şartı olarak arabuluculuğun düzenlendiği ve 22. fıkrasının son cümlesinde "Arabuluculuğa başvuru usulü, arabulucunun görevlendirilmesi ve arabuluculuk görüşmelerine ilişkin diğer hususlar Adalet Bakanlığınca yürürlüğe konulan yönetmelikle belirlenir." kuralının yer aldığı, bu halde Yönetmeliğin dava konusu edilen, dava şartı olarak arabuluculuğa ilişkin özel hükümleri saklı tutan kuralının yasal dayanağının bulunduğu; bununla birlikte, "Ancak dava şartı olarak arabuluculuğa ilişkin özel hükümler saklıdır." cümlesini içeren Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu Yönetmeliği'nin 5. maddesinin, Yönetmeliğin "Genel Hükümler" inin yer aldığı birinci kısmının, "Arabuluculuğun Temel İlkeleri" ne ilişkin ikinci bölümünde düzenlendiği, "Dava Şartı Olarak Arabuluculuk" a ilişkin hükümlere ise Yönetmeliğin ikinci kısmı olan "Özel Hükümler" altında yer verildiği, bu bakımdan düzenleniş tekniğinin de usul ve esaslara uygun olduğu görülmekle, iptali için ileri sürülen hususların yasal dayanağı bulunmadığından, dava konusu düzenleyici işlemde hukuka aykırılık görülmemiştir.

Dava Konusu Yönetmeliğin 24. maddesinin 2. fıkrasının incelenmesi:

Davacı tarafından, 02/06/2018 tarih ve 30439 sayılı Resmi Gazete'de yayımlanan Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu Yönetmeliği'nin 24. maddesinin 2. fıkrasının 1. cümlesinde yer alan, "Başvuran taraf, kendisine ve elinde bulunması hâlinde karşı tarafa ait her türlü iletişim bilgisini adliye arabuluculuk bürosuna verir." kuralının 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun kişisel verilerin ilgili kişinin açıkça rızası olmaksızın işlenemeyeceği ve aktarılamayacağı yönündeki hükümlerine aykırı olduğu, anılan Kanun'un 8. maddesinin 3. fıkrasında "Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır." hükmü düzenlendiğinden kişisel verilerin aktarılması konusunda sadece kanunlarla istisnai hükümler konulabileceği, bu bakımdan kuralın bir yönetmelik maddesiyle düzenlenmesinin 6698 sayılı KVKK'nın 8. maddesine ve normlar hiyerarşisine aykırılık oluşturduğu iddia edilerek, Yönetmeliğin 24. maddesinin 2. fıkrasının iptali istenilmektedir.

6698 sayılı KVKK'nın 4. maddesinin 1. fıkrasında, "(1)Kişisel veriler, ancak bu kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir"; 5. maddesinin 1. fıkrası ile 2. fıkrası ve "a" bendinde, "(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (2) Aşağıdaki şartlardan birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür: a)Kanunlarda açıkça öngörülmesi."; 8. maddesinin 1. ve 3. fıkralarında, "(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz. (3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır." hükümleri bulunmaktadır.

Dava konusu düzenlemenin yer aldığı HUAKY'nin 24. maddesinin başlığının "Dava şartı olarak arabuluculukta arabulucunun görevlendirilmesi" olduğu, dava şartı olarak arabuluculuğun düzenlendiği 7036 sayılı İş Mahkemeleri Kanunu'nun 3. maddesinin 7. fıkrasının 1. cümlesinde, "Başvuran taraf, kendisine ve elinde bulunması hâlinde karşı tarafa ait her türlü iletişim bilgisini arabuluculuk bürosuna verir." hükmünün düzenlendiği ve aynı maddenin yukarıda yer verilen 22. fıkrasına istinaden yasal dayanağına uygun olarak Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu Yönetmeliği'nin 24. maddesinin 2. fıkrasının 1. cümlesinde dava konusu edilen düzenlemeye yer verildiği, HUAKY'nin 24. maddesinin 2. fıkrasında yer alan diğer hükümlerin de 7036 sayılı Kanun'un 3. maddesinin 7. fıkrası hükmüne uygun olarak düzenlendiği, bununla birlikte başvuranın adliye arabuluculuk bürosuna verdiği bilginin dava şartı olarak arabuluculuk müessesinin uygulanabilmesi bakımından en temelde ihtiyaç duyulan iletişim bilgilerine yönelik olduğu görülmekle dava konusu düzenleyici işlem hükmünde hukuka aykırılık bulunmadığı sonucuna varılmıştır.

Dava Konusu Yönetmeliğin 25. maddesinin 2. fıkrasının incelenmesi:

02/06/2018 tarih ve 30439 sayılı Resmi Gazete'de yayımlanan Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu Yönetmeliği'nin 25. maddesinin 2. fıkrasında, "Arabulucu adliye arabuluculuk bürosu tarafından görevlendirildikten sonra ilk önce başvuran taraftan başlamak üzere asiller ile ön görüşme yapar, başvurucudan ve diğer taraftan uyuşmazlığın esasını öğrenir." hükmü düzenlenmiştir. Davacı tarafından, arabulucunun ilk önce asille görüşecek olmasını emredici nitelikte düzenlemesiyle hak arama hürriyeti ve etkin savunma hakkını ihlal ettiği, vekille temsil edilen asille doğrudan görüşülmesinin bağımsız savunmanın serbestçe temsili ve Avukatlık Kanunu'nda yer alan avukatlığın amacının gerçekleştirilmesi önünde bir engel olduğu, savunmayı temsil eden avukatın arabuluculuk sürecinden dışlanması anlamına geldiği ve adil yargılanma ilkesinin ihlal edildiği, öte yandan Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu'nda ilk önce asille görüşülmesi konusunda bir hüküm bulunmadığı iddia edilerek Yönetmeliğin 25. maddesinin 2. fıkrasının iptali istenilmektedir.

1136 sayılı Avukatlık Kanunu'nun 1. maddesinin 2. fıkrasında, " Avukat, yargının kurucu unsurlarından olan bağımsız savunmayı serbestçe temsil eder."; 2. maddesinin 1. ve 2. fıkralarında, "Avukatlığın amacı; hukuki münasebetlerin düzenlenmesini, her türlü hukuki mesele ve anlaşmazlıkların adalet ve hakkaniyete uygun olarak çözümlenmesini ve hukuk kurallarının tam olarak uygulanmasını her derecede yargı organları, hakemler, resmi ve özel kişi, kurul ve kurumlar nezdinde sağlamaktır. Avukat bu amaçla hukuki bilgi ve tecrübelerini adalet hizmetine ve kişilerin yararlanmasına tahsis eder." hükümleri düzenlenmiştir.

6325 sayılı Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu'nun 1. maddesinin 1. fıkrasında, " Bu kanunun amacı, hukuk uyuşmazlıklarının arabuluculuk yoluyla çözümlenmesinde uygulanacak usul ve esasları düzenlemektir."; 8. maddesinde, "(1) Arabulucu, tarafların her biri ile ayrı ayrı veya birlikte görüşebilir ve iletişim kurabilir"; 11. maddesinde, " (1) Arabulucu, arabuluculuk faaliyetinin başında, tarafları arabuluculuğun esasları, süreci ve sonuçları hakkında gerektiği gibi aydınlatmakla yükümlüdür"; 15. maddesinin ilgili fıkralarında, " (1) Arabulucu, seçildikten sonra tarafları en kısa sürede ilk toplantıya davet eder. (2) Taraflar, emredici hukuk kurallarına aykırı olmamak kaydıyla arabuluculuk usulünü serbestçe kararlaştırabilirler. (...) (6) (Değişik: 12/10/2017-7036/22 md.) Arabuluculuk müzakerelerine taraflar bizzat, kanuni temsilcileri veya avukatları aracılığıyla katılabilirler. Uyuşmazlığın çözümüne katkı sağlayabilecek uzman kişiler de müzakerelerde hazır bulundurulabilir. (8) (Değişik: 12/10/2017-7036/22 md.) Arabuluculuk müzakerelerinde idareyi, üst yönetici tarafından belirlenen iki üye ile hukuk birimi amiri veya onun belirleyeceği bir avukat ya da hukuk müşavirinden oluşan komisyon temsil eder. Komisyon, arabuluculuk müzakereleri sonunda gerekçeli bir rapor düzenler ve beş yıl boyunca saklar." (...) (10) (Değişik: 12/10/2017-7036/22 md.) Bu maddenin uygulanmasına ilişkin usul ve esaslar Bakanlıkça yürürlüğe konulan yönetmelikle düzenlenir."; 6/12/2018 tarih ve 7155 sayılı Kanun'un 23. maddesiyle eklenen 18/A maddesinin 19 ve 20. fıkralarında da, " (19) İlgili kanunlarda dava şartı olarak arabuluculuğa ilişkin kabul edilen özel hükümler saklıdır. (20) Bu bölümde hüküm bulunmayan hâllerde niteliğine uygun düştüğü ölçüde bu Kanunun diğer hükümleri uygulanır." hükümlerine yer verilmiştir.

7036 sayılı İş Mahkemeleri Kanunu'nun "Dava şartı olarak arabuluculuğu" düzenleyen 3. maddesinin 18, 21 ve 22. fıkralarında ise " (18) Arabuluculuk görüşmelerine taraflar bizzat, kanuni temsilcileri veya avukatları aracılığıyla katılabilirler. İşverenin yazılı belgeyle yetkilendirdiği çalışanı da görüşmelerde işvereni temsil edebilir ve son tutanağı imzalayabilir. (21) Bu maddede hüküm bulunmayan hâllerde niteliğine uygun düştüğü ölçüde 7/6/2012 tarihli ve 6325 sayılı Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu hükümleri uygulanır. (22) Arabuluculuğa başvuru usulü, arabulucunun görevlendirilmesi ve arabuluculuk görüşmelerine ilişkin diğer hususlar Adalet Bakanlığınca yürürlüğe konulan yönetmelikle belirlenir." hükümleri düzenlenmiştir.

İlgili mevzuat hükümleri incelendiğinde, avukatı arabuluculuk sürecinin herhangi bir aşamasından ayrık tutan yasal bir düzenlemenin bulunmadığı, bu bakımdan asillerin talep etmesi halinde avukat olan vekilin Yönetmelikte yer alan dava konusu düzenlemeye dayanılarak arabuluculuğun herhangi bir aşamasının dışında bırakılmayacağı, bu bakımdan arabuluculuk sürecinde asillerinin kendilerini vekille temsiline engel olunmasının hukuka uygun bulunmadığı sonucuna varılmıştır.

KARAR SONUCU:

Açıklanan nedenlerle;

1. 02/06/2018 tarih ve 30439 sayılı Resmi Gazete'de yayımlanan Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu Yönetmeliği'nin 5. maddesinin 1. fıkrasının, 24. maddesinin 2. fıkrasının ve 25. maddesinin 2. fıkrasının "Arabulucu adliye arabuluculuk bürosu tarafından görevlendirildikten sonra ilk önce başvuran taraftan başlamak üzere asiller ile ön görüşme yapar, başvurucudan ve diğer taraftan uyuşmazlığın esasını öğrenir." hükmü dışında kalan diğer kısımlarının iptali istemi yönünden DAVANIN REDDİNE,
2. 02/06/2018 tarih ve 30439 sayılı Resmi Gazete'de yayımlanan Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu Yönetmeliği'nin 25. maddesinin 2. fıkrasında yer alan "Arabulucu adliye arabuluculuk bürosu tarafından görevlendirildikten sonra ilk önce başvuran taraftan başlamak üzere asiller ile ön görüşme yapar, başvurucudan ve diğer taraftan uyuşmazlığın esasını öğrenir." hükmünün İPTALİNE,
3. Ayrıntısı aşağıda gösterilen toplam ... TL yargılama giderinin takdiren, ... TL'sinin davacı üzerinde bırakılmasına, geriye kalan ... TL'sinin davalı idareden alınarak davacıya verilmesine,
4. Karar tarihinde yürürlükte bulunan Avukatlık Asgari Ücret Tarifesi uyarınca duruşmalı işler için belirlenen ... TL vekâlet ücretinin davacıdan alınarak davalı idareye verilmesine; davacı vekilinin duruşmaya katılmadığı görüldüğünden duruşmasız işler için belirlenen ... TL vekalet ücretinin davalı idareden alınarak davacıya verilmesine,
5. Posta gideri avansından artan tutarın kararın kesinleşmesinden sonra davacıya iadesine,
6. Bu kararın tebliğ tarihini izleyen 30 (otuz) gün içerisinde Danıştay İdari Dava Daireleri Kuruluna temyiz yolu açık olmak üzere, 08/04/2021 tarihinde oy birliğiyle karar verildi.

Danıştay Kararı - 13. Daire (E. 2018/2910)

Danıştay Kararı - 13. D., E. 2018/2910 K. 2020/3772 T. 22.12.2020

T.C. DANIŞTAY ONÜÇÜNCÜ DAİRE

Esas No: 2018/2910

Karar No: 2020/3772

DAVACI: ... Elektrik Perakende Satış A.Ş.

VEKİLLERİ: Av. ...

DAVALI: ... Kurumu

VEKİLLERİ: Av. ...

DAVANIN KONUSU:

30/05/2018 tarih ve 30436 sayılı Resmî Gazete'de yayımlanan Elektrik Piyasası Tüketici Hizmetleri Yönetmeliği'nin 4. maddesinin (y) bendinin, 58., 62., 13., 14., 15., 16., 18., 20., 9., ve 10. maddelerinin tamamının, 35. maddesinin ikinci, üçüncü ve dördüncü fıkralarının, 35. maddesinin beşinci fıkrasının (a) bendinin 1 ve 2 numaralı alt bentlerinin, 12. maddesinin birinci fıkrasının, 37. maddenin sekizinci fıkrasının ve 57. maddesinin ikinci fıkrasının iptali istenilmektedir.

DAVACININ İDDİALARI:

İkili anlaşma şartlarının Kurul tarafından belirlenebileceğine ilişkin Kanun maddesi bulunmadığından ikili anlaşmaların içeriğini düzenleyen Yönetmelik maddelerinin hukuka aykırı olduğu, Yönetmeliğin "İkili anlaşmanın tarafları" başlıklı 9. maddesi ile "Tanımlar" başlıklı 4. maddesinin (y) bendinde yer alan "tüketimi düşük serbest tüketici" tanımının 6446 sayılı Kanun'a, Türk Borçlar Kanunu ve Türk Ticaret Kanunu'na aykırı olduğu, Yönetmeliğin 10. maddesinde yer verilen "İkili anlaşma türleri ve genel esaslar" başlıklı düzenlemenin üst hukuk normlarına uygun olmadığı, Yönetmelikte tüketicilerin telefon numarası ve e-posta adreslerinin bulunması hâlinde kayıt altına alınacağı öngörülmüşken, tüketiciye kalıcı veri saklayıcısı ile bildirim yapılmasının zorunlu tutulduğu, tüketicilere cayma hakkı tanınmasının hukuka aykırı olduğu, Kanunlarda sınırlı sayıdaki sözleşme tipleri için cayma hakkının düzenlendiği, cayma hakkı için verilen sürenin uzun

olduđu, sözleşme imzalandıktan sonra enerji alımı yapıldığı, bu maddenin tedarik şirketlerine mali külfet yaratacağı ileri sürülmüştür.

DAVALININ SAVUNMASI:

Öncelikle, usûle ilişkin olarak, davanın süre açısından incelenmesi, süresinde açılmayan davanın süre aşımı nedeniyle reddedilmesi gerektiği; esasa ilişkin olarak ise, 4628 sayılı Kanun'un 5. maddesinin 6. fıkrasının (c) bendinde "Tüketicilere güvenilir, kaliteli, kesintisiz ve düşük maliyetli elektrik enerjisi hizmetini verilmesini teminen gerekli düzenlemeleri yapma" yetkisinin Kurul'a verildiği, Kanun'un 9. maddesinin 2. fıkrasının (a) bendinde Elektrik Piyasası Dairesi Başkanlığı'na tüketici şikâyetlerini inceleme görev ve yetkisi verildiği, 6446 sayılı Kanun'un 1. maddesinde yer verilen Kanun'un amacı ve 4. maddesinde yer verilen "Piyasada faaliyet gösterecek tüzel kişilerin faaliyetlerinde uymaları gereken usul ve esaslar yönetmelikle düzenlenir" kuralı ile 10. maddesinde yer verilen "Toptan ve perakende satış faaliyetleri, üretim şirketleri ile tedarik lisansı kapsamında kamu ve özel sektör tedarik şirketleri tarafından, bu Kanun ve bu Kanun'a göre çıkarılan yönetmelikler uyarınca yürütülür" kuralı gereği Kurul'un ikili anlaşmalara ilişkin düzenleme yetkisi bulunduğu açık olduđu, Yönetmelik ile tedarikçilerin tek taraflı olarak standart ve genel işlem koşulu içerecek şekilde düzenledikleri ikili anlaşmalarda menfaat dengelerine aykırı şekilde tüketici aleyhine öngördükleri ve özellikle Kurum'a ulaşan serbest tüketici şikâyetlerinin yoğunlaştığı konularda düzenleme yapıldığı, ikili anlaşmalarda yer verilen düzenlemelerin diğer tedarikçiler aleyhine piyasayı kapama etkisine sahip olduđu ve haksız rekabete neden olduđu, Yönetmelik ile ikili anlaşma tanımına bağlı kalındığı, bu sözleşmelerin doğrudan ya da dolaylı olarak Kurul onayına tabi tutulmasına ilişkin kural öngörülmediği, ikili anlaşmaların özel hukuk rejimine tabi olmasını engelleyici düzenleme yapılmadığı, Yönetmelik ile "tüketimi düşük serbest tüketici" tanımı getirildiği, yıllık elektrik enerjisi tüketiminin 100.000 kWh'den düşük olan serbest tüketicilerin tüketimi düşük serbest tüketici olarak tanımlandığı, belirlenen bu eşiğin toplam abonelerin %92'sine, toplam tüketimin ise %52'sine tekabül ettiği, ikili anlaşmalarda Yönetmelik maddelerine uygun davranmalarının amaçlandığı, mesken, tarımsal sulama, küçük ticarethane ve sanayi tüketicileri ile tedarikçiler arasındaki teknik ve hukuki bilgi asimetrisinin mevcudiyeti nedeniyle tedarikçiler tarafından standart veya genel işlem koşulu içerecek şekilde düzenlenecek ikili anlaşmalarda öngörülen haksız şart oluşturan ifadeler ve tüketiciler aleyhine muğlak ifadeler nedeniyle tüketici mağduriyetlerinin önüne geçilmesinin amaçlandığı, davacının iddialarının aksine mülga Yönetmelik döneminde de ikili anlaşmalara ilişkin düzenlemelerin bulunduğu, Yönetmelik ile süreli sözleşmelerin azami sınırının 3 yıl olarak belirlenerek süre kısıtı ile piyasa kapama etkisinin önüne geçilmesinin istendiği, Yönetmelikte

bildirim yapılmasının öngörüldüğü söz konusu iletişim bilgileri bulunmadığını beyan eden tüketiciler için Yönetmelik kapsamındaki bildirimlerin tedarikçiler tarafından kalıcı veri saklayıcı ile yapılmasının beklenmediği, Yönetmeliğin 12. maddesi ile, ikili anlaşmalar kurulmadan ve yenilenmeden önce serbest tüketicilerin genel olarak hakları ile, tüketicinin ikili anlaşmalar kapsamındaki esaslı yükümlülükleri ve maliyet doğuran yan yükümlülükleri hakkında standart formlar ile bilgilendirilmelerinin sağlanmasının amaçlandığı, cayma hakkının fiziken alım yapılmasından önce olacak şekilde 14 gün olarak belirlendiği, 14 günlük sürenin belirlenmesinde diğer mevzuat takviminin dikkate alındığı, haklı fesih sebeplerinin neler olacağını Yönetmelikte belirlendiği, ikili anlaşmalardaki gecikme faizi ile güvence bedeline ilişkin bir sınırlama getirilmediği, cayma bedeli ve cezai şartlara sınır getirildiği, piyasada tedarik firmalarının yüksek cayma bedeli ve ceza koşulu belirleyerek tedarikçi değişikliklerini engellediğinin görüldüğü, Yönetmeliğin yürürlüğe girmesi için verilen sürenin yeterli olduğu savunulmuştur.

DANIŞTAY TETKİK HÂKİMİ ...'NİN DÜŞÜNCESİ: Davanın reddi gerektiği düşünülmektedir.

DANIŞTAY SAVCISI ...'İN DÜŞÜNCESİ: Dava; sahip olduğu tedarik lisansı kapsamında görevli tedarik şirketi olarak çalışan davacı şirket tarafından; 30/05/2018 tarih ve 30436 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Elektrik Piyasası Tüketici Hizmetleri Yönetmeliği'nin 4/y., 9., 10., 12/1.,13., 14., 15., 16., 18., 20., 35/2.,3.,4. ve 5.fıkrasının a bendinin 1 ve 2 numaralı alt bentlerinin, 37/8., 57/2., 58. ve 62. maddelerinin; 6446 sayılı Elektrik Piyasası Kanunu, Türk Borçlar Kanunu, Tüketicinin Korunması Hakkında Kanun ve Türk Ticaret Kanunu ile Anayasa'nın ilgili maddelerine aykırılık teşkil ettiği ileri sürülerek iptali istemi ile açılmıştır.

4628 sayılı Enerji Piyasası Düzenleme Kurumu'nun Teşkilat ve Görevleri Hakkında Kanun'un 4. maddesinde, "Kurum, tüzel kişilerin yetkili oldukları faaliyetleri ve bu faaliyetlerden kaynaklanan hak ve yükümlülüklerini tanımlayan Kurul onaylı lisansların verilmesinden, işletme hakkı devri kapsamındaki mevcut sözleşmelerin bu Kanun hükümlerine göre düzenlenmesinden, piyasa performansının izlenmesinden, performans standartlarının ve dağıtım ve müşteri hizmetleri yönetmeliklerinin oluşturulmasından, tadilinden ve uygulattırılmasından, denetlenmesinden, bu Kanunda yer alan fiyatlandırma esaslarını tespit etmekten, piyasa ihtiyaçlarını dikkate alarak serbest olmayan tüketicilere yapılan elektrik satışında uygulanacak fiyatlandırma esaslarını tespit etmekten ve bu fiyatlarda enflasyon nedeniyle ihtiyaç duyulacak ayarlamalara ilişkin formülleri uygulamaktan ve bunların denetlenmesinden ve piyasada bu Kanuna uygun şekilde davranılmasını sağlamaktan sorumludur." hükmüne yer verilmiş; 5. maddesinin altıncı fıkrasının (c) bendinde, "Tüketicilere güvenilir, kaliteli, kesintisiz ve düşük maliyetli elektrik enerjisi hizmeti verilmesini teminen gerekli

düzenlemeleri yapmak." Kurul'un görevleri arasında sayılmış; 9. maddesinin 2. fıkrasının (a) bendi ile de, "Bu Kanun ve diğer kanunlarla Kuruma verilen elektrik piyasası ile ilgili düzenleme, rekabet şartlarını oluşturma, tüketici haklarının korunması ile tüketici şikayetlerinin incelenmesi çalışmalarını yapmak...." görevi Elektrik Piyasası Dairesi Başkanlığına verilmiştir.

6446 sayılı Elektrik Piyasası Kanununun "Amaç" başlıklı 1. maddesinde, "Bu Kanunun amacı; elektriğin yeterli, kaliteli, sürekli, düşük maliyetli ve çevreyle uyumlu bir şekilde tüketicilerin kullanımına sunulması için, rekabet ortamında özel hukuk hükümlerine göre faaliyet gösteren, mali açıdan güçlü, istikrarlı ve şeffaf bir elektrik enerjisi piyasasının oluşturulması ve bu piyasada bağımsız bir düzenleme ve denetimin yapılmasının sağlanmasıdır." hükmü yer almış; 3. maddesinin birinci fıkrasının (j) bendinde, "Gerçek veya tüzel kişiler arasında özel hukuk hükümlerine tabi olarak, elektrik enerjisi ve/veya kapasitesinin alınıp satılmasına dair yapılan ve Kurul onayına tabi olmayan ticari anlaşmalar" "İkili anlaşma" olarak tanımlanmış; 4. maddesinin 2. fıkrasında, piyasada faaliyet gösterecek tüzel kişilerin faaliyetlerinde uymaları gereken usul ve esasların yönetmelikle düzenleneceği ifade edilmiş, 10. maddesinin birinci fıkrasında ise, toptan ve perakende satış faaliyetlerinin, üretim şirketleri ile tedarik lisansı kapsamında kamu ve özel sektör tedarik şirketleri tarafından, bu Kanun ve bu Kanuna göre çıkarılan yönetmelikler uyarınca yürütüleceği kurala bağlanmıştır.

Elektrik piyasasında serbest olmayan tüketiciler, elektrik enerjisi ve/veya kapasite alımlarını davalı idare tarafından belirlenen tarifeler üzerinden sadece bölgesinde bulunduğu görevli tedarik şirketinden yapabilirler. Görevli tedarik şirketleri de, serbest olmayan tüketicilere elektrik tedarik etmek zorundadır. Söz konusu tüketiciler elektrik alabilmek için, bölgelerindeki görevli tedarik şirketi ile Kurul onayına tabi perakende satış sözleşmesi imzalamak zorundadır. Serbest tüketiciler, istedikleri tedarik şirketi ile mali hükümleri ve içeriği karşılıklı belirlenebilecek ikili anlaşma imzalamak suretiyle elektrik enerjisi alabilirler. İkili anlaşmalar 6446 sayılı Kanunda tanımlanmış gibi Kurum onayına tabi olmayan, anlaşmalardır. Ancak bu ikili anlaşmalar tüketiciyle tek tek müzakere edilmek suretiyle karşılıklı olarak hüküm ve şartları kararlaştırılmayıp, aksine tedarikçi tarafından önceden tek taraflı olarak düzenlenip tüketicilere imzalatılmakta ve bu anlaşma hükümlerine göre de piyasa işleyerek şekillenmektedir. Kuruma tüketici ve tedarikçiler tarafından yapılan şikayet ve bilgi edinme başvuruları üzerine yapılan inceleme ve araştırmalarda ikili anlaşmaların tüketici aleyhine şekillenerek mağduriyete yol açtığından bahisle konuyla ilgili tedbirlerin alınması ihtiyacı doğduğu anlaşıldığından dava konusu düzenlemenin getirildiği görülmektedir.

Yönetmelik, serbest, serbest olmayan ve son kaynak tedariki kapsamındaki tüketicilere elektrik enerjisi ve kapasite satışı ile buna ilişkin hizmetlerin sunulmasında tüketici, tedarikçiler ve dağıtım şirketleri arasındaki iş ve işlemlere esas asgari standartlar ile usul ve esasların belirlenmesine yönelik olup elektrik piyasasında, tedarikçiler ile tüketimi düşük serbest tüketiciler arasında yapılacak ikili anlaşmada yer alacak asgari usul ve esaslarla, görevli tedarik şirketleri ile serbest olmayan tüketiciler ya da son kaynak tedariki kapsamındaki tüketiciler arasında yapılacak perakende satış sözleşmesinde yer alacak asgari usul ve esasları ve dağıtım şirketleri ile tüketiciler ve tedarikçiler arasında yapılacak bazı iş ve işlemlere ilişkin hükümleri kapsamaktadır.

Yönetmelik hükümleri ile genel olarak; tedarikçiler ile tüketimi düşük serbest tüketiciler arasında yapılacak ikili anlaşmaların bu yönetmelikte belirlenen usul ve esaslara uygun olmasının zorunlu olduğu, tedarikçilerin tüketimi düşük serbest tüketicilerle belirli süreyle veya belirsiz süreli ikili anlaşma yapabilecekleri, belirli süreli anlaşmaların 3 yılı geçemeyeceği, bu ikili anlaşmanın yazılı ya da mesafeli olarak kurulabileceği, tedarikçilerin ikili anlaşma kurulmadan önce, açık ve anlaşılabilir bir şekilde tüketiciyi bilgilendirmek ve tüketicinin söz konusu bilgileri edindiğini teyit etmek zorunda olduğu, bilgilendirmenin yapıldığına ve tüketici tarafından onaylandığına ilişkin ispat yükümlülüğünün tedarikçiye ait bulunduğu, bilgilendirmenin gereği gibi ya da hiç yapılmamasının tüketici açısından haklı fesih sebebi olduğu, elektrik tüketimi düşük serbest kullanıcıların, ikili anlaşmanın kurulduğu veya yenilendiği tarihten itibaren 14 gün içerisinde herhangi bir gerekçe göstermeden, cayma bedeli ödemeksizin telefonla, e-postayla veya yazılı olarak bildirim yapmak suretiyle anlaşmadan cayma haklarının bulunduğu, belirli süreli ikili anlaşmanın süre sonunda kendiliğinden sona ereceği ve otomatik yenilenmeyeceği, sözleşmeye aksine hüküm konulamayacağı, tedarikçinin ikili anlaşmanın sona ereceği tarihten en az 60 gün önce durumu tüketiciye bildirmek ve bunu kayıt altına almak zorunda olduğu, ikili anlaşma hükümlerinde sözleşme süresince tüketici aleyhine değişiklik yapılamayacağı, tedarikçiye tek taraflı değişiklik yapma yetkisi veren hükmün sözleşmeye konulamayacağı, tedarikçinin değişiklik teklifinin kayıt altına alınarak iletilmesi ve tüketici tarafından kabulü halinde yürürlüğe girebileceği, buna ilişkin ispat yükünün tedarikçide olduğu, aksi halde değişikliğin yapılmamış sayılacağı, belirli süreli anlaşmalarda, tarafların haklı sebebe dayanarak cayma bedeli ve ceza koşulu ödemediği önceden bildirim yaparak fesih hakkını kullanabilecekleri, belirsiz süreli anlaşmalarda ise tüketicinin herhangi bir gerekçe göstermeden cayma bedeli ve ceza koşulu ödemeksizin her zaman fesih hakkını kullanabileceği, fesih yazılı olarak bildirilebileceği gibi kayıt altına alınmak şartıyla telefon ve e-posta yoluyla da yapılabileceği, sınırlı sayıda sayma usulü ile ikili anlaşma kapsamında alınacak bedellerin belirtildiği, bunun haricinde sözleşmeye hüküm koyma imkanının getirilmediği, belirli

sürelili ikili anlaşmalarda tedarikçi ya da tüketimi düşük serbest tüketici aleyhine ceza koşullunun ancak haksız fesih için kararlaştırılabileceği yolunda birtakım kurallar getirilmiştir.

Bulunduğu dağıtım bölgesindeki serbest tüketici olmayan tüketiciler ile serbest tüketici niteliğini haiz olduğu halde, başka bir tedarikçiden elektrik enerjisi temin etmeyen tüketicilere, son kaynak tedarikçisi sıfatıyla elektrik enerjisi sağlamakla yükümlü bulunan görevli tedarik şirketi olan davacı şirket tarafından; Yönetmelikle tüketici Haklarını Koruma Kanundaki tüketici kavramının genişletildiği, tacir sıfatına haiz bazı meslek gurubunun da burada tüketimi düşük serbest tüketici sayıldığı, Yönetmeliğin belirlediği limit ile tacirler ile tedarikçi arasındaki ikili anlaşmalara da müdahale edildiği, TTK'nun basiretli bir iş adamı gibi davranma yükümlülüğü getirdiği tacirleri de TBK kapsamında genel işlem koşulları vasıtasıyla hukuki bir koruma getirdiği, böylece serbestleşmenin önünü tıkayan, adil bir rekabet ortamının kurulmasına engel teşkil eder nitelikte, Borçlar Kanunu ve Ticaret Kanunu ile düzenlenen, Anayasa ile güvence altına alınan sözleşme hürriyeti ilkesine ve üst hukuk normlarına aykırı olduğu ileri sürülerek yönetmelik maddelerinin iptali istenilmektedir.

İptali istenilen Yönetmeliğin 4. maddesinin 1. fıkrasının (y) bendinde "Tüketimi düşük serbest tüketici", "Yıllık elektrik enerjisi tüketimi 100.00 kWh'tan düşük olan serbest tüketici" şeklinde tanımlanmıştır.

Yönetmeliğin "İkili anlaşmanın tarafları" başlıklı 9. maddesinde, "Bu bölümde yer alan ikili anlaşmaya ilişkin usul ve esaslar, tüketimi düşük serbest tüketicilerle tedarikçiler arasında yapılan ikili anlaşmaları kapsar." kuralı, Yönetmeliğin 10. maddesinde ise; (1) Tedarikçiler tüketimi düşük serbest tüketicilere belirli süreli ya da belirsiz süreli ikili anlaşma önerebilir.

(2) Belirli süreli ikili anlaşmaların süresi üç yıldan fazla olamaz.

(3) İkili anlaşma ve ekleri ile Tüketici Hakları Bilgilendirme Formu (EK-1), İkili Anlaşma Ön Bilgilendirme Formu (EK-2-A) ve İkili Anlaşma Değişiklik Bildirimi (EK-3) en az on iki punto büyüklüğünde, anlaşılabilir bir dilde, açık, sade ve okunabilir bir şekilde düzenlenir.

(4) Tedarikçinin ikili anlaşmanın kurulmasına, yenilenmesine ve ikili anlaşmada değişiklik yapılmasına ilişkin önerisi karşısında tüketicinin susması veya açıkça reddetmemesi önerinin kabulü olarak yorumlanamaz ve aksi hükme ikili anlaşmada yer verilemez",

12/1. maddesinde de; "Tedarikçi ikili anlaşma kurulmadan önce EK-1 ve EK-2'de yer alan standart formlarla açık ve anlaşılabilir bir şekilde kayıt altına almak suretiyle kağıt üzerinde veya kalıcı veri saklayıcısı ile tüketiciyi bilgilendirmek ve tüketicinin söz konusu bilgileri edindiğini teyit etmesini

sağlamak zorundadır. Söz konusu bilgilendirmenin yapıldığına ve tüketici tarafından teyit edildiğine ilişkin ispat yükü tedarikçiye aittir. Bilgilendirmenin gereği gibi ya da hiç yapılmamış olması tüketici için haklı fesih sebebidir." düzenlemeleri getirilmiştir.

Yönetmeliğe göre, elektrik enerjisini satın alacağı tedarikçiyi seçme hakkına sahip olan serbest tüketicilerden, yıllık elektrik enerjisi tüketimi 100.000 kWh'dan düşük olanlar Tüketimi Düşük Serbest Tüketici diye tabir edilmekte ve bunların tedarikçisi ile yapacağı ikili anlaşmaların bu yönetmelikte belirlenen usul ve esaslara uygun olması öngörülmekte diğer serbest tüketicilerin ikili anlaşmalarının Yönetmelik kapsamına alınmasına zorunluluk getirilmemektedir. Ancak istendiği takdirde ikili anlaşmalarına bu yönde bir hüküm getirmelerine de bir engel konulmamaktadır. Buradaki amaç tedarikçilerin tüketimi düşük serbest tüketicilerle yapılan ikili anlaşmalarda Yönetmelikle öngörülen hükümlere riayet etmelerine zorunluluk getirerek bu tür tüketicilere hukuki güvenlik sağlamak ve tedarikçilerin anlaşma öncesi bazı yükümlülüklerini yerine getirmelerini sağlayarak tüketici aleyhine oluşabilecek ve piyasa düzenini bozacak aksamaların önüne geçilmesidir. Mesken, tarımsal sulama, küçük ticarethane ve sanayi tüketicilerin tedarikçiler ile denk hukuki ve teknik bilgi gücüne sahip olması düşünülemeyeceğinden, tedarikçiler tarafından standart veya genel işlem koşulu içerecek şekilde düzenlenen ikili anlaşmalarda öngörülen haksız şart ve tüketici aleyhine uygulanan muğlak ifadeler nedeniyle oluşan tüketici mağduriyetinin önüne geçmek düşüncesiyle, Tüketimi düşük serbest tüketici ile yapılacak ikili anlaşmaların asgari standardının belirlenmesindeki asıl amacın; Avrupa Enerji Düzenleyicileri Konseyi (CEER) raporlarına da giren; ikili anlaşmaların kurulması öncesinde tüketiciyi bilgilendirme yükümlülüğünün gereği gibi yerine getirilmemesi, belirli süreli ikili anlaşmaların süresi sonunda sona ermesinin ikili anlaşma hükümleri ile zorlaştırılması ve engellenmesi, tüketicinin bilgisi ve iradesi dışında anlaşma hükümlerinde değişiklik yapılması, fesih hallerinde tüketiciden yüksek tutarlarda ceza koşulu istenilmesi ve bütün bunların sonucunda perakende elektrik piyasasının etkin ve verimli şekilde işleyişine zarar verilmesi, diğer tedarikçiler aleyhine piyasayı kapama ve haksız rekabete sebep olma gibi birtakım olumsuzlukları önlemek olduğu anlaşıldığından, Yönetmeliğin bu hükümlerinde hukuka aykırılık görülmemiştir.

Davacı tarafından, yasada olmayan bu ayırımın yönetmelikle getirilemeyeceği, 6446 sayılı Kanun ile 6502 sayılı Tüketicinin Korunması Hakkında Kanun hükümlerinde böyle bir tanım yer almamasına rağmen Yönetmelik ile getirilerek bu tanımlamanın içinde kalan kişilerle yapılacak sözleşmelere Yönetmelik ile müdahale edilmesinin anlaşma özgürlüğüne (sözleşmelerin iradiliği) ilkesine ve Anayasa da belirlenen eşitlik ilkesine aykırı olduğu, Türk Ticaret Kanunu uyarınca tacir sayılan kişilere tüketimi düşük serbest tüketici kavramı ile koruma sağlandığı, bu nedenle yönetmeliğin bu

hükümünün TKHK ve TTK'na aykırı olduğu, ayrıca ikili anlaşmalara şekil verilmeye çalışıldığı, bunun doğrudan sözleşme hürriyetine müdahale olduğu ileri sürülmekte ise de, idarenin bu konudaki düzenleme yetkisi ve piyasa koşulları dikkate alındığında, genelde tedarikçilerin kurduğu anlaşma modelinin tüketicinin aleyhine olduğu ve adeta bu anlaşmaya hapsolüdüğü, bu nedenle tüketimi belli bir seviyenin altında kalan piyasa tüketicilerinin yapacağı ikili anlaşmalarda asgari bir standartın getirilmesinin hukuka aykırı olmadığı sonucuna ulaşıldığından bu iddialara itibar edilememiştir.

İkili anlaşmanın kurulması sırasında tüketimi düşük tüketicinin iradesinin zaafa uğratılmaması açısından susması yada açıkca reddetmemesinin kabul anlamına gelmediği, açık irade beyanı ile anlaşmanın kurulması zorunluluğu da tüketiciyi koruma amacına yönelik olduğundan 10. maddenin bu hükmü de sözleşme serbestisinin özünü kısıtlayan bir husus olarak görülmemiştir.

Diğer taraftan; belirli süreli ikili anlaşmaların en fazla 3 yıl ile sınırlandırılmasının ve tedarikçiye getirilen tüketiciyi bilgilendirme ve bunu ispatlama yükümlülüğünün tek taraflı olarak tedarikçi aleyhine aşırı yük getirdiği düşünölmeyeceği gibi sözleşme hürriyeti ve düzenleyici işlemlerin ölçülülüğü ilkesine de aykırılık görülmemiştir. Yönetmeliğin "Cayma hakkı" başlıklı 13. maddesinde, "Tüketimi düşük serbest tüketici, ikili anlaşmanın kurulduğu ya da yenilendiği tarihten itibaren 14 gün içerisinde herhangi bir gerekçe göstermeksizin ve cayma bedeli ödemeksizin telefonla, e-postayla veya yazılı olarak bildirim yapmak suretiyle anlaşmadan cayma hakkına sahiptir." düzenlemesi yer almaktadır.

Uygulamada, rakamsal olarak kendisine sunulan indirimin uygulanacağını düşünen tüketicinin, elektrik faturasının yüksek olduğunu farketdiğinde tedarikçisinden ayrırlıp başka bir tedarikçiye geçmek istediğinde yüksek tutarda ceza koşuluyla karşılaşacağını düşündüğünden, anlaşmaya devam etmek zorunda kaldığı ve tedarikçisini değiştiremediği; bu kapsamda, 1 yıllık bir anlaşmanın hukuken belirlenen süre sonunda sona ermesi beklenirken tedarikçiler tarafından anlaşmanın sona ermesi için tüketicilerden 2-3 aylık süre öncesinden noter kanalıyla fesih bildiriminde bulunmalarının istendiği, aksi halde anlaşmanın aynı süre kadar ya da belirsiz süreli uzayacağına ilişkin anlaşmalarda düzenlemeler bulunduğu, öte yandan, tüketicilerin anlaşma fesih bildirimlerinin tedarikçiler tarafından dikkate alınmadığı, alınsa dahi tüketiciden yüksek tutarda ceza koşulu istendiği, dolayısıyla, anlaşmayı süresinde feshettiğini düşünen tüketicinin başka bir tedarikçiyle anlaşma yapıp sonraki faturasını yeni tedarikçiden almayı beklerken eski tedarikçinin anlaşmanın devam ettiğinden bahisle fatura düzenlemeye devam ettiği, yeni tedarikçinin de anlaşmaya aykırı davrandığı gerekçesiyle tüketiciden cayma bedeli ya da ceza koşulu istediği ya da yeni tedarikçinin

yeni anlaşma kapsamında fatura düzenlemeye başladığı ve fakat eski tedarikçinin ceza koşulu istediği görülmektedir.

Düzenleme ile ikili anlaşmanın kurulmasından ya da yenilenmesinden itibaren ceza koşulu ödemeksizin kullanılan cayma hakkı 14 gün ile sınırlandırılmış ve bildirim yükümlülüğünün yazılı yapılabileceği gibi telefon veya e-postayla yapılabileceği belirtilerek kolaylık imkanı sağlanmıştır. Burada, tedarikçi tüketiciye fiziken elektrik tesliminde bulunmadan yani tüketicinin tedarikçiden hiç elektrik almadan ikili anlaşmadan cayabileceği öngörüldüğünden tedarikçinin bir zarara uğraması da söz konusu olmadığı gibi, yukarıda dile getirilen tüketicinin haklarını olumsuz yönde etkileyen uygulamaların engellenmesi amaçlanarak, tüketicinin tedarikçi seçme hakkının ceza koşulu ödenmeksizin seçmesinin önü açılmıştır. Burada TTK'nun 18. maddesi hükmüne aykırı olarak tacirlerin cayma hakkının tek taraflı ve telefonla kullanması imkanının getirilmesinin, sözleşmedeki taraf dengesinin tüketimi düşük tüketici tacir lehine bozduğu ve bunun yönetmelik ile getiriliyor olmasının hukuki güvenirlik ve belirlilik ilkesini zedeleyeceğine ilişkin iddiaya itibar edilemez ve tüketimi düşük serbest tüketiciyi koruma amaçlı getirilen düzenlemede sözleşme serbestine ve hukuka aykırılık görülmediği gibi tedarikçinin Kanunlardan doğan cayma hakkına dokunulmadığı da açıktır.

Yönetmeliğin 14. maddesinde; belirli süreli ikili anlaşmanın süre sonunda kendiliğinden sona ereceği ve otomatik yenilenmeyeceği, sözleşmeye aksine hüküm konulamayacağı, tedarikçinin ikili anlaşmanın sona ereceği tarihten en az 60 gün önce durumu tüketiciye bildirmek ve bunu kayıt altına almak zorunda olduğu, 15. maddesinde de; ikili anlaşma hükümlerinde sözleşme süresince tüketici aleyhine değişiklik yapılamayacağı, tedarikçiye tek taraflı değişiklik yapma yetkisi veren hükmün sözleşmeye konulamayacağı, tedarikçinin değişiklik teklifinin kayıt altına alınarak iletilmesi ve tüketici tarafından kabulü halinde yürürlüğe girebileceği, buna ilişkin ispat yükünün tedarikçide olduğu, aksi halde değişikliğin yapılmamış sayılacağı, düzenlemeleri yer almıştır.

Belirli süreli ikili anlaşmanın süre sonunda kendiliğinden sona ereceği ve otomatik yenilenmeyeceği, sözleşmeye aksine hüküm konulamayacağı, tedarikçinin ikili anlaşmanın sona ereceği tarihten en az 60 gün önce durumu tüketiciye bildirmek ve bunu kayıt altına almak zorunda olduğu, hükümlerinin sözleşme serbestisi ile bağdaşmadığı, tarafların iradesine müdahale anlamı taşıdığı ileri sürülmekte ise de; tüketimi düşük serbest tüketicinin açık iradesi ile TTK ve TKHK hükümlerine uygun olarak ikili anlaşmanın kurulması ve yenilenmesi amacına matuf olduğundan, idarenin düzenleme yetkisi sınırları içinde yapılan ve ölçülülük ilkesini aşmayan düzenleme olarak görülmüştür.

İkili anlaşma hükümlerinde sözleşme süresince tüketici aleyhine değişiklik yapılamayacağı, tedarikçiye tek taraflı değişiklik yapma yetkisi veren hükmün sözleşmeye konulamayacağı, tedarikçinin değişiklik teklifinin tüketici tarafından kabulü halinde yürürlüğe girebileceği, buna ilişkin ispat yükünün tedarikçiye olduğu, sözleşmenin iradiliği ilkesi ile çelişen bir husus olarak görülmemiştir.

Yönetmeliğin 16. maddesinde haklı fesih sebepleri burada belirtilenlerle sınırlı olmamak üzere sayılmış olup, haklı fesih hallerinde tarafların cayma bedeli ödemesi söz konusu değildir.

Davacı tarafından anılan düzenlemeye yönelik olarak, ikili anlaşmaya müdahale edildiği, düzenlemenin belirsizlikler içerdiği öne sürülmekte ise de haklı fesih sebebi ile ikili anlaşmanın sona erdirilmesinin ve ceza koşulu ödenmemesinin hukukun genel ilkelerinden olduğu, maddede sayılanlar haricinde haklı fesih sebebi bulunan tüketiciye aynı tedarikçiden enerji alımının zorlanamayacağı yada ceza koşulu istenemeyeceği hakkaniyet ilkelerine de uygun olduğundan iptali istenen maddede hukuka aykırılık görülmemiştir.

Yönetmeliğin 18. maddesinde;"(1) İkili anlaşma kapsamında elektrik enerjisi ve kapasite satışına ilişkin aktif enerji bedeli ile tahsilatına aracı olunan ilgili mevzuat gereği uygulanan dağıtım sistem kullanım bedeli ve diğer mevzuat gereği fon, pay ve vergiler ile bunun dışında Kurulca onaylanmış ve tahsilinde aracı olunan bedeller de yer alır. Tahsilatına aracı olunan bu bedellerin neler olduğu ile bunların anlaşmanın düzenlendiği tarihteki tutarı ve değişmesi durumunda yeni tutarların tüketiciye ne şekilde bildirileceğine ilişkin bilgiye ikili anlaşmada yer verilir. (EK-2-B)

(2) Tedarikçi ikili anlaşma kapsamında yapacağı elektrik enerjisi ve/veya kapasite satışı için tek ya da çok zamanlı dilimlerinde olmak üzere aktif enerji bedelini kr/kWh olarak fiyatlandırır. Fiyatlandırma yönteminde düzenlemeye tabi fiyatlarla mukayese edebilirlik esas alınır. " düzenlemeleri getirilmiştir.

Genel olarak ikili anlaşmanın kurulması, yenilenmesi, sona ermesi, cayma ve fesih hakkı, anlaşmada değişiklik yapılması, anlaşmanın kapsamına, ceza koşuluna ve fatura düzenlenmesine, ikili anlaşma kapsamında yer alacak bedellerin belirlenmesine ve bildirimine ilişkin hükümlerin düzenlenmesinin, ikili anlaşmanın kurulmasına müdahale, tarafların sözleşme iradesinin tecellisini engellenmesi ve bu konudaki üst hukuk normları ile Ticaret Kanunu ve Borçlar Kanunu hükümlerine aykırılık olduğu ileri sürülmekte ise de; idarenin kanunla verilen düzenleme yetkisinin sınırları içinde kalan ölçülülük ilkesine aykırılık teşkil etmeyen ve piyasada dengeyi sağlamak, tüketiciye bir takım kolaylıklar sunmak amacına hizmet eden yönetmeliğin bu hükümlerinde iptali gerektirir hukuka aykırılık görülmemiştir.

Maddenin 2. bendi açısından; tüketicinin gerçekten ucuza elektrik enerjisi alıp almadığını öğrenebilmesi ve ikili anlaşma önerisinde bulunan tedarikçinin fiyatını kabul edip etmeyeceğine karar verebilmesi ancak tedarikçinin kendisine önerdiği fiyatların karşılaştırılabilir olmasına bağlıdır. Bu da ancak aktif enerji bedelinin kr/kWh olarak fiyatlandırılmasıyla mümkündür. Aksi halde tüketicinin pahalıya elektrik alması halinde bundan haberi dahi olmayacaktır.

Bu durumda, şeffaflık ilkesi uyarınca, tüketicinin aldığı hizmetin bedelini net olarak görmesini sağlayacak olması nedeniyle, anılan ibarede hukuki isabetsizlik bulunmamaktadır.

Yönetmeliğin "Ceza koşulu/cayma bedeli" başlıklı

20. maddesinde, "(1)Belirli süreli ikili anlaşmada tedarikçi ya da tüketimi düşük serbest tüketici aleyhine ceza koşulu ancak haksız fesih işlemleri için karşılaştırılabilir. Haksız fesih, haklı bir sebebe dayanmaksızın yapılan fesihtir.

(2) 7/11/2013 tarihli ve 6502 sayılı Tüketicinin Korunması Hakkında Kanun ve ilgili ikincil mevzuat kapsamındaki tüketiciler hariç tüketimi düşük serbest tüketicinin ödeyeceği cayma bedeli ve/veya ceza koşulu cayma tarihi ya da fesih tarihi öncesi tüketicinin son 12 aylık tüketim toplamı ile cayma tarihinde ya da fesih tarihinde uygulanan fiyat esas alınarak hesaplanan toplam tutarın % 10'unu geçemez.

(3) Tedarikçi tarafından anlaşmanın haksız feshedilmesi durumunda tedarikçi tüketimi düşük serbest tüketiciye ikinci fıkra kapsamında belirlenen tutarda ceza koşulu öder." düzenlemesi yer almaktadır.

Yönetmeliğin 16. maddesinde, tedarikçi ve tüketimi düşük serbest tüketici bakımından haklı fesih nedenlerine yer verilmiş, yine aynı maddede sayılan fesih hallerinin sınırlı sayıda olmadığı ifade edilmiştir. 16.madde hükmünde sayılan hallerde yani haklı fesih hallerinde tüketicinin cayma bedeli ödemesi söz konusu değildir. Yönetmelikte haksız fesih hallerinin neler olduğuna ilişkin bir düzenlemeye ise yer verilmemiş, iptali istenen madde hükmü uyarınca haksız fesih, haklı bir sebebe dayanmaksızın yapılan fesih olarak nitelendirilmiştir.

Bu durumda, ceza koşulunun ancak haksız fesih işlemleri için karşılaştırılabileceğine ilişkin düzenlemede hukukun genel prensiplerine uygun olduğu açıktır. Her ne kadar davacı, ikili anlaşmanın onaya ve düzenlemeye tabi olmayan anlaşmalar olduğu, 6446 sayılı EPK'da bunun açıkça belirtildiği, ceza koşulunun miktarının ve hangi durumlarda tahsil edilebileceğinin yönetmelikle sınırlandırılmasının sözleşme hürriyetine aykırı olduğu iddiasında bulunmakta ise de, idarenin bu konudaki piyasayı düzenleme yetkisinin ölçülülük ilkesi çerçevesinde gerçekleştiği, zaten haklı fesih

hallerinde cezai şart uygulanmasının mevzuat uyarınca hiçbir şekilde mümkün olmaması da dikkate alındığında madde hükmünde üst hukuk normlarına ve hukuka aykırılık görülmemiştir.

Yönetmeliğin 35. maddesinin ikinci fıkrasının "Görevli tedarik şirketi yazılı bildirimle birlikte kalıcı veri saklayıcılarından en az birini kullanarak tüketiciyi bilgilendirmek zorundadır." ibaresinin, üçüncü fıkrasının "Kalıcı veri saklayıcılarından en az biriyle ve" ibaresinin, dördüncü fıkrasının "Tüketiciye elektriğinin kesildiği, ayrıca kalıcı veri saklayıcıyla da bildirilir" ibaresinin, beşinci fıkrasının (a) bendinin birinci ve ikinci paragrafında yer alan "ve kalıcı veri saklayıcılarından en az birini kullanarak" ibaresinin, Sayacın doğru tüketim kaydetmemesi halinde tüketim miktarının tespiti başlıklı 37. maddesinin sekizinci fıkrasının "Ayrıca kalıcı veri saklayıcı ile de tüketici bilgilendirilir" ibaresinin iptali istemine gelince;

Yönetmeliğin 35. maddesinde; perakende satış sözleşmesi kapsamında zamanında ödenmeyen borçlarla ilgili düzenlemelere yer verilmiştir. Buna göre, tüketici elektrik enerjisi tüketimine ilişkin ödemeleri faturada belirtilen son ödeme tarihine kadar yapmazsa görevli tedarik şirketi tüketiciye ikinci bildirimde bulunacak, bu bildirimde hem tüketiciye borcunu ödemesi için en az 5 iş günü ödeme süresi tanınacak, hem de bu süre içinde borcunu ödemezse elektriğin kesileceği bildirilecektir. Tüketici bu süre içinde de borcunu ödemezse görevli tedarik şirketinin bölgedeki dağıtım şirketine tüketicinin elektriğini kesmesini bildirmesinin ardından bildirim tarihinden itibaren en geç 5 iş günü içinde tüketicinin elektriği dağıtım şirketince kesilecektir. Bundan önceki mülga yönetmelikte de bu hususa ilişkin olarak buraya kadar aynı hükümlere yer verilmiş ve yazılı bildirim yanı sıra tüketiciye ayrıca e-posta, kısa mesaj gibi diğer haberleşme kanallarıyla bildirimde bulunulması görevli tedarik şirketinin takdirine bırakılmış iken, dava konu Yönetmelik ile mülga yönetmelikten farklı olarak ikinci bildirim hem yazılı hem de kalıcı veri saklayıcılarından (e-posta, kısa mesaj) en az birisi ile gönderilmesi koşulu getirilmiş, bu hükme uymaksızın kalıcı veri saklayıcı ile bildirimde bulunulmayan yerlerin elektriğinin kesilemeyeceği de hüküm altına alınmıştır.

Elektriğin kesilmesinin perakende satış sözleşmesine taraf olan mesken, ticarethane, sanayi, tarımsal sulama, aydınlatma tüketici grubundaki tüm tüketicilerin hem günlük hem de ticari hayatını büyük ölçüde etkileyeceği dikkate alındığında, elektriğin kesilmesinden önceki ikinci bildirimden tüketicinin zamanında haberdar edilmesi o kadar önem arz etmektedir. Dolayısıyla, tüketici şikayetleri de göz önünde bulundurulduğunda yazılı bildirimle birlikte günlük kullanımda yaygın olan ve tüketiciye ulaşması yönünden daha garanti e-posta, kısa mesaj yoluyla da bildirim yapılmasında piyasa açısından kamu yararı bulunduğu açıktır.

Tüketicinin GSM numarasının ya da e-posta adresinin görevli tedarik şirketine beyan edilmemesi, perakende satış sözleşmesinin kurulmasına engel oluşturmadığından, görevli tedarik şirketinin bildirimine rağmen, bildirimlerin yapılacağı GSM numarasının ya da e-posta adresinin bulunmadığını beyan eden tüketicilerin ödenmeyen borcu nedeniyle elektriğinin kesilmesine Yönetmelik kapsamında bir engel bulunmadığından davacının iddialarına itibar edilmemiştir.

Yönetmeliğin 57. maddesinde; "(1) Tedarikçi, bu Yönetmelik kapsamında düzenlenen her bir işleme ilişkin bilgi ve belgeyi; perakende satış sözleşmesi için sözleşmenin sonlanmasını izleyen 10 yıl süresince, ikili anlaşma için ise anlaşmanın sonlanmasını izleyen 3 yıl süresince saklamak zorundadır.

(2) Tedarikçi, tüketiciye ait bilgileri başka bir amaçla kendisinin ilişkide bulunduğu faaliyetlerde kullanamaz, aksi belirtilmemiş hususlar dışında diğer tedarikçilerle paylaşamaz."

İptali istenilen 57/2. madde hükmünün 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuat bakımından sağlanan hakları ve getirilen uygulamaları engeller nitelikte olduğundan üst hukuk normlarına aykırı olduğu, kanunun kişinin açık rızası halinde genel hükümler çerçevesinde verilerin işleneceği ve paylaşılacağı öngörüldüğünden, Yönetmeliğin Kanuna ve rekabet ortamının tesis edilmesi amacına aykırı olduğu ileri sürülmekte ise de; sözleşmeyle aksi belirtilmediği takdirde tüketicinin bilgilerinin başka tedarikçiler ile paylaşılacağı ve başka bir amaç için kullanılmayacağı yolundaki hüküm kişisel verilerin korunması ve gizliliğin sağlanması amacına yönelik ve tüketicinin hukuken korunması gereken bir menfaati olduğundan hukuka aykırılık bulunmamaktadır.

Yönetmeliğin 58. maddesinde; İkili anlaşmayla veya müstakil bir yetki sözleşmesiyle, mahkemelerin ve icra dairelerinin yetkisi tüketicinin hak arama özgürlüğünü ve savunma hakkını kullanmasını güçleştirecek şekilde belirlenemeyeceği ve Hukuk Muhakemeleri Kanunu ile İcra ve İflas Kanunu hükümlerince yetkili sayılan mahkemelerin ve icra dairelerinin yetkisinin kaldırılamayacağı yolundaki kural; ikili anlaşmalarla yada ayrıca yapılacak sözleşme ile tüketicinin yetkili kılınmış mahkemeler ve icra daireleri önünde hak arama özgürlüğünü ya da savunma hakkına engelleyecek, kısıtlayacak yada zora sokacak şekilde mahkemelere ilişkin yetki sözleşmesi yapılamayacağı ve kanunlarla belirlenen yetkilerin kaldırılamayacağı hüküm altına alınmış ve tarafların sözleşme hürriyeti engellenmemiş olduğundan hukuka aykırılık görülmemiştir.

Yönetmeliğin 62. maddesindeki, yürürlük hükümlerinde de hukuk kurallarına aykırılık görülmemiştir.

Açıklanan nedenlerle dava konusu edilen Yönetmelik maddesi hükümlerinde üst hukuk normlarına ve hukuka aykırılık görülmediğinden davanın reddine karar verilmesi gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay Onüçüncü Dairesince duruşma için taraflara önceden bildirilen 22/12/2020 tarihinde, davacı vekili Av. ...'un ve davalı idare vekilleri Av. ... ile Av. ...'ın geldiği, Danıştay Savcısının hazır olduğu görülmekle, açık duruşmaya başlandı. Taraflara usulüne uygun olarak söz verilerek dinlendikten ve Danıştay Savcısının düşüncesi alındıktan sonra taraflara son kez söz verilip, duruşma tamamlandı. Tetkik Hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereği görüldü:

MADDİ OLAY VE HUKUKİ SÜREÇ:

30/05/2018 tarih ve 30436 sayılı Resmî Gazete'de serbest, serbest olmayan ve son kaynak tedariki kapsamındaki tüketicilere elektrik enerjisi ve/veya kapasite satışı ile buna ilişkin hizmetlerin sunulmasında tüketici, tedarikçiler ve/veya dağıtım şirketleri arasındaki iş ve işlemlere esas asgari standart, usul ve esasların belirlenmesi amacıyla tüketicilere hizmetlerin yeterli, kaliteli ve sürekli olarak sunulması için; (a) Tedarikçiler ile tüketimi düşük serbest tüketiciler arasında yapılacak ikili anlaşmada yer alacak asgari usul ve esaslara, (b) Görevli tedarik şirketleri ile serbest olmayan tüketiciler ya da son kaynak tedariki kapsamındaki tüketiciler arasında yapılacak perakende satış sözleşmesinde yer alacak asgari usul ve esaslara, (c) Dağıtım şirketleri ile tüketiciler ve tedarikçiler arasında; (1) Savaş ve sayaca erişim, okunmasına ve kontrolüne, (2) Kaçak ve usulsüz elektrik enerjisi kullanımının tespiti ve bu kapsamda yapılacak iş ve işlemlere, (3) Elektriğin kesilmesi ve bağlanmasına, (ç) Tüketici şikâyetlerinin yapılması, bu şikâyetlerin değerlendirilmesi ve sonuçlandırılması ile tüketicilerin bilgilendirilmesine yönelik usul ve esaslara, (d) Tüketicilerin hak ve yükümlülüklerine ilişkin hükümleri kapsamak üzere Elektrik Piyasası Tüketici Hizmetleri Yönetmeliği yayımlanmıştır.

Davacı şirket tarafından, Yönetmeliğin 4. maddesinin (y) bendinin, 58., 62., 13., 14., 15., 16., 18., 20., 9., ve 10. maddelerinin tamamının, 35. maddesinin ikinci, üçüncü ve dördüncü fıkralarının, 35. maddesinin beşinci fıkrasının (a) bendinin 1 ve 2 numaralı alt bentlerinin, 12. maddesinin birinci fıkrasının, 37. maddenin sekizinci fıkrasının ve 57. maddesinin ikinci fıkrasının iptali istemiyle bakılan dava açılmıştır.

İNCELEME VE GEREKÇE:

USUL YÖNÜNDEN:

Davalı idarenin usûle ilişkin itirazı geçerli görülmeyle esasın incelenmesine geçildi.

ESAS YÖNÜNDEN:

İLGİLİ MEVZUAT:

4628 sayılı Enerji Piyasası Düzenleme Kurumu'nun Teşkilat ve Görevleri Hakkında Kanun'un 4. maddesinde, "Kurum, tüzel kişilerin yetkili oldukları faaliyetleri ve bu faaliyetlerden kaynaklanan hak ve yükümlülüklerini tanımlayan Kurul onaylı lisansların verilmesinden, işletme hakkı devri kapsamındaki mevcut sözleşmelerin bu Kanun hükümlerine göre düzenlenmesinden, piyasa performansının izlenmesinden, performans standartlarının ve dağıtım ve müşteri hizmetleri yönetmeliklerinin oluşturulmasından, tadilinden ve uygulattırılmasından, denetlenmesinden, bu Kanunda yer alan fiyatlandırma esaslarını tespit etmekten, piyasa ihtiyaçlarını dikkate alarak serbest olmayan tüketicilere yapılan elektrik satışında uygulanacak fiyatlandırma esaslarını tespit etmekten ve bu fiyatlarda enflasyon nedeniyle ihtiyaç duyulacak ayarlamalara ilişkin formülleri uygulamaktan ve bunların denetlenmesinden ve piyasada bu Kanuna uygun şekilde davranılmasını sağlamaktan sorumludur." kuralına yer verilmiş; 5. maddesinin altıncı fıkrasının (c) bendinde, "Tüketicilere güvenilir, kaliteli, kesintisiz ve düşük maliyetli elektrik enerjisi hizmeti verilmesini teminen gerekli düzenlemeleri yapmak."; 7. fıkrasının (a) bendinde ise, "Bu Kanun hükümlerinin uygulanması ve bu Kanunla kendisine verilen görevleri yerine getirmek için gerekli olan ve piyasada rekabeti geliştirmeye yönelik olarak gerçek ve tüzel kişilerin uymaları gereken, talimatları ve tebliğleri, şebeke yönetmeliğini, dağıtım yönetmeliğini, müşteri hizmetleri yönetmeliğini ve dengeleme ve uzlaştırma yönetmeliğini onaylamak" Kurulun yetkileri arasında sayılmış; 9. maddesinin 2. fıkrasının (a) bendi ile de, "Bu Kanun ve diğer kanunlarla Kuruma verilen elektrik piyasası ile ilgili düzenleme, rekabet şartlarını oluşturma, tüketici haklarının korunması ile tüketici şikâyetlerinin incelenmesi çalışmalarını yapmak...." görevi Elektrik Piyasası Dairesi Başkanlığına verilmiştir.

6446 sayılı Elektrik Piyasası Kanununun "Amaç" başlıklı 1. maddesinde, "Bu Kanunun amacı; elektriğin yeterli, kaliteli, sürekli, düşük maliyetli ve çevreyle uyumlu bir şekilde tüketicilerin kullanımına sunulması için, rekabet ortamında özel hukuk hükümlerine göre faaliyet gösteren, mali açıdan güçlü, istikrarlı ve şeffaf bir elektrik enerjisi piyasasının oluşturulması ve bu piyasada bağımsız bir düzenleme ve denetimin yapılmasının sağlanmasıdır." kuralı yer almış; 3. maddesinin birinci fıkrasının (j) bendinde, "Gerçek veya tüzel kişiler arasında özel hukuk hükümlerine tabi olarak, elektrik enerjisi ve/veya kapasitesinin alınıp satılmasına dair yapılan ve Kurul onayına tabi olmayan ticari anlaşmalar" "İkili anlaşma" olarak tanımlanmış; 4. maddesinin 2. fıkrasında, piyasada faaliyet gösterecek tüzel kişilerin faaliyetlerinde uymaları gereken usul ve esasların yönetmelikle

düzenleneceği ifade edilmiş, 10. maddesinin birinci fıkrasında ise, toptan ve perakende satış faaliyetlerinin, üretim şirketleri ile tedarik lisansı kapsamında kamu ve özel sektör tedarik şirketleri tarafından, bu Kanun ve bu Kanuna göre çıkarılan yönetmelikler uyarınca yürütüleceği kurala bağlanmıştır.

HUKUKİ DEĞERLENDİRME:

Sözlük anlamı ile "düzenli hâle koymak, düzen vermek, tanzim ve tertip etmek" olarak tanımlanan "düzenleme", kamu hukukunda kural koyma ile eş anlamlıdır. Kural ise; sürekli, soyut, nesnel, genel (kişilik dışı) durumları belirleyen ve gösteren norm olarak tanımlanmaktadır. (ÖZAY İL Han, Günışığında Yönetim, 2017, İstanbul, s. 426). Yasama organının yasama tasarrufları dışında, idare, Anayasa ve kanunlardan aldığı yetki ile, kural koyma (düzenleme yapma) yetkisine sahiptir. "Kural işlemler" (ya da diğer adıyla genel düzenleyici işlemler), üst hukuk kurallarına uygun olarak hukuk düzenine yeni kural getiren ya da mevcut bir kuralı değiştiren veya kaldıran tek yanlı idarî işlemlerdir. Düzenleme yetkisini kullanarak tüzük, yönetmelik, tebliğ, genelge gibi genel düzenleyici işlemleri yapan idarenin bir işleminin düzenleyici nitelik taşıdığı kabul edilebilmesi için, söz konusu işlemin sürekli, soyut, nesnel, genel durumları belirleyen ve gösteren hükümler içermesi, başka bir anlatımla, belirtilen nitelikte kurallar konulmuş olması zorunlu olup, bu genel düzenlemelerin üst hukuk kurallarına aykırı hükümler içermemesi gerekir.

Düzenleyici kurumlar, ilgili buldukları piyasada düzenleme ve denetleme görevi üstlenmekte olup, bu kuruluşların temel işlevi, toplumsal ve ekonomik hayatın temel hak ve özgürlükler ile yakından ilişkili alanlarındaki kamusal ve özel kesim etkinliklerini, birtakım kurallar koyarak düzenlemek, konulan kurallara uyulup uyulmadığını izlemek ve denetlemektir. Elektrik piyasası ile ilgili olarak düzenlemeler yapma yetkisine sahip olan davalı Kurumun, 4628 sayılı Kanun ve 6446 sayılı Kanun ile kendisine tanınan bu yetkiyi dava konusu kuralları yürürlüğe koymak suretiyle kullandığı görülmektedir.

Elektriğin yeterli, kaliteli, sürekli, düşük maliyetli ve çevreyle uyumlu bir şekilde tüketicilerin kullanımına sunulması için, rekabet ortamında özel hukuk hükümlerine göre faaliyet gösteren, malî açıdan güçlü, istikrarlı ve şeffaf bir elektrik enerjisi piyasasının oluşturulmasında düzenleme ve denetleme yapmakla görevli Kurum, piyasa aktörlerinin eylemlerini gözetleme ve bundan hareketle tedbir alma konusunda görevlidir.

Elektrik piyasasında serbest olmayan tüketiciler, elektrik enerjisi ve/veya kapasite alımlarını davalı idare tarafından belirlenen tarifeler üzerinden sadece bölgesinde bulunduğu görevli tedarik şirketinden yapabilirler. Görevli tedarik şirketleri de, serbest olmayan tüketicilere elektrik tedarik

etmek zorundadır. Söz konusu tüketiciler elektrik alabilmek için, bölgelerindeki görevli tedarik şirketi ile Kurul onayına tabi perakende satış sözleşmesi imzalamak zorundadır.

Serbest tüketiciler ise, istedikleri tedarik şirketi ile mali hükümleri ve içeriği karşılıklı belirlenebilecek ikili anlaşma imzalamak suretiyle elektrik enerjisi alabilirler. İkili anlaşmalar 6446 sayılı Kanunda tanımlanmış gibi Kurum onayına tabi olmayan anlaşmalardır. Ancak bu ikili anlaşmalar tüketicilerle tek tek müzakere edilmek suretiyle karşılıklı olarak şartları kararlaştırılmayıp, aksine tedarikçi tarafından önceden tek taraflı olarak düzenlenip tüketicilere imzalatılmakta ve bu anlaşma hükümlerine göre piyasa işleyerek şekillenmektedir. Kuruma tüketici ve tedarikçiler tarafından yapılan şikâyet ve bilgi edinme başvuruları üzerine yapılan inceleme ve araştırmalarda ikili anlaşmaların tüketici aleyhine şekillenerek mağduriyete yol açtığından bahisle konuyla ilgili tedbirlerin alınması ihtiyacı doğduğu anlaşıldığından dava konusu Yönetmeliğin yürürlüğe konduğu görülmektedir.

Yönetmelik, serbest, serbest olmayan ve son kaynak tedariki kapsamındaki tüketicilere elektrik enerjisi ve kapasite satışı ile buna ilişkin hizmetlerin sunulmasında tüketici, tedarikçiler ve dağıtım şirketleri arasındaki iş ve işlemlere esas asgarî standartlar ile usûl ve esasların belirlenmesine yönelik olup, elektrik piyasasında, tedarikçiler ile tüketimi düşük serbest tüketiciler arasında yapılacak ikili anlaşmada yer alacak asgari usul ve esaslarla, görevli tedarik şirketleri ile serbest olmayan tüketiciler ya da son kaynak tedariki kapsamındaki tüketiciler arasında yapılacak perakende satış sözleşmesinde yer alacak asgari usul ve esasları ve dağıtım şirketleri ile tüketiciler ve tedarikçiler arasında yapılacak bazı iş ve işlemlere ilişkin kuralları kapsamaktadır.

Yönetmeliğin 4. maddesinin 1. fıkrasının (y) bendinde, "Tüketimi düşük serbest tüketici", "Yıllık elektrik enerjisi tüketimi 100.000 kWh'tan düşük olan serbest tüketici" şeklinde tanımlanmış; 9. maddesinde, "Bu bölümde yer alan ikili anlaşmaya ilişkin usul ve esaslar, tüketimi düşük serbest tüketicilerle tedarikçiler arasında yapılan ikili anlaşmaları kapsar." kuralına; 10. maddesinde ise, (1) Tedarikçiler tüketimi düşük serbest tüketicilere belirli süreli ya da belirsiz süreli ikili anlaşma önerebilir.

(2) Belirli süreli ikili anlaşmaların süresi üç yıldan fazla olamaz.

(3) İkili anlaşma ve ekleri ile Tüketici Hakları Bilgilendirme Formu (EK-1), İkili Anlaşma Ön Bilgilendirme Formu (EK-2-A) ve İkili Anlaşma Değişiklik Bildirimi (EK-3) en az on iki punto büyüklüğünde, anlaşılabilir bir dilde, açık, sade ve okunabilir bir şekilde düzenlenir.

(4) Tedarikçinin ikili anlaşmanın kurulmasına, yenilenmesine ve ikili anlaşmada değişiklik yapılmasına ilişkin önerisi karşısında tüketicinin susması veya açıkça reddetmemesi önerinin kabulü olarak yorumlanamaz ve aksi hükme ikili anlaşmada yer verilemez" kuralına; 12/1. maddesinde de, "Tedarikçi ikili anlaşma kurulmadan önce EK-1 ve EK-2'de yer alan standart formlarla açık ve anlaşılabilir bir şekilde kayıt altına almak suretiyle kâğıt üzerinde veya kalıcı veri saklayıcısı ile tüketiciyi bilgilendirmek ve tüketicinin söz konusu bilgileri edindiğini teyit etmesini sağlamak zorundadır. Söz konusu bilgilendirmenin yapıldığına ve tüketici tarafından teyit edildiğine ilişkin ispat yükü tedarikçiye aittir. Bilgilendirmenin gereği gibi ya da hiç yapılmamış olması tüketici için haklı fesih sebebidir." kuralına yer verilmiştir.

Yönetmeliğe göre, elektrik enerjisini satın alacağı tedarikçiyi seçme hakkına sahip olan serbest tüketicilerden, yıllık elektrik enerjisi tüketimi 100.000 kWh'dan düşük olanlar "tüketimi düşük serbest tüketici" şeklinde tanımlanmakta ve bunların tedarikçisi ile yapacağı ikili anlaşmaların bu yönetmelikte belirlenen usûl ve esaslara uygun olması öngörülmekte, diğer serbest tüketicilerin ikili anlaşmalarının Yönetmelik kapsamına alınmasına zorunluluk getirilmemektedir. Burada hedeflenenin, tedarikçilerin tüketimi düşük serbest tüketicilerle yapılan ikili anlaşmalarda Yönetmelikle öngörülen kurallara riayet etmelerine zorunluluk getirerek bu tür tüketicilere hukuki güvenlik sağlamak ve tedarikçilerin anlaşma öncesi bazı yükümlülüklerini yerine getirmelerini sağlayarak tüketici aleyhine oluşabilecek ve piyasa düzenini bozacak aksamaların önüne geçilmesi olduğu görülmektedir. Mesken, tarımsal sulama, küçük ticarethane ve sanayi grubu tüketicilerin tedarikçiler ile denk hukukî ve teknik bilgi gücüne sahip olması düşünülmemeyeceğinden, tedarikçiler tarafından standart veya genel işlem koşulu içerecek şekilde düzenlenen ikili anlaşmalarda öngörülen haksız şart ve tüketici aleyhine uygulanan muğlak ifadeler nedeniyle oluşan tüketici mağduriyetinin önüne geçmek düşüncesiyle, tüketimi düşük serbest tüketici ile yapılacak ikili anlaşmaların asgari standardının belirlenmesindeki asıl amacın; ikili anlaşmaların kurulması öncesinde tüketiciyi bilgilendirme yükümlülüğünün gereği gibi yerine getirilmemesi, belirli süreli ikili anlaşmaların süresi sonunda sona ermesinin ikili anlaşma hükümleri ile zorlaştırılması ve engellenmesi, tüketicinin bilgisi ve iradesi dışında anlaşma hükümlerinde değişiklik yapılması, fesih hâllerinde tüketiciden yüksek tutarlarda ceza koşulu istenilmesi ve bütün bunların sonucunda perakende elektrik piyasasının etkin ve verimli şekilde işleyişine zarar verilmesi, diğer tedarikçiler aleyhine piyasayı kapama ve haksız rekabete sebep olma gibi birtakım olumsuzlukları önlemek olduğu anlaşılmaktadır. Davalı idarenin düzenleme yetkisi ve piyasa koşulları dikkate alındığında, genelde tedarikçilerin kurduğu anlaşma modelinin tüketicinin aleyhine olduğu ve adeta bu anlaşmaya

hapsolunduđu, bu nedenle tüketimi belli bir seviyenin altında kalan piyasa tüketicilerinin yapacağı ikili anlaşmalarda asgari bir standardın getirilmesinde hukuka aykırılık bulunmamaktadır.

İkili anlaşmanın kurulması sırasında tüketimi düşük tüketicinin iradesinin zaafa uğratılmaması açısından susması ya da açıkça reddetmemesinin kabul anlamına gelmediđi, açık irade beyanı ile anlaşmanın kurulması zorunluluđu da tüketiciyi koruma amacına yönelik olduğundan sözleşme serbestisini kısıtlayan bir husus olarak görülmemiştir.

Diđer taraftan, belirli süreli ikili anlaşmaların en fazla 3 yıl ile sınırlandırılmasının ve tedarikçiye getirilen tüketiciyi bilgilendirme ve bunu ispatlama yükümlülüğünün tek taraflı olarak tedarikçi aleyhine aşırı yük getirdiđi düşünölmeyeceđi gibi, sözleşme hürriyeti ve düzenleyici işlemlerin ölçölülüđu ilkesine de aykırılık görülmemiştir.

Yönetmeliğin "Cayma hakkı" başlıklı 13. maddesinde, "Tüketimi düşük serbest tüketici, ikili anlaşmanın kurulduđu ya da yenilendiđi tarihten itibaren 14 gün içerisinde herhangi bir gerekçe göstermeksizin ve cayma bedeli ödemeksizin telefonla, e-postayla veya yazılı olarak bildirim yapmak suretiyle anlaşmadan cayma hakkına sahiptir." kuralı yer almaktadır.

Düzenleme ile ikili anlaşmanın kurulmasından ya da yenilenmesinden itibaren ceza koşulu ödemeksizin kullanılan cayma hakkı 14 gün ile sınırlandırılmış ve bildirim yükümlülüğünün yazılı yapılabileceđi gibi telefon veya e-postayla da yapılabileceđi belirtilerek kolaylık imkânı sağlanmıştır. Tedarikçi tarafından tüketiciyeye fiziken elektrik tesliminde bulunulmadan, yani tüketicinin tedarikçiden hiç elektrik almadan ikili anlaşmadan cayabileceđi öngörüldüğünden tedarikçinin bir zarara uğraması da söz konusu olmadığı gibi, tüketicinin haklarını olumsuz yönde etkileyen uygulamaların engellenmesi amaçlanarak, tüketicinin tedarikçi seçme hakkının ceza koşulu ödenmeksizin kullanılmasının önü açılmıştır. Tüketimi düşük serbest tüketiciyi koruma amaçlı getirilen düzenlemede sözleşme serbestine ve hukuka aykırılık görülmemiştir.

Öte yandan, Yönetmelik maddesi ile tedarikçinin Kanunlardan doğan cayma hakkına dokunulmadığı gibi, mülga Ticaret Kanunu'ndaki kuralın aksine Türk Ticaret Kanunu'nun 18. maddesinde tacirler arasında bildirimlere ilişkin şekil kurallarının geçerlilik şartı olmadığı göz önüne alındığında, tacirlerin cayma hakkını tek taraflı ve telefonla kullanması imkânının getirilmesinin, sözleşmedeki taraf dengesini tüketimi düşük serbest tüketici tacir lehine bozduğu söylenemez.

Yönetmeliğin 14. maddesinde, belirli süreli ikili anlaşmanın süre sonunda kendiliğinden sona ereceđi ve otomatik yenilenmeyeceđi, sözleşmeye aksine hüküm konulamayacağı, tedarikçinin ikili anlaşmanın sona ereceđi tarihten en az 60 gün önce durumu tüketiciyeye bildirmek ve bunu kayıt altına

almak zorunda olduđu; 15. maddesinde de, ikili anlaşma hükümlerinde sözleşme süresince tüketici aleyhine değişiklik yapılamayacağı, tedarikçiye tek taraflı değişiklik yapma yetkisi veren hükmün sözleşmeye konulamayacağı, tedarikçinin değişiklik teklifinin kayıt altına alınarak iletilmesi ve tüketici tarafından kabulü hâlinde yürürlüğe girebileceği, buna ilişkin ispat yükünün tedarikçide olduğu, aksi hâlde değişikliğin yapılmamış sayılacağı düzenlemeleri yer almıştır.

Bir yıllık bir anlaşmanın hukuken belirlenen süre sonunda sona ermesi beklenirken tedarikçiler tarafından anlaşmanın sona ermesi için tüketicilerden 2-3 aylık süre öncesinden noter kanalıyla fesih bildiriminde bulunmalarının istendiği, aksi hâlde anlaşmanın aynı süre kadar ya da belirsiz süreli uzayacağına ilişkin anlaşmalarda düzenlemeler bulunduğu, öte yandan, tüketicilerin anlaşma fesih bildirimlerinin tedarikçiler tarafından dikkate alınmadığı, alınsa dahi tüketiciden yüksek tutarda ceza koşulu istendiği, dolayısıyla, anlaşmayı süresinde feshettiğini düşünen tüketicinin başka bir tedarikçiyle anlaşma yapıp sonraki faturasını yeni tedarikçiden almayı beklerken eski tedarikçinin anlaşmanın devam ettiğinden bahisle fatura düzenlemeye devam ettiği, yeni tedarikçinin de anlaşmaya aykırı davrandığı gerekçesiyle tüketiciden cayma bedeli ya da ceza koşulu istediği ya da yeni tedarikçinin yeni anlaşma kapsamında fatura düzenlemeye başladığı ve fakat eski tedarikçinin ceza koşulu istediği görüldüğünden, anılan maddelerin tüketimi düşük serbest tüketicinin açık iradesi ile Türk Ticaret Kanunu ve Tüketicinin Korunması Hakkında Kanun hükümlerine uygun olarak ikili anlaşmanın kurulması ve yenilenmesi amacına matuf olduğundan, Yönetmelik maddelerinin idarenin düzenleme yetkisi sınırları içinde olan ve ölçülülük ilkesini aşmayan kurallar olduğu görülmektedir.

İkili anlaşma hükümlerinde sözleşme süresince tüketici aleyhine değişiklik yapılamayacağı, tedarikçiye tek taraflı değişiklik yapma yetkisi veren hükmün sözleşmeye konulamayacağı, tedarikçinin değişiklik teklifinin tüketici tarafından kabulü hâlinde yürürlüğe girebileceği, buna ilişkin ispat yükünün tedarikçide olması hususları, sözleşmelerde irade serbestisi ilkesi ile çelişen bir husus olarak görülmemiştir.

Yönetmeliğin "haklı fesih sebepleri" başlıklı 16. maddesinde, tüketimi düşük serbest tüketici ya da tedarikçinin belirli süreli ikili anlaşmayı süresi sona ermeden önce maddede sayılanlarla sınırlı olmamakla birlikte maddede yer verilen haklı sebeplerden bir veya birkaçına dayanarak cayma bedeli ve/veya ceza koşulu ödemeksizin önceden bildirim yapmak suretiyle feshedebileceği kurala bağlanmıştır. Anılan madde ile, hem tüketimi düşük tüketiciler için hem de tedarikçiler için örnekseyici sayımla haklı nedenle fesih sebepleri gösterilmiştir. Davalı idarenin düzenleme yetkisi ve

piyasa kořulları dikkate alındığında, hakkaniyet ilkelerine de uygun olan düzenlemede hukuka aykırılık görölmemiřtir.

Yönetmeliğin "ikili anlaşma kapsamında yer alacak bedeller" başlıklı 18. maddesinde, "(1) İkili anlaşma kapsamında elektrik enerjisi ve kapasite satışına ilişkin aktif enerji bedeli ile tahsilatına aracı olunan ilgili mevzuat geređi uygulanan dağıtım sistem kullanım bedeli ve diđer mevzuat geređi fon, pay ve vergiler ile bunun dışında Kurulca onaylanmış ve tahsilinde aracı olunan bedeller de yer alır. Tahsilatına aracı olunan bu bedellerin neler olduđu ile bunların anlaşmanın düzenlendiđi tarihteki tutarı ve deđiřmesi durumunda yeni tutarların tüketiciye ne şekilde bildirileceđine ilişkin bilgiye ikili anlaşmada yer verilir. (EK-2-B)

(2) Tedarikçi ikili anlaşma kapsamında yapacađı elektrik enerjisi ve/veya kapasite satışı için tek ya da çok zamanlı dilimlerinde olmak üzere aktif enerji bedelini kr/kWh olarak fiyatlandırır. Fiyatlandırma yönteminde düzenlemeye tabi fiyatlarla mukayese edebilirlik esas alınır. " düzenlemeleri getirilmiřtir.

Genel olarak ikili anlaşmanın kurulması, yenilenmesi, sona ermesi, cayma ve fesih hakkı, anlaşmada deđiřiklik yapılması, anlaşmanın kapsamına, ceza kořuluna ve fatura düzenlenmesine, ikili anlaşma kapsamında yer alacak bedellerin belirlenmesine ve bildirimine ilişkin kurallara yer verilmesinin, ikili anlaşmanın kurulmasına müdahale, tarafların sözleşme iradesinin tecellisini engellenmesi ve bu konudaki üst hukuk normları ile Ticaret Kanunu ve Borçlar Kanunu hükümlerine aykırılık olduđu ileri sürölmekte ise de; idarenin kanunla verilen düzenleme yetkisinin sınırları içinde kalan ölçölülük ilkesine aykırılık teşkil etmeyen ve piyasada dengeyi sađlamak, tüketiciye birtakım kolaylıklar sunmak amacıyla yürürlüđe konan Yönetmeliğin bu maddelerinde hukuka aykırılık görölmemiřtir.

Yönetmeliğin 18. maddesinin 2. bendi açısından ise, tüketicinin gerçekten ucuza elektrik enerjisi alıp almadığını öđrenebilmesi ve ikili anlaşma önerisinde bulunan tedarikçinin fiyatını kabul edip etmeyeceđine karar verebilmesi tedarikçiler tarafından kendisine önerilen fiyatların karşılaştırılabilir olmasına bađlı olduđu açıktır. Tedarikçilerin fiyatlarının karşılaştırılabilmesi ise ancak aktif enerji bedelinin aynı ölçü ile fiyatlandırılması ile mümkündür. Aktif enerji bedelinin kr/kWh olarak fiyatlandırılmasına ilişkin kuralda, şeffaflık ilkesi uyarınca, tüketicinin aldıđı hizmetin bedelini net olarak görmesini sađlayacak olması dolayısıyla, hukuka aykırılık bulunmamaktadır.

Yönetmeliğin "Ceza kořulu/cayma bedeli" başlıklı 20. maddesinde, "(1)Belirli süreli ikili anlaşmada tedarikçi ya da tüketimi düşük serbest tüketici aleyhine ceza kořulu ancak haksız fesih işlemleri için kararlaştırılabilir. Haksız fesih, haklı bir sebebe dayanmaksızın yapılan fesihtir.

(2) 7/11/2013 tarihli ve 6502 sayılı Tüketicinin Korunması Hakkında Kanun ve ilgili ikincil mevzuat kapsamındaki tüketiciler hariç tüketimi düşük serbest tüketicinin ödeyeceği cayma bedeli ve/veya ceza koşulu cayma tarihi ya da fesih tarihi öncesi tüketicinin son 12 aylık tüketim toplamı ile cayma tarihinde ya da fesih tarihinde uygulanan fiyat esas alınarak hesaplanan toplam tutarın % 10'unu geçemez.

(3) Tedarikçi tarafından anlaşmanın haksız feshedilmesi durumunda tedarikçi tüketimi düşük serbest tüketiciye ikinci fıkra kapsamında belirlenen tutarda ceza koşulu öder." kuralı yer almaktadır.

Yönetmeliğin 16. maddesinde, tedarikçi ve tüketimi düşük serbest tüketici bakımından haklı fesih nedenlerine yer verilmiş, yine aynı maddede sayılan fesih hâllerinin sınırlı sayıda olmadığı ifade edilmiştir. 16. maddede sayılan hâllerde yani haklı fesih hâllerinde tüketicinin cayma bedeli ödemesi söz konusu değildir. Yönetmelikte haksız fesih hâllerinin neler olduğuna ilişkin bir düzenlemeye ise yer verilmemiş, iptali istenen madde uyarınca haksız fesih, haklı bir sebebe dayanmaksızın yapılan fesih olarak nitelendirilmiştir. Bu durumda, ceza koşulunun ancak haksız fesih işlemleri için kararlaştırılabileceğine ilişkin düzenlemede, idarenin bu konudaki piyasayı düzenleme yetkisinin ölçülülük ilkesi çerçevesinde kullanıldığı dikkate alındığında maddede üst hukuk kurallarına ve hukuka aykırılık görülmemiştir.

Yönetmeliğin "zamanında ödenmeyen borçlar" başlıklı 35. maddesinin 2. ve 3. fıkrası, 5. fıkrasının (a) bendinin birinci ve ikinci paragrafı ile "sayacın doğru tüketim kaydetmemesi hâlinde tüketim miktarının tespiti" başlıklı 37. maddesinin sekizinci fıkrasında yer verilen "(8) Bu madde kapsamında hesaplamalara ilişkin EK-7'de yer alan form düzenlenir ve EK-7 formu ilgili tedarik şirketi tarafından ödeme bildirim/fatura ile birlikte ya da ödeme bildirim/fatura gönderilmeden önce tüketiciye gönderilir. Ayrıca kalıcı veri saklayıcısı ile de tüketiciler bilgilendirilir." kuralı açısından yapılan incelemede,

Yönetmeliğin 35. maddesinde, perakende satış sözleşmesi kapsamında zamanında ödenmeyen borçlarla ilgili düzenlemelere yer verilmiştir. Buna göre, tüketici elektrik enerjisi tüketimine ilişkin ödemeleri faturada belirtilen son ödeme tarihine kadar yapmazsa görevli tedarik şirketi tüketiciye ikinci bildirimde bulunacak, bu bildirimde hem tüketiciye borcunu ödemesi için en az 5 iş günü ödeme süresi tanınacak, hem de bu süre içinde borcunu ödemezse elektriğin kesileceği bildirilecektir. Tüketici bu süre içinde de borcunu ödemezse görevli tedarik şirketinin bölgedeki dağıtım şirketine tüketicinin elektriğini kesmesini bildirmesinin ardından, bildirim tarihinden itibaren en geç 5 iş günü içinde tüketicinin elektriği dağıtım şirketince kesilecektir. Bundan önceki mülga Yönetmelikte de bu hususa ilişkin olarak benzer kurallara yer verilmiş ve yazılı bildirim yanı sıra tüketiciye ayrıca e-

posta, kısa mesaj gibi diğ er haberleřme kanallarıyla bildirimde bulunulması g revli tedarik řirketinin takdirine bırakılmıř iken, dava konu Y netmelik ile m lga Y netmelikten farklı olarak ikinci bildirim hem yazılı hem de kalıcı veri saklayıcılarından (e-posta, kısa mesaj) en az birisi ile g nderilmesi kořulu getirilmiř, bu kurala uymaksızın kalıcı veri saklayıcı ile bildirimde bulunulmayan yerlerin elektriğinin kesilemeyeceđi de d zenlenmiřtir.

Y netmeliğın 4. maddesinde, kalıcı veri saklayıcısı, "T keticinin g nderdiđi veya kendisine g nderilen bilgiyi, bu bilginin amacına uygun olarak incelemesine elverecek řekilde kaydedilmesini ve deđiřtirilmeden kopyalanmasını sađlayan ve bu bilgiye aynen ulařılmasına imk n veren kısa mesaj, elektronik posta, internet, disk, CD, DVD, hafıza kartı ve benzeri her t rl  ara veya ortamı" řeklinde tanımlanmıřtır. Elektriğın kesilmesinin perakende satıř s zleřmesine taraf olan mesken, ticarethane, sanayi, tarımsal sulama, aydınlatma t keticisi grubundaki t m t keticilerin hem g nl k hem de ticari hayatını b y k  lde etkileyeceđi dikkate alındıđında, elektriğın kesilmesinden  nceki ikinci bildirimden t keticinin zamanında haberdar edilmesi b y k  nem arz etmektedir. Dolayısıyla, t keticisi Őik yetleri de g z  n nde bulundurulduđunda yazılı bildirimle birlikte g nl k kullanımda yaygın olan ve t keticisiye ulařması y n nden daha garanti e-posta, kısa mesaj yoluyla da bildirim yapılmasında piyasa aısından kamu yararı bulunduđu aıktır.

T keticinin GSM numarasının ya da e-posta adresinin g revli tedarik řirketine beyan edilmemesi, perakende satıř s zleřmesinin kurulmasına engel oluřturmadıđından, g revli tedarik řirketinin bildirimine rađmen, bildirimlerin yapılacađı GSM numarasının ya da e-posta adresinin bulunmadıđını beyan eden t keticilerin  denmeyen borcu nedeniyle elektriğinin kesilmesine Y netmelik kapsamında bir engel bulunmamaktadır. Zira, dađıtım řirketlerinin t m uyarılara rađmen bu iletiřim aralarına iliřkin bilgileri paylařılmadıđından bahisle t keticisiye bu bildirim yapılmasının imk nsız olduđu durumlarda, kalıcı veri saklayıcılarıyla t keticisiye bildirim yapılması zorunluluđunun ortadan kalkacađı aıktır.

Y netmeliğın 57. maddesinin 2. fıkrasında, "(2) Tedariki, t keticisiye ait bilgileri bařka bir amala kendisinin iliřkide bulunduđu faaliyetlerde kullanamaz, aksi belirtilmemiř hususlar dıřında diğ er tedarikilerle paylařamaz." kuralına yer verilmiřtir.

Y netmeliğın 57/2. maddesinin, 6698 sayılı Kiřisel Verilerin Korunması Kanunu ve ilgili mevzuat bakımından sađlanan hakları ve getirilen uygulamaları engeller nitelikte olduđundan  st hukuk normlarına aykırı olduđu, kanunda kiřinin aık rızası h linde genel h k mler erevesinde verilerin iřleneceđi ve paylařılacađı  ng r ld đ nden, Y netmeliğın Kanuna ve rekabet ortamının tesis edilmesi amacına aykırı olduđu ileri s r lmekte ise de, t keticinin bilgilerinin bařka tedarikiler ile

paylaşamayacağı ve başka bir amaç için kullanılmayacağı yolundaki kuralın kişisel verilerin korunması ve gizliliğin sağlanması amacına yönelik olduğu ve tüketicinin hukuken korunması gereken bir menfaati bulunduğundan anılan kuralda hukuka aykırılık bulunmamaktadır.

"İkili anlaşma uyuşmazlıklarında yetkili çözüm mercii" başlıklı Yönetmeliğin 58. maddesinde, ikili anlaşma veya müstakil bir yetki sözleşmesiyle, mahkemelerin ve icra dairelerinin yetkisinin tüketicinin hak arama özgürlüğünü ve savunma hakkını kullanmasını güçleştirecek şekilde belirlenemeyeceği ve Hukuk Muhakemeleri Kanunu ile İcra ve İflas Kanunu hükümlerince yetkili sayılan mahkemelerin ve icra dairelerinin yetkisinin kaldırılamayacağı kurala bağlanmıştır. İdarenin kanunla verilen düzenleme yetkisinin sınırları içinde kalan, ölçülülük ilkesine aykırılık teşkil etmeyen ve piyasada dengeyi sağlamak, tüketiciye birtakım kolaylıklar sunmak amacıyla yürürlüğe konan Yönetmeliğin bu maddesinde hukuka aykırılık görülmemiştir.

Yönetmeliğin "Yürürlük" başlıklı" 62. maddesinde "(1) Bu Yönetmeliğin Üçüncü Bölüm ve Altıncı Bölüm hükümleri 1/7/2018 tarihinde, diğer hükümleri yayımı tarihinde yürürlüğe girer." kuralına yer verilmiştir. Yürürlük maddesi ile, tüketimi düşük serbest tüketicilerle tedarikçiler arasında yapılan ikili anlaşmalara ilişkin kurallara yer verilen Yönetmeliğin Üçüncü Bölümü ile, "Tedarikçi ve Tüketicilerin Hak ve Yükümlülükleri, Serbest Tüketici Limitinin Belirlenmesi" başlıklı Yönetmeliğin Altıncı Bölümü'nün 01/07/2018 tarihinde, diğer maddelerin ise 30/05/2018 olan Yönetmeliğin yayımı tarihinde yürürlüğe gireceği kurala bağlanmıştır. Yönetmelik ile ilk defa kurala bağlanan düzenleme alanları için yaklaşık bir ay süre verilmesinde hukuka aykırılık görülmemiştir.

Bu itibarla, Yönetmeliğin dava konusu 4. maddesinin (y) bendinde, 58., 62., 13., 14., 15., 16., 18., 20., 9., ve 10. maddelerinde, 35. maddesinin ikinci, üçüncü ve dördüncü fıkralarında, 35. maddesinin beşinci fıkrasının (a) bendinin 1 ve 2 numaralı alt bentlerinde, 12. maddesinin birinci fıkrasında, 37. maddenin sekizinci fıkrası ile 57. maddesinin ikinci fıkrasında hukuka aykırılık bulunmamaktadır.

KARAR SONUCU:

Açıklanan nedenlerle;

1. DAVANIN REDDİNE,
2. Ayrıntısı aşağıda gösterilen toplam ...-TL yargılama giderinin davacı üzerinde bırakılmasına,
3. Avukatlık Asgari Ücret Tarifesi uyarınca ...-TL vekâlet ücretinin davacıdan alınarak davalı idareye verilmesine,
4. Posta gideri avansından artan tutarın kararın kesinleşmesinden sonra davacıya iadesine,

5. Bu kararın tebliğ tarihini izleyen 30 (otuz) gün içerisinde Danıştay İdari Dava Daireleri Kurulu'na temyiz yolu açık olmak üzere, 22/12/2020 tarihinde oybirliğiyle karar verildi.

Danıştay Kararı - 15. Daire (E. 2018/844)

Danıştay Kararı - 15. D., E. 2018/844 K. YD T. 14.3.2018

Bakanlığın Anayasanın 20. maddesi ve 6698 sayılı Kanununun 6/3. maddesi hükümleri gereği kişisel sağlık verilerini merkezi sağlık veri sistemine zaten aktarabildikleri, 6698 sayılı Kanun m. 6/III hükümlerinin Anayasaya ve uluslararası Sözleşmelere aykırılığı iddiası hakkında: Anayasa'nın 20 nci maddesinin üçüncü fıkrasında; "Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usûller kanunla düzenlenir." hükmünün bulunduğu, dolayısıyla Anayasa'da konuya ilişkin olarak iki şart öngörüldüğü ve bu şartlardan herhangi birinin sağlandığı durumlarda kişisel verilerin hukuka uygun bir şekilde işlenmiş olarak kabul edileceğinin hüküm altına alındığı, "Kanunda öngörülmüş olma" halinin, kişisel verilerin hukuka uygun olarak işlenebileceği iki şarttan biri olarak belirlendiği, 6698 sayılı Kanun'un 6. maddesinin üçüncü fıkrasında öngörülen "kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi sağlık hizmetleri ile finansmanının planlanması ve yönetimi" amaçları ile kişisel verilerin işlenmesinin, uluslararası sözleşme hükümlerine ve Anayasa'ya aykırılık teşkil etmediği, 108 sayılı Sözleşme'nin tarafı olan AB üyesi ülkelerin tamamında 1998 yılından itibaren geçerli olan 95/46 sayılı Direktifte de aynı amaçlarla kişisel verilerin işlenebileceğinin hüküm altına alındığı gibi, 2018 yılından itibaren geçerli olacak olan Genel Veri Koruma Tüzüğü'nde de aynı amaçlarla kişisel verilerin, ilgili kişilerin açık rızası olmaksızın işlenebileceği, yukarıda sayılan amaçların, doğrudan Anayasa'nın 20. maddesinde öngörülen kanun olan 6698 sayılı Kanun'da düzenlendiği, Anayasa uyarınca "kanunda öngörülmüş olma" halinin kişisel verilerin hukuka uygun olarak işlenebileceği hallerden olduğu için, bu amaçlarla kişisel verilerin işlenmesinde Anayasa'ya hiçbir aykırılık bulunmadığı, 6698 sayılı Kanun m. 6/IV uyarınca yeterli önlemlerin henüz belirlenmemiş olduğu iddiası hakkında: 6698 sayılı Kanun'un yürürlüğe girmiş olması ve 6. maddesinin dördüncü fıkrasında değinilen yeterli önlemlerin henüz belirlenmemiş olmasını, kişisel sağlık verilerinin tarafından işlenmemesi için ileri sürmenin izahtan varestede olduğu, bu iddianın doğruluğunu savunmanın, özel nitelikli kişisel verilerden olan kişisel sağlık verilerinin yalnızca tarafından değil, aynı zamanda hiçbir kişi (hekim), kurum ve kuruluş (özel ve kamu sağlık tesisleri) tarafından işlenmemesini de beraberinde getireceği, ki bunun da ülkemizdeki tüm sağlık hizmetlerinin durması anlamına geldiği, hatta dernek üyeliğinin de özel nitelikli kişisel veriler arasında zikredilmiş olması göz önünde bulundurulduğunda, davacı ile 'nin

kendi üyelerine ilişkin verileri işleyememesi, dernek üyesi olmaları gerekçesiyle üyelerine hiçbir iş ve işlemde bulunamayacağı, hiçbir şekilde iletişime geçemeyeceği ki bu durumun hayatın olağan akışına aykırı olduğu, nitekim, 6698 sayılı Kanun'un 6. maddesinin dördüncü fıkrasında öngörülen ve Kurul tarafından belirlenecek yeterli önlemlerin alınması şartının, yalnızca aynı maddenin üçüncü fıkrası uyarınca istisnai hallerde işlenen özel nitelikli kişisel veriler için değil, aynı zamanda açık rıza ile işlenen özel nitelikli kişisel veriler için de geçerli olduğu, Kanun hükmünün yalnızca nı değil, özel nitelikli kişisel veri işleyen tüm gerçek kişiler ile özel hukuk ve kamu hukuku tüzel kişilerini bağladığı, dolayısı ile özel nitelikli kişisel verilerin işlenmesinde gerekli olan yeterli önlemlerin Kurul tarafından henüz belirlenmemiş olması hususunu, kişisel sağlık verilerinin tarafından işlenememesi için bir gerekçe olarak sunmanın tutarlı hiçbir tarafı bulunmadığı, 6698 sayılı Kanun'un 7. maddesinin dördüncü fıkrası uyarınca özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınmasının şart olduğu, bu yeterli önlemlerin Kurul tarafından yayımlandığı anda bu şartın aranmaya başlayacağı, Kanun ve Yönetmeliğin 108 sayılı Sözleşmeye aykırılık iddiası hakkında: Türkiye'nin, Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne (108 sayılı Sözleşme), 28 Ocak 1981 tarihinde imza atmış olmasına rağmen, uzun bir süre Sözleşmeyi onaylanmadığı, Sözleşmenin nihayet 30.01.2016 tarihinde onaylandığı, 18.02.2016 tarihli ve 29628 sayılı Resmî Gazete'de yayımlandığı, 108 sayılı Sözleşmenin, 6669 sayılı Kanun'un 2. maddesi gereği, Resmî Gazete'de yayımlandığı gün olan 18.02.2016 tarihinde yürürlüğe girdiği, Anayasa'nın 90. maddesinin 5. fıkrasında; "Usulüne göre yürürlüğe konulmuş milletlerarası anlaşmalar kanun hükmündedir. Bunlar hakkında Anayasaya aykırılık iddiası ile Anayasa Mahkemesine başvurulamaz. (Ek cümle: 7/5/20045170/7 md.) Usûlüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası anlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası anlaşma hükümleri esas alınır." hükmünün bulunduğu, madde metninden, usulüne göre yürürlüğe konulan 108 sayılı Sözleşme ile 6698 sayılı Kanun'un, aynı konuda farklı hükümler içermesi halinde 108 sayılı Sözleşme hükümlerinin esas alınacağına anlaşıldığı, bununla birlikte usulüne göre yürürlüğe konulan milletlerarası anlaşmaların, Anayasa'ya üstünlüğünün bulunmadığı, bunlar hakkında Anayasa'ya aykırılık iddiası ile Anayasa Mahkemesine başvurulamamasının, bu anlaşmaların Anayasa'dan üstün olduğu anlamına gelmediği, Anayasa'nın 20. maddesinde ise kişisel verilerin hangi hallerde işlenebileceğinin açık bir şekilde hüküm altına alındığı, diğer taraftan 108 sayılı Sözleşme'nin 6. maddesinde "iç hukukta uygun güvenceler sağlanmadıkça otomatik işleme tabi tutulmalarının yasaklandığı" verilerin yalnızca kişisel sağlık verileri olmadığı, ceza mahkumiyetine ilişkin kişisel verilerin de madde metninde vurgulandığı, bununla birlikte Ulusal Yargı Ağı Projesi (UYAP)

kapsamında ceza mahkumiyetine ilişkin kişisel verilerin, uzun zamandır otomatik işleme tabi tutulduğu, dolayısı ile ülkemizin “iç hukukta uygun güvenceler sağlayamadığı” iddiasının doğru kabul edilmesi halinde, UYAP’ın da hukuki dayanaktan yoksun kalacağı. Ayrıca, 108 sayılı Sözleşme’nin 9. maddesinde, “Devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi” gibi durumların varlığı halinde, Sözleşmenin 5, 6 ve 8 inci maddelerine sınırlama getirilebileceği hükmünün yer aldığı, dolayısı ile 108 sayılı Sözleşme’nin 9 uncu maddesinin, aralarında “kamu güvenliği”nin de bulunduğu bir takım sebeplerin söz konusu olduğu durumlarda, 6. maddenin sınırlandırılabilceğini hüküm altına aldığı, bu yönüyle de 6698 sayılı Kanun ile Yönetmelik hükümlerinin, 108 sayılı Sözleşme ile uyumsuzluk arz etmediği, Amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırılık iddiası hakkında: Bakanlığın uygulama ve süreçlerinde, 6698 sayılı Kanun’un “Genel ilkeler” başlıklı 4. maddesinde belirtilen ilkelerin göz önünde bulundurulduğu ve bu ilkeleri ihlal edecek uygulamalardan kaçınıldığı, kişilerin sağlık verileri toplanmaksızın doğru sağlık politikaları oluşturmanın mümkün olmayacağı, büyük veri (big data) çağında bulunduğumuz günümüzün “petrolü”nün veri olduğu, gelişmiş ülkelerin çok büyük bütçeler ayırmalarına karşın başaramadıkları teknik alt yapının, Bakanlık tarafından emsallerine oranla çok daha küçük bütçelerle son derece başarılı bir şekilde hazırlandığı, bu teknik alt yapı ile son derece verimli analizler, istatistiksel çalışmalar yapıldığı, bu çalışmalarla kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi konularında emsalsiz faydalar sağlandığı, yalnızca Tip-II diyabetin ülkemize yıllık maliyetinin 15 milyar TL civarında olduğu göz önünde bulundurulduğunda, bu sistemlerin “devletin mali menfaatlerine” olan katkısının boyutunun da tartışılmayacak seviyede olduğu, tüm işlemlerin iz (log) kayıtlarının tutulduğu, yetkisiz erişimlerin her zaman görüntülenebildiği, toplanan verilerin USS’de anonim hale getirilerek tutulduğu, ancak ilgili kişinin e-Nabız profili oluşturması halinde kişi ile ilişkilendiriliği ve verilere yalnızca kişinin kendisi ile yetki verdiği üçüncü kişilerce erişilebildiği, sonuç olarak, ulusal ve uluslar arası düzenlemelerde öngörülen ilkelere riayet edildiği, Merkezi sağlık veri sistemi ile ilgili iddialar hakkında: Anayasa’nın 56. maddesinde “Devlet, herkesin hayatını, beden ve ruh sağlığı içinde sürdürmesini sağlamak; insan ve madde gücünde tasarruf ve verimi artırarak, işbirliğini gerçekleştirmek amacıyla sağlık kuruluşlarını tek elden planlayıp hizmet vermesini düzenler. Devlet, bu görevini kamu ve özel kesimlerdeki sağlık ve sosyal kurumlarından yararlanarak, onları denetleyerek yerine getirir.” hükmünün bulunduğu, 663 sayılı KHK’nın 2. maddesinin birinci fıkrası ile herkesin bedenî, zihnî ve sosyal bakımdan tam bir iyilik hâli içinde hayatını sürdürmesini sağlama görevinin, na verildiği, 663 sayılı KHK’nın 11. maddesinde “Kişisel sağlık verileri ile ülke düzeyinde

sağlık durumu ve sağlık hizmetlerine ilişkin veri ve bilgi akışını içeren her türden bilgi sistemleri ve projelerini yapmak ve yaptırmak” ve “Sağlık bilişimi ve teknolojisi alanında çalışacak kamu ve özel hukuk tüzel kişileri ile gerçek kişilerin uyacakları kuralları belirlemek, uygulamak, gerektiğinde bunların yazılım ve ürünlerinin uygunluğuna karar vermek ve müelliflerini yetkilendirmek” görevlerinin ise Sağlık Bilgi Sistemleri Genel Müdürlüğüne tevdi edildiği, 3359 sayılı Sağlık Hizmetleri Temel Kanunu’nun 3. maddesinin birinci fıkrasının (f) bendinde, yukarıdaki hükmü destekler nitelikteki “Herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi maksadıyla, ve bağlı kuruluşlarınca gerekli kayıt ve bildirim sistemi kurulur. Bu sistem, e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabilir. Bu amaçla, nca, bağlı kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemi kurulabilir.” hükmünün yer aldığı Anayasa’nın 125. maddesinde; “Yargı yetkisi, idarî eylem ve işlemlerin hukuka uygunluğunun denetimi ile sınırlı olup, hiçbir surette yerindelik denetimi şeklinde kullanılamaz. Yürütme görevinin kanunlarda gösterilen şekil ve esaslara uygun olarak yerine getirilmesini kısıtlayacak, idarî eylem ve işlem niteliğinde veya takdir yetkisini kaldırarak biçimde yargı kararı verilemez.” hükmünün bulunduğu, yukarıda anılan hükümler uyarınca Bakanlığın, merkezi sağlık veri sistemi olan USS ile bu sisteme bağlı olarak çalışan e-Nabız’ın oluşturulduğu, her iki sistem de temelini kanuni düzenlemelerden aldığı, Kamu kurumları arasında veri paylaşımının, Yönetmeliğin 8. maddesinin üçüncü fıkrası uyarınca Protokol ile yapıldığı, hukuki düzenlemelere aykırı olan durumlarda veri aktarımı yapılmadığı, Protokol ile veri aktarımının ancak veri aktarımının hukuka uygun olduğu hallerde yapıldığı, hukuka uygun olmayan veri aktarımı taleplerinin Bakanlıkça birçok kez reddedildiği, veri aktarımı taleplerinin değerlendirilmesinde, 6698 sayılı Kanun’un 8. maddesinin göz önünde bulundurulduğu,

T.C. DANIŞTAY ONBEŞİNCİ DAİRE

Esas No: 2018/844

Davacılar ve Yürütmenin Durdurulmasını İsteyenler: 1-

2-

Vekilleri:

Davalılar: 1-

Vekili:

2-

Vekili:

İstemin Özeti: 20.10.2016 tarihli ve 29863 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin, yetki unsuru yönünden tamamının, 4. maddesinin 1. fıkrasının (h), (n) ve (o) bentlerinin, 5. maddesinin 8. fıkrasının, 7. maddesinin 1. fıkrasının, 8. maddesinin 1. ve 3. fıkralarının, 9. maddesinin 1. fıkrasının, 11. maddesinin, 12. maddesinin ve 14. maddesinin 1. fıkrasının hukuka aykırı olmaları nedeniyle yürütmesinin durdurulması ve iptali istenilmektedir.

.....'nın Savunmasının Özeti: Bakanlığın Anayasanın 20. maddesi ve 6698 sayılı Kanunun 6/3. maddesi hükümleri gereği kişisel sağlık verilerini merkezi sağlık veri sistemine zaten aktarabildikleri, 6698 sayılı Kanun m. 6/III hükümlerinin Anayasaya ve uluslararası Sözleşmelere aykırılığı iddiası hakkında:

Anayasa'nın 20 nci maddesinin üçüncü fıkrasında;

"Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usûller kanunla düzenlenir." hükmünün bulunduğu, dolayısıyla Anayasa'da konuya ilişkin olarak iki şart öngörüldüğü ve bu şartlardan herhangi birinin sağlandığı durumlarda kişisel verilerin hukuka uygun bir şekilde işlenmiş olarak kabul edileceğinin hüküm altına alındığı, "Kanunda öngörülmüş olma" halinin, kişisel verilerin hukuka uygun olarak işlenebileceği iki şarttan biri olarak belirlendiği, 6698 sayılı Kanun'un 6. maddesinin üçüncü fıkrasında öngörülen "kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi sağlık hizmetleri ile finansmanının planlanması ve yönetimi" amaçları ile kişisel verilerin işlenmesinin, uluslararası sözleşme hükümlerine ve Anayasa'ya aykırılık teşkil etmediği, 108 sayılı Sözleşme'nin tarafı olan AB üyesi ülkelerin tamamında 1998 yılından itibaren geçerli olan 95/46 sayılı Direktifte de aynı amaçlarla kişisel verilerin işlenebileceğinin hüküm altına alındığı gibi, 2018 yılından itibaren geçerli olacak olan Genel Veri Koruma Tüzüğü'nde de aynı amaçlarla kişisel verilerin, ilgili kişilerin açık rızası olmaksızın işlenebileceği, yukarıda sayılan amaçların, doğrudan Anayasa'nın 20. maddesinde öngörülen kanun olan 6698 sayılı Kanun'da düzenlendiği, Anayasa uyarınca "kanunda öngörülmüş olma" halinin kişisel verilerin hukuka uygun olarak işlenebileceği hallerden olduğu için, bu amaçlarla kişisel verilerin işlenmesinde Anayasa'ya hiçbir aykırılık bulunmadığı,

6698 sayılı Kanun m. 6/IV uyarınca yeterli önlemlerin henüz belirlenmemiş olduğu iddiası hakkında:

6698 sayılı Kanun'un yürürlüğe girmiş olması ve 6. maddesinin dördüncü fıkrasında değinilen yeterli önlemlerin henüz belirlenmemiş olmasını, kişisel sağlık verilerinin tarafından işlenememesi için ileri sürmenin izahtan varestede olduğu, bu iddianın doğruluğunu savunmanın, özel nitelikli kişisel verilerden olan kişisel sağlık verilerinin yalnızca tarafından değil, aynı zamanda hiçbir kişi (hekim), kurum ve kuruluş (özel ve kamu sağlık tesisleri) tarafından işlenmemesini de beraberinde getireceği, ki bunun da ülkemizdeki tüm sağlık hizmetlerinin durması anlamına geldiği, hatta dernek üyeliğinin de özel nitelikli kişisel veriler arasında zikredilmiş olması göz önünde bulundurulduğunda, davacı ile 'nin kendi üyelerine ilişkin verileri işleyememesi, dernek üyesi olmaları gerekçesiyle üyelerine hiçbir iş ve işlemde bulunamayacağı, hiçbir şekilde iletişime geçemeyeceği ki bu durumun hayatın olağan akışına aykırı olduğu, nitekim, 6698 sayılı Kanun'un 6. maddesinin dördüncü fıkrasında öngörülen ve Kurul tarafından belirlenecek yeterli önlemlerin alınması şartının, yalnızca aynı maddenin üçüncü fıkrası uyarınca istisnai hallerde işlenen özel nitelikli kişisel veriler için değil, aynı zamanda açık rıza ile işlenen özel nitelikli kişisel veriler için de geçerli olduğu, Kanun hükmünün yalnızca nı değil, özel nitelikli kişisel veri işleyen tüm gerçek kişiler ile özel hukuk ve kamu hukuku tüzel kişilerini bağladığı, dolayısı ile özel nitelikli kişisel verilerin işlenmesinde gerekli olan yeterli önlemlerin Kurul tarafından henüz belirlenmemiş olması hususunu, kişisel sağlık verilerinin tarafından işlenememesi için bir gerekçe olarak sunmanın tutarlı hiçbir tarafı bulunmadığı,

6698 sayılı Kanun'un 7. maddesinin dördüncü fıkrası uyarınca özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınmasının şart olduğu, bu yeterli önlemlerin Kurul tarafından yayımlandığı anda bu şartın aranmaya başlayacağı,

Kanun ve Yönetmeliğin 108 sayılı Sözleşmeye aykırılık iddiası hakkında:

Türkiye'nin, Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne (108 sayılı Sözleşme), 28 Ocak 1981 tarihinde imza atmış olmasına rağmen, uzun bir süre Sözleşmeyi onaylanmadığı, Sözleşmenin nihayet 30.01.2016 tarihinde onaylandığı, 18.02.2016 tarihli ve 29628 sayılı Resmî Gazete'de yayımlandığı, 108 sayılı Sözleşmenin, 6669 sayılı Kanun'un 2. maddesi gereği, Resmî Gazete'de yayımlandığı gün olan 18.02.2016 tarihinde yürürlüğe girdiği, Anayasa'nın 90. maddesinin 5. fıkrasında; "Usulüne göre yürürlüğe konulmuş milletlerarası anlaşmalar kanun hükmündedir. Bunlar hakkında Anayasaya aykırılık iddiası ile Anayasa Mahkemesine başvurulamaz. (Ek cümle: 7/5/20045170/7 md.) Usûlüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası anlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası anlaşma hükümleri esas alınır." hükmünün bulunduğu, madde metninden, usulüne göre yürürlüğe konulan 108 sayılı Sözleşme ile

6698 sayılı Kanun'un, aynı konuda farklı hükümler içermesi halinde 108 sayılı Sözleşme hükümlerinin esas alınacağına anlaşıldığı, bununla birlikte usulüne göre yürürlüğe konulan milletlerarası anlaşmaların, Anayasa'ya üstünlüğünün bulunmadığı, bunlar hakkında Anayasa'ya aykırılık iddiası ile Anayasa Mahkemesine başvurulamamasının, bu anlaşmaların Anayasa'dan üstün olduğu anlamına gelmediği, Anayasa'nın 20. maddesinde ise kişisel verilerin hangi hallerde işlenebileceğinin açık bir şekilde hüküm altına alındığı, diğer taraftan 108 sayılı Sözleşme'nin 6. maddesinde "iç hukukta uygun güvenceler sağlanmadıkça otomatik işleme tabi tutulmalarının yasaklandığı" verilerin yalnızca kişisel sağlık verileri olmadığı, ceza mahkumiyetine ilişkin kişisel verilerin de madde metninde vurgulandığı, bununla birlikte Ulusal Yargı Ağı Projesi (UYAP) kapsamında ceza mahkumiyetine ilişkin kişisel verilerin, uzun zamandır otomatik işleme tabi tutulduğu, dolayısı ile ülkemizin "iç hukukta uygun güvenceler sağlayamadığı" iddiasının doğru kabul edilmesi halinde, UYAP'ın da hukuki dayanaktan yoksun kalacağı,

Ayrıca, 108 sayılı Sözleşme'nin 9. maddesinde, "Devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi" gibi durumların varlığı halinde, Sözleşmenin 5, 6 ve 8 inci maddelerine sınırlama getirilebileceği hükmünün yer aldığı, dolayısı ile 108 sayılı Sözleşme'nin 9 uncu maddesinin, aralarında "kamu güvenliği"nin de bulunduğu bir takım sebeplerin söz konusu olduğu durumlarda, 6. maddenin sınırlandırılabilirliğini hüküm altına aldığı, bu yönüyle de 6698 sayılı Kanun ile Yönetmelik hükümlerinin, 108 sayılı Sözleşme ile uyumsuzluk arz etmediği,

Amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırılık iddiası hakkında:

Bakanlığın uygulama ve süreçlerinde, 6698 sayılı Kanun'un "Genel ilkeler" başlıklı 4. maddesinde belirtilen ilkelerin göz önünde bulundurulduğu ve bu ilkeleri ihlal edecek uygulamalardan kaçınıldığı, kişilerin sağlık verileri toplanmaksızın doğru sağlık politikaları oluşturmanın mümkün olmayacağı, büyük veri (big data) çağında bulunduğumuz günümüzün "petrolü"nü veri olduğu, gelişmiş ülkelerin çok büyük bütçeler ayırmalarına karşın başaramadıkları teknik alt yapının, Bakanlık tarafından emsallerine oranla çok daha küçük bütçelerle son derece başarılı bir şekilde hazırlandığı, bu teknik alt yapı ile son derece verimli analizler, istatistiksel çalışmalar yapıldığı, bu çalışmalarla kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi konularında emsalsiz faydalar sağlandığı, yalnızca Tip-II diyabetin ülkemize yıllık maliyetinin 15 milyar TL civarında olduğu göz önünde bulundurulduğunda, bu sistemlerin "devletin mali menfaatlerine" olan katkısının boyutunun da tartışılmayacak seviyede olduğu, tüm işlemlerin iz (log) kayıtlarının tutulduğu, yetkisiz erişimlerin her zaman görüntülenebildiği, toplanan verilerin USS'de anonim hale

getirilerek tutulduğu, ancak ilgili kişinin e-Nabız profili oluşturması halinde kişi ile ilişkilendiriliği ve verilere yalnızca kişinin kendisi ile yetki verdiği üçüncü kişilerce erişilebildiği, sonuç olarak, ulusal ve uluslar arası düzenlemelerde öngörülen ilkelere riayet edildiği,

Merkezi sağlık veri sistemi ile ilgili iddialar hakkında:

Anayasa'nın 56. maddesinde "Devlet, herkesin hayatını, beden ve ruh sağlığı içinde sürdürmesini sağlamak; insan ve madde gücünde tasarruf ve verimi artırarak, işbirliğini gerçekleştirmek amacıyla sağlık kuruluşlarını tek elden planlayıp hizmet vermesini düzenler. Devlet, bu görevini kamu ve özel kesimlerdeki sağlık ve sosyal kurumlarından yararlanarak, onları denetleyerek yerine getirir." hükmünün bulunduğu, 663 sayılı KHK'nın 2. maddesinin birinci fıkrası ile herkesin bedenî, zihnî ve sosyal bakımdan tam bir iyilik hâli içinde hayatını sürdürmesini sağlama görevinin, na verildiği, 663 sayılı KHK'nın 11. maddesinde "Kişisel sağlık verileri ile ülke düzeyinde sağlık durumu ve sağlık hizmetlerine ilişkin veri ve bilgi akışını içeren her türden bilgi sistemleri ve projelerini yapmak ve yaptırmak" ve "Sağlık bilişimi ve teknolojisi alanında çalışacak kamu ve özel hukuk tüzel kişileri ile gerçek kişilerin uyacakları kuralları belirlemek, uygulamak, gerektiğinde bunların yazılım ve ürünlerinin uygunluğuna karar vermek ve müelliflerini yetkilendirmek" görevlerinin ise Sağlık Bilgi Sistemleri Genel Müdürlüğüne tevdi edildiği, 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 3. maddesinin birinci fıkrasının (f) bendinde, yukarıdaki hükmü destekler nitelikteki "Herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi maksadıyla, ve bağlı kuruluşlarınca gerekli kayıt ve bildirim sistemi kurulur. Bu sistem, e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabilir. Bu amaçla, nca, bağlı kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemi kurulabilir." hükmünün yer aldığı Anayasa'nın 125. maddesinde; "Yargı yetkisi, idarî eylem ve işlemlerin hukuka uygunluğunun denetimi ile sınırlı olup, hiçbir surette yerindelik denetimi şeklinde kullanılamaz. Yürütme görevinin kanunlarda gösterilen şekil ve esaslara uygun olarak yerine getirilmesini kısıtlayacak, idarî eylem ve işlem niteliğinde veya takdir yetkisini kaldırarak biçimde yargı kararı verilemez." hükmünün bulunduğu, yukarıda anılan hükümler uyarınca Bakanlığın, merkezi sağlık veri sistemi olan USS ile bu sisteme bağlı olarak çalışan e-Nabız'ın oluşturulduğu, her iki sistem de temelini kanuni düzenlemelerden aldığı,

Kamu kurumları arasında veri paylaşımının, Yönetmeliğin 8. maddesinin üçüncü fıkrası uyarınca Protokol ile yapıldığı, hukuki düzenlemelere aykırı olan durumlarda veri aktarımı yapılmadığı, Protokol ile veri aktarımının ancak veri aktarımının hukuka uygun olduğu hallerde yapıldığı, hukuka

uygun olmayan veri aktarımı taleplerinin Bakanlıkça birçok kez reddedildiği, veri aktarımı taleplerinin değerlendirilmesinde, 6698 sayılı Kanun'un 8. maddesinin göz önünde bulundurulduğu, Davacının, 6698 sayılı Kanun'un 22. maddesinin birinci fıkrasının (h) bendi gereği, kişisel verilere ilişkin hüküm içeren mevzuat taslaklarını hazırlarken Kurul'dan görüş alınmasının zorunlu olduğunu ifade ettiği, oysa Kanun'da böyle bir zorunluluğun bulunmadığı, ilgili hükümde, "Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek" hususunun, Kurul'un görev ve yetkileri arasında zikredildiği, bu hükmün, Yönetmeliğin çıkartılmasında Kurul'dan görüş alınmasının zorunlu olduğu anlamına gelmediği, ayrıca, Yönetmeliğin çıkartıldığı tarihte Kurulun henüz teşekkül etmediği, teşekkül etmeyen bir Kurul'dan görüş alınmasının da mümkün olmadığı, hatta Kanun'un Geçici Madde 1'in birinci fıkrası uyarınca en geç 07.10.2016 tarihinde oluşması gereken Kurulun, bu tarihten ancak aylar sonra oluştuğu, Yönetmeliğin ise 20.10.2016 tarihinde Resmî Gazete'de yayımlanarak yürürlüğe girdiği,

İç hukukta gerekli güvencelerin sağlanmamış olduğu iddiası hakkında:

6698 sayılı Kanununun 07.04.2016 tarihi ile yürürlükte olduğu ve Anayasa'nın 20. maddesinde öngörülen hükmün bu Kanun ile yerine getirildiği, iç hukukta uygun güvencelerin sağlanması ön koşulunun yerine getirilmediğini iddia etmenin, yürürlükte olan Kanunu yok saymak anlamına geldiği,

Veri sorumlusunun kim olduğunun Yönetmelikte işaret edilmediğinin iddia edildiği, oysa veri sorumlusunun tanımına, Yönetmeliğin 4. maddesinin birinci fıkrasının (o) bendinde yer verildiği, Dünyanın hiçbir yerinde, konuya ilişkin hiçbir hukuki düzenlemede veri sorumlusunun kim olduğu somut olarak ifade edilmediği, hukuki düzenlemelerde böyle bir teknik bulunmadığı, bunun yerine veri sorumlusunun tanımına yer verildiği, veri sorumlularının görev, yetki ve sorumlulukları ile kişisel verilerin işlenmesindeki rollerinin izah edildiği,

Davacının, Komisyon'un dayanağını yasalardan almadığını iddia ettiği, Kişisel Sağlık Verileri Komisyonunun Yönetmeliğin 12. maddesi uyarınca oluşturulduğu, Yönetmeliğin ise 6698 sayılı Kanun ile üzerinde değişiklik yapılan 663 sayılı KHK'nın 47. maddesinin altıncı fıkrası uyarınca yürürlüğe konulduğu, Komisyonun yetki alanının sınırsız olmayıp, yalnızca ve bağlı kuruluşları ile bunların bünyesinde faaliyet gösteren ve birinci, ikinci ve üçüncü basamakta sağlık hizmeti sunmakta olan sağlık tesislerini kapsadığı, Komisyon'un görev ve yetki alanı kişisel sağlık verisi işleyen tüm gerçek kişiler ile özel hukuk ve kamu hukuku tüzel kişilerinden oluşuyor olsaydı davacının iddiasını yerinde bulmanın mümkün olabileceği, fakat Komisyon'un görev ve yetki alanının yalnızca Bakanlık

ve bağı kuruluşları ile bunların bünyesinde faaliyet gösteren ve birinci, ikinci ve üçüncü basamakta sağlık hizmeti sunmakta olan sağlık tesislerini kapsadığı, Bakanlığın kendi iç işleyişi ile ilgili süreçleri bakımından öngördüğü Komisyon'un "alana ilişkin meslek örgütlerinin katılımıyla oluşan bir oluşum olması" zorunluluğu bulunmadığı gibi, böyle bir Komisyon'un kurulması için kanun düzeyinde bir düzenleme ile öngörülmüş olma zorunluluğu da bulunmadığı savunulmuştur.

'nın Savunmasının Özeti: 6698 sayılı Kanununun 21. maddesi hükümlerine göre, Kişisel Verileri Koruma Kurulu üyelerinin seçimlerinin 12 Ocak 2017'de tamamlanabildiği, Yargıtay 1. Başkanlık Kurulu huzurunda yemin ettikleri, 30 Ocak 2017'de Başkan ve 2. Başkanın seçildiği, dava konusu Yönetmeliğin yayımlandığı 20.10.2016 tarihinde henüz usulüne uygun olarak teşekkül etmemiş Kurulunun nca çıkarılan Yönetmeliğin hazırlanma sürecinde herhangi bir görüş, katkı, ya da değerlendirme yapma imkânının bulunmadığı, bu davada taraf sıfatını haiz olmadıkları,

6698 sayılı Kanununun Geçici 1. maddesinde, yer alan "...Bu Kanunun yayımı tarihinden önce işlenmiş olan kişisel veriler, yayımı tarihinden itibaren iki yıl içinde bu Kanun hükümlerine uygun hâle getirilir. Bu Kanun hükümlerine aykırı olduğu tespit edilen kişisel veriler derhâl silinir, yok edilir veya anonim hâle getirilir..." hükmü gereği veri sorumlularının kişisel verileri işleme faaliyetlerini Kanuna uyumlu hale getirebilmesi için öngörülen iki yıllık sürenin Kanunun yayım tarihi olan 07.04.2016'da başladığı; Kurulun henüz teşekkül etmemiş ve özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemlerin tespit edilmemiş olmasının diğer kurum ve kuruluşlarca kişisel verilere ilişkin hüküm içeren düzenleyici işlem yapılmasına engel teşkil etmeyeceği,

Anayasa'nın 20. maddesinin 3. fıkrasındaki, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenlenmesi hükmünün, bu alanın yalnızca kanunla düzenleneceği anlamına gelmediği, 6698 sayılı Kişisel Verilerin Korunması Kanununun, kişisel verilerin korunmasına ilişkin esas ve usullerin düzenlenmesi amacıyla yürürlüğe girdiği; Kanunda temel ilkelerin düzenlendiği; Anayasanın 124. maddesinde belirtilen idarenin düzenleme yetkisi çerçevesinde anılan Kanuna istinaden Yönetmelikler çıkarılmasına hukuki bir engel bulunmadığı,

6698 sayılı Kanununun 6. maddesinde özel nitelikli kişisel verilerin ilgilinin açık rızası olmaksızın işlenebileceği hallerin tahdidi olarak sayıldığı; bunların 108 nolu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Sözleşme ve 95/46 sayılı Direktifte yer alan hükümlere uygun olduğu, Anayasanın 20. maddesinde yer alan "kanunda öngörülen hallerde" şartının da 6698 sayılı Kanununun 6. maddesindeki düzenlemeyle sağlandığı; anılan hüküm ve 663

sayılı Kanun Hükmünde Kararname'nin 47. maddesinin iptali talebinin de Anayasa Mahkemesi tarafından reddedildiği,

6698 sayılı Kanunun "veri sorumlusu" kavramını net olarak ortaya koyduğu; Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade ettiğinin belirtildiği; Kanunun düzenlemesi karşısında Yönetmelikte farklı bir yorum yapılması mümkün olmayacağından bu hususa ilişkin tartışmaya mahal olmayacağı,

Kişisel verilerin işlenmesinde uyulması zorunlu ilkelerin 6698 sayılı Kanunun 4. maddesinde düzenlendiği; bu ilkelere birinin "ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" olduğu; işlendikleri amaç için gerekli olan azami sürenin tespitinde dikkate alınması gereken hususların 30.12.2017 tarihli ve 30286 sayılı Resmi Gazete'de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmeliğin 9. maddesinin 4. fıkrasında tek tek sayıldığı; Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 5. maddesinde yer alan, "Kanunun 16 ncı maddesi gereğince Veri Sorumluları Siciline kayıt olmakla yükümlü olan veri sorumluları, kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası hazırlamakla yükümlüdür." hükmüne göre veri sorumlularının, veri saklama ve imha politikası, verilerin saklanması ve imhasına ilişkin yaptıkları işlemler ve saklama sürelerinin belirli ve Kanun ve Yönetmelikte öngörülen usul ve esaslara uygunluğu yönünden denetlenebilir olması açısından önem arz ettiği,

Kanunun 11. maddesinde ilgili kişinin haklarının sayıldığı; bunların arasında "7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme" olduğu, buna göre ilgili kişinin, kişisel verilerinin silinmesini veya yok edilmesini isteme hakkının sınırsız olmayıp, Kanunun 7. maddesinde öngörülen şartlarla bu hakkın kullanılabilmesinin mümkün olduğu savunulmuştur.

Düşüncesi: 'ndan görüş alınmadan hazırlanan dava konusu düzenlemede mevzuata ve hukuka uygunluk bulunmadığından yürütmenin durdurulması isteminin kabulü gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay Onbeşinci Dairesince hasım konumuna alınan 'nun da birinci savunması alındıktan sonra incelenmesine karar verilen yürütmenin durdurulması istemi, savunmanın verildiği görülmüş olmakla incelenerek işin gereği görüldü:

Dava, 20.10.2016 tarihli ve 29863 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin muhtelif maddelerinin ve tamamının yürütmesinin durdurulması ve iptali istemiyle açılmıştır.

Davacılar, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun uygulamasını belirlemekte yasa koyucunun asıl yetkiyi 'na verdiği, Kurumun karar organı olan Kişisel Verileri Koruma Kurulu'na da bu alana dair ülkesel uygulamanın ilkelerini belirleme yetki ve görevi verildiği, dolayısıyla Türkiye'deki Kişisel Verileri Koruma Kanunu'nun uygulanmasında temel ilkeler belirlendikten sonra ilgili alanların ihtiyacına ve özelliğine uygun düzenleyici işlemler yapılabileceği, Kanunun 6/4. maddesinde, "Özel nitelikteki kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.", 16. maddesinin 1. ve 2. fıkralarında, "(1) Kurulun gözetiminde, Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili tutulur. (2) Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır..." hükümlerinin bulunduğu, henüz ne Kurum ne de Kurul oluşturulmadığı, bunun sonucu olarak verilerin işlenmesinde alınması gereken önlemlerin belirlenmediği, Veri Sorumluları Sicilinin oluşturulmadığı, 663 sayılı KHK'nın 47. maddesinin 6. fıkrasıyla na verilen düzenleme yetkisinin bağlı yetki olduğu, takdir yetkisinin sınırının Kişisel Verileri Koruma Kurulu'nun belirleyeceği ilkeler olduğu, Kanunun 31. maddesindeki "Bu Kanunun uygulanmasına ilişkin yönetmelikler Kurum tarafından yürürlüğe konulur." hükmü ile ikincil düzenleyici işlem yapma yetkisinin asıl olarak 'na verildiği, Kanunun 22. maddesine göre de tarafından hazırlanan mevzuat taslağının Kurul'dan görüş alındıktan sonra çıkarılması gerektiği, bu nedenlerle bağlı yetkinin sınırlarına aykırı işlem olması nedeniyle yetki unsuru yönünden hukuka aykırı olan Yönetmeliğin tamamının iptalinin gerektiği,

Yönetmeliğin kişisel sağlık verileriyle ilgili bir takım iş ve işlemlere dair usul ve esasları belirlemek amacıyla çıkarılmasına karşın, kişisel sağlık verilerinin işleme amaçlarını ve vasıtalarını belirleme yetkisinin veri sorumlusuna ait olduğunun belirtilmesiyle yetinildiği, bu kişinin niteliklerine dair bir belirleme yapılmadığı, veri sorumlusunun özel hukuk tüzel kişisi olup olamayacağı, böyleyse Kamu İhale Kanunu ve diğer mevzuat çerçevesinde hizmet alımı yapıp yapılamayacağının belirsiz olduğu, tüm kişisel sağlık verileriyle ilgili belirleme yapmaya dair bu denli büyük yetkilerle donatılan gerçek veya tüzel kişinin kim olacağı, bu kişinin veri işleyene yetkiyi nasıl devredeceğinin Yönetmelikle belirlenmediği, 6698 sayılı yasanın soyut düzenlemesinin tekrarıyla yetinildiği, bu nedenle 4. maddesinin 1. fıkrasının (n) ve (o) bentleri ile 11. maddesinin eksik düzenleme olması nedeniyle hukuka aykırı oldukları,

Yönetmeliğin, kişisel verilerin sınırsız olarak hiçbir ayırım yapılmadan merkezi sisteme aktarılmasına ve Bakanlığın da bu verileri diğer kamu kurum ve kuruluşlarına aktarabileceğine dair 5/8., 7/1., 8/1. ve 14/1. maddelerinin temel hakkın özüne zarar veren, amaçla uygun olmayan bir müdahale niteliğinde olduğu, kişisel sağlık verilerinin ancak sınırlı sebepler gerçekleştiğinde istisnai olarak işlenebileceği, Yönetmelikte ise bu ilkenin ters çevrilerek sağlık verilerinin işlenmesinin kural işlenmemesinin ise istisna sayıldığı, dayanak yasada böyle bir yetki verilmediği halde Bakanlığın elde ettiği verileri açık rıza aranmaksızın protokolle diğer kurumlarla paylaşabileceğinin düzenlendiği, Yönetmeliğin 9. maddesinin 1. fıkrasında kişisel sağlık verilerinin silinmesini talep etme hakkına ölçüsüz sınırlama getirildiği, bunun yanı sıra resen silmeye dair herhangi bir düzenleme içermediği ve verilerin tutulmasına dair azami süre öngörmediği,

3046 sayılı Bakanlıkların Kuruluş ve Görev Esasları Hakkında Kanununun 12. ve 13. maddelerinde Bakanlık ve bağlı kuruluşların merkez teşkilatındaki danışma, denetim ve yardımcı birimlerinin belirlendiği; 14. maddesinde, ilgili kuruluşlarda hizmet özelliklerine göre hangi danışma, denetim ve yardımcı birimlerin kurulacağı bu kuruluşların kuruluş kanunu veya statülerinde belirleneceğinin düzenlendiği; 39. maddesinde, Bakanlıklarda ve bağlı kuruluşlarda hizmetin kurul biçiminde yürütülmesi gerektiğinde, görevleri ve teşekkül tarzı kuruluş kanunlarında veya diğer kanunlarda gösterilmek kaydıyla sürekli kurullar kurulabileceğinin düzenlendiği; dava konusu Yönetmelikle kurulan Kişisel Sağlık Verileri Komisyonuna, danışmanlık, denetim, anlaşmazlıkların çözülmesi ve veri aktarımı başvurularının değerlendirilmesi gibi çok önemli yetkiler verilmiş olmasına karşın 663 sayılı KHK'da böyle bir birim bulunmadığı,

Ayrıca, Komisyona tanımlanan görevin objektif biçimde yerine getirilebilmesi ile hastaların haklarının korunması bakımından Komisyon bileşiminin demokratik katılıma olanak verecek şekilde düzenlenmesi, ilgili meslek kuruluşları ile hasta hakları kuruluşlarının da Komisyona etkin katılımının sağlanmasının gerektiği, bütün bunlara aykırı olan Yönetmeliğin 4. maddesinin 1. fıkrasının (h) bendi ve 12. maddesinin iptalinin gerektiğini ileri sürerek, düzenlemenin yürütmesinin durdurulması ve iptalini istemektedirler.

07.04.2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu, Türkiye Büyük Millet Meclisi'ne sunulan genel gerekçesinden de anlaşılacağı üzere, kişisel verilerin korunması konusunun pek çok sektörü ve kamu ya da özel pek çok kurumu ilgilendirmesi nedeniyle bir "çerçeve kanun" olarak hazırlanmıştır.

Bu Kanuna neden ihtiyaç duyulduğunu açıklayan genel gerekçede, Türk Ceza Kanunu'nun 135 ve devamı maddelerinde kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa

edilmesi fiillerinin suç olarak düzenlendiği ve yaptırıma bağlandığı, ancak kişisel verilerin işlenmesine yönelik özel bir kanun bulunmaması sebebiyle, bu fiillerin ne zaman hukuka aykırı ne zaman hukuka uygun olduğunun belirlenmesinde tereddütler yaşandığı vurgulanmaktadır. Ayrıca 2010 yılında Anayasa'nın 20. maddesinde yapılan düzenlemeyle kişisel verilerin korunması temel bir insan hakkı olarak güvence altına alınmış ve konuya ilişkin usul ve esasların kanunla düzenleneceği öngörülmüştür.

Genel gerekçede, kişisel verilerin korunmasına yönelik bir kanuni düzenleme olmamasının uluslararası ilişkiler açısından da sorunlar yarattığı, EUROPOL, EUROJUST gibi Avrupa kurumları ile ilişkilerin sekteye uğradığı, sağlık kuruluşlarınca tutulan kişisel verilerin güvenliğinin sağlanmasında yeterli yasal önlem olmamasının Avrupa İnsan Hakları Mahkemesince özel hayatın gizliliğine müdahale olarak kabul edildiği ve bu nedenle ihlal kararları verildiği belirtilmektedir. Yine genel gerekçede, bu Kanunun Türkiye'nin Avrupa Birliği'ne üyelik süreci açısından da önemine dikkat çekilmekte, Türkiye'nin, Avrupa Konseyi tarafından tüm üye ülkelerde kişisel verilerin aynı standartlarda korunması ve sınır ötesi veri akışı ilkelerinin belirlenmesi amacıyla hazırlanan 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"ne de 1981 yılından itibaren taraf olduğu ifade edilmektedir.

Bütün bu hususlardan anlaşılacağı üzere 6698 sayılı Kanun, kişisel verilerin korunması konusunda önemli bir yasal boşluğu doldurmak amacıyla kabul edilen çerçeve niteliğinde bir yasal düzenlemedir. Genel gerekçede yer verilen şu tespit Kanun ile oluşturulan Kurulu'nun genel kontrol ve denetleme işlevlerine dikkat çekmesi bakımından önemlidir: "Ülkemizde kişisel verilerin işlenmesi sürecini kontrol edecek ve denetleyecek bir kurum bulunmamaktadır. Bunun bir sonucu olarak halen kişisel veriler yeterli düzenleme ve denetime tabi olmaksızın, birçok kişi veya kurum tarafından kullanılabilen ve bu durum bazı hak ihlallerinin yaşanmasına sebep olabilmektedir."

6698 sayılı Kanunun 21. maddesi hükümlerine göre oluşturulan 'nun görev ve yetkileri, aynı Kanun'un 22. maddesiyle belirlenmiştir. 22. maddenin 1. fıkrasının (h) bendinde "Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek." hükmüne yer verilmiştir.

Anılan Kanun'un, "Özel nitelikli kişisel verilerin işleme şartları" başlıklı 6. maddesinin 1. fıkrasında, dava konusu Yönetmelikle düzenlenen, sağlık verilerinin de özel nitelikli kişisel veri olduğu belirtilmiş; maddenin 4. fıkrasında, "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü getirilmiştir.

6698 sayılı Kanunun Geçici 1. maddesi hükmü uyarınca, Kanunun 21. maddesine göre oluşturulacak Kişisel Verileri Koruma Kurulu'nun, Kanunun Resmi Gazete'de yayımlandığı 7/4/2016 tarihinden itibaren altı ay içinde üyelerinin seçiminin tamamlanması gerekmekte iken, bu yasal gerekliliğin ancak 30.01.2017 tarihinde yerine getirilebildiği anlaşılmaktadır.

Davalıların savunmaları ve dosya içeriğinden, dava konusu Yönetmeliğin Resmî Gazete'de yayımlandığı tarih olan 20.10.2016'da Kişisel Verileri Koruma Kurulu'nun henüz oluşturulmadığı, dolayısıyla 6698 sayılı Kanun'un 6. maddesinin 4. fıkrasında belirtilen yeterli önlemlerin Kurul tarafından belirlenmediği ve Kanun'un 22. maddesinin 1. fıkrasının (h) bendine göre diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında Kurul görüşü alınmadan dava konusu düzenlemenin tesis edildiği görülmektedir.

Yukarıda yer verilen genel gerekçe ve Kanun hükümlerine göre, Kişisel Verileri Koruma Kurulu'nun kişisel verilerin korunması konusunda genel nitelikte bir kontrol ve denetim yetkisine sahip olduğu, diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hükümler içeren mevzuat taslakları hakkında Kişisel Verileri Koruma Kurulu'ndan görüş alınmasının şart olduğu, Kurulu'nun kontrol ve denetiminden geçirilmeksizin hazırlanan ve 20/10/2016 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe giren dava konusu düzenlemede bu nedenle mevzuata ve hukuka uygunluk bulunmadığı sonucuna ulaşılmıştır.

Açıklanan nedenlerle, olayda 2577 sayılı İdari Yargılama Usulü Kanunu'nun 6352 sayılı Yasa ile değişik 27. maddesinin 2. fıkrasında sayılan koşullar gerçekleşmiş olduğundan yürütmenin durdurulması isteminin kabulüne, 20.10.2016 tarihli ve 29863 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin yürütmesinin durdurulmasına, bu kararın tebliğini izleyen günden itibaren yedi gün içinde İdari Dava Daireleri Kurulu'na itiraz yolu açık olmak üzere, 26/06/2018 tarihinde oybirliğiyle karar verildi.

Danıştay Kararı - 15. Daire (E. 2018/530)

Danıştay Kararı - 15. D., E. 2018/530 K. YD T. 20.2.2018

T.C. DANIŞTAY ONBEŞİNCİ DAİRE

Esas No: 2018/530

DAVACI VE YÜRÜTMENİN DURDURULMASINI İSTEYEN:

VEKİLLERİ:

DAVALI:

VEKİLLERİ:

İSTEMİN KONUSU:

1. 12/12/2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 3. maddesi ile değiştirilen asıl Yönetmeliğin 19. maddesinin 3. fıkrasının iptali ve yürütmesinin durdurulması istenilmektedir.
2. Anılan Yönetmeliğin 4. maddesi ile değiştirilen asıl Yönetmeliğin 27. maddesinin 8. fıkrasının iptali ve yürütmesinin durdurulması istenilmektedir.
3. Anılan Yönetmeliğin 5. maddesi ile değiştirilen asıl Yönetmeliğin Ek-1. maddesinin 16. fıkrasının iptali ve yürütmesinin durdurulması istenilmektedir.
4. Anılan Yönetmeliğin 5. maddesi ile asıl Yönetmeliğe eklenen Ek-1. maddesinin 18. fıkrasının iptali ve yürütmesinin durdurulması istenilmektedir.
5. Anılan Yönetmeliğin 8. maddesi ile değiştirilen asıl Yönetmeliğin ekinde yer alan EK-9'daki 1 sayılı Liste ve 2 sayılı Listenin iptali ve yürütmenin durdurulması istenilmektedir.

DAVACININ İDDİALARI:

Dava konusu Yönetmeliğin 3. maddesi ile değiştirilen asıl Yönetmeliğin 19. maddesinin 3. fıkrasına ilişkin olarak; yan dal uzmanı olan hekimlerin, sahip oldukları uzmanlık diplomalarına dayalı olarak özel hastanelerde mesleklerini icra etme olanaklarının yasal dayanağı olmaksızın sınırlandırıldığı, Bakanlığın konuyu hangi kriterlere göre değerlendireceği, bu değerlendirmeyi ne kadar süre

içerisinde yapacağı hususlarına yer verilmediğinden hekimler yönünden yaratılan belirsizlik ve keyfi uygulamaların önünün açıldığı, özel sağlık kuruluşlarında çalışacak yan dal unvanına sahip bir hekimin çalışma izninin, kamudaki yan dal uzmanlığına sahip eğitici ihtiyacının bulunmaması koşuluna bağlı kılındığı, oysa yasalar ile atama usulü özel olarak belirlenmiş eğitici kadrolarına, kamu ile bağı bulunmayan hekimlerin doğrudan atanmasının söz konusu olmadığı, kişiler eğitici olmak istemezlerse zorla kamusal eğitim kadrolarına atanmalarının söz konusu olmayacağı, akademik kadrolar için aranan tek niteliğin de yan dal uzmanlığı olmadığı, Yasada tanınan hekimlik yetkisini normlar hiyerarşisine aykırı biçimde ortadan kaldıran, hukuki güvenlik ilkesini, hekimlerin maddi ve manevi varlığını geliştirme hakkını, bilim ve sanatı serbestçe öğrenme hakkını ve çalışma hak ve özgürlüğünün özünü zedeleyen düzenlemede hukuka uyarlık bulunmadığı ileri sürülmektedir.

Dava konusu Yönetmeliğin 4. maddesi ile değiştirilen asıl Yönetmeliğin 27. maddesinin 8. fıkrasına ilişkin olarak; 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesi üzerine hastanın rızası dahi aranmaksızın ve sınırsız biçimde sağlık verilerinin toplanması anlamına gelen dava konusu düzenlemenin tesis edildiği, 6698 sayılı Kanunun uygulanabilmesi için gereken kurum ve kurullar oluşturulmadan, bu Kurul tarafından belirlenmesi gereken önlemler tanımlanmadan, veri sorumlusu sicili oluşturulmadan alana ilişkin düzenleme yapılmasının hukuka aykırı olduğu, dava konusu düzenlemede "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Sözleşme"de yer verilen istisnalardan hiçbirine yer verilmediği, sağlık politikalarına yön vermek için sağlık hizmeti verilerinin kişisel bilgilerden arınmış bir şekilde anonim hale getirilip toplanabileceği, dava konusu değişikliğin uygulamayı göstermekten uzak olduğu ileri sürülmektedir.

Dava konusu Yönetmeliğin 5. maddesi ile değiştirilen asıl Yönetmeliğin Ek-1. maddesinin 16. fıkrasına ilişkin olarak; bazı koşullarda hekimin diğer bir ilde çalışmasının söz konusu olabileceği ancak, bu hakkın koşullarının daima güncel olarak değerlendirilmesi ve düzenlenmesi gerektiği, Yönetmeliğin ise bu içerikten yoksun olduğu, söz konusu değişikliğin yeni bir hekim istihdamı yerine işverenin bir çok sorumluluktan kurtulması için ticari kaygılara dayalı olarak yapıldığı, birden çok ilde çalışmanın hekimin esas görevinin yanı sıra diğer ek görevlerinde de veriminin azalmasına ve mesleki uygulama sorunlarına yol açacağı, hekimin hastalarını takip edebilmesinin ve hastanın da hekime ulaşmasının zorlaşacağı ileri sürülmektedir.

Dava konusu Yönetmeliğin 5. maddesi ile asıl Yönetmeliğe eklenen Ek-1. maddesinin 18. fıkrasına ilişkin olarak; değişikliğin özel sağlık kuruluşlarında çalışan tabip/uzman tabiplerin başka bir özel

hastanede çalışmasını nöbetle sınırlandırdığı, özel sağlık kuruluşunda nöbet tutabilmek için bir sağlık kuruluşunda çalışıyor olmanın zorunlu hale getirildiği, özel hastanelerde çalışanların nöbet dışında başka bir sağlık kuruluşunda çalışabilmesinin kurumsal sözleşmeye bağlı kılındığı, 1219 sayılı Kanun'un 12. maddesinde tanınan hakkın nöbetle sınırlanmasının mümkün olmadığı, düzenlemenin Yönetmeliğin Ek 1. maddesinin 2. fıkrasında yer alan hüküm ile de çeliştiği, bu hükmü örtülü bir biçimde yürürlükten kaldırdığı, maddede ayrıca özel hastane kadrosunda çalışan tabibin başka bir özel hastane ya da tıp merkezinde kısmi zamanlı çalışabilmesi için kurumsal sözleşme yapılmasının ve çalışacak hekimin muvafakat vermesinin gerekliliğinin düzenlendiği, söz konusu düzenleme ile hekimin iradesinin yok sayıldığı, bu şekilde çalışmanın işverenin iradesine bağlı kılındığı, özel hastane sahibinin zincir hastane veya anlaşmalı olduğu bir başka sağlık kuruluşu ile anlaşarak hekimin ikinci bir yerde çalışmasını zorunlu kılacağı, işten atılma tehdidi karşısında hekimin muvafakat vermemesinin olanaklı olmadığı, planlama amacıyla yapılan bu düzenlemenin bu amaca değil ticari kaygılara hizmet edeceği, parçalı istihdamına karar verilen hekimin mesai sonrası nöbet tutmak zorunda bırakılmasının angarya yaşağının ihlali anlamına geldiği, bunun toplum sağlığını da tehdit edeceği ileri sürülmektedir.

Dava konusu Yönetmeliğin 8. maddesi ile değiştirilen asıl Yönetmeliğin ekinde yer alan EK-9'daki 1 sayılı Liste ve 2 sayılı Liste'ye ilişkin olarak; tıbbın dinamik bir alan olduğu, sürekli değişim ve gelişim gösteren bu alanda yapılabilecek olan işlemlerin sayma yoluyla belirlenmesinin olanaklı olmadığı, yapılabilecek işlemleri sayma yoluyla gösteren düzenlemenin genel, sürekli ve soyut olamayacağı, bu haliyle çalışma hakkını ve sağlık hizmetlerine ulaşım hakkını sınırlayan bir metin olduğu, düzenlemenin hukuki güvenlik ve belirlilik ilkelerine dolayısıyla hukuk devleti ilkesine aykırı olduğu, düzenleme yapılırken uzmanlık deneklerinden ve meslek örgütlerinden görüş alınmadığı, düzenlenmenin bilimsel bir çalışmaya dayanmadığı ileri sürülmektedir.

DAVALININ SAVUNMASI:

Dava konusu Yönetmeliğin 3. maddesi ile değiştirilen asıl Yönetmeliğin 19. maddesinin 3. fıkrasına ilişkin olarak; dava konusu değişiklik ile Planlama İstihdam Komisyonu ibaresinin madde metninden çıkarıldığı, yapılan değişikliğin bundan ibaret olduğu, düzenlemenin amacının, yan dal insan kaynağının ülkemizde oldukça kısıtlı olması, yan dal uzmanlığı konusunda önceliğin yan dala ilişkin uzmanlık eğitimine verilmesinin gerekmesi ve yan dal uzmanlık eğitiminin kaliteli bir şekilde verilebilmesi için yeterli uzman kaynağının eğitim kurumlarında mutlaka sağlanması gerekliliği nedeniyle yan dal uzmanlık eğitiminin sürdürülebilirliğinin sağlanması olduğu, yan dal ve ana dalın birlikte çalışmasının ihtiyaç ve zorunluluk olduğu, hizmet gereği kamu hastaneleri ve üniversite

hastanelerinde ana dal ve yan dal uzman kaynağının korunması gerektiği, düzenlemenin eğitim kurumlarında yan dal uzman insan gücünü korumak için yapıldığı, bu eğitim kurumlarının yan dal uzman ihtiyacı karşılandığında yan dal uzmanlarının özel sektörde ana dalda çalışabilecekleri, örneğin ülke ve ilde eğitici ihtiyacı bulunmayan algoloji gibi yan dallarda anadal uzmanlık kadrolarında çalışmasına izin verildiği, düzenlemenin kamu yararı amacı güttüğü savunulmaktadır.

Dava konusu Yönetmeliğin 4. maddesi ile değiştirilen asıl Yönetmeliğin 27. maddesinin 8. fıkrasına ilişkin olarak; kanunkoyucu tarafından, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyenlerin yükümlülükleri ile uyacakları usul ve esasları belirlemek üzere 6698 sayılı Kanun'un yürürlüğe girdiği, bu Kanunla 663 sayılı Kanun Hükmünde Kararnamenin 47. maddesinin yeniden düzenlendiği, bu düzenlemelerin Anayasa Mahkemesince Anayasaya uygun bulunduğu, Anayasaya uygun bulunan bir Kanun hükmünün uygulanacağını gösteren Yönetmelik hükmünün uygulanmasının yargı kararı ile engellenemeyeceği, dava konusu düzenlemenin 6698 sayılı Kanun'a yapılan atıftan ibaret olduğu, kişisel verilere yönelik yeni bir hüküm ihtiva etmediği, davacının iddia ettiğinin aksine hükmün yayımlandığı tarihte Kişisel Veriler Kurulu'nun oluşturulduğu, Kurul tarafından bu alana ilişkin önlemlerin belirlendiği savunulmaktadır.

Dava konusu Yönetmeliğin 5. maddesi ile değiştirilen asıl Yönetmeliğin Ek-1. maddesinin 16. fıkrasına ilişkin olarak; düzenleme ile özel sağlık kuruluşlarında meslek icrasının aynı il içerisinde sınırlandırılmayarak hekimlerin iller arasında çalışmalarına izin verildiği, hükmün hekimlerin aleyhine değil lehine olduğu, düzenlemenin 1219 sayılı Kanun'un 12. maddesi hükmüne aykırı olmadığı, nitekim tabiplerin birden fazla sağlık kuruluşunda çalışmasına yönelik Yönetmelikte süre ve yer yönünden öngörülen kısıtlamaların 1219 sayılı Kanun'un 12. maddesine aykırı bulunarak Danıştayca iptal edildiği savunulmaktadır.

Dava konusu Yönetmeliğin 5. maddesi ile asıl Yönetmeliğe eklenen Ek-1. maddesinin 18. fıkrasına ilişkin olarak; maddede nöbet ve kurumsal sözleşmeye ilişkin düzenleme yapıldığı, özel sağlık kuruluşlarında çalışan tabip ve uzman tabiplerin başka bir özel hastanede çalışmasının sadece nöbetle sınırlandırılmadığı, Yönetmeliğin Ek 1. maddesinin 2. fıkrası ile bulunduğu ilde birden fazla özel sağlık kuruluşunda çalışabilmelerine, Ek 1. maddenin 16. fıkrası kapsamında da iller arası çalışmalarına izin verildiği, bunların yanı sıra nöbet tutarak çalışmanın da hekimlerin lehine bir düzenleme olarak Yönetmeliğe eklendiği, ayrıca hüküm ile hekimlerin tıp merkezlerinde planlama kapsamında kadrolu çalışmaları halinde kurumsal sözleşme yaparak diğer özel sağlık kuruluşlarında

çalışabileceğinin belirtildiği, hekimlerin çalışmasına yönelik herhangi bir kısıtlama getirilmediği, tüm tıp merkezlerinin sabitlenen kadroları doğrultusunda kadrolu çalışma halinde sözleşmeli çalışmanın da söz konusu olabileceğinin kurala bağlandığı, kurumsal sözleşmenin maksadının planlama kapsamındaki kısıtlı tabip insan gücünün özel sektör içinde kullanılabilmesi ve böylece sağlık hizmeti sunumunda verimin, ulaşılabilirliğin ve kalitenin artması olduğu, bu çalışmanın hekimin bilgisi ve isteği dışında olmadığı, kurumsal sözleşme ve hekimin muvafakati şartının getirildiği, hükümde hekimlerin çalışma şartlarını zorlaştıran ya da ağırlaştıran bir düzenleme bulunmadığı, düzenlemenin kamu hizmeti gerekleri gözetilerek yapıldığı savunulmaktadır.

Dava konusu Yönetmeliğin 8. maddesi ile değiştirilen asıl Yönetmeliğin ekinde yer alan EK-9'daki 1 sayılı Liste ve 2 sayılı Liste'ye ilişkin olarak; tıp merkezlerinde yapılabilecek ve yapılamayacak işlemler listesinin, ilgili cerrahi uzmanlık dallarından hekimlerin katılımıyla toplanan komisyon tarafından, Sağlık Uygulama Tebliği ekinde yer alan Ek-2/C ve Ek-2/B Listeleri ve Yönetmeliğin 23. maddesi hükmü baz alınarak belirlendiği, önceki düzenlemede de listenin sayma yoluyla belirlendiği ve bu düzenlemenin Danıştay incelemesinden geçerek hukuka uygun bulunduğu, listenin her bir uzmanlık dalından uzmanlar tarafından ayrı ayrı ve tıp merkezinin standartları esas alınarak belirlendiği, listenin sayma yoluyla belirlenmesinin belirlilik ilkesine uygun olduğu, konunun muhatapları için bilinebilir ve öngörülebilir olması gerektiği savunulmaktadır.

DANIŞTAY TETKİK HÂKİMİ ... DÜŞÜNCESİ: Yürütmenin durdurulması isteminin reddi gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay Onbeşinci Dairesince, Ara Kararına cevap alındıktan sonra incelenmesine karar verilen yürütmenin durdurulması istemi, Ara Kararı cevabının geldiği görülmüş olmakla yeniden incelendi, gereği görüldü:

İNCELEME VE GEREKÇE:

MADDİ OLAY:

15/02/2008 tarihli ve 26788 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmeliğin muhtelif maddelerinde 12/12/2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Yönetmelik ile değişiklik yapılmıştır.

Bu değişiklik üzerine dava konusu düzenlemelerin iptali istemiyle bakılan dava açılmıştır.

İLGİLİ MEVZUAT:

2577 sayılı İdari Yargılama Usulü Kanunu'nun 27. maddesinin 2. fıkrasında, idari işlemin uygulanması hâlinde giderilmesi güç veya olanaksız zararların doğması ve idari işlemin açıkça hukuka aykırı olması koşullarının birlikte gerçekleşmesi durumunda yürütmenin durdurulmasına karar verileceği kuralı yer almıştır.

Anayasanın 56. maddesinin birinci fıkrasında, herkesin, sağlıklı ve dengeli bir çevrede yaşama hakkına sahip olduğu; üçüncü fıkrasında, Devletin, herkesin hayatını, beden ve ruh sağlığı içinde sürdürmesini sağlamak; insan ve madde gücünde tasarruf ve verimi artırarak, işbirliğini gerçekleştirmek amacıyla sağlık kuruluşlarını tek elden planlayıp hizmet vermesini düzenleyeceği; dördüncü fıkrasında da, Devletin, bu görevini kamu ve özel kesimlerdeki sağlık ve sosyal kurumlarından yararlanarak, onları denetleyerek yerine getireceği hükmüne yer verilmiştir.

3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 1. maddesinde; kanunun amacının, sağlık hizmetleri ile ilgili temel esasları belirlemek olduğu, 2. maddesinde; Milli Savunma Bakanlığı hariç bütün kamu kurum ve kuruluşları ile özel hukuk tüzelkişileri ve gerçek kişileri kapsadığı, 3. maddesinin (a) bendinde; sağlık kurum ve kuruluşlarının yurt sathında eşit, kaliteli ve verimli hizmet sunacak şekilde Sağlık ve Sosyal Yardım Bakanlığınca, diğer ilgili bakanlıkların da görüşü alınarak plânlanacağı, koordine edileceği, mali yönden destekleneceği ve geliştirileceği, (c) bendinde; bütün sağlık kurum ve kuruluşları ile sağlık personelinin ülke sathında dengeli dağılımı ve yaygınlaştırılmasının esas olduğu, sağlık kurum ve kuruluşlarının kurulması ve işletilmesinin bu esas içerisinde Sağlık ve Sosyal Yardım Bakanlığınca düzenleneceği, (e) bendinde; tesis edilecek eğitim, denetim, değerlendirme ve oto kontrol sistemi ile sağlık kuruluşlarının tespit edilen standart ve esaslar içinde hizmet vermesinin sağlanacağı, (f) bendinde; herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi maksadıyla, ve bağlı kuruluşlarınca gerekli kayıt ve bildirim sisteminin kurulacağı, bu sistemin, e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabileceği, bu amaçla, nca, bağlı kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemi kurulabileceği, 9. maddesinin (c) bendinde; bütün kamu ve özel sağlık kuruluşlarının tesis, hizmet, personel, kıstaslarını belirlemeye, sağlık kurum ve kuruluşlarını sınıflandırmaya ve sınıflarının değiştirilmesine, sağlık kuruluşlarının amaca uygun olarak teşkilatlanmalarına, sağlık hizmet zinciri oluşturulmasına, hizmet içi eğitim usul ve esasları ile sağlık kurum ve kuruluşlarının koordineli çalışma ve hizmet standartlarının tespiti ve denetimi ile bu Kanunla ilgili diğer hususların Sağlık ve Sosyal Yardım Bakanlığınca çıkarılacak yönetmelikle tespit edileceği belirlenmiştir.

663 sayılı -dava konusu işlemlerin tesis edildiği tarihteki adıyla- ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin yine dava konusu işlemlerin tesis edildiği tarihte yürürlükte olan haliyle 8. maddesinin birinci fıkrasının (j) bendinde; ilgili mevzuat çerçevesinde kişisel verilen korunmasına ve veri mahremiyetinin sağlanmasına yönelik düzenleme yapmak Sağlık Hizmetleri Genel Müdürlüğü'nün görevleri arasında sayılmış, 40. maddesinde ise; Bakanlık ve bağlı kuruluşların görev, yetki ve sorumluluk alanına giren ve önceden kanunla düzenlenmiş konularda idarî düzenlemeler yapabilecekleri hükmüne yer verilmiştir.

Anılan mevzuat hükümlerine dayanılarak, kaynak israfı ve atıl kapasiteye yol açılmaksızın ülke düzeyinde dengeli, verimli ve kaliteli sağlık hizmeti sunulmasını sağlamak üzere ayakta teşhis ve tedavi yapılan özel sağlık kuruluşlarının yapılandırılmaları, ruhsatlandırma işlemleri, faaliyetleri ve faaliyetlerine son verilmesi, denetimleri ve diğer hususlar ile ilgili usûl ve esasları düzenlemek amacıyla Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelik 15/02/2008 tarihli ve 26788 sayılı Resmî Gazete'de yayımlanmıştır.

12/12/2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik ile asıl Yönetmeliğin bazı maddelerinde değişiklik yapılmıştır.

HUKUKİ DEĞERLENDİRME:

Davanın durumu ve uyuşmazlığın hukukî niteliğine göre, 12/12/2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 3. maddesi ile değiştirilen asıl Yönetmeliğin 19. maddesinin 3. fıkrasının, 5. maddesi ile değiştirilen asıl Yönetmeliğin Ek-1. maddesinin 16. fıkrasının, 5. maddesi ile asıl Yönetmeliğe eklenen Ek-1. maddesinin 18. fıkrasının, 8. maddesi ile değiştirilen asıl Yönetmeliğin ekinde yer alan EK-9'daki 1 sayılı Liste ve 2 sayılı Listenin yürütmesinin durdurulması istemine ilişkin olarak; 2577 sayılı İdari Yargılama Usulü Kanununun 27. maddesinde öngörülen koşulların bu aşamada gerçekleşmediği anlaşılmaktadır.

12/12/2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 4. maddesi ile değiştirilen asıl Yönetmeliğin 27. maddesinin 8. fıkrasının yürütmesinin durdurulması istemi incelendiğinde:

15/02/2008 tarihli ve 26788 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmeliğin 27. maddesinin 8. fıkrasında; "Sağlık kuruluşları,

istenecek tıbbi kayıtları, belirlenen formata uygun şekilde ve belirli aralıklarla Bakanlığa gönderir." hükmü yer almakta iken; dava konusu değişiklik ile, "Sağlık kuruluşları tarafından kayıt altına alınan kişisel sağlık verileri, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununa uygun bir şekilde işlenir ve Bakanlıkça belirlenen usul ve esaslara uygun bir şekilde merkezi sağlık veri sistemine aktarılır. Bakanlık tarafından kurulan kayıt ve bildirim sistemine ve Bakanlıkça yapılacak diğer iş ve işlemlere esas olmak üzere, istenilen bilgi ve belgelerin Bakanlığa gönderilmesi zorunludur." şeklinde yeniden düzenlenmiştir.

Anılan değişiklik ile sağlık kuruluşları tarafından kayıt altına alınan kişisel sağlık verilerinin, 6698 sayılı Kişisel Verilerin Korunması Kanununa uygun bir şekilde işleneceği ve Bakanlıkça belirlenen usul ve esaslara uygun bir şekilde merkezi sağlık veri sistemine aktarılacağı kuralına yer verilmiştir.

07/04/2016 tarih ve 29677 sayılı Resmî Gazete'de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu, Türkiye Büyük Millet Meclisi'ne sunulan genel gerekçesinden de anlaşılacağı üzere, kişisel verilerin korunması konusunun pek çok sektörü ve kamu ya da özel kurumu ilgilendirmesi nedeniyle bir "çerçeve kanun" olarak hazırlanmıştır.

Bu Kanuna neden ihtiyaç duyulduğunu açıklayan genel gerekçede, Türk Ceza Kanunu'nun 135. ve devamı maddelerinde kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa edilmesi fiillerinin suç olarak düzenlendiği ve yaptırıma bağlandığı, ancak kişisel verilerin işlenmesine yönelik özel bir kanun bulunmaması sebebiyle, bu fiillerin ne zaman hukuka aykırı ne zaman hukuka uygun olduğunun belirlenmesinde tereddütler yaşandığı vurgulanmaktadır.

Ayrıca 2010 yılında Anayasa'nın 20. maddesinde yapılan düzenlemeyle kişisel verilerin korunması temel bir insan hakkı olarak güvence altına alınmış ve konuya ilişkin usul ve esasların kanunla düzenleneceği öngörülmüştür.

Genel gerekçede, kişisel verilerin korunmasına yönelik bir kanunî düzenleme olmamasının uluslararası ilişkiler açısından da sorunlar yarattığı, EUROPOL, EUROJUST gibi Avrupa kurumları ile ilişkilerin sekteye uğradığı, sağlık kuruluşlarınca tutulan kişisel verilerin güvenliğinin sağlanmasında yeterli yasal önlem olmamasının Avrupa İnsan Hakları Mahkemesince özel hayatın gizliliğine müdahale olarak kabul edildiği ve bu nedenle ihlal kararları verildiği belirtilmektedir. Yine genel gerekçede, bu Kanunun Türkiye'nin Avrupa Birliği'ne üyelik süreci açısından da önemine dikkat çekilmekte, Türkiye'nin, Avrupa Konseyi tarafından tüm üye ülkelerde kişisel verilerin aynı standartlarda korunması ve sınır ötesi veri akışı ilkelerinin belirlenmesi amacıyla hazırlanan 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"ne de 1981 yılından itibaren taraf olduğu ifade edilmektedir.

Bütün bu hususlardan anlaşılacağı üzere 6698 sayılı Kanun, kişisel verilerin korunması konusunda önemli bir yasal boşluğu doldurmak amacıyla kabul edilen çerçeve niteliğinde bir yasal düzenlemedir. Genel gerekçede yer verilen şu tespit Kanun ile oluşturulan Kişisel Verileri Koruma Kurulu'nun genel kontrol ve denetleme işlevlerine dikkat çekmesi bakımından önemlidir: "Ülkemizde kişisel verilerin işlenmesi sürecini kontrol edecek ve denetleyecek bir kurum bulunmamaktadır. Bunun bir sonucu olarak halen kişisel veriler yeterli düzenleme ve denetime tabi olmaksızın, birçok kişi veya kurum tarafından kullanılabilmekte ve bu durum bazı hak ihlallerinin yaşanmasına sebep olabilmektedir."

Bu bağlamda, 6698 sayılı Kanununun 21. maddesi hükümlerine göre oluşturulan Kişisel Verileri Koruma Kurulu'nun görev ve yetkileri, aynı Kanun'un 22. maddesiyle belirlenmiştir. 22. maddenin 1. fıkrasının (h) bendinde "Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek" hükmüne yer verilmiştir.

Anılan Kanun'un, "Özel nitelikli kişisel verilerin işleme şartları" başlıklı 6. maddesinin 1. fıkrasında, dava konusu Yönetmelikle düzenlenen, sağlık verilerinin de özel nitelikli kişisel veri olduğu belirtilmiş; maddenin 4. fıkrasında, "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü getirilmiştir.

Anılan Kanun hükümleri çerçevesinde, Dairemizin 03/07/2018 tarihli Ara Kararı ile davalı idareden, kişisel verilere ilişkin dava konusu düzenleme yapılırken Kişisel Verileri Koruma Kurulu'nun görüşünün alınıp alınmadığı sorulmuş, davalı idare ara kararı cevabında, Kişisel Sağlık Verilerinin Korunması ve Mahremiyetinin Sağlanması Hakkında Yönetmelik için Kişisel Verileri Koruma Kurumu'ndan görüş sorulduğu, 6698 sayılı Kanun'un 22. Maddesinin birinci fıkrasının (h) bendi uyarınca tesis edilen Kurul kararı doğrultusunda Bakanlıklarına görüş bildirildiği, dava konusu düzenlemenin de bu görüş doğrultusunda yapıldığı yönünde açıklamada bulunmuştur.

Ara Kararı cevabı ekinde yer alan evraktan, 20/10/2016 tarihli ve 29863 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verilerinin Korunması ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'te değişiklik yapılması düşünüldüğünden bahisle bu değişikliklere ilişkin olarak Kişisel Verileri Koruma Kurulu'ndan görüş istendiği ve Kurulun da bu değişikliklere yönelik davalı idareye görüş verdiği, bu görüşün dava konusu düzenlemeye yönelik verilmiş bir görüş olmadığı anlaşılmaktadır.

Buna göre, anılan Kanun hükümleri çerçevesinde, dava konusu düzenleme tesis edildiğinde özel nitelikli kişisel veri olarak kabul edilen sağlık verilerinin işlenmesinde alınması gerekli olan önlemlerin Kişisel Verileri Koruma Kurulu tarafından belirlenmediği ve Kanun'un 22. maddesinin 1.

fıkrasının (h) bendine göre diğerkurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında Kurul görüşü alınmadan dava konusu düzenlemenin tesis edildiği görülmekte olup, bu yönüyle dava konusu Yönetmelik hükmünde hukuka uygunluk bulunmamaktadır.

Nitekim, davalı idare tarafından, 6698 sayılı Kişisel Verilerin Korunması Kanununa istinaden hazırlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik 20/10/2016 tarihli ve 29863 sayılı Resmî Gazete'de yayımlanmış, anılan Yönetmeliğin muhtelif maddelerinin ve tümünün yürütmesinin durdurulması ve iptali istemiyle açılan davada, Dairemizin 06/07/2017 tarihli ve E.2016/10500 sayılı kararı ile "Yukarıda yer verilen genel gerekçe ve Kanun hükümlerine göre, Kişisel Verileri Koruma Kurulu'nun kişisel verilerin korunması konusunda genel nitelikte bir kontrol ve denetim yetkisine sahip olduğu, diğerkurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hükümler içeren mevzuat taslakları hakkında Kişisel Verileri Koruma Kurulu'ndan görüş alınmasının şart olduğu, Kişisel Verileri Koruma Kurulu'nun kontrol ve denetiminden geçirilmeksizin hazırlanan ve 20/10/2016 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe giren dava konusu düzenlemede bu nedenle mevzuata ve hukuka uygunluk bulunmadığı sonucuna ulaşılmıştır." gerekçesiyle 20/10/2016 tarih ve 29863 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin yürütmesinin durdurulmasına karar verilmiştir.

Bu durumda, 6698 sayılı Kişisel Verilerin Korunması Kanunu'na göre sağlık gibi özel nitelikli verilerin işlenmesinde uyulacak önlemleri belirlemekle yetkili olan Kişisel Verileri Koruma Kurulu tarafından bu alana ilişkin yeterli önlemler belirlenmeden ve mevzuat taslağı hakkında Kurul görüşü alınmadan tesis olunan dava konusu düzenlemede hukuka uyarlık bulunmamaktadır.

Anılan düzenlemenin uygulanması halinde giderilmesi güç veya olanaksız zararların doğmasına yol açacağı sonucuna ulaşılmıştır.

KARAR SONUCU:

Açıklanan nedenlerle,

1. 2577 sayılı Kanunun 27. Maddesinde öngörülen koşulların birlikte gerçekleşmiş bulunduğu anlaşıldığından, 12/12/2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 4. maddesi ile değiştirilen asıl Yönetmeliğin 27. maddesinin 8. fıkrasının YÜRÜTMESİNİN DURDURULMASINA,

2. 2577 sayılı Kanununun 27. maddesinde öngörülen koşulların bu aşamada gerçekleşmediği anlaşıldığından, 12/12/2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 3. maddesi ile değiştirilen asıl Yönetmeliğin 19. maddesinin 3. fıkrasının, 5. maddesi ile değiştirilen asıl Yönetmeliğin Ek-1. maddesinin 16. fıkrasının, 5. maddesi ile asıl Yönetmeliğe eklenen Ek-1. maddesinin 18. fıkrasının, 8. maddesi ile değiştirilen asıl Yönetmeliğin ekinde yer alan EK-9'daki 1 sayılı Liste ve 2 sayılı Listenin YÜRÜTMESİNİN DURDURULMASI İSTEMİNİN REDDİNE,

3. Bu kararın tebliğini izleyen günden itibaren 7 (yedi) gün içinde İdari Dava Daireleri Kurulu'na itiraz yolu açık olmak üzere, 15/01/2019 tarihinde oybirliğiyle karar verildi.

Danıştay Kararı - 15. Daire (E. 2018/251)

Danıştay Kararı - 15. D., E. 2018/251 K. YD T. 21.2.2018

Dava konusu düzenlemenin üst normlara ve hukuka uygun olduğu, yürütmenin durdurulması isteminin ve davanın reddi gerektiği savunulmaktadır.

Danıştay Tetkik Hakimi:

Düşüncesi: Yürütmenin durdurulması isteminin kabulü gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA Karar veren Danıştay Onbeşinci Dairesince davalı idarelerin birinci savunmaları alındıktan sonra incelenmesine karar verilen yürütmenin durdurulması istemi, savunmaların verildiği görülmüş olmakla incelenerek işin gereği görüşüldü: Dava, 24/11/2017 tarih ve 30250 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin tamamı ile anılan Yönetmelikle değiştirilen 20/10/2016 tarih ve 29863 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin; 15. maddesinin birinci ve beşinci fıkralarının, 9. maddesinin birinci fıkrasının, 7. maddesinin dördüncü fıkrasının, 6. maddesinin ikinci fıkrasının, 18. maddesinin, 11. maddesinin üçüncü fıkrasının ve 4. maddesinin yürütmesinin durdurulması ve iptali istemiyle açılmıştır.

T.C. DANIŞTAY ONBEŞİNCİ DAİRE

Esas No: 2018/251

Davacılar ve Yürütmenin Durdurulmasını İsteyenler:1

2-

3-

Vekilleri:

Davalılar: 1-

Vekilleri:

2-

Vekili:

İstemin Özeti: 24/11/2017 tarih ve 30250 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin tamamı ile anılan Yönetmelikle değiştirilen 20/10/2016 tarih ve 29863 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin; 15. maddesinin birinci ve beşinci fıkralarının, 9. maddesinin birinci fıkrasının, 7. maddesinin dördüncü fıkrasının, 6. maddesinin ikinci fıkrasının, 18. maddesinin, 11. maddesinin üçüncü fıkrasının ve 4. maddesinin iptali ve yürütmesinin durdurulması istenilmektedir.

Savunmaların Özeti: Dava konusu düzenlemenin üst normlara ve hukuka uygun olduğu, yürütmenin durdurulması isteminin ve davanın reddi gerektiği savunulmaktadır.

Danıştay Tetkik Hakimi:

Düşüncesi: Yürütmenin durdurulması isteminin kabulü gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay Onbeşinci Dairesince davalı idarelerin birinci savunmaları alındıktan sonra incelenmesine karar verilen yürütmenin durdurulması istemi, savunmaların verildiği görülmüş olmakla incelenerek işin gereği görüşüldü:

Dava, 24/11/2017 tarih ve 30250 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin tamamı ile anılan Yönetmelikle değiştirilen 20/10/2016 tarih ve 29863 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin; 15. maddesinin birinci ve beşinci fıkralarının, 9. maddesinin birinci fıkrasının, 7. maddesinin dördüncü fıkrasının, 6. maddesinin ikinci fıkrasının, 18. maddesinin, 11. maddesinin üçüncü fıkrasının ve 4. maddesinin yürütmesinin durdurulması ve iptali istemiyle açılmıştır.

Davacılar tarafından, dava konusu Yönetmelik ile Danıştay tarafından yürütmesi durdurulan ve uygulanma olanağı kalmayan Kişisel Sağlık Verilerinin İşlenmesi Ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'te değişiklik yapıldığı, bu eksikliğin tüm maddeleri yoklukla malûl kıldığı,

Dava konusu hükümler ile kişisel sağlık verisi sahiplerinin verilerini yönetme ve silme hakkının Yönetmelik'ten çıkarıldığı, kişisel veri sahibi gerçek kişinin temel haklarından birinin kendisine ait verinin silinmesini talep etme hakkı olduğu, bu hakkın Anayasa'da herhangi bir sınırlama getirilmeden mutlak bir hak olarak düzenlendiği, bu hakkın verilerin tutulduğu sistemlere erişme,

verilerin düzeltilmesini talep etme, aktarımına itiraz etme, silinmesini isteme gibi haklarının güvence altına alınmasını kapsadığı, esas Yönetmelik'te yer alan "her vatandaşın kendisine ait sağlık kayıtlarını yönetmek hakkının" daraltılarak "kendisine ait sağlık kayıtlarını görüntülemek" şekline dönüştürüldüğü, "kendisine ait sağlık verilerini yönetebilir, bu verileri silebilir" hükmünün ise "kendisine ait sağlık verilerini görüntüleyebilir" olarak değiştirildiği,

108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Sözleşmenin 6. maddesinde sağlık verilerinin özel kategoride hassas veriler olarak kabul edildiği ve iç hukukta uygun güvenceler sağlanmadıkça otomatik işleme tabi tutulmalarının yasak olduğu, bu güvencelerin kişisel veri sahiplerinin bu verilerin tutulduğu sistemlere erişme, verilerin düzeltilmesini talep etme, aktarımına itiraz etme ve silinmesini isteme gibi hakları temin eden hukuki düzenlemelerin hayata geçirilmesi olduğu, Sözleşmenin 5. maddesinin (e) bendinde yer alan, otomatik işleme tabi tutulan kişisel verilerin "Kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkân veren bir biçimde saklanır." hükmü gereği kaydedilme amacı ya da işleme şartları ortadan kalkan verilerin derhal silinmesi gerektiği, veri sahibinin bu yönde bir talebi varsa silmenin veri sorumlusu açısından zorunlu olduğu, ilgili kişinin işlenen kişisel verilerinin tümünden bilgi sahibi olması, sisteme erişim, kişisel verilerinin silinmesini veya bilgilerinin düzeltilmesini isteme ve işlenen kişisel verilerin hukuki dayanağının, amacının ve aktarım yapılan üçüncü kişileri bilme hakkının 6698 sayılı Kanun'un 11. maddesinde düzenlenen "ilgili kişinin hakları" arasında sayıldığı belirtilerek dava konusu Yönetmelik değişiklikleri ile sağlık verisi sahibi kişilerin bu haklarını temin etmeye yönelik bir düzenlemeye yer verilmediği,

Yönetmeliğin uygulamayı somut, objektif ve denetlenebilir kurallarla düzenlemediği, idare tarafından ne zaman çıkarılacağı ve içeriğinin ne olacağı belirsiz olan idari tasarruflara atıf yapmakla yetinildiği, 7. maddesinin dördüncü fıkrası, 6. maddesinin ikinci fıkrası, 11. maddesinin üçüncü fıkrası ve 18. maddesinde yapılan değişikliklerle veri güvenliğinin sağlanması için alınması gerekli tedbirlerin ne olduğu kararının idareye veya veri sorumlularına verildiği, bu kararların ilgili kişi ya da kamuoyu nezdinde denetlenebilirliğinin olmayacağı, idari ve teknik tedbirlerin belirlenmemesinin uygulamada birlik sağlanamamasına ve farklı yöntemlerin uygulanmasına neden olacağı,

Kişisel sağlık verilerinin işlenmesine ilişkin süreçte denetim ve gözlem görevi olan 'bilgi güvenliği yetkilisi' ile siber saldırılara karşı sistemi koruma görevi bulunan 'siber olaylara müdahale ekibi' kavramlarının Yönetmelikten çıkarıldığı, zaten yetersiz olan düzenlemelerin içinin daha da boşaltılmış olduğu,

Kişisel verilerin mahremiyetinin korunması için gereken tedbirlerin neler olduğunun düzenlenmediği, subjektif ve soyut ifadelerle içi doldurulmamış tedbirlerin alınacağı ifade edilmekle yetinildiği, verilerin kanuni olmayan yöntemlerle işlenmesi halinde sorumlulara uygulanacak yaptırımlara da yer verilmediği ileri sürerek düzenlemenin yürütmesinin durdurulması ve iptali istenilmektedir.

Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek amacıyla düzenlenen 24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu, Türkiye Büyük Millet Meclisi'ne sunulan genel gerekçesinden de anlaşılacağı üzere, kişisel verilerin korunması konusunun pek çok sektörü ve kamu ya da özel pek çok kurumu ilgilendirmesi nedeniyle bir "çerçeve kanun" olarak hazırlanmıştır.

Bu Kanuna neden ihtiyaç duyulduğunu açıklayan genel gerekçede, Türk Ceza Kanunu'nun 135 ve devamı maddelerinde kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa edilmesi fiillerinin suç olarak düzenlendiği ve yaptırıma bağlandığı, ancak kişisel verilerin işlenmesine yönelik özel bir kanun bulunmaması sebebiyle, bu fiillerin ne zaman hukuka aykırı ne zaman hukuka uygun olduğunun belirlenmesinde tereddütler yaşandığı vurgulanmaktadır. Ayrıca 2010 yılında Anayasa'nın 20. maddesinde yapılan düzenlemeyle kişisel verilerin korunması temel bir insan hakkı olarak güvence altına alınmış ve konuya ilişkin usul ve esasların kanunla düzenleneceği öngörülmüştür.

Genel gerekçede, kişisel verilerin korunmasına yönelik bir kanuni düzenleme olmamasının uluslararası ilişkiler açısından da sorunlar yarattığı, EUROPOL, EUROJUST gibi Avrupa kurumları ile ilişkilerin sekteye uğradığı, sağlık kuruluşlarınca tutulan kişisel verilerin güvenliğinin sağlanmasında yeterli yasal önlem olmamasının Avrupa İnsan Hakları Mahkemesince özel hayatın gizliliğine müdahale olarak kabul edildiği ve bu nedenle ihlal kararları verildiği belirtilmektedir. Yine genel gerekçede, bu Kanunun Türkiye'nin Avrupa Birliği'ne üyelik süreci açısından da önemine dikkat çekilmekte, Türkiye'nin, Avrupa Konseyi tarafından tüm üye ülkelerde kişisel verilerin aynı standartlarda korunması ve sınır ötesi veri akışı ilkelerinin belirlenmesi amacıyla hazırlanan 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"ne de 1981 yılından itibaren taraf olduğu ifade edilmektedir.

Bütün bu hususlardan anlaşılacağı üzere 6698 sayılı Kanun, kişisel verilerin korunması konusunda önemli bir yasal boşluğu doldurmak amacıyla kabul edilen çerçeve niteliğinde bir yasal düzenlemedir. Genel gerekçede yer verilen şu tespit Kanun ile oluşturulan Kişisel Verileri Koruma

Kurulu'nun genel kontrol ve denetleme işlevlerine dikkat çekmesi bakımından önemlidir: "Ülkemizde kişisel verilerin işlenmesi sürecini kontrol edecek ve denetleyecek bir kurum bulunmamaktadır. Bunun bir sonucu olarak halen kişisel veriler yeterli düzenleme ve denetime tabi olmaksızın, birçok kişi veya kurum tarafından kullanılabilmekte ve bu durum bazı hak ihlallerinin yaşanmasına sebep olabilmektedir."

6698 sayılı Kanununun 21. maddesi hükümlerine göre oluşturulan Kişisel Verileri Koruma Kurulu'nun görev ve yetkileri, aynı Kanun'un 22. maddesiyle belirlenmiştir. 22. maddenin birinci fıkrasının (h) bendinde "Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek" hükmüne yer verilmiştir.

Anılan Kanun'un, "Özel nitelikli kişisel verilerin işleme şartları" başlıklı 6. maddesinin birinci fıkrasında, dava konusu Yönetmelikle düzenlenen, sağlık verilerinin de özel nitelikli kişisel veri olduğu belirtilmiş; maddenin dördüncü fıkrasında, "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü getirilmiştir.

Dava dosyasının incelenmesinden; mülga 11/10/2011 tarihli ve 663 sayılı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 8. maddesinin birinci fıkrasının (j) bendi ile 47. maddesi ve 07/05/1987 tarihli ve 3359 sayılı Sağlık Hizmetleri Temel Kanununun 3. maddesinin birinci fıkrasının (f) bendine dayanılarak hazırlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'in 20/10/2016 tarih ve 29863 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girdiği ve anılan Yönetmelik ile; kişisel verilerin korunması ve veri mahremiyetinin sağlanmasına, kişisel sağlık verilerini toplama, işleme, aktarma, bu verilere erişim için kurulacak sisteme, kişisel sağlık verisi kaydı tutulan sistemlerin güvenliği ve denetimi ile sağlık hizmeti sunumundaki personel hareketlerinin Bakanlığa bildirilmesine ilişkin işlemlerde uyulacak usul ve esasların düzenlendiği,

Anılan Yönetmeliğin tamamının ve muhtelif maddelerinin iptali istemiyle davacılarından ile tarafından açılan davada, Dairemizin 06/07/2017 tarihli ve E:2016/10500 sayılı kararı ile Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin tamamının yürütmesinin durdurulmasına karar verildiği,

Söz konusu Karar gerekçesinde ise, "dava konusu Yönetmeliğin Resmî Gazete'de yayımlandığı tarih olan 20/10/2016'da Kişisel Verileri Koruma Kurulu'nun henüz oluşturulmadığı, dolayısıyla 6698 sayılı Kanun'un 6. maddesinin dördüncü fıkrasında belirtilen yeterli önlemlerin Kurul tarafından belirlenmediği ve Kanun'un 22. maddesinin birinci fıkrasının (h) bendine göre diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında Kurul

görüşü alınmadan dava konusu düzenlemenin tesis edildiği, Kanun'un genel gerekçesi ve Kanun hükümlerine göre, Kişisel Verileri Koruma Kurulu'nun kişisel verilerin korunması konusunda genel nitelikte bir kontrol ve denetim yetkisine sahip olduğu, diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hükümler içeren mevzuat taslakları hakkında Kişisel Verileri Koruma Kurulu'ndan görüş alınmasının şart olduğu, Kişisel Verileri Koruma Kurulu'nun kontrol ve denetiminden geçirmeksizin hazırlanan ve 20/10/2016 tarihinde Resmî Gazete'de yayımlanarak yürürlüğe giren dava konusu düzenlemede bu nedenle mevzuata ve hukuka uygunluk bulunmadığı" tespitlerine yer verildiği,

Ancak anılan kararının ardından davalı tarafından Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik ile hakkında yürütmenin durdurulması kararı verilen esas Yönetmeliğin muhtelif maddelerinde değişiklik yapılarak 24/11/2017 tarih ve 30250 sayılı Resmî Gazete'de yayımlandığı ve görülmekte olan davanın açıldığı anlaşılmaktadır.

Anayasanın 138. maddesinin son fıkrasında "Yasama ve yürütme organları ile idare, mahkeme kararlarına uymak zorundadır; bu organlar ve İdare, mahkeme kararlarını hiçbir suretle değiştiremez ve bunların yerine getirilmesini geciktiremez" kuralı yer almaktadır.

Öte yandan, 2577 sayılı İdari Yargılama Usulü Kanununun 28. maddesinde; "Danıştay, bölge idare mahkemeleri, idare ve vergi mahkemelerinin esasa ve yürütmenin durdurulmasına ilişkin kararlarının icaplarına göre idare, gecikmeksizin işlem tesis etmeye veya eylemde bulunmaya mecburdur. Bu süre hiçbir şekilde kararın idareye tebliğinden başlayarak otuz günü geçemez. Ancak, haciz veya ihtiyati haciz uygulamaları ile ilgili davalarda verilen kararlar hakkında, bu kararların kesinleşmesinden sonra idarece işlem tesis edilir." kuralına yer verilmiştir.

Bir düzenleyici işlemin iptaline karşı dava açılması durumunda yargı organlarınca düzenleyici işlemin ilgili maddesinin yürütülmesinin durdurulması ve iptali yolunda verdiği kararlar sonucunda oluşan hukuksal boşluk nedeniyle o alanın yeniden düzenlenmesi ve hukuk devletinin gereği olarak idari yargı merciielerince verilen kararların, fiili ve hukuki imkânsızlık dışında gecikmeksizin yerine getirilmesi gerekmektedir. Aksine bir davranışın, yasama ve yürütme organları ile idarenin mahkeme kararlarına uymak zorunda oldukları yolundaki Anayasanın 138. maddesine aykırı olacağı açıktır. Böylece idarenin, uygulanmasında maddi ve hukuki imkânsızlık bulunanlar dışında yargı kararlarını "aynen" ve "gecikmeksizin" uygulamaktan başka bir seçeneği bulunmamaktadır. Başka bir deyişle, yargı kararlarının uygulanması bakımından idare "bağlı yetki" içerisinde bulunmaktadır.

Davalı idare savunmasında; 6698 sayılı Kanun uyarınca Kişisel Verileri Koruma Kurulu üyelerinin ancak 2017 yılının Ocak ayında belirlenebildiği ve bu nedenle Esas Yönetmelik hakkında Kurul görüşünün alınmasının mümkün olmadığı, Kişisel Verileri Koruma Kurulu üyelerinin belirlenmesini müteakip görüşmelere başlandığı, Yönetmelik hakkında Kurul üyelerinden şifahi görüşlerin alındığı, toplantılarda dile getirilen görüşler çerçevesinde Yönetmeliğin revize edilmesine yönelik çalışmalara başlanıldığı, hazırlanan Esas Yönetmelikte değişiklik yapmak üzere hazırlanan Yönetmelik Taslağının Kişisel Verileri Koruma Kuruluna gönderildiği ve görüşünün alındığı, Kurul görüşü çerçevesinde revize edilen Taslağın Kurula ikinci kez gönderildiği ve görüşlerin tamamının Taslağa yansıtıldığı ve Esas Yönetmelik'te gerekli değişikliklerin yapıldığı, Esas Yönetmelik hakkında açılan davada henüz yürütmenin durdurulması kararı verilmeden önce kararda gerekçe gösterilen "Kurul'dan görüş alınmamış olması" eksikliğinin giderilmesine yönelik çalışmalara başlanmış olduğu, yürütmenin durdurulması kararının verildiği 06.07.2017 tarihinden önce Kurul görüşü alındığı, dolayısı ile yürütmenin durdurulması kararı henüz verilmeden, gecikmeksizin işlem tesis edildiği ve yürütmenin durdurulması kararının gereğinin yerine getirildiği, eksik bulunan hususun tamamlanmış olduğu iddia edilmekte ise de, Dairemizce verilen yürütmenin durdurulması kararı üzerine Kişisel Verileri Koruma Kurulundan görüş alınarak oluşturulduğu iddia edilen yeni bir Yönetmeliğin Resmî Gazete'de yayımlanmadığı, hakkında yürütmenin durdurulması kararı verilen Esas Yönetmelikte yapılan kısmi değişiklik metninin yayımlandığı görülmektedir.

Buna göre, bir düzenlemenin tamamının yürütülmesinin durdurulması veya iptal edilmesi üzerine, bu kararın gereğini yerine getirecek yeni bir düzenleme yürürlüğe konulmadığı sürece, önceki düzenlemede kısmi değişiklikler yapılmak suretiyle hukuka aykırılığı saptanmış olan düzenlemenin canlandırılması hukuken mümkün değildir. Zira düzenlemenin tamamının yürütülmesinin durdurulması veya iptali üzerine bu düzenlemede kısmen değişikliğe gidilmesi durumunda, değiştirilmeyen hükümlerin hukuken sakat olacağı da açıktır.

Bu durumda, Anayasada ve 2577 sayılı Kanun'da yer alan emredici kurallar karşısında, idarenin, yürütmenin durdurulması kararının gereğini yerine getirecek şekilde düzenleme yapması gerekirken, maddi ve hukuki koşullara göre uygulanabilir nitelikte olan bir yargı kararını aynen ve gecikmeksizin uygulamaktan kaçınarak, hakkında yürütmenin durdurulması kararı verilen Yönetmelikte kısmi değişiklikler yaparak yürürlüğe koymasında hukuka uygunluk bulunmamaktadır.

Açıklanan nedenlerle, olayda 2577 sayılı İdari Yargılama Usulü Kanunu'nun 4001 sayılı Yasa ile değişik 27. maddesinin ikinci fıkrasında sayılan koşullar gerçekleşmiş olduğundan yürütmenin

durdurulması isteminin kabulüne, 24/11/2017 tarih ve 30250 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin yürütmesinin durdurulmasına, bu kararın tebliğini izleyen günden itibaren yedi gün içinde İdari Dava Daireleri Kurulu'na itiraz yolu açık olmak üzere 09/10/2018 tarihinde oybirliğiyle karar verildi.

Danıştay Kararı - 8. Daire (E. 2017/7307)

Danıştay Kararı - 8. D., E. 2017/7307 K. 2020/3063 T. 2.7.2020

Temyiz İsteminde Bulunan (Davalı): Türkiye Kamu Hastaneleri Kurumu

Vekili: Av. K1

Karşı Taraf(Davacı): K2

Vekili: Av. K3

İstem Özet: Batman İdare Mahkemesinin 12/02/2015 gün ve E:2014/15, K:2015/322 sayılı kararının hukuka aykırı olduğu öne sürülerek, 2577 sayılı Kanunun 49. maddesi uyarınca temyizen incelenerek bozulması istemidir.

Savunmanın Özeti: Savunma verilmemiştir.

Danıştay Tetkik Hakimi: K4

Düşüncesi: İstem kabulü ile Mahkeme kararının bozulması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Hüküm veren Danıştay Sekizinci Dairesince işin gereği görüldü:

Dava, davacı vekili tarafından, davacının geçirmiş olduğu trafik kazası sebebiyle tedavi gördüğü Siirt Devlet Hastanesi'nde bulunan davacıya ait tüm tedavi evrakının bir örneğinin trafik sigortasına başvurmak üzere verilmesi istemiyle yapılan başvurunun reddine ilişkin işlemin iptali istemiyle açılmıştır.

İdare Mahkemesince, davacının avukat olan vekilince, sigorta şirketine başvurulacağı şeklinde sebebi açıklanmak ve ekinde vekaletname sunmak suretiyle tüm tedavi evrakının onaylı birer örneğinin verilmesi istemiyle yaptığı başvurunun, istenilen belgelerin yasalarca istisna kapsamında tutulan bilgi ve belgelerden olmaması nedeniyle 1136 sayılı Avukatlık Kanununun 2. maddesi gereğince kabulü gerektiğinden aksi yönde tesis edilen dava konusu işlemde hukuka uygunluk bulunmayarak dava konusu işlemin iptaline karar verilmiştir.

Türkiye Cumhuriyeti Anayasa'sının "Özel hayatın gizliliği" başlıklı 20/3. maddesinde, "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini

talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmü yer almaktadır.

07.04.2016 tarih ve 29677 sayılı Resmi Gazete'de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Amaç" başlıklı 1. maddesinde, "Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir."; "Tanımlar" başlıklı 3. maddesinin 1. fıkrasında; "a) Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı, (...) d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi, e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi, (...) ifade eder." ; "Özel nitelikli kişisel verilerin işleme şartları" başlıklı 6. maddesinin 1. fıkrasında, "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir."; 2. fıkrasında, "Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır."; 3. fıkrasında ise, "Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir." hükümlerine yer verilmiştir.

4982 sayılı Bilgi Edinme Hakkı Kanunu'nun "Bilgi verme yükümlülüğü" başlıklı 5/1. maddesinde, "Kurum ve kuruluşlar, bu Kanunda yer alan istisnalar dışındaki her türlü bilgi veya belgeyi başvuranların yararlanmasına sunmak ve bilgi edinme başvurularını etkin, süratli ve doğru sonuçlandırmak üzere, gerekli idari ve teknik tedbirleri almakla yükümlüdürler." hükmüne yer verilmiş; öte yandan bilgi edinme hakkının sınırlarının düzenlendiği dördüncü bölüm altında yer alan "Özel hayatın gizliliği" başlıklı 21. maddesinde ise, "Kişinin izin verdiği haller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması halinde kişinin sağlık bilgileri ile özel ve aile hayatına,

şeref ve haysiyetine, mesleki ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır. Kamu yararının gerektirdiği hallerde, kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir." düzenlemesine yer verilmek suretiyle kişilerin sağlık bilgilerinin anılan Kanun kapsamı dışında yer aldığı ifade edilmiştir.

1136 sayılı Avukatlık Kanunu'nun "Avukatlığın amacı" başlıklı 2. maddesinin 3. fıkrasında, "Yargı organları, emniyet makamları, diğer kamu kurum ve kuruluşları ile kamu iktisadi teşebbüsleri, özel ve kamuya ait bankalar, noterler, sigorta şirketleri ve vakıflar avukatlara görevlerinin yerine getirilmesinde yardımcı olmak zorundadır. Kanunlarındaki özel hükümler saklı kalmak kaydıyla, bu kurumlar avukatın gerek duyduğu bilgi ve belgeleri incelemesine sunmakla yükümlüdür. Bu belgelerden örnek alınması vekaletname ibrazına bağlıdır. (...)" hükmüne yer verilmiştir.

Dosyanın incelenmesinden, davacı vekili tarafından, davacının 2011 yılında trafik kazası geçirmesi sebebiyle Siirt Devlet Hastanesi'nde tedavi gördüğünden bahisle, davacıya ait tüm tedavi evrakının bir örneğinin trafik sigortasına verilmek üzere 1136 sayılı Avukatlık Kanunu'nun 2. maddesine dayanılarak 26.11.2013 tarihli dilekçe ile istenilmesi üzerine, dilekçe ile talep edilen bilgi ve belgelerin Mahkemece resmi yazıyla evrak talep edildiği takdirde verilebileceği gerekçesiyle 29.11.2013 tarih ve 4187 sayılı işlemle reddedilmesi üzerine bakılmakta olan davanın açıldığı anlaşılmaktadır.

Yukarıda yer verilen 6698 sayılı Kanun'un 3. maddesine göre kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Anayasa Mahkemesinin kararlarında da belirtildiği üzere "... adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler" kişisel veri olarak kabul edilmektedir.

6698 sayılı Kanunda kişisel verilerin işlenmesine ilişkin genel şartlar ortaya konulmakla birlikte yasa koyucunun takdir yetkisi kapsamında kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri gibi özel nitelikli kişisel verilerin işlenme şartlarının ayrı bir düzenlemeye tabi tutulduğu, bu düzenlemeyle birtakım kişisel verilerin özel hukuki koruma altına alındığı görülmektedir.

Özel nitelikli kişisel verilerin işlenebilmesi için kural olarak ilgililerin açık rızasının bulunması gerekmektedir. Ancak 6698 sayılı Kanun'un 6. maddesinin 3. fıkrasında, sağlık ve cinsel hayat dışındaki özel nitelikli kişisel verilerin, "Kanunlarda öngörülen hallerde" ilgililerin açık rızası aranmaksızın da işlenebileceği belirtilmek suretiyle anılan kuralın istisnasına yer verilmiştir. Bununla birlikte sağlık ve cinsel hayata ilişkin kişisel verilerin ise bu istisnadan da istisna edilerek ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği ifade edilmek suretiyle, önemine binaen "Kanunlarda öngörülen hallerde" şeklinde bir ifade biçimiyle yetinilmeyerek, bu verilerin ilgililerin açık rızası aranmaksızın işlenebileceği hallerin doğrudan Kanun maddesinde düzenlendiği görülmektedir.

Şu halde, kökeni Roma Hukukuna dayanan ve günümüzde genel hukuk kaidesi olarak kabul gören "istisna içerikli hükümlerin dar yorumlanması" (singularia non sunt extenda) ilkesi uyarınca, işleme şartları bizzat 6698 sayılı Kanun'da yer alan kişilerin sağlık verilerine ilişkin bilgilerin, ancak kişinin açık rızası halinde işlenebileceği, "işlenme" ifadesinden ise, ilgili verinin açıklanması, aktarılması, elde edilebilir hale getirilmesi gibi her türlü işlemin anlaşılması gerektiği açıktır.

Diğer taraftan, Avukat-müvekkil ilişkisi temelde 6098 sayılı Türk Borçlar Kanunu'nun 502 ve devamı maddelerinde yer alan "vekalet sözleşmesi"ne dayanmakta olup; vekilin üstlendiği iş ve hizmetleri, vekalet verenin haklı menfaatlerini gözeterek, sadakat ve özenle yürütme ödevi bulunmaktadır. Bu özen görevi, 1136 sayılı Kanun'da da avukatın işini özenle ve sonuna kadar takip etme (m. 34 ve 171) ödeviyle de somutlaştırılmış bulunmaktadır. Öte yandan 1136 sayılı Avukatlık Kanunu'nun 2. maddesinde, avukatlığın amacının, hukuki münasebetlerin düzenlenmesini, her türlü hukuki mesele ve anlaşmazlıkların adalet ve hakkaniyete uygun olarak çözümlenmesini ve hukuk kurallarının tam olarak uygulanmasını her derecede yargı organları, hakemler, resmi ve özel kişi, kurul ve kurumlar nezdinde sağlamak olduğu, avukatın bu amaçla hukuki bilgi ve tecrübelerini adalet hizmetine ve kişilerin yararlanmasına tahsis edeceği ifade edildikten sonra aynı maddenin 3. fıkrasında, madde metninde sayılan kamu kurum ve kuruluşları ile özel hukuk tüzel kişilerinin avukatların ihtiyaç duyduğu bilgi ve belgeleri incelemeye sunmakla yükümlü kılınarak avukatlara görevlerinin yerine getirilmesi kapsamında, müvekkilinin hukukunu savunabilmesine, haklarını dava etmesine, yargılama sürecinin çabuklaştırılmasına ve uyuşmazlıkların adalet ve hakkaniyete uygun olarak çözümlenmesine yardımcı olma görevinin yüklendiği anlaşılmaktadır. Şüphesiz bu yükümlülük,

"Kanunlardaki özel hükümler saklı kalmak kaydıyla" ilgili kurum ve kuruluşlara getirilmiş olup mutlak değildir.

Buna göre, avukatın müvekkiliyle iş ilişkisi içinde üstlendiği bir işin mahiyetine göre gerek duyduğu bilgi ve belgeyi başka kurum, kuruluş veya özel hukuk tüzel kişilerinden vekalet görevi kapsamında talep etmesi avukatın vekalet görevini özenle ifa etme yükümlülüğü çerçevesinde değerlendirilmekle birlikte, müvekkilinin özel nitelikli kişisel veri mahiyetinde bulunan sağlık bilgilerine ilişkin kayıtların, yukarıda yer verilen mevzuat hükümleri doğrultusunda ancak ilgilinin açık rızasıyla davalı idarece verilebilmesi mümkün bulunduğundan, davacı vekilinin davacıdan aldığı "genel vekaletname" ile müvekkiline ait sağlık bilgilerine ilişkin kayıtları talep ettiği anlaşıldığından, davalı idare tarafından tesis edilen dava konusu işlemde ifade edilen yönüyle hukuka aykırılık; aksi yönde karar veren İdare Mahkemesi kararında ise hukuki isabet bulunmamaktadır.

Açıklanan nedenlerle; Batman İdare Mahkemesinin temyize konu kararının bozulmasına, dosyanın yeniden bir karar verilmek üzere anılan Mahkemeye gönderilmesine, bu kararın tebliğ tarihini izleyen 15 (onbeş) gün içerisinde kararın düzeltilmesi yolu açık olmak üzere, 02/07/2020 tarihinde oybirliği ile karar verildi.

Danıştay Kararı - 10. Daire (E. 2017/4211)

Danıştay Kararı - 10. D., E. 2017/4211 K. 2020/5468 T. 26.11.2020

T.C. DANIŞTAY ONUNCU DAİRE

Esas No: 2017/4211

Karar No: 2020/5468

DAVACI: ... Başkanlığı

VEKİLLERİ: Av. ...

DAVALI: ... Kurumu

VEKİLİ: Av. ...

DAVANIN KONUSU: 28/10/2017 tarih ve 30224 sayılı Resmi Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 7. maddesinin 1. ve 5. fıkrasının, 8. maddesinin 2. fıkrasının, 9. maddesinin 2. fıkrasının, 10. maddesinin 3. fıkrasının, 11. maddesinin ve 12. maddesinin 1. fıkrasının (a) bendinin "Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu talebe konu kişisel verileri siler, yok eder ve veya anonim hale getirir." şeklindeki ilk cümlesinin, ve 12. maddesinin 1. fıkrasının (b) bendinin iptali istemiyle açılmıştır.

DAVACININ İDDİALARI:

Davacı tarafından,

Yönetmeliğin; 7. maddesinin 1. ve 5. fıkrası, 11. maddesinin 1. fıkrası, 12. maddesinin 1. fıkrasının (a) bendinin "Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu talebe konu kişisel verileri siler, yok eder veya anonim hale getirir." şeklindeki ilk cümlesi ve (b) bendi yönünden;

- Kişisel veri sahibi gerçek kişinin temel haklarından birinin kendine ait verinin silinmesini talep etme hakkı olduğu, bu hakkın Anayasanın 20. maddesinin son fıkrasında herhangi bir sınırlama getirilmeden mutlak bir hak olarak düzenlediği,

- 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Sözleşmenin 5. maddesinde kişisel verilerin yasal yoldan elde edileceği ve işlenebileceği, belli ve meşru amaçlar için kaydedileceği, bu amaçlara aykırı şekilde kullanılmayacağı, kaydedilme amacına

göre aşırı olamayacağı, verilerin doğru ve güncel olması gerektiği belirtilmiş, 6. maddesinde sağlık verilerinin özel kategoride hassas veriler olarak kabul edildiği ve iç hukukta uygun güvenceler sağlanmadıkça otomatik işleme tabi tutulmalarının yasaklandığı, kişisel verilerin kaydedilme amaçlarını gerçekleştirmek için gerekli olacak süreyi aşmayacak şekilde saklanacağı belirtilmiştir, bu hükme göre kaydedilme amacı yada işleme şartları ortadan kalkan verilerin derhal silinmesinin gerektiği,

- Bu kapsamda Kişisel Verilerin Korunması Kanunu'nun 11. maddesinde; işlenen verilerin tümünden ilgilinin haberdar olması gerektiği, sisteme erişim, bilgilerin düzeltilmesini yada silinmesini isteme haklarının temin edilmesi gerektiği, veri işlemenin hukuki dayanağının, amacının ve aktarım yapılan 3. kişilerin kimliğinin bilinir olması zorunluluğu haklarının düzenlendiği, ancak dava konusu Yönetmelikte sağlık verisi sahibi kişilerin bu haklarını temin etmeye yönelik bir hüküm bulunmadığı, örneğin kişinin verisinin düzeltilmesini talep hakkına ilişkin bir düzenlemenin Yönetmelikte olmadığı,

- Kişisel veri sahibi gerçek kişinin verinin silinmesini talep hakkının ortadan kaldırıldığı,

- Dava konusu maddeler ile idareye veriyi silme ya da anonim hale getirme konusunda sınırsız bir takdir yetkisi tanındığı, veri sahibi kişilerin sürece hiçbir şekilde müdahalede bulunamayan, itiraz hakları olmayan pasif sükûterler olarak tasarlandığı,

- Bu hükmün doğal sonucu olarak kişilere ait sağlık verileri gibi hassas verilerde dâhil olmak üzere birçok bilginin işlendikleri sistemde işleme koşulları ortadan kalksa da tutulmaya devam edileceği, örneğin bir suç şüphelisi olarak sizden alınan DNA örneğinin beraat etseniz dahi sistemde tutulmaya devam edilebileceği, sağlıkla ilgili bilgiler otomatik olarak işlendiğinde ve özel bir şirkete aktarıldığında bu verilerin silinmesini sağlamanın olanaksız hale geleceği, veriyi anonim hale getirmenin bunu engelleyeceği düşünülse de verilerin nasıl anonimleştirileceğinin gereği gibi düzenlenmemesi nedeniyle veri işleyen herkesin bunu kendi belirlediği yöntemle yapacağı, yöntemin yetersizliğinin telafisi imkansız zararlara yol açabileceği, bu yöntemin veri sahibince bilinebilir ve denetlenebilir olmadığı,

- AİHM'in kişilerin DNA profillerinin devletin veri tabanında bulunmasını özel hayatın ihlali saydığı, tutulma gerekçeleri ortadan kalkan kişisel verilerin milli güvenlik gerekçesiyle saklanmasını özel hayatın gizliliğine ölçsüz müdahale saydığı,

- Otomatik işleme tabi tutulan kişisel verilerin nasıl korunacağına ilişkin yeterli teknik ve idari tedbirlerin hukukumuzda düzenlenmediği, bu şekilde otomatik işleme tabi tutulan kişisel verilerin

işlenme şartları ortadan kalkmasına rağmen güvenilir olmayan sistemde tutulmaya devam edilmesinin telafisi olanaksız zararlar doğuracağı,

Yönetmeliğin 8. maddesinin 2. fıkrası, 9. maddesinin 2. fıkrası, 10. maddesinin 3. fıkrası, 12. maddesinin 1. fıkrasının (b) bendi yönünden;

- Soyut biçimde ifade edilen “her türlü tedbir” gibi ifadelerin içini dolduran hükümlere Yönetmelikte yer verilmediği,

- Düzenlemelerde bu haliyle gerekli tedbirlerin ne olduğunun kararını ya idarenin ya da veri sorumlularının vereceği, bu kararların ilgili kişi veya kamuoyu nezdinde denetlenebilir olmayacağı, ayrıca idari ve teknik tedbirlerin muğlaklığının uygulamada birlik sağlanmasına ve her veri sorumlusunun kendi belirlediği yöntemlerle hareket etmesine neden olacağı, üstelik Yönetmelikteki esaslara yada veri sorumlusunun veri saklama ve imha politikasında verdiği taahhütlere aykırı davranılması durumunda ne olacağının ve yaptırımlarının Yönetmelikte düzenlenmediği, toplamda 15 maddeden oluşmakla birlikte esas itibariyle usule ilişkin hükümler dışında 9 maddeden oluşan Yönetmelikle kişisel verilerin silinmesi/yok edilmesi/anonimleştirilmesi gibi önemli ve son derece teknik ayrıntıya sahip bir alanın uygulamayı gösterir biçimde düzenlenebilmesinin söz konusu olmadığı,

- İdarenin bu alanı gereği gibi düzenlemek yerine veri sorumlusunca oluşturulacak “veri saklama ve imha politikasında” verdiği taahhütlerle uygulamayı yürütmek istediği, bu nedenle dava konusu düzenlemelerde işlenen kişisel verilerin silinmesi, yok edilmesi, anonimleştirilmesi konusundaki esasları ayrıntılı olarak belirlenmeden idareye ucu açık, çerçevesi çizilmemiş, sınırsız bir yetki verildiği, Yönetmelikle düzenlenmesi gereken hususların idarenin keyfiyetine bırakıldığı,

- Bu yükümlülüğü yerine getirecek olan başta veri sorumluları olmak üzere tüm uygulayıcıların kişisel verilerin hangi hallerde işlenebileceğini, bu koşulların hangi hallerde doğacağını, uygulamanın nasıl yapılacağını bilmelerinin gerektiği, başka bir deyişle dava konusu düzenlemelerin herhangi bir yol göstermeye, yoruma gerek duyulmaksızın uygulamayı göstermesi gerektiği,

- Kanunun kendisi son derece muğlak iken uygulamayı gösteren düzenlemelerin hukuka aykırı ve muğlak oluşunun, kişisel verilerin işlenmesine ilişkin iş ve işlemleri uygulayıcıların keyfiyetine teslim ettiği, örneğin Kanunun 5. maddesinin 1. fıkrasında “(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.” ana kuralına yer verilmişken 2. fıkrasında “(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür: a) Kanunlarda açıkça öngörülmesi. b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda

bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması. c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması. ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması. d) İlgili kişinin kendisi tarafından alenileştirilmiş olması. e) Bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması. f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.” denilmek suretiyle muğlak ve 105 sayılı sözleşmede yer almayan hallerde yer verildiği, veri sorumlusunun bu hallerin doğduğunu ya da ortadan kalktığını hangi ölçütlere göre değerlendireceği, bu ölçütlerin Yönetmelikte gösterilmesi gerektiği, uygulamanın veri sorumlularının kanaatlerine ve Kanunun ilgili maddelerinden ne anladıklarına göre şekilleneceği, veri sahibi kişiler yönünden telafisi imkânsız zararlar doğacağı,

Yönetmeliğin 11. maddesi yönünden;

- Yönetmeliğin 11. maddesinde işlenen verileri silmesi için veri sorumlusuna tanınan sürelerin uzun olduğu,

- Veri sorumlusunun derhal harekete geçerek işleme nedeni ortadan kalkan verileri silme, yok etme veya anonim hale getirme zorunda olmadığı, periyodik imhanın hangi aralıkla yapılacağına veri sorumlusunun karar vereceğinin belirtildiği, sadece altı aylık azami sürenin belirlendiği, silinmesi gereken verinin 6 ay sistemde tutulmasının hakkın özüne dokunduğu, sürenin uzun olduğu, silme, yok etme veya anonim hale getirme işlemlerine derhal başlanması gerektiği,

- Yasayla belirlenen koşulların ortadan kalkmasına rağmen verilerin 6 ay daha veri sorumlusunun hakimiyetinde olmasının usulsüz erişim niteliğinde olduğu ve Türk Ceza Kanununun 138. maddesinde düzenlenen kişisel verileri yok etmeme suçunu oluşturduğu, yönetmelik ile suç olan bir davranışa meşruiyet kazandırılmayacağı,

- 11. maddenin 4. fıkrasında; “Kurul, telafisi güç veya imkansız zararların doğması ve açıkça hukuka aykırılık olması halinde, bu maddede belirlenen süreleri kısaltabilir.” hükmüne yer verilmiş ise de zarar oluşmadan “ihtiyatlılık” ilkesi gereği sürelerin minimum düzeyde tutulması gerektiği,

- 11. maddenin 3. fıkrasında; Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusundan bahsedilmekte ve bu kapsamdaki kişi ve kuruluşlara kişisel verileri silme, yok etme veya anonim hale getirme için üç aylık süre tanındığı, yönetmelikte Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusundan ne anlaşılması gerektiğinin

düzenlenmediği, bir kısım otomatik veri işleyen kişi yada kuruluşların alana ilişkin yükümlülüklerden muaf tutulduğu, bunların kimler olduğunun ve hangi ölçütlere göre belirleneceğinin Yönetmelikten anlaşılamadığı,

iddialarıyla iptalleri gerektiği ileri sürülmektedir.

DAVALININ SAVUNMASI:

Davalı idare tarafından,

Yönetmeliğin; 7. maddesinin 1. ve 5. fıkrası, 11. maddesinin 1. fıkrası, 12. maddesinin 1. fıkrasının (a) bendinin "Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu talebe konu kişisel verileri siler, yok eder veya anonim hale getirir." şeklindeki ilk cümlesi ve (b) bendi yönünden;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 6. maddesinde sağlık verilerinin özel nitelikli kişisel veri olduğunun, özel nitelikli kişisel verilerin ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğunun, sağlık ve cinsel hayat dışındaki verilerin kanunlarda öngörülen hallerde kişinin açık rızası aranmaksızın işlenebileceğinin düzenlendiği,

- Sağlık ve cinsel hayata ilişkin kişisel verilerin ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği, özel nitelikli kişisel verilerin işlenmesinde ayrıca Kişisel Verileri Koruma Kurulu tarafından belirlenen yeterli önlemlerin alınmasının şart olduğu, bu önlemlerin kurulca belirlenerek 07/03/2018 tarihli, Resmi Gazetede yayımlandığı,

- Yönetmeliğin 7. maddesinin birinci fıkrasında; "Kanunun 5 inci ve 6 ncı maddelerinde yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin veri sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekir." denilmek suretiyle 6698 sayılı Kanun'un 7. maddesi hükmüne uygun olarak veri sorumlusu tarafından kişisel verilerin hangi şartlarda silinmesi, yok edilmesi veya anonim hale getirilmesi gerekliliğinin açıkça hükme bağlandığı,

- Kişisel verilerin muhafazası konusunda dava dilekçesinde iddia edildiğinin aksine belirsiz, sübjektif ve çok uzun sürelerle kişisel verilerin muhafaza edilmesi gerektiği yaklaşımının aksine, kişisel verilerin muhafaza sürelerinin de belli kriterlere bağlı olarak belirlenmesi ve ilgili kişinin de bu süreler hakkında bilgi sahibi olmasının genel ilke olarak kabul edildiği, Nitekim 108 sayılı sözleşmenin 5. maddesine benzer bir düzenlemeyle 6698 sayılı Kanunun kişisel verilerin

işlenmesinde zorunlu olan ilkelerin 4. maddesinde; “(1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir. (2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur: a) Hukuka ve dürüstlük kurallarına uygun olma. b) Doğru ve gerektiğinde güncel olma. c) Belirli, açık ve meşru amaçlar için işlenme. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.” şeklinde sayıldığı,

- Kanunun 4. maddesindeki genel ilkelerin 5. maddesinde ve 6. maddesinde düzenlenen veriler bakımından da uyulması gereken ilkeler olduğu, verilerin genel ilkelerden biri olan “İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme” ilkesine uygun olarak muhafaza edilmesinin gerektiği, işlenen verilerin gerekli olan süre kadar muhafaza edileceği, verilerin saklanması için geçerli bir sebep olmaması halinde Kanunun 7. maddesi ve dava konusu yönetmelik hükümleri gereğince verinin silinmesinin, yok edilmesinin veya anonim hale getirilmesinin gerekeceği, yine bu ilkeye bağlı olarak veri sorumlusunun, kişisel veri, saklama ve imha politikası ve esaslarını oluşturmak, saklama süreleri ve kişisel verilerin muhafazasında uygulanacak teknik ve idari, tedbirleri belirlemek ve kişisel verilerin bu esaslara uygun olarak muhafazasını sağlamakla yükümlü olduğu, veri sorumlularının bu yükümlülüklerini yerine getirirken belirlemesi öngörülen kişisel verilerin işlendikleri amaç için gerekli olan azami sürenin tespitinde dikkate alması gereken hususların neler olduğunun ise 01/01/2008 tarihinde yürürlüğe girmek üzere 30/12/2017 tarihli Resmi Gazetede yayımlanan Veri Sorumluları Sicili Hakkında Yönetmeliğin 9. maddesinin 4. fıkrasında sayıldığı,

- Ayrıca dava konusu Yönetmeliğin 5. maddesinin 1. fıkrasında 6698 sayılı Kanunun 16. maddesi gereğince Veri Sorumluları Siciline kayıt olmakla yükümlü olan veri sorumlularının kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası hazırlamakla yükümlü olduğunun belirtildiği,

- Diğer taraftan, Kişisel Verileri Koruma Kurulu gözetiminde Başkanlık tarafından kamuya açık olarak tutulan Veri Sorumluları Sicilinde kişisel verilerin işlendikleri amaç için gerekli olan azami sürenin de kamuya açıklanacak bilgiler arasında yer aldığı, bu sayede ilgili kişilerin Sicile erişim sağlamak suretiyle kendilerine ait kişisel verinin yer aldığı kişisel veri kategorisinin azami saklama süresi hakkında bilgi sahibi olabileceği,

- Davacı tarafından; Yönetmelikte kişisel verilerin silinmesini talep hakkını kısıtlayıcı veya ortadan kaldıran hükümlere yer verildiği iddia edilmekte ise de, bu iddianın gerçeklikten ve hukukilikten uzak olduğu, söz konusu maddeden anlaşılacağı üzere ilgili kişinin verilerinin silinmesini veya yok

edilmesini isteme hakkının sınırsız olmadığı, Kanunun 7. maddesindeki şartlarla sınırlı olarak bu hakkını kullanabilmesinin öngörüldüğü, kişilerin verilerinin silinmesini veya yok edilmesini istenmesinin tek başına yeterli olmadığı Kanunun 5. ve 6. maddelerinde öngörülen verilerin işleme şartlarının ortadan kalkmasının gerekli olduğu,

- Kişisel verilerin silinmesini veya yok edilmesini isteme hakkının mutlak bir hak olmadığı, hakkın özüne dokunmamak kaydıyla ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması veya devlete yüklenen ödevler nedeniyle Kanunla sınırlama getirilebileceği, 6698 sayılı Kanun 7. maddesi ve Yönetmeliğin 7. maddesinin 1. fıkrası hükmü ile kişisel verilerin silinmesini veya yok edilmesini isteme hakkının kişisel verilerin işleme şartlarının tamamının ortadan kalkması şartına bağlandığı, Yönetmeliğin bu hükmünün Anayasaya aykırı olmadığı,

- Söz konusu hükümlerin kişisel verinin silinmesini veya yok edilmesini isteme hakkını kaldıran hükümler olmadığı, bu hakkın nasıl kullanılacağına ilişkin esas ve usulleri belirlediği, veri sorumlusunu sınırlandırdığı, veri sorumlusunun silme, yok etme veya anonim hale getirme işleminin şartlarının oluşup oluşmadığı, hangi yöntemin uygun olduğu konusunda sınırsız yetkiye sahip olmadığı, ilgili kişiye bunun gerekçesini açıklamakla yükümlü olduğu, diğer taraftan veri sorumlusunun Yönetmeliğin 7. maddesinin 2. fıkrası gereğince, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Kanunun 4. maddesindeki genel ilkeler ile 12. maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve kişisel veri saklama ve imha politikasına uygun hareket etmek zorunda olduğu,

- 6698 sayılı Kanunun 13. maddesinde ve 10/03/2018 tarihli Resmi Gazetede yayımlanan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ ile ilgili kişinin 11. maddede sayılan haklarının etkin bir şekilde kullanılmasını teminen uyulması gereken usul ve esasların ayrıntılı olarak düzenlendiği, ayrıca Kurula şikayet başlıklı 14. madde ve şikayet üzerine veya resen incelemenin usul ve esasları başlıklı 15. madde hükmü ile de bu hakların kullanılmasına ilişkin olarak veri sorumlusuna yapılacak başvurunun veri sorumlusu tarafından reddedilmesi, verilen cevabın yetersiz olması veya süresinde başvuruya cevap verilmemesi halinde ilgili kişinin Kurula şikayet hakkının düzenleme altına alındığı, veri sorumlusunun idari yünden de denetime tabi tutulması ve hukuka aykırılığın tespiti halinde verilen idari yaptırım kararlarıyla ilgili kişinin haklarının korunmasının amaçlandığı, böylelikle ilgili kişilerin kişisel verilerinin korunmasına ilişkin haklarını kullanırken doğrudan yargı yoluna başvurabilmelerinin yanı sıra 6698 sayılı Kanunla getirilen diğer hak arama yöntemlerini kullanabilecekleri, buradan hareketle, 6698 sayılı Kanun ve dava konusu Yönetmelik hükümleriyle sınırlama aracının sınırlama amacına uygun ve orantılı şekilde kullanılmasını sağlayacak yasal

güvencelere yer verildiği ve yeterli korumanın sağlandığı da dikkate alındığında yapılan düzenlemelerin ilgili kişinin kişisel verilerin korunması hakkının özünü zedelediği gibi amaç ve araç arasında makul bir dengenin kurulduğunun açıkça görüldüğü,

Yönetmeliğin 8. maddesinin 2. fıkrası, 9. maddesinin 2. fıkrası, 10. maddesinin 3. fıkrası, 12. maddesinin 1. fıkrasının (b) bendi yönünden;

- Dava konusu Yönetmeliğin kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasları objektif, somut ve yeterli kurallarla ayrıntılı bir şekilde düzenlemediği, muğlak ifadeler içermesi sebebiyle uygulamada birlik sağlanamayacağı, veri sorumlularının keyfi uygulamalarına yol açacağı, hukuka aykırı olduğu, eksik düzenleme niteliği taşıdığı iddia edilmekte ise de bu iddiaların kabulünün hukuken mümkün olmadığı,

- Yönetmeliğin 8. maddesinin 1. fıkrasında; kişisel verilerin silinmesinin, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi olarak tanımlandığı, bu tanımdan hareketle “ilgili kullanıcı” verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi yada birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişileri kapsadığı, Yönetmelikte tanımlandığı şekilde silme işleminden bahsedebilmek için silinen kişisel verinin ilgili kullanıcılar tarafından daha sonra erişilememesinin ve kullanılamamasının gerektiği,

- Yönetmeliğin 9. maddesinin 1. fıkrasında; kişisel verilerin yok edilmesinin, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi olarak tanımlandığı, bu şekilde bir yok etmeden bahsedebilmek için verilerin kayıtlı olduğu tüm kopyaların tespit edilerek belirli yöntemlerle geri getirilemeyecek hale getirilmesi gerektiği,

- Yönetmeliğin 10. maddesinin 1. fıkrasında; kişisel verilerin anonim hale getirilmesinin, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi işlemi olarak tanımlandığı, 2. fıkrasında, kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerektiğinin belirtildiği,

- Bu tedbirlerin standart bir şekilde Yönetmelikte yer almasının birbirinden çok farklı kayıt sistemlerine sahip veri sorumluları açısından uygulamada yaratacağı sorunlar, bununla birlikte

gelişen teknoloji, öngörülemezlik ve yöntemler karşısında Yönetmelikte düzenlenecek yöntemlerin yetersiz kalma riskinin olması ve sık sık güncellenmesinin gerekeceği dikkate alınarak, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesinde uygulanacak teknik yöntemlerin, alınacak teknik ve idari tedbirlerin uygulamada açıklık sağlaması ve iyi uygulama örnekleri oluşturma amacıyla Kişisel Verileri Koruma Kurulu kararları ile “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi” ile kişisel verilerin işleme sürecinde veri sorumlularının alması gereken tedbir ve idari tedbirler konusunda da uygulamada açıklık sağlanması ve iyi uygulama örnekleri oluşturmaya amacıyla “Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)” hazırlandığı ve kamuoyuna sunulduğu,

- Yönetmeliğin 7. maddesinin 2. fıkrasında; “Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Kanunun 4 üncü maddesindeki genel ilkeler ile 12 nci maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve kişisel veri saklama ve imha politikasına uygun hareket edilmesi zorunludur.” denilmek suretiyle rehberlerde belirlenen esas ve usuller ile birlikte, veri sorumlusu tarafından oluşturulan kişisel veri saklama ve imha politikasına veri sorumluları tarafından uyulmasının zorunlu olduğunun düzenleme altına alındığı,

- Dava konusu Yönetmeliğin 12. maddesinin 1. fıkrasının (b) bendinde de, ilgili kişinin veri sorumlusuna başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep etmesi durumunda kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa veri sorumlusu bu durumu üçüncü kişiye bildireceği; üçüncü kişi nezdinde bu Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin edeceğinin düzenlendiği, burada yer alan gerekli işlemler ifadesinin soyut ve belirsiz durumları ifade etmediği, üçüncü kişilere aktarılan kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Yönetmelikte düzenlenen ve veri sorumlusunun yerine getirmekle yükümlü olduğu usul ve esaslara atıf yapılarak aynı işlemlerin bu kişisel veriler içinde uygulanması gerekliliğinin belirtildiği,

- 6698 sayılı Kanunun 5. maddesinin 1. fıkrasında; kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğinin belirtildiği ancak 2. fıkrasındaki şartların varlığı halinde açık rızanın aranmayacağı, 6. maddesinin 1. fıkrasında ise; kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerin özel nitelikli kişisel veri olduğunun, 2. fıkrasında, özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğunun, 3. fıkrasında ise birinci fıkrada sayılan sağlık ve

cinsel hayat dışındaki kişisel verilerin, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebileceğinin, sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceğinin hüküm altına alındığı,

- Görüleceği üzere kişisel veri işleme şartlarının Kanunda ayrıntılı bir şekilde düzenlendiği, bu şartların ikincil düzenlemeler ile genişletilmesinin mümkün olmadığı, her bir kişisel veri işleme faaliyetinin amacının Kanun bakımından hukuki dayanağının olduğu, kişisel veri işleme faaliyetinin amacında birden fazla sayıda kişisel veri işleme şartının bulunabilmesinin mümkün olduğu, bu açıdan veri sorumlusunun verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine karar verirken kişisel veri işleme şartlarının tamamının ortadan kalkıp kalkmadığını belirlemesinin gerektiği,

- Anayasa Mahkemesinin 28/09/2017 tarih ve E:2016/125, K:2017/143 sayılı kararında 6698 sayılı Kanunun 5/2-c, ç, e, f maddeleri yönünden “bu bağlamda dava konusu kurallar madde gerekçeleriyle birlikte değerlendirildiğinde ilgili kişinin açık rızası olmaksızın kişisel verilerin işlenmesinin mümkün olduğu hallerin kapsam, amaç ve sınırlarının Kanun’da açıkça yer alması karşısında kuralların belirsiz olduğu söylenemez” gerekçesine yer verildiği,

Yönetmeliğin 11. maddesi yönünden;

- Yönetmeliğin 4. maddesinde; Periyodik imhanın, Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi olarak tanımlandığı, tanımdan da açıkça anlaşılacağı üzere özellikle çok sayıda ve çeşitlilikte kişisel veri işleyen veri sorumlularının belli periyotlarla silmeleri, yok etmeleri veya anonim hale getirmeleri gereken kişisel verileri tespit ederek resen bu işlemleri gerçekleştirmelerinin teminen bu usulün getirildiği, veri sorumlusunun kişi talebini beklemeksizin kendi içinde süreci belli periyotlarla kontrol ederek bu verilerin gecikmeksizin silinmesinin, yok edilmesinin veya anonim hale getirilmesinin amaçlandığı,

- Yönetmeliğin 11. maddesi ile; kişisel veri saklama ve imha politikası hazırlamış olan veri sorumlusunun, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işlemi, kişisel verileri sileceğinin, yok edeceğinin veya anonim hale getireceğinin, bu sürenin her halde altı ayı geçemeyeceğinin düzenlendiği,

- Aynı maddenin 3. fıkrasında ise; kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusunun, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden üç ay içinde bu yükümlülüğünü yerine getireceğinin düzenlendiği,

- Söz konusu maddede geçen sürelerin maksimum süreler olduğu, maksimum süreler kadar beklenene ilişkin olarak Yönetmelikte hüküm olmadığı,

- Maksimum süreler konularak sürelerle ilişkin suistimallerin önüne geçilmesinin amaçlandığı,

- Yönetmeliğin 5. maddesinin 1. fıkrasında; Kanunun 16. maddesi gereğince Veri Sorumluları Siciline kayıt olmakla yükümlü olan veri sorumlularının, kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası hazırlamakla yükümlü olduğunun belirtildiği, veri sorumluları siciline kayıt olmakla yükümlü olmayan veri sorumlularının kişisel veri saklama ve imha politikası hazırlamakla yükümlü olmadığı, bunların 6698 sayılı Kanun'un 16. maddesinde, 28. maddesinin 2. fıkrasında ve Veri Sorumluları Sicili Hakkında Yönetmeliğin 15. maddesinde sayıldığı,

belirilerek davanın reddi gerektiği savunulmaktadır.

DANIŞTAY TETKİK HAKİMİ: ...

DÜŞÜNCEİ: Davanın reddi gerektiği düşünülmektedir.

DANIŞTAY SAVCISI: ...

DÜŞÜNCEİ: Dava, 28/10/2017 tarih ve 30224 sayılı Resmi Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 7. maddesinin 1. ve 5. fıkrasının, 11. maddesinin ve 12. maddesinin 1. fıkrasının (a) bendinin "Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu talebe konu kişisel verileri siler, yok eder ve veya anonim hale getirir." ilk cümlesinin, 8. maddesinin 2. fıkrasının, 9. maddesinin 2. fıkrasının ve 10. maddesinin 3. fıkrasının, 12. maddesinin 1. fıkrası (b) bendinin hukuka aykırılığı ve noksan düzenleme nedeniyle iptali istemiyle açılmıştır.

Anayasamızın, "Kişinin Hakları ve Ödevleri" başlıklı İkinci Bölüm altında "A. Özel hayatın gizliliği" başlıklı 20. maddesinde; Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.(...)

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de

kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmü yer almıştır.

Türkiye tarafından da 30/01/2016 tarihinde 6669 sayılı Kanunla onaylanması uygun bulunan Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin 9. maddesinde de; Devlet güvenliği, kamu güvenliği, Devletin ekonomik menfaatlerinin korunması ve suçların önlenmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması ile verilerin istatistiki veya bilimsel amaçlarla kullanılması durumlarında kişisel verilerin korunmasına sınırlama getirilmesi kabul edilmiştir.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 4. maddesinde; (1) Kişisel verilerin, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği, (2) Kişisel verilerin işlenmesinde; a) Hukuka ve dürüstlük kurallarına uygun olma, b) Doğru ve gerektiğinde güncel olma, c) Belirli, açık ve meşru amaçlar için işlenme, ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme, ilkelerine uyulmasının zorunlu olduğu, "Kişisel verilerin işlenme şartları" başlıklı 5. maddesinde; (1) Kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) Aşağıdaki şartlardan birinin varlığı hâlinde; a) Kanunlarda açıkça öngörülmesi., b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması., c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması., ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması., d) İlgili kişinin kendisi tarafından alenileştirilmiş olması., e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması., f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu, "Özel nitelikli kişisel verilerin işlenme şartları" başlıklı 6. maddesinde; (1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerinin özel nitelikli kişisel veri olduğu, (2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğu, (3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel verilerin, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebileceği, sağlık ve cinsel hayata ilişkin kişisel verilerin ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve

bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği, (4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınmasının şart olduğu, hükmüne yer verilmiş, 7. maddesinin 3. fıkrasında; "Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esasların yönetmelikle düzenleneceği hükme bağlanmış, "Kurulun görev ve yetkileri" başlıklı 22. maddesinin 1. fıkrası e) bendinde; "Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmak, görevi Kurulun görev ve yetkileri arasında sayılmıştır.

Anılan Yasa hükümleri dayanak alınmak suretiyle Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasları belirlemek amacıyla, Kanunun 7. maddesi uyarınca veri sorumluları hakkında uygulanmak üzere yayımlanmıştır.

Yönetmeliğin 7.maddesinin 1. fıkrasında; Kanunun 5 inci ve 6 ncı maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin veri sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekir.", 5. fıkrasında; "Veri sorumlusu, Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçer. İlgili kişinin talebi halinde uygun yöntemi gerekçesini açıklayarak seçer.", "Kişisel verilerin silinmesi" başlıklı 8. maddesinin 2. fıkrasında; veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.", "Kişisel verilerin yok edilmesi" başlıklı 9. maddesinin 2. fıkrasında; "Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.", "Kişisel verilerin anonim hale getirilmesi" başlıklı 10. maddesinin 3. fıkrasında; "Veri sorumlusu, kişisel verilerin anonim hale getirilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.", "Kişisel verileri resen silme, yok etme veya anonim hale getirme süreleri" başlıklı 11. maddesinde; "(1) Kişisel veri saklama ve imha politikası hazırlamış olan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.

(2) Periyodik imhanın gerçekleştirileceği zaman aralığı, veri sorumlusu tarafından kişisel veri saklama ve imha politikasında belirlenir. Bu süre her halde altı ayı geçemez.

(3) Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden üç ay içinde, kişisel verileri siler, yok eder veya anonim hale getirir.

(4) Kurul, telafisi güç veya imkansız zararların doğması ve açıkça hukuka aykırılık olması halinde, bu maddede belirlenen süreleri kısaltabilir.", "Kişisel verileri ilgili kişinin talep etmesi durumunda silme ve yok etme süreleri" başlıklı 12. maddesinin 1. fıkrasının; İlgili kişi, Kanununun 13 üncü maddesine istinaden veri sorumlusuna başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde; a) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Veri sorumlusu, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir. b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa veri sorumlusu bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde bu Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder." kuralı getirilmiştir.

Anayasamız özel hayatın gizliliğini güvence altına almakla birlikte bazı hallerde; milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması gibi hallerde özel hayatın gizliliğine dokunulabilmesini olanaklı kılınmıştır.

Bu halde, temel hak ve özgürlükler özlerine dokunulmaksızın Anayasamızda öngörülen sebeplerle demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine uygun olarak ve ancak Kanunla sınırlanabilecektir.

Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek amacıyla 6698 sayılı Kanun hazırlanmıştır.

Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi kişisel veri olarak tanımlanırken, kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem, kişisel verilerin işlenmesi olarak ifade edilmiştir.

Davacı tarafından, Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, ülkemizce onaylanarak iç hukukta yasalar üstü bir hukuki statü kazandırıldığı ve bu

Sözleşmede sağlık verilerinin özel kategoride hassas veriler olarak kabul edildiği, iç hukukta uygun güvenceler sağlanmadıkça otomatik işleme tabi tutulmalarının yasaklandığı, dolayısıyla iç hukukta sağlanması gereken güvencelerden birinin kişisel verilerin silinmesini, kullanılamaz hale getirilmesini ve anonimleştirilmesini temin eden düzenlemelerin yapılması ve kaydedilme amacını aşmayacak şekilde saklanmalarının gerekliliği, amacı ve işleme şartları ortadan kalkan verilerin derhal silinmesi zorunluluğuna karşın, Yönetmelikte sağlık verisi sahibi kişilerin bu haklarını temin etmeye yönelik hüküm bulunmadığı ileri sürülmüştür.

Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesinin yasak olmasına karşın istisnası olarak özel nitelikli kişisel verilerden olan sağlık ve cinsel hayata ilişkin kişisel verilerin, ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği yasa ile düzenlenmiştir. Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esasları Yönetmeliğe bırakan Yasa hükmüne göre sağlığa ilişkin kişisel verilerin silinme talep hakkını Yönetmeliğin 7. maddesi ilgiliye tanımıştır. Ancak silinmenin ön şartı, kişisel verilerin işleme şartlarının tamamının ortadan kalkması halidir. Şartların tamamının ortadan kalkıp kalkmadığının denetimi Veri Sorumlusu Sicili Hakkında Yönetmeliğin 9. maddesinde yer verilen Sicile yapılan kayıt başvurusu sırasında iletilecek bilgiler arasında; kişisel verilerin hangi amaçla işleneceği, kişisel verilerin mevzuatta öngörülen veya işlendikleri amaç için gerekli olan azami muhafaza edilme süresi ve bu sürenin veri kategorileri ile eşleştirilerek Sicile bildirim ile amaç için gerekli olan azami muhafaza süresi belirlenirken dikkate alınacak olan; faaliyet gösterilen sektörde genel teammül gereği kabul edilen süre, ilgili kişiyle tesis edilen hukuki ilişkinin devam edeceği süre, işleme amacına bağlı olarak saklanmasının yaratacağı risk, maliyet ve sorumlulukların devam edeceği süre, verilerin saklanmasının zorunlu olduğu süre ve zamanaşımı gibi sürelerin bildirim yükümlülüğünün bulunduğu dikkate alındığında, kişisel verilerin işleme şartlarının ortadan kalkma halinin belirlenmesi sağlanmıştır.

Yönetmeliğin 11. maddesinin, "kişisel veri saklama ve imha politikası hazırlamış olan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihini takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir" kuralındaki yükümlülüğün ortaya çıkma halinin de yine Veri Sorumluları Sicil Yönetmeliği hükümleri ile değerlendirildiğinde, kayıt altına alınan, tespit edilebilir bir ortaya çıkma halinin mevcut

olduđu ve anılan Madde hükmündeki altı ay olarak belirtilen sürenin ise azami süre olduđu görölmektedir.

Kişisel verilerin işlendikleri amaç için gerekli olan azami sürenin belirlenmesi, bu sürelerin kişisel veri işleme envanterinde belirtilen bilgilerle uyumu ve azami sürenin aşılp aşılmadığının takibinde, veri sorumlularınca hazırlanan, kişisel veri saklama ve imha politikasında kayıt altına alınan sürelerle denetimi mümkün kılınmıştır.

Özel nitelikli Kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemlerin, 07/03/2018 tarihli Resmi Gazete de yayımlanan 31/01/2018 tarihli Kişisel Verileri Koruma Kurul Kararı ve Kurumca yayımlanan Kişisel Veri Güvenliği Rehberi ile uygun güvenlik düzeyinin teminine yönelik idari tedbirlerin açıklığa kavuşturulduđu görölmektedir.

Kişisel verilerin elde edilmesi sırasında veri sorumluları veya yetkilendirdiđi kişilerce, ilgili kişilerin bilgilendirilmesi gerekmekte ve asgari olarak veri sorumlusunun ve varsa temsilcisinin kimliđi, kişisel verilerin hangi amaçla işleneceđi, kişisel verilerin kimlere ve hangi amaçla aktarılabilceđi, kişisel veri toplamanın yöntemi ve hukuki sebebini ortaya koyan aydınlatma yükümlülüđünün yerine getirilmesi sırasında uyulacak usul ve esaslar ile kişisel verilerin ilgili kişiden elde edilmemesi halinde aydınlatma yükümlülüđü, idare tarafından yürürlüđe konulan Tebliđ ile açıklığa kavuşturulmuştur.

Dava konusu Yönetmeliđin 7. maddesinin 5. fıkrasına yönelik olarak; madde metninde "veri sorumlusu, Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçer." kuralına yer verilmiş, ancak veri sorumlusu tarafından resen kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüđünün ortaya çıkması halinde, hangi yöntemle bu işlemi gerçekleştireceđi, bir başka deyişle hangi durumda tercihini nasıl kullanacağı ya da kullandığı yöntemin dođru yöntem olup olmadığının denetimine olanak sađlayan bir düzenleme yapılmamıştır. İlgili kişinin talebi halinde uygun yöntemin gerekçesinin açıklanması bir zorunluluk olmakla birlikte, resen karar vermesi halinde uygun yöntemin denetimine olanak sađlanmamıştır.

Açıklanan nedenlerle, davanın; Yönetmeliđin 7/1, 8/2, 9/2 10/3 ve 11 12/1-a(ilk cümlesi) ve 12/b maddelerine yönelik olarak reddine, 7/5 fıkrasına yönelik olarak eksik düzenleme nedeniyle iptaline karar verilmesi gerektiđi, düşünölmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay Onuncu Dairesince duruşma için taraflara önceden bildirilen 26/11/2020 tarihinde, davacı vekili Av. ...'un ve davalı idare vekili Av. ...'ün geldiği, Danıştay Savcısının hazır olduğu görülmekle, açık duruşmaya başlandı. Taraflara usulüne uygun olarak söz verilerek dinlendikten ve Danıştay Savcısının düşüncesi alındıktan sonra taraflara son kez söz verilip, duruşma tamamlandı. Tetkik Hâkiminin açıklamaları dinlendikten ve dosyadaki belgeler incelendikten sonra gereği görüldü:

MADDİ OLAY VE HUKUKİ SÜREÇ:

Dava, 28/10/2017 tarih ve 30224 sayılı Resmi Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 7. maddesinin 1. ve 5. fıkrasının, 11. maddesinin ve 12. maddesinin 1. fıkrasının (a) bendinin "Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu talebe konu kişisel verileri siler, yok eder ve veya anonim hale getirir." şeklindeki ilk cümlesinin, 8. maddesinin 2. fıkrasının, 9. maddesinin 2. fıkrasının, 10. maddesinin 3. fıkrasının ve 12. maddesinin 1. fıkrasının (b) bendinin iptali istemiyle açılmıştır.

İNCELEME VE GEREKÇE:

İlgili Mevzuat:

Anayasanın, "Özel hayatın gizliliği" başlıklı 20. maddesinde; "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.(...)

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmü yer almıştır.

Türkiye tarafından 30/01/2016 tarihinde 6669 sayılı Kanunla onaylanması uygun bulunan Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin 5. maddesinde, otomatik işleme konu olan kişisel verilerin, adil biçimde ve yasal yoldan elde edileceği ve işleneceği, belli ve meşru amaçlar için kaydedileceği ve bu amaçlara aykırı şekilde kullanılmayacağı, kaydedilme amaçlarına göre uygun ve yerinde olacağı ve aşırı olamayacağı, doğru bilgileri yansıtacağı ve gerektiğinde güncelleneceği, kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkan veren bir şekilde saklanacağı belirtilmiş; 6. maddesinde, iç hukukta uygun güvenceler sağlanmadıkça ırksal

kökeni, siyasi düşünceleri, dini veya diğer inançları ortaya koyan kişisel veriler ile sağlık veya cinsel hayatla ilgili kişisel verilerin, otomatik işlemeye tabi tutulmayacağı, aynı şeyin ceza mahkumiyetiyle ilgili kişisel veriler için de geçerli olduğu düzenlenmiş, 9. maddesinde de, Devlet güvenliği, kamu güvenliği, Devletin ekonomik menfaatlerinin korunması ve suçların önlenmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması ile verilerin istatistiki veya bilimsel amaçlarla kullanılması durumlarında kişisel verilerin korunmasına sınırlama getirilebileceği kabul edilmiştir.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 4. maddesinde; (1) Kişisel verilerin, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği, (2) Kişisel verilerin işlenmesinde; a) Hukuka ve dürüstlük kurallarına uygun olma, b) Doğru ve gerektiğinde güncel olma, c) Belirli, açık ve meşru amaçlar için işlenme, ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme, ilkelerine uyulmasının zorunlu olduğu, "Kişisel verilerin işlenme şartları" başlıklı 5. maddesinde; (1) Kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) Aşağıdaki şartlardan birinin varlığı hâlinde; a) Kanunlarda açıkça öngörülmesi., b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması., c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması., ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması., d) İlgili kişinin kendisi tarafından alenileştirilmiş olması., e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması., f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu, "Özel nitelikli kişisel verilerin işlenme şartları" başlıklı 6. maddesinde; (1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerinin özel nitelikli kişisel veri olduğu, (2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğu, (3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel verilerin, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebileceği, sağlık ve cinsel hayata ilişkin kişisel verilerin ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği, (4) Özel nitelikli kişisel verilerin

işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınmasının şart olduğu, hükmüne yer verilmiş, 7. maddesinin 1. fıkrasında; Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silineceği, yok edileceği veya anonim hâle getirileceği, 3. fıkrasında; Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esasların yönetmelikle düzenleneceği hükme bağlanmış, "Kurulun görev ve yetkileri" başlıklı 22. maddesinin 1. fıkrasının (e) bendinde; Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmak, Kurulun görev ve yetkileri arasında sayılmıştır.

Anılan Yasa hükümleri dayanak alınmak suretiyle Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasları belirlemek amacıyla, Kanunun 7. maddesi uyarınca veri sorumluları hakkında uygulanmak üzere hazırlanmış ve 28/10/2017 tarih ve 30224 sayılı Resmi Gazete'de yayımlanmıştır.

Dava Konusu Yönetmeliğin 7. maddesinin 1. ve 5. fıkrasının, 11. maddesinin 1. fıkrasının, 12. maddesinin 1. fıkrasının (a) bendinin "Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu talebe konu kişisel verileri siler, yok eder veya anonim hale getirir." şeklindeki ilk cümlesinin ve (b) bendinin İncelenmesi:

Davacı tarafından, Yönetmeliğin 7. maddesinin 1. ve 5. fıkrası, 11. maddesinin 1. fıkrası ile 12. maddesinin 1. fıkrasının (a) bendinin ilk cümlesinde yer alan düzenlemelere yönelik olarak; kişisel verinin ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin hükümlerin, idareye verinin akıbeti konusunda sınırsız bir takdir yetkisi tanınması anlamına geldiği, kişilere ait sağlık verileri gibi hassas verilerin işlendikleri sistemde işlenme koşulları kalksa da -talep olmadığı için- tutulmaya devam edilmesine yol açacağı, bu yöntemin kişisel veri sahibince bilinebilir ve denetlenebilir olmadığı; veri sorumlusunun resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı seçmesini öngören hükümlerin ise, kişisel veri sahibi kişiyi sürece hiçbir biçimde müdahalede bulunamayan, itiraz hakkı olmayan pasif süje haline getirdiği, bu durumun ülkemizce usulüne uygun biçimde onaylanarak yürürlüğe giren 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin 5/e maddesine ve Anayasa'nın 20. maddesine aykırı olduğu ileri sürülmektedir.

Yönetmeliğin 7. maddesinin 1. fıkrasında, Kanunun 5. ve 6. maddelerinde yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin veri sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesinin gerektiği; 5. fıkrasında, veri sorumlusunun, Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçeceği, ilgili kişinin talebi halinde uygun yöntemi gerekçesini açıklayarak seçeceği belirtilmiştir; 11. maddesinin 1. fıkrasında, kişisel veri saklama ve imha politikası hazırlamış olan veri sorumlusunun, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri sileceği, yok edeceği veya anonim hale getireceği düzenlenmiştir; 12. maddesinin 1. fıkrasının (a) bendinin ilk cümlesinde, ilgili kişi talep ettiğinde, kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusunun talebe konu kişisel verileri sileceği, yok edeceği veya anonim hale getireceği düzenlenmiştir.

Anayasa'nın "Özel hayatın gizliliği" başlıklı 20. maddesinin 3. fıkrasında "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilmiştir.

Bu doğrultuda, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek amacıyla çıkarılan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 7. maddesinde "(1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir. (2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır. (3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir." şeklinde düzenlemeler bulunmaktadır.

Yönetmeliğin dava konusu edilen; 6698 sayılı Kanun'un 5. ve 6. maddelerinde yer alan kişisel verilerin, işleme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin veri sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hale getirilmesinin gerektiğini; veri sorumlusunun, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçmesini; kişisel veri saklama ve imha politikası hazırlamış

olan veri sorumlusunun, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri silmesi, yok etmesi veya anonim hale getirmesini; ilgili kişinin veri sorumlusuna başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde, kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa, veri sorumlusunun talebe konu kişisel verileri silmesi, yok etmesi veya anonim hale getirmesini öngören hükümleri incelendiğinde; Yönetmeliğin 7. maddesinin 1. fıkrasının, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 7. maddesinin 1. fıkrasında yer alan düzenlemeyle aynı mahiyette olduğu, kişisel verilerin işlenmeleri için gerekli şartlar ortadan kalktığında periyodik aralıklarla resen silme, yok etme veya anonim hale getirme işlemlerinden birinin gerçekleştirileceği, bunun için muhakkak kişinin talebinin aranmadığı, resen silme, yok etme, anonim hale getirme işlemlerinden birine konu edilecek kişisel verinin talep üzerine bu işlemlerden birine tabi tutulmasına engel hüküm de bulunmadığı, 6698 sayılı Kanun'un 13. maddesi uyarınca ilgili kişinin, veri sorumlusuna başvurarak Kanun'un 11. maddesinde düzenlenen kendisiyle ilgili; a) Kişisel veri işlenip işlenmediğini öğrenme, b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme, c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme haklarını kullanabileceği, başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde 6698 sayılı Kanun'un 14. maddesi uyarınca Kurula şikâyette bulunabileceği görüldüğünden, bu haliyle kişisel verilerin resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin düzenlemeler içeren, iptali istenilen Yönetmelik hükümlerinde Anayasa, Kanun'a ve hukuka aykırı bir yön bulunmamaktadır.

Dava Konusu Yönetmeliğin 8. maddesinin 2. fıkrasının, 9. maddesinin 2. fıkrasının, 10. maddesinin 3. fıkrasının, 12. maddesinin 1. fıkrasının (b) bendinin İncelenmesi:

Davacı tarafından, Yönetmeliğin 8. maddesinin 2. fıkrası, 9. maddesinin 2. fıkrası, 10. maddesinin 3. fıkrası ve 12. maddesinin 1. fıkrasının (b) bendinde yer alan düzenlemelere yönelik olarak; Kanun'un 7/3. maddesi uyarınca kişisel verilerin silinmesine, yok edilmesine veya anonim hale getirilmesine

ilişkin usul ve esasların yönetmelikle düzenlenmesi gerekirken, Yönetmeliğin bu hususlarda yeterli ve objektif hükümler içermediği, maddelerde yer alan 'gerekli her türlü teknik ve idari tedbirler'in neler olduğunun Yönetmelik'te gösterilmediği, uygulamanın idarenin keyfiyetine ve kanaatine bırakıldığı, bu şekilde alınan kararların ilgili kişi ya da kamuoyu nezdinde denetlenebilirliği olmayacağı ve uygulamada birlik sağlanmasını zorlaştıracacağı, anılan hükümlerin hukuka aykırı ve noksan düzenleme niteliği taşıması nedeniyle iptali gerektiği ileri sürülmektedir.

Yönetmeliğin 8. maddesinin 2. fıkrasında, veri sorumlusunun, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlü olduğu; 9. maddesinin 2. fıkrasında, veri sorumlusunun, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlü olduğu, 10. maddesinin 3. fıkrasında, veri sorumlusunun, kişisel verilerin anonim hale getirilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlü olduğu belirtilmiştir; 12. maddesinin 1. fıkrasının (b) bendinde ilgili kişinin, veri sorumlusuna başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde; kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa veri sorumlusunun bu durumu üçüncü kişiye bildireceği, üçüncü kişi nezdinde bu Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin edeceği düzenlenmiştir.

Yönetmelik'te yer alan düzenlemeler bir bütün olarak incelendiğinde, Yönetmeliğin silme, yok etme ve anonim hale getirme kavramlarının tanımlandığı 8., 9. ve 10. maddelerinde veri sorumlusunun bu işlemlerle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlü olduğu belirtilmiştir. Silme, yok etme ve anonim hale getirmeye ilişkin hususların ayrıntılı bir şekilde ve standart olarak Yönetmelikle düzenlenmesinin birbirinden çok farklı kayıt sistemlerine sahip veri sorumluları açısından uygulamada sorunlar yaratabileceği, bunun yanında gelişen teknoloji, öngörülemeyen değişik durum ve yöntemler karşısında Yönetmelikte düzenlenecek usullerin yetersiz kalma riskinin olabileceği ve yönetmeliğin sık sık güncellenmesinin gerekebileceği açıktır. Yönetmeliğin 7. maddesinin 2. fıkrasında, Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Kanunun 4. maddesindeki genel ilkeler ile 12. maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve kişisel veri saklama ve imha politikasına uygun hareket edilmesinin zorunlu olduğu düzenlenmiştir. Bu kapsamda kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesinde uygulanacak teknik yöntemlerin, alınacak teknik ve idari tedbirlerin uygulamada açıklık sağlaması ve iyi uygulama örnekleri oluşturma amacıyla Kişisel Verileri Koruma Kurulu kararları ile "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale

Getirilmesi Rehberi" ile kişisel verilerin işleme sürecinde veri sorumlularının alması gereken tedbir ve idari tedbirler konusunda uygulamada açıklık sağlanması ve iyi uygulama örnekleri oluşturulması amacıyla "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)" hazırlandığı görülmektedir. Yönetmeliğin 12. maddesinin 1. fıkrasının (b) bendinde, ilgili kişinin veri sorumlusuna başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep etmesi durumunda kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa veri sorumlusu bu durumu üçüncü kişiye bildireceği; üçüncü kişi nezdinde bu Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin edeceğinin düzenlendiği, burada yer alan gerekli işlemler ifadesinin soyut ve belirsiz olmadığı, üçüncü kişilere aktarılan kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Yönetmelikte düzenlenen ve veri sorumlusunun yerine getirmekle yükümlü olduğu usul ve esasların bu kişisel veriler içinde uygulanacağını düzenlediği görülmektedir. Bu haliyle kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin düzenlemeler içeren, iptali istenilen Yönetmelik hükümlerinde Anayasa, Kanun'a ve hukuka aykırılık bulunmamaktadır.

Dava Konusu Yönetmeliğin 11. maddesinin İncelenmesi:

Davacı tarafından, Yönetmeliğin kişisel verileri resen silme, yok etme veya anonim hale getirme sürelerine ilişkin 11. maddesinde yer alan düzenlemelere yönelik olarak; 108 sayılı Sözleşme ile kişisel verilerin "kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde" saklanacağını kurala bağlandığı, dolayısıyla ilkesel olarak işleniş amacı ortadan kalkan verinin derhal sistemden silinmesi gerektiği, buna rağmen madde ile veri sorumlusuna veriyi imha için tanınan zaman aralıklarının ölçsüz biçimde uzun olduğu, derhal silinmesi gereken verinin ilk periyodik imha işlemine kadar sistemde tutulmasının hakkın özüne dokunur nitelikte olduğu, Kanunla belirlenen koşullar gerçekleştiği halde verinin periyodik imha işlemi için öngörülen altı aylık süre boyunca sistemde kalmasının Türk Ceza Kanunu'nun 138. maddesi kapsamında "Kişisel verileri yok etmeme" suçunu oluşturacağı, Yönetmelikle suç olan bir davranışa meşruiyet kazandırıldığı, ihtiyatlılık ilkesi uyarınca telafisi güç veya imkansız zararların doğması beklenilmeden sürelerin minimum düzeyde tutulması gerektiği, hukuka aykırı düzenlemeler içeren hükmün tamamının iptali gerektiği ileri sürülmektedir.

Yönetmeliğin 11. maddesinde, "(1) Kişisel veri saklama ve imha politikası hazırlamış olan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.

(2) Periyodik imhanın gerçekleştirileceği zaman aralığı, veri sorumlusu tarafından kişisel veri saklama ve imha politikasında belirlenir. Bu süre her halde altı ayı geçemez.

(3) Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden üç ay içinde, kişisel verileri siler, yok eder veya anonim hale getirir.

(4) Kurul, telafisi güç veya imkansız zararların doğması ve açıkça hukuka aykırılık olması halinde, bu maddede belirlenen süreleri kısaltabilir." hükümleri yer almaktadır.

Kişisel verilerin işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi ilkesi kişisel verilerin korunmasının en önemli ilkelerinden biridir. 6698 sayılı Kanun'un 7. maddesinde işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silineceği, yok edileceği veya anonim hale getirileceği kuralı getirilmiştir. Yönetmeliğin 4/ğ maddesinde "Periyodik imha: Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi" olarak tanımlanmıştır. Böylelikle kişinin talebi beklenmeksizin belli periyotlarla verilerin silinmesinin sağlanması amaçlanmıştır. Buna göre, kişisel verilerin bu işlemlere tabi tutulması için ilgilinin talebinin olmadığı hallerde periyodik aralıklarla idarece resen silinmesi, yok edilmesi, anonim hale getirilmesi verilerin süresiz biçimde muhafaza edilmesi ihtimalini ortadan kaldırmaya yöneliktir. Bu haliyle kişisel verileri resen silme, yok etme veya anonim hale getirme sürelerine ilişkin düzenlemeler içeren, iptali istenilen Yönetmelik hükümlerinde Anayasa, Kanun'a ve hukuka aykırılık bulunmamaktadır.

KARAR SONUCU:

Açıklanan nedenlerle;

1. 28/10/2017 tarih ve 30224 sayılı Resmi Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 7. maddesinin 1. ve 5. fıkrasının, 8. maddesinin 2. fıkrasının, 9. maddesinin 2. fıkrasının, 10. maddesinin 3. fıkrasının, 11. maddesinin ve 12. maddesinin 1. fıkrasının (a) bendinin "Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu talebe konu kişisel verileri siler, yok eder ve veya anonim hale getirir." şeklindeki ilk cümlesinin ve 12. maddesinin 1. fıkrasının (b) bendinin iptali istemiyle açılan DAVANIN REDDİNE,
2. Ayrıntısı aşağıda gösterilen toplam ... TL yargılama giderinin davacı üzerinde bırakılmasına,

3. Karar tarihinde yürürlükte bulunan Avukatlık Asgari Ücret Tarifesi uyarınca duruşmalı işler için belirlenen ... TL vekâlet ücretinin davacıdan alınarak davalı idareye verilmesine,
4. Posta gideri avansından artan tutarın kararın kesinleşmesinden sonra davacıya iadesine,
5. Bu kararın tebliğinden itibaren 30 (otuz) gün içerisinde Danıştay İdari Dava Daireleri Kuruluna temyiz yolu açık olmak üzere, Yönetmeliğin 7. maddesinin 5. fıkrası yönünden oy çokluğuyla, diğer maddeler yönünden oy birliğiyle, 26/11/2020 tarihinde karar verildi.

X -

KARŞI OY

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 4. maddesinde, imha; kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi olarak tanımlanmış; 7. maddesinin 5. fıkrasında, veri sorumlusunun, Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçeceği, ilgili kişinin talebi halinde uygun yöntemi gerekçesini açıklayarak seçeceği belirtilmiştir.

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 7. maddesinin 5. fıkrasında, veri sorumlusunun resen imha yükümlülüğünün ortaya çıkması halinde, hangi yöntemle imha işlemini gerçekleştireceğine, hangi durumlarda hangi imha yöntemini tercih edeceğine, tercih ettiği imha yönteminin nasıl denetleneceğine ilişkin bir düzenleme yapılmamıştır. Fıkra ilgili kişinin talebi halinde uygun yöntemin gerekçesi açıklanarak seçileceği düzenlenmesine rağmen imha yöntemine resen karar vermesi halinde bu seçimin gerekçesinin denetimine olanak sağlanmamıştır. Bu yönüyle Yönetmeliğin 7. maddesinin 5. fıkrasında, eksik düzenleme nedeniyle hukuka uygunluk bulunmamaktadır.

Açıklanan nedenlerle, Yönetmeliğin 7. maddesinin 5. fıkrasının iptaline karar verilmesi gerektiği oyuyla Daire kararına katılmıyorum.

Danıştay Kararı - 8. Daire (E. 2017/1388)

Danıştay Kararı - 8. D., E. 2017/1388 K. 2020/2838 T. 25.6.2020

Temyiz İsteminde Bulunan (Davalı): Türkiye Kamu Hastaneleri Kurumu

Vekili: Av. K1

Karşı Taraf(Davacı): K2

Vekili: Av. K3

İstemin Özeti: Malatya İdare Mahkemesinin 06/04/2016 gün ve E:2016/3, K:2016/426 sayılı kararının hukuka aykırı olduğu öne sürülerek, 2577 sayılı Kanunun 49. maddesi uyarınca temyizen incelenerek bozulması istemidir.

Savunmanın Özeti: Savunma verilmemiştir.

Danıştay Tetkik Hakimi: K4

Düşüncesi: Davalı idare tarafından yapılan temyiz isteminin reddedilerek Mahkeme kararının belirtilen gerekçe ile onanması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Hüküm veren Danıştay Sekizinci Dairesince işin gereği görüşüldü:

Dava, davacı vekili tarafından, davacının geçirmiş olduğu trafik kazası sebebiyle tedavi gördüğü Malatya Devlet Hastanesi'nde bulunan davacıya ait tüm tedavi evrakının bir örneğinin trafik sigortasına başvurmak üzere verilmesi istemiyle yapılan başvurunun reddine ilişkin işlemin iptali istemiyle açılmıştır.

İdare Mahkemesince, davacının avukat olan vekilince, sigorta şirketine başvurulacağı şeklinde sebebi açıklanmak ve ekinde vekaletname sunmak suretiyle tüm tedavi evrakının onaylı birer örneğinin verilmesi istemiyle yapılan başvurunun, istenilen belgelerin yasalarca istisna kapsamında tutulan bilgi ve belgelerden olmaması nedeniyle 1136 sayılı Avukatlık Kanununun 2. maddesi gereğince kabulü gerekirken, aksi yönde tesis edilen dava konusu işlemde hukuka uyarlık bulunmadığı gerekçesiyle dava konusu işlemin iptaline karar verilmiştir.

Türkiye Cumhuriyeti Anayasa'sının "Özel hayatın gizliliği" başlıklı 20/3. maddesinde, "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili

kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmü yer almaktadır.

07.04.2016 tarih ve 29677 sayılı Resmi Gazete'de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Amaç" başlıklı 1. maddesinde, "Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.;" "Tanımlar" başlıklı 3. maddesinin 1. fıkrasında; "a) Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı, (...) d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi, e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi, (...) ifade eder." ; Özel nitelikli kişisel verilerin işlenme şartları" başlıklı 6. maddesinin 1. fıkrasında, "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği,sağlığı,cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.;" 2. fıkrasında, "Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.;" 3. fıkrasında ise, "Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir." hükümlerine yer verilmiştir.

4982 sayılı Bilgi Edinme Hakkı Kanunu'nun "Bilgi verme yükümlülüğü" başlıklı 5/1. maddesinde, "Kurum ve kuruluşlar, bu Kanunda yer alan istisnalar dışındaki her türlü bilgi veya belgeyi başvuranların yararlanmasına sunmak ve bilgi edinme başvurularını etkin, süratli ve doğru sonuçlandırmak üzere, gerekli idari ve teknik tedbirleri almakla yükümlüdürler." hükmüne yer verilmiş; öte yandan bilgi edinme hakkının sınırlarının düzenlendiği dördüncü bölüm altında yer alan "Özel hayatın gizliliği" başlıklı 21. maddesinde ise, "Kişinin izin verdiği haller saklı kalmak üzere,

özel hayatın gizliliği kapsamında, açıklanması halinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, mesleki ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır. Kamu yararının gerektirdiği hallerde, kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir." düzenlemesine yer verilmek suretiyle kişilerin sağlık bilgilerinin anılan Kanun kapsamı dışında yer aldığı ifade edilmiştir.

1136 sayılı Avukatlık Kanunu'nun "Avukatlığın amacı" başlıklı 2. maddesinin 3. fıkrasında, "Yargı organları, emniyet makamları, diğer kamu kurum ve kuruluşları ile kamu iktisadi teşebbüsleri, özel ve kamuya ait bankalar, noterler, sigorta şirketleri ve vakıflar avukatlara görevlerinin yerine getirilmesinde yardımcı olmak zorundadır. Kanunlarındaki özel hükümler saklı kalmak kaydıyla, bu kurumlar avukatın gerek duyduğu bilgi ve belgeleri incelemesine sunmakla yükümlüdür. Bu belgelerden örnek alınması vekaletname ibrazına bağlıdır. (...)" hükmüne yer verilmiştir.

Dosyanın incelenmesinden, davacı vekili tarafından, davacının 25.03.2015 tarihinde trafik kazası geçirmesi sebebiyle Malatya Devlet Hastanesi'nde tedavi gördüğünden bahisle, davacıya ait tüm tedavi evrakının bir örneğinin trafik sigortasına verilmek üzere 1136 sayılı Avukatlık Kanunu'nun 2. maddesine dayanılarak 14.05.2015 tarihli dilekçe ile istenilmesi üzerine, davacıya ait vekaletnamenin usulüne uygun bulunmadığı ancak eksikliklerin giderilmesi halinde ilgili bilgi-belgelerin gönderilebileceği gerekçesiyle 18.05.2015 tarih ve 05 sayılı işlemle reddedilmesi üzerine bakılmakta olan davanın açıldığı anlaşılmaktadır.

Yukarıda yer verilen 6698 sayılı Kanun'un 3. maddesine göre kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Anayasa Mahkemesinin kararlarında da belirtildiği üzere "... adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler" kişisel veri olarak kabul edilmektedir.

6698 sayılı Kanunda kişisel verilerin işlenmesine ilişkin genel şartlar ortaya konulmakla birlikte yasa koyucunun takdir yetkisi kapsamında kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri gibi

özel nitelikli kişisel verilerin işleme şartlarının ayrı bir düzenlemeye tabi tutulduğu, bu düzenlemeyle birtakım kişisel verilerin özel hukuki koruma altına alındığı görülmektedir.

Özel nitelikli kişisel verilerin işlenebilmesi için kural olarak ilgililerin açık rızasının bulunması gerekmektedir. Ancak 6698 sayılı Kanun'un 6. maddesinin 3. fıkrasında, sağlık ve cinsel hayat dışındaki özel nitelikli kişisel verilerin, "Kanunlarda öngörülen hallerde" ilgililerin açık rızası aranmaksızın da işlenebileceği belirtilmek suretiyle anılan kuralın istisnasına yer verilmiştir. Bununla birlikte sağlık ve cinsel hayata ilişkin kişisel verilerin ise bu istisnadan da istisna edilerek ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği ifade edilmek suretiyle, önemine binaen "Kanunlarda öngörülen hallerde" şeklinde bir ifade biçimiyle yetinilmeyerek, bu verilerin ilgililerin açık rızası aranmaksızın işlenebileceği hallerin doğrudan Kanun maddesinde düzenlendiği görülmektedir.

Şu halde, kökeni Roma Hukukuna dayanan ve günümüzde genel hukuk kaidesi olarak kabul gören "istisna içerikli hükümlerin dar yorumlanması" (singularia non sunt extenda) ilkesi uyarınca, işleme şartları bizzat 6698 sayılı Kanun'da yer alan kişilerin sağlık verilerine ilişkin bilgilerin, ancak kişinin açık rızası halinde işlenebileceği, "işlenme" ifadesinden ise, ilgili verinin açıklanması, aktarılması, elde edilebilir hale getirilmesi gibi her türlü işlemin anlaşılması gerektiği açıktır.

Diğer taraftan, Avukat-müvekkil ilişkisi temelde 6098 sayılı Türk Borçlar Kanunu'nun 502 ve devamı maddelerinde yer alan "vekalet sözleşmesi"ne dayanmakta olup; vekilin üstlendiği iş ve hizmetleri, vekalet verenin haklı menfaatlerini gözeterek, sadakat ve özenle yürütme ödevi bulunmaktadır. Bu özen görevi, 1136 sayılı Kanun'da da avukatın işini özenle ve sonuna kadar takip etme (m. 34 ve 171) ödeviyle de somutlaştırılmış bulunmaktadır. Öte yandan 1136 sayılı Avukatlık Kanunu'nun 2. maddesinde, avukatlığın amacının, hukuki münasebetlerin düzenlenmesini, her türlü hukuki mesele ve anlaşmazlıkların adalet ve hakkaniyete uygun olarak çözümlenmesini ve hukuk kurallarının tam olarak uygulanmasını her derecede yargı organları, hakemler, resmi ve özel kişi, kurul ve kurumlar nezdinde sağlamak olduğu, avukatın bu amaçla hukuki bilgi ve tecrübelerini adalet hizmetine ve kişilerin yararlanmasına tahsis edeceği ifade edildikten sonra aynı maddenin 3. fıkrasında, madde metninde sayılan kamu kurum ve kuruluşları ile özel hukuk tüzel kişilerinin avukatların ihtiyaç duyduğu bilgi ve belgeleri incelemeye sunmakla yükümlü kılınarak avukatlara görevlerinin yerine getirilmesi kapsamında, müvekkilinin hukukunu savunabilmesine, haklarını dava etmesine, yargılama sürecinin çabuklaştırılmasına ve uyuşmazlıkların adalet ve hakkaniyete uygun olarak

çözümlemesine yardımcı olma görevinin yüklendiği anlaşılmaktadır. Şüphesiz bu yükümlülük, "Kanunlardaki özel hükümler saklı kalmak kaydıyla" ilgili kurum ve kuruluşlara getirilmiş olup mutlak değildir.

Olayda, davacının Malatya 1. Noterliği'nin 05.05.2015 tarih ve 7970 yevmiye numaralı vekaletnamesi ile davacı vekiline verdiği vekaletname içeriğinde, "... adıma hastanelerde gerekli evraklar ile tüm tedavi evraklarını almaya (...) yetkili olmak üzere" ifadesiyle açıkça avukat olan vekilini yetkilendirdiği görülmekte olup, davacının açık rızasını yansıtan bu ifadenin özel nitelikli kişisel veri mahiyetinde bulunan sağlık bilgilerine ilişkin kayıtların 1136 sayılı Kanun ve 6698 sayılı Kanun hükümleri çerçevesinde avukatı tarafından istenebilmesine olanak tanıdığından, vekaletnamenin usulüne uygun bulunmadığı gerekçesiyle talebin reddedilmesine ilişkin dava konusu işlemde hukuka uyarlık bulunmamaktadır.

İdare ve vergi mahkemeleri tarafından verilen kararların temyiz yolu ile incelenip bozulabilmeleri 2577 sayılı İdari Yargılama Usulü Kanununun 49. maddesinin 1. fıkrasında yazılı nedenlerin bulunmasına bağlıdır.

Açıklanan nedenlerle, davalı idarenin temyiz isteminin reddiyle Malatya İdare Mahkemesince verilen ve hüküm fıkrası itibarıyla hukuka uygun bulunan kararın yukarıda belirtilen gerekçeyle onanmasına ve temyiz giderlerinin istemde bulunan üzerinde bırakılmasına, bu kararın tebliğ tarihini izleyen 15 (onbeş) gün içerisinde kararın düzeltilmesi yolu açık olmak üzere, 25/06/2020 tarihinde gerekçede oyçokluğu; esasta oybirliği ile karar verildi.

KARŞIOY:

- İdare ve vergi mahkemeleri tarafından verilen kararların temyiz yolu ile incelenip bozulabilmeleri 2577 sayılı İdari Yargılama Usulü Kanununun 49. maddesinin 1. fıkrasında yazılı nedenlerin bulunmasına bağlıdır.

İdare Mahkemesince verilen karar ve dayandığı gerekçe usul ve yasaya uygun olup, değişik gerekçeyle onanmasını gerektiren bir neden bulunmadığından, Mahkeme kararının onanması gerektiği görüşüyle çoğunluk kararına katılmıyorum.

Danıştay Kararı - 10. Daire (E. 2017/1141)

Danıştay Kararı - 10. D., E. 2017/1141 K. 2018/1737 T. 14.5.2018

İstemin Özeti: İstanbul 8. İdare Mahkemesi'nin davanın reddi yolunda verilen 18/12/2015 tarih ve E:2015/1370, K:2015/2690 sayılı kararının hukuka uygun olmadığı ileri sürülerek temyizen incelenerek bozulması davacı sendika tarafından istenilmektedir.

Savunmanın Özeti: Temyiz isteminin reddi gerektiği savunulmaktadır.

Danıştay Tetkik Hakimi: K1

Düşüncesi: İdare Mahkemesi kararının bozulması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Hüküm veren Danıştay Onuncu Dairesi'nce gereği görüşüldü:

Dava, davacı sendika tarafından, davalı idarenin taşra birimlerinde görev yapan personelin izlenmesini teminen odalarına monitor yerleştirildiği ve kamera kayıt sisteminin kurulduğu, güvenlik amacıyla binaların girişlerine yerleştirilenler dışında çalışanların birimlerde (odalarda) izlenmesine imkan veren kamera sisteminin kişi mahremiyetini ihlal edeceği ileri sürülerek, personelin izlenmesine imkan veren kamera sisteminin kaldırılması talebiyle 06/04/2015 tarih ve 269 sayılı dilekçe ile yapılan başvurunun zımnen reddine yönelik davalı idare işleminin iptali istemiyle açılmıştır.

İstanbul 8. İdare Mahkemesi'nce; davalı idarenin kaçakçılıkla mücadele kapsamında 5607 sayılı Kanun kapsamında bir takım yükümlülüklerinin bulunduğu, kapalı devre kamera sisteminin bu yükümlülüğün yerine getirilmesi ve görevin önem ve özelliği dikkate alınarak gümrük idarelerinin takibi amacıyla kurulduğu, bu kapsamda hizmet binalarının koridor, giriş-çıkış ve mükelleflerin yoğun olduğu bölümlerine kapalı devre kamera sistemi kurulmasının kamu yararını gerçekleştirme amacına uygun olduğu, Anayasa'nın 20. maddesi ile güvence altına alınan özel hayatın gizliliğinin ihlalinin söz konusu olmadığı, davacı sendikanın taşra birimlerine kurulan kapalı devre kamera sisteminin kaldırılması talebinin zımnen reddine ilişkin işlemde hukuka aykırılık bulunmadığı gerekçeleriyle davanın reddine karar verilmiştir.

Davacı sendika tarafından, yapılan uygulamanın ve tesis edilen işlemin çalışanların özel hayatının gizliliğini ihlal ettiği ve bu nedenle hukuka aykırı olduğu ileri sürülerek İdare Mahkemesi kararının temyizen incelenerek bozulması istenilmektedir.

Davacı sendikanın temyiz gerekçesi olarak özel hayatın gizliliği ve mahremiyet hakkını ileri sürmüş olması dikkate alındığında, davanın incelenmesinde öncelikle özel hayat kavramının mahkeme kararları da dikkate alınarak Anayasal ve yasal açıdan değerlendirilmesi ve bu hakkın sınırlarını da ortaya koyacak şekilde çerçevesinin çizilmesi gerekmektedir.

Anayasa Mahkemesinin özel hayatın gizliliği ve mahremiyet hakkını dikkate alarak vermiş olduğu Başvuru No:2014/12591, Başvuru No:2014/11218, Başvuru No:2016/431 gibi bir çok farklı kararında şu tespitler yer almıştır.

Özel hayat kavramı eksiksiz bir tanımı bulunmayan geniş bir kavramdır. Bu kapsamda korunan hukuki değer esasen kişisel bağımsızlıktır. Özel hayata saygı hakkının kapsamının belirlenmesinde "bireyin kişiliğini geliştirmesi ve gerçekleştirilmesi" kavramı temel alınmaktadır. Anılan hak, herkesin istenmeyen bütün müdahalelerden uzak kendine özel bir ortamda yaşama hakkına sahip olduğuna işaret etmekle birlikte, kişiliğin serbestçe geliştirilmesiyle uyumlu birçok hukuki menfaati de içermektedir.(Serap Tortuk, B. No: 2013/9660, 21/1/2015, §§ 31-36; Bülent Polat [GK], B. No: 2013/7666, 10/12/2015, §§ 61-63; Tefvik Türkmen [GK], B. No: 2013/9704, 3/3/2016, §§ 50-52; Ata Türkeri, B. No: 2013/6057, 16/12/2015, §§ 30-32).

Özel hayata saygı hakkı kapsamında korunan hukuksal çıkarlardan biri de bireyin mahremiyet hakkıdır. Özel hayata saygı hakkı, ilişki kurmak ve geliştirmek üzere çevresinde bulunanlarla temas kurma hakkını da içermektedir. Kişilerin mesleki hayatı özel hayatlarıyla sıkı bir irtibat içindedir. Özel hayata dair hususlar kişinin mesleği ile ilgili tasarruflara esas alınmışsa özel hayata saygı hakkı gündeme gelecektir. (Bülent Polat, § 62; Ata Türkeri, § 31).

Gelişen teknolojinin, kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması amacıyla, kamu kesiminde kullanılmaya başlanması doğaldır. Ancak; teknoloji kullanılarak kişisel görüntülerin kayıt altına alınmasında özel hayatın gizliliği ve kişilerin mahremiyet hakkı da dikkate alınarak uygulama yapılması gerektiğinde kuşku ve duraksamaya yer bulunmamaktadır.

Buna ek olarak, kamu çalışanlarının faaliyet yürüttüğü servislerde çalışanların çalışma alanlarını ve dolayısıyla çalışanları görecektir şekilde yerleştirilen, güvenlik ve suçun önlenmesi gibi nedenlerle uygulandığı ileri sürülen kameralı takip sistemleri kullanılarak kişisel görüntülerin alınması, temel hak ve hürriyetler içerisinde sayılan özel hayatın gizliliği ilkesi kapsamında özel hayata müdahale

olarak ele alınmalı, bu müdahalenin hukuka uygunluğunun değerlendirilmesi ise kanunilik, ölçülülük gibi anayasal kavramlar yanında Avrupa İnsan Hakları Mahkemesi kararları ve Anayasa Mahkemesi kararları dikkate alınarak yapılmalıdır.

Yukarıda anılan müdahale, Anayasa'nın 13. maddesinde belirtilen koşulları yerine getirmediği müddetçe aynı zamanda Anayasa'nın 20. maddesinin ihlalini de teşkil edecektir.

Anayasa'mızın 13. maddesi "Temel hak ve hürriyetler, ... yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, ... demokratik toplum düzeninin... gereklerine ve ölçülülük ilkesine aykırı olamaz. " şeklindedir.

Bu sebeple müdahalenin ihlal oluşturup oluşturmadığının belirlenmesinde, Anayasa'nın 13. maddesinde öngörülen ve somut başvuruya uygun düşen kanunlar tarafından öngörülme, Anayasa'nın ilgili maddesinde belirtilen nedenlere dayanma, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmama koşulları yönünden inceleme yapılması gerekir.

Anayasa'nın 13. maddesi, temel hak ve özgürlüklerin sınırlandırılmasını, ilgili hak ve özgürlüğe ilişkin Anayasa maddesinde gösterilen özel sınırlandırma sebeplerinin bulunmasına bağlı kılmıştır. Bununla birlikte Anayasa Mahkemesinin kararlarına göre, özel sınırlama nedeni öngörülmemiş olan hakların dahi, hakkın doğasından kaynaklanan bazı sınırları bulunmaktadır. Ayrıca Anayasa'nın diğer maddelerinde yer alan kurallara dayanılarak da bu hakların sınırlanması mümkün olabilmektedir. Buna göre, Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebileceği kabul edilmektedir (AYM, E.2014/87, K.2015/112).

Anayasa'nın 20. maddesi "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kağıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakim tarafından onayına sunulur. Hakim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar." hükmünü haizdir.

Anayasa'nın 20. Maddesinin 1. fıkrası yönünden özel sınırlama nedeni düzenlenmemiştir. Maddenin ikinci fıkrasında, birtakım sınırlama sebeplerine yer verilmiş olmakla beraber bu sebepler sadece

arama ve elkoyma tedbirlerine yöneliktir. Dolayısıyla bu sebeplerin özel hayata saygı hakkının tüm boyutları yönünden uygulanması mümkün görünmemektedir.

Bu durumda, Anayasa'nın diğer maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin somut olay bakımından sınırlandırma sebebi olarak kabul edilip edilemeyeceği araştırılmalıdır.

Anayasa'nın 5. maddesinde, "Devletin temel amaç ve görevleri, Türk Milletinin bağımsızlığını ve bütünlüğünü, ülkenin bölünmezliğini, Cumhuriyeti ve demokrasiyi korumak, kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak; kişinin temel hak ve hürriyetlerini, sosyal hukuk devleti ve adalet ilkeleriyle bağdaşmayacak surette sınırlayan siyasal, ekonomik ve sosyal engelleri kaldırmaya, insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmaktır. " denilmektedir. Buna göre kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak devletin temel amaç ve görevlerindedir.

Kişinin ve toplumun refah, huzur ve mutluluğunu sağlamanın ön koşulu milli güvenlik ve kamu düzeninin tesisidir. Milli güvenlik ve kamu düzeninin sağlanmadığı bir ortamda, hak ve özgürlüklerden gereği gibi yararlanılması, kişinin maddi ve manevi varlığını geliştirmesi mümkün değildir. Devletin hak ve özgürlükleri koruma ödevinin yanında, milli güvenliği ve kamu düzenini sağlama görevi de bulunmaktadır.

Yukarıda ifade edilen sınırlama nedenleri de dikkate alındığında uyuşmazlığın sağlıklı çözümü için; sınırlandırmanın, "demokratik toplum düzeninin gereklerinden olması" ve "ölçülülük ilkesine uygun olması"nın ne anlama geldiğinin de ortaya konması gerekmektedir.

"Demokratik toplum düzeninin gereklerinden olma, bir sınırlamanın demokratik bir toplumda zorlayıcı bir toplumsal ihtiyacın karşılanması amacıyla yönelik olmasını ifade etmektedir. Buna göre sınırlayıcı tedbir, bir toplumsal ihtiyacı karşılamıyorsa ya da başvurulabilecek son çare niteliğinde değilse demokratik toplum düzeninin gereklerine uygun bir tedbir olarak değerlendirilemez. (AYM, E.2015/96, K.2016/9, 10/2/2016 § 13; ifade özgürlüğü bağlamında Bekir Coşkun [GK], B. No: 2014/12151, 4/6/2015, § 51; özel hayatın gizliliği hakkı bağlamında Ata Türkeri, § 44;İ.F.A., B. No: 2013/8564, 17/2/2016, § 62).

Bu kapsamda kamu makamlarının faaliyetin niteliği ve sınırlamanın amacına göre değişen geniş bir takdir yetkisinin bulunması doğaldır. Ancak özel hayatın gizliliği hakkının mahremiyet hakkı gibi en gizli yönleri söz konusu olduğunda kamu makamlarının takdir yetkisi daha dardır ve bu alanlara

yönelik müdahalelerin haklı olduğunun kabul edilebilmesi için kamu makamlarınca özellikle ciddi gerekçelerin gösterilmesi gerekir. (Ata Türkeri, § 47).

Kamu makamlarının özel hayata müdahaleleriyle ilgili olarak, müdahaleye yol açan karar alma sürecinde de keyfi davranmadıklarını kanıtlamaları gereklidir. Ancak bu halde de sınırlandırmanın ölçülülük ilkesine uygun olması gereklidir. (Ata Türkeri, § 48).

Anayasa Mahkemesi kararları uyarınca ölçülülük ilkesi, sınırlayıcı önlemin öngörülen amaç için zorunlu ve amaca ulaşmaya elverişli olmasını ayrıca amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder. Ölçülülük ilkesinin amacı da temel hak ve özgürlüklerin gereğinden fazla sınırlandırılmasının önlenmesidir (AYM, E.2015/102, K.2016/151, 7/9/2016, § 22; E.2012/100, K.2013/84, 4/7/2013; Marcus Frank Cerny, B. No: 2013/5126, 2/7/2015, § 72).

Avrupa İnsan Hakları Sözleşmesi'nin "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesi şöyledir: "(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. (2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir. "

Kamu makamlarının özel hayata saygı hakkına keyfi bir şekilde müdahale etmelerinin önlenmesi, Sözleşme'nin 8. maddesi ile sağlanan güvenceler kapsamında yer almaktadır. Avrupa İnsan Hakları Mahkemesi (AİHM), devletin özel hayata saygı hakkı kapsamında bulunan bir menfaate müdahale ettiğini tespit ettiğinde, 8. maddenin ikinci fıkrasında belirtilen koşulları incelemektedir. Buna göre kamu makamlarının müdahalesinin yasal bir dayanağı olup olmadığı, anılan fıkrada yer alan meşru amaçlara dayalı olup olmadığı, demokratik bir toplumda gerekli ve öngörülen amaçla orantılı olup olmadığı araştırılmaktadır. (AİHM Dudgeon/Birleşik Krallık, § 43; Olsson/İsveç No.1, B. No: 10465/83, 24/3/1988, § 59)

Ayrıca, AİHM kararlarına göre Sözleşme'nin 8. maddesi açıkça usul şartları içermemekle birlikte anılan maddeyle güvence altına alınan haklardan etkili bir şekilde yararlanılabilmesi için müdahaleyi doğuran karar alma sürecinin bu maddeyle korunan hak ve özgürlüklere gerekli saygıyı sağlayacak nitelikte ve adil olması gerekir. Bu şekildeki bir süreç başvurusunun 8. maddedeki haklarını -deliller ve kanıtlanma konuları dahil- adil şartlarda savunabileceği usule ilişkin etkili güvencelerden yararlandırılmasını gerektirir. AİHM'e göre bu şekildeki güvencelerin amacı 8. maddede yer alan haklara keyfi şekilde müdahalede bulunulmasını önlemek, müdahalenin gerekçelendirilmesini

sağlamaktır (AİHM Ciubotaru/Moldova, B. No: 27138/04, 27/4/2010, § 51; T.P. ve K.M./Birleşik Krallık, B. No: 28945/95, 10/5/2001, § 72).

AİHM'e göre gerek negatif yükümlülükler gerekse pozitif yükümlülükler bakımından söz konusu usule ilişkin etkili güvencelerin sunulması gerekmektedir. (Benzer yöndeki AİHM kararı için bkz. Hokkanen/Finlandiya, B.No: 19823/92, 23/9/1994, §§ 55-58; Glaser/Birleşik Krallık, B. No: 32346/96, 19/9/2000, §§ 63-66; Bajrami/Arnavutluk, B. No: 35853/04, 12/12/2006, §§ 50-55; Abdulaziz, Cabales ve Balkandali/Birleşik Krallık, B. No: 9214/80, 28/5/1985, § 67).

Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesinin "Mahremiyet Hakkı" başlıklı 17. maddesinde de, hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemeyeceği; onuru veya itibarının hukuka aykırı saldırılara maruz bırakılmayacağına, herkesin bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahip olduğu belirtilmiştir.

Avrupa İnsan Hakları Mahkemesinin Antovic ve Mirkovic v. Sırbistan ve Karadağ (Başvuru No. 70838/13) kararında, çalıştıkları anfi alanlarına demirbaş ve öğrenciler de dahil kişi güvenliğinin sağlanması amacıyla kamera sistemi kurulan iki profesörün özel hayatlarının gizliliğinin ihlal edildiğine karar vermiştir. Kararda özellikle Avrupa İnsan Hakları Mahkemesinin daha öncede benzer konularda vermiş olduğu kararlara atıfta bulunularak bazı tespitlere de yer verilmiştir.

Bu tespitler arasında özellikle kişilerin iş yerinde ve çalışma ortamında yani kamusal bir alanda bulunsa da, özel hayatın profesyonel aktiviteler ve dış dünya ile ilişkileri de kapsayan ve Avrupa İnsan Hakları Mahkemesinin "sosyal özel hayat" olarak adlandırdığı bir alanı da kapsadığı ve bu alanın da korunması gerektiği, kamera sistemleri ile kişilerin sosyal özel hayatlarının izlenmesinin "ciddi bir müdahale" olarak kabul edilmesi gerektiği, kişilerin güvenliği veya işverenin hakları başka yollarla korunamıyorsa ancak son çare olarak kamera sistemlerinin kişilerin çalışma alanlarını göreceği şekilde kurulmasının kabul edilebilir olacağı tespitlerine yer verilmiştir. Yine Avrupa İnsan Hakları Mahkemesinin Lopez Ribalba ve Ötekiler v. İspanya (Başvuru No. 1874/13) kararında da iş verenin başka yollarla korunabilecek haklarını kamera sistemi yoluyla korumasının son çare olduğu, bu durumda bile kamera sistemleri ile ilgili olarak bildirimde bulunması ve usulleri belirlemesi gerektiği vurgulanmıştır.

Yine yukarıda yer verilen kararlardan, farklı güvenlik önlemleri yoluyla korunabilecek haklar veya önlenilecek olaylara yönelik olarak kamera sistemleri kurulmaması gerekeceği ve çalışanların doğrudan çalışma alanlarını görüntüleme şeklinde kişilerin özel hayatına müdahale anlamına gelen

bu sistemlerin bu durumlarda kullanılmaması gerekeceği, aksinin ölçülülük ilkesine aykırı olacağı sonucuna ulaşılmaktadır.

Avrupa İnsan Hakları Mahkemesi kararlarında yukarıda ifade edilen Antovic ve Mirkovic v. Sırbistan ve Karadağ (Başvuru No. 70838/13) kararında da yer aldığı gibi kamera sistemleri ile ilgili olarak belli başlı şartların ortaya konulması gerektiği de ifade edilmiştir. Bunlar özellikle uygulamanın kanuni bir dayanağı olması, sınırlı bir izleme olması ve kötüye kullanmaya karşı garantiler olması gerektiğidir.

Türk Ceza Kanunu'nun "Özel hayatın gizliliğini ihlal" başlıklı 134. maddesi "Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.", "Kişisel verilerin kaydedilmesi" başlıklı 135. maddesi ise "Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir." hükmü yer almaktadır.

Ceza Muhakemesi Kanunu'nun "İletişimin tespiti, dinlenmesi ve kayda alınması" başlıklı 135. maddesi düzenlemesi de "başka suretle delil elde edilmesi imkânının bulunmaması durumunda" iletişimin kayda alınabileceğini, "Teknik araçlarla izleme" başlıklı 140. maddesi ise "başka suretle delil elde edilememesi hâlinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyeri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabilir" hükmü yer almakta olup, bu düzenlemeler de suça yönelik kuvvetli şüphe halinde bile en son çare olarak ses ve görüntü kaydına başvurulması gerektiğini ortaya koymaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanunu, 07.04.2016 tarihli ve 29677 Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Dava konusu işlem tarihinde yürürlükte bulunmamakla beraber konunun önemine binaen, dava konusu edilen kamera sistemleri ile ilgili belli başlı düzenlemelere de yer vermiştir. Neden bu sistemine ihtiyaç duyulduğunun ortaya konulması, sistemden kimin veya kimlerin yasal olarak sorumlu olduğunun belirlenmesi, sisteminin maksada uygun olup olmadığının ortaya konulması, özel hayatın gizliliğinin ihlal edilip edilmediğini kimin kontrol edeceğinin ve görüntülere kimin ulaşımı olacağının belirlenmesi ve bu hususların olarak kayıt altına alınması, kayıtlarının güvenliğinin ve gizliliğinin sağlanması güvenlik prosedürleri hazırlanması, kameralarla gözlemlenen bölgelerin girişinde ve içerideki uygun yerlerde bölgenin kamera sistemleri tarafından gözetlendiği ve kayıt altına alındığının belirtilmesi gerektiği, sistemin kuruluş maksadıyla bağdaşmayan görüntülerin gereğinden uzun süre saklanmaması, kişilerin özel hayatın gizliliğinin sağlanması yönünde beklentisinin olabileceği görüntülerin yetkili kişiler haricinde hiç kimse tarafından izlenememesi için alınacak önlemler gibi bir çok konuda düzenleme getirilmiştir.

Tüm bu açıklamalar ışığında dava konusu işlem incelendiğinde, Avrupa İnsan Hakları Mahkemesi kararları da dikkate alındığında hakların korunması başka şekilde sağlanamıyorsa kamera sistemlerinin çalışanların çalışma alanlarını görecektir şekilde kurulmasının mümkün olduğu ancak bunun bir son çare olarak değerlendirildiği ve bu düzenlemenin içeriğini ayrıntılı olarak ortaya koyan bir özel düzenleyici işlem olması gerektiği, kamera sistemlerinin çalışma alanlarını çekmesinin özel hayatın gizliliğini ihlal ettiği, sınırlı bir izleme sağlayacak şekilde güvenlik amacıyla giriş ve çıkışları izlemek üzere veya vatandaşlara da açık olan ortak alanlar ve iş sahiplerinin de giriş çıkışına açık, yoğun bir alışveriş trafiği olan alanlarda kurulabileceği ancak bu kameraların da çalışanların iş yapış şekillerini denetlemek veya sürekli olarak belli kişileri çekecek şekilde kurulmaması gerektiği, güvenlik amacıyla kurulmuş olmaları gerektiği ve bu nedenle amaca hizmet eder şekilde konumlandırılması gerektiği anlaşılmaktadır.

Yine kamera sistemlerinin zorunlu güvenlik amacı ile ve başka bir yolla bu güvenlik amacı sağlanamıyorsa kurulabilmesi mümkün olsa da, yukarıda yer verilen açıklamalar ışığında uygulamanın usul ve esaslarını gösteren yasal dayanağının bulunması, açık ve anlaşılabilir olması ve ilgililerin bu konudaki hakları ve kamera sistemi ile ilgili olarak bilgilendirilmiş olması gerektiği, toplanan görüntülerle ilgili güvencelerin sağlanması gerektiği, dava konusu işlemin bu haliyle sınırları belirlenmemiş, yasal dayanağı olmayan, uygulamaya dair usul ve esaslar ile güvenceleri düzenlenmemiş bir sistemle yürütüldüğü ve bu haliyle kamu yararına yönelik olduğunu kabul etmeye imkan olmadığı; Anayasal bir ilke olan ölçülülük ilkesine aykırılık teşkil ettiği ve mahremiyet hakkını ihlal ettiği anlaşılmakta olup, kişilik haklarına aykırı şekilde kamu görevlilerinin tüm faaliyetlerinin izlenmesine imkan tanıyan uygulamada isabet bulunmamaktadır.

Kameralı takip sistemi ile kurumca amaçlanan kamu yararı arasında orantılılık bulunmadığından uygulama ölçülülük ilkesine de aykırılık teşkil etmektedir. Anayasa'nın 13. maddesinde, temel hak ve hürriyetlerin ancak kanunla sınırlanabileceği, değişik 20/3. maddesinde de, kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceğinin belirtildiği, ancak konuyla ilgili dava konusu işlemin gerçekleştirildiği aşamada yasal bir düzenlemenin yapılmadığı anlaşılmaktadır.

İdarelerin teknolojik gelişmelerden de yararlanarak kamu çalışanlarının faaliyet yürüttüğü alanda güvenlik ve suçun önlenmesi amacıyla kameralı takip sistemi uygulamasının, güvenlik amaçlı olarak giriş ve çıkışlar ve güvenliğin özel önem arz ettiği alanlar dışında, günlük iş ve işlemleri yürüten çalışanların çalışma odalarını ve servisleri çekecek şekilde yerleştirildiği durumlarda, kamusal alanda da olsa "özel hayatın gizliliği" ilkesi kapsamında bulunduğu Avrupa İnsan Hakları Mahkemesi

kararları ve Dairemizin daha önceki tarihli kararlarından anlaşılmaktadır. Yine uygulamanın sınırlarını, usul ve esaslarını gösteren bir yasal dayanağın bulunması, toplanan görüntülerin ileride başka bir şekilde kullanılmayacağına dair bir güvencenin mevcut olması gerektiği de anlaşılmaktadır.

İdarenin güvenlik ve kamu yararını sağlama ihtiyacı ve çalışanların özel hayatın gizliliği gibi haklarının karşı karşıya geldiği bu gibi uyuşmazlıklarda, olayın dosyaya özel olarak ele alınması ve değerlendirilmesi gerektiği açıktır.

Uyuşmazlığın bu davaya özgü hali değerlendirildiğinde; dava konusu olayda davalı idarenin taşra birimlerinde görev yapan personelin izlenmesini teminen odalarına monitor yerleştirildiği ve kamera kayıt sisteminin kurulduğu ileri sürülerek güvenlik amacıyla binaların girişlerine yerleştirilenler dışında çalışanların birimlerde (odalarda) izlenmesine imkan veren kamera sisteminin kaldırılması talebiyle davacı sendika tarafından başvuru yapıldığı anlaşılmakta olup; uygulamanın sınırlarını, usul ve esaslarını gösteren bir yasal dayanağın bulunmaması, toplanan görüntülerin ileride başka bir şekilde kullanılmayacağına dair bir güvencenin mevcut olmaması ve iş yerinin güvenliğini sağlama amacını aşarak, doğrudan çalışan memurun kendisinin, diğer memurlarla ya da iş sahipleriyle ilişkisinin ve kamu hizmetinin görülmesi sırasında yaptığı her türlü haberleşmesinin, çalışma alanı ve masasının gözlemlendiği kamera takip sisteminin kurulmasının özel hayatın gizliliğini ihlal ettiği ve bu haliyle yukarıda belirtilen temel haklar ve Anayasal ilkelerle bağdaşmaması nedeniyle dava konusu işlemin iptaline karar verilmesi gerekirken davanın reddi yolunda verilen mahkeme kararının hukuka aykırı olduğu sonucuna varılmıştır.

Açıklanan nedenlerle, temyiz isteminin kabulüyle, İstanbul 8. İdare Mahkemesi'nin 18/12/2015 tarih ve E:2015/1370, K:2015/2690 sayılı kararının BOZULMASINA, yeniden bir karar verilmek üzere dosyanın adı geçen mahkemeye gönderilmesine, 2577 sayılı Kanun'un (Geçici 8. maddesi uyarınca uygulanmasına devam edilen) 54. maddesinin 1. fıkrası uyarınca bu kararın tebliğ tarihini izleyen günden itibaren onbeş gün içinde karar düzeltme yolu açık olmak üzere, 14/05/2018 tarihinde oybirliğiyle karar verildi.

Danıştay Kararı - 11. Daire (E. 2017/816)

Danıştay Kararı - 11. D., E. 2017/816 K. 2017/4906 T. 13.6.2017

İstemın Özetı: İstanbul 6. İdare Mahkemesince verilen 26.12.2014 tarih ve E:2013/2241; K:2014/2504sayılı kararın; davacı tarafından, temyizen incelenerek bozulması istenilmektedir.

Savunmanın Özetı: Savunma verilmemiştir.

Danıştay Tetkik Hâkimi: K1

Düşüncesi: Mesai takibi amacıyla yüzün belirli referans noktalarının alınarak bu verilerin sisteme kaydedilmesi, daha sonra personel geçişlerinde mevcut veri ile, o esnada alınan görüntünün karşılaştırılmak suretiyle eşleştirilmesi mantığına dayanan "yüz tarama" uygulamasında, kişinin görüntüsünün veri tabanında kaydedilmesi, niteliği itibarıyla kişisel veri alınması olduğundan; "özel hayatın gizliliği" kapsamında değerlendirilmesi gereken davalı idare işleminin Anayasal ilkelerle bağdaşmadığı, belirtilen nedenle temyizen incelenen ve dava konusu işlemi hukuka uygun bulan davanın reddi yönündeki mahkeme kararının bozulması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Hüküm veren Danıştay Onbirinci Dairesince, Danıştay Başkanlık Kurulunun 29.12.2016 tarih ve K:2016/72 sayılı kararı uyarınca Dairemize devredilen dosya incelenerek, işin gereği görüldü:

Dava, davalı idarenin toptancı hali biriminde görev yapan personelin mesai takibinin sağlanması amacıyla başlatılan yüz tarama sistemi uygulamasına son verilmesi talebi ile davacı sendika tarafından yapılan başvurunun reddine ilişkin işlemin iptali istemiyle açılmıştır.

İdare mahkemesince; davalı idarenin tüm birimlerinin mesai takibinde anılan yöntemin kullanılmadığı, uygulamanın gerçekleştirildiği birimin konumu ve vardiyalı çalışma sistemi nedeniyle personelin kontrol ve denetiminde güçlük yaşanması karşısında bahse konu uygulamaya geçildiği; yüz tanıma sisteminde personelin yüz görüntüsünün sayısal kodlara çevrilerek karşılaştırma yapmak suretiyle çalıştığı göz önünde bulundurulduğunda, yapılan uygulamanın veri kaydetme olarak nitelendirilemeyeceği gerekçesiyle, hukuka aykırılık bulunmadığı sonucuna varılan dava konusu işlemin iptali istemiyle açılan davanın reddine karar verilmiştir.

Davacı sendika, mahkeme kararının hukuka aykırı olduğunu ileri sürmekte ve temyizen incelenerek bozulmasını istemektedir.

Anayasanın "Temel Hak ve Hürriyetlerin Niteliği" başlıklı 12. maddesinde, "Herkes, kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlere sahiptir. Temel hak ve hürriyetler, kişinin topluma, ailesine ve diğer kişilere karşı ödev ve sorumluluklarını da ihtiva eder." kuralına;"Temel Hak ve Hürriyetlerin Sınırlanması" başlıklı değişik 13. maddesinde, "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz." kuralına;"Özel Hayatın Gizliliği" başlıklı değişik 20. maddesinde ise, "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir, özel hayatın ve aile hayatının gizliliğine dokunulamaz. Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kağıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakim onayına sunulur. Hakim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar. Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." kuralına yer verilmiştir.

Avrupa İnsan Hakları Sözleşmesinin "Özel Hayatın ve Aile Hayatının Korunması" başlıklı 8. maddesinde, herkesin özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahip olduğu; Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesinin "Mahremiyet Hakkı" başlıklı 17. maddesinde de, hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemeyeceği; onuru veya itibarının hukuka aykırı saldırılara maruz bırakılmayacağına, herkesin bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahip olduğu belirtilmiştir.

657 sayılı Devlet Memurları Kanunu'nun 99 ve devam eden maddelerinde Devlet memurlarının çalışma saatleri ile günlük çalışma saatlerinin başlama ve bitme saatlerinin tespitine yönelik düzenlemelere yer verilmiş olmakla birlikte, kamu görevlilerinin mesaiye devam durumlarının kontrolü konusunda ayrıntılı bir yasal düzenleme mevzuatımızda bulunmamaktadır. İdarelerce,

gelişen teknolojinin kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması amacıyla, kamu kesiminde kullanılmaya başlamasını doğal karşılamak gerekir. Ancak; teknolojinin kullanılarak kişisel verilerin kayıt altına alınması uygulamasının yukarıda belirtilen hükümlere uygun olması gerektiği kuşkusuzdur.

Bu bağlamda, personelin yüz tanıma sistemi ile mesai kontrolünün yapılması uygulamasının, temel hak ve hürriyetler içerisinde sayılan özel hayatın gizliliği ilkesi kapsamında kişisel bilgi veya kişisel verilerin alınması kavramları içinde değerlendirilmesi gerekmektedir.

Olayda, personelden kişisel veri alınması kapsamında olan "yüz tanıma sistemi" ile mesai takibi uygulamasının, kamusal alanda da olsa "özel hayatın gizliliği" ilkesi kapsamında bulunduğu açık olup, dava konusu işlem tarihi itibarıyla uygulamanın sınırlarını usul ve esaslarını gösteren bir yasal dayanağın bulunmaması, toplanan verilerin ileride başka bir şekilde kullanılmayacağına dair bir güvencenin mevcut olmaması gözönüne alındığında, yukarıda belirtilen temel haklar ve Anayasal ilkelerle bağdaşmayan dava konusu işlemde ve davanın reddi yolundaki mahkeme kararında hukuka uygunluk bulunmamaktadır.

Açıklanan nedenlerle, davacının temyiz isteminin kabulü ile mahkeme kararının BOZULMASINA; dosyanın yeniden bir karar verilmek üzere anılan mahkemeye gönderilmesine, kararın tebliğ tarihini izleyen 15 (onbeş) gün içinde Danıştayda karar düzeltme yolu açık olmak üzere, 13.06.2017 tarihinde oybirliği ile karar verildi.

Danıştay Kararı - 15. Daire (E. 2016/10500)

Danıştay Kararı - 15. D., E. 2016/10500 K. YD. T. 6.7.2017

İstem Özet: 20.10.2016 tarihli ve 29863 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin muhtelif maddelerinin ve tümünün yürütmesinin durdurulması ve iptali istenilmektedir.

Sağlık Bakanlığı'nın Savunmasının Özeti: Kişisel Verilerin İşlenmesine İlişkin Usûl ve Esasların Ancak Kanunla Düzenlenebileceği iddiası hakkında; Anayasa'nın 20 nci maddesinin üçüncü fıkrasının son cümlesinde "Kişisel verilerin korunmasına ilişkin esas ve usûller kanunla düzenlenir." hükmünün bulunduğu, Anayasa'da, "Kişisel verilerin otomatik işleme tabi tutulmasına ilişkin usûl ve esasların ancak kanunla düzenlenebileceğine" ilişkin herhangi bir hüküm bulunmadığı, davacının, aynı fıkranın bir önceki "Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir." cümlesi ile bu hükmü karıştırdığının düşünüldüğü, ayrıca, Yönetmeliğin dayanağı olan 663 sayılı KHK'nın 47 nci maddesinin, 6698 sayılı Kanun'un 30 uncu maddesinin yedinci fıkrası ile düzenlendiği, dolayısı ile kişisel sağlık verilerinin işlenmesine ilişkin usûl ve esasların Bakanlıkça yürürlüğe konulacak bir yönetmelikle düzenleneceği hususunun, 6698 sayılı Kanun'un emredici hükmüne dayandığı, Anayasa'nın 20 nci maddesinde öngörülen kanun olan 6698 sayılı Kanunun 07.04.2016 tarihi itibarıyla yürürlükte olduğu ve Anayasa'nın 20 nci maddesinde öngörülen hükmün bu Kanun ile yerine getirildiği, iç hukukta uygun güvencelerin sağlanması ön koşulunun yerine getirilmediğini iddia etmenin, yürürlükte olan Kanunu yok saymak anlamına geldiği,

6698 sayılı Kanun m. 6/IV Uyarınca Yeterli Önlemlerin Henüz Belirlenmemiş Olduğu iddiası hakkında; 6698 sayılı Kanun'un yürürlüğe girmiş olması ve 6 nci maddesinin dördüncü fıkrasında değinilen yeterli önlemlerin henüz belirlenmemiş olmasının, kişisel sağlık verilerinin Sağlık Bakanlığı tarafından işlenmemesi için ileri sürmenin izahtan varestede olduğu, bu iddianın doğruluğunu savunmanın, özel nitelikli kişisel verilerden olan kişisel sağlık verilerinin yalnızca Sağlık Bakanlığı tarafından değil; aynı zamanda hiçbir kişi (hekim), kurum ve kuruluş (özel ve kamu sağlık tesisleri) tarafından işlenmemesini de beraberinde getireceğinin ki bunun da ülkemizdeki tüm sağlık hizmetlerinin durması anlamına geleceği, hatta dernek üyeliğinin de özel nitelikli kişisel veriler arasında zikredilmiş olması göz önünde bulundurulduğunda, davacı F1 Derneği ile F2 Derneğinin kendi üyelerine ilişkin verileri işleyemeyecekleri, dernek üyesi olmaları gerekçesiyle üyelerine hiçbir

iş ve işlemde bulunamayacakları, ki bu durumun hayatın olağan akışına aykırı olduğu, nitekim, 6698 sayılı Kanun'un 6 ncı maddesinin dördüncü fıkrasında öngörülen ve Kurul tarafından belirlenecek yeterli önlemlerin alınması şartının, yalnızca aynı maddenin üçüncü fıkrası uyarınca istisnai hallerde işlenen özel nitelikli kişisel veriler için değil; aynı zamanda açık rıza ile işlenen özel nitelikli kişisel veriler için de geçerli olduğu, Kanun hükmünün yalnızca Sağlık Bakanlığını değil; özel nitelikli kişisel veri işleyen tüm gerçek kişiler ile özel hukuk ve kamu hukuku tüzel kişilerini bağladığı, dolayısı ile özel nitelikli kişisel verilerin işlenmesinde gerekli olan yeterli önlemlerin Kurul tarafından henüz belirlenmemiş olması hususunu, kişisel sağlık verilerinin Sağlık Bakanlığı tarafından işlenememesi için bir gerekçe olarak sunmanın, tutarlı hiçbir tarafı bulunmadığı, 6698 sayılı Kanun'un 6 ncı maddesinin dördüncü fıkrası uyarınca özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınmasının şart olduğu, bu yeterli önlemlerin ise Kurul tarafından henüz belirlenmediği,

6698 sayılı Kanun'un 22 nci maddesinin birinci fıkrasının (h) bendi gereği, kişisel verilere ilişkin hüküm içeren mevzuat taslaklarını hazırlarken Kurul'dan görüş alınmasının zorunlu olduğu davacı tarafından iddia edilmekte ise de, Kanun'da böyle bir zorunluluk bulunmadığı, ilgili hükümde, "Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek" hususunun, Kurul'un görev ve yetkileri arasında zikredildiği, bu hükmün, Yönetmeliğin çıkartılmasında Kurul'dan görüş alınmasının zorunlu olduğu anlamına gelmediği, ayrıca, Yönetmeliğin çıkartıldığı tarihte Kurulun henüz teşekkül etmediği, teşekkül etmeyen bir Kurul'dan görüş alınmasının da mümkün olmadığı, Kanun'un Geçici 1 inci maddesinin 1. fıkrası uyarınca en geç 07.10.2016 tarihinde oluşması gereken Kurulun, bu tarihten ancak aylar sonra oluşturulduğu, Yönetmeliğin ise 20.10.2016 tarihinde Resmî Gazete'de yayımlanarak yürürlüğe girdiği,

Dava konusu Yönetmelik hükümlerinin, en başta Anayasa olmak üzere kişisel veriler hukuku ile ilgili milletlerarası hukuk kurallarına, kanunlara ve hizmet gereklerine tamamiyle uygun olduğu savunulmaktadır.

Kişisel Verileri Koruma Kurumu'nun Savunmasının Özeti:12 Ocak 2017'de, 6698 sayılı Kanununun 21. maddesi hükümlerine göre, -en son iki üyesi 4 Ocak 2017'de TBMM Genel Kurulu Kararıyla seçilmiş- seçilen Kişisel Verileri Koruma Kurulu üyelerinin Yargıtay 1. Başkanlık Kurulu huzurunda yemin ettikleri, 30 Ocak 2017'de Başkan ve 2. Başkanın seçildiği, Kurum tarafından halihazırda başta hizmet birimlerinin çalışma usul ve esaslarını belirleyen teşkilat yönetmeliğinin hazırlanması ile diğer mevzuat hazırlıkları, idari ve teknik çalışmalarının yürütüldüğü,

Sağlık Bakanlığı tarafından çıkarılan dava konusu yönetmeliğin hazırlanma sürecinde Kurumun dahlinin bulunmadığı, işbu davada taraf sıfatına haiz olmadıkları,

Anayasa'nın 20. maddesinin 3. fıkrasındaki, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenlenmesi hükmünün, bu alanın yalnızca kanunla düzenleneceği anlamına gelmediği,

Anayasa'nın 20 nci maddesinde öngörülen kanun olan 6698 sayılı Kanun ile düzenleme altına alınan fiillerin ne zaman hukuka aykırı, ne zaman hukuka uygun olduğunun tereddütsüz olarak belirlendiği, suç teşkil eden fiiller bakımından da Kanundan önce yürürlükte bulunan Türk Ceza Kanunu'nun 135-140. maddelerine özel olarak atıfta bulunulduğu, sağlık verilerinin özel nitelikli kişisel veri olduğu, bu konunun da Kanunun 6. maddesi ile düzenlendiği, özel nitelikli kişisel verilere rastgele, dayanaksız bir müdahalede bulunulmasının söz konusu olmadığı savunulmaktadır.

Danıştay Tetkik Hakimi: K1

Düşüncesi: Yönetmeliğin iptali istenen maddelerinin incelemesine geçilmesi gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Hüküm veren Danıştay Onbeşinci Dairesince davalı idarelerin birinci savunmaları alındıktan sonra incelenmesine karar verilen yürütmenin durdurulması istemi, savunmaların verildiği görülmüş olmakla incelenerek işin gereği görüşüldü:

Dava, 20.10.2016 tarihli ve 29863 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin muhtelif maddelerinin ve tümünün yürütmesinin durdurulması ve iptaliyle açılmıştır.

Davacılar, Anayasa'da kişisel verilerin otomatik işleme tabi tutulmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceği belirtilmişken, sağlık verilerinin işleme ve korunma kurallarının yönetmelikle düzenlendiği,

6698 sayılı Kanun'da sağlık gibi özel nitelikli verilerin işlenmesinde uyulacak önlemleri belirlemekle yetkili olan Kişisel Verileri Koruma Kurulu oluşturulmadan alana ilişkin düzenleme yapıldığı, Kanunun 22. maddesinin 1. fıkrasının (h) bendine göre diğer kurum ve kuruluşların kişisel verilere ilişkin hüküm içeren mevzuat taslaklarını hazırlarken Kurul'dan görüş almasının zorunlu olduğu,

Dava konusu düzenlemede sağlık hizmeti ilişkisinin iki tarafı olan hekimlerin sır saklama başta olmak üzere mesleki hak ve yükümlülükleri ile veri sahibi hastanın haklarının yok sayıldığı, bu

durumun aynı zamanda hastanın Anayasa'nın 56. maddesinde güvence altına alınan sağlık hakkını ihlal ettiği,

Sağlık verilerinin rıza alınmaksızın işlenebileceği istisnai hallerin Yönetmelik ve dayanak kanunda, ülkemizce usulüne uygun olarak onaylanarak yürürlüğe giren 1981 tarihli ve 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Sözleşme"ye aykırı biçimde geniş tutulduğu, özel hayatın korunması ilkesinin özünün zedelendiği,

Sözleşmenin 9. maddesinin 2. fıkrasında sağlık verilerinin işlenmeme yasağına sadece "devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi ile ilgili kişinin veya başkasının hak ve özgürlüklerinin korunması" halinde istisna getirilebileceği; ancak bu istisnaların da kanunla düzenlenmesinin ve demokratik bir toplumda zorunlu olmasının ön koşul olduğu, maddenin 1. fıkrasına göre ise sayılan bu haller dışında devletlerin başka istisnai halleri düzenleyemeyeceği,

Dava konusu Yönetmeliğin "Kişisel sağlık verilerinin işlenmesi" başlıklı 7. maddesinin 1. fıkrasında "Kişisel sağlık verileri; kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği"nin belirtilerek sözleşmedeki hallerin keyfi biçimde genişletildiği, bu maddenin 6698 sayılı Kanun'un 6. maddesinin 3. fıkrasının aynen tekrarı olduğu, diğer dayanak 663 sayılı KHK'nın 47. maddesinin 2. fıkrasında da yer aldığı,

Maddede sayılan hallerin hiçbirinin demokratik bir toplumda gerekli, elzem, amaçla orantılı ve ölçülü bir tedbir olmadığı,

Neredeyse hiçbir istisna hali bırakılmaksızın niteliği ne olursa olsun tüm sağlık verilerinin işlenmesi, kamu kurumları arasında paylaşılması ve uluslararası güçlere aktarılmasının toplumsal kaygılarla kişileri sağlık hizmeti almaktan alıkoyabileceği, kişilerin bilgilerinin kamusal olarak kaydedilmesinden endişe ederek, bazı temel hak ve hürriyetlerini kullanmaktan imtina edebilecekleri,

Bu nedenlerle, Yönetmeliğin 8. maddesinin 1. fıkrası ile 7. maddesinin 1. fıkrasının ve bu fıkranın dayanağı olan 6698 sayılı Yasa'nın 6. maddesinin 3. fıkrasının ve 663 sayılı KHK'nın 47. maddesinin, Anayasa'nın 2., 17., 20., 56. maddelerine, 108 sayılı Sözleşmenin 9. maddesinin 2. fıkrasına ve BİYOTIP Sözleşmesi'nin özel hayat ve bilgi edinme hakkına yönelik 10. maddesine aykırılığından hareketle Anayasa'nın 90. maddesine aykırı olduğu,

Nitekim, 6698 sayılı Yasa'nın bir çok hükmünün ana muhalefet partisi tarafından Anayasa Mahkemesi'ne götürüldüğü, bu hükümler içerisinde 6. maddesinin 3. fıkrasının ve 663 sayılı KHK'nın 47. maddesinin de bulunduğu,

Yönetmeliğin sağlık verilerinin korunmasına ilişkin yeterli ve objektif hükümler içermediği,

6. maddenin, 2. fıkrasındaki "Sağlık hizmet sunucuları, kişisel sağlık verilerinin mahremiyetini sağlamak amacıyla Bakanlıkça belirlenen tüm önlemleri alır."

7. fıkrasının son cümlesindeki "Yetkilendirme, kayıt altına alma ve verilerin muhafazasına ilişkin hususlar, Genel Müdürlükçe belirlenir."

8. fıkrasındaki "Kişisel sağlık verilerinin bulunduğu bilgi sistemlerine erişen kullanıcıların erişim kaydı, sağlık hizmet sunucularının sistemlerinde Bakanlıkça belirlenen standartlara uygun olarak tutulur."

7. maddenin 4. fıkrasındaki "Kişisel sağlık verilerinin işlenmesinde ayrıca Kurul tarafından belirlenen yeterli önlemler de alınır."

8. maddenin 3. fıkrasındaki "Kanun ile belirlenmiş olan görev ve sorumluluklarını yerine getirmek üzere veri talebinde bulunan kamu kurum ve kuruluşları ile Bakanlık veya bağlı kurum ve kuruluşları arasında yapılacak veri aktarımı; aktarımın usulünü ve diğer gerekli hususları belirleyen bir protokol aracılığı ile yapılır." ibarelerinde sağlık verilerini korumanın yöntemi, esasları, kapsamı tam belirlenmeden idareye ucu açık, çevresi çizilmemiş, sınırsız bir yetki verildiği; yönetmelikle düzenlenmesi gereken hususların idarenin keyfine bırakıldığı, kişisel sağlık verilerinin idare tarafından işlenerek içeriği belirsiz protokoller ile diğer kamu kurum ve kuruluşlarına aktarılabilmesi, veri sahiplerinin ise bu protokol içeriklerine müdahale edemeyecekleri, aktarımda uygulanacak kuralların belirli biçimde düzenlenmemesi ve protokole bırakılması nedeniyle aktarımda uyulacak esasların da bilinmeyeceği,

Yönetmeliğin 4. maddesinin 1. fıkrasının (o) bendinde yer alan veri sorumlusunun 6698 sayılı Yasanın 3. maddesinin (ı) bendinin aynen tekrarı olduğu, 11. maddesinde de veri sorumlusunun görevi, yetkileri ve sorumluluk sınırlarının düzenlendiği, ancak veri sorumlusunun kim olacağının belirtilmediği, oysa sağlık verilerini işlemeye girişen, bu sistemi kuran sağlık hizmet sunucularını buna uymaya zorlayan idarenin bu sorumluluğu da üstlenerek veri sorumlusu olarak kabulünün gerektiği, veri sorumlusunun kim olacağının yoruma yer bırakmayacak şekilde açıkça düzenlenmesinin gerektiği, yani mevcut hükümlerin noksan düzenleme nedeniyle hukuka aykırı oldukları,

Sağlık verisi sahibinin Anayasa ve 108 nolu Sözleşme ile güvence altına alınan haklarının yönetmelikle ortadan kaldırıldığı,

Örneğin, veri sahibi kişilerin tutulan sağlık verilerinin başka kurumlara ya da özel firmalara aktarılmasına rıza göstermeme gibi bir hakka sahip olmadığı, bu durumun verilerin silinmesini talep hakkı için de geçerli olduğunu, Yönetmeliğin 15. maddesinin 5. fıkrasında “İlgili kişi, kişisel sağlık kaydı sistemi üzerinden kendisine ilişkin sağlık verilerini yönetebilir, bu verileri silebilir, eksik bilgilerinin sisteme eklenmesini, yanlış bilgilerin düzeltilmesini veya silinmesini talep edebilir, kullanıcı hesabını dondurabilir.” düzenlemesine yer verildiğini , ancak verilerin asıl tutulduğu ve Bakanlığın elinde olan sistemin “Merkezi Sağlık Veri Sistemi” olduğu, veri sahibinin bu sisteme müdahale olanağının bulunmadığı, sadece kendi hesabı olan kişisel sağlık kaydı sistemi üzerinde değişiklik yapmasının bir anlamının bulunmadığı,

Yönetmeliğin 5. maddesinin 2. fıkrasının (d) bendine göre sağlık verilerinin işlendikleri amaç için gerekli olan süre kadar saklanabileceğinin belirtildiği, ancak verilerin hangi süreden sonra silineceğinin düzenlenmediği, 9. maddenin 3. fıkrasında işlenen sağlık verilerinin yerel veri tabanından 10 yıl sonra silineceğinin belirtildiği, ancak sistemin ana bilgi deposu olan merkezi sağlık veri sisteminden ne zaman silineceğinin düzenlenmediği,

9. maddenin 1. fıkrasındaki “Bu Yönetmelik, 6698 sayılı Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel sağlık verileri, ilgili kişinin talebi üzerine veri sorumlusu tarafından anonim hale getirilir veya silinir.” ibaresi ile idareye takdir hakkı tanındığı, oysa işlenme sebebi ortadan kalkmaz verinin silinmesinin esas olması gerektiği,

9. maddenin 2. fıkrası ile sağlık verisi sahibinin silinme talep etmesine rağmen idare tarafından “bir hakkın tesisi, kullanılması veya korunması ya da verilerin ihtiyaç halinde adli mercilere verilebilmesi” gibi son derece muğlak ve her durumu kapsayan hallerde verilerin silinmeyip arşivlendiği,

Bu nedenlerle, Yönetmeliğin 9. maddesinin 1., 2. ve 3. fıkralarının hukuka aykırı olduğu,

Yönetmelikle “Kişisel Sağlık Verileri Komisyonu” adı altında dayanak yasalarda öngörülmemeyen bir komisyonun oluşturulduğu, Kişisel Verileri Koruma Kurulu’nun yurtdışına veri aktarılmasına karar verme yetkisinin Komisyona verildiği,

“Sağlık Verileri Komisyonu” başlıklı 12. maddenin 1. fıkrasında “Kişisel sağlık verilerine ilişkin hususlarda, Kanunun ve Kişisel Verileri Koruma Kurulunun belirlediği ilkelere uygun olarak

Bakanlık politikasının belirlenmesine yardımcı olmak, görüş belirtmek, anlaşmazlıkları çözümlmek, veri aktarımına ilişkin başvuruları değerlendirmek, şikayetleri incelemek ve gerekli denetimleri yapmak üzere, Müsteşara bağlı olarak görev yapacak Kişisel Sağlık Verileri Komisyonunun oluşturulduğu”

2. fıkrasında “Komisyonun, Müsteşarın veya görevlendirdiği Müsteşar Yardımcısının başkanlığında, Hukuk Müşavirliği, Sağlık Hizmetleri Genel Müdürlüğü, Sağlık Bilgi Sistemleri Genel Müdürlüğü, Yönetim Hizmetleri Genel Müdürlüğü, Acil Sağlık Hizmetleri Genel Müdürlüğü, Türkiye Kamu Hastaneleri Kurumu, Türkiye Halk Sağlığı Kurumu, Türkiye İlaç ve Tıbbi Cihaz Kurumu ve Türkiye Hudut ve Sahiller Sağlık Genel Müdürlüğünün bu işle ilgili yetkilendirdikleri birer üyeden oluşacağı” düzenlendiği,

Alana ilişkin önemli kararları alan sürekli kurulların Bakanlıkların görev ve yetkisini düzenleyen kanunlarda açıkça düzenlenmiş ya da kurulmasına olanak sağlanmış olmasının şart olduğu, bu haliyle Komisyonun kuruluş meşruiyetini yasadan alan, tarafsız ve alana ilişkin meslek örgütlerinin katılımıyla oluşan bir oluşum olmadığı, bu nedenle 12. maddenin tamamının hukuka aykırı olduğu, Yönetmeliğin 8. maddesinin 4. fıkrasındaki “Kişisel sağlık verilerinin uluslararası aktarımına ilişkin her türlü talep ile bu maddede sayılanlar dışındaki veri aktarımı talepleri, Kanunda öngörülen hükümler çerçevesinde, genetik verilerin hassasiyeti hususu da dikkate alınarak Komisyon tarafından değerlendirilir.” ibaresinin, 6698 sayılı Kanunun 9. maddesine açıkça aykırı olduğu, Kanunda yurt dışına veri aktarılmasına yönelik talepler hakkında karar verme yetkisinin Kişisel Verileri Koruma Kurulu’nda olduğunu ileri sürerek, düzenlemenin yürütmesinin durdurulması ve iptalini istemektedirler.

07.04.2016 tarihli ve 29677 sayılı Resmî Gazete’de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu, Türkiye Büyük Millet Meclisi’ne sunulan genel gerekçesinden de anlaşılacağı üzere, kişisel verilerin korunması konusunun pek çok sektörü ve kamu ya da özel pek çok kurumu ilgilendirmesi nedeniyle bir "çerçeve kanun" olarak hazırlanmıştır.

Bu Kanuna neden ihtiyaç duyulduğunu açıklayan genel gerekçede, Türk Ceza Kanunu'nun 135 ve devamı maddelerinde kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa edilmesi fiillerinin suç olarak düzenlendiği ve yaptırıma bağlandığı, ancak kişisel verilerin işlenmesine yönelik özel bir kanun bulunmaması sebebiyle, bu fiillerin ne zaman hukuka aykırı ne zaman hukuka uygun olduğunun belirlenmesinde tereddütler yaşandığı vurgulanmaktadır. Ayrıca 2010 yılında Anayasa'nın 20. maddesinde yapılan düzenlemeyle kişisel verilerin korunması temel bir

insan hakkı olarak güvence altına alınmış ve konuya ilişkin usul ve esasların kanunla düzenleneceği öngörülmüştür.

Genel gerekçede, kişisel verilerin korunmasına yönelik bir kanuni düzenleme olmamasının uluslararası ilişkiler açısından da sorunlar yarattığı, EUROPOL, EUROJUST gibi Avrupa kurumları ile ilişkilerin sekteye uğradığı, sağlık kuruluşlarınca tutulan kişisel verilerin güvenliğinin sağlanmasında yeterli yasal önlem olmamasının Avrupa İnsan Hakları Mahkemesince özel hayatın gizliliğine müdahale olarak kabul edildiği ve bu nedenle ihlal kararları verildiği belirtilmektedir. Yine genel gerekçede, bu Kanunun Türkiye'nin Avrupa Birliği'ne üyelik süreci açısından da önemine dikkat çekilmekte, Türkiye'nin, Avrupa Konseyi tarafından tüm üye ülkelerde kişisel verilerin aynı standartlarda korunması ve sınır ötesi veri akışı ilkelerinin belirlenmesi amacıyla hazırlanan 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"ne de 1981 yılından itibaren taraf olduğu ifade edilmektedir.

Bütün bu hususlardan anlaşılacağı üzere 6698 sayılı Kanun, kişisel verilerin korunması konusunda önemli bir yasal boşluğu doldurmak amacıyla kabul edilen çerçeve niteliğinde bir yasal düzenlemedir. Genel gerekçede yer verilen şu tespit Kanun ile oluşturulan Kişisel Verileri Koruma Kurulu'nun genel kontrol ve denetleme işlevlerine dikkat çekmesi bakımından önemlidir: "Ülkemizde kişisel verilerin işlenmesi sürecini kontrol edecek ve denetleyecek bir kurum bulunmamaktadır. Bunun bir sonucu olarak halen kişisel veriler yeterli düzenleme ve denetime tabi olmaksızın, birçok kişi veya kurum tarafından kullanılabilen ve bu durum bazı hak ihlallerinin yaşanmasına sebep olabilmektedir."

6698 sayılı Kanununun 21. maddesi hükümlerine göre oluşturulan Kişisel Verileri Koruma Kurulu'nun görev ve yetkileri, aynı Kanun'un 22. maddesiyle belirlenmiştir. 22. maddenin 1. fıkrasının (h) bendinde "Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat tasarıları hakkında görüş bildirmek" hükmüne yer verilmiştir.

Anılan Kanun'un, "Özel nitelikli kişisel verilerin işleme şartları" başlıklı 6. maddesinin 1. fıkrasında, dava konusu Yönetmelikle düzenlenen, sağlık verilerinin de özel nitelikli kişisel veri olduğu belirtilmiş; maddenin 4. fıkrasında, "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü getirilmiştir.

6698 sayılı Kanununun Geçici 1. maddesi hükmü uyarınca, Kanununun 21. Maddesine göre oluşturulacak Kişisel Verileri Koruma Kurulu'nun Kanununun Resmi Gazete'de yayımlandığı 7/4/2016 tarihinden itibaren altı ay içinde üyelerinin seçiminin tamamlanması gerekmekte iken, bu yasal gerekliliğin ancak 30.01.2017 tarihinde yerine getirilebildiği anlaşılmaktadır.

Davalıların savunmaları ve dosya içeriğinden, dava konusu Yönetmeliğin Resmî Gazete'de yayımlandığı tarih olan 20.10.2016'da Kişisel Verileri Koruma Kurulu'nun henüz oluşturulmadığı, dolayısıyla 6698 sayılı Kanun'un 6. maddesinin 4. fıkrasında belirtilen yeterli önlemlerin Kurul tarafından belirlenmediği ve Kanun'un 22. maddesinin 1. fıkrasının (h) bendine göre diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında Kurul görüşü alınmadan dava konusu düzenlemenin tesis edildiği görülmektedir.

Yukarıda yer verilen genel gerekçe ve Kanun hükümlerine göre, Kişisel Verileri Koruma Kurulu'nun kişisel verilerin korunması konusunda genel nitelikte bir kontrol ve denetim yetkisine sahip olduğu, diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hükümler içeren mevzuat taslakları hakkında Kişisel Verileri Koruma Kurulu'ndan görüş alınmasının şart olduğu, Kişisel Verileri Koruma Kurulu'nun kontrol ve denetiminden geçirilmeksizin hazırlanan ve 20/10/2016 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe giren dava konusu düzenlemede bu nedenle mevzuata ve hukuka uygunluk bulunmadığı sonucuna ulaşılmıştır.

Açıklanan nedenlerle, olayda 2577 sayılı İdari Yargılama Usulü Kanunu'nun 4001 sayılı Yasa ile değişik 27. maddesinin 2. fıkrasında sayılan koşullar gerçekleşmiş olduğundan yürütmenin durdurulması isteminin kabulüne, 20.10.2016 tarihli ve 29863 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin yürütmesinin durdurulmasına, bu kararın tebliğini izleyen günden itibaren 7 gün içinde İdari Dava Daireleri Kurulu'na itiraz yolu açık olmak üzere 06/07/2017 tarihinde oyçokluğu ile karar verildi.

KARŞI OY:

07.04.2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30. maddesi ile 1/10/2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 47. maddesine getirilen "Bilgi toplama, işleme ve paylaşma yetkisi" başlıklı hüküm aşağıdaki şekildedir;

"MADDE 47- (Değişik: 24/3/2016-6698/30 md.)

(1) Sağlık hizmeti almak üzere, kamu veya özel sağlık kuruluşları ile sağlık mesleği mensuplarına müracaat edenlerin, sağlık hizmetinin gereği olarak vermek zorunda oldukları veya kendilerine verilen hizmete ilişkin kişisel verileri işlenebilir.

(2) Sağlık hizmetinin verilmesi, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve maliyetlerin

hesaplanması amacıyla Bakanlık, birinci fıkra kapsamında elde edilen verileri alarak işleyebilir. Bu veriler, Kişisel Verilerin Korunması Kanununda öngörülen şartlar dışında aktarılamaz.

(3) Bakanlık, ikinci fıkra gereğince toplanan ve işlenen kişisel verilere, ilgili kişilerin kendilerinin veya yetki verdikleri üçüncü kişilerin erişimlerini sağlayacak bir sistem kurar.

(4) Üçüncü fıkraya göre kurulan sistemlerin güvenliği ve güvenilirliği ile ilgili standartlar Kişisel Verileri Koruma Kurulunun belirlediği ilkelere uygun olarak Bakanlıkça belirlenir. Bakanlık, bu Kanun uyarınca elde edilen kişisel sağlık verilerinin güvenliğinin sağlanması için gerekli tedbirleri alır. Bu amaçla, sistemde kayıtlı bilgilerin hangi görevli tarafından ne amaçla kullanıldığının denetlenmesine imkân tanıyan bir güvenlik sistemi kurar.

(5) Sağlık personeli istihdam eden kamu kurum ve kuruluşları ile özel hukuk tüzel kişileri ve gerçek kişiler, istihdam ettiği personeli ve personel hareketlerini Bakanlığa bildirmekle yükümlüdür.

(6) Kişisel sağlık verilerinin işlenmesi, güvenliği ve bu maddenin uygulanması ile ilgili diğer hususlar Bakanlıkça yürürlüğe konulan yönetmelikle düzenlenir."

Anılan maddenin son fıkrasıyla Sağlık Bakanlığı'na Yönetmelik çıkarma yetkisi ve görevi verilmiştir.

Mezkur Kanun'un 21. maddesi hükümlerine göre oluşturulan Kişisel Verileri Koruma Kurulu'nun görev ve yetkilerinin belirlendiği, aynı Kanun'un 22. maddesinin 1. fıkrasının (h) bendindeki "Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek" hükmünden diğer kurum ve kuruluşlarca hazırlanacak mevzuat taslakları hakkında Kurul'dan görüş alınmasının zorunlu olduğu anlamı çıkarılamaz.

Kaldı ki, anılan Kanun'un Geçici 1 inci maddesinin 1. fıkrasında, "Bu Kanunun yayımı tarihinden itibaren altı ay içinde 21 inci maddede öngörülen usule göre Kurul üyeleri seçilir ve Başkanlık teşkilatı oluşturulur." hükmüne yer verilmiştir. Bu hüküm uyarınca en geç 07.10.2016 tarihinde oluşması gereken Kurul, Yönetmeliğin çıkartıldığı 20.10.2016 tarihinde henüz teşekkül etmemiştir. Teşekkül etmeyen bir Kurul'dan görüş alınması da mümkün değildir.

Ayrıca, anılan Kanun'un 6. maddesinin 4. fıkrasında, "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü yer almaktadır. Bu hükme göre Kurul tarafından yeterli önlemlerin belirlenmemesinin diğer kurum ve kuruluşlarca düzenleyici işlem yapılmasına engel teşkil edeceği düşünülemez. Anılan hükme göre Kurum ve kuruluşların, mevzuat taslaklarını hazırlarken, Kurul tarafından belirlenmiş önlemler varsa bunları dikkate alacakları konusunda kuşku yoktur. Ancak maddede sözü geçen önlemler Kurul tarafından bir kereye mahsus kararlaştırılıp daha sonra değiştirilemeyecek önlemler değildir. Kurul her zaman,

belirlediđi önlemleri deđiřtirebilir, uluslararası geliřmelere, zamanın gereklerine vs. göre yenilerini ekleyebilir. Kiřisel verileri iřleyenlerin, Kurul tarafından herhangi bir zamanda belirlenelen önlemleri her zaman alacađı açıktır. Nitekim, İptali istenen Yönetmeliđin 7. maddesinin 4. fıkrasında "Kiřisel sađlık verilerinin iřlenmesinde ayrıca Kurul tarafından belirlenen yeterli önlemler de alınır." hükmüne yer verilmiřtir. Yani kurum ve kuruluşlarca, Kurul tarafından -ister Yönetmelik çıkarılmadan önce ister çıkarıldıktan sonra belirlensin- belirlenen tüm önlemler alınacaktır.

Açıklanan nedenlerle, dava konusu düzenlemede bu yönüyle hukuka aykırılık bulunmadıđı, Yönetmeliđin iptali istenen maddelerinin incelemesine geçilmesi gerektiđi düşünceyle çođunluk kararına katılmıyoruz.

Danıştay Kararı - 15. D., E. 2016/10488 YD. T. 6.7.2017

İstem Özet: 20.10.2016 tarihli ve 29863 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin, 5. maddesinin 5. fıkrası ile 14. maddesinin yürütmesinin durdurulması ve iptali istenilmektedir.

Sağlık Bakanlığı'nın Savunmasının Özeti: Kişisel Sağlık Verileri hukukunun uluslararası ve iç hukuktaki durumu ile Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin çıkarılma gerekçelerinin, aynı Yönetmeliğe karşı Danıştay 15. Daire'nin 2016/10500 Esas sayılı dosyasında açılan davaya karşı sunulan savunmalarında teferruatlı olarak belirtildiği ve hukuka uygunluğunun ortaya konulduğu, işbu davanın tevcih olunduğu maddelerinin de tamamıyla hizmet gereklerine ve hukuka uygun olduğu; serbest eczane sahibi eczacıların, kişisel sağlık verisi işliyor olmaları sebebiyle Yönetmelik hükümlerine tabi olmakla birlikte, Yönetmeliğin "sağlık hizmeti sunucuları" için öngörülen hükümlerine tabi olmadıkları, serbest eczane sahibi eczacıların, Yönetmelik uyarınca sağlık hizmeti sunucusu olarak değerlendirilmediği, buradaki karışıklığın, Sosyal Güvenlik Kurumu (SGK) mevzuatından kaynaklandığının düşünüldüğü, SGK tarafından çıkartılan Sosyal Güvenlik Kurumu Sağlık Uygulama Tebliği'nin (SUT) "Sağlık hizmeti sunucuları" başlıklı ve 1.4 numaralı maddesinde, 6197 sayılı Eczacılar ve Eczaneler Hakkında Kanun kapsamında serbest faaliyet gösteren ve birinci basamak sağlık kuruluşu olan eczanelerin, sağlık hizmeti sunucuları arasında zikredildiği, Yönetmelikte kullanılan "sağlık hizmeti sunucusu" ile ifade edilmek istenenin, Sağlık Bakanlığı ve bağlı kuruluşları bünyesinde faaliyet gösteren ve birinci, ikinci ve üçüncü basamakta sağlık hizmeti sunmakta olan bütün sağlık tesisleri olduğu, Sağlık Bakanlığı tarafından yayımlanan hukuki ve idari düzenlemelerde "sağlık hizmeti sunucusu" ifadesinin kapsamının bu olduğu, serbest eczane sahibi eczacıların Yönetmelik kapsamında sağlık hizmeti sunucusu olarak değerlendirilmesi ve Yönetmeliğin 5 inci maddesinin beşinci fıkrasına tabi olduğunun düşünülmesi halinde, Yönetmeliğin 6698 sayılı Kişisel Verilerin Korunması Kanunu'na aykırılık teşkil edeceği ve bunun genel hukuk ilkeleri ile bağdaşmayacağı, 6698 sayılı Kanun'un "Kişisel verilerin aktarılması" başlıklı 8 inci maddesinin ikinci fıkrasının (a) bendinde atıf yapılan aynı Kanun'un 5 inci maddesinin ikinci fıkrasının (ç) bendi gereği veri sorumlusunun hukuki yükümlülüğünü yerine getirmek için kişisel veri işlemesi zorunluluk arz ediyorsa, ilgili kişinin açık rızası olmaksızın bunu yapabileceği, dolayısı ile bu durumun da serbest eczane sahibi eczacıların

Yönetmelikteki “sağlık hizmeti sunucusu” ifadesi kapsamına girmediğini gösterdiği, sonuç olarak, Yönetmeliğin sağlık hizmeti sunucuları için öngörülen hükümlerinden birçoğuna (m. 5/6, m. 5/8, m. 6/2, m. 14/1, m. 16/1) bakıldığında, serbest eczane sahibi eczacıların, Yönetmelikteki “sağlık hizmeti sunucusu” ifadesinin kapsamına girmedikleri hususunun, öngörülen hükümlerin veya yükümlülüklerin serbest eczane sahibi eczacılar tarafından yerine getirilmesinin teknik olarak mümkün olmamasından anlaşıldığı, dolayısı ile işbu hükmü iptalini talep etmekte davacı tarafın menfaati bulunmadığından davanın evleviyetle bu hüküm bakımından usulden de reddinin gerektiği,

Yönetmelikte; Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü tarafından geliştirilen Ulusal Sağlık Sistemi’nden (USS), merkezi sağlık veri sistemi olarak bahsedildiği, Yönetmeliğin 14 üncü maddesi uyarınca sağlık hizmeti sunucularının, merkezi sağlık veri sistemine, Bakanlıkça belirlenen standartlara uygun bir şekilde veri aktarımı yapmalarının gerektiği, bununla birlikte serbest eczane sahibi eczacılardan, USS’ye veri gönderimi yapmalarının talep edilmediği, madde metninde yer alan “(...) Bakanlıkça belirlenen standartlara uygun (...)” ifadesi ile atıf yapılan düzenlemenin, Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü’nün 2015/17 sayılı Genelgesi olduğu, bu Genelgede Hastane Bilgi Yönetim Sistemi (HBYS) ve Sağlık Bilgi Yönetim Sistemi’ne (SBYS) ilişkin düzenlemelerin yer aldığı; serbest eczane sahibi eczacıların kullandığı veya kullanabilecekleri yazılımlardan bahsedilmediği, Genelgede bahsedilen, tüm sağlık tesislerinde kullanılan sağlık uygulama yazılımlarını üreten kamu ve özel kurum ve kuruluşlarının kayıt ve tescil işlemlerini düzenlemek için Bakanlık bünyesinde oluşturulan Kayıt Tescil Sistemi’nde (KTS), eczanelerin kullandıkları yazılımların tescil edilmediği ve eczanelerde kullanılacak yazılımlar için böyle bir tescil şartı aranmadığı, davacı tarafından iddia edildiği üzere eczacıların, Bakanlıkça verilen yetki belgesine sahip ve Bakanlıkça belirlenen standartlar ile uyumlu yazılımlar kullanmak zorunda bırakılmadıkları, davacının bu konudaki iddialarının Yönetmelikten değil, konuyu yanlış yorumlamasından kaynaklandığı savunulmaktadır.

Kişisel Verileri Koruma Kurumu'nun Savunmasının Özeti: 12 Ocak 2017’de, 6698 sayılı Kanununun 21. maddesi hükümlerine göre, -en son iki üyesi 4 Ocak 2017’de TBMM Genel Kurulu Kararıyla seçilmiş- seçilen Kişisel Verileri Koruma Kurulu üyelerinin Yargıtay 1. Başkanlık Kurulu huzurunda yemin ettikleri, 30 Ocak 2017’de Başkan ve 2. Başkanın seçildiği, Kurum tarafından halihazırda başta hizmet birimlerinin çalışma usul ve esaslarını belirleyen teşkilat yönetmeliğinin hazırlanması ile diğer mevzuat hazırlıkları, idari ve teknik çalışmalarının yürütüldüğü, Sağlık Bakanlığı tarafından çıkarılan dava konusu yönetmeliğin hazırlanma sürecinde Kurumun dahilinin bulunmadığı, işbu davada taraf

sıfatını haiz olmadıkları, Anayasa'nın 20. maddesinin 3. fıkrasındaki, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenlenmesi hükmünün, bu alanın yalnızca kanunla düzenleneceği anlamına gelmediği savunulmaktadır.

Danıştay Tetkik Hakimi: K1

Düşüncesi: Yönetmeliğin iptali istenen maddelerinin esastan incelenmesi gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Hüküm veren Danıştay Onbeşinci Dairesince davalı idarelerin birinci savunmaları alındıktan sonra incelenmesine karar verilen yürütmenin durdurulması istemi, savunmaların verildiği görülmüş olmakla incelenerek işin gereği görüşüldü:

Dava, 20.10.2016 tarihli ve 29863 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin, 5. maddesinin 5. fıkrası ile 14. maddesinin yürütmesinin durdurulması ve iptali istemiyle açılmıştır.

Davacı, eczacıların hem elden satışlarda hem de SGK'ya yapılan satışlarda İlaç Takip Sistemine bildirimde bulduklarını, ilaçları hastaya sistemden onay aldıktan sonra teslim ettiklerini, eczacıların reçete karşılığında İlaç Takip Sistemi ile bağlantılı eczane programları kullandıklarını, bu programlar vasıtasıyla reçete kayıt defterlerinin elektronik ortamda tutma imkânının bulunduğunu, söz konusu programlar ve eczanelerin iç işleyişi sebebiyle eczanelerde kişisel sağlık verilerinin kaydedildiğini,

Eczacılar ve Eczaneler Hakkında Yönetmeliğin "Eczane defter ve kayıtları" başlıklı 45. maddesinin 1. fıkrasında "Eczanede satışı yapılan tüm ilaçlar elektronik ortamda kaydedilir. Bu kayıtlar denetimlerde istenilmesi hâlinde sunulmak üzere saklanır." hükmünün bulunduğunu; Yönetmeliğin 5. maddesinin 5. fıkrası ile kişisel sağlık verilerinin mahremiyeti sağlanmaya çalışılırken, eczacıların özel mevzuatları ile çelişen ve uygulanması fiilen imkânsız bir yükümlülük altına sokulduklarını,

Yönetmeliğin 14. maddesi ile eczacıların davalı Bakanlıkça verilen yetki belgesine sahip ve Bakanlıkça belirlenen standartlar ile uyumlu yazılımları kullanmak zorunda bırakıldığını, eczacıların halen kullandıkları piyasada mevcut programların bu özellikleri taşımadığını, bu durumun eczacıların sağlık hizmeti sunumunu aksatacağını ileri sürerek, düzenlemenin yürütmesinin durdurulması ve iptalini istemektedir.

07.04.2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu, Türkiye Büyük Millet Meclisi'ne sunulan genel gerekçesinden de

anlaşılacağı üzere, kişisel verilerin korunması konusunun pek çok sektörü ve kamu ya da özel pek çok kurumu ilgilendirmesi nedeniyle bir "çerçeve kanun" olarak hazırlanmıştır.

Bu Kanuna neden ihtiyaç duyulduğunu açıklayan genel gerekçede, Türk Ceza Kanunu'nun 135 ve devamı maddelerinde kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa edilmesi fiillerinin suç olarak düzenlendiği ve yaptırıma bağlandığı, ancak kişisel verilerin işlenmesine yönelik özel bir kanun bulunmaması sebebiyle, bu fiillerin ne zaman hukuka aykırı ne zaman hukuka uygun olduğunun belirlenmesinde tereddütler yaşandığı vurgulanmaktadır. Ayrıca 2010 yılında Anayasa'nın 20. maddesinde yapılan düzenlemeyle kişisel verilerin korunması temel bir insan hakkı olarak güvence altına alınmış ve konuya ilişkin usul ve esasların kanunla düzenleneceği öngörülmüştür.

Genel gerekçede, kişisel verilerin korunmasına yönelik bir kanuni düzenleme olmamasının uluslararası ilişkiler açısından da sorunlar yarattığı, EUROPOL, EUROJUST gibi Avrupa kurumları ile ilişkilerin sekteye uğradığı, sağlık kuruluşlarınca tutulan kişisel verilerin güvenliğinin sağlanmasında yeterli yasal önlem olmamasının Avrupa İnsan Hakları Mahkemesince özel hayatın gizliliğine müdahale olarak kabul edildiği ve bu nedenle ihlal kararları verildiği belirtilmektedir. Yine genel gerekçede, bu Kanunun Türkiye'nin Avrupa Birliği'ne üyelik süreci açısından da önemine dikkat çekilmekte, Türkiye'nin, Avrupa Konseyi tarafından tüm üye ülkelerde kişisel verilerin aynı standartlarda korunması ve sınır ötesi veri akışı ilkelerinin belirlenmesi amacıyla hazırlanan 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"ne de 1981 yılından itibaren taraf olduğu ifade edilmektedir.

Bütün bu hususlardan anlaşılacağı üzere 6698 sayılı Kanun, kişisel verilerin korunması konusunda önemli bir yasal boşluğu doldurmak amacıyla kabul edilen çerçeve niteliğinde bir yasal düzenlemedir. Genel gerekçede yer verilen şu tespit Kanun ile oluşturulan Kişisel Verileri Koruma Kurulu'nun genel kontrol ve denetleme işlevlerine dikkat çekmesi bakımından önemlidir: "Ülkemizde kişisel verilerin işlenmesi sürecini kontrol edecek ve denetleyecek bir kurum bulunmamaktadır. Bunun bir sonucu olarak halen kişisel veriler yeterli düzenleme ve denetime tabi olmaksızın, birçok kişi veya kurum tarafından kullanılabilmekte ve bu durum bazı hak ihlallerinin yaşanmasına sebep olabilmektedir."

6698 sayılı Kanununun 21. maddesi hükümlerine göre oluşturulan Kişisel Verileri Koruma Kurulu'nun görev ve yetkileri, aynı Kanun'un 22. maddesiyle belirlenmiştir. 22. maddenin 1. fıkrasının (h) bendinde "Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek" hükmüne yer verilmiştir.

Anılan Kanun'un, "Özel nitelikli kişisel verilerin işleme şartları" başlıklı 6. maddesinin 1. fıkrasında, dava konusu Yönetmelikle düzenlenen, sağlık verilerinin de özel nitelikli kişisel veri olduğu belirtilmiş;maddenin 4. fıkrasında, "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü getirilmiştir.

6698 sayılı Kanununun Geçici 1. maddesi hükmü uyarınca, Kanununun 21. maddesine göre oluşturulacak Kişisel Verileri Koruma Kurulu'nun Kanununun Resmi Gazete'de yayımlandığı 7/4/2016 tarihinden itibaren altı ay içinde üyelerinin seçiminin tamamlanması gerekmekte iken, bu yasal gerekliliğin ancak 30.01.2017 tarihinde yerine getirilebildiği anlaşılmaktadır.

Davalıların savunmaları ve dosya içeriğinden, dava konusu Yönetmeliğin Resmî Gazete'de yayımlandığı tarih olan 20.10.2016'da Kişisel Verileri Koruma Kurulu'nun henüz oluşturulmadığı, dolayısıyla 6698 sayılı Kanun'un 6. maddesinin 4. fıkrasında belirtilen yeterli önlemlerin Kurul tarafından belirlenmediği ve Kanun'un 22. maddesinin 1. fıkrasının (h) bendine göre diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında Kurul görüşü alınmadan dava konusu düzenlemenin tesis edildiği görülmektedir.

Yukarıda yer verilen genel gerekçe ve Kanun hükümlerine göre, Kişisel Verileri Koruma Kurulu'nun kişisel verilerin korunması konusunda genel nitelikte bir kontrol ve denetim yetkisine sahip olduğu, diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hükümler içeren mevzuat taslakları hakkında Kişisel Verileri Koruma Kurulu'ndan görüş alınmasının şart olduğu, Kişisel Verileri Koruma Kurulu'nun kontrol ve denetiminden geçirilmeksizin hazırlanan ve 20/10/2016 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe giren dava konusu düzenlemede bu nedenle mevzuata ve hukuka uygunluk bulunmadığı sonucuna ulaşılmıştır.

Açıklanan nedenlerle, olayda 2577 sayılı İdari Yargılama Usulü Kanunu'nun 4001 sayılı Yasa ile değişik 27. maddesinin 2. fıkrasında sayılan koşullar gerçekleşmiş olduğundan yürütmenin durdurulması isteminin kabulüne, 20.10.2016 tarihli ve 29863 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin 5. maddesinin 5. fıkrası ile 14. maddesinin yürütmesinin durdurulmasına, bu kararın tebliğini izleyen günden itibaren 7 gün içinde İdari Dava Daireleri Kurulu'na itiraz yolu açık olmak üzere 06/07/2017 tarihinde oyçokluğu ile karar verildi.

KARŞI OY:

07.04.2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30. maddesi ile 1/10/2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 47. maddesine getirilen "Bilgi toplama, işleme ve paylaşma yetkisi" başlıklı hüküm aşağıdaki şekildedir; "MADDE 47- (Değişik: 24/3/2016-6698/30 md.)

(1) Sağlık hizmeti almak üzere, kamu veya özel sağlık kuruluşları ile sağlık mesleği mensuplarına müracaat edenlerin, sağlık hizmetinin gereği olarak vermek zorunda oldukları veya kendilerine verilen hizmete ilişkin kişisel verileri işlenebilir.

(2) Sağlık hizmetinin verilmesi, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve maliyetlerin hesaplanması amacıyla Bakanlık, birinci fıkra kapsamında elde edilen verileri olarak işleyebilir. Bu veriler, Kişisel Verilerin Korunması Kanununda öngörülen şartlar dışında aktarılamaz.

(3) Bakanlık, ikinci fıkra gereğince toplanan ve işlenen kişisel verilere, ilgili kişilerin kendilerinin veya yetki verdikleri üçüncü kişilerin erişimlerini sağlayacak bir sistem kurar.

(4) Üçüncü fıkraya göre kurulan sistemlerin güvenliği ve güvenilirliği ile ilgili standartlar Kişisel Verileri Koruma Kurulunun belirlediği ilkelere uygun olarak Bakanlıkça belirlenir. Bakanlık, bu Kanun uyarınca elde edilen kişisel sağlık verilerinin güvenliğinin sağlanması için gerekli tedbirleri alır. Bu amaçla, sistemde kayıtlı bilgilerin hangi görevli tarafından ne amaçla kullanıldığının denetlenmesine imkân tanıyan bir güvenlik sistemi kurar.

(5) Sağlık personeli istihdam eden kamu kurum ve kuruluşları ile özel hukuk tüzel kişileri ve gerçek kişiler, istihdam ettiği personeli ve personel hareketlerini Bakanlığa bildirmekle yükümlüdür.

(6) Kişisel sağlık verilerinin işlenmesi, güvenliği ve bu maddenin uygulanması ile ilgili diğer hususlar Bakanlıkça yürürlüğe konulan yönetmelikle düzenlenir."

Anılan maddenin son fıkrasıyla Sağlık Bakanlığı'na Yönetmelik çıkarma yetkisi ve görevi verilmiştir. Mezkur Kanun'un 21. maddesi hükümlerine göre oluşturulan Kişisel Verileri Koruma Kurulu'nun görev ve yetkilerinin belirlendiği, aynı Kanun'un 22. maddesinin 1. fıkrasının (h) bendindeki "Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek" hükmünden diğer kurum ve kuruluşlarca hazırlanacak mevzuat taslakları hakkında Kurul'dan görüş alınmasının zorunlu olduğu anlamı çıkarılamaz.

Kaldı ki, anılan Kanun'un Geçici 1 inci maddesinin 1. fıkrasında, "Bu Kanunun yayımı tarihinden itibaren altı ay içinde 21 inci maddede öngörülen usule göre Kurul üyeleri seçilir ve Başkanlık teşkilatı oluşturulur." hükmüne yer verilmiştir. Bu hüküm uyarınca en geç 07.10.2016 tarihinde oluşması gereken Kurul, Yönetmeliğin çıkartıldığı 20.10.2016 tarihinde henüz teşekkül etmemiştir. Teşekkül etmeyen bir Kurul'dan görüş alınması da mümkün değildir.

Ayrıca, anılan Kanun'un 6. maddesinin 4. fıkrasında, "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü yer almaktadır. Bu hükme göre Kurul tarafından yeterli önlemlerin belirlenmemesinin diğer kurum ve kuruluşlarca düzenleyici işlem yapılmasına engel teşkil edeceği düşünülemez. Anılan hükme göre Kurum ve kuruluşların, mevzuat taslaklarını hazırlarken, Kurul tarafından belirlenmiş önlemler varsa bunları dikkate alacakları konusunda kuşku yoktur. Ancak maddede sözü geçen önlemler Kurul tarafından bir kereye mahsus kararlaştırılıp daha sonra değiştirilemeyecek önlemler değildir. Kurul her zaman, belirlediği önlemleri değiştirebilir, uluslararası gelişmelere, zamanın gereklerine vs. göre yenilerini ekleyebilir. Kişisel verileri işleyenlerin, Kurul tarafından herhangi bir zamanda belirlenelen önlemleri her zaman alacağı açıktır. Nitekim, İptali istenen Yönetmeliğin 7. maddesinin 4. fıkrasında "Kişisel sağlık verilerinin işlenmesinde ayrıca Kurul tarafından belirlenen yeterli önlemler de alınır." hükmüne yer verilmiştir. Yani kurum ve kuruluşlarca, Kurul tarafından-ister Yönetmelik çıkarılmadan önce ister çıkarıldıktan sonra belirlensin-belirlenen tüm önlemler alınacaktır.

Açıklanan nedenlerle, dava konusu düzenlemede bu yönüyle hukuka aykırılık bulunmadığı, Yönetmeliğin iptali istenen maddelerinin incelemesine geçilmesi gerektiği düşüncesiyle çoğunluk kararına katılmıyoruz.

Danıştay Kararı - 8. Daire (E. 2016/3355)

Danıştay Kararı - 8. D., E. 2016/3355 K. 2020/281 T. 28.1.2020

İstemin Özeti: Sivas İdare Mahkemesinin 17/12/2015 gün ve E:2015/1011, K:2015/2026 sayılı kararının hukuka aykırı olduğu öne sürülerek, 2577 sayılı Kanununun 49. maddesi uyarınca temyizden incelenerek bozulması istemidir.

Savunmanın Özeti: Savunma verilmemiştir.

Danıştay Tetkik Hakimi: K1

Düşüncesi: İstemin kabulü ile Mahkeme kararının bozulması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Hüküm veren Danıştay Sekizinci Dairesince işin gereği görüşüldü:

Dava, davacı vekili tarafından, davacının geçirmiş olduğu trafik kazası sebebiyle tedavi gördüğü Sivas Numune Hastanesi'nde bulunan davacıya ait tüm tedavi evrakının bir örneğinin trafik sigortasına başvurmak üzere verilmesi istemiyle yapılan başvurunun reddine ilişkin işlemin iptali istemiyle açılmıştır.

İdare Mahkemesince, davacı vekili tarafından talep edilen hususun, müvekkilinin geçirmiş olduğu trafik kazası neticesinde sigorta şirketi ile arasındaki ilişki nedeniyle ihtiyaç duyulan tedavi evraklarına ilişkin olduğu, Hasta Hakları Yönetmeliği'nin 16. maddesi uyarınca, hastanın kendisi veya vekili vasıtasıyla sağlık durumu ile ilgili bilgiler bulunan dosyayı ve kayıtları, doğrudan veya vekili veya kanuni temsilcisi vasıtasıyla inceleyebilme ve bir suretini alabilme hususunda tanınan hakkın kullanımına engel olabilecek herhangi bir istisnaya yer verilmediği, anılan Yönetmeliğin 23. maddesinde düzenlenen hususun ise sağlık hizmetinin verilmesi sebebiyle edinilen bilgilerin açıklanmasına ilişkin olduğu ve davacı vekili tarafından yapılan başvurunun anılan madde kapsamında değerlendirilemeyeceği, buna göre davacı vekili tarafından yapılan başvuru üzerine tedavi evraklarının davacıya verilmesinde herhangi bir hukuki engel bulunmadığından yapılan başvurunun reddine ilişkin dava konusu işlemde hukuka uyarlık bulunmayarak dava konusu işlemin iptaline karar verilmiştir.

Türkiye Cumhuriyeti Anayasa'sının "Özel hayatın gizliliği" başlıklı 20/3. maddesinde, "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili

kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmü yer almaktadır.

07.04.2016 tarih ve 29677 sayılı Resmi Gazete'de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Amaç" başlıklı 1. maddesinde, "Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir."; "Tanımlar" başlıklı 3. maddesinin 1. fıkrasında; "a) Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı, (...) d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi, e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi, (...) ifade eder." ; "Özel nitelikli kişisel verilerin işlenme şartları" başlıklı 6. maddesinin 1. fıkrasında, "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir."; 2. fıkrasında, "Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır."; 3. fıkrasında ise, "Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir." hükümlerine yer verilmiştir.

4982 sayılı Bilgi Edinme Hakkı Kanunu'nun "Bilgi verme yükümlülüğü" başlıklı 5/1. maddesinde, "Kurum ve kuruluşlar, bu Kanunda yer alan istisnalar dışındaki her türlü bilgi veya belgeyi başvuranların yararlanmasına sunmak ve bilgi edinme başvurularını etkin, süratli ve doğru sonuçlandırmak üzere, gerekli idari ve teknik tedbirleri almakla yükümlüdürler." hükmüne yer verilmiş; öte yandan bilgi edinme hakkının sınırlarının düzenlendiği dördüncü bölüm altında yer alan "Özel hayatın gizliliği" başlıklı 21. maddesinde ise, "Kişinin izin verdiği haller saklı kalmak üzere,

özel hayatın gizliliği kapsamında, açıklanması halinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, mesleki ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır. Kamu yararının gerektirdiği hallerde, kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir." düzenlemesine yer verilmek suretiyle kişilerin sağlık bilgilerinin anılan Kanun kapsamı dışında yer aldığı ifade edilmiştir.

1136 sayılı Avukatlık Kanunu'nun "Avukatlığın amacı" başlıklı 2. maddesinin 3. fıkrasında, "Yargı organları, emniyet makamları, diğer kamu kurum ve kuruluşları ile kamu iktisadi teşebbüsleri, özel ve kamuya ait bankalar, noterler, sigorta şirketleri ve vakıflar avukatlara görevlerinin yerine getirilmesinde yardımcı olmak zorundadır. Kanunlarındaki özel hükümler saklı kalmak kaydıyla, bu kurumlar avukatın gerek duyduğu bilgi ve belgeleri incelemesine sunmakla yükümlüdür. Bu belgelerden örnek alınması vekaletname ibrazına bağlıdır. (...)" hükmüne yer verilmiştir.

Dosyanın incelenmesinden, davacı vekili tarafından, davacının 2007 yılında trafik kazası geçirmesi sebebiyle Sivas Numune Hastanesi'nde tedavi gördüğünden bahisle, davacıya ait tüm tedavi evrakının bir örneğinin trafik sigortasına verilmek üzere 1136 sayılı Avukatlık Kanunu'nun 2. maddesine dayanılarak 13.07.2015 tarihli dilekçe ile istenilmesi üzerine, başvuru dilekçesi ekinde yer alan vekaletnamenin genel vekaletname mahiyetinde olduğu, talep edilen bilgi ve belgelerin ise davacıya ait kişisel veri niteliği taşıdığı, bu nedenle özel vekaletname ibrazı yahut genel vekaletnameyle birlikte davacının dilekçesinin de ibraz edilmesi durumunda söz konusu bilgi ve belgelerin verilebileceği gerekçesiyle 22.07.2015 tarih ve 1038 sayılı işlemle reddedilmesi üzerine bakılmakta olan davanın açıldığı anlaşılmaktadır.

Yukarıda yer verilen 6698 sayılı Kanun'un 3. maddesine göre kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Anayasa Mahkemesinin kararlarında da belirtildiği üzere "... adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler" kişisel veri olarak kabul edilmektedir.

6698 sayılı Kanunda kişisel verilerin işlenmesine ilişkin genel şartlar ortaya konulmakla birlikte yasa koyucunun takdir yetkisi kapsamında kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel

hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri gibi özel nitelikli kişisel verilerin işleme şartlarının ayrı bir düzenlemeye tabi tutulduğu, bu düzenlemeyle birtakım kişisel verilerin özel hukuki koruma altına alındığı görülmektedir.

Özel nitelikli kişisel verilerin işlenebilmesi için kural olarak ilgililerin açık rızasının bulunması gerekmektedir. Ancak 6698 sayılı Kanun'un 6. maddesinin 3. fıkrasında, sağlık ve cinsel hayat dışındaki özel nitelikli kişisel verilerin, "Kanunlarda öngörülen hallerde" ilgililerin açık rızası aranmaksızın da işlenebileceği belirtilmek suretiyle anılan kuralın istisnasına yer verilmiştir. Bununla birlikte sağlık ve cinsel hayata ilişkin kişisel verilerin ise bu istisnadan da istisna edilerek ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği ifade edilmek suretiyle, önemine binaen "Kanunlarda öngörülen hallerde" şeklinde bir ifade biçimiyle yetinilmeyerek, bu verilerin ilgililerin açık rızası aranmaksızın işlenebileceği hallerin doğrudan Kanun maddesinde düzenlendiği görülmektedir.

Şu halde, kökeni Roma Hukukuna dayanan ve günümüzde genel hukuk kaidesi olarak kabul gören "istisna içerikli hükümlerin dar yorumlanması" (singularia non sunt extenda) ilkesi uyarınca, işleme şartları bizzat 6698 sayılı Kanun'da yer alan kişilerin sağlık verilerine ilişkin bilgilerin, ancak kişinin açık rızası halinde işlenebileceği, "işlenme" ifadesinden ise, ilgili verinin açıklanması, aktarılması, elde edilebilir hale getirilmesi gibi her türlü işlemin anlaşılması gerektiği açıktır.

Diğer taraftan, Avukat-müvekkil ilişkisi temelde 6098 sayılı Türk Borçlar Kanunu'nun 502 ve devamı maddelerinde yer alan "vekalet sözleşmesi"ne dayanmakta olup; vekilin üstlendiği iş ve hizmetleri, vekalet verenin haklı menfaatlerini gözeterek, sadakat ve özenle yürütme ödevi bulunmaktadır. Bu özen görevi, 1136 sayılı Kanun'da da avukatın işini özenle ve sonuna kadar takip etme (m. 34 ve 171) ödeviyle de somutlaştırılmış bulunmaktadır. Öte yandan 1136 sayılı Avukatlık Kanunu'nun 2. maddesinde, avukatlığın amacının, hukuki münasebetlerin düzenlenmesini, her türlü hukuki mesele ve anlaşmazlıkların adalet ve hakkaniyete uygun olarak çözümlenmesini ve hukuk kurallarının tam olarak uygulanmasını her derecede yargı organları, hakemler, resmi ve özel kişi, kurul ve kurumlar nezdinde sağlamak olduğu, avukatın bu amaçla hukuki bilgi ve tecrübelerini adalet hizmetine ve kişilerin yararlanmasına tahsis edeceği ifade edildikten sonra aynı maddenin 3. fıkrasında, madde metninde sayılan kamu kurum ve kuruluşları ile özel hukuk tüzel kişilerinin avukatların ihtiyaç duyduğu bilgi ve belgeleri incelemeye sunmakla yükümlü kılınarak avukatlara görevlerinin yerine getirilmesi kapsamında, müvekkilinin hukukunu savunabilmesine, haklarını dava etmesine,

yargılama sürecinin çabuklaştırılmasına ve uyuşmazlıkların adalet ve hakkaniyete uygun olarak çözümlenmesine yardımcı olma görevinin yüklendiği anlaşılmaktadır. Şüphesiz bu yükümlülük, "Kanunlardaki özel hükümler saklı kalmak kaydıyla" ilgili kurum ve kuruluşlara getirilmiş olup mutlak değildir.

Buna göre, avukatın müvekkiliyle iş ilişkisi içinde üstlendiği bir işin mahiyetine göre gerek duyduğu bilgi ve belgeyi başka kurum, kuruluş veya özel hukuk tüzel kişilerinden vekalet görevi kapsamında talep etmesi avukatın vekalet görevini özenle ifa etme yükümlülüğü çerçevesinde değerlendirilmekle birlikte, müvekkilinin özel nitelikli kişisel veri mahiyetinde bulunan sağlık bilgilerine ilişkin kayıtların, yukarıda yer verilen mevzuat hükümleri doğrultusunda ancak ilgilinin açık rızasıyla davalı idarece verilebilmesi mümkün bulunduğundan, davacı vekilinin davacıdan aldığı "genel vekaletname" ile müvekkiline ait sağlık bilgilerine ilişkin kayıtların istenemeyeceğine ilişkin dava konusu işlemde hukuka aykırılık; aksi yönde karar veren İdare Mahkemesi kararında ise hukuki isabet bulunmamaktadır.

Açıklanan nedenlerle; Sivas İdare Mahkemesinin temyize konu kararının bozulmasına, dosyanın yeniden bir karar verilmek üzere anılan Mahkemeye gönderilmesine, bu kararın tebliğ tarihini izleyen 15 (onbeş) gün içerisinde kararın düzeltilmesi yolu açık olmak üzere, 28/01/2020 tarihinde oyçokluğu ile karar verildi.

KARŞIOY:

- Dava, davacı vekili tarafından, davacının geçirmiş olduğu trafik kazası sebebiyle tedavi gördüğü Sivas Numune Hastanesi'nde bulunan davacıya ait tüm tedavi evrakının bir örneğinin trafik sigortasına başvurmak üzere verilmesi istemiyle yapılan başvurunun reddine ilişkin işlemin iptali istemiyle açılmıştır.

1136 sayılı Avukatlık Kanununun "Avukatlığın amacı" başlıklı 2. maddesinde, "Avukatlığın amacı; hukuki münasebetlerin düzenlenmesini, her türlü hukuki mesele ve anlaşmazlıkların adalet ve hakkaniyete uygun olarak çözümlenmesini ve hukuk kurallarının tam olarak uygulanmasını her derecede yargı organları, hakemler, resmi ve özel kişi, kurul ve kurumlar nezdinde sağlamaktır.

Avukat bu amaçla hukuki bilgi ve tecrübelerini adalet hizmetine ve kişilerin yararlanmasına tahsis eder.

Yargı organları, emniyet makamları, diğer kamu kurum ve kuruluşları ile kamu iktisadi teşebbüsleri, özel ve kamuya ait bankalar, noterler, sigorta şirketleri ve vakıflar avukatlara görevlerinin yerine getirilmesinde yardımcı olmak zorundadır. Kanunlarındaki özel hükümler saklı kalmak kaydıyla, bu

kurumlar avukatın gerek duyduğu bilgi ve belgeleri incelemesine sunmakla yükümlüdür. Bu belgelerden örnek alınması vekaletname ibrazına bağlıdır. Derdest davalarda müzekkereler duruşma günü beklenmeksizin mahkemedен alınabilir." hükmüne yer verilmiştir.

Dava dosyasının incelenmesinden; davacının geçirmiş olduğu trafik kazası sonucu sigorta şirketine başvurulacağından bahisle tüm tedavi evrakının onaylı birer örneğinin verilmesi istemiyle avukatı tarafından 13.07.2015 tarihinde Sivas Kamu Hastaneleri Birliği Genel Sekreterliği'ne yapılan başvurunun 22.07.2015 tarih ve 1038 sayılı işlemle reddedilmesi üzerine bakılan davanın açıldığı anlaşılmaktadır.

Danıştay 1. Dairesi'nin 10.04.2002 tarih ve E:2002/26 K:2002/52 sayılı avukatların kamu kurum ve kuruluşlarından isteyebileceği bilgi ve belgelerin kapsam ve sınırlarına ilişkin görüş yazısında, 1136 sayılı Avukatlık Kanunu'nun 2. maddesinin 3. fıkrasında yer alan "avukatın gerek duyduğu bilgi ve belge" ifadesinin anlam ve kapsamına açıklık getirilerek, "gerek duyma" ifadesinin keyfi, hiçbir nedene bağlı olmaksızın bir şeyi istemek iradesi anlamına gelmediği, herhangi bir işin yapılabilmesine bağlı bir istemi ifade ettiği, dolayısıyla avukatın gerek duyduğu bilgi ve belgeleri hangi işin yapılabilmesine bağlı olarak incelemek istediğini, gerekliliği açıklayan nedenlerle birlikte belirtmesinin ve bu belgelerin incelemesine sunulmasının Yasa hükmü gereği zorunlu olduğu belirtilmiştir.

Olayda, davacının avukat olan vekilince, sigorta şirketine başvurulacağı şeklinde sebebi de açıklanmak ve ekinde vekaletname sunmak suretiyle tüm tedavi evrakının onaylı birer örneğinin verilmesi istemiyle yaptığı başvurunun, 1136 sayılı Avukatlık Kanununun 2. maddesi gereğince kabulü gerektiğinden aksi yönde tesis edilen dava konusu işlemde hukuka uyarlık bulunmadığı sonucuna varılmaktadır.

Açıklanan nedenlerle, temyize konu Mahkeme kararının belirtilen gerekçeyle onanması gerektiği görüşüyle çoğunluk kararına katılmıyorum.

Danıştay Kararı - 8. Daire (E. 2016/3316)

Danıştay Kararı - 8. D., E. 2016/3316 K. 2020/280 T. 28.1.2020

İstem Özet: Sivas İdare Mahkemesinin 17/12/2015 gün ve E:2015/1012, K:2015/2027 sayılı kararının hukuka aykırı olduğu öne sürülerek, 2577 sayılı Kanununun 49. maddesi uyarınca temyizden incelenerek bozulması istemidir.

Savunmanın Özeti: Savunma verilmemiştir.

Danıştay Tetkik Hakimi: K1

Düşüncesi: İstem kabulü ile Mahkeme kararının bozulması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Hüküm veren Danıştay Sekizinci Dairesince işin gereği görüşüldü:

Dava, davacı vekili tarafından, davacının geçirmiş olduğu trafik kazası sebebiyle tedavi gördüğü Sivas Numune Hastanesi'nde bulunan davacıya ait tüm tedavi evrakının bir örneğinin trafik sigortasına başvurmak üzere verilmesi istemiyle yapılan başvurunun reddine ilişkin işlemin iptali istemiyle açılmıştır.

İdare Mahkemesince, davacı vekili tarafından talep edilen hususun, müvekkilinin geçirmiş olduğu trafik kazası neticesinde sigorta şirketi ile arasındaki ilişki nedeniyle ihtiyaç duyulan tedavi evraklarına ilişkin olduğu, Hasta Hakları Yönetmeliği'nin 16. maddesi uyarınca, hastanın kendisi veya vekili vasıtasıyla sağlık durumu ile ilgili bilgiler bulunan dosyayı ve kayıtları, doğrudan veya vekili veya kanuni temsilcisi vasıtasıyla inceleyebilme ve bir suretini alabilme hususunda tanınan hakkın kullanımına engel olabilecek herhangi bir istisnaya yer verilmediği, anılan Yönetmeliğin 23. maddesinde düzenlenen hususun ise sağlık hizmetinin verilmesi sebebiyle edinilen bilgilerin açıklanmasına ilişkin olduğu ve davacı vekili tarafından yapılan başvurunun anılan madde kapsamında değerlendirilemeyeceği, buna göre davacı vekili tarafından yapılan başvuru üzerine tedavi evraklarının davacıya verilmesinde herhangi bir hukuki engel bulunmadığından yapılan başvurunun reddine ilişkin dava konusu işlemde hukuka uyarlık bulunmayarak dava konusu işlemin iptaline karar verilmiştir.

Türkiye Cumhuriyeti Anayasa'sının "Özel hayatın gizliliği" başlıklı 20/3. maddesinde, "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini

talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmü yer almaktadır.

07.04.2016 tarih ve 29677 sayılı Resmi Gazete'de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Amaç" başlıklı 1. maddesinde, "Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir."; "Tanımlar" başlıklı 3. maddesinin 1. fıkrasında; "a) Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı, (...) d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi, e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi, (...) ifade eder." ; "Özel nitelikli kişisel verilerin işleme şartları" başlıklı 6. maddesinin 1. fıkrasında, "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir."; 2. fıkrasında, "Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır."; 3. fıkrasında ise, "Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir." hükümlerine yer verilmiştir.

4982 sayılı Bilgi Edinme Hakkı Kanunu'nun "Bilgi verme yükümlülüğü" başlıklı 5/1. maddesinde, "Kurum ve kuruluşlar, bu Kanunda yer alan istisnalar dışındaki her türlü bilgi veya belgeyi başvuranların yararlanmasına sunmak ve bilgi edinme başvurularını etkin, süratli ve doğru sonuçlandırmak üzere, gerekli idari ve teknik tedbirleri almakla yükümlüdürler." hükmüne yer verilmiş; öte yandan bilgi edinme hakkının sınırlarının düzenlendiği dördüncü bölüm altında yer alan "Özel hayatın gizliliği" başlıklı 21. maddesinde ise, "Kişinin izin verdiği haller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması halinde kişinin sağlık bilgileri ile özel ve aile hayatına,

şeref ve haysiyetine, mesleki ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır. Kamu yararının gerektirdiği hallerde, kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir." düzenlemesine yer verilmek suretiyle kişilerin sağlık bilgilerinin anılan Kanun kapsamı dışında yer aldığı ifade edilmiştir.

1136 sayılı Avukatlık Kanunu'nun "Avukatlığın amacı" başlıklı 2. maddesinin 3. fıkrasında, "Yargı organları, emniyet makamları, diğer kamu kurum ve kuruluşları ile kamu iktisadi teşebbüsleri, özel ve kamuya ait bankalar, noterler, sigorta şirketleri ve vakıflar avukatlara görevlerinin yerine getirilmesinde yardımcı olmak zorundadır. Kanunlarındaki özel hükümler saklı kalmak kaydıyla, bu kurumlar avukatın gerek duyduğu bilgi ve belgeleri incelemesine sunmakla yükümlüdür. Bu belgelerden örnek alınması vekaletname ibrazına bağlıdır. (...)" hükmüne yer verilmiştir.

Dosyanın incelenmesinden, davacı vekili tarafından, davacının 25.11.2014 tarihinde trafik kazası geçirmesi sebebiyle Sivas Numune Hastanesi'nde tedavi gördüğünden bahisle, davacıya ait tüm tedavi evrakının bir örneğinin trafik sigortasına verilmek üzere 1136 sayılı Avukatlık Kanunu'nun 2. maddesine dayanılarak 13.07.2015 tarihli dilekçe ile istenilmesi üzerine, başvuru dilekçesi ekinde yer alan vekaletnamenin genel vekaletname mahiyetinde olduğu, talep edilen bilgi ve belgelerin ise davacıya ait kişisel veri niteliği taşıdığı, bu nedenle özel vekaletname ibrazı yahut genel vekaletnameyle birlikte davacının dilekçesinin de ibraz edilmesi durumunda söz konusu bilgi ve belgelerin verilebileceği gerekçesiyle 22.07.2015 tarih ve 1037 sayılı işlemle reddedilmesi üzerine bakılmakta olan davanın açıldığı anlaşılmaktadır.

Yukarıda yer verilen 6698 sayılı Kanun'un 3. maddesine göre kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Anayasa Mahkemesinin kararlarında da belirtildiği üzere "... adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler" kişisel veri olarak kabul edilmektedir.

6698 sayılı Kanunda kişisel verilerin işlenmesine ilişkin genel şartlar ortaya konulmakla birlikte yasa koyucunun takdir yetkisi kapsamında kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri gibi

özel nitelikli kişisel verilerin işleme şartlarının ayrı bir düzenlemeye tabi tutulduğu, bu düzenlemeyle birtakım kişisel verilerin özel hukuki koruma altına alındığı görülmektedir.

Özel nitelikli kişisel verilerin işlenebilmesi için kural olarak ilgililerin açık rızasının bulunması gerekmektedir. Ancak 6698 sayılı Kanun'un 6. maddesinin 3. fıkrasında, sağlık ve cinsel hayat dışındaki özel nitelikli kişisel verilerin, "Kanunlarda öngörülen hallerde" ilgililerin açık rızası aranmaksızın da işlenebileceği belirtilmek suretiyle anılan kuralın istisnasına yer verilmiştir. Bununla birlikte sağlık ve cinsel hayata ilişkin kişisel verilerin ise bu istisnadan da istisna edilerek ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği ifade edilmek suretiyle, önemine binaen "Kanunlarda öngörülen hallerde" şeklinde bir ifade biçimiyle yetinilmeyerek, bu verilerin ilgililerin açık rızası aranmaksızın işlenebileceği hallerin doğrudan Kanun maddesinde düzenlendiği görülmektedir.

Şu halde, kökeni Roma Hukukuna dayanan ve günümüzde genel hukuk kaidesi olarak kabul gören "istisna içerikli hükümlerin dar yorumlanması" (singularia non sunt extenda) ilkesi uyarınca, işleme şartları bizzat 6698 sayılı Kanun'da yer alan kişilerin sağlık verilerine ilişkin bilgilerin, ancak kişinin açık rızası halinde işlenebileceği, "işlenme" ifadesinden ise, ilgili verinin açıklanması, aktarılması, elde edilebilir hale getirilmesi gibi her türlü işlemin anlaşılması gerektiği açıktır.

Diğer taraftan, Avukat-müvekkil ilişkisi temelde 6098 sayılı Türk Borçlar Kanunu'nun 502 ve devamı maddelerinde yer alan "vekalet sözleşmesi"ne dayanmakta olup; vekilin üstlendiği iş ve hizmetleri, vekalet verenin haklı menfaatlerini gözeterek, sadakat ve özenle yürütme ödevi bulunmaktadır. Bu özen görevi, 1136 sayılı Kanun'da da avukatın işini özenle ve sonuna kadar takip etme (m. 34 ve 171) ödeviyle de somutlaştırılmış bulunmaktadır. Öte yandan 1136 sayılı Avukatlık Kanunu'nun 2. maddesinde, avukatlığın amacının, hukuki münasebetlerin düzenlenmesini, her türlü hukuki mesele ve anlaşmazlıkların adalet ve hakkaniyete uygun olarak çözümlenmesini ve hukuk kurallarının tam olarak uygulanmasını her derecede yargı organları, hakemler, resmi ve özel kişi, kurul ve kurumlar nezdinde sağlamak olduğu, avukatın bu amaçla hukuki bilgi ve tecrübelerini adalet hizmetine ve kişilerin yararlanmasına tahsis edeceği ifade edildikten sonra aynı maddenin 3. fıkrasında, madde metninde sayılan kamu kurum ve kuruluşları ile özel hukuk tüzel kişilerinin avukatların ihtiyaç duyduğu bilgi ve belgeleri incelemeye sunmakla yükümlü kılınarak avukatlara görevlerinin yerine getirilmesi kapsamında, müvekkilinin hukukunu savunabilmesine, haklarını dava etmesine, yargılama sürecinin çabuklaştırılmasına ve uyuşmazlıkların adalet ve hakkaniyete uygun olarak

çözümlemesine yardımcı olma görevinin yüklendiği anlaşılmaktadır. Şüphesiz bu yükümlülük, "Kanunlardaki özel hükümler saklı kalmak kaydıyla" ilgili kurum ve kuruluşlara getirilmiş olup mutlak değildir.

Buna göre, avukatın müvekkiliyle iş ilişkisi içinde üstlendiği bir işin mahiyetine göre gerek duyduğu bilgi ve belgeyi başka kurum, kuruluş veya özel hukuk tüzel kişilerinden vekalet görevi kapsamında talep etmesi avukatın vekalet görevini özenle ifa etme yükümlülüğü çerçevesinde değerlendirilmekle birlikte, müvekkilinin özel nitelikli kişisel veri mahiyetinde bulunan sağlık bilgilerine ilişkin kayıtların, yukarıda yer verilen mevzuat hükümleri doğrultusunda ancak ilgilinin açık rızasıyla davalı idarece verilebilmesi mümkün bulunduğundan, davacı vekilinin davacıdan aldığı "genel vekaletname" ile müvekkiline ait sağlık bilgilerine ilişkin kayıtların istenemeyeceğine ilişkin dava konusu işlemde hukuka aykırılık; aksi yönde karar veren İdare Mahkemesi kararında ise hukuki isabet bulunmamaktadır.

Açıklanan nedenlerle; Sivas İdare Mahkemesinin temyize konu kararının bozulmasına, dosyanın yeniden bir karar verilmek üzere anılan Mahkemeye gönderilmesine, bu kararın tebliğ tarihini izleyen 15 (onbeş) gün içerisinde kararın düzeltilmesi yolu açık olmak üzere, 28/01/2020 tarihinde oyçokluğu ile karar verildi.

KARŞIOY:

- Dava, davacı vekili tarafından, davacının geçirmiş olduğu trafik kazası sebebiyle tedavi gördüğü Sivas Numune Hastanesi'nde bulunan davacıya ait tüm tedavi evrakının bir örneğinin trafik sigortasına başvurmak üzere verilmesi istemiyle yapılan başvurunun reddine ilişkin işlemin iptali istemiyle açılmıştır.

1136 sayılı Avukatlık Kanununun "Avukatlığın amacı" başlıklı 2. maddesinde, "Avukatlığın amacı; hukuki münasebetlerin düzenlenmesini, her türlü hukuki mesele ve anlaşmazlıkların adalet ve hakkaniyete uygun olarak çözümlenmesini ve hukuk kurallarının tam olarak uygulanmasını her derecede yargı organları, hakemler, resmi ve özel kişi, kurul ve kurumlar nezdinde sağlamaktır.

Avukat bu amaçla hukuki bilgi ve tecrübelerini adalet hizmetine ve kişilerin yararlanmasına tahsis eder.

Yargı organları, emniyet makamları, diğer kamu kurum ve kuruluşları ile kamu iktisadi teşebbüsleri, özel ve kamuya ait bankalar, noterler, sigorta şirketleri ve vakıflar avukatlara görevlerinin yerine getirilmesinde yardımcı olmak zorundadır. Kanunlarındaki özel hükümler saklı kalmak kaydıyla, bu kurumlar avukatın gerek duyduğu bilgi ve belgeleri incelemesine sunmakla yükümlüdür. Bu

belgelerden örnek alınması vekaletname ibrazına bağlıdır. Derdest davalarda müzekkereler duruşma günü beklenmeksizin mahkemeden alınabilir." hükmüne yer verilmiştir.

Dava dosyasının incelenmesinden; davacının geçirmiş olduğu trafik kazası sonucu sigorta şirketine başvurulacağından bahisle tüm tedavi evrakının onaylı birer örneğinin verilmesi istemiyle avukatı tarafından 13.07.2015 tarihinde Sivas Kamu Hastaneleri Birliği Genel Sekreterliği'ne yapılan başvurunun 22.07.2015 tarih ve 1037 sayılı işlemle reddedilmesi üzerine bakılan davanın açıldığı anlaşılmaktadır.

Danıştay 1. Dairesi'nin 10.04.2002 tarih ve E:2002/26 K:2002/52 sayılı avukatların kamu kurum ve kuruluşlarından isteyebileceği bilgi ve belgelerin kapsam ve sınırlarına ilişkin görüş yazısında, 1136 sayılı Avukatlık Kanunu'nun 2. maddesinin 3. fıkrasında yer alan "avukatın gerek duyduğu bilgi ve belge" ifadesinin anlam ve kapsamına açıklık getirilerek, "gerek duyma" ifadesinin keyfi, hiçbir nedene bağlı olmaksızın bir şeyi istemek iradesi anlamına gelmediği, herhangi bir işin yapılabilmesine bağlı bir istemi ifade ettiği, dolayısıyla avukatın gerek duyduğu bilgi ve belgeleri hangi işin yapılabilmesine bağlı olarak incelemek istediğini, gerekliliği açıklayan nedenlerle birlikte belirtmesinin ve bu belgelerin incelemesine sunulmasının Yasa hükmü gereği zorunlu olduğu belirtilmiştir.

Olayda, davacının avukat olan vekilince, sigorta şirketine başvurulacağı şeklinde sebebi de açıklanmak ve ekinde vekaletname sunmak suretiyle tüm tedavi evrakının onaylı birer örneğinin verilmesi istemiyle yaptığı başvurunun, 1136 sayılı Avukatlık Kanununun 2. maddesi gereğince kabulü gerektiğinden aksi yönde tesis edilen dava konusu işlemde hukuka uyarlık bulunmadığı sonucuna varılmaktadır.

Açıklanan nedenlerle, temyize konu Mahkeme kararının belirtilen gerekçeyle onanması gerektiği görüşüyle çoğunluk kararına katılmıyorum.

Danıştay Kararı - 8. Daire (E. 2016/2727)

Danıştay Kararı - 8. D., E. 2016/2727 K. 2020/701 T. 11.2.2020

İstemin Özeti: Malatya İdare Mahkemesinin 02/12/2015 gün ve E:2015/990, K:2015/1483 sayılı kararının hukuka aykırı olduğu öne sürülerek, 2577 sayılı Kanununun 49. Maddesi uyarınca temyizen incelenerek bozulması istemidir.

Savunmanın Özeti: Savunma verilmemiştir.

Danıştay Tetkik Hakimi: K1

Düşüncesi: İstemin reddi gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Hüküm veren Danıştay Sekizinci Dairesince işin gereği görüşüldü:

Dava, davacı vekili tarafından, davacının geçirmiş olduğu trafik kazası sebebiyle tedavi gördüğü Malatya Devlet Hastanesi'nde bulunan davacıya ait tüm tedavi evrakının bir örneğinin trafik sigortasına başvurmak üzere verilmesi istemiyle yapılan başvurunun reddine ilişkin işlemin iptali istemiyle açılmıştır.

İdare Mahkemesince, davacının avukat olan vekilince, sigorta şirketine başvurulacağı şeklinde sebebi açıklanmak ve ekinde vekaletname sunmak suretiyle tüm tedavi evrakının onaylı birer örneğinin verilmesi istemiyle yapılan başvurunun, istenilen belgelerin yasalarca istisna kapsamında tutulan bilgi ve belgelerden olmaması nedeniyle 1136 sayılı Avukatlık Kanununun 2. Maddesi gereğince kabulü gerekirken, aksi yönde tesis edilen dava konusu işlemde hukuka uyarlık bulunmadığı gerekçesiyle dava konusu işlemin iptaline karar verilmiştir.

Türkiye Cumhuriyeti Anayasa'sının "Özel hayatın gizliliği" başlıklı 20/3. Maddesinde, "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." Hükmü yer almaktadır.

07.04.2016 tarih ve 29677 sayılı Resmi Gazete'de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Amaç" başlıklı 1. Maddesinde, "Bu Kanunun amacı, kişisel verilerin işlenmesinde

başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.”; “Tanımlar” başlıklı 3. Maddesinin 1. Fıkrasında; “a) Açık rıza: Belirli bir konuya ilişkin, bilgilendirilme ve özgür iradeyle açıklanan rıza”, (...) d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi, e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi, (...) ifade eder.” ; Özel nitelikli kişisel verilerin işleme şartları” başlıklı 6. Maddesinin 1. Fıkrasında, “Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği,sağlığı,cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.”; 2. Fıkrasında, “Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.”; 3. Fıkrasında ise, “Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.” Hükümlerine yer verilmiştir.

4982 sayılı Bilgi Edinme Hakkı Kanunu’nun “Bilgi verme yükümlülüğü” başlıklı 5/1. Maddesinde, “Kurum ve kuruluşlar, bu Kanunda yer alan istisnalar dışındaki her türlü bilgi veya belgeyi başvuranların yararlanmasına sunmak ve bilgi edinme başvurularını etkin, süratli ve doğru sonuçlandırmak üzere, gerekli idari ve teknik tedbirleri almakla yükümlüdürler.” Hükmüne yer verilmiş; öte yandan bilgi edinme hakkının sınırlarının düzenlendiği dördüncü bölüm altında yer alan “Özel hayatın gizliliği” başlıklı 21. Maddesinde ise, “Kişinin izin verdiği haller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması halinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, mesleki ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır. Kamu yararının gerektirdiği hallerde, kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir.” Düzenlemesine yer verilmek suretiyle kişilerin sağlık bilgilerinin anılan Kanun kapsamı dışında yer aldığı ifade edilmiştir.

1136 sayılı Avukatlık Kanunu'nun "Avukatlığın amacı" başlıklı 2. Maddesinin 3. Fıkrasında, "Yargı organları, emniyet makamları, diğer kamu kurum ve kuruluşları ile kamu iktisadi teşebbüsleri, özel ve kamuya ait bankalar, noterler, sigorta şirketleri ve vakıflar avukatlara görevlerinin yerine getirilmesinde yardımcı olmak zorundadır. Kanunlarındaki özel hükümler saklı kalmak kaydıyla, bu kurumlar avukatın gerek duyduğu bilgi ve belgeleri incelemesine sunmakla yükümlüdür. Bu belgelerden örnek alınması vekaletname ibrazına bağlıdır. (...)" hükmüne yer verilmiştir.

Dosyanın incelenmesinden, davacı vekili tarafından, davacının 25.03.2015 tarihinde trafik kazası geçirmesi sebebiyle Malatya Devlet Hastanesi'nde tedavi gördüğünden bahisle, davacıya ait tüm tedavi evrakının bir örneğinin trafik sigortasına verilmek üzere 1136 sayılı Avukatlık Kanunu'nun 2. Maddesine dayanılarak 14.05.2015 tarihli dilekçe ile istenilmesi üzerine, davacıya ait vekaletnamenin usulüne uygun bulunmadığı ancak eksikliklerin giderilmesi halinde ilgili bilgi-belgelerin gönderilebileceği gerekçesiyle 18.05.2015 tarih ve 05 sayılı işlemle reddedilmesi üzerine bakılmakta olan davanın açıldığı anlaşılmaktadır.

Yukarıda yer verilen 6698 sayılı Kanun'un 3. Maddesine göre kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Anayasa Mahkemesinin kararlarında da belirtildiği üzere "... adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler" kişisel veri olarak kabul edilmektedir.

6698 sayılı Kanunda kişisel verilerin işlenmesine ilişkin genel şartlar ortaya konulmakla birlikte yasa koyucunun takdir yetkisi kapsamında kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri gibi özel nitelikli kişisel verilerin işleme şartlarının ayrı bir düzenlemeye tabi tutulduğu, bu düzenlemeyle birtakım kişisel verilerin özel hukuki koruma altına alındığı görülmektedir.

Özel nitelikli kişisel verilerin işlenebilmesi için kural olarak ilgililerin açık rızasının bulunması gerekmektedir. Ancak 6698 sayılı Kanun'un 6. Maddesinin 3. Fıkrasında, sağlık ve cinsel hayat dışındaki özel nitelikli kişisel verilerin, "Kanunlarda öngörülen hallerde" ilgililerin açık rızası aranmaksızın da işlenebileceği belirtilmek suretiyle anılan kuralın istisnasına yer verilmiştir. Bununla birlikte sağlık ve cinsel hayata ilişkin kişisel verilerin ise bu istisnadan da istisna edilerek ancak kamu

sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği ifade edilmek suretiyle, önemine binaen “Kanunlarda öngörülen hallerde” şeklinde bir ifade biçimiyle yetinilmeyerek, bu verilerin ilgililerin açık rızası aranmaksızın işlenebileceği hallerin doğrudan Kanun maddesinde düzenlendiği görülmektedir.

Şu halde, kökeni Roma Hukukuna dayanan ve günümüzde genel hukuk kaidesi olarak kabul gören “istisna içerikli hükümlerin dar yorumlanması” (singularia non sunt extenda) ilkesi uyarınca, işleme şartları bizzat 6698 sayılı Kanun’da yer alan kişilerin sağlık verilerine ilişkin bilgilerin, ancak kişinin açık rızası halinde işlenebileceği, “işlenme” ifadesinden ise, ilgili verinin açıklanması, aktarılması, elde edilebilir hale getirilmesi gibi her türlü işlemin anlaşılması gerektiği açıktır.

Diğer taraftan, Avukat-müvekkililişkisi temelde 6098 sayılı Türk Borçlar Kanunu’nun 502 ve devamı maddelerinde yer alan “vekalet sözleşmesi”ne dayanmakta olup; vekilin üstlendiği iş ve hizmetleri, vekalet verenin haklı menfaatlerini gözeterek, sadakat ve özenle yürütme ödevi bulunmaktadır. Bu özen görevi, 1136 sayılı Kanun’da da avukatın işini özenle ve sonuna kadar takip etme (m. 34 ve 171) ödeviyle de somutlaştırılmış bulunmaktadır. Öte yandan 1136 sayılı Avukatlık Kanunu’nun 2. Maddesinde, avukatlığın amacının, hukuki münasebetlerin düzenlenmesini, her türlü hukuki mesele ve anlaşmazlıkların adalet ve hakkaniyete uygun olarak çözümlenmesini ve hukuk kurallarının tam olarak uygulanmasını her derecede yargı organları, hakemler, resmi ve özel kişi, kurul ve kurumlar nezdinde sağlamak olduğu, avukatın bu amaçla hukuki bilgi ve tecrübelerini adalet hizmetine ve kişilerin yararlanmasına tahsis edeceği ifade edildikten sonra aynı maddenin 3. Fıkrasında, madde metninde sayılan kamu kurum ve kuruluşları ile özel hukuk tüzel kişilerinin avukatların ihtiyaç duyduğu bilgi ve belgeleri incelemeye sunmakla yükümlü kılınarak avukatlara görevlerinin yerine getirilmesi kapsamında, müvekkilinin hukukunu savunabilmesine, haklarını dava etmesine, yargılama sürecinin çabuklaştırılmasına ve uyuşmazlıkların adalet ve hakkaniyete uygun olarak çözümlenmesine yardımcı olma görevinin yüklendiği anlaşılmaktadır. Şüphesiz bu yükümlülük, “Kanunlardaki özel hükümler saklı kalmak kaydıyla” ilgili kurum ve kuruluşlara getirilmiş olup mutlak değildir.

Olayda, davacının Malatya 1. Noterliği’nin 05.05.2015 tarih ve 7970 yevmiye numaralı vekaletnamesi ile davacı vekiline verdiği vekaletname içeriğinde, “... adıma hastanelerde gerekli evraklar ile tüm tedavi evraklarını almaya (...) yetkili olmak üzere” ifadesiyle açıkça avukat olan vekilini yetkilendirdiği görülmekte olup, davacının açık rızasını yansıtan bu ifadenin özel nitelikli kişisel veri

mahiyetinde bulunan sađlık bilgilerine iliřkin kayıtların 1136 sayılı Kanun ve 6698 sayılı Kanun h k mleri  er evesinde avukatı tarafından istenebilmesine olanak tanıdıđından, vekaletnamenin usul ne uygun bulunmadıđı gerek esiyle talebin reddedilmesine iliřkin dava konusu iřlemde hukuka uyarlık bulunmamaktadır.

İdare ve vergi mahkemeleri tarafından verilen kararların temyiz yolu ile incelenip bozulabilmeleri 2577 sayılı İdari Yargılama Usul  Kanununun 49. Maddesinin 1. Fıkrasında yazılı nedenlerin bulunmasına bađlıdır.

A ıklanan nedenlerle, davalı idarenin temyiz isteminin reddiyle Malatya İdare Mahkemesince verilen ve h k m fıkrası itibariyle hukuka uygun bulunan kararın yukarıda belirtilen gerek eyle onanmasınave temyiz giderlerinin istemde bulunan  zerinde bırakılmasına, bu kararın tebliđ tarihini izleyen 15 (onbeř) g n i erisinde kararın d zeltilmesi yolu a ık olmak  zere, 11/02/2020 tarihinde gerek ede oy okluđu; esasta oybirliđi ile karar verildi.

GEREK EDE KARŐIOY:

- İdare ve vergi mahkemeleri tarafından verilen kararların temyiz yolu ile incelenip bozulabilmeleri 2577 sayılı İdari Yargılama Usul  Kanununun 49. Maddesinin 1. Fıkrasında yazılı nedenlerin bulunmasına bađlıdır.

İdare Mahkemesince verilen karar ve dayandıđı gerek e usul ve yasaya uygun olup, deđiřik gerek eyle onanmasını gerektiren bir neden bulunmadıđından, Mahkeme kararının onanması gerektiđi g r ř yle  ođunluk kararına katılmıyorum.

Danıştay Kararı - 15. D., E. 2015/6279 K. 2017/7022 T. 29.11.2017

05/02/2015 tarih ve 29258 sayılı Resmî Gazete'de yayımlanan Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği'nin, Anayasa'ya aykırı kanun hükmüne dayanılarak çıkartıldığından hukuka aykırı olması nedeniyle tümünün, ayrıca, 4. maddesinin 1. fıkrasının (n) bendinde yer alan "denetleyen" ibaresinin, 9. maddesinin 1. fıkrasının (f) bendinin, 13. maddesinin 1. fıkrasının (c), (ç), ve (d) bentlerinin, 45. maddesinin 2. fıkrasının (d) bendinin, 5258 sayılı Aile Hekimliği Kanunu'na göre, kişiye yönelik koruyucu sağlık hizmetleri ile birinci basamak teşhis, tedavi ve rehabilite edici sağlık hizmetlerinin "aile hekimliği hizmetleri" olarak tanımlandığı, bunun dışında kalan birinci basamak sağlık hizmetlerinin ise toplum sağlığı merkezleri tarafından sunulması gerektiği hususunun hükme bağlandığı, ancak, dava konusu düzenlemenin bu Kanuna aykırı hükümler içerdiği; anılan düzenleme ile aile hekimlerinin özlük haklarına müdahale edildiği; toplum sağlığı merkezlerinin görev ve sorumluluklarının aile hekimlerine yıkılmaya çalışıldığı; aile hekimleri üzerinde denetim yetkisi olmayan toplum sağlığı merkezinin denetim merkezi gibi yetkilendirildiği; aile hekimlerinin birey odaklı birinci basamak sağlık hizmeti sunarken, toplum sağlığı merkezinin toplum odaklı birinci basamak sağlık hizmeti sunduğu, iki ayrı hizmet sunucusu olan kurumlar arasında astlık-üstlük ilişkisinin bulunmadığı halde dava konusu düzenleme ile toplum sağlığı merkezine aile hekimleri üzerinde görev veren üst kurum nitelendirilmesinin yapıldığı; aile hekimlerinin, 5258 sayılı Aile Hekimliği Kanunu uyarınca, adına Valilik ile sözleşme imzaladığı, gerek Aile Hekimliği Uygulama Yönetmeliği gerekse Aile Hekimliği Uygulaması Kapsamında nca Çalıştırılan Personele Yapılacak Ödemeler İle Sözleşme Usul ve Esasları Hakkında Yönetmelik hükümlerine göre, aile hekimlerinin amirinin Vali olduğu, buna rağmen dava konusu Yönetmelikte 5258 sayılı Aile Hekimliği Kanunu ve ilgili yönetmelik hükümlerine aykırı düzenlemelere yer verildiği ileri sürülerek, 10. maddesinin 1. fıkrasının (a) bendinin, dava konusu düzenleme ile toplum sağlığı merkezine, Bakanlığın belirlemiş olduğu standartlara uygun olarak bölgedeki sağlık hizmeti sunucularından veri toplamak, yürütülen hizmetlerin kayıt ve istatistiklerini elektronik veya basılı ortamda tutmak, olağanüstü durumlarda bölgedeki sağlık hizmeti sunucularından yazılı olarak da veri toplamak, topladığı verileri zamanında müdürlüğe iletmek görevi verildiği, bu durumun kişisel verilerin gizliliği hükmünü ihlal ettiği, düzenlemenin Anayasaya aykırı olduğu ileri sürülerek, 21. maddesinin 1. fıkrasının (a) bendinin, anılan düzenlemede, Adli Tıp Kurumunun doğrudan hizmet

vermediği yerlerde, adli tıbbi hizmetler konusunda Cumhuriyet Savcılığı, ilçe sağlık müdürlüğü, aile hekimliği birimleri ve diğer sağlık kurum ve kuruluşları ile işbirliği içinde çalışarak bu hizmetlerin 25/1/2013 tarihli ve 28539 sayılı Resmî Gazete’de yayımlanan Aile Hekimliği Uygulama Yönetmeliği çerçevesinde yürütülmesini sağlamak görevinin toplum sağlığı merkezlerinin görevleri arasında sayıldığı, ancak, adli tabiplik hizmetlerinin koruyucu, tedavi edici sağlık hizmeti kapsamında olmadığı, bu sebeple de toplum sağlığı merkezi hekimlerine ve aile hekimlerine adli tabiplik hizmetinin yüklenmesinin Kanuna aykırılık teşkil ettiği ileri sürülerek, 22. maddesinin 1. fıkrasının (a) bendinde yer alan "buldukları ekipmanlar ölçüsünde acil sağlık hizmeti sunmak ve" ibaresinin ve (b) bendinde yer alan "uygulamak" ibaresinin, söz konusu madde ile toplum sağlığı merkezi hekimlerine acil sağlık hizmeti sunma görevi verilmiş ise de, bu hekimlerin asıl görevinin koruyucu hekimlik içeren birinci basamak sağlık hizmeti sunumu olduğu, koruyucu sağlık hizmetlerinin acil sağlık hizmetlerinden çok farklı nitelikler taşıdığı, acil sağlık hizmetlerinin niteliği gereği acil sağlık hizmeti sunacakların bu konuda eğitim alması ve deneyim sahibi olması gerektiği, hastaların gereksinim duyduğu sağlık hizmetini nitelikli bir şekilde alma haklarının ihlal edildiği ileri sürülerek, 4. maddesinin 1. fıkrasının (ö) bendinin, 26. maddesinin 1. fıkrasının (a) ve (c) bentlerinin, anılan hükümler ile toplum sağlığı merkezlerine kendilerine bağlı iş sağlığı ve güvenliği birimi kurma ve çalışan sağlığı ve güvenliği hizmetlerini verme yetkisinin düzenlendiği; kamu görevlilerinin görev tanımları dışında çalıştırılmayacakları, başka kurum ve kuruluşlarda görevlendirmelerinin ancak yasal düzenlemelerle yapmanın mümkün olduğu; toplum sağlığı merkezlerinin kadrosunda işyeri hekimi veya iş güvenliği uzmanının bulunmadığı, dolayısıyla düzenlemenin hukuka aykırı olduğu ileri sürülerek, 30. maddesinin 2. fıkrasının, dava konusu düzenlemede, toplum sağlığı merkezlerinin nüfus hareketlerine ilişkin görevlerinin kapsamının tarım işçileri ile kısıtlanmasının hukuka aykırı olduğu ileri sürülerek, dava konusu Yönetmeliğin 21. maddesi ile atıfta bulunulan 25/01/2013 tarih ve 28539 sayılı Resmî Gazete’de yayımlanan Aile Hekimliği Uygulama Yönetmeliği’nin 10. maddesinin 5. fıkrasının, dava konusu Yönetmeliğin 21. maddesinin 1. fıkrasının (a) bendinin yollama yaptığı Aile Hekimliği Uygulama Yönetmeliğinin 10. maddesi ile gerek aile hekimlerine gerekse toplum sağlığı merkezi hekimlerine, 5258 sayılı Kanunda verilen görev kapsamını aşacak nitelikte adli tabiplik görevinin verilmesinin Kanuna aykırılık teşkil ettiği, belirtilen sebeplerle dava konusu düzenlemenin kamu yararı, hizmet gerekleri, üst hukuk normlarına ve hukuka aykırı olduğu ileri sürülerek iptali ile yine dava konusu Yönetmeliğin dayanakları arasında yer alan 5258 sayılı Aile Hekimliği Kanunu’nun 5. maddesinin 2. fıkrasındaki "Aile hekimliği hizmetleri dışında kalan birinci basamak sağlık hizmetleri toplum sağlığı merkezleri tarafından verilir ve bu merkezlerin organizasyonu, kadroları, görevleri ile çalışma usûl ve esasları nca belirlenir." düzenlemesinin,

toplum sađlıđı merkezinde sunulan sađlık hizmetinin, kamu grevlileri eliyle yrtlmesi sebebiyle, grev, yetki, hak ve ykmllklerin kanunla dzenlenmesi gerektiđi halde bu alanda dzenleme yetkisinin anılan Kanun ile na bırakılmıř olmasının yasama yetkisinin devri niteliđinde olduđu ve Anayasanın 2., 7., 8., 123., ve 128. maddelerine aykırılık teřkil ettiđi iddiasıyla iptali iin Anayasa Mahkemesine bařvurulması istenilmektedir.

Savunmanın zeti: 663 sayılı ve Bađlı Kuruluřlarının Teřkilat ve Grevleri Hakkında Kanun Hkmnde Kararname geređince, temel sađlık hizmetlerini, bu kapsamda birinci basamak sađlık hizmetlerini, Bakanlık hedef ve politikalarına uygun olarak yrtmek ve bu hususta gerekli dzenlemeleri yapmak grev ve yetkisinin uhdelerinde olduđu; 3359 sayılı Sađlık Hizmetleri Temel Kanunu, 5258 sayılı Kanun'un 5. maddesi ve 663 sayılı KHK'nın 36. maddesine istinaden hazırlanan Toplum Sađlıđı Merkezi ve Bađlı Birimler Ynetmeliđi ile toplum sađlıđı merkezleri ve bađlı birimlerinin aılması, kapatılması, organizasyonu ve grevleriyle ilgili usul ve esasların dzenlenmiř olduđu; anılan dzenlemenin, toplum sađlıđı merkezlerini gçlendirerek hizmetlerin kaliteli, etkin, verimli bir řekilde sunulmasına katkı sađlamak, aile hekimliđi haricindeki birinci basamak sađlık hizmetlerinin etkinliđini artırmak, aile hekimliđi hizmetlerine eriřimi kolaylařtırmak, bireye ynelik birinci basamak sađlık hizmetleri ile topluma ynelik birinci basamak sađlık hizmetlerinin daha btnleřik bir yapıda yrtlmesini sađlamak amacı tařıdıđı; Ynetmelik kapsamında, Halk Sađlıđı Kurumu tařra teřkilatı hizmet birimleri arasında yer alan toplum sađlıđı merkezlerine, organizasyon, eřgdm, eđitim ve denetim grevleriyle birlikte toplumsal sađlık hizmeti sunma grevi verildiđi, bylelikle toplum sađlıđı hizmetlerinin mnhasıran bu hizmete ynelik grevleri olan merkezler marifetiyle layıkıyla verilebilir hale getirilmesinin hedeflendiđi; bu bađlamda, toplum sađlıđı merkezlerinin organizasyon, eřgdm, eđitim ve denetim grevleriyle birlikte toplumsal sađlık hizmeti sunma grevleri gz nne alındıđında, birinci basamak sađlık hizmetlerinin sunumu noktasında halk sađlıđı mdrlđ adına izleme ve deđerlendirme alıřmalarının sekreteryasını yrtmesinde hukuka aykırılık bulunmadıđı; adı geen merkezlerin Bakanlık ve Kurum idari yapısındaki yerinin ilgili mevzuat hkmleri kapsamında belirlendiđi, bu bađlamda, toplum sađlıđı merkezlerinin tařra teřkilatı ierisinde halk sađlıđı mdrlđnn izdřm ve mdrlk yetkilerini kullanan idari birimler olduđu; dava konusu dzenlemenin st hukuk normlarına, kamu menfaatine ve hizmet gereklerine uygun olduđu ileri srlerek davanın reddi gerektiđi savunulmaktadır.

Danıřtay Tetkik Hakimi:

Dřncesi: Dava konusu dzenlemede hizmet gereklerine, kamu yararına, st hukuk normlarına ve hukuka aykırılık bulunmadıđı, davanın reddi gerektiđi dřnlmektedir. **Danıřtay Savcısı:**

Düşüncesi: Dava; 05.02.2015 tarih ve 29258 sayılı Resmi Gazete'de yayımlanan Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği'nin 4. maddesinin 1. fıkrasının (n) bendinde yer alan "denetleyen" ibaresinin ve (ö) bendinin, 9. maddesinin (f) bendinin, 10. maddesinin 1. fıkrasının (a) bendinin, 13. maddesinin 1. fıkrasının (c), (ç), ve (d) bentlerinin, 21. maddesinin 1. fıkrasının (a) bendinin, 22. maddesinin 1. fıkrasının (a) bendinde yer alan "buldukları ekipmanlar ölçüsünde acil sağlık hizmeti sunmak ve" ibaresinin ve (b) bendinde yer alan "uygulamak" ibaresinin, 26. maddesinin (a) ve (c) bentlerinin, 30. maddesinin 2. fıkrasının, 45. maddesinin 2. fıkrasının (d) bendinin ve bu Yönetmelik ile atıfta bulunulan 25.01.2013 tarih ve 28539 sayılı Resmi Gazete'de yayımlanan Aile Hekimliği Uygulama Yönetmeliği'nin 10. maddesinin 5. fıkrasının iptali ile yine dava konusu Yönetmeliğin dayanağı olan 5258 sayılı Aile Hekimliği Kanununun 5. maddesinin Anayasaya aykırı olduğu iddiasıyla iptali için Anayasa mahkemesine başvurulması istemiyle açılmıştır.

T.C. DANIŞTAY ONBEŞİNCİ DAİRE

Esas No: 2015/6279

Karar No: 2017/7022

Davacı:

Vekili:

Davalı:

Vekilleri:

Davanın Özeti: 05/02/2015 tarih ve 29258 sayılı Resmî Gazete'de yayımlanan Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği'nin, Anayasa'ya aykırı kanun hükmüne dayanılarak çıkartıldığından hukuka aykırı olması nedeniyle tümünün, ayrıca, 4. maddesinin 1. fıkrasının (n) bendinde yer alan "denetleyen" ibaresinin, 9. maddesinin 1. fıkrasının (f) bendinin, 13. maddesinin 1. fıkrasının (c), (ç), ve (d) bentlerinin, 45. maddesinin 2. fıkrasının (d) bendinin, 5258 sayılı Aile Hekimliği Kanunu'na göre, kişiye yönelik koruyucu sağlık hizmetleri ile birinci basamak teşhis, tedavi ve rehabilite edici sağlık hizmetlerinin "aile hekimliği hizmetleri" olarak tanımlandığı, bunun dışında kalan birinci basamak sağlık hizmetlerinin ise toplum sağlığı merkezleri tarafından sunulması gerektiği hususunun hükme bağlandığı, ancak, dava konusu düzenlemenin bu Kanuna aykırı hükümler içerdiği; anılan düzenleme ile aile hekimlerinin özlük haklarına müdahale edildiği; toplum sağlığı merkezlerinin görev ve sorumluluklarının aile hekimlerine yıkılmaya çalışıldığı; aile hekimleri üzerinde denetim yetkisi olmayan toplum sağlığı merkezinin denetim merkezi gibi yetkilendirildiği;

aile hekimlerinin birey odaklı birinci basamak sağlık hizmeti sunarken, toplum sağlığı merkezinin toplum odaklı birinci basamak sağlık hizmeti sunduğu, iki ayrı hizmet sunucusu olan kurumlar arasında astlık-üstlük ilişkisinin bulunmadığı halde dava konusu düzenleme ile toplum sağlığı merkezine aile hekimleri üzerinde görev veren üst kurum nitelendirilmesinin yapıldığı; aile hekimlerinin, 5258 sayılı Aile Hekimliği Kanunu uyarınca, adına Valilik ile sözleşme imzaladığı, gerek Aile Hekimliği Uygulama Yönetmeliği gerekse Aile Hekimliği Uygulaması Kapsamında nca Çalıştırılan Personele Yapılacak Ödemeler İle Sözleşme Usul ve Esasları Hakkında Yönetmelik hükümlerine göre, aile hekimlerinin amirinin Vali olduğu, buna rağmen dava konusu Yönetmelikte 5258 sayılı Aile Hekimliği Kanunu ve ilgili yönetmelik hükümlerine aykırı düzenlemelere yer verildiği ileri sürülerek, 10. maddesinin 1. fıkrasının (a) bendinin, dava konusu düzenleme ile toplum sağlığı merkezine, Bakanlığın belirlemiş olduğu standartlara uygun olarak bölgedeki sağlık hizmeti sunucularından veri toplamak, yürütülen hizmetlerin kayıt ve istatistiklerini elektronik veya basılı ortamda tutmak, olağanüstü durumlarda bölgedeki sağlık hizmeti sunucularından yazılı olarak da veri toplamak, topladığı verileri zamanında müdürlüğe iletmek görevi verildiği, bu durumun kişisel verilerin gizliliği hükmünü ihlal ettiği, düzenlemenin Anayasaya aykırı olduğu ileri sürülerek, 21. maddesinin 1. fıkrasının (a) bendinin, anılan düzenlemede, Adli Tıp Kurumunun doğrudan hizmet vermediği yerlerde, adli tıbbi hizmetler konusunda Cumhuriyet Savcılığı, ilçe sağlık müdürlüğü, aile hekimliği birimleri ve diğer sağlık kurum ve kuruluşları ile işbirliği içinde çalışarak bu hizmetlerin 25/1/2013 tarihli ve 28539 sayılı Resmî Gazete’de yayımlanan Aile Hekimliği Uygulama Yönetmeliği çerçevesinde yürütülmesini sağlamak görevinin toplum sağlığı merkezlerinin görevleri arasında sayıldığı, ancak, adli tabiplik hizmetlerinin koruyucu, tedavi edici sağlık hizmeti kapsamında olmadığı, bu sebeple de toplum sağlığı merkezi hekimlerine ve aile hekimlerine adli tabiplik hizmetinin yüklenmesinin Kanuna aykırılık teşkil ettiği ileri sürülerek, 22. maddesinin 1. fıkrasının (a) bendinde yer alan "buldukları ekipmanlar ölçüsünde acil sağlık hizmeti sunmak ve" ibaresinin ve (b) bendinde yer alan "uygulamak" ibaresinin, söz konusu madde ile toplum sağlığı merkezi hekimlerine acil sağlık hizmeti sunma görevi verilmiş ise de, bu hekimlerin asıl görevinin koruyucu hekimlik içeren birinci basamak sağlık hizmeti sunumu olduğu, koruyucu sağlık hizmetlerinin acil sağlık hizmetlerinden çok farklı nitelikler taşıdığı, acil sağlık hizmetlerinin niteliği gereği acil sağlık hizmeti sunacakların bu konuda eğitim alması ve deneyim sahibi olması gerektiği, hastaların gereksinim duyduğu sağlık hizmetini nitelikli bir şekilde alma haklarının ihlal edildiği ileri sürülerek, 4. maddesinin 1. fıkrasının (ö) bendinin, 26. maddesinin 1. fıkrasının (a) ve (c) bentlerinin, anılan hükümler ile toplum sağlığı merkezlerine kendilerine bağlı iş sağlığı ve güvenliği birimi kurma ve çalışan sağlığı ve güvenliği hizmetlerini verme yetkisinin düzenlendiği; kamu görevlilerinin görev

tanımları dışında çalıştırılmayacakları, başka kurum ve kuruluşlarda görevlendirmelerinin ancak yasal düzenlemelerle yapmanın mümkün olduğu; toplum sağlığı merkezlerinin kadrosunda işyeri hekimi veya iş güvenliği uzmanının bulunmadığı, dolayısıyla düzenlemenin hukuka aykırı olduğu ileri sürülerek, 30. maddesinin 2. fıkrasının, dava konusu düzenlemede, toplum sağlığı merkezlerinin nüfus hareketlerine ilişkin görevlerinin kapsamının tarım işçileri ile kısıtlanmasının hukuka aykırı olduğu ileri sürülerek, dava konusu Yönetmeliğin 21. maddesi ile atıfta bulunulan 25/01/2013 tarih ve 28539 sayılı Resmî Gazete'de yayımlanan Aile Hekimliği Uygulama Yönetmeliği'nin 10. maddesinin 5. fıkrasının, dava konusu Yönetmeliğin 21. maddesinin 1. fıkrasının (a) bendinin yollama yaptığı Aile Hekimliği Uygulama Yönetmeliğinin 10. maddesi ile gerek aile hekimlerine gerekse toplum sağlığı merkezi hekimlerine, 5258 sayılı Kanunda verilen görev kapsamını aşacak nitelikte adli tabiplik görevinin verilmesinin Kanuna aykırılık teşkil ettiği, belirtilen sebeplerle dava konusu düzenlemenin kamu yararı, hizmet gerekleri, üst hukuk normlarına ve hukuka aykırı olduğu ileri sürülerek iptali ile yine dava konusu Yönetmeliğin dayanakları arasında yer alan 5258 sayılı Aile Hekimliği Kanunu'nun 5. maddesinin 2. fıkrasındaki "Aile hekimliği hizmetleri dışında kalan birinci basamak sağlık hizmetleri toplum sağlığı merkezleri tarafından verilir ve bu merkezlerin organizasyonu, kadroları, görevleri ile çalışma usûl ve esasları nca belirlenir." düzenlemesinin, toplum sağlığı merkezinde sunulan sağlık hizmetinin, kamu görevlileri eliyle yürütülmesi sebebiyle, görev, yetki, hak ve yükümlülüklerin kanunla düzenlenmesi gerektiği halde bu alanda düzenleme yetkisinin anılan Kanun ile na bırakılmış olmasının yasama yetkisinin devri niteliğinde olduğu ve Anayasanın 2., 7., 8., 123., ve 128. maddelerine aykırılık teşkil ettiği iddiasıyla iptali için Anayasa Mahkemesine başvurulması istenilmektedir.

Savunmanın Özeti: 663 sayılı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname gereğince, temel sağlık hizmetlerini, bu kapsamda birinci basamak sağlık hizmetlerini, Bakanlık hedef ve politikalarına uygun olarak yürütmek ve bu hususta gerekli düzenlemeleri yapmak görev ve yetkisinin uhdelerinde olduğu; 3359 sayılı Sağlık Hizmetleri Temel Kanunu, 5258 sayılı Kanun'un 5. maddesi ve 663 sayılı KHK'nın 36. maddesine istinaden hazırlanan Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği ile toplum sağlığı merkezleri ve bağlı birimlerinin açılması, kapatılması, organizasyonu ve görevleriyle ilgili usul ve esasların düzenlenmiş olduğu; anılan düzenlemenin, toplum sağlığı merkezlerini güçlendirerek hizmetlerin kaliteli, etkin, verimli bir şekilde sunulmasına katkı sağlamak, aile hekimliği haricindeki birinci basamak sağlık hizmetlerinin etkinliğini artırmak, aile hekimliği hizmetlerine erişimi kolaylaştırmak, bireye yönelik birinci basamak sağlık hizmetleri ile topluma yönelik birinci basamak sağlık hizmetlerinin daha bütünleşik bir yapıda yürütülmesini sağlamak amacı taşıdığı; Yönetmelik kapsamında, Halk Sağlığı

Kurumu taşra teşkilatı hizmet birimleri arasında yer alan toplum sağlığı merkezlerine, organizasyon, eşgüdüm, eğitim ve denetim görevleriyle birlikte toplumsal sağlık hizmeti sunma görevi verildiği, böylelikle toplum sağlığı hizmetlerinin münhasıran bu hizmete yönelik görevleri olan merkezler marifetiyle layıkıyla verilebilir hale getirilmesinin hedeflendiği; bu bağlamda, toplum sağlığı merkezlerinin organizasyon, eşgüdüm, eğitim ve denetim görevleriyle birlikte toplumsal sağlık hizmeti sunma görevleri göz önüne alındığında, birinci basamak sağlık hizmetlerinin sunumu noktasında halk sağlığı müdürlüğü adına izleme ve değerlendirme çalışmalarının sekreteryasını yürütmesinde hukuka aykırılık bulunmadığı; adı geçen merkezlerin Bakanlık ve Kurum idari yapısındaki yerinin ilgili mevzuat hükümleri kapsamında belirlendiği, bu bağlamda, toplum sağlığı merkezlerinin taşra teşkilatı içerisinde halk sağlığı müdürlüğünün izdüşümü ve müdürlük yetkilerini kullanan idari birimler olduğu; dava konusu düzenlemenin üst hukuk normlarına, kamu menfaatine ve hizmet gereklerine uygun olduğu ileri sürülerek davanın reddi gerektiği savunulmaktadır.

Danıştay Tetkik Hakimi:

Düşüncesi: Dava konusu düzenlemede hizmet gereklerine, kamu yararına, üst hukuk normlarına ve hukuka aykırılık bulunmadığı, davanın reddi gerektiği düşünülmektedir.

Danıştay Savcısı:

Düşüncesi: Dava; 05.02.2015 tarih ve 29258 sayılı Resmi Gazete'de yayımlanan Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği'nin 4. maddesinin 1. fıkrasının (n) bendinde yer alan "denetleyen" ibaresinin ve (ö) bendinin, 9. maddesinin (f) bendinin, 10. maddesinin 1. fıkrasının (a) bendinin, 13. maddesinin 1. fıkrasının (c), (ç), ve (d) bentlerinin, 21. maddesinin 1. fıkrasının (a) bendinin, 22. maddesinin 1. fıkrasının (a) bendinde yer alan "buldukları ekipmanlar ölçüsünde acil sağlık hizmeti sunmak ve" ibaresinin ve (b) bendinde yer alan "uygulamak" ibaresinin, 26. maddesinin (a) ve (c) bentlerinin, 30. maddesinin 2. fıkrasının, 45. maddesinin 2. fıkrasının (d) bendinin ve bu Yönetmelik ile atıfta bulunulan 25.01.2013 tarih ve 28539 sayılı Resmi Gazete'de yayımlanan Aile Hekimliği Uygulama Yönetmeliği'nin 10. maddesinin 5. fıkrasının iptali ile yine dava konusu Yönetmeliğin dayanağı olan 5258 sayılı Aile Hekimliği Kanununun 5. maddesinin Anayasaya aykırı olduğu iddiasıyla iptali için Anayasa mahkemesine başvurulması istemiyle açılmıştır.

Davacının Anayasaya aykırılık iddiası yerinde görülmemiştir.

Davanın, 05.02.2015 tarih ve 29258 sayılı Resmi Gazete'de yayımlanan Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği'nin 4. maddesinin 1. fıkrasının (n) bendinde yer alan "denetleyen"

ibaresinin ve (ö) bendinin, 9. maddesinin (f) bendinin, 10. maddesinin 1. fıkrasının (a) bendinin, 13. maddesinin 1. fıkrasının (c), (ç), ve (d) bentlerinin, 21. maddesinin 1. fıkrasının (a) bendinin, 22. maddesinin 1. fıkrasının (a) bendinde yer alan "buldukları ekipmanlar ölçüsünde acil sağlık hizmeti sunmak ve" ibaresinin ve (b) bendinde yer alan "uygulamak" ibaresinin, 26. maddesinin (a) ve (c) bentlerinin, 30. maddesinin 2. fıkrasının, 45. maddesinin 2. fıkrasının (d) bendinin iptali istemine ilişkin kısmının incelenmesinden,

Anayasa'nın 56. maddesinin birinci fıkrasında, herkesin, sağlıklı ve dengeli bir çevrede yaşama hakkına sahip olduğu; üçüncü fıkrasında, Devletin, herkesin hayatını, beden ve ruh sağlığı içinde sürdürmesini sağlamak; insan ve madde gücünde tasarruf ve verimi artırarak, işbirliğini gerçekleştirmek amacıyla sağlık kuruluşlarını tek elden planlayıp hizmet vermesini düzenleyeceği; dördüncü fıkrasında da, Devletin, bu görevini kamu ve özel kesimlerdeki sağlık ve sosyal kurumlarından yararlanarak, onları denetleyerek yerine getireceği, 124. maddesinde, bakanlıkların kendi görev alanlarını ilgilendiren kanunların ve tüzüklerin uygulanmasını sağlamak üzere ve bunlara aykırı olmamak şartıyla yönetmelik çıkarabilecekleri hükme bağlanmıştır.

Sağlık hizmeti sunulmasına ilişkin olarak Devlete verilmiş olan görevler, 663 sayılı ve Bağlı Kuruluşların Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname gereğince nca yürütülmektedir. Anılan Kanun Hükmünde Kararname'nin; 2. maddesinin ikinci fıkrasının (a) bendinde, halk sağlığının korunması ve geliştirilmesi hastalık risklerinin azaltılması ve önlenmesi, (e) bendinde insan gücünde ve maddi kaynaklarda tasarruf sağlamak ve verimi artırmak, sağlık insan gücünün ülke sathında dengeli dağılımını sağlamak ve bütün paydaşlar arasında işbirliğini gerçekleştirmek suretiyle yurt sathında eşit, kaliteli ve verimli hizmet sunumunu sağlamak, (f) bendinde kamu ve özel tüzel kişileri ile gerçek kişiler tarafından açılacak sağlık kuruluşlarının ülke sathında planlanması ve yaygınlaştırılması ile ilgili olarak sağlık sistemini yönetmek ve politikaları belirlemek 'nın görevleri arasında sayılmış, 40. maddesinde ise, Bakanlık ve bağlı kuruluşların görev, yetki ve sorumluluk alanına giren ve önceden kanunla düzenlenmiş konularda idari düzenlemeler yapabileceği belirtilmiştir.

663 sayılı Kanun Hükmünde Kararname'nin işlem tarihinde yürürlükte bulunan Mülga 26. maddesi ile Bakanlık politika ve hedeflerine uygun olarak, temel sağlık hizmetlerini yürütmekle görevli, Bakanlığa bağlı kurulmuş, halk sağlığını korumak ve geliştirmek, sağlık için risk oluşturan faktörlerle mücadele etmek ve birinci basamak sağlık hizmetlerini yürütmek, bu hususta gerekli düzenlemeleri yapmak Kurumun görev ve yetkileri arasında sayılmıştır.

3359 sayılı Sağlık Hizmetleri Temel Kanununun; 3. maddesinin birinci fıkrasının (a) bendinde, sağlık kurum ve kuruluşlarının yurt sathında eşit, kaliteli ve verimli hizmet sunacak şekilde Sağlık ve Sosyal Yardım Bakanlığınca, diğer ilgili bakanlıkların da görüşü alınarak plânlanacağı, koordine edileceği, mali yönden destekleneceği ve geliştirileceği; (c) bendinde, bütün sağlık kurum ve kuruluşları ile sağlık personelinin ülke sathında dengeli dağılımı ve yaygınlaştırılmasının esas olduğu, sağlık kurum ve kuruluşlarının kurulması ve işletilmesinin bu esas içerisinde Sağlık ve Sosyal Yardım Bakanlığınca düzenleneceği, (e) bendinde, tesis edilecek eğitim, denetim, değerlendirme ve oto kontrol sistemi ile sağlık kuruluşlarının tespit edilen standart ve esaslar içinde hizmet vermesinin sağlanacağı, (i) bendinde, sağlık hizmetlerinin yurt çapında istenilen seviyeye ulaştırılması amacıyla; bakanlıklar seviyesinden en uçtaki hizmet birimine kadar kamu ve özel sağlık kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları arasında koordinasyon ve işbirliği yapılacağı, sağlık kurum ve kuruluşlarının coğrafik ve fonksiyonel hizmet alanlarının, verecekleri hizmetler, yönetim, hizmet ilişki ve bağlantıları gibi konularda tespit edilen esaslara uymak ve verilen görevleri yapmakla yükümlü oldukları belirtilmiştir.

Anılan Kanunun 9. maddesinin birinci fıkrasının (c) bendinde ise; bütün kamu ve özel sağlık kuruluşlarının tesis, hizmet, personel, kıstaslarının belirlenmesinin, sağlık kurum ve kuruluşlarının sınıflandırılmasının ve sınıflarının değiştirilmesinin, sağlık kuruluşlarının amaca uygun olarak teşkilatlanmalarının, sağlık hizmet zinciri oluşturulmasının, hizmet içi eğitim usul ve esasları ile sağlık kurum ve kuruluşlarının koordineli çalışma ve hizmet standartlarının tespiti ve denetimi ile bu Kanunla ilgili diğer hususların Sağlık ve Sosyal Yardım Bakanlığınca çıkarılacak yönetmelikle düzenleneceği hükme bağlanmıştır.

Diğer taraftan, 5258 sayılı Aile Hekimliği Kanununun 5. maddesinde, "Aile hekimliği uygulamasına geçilen yerlerde kişilerin aile hekimine kaydı yapılır. Bakanlıkça belirlenen süre sonunda kişiler aile hekimlerini değiştirebilirler. Her bir aile hekimi için kayıtlı kişi sayısı; asgarî 1000, azamî 4000'dir. Aralıksız iki ayı aşmayan süreyle kayıtlı kişi sayısı 1000'den az olabilir.

Aile hekimliği hizmetleri ücretsizdir; acil haller hariç, haftada kırk saatten az olmamak kaydı ile Bakanlıkça belirlenen kıstaslar çerçevesinde ilgili aile hekiminin talebi ve o yerin sağlık idaresince onaylanan çalışma saatleri içinde yerine getirilir. (Ek cümle: 10/9/2014-6552/117 md.) nca belirlenen aile sağlığı merkezlerinde çalışma saatleri dışında, aile hekimleri ve aile sağlığı elemanları ile gerektiğinde ve bağlı kuruluşları personeline nöbet görevi verilebilir. Aile hekimliği uygulamasına geçilen yerlerde acil haller ve mücbir sebepler dışında, kişi hangi sosyal güvenlik kuruluşuna tâbi olursa olsun, aile hekiminin sevki olmaksızın sağlık kurum ve kuruluşlarına müracaat edenlerden

katkı payı alınır. Alınacak katkı payı tutarı Sağlık, Maliye ve Çalışma ve Sosyal Güvenlik bakanlıklarınca müştereken belirlenir. Aile hekimliği uygulamasına geçilen yerlerde, diğer kanunların aile hekimliği hizmetleri kapsamındaki hizmetlerin sunumu ile sevk ve müracaata ilişkin hükümleri uygulanmaz. (Ek cümle:11/10/2011-KHK-663/58 md.) Aile hekimliği hizmetleri dışında kalan birinci basamak sağlık hizmetleri toplum sağlığı merkezleri tarafından verilir ve bu merkezlerin organizasyonu, kadroları, görevleri ile çalışma usûl ve esasları nca belirlenir. Yabancılar hakkında ilgili mevzuat hükümleri uygulanır." hükmü yer almıştır.

Yukarıda yer verilen mevzuat hükümlerine dayalı olarak hazırlanıp yürürlüğe konulan Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliğinin 1. maddesinde, Bu Yönetmeliğin amacının; taşra teşkilatı yapılanmasında yer alan toplum sağlığı merkezleri ve bağlı birimlerinin açılması, kapatılması, organizasyonu ve görevleri ile ilgili usul ve esasları düzenlemek olduğu, 2. maddesinde, Bu Yönetmeliğin, toplum sağlığı merkezleri ile bağlı birimlerinin fiziki ve teknik yapısını, görev ve yetkilerini, diğer kurum ve kuruluşlarla olan ilişki ve işbirliğini kapsadığı belirtilmiş; 4/(n) maddesinde; Toplum sağlığı merkezi (TSM): "Bölgesinde yaşayan toplumun sağlığını korumak ve geliştirmek maksadıyla sağlıkla ilgili risk ve sorunları belirleyen, bunlarla ilgili düzeltici ve önleyici faaliyetleri gerçekleştiren; birinci basamak koruyucu, iyileştirici ve rehabilite edici sağlık hizmetlerini koordine eden ve bu hizmetlerin etkin ve verimli bir şekilde sunulmasını izleyen, değerlendiren, denetleyen ve destekleyen; bölgesinde bulunan sağlık kuruluşları ile diğer kurum ve kuruluşlar arasındaki koordinasyonu sağlayan sağlık kuruluşunu", (ö) bendinde, "TSM İSG (İş Sağlığı ve Güvenliği) birimi: İş sağlığı ve güvenliği hizmetlerini yürütmek üzere Çalışma ve Sosyal Güvenlik Bakanlığınca yetkilendirilen toplum sağlığı merkezi bağlı birimini" ifade edeceği hükme bağlanmış; 9. maddesinde, TSM'nin idari ve mali işlere ilişkin görevleri, 10. maddesinde, TSM'nin kayıt ve istatistiğe ilişkin görevleri, 13. maddesinde, TSM'nin izleme ve değerlendirme çalışmalarına ilişkin görevleri, 21. maddesinde, TSM'nin adli tıbbi hizmetler ve ölüm kayıt hizmetlerine ilişkin görevleri, 22. maddesinde TSM'nin acil sağlık hizmetlerine ilişkin görevleri, 26. maddesinde, TSM'nin çalışan sağlığı ve güvenliği hizmetlerine ilişkin görevleri, 30. maddesinde, TSM'nin toplu yaşam alanları ve okul sağlığı hizmetlerine ilişkin görevleri ve 45. maddesinde de TSM başkanının görevleri sayılmıştır.

Davacı tarafından özetle, anılan yönetmeliğin davaya konu maddeleriyle aile hekimlerinin özlük haklarına müdahale edildiği, toplum sağlığı merkezlerinin görev ve sorumluluklarının aile hekimlerine yıkılmaya çalışıldığı, aile hekimleri üzerinde denetim yetkisi olmayan anılan merkezin denetim merkezi gibi yetkilendirildiği, anılan yönetmeliğin 5258 sayılı yasa ve yönetmelik hükümlerine aykırı düzenlemeler içerdiği ileri sürülerek istemin özeti kısmında belirtilen madde ve

ibarelerin iptali istenilmekte, davalı idare ise savunmasında, bireye yönelik, sağlık ocakları, AÇSAP merkezleri, verem savaş dispanserleri gibi kurumların sunduğu koruyucu ve tedavi edici sağlık hizmetlerinin büyük bir kısmının aile hekimlerine verildiği, topluma yönelik birinci basamak sağlık hizmetlerinin bakanlık eliyle yürütülebilmesi için yeni bir teşkilat yapılanmasına gerek duyulduğu, 5258 ve 3359 sayılı yasa ile 663 sayılı KHK'nın verdiği yetki çerçevesinde çıkarılan dava konusu yönetmelik kapsamında toplum sağlığı merkezlerine organizasyon, eşgüdüm, eğitim ve denetim görevleriyle birlikte toplumsal sağlık hizmeti sunma görevi veldiği, böylelikle toplum sağlığı hizmetlerinin münhasıran bu hizmete yönelik görevleri olan merkezler marifetiyle verilebilir hale getirildiği bu nedenle anılan düzenlemenin hukuka uygun olduğunu ileri sürmektedir.

Dava konusu yönetmelik hükümleri bir bütün olarak değerlendirildiğinde; (Mülga) taşra teşkilatı yapılanmasında yer alan toplum sağlığı merkezleri ve bağlı birimlerinin açılması, kapatılması, organizasyonu ve görevleri ile ilgili usul ve esasları düzenleyen yönetmelikle, toplum sağlığı merkezleri ile bağlı birimlerinin fiziki ve teknik yapısını, görev ve yetkilerini, diğer kurum ve kuruluşlarla olan ilişki ve işbirliğini kapsar şekilde kurallar getirilmiş; bu bağlamda, anılan merkezlerin, aile hekimlerine aşılama, ana çocuk sağlığı ve aile planlaması gibi öncelikli hizmet alanlarında, 'nın yıllık programına uygun olarak lojistik destekte bulunullması sağlanmış, bu merkezlerin, bölgesinde yürüteceği sağlık hizmetini bir bütün olarak değerlendirerek, sağlık kuruluşları ile koordinasyonu sağlamak, gerektiğinde diğer kuruluşlarla işbirliği yapmak suretiyle toplumun ve bireylerin sağlığını korumak ve sağlık düzeylerini yükseltmekten sorumlu tutulduğu, bunun için de, Toplum sağlığı merkezinin,

- " a) İdari ve mali işler,
- b) Kayıt ve istatistik,
- c) Plan ve program yapma,
- ç) Diğer kurumlarla işbirliği,
- d) İzleme ve değerlendirme çalışmaları,
- e) Bulaşıcı hastalıklar, bağışıklama ve salgın kontrolü,
- f) Tüberküloz kontrolü,
- g) Zoonotik ve vektörel hastalıkların kontrolü,
- ğ) Erken uyarı ve cevap sistemi çalışmaları,
- h) Bulaşıcı olmayan hastalıkların kontrolü,

- ı) Kadın ve üreme sağlığı hizmetleri,
- ı) Çocuk ve ergen sağlığı hizmetleri,
- j) Kanseri erken teşhis, tarama ve eğitim hizmetleri,
- k) Ruh sağlığı programlarına dair hizmetler,
- l) Ulusal programlar ile ilgili hizmetler,
- m) Adli tıbbi hizmetler ve ölüm kayıt hizmetleri,
- n) Acil sağlık hizmetleri,
- o) Kaza ve yaralanmalardan korunma hizmetleri,
- ö) Görüntüleme ve laboratuvar hizmetleri,
- p) Çevre sağlığı hizmetleri,
- r) Çalışan sağlığı ve güvenliğine dair hizmetler,
- s) Olağan dışı durumlar ve afet sağlığı hizmetleri,
- ş) Toplu yaşam alanları ve okul sağlığı hizmetleri
- t) Evde sağlık hizmetleri,
- u) Ağız ve diş sağlığı hizmetleri,
- ü) Sağlığın geliştirilmesi ve teşviki çalışmaları,
- v) Sosyal hizmet çalışmaları,
- y) Hizmet içi eğitimler,
- z) Diğer görevler." i sunmakla görevlendirilmiş olduğu anlaşılmıştır.

Buna göre, dava konusu Yönetmelikte, bölgesinde yaşayan toplumun sağlığını geliştirmeyi ve korumayı ön plana alarak sağlıkla ilgili risk ve sorunları belirleyen, bu sorunları gidermek için planlama yapan ve bu planları uygulayan, uygulatan; birinci basamak koruyucu, iyileştirici ve rehabilite edici sağlık hizmetlerini müdürlüğün sevk ve idaresinde organize eden, bu hizmetlerin verimli şekilde sunulmasını izleyen, değerlendiren ve destekleyen, bölgesinde bulunan sağlık kuruluşları ile diğer kurum ve kuruluşlar arasındaki koordinasyonu sağlamak üzere kurulan sağlık kuruluşuna toplum sağlığı merkezi denildiği, sağlık ocakları, AÇSAP merkezleri, verem savaş dispanserleri gibi kurumların sunduğu topluma yönelik koruyucu ve tedavi edici sağlık hizmetlerinin entegre yürütülmesinin toplum sağlığı açısından büyük önem taşıması nedeniyle, İlçe

sağlık idaresinin yönetiminde, merkez ilçeler dahil her ilçede en az bir adet olmak üzere toplum sağlığı merkezi oluşturulduğu, bu merkezlerin aile hekimliği uygulamasında gerekli tetkik ve tahlilleri yapmanın yanısıra, aile hekiminin görevi dışında kalan diğer temel sağlık hizmetlerini yürüteceği ve bu sayede, bireye yönelik koruyucu sağlık hizmetleri, tanı ve tedavi hizmetleri ile rehabilitasyon hizmetleri dışında kalan temel sağlık hizmetlerinin tek çatı altında toplanması suretiyle, daha etkili ve verimli hizmet sunabilmelerinin sağlanmasının amaçlandığı anlaşılmaktadır.

Bu açıklamalar çerçevesinde, 663 sayılı Kanun Hükmünde Kararname gereğince, temel sağlık hizmetlerini, bu kapsamda birinci basamak sağlık hizmetlerini, Bakanlık hedef ve politikalarına uygun olarak yürütmek ve bu hususta gerekli düzenlemeleri yapmak görev ve yetkisinin davalı Kuruma ait olduğu açık olup; bu yetki kapsamında davalı idarece, toplum sağlığı merkezlerinin güçlendirilerek sağlık hizmetlerinin daha kaliteli, etkin, verimli bir şekilde sunulmasına katkı sağlamak, aile hekimliği haricindeki birinci basamak sağlık hizmetlerinin etkinliğini artırmak, aile hekimliği hizmetlerine erişimi kolaylaştırmak, bireye yönelik birinci basamak sağlık hizmetleri ile topluma yönelik birinci basamak sağlık hizmetlerinin daha bütünleşik bir yapıda yürütülmesinin sağlamak amacıyla anılan düzenlemenin getirildiği görülmekte olup, dava konusu yönetmeliğin iptali istenilen hükümlerinde kamu yararı, hizmet gerekleri ve üst hukuk normlarına aykırılık bulunmamaktadır.

Davanın Aile Hekimliği Uygulama Yönetmeliği'nin 10. maddesinin 5. fıkrasının iptali istemine yönelik kısmına gelince,

Aile Hekimliği Kanununun 8. maddesinde, "Aile hekimi ve aile sağlığı elemanlarının çalışma usul ve esasları; çalışılan yer, kurum ve statülerine göre öncelik sıralaması; aile hekimliği uygulamasına geçiş ve nakillere ilişkin puanlama sistemi ve sayıları; aile sağlığı merkezi olarak kullanılacak yerlerde aranacak fizikî ve teknik şartlar; meslek ilkeleri; iş tanımları; performans ve hizmet kalite standartları; hasta sevk evrakı, reçete, rapor ve diğer kullanılacak belgelerin şekli ve içeriği, kayıtların tutulması ile çalışma ve denetime ilişkin usul ve esaslar, nca çıkarılacak yönetmelikle düzenlenir.

Aile hekimi ve aile sağlığı elemanlarıyla yapılacak sözleşmede yer alacak hususlar ve bu Kanunda belirlenen esaslar çerçevesinde bunlara yapılacak ödeme tutarları ile bu ücretlerden indirim oran ve şartları, sözleşmenin feshini gerektiren nedenler, Maliye Bakanlığının uygun görüşü alınarak, nın teklifi üzerine Bakanlar Kurulunca çıkarılacak yönetmelikle düzenlenir." hükmüne yer verilmiştir.

Anılan düzenlemeye dayalı olarak yürürlüğe konulan Aile hekimliği Uygulama Yönetmeliğinin 10. maddesinin iptali istenilen (5). fıkrasında, "Adli tıp kurumunun doğrudan hizmet vermediği ve hastane bulunan yerlerde yerinde ölü muayenesi dışındaki adli tıp hizmetleri hastaneler tarafından

verilir. Yerinde ölü muayenesi hizmetleri, mesai saatleri içinde toplum sağlığı merkezi hekimlerince, mesai saatleri dışında öncelikle toplum sağlığı merkezi hekimleri olmak üzere aile hekimleri ve kamu hastaneleri dışındaki diğer kamu kurum ve kuruluşlarındaki hekimlerin de dâhil edilebileceği icap nöbeti şeklinde sunulur. Hastane bulunmayan ilçe merkezleri ve entegre sağlık hizmetinin sunulduğu merkezlerde acil sağlık hizmetleri ile adli tabiplik hizmetleri; mesai saatleri içinde aile hekimleri, mesai saatleri dışında ve resmi tatil günlerinde ise ilçe merkezindeki, toplum sağlığı merkezi hekimleri, entegre sağlık hizmeti sunulan merkezlerde çalışan hekimler ve aile hekimlerinin toplamı dikkate alınarak aşağıdaki gibi icap veya aktif nöbet uygulamaları şeklinde yürütülür." hükmü yer almış olup; anılan hükümle Adli tabiplik hizmetlerinin adli tıp kurumu olan yerlerde burada görev yapan hekimlerce yapılması esas olmakla birlikte, bunun istisnası olarak bu hekimlerin bulunmadığı yer ve durumlarda bu hizmetlerin toplum sağlığı merkezi hekimleri ve aile hekimi de dahil olmak üzere diğer hekimler eliyle verilmesinin sağlandığı görülmekle anılan düzenlemede de kamu yararı hizmet gerekleri ve üst hukuk normlarına aykırılık görülmemiştir.

Açıklanan nedenlerle davanın reddi yolunda karar verilmesi gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay Onbeşinci Dairesi'nce, duruşma için taraflara önceden bildirilmiş bulunan 29/11/2017 tarihinde davacı vekili 'un geldiği, davalı 'nı temsilen Hukuk Müşaviri ... ile Hukuk Müşaviri ...'ın geldikleri, Danıştay Savcısı'nın hazır olduğu görülmekle açık duruşmaya başlandı. Taraflara usulüne uygun olarak söz verilerek dinlendikten ve Danıştay Savcısı'nın düşüncesi alındıktan sonra taraflara son kez söz verilip duruşma tamamlandı. 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'na ekli (I) sayılı cetvelde yer aldığı cihetle 659 sayılı Kanun Hükmünde Kararname'nin 2/1-ç ve 6/1 maddeleri uyarınca taraf sıfatını haiz bulunduğu davada hasım mevkiine alınan 'nun, 25/08/2017 tarih ve 30165 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 694 sayılı Kanun Hükmünde Kararname'nin 203. maddesi ile 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'na ekli (I) sayılı cetvelden çıkartılarak anılan Kanun Hükmünde Kararname'nin 185. maddesi ile Halk Sağlığı Genel Müdürlüğü adıyla 'nın hizmet birimi olarak teşkilatlandırıldığı anlaşıldığından, dosya husumetiyle ele alınıp, dosyadaki belgeler incelenerek gereği görüldü:

Dava, 05/02/2015 tarih ve 29258 sayılı Resmî Gazete'de yayımlanan Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği'nin Anayasa'ya aykırı kanun hükmüne dayanılarak çıkartıldığından hukuka aykırı olması nedeniyle tümünün, ayrıca, 4. maddesinin 1. fıkrasının (n) bendinde yer alan "denetleyen" ibaresinin ve (ö) bendinin, 9. maddesinin 1. fıkrasının (f) bendinin, 10. maddesinin 1. fıkrasının (a) bendinin, 13. maddesinin 1. fıkrasının (c), (ç), ve (d) bentlerinin, 21. maddesinin 1.

fıkrasının (a) bendinin, 22. maddesinin 1. fıkrasının (a) bendinde yer alan "buldukları ekipmanlar ölçüsünde acil sağlık hizmeti sunmak ve" ibaresinin ve (b) bendinde yer alan "uygulamak" ibaresinin, 26. maddesinin 1. fıkrasının (a) ve (c) bentlerinin, 30. maddesinin 2. fıkrasının, 45. maddesinin 2. fıkrasının (d) bendinin, dava konusu Yönetmelik ile atıfta bulunulan 25/01/2013 tarih ve 28539 sayılı Resmî Gazete'de yayımlanan Aile Hekimliği Uygulama Yönetmeliği'nin 10. maddesinin 5. fıkrasının iptali ile yine dava konusu Yönetmeliğin dayanakları arasında yer alan 5258 sayılı Aile Hekimliği Kanunu'nun 5. maddesinin 2. fıkrasındaki "Aile hekimliği hizmetleri dışında kalan birinci basamak sağlık hizmetleri toplum sağlığı merkezleri tarafından verilir ve bu merkezlerin organizasyonu, kadroları, görevleri ile çalışma usûl ve esasları nca belirlenir." düzenlemesinin Anayasanın 2., 7., 8., 123., ve 128. maddelerine aykırı olduğu iddiasıyla iptali için Anayasa Mahkemesine başvurulması istemiyle açılmıştır.

Davacı tarafın Anayasaya aykırılık iddiası yerinde görülmemiştir.

Anayasanın 56. maddesinin 1. fıkrasında, herkesin, sağlıklı ve dengeli bir çevrede yaşama hakkına sahip olduğu; 3. fıkrasında, Devletin, herkesin hayatını, beden ve ruh sağlığı içinde sürdürmesini sağlamak; insan ve madde gücünde tasarruf ve verimi artırarak, işbirliğini gerçekleştirmek amacıyla sağlık kuruluşlarını tek elden planlayıp hizmet vermesini düzenleyeceği; 4. fıkrasında da, Devletin, bu görevini kamu ve özel kesimlerdeki sağlık ve sosyal kurumlarından yararlanarak, onları denetleyerek yerine getireceği; 124. maddesinde, bakanlıkların kendi görev alanlarını ilgilendiren kanunların ve tüzüklerin uygulanmasını sağlamak üzere ve bunlara aykırı olmamak şartıyla yönetmelik çıkarabilecekleri hükme bağlanmıştır.

11/10/2011 tarihli ve 663 sayılı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 2. maddesinin 2. fıkrasının (a) bendinde, halk sağlığının korunması ve geliştirilmesi hastalık risklerinin azaltılması ve önlenmesi, (e) bendinde insan gücünde ve maddi kaynaklarda tasarruf sağlamak ve verimi artırmak, sağlık insan gücünün ülke sathında dengeli dağılımını sağlamak ve bütün paydaşlar arasında işbirliğini gerçekleştirmek suretiyle yurt sathında eşit, kaliteli ve verimli hizmet sunumunu sağlamak, (f) bendinde kamu ve özel tüzel kişileri ile gerçek kişiler tarafından açılacak sağlık kuruluşlarının ülke sathında planlanması ve yaygınlaştırılması ile ilgili olarak sağlık sistemini yönetmek ve politikaları belirlemek 'nin görevleri arasında sayılmış; 40. maddesinde de, Bakanlık ve bağlı kuruluşların görev, yetki ve sorumluluk alanına giren ve önceden kanunla düzenlenmiş konularda idari düzenlemeler yapabileceği belirtilmiştir.

Anılan Kanun Hükmünde Kararname'nin -işlem tarihinde yürürlükte bulunan- (mülga) 26. maddesi ile Bakanlık politika ve hedeflerine uygun olarak, temel sağlık hizmetlerini yürütmekle görevli,

Bakanlığa bağlı kurulmuş; halk sağlığını korumak ve geliştirmek, sağlık için risk oluşturan faktörlerle mücadele etmek; birinci basamak sağlık hizmetlerini yürütmek, bu hususta gerekli düzenlemeleri yapmak; bulaşıcı, bulaşıcı olmayan, kronik hastalıklar ve kanser ile anne, çocuk, ergen, yaşlı ve engelli gibi risk gruplarıyla ilgili olarak izleme, sürveyans, inceleme, araştırma, bağışıklama ve kontrol çalışmaları yapmak, bununla ilgili verilerin toplanmasını sağlamak, belirlenen hedefler doğrultusunda plan ve programlar hazırlamak, uygulamaya koymak, denetlenmesini sağlamak, değerlendirmek, gerekli önlemleri almak, bu konuda politika ve düzenlemelerin oluşturulması için Bakanlığa teklifte bulunmak; yaşam kalitesini yükseltecek alışkanlıkları kazandırarak toplumdaki tüm bireylerin sağlığını geliştirmek; hatalı beslenme alışkanlıkları, obezite, sigara ve benzeri zararlı maddelerin yol açtığı sağlık riskleri ve tehditleri ile mücadele etmek, bu hususları izlemek, araştırmak, veri toplanmasını sağlamak ve değerlendirmek, Kurumun görev ve yetkileri arasında sayılmıştır.

663 sayılı Kanun Hükmünde Kararname'nin 36. maddesinin 4. fıkrasında, hizmet birimlerinin görev tanımları, yetki ve sorumlulukları ile çalışma usûl ve esaslarının Bakanlıkça çıkarılacak yönetmelikle belirleneceği hususu hüküm altına alınmış; bu hükme istinaden hazırlanan ve 7/3/2012 tarihli ve 28226 sayılı Resmî Gazete'de yayımlanan Bağlı Kuruluşları Hizmet Birimlerinin Görevleri İle Çalışma Usul ve Esasları Hakkında Yönetmeliğin 15. maddesinde, "(1) Bağlı kuruluşların taşra hizmet birimlerinin görevleri, çalışma usul ve esasları, kadro standartları ve iş tanımları ile ilgili diğer hususlar Kurumlarının teklifi ve Bakan onayı ile yürürlüğe konulacak yönerge ile belirlenir." hükmüne yer verilmiş; anılan hükme dayanılarak çıkarılan Taşra Teşkilatı Hizmet Birimlerinin Görevleri, Çalışma Usul ve Esasları İle Kadro Standartları Hakkında Yönerge'nin 6. maddesinde de, taşra teşkilatının halk sağlığı müdürlükleri, toplum sağlığı merkezleri ve halk sağlığı laboratuvarlarından oluştuğu hükmü yer almıştır.

3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 9. maddesinin birinci fıkrasının (c) bendinde, bütün kamu ve özel sağlık kuruluşlarının tesis, hizmet, personel, kıstaslarının belirlenmesinin, sağlık kurum ve kuruluşlarının sınıflandırılmasının ve sınıflarının değiştirilmesinin, sağlık kuruluşlarının amaca uygun olarak teşkilatlanmalarının, sağlık hizmet zinciri oluşturulmasının, hizmet içi eğitim usul ve esasları ile sağlık kurum ve kuruluşlarının koordineli çalışma ve hizmet standartlarının tespiti ve denetimi ile bu Kanunla ilgili diğer hususların Sağlık ve Sosyal Yardım Bakanlığınca çıkarılacak yönetmelikle düzenleneceği hükme bağlanmıştır.

Diğer taraftan, 9/12/2004 tarihli ve 25665 sayılı Resmî Gazete'de yayımlanan 5258 sayılı Aile Hekimliği Kanunu'nun 2. maddesinde, "Aile hekimi, kişiye yönelik koruyucu sağlık hizmetleri ile birinci

basamak teşhis, tedavi ve rehabilite edici sağlık hizmetlerini yaş, cinsiyet ve hastalık ayrımı yapmaksızın her kişiye kapsamlı ve devamlı olarak belli bir mekânda vermekle yükümlü, gerektiği ölçüde gezici sağlık hizmeti veren ve tam gün esasına göre çalışan aile hekimliği uzmanı veya nın öngördüğü eğitimleri alan uzman tabip veya tabiptir." tanımlamasına yer verilmiştir.

Aynı Kanun'un 5. maddesinde, "Aile hekimliği uygulamasına geçilen yerlerde kişilerin aile hekimine kaydı yapılır. Bakanlıkça belirlenen süre sonunda kişiler aile hekimlerini değiştirebilirler. Her bir aile hekimi için kayıtlı kişi sayısı; asgarî 1000, azamî 4000'dir. Aralıksız iki ayı aşmayan süreyle kayıtlı kişi sayısı 1000'den az olabilir.

Aile hekimliği hizmetleri ücretsizdir; acil haller hariç, haftada kırk saatten az olmamak kaydı ile Bakanlıkça belirlenen kıstaslar çerçevesinde ilgili aile hekiminin talebi ve o yerin sağlık idaresince onaylanan çalışma saatleri içinde yerine getirilir. (Ek cümle: 10/9/2014-6552/117 md.) nca belirlenen aile sağlığı merkezlerinde çalışma saatleri dışında, aile hekimleri ve aile sağlığı elemanları ile gerektiğinde ve bağlı kuruluşları personeline nöbet görevi verilebilir. Aile hekimliği uygulamasına geçilen yerlerde acil haller ve mücbir sebepler dışında, kişi hangi sosyal güvenlik kuruluşuna tâbi olursa olsun, aile hekiminin sevki olmaksızın sağlık kurum ve kuruluşlarına müracaat edenlerden katkı payı alınır. Alınacak katkı payı tutarı Sağlık, Maliye ve Çalışma ve Sosyal Güvenlik bakanlıklarınca müştereken belirlenir. Aile hekimliği uygulamasına geçilen yerlerde, diğer kanunların aile hekimliği hizmetleri kapsamındaki hizmetlerin sunumu ile sevk ve müracaata ilişkin hükümleri uygulanmaz. (Ek cümle:11/10/2011-KHK-663/58 md.) Aile hekimliği hizmetleri dışında kalan birinci basamak sağlık hizmetleri toplum sağlığı merkezleri tarafından verilir ve bu merkezlerin organizasyonu, kadroları, görevleri ile çalışma usûl ve esasları nca belirlenir. Yabancılar hakkında ilgili mevzuat hükümleri uygulanır." hükmü yer almıştır.

Yukarıda yer verilen mevzuat hükümlerine istinaden, taşra teşkilatı yapılanmasında yer alan toplum sağlığı merkezleri ve bağlı birimlerinin açılması, kapatılması, organizasyonu ve görevleri ile ilgili usul ve esasları düzenlemek amacıyla hazırlanan Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği 05/02/2015 tarihli ve 29258 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir.

Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği'nin Anayasa'ya aykırı kanun hükmüne dayanılarak çıkartıldığından hukuka aykırı olması nedeniyle tümünün iptali istemi yönünden:

Davacı tarafından, toplum sağlığı merkezinde sunulan sağlık hizmetinin, kamu görevlileri eliyle yürütülmesi sebebiyle, görev, yetki, hak ve yükümlülüklerin kanunla düzenlenmesi gerektiği halde, dava konusu Yönetmeliğin dayanakları arasında yer alan 5258 sayılı Aile Hekimliği Kanunu'nun 5. maddesinin 2. fıkrasında yer alan "Aile hekimliği hizmetleri dışında kalan birinci basamak sağlık

hizmetleri toplum sađlıđı merkezleri tarafından verilir ve bu merkezlerin organizasyonu, kadroları, görevleri ile alıřma usul ve esasları nca belirlenir." hkm ile bu alanda dzenleme yetkisinin na bırakılmıř olmasının yasama yetkisinin devri niteliđinde olduđu; dolayısıyla, Ynetmeliđin, Anayasaya aykırı kanun hkmne dayanılarak kartıldıđından bahisle tmnn hukuka aykırı olduđu ileri srlmektedir.

Dava dosyasının incelenmesinden ve Ynetmeliđin bir btn olarak deđerlendirilmesinden, 5258 ve 3359 sayılı Kanun ile 663 sayılı Kanun Hkmnde Kararnamenin verdiđi yetki kapsamında, davalı idarece, toplum sađlıđı merkezlerinin glendirilerek sađlık hizmetlerinin kaliteli, etkin, verimli bir şekilde sunulmasına katkı sađlamak, aile hekimliđi haricindeki birinci basamak sađlık hizmetlerinin etkinliđini artırmak, aile hekimliđi hizmetlerine eriřimi kolaylařtırmak, bireye ynelik birinci basamak sađlık hizmetleri ile topluma ynelik birinci basamak sađlık hizmetlerinin daha btnleřik bir yapıda yrtlmesini sađlamak amacıyla, kamu yararı ve hizmet gerekleri gzetilerek dava konusu dzenlemenin hazırlandıđı ve yrrlđe konuduđu anlařılmakla, bu ynyle anılan dzenlemede st hukuk normlarına ve hukuka aykırılık bulunmamaktadır.

Toplum Sađlıđı Merkezi ve Bađlı Birimler Ynetmeliđi'nin 4. maddesinin 1. fıkrasının (n) bendinde yer alan "denetleyen" ibaresinin, 9. maddesinin 1. fıkrasının (f) bendinin, 13. maddesinin 1. fıkrasının (c), (), ve (d) bentlerinin, 45. maddesinin 2. fıkrasının (d) bendinin iptali istemi ynnden:

Dava konusu Ynetmeliđin "Tanımlar" bařlıklı 4. maddesinin 1. fıkrasının (n) bendinde, toplum sađlıđı merkezi; blgesinde yařayan toplumun sađlıđını korumak ve geliřtirmek maksadıyla sađlıkla ilgili risk ve sorunları belirleyen, bunlarla ilgili dzeltici ve nleyici faaliyetleri gerekleřtiren; birinci basamak koruyucu, iyileřtirici ve rehabilite edici sađlık hizmetlerini koordine eden ve bu hizmetlerin etkin ve verimli bir şekilde sunulmasını izleyen, deđerlendiren, denetleyen ve destekleyen; blgesinde bulunan sađlık kuruluřları ile diđer kurum ve kuruluřlar arasındaki koordinasyonu sađlayan sađlık kuruluřu olarak tanımlanmıřtır.

Anılan Ynetmeliđin, 9. maddesinin 1. fıkrasının (f) bendinde, aile hekimlerinin alıřma saatlerine uyumunu ve alıřmalarını izlemek ve deđerlendirmek grevi, toplum sađlıđı merkezinin grevleri arasında sayılmıřtır.

Aynı Ynetmeliđin "İzleme ve deđerlendirme alıřmaları" bařlıklı 13. maddesinin (c), () ve (d) bentlerinde, "(1) TSM'nin izleme ve deđerlendirme alıřmalarına iliřkin grevleri řunlardır:

...

c) Bölgesindeki aile hekimliği birimlerinin çalışma düzenine uyumlarını ilgili mevzuatına göre izlemek ve değerlendirmek, hazırladığı raporu müdürlüğe iletmek,

ç) Bölgesinde hizmet veren aile hekimliği birimlerinin çalışmalarını ve kayıtlarını ilgili mevzuatına göre izlemek ve değerlendirmek amacıyla aile sağlığı merkezlerini ziyaret etmek, mevzuatın izin verdiği sınırlar çerçevesinde her türlü kayıtlarına erişmek, elde ettiği verileri ve yaptığı değerlendirmeleri öncelikli olarak aile sağlığı merkezi çalışanlarına yazılı ya da sözlü olarak, ayrıca altışar aylık dönemlerde de müdürlüğe yazılı olarak ya da elektronik ortamda bildirmek, bu görevi yaparken hasta ve çalışan hakları ile kişisel mahremiyetin korunması ilkelerine riayet etmek,

d) Bölgesinde hizmet veren aile hekimliği birimlerinin gezici sağlık hizmeti planlarını bir önceki ayın son haftası içinde aile hekimlerinden almak, plana uyulup uyulmadığını izlemek ve değerlendirmek, hazırladığı raporu müdürlüğe bildirmek" hükmüne yer verilmiştir.

Dava konusu Yönetmeliğin 45. maddesinin 2. fıkrasının (d) bendinde, müdürlüğün planlamaları doğrultusunda, aile hekimliği birimlerinin vermiş oldukları hizmetlerin izlenmesini ve değerlendirilmesini gerçekleştirmek, hazırladığı raporu müdürlüğe bildirmek toplum sağlığı merkezi başkanının görevleri arasında sıralanmıştır.

Davacı tarafından, 5258 sayılı Aile Hekimliği Kanunu'na göre, kişiye yönelik koruyucu sağlık hizmetleri ile birinci basamak teşhis, tedavi ve rehabilite edici sağlık hizmetlerinin "aile hekimliği hizmetleri" olarak tanımlandığı, bunun dışında kalan birinci basamak sağlık hizmetlerinin ise toplum sağlığı merkezleri tarafından sunulması gerektiği hususunun hükme bağlandığı, ancak, dava konusu düzenlemenin bu Kanuna aykırı hükümler içerdiği; toplum sağlığı merkezlerinin görev ve sorumluluklarının aile hekimlerine yıkılmaya çalışıldığı; dava konusu Yönetmelik hükümleri ile toplum sağlığı merkezine yetkiye ihtiyaç duyulmadan denetim yapma yetkisinin verilmesinin üst hukuk normlarına aykırılık teşkil ettiği, aile hekimlerinin özlük haklarının ihlali niteliğinde olduğu ileri sürülerek iptali istenilmiştir.

Anılan düzenlemede, toplum sağlığı merkezinin, bölgesinde yaşayan toplumun sağlığını korumak ve geliştirmek maksadıyla sağlıkla ilgili risk ve sorunları belirleyen, bunlarla ilgili düzeltici ve önleyici faaliyetleri gerçekleştiren; birinci basamak koruyucu, iyileştirici ve rehabilite edici sağlık hizmetlerini koordine eden ve bu hizmetlerin etkin ve verimli bir şekilde sunulmasını izleyen, değerlendiren, denetleyen ve destekleyen; bölgesinde bulunan sağlık kuruluşları ile diğer kurum ve kuruluşlar arasındaki koordinasyonu sağlayan sağlık kuruluşu olarak tanımlandığı; adı geçen merkezlere, organizasyon, eşgüdüm, eğitim ve denetim görevleriyle birlikte toplumsal sağlık hizmeti sunma görevi verildiği; anılan merkezlerin Bakanlık ve Kurum idari yapısındaki yerinin ilgili

mevzuat hükümleri kapsamında belirlendiği, bu bağlamda, toplum sağlığı merkezlerinin taşra teşkilatı içerisinde halk sağlığı müdürlüğünün izdüşümü ve müdürlük yetkilerini kullanan idari birimler olduğu görülmekle; bu yönüyle, adı geçen merkezlerin, birinci basamak sağlık hizmetlerinin sunumu noktasında halk sağlığı müdürlüğü adına izleme ve değerlendirme çalışmalarını yürütmesine ilişkin dava konusu düzenlemelerde hizmet gerekleri ve hukuka aykırılık bulunmadığı anlaşılmaktadır.

Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği'nin 10. maddesinin 1. fıkrasının (a) bendinin iptali istemi yönünden:

Dava konusu Yönetmeliğin "Kayıt ve istatistik" başlıklı 10. maddesinin 1. fıkrasının (a) bendinde, "(1) TSM'nin kayıt ve istatistiğe ilişkin görevleri şunlardır:

a) Bakanlığın belirlemiş olduğu standartlara uygun olarak bölgedeki sağlık hizmeti sunucularından veri toplamak, yürütülen hizmetlerin kayıt ve istatistiklerini elektronik veya basılı ortamda tutmak, olağanüstü durumlarda bölgedeki sağlık hizmeti sunucularından yazılı olarak da veri toplamak, topladığı verileri zamanında müdürlüğe iletmek," hükmüne yer verilmiştir.

Dava konusu düzenleme ile toplum sağlığı merkezine, Bakanlığın belirlemiş olduğu standartlara uygun olarak bölgedeki sağlık hizmeti sunucularından veri toplamak, yürütülen hizmetlerin kayıt ve istatistiklerini elektronik veya basılı ortamda tutmak, olağanüstü durumlarda bölgedeki sağlık hizmeti sunucularından yazılı olarak da veri toplamak, topladığı verileri zamanında müdürlüğe iletmek görevi verilmiştir.

Bilindiği gibi kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır. Kişinin bedensel ya da zihinsel sağlığına ilişkin kayıt edilmiş bilgilerinin tamamından oluşan sağlık bilgileri, aralarında bireyin ırk, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, özel yaşamları ve her türlü mahkûmiyetleri ile ilgili verilerin de bulunduğu "hassas" veya " özel niteliği olan" kişisel veriler kategorisinde yer almakta olup, bu yönüyle özel bir öneme sahiptir.

Bu bağlamda Anayasa'nın 20. maddesinin üçüncü fıkrasının son cümlesinde, "Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilerek kişisel verilerin korunması hakkı anayasal güvenceye bağlanmış ve bu şekilde kamu makamlarının keyfi müdahalelerine karşı koruma altına alınmıştır.

Davacı tarafından, kişisel verilerin işleyişi ile ilgili olarak, usul ve esasların kanunla belirlenmesinin Anayasal bir zorunluluk olduğu, dava konusu Yönetmeliğin dayanağı olan 663 sayılı KHK'nın 47. maddesinin birinci, ikinci ve üçüncü fıkralarının, Anayasa Mahkemesi'nin 04/12/2014 tarih ve E:2013/114, K:2014/184 sayılı kararı ile iptal edildiği, böylece dava konusu Yönetmelik hükmünün dayanağının ortadan kalktığı, Bakanlığın kişinin yazılı onayı olmaksızın kişisel verileri ve sağlık kayıtlarını toplama yetkisinin bulunmadığı, düzenlemenin üst hukuk normlarına aykırı olduğu ileri sürülerek iptali istenilmiş; davalı idarece, Anayasa Mahkemesinin kararının verilerin paylaşılmasına ilişkin olduğu, oysa düzenlemenin, verilerin toplanması ve kayıtlarının tutulmasına yönelik olduğu; toplanan verilerin kişilerin rızasını gerektirecek nitelikte kişisel bilgi içeren veriler olmadığı, yürütülen hizmetlerin kayıt ve istatistiklerini içeren veriler olduğu, söz konusu verilerin toplumdaki prevalans (sıklık) değerlerini içerdiği, istatistikî verilerin toplanmasında hukuka aykırılık bulunmadığı savulmuştur.

Anayasa'nın 20. maddesine 5982 sayılı Kanun'un 2. maddesi ile eklenen fıkrada, "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilmiştir.

Anayasa'nın bu hükmünde kişisel verilerin korunmasını isteme hakkının neleri kapsadığı hususunun özellikle vurgulanmış olması karşısında, hassas veri kabul edilen kişisel sağlık verilerinin toplanması ve işlenmesinin kapsamı, koşulları ve bu verilerin korunmasına ilişkin usul ve esasları içermeyen yasal düzenlemelerin, Anayasa'nın 20. maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceğine ilişkin güvenceyi sağlamaktan uzak olduğu sonucuna ulaşılmıştır.

Bu kapsamda, dava konusu Yönetmelik hükmünün dayanağı 663 sayılı Kanun Hükmünde Kararname'nin 47. maddesinin 1. ve 3. fıkraları Anayasa Mahkemesi'nin 14/02/2013 tarih ve E:2011/150, K:2013/30 sayılı kararı ile iptal edilmiş, ardından 12/07/2013 tarihinde kabul edilen ve 02/08/2013 tarih ve 28726 sayılı Resmî Gazete'de yayımlanan 6495 sayılı Bazı Kanun ve Kanun

Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un 73. maddesinin (h) bendinin üçüncü alt bendi ile 663 sayılı Kanun Hükmünde Kararname'nin Anayasa Mahkemesi'nce iptal edilen hükümleri yeniden düzenlenmiştir.

Bu kez de anılan hüküm, Anayasa Mahkemesi'nin 04/12/2014 tarih ve 2013/114, 2014/184 sayılı kararıyla; dava konusu kuralla sadece demokratik toplum düzeni yönünden zorunlu olan sınırlamalar değil, özel hayatın ve kişisel verilerin korunması haklarına yapılabilecek her türlü sınırlamaya izin verilmesi, bir başka ifade ile kuralda anılan haklara sınırlama getirilirken sınırlama aracının sınırlama amacına uygun ve orantılı olarak kullanılmasını temin edecek güvencelere yer verilmemesinin ölçülülük ilkelerine aykırı düştüğü gerekçesiyle iptal edilmiştir.

Son durumda ise, 24/03/2016 tarihinde kabul edilen ve 07/04/2016 tarih ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30. maddesi ile 663 sayılı Kanun Hükmünde Kararname'nin 47. maddesi yeniden düzenlenmiştir.

Bununla birlikte anılan Kanun'un 30. maddesi ile 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 3. maddesinin (f) bendi de değiştirilmiş; buna göre, maddede, "Herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi amacıyla, ve bağlı kuruluşlarınca gerekli kayıt ve bildirim sistemi kurulur. Bu sistem, e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabilir. Bu amaçla, nca, bağlı kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemi kurulabilir." hükmüne yer verilmiştir.

Her ne kadar 663 sayılı Kanun Hükmünde Kararname'nin 47. maddesi ve 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 3. maddesinin (f) bendi yeniden düzenlemiş ise de sonradan yürürlüğe giren yasal düzenlemelerin önceden yürürlüğe giren Yönetmeliğin dayanağı olamayacağı açıktır. Bu nedenle, dava konusu maddede hukuka uyarlık bulunmamaktadır.

Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği'nin 21. maddesinin 1. fıkrasının (a) bendinin ve Aile Hekimliği Uygulama Yönetmeliği'nin 10. maddesinin 5. fıkrasının iptali istemi yönünden:

Dava konusu Yönetmeliğin, toplum sağlığı merkezinin adli tıbbi hizmetler ve ölüm kayıt hizmetlerine ilişkin görevlerinin yer aldığı 21. maddesinin 1. fıkrasının (a) bendinde, "Adli Tıp Kurumunun doğrudan hizmet vermediği yerlerde, adli tıbbi hizmetler konusunda Cumhuriyet Savcılığı, ilçe sağlık müdürlüğü, aile hekimliği birimleri ve diğer sağlık kurum ve kuruluşları ile işbirliği içinde çalışarak bu hizmetlerin 25/1/2013 tarihli ve 28539 sayılı Resmî Gazete'de yayımlanan Aile Hekimliği Uygulama Yönetmeliği çerçevesinde yürütülmesi sağlamak" hükmü düzenlenmiştir.

25/1/2013 tarihli ve 28539 sayılı Resmî Gazete'de yayımlanan Aile Hekimliği Uygulama Yönetmeliği'nin "Çalışma saatleri" başlıklı 10. maddesinin 5. fıkrasında da, "Adli tıp kurumunun doğrudan hizmet vermediği ve hastane bulunan yerlerde yerinde ölü muayenesi dışındaki adli tıp hizmetleri hastaneler tarafından verilir. Yerinde ölü muayenesi hizmetleri, mesai saatleri içinde toplum sağlığı merkezi hekimlerince, mesai saatleri dışında öncelikle toplum sağlığı merkezi hekimleri olmak üzere aile hekimleri ve kamu hastaneleri dışındaki diğer kamu kurum ve kuruluşlarındaki hekimlerin de dâhil edilebileceği icap nöbeti şeklinde sunulur. Hastane bulunmayan ilçe merkezleri ve entegre sağlık hizmetinin sunulduğu merkezlerde acil sağlık hizmetleri ile adli tabiplik hizmetleri; mesai saatleri içinde aile hekimleri, mesai saatleri dışında ve resmi tatil günlerinde ise ilçe merkezindeki, toplum sağlığı merkezi hekimleri, entegre sağlık hizmeti sunulan merkezlerde çalışan hekimler ve aile hekimlerinin toplamı dikkate alınarak aşağıdaki gibi icap veya aktif nöbet uygulamaları şeklinde yürütülür." hükmüne yer verilmiştir.

Dava konusu düzenlemede, Adli Tıp Kurumu'nun doğrudan hizmet vermediği yerlerde, adli tıbbi hizmetler konusunda Cumhuriyet Savcılığı, ilçe sağlık müdürlüğü, aile hekimliği birimleri ve diğer sağlık kurum ve kuruluşları ile işbirliği içinde çalışarak bu hizmetlerin 25/1/2013 tarihli ve 28539 sayılı Resmî Gazete'de yayımlanan Aile Hekimliği Uygulama Yönetmeliği çerçevesinde yürütülmesini sağlamak görevi toplum sağlığı merkezlerinin görevleri arasında sayılmıştır.

Davacı tarafından, 5258 sayılı Aile Hekimliği Kanunu'na göre, kişiye yönelik koruyucu sağlık hizmetleri ile birinci basamak teşhis, tedavi ve rehabilite edici sağlık hizmetlerinin "aile hekimliği hizmetleri" olarak tanımlandığı, bunun dışında kalan birinci basamak sağlık hizmetlerinin ise toplum sağlığı merkezleri tarafından sunulması gerektiği hususunun hükme bağlandığı, buna göre, adli tabiplik hizmetlerinin koruyucu, tedavi edici sağlık hizmeti kapsamında olmadığı, bu sebeple de toplum sağlığı merkezi hekimlerine adli tabiplik hizmetinin yüklenmesinin kanuna aykırılık teşkil ettiği ileri sürülerek iptali istenilmiş; davalı idarece, Ülkemizde Adli Tıp Kurumunun taşra teşkilatını tamamlayamamış olması, adli hekim sayısının yetersizliği ve hastane bulunmayan idari birimlerin mevcudiyeti dikkate alındığında, ülke genelinde yaygın sağlık hizmeti sunan Bakanlık personeli yardımı ile adli tabiplik hizmetlerinin gördürülmesinin hizmet gerekleri ve kamu yararına uygun olduğu; adli tabiplik hizmetlerinin esas olarak adli vakaların değerlendirilmesi, adli ölü muayenesi ve otopsi işlemlerinden oluştuğu, yerinde ölü muayenesi ve otopsi işlemlerinin birbirlerinden farklı işlemler olduğu, adli tıp kurumunun örgütlendiği yerde veya hastane bulunan yerlerde bu görevlerin adı geçen kuruluşlarca yapılacağı savunulmuştur.

Dava dosyasının Yönetmelik hükümleriyle birlikte değerlendirilmesinden; adli tabiplik hizmetlerinin adli tıp kurumu olan yerlerde burada görev yapan hekimlerce yapılmasının esas olduğu, bunun istisnası olarak bu hekimlerin bulunmadığı yer ve durumlarda bu hizmetlerin toplum sağlığı merkezi hekimleri ve aile hekimi de dahil olmak üzere diğer hekimler eliyle verilmesinin sağlandığı görülmekle, anılan düzenlemede kamu yararı, hizmet gerekleri ve üst hukuk normlarına aykırılık görülmemiştir.

Aile Hekimliği Uygulama Yönetmeliği'nin 10. maddesinin 5. fıkrasının iptali istemi incelendiğinde; 2577 sayılı İdari Yargılama Usulü Kanunu'nun 7. maddesinin 1. fıkrasında, dava açma süresinin, özel yasalarında ayrı süre gösterilmeyen hallerde Danıştay'da ve idare mahkemelerinde altmış gün olduğu, aynı maddenin 4. fıkrasında, ilanı gereken düzenleyici işlemlerde dava süresinin, ilan tarihini izleyen günden itibaren başlayacağı, ancak bu işlemlerin uygulanması üzerine ilgililerin, düzenleyici işlem veya uygulanan işlem yada her ikisine karşı dava açabilecekleri belirtilmiştir.

Buna göre, ilanı tarihini izleyen günden itibaren işlemeye başlayan dava açma süresi içerisinde idari davaya konu edilmeyen düzenleyici işlemlerin, bu tarihten sonra davaya konu edilebilmeleri için, ilgili hakkında uygulama işlemi yapılmış olması, bireysel işlemin ise birlikte dava konusu yapıldığı düzenleyici işlemin uygulanması niteliğinde bulunması gerekmektedir.

Bu kapsamda, Aile Hekimliği Uygulama Yönetmeliği, 25/1/2013 tarihli ve 28539 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girdiği halde, davacı tarafından, Yönetmeliğin dava konusu edilen maddesine karşı yayımlanma tarihini izleyen günden itibaren 2577 sayılı İdari Yargılama Usulü Kanunu'nun 7. maddesinin 1. fıkrası uyarınca altmış gün içinde dava açma yoluna gidilmemiş; ancak, dava açma süreleri geçirildikten sonra, davaya konu Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği'nin 21. maddesi ile atıfta bulunulduğundan bahisle 06/04/2015 tarihinde bakılan işbu davayı açmıştır.

Her ne kadar dava konusu Yönetmeliğin 21. maddesi ile atıfta bulunulduğundan bahisle Aile Hekimliği Uygulama Yönetmeliği'nin 10. maddesinin 5. fıkrasının iptali istenilmiş ise de; anılan düzenleyici işlemde atıf yapılmasının dava açma süresini yeniden ihya etmeyeceği açıktır.

Bu durumda, yürürlüğe girerek hukukî sonuçlarını doğurmuş olan Yönetmeliğin anılan maddesine karşı dava açma süresi içinde dava açmayan davacının, dava açma süresinin geçirilmesinden sonra, başka bir düzenleyici işlemde yapılan atıf sebebiyle açılan işbu davanın Aile Hekimliği Uygulama Yönetmeliği'nin 10. maddesinin 5. fıkrasına yönelik kısımlarının süre aşımı nedeniyle incelenemeyeceği sonucuna ulaşılmıştır.

Toplum Saęlıęı Merkezi ve Baęlı Birimler Yönetmelięi'nin 22. maddesinin 1. fıkrasının (a) bendinde yer alan "buldukları ekipmanlar ölçüsünde acil saęlık hizmeti sunmak ve" ibaresinin ve (b) bendinde yer alan "uygulamak" ibaresinin iptali istemi yönünden:

Dava konusu Yönetmelięin "Acil saęlık hizmetleri" başlıklı 22. maddesinde, "(1) TSM'nin acil saęlık hizmetlerine ilişkin görevleri şunlardır:

a) Görev tanımı içerisinde yer alan hizmetleri almak üzere başvuranlardan ihtiyacı olanlara, buldukları ekipmanlar ölçüsünde acil saęlık hizmeti sunmak ve bu hastaları acil saęlık komuta kontrol merkezine bildirmek,

b) Müdürlükçe entegre saęlık hizmeti sunulan yerler kapsamına alınan ilçelerde, ilgili mevzuatı doğrultusunda acil saęlık hizmetlerini planlayarak uygulamak ve uygulatmak" hükmü yer almıştır.

Bu bağlamda, acil saęlık hizmetlerinin yurt sathında eşit, ulaşılabilir, kaliteli, süratli ve verimli olarak yürütülmesini saęlamak maksadıyla, saęlık hizmeti sunan ve saęlık hizmeti ile ilgili olan bütün kurum ve kuruluşların uymakla mükellef oldukları esaslar ile bu kuruluşlar arasında koordinasyon temin edilmesine ve Bakanlık tarafından yürütülecek olan acil saęlık hizmetlerinin sevk ve idaresine dair usul ve esasları belirlemek amacıyla hazırlanan Acil Saęlık Hizmetleri Yönetmelięi 11/05/2000 tarih ve 24046 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir.

Acil Saęlık Hizmetleri Yönetmelięi'nin 4. maddesinin 1. fıkrasının (1) bendinde, acil tedavi, hastaneler ile dięer saęlık kurum ve kuruluşlarında acil tıbbî tedaviye ihtiyacı olanlara sunulan hizmetlerin bütünü olarak tanımlanmış ve anılan Yönetmelik ile acil saęlık hizmeti, temel hizmet birimleri arasında sayılmayan ve hizmet içerisinde bir görev üstlenmemiş, ancak, ilk ve acil yardıma ihtiyacı olanların müracaat edebilecekleri kamu veya özel sektöre ait saęlık kuruluşlarının bu alandaki görev ve yetkileri açıkça düzenlenmiştir.

Davacı tarafından, dava konusu madde ile toplum saęlıęı merkezi hekimlerine acil saęlık hizmeti sunma görevi verildięi, ancak, bu hekimlerin asıl görevinin koruyucu hekimlik içeren birinci basamak saęlık hizmeti sunumu olduęu, koruyucu saęlık hizmetlerinin acil saęlık hizmetlerinden çok farklı nitelikler taşıdıęı, acil saęlık hizmetlerinin nitelięi gereęi acil saęlık hizmeti sunacakların bu konuda eğitim alması ve deneyim sahibi olması gerektięi, hastaların gereksinim duyduęu saęlık hizmetini nitelikli bir şekilde alma haklarının ihlal edildięi ileri sürülerek iptali istenilmiş ise de; ilgili mevzuatta, acil tedavinin, hastaneler ile dięer saęlık kurum ve kuruluşlarında acil tıbbî tedaviye ihtiyacı olanlara sunulan hizmetlerin bir bütünü olarak tanımlandıęı; acil saęlık hizmeti gibi son derece hayati önemi haiz bir hizmetin yurt sathında eşit, ulaşılabilir, kaliteli, süratli ve verimli olarak

yürütülmesini sağlamak maksadıyla, sağlık hizmeti ile ilgili olan bütün kurum ve kuruluşların gerektiğinde acil sağlık hizmeti sunmak zorunda oldukları anlaşılmakla, dava konusu düzenlemede, kamu yararı, hizmet gerekleri ve hukuka aykırılık bulunmamıştır.

Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği'nin 4. maddesinin 1. fıkrasının (ö) bendinin ve 26. maddesinin 1. fıkrasının (a) ve (c) bentlerinin iptali istemi yönünden:

Dava konusu Yönetmeliğin "Tanımlar" başlıklı 4. maddesinin 1. fıkrasının (ö) bendinde, TSM İSG (İş Sağlığı ve Güvenliği) birimi, iş sağlığı ve güvenliği hizmetlerini yürütmek üzere Çalışma ve Sosyal Güvenlik Bakanlığınca yetkilendirilen toplum sağlığı merkezi bağlı birimi olarak tanımlanmıştır.

Anılan Yönetmeliğin "Çalışan sağlığı ve güvenliği hizmetleri" başlıklı 26. maddesinin 1. fıkrasının (a) ve (c) bentlerinde, "a) Çalışan sağlığı ve güvenliği hizmetlerini müdürlüğün eş güdümünde yürütmek,

c) Bünyesinde TSM İSG birimi bulunması durumunda iş sağlığı ve güvenliği hizmetlerini sunmak üzere müdürlükle birlikte planlama ve organizasyon yapmak, bu birimin ihtiyaçlarını ilgili mevzuata uygun olarak temin etmek" Bölgesinde bulunan sağlık kurum ve kuruluşlarında İSG konusunda yapılan çalışmaları izlemek ve değerlendirmek" kuralına yer verilmiştir.

Davacı tarafından, anılan hükümler ile toplum sağlığı merkezlerine kendilerine bağlı iş sağlığı ve güvenliği birimi kurma ve çalışan sağlığı ve güvenliği hizmetlerini verme yetkisi düzenlendiği, ancak, kamu görevlilerinin görev tanımları dışında çalıştırılmayacakları, başka kurum ve kuruluşlarda görevlendirmelerinin yasal düzenlemelerle yapmanın mümkün olduğu; toplum sağlığı merkezlerinin kadrosunda işyeri hekimi veya iş güvenliği uzmanının bulunmadığı; bünyesinde TSM İSG birimi bulunması durumunda iş sağlığı ve güvenliği hizmetlerini sunmak üzere müdürlükle birlikte planlama ve organizasyon yapmak, bu birimin ihtiyaçlarını ilgili mevzuata uygun olarak temin etmek görevinin toplum sağlığı merkezlerine verildiği, böylelikle TSM İSG birimlerinin, dışarıdan hizmet satın almasına dayanak oluşturulduğu, bu durumun hukuka ve hizmet gereklerine aykırı olduğu ileri sürülerek anılan hükmün iptali istenilmiştir.

Dosyanın incelenmesinden; Ülkemizde iş sağlığı ve güvenliği hizmetlerinin İşyeri Sağlık ve Güvenlik Birimleri (İSGB), Ortak Sağlık Güvenlik Birimleri (OSGB) ve Çalışma ve Sosyal Güvenlik Bakanlığınca yetkilendirilmiş Toplum Sağlığı Merkezi İş Sağlığı ve Güvenliği Birimleri (TSMİSG) olmak üzere üç farklı model tarafından sunulduğu, bu bağlamda, dava konusu düzenleme ile toplum sağlığı merkezinin çalışan sağlığı ve güvenliği hizmetlerine ilişkin görevleri arasında, bölgesinde bulunan sağlık kurum ve kuruluşlarında İş Sağlığı Güvenliği konusunda yapılan çalışmaları izlemek ve

değerlendirmek görevinin yer aldığı, iş sağlığı ve güvenliği hizmetlerinin ulusal boyutta Çalışma ve Sosyal Güvenlik Bakanlığı ile koordineli yürütüldüğü anlaşıldığından, dava konusu düzenlemede hukuka aykırılık görülmemiştir.

Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği'nin 30. maddesinin 2. fıkrasının iptali istemi yönünden:

Dava konusu Yönetmeliğin 30. maddesinin 2. fıkrasında, "(2) TSM'nin mevsimlik nüfus hareketlerine ilişkin görevleri şunlardır:

- a) Mevsimlik tarım işçilerine yönelik birinci basamak sağlık hizmetlerini planlamak, sunmak veya sunulmasını sağlamak ve bu hizmetleri koordine etmek,
- b) Mevsimsel tarım işçilerine sunulan sağlık hizmetlerinin kayıtlarını, Kurumun belirlediği standartlar doğrultusunda tutmak; bu kayıtları ilgili mevzuat hükümleri doğrultusunda kişinin kayıtlı olduğu aile hekimliği birimi ve TSM ile paylaşmak,
- c) Mevsimlik tarım işçilerine yönelik sağlık hizmetleri konusunda personel farkındalığı oluşturmak ve gerekli eğitimleri vermek,
- ç) Mevsimlik tarım işçilerine yönelik farkındalık eğitimleri düzenlemek,
- d) Bölgesindeki mevsimsel nüfus hareketlerini ilgili kurum ve kuruluşlarla birlikte takip etmek, görev tanımı içerisinde yer alan tedbirleri almak." kuralı yer almıştır.

Davacı tarafından, toplum sağlığı merkezlerinin nüfus hareketlerine ilişkin görevlerinin kapsamının tarım işçileri ile kısıtlanmasının hukuka aykırı olduğu, bu yönüyle düzenlemenin eksik olduğu ileri sürülmekte ise de, toplum sağlığı merkezinin tanımına ve bu merkezlerin görevleri ile ilgili olarak Yönetmeliğin bütününe bakıldığında, bu alanda eksik bir düzenlemeden bahsedilemeyeceği anlaşılmaktadır.

Bu durumda, toplum sağlığı merkezlerinin güçlendirilerek sağlık hizmetlerinin daha kaliteli, etkin, verimli bir şekilde sunulmasına katkı sağlamak, aile hekimliği haricindeki birinci basamak sağlık hizmetlerinin etkinliğini artırmak, aile hekimliği hizmetlerine erişimi kolaylaştırmak, bireye yönelik birinci basamak sağlık hizmetleri ile topluma yönelik birinci basamak sağlık hizmetlerinin daha bütünleşik bir yapıda yürütülmesini sağlamak amacıyla getirilen dava konusu düzenlemede, kamu yararı ve hizmet gereklerine, hukuka aykırılık bulunmamaktadır.

Açıklanan nedenlerle, 05/02/2015 tarih ve 29258 sayılı Resmî Gazete'de yayımlanan Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği'nin 10. maddesinin 1. fıkrasının (a) bendinin -oyçokluğuyla-

İPTALİNE, Aile Hekimliği Uygulama Yönetmeliği'nin 10. maddesinin 5. fıkrasına yönelik kısımlarının süre aşımı nedeniyle -oybirliğiyle- REDDİNE, diğer maddeler bakımından -oybirliğiyle- DAVANIN REDDİNE, dava kısmen iptal, kısmen süre ret, kısmen ret şeklinde sonuçlandığından aşağıda dökümü yapılan 372,60-TL. yargılama giderinin yarısı olan 186,30-TL.'nin davacı üzerinde bırakılmasına, geri kalan 186,30-TL.'nin davalı idareden alınarak davacıya verilmesine, Avukatlık Asgari Ücret Tarifesi uyarınca belirlenen 3.000,00-TL. avukatlık ücretinin davalıdan alınarak davacıya verilmesine, 3.000,00-TL. avukatlık ücretinin de davacıdan alınarak davalı idareye verilmesine, kararın tebliğini izleyen günden itibaren 30 (otuz) gün içinde İdari Dava Daireleri Kuruluna temyiz yoluna başvurulabileceğinin taraflara bildirilmesine 29/11/2017 tarihinde karar verildi.

Başkan

Üye

Üye

Üye

Üye

KARŞI OY

Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği'nin 10. maddesinin 1. fıkrasının (a) bendinde, "(1) TSM'nin kayıt ve istatistiğe ilişkin görevleri şunlardır:

a) Bakanlığın belirlemiş olduğu standartlara uygun olarak bölgedeki sağlık hizmeti sunucularından veri toplamak, yürütülen hizmetlerin kayıt ve istatistiklerini elektronik veya basılı ortamda tutmak, olağanüstü durumlarda bölgedeki sağlık hizmeti sunucularından yazılı olarak da veri toplamak, topladığı verileri zamanında müdürlüğe iletmek," hükmüne yer verilmiştir.

Anılan düzenleme ile toplum sağlığı merkezine, Bakanlığın belirlemiş olduğu standartlara uygun olarak bölgedeki sağlık hizmeti sunucularından veri toplamak, yürütülen hizmetlerin kayıt ve istatistiklerini elektronik veya basılı ortamda tutmak, olağanüstü durumlarda bölgedeki sağlık hizmeti sunucularından yazılı olarak da veri toplamak, topladığı verileri zamanında müdürlüğe iletmek görevi verilmiştir.

Dava konusu düzenleme tarihinde yürürlükte olan 663 sayılı Kanun Hükmünde Kararname'nin 47. maddesinde, 'nın yetki, görev ve hizmet alanına giren konularda, bütün kamu ve özel sağlık kurum ve kuruluşlarından istatistiki bilgi toplamaya yetkili olduğu hükmü yer almıştır.

Buna göre, yukarıdaki hüküm uyarınca davalı idare tarafından sadece istatistikî bilgilerin edinilmesinin amaçlandığı anlaşılmakta olup, dava konusu hükümlerde hukuka ve mevzuata aykırı bir durum bulunmamaktadır.

Açıklanan nedenlerle, dava konusu Yönetmeliğin 10. maddesinin 1. fıkrasının (a) bendinin iptali istemi yönünden davanın reddine karar verilmesi gerektiği oyuyla çoğunluk kararının bu kısmına katılmıyoruz.

Başkan Üye

Danıştay Kararı - 10. Daire (E. 2015/5219)

Danıştay Kararı - 10. D., E. 2015/5219 K. 2018/1739 T. 14.5.2018

İstemın Özeti: Ankara 8. İdare Mahkemesi'nin davanın reddi yolunda verilen 18/03/2015 tarih ve E:2013/710, K:2015/468 sayılı kararının hukuka uygun olmadığı ileri sürülerek temyizden incelenerek bozulması davacı tarafından istenilmektedir.

Savunmanın Özeti: Temyiz isteminin reddi gerektiği savunulmaktadır.

Danıştay Tetkik Hakimi: K1

Düşüncesi: İdare Mahkemesi kararının bozulması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Hüküm veren Danıştay Onuncu Dairesi'nce gereği görüldü:

Dava; Ankara 11. İcra Müdürü olarak görev yapmakta olan davacının, hiçbir mahkeme ve müdürlükte uygulanmadığı ileri sürülerek sadece icra dairelerinde uygulanan kamera takip sisteminin ve makam odasının kamera ile izlenmesi uygulamasının kaldırılması talebiyle 12/02/2013 tarihinde Ankara Cumhuriyet Başsavcılığına yaptığı başvurunun cevap verilmemek suretiyle zımnen reddine ilişkin işlemin iptali istemiyle açılmıştır.

Ankara 8. İdare Mahkemesi'nce; icra dairelerinde kamera sistemi uygulaması ile icra dairelerindeki çalışanların, avukatların ve tarafların daha güvenli bir ortamda çalışması ve hizmet alması ile kendilerine yapılması olası şiddet eylemlerinin faillerinin tespit edilebilmesine yönelik kamera konulduğu, bu durumun özel hayatın gizliliğini ihlal etmediği ve davalı idarenin kamu yararı ve hizmet gerekleri doğrultusunda hareket ettiği sonucuna ulaşıldığı, kamera sisteminin kaldırılması yönünde yapılan başvurunun reddine ilişkin dava konusu işlemde hukuka aykırılık bulunmadığı gerekçeleriyle davanın reddine karar verilmiştir.

Davacı tarafından, yapılan uygulamanın ve tesis edilen işlemin özel hayatının gizliliğini ihlal ettiği ve bu nedenle hukuka aykırı olduğu ileri sürülerek İdare Mahkemesi kararının temyizden incelenerek bozulması istenilmektedir.

Davacının temyiz gerekçesi olarak özel hayatın gizliliği ve mahremiyet hakkını ileri sürmüş olması dikkate alındığında, davanın incelenmesinde öncelikle özel hayat kavramının mahkeme kararları da

dikkate alınarak Anayasal ve yasal açıdan değerlendirilmesi ve bu hakkın sınırlarını da ortaya koyacak şekilde çerçevesinin çizilmesi gerekmektedir.

Anayasa Mahkemesinin özel hayatın gizliliği ve mahremiyet hakkını dikkate alarak vermiş olduğu Başvuru No:2014/12591, Başvuru No:2014/11218, Başvuru No:2016/431 gibi bir çok farklı kararında şu tespitler yer almıştır.

Özel hayat kavramı eksiksiz bir tanımı bulunmayan geniş bir kavramdır. Bu kapsamda korunan hukuki değer esasen kişisel bağımsızlıktır. Özel hayata saygı hakkının kapsamının belirlenmesinde "bireyin kişiliğini geliştirmesi ve gerçekleştirilmesi" kavramı temel alınmaktadır. Anılan hak, herkesin istenmeyen bütün müdahalelerden uzak kendine özel bir ortamda yaşama hakkına sahip olduğuna işaret etmekle birlikte, kişiliğin serbestçe geliştirilmesiyle uyumlu birçok hukuki menfaati de içermektedir.(Serap Tortuk, B. No: 2013/9660, 21/1/2015, §§ 31-36; Bülent Polat [GK], B. No: 2013/7666, 10/12/2015, §§ 61-63; Tefik Türkmen [GK], B. No: 2013/9704, 3/3/2016, §§ 50-52; Ata Türkeri, B. No: 2013/6057, 16/12/2015, §§ 30-32).

Özel hayata saygı hakkı kapsamında korunan hukuksal çıkarılardan biri de bireyin mahremiyet hakkıdır. Özel hayata saygı hakkı, ilişki kurmak ve geliştirmek üzere çevresinde bulunanlarla temas kurma hakkını da içermektedir. Kişilerin mesleki hayatı özel hayatlarıyla sıkı bir irtibat içindedir. Özel hayata dair hususlar kişinin mesleği ile ilgili tasarruflara esas alınmışsa özel hayata saygı hakkı gündeme gelecektir. (Bülent Polat, § 62; Ata Türkeri, § 31).

Gelişen teknolojinin, kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması amacıyla, kamu kesiminde kullanılmaya başlanması doğaldır. Ancak; teknoloji kullanılarak kişisel görüntülerin kayıt altına alınmasında özel hayatın gizliliği ve kişilerin mahremiyet hakkı da dikkate alınarak uygulama yapılması gerektiğinde kuşku ve duraksamaya yer bulunmamaktadır.

Buna ek olarak, kamu çalışanlarının faaliyet yürüttüğü servislerde çalışanların çalışma alanlarını ve dolayısıyla çalışanları görece şekilde yerleştirilen, güvenlik ve suçun önlenmesi gibi nedenlerle uygulandığı ileri sürülen kameralı takip sistemleri kullanılarak kişisel görüntülerin alınması, temel hak ve hürriyetler içerisinde sayılan özel hayatın gizliliği ilkesi kapsamında özel hayata müdahale olarak ele alınmalı, bu müdahalenin hukuka uygunluğunun değerlendirilmesi ise kanunilik, ölçülülük gibi anayasal kavramlar yanında Avrupa İnsan Hakları Mahkemesi kararları ve Anayasa Mahkemesi kararları dikkate alınarak yapılmalıdır.

Yukarıda anılan müdahale, Anayasa'nın 13. maddesinde belirtilen koşulları yerine getirmediği müddetçe aynı zamanda Anayasa'nın 20. maddesinin ihlalini de teşkil edecektir.

Anayasa'mızın 13. maddesi "Temel hak ve hürriyetler, ... yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, ... demokratik toplum düzeninin... gereklerine ve ölçülülük ilkesine aykırı olamaz. " şeklindedir.

Bu sebeple müdahalenin ihlal oluşturup oluşturmadığının belirlenmesinde, Anayasa'nın 13. maddesinde öngörülen ve somut başvuruya uygun düşen kanunlar tarafından öngörülme, Anayasa'nın ilgili maddesinde belirtilen nedenlere dayanma, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmama koşulları yönünden inceleme yapılması gerekir.

Anayasa'nın 13. maddesi, temel hak ve özgürlüklerin sınırlandırılmasını, ilgili hak ve özgürlüğe ilişkin Anayasa maddesinde gösterilen özel sınırlandırma sebeplerinin bulunmasına bağlı kılmıştır. Bununla birlikte Anayasa Mahkemesinin kararlarına göre, özel sınırlama nedeni öngörülmemiş olan hakların dahi, hakkın doğasından kaynaklanan bazı sınırları bulunmaktadır. Ayrıca Anayasa'nın diğer maddelerinde yer alan kurallara dayanılarak da bu hakların sınırlanması mümkün olabilmektedir. Buna göre, Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebileceği kabul edilmektedir (AYM, E.2014/87, K.2015/112).

Anayasa'nın 20. maddesi "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kağıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakimın onayına sunulur. Hakim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar." hükmünü haizdir.

Anayasa'nın 20. maddesinin birinci fıkrası yönünden özel sınırlama nedeni düzenlenmemiştir. Maddenin ikinci fıkrasında, birtakım sınırlama sebeplerine yer verilmiş olmakla beraber bu sebepler sadece arama ve elkoyma tedbirlerine yöneliktir. Dolayısıyla bu sebeplerin özel hayata saygı hakkının tüm boyutları yönünden uygulanması mümkün görünmemektedir.

Bu durumda, Anayasa'nın diğer maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin somut olay bakımından sınırlandırma sebebi olarak kabul edilip edilemeyeceği araştırılmalıdır.

Anayasa'nın 5. maddesinde, "Devletin temel amaç ve görevleri, Türk Milletinin bağımsızlığını ve bütünlüğünü, ülkenin bölünmezliğini, Cumhuriyeti ve demokrasiyi korumak, kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak; kişinin temel hak ve hürriyetlerini, sosyal hukuk devleti ve adalet ilkeleriyle bağdaşmayacak surette sınırlayan siyasal, ekonomik ve sosyal engelleri kaldırmaya, insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmaktır. " denilmektedir. Buna göre kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak devletin temel amaç ve görevlerindedir.

Kişinin ve toplumun refah, huzur ve mutluluğunu sağlamanın ön koşulu milli güvenlik ve kamu düzeninin tesisidir. Milli güvenlik ve kamu düzeninin sağlanmadığı bir ortamda, hak ve özgürlüklerden gereği gibi yararlanılması, kişinin maddi ve manevi varlığını geliştirmesi mümkün değildir. Devletin hak ve özgürlükleri koruma ödevinin yanında, milli güvenliği ve kamu düzenini sağlama görevi de bulunmaktadır.

Yukarıda ifade edilen sınırlama nedenleri de dikkate alındığında uyumsuzluğun sağlıklı çözümü için; sınırlandırmanın, "demokratik toplum düzeninin gereklerinden olması" ve "ölçülülük ilkesine uygun olması"nın ne anlama geldiğinin de ortaya konması gerekmektedir.

"Demokratik toplum düzeninin gereklerinden olma, bir sınırlamanın demokratik bir toplumda zorlayıcı bir toplumsal ihtiyacın karşılanması amacına yönelik olmasını ifade etmektedir. Buna göre sınırlayıcı tedbir, bir toplumsal ihtiyacı karşılamıyorsa ya da başvurulabilecek son çare niteliğinde değilse demokratik toplum düzeninin gereklerine uygun bir tedbir olarak değerlendirilemez. (AYM, E.2015/96, K.2016/9, 10/2/2016 § 13; ifade özgürlüğü bağlamında Bekir Coşkun [GK], B. No: 2014/12151, 4/6/2015, § 51; özel hayatın gizliliği hakkı bağlamında Ata Türkeri, § 44;İ.FA., B. No: 2013/8564, 17/2/2016, § 62).

Bu kapsamda kamu makamlarının faaliyetin niteliği ve sınırlamanın amacına göre değişen geniş bir takdir yetkisinin bulunması doğaldır. Ancak özel hayatın gizliliği hakkının mahremiyet hakkı gibi en gizli yönleri söz konusu olduğunda kamu makamlarının takdir yetkisi daha dardır ve bu alanlara yönelik müdahalelerin haklı olduğunun kabul edilebilmesi için kamu makamlarınca özellikle ciddi gerekçelerin gösterilmesi gerekir. (Ata Türkeri, § 47).

Kamu makamlarının özel hayata müdahaleleriyle ilgili olarak, müdahaleye yol açan karar alma sürecinde de keyfi davranmadıklarını kanıtlamaları gereklidir. Ancak bu halde de sınırlandırmanın ölçülülük ilkesine uygun olması gereklidir. (Ata Türkeri, § 48).

Anayasa Mahkemesi kararları uyarınca ölçülülük ilkesi, sınırlayıcı önlemin öngörülen amaç için zorunlu ve amaca ulaşmaya elverişli olmasını ayrıca amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder. Ölçülülük ilkesinin amacı da temel hak ve özgürlüklerin gereğinden fazla sınırlandırılmasının önlenmesidir (AYM, E.2015/102, K.2016/151, 7/9/2016, § 22; E.2012/100, K.2013/84, 4/7/2013; Marcus Frank Cerny, B. No: 2013/5126, 2/7/2015, § 72).

Avrupa İnsan Hakları Sözleşmesi'nin "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesi şöyledir: "(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. (2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir. "

Kamu makamlarının özel hayata saygı hakkına keyfi bir şekilde müdahale etmelerinin önlenmesi, Sözleşme'nin 8. maddesi ile sağlanan güvenceler kapsamında yer almaktadır. Avrupa İnsan Hakları Mahkemesi (AİHM), devletin özel hayata saygı hakkı kapsamında bulunan bir menfaate müdahale ettiğini tespit ettiğinde, 8. maddenin ikinci fıkrasında belirtilen koşulları incelemektedir. Buna göre kamu makamlarının müdahalesinin yasal bir dayanağı olup olmadığı, anılan fıkrada yer alan meşru amaçlara dayalı olup olmadığı, demokratik bir toplumda gerekli ve öngörülen amaçla orantılı olup olmadığı araştırılmaktadır.(AİHM Dudgeon/Birleşik Krallık, § 43; Olsson/İsveç No.1, B. No: 10465/83, 24/3/1988, § 59)

Ayrıca, AİHM kararlarına göre Sözleşme'nin 8. maddesi açıkça usul şartları içermemekle birlikte anılan maddeyle güvence altına alınan haklardan etkili bir şekilde yararlanılabilmesi için müdahaleyi doğuran karar alma sürecinin bu maddeyle korunan hak ve özgürlüklere gerekli saygıyı sağlayacak nitelikte ve adil olması gerekir. Bu şekildeki bir süreç başvurusunun 8. maddedeki haklarını -deliller ve kanıtlama konuları dahil- adil şartlarda savunabileceği usule ilişkin etkili güvencelerden yararlandırılmasını gerektirir. AİHM'e göre bu şekildeki güvencelerin amacı 8. maddede yer alan haklara keyfi şekilde müdahalede bulunulmasını önlemek, müdahalenin gerekçelendirilmesini sağlamaktır (AİHM Ciubotaru/Moldova, B. No: 27138/04, 27/4/2010, § 51; T.P. ve K.M./Birleşik Krallık, B. No: 28945/95, 10/5/2001, § 72).

AİHM'e göre gerek negatif yükümlülükler gerekse pozitif yükümlülükler bakımından söz konusu usule ilişkin etkili güvencelerin sunulması gerekmektedir. (Benzer yöndeki AİHM kararı için bkz. Hokkanen/Finlandiya, B.No: 19823/92, 23/9/1994, §§ 55-58; Glaser/Birleşik Krallık, B. No: 32346/96,

19/9/2000, §§ 63-66; Bajrami/Arnavutluk, B. No: 35853/04, 12/12/2006, §§ 50-55; Abdulaziz, Cabales ve Balkandali/Birleşik Krallık, B. No: 9214/80, 28/5/1985, § 67).

Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesinin "Mahremiyet Hakkı" başlıklı 17. maddesinde de, hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemeyeceği; onuru veya itibarının hukuka aykırı saldırılara maruz bırakılmayacağına, herkesin bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahip olduğu belirtilmiştir.

Avrupa İnsan Hakları Mahkemesinin Antovic ve Mirkovic v. Sırbistan ve Karadağ (Başvuru No. 70838/13) kararında, çalıştıkları anfi alanlarına demirbaş ve öğrenciler de dahil kişi güvenliğinin sağlanması amacıyla kamera sistemi kurulan iki profesörün özel hayatlarının gizliliğinin ihlal edildiğine karar vermiştir. Kararda özellikle Avrupa İnsan Hakları Mahkemesinin daha öncede benzer konularda vermiş olduğu kararlara atıfta bulunularak bazı tespitlere de yer verilmiştir.

Bu tespitler arasında özellikle kişilerin iş yerinde ve çalışma ortamında yani kamusal bir alanda bulunsa da, özel hayatın profesyonel aktiviteler ve dış dünya ile ilişkileri de kapsayan ve Avrupa İnsan Hakları Mahkemesinin "sosyal özel hayat" olarak adlandırdığı bir alanı da kapsadığı ve bu alanın da korunması gerektiği, kamera sistemleri ile kişilerin sosyal özel hayatlarının izlenmesinin "ciddi bir müdahale" olarak kabul edilmesi gerektiği, kişilerin güvenliği veya işverenin hakları başka yollarla korunamıyorsa ancak son çare olarak kamera sistemlerinin kişilerin çalışma alanlarını görecekte kurulmasının kabul edilebilir olacağı tespitlerine yer verilmiştir. Yine Avrupa İnsan Hakları Mahkemesinin Lopez Ribalba ve Ötekiler v. İspanya (Başvuru No. 1874/13) kararında da iş verenin başka yollarla korunabilecek haklarını kamera sistemi yoluyla korumasının son çare olduğu, bu durumda bile kamera sistemleri ile ilgili olarak bildirimde bulunması ve usulleri belirlemesi gerektiği vurgulanmıştır.

Yine yukarıda yer verilen kararlardan, farklı güvenlik önlemleri yoluyla korunabilecek haklar veya önenebilecek olaylara yönelik olarak kamera sistemleri kurulmaması gerekeceği ve çalışanların doğrudan çalışma alanlarını görüntüleme şeklinde kişilerin özel hayatına müdahale anlamına gelen bu sistemlerin bu durumlarda kullanılmaması gerekeceği, aksinin ölçülülük ilkesine aykırı olacağı sonucuna ulaşılmaktadır.

Avrupa İnsan Hakları Mahkemesi kararlarında yukarıda ifade edilen Antovic ve Mirkovic v. Sırbistan ve Karadağ (Başvuru No. 70838/13) kararında da yer aldığı gibi kamera sistemleri ile ilgili olarak belli başlı şartların ortaya konulması gerektiği de ifade edilmiştir. Bunlar özellikle uygulamanın kanuni

bir dayanağı olması, sınırlı bir izleme olması ve kötüye kullanmaya karşı garantiler olması gerektiğidir.

Türk Ceza Kanunu'nun "Özel hayatın gizliliğini ihlal" başlıklı 134. maddesi "Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.", "Kişisel verilerin kaydedilmesi" başlıklı 135. maddesi ise "Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir." hükmü yer almaktadır.

Ceza Muhakemesi Kanunu'nun "İletişimin tespiti, dinlenmesi ve kayda alınması" başlıklı 135. maddesi düzenlemesi de "başka suretle delil elde edilmesi imkânının bulunmaması durumunda" iletişimin kayda alınabileceğini, "Teknik araçlarla izleme" başlıklı 140. maddesi ise "başka suretle delil elde edilememesi hâlinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyeri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabilir" hükmü yer almakta olup, bu düzenlemeler de suça yönelik kuvvetli şüphe halinde bile en son çare olarak ses ve görüntü kaydına başvurulması gerektiğini ortaya koymaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanunu, 07.04.2016 tarihli ve 29677 Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Dava konusu işlem tarihinde yürürlükte bulunmamakla beraber konunun önemine binaen, dava konusu edilen kamera sistemleri ile ilgili belli başlı düzenlemelere de yer vermiştir. Neden bu sistemine ihtiyaç duyulduğunun ortaya konulması, sistemden kimin veya kimlerin yasal olarak sorumlu olduğunun belirlenmesi, sisteminin maksada uygun olup olmadığının ortaya konulması, özel hayatın gizliliğinin ihlal edilip edilmediğini kimin kontrol edeceğinin ve görüntülere kimin ulaşımı olacağına belirlenmesi ve bu hususların olarak kayıt altına alınması, kayıtlarının güvenliğinin ve gizliliğinin sağlanması güvenlik prosedürleri hazırlanması, kameralarla gözlemlenen bölgelerin girişinde ve içerideki uygun yerlerde bölgenin kamera sistemleri tarafından gözetlendiği ve kayıt altına alındığının belirtilmesi gerektiği, sistemin kuruluş maksadıyla bağdaşmayan görüntülerin gereğinden uzun süre saklanmaması, kişilerin özel hayatın gizliliğinin sağlanması yönünde beklentisinin olabileceği görüntülerin yetkili kişiler haricinde hiç kimse tarafından izlenememesi için alınacak önlemler gibi bir çok konuda düzenleme getirilmiştir.

Tüm bu açıklamalar ışığında dava konusu işlem incelendiğinde, Avrupa İnsan Hakları Mahkemesi kararları da dikkate alındığında hakların korunması başka şekilde sağlanamıyorsa kamera sistemlerinin çalışanların çalışma alanlarını görecektir şekilde kurulmasının mümkün olduğu ancak bunun bir son çare olarak değerlendirildiği ve bu düzenlemenin içeriğini ayrıntılı olarak ortaya koyan bir özel düzenleyici işlem olması gerektiği, kamera sistemlerinin çalışma alanlarını çekmesinin özel

hayatın gizliliğini ihlal ettiği, sınırlı bir izleme sağlayacak şekilde güvenlik amacıyla giriş ve çıkışları izlemek üzere veya vatandaşlara da açık olan ortak alanlar ve iş sahiplerinin de giriş çıkışına açık, yoğun bir alış veriş trafiği olan alanlarda kurulabileceği ancak bu kameraların da çalışanların iş yapış şekillerini denetlemek veya sürekli olarak belli kişileri çekecek şekilde kurulmaması gerektiği, güvenlik amacıyla kurulmuş olmaları gerektiği ve bu nedenle amaca hizmet eder şekilde konumlandırılması gerektiği anlaşılmaktadır.

Yine kamera sistemlerinin zorunlu güvenlik amacı ile ve başka bir yolla bu güvenlik amacı sağlanamıyorsa kurulabilmesi mümkün olsa da, yukarıda yer verilen açıklamalar ışığında uygulamanın usul ve esaslarını gösteren yasal dayanağının bulunması, açık ve anlaşılabilir olması ve ilgililerin bu konudaki hakları ve kamera sistemi ile ilgili olarak bilgilendirilmiş olması gerektiği, toplanan görüntülerle ilgili güvencelerin sağlanması gerektiği, dava konusu işlemin bu haliyle sınırları belirlenmemiş, yasal dayanağı olmayan, uygulamaya dair usul ve esaslar ile güvenceleri düzenlenmemiş bir sistemle yürütüldüğü ve bu haliyle kamu yararına yönelik olduğunu kabul etmeye imkan olmadığı; Anayasal bir ilke olan ölçülülük ilkesine aykırılık teşkil ettiği ve mahremiyet hakkını ihlal ettiği anlaşılmakta olup, kişilik haklarına aykırı şekilde kamu görevlilerinin tüm faaliyetlerinin izlenmesine imkan tanıyan uygulamada isabet bulunmamaktadır.

Kameralı takip sistemi ile kurumca amaçlanan kamu yararı arasında orantılılık bulunmadığından uygulama ölçülülük ilkesine de aykırılık teşkil etmektedir. Anayasa'nın 13. maddesinde, temel hak ve hürriyetlerin ancak kanunla sınırlanabileceği, değişik 20/3. maddesinde de, kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceğinin belirtildiği, ancak konuyla ilgili dava konusu işlemin gerçekleştirildiği aşamada yasal bir düzenlemenin yapılmadığı anlaşılmaktadır.

İdarelerin teknolojik gelişmelerden de yararlanarak kamu çalışanlarının faaliyet yürüttüğü alanda güvenlik ve suçun önlenmesi amacıyla kameralı takip sistemi uygulaması, güvenlik amacı ile giriş ve çıkışlar gibi alanlar dışında kameraların çalışanların çalışma odalarını ve servisleri çekecek şekilde yerleştirildiği durumlarda, kamusal alanda da olsa "özel hayatın gizliliği" ilkesi kapsamında bulunduğu Avrupa İnsan Hakları Mahkemesi kararları ve Dairemizin daha önceki tarihli kararlarından anlaşılmaktadır. Yine uygulamanın sınırlarını, usul ve esaslarını gösteren bir yasal dayanağın bulunması, toplanan görüntülerin ileride başka bir şekilde kullanılmayacağına dair bir güvencenin mevcut olması gerektiği de anlaşılmaktadır.

İdarenin güvenlik ve kamu yararını sağlama ihtiyacı ve çalışanların özel hayatın gizliliği gibi haklarının karşı karşıya geldiği bu gibi uyumsuzluklarda, olayın dosyaya özel olarak ele alınması ve değerlendirilmesi gerektiği açıktır.

Uyumsuzluğun bu davaya özgü hali değerlendirildiğinde; dosyada yer alan fotoğraflardan kamera sisteminin yerleştirildiği konum ve çektiği alan dikkate alındığında, iş yerinin güvenliğini sağlama amacını aşarak, doğrudan çalışan memurun kendisinin, diğer memurlarla ya da iş sahipleriyle ilişkisinin ve kamu hizmetinin görülmesi sırasında yaptığı her türlü haberleşmesinin, çalışma alanı ve masasının gözlemlendiği kamera takip sistemi kurulmasının özel hayatın gizliliğini ihlal ettiği anlaşılmakta olup; uygulamanın sınırlarını, usul ve esaslarını gösteren bir yasal dayanağın bulunmaması, toplanan görüntülerin ileride başka bir şekilde kullanılmayacağına dair bir güvencenin mevcut olmaması ve bu haliyle yukarıda belirtilen temel haklar ve Anayasal ilkelerle bağdaşmaması nedeniyle dava konusu işlemin iptaline karar verilmesi gerekirken davanın reddi yolunda verilen mahkeme kararının hukuka aykırı olduğu sonucuna varılmıştır.

Açıklanan nedenlerle, temyiz isteminin kabulüyle, Ankara 8. İdare Mahkemesi'nin 18/03/2015 tarih ve E:2013/710, K:2015/468 sayılı kararının BOZULMASINA, yeniden bir karar verilmek üzere dosyanın adı geçen mahkemeye gönderilmesine, 2577 sayılı Kanun'un (Geçici 8. maddesi uyarınca uygulanmasına devam edilen) 54. maddesinin 1. fıkrası uyarınca bu kararın tebliğ tarihini izleyen günden itibaren onbeş gün içinde karar düzeltme yolu açık olmak üzere, 14/05/2018 tarihinde oybirliğiyle karar verildi.

Danıştay Kararı - 10. Daire (E. 2015/3902)

Danıştay Kararı - 10. D., E. 2015/3902 K. 2018/1738 T. 14.5.2018

İstem Özet: Edirne İdare Mahkemesi'nin davanın reddine ilişkin 30/04/2015 tarih ve E:2014/646, K:2015/574 sayılı kararının, hukuka uygun olmadığı ileri sürülerek temyizen incelenerek bozulması istenilmektedir.

Savunmanın Özeti: Savunma verilmemiştir.

Danıştay Tetkik Hakimi: K1

Düşüncesi: İdare Mahkemesi kararının bozulması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Hüküm veren Danıştay Onuncu Dairesi'nce gereği görüldü:

Dava, davacı sendika tarafından, İpsala Kaymakamlığı Gümrük Saymanlık Müdürlüğü'ne bağlı vezne servislerinde görev yapan personelin takip edilmesi amacıyla veznelere kamera yerleştirilmesi ve personelin kayıt altına alınması uygulamasına son verilmesi talebiyle yapılan başvurunun reddine ilişkin İpsala Kaymakamlığı Gümrük Saymanlık Müdürlüğü'nün 09/04/2014 tarih ve 156 sayılı işleminin iptali istemiyle açılmıştır.

Edirne İdare Mahkemesince; İpsala Kaymakamlığı Gümrük Saymanlık Müdürlüğü'ne bağlı veznelere, personelin görevli olduğu alanın "vatandaş ile iletişim içerisinde olunan kısmının" kamera alanında olacak biçimde kamera yerleştirildiği, veznelerde yapılan işin niteliği ve önemi de dikkate alındığında, vezne işinin gereği olan para alış verişinin görüntülenmesi ve verilen paranın miktarı ile para üstünün sağlıklı olarak tespit edilerek ileride ortaya çıkacak kargaşanın önlenmesi amacıyla gerek personelin gerekse de vatandaşın huzur ve güvenliğinin sağlanması kapsamında ve personelin görevli olduğu alanın sadece para alışverişinin yapıldığı kısmı görüntüleyecek şekilde kamera yerleştirilmesi uygulamasının, idarenin, 5442 sayılı İl idaresi Kanununun 11/C madesinde belirtilen yetkisi dahilinde yapıldığı, kamu yararı ve hizmet gereklerine uygun olduğu, yapılan işlemde hukuka ve mevzuata aykırılık bulunmadığı gerekçeleriyle davanın reddine karar verilmiştir.

Davacı sendika tarafından, yapılan uygulamanın ve tesis edilen işlemin çalışanların özel hayatının gizliliğini ihlal ettiği ve bu nedenle hukuka aykırı olduğu ileri sürülerek İdare Mahkemesi kararının temyizen incelenerek bozulması istenilmektedir.

Davacı sendikanın temyiz gerekçesi olarak özel hayatın gizliliği ve mahremiyet hakkını ileri sürmüş olması dikkate alındığında, davanın incelenmesinde öncelikle özel hayat kavramının mahkeme kararları da dikkate alınarak Anayasal ve yasal açıdan değerlendirilmesi ve bu hakkın sınırlarını da ortaya koyacak şekilde çerçevesinin çizilmesi gerekmektedir.

Anayasa Mahkemesinin özel hayatın gizliliği ve mahremiyet hakkını dikkate alarak vermiş olduğu Başvuru No:2014/12591, Başvuru No:2014/11218, Başvuru No:2016/431 gibi bir çok farklı kararında şu tespitler yer almıştır.

Özel hayat kavramı eksiksiz bir tanımı bulunmayan geniş bir kavramdır. Bu kapsamda korunan hukuki değer esasen kişisel bağımsızlıktır. Özel hayata saygı hakkının kapsamının belirlenmesinde "bireyin kişiliğini geliştirmesi ve gerçekleştirilmesi" kavramı temel alınmaktadır. Anılan hak, herkesin istenmeyen bütün müdahalelerden uzak kendine özel bir ortamda yaşama hakkına sahip olduğuna işaret etmekle birlikte, kişiliğin serbestçe geliştirilmesiyle uyumlu birçok hukuki menfaati de içermektedir.(Serap Tortuk, B. No: 2013/9660, 21/1/2015, §§ 31-36; Bülent Polat [GK], B. No: 2013/7666, 10/12/2015, §§ 61-63; Tefvik Türkmen [GK], B. No: 2013/9704, 3/3/2016, §§ 50-52; Ata Türkeri, B. No: 2013/6057, 16/12/2015, §§ 30-32).

Özel hayata saygı hakkı kapsamında korunan hukuksal çıkarlardan biri de bireyin mahremiyet hakkıdır. Özel hayata saygı hakkı, ilişki kurmak ve geliştirmek üzere çevresinde bulunanlarla temas kurma hakkını da içermektedir. Kişilerin mesleki hayatı özel hayatlarıyla sıkı bir irtibat içindedir. Özel hayata dair hususlar kişinin mesleği ile ilgili tasarruflara esas alınmışsa özel hayata saygı hakkı gündeme gelecektir. (Bülent Polat, § 62; Ata Türkeri, § 31).

Gelişen teknolojinin, kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması amacıyla, kamu kesiminde kullanılmaya başlanması doğaldır. Ancak; teknoloji kullanılarak kişisel görüntülerin kayıt altına alınmasında özel hayatın gizliliği ve kişilerin mahremiyet hakkı da dikkate alınarak uygulama yapılması gerektiğinde kuşku ve duraksamaya yer bulunmamaktadır.

Buna ek olarak, kamu çalışanlarının faaliyet yürüttüğü servislerde çalışanların çalışma alanlarını ve dolayısıyla çalışanları görecektir şekilde yerleştirilen, güvenlik ve suçun önlenmesi gibi nedenlerle uygulandığı ileri sürülen kameralı takip sistemleri kullanılarak kişisel görüntülerin alınması, temel hak ve hürriyetler içerisinde sayılan özel hayatın gizliliği ilkesi kapsamında özel hayata müdahale olarak ele alınmalı, bu müdahalenin hukuka uygunluğunun değerlendirmesi ise kanunilik, ölçülülük gibi anayasal kavramlar yanında Avrupa İnsan Hakları Mahkemesi kararları ve Anayasa Mahkemesi kararları dikkate alınarak yapılmalıdır.

Yukarıda anılan müdahale, Anayasa'nın 13. maddesinde belirtilen koşulları yerine getirmediği müddetçe aynı zamanda Anayasa'nın 20. maddesinin ihlalini de teşkil edecektir.

Anayasa'mızın 13. maddesi "Temel hak ve hürriyetler, ... yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, ... demokratik toplum düzeninin... gereklerine ve ölçülülük ilkesine aykırı olamaz. " şeklindedir.

Bu sebeple müdahalenin ihlal oluşturup oluşturmadığının belirlenmesinde, Anayasa'nın 13. maddesinde öngörülen ve somut başvuruya uygun düşen kanunlar tarafından öngörülme, Anayasa'nın ilgili maddesinde belirtilen nedenlere dayanma, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmama koşulları yönünden inceleme yapılması gerekir.

Anayasa'nın 13. maddesi, temel hak ve özgürlüklerin sınırlandırılmasını, ilgili hak ve özgürlüğe ilişkin Anayasa maddesinde gösterilen özel sınırlandırma sebeplerinin bulunmasına bağlı kılmıştır. Bununla birlikte Anayasa Mahkemesinin kararlarına göre, özel sınırlama nedeni öngörülmemiş olan hakların dahi, hakkın doğasından kaynaklanan bazı sınırları bulunmaktadır. Ayrıca Anayasa'nın diğer maddelerinde yer alan kurallara dayanılarak da bu hakların sınırlanması mümkün olabilmektedir. Buna göre, Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebileceği kabul edilmektedir (AYM, E.2014/87, K.2015/112).

Anayasa'nın 20. maddesi "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kağıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakim tarafından onayına sunulur. Hakim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar." hükmünü haizdir.

Anayasa'nın 20. maddesinin birinci fıkrası yönünden özel sınırlama nedeni düzenlenmemiştir. Maddenin ikinci fıkrasında, birtakım sınırlama sebeplerine yer verilmiş olmakla beraber bu sebepler sadece arama ve elkoyma tedbirlerine yöneliktir. Dolayısıyla bu sebeplerin özel hayata saygı hakkının tüm boyutları yönünden uygulanması mümkün görünmemektedir.

Bu durumda, Anayasa'nın diğere maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin somut olay bakımından sınırlandırma sebebi olarak kabul edilip edilemeyeceğı araştırılmalıdır.

Anayasa'nın 5. maddesinde, "Devletin temel amaç ve görevleri, Türk Milletinin bağımsızlığını ve bütünlüğünü, ülkenin bölünmezliğini, Cumhuriyeti ve demokrasiyi korumak, kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak; kişinin temel hak ve hürriyetlerini, sosyal hukuk devleti ve adalet ilkeleriyle bağdaşmayacak surette sınırlayan siyasal, ekonomik ve sosyal engelleri kaldırmaya, insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmaktır. " denilmektedir. Buna göre kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak devletin temel amaç ve görevlerindedir.

Kişinin ve toplumun refah, huzur ve mutluluğunu sağlamanın ön koşulu milli güvenlik ve kamu düzeninin tesisidir. Milli güvenlik ve kamu düzeninin sağlanmadığı bir ortamda, hak ve özgürlüklerden gereğı gibi yararlanılması, kişinin maddi ve manevi varlığını geliştirmesi mümkün değildir. Devletin hak ve özgürlükleri koruma ödevinin yanında, milli güvenliğı ve kamu düzenini sağlama görevi de bulunmaktadır.

Yukarıda ifade edilen sınırlama nedenleri de dikkate alındığında uyumsuzluğun sağlıklı çözümü için; sınırlandırmanın, "demokratik toplum düzeninin gereklerinden olması" ve "ölçülülük ilkesine uygun olması"nın ne anlama geldiğinin de ortaya konması gerekmektedir.

"Demokratik toplum düzeninin gereklerinden olma, bir sınırlamanın demokratik bir toplumda zorlayıcı bir toplumsal ihtiyacın karşılanması amacına yönelik olmasını ifade etmektedir. Buna göre sınırlayıcı tedbir, bir toplumsal ihtiyacı karşılamıyorsa ya da başvurulabilecek son çare niteliğinde değilse demokratik toplum düzeninin gereklerine uygun bir tedbir olarak değerlendirilemez. (AYM, E.2015/96, K.2016/9, 10/2/2016 § 13; ifade özgürlüğü bağlamında Bekir Coşkun [GK], B. No: 2014/12151, 4/6/2015, § 51; özel hayatın gizliliğı hakkı bağlamında Ata Türkeri, § 44;İ.FA., B. No: 2013/8564, 17/2/2016, § 62).

Bu kapsamda kamu makamlarının faaliyetin niteliğı ve sınırlamanın amacına göre değışen geniş bir takdir yetkisinin bulunması doğaldır. Ancak özel hayatın gizliliğı hakkının mahremiyet hakkı gibi en gizli yönleri söz konusu olduğunda kamu makamlarının takdir yetkisi daha dardır ve bu alanlara yönelik müdahalelerin haklı olduğunun kabul edilebilmesi için kamu makamlarınca özellikle ciddi gerekçelerin gösterilmesi gerekir. (Ata Türkeri, § 47).

Kamu makamlarının özel hayata müdahaleleriyle ilgili olarak, müdahaleye yol açan karar alma sürecinde de keyfi davranmadıklarını kanıtlamaları gereklidir. Ancak bu halde de sınırlandırmanın ölçülülük ilkesine uygun olması gereklidir. (Ata Türkeri, § 48).

Anayasa Mahkemesi kararları uyarınca ölçülülük ilkesi, sınırlayıcı önlemin öngörülen amaç için zorunlu ve amaca ulaşmaya elverişli olmasını ayrıca amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder. Ölçülülük ilkesinin amacı da temel hak ve özgürlüklerin gereğinden fazla sınırlandırılmasının önlenmesidir (AYM, E.2015/102, K.2016/151, 7/9/2016, § 22; E.2012/100, K.2013/84, 4/7/2013; Marcus Frank Cerny, B. No: 2013/5126, 2/7/2015, § 72).

Avrupa İnsan Hakları Sözleşmesi'nin "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesi şöyledir: "(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. (2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir. "

Kamu makamlarının özel hayata saygı hakkına keyfi bir şekilde müdahale etmelerinin önlenmesi, Sözleşme'nin 8. maddesi ile sağlanan güvenceler kapsamında yer almaktadır. Avrupa İnsan Hakları Mahkemesi (AİHM), devletin özel hayata saygı hakkı kapsamında bulunan bir menfaate müdahale ettiğini tespit ettiğinde, 8. maddenin ikinci fıkrasında belirtilen koşulları incelemektedir. Buna göre kamu makamlarının müdahalesinin yasal bir dayanağı olup olmadığı, anılan fıkrada yer alan meşru amaçlara dayalı olup olmadığı, demokratik bir toplumda gerekli ve öngörülen amaçla orantılı olup olmadığı araştırılmaktadır. (AİHM Dudgeon/Birleşik Krallık, § 43; Olsson/İsveç No.1, B. No: 10465/83, 24/3/1988, § 59)

Ayrıca, AİHM kararlarına göre Sözleşme'nin 8. maddesi açıkça usul şartları içermemekle birlikte anılan maddeyle güvence altına alınan haklardan etkili bir şekilde yararlanılabilmesi için müdahaleyi doğuran karar alma sürecinin bu maddeyle korunan hak ve özgürlüklere gerekli saygıyı sağlayacak nitelikte ve adil olması gerekir. Bu şekildeki bir süreç başvurusunun 8. maddedeki haklarını -deliller ve kanıtlanma konuları dahil- adil şartlarda savunabileceği usule ilişkin etkili güvencelerden yararlandırılmasını gerektirir. AİHM'e göre bu şekildeki güvencelerin amacı 8. maddede yer alan haklara keyfi şekilde müdahalede bulunulmasını önlemek, müdahalenin gerekçelendirilmesini sağlamaktır (AİHM Ciubotaru/Moldova, B. No: 27138/04, 27/4/2010, § 51; T.P. ve K.M./Birleşik Krallık, B. No: 28945/95, 10/5/2001, § 72).

AİHM'e göre gerek negatif yükümlülükler gerekse pozitif yükümlülükler bakımından söz konusu usule ilişkin etkili güvencelerin sunulması gerekmektedir. (Benzer yöndeki AİHM kararı için bkz. Hokkanen/Finlandiya, B.No: 19823/92, 23/9/1994, §§ 55-58; Glaser/Birleşik Krallık, B. No: 32346/96, 19/9/2000, §§ 63-66; Bajrami/Arnavutluk, B. No: 35853/04, 12/12/2006, §§ 50-55; Abdulaziz, Cabales ve Balkandali/Birleşik Krallık, B. No: 9214/80, 28/5/1985, § 67).

Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesinin "Mahremiyet Hakkı" başlıklı 17. maddesinde de, hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemeyeceği; onuru veya itibarının hukuka aykırı saldırılara maruz bırakılmayacağına, herkesin bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahip olduğu belirtilmiştir.

Avrupa İnsan Hakları Mahkemesinin Antovic ve Mirkovic v. Sırbistan ve Karadağ (Başvuru No. 70838/13) kararında, çalıştıkları anfi alanlarına demirbaş ve öğrenciler de dahil kişi güvenliğinin sağlanması amacıyla kamera sistemi kurulan iki profesörün özel hayatlarının gizliliğinin ihlal edildiğine karar vermiştir. Kararda özellikle Avrupa İnsan Hakları Mahkemesinin daha öncede benzer konularda vermiş olduğu kararlara atıfta bulunularak bazı tespitlere de yer verilmiştir.

Bu tespitler arasında özellikle kişilerin iş yerinde ve çalışma ortamında yani kamusal bir alanda bulunsa da, özel hayatın profesyonel aktiviteler ve dış dünya ile ilişkileri de kapsayan ve Avrupa İnsan Hakları Mahkemesinin "sosyal özel hayat" olarak adlandırdığı bir alanı da kapsadığı ve bu alanın da korunması gerektiği, kamera sistemleri ile kişilerin sosyal özel hayatlarının izlenmesinin "ciddi bir müdahale" olarak kabul edilmesi gerektiği, kişilerin güvenliği veya işverenin hakları başka yollarla korunamıyorsa ancak son çare olarak kamera sistemlerinin kişilerin çalışma alanlarını görece şekilde kurulmasının kabul edilebilir olacağı tespitlerine yer verilmiştir. Yine Avrupa İnsan Hakları Mahkemesinin Lopez Ribalba ve Ötekiler v. İspanya (Başvuru No. 1874/13) kararında da iş verenin başka yollarla korunabilecek haklarını kamera sistemi yoluyla korumasının son çare olduğu, bu durumda bile kamera sistemleri ile ilgili olarak bildirimde bulunması ve usulleri belirlemesi gerektiği vurgulanmıştır.

Yine yukarıda yer verilen kararlardan, farklı güvenlik önlemleri yoluyla korunabilecek haklar veya önlenilecek olaylara yönelik olarak kamera sistemleri kurulmaması gerekeceği ve çalışanların doğrudan çalışma alanlarını görüntüleme şeklinde kişilerin özel hayatına müdahale anlamına gelen bu sistemlerin bu durumlarda kullanılmaması gerekeceği, aksinin ölçülülük ilkesine aykırı olacağı sonucuna ulaşılmaktadır.

Avrupa İnsan Hakları Mahkemesi kararlarında yukarıda ifade edilen Antovic ve Mirkovic v. Sırbistan ve Karadağ (Başvuru No. 70838/13) kararında da yer aldığı gibi kamera sistemleri ile ilgili olarak belli başlı şartların ortaya konulması gerektiği de ifade edilmiştir. Bunlar özellikle uygulamanın kanuni bir dayanağı olması, sınırlı bir izleme olması ve kötüye kullanmaya karşı garantiler olması gerektiğidir.

Türk Ceza Kanunu'nun "Özel hayatın gizliliğini ihlal" başlıklı 134. maddesi "Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.", "Kişisel verilerin kaydedilmesi" başlıklı 135. maddesi ise "Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir." hükmü yer almaktadır.

Ceza Muhakemesi Kanunu'nun "İletişimin tespiti, dinlenmesi ve kayda alınması" başlıklı 135. maddesi düzenlemesi de "başka suretle delil elde edilmesi imkânının bulunmaması durumunda" iletişimin kayda alınabileceğini, "Teknik araçlarla izleme" başlıklı 140. maddesi ise "başka suretle delil elde edilememesi hâlinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyeri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabilir" hükmü yer almakta olup, bu düzenlemeler de suça yönelik kuvvetli şüphe halinde bile en son çare olarak ses ve görüntü kaydına başvurulması gerektiğini ortaya koymaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanunu, 07.04.2016 tarihli ve 29677 Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Dava konusu işlem tarihinde yürürlükte bulunmamakla beraber konunun önemine binaen, dava konusu edilen kamera sistemleri ile ilgili belli başlı düzenlemelere de yer vermiştir. Neden bu sistemine ihtiyaç duyulduğunun ortaya konulması, sistemden kimin veya kimlerin yasal olarak sorumlu olduğunun belirlenmesi, sisteminin maksada uygun olup olmadığının ortaya konulması, özel hayatın gizliliğinin ihlal edilip edilmediğini kimin kontrol edeceğinin ve görüntülere kimin ulaşımı olacağına belirlenmesi ve bu hususların olarak kayıt altına alınması, kayıtlarının güvenliğinin ve gizliliğinin sağlanması güvenlik prosedürleri hazırlanması, kameralarla gözlemlenen bölgelerin girişinde ve içerideki uygun yerlerde bölgenin kamera sistemleri tarafından gözetlendiği ve kayıt altına alındığının belirtilmesi gerektiği, sistemin kuruluş maksadıyla bağdaşmayan görüntülerin gereğinden uzun süre saklanmaması, kişilerin özel hayatın gizliliğinin sağlanması yönünde beklentisinin olabileceği görüntülerin yetkili kişiler haricinde hiç kimse tarafından izlenememesi için alınacak önlemler gibi bir çok konuda düzenleme getirilmiştir.

Tüm bu açıklamalar ışığında dava konusu işlem incelendiğinde, Avrupa İnsan Hakları Mahkemesi kararları da dikkate alındığında hakların korunması başka şekilde sağlanamıyorsa kamera

sistemlerinin çalışanların çalışma alanlarını görecektir şekilde kurulmasının mümkün olduğu ancak bunun bir son çare olarak değerlendirildiği ve bu düzenlemenin içeriğini ayrıntılı olarak ortaya koyan bir özel düzenleyici işlem olması gerektiği, kamera sistemlerinin çalışma alanlarını çekmesinin özel hayatın gizliliğini ihlal ettiği, sınırlı bir izleme sağlayacak şekilde güvenlik amacıyla giriş ve çıkışları izlemek üzere veya vatandaşlara da açık olan ortak alanlar ve iş sahiplerinin de giriş çıkışına açık, yoğun bir alış veriş trafiği olan alanlarda kurulabileceği ancak bu kameraların da çalışanların iş yapış şekillerini denetlemek veya sürekli olarak belli kişileri çekecek şekilde kurulmaması gerektiği, güvenlik amacıyla kurulmuş olmaları gerektiği ve bu nedenle amaca hizmet eder şekilde konumlandırılması gerektiği anlaşılmaktadır.

Yine kamera sistemlerinin zorunlu güvenlik amacı ile ve başka bir yolla bu güvenlik amacı sağlanamıyorsa kurulabilmesi mümkün olsa da, yukarıda yer verilen açıklamalar ışığında uygulamanın usul ve esaslarını gösteren yasal dayanağının bulunması, açık ve anlaşılabilir olması ve ilgililerin bu konudaki hakları ve kamera sistemi ile ilgili olarak bilgilendirilmiş olması gerektiği, toplanan görüntülerle ilgili güvencelerin sağlanması gerektiği, dava konusu işlemin bu haliyle sınırları belirlenmemiş, yasal dayanağı olmayan, uygulamaya dair usul ve esaslar ile güvenceleri düzenlenmemiş bir sistemle yürütüldüğü ve bu haliyle kamu yararına yönelik olduğunu kabul etmeye imkan olmadığı; Anayasal bir ilke olan ölçülülük ilkesine aykırılık teşkil ettiği ve mahremiyet hakkını ihlal ettiği anlaşılmakta olup, kişilik haklarına aykırı şekilde kamu görevlilerinin tüm faaliyetlerinin izlenmesine imkan tanıyan uygulamada isabet bulunmamaktadır.

Kameralı takip sistemi ile kurumca amaçlanan kamu yararı arasında orantılılık bulunmadığından uygulama ölçülülük ilkesine de aykırılık teşkil etmektedir. Anayasa'nın 13. maddesinde, temel hak ve hürriyetlerin ancak kanunla sınırlanabileceği, değişik 20/3. maddesinde de, kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceğinin belirtildiği, ancak konuyla ilgili dava konusu işlemin gerçekleştirildiği aşamada yasal bir düzenlemenin yapılmadığı anlaşılmaktadır.

İdarelerin teknolojik gelişmelerden de yararlanarak kamu çalışanlarının faaliyet yürüttüğü alanda güvenlik ve suçun önlenmesi amacıyla kameralı takip sistemi uygulamasının, güvenlik amaçlı olarak giriş ve çıkışlar ve güvenliğin özel önem arz ettiği alanlar dışında, günlük iş ve işlemleri yürüten çalışanların çalışma odalarını ve servisleri çekecek şekilde yerleştirildiği durumlarda, kamusal alanda da olsa "özel hayatın gizliliği" ilkesi kapsamında bulunduğu Avrupa İnsan Hakları Mahkemesi kararları ve Dairemizin daha önceki tarihli kararlarından anlaşılmaktadır. Yine uygulamanın sınırlarını, usul ve esaslarını gösteren bir yasal dayanağın bulunması, toplanan görüntülerin ileride

başka bir şekilde kullanılamayacağına dair bir güvencenin mevcut olması gerektiği de anlaşılmaktadır.

İdarenin güvenlik ve kamu yararını sağlama ihtiyacı ve çalışanların özel hayatın gizliliği gibi haklarının karşı karşıya geldiği bu gibi uyuşmazlıklarda, olayın dosyaya özel olarak ele alınması ve değerlendirilmesi gerektiği açıktır.

Uyuşmazlığın bu davaya özgü hali değerlendirildiğinde; vezne servislerinde görev yapan personelin takip edilmesi amacıyla veznelere kamera yerleştirilmesi ve personelin kayıt altına alınması uygulamasına son verilmesi talebiyle davacı sendika tarafından başvuru yapıldığı anlaşılmakta olup; uygulamanın sınırlarını, usul ve esaslarını gösteren bir yasal dayanağın bulunmaması, toplanan görüntülerin ileride başka bir şekilde kullanılamayacağına dair bir güvencenin mevcut olmaması ve iş yerinin güvenliğini sağlama amacını aşarak, doğrudan çalışan memurun kendisinin, diğer memurlarla ya da iş sahipleriyle ilişkisinin ve kamu hizmetinin görülmesi sırasında yaptığı her türlü haberleşmesinin, çalışma alanı ve masasının gözlemlendiği kamera takip sisteminin kurulmasının özel hayatın gizliliğini ihlal ettiği ve bu haliyle yukarıda belirtilen temel haklar ve Anayasal ilkelerle bağdaşmaması nedeniyle dava konusu işlemin iptaline karar verilmesi gerekirken davanın reddi yolunda verilen mahkeme kararının hukuka aykırı olduğu sonucuna varılmıştır.

Açıklanan nedenlerle, temyiz isteminin kabulüyle, Edirne İdare Mahkemesi'nin 30/04/2015 tarih ve E:2014/646, K:2015/574 sayılı kararının BOZULMASINA, yeniden bir karar verilmek üzere dosyanın adı geçen Mahkemeye gönderilmesine, 2577 sayılı Kanun'un (Geçici 8. maddesi uyarınca uygulanmasına devam edilen) 54. maddesinin 1. fıkrası uyarınca bu kararın tebliğ tarihini izleyen günden itibaren onbeş gün içinde karar düzeltme yolu açık olmak üzere, 14/05/2018 tarihinde oybirliğiyle karar verildi.

Danıştay Kararı - 15. Daire (E. 2015/3035)

Danıştay Kararı - 15. D., E. 2015/3035 K. 2017/6611 T. 14.11.2017

Davanın Özeti: nın 05.02.2015 tarihli ve "e-Nabız Projesi" konulu Genelgesi'nin iptali istenilmektedir.

Savunmanın Özeti: Dava konusu Genelgede düzenlenen e-Nabız sistemine ilişkin olarak, savunma dilekçesinde öncelikle sistemin tanıtılmasına ve sürecine ilişkin detaylı açıklamalara yer verilmiş olup, Sağlık Bakanlığının sağlık hizmetlerini yürütme görevini Anayasa ve 663 sayılı KHK çerçevesinde yürüttüğü, 3359 sayılı Sağlık Hizmetleri Kanununun 3/f maddesinde, 5258 sayılı Aile Hekimliği Kanunundaki ve bu Kanuna istinaden çıkarılan normatif işlemlerdeki hükümlerde, Anayasanın 20 nci maddesine eklenen üçüncü fıkrada, Tıbbi Deontoloji Nizamnamesinde yer alan düzenlemeler ile 663 sayılı KHK'daki muhtelif hükümlerde kişisel sağlık kayıtlarına dair hükümlere yer verildiği ve Sağlık Bakanlığına buna ilişkin verilen görevler bulunduğu, E-Nabız Kişisel Sağlık Sisteminin; sağlık kuruluşlarından toplanan sağlık verilerine vatandaşların ve sağlık profesyonellerinin internet ve mobil cihazlar üzerinden erişebilmelerine olanak sağlayan bir uygulama olduğu, vatandaşların 01.01.2015 tarihinden itibaren girmiş oldukları sağlık kuruluşlarına ait bilgilere, kendilerine yazılmış reçetelere, ilaç bilgilerine, tahlil sonuçlarına, rapor bilgilerine, tıbbi görüntülerine ve kendilerine ait birçok sağlık verisine bu sistem üzerinden ulaşabildikleri, sağlık hizmetinin tüm aşamalarında hasta ve tedavi bilgilerinin kayıt altına alınmasının birçok açıdan gereklilik içerdiği, bugüne kadar bu bilgilerin tedavinin sürekliliğinin yanı sıra bilimsel ve istatistiksel değerlendirmeler için de önemli kaynak işlevi gördüğü, toplum sağlığına önemli katkılarda bulunduğu, ayrıca kayıtlı bilgilerin hukuksal durumlarında belge işlevi özelliğini de üstlendiğini, Bakanlığın bu yetki ve görevi Anayasanın 56 ncı maddesinden aldığı, sağlık verilerinin işlenmesinin temel, mutlak ve yegane koşul olarak bireyin rızasına bağlanmasının ve bazı istisnaların kabul edilmemesi halinde ülkenin sağlık hizmet sunumu ve sağlık hizmeti yönetimi anlamında ciddi dar boğazlara gireceğinin aşikâr olduğu, Anayasanın 20 nci maddesine eklenen hükme uygun olarak vatandaşların, e-nabız sisteminde kendisine ait verileri tamamen silebileceği gibi sağlık tesisi ziyareti bazında da teker teker silebildiği, dilerse e-nabız hesabını kendisinin karar verdiği süre kadar da dondurabildiği, sağlık verilerinin kontrolünün tamamen kişinin kendi rızasına ve kendi kontrolüne bırakılmış olduğu, sistemin buna göre tasarlandığı, e-nabız profili dondurma ve kapatma işlemleri yapılırken kişinin kendi sisteme giriş işlemini güvenli e-devlet kapısı üzerinden gerçekleştirilmiş olduğunun esas olduğu, 663 sayılı KHK'nın 8 inci maddesinin (j) bendi ile sağlık hizmet sektöründe kişisel verilerin korunması ve veri mahremiyetinin sağlanması görevinin zaten Sağlık Bakanlığına

verildiđi, diđer taraftan 3359 sayılı Kanun'un ilgili maddeleri ile kişisel sađlık verilerinin kayıt altına alınmasının dođrudan düzenlendiđi, bu hükümlerde kayıt ve bildirim sistemin kurulması için herhangi bir sınırlama getirilmediđi, zaten mevzuat hükümleri geređi sađlık hizmeti sunan gerçek ya da tüzel kişiler, ister kamu kurumu olsun ister özel kurum olsun kendisine başvuran herkesin tıbbi kayıtlarını tutmakla yükümlü oldukları, işlemin yöneldiđi amacın Bakanlıđın asli görevi olan sađlık hizmetini, nitelikli, hızlı, ekonomik ve hakkaniyete uygun olarak toplumun her kesimine, herkese, ulaştırmaya devam etmekte olduđu, bu işlemin münhasıran kamu yararının gerçekleştirilmesine yönelik olduđu, nitekim bu konuda İstanbul Üniversitesi Hukuk Fakültesi İdare Hukuku Anabilim Dalı ve Anayasa Hukuku Anabilim Dalından alınan hukuki mütalaanın bu hususu bilimsel olarak ortaya koyduđunu, sonuç olarak dava konusu düzenlemenin hukuka uygun olduđu savunulmaktadır.

Danıştay Tetkik Hakimi:

Düşüncesi: Yasal dayanađı bulunmayan Genelgenin iptali gerektiđi düşünülmektedir.

Danıştay Savcısı:

Düşüncesi: Dava; 5.2.2015 tarihli ve "e-Nabız Projesi" konulu Genelgesi'nin iptali istemiyle açılmıştır.

Davalı idare tarafından verilen savunmada dava konusu düzenlemeye dayanak oluşturabilecek kanun hükümleri sayılmış, bu mevzuat arasında Anayasa'nın 20 nci ve 56 ncı maddelerine, 3359 sayılı Sađlık Hizmetleri Temel Kanunu'nun 3 üncü maddesinin (f), (i), (j) bentleri ile 663 sayılı Kanun Hükmünde Kararname'nin 8 inci maddesinin birinci fıkrası (j) bendine yer verilmiştir.

Söz konusu mevzuat hüküm arasında yer alan 3359 sayılı Sađlık Hizmetleri Temel Kanunu'nun 3 üncü maddesinde, sađlık hizmetleriyle ilgili temel esaslar sayılmış olup; (f) bendinde, "Herkesin sađlık durumunu takip edebilmek için gerekli kayıt ve bildirim sistemi kurulur." hükmü, (i) bendinde, "Sađlık hizmetlerinin yurt çapında istenilen seviyeye ulaştırılması amacıyla, bakanlıklar seviyesinden en uçtaki hizmet birimine kadar kamu ve özel sađlık kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları arasında koordinasyon ve işbirliđi yapılır. Sađlık kurum ve kuruluşları cođrafik ve fonksiyonel hizmet alanları, verecekleri hizmetler, yönetim, hizmet ilişki ve bağlantıları gibi konularda tespit edilen esaslara uymak ve verilen görevleri yapmakla yükümlüdürler. Çađdaş tıbbi bilgi ve teknolojinin ülkeye getirilmesi ve teşviki sađlanır." hükmü, (j) bendinde, "Vatandaşların hastalıktan korunması, sađlıklı çevre, beslenme, ana çocuk sađlığı ve aile planlaması, ve benzeri konularda eğitilmeleri ve takipleri bütün kamu kurumu niteliğindeki meslek kuruluşları, özel ve gönüllü kuruluşların işbirliđi içerisinde gerçekleştirilir." hükmü yer almış, 663 sayılı Kanun

Hükmünde Kararnamenin 8 inci maddesinin birinci fıkrası (j) bendinde ise, ilgili mevzuat çerçevesinde kişisel verilerin korunması ve veri mahremiyetinin sağlanmasına yönelik düzenleme yapmanın Sağlık Hizmetleri Genel Müdürlüğünün görevleri arasında bulunduğuna işaret edilmiştir.

Görüldüğü üzere, 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 3 üncü maddesinin (f) bendinde, "Herkesin sağlık durumunu takip edebilmek için gerekli kayıt ve bildirim sistemi kurulur." hükmü yer almakta olup; bu hüküm, kayıt ve bildirim sisteminin internet üzerinden bir yazılım yoluyla yapılacağına ve kişisel sağlık verilerinin bu sisteme aktarılacağına yönelik bir düzenleme içermemekte, 663 sayılı Kanun Hükmünde Kararname'nin 8 inci maddesinin birinci fıkrasında ise Sağlık Hizmetleri Genel Müdürlüğünün görevleri sayılmaktadır.

Anayasa'nın 20 nci maddesine 5982 sayılı Kanun'un 2 nci maddesi ile eklenen fıkrada, "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilmiştir.

Dosyanın incelenmesinden, dava konusu "e-Nabız Projesi" konulu Genelge'de, fert ve toplum sağlığının korunması iyileştirilmesi ve geliştirilmesi için kişisel sağlık kayıtlarının gizlilik, güvenlik bütünlük ve mahremiyetinin korunarak kişilerin dijital sağlık kayıtlarına erişebilmesini sağlayacak olan ve e-Nabız adı verilen Sağlık.Net Online Sisteminin kurulduğu belirtilmiş, söz konusu Genelge'de sistemin amacı ve işleyişine dair bazı açıklamalara yer verildikten sonra sonuç kısmında; tıbbi kayıtlara kişilerin kendi erişiminin sağlanabilmesi için 1 Ocak 2015 tarihinden itibaren tutulan tüm kayıtların hizmet sunucuları tarafından sisteme gönderilmesinin gerektiği ifade edilmiştir.

Kişisel verilerin korunması gerçek veya tüzel kişilere ait olan ve onların belirlenebilir, bir başka ifadeyle teşhis edilebilir olmasını sağlayan şahsa özgü ve özel bilgilerin koruma altına alınmasını ifade etmekte olup; kişilerin bedensel ve psikolojik sağlık durumlarına ilişkin bilgileri içeren merkezi bir sistemin kurulmasının ve bu sistemin işleyişine ilişkin temel esas ve usullerin Anayasa'nın anılan 20. maddesi hükmü uyarınca kanun ile düzenlenmesinin sistemde mahrem bilgileri yer alan kişiler açısından zorunlu hukuki güvenceyi sağlayacağı tartışmasızdır.

Açıklanan nedenlerle, yasal dayanağı bulunmadığı anlaşıldığından 5.2.2015 tarihli ve "e-Nabız Projesi" konulu Genelgesi'nin iptali gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Karar veren Danıştay Onbeşinci Dairesi'nce Tetkik Hakiminin açıklamaları dinlenildikten sonra gereği görüldü:

Dava; 05.02.2015 tarihli ve "e-Nabız Projesi" konulu Genelgesi'nin iptali istemiyle açılmıştır.

Dava konusu Genelge'nin incelenmesinden; fert ve toplum sağlığının korunması, iyileştirilmesi ve geliştirilmesi için kişisel sağlık kayıtlarının gizlilik, güvenlik, bütünlük ve mahremiyetinin korunarak kişilerin kendileri tarafından kendi dijital sağlık kayıtlarına erişebilmesine sağlayacak olan ve e-Nabız adı verilen Sağlık.Net Online Sisteminin kurulduğu görülmekte olup, bu proje kapsamında Kişisel Sağlık Sistemi (KSS) ile Teletıp ve Teleradyoloji Sisteminin (TTS) geliştirildiği, bu sistemlerin bütünlük, sürekli ve kesintisiz işlerliğini teminen; sağlık hizmeti ve dolayısıyla sağlık verisi üretmekte olan kamu ve özel tüm kişilere ve kuruluşlara bu Genelgenin ulaştırılması, tıbbi kayıtlara kişilerin kendilerinin erişiminin sağlanabilmesi için 01 Ocak 2015 tarihinden itibaren tutulan kayıtların hizmet sunucuları tarafından sisteme gönderilmesi, sağlık hizmet sunucuları ve yazılım üreticilerinin acil sağlık verileri başta olmak üzere kişinin kendi sağlık bilgisine erişiminin sağlanmasından sorumlu olduğunun bilinmesi, tüm sağlık hizmet sunucularının üretmiş oldukları bilgilerin mekandan bağımsız olarak bu sistem üzerinden sahibine sunulabilmesi için gerekli tedbirlerin alınması, Bakanlığa bağlı sağlık tesislerinin entegrasyonunun büyük ölçüde tamamlanmış olduğu, tamamlanmamış sağlık tesislerinin de ivedilikle sisteme entegre edilerek veri gönderimine başlaması, Aile Hekimliği Bilgi Sistemlerinin en geç 01 Mart 2015 tarihinde sisteme entegre edilmiş ve veri gönderiyor olması, Üniversite Hastaneleri ve tüm Özel Sağlık Hizmeti Sunucularının yazılımlarının en geç 01 Mart 2015 tarihinde sisteme entegre edilmiş ve veri gönderiyor olması hususlarının 81 İl Valiliğine bildirildiği anlaşılmaktadır.

Davacı tarafından, kişisel verilerin işleyişi ile ilgili olarak, usul ve esasların kanunla belirlenmesinin Anayasal bir zorunluluk olduğu, bu konunun genelge ya da yönetmeliklerle düzenlenemeyeceği, yasama yetkisinin yürütme organına devredilemeyeceği, ayrıca dava konusu Genelgede ne tür sağlık verilerinin hangi koşullarda toplanacağı, hangi sağlık verileri için hastaların rızasının alınacağı ve bu rızanın alınma usulü hakkında hiçbir düzenleme ve açıklamanın bulunmadığı, anılan Genelgenin "Sağlık Net 2 Veri Gönderimi" başlıklı ve Danıştay tarafından yürütülmesinin durdurulmasına karar verilen başka bir genelgenin farklı bir yöntemle ve fakat aynı saikle uygulanma isteğinin tekrarından ibaret olduğu, 663 sayılı KHK'nın 47 nci maddesinin birinci, ikinci ve üçüncü fıkralarının yeniden değiştirildiği, bu değişikliğe göre Sağlık Bakanlığı ve Bağlı Kuruluşlarının e-devlet uygulamalarını yerine getirebilmek amacıyla bütün kamu ve özel sağlık kurum ve kuruluşlarından sağlık hizmeti alanların, aldıkları sağlık hizmetinin gereği olarak ilgili sağlık kurum ve kuruluşlarına vermek

zorunda oldukları kişisel bilgileri ve bu kimselere verilen hizmete ilişkin bilgileri her türlü vasıtasıyla toplamaya, işlemeye, paylaşmaya ve istemeye yetkili hale getirildiği, ayrıca ilgili kişi ve kuruluşların istenilen bilgileri vermekle yükümlü kılındığı, Anayasa Mahkemesinin 04.12.2014 tarihli ve E:2013/114, K:2014/184 sayılı kararı ile bu değişikliğin iptal edildiği, böylece dava konusu Genelgenin, hukuka, tıp mesleğinin doğasına ve düzenlemelerine, kazanılmış haklara, kişi hak ve özgürlüklerine ve konu hakkında evvelce verilmiş mahkeme kararlarına aykırı hükümler içermesi nedeniyle iptali istenilmektedir.

Dairemizin 20.04.2015 tarihli ara kararı ile dava konusu Genelge'de, kişilerin tıbbi kayıtlarına kendilerinin erişimlerinin sağlanabilmesi amacıyla e-Nabız Projesi kapsamında Kişisel Sağlık Sistemi (KSS) ile Teletıp ve Teleradyoloji Sisteminin (TTS) devreye alındığı, sistemin bütünleşik, sürekli ve kesintisiz işlerliğini teminen sağlık hizmeti veren tüm sağlık kurum ve kuruluşlarının, 01 Mart 2015 tarihinden itibaren tüm sağlık verilerini sisteme göndermelerinin gerektiği ifade edildiğinden; KSS ve TTS Sistemlerinin hangi yasal düzenleme veya düzenleyici işlemlere dayalı olarak kurulduğu hususunun sorulmasına ve uyuşmazlığın çözümünde gerekli tüm bilgi ve belgelerin istenilmesine karar verildiği, buna istinaden sunulan davalı idarenin savunma dilekçesinde, anılan Genelgenin yasal dayanakları arasında, Anayasanın 20 nci ve 56 ncı maddeleri, 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 3 üncü maddesinin (f), (i), (j) bentleri, 5258 sayılı Aile Hekimliği Kanunu'nun 1 inci ve 5 inci maddesinin üçüncü fıkrası ile 663 sayılı Kanun Hükmünde Kararnamenin 8 inci maddesinin birinci fıkrası (j) bendi hükümlerine yer verildiği görülmüştür.

Söz konusu hükümlere bakıldığında;

3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 3 üncü maddesinde sağlık hizmetleriyle ilgili temel esaslar sayılmış olup (f) bendinde, -işlemin tesis edildiği tarih itibarıyla- "Herkesin sağlık durumunu takip edebilmek için gerekli kayıt ve bildirim sistemi kurulur." hükmü , (i) bendinde "Sağlık hizmetlerinin yurt çapında istenilen seviyeye ulaştırılması amacıyla, bakanlıklar seviyesinden en uçtaki hizmet birimine kadar kamu ve özel sağlık kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları arasında koordinasyon ve işbirliği yapılır. Sağlık kurum ve kuruluşları coğrafik ve fonksiyonel hizmet alanları, verecekleri hizmetler, yönetim, hizmet ilişki ve bağlantıları gibi konularda tespit edilen esaslara uymak ve verilen görevleri yapmakla yükümlüdürler. Çağdaş tıbbi bilgi ve teknolojinin ülkeye getirilmesi ve teşviki sağlanır." hükmü, (j) bendinde "vatandaşların hastalıktan korunması, sağlıklı çevre, beslenme, ana çocuk sağlığı ve aile planlaması, ve benzeri konularda eğitilmeleri ve takipleri bütün kamu kurumu niteliğindeki meslek kuruluşları, özel ve gönüllü kuruluşların işbirliği içerisinde gerçekleştirilir." hükmünün yer aldığı,

5258 sayılı Aile Hekimliği Kanunu'nun 1 inci maddesinde; "Bu Kanunun amacı; Sağlık Bakanlığının belirleyeceği illerde, birinci basamak sağlık hizmetlerinin geliştirilmesi, birey ihtiyaçları doğrultusunda koruyucu sağlık hizmetlerine ağırlık verilmesi, kişisel sağlık kayıtlarının tutulması ve bu hizmetlere eşit erişimin sağlanması amacıyla aile hekimliği hizmetlerinin yürütülebilmesini teminen görevlendirilecek veya çalıştırılacak sağlık personelinin statüsü ve malî hakları ile hizmetin esaslarını düzenlemektir." hükmü ile 5 inci maddesinin üçüncü fıkrasında, "Aile hekimlerinin şahsî kayıtları ilgili il ve ilçe sağlık idare birimlerinde tutulur. Aile hekimlerinin kullandığı basılı veya elektronik ortamda tutulan kayıtlar, kişilerin sağlık dosyaları ile raporlar, sevk belgesi ve reçete gibi belgeler resmî kayıt ve evrak niteliğindedir. Bu kayıt ve belgeler, hekimin ayrılması veya kişinin hekim değiştirmesi halinde eksiksiz olarak devredilir. İlgili mevzuatta birinci basamak sağlık kuruluşları ve resmî tabiplerce düzenlenmesi öngörülen her türlü rapor, sevk evrakı, reçete ve sair belgeler, aile hekimliği uygulamasına geçilen yerlerde aile hekimleri tarafından düzenlenir." kuralına yer verildiği,

663 sayılı Kanun Hükmünde Kararnamenin 8 inci maddesinin birinci fıkrasının (j) bendinde ise, "İlgili mevzuat çerçevesinde kişisel hususunun verilerin korunmasına ve veri mahremiyetinin sağlanmasına yönelik düzenleme yapmak." hususunun Sağlık Hizmetleri Genel Müdürlüğünün görevleri arasında sayıldığı görülmektedir.

Öte yandan 08.12.2015 tarihinde Danıştay Başkanlığı kayıtlarına giren idarenin ek beyan dilekçesinin ekinde İstanbul Üniversitesi Hukuk Fakültesi İdare Hukuku ve Anayasa Hukuku Anabilim Dallarından Genelgenin yasal dayanağının değerlendirilmesine ilişkin olarak hukuki mütalaa sunulmuş, anılan mütalaanın sonuç bölümünde "Taraflar arasında ihtilaf konusu olmadığı gibi, 2015/5 sayılı Genelge ile Anayasanın 20 nci maddesinin son fıkrasında yer alan kişisel verilerin işlenmesine imkân tanıyan bir düzenleme yapılmaktadır. Bu düzenleme ile kişilerin hassas verileri arasında yer alan sağlık bilgileri otomatik işleme tabi tutulduğu gibi ilgili sağlık kuruluşlarına bu bilgileri verme bakımından bir yükümlülük getirilmektedir. Bu nitelikteki bir düzenleme temel hak ve hürriyetler bakımından bir sınırlama kabul edilir.

Anayasa'nın 13 üncü maddesi ve konuyu doğrudan düzenleyen 20 nci maddesinin son fıkrasına göre böyle bir sınırlamanın kanunla yapılması gerekir. Bu Genelgenin yasal dayanağı olarak belki sadece 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 3 üncü maddesinin (f) fıkrası gösterilebilir. Bu fıkarda yer alan "Herkesin sağlık durumunu takip edebilmek için gerekli kayıt ve bildirim sistemi kurulur" şeklindeki genel hüküm ile Sağlık Bakanlığına, gerekli kayıt ve bildirim sistemini kurma adına "veri işleme" [data processing] yetkisi verildiği görülmektedir. Hak ve özgürlüklere ilişkin

sınırlama getiren bu hüküm Anayasa Mahkemesi içtihatları uyarınca "herhangi bir duraksamaya ve kuşkuya yer vermeyecek şekilde açık, net, anlaşılır ve uygulanabilir olmamakla" birlikte, veri koruma hukuku uyarınca "veri işleme" [data processing] tabirinin, verilerin elde edilmesi ile başlayan ve kaydedilmesi, düzenlenmesi, uyarlanması, değiştirilmesi, düzeltilmesi, incelenmesi, kullanılması, açıklanması, sıralanması, birleştirilmesi, korunması ve silinmesi ile devam eden birçok alt kavramı bünyesinde barındırması karşısında, Genelge bakımından yasal dayanak oluşturabileceği ileri sürülebilir." açıklamalarına yer verilmiştir.

Daha önce yayımlanan benzer nitelikteki Sağlıknet2 Veri Gönderimi konulu Genelge ile ilgili olarak Dairemizin 18/11/2015 tarihli ve E:2012/12338-K:2015/7780 sayılı kararında da tespit edildiği üzere, dava konusu Genelgenin dayanağı olabileceği ileri sürülen hükümler incelendiğinde, düzenlemenin yapıldığı tarihte yürürlükte bulunan 3359 sayılı Kanunun 3 üncü maddesinin (f) bendinin genel bir düzenleme olup, kayıt ve bildirim sisteminin internet üzerinden bir yazılım yoluyla yapılacağı ve kişisel sağlık verisi kapsamındaki verilerin bu sisteme aktarılacağına yönelik bir düzenleme içermediği, 5258 sayılı Kanunun aile hekimlerine ilişkin olduğu, 663 sayılı Kanun Hükmünde Kararnamenin 8 inci maddesinin birinci fıkrasının ise Sağlık Hizmetleri Genel Müdürlüğünün görevlerine ilişkin olduğu görülmüştür.

Anayasa'nın 20 nci maddesine 5982 sayılı Kanun'un 2 nci maddesi ile eklenen fıkrada "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilmiştir.

Anayasa'nın bu hükmünde kişisel verilerin korunmasını isteme hakkının neleri kapsadığı hususunun özellikle vurgulanmış olması karşısında, hassas veri kabul edilen kişisel sağlık verilerinin toplanması ve işlenmesinin kapsamı, koşulları ve bu verilerin korunmasına ilişkin usul ve esasları içermeyen söz konusu yasal düzenlemelerin, Anayasa'nın 20 nci maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceğine ilişkin güvenceyi sağlamaktan uzak olduğu sonucuna ulaşılmıştır.

Bu nedenle, yasal dayanağı bulunmayan Genelge'de hukuka uyarlık görülmemiştir.

Diğer taraftan, bu konuda daha ayrıntılı düzenlemeler içeren 663 sayılı Kanun Hükmünde Kararname'nin 47 nci maddesinin birinci ve üçüncü fıkraları Anayasa Mahkemesi'nin 14.02.2013 tarih ve E:2011/150, K:2013/30 sayılı kararı ile iptal edilmiş, ardından 12.07.2013 tarihinde kabul edilen ve

02.08.2013 tarih ve 28726 sayılı Resmî Gazete'de yayımlanan 6495 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun'un 73 üncü maddesinin (h) bendinin üçüncü alt bendi ile 663 sayılı Kanun Hükmünde Kararname'nin Anayasa Mahkemesi'nce iptal edilen hükümleri yeniden düzenlenmiştir. Bu kez de anılan hüküm, Anayasa Mahkemesi'nin 16.07.2015 tarih ve 29418 sayılı Resmî Gazete'de yayımlanan 04.12.2014 tarih ve 2013/114, 2014/184 sayılı kararıyla; dava konusu kuralla sadece demokratik toplum düzeni yönünden zorunlu olan sınırlamalar değil, özel hayatın ve kişisel verilerin korunması haklarına yapılabilecek her türlü sınırlamaya izin verilmesi, bir başka ifade ile kuralda anılan haklara sınırlama getirilirken sınırlama aracının sınırlama amacına uygun ve orantılı olarak kullanılmasını temin edecek güvencelere yer verilmemesinin ölçülülük ilkelerine aykırı düştüğü gerekçesiyle iptal edilmiştir.

Son durumda ise, 24.03.2016 tarihinde kabul edilen ve 07.04.2016 tarih ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30 uncu maddesi ile 663 sayılı Kanun Hükmünde Kararnamenin 47 nci maddesi yeniden düzenlenmiştir.

Bununla birlikte 6698 sayılı Kanun'un 30 uncu maddesi ile 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 3 üncü maddesinin (f) bendi de değiştirilmiş olup, "f) Herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi maksadıyla, Sağlık Bakanlığı ve bağlı kuruluşlarınca gerekli kayıt ve bildirim sistemi kurulur. Bu sistem, e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabilir. Bu amaçla, Sağlık Bakanlığınca, bağlı kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemi kurulabilir." hükmüne yer verilmiştir.

Her ne kadar Genelgenin yürürlüğe girmesinden sonra 663 sayılı Kanun Hükmünde Kararname'nin 47 nci maddesi ile 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 3 üncü maddesinin (f) bendi yeniden düzenlemiş ise de sonradan yürürlüğe giren yasal düzenlemelerin önceden yürürlüğe giren Genelge'nin dayanağı olamayacağı açıktır.

Açıklanan nedenlerle 05.02.2015 tarihli ve "e-Nabız Projesi" konulu Genelgesi'nin İPTALİNE, aşağıda dökümü yapılan 261,90 TL yargılama gideri ile kararın verildiği tarihte yürürlükte olan Avukatlık Asgari Ücret Tarifesine göre belirlenen 1.800,00 TL avukatlık ücretinin davalı idareden alınarak davacıya verilmesine, artan posta ücretinin kararın kesinleşmesinden sonra davacıya iadesine, kararın tebliği tarihini izleyen günden itibaren 30 (otuz) gün içinde Danıştay İdari Dava Daireleri Kuruluna temyiz yolu açık olmak üzere, 14/11/2017 tarihinde oybirliğiyle karar verildi.

Danıştay Kararı - 10. Daire (E. 2015/2995)

Danıştay Kararı - 10. D., E. 2015/2995 K. 2018/1736 T. 14.5.2018

İstemin Özeti: Kırıkkale İdare Mahkemesi'nin davanın reddi yolunda verilen 12/03/2015 tarih ve E:2014/543, K:2015/162 sayılı kararının hukuka uygun olmadığı ileri sürülerek temyizden incelenerek bozulması davacı sendika tarafından istenilmektedir.

Savunmanın Özeti: Temyiz isteminin reddi gerektiği savunulmaktadır.

Danıştay Tetkik Hakimi: K1

Düşüncesi: İdare Mahkemesi kararının bozulması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Hüküm veren Danıştay Onuncu Dairesi'nce gereği görüldü:

Dava; davacı Sendikanın Kırıkkale Üniversitesi hizmet binaları içerisinde mevcut kamera ile izleme sisteminin risk oluşturmayan birim ve bölgelerde kaldırılması istemiyle yaptığı 16/07/2014 tarihli başvurusunun reddine ilişkin 05/08/2014 tarih ve 6217 sayılı işlemin iptali istemiyle açılmıştır.

Kırıkkale İdare Mahkemesi'nce; dava konusu kameraların davalı idare tarafından görev yapmakta olan akademik personel ile diğer personelin ve öğrenim görmekte olan öğrencilerin güvenliğini sağlamak amacıyla konulduğu, idarenin gerektiği zaman bu tür güvenlik önlemlerini alma konusunda yetkili olduğu, üniversite alanı içerisinde güvenlik kamerası konulmasını gerekli kılan asayiş olaylarının yaşanmakta olduğunu gösteren belgelerin savunma dilekçesi ekinde dosyaya sunulduğu, bu kameraların güvenlik amacı dışında personelin mesaiye geliş gidişleri veya güvenlik amacı dışındaki diğer başka yönlerden takibinde kullanıldıklarına ilişkin somut bilgi ve belge bulunmadığı gerekçeleriyle davanın reddine karar verilmiştir.

Davacı sendika tarafından, yapılan uygulamanın ve tesis edilen işlemin çalışanların özel hayatının gizliliğini ihlal ettiği ve bu nedenle hukuka aykırı olduğu ileri sürülerek İdare Mahkemesi kararının temyizden incelenerek bozulması istenilmektedir.

Davacı sendikanın temyiz gerekçesi olarak özel hayatın gizliliği ve mahremiyet hakkını ileri sürmüş olması dikkate alındığında, davanın incelenmesinde öncelikle özel hayat kavramının mahkeme

kararları da dikkate alınarak Anayasal ve yasal açıdan değerlendirilmesi ve bu hakkın sınırlarını da ortaya koyacak şekilde çerçevesinin çizilmesi gerekmektedir.

Anayasa Mahkemesinin özel hayatın gizliliği ve mahremiyet hakkını dikkate alarak vermiş olduğu Başvuru No:2014/12591, Başvuru No:2014/11218, Başvuru No:2016/431 gibi bir çok farklı kararında şu tespitler yer almıştır.

Özel hayat kavramı eksiksiz bir tanımı bulunmayan geniş bir kavramdır. Bu kapsamda korunan hukuki değer esasen kişisel bağımsızlıktır. Özel hayata saygı hakkının kapsamının belirlenmesinde "bireyin kişiliğini geliştirmesi ve gerçekleştirilmesi" kavramı temel alınmaktadır. Anılan hak, herkesin istenmeyen bütün müdahalelerden uzak kendine özel bir ortamda yaşama hakkına sahip olduğuna işaret etmekle birlikte, kişiliğin serbestçe geliştirilmesiyle uyumlu birçok hukuki menfaati de içermektedir.(Serap Tortuk, B. No: 2013/9660, 21/1/2015, §§ 31-36; Bülent Polat [GK], B. No: 2013/7666, 10/12/2015, §§ 61-63; Tefvik Türkmen [GK], B. No: 2013/9704, 3/3/2016, §§ 50-52; Ata Türkeri, B. No: 2013/6057, 16/12/2015, §§ 30-32).

Özel hayata saygı hakkı kapsamında korunan hukuksal çıkarılardan biri de bireyin mahremiyet hakkıdır. Özel hayata saygı hakkı, ilişki kurmak ve geliştirmek üzere çevresinde bulunanlarla temas kurma hakkını da içermektedir. Kişilerin mesleki hayatı özel hayatlarıyla sıkı bir irtibat içindedir. Özel hayata dair hususlar kişinin mesleği ile ilgili tasarruflara esas alınmışsa özel hayata saygı hakkı gündeme gelecektir. (Bülent Polat, § 62; Ata Türkeri, § 31).

Gelişen teknolojinin, kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması amacıyla, kamu kesiminde kullanılmaya başlanması doğaldır. Ancak; teknoloji kullanılarak kişisel görüntülerin kayıt altına alınmasında özel hayatın gizliliği ve kişilerin mahremiyet hakkı da dikkate alınarak uygulama yapılması gerektiğinde kuşku ve duraksamaya yer bulunmamaktadır.

Buna ek olarak, kamu çalışanlarının faaliyet yürüttüğü alanlarda çalışanların çalışma alanlarını ve dolayısıyla çalışanları görecektir şekilde yerleştirilen, güvenlik ve suçun önlenmesi gibi nedenlerle uygulandığı ileri sürülen kameralı takip sistemleri kullanılarak kişisel görüntülerin alınması, temel hak ve hürriyetler içerisinde sayılan özel hayatın gizliliği ilkesi kapsamında özel hayata müdahale olarak ele alınmalı, bu müdahalenin hukuka uygunluğunun değerlendirilmesi ise kanunilik, ölçülülük gibi anayasal kavramlar yanında Avrupa İnsan Hakları Mahkemesi kararları ve Anayasa Mahkemesi kararları dikkate alınarak yapılmalıdır.

Yukarıda anılan müdahale, Anayasa'nın 13. maddesinde belirtilen koşulları yerine getirmediği müddetçe aynı zamanda Anayasa'nın 20. maddesinin ihlalini de teşkil edecektir.

Anayasa'mızın 13. maddesi "Temel hak ve hürriyetler, ... yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, ... demokratik toplum düzeninin... gereklerine ve ölçülülük ilkesine aykırı olamaz. " şeklindedir.

Bu sebeple müdahalenin ihlal oluşturup oluşturmadığının belirlenmesinde, Anayasa'nın 13. maddesinde öngörülen ve somut başvuruya uygun düşen kanunlar tarafından öngörülme, Anayasa'nın ilgili maddesinde belirtilen nedenlere dayanma, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmama koşulları yönünden inceleme yapılması gerekir.

Anayasa'nın 13. maddesi, temel hak ve özgürlüklerin sınırlandırılmasını, ilgili hak ve özgürlüğe ilişkin Anayasa maddesinde gösterilen özel sınırlandırma sebeplerinin bulunmasına bağlı kılmıştır. Bununla birlikte Anayasa Mahkemesinin kararlarına göre, özel sınırlama nedeni öngörülmemiş olan hakların dahi, hakkın doğasından kaynaklanan bazı sınırları bulunmaktadır. Ayrıca Anayasa'nın diğer maddelerinde yer alan kurallara dayanılarak da bu hakların sınırlanması mümkün olabilmektedir. Buna göre, Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebileceği kabul edilmektedir (AYM, E.2014/87, K.2015/112).

Anayasa'nın 20. maddesi "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kağıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakimın onayına sunulur. Hakim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar." hükmünü haizdir.

Anayasa'nın 20. maddesinin birinci fıkrası yönünden özel sınırlama nedeni düzenlenmemiştir. Maddenin ikinci fıkrasında, birtakım sınırlama sebeplerine yer verilmiş olmakla beraber bu sebepler sadece arama ve elkoyma tedbirlerine yöneliktir. Dolayısıyla bu sebeplerin özel hayata saygı hakkının tüm boyutları yönünden uygulanması mümkün görünmemektedir.

Bu durumda, Anayasa'nın diğer maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin somut olay bakımından sınırlandırma sebebi olarak kabul edilip edilemeyeceği araştırılmalıdır.

Anayasa'nın 5. maddesinde, "Devletin temel amaç ve görevleri, Türk Milletinin bağımsızlığını ve bütünlüğünü, ülkenin bölünmezliğini, Cumhuriyeti ve demokrasiyi korumak, kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak; kişinin temel hak ve hürriyetlerini, sosyal hukuk devleti ve adalet ilkeleriyle bağdaşmayacak surette sınırlayan siyasal, ekonomik ve sosyal engelleri kaldırmaya, insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmaktır. " denilmektedir. Buna göre kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak devletin temel amaç ve görevlerindedir.

Kişinin ve toplumun refah, huzur ve mutluluğunu sağlamanın ön koşulu milli güvenlik ve kamu düzeninin tesisidir. Milli güvenlik ve kamu düzeninin sağlanmadığı bir ortamda, hak ve özgürlüklerden gereği gibi yararlanılması, kişinin maddi ve manevi varlığını geliştirmesi mümkün değildir. Devletin hak ve özgürlükleri koruma ödevinin yanında, milli güvenliği ve kamu düzenini sağlama görevi de bulunmaktadır.

Yukarıda ifade edilen sınırlama nedenleri de dikkate alındığında uyumsuzluğun sağlıklı çözümü için; sınırlandırmanın, "demokratik toplum düzeninin gereklerinden olması" ve "ölçülülük ilkesine uygun olması"nın ne anlama geldiğinin de ortaya konması gerekmektedir.

"Demokratik toplum düzeninin gereklerinden olma, bir sınırlamanın demokratik bir toplumda zorlayıcı bir toplumsal ihtiyacın karşılanması amacına yönelik olmasını ifade etmektedir. Buna göre sınırlayıcı tedbir, bir toplumsal ihtiyacı karşılamıyorsa ya da başvurulabilecek son çare niteliğinde değilse demokratik toplum düzeninin gereklerine uygun bir tedbir olarak değerlendirilemez. (AYM, E.2015/96, K.2016/9, 10/2/2016 § 13; ifade özgürlüğü bağlamında Bekir Coşkun [GK], B. No: 2014/12151, 4/6/2015, § 51; özel hayatın gizliliği hakkı bağlamında Ata Türkeri, § 44;İ.FA., B. No: 2013/8564, 17/2/2016, § 62).

Bu kapsamda kamu makamlarının faaliyetin niteliği ve sınırlamanın amacına göre değişen geniş bir takdir yetkisinin bulunması doğaldır. Ancak özel hayatın gizliliği hakkının mahremiyet hakkı gibi en gizli yönleri söz konusu olduğunda kamu makamlarının takdir yetkisi daha dardır ve bu alanlara yönelik müdahalelerin haklı olduğunun kabul edilebilmesi için kamu makamlarınca özellikle ciddi gerekçelerin gösterilmesi gerekir. (Ata Türkeri, § 47).

Kamu makamlarının özel hayata müdahaleleriyle ilgili olarak, müdahaleye yol açan karar alma sürecinde de keyfi davranmadıklarını kanıtlamaları gereklidir. Ancak bu halde de sınırlandırmanın ölçülülük ilkesine uygun olması gereklidir. (Ata Türkeri, § 48).

Anayasa Mahkemesi kararları uyarınca ölçülülük ilkesi, sınırlayıcı önlemin öngörülen amaç için zorunlu ve amaca ulaşmaya elverişli olmasını ayrıca amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder. Ölçülülük ilkesinin amacı da temel hak ve özgürlüklerin gereğinden fazla sınırlandırılmasının önlenmesidir (AYM, E.2015/102, K.2016/151, 7/9/2016, § 22; E.2012/100, K.2013/84, 4/7/2013; Marcus Frank Cerny, B. No: 2013/5126, 2/7/2015, § 72).

Avrupa İnsan Hakları Sözleşmesi'nin "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesi şöyledir: "(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. (2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir. "

Kamu makamlarının özel hayata saygı hakkına keyfi bir şekilde müdahale etmelerinin önlenmesi, Sözleşme'nin 8. maddesi ile sağlanan güvenceler kapsamında yer almaktadır. Avrupa İnsan Hakları Mahkemesi (AİHM), devletin özel hayata saygı hakkı kapsamında bulunan bir menfaate müdahale ettiğini tespit ettiğinde, 8. maddenin ikinci fıkrasında belirtilen koşulları incelemektedir. Buna göre kamu makamlarının müdahalesinin yasal bir dayanağı olup olmadığı, anılan fıkrada yer alan meşru amaçlara dayalı olup olmadığı, demokratik bir toplumda gerekli ve öngörülen amaçla orantılı olup olmadığı araştırılmaktadır.(AİHM Dudgeon/Birleşik Krallık, § 43; Olsson/İsveç No.1, B. No: 10465/83, 24/3/1988, § 59)

Ayrıca, AİHM kararlarına göre Sözleşme'nin 8. maddesi açıkça usul şartları içermemekle birlikte anılan maddeyle güvence altına alınan haklardan etkili bir şekilde yararlanılabilmesi için müdahaleyi doğuran karar alma sürecinin bu maddeyle korunan hak ve özgürlüklere gerekli saygıyı sağlayacak nitelikte ve adil olması gerekir. Bu şekildeki bir süreç başvurusunun 8. maddedeki haklarını -deliller ve kanıtlama konuları dahil- adil şartlarda savunabileceği usule ilişkin etkili güvencelerden yararlandırılmasını gerektirir. AİHM'e göre bu şekildeki güvencelerin amacı 8. maddede yer alan haklara keyfi şekilde müdahalede bulunulmasını önlemek, müdahalenin gerekçelendirilmesini sağlamaktır (AİHM Ciubotaru/Moldova, B. No: 27138/04, 27/4/2010, § 51; T.P. ve K.M./Birleşik Krallık, B. No: 28945/95, 10/5/2001, § 72).

AİHM'e göre gerek negatif yükümlülükler gerekse pozitif yükümlülükler bakımından söz konusu usule ilişkin etkili güvencelerin sunulması gerekmektedir. (Benzer yöndeki AİHM kararı için bkz. Hokkanen/Finlandiya, B.No: 19823/92, 23/9/1994, §§ 55-58; Glaser/Birleşik Krallık, B. No: 32346/96,

19/9/2000, §§ 63-66; Bajrami/Arnavutluk, B. No: 35853/04, 12/12/2006, §§ 50-55; Abdulaziz, Cabales ve Balkandali/Birleşik Krallık, B. No: 9214/80, 28/5/1985, § 67).

Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesinin "Mahremiyet Hakkı" başlıklı 17. maddesinde de, hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemeyeceği; onuru veya itibarının hukuka aykırı saldırılara maruz bırakılmayacağına, herkesin bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahip olduğu belirtilmiştir.

Avrupa İnsan Hakları Mahkemesinin Antovic ve Mirkovic v. Sırbistan ve Karadağ (Başvuru No. 70838/13) kararında, çalıştıkları anfi alanlarına demirbaş ve öğrenciler de dahil kişi güvenliğinin sağlanması amacıyla kamera sistemi kurulan iki profesörün özel hayatlarının gizliliğinin ihlal edildiğine karar vermiştir. Kararda özellikle Avrupa İnsan Hakları Mahkemesinin daha öncede benzer konularda vermiş olduğu kararlara atıfta bulunularak bazı tespitlere de yer verilmiştir.

Bu tespitler arasında özellikle kişilerin iş yerinde ve çalışma ortamında yani kamusal bir alanda bulunsa da, özel hayatın profesyonel aktiviteler ve dış dünya ile ilişkileri de kapsayan ve Avrupa İnsan Hakları Mahkemesinin "sosyal özel hayat" olarak adlandırdığı bir alanı da kapsadığı ve bu alanın da korunması gerektiği, kamera sistemleri ile kişilerin sosyal özel hayatlarının izlenmesinin "ciddi bir müdahale" olarak kabul edilmesi gerektiği, kişilerin güvenliği veya işverenin hakları başka yollarla korunamıyorsa ancak son çare olarak kamera sistemlerinin kişilerin çalışma alanlarını göreceği şekilde kurulmasının kabul edilebilir olacağı tespitlerine yer verilmiştir. Yine Avrupa İnsan Hakları Mahkemesinin Lopez Ribalba ve Ötekiler v. İspanya (Başvuru No. 1874/13) kararında da iş verenin başka yollarla korunabilecek haklarını kamera sistemi yoluyla korumasının son çare olduğu, bu durumda bile kamera sistemleri ile ilgili olarak bildirimde bulunması ve usulleri belirlemesi gerektiği vurgulanmıştır.

Yine yukarıda yer verilen kararlardan, farklı güvenlik önlemleri yoluyla korunabilecek haklar veya önlenebilecek olaylara yönelik olarak kamera sistemleri kurulmaması gerekeceği ve çalışanların doğrudan çalışma alanlarını görüntüleme şeklinde kişilerin özel hayatına müdahale anlamına gelen bu sistemlerin bu durumlarda kullanılmaması gerekeceği, aksinin ölçülülük ilkesine aykırı olacağı sonucuna ulaşılmaktadır.

Avrupa İnsan Hakları Mahkemesi kararlarında yukarıda ifade edilen Antovic ve Mirkovic v. Sırbistan ve Karadağ (Başvuru No. 70838/13) kararında da yer aldığı gibi kamera sistemleri ile ilgili olarak belli başlı şartların ortaya konulması gerektiği de ifade edilmiştir. Bunlar özellikle uygulamanın kanuni

bir dayanağı olması, sınırlı bir izleme olması ve kötüye kullanmaya karşı garantiler olması gerektiğidir.

Türk Ceza Kanunu'nun "Özel hayatın gizliliğini ihlal" başlıklı 134. maddesi "Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.", "Kişisel verilerin kaydedilmesi" başlıklı 135. maddesi ise "Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir." hükmü yer almaktadır.

Ceza Muhakemesi Kanunu'nun "İletişimin tespiti, dinlenmesi ve kayda alınması" başlıklı 135. maddesi düzenlemesi de "başka suretle delil elde edilmesi imkânının bulunmaması durumunda" iletişimin kayda alınabileceğini, "Teknik araçlarla izleme" başlıklı 140. maddesi ise "başka suretle delil elde edilememesi hâlinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyeri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabilir" hükmü yer almakta olup, bu düzenlemeler de suça yönelik kuvvetli şüphe halinde bile en son çare olarak ses ve görüntü kaydına başvurulması gerektiğini ortaya koymaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanunu, 07.04.2016 tarihli ve 29677 Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Dava konusu işlem tarihinde yürürlükte bulunmamakla beraber konunun önemine binaen, dava konusu edilen kamera sistemleri ile ilgili belli başlı düzenlemelere de yer vermiştir. Neden bu sistemine ihtiyaç duyulduğunun ortaya konulması, sistemden kimin veya kimlerin yasal olarak sorumlu olduğunun belirlenmesi, sisteminin maksada uygun olup olmadığının ortaya konulması, özel hayatın gizliliğinin ihlal edilip edilmediğini kimin kontrol edeceğinin ve görüntülere kimin ulaşımı olacağına belirlenmesi ve bu hususların olarak kayıt altına alınması, kayıtlarının güvenliğinin ve gizliliğinin sağlanması güvenlik prosedürleri hazırlanması, kameralarla gözlemlenen bölgelerin girişinde ve içerideki uygun yerlerde bölgenin kamera sistemleri tarafından gözetlendiği ve kayıt altına alındığının belirtilmesi gerektiği, sistemin kuruluş maksadıyla bağdaşmayan görüntülerin gereğinden uzun süre saklanmaması, kişilerin özel hayatın gizliliğinin sağlanması yönünde beklentisinin olabileceği görüntülerin yetkili kişiler haricinde hiç kimse tarafından izlenememesi için alınacak önlemler gibi bir çok konuda düzenleme getirilmiştir.

Tüm bu açıklamalar ışığında dava konusu işlem incelendiğinde, Avrupa İnsan Hakları Mahkemesi kararları da dikkate alındığında hakların korunması başka şekilde sağlanamıyorsa kamera sistemlerinin çalışanların çalışma alanlarını görecektir şekilde kurulmasının mümkün olduğu ancak bunun bir son çare olarak değerlendirildiği ve bu düzenlemenin içeriğini ayrıntılı olarak ortaya koyan bir özel düzenleyici işlem olması gerektiği, kamera sistemlerinin çalışma alanlarını çekmesinin özel

hayatın gizliliğini ihlal ettiği, sınırlı bir izleme sağlayacak şekilde güvenlik amacıyla giriş ve çıkışları izlemek üzere veya vatandaşlara da açık olan ortak alanlar ve iş sahiplerinin de giriş çıkışına açık, yoğun bir alış veriş trafiği olan alanlarda kurulabileceği ancak bu kameraların da çalışanların iş yapış şekillerini denetlemek veya sürekli olarak belli kişileri çekecek şekilde kurulmaması gerektiği, güvenlik amacıyla kurulmuş olmaları gerektiği ve bu nedenle amaca hizmet eder şekilde konumlandırılması gerektiği anlaşılmaktadır.

Yine kamera sistemlerinin zorunlu güvenlik amacı ile ve başka bir yolla bu güvenlik amacı sağlanamıyorsa kurulabilmesi mümkün olsa da, yukarıda yer verilen açıklamalar ışığında uygulamanın usul ve esaslarını gösteren yasal dayanağının bulunması, açık ve anlaşılabilir olması ve ilgililerin bu konudaki hakları ve kamera sistemi ile ilgili olarak bilgilendirilmiş olması gerektiği, toplanan görüntülerle ilgili güvencelerin sağlanması gerektiği, dava konusu işlemin bu haliyle sınırları belirlenmemiş, yasal dayanağı olmayan, uygulamaya dair usul ve esaslar ile güvenceleri düzenlenmemiş bir sistemle yürütüldüğü ve bu haliyle kamu yararına yönelik olduğunu kabul etmeye imkan olmadığı; Anayasal bir ilke olan ölçülülük ilkesine aykırılık teşkil ettiği ve mahremiyet hakkını ihlal ettiği anlaşılmakta olup, kişilik haklarına aykırı şekilde kamu görevlilerinin tüm faaliyetlerinin izlenmesine imkan tanıyan uygulamada isabet bulunmamaktadır.

Kameralı takip sistemi ile kurumca amaçlanan kamu yararı arasında orantılılık bulunmadığından uygulama ölçülülük ilkesine de aykırılık teşkil etmektedir. Anayasa'nın 13. maddesinde, temel hak ve hürriyetlerin ancak kanunla sınırlanabileceği, değişik 20/3. maddesinde de, kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceğinin belirtildiği, ancak konuyla ilgili dava konusu işlemin gerçekleştirildiği aşamada yasal bir düzenlemenin yapılmadığı anlaşılmaktadır.

İdarelerin teknolojik gelişmelerden de yararlanarak kamu çalışanlarının faaliyet yürüttüğü alanda güvenlik ve suçun önlenmesi amacıyla kameralı takip sistemi uygulamasının, güvenlik amaçlı olarak giriş ve çıkışlar ve güvenliğin özel önem arz ettiği alanlar dışında, günlük iş ve işlemleri yürüten çalışanların çalışma odalarını ve servisleri çekecek şekilde yerleştirildiği durumlarda, kamusal alanda da olsa "özel hayatın gizliliği" ilkesi kapsamında bulunduğu Avrupa İnsan Hakları Mahkemesi kararları ve Dairemizin daha önceki tarihli kararlarından anlaşılmaktadır. Yine uygulamanın sınırlarını, usul ve esaslarını gösteren bir yasal dayanağın bulunması, toplanan görüntülerin ileride başka bir şekilde kullanılmayacağına dair bir güvencenin mevcut olması gerektiği de anlaşılmaktadır.

İdarenin güvenlik ve kamu yararını sağlama ihtiyacı ve çalışanların özel hayatın gizliliği gibi haklarının karşı karşıya geldiği bu gibi uyuşmazlıklarda, olayın dosyaya özel olarak ele alınması ve değerlendirilmesi gerektiği açıktır.

Uyuşmazlığın bu davaya özgü hali değerlendirildiğinde; hizmet binaları içerisinde mevcut kamera ile izleme sisteminin risk oluşturmayan birim ve bölgelerde kaldırılması istemiyle davacı sendika tarafından başvuru yapıldığı anlaşılmakta olup; uygulamanın sınırlarını, usul ve esaslarını gösteren bir yasal dayanağın bulunmaması, toplanan görüntülerin ileride başka bir şekilde kullanılmayacağına dair bir güvencenin mevcut olmaması ve üniversite alanı içinde giriş ve çıkışlar gibi güvenlik açısından önem arz eden alanların halihazırda kamera sistemleri ile izlendiği, anfi ve derslikler gibi alanlara yerleştirilen kameraların iş yerinin güvenliğini sağlama amacını aşarak, doğrudan çalışan memurun kendisinin, diğer memurlarla ya da iş sahipleriyle ve dava konusu uyuşmazlık açısından öğrenciler ve öğretim görevlilerin ilişkisinin ve iletişiminin ve kamu hizmetinin görülmesi sırasında yapılan her türlü haberleşmesinin gözlemlendiği kamera takip sisteminin kurulmasının özel hayatın gizliliğini ihlal ettiği ve bu haliyle yukarıda belirtilen temel haklar ve Anayasal ilkelerle bağdaşmaması nedeniyle dava konusu işlemin iptaline karar verilmesi gerekirken davanın reddi yolunda verilen mahkeme kararının hukuka aykırı olduğu sonucuna varılmıştır.

Açıklanan nedenlerle, temyiz isteminin kabulüyle, Kırıkkale İdare Mahkemesi'nin 12/03/2015 tarih ve E:2014/543, K:2015/162 sayılı kararının BOZULMASINA, yeniden bir karar verilmek üzere dosyanın adı geçen mahkemeye gönderilmesine, 2577 sayılı Kanun'un (Geçici 8. maddesi uyarınca uygulanmasına devam edilen) 54. maddesinin 1. fıkrası uyarınca bu kararın tebliğ tarihini izleyen günden itibaren onbeş gün içinde karar düzeltme yolu açık olmak üzere, 14/05/2018 tarihinde oybirliğiyle karar verildi.

Danıştay Kararı - 10. Daire (E. 2015/2787)

Danıştay Kararı - 10. D., E. 2015/2787 K. 2018/775 T. 20.2.2018

İstemin Özeti: Eskişehir 1. İdare Mahkemesi'nin davanın reddi yolunda verilen 30/04/2015 tarih ve E:2014/1039, K:2015/540 sayılı kararının hukuka uygun olmadığı ileri sürülerek temyizden incelenerek bozulması davacı sendika tarafından istenilmektedir.

Savunmanın Özeti: Temyiz isteminin reddi gerektiği savunulmaktadır.

Danıştay Tetkik Hakimi: K1

Düşüncesi: İdare Mahkemesi kararının bozulması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Hüküm veren Danıştay Onuncu Dairesi'nce gereği görüldü:

Dava; Eskişehir Vergi Dairesi Başkanlığı bünyesinde kamu çalışanlarının faaliyet yürüttüğü servislere bakacak şekilde uygulanan kameralı takip sisteminin güvenlik amacıyla binaların girişlerine yerleştirilenler dışında, çalışanların izlenmesine imkan veren kamera sisteminin kişi mahremiyetini ihlal edeceği ileri sürülerek, personelin izlenmesine imkan veren kamera sisteminin kaldırılması talebiyle yapılan başvurunun reddine dair 01/09/2014 tarih ve 6499 sayılı işleminiptali istemiyle açılmıştır.

Eskişehir 1. İdare Mahkemesi'nce; dosyaya sunulan fotoğraflar ve davalı idarenin savunması dikkate alınarak personelin çalıştığı kapalı alanlarda herhangi bir kameranın bulunmadığı, açık alanlar ve ziyaretçi yoğunluğunun bulunduğu alanlarla kamu hizmeti alan ve verenlerin birlikte buldukları alanlarda kamera kaydı alındığı, kamera kayıtlarının ise güvenlik hizmeti ile bağlantısı olmayan hiçbir yönetici veya personel tarafından görülmesinin mümkün olmadığı, sistemde bulunan verilerin sadece kurum bünyesinde bulunduğu ve en fazla 20 gün geriye dönük kayıtların saklandığı, bu itibarla yapılan uygulamanın meşru, kurum güvenlik amacına uygun ve bu amaçla sınırlı olduğu, bu haliyle söz konusu uygulamanın özel hayatın gizliliğini ihlal ettiğinden bahsedilemeyeceği, aksine kamu hizmetinin verildiği ve alındığı alanın güvenliği için gerekli olduğu anlaşılacakla, Eskişehir Vergi Dairesi Başkanlığı bünyesinde kamu çalışanlarının faaliyet yürüttüğü servislerde uygulanan kameralı takip sistemine son verilmesi yolunda davacı Sendika tarafından yapılan başvurunun

reddine dair 01/09/2014 tarih ve 6499 sayılı işlemde hukuka aykırılık bulunmadığı gerekçeleriyle davanın reddine karar verilmiştir.

Davacı sendika tarafından, yapılan uygulamanın ve tesis edilen işlemin çalışanların özel hayatının gizliliğini ihlal ettiği ve bu nedenle hukuka aykırı olduğu ileri sürülerek İdare Mahkemesi kararının temyizden incelenerek bozulması istenilmektedir.

Davacı sendikanın temyiz gerekçesi olarak özel hayatın gizliliği ve mahremiyet hakkını ileri sürmüş olması dikkate alındığında, davanın incelenmesinde öncelikle özel hayat kavramının mahkeme kararları da dikkate alınarak Anayasal ve yasal açıdan değerlendirilmesi ve bu hakkın sınırlarını da ortaya koyacak şekilde çerçevesinin çizilmesi gerekmektedir.

Anayasa Mahkemesinin özel hayatın gizliliği ve mahremiyet hakkını dikkate alarak vermiş olduğu Başvuru No:2014/12591, Başvuru No:2014/11218, Başvuru No:2016/431 gibi bir çok farklı kararında şu tespitler yer almıştır.

Özel hayat kavramı eksiksiz bir tanımı bulunmayan geniş bir kavramdır. Bu kapsamda korunan hukuki değer esasen kişisel bağımsızlıktır. Özel hayata saygı hakkının kapsamının belirlenmesinde "bireyin kişiliğini geliştirmesi ve gerçekleştirilmesi" kavramı temel alınmaktadır. Anılan hak, herkesin istenmeyen bütün müdahalelerden uzak kendine özel bir ortamda yaşama hakkına sahip olduğuna işaret etmekle birlikte, kişiliğin serbestçe geliştirilmesiyle uyumlu birçok hukuki menfaati de içermektedir.(Serap Tortuk, B. No: 2013/9660, 21/1/2015, §§ 31-36; Bülent Polat [GK], B. No: 2013/7666, 10/12/2015, §§ 61-63; Tefvik Türkmen [GK], B. No: 2013/9704, 3/3/2016, §§ 50-52; Ata Türkeri, B. No: 2013/6057, 16/12/2015, §§ 30-32)

Özel hayata saygı hakkı kapsamında korunan hukuksal çıkarılardan biri de bireyin mahremiyet hakkıdır. Özel hayata saygı hakkı, ilişki kurmak ve geliştirmek üzere çevresinde bulunanlarla temas kurma hakkını da içermektedir. Kişilerin mesleki hayatı özel hayatlarıyla sıkı bir irtibat içindedir. Özel hayata dair hususlar kişinin mesleği ile ilgili tasarruflara esas alınmışsa özel hayata saygı hakkı gündeme gelecektir. (Bülent Polat, § 62; Ata Türkeri, § 31)

Gelişen teknolojinin, kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması amacıyla, kamu kesiminde kullanılmaya başlanması doğaldır. Ancak; teknoloji kullanılarak kişisel görüntülerin kayıt altına alınmasında özel hayatın gizliliği ve kişilerin mahremiyet hakkı da dikkate alınarak uygulama yapılması gerektiğinde kuşku ve duraksamaya yer bulunmamaktadır.

Buna ek olarak, kamu çalışanlarının faaliyet yürüttüğü servislerde çalışanların çalışma alanlarını ve dolayısıyla çalışanları görecektir şekilde yerleştirilen, güvenlik ve suçun önlenmesi gibi nedenlerle

uygulandığı ileri sürülen kameralı takip sistemleri kullanılarak kişisel görüntülerin alınması, temel hak ve hürriyetler içerisinde sayılan özel hayatın gizliliği ilkesi kapsamında özel hayata müdahale olarak ele alınmalı, bu müdahalenin hukuka uygunluğunun değerlendirilmesi ise kanunilik, ölçülülük gibi anayasal kavramlar yanında Avrupa İnsan Hakları Mahkemesi kararları ve Anayasa Mahkemesi kararları dikkate alınarak yapılmalıdır.

Yukarıda anılan müdahale, Anayasa'nın 13. maddesinde belirtilen koşulları yerine getirmediği müddetçe aynı zamanda Anayasa'nın 20. maddesinin ihlalini de teşkil edecektir.

Anayasa'nın 13. maddesi, "Temel hak ve hürriyetler, ... yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, ... demokratik toplum düzeninin... gereklerine ve ölçülülük ilkesine aykırı olamaz." şeklindedir.

Bu sebeple müdahalenin ihlal oluşturup oluşturmadığının belirlenmesinde, Anayasa'nın 13. maddesinde öngörülen ve somut başvuruya uygun düşen kanunlar tarafından öngörülme, Anayasa'nın ilgili maddesinde belirtilen nedenlere dayanma, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmama koşulları yönünden inceleme yapılması gerekir.

Anayasa'nın 13. maddesi, temel hak ve özgürlüklerin sınırlandırılmasını, ilgili hak ve özgürlüğe ilişkin Anayasa maddesinde gösterilen özel sınırlandırma sebeplerinin bulunmasına bağlı kılmıştır. Bununla birlikte Anayasa Mahkemesinin kararlarına göre, özel sınırlama nedeni öngörülmemiş olan hakların dahi, hakkın doğasından kaynaklanan bazı sınırları bulunmaktadır. Ayrıca Anayasa'nın diğer maddelerinde yer alan kurallara dayanılarak da bu hakların sınırlanması mümkün olabilmektedir. Buna göre, Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebileceği kabul edilmektedir. (AYM, E.2014/87, K.2015/112)

Anayasa'nın 20. maddesi "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kağıtları ve eşyası aranmaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakim onayına sunulur. Hakim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar." hükmünü haizdir.

Anayasa'nın 20. maddesinin 1. fıkrası yönünden özel sınırlama nedeni düzenlenmemiştir. Maddenin ikinci fıkrasında, birtakım sınırlama sebeplerine yer verilmiş olmakla beraber bu sebepler sadece arama ve elkoyma tedbirlerine yöneliktir. Dolayısıyla bu sebeplerin özel hayata saygı hakkının tüm boyutları yönünden uygulanması mümkün görünmemektedir.

Bu durumda, Anayasa'nın diğer maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin somut olay bakımından sınırlandırma sebebi olarak kabul edilip edilemeyeceği araştırılmalıdır.

Anayasa'nın 5. maddesinde, "Devletin temel amaç ve görevleri, Türk Milletinin bağımsızlığını ve bütünlüğünü, ülkenin bölünmezliğini, Cumhuriyeti ve demokrasiyi korumak, kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak; kişinin temel hak ve hürriyetlerini, sosyal hukuk devleti ve adalet ilkeleriyle bağdaşmayacak surette sınırlayan siyasal, ekonomik ve sosyal engelleri kaldırmaya, insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmaktır." denilmektedir. Buna göre kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak devletin temel amaç ve görevlerindedir.

Kişinin ve toplumun refah, huzur ve mutluluğunu sağlamanın ön koşulu milli güvenlik ve kamu düzeninin tesisidir. Milli güvenlik ve kamu düzeninin sağlanmadığı bir ortamda, hak ve özgürlüklerden gereği gibi yararlanılması, kişinin maddi ve manevi varlığını geliştirmesi mümkün değildir. Devletin hak ve özgürlükleri koruma ödevinin yanında, milli güvenliği ve kamu düzenini sağlama görevi de bulunmaktadır.

Yukarıda ifade edilen sınırlama nedenleri de dikkate alındığında uyumsuzluğun sağlıklı çözümü için; sınırlandırmanın, "demokratik toplum düzeninin gereklerinden olması" ve "ölçülülük ilkesine uygun olması"nın ne anlama geldiğinin de ortaya konması gerekmektedir.

"Demokratik toplum düzeninin gereklerinden olma, bir sınırlamanın demokratik bir toplumda zorlayıcı bir toplumsal ihtiyacın karşılanması amacına yönelik olmasını ifade etmektedir. Buna göre sınırlayıcı tedbir, bir toplumsal ihtiyacı karşılamıyorsa ya da başvurulabilecek son çare niteliğinde değilse demokratik toplum düzeninin gereklerine uygun bir tedbir olarak değerlendirilemez. (AYM, E.2015/96, K.2016/9, 10/2/2016 § 13; ifade özgürlüğü bağlamında Bekir Coşkun [GK], B. No: 2014/12151, 4/6/2015, § 51; özel hayatın gizliliği hakkı bağlamında Ata Türkeri, § 44; İ.F.A., B. No: 2013/8564, 17/2/2016, § 62)

Bu kapsamda kamu makamlarının faaliyetin niteliği ve sınırlamanın amacına göre değişen geniş bir takdir yetkisinin bulunması doğaldır. Ancak özel hayatın gizliliği hakkının mahremiyet hakkı gibi en

gizli yönleri söz konusu olduğunda kamu makamlarının takdir yetkisi daha dardır ve bu alanlara yönelik müdahalelerin haklı olduğunun kabul edilebilmesi için kamu makamlarınca özellikle ciddi gerekçelerin gösterilmesi gerekir. (Ata Türkeri, § 47)

Kamu makamlarının özel hayata müdahaleleriyle ilgili olarak, müdahaleye yol açan karar alma sürecinde de keyfi davranmadıklarını kanıtlamaları gereklidir. Ancak bu halde de sınırlandırmanın ölçülülük ilkesine uygun olması gereklidir. (Ata Türkeri, § 48)

Anayasa Mahkemesi kararları uyarınca ölçülülük ilkesi, sınırlayıcı önlemin öngörülen amaç için zorunlu ve amaca ulaşmaya elverişli olmasını ayrıca amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder. Ölçülülük ilkesinin amacı da temel hak ve özgürlüklerin gereğinden fazla sınırlandırılmasının önlenmesidir (AYM, E.2015/102, K.2016/151, 7/9/2016, § 22; E.2012/100, K.2013/84, 4/7/2013; Marcus Frank Cerny, B. No: 2013/5126, 2/7/2015, § 72)

Avrupa İnsan Hakları Sözleşmesi'nin "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesi şöyledir: "(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. (2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir. "

Kamu makamlarının özel hayata saygı hakkına keyfi bir şekilde müdahale etmelerinin önlenmesi, Sözleşme'nin 8. maddesi ile sağlanan güvenceler kapsamında yer almaktadır. Avrupa İnsan Hakları Mahkemesi (AİHM), devletin özel hayata saygı hakkı kapsamında bulunan bir menfaate müdahale ettiğini tespit ettiğinde, 8. maddenin ikinci fıkrasında belirtilen koşulları incelemektedir. Buna göre kamu makamlarının müdahalesinin yasal bir dayanağı olup olmadığı, anılan fıkrada yer alan meşru amaçlara dayalı olup olmadığı, demokratik bir toplumda gerekli ve öngörülen amaçla orantılı olup olmadığı araştırılmaktadır. (AİHM Dudgeon/Birleşik Krallık, § 43; Olsson/İsveç No.1, B. No: 10465/83, 24/3/1988, § 59)

Ayrıca, AİHM kararlarına göre Sözleşme'nin 8. maddesi açıkça usul şartları içermemekle birlikte anılan maddeyle güvence altına alınan haklardan etkili bir şekilde yararlanılabilmesi için müdahaleyi doğuran karar alma sürecinin bu maddeyle korunan hak ve özgürlüklere gerekli saygıyı sağlayacak nitelikte ve adil olması gerekir. Bu şekildeki bir süreç başvurusunun 8. maddedeki haklarını -deliller ve kanıtlanma konuları dahil- adil şartlarda savunabileceği usule ilişkin etkili güvencelerden yararlandırılmasını gerektirir. AİHM'e göre bu şekildeki güvencelerin amacı 8. maddede yer alan haklara keyfi şekilde müdahalede bulunulmasını önlemek, müdahalenin gerekçelendirilmesini

sağlamaktır (AİHM Ciubotaru/Moldova, B. No: 27138/04, 27/4/2010, § 51; T.P. ve K.M./Birleşik Krallık, B. No: 28945/95, 10/5/2001, § 72)

AİHM'e göre gerek negatif yükümlülükler gerekse pozitif yükümlülükler bakımından söz konusu usule ilişkin etkili güvencelerin sunulması gerekmektedir. (Benzer yöndeki AİHM kararı için bkz. Hokkanen/Finlandiya, B.No: 19823/92, 23/9/1994, §§ 55-58; Glaser/Birleşik Krallık, B. No: 32346/96, 19/9/2000, §§ 63-66; Bajrami/Arnavutluk, B. No: 35853/04, 12/12/2006, §§ 50-55; Abdulaziz, Cabales ve Balkandali/Birleşik Krallık, B. No: 9214/80, 28/5/1985, § 67)

Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesinin "Mahremiyet Hakkı" başlıklı 17. maddesinde de, hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemeyeceği; onuru veya itibarının hukuka aykırı saldırılara maruz bırakılmayacağına, herkesin bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahip olduğu belirtilmiştir.

Avrupa İnsan Hakları Mahkemesinin Antovic ve Mirkovic v. Sırbistan ve Karadağ (Başvuru No. 70838/13) kararında, çalıştıkları anfi alanlarına demirbaş ve öğrenciler de dahil kişi güvenliğinin sağlanması amacıyla kamera sistemi kurulan iki profesörün özel hayatlarının gizliliğinin ihlal edildiğine karar vermiştir. Kararda özellikle Avrupa İnsan Hakları Mahkemesinin daha öncede benzer konularda vermiş olduğu kararlara atıfta bulunularak bazı tespitlere de yer verilmiştir.

Bu tespitler arasında özellikle kişilerin iş yerinde ve çalışma ortamında yani kamusal bir alanda bulunsa da, özel hayatın profesyonel aktiviteler ve dış dünya ile ilişkileri de kapsayan ve Avrupa İnsan Hakları Mahkemesinin "sosyal özel hayat" olarak adlandırdığı bir alanı da kapsadığı ve bu alanın da korunması gerektiği, kamera sistemleri ile kişilerin sosyal özel hayatlarının izlenmesinin "ciddi bir müdahale" olarak kabul edilmesi gerektiği, kişilerin güvenliği veya işverenin hakları başka yollarla korunamıyorsa ancak son çare olarak kamera sistemlerinin kişilerin çalışma alanlarını görecektir şekilde kurulmasının kabul edilebilir olacağı tespitlerine yer verilmiştir. Yine Avrupa İnsan Hakları Mahkemesinin Lopez Ribalba ve Ötekiler v. İspanya (Başvuru No. 1874/13) kararında da iş verenin başka yollarla korunabilecek haklarını kamera sistemi yoluyla korumasının son çare olduğu, bu durumda bile kamera sistemleri ile ilgili olarak bildirimde bulunması ve usulleri belirlemesi gerektiği vurgulanmıştır.

Yine yukarıda yer verilen kararlardan, farklı güvenlik önlemleri yoluyla korunabilecek haklar veya önlenilecek olaylara yönelik olarak kamera sistemleri kurulmaması gerekeceği ve çalışanların doğrudan çalışma alanlarını görüntüleme şeklinde kişilerin özel hayatına müdahale anlamına gelen

bu sistemlerin bu durumlarda kullanılmaması gerekeceği, aksinin ölçülülük ilkesine aykırı olacağı sonucuna ulaşılmaktadır.

Avrupa İnsan Hakları Mahkemesi kararlarında yukarıda ifade edilen Antovic ve Mirkovic v. Sırbistan ve Karadağ (Başvuru No. 70838/13) kararında da yer aldığı gibi kamera sistemleri ile ilgili olarak belli başlı şartların ortaya konulması gerektiği de ifade edilmiştir. Bunlar özellikle uygulamanın kanuni bir dayanağı olması, sınırlı bir izleme olması ve kötüye kullanmaya karşı garantiler olması gerektiğidir.

5237 sayılı Türk Ceza Kanunu'nun "Özel hayatın gizliliğini ihlal" başlıklı 134. maddesinde, "Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.", "Kişisel verilerin kaydedilmesi" başlıklı 135. maddesinde ise "Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir." hükmü yer almaktadır.

5271 sayılı Ceza Muhakemesi Kanunu'nun "İletişimin tespiti, dinlenmesi ve kayda alınması" başlıklı 135. maddesi düzenlemesinde "başka suretle delil elde edilmesi imkânının bulunmaması durumunda" iletişimin kayda alınabileceği, "Teknik araçlarla izleme" başlıklı 140. maddesi ise, "başka suretle delil elde edilememesi hâlinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyeri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabilir." hükmü yer almakta olup, bu düzenlemeler de suça yönelik kuvvetli şüphe halinde bile en son çare olarak ses ve görüntü kaydına başvurulması gerektiğini ortaya koymaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanunu, 07/04/2016 tarihli ve 29677 Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Dava konusu işlem tarihinde yürürlükte bulunmamakla beraber konunun önemine binaen, dava konusu edilen kamera sistemleri ile ilgili belli başlı düzenlemelere de yer vermiştir. Neden bu sistemine ihtiyaç duyulduğunun ortaya konulması, sistemden kimin veya kimlerin yasal olarak sorumlu olduğunun belirlenmesi, sisteminin maksada uygun olup olmadığının ortaya konulması, özel hayatın gizliliğinin ihlal edilip edilmediğini kimin kontrol edeceğinin ve görüntülere kimin ulaşımı olacağına belirlenmesi ve bu hususların olarak kayıt altına alınması, kayıtlarının güvenliğinin ve gizliliğinin sağlanması güvenlik prosedürleri hazırlanması, kameralarla gözlemlenen bölgelerin girişinde ve içerideki uygun yerlerde bölgenin kamera sistemleri tarafından gözetlendiği ve kayıt altına alındığının belirtilmesi gerektiği, sistemin kuruluş maksadıyla bağdaşmayan görüntülerin gereğinden uzun süre saklanmaması, kişilerin özel hayatın gizliliğinin sağlanması yönünde beklentisinin olabileceği görüntülerin yetkili kişiler haricinde hiç kimse tarafından izlenememesi için alınacak önlemler gibi bir çok konuda düzenleme getirilmiştir.

Tüm bu açıklamalar ışığında dava konusu işlem incelendiğinde, Avrupa İnsan Hakları Mahkemesi kararları da dikkate alındığında hakların korunması başka şekilde sağlanamıyorsa kamera sistemlerinin çalışanların çalışma alanlarını görecektir şekilde kurulmasının mümkün olduğu ancak bunun bir son çare olarak değerlendirildiği ve bu düzenlemenin içeriğini ayrıntılı olarak ortaya koyan bir özel düzenleyici işlem olması gerektiği, kamera sistemlerinin çalışma alanlarını çekmesinin özel hayatın gizliliğini ihlal ettiği, sınırlı bir izleme sağlayacak şekilde güvenlik amacıyla giriş ve çıkışları izlemek üzere veya vatandaşlara da açık olan ortak alanlar ve iş sahiplerinin de giriş çıkışına açık, yoğun bir alışveriş trafiği olan alanlarda kurulabileceği ancak bu kameraların da çalışanların iş yapış şekillerini denetlemek veya sürekli olarak belli kişileri çekecek şekilde kurulmaması gerektiği, güvenlik amacıyla kurulmuş olmaları gerektiği ve bu nedenle amaca hizmet eder şekilde konumlandırılması gerektiği anlaşılmaktadır.

Yine kamera sistemlerinin zorunlu güvenlik amacı ile ve başka bir yolla bu güvenlik amacı sağlanamıyorsa kurulabilmesi mümkün olsa da, yukarıda yer verilen açıklamalar ışığında uygulamanın usul ve esaslarını gösteren yasal dayanağının bulunması, açık ve anlaşılabilir olması ve ilgililerin bu konudaki hakları ve kamera sistemi ile ilgili olarak bilgilendirilmiş olması gerektiği, toplanan görüntülerle ilgili güvencelerin sağlanması gerektiği, dava konusu işlemin bu haliyle sınırları belirlenmemiş, yasal dayanağı olmayan, uygulamaya dair usul ve esaslar ile güvenceleri düzenlenmemiş bir sistemle yürütüldüğü ve bu haliyle kamu yararına yönelik olduğunu kabul etmeye imkan olmadığı; Anayasal bir ilke olan ölçülülük ilkesine aykırılık teşkil ettiği ve mahremiyet hakkını ihlal ettiği anlaşılmakta olup, kişilik haklarına aykırı şekilde kamu görevlilerinin tüm faaliyetlerinin izlenmesine imkan tanıyan uygulamada isabet bulunmamaktadır.

Kameralı takip sistemi ile kurumca amaçlanan kamu yararı arasında orantılılık bulunmadığından uygulama ölçülülük ilkesine de aykırılık teşkil etmektedir. Anayasa'nın 13. maddesinde, temel hak ve hürriyetlerin ancak kanunla sınırlanabileceği, değişik 20/3. maddesinde de, kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceğinin belirtildiği, ancak konuyla ilgili dava konusu işlemin gerçekleştirildiği aşamada yasal bir düzenlemenin yapılmadığı anlaşılmaktadır.

İdarelerin teknolojik gelişmelerden de yararlanarak kamu çalışanlarının faaliyet yürüttüğü alanda güvenlik ve suçun önlenmesi amacıyla kameralı takip sistemi uygulamasının, güvenlik amaçlı olarak giriş ve çıkışlar ve güvenliğin özel önem arz ettiği alanlar dışında, günlük iş ve işlemleri yürüten çalışanların çalışma odalarını ve servisleri çekecek şekilde yerleştirildiği durumlarda, kamusal alanda da olsa "özel hayatın gizliliği" ilkesi kapsamında bulunduğu Avrupa İnsan Hakları Mahkemesi

kararları ve Dairemizin daha önceki tarihli kararlarından anlaşılmaktadır. Yine uygulamanın sınırlarını, usul ve esaslarını gösteren bir yasal dayanağın bulunması, toplanan görüntülerin ileride başka bir şekilde kullanılmayacağına dair bir güvencenin mevcut olması gerektiği de anlaşılmaktadır.

İdarenin güvenlik ve kamu yararını sağlama ihtiyacı ve çalışanların özel hayatın gizliliği gibi haklarının karşı karşıya geldiği bu gibi uyuşmazlıklarda, olayın dosyaya özel olarak ele alınması ve değerlendirilmesi gerektiği açıktır.

Uyuşmazlığın bu davaya özgü hali değerlendirildiğinde, dava dosyasında yer alan kamera konumlarına dair fotoğraflar incelendiğinde doğrudan servis görevlilerinin çalışma alanlarının üzerine yerleştirilen ve vatandaşların geçişine imkan bulunmayan bu alanları çeken kameraların da olduğu görülmekte olup İdare Mahkemesi kararında bu kameraların dikkate alınmadığı, yine davalı idarenin görüntüleri kimlerin izleyebileceği, saklanma süresi gibi açıklamaları ile ilgili bir dayanak sunulmadığı, herhangi bir düzenleme olmadığı ve başka şekilde uygulamalar yapılmasının mümkün olduğu, görüntülerin farklı şekillerde kullanılmasının önlenmesi yönünde ve görüntüsü çekilenlerin haklarının korunması adına önleyici bir usul bulunmadığı dikkate alınmadan ve bu konularda ek bir inceleme yapılmadan davalı idarenin savunmasında yer alan bu hususların karar gerekçesine dayanak alındığı da görülmektedir.

Açıklanan nedenlerle, temyiz isteminin kabulüyle, Eskişehir 1. İdare Mahkemesi'nin 30/04/2015 tarih ve E:2014/1039, K:2015/540 sayılı kararının BOZULMASINA, yeniden bir karar verilmek üzere dosyanın adı geçen mahkemeye gönderilmesine, 2577 sayılı Kanun'un (Geçici 8. maddesi uyarınca uygulanmasına devam edilen) 54. maddesinin 1. fıkrası uyarınca bu kararın tebliğ tarihini izleyen günden itibaren onbeş gün içinde karar düzeltme yolu açık olmak üzere, 20/02/2018 tarihinde oybirliğiyle karar verildi.

Danıştay Kararı - 10. Daire (E. 2015/2696)

Danıştay Kararı - 10. D., E. 2015/2696 K. 2018/776 T. 20.2.2018

İstemın Özeti: Ankara 11. İdare Mahkemesi'nin 07/11/2014 tarih ve E:2014/610, K:2014/1501 sayılı kararının hukuka uygun olmadığı ileri sürülerek temyizen incelenerek bozulması davacı sendika tarafından istenilmektedir.

Savunmanın Özeti : Savunma verilmemiştir.

Danıştay Tetkik Hakimi: K1

Düşüncesi: İdare Mahkemesi kararının bozulması gerektiği düşünülmektedir.

TÜRK MİLLETİ ADINA

Hüküm veren Danıştay Onuncu Dairesi'nce gereği görüldü:

Dava, davacı sendika tarafından, davalı idarenin taşra birimlerinde görev yapan personelin izlenmesini teminen odalarına monitor yerleştirildiği ve kamera kayıt sisteminin kurulduğu, güvenlik amacıyla binaların girişlerine yerleştirilenler dışında çalışanların birimlerde (odalarda) izlenmesine imkan veren kamera sisteminin kişi mahremiyetini ihlal edeceği ileri sürülerek, personelin izlenmesine imkan veren kamera sisteminin kaldırılması talebiyle 5/12/2013 tarih ve 825 sayılı dilekçe ile yapılan başvurunun zımnen reddine yönelik davalı idare işleminin iptali istemiyle açılmıştır.

Ankara 11. İdare Mahkemesi'nce; davalı idarenin kaçakçılıkla mücadele kapsamında 5607 sayılı Kanun kapsamında bir takım yükümlülüklerinin bulunduğu, kapalı devre kamera sisteminin bu yükümlülüğün yerine getirilmesi ve görevin önem ve özelliği dikkate alınarak gümrük idarelerinin takibi amacıyla kurulduğu, bu kapsamda hizmet binalarının koridor, giriş-çıkış ve mükelleflerin yoğun olduğu bölümlerine kapalı devre kamera sistemi kurulmasının kamu yararını gerçekleştirme amacına uygun olduğu, dolayısıyla Anayasa'nın 20. maddesi ile güvence altına alınan özel hayatın gizliliğinin ihlalinin söz konusu olmadığı, kamu yararı ve hizmet gereklerine uygun olduğu, yapılan işlemde hukuka ve mevzuata aykırılık bulunmadığı gerekçeleriyle davanın reddine karar verilmiştir.

Davacı sendika tarafından, yapılan uygulamanın ve tesis edilen işlemin çalışanların özel hayatının gizliliğini ihlal ettiği ve bu nedenle hukuka aykırı olduğu ileri sürülerek İdare Mahkemesi kararının temyizen incelenerek bozulması istenilmektedir.

Davacı sendikanın temyiz gerekçesi olarak özel hayatın gizliliği ve mahremiyet hakkını ileri sürmüş olması dikkate alındığında, davanın incelenmesinde öncelikle özel hayat kavramının mahkeme kararları da dikkate alınarak Anayasal ve yasal açıdan değerlendirilmesi ve bu hakkın sınırlarını da ortaya koyacak şekilde çerçevesinin çizilmesi gerekmektedir.

Anayasa Mahkemesinin özel hayatın gizliliği ve mahremiyet hakkını dikkate alarak vermiş olduğu Başvuru No:2014/12591, Başvuru No:2014/11218, Başvuru No:2016/431 gibi bir çok farklı kararında şu tespitler yer almıştır.

Özel hayat kavramı eksiksiz bir tanımla bulunmayan geniş bir kavramdır. Bu kapsamda korunan hukuki değer esasen kişisel bağımsızlıktır. Özel hayata saygı hakkının kapsamının belirlenmesinde "bireyin kişiliğini geliştirmesi ve gerçekleştirilmesi" kavramı temel alınmaktadır. Anılan hak, herkesin istenmeyen bütün müdahalelerden uzak kendine özel bir ortamda yaşama hakkına sahip olduğuna işaret etmekle birlikte, kişiliğin serbestçe geliştirilmesiyle uyumlu birçok hukuki menfaati de içermektedir.(Serap Tortuk, B. No: 2013/9660, 21/1/2015, §§ 31-36; Bülent Polat [GK], B. No: 2013/7666, 10/12/2015, §§ 61-63; Tefvik Türkmen [GK], B. No: 2013/9704, 3/3/2016, §§ 50-52; Ata Türkeri, B. No: 2013/6057, 16/12/2015, §§ 30-32)

Özel hayata saygı hakkı kapsamında korunan hukuksal çıkarılardan biri de bireyin mahremiyet hakkıdır. Özel hayata saygı hakkı, ilişki kurmak ve geliştirmek üzere çevresinde bulunanlarla temas kurma hakkını da içermektedir. Kişilerin mesleki hayatı özel hayatlarıyla sıkı bir irtibat içindedir. Özel hayata dair hususlar kişinin mesleği ile ilgili tasarruflara esas alınmışsa özel hayata saygı hakkı gündeme gelecektir. (Bülent Polat, § 62; Ata Türkeri, § 31)

Gelişen teknolojinin, kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması amacıyla, kamu kesiminde kullanılmaya başlanması doğaldır. Ancak; teknoloji kullanılarak kişisel görüntülerin kayıt altına alınmasında özel hayatın gizliliği ve kişilerin mahremiyet hakkı da dikkate alınarak uygulama yapılması gerektiğinde kuşku ve duraksamaya yer bulunmamaktadır.

Buna ek olarak, kamu çalışanlarının faaliyet yürüttüğü servislerde çalışanların çalışma alanlarını ve dolayısıyla çalışanları görecektir şekilde yerleştirilen, güvenlik ve suçun önlenmesi gibi nedenlerle uygulandığı ileri sürülen kameralı takip sistemleri kullanılarak kişisel görüntülerin alınması, temel hak ve hürriyetler içerisinde sayılan özel hayatın gizliliği ilkesi kapsamında özel hayata müdahale olarak ele alınmalı, bu müdahalenin hukuka uygunluğunun değerlendirmesi ise kanunilik, ölçülülük gibi anayasal kavramlar yanında Avrupa İnsan Hakları Mahkemesi kararları ve Anayasa Mahkemesi kararları dikkate alınarak yapılmalıdır.

Yukarıda anılan müdahale, Anayasa'nın 13. maddesinde belirtilen koşulları yerine getirmediği müddetçe aynı zamanda Anayasa'nın 20. maddesinin ihlalini de teşkil edecektir.

Anayasa'mızın 13. maddesi, "Temel hak ve hürriyetler, ... yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, ... demokratik toplum düzeninin... gereklerine ve ölçülülük ilkesine aykırı olamaz. " şeklindedir.

Bu sebeple müdahalenin ihlal oluşturup oluşturmadığının belirlenmesinde, Anayasa'nın 13. maddesinde öngörülen ve somut başvuruya uygun düşen kanunlar tarafından öngörülme, Anayasa'nın ilgili maddesinde belirtilen nedenlere dayanma, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmama koşulları yönünden inceleme yapılması gerekir.

Anayasa'nın 13. maddesi, temel hak ve özgürlüklerin sınırlandırılmasını, ilgili hak ve özgürlüğe ilişkin Anayasa maddesinde gösterilen özel sınırlandırma sebeplerinin bulunmasına bağlı kılmıştır. Bununla birlikte Anayasa Mahkemesinin kararlarına göre, özel sınırlama nedeni öngörülmemiş olan hakların dahi, hakkın doğasından kaynaklanan bazı sınırları bulunmaktadır. Ayrıca Anayasa'nın diğer maddelerinde yer alan kurallara dayanılarak da bu hakların sınırlanması mümkün olabilmektedir. Buna göre, Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin özel sınırlama sebebi gösterilmemiş hak ve özgürlüklere sınır teşkil edebileceği kabul edilmektedir. (AYM, E.2014/87, K.2015/112)

Anayasa'nın 20. maddesi, "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kağıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakim tarafından onayına sunulur. Hakim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar." hükmünü haizdir.

Anayasa'nın 20. maddesinin 1. fıkrası yönünden özel sınırlama nedeni düzenlenmemiştir. Maddenin ikinci fıkrasında, birtakım sınırlama sebeplerine yer verilmiş olmakla beraber bu sebepler sadece arama ve elkoyma tedbirlerine yöneliktir. Dolayısıyla bu sebeplerin özel hayata saygı hakkının tüm boyutları yönünden uygulanması mümkün görünmemektedir.

Bu durumda, Anayasa'nın diğere maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin somut olay bakımından sınırlandırma sebebi olarak kabul edilip edilemeyeceğı araştırılmalıdır.

Anayasa'nın 5. maddesinde, "Devletin temel amaç ve görevleri, Türk Milletinin bağımsızlığını ve bütünlüğünü, ülkenin bölünmezliğini, Cumhuriyeti ve demokrasiyi korumak, kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak; kişinin temel hak ve hürriyetlerini, sosyal hukuk devleti ve adalet ilkeleriyle bağdaşmayacak surette sınırlayan siyasal, ekonomik ve sosyal engelleri kaldırmaya, insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmaktır. " denilmektedir. Buna göre kişilerin ve toplumun refah, huzur ve mutluluğunu sağlamak devletin temel amaç ve görevlerindedir.

Kişinin ve toplumun refah, huzur ve mutluluğunu sağlamanın ön koşulu milli güvenlik ve kamu düzeninin tesisidir. Milli güvenlik ve kamu düzeninin sağlanmadığı bir ortamda, hak ve özgürlüklerden gereğı gibi yararlanılması, kişinin maddi ve manevi varlığını geliştirmesi mümkün değildir. Devletin hak ve özgürlükleri koruma ödevinin yanında, milli güvenliğı ve kamu düzenini sağlama görevi de bulunmaktadır.

Yukarıda ifade edilen sınırlama nedenleri de dikkate alındığında uyumsuzluğun sağlıklı çözümü için; sınırlandırmanın, "demokratik toplum düzeninin gereklerinden olması" ve "ölçülülük ilkesine uygun olması"nın ne anlama geldiğinin de ortaya konması gerekmektedir.

"Demokratik toplum düzeninin gereklerinden olma, bir sınırlamanın demokratik bir toplumda zorlayıcı bir toplumsal ihtiyacın karşılanması amacına yönelik olmasını ifade etmektedir. Buna göre sınırlayıcı tedbir, bir toplumsal ihtiyacı karşılamıyorsa ya da başvurulabilecek son çare niteliğinde değilse demokratik toplum düzeninin gereklerine uygun bir tedbir olarak değerlendirilemez. (AYM, E.2015/96, K.2016/9, 10/2/2016 § 13; ifade özgürlüğü bağlamında Bekir Coşkun [GK], B. No: 2014/12151, 4/6/2015, § 51; özel hayatın gizliliğı hakkı bağlamında Ata Türkeri, § 44; İ.F.A., B. No: 2013/8564, 17/2/2016, § 62)

Bu kapsamda kamu makamlarının faaliyetin niteliğı ve sınırlamanın amacına göre değışen geniş bir takdir yetkisinin bulunması doğaldır. Ancak özel hayatın gizliliğı hakkının mahremiyet hakkı gibi en gizli yönleri söz konusu olduğunda kamu makamlarının takdir yetkisi daha dardır ve bu alanlara yönelik müdahalelerin haklı olduğunun kabul edilebilmesi için kamu makamlarınca özellikle ciddi gerekçelerin gösterilmesi gerekir. (Ata Türkeri, § 47)

Kamu makamlarının özel hayata müdahaleleriyle ilgili olarak, müdahaleye yol açan karar alma sürecinde de keyfi davranmadıklarını kanıtlamaları gereklidir. Ancak bu halde de sınırlandırmanın ölçülülük ilkesine uygun olması gereklidir. (Ata Türkeri, § 48)

Anayasa Mahkemesi kararları uyarınca ölçülülük ilkesi, sınırlayıcı önlemin öngörülen amaç için zorunlu ve amaca ulaşmaya elverişli olmasını ayrıca amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder. Ölçülülük ilkesinin amacı da temel hak ve özgürlüklerin gereğinden fazla sınırlandırılmasının önlenmesidir. (AYM, E.2015/102, K.2016/151, 7/9/2016, § 22; E.2012/100, K.2013/84, 4/7/2013; Marcus Frank Cerny, B. No: 2013/5126, 2/7/2015, § 72)

Avrupa İnsan Hakları Sözleşmesi'nin "Özel ve aile hayatına saygı hakkı" kenar başlıklı 8. maddesi şöyledir: "(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. (2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir. "

Kamu makamlarının özel hayata saygı hakkına keyfi bir şekilde müdahale etmelerinin önlenmesi, Sözleşme'nin 8. maddesi ile sağlanan güvenceler kapsamında yer almaktadır. Avrupa İnsan Hakları Mahkemesi (AİHM), devletin özel hayata saygı hakkı kapsamında bulunan bir menfaate müdahale ettiğini tespit ettiğinde, 8. maddenin ikinci fıkrasında belirtilen koşulları incelemektedir. Buna göre kamu makamlarının müdahalesinin yasal bir dayanağı olup olmadığı, anılan fıkrada yer alan meşru amaçlara dayalı olup olmadığı, demokratik bir toplumda gerekli ve öngörülen amaçla orantılı olup olmadığı araştırılmaktadır. (AİHM Dudgeon/Birleşik Krallık, § 43; Olsson/İsveç No.1, B. No: 10465/83, 24/3/1988, § 59)

Ayrıca, AİHM kararlarına göre Sözleşme'nin 8. maddesi açıkça usul şartları içermemekle birlikte anılan maddeyle güvence altına alınan haklardan etkili bir şekilde yararlanılabilmesi için müdahaleyi doğuran karar alma sürecinin bu maddeyle korunan hak ve özgürlüklere gerekli saygıyı sağlayacak nitelikte ve adil olması gerekir. Bu şekildeki bir süreç başvurusunun 8. maddedeki haklarını -deliller ve kanıtlanma konuları dahil- adil şartlarda savunabileceği usule ilişkin etkili güvencelerden yararlandırılmasını gerektirir. AİHM'e göre bu şekildeki güvencelerin amacı 8. maddede yer alan haklara keyfi şekilde müdahalede bulunulmasını önlemek, müdahalenin gerekçelendirilmesini sağlamaktır. (AİHM Ciubotaru/Moldova, B. No: 27138/04, 27/4/2010, § 51; T.P. ve K.M./Birleşik Krallık, B. No: 28945/95, 10/5/2001, § 72)

AİHM'e göre gerek negatif yükümlülükler gerekse pozitif yükümlülükler bakımından söz konusu usule ilişkin etkili güvencelerin sunulması gerekmektedir. (Benzer yöndeki AİHM kararı için bkz. Hokkanen/Finlandiya, B.No: 19823/92, 23/9/1994, §§ 55-58; Glaser/Birleşik Krallık, B. No: 32346/96, 19/9/2000, §§ 63-66; Bajrami/Arnavutluk, B. No: 35853/04, 12/12/2006, §§ 50-55; Abdulaziz, Cabales ve Balkandali/Birleşik Krallık, B. No: 9214/80, 28/5/1985, § 67).

Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesinin "Mahremiyet Hakkı" başlıklı 17. maddesinde de, hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemeyeceği; onuru veya itibarının hukuka aykırı saldırılara maruz bırakılmayacağına, herkesin bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahip olduğu belirtilmiştir.

Avrupa İnsan Hakları Mahkemesinin Antovic ve Mirkovic v. Sırbistan ve Karadağ (Başvuru No. 70838/13) kararında, çalıştıkları anfi alanlarına demirbaş ve öğrenciler de dahil kişi güvenliğinin sağlanması amacıyla kamera sistemi kurulan iki profesörün özel hayatlarının gizliliğinin ihlal edildiğine karar vermiştir. Kararda özellikle Avrupa İnsan Hakları Mahkemesinin daha öncede benzer konularda vermiş olduğu kararlara atıfta bulunularak bazı tespitlere de yer verilmiştir.

Bu tespitler arasında özellikle kişilerin iş yerinde ve çalışma ortamında yani kamusal bir alanda bulunsa da, özel hayatın profesyonel aktiviteler ve dış dünya ile ilişkileri de kapsayan ve Avrupa İnsan Hakları Mahkemesinin "sosyal özel hayat" olarak adlandırdığı bir alanı da kapsadığı ve bu alanın da korunması gerektiği, kamera sistemleri ile kişilerin sosyal özel hayatlarının izlenmesinin "ciddi bir müdahale" olarak kabul edilmesi gerektiği, kişilerin güvenliği veya işverenin hakları başka yollarla korunamıyorsa ancak son çare olarak kamera sistemlerinin kişilerin çalışma alanlarını görecektir şekilde kurulmasının kabul edilebilir olacağı tespitlerine yer verilmiştir. Yine Avrupa İnsan Hakları Mahkemesinin Lopez Ribalba ve Ötekiler v. İspanya (Başvuru No. 1874/13) kararında da iş verenin başka yollarla korunabilecek haklarını kamera sistemi yoluyla korumasının son çare olduğu, bu durumda bile kamera sistemleri ile ilgili olarak bildirimde bulunması ve usulleri belirlemesi gerektiği vurgulanmıştır.

Yine yukarıda yer verilen kararlardan, farklı güvenlik önlemleri yoluyla korunabilecek haklar veya önlenilecek olaylara yönelik olarak kamera sistemleri kurulmaması gerekeceği ve çalışanların doğrudan çalışma alanlarını görüntüleme şeklinde kişilerin özel hayatına müdahale anlamına gelen bu sistemlerin bu durumlarda kullanılmaması gerekeceği, aksinin ölçülülük ilkesine aykırı olacağı sonucuna ulaşılmaktadır.

Avrupa İnsan Hakları Mahkemesi kararlarında yukarıda ifade edilen Antovic ve Mirkovic v. Sırbistan ve Karadağ (Başvuru No. 70838/13) kararında da yer aldığı gibi kamera sistemleri ile ilgili olarak belli başlı şartların ortaya konulması gerektiği de ifade edilmiştir. Bunlar özellikle uygulamanın kanuni bir dayanağı olması, sınırlı bir izleme olması ve kötüye kullanmaya karşı garantiler olması gerektiğidir.

5237 sayılı Türk Ceza Kanunu'nun "Özel hayatın gizliliğini ihlal" başlıklı 134. maddesinde "Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.", "Kişisel verilerin kaydedilmesi" başlıklı 135. maddesinde ise "Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir." hükmü yer almaktadır.

5271 sayılı Ceza Muhakemesi Kanunu'nun "İletişimin tespiti, dinlenmesi ve kayda alınması" başlıklı 135. maddesi düzenlemesinde "başka suretle delil elde edilmesi imkânının bulunmaması durumunda" iletişimin kayda alınabileceği, "Teknik araçlarla izleme" başlıklı 140. maddesi ise, "başka suretle delil elde edilememesi hâlinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyeri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabilir" hükmü yer almakta olup, bu düzenlemeler de suça yönelik kuvvetli şüphe halinde bile en son çare olarak ses ve görüntü kaydına başvurulması gerektiğini ortaya koymaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanunu, 07/04/2016 tarihli ve 29677 Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Dava konusu işlem tarihinde yürürlükte bulunmamakla beraber konunun önemine binaen, dava konusu edilen kamera sistemleri ile ilgili belli başlı düzenlemelere de yer vermiştir. Neden bu sisteme ihtiyaç duyulduğunun ortaya konulması, sistemden kimin veya kimlerin yasal olarak sorumlu olduğunun belirlenmesi, sisteminin maksada uygun olup olmadığının ortaya konulması, özel hayatın gizliliğinin ihlal edilip edilmediğini kimin kontrol edeceğinin ve görüntülere kimin ulaşımı olacağına belirlenmesi ve bu hususların olarak kayıt altına alınması, kayıtlarının güvenliğinin ve gizliliğinin sağlanması güvenlik prosedürleri hazırlanması, kameralarla gözlemlenen bölgelerin girişinde ve içerideki uygun yerlerde bölgenin kamera sistemleri tarafından gözetlendiği ve kayıt altına alındığının belirtilmesi gerektiği, sistemin kuruluş maksadıyla bağdaşmayan görüntülerin gereğinden uzun süre saklanmaması, kişilerin özel hayatın gizliliğinin sağlanması yönünde beklentisinin olabileceği görüntülerin yetkili kişiler haricinde hiç kimse tarafından izlenememesi için alınacak önlemler gibi bir çok konuda düzenleme getirilmiştir.

Tüm bu açıklamalar ışığında dava konusu işlem incelendiğinde, Avrupa İnsan Hakları Mahkemesi kararları da dikkate alındığında hakların korunması başka şekilde sağlanamıyorsa kamera sistemlerinin çalışanların çalışma alanlarını göreceğ şekilde kurulmasının mümkün olduğu ancak

bunun bir son çare olarak değerlendirildiği ve bu düzenlemenin içeriğini ayrıntılı olarak ortaya koyan bir özel düzenleyici işlem olması gerektiği, kamera sistemlerinin çalışma alanlarını çekmesinin özel hayatın gizliliğini ihlal ettiği, sınırlı bir izleme sağlayacak şekilde güvenlik amacıyla giriş ve çıkışları izlemek üzere veya vatandaşlara da açık olan ortak alanlar ve iş sahiplerinin de giriş çıkışına açık, yoğun bir alış veriş trafiği olan alanlarda kurulabileceği ancak bu kameraların da çalışanların iş yapış şekillerini denetlemek veya sürekli olarak belli kişileri çekecek şekilde kurulmaması gerektiği, güvenlik amacıyla kurulmuş olmaları gerektiği ve bu nedenle amaca hizmet eder şekilde konumlandırılması gerektiği anlaşılmaktadır.

Yine kamera sistemlerinin zorunlu güvenlik amacı ile ve başka bir yolla bu güvenlik amacı sağlanamıyorsa kurulabilmesi mümkün olsa da, yukarıda yer verilen açıklamalar ışığında uygulamanın usul ve esaslarını gösteren yasal dayanağının bulunması, açık ve anlaşılabilir olması ve ilgililerin bu konudaki hakları ve kamera sistemi ile ilgili olarak bilgilendirilmiş olması gerektiği, toplanan görüntülerle ilgili güvencelerin sağlanması gerektiği, dava konusu işlemin bu haliyle sınırları belirlenmemiş, yasal dayanağı olmayan, uygulamaya dair usul ve esaslar ile güvenceleri düzenlenmemiş bir sistemle yürütüldüğü ve bu haliyle kamu yararına yönelik olduğunu kabul etmeye imkan olmadığı; Anayasal bir ilke olan ölçülülük ilkesine aykırılık teşkil ettiği ve mahremiyet hakkını ihlal ettiği anlaşılmakta olup, kişilik haklarına aykırı şekilde kamu görevlilerinin tüm faaliyetlerinin izlenmesine imkan tanıyan uygulamada isabet bulunmamaktadır.

Kameralı takip sistemi ile kurumca amaçlanan kamu yararı arasında orantılılık bulunmadığından uygulama ölçülülük ilkesine de aykırılık teşkil etmektedir. Anayasa'nın 13. maddesinde, temel hak ve hürriyetlerin ancak kanunla sınırlanabileceği, değişik 20/3. maddesinde de, kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceğinin belirtildiği, ancak konuyla ilgili dava konusu işlemin gerçekleştirildiği aşamada yasal bir düzenlemenin yapılmadığı anlaşılmaktadır.

İdarelerin teknolojik gelişmelerden de yararlanarak kamu çalışanlarının faaliyet yürüttüğü alanda güvenlik ve suçun önlenmesi amacıyla kameralı takip sistemi uygulamasının, güvenlik amaçlı olarak giriş ve çıkışlar ve güvenliğin özel önem arz ettiği alanlar dışında, günlük iş ve işlemleri yürüten çalışanların çalışma odalarını ve servisleri çekecek şekilde yerleştirildiği durumlarda, kamusal alanda da olsa "özel hayatın gizliliği" ilkesi kapsamında bulunduğu Avrupa İnsan Hakları Mahkemesi kararları ve Dairemizin daha önceki tarihli kararlarından anlaşılmaktadır. Yine uygulamanın sınırlarını, usul ve esaslarını gösteren bir yasal dayanağın bulunması, toplanan görüntülerin ileride

başka bir şekilde kullanılamayacağına dair bir güvencenin mevcut olması gerektiği de anlaşılmaktadır.

İdarenin güvenlik ve kamu yararını sağlama ihtiyacı ve çalışanların özel hayatın gizliliği gibi haklarının karşı karşıya geldiği bu gibi uyuşmazlıklarda, olayın dosyaya özel olarak ele alınması ve değerlendirilmesi gerektiği açıktır.

Uyuşmazlığın bu davaya özgü hali değerlendirildiğinde; dava konusu olayda davalı idarenin taşra birimlerinde görev yapan personelin izlenmesini teminen odalarına monitor yerleştirildiği ve kamera kayıt sisteminin kurulduğu ileri sürülerek güvenlik amacıyla binaların girişlerine yerleştirilenler dışında çalışanların birimlerde (odalarda) izlenmesine imkan veren kamera sisteminin kaldırılması talebiyle davacı sendika tarafından başvuru yapıldığı anlaşılmakta olup; uygulamanın sınırlarını, usul ve esaslarını gösteren bir yasal dayanağın bulunmaması, toplanan görüntülerin ileride başka bir şekilde kullanılamayacağına dair bir güvencenin mevcut olmaması ve iş yerinin güvenliğini sağlama amacını aşarak, doğrudan çalışan memurun kendisinin, diğer memurlarla ya da iş sahipleriyle ilişkisinin ve kamu hizmetinin görülmesi sırasında yaptığı her türlü haberleşmesinin, çalışma alanı ve masasının gözlemlendiği kamera takip sisteminin kurulmasının özel hayatın gizliliğini ihlal ettiği ve bu haliyle yukarıda belirtilen temel haklar ve Anayasal ilkelerle bağdaşmaması nedeniyle dava konusu işlemin iptaline karar verilmesi gerekirken davanın reddi yolunda verilen mahkeme kararının hukuka aykırı olduğu sonucuna varılmıştır.

Açıklanan nedenlerle, temyiz isteminin kabulüyle, Ankara 11. İdare Mahkemesi'nin 07/11/2014 tarih ve E:2014/610, K:2014/1501 sayılı kararının BOZULMASINA, yeniden bir karar verilmek üzere dosyanın adı geçen mahkemeye gönderilmesine, 2577 sayılı Kanun'un (Geçici 8. maddesi uyarınca uygulanmasına devam edilen) 54. maddesinin 1. fıkrası uyarınca bu kararın tebliğ tarihini izleyen günden itibaren onbeş gün içinde karar düzeltme yolu açık olmak üzere, 20/02/2018 tarihinde oybirliğiyle karar verildi.

BÖLGE İDARE MAHKEMESİ KARARLARI

Bölüm İçeriği

- Ankara BİM 1. İdari Dava Dairesi (E. 2020/557)
- Ankara BİM 1. İdari Dava Dairesi (E. 2020/324)
- İstanbul BİM 7. İdari Dava Dairesi (E. 2020/412)
- İstanbul BİM 7. İdari Dava Dairesi (E. 2020/288)
- İstanbul BİM 7. İdari Dava Dairesi (E. 2020/284)
- İstanbul BİM 3. İdari Dava Dairesi (E. 2017/1689)
- İzmir BİM 6. İdari Dava Dairesi (E. 2017/1238)
- Konya BİM 4. İdari Dava Dairesi (E. 2020/731)

Ankara BİM - 1. İdari Dava Dairesi (E. 2020/557)

Ankara Bölge İdare Mahkemesi, 1. İDD, E. 2020/557 K. 2020/780 T. 11.3.2020

Esas No.: 2020/557

Karar No.: 2020/780

Karar Tarihi: 11.03.2020

İSTEMİN ÖZETİ: İzmir ili Çeşme ilçesi X1 Devlet Hastanesi'ne sözleşmeli personel statüsünde hemşire olarak yerleştirmesi yapılan davacı tarafından, güvenlik soruşturması ve arşiv araştırması sonucuna göre 657 sayılı Devlet Memurları Kanunu'nun 48. maddesinin 1. fıkrasının (A) bendindeki şartları taşımadığından bahisle atamasının yapılmamasına ilişkin 22.04.2019 tarih ve 2586 sayılı işlemin iptali ile bu işlem nedeniyle yoksun kalınan parasal ve özlük haklarının yasal faiziyle birlikte ödenmesine karar verilmesi istemiyle açılan davanın; dava konusu işlemde hukuka aykırılık bulunmadığı gerekçesiyle reddine ilişkin olarak Ankara 15. İdare Mahkemesi'nce verilen 27/11/2019 gün ve E:2019/1059, K:2019/1920 sayılı kararın; hukuka, temel hak ve özgürlüklere aykırı olduğu, verilen kararın Anayasa'ya ve Avrupa İnsan Hakları Sözleşmesi hükümlerine uygun olmadığı, hak ihlali doğurduğu ileri sürülerek kaldırılması istenilmektedir.

SAVUNMANIN ÖZETİ: Mahkeme kararında hukuka aykırılık bulunmadığı ileri sürülerek, istinaf isteminin reddi gerektiği savunulmuştur.

TÜRK MİLLETİ ADINA

Karar veren Ankara Bölge İdare Mahkemesi 1. İdari Dava Dairesince, 6100 sayılı Hukuk Muhakemeleri Kanunu'nun 335. maddesi uyarınca, davacının adli yardım isteminin kabul edilmesi yönündeki ilk derece mahkemesi kararının hüküm kesinleşinceye kadar devam ettiği gözetilip 2577 sayılı Yasanın değişik 45. maddesi uyarınca dava dosyası incelenerek gereği görüldü :

Dava; İzmir ili Çeşme ilçesi X1 Devlet Hastanesi'ne sözleşmeli personel statüsünde hemşire olarak yerleştirmesi yapılan davacı tarafından, güvenlik soruşturması ve arşiv araştırması sonucuna göre 657 sayılı Devlet Memurları Kanunu'nun 48. maddesinin 1. fıkrasının (A) bendindeki şartları taşımadığından bahisle atamasının yapılmamasına ilişkin 22.04.2019 tarih ve 2586 sayılı işlemin iptali ile bu işlem nedeniyle yoksun kalınan parasal ve özlük haklarının yasal faiziyle birlikte ödenmesine karar verilmesi istemiyle açılmıştır.

657 sayılı Devlet Memurları Kanunu'nun 4.maddesinin (B) fıkrası hükmü uyarınca, kamu idare, kamu kurum ve kuruluşlarında sözleşmeli olarak çalıştırılacak personelin tabi olacağı esasları belirlemek üzere 06/06/1978 tarih ve 15754 sayılı Bakanlar Kurulu kararı ile çıkarılan "Sözleşmeli Personel Çalıştırılmasına İlişkin Esaslar"ın 20/02/2017 tarih ve 2017/9949 sayılı Bakanlar Kurulu kararı ile değişik 12.maddesinin 1.fıkrasında, sözleşmeli olarak çalışacakların ilgili kurumun saptayacağı özel koşulların yanı sıra, 657 sayılı Kanununun 48. maddesinin 1. fıkrasının (A) bendinin, (4), (5), (6), (7) ve (8) numaralı alt bentlerinde belirtilen koşulları taşımalarının gerekli olduğu hükme bağlanmıştır.

657 sayılı Devlet Memurları Kanunu'nun "Genel ve Özel Şartlar" başlıklı 48.maddesinin 1.fıkrasının (A) bendine, önce 676 sayılı OHAL Kanun Hükmünde Kararnamesi'nin 74.maddesiyle daha sonra 7070 sayılı Kanununun 60.maddesi ile de aynen kabul edilen düzenleme ile sekizinci alt bent olarak "Güvenlik soruşturması ve/veya arşiv araştırması yapılmış olmak" hükmü eklenerek, Devlet Memuru olabilmek için ilgili hakkında güvenlik soruşturması ve/veya arşiv araştırması yapılmış olunması şartı getirilmiştir.

Dava konusu işlem yukarıda belirtilen mevzuat hükmü uyarınca 657 sayılı Kanununun 48.maddesinin 1.fıkrasının (A) bendinin yukarıda sözü edilen (8) numaralı alt bendi hükmüne dayanılarak tesis edilmiştir.

Anayasa Mahkemesi'nin 24/07/2019 günlü, E:2018/73, K:2019/65 sayılı kararı ile;Anayasa Mahkemesinin yerleşik kararlarında da belirtildiği üzere "adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, öz geçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunduğu kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri" gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm verilerin kişisel veri olarak kabul edildiği, bu bağlamda güvenlik araştırması ve arşiv araştırmasıyla elde edilen verilerin kişisel veri niteliğinde olduğu, 657 sayılı Kanununun 48.maddesinin 1.fıkrasının (A) bendine (8) numaralı alt bent olarak eklenen söz konusu kuralla güvenlik soruşturması ve arşiv araştırması kapsamında kamu mercileri tarafından özel yaşamı ile ilgili sorular sorulması da dahil olmak üzere bir bireyin özel hayatı, iş ve sosyal yaşamıyla ilgili bilgilerin alınmasının, kaydedilmesinin ve kullanılmasının özel hayata saygı hakkına sınırlama niteliğinde olduğu,

Anayasa'nın 129.maddesinin birinci fıkrasında memurlar ve kamu görevlilerinin Anayasa ve kanunlara sadık kalarak faaliyette bulunma yükümlülüklerinin düzenlendiği, belirtilen hususlar gözetilerek kamu görevlerine atanacak kişiler bakımından birtakım şartlar getirilmesinin doğal olduğu, bu şekilde aranan niteliklerin, kamu hizmetinin etkin ve sağlıklı bir biçimde yürütülmesi

amacına yönelik olduğu, dolayısıyla kamu görevine atanmadan önce kişilerin güvenlik soruşturması ve arşiv araştırmasının yapılmasını öngören kuralın kanun koyucunun takdir yetkisinde olduğu, ancak bu alanda düzenleme getiren kuralların, kamu makamlarına hangi koşullarda ve hangi sınırlar içinde tedbir uygulama ve özel hayatın gizliliğine yönelik müdahalelerde bulunma yetkisi verildiğinin yeterince açık olarak göstermesi ve olası kötüye kullanımlara karşı yeterli güvenceleri sağlaması gerektiği, kuralda güvenlik soruşturması ve/veya arşiv araştırması yapılması memurluğa alımlarda genel şartlar arasında sayılmasına karşın, güvenlik soruşturmasına ve arşiv araştırmasına konu edilecek bilgi ve belgelerin neler olduğuna, bu bilgilerin ne şekilde kullanılacağına, hangi mercilerin soruşturma ve araştırmayı yapacağına ilişkin herhangi bir düzenlemenin yapılmamış olduğu, diğer bir ifadeyle güvenlik soruşturması ve arşiv araştırmasının yapılmasına ve elde edilecek verilerin kullanılmasına ilişkin temel ilkeler belirlenmeksizin, kuralla sadece güvenlik soruşturması ve arşiv araştırması yapılmasının devlet memurluğuna alımlarda aranacak şartlar arasında sayıldığı, güvenlik soruşturması ve arşiv araştırması sonucunda devlet memurluğuna alınmada esas alınacak kişisel veri niteliğindeki bilgilerin alınmasına, kullanılmasına ve işlenmesine yönelik güvenceler ve temel ilkeler kanunla belirlenmeksizin bunların alınmasına ve kullanılmasına izin verilmesinin Anayasa'nın 13. 20. ve 128. maddesiyle bağdaşmadığı ve bu nedenle dava konusu kuralın Anayasa'nın anılan maddelerine aykırı olduğu belirtilerek; 7070 sayılı Kanunun 60.maddesiyle 657 sayılı Kanunun 48.maddesinin 1.fıkrasının (A) bendine eklenen (8) numaralı alt bendinin iptaline karar verilmiştir.

Anayasa Mahkemesi'nin bu kararı 29/11/2019 günlü, 30963 sayılı Resmi Gazete'de yayımlanmıştır. Anayasa Mahkemesi bu düzenlemeyi iptal ederken ileri tarihli bir yürürlük süresi öngörmemiştir. Dolayısıyla, anılan karar Resmi Gazetede yayımlandığı tarihte yürürlüğe girmiştir.

Anayasa Mahkemesinin sözü edilen kararı ile iptal edilen yasa kuralı (657 sayılı Kanunun 48/1-A-8.bendi) dışında, farklı statüde ya da gizlilik derecesine sahip bazı yerlerde görev yapan kamu görevlileri ile ilgili olarak güvenlik soruşturması ve/veya arşiv araştırması yapılmasını öngören ayrı yasal düzenlemeler bulunmaktadır.

4045 sayılı Kanun, yetkili olmayan kişilerin bilgi sahibi olmaları halinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile Genelkurmay Başkanlığı, Milli Savunma Bakanlığı, jandarma, emniyet, sahil güvenlik ve istihbarat teşkilatlarında çalıştırılacak kamu personeli ile ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında güvenlik soruşturması ve arşiv araştırması yapılmasını düzenlemektedir. 12/04/2000 tarihli ve 24018 sayılı Resmi Gazete'de

yayımlanan "Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği" de 4045 sayılı Kanun'un 1. maddesi uyarınca çıkarılmıştır.

Ayrıca, 399 sayılı Kanun Hükmünde Kararnamenin 7.maddesinin (f) bendi, 233 sayılı KHK'ya tabi Kamu İktisadi Teşebbüslerinde ve bağlı ortaklıklarda sözleşmeli personel olarak işe alınacaklarda güvenlik soruşturması ve arşiv araştırması yapılmış olmak koşulunun aranacağını kurala bağlamıştır.

4045 sayılı Kanunun 1.maddesi ve 399 sayılı KHK'nın 7.maddesinin (f) bendi yönünden Anayasa Mahkemesince verilmiş iptal kararı bulunmamaktadır. Dolayısıyla, anılan düzenlemeler kapsamında kalan kamu görevleri bakımından güvenlik soruşturması ve arşiv araştırması uygulamasının dayanağı kurallar halen yürürlükte bulunmaktadır. Bununla birlikte, Dairemizin 31/12/2019 tarihli ve E:2019/4902 sayılı kararı ile 4045 sayılı Kanunun 1.maddesinin, yine Dairemizin 31/12/2019 tarih ve E:2019/4116 sayılı kararı ile de 399 sayılı KHK'nın 7.maddesinin (f) bendinin Anayasa'nın 13.20. ve 128.maddelerine aykırı olduğundan bahisle iptalleri istemiyle itiraz yolu ile Anayasa Mahkemesine başvurulmuştur.

Dava konusu edilen işlemin dayanağını oluşturan yasa kuralı ise sözü edilen Anayasa Mahkemesi'nce iptal edildiğinden, Anayasa Mahkemesi kararının geriye yürümesi ve söz konusu karardan önce yürürlükte olan Anayasaya aykırı kurala göre tesis edilen işlemlere karşı açılan ve halen görülmekte olan davaların (olayımızda olduğu gibi), Anayasa Mahkemesi kararından ne şekilde etkileneceği hususunun öncelikle açıklığa kavuşturulması gerekmektedir.

Anayasa'nın153.maddesinin 3.fıkrası, "Kanun, Cumhurbaşkanlığı kararnamesi veya Türkiye Büyük Millet Meclisi İçtüzüğü yada bunların hükümleri, iptal kararlarının Resmi Gazete'de yayımlandığı tarihte yürürlükten kalkar. Gereken hallerde Anayasa Mahkemesi iptal hükmünün yürürlüğe gireceği tarihi ayrıca kararlaştırabilir. Bu tarih, Resmi Gazete'de yayımlandığı günden başlayarak bir yılı geçemez";5.fıkrası, "İptal kararları geriye yürümez"; 6.fıkrası ise, "Anayasa Mahkemesi Kararları Resmi Gazete'de hemen yayımlanır ve yasama, yürütme ve yargı organlarını, idare makamlarını, gerçek ve tüzel kişileri bağlar." kurallarını içermektedir.

Anayasa Mahkemesince bir kanunun veya kanun hükmünde kararnamenin tümünün ya da bunların belirli hükümlerinin Anayasa'ya aykırı bulunarak iptal edilmiş olduğu bilindiği halde eldeki davaların Anayasa'ya aykırılığı saptanmış olan kurallara göre görüşülüp çözümlenmesi, Anayasa'nın üstünlüğü prensibine ve hukuk devleti ilkesine aykırı düşeceği için uygun görülemez. Aksine bir durum, Anayasa'nın 153.maddesinde yer alan Anayasa Mahkemesi kararlarının bağlayıcı olduğu yönündeki hükme aykırılık oluşturur.

Öte yandan, Anayasanın 153.maddesinin 5.fıkrasında yer alan ve iptal kararlarının geriye yürümezliğine ilişkin bulunan kural, iptal edilen hükümlere göre kazanılmış olan hakların ortadan kaldırılmasına veya toplumun huzurunun bozulmasına yol açacak sonuçları önlemek amacıyla kabul edilmiş olup, bu kuralın mutlak anlamda anlaşılıp uygulanamayacağı açıktır.

Yargıtay'ın bir kararında belirtildiği üzere; Türk Anayasa sisteminde benimsenen iptal kararının geriye yürümezliği kuralının getiriliş amacı, kazanılmış hakları ve hukuksal güvenliği ortadan kaldırıcı ya da toplumun adalet anlayışını zedeleyici sonuçlar doğurmasından kaygı duyulmasını önlemek, devlete olan güven duygularını sarsmamak, devlet yaşamında hukuk kargaşasına neden olmamak, hukuk güvenliğini ve istikrarını sağlamak olarak özetlenebilir. (Yargıtay 8.Hukuk Dairesi'nin 22/12/2011 tarih ve E:2010/508, K:2011/7468 sayılı kararı)

Bu bakımdan iptal kararlarının geriye yürümezliği ilkesi, kabul edilen önemli bir ilkedir.

Nitekim, Anayasa Mahkemesi, 12/12/1989 tarihli ve E:1989/11, K:1989/48 sayılı kararında, "Türk Anayasa sisteminde Devlete güven ilkesini sarsmamak ve ayrıca Devlet yaşamında bir karmaşaya neden olmamak için iptal kararlarının geriye yürümezliği kuralı kabul edilmiştir. Böylece, hukuksal ve nesnel alanda sonuçlarını doğuramaz bulunan durumların iptal kararlarının yürürlüğe gireceği güne kadarki dönem için geçerli sayılması sağlanmıştır." denilmek suretiyle konunun önemi vurgulanmıştır.

Anayasa Mahkemesi'nin 19/12/1989 tarihli ve E:1998/14, K: 1989/49 sayılı kararında da aynen; "bir hukuk kuralının yürürlüğü sırasında, bu kurala uygun bir biçimde tüm sonuçlarıyla kesin olarak edinilmiş hakların korunmasının Hukuk Devleti'nin gereği olduğu" vurgulanmaktadır.

Aktarılan Anayasa Mahkemesi kararları, iptal kararlarının geriye yürümezliği kuralının kazanılmış olan hakların ortadan kaldırılmasını önlemek amacıyla getirilen bir kural olduğunu açıkça ortaya koymaktadır.

Anayasa Mahkemesi'nin bahsedilen kararları ile aynı yönde olmak üzere Danıştay'ın kararlarında da istikrarlı bir şekilde, "iptal kararlarının geriye yürümeyeceği" kuralının, kazanılmış hakları saklı tutmak, hukuki istikrarı ve hukuk güvenliğini sağlamak ve kamu idaresini korumak amacıyla getirildiği ve anılan kuralın belirtilen amaca uygun olarak yorumlanıp uygulanması gerektiği görüşü benimsenmiştir. (Danıştay 8.Daire E:1967/153, K:1968/2783; Danıştay 10.Daire E:1996/9928, K:1999/2597; Danıştay 2.Daire E:2004/1545, K:2005/1886; Danıştay 2.Daire E:2004/7423, K:2005/113; Danıştay İDDK E: 2007/2326, K:2008/1724; Danıştay İDDK E:2010/2292, K:2013/3366; Danıştay İDDK

E:2013/826, K:2015/1654; Danıştay 5.Daire E:2010/6456, K:2013/5790; Danıştay 4.Daire E:2011/2546, K:2011/3384, Danıştay 3.Daire E:2015/31, K:2015/4299)

Belirtilen hukuksal durumun doğal sonucu olarak, bir kanun ya da kanun hükmünde kararnamenin uygulanması nedeniyle dava açmak durumunda kalan ve Anayasa'nın 153. maddesi uyarınca itiraz yoluyla Anayasa Mahkemesine başvurulmasını isteme hakkına sahip olan kişilerin de, olayımızda olduğu gibi, hak ve menfaatlerini ihlal eden kuralın iptal davası veya itiraz yoluyla daha önce yapılan başvuru sonucunda Anayasa Mahkemesince iptal edilmiş olması halinde iptal hükmünün hukuki sonuçlarından yararlanmaları gerektiği açıktır.

Bu nedenle, sözü edilen Anayasa Mahkemesi kararı ile Anayasa'ya aykırılığı nedeniyle iptal edilen 657 sayılı Kanun'un 48.maddesinin 1.fıkrasının (A) bendinin (8) numaralı alt bendine dayanılarak tesis edilen dava konusu işlemde hukuka uyarlık bulunmamaktadır.

Davacının, dava konusu işlem nedeniyle yoksun kaldığı haklarının ve oluşan maddi zararlarının yasal faiziyle birlikte tazmini istemine gelince;

Anayasa'nın 129. maddesinin birinci fıkrasında, memurlar ve kamu görevlilerinin Anayasa ve Kanunlara sadık kalarak faaliyette bulunma yükümlülükleri düzenlenmiştir. Ayrıca, 657 sayılı Kanun'da bu sadakat yükümlülüğünün yanı sıra kamu görevlilerine tarafsızlık ve devlete bağlılık yükümlülükleri de getirilmiştir. Sözü edilen Anayasa Mahkemesi kararında da açıklandığı üzere, belirtilen hususlar gözetilerek kamu görevlerine atanacak kişiler bakımından bir takım şartlar getirilmesi doğaldır. Bu şekilde aranan nitelikler ve kanunda öngörülen kısıtlamalar, kamu hizmetinin etkin ve sağlıklı bir şekilde yürütülmesi amacına yöneliktir. Dolayısıyla, idarenin kamu görevine atanacak kişilerin tabi olacağı güvenlik soruşturması ve arşiv araştırması konusunda kanunla temel çerçeveyi ortaya koyan kurallar getirmesi elbette mümkündür.

Avrupa İnsan Hakları Mahkemesi (AİHM), devletlerin milli güvenliğin korunması amacını gerçekleştirmede sahip oldukları takdir yetkisinin geniş olduğunu kabul etmektedir. AİHM, Sözleşme'ye taraf devletin milli güvenliği korumak için yetkili ulusal makamlarına ilk olarak kişiler hakkında bilgi toplama ve halka açık olmayan siciller tutma, ikinci olarak milli güvenlik bakımından önemli kadrolarda çalışmak isteyen adayların bu işe uygunluğunu takdir ederken bu bilgiyi kullanma yetkisi veren kurallara sahip olmaları gerektiğinde kuşku bulunmadığını belirtmektedir. (Leander/İsveç, SB.No: 9248/81, 26/3/1987)

Anayasa Mahkemesinin kararına ve AİHM içtihatlarına göre; kamu görevine atanmadan önce kişilerin güvenlik soruşturması ve arşiv araştırmasının yapılmasını öngören kural getirilmesi kanun

koyucunun takdir yetkisindedir. Ancak, bu alanda düzenleme getiren kuralların kamu makamlarına hangi koşullarda ve hangi sınırlar içinde tedbir uygulama ve özel hayatın gizliliğine yönelik müdahalelerde bulunma yetkisi verildiğini yeterince açık göstermesi ve olası kötüye kullanmalara karşı yeterli güvenceleri sağlaması gerekir.

Bu bağlamda, Anayasa Mahkemesi'nin sözü edilen iptal kararının gerekçesi dikkate alındığında, Anayasa Mahkemesi kararı, güvenlik soruşturmasının hiçbir şekilde yapılmayacağını değil, aksine güvenlik soruşturması detaylarının kanunda gösterilmesi, kişisel verilerin güvenliğine ve özel hayatın gizliliğine ilişkin güvenceleri sağlayan kuralların kanunda yer alması koşuluyla güvenlik soruşturmasının ve arşiv araştırmasının yapılabileceğini ortaya koymuştur.

Diğer yandan; bakılan davada, Anayasa Mahkemesi kararının Resmi Gazete'de yayımlandığı tarihten önce dava konusu işlemin hukuka aykırı olduğunu tespit eden, dolayısıyla uyuşmazlığın esası yönünden verilen bu nedenle de davacının atanması sonucunu doğuracak nitelikte bir karar (yürütmenin durdurulması ya da iptal kararı) bulunmamaktadır.

Belirtilen hukuki çerçevede konu incelendiğinde, dava konusu işlemin dayanağı yasa kuralının Anayasa Mahkemesi'nce iptal edilmesi nedeniyle dava konusu işlemin iptali yönünde verilen iş bu kararın, davacının hiç bir işleme gerek olmadan doğrudan kamu görevine atanması sonucunu doğurmayacağı sonucuna ulaşılmaktadır.

Anayasa Mahkemesi kararında belirtildiği üzere yeterli güvenceleri sağlayacak yeni bir yasal düzenleme yapılması durumunda, bu yasal düzenlemeye göre davacının durumunun davalı idarece makul bir süre içinde yeniden değerlendirmeye tabi tutulabileceği ve bu değerlendirmenin sonucunda davacının uyuşmazlığa konu kamu görevine atanıp atanamayacağına ilişkin yeniden bir işlem tesis edilmesi gerektiği kuşkusuzdur. Ayrıca, yeni yasal düzenleme uyarınca yapılacak değerlendirmenin sonucunda davacı açısından yine olumsuz bir sonucun ortaya çıkması halinde, bunun yargısal denetiminin mümkün olması nedeniyle, davacının durumunun yeniden değerlendirilmesi davacıyı güvencesiz bırakmadığı gibi, Anayasa Mahkemesinin aktarılan gerekçesi karşısında bu durum, bir hak ihlali de doğurmamaktadır.

Bu itibarla, dava konusu işlemin iptali yönündeki Dairemiz kararının davacının doğrudan atanması sonucu doğurmaması ve Anayasa Mahkemesi kararının yayımlanmasının öncesinde dava konusu işlemin esas yönüyle hukuka aykırılığını tespit eden ve davacının atanması sonucu doğurabilecek bir yargı kararının da bulunmaması karşısında, dava konusu işlem nedeniyle davacının hak kayıplarının ve oluşan maddi zararlarının tazmini istemi hakkında bu aşamada bir karar verilmesine yer bulunmamaktadır.

Açıklanan nedenlerle; davacı tarafın İSTİNAF BAŞVURUSUNUN KABULÜNE,Ankara 15. İdare Mahkemesi'nce verilen 27/11/2019 gün ve E:2019/1059, K:2019/1920 sayılı kararın KALDIRILMASINA;2577 sayılı Yasanın değişik 45. maddesinin 4. fıkrası uyarınca esastan incelenen davada, dava konusu işlemin İPTALİNE; dava konusu işlem nedeniyle davacının yoksun kaldığı haklarının ve oluşan maddi zararının yasal faiziyle tazmini istemi yönünden KARAR VERİLMESİNE YER OLMADIĞINA, davacının adli yardım istemi Mahkeme aşamasında kabul edilmiş olduğundan, davacıdan alınmayan aşağıda dökümü yapılan, mahkeme ve istinaf safhasına ait toplam 366,60 TL yargılama giderinin İdare Mahkemesince davacıdan tahsil edilmesine ve bu amaçla Mahkemesince Veraset ve Harçlar Vergi Dairesine müzekkere yazılması gerektiğine, dava iptal kararı ile sonuçlandığından davacı tarafından yapılan 366,60 TL'nin davalı idareden alınarak davacıya verilmesine ve hüküm tarihindeki Avukatlık Asgari Ücreti Tarifesine göre 1.700,00 TL avukatlık ücretinin davalı idareden alınarak davacı tarafa verilmesine, posta gideri avansından artan miktarın ise istinaf başvurusunda bulunan tarafa iadesine, 11/03/2020 tarihinde oyçokluğuyla ve kesin olarak karar verildi.

AZLIK OYU :Uyuşmazlık, kamu görevine yerleştirilmiş olan davacı hakkında Devlet memurluğuna alınacaklar için genel atama koşulları arasında sayılan 657 sayılı Kanununun 48. maddesinin 1. fıkrasının A-8 bendi gereğince davalı idarece yaptırılan güvenlik soruşturması ve arşiv araştırması sonucunun davalı idare bünyesinde oluşturulan Değerlendirme Komisyonu tarafından olumsuz olarak değerlendirildiğinden bahisle atamasının yapılmaması yönünde tesis edilen işlemin iptali isteminden kaynaklanmıştır.

Olağanüstü dönemde çıkarılan 03/10/2016 kabul tarihli 676 sayılı Kanun Hükmünde Kararnamenin 74. maddesi ile 657 sayılı Devlet Memurları Kanunu'nun Devlet memurluğuna alınacaklarda aranacak genel ve özel şartların düzenlendiği48. maddesinin1. fıkrasının A bendine "Güvenlik soruşturması ve/veya arşiv araştırması yapılmış olmak "şartını içeren 8 numaralı alt bendin eklendiği, bilahare 01/02/2018 tarihli, 7070 sayılı Olağanüstü Hal Kapsamında Bazı Düzenlemeler Yapılması Hakkında Kanununun 60. maddesi ile aynen kabulüne karar verilen (8) numaralı alt bent hükmü gereğince Devlet memurluğuna alınan kişilerin, herhangi bir özel görev ve kurum sınırlamasına tabi tutulmaksızın güvenlik soruşturması ve arşiv araştırmalarının yapılmasının, gerek doğrudan bu yasaya tabi olan, gerekse bu yasa maddesine yollamada bulunulan diğer özel mevzuata tabi idarelerce zorunlu hale getirildiği görülmektedir.

Yukarıda belirtilen 657 sayılı Kanununun 48. maddesinin 1/A fıkrasının (8) numaralı alt bent hükmünü aynen kabul ederek yasalaştıran 01/02/2018 tarihli, 7070 sayılı Kanununun 60. maddesiyle 657 sayılı

Kanunun 48. maddesinin 1/A fıkrasına eklenen 8 numaralı bendin, Anayasaya aykırılığı nedeniyle Anayasa Mahkemesine gidilmiş ve Anayasa Mahkemesi'nce; bu kuralda güvenlik soruşturması ve arşiv araştırmasına konu edilen bilgi ve belgelerin neler olduğu, bu bilgilerin ne şekilde kullanılacağı, hangi mercilerin soruşturma ve araştırmayı yapacağına ilişkin herhangi bir düzenleme yapılmadığı, bir başka ifadeyle temel ilkeler belirlenmeksizin Devlet memurluğuna alınma şartı olarak getirildiği belirtilerek Devlet memurluğuna atanmada kişisel veri niteliğindeki bilgilerin alınmasına, kullanılmasına ve işlenmesine yönelik güvenceler ve temel ilkeler kanunla belirlenmeksizin bunların alınmasına ve kullanılmasına izin verilmesinin Anayasanın 13., 20. ve 128. maddeleriyle bağdaşmadığı gerekçesiyle 657 sayılı Kanunun 48. maddesinin 1/A fıkrasına eklenen 8 numaralı alt bentte yer alan "Güvenlik soruşturması ve/veya arşiv araştırması yapılmış olmak." ibaresi iptal edilmişse de, Türkiye Cumhuriyeti Anayasasının 153. maddesinde; "Anayasa Mahkemesinin kararları kesindir. İptal kararları gerekçesi yazılmadan açıklanamaz...Kanun, Cumhurbaşkanlığı kararnamesi veya Türkiye Büyük Millet Meclisi İçtüzüğü ya da bunların hükümleri, iptal kararlarının Resmî Gazetede yayımlandığı tarihte yürürlükten kalkar...İptal kararının yürürlüğe girişinin ertelendiği durumlarda, Türkiye Büyük Millet Meclisi, iptal kararının ortaya çıkardığı hukuki boşluğu dolduracak kanun (...) teklifini öncelikle görüşüp karara bağlar..." hükmü gereğince eldeki uyuşmazlıklar bakımından; Anayasa Mahkemesi'nin öncelikle Anayasanın 13., 20. ve 128. maddelerinde düzenlemesini bulan kanunilik ilkesine aykırılığından bahisle verilmiş olduğu görülen iptal kararının gerekçesi uyarınca yasama organının düzenleme yapmadığı durumlarda, diğer hukuk normlarında yer alan düzenlemelerden hareketle Türk Medeni Kanunu'nun 1. maddesinin ikinci fıkrasında yer alan "Kanunda uygulanabilir bir hüküm yoksa, hakim örf ve adet hukukuna göre, bu da yoksa kanun koyucu olsaydı nasıl bir kural koyacak idiyse ona göre karar verir" kuralı karşısında, Anayasa Mahkemesi'nce verilen kararın gerekçesi ve hukukun genel prensipleri gözetilerek, yargı içtihatlarıyla çözüme gidileceğinin kabulü gerekmektedir.

Danıştay İdari Dava Daireleri Kurulu'nun 21/11/2012 tarihli, E:2008/3456, K:2012/2162 sayılı ve benzer nitelikteki kararlarında belirtildiği gibi; Anayasanın 153. maddesinin son fıkrası hükmü, Anayasa Mahkemesi kararlarının sadece hüküm fıkralarının değil, hükme dayanak oluşturan temel gerekçelerinin de bağlayıcı olduğunun kabul edilmesini zorunlu kılmaktadır. Buna göre, yargı kararlarının gerekçeleriyle birlikte değerlendirilmesi gerekmekte olup gerek Anayasa Mahkemesinin, gerekse Danıştayın konuya ilişkin kararları ışığında, somut olay çözümlenirken Anayasa Mahkemesi kararında belirtilen sınırlamalar kapsamında adil, hakkaniyetli, objektif hukuk kuralları işletilerek kişisel verilerin güvenlik soruşturması ve arşiv araştırması sonucunun olumsuz olarak

değerlendirilmesini gerektirip gerektirmediği hususunun hukukiliğinin irdelenmesine engel teşkil edecek bir durum bulunmamaktadır.

Anayasa'nın 152. ve 153. maddelerinde belirtildiği üzere; mahkemeler bir yasa kuralının Anayasa Mahkemesince iptal edilmesi halinde yüksek mahkemenin kararına ve dayandığı gerekçeye uygun karar vermek zorundadır.

Kanunlar, lafzı ve ruhuyla bir bütündür, o halde Anayasa Mahkemesi'nin mezkur iptal hükmünün; bu hükmün dayandığı kişisel hak ihlaline neden olabilecek unsurlar ve kanunilik ilkesi yönünden uyuşmazlık üzerindeki hukuki etki ve sonuçlarının, Anayasanın 153. maddesinde yer alan anayasal hüküm gereğince iptal gerekçesiyle birlikte değerlendirilmesi gerekmekte olup iptal edilen şart hüküm gereğince yapılmış olan güvenlik soruşturması ve arşiv araştırması sonucunun davacı yönünden değerlendirme dışı bırakılacağından söz edilemez.

Mezkur iptal kararının yayımlandığı Resmi Gazetede, yürürlük tarihi olarak Anayasa Mahkemesince ileri bir tarih öngörülmemiştir. Anayasamızın 153. maddesinde hüküm altına alınan amir kural; iptal kararlarının Resmî Gazetede yayımlandığı tarihte yürürlükten kalkmasıdır. İptal kararlarının yürürlüğe girişinin ertelendiği durumlarda ise, iptal kararıyla çıkan hukuki boşluğun giderilmesi için idareye yeni bir düzenleme yapmasına olanak sağlayacak süre tanınmasıdır. Anayasa Mahkemesi'nin; güvenlik soruşturması ve arşiv araştırmasının esasen idarelerin takdirinde olduğu gerekçesine dayalı olarak anılan iptal kararının, hukuki bir boşluğa sebebiyet vermediği, eldeki uyuşmazlıklarda yine Anayasa Mahkemesi'nce verilmiş önceki kararlarından hareketle öncelikle iptal gerekçesindeki hususlara bağlı kalınarak bu konuda diğer veya varsa özel mevzuatla getirilmiş kuralların uygulanmasına engel bir durum doğmadığı sonucuna varılmaktadır.

Anayasa Mahkemesi'nin iptal gerekçesinde ayrıntılı olarak bahsolunan; kişisel haklarla ilgili veriler bakımından şahıs hakkında elde edilen bilgi ve belgelere yönelik olarak kişisel hakların ihlaline sebebiyet vermeyecek şekilde davacı hakkında yapılmış olan soruşturma ve araştırmanın sonucunun hukukiliğinin irdelenmesine engel bir hüküm içermediğinin anlaşılması karşısında, uyuşmazlığın çözümünde bu konuda özel mevzuat niteliğinde olan 4045 sayılı Kanun ve ilgili Yönetmeliğin esas alınabileceği kabul edilmelidir.

Anayasa'nın 13. maddesinde, temel hak ve hürriyetlerin yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği ifade edilmiş, milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya (pozitif ayrımcılık yapılarak) başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı

olarak kişisel verilerin, çalışma hakkı bakımından açılan bu davalarda irdelenmesi, anayasal dayanaktan yoksun bırakılmamıştır.

Anayasanın 20. maddesinde öngörülen 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun yürürlükte olduğu ve bu Kanunun amaç maddesinden hareketle hangi hallerde Kanun hükümlerinin uygulanmayacağı kuralı, bu Kanunun 28. maddesinde düzenlenmiş olup Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu; zararın giderilmesini talep etme hakkı hariç ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddelerinin uygulanmayacağı haller sayılmış olup "a) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç araştırması için gerekli olması, b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi. c) Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması" hallerinde bu Kanunun uygulanmayacağı hükmü yer almakta olup ülke menfaatleri, kamu yararı ve hizmet gerekleri ilkeleri gereğince davacı hakkındaki güvenlik soruşturması sonucunun, üstün yarar ve amaçlar doğrultusunda, ancak temel ilkelere uygun ve orantılı olmak üzere ilgili mevzuatta sınırları gösterilen hukuki düzeyde irdelenmesi gerektiği kabul edilmelidir.

Anılan kuralın iptaline dair Anayasa Mahkemesi kararından anlaşıldığı üzere; kamu görevine ilk defa atanacaklar (ve belli kadroları kendi özel mevzuatına göre kazanacak olanlar) bakımından güvenlik soruşturması ve arşiv araştırması yapılması suretiyle Devletin kamu gücünü kullanarak tek taraflı, keyfi ve sui niyetle hak ihlaline sebep olunduğu değil, bu soruşturma ve araştırmayı yapan ve yaptıran yetkililerce başvuru usul ve esaslar ile öncelikle ilgiliye ait kişisel bilgilerin elde edilme aşamasındaki faaliyetler, bilahare bireyler hakkında ehil ve eğitimli görevlilerce yürütülen çalışmalarda elde edilecek olan soruşturma ve araştırma sonuçlarının ilgili mercilere sevki, elde edilme amacı, saklanması ve kamu görevinin niteliğine, yürütülecek görevin özelliğine göre ilgili idarece yasal mevzuat gereğince oluşturulan komisyon tarafından yapılacak değerlendirmede eşitlik, adalet, hakkaniyet, istikrar, idari güven ilkelerinin sağlanmasına yönelik kriterlerin dikkate alınmasının kurala bağlanması ve izlenecek bu yolda faaliyet gösteren kamu görevlilerine yönelik olarak gerekirse verilecek eğitimin ve arşiv kayıtları ile ilgili bilgilere dair her türlü gizliliğin sağlanması, kişisel hakların kötüye kullanılmasının önlenmesi ve bu doğrultuda istenilme amacı dışında ve kötüye kullanılmasına meydan vermeyecek şekilde hak ihlaline yol açılmaması, Anayasamızın 129. maddesinde yer alan hükümlerden hareketle de, güvenlik soruşturması ve arşiv

araştırması yapan, yaptıran, değerlendiren ve denetimini yapan idari ve adli mercilerle bu bilgilere erişimi mümkün olan her kademedeki kamu görevlilerinin, yetkilerini kötüye kullanmasının ve bilgilerin elde edilme amacı dışında kullanılmasının önlenmesi ve gerektiğinde yaptırma bağlanması, sorumlularının ve sorumluluklarının bilinmesi olduğu, hatta bu verilerin kişinin iznine bağlı olarak işlenebileceği ve kullanılacağı, istisnasının ise ülke menfaatleri, kamu düzeni olduğu açıktır.

Kaldı ki, bu ve benzeri dava dosyalarında, ilgililerin öncelikle ikamet yerlerine ait mülki idare amirliklerine bağlı emniyet birimlerince elde edilen istihbari bilgilerin, "gizli" kaydıyla, teyide muhtaç olup olmadığı, aksine kullanımlarda sorumluları hatırlatılarak ve imhasının sağlanacağı bildirilerek sunulu olduğu, yine bu bilgilere ikamet yerlerine ait birimlerden ulaşılamaması nedeniyle mahkemelerce emniyet teşkilatının konuyla ilgili merkez teşkilatı birimlerinden istenilmesi halinde arşiv kaydına alınmış olan bilgilerin ilgili Mahkemeye sunulduğu, Emniyet Teşkilatının farklı birimlerinin diğer birimlerce elde edilen kayıtlardan haberdar olmadığı, dolayısıyla talep makamlarınca yaptırılan ve Güvenlik Soruşturması ve Arşiv Araştırması Kanunu ve Yönetmeliği ile belirlenen usul ve esaslar çerçevesinde sonuçlandırıldığı görülen güvenlik soruşturması ve arşiv araştırması kapsamında yetkili istihbarat ve emniyet birimlerince toplanan bilgi ve belgelerin bu defa değerlendirilmek üzere talep makamlarına iletilmesine ve yargı mercilerince somut ve kanıtlanabilir nitelikte olup olmadığına dair hukukilik incelemesi yapılmasına kadar uzanan süreçte, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve Yönetmeliğine aykırı bir durum doğduğundan, dolayısıyla idarenin takdir yetkisine dayalı olarak tesis edildiği kabul edilmesi gereken bireysel işlemlerin, hukuken geçerli, somut bilgi ve belgelere dayalı olarak incelenmesi suretiyle çözüme kavuşturulmasına engel bir durum bulunduğundan söz edilmesi olanaklı değildir.

657 sayılı Kanununun 48. maddesinde yer alan genel şartlar arasında sayılan güvenlik soruşturması ve arşiv araştırması yapılmış olmak şartının iptal edilmiş olmasının, aynı maddede yer bulan; kurumların özel kanun veya diğer mevzuatında aranan şartların taşınması gerektiğine dair özel mevzuatın uygulanmasına engel teşkil etmeyeceği, zira 19 Temmuz 2018 tarihinden itibaren OHAL döneminin sona ermesiyle 4045 sayılı Kanuna dayanılarak 228 sayılı Cumhurbaşkanlığı kararıyla Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliğinde yapılan düzenlemenin, ilk defa kamu görevine girecekler için de yürürlüğünü sürdüren kuralları içerdiği konusunda kuşku bulunmamaktadır.

Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu personeli İle Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik

Yapılmasına İlişkin 4045 sayılı Kanununun 1. maddesinin son fıkrasında; "Devletin güvenliğini, ulusun varlığını ve bütünlüğünü iç ve dış menfaatlerinin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeler ile gizlilik dereceli kamu personeli ile meslek gruplarının tespiti, birim ve kısımların tanımlarının yapılması, güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak merciler ve üst kademe yöneticilerinin kimler olduğu Cumhurbaşkanınca yürürlüğe konulacak yönetmelik ile düzenlenir." hükmü yer almaktadır.

Türkiye Cumhuriyeti Anayasasının "Yürütme" ana başlıklı İkinci Bölümünde Cumhurbaşkanının görev ve yetkilerine hükmeden 104. maddenin 18. fıkrasında; "Cumhurbaşkanı, kanunların uygulanmasını sağlamak üzere ve bunlara aykırı olmamak şartıyla, yönetmelikler çıkarabilir." hükmü yer almakta olup yukarıda bahsi geçen yönetmelikte, düzenleme yetkisi Cumhurbaşkanı tarafından kullanılmış ve bu bağlamda, yukarıda bahsi geçen 4045 sayılı Kanununun 1. maddesine dayalı olarak çıkarılmış olan Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliğinin "Amaç" başlıklı 1. maddesine, 25/10/2018 tarihli ve 30576 sayılı Resmi Gazetede yayımlanan 228 sayılı Cumhurbaşkanlığı Kararı ile; "personel" ibaresinden sonra gelmek üzere "ile ilk defa veya yeniden kamu hizmeti ve görevlerine atanacaklar" ibaresi eklenmiş olup anılan maddede; "Bu Yönetmeliğin amacı; yetkili olmayan kişilerin bilgi sahibi olmaları halinde Devletin güvenliğinin, iç ve dış menfaatlerinin, ulusal varlığın ve bütünlüğün zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu bakanlıklar ile kamu kurum ve kuruluşlarının gizlilik dereceli birim ve kısımlarını belirlemek, Türk Silahlı Kuvvetlerinde, emniyet ve istihbarat teşkilatlarında, ceza infaz kurumları ve tutukevlerinde çalışacak personel ile ilk defa veya yeniden kamu hizmeti ve görevlerine atanacaklar hakkında yapılacak güvenlik soruşturması ve arşiv araştırmasını düzenlemektir." kuralı ile "Kapsam" başlıklı 2. Maddesine yine 25/10/2018 tarihli ve 30576 sayılı Resmi Gazetede yayımlanan 228 sayılı Cumhurbaşkanlığı Kararı ile; "çalışacak personeli," ibaresinden sonra gelmek üzere "ilk defa veya yeniden kamu hizmeti ve görevlerine atanacakları" ibaresi eklenmiş olup bahsi geçen 2. maddede; "Bu Yönetmelik; yetkili olmayan kişilerin bilgi sahibi olmaları halinde Devletin güvenliğinin, iç ve dış menfaatlerinin, ulusal varlığın ve bütünlüğün zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeleri, bunların toplanmasını ve işlemini yürüten bakanlıklar ile kamu kurum ve kuruluşlarının ilgili birim ve kısımlarının belirlenmesini, Türk Silahlı Kuvvetlerinde, emniyet ve istihbarat teşkilatlarında, ceza infaz kurumları ve tutukevlerinde çalışacak personeli, ilk defa veya yeniden kamu hizmeti ve görevlerine atanacakları ayrıca bakanlıklar ile kamu kurum ve kuruluşlarının yurtdışı teşkilatlarında sürekli görevlendirilecek bütün personel için yapılacak güvenlik soruşturması ve arşiv araştırmasının esas ve usullerini, bunu yapacak mercileri, hakkında güvenlik soruşturması ve arşiv araştırması yapılacak gizlilik dereceli yerlerde çalışan kamu personeli

ile meslek grupları ve üst kademe yöneticilerini kapsar." kuralı getirilmiş olup yürürlükteki bu Yönetmelik ile güvenlik soruşturması ve arşiv araştırmasını yapacak makamların, personelin, izlenecek yöntemin, güvenlik soruşturması ve arşiv araştırmasının her evresinde kesinlikle gizliliğe uyulacağı, soruşturma ve araştırma evre ve sonucunun bilmesi gerekenlerden başkasına açıklanmayacağına kurala bağlandığı görülmektedir.

Öte yandan, kanun koyucu demokratik toplum ve ölçülülük ilkesiyle bağlıdır ve temel hak ve hürriyetler üzerine getirilen sınırlamaların ölçülü olabilmesi için de, önleyici düzenleme ile öngörülen çözüm arasında adaletli ve kabul edilebilir bir denge kurulmaya çalışılması ve önleyici araç ile ulaşılmak istenen amaç arasındaki mantıki bağın kaybolmaması gerekmektedir.

Avrupa Konseyi Bakanlar Komitesince 11 Mart 1980 tarihinde kabul edilen "İdari Takdir Yetkisinin Kullanılmasına İlişkin R(80) 2 sayılı Tavsiye kararında; idari takdir yetkisinin kullanılmasında uygulanacak temel ilkelere göre takdir yetkisini kullanan bir idari makamın yetkinin verilmiş amacından başka amaç güdemeyeceği, yalnızca somut olaya ilişkin unsurları hesaba katarak nesnellığe ve tarafsızlığa uyacağı, hakkaniyete uymayan ayrımcılıktan kaçınarak yasa önünde eşitlik ilkesini gözeticeği, işlemin amacıyla kişilerin hakları, özgürlükleri ve menfaatleri üzerindeki olumsuz etkileri arasında denge sağlayacağı, idarelerin yasalarla kendisine tanınan takdir yetkisini adalet, hakkaniyet ve kamu yararı ölçütlerini göz önünde tutarak kullanması, Anayasanın 10. maddesi kapsamında kanun önünde eşitlik ilkesine uygun hareket etmesi gerekmekte olduğuna vurgu yapılmıştır.

Bu durumda, Anayasa Mahkemesi'nin iptal kararının gerekçesine bağlı kalınarak Devlet memurluğuna alınma şartları arasından çıkarıldığına kabulüne olanak bulunmayan güvenlik soruşturması ve arşiv araştırması sonucuna dayalı olarak dava konusu işlemin tesisine yol açan sebebin, bireyin atamasının yapılmasına engel teşkil edecek nitelik ve ağırlıkta olup olmadığının saptanması, idare hukukunun yargısal denetim yetkisi içinde olup ilk defa veya yeniden kamu hizmeti ve görevlerine atanacaklar bakımından yapılacak güvenlik soruşturması ve arşiv araştırmasına dair usul ve esasların, alınacak tedbirlerin, gizlilik ilkelerinin açık ve net olarak ilgili mevzuatta kurala bağlandığının, kişisel verilerin teminat altına kanunla alındığının görülmesi karşısında davacı yönünden (Danıştay Birinci Dairesi'nin 25/03/2003 tarihli ve E:2003/15, K:2003/40 sayılı kararında belirtildiği üzere, Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği hükümlerinin, hakkında güvenlik soruşturması ve arşiv araştırması yapılacak kişilerle sınırlı olmayıp kişi hakkında yeterli ve sağlıklı bir değerlendirme yapılabilmesi için ilgilinin içinde bulunduğu ortam ile yakınlarını ve birinci derece akrabalarını da kapsayacak şekilde) somut ve kanıtlanabilir nitelikteki

bilgi ve belgelerin tespitine yönelik hukukilik incelemesi yapıldığında, istihbari bilgilerin niteliği itibariyle Mahkemece verilen kararda hukuka aykırılık bulunmadığı oyuyla; çoğunluk kararına esas ve gerekçe yönlerinden katılmıyorum.

Ankara BİM - 1. İdari Dava Dairesi (E. 2020/324)

Ankara Bölge İdare Mahkemesi, 1. İDD, E. 2020/324 K. 2020/791 T. 11.3.2020

Esas No.: 2020/324

Karar No.: 2020/791

Karar tarihi: 11.03.2020

İSTEMİN ÖZETİ: 2019 Yılı İlk Defa ve Yeniden Atama Kurası sonucu N1 Nolu Acil Sağlık Hizmetleri İstasyonuna tabip olarak yerleştirilmesi yapılan davacı tarafından, 657 sayılı Devlet Memurları Kanununun 48. maddesinin 1. fıkrasının (A) bendindeki atama şartlarını taşımadığından bahisle atamasının yapılmamasına yönelik Sağlık Bakanlığı Yönetim Hizmetleri Genel Müdürlüğünün 16.05.2019 tarih ve 903.02.01 sayılı işleminin iptali istemiyle açılan davanın; dava konusu işlemde hukuka aykırılık bulunmadığı gerekçesiyle reddine ilişkin olarak Ankara 10. İdare Mahkemesi'nce verilen 20/11/2019 gün ve E:2019/1242, K:2019/2191 sayılı kararın; hukuka, temel hak ve özgürlüklere aykırı olduğu, verilen kararın Anayasa'ya ve Avrupa İnsan Hakları Sözleşmesi hükümlerine uygun olmadığı, hak ihlali doğurduğu ileri sürülerek kaldırılması istenilmektedir.

SAVUNMANIN ÖZETİ: Mahkeme kararında hukuka aykırılık bulunmadığı ileri sürülerek, istinaf isteminin reddi gerektiği savunulmuştur.

TÜRK MİLLETİ ADINA

Karar veren Ankara Bölge İdare Mahkemesi 1. İdari Dava Dairesince, 2577 sayılı Yasanın değişik 45. maddesi uyarınca dava dosyası incelenerek gereği görüldü:

Dava; 2019 Yılı İlk Defa ve Yeniden Atama Kurası sonucu N1 Nolu Acil Sağlık Hizmetleri İstasyonuna tabip olarak yerleştirilmesi yapılan davacı tarafından, 657 sayılı Devlet Memurları Kanununun 48. maddesinin 1. fıkrasının (A) bendindeki atama şartlarını taşımadığından bahisle atamasının yapılmamasına yönelik Sağlık Bakanlığı Yönetim Hizmetleri Genel Müdürlüğünün 16.05.2019 tarih ve 903.02.01 sayılı işleminin iptali istemiyle açılmıştır.

657 sayılı Devlet Memurları Kanunu'nun "Genel ve Özel Şartlar" başlıklı 48.maddesinin 1.fıkrasının (A) bendine, önce 676 sayılı OHAL Kanun Hükmünde Kararnamesi'nin 74.maddesiyle daha sonra 7070 sayılı Kanunun 60.maddesi ile de aynen kabul edilen düzenleme ile sekizinci alt bent olarak "Güvenlik soruşturması ve/veya arşiv araştırması yapılmış olmak" hükmü eklenerek, Devlet Memuru

olabilmek için ilgili hakkında güvenlik soruşturması ve/veya arşiv araştırması yapılmış olunması şartı getirilmiştir.

Dava konusu işlem yukarıda belirtilen mevzuat hükmü uyarınca 657 sayılı Kanunun 48.maddesinin 1.fıkrasının (A) bendinin yukarıda sözü edilen (8) numaralı alt bendi hükmüne dayanılarak tesis edilmiştir.

Anayasa Mahkemesi'nin 24/07/2019 günlü, E:2018/73, K:2019/65 sayılı kararı ile;Anayasa Mahkemesinin yerleşik kararlarında da belirtildiği üzere "adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, öz geçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunduğu kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri" gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm verilerin kişisel veri olarak kabul edildiği, bu bağlamda güvenlik araştırması ve arşiv araştırmasıyla elde edilen verilerin kişisel veri niteliğinde olduğu, 657 sayılı Kanunun 48.maddesinin 1.fıkrasının (A) bendine (8) numaralı alt bent olarak eklenen söz konusu kuralla güvenlik soruşturması ve arşiv araştırması kapsamında kamu mercileri tarafından özel yaşamı ile ilgili sorular sorulması da dahil olmak üzere bir bireyin özel hayatı, iş ve sosyal yaşamıyla ilgili bilgilerin alınmasının, kaydedilmesinin ve kullanılmasının özel hayata saygı hakkına sınırlama niteliğinde olduğu,

Anayasa'nın 129.maddesinin birinci fıkrasında memurlar ve kamu görevlilerinin Anayasa ve kanunlara sadık kalarak faaliyette bulunma yükümlülüklerinin düzenlendiği, belirtilen hususlar gözetilerek kamu görevlerine atanacak kişiler bakımından birtakım şartlar getirilmesinin doğal olduğu, bu şekilde aranan niteliklerin, kamu hizmetinin etkin ve sağlıklı bir biçimde yürütülmesi amacına yönelik olduğu, dolayısıyla kamu görevine atanmadan önce kişilerin güvenlik soruşturması ve arşiv araştırmasının yapılmasını öngören kuralın kanun koyucunun takdir yetkisinde olduğu, ancak bu alanda düzenleme getiren kuralların, kamu makamlarına hangi koşullarda ve hangi sınırlar içinde tedbir uygulama ve özel hayatın gizliliğine yönelik müdahalelerde bulunma yetkisi verildiğinin yeterince açık olarak göstermesi ve olası kötüye kullanmalara karşı yeterli güvenceleri sağlaması gerektiği, kuralda güvenlik soruşturması ve/veya arşiv araştırması yapılması memurluğa alımlarda genel şartlar arasında sayılmasına karşın, güvenlik soruşturmasına ve arşiv araştırmasına konu edilecek bilgi ve belgelerin neler olduğuna, bu bilgilerin ne şekilde kullanılacağına, hangi mercilerin soruşturma ve araştırmayı yapacağına ilişkin herhangi bir düzenlemenin yapılmamış olduğu, diğer bir ifadeyle güvenlik soruşturması ve arşiv araştırmasının yapılmasına ve elde edilecek verilerin kullanılmasına ilişkin temel ilkeler belirlenmeksizin, kuralla sadece güvenlik soruşturması

ve arşiv araştırması yapılmasının devlet memurluğuna alımlarda aranacak şartlar arasında sayıldığı, güvenlik soruşturması ve arşiv araştırması sonucunda devlet memurluğuna alınmada esas alınacak kişisel veri niteliğindeki bilgilerin alınmasına, kullanılmasına ve işlenmesine yönelik güvenceler ve temel ilkeler kanunla belirlenmeksizin bunların alınmasına ve kullanılmasına izin verilmesinin Anayasa'nın 13. 20. ve 128. maddesiyle bağdaşmadığı ve bu nedenle dava konusu kuralın Anayasa'nın anılan maddelerine aykırı olduğu belirtilerek; 7070 sayılı Kanununun 60.maddesiyle 657 sayılı Kanununun 48.maddesinin 1.fıkrasının (A) bendine eklenen (8) numaralı alt bendinin iptaline karar verilmiştir.

Anayasa Mahkemesi'nin bu kararı 29/11/2019 günlü, 30963 sayılı Resmi Gazete'de yayımlanmıştır. Anayasa Mahkemesi bu düzenlemeyi iptal ederken ileri tarihli bir yürürlük süresi öngörmemiştir. Dolayısıyla, anılan karar Resmi Gazetede yayımlandığı tarihte yürürlüğe girmiştir.

Anayasa Mahkemesinin sözü edilen kararı ile iptal edilen yasa kuralı (657 sayılı Kanununun 48/1-A-8.bendi) dışında, farklı statüde ya da gizlilik derecesine sahip bazı yerlerde görev yapan kamu görevlileri ile ilgili olarak güvenlik soruşturması ve/veya arşiv araştırması yapılmasını öngören ayrı yasal düzenlemeler bulunmaktadır.

4045 sayılı Kanun, yetkili olmayan kişilerin bilgi sahibi olmaları halinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile Genelkurmay Başkanlığı, Milli Savunma Bakanlığı, jandarma, emniyet, sahil güvenlik ve istihbarat teşkilatlarında çalıştırılacak kamu personeli ile ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında güvenlik soruşturması ve arşiv araştırması yapılmasını düzenlemektedir. 12/04/2000 tarihli ve 24018 sayılı Resmi Gazete'de yayımlanan "Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği" de 4045 sayılı Kanun'un 1. maddesi uyarınca çıkarılmıştır.

Ayrıca, 399 sayılı Kanun Hükmünde Kararnamenin 7.maddesinin (f) bendi, 233 sayılı KHK'ya tabi Kamu İktisadi Teşebbüslerinde ve bağlı ortaklıklarda sözleşmeli personel olarak işe alınacaklarda güvenlik soruşturması ve arşiv araştırması yapılmış olmak koşulunun aranacağını kurala bağlamıştır.

4045 sayılı Kanununun 1.maddesi ve 399 sayılı KHK'nın 7.maddesinin (f) bendi yönünden Anayasa Mahkemesince verilmiş iptal kararı bulunmamaktadır. Dolayısıyla, anılan düzenlemeler kapsamında kalan kamu görevleri bakımından güvenlik soruşturması ve arşiv araştırması uygulamasının dayanağı kurallar halen yürürlükte bulunmaktadır. Bununla birlikte, Dairemizin 31/12/2019 tarihli ve E:2019/4902 sayılı kararı ile 4045 sayılı Kanununun 1.maddesinin, yine Dairemizin 31/12/2019 tarih ve E:2019/4116 sayılı kararı ile de 399 sayılı KHK'nın 7.maddesinin (f) bendinin Anayasa'nın 13.20. ve

128.maddelerine aykırı olduğundan bahisle iptalleri istemiyle itiraz yolu ile Anayasa Mahkemesine başvurulmuştur.

Dava konusu edilen işlemin dayanağını oluşturan yasa kuralı ise sözü edilen Anayasa Mahkemesi'nce iptal edildiğinden, Anayasa Mahkemesi kararının geriye yürümesi ve söz konusu karardan önce yürürlükte olan Anayasaya aykırı kurala göre tesis edilen işlemlere karşı açılan ve halen görülmekte olan davaların (olayımızda olduğu gibi), Anayasa Mahkemesi kararından ne şekilde etkileneceği hususunun öncelikle açıklığa kavuşturulması gerekmektedir.

Anayasa'nın153.maddesinin 3.fıkrası, "Kanun, Cumhurbaşkanlığı kararnamesi veya Türkiye Büyük Millet Meclisi İçtüzüğü yada bunların hükümleri, iptal kararlarının Resmi Gazete'de yayımlandığı tarihte yürürlükten kalkar. Gereken hallerde Anayasa Mahkemesi iptal hükmünün yürürlüğe gireceği tarihi ayrıca kararlaştırabilir. Bu tarih, Resmi Gazete'de yayımlandığı günden başlayarak bir yılı geçemez";5.fıkrası, "İptal kararları geriye yürümez"; 6.fıkrası ise, "Anayasa Mahkemesi Kararları Resmi Gazete'de hemen yayımlanır ve yasama, yürütme ve yargı organlarını, idare makamlarını, gerçek ve tüzel kişileri bağlar." kurallarını içermektedir.

Anayasa Mahkemesince bir kanunun veya kanun hükmünde kararnamenin tümünün ya da bunların belirli hükümlerinin Anayasa'ya aykırı bulunarak iptal edilmiş olduğu bilindiği halde eldeki davaların Anayasa'ya aykırılığı saptanmış olan kurallara göre görüşülüp çözümlenmesi, Anayasa'nın üstünlüğü prensibine ve hukuk devleti ilkesine aykırı düşeceği için uygun görülemez. Aksine bir durum, Anayasa'nın 153.maddesinde yer alan Anayasa Mahkemesi kararlarının bağlayıcı olduğu yönündeki hükme aykırılık oluşturur.

Öte yandan, Anayasanın 153.maddesinin 5.fıkrasında yer alan ve iptal kararlarının geriye yürümezliğine ilişkin bulunan kural, iptal edilen hükümlere göre kazanılmış olan hakların ortadan kaldırılmasına veya toplumun huzurunun bozulmasına yol açacak sonuçları önlemek amacıyla kabul edilmiş olup, bu kuralın mutlak anlamda anlaşılıp uygulanamayacağı açıktır.

Yargıtay'ın bir kararında belirtildiği üzere; Türk Anayasa sisteminde benimsenen iptal kararının geriye yürümezliği kuralının getiriliş amacı, kazanılmış hakları ve hukuksal güvenliği ortadan kaldıracı ya da toplumun adalet anlayışını zedeleyici sonuçlar doğurmasından kaygı duyulmasını önlemek, devlete olan güven duygularını sarsmamak, devlet yaşamında hukuk kargaşasına neden olmamak, hukuk güvenliğini ve istikrarını sağlamak olarak özetlenebilir. (Yargıtay 8.Hukuk Dairesi'nin 22/12/2011 tarih ve E:2010/508, K:2011/7468 sayılı kararı)

Bu bakımdan iptal kararlarının geriye yürümezliği ilkesi, kabul edilen önemli bir ilkedir.

Nitekim, Anayasa Mahkemesi, 12/12/1989 tarihli ve E:1989/11, K:1989/48 sayılı kararında, "Türk Anayasa sisteminde Devlete güven ilkesini sarsmamak ve ayrıca Devlet yaşamında bir karmaşaya neden olmamak için iptal kararlarının geriye yürümezliği kuralı kabul edilmiştir. Böylece, hukuksal ve nesnel alanda suçlarını doğuramaz bulunan durumların iptal kararlarının yürürlüğe gireceği güne kadarki dönem için geçerli sayılması sağlanmıştır." denilmek suretiyle konunun önemi vurgulanmıştır.

Anayasa Mahkemesi'nin 19/12/1989 tarihli ve E:1998/14, K: 1989/49 sayılı kararında da aynen; "bir hukuk kuralının yürürlüğü sırasında, bu kurala uygun bir biçimde tüm sonuçlarıyla kesin olarak edinilmiş hakların korunmasının Hukuk Devleti'nin gereği olduğu" vurgulanmaktadır.

Aktarılan Anayasa Mahkemesi kararları, iptal kararlarının geriye yürümezliği kuralının kazanılmış olan hakların ortadan kaldırılmasını önlemek amacıyla getirilen bir kural olduğunu açıkça ortaya koymaktadır.

Anayasa Mahkemesi'nin bahsedilen kararları ile aynı yönde olmak üzere Danıştay'ın kararlarında da istikrarlı bir şekilde, "iptal kararlarının geriye yürümeyeceği" kuralının, kazanılmış hakları saklı tutmak, hukuki istikrarı ve hukuk güvenliğini sağlamak ve kamu idaresini korumak amacıyla getirildiği ve anılan kuralın belirtilen amaca uygun olarak yorumlanıp uygulanması gerektiği görüşü benimsenmiştir. (Danıştay 8.Daire E:1967/153, K:1968/2783; Danıştay 10.Daire E:1996/9928, K:1999/2597; Danıştay 2.Daire E:2004/1545, K:2005/1886; Danıştay 2.Daire E:2004/7423, K:2005/113; Danıştay İDDK E: 2007/2326, K:2008/1724; Danıştay İDDK E:2010/2292, K:2013/3366; Danıştay İDDK E:2013/826, K:2015/1654; Danıştay 5.Daire E:2010/6456, K:2013/5790; Danıştay 4.Daire E:2011/2546, K:2011/3384, Danıştay 3.Daire E:2015/31, K:2015/4299)

Belirtilen hukuksal durumun doğal sonucu olarak, bir kanun ya da kanun hükmünde kararnamenin uygulanması nedeniyle dava açmak durumunda kalan ve Anayasa'nın 153. maddesi uyarınca itiraz yoluyla Anayasa Mahkemesine başvurulmasını isteme hakkına sahip olan kişilerin de, olayımızda olduğu gibi, hak ve menfaatlerini ihlal eden kuralın iptal davası veya itiraz yoluyla daha önce yapılan başvuru sonucunda Anayasa Mahkemesince iptal edilmiş olması halinde iptal hükmünün hukuki sonuçlarından yararlanmaları gerektiği açıktır.

Bu nedenle, sözü edilen Anayasa Mahkemesi kararı ile Anayasa'ya aykırılığı nedeniyle iptal edilen 657 sayılı Kanun'un 48.maddesinin 1.fıkrasının (A) bendinin (8) numaralı alt bendine dayanılarak tesis edilen dava konusu işlemde hukuka uyarlık bulunmamaktadır.

Öte yandan; Anayasa'nın 129. maddesinin birinci fıkrasında, memurlar ve kamu görevlilerinin Anayasa ve Kanunlara sadık kalarak faaliyette bulunma yükümlülükleri düzenlenmiştir. Ayrıca, 657 sayılı Kanun'da bu sadakat yükümlülüğünün yanı sıra kamu görevlilerine tarafsızlık ve devlete bağlılık yükümlülükleri de getirilmiştir. Sözü edilen Anayasa Mahkemesi kararında da açıklandığı üzere, belirtilen hususlar gözetilerek kamu görevlerine atanacak kişiler bakımından bir takım şartlar getirilmesi doğaldır. Bu şekilde aranan nitelikler ve kanunda öngörülen kısıtlamalar, kamu hizmetinin etkin ve sağlıklı bir şekilde yürütülmesi amacına yöneliktir. Dolayısıyla, idarenin kamu görevine atanacak kişilerin tabi olacağı güvenlik soruşturması ve arşiv araştırması konusunda kanunla temel çerçeveyi ortaya koyan kurallar getirmesi elbette mümkündür.

Avrupa İnsan Hakları Mahkemesi (AİHM), devletlerin milli güvenliğin korunması amacını gerçekleştirmede sahip oldukları takdir yetkisinin geniş olduğunu kabul etmektedir. AİHM, Sözleşme'ye taraf devletin milli güvenliği korumak için yetkili ulusal makamlarına ilk olarak kişiler hakkında bilgi toplama ve halka açık olmayan siciller tutma, ikinci olarak milli güvenlik bakımından önemli kadrolarda çalışmak isteyen adayların bu işe uygunluğunu takdir ederken bu bilgiyi kullanma yetkisi veren kurallara sahip olmaları gerektiğinde kuşku bulunmadığını belirtmektedir. (Leander/İsveç, SB.No: 9248/81, 26/3/1987)

Anayasa Mahkemesinin kararına ve AİHM içtihatlarına göre; kamu görevine atanmadan önce kişilerin güvenlik soruşturması ve arşiv araştırmasının yapılmasını öngören kural getirilmesi kanun koyucunun takdir yetkisindedir. Ancak, bu alanda düzenleme getiren kuralların kamu makamlarına hangi koşullarda ve hangi sınırlar içinde tedbir uygulama ve özel hayatın gizliliğine yönelik müdahalelerde bulunma yetkisi verildiğini yeterince açık göstermesi ve olası kötüye kullanmalara karşı yeterli güvenceleri sağlaması gerekir.

Bu bağlamda, Anayasa Mahkemesi'nin sözü edilen iptal kararının gerekçesi dikkate alındığında, Anayasa Mahkemesi kararı, güvenlik soruşturmasının hiçbir şekilde yapılmayacağını değil, aksine güvenlik soruşturması detaylarının kanunda gösterilmesi, kişisel verilerin güvenliğine ve özel hayatın gizliliğine ilişkin güvenceleri sağlayan kuralların kanunda yer alması koşuluyla güvenlik soruşturmasının ve arşiv araştırmasının yapılabileceğini ortaya koymuştur.

Diğer yandan; bakılan davada, Anayasa Mahkemesi kararının Resmi Gazete'de yayımlandığı tarihten önce dava konusu işlemin hukuka aykırı olduğunu tespit eden, dolayısıyla uyuşmazlığın esası yönünden verilen bu nedenle de davacının atanması sonucunu doğuracak nitelikte bir karar (yürütmenin durdurulması ya da iptal kararı) bulunmamaktadır.

Belirtilen hukuki çerçevede konu incelendiğinde, dava konusu işlemin dayanağı yasa kuralının Anayasa Mahkemesi'nce iptal edilmesi nedeniyle dava konusu işlemin iptali yönünde verilen iş bu kararın, davacının hiç bir işleme gerek olmadan doğrudan kamu görevine atanması sonucunu doğurmayacağı sonucuna ulaşılmaktadır.

Anayasa Mahkemesi kararında belirtildiği üzere yeterli güvenceleri sağlayacak yeni bir yasal düzenleme yapılması durumunda, bu yasal düzenlemeye göre davacının durumunun davalı idarece makul bir süre içinde yeniden değerlendirmeye tabi tutulabileceği ve bu değerlendirmenin sonucunda davacının uyuşmazlığa konu kamu görevine atanıp atanamayacağına ilişkin yeniden bir işlem tesis edilmesi gerektiği kuşkusuzdur. Ayrıca, yeni yasal düzenleme uyarınca yapılacak değerlendirmenin sonucunda davacı açısından yine olumsuz bir sonucun ortaya çıkması halinde, bunun yargısal denetiminin mümkün olması nedeniyle, davacının durumunun yeniden değerlendirilmesi davacıyı güvencesiz bırakmadığı gibi, Anayasa Mahkemesinin aktarılan gerekçesi karşısında bu durum, bir hak ihlali de doğurmamaktadır.

Açıklanan nedenlerle; davacı tarafın İSTİNAF BAŞVURUSUNUN KABULÜNE,Ankara 10. İdare Mahkemesi'nce verilen 20/11/2019 gün ve E:2019/1242, K:2019/2191 sayılı kararın KALDIRILMASINA;2577 sayılı Yasanın değişik 45. maddesinin 4. fıkrası uyarınca esastan incelenen davada, dava konusu işlemin İPTALİNE; aşağıda dökümü yapılan, mahkeme ve istinaf safhasına ait toplam 690,50 TL yargılama giderinin ve hüküm tarihindeki Avukatlık Asgari Ücreti Tarifesine göre 1.700,00 TL avukatlık ücretinin davalı idareden alınarak davacı tarafa verilmesine, posta gideri avansından artan miktarın istenilmesi halinde istinaf başvurusunda bulunan tarafa iadesine, 11/03/2020 tarihinde oyçokluğuyla ve kesinolarak karar verildi.

AZLIK OYU :Uyuşmazlık, kamu görevine yerleştirilmiş olan davacı hakkında Devlet memurluğuna alınacaklar için genel atama koşulları arasında sayılan 657 sayılı Kanununun 48. maddesinin 1. fıkrasının A-8 bendi gereğince davalı idarece yaptırılan güvenlik soruşturması ve arşiv araştırması sonucunun davalı idare bünyesinde oluşturulan Değerlendirme Komisyonu tarafından olumsuz olarak değerlendirildiğinden bahisle atamasının yapılmaması yönünde tesis edilen işlemin iptali isteminden kaynaklanmıştır.

Olağanüstü dönemde çıkarılan 03/10/2016 kabul tarihli 676 sayılı Kanun Hükmünde Kararnamenin 74. maddesi ile 657 sayılı Devlet Memurları Kanunu'nun Devlet memurluğuna alınacaklarda aranacak genel ve özel şartların düzenlendiği48. maddesinin1. fıkrasının A bendine "Güvenlik soruşturması ve/veya arşiv araştırması yapılmış olmak" şartını içeren 8 numaralı alt bendin eklendiği, bilahare 01/02/2018 tarihli, 7070 sayılı Olağanüstü Hal Kapsamında Bazı Düzenlemeler Yapılması

Hakkında Kanunun 60. maddesi ile aynen kabulüne karar verilen (8) numaralı alt bent hükmü gereğince Devlet memurluğuna alınan kişilerin, herhangi bir özel görev ve kurum sınırlamasına tabi tutulmaksızın güvenlik soruşturması ve arşiv araştırmalarının yapılmasının, gerek doğrudan bu yasaya tabi olan, gerekse bu yasa maddesine yollamada bulunulan diğer özel mevzuata tabi idarelerce zorunlu hale getirildiği görülmektedir.

Yukarıda belirtilen 657 sayılı Kanunun 48. maddesinin 1/A fıkrasının (8) numaralı alt bent hükmünü aynen kabul ederek yasalaştıran 01/02/2018 tarihli, 7070 sayılı Kanunun 60. maddesiyle 657 sayılı Kanunun 48. maddesinin 1/A fıkrasına eklenen 8 numaralı bendin, Anayasaya aykırılığı nedeniyle Anayasa Mahkemesine gidilmiş ve Anayasa Mahkemesi'nce; bu kuralda güvenlik soruşturması ve arşiv araştırmasına konu edilen bilgi ve belgelerin neler olduğu, bu bilgilerin ne şekilde kullanılacağı, hangi mercilerin soruşturma ve araştırmayı yapacağına ilişkin herhangi bir düzenleme yapılmadığı, bir başka ifadeyle temel ilkeler belirlenmeksizin Devlet memurluğuna alınma şartı olarak getirildiği belirtilerek Devlet memurluğuna atanmada kişisel veri niteliğindeki bilgilerin alınmasına, kullanılmasına ve işlenmesine yönelik güvenceler ve temel ilkeler kanunla belirlenmeksizin bunların alınmasına ve kullanılmasına izin verilmesinin Anayasanın 13., 20. ve 128. maddeleriyle bağdaşmadığı gerekçesiyle 657 sayılı Kanunun 48. maddesinin 1/A fıkrasına eklenen 8 numaralı alt bentte yer alan "Güvenlik soruşturması ve/veya arşiv araştırması yapılmış olmak." ibaresi iptal edilmişse de, Türkiye Cumhuriyeti Anayasasının 153. maddesinde; "Anayasa Mahkemesinin kararları kesindir. İptal kararları gerekçesi yazılmadan açıklanamaz...Kanun, Cumhurbaşkanlığı kararnamesi veya Türkiye Büyük Millet Meclisi İçtüzüğü ya da bunların hükümleri, iptal kararlarının Resmî Gazetede yayımlandığı tarihte yürürlükten kalkar...İptal kararının yürürlüğe girişinin ertelendiği durumlarda, Türkiye Büyük Millet Meclisi, iptal kararının ortaya çıkardığı hukuki boşluğu dolduracak kanun (...) teklifini öncelikle görüşüp karara bağlar..." hükmü gereğince eldeki uyumsuzluklar bakımından; Anayasa Mahkemesi'nin öncelikle Anayasanın 13., 20. ve 128. maddelerinde düzenlemesini bulan kanunilik ilkesine aykırılığından bahisle verilmiş olduğu görülen iptal kararının gerekçesi uyarınca yasamaorganının düzenleme yapmadığı durumlarda, diğer hukuk normlarında yer alan düzenlemelerden hareketle Türk Medeni Kanunu'nun 1. maddesinin ikinci fıkrasında yer alan "Kanunda uygulanabilir bir hüküm yoksa, hakim örf ve adet hukukuna göre, bu da yoksa kanun koyucu olsaydı nasıl bir kural koyacak idiyse ona göre karar verir" kuralı karşısında, Anayasa Mahkemesi'nce verilen kararın gerekçesi ve hukukun genel prensipleri gözetilerek, yargı içtihatlarıyla çözüme gidileceğinin kabulü gerekmektedir.

Danıştay İdari Dava Daireleri Kurulu'nun 21/11/2012 tarihli, E:2008/3456, K:2012/2162 sayılı ve benzer nitelikteki kararlarında belirtildiği gibi; Anayasanın 153. maddesinin son fıkrası hükmü, Anayasa Mahkemesi kararlarının sadece hüküm fıkralarının değil, hükme dayanak oluşturan temel gerekçelerinin de bağlayıcı olduğunun kabul edilmesini zorunlu kılmaktadır. Buna göre, yargı kararlarının gerekçeleriyle birlikte değerlendirilmesi gerekmekte olup gerek Anayasa Mahkemesinin, gerekse Danıştayın konuya ilişkin kararları ışığında, somut olay çözümlenirken Anayasa Mahkemesi kararında belirtilen sınırlamalar kapsamında adil, hakkaniyetli, objektif hukuk kuralları işletilerek kişisel verilerin güvenlik soruşturması ve arşiv araştırması sonucunun olumsuz olarak değerlendirilmesini gerektirip gerektirmediği hususunun hukukiliğinin irdelenmesine engel teşkil edecek bir durum bulunmamaktadır.

Anayasa'nın 152. ve 153. maddelerinde belirtildiği üzere; mahkemeler bir yasa kuralının Anayasa Mahkemesince iptal edilmesi halinde yüksek mahkemenin kararına ve dayandığı gerekçeye uygun karar vermek zorundadır.

Kanunlar, lafzı ve ruhuyla bir bütündür, o halde Anayasa Mahkemesi'nin mezkur iptal hükmünün; bu hükmün dayandığı kişisel hak ihlaline neden olabilecek unsurlar ve kanunilik ilkesi yönünden uyumsuzluk üzerindeki hukuki etki ve sonuçlarının, Anayasanın 153. maddesinde yer alan anayasal hüküm gereğince iptal gerekçesiyle birlikte değerlendirilmesi gerekmekte olup iptal edilen şart hüküm gereğince yapılmış olan güvenlik soruşturması ve arşiv araştırması sonucunun davacı yönünden değerlendirme dışı bırakılacağından söz edilemez.

Mezkur iptal kararının yayımlandığı Resmi Gazetede, yürürlük tarihi olarak Anayasa Mahkemesince ileri bir tarih öngörülmemiştir. Anayasamızın 153. maddesinde hüküm altına alınan amir kural; iptal kararlarının Resmî Gazetede yayımlandığı tarihte yürürlükten kalkmasıdır. İptal kararlarının yürürlüğe girişinin ertelendiği durumlarda ise, iptal kararıyla çıkan hukuki boşluğun giderilmesi için idareye yeni bir düzenleme yapmasına olanak sağlayacak süre tanınmasıdır. Anayasa Mahkemesi'nin; güvenlik soruşturması ve arşiv araştırmasının esasen idarelerin takdirinde olduğu gerekçesine dayalı olarak anılan iptal kararının, hukuki bir boşluğa sebebiyet vermediği, eldeki uyumsuzluklarda yine Anayasa Mahkemesi'nce verilmiş önceki kararlarından hareketle öncelikle iptal gerekçesindeki hususlara bağlı kalınarak bu konuda diğer veya varsa özel mevzuatla getirilmiş kuralların uygulanmasına engel bir durum doğmadığı sonucuna varılmaktadır.

Anayasa Mahkemesi'nin iptal gerekçesinde ayrıntılı olarak bahsolunan; kişisel haklarla ilgili veriler bakımından şahıs hakkında elde edilen bilgi ve belgelere yönelik olarak kişisel hakların ihlaline sebebiyet vermeyecek şekilde davacı hakkındayapılmış olan soruşturma ve araştırmanın sonucunun

hukukiliğinin irdelenmesine engel bir hüküm içermediğinin anlaşılması karşısında, uyuşmazlığın çözümünde bu konuda özel mevzuat niteliğinde olan 4045 sayılı Kanun ve ilgili Yönetmeliğin esas alınabileceği kabul edilmelidir.

Anayasa'nın 13. maddesinde, temel hak ve hürriyetlerin yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği ifade edilmiş, milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya (pozitif ayrımcılık yapılarak) başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak kişisel verilerin, çalışma hakkı bakımından açılan bu davalarda irdelenmesi, anayasal dayanaktan yoksun bırakılmamıştır.

Anayasanın 20. maddesinde öngörülen 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun yürürlükte olduğu ve bu Kanunun amaç maddesinden hareketle hangi hallerde Kanun hükümlerinin uygulanmayacağı kuralı, bu Kanunun 28. maddesinde düzenlenmiş olup Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu; zararın giderilmesini talep etme hakkı hariç ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddelerinin uygulanmayacağı haller sayılmış olup "a) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç araştırması için gerekli olması,b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi. c) Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması" hallerinde bu Kanunun uygulanmayacağı hükmü yer almakta olup ülke menfaatleri, kamu yararı ve hizmet gerekleri ilkeleri gereğince davacı hakkındaki güvenlik soruşturması sonucunun, üstün yarar ve amaçlar doğrultusunda, ancak temel ilkelere uygun ve orantılı olmak üzere ilgili mevzuatta sınırları gösterilen hukuki düzeyde irdelenmesi gerektiği kabul edilmelidir.

Anılan kuralın iptaline dair Anayasa Mahkemesi kararından anlaşıldığı üzere; kamu görevine ilk defa atanacaklar (ve belli kadroları kendi özel mevzuatına göre kazanacak olanlar) bakımından güvenlik soruşturması ve arşiv araştırması yapılması suretiyle Devletin kamu gücünü kullanarak tek taraflı, keyfi ve sui niyetle hak ihlaline sebep olunduğu değil, bu soruşturma ve araştırmayı yapan ve yaptırın yetkililerce başvuru usul ve esaslar ile öncelikle ilgiliye ait kişisel bilgilerin elde edilme aşamasındaki faaliyetler, bilahare bireyler hakkında ehil ve eğitimli görevlilerce yürütülen çalışmalarda elde edilecek olan soruşturma ve araştırma sonuçlarının ilgili mercilere sevki, elde edilme amacı, saklanması ve kamu görevinin niteliğine, yürütülecek görevin özelliğine göre ilgili

idarece yasal mevzuat gereğince oluşturulan komisyon tarafından yapılacak değerlendirmede eşitlik, adalet, hakkaniyet, istikrar, idari güven ilkelerinin sağlanmasına yönelik kriterlerin dikkate alınmasının kurala bağlanması ve izlenecek bu yolda faaliyet gösteren kamu görevlilerine yönelik olarak gerekirse verilecek eğitimin ve arşiv kayıtları ile ilgili bilgilere dair her türlü gizliliğin sağlanması, kişisel hakların kötüye kullanılmasının önlenmesi ve bu doğrultuda istenilme amacı dışında ve kötüye kullanılmasına meydan vermeyecek şekilde hak ihlaline yol açılmaması, Anayasamızın 129. maddesinde yer alan hükümlerden hareketle de, güvenlik soruşturması ve arşiv araştırması yapan, yaptıran, değerlendiren ve denetimini yapan idari ve adli mercilerle bu bilgilere erişimi mümkün olan her kademedeki kamu görevlilerinin, yetkilerini kötüye kullanmasının ve bilgilerin elde edilme amacı dışında kullanılmasının önlenmesi ve gerektiğinde yaptırma bağlanması, sorumlularının ve sorumluluklarının bilinmesi olduğu, hatta bu verilerin kişinin iznine bağlı olarak işlenebileceği ve kullanılacağı, istisnasının ise ülke menfaatleri, kamu düzeni olduğu açıktır.

Kaldı ki, bu ve benzeri dava dosyalarında, ilgililerin öncelikle ikamet yerlerine ait mülki idare amirliklerine bağlı emniyet birimlerince elde edilen istihbari bilgilerin, "gizli" kaydıyla, teyide muhtaç olup olmadığı, aksine kullanımlarda sorumluları hatırlatılarak ve imhasının sağlanacağı bildirilerek sunulu olduğu, yine bu bilgilere ikamet yerlerine ait birimlerden ulaşılamaması nedeniyle mahkemelerce emniyet teşkilatının konuyla ilgili merkez teşkilatı birimlerinden istenilmesi halinde arşiv kaydına alınmış olan bilgilerin ilgili Mahkemeye sunulduğu, Emniyet Teşkilatının farklı birimlerinin diğer birimlerce elde edilen kayıtlardan haberdar olmadığı, dolayısıyla talep makamlarınca yaptırılan ve Güvenlik Soruşturması ve Arşiv Araştırması Kanunu ve Yönetmeliği ile belirlenen usul ve esaslar çerçevesinde sonuçlandırıldığı görülen güvenlik soruşturması ve arşiv araştırması kapsamında yetkili istihbarat ve emniyet birimlerince toplanan bilgi ve belgelerin bu defa değerlendirilmek üzere talep makamlarına iletilmesine ve yargı mercilerince somut ve kanıtlanabilir nitelikte olup olmadığına dair hukukilik incelemesi yapılmasına kadar uzanan süreçte, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve Yönetmeliğine aykırı bir durum doğduğundan, dolayısıyla idarenin takdir yetkisine dayalı olarak tesis edildiği kabul edilmesi gereken bireysel işlemlerin, hukuken geçerli, somut bilgi ve belgelere dayalı olarak incelenmesi suretiyle çözüme kavuşturulmasına engel bir durum bulunduğu söz edilmesi olanaklı değildir.

657 sayılı Kanununun 48. maddesinde yer alan genel şartlar arasında sayılan güvenlik soruşturması ve arşiv araştırması yapılmış olmak şartının iptal edilmiş olmasının, aynı maddede yer bulan; kurumların özel kanun veya diğer mevzuatında aranan şartların taşınması gerektiğine dair özel

mevzuatın uygulanmasına engel teşkil etmeyeceği, zira 19 Temmuz 2018 tarihinden itibaren OHAL döneminin sona ermesiyle 4045 sayılı Kanuna dayanılarak 228 sayılı Cumhurbaşkanlığı kararıyla Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliğinde yapılan düzenlemenin, ilk defa kamu görevine girecekler için de yürürlüğünü sürdüren kuralları içerdiği konusunda kuşku bulunmamaktadır.

Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu personeli İle Kamu Görevine Alınmayanların Haklarının Geri Verilmesine ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin 4045 sayılı Kanunun 1. maddesinin son fıkrasında; "Devletin güvenliğini, ulusun varlığını ve bütünlüğünü iç ve dış menfaatlerinin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeler ile gizlilik dereceli kamu personeli ile meslek gruplarının tespiti, birim ve kısımların tanımlarının yapılması, güvenlik soruşturmasının ve arşiv araştırmasının usul ve esasları ile bunu yapacak merciler ve üst kademe yöneticilerinin kimler olduğu Cumhurbaşkanınca yürürlüğe konulacak yönetmelik ile düzenlenir." hükmü yer almaktadır.

Türkiye Cumhuriyeti Anayasasının "Yürütme" ana başlıklı İkinci Bölümünde Cumhurbaşkanının görev ve yetkilerine hükmeden 104. maddenin 18. fıkrasında; "Cumhurbaşkanı, kanunların uygulanmasını sağlamak üzere ve bunlara aykırı olmamak şartıyla, yönetmelikler çıkarabilir." hükmü yer almakta olup yukarıda bahsi geçen yönetmelikte, düzenleme yetkisi Cumhurbaşkanı tarafından kullanılmış ve bu bağlamda, yukarıda bahsi geçen 4045 sayılı Kanunun 1. maddesine dayalı olarak çıkarılmış olan Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliğinin "Amaç" başlıklı 1. maddesine, 25/10/2018 tarihli ve 30576 sayılı Resmi Gazetede yayımlanan 228 sayılı Cumhurbaşkanlığı Kararı ile; "personel" ibaresinden sonra gelmek üzere "ile ilk defa veya yeniden kamu hizmeti ve görevlerine atanacaklar" ibaresi eklenmiş olup anılan maddede; "Bu Yönetmeliğin amacı; yetkili olmayan kişilerin bilgi sahibi olmaları halinde Devletin güvenliğinin, iç ve dış menfaatlerinin, ulusal varlığın ve bütünlüğün zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu bakanlıklar ile kamu kurum ve kuruluşlarının gizlilik dereceli birim ve kısımlarını belirlemek, Türk Silahlı Kuvvetlerinde, emniyet ve istihbarat teşkilatlarında, ceza infaz kurumları ve tutukevlerinde çalışacak personel ile ilk defa veya yeniden kamu hizmeti ve görevlerine atanacaklar hakkında yapılacak güvenlik soruşturması ve arşiv araştırmasını düzenlemektir." kuralı ile "Kapsam" başlıklı 2. Maddesine yine 25/10/2018 tarihli ve 30576 sayılı Resmi Gazetede yayımlanan 228 sayılı Cumhurbaşkanlığı Kararı ile; "çalışacak personeli," ibaresinden sonra gelmek üzere "ilk defa veya yeniden kamu hizmeti ve görevlerine atanacakları" ibaresi eklenmiş olup bahsi geçen 2. maddede; "Bu Yönetmelik; yetkili olmayan kişilerin bilgi sahibi olmaları halinde Devletin

güvenliğinin, iç ve dış menfaatlerinin, ulusal varlığın ve bütünlüğün zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgeleri, bunların toplanmasını ve işlemini yürüten bakanlıklar ile kamu kurum ve kuruluşlarının ilgili birim ve kısımlarının belirlenmesini, Türk Silahlı Kuvvetlerinde, emniyet ve istihbarat teşkilatlarında, ceza infaz kurumları ve tutukevlerinde çalışacak personeli, ilk defa veya yeniden kamu hizmeti ve görevlerine atanacakları ayrıca bakanlıklar ile kamu kurum ve kuruluşlarının yurtdışı teşkilatlarında sürekli görevlendirilecek bütün personel için yapılacak güvenlik soruşturması ve arşiv araştırmasının esas ve usullerini, bunu yapacak mercileri, hakkında güvenlik soruşturması ve arşiv araştırması yapılacak gizlilik dereceli yerlerde çalışan kamu personeli ile meslek grupları ve üst kademe yöneticilerini kapsar." kuralı getirilmiş olup yürürlükteki bu Yönetmelik ile güvenlik soruşturması ve arşiv araştırmasını yapacak makamların, personelin, izlenecek yöntemin, güvenlik soruşturması ve arşiv araştırmasının her evresinde kesinlikle gizliliğe uyulacağı, soruşturma ve araştırma evre ve sonucunun bilmesi gerekenlerden başkasına açıklanmayacağına kurala bağlandığı görülmektedir.

Öte yandan, kanun koyucu demokratik toplum ve ölçülülük ilkesiyle bağlıdır ve temel hak ve hürriyetler üzerine getirilen sınırlamaların ölçülü olabilmesi için de, önleyici düzenleme ile öngörülen çözüm arasında adaletli ve kabul edilebilir bir denge kurulmaya çalışılması ve önleyici araç ile ulaşılmak istenen amaç arasındaki mantıki bağın kaybolmaması gerekmektedir.

Avrupa Konseyi Bakanlar Komitesince 11 Mart 1980 tarihinde kabul edilen "İdari Takdir Yetkisinin Kullanılmasına İlişkin R(80) 2 sayılı Tavsiye kararında; idari takdir yetkisinin kullanılmasında uygulanacak temel ilkelere göre takdir yetkisini kullanan bir idari makamın yetkinin verilmiş amacından başka amaç güdemeyeceği, yalnızca somut olaya ilişkin unsurları hesaba katarak nesnellığe ve tarafsızlığa uyacağı, hakkaniyete uymayan ayrımcılıktan kaçınarak yasa önünde eşitlik ilkesini gözeticeği, işlemin amacıyla kişilerin hakları, özgürlükleri ve menfaatleri üzerindeki olumsuz etkileri arasında denge sağlayacağı, idarelerin yasalarla kendisine tanınan takdir yetkisini adalet, hakkaniyet ve kamu yararı ölçütlerini göz önünde tutarak kullanması, Anayasanın 10. maddesi kapsamında kanun önünde eşitlik ilkesine uygun hareket etmesi gerekmekte olduğuna vurgu yapılmıştır.

Bu durumda, Anayasa Mahkemesi'nin iptal kararının gerekçesine bağlı kalındığında, Devlet memurluğuna alınma şartları arasından çıkarıldığına kabulüne olanak bulunmayan güvenlik soruşturması ve arşiv araştırması sonucuna dayalı olarak dava konusu işlemin tesisine yol açan sebebin, bireyin atamasının yapılmasına engel teşkil edecek nitelik ve ağırlıkta olup olmadığının saptanması, idare hukukunun yargısal denetim yetkisi içinde olup ilk defa veya yeniden kamu

hizmeti ve görevlerine atanacaklar bakımından yapılacak güvenlik soruşturması ve arşiv araştırmasına dair usul ve esasların, alınacak tedbirlerin, gizlilik ilkelerinin açık ve net olarak ilgili mevzuatta kurala bağlandığının, kişisel verilerin teminat altına kanunla alındığının görülmesi karşısında, güvenlik soruşturması sonucu düzenlenen raporların, istihbari nitelikte bilgiler içermeleri halinde hukuken geçerli başka bilgi ve belgelerle doğrulanmadıkça ilgililer hakkında aleyhe sonuç doğuracak bir nitelik ve değerlendirme yapılmasının hukuk devleti ilkesiyle de bağdaştırılmayacağı yönündeki Danıştayın yerleşik içtihatlarından hareketle davacı yönünden (Danıştay Birinci Dairesi'nin 25/03/2003 tarihli ve E:2003/15, K:2003/40 sayılı kararında belirtildiği üzere, Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği hükümlerinin, hakkında güvenlik soruşturması ve arşiv araştırması yapılacak kişilerle sınırlı olmayıp kişi hakkında yeterli ve sağlıklı bir değerlendirme yapılabilmesi için ilgilinin içinde bulunduğu ortam ile yakınlarını ve birinci derece akrabalarını da kapsayacak şekilde) hukukilik incelemesi yapılarak Mahkemece verilen kararda idare hukuku ilkeleri kapsamında hukuka aykırı bir yön bulunmadığı oyuyla; Anayasa Mahkemesi'nin iptal kararının salt sonucu dikkate alınarak güvenlik soruşturması ve arşiv araştırması sonucunun yasal dayanağının ortadan kalktığı gerekçesiyle verilen çoğunluk kararına katılmıyorum.

İstanbul BİM - 7. İdari Dava Dairesi (E. 2020/412)

İstanbul Bölge İdare Mahkemesi, 7. İDD, E. 2020/412 K. 2020/1656 T. 8.10.2020

Esas No.: 2020/412

Karar No.: 2020/1656

Karar Tarihi: 08.10.2020

İSTEMİN ÖZETİ: Davacı şirkete ait dış polikliniğinin 14/12/2018 tarihi itibariyle Sağlık Net'e veri gönderimi yapılmadığından bahisle Ağız ve Diş Sağlığı Hizmeti Sunulan Özel Sağlık Kuruluşları Hakkındaki Yönetmeliğin Ek-8 Müeyyide Formu 17 maddesi uyarınca "24. maddesinin 7. fıkrasına aykırılık nedeniyle" mesul müdürün uyarılmasına dair Tekirdağ Valiliği İl Sağlık Müdürlüğü'nün 08.01.2019 tarih ve ...E.28 sayılı işleminin iptali istemiyle açılan davada; dava konusu işlemi iptal eden Tekirdağ 1. İdare Mahkemesi'nin 11/11/2019 gün ve E:2019/207, K:2019/1076 sayılı kararının; davalı idare tarafından, usule ilişkin olarak davanın süresinde açılmadığı ve işlemin icrai olmadığı, esasa ilişkin olarak ise, vatandaşlara ait sağlık verilerinin sisteme gönderilmemesinin, geçmiş sağlık verilerine ihtiyaç anında erişilememesine dolayısıyla vatandaşın etkin sağlık hizmeti elde edememesine neden olduğu, sisteme veri gönderilmemesi sebebiyle Sağlık Bakanlığı'nca ülke çapında sağlık hizmetine ilişkin tam olarak planlama yapılmasının ve vatandaşın hızlı, nitelikli sağlık hizmeti almasının engellendiği, Sağlık.Net'e ve E-Nabız sistemine Türkiyede çoğu özel hastaneler tarafından veri gönderimi yapıldığı, davacının veri göndermeyerek ülkede sağlık planlaması yapılmasına engel olduğu ileri sürülerek kaldırılması ve istinaf yoluyla işin esası hakkında yeniden karar verilmesi istenilmektedir.

SAVUNMANIN ÖZETİ: Ağız ve Diş Sağlığı Hizmeti Sunulan Özel Sağlık Kuruluşları Hakkında Yönetmeliğinin 24. maddesinin yedinci fıkrasındaki istatistiki veri paylaşımı yükümlülüğünün tam olarak yerine getirildiği, yerine getirilen bu yükümlülük nedeniyle yaptırım uygulanmasının hukuka aykırı olduğu ileri sürülerek Mahkeme kararının hukuka uygun olduğu, istinaf başvurusunun reddi gerektiği savunulmaktadır.

TÜRK MİLLETİ ADINA

Karar veren İstanbul Bölge İdare Mahkemesi Yedinci İdare Dava Dairesi'nce, dava dosyası incelenerek gereği görüldü:

Dava, davacı şirkete ait diş polikliniğinin 14/12/2018 tarihi itibariyle Sağlık Net'e veri gönderimi yapılmadığından bahisle Ağız ve Diş Sağlığı Hizmeti Sunulan Özel Sağlık Kuruluşları Hakkındaki Yönetmeliğin Ek-8 Müeyyide Formu 17 maddesi uyarınca "24. maddesinin 7. fıkrasına aykırılık nedeniyle" mesul müdürün uyarılmasına dair Tekirdağ Valiliği İl Sağlık Müdürlüğü'nün 08.01.2019 tarih ve ...E.28 sayılı işleminin iptali istemiyle açılmıştır.

3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun "Yönetmelikler" başlıklı 9 uncu maddesinin (c) bendinde; "Bütün kamu ve özel sağlık kuruluşlarının tesis, hizmet, personel kıstaslarını belirlemeye, sağlık kurum ve kuruluşlarını sınıflandırmaya ve sınıfların değiştirilmesine, sağlık kuruluşlarının amaca uygun teşkilatlandırılmasına, sağlık hizmet zinciri oluşturulmasına, hizmet içi eğitim usul ve esasları ile sağlık kurum ve kuruluşlarının koordineli çalışma ve hizmet standartlarının tespiti ve denetimi ile bu Kanunla ilgili diğer hususlar Sağlık ve Sosyal Yardım Bakanlığınca çıkarılacak yönetmelikle tespit edilir." hükmü yer almaktadır.

Fertlerin ve toplumun sağlığını korumak maksadıyla, mesleğini serbest olarak icra etmek yetkisine sahip olan diş hekimlerinin münferiden ve müştereken ağız ve diş sağlığı hizmeti verdikleri muayenehanelerin, özel ağız ve diş sağlığı poliklinikleri ile merkezlerinin açılması, faaliyetleri, denetimleri, faaliyetlerine son verilmesi ve diğer hususlara ilişkin usul ve esasları düzenlemek amacıyla, 11.4.1928 tarihli ve 1219 sayılı Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanun hükümlerine, 7.5.1987 tarihli ve 3359 sayılı Sağlık Hizmetleri Temel Kanununun 9 uncu maddesinin (c) bendi ile Ek 11 inci maddesine ve 11.10.2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 40 ıncı maddesine dayanılarak hazırlanan Ağız ve Diş Sağlığı Hizmeti Sunulan Özel Sağlık Kuruluşları Hakkında Yönetmeliğinin "Diş hekimleri ve uzmanlar" başlıklı 15. maddesinin 3. fıkrasının (a) bendinde, "Poliklinik veya ADSM'de çalışan diş hekimleri ve uzmanlar; Hastasına ait muayene, teşhis ve tedavi işlemlerini Bakanlıkça belirlenen esaslara uygun şekilde kaydetmekten sorumludur.", "Kayıt Sistemi" başlıklı 24. maddesinin yedinci fıkrasında, "Sağlık kuruluşları, kuruluştaki sunulan sağlık hizmetlerine ilişkin istatistiki verileri belirlenen formata uygun şekilde ve belirli aralıklarla Bakanlığa gönderir.", "Müeyyideler" başlıklı 32. maddesinde, "Bu Yönetmelikte belirlenen usul ve esaslara uymayanlar hakkında, Ek-8'te yer alan müeyyideler ve ilgili diğer mevzuat hükümleri uygulanır." düzenlemesine yer verilmiş, Yönetmelik eki EK 8 Müeyyide Formununun 17. maddesinde, 24. maddeye aykırılık halinde, 1. ve 2. tespitte uyarı üçüncü tespitte, bir önceki aya ait brüt hizmet gelirinin yüzde biri oranında idari para cezası verileceği hüküm altına alınmıştır.

Dosyanın incelenmesinden, Özel Düzgen Ağız ve Diş Sağlığı Polikliniğinden, Ağız ve Diş Sağlığı Hizmeti Sunulan Özel Sağlık Kuruluşları Hakkındaki Yönetmeliğin 24. maddesinin yedinci fıkrası hükümlerine aykırı olarak, 14.12.2018 tarihi itibariyle sağlık net'e veri gönderimi yapılmadığından bahisle anılan Yönetmeliğin Ek-8 Müeyyide Formu 17 maddesi uyarınca ilgili sağlık kuruluşu mesul müdürün uyarılmasına ilişkin 08.01.2019 tarihli ve ...E.28 sayılı Tekirdağ Valiliği İl Sağlık Müdürlüğü işleminin iptali istemiyle iş bu davanın açıldığı anlaşılmaktadır.

Uyuşmazlıkta, davacı tarafından, ilgili mevzuat hükmü uyarınca gönderilmesi gereken istatistiki verilerin sisteme gönderildiğinin ileri sürülerek konuya ilişkin bilgi ve belgelerin dava dosyasına eklenmesi üzerine, Dairemizin 03.07.2020 tarihli ara kararı ile, "Dava konusu işlemin incelenmesinden, işlemin Ağız ve Diş Sağlığı Hizmeti Sunan Özel Sağlık Kuruluşları Hakkında Yönetmeliğin 24. maddesinin yedinci fıkrasında yer alan "Sağlık kuruluşları, kuruluştaki sunulan sağlık hizmetlerine ilişkin istatistiki verileri belirlenen formata uygun şekilde ve belirlenen aralıklarla Bakanlığa gönderilir." düzenlemesine istinaden tesis edildiği,

-Davacılar tarafından, Ağız ve Diş Sağlığı Hizmeti Sunan Özel Sağlık Kuruluşları Hakkında Yönetmeliğin 24. maddesinin yedinci fıkrası uyarınca, hastalarla ilgili olarak idareye sunulması gereken istatistiki verilerin her ay düzenli olarak gönderildiğinin belirtilerek, bildirimlere ilişkin bilgi ve belgelerin dosyaya sunulduğu ,

-Ancak, gerek İlk Derece Mahkemesine sunulan savunma dilekçesinde gerekse Dairemize sunulan istinaf dilekçesinde konuya ilişkin genel açıklamalara yer verilmekle birlikte, davacılar tarafından işletilmekte olan diş polikliniğine ilişkin olarak sunulması istenilen ancak davacılar tarafından sunulmadığı iddia edilen hasta verilerine ilişkin istatistiki verilerin neler olduğu, davacılar tarafından, düzenli olarak sunulduğu iddia edilen ve dosyasına sunulan istatistiki verilerin neden yeterli görülmediği vs. konularında yeterli açıklama yapılmadığı görüldüğünden,

1-Sağlık kuruluşları, kuruluştaki sunulan sağlık hizmetlerine ilişkin istatistiki veriler ibaresi ile hangi verilerin kastedildiği, sunulması istenilen istatistiki verilerin tam olarak neleri içermesi gerektiği,(hasta ad- soyadı, konulan teşhis vs.),

2-Davacılar tarafından, düzenli olarak sunulduğu iddia edilen ve dosyasına sunulan istatistiki verilerin neden yeterli görülmediği (hangi bilgileri içermemesi sebebiyle kabul edilmediği - davacı şirket tarafından davalı idareye gönderilen istatistiki belgeler üzerinde format gereğince eksik olan hususlar da işaretlenerek),

3-Ağız ve Diş Sağlığı Hizmeti Sunan Özel Sağlık Kuruluşları Hakkında Yönetmeliğin 24. maddesinin yedinci fıkrasında "Sağlık kuruluşları, kuruluştta sunulan sağlık hizmetlerine ilişkin istatistiki verileri belirlenen formata uygun şekilde ve belirlenen aralıklarla Bakanlığa gönderilir." düzenlemesine yer verildiği, Yönetmelik eklerinin incelenmesinden istatistiki verilerin sunulması istenilen formata ilişkin herhangi bir düzenleme yapılmadığı görüldüğünden,

-istatistiki verilerin gönderilmesi gereken formatın (formatın nasıl olması, hangi bilgileri içermesi gerektiği vs.) nasıl olması gerektiği, hususlarına ilişkin olarak bilgi ve belgeye dayalı olarak, (dayanak mevzuat hükümleri açıkça belirtilerek) tereddüte mahal bırakmayacak şekilde açıklama yapılmasının istenilmesine karar verilmiş, anılan ara kararımıza davalı idare tarafından sunulan ve 20.08.2020 tarihinde Dairemiz kayıtlarına giren cevabi yazı da, Sağlık Bakanlığı uygulamalarından olan Temel Sağlık İstatistik Modülünde istenilen verilerin EK-1 tabloda gönderildiği, ayrıca EK 2 olarak sunulan tabloda yer alan verilerinde istenildiği, davacı tarafından EK-1'de gönderilen tablonun düzenli olarak gönderildiği ancak Ek-2'de yer alan tablonun alındığı sağlık-net sistemine herhangi bir veri gönderilmediği, s istemlerini Sağlık-Net'e entegre etmedikleri belirtilmiş, ara kararı eki EK 2 tabloda ise, hasta kayıt paketi adı altında hasta kimlik numarası, ad, soyad, doğum tarihi, anne kimlik numarası, adres bilgisi vs, hizmet ilaç malzeme paketi altında, "Hasta İşlem Bilgileri, Muayene Bilgisi Kayıt, Reçete Bilgisi vs. verilerin bulunduğu anlaşılmaktadır.

Bu kapsamda, ilk olarak davalı idare tarafından işlenmesi istenilen EK 2 olarak sunulan tabloda yer alan verilerin niteliğinin açıklığa kavuşturulması gerekmektedir.

6698 sayılı Kişisel Verileri Koruma Kanununun "Tanımlar" başlıklı 3. maddesinde, "d)Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi, e)Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem, f)Kurul: Kişisel Verileri Koruma Kurulu, g) Kurum: Kişisel Verileri Koruma Kurumu, ğ) Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi" olarak tanımlanmıştır.

Bu kapsamda, davalı idare tarafından işlenmesi istenilen EK 2 olarak sunulan tabloda yer alan verilerin kişisel veri olduğu sonuç ve kanaatine ulaşılmıştır.

İkinci olarak ise, kişisel verilerin sisteme işlenmesinin istenilip istenilemeyeceği hususunun açıklığa kavuşturulması gerekmektedir.

10.07.2018 tarihli ve 30474 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında 1 Numaralı Cumhurbaşkanlığı Kararnamesinin "Bilgi toplama, işleme ve paylaşma yetkisi" başlıklı 378. maddesinde, "(1) Sağlık hizmeti almak üzere, kamu veya özel sağlık kuruluşları ile sağlık mesleği mensuplarına müracaat edenlerin, sağlık hizmetinin gereği olarak vermek zorunda oldukları veya kendilerine verilen hizmete ilişkin kişisel verileri işlenebilir.

2) Sağlık hizmetinin verilmesi, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve maliyetlerin hesaplanması amacıyla Bakanlık, birinci fıkra kapsamında elde edilen verileri alarak işleyebilir. Bu veriler, Kişisel Verilerin Korunması Kanununda öngörülen şartlar dışında aktarılamaz." düzenlemesine yer verilmiştir.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Özel nitelikli kişisel verilerin işleme şartları" başlıklı 6'ncı maddesinde; (1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.

" düzenlemesine yer verilmiştir.

İlgili mevzuat hükmü uyarınca, sağlık ve cinsel hayat dışındaki kişisel verilerin, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebileceği, sağlık ve cinsel hayata ilişkin kişisel verilerin ise kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin

açık rızası aranmaksızın işlenebileceği, özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınmasının şart olduğu açıktır.

Nitekim, 12.12.2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 4. maddesi ile değiştirilen asıl Yönetmeliğin 27. maddesinin 8. fıkrasının ("Sağlık kuruluşları tarafından kayıt altına alınan kişisel sağlık verileri, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununa uygun bir şekilde işlenir ve Bakanlıkça belirlenen usul ve esaslara uygun bir şekilde merkezi sağlık veri sistemine aktarılır. Bakanlık tarafından kurulan kayıt ve bildirim sistemine ve Bakanlıkça yapılacak diğer iş ve işlemlere esas olmak üzere, istenilen bilgi ve belgelerin Bakanlığa gönderilmesi zorunludur." şeklinde yeniden düzenlenen) iptali istemiyle Danıştay Onbeşinci Daire Başkanlığının 2018/530 esasına kayıtlı dosyasında açılan davada anılan Dairenin 15.01.2019 tarihli kararı ile "..6698 sayılı Kişisel Verilerin Korunması Kanunu'na göre sağlık gibi özel nitelikli verilerin işlenmesinde uyulacak önlemleri belirlemekle yetkili olan Kişisel Verileri Koruma Kurulu tarafından bu alana ilişkin yeterli önlemler belirlenmeden ve mevzuat taslağı hakkında Kurul görüşü alınmadan tesis olunan dava konusu düzenlemede hukuka uyarlık bulunmadığı" gerekçesiyle 12.12.2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 4. maddesi ile değiştirilen asıl Yönetmeliğin 27. maddesinin 8. fıkrasının yürütmesinin durdurulmasına karar verilmiş, anılan karara yapılan itiraz Danıştay İdari Dava Daireleri Kurulunun 26.06.2019 tarihli, 2019/713 YD İtiraz No.lu kararı ile reddedilmiştir.

İlk Derece Mahkemesince, 6698 sayılı Kişisel Verilerin Korunması Kanun'unun 6. maddesi uyarınca hasta verilerinin işlenebilmesi için anılan Kanun'un 6'ncı maddesinin 2'nci fıkrası uyarınca ilgilinin açık rızasının bulunması gerektiği gerekçesine yer verilmiş ise de, Kurul tarafından belirlenen yeterli önlemlerin alınması şartıyla sağlık ve cinsel hayata ilişkin kişisel verilerin kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği açık olduğundan İlk Derece Mahkemesinin anılan gerekçesi yerinde görülmemiştir.

Bu durumda, davalı idarece işlenmesi istenilen verilerin özel nitelikli kişisel veri olduğu anılan verilerin Kişisel Verileri Koruma Kurulu tarafından bu alana ilişkin yeterli önlemler belirlenmeden sisteme işlenemeyeceği sonuç ve kanaatine ulaşılmış olup, uyuşmazlıkta Kişisel Verileri Koruma Kurulu tarafından bu alana ilişkin yeterli önlemler alındığına ilişkin bilgi ve belgelerin sunulmadığı

diğer taraftan davacı tarafından işletilmekte olan sağlık kuruluşuyla ilgili istatistiki verilerin her ay Sağlık Bakanlığı Temel Sağlık İstatistikleri Modülü (TSİM) üzerinden Bakanlığa düzenli olarak gönderildiği (davalı idarenin 20.08.2020 tarihinde Dairemiz kayıtlarına giren cevabi yazısında açıkça beyan edilmiştir) hususları birlikte değerlendirildiğinde, davacı tarafından işletilmekte olan sağlık kuruluşu mesul müdürünün uyarılmasına ilişkin dava konusu işlemde hukuka uyarlık, İlk Derece Mahkemesi kararında sonucu itibariyle hukuki isabetsizlik görülmemiştir.

Açıklanan nedenlerle, davalı idarenin istinaf başvurusunun yukarıda belirtilen gerekçeyle reddine, aşağıda dökümü gösterilen kanun yolu aşamasına ait 101,75.-TL yargılama giderlerinin istinaf yoluna başvuranın üzerinde bırakılmasına, artan posta avansının resen ilgisine iadesine, temyiz yolu kapalı olmak üzere kesin olarak 08/10/2020 tarihinde oybirliğiyle karar verildi.

İstanbul BİM - 7. İdari Dava Dairesi (E. 2020/288)

İstanbul Bölge İdare Mahkemesi, 7. İDD, E. 2020/288 K. 2020/1648 T. 7.10.2020

Esas No.: 2020/288

Karar No.: 2020/1648

Karar Tarihi: 07.10.2020

İSTİNAF YOLUNA

BAŞVURAN(DAVALI): TEKİRDAĞ VALİLİĞİ

VEKİLİ: AV. K1

KARŞI TARAF (DAVACILAR): 1- K2

2- K3

VEKİLİ: AV. K4

İSTEMİN ÖZETİ: Özel F1 Ağız ve Diş Sağlığı Polikliniğinin işletmecisi olan davacılar tarafından; anılan poliklinikten 14.12.2018 tarihi itibariyle sağlık net'e veri gönderimi yapılmadığından bahisle Ağız ve Diş Sağlığı Hizmeti Sunulan Özel Sağlık Kuruluşları Hakkındaki Yönetmeliğin Ek-8 Müeyyide Formu 17 maddesi uyarınca (anılan Yönetmeliğin 24. maddesinin 7. fıkrasına aykırılık nedeniyl) anılan poliklinik mesul müdürün uyarılmasına ilişkin 08.01.2019 tarihli ve ...E.21 sayılı Tekirdağ Valiliği İl Sağlık Müdürlüğü işleminin iptali istemiyle açılan davada;"...işlemin dayanağı Ağız ve Diş Sağlığı Hizmeti Sunulan Özel Sağlık Kuruluşları Hakkındaki Yönetmeliğin Ek-8 Müeyyide Formu 17 maddesi uyarınca "24. Maddeye aykırılık nedeniyle" davacı şirket mesul müdürlüğünün uyarılmasına dair işlem olduğu dikkate alındığında yönetmeliğin açık hükmü gözetilerek Sağlık Bakanlığı Temel Sağlık İstatistikleri Modülü (TSİM) üzerinden sağlık kuruluşuyla ilgili bilgilerin yanı sıra yönetmelikte öngörülen hastalarla ilgili istatistiki verilerin her ay Bakanlığa düzenli olarak gönderilmiş olması karşısında, davacının uyarılmasına ilişkin dava konusu işlemde hukuka uyarlık bulunmadığı" gerekçesiyle dava konusu işlemin iptaline karar veren Tekirdağ 1. İdare Mahkemesinin 11.11.2019 tarihli ve E:2019/217, K:2019/1071 sayılı kararının; usule ilişkin olarak; davanın süresinde açılmadığı, işlemin icrai olmadığı, esasa ilişkin olarak ise, vatandaşlara ait sağlık verilerinin sisteme gönderilmemesinin, geçmiş sağlık verilerine ihtiyaç anında erişilememesine dolayısıyla vatandaşın etkin sağlık hizmeti elde edememesine neden olduğu, sisteme veri gönderilmemesi sebebiyle Sağlık Bakanlığınca ülke çapında sağlık hizmetine ilişkin tam olarak

planlama yapılmasının ve vatandaşın hızlı, nitelikli sağlık hizmeti almasının engellendiği, Sağlık.Net'e ve E-Nabız sistemine Türkiyede çoğu özel hastaneler tarafından veri gönderimi yapıldığı, davacının veri göndermeyerek ülkede sağlık planlaması yapılmasına engel olduğu ileri sürülerek istinaf yoluyla incelenerek kaldırılması, davanın reddine karar verilmesi istenilmektedir.

SAVUNMANIN ÖZETİ: Ağız ve Diş Sağlığı Hizmeti Sunulan Özel Sağlık Kuruluşları Hakkında Yönetmeliğinin 24. maddesinin yedinci fıkrasındaki istatistiki veri paylaşımı yükümlülüğünün tam olarak yerine getirildiği, yerine getirilen bu yükümlülük nedeniyle yaptırım uygulanmasının hukuka aykırı olduğu ileri sürülerek Mahkeme kararının hukuka uygun olduğu, istinaf başvurusunun reddi gerektiği savunulmaktadır.

TÜRK MİLLETİ ADINA

Karar veren İstanbul Bölge İdare Mahkemesi Yedinci İdare Dava Dairesi'nce, davalı idarenin usule ilişkin itirazları yerinde görülmeyerek dava dosyası incelenerek gereği görüldü:

Dava, Özel F1 Ağız ve Diş Sağlığı Polikliniğinden 14.12.2018 tarihi itibariyle sağlık net'e veri gönderimi yapılmadığından bahisle Ağız ve Diş Sağlığı Hizmeti Sunulan Özel Sağlık Kuruluşları Hakkındaki Yönetmeliğin Ek-8 Müeyyide Formu 17 maddesi uyarınca (anılan Yönetmeliğin 24. maddesinin 7. fıkrasına aykırılık nedeniyle) anılan poliklinik mesul müdürün uyarılmasına ilişkin 08.01.2019 tarihli ve ...E.21 sayılı Tekirdağ Valiliği İl Sağlık Müdürlüğü işleminin iptali istemiyle açılmıştır.

3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun "Yönetmelikler" başlıklı 9 uncu maddesinin (c) bendinde; "Bütün kamu ve özel sağlık kuruluşlarının tesis, hizmet, personel kıstaslarını belirlemeye, sağlık kurum ve kuruluşlarını sınıflandırmaya ve sınıfların değiştirilmesine, sağlık kuruluşlarının amaca uygun teşkilatlandırılmasına, sağlık hizmet zinciri oluşturulmasına, hizmet içi eğitim usul ve esasları ile sağlık kurum ve kuruluşlarının koordineli çalışma ve hizmet standartlarının tespiti ve denetimi ile bu Kanunla ilgili diğer hususlar Sağlık ve Sosyal Yardım Bakanlığınca çıkarılacak yönetmelikle tespit edilir." hükmü yer almaktadır.

Fertlerin ve toplumun sağlığını korumak maksadıyla, mesleğini serbest olarak icra etmek yetkisine sahip olan diş hekimlerinin münferiden ve müştereken ağız ve diş sağlığı hizmeti verdikleri muayenehanelerin, özel ağız ve diş sağlığı poliklinikleri ile merkezlerinin açılması, faaliyetleri, denetimleri, faaliyetlerine son verilmesi ve diğer hususlara ilişkin usul ve esasları düzenlemek amacıyla, 11.4.1928 tarihli ve 1219 sayılı Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanun hükümlerine, 7.5.1987 tarihli ve 3359 sayılı Sağlık Hizmetleri Temel Kanununun 9 uncu maddesinin

(c) bendi ile Ek 11 inci maddesine ve 11.10.2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 40 inci maddesine dayanılarak hazırlanan Ağız ve Diş Sağlığı Hizmeti Sunulan Özel Sağlık Kuruluşları Hakkında Yönetmeliğinin "Diş hekimleri ve uzmanlar" başlıklı 15. maddesinin 3. fıkrasının (a) bendinde, "Poliklinik veya ADSM'de çalışan diş hekimleri ve uzmanlar; Hastasına ait muayene, teşhis ve tedavi işlemlerini Bakanlıkça belirlenen esaslara uygun şekilde kaydetmekten sorumludur.", "Kayıt Sistemi" başlıklı 24. maddesinin yedinci fıkrasında, "Sağlık kuruluşları, kuruluştta sunulan sağlık hizmetlerine ilişkin istatistiki verileri belirlenen formata uygun şekilde ve belirli aralıklarla Bakanlığa gönderir.", "Müeyyideler" başlıklı 32. maddesinde, " Bu Yönetmelikte belirlenen usul ve esaslara uymayanlar hakkında, Ek-8'te yer alan müeyyideler ve ilgili diğer mevzuat hükümleri uygulanır." düzenlemesine yer verilmiş, Yönetmelik eki EK 8 Müeyyide Formunun 17. maddesinde, 24. maddeye aykırılık halinde, 1. ve 2. tespitte uyarı üçüncü tespitte, bir önceki aya ait brüt hizmet gelirinin yüzde biri oranında idari para cezası verileceği hüküm altına alınmıştır.

Dosyanın incelenmesinden, Özel F1 Ağız ve Diş Sağlığı Polikliniğinden, Ağız ve Diş Sağlığı Hizmeti Sunulan Özel Sağlık Kuruluşları Hakkındaki Yönetmeliğin 24. maddesinin yedinci fıkrası hükümlerine aykırı olarak, 14.12.2018 tarihi itibariyle sağlık net'e veri gönderimi yapılmadığından bahisle anılan Yönetmeliğin Ek-8 Müeyyide Formu 17 maddesi uyarınca ilgili sağlık kuruluşu mesul müdürün uyarılmasına ilişkin 08.01.2019 tarihli ve ...E.21 sayılı Tekirdağ Valiliği İl Sağlık Müdürlüğü işleminin iptali istemiyle iş bu davanın açıldığı anlaşılmaktadır.

Uyuşmazlıkta, davacılar tarafından, ilgili mevzuat hükmü uyarınca gönderilmesi gereken istatistiki verilerin sisteme gönderildiğinin ileri sürülerek konuya ilişkin bilgi ve belgelerin dava dosyasına eklenmesi üzerine, Dairemizin 01.07.2020 tarihli ara kararı ile, "Dava konusu işlemin incelenmesinden, işlemin Ağız ve Diş Sağlığı Hizmeti Sunan Özel Sağlık Kuruluşları Hakkında Yönetmeliğin 24. maddesinin yedinci fıkrasında yer alan "Sağlık kuruluşları, kuruluştta sunulan sağlık hizmetlerine ilişkin istatistiki verileri belirlenen formata uygun şekilde ve belirlenen aralıklarla Bakanlığa gönderilir." düzenlemesine istinaden tesis edildiği,

-Davacılar tarafından, Ağız ve Diş Sağlığı Hizmeti Sunan Özel Sağlık Kuruluşları Hakkında Yönetmeliğin 24. maddesinin yedinci fıkrası uyarınca, hastalarla ilgili olarak idareye sunulması gereken istatistiki verilerin her ay düzenli olarak gönderildiğinin belirtilerek, bildirimlere ilişkin bilgi ve belgelerin dosyaya sunulduğu ,

-Ancak, gerek İlk Derece Mahkemesine sunulan savunma dilekçesinde gerekse Dairemize sunulan istinaf dilekçesinde konuya ilişkin genel açıklamalara yer verilmekle birlikte, davacılar tarafından

işletilmekte olan dış polikliniğine ilişkin olarak sunulması istenilen ancak davacılar tarafından sunulmadığı iddia edilen hasta verilerine ilişkin istatistiki verilerin neler olduğu, davacılar tarafından, düzenli olarak sunulduğu iddia edilen ve dosyasına sunulan istatistiki verilerin neden yeterli görülmediği vs. konularında yeterli açıklama yapılmadığı görüldüğünden,

1-Sağlık kuruluşları, kuruluştaki sunulan sağlık hizmetlerine ilişkin istatistiki veriler ibaresi ile hangi verilerin kastedildiği, sunulması istenilen istatistiki verilerin tam olarak neleri içermesi gerektiği,(hasta ad- soyadı, konulan teşhis vs.),

2-Davacılar tarafından, düzenli olarak sunulduğu iddia edilen ve dosyasına sunulan istatistiki verilerin neden yeterli görülmediği (hangi bilgileri içermemesi sebebiyle kabul edilmediği - davacı şirket tarafından davalı idareye gönderilen istatistiki belgeler üzerinde format gereğince eksik olan hususlar da işaretlenerek),

3-Ağız ve Diş Sağlığı Hizmeti Sunan Özel Sağlık Kuruluşları Hakkında Yönetmeliğin 24. maddesinin yedinci fıkrasında "Sağlık kuruluşları, kuruluştaki sunulan sağlık hizmetlerine ilişkin istatistiki verileri belirlenen formata uygun şekilde ve belirlenen aralıklarla Bakanlığa gönderilir." düzenlemesine yer verildiği, Yönetmelik eklerinin incelenmesinden istatistiki verilerin sunulması istenilen formata ilişkin herhangi bir düzenleme yapılmadığı görüldüğünden,

-istatistiki verilerin gönderilmesi gereken formatın (formatın nasıl olması, hangi bilgileri içermesi gerektiği vs.) nasıl olması gerektiği, hususlarına ilişkin olarak bilgi ve belgeye dayalı olarak, (dayanak mevzuat hükümleri açıkça belirtilerek) tereddüte mahal bırakmayacak şekilde açıklama yapılmasının istenilmesine karar verilmiş, anılan ara kararımıza davalı idare tarafından sunulan ve 20.08.2020 tarihinde Dairemiz kayıtlarına giren cevabi yazı da, Sağlık Bakanlığı uygulamalarından olan Temel Sağlık İstatistik Modülünde istenilen verilerin EK-1 tabloda gönderildiği, ayrıca EK 2 olarak sunulan tabloda yer alan verilerinde istenildiği, davacılar tarafından EK-1'de gönderilen tablonun düzenli olarak gönderildiği ancak Ek-2'de yer alan tablonun alındığı sağlık-net sistemine herhangi bir veri gönderilmediği, sistemlerini Sağlık-Net'e entegre etmedikleri belirtilmiş, ara kararı eki EK 2 tabloda ise, hasta kayıt paketi adı altında hasta kimlik numarası, ad, soyad, doğum tarihi, anne kimlik numarası, adres bilgisi vs, hizmet ilaç malzeme paketi altında, "Hasta İşlem Bilgileri, Muayene Bilgisi Kayıt, Reçete Bilgisi vs. verilerin bulunduğu anlaşılmaktadır.

Bu kapsamda, ilk olarak davalı idare tarafından işlenmesi istenilen EK 2 olarak sunulan tabloda yer alan verilerin niteliğinin açıklığa kavuşturulması gerekmektedir.

6698 sayılı Kişisel Verileri Koruma Kanununun "Tanımlar" başlıklı 3. maddesinde, "d)Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi, e)Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem, f)Kurul: Kişisel Verileri Koruma Kurulu, g) Kurum: Kişisel Verileri Koruma Kurumu, ğ) Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi" olarak tanımlanmıştır.

Bu kapsamda, davalı idare tarafından işlenmesi istenilen EK 2 olarak sunulan tabloda yer alan verilerin kişisel veri olduğu sonuç ve kanaatine ulaşılmıştır.

İkinci olarak ise, kişisel verilerin sisteme işlenmesinin istenilip istenilemeyeceği hususunun açıklığa kavuşturulması gerekmektedir.

10.07.2018 tarihli ve 30474 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında 1 Numaralı Cumhurbaşkanlığı Kararnamesinin "Bilgi toplama, işleme ve paylaşma yetkisi" başlıklı 378. maddesinde, "(1) Sağlık hizmeti almak üzere, kamu veya özel sağlık kuruluşları ile sağlık mesleği mensuplarına müracaat edenlerin, sağlık hizmetinin gereği olarak vermek zorunda oldukları veya kendilerine verilen hizmete ilişkin kişisel verileri işlenebilir.

2) Sağlık hizmetinin verilmesi, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve maliyetlerin hesaplanması amacıyla Bakanlık, birinci fıkra kapsamında elde edilen verileri alarak işleyebilir. Bu veriler, Kişisel Verilerin Korunması Kanununda öngörülen şartlar dışında aktarılamaz." düzenlemesine yer verilmiştir.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Özel nitelikli kişisel verilerin işlenme şartları" başlıklı 6'ncı maddesinde; (1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler

ise ancak kamu sađlıđının korunması, koruyucu hekimlik, tıbbî teŖhis, tedavi ve bakım hizmetlerinin yrtlmesi, sađlık hizmetleri ile finansmanının planlanması ve ynetimi amacıyla, sır saklama ykmllđ altında bulunan kiŖiler veya yetkili kurum ve kuruluŖlar tarafından ilgilinin aık rızası aranmaksızın iŖlenebilir.

(4) zel nitelikli kiŖisel verilerin iŖlenmesinde, ayrıca Kurul tarafından belirlenen yeterli nlemlerin alınması Ŗarttır.

" dzenlemesine yer verilmiŖtir.

İlgili mevzuat hkm uyarınca, sađlık ve cinsel hayat dıŖındaki kiŖisel verilerin, kanunlarda ngrlen hllerde ilgili kiŖinin aık rızası aranmaksızın iŖlenebileceđi, sađlık ve cinsel hayata iliŖkin kiŖisel verilerin ise kamu sađlıđının korunması, koruyucu hekimlik, tıbbî teŖhis, tedavi ve bakım hizmetlerinin yrtlmesi, sađlık hizmetleri ile finansmanının planlanması ve ynetimi amacıyla, sır saklama ykmllđ altında bulunan kiŖiler veya yetkili kurum ve kuruluŖlar tarafından ilgilinin aık rızası aranmaksızın iŖlenebileceđi, zel nitelikli kiŖisel verilerin iŖlenmesinde, ayrıca Kurul tarafından belirlenen yeterli nlemlerin alınmasının Ŗart olduđu aıktır.

Nitekim, 12.12.2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta TeŖhis ve Tedavi Yapılan zel Sađlık KuruluŖları Hakkında Ynetmelikte DeđiŖlik Yapılmasına Dair Ynetmeliđin 4. maddesi ile deđiŖtirilen asıl Ynetmeliđin 27. maddesinin 8. fıkrasının ("Sađlık kuruluŖları tarafından kayıt altına alınan kiŖisel sađlık verileri, 24/3/2016 tarihli ve 6698 sayılı KiŖisel Verilerin Korunması Kanununa uygun bir Ŗekilde iŖlenir ve Bakanlıka belirlenen usul ve esaslara uygun bir Ŗekilde merkezi sađlık veri sistemine aktarılır. Bakanlık tarafından kurulan kayıt ve bildirim sistemine ve Bakanlıka yapılacak diđer iŖ ve iŖlemlere esas olmak zere, istenilen bilgi ve belgelerin Bakanlıka gnderilmesi zorunludur." Ŗeklinde yeniden dzenlenen) iptali istemiyle DanıŖtay OnbeŖinci Daire BaŖkanlıđının 2018/530 esasına kayıtlı dosyasında aılan davada anılan Dairenin 15.01.2019 tarihli kararı ile ".6698 sayılı KiŖisel Verilerin Korunması Kanunu'na gre sađlık gibi zel nitelikli verilerin iŖlenmesinde uyulacak nlemleri belirlemekle yetkili olan KiŖisel Verileri Koruma Kurulu tarafından bu alana iliŖkin yeterli nlemler belirlenmeden ve mevzuat taslađı hakkında Kurul grŖ alınmadan tesis olunan dava konusu dzenlemede hukuka uyarlılık bulunmadıđı" gerekesiyle 12.12.2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta TeŖhis ve Tedavi Yapılan zel Sađlık KuruluŖları Hakkında Ynetmelikte DeđiŖlik Yapılmasına Dair Ynetmeliđin 4. maddesi ile deđiŖtirilen asıl Ynetmeliđin 27. maddesinin 8. fıkrasının yrtmesinin durdurulmasına karar verilmiŖ, anılan karara yapılan itiraz DanıŖtay İdari Dava Daireleri Kurulunun 26.06.2019 tarihli, 2019/713 YD İtiraz No.lu kararı ile reddedilmiŖtir.

İlk Derece Mahkemesince, 6698 sayılı Kişisel Verilerin Korunması Kanun'unun 6. maddesi uyarınca hasta verilerinin işlenebilmesi için anılan Kanun'unun 6'ncı maddesinin 2'nci fıkrası uyarınca ilgilinin açık rızasının bulunması gerektiği gerekçesine yer verilmiş ise de, Kurul tarafından belirlenen yeterli önlemlerin alınması şartıyla sağlık ve cinsel hayata ilişkin kişisel verilerin kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği açık olduğundan İlk Derece Mahkemesinin anılan gerekçesi yerinde görülmemiştir.

Bu durumda, davalı idarece işlenmesi istenilen verilerin özel nitelikli kişisel veri olduğu anılan verilerin Kişisel Verileri Koruma Kurulu tarafından bu alana ilişkin yeterli önlemler belirlenmeden sisteme işlenemeyeceği sonuç ve kanaatine ulaşılmış olup uyuşmazlıkta Kişisel Verileri Koruma Kurulu tarafından bu alana ilişkin yeterli önlemler alındığına ilişkin bilgi ve belgelerin sunulmadığı diğer taraftan davacılar tarafından işletilmekte olan sağlık kuruluşuyla ilgili istatistiki verilerin her ay Sağlık Bakanlığı Temel Sağlık İstatistikleri Modülü (TSİM) üzerinden Bakanlığa düzenli olarak gönderildiği (davalı idarenin 20.08.2020 tarihinde Dairemiz kayıtlarına giren cevabi yazısında açıkça beyan edilmiştir) hususları birlikte değerlendirildiğinde, davacılar tarafından işletilmekte olan sağlık kuruluşu mesul müdürünün uyarılmasına ilişkin dava konusu işlemde hukuka uyarlık, İlk Derece Mahkemesi kararında sonucu itibariyle hukuki isabetsizlik görülmemiştir.

Açıklanan nedenlerle, davalı idarenin istinaf başvurusunun yukarıda belirtilen gerekçeyle reddine, aşağıda dökümü yapılan istinaf yargılama giderinin istinaf yoluna başvuran üzerinde bırakılmasına, istinaf aşamasındaki posta gideri avansından artan kısmın mahkemesince ilgisine iadesine, 2577 sayılı İdari Yargılama Usulü Kanunu'nun 45. maddesinin 6. fıkrası uyarınca kararın taraflara tebliği için dosyanın ait olduğu mahkemesine gönderilmesine, anılan madde uyarınca temyizi kabil olmamak üzere kesin olarak 07.10.2020 tarihinde oybirliğiyle karar verildi.

İstanbul BİM - 7. İdari Dava Dairesi (E. 2020/284)

İstanbul Bölge İdare Mahkemesi, 7. İDD, E. 2020/284 K. 2020/1658 T. 8.10.2020

Esas No.: 2020/284

Karar No.: 2020/1658

Karar Tarihi: 08.10.2020

İSTEMİN ÖZETİ: Davacı şirkete ait dış polikliniğinin 14/12/2018 tarihi itibariyle Sağlık Net'e veri gönderimi yapılmadığından bahisle Ağız ve Diş Sağlığı Hizmeti Sunulan Özel Sağlık Kuruluşları Hakkındaki Yönetmeliğin Ek-8 Müeyyide Formu 17 maddesi uyarınca "24. Maddesinin 7. fıkrasına aykırılık nedeniyle" mesul müdürün uyarılmasına dair Tekirdağ Valiliği İl Sağlık Müdürlüğü'nün 07.01.2019 tarih ve ...E.14 sayılı işleminin iptali istemiyle açılan davada; dava konusu işlemi iptal eden Tekirdağ 1. İdare Mahkemesi'nin 11/11/2019 gün ve E:2019/406, K:2019/1075 sayılı kararının; davalı idare tarafından, usule ilişkin olarak; davanın süresinde açılmadığı, işlemin icrai olmadığı, esasa ilişkin olarak ise, vatandaşlara ait sağlık verilerinin sisteme gönderilmemesinin, geçmiş sağlık verilerine ihtiyaç anında erişilememesine dolayısıyla vatandaşın etkin sağlık hizmeti elde edememesine neden olduğu, sisteme veri gönderilmemesi sebebiyle Sağlık Bakanlığı'nca ülke çapında sağlık hizmetine ilişkin tam olarak planlama yapılmasının ve vatandaşın hızlı, nitelikli sağlık hizmeti almasının engellendiği, Sağlık.Net'e ve E-Nabız sistemine Türkiyede çoğu özel hastaneler tarafından veri gönderimi yapıldığı, davacının veri göndermeyerek ülkede sağlık planlaması yapılmasına engel olduğu ileri sürülerek kaldırılması ve istinaf yoluyla işin esası hakkında yeniden karar verilmesi istenilmektedir.

SAVUNMANIN ÖZETİ: Ağız ve Diş Sağlığı Hizmeti Sunulan Özel Sağlık Kuruluşları Hakkında Yönetmeliğinin 24. maddesinin yedinci fıkrasındaki istatistiki veri paylaşımı yükümlülüğünün tam olarak yerine getirildiği, yerine getirilen bu yükümlülük nedeniyle yaptırım uygulanmasının hukuka aykırı olduğu ileri sürülerek Mahkeme kararının hukuka uygun olduğu, istinaf başvurusunun reddi gerektiği savunulmaktadır.

TÜRK MİLLETİ ADINA

Karar veren İstanbul Bölge İdare Mahkemesi Yedinci İdare Dava Dairesi'nce, dava dosyası incelenerek gereği görüldü:

Dava, davacı şirkete ait diş polikliniğinin 14/12/2018 tarihi itibariyle Sağlık Net'e veri gönderimi yapılmadığından bahisle Ağız ve Diş Sağlığı Hizmeti Sunulan Özel Sağlık Kuruluşları Hakkındaki Yönetmeliğin Ek-8 Müeyyide Formu 17 maddesi uyarınca "24. Maddesinin 7. fıkrasına aykırılık nedeniyle" mesul müdürün uyarılmasına dair Tekirdağ Valiliği İl Sağlık Müdürlüğü'nün 07.01.2019 tarih ve ...E.14 sayılı işleminin iptali istemiyle açılmıştır.

3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun "Yönetmelikler" başlıklı 9 uncu maddesinin (c) bendinde; "Bütün kamu ve özel sağlık kuruluşlarının tesis, hizmet, personel kıstaslarını belirlemeye, sağlık kurum ve kuruluşlarını sınıflandırmaya ve sınıfların değiştirilmesine, sağlık kuruluşlarının amaca uygun teşkilatlandırılmasına, sağlık hizmet zinciri oluşturulmasına, hizmet içi eğitim usul ve esasları ile sağlık kurum ve kuruluşlarının koordineli çalışma ve hizmet standartlarının tespiti ve denetimi ile bu Kanunla ilgili diğer hususlar Sağlık ve Sosyal Yardım Bakanlığınca çıkarılacak yönetmelikle tespit edilir." hükmü yer almaktadır.

Fertlerin ve toplumun sağlığını korumak maksadıyla, mesleğini serbest olarak icra etmek yetkisine sahip olan diş hekimlerinin münferiden ve müştereken ağız ve diş sağlığı hizmeti verdikleri muayenehanelerin, özel ağız ve diş sağlığı poliklinikleri ile merkezlerinin açılması, faaliyetleri, denetimleri, faaliyetlerine son verilmesi ve diğer hususlara ilişkin usul ve esasları düzenlemek amacıyla, 11.4.1928 tarihli ve 1219 sayılı Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanun hükümlerine, 7.5.1987 tarihli ve 3359 sayılı Sağlık Hizmetleri Temel Kanununun 9 uncu maddesinin (c) bendi ile Ek 11 inci maddesine ve 11.10.2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 40 ıncı maddesine dayanılarak hazırlanan Ağız ve Diş Sağlığı Hizmeti Sunulan Özel Sağlık Kuruluşları Hakkında Yönetmeliğinin "Diş hekimleri ve uzmanlar" başlıklı 15. maddesinin 3. fıkrasının (a) bendinde, "Poliklinik veya ADSM'de çalışan diş hekimleri ve uzmanlar; Hastasına ait muayene, teşhis ve tedavi işlemlerini Bakanlıkça belirlenen esaslara uygun şekilde kaydetmekten sorumludur.", "Kayıt Sistemi" başlıklı 24. maddesinin yedinci fıkrasında, "Sağlık kuruluşları, kuruluştta sunulan sağlık hizmetlerine ilişkin istatistiki verileri belirlenen formata uygun şekilde ve belirli aralıklarla Bakanlığa gönderir.", "Müeyyideler" başlıklı 32. maddesinde, "Bu Yönetmelikte belirlenen usul ve esaslara uymayanlar hakkında, Ek-8'te yer alan müeyyideler ve ilgili diğer mevzuat hükümleri uygulanır." düzenlemesine yer verilmiş, Yönetmelik eki EK 8 Müeyyide Formununun 17. maddesinde, 24. maddeye aykırılık halinde, 1. ve 2. tespitte uyarı üçüncü tespitte, bir önceki aya ait brüt hizmet gelirinin yüzde biri oranında idari para cezası verileceği hüküm altına alınmıştır.

Dosyanın incelenmesinden, Özel Kapaklı Ağız ve Diş Sağlığı Polikliniğinden, Ağız ve Diş Sağlığı Hizmeti Sunulan Özel Sağlık Kuruluşları Hakkındaki Yönetmeliğin 24. maddesinin yedinci fıkrası hükümlerine aykırı olarak, 14.12.2018 tarihi itibariyle sağlık net'e veri gönderimi yapılmadığından bahisle anılan Yönetmeliğin Ek-8 Müeyyide Formu 17 maddesi uyarınca ilgili sağlık kuruluşu mesul müdürün uyarılmasına ilişkin 07.01.2019 tarihli ve ...E.14 sayılı Tekirdağ Valiliği İl Sağlık Müdürlüğü işleminin iptali istemiyle iş bu davanın açıldığı anlaşılmaktadır.

Uyuşmazlıkta, davacı tarafından, ilgili mevzuat hükmü uyarınca gönderilmesi gereken istatistiki verilerin sisteme gönderildiğinin ileri sürülerek konuya ilişkin bilgi ve belgelerin dava dosyasına eklenmesi üzerine, Dairemizin 03.07.2020 tarihli ara kararı ile, "Dava konusu işlemin incelenmesinden, işlemin Ağız ve Diş Sağlığı Hizmeti Sunan Özel Sağlık Kuruluşları Hakkında Yönetmeliğin 24. maddesinin yedinci fıkrasında yer alan "Sağlık kuruluşları, kuruluştaki sunulan sağlık hizmetlerine ilişkin istatistiki verileri belirlenen formata uygun şekilde ve belirlenen aralıklarla Bakanlığa gönderilir." düzenlemesine istinaden tesis edildiği,

-Davacılar tarafından, Ağız ve Diş Sağlığı Hizmeti Sunan Özel Sağlık Kuruluşları Hakkında Yönetmeliğin 24. maddesinin yedinci fıkrası uyarınca, hastalarla ilgili olarak idareye sunulması gereken istatistiki verilerin her ay düzenli olarak gönderildiğinin belirtilerek, bildirimlere ilişkin bilgi ve belgelerin dosyaya sunulduğu,

-Ancak, gerek İlk Derece Mahkemesine sunulan savunma dilekçesinde gerekse Dairemize sunulan istinaf dilekçesinde konuya ilişkin genel açıklamalara yer verilmekle birlikte, davacılar tarafından işletilmekte olan diş polikliniğine ilişkin olarak sunulması istenilen ancak davacılar tarafından sunulmadığı iddia edilen hasta verilerine ilişkin istatistiki verilerin neler olduğu, davacılar tarafından, düzenli olarak sunulduğu iddia edilen ve dosyasına sunulan istatistiki verilerin neden yeterli görülmediği vs. konularında yeterli açıklama yapılmadığı görüldüğünden,

1-Sağlık kuruluşları, kuruluştaki sunulan sağlık hizmetlerine ilişkin istatistiki veriler ibaresi ile hangi verilerin kastedildiği, sunulması istenilen istatistiki verilerin tam olarak neleri içermesi gerektiği,(hasta ad- soyadı, konulan teşhis vs.),

2-Davacılar tarafından, düzenli olarak sunulduğu iddia edilen ve dosyasına sunulan istatistiki verilerin neden yeterli görülmediği (hangi bilgileri içermemesi sebebiyle kabul edilmediği - davacı şirket tarafından davalı idareye gönderilen istatistiki belgeler üzerinde format gereğince eksik olan hususlar da işaretlenerek),

3-Ağız ve Diş Sağlığı Hizmeti Sunan Özel Sağlık Kuruluşları Hakkında Yönetmeliğin 24. maddesinin yedinci fıkrasında "Sağlık kuruluşları, kuruluştaki sunulan sağlık hizmetlerine ilişkin istatistikî verileri belirlenen formata uygun şekilde ve belirlenen aralıklarla Bakanlığa gönderilir." düzenlemesine yer verildiği, Yönetmelik eklerinin incelenmesinden istatistikî verilerin sunulması istenilen formata ilişkin herhangi bir düzenleme yapılmadığı görüldüğünden,

-istatistikî verilerin gönderilmesi gereken formatın (formatın nasıl olması, hangi bilgileri içermesi gerektiği vs.) nasıl olması gerektiği, hususlarına ilişkin olarak bilgi ve belgeye dayalı olarak, (dayanak mevzuat hükümleri açıkça belirtilerek) tereddüte mahal bırakmayacak şekilde açıklama yapılmasının istenilmesine karar verilmiş, anılan ara kararımıza davalı idare tarafından sunulan ve 20.08.2020 tarihinde Dairemiz kayıtlarına giren cevabi yazı da, Sağlık Bakanlığı uygulamalarından olan Temel Sağlık İstatistik Modülünde istenilen verilerin EK-1 tabloda gönderildiği, ayrıca EK 2 olarak sunulan tabloda yer alan verilerinde istenildiği, davacı tarafından EK-1'de gönderilen tablonun düzenli olarak gönderildiği ancak Ek-2'de yer alan tablonun alındığı sağlık-net sistemine herhangi bir veri gönderilmediği, sistemlerini Sağlık-Net'e entegre etmedikleri belirtilmiş, ara kararı eki EK 2 tabloda ise, hasta kayıt paketi adı altında hasta kimlik numarası, ad, soyad, doğum tarihi, anne kimlik numarası, adres bilgisi vs, hizmet ilaç malzeme paketi altında, "Hasta İşlem Bilgileri, Muayene Bilgisi Kayıt, Reçete Bilgisi vs. verilerin bulunduğu anlaşılmaktadır.

Bu kapsamda, ilk olarak davalı idare tarafından işlenmesi istenilen EK 2 olarak sunulan tabloda yer alan verilerin niteliğinin açıklığa kavuşturulması gerekmektedir.

6698 sayılı Kişisel Verileri Koruma Kanununun "Tanımlar" başlıklı 3. maddesinde, "d)Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi, e)Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem, f)Kurul: Kişisel Verileri Koruma Kurulu, g) Kurum: Kişisel Verileri Koruma Kurumu,ğ) Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi" olarak tanımlanmıştır.

Bu kapsamda, davalı idare tarafından işlenmesi istenilen EK 2 olarak sunulan tabloda yer alan verilerin kişisel veri olduğu sonuç ve kanaatine ulaşılmıştır.

İkinci olarak ise, kişisel verilerin sisteme işlenmesinin istenilip istenilemeyeceği hususunun açıklığa kavuşturulması gerekmektedir.

10.07.2018 tarihli ve 30474 sayılı Cumhurbaşkanlığı Teşkilatı Hakkında 1 Numaralı Cumhurbaşkanlığı Kararnamesinin "Bilgi toplama, işleme ve paylaşma yetkisi" başlıklı 378. maddesinde, "(1) Sağlık hizmeti almak üzere, kamu veya özel sağlık kuruluşları ile sağlık mesleği mensuplarına müracaat edenlerin, sağlık hizmetinin gereği olarak vermek zorunda oldukları veya kendilerine verilen hizmete ilişkin kişisel verileri işlenebilir.

2) Sağlık hizmetinin verilmesi, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve maliyetlerin hesaplanması amacıyla Bakanlık, birinci fıkra kapsamında elde edilen verileri alarak işleyebilir. Bu veriler, Kişisel Verilerin Korunması Kanununda öngörülen şartlar dışında aktarılamaz." düzenlemesine yer verilmiştir.

6698

sayılı Kişisel Verilerin Korunması Kanunu'nun "Özel nitelikli kişisel verilerin işleme şartları" başlıklı 6'ncı maddesinde; (1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.

" düzenlemesine yer verilmiştir.

İlgili mevzuat hükmü uyarınca, sağlık ve cinsel hayat dışındaki kişisel verilerin, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebileceği, sağlık ve cinsel hayata ilişkin kişisel verilerin ise kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin

açık rızası aranmaksızın işlenebileceği, özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınmasının şart olduğu açıktır.

Nitekim, 12.12.2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 4. maddesi ile değiştirilen asıl Yönetmeliğin 27. maddesinin 8. fıkrasının ("Sağlık kuruluşları tarafından kayıt altına alınan kişisel sağlık verileri, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununa uygun bir şekilde işlenir ve Bakanlıkça belirlenen usul ve esaslara uygun bir şekilde merkezi sağlık veri sistemine aktarılır. Bakanlık tarafından kurulan kayıt ve bildirim sistemine ve Bakanlıkça yapılacak diğer iş ve işlemlere esas olmak üzere, istenilen bilgi ve belgelerin Bakanlığa gönderilmesi zorunludur." şeklinde yeniden düzenlenen) iptali istemiyle Danıştay Onbeşinci Daire Başkanlığının 2018/530 esasına kayıtlı dosyasında açılan davada anılan Dairenin 15.01.2019 tarihli kararı ile ".6698 sayılı Kişisel Verilerin Korunması Kanunu'na göre sağlık gibi özel nitelikli verilerin işlenmesinde uyulacak önlemleri belirlemekle yetkili olan Kişisel Verileri Koruma Kurulu tarafından bu alana ilişkin yeterli önlemler belirlenmeden ve mevzuat taslağı hakkında Kurul görüşü alınmadan tesis olunan dava konusu düzenlemede hukuka uyarlık bulunmadığı" gerekçesiyle 12.12.2017 tarihli ve 30268 sayılı Resmî Gazete'de yayımlanan Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 4. maddesi ile değiştirilen asıl Yönetmeliğin 27. maddesinin 8. fıkrasının yürütmesinin durdurulmasına karar verilmiş, anılan karara yapılan itiraz Danıştay İdari Dava Daireleri Kurulunun 26.06.2019 tarihli, 2019/713 YD İtiraz No.lu kararı ile reddedilmiştir.

İlk Derece Mahkemesince, 6698 sayılı Kişisel Verilerin Korunması Kanun'unun 6. maddesi uyarınca hasta verilerinin işlenebilmesi için anılan Kanun'un 6'ncı maddesinin 2'nci fıkrası uyarınca ilgilinin açık rızasının bulunması gerektiği gerekçesine yer verilmiş ise de, Kurul tarafından belirlenen yeterli önlemlerin alınması şartıyla sağlık ve cinsel hayata ilişkin kişisel verilerin kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği açık olduğundan İlk Derece Mahkemesinin anılan gerekçesi yerinde görülmemiştir.

Bu durumda, davalı idarece işlenmesi istenilen verilerin özel nitelikli kişisel veri olduğu anılan verilerin Kişisel Verileri Koruma Kurulu tarafından bu alana ilişkin yeterli önlemler belirlenmeden sisteme işlenemeyeceği sonuç ve kanaatine ulaşılmış olup uyuşmazlıkta Kişisel Verileri Koruma Kurulu tarafından bu alana ilişkin yeterli önlemler alındığına ilişkin bilgi ve belgelerin sunulmadığı

diğer taraftan davacı tarafından işletilmekte olan sağlık kuruluşuyla ilgili istatistiki verilerin her ay Sağlık Bakanlığı Temel Sağlık İstatistikleri Modülü (TSİM) üzerinden Bakanlığa düzenli olarak gönderildiği (davalı idarenin 20.08.2020 tarihinde Dairemiz kayıtlarına giren cevabi yazısında açıkça beyan edilmiştir) hususları birlikte değerlendirildiğinde, davacılar tarafından işletilmekte olan sağlık kuruluşu mesul müdürünün uyarılmasına ilişkin dava konusu işlemde hukuka uyarlık, İlk Derece Mahkemesi kararında sonucu itibariyle hukuki isabetsizlik görülmemiştir.

Açıklanan nedenlerle, davalı idarenin istinaf başvurusunun yukarıda belirtilen gerekçeyle reddine, aşağıda dökümü gösterilen kanun yolu aşamasına ait 101,75.-TL yargılama giderlerinin istinaf yoluna başvuranın üzerinde bırakılmasına, artan posta avansının resen ilgisine iadesine, temyiz yolu kapalı olmak üzere kesin olarak 08/10/2020 tarihinde oybirliğiyle karar verildi.

İstanbul Bölge İdare Mahkemesi, 3. İDD, E. 2017/1689 K. 2018/62 T. 18.1.2018

Esas No.: 2017/1689

Karar No.: 2018/62

Karar Tarihi: 18.01.2018

İSTEMİN ÖZETİ: Davacının, personelin mesai giriş çıkışlarında parmak resmi eşleştirme işleminin kaldırılması istemiyle yapmış olduğu başvurusunun reddine ilişkin 28/12/2016 tarih ve 795 sayılı işlemin iptali istemiyle açılan davada, davanın reddine ilişkin olarak İstanbul 4. İdare Mahkemesi'nce verilen 30/06/2017 tarih ve E:2017/296, K:2017/1477 sayılı karara karşı davacı tarafından; işlemin Anayasal haklara uluslararası sözleşmelere, yüksek yargı kararlarına aykırı olduğu iddialarıyla istinaf yoluna başvurulmaktadır.

SAVUNMANIN ÖZETİ: İstem reddi gerektiği savunulmaktadır.

TÜRK MİLLETİ ADINA

Karar veren İstanbul Bölge İdare Mahkemesi Üçüncü İdare Dava Dairesince işin gereği görüşüldü:

Dava; davacının, personelin mesai giriş çıkışlarında parmak resmi eşleştirme işleminin kaldırılması istemiyle yapmış olduğu başvurusunun reddine ilişkin 28/12/2016 tarih ve 795 sayılı işlemin iptali istemiyle açılmıştır.

İdare Mahkemesince "...davalı idarece, son dönem artan terör saldırıları, personel kimlik kartlarının kayıp edilmesi sonucu ortaya çıkan güvenlik zafiyetlerinin önüne geçilmesi ve personel arasında mesai saatlerine uyulması hususundaki eşitliği sağlamak amacıyla "Personel Kontrol Sistemi" kurulduğu ve bu şekilde başta kurum çalışanlarının ve işlerinin takibi için kuruma gelen vatandaşların emniyetinin sağlandığı, personelin işe devam durumunun elektronik ortamda denetlendiği, davacı tarafından, yapılan bu uygulamanın Anayasa ve uluslararası anlaşmalarla korunan kişi hürriyeti ve özel yaşamın gizliliği ile kişisel verilerin korunması ilkesine aykırı olduğu ileri sürülerek bakılan davanın açıldığı, davalı idarece kurulan "Personel Kontrol Sistemi" incelendiğinde, bu sistemde personelin parmak izinin kriminal anlamda alınan parmak izinden farklı olduğu ve cihazla alınan parmak izinin harf sayısı ve değişik işaretlerden oluşan bir koda dönüştürüldüğü, söz konusu kod kullanılarak parmak izine ulaşmanın ise mümkün olmadığı, bu bağlamda kişilerin parmak izinden üretilen işaretlerin bireyin fiziksel olarak belirlenmesini

sağlamadan uzak olduğu ve bu anlamda kişisel veri olarak değerlendirilemeyeceği, kaldı ki hiçbir verinin kayıt altına alınmadığı, nitekim "Personel Kontrol Sistemi"nin personel disiplinini sağlayarak verimliliği artırma, kamu hizmetlerinin kesintisiz olarak yerine getirilmesi, kamu güvenliği gibi amaçlara hizmet ettiği anlaşıldığı, öte yandan ülkemizde ve coğrafyamızda giderek artan terör saldırıları karşısında ortaya çıkan güvenlik zafiyetlerinin önlenmesi, kamu kurumunda çalışan personellerin ve kuruma gelen vatandaşların can ve mal güvenliğinin önceliği, davalı idare tarafından kurulan cihazın kişisel verileri kayıt altına almadığı dikkate alındığında davacının davalı Kurum personelinin çalışmalarının personel takip sistemi ile takip edilmesi uygulamasından vazgeçilmesi yolundaki başvurusunun reddine ilişkin işlemde hukuka aykırılık bulunmadığı sonucuna ulaşıldığı..." gerekçesiyle davanın reddine karar verilmiştir.

Anayasanın "Temel Hak ve Hürriyetlerin Niteliği" başlıklı 12. maddesinde; "Herkes, kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlere sahiptir. Temel hak ve hürriyetler, kişinin topluma, ailesine ve diğer kişilere karşı ödev ve sorumluluklarını da ihtiva eder." hükmüne, "Temel Hak ve Hürriyetlerin Sınırlanması" başlıklı değişik 13. maddesinde, "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz." hükmüne, "Özel Hayatın Gizliliği" başlıklı değişik 20. maddesinde ise, "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir, özel hayatın ve aile hayatının gizliliğine dokunulamaz. Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar. Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilmiştir.

Avrupa İnsan Hakları Sözleşmesinin "Özel Hayatın ve Aile Hayatının Korunması" başlıklı 8. maddesinde, herkesin özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahip olduğu, Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesinin "Mahremiyet Hakkı" başlıklı 17. maddesinde de, hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemeyeceği; onuru veya itibarının hukuka aykırı saldırılara maruz bırakılmayacağına, herkesin bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahip olduğu belirtilmiştir.

Öte yandan, 07.04.2016 tarih ve 29677 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun'un 1. maddesinde; bu Kanunun, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek amacıyla çıkarıldığı, 2. maddesinde; bu Kanun hükümlerinin, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanacağı hükme bağlandıktan sonra, "Tanımlar" başlıklı 3. maddesinde; açık rızanın; belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı, kişisel verinin; kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi, kişisel verilerin işlenmesinin; kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi, veri sorumlusunun; kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi, ifade edeceği düzenlenmiştir.

Kanunun 'Genel İlkeler' başlıklı 4. maddesinde, "(1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.

(2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

- a) Hukuka ve dürüstlük kurallarına uygun olma.
- b) Doğru ve gerektiğinde güncel olma.
- c) Belirli, açık ve meşru amaçlar için işlenme.
- ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.” hükmüne;

‘Kişisel verilerin işleme şartları’ başlıklı 5. maddesinde, “(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.” hükmüne;

‘Özel nitelikli kişisel verilerin işleme şartları’ başlıklı 6. maddesinde, “(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmüne;

'İstisnalar' başlıklı 28. maddesinde ise, "(1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:

a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklerle uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi.

b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.

c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.

ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

(2) Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri aşağıdaki hâllerde uygulanmaz:

a) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.

b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.

c) Kişisel veri işlemenin kanunun verdiği yetkiye dayanarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.

ç) Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması." hükmüne yer verilmiştir.

Davaya konu işlemle, Beşiktaş Belediyesinde parmak üstü resmi ile personel takip ve kontrol sistemine geçilmesi kararlaştırılmış olup, uyuşmazlığın, başta özel hayatın gizliliği olmak üzere

kişilerin temel hak ve özgürlüklerinin korunması ve kişisel verilerin işlenmesi çerçevesinde değerlendirilmesi gerektiğinde kuşku bulunmamaktadır.

657 sayılı Devlet Memurları Kanununun 99 ve devam eden maddelerinde, Devlet memurlarının çalışma saatleri ile günlük çalışma saatlerinin başlama ve bitme saatlerinin tespitine yönelik düzenlemelere yer verilmiş olmakla birlikte, kamu görevlilerinin mesaiye devam durumlarının kontrolü konusunda ayrıntılı bir yasal düzenleme mevzuatımızda bulunmamakta ise de, idarelerce, gelişen teknolojinin kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması amacıyla, kamu kesiminde kullanılmaya başlamasını doğal karşılamak gerekmekte, buna karşılık, teknolojik imkânlar kullanılarak kişisel verilerin kayıt altına alınması ve işlenmesi uygulamasının yukarıda belirtilen düzenlemelere uygun olması zorunlu bulunmaktadır.

Yukarıda aktarılan düzenlemeler birlikte incelendiğinde, Anayasa'nın 20. maddesi ile, kişisel verilerin, ancak "kanunda öngörülen hallerde" veya "kişinin açık rızasıyla" işlenebileceğinin öngörüldüğü, konuyla ilgili olarak yürürlüğe konulan 6698 sayılı Kanunda, kişisel verinin, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi, kişisel verilerin işlenmesinin ise, kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade ettiğinin belirtildiği görülmekte, anılan kanunda, kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği hükme bağlanarak, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesini mümkün kılan şartların da düzenlendiği, kişilerin biyometrik verilerinin ise özel nitelikli kişisel veri olarak kabul edilerek, bu verilerin işlenmesinin kişilerin açık rızasına bağlandığı anlaşılmaktadır.

Diğer taraftan, "Biyometrik" kavramı, kullanıcının fiziksel veya davranışsal özelliklerini tanıyarak kimlik saptamak üzere geliştirilmiş bilgisayar kontrollü, otomatik sistemler için kullanılan genel bir terim şeklinde tanımlanmakta, "biyometrik yöntemler" ise, ölçülebilir fizyolojik ve bireysel özellikleri aracılığıyla gerçekleştirilen ve otomatik şekilde doğrulanabilen kimlik denetleme tekniklerini ifade etmekte olup, biyometrik yöntemlerin uygulanması suretiyle elde edilen verilerin kişisel veri olduğunda kuşku bulunmamaktadır.

Somut olayda, davalı idarece her ne kadar, Web tabanlı personel takip sisteminde kullanılan cihazlar ile biyometrik veri olan parmak izinin alınmadığı, cihazın parmağın fotoğrafını bile kaydetmediği, belediye çalışanlarının açık rızaları ile sisteme dâhil oldukları, sistemin güvenilirliği konusunda

taahhütname hazırlanarak imza altına alındığı ve isteği halinde personele dağıtıldığı, çalışanların kişisel verilerinin alınmasının söz konusu olmadığı, sistemden alınan tek veri olan personelin giriş çıkış zaman hareketlerinin yetkisiz kişi ve kurumlarca paylaşılmayacağı, davaya konu uygulama ile 0 ve 1 den oluşan rakamsal bir algoritma oluşturularak, bu rakamlarla kişinin parmağının (azami üç parmak) belli noktalarının ölçülerek, taranıp rakamsal olarak cihaz hafızasında tutulduğu, oluşturulan bu rakamsal verilerin kurum yazılımında saklanması nedeniyle başka bir cihaza da aktarılmadığı, cihaza parmağın dokunması ile tanımlamanın sayısal olarak gerçekleştiği ve bu sayı, yazılımdaki unique numara ile eşleştğinde cihaz üzerindeki parmak görselini sildiği, yani uygulamanın parmak yapısını sayısallaştırarak cihaz üzerinde benzersiz bir numaraya dönüştürme ve personelin kurum sicil numarası ile eşleştirme yaptığı, dava konusu uygulama ile kişisel verilerin alınması ve işlenmesinin söz konusu olmadığı ileri sürülmekte ise de; 0 ve 1 den oluşan rakamsal bir algoritma oluşturularak, bu rakamlarla kişinin parmağının (azami üç parmak) belli noktalarının ölçülerek, taranıp rakamsal olarak kaydedilmesinin biyometrik yöntemlerden olduğu, biyometrik yöntemle elde edilen verilerin de kişisel veri olduğunda kuşku bulunmadığı, biyometrik yöntemlerin kullanılması şeklinde bir uygulamanın ise, kamusal alanda da olsa bireyin temel haklarından olup, anayasada ve uluslararası sözleşmelerle güvence altına alınan "özel hayatın gizliliği" ilkesi kapsamında olduğu, nitekim, Avrupa İnsan Hakları Mahkemesince de, kişisel verilerin Avrupa İnsan Hakları Sözleşmesinin 'Özel ve aile hayatına saygı hakkı' başlıklı 8. maddesi kapsamında olduğunun kabul edildiği, kaldı ki, kişilerin biyometrik verilerinin 6698 sayılı Kanun gereği özel nitelikli kişisel veri olup, kanunla, özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesinin yasaklandığının anlaşılması karşısında, davalı idarenin anılan iddialarına itibar edilememiştir.

Bu durumda, biyometrik yöntemle elde edilen kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda tanımlanan özel nitelikli kişisel veri niteliğinde bulunduğu, ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğu açık olup, kanunda sayılan ve ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesini mümkün kılan şartların somut olayda mevcut olmadığı da dikkate alındığında, personelden kişisel veri alınması kapsamında olan "parmak üstü resmi" ile mesai takibi ve kontrolü uygulamasının, kamusal alanda da olsa "özel hayatın gizliliği" ilkesi kapsamında olması, 6698 sayılı Kanunda öngörülen hallerden olmaması nedeniyle kişinin açık rızası ile işlenebilmesinin mümkün bulunması, dava konusu parmak üstü resmi ile personel takip ve kontrol sistemine davacının açık rızası olmadan geçildiğinin anlaşılması karşısında, yukarıda belirtilen temel haklar, Anayasal ilkeler, uluslararası sözleşme kuralları ve 6698 sayılı Kanun hükümleri ile bağdaşmayan dava konusu işlemde hukuka uyarlık bulunmadığı sonucuna varılmıştır.

Açıklanan nedenlerle, davacı istinaf başvurusunun kabulüne, İstanbul 4. İdare Mahkemesi'nce verilen 30/06/2017 tarih ve E:2017/296, K:2017/1477 sayılı kararın kaldırılmasına, dava konusu işlemin iptaline, aşağıda dökümü yapılan 312,05-TL yargılama gideri ile Avukatlık Asgari Ücret Tarifesi uyarınca takdir edilen 1090,00-TL vekalet ücretinin davalı idareden alınıp davacıya verilmesine, artan posta ücretinin ilgisine iadesine, kararın taraflara tebliğ için dosyanın ait olduğu mahkemeye gönderilmesine kesin olarak, 18/01/2018 tarihinde karar sonucunda oybirliği, gerekçede oyçokluğuyla karar verildi.

AZLIK OYU: Kişisel verilerin korunması hakkı, kişinin insan onurunun korunması ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı ifade etmektedir. Bununla birlikte, sözkonusu hak mutlak ve sınırsız olmayıp, Anayasa'nın 13. ve 20. maddeleri gereğince belirli koşullarda, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmamak üzere yasayla sınırlanabilir. Bu bağlamda, kişisel verilerin sistematik biçimde kayıt altına alınabilmesi için verilerin korunmasına ilişkin esas ve usullerin yasayla düzenlenmesi zorunludur. Diğer bir deyişle, kişisel verilerin korunmasına ilişkin gerekli yasal düzenlemeye ve teknik olanaklara sahip olmayan bir idarenin, kişinin rızasını alsa dahi bu konudaki işleminin hukuka uygunluğundan söz etmek olanaklı olmayacaktır.

Bu çerçevede, idarelerce gelişen teknolojinin, kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması nedeniyle, kamu kesiminde kullanılmaya başlanması doğal olmakla birlikte, teknoloji kullanılarak kişisel verilerin kayıt altına alınması uygulamasının yukarıda belirtilen hükümlere uygun olması gerektiğinde kuşku bulunmamaktadır.

Anayasa'da, ülkemizin tarafı olduğu ve yine Anayasa'nın 90. maddesi uyarınca kanun hükmünde olan uluslararası sözleşmelerde, kişilerin özel hayatı ile aile hayatının ve kişisel verilerinin gizliliğine saygı gösterilmesi gerektiği ve bu gizliliğe müdahale edilemeyeceği açıkça hüküm altına alınmış olup, bu gizliliğe müdahalenin milli güvenlik, kamu düzeni gibi zorunluluk arz eden durumlara münhasır olarak ve yasayla öngörülmek şartıyla mümkün olduğu anlaşılmaktadır.

Bu durumda, ilgililerden kişisel veri alınması niteliğinde olan "parmak resmi eşleştirmesinin" "özel hayatın gizliliği" ilkesi kapsamında bulunması karşısında uygulamanın sınırlarını, usul ve esaslarını gösteren bir yasal dayanak kapsamında gerçekleştirildiğinin ortaya konulmaması toplanan verilerin ileride başka bir şekilde kullanılmayacağına dair bir güvencenin mevcut olmaması gözönüne alındığında, yukarıda belirtilen temel haklar ve Anayasal ilkeler ile uluslararası sözleşme kuralları ile

bağdaşmayan dava konusu işlemde hukuka uygunluk bulunmadığı gerekçesiyle karar verilmesi gerektiği görüşüyle kararın gerekçesine katılmıyorum.

İzmir BİM - 6. İdari Dava Dairesi (E. 2017/1238)

İzmir Bölge İdare Mahkemesi, 6. İDD, E. 2017/1238 K. 2017/1815 T. 14.12.2017

Esas No.: 2017/1238

Karar No.: 2017/1815

Karar Tarihi: 14.12.2017

İSTEMİN ÖZETİ: Davacı tarafından, özürlü raporunun Sağlık-net ve Medula sisteminden silinmesi istemiyle yaptığı 29.09.2016 tarihli başvurunun reddine ilişkin Denizli Devlet Hastanesi Yöneticiliği'nin 03.11.2016 tarih ve 56834361/774.09.E.13852 sayılı işleminin iptali istemiyle açılan davada; 2709 sayılı Türkiye Cumhuriyeti Anayasası'nın 20/3. maddesi uyarınca davacının kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı kapsamında kişisel verilerinin silinmesini talep edebileceği, yine Anayasa'nın 41. maddesi uyarınca Devletin çocukların (davacının) korunması için gereken tedbirleri alacağı, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 7/1. maddesi ve Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'in 9/1. maddesi hükümleri uyarınca işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel sağlık verilerinin, ilgili kişinin talebi üzerine veri sorumlusu tarafından anonim hale getirileceği veya silineceği, öte yandan; 222 sayılı İlköğretim ve Eğitim Kanunu'nun 2. maddesi uyarınca kız ve erkek öğrenciler için ilköğretimin mecburi olduğu, aynı Kanun'un 3. maddesi uyarınca mecburi ilköğretim çağının çocuğun 5 yaşını bitirdiği yılın eylül ayı sonunda başlayacağı, Milli Eğitim Bakanlığı Okul Öncesi Eğitim ve İlköğretim Kurumları Yönetmeliği'nin 11/2 ve 11/6-a maddeleri uyarınca okul yönetiminin ilkokulların birinci sınıfına, kayıtların yapıldığı yılın eylül ayı sonu itibarıyla 66 ayını dolduran çocukların kaydını e-okul sistemi üzerinden yapacağı, aynı Yönetmeliğin 11/6-b maddesi uyarınca Okul müdürlüklerinin, yaşça kayıt hakkını elde eden çocuklardan 66, 67 ve 68 aylık olanları velisinin vereceği dilekçe; 69, 70 ve 71 aylık olanların ise ilkokula başlamaya hazır olmadıklarını belgeleyen sağlık raporu ile okul öncesi eğitime yönlendirebilecekleri veya kayıtlarını bir yıl erteleyebilecekleri, 09.08.2010 doğumlu olan davacının ailesinin de, rapor tarihi itibarıyla 70 aylık olan davacının ilkokula yapılan kaydının 1 yıl ertelenmesi amacıyla rapor almak için davalı idareye başvurduğu, davalı idarece davacı hakkında "hafif bilişsel gelişimde gecikme" teşhisiyle "özür durumuna göre tüm vücut fonksiyon kaybının % 50" olduğuna ilişkin 06.06.2016 tarih ve 3537 sayılı engelli sağlık kurulu raporu verildiği, davacının ailesinin itiraz etmesi üzerine yeniden yapılan muayene sonucunda "normal bilişsel gelişim" teşhisiyle "özür durumuna göre tüm vücut fonksiyon

kaybının % 0"olduđuna iliřkin 13.07.2016 tarih ve 4194 sayılı engelli sađlık kurulu raporu verildiđi, bu durumda ortada davacı hakkında verilmiř taban tabana zıt iki ayrı sađlık kurulu raporu bulunduđu, davalı idarenin davacı hakkında "normal biliřsel geliřim" teřhisiyle verilen 13.07.2016 tarih ve 4194 sayılı engelli sađlık kurulu raporunun geđerli olduđunun belirtildiđi, her ne kadar davalı idarece ilk olarak verilen ve davacının "hafif biliřsel geliřimde gecikme" teřhisini iđereren 06.06.2016 tarih ve 3537 sayılı raporun da bilimsel olduđu iddia edilmiř ise de, iki rapor arasında yaklařık 1 aylık bir zaman farkı olduđu dūřünüldüđünde 06.06.2016 tarihli ilk raporun hayatın olađan akıřına aykırı dūřtüđü ve davacının ilkokula kaydının 1 yıl ertelenmesi iđerin yardımcı olma amaçlı olarak verildiđi, bu nedenle geđerliliđi bulunmadıđı davacı tarafından da kabul edilen ve davacının gerçek durumunu yansıtmayan 06.06.2016 tarihli ilk raporun; iđereri de dikkate alındıđında sistemde kayıtlı kalmasının davacının menfaatine uygun dūřmeyeceđi, diđer yandan her ne kadar davalı idarece söz konusu raporun sistem üzerinden geriye dönük olarak silinmesinin mümkün olmadığı iddia edilmiř ise de, raporun ortadan kalkmasını gerektiren řartların olduđu, davacının talebinin bu raporun sistemden silinmesi olduđu, raporun sistemden silinmesinin ise yukarıda anılan Kiřisel Sađlık Verilerinin İřlenmesi ve Mahremiyetinin Sađlanması Hakkında Yönetmelik'in 9/1. maddesi uyarınca mümkün olduđu, bu haliyle davacının söz konusu raporun sistemden silinmesine yönelik talebinin davalı idarece olumlu řekilde karřılanması gerekirken, aksi yönde tesis edilen dava konusu iřlemde hukuka uyarlık bulunmadıđı gerekçesiyle dava konusu iřlemin iptali yolunda Denizli İdare Mahkemesince verilen 05/06/2017 tarih, E: 2017/399, K: 2017/1099sayılı kararın; dava konusu iřlemin bilgilendirme mahiyetinde bir iřlem olduđu, kesin ve yürütülebilir niteliđinin bulunmadıđı, davacının hukuki yararının bulunmadıđı, söz konusu raporların kaldırılması konusunda idarelerinin yetkisi bulunmadıđı ileri sürülerek istinaf yoluyla kaldırılması istenilmektedir.

SAVUNMANIN ÖZETİ: Dava konusu iřlemin, kesin ve yürütülmesi gereken bir iřlem niteliđinde olduđu, sisteme kaydını yapan idarenin bu bilgilerin silinmesi konusunda yetkisiz olduđunun kabul edilemeyeceđi, istinaf talebinin reddi gerektiđi savunulmaktadır.

TÜRK MİLLETİ ADINA

Hüküm veren İzmir Bölge İdare Mahkemesi Altıncı İdare Dava Dairesince; 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'na ekli (I) sayılı cetvelde yer aldıđından 659 sayılı Kanun Hükmünde Kararname'nin 2/1-ç ve 6/1 maddeleri uyarınca taraf sıfatına haiz bulunan ve bu nedenle hasım durumuna alınan Türkiye Kamu Hastaneleri Kurumunun, 25.08.2017 tarih ve 30165 sayılı Resmi Gazete'de yayınlanarak yürürlüğe giren 694 sayılı Kanun Hükmünde Kararnamenin 203/1-ğ maddesi ile 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'na ekli (I) sayılı cetveldən çıkartılarak anılan

Kanun Hükümünde Kararname'nin 184. maddesi ile Kamu Hastaneleri Genel Müdürlüğü adıyla Sağlık Bakanlığının hizmet birimi olarak teşkilatlandırıldığı anlaşıldığından, Türkiye Kamu Hastaneleri Kurumu hasım mevkiinden çıkarılıp Sağlık Bakanlığı hasım mevkiine alınarak, dava dosyasında yer alan bilgi ve belgeler incelenerek işin gereği görüldü:

2577 sayılı İdari Yargılama Usulü Kanununun "İstinaf" başlıklı 45. maddesinde, "... İstinaf, temyizın şekil ve usullerine tabidir.

Bölge idare mahkemesi, yaptığı inceleme sonunda ilk derece mahkemesi kararını hukuka uygun bulursa istinaf başvurusunun reddine karar verir. Karardaki maddi yanlışlıkların düzeltilmesi mümkün ise gerekli düzeltmeyi yaparak aynı kararı verir.

Bölge idare mahkemelerinin 46 ncı maddeye göre temyize açık olmayan kararları kesindir..." kuralına yer verilmiş; "Temyiz" başlıklı 46. maddesinde Bölge İdare Mahkemelerinin kararlarının tebliğini izleyen 30 gün içerisinde Danıştayda temyiz edilebileceği öngörüldükten sonra temyize tabi kararlarının hangileri olduğu sayma yoluyla sınırlanarak belirlenmiş, "temyiz incelemesi üzerine verilecek kararlar" başlıklı 49. maddesinin 2. fıkrasında, "a) Görev ve yetki dışında bir işe bakılmış olması, b) Hukuka aykırı karar verilmesi, c) Usul hükümlerinin uygulanmasında kararı etkileyebilecek nitelikte hata veya eksikliklerin bulunması" kaldırma nedenleri olarak sayılmıştır.

Dosyadaki belgeler ile başvuru dilekçesindeki iddiaların incelenmesinden, istinaf başvurusuna konu kararın hukuka ve usule uygun olduğu, kararın kaldırılmasını gerektirecek yasal bir sebebin bulunmadığı sonucuna varılmıştır.

Açıklanan nedenlerle; Denizli İdare Mahkemesince verilen 05/06/2017 tarih, E:2017/399, K: 2017/1099 sayılı karara karşı yapılan istinaf başvurusunun reddine, aşağıda dökümü yapılan yargılama giderlerinin istinaf isteminde bulunan üzerinde bırakılmasına, yatırılan posta gideri avansından artan miktarın Mahkemesince yatırına iadesine, kesin olarak 14/12/2017 tarihinde oybirliğiyle karar verildi.

Konya BİM - 4. İdari Dava Dairesi (E. 2020/731)

Konya Bölge İdare Mahkemesi, 4. İDD, E. 2020/731 K. 2020/495 T. 1.6.2020

Esas No.: 2020/731

Karar No.: 2020/495

Karar Tarihi: 01.06.2020

DAVANIN KONUSU: Davacı tarafından, Isparta ili X1 Komutanlığı Terörizmle Mücadele Eğitim ve Tatbikat Merkezi Komutanlığında uzman erbaş kursiyeri olarak görev yapmakta iken güvenlik soruşturması olumsuz neticelendiği gerekçesiyle sözleşmesinin feshedilerek ilişkisinin kesilmesine ilişkin 01/06/2018 tarih ve MRK.Ş.:17217803-1980-1334581-18 sayılı işlemin iptali ile yoksun kaldığı parasal hakların tahakkuk tarihinden itibaren işleyecek yasal faizi ile ödenmesi istemiyle açılmıştır.

YARGILAMA SÜRECİ:

Isparta İdare Mahkemesi'nin 19/12/2018 tarih ve E:2018/994, K:2018/1765 sayılı kararı ile; davacının uzman erbaş sözleşmesinin feshedilmesine neden olarak suç uydurma suçundan 16 gün hapis cezası ile cezalandırılmasının gösterildiği, Konya 3. Çocuk Mahkemesince hükmedilen cezanın otuz günden daha fazla hapis cezası olmadığı, Konya (Kapatılan) 3. Çocuk Mahkemesinin 07.09.2018 tarihli kararı ile davanın düşmesine karar verildiği, bunların yanında ceza mahkemesi kararının içeriği incelendiğinde davacının eyleminin uzman erbaşlık göreviyle bağdaşmayacak nitelik de taşımadığı, bu nedenle güvenlik soruşturması ve arşiv araştırmasının olumsuz sonuçlandığından bahisle sözleşmesinin feshine ilişkin dava konusu işlemde hukuka uyarlık bulunmadığı gerekçesiyle iptaline, davacının işlem nedeniyle yoksun kaldığı parasal haklarının (görev aylıkları ve aylık farklarının) tahakkuk tarihlerinden itibaren işletilecek yasal faiziyle birlikte ödenmesine karar verilmiştir.

Davacının istinaf başvurusunu inceleyen Dairemizin 18/04/2019 tarih ve E:2019/301, K:2019/531 sayılı kararı ile; davacının Konya 3. Çocuk Mahkemesi'nin 25.11.2014 tarih ve E:2014/464, K:2014/719 sayılı kararıyla cürüm tasnii suçundan 16 gün hapis cezası ile cezalandırılmasına, hükmün açıklanmasının geri bırakılmasına ve 3 yıl süre ile herhangi yükümlülük belirlenmeden denetim süresine tabi tutulmasına karar verildiği, bu kararın güvenlik soruşturmasının olumsuz sonuçlanmasına dayanak teşkil ettiği, davacının 3 yıllık denetim süresi içerisinde yeni bir suç işlememesi üzerine Konya (Kapatılan) 3. Çocuk Mahkemesi'nin 07.09.2018 tarihli kararı ile davanın düşmesine karar verildiği, güvenlik soruşturmasının olumsuz sonuçlanmasının sözleşmenin feshi sebebi sayılacağı, verilen ceza

ertelense, seçenek yaptırımlara çevrilse, hükmün açıklanması geri bırakılsa veya affa uğrasa bile "cürüm tasnii" suçundan dolayı mahkum olunmasının göreve engel hal olduğu, bu nedenle davacının sözleşmesinin feshine ilişkin dava konusu işlemde hukuka aykırılık, İdare Mahkemesi kararında hukuki isabet bulunmadığı gerekçesiyle istinaf başvurusunun kabulü ile idare mahkemesi kararının kaldırılmasına, davanın reddine karar karar verilmiştir.

Davacının temyiz istemini inceleyen Danıştay 12. Dairesi'nin, 27/11/2019 tarih ve E:2019/3372, K:2019/9303 sayılı kararı ile;10.10.1996 doğumlu olan ve hakkındaki ceza mahkûmiyetine konu suçu işlediği 14.07.2014 tarihinde on sekiz yaşından küçük olan davacının, on sekiz yaşından küçükken işlediği bu suça ilişkin kayıtların Konya Valiliği İl Emniyet Müdürlüğü tarafından Milli Savunma Bakanlığı Personel Temin Daire Başkanlığına verilmesi üzerine, ilgili kurum tarafından bu kaydın dikkate alınması suretiyle davacı hakkındaki güvenlik soruşturmasının olumsuz sonuçlandığının görüldüğü, bu durumda, davacının adli sicil kaydında görünmeyen, on sekiz yaşından küçükken işlediği suça ilişkin kaydın, Kanun ve Yönetmelik hükümleri uyarınca, ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebileceği açık olduğu, kişisel veri niteliğinde olan bu kaydın, güvenlik soruşturması kapsamında ilgili kamu kurumuna verilmesi ve güvenlik soruşturmasında kullanılmasının hukuka aykırı olduğu, hukuka aykırı şekilde idari makamlara verilen bu kaydın değerlendirilmesi suretiyle güvenlik soruşturmasının olumsuz sonuçlandırılması, Anayasa'nın 20. maddesi ve Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi uyarınca "özel hayata saygı hakkının" ihlâli sonucunu doğurduğu, bu itibarla, davacının on sekiz yaşından küçükken işlediği suça ilişkin kayda dayanılarak güvenlik soruşturmasının olumsuz sonuçlanması suretiyle öğrencilikten ilişkisinin kesilmesine ilişkin dava konusu işlemde hukuka aykırılık, davanın reddi yönündeki Bölge İdare Mahkemesi kararında hukuki isabet görülmediği, dava konusu işlemin iptali yönündeki Isparta İdare Mahkemesi kararına karşı yapılan istinaf başvurusunun kabulü yolundaki temyize konu Bölge Mahkemesi kararında hukuki isabet bulunmadığı gerekçesiyle, davacının temyiz isteminin kabulüyle, Dairemizin 18/04/2019 tarih ve E:2019/301, K:2019/531 sayılı kararının bozulmasına karar verilmiştir.

TÜRK MİLLETİ ADINA

Karar veren Konya Bölge İdare Mahkemesi 4. İdari Dava Dairesi'nce, Danıştay 12. Dairesi'nin, 27/11/2019 tarih ve E:2019/3372, K:2019/9303sayılıbozma kararına uyularakdava dosyası yeniden incelenmek suretiyle gereği görüldü.

MADDİ OLAY:

Davacı, Isparta Terörizmle Mücadele Eğitim ve Tatbikat Merkez Komutanlığı'nda uzman erbaş kursiyeri olarak görev yapmaktadır.

Davacı hakkında yaptırılan güvenlik soruşturması ve arşiv araştırması sonucu, 14.07.2014 tarihinde (18 yaşından küçük olduğu dönem) işlediği iddia edilen bir fiil nedeniyle "suç uydurma" suçundan yargılandığı ve Konya 3. Çocuk Mahkemesi'nin 25.11.2014 tarihli ve E:2014/464, K:2014/719 sayılı kararı ile 16 gün hapis cezası ile cezalandırılmasına, hükmün açıklanmasının geri bırakılmasına, üç yıl süreyle denetime tabi tutulmasına karar verildiği yolundaki bilgi notu üzerine güvenlik soruşturması ve arşiv araştırması olumsuz değerlendirilerek 01.06.2018 tarihli ve 1334581-18 sayılı dava konusu işlemde sözleşmesinin feshine karar verildiği, bunun üzerine bakılan davanın açıldığı anlaşılmıştır.

Davacı hakkında verilen bu karardan sonra üç yıllık denetim süresinin dolması üzerine davacı tarafından 05.09.2018 havale tarihli dilekçe ile yapılan başvuru sonunda Konya (Kapatılan) 3. Çocuk Mahkemesi'nin 07.09.2018 tarihli ve E:2014/464, K:2014/719 sayılı kararı ile davanın düşmesine karar verilmiştir.

İLGİLİ MEVZUAT:

Anayasa'nın "Özel hayatın gizliliği" başlıklı 20. maddesinin birinci fıkrasında;

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz" hükmüne, üçüncü fıkrasında; "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilmiştir.

Avrupa İnsan Hakları Sözleşmesinin "Özel ve aile hayatına saygı hakkı" başlıklı 8. maddesinde de;

"(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir," hükmü yer almaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 6. maddesinde;

"(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü yer almaktadır.

657 sayılı Devlet Memurları Kanunu'nun 48. maddesinde devlet memurluğuna alınmaya ilişkin genel ve özel şartlar düzenlenmiş; B/2 bendinde "Kurumların özel kanun veya diğer mevzuatında aranan şartları taşımak" özel şartlar arasında sayılmıştır.

5352 sayılı Adli Sicil Kanunu'nun 10. maddesinin üçüncü fıkrasında, "Onsekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebilir." hükmü yer almaktadır.

07/09//2005 tarihli ve 25929 sayılı Resmi Gazete'de yayımlanan Adli Sicil Yönetmeliği'nin 12. maddesinin dördüncü fıkrasında, "Onsekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere mahkeme, hâkim veya savcılıklarca istenebilir." hükmü ile 14. maddesinin birinci fıkrasında, "Onsekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere mahkeme, hâkim veya savcılıklara talep halinde verilir." hükmü yer almaktadır.

HUKUKİ DEĞERLENDİRME:

Anayasa Mahkemesi'nin 27/02/2019 tarihli ve 2014/7256 Başvuru no'lu kararında özetle;

"..Somut olayda başvuruçunun on sekiz yaşından küçükken işlediği suçun kayıtlarının Adana Valiliği Emniyet Müdürlüğü tarafından Komisyon Başkanlığına verildiği, bu kaydın dikkate alınmak

suretiyle güvenlik soruşturmasının olumsuz sonuçlandığı, başvuruçunun sözleşmeli infaz ve koruma memurluğuna atamasının yapılmadığı anlaşılmaktadır.

Resmi makamlar tarafından muhafaza edilmekte olan, başvuruçunun hakkında yürütülen ceza yargılamasına dair bilgilerin özel hayata saygı hakkı anlamında kişisel nitelikli veriler olduğu açıktır. Söz konusu kişisel verinin kamu kurumlarıyla paylaşılması ve güvenlik soruşturmalarında kullanılmasının Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkına bir müdahale oluşturduğu sonucuna varılmıştır...

Öte yandan somut olayda başvuruçunun yazılı ve sözlü sınavı kazandığının ilan edilmiş olduğu, on sekiz yaşından küçükken işlediği suçla ilişkin kaydın 5352 sayılı Kanun'un 10. maddesinin (3) numaralı fıkrasında yer alan hükme açıkça aykırı şekilde idari makamlara verilmiş olduğu dikkate alındığında özel hayata saygı hakkına yönelik müdahalenin bu yönüyle de kanuni dayanaktan yoksun olduğu anlaşılmaktadır..." değerlendirmelerine yer verilmiştir.

Dosya içerisinde yer alan bilgi ve belgeler ile Anayasa Mahkemesi kararı doğrultusunda dava konusu olay incelendiğinde, 10.10.1996 doğumlu olan ve hakkındaki ceza mahkûmiyetine konu suçunu işlediği 14.07.2014 tarihinde on sekiz yaşından küçük olan davacının, on sekiz yaşından küçükken işlediği bu suçla ilişkin kayıtların Konya Valiliği İl Emniyet Müdürlüğü tarafından Milli Savunma Bakanlığı Personel Temin Daire Başkanlığına verilmesi üzerine, ilgili kurum tarafından bu kaydın dikkate alınması suretiyle davacı hakkındaki güvenlik soruşturmasının olumsuz sonuçlandığı görülmüştür.

Bu durumda, davacının adli sicil kaydında görünmeyen, on sekiz yaşından küçükken işlediği suçla ilişkin kaydın, yukarıda yazılı Kanun ve Yönetmelik hükümleri uyarınca, ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebileceği açık olduğundan, kişisel veri niteliğinde olan bu kaydın, güvenlik soruşturması kapsamında ilgili kamu kurumuna verilmesi ve güvenlik soruşturmasında kullanılması hukuka aykırı olduğundan, hukuka aykırı şekilde idari makamlara verilen bu kaydın değerlendirilmesi suretiyle güvenlik soruşturmasının olumsuz sonuçlandırılması, Anayasa'nın 20. maddesi ve Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi uyarınca "özel hayata saygı hakkının" ihlâli sonucunu doğurmaktadır.

Bu itibarla, davacının on sekiz yaşından küçükken işlediği suçla ilişkin kayda dayanılarak güvenlik soruşturmasının olumsuz sonuçlanması suretiyle öğrencilikten ilişığının kesilmesine ilişkin dava konusu işlemde hukuka uyarlık görülmemiştir.

Açıklanan nedenlerle, dava konusu işlemin iptali ile davacının yoksun kaldığı parasal hakların kabulüne dair yerel Mahkeme kararında hukuka aykırılık bulunmadığından, istinaf başvurusunun reddi gerekmektedir.

KARAR SONUCU: Açıklanan nedenlerle,

1-Yukarıda anılan Danıştay 12. Dairesi'nin 27/11/2019 tarih ve E:2019/3372, K:2019/9303 sayılıbozma kararına uyularak, işlemin iptali ile yoksun kalınan parasal hakların kabulü yolunda verilen ilk derece mahkemesi kararına yapılan istinaf başvurusunun yukarıda anılan gerekçe ile reddine,

2- Aşağıda dökümü yapılan temyiz aşamasına ilişkin toplam 455,80-TL yargılama giderlerinin davalı idareden alınarak davacıya verilmesine, hukuka uygun bulunan ilk derece mahkemesi kararında davacı lehine vekalet ücretine hükmedildiğinden bu konuda tekrar hüküm kurulmasına yer olmadığına,

3-Aşağıda dökümü yapılan istinaf aşamasına ilişkin 72,00-TL yargılama giderinin davalı idare üzerinde bırakılmasına,

4-Temyiz aşamasında kullanılmayan 73,10-TL yürütmeyi durdurma harcının istemi halinde davacıya iadesine,

5-Artan posta avansının kararın kesinleşmesinden sonra taraflara Mahkemesince iadesine,

2577 sayılı Kanun'un 46/c maddesi uyarınca bu kararın tebliğinden itibaren 30 gün içinde Danıştay'a temyiz yolu açık olmak üzere 01/06/2020 tarihinde oybirliği ile karar verildi.

UYUŞMAZLIK MAHKEMESİ KARARLARI

Bölüm İçeriği

- Uyuşmazlık Mahkemesi HB. (E. 2021/313)

Uyuşmazlık Mahkemesi Kararı - HB. (E. 2021/313)

Uyuşmazlık Mahkemesi Kararı - HB., E. 2021/313 K. 2021/395 T. 5.7.2021

ÖZET: 6698 sayılı Kanun uyarınca verilen idari para cezasının iptali istemiyle açılan davanın 5326 sayılı Kanun'un 3 ve 27/1. maddesi uyarınca ADLİ YARGI YERİNDE çözümlenmesi gerektiği hk.

KARAR

Davacı: M. Yazılım Medya Bilişim Basım Yayıncılık Reklam İç ve Dış Tic. A.Ş.

Vekili: Av. Ç.Ü.

Davalı: Kişisel Verileri Koruma Kurumu

Vekili: Av. Y. Ö.

I. DAVA KONUSU OLAY

1. Kişisel Verileri Koruma Kurumu Kişisel Verileri Koruma Kurulunun 03/03/2020 tarihli ve 2020/196 sayılı kararı ile, davacı şirkete ait internet sitesinin ana sayfasında 22/05/2018 tarihinde yayımlanan Bir disiplin soruşturmasıyla, denetmen yardımcısını memurluğa düşürdüler başlıklı haberin altında yapılan yorumlarla ilgili olarak ilgili kişi Y.A.'e ait kişisel verinin Türkiye İlaç ve Tıbbi Cihaz Kurumuna aktarılmasına dair başvurunun incelenmesi neticesinde, 375 sayılı Kanun Hükmünde Kararnamenin Ek 24. maddesi uyarınca sağlık denetçilerinin görev ve yetkileri kapsamında, davacı şirketten denetim için gerekli olan bütün bilgi ve belgelerin talep edilmesi şeklinde gerçekleşen kişisel veri işleme faaliyetinin, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 5. maddesinin ikinci fıkrasının (a) bendinde yer alan "kanunlarda açıkça öngörülme" hükmü kapsamında olduğu, diğer yandan davacının söz konusu verileri aktarmasının Kanun'un 5. maddesinin ikinci fıkrasının (ç) bendi hükmüne göre "veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" hükmü kapsamında olduğu, bu çerçevede söz konusu verilerin Kanun'un 8. maddesinin ikinci fıkrasının (a) bendi uyarınca aktarıldığı değerlendirilmekle birlikte, söz konusu aktarım ile soruşturmanın konusu olmayan üçüncü kişilerin kişisel verilerinin de veri sorumlusu davacı tarafından aktarıldığı dikkate alındığında, soruşturma konusu olmayan söz konusu kişisel verilerin aktarılmasının Kanun'un 4. maddesinin ikinci fıkrasının (ç) bendinde yer alan "amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesine aykırı olduğu, bu itibarla Kanun'un 12. maddesinin birinci fıkrasında

yer alan veri güvenliğine ilişkin yükümlülükleri yerine getiremeyen veri sorumlusu davacı hakkında 18. maddesinin birinci fıkrasının (b) bendi uyarınca 50.000 TL idari para cezası uygulanmasına;

2. T.C. Sağlık Bakanlığı Türkiye İlaç ve Tıbbi Cihaz Kurumunun, söz konusu soruşturma kapsamında davacı şirketten ilgili habere yorum yapan kullanıcıların tamamının İP adreslerini talep etmesi göz önüne alındığında, denetim faaliyetlerinde 6698 sayılı Kanun'un 4. maddesinde yer alan genel ilkeler başta olmak üzere Kanun hükümlerine uyum hususunda azami dikkat ve özeni göstermesi, öte yandan, söz konusu soruşturma kapsamında elde edilmiş ve soruşturma konusuyla ilgili olmayan üçüncü kişilere ait kişisel verilerin Kanun'un 7. maddesinde yer alan hükümler çerçevesinde silinmesi veya yok edilmesi ve sonucundan Kurula bilgi verilmesi hususlarında talimatlandırılmasına karar verilmiştir.

3. Davacı vekili, kurul kararı ile uygulanan idari para cezasının iptali istemiyle adli yargı yerine başvuruda bulunmuştur.

II. UYUŞMAZLIĞA İLİŞKİN BAŞVURU SÜRECİ

A. Adli Yargıda

4. Ankara 5. Sulh Ceza Hâkimliği 28/12/2020 tarihli ve D.İş. No. 2020/3184 sayılı kararı ile, kurul kararında idari para cezası ile birlikte üçüncü kişilere ait kişisel verilerin Kanun'un 7. maddesinde yer alan hükümler çerçevesinde silinmesi veya yok edilmesi ve sonucundan Kurula bilgi verilmesi kararının da bulunduğu, bu kararın da iptalinin istendiğini belirterek, bu durumda 5326 sayılı Kabahatler Kanunu'nun 27/8. maddesine göre idari yaptırım kararının verildiği işlem kapsamında aynı kişi ile ilgili olarak idari yargının görev alanına giren kararın da verilmiş olması nedeniyle yapılan başvuru konusunda karar verme görevinin idari yargı yerine ait olduğu gerekçesiyle başvurunun görev yönünden reddine karar vermiş, verilen karar itiraz edilmeden kesinleşmiştir.

5. Davacı vekili, bu kez, aynı istemle idari yargı yerinde dava açmıştır.

B. İdari Yargıda

6. Ankara 14. İdare Mahkemesi 30/03/2021 tarihli ve E.2021/96 sayılı kararı ile, 6698 sayılı Kanun uyarınca verilen idari para cezasına karşı açılan davanın çözümünün, anılan Kanun'da idari yaptırım kararına karşı kanun yolu gösterilmediği, diğer tedbir kararlarının Türkiye İlaç ve Tıbbi Cihaz Kurumu adına verildiği, 5326 sayılı Kanun'un 27/8. maddesinin uygulanma kabiliyeti bulunmadığını belirterek, 5326 sayılı Kabahatler Kanunu uyarınca adli yargı yerine ait olduğu gerekçesiyle, 2247 sayılı Kanun'un 19. maddesi uyarınca görevli yargı yerinin belirlenmesi için Uyuşmazlık

Mahkemesine başvurulmasına ve davanın incelenmesinin Uyuşmazlık Mahkemesince karar verilinceye kadar ertelenmesine karar vermiştir.

III. İLGİLİ HUKUK

7. 375 sayılı Kanun Hükmünde Kararnamenin "Müfettiş, denetmen, denetçi, kontrolör, aktüer istihdamı" başlıklı Ek 24. maddesinin son fıkrası şöyledir:

Denetime tabi gerçek ve tüzel kişiler, denetim için gereken gizli dahi olsa bütün belge, defter ve bilgileri talep edildiği takdirde ibraz etmek, para ve para hükmündeki evrakı ve ayniyatı ilk talep halinde göstermek, sayılmasına ve incelemesine yardımcı olmak zorundadır. Müfettiş, denetmen, denetçi, kontrolör ve aktüerler ile bunların yardımcı ve stajyerleri, görevleri sırasında tüm resmi daire, kurum, kuruluş ve kamuya yararlı derneklerle, gerçek ve tüzel kişilerden gerekli yardım, bilgi, evrak, kayıt ve belgeleri istemeye yetkili olup, kanuni bir engel olmadıkça bu isteğin yerine getirilmesi zorunludur."

8. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Amaç" başlıklı 1. maddesi şöyledir:

" (1) Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir."

9. "Kapsam" başlıklı 2. maddesi şöyledir:

" (1) Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır."

10. "Genel ilkeler" başlıklı 4. maddesi şöyledir:

" (1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.

(2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

a) Hukuka ve dürüstlük kurallarına uygun olma.

b) Doğru ve gerektiğinde güncel olma.

c) Belirli, açık ve meşru amaçlar için işlenme.

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme."

11. "Kişisel verilerin işleme şartları" başlıklı 5. maddesi şöyledir:

" (1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması."

12. "Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi" başlıklı 7. maddesi şöyledir:

" (1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.

(2). Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır.

(3). Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir."

13. "Kişisel verilerin aktarılması" başlıklı 8. maddesi şöyledir:

" (1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz.

(2) Kişisel veriler;

a) 5 inci maddenin ikinci fıkrasında,

b) Yeterli önlemler alınmak kaydıyla, 6 ncı maddenin üçüncü fıkrasında,

belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir.

(3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır."

14. "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12.. maddesi şöyledir:

" (1) Veri sorumlusu;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak,

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

(2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

(3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

(4) Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

(5) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir."

15. "Şikâyet üzerine veya resen incelemenin usul ve esasları" başlıklı 15. maddesinin ilgili fıkraları şöyledir:

" (1) Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapar.

(5) Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması hâlinde Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ eder. Bu karar, tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilir.

16. "Kabahatler" başlıklı 18. maddesi şöyledir:

"(1) Bu Kanunun;

a) 10 uncu maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar,

b) 12 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar,

c) 15 inci maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar,

idari para cezası verilir.

(2) Bu maddede öngörülen idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır.

(3) Birinci fıkrada sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu Kurula bildirilir."

17. 6698 sayılı Kanun'da idari para cezasına ve idari tedbirlere karşı kanun yoluna ilişkin bir düzenlemeye yer verilmemiştir.

18. Öte yandan, 30/03/2005 tarihli ve 5326 sayılı Kabahatler Kanunu'nun 3.maddesini değiştiren 06/12/2006 tarihli, 5560 sayılı Kanun'un 31. maddesi şöyledir:

" (1) Bu Kanunun;

a) İdari yaptırım kararlarına karşı kanun yoluna ilişkin hükümleri, diğer kanunlarda aksine hüküm bulunmaması halinde,

b) Diğer genel hükümleri, idari para cezası veya mülkiyetin kamuya geçirilmesi yaptırımını gerektiren bütün fiiller hakkında,

uygulanır."

19. Anılan Kanun'un birinci maddesi şöyledir:

"Bu Kanunda; toplum düzenini, genel ahlâkı, genel sağlığı, çevreyi ve ekonomik düzeni korumak amacıyla;

a) Kabahatlere ilişkin genel ilkeler,

- b) Kabahatler karşılığında uygulanabilecek olan idari yaptırımların türleri ve sonuçları,
- c) Kabahatler dolayısıyla karar alma süreci,
- d) İdari yaptırıma ilişkin kararlara karşı kanun yolu,
- e) İdari yaptırım kararlarının yerine getirilmesine ilişkin esaslar,

Belirlenmiş ve çeşitli kabahatler tanımlanmıştır.”

20. Kanun'un ikinci kısmında yer alan 32. ila 43. maddelerinde, Türk Ceza Kanunu kapsamı dışında kalan çeşitli kabahatler sayılarak, bu eylemlere yaptırımlar öngörülmüştür.

21. Aynı Kanun'un 2. maddesinde, kabahat deyiminden, kanunun karşılığında idari yaptırım uygulanmasını öngördüğü haksızlığın anlaşılacağı; “Kanunilik İlkesi” başlıklı 4. maddesinin birinci fıkrasında; “Hangi fiillerin kabahat oluşturduğu, kanunda açıkça tanımlanabileceği gibi; kanunun kapsam ve koşulları bakımından belirlediği çerçeve hükmün içeriği, idarenin genel ve düzenleyici işlemleriyle de doldurulabilir.” hükmü, ikinci fıkrasında da “Kabahat karşılığı olan yaptırımların türü, süresi ve miktarı, ancak kanunla belirlenebilir.” hükmü yer almakta, böylece hangi fiillerin kabahat oluşturduğunun kanunda açıkça tanımlanabileceği hususunun yanı sıra, idarenin de genel ve düzenleyici işlemleriyle tanımlama yapabileceğinin belirtildiği, ayrıca işlenen bir kabahatin karşılığı olan yaptırımın türü, süresi, miktarının ancak kanun ile belirlenebileceğinin de ifade edilmiş olduğu; 16. maddesinde, kabahatler karşılığında uygulanacak olan idari yaptırımların idari para cezası ve idari tedbirlerden ibaret bulunduğu; idari tedbirlerin de mülkiyetin kamuya geçirilmesi ve ilgili kanunlarda yer alan diğer tedbirler olduğu belirtilmiştir.

22. Kanun'un “Başvuruyolu” başlıklı 27. maddesinin birinci fıkrası şöyledir:

“İdari para cezası ve mülkiyetin kamuya geçirilmesine ilişkin idari yaptırım kararına karşı, kararın tebliği veya tefhimi tarihinden itibaren en geç on beş gün içinde, sulh ceza mahkemesine başvurulabilir. Bu süre içinde başvurunun yapılmamış olması halinde idari yaptırım kararı kesinleşir.”

IV. İNCELEME VE GEREKÇE

A. İlk İnceleme

23. Uyuşmazlık Mahkemesinin Celal Mümtaz AKINCI'nın başkanlığında, Üyeler Şükrü BOZER, Mehmet AKSU, Birol SONER, Aydemir TUNÇ, Nurdane TOPUZ ve Ahmet ARSLAN'ın katılımlarıyla yapılan 05/07/2021 tarihli toplantısında; 2247 sayılı Kanun'un 27. maddesi uyarınca yapılan incelemeye göre, İdare Mahkemesince, anılan Kanun'un 19. maddesine göre başvuruda

bulunmuş olduğu, Mahkemece idari yargı dosyasının ekinde adli yargı dosyası ile birlikte Uyuşmazlık Mahkemesine gönderildiği ve usule ilişkin herhangi bir noksanlık bulunmadığı anlaşıldığından görev uyuşmazlığının esasının incelenmesine oy birliği ile karar verildi.

B. Esasın İncelenmesi

24. Raportör-Hâkim Gülten Fatma BÜYÜKEREN'in, davanın çözümünde adli yargının görevli olduğu yolundaki raporu ile dosyadaki belgeler okunduktan, ilgili Başsavcılarca görevlendirilen Yargıtay Cumhuriyet Savcısı Halil İbrahim ÇİFTÇİ ile Danıştay Savcısı Yakup BAL'ın adli yargının görevli olduğu yolundaki sözlü açıklamaları da dinlendikten sonra; gereği görüldüğü düşünülür:

25. Dava, 6698 sayılı Kanun uyarınca 03/03/2020 tarihli ve 2020/196 sayılı karar ile davacı adına verilen idari para cezasının iptali istemiyle açılmıştır.

26. Yukarıda izah edilen düzenlemelere göre; Kabahatler Kanunu'nun, idarî yaptırım kararlarına karşı kanun yoluna ilişkin hükümlerinin, diğer kanunlarda aksine hüküm bulunmaması halinde uygulanacağı; diğer kanunlarda görevli mahkemenin gösterilmesi durumunda ise uygulanmayacağı açıktır.

27. Görev kuralları kamu düzenine ilişkin olduğundan, görev konusunda taraflar için bir müktesep hak doğmayacağı; bu nedenle, yeni bir kanunla kabul edilen görev kurallarının, geçmişe de etkili olacağı, bilinen bir genel hukuk ilkesidir.

28. Davanın açıldığı andaki kurallara göre görevli olan mahkeme, yeni bir kanun ile görevsiz hale gelmiş ise, (davanın açıldığı anda görevli olan ve fakat yeni kanuna göre görevsiz hale gelen) mahkemenin görevsizlik kararı vermesi gerekeceği; ancak, yeni kanundaki görev kuralının, değişikliğin yürürlüğe girmesinden sonra açılacak davalarda uygulanacağına dair intikal hükümlerinin varlığı halinde, mahkemece görevsizlik kararı verilemeyeceği açıktır.

29. Diğer taraftan, dava görevsiz mahkemede açılmış, bu sırada yapılan bir kanun değişikliği ile görevsiz mahkeme o dava için görevli hale gelmiş ise, mahkemenin davaya bakmaya devam etmesi gerekir.

30. İncelenen uyuşmazlıkta, öngörülen idari para cezasının 5326 sayılı Kanun'un 16. maddesinde belirtilen idari yaptırım türlerinden biri olduğu, 6698 sayılı Kanun'da idari para cezasına itiraz konusunda görevli mahkemenin gösterilmediği anlaşılmıştır. Bu durumda, Kabahatler Kanunu'nun 5560 sayılı Kanun'la değişik 3. maddesinde bu Kanun'un, idari yaptırım kararlarına karşı kanun yoluna ilişkin hükümlerinin, diğer kanunlarda aksine hüküm bulunmaması halinde uygulanacağı belirtildiğinden, dava konusu idari para cezasına karşı açılan davanın görüm ve çözümünde, anılan

Kanun'un 27. maddesinin (1) numaralı bendi uyarınca adli yargı yerinin görevli olduđu sonucuna varılmıştır.

31. Yukarıda belirtilen hususlar göz önünde bulundurularak, Ankara 14. İdare Mahkemesince yapılan başvurunun kabulü ile, Ankara 5. Sulh Ceza Hâkimliğince verilen 28/12/2020 tarihli ve D.İş. No. 2020/3184 sayılı görevsizlik kararının kaldırılması gerekmiştir.

V. HÜKÜM

Açıklanan gerekçelerle;

A. Davanın çözümünde ADLİ YARGININ GÖREVLİ OLDUĞUNA,

B. Ankara 14. İdare Mahkemesince yapılan BAŞVURUNUN KABULÜ ile, Ankara 5. Sulh Ceza Hâkimliğince verilen 28/12/2020 tarihli ve D.İş No.2020/3184 sayılı GÖREVSİZLİK KARARININ KALDIRILMASINA,

05/07/2021 tarihinde, OY BİRLİĞİ İLE KESİN OLARAK karar verildi.

BÖLGE ADLİYE MAHKEMESİ KARARLARI

Bölüm İçeriği

- Ankara BAM 19. Hukuk Dairesi (E. 2019/3312)
- Ankara BAM 3. Hukuk Dairesi (E. 2017/388)
- Bursa BAM 6. Hukuk Dairesi (E. 2019/2251)
- Bursa BAM 9. Hukuk Dairesi (E. 2018/2576)
- İstanbul BAM 41. Hukuk Dairesi (E. 2020/1833)
- İstanbul BAM 43. Hukuk Dairesi (E. 2020/448)
- İstanbul BAM 21. Hukuk Dairesi (E. 2018/3160)
- İstanbul BAM 4. Hukuk Dairesi (E. 2017/1495)
- İstanbul BAM 23. Hukuk Dairesi (E. 2017/596)
- İzmir BAM 12. Hukuk Dairesi (E. 2019/2210)
- İzmir BAM 12. Hukuk Dairesi (E. 2019/2033)
- İzmir BAM 12. Hukuk Dairesi (E. 2019/1873)
- İzmir BAM 9. Hukuk Dairesi (E. 2018/2398)
- İzmir BAM 8. Hukuk Dairesi (E. 2018/2146)
- İzmir BAM 8. Hukuk Dairesi (E. 2018/1633)
- İzmir BAM 12. Hukuk Dairesi (E. 2017/499)
- İzmir BAM 12. Hukuk Dairesi (E. 2017/498)
- İzmir BAM 12. Hukuk Dairesi (E. 2016/59)
- Samsun BAM 4. Hukuk Dairesi (E. 2018/3525)
- Samsun BAM 4. Hukuk Dairesi (E. 2018/3158)
- Samsun BAM 4. Hukuk Dairesi (E. 2018/1643)

Ankara Bölge Adliye Mahkemesi, 19. HD., E. 2019/3312 K. 2020/1218 T. 24.6.2020

Esas No.: 2019/3312

Karar No.: 2020/1218

Karar Tarihi: 24.06.2020

KARAR

DAVANIN KONUSU: ŞİKAYET

Yukarıda tarih ve numarası yazılı mahkeme kararı aleyhine süresi içinde davalı borçlu vekili tarafından istinaf yoluna başvurulmuş olmakla, HMK'nın 353.maddesi gereğince dosya üzerinden yapılan inceleme neticesinde işin gereği görüşülüp düşünüldü:

Şikayetçi alacaklı mahkemeye sunduğu şikayet dilekçesinde; 28.11.2016 tarihinde borçlu Sulama Birliği üyelerinin yıl içerisinde Birliğe sulama ücreti, aidat vs.adı altında yaptıkları ödemeler üzerine 89/1 haciz ihbarnamesi gönderilerek haciz konulması amacıyla Birlik üyelerinin ad, soyad, kimlik bilgileri ve adreslerinin DSİ Ereğli İlçe Müdürlüğünden sorulması talebinde bulunduğunu, müdürlükçe talep tarihinden 5 ay 6 gün sonra Birlik üyelerinin 3.kişiler olduğu, icra müdürlüğünün 3.kişiler yönünden tespit ve araştırma yapma yükümlülüğü bulunmadığı ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu uyarınca bu kişilerle ilgili araştırma yapılmasının mümkün olmadığı, ilgili kişilerin araştırılarak tespiti ile icra müdürlüğüne bildirilmesi halinde 1.haciz ihbarnamesi gönderilebileceğinden bahisle bu talebin reddedildiğini, icra müdürlüğünün alacağın tahsiline yönelik işlemleri yönetmesi ve bunun için gerekli bilgileri toplama görevi olduğunu, şahıs olarak sözkonusu bilgilere ulaşmasının mümkün bulunmadığını belirterek müdürlüğün 04.05.2017 tarihli kararının kaldırılmasını ve talebi doğrultusunda işlem yapılmasına karar verilmesini talep etmiştir.

Davalı borçlu vekili cevap dilekçesinde; müdürlük kararının usul ve yasa uygun olduğunu, icra takibi yapılan üyelerin listesinin Ereğli icra müdürlüklerinden alınabileceğini, müvekkili kamu kurumu sıfatına haiz olduğundan icra müdürlüğünce böyle bir bilgi istenilmesi halinde ilgili Bakanlıktan istenmesinin uygun olacağı yönünde cevap verilebileceğini, şikayetçinin kötü niyetli olduğunu belirterek davanın reddine karar verilmesini istemiştir.

Mahkemece yapılan yargılama neticesinde; davacı alacaklının talebiyle ilgili 04/05/2017 tarihinde karar verildiği, davacı alacaklının dosyayı takip tarihi olan 22/12/2008 tarihinden itibaren vekili

olmaksızın takip etmesine ve işlem yapmasına rağmen karar tarihinden itibaren yedi günlük şikayet süresi içerisinde şikayet hakkını kullanmadığı, yasal sürenin sonunda şikayet hakkını kullanarak memur işlemini şikayet ettiği gerekçesiyle "Şikayet süresinde olmadığından REDDİNE, İcra takibinin DEVAMINA" karar verilmiştir.

Şikayetçi alacaklı vekili tarafından istinaf yoluna başvurulması üzerine Dairemizin 13.03.2019 tarih ve 2018/357 E - 2019/603 K. sayılı kararı ile şikayete konu icra müdürlüğü işlemi İİK.'nın 16/2.maddesine göre süreye tabi olmadığından şikayetçi tarafından ileri sürülen hususlar hakkında mahkemece gerekli delillerin toplanması ve sonrasında oluşacak sonuca göre bir karar verilmesi gerekirken şikayetin süre aşımı nedeniyle reddine karar verilmesinin usul ve yasaya uygun bulunmadığı gerekçesi ile esası incelenmeksizin ilk derece mahkemesi kararının kaldırılmasına ve davanın yeniden görülmek üzere dosyanın mahkemesine gönderilmesine karar verilmiştir.

Mahkemece yeniden yapılan yargılama neticesinde; şikayetçinin şikayete konu talebinin cebri icra işlemi niteliğinde olduğu, işbu talebinde müzekkere yazılacak yerleri de göstererek istenilen bilgilerin ne amaçla kullanılacağını da belirttiği, artık bu talebin Kişisel Verilerin Korunması Kanunu kapsamında düşünülemeyeceği, talebin icra müdürlüğünün cebri icra görevi dahilinde yapılması gereken bir işlem olduğu anlaşıldığından artık icra müdürlüğünün bu işlemi yerine getirmesi gerektiği, kaldı ki talebin icra dosyası tarafları ile hiçbir ilgisi olmadığı da söylenemeyeceği, borçlu Sol Sahil Sulama Birliği üye ve yetkililerinin 89/1 haciz ihbarnamesi gönderilebilecek kişilerden olduğu, diğer yandan şikayetçi tarafından kendi imkanları ile birliğin üye ve yetkililerin isimlerini ve adreslerini bulamayacağı, bu işlemin devlet organları eli ile yapılmasının icra dairelerinin görev kapsamına da uygun olduğu, icra müdürlüğünün taleple bağlılığının zorunlu olduğu ve devamında icra müdürlüğü işleminin sonucu hakkında bir itiraz yada şikayet olursa bunun da icra mahkemesince çözümlenebileceği anlaşıldığından şikayetçinin itirazlarının yerinde olduğu yönündeki gerekçe ile "Şikayetin KABULÜ ile; Ereğli İcra Müdürlüğünün 2010/1733 Esas sayılı dosyasından verilen 04/05/2017 tarihli 3. Kişiler yönünden tespit yapılması talebinin reddine ilişkin işlemin İPTALİNE" karar verilmiştir.

Davalı borçlu vekili istinaf dilekçesinde; davaya konu icra dosyası üzerinden müvekkili birlik üyelerinin ad, soyad ve TC kimlik numaralarının istenilmesine ilişkin talebin ret kararının hukuka uygun olduğunu, birlik üyelerine borçlu sıfatıyla işlem yapılamayacağını, birlik üyesi borçlu ise hakkında icra takibi yoluna başvurulması gerektiğini, 89/1 kapsamında 3.kişilere ihbarneme gönderilmesi için alacaklı tarafından dosya borçlusuna borcu olan/olabilecek olan kişilerin icra dairesine bildirilmesi gerektiğini, borcu olan kişileri bilip bildirecek olan alacaklının kendisi olup icra

dairesinin binlerce üyesi bulunan birliğin bütün üyelerini araştırma ve bilgilerine ulaşma yükümlülüğü altında olmadığını belirterek mahkeme kararının kaldırılmasını talep etmiştir.

Uyuşmazlık; icra müdürlüğü işleminin iptali istemine ilişkin şikayet niteliğindedir.

Takip dosyasının incelenmesinde; şikayetçi alacaklı tarafından davalı Sulama Birliği hakkında 22.12.2008 tarihinde ilamlı icra takibi başlatıldığı, alacaklı tarafından 25.11.2016 tarihinde icra dairesinden üyelerin Birliğe yaptıkları ödemeler üzerine birinci haciz ihbarnamesi ile haciz konulabilmesi için "Birlik üyelerinin ad, soyad, TC kimlik no ve adreslerinin gerek DSİ Ereğli İlçe Müdürlüğünden, gerekse borçlu birlikten istenmesi" yönünde talepte bulunulduğu, icra müdürlüğüne 04.05.2017 tarihinde"6698 Sayılı Kişisel Verilerin Korunması Kanunu gereğince 3. kişiler yönünden tespit yapılması talebinin reddine, alacaklı vekili tarafından ilgililerin bildirilmesi ve masrafın karşılanması durumunda bildirilen ilgililere talep gereği 1. haciz ihbarnamesi gönderilmesine"karar verildiği görülmüştür.

Dairemizce yapılan değerlendirmeler neticesinde; her ne kadar HGK'nun 31.03.2004 tarih 2004/12-202 E-196 K.sayılı kararında da belirtildiği üzere icra memurunun alacaklının alacağına kavuşması için gerekli olan takip işlemlerini yapması gerekmekte ise de; borçlu dışında kalan Birlik üyelerinin ad, soyad, TC kimlik no ve adreslerinin sorgulamasının ve araştırma yapılmasının icra dosyası ile ilgisi olmayan 3.kişiler yönünden uygulanmasının mümkün olmadığı, nüfus kaydı ve diğer sorgulama işlemlerinin hakkında takip kesinleşen borçlular yönünden uygulanacağı, 3.kişiler ile ilgili yapılacak sorgulamaların Anayasanın 20.Maddesinde düzenlenen temel hak ve hürriyetlere aykırılık oluşturduğu, kişisel verilerin gizliliğinin güvence altına alındığını, takip ile ilgisi bulunmayan borçlu durumunda olmayan kişilerin kişisel kimlik bilgileri ile durumlarının araştırılmasının icra müdürlüğünde görevli katip ve müdürlerin görevleri kapsamında bulunmadığı anlaşıldığından mahkemece şikayetin reddine karar verilmesi gerekirken yazılı gerekçe ile sonuca gidilmesinin isabetsiz olduğu anlaşıldığından davalı borçlu vekilinin istinaf talebinin esastan kabulüne karar vermek gerekmiş ve aşağıdaki hüküm kurulmuştur.

HÜKÜM: Yukarıda açıklanan sebeplerle;

Davalı borçlu vekilinin istinaf başvurusunun esastan KABULÜNE,

Ereğli (Konya) İcra Hukuk Mahkemesinin 19.06.2019 tarih ve 2019/101 E.- 2019/233 K.sayılı kararının KALDIRILMASINA,

Şikayetin REDDİNE,

İlk derece yargılaması açısından;

Alınması gereken 54,40 TL karar ve ilam harcından peşin alınan 31,40 TL harcın mahsubu ile bakiye 23,00 TL karar harcının şikayetçi alacaklıdan tahsili ile Hazineye gelir kaydına,

Yargılama giderlerinin şikayetçi alacaklı üzerinde bırakılmasına,

Davalı borçlu kendisini vekille temsil ettirdiğinden karar tarihinde yürürlükte bulunan A.A.Ü.T gereğince hesaplanan 1.130,00 TL vekalet ücretinin şikayetçi alacaklıdan alınarak davalı borçluya verilmesine,

Bakiye gider avansının karar kesinleştiğinde ve talep halinde yatırana iadesine,

İstinaf yargılaması açısından;

İstinaf başvuru harcı 121,30TL dışında alınan 44,40 TL harcın istek halinde davalı borçluya iadesine,

Davalı borçlu tarafından yapılan 121,30 TL harç, 53,00 TL posta gideri olmak üzere toplam 174,30 TL yargılama giderinin şikayetçi alacaklıdan alınarak davalı borçluya verilmesine,

İstinaf yargılamasında duruşma açılmadığından davalı alacaklıyararına istinaf vekalet ücreti verilmesine yer olmadığına,

Dair, İİK.nın 364, 366 ve 7035 Sayılı Kanununun 31.maddesi ile değişik HMK.nın 361/1 maddeleri gereğince 2 hafta içinde temyiz yolu açık olmak üzere dosya üzerinden yapılan inceleme sonucu 24.06.2020 tarihinde oybirliğiyle karar verildi.

Ankara BAM - 3. Hukuk Dairesi (E. 2017/388)

Biyometrik veri işleminin zorunlu tutulmasına ilişkin BAM kararı

Ankara Bölge Adliye Mahkemesi, 3. HD., E. 2017/388 K. 2017/401 T. 20.4.2017

Esas No.: 2017/388

Karar No.: 2017/401

Karar Tarihi: 20.04.2017

DAVA: Tüketicinin Açtığı Ayıplı Hizmetin Tespiti

Mahkemece yapılan yargılama sonucunda verilen karara karşı, süresinde istinaf kanun yoluna başvurulması üzerine dava dosyası incelendi, gereği görüşülüp düşünüldü.

TARAFLARIN İDDİA VE SAVUNMALARININ ÖZETİ:

Davacı vekili 24/05/2016 tarihli dava dilekçesiyle; taraflar arasında 10 yıl süreli ve 10.500-TL üyelik bedeli olan 31/05/2015 tarihli sözleşme imzalandığını, sözleşme başlangıç ve bitiş tarihlerinin 01/06/2015 ile 01/06/2025 olduğu, sözleşmede "üye, tesise üyelik kimlik kartını göstererek girer" hükmüne yer verildiğini, davalının giriş sistemini değiştirerek üyelere biyometrik el tanımlama işlemi yaparak giriş yaptırılmaya başladığını, müvekkilinin sözleşmede yazmayan, yeni getirilen sistemin güvenli ve korunaklı olduğunu öğrenmeden biyometrik el tarama izni vermediğini, sertifikasız bir sistemin kullanılmasında güvenlik zafiyetin doğabileceğini, hukuka aykırı ve suç amaçlı kullanılabileceği düşüncesiyle el izi vermekten kaçındığını, el tanıma sisteminin uluslararası güvenlik sertifikasının kendisine gösterilmesi halinde bu durumu kabul edeceğini, sözleşmede olmayan şartın sonradan dayatıl- lamayacağını sözlü olarak bildirdiğini, 02/05/2016 tarih ve 2016/0735 sayılı yazı ile tesis kurallarına uyulmadığı iddiasıyla sözleşmenin hukuka aykırı olarak feshedildiğini belirterek davalı tarafından yapılan feshin haksız olduğunun tespitini istemiştir.

Davalı vekili cevap dilekçesiyle; davacının, tarafların imzalamış olduğu 1045540 nolu üyelik sözleşmesi kapsamında müvekkilinin Bilkent/Ankara tesisinden yararlandığını, müvekkilinin 1995 yılından beri hizmet verdiğini, günün koşulları, güvenlik ve teknolojik gereksinimlerin zaman içinde değişim gösterdiğini, müvekkilinin amacının tüm üyelerin güven ve huzur içinde tesisini kullanmalarını sağlamak olduğunu, sistemin biyometrik değil, geometrik el tanıma sistemi olduğunu, kişinin el izi alınmadan elin 3 boyutlu şeklinin alındı- ğını ve koda çevrildiğini, parmak izi

ve avuç içi izi alınmadığını, sözleşmenin 6. maddesinde üyelerin kurallara uymakla yükümlü olduğunu, sistemin kullanılması yönünde davacının sözlü ve yazılı olarak uyarıldığını, sözleşmenin ilgili maddesi uyarınca sözleşmenin feshedildiğini belirterek davanın reddini istemiştir.

İLK DERECE MAHKEMESİ KARARI:

Mahkemece taraflar arasında yapılan sözleşmenin 6 ve 8. maddeleri ile geometrik el okuma isteminin davacı tüketicinin sözleşmeden doğan hak ve yükümlülüklerinde dürüstlük kurallarına aykırı düşecek biçimde tüketici aleyhine dengesizliğe neden olmadığı, sistemi kuran davalıya külfet getirdiği, üyenin sözleşmeden kaynaklanan yükümlülüklerini ihlal etmesi halinde sözleşmenin haklı nedenle feshedilebileceği, davalının sözleşmeyi haklı olarak bakiye aidatın ödenmesi sureti ile feshettiği, davacının davasında haksız olduğu gerekçesiyle davanın reddine karar verilmiştir.

İSTİNAF SEBEBİ:

Davacı vekili istinaf talebinde; davalının yaptığı eylemin tüketici kanununa aykırı olduğunu, 6502 Sayılı Kanununun 4/2. maddesine göre, sözleşme koşullarının sözleşme süresi içinde tüketici aleyhine değiştirilemeyeceğini, sözleşmede üyenin tesise üyelik kimlik kartını göstererek gireceğinin düzenlendiğini, müvekkilinin de bu şarta rıza göstererek sözleşmeyi imzaladığını, fakat sözleşme imzalandıktan sonra davalının spor tesisinin giriş sistemini değiştirdiğini, bilirkişi raporunda bu hususa değinilmediğini, raporun tarafsız olmadığını, bilgi güvenliğine ilişkin ISO 27001:2005 sertifikası dahi olmayan davalının, depo ettiği el şeklini güvenli bir şekilde sakladığına dair hiçbir geçerli sertifika sunmadığını, müvekkilinin kişisel verileri depolamaya ait güvenlik sertifikasının ibrazı halinde el izini vereceğini, aksi halde el izini vermeyeceğini, kimlik kartının yeterli olduğunu belirterek mahkeme kararının kaldırılarak davanın kabulüne karar verilmesini istemiştir.

GEREKÇE:

Dava dosyası kapsamı, mevcut kanıt durumu ve ileri sürülen istinaf sebepleri birlikte değerlendirildiğinde;

Davacı tüketici, davalı sağlayıcıya karşı açtığı dava ile aralarında 31/05/2015 tarih ve 1045540 nolu, 10 yıl süreli, 10.500-TL bedelli olarak yaptıkları Bilkent Fitness ve Spor Merkezi Üyelik Anlaşmasının, geometrik el tarama sistemine uygun davranmaması nedeniyle davalı tarafından 02/05/2016 tarihinde yapılan sözleşmenin feshinin haksız olduğunun tespiti istemiştir.

Mahkemece, davalının spor merkezinin geçiş kontrol noktasında kurduğu geometrik el tarama sisteminin el ya da avuç izi almaksızın, kişilerin el ve parmak karakteristiklerinin üç boyutlu olarak taranması ile şekilsel durumun matematiksel olarak test edilmesi sonucu onay vermesi ya da

vermemesi şeklinde gerçekleştiği, cihaz tarafından depolanan verinin HandKey II dışında bir yerde kullanılamayacağı, üyelere ait el ve parmak karakteristik taramalarının farklı yerlerde farklı amaçlarla kullanılma imkanının bulunmadığı, davalı tarafından kurulan sistemin 6698 Sayılı Kişisel Verilerin Korunması Kanununun tanımladığı şekilde geniş anlamda kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm verileri içerecek şekilde biyometrik kişisel veri kaydı yapmadığı tespit edilmiştir.

Davacının geometrik yöntemle kimlik doğrulamasına rıza göstermediği gerekçesiyle sözleşmenin 6/c ve 8/d maddelerine göre 06/04/2016 tarihli yazı ile uyarıldığı, 02/05/2016 tarihli yazı ile üyelik sözleşmesinin kalan üyelik süresine ilişkin bedel iade edilerek sözleşmenin davalı tarafından tek tarafı olarak feshedildiği, geometrik el okuma sisteminin davacının sözleşmeden doğan hak ve yükümlülüklerinde dürüstlük kurallarına aykırı düşecek şekilde tüketici aleyhine dengesizliğe neden olmadığı gibi sözleşmede öngörülen koşulların, sözleşme süresi içinde tüketici aleyhine değiştirilmesi anlamına da gelmediği, ortada davacının katlanması gereken bir külfet olmadığı, sözleşme hükümlerine göre davalının güvenlik tedbirleri alabileceği ayrıca Türkiye çapında 46.926, dava konusu Ankara-Bilkent tesisinde ise 12.000 aktif üyesi olduğu belirtilen spor merkezinde davalının, spor tesisinin giriş sisteminde üye ve yakınları haricinde, sahte üyelik kartı kullananların engellenmesi ve güvenlik amacı ile 01/03/2016 tarihinde değişiklik yaparak kimlik kartı uygulamasından daha gelişmiş el geometrisi okuma sistemine geçerek güvenlik tedbirleri almasında hukuka aykırılık bulunmadığı görülmekle, davalı tarafından sözleşmenin haklı nedenlerle feshedildiğine dair mahkeme kararında isabetsizlik yoktur.

Yukarıda açıklanan nedenlerle mahkeme kararının usul ve yasaya uygun olduğu anlaşıldığından davacının istinaf talebinin reddine karar vermek gerekmiştir.

HÜKÜM:

Gerekçesi ve ayrıntıları yukarıda açıklandığı üzere;

- 1-Davacının istinaf talebinin ESASTAN REDDİNE,
- 2-Davacı tüketici harçtan muaf olduğundan harç alınmasına yer olmadığına,
- 3-Davacıdan alınan 117,10-TL istinaf harcının isteği halinde davacıya iadesine,
- 4-Davacı tarafından yapılan istinaf yargılama giderlerinin üzerinde bırakılmasına,
- 5-Davalı tarafından istinaf gideri yapılmadığından karar verilmesine yer olmadığına,
- 6-Mahkememizce verilen kararın ilk derece mahkemesince taraflara tebliğine,

Dair verilen karar, HMK'nın 353/1-b-1 maddesi geređince, dava dosyası üzerinden yapılan inceleme sonucunda, kesin olmak üzere, 20/04/2017 tarihinde oybirliđi ile hüküm altına alındı.

Bursa BAM, 6. HD., E. 2019/2251 K. 2020/62 T. 8.1.2020

Esas No.: 2019/2251

Karar No.: 2020/62

Karar Tarihi: 8.1.2020

TÜRK MİLLETİ ADINA

İSTİNAF KARARI

DAVACI: F1 BANKASI TÜRK ANONİM ORTAKLIĞI

VEKİLİ: Av. K1

DAVALILAR: 1 -K2 - N1, 2 -K3 - N2

DAVANIN KONUSU: Şikayet (İcra Memur Muamelesi)

Yukarıdaki mahal esas ve karar numarası ayrıntılı olarak belirtilen İlk Derece Mahkeme kararının süresi içinde istinaf kanun yoluna başvurulmuş olmakla dosya mündericatına tüm bilgi ve belger okunup tetkik edildikten sonra heyetçe yapılan müzakere sonunda duruşma açılmasına gerek görülmeksizin gereği görüşülüp düşünüldü.

GEREĞİ DÜŞÜNÜLDÜ:

Davacı vekili 17/05/2019 tarihli dava dilekçesinde özetle; borçlular hakkında yürütülen icra takibi sırasında icra müdürlüğünden borçluların nüfus kayıt örneği çıkarılarak vefat eden anne babasından borçlulara intikal etmiş ya da edecek taşınır ve taşınmazların olup olmadığının sorgulanarak olduğu tespit edilirse bunlara haciz konulmasının talep edildiğini, icra müdürlüğünce talebin 14.05.2019 tarihinde reddedildiğini, bu ret kararının usul ve yasaya aykırı olduğunu belirtip, davanın kabulü ile icra müdürlüğünün 14.05.2019 tarihli işleminin iptalini talep ve dava etmiştir.

İlk Derece Mahkemesi Kararının Özeti : İlk derece mahkemesince yapılan yargılama neticesinde, "İİK.'nun 85 vd. maddeleri ile İİK.'nun 367. maddesine göre kural olarak icra müdürlüğünce haczi kabil olan borçluya ait mal ve haklarla ilgili bilgi toplanıp bunların haciz ve muhafazası yoluna

gidilebilir. Bunun dışındaki icra müdürlüğünün 3. kişilere ait mal ve haklarla ilgili borçluya ait olup devredilmiş de olsa bilgi ve belge toplamak gibi bir görevi mevcut değildir. Bu nedenlerle icra müdürlüğünün şikayete konu 14.05.2019 tarihli işlemi usul ve yasaya uygundur." gerekçesi ile şikayetin reddine karar verilmiştir.

İSTİNAF SEBEPLERİ : İlk derece mahkemesi kararına karşı, davacı alacaklı vekili tarafından yasal süresi içerisinde istinaf talebinde bulunulmuş olup, davacı kurum niteliği itibari ile harçtan muaftır.

Davacı alacaklı vekili istinaf dilekçesinde; Borçlunun anne babasının vefat edip etmemiş olduğunun başka yollardan tespitinin mümkün olmadığını, mevcut durumun mal kaçırmak kastı ile hareket eden borçluların, kötü niyetli davranışlarını desteklediğini, icra dairelerinin en temel görevinin alacaklının alacağına en kısa sürede ulaşmasını sağlamak olduğunu, bu nedenlerle ilk derece mahkemesi kararının hukuka aykırı olduğunu belirtmiştir.

DELİLLERİN DEĞERLENDİRİLMESİ ve GEREKÇE : Tüm dosya kapsamı uyarınca; Başvuru, takip borçlusunun miras bırakanlarının nüfus kayıtlarının sorgulanması ve mirasen intikal edecek mal varlıklarına haciz konulması talebinin reddi işleminin iptali istemine ilişkindir.

Konu ile ilgili mevzuat hükümleri incelendiğinde;

TC Anayasası madde 13: Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.

TC Anayasası madde 20/3: Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.

Avrupa İnsan Hakları Sözleşmesi madde 8: 1-Herkes, özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

2-Bu hakkın kullanımına, yasa/hukuk uyarınca olması ve ulusal güvenlik, kamu emniyeti ya da ülkenin ekonomik refahı, düzensizliğin ya da suçun önlenmesi, sağlığın ya da ahlakın korunması ya da başkalarının haklarının ve özgürlüklerinin korunması için demokratik toplumda gerekli olması hali istisna olmak üzere, bir kamu makamı tarafından bulunulmayacaktır.

Kişisel Verilerin Korunması Kanunu madde 3/1-d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

Madde 3/1-e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

Madde 5: 1- Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

2- Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

- a) Kanunlarda açıkça öngörülmesi.
- b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
- c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Madde 28: 1-Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:... d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi, düzenlemelerine rastlanmaktadır.

Yukarıda yer verilen mevzuat hükümlerine göre kişilerin nüfus kayıt ve mal varlığı bilgilerinin kişisel veri niteliğinde olduğu tartışmasızdır.

Somut olayda, icra dosyasının tarafı olmayan 3. Kişilere ait kişisel veri niteliğinde bulunan nüfus kayıtlarının icra müdürlüğüne sorgulanamayacağı, yargısal organlara tanınan istisnanın, ancak uyumsuzluğun tarafları açısından geçerli olabileceği, Anayasa'nın 20/3. maddesine göre aynı zamanda

temel haklardan olan kişisel verilerin korunmasını isteme hakkının, 6698 Sayılı Yasanın 28/1-d maddesinin geniş yorumlanması ile daraltılmayacağı açıktır.

Bu itibarla, şikayete konu 14/05/2019 tarihli memur işlemi hukuken isabetli olup, açıklanan nedenlerle şikayetin reddine karar verilmesi gerekir ki, ilk derece mahkemesinin kararı da bu cihettedir.

HMK'nun 355. Maddesi kapsamında dairemizce resen dikkate alınması gereken herhangi bir kamu düzenine aykırılık da bulunmamaktadır.

Dolayısı ile tarafımızca izah olunan bu gerekçelerle ilk derece mahkemesi kararının usul ve esas yönünden hukuka uygun olduğu anlaşıldığından, davacı tarafın istinaf başvurusunun HMK'nun 353/1-b-1 maddesi uyarınca esastan reddine oy birliği ile karar verilmiştir.

HÜKÜM : Gerekçesi yukarıda izah edildiği üzere;

- 1- Davacı tarafın istinaf başvurusunun HMK'nun 353/1-b-1 maddesi uyarınca ESASTAN REDDİNE
- 2- Davacı kurum niteliği itibariyle istinaf harçlarından muaf olduğundan başkaca harç alınmasına yer olmadığına,
- 3- Davacı tarafça yapılan istinaf yargılama giderlerinin davacı üzerinde bırakılmasına,
- 4- Dosyadaki gider avansından artan kısmın karar kesinleştiğinde ilk derece mahkemesince ilgisine iadesine,
- 5- Gerekçeli kararın taraflara tebliğine,

Dair yapılan inceleme sonunda İİK'nun 364. ve 7035 Sayılı Kanununun 31. Maddesi ile değişik HMK'nun 361/1 Maddeleri gereğince kararın taraflara tebliğinden itibaren 2 haftalık yasal süre içerisinde Yargıtay'a temyiz yolu açık olmak üzere oy birliği ile karar verildi. 08/01/2020

Bursa Bölge Adliye Mahkemesi, 9. HD., E. 2018/2576 K. 2019/643 T. 14.3.2019

Esas No.: 2018/2576

Karar No.: 2019/643

Karar Tarihi: 14.03.2019

TÜRK MİLLETİ ADINA

Bozüyük 1. Asliye Hukuk (İş) Mahkemesi'nin yukarıda esas ve karar numarası yazılı kararına karşı davalı tarafından istinaf yoluna başvurulduğundan dosya incelendi.

TARAFLARIN İDDİA VE SAVUNMALARININ ÖZETİ:

Davacı vekili dava dilekçesinde özetle; Davacının, Bozüyük Şube Müdürü olarak çalıştığını, iş akdinin 05/10/2016 tarihinde haksız bir şekilde feshedildiğini ileri sürerek belirterek feshin geçersizliği ile davacının işe iadesine karar verilmesini talep etmiştir.

Davalı vekili cevap dilekçesinde özetle; Davacının iş akdinin, 27/09/2016 tarihli Disiplin Kurulu kararı gereğince feshedildiğini, dava dilekçesinde ileri sürülen iddiaların tamamen asılsız ve gerçek dışı olduğunu belirterek davanın reddine karar verilmesini talep etmiştir.

İLK DERECE MAHKEMESİNİN KARARININ ÖZETİ:

"Davacı, davalı işyerinde şube müdürü olarak çalışmakta iken iş sözleşmesinin geçersiz nedenlerle feshedildiğini, disiplin kurulu kararının hiç tebliğ edilmediğini, disiplin kurulu kararından sonra 8 ay kadar daha çalıştığını bu nedenlerle işe iadesini dava ve talep etmiştir. Davalı, cevap dilekçesi ise iddiaları kabul etmemiş, 27/09/2016 tarihli disiplin kurulu kararı ile davacının iş akdinin feshedildiğini, davacının şube müdürü olması nedeni ile işe iade talep edemeyeceğini, feshin geçerli nedenlerle yapıldığını, davacının bankadaki gecikmeli kredi ödemeleri ve olumsuz istihbarat kayıtlarından haberdar olmasına rağmen müşteriye eşi üzerine kurulan firmalar aracılığı ile şube yetkisinde finansman sağlaması ve risk grubu tanımlamasını gerçekleştirmemesi nedeniyle feshin yapıldığını, iddiaların gerçeği yansıtmadığını bu nedenle davanın reddini talep etmiştir. İddia edilen riskli işlemlerin var olup olmadığının denetlenmesi amacı ile dosyanın bankacılık işlemleri konusunda uzman bir bilirkişiye tevdiine karar verilmiş, dosya bilirkişiye teslim edilmiştir. Bilirkişi ön rapor ile gerekli incelemenin yapılması için gerekli bilgi ve belgelerin teminini talep etmiş, bu kapsamda davalı bankaya iki kez müzekkere yazılmış ancak davalı banka tarafından bankacılık sırrı

kapsamında bilirkişi tarafından istenilen bilgi ve belgelerin sunulamayacağı belirtilmiştir. Bu kapsamda davalı tarafından istenilen bilgi ve belgelerin sunulamaması nedeni ile gerekli bilirkişi incelemesi yapılamamış ve davalı tarafça iş akdinin haklı nedenle feshedildiğinin ispatı sağlanamamıştır. Tüm bu hususlar birlikte incelenip değerlendirildiğinde davacının iş akdinin haklı nedenlerle feshi davalı tarafça ispatlanamadığı" gerekçesiyle davanın kabulü ile feshin geçersizliği ile davacının işe iadesine karar verilmiştir.

İLERİ SÜRÜLEN İSTİNAF NEDENLERİ:

Davalı vekili istinaf dilekçesinde özetle; HMK'nın 6. maddesi uyarınca, genel yetkili mahkemenin tüzel kişinin yerleşim yerinin (merkezinin) bulunduğu İstanbul İş Mahkemesi olduğunu, davacının, bankadaki gecikmeli kredi ödemeleri ve olumsuz istihbarat kayıtlarından haberdar olmasına rağmen bir takım müşterilere eşi üzerine kurulan firmalar aracılığı ile şube yetkisinde finansman sağladığı ve şube yetkisinde limit tahsis edilmesini sağlayabilmek amacıyla da risk grubu tanımlamasını gerçekleştirmediğinin tespiti üzerine Disiplin Kurulu kararı gereğince, • "Plasman yönetiminde ileride tehlikeli risk yaratabilecek nitelikte işlemler yapmak" eylemini düzenleyen "Ağır Kınamayı Gerektiren Haller/17 " hükmü uyarınca "Ağır Kınama" ile, • "Kullandırılan kredilerde tasfiyesi mümkün olmayacak şekilde önemli risk doğurucu yetki dışı işlem yapmak" eylemini düzenleyen "İş Akdinin Feshini Gerektiren Haller/37" hükmü uyarınca "İş Akdinin Feshi" ile , • "Kredi şartlarına, tahsis ve teminat koşullarına aykırı davranarak Bankayı zarara uğratmak" eylemini düzenleyen "İş Akdinin Feshini Gerektiren Haller/39" hükmü uyarınca "İş Akdinin Feshi" ile ve netice itibari ile İş Akdinin Feshi ile cezalandırılmasına" karar verildiğini, 4857 sayılı Kanun'un 17. ve 18. maddeleri uyarınca tüm yasal hakları ödenmek suretiyle geçerli ve hukuka uygun olarak iş akdinin feshedildiğini, işçinin davranışından ve yetersizliğinden kaynaklanan sözleşmesel yükümlülüğe aykırı davranış halinde iş sözleşmesinin feshinin 4857 sayılı Kanun'un 18/1.maddesine göre geçerli nedenle fesih olarak kabul edildiğini, davacının disiplin kurulu kararından haberdar olmadığına ve bu nedenle feshin geçersiz olduğuna ilişkin iddialarının tamamen gerçek dışı olduğunu, 05.10.2016 tarihli fesih bildiriminde fesih nedeni olan 176. disiplin kurulu kararının tarihinin sehven 09.02.2016 yazıldığını, 176. Disiplin Kurulu Kararının tarihinin 27.09.2016 olduğunu, dolayısı ile iş akdinin disiplin kurulu kararından 8 ay sonra feshedilmesi gibi bir durumun söz konusu olmadığını, davacının iş akdinin disiplin kurulu kararından 8 gün sonra feshedildiğini, soruşturma/teftiş ve disiplin süreçlerinin usullere uygun olarak yerine getirildiğini, bu süreç içerisinde davacının konudan haberdar edildiğini ve müfettişler tarafından davacının bilgisi dahilinde şubede inceleme ve soruşturma yapıldığını, yine bu süreçte kendisini yeterli savunma imkânının da tanındığını, nitekim

disiplin kurulu kararından sonra, iş akdinin feshinden önce davalı Banka tarafından 30.09.2016 tarihli yazı ile bir kere daha davacının savunmasının talep edildiğini, savunmasında teftiş kurulu soruşturmasından da disiplin kurulu kararından da haberdar olduğunu ve bu süreçte yazılı savunma yapmış olduğunu açık bir şekilde kabul ve beyan ettiğini, mobbing iddialarının yersiz olduğunu, kabul anlamına gelmemek kaydı ile 5 aylık işe başlatmama tazminatının fazla olduğunu, davacı tanığının tanıklığına itibar edilerek hüküm kurulmasının haksız ve hukuka aykırı olduğunu, tanığın davalı bankadan 2013 yılında ayrıldığını, işyerinden ayrılma tarihinden 3 yıl sonra gerçekleşen bir olay ile ilgili bilgi sahibi olabilmesinin ya da kendi bu kadar uzun zaman geçtikten sonra davacının o işyerindeki durumu ile ilgili bilgi görgü sahibi olabilmesinin söz konusu olamayacağını, bilirkişinin ön raporunda talep edilen bilgi ve belgelerin uyumsuzluk konusunu fazlasıyla aşar nitelikte olduğunu, bilirkişi ön raporunda talep edilen bilgi ve belgelerin ibrazının 5411 sayılı Bankacılık Kanunu'nda düzenlenen sır saklama yükümlülüğü dışında 6698 Kişisel Verilerin Korunması Kanunu uyarınca da Bankanın söz konusu bilgi ve belgeleri paylaşmak hususunda sınırlamalara tabi olduğunu, aksi takdirde idari ve adli cezalara maruz kalacağını, bu nedenle bilirkişi tarafından talep edilen belgelerin dosyaya sunulmadığını, 07/03/2018 tarihli duruşmada tesis edilen (2) numaralı ara karardan rücu edilmesinin talep edildiğini, mahkemece rücu talepleri ve bu konudaki beyanları dikkate alınmaksızın "...bilirkişi tarafından talep edilen bilgi ve belgelerin sunulmaması nedeniyle gerekli bilirkişi incelemesi yapılmadığı ve davalı müvekkil tarafından iş akdinin haklı nedenle feshedildiğinin ispatlanamadığı..." gerekçesi ile davanın kabulüne karar verilmesinin haksız ve hukuka aykırı olduğunu ileri sürmüştür.

İSTİNAF NEDENLERİNİN İNCELENMESİ VE GEREKÇE:

HMK'nın 341. maddesinde yer alan "istinaf başvuru dilekçesinde başvuru sebepleri ve gerekçesinin bildirilmesi", 355. maddesinde yer alan "incelemenin, istinaf dilekçesinde belirtilen sebeplerle sınırlı olarak yapılacağı ancak, bölge adliye mahkemesinin kamu düzenine aykırılık gördüğü takdirde bunu resen gözeteyeceği" ve 357. maddesinde yer alan "bölge adliye mahkemesince resen göz önünde tutulacaklar dışında, ilk derece mahkemesinde ileri sürülmeyen iddia ve savunmaların dinlenemeyeceği, yeni delillere dayanılamayacağı" ve "ilk derece mahkemesinde usulüne uygun olarak gösterildiği hâlde incelenmeden reddedilen veya mücbir bir sebeple gösterilmesine olanak bulunmayan delillerin bölge adliye mahkemesince incelenebileceği" hükümleri doğrultusunda istinaf başvuru dilekçesinde herhangi bir gerekçe içermeyen soyut ve yasanın amacına uygun olmayan sebepler nazara alınmaksızın gerekçeli olarak ileri sürülen istinaf sebepleri ile kamu düzenine ilişkin hususlar inceleme konusu yapılmıştır.

Feshin haklı veya geçerli nedene dayanıp dayanmadığı uyuşmazlık konusudur.

4857 sayılı İş Kanunu'nun 18. maddesi, "Otuz veya daha fazla işçi çalıştıran işyerlerinde en az altı aylık kıdemi olan işçinin belirsiz süreli iş sözleşmesini fesheden işveren, işçinin yeterliliğinden veya davranışlarından ya da işletmenin, işyerinin veya işin gereklerinden kaynaklanan geçerli bir sebebe dayanmak zorundadır." aynı Kanunun 19. maddesi ise, "İşveren fesih bildirimini yazılı olarak yapmak ve fesih sebebini açık ve kesin bir şekilde belirtmek zorundadır. Hakkındaki iddialara karşı savunmasını almadan bir işçinin belirsiz süreli iş sözleşmesi, o işçinin davranışı veya verimi ile ilgili nedenlerle feshedilemez. Ancak, işverenin 25. maddenin (II) numaralı bendi şartlarına uygun fesih hakkı saklıdır." hükümlerini içermektedir.

4857 sayılı İş Kanunu'nun 20/2 maddesinde açıkça, feshin geçerli nedenlere dayandığının ispat yükü davalı işverene verilmiştir. İşveren ispat yükünü yerine getirirken, öncelikle feshin biçimsel koşullarına uyduğunu, daha sonra, içerik yönünden fesih nedenlerinin geçerli (veya haklı) olduğunu kanıtlayacaktır. İşçi, feshin başka bir sebebe dayandığını iddia ettiği takdirde, bu iddiasını ispatla yükümlüdür.

Öte yandan işveren fesih bildirimindeki fesih nedeni ile bağlı olup sonradan bunu değiştiremeyeceği gibi başka bir nedene de dayanamaz.

1-Somut olayda davacının Bursa Yıldırım Şubesi işyerinde çalıştığı açıktır. Dava tarihi itibarıyla yürürlükteki 5521 sayılı Kanun'un 5. maddesine göre davanın çalışmanın geçtiği yer mahkemesinde açılması mümkün bulunduğundan davalı vekilinin yetkili mahkemeye yönelik istinaf nedeni yerinde bulunmamaktadır.

2-Davalı işverence 05/10/2016 tarihli fesih bildiriminde özetle,"...Şube müdürü olarak çalışmakta olduğunuz Bozüyük şubesi nezdinde bankamız müfettişlerince yapılan soruşturma sonucunda, bankamızdaki gecikmeli kredi ödemeleri ve olumsuz istihbarat kayıtlarından haberdar olmanıza karşın müşteriye eşi üzerine kurulan firmalar aracılığıyla şube yetkisinde finansman sağladığınız ve şube yetkisinde limit tahsis edilmesini sağlayabilmek amacıyla risk grubu tanımlamasını gerçekleştirmediğiniz tespit edilmiştir. Bu tespitlerle ilgili olarak tarafınızdan yazılı savunma istenmiş ve alınan savunmanız yetersiz bulunmuştur. Yukarıda açıklanan nedenlerle 09/02/2016 tarihinde düzenlenen 176. Disiplin Kurulu toplantısı kararı gereğince iş sözleşmenizin 4857 sayılı İş Kanunu'nun 17. ve 18. Maddeleri uyarınca 05/10/2016 tarihi itibarıyla feshedildiğini....." denilmek suretiyle iş akdinin feshedildiği, SGK'ya verilen ayrılış bildirgesinde işten ayrılış kodunun 26 "disiplin kurulu kararı ile fesih" olarak gösterildiği anlaşılmaktadır.

Davalı işveren, davacının iş akdini geçerli nedenle feshettiğini savunmuş ise de; bu iddiasını somut veriler ve deliller ile kanıtlamış değildir. Davalının yukarıda açıklanan ilkeler doğrultusunda feshin geçerli nedene dayanıp dayanmadığının denetimi için gerekli görülen belgeleri 2 kez istenilmesine rağmen ibraz etmediği de açıktır. Fesih gerekçesi yapılan iddiaların varlığının denetlenmesi amacı ile dayanak belgelerin celbi isteği davalı tarafça mesleki sır olduğu gerekçesiyle sunulmamış olup bu durumda feshin geçerli nedene dayandığını ispat yükümlülüğü üzerinde bulunan davalı işverenin bunu yerine getirmemesi karşısında mahkemece verilen kararda isabetsizlik bulunmamıştır.

Sonuç olarak; dosya kapsamına, mevcut delil durumuna ve yukarıda belirtilen ölçütlere göre yapılan inceleme sonucunda ilk derece mahkemesinin vakıa ve hukuki değerlendirmesinde usul ve esas yönünden yasaya aykırılık bulunmadığı anlaşıldığından yerinde görülmeyen istinaf başvurusunun esastan reddine karar verilmesi gerekmiştir.

HÜKÜM: Yukarıda açıklanan nedenlerle;

Davalının istinaf başvurusunun HMK 353/1-b-1 maddesi gereğince ESASTAN REDDİNE,

Alınması gerekli istinaf karar harcı 44,40 TL olduğundan, davalı tarafından yatırılan 35,90 TL harcın mahsubu ile bakiye 8,50 TL istinaf karar harcının davalıdan tahsili ile Hazineye irat kaydına,

Davalının yaptığı istinaf yargılama masraflarının kendi üzerinde bırakılmasına,

HMK 333. maddesi uyarınca artan gider avanslarının yatırana iadesine,

Kararın tebliği ile harç ve gider avansı iadesine ilişkin işlemlerin ilk derece mahkemesi tarafından yerine getirilmesine,

Dosya üzerinde yapılan inceleme sonucu 7036 sayılı Kanun'un 8/1-a maddesi gereğince KESİN olmak üzere 14/03/2019 tarihinde oybirliği ile karar verildi.

İstanbul Bölge Adliye Mahkemesi, 41. HD., E. 2020/1833 K. 2020/1649 T. 26.11.2020

Esas No.: 2020/1833

Karar No.: 2020/1649

Karar Tarihi: 26.11.2020

TÜRK MİLLETİ ADINA

İSTİNAF KARARI

DAVANIN KONUSU: Tespit (İşe İade İstemli)

Lüleburgaz'ın Mahkemesi' nin 07/05/2020 tarih ve 2019/404 Esas- 2020/179 Karar sayılı kararına karşı istinaf kanun yoluna başvurulması üzerine dosyanın dairemize tevzi edildiği anlaşılmakla, dosya ve ekleri incelendi.

TALEP:

Davacı vekili dava dilekçesinde özetle; davacının 10.11.2004 - 04.10.2019 tarihleri arasında son 11 yılı mağaza sorumlusu olarak 15 yıl sürekli çalıştığını, 04.10.2019 Cuma günü bölge sorumluları K1 ve K2'ın çalıştığı işyerine gelerek "şirket seni işten çıkardı, üzerinde zimmetli olan şirkete ait malzemeleri ve kasayı sayıp teslim et sonra işyerinden ayrıl git " demeleri üzerine gerekeni yapıp işyerinden ayrıldığını, 05.10.2019 günü hastalık raporu aldığını, 06.10.2019 Pazar günü sabahı yazılı fesih yapılmadığından işyerine gittiğinde de görevlilerce "Merkez senin işten çıkarıldığını, işyerine sokulmamanı söyledi kusura bakma içeri alamayız" diyerek işe almadıklarını, feshin sebeplerinin yazılı olarak belirtilemediğini, sözlü bildirim ile işten çıkartıldığını, müvekkilinin 6 aydan fazla kıdemi olduğunu, işverenin de ülke çapında çok azla çalışanın olduğunu, müvekkilinin İş Kanununun 18. ve devamı maddelere göre işe iade davası açma hakkının bulunduğunu, en son aylık brüt ücretinin 5.300,00 TL olup, her ay 210,00 TL yemek parası, 210,00 TL servis yardımı, 530,00 TL performans primi ve 100,00 TL kasa tazminatı ödendiğini beyanla; boşta geçen süre ücret ve diğer hakları alacağı, işe başlatamama tazminatı talep etmektedir.

SAVUNMA:

Davalı vekili cevap dilekçesinde özetle; davacının müvekkili şirkete ait işyerlerinde mağaza sorumlusu olarak 10.11.2004 tarihinden iş akdinin haklı olarak feshedildiği 04.10.2019 tarihine kadar

son aylık brüt 4.249,00 TL maaşla çalıştığını, davacının mağazanın yetkili amiri olarak çalışmakta iken X1 mesajlaşma grubunda, bölge sorumlusu K1'i istediği gibi yönlendiremediğini, bölge sorumlusu K1'den memnun olmadığını dile getirerek diğer çalışanları da amiri K1'e karşı örgütlemeye çalıştığını, birlikte hareket etmeleri halinde K1'i sıkıştıracaklarını vb beyanlarla çalışanların iradelerini etkilemeye çalıştığını, diğer çalışanları K1'e karşı kışkırttığını, davacının eylemlerinden dolayı kendisinden savunma talep edildiğini, davacının kendi el yazısı ile savunmasını yazarak amiri K1'e teslim ettiğini, davacının işyeri çalışanlarını işverene karşı kışkırtarak işyeri düzenini ortadan kaldırmayı hedeflediğini, kabul anlamına gelmemek üzere eylemlerinin haklı nedenle fesih olarak değerlendirilemese dahi geçerli nedenle fesih gerekçesini oluşturduğunu, iş akdinin eylemlerinden dolayı Beyoğlu 30. Noterliğinin 04.10.2019 tarih ve 12230 yevmiye nolu ihtarnamesi ile haklı olarak feshedildiğini beyanla davanın reddini talep etmektedir.

İLK DERECE MAHKEMESİ KARARI:

"1-Davanın REDDİNE,

2-Gider avansından artan kısmın karar kesinleştikten sonra ilgisine iadesine,..." şeklinde karar verilmiştir.

İSTİNAF SEBEPLERİ:

İlk Derece Mahkemesi'nce yazılan gerekçeli karar, taraflara usulüne uygun tebliğ edilmiştir.

İstinaf Kanun Yoluna yasal süresinde davacı ve davalı tarafından müracaat edilmiştir.

Davacı vekili gerekçeli istinaf dilekçesinde özetle; mobingten kıdeminden öncekilerle sorun yaşamadığını, yönetici K1'in kendisine karşı onur kırıcı ve sert davrandığını, davacının bu durumdan bunaldığını ve bu sebeple gece arkadaşlarına söz konusu mesajları attığını, mesajlarda hakaret etmediğini, davanın kabulüne kara verilmesi gerektiğini belirterek istinaf yasa yoluna başvurmuştur.

Davalı vekili gerekçeli istinaf dilekçesinde özetle; yerel mahkemenin davayı red gerekçesiyle dayanak kanun maddesiyle çelişkili olup dava konusu eylemleri geçerli neden saymasının usul ve yasaya aykırı olduğunu, izah edilmeye çalışılan nedenlerle ve cevap dilekçesinde detaylı şekilde anlattığı üzere işçinin arkadaşlarını çalışmama konusunda kışkırtması ve işverene karşı yapmış olduğu örgütlenme planları iş akdinin feshi için geçerli neden değil haklı neden teşkil ettiğini, geçerli nedenle fesih sebebi olduğunu belirterek istinaf yasa yoluna başvurmuştur.

DELİLLERİN DEĞERLENDİRİLMESİ VE GEREKÇE:

6100 sayılı Hukuk Muhakemeleri Kanununun 341 ve devamı maddeleri uyarınca ve özellikle istinaf incelemesinin kapsamının öngörüldüğü 355. maddeye göre re'sen gözetilecek kamu düzenine aykırılık halleri dışında istinaf incelemesi istinaf dilekçesinde belirtilen sebeplerle sınırlı olarak yapılır.

4857 sayılı yasanın 18 ve 20. maddelerinde düzenlenen işe iade davasının ön koşulları yönünden bir eksikliğin bulunmadığı anlaşılmıştır.

İş sözleşmesinin, işçinin doğruluk ve bağlılığa aykırı davranışları sebebiyle işverence haklı olarak feshedilip feshedilmediği noktasında taraflar arasında uyuşmazlık söz konusudur.

4857 sayılı İş Kanunu'nun 25 inci maddesinin (II) numaralı bendinde, ahlâk ve iyi niyet kurallarına uymayan haller sıralanmış ve belirtilen durumlar ile benzerlerinin varlığı halinde, işverenin iş sözleşmesini haklı fesih imkânının olduğu açıklanmıştır. Yasadaki haller sınırlı sayıda olmayıp, genel olarak işçinin sadakat borcuna aykırılık oluşturan söz ve davranışları işverene fesih imkânı tanımaktadır.

24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Amaç" kenar başlıklı 1. maddesinin ilgili kısmı şöyledir:

"Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir."

6698 sayılı Kanun'un "Kapsam" kenar başlıklı 2. maddesi şöyledir:

"Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır."

6698 sayılı Kanun'un "Tanımlar" kenar başlıklı 3. maddesinin ilgili kısmı şöyledir:

" (1) Bu Kanunun uygulanmasında;

a) Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,...

d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması,

devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,"

6698 sayılı Kanun'un "Kişisel verilerin işleme şartları" kenar başlıklı 5. maddesi şöyledir:

" (1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması."

6698 sayılı Kanun'un "Veri sorumlusunun aydınlatma yükümlülüğü" kenar başlıklı 10. maddesi şöyledir:

"(1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere;

a) Veri sorumlusunun ve varsa temsilcisinin kimliği,

b) Kişisel verilerin hangi amaçla işleneceği,

c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabilceği,

ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,

d) 11 inci maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür."

6698 sayılı Kanun'un "İlgili kişinin hakları" kenar başlıklı 11. maddesi şöyledir:

"(1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

- a) Kişisel veri işlenip işlenmediğini öğrenme,
- b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- c) Kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
- e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
- f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir."

Avrupa İnsan Hakları Mahkemesi (AİHM) içtihatlarında özel hayatın eksiksiz bir tanımı bulunmayan geniş bir kavram olduğunu belirtmektedir. Özel hayata saygı hakkı alt kategorisinde geçen özel hayat kavramı AİHM tarafından oldukça geniş yorumlanmakta ve bu kavrama ilişkin tüketici bir tanım yapılmaktan özellikle kaçınılmaktadır (Koch/Almanya, B. No: 497/09, 19/7/2012, § 51). Bununla birlikte Sözleşme'nin denetim organlarının içtihatlarında bireyin kişiliğini serbestçe geliştirmesi ve gerçekleştirilmesi ile kişisel bağımsızlık kavramlarının özel hayata saygı hakkının kapsamının belirlenmesinde temel alındığı anlaşılmaktadır (Sidabras ve Džiautas/Litvanya, B. No: 55480/00, 59330/00, 27/7/2004, § 43; K.A. ve A.D./Belçika, B. No: 42758/98, 45558/99, 17/2/2005, § 83; Pretty/Birleşik Krallık, B. No: 2346/02, 29/4/2002, § 61; Christine Goodwin/Birleşik Krallık [BD], B. No: 28957/95, 11/7/2002, § 90). AİHM'e göre mesleki hayat özel hayat kavramı dışında tutulamaz. Özel hayat unsurları gerekçe gösterilerek mesleki hayata getirilen sınırlamalar, bireyin sosyal kimliğini etkilediği ölçüde Sözleşme'nin 8. maddesi kapsamına girebilmektedir. AİHM bireylerin genellikle iş yaşamında dış dünyayla ilişkiler kurduğunu hatırlatarak bireyin kimliğini oluşturmasının ve sosyalleşmesinin önemli bir aracı olan dış dünyayla ilişki kurma hakkının bireyin iş çevresini de kapsadığını, bu durumun serbest meslek bağlamında özellikle geçerli olduğunu ifade etmiştir (Niemitz/Almanya, B. No: 137/1088, 16/12/1992, § 29; Özpınar/Türkiye, B. No: 20999/04, 19/10/2010, § 45; Campagnano/İtalya, B. No: 77955/01, 23/3/2006, § 53). Sözleşme'nin 8. maddesinde geçen yazışma

teriminin mektup gibi geleneksel iletişim araçları yanında telefon, faks ve e-posta gibi yeni teknolojik araçlarla yapılan iletişimi de kapsadığını, özel hayata saygı hakkı ve bu hakkın bir görünümü olan haberleşme hürriyetinin işyerindeki iletişim bakımından da uygulanabilir nitelikte olduğunu tespit eden AİHM, özel hukuk iş ilişkilerinde Sözleşme'nin 8-11. maddelerinin ihlal edildiği iddiasıyla önüne gelen davalarda devletin pozitif yükümlülükleri bağlamında inceleme yapmakta ve anılan hakların ulusal mahkemelerce yeterli derecede korunup korunmadığını irdelemektedir (Palomo Sanchez ve diğerleri/İspanya [BD], B. No: 28955/06..., 12/9/2011, § 61, Bărbulescu/Romanya [BD], B. No: 61496/08, 5/9/2017, §§ 69-81).

Anayasa'nın 20. maddesinin üçüncü fıkrasının birinci cümlesinde genel olarak herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu belirtilmiş, ikinci cümlesinde kişisel veriler bağlamında bazı özel güvenceler sayılmış, üçüncü cümlesinde kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği düzenlenmiş, dördüncü cümlesinde ise kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hüküm altına alınmıştır. Buna göre lafzı dikkate alındığında Anayasa'nın 20. maddesinin üçüncü fıkrasının kişisel verilerin korunmasını isteme hakkı kapsamında sadece işleme şeklindeki sınırlama ya da müdahalelere karşı değil kişisel verilere yönelik her türlü müdahale ve sınırlamalara karşı güvence getirdiği anlaşılmaktadır.

Anayasa'nın "Haberleşme hürriyeti" kenar başlıklı 22. maddesi şöyledir:

"Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.

İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir."

Yukarıda belirtilen hususlar gözetilerek işverenin işçinin iletişimini denetlemesi yetkisini kişisel verilerin korunmasını isteme hakkı ve haberleşme hürriyeti bağlamında devletin pozitif yükümlülükleri kapsamında irdelemek gerekmektedir. Öncelikle somut olayda olduğu gibi teknolojik gelişmelerin imkânlarından yararlanmak isteyen işverenlerin bilgisayar, internet, e-posta

gibi iletişim araç ve gereçlerini çalışanın kullanıma sunması nedeniyle oluşan uyuşmazlıklarda işverenin menfaatleri ile işçinin temel hak ve özgürlükleri arasında bir dengeleme yapma gerekliliği doğmaktadır. Bu bağlamda işveren ile çalışan arasındaki ilişkinin iki taraf açısından da belirli hak ve yükümlülükler öngören ve esasen güven ilişkisi üzerine kurulu iş sözleşmesiyle şekillendiği unutulmamalıdır. Somut uyuşmazlığın ilgili olduğu iş hukukunun dinamik bir niteliğinin olduğu, ayrıca iş ilişkilerinin genel kurallardan farklı, kendine özgü bazı hukuki kurallar içerdiği de dikkate alınmalıdır. Bu bağlamda işlerin etkin bir şekilde yürütülmesi ile bilgi akışının kontrolünü sağlamak, işçinin eylemlerine bağlı cezai ve hukuki sorumluluğa karşı korunmak, verimliliği ölçmek veya güvenlik endişeleri gibi haklı ve meşru görülebilecek nedenlerle işverenin yönetim yetkisi kapsamında kural olarak işçinin kullanımına sunduğu iletişim araçlarını denetleyebileceği ve kullanıma ilişkin sınırlamalar öngörebileceği söylenebilir. Ancak işverenin yönetim yetkisinin işyerinde işin yürütülmesi, işyerinin düzeninin ve güvenliğinin sağlanmasıyla sınırlı olduğu unutulmamalıdır. Bu bağlamda işverenin yetki ve haklarının sınırsız olmadığı, çalışana tanınan temel hak ve özgürlüklerin somut olayda haberleşme hürriyeti ve kişisel verilerin korunmasını isteme hakkının işyeri sınırları dâhilinde de korunduğu, aynı zamanda kısıtlayıcı ve uyulması zorunlu işyeri kurallarının çalışanların temel haklarının özünü zedeleyecek nitelikte olmaması gerektiği vurgulanmalıdır. Bu çerçevede işyerinde kullanıma sunulan iletişim araçlarının işverene ait olduğu gözetilerek sırf bu nedenle bile işverenin iletişim araçları üzerinde sınırsız ve mutlak bir gözetleme ve denetleme yetkisinin olduğunu kabul etmek, işçinin demokratik bir toplumda temel hak ve özgürlüklerine işyerinde de saygı gösterilmesi gerektiği yönündeki haklı beklentisiyle uyuşmayacaktır. Demokratik bir toplumda iletişimin denetlenmesi ve kişisel verilerin işlenmesi süreci şeffaf bir şekilde gerçekleştirilmeli ve bunun bir gereği olarak da süreçle ilgili olarak çalışanlar işveren tarafından önceden bilgilendirilmelidir. Uluslararası hukuk ve karşılaştırmalı hukuk dikkate alındığında bu bilgilendirmenin -somut olayın özelliklerine uygun düştüğü ölçüde- en azından iletişimin denetlenmesi ile kişisel verilerin işlenmesinin hukuki dayanağı ve amaçları, denetlemenin ve veri işlemenin kapsamı, verilerin saklanacağı süre, veri sahibinin hakları, denetlemenin ve işlemenin sonuçları ile verilerin muhtemel yararlanıcıları hususlarını kapsamaması gerekir. Ayrıca bildirimde iletişim araçlarının kullanımına ilişkin olarak işveren tarafından öngörülen sınırlamalara da yer verilmelidir. Bilgilendirmenin mutlaka belli şekilde yapılması şart olmayıp şeffaflığı sağlamak bakımından bireylere, kişisel verilerin işlenmesine ve iletişimin denetlenmesine ilişkin süreçten yukarıda belirtilen kapsamda haberdar olma imkânı sağlayan uygun bir yöntem tercih edilebilir.

Somut olayda; davacının iş sözleşmesinin haklı nedenle feshedildiği iddia edilmiş olup, bu hususta whatsapp konuşmalarının feshe dayanak yapıldığı görülmüştür. Söz konusu whatsapp grubunun

işçiler tarafından kurulan bir grup olduğu ve işçilerin burada iletişimde bulunmalarının kişisel veri olarak değerlendirilmesi gerektiği, söz konusu görüşme içeriklerinin kullanılacağına işveren tarafından işçilere bildirilmediği, görüşme içeriklerine bakıldığında işçiler tarafından iş dışında da iletişime geçilen özel bir grup olduğu ve konuşmaların gizli kalması gerektiği, işveren tarafından bu gizli kalması gereken verilerin yasak bir şekilde elde edilmesi ve bu konuşmaların dayanak yapılarak iş sözleşmesinin feshedilmesinin geçersiz nedene dayandığı anlaşılmış, ayrıca feshe dayanak yapılan eylemlerin de eleştiri ve hak savunma noktasında olduğu görülmüş davalı vekilinin istinaf sebepleri reddine karar verilmiş, davacının istinafının kabulü ile davacı işçinin işe iadesine, işçinin kıdemi dikkate alınarak işe başlatmama tazminatının 5 ay olarak belirlenmesinin ve 4 aylık boşta geçen süre ücretine hükmedilmesi gerektiği anlaşılmıştır. Dosyada bulunan 25/12/2019 tarihli bilirkişi raporunun 1. seçenek üzerinden göre hesaplamaya göre giydirilmiş ve çıplak brüt ücret tespit edilmiştir. Buna göre çıplak brüt ücretin 4.249,00 TL giydirilmiş brüt ücretin 5.122,10 TL olduğu görülmüştür. Davalının istinaf başvurusunun yerinde olmadığı görüldüğünden istinaf başvurusunun esastan reddine karar verilmiştir.

Yukarıda açıklanan nedenlerle davacı vekilinin istinaf başvurularının yerinde olduğu, mahkeme kararının usul ve yasaya aykırı olduğu ancak delillerin toplanmış olmasına göre karardaki hata ve eksikliklerin yerel mahkemesine gönderilmeksizin dosya üzerinden ve yukarıda yapılan açıklamalar doğrultusunda HMK'nun 353/1-b/2.bendi uyarınca Dairemizce değerlendirilebileceği sonucuna varıldığından yeniden hüküm kurulmasının doğru olacağına dair aşağıdaki hüküm tesis edilmiştir.

KARAR: Gerekçesi Yukarıda İzah Edildiği Üzere;

1- Davalının istinaf başvurusunun HMK 353/1-b-1 maddesi gereğince ESASTAN REDDİNE,

2- Davacı istinaf itirazının yerinde olduğu, buna göre ilk derece mahkemesince verilen kararın kısmen usul ve yasaya aykırı olduğu, lakin dosyada delillerin toplanmış olmasına göre karardaki hata ve eksikliklerin yerel mahkemesine gönderilmeksizin dosya üzerinden Dairemizce değerlendirilip yeniden hüküm kurulabileceği anlaşıldığından, HMK 'nun 353/1-b.2 maddesi uyarınca İlk Derece Mahkemesinin kararının KALDIRILMASINA,

A) Davanın KABULÜNE,

-Feshin GEÇERSİZLİĞİ ile ve davacının İŞE İADESİNE,

-Davacının yasal süre içerisinde başvurusuna rağmen davalı işverence süre içerisinde işe başlatılmaması halinde ödenmesi gereken tazminat miktarının davacının kıdemi, fesih nedeni

dikkate alınarak takdiren 5 aylık brüt ücreti tutarı olan brüt 21.245,00 TL tutarında tazminatın davalıdan alınarak davacıya ödenmesi gerektiğinin TESPİTİNE,

-Davacı işçinin işe iadesi için işverene süresi içinde müracatı halinde hak kazanılacak olan ve kararın kesinleşmesine kadar en çok 4 aya kadar ücret ve diğer hakları olan brüt 20.488,40 TL tutarında tazminatın davalıdan alınarak davacıya ödenmesi gerektiğinin TESPİTİNE,

-Davacı işçinin süresi içerisinde işe başlatılması durumunda varsa bu alaktan peşin ödenen kıdem ve ihbar tazminatının MAHSUBUNA,

B) İlk derece yargılaması yönünden alınması gereken 54,40 TL karar ve ilam harcından peşin olarak alınan 44,40 TL'nin mahsubu ile 10,00 TL harcın davalıdan alınarak Hazineye irad kaydına,

C) Davacı tarafça ilk derece yargılaması sırasında yapılan 88,80 TL harç ve 300,15 TL posta gideri, 450,00 TL bilirkişi olmak üzere toplam 838,95 TL'nin davalıdan alınarak davacıya verilmesine,

D) Davacı ilk derece yargılamasında vekille temsil edildiğinden karar tarihinde yürürlükte bulunan A.A.Ü.T. gereğince belirlenen 4.080,00 TL vekalet ücretinin davalıdan alınarak davacıya verilmesine,

E) Harcanmayan gider avanslarının karar kesinleştiğinde ve talepleri halinde ilgisine iadesine,

3- Davacıdan peşin olarak alınan istinaf karar harcının talebi halinde davacıya iadesine,

4- Davalıdan alınması gereken istinaf karar harcı peşin olarak alındığından tekrar harç alınmasına yer olmadığına,

5- Davacı tarafından istinaf yargılama gideri olarak yapılan 148,60 TL başvuru harcı, 71,50 TL posta gideri olmak üzere toplam 220,10 TL'nin davalıdan alınarak davacıya verilmesine,

6- Davalı tarafından yapılan istinaf yargılama giderlerinin kendisi üzerinde bırakılmasına,

7- İstinaf incelemesi duruşmasız yapıldığından taraflar lehine istinaf vekalet ücreti taktirine yer olmadığına,

8- Karar tebliği ve harç tahsil müzekkeresi yazılması işlemlerinin ilk derece mahkemesi tarafından yapılmasına,

Dair, dosya üzerinden yapılan inceleme sonucunda, 7036 Sayılı Kanun'un 9. maddesi atfıyla 6100 Sayılı HMK'nın 362/1-a maddesi uyarınca KESİN olmak üzere 26/11/2020 tarihinde oybirliğiyle karar verildi.

İstanbul Bölge Adliye Mahkemesi, 43. HD, E. 2020/448 K. 2021/1394 T. 18.11.2021

Esas No.: 2020/448

Karar No.: 2021/1394

Karar Tarihi: 18.11.2021

MAHKEMESİ: İSTANBUL 15. ASLİYE TİCARET MAHKEMESİ

TARİHİ: 25/01/2019

NUMARASI: 2016/227 Esas - 2019/36 Karar

DAVA: Alacak (Bankacılık İşlemlerinden Kaynaklanan)

İSTİNAF KARAR TARİHİ: 18/11/2021

Taraflar arasında görülen dava neticesinde ilk derece mahkemesince verilen hükmün Davacı vekilince istinaf edilmesi üzerine düzenlenen rapor ve dosya kapsamı incelenip gereği görüşülüp düşünüldü;

TARAFLARIN İDDİA VE SAVUNMALARININ ÖZETİ

DAVA: Davacı vekili dava dilekçesinde özetle; müvekkili ...'in, 30/08/1971 tarihinden bu yana Birleşik Krallıkta ikamet etmekte ve 23/04/1986 yılından bu yana da Birleşik Krallıkta süresiz ve sınırsız oturma iznine sahip olduğunu, Birleşik Krallık'ta yaşadığı süre boyunca ticari alandaki yüksek başarısı sayesinde "Kraliyet Ticaret Sicili"ne kayıtlı ... Ltd. Şti şirketini kurduğunu, halen de işbu şirketin tek ortağı ve yöneticisi konumunda bulunduğunu, Türkiye'ye vaki ziyaretlerinde ailesine ait konutlarda misafir kalmakta olduğunu, müvekkilinin aynı zamanda ... A.Ş.'nin de 13 yıldan bu yana 9123 müşteri numaralı müşterisi olduğunu, müvekkilinin davalı banka nezdinde bulunan hesapları müvekkilinin yurt içerisinde herhangi bir ticari faaliyeti, kazancı, adına kayıtlı gayrimenkulü veya sürekli kaldığı bir ikametgahı bulunmadığı için yurtdışında mukim gerçek kişilere özgü bir banka hesabı açılması gerekirken bu hesapların davalı bankanın ve çalışanlarının hatası eğitimsizliği nedenine bağlı olarak "Yurtiçinde Yerleşik Gerçek Kişi" olarak açıldığını, ardından yine davalı bankanın çalışanlarından ... isimli şahsın Bankacılık Kanunu 73, 153 ve 159 maddeleri ile TCK 239 maddesine muhalefet ederek maliyeye ihbarı sonucunda, müvekkili aleyhine vergi bildirimini yapmadığı gerekçesiyle resen takdire gidildiğini, müvekkiline, usulsüzlük ve vergi ziyayı cezaları

tertip edildiğini, banka çalışanı hakkında savcılık nezdinde suç duyurusunda bulunulup buna ilişkin olarak hazırlık numarasını da mahkeme dosyasına bildireceklerini, davalının müvekkiline karşı, TBK 58, 116, 112, 114/2, 49, 50 hükümlerine göre sorumlu olduğunu, Gelir İdaresi Başkanlığına savunmalarını verdiklerini ve kendi hatalarından kaynaklandığı için bu sürece davalı bankayı da mümkün mertebe dahil etmeye çalıştıklarını, yapılan işbu görüşmelerde müvekkilin defalarca davalı bankadan zararının karşılanmasını talep etmiş ise de müspet bir sonuç elde edemediğini, bunun üzerine müvekkilin, gerek prestijinin ve saygınlığının sarsılmasını istemediğinden gerekse devletine vergi borçlusunu olarak kalmayı istemediğinden Gelir İdaresi Başkanlığı ile uzlaşma yapmak zorunda kaldığını ve sonuçta 26/08/2015 tarihli uzlaşma tutanağı ile müvekkilin, gecikme faizi hariç olmak üzere 70.000,00TL üzerinden uzlaşabildiğini ve müvekkilin uzlaşma kararı sonucu faizi ile birlikte 103.000,00TL olarak ödeme yaptığını, davalının müvekkiline karşı, TBK 58, 116, 112, 114/2, 49, 50 hükümlerine göre sorumlu olduğunu, davalının, çalışanlarına gereken eğitimi vermemiş olması TBK 116 sorumluluğu, ağır sorumluluğu nedeniyle müvekkilin son derece yıpranmış, vatanına sadece ailesini ve sevdiklerini görmek için gelebiliyorken sürekli bu sorunlarla ilgilenip, devamlı olarak vergi daireleri, noterler ve bankalara gitmek zorunda kaldığını, bu durum müvekkilin vatanında geçirdiği, zaten kısıtlı olan zamanında ailesi ve sevdikleriyle zaman geçirmesini engellediğini, sonuç olarak müvekkilin bu durumdan geri dönülmesi imkansız ve tarifsiz elem ve ızdırap duyduğundan bahisle fazlaya ilişkin hakları saklı kalmak kaydı ile, açıklanan nedenler karşısında; 103.000,00TL maddi ve 50.000,00TL manevi olmak üzere toplam 153.000,00TL'nin ihtarnamenin tebliğ tarihi olan 25/09/2015 tarihinden itibaren işleyecek ticari faiziyle birlikte davalılardan alınıp müvekkiline verilmesine, vekalet ücreti ve sair yargılama giderinin davalıya tahmiline karar verilmesini talep ve dava etmiştir.

CEVAP: Davalı ... A.Ş. vekili cevap dilekçesinde özetle; husumet itirazlarının bulunduğunu, davacının hesabının müvekkili banka nezdinde değil ... Ltd isimli KKTC'de kurulu banka nezdinde açıldığını, davaya konu sözde zararın davacının vergisel yükümlülüklerini yerine getirmemesi nedeniyle tamamen davacının münferit ve ağır kusuruyla meydana geldiğini, davacının mevzuat hükümleri gereğince gelir vergisi mükellefi olduğu sonucuna varıldığını, davacının Gelir Vergisi Kanunu, tebliğ ve uluslararası anlaşma muvacehesinde tam mükellef kabul edildiğini, mevzuat hükümleriyle birlikte Danıştay kararlarında davacının tam mükellefiyetini ortaya koyduğunu, davacının davaya konu vergi ve vergi cezalarına ilişkin iptal davası açmayıp uzlaşma yoluyla ödemesinin de davacının zararın meydana gelmesinde kusurlu olduğuna açık bir şekilde delalet edeceğini, yanlış hesap açıldığı ve banka çalışanı ...'ın maliyeye ihbarı ile zararın meydana geldiği iddiasının afaki ve soyut bir iddia olduğunu, müvekkili bankanın haksız fiil sorumluluğu

bulunmadığını, dava konusu zararın bankacılık işleminden sadır olmadığı gibi yapılan işlemin müvekkilinin gözetim ve denetimine tabi olmadığını, müvekkili bankanın özen yükümlülüğünü yerine getirdiğinden somut olayda müvekkili bankanın adam çalıştıran olarak sorumlu tutulamayacağını, müvekkili banka çalışanının davacıyı ihbar etmesi nedeniyle müvekkili bankanın bankacılık ve ceza hukuku anlamında sır saklama yükümlülüğünü ihlal ettiği iddiasının hukuki dayanaktan yoksun olduğunu, davacının davaya konu olan vergi ve vergi ziyayı cezalarını müvekkili bankadan tahsil etmeye çalışmasının dürüstlük kuralına aykırı olup, hakkın kötüye kullanılması niteliğinde olduğundan bahisle öncelikle davanın pasif husumet yokluğu nedeniyle usulden reddine, davacı tarafın ikame etmiş olduğu hukuki dayanaktan yoksun ve mesnetsiz işbu davanın reddine, vekalet ücreti ve yargılama giderlerinin davacıya tahmiline karar verilmesini talep etmiştir. Davalı ... cevap dilekçesinde özetle; Ticaret mahkemesinin görevli olmadığını, davacının iddialarına ilişkin delil sunmadığından davanın reddedilmesi gerektiğini, İstanbul Cumhuriyet Başsavcılığı'nca "Ticari Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi veya Belgeleri Açıklamak" suçundan hakkında yürütülen soruşturma sonucu Kovuşturmaya Yer Olmadığına Dair Karar verildiğini, davacının hesabı bulunan ... Ltd ile herhangi bir sıfat ile görevinin olmadığını, davacıyla herhangi bir bankacılık işlemi gerçekleştirmediğini, zan ile dava açılmayacağından davanın reddi gerektiğini, davacılarının iddialarının aksine İstanbul Cumhuriyet Başsavcılığı'nın verdiği hüküm ile kanuna aykırı herhangi bir durum söz konusu olmadığından davanın reddine karar verilmesini talep etmiştir.

İLK DERECE MAHKEMESİ KARARI: İstinaf incelemesine konu kararı veren ilk derece Mahkemesince eldeki dava hakkında yapılan yargılama sonunda, "Davacı taraf, davalıların sır saklama yükümlülüğüne aykırı hareket ettiklerinden bahisle maddi zararının giderilmesi ile manevi tazminat talep etmiş ise de; davacı taraf kendi eylem ve işlemleriyle vergi ve cezalara muhatap olduğu, tüm vergi ve vergi cezalarının mevzuat ve uluslararası anlaşma hükümlerine uygun olduğu, davacının vergisel ödevlerini yerine getirmeksizin vergi kayıp ve kaçığına neden olması sonucunda vergi ve cezalara muhatap kalmasında davalıların herhangi bir kusurunun ve haksız fiilinin bulunmadığı, davacının talepleri yönünden davalılara bir sorumluluk yüklenemeyeceği anlaşıldığından davanın reddine, ..." karar verilmiştir.

İLERİ SÜRÜLEN İSTİNAF SEBEPLERİ: Davacı vekili istinaf dilekçesinde özetle; mahkeme kararında red sebebine ilişkin hiç bir gerekçe sunulmadığını, dosyaya intikal eden bilirkişi raporuna itirazda bulunulmuş ve dosyanın yeni bilirkişi heyetine tevdi istenilmiş ve bu konularda uzman vergi konusunda maliye baş müfettişliği yapmış , yeminli mali müşavir ... mütalaası ile bankacılık konusunda uzman banka genel müdür yardımcılığı yapmış ... mütalaası sunulmuş olmasına rağmen

bilirkişi raporuna itirazların dahi değerlendirilmediğini, mahkeme dosyasına sunulan Yeminli Mali Müşavir , Vergi Konusunda Eski Maliye Başmüfettişi ...nın ve bankacılık konusunda uzman genel müdür yardımcılığı yapmış ...ın HMK 293/3 maddesi uyarınca çağrılmasına ilişkin talebin değerlendirilmediğini, hesabın yurt dışı yerleşik kişi olarak açılmış olması halinde ... tarafından böyle bir ihbarın yapılamayacağını ve müvekkilinin vergi mükellefi olmayacağını, ...'ın adam çalıştırmanın sorumluluğu çerçevesinden sorumlu olduğunu, müvekkilinin mükellef olup olmadığı ile, ...'ın ve davalı ... in sorumluluğuna ilişkin tespitlerin yapılmadığını, usul ve yasaya aykırı hiç bir bilimsel gerekçeye ve tespite dayanmayan, baştan savma olarak düzenlenen, hukuki dayanaktan yoksun, bilimsel dayanaktan yoksun bilirkişi raporuna karşı itirazları doğrultusunda HMK 281/3 maddesi uyarınca yetkin, konusunda uzman (üniversiteden profesör) kişiler tarafından yeni bir bilirkişi raporu tanzim edilmesinin talep edilmesine rağmen mahkemenin bunu görmezden geldiğini beyanla, ilk derece Mahkemesince verilen kararın kaldırılmasını ve davanın kabulüne karar verilmesini talep ve istinaf etmiştir.

GEREKÇE: Dava, banka çalışanın usulsüz ihbarı nedeniyle vergi dairesince tahakkuk ve tahsil edilen gelir vergisi ve vergi ziyai cezasından dolayı uğranılan zarar nedeniyle maddi ve manevi tazminat davasıdır. İstinafa gelen uyuşmazlık temelinde, davalı bankanın hesap açılışında yurt içi gerçek kişi olarak hesap açması nedeniyle davacının zarara uğrayıp uğramadığı ve davacının tam mükellef olup olmadığı noktasındadır. Davacı, davalı Bankanın ... numaralı müşterisi olup, dosyada mevcut yazılara göre davacıya sehven yurt içi yerleşik gerçek kişi olarak hesap açıldığı anlaşılmaktadır. Daha sonra süreç içerisinde davalı ...'ın ihbarı üzerine vergi müfettişlerince hazırlanan 2009 dönemi için 21/01/2015 tarih ve ..., 2010 dönemi için 26/05/2015 tarih ve ..., 2011 dönemi için 26/05/2015 tarih ve ... ve 2013 dönemi için 26/06/2015 tarih ve ... sayılı inceleme raporlarında davacının, ... Ltd. Nezdinde bulunan mevduatının faiz getirisine ilişkin olarak, yurda giriş çıkış kayıtları incelenerek bir takvim yılı içinde Türkiye'de devamlı olarak 6 aydan fazla oturduğu kabul edilerek mükellefin inceleme dönemlerine ilişkin gelir vergisi beyanının yeniden düzenlenmesi ve gelir vergisinin re'sen tarh edilmesi, ayrıca tarh edilecek fark gelir vergisi tutarı üzerinden vergi ziyai cezası kesilmesi ve mükellefe nakden yapılan haksız iade tutarının geri alınması, geri alınacak haksız iade tutarı üzerinden vergi ziyai cezası kesilmesi şeklinde kanaat bildirilmiştir. Daha sonra 26/08/2015 tarihinde gelir vergisi ve vergi ziyai cezalarına ilişkin 2015/372 karar sayılı uzlaşma tutanağı düzenlenmiştir. Davacı, banka hesabının yurt içi gerçek kişi olarak yapılması ve davalı banka çalışanı ...'ın Bankacılık Kanunu 73, 153 ve 159 maddeleri ile TCK 239 maddesine muhalefet ederek Maliye'ye ihbarı sonucunda, aleyhine vergi bildirimini yapmadığı gerekçesiyle resen tarhiyat yapılması suretiyle uğradığı zararın tazmini istemli olarak eldeki davayı

açmıştır. Ancak vergi dairesince hazırlanan raporlara göre, incelemeye konu dönemlere ilişkin gelir vergisi ve vergi ziyai cezasının, davalı bankanın davacı adına açtığı hesabı yurt içi gerçek kişi olarak açmasından değil, davacının bir takvim yılı içinde Türkiye'de devamlı olarak 6 aydan fazla oturması nedeniyle tam mükellef kabul edilmesinden dolayı tahakkuk ettirildiği anlaşılmaktadır. Davacı tam mükellef kabul edilmesiyle Vergi dairesi ile davacı arasında oluşan uyuşmazlık uzlaşma ile çözüme kavuşturulmuş ve uzlaşma tutanağında sonuca bağlanan tutar davacı tarafından vergi dairesine ödenmiştir. Bu halde, davacının Türkiyede yerleşik olup olmadığı ve ... Ltd. Nezdinde bulunan mevduatının faiz getirisinin Türkiye'de vergilendirmeye tabi olup olmadığı ve sonuç olarak davacının tam mükellef olup olmadığı hususları vergi yargısının konusu olup, bunların adli yargı eliyle ve hatta vergi dairesinin taraf olmadığı bir davada yargılamaya konu edilmesi mümkün değildir. Davacı, mevcut durum itibariyle ... Ltd. Nezdinde bulunan mevduatının faiz getirisine ilişkin olarak Türkiye'de tam mükellef olup, davalı bankanın bu mevduatın bulunduğu hesabı yurt içi gerçek kişi olarak açması sonuca etkili değildir. Ayrıca, uzlaşma tutanağı ile sonuca bağlanarak davacı tarafından yapılan ödeme Anayasanın 73. Maddesinde ifadesini bulan vergi ödevinin bir gereği olup, bu ödemenin zarar olarak değerlendirilmesi mümkün değildir. Bu halde, davalı Bankanın davacıya karşı sorumlu olmasını gerektiren herhangi bir durum söz konusu değildir.

1905 sayılı Menkul Ve Gayrimenkul Emval İle Bunların İntifa Haklarının Ve Daimi Vergilerin Mektumlarını Haber Verenlere Verilecek ikramiyelere Dair Kanun'un 1. maddesi; umumi veya hususi kanunlar ve muahedeler ahkamına göre Devlete ait veya Hazine emrine mevdu olması lazım geldiği halde Hükümetin kayda müstenit ittilai haricinde kalmış olan bilümmen menkul ve gayrimenkul emval veya bu nevi emvalin intifa hakları ile senede merbut veya ipotekli ve ipoteksiz alacakları ve her nevi mevduat ve emanet ile esham ve tahvilatı ve sigorta matluplarını ihbar edenlere ihbar edilen emvalin veya intifa hakkının Hazineye aidiyeti tahakkuk ettikten sonra bu emvalin kıymetleri veya iki senelik intifa baliğleri üzerinden (belirlenen) nispetlere göre ikramiye verilir, şeklinde düzenlenmiştir. Buna göre vergi ödevinin bütün mükellefler tarafından sağlıklı bir şekilde yerine getirilmesini sağlamak için ihbar müessesesi yasal olarak kabul edilmiş durumdadır. 5411 sayılı Bankacılık Kanunu'nun 73/3. Maddesinde müşteri sırrı ve banka sırrı ve istisnaları düzenlenmiştir. Buna göre; Sıfat ve görevleri dolayısıyla bankalara veya müşterilerine ait sırları öğrenenler, söz konusu sırları bu konuda kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamazlar. Bu yükümlülük görevden ayrıldıktan sonra da devam eder. Bankacılık faaliyetlerine özgü olarak bankalarla müşteri ilişkisi kurulduktan sonra oluşan gerçek ve tüzel kişilere ait veriler, müşteri sırrı hâline gelir. Diğer kanunların emredici hükümleri saklı kalmak kaydıyla, müşteri sırrı niteliğindeki bilgiler, bu maddede belirtilen sır saklama yükümlülüğünden istisna tutulan hâller

haricinde, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca müşterinin açık rızası alınsa dahi, müşteriden gelen bir talep ya da talimat olmaksızın yurt içindeki ve yurt dışındaki üçüncü kişilerle paylaşamaz ve bunlara aktarılamaz. Bu maddede belirtilen sır saklama yükümlülüğünden istisna tutulan hâllerde yapılacak paylaşımlar da dâhil olmak üzere, müşteri sırrı ve banka sırrı niteliğindeki bilgiler, sadece belirtilen amaçlarla sınırlı olmak ve ölçülülük ilkesine uygun olarak bu amaçların gerektirdiği kadar veriyi içermek kaydıyla paylaşılabilir. 193 sayılı Gelir Vergisi Kanunu(G.V.K.)'nun 75. maddesinde mevduat faizleri menkul sermaye iradı olarak sayılmıştır. Kanun'un 2. Maddesinde menkul sermaye iratları, gelir vergisine tabi tutulmuştur. Kanun'un 83. Maddesinde Gelir Vergisinin mükellefin veya vergi sorumlusunun beyanı üzerine tarh olunacağını, 85/1. maddesinde ise mükelleflerin 2 nci maddede yazılı kaynaklardan bir takvim yılı içinde elde ettikleri kazanç ve iratları için bu Kanunda aksine hüküm olmadıkça yıllık beyanname verecekleri düzenlenmiştir. Davacı vergi mükellefi olup, vergi dairesi de vergi alacaklısı durumundadır. Anılan yasal düzenlemeler uyarınca davacı elde ettiği mevduat faizi gelirini beyan esasına göre beyanname düzenleyerek vergi dairesine vermesi gerekir. Bu halde davacının vergi dairesine zaten beyanla yükümlü olduğu bir hususun 1905 sayılı yasanın verdiği imkanla ihbar edilmiş olması müşteri ve banka sırrının açıklanması anlamına gelmez. Zira yasal olarak vergi dairesinin vergi tarh ve tahakkuk işlemlerini yerine getirebilmesi için vergiyi doğuran olaydan haberdar olması gerekir. Vergi Usul Kanunu(VUK)'un 142. Maddesine göre, beyan dışında ihbar veya yapılan incelemeler dolayısıyla vergi dairesi vergiyi doğuran olaydan haberdar olabilmektedir. Dolayısıyla davacının mevduat faizi geliri elde etmesi vergi dairesi bakımından müşteri sırrı ve banka sırrı olarak değerlendirilemez. Bu bakımdan davalı ...'ın vergi dairesine ihbarda bulunması suretiyle, müşteri sırrının Bankacılık Kanunu'na aykırı olarak açıkladığının kabulü mümkün değildir. Davacı tarafca iki adet uzman görüşü sunulmuş ise de, bunlar varsayımsal ve subjektif değerlendirmeler içerdiğinden hükme esas alınamazlar. Kaldı ki her iki uzman görüşünde de davalı ...'ın ihbarının mevzuata aykırı olduğuna dair bir tespit yer almamaktadır. Her ne kadar davacının hesabının yurtiçi yerleşik gerçek kişi hesabı olarak açılmamış olsa davalı ... tarafından ihbarın yapılmayacağını davacının resen vergi incelemesine tabi tutulma olasılığının çok düşük olduğu görüş olarak ileri sürülmüş ise de, bu hususlar davalı ...'ın ihbara hakkı olduğu ve davacının tam mükellef olduğu hususları üzerinde etkili değildir. Bu haliyle davacının davalı ... hakkındaki davası da yerinde değildir. Sonuç itibariyle Mahkemece davanın reddine karar verilmesinde herhangi bir isabetsizlik görülmemiştir. HMK'nın 355. Maddesi uyarınca kamu düzenine aykırılık ve istinaf dilekçesinde belirtilen sebeplerle sınırlı olarak yapılan istinaf incelemesi sonunda; ilk derece mahkemesi kararının

usul ve esas yönünden hukuka uygun olduğu anlaşıldığından davacı vekilinin yerinde görülmeven istinaf başvurusunun reddine karar vermek gerekmiştir.

KARAR: Yukarıda ayrıntısı ile açıklanan nedenlerle; 1-Davacı vekilinin istinaf başvurusunun HMK'nın 353(1)b-1 maddesi uyarınca ESASTAN REDDİNE, 2-Davacı tarafından başvuru sırasında istinaf karar harcı peşin olarak yatırıldığından başkaca harç alınmasına yer olmadığına, 3-Davacı tarafından istinaf aşamasında yapılan yargılama giderlerinin kendi üzerinde bırakılmasına, 4-Kararın, HMK'nın 359/4 maddesi uyarınca Dairemiz Yazı İşleri Müdürlüğünce taraflara resen tebliğine, Dair, dosya üzerinden yapılan inceleme sonunda, gerekçeli kararın taraflara tebliğinden itibaren 2(iki) hafta içerisinde Yargıtay'a temyiz yasa yolu açık olmak üzere oy birliğiyle karar verildi.18/11/2021

İstanbul Bölge Adliye Mahkemesi, 21. HD., E. 2018/3160 K. 2019/801 T. 15.4.2019

Esas No.: 2018/3160

Karar No.: 2019/801

Karar Tarihi: 15.04.2019

İSTİNAF KARARI

DAVANIN KONUSU: Şikayet (İcra Memur Muamelesi)

Yukarıda tarih ve numarası yazılı mahkeme kararının istinaf yolu ile incelenmesi talep edilmiş olup, dosya yerel mahkemece Dairemize gönderilmiş olmakla, üye hakim tarafından düzenlenen rapor dinlendikten ve dosyadaki tüm belgeler okunup incelendikten sonra gereği görüşülüp, düşünüldü.

İDDİA VE SAVUNMANIN ÖZETİ:

Davacı vekili dava dilekçesinde özetle ; İstanbul Anadolu 2. İcra Müdürlüğü'nün 2017/8676 Esas sayılı dosyasında dosya borçluları yönünden icra müdürlüğü UYAP ekranı kullanılarak " dava açılış taraf vekil işlemleri sekmesinden borluya ait alacaklı olduğu icra takip dosyalarının sorgulanmasını ve tespit edilen dosyaların haczi için ilgili icra dairesine UYAP vasıtasıyla yazı yazılması " talebinde bulduklarını, icra müdürlüğünün yapılacak sorgulamanın Anayasa'nın 20. Maddesinde düzenlenen temel hak ve hürriyetlere aykırılık oluşturacağı gibi kişisel gizliliği ihlal eden durumlara da yol açabileceği gerekçesiyle reddettiğini, red kararının usul ve yasaya aykırı olduğunu söyleyerek icra müdürlüğünün 29/08/2018 tarihli red kararının kaldırılmasını istemiştir.

İLK DERECE MAHKEMESİ KARARININ ÖZETİ:

İlk derece mahkemesince: " İcra dosyasının incelenmesinde; alacaklı F1 Factoring A.Ş. Vekili tarafından borçlu F3 Tekstil San ve Tic. Ltd Şti, F2 İnş Temizlik Görüntüleme ve Rehabilitasyon Tic. Ltd Şti ve K1 aleyhine 52.000,00 TL bedelli çekin tahsili amacıyla takip başlatıldığı görülmüştür.

İstanbul Bölge Adliye Mahkemesi 23. Hukuk Dairesinin 2017/596 E 2017/527 K sayılı ilamında; "İcra dosyasının tarafı olmayan üçüncü kişiye ait 6698 sayılı Yasanın 3/1-d maddesi kapsamında kişisel veri niteliğinde bulunan tapu kaydı ve satış sözleşmelerinin icra müdürlüğünce celbinin istenemeyeceği, aynı Yasanın 28/1-d maddesindeki yargısal organlara tanınan istisnanın, ancak uyuşmazlığı tarafları açısından geçerli olabileceği, Anayasa'nın 20/3.maddesine göre aynı zamanda

temel haklardan olan kişisel verilerin korunmasını isteme hakkının, 6698 sayılı Yasanın 28/1-d maddesinin geniş yorumlanması ile daraltılmayacağı, Mülkiyet hakkının korunması zımında açılacak bir davanın taraflarını tespit edebilmek için 1136 sayılı Avukatlık Kanununun 2/3. Maddesine ve Başbakanlık Tapu Kadastro Genel Müdürlüğü'nün 2001/11 sayılı Genelgesine göre avukatın yazılı başvuru ile tapu sicilinde inceleme yapabileceği ve kanunda kısıtı olarak öngörülen kişisel verilere ulaşma imkanının bu şekilde sağlanması ile hukuki denetimin de yapılabileceği bu verilere ulaşma imkanının birden fazla yolla sağlanması halinde, verilere kimlerin ulaştığının denetiminin zorlaşacağı nazara alınarak, icra müdürlüğü kararının isabetli olduğu, alacaklının hukuki menfaatinin, 3. şahısların Anayasa ile korunan özel hayatın gizliliğine ilişkin temel hakkından üstün tutulmasının mümkün olmadığı..." şeklinde karar verildiği görülmüştür.

Yargıtay 12. Hukuk Dairesinin 2015/33810 E 2016/13366 K sayılı ilamında; "Takip borçlusunun anne ve babasını gösterir nüfus kayıt örneklerinin çıkartılması ölü olmaları halinde takbis sisteminden anne ve babasına ait kayıtlı taşınmazların sorgulanması ile borçluya intikal edecek hisseleri üzerine haciz konulması ile müzekkere yazılmasını talep ettiği, talebinin reddedilmesinin üzerine yapılan şikayetin incelenmesinde; 3.kişiler ile ilgili yapılacak sorgulamaların Anayasa'nın 20. Maddesinde düzenlenen temel hak ve hürriyetlere aykırılık oluşturduğu, kişilerin verilen gizliliğinin güvence altına alındığı, takip ile ilgisi bulunmayan borçlu durumunda olmayan kişilerin kişisel kimlik bilgileri ile durumlarının araştırılmasının icra müdürlüğünde görevli katip ve müdürlerin görevleri kapsamında bulunmadığı, alacaklı vekiline, borçlunun anne ve babasının ölmüş olduğunun bildirilmesi ve taşınmaz bilgilerinin sunulması halinde İİK.'nin 94. Maddesi gereğince işlem yapılabileceği belirlendiğinden şikayetin reddine dair tesis edilen karar uygun görülmüştür." şeklinde karar verildiği görülmüştür.

İlgili icra müdürlüğü'nün 29/08/2018 tarihli kararında; "Talebe konu UYAP ekran içeriğinin incelemesinden takip borçlusunun alacaklı olduğu dosyaların sorgulanmasına imkan veren ekranda aynı zamanda adı geçen kişi yönünden yakalama, tutuklama ve diğer davalar gibi bilgilerin de yer aldığı görülmekte olup bu şekilde yapılacak sorgulamanın Anayasanın 20. Maddesinde düzenlenen temel hak ve hürriyetlere aykırılık oluşturacağı gibi kişisel gizliliği ihlal eden durumlara da yol açabileceğinden talebin reddine" dair karar verildiği, yukarıda bahsolunan İstinaf ve Yargıtay kararlarına göre takibin tarafı olmayan kişilerin bilgilerinin sorgulanması talebinin Anayasa'nın 20. Maddesinde düzenlenen temel hak ve hürriyetlere aykırılık oluşturduğu, kişilerin verilen gizliliğinin güvence altına alındığı, takip ile ilgisi bulunmayan borçlu durumunda olmayan kişilerin kişisel kimlik bilgileri ile durumlarının araştırılmasının icra müdürlüğünde görevli katip ve

müdürlerin görevleri kapsamında bulunmadığı kanaatine varılarak ilgili icra müdürlüğü kararının hukuka ve usule uygun olduğu görülmele şikayetin reddine " karar verildiği görülmüştür.

İLERİ SÜRÜLEN İSTİNAF SEBEPLERİ:

Davacı vekili istinaf dilekçesinde özetle ; Adana 1. İcra Hukuk Mahkemesi'nin 2018/438 Esas sayılı dosyasında huzurdaki şikayet ile birebir aynı olan 31/07/2018 tarihinde verilen kararın emsal olarak icra müdürlüğüne sunulduğunu, icra dairesince taleplerinin reddedildiğini, başka icra daireleri tarafından kabul edilen talebin İstanbul Anadolu 2. İcra Dairesi ve İstanbul Anadolu 6. İcra Hukuk Mahkemesi tarafından reddedildiğini, borçluların alacaklısı olduğu dosyaların UYAP ekranından sorgusunun yapılmasına ilişkin kabul edilip edilmemesine dair farklı kararlar olması üzerine Adalet Bakanlığı Hukuk İşleri Genel Müdürlüğü görüş bildirmek zorunda kaldığını, ayrıca kesinleşen icra takip dosyasında borçlu olan kişilerin alacaklısı olduğu dosyalarda sorgulanması ve tespiti halinde haczini istediklerini, icra dairesinin dar yetkili olduğunu, kesinleşen takip dosyasında alacaklı vekilince sunulan haciz talebini reddetme yetkisinin bulunmadığını, verilen kararın yasaya aykırı olduğunu söyleyerek kararın kaldırılmasını, taleple ilgili işlem yapılmasını istemiştir.

DELİLLERİN DEĞERLENDİRİLMESİ VE GEREKÇE:

İncelenen icra dosyası fotokopisi, ilk derece mahkeme kararı ve tüm dosya kapsamına göre ; şikayete konu icra müdürlüğü ekranından takip borçlusunun alacaklı olduğu, icra takip dosyalarının sorgulanmasına ilişkin talep İİK 78 ve devamı maddelerinde düzenlenen haciz talebi niteliğinde olmayıp ayrıca şikayete konu bu talep takibin yürütülmesine yönelik icra müdürlüğüne alacaklının talebi üzerine yasa gereği yapılması zorunlu olan bir işlem olmadığı gibi yapılacak sorgulamanın Anayasa'nın 20. Maddesindeki düzenlemeye de aykırılık teşkil ettiğinden ilk derece mahkemesi kararı yasaya uygun olmakla davacının istinaf talebinin esastan reddine karar vermek gerekmiş ve aşağıdaki şekilde hüküm kurulmuştur.

HÜKÜM: Yukarıda açıklanan nedenlerle;

1-Davacının istinaf başvurusunun Hukuk Muhakemeleri Kanununun 353/1-b.1 maddesi gereğince ESASTAN REDDİNE,

2-a-) Peşin harcın mahsubu ile bakiye 8,50 TL karar harcının davacıdan alınarak hazineye gelir kaydına,

b-)İstinaf yargılama giderlerinin başvuran üzerinde bırakılmasına;

Gerekçeli kararın tebliğinden itibaren 7035 Sayılı Kanunla değişik 6100 Sayılı HMK'nun 361/1.md.gereğince 2 (iki) hafta içerisinde Dairemize veya Dairemize gönderilmek üzere başka yer Bölge Adliye Mahkemesi Hukuk Dairesine veya İlk Derece Mahkemesine dilekçe verilmek suretiyle Yargıtayın ilgili Hukuk Dairesince incelenmek üzere temyiz yasa yoluna başvurma hakkı bulunduğuna oy birliği ile karar verildi. 15.04.2019

İstanbul Bölge Adliye Mahkemesi, 4. HD., E. 2017/1495 K. 2017/1619 T. 27.11.2017

Esas No.: 2017/1495

Karar No.: 2017/1619

Karar Tarihi: 27.11.2017

İSTİNAF KARARI

DAVANIN KONUSU: Maddi ve Manevi Tazminat, Sigorta Muafiyetinin İptali

Yukarıda yazılı ilk derece mahkemesi kararına karşı davacı tarafca istinaf kanun yoluna başvurulmuş olmakla HMK 353. maddesi uyarınca dosya incelendi,

GEREĞİ GÖRÜŞÜLÜP DÜŞÜNÜLDÜ:

DAVA: Davacı vekili ilk derece mahkemesine sunduğu dava dilekçesinde özetle; davacının F1 Havayollarında uçuşa elverişlilik kontrol müdürü olarak görev yaptığını, çalışmakta olduğu F1 Havayolları aracılığı ile F2 Sigorta A.Ş.' nden özel sağlık sigortası yaptırdığını, 04/09/2013 tarihinde Acıbadem Hastanesinde operasyon geçirdiğini ve tedavi giderlerinin poliçe kapsamında F2 Sigorta A.Ş. tarafından ödendiğini, daha sonrasında davalı F2 Sigorta A.Ş.' nin 2009 yılındaki tıbbi kayıtlara dayanarak sağlık poliçesine muafiyet koyduğunu, davalı F2 Sigorta A.Ş. ' nin bu tıbbi bilgileri diğer davalının yapmış olduğu araştırma sonucunda elde ettiğini, kendisinin her iki davalıya da gizli sağlık bilgilerini araştırması yönünde bir talimat yada izin vermediğini bildirerek, geçmişe dönük hasta bilgilerinin rızası dışında hukuka aykırı olarak araştırılması ve rızası dışında üçüncü kişiler ile paylaşılması nedeni ile 20.000.00-TL manevi tazminatın ve 1.000,00-TL maddi tazminatın davalılardan tahsilini, sağlık sigorta poliçesine konulan muafiyetin kaldırılmasını talep ve dava etmiştir.

CEVAP: Davalı F2 Sigorta A.Ş. vekili cevap dilekçesinde özetle; davacının hasta olarak değil sigortalı olarak nitelendirilmesi gerektiğini, davalı olarak gösterilen sigorta şirketi de bir hastane veya sağlık sektörü kurumu olmadığından davanın sağlık hukukundan çok sigorta hukuku kapsamında değerlendirmesi gerektiğini, hasta bilgilerinin gizliliğinin hukuka aykırı biçimde ihlal edilmiş olduğu iddiasının gerçek durum ile bağdaşmadığını, sağlık bilgilerinin tüm şirket çalışanları ile paylaşıldığı iddiasının da gerçeği yansıtmadığını, davacının muafiyetinin hukuka aykırı olarak konulduğu

iddiasının kabul edilemez olduğunu, davacı uygulanan muafiyetler nedeniyle uğrayacağı muhtemel zararlarının giderilmesini isteyemeyeceğini bildirerek davanın reddi gerektiğini savunmuştur.

Davalı F3 Medical Bilgi Sistemleri A.Ş. vekili cevap dilekçesinde özetle; davalı müvekkilinin yıllardır sağlık kuruluşlarına ve sigorta şirketlerine yazılım, danışmanlık ve çeşitli alt yapı hizmetleri verdiğini, davalı şirketin sadece sigorta şirketi ile sigortalı arasındaki hukuki ilişkiye uygun olarak sigorta kapsamında gerekli işlemlerin yürütülmesine yardımcı olduğunu, davacı tarafla bir hukuki ilişkisi bulunmadığından öncelikle husumet yönünden davanın reddi gerektiğini, TTK 1147 maddesi gereğince uygulamada tüm sigorta şirketlerinin sigortalıdan aldıkları başvuru formundaki yazılı izin ile sigortalı hakkında sağlık kuruluşları nezdinde araştırma yaptıklarını, müvekkilinin de davacının yazılı izni kapsamında gerekli araştırmayı yaptığını, sigortalının yazılı izni bulunduğundan davanın mesnetsiz olduğunu, ayrıca davacının bilgilerinin üçüncü kişilerle paylaşılmadığını, hukuka aykırı bir fiillerinin bulunmadığını, zarar oluşmadığını, tazminat koşullarının bulunmadığını, ayrıca talep edilen tazminatın fahiş olduğunu bildirerek, davanın reddi gerektiğini savunmuştur.

DELİLLER: Sağlık Hizmetleri Sözleşmesi, Sigorta poliçesi, Grup Sağlık Sigorta Sertifikası ve poliçesi, e-posta yazışmaları, hasta bilgileri, maaş bordrosu, sigorta muafiyet bildirim, grup sağlık sigortası başvuru formu, bilirkişi raporları.

İLK DERECE MAHKEMESİ KARARI: İlk derece mahkemesince yapılan yargılama sonucunda; davanın esastan reddine karar verilmiştir.

İSTİNAF SEBEPLERİ: Davacı vekili istinaf başvuru dilekçesinde özetle; müvekkilinin matbu olarak hazırlanmış formu imzalamış olmasının, kişisel verilerinin elde edilmesi hususunda geçerli bir rıza olarak kabul edilemeyeceğini, müvekkiline bu hususta yeterli bilgi verilmeksizin ve aydınlatılmadan imza atıldığını, 6698 sayılı yasa gereğince sadece o işlemle sınırlı, özgür iradeyle onay alınması gerektiğini, müvekkilinin çalıştığı kurumun kendisine sağladığı sigorta imkanından faydalanabilmek adına matbu formu imzalamak zorunda kaldığını, açık rızasının bulunmadığını, formun TBK 21. maddesine de uygun olmadığını, formun genel ve matbu olup özel olarak müvekkili için hazırlanmadığını, aksi kabul edilse bile formdaki iznin sadece sigorta şirketine araştırma yetkisi verdiğini, bilgilerin üçüncü kişilerle de paylaşılmış olduğunu, poliçeye muafiyet eklenmesinin de TTK hükümlerine uygun olmadığını, müvekkilinin kronik veya takipli hasta olmadığını, muafiyete esas alınan belge ve raporların eski tarihli olduğunu, bilirkişi raporları arasındaki çelişki giderilmeden karar verildiğini, davalıların eylemlerinin tazminatı gerektirdiğini bildirerek istinaf başvurularının kabulü ile yerel mahkeme kararının kaldırılmasını ve davanın kabulünü talep etmiştir.

DEĞERLENDİRME VE GEREKÇE: Dava; kişilik haklarına saldırı iddiasına dayalı maddi ve manevi tazminat ile birlikte sağlık sigorta poliçesine konulan muafiyetin kaldırılması talebine ilişkindir. İlk derece mahkemesince davanın reddine karar verilmiş, karar davacı tarafça istinaf edilmiştir.

Tüm dosya kapsamına göre; davacının dava dışı F1 Havayolları şirketinin çalışanı olduğu, dava dışı havayolu şirketi ile davalı sigorta şirketi arasında yapılan sağlık hizmetleri sözleşmesi uyarınca havayolu çalışanlarının sigortalanabilmesi için grup sağlık sigortası başvuru formu düzenlendiği, dosyada mevcut 28/05/2013 tarihli grup sağlık sigortası başvuru formunun davacı tarafından doldurulup imzalandığı, formun son sayfasında yer alan sigortalı adaylarının sağlık beyanı kısmında "başvuru formumun kabulü halinde beyanda bulunduğum tüm hususlar hakkında F2 Sigortayı, doktor, sağlık kuruluşları, sigorta şirketleri ya da idari ve resmi tüm kuruluşlardan bilgi almaya ve vermeye yetkili kıldığımı, farklı bir bilgi alınması durumunda, şirketin bilmesi gereken herhangi bir hususu gizlediğim ya da formda eksik ya da hatalı bilgi verdiğim takdirde TTK ve Sağlık Sigortası genel şartları uyarınca, bu hususun tazminat talebinin reddine ve sigorta poliçesinin iptaline neden olacağını bilmekle doğru beyan verdiğimi kabul ve taahhüt ederim." şeklindeki kabul beyanı ile davacının, kişisel sağlık ve hastalık bilgilerinin araştırılması hususunda davalı sigorta şirketine tam yetki verdiği, davalı sigorta şirketinin davacının hastalık bilgilerini araştırmasının hukuka aykırı bir davranış olmadığı, bilakis davacının rızasına ve dava dışı hava yolu şirketi ile yaptığı sözleşme hükümlerine uygun olduğu, sağlık sigorta poliçesi genel şartlarınının 6. maddesine göre, sigorta ettirenin sözleşme yapılırken beyan yükümlülüğüne yer verildiği, buna göre sigorta ettirenin/sigortalının teklifname ve bunu tamamlayıcı belgelerde kendisine sorulan sorulara doğru cevap vermek ve rizikonun konusunu teşkil eden, rizikonun takdirine etkili olacak hususlardan kendisince bilinenleri de beyan etmekle yükümlü olduğu, aynı şartın sözleşmenin 6. maddesinde de yer aldığı, sağlık konusundaki eksik beyandan sigorta ettirenin sorumlu tutulduğu, TTK' nun 1435. maddesi gereğince de sigorta ettirenin sözleşmenin yapılması sırasında bildiği veya bilmesi gereken tüm önemli hususları sigortacıya bildirmekle yükümlü olduğu, sigortacıya bildirilmeyen, eksik veya yanlış bildirilen hususlar, sözleşmenin yapılmamasını veya değişik şartlarda yapılmasını gerektirecek nitelikte olduğu takdirde önemli kabul edildiği, aynı yasanın 1440 maddesi gereğince böyle bir durumda sigorta şirketinin belirtilen süre içinde sözleşmeden cayabileceği ya da prim farkı isteyebileceği, yine 09.08.2008 tarihli Sigorta Bilgi ve Gözetim Merkezi Yönetmeliğinin 14.maddesine göre; Sağlık Sigortaları Bilgi ve Gözetim Merkezinin amacının sağlık ve hastalık branşları altında sunulan sigorta ürünlerine ilişkin güvenilir istatistiklerin üretilmesi, kamu gözetim ve denetiminin daha etkin bir şekilde yerine getirilmesi olduğu, üye sigorta şirketlerinin sağlık ve hastalık branşlarında düzenledikleri sigorta sözleşmelerine ilişkin kayıtların en çok bir gün gecikmeyle

tutulduğu bir veri tabanı oluşturmak, sigortalıya ait kayıtları üye sigorta şirketlerine bedelsiz olarak vermek, üye sigorta şirketlerinin Merkez nezdinde oluşturulan veri tabanında bilgileri tutulan sigortalılara ilişkin uygulamalarını takip etmek, Merkez nezdinde oluşturulan veri tabanında bilgileri tutulan sigortalılara ilişkin tarifelerin oluşturulmasını teminen çalışmalar yapmak ve bu çalışmaları Müsteşarlığa ve Birliğe göndermek görevinin bu merkeze verildiği, davacının imzalamış olduğu grup sağlık sigortası başvuru formu ile davalı sigorta şirketini sağlık kuruluşları, sigorta şirketleri yada idari ve resmi tüm kuruluşlardan bilgi almaya ve vermeye yetkili kıldığı, davacının kendisinde daha önce var olan rahatsızlıklar nedeniyle davalının poliçeye muafiyet koymasının olanaklı olduğu, sigorta şirketinin sigortalısında var olan hastalıkları poliçeye yazmış olduğu özel şart ile kapsam dışında bırakabileceği anlaşılmıştır.

Sonuç olarak davalıların eylemleri haksız fiil niteliğinde değildir, ortada hukuka aykırı bir fiil, kanıtlanmış bir zarar da yoktur. Maddi ve manevi tazminat koşulları da oluşmamıştır. Dosya kapsamında yer alan dört bilirkişiden oluşan heyet raporunda da belirlendiği üzere, davalının sigortalısında var olan hastalıkları poliçeye yazmış olduğu özel şart ile kapsam dışında bırakmasında hukuka aykırılık da yoktur. Yine davacı vekilinin iddiasının aksine temelde bilirkişi raporları arasında bir çelişki yoktur. Zira ilk bilirkişi raporunda da sigorta ettirenin verdiği bir onam olmaması halinde kişinin özel tıbbi bilgilerinin edinilmesinin hukuka aykırı olduğu belirlenmiştir.

Açıklanan gerekçelerle ilk derece mahkemesinin kararında usul ve yasaya aykırı bir yön bulunmadığından sonuç olarak; dosya kapsamı, delil durumu, ilk derece mahkemesi kararında mahkemenin vakıa ve hukuki değerlendirmesi bakımından usul ve esas itibariyle yasaya aykırı bir durum bulunmamasına göre, davacı vekilinin istinaf başvurusunun Hukuk Muhakemeleri Kanununun 353/1-b.1 maddesi gereğince esastan reddine karar vermek gerekmiştir. Bu itibarla aşağıdaki hüküm kurulmuştur.

HÜKÜM: Gerekçesi yukarıda açıklandığı üzere;

- 1- İstanbul 9. Asliye Ticaret Mahkemesinin 2014/1180 Esas, 2017/1117 Karar sayılı kararı usul ve yasaya uygun olduğundan davacının istinaf başvurusunun REDDİNE,
- 2- Davacı tarafca yatırılan istinaf karar harcının mahsubuna, başkaca harç alınmasına yer olmadığına,
- 3- Davacı tarafından yapılan istinaf başvuru giderlerinin üzerinde bırakılmasına,
- 4- Harcanmayan avansın karar kesinleştiğinde yatırana iadesine,

Dosya üzerinde yapılan inceleme sonunda, HMK'nun deęişik 361/1 maddesi uyarınca kararın teblięinden itibaren iki hafta içinde Yargıtay'a temyiz yolu açık olmak üzere oy birlięi ile karar verildi.

27/11/2017

İstanbul Bölge Adliye Mahkemesi, 23. HD., E. 2017/596 K. 2017/527 T. 31.3.2017

Esas No.: 2017/596

Karar No.: 2017/527

Karar Tarihi: 31.03.2017

TÜRK MİLLETİ ADINA

Yukarıda ayrıntıları belirtilen mahkeme kararının süresi içinde istinafen incelenmesi davacı/alacaklı tarafından talep edilmekle, görevlendirilen Üye Hakim tarafından hazırlanan ön inceleme ve inceleme raporu dinlendikten ve dosya içerisindeki tüm belgeler okunup incelendikten sonra heyetçe yapılan müzakere sonucunda duruşma açılmaksızın gereği görüşülüp düşünüldü:

Davacı vekili dava dilekçesinde, icra müdürlüğünden borçlunun pasif tapu kaydı sorgusu yapılmasını talep ettiklerini, borçlu şirket hakkında pasif tapu kaydı çıktığını ancak müdürlükçe taşınmazların hangi tarihte kime ne bedelle satıldıklarının sorulması taleplerinin reddedildiğini belirterek icra müdürlüğü işleminin iptalini talep etmiş, mahkemece davanın reddine karar verilmesi üzerine davacı tarafından dava dilekçesindeki sebeplerle istinaf isteminde bulunmuştur.

İcra dosyasının tarafı olmayan üçüncü kişiye ait 6698 Sayılı Yasa'nın 3/1-d maddesi kapsamında kişisel veri niteliğinde bulunan tapu kaydı ve satış sözleşmelerinin icra müdürlüğünce celbinin istenemeyeceği, aynı Yasanın 28/1-d maddesindeki yargısal organlara tanınan istisnanın, ancak uyuşmazlığın tarafları açısından geçerli olabileceği, Anayasa'nın 20/3. maddesine göre aynı zamanda temel haklardan olan kişisel verilerin korunmasını isteme hakkının, 6698 Sayılı Yasanın 28/1-d maddesinin geniş yorumlanması ile daraltılamayacağı, mülkiyet hakkının korunması zımında açılacak bir davanın taraflarını tespit edebilmek için 1136 sayılı Avukatlık Kanununun 2/3. maddesine ve Başbakanlık Tapu Kadastro Genel Müdürlüğünün 2001/11 sayılı Genelgesine göre avukatın yazılı başvuru ile tapu sicilinde inceleme yapabileceği ve kanunda kısıtlı olarak öngörülen kişisel verilere ulaşma imkanının bu şekilde sağlanması ile hukuki denetimin de yapılabileceği bu verilere ulaşma imkanının birden fazla yolla sağlanması halinde, verilere kimlerin ulaştığının denetiminin zorlaşacağı nazara alınarak, icra müdürlüğü kararının isabetli olduğu, alacaklının hukuki menfaatinin, 3. şahısların Anayasa ile korunan özel hayatın gizliliğine ilişkin temel hakkından üstün tutulmasının

mümkün olmadığı, belirtilen nedenlerle ilk derece mahkemesinin kararının usul ve yasaya uygun olduğu anlaşıldığından davacının istinaf talebinin esastan reddine karar vermek gerekmiştir.

HÜKÜM: Gerekçesi yukarıda açıklandığı üzere;

1- İstanbul 5. İcra Hukuk Mahkemesi'nin 2017/145 Esas ve 2017/131 Karar sayılı 07.02.2017 tarihli kararında sonucu itibariyle usul ve yasaya aykırılık bulunmadığından, davacının istinaf başvurusunun HMK 353/1-b-1. bendi gereğince ESASTAN REDDİNE,

2- İstinaf harçları peşin olarak alındığından ve yeterli görüldüğünden, yeniden harç alınmasına yer olmadığına,

Dair, dosya üzerinde yapılan inceleme ve müzakere neticesinde, istinafa konu ihtilaf dava değeri dikkate alınarak İİK' nın 364. maddesi gereğince KESİN olmak üzere oy birliğiyle karar verildi.31/03/2017

İzmir BAM - 12. Hukuk Dairesi (E. 2019/2210)

İzmir Bölge Adliye Mahkemesi, 12. HD., E. 2019/2210 K. 2020/1208 T. 7.7.2020

Esas No.: 2019/2210

Karar No.: 2020/1208

Karar Tarihi: 07.07.2020

İSTİNAF KARARI

DAVANIN KONUSU: Şikayet (İcra Memur Muamelesi)

İlk Derece Mahkemesi tarafından verilen karara karşı süresinde istinaf kanun yoluna başvurulması üzerine dosya incelendi, gereği görüşülüp düşünüldü;

DAVA: Davacı vekili dava dilekçesinde özetle; İzmir 18. İcra Müdürlüğünün 2016/15982 Esas sayılı dosyasının 02/12/2016 tarihinde açılmış olduğunu, tebligatın 10/03/2017 tarihinde borçlu K1'e 21.mad. göre muhtara teslim edilerek kesinleştiğini, icra dosyasında ve ticari çevrede yaptıkları talepleri gereği borçlunun, borcu karşılayabilecek taşınır taşınmaz mal varlığının araştırılması sonucunda taşınır hiçbir mal varlığına rastlanmadığını, sadece taşınmaz mal varlığı olarak tespit edilen İzmir, Tire, A1 Mah., A2 mevkii, 614 nolu parselde 414 m2 olarak avlulu kargir dam niteliğindeki 20.000,00-TL değerindeki taşınmazı üzerinde 200.000,00 TL'ye yakın haciz şerhi bulunduğu görüldüğünü, düşük kıymet nedeniyle borcun anılan taşınmazdan tahsili kabiliyetinin olmadığını, borçlunun çevresine çok büyük borçları olduğunu ve kötü niyetli olarak üzerindeki malı aile fertleri üzerine kaçırdığı duyumları almaları nedeniyle, 09/09/2019 tarihinde YMK.nun 202-210 ve ilgili sair maddeleri gereğince icra dosyasında yaptıkları taleplerinde borçlu- K1'in üst ve alt soyunu gösterir meşruhatlı aile nüfus tablosunun UYAP aracılığıyla çıkarılarak, bir örneğinin dosya içerisine alınmasına, baba hanesinden meşruhatlı çıkartılan nüfus aile tablosuna göre babasının ve annesinin vefat etmesi durumunda, murisinden borçlu üzerine mirasen intikal edebilecek mal varlığının olup olmadığının sorgulanmasına, mal kaçırma ihtimaline binaen, 01/01/2002 tarihinde yürürlüğe giren YMK.nun 202-210 ve ilgili sair maddeleri gereğince borçlunun eşi ve tasarrufun yapıldığı reşit olmayan çocukları adına 01/01/2002 tarihinden sonra edinilmiş veya borçludan devrolan taşınır veya taşınmaz kayıtlarının olup olmadığının araştırılmasına karar verilmesini istediklerini, ancak İzmir 18.İcra Müdürlüğünün 10/09/2019 gün ve 2016/15982E.nosuyla," Alacaklı vekilinin muris mal varlığı, pasif tapu sorgusu ve borçlu dışındaki ilgililere yönelik tüm taleplerinin reddine " karar verildiğini,

verilen kararın yasal dayanağının olmadığını, 4721 s. y.nın 210 .md. “Mal ortaklığını kabul etmiş eşlerden birine karşı icra takibinde bulunan alacaklı, haczin uygulanmasında zarara uğrarsa, hakimden mal ayrılığına karar vermesini isteyebilir.....”denildiğini, bu kapsamda Aile Mahkemesinden alınacak kararlar 01/01/2002 tarihinden itibaren eşler arasındaki mal ortaklığı rejiminin iptal edilerek, mal ayrılığı rejimine dönüştürülüp ½ oranındaki borçlu eşin hissesi üzerinden borçların tahsili veya bu dönemde reşit olmayan çocukları adına alınan malların üzerinden borçların tahsili imkanı bulunduğundan dolayı İzmir 18.İcra Müdürlüğünün 2016/15982 E. nolu dosyasında borçlu eşi veya tasarruf sırasında reşit olmayan çocuğunun üzerine geçirilen mal varlığının veya anne babasından mirasın gelip henüz adına tescil edilmemiş mal varlıklarının bilgi mahiyetinde dökümünün öğrenilmesi doğrultusunda 09/09/2019 tarihinde yaptıkları taleplerin reddine ilişkin kararın iptaline, 09/09/2019 tarihinde bilgi edinme amacıyla yaptıkları taleplerinin kabul edilerek borçlu K1’in, meşruhatlı aile tablosundan kimliği tespit edilecek eşinin ve 01/01/2002 tarihinden sonra tasarruf sırasında reşit olmayan çocuklarının adına alınan veya borçlu tarafından bu kişiler üzerine geçirilmiş mal varlığının, baba veya annesinin ölümü halinde varsa halen tapuda borçlu üzerine geçişi yapılmamış olan malvarlığının tespiti için alt ve üst soydan meşruhatlı aile nüfus tablosunun çıkartılarak, eş, çocuk, anne, baba adına taşınır taşınmaz dökümünün tespit edilerek buna dair bilgilerin taraflarına verilmesine karar verilmesini talep etmiştir.

CEVAP: Dava hasımsız açılmıştır.

İLK DERECE MAHKEMESİ KARARI: İzmir 10. İcra Hukuk Mahkemesince yapılan yargılama neticesinde, şikayetin reddine karar verilmiştir.

İSTİNAF SEBEPLERİ: Davacı vekili istinafa başvuru dilekçesinde özetle; dava dilekçesindeki beyanlarını tekrar ederek, borçlunun eşinin, reşit olmayan çocuklarının, anne ve babasından mirasın gelip henüz borçlu adına tescil edilmemiş mal varlığının taraflarınca haricen tespit edilemediğini, bu kapsamda aile mahkemesinden alınacak kararlar 01/01/2002 tarihinden itibaren eşler arasındaki mal ortaklığı rejiminin iptal edilerek, mal ayrılığı rejimine dönüştürülüp 1/2 oranındaki borçlu eşin hissesi üzerinden borçların tahsili veya bu dönemde reşit olmayan çocukları adına alınan malların üzerinden borçların tahsili imkanı bulunduğunu, bu konudaki taleplerinin icra müdürlüğüne reddedilmesinin ve mahkemece şikayetin reddine karar verilmesinin usul ve yasaya aykırı olduğunu ileri sürerek, istinaf isteminin kabulü ile ilk derece mahkemesi kararının kaldırılmasına, şikayetin kabulüne karar verilmesini talep ve istinaf etmiştir.

GEREKÇE: İzmir 18. İcra Müdürlüğünün 2016/15982 esas sayılı dosyasının incelenmesinde, şikayetçi-alacaklı tarafından borçlu K1 aleyhine kambyo senetlerine mahsus haciz yolu ile ilamsız 10

örnek icra takibi başlatıldığı, ödeme emrinin borçluya 10/03/2017 tarihinde tebliğ edildiği, alacaklı vekili tarafından 10/09/2019 tarihinde, "borçlunun üst ve alt soyunu gösterir aile nüfus tablosunun UYAP aracılığıyla çıkarılarak, bir örneğinin dosya içerisine alınması için gereğinin yapılmasına, baba hanesi ile birlikte meşruhatlı nüfus aile tablosunun çıkartılarak, baba ve anne isimleri üzerinden mirasen mal intikalinin olup olmadığının sorgulanmasına, mal kaçırma ihtimaline binaen tapu kayıtlarının borçlunun eşi adına ve çocukları adına 01/01/2002 tarihinden sonra edinilmiş, borçludan devrolan taşınır veya taşınmaz kayıtlarının olup olmadığının araştırılmasına" şeklinde talepte bulunulduğu, icra müdürlüğü tarafından 10/09/2019 tarihinde alacaklı vekilinin talebinin "alacaklı vekili her ne kadar borçlunun murisinin dosyaya taraf olarak eklenmesini ve mal varlığı sorgulamasını talep etmiş ise de; (Yargıtay 12.Hukuk Dairesi Başkanlığının 05.05.2016 tarih ve 2015/33810 Esas 2016/13366 Karar sayılı ilamı) borçlu dışında kalan aile efradından olan anne, baba ve eşin nüfus kaydının alınarak ölü olup olmadıkları ve ölmüş iseler dosyaya taraf kaydederek mal varlığı sorgulamasının ve araştırmasının yapılmasının icra dosyası ile ilgisi olmayan üçüncü kişiler yönünden uygulanmasının mümkün olmadığı, nüfus kaydı ve diğer sorgulama işlemlerinin hakkında takip kesinleşen borçlular yönünden uygulanacağı, 3.kişiler ile ilgili yapılacak sorgulamaların Anayasa'nın 20. maddesinde düzenlenen temel hak ve hürriyetlere aykırılık oluşturduğu, kişisel verilerin gizliliğinin güvence altına alındığı, takip ile ilgisi bulunmayan borçlu durumunda olmayan kişilerin kişisel kimlik bilgileri ile durumlarının araştırılmasının İcra Müdürlüğü'nün görevleri kapsamında bulunmadığı, alacaklı vekilince borçlunun murislerinin ölmüş olduğunun bildirilmesi ve taşınmaz/taşınır bilgilerinin sunulması halinde İİK'nun 94. maddesi gereğince işlem yapılabileceğinin aşikar olduğundan tüm bu nedenlerle alacaklı vekilinin talebinin reddine karar verilmiştir." gerekçesi ile reddine karar verildiği görülmüştür.

Dava; memur muamelesini şikayete yöneliktir.

Konu ile ilgili mevzuat hükümleri incelendiğinde,

TC Anayasası madde 13: Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.

TC Anayasası madde 20/3: Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya

kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.

Avrupa İnsan Hakları Sözleşmesi madde 8: 1-Herkes, özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

2- Bu hakkın kullanımına, yasa/hukuk uyarınca olması ve ulusal güvenlik, kamu emniyeti ya da ülkenin ekonomik refahı, düzensizliğin ya da suçun önlenmesi, sağlığın ya da ahlakın korunması ya da başkalarının haklarının ve özgürlüklerinin korunması için demokratik toplumda gerekli olması hali istisna olmak üzere, bir kamu makamı tarafından bulunulmayacaktır.

Nüfus Hizmetleri Kanunu madde 9:1-Nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Bunlar, yetkili ve sorumlu memurlar ile teftiş ve denetim yetkisi olanlar dışında kimse tarafından görülüp incelenemez. Mahkemeler bu hükmün dışındadır.

2- Nüfus kayıtlarına bu bilgileri işleyen memurlar ve Kimlik Paylaşımı Sistemi kapsamında nüfus kayıtlarından faydalanan diğer görevliler de bu gizliliğe uymak zorundadırlar. Bu yükümlülük, kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam eder.

Madde 44: 1- Nüfus kayıt örneklerini;ç) Adli makamlar,nüfus müdürlüklerinden doğrudan almaya yetkilidirler.

Kişisel Verilerin Korunması Kanunu madde 3/1- d)Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

Madde 3/1-e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

Madde 5:1- Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

2- Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

- c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- e) Bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması.
- f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Madde 28:1-Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:....d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi, düzenlemelerine rastlanmaktadır.

Yukarıda yer verilen mevzuat hükümlerine göre kişinin nüfus kaydının kişisel veri niteliğinde olduğu tartışmasızdır. (Kişisel Verilerin Korunması Kanunu madde 3/1-d) Kişisel verilerin tamamen veya kısmen elde edilerek kaydedilmesi ise kişisel verilerin işlenmesidir. (Kişisel Verilerin Korunması Kanunu madde 3/1-e) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (Kişisel Verilerin Korunması Kanunu madde 5) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenebilmesi ise bu kuralın istisnasıdır.(Kişisel Verilerin Korunması Kanunu madde 28/1-d) Kişisel veri olduğu açık olan nüfus kaydına ilişkin bir başka düzenleme olan Nüfus Hizmetleri Kanununun 9. maddesine göre ise nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Tüm bu hususlardan açıkça anlaşıldığı üzere kişisel veriler ve bu bağlamda nüfus kayıtları gizlidir, edinilip kaydedilmeleri ilgili kişinin açık rızasına bağlıdır ve bu durum gerek Anayasa, gerek Avrupa İnsan Hakları Sözleşmesi ve gerekse kanunlarla düzenlenerek koruma altına alınmıştır.

Somut olayda; icra dosyasında borçlu sıfatı bulunmayan şahısların malvarlığına haciz uygulanamayacağından ve 3.şahısların malvarlığı ile ilgili araştırma yapılamayacağından icra memurluğu tarafından borçlunun eşi ve çocukları yönünden verilen red kararında usul ve yasaya aykırı bir husus bulunmadığı, alacaklı vekili tarafından 11.05.2017 tarihinde yapılan talep üzerine borçlunun babasından intikal edecek mal varlığı üzerine haciz uygulanmasına karar verildiği, ancak uygulanan bir haczin bulunmadığı, borçlunun babasının nüfus kaydının dosyada mevcut olduğu, yine alacaklı vekilinin 01.08.2017 tarihindeki talebi üzerine borçlunun aktif ve pasif mal varlığı sorgusunun yapılmış olduğu, annesi ile ilgili olarak bir araştırma yapılmadığı ancak doğrudan borçlu olmayan şahısların icra dosyasına borçlu sıfatı ile eklenerek bu şahısların tüm mal varlıklarının araştırılmasının

kişisel verilerin gizliliğine aykırılık teşkil edeceği anlaşıldığından alacaklı tarafın taleplerinin doğrudan üçüncü şahısların mal varlığına yönelik olması sebebi ile icra memurluğunca verilen red kararında ve mahkemece şikayetin reddine karar verilmiş olmasında bir isabetsizlik görülmemiş, davacı vekilinin istinaf başvurusunun esastan reddine karar verilmiştir.

HÜKÜM: Yukarıda açıklanan nedenlerle;

İzmir 10. İcra Hukuk Mahkemesi'nin 30/09/2019 tarihli, 2019/789 Esas, 2019/773 Karar sayılı kararına yönelik istinaf başvurusunun Hukuk Muhakemeleri Kanununun 353/1- b. 1 maddesi gereğince ESASTAN REDDİNE,

Alınması gerekli 54,40-TL istinaf karar harcından peşin alınan 44,40-TL'nin mahsubu ile bakiye 10,00-TL harcın davacıdan alınarak hazineye irat kaydına,

İstinaf kanun yolu yargılama giderlerinin istinaf eden üzerinde bırakılmasına,

HMK 333. madde gereğince kararın kesinleşmesinden sonra kullanılmayan gider avansının yatırana iadesine,

Kararın taraflara tebliğine,

Dair, dosya üzerinde yapılan inceleme sonucunda 6100 sayılı HMK 'nun 361 maddesi uyarınca kararın tebliğinden itibaren iki hafta içerisinde Yargıtay'a temyiz yolu açık olmak üzere oy birliği ile karar verildi. 07/07/2020

İzmir Bölge Adliye Mahkemesi, 12. HD., E. 2019/2033 K. 2020/1101 T. 26.6.2020

Esas No.: 2019/2033

Karar No.: 2020/1101

Karar Tarihi: 26.06.2020

İSTİNAF KARARI

DAVANIN KONUSU: Şikayet (İcra Memur Muamelesi)

İlk Derece Mahkemesi tarafından verilen karara karşı süresinde istinaf kanun yoluna başvurulması üzerine dosya incelendi, gereği görüşülüp düşünüldü;

DAVA: Şikayetçi vekili şikayet dilekçesinde özetle; müvekkili bankanın alacağı tahsili amacıyla İzmir 24. İcra Müdürlüğü'nün 2017/3203 Esas sayılı dosyasında K1 hakkında ilamsız icra takibi başlatıldığını, hakkında alınmış olan ihtiyati haciz kararı çerçevesinde borçlu adına kayıtlı iken devri yapılmış olan pasif taşınmazların sorgusunun talep edildiğini ve taleplerinin kabul edilerek yapılan sorgulama neticesinde 4 adet taşınmazın borçlu tarafından devredildiğinin tespit edildiğini, icra müdürlüğüne borçlu K1 tarafından devredilen gayrimenkullerin devir aşamalarını ve sadece kimlere devredildiğini gösteren pasif tapu takyidat ve resmi senet örneklerinin Tapu Müdürlüğünden istenmesi talebinin ise reddine karar verildiğini, borçlu adına kayıtlı olup ta icra takibinden önce devri yapılan taşınmazların sorgulamalarının nedeninin İİK 277 ve devamında düzenlenmiş olan tasarrufun iptali davası açmak suretiyle iptalini talep ve nihayetinde alacağı tahsil etmek olduğunu beyanla şikayetin kabulü ile 16/07/2019 tarihli müdürlük işleminin iptaline karar verilmesini talep etmiştir.

CEVAP: Dava hasımsız açılmıştır.

İLK DERECE MAHKEMESİ KARARI: İzmir 2.İcra Hukuk Mahkemesince yapılan yargılama neticesinde şikayetin reddine karar verilmiştir.

İSTİNAF SEBEPLERİ: Davacı vekili istinaf başvuru dilekçesinde özetle; dava dilekçesindeki hususları aynen tekrar etmiş, alacaklı vekili sıfatıyla borçlu K1 hakkında başlattıkları takibin kesinleştiğini, İİK çerçevesinde borçlu adına kayıtlı iken devri yapılmış olan pasif taşınmazların sorgulanması neticesinde 4 adet taşınmazın borçlu tarafından bankadan kredi kullandıktan sonra ve hakkında icra takip işlemleri başlamadan hemen önce devredildiğinin tespit edildiğini, tespit edilen

taşınmazların devir aşamalarını ve kimlere devredildiğini gösteren pasif tapu takyidat örneklerinin tapu müdürlüğünden istenmesi talebinin hukuka ve kanuna aykırı olarak Kişisel Verilerin Korunması Kanunu'na aykırı olduğu belirtilerek reddedildiğini, bu işlemin usul ve yasaya aykırı olduğunu, bu kararın doğru kabul edilmesi halinde İİK 'da düzenlenmiş ve etkili bir tahsilat mekanizması olan tasarrufun iptali davasının işletilemeyeceğini beyanla istinaf başvurusunun kabulü ile ilk derece mahkemesinin kararının kaldırılmasına karar verilmesini talep etmiştir.

GEREKÇE: Alacaklı şikayetçi tarafından borçlu K1 aleyhine ilamsız icra yoluyla icra takibi başlatıldığı, örnek 7 ödeme emrinin borçluya tebliğinden sonra takibin kesinleştiği, alacaklı vekili tarafından talep edilmesi üzerine borçlu adına kayıtlı iken devri yapılmış olan pasif taşınmazların sorgulamasının icra müdürlüğünce yapılmış olduğu, alacaklı vekilinin borçlu adına kayıtlı olup ta icra takibinden önce devri yapılan taşınmazların devir aşamaları ve kimlere devredildiğini gösteren pasif tapu takyidat örneklerinin tapu sicil müdürlüğünden istenmesini talep ettiği, 16/07/2019 tarihinde icra müdürlüğü tarafından alacaklı vekilinin 3.kişilere devredilmiş olan taşınmazların devir işlemlerine ilişkin tapu kaydı ve satış sözleşmelerinin takip dosyasına istenilmesi yönündeki talebin reddine karar verildiği görülmüştür.

Dava; memur muamelesini şikayete yöneliktir.

Konu ile ilgili mevzuat hükümleri incelendiğinde,

TC Anayasası madde 13: Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.

TC Anayasası madde 20/3: Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.

Avrupa İnsan Hakları Sözleşmesi madde 8: 1-Herkes, özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

2-Bu hakkın kullanımına, yasa/hukuk uyarınca olması ve ulusal güvenlik, kamu emniyeti ya da ülkenin ekonomik refahı, düzensizliğin ya da suçun önlenmesi, sağlığın ya da ahlakın korunması ya

da başkalarının haklarının ve özgürlüklerinin korunması için demokratik toplumda gerekli olması hali istisna olmak üzere, bir kamu makamı tarafından bulunulmayacaktır.

Nüfus Hizmetleri Kanunu madde 9: 1-Nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Bunlar, yetkili ve sorumlu memurlar ile teftiş ve denetim yetkisi olanlar dışında kimse tarafından görülüp incelenemez. Mahkemeler bu hükmün dışındadır.

2-Nüfus kayıtlarına bu bilgileri işleyen memurlar ve Kimlik Paylaşımı Sistemi kapsamında nüfus kayıtlarından faydalanan diğer görevliler de bu gizliliğe uymak zorundadırlar. Bu yükümlülük, kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam eder.

Madde 44: 1- Nüfus kayıt örneklerini;ç) Adli makamlar,nüfus müdürlüklerinden doğrudan almaya yetkilidirler.

Kişisel Verilerin Korunması Kanunu madde 3/1-d)Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

Madde 3/1-e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

Madde 5:1- Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

2- Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

- a) Kanunlarda açıkça öngörülmesi.
- b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
- c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Madde 28:1-Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:....d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi, düzenlemelerine rastlanmaktadır.

Yukarıda yer verilen mevzuat hükümlerine göre kişinin nüfus kaydının kişisel veri niteliğinde olduğu tartışmasızdır. (Kişisel Verilerin Korunması Kanunu madde 3/1-d) Kişisel verilerin tamamen veya kısmen elde edilerek kaydedilmesi ise kişisel verilerin işlenmesidir. (Kişisel Verilerin Korunması Kanunu madde 3/1-e) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (Kişisel Verilerin Korunması Kanunu madde 5) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenebilmesi ise bu kuralın istisnasıdır.(Kişisel Verilerin Korunması Kanunu madde 28/1-d) Kişisel veri olduğu açık olan nüfus kaydına ilişkin bir başka düzenleme olan Nüfus Hizmetleri Kanununun 9. maddesine göre ise nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Tüm bu hususlardan açıkça anlaşıldığı üzere kişisel veriler ve bu bağlamda nüfus kayıtları gizlidir, edinilip kaydedilmeleri ilgili kişinin açık rızasına bağlıdır ve bu durum gerek Anayasa, gerek Avrupa İnsan Hakları Sözleşmesi ve gerekse kanunlarla düzenlenerek koruma altına alınmıştır.

Somut olayda davacı alacaklı vekilince icra müdürlüğünden sadece takip borçlusuna ait pasif tapu kayıtlarının celp edilmesi talep edilseydi bu talebin reddedilmesinin yukarıda ki anlatımlar ve mevzuat doğrultusunda usulüne uygun olmayacağı, nitekim borçlunun varsa pasif taşınmaz kayıtlarının sorgulanmasının , alacaklının bu yöndeki bir bilgiye kendisi ulaşamayacağından ve bu talebin yerine getirilmesi halinde ulaşacağı pasif taşınmaz kaydı vasıtası ile örneğin tasarrufun iptali gibi bir dava açarak alacağına kavuşma imkanına sahip olabileceğinden, pasif tapu kaydı sorgulamasında ulaşılacak bilginin borçlu adına daha önce kayıtlı bulunan taşınmaz bilgisi olup bu bilginin bu taşınmazın şimdiki maliki hakkında herhangi bir bilgi içermeyeceği, bu nedenle bu kaydın dosyaya dahil edilmesi, borçlu dışındaki herhangi bir 3.kişinin bilgilerinin dosyaya yansımaları sonucunu doğurmayacağı gibi borcun tahsili için imkan sağlayabileceğinden pasif tapu kaydı istenmesinde alacaklının haklı menfaati bulunduğu, dosya kapsamına göre davacı alacaklı vekilince daha önce borçlu adına kayıtlı iken devri yapılmış olan pasif taşınmazların sorgulanmasının talep olduğu ve icra müdürlüğünce pasif taşınmazların sorgulamasının yapıldığı, davacı alacaklı vekilinin daha sonra ise taşınmazların devrine ilişkin bilgilerin celbini talep ettiği, bu durumun takipte taraf olmayan yeni maliklere ilişkin kişisel verilerin dosyaya celp edilmesi gibi bir sonuç

doğuracağından icra müdürlüğünün şikayete konu işleminin usul ve yasaya uygun olduğu, dolayısıyla ilk derece mahkemesince verilen kararda herhangi bir isabetsizlik bulunmadığı anlaşılmış, davacı vekilinin yerinde görülmeyen istinaf başvurusunun esastan reddine karar vermek gerekmiştir.

HÜKÜM: Yukarıda açıklanan nedenlerle;

1- İzmir 2. İcra Hukuk Mahkemesi'nin 15/08/2019 tarihli, 2019/560 E. ve 2019/651 K. sayılı kararına yönelik istinaf başvurusunun Hukuk Muhakemeleri Kanununun 353/1- b. 1 maddesi gereğince ESASTAN REDDİNE,

2- Alınması gerekli 54,40 TL İstinaf karar harcından peşin alınan 44,40 TL'nin mahsubu ile bakiye 10,00 TL harcın istinaf edenden tahsili ile hazineye irat kaydına,

3- İstinaf kanun yolu yargılama giderlerinin, istinaf eden üzerinde bırakılmasına,

4- Kararın taraflara tebliğine,

5- HMK 333. madde gereğince kararın kesinleşmesinden sonra kullanılmayan gider avansının yatırana iadesine,

Dair, dosya üzerinde yapılan inceleme sonucunda 6100 sayılı HMK 'nun 361 maddesi uyarınca kararın tebliğinden itibaren iki hafta içerisinde Yargıtay'a temyiz yolu açık olmak üzere oy birliği ile karar verildi. 26/06/2020

İzmir Bölge Adliye Mahkemesi, 12. HD., E. 2019/1873 K. 2020/737 T. 15.5.2020

Esas No.: 2019/1873

Karar No.: 2020/737

Karar tarihi: 15.05.2020

İSTİNAF KARARI

DAVA: ŞİKAYET

İlk Derece Mahkemesi tarafından verilen karara karşı süresinde istinaf kanun yoluna başvurulması üzerine dosya incelendi.

DAVA: Davacı vekili dava dilekçesinde özetle: müvekkili bankanın alacağı tahsili amacıyla başlattıkları İzmir 13. İcra Müdürlüğü'nün 2016/9237 esas sayılı takip dosyasında dava dışı borçlu K1'a ait olduğu tespit edilen 3 adet taşınmazın pasif tapu kayıtlarının celbi için icra müdürlüğünden talepte bulduklarını, ancak icra müdürlüğünce şikayete konu 07/01/2019 tarihli pasif taşınmaz kayıtlarının celbi talebinin reddine karar verildiğini, verilen kararın usul ve yasaya uygun olmadığından bahisle memur işleminin iptaline karar verilmesini talep ve dava etmiştir.

CEVAP: Dava hasımsız açılmış, mahkemece evrak üzerinden karar verildiği görülmüştür.

İLK DERECE MAHKEMESİ KARARI: İzmir 11. İcra Hukuk Mahkemesince yapılan yargılama neticesinde şikayetin reddine verilmiştir.

İSTİNAF SEBEPLERİ: Davacı vekili istinaf başvuru dilekçesinde özetle; ilk derece mahkemesi kararının usul ve yasaya aykırı olduğunu, icra müdürlüğünden takip borçlusuna ait pasif tapu kaydı ile birlikte taşınmazların hangi tarihte, kime satıldığına ilişkin belgelerin istenmesinin amacının, söz konusu satışların gerçek satış olup olmadığı ve ne kadar bedelle satıldığı hususlarının anlaşılabilmesi, ayrıca aşırı bedel farklarının varsa tespit edilebilmesi için önem arz ettiğini, bu belgelerin istenmesinde alacaklı müvekkilinin haklı menfaati bulunduğu gibi pasif kayıtların celbinin kişisel verileri de etkilemediğini, bu nedenlerle ilk derece mahkemesi kararının kaldırılarak, şikayetin kabulüne, memur işleminin iptaline karar verilmesini talep etmiştir.

GEREKÇE: Dava konusu İzmir 13. İcra Müdürlüğü'nün 2016/9237 Esas sayılı dosyasının incelemesinde: alacaklının davacı F1bank T.A.Ş. , borçlunun K1 olduğu, 10/06/2016 tarihli 7 örnek

örnek ödeme emri ile, 184.920,00- TL asıl alacak üzerinden ilamsız icra takibi yapıldığı, alacaklı vekilinin 04/01/2019 tarihli 3 adet taşınmazın pasif kayıtlı olarak borçlu adına tesbit edildiğini, pasif kayıtlı taşınmazların hangi tarihte kime satıldığı, satışa ilişkin evrak örneklerinin celbine ilişkin talebinin icra müdürlüğüne 07/01/2019 tarihli kararı ile reddedildiği, şikayete konu işlemin bu olduğu anlaşılmıştır.

Dava; memur muamelesini şikayete yöneliktir.

Konu ile ilgili mevzuat hükümleri incelendiğinde

TC Anayasası madde 13: Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.

TC Anayasası madde 20/3: Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.

Avrupa İnsan Hakları Sözleşmesi madde 8: 1-Herkes, özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

2-Bu hakkın kullanımına, yasa/hukuk uyarınca olması ve ulusal güvenlik, kamu emniyeti ya da ülkenin ekonomik refahı, düzensizliğin ya da suçun önlenmesi, sağlığın ya da ahlakın korunması ya da başkalarının haklarının ve özgürlüklerinin korunması için demokratik toplumda gerekli olması hali istisna olmak üzere, bir kamu makamı tarafından bulunulmayacaktır.

Nüfus Hizmetleri Kanunu madde 9: 1-Nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Bunlar, yetkili ve sorumlu memurlar ile teftiş ve denetim yetkisi olanlar dışında kimse tarafından görülüp incelenemez. Mahkemeler bu hükmün dışındadır.

2-Nüfus kayıtlarına bu bilgileri işleyen memurlar ve Kimlik Paylaşımı Sistemi kapsamında nüfus kayıtlarından faydalanan diğer görevliler de bu gizliliğe uymak zorundadırlar. Bu yükümlülük, kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam eder.

Madde 44:1- Nüfus kayıt örneklerini;ç) Adlî makamlar,nüfus müdürlüklerinden doğrudan almaya yetkilidirler.

Kişisel Verilerin Korunması Kanunu madde 3/1-d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

Madde 3/1-e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

Madde 5: 1- Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

2- Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Madde 28:1-Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:....d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi,

düzenlemelerine rastlanmaktadır.

Yukarıda yer verilen mevzuat hükümlerine göre kişinin nüfus kaydının kişisel veri niteliğinde olduğu tartışmasızdır. (Kişisel Verilerin Korunması Kanunu madde 3/1-d) Kişisel verilerin tamamen

veya kısmen elde edilerek kaydedilmesi ise kişisel verilerin işlenmesidir. (Kişisel Verilerin Korunması Kanunu madde 3/1-e) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (Kişisel Verilerin Korunması Kanunu madde 5) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenebilmesi ise bu kuralın istisnasıdır.(Kişisel Verilerin Korunması Kanunu madde 28/1-d) Kişisel veri olduğu açık olan nüfus kaydına ilişkin bir başka düzenleme olan Nüfus Hizmetleri Kanununun 9. maddesine göre ise nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Tüm bu hususlardan açıkça anlaşıldığı üzere kişisel veriler ve bu bağlamda nüfus kayıtları gizlidir, edinilip kaydedilmeleri ilgili kişinin açık rızasına bağlıdır ve bu durum gerek Anayasa, gerek Avrupa İnsan Hakları Sözleşmesi ve gerekse kanunlarla düzenlenerek koruma altına alınmıştır.

Somut olayda davacı alacaklı vekilince icra müdürlüğünden sadece takip borçlusuna ait pasif tapu kayıtlarının celp edilmesi talep edilseydi bu talebin reddedilmesinin yukarıda ki anlatımlar ve mevzuat doğrultusunda usulüne uygun olmayacağı, nitekim borçlunun varsa pasif taşınmaz kayıtlarının sorgulanmasının , alacaklının bu yöndeki bir bilgiye kendisi ulaşamayacağından ve bu talebin yerine getirilmesi halinde ulaşacağı pasif taşınmaz kaydı vasıtası ile örneğin tasarrufun iptali gibi bir dava açarak alacağına kavuşma imkanına sahip olabileceğinden, pasif tapu kaydı sorgulamasında ulaşılabilecek bilginin borçlu adına daha önce kayıtlı bulunan taşınmaz bilgisi olup bu bilginin bu taşınmazın şimdiki maliki hakkında herhangi bir bilgi içermeyeceği, bu nedenle bu kaydın dosyaya dahil edilmesi, borçlu dışındaki herhangi bir 3.kişinin bilgilerinin dosyaya yansımaları sonucunu doğurmayacağı gibi borcun tahsili için imkan sağlayabileceğinden pasif tapu kaydı istenmesinde alacaklının haklı menfaati bulunduğu açık ise de davacı alacaklı vekili taşınmazların pasif tapu kayıtlarını değil, üçüncü kişilere satışına ilişkin evrakların da celbini talep etmiş olup bu durumda takipte taraf olmayan yeni maliklere ilişkin kişisel verilerin dosyaya celp edilmesi gibi bir sonuç doğuracağından icra müdürlüğünün şikayete konu işleminin usul ve yasaya uygun olduğu, dolayısıyla ilk derece mahkemesince verilen kararda herhangi bir isabetsizlik bulunmadığı anlaşılmış, davacı vekilinin yerinde görülmeyen istinaf başvurusunun esasın reddine karar vermek gerekmiştir.

HÜKÜM: Yukarıda açıklanan nedenlerle;

1- İzmir 11. İcra Hukuk Mahkemesi'nin 09/08/2019 tarih, 2019/470 E, 2019/611 K. sayılı kararına yönelik davacı vekilinin istinaf başvurusunun Hukuk Muhakemeleri Kanununun 353/1- b. 1 maddesi gereğince ESASTAN REDDİNE ,

2- Alınması gerekli 54,40 TL istinaf karar harcından peşin alınan 44,40 TL'nin mahsubu ile bakiye 10,00 TL harcın istinaf edenden alınarak hazineye irat kaydına,

3- İstinaf kanun yolu yargılama giderlerinin, istinaf eden üzerinde bırakılmasına,

4- HMK 333. madde gereğince kararın kesinleşmesinden sonra kullanılmayan gider avansının yatırana iadesine,

5- Kararın taraflara tebliğine,

Dair, dosya üzerinde yapılan inceleme sonucunda 6100 sayılı HMK'nun 361 maddesi uyarınca kararın tebliğinden itibaren 2 hafta içerisinde Yargıtay'a temyiz yolu açık olmak üzere oy birliği ile karar verildi.15/05/2020

İzmir BAM - 9. Hukuk Dairesi (E. 2018/2398)

İşyerinde cep telefonu kullanım yasağının ihlaline ilişkin BAM kararı

İzmir Bölge Adliye Mahkemesi, 9. HD., E. 2018/2398 K. 2019/764 T. 10.6.2019

Esas No.: 2018/2398

Karar No.: 2019/764

Karar Tarihi: 10.06.2019

İSTİNAF KARARI

DAVANIN KONUSU: Tespit (İşe İade İstemli)

İzmir 3. İş Mahkemesi'nin 07/05/2018 tarih ve 2017/602 Esas, 2018/172 Karar sayılı kararına karşı davalı vekilince istinaf kanun yoluna başvurulmuş, dosya istinaf incelemesi yapılmaküzere dairemize gönderilmiş olup, tüm dosya kapsamı incelendi, 6100 Sayılı HMK'nın 352.maddesi uyarınca eksiklik bulunmadığı anlaşıldığından;

GEREĞİ DÜŞÜNÜLDÜ:

TALEP:

Davacı vekili dava dilekçesi ile; davacının, 02/04/2012 tarihinde yapılan sözleşme gereğince davalı şirkette çalışmaya başladığını, yaklaşık 5 yıl süre ile davalı iş yerinde çalışan davacının iş yeri güvenliğini ihlal etmekten dolayı iş akdinin sona erdirildiğini, çalışanların çoğu hakkında iş yeri içerisinde telefon görüşmesi nedeniyle tutulan tutanaklara rağmen iş akdinin feshi yoluna gidilmediğini, davacının fesih tarihinden 4 ay önce üyesi olarak bulunduğu sendikanın davalı iş yerinde örgütlenmeye başladığını, davacının sendikaya üye olduğu için iş akdinin feshedildiğini, davacının telefon görüşmesinin ise dışarıdan 3.bir kişi ile değil iş yerinde çalışan başka bir arkadaşı ile olduğunu, feshin haksız nedenle olduğunu belirterek, yapılan fesih işleminin geçersizliği ile davacının işe iadesine, yasal süresi için işe başvurması halinde hak kazanacağı 4 aylık boşta geçen süre ücreti ve diğer haklarının ödenmesine, işe başlatılmaması halinde bir yıllık ücreti tutarında işe başlatmama tazminatına karar verilmesini talep ve dava etmiştir.

SAVUNMA:

Davalı vekili cevap dilekçesi ile; davacının, 02.04.2012 tarihinde çalışmaya başladığını, 15.08.2017 tarihi itibarıyla iş akdinin haklı nedenlerle feshedildiğini, müvekkili şirketin, 6698 Sayılı Kişisel Verilerin Korunması Kanunu gibi yasal mevzuat gereğince, bilgi-belge güvenliğinin sağlanması için yasal yükümlülükleri olduğunu, ihlali halinde uygulanacak ağır maddi yaptırımların söz konusu olduğunu, davacının da, söz konusu bilgi - belgelere ulaşma imkanı olan personellerden olduğunu, iş sözleşmesinin 1.2. maddesinin "Personel, görevin ifasında ve iş disiplinin sağlanmasında, şirketin talimatlarına, işveren tarafından belirlenen çalışma kurallarına, işyerinin genel politikalarına uyacağını kabul ve taahhüt eder. Personel verilen işi özenle yapmak, ahlak ve iyiniyet kurallarına uymak, işçi sağlığı ve işyeri güvenliği tedbirlerine uymakla yükümlüdür" şeklinde olduğunu, 14.08.2017 tarihinde saat 15:37 sıralarında, çalışma saatleri içinde ve çalışma alanı içinde olduğu sırada, davacının üzerinde görüntü kaydedebilen cep telefonu cihazı bulunduğu ve davacının telefon görüşmesi yaptığının şirketin yetkili çalışanları tarafından tespit edildiğini, kamera kayıtları ile de doğrulandığını, bu durumun işyerindeki yetkili personel tarafından tutanak altına alındığını, 14.08.2017 tarihinde olayın tespit edilmesi ve aynı gün davacının savunmasının alınmasından sonra, olay 4857 Sayılı Kanun'un 25/II-e. bendine göre "işverenin güvenini kötüye kullanmak, işverenin meslek sırlarını ortaya atmak gibi doğruluk ve bağlılığa uymayan davranışlarda bulunmak" kapsamında değerlendirilerek davacının iş akdinin haklı nedenle ve bildirimsiz olarak feshedilmesine karar verildiğini, davacının davranışının işverenin güvenini sarsan davranışlardan olduğunu, davacının sendikaya üye olması nedeniyle işten çıkarılmasının söz konusu olmadığını, davalı şirketin hangi çalışanların hangi sendikaya üye olduğuna dair bir bilgisi olmadığını savunup davanın reddini istemiştir.

İLK DERECE MAHKEMESİ KARARININ ÖZETİ:

İlk derece mahkemesince; "Davanın kabulü ile,

-Davalı işveren tarafından yapılan feshin geçersiz olduğunun tespitine ve davacının işe iadesine,

-6356 Sayılı Kanununun 25/5 maddesi gereğince, feshin sendikal sebeplere dayanması sebebiyle davacının 1 yıllık brüt ücreti tutarında sendikal tazminatın davalıdan alınarak davacıya ödenmesi gerektiğinin tespitine,

-Davacının işe iade için işverene süresi içinde başvurması halinde hak kazanılacak olan ve kararın kesinleşmesine kadar doğmuş bulunan en çok 4 aylık ücret ve diğer haklarının davacıya ödenmesi gerektiğinin belirlenmesine," karar verilmiştir.

TARAFLARCA İLERİ SÜRÜLEN İSTİNAF SEBEPLERİ:

Davalı vekili istinaf dilekçesi ile; mahkemenin kararının usul ve yasaya aykırı olduğunu, davacı ve müvekkili arasında imzalanan hizmet sözleşmesinin saha içinde cep telefonunu kullanmayı yasakladığını, aynı zamanda müvekkili şirket ile davacı arasında imzalanan ve şirket ile davacı arasında imzalanan ve iş sözleşmesinin ayrılmaz parçası niteliğindeki "Cep telefonu ve Kilitli Kutu Kullanma Talimatı"nı ve içinde yer alan hususlar dikkate alındığında görüleceği üzere personele saha içerisinde cep telefonu kullanılmasına ilişkin eğitim verildiğini, dahası her personelin telefonu kilit altında tutması amacıyla kilitli kutular oluşturduğunu, ayrıca zaman zaman verilen eğitimlerle personele iş sahasında cep telefonu bulundurmanın yasak olduğu yönünde tekrarlanan bilgi akışları sağlandığını, açıklanan nedenle davacının eyleminin mahiyeti hakkında bilgi sahibi kabul edilmesi gerekirken anılan şekilde karar verilmiş olmasının hatalı olduğunu, müvekkili şirketin kişisel veri depolama faaliyetiyle iştigal ettiğinden işin devamlılığını sağlayabilmek adına gizliliğin esas olduğunu, müvekkili şirketin bilgi güvenliğinin ihlali durumunda hem yasal hem de sözleşme kaynaklı ağır tazminat yükümlülükleri altında olduğunu, davacı yanın hizmet sözleşmesine aykırı eylemde bulduklarını kabul ettiğini, yerel mahkemenin yaptığı incelemede bu hususu tamamen görmezden geldiğini, davacının günlük telefon teslim tutanağına telefonunu teslim ettiğini beyan eden imza attığını ve işverence duyulan güven duygusuna ihanet ettiğini, kaldı ki işyerinde davacının yaşadığını iddia ettiği gibi özel durumlarda işçilerin ortak kullanması için tahsis edilmiş telefonların da bulunduğunu, sendikal fesih değerlendirmesine ilişkin olarak da feshin sendikal nedenle olduğunun tespitinde yüksek mahkeme kriterlerinin değerlendirilmediğini, işyerinde sendikal baskının işveren tarafından değil, sendika tarafından yapıldığını ve bu durumun dosya kapsamında sabit olduğunu, somut olay bakımından işin önemi ve güvenlik önlemi nedeniyle gerek iş sözleşmeleri gerekse iş sözleşmesi ekleri ile ayrı ayrı yapılan sözleşmeler ve bu konuda ayrıca personele verilen eğitimlerin taraflarca uyumsuzluk konusu olmadığını, aynı sebeple işten çıkarılmış işçiler bulunmaktayken salt sendika üyesi olması nedeniyle kat bekat daha fazla tazminat ödenecek olmasının İş Hukukunun temel ilkelerine göre adil kabul edilemeyeceğini, yerel mahkemenin sendikal neden iddiasının aslında iş disiplini konusunda yetersiz işçilerin bahanesi olup olmadığı hususunu hiç araştırmadan hüküm verdiğini beyan ederek, istinaf taleplerinin kabulü ile, hükmün bozulmasına, şayet hükmün bozulması yerine davanın yeniden görülmesine karar verildiği takdirde ilk derece mahkemesi hükmünün kaldırılarak davanın reddine karar verilmesini talep etmiştir.

GEREKÇE:

Dava, 4857 sayılı İş Kanun'unun 18. ve devamı maddeleri uyarınca açılmış işe iade istemine ilişkindir.

Dosya kapsamından; davacının, davalı işyerinde belirsiz süreli hizmet akdi ile çalıştığı, kıdeminin 6 aydan fazla olduğu, işveren vekilliği sıfatının bulunmadığı, davalı şirkette çalışan işçi sayısının 30'dan fazla olduğu, davanın da fesih bildirimının tebliğ edildiği tarihten itibaren 1 ay içinde açıldığı anlaşılmalı, davanın 4857 sayılı İş Kanun'unun 18 ve 20. maddelerinde öngörülen dava şartlarını taşıdığı tespit edilmiştir.

Davalı işveren noter marifetiyle düzenlemiş olduğu 15/08/2017 tarihli fesih bildiriminde; "... F2 Bilişim San. ve Tic. A.Ş ünvanlı işyerimizin arşiv operatörü görevinde çalışmaktasınız. Aramızda 02/04/2012 tarihinde yapılan Belirsiz Süreli İş Sözleşmesi 14.08.2017 tarihinde operasyon içerisinde cep telefonu kullanarak bilgi güvenliğini ihlal etmeniz nedeni ile İş Kanun'unun 4857/II-e bendi uyarınca 15.08.2017 tarihi itibarıyla tek taraflı ve tazminatsız olarak feshedilmiştir. " diyerek davacının iş akdini feshetmiştir.

Davalı işveren, davacının iş akdinin bilgi güvenliğini ihlal etmesi nedeniyle haklı sebeple feshedildiğini savunmaktadır .

Dosyaya davalı işveren tarafından hizmet sözleşmesi ekinde sunulan "Personel Gizlilik ve Sır Saklama Taahhütnamesi" başlıklı belgede, işyerinde telefon bulundurup, kullanmanın yasak olduğu yönünde bir hüküm bulunmadığı görülmektedir.

23.02.2015 tarihli "Cep Telefonu ve Kilitli Kutu Kullanma Talimatı" başlıklı belgede; " MADDELER:

- İlgili amirinden yazılı izni olan çalışanlar dışında tüm şirket çalışanları cep telefonlarını servis büro dışında bulunan kilitli telefon kutularına bırakarak servis büro alanına giriş yapmalıdırlar.

- Bir kutuyu kendilerinin belirlediği 4 yada 5 personel kullanmalıdır. Bu personellere de o kutunun anahtarı verilerek güvenli bir şekilde kullanmaları gerekmektedir.

- Personel telefonunu kutudan aldıktan sonra muhakkak kutuyu kilitlemek zorundadır.

- Anahtar kaybolduğunda kaybeden personel sorumludur.

- Kutuya telefondan başka hiç bir şey bırakılmamalıdır.

- Cep telefonları sadece öğle molasında ve bina dışında kullanılmalı ve mola bitiminde tekrar kutularına konulup servis büro alanına girilmelidir.

- Cep telefonu, fotoğraf makinesi ve tüm ses - görüntü medya cihazlarıyla şirket içerisinde, servis büro alınanda, tüm depo alanlarında ve yemekhanede kesinlikle fotoğraf çekilmemeli, ses veya video kaydı yapılmamalıdır.

- Kişiler sadece kendilerine ait telefonları kutulardan almalıdır.

- Çalışma alanı içerisinde telefon kullanması gereken personeller, ilgili amirden imzalı onay belgesini sekreteryaya teslim ederek telefonlarını kullanmalıdırlar.

UYARILAR:

- Cep telefonunu servis büro içerisine alan personeller tespit edildiğinde hakkında Bilgi Güvenliği İhlali riski gereği firma tarafından cezai işlem uygulanacaktır. " denildiği ve davacının da imzasını taşıdığı belirlenmiştir.

Davacı hakkında daha önce talimatlara uymamakla ilgili herhangi bir tutanak ve uyarı yazısının bulunmadığı anlaşılmıştır. Feshe konu olan olayla ilgili düzenlenen 14.08.2017 tarihli tutanakta; davacının servis büro içerisinde telefon kullanmak yasak olduğu ve cep telefonunu kilitli dolaplara bırakması gerektiği halde servis büro içerisinde üzerinde cep telefonu taşıdığı saat 15:37'de telefon görüşmesi yaptığı kameralarca tespit edildiğinden dolayı bilgi güvenliği ihlaline neden olduğu belirtilmiş, davacı tutanağın altına el yazısı ile yazdığı savunmasında "9 aylık kızım var ishal oldu ve çok hasta, rapor alıp gelmemelik yapamadım onlarla, eşimle irtibat kurmak için telefon kullandım. Ben 5 yıllık depo personeliyim ve sicilim tertemiz. Bilgi güvenliğini 5 yıllık çalışma döneminde hiçbir şekilde ihlal etmedim. İşimi seviyorum. Bir daha da tekrarlanmayacağını taahhüt ediyorum." şeklinde beyanda bulunduğu görülmektedir.

Gerek Gizlilik Sözleşmesinde, gerekse Cep Telefonu ve Kilitli Kutu Kullanma Talimatında davacının servis büro içerisinde cep telefonu taşıma eylemi ile ilgili olarak bir müeyyidenin öngörülmediği, sadece cep telefonunu servis büro içerisine alan personeller tespit edildiğinde hakkında Bilgi Güvenliği ihlal riski gereği firma tarafından cezai işlem uygulanacağı belirtilmiştir.

Davacının servis büro içerisinde cep telefonu taşımak şeklindeki eylemi gerçekte bilgi güvenliği ihlali değil, bilgi güvenliği ihlali riske taşıyan bir davranıştır. Dolayısıyla bilgi güvenliği riski taşıyan davacının bu davranışı iş akdinin feshini gerektirir ağırlıkta bir fiil değildir.

İşveren iş sözleşmesine aykırı bir davranışta bulunan işçiye yaptığı eylemle orantılı bir yaptırım uygulamalıdır. Yapılan eylemle orantılı olmayan ve ölçüsüz olarak nitelendirilebilecek bir yaptırım mazur görülemez. Sonuç itibarıyla fesih bir cezadır. Ölçülülük ilkesi uyarınca uygulanacak önlem ulaşılmak istenen amacı gerçekleştirmeye elverişli olmalı bir başka anlatımla tedbir uygun olmalı, ulaşılmak istenen amaç açısından gerekli olmalı ve uygulanacak tedbirin sonucu olan müdahale ile ulaşılmak istenen amaç ölçüsüz bir oran içerisinde bulunmamalıdır.

Davacının servis büro içerisinde cep telefonu taşıması eylemiyle henüz bilgi güvenliği ihlali olmadığı, işyerinin arşivlediği bir belgenin dışarıya sızdırılmadığı ve bu nedenlerle de işveren ya da belgeleri

arşivlenin müşterilerin herhangi bir zarara uğramadığı da gözetildiğinde, davacının bu davranışına bağlanan fesih yaptırımını ağır bir sonuç olacağından, fesih yetkisinin ölçülülük ilkesine aykırı olarak kullanılmış olması sebebiyle yerel mahkemenin fesih işleminin geçersizliğine, davacının işe iadesine ilişkin vermiş olduğu kararda hatalı bir yön bulunmamaktadır.

Her ne kadar davacı iş akdinin sendikaya üye olduğundan dolayı feshedildiğini iddia ederek, bir yıllık brüt ücreti tutarında işe başlatmama tazminatına hükmedilmesini talep etmiş, yerel mahkeme tarafından da davacının sendikal tazminat talebi kabul edilmiş ise de; F1 Sendikası'na 06/11/2017 tarihli cevabi yazıda, sendikanın işletmede %40 çoğunluğu sağladığı, bunun üzerine 15/08/2017 tarihinde Çalışma ve Sosyal Güvenlik Bakanlığına yetki başvurusunda bulunulduğu ve bakanlığın 23/08/2017 tarihli "yetki tespiti" yazısı ile işletmede çalışan sayısının 853 işçiden 359 üye sayısı ile "gerekli çoğunluğu" sağladıklarının bildirildiği, davacının 08/03/2016 tarihinden bu yana sendika üyesi olduğu, 14/08/2017 tarihi itibarıyla davalı işyerinde çalışan üye sayısının 354 olduğunun bildirilmiş olması ve davacı tanıklarının davacının sadece sendika üyesi olduğunu söylemeleri, davacının aktif olarak sendikal faaliyetlerde yer aldığı hususunda beyanda bulunmaması nedeniyle davacının, iş akdinin sendikal nedenle feshedildiğini somut delillerle ispat ettiğini söylemek mümkün olmayacaktır.

Bu nedenle de; yerel mahkemenin davacının sendikal tazminat talebini reddetmesi gerekirken kabul etmesi hatalı olduğundan, HMK'nın 353/1.b-2 maddesi uyarınca ilk derece mahkemesi kararı kaldırılmış ve yeniden esas hakkında aşağıdaki hüküm tesis edilmiştir.

HÜKÜM: Yukarıda açıklanan nedenlerle;

A) Davalı vekilinin, istinaf başvurusunun kısmen KABULÜ ile; İzmir 3. İş Mahkemesi'nin 07/05/2018 tarih ve 2017/602 Esas, 2018/172 Karar sayılı kararının düzeltilip yeniden esas hakkında karar verilmek üzere HMK'nın 353/1.b-2 maddesi gereğince KALDIRILMASINA,

B) 1- Davanın KABULÜ ile;

a) Davalı işverenin, davacının iş akdinin feshine ilişkin işleminin geçersizliğinin TESPİTİNE ve davacının İŞE İADESİNE,

b) Davacının yasal süresinde başvurmasına rağmen davalı işverence süresi içerisinde işe başlatılmaması halinde ödenmesi gereken tazminat miktarının davacının kıdemi, fesih nedeni dikkate alınarak 5 aylık brüt ücreti tutarında BELİRLENMESİNE,

c) Davacının işe iade için işverene süresi içinde müracaatı halinde hak kazanacak olan ve kararın kesinleşmesine kadar en çok 4 aya kadar ücret ve diğer hakların davalıdan tahsili GEREKTİĞİNE,

2 -44,40 TL karar ve ilam harcı tayini ile peşin alınan 31,40 TL harcın mahsubu ile bakiye 13,00 TL harcın davalıdan tahsiline,

3- Davacı yararına karar tarihinde yürürlükte olan Avukatlık Asgari Ücret Tarifesi gereğince 2.725,00 TL vekalet ücreti takdiri ile davalıdan alınarak, davacıya verilmesine,

4- Davacı tarafından yapılmış olduğu anlaşılan 31,40 TL başvurma harcı, 31,40 TL peşin harç, 4,60 TL vekalet harcı, 109,00 TL tebligat masrafı, 60,00 TL tanıklık ücreti, 26,80 TL posta masrafı olan toplam 263,20 TL yargılama giderinin davalıdan alınarak, davacıya verilmesine,

- Davalı tarafından yapılan yargılama giderlerinin üzerinde bırakılmasına,

C) 1-Davalıdan alınan 35,90 TL peşin istinaf harcının isteği halinde davalıya iadesine,

2- İstinaf incelemesi sırasında duruşma açılmadığından, vekalet ücreti takdirine yer olmadığına,

3- HMK'nın 333. maddesi uyarınca artan dava ve delil gider avansının istekleri halinde ilgisine iadesine,

Dosya üzerinde yapılan inceleme sonucunda 25/10/2017 tarihinde yürürlüğe giren 7036 sayılı Kanun'un 8/1-a maddesi uyarınca KESİN olmak üzere 10/06/2019 tarihinde oybirliği ile karar verildi.

İzmir Bölge Adliye Mahkemesi, 8. HD., E. 2018/2146 K. 2019/655 T. 6.3.2019

Esas No.: 2018/2146

Karar No.: 2019/655

Karar Tarihi: 06.03.2019

TÜRK MİLLETİ ADINA

İzmir 10. İcra Hukuk Mahkemesinin 2018/429 Esas, 2018/543 Karar sayılı dosyasında verilen şikayetin reddi kararına karşı, davacı vekili tarafından istinaf kanun yoluna başvurulmakla, Dairemize gönderilen ve heyetçe incelenen dosyada;

İSTEM: Davacı vekili dava dilekçesinde özetle, İzmir 28. İcra Müdürlüğünün 2018/6130 Esas sayılı dosyasında borçlular adına kayıtlı aktif ve pasif tapu kayıtlarının tespiti ile taşınmazların kime hangi tarihte satıldığı ve son takyidatlı raporları ile devir resmi senet suretlerinin ilgili tapu müdürlüklerinden istenmesini talep ettiklerini, icra müdürlüğünce devir bilgilerinin istenilmesi talebinin reddine şeklinde karar verildiğini, ancak verilen kararın hukuki dayanaktan yoksun olduğunu, pasif sorgu yapılması ve tespit edilen taşınmazlara ilişkin araştırma yapılarak bilgi toplanması taleplerinin alacağın tahsiline yönelik olduğunu, talebin reddi kararının İİK'nın 277 ve devamı maddelerinde düzenlenen tasarrufun iptali davası hükümlerine de aykırı olduğunu, devre konu taşınmazlara ilişkin ipotek bilgilerini alacaklıdan mal kaçırmak amacıyla yapılan devirlerle ilgili bilgi edinip, müvekkilinin haklarını korumak ve alacağın tahsilini sağlamak amacıyla gerekli yasal girişimleri başlatmak için talep ettiklerini belirterek, 23/05/2018 tarihli kararın kaldırılmasına ve talepleri gibi işlem yapılmasına karar verilmesini istemiştir.

İLK DERECE MAHKEMESİNİN KARARI: İlk derece mahkemesince dosya üzerinde yapılan inceleme sonucunda, şikayetin reddine karar verilmiştir.

İSTİNAF SEBEPLERİ: Davacı vekili istinaf başvuru dilekçesinde özetle, dava dilekçesini tekrarlayarak, icra müdürlüğü kararının hukuki dayanaktan yoksun olduğunu, bu konuda emsal mahkeme kararları ve Bölge Adliye Mahkemesi kararları bulunduğunu, icra müdürlüğünün pasif kayıtların istenilmesi talebinin reddi kararının İİK'nın 277 ve devamı maddelerinde düzenlenen tasarrufun iptali davası hükümlerine de aykırı olduğunu, red kararı ile bu madde uyarınca alacaklının dava açma hakkının engellendiğini, alacaklıdan mal kaçırmak amacıyla yapılan devirlerle ilgili bilgi

edinip, müvekkilinin haklarını korumak ve alacağın tahsilini sağlamak amacıyla gerekli yasal girişimleri başlatmak üzere talepte bulduklarını belirterek, kararın kaldırılmasını ve talepleri doğrultusunda işlem yapılmasını istemiştir.

DEĞERLENDİRME VE GEREKÇE: Dava, İİK'nın 16. maddesi uyarınca takip alacaklısının borçlu tarafından devredilmiş taşınmazlar varsa, buna ilişkin belgelerin ilgili tapu müdürlüğünden istenilmesi talebinin reddi kararının iptali isteğidir.

İzmir 28. İcra Müdürlüğünün 2018/6130 Esas sayılı takip dosyasının incelenmesinde, davacı alacaklı tarafından borçlular K1 ve diğerleri aleyhine toplam 8.132.719,07 TL asıl alacağın tahsili amacıyla ilamsız icra takibine geçildiği, alacaklı vekilinin 23/05/2018 tarihinde ihtiyati haciz kararının uygulanmasını ve borçluların pasif taşınmazlarının tespiti ile taşınmazların kime hangi tarihte ve son takyidatlı tapu kayıtları ile resmi devir senet suretlerinin ilgili tapu müdürlüklerinden istenmesini talep ettiği, icra müdürlüğünce aynı tarihte devir bilgilerinin celbi talebinin reddine karar verildiği, kararın alacaklı vekiline tebliğ edilmediği, davanın yasal süresi içinde açıldığı anlaşılmıştır.

İcra dosyasının tarafı olmayan üçüncü kişiye ait 6698 Sayılı Yasanın 3/1-d maddesi kapsamında kişisel veri niteliğinde bulunan tapu kaydı ve satış sözleşmelerinin icra müdürlüğünce istenmesi mümkün değildir. Aynı Yasanın 28/1-d maddesindeki yargısal organlara tanınan istisna, ancak uyuşmazlığın tarafları açısından geçerli olabilecektir. T.C. Anayasası'nın 20/3. maddesine göre aynı zamanda temel haklardan olan kişisel verilerin korunmasını isteme hakkı, 6698 Sayılı Yasanın 28/1-d maddesinin geniş yorumlanması ile daraltılamaz.

İcra müdürlüğü gerekli araştırma ve sorgulama işlemlerini alacağın tahsiline yönelik sınırlı işlemler için gerçekleştirebilir. Takip alacaklılarının ileride açabilecekleri muhtemel davaların malzemelerinin toplanması ödevi icra müdürlüğüne ait değildir. Mülkiyet hakkının korunması amacıyla açılacak bir davanın taraflarını tespit edebilmek için 1136 sayılı Avukatlık Kanunu'nun 2/3. maddesine göre avukat yazılı başvuru ile tapu sicilinde inceleme yapabilir. Alacaklının hukuki yararının, üçüncü şahısların Anayasa ile korunan özel hayatın gizliliğine ilişkin temel hakkından üstün tutulması mümkün değildir.

Somut olayda, borçlular adına pasif taşınmaz kayıtlarının tespiti ile sorgulaması yapılan taşınmazların resmi senet ve ilgili evraklarının getirtilmesinin istendiği dikkate alındığında, icra müdürünün şikayete konu kararında usul ve yasaya aykırı bir yön bulunmadığından, davacının istinaf başvuru nedenleri görülmemiştir.

Yukarıda açıklanan nedenlerle, ilk derece mahkemesi kararının usul ve yasaya uygun olduğu, kararda kamu düzenine aykırı bir yön de bulunmadığı anlaşılmalı, HMK'nın 353/1-b/1 maddesi uyarınca davacının istinaf başvurusunun esastan reddine karar verilmesi gerekmiştir.

HÜKÜM: Gerekçesi yukarıda açıklandığı üzere;

1- İzmir 10. İcra Hukuk Mahkemesinin 2018/429 Esas, 2018/543 Karar sayılı kararı usul ve esas yönünden hukuka uygun bulunduğundan, davacının istinaf başvurusunun 6100 sayılı HMK'nın 353/1-b/1 maddesi uyarınca ESASTAN REDDİNE,

2- Alınması gerekli 44,40 TL istinaf karar harcından, peşin alınan 35,90 TL harç indirilerek, kalan 8,50 TL harcın davacıdan alınmasına,

3- Davacı tarafından yapılan istinaf yargılama giderinin üzerinde bırakılmasına,

4- HMK'nın 333. maddesi uyarınca kalan gider avansının yatıran tarafa geri verilmesine,

İlişkin, dosya üzerinde yapılan inceleme sonunda İİK'nın 364/1 maddesi ve HMK'nın 361/1 maddesi uyarınca kararın tebliğinden itibaren 2 haftalık yasal süre içinde temyiz yolu açık olmak üzere oy birliği ile karar verildi. 06/03/2019

İzmir Bölge Adliye Mahkemesi, 8. HD., E. 2018/1633 K. 2019/269 T. 4.2.2019

Esas No.: 2018/1633

Karar No.: 2019/269

Karar Tarihi: 04.02.2019

TÜRK MİLLETİ ADINA

İSTİNAF KARARI

İzmir 3. İcra Hukuk Mahkemesinin 2018/182 Esas, 2018/441 Karar sayılı dosyasında verilen şikayetin reddi kararına karşı, davacı vekili tarafından istinaf kanun yoluna başvurulması üzerine istinaf incelemesi yapılmak üzere Dairemize gönderilen ve heyetçe incelenen dosyada;

İSTEM: Davacı vekili dava dilekçesinde özetle, İzmir 1. İcra Müdürlüğünün 2017/13761 Esas sayılı dosyası ile yürütülen takip kapsamında icra müdürlüğünden borçlu adına kayıtlı iken satılan araç olup olmadığı, varsa kayıtların bildirilmesi, borçlu adına tesis edilmiş rehin bilgileri ile varsa takip icra müdürlüğünün adı ve dosya numarasının sorulması, borçlu adına geriye doğru son 5 yıl içinde satışı yapılan araç var ise kimlere satış yapıldığını ve plaka bilgilerinin sorulması yönünde talepte bulunulduğunu, icra müdürlüğünün 05/04/2018 tarihli kararı ile talebi reddettiğini, Trafik Tescil Müdürlüğünden 3. kişilere yönelik sorgulama yapmalarının mümkün olmadığını, bu bilgilere ancak icra müdürlüğü aracılığıyla ulaşılabileceğini, talebin yerine getirilmemesinin alacaklıyı zarara sokacağını bildirerek 05/04/2018 tarihli icra müdürlüğü kararının iptaline karar verilmesini istemiştir.

İLKDERECE MAHKEMESİNİN KARARI: İlk derece mahkemesince dosya üzerinde yapılan inceleme sonunda şikayetin reddine karar verilmiştir.

İSTİNAF SEBEPLERİ: Davacı vekili istinaf dilekçesinde özetle; dava dilekçesindeki beyanlarını tekrarlar, ilk derece mahkemesi kararının takip dosyasındaki yasal işlem süresi ve alacağın tahsili kabiliyetini kısıtladığını bildirerek ilk derece mahkemesi kararının kaldırılmasına, şikayetin kabulüne karar verilmesini istemiştir.

DEĞERLENDİRME VE GEREKÇE: Dava, İİK'nın 16. maddesine dayalı icra memur işlemini şikayete ilişkindir.

İzmir 1. İcra Müdürlüğünün 2017/13761 Esas sayılı dosyasının incelenmesinde; alacaklı davacı tarafından dava dışı borçlu K1 aleyhine toplam 48.198,29 TL alacağın tahsili amacıyla başlatılan ilamsız icra takibi olduğu, ödeme emrinin borçluya 05/01/2018 tarihinde tebliğ edildiği, takibin itiraz edilmeksizin kesinleştiği, 02/04/2018 tarihinde alacaklı vekilinin borçlu adına kayıtlı iken 3. kişiye satılan araç olup olmadığı, varsa araç kayıtlarının dosyaya bildirilmesi, borçlu adına tesis edilmiş ise rehin bilgileri ile varsa takip icra müdürlüğünün adı ve dosya numarasının, borçlu adına geriye doğru son 5 yıl içinde satışı yapılan araç var ise kimlere satış yapıldığını ve plaka bilgilerinin sorulması yönünde talepte bulunduğu, icra müdürlüğünün aynı tarihli kararı ile talebi reddettiği, alacaklı vekilinin 04/04/2018 tarihinde aynı yönde talepte bulunduğu, icra müdürlüğünün 05/04/2018 tarihli kararı ile talebin reddine karar verildiği, bu kararın alacaklı vekiline tebliğ edilmediği, şikayetin süresinde olduğu anlaşılmıştır.

İcra müdürlüğünün görev ve yetkileri 2004 Sayılı İcra İflas Kanunu'nda ayrıntılı olarak düzenlenmiştir. İcra müdürlüğünce gerekli araştırma ve sorgulama işlemleri alacağın tahsiline yönelik sınırlı işlemler için gerçekleştirilebilecektir. Aksi durumun kabulü, kişisel verilerin korunması kuralının ihlali sonucunu doğuracaktır.

İcra dosyasının tarafı olmayan üçüncü kişiye ait 6698 Sayılı Kanunun 3/1-d maddesi kapsamında kişisel veri niteliğinde bulunan araç kayıtlarındaki bilgilerin icra müdürlüğünce istenmesi mümkün değildir. Aynı kanunun 28/1-d maddesindeki yargısal organlara tanınan istisna ancak uyumsuzluğun tarafları açısından geçerli olabilecektir. T.C Anayasasının 20/3. maddesine göre, aynı zamanda temel haklardan olan kişisel verilerin korunmasını isteme hakkının, 6698 Sayılı Kanunun 28/1-d maddesinin geniş yorumlanması ile daraltılması da mümkün değildir. Alacaklının bu talebi ile yapılacak sorgulama ile takip dosyası tarafı olmayan 3. kişilerin bilgilerine ulaşılması mümkün olduğundan, bu istem Anayasal güvenceye bağlanan kişisel verilerin korunması düzenlenmesine aykırıdır. Alacaklının hukuki yararının, üçüncü kişilerin Anayasa ile korunan özel hayatın gizliliğine ilişkin temel hakkından daha üstün tutulmasına olanak bulunmamaktadır.

Davacının dile getirdiği üzere, borçlu adına geriye yönelik son 5 yıl içerisinde satışı yapılan araç var ise kimlere satış yapıldığının ve plaka bilgilerinin tespitinin, borcu tahsilde alacaklı tarafa katkı sağlayacağı muhakkaktır. Ancak kişisel verilerin bu şekilde elde edilmesinde, muhtemel yararların yanı sıra doğabilecek zararlar da birlikte değerlendirilmelidir. Anayasa Mahkemesinin 09/04/2014 tarihli 2013/122 Esas, 2014/74 Karar sayılı kararında kişisel verilerin niçin gizli tutulması gerektiği ayrıntılı olarak açıklanmış olup, yapılacak bir fayda-zarar kıyaslamasında kişisel verilere kolaylıkla ulaşılmasının yaratması muhtemel olan zararlarının, sağlanması muhtemel olan yararlarına göre daha

fazla ve daha mühim olduđu anlaşılmaktadır. Bu açıklamalar ışığında somut olaya bakıldığında, ilk derece mahkemesi kararında herhangi bir isabetsizlik bulunmamaktadır.

Yukarıda açıklanan nedenlerle, ilk derece mahkemesi kararının usul ve yasaya uygun olduđu, davacının istinaf başvuru nedenlerinin yerinde olmadığı, kararda kamu düzenine aykırı bir yön de bulunmadığı anlaşılmakla, HMK'nın 353/1-b/1 maddesi uyarınca davacının istinaf başvurusunun esastan reddine karar verilmesi gerekmiştir.

HÜKÜM: Gerekçesi yukarıda açıklandığı üzere;

1- İzmir 3. İcra Hukuk Mahkemesinin 2018/182 Esas, 2018/441 Karar sayılı kararı usul ve esas yönünden hukuka uygun bulunduğundan, davacının istinaf başvurusunun 6100 sayılı HMK'nın 353/1-b/1 maddesi uyarınca ESASTAN REDDİNE,

2- Alınması gereken 44,40 TL karar ve ilam harcından peşin alınan 35,90 TL harç indirilerek kalan 8,50 TL harcın davacıdan alınmasına,

3- Davacı tarafından yapılan istinaf yargılama giderlerinin üzerinde bırakılmasına,

4- HMK'nın 333. maddesi gereğince karar kesinleştğinde kalan gider avansının yatıran tarafa geri verilmesine,

İlişkin, dosya üzerinde yapılan inceleme sonunda HMK'nın 361/1 maddesi ve İİK'nın 364/1 maddesi uyarınca kararın tebliğinden itibaren 2 haftalık yasal süre içinde temyiz yolu açık olmak üzere oy birliği ile karar verildi. 04/02/2019

İzmir BAM - 12. Hukuk Dairesi (E. 2017/499)

İzmir Bölge Adliye Mahkemesi, 12. HD., E. 2017/499 K. 2017/660 T. 23.3.2017

Esas No.: 2017/499

Karar No.: 2017/660

Karar Tarihi: 23.03.2017

DAVANIN KONUSU: Şikayet

Erdek İcra Hukuk Mahkemesi'nin 12/10/2016 gün ve 2016/73 E, 2016/64 K sayılı kararına karşı istinaf kanun yoluna başvurulması üzerine dosya incelendi, gereği görüşülüp düşünüldü:

DAVA: Davacı vekili dava dilekçesinde özetle; Erdek İcra Müdürlüğü'nün 2016/800 Esas sayılı dosyasından borçlu K1 ve K2'ya ait intikal edecek olan taşınmaz ve araç olup olmadığının araştırılması ve borçluya, aile nüfus kayıt örneklerinin çıkartılması taleplerinin reddine karar verildiğini, kararın yasal olmadığını, kaldırılması gerektiğini, zira talebin 3. kişilere ait taşınmaz ve araçlar olmayıp borçluya miras olarak intikal edecek taşınmaz ve araçlar olduğunu, borcun tahsili açısından söz konusu sorgulamaların icra müdürlüğüne yapılması gerektiğini belirterek Erdek İcra Müdürlüğü'nün 2016/800 Esas sayılı dosyasından verilmiş olan, taleplerinin reddine ilişkin 01.08.2016 tarihli kararın kaldırılarak, talepleri doğrultusunda borçluya intikal edecek olan araç ve taşınmazların sorgulanmasına ve borçluya ait aile nüfus kayıt örneğinin çıkartılmasına karar verilmesini talep ve dava etmiştir.

CEVAP: Dava icra müdürlüğünün işlemine karşı şikayet davası olup hasımsızdır.

İLK DERECE MAHKEMESİ KARARI: Açılan dava sonucu Erdek İcra Hukuk Mahkemesinin 2016/73-64 E.K. sayılı kararı ile şikayetin reddine karar verilmiştir.

İSTİNAF SEBEPLERİ: Davacı taraf istinaf dilekçesinde;

- 1- Tahsil edilmemiş bir borç için takip başlatıldıktan sonra alacak tahsil edilemediğinde borçlunun miras hissesinin haczi için nüfus kaydı çıkarılmasının istenmesinin özel hayatın ihlali olarak değerlendirilmesinin hukuken hatalı olduğunu,
- 2- Borçlunun henüz kendisine intikali yapılmamış olan miras hissesine isabet eden mal varlığının başka bir şekilde tespitinin mümkün olmadığını,
- 3- Uygulamanın bu şekilde olmasının alacaklının mağduriyetine sebep olacağını,

4- Dosyaların yalnızca taraflar ve vekilleri tarafından incelenebildiğini, bu nedenle bilgilerin kötünietli 3.kişilerin eline geçmesinin mümkün olmadığını,

5- Borçluların kanunları kötüye kullanarak alacaklıları mağdur ettiklerini, hukuki boşlukların buna imkan tanıdığını, buna rağmen alacaklı veya vekili kötüye kullanabilir diye borçlunun mallarına erişimi sağlayacak bilgilerin kısıtlanmaması gerektiğini beyan ederek Erdek İcra Hukuk Mahkemesinin 2016/73-64 E.K. sayılı kararının kaldırılmasına karar verilmesini talep etmiştir.

GEREKÇE: Davacı alacaklı taraf icra müdürlüğüne sunduğu talebi ile borçlunun mirasçılık durumunun sözkonusu olup olmadığının tespiti için vukuatlı nüfus kaydının çıkarılmasını, mirasçılık durumu sözkonusu ise miras hissesi oranında haciz konulmasını talep etmiş, müdürlük bu talebi reddetmiştir. Şikayete konu karar bu karardır. Burada çözülmesi gereken ihtilaf borçlu dışındaki kişilerin nüfus kayıt bilgilerinin takip dosyası kapsamında temin edilerek açığa çıkarılmasının mümkün olup olmadığıdır.

Konu ile ilgili mevzuat hükümleri incelendiğinde;

TC Anayasası madde 13: Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.

TC Anayasası madde 20/3: Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.

Avrupa İnsan Hakları Sözleşmesi madde 8: 1-Herkes, özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

2- Bu hakkın kullanımına, yasa/hukuk uyarınca olması ve ulusal güvenlik, kamu emniyeti ya da ülkenin ekonomik refahı, düzensizliğin ya da suçun önlenmesi, sağlığın ya da ahlakın korunması ya da başkalarının haklarının ve özgürlüklerinin korunması için demokratik toplumda gerekli olması hali istisna olmak üzere, bir kamu makamı tarafından bulunulmayacaktır.

Nüfus Hizmetleri Kanunu madde 9: 1-Nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Bunlar, yetkili ve sorumlu memurlar ile teftiş ve denetim yetkisi olanlar dışında kimse tarafından görülüp incelenemez. Mahkemeler bu hükmün dışındadır.

2- Nüfus kayıtlarına bu bilgileri işleyen memurlar ve Kimlik Paylaşımı Sistemi kapsamında nüfus kayıtlarından faydalanan diğer görevliler de bu gizliliğe uymak zorundadırlar. Bu yükümlülük, kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam eder.

Madde 44: 1- Nüfus kayıt örneklerini;ç) Adli makamlar,nüfus müdürlüklerinden doğrudan almaya yetkilidirler.

Kişisel Verilerin Korunması Kanunu madde 3/1-d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

madde 3/1-e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

madde 5: 1- Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

2- Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

- a) Kanunlarda açıkça öngörülmesi.
- b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
- c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Madde 28: 1-Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:....d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

düzenlemelerine rastlanmaktadır.

Yukarıda yer verilen mevzuat hükümlerine göre kişinin nüfus kaydının kişisel veri niteliğinde olduğu tartışmasızdır. (Kişisel Verilerin Korunması Kanunu madde 3/1-d) Kişisel verilerin tamamen veya kısmen elde edilerek kaydedilmesi ise kişisel verilerin işlenmesidir. (Kişisel Verilerin Korunması Kanunu madde 3/1-e) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (Kişisel Verilerin Korunması Kanunu madde 5) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenebilmesi ise bu kuralın istisnasıdır.(Kişisel Verilerin Korunması Kanunu madde 28/1-d) Kişisel veri olduğu açık olan nüfus kaydına ilişkin bir başka düzenleme olan Nüfus Hizmetleri Kanununun 9. maddesine göre ise nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Tüm bu hususlardan açıkça anlaşıldığı üzere kişisel veriler ve bu bağlamda nüfus kayıtları gizlidir, edinilip kaydedilmeleri ilgili kişinin açık rızasına bağlıdır ve bu durum gerek Anayasa, gerek Avrupa İnsan Hakları Sözleşmesi ve gerekse kanunlarla düzenlenerek koruma altına alınmıştır. Somut olayda nüfus kaydına ulaşması ve kaydetmesi istenen kurum icra müdürlüğü olup bu kurumun yukarıda belirtilen istisnalar arasında sayılan kurumlardan olmadığı da açıktır.

Davacı tarafın beyanlarında dile getirdiği gibi borçlunun murisi olabilecek kişilerin nüfus kaydına erişilmesinin ve onların ölmüş olup olmadıklarının tespitinin borcu tahsilde alacaklı tarafa katkı sağlayacağı muhakkaktır. Hatta bu durum murisinden kendisine intikal eden malları adına tescil ettirmeyen borçluların bu şekilde davranmalarının önüne geçmek sonucunu da doğurabilecektir. Ancak kişisel verilerin bu şekilde işlenmesi ile elde edilmesi muhtemel yararların yanısıra doğabilecek zararlar da birlikte değerlendirilmelidir. Anayasa Mahkemesinin 09/04/2014 tarih ve 2013/122-2014/74 EK sayılı kararında kişisel verilerin niçin gizli tutulması gerektiği ayrıntılı olarak açıklanmıştır. "Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Bilişim teknolojilerindeki gelişmeler sonucunda, geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi; daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması; verilere erişim ve veri transferinin kolaylaşması;

kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler, günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır. Bu bağlamda Anayasa'nın 20. Maddesinin üçüncü fıkrasının son cümlesinde, "Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilerek kişisel verilerin korunması hakkı anayasal güvenceye bağlanmış ve bu şekilde kamu makamlarının keyfi müdahalelerine karşı koruma altına alınmıştır." O halde yapılacak bir fayda-zarar kıyaslamasında kişisel verilere kolaylıkla ulaşılmasının yaratması muhtemel olan zararlarının sağlanması muhtemel olan yararlarına göre daha fazla ve daha mühim olduğu anlaşılmaktadır.

Tüm bu açıklamalar çerçevesinde davacı tarafın icra müdürlüğüne yaptığı borçlunun mirasçılık durumunun sözkonusu olup olmadığının tespiti için vukuatlı nüfus kaydının çıkarılmasına, mirasçılık durumu sözkonusu ise miras hissesi oranında haciz konulmasına ilişkin talebi yerinde olmayıp bu talebin reddine ilişkin müdürlük kararı doğrudur. Nitekim bu hususta yerleşmeye başlayan uygulama kapsamında da mahkemelerce verilen benzer mahiyetteki kararlar Yargıtay tarafından da onanmaktadır. (Benzer mahiyette Yargıtay 12 HD' nin 05/05/2016 tarih ve 2015/33810-2016/13366 EK sayılı onama kararı)

Yukarıda açıklanan nedenlerle istinaf isteminin reddine karar verilmiş ve aşağıdaki şekilde hüküm kurulmuştur.

HÜKÜM: Yukarıda açıklanan nedenlerle;

Erdek İcra Hukuk Mahkemesi'nin 12/10/2016 gün ve 2016/73 E, 2016/64 K sayılı kararına yönelik davacı vekilinin istinaf başvurusunun Hukuk Muhakemeleri Kanununun 353/1- b. 1 maddesi gereğince esastan REDDİNE ,

Davacı harçtan muaf olduğundan, ilk derece mahkemesince alınan 47,00 TL ilk harç ve 117,10 TL istinaf kanun yolu harcının davacıya iadesine,

İstinaf kanun yolu yargılama giderlerinin, istinaf eden üzerinde bırakılmasına,

HMK 333.madde gereğince kullanılmayan gider avansının kararın kesinleşmesi halinde yatırana iadesine,

Kararın taraflara tebliğine,

Dair, dosya üzerinde yapılan inceleme sonunda İİK'nun 364.maddesi gereğince takip konusu esas alacağın miktarı 40.000,00 TL'yi geçmediğinden miktar itibariyle kesin olmak üzere oy birliği ile karar verildi. 23/03/2017

İzmir Bölge Adliye Mahkemesi, 12. HD., E. 2017/498 K. 2017/668 T. 24.3.2017

Esas No.: 2017/498

Karar No.: 2017/668

Karar Tarihi: 24.03.2017

DAVANIN KONUSU: Şikayet (İcra Memur Muamelesi)

İlk Derece Mahkemesi tarafından verilen karara karşı süresinde istinaf kanun yoluna başvurulmasına üzerine dosya incelendi.

DAVA: Davacı vekili dava dilekçesinde özetle, Erdek İcra Müdürlüğü'nün 2016/801 esas sayılı dosyasından borçlu K1' e ait intikal edecek olan taşınmaz ve araç olup olmadığının araştırılması ve borçluya aile nüfus kayıt örneklerinin çıkartılması taleplerinin reddine karar verildiğini, kararın yasal olmadığını, kaldırılması gerektiğini, zira talebin 3. kişilere ait taşınmaz ve araçlar olmayıp borçluya miras olarak intikal edecek taşınmaz ve araçlar olduğunu, borcun tahsili açısından söz konusu sorgulamaların icra müdürlüğünce yapılması gerektiğini belirterek Erdek İcra Müdürlüğü'nün 2016/801 esas sayılı dosyasından verilmiş olan, taleplerinin reddine ilişkin 02.08.2016 tarihli kararın kaldırılarak, talepleri doğrultusunda borçluya intikal edecek olan araç ve taşınmazların sorgulanmasına ve borçluya ait aile nüfus kayıt örneğinin çıkartılmasına karar verilmesini talep ve dava etmiştir.

CEVAP: Dava hasımsız açılmıştır.

İLK DERECE MAHKEMESİ KARARI: Mahkemece davanın reddine karar verilmiştir.

İSTİNAF SEBEPLERİ: Davacı vekili istinaf dilekçesinde; verilen kararın usul ve yasaya aykırı olduğunu, söz konusu talep ile araştırılması istenen hususların 3.kişilere ait taşınmaz ve araçlar olmayıp borçluya miras olarak intikal edecek taşınmaz ve araçlar olduğunu, ölen kişilere ait mal varlığı sorgulamasında Anayasanın 20.maddesine aykırılığın söz konusu olmayacağını, ayrıca müvekkili F1 Yönetim Şirketi harçtan muaf olduğu halde peşin yatırılan harcın kendilerine iade edilmediğini belirterek ilk derece mahkemesi kararının kaldırılmasına karar verilmesini talep etmiştir.

GEREKÇE: Davacı alacaklı taraf icra müdürlüğüne sunduğu talebi ile borçlunun mirasçılık durumunun sözkonusu olup olmadığının tespiti için vukuatlı nüfus kaydının çıkarılmasını,

mirasçılık durumu sözkonusu ise miras hissesi oranında haciz konulmasını talep etmiş, müdürlük bu talebi reddetmiştir. Şikayete konu karar bu karardır. Burada çözülmesi gereken ihtilaf borçlu dışındaki kişilerin nüfus kayıt bilgilerinin takip dosyası kapsamında temin edilerek açığa çıkarılmasının mümkün olup olmadığıdır.

Konu ile ilgili mevzuat hükümleri incelendiğinde;

TC Anayasası madde 13: Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.

TC Anayasası madde 20/3: Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.

Avrupa İnsan Hakları Sözleşmesi madde 8: 1-Herkes, özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

2-Bu hakkın kullanımına, yasa/hukuk uyarınca olması ve ulusal güvenlik, kamu emniyeti ya da ülkenin ekonomik refahı, düzensizliğin ya da suçun önlenmesi, sağlığın ya da ahlakın korunması ya da başkalarının haklarının ve özgürlüklerinin korunması için demokratik toplumda gerekli olması hali istisna olmak üzere, bir kamu makamı tarafından bulunulmayacaktır.

Nüfus Hizmetleri Kanunu madde 9: 1-Nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Bunlar, yetkili ve sorumlu memurlar ile teftiş ve denetim yetkisi olanlar dışında kimse tarafından görülüp incelenemez. Mahkemeler bu hükmün dışındadır.

2-Nüfus kayıtlarına bu bilgileri işleyen memurlar ve Kimlik Paylaşımı Sistemi kapsamında nüfus kayıtlarından faydalanan diğer görevliler de bu gizliliğe uymak zorundadırlar. Bu yükümlülük, kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam eder.

Madde 44: 1- Nüfus kayıt örneklerini;ç) Adli makamlar,nüfus müdürlüklerinden doğrudan almaya yetkilidirler.

Kişisel Verilerin Korunması Kanunu madde 3/1-d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

Madde 3/1-e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt

sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi,

değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması

ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

madde 5: 1- Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

2- Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Madde 28: 1-Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:....d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi,

düzenlemelerine rastlanmaktadır.

Yukarıda yer verilen mevzuat hükümlerine göre kişinin nüfus kaydının kişisel veri niteliğinde olduğu tartışmasızdır. (Kişisel Verilerin Korunması Kanunu madde 3/1-d) Kişisel verilerin tamamen

veya kısmen elde edilerek kaydedilmesi ise kişisel verilerin işlenmesidir. (Kişisel Verilerin Korunması Kanunu madde 3/1-e) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (Kişisel Verilerin Korunması Kanunu madde 5) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenebilmesi ise bu kuralın istisnasıdır.(Kişisel Verilerin Korunması Kanunu madde 28/1-d) Kişisel veri olduğu açık olan nüfus kaydına ilişkin bir başka düzenleme olan Nüfus Hizmetleri Kanununun 9. maddesine göre ise nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Tüm bu hususlardan açıkça anlaşıldığı üzere kişisel veriler ve bu bağlamda nüfus kayıtları gizlidir, edinilip kaydedilmeleri ilgili kişinin açık rızasına bağlıdır ve bu durum gerek Anayasa, gerek Avrupa İnsan Hakları Sözleşmesi ve gerekse kanunlarla düzenlenerek koruma altına alınmıştır. Somut olayda nüfus kaydına ulaşması ve kaydetmesi istenen kurum icra müdürlüğü olup bu kurumun yukarıda belirtilen istisnalar arasında sayılan kurumlardan olmadığı da açıktır.

Davacı tarafın beyanlarında dile getirdiği gibi borçlunun murisi olabilecek kişilerin nüfus kaydına erişilmesinin ve onların ölmüş olup olmadıklarının tespitinin borcu tahsilde alacaklı tarafa katkı sağlayacağı muhakkaktır. Hatta bu durum murisinden kendisine intikal eden malları adına tescil ettirmeyen borçluların bu şekilde davranmalarının önüne geçmek sonucunu da doğurabilecektir. Ancak kişisel verilerin bu şekilde işlenmesi ile elde edilmesi muhtemel yararların yanısıra doğabilecek zararlar da birlikte değerlendirilmelidir. Anayasa Mahkemesinin 09/04/2014 tarih ve 2013/122-2014/74 EK sayılı kararında kişisel verilerin niçin gizli tutulması gerektiği ayrıntılı olarak açıklanmıştır. "Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Bilişim teknolojilerindeki gelişmeler sonucunda, geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi; daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması; verilere erişim ve veri transferinin kolaylaşması; kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler, günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır. Bu bağlamda Anayasa'nın 20. Maddesinin üçüncü fıkrasının son cümlesinde, "Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilerek kişisel verilerin korunması hakkı anayasal güvenceye bağlanmış ve bu şekilde kamu makamlarının keyfi müdahalelerine karşı koruma altına alınmıştır."

O halde yapılacak bir fayda-zarar kıyaslamasında kişisel verilere kolaylıkla ulaşılmamasının yaratması muhtemel olan zararlarının sağlanması muhtemel olan yararlarına göre daha fazla ve daha mühim olduğu anlaşılmaktadır.

Tüm bu açıklamalar çerçevesinde davacı tarafın icra müdürlüğüne yaptığı borçlunun mirasçılık durumunun sözkonusu olup olmadığının tespiti için vukuatlı nüfus kaydının çıkarılmasına, mirasçılık durumu sözkonusu ise miras hissesi oranında haciz konulmasına ilişkin talebi yerinde olmayıp bu talebin reddine ilişkin müdürlük kararı doğrudur. Nitekim bu hususta yerleşmeye başlayan uygulama kapsamında da mahkemelerce verilen benzer mahiyetteki kararlar Yargıtay tarafından da onanmaktadır. (Benzer mahiyette Yargıtay 12 HD' nin 05/05/2016 tarih ve 2015/33810-2016/13366 EK sayılı onama kararı)

Yukarıda açıklanan nedenlerle incelenen mahkeme kararının yerinde olduğu anlaşıldığından istinaf başvurusunun esastan reddine karar verilerek aşağıdaki gibi hüküm kurmak gerekmiştir.

HÜKÜM: Yukarıda açıklanan nedenlerle;

1- Erdek İcra Hukuk Mahkemesi'nin, 05/10/2016 tarihli, 2016/71 E, 2016/59 K sayılı kararına yönelik davacı vekilinin istinaf başvurusunun Hukuk Muhakemeleri Kanununun 353/1- b. 1 maddesi gereğince ESASTAN REDDİNE ,

Davacı harçtan muaf olduğundan, ilk derece mahkemesince alınan 47,00 TL ilk harç ve 117,10 TL istinaf kanun yolu harcının davacıya iadesine,

2- İstinaf kanun yolu yargılama giderlerinin, istinaf eden üzerinde bırakılmasına,

3- Kararın taraflara tebliğine,

4- HMK 333. madde gereğince kararın kesinleşmesinden sonra kullanılmayan gider avansının yatırana iadesine,

Dair, dosya üzerinde yapılan inceleme sonunda İİK'nun 364.maddesi gereğince takip konusu esas alacağın miktarı 40.000,00 TL'yi geçmediğinden miktar itibariyle kesin olmak üzere oy birliği ile karar verildi. 24/03/2017

İzmir BAM - 12. Hukuk Dairesi (E. 2016/59)

İcra dosyasına taraf olmayan 3. Kişilere ait kişisel niteliğini haiz tapu kaydı ve satış sözleşmelerinin icra müdürlüğüne celbinin istenemeyeceğine ilişkin bam kararı

İzmir Bölge Adliye Mahkemesi 12. HD., E. 2016/59 K. 2016/68 T. 13.10.2016

Esas No.: 2016/59

Karar No.: 2016/68

Karar Tarihi: 13.10.2016

ÖZET: Kişinin nüfus kaydının kişisel veri niteliğinde olduğu tartışmasızdır. Kişisel verilerin tamamen veya kısmen elde edilerek kaydedilmesi ise kişisel verilerin işlenmesidir. Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenebilmesi ise bu kuralın istisnasıdır. Olayda nüfus kaydına ulaşması ve kaydetmesi istenen kurum icra müdürlüğü olup bu kurumun belirtilen istisnalar arasında sayılan kurumlardan olmadığı açıktır. Yapılacak bir fayda-zarar kıyaslamasında kişisel verilere kolaylıkla ulaşılmasının yaratması muhtemel olan zararlarının sağlanması muhtemel olan yararlarına göre daha fazla ve daha mühim olduğu anlaşılmaktadır. Bu açıklamalar çerçevesinde davacı tarafın icra müdürlüğüne yaptığı borçlunun anne babasını gösterir aile nüfus kaydının sorgulanarak muris tespit edilmesi halinde adına kayıtlı taşınmaz bulunup bulunmadığının sorgulanmasına ilişkin talebi yerinde olmayıp bu talebin reddine ilişkin müdürlük kararı doğrudur.

Davacı tarafın diğer talebi ise borçlunun varsa pasif taşınmaz kayıtlarının sorgulanması talebidir. Pasif tapu kaydı sorgulamasın da ulaşılacak bilgi borçlu adına daha önce kayıtlı bulunan taşınmaz bilgisi olup bu bilgi bu taşınmazın şimdiki maliki hakkında herhangi bir bilgi içermeyecektir. Bu nedenle bu kaydın dosyaya dahil edilmesi, borçlu dışındaki herhangi bir 3. kişinin bilgilerinin dosyaya yansması sonucunu doğurmayacağı gibi borcun tahsili için imkan sağlayabilecektir. O halde bu yöndeki talebin icra müdürlüğüne ve özellikle de dosyanın infazına yarar sağlamayacağı ve borçlu aleyhine delil toplanamayacağı gerekçesi ile reddi yerinde değildir. Davacı tarafın istinaf

başvurusunun kısmen kabulü ile istinafa konu kararın düzeltilerek yeniden esas hakkında karar verilmesi gerekir.

DAVA: Manisa 1. İcra Hukuk Mahkemesinin 11/08/2016 gün 2016/364 Esas - 2016/468 Karar sayılı kararına karşı davacı vekili tarafından istinaf kanun yoluna başvurulması üzerine dosya incelendi:

KARAR: Davacı vekili tarafından Manisa 5. İcra Müdürlüğünün 2016/2488 esas sayılı takibi kapsamında müdürlükçe alınan 24/06/2016 tarihli kararın ortadan kaldırılmasına karar verilmesi talep edilmiştir.

CEVAP: Dava icra müdürlüğünün işlemine karşı şikayet davası olup hasımsızdır.

İLK DERECE MAHKEMESİ KARARI: Açılan dava sonucu Manisa 1. İcra Hukuk Mahkemesinin 2016/364-468 E.K. sayılı kararı ile şikayetin reddine karar verilmiştir.

İSTİNAF SEBEPLERİ: Davacı taraf istinaf dilekçesinde;

1- Taleplerinde 3. kişilere ait bir sorgu veya malvarlığı araştırması bulunmadığını, sorgulanmasını istedikleri nüfus kaydının borçlunun aile nüfus kaydı olduğunu, bu uygulamanın yaygınlaşmasının kötü niyetli borçlulara imkan sağlayacağını, adli makamların nüfus kayıtlarını almasının mümkün olduğunu,

2- Pasif taşınmazlara ilişkin sorgu işlemlerinin 3. kişilerin temel hak ve hürriyetlerine aykırılık teşkil etmeyeceğini, yapılacak sorguda borçlunun herhangi bir taşınmazını satıp satmadığının tespit edileceğini, satmış ise kime sattığının ve halen kim adına kayıtlı olduğunun tespit edilmeyeceğini,

3- Talebin kabul edilmesinin dosyanın infazına yarar sağlamayacağına ilişkin gerekçenin ise kabul edilmesinin mümkün olmadığını beyan ederek Manisa 1. İcra Hukuk Mahkemesinin 2016/364-468 E.K. sayılı kararının kaldırılmasına karar verilmesini talep etmiştir.

GEREKÇE: Davacı alacaklı taraf icra müdürlüğüne sunduğu talebi ile borçlu adına kayıtlı pasif taşınmaz kaydı olup olmadığının sorgulanmasını ve borçlunun anne babasını gösterir aile nüfus kaydının sorgulanarak muris tespit edilmesi halinde adına kayıtlı taşınmaz bulunup bulunmadığının sorgulanmasını talep etmiş, müdürlük bu talebi reddetmiştir. Şikayete konu karar bu karardır. Burada çözülmesi gereken ilk ihtilaf borçlu dışındaki kişilerin nüfus kayıt bilgilerinin takip dosyası kapsamında temin edilerek açığa çıkarılmasının mümkün olup olmadığıdır.

Konu ile ilgili mevzuat hükümleri incelendiğinde TC Anayasası madde 13: Temel hak ve hürriyetler, özlere dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak

ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.

TC Anayasası madde 20/3: Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.

Avrupa İnsan Hakları Sözleşmesi madde 8: 1- Herkes, özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

2- Bu hakkın kullanımına, yasa/hukuk uyarınca olması ve ulusal güvenlik, kamu emniyeti ya da ülkenin ekonomik refahı, düzensizliğin ya da suçun önlenmesi, sağlığın ya da ahlakın korunması ya da başkalarının haklarının ve özgürlüklerinin korunması için demokratik toplumda gerekli olması hali istisna olmak üzere, bir kamu makamı tarafından bulunulmayacaktır.

Nüfus Hizmetleri Kanunu madde 9: 1- Nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Bunlar, yetkili ve sorumlu memurlar ile teftiş ve denetim yetkisi olanlar dışında kimse tarafından görülüp incelenemez. Mahkemeler bu hükmün dışındadır.

2- Nüfus kayıtlarına bu bilgileri işleyen memurlar ve Kimlik Paylaşımı Sistemi kapsamında nüfus kayıtlarından faydalanan diğer görevliler de bu gizliliğe uymak zorundadırlar. Bu yükümlülük, kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam eder.

Madde 44: 1- Nüfus kayıt örneklerini; ç) Adli makamlar, nüfus müdürlüklerinden doğrudan almaya yetkilidirler.

Kişisel Verilerin Korunması Kanunu madde 3/1-d) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

Madde 3/1-e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

Madde 5: 1 - Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

2- Aşağıdaki şartlardan birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

- a) Kanunlarda açıkça öngörülmesi.
- b) Fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
- c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- d) ilgili kişinin kendisi tarafından alenileştirilmiş olması.
- e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Madde 28: 1- Bu Kanun hükümleri aşağıdaki hallerde uygulanmaz: ... d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi, düzenlemelerine rastlanmaktadır.

Yukarıda yer verilen mevzuat hükümlerine göre kişinin nüfus kaydının kişisel veri niteliğinde olduğu tartışmasızdır. (Kişisel Verilerin Korunması Kanunu madde 3/1-d) Kişisel verilerin tamamen veya kısmen elde edilerek kaydedilmesi ise kişisel verilerin işlenmesidir. (Kişisel Verilerin Korunması Kanunu madde 3/1-e) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (Kişisel Verilerin Korunması Kanunu madde 5) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenebilmesi ise bu kuralın istisnasıdır.(Kişisel Verilerin Korunması Kanunu madde 28/1-d) Kişisel veri olduğu açık olan nüfus kaydına ilişkin bir başka düzenleme olan Nüfus Hizmetleri Kanununun 9. maddesine göre ise nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Tüm bu hususlardan açıkça anlaşıldığı üzere kişisel veriler ve bu bağlamda nüfus kayıtları gizlidir, edinilip kaydedilmeleri ilgili kişinin açık rızasına bağlıdır ve bu durum gerek Anayasa, gerek Avrupa İnsan Hakları Sözleşmesi ve gerekse kanunlarla düzenlenerek koruma altına alınmıştır. Somut olayda nüfus kaydına ulaşması ve kaydetmesi istenen kurum icra müdürlüğü olup bu kurumun yukarıda belirtilen istisnalar arasında sayılan kurumlardan olmadığı da açıktır.

Davacı tarafın beyanlarında dile getirdiği gibi borçlunun murisi olabilecek kişilerin nüfus kaydına erişilmesinin ve onların ölmüş olup olmadıklarının tespitinin borcu tahsilde alacaklı tarafa katkı sağlayacağı muhakkaktır. Hatta bu durum murisinden kendisine intikal eden malları adına tescil ettirmeyen borçluların bu şekilde davranmalarının önüne geçmek sonucunu da doğurabilecektir. Ancak kişisel verilerin bu şekilde işlenmesi ile elde edilmesi muhtemel yararların yanısıra doğabilecek zararlar da birlikte değerlendirilmelidir.

Anayasa Mahkemesinin 09/04/2014 tarih ve 2013/122 - 2014/74 E. K. sayılı kararında kişisel verilerin niçin gizli tutulması gerektiği ayrıntılı olarak açıklanmıştır. "Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Bilişim teknolojilerindeki gelişmeler sonucunda, geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi; daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkanlarla analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması; verilere erişim ve veri transferinin kolaylaşması; kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler, günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır. Bu bağlamda Anayasa'nın 20. Maddesinin üçüncü fıkrasının son cümlesinde, "Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilerek kişisel verilerin korunması hakkı anayasal güvenceye bağlanmış ve bu şekilde kamu makamlarının keyfi müdahalelerine karşı koruma altına alınmıştır."

O halde yapılacak bir fayda-zarar kıyaslamasında kişisel verilere kolaylıkla ulaşılmamasının yaratması muhtemel olan zararlarının sağlaması muhtemel olan yararlarına göre daha fazla ve daha mühim olduğu anlaşılmaktadır. Tüm bu açıklamalar çerçevesinde davacı tarafın icra müdürlüğüne yaptığı borçlunun anne babasını gösterir aile nüfus kaydının sorgulanarak muris tespit edilmesi halinde adına kayıtlı taşınmaz bulunup bulunmadığının sorgulanmasına ilişkin talebi yerinde olmayıp bu talebin reddine ilişkin' müdürlük kararı doğrudur. Nitekim bu hususta yerleşmeye başlayan uygulama kapsamında da mahkemelerce verilen benzer mahiyetteki kararlar Yargıtay tarafından da onanmaktadır. (Benzer mahiyette Yargıtay 12 H.D.' nin 05/05/2016 tarih ve 2015/33810-2016/13366 E.K. sayılı onama kararı) Davacı tarafın diğer talebi ise borçlunun varsa pasif taşınmaz kayıtlarının sorgulanması talebidir. Alacaklı bu yöndeki bir bilgiye kendisi ulaşamaz. Ancak bu talebin yerine

getirilmesi halinde ulaşacağı pasif taşınmaz kaydı vasıtası ile örneğin tasarrufun iptali gibi bir dava açarak alacağına kavuşma imkanına sahip olabilir. Pasif tapu kaydı sorgulanması da ulaşılacak bilgi borçlu adına daha önce kayıtlı bulunan taşınmaz bilgisi olup bu bilgi bu taşınmazın şimdiki maliki hakkında herhangi bir bilgi içermeyecektir. Bu nedenle bu kaydın dosyaya dahil edilmesi, borçlu dışındaki herhangi bir 3. kişinin bilgilerinin dosyaya yansımaları sonucunu doğurmayacağı gibi borcun tahsili için imkan sağlayabilecektir. O halde bu yöndeki talebin icra müdürlüğünce ve özellikle de dosyanın infazına yarar sağlamayacağı ve borçlu aleyhine delil toplanamayacağı gerekçesi ile reddi yerinde değildir. Davacı tarafın şikayetinin borçlunun varsa pasif taşınmaz kayıtlarının sorgulanması talebinin reddine ilişkin karara karşı yapmış olduğu şikayet yerinde olup, şikayetin bu kısmının da mahkemece reddedilmiş olması yerinde değildir. Yukarıda açıklanan nedenlerle davacı tarafın istinaf başvurusunun kısmen kabulü ile HMK 353/1-b-2 maddesi gereği istinafa konu kararın düzeltilerek yeniden esas hakkında karar verilmesi gerekmiş ve aşağıdaki şekilde hüküm kurulmuştur.

SONUÇ: Yukarıda açıklanan nedenlerle;

Manisa 1. İcra Hukuk Mahkemesinin 2016/364-468 E.K. sayılı kararı HMK 353/1-b-2 maddesi gereği kaldırılarak; Davacı tarafın şikayetinin kısmen kabulü ile; Manisa 5. İcra Müdürlüğünün 2016/2488 esas sayılı takibi kapsamında müdürlükçe alınan 24/06/2016 tarihli kararının "borçlu adına pasif taşınmaz kaydı sorgulanması talebinin reddine" kısmının kaldırılmasına, Aynı kararda borçlunun anne babasını gösterir aile nüfus kaydının sorgulanarak muris tespit edilmesi halinde adına kayıtlı taşınmaz bulunup bulunmadığının sorgulanması talebine yönelik verilen red kararına karşı yapılan şikayetin reddine, Maktu karar harcı ve istinaf yoluna başvurma harcı peşin alındığından yeniden alınmalarına yer olmadığına, Davanın niteliği gereği davacı tarafça yapılan yargılama giderlerinin kendi üzerinde bırakılmasına, Kararın taraflara tebliğine, Dair, dosya üzerinde yapılan inceleme sonucunda 6100 sayılı HMK 'nun 361. maddesi uyarınca kararın tebliğinden itibaren bir ay içerisinde Yargıtay'a temyiz yolu açık olmak üzere, 13.10.2016 tarihinde oybirliği ile karar verildi

Samsun Bölge Adliye Mahkemesi, 4. HD., E. 2018/3525 K. 2019/703 T. 6.3.2019

Esas No.: 2018/3525

Karar No.: 2019/703

Karar Tarihi: 06.03.2019

TÜRK MİLLETİ ADINA

Dairemizce yapılan dosya üzerinden inceleme sonucunda;

GEREĞİ DÜŞÜNÜLDÜ:

İSTEM: Davacı vekili 14/08/2018 havale tarihli dava dilekçesi ile; Borçlu K1 ve F1 Teks. İth. İhr. San. Ve Tic. Ltd. Şti.'nin müvekkili bankaya 3.700.000,00 TL bedelli borcun dolayı Samsun Asliye Ticaret Mahkemesinin 2018/539 Değişik iş 2018/540 karar sayılı kararına istinaden 26/07/2018 tarihinde Samsun icra müdürlüğünün 2018/76840 esas sayılı dosyası ile kambiyo senetlerine özgü haciz yolu ile takip başlatıldığını, yine borçlu K2'nin müvekkili bankaya 200.000,00 TL bedelli borcundan dolayı Samsun Asliye Ticaret Mahkemesinin 2018/255 Değişik iş ve karar sayılı kararına istinaden 09/04/2018 tarihinde Samsun icra müdürlüğünün 2018/39474 esas sayılı dosyası ile kambiyo senetlerine özgü haciz yolu ile takip başlatıldığını, diğer borçlular K3 ve K4 müvekkili bankaya 74.000,00 TL bedelli borcundan dolayı Samsun Asliye Ticaret Mahkemesinin 2018/511 değişik iş 2018/513 karar sayılı kararına istinaden 13/07/2018 tarihinde Samsun icra müdürlüğünün 2018/72628 esas sayılı dosyası ile kambiyo senetlerine özgü haciz yolu ile takip başlatıldığını, Samsun icra müdürlüğünün 2018/39474, 2018/76840 ve 2018/72628 esas sayılı dosyası ile başlatılan takip sonrasında, borçlunun mal kaçırma ihtimalinin bulunmasının öğrenilmesi üzerine Samsun icra müdürlüğünden borçlular adına daha önce kaydı bulunmuş olup 3.kişilere devri yapılmış taşınmazlar var ise araştırılmasının yapılması için icra müdürlüğünden talep edildiğini, icra müdürlüğünce haksız ve hukuka aykırı olarak talebin reddedildiğini, ret gerekçesi olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun 3/1-d maddesine atıf yapılarak 3.şahsın kişisel bilgilerini içerdiği için reddedildiğini, Avukatlık Kanununun 2/3.maddesi uyarınca pasif trafik ve tapu kayıtlarının inceleme yapılmasının mümkün olmadığını, alacağına kavuşmak isteyen alacaklı borçlunun aktif malvarlığı yoksa yahut aktif malvarlığı ile alacağını karşılayamamışsa pasif malvarlığı üzerinden tasarrufun iptali davası açarak dava sonucuna göre alacağını tahsil edebildiğini, iş bu sebeplerle Samsun icra müdürlüğünün

talebi reddetmesinin haksız ve hukuka aykırı olduğunu, 6698 Sayılı Kanunun 3.maddesi ve anayasasının 20.maddesi gerekçe gösterilerek taleplerin reddi usule ve hukuka aykırı olduğunu kanun koyucunun kurallarla zorunlu ve gerekli olan hallerle sınırlı olarak belirtilen konularda ilgili kişinin açık rızası olmaksızın kişisel verilerinin işlenebilmesine olanak sağlamak suretiyle toplumsal yaşamda belirtilen konularda ortaya çıkabilecek gecikme, aksaklık veya düzensizlikler ile hak ve menfaat kayıtlarının engellenmesini sağlamayı amaçladığını, bir hakkın sebepsiz yere sürüncemede bırakılması veya reddedilmesinden dolayı ve bu halin icra ve iflas kanunu hükümlerine ve sair mevzuat hükümlerine aykırı olması nedeni ile icra müdürlüğünün iş bu sürüncemede bıraktığı işlemler hakkında şikayette bulunmak gerektiğini beyanla icra müdürlüğünün red kararının kaldırılarak, İcra müdürlüğünce son 5 yıl içerisinde üçüncü kişilere devri yapılmış olan taşınmazların araştırılıp takdiyatlarının satış ile ilgili tüm tapu resmi senetlerinin uyap dosyasına gönderilmesi pasif kayıtları için uyap kep sistemi üzerinde ilgili tapu müdürlüklerine müzekkere yazılmasına karar verilmesini talep ve dava etmiştir.

SAVUNMA: Dava hasımsız dava olduğundan davalının savunması alınmamıştır.

DELİLLER: Samsun icra müdürlüğünün 2018/72628 esas sayılı dosyası.

İLK DERECE MAHKEMESİ KARAR ÖZETİ: Mahkemesince yapılan yargılama sonucunda; Her ne kadar şikayetçi alacaklı yanın takip dosyasları kapsamında borçluların devir ettiği taşınmazların tespiti amacı ile pasif sorgulama talebinde bulunma hakkı olduğu kabul edilse bile; pasif sorgulama sonucu 3. kişilere devri gerçekleşen taşınmazların kime satıldığı, alıcısı ve satıcısının ad soyad bilgilerinin, satış sözleşmelerinin ve satışa ait akit tablolarının ilgili Tapu Müdürlüğünden sorulması yönündeki talep, yapılacak sorgulamada hali hazırdaki malike ait kişisel bilgilere de ulaşılması mümkün olduğundan Anayasal güvenceye bağlanan kişisel verilerin korunması düzenlemesine aykırı olduğu, kaldı ki, icra müdürlüğünün böyle bir görevi de bulunmadığı, aksi durumun kabulü yukarıda belirtilen kişisel verilerin korunması kuralının ihlali sonucunu doğuracağı, somut olayda alacaklı vekilinin talebi doğrultusunda uyap takbis üzerinden pasif sorgulamanın yapıldığı, ancak alacaklı vekilinin pasif sorgulama sonucu 3. kişilere devri gerçekleşen taşınmazların kime satıldığı, alıcısı ve satıcısının ad soyad bilgilerinin, satış sözleşmelerinin ve satışa ait akit tablolarının ilgili Tapu Müdürlüğünden sorulmasına ilişkin talebinin reddi yönündeki icra müdürlüğünce 2018/72628-2018/76840 ve 2018/39774 esas sayılı dosyaları üzerinden verilen 07-08-09/08/2018 tarihli kararlarının kişisel verilerin korunması kuralı kapsamında usul ve yasaya uygun olduğu belirtilerek, şikayetin reddine karar verilmiştir.

İSTİNAFA BAŞVURAN TARAF VE İLERİ SÜRÜLEN İSTİNAF SEBEPLERİ: Davacı vekili tarafından, dava dilekçesindeki nedenler tekrarlanarak istinaf yasa yoluna başvurulmuştur.

DELİLLERİN DEĞERLENDİRİLMESİ VE GEREKÇE:

Dava; icra müdürlüğünce atkit sorgu yapılmamasına yörelık işleme ilişkin şikayettir.

Samsun İcra Müdürlüğünün 2018/39474 esas sayılı takip dosyası incelendiğinde;alacaklı banka tarafından borçlu K2 hakkında 170.903,08 TL'nin tahsili amacıyla kambiyo senetlerine özgü haciz yoluyla takip başlatıldığı, borçluya ödeme emrinin 03/05/2018 tarihinde tebliğ edildiği, alacaklı vekili tarafından 07/08/2018 tarihli dilekçesi ile borçlu için daha önce kaydı bulunan ve müdürlükçe yapılan takbis sorgusunda üzerinden devir ettiği tespit edilen taşınmazlar ile ilgili son 5 yıl içerisinde 3. kişilere takdiyatlarının, satış ile ilgili tüm tapu resmi senetlerinin dosyaya gönderilmesi için ilgili tapu müdürlüğüne müzekkere yazılmasını talep ettiği, icra müdürlüğünce aynı tarihli kararı ile "Yukarıda anılan mahkeme kararı ve içtihatla belirtildiği üzere, borçlunun uypak takbis sorgusunda çıkan pasif taşınmazlar ile ilgili olarak, KİMLERE, HANGİ TARİHTE VE HANGİ BEDELLE SATILDIĞININ, ALICILARIN AD, SOYAD VE ADRESLERİNİN, SATIŞ SÖZLEŞMESİNİN, SATIŞA İLİŞKİN AKİT TABLOLARININ, ipotekli taşınmazlar için için, İPOTEĞİN DEVAM EDİP ETMEDİĞİ, İPOTEK BORCUNUN KİM TARAFINDAN ÖDENDİĞİ v.b. şeklindeki taleplerinin REDDİNE,"şeklinde karar verildiği anlaşılmıştır.

Samsun İcra Müdürlüğünün 2018/76840 esas sayılı takip dosyası incelendiğinde;alacaklı banka tarafından borçlular K1 ve F1 Teks. İth. İhr. San. Ve Tic. Ltd. Şti. hakkında 3.636.279,92 TL'nin tahsili amacıyla kambiyo senetlerine özgü haciz yoluyla takip başlatıldığı, borçlu K1'ya ödeme emrinin 31/07/2018 tarihinde tebliğ edildiğini, alacaklı vekili tarafından 08/08/2018 tarihli dilekçesi ile borçlu K1 için daha önce kaydı bulunan ve müdürlükçe yapılan takbis sorgusunda üzerinden devir ettiği tespit edilen taşınmazlar ile ilgili son 5 yıl içerisinde 3.kişilere takdiyatlarının, satış ile ilgili tüm tapu resmi senetlerinin dosyaya gönderilmesi için ilgili tapu müdürlüğüne müzekkere yazılmasını talep ettiği, icra müdürlüğünce aynı tarihli kararı ile "Yukarıda anılan mahkeme kararı ve içtihatla belirtildiği üzere, borçlunun uypak takbis sorgusunda çıkan pasif taşınmazlar ile ilgili olarak, KİMLERE, HANGİ TARİHTE VE HANGİ BEDELLE SATILDIĞININ, ALICILARIN AD, SOYAD VE ADRESLERİNİN, SATIŞ SÖZLEŞMESİNİN, SATIŞA İLİŞKİN AKİT TABLOLARININ, ipotekli taşınmazlar için için, İPOTEĞİN DEVAM EDİP ETMEDİĞİ, İPOTEK BORCUNUN KİM TARAFINDAN ÖDENDİĞİ v.b. şeklindeki taleplerinin REDDİNE,"şeklinde karar verildiği anlaşılmıştır.

Samsun İcra Müdürlüğünün 2018/72628 esas sayılı takip dosyası incelendiğinde;alacaklı banka tarafından borçlular K4 ve K3 hakkında 71.959,65TL'nin tahsili amacıyla kambiyo senetlerine özgü haciz yoluyla takip başlatıldığı,borçlu K3'a ödeme emrinin 04/09/2018 tarihinde tebliğ edildiği, alacaklı vekili tarafından 09/08/2018 tarihli dilekçesi ile borçlu K3 için daha önce kaydı bulunan ve müdürlükçe yapılan takbis sorgusunda üzerinden devir ettiği tespit edilen taşınmazlar ile ilgili son 5 yıl içerisinde 3.kişilere takdiyatlarının, satış ile ilgili tüm tapu resmi senetlerinin dosyaya gönderilmesi için ilgili tapu müdürlüğüne müzekkere yazılmasını talep ettiği,icra müdürlüğünce aynı tarihli kararı ile "borçlunun uypap takbis sorgusunda çıkan pasif taşınmazlar ile ilgili olarak, KİMLERE, HANGİ TARİHTE VE HANGİ BEDELLE SATILDIĞININ, ALICILARIN AD, SOYAD VE ADRESLERİNİN, SATIŞ SÖZLEŞMESİNİN, SATIŞA İLİŞKİN AKİT TABLOLARINA AİT BİLGİLERİN İSTENMESİ ile ipotekli taşınmazlar için için İPOTEĞİN DEVAM EDİP ETMEDİĞİ, İPOTEK BORCUNUN KİM TARAFINDAN ÖDENDİĞİ v.b. şeklinde 3. ŞAHISLARIN KİŞİSEL BİLGİLERİNİ İÇEREN taleplerinin REDDİNE,"şeklinde karar verildiği anlaşılmıştır.

Davacı vekilinin istinafi üzerine Dairemizce yapılan inceleme sonunda;İcra dosyasının tarafı olmayan üçüncü kişiye ait 6698 Sayılı Yasa'nın 3/1-d maddesi kapsamında kişisel veri niteliğinde bulunan tapu kaydı ve satış sözleşmelerinin icra müdürlüğünce celbinin istenemeyeceği, aynı Yasanın 28/1-d maddesindeki yargısal organlara tanınan istisnanın, ancak uyumsuzluğun tarafları açısından geçerli olabileceği, Anayasa'nın 20/3. maddesine göre aynı zamanda temel haklardan olan kişisel verilerin korunmasını isteme hakkının, 6698 Sayılı Yasanın 28/1-d maddesinin geniş yorumlanması ile daraltılmayacağı, mülkiyet hakkının korunması zimmında açılacak bir davanın taraflarını tespit edebilmek için 1136 sayılı Avukatlık Kanununun 2/3. maddesine ve Başbakanlık Tapu Kadastro Genel Müdürlüğünün 2001/11 sayılı Genelgesine göre avukatın yazılı başvuru ile tapu sicilinde inceleme yapabileceği ve kanunda kısıtlı olarak öngörülen kişisel verilere ulaşma imkanının bu şekilde sağlanması ile hukuki denetimin de yapılabileceği bu verilere ulaşma imkanının birden fazla yolla sağlanması halinde, verilere kimlerin ulaştığının denetiminin zorlaşacağı nazara alınarak icra müdürlüğünün her bir dosya yönünden borçlulara ait pasif taşınmaz kaydı dışında kalan sorgulama taleplerinin reddine yönelik kararının ve bu karara yönelik şikayetin mahkemesince reddinin isabetli olduğu sonucuna ulaşılmıştır.

Kaldı ki davacı vekilinin borçluya ait pasif kayıtların celbedilmesine yönelik talebi Yargıtay 12. H.D'nin bu yöndeki uygulaması nazara alınarak İcra Müdürlüğünce şikayete konu edilen her bir dosyada kabul edilmiş, gerekli sorgulama da yapılmıştır.

Dava ve takip dosyası içeriğine, dosyadaki yazılara göre ilk derece mahkemesi kararında usule ve esasa ilişkin herhangi bir aykırılığın bulunmadığı, davanın esasıyla ilgili hükme etki edecek tüm delillerin dava ve takip dosyası içinde bulunduğu, kanunun olaya uygulanmasında ve gerekçede hata edilmediği, Mahkemece de belirtildiği üzere, davacı vekilinin pasif taşınmazların devir sözleşmelerinin gönderilmesine, taşınmazları devralan şahıslara ilişkin kimlik bilgileri ile açık adreslerinin gönderilmesine yönelik talebinin dosyanın tarafı olmayan üçüncü şahıslar açısından kişi bilgilerinin gizliliğine aykırılık teşkil edeceği, bu hususun talep eden vekili tarafından tapu müdürlüğünden tespit edilebileceği, bu nedenle inceleme konusu kararın usul ve esas yönünden hukuka uygun olduğu anlaşıldığından, istinaf isteminin esastan reddi gerektiği kanaatine varılarak aşağıdaki şekilde hüküm kurulmuştur.

HÜKÜM: Gerekçesi yukarıda açıklandığı üzere;

1- Davacı vekilinin istinaf başvurusunun 6100 sayılı HMK'nun 353/1-b-1 maddesi gereğince ESASTANREDDİNE,

2- Alınması gereken 44,40 TL karar harcından peşin alınan 35,90 TL harcın mahsubu ile eksik 8,50 TL harcın davacıdan alınarak hazineye gelir kaydına,

3- Dosyanın İstinaf Mahkemesine gönderilmesi amacıyla yapılan harç, posta masrafı ve tebligat giderlerinin istinaf kanun yoluna başvuran taraf üzerinde bırakılmasına,

4- İnceleme duruşmasız yapıldığından vekalet ücretine hükmedilmesine yer olmadığına,

5- Kararın taraflara tebliğine,

Dair, HMK'nın 353/1-b-1 maddesi uyarınca dosya üzerinden yapılan inceleme sonunda, HMK'nın 361. maddesi uyarınca kararın tebliğinden itibaren 2 hafta içerisinde Yargıtay temyiz yolu açık olmak üzere oy birliğiyle karar verildi. 06/03/2019

Samsun Bölge Adliye Mahkemesi, 4. HD., E. 2018/3158 K. 2019/845 T. 18.3.2019

Esas No.: 2018/3158

Karar No.: 2019/845

Karar Tarihi: 18.03.2019

TÜRK MİLLETİ ADINA

DAVANIN KONUSU: Şikayet (İcra Memur Muamelesi)

Dairemizce yapılan dosya üzerinden inceleme sonucunda;

GEREĞİ DÜŞÜNÜLDÜ:

İSTEM: Davacı vekili dava dilekçesinde özetle; müvekkilinin alacaklı olduğu Samsun 9.İcra Müdürlüğü'nün 2018/98579 Esas sayılı dosyasında borçlunun anne baba kaydını gösterir nüfus aile kayıt örneği talep edildiğini, bu hususa ilişkin talebinin sebebi dosya borçlularının anne babalarının ölü olup olmadığının ve ölü ise borçluların mirasçı olup olmadığına ilişkin veraset ilamını çıkarmak ve intikal edecek malvarlığının sorgulanması ve müvekkilin alacağını tahsil amacıyla intikal edecek malvarlığına haciz konulma süresinin başlatılması olduğunu, hukuka aykırı olarak talebin reddedildiğini, şikayetin kabulü ile red işleminin iptaline karar verilmesini talep ve dava etmiştir.

SAVUNMA: Evrak üzerinden inceleme yapılmıştır.

DELİLLER: Samsun 9.İcra Müdürlüğü'nün 2018/98579 Esas sayılı dosyası.

İLK DERECE MAHKEMESİ KARAR ÖZETİ: Mahkemece yapılan yargılama sonucunda borçlu dışında kalan aile efradından olan anne, baba ve eşin nüfus kaydının alınarak ölü olup olmadıkları ve ölmüş iseler dosyaya taraf kaydederek mal varlığı sorgulamasının ve araştırmasının yapılmasının icra dosyası ile ilgisi olmayan 3. kişiler yönünden uygulanmasının mümkün olmadığı, nüfus kaydı ve diğer sorgulama işlemlerinin hakkında takip kesinleşen borçlular yönünden uygulanacağı, 3. kişiler ile ilgili yapılacak sorgulamaların Anayasanın 20. Maddesinde düzenlenen temel hak ve hürriyetlere aykırılık oluşturduğu, kişilerin verilen gizliliğinin güvence altına alındığı, takip ile ilgisi bulunmayan borçlu durumunda olmayan kişilerin kişisel kimlik bilgileri ile durumlarının araştırılmasının icra müdürlüğünde görevli katip ve müdürlerin görevleri kapsamında bulunmadığı, alacaklı vekilince, borçlunun anne ve babasının ölmüş olduğunun bildirilmesi ve taşınmaz

bilgilerinin sunulması halinde İİK'nun 94.maddesi gereğince işlem yapılabileceği belirtilerek şikayetin reddine karar verildiği görülmüştür.

İSTİNAFA BAŞVURAN TARAF VE İLERİ SÜRÜLEN İSTİNAF SEBEPLERİ: Davacı vekili tarafından, dava dilekçesindeki nedenler tekrarlanarak istinaf yasa yoluna başvurulmuştur.

DELİLLERİN DEĞERLENDİRİLMESİ VE GEREKÇE:

Davanın İİK'nun 16. v.d. maddeleri uyarınca açılmış Şikayete ilişkin olduğu anlaşılmıştır.

Davacı vekili, dava dilekçesi ile müvekkilinin alacaklı olduğu Samsun 9.İcra Müdürlüğü'nün 2018/98579 Esas sayılı dosyasında borçluların anne babalarının ölü olup olmadığı, ölü ise borçluların mirasçı olup olmadığına ilişkin veraset ilamını çıkarmak ve intikal edecek malvarlığının sorgulanması ve müvekkilin alacağını tahsil amacıyla intikal edecek malvarlığına haciz konulma süresinin başlatılması maksadıyla borçlunun anne baba kaydını gösterir nüfus aile kayıt örneği taleplerinin icra müdürlüğüne hukuka aykırı olarak reddedildiğini bildirerek icra müdürlüğünün red işleminin iptaline karar verilmesini talep etmiş, Mahkemece yukarıda anılan gerekçe ile şikayetin reddine karar verilmesi üzerine davacı tarafca istinafa gelindiği anlaşılmıştır.

Uyuşmazlığın çözümü için somut olayda çözülmesi gereken ihtilaf borçlu dışındaki kişilerin nüfus kayıt bilgilerinin takip dosyası kapsamında temin edilerek çıkarılmasının mümkün olup olmadığıdır.

İcra dosyasının tarafı olmayan üçüncü kişiye ait 6698 sayılı yasanın 3/1-d maddesi kapsamında kişisel veri niteliğinde bulunan nüfus kayıtlarının icra müdürlüğüne istenmesi mümkün değildir. Aynı yasanın 28/1-d maddesindeki yargısal organlara tanınan istisna ancak uyuşmazlığın tarafları açısından geçerli olabilir. T.C Anayasasının 20/3. maddesine göre aynı zamanda temel haklardan olan kişisel verilerin korunmasını isteme hakkının, 6698 sayılı yasanın 28/1-d maddesinin geniş yorumlanması ile daraltılması da mümkün değildir. Vekilin, Avukatlık Yasası'nın 2/3 maddesinden kaynaklanan yetkisi ile nüfus kayıtlarına ulaşarak borçlu veya 3. kişilere karşı yasadan doğan dava hakkını kullanması mümkündür. Alacaklının bu talebi ile yapılacak sorgulama ile takip dosyası tarafı olmayan 3. kişilerin bilgilerine ulaşılması mümkün olduğundan, bu istem Anayasal güvenceye bağlanan kişisel verilerin korunması düzenlenmesine aykırıdır. Alacaklının hukuki yararının, üçüncü kişilerin Anayasa ile korunan özel hayatın gizliliğine ilişkin temel hakkından daha üstün tutulması mümkün değildir.

İcra müdürlüğünün görev ve yetkileri 2004 Sayılı İcra İflas Kanunu'nda ayrıntılı olarak düzenlenmiştir. İcra müdürlüğüne gerekli araştırma ve sorgulama işlemleri alacağın tahsiline

yönelik sınırlı işlemler için gerçekleştirilebilir. Aksi durumun kabulü kişisel verilerin korunması kuralının ihlali sonucunu doğurur.

Öte yandan; borçlunun murisi olabilecek kişilerin nüfus kaydına erişilmesinin ve onların ölmüş olup olmadıklarının tespitinin alacağın tahsilinde alacaklı tarafa katkı sağlayacağı muhakkaktır. Hatta bu durum murisinden kendisine intikal eden malları adına tescil ettirmeyen borçluların bu şekilde davranmalarının önüne geçmek sonucunu da doğurabilir. Ancak kişisel verilerin bu şekilde işlenmesi ile elde edilmesi muhtemel yararların yanısıra doğabilecek zararlar da birlikte değerlendirilmelidir. Anayasa Mahkemesinin 09/04/2014 tarih ve 2013/122-2014/74 EK sayılı kararında kişisel verilerin niçin gizli tutulması gerektiği ayrıntılı olarak açıklanmıştır. "Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Bilişim teknolojilerindeki gelişmeler sonucunda, geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi; daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması; verilere erişim ve veri transferinin kolaylaşması; kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler, günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır. Bu bağlamda Anayasa'nın 20. Maddesinin üçüncü fıkrasının son cümlesinde, "Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilerek kişisel verilerin korunması hakkı anayasal güvenceye bağlanmış ve bu şekilde kamu makamlarının keyfi müdahalelerine karşı koruma altına alınmıştır." Bu durumda, yapılacak bir fayda-zarar kıyaslamasında kişisel verilere kolaylıkla ulaşılmasının yaratması muhtemel olan zararlarının, sağlanması muhtemel olan yararlarına göre daha fazla ve daha mühim olduğu anlaşılmaktadır.

Açıklanan sebeplerle; ilk derece mahkemesi kararının usul ve yasaya uygun olduğu, davacının istinaf başvuru nedenlerinin yerinde olmadığı, kararda kamu düzenine aykırılık da bulunmadığı anlaşılmakla HMK'nın 353/1-b-1 maddesi gereğince başvurunun esastan reddine karar verilmesi gerekmiştir.

HÜKÜM: Gerekçesi yukarıda açıklandığı üzere;

1- Davacı vekilinin istinaf başvurusunun 6100 sayılı HMK.nun 353/1-b-1 maddesi gereğince ESASTANREDDİNE,

2- Alınması gereken 44,40 TL karar harcından peşin alınan 35,90 TL harcın mahsubu ile eksik 8,50 TL harcın davacıdan alınarak hazineye gelir kaydına,

3- Dosyanın İstinaf Mahkemesine gönderilmesi amacıyla yapılan harç, posta masrafı ve tebligat giderlerinin istinaf kanun yoluna başvuran taraf üzerinde bırakılmasına,

4- İnceleme duruşmasız yapıldığından vekalet ücretine hükmedilmesine yer olmadığına,

5- Kararın taraflara tebliğine

Dair, HMK'nın 353/1-b-1 maddesi uyarınca dosya üzerinden yapılan inceleme sonunda, HMK'nın 361. maddesi uyarınca kararın tebliğinden itibaren 2 hafta içerisinde Yargıtay temyiz yolu açık olmak üzere oy birliğiyle karar verildi.18/03/2019

Samsun Bölge Adliye Mahkemesi, 4. HD., E. 2018/1643 K. 2018/2511 T. 1.11.2018

Esas No.: 2018/1643

Karar No.: 2018/2511

Karar Tarihi: 01.11.2018

TÜRK MİLLETİ ADINA

DAVANIN KONUSU: Şikayet (İcra Memur Muamelesi)

Dairemizce yapılan dosya üzerinden inceleme sonucunda;

GEREĞİ DÜŞÜNÜLDÜ:

İSTEM: Davacı vekili 22/03/2018 havale tarihli dava dilekçesi ile; Samsun 9.İcra Müdürlüğünün 2017/147084 Esas sayılı dosyası ile takip başlatıldığını, borçlunun babası K1'nin vefat ettiğini, bu nedenle Samsun 6. Noterliğinden icra dairesinden alınan yetkiye istinaden borçlunun babasının mirasçılarını gösterir veraset ilamı temin edildiğini, bunun üzerine Samsun 9. İcra Müdürlüğüne talep gönderildiğini, borçlu K2'nin dedesinin sisteme muris olarak kaydedilmesini borçluya babasından intikal eden taşınır ve taşınmaz malların sorgulanmasını talep ettiklerini icra müdürlüğünün bu talebi reddettiğini, borçluya intikali gerçekleşek olan taşınır ve taşınmaz malların sorgulanarak tespit edilmesi ve ilerde oluşan iş bu elbirliği mülkiyetinin sona ermesi durumunda borçluya ait olacak payın belirlenebilmesine ilişkin taleplerinin bulunduğunu, bu malların iştirak halinde olsa da borçlunun mal varlığı içinde olduğunu talep ile mal varlığının tespitinden sonra haciz intikal ve satış işlemleri prosedürü işyeleceğini, bu duruma ilişkin icra müdürlüğünün 14/03/2018 tarihli kararının düzeltilmesini talep ettiği, icra takibi neticesinde borçlulardan F1 Anonim Şirketi üzerine düşen tutarı dosyaya ödediğini, ancak icra müdürlüğü tarafından ödeme yapılırken yapılacak tutar ile ilgili yanlış hesaplamalar yapıldığını, borçlu F1 Anonim Sigorta Şirketi tarafından dosyaya mehil vesikası verildiğini bu borçlu yönünden haciz işleminin uygulanmadığını, bu borçlunun ödemesi yönünden tahsil harcının hacizli malı bulan borçlular tarafından yapılan ödemeye ilişkin oranlara göre hesaplanarak kesilmesinin (%9,10 üzerinden) usul ve yasaya aykırı olduğunu, tahsil harcının hesaplandığı %9,10 oranının hatalı olduğunun tespit edilmesini ve bu işlemin kaldırılmasına karar verilmesini talep ve dava etmiştir.

SAVUNMA: Dosya üzerinden karar verildiğinden davalının savunması alınmamıştır.

DELİLLER: Samsun 9.İcra Müdürlüğünün 2017/147084 Esas sayılı dosyası.

İLK DERECE MAHKEMESİ KARAR ÖZETİ: Mahkemesince yapılan yargılama sonucunda; icra müdürlüğünün 14/03/2018 tarihinde henüz borçlu adına tescili yapılmayan taşınmaz üzerine haciz konulmasının mümkün olmadığı gibi satış isteme hakkı vermemesi sebebiyle konulsa dahi alacaklı tarafa hiç bir hukuki yarar sağlamayacağını, bu aşamada borçlu adına henüz intikali yapılmamış mal üzerine haciz konulması talebinin reddine dair vermiş olduğu kararın usul ve yasaya uygun bulunduğunu, davacının bu yöndeki şikayetinin reddine karar verilmesi gerektiğini, yine her ne kadar davacı vekilince F1 Anonim Türk Sigorta Şirketi Yönünden mehil vesikası verildiğinden haciz işlemi uygulanmadığını, sigorta şirketi yönünden istinaf başvurusunun kabul edildiğini, alacak kalemlerinin sigorta şirketi yönünden değiştirildiği ve sorumluluk tutarının istinaf mahkemesi kararı ile belirlendiğini, bunun üzerine sigorta şirketi tarafından sorumluluk tutarı borç miktarının takip dosyasına yatırıldığını, diğer borçlular yönünden herhangi bir ödemenin sözkonusu olmadığını, bu nedenle yalnız ödeme yapan borçlu yönünden tahsil harcı kesilmesi gerekirken tüm borç tutarı ödenmiş gibi tahsil harcı kesilmesinin usul ve yasaya uygun bulunmadığı belirtilmişse de diğer borçluların sigorta şirketinin sorumlu bulunduğu tutardan müteselsilen sorumlu buldukları ve bu borçlular yönünden takip dosyası kapsamında haciz işleminin uygulandığını, icra takibi sonucunda kesinleşen borç miktarının dosya kapsamına yatırılan miktardan daha fazla olduğunu, bu hali ile icra müdürlüğünce alacaklı vekiline ödeme yapılırken dosya kapsamına yatırılan toplam tutar üzerinden % 9,10 oranında tahsil harcı ile % 2 oranında cezaevi harcı alınmasına ilişkin 12/03/2018 tarihli kararın usul ve yasaya uygun bulunduğu sonuç ve kanaatine ulaşılarak açılan davanın kabulüne karar verilmiştir.

İSTİNAFA BAŞVURAN TARAF VE İLERİ SÜRÜLEN İSTİNAF SEBEPLERİ: Davacı vekili tarafından, dava dilekçesindeki nedenler tekrarlanarak istinaf yasa yoluna başvurulmuştur.

DELİLLERİN DEĞERLENDİRİLMESİ VE GEREKÇE:

Dava; İİK'nın 16 vd. maddeleri kapsamında şikayettir.

Samsun 9. İcra Müdürlüğünün 2017/147084 takip sayılı dosyasının incelenmesinde; alacaklılar K3, K4, K5 ve K6 tarafından borçlular F2 Ev Aletleri San. Gıda ve Paz. Tic. Ltd. Şti, K2 ve F1 Sigorta A.Ş hakkında Samsun Asliye Ticaret Mahkemesinin 2016/931 esas 2017/926 karar sayılı ilamına ilişkin 886.753,06TL alacağın tahsili amacı ile icra takibi başlatıldığı, davacı alacaklı vekili tarafından borçlunun babasının taraf olarak takip dosyasına eklenmesine yönelik talepte bulunulduğu, bu talebinin icra müdürlüğünce 14/03/2018 tarihinde "talabindavacı tarafa hiç bir hukuki yarar sağlamayacağı, ayrıca mirasçılık ilişkisini ispata yarar veraset ilamı dosyada bulunmadığı,

dolayısıyla mirasın borçluya intikal edip etmeyeceğinin henüz belli olmayacağı, belirtilerek reddine karar verildiği görülmüştür.

Borçlunun K2nin dedesinin sisteme muris olarak kaydedilerek malvarlığının sorgulanması talebinin reddine yönelik istinaf başvurusu hakkında yapılan değerlendirmede;

İstinaf itirazının sağlıklı bir şekilde yapılabilmesi için borçlu dışındaki kişilerin nüfus kayıt bilgilerinin takip dosyası kapsamında temin edilerek açığa çıkarılmasının mümkün olup olmadığı hususunun açıklığa kavuşturulması gerekir.Bunun için konuyla ilgili mevzuat hükümlerinin incelenmesi gerekir.

TC Anayasasının 13.maddesinde; "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz."

TC Anayasası madde 20/3 maddesinde; "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." düzenlemeleri yer almaktadır.

Avrupa İnsan Hakları Sözleşmesi madde 8 maddesinde de; "1-Herkes, özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

2-Bu hakkın kullanımına, yasa/hukuk uyarınca olması ve ulusal güvenlik, kamu emniyeti ya da ülkenin ekonomik refahı, düzensizliğin ya da suçun önlenmesi, sağlığın ya da ahlakın korunması ya da başkalarının haklarının ve özgürlüklerinin korunması için demokratik toplumda gerekli olması hali istisna olmak üzere, bir kamu makamı tarafından bulunulmayacaktır. " hükümlerine yer verilmiştir.

Nüfus Hizmetleri Kanunu 9.maddesine göre de;"1-Nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Bunlar, yetkili ve sorumlu memurlar ile teftiş ve denetim yetkisi olanlar dışında kimse tarafından görülüp incelenemez. Mahkemeler bu hükmün dışındadır.

2- Nüfus kayıtlarına bu bilgileri işleyen memurlar ve Kimlik Paylaşımı Sistemi kapsamında nüfus kayıtlarından faydalanan diğer görevliler de bu gizliliğe uymak zorundadırlar. Bu yükümlülük, kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam eder.

Aynı kanunun44.maddesine göre,1- Nüfus kayıt örneklerini;ç) Adlî makamlar,nüfus müdürlüklerinden doğrudan almaya yetkilidirler.

Kişisel Verilerin Korunması Kanunu madde 3/1-d maddesinde;Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

Madde 3/1-e) Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

Madde 5: 1- Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

Madde 28: 1-Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:....d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi" şeklinde düzenleme yapıldığı görülmektedir.

Açıklanan bu hükümlere göre, kişinin nüfus kaydı kişisel veri niteliğinde olup nüfus kayıtlarının tamamen veya kısmen elde edilerek kaydedilmesi ise kişisel verilerin işlenmesidir. Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenebilmesi ise bu kuralın istisnasıdır. Kişisel veri olduğu açık olan nüfus kaydına ilişkin bir başka düzenleme olan Nüfus Hizmetleri Kanununun 9. maddesine göre ise nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Tüm bu düzenlemelerden açıkça anlaşıldığı üzere kişisel veriler ve bu bağlamda nüfus kayıtları gizli olup edinilip kaydedilmeleri ilgili kişinin açık rızasına bağlıdır ve bu durum gerek Anayasa, gerek Avrupa İnsan Hakları Sözleşmesi ve gerekse kanunlarla düzenlenerek koruma altına alınmıştır. Somut olayda nüfus kaydına ulaşması ve kaydetmesi istenen kurum icra müdürlüğü olup bu kurum yukarıda belirtilen istisnalar arasında sayılan kurumlardan değildir.

Esasen alacaklı tarafın borçlunun murisi olabilecek kişilerin nüfus kaydına erişilmesinin ve onların ölmüş olup olmadıklarının tespitini istemekte borcu tahsil bakımından yararı bulunduğu açıktır. Ancak kişisel verilerin bu şekilde işlenmesi ile elde edilmesi muhtemel yararların yanısıra doğabilecek zararlar da birlikte değerlendirilmelidir. Anayasa Mahkemesinin 09/04/2014 tarih ve 2013/122-2014/74 EK sayılı kararında kişisel verilerin niçin gizli tutulması gerektiği ayrıntılı olarak açıklanmıştır. "Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel

verilerin işlenmesi sırasında korumayı amaçlamaktadır. Bilişim teknolojilerindeki gelişmeler sonucunda, geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi; daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması; verilere erişim ve veri transferinin kolaylaşması; kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler, günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır. Bu bağlamda Anayasa'nın 20. Maddesinin üçüncü fıkrasının son cümlesinde, "Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilerek kişisel verilerin korunması hakkı anayasal güvenceye bağlanmış ve bu şekilde kamu makamlarının keyfi müdahalelerine karşı koruma altına alınmıştır." O halde yapılacak bir fayda-zarar kıyaslamasında kişisel verilere kolaylıkla ulaşılmasının yaratması muhtemel olan zararlarının sağlamsa muhtemel olan yararlarına göre daha fazla ve daha mühim olduğu anlaşılmaktadır.

Tüm bu açıklamalar çerçevesinde davacı tarafın icra müdürlüğüne yaptığı borçlunun dedesinin sisteme kaydedilerek taşınmaz bilgilerinin sorgulanmasına ilişkin talebi yerinde olmayıp bu talebin reddine ilişkin müdürlük kararı doğrudur. Nitekim bu hususta yerleşmeye başlayan uygulama kapsamında da mahkemelerce verilen benzer mahiyetteki kararlar Yargıtay tarafından da onanmaktadır. (Benzer mahiyette Yargıtay 12 HD' nin 05/05/2016 tarih ve 2015/33810-2016/13366 Esas Karar ve yine aynı Dairenin 15.02.2018 tarih ve 2016/32416 esas 2018/1370 karar sayılı onama kararları) Davacı tarafın buna yönelik istinaf itirazının esastan reddi gerekir.

Davacı vekili, yalnız ödeme yapan borçlu yönünden tahsil harcı kesilmesi gerekirken tüm borç tutarı ödenmiş gibi tahsil harcı kesilmesinin usul ve yasaya uygun bulunmadığını belirtmiştir; ancak, diğer borçluların sigorta şirketinin sorumlu bulunduğu tutardan müteselsilen sorumlu buldukları ve icra takibi sonucunda kesinleşen borç miktarının dosya kapsamına yatırılan miktardan daha fazla olduğu, bu hali ile icra müdürlüğüne alacaklı vekiline ödeme yapılırken dosya kapsamına yatırılan toplam tutar üzerinden tahsil harcı kesilmesinde ve aynı gerekçe ile şikayetin reddine karar verilmesinde bir isabetsizlik bulunmamaktadır.

Davacı vekilinin tahsil harcının oranına yönelik istinaf istemine gelince, 492 Sayılı Harçlar Kanunu'na ekli (1) sayılı tarifinin icra harçlarını düzenleyen B-1/3-a maddesine göre; ödeme, ödeme ve icra emrinin tebliğinden sonra, fakat hacizden önce yapılmışsa, ödenen paralardan % 4,55 tahsil harcı

alınmaktadır. Aynı Yasa'nın 3/b bendinde ise; tahsil harcının, "hacizden sonra ve satıştan önce ödenen paralardan % 9,10 oranında kesileceği öngörülmüştür. Somut olayda; takip borçlusu F1 Sigorta A.Ş tarafından henüz kendisi yönünden haciz yapılmadan 27.02.2018 tarihinde 102.317,00 TL ödeme yapıldığı görülmektedir. Bu nedenle, ödenen paradan % 4,55 oranında tahsil harcı kesilmesi gerekirken % 9.10 oranında tahsil harcı kesilmesi hatalıdır.

HMK 353/1-b-2 maddesine göre ön inceleme sonunda dosyada eksiklik bulunmadığı anlaşılırsa; yargılamada eksiklik bulunmamakla beraber, kanunun olaya uygulanmasında hata edilip de yeniden yargılama yapılmasına ihtiyaç duyulmadığı takdirde veya kararın gerekçesinde hata edilmiş ise düzelterek yeniden esas hakkında, duruşma yapılmadan karar verilir. Gerçekleşen bu durum karşısında; kararın kaldırılarak, belirlenen gerekçe çerçevesinde şikayetin tahsil harcı yönünden kabulüne, 12.03.2018 tarihli kararın harç oranı yönünden iptaline, diğer şikayetlerin reddine dair yeni bir hüküm kurulması gerektiğikanaatine varılarak aşağıdaki şekilde hüküm kurulmuştur.

HÜKÜM: Gerekçesi yukarıda açıklandığı üzere;

1-Davacı vekilinin istinaf başvurusunun; 6100 sayılı HMK.nun 353/1-b-2 maddesi uyarınca tahsil harcı yönünden KABULÜ ile, Samsun 1.İcra Hukuk Mahkemesinin 2018/160 E - 2018/196 K sayılı kararının KALDIRILMASINA, yerine aşağıdaki hükmün oluşturulmasına,

"1-Davacının şikayetinin tahsil harcı yönünden KABULÜ ile, Samsun9. İcra Müdürlüğü'nün 2017/147084 esas sayılı takip dosyasında 12/03/2018 tarihli kararın harç oranı yönünden İPTALİNE, diğer şikayetlerinin REDDİNE,

2- Harç peşin alınmış olmakla yeniden harç alınmasına yer olmadığına,

3- Şikayetin niteliği ve duruşma açılmaması nazara alınarak yargılama giderlerinin davacı üzerinde bırakılmasına, vekalet ücreti takdirine yer olmadığına,

4- Taraflarca yatırılan gider avansından arta kalan kısmın Yönetmeliğin 5. maddesi gereğince hüküm kesinleştiğinde taraflar hesap numarası bildirmiş ise elektronik ortamda, bildirmemiş ise masrafı avanstaki karşılama suretiyle PTT vasıtasıyla adreste ödemeli olarak kendisine gönderilmesine,"

2- Harç peşin olarak alındığından yeniden harç alınmasına yer olmadığına,

3- Dosyanın İstinaf Mahkemesine gönderilmesi amacıyla davacı tarafından yapılan masrafların kendi üzerinde bırakılmasına,

4- İnceleme duruşmasız yapıldığından, vekalet ücretine hükmedilmesine yer olmadığına,

5- Kararın davacı tarafa tebliğine,

HMK'nın 353/1-b-2 maddesi uyarınca dosya üzerinden yapılan inceleme sonunda, HMK'nın 361. maddesi uyarınca kararın tebliğinden itibaren 2 hafta içerisinde temyiz yolu açık olmak üzere oy birliğiyle karar verildi. 01/11/2018

ADLİ YARGI İLK DERECE MAHKEMELERİ KARARLARI

Bölüm İçeriği

- İstanbul 10. Asliye Ticaret Mahkemesi (E. 2020/616)
- İstanbul 4. Asliye Ticaret Mahkemesi (E. 2019/279)

İstanbul 10. Asliye Ticaret Mahkemesi (E. 2020/616)

İstanbul 10. Asliye Ticaret Mahkemesi, E. 2020/616 K. 2021/64, T. 27.1.2021

DAVA: Bilgi Alma Ve İnceleme Hakkı İhlali

DAVA TARİHİ: 06/11/2020

Mahkememizde görülmekte olan Ticari Şirket (Bilgi Alma Ve İnceleme Hakkı İhlali) davasının yapılan açık yargılaması sonunda,

DAVA: Davacı mahkememize vermiş olduğu dava dilekçesi ile, davalı şirketin azınlık pay sahibi olduğunu, TTK'nun 437.mad ile tanınan bilgi alma ve inceleme hakkını kullanarak, şirkete 01/10/2020 ve 12/10/2020 tarihlerinde, davalı şirkete e-posta yoluyla müracaat ederek çoğunluk pay sahiplerinin belirlediği yönetim kurulundan tüm personelin 2018,2019,2020 Mart aylarına ait maaş bordrolarını, 2017,2018,2019 yıllarına ait olağan genel kurul toplantısı gününde pay sahibi olanların listelerini istediğini bu yöndeki talebinin 08/10/2020 ve 30/10/2020 tarihlerinde, isimsiz imzasız cevap ile haksız olarak red edildiğini, bilgi alma hakkının, pay sahipliği haklarının kullanılabilmesi için gerekli olması koşuluna bağlandığını, bilgi alma hakkının, bu hakkın kullanıldığı genel kurul toplantısının gündemindeki konularla da sınırlı olmadığını, şirket yöneticileri ve denetçilerin, pay sahibinin bilgi alma hakkını kullanırken istediği bilgileri vermekten ancak şirket sırrı ve korunmaya değer şirket menfaatleri kriterlerine uygun bir gerekçe ile kaçınabildiklerini, TTK'nun bir yenilik olarak, aktif bilgi alma ve inceleme hakkının kullanılması talebinin, anonim şirket genel kurulu veya yönetim kurulu tarafından haksız yere red edilmesi halinde, pay sahibine mahkemeye müracaat hakkı tanıdığını, Medeni Kanununun 2.maddesine göre de ancak dürüstlük kuralına aykırı talebin redde söz konusu olabileceğini, bunların dışında bir sebeple alma hakkı ret edilemez, davalı şirketin ret gerekçesi olarak KVKK göstermesinin de saygısızlık olduğunu beyanla, davanın kabulüne, davalıdan talep ettiği 6 ayrı belgeyi bilgisayar dosyası olarak tarafına verilmesine karar verilmesini talep ve dava etmiştir.

CEVAP: Davalı vekili mahkememize vermiş olduğu cevap dilekçesi ile, davacının 20/03/2020 tarihli olağan genel kurul toplantı tarihi itibarıyla davalı şirketin yüz binde 6,01 payına sahip ortağı olduğunu, genel kurul toplantısının 2 numaralı gündemi ile şirketin nakit durum ve yönetimine ilişkin soru sorduğu, 3 numaralı gündemi görüşülürken davacının şirket çalışanlarına yapılan ödemeler hakkında bilgi talep ettiğini, yine 7 numaralı gündemi görüşülürken davacının yönetim kurulu üyeliklerinin belirlenmesine ilişkin soru yönelttiğini ve davacı tarafından sorulan sorulara

yönelik genel müdür tarafından açıklama yapıldığını, davacının gündemin 2,3 ve 7.maddelerine yönelik muhalefet şerhini yazdırmadığını, davacının 20/03/2020 tarihli olağan genel kurul toplantısından 7 ayı aşkın bir süre geçtikten sonra gmail adresinden gönderdiği e-posta ile davalı şirketten talepte bulunduğunu, davacının dava konusu hususlarda genel kurulda bilgi alma ve inceleme talebinde bulunmadığından dava şartının gerçekleşmediğini, TTKnun 437.maddesinde mahkemeden bilgi isteme ve inceleme talebinde bulunabilmek için pay sahibinin genel kurulda bu hususta istemde bulunmuş olmasının özel bir dava şartı olduğunu, TTKnun 437/5.maddesinde ön görülen 10 günlük hak düşürücü süre dolduğundan HMKnun 142.maddesi uyarınca davanın usulden reddine karar verilmesi gerektiğini, davacının TTKnun 437/5 maddesi uyarınca toplantı tarihini izleyen on günlük sürenin sonu olan 31/03/2020 tarihine kadar bilgi alma ve inceleme hakkının ihlali davası açması gerekirken, 10 günlük hak düşürücü süre geçtikten sonra 7 ay sonra 06/11/2020 tarihinde dava açtığını, davacıya davalı şirketin tüm personelinin maaş bordrolarının bilgisayar ortamında verilmesinin, 6698 sayılı KVKK'na aykırı ve TCK uyarınca suç teşkil ettiği gibi şirket sırlarını da ifşa edeceğinden davacının maaş bordrolarının bilgisayar ortamında verilmesi talebinin de kanuna aykırı olduğunu, davacının MKK nezdinde tutulan pay defterinden sadece kendi paylarına ilişkin inceleme yapabileceğini, genel kurul toplantısına katılan tüm pay sahiplerinin KAP'ta yayımlanan olağan genel kurul toplantısında hazır bulunanlar listesinden incelenmesi mümkün olmasına rağmen davacının pay sahipleri listesini talep etmesinde hukuki yarar bulunmadığını, davacının davalı şirketin hak ve yetkisi olmayan bir ifayı yerine getirmesini hukuka aykırı olarak talep ettiğini beyanla, davanın reddine karar verilmesini talep etmiştir.

DELİLLER VE GEREKÇE:

Taraflara usulüne uygun davetiye tebliğ edilmiş olup, g-mail yazışmaları, portföy hesap bakiyesi, 30/09/2020 ve 09/10/2020 tarihli olağan genel kurul pay sahipleri listesi, bilgi alma ve inceleme haklarının kullanılmasına yönelik makaleler, 20/03/2020 tarihli olağan genel kurul toplantısına ait hazır bulunanlar listesi, olağan genel kurul toplantı tutanağı, Yargıtay ilamı, veri kategorileri, 20/03/2020 ... AŞ genel kurul toplantısı 2.gündem maddesi müzakeresi, ... yönetim kurul faaliyet raporu celp olunmuştur.

Dava, davacının hissedarı olduğu davalı şirketten bilgi edinme ve inceleme hakkının kullanılmasına yönelik dava olduğunun tespitine ilişkindir.

6102 sayılı TTK'nun 437.maddesinde; "(1) Finansal tablolar, konsolide finansal tablolar, yönetim kurulunun yıllık faaliyet raporu, denetleme raporları ve yönetim kurulunun kâr dağıtım önerisi, genel kurulun toplantısından en az onbeş gün önce, şirketin merkez ve şubelerinde, pay sahiplerinin

incelemesine hazır bulundurulur. Bunlardan finansal tablolar ve konsolide tablolar bir yıl süre ile merkezde ve şubelerde pay sahiplerinin bilgi edinmelerine açık tutulur. Her pay sahibi, gideri şirkete ait olmak üzere gelir tablosuyla bilançonun bir suretini isteyebilir. 2) Pay sahibi genel kurulda, yönetim kurulundan, şirketin işleri; denetçilerden denetimin yapılma şekli ve sonuçları hakkında bilgi isteyebilir. Bilgi verme yükümü, 200 üncü madde çerçevesinde şirketin bağlı şirketlerini de kapsar. Verilecek bilgiler, hesap verme ve dürüstlük ilkeleri bakımından özenli ve gerçeğe uygun olmalıdır. Pay sahiplerinden herhangi birine bu sıfatı dolayısıyla genel kurul dışında bir konuda bilgi verilmişse, diğer bir pay sahibinin istemde bulunması üzerine, aynı bilgi, gündemle ilgili olmasa da aynı kapsam ve ayrıntıda verilir. Bu hâlde yönetim kurulu bu maddenin üçüncü fıkrasına dayanamaz.(3) Bilgi verilmesi, sadece, istenilen bilgi verildiği takdirde şirket sırlarının açıklanacağı veya korunması gereken diğer şirket menfaatlerinin tehlikeye girebileceği gerekçesi ile reddedilebilir.(4) Şirketin ticari defterleriyle yazışmalarının, pay sahibinin sorusunu ilgilendiren kısımlarının incelenebilmesi için, genel kurulun açık izni veya yönetim kurulunun bu hususta kararı gerekir. İzin alındığı takdirde inceleme bir uzman aracılığıyla da yapılabilir.(5) Bilgi alma veya inceleme istemleri cevapsız bırakılan, haksız olarak reddedilen, ertelenen ve bu fıkra anlamında bilgi alamayan pay sahibi, reddi izleyen on gün içinde, diğer hâllerde de makul bir süre sonra şirketin merkezinin bulunduğu asliye ticaret mahkemesine başvurabilir. Başvuru basit yargılama usulüne göre incelenir. Mahkeme kararı, bilginin genel kurul dışında verilmesi talimatını ve bunun şeklini de içerebilir. Mahkeme kararı kesindir. (6) Bilgi alma ve inceleme hakkı, esas sözleşmeyle ve şirket organlarından birinin kararıyla kaldırılamaz ve sınırlandırılmaz." denilmektedir.

Yapılan yargılama, davacı tarafın iddiaları, davalının beyanları, tüm dosya kapsamı birlikte değerlendirildiğinde; anonim şirketlerde pay sahiplerinin bilgi alma ve inceleme hakları 3 farklı şekilde düzenlenmiştir. Somut olaya geçmeden önce bu bilgi edinme ve inceleme hakkıyla ilgili genel bir değerlendirme yapmak gerekmektedir. Bu 3 farklı şekildeki düzenleme sırasıyla şu şekildedir:

- 1- Genel kuruldan önce inceleme hakkı,
- 2- Genel kurulda bilgi alma hakkı,
- 3- Genel kuruldan sonra inceleme hakkı,

1- Genel Kuruldan önce inceleme hakkı: TTK'nın 437/1 maddesine göre finansal tablolar, konsolide finansal tablolar, yönetim kurulunun yıllık faaliyet raporu, denetleme raporları ve yönetim kurulunun kar dağıtım önerisi, genel kurulun toplantısında en az 15 gün önce şirketin merkez ve şubelerinde pay sahiplerinin incelemesine hazır bulundurulur. Bunlardan finansal tablolar ve konsolide tabloların 1 yıl süreyle merkezde ve şubelerde pay sahiplerinin bilgi edinmelerine açık

tutulur. Her pay sahibi gideri şirkete ait olmak üzere gelir tablosuyla, bilançonun bir suretini isteyebilir. Hükmü uyarınca genel kuruldan önce bilgi alma ve inceleme hakkı sadece TTK 437/1 maddesinde belirtilen finansal tablolar, yönetim kurulunun yıllık faaliyet raporu, denetlenme raporları ve yönetim kurulunun kar dağıtım önerisi ile sınırlı olarak ve genel kuruldan 15 gün öncesinden itibaren kullanılabilir. Somut olayda davacı bu maddeye dayanmamıştır ki, zaten talep ettiği, bilgi ve inceleme istemleri de bu madde de sayılanlarla alakalı değildir.

2- Genel kurulda bilgi alma hakkı: Yasal düzenleme dikkate alındığında yönetim kurulu üyesi dışındaki ortakların bilgi alma ve inceleme hakkı hem zaman olarak hem de nitelik olarak sınırlandırılmış durumdadır. Genel olarak bilgi alma hakkı ana kural uyarınca genel kurulda kullanılmaktadır. Her pay sahibi genel kurulda şirket işleyişi bakımından yönetim kurulundan ve denetim kurulundan bilgi verilme ve inceleme hakkı talebinde bulunabilecektir. Genel kurulda bilgi ve inceleme hakkı talebinde bulunan ortağın bilgi alma ve inceleme talebi genel kurul tarafından reddedilebileceği gibi kabul de edilebilecektir. Bilgi alma ve inceleme istemi genel kurul tarafından kabul edildiğinde, söz konusu bilgi hakkı ve inceleme hakkı genel kurulda kullanılabilir gibi genel kurul dışında da bilgi alma ve inceleme hakkının kullanılması öngörülebilir. Genel kurul dışında bilgi ve inceleme hakkının kullanılabilmesi için (genel kurulda bilgi verilmesi kabul edilmiş ise) bu konuda genel kurulda bir karar alınmış olması ya da istenen bilginin daha öncesinde genel kurul dışında başka bir pay sahibine kullanılmış olması gerekmektedir. Genel kurulda bilgi edinme hakkı ve inceleme hakkı yönündeki talepleri reddedilen veya cevapsız bırakılan kişiler reddi izleyen tarihten itibaren 10 gün içinde diğer hallerde ise makul bir süre sonra şirketin merkezinin bulunduğu Asliye Ticaret Mahkemesine başvurabilir. Başvuru basit yargılama usulüne göre incelenir. Mahkeme bilginin genel kurul dışında verilmesi talimatını ve bunun şeklini de içerebilir. Davacının istemi genel kurulda kullanılan bilgi edinme veya inceleme hakkının cevapsız bırakılması, reddi, ertelenmesi ya da kendisinin genel kurulda bilgi alamadığı iddiasına da yönelik değildir. Nitekim önceki genel kurulda davacı mahkememize açtığı davada bilgi ve inceleme hakkı talep ettiği hususlarla ilgili olarak genel kurulda herhangi bir talepte bulunmuş da değildir. Bu bağlamda somut olayda bilgi alma hakkının genel kurulda kullanılmasına yönelik bir istem de mevcut değildir.

3- İnceleme hakkının genel kuruldan sonra kullanılması: Esasen biraz önce de söylenildiği üzere, bilgi alma ve inceleme hakkı genel kural olarak, genel kurulda kullanılabilir. Genel kuruldan sonra bilgi alma ve inceleme hakkının kullanılması sınırlı hallerde mümkündür. Bunlardan bir tanesi, genel kurulda TTK 437. Maddesi uyarınca bilgi alma hakkı ve inceleme hakkı başvurusu yapan ortağın bilgi alma ve inceleme hakkının kabul edilmesi ve fakat bu bilgi alma ve inceleme hakkının genel kuruldan

sonra kullanılması yönünde karar alınmasıdır. İkinci bir yöntem, yine genel kurulda bilgi alma ve inceleme hakkı istemi reddedilen, cevapsız bırakılan, ertelenen pay sahibinin mahkemeye başvurması ve mahkeme tarafından bu davanın kabul edilerek bilgi alma ve inceleme hakkının genel kurul dışında kullanılmasına izin verilmesine ilişkin karardır. Üçüncü bir yöntem ise, TTK 437/4 maddesi uyarınca genel kurulun açık izni veya yönetim kurulunun kararıyla şirketin ticari defterleriyle yazışmalarının pay sahibinin sorusunu ilgilendiren kısımlarının incelenebilmesi için defterlerin incelenme hakkıdır. Bunun için de genel kurulun açık izni veya yönetim kurulunun kararı gerekmektedir. Pay sahiplerinin genel kurul dışında da genel kurulda sorabileceği sorulardan bağımsız olduğu yönetim kurulunda yazılı olarak bilgi talep edebilmeleri Türk Hukukunda tanınan bir hak değildir. Davacı 01/10/2020 ve 12/10/2020 tarihlerinde e-posta yolu ile yapmış olduğu müracaatta, tüm çalışanların 2018, 2019, 2020 Mart aylarına ait maaş bordrolarını ve 2017, 2018, 2019 yıllarına ait olağan genel kurul toplantısı yönünden pay sahibi olanların listesini istemiştir. Davacı tarafın bu talebi davalı yönetim kurulu tarafından davalı şirketin tüm personelinin maaş bordrolarının verilmesinin 6698 sayılı kişisel verilerin korunması kanuna kanuna aykırı olduğu, ayrıca ilgili genel kurul toplantısına katılan tüm pay sahiplerinin hazır bulunanlar listesinin KAP'ta yayımlandığını, belirterek reddetmiştir. Yönetim kurulu tarafından reddedilen bu isteme karşı pay sahibinin genel kurul dışında bilgi alma ve inceleme hakkı yasada sınırlı olarak sayıldığından ve yönetim kurulunun bu red kararına karşın dava açılacağına yönelik yasal bir düzenleme bulunmaması, ayrıca verilen cevabi yazı içeriği dikkate alındığında tüm çalışanların maaş bordrolarının istenmesinin Kişisel Verilerin Korunması Kanununa da aykırılık teşkil etmesi, 2017, 2018, 2019 yıllarına ait genel kurula katılanların kamuyu aydınlatma platformunda yayınlanmış oluşu, davacının bu bilgileri, KAP'dan da elde edebileceği, bu itibarla davacının davasının reddi gerektiği görülmüş, bu nedenle davacının davasının istediği bilgileri ve inceleme hakkını genel kurul dışında kullanılması mümkün görülmediğinden usulden reddine karar vermek gerekmiştir.

HÜKÜM: Yukarıda açıklanan nedenler ve dosya içeriğine göre;

- 1- Davacının davasının usulden REDDİNE,
- 2- Harçlar tarifesi gereğince alınması gereken 59,30TL karar harcından peşin olarak alınan 54,40TLnin mahsubu ile bakiye 4,90TLnin davacıdan alınarak Hazine'ye irat kaydına,
- 3- Karar tarihinde yürürlükte bulunan A.A.Ü.T gereğince; 4.080,00TL ücreti vekaletin davacıdan alınarak kendini vekil ile temsil ettiren davalıya verilmesine,
- 4- Davacı tarafından yapılan giderlerin üzerinde bırakılmasına,

5- Davalı tarafından yapılan yargılama gideri bulunmadığından bu konuda karar verilmesine yer olmadığına,

6- Taraflarca yatırılan ve kullanılmayan gider avansının talep halinde ve karar kesinleştiğinde yatıran davacıya İADESİNE,

Dair, davacı asil ve davalı vekilinin yüzüne karşı, kararın tebliğinden itibaren 2 Hafta süre içerisinde Bölge Adliye Mahkemesine İSTİNAF yolu açık olmak üzere oy birliğiyle verilen karar açıkça okunup, usulen anlatıldı. 27/01/2021

İstanbul 4. Asliye Ticaret Mahkemesi, E. 2019/279 K. 2019/661, T. 5.7.2019

DAVA: BİLGİ EDİNME VE İNCELEME HAKKI TALEBİ

DAVA TARİHİ: 15/05/2019

Mahkememizde görülmekte olan Tespit davasının yapılan açık yargılaması sonunda,

GEREĞİ DÜŞÜNÜLDÜ:

Davacı vekili mahkememize verdiği dava dilekçesinde özetle; Müvekkillerinin miras bırakanı ...'ın vefatı sonrası murislerinin ... Ltd Şti'ndeki %50 hissesini 16/02/2016 tarihinde miras yoluyla edindiklerini, şirketin %50 hissesinin diğer ortak ...'a ait olduğunu, sağlığında müvekkilleri murisi ... ile diğer ortak ...'ın şirket müdürü olarak seçildiklerini, müdürlerin münferit imzaları ile şirketi idare ettiklerini, müvekkillerinin murisi ...'ın vefatı ile 16/02/2016 tarihinde buyana %50 oranında ortak olan ...'ın tek başına müdür sıfatıyla şirketi idare ederek, genel kurul kararı olmadığı halde şirketin gelirinin büyük bir kısmını keyfi olarak ücret adı altında kendisine mal ettiğini, TTK. Nun 614/1 md. Gereğince limited şirketlerde her ortağın müdürlerden şirketin bütün işleri ve hesapları hakkında bilgi isteyebileceğinin sabit olduğunu, müvekkillerinin buna istinaden ... 19.Noterliğinin ... tarih ... yevmiye ve ... 1.Noterliğinin ... tarih ve ... yevmiye nolu ihtarnameleri ile şirketin, 01.01.2018-31.12.2018 dönemine ait mizan, kurumlar vergi beyannamesi ve tahakkuk fişleri, 2018 yılı içinde verilen tüm geçici vergi beyannameleri ve tahakkuk fişleri, 01.01.2018- 31.12.2018 dönemi içinde şirket müdürünün şirketten aldığı avans ve ücretlerin aylara göre ve Yıllık toplam brüt miktarını gösterir makbuz ve bordrolar, Şirketin tüm banka hesapları ile kredi kartlarının 2015-2016-2017-2018 yılı dökümlerini, Şirketin Temsilciliği ve acenteliğini yaptığı tüm yerli ve yabancı şirketlerin ünvanları ile bu şirketleri temsile yetkili kişilerin isim , telefon , e-posta iletişim bilgilerinin, ve daha önce tüm taleplerine rağmen kendilerine gösterilmeyen 2015- 2016- 2017 -2018 yılları yevmiye, kebir ve envanter defterlerini incelemek istediklerini davalı şirket müdürüne tebliğ ettiklerini, ancak davalı şirket müdürünün yurt içi ve yurt dışında şirket dışı işlerde kullanıldığı duyumunu aldıkları şirketin kredi kartlarının 2015- 2016- 2017 -2018 yılı harcama dökümlerini müvekkillerine vermediğini, kredi kartlarının şirket işleri için mi yoksa başka amaçlar için mi kullanıldığını tespit etmek ve genel kurulda haklarını kullanabilmek için ortakların bunları incelemesi gerektiğini, ayrıca şirketin temsilciliği ve acenteliğini yaptığı yerli ve yabancı şirketlerin ünvanları ile bu şirketleri temsil ve yetkili kişilerin isim , telefon ve diğer iletişim bilgilerini müvekkillerine yazılı olarak tebliğ ettiğini,

şirket müdürünün şirketin defterlerinin inceleme taleplerini kabul ettiğini ancak incelemek için iki defa gidilmesine rağmen defterlerin müvekkillerine gösterilmediğini, bu nedenle müvekkillerinin 27/04/2019 tarihinde yapılan 2018 yılı genel kurulunda kendilerine verilmeyen bilgi ve belgelerin verilmesini talep ederek genel kurulun bu konuda karar vermesini istediğini, ancak şirket müdürünün istenen belgeleri daha önce verdiğini iddia ederek söz konusu bilgi ve belgelerin verilmesini reddettiğini, bu nedenle huzurdaki davayı ikame ettiklerini beyan ederek ,TTK.614/3.madde gereğince davalı şirketin 2015-2016-2017-2018 yılı kredi kartı harcama dökümleri ve davalı şirketin temsilcilik ve acenteliğini yaptığı yerli ve yabancı şirketlerin ünvanları ile bu şirketleri temsile yetkili kişilerin izim, telefon, e-posta iletişim bilgilerinin müvekkillerine verilmesine, davacılara ... Ltd Şti'nin 2015-2016-2017-2018 yıllarına ait yevmiye defterleri, defteri kebir ve envanter defterlerini inceleme yetkisi verilmesine karar verilerek yargılama gideri ve vekalet ücretinin davalıya yükletilmesini talep ve dava etmiştir.

Davacı Vekili Davasında:

Dava Dilekçesini tekrar ederek davanın kabulüne karar verilmesini talep ettiği görülmüştür.

Davalı vekili Davasında:

Davalı vekili mahkememize hitaben verdiği cevap dilekçesinde özetle; davacının iddia ve taleplerinin maddi ve hukuki dayanaktan yoksun olduğunu, müvekkili şirket müdürünün şirket gelirlerini kendisine mal ettiği iddiasının davacının şirket yetkili müdürü hakkında olumsuz algı oluşturmaya yönelik çabalar olduğunu, davacının bu iddialarının ... 8.ATM nin ... sayılı dosyasında yargılama konusu yapıldığını, yine aynı şekilde tarafların oraklığındaki Ltd Şti aleyhine ... 6 ATM nin ... sayılı dosyasında aynı talepli dava açıldığını, bu dosyada her iki şirkete ait ticari defter ve kayıtların bir arada incelendiğini, inceleme sonucu alınan raporda şirket müdürünün gelirlerini kendisine mal ettiğine dair herhangi bir tespit yata değerlendirme yapılmadığını, davacıların bilgi edinme ve inceleme hakkının kullanılmasının engellendiğine ilişkin iddiaların da asılsız olduğunu, müvekkilinin noter ihtarı ile davacıları şirket hesapları hakkında bilgilendirdiğini, ayrıca kişisel verilerin korunması kanunu kapsamında kalan kişisel verilere ilişkin bilgi talepleri dışında kalan bütün bilgi ve belgelerin ve bilgilerin sunulacağına davacılar vekiline bildirildiğini ve bunun üzerine tutulan 30/11/2018 tarihli tutanaktanda anlaşılacağı üzere tavaacıları temsilen SMMM ... ve ...'ın müvekkil şirket merkezine gelerek istenilen bilgi ve belgelerin kendilerine sunulduğunu ve incelemelerin yapıldığını, davacılar tarafından iş bu dava ile inceleme yetkisi istenilen bilgi ve belgelerin davacılar ile haricen paylaşılmasına rağmen dilekçeleri ekinde buna ilişkin bilgileri içerir CD yi mahkemeye sunduklarını, kredi kartı bilgilerinin incelenmesine ilişkin taleplerinde bu kartlara yapılan ödemeler

de şirket kayıtlarında eksiksiz işlendiğini, davacıların temsilcileri tarafından da bu kayıtların iki defa incelendiğine herhangi bir usulsüzlüğün rapor edilmediğini, müvekkili şirketin ilişkide olduğu şirketlere ilişkin bilgilerin verilmesi yönündeki taleplerinin ise davacılar ile paylaşılan şirkete ait mizanlarda açık şekilde görüldüğünü, bütün yılları ilişkin mizanların davacılar ile paylaşıldığını, bu mizanlara bakarak hangi şirketler ile ticari ilişkinin devam edip etmediğinin hatta ticaret hacmini de rahatlıkla görüldüğünü, davacıların bu şirketler ile ilgili yetkili kişilerin isim ve soy isim ve telefon ile e-posta bilgilerinin paylaşılmasına ilişkin taleplerin ise çoğu Avrupa da bulunan bu şirketlerin müvekkil şirket ile aralarındaki ticari ilişki çerçevesinde ve bu ilişkinin yürütülmesine dönük olarak müvekkiline verdiği bilgiler olduğunu bu bilgilerin AB Hukuku gereği gerekse şirketlerin yerel hukukları gereği ve gerekse 6698 sayılı kanunun hükümleri gereği kişisel veri niteliğinde olduğunu müvekkilinin bu verilerin paylaşılması husunda ilgilerden izin de alamadığını ve bu durumu da noter vasıtasıyla davacılar bildirdiğini, davacılarının bu taleplerinin birtakım duyumlar üzerine talep etmeleri ve bunu somutlaştıran hiçbir delil de dosyaya sunmadıklarını beyan ederek maddi ve hukuki dayanaktan yoksun davanın reddine karar verilerek yargılama gideri ve vekalet ücretinin karşı tarafa tamlıne karar verilmesini talep etmiştir.

Toplanan Deliller:

Taraflarca ibraz edilen deliller incelenmiştir.

8.Asliye Ticaret Mahkemesinin ... Esas sayılı dosyasını ile ... 6.Asliye Ticaret Mahkemesinin ... Esas sayılı dosyasının dava dilekçesi ve cevap dilekçesi celp edilip incelenmiştir.

Delillerin Değerlendirilmesi:

Tüm dosya kapsamı dikkate alınarak; Davacı tarafın davası 6102 Sayılı Kanunun 614.md ifadesini bulan "Bilgi alma ve inceleme hakkı" talebine ilişkindir. Davacı tarafın talebinin değerlendirilmesi için 6102 Sayılı Kanunun 614.md incelenmesi gerekmektedir. 6102 Sayılı Kanunun 614.md aynen " MADDE 614- (1) Her ortak, müdürlerden, şirketin bütün işleri ve hesapları hakkında bilgi vermelerini isteyebilir ve belirli konularda inceleme yapabilir. (2) Ortağın, elde ettiği bilgileri şirketin zararına olacak şekilde kullanması tehlikesi varsa, müdürler, bilgi alınmasını ve incelemeyi gerekli ölçüde engelleyebilir; bu konuda ortağın başvurusu üzerine genel kurul karar verir.(3) Genel kurul, bilgi alınmasını ve incelemeyi haksız yere engellerse, ortağın istemi üzerine mahkeme bu hususta karar verir. Mahkeme kararı kesindir. " şeklindedir. Dava konusu somut olayda davacı taraf, davalı taraf adına ihtarname keşide ederek dava konusu talepleri hakkında inceleme kararı talebinde bulunmuştur. Davalı tarafça ibraz edilen 30/11/2018 ve 22/04/2019 tarihli tutanaklarla davalı tarafın ticari kayıtlarının incelemeye sunulduğu, davacı tarafın temsilcileri olan Mali Müşavirler tarafından

herhangi bir itirazi kayıt şerh düşülmeden inceleme tutanağının imzalandığı görülmüş olmakla davalı şirketin 6102 sayılı Kanununun 614.md si uyarınca üzerine düşen yükümlülüğü yerine getirdiği mahkememizce tespit edilmiştir. Davacı taraf ticari kayıtlarla birlikte ... Bankası kredi kartı dökümlerinin celbini talep etmiş ise de; davalı tarafın böyle bir kart bulunmadığını ileri sürdüğü ve taraflar arasında yapılan inceleme sırasında düzenlenen tutanakta şirketin gelir ve gider tablolarının incelemesinde şirket hesaplarına bağlı böyle bir kartın varlığının itirazi kayıt ileri sürülerek tespitinin yapılmadığı görülmüş olmakla davacı tarafın bu yönde ki talebi mahkememizce yerinde görülmemiştir. Kaldı ki; taraflar arasında devam eden ... 8.Asliye Ticaret Mahkemesinin ... Esas sayılı dosyası ile ... 6.Asliye Ticaret Mahkemesinin ... Esas sayılı dosyasında celp edilecek deliller ile yapılan ve yapılacak Bilirkişi incelemelerinde bu husus açıkça davacı tarafça incelenebilecektir. Davacı taraf aynı zamanda davalı şirketin ticari ilişkide bulunduğu yerli ve yabancı şirketin açık kimlik bilgileri ve iletişim bilgilerini talep etmiş ise de; taraflar arasında düzenlenen 30/11/2018 ve 22/04/2019 tarihli tutanaklar ile incelemeye sunulan belgelerde davacı tarafın ticari ilişkide bulunduğu tacirlerin açık bilgilerinin tespit edilebileceği anlaşılacakla birlikte davalı taraf istenen diğer diğer bilgilerin kişisel veri niteliğinde olacağı bu hali ile cezai ve hukuki sorumluluğu gerektireceği iddiası karşısında davalı tarafın gerekçesi 6698 sayılı kanunun açıklığı karşısında mahkememizce yerinde görüldüğünden davacı tarafın talebinin reddine karar verilmiştir.

HÜKÜM; Yukarıda açıklanan nedenlerle;

- 1-) Davacı tarafın davasının REDDİNE;
- 2-) Peşin alınan harç Karar ve İlam harcını karşıladığından harç alınmasına yer olmadığına,
- 3-) Davacı tarafından yapılan yargılama giderlerinin davacı taraf üzerinde bırakılmasına,
- 4-) Davalı vekili lehine 2.725.TL. vekalet ücretinin davacılar tarafından müştereken ve müteselsilen tahsili ile davalı tarafa verilmesine,
- 5-) Davacı tarafından yatırılan ve artan gider avansının karar kesinleştiğinde bakiye kısmının yatıran tarafa iadesine,

6102 sayılı Kanununun 614.md uyarınca KESİN olmak üzere oy birliği ile dosya üzerinde inceleme neticesinde karar verildi. 05/07/2019

KAMU İHALE KURULU KARARLARI

Bölüm İçeriđi

- Kamu İhale Kurulu KİK (K. 2021/UH.II-111)
- Kamu İhale Kurulu KİK (K. 2020/UY.I-470)
- Kamu İhale Kurulu KİK (K. 2018/UH.II-1130)
- Kamu İhale Kurulu KİK (K. 2016/UH.II-1732)

Kamu İhale Kurulu Kararı - KİK (K. 2021/UH.II-111)

Kamu İhale Kurulu Kararı - KİK, K. 2021/UH.II-111 T. 13.01.2021

BAŞVURU SAHİBİ: Ventura Yazılım Anonim Şirketi,

İHALEYİ YAPAN İDARE: T.C. Sağlık Bakanlığı S.B.Ü. Ankara Eğitim Ve Araştırma Hastanesi Başhekimliği,

BAŞVURUYA KONU İHALE: 2020/405858 İhale Kayıt Numaralı "36 Aylık Sağlık Bilgi Yönetim Sistemleri (Sbys - Hbys) Hizmet Alımı" İhalesi

KURUM TARAFINDAN YAPILAN İNCELEME:

T.C. Sağlık Bakanlığı S.B.Ü. Ankara Eğitim ve Araştırma Hastanesi Başhekimliği tarafından 10.09.2020 tarihinde açık ihale usulü ile gerçekleştirilen "36 Aylık Sağlık Bilgi Yönetim Sistemleri (Sbys - Hbys) Hizmet Alımı" ihalesine ilişkin olarak Ventura Yazılım A.Ş.nin 25.11.2020 tarihinde yaptığı şikâyet başvurusunun, idarenin 03.12.2020 tarihli yazısı ile reddi üzerine, başvuru sahibince 14.12.2020 tarih ve 56398 sayılı Kurum kayıtlarına alınan 14.12.2020 tarihli dilekçe ile itirazın şikâyet başvurusunda bulunulmuştur.

Başvuruya ilişkin olarak 2020/2010 sayılı itirazın şikâyet dosyası kapsamında yapılan inceleme neticesinde esas inceleme raporu tanzim edilmiştir.

KARAR:

Esas inceleme raporu ve ekleri incelendi.

İtirazın şikâyet dilekçesinde özetle, ihale üzerinde bırakılan isteklinin teklif ettiği sisteme ilişkin olarak Teknik Şartname'nin 4'üncü maddesi uyarınca demonstrasyon yapılmadığı, özellikle demirbaş ve varlık yönetim sistemi, görüntü arşivleme ve iletişim sistemi, ihtiyaç yönetim bilgi sistemi, klinik mühendislik bilgi yönetim sistemi için demonstrasyon yapılmadığı,

Teknik Şartname'nin 4.13.2'nci maddesinde isteklilerden 15 takvim günü içerisinde idarenin belirlediği mekanda tüm veriyi eksiksiz olarak aktarmalarının istenileceğinin belirtildiği, bu madde uyarınca idarenin veri aktarımı için tek bir mekan belirleyebileceği, bunun da hayatın olağan akışı gereği Ankara Eğitim ve Araştırma Hastanesi binalarından biri olduğu, oysaki idare tarafından verilerin ihale üzerinde bırakılan istekliye harici disk ile teslim edildiği, ihale üzerinde bırakılan

isteklinin de bu veriyi kendi adresinde aktardığı, şikâyet konusu ihaleye halihazırda teklif verebilecek 57 firma varken 3 isteklinin ihaleye katıldığı, bu durumun Teknik Şartname düzenlemeleri uyarınca verilerin 15 gün boyunca hastane ortamında gerçekleştirilecek olmasından kaynaklandığı, şöyle ki 15 gün boyunca veri aktarımı yapacak personelin ciddi bir personel gideri oluşturduğu, verilerin hastane ortamında değil de isteklilerin kendi adreslerinde aktarılacağı bilinmesi durumunda ihaleye daha çok isteklinin katılmasının mümkün olduğu,

Panates Bilişim ve Teknoloji San. Tic. Ltd. Şti.nin de demonstrasyon işlemlerine katılmamasının sebebinin verilerin aktarımının hastane ortamında yapılacak olması olduğu,

Bununla birlikte şikâyete konu ihaleye ilişkin olarak düzeltici işlem kararı değil ihalenin iptali kararı verilmesi gerektiği, zira ihale üzerinde bırakılan istekli tarafından veri aktarımının ofis ortamında yapıldığı, dolayısıyla halihazırda işi yürüten grup firmaları olan Bilfo Bilgisayar ve Bilişim Sistemleri Ltd. Şti.nin tüm veri tabanı altyapılarının rakip firmanın eline geçtiği, bu usulsüzlüğün düzeltici işlem kararı ile giderilmesinin mümkün olmadığı,

İdare tarafından ihale üzerinde bırakılan istekliye 6698 sayılı Kişisel Verileri Koruma Kanunu'na aykırı olarak hastaların kişisel verilerinin ve sağlık verilerinin teslim edildiği, Kişisel Sağlık Verileri Hakkında Yönetmelik'in 15'inci maddesinin 3'üncü fıkrasında "Kişisel sağlık verilerinin aktarımı talepleri, talep edilen sağlık verilerinin ilgili olduğu Bakanlık birimi tarafından Kanun ve ilgili diğer mevzuat açısından değerlendirilir, değerlendirme sonucuna göre Genel Müdürlükçe işlem tesis edilir" düzenlemesinin yer aldığı, bu hüküm uyarınca idare tarafından ihale üzerinde bırakılan istekliye veriler teslim edilmeden önce sağlık bakanlığından izin alınması gerektiği, ancak idare tarafından böyle bir izin alınmadığı iddialarına yer verilmiştir.

Başvuru sahibinin iddialarının değerlendirilmesi sonucunda aşağıdaki hususlar tespit edilmiştir.

4734 sayılı Kamu İhale Kanunu'nun "Şartnameler" başlıklı 12'nci maddesinde "İhale konusu mal veya hizmet alımları ile yapım işlerinin her türlü özelliğini belirten idari ve teknik şartnamelerin idarelerce hazırlanması esastır. Ancak, mal veya hizmet alımları ile yapım işlerinin özelliği nedeniyle idarelerce hazırlanmasının mümkün olmadığı ihale yetkilisi tarafından onaylanması kaydıyla, teknik şartnameler bu Kanun hükümlerine göre hazırlanabilir.

İhale konusu mal veya hizmet alımları ile yapım işlerinin teknik kriterlerine ihale dokümanının bir parçası olan teknik şartnamelerde yer verilir. Belirlenecek teknik kriterler, verimliliği ve fonksiyonelliği sağlamaya yönelik olacak, rekabeti engelleyici hususlar içermeyecek ve bütün istekliler için fırsat eşitliği sağlayacaktır.

Teknik şartnamelerde, varsa ulusal ve/veya uluslararası teknik standartlara uygunluğu sağlamaya yönelik düzenlemeler de yapılır. Bu şartnamelerde teknik özelliklere ve tanımlamalara yer verilir. Belli bir marka, model, patent, menşei, kaynak veya ürün belirtilemez ve belirli bir marka veya modele yönelik özellik ve tanımlamalara yer verilmeyecektir..." hükmü yer almaktadır.

İdari Şartname'nin "İhale konusu işe ilişkin bilgiler" başlıklı 2'nci maddesinde "2.1. İhale konusu hizmetin;

a) Adı: 36 AYLIK SAĞLIK BİLGİ YÖNETİM SİSTEMLERİ (SBYS - HBYS) HİZMET ALIMI

b) Miktarı ve türü:

36 AYLIK SAĞLIK BİLGİ YÖNETİM SİSTEMLERİ (SBYS - HBYS) HİZMET ALIMI

Ayrıntılı bilgi idari şartnamenin ekinde yer almaktadır.

c) Yapılacağı yer: T.C. Sağlık Bakanlığı S.B.Ü Ankara Eğitim ve Araştırma Hastanesi

ç) Bu bent boş bırakılmıştır." düzenlemesi,

Aynı Şartname'nin "İhaleye katılabilmek için gereken belgeler ve yeterlik kriterleri" başlıklı 7'nci maddesinde "...7.5.4 İsteklinin teklifi kapsamında sunması gerektiği teknik şartnamede belirtilen belgeler..." düzenlemesi yer almaktadır.

Teknik Şartname'nin "Demonstrasyon ve içeriği" başlıklı 4'üncü maddesinde "4.1. hastanemizde hizmetin kesintiye uğramadan devam etmesi esasına dayanılarak bu hizmet kapsamında alınacak olan sistemin ve hizmetlerin Teknik Şartnameye uygunluğunun teyit edilebilmesi için uygulamalı demo yapılacaktır. İstekliler, demo için herhangi bir ücret talep edemezler. Demo için gerekli olan tüm donanım ve sarf ücretleri isteklilerce karşılanacaktır...

4.2. Demonstrasyon işlemleri (demo) idare tarafından belirlenecek işin idari ve teknik boyutta değerlendirilmesini sağlayacak personel tarafından yapılacaktır.

4.3. Demo, İdarenin sağlayacağı bir mekanda yapılacaktır. İsteklilerin demoya davet yazısında belirtilmiş olan tarih ve saatte demo yapmaları gerekmektedir...

...

4.6. Yapılacak olan demo sonucunda ihale komisyonu üyeleri ve firma yetkilisi/yetkilileri tarafından imzalanmış demo raporunun tutulması ve ihale dosyasında saklanması gerekmektedir...

4.7. İsteklinin yapacağı yeterlilik demosu sonunda ihale komisyonundan yeterlilik alması zorunludur. Demo, ihale komisyonunca yapılan belge değerlendirmesi teklifi geçerli sayılan en

düşük/avantajlı teklifi veren firmadan başlanacak şekilde yapılacaktır. Demo sonucuna göre yeterli görülen 1. ve 2. En avantajlı olarak belirlenen istekliler tespit edildiğinde diğer isteklilerden demo yapmaları istenmeyebilecektir.

4.11 Demo sırasında kullanılacak sette, kişilere ait gerçek vatandaşlık numarası veya gerçek vatandaşlık numarasına erişimi mümkün kılan gerçek veri hükümleri yer almayacak, ancak aynı karakter dizinine sahip verilerle sanallaştırılmış kişiler üzerinden hazırlanan veriler yer alacaktır. Bildirilen/tebliğ edilen tarihte istekli demo için kurumumuzda hazır bulunacaktır. Demo saatinden önce istekli firmanın hazırlıklarını tamamlaması için demo yapılacak yer teslim edilecek ve demo için kurumumuzun imkanları ölçüsünde yardımcı olunacaktır. İstekli firma demo saatinden 1 saat önce hazırlıklarını tamamlamış olacaktır.

4.12. Demonstrasyon sürecinde aşağıdaki sırayla gidilecektir. Herhangi bir aşamayı geçemeyen istekliler için bir sonraki aşama uygulanmayacak ve istekliler teknik olarak yetersiz kabul edilecektir...

...

4.13. Birinci aşama -veri aktarım yeteneği

4.13.1 Genel müdürlük tarafından verilen Veri modeli oluşturma ve veri aktarımı ile yeterlik belgesi" sahibi olan istekliler ihale sürecinde veri aktarımı ve teslimiyle ilgili demonstrasyonun bu bölümünden başarıyla geçmiş sayılacak ve bu yazılımlar için kendilerinden veri aktarım demonstrasyonu istenmeyecektir.

4.13.2. "Veri modeli oluşturma ve veri aktarımı yeterlik belgesi" olmayan isteklilere en az 2019 yılına ait tüm tablolar, VEM görüntüleri ve referans kodlar teslim edilecek ve isteklilerin 15 (on beş) takvim günü içerisinde idarenin belirlediği mekanda tüm veriyi eksiksiz olarak aktarması istenecektir.

4.14. İkinci aşama -programın genel işleyişi ve ihtiyacı karşılama yeteneği

Teknik şartname ve ekinde bulunan sistemler komisyon tarafından detaylı olarak incelenecek ve herhangi bir şartname maddesini yerine getirmeyen istekliler yetersiz olarak kabul edilecek ve ihale dışı bırakılacaktır.

4.15 Üçüncü aşama -log tutma ve analizi

Bu klavuzun "Loglama ve Performans" başlığı altında bulunan loglama işlemleri bölümünde tanımlanan logların tutulup tutulmadığı, 01.03.2018 tarihinden sonra genel müdürlük tarafından yayımlanan samilog dokümanı temel alınarak, kontrol edilecektir.

4.16. Demo süresii her bir istekli için bildirim süreleri hariç olmak üzere en fazla 5 (beş) iş gününü aşmayacaktır. Demo planı kurum tarafından isteklilere Demo daveti ile birlikte gönderilecektir. Demo için davetler EKAP üzerinden yapılacaktır.” düzenlemesi yer almaktadır.

Yukarıda aktarılan Teknik Şartname düzenlemelerinden demonstrasyon sırasında kullanılacak sette kişilere ait gerçek vatandaşlık numarası veya gerçek vatandaşlık numarasına erişimi mümkün kılan gerçek veri kümelerinin yer almayacağı, demonstrasyon işlemlerinin üç aşamadan oluştuğu, birinci aşamanın veri aktarım yeteneği aşaması olduğu bu kapsamda “Veri modeli oluşturma ve veri aktarımı yeterlik belgesi” olmayan isteklilere en az 2019 yılına ait tüm tablolar, VEM görüntüleri ve referans kodların teslim edileceği ve isteklilerden 15 (on beş) takvim günü içerisinde idarenin belirlediği mekanda tüm veriyi eksiksiz olarak aktarmalarının isteneceği, ikinci aşamanın programın genel işleyişi ve ihtiyacı karşılama yeteneği aşaması olduğu, bu aşamada Teknik Şartname ve ekinde bulunan tüm sistemlerin komisyon tarafından detaylı olarak inceleneceği, demonstrasyonun üçüncü aşamasının ise Log tutma ve analiz aşaması olduğu, ayrıca demonstrasyon süresinin her bir istekli için bildirim süreleri hariç olmak üzere en fazla 5 iş günü olduğu anlaşılmıştır.

Şikâyete konu ihalenin Ankara Eğitim ve Araştırma Hastanesine ait “36 Aylık Sağlık Bilgi Yönetim Sistemleri (Sbys - Hbys) Hizmet Alımı” ihalesi olduğu, 10.09.2020 tarihinde gerçekleştirilen şikâyete konu ihaleye 3 isteklinin katıldığı, 24.11.2020 tarihli ihale komisyonu kararı ile ihalenin Akgün Bilgisayar Program ve Hizmetleri San. Tic. A.Ş. bırakıldığı, ekonomik açıdan en avantajlı ikinci teklif sahibi belirlenmediği anlaşılmıştır.

İhale işlem dosyası üzerinden gerçekleştirilen incelemede;

İhale komisyonu üyeleri tarafından düzenlenen 23.09.2020 tarihli tutanakta

“1- isteklilerin dosyaları incelenmiş olup herhangi bir bilgi ve belge eksikliğine rastlanmamıştır.

2- Sözleşmesi devam eden Bilfo Bilişim A.Ş. yüklenicisinden 1 aylık VEM DATA bilgilerinin kontrol teşkilatı tarafından istenmesine karar verilmiştir.

3- VEM Data bilgilerinin gelmesinden sonra ihaleye teklif veren 1. ve 2. Fiyat avantajlı isteklilerin DEMO için her firmaya 5 iş günü süreyle DEMO yapılmasına karar verilmiştir.” ifadelerine yer verildiği,

Daha sonra 07.10.2020 ve 12.10.2020 tarihlerinde EKAP üzerinden sırasıyla Panates Bilişim ve Teknoloji San. Tic. Ltd. Şti. ve Akgün Bilgisayar Program ve Hizmetleri San. Tic. A.Ş. ye gönderilen “Demonstrasyon yapılması” konulu yazılar ile anılan isteklilerin Teknik Şartname’nin 4’üncü maddesinde istinaden demonstrasyon yapmak üzere belirtilen tarihler arasında hastane seminer

salonunda hazır bulunmaları gerektiğinin ifade edildiği ve söz konusu yazı ekinde demonstrasyon sürecine ilişkin programa yer verildiği,

Panates Bilişim ve Teknoloji San. Tic. Ltd. Şti. tarafından idareye gönderilen 05.10.2020 tarihli yazıda mevcutta farklı bir kurulum aşamasında olduklarından demo ve diğer ihale süreçlerine katılamayacaklarının ifade edildiği,

İdare tarafından Akgün Bilgisayar Program ve Hizmetleri San. Tic. A.Ş.ye 02.11.2020 tarihinde EKAP üzerinden gönderilen yazı ile Teknik Şartname'nin 4.13.2'nci maddesi uyarınca hasta ve personele ait verilerin taraflarına teslim edildiğinin ifade edildiği,

16.11.2020 tarihli SBYS veri aktarım komisyon tutanağında "2020/405858 ihale sayı numarası ile ihalesi yapılan SBYS (sağlık bilgi yönetim sistemi) sistemine ait maskelenmiş veriler ile veri aktarım kontrolü yapılmıştır. Yapılan kontrollerde 2019 yılına ait hastalar rastgele seçilmiş olup demo isteklisi AKGÜN YAZILIM firmasına bu hastalar ile ilgili veriler sorulmuştur. İlgili istekli firmaya teslim edilen verilerin uygun şekilde aktarıldığı tarafımızca tespit edilmiştir. Bu sonuca göre firma veri aktarımında başarılı kabul edilmiş ve SBYS yazılım demosuna geçmeye hak kazanmıştır." ifadelerine yer verildiği ve ilgili tutanağın ihale komisyonu üyeleri tarafından imzalandığı,

23.11.2020 tarihli HBYS Demo komisyon raporu tutanağında "2020/405858 sayılı ihale kapsamında 2. Avantajlı firma olan Akgün bilgisayar usulüne uygun olarak demo için davet edilmiştir.

Şartname maddeleri gereği;

1.Aşama: Veri aktarım yeteneği değerlendirilmiş ve uygun bulunmuştur.

2.Aşama: Teknik Şartname ekinde bulunan tüm sistemlerin yazılım modülleri incelenmiş ve uygun bulunmuştur.

3.Aşama Log tutma ve samilog dokümanı kontrol edilmiş ve uygun bulunmuştur."

İfadelerine yer verilerek ihale komisyonu üyeleri ve Akgün Bilgisayar Program ve Hizmetleri San. Tic. A.Ş. tarafından imzalandığı, 24.11.2020 tarihli ihale komisyonu kararı ile ihalenin Akgün Bilgisayar Program ve Hizmetleri San. Tic. A.Ş. üzerinde bırakıldığı anlaşılmıştır.

Başvuru sahibi isteklinin, ihale üzerinde bırakılan isteklinin teklif ettiği sistemlere ilişkin olarak Teknik Şartname'nin 4'üncü maddesi uyarınca demonstrasyon yapılmadığı, özellikle demirbaş ve varlık yönetim sistemi, görüntü arşivleme ve iletişim sistemi, ihtiyaç yönetim bilgi sistemi, klinik mühendislik bilgi yönetim sistemi için demonstrasyon yapılmadığı, veri aktarımının hastane ortamında yapılması gerekirken verilerin ihale üzerinde bırakılan istekliye harici disk ile verildiği ve

veri aktarımının anılan isteklinin kendi adresinde yapıldığı, halihazırda ihale konusu alanda faaliyet gösteren 54 firmanın şikâyet konusu ihaleye katılmamasının keza Panates Bilişim ve Teknoloji San. Tic. Ltd. Şti.nin de demonstrasyon işlemlerine katılmamasının sebebinin verilerin aktarımının hastane ortamında yapılacak olması olduğu iddiasına ilişkin olarak;

Teknik Şartname düzenlemeleri incelendiğinde veri aktarımının idarenin belirlediği bir mekanda yapılacağı belirtilmiştir ve bu sürenin de en fazla 15 gün olarak belirlendiği, aynı Şartname'nin 4.16'ncı maddesinde de bu sürenin en fazla 5 iş günü olarak düzenlendiği, ihale üzerinde bırakılan istekliye gönderilen 12.10.2020 tarihli yazıda demonstrasyon işlemlerini yapmak üzere belirtilen tarihlerde hastane seminer salonunda bulunmasının istenildiği, 16.11.2020 tarihli SBYS Veri Aktarım Komisyon Tutanağında ise veri aktarımının nerede yapıldığına ilişkin bir ifade bulunmadığı, ancak Teknik Şartname'nin 4.13.2'nci maddesinde belirtildiği üzere veri aktarımının idarenin belirleyeceği bir mekanda yapılacağı, bu konudaki takdir yetkisinin ve sorumluluğun idarede olduğu, 16.11.2020 tarihli SBYS Veri Aktarım Komisyon Tutanağından da anlaşılacağı üzere anılan firma tarafından yapılan veri aktarımının başarılı kabul edildiği ve SBYS yazılım demosuna geçmeye hak kazandığı, öte yandan 23.11.2020 tarihli HBYS Demo komisyon raporu ve demonstrasyon planı bir arada değerlendirildiğinde demonstrasyonunun ikinci aşamasında demonstrasyon planında belirtilen tüm sistemler için demonstrasyon yapıldığı, öte yandan Panates Bilişim ve Teknoloji San. Tic. Ltd. Şti. tarafından idareye gönderilen 05.10.2020 tarihli yazıda mevcutta farklı bir kurulum aşamasında olduklarından demonstrasyon ve diğer ihale süreçlerine katılmayacaklarının ifade edildiği, yine ihale konusu alanda faaliyet gösteren isteklilerin şikâyet konusu ihaleye katılmama nedenlerinin mevcut doküman düzenlemelerinden kaynaklandığına ilişkin bir değerlendirme yapılmasının mümkün olmadığı anlaşılmış olup başvuru sahibinin iddiaları yerinde görülmemiştir.

Başvuru sahibi isteklinin, şikâyete konu ihaleye ilişkin olarak düzeltici işlem kararı değil ihalenin iptali kararı verilmesi gerektiği, zira ihale üzerinde bırakılan istekli tarafından veri aktarımının ofis ortamında yapıldığı, dolayısıyla halihazırda işi yürüten kendi grup firmaları olan Bilfo Bilgisayar ve Bilişim Sistemleri Ltd. Şti.nin tüm veri tabanı altyapı formatlarının rakip firmanın eline geçtiği, bu usulsüzlüğün düzeltici işlem kararı ile giderilmesinin mümkün olmadığı, idare tarafından Kişisel Verileri Koruma Kanununa aykırı olarak hastaların kişisel verilerinin ve sağlık verilerinin ihale üzerinde bırakılan istekliye teslim edildiği yönündeki iddialara ilişkin olarak;

Yukarıdan aktarılan doküman düzenlemeleri uyarınca yapılan incelemede, halihazırda işi yürüten firmadan ihale üzerinde bırakılan isteklinin demonstrasyon işlemlerinin gerçekleştirilmesini teminen Vem Data bilgilerinin istenildiği, bunun işin doğası gereği olduğu, anılan Vem Data bilgilerinin ihale

üzerinde bırakılan istekliye verilmesin halihazırda işi yürüten firmanın veri tabanı alt yapı formatlarının ihale üzerinde bırakılan istekliye teslim edildiği şeklinde yorumlanamayacağı, ihale işlem dosyasında yer alan bilgi ve belgelerden buna ilişkin bir tespit de yapılamayacağı, kaldı ki esas itibari ile ticari bir sır olduğu iddia edilen bu veri tabanı altyapı formatlarının başka birine teslim edilemeyeceği yönündeki iddiaların ihale sürecine ilişkin olmadığı, dolayısıyla Kurumun görev alanında bulunmadığı bu yöndeki iddiaların bağımsız mahkemelerde dava konusu edilebileceği, yine aynı şekilde hastaların ve personelin kişisel verilerinin Kişisel Verileri Koruma Kanunu'na aykırı bir şekilde ihale üzerinde bırakılan istekliye teslim edildiği yönündeki iddiasının da ihale sürecine ilişkin olmadığı, dolayısıyla Kurumun görev alanında bulunmadığı anlaşılmış olup başvuru sahibinin iddiaları yerinde görülmemiştir.

Açıklanan nedenlerle, 4734 sayılı Kanun'un 65'inci maddesi uyarınca bu kararın tebliğ edildiği veya tebliğ edilmiş sayıldığı tarihi izleyen 30 gün içerisinde Ankara İdare Mahkemelerinde dava yolu açık olmak üzere,

Anılan Kanun'un 54'üncü maddesinin onbirinci fıkrasının (c) bendi gereğince itirazın şikâyet başvurusunun reddine,

Oybirliği ile karar verildi.

Kamu İhale Kurulu Kararı - KİK (K. 2020/UY.I-470)

Kamu İhale Kurulu Kararı - KİK, K. 2020/UY.I-470 T. 04.03.2020

BAŞVURU SAHİBİ: Raymak Yapı A.Ş.,

İHALEYİ YAPAN İDARE: Sağlık Bakanlığı Sağlık Yatırımları Genel Müdürlüğü,

BAŞVURUYA KONU İHALE: 2019/408602 İhale Kayıt Numaralı “Muğla Marmaris 125 Yataklı Devlet Hastanesi Yapım İşi” İhalesi

KURUM TARAFINDAN YAPILAN İNCELEME:

Sağlık Bakanlığı Sağlık Yatırımları Genel Müdürlüğü tarafından 11.11.2019 tarihinde açık ihale usulü ile gerçekleştirilen “Muğla Marmaris 125 Yataklı Devlet Hastanesi Yapım İşi” ihalesine ilişkin olarak Raymak Yapı A.Ş.nin 12.02.2020 tarihinde yaptığı şikâyet başvurusunun, idarenin 14.02.2020 tarihli yazısı ile reddi üzerine, başvuru sahibince 26.02.2020 tarih ve 10331 sayı ile Kurum kayıtlarına alınan 26.02.2020 tarihli dilekçe ile itirazın şikâyet başvurusunda bulunulmuştur.

Başvuruya ilişkin olarak 2020/392 sayılı itirazın şikâyet dosyası kapsamında yapılan inceleme neticesinde esas inceleme raporu tanzim edilmiştir.

KARAR:

Esas inceleme raporu ve ekleri incelendi.

İtirazın şikâyet dilekçesinde özetle, başvuruya konu elektronik ihaleye teklif verildiği, ancak 30.01.2020 tarihli ihale komisyonu kararına göre; yeterlik bilgileri tablosunda şirket ortakları ile yetkililerinin T.C. kimlik numaraları belirtilmiş olmakla birlikte, söz konusu bilgilerin teyidinin yapılabileceği belge olarak beyan edilen Ticaret Sicili Gazetelerinde şirket ortaklarına ait T.C. kimlik bilgisi bulunmadığından ve ayrıca yeterlik belgeleri tablosunun “Diğer belgeler kullanılarak tevsik ediliyorsa bu belgelerin tarih ve sayısı ile düzenleyen gerçek/tüzel kişi” bölümünün doldurulmadığından tekliflerinin değerlendirme dışı bırakıldığı, tekliflerinin değerlendirmeye alınmasına yönelik idareye yaptıkları şikâyet başvurularının ise reddedildiği,

Aşağıda belirtilen iddialar kapsamında tekliflerinin değerlendirme dışı bırakılmaması gerektiği,

Yeterlik bilgileri tablosunda beyan edilen bilgi ve belgeler dışında bu tabloya haricen bir belgenin bilgisayardan taratılarak yüklenmesinin teknik olarak mümkün olmadığı, EKAP sistemine kayıt

olunabilmesi için şirkete ait her türlü yeterlik bilgisi ve belgelerinin kaydedilmesinin zorunlu olduğu, şirketlerinin de EKAP kaydının bulunduğu, ihaleye e-teklif verebildikleri ve bu teklifin sistem tarafından kabul edildiği göz önünde bulundurulduğunda EKAP üzerinde şirketlerine ait bilgi ve belge eksikliğinin olmadığı, ayrıca beyan edilen yeterlik bilgileri tablosunda şirket ortaklarından Ahmet Adnan Karacan ve Tahsin Gürboğa'nın şirketteki hisse oranları ile T.C. kimlik numaralarının açıkça beyan edilmiş olduğu, bununla birlikte yine yeterlik bilgileri tablosunda beyan edilen ve EKAP üzerinden sorgulanabilen iş deneyim belgesinden de şirketin %51 hisse sahibi ortağı olan Ahmet Adnan Karacan'ın kimlik numarasının bahse konu belgeden de görülebileceği, diğer taraftan şirketlerine ait yeterlik bilgileri EKAP üzerinden görülebileceğinden Ticaret Sicili Gazetesinde tam olarak yer almayan kimlik numaralarının EKAP sistemindeki diğer belgelerden ya da beyanlarından sorgulanıp teyit edilmesinin mümkün olduğu,

Ticaret Sicili Gazetelerinde bazı kimlik numaralarının açıkça yazıldığı, bazılarının kısmen yazıldığı, bazılarının ise hiç yazılmadığı, bu durumun belirlenmesine ilişkin kendilerinin müdahale imkanlarının olmadığı, nitekim bu durumla ilgili Ankara Ticaret Odası Ticaret Sicil Müdürlüğüne başvurdukları, ilgili Müdürlükçe verilen cevap yazısında T.C. kimlik numaralarının Ticaret Sicili Gazetelerinde yayınlanmamasının 6698 sayılı Kişisel Verilerin Korunması Kanunu ile 6102 sayılı Türk Ticaret Kanunu'na dayandığının ifade edildiği, ayrıca Ticaret Sicil Yönetmeliği'nin 15.3'üncü maddesinde "Elektronik ortamda yapılacak olan incelemelerde de kişisel verilerin korunmasını ve bilgi güvenliğini sağlayacak tedbirler alınır." hükmü ile aynı Yönetmelik'in 41.2'nci maddesinde "Bu Yönetmelik uyarınca tescil edilen gerçek kişilerin kimlik numaraları ilan edilmez." hükümlerinin de bulunduğu, şirket ortaklarının T.C. kimlik numaralarının Ticaret Sicili Gazetelerinde bulunma zorunluluğunun olmadığından ihaleye iştirak eden istekli firmaların bu durumdan sorumlu tutulmasının söz konusu olmayacağı,

İdarenin şikâyete verdiği cevap yazısında belirttiği üzere yeterlik bilgileri tablosunu tevsik edici belge olarak haricen belge (örneğin nüfus cüzdanı) taranarak sisteme eklenmesinin mümkün olmadığı, nüfus cüzdanı, pay defteri, karar defteri gibi belgeler ihale komisyonu tarafından EKAP sisteminde görülemeyeceğinden fiilen teyit edilmesi imkanının bulunmadığı, kaldı ki, teklifin asli unsurlarından birisi olan imza sirkülerine ait bilgilerin yeterlik bilgileri tablosunda beyan şeklinde yer aldığı için ihale komisyonunca fiilen teyit edilemediği halde yeterli sayılmasına rağmen, şirket ortakları ile temsilcisine ait T.C. kimlik numaraları EKAP bilgilerinde yer aldığı halde teyit edilemediği gerekçesiyle değerlendirme dışı bırakılmalarının elektronik ihale usulünün beyana ilişkin mantığına

uygun düşmediği, yeterlik bilgileri tablosunda yer alan her belgenin ihale komisyonu tarafından önceden fiilen teyit edilebiliyormuş gibi davranılmasının doğru olmadığı,

İdarenin vermiş olduğu şikâyete cevap yazısında yukarıda belirtilen iddiaların kabul edilmediği, ayrıca cevap yazısında idarelerin ihaleye katılan isteklilerin ortakları, ortaklık oranları ve yönetimindeki görevlilere ilişkin bilgileri EKAP üzerinden sorgulayarak belge tamamlama sorumluluğu bulunmadığının ifade edildiği, ancak kendilerinin bir belge tamamlama taleplerinin bulunmadığı, zaten EKAP'ta var olan bilgilerin yine bu sistem üzerinden sorgulanarak teyit edilmesi taleplerinin bulunduğu, başvuruya konu ihalenin e-teklif alınarak yapıldığı göz önüne alındığında bilgilerin EKAP veya diğer kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının internet sayfası üzerinden sorgulanması esasına dayanan e-ihalede, bu hususa ilişkin teyidin EKAP üzerinden yapılmasının ihalenin yapılış şekline son derece uygun olacağı, ayrıca idareye yapılan şikâyet başvurularına verilen cevap yazısında; Ticaret Sicil Müdürlüğü'nden alınan yazı ile şirket ortaklarından Ahmet Adnan Karacan'a ait T.C. kimlik numarasının EKAP sisteminde kayıtlı olan iş deneyim belgesinde yer aldığı hususuyla ilgili idarece herhangi bir cevap verilmediği, Aynı idarenin daha önceden fiziki ortamda yapmış olduğu ihalelerde ve başka idarelerin yapmış oldukları ihalelerde teklifleri kapsamında aynı ticaret sicil gazetelerinin sunulduğu ve bu ihalelerde yeterli kabul edildikleri, ancak başvuruya konu ihalede yeterlik bilgileri tablosunda aynı ticaret sicil gazetelerine ilişkin bilgiler beyan edilmesine rağmen yeterli bulunmamalarının kabul edilemeyeceği, belgelere ilişkin sorgulamanın sadece ve sadece EKAP veya diğer kamu kurumlarının internet sayfaları üzerinden yapılmasını zorunlu kılan bir mevzuat olmadığı, idarede bulunan şirketlerine ait sözleşme ve ihale dosyalarındaki fiziki belgelerden faydalanılarakta bu sorgulamaların yapılmasının mümkün olduğu şirketlerine ait bilgilerin e-teklif kapsamında EKAP'ta kayıtlı diğer bilgilerden yararlanılarak teyit edilmesi mümkünken idarece "...yeterlik bilgileri tablosunda beyan edilmeyen hiçbir belgenin sorgulanması mümkün olmamaktadır. " şeklindeki cevaba katılmalarının mümkün olmadığı,

İhale komisyonunun ihale sürecinde bilgi eksikliğinin tamamlanması veya mevcut bir belge üzerindeki tereddütlerin giderilmesi için ilgili kurumlar nezdinde araştırma yapma yetkisi olduğu halde idarece bu araştırmanın yapılmadığı, nasıl ki yeterlik belgeleri arasında yer alan bir iş deneyim belgesinde tereddüt oluştuğunda belgeyi düzenleyen ilgili kurumlar nezdinde araştırma yapılıyorsa, burada da Ankara Ticaret Sicil Müdürlüğü nezdinde kolaylıkla araştırma yapılması ve değerlendirmenin bu kapsamda yapılması gerektiği, yeterlik bilgileri tablosunda şirket ortağı ve yetkililerine ait T.C. kimlik numaralarının açıkça beyan edildiği ve beyan edildiği hususun ihale

komisyonu tarafından da kabul edildiği, bu konuyla ilgili idarece eğer tereddüt oluştursa bunların teyidi için idarece EKAP üzerinden araştırma yapılmasının gerektiği, eğer EKAP üzerinden gerekli bilgileri elde etmede idarece yetersiz kalınıyorsa bu defa firmalarından gerekli bilgilerin istenmesi ya da ilgili kurum nezdinde araştırma yapılmasının gerektiği, bu haliyle söz konusu hususla ilgili gereken belgelendirmenin taraflarınca yapılabileceği, ihale mevzuatına göre bilgi eksikliğinin tamamlanması hususunun ihale komisyonunun isteğine veya iradesine bağlı olmadığı, 4734 sayılı Kamu İhale Kanunu'nun 37'nci maddesinin ikinci fıkrasındaki emredici hükmüne ve Kamu İhale Genel Tebliği'nin 16.6.1(b) maddesindeki açıklamalara dayandığı, belgenin içeriğine ilişkin tereddüt yaratacak nitelikte olan ve belgeyi düzenleyen kurum, kuruluş veya kişilerden kaynaklanan bilgi eksikliklerinin giderilmesine ilişkin belgelerin idarelerce tamamlanması gerektiği halde ihale komisyonunca böyle bir işlem yapılmadığı, ayrıca kamu ihale mevzuatında, şirket ortaklarının ve/veya yöneticilerinin T.C. kimlik numaralarının ayrıca bir belge ile tevsik edilmesi gerektiği yönünde bir düzenleme de bulunmadığı,

Başvuruya konu ihalede istekliler tarafından sunulan teklif miktarları ile sınır değer miktarından da anlaşılacağı üzere, esasen ekonomik açıdan en avantajlı birinci teklif sahibi olmalarına rağmen, EKAP bilgileri incelenmeden, şirketlerinden tereddütleri giderici veya tevsik edici herhangi bir bilgi istenilmeden yahut belgeyi düzenleyen Kurumlar nezdinde de bir araştırma yapılmadan ve en önemlisi de ihaleye sunulan teklif miktarları itibariyle kendi teklif miktarları ile ihale üzerinde bırakılan isteklinin teklifi arasındaki yüksek miktardaki fiyat farkı dikkate alınmadan karar verildiği ve kamu menfaatinin göz ardı edildiği,

Ayrıca ihaleye sunulan belgelerin içeriğinde şirket ortaklarına ait T.C. kimlik numaralarının yer almaması hususu teklifin esasını değiştirecek nitelikte görülmemekle bu gibi bilgi eksikliğinin idarece tamamlanması gerektiğine karar verilen birçok İdare Mahkemesi ve Danıştay kararlarının da bulunduğu, özellikle Danıştay Onüçüncü Dairesinin konuya ilişkin sundukları emsal kararlara göre; teklif dosyasına sunulan belgelerin içinde T.C. kimlik numarası hiç yer almayan bir isteklinin belgesinin bilgi eksikliği kapsamında tamamlanması gerektiğine hükmedildiği halde; bahse konu ihaleye e-teklif şeklinde sundukları yeterlik bilgileri tablosunun ticaret sicili bilgileri bölümünde şirket ortakları ile yönetici ortağına ait T.C. kimlik numaralarının açıkça yazılıp beyan edildiği halde başvuruya konu ihalede tekliflerinin değerlendirme dışı bırakılmasının uygun olmadığı, bununla birlikte ihale üzerinde bırakılan isteklinin teklif fiyatı ile kendi teklifleri arasındaki fark göz önüne alındığında, ihalenin bu şekilde sonuçlandırılmasının kamu zararına neden olacağı,

4734 sayılı Kanun'un 37'nci maddesi, Yapım İşleri İhaleleri Uygulama Yönetmeliği'nin 57'nci maddesinin beşinci fıkrası ile aynı Yönetmelik'in 60/A maddesinin dokuzuncu fıkrası, İdari Şartname'nin 22.8'inci ve 31.3'üncü maddesi ile Kamu İhale Genel Tebliği'nin 16.6.l/b maddesine göre idarelerin isteklilerce sunulan belgelerin içeriğine ilişkin teyit amaçlı bilgi ve belge isteyebileceği, bilgi eksikliklerinin tamamlanabileceğinin hüküm altına alındığı, idarelerin bu konuda sorumlu oldukları, Elektronik İhale Uygulama Yönetmeliği'nde, teklifin esasını değiştirecek nitelikte olmayan bilgi eksikliklerinin tamamlanacağına dair açık bir düzenleme olmadığından, anılan Yönetmelik'in 29'uncü maddesine istinaden ilgili Yapım İşleri İhaleleri Uygulama Yönetmeliği'nin 57'nci maddesinin beşinci fıkrasındaki hüküm gereği belgelerdeki bilgi eksikliğinin tamamlanması cihetine gidilmesi gerektiği, ancak bahse konu ihalede en düşük teklif olmalarına rağmen idarece taraflarından herhangi bir bilgi talebinde bulunulmadığı,

Ayrıca idarenin şikâyete cevap yazısında, Danıştay Onüçüncü Dairesinin e-ihale olarak yapılan ihalelerde T.C. kimlik numaraları hususu ile ilgili henüz bir kararı olmadığını belirtildiği, idarenin buna sığınarak şikâyet başvuru dilekçesinde belirtilen yasal gerekçeler ve Danıştay kararlarını görmezlikten gelmesinin doğru olmadığı, bir konuda karar verilebilmesi için mutlak şekilde Danıştay kararına ihtiyaç duyulmasının doğru olmadığı iddialarına yer verilmiştir.

Başvuru sahibinin iddialarının değerlendirilmesi sonucunda aşağıdaki hususlar tespit edilmiştir.

İdarece ihale işlem dosyası kapsamında gönderilen 30.01.2020 tarihli ihale komisyonu kararı incelendiğinde, başvuruya konu ihaleye 18 istekli tarafından teklif sunulduğu,

Hsy Yapı İnşaat San. ve Tic. A.Ş. - Makro Anadolu İnşaat Madencilik Enerji Yol Yapı San. ve Ltd. Şti. İş Ortaklığının geçici teminat mektubu usulüne uygun olmadığından, Doku İnşaat Turizm Enerji San. ve Tic. A.Ş.- Krom İnşaat Turizm İthalat İhracat San. ve Ltd. Şti. İş Ortaklığının ise geçici teminat tutarı asgari kriteri sağlamadığından söz konusu iki isteklinin tekliflerinin geçersiz teklif olarak belirlendiği, Söz konusu ihale komisyonu kararında ilk oturumda geçerli teklif olarak belirlenen başvuru sahibi istekli dahil 9 adet isteklinin elektronik teklif mektubu ekinde sunmuş oldukları yeterlik bilgileri tablosunda genel olarak; beyan edilen bilgilerin teyit kriterine uygun olarak teyit edilememesinden, yeterlik bilgileri tablosunda beyan edilen bilgilerin teyit kriterlerine dayanak gösterilen belgelerde bulunmamasından veya bu bilgilerin söz konusu teyit belgelerinde beyan edilenden farklı şekilde bulunmasından ve beyan edilen yeterlik kriterlerinin başvuruya konu ihaledeki yeterlik kriterlerini karşılamadığından söz konusu 9 isteklinin tekliflerinin değerlendirme dışı bırakıldığı,

Geçici teminat mektubu uygun olan 16 adet geçerli teklif üzerinden yapılan sınır değer hesaplamasında sınır değerın 84.835.670,29 TL olarak hesaplandıđı, sınır değerin altında teklif sunan Metro Mühendislik Gıda Maddeleri San. ve Tic. Ltd. Şti. - Mustafa Özyaydın İş Ortaklığı, Alfen Taahhüt İnşaat Maden Nakliye San. ve Tic. Ltd. Şti. - Magnesia Yapı İnşaat San. ve Tic. Ltd. Şti. İş Ortaklığı ve Tetiş Yapı İnşaat Sanayi ve Ticaret A.Ş.den idarece aşırı düşük teklif açıklaması istenildiđi, ancak söz konusu istekliler aşırı düşük teklif açıklamasında bulunmadıđından söz konusu isteklilerin tekliflerinin reddedildiđi,

Akabinde ekonomik açıdan en avantajlı birinci teklif olması öngörülen Holođlu İnş. Tic. ve San. Ltd. Şti. ile ikinci teklif olması öngörülen Erensan İnş. Mlz.ve İnş. Orm. Ürn. San. ve Tic. Ltd. Şti.den, Elektronik İhale Uygulama Yönetmeliđi'nin 21'inci maddesinin ikinci fıkrasına uygun olarak alınmayan geçici teminat mektupları ile yeterlik bilgileri tablosunda beyan ettikleri bilgi ve belgelerden, EKAP veya diđer kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının internet sayfası üzerinden sorgulanarak temin veya teyit edilemeyen belgeleri, belgelerin sunuluş şekline uygun olarak sunmalarının istenildiđi, söz konusu isteklilerin idarece istenilen belgeleri belgelerin sunuluş şekline uygun olarak sunduđu ve idarece yapılan değerdendirme neticesinde ihalenin Holođlu İnş. Tic. ve San. Ltd. Şti.nin üzerinde bırakıldıđı, Erensan İnş. Mlz. ve İnş. Orm. Ürn. San. ve Tic. Ltd. Şti.nin teklifinin ise ekonomik açıdan en avantajlı ikinci teklif sahibi olarak belirlendiđi görülmüştür.

30.01.2020 tarihli ihale komisyonu kararında başvuru sahibinin teklifinin değerdendirme dıřı bırakılma gerekçelerinin "...Yeterlik bilgileri tablosunda Raymak Yapı A. Ş. tarafından beyan edilen 02.08.2019 tarih ve 9**2 sayılı, 11.08.2016 tarih ve 9**5 sayılı, 14.08.2015 tarih ve 8**4 sayılı Ticaret Sicil Gazetelerinin "www.ticaretsicil.gov.tr" adresinden sorgulanması neticesinde, ortakların ad, soyad ve ortaklık oranlarına yer verildiđi, söz konusu gazetelerde şirket ortaklarından "A. A. KARACAN" ve "T. GÜRBOĐA " ya ait T.C. kimlik numaralarına yer verilmediđi görülmüştür...

Raymak Yapı A.Ş. tarafından yeterlik bilgileri tablosunda şirket ortakları ve yetkililerinin T.C. kimlik numaraları belirtilmiş ise de, söz konusu bilgilerin teyidinin yapılabileceđi belge olarak beyan edilen 02.08.2019 tarih ve 9**2 sayılı, 11.08.2016 tarih ve 9**5 sayılı, 14.08.2015 tarih ve 8**4 sayılı Ticaret Sicil Gazetelerinde şirket ortaklarından A. KARACAN ve T. GÜRBOĐA' ya ait T.C. kimlik numarası bilgisinin bulunmadıđı, ayrıca yeterlik bilgileri tablosunun "Diđer belgeler kullanılarak tevsik ediliyorsa bu belgelerin tarih ve sayısı ile düzenleyen gerçek/tüzel kiři " bölümünün doldurulmaması nedeniyle söz konusu bilgilerin teyidinin yapılamadıđı göz önünde bulundurulduđunda, Raymak Yapı A.Ş.'nin e-teklifi değerdendirme dıřı bırakılmıştır." şeklinde olduđu görülmüştür.

Bu kapsamda ihale komisyonu kararında başvuru sahibinin teklifinin değerlendirme dışı bırakılma gerekçelerine bakıldığında, başvuru sahibi tarafından yeterlik bilgileri tablosunda ortakların kimlik numaralarının belirtildiği, ancak bu bilgilerin teyit edilmesine dayanak gösterilen ticaret sicil gazetelerinde ortakların kimlik numaraları bilgisine ulaşılamadığı gerekçesine yer verildiği anlaşılmıştır.

Yapım İşleri İhaleleri Uygulama Yönetmeliği'nin "Aday veya isteklinin mesleki faaliyetini sürdürdüğünü ve teklif vermeye yetkili olduğunu gösteren belgeler" başlıklı 38'inci maddesinde "(1) İhalelere katılacak aday veya istekliler tarafından,

a) Gerçek kişi olması halinde, noter tasdikli imza beyannamesinin,

b) Tüzel kişi olması halinde, ilgisine göre tüzel kişiliğin ortakları, üyeleri veya kurucuları ile tüzel kişiliğin yönetimindeki görevlileri belirten son durumu gösterir Ticaret Sicil Gazetesi, bu bilgilerin tamamının bir Ticaret Sicil Gazetesinde bulunmaması halinde, bu bilgilerin tümünü göstermek üzere ilgili Ticaret Sicil Gazeteleri veya bu hususları gösteren belgeler ile tüzel kişiliğin noter tasdikli imza sirkülerinin,

teklif kapsamında sunulması zorunludur..." hükmü,

Anılan Yönetmelik'in "Elektronik ihale" başlıklı 60/A maddesinde "...(9) İhale dokümanında belirtilen geçici teminat mektubu, katılım belgeleri ve yeterlik kriterleri ile fiyat dışı unsurlara ilişkin değerlendirme, istekliler tarafından beyan edilen bilgi ve belgelerden; EKAP veya diğer kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının internet sayfası üzerinden sorgulanarak temin veya teyit edilebilenler için, sorgulama sonucunda elde edilen bilgiler; belirtilen yöntemle temin veya teyit edilemeyenler için ise yeterlik bilgileri tablosunda beyan edilen bilgiler esas alınarak yapılır. Bu değerlendirme sonucunda ihalede öngörülen şartları sağlamadığı anlaşılan teklifler değerlendirme dışı bırakılır..." hükmü,

Elektronik İhale Uygulama Yönetmeliği'nin "e-tekliflerin değerlendirilmesi" başlıklı 24'üncü maddesinde "...(3) İhale dokümanında belirtilen katılım belgeleri ve yeterlik kriterleri ile ilgili değerlendirme, e-teklif kapsamında yüklü olan belgelerin ve EKAP üzerinden ilgili kurum ve kuruluşların sistemlerinden sorgulama suretiyle elde edilen bilgilerin değerlendirilmesi suretiyle yapılır.

(4)Yeterlik kriterlerinin istekliler tarafından karşılanıp karşılanmadığına ilişkin değerlendirme ihale dokümanında yer alan hükümler çerçevesinde yapılır. Yeterlik kriterlerini karşılamayan isteklilerin

teklifleri değerlendirme dışı bırakılır ve bu husus gerekçesi de açıkça belirtilmek suretiyle EKAP'a kaydedilir." hükmü,

Kamu İhale Genel Tebliği'nin "Tüzel kişilerin teklif vermeye yetkili olduğunu gösteren belgeler" başlıklı 10/A maddesinde "10/A.1 İhaleye katılabilmek için başvuru veya teklif dosyasında sunulması gereken, tüzel kişi aday ve isteklilerin teklif vermeye yetkili olduğu hususunda son durumu gösterir belgelere ilişkin mevzuatta geçen "tüzel kişi ortakları" ifadesinden, bu ortakların ilgisine göre ad, soyad/ticaret unvanı, T.C. kimlik numarası/vergi kimlik numarası ile ortaklık oranları (halka arz edilen hisseler hariç); "tüzel kişilerin yönetimindeki görevliler" ifadesinden ise, teklif veya başvuru mektubu ya da sözleşmeyi imzalayanlar da dahil olmak üzere tüzel kişilikteki yönetim, temsil ve ilzama yetkili kişiler anlaşılır." açıklaması yer almaktadır.

İdari Şartname'nin "İhale konusu işe/alıma ilişkin bilgiler" başlıklı 2'nci maddesinde "2.1. İhale konusu işin/alımın;

- a) Adı: Muğla Marmaris 125 Yataklı Devlet Hastanesi Yapım İşi
- b) Türü: Yapım işleri
- c) İlgili Uygulama Yönetmeliği: Yapım İşleri İhaleleri Uygulama Yönetmeliği
- ç) Yatırım proje no'su (yapım işlerinde): 1991I000090
- d) Kodu:
- e) Miktarı: 1 Adet Üst Yapı Hastane İnşaatı: 2B+Z+5 Katlı Ayrıntılı bilgi idari şartnamenin ekinde yer almaktadır.

f) İşin yapılacağı/malın teslim edileceği yer: Muğla İli Marmaris İlçesi" düzenlemesi,

Anılan Şartname'nin "İhaleye ilişkin bilgiler" başlıklı 3'üncü maddesinde "3.1.

- a) İhale kayıt numarası: 2019/408602
- b) İhale usulü: Açık ihale.
- c) İhale (son teklif verme) tarihi ve saati: 11.11.2019 Saat: 10:30
- ç) İhale komisyonunun toplantı yeri (e-tekliflerin açılacağı adres): Sağlık Yatırımları Genel Müdürlüğü İhale Daire Başkanlığı, Bilkent Yerleşkesi Üniversiteler Mahallesi Dumlupınar Bulvarı 6001. Cadde No:9 Zemin Kat 3 Nolu Toplantı Salonu Çankaya Ankara

3.2. Teklifler, ihale (son teklif verme) tarih ve saatine kadar EKAP üzerinden e-teklif olarak sunulur. İhale (son teklif verme) saatine kadar EKAP'a yüklenemeyen teklifler değerlendirmeye alınmaz." düzenlemesi,

Aynı Şartname'nin "İhaleye katılabilmek için gereken belgeler ve yeterlik kriterleri" başlıklı 7'nci maddesinde "7.1. İsteklilerin ihaleye katılabilmeleri için aşağıda sayılan belgeler ve yeterlik kriterleri ile fiyat dışı unsurlara ilişkin bilginlerin e-teklifleri kapsamında beyan etmeleri gerekmektedir.:

a) Teklif vermeye yetkili olduğunu gösteren imza beyannamesi veya imza sirküleri;

1) Gerçek kişi olması halinde, noter tasdikli imza beyannamesi,

2) Tüzel kişi olması halinde, ilgisine göre tüzel kişiliğin ortakları, üyeleri veya kurucuları ile tüzel kişiliğin yönetimindeki görevlileri belirten son durumu gösterir Ticaret Sicil Gazetesi, bu bilgilerin tamamının bir Ticaret Sicil Gazetesinde bulunmaması halinde, bu bilgilerin tümünü göstermek üzere ilgili Ticaret Sicil Gazeteleri veya bu hususları gösteren belgeler ile tüzel kişiliğin noter tasdikli imza sirküleri..." düzenlemesi,

"Tekliflerin sunulma şekli" başlıklı 22'nci maddesinde "22.1. e-teklifler istekliler tarafından EKAP üzerinden, yalnızca teklif mektubu ve ekleri doldurularak hazırlandıktan sonra e-imza ile imzalanarak ihale tarih ve saatine kadar gönderilir. Ortak girişimlerde e-teklifin ortakların tamamı tarafından e-imza ile imzalanması zorunludur. Teklife ilişkin e-anahtar, e-teklif ile birlikte ihale tarih ve saatine kadar EKAP üzerinden gönderilir.

22.2. Yeterlik bilgileri tablosunda ihaleye katılabilmek için gereken belgeler ve yeterlik kriterleri ile fiyat dışı unsurlar, teknik şartnameye cevaplar ve açıklamalar standart formunda ise açıklama istenen teknik özellikler için ayrı satırlar açılmış olup, istekliye ait hangi belgeler esas alınarak ihaleye katılım sağlanmış ise o belgelere ilişkin tarih, sayı, yevmiye numarası gibi bilgiler ile istenen kriterlere ve açıklamalara ilişkin belgelerde yer alan gerekli bilgiler eksiksiz olarak açık ve anlaşılır bir şekilde belirtilmek suretiyle ekli standart formlara uygun şekilde doldurulacaktır..." düzenlemesi,

"Tekliflerin değerlendirilmesi" başlıklı 31'inci maddesinde "31.1. İlk oturumun kapatılmasından sonra, ihale komisyonu belirleyeceği bir tarih ve saatte toplanır ve EKAP üzerinde tekliflerin değerlendirilmesine başlanır. Teklif değerlendirme işlemleri birden fazla oturumda yapılabilir. Her oturum kapatılmadan önce bilgiler EKAP'a kaydedilir ve düzenlenen tutanakların bir çıktısı alınarak ihale komisyonu üyeleri tarafından imzalanır.

31.2. Teklif deęerlendirmesinde öncelikle ilk oturumda 30 uncu madde uyarınca e-teklifinin açılmadığı veya teklif mektubu ile geçici teminatının uygun olmadığı tespit edilen isteklilerin teklifleri deęerlendirme dıőı bırakılır.

31.3. İhale dokümanında belirtilen geçici teminat mektubu, katılım belgeleri ve yeterlik kriterleri ile fiyat dıőı unsurlara ve istenilmişse teknik şartnameye cevaplar ve açıklamalara ilişkin deęerlendirme, istekliler tarafından beyan edilen bilgi ve belgelerden; EKAP veya dięer kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının internet sayfası üzerinden sorgulanarak temin veya teyit edilebilenler için, sorgulama sonucunda elde edilen bilgiler; belirtilen yöntemle temin veya teyit edilemeyenler için ise beyan edilen bilgiler esas alınarak yapılır...” düzenlemesi yer almaktadır.

Yukarıda aktarılan mevzuat hüküm ve açıklamaları ile ihale dokümanında yer alan düzenlemelerden; e-teklif alınmak suretiyle yapılan ihalelerde, Elektronik İhale Uygulama Yönetmelięi'nin ekinde bulunan “Yeterlik Bilgileri Tablosu Sunulan ve Tekliflerin Elektronik Ortamda Alındığı İhalelerde Uygulanacak Tip İdari Şartname” ve ilgili yönetmeliklerin ekinde bulunan dięer standart formların kullanılacağı, bu doğrultuda teklif mektubunun eklerinden biri olan yeterlik bilgileri tablosunun da EKAP üzerinden isteklilerce hangi belgeler esas alınarak ihaleye katılım sağlanmış ise o belgelere ilişkin tarih, sayı, yevmiye numarası gibi bilgiler ile istenen kriterlere ve açıklamalara ilişkin belgelerde yer alan gerekli bilgiler eksiksiz olarak açık ve anlaşılır bir şekilde belirtilmek suretiyle, ihale dokümanı ekinde verilen standart forma uygun şekilde doldurulacağı,

İhale dokümanında belirtilen geçici teminat mektubu, katılım belgeleri ve yeterlik kriterleri ile fiyat dıőı unsurlara ilişkin deęerlendirmenin, istekliler tarafından beyan edilen bilgi ve belgelerden; EKAP veya dięer kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının internet sayfası üzerinden sorgulanarak temin veya teyit edilebilenler için sorgulama sonucunda elde edilen bilgiler; belirtilen yöntemle temin veya teyit edilemeyenler için ise yeterlik bilgileri tablosunda beyan edilen bilgiler esas alınarak yapılacağı, bu deęerlendirme sonucunda ihalede öngörülen şartları sağlamadığı anlaşılan tekliflerin deęerlendirme dıőı bırakılacağı anlaşılmaktadır.

Başvuruya konu ihalede, isteklilerin ihaleye katılabilmeleri için, teklif vermeye yetkili olduğunu gösteren imza beyannamesi veya imza sirkülerini ve tüzel kiői olmaları halinde, ilgisine göre tüzel kiőiliğın ortakları, üyeleri veya kurucuları ile tüzel kiőiliğın yönetimindeki görevlileri belirten son durumu gösterir Ticaret Sicili Gazetesi/Gazetelerini veya bu hususları gösteren belgeleri e-teklifleri kapsamında beyan etmeleri gerektięi, bu doğrultuda ihale dokümanı kapsamında verilen yeterlik bilgileri tablosunun “İhaleye Katılmak İçin Gereken Belgeler ve Yeterlik Kriterleri” sütununun “Teklif Vermeye Yetkili Olunduğuna İlişkin Bilgiler” satırının “Ticaret Sicili Bilgileri” bölümünde bulunan;

“Ortaklara Ait Bilgiler (Halka Arz Edilen Hisseler Hariç) [Ortakların: Gerçek Kişi Olması Durumunda Ad-Soyad/TC Kimlik Numarası/ Ortaklık Oranı/ Varsa İşletme Adı ve Ticaret Unvanı; Tüzel Kişi Olması Durumunda Ticaret Unvanı/Vergi Kimlik Numarası/Ortaklık Oranı/Varsa İşletme Adı]”,

“Yöneticilere Ait Bilgiler(Ad-Soyad/TC Kimlik Numarası ve Görevi)”,

“Ticaret Sicili Gazetesi/Gazetelerinin Tarihi, Sayısı ve Sicil Müdürlüğü” ve

“Diğer Belgeler Kullanılarak Tevsik Ediliyorsa Bu Belgelerin Tarih ve Sayısı ile Düzenleyen Gerçek/Tüzel Kişi” kısımların ilgisine göre, isteklilerce hangi belgeler esas alınarak ihaleye katılım sağlanmış ise o belgelere ilişkin tarih, sayı, yevmiye numarası gibi bilgiler ile istenen kriterlere ve açıklamalara ilişkin belgelerde yer alan gerekli bilgilere göre eksiksiz olarak açık ve anlaşılır bir şekilde doldurulması gerektiği anlaşılmaktadır.

İdarece gönderilen ihale işlem dosyası incelendiğinde; başvuru sahibi Raymak Yapı A.Ş. tarafından yeterlik bilgileri tablosunun “İhaleye Katılmak İçin Gereken Belgeler ve Yeterlik Kriterleri” sütununun “Teklif Vermeye Yetkili Olduğuna İlişkin Bilgiler” satırının “Ticaret Sicili Bilgileri”nin gösterildiği bölümde yer alan;

- “Ortaklara Ait Bilgiler (Halka Arz Edilen Hisseler Hariç) [Ortakların: Gerçek Kişi Olması Durumunda Ad-Soyad/TC Kimlik Numarası/ Ortaklık Oranı/ Varsa İşletme Adı ve Ticaret Unvanı; Tüzel Kişi Olması Durumunda Ticaret Unvanı/Vergi Kimlik Numarası/Ortaklık Oranı/Varsa İşletme Adı]” kısmında,

“Ahmet Adnan Karacan, 65*****, %51”,

“Tahsin Gürboğa, 33*****, %49” şeklinde,

-“Yöneticilere Ait Bilgiler Ad-Soyad/TC Kimlik Numarası ve Görevi” kısmında “Tahsin Gürboğa, 33*****, Yönetim Kurulu Başkanı” şeklinde,

- “Ticaret Sicili Gazetesi/Gazetelerinin Tarihi, Sayısı ve Sicil Müdürlüğü” kısmında, “14.08.2015, 8884-Sayfa:20, Ankara Ticaret Sicil Müdürlüğü”

“11.08.2016, 9135-Sayfa:44-45, Ankara Ticaret Sicil Müdürlüğü”

“02.08.2019, 9882-Sayfa:40, Ankara Ticaret Sicil Müdürlüğü” şeklinde beyanın yer aldığı,

- “Diğer Belgeler Kullanılarak Tevsik Ediliyorsa Bu Belgelerin Tarih ve Sayısı İle Düzenleyen Gerçek/Tüzel Kişi” kısmında ise herhangi bir bilginin beyan edilmediği tespit edilmiştir.

Başvuru sahibi istekli tarafından teklif vermeye yetkili olduğu hususunda son durumu gösterir belgelere ilişkin yeterlik bilgileri tablosunda beyan edilen; 14.08.2015 tarih ve 8884 sayılı, 11.08.2016 tarih ve 9135 sayılı ve 02.08.2019 tarih ve 9882 sayılı Ticaret Sicili Gazetelerinin “www.ticaretsicil.gov.tr” adresinden sorgulanması neticesinde, söz konusu gazetelerde son ortaklık yapısına ilişkin ortakların ad, soyad ve ortaklık oranlarına yer verildiği, bu durumda şirket ortaklarının ve ortaklık hisselerinin “Ahmet Adnan Karacan (%51)” ve “Tahsin Gürboğa (%49)” şeklinde olduğu görülmekle birlikte, anılan gazetelerde söz konusu kişilere ait T.C. kimlik numaralarına yer verilmediği görülmüştür.

Yapım İşleri İhaleleri Uygulama Yönetmeliği'nin 38.1.(b) maddesindeki hükümler uyarınca tüzel kişiliğin ortakları, üyeleri veya kurucuları ile tüzel kişiliğin yönetimindeki görevlilerine ilişkin bilgilerin, son durumu gösterir Ticaret Sicili Gazetesi ya da bu hususları gösteren belgeler ile tevsik edilmesi gerektiği, e-teklif alınarak gerçekleştirilen ihalelerde ise yeterlik bilgileri tablosunda bu durumu gösteren ilgili Ticaret Sicili Gazetesi/Gazetelerinin beyan edileceği, bu bilgilerin Ticaret Sicili Gazetesinde bulunmaması halinde söz konusu bilgilerin teyidinin diğer belgeler üzerinden yapılmasına da imkân tanındığı ve bu durumda yeterlik bilgileri tablosunun “Diğer belgeler kullanılarak tevsik ediliyorsa bu belgelerin tarih ve sayısı ile düzenleyen gerçek/tüzel kişi” bölümünün doldurulması gerektiği,

Kamu İhale Genel Tebliği'nin “Tüzel kişilerin teklif vermeye yetkili olduğunu gösteren belgeler” başlıklı 10/A maddesindeki açıklamalardan ise tüzel kişi aday ve isteklilerin teklif vermeye yetkili olduğu hususunda son durumu gösterir belgelere ilişkin mevzuatta geçen “tüzel kişi ortakları” ifadesinden, bu ortakların ilgisine göre ad, soyad/ticaret unvanı, T.C. kimlik numarası/vergi kimlik numarası ile ortaklık oranlarının anlaşılması gerektiği açıklanmıştır.

Başvuru sahibi isteklinin itirazın şikayet başvuru dilekçesinde iddia ettiği hususlara bakıldığında genel olarak, yeterlik bilgileri tablosunda beyan etmiş olduğu ortaklara ait T.C. kimlik numaralarının ilgili Ticaret Sicili Gazetelerinde gözükmemesinden dolayı idare tarafından tekliflerinin değerlendirme dışı bırakılmasının yerinde olmadığı, söz konusu ortaklara ait T.C. kimlik numaralarına ilişkin sorgulamaların idarece gerek elektronik ortamda gerekse de fiziki ortamda farklı şekillerde yapılmasının mümkün olduğu, şayet bu sorgulamalar idare tarafından yapılmıyorsa bu hususa ilişkin bilgi eksikliği kapsamında işlem yapılması gerektiği, ortaklara ait T.C. kimlik numaralarının tevsik edilmediği durumlara ilişkin bu hususun teklifin esasına etki etmediğine yönelik farklı ve birçok İdare Mahkemesi ve Danıştay kararlarının bulunduğu, dolayısıyla ihale

üzerinde bırakılan istekliye kıyasla düşük tutarda olan tekliflerinin bu gerekçeyle değerlendirme dışı bırakılmaması ve kamu zararına sebebiyet verilmemesi gerektiği iddia edilmektedir.

Başvuruya konu ihalenin elektronik ihale şeklinde yapıldığı, bu kapsamda fiziki ortamda yapılan ihalelerden farklı olarak yukarıda aktarılan mevzuat hükümleri ve doküman düzenlemelerine göre ihale dokümanında belirtilen yeterlik kriterleri ile ilgili değerlendirmenin istekliler tarafından beyan edilen bilgi ve belgeler üzerinden yapılacağı, istekliler tarafından beyan edilen bilgi ve belgelerden, EKAP veya diğer kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının internet siteleri üzerinden sorgulanabilenlerin, söz konusu belgelerdeki kayıtlı bilgiler esas alınarak değerlendirmeye tabi tutulacağı anlaşılmıştır.

Bu kapsamda istekliler tarafından yeterlik bilgileri tablosunda beyan edilen bilgi ve belgelere, idarece gerek elektronik ortamda gerekse de fiziki ortamda ulaşılabilese dahi, yeterlik bilgileri tablosunda isteklinin ayrıca sorgulamanın hangi bilgi ve belgeler kapsamında yapılacağına ilişkin beyanı da bulunduğundan ve idarece yapılacak değerlendirmede bu beyanın esas alınması gerektiğinden, idare tarafından yapılması gereken sorgulamanın, istekli tarafından yeterlik bilgileri tablosunda beyan edilen sorgulama kriterine göre yapılması gerekmektedir. Akabinde isteklinin yeterlik bilgileri tablosunda yeterliğe ilişkin beyan ettiği bilgi ve belgelerin yine isteklinin yeterlik bilgileri tablosunda beyan ettiği sorgulama kriterine göre idare tarafından sorgulanması neticesinde isteklinin bu bilgi ve belgeler kapsamında yeterli olup olmadığı değerlendirmesi yapılacaktır.

Ayrıca isteklilerin yeterlik bilgileri tablosunda beyan ettikleri bilgi ve belgelerden, EKAP veya diğer kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının internet siteleri üzerinden sorgulanamayanların değerlendirmesi ise yine ilk olarak isteklinin beyanı üzerinden yapılacak, daha sonra şayet isteklinin elektronik ortamda sorgulanamayan yeterlik belgelerinin idare tarafından belgelerin sunuluş şekline uygun olarak sunulması istenirse söz konusu beyanın doğruluğu ve teklif değerlendirmesiyle ilgili değerlendirme bu aşamada yapılacaktır.

Bu bağlamda elektronik ihalede yapılacak teklif değerlendirmesi, fiziki ortamda yapılan teklif değerlendirmelerinden farklılık arz ettiği için, başvuru sahibi isteklinin fiziki ortamda gerçekleştirilen ihalelerdeki usuller esas alınarak oluşturduğu iddialara ilişkin hususların ve bu iddialara dayanak emsal göstermiş olduğu mahkeme kararlarına ilişkin değerlendirmelerin başvuruya konu ihalede uygulanma imkanı bulunmamaktadır.

Yapılan incelemede başvuru sahibi istekli tarafından yeterlik bilgileri tablosunda şirket ortakları ve yetkililerinin T.C. kimlik numarası belirtilmiş ise de, söz konusu bilgilerin teyidinin yapılabileceği belge olarak beyan edilen Ticaret Sicili Gazetelerinde anılan kişilere ait T.C. kimlik numarası

bilgisinin açıkça belirtilmediği, dolayısıyla idarece istekli tarafından beyan edilen bilgilerin teyidinin yapılabileceği belge olarak beyan edilen Ticaret Sicili Gazeteleri sorgulandığında kimlik numaralarına ilişkin teyidin yapılamadığı, ayrıca başvuru sahibi istekli tarafından yeterlik bilgileri tablosunun ortaklara ait T.C. kimlik numaralarının elektronik ortam dışında teyit edilmesine olanak sağlayan “Diğer belgeler kullanılarak tevsik ediliyorsa bu belgelerin tarih ve sayısı ile düzenleyen gerçek/tüzel kişi” bölümünün de doldurulmaması nedeniyle kimlik numaralarına ilişkin bilgilerin teyidinin bu şekilde de yapılamadığı, göz önünde bulundurulduğunda başvuru sahibinin teklifinin bu gerekçeyle değerlendirme dışı bırakılmasında mevzuata aykırılık bulunmadığı ve başvuru sahibinin söz konusu iddiasının yerinde olmadığı sonucuna varılmıştır.

Ayrıca İdari Şartname'nin “Tekliflerin sunulma şekli” başlıklı 22'nci maddesinin ikinci fıkrasında yeterlik bilgileri tablosunun EKAP üzerinden isteklilerce hangi belgeler esas alınarak ihaleye katılım sağlanmış ise o belgelere ilişkin tarih, sayı, yevmiye numarası gibi bilgiler ile istenen kriterlere ve açıklamalara ilişkin belgelerde yer alan gerekli bilgiler eksiksiz olarak açık ve anlaşılır bir şekilde belirtilmek suretiyle, ihale dokümanı ekinde verilen standart forma uygun şekilde doldurulacağını açık bir şekilde düzenlendiği, bu kapsamda söz konusu hususun eksik bilgi kapsamında tamamlanmasına da imkan bulunmadığı anlaşıldığından başvuru sahibinin itirazın şikayete konu olan hususların bilgi eksikliği kapsamında tamamlanması gerektiğine ilişkin iddiasının da yerinde olmadığı sonucuna varılmıştır.

Diğer taraftan başvuru sahibi isteklinin teklifinin yukarıda belirtilen gerekçelerle değerlendirme dışı bırakılmasında mevzuata aykırılık bulunmadığı, dolayısıyla teklifi geçersiz olan başvuru sahibi isteklinin teklifi ile ihale üzerinde bırakılan isteklinin geçerli teklifi arasında kamu zararı değerlendirmesinin yapılamayacağı anlaşıldığından, başvuru sahibi isteklinin bu konuyla ilgili iddialarının da yerinde olmadığı sonucuna varılmıştır.

Netice itibariyle başvuru sahibinin iddiaları yerinde bulunmadığından anılan isteklinin teklifinin değerlendirme dışı bırakılmasında mevzuata aykırılık bulunmadığı sonucuna varılmıştır.

Açıklanan nedenlerle, 4734 sayılı Kanun'un 65'inci maddesi uyarınca bu kararın tebliğ edildiği veya tebliğ edilmiş sayıldığı tarihi izleyen 30 gün içerisinde Ankara İdare Mahkemelerinde dava yolu açık olmak üzere,

Anılan Kanun'un 54'üncü maddesinin onbirinci fıkrasının (c) bendi gereğince itirazın şikâyet başvurusunun reddine,

Oybirliği ile karar verildi.

Kamu İhale Kurulu Kararı - KİK (K. 2018/UH.II-1130)

Kamu İhale Kurulu Kararı - KİK, K. 2018/UH.II-1130 T. 06.06.2018

BAŞVURU SAHİBİ: Universal Yazılım Anonim Şirketi,

İHALEYİ YAPAN İDARE: Kadıköy Belediye Başkanlığı Bilgi İşlem Müdürlüğü,

BAŞVURUYA KONU İHALE: 2018/57143 İhale Kayıt Numaralı "Süreç Bazlı Web Tabanlı Yönetim Bilgi Sistemi Yazılım Modülleri ve Elektronik Belge Yönetim Sistemi Hizmeti Alımı" İhalesi

KURUM TARAFINDAN YAPILAN İNCELEME:

Kadıköy Belediye Başkanlığı Bilgi İşlem Müdürlüğü tarafından 14.03.2018 tarihinde açık ihale usulü ile gerçekleştirilen "Süreç Bazlı Web Tabanlı Yönetim Bilgi Sistemi Yazılım Modülleri ve Elektronik Belge Yönetim Sistemi Hizmeti Alımı" ihalesine ilişkin olarak Universal Yazılım Anonim Şirketinin 05.03.2018 tarihinde yaptığı şikâyet başvurusunun, idarenin 13.03.2018 tarihli yazısı ile reddi üzerine, başvuru sahibince 20.03.2018 tarih ve 18454 sayılı Kurum kayıtlarına alınan 20.03.2018 tarihli dilekçe ile itirazen şikâyet başvurusunda bulunulmuştur.

Başvuruya ilişkin olarak 2018/465 sayılı itirazen şikâyet dosyası kapsamında yapılan inceleme neticesinde esas inceleme raporu tanzim edilmiştir.

KARAR:

Esas inceleme raporu ve ekleri incelendi.

İtirazen şikâyet dilekçesinde özetle,

- 1) Benzer iş tanımının ihale konusu iş ile aynı olmaması gerektiği, söz konusu ihaledeki benzer iş tanımının değiştirilmesi ve rekabete engel olmayacak şekilde düzenlenmesi gerektiği,
- 2) İdari Şartname'nin 5.1.5'inci ve 7.1.5'inci maddesinde iş zekâsı uygulamasına ilişkin düzenleme bulunduğu, idarece iş zekâsı modülünün şart olmadığı belirtilmekle birlikte bu değerlendirmenin hatalı olduğu, iş zekâsı modülü gerekli olsun olmasın personel niteliklerinin belirtilmemesinin de tereddütlere sebebiyet vereceği, Teknik Şartname'nin 9.24'üncü maddesinde iş zekâsı uygulama modülüne müdahil olacağı belirtilen personelin idari ve teknik yeterliliğinin bulunmadığı,
- 3) a- Teknik Şartname'nin 20.1.2'nci, 18.5'inci ve 19.5.2'nci maddelerinde "Oracle veri tabanı üzerinde çalışmalıdır." hükmü ile İdari Şartname'nin 7.1.h.5'inci maddesinde Oracle markasının aleni olarak

işaret edildiği, söz konusu düzenlemeler ile tek bir ürüne işaret edildiği, 4734 sayılı Kamu İhale Kanunu'nun temel ilkelerinin ihlal edildiği, idarenin Teknik Şartname düzenlemelerinin mevcut sistem göz önüne alınarak yapıldığı anlaşılmakta ise de düzenlemenin Oracle marka teklif edecek istekliler lehine maliyet avantajı yarattığı, alternatif bir çok VTYS (Veri Tabanlı Yönetim Sistemi) bulunduğu, Oracle Enterprise'in alternatifleri arasında maliyeti en yüksek VTYS olduğu,

b- İdarenin hali hazırda VTYS (Veri Tabanlı Yönetim Sistemi) olarak Oracle Standart Edition(SE) lisansı bulunduğu, idarenin mevcut lisansı ile ihale konusu ürün ve modüllerin kullanılmasının mümkün olduğu, ihale kapsamında bu lisansın kullanılmayarak tekrardan satın alınmasının kamu zararına ve ihale üzerinde bırakılacak istekinin sebepsiz zenginleşmesine neden olacağı, Teknik Şartname'nin 18.1'inci maddesi kapsamında talep edilen Oracle Enterprise Edition 4 CPU lisansının ihale konusu işe ilişkin modüllerin çalışması için zorunluluk arz etmediği, söz konusu lisansın neden talep edildiğinin belirtilmediği,

c) Teknik Şartname'nin 18.2'inci maddesinde Oracle Türkiye temsilciliğinden idare adına alınması istenilen lisans zorunluluğu ve özel yetki belgesi talep edildiği, söz konusu düzenleme ile rekabet ortamının ortadan kaldırıldığı, ihaleye katılmak isteyenlerin katılımın engellendiği, Türkiye'de özel şirket olarak faaliyet gösteren bir şirketten alınacak bir belgenin 4734 sayılı Kamu İhale Kanunu kapsamında yapılacak bir ihalede yeterlik belgesi olarak belirlenmesinin rekabeti engelleyici olduğu ve kamu menfaatine aykırı olduğu,

4) Teknik Şartname'nin "İşin Süresi ve Projenin Fazları" başlıklı 11'inci maddesinde "1.1. Birinci Faz: Sözleşmenin imzalanmasından 90 gün sonra tamamlanmalıdır. Ekli listede belirtilen yaklaşık 500 adet iş sürecinin (ana ve alt süreçler dahil olmak üzere) analizinin yapılması ... gerekmektedir." düzenlemesinin bulunduğu, söz konusu düzenlemede yer alan süreç yapısının tam olarak neyi ifade ettiğinin tam olarak anlaşılmadığı, süreçlerin idarenin ürettiği Yönetim Bilgi Sistemi (YBS) verileri kullanılarak çalışır hale getirilmesi gerektiği, söz konusu düzenlemede bahsi geçen Faz 1'de bahsi geçen süreç çalışmasının reel hayatta karşılığının teknik olarak mümkün olmadığı, ayrıca Teknik Şartname'nin 10.5'inci maddesinde yer alan tabloda "Yönetim Bilgi Sistemi İş Süreçleri Analizi (İdare'nin yaklaşık 500 adet sürecinin tanımlanması)" şeklinde belirtilen cümlede bahsi geçen yaklaşık ifadesine ek olarak süreç kavramının teknik olarak nasıl yapılacağından hiçbir şekilde bahsedilmediği,

5) Sözleşme Tasarısı'nın 15'inci maddesinde ihale konusu hizmetin tamamının veya bir kısmının alt yükleniciye yaptırılmayacağına ilişkin düzenleme yapıldığı, Teknik Şartname'nin 3.9'uncu maddesinin söz konusu düzenlemeye aykırı olduğu,

6) İdari Şartname’de TSE 13298/T1 belgesinin yeterlik kriteri olarak belirlendiği, bu belgeye sahip olanlar göz önüne alındığında ve bu şirketlerin çözümleri, hizmetleri ve referansları değerlendirildiğinde İdari Şartname’nin 7.6’ncı maddesinde istenilen iş deneyim içerisinde sadece bir şirketin bulunduğu, bu durumun rekabet ortamının oluşmasına engel olduğu, benzer işe sahip olan şirketin TSE 13298/T1 belgesinin geçerlilik süresinin 06.09.2018 olduğu, şikayete konu işin süresi göz önüne alındığında iş bitim tarihinde belgenin geçerliliğinin kalmayacağı, söz konusu belgenin teklif aşamasında değil, proje sonunda idareye teslim edilmesinin projenin başarıya ulaşmasına katkı sağlayacağı ve rekabet ortamının sağlanmasına katkı sağlayacağı,

7) a- Teknik Şartname’nin 3.5’inci maddesi ile 3.6’ncı maddelerinin birbiri ile tutarsız olduğu, Teknik Şartname’nin 3.6’ncı maddesinde bakım sürecinin başlangıç tarihi olarak proje süresinin bitişi ifade edildiği, fakat anılan Şartname’nin 3.5’inci maddesinde yer alan garanti şartları göz önüne alındığında bakım süresinin başlangıcı proje süresinin sonunda başlaması gerektiği,

b- Teknik Şartname’nin 3.6’ncı maddesinde ihale bedelinin %18’ini aşmayacak şekilde bakım sözleşmesi imzalanacağı belirtilmiş, aynı cümlede bakım tutarında personel hariç ibaresinin bulunduğu, söz konusu ihalenin götürü bedel usulü ile yapılması yani maliyet detaylarının (lisans, personel, çözüm, hizmet vb.) belli olmaması alınacak olan bedelin içerisinde personel maliyetlerini de barındıracağı, bunun kamu zararı doğuracağı, bu nedenle personel hariç ibaresi yerine personel dahil ibaresinin konulması gerektiği ya da işin birim fiyat teklif usulü ile yeniden ihale edilmesi gerektiği,

c- Teknik Şartname’nin 3.6’ncı maddesinde çerçevesinde işin süresinin ve iş artışı oranlarının tespit edilmesinin Kamu İhale Kanunu’na aykırı olduğu, böyle bir iş artışının yüklenicinin haksız kazanç elde etmesine sebebiyet vereceği, kamu zararına yol açacağı,

8) Teknik Şartname’nin 3.5’inci maddesinde belirtilen garanti hükümlerin belirtildiği ancak Sözleşme Tasarısı’nın 34’üncü maddesinde garanti hükümlerine yer verilmediği,

9) Teknik Şartname’nin 9.19’uncu ve 14.2.5’inci maddelerinde istenilen belgelerin İdari Şartname’nin 7’nci maddesinde belirtilmediği,

10) Teknik Şartname ile İdari Şartname arasında tezatlıklar bulunduğu,

11) Teknik Şartname ile Sözleşme Tasarısı’nda yer alan cezai yaptırımların birbiri ile uyumlu olmadığı, Sözleşme Tasarısı’nın 16.1.1’inci maddesinde yer alan “1- Sözleşme hükümlerinin tamamı yerine getirilmediği takdirde % 0,05 oranında gecikme cezası uygulanır...” ibaresindeki “tamamı” kelimesi yerine “her birini” ibaresinin yer alması gerektiği, ihale dokümanında işin tekrar eden

kısımlarının sözleşmeye uygun olarak gerçekleştirilmemesi hâlinde idarece her bir aykırılık için ayrı ayrı uygulanmak üzere kesilecek ceza miktarının belirlendiği, ancak bu aykırılıkların ardı ardına veya aralıklı olarak gerçekleştirilmek suretiyle belli bir sayıya ulaşması durumunda sözleşmenin feshedileceği hususunda bir belirleme yapılmadığı, söz konusu düzenlemelerin 4735 sayılı Kamu İhale Kanunu'nda yer alan emredici hükümlere aykırı olduğu,

12) Şikayete konu ihaleye ait Teknik Şartname'nin Darıca Belediye Başkanlığı ve Beykoz Belediye Başkanlığı tarafından gerçekleştirilen benzer işe ait ihalelerin teknik şartnameleri ile birebir benzerlik taşıdığı, ihaleye ait şartnamelerin idarelerce hazırlanmasının Kamu İhale Kanunu'nun 12'inci maddesinde hüküm altına alındığı, şikayete konu ihalenin Teknik Şartnamesi'nin Darıca Belediye Başkanlığı ve Beykoz Belediye Başkanlığı'nın benzer ihalelerini kazanan şirketin kazanmasına yönelik olarak hazırlandığı,

13) Söz konusu ihale kapsamında alımı düşünülen otomasyon sisteminin 6698 sayılı Kişisel Verilerin Korunması Kanunu'na uygun olarak çalışması gerektiği iddialarına yer verilmiştir.

A) Başvuru sahibinin iddialarının değerlendirilmesi sonucunda aşağıdaki hususlar tespit edilmiştir.

1) Başvuru sahibinin 1'inci ve 6'ncı iddialarına ilişkin olarak:

4734 sayılı Kamu İhale Kanunu'nun 54'üncü maddesinin birinci fıkrasında "İhale sürecindeki hukuka aykırı işlem veya eylemler nedeniyle bir hak kaybına veya zarara uğradığını veya zarara uğramasının muhtemel olduğunu iddia eden aday veya istekli ile istekli olabilecekler, bu Kanunda belirtilen şekil ve usul kurallarına uygun olmak şartıyla şikâyet ve itirazın şikâyet başvurusunda bulunabilirler." hükmü,

4734 Sayılı Kamu İhale Kanunu'nun "İdareye şikâyet başvurusu" başlıklı 55'inci maddesinde "Şikâyet başvurusu, ihale sürecindeki işlem veya eylemlerin hukuka aykırılığı iddiasıyla bu işlem veya eylemlerin farkına varıldığı veya farkına varılmış olması gereken tarihi izleyen günden itibaren 21 inci maddenin (b) ve (c) bentlerine göre yapılan ihalelerde beş gün, diğer hallerde ise on gün içinde ve sözleşmenin imzalanmasından önce, ihaleyi yapan idareye yapılır. İlanda yer alan hususlara yönelik başvuruların süresi ilk ilan tarihinden, ön yeterlik veya ihale dokümanının ilana yansımaya diğer hükümlerine yönelik başvuruların süresi ise dokümanın satın alındığı tarihte başlar.

İlan, ön yeterlik veya ihale dokümanına ilişkin şikâyetler birinci fıkradaki süreleri aşmamak üzere en geç ihale veya son başvuru tarihinden üç iş günü öncesine kadar yapılabilir. Bu yöndeki başvuruların idarelerce ihale veya son başvuru tarihinden önce sonuçlandırılması esastır..." hükmü,

İhalelere Yönelik Başvurular Hakkında Yönetmelik'in "Başvuru Süreleri" başlıklı 6'ncı maddesinde "(1) İdareye şikayet süresi; ihale sürecindeki şikayete konu işlem veya eylemlerin farkına varıldığı veya farkına varılmış olması gerektiği tarihi izleyen günden itibaren Kanunun 21 inci maddesinin birinci fıkrasının (b) ve (c) bentlerine göre yapılan ihalelere yönelik başvurularda beş gün, diğer hallerde on gündür.

(2) Ancak, ilan ile ön yeterlik veya ihale dokümanına yönelik şikayetler, birinci fıkradaki süreleri aşmamak kaydıyla başvuru veya teklif sunulmadan önce en geç ihale veya son başvuru tarihinden üç iş günü öncesine kadar yapılabilir." hükmü yer almaktadır.

09.02.2018 tarihli İhale İlanı'nın "İhaleye katılabilme şartları ve istenilen belgeler ile yeterlik değerlendirmesinde uygulanacak kriterler" başlıklı 4'üncü maddesinde "4.1. İhaleye katılma şartları ve istenilen belgeler:

4.1.1.3. İhale konusu işin yerine getirilmesi için alınması zorunlu olan ve ilgili mevzuatında o iş için özel olarak düzenlenen sicil, izin, ruhsat vb. belgeler,

1-TSE 13298/T1 (18.02.2016)

...

4.4. Bu ihalede benzer iş olarak kabul edilecek işler:

4.4.1. Kamuda ve/veya özel sektörde süreç bazlı web tabanlı yönetim bilgi sistemi yazılım modülleri ve elektronik belge yönetim sistemi hizmet işini yapmış olmak" düzenlemesi bulunmaktadır.

Yapılan inceleme sonucunda, başvuru sahibinin söz konusu iddialarının ihale dokümanının ilana yansıyan hükümlerine ilişkin olduğu ve bu işleme karşı 05.03.2018 tarihinde idareye şikayet başvurusunda bulunduğu, şikayetçinin şikayet konusu işlemi fark etmesi veya öğrenmesi gereken tarih olan 09.02.2018 tarihini (ihale ilan tarihi) izleyen 10 (on) gün içinde 19.02.2018 tarihine kadar idareye şikayet başvurusunda bulunması gerekirken, bu süreyi geçirdikten sonra şikayet başvurusunda bulunduğu anlaşılmıştır. Bu nedenle başvuru sahibinin 1'inci ve 6'ncı iddialarının süre yönünden reddedilmesi gerektiği sonucuna varılmıştır.

2) Başvuru sahibinin 2'nci iddiasına ilişkin olarak:

İdari Şartname'nin "İhale dokümanının kapsamı" başlıklı 5'inci maddesinde "5.1. İhale dokümanı aşağıdaki belgelerden oluşmaktadır:

a) İdari Şartname.

b) Teknik Şartname.

c) Sözleşme Tasarısı.

ç) Hizmet İşleri Genel Şartnamesi (İhale dokümanı kapsamında verilmemiştir.)

d) Standart formlar:

Standart Form-KİK015.2/H: Götürü Bedel Teklif Mektubu, Standart Form-KİK022.0/H: İş Ortaklığı Beyannamesi, Standart Form-KİK024.1/H: Geçici Teminat Mektubu, Standart Form-KİK024.2/H: Kesin Teminat Mektubu, Standart Form-KİK026.1/H: İş Bitirme Belgesi, Standart Form-KİK026.2/H: Alt yüklenici İş Bitirme Belgesi, Standart Form-KİK027.0/H: Ortaklık Durum Belgesi, Standart Form-KİK025.1/H: Bilanço Bilgileri Tablosu

e) 1- TSE 13298/T1 (18.02.2016)

2- Kadıköy Belediyesi ölçeğinde en az 3 belediyede iş süreçlerini de kapsayan bir sistemi kurmuş, çalışır vaziyette teslim etmiş ve destek vermiş olduğuna dair referans belgeleri

3- TUBİTAK Kamu Sertifikasyon Merkezi tarafından verilen E-İmza uyum değerlendirme raporu

4- VTYS'nin (Veri Tabanı Yönetim Sistemi)Türkiye'deki ana dağıtıcı firma statüsündeki şirketten bu ihaleye özel yetki belgesi

5- İş Zekası Uygulamasının Türkiye'deki ana dağıtıcı firma statüsündeki şirketten bu ihaleye özel yetki belgesi" düzenlemesi,

Aynı Şartname'nin "İhaleye katılabilmek için gereken belgeler ve yeterlik kriterleri" başlıklı 7'nci maddesinde "7.1. İsteklilerin ihaleye katılabilmeleri için aşağıda sayılan belgeleri teklifleri kapsamında sunmaları gerekir:

...

h) 1-TSE 13298/T1 (18.02.2016)

2-Kadıköy Belediyesi ölçeğinde en az 3 belediyede iş süreçlerini de kapsayan bir sistemi kurmuş, çalışır vaziyette teslim etmiş ve destek vermiş olduğuna dair referans belgeleri

3- TUBİTAK Kamu Sertifikasyon Merkezi tarafından verilen E-İmza uyum değerlendirme raporu

4- VTYS'ninü (Veri Tabanı Yönetim Sistemi)Türkiye'deki ana dağıtıcı firma statüsündeki şirketten bu ihaleye özel yetki belgesi

5-İş Zekası Uygulamasının Türkiye'deki ana dağıtıcı firma statüsündeki şirketten bu ihaleye özel yetki belgesi" düzenlemesi,

Teknik Şartname'nin "İşin Konusu ve Amaç" başlıklı 1'inci maddesinde "T.C. Kadıköy Belediyesi'nin 2015-2019 Stratejik Planında belirtilen stratejik amaçlarından birisi de, "Kurumumuz ve kentimiz için eşitlikçi, iletişimi güçlü, insan kaynakları ve eğitim politikasını belirlemiş, kaynaklarını ve iş süreçlerini iç kontrol sistemine göre yöneten, iş güvenliği standartlarına uygun hizmet veren, yenilikçi, teknolojik sistemlerle desteklenen, çağdaş ve sürdürülebilir kurumsal yapıya ulaşmak" olarak belirlenmiştir.

Bu kapsamda, Belediyenin ihtiyacı olan, iş süreçleri bazlı, web tabanlı ve Elektronik Belge Yönetim Sistemi ve dijital arşivle bütünleşik bir yapıda çalışacak, Coğrafi Bilgi Sistemi ile entegre bir Yönetim Bilgi Sisteminin oluşturulması amaçlanmaktadır.

Alımı yapılacak bu hizmetle birlikte, bütün iş süreçlerinin analiz edilip sisteme aktarılması ve takibi; veri kayıtlarının yönetimi; analiz ve raporlamaların da yapılacağı web tabanlı yazılım modüllerinin kurulması; tüm dijital birim arşivleriyle entegrasyonun sağlanması ve EBYS ile süreç yönetimine eklenmesi; anlık analiz ve raporlamalarla, performans ölçümünün sağlanması için Yönetim Bilgi Sistemi ile bütünleşik çalışan bir iş zekası uygulamasının kurulması sağlanacaktır." düzenlemesi,

Aynı Şartname'nin "Yüklenici'nin Yükümlülükleri" başlıklı 9'uncu maddesinde "9.24. Yüklenici, işin öngörülen sürede yapılması için gerekli olan iş gücü ve insan kaynakları planlamasını yapacak ve İdare'ye bir proje yöneticisi atayacaktır. Yüklenici, söz konusu uzman proje yöneticisi dahil olmak üzere, en az 5 (beş) kişiden oluşan bir proje analiz ve destek ekibi teşkil edecek ve bu ekibi Proje Süresi boyunca İdare'de görevlendirecektir. Yüklenici, bu ekibin sağlayacağı hizmetler de dahil olmak üzere, diğer hizmetlerinde, geliştirme, kurulum, güncelleme, uyarlama ve uygulama faaliyetlerinde kendi iş gücü ve insan kaynaklarını kullanacaktır. İdare Yüklenici'nin bu Şartname'ye konu iş için görevlendirdiği personeli herhangi bir gerekçe belirtmeden değiştirme talebinde bulunduğu; Yüklenici bu değişiklik talebini en geç 3 (üç) iş günü içerisinde yerine getirecektir. Yüklenici İdare'nin onayı olmadan iş için görevlendirdiği herhangi bir personeli geri çekemez veya başka bir projede görevlendiremez. Böyle bir durumda, bu durumun yaşandığı tarihten itibaren ihalede teklif edilen bedelin % 1'i (yüzde bir) oranında günlük para cezası kesilecektir. Yüklenici ayrıca İdare tarafından teşkil edilecek ilave bir analiz ve destek ekibinin yönetimini ve eğitimini de üstlenecektir." düzenlemesi,

Anılan Şartname'nin "Entegre İş Zekası Uygulaması (BI) ve İş Zekası Veri Tabanı Modeli (Datamart) Teknik Özellikleri" başlıklı 20'nci maddesinde "İdaremiz iş süreçlerinde tıkanan noktaların tespiti, kurum-birim-personel bazında performansın ölçülmesi, süreçlerin iyileştirilmesi vb. işlemlerinin yapılmasına dayanak teşkil eden kurumsal analiz ve raporların, üst yönetici ve kullanıcı analizlerinin

iş zekası ile hazırlanmasını amaçlamaktadır. Bu amaçla, yeni kurulacak Süreç Bazlı Web Tabanlı Yönetim Bilgi Sistemi ve bütünleşik Elektronik Bilgi Belge Arşiv Yönetim Sistemi, süreçlerde karar destek bilgilerinin ve faaliyetlerin anlık izlenmesini sağlayan, gerekli dinamik raporlamaları yapabilecek, tam bütünleşik bir İş Zekası Uygulaması ve İş Zekası Veri Tabanı Modeline (Datamart) sahip olmalıdır.” düzenlemesi,

Anılan Şartname'nin “İş Zekası Uygulaması Genel Özellikleri” başlıklı 20.1'inci maddesinde “20.1.3. En az 50 (elli) kullanıcı olmalıdır.” düzenlemesi yer almaktadır.

Yukarıda yer verilen ihale dokümanı düzenlemeleri incelendiğinde, ihale konusu iş kapsamında iş zekası uygulaması alımının da bulunduğu, başvuru sahibinin iddiasında yer verilen 4.4.1'inci maddesinin Teknik Şartname'de yer almadığı, Teknik Şartname'nin 9.24'üncü maddesinde idarenin kendi personelinden bahsedilmediği, projenin yürütülmesinde görev alacak biri proje yöneticisi olmak üzere en az beş kişiden oluşan proje analiz ve destek ekibi olan yüklenici personelinden bahsedildiği, iş zekası uygulama modülünün kullanıcı sayısının Teknik Şartname'nin 20.1'inci maddesinde belirlendiği, ihale dokümanında yer alan düzenlemeler dikkate alındığında isteklilerce maliyet hesaplaması yapılmasının mümkün olduğu, söz konusu düzenlemelerin tekliflerin oluşturulmasını engeller nitelikte olmadığı anlaşıldığından başvuru sahibinin iddiasının yerinde olmadığı sonucuna varılmıştır.

3) Başvuru sahibinin 3'üncü iddiasına ilişkin olarak:

4734 sayılı Kamu İhale Kanunu'nun “Temel ilkeler” başlıklı 5'inci maddesinde “İdareler, bu Kanuna göre yapılacak ihalelerde; saydamlığı, rekabeti, eşit muameleyi, güvenilirliği, gizliliği, kamuoyu denetimini, ihtiyaçların uygun şartlarla ve zamanında karşılanmasını ve kaynakların verimli kullanılmasını sağlamakla sorumludur.” hükmü,

Aynı Kanun'un “Şartnameler” başlıklı 12'nci maddesinde “... İhale konusu mal veya hizmet alımları ile yapım işlerinin teknik kriterlerine ihale dokümanının bir parçası olan teknik şartnamelerde yer verilir. Belirlenecek teknik kriterler, verimliliği ve fonksiyonelliği sağlamaya yönelik olacak, rekabeti engelleyici hususlar içermeyecek ve bütün istekliler için fırsat eşitliği sağlayacaktır.

Teknik şartnamelerde, varsa ulusal ve/veya uluslararası teknik standartlara uygunluğu sağlamaya yönelik düzenlemeler de yapılır. Bu şartnamelerde teknik özelliklere ve tanımlamalara yer verilir. Belli bir marka, model, patent, menşei, kaynak veya ürün belirtilemez ve belirli bir marka veya modele yönelik özellik ve tanımlamalara yer verilmeyecektir.

Ancak, ulusal ve/veya uluslararası teknik standartların bulunmaması veya teknik özelliklerin belirlenmesinin mümkün olmaması hallerinde "veya dengi" ifadesine yer verilmek şartıyla marka veya model belirtilebilir." hükmü,

Teknik Şartname'nin "Süreç Bazlı Web Tabanlı Yönetim Bilgi Sistemi ve Elektronik Bilgi Belge Arşiv Yönetim Sistemi Veri Tabanı Yönetim Sistemi (Vtys) Özellikleri" başlıklı 18'inci maddesinde "Yeni kurulacak, tam bütünleşik Süreç Bazlı Web Tabanlı Yönetim Bilgi Sistemi ve Elektronik Bilgi Belge Arşiv Yönetim Sistemi, İdare'de tek ve ana bir ilişkisel Veri Tabanı Yönetim Sistemi (VTYS) üzerinde çalışacaktır.

İdare'nin mevcut otomasyon verileri halihazırda Oracle veri tabanı üzerinde tutulmaktadır. İdareimiz tarafından yeni Sistem'e veri aktarımının, aynı altyapıya sahip kurumsal bir veri tabanı yönetim sistemiyle yapılması talep edilmektedir.

18.1. İstekliler, mevcut veri tabanı ile uyum, yedekleme kurgusu, felaket kurtarma altyapısı ve sürdürülebilir çalışmayı dikkate alarak, Sistem'de kullanılacak Veri Tabanı Yönetim Sistemini (VTYS), en az 4 (Dört) CPU Lisanslı Oracle Enterprise Edition olarak teklif edecektir. Core sayısı en az 4 olmalıdır.

18.2. İstekli, teklif ettiği VTYS'nin Türkiye'deki ana dağıtıcı firma statüsündeki şirketten bu ihaleye özel yetki belgesi alacak ve teklifiyle birlikte İdare'ye sunacaktır." düzenlemesi,

Aynı Şartname'nin "Entegre İçerik Yönetim Sistemi Genel Özellikleri" başlıklı 19.5'inci maddesinde "19.5.2. Oracle ve Microsoft SQL veritabanları üzerinde çalışabilir nitelikte olmalıdır." düzenlemesi,

Anılan Şartname'nin "İş Zekası Uygulaması Genel Özellikleri" başlıklı 20.1'inci maddesinde "20.1.2. Oracle veri tabanı üzerinde çalışmalıdır." düzenlemesi bulunmaktadır.

Yukarıda yer verilen Teknik Şartname'nin ilgili düzenlemelerinden idare tarafından ihale konusu iş kapsamında Oracle marka Enterprise Edition model "Veri Tabanı Yönetim Sistemi" lisansının talep edildiği, idareye özel oluşturulacak yazılım olarak da "Entegre İçerik Yönetim Sistemi", "Entegre İş Zekası Uygulaması (BI)", "Web Tabanlı Yönetim Bilgi Sistemi" ve "Elektronik Bilgi Belge Arşiv Yönetim Sistemi" yazılımlarının alımının gerçekleştirilmesinin planlandığı, söz konusu bu yazılımların Oracle marka veri tabanı yönetim sistemi ile uyumlu olmasının şart koşulduğu görülmektedir.

Söz konusu iddialara ilişkin Kurum tarafından ihaleyi gerçekleştiren idareye gönderilen 16.04.2018 tarihli yazıda "... Yapılan incelemede, ek olarak aşağıda belirtilen bilgi ve belgelere de ihtiyaç duyulmuştur:

1) Teknik Şartname'nin 18.1'inci maddesinde veri tabanı yönetim sisteminin (VTYS) en az 4 (Dört) CPU Lisanslı Oracle Enterprise Edition olarak talep edilmesinin ihale konusu iş için bir zorunluluk olup olmadığına ilişkin dayanakları ile birlikte teknik açıklaması,

2) Teknik Şartname gereğince talep edilen Oracle Enterprise Edition'ın alternatif marka ve modellerinin bulunup bulunmadığı, alternatifleri bulunuyor ise isimleri ve idarenizce ihale konusu iş kapsamında tercih edilmeme gerekçeleri, bu çerçevede ihale konusu hizmet ile alınacak veri tabanı yönetim sisteminin idarenizin mevcut sistemi ile entegrasyonunun alternatif marka ve modellerle mümkün olup olmadığı konusunda teknik açıklama," ifadelerine yer verilerek açıklama talep edilmiştir.

İdare tarafından Kurum'a gönderilen 08.05.2018 tarihli yazıda "1) Teknik Şartname'nin 18.1'inci maddesinde veri tabanı yönetim sisteminin en az 4 CPU Lisanslı Oracle Enterprise Edition olarak talep edilmesinin ihale konusu iş için bir zorunluluk olup olmadığına ilişkin dayanakları ile birlikte teknik açıklaması.

24.04.2018 Tarihli Açıklama:

İhale konusu iş için idaremizdeki donanım altyapısına (sunucu, disk ve ağ bileşenleriyle birlikte) ve bu altyapının veri tabanı güvenliği, performans, yedeklilik, felaket kurtarma ve iş sürekliliğini hedefleyerek geliştirilmesine yönelik bir veri tabanı yönetim sistemi kullanımı öngörülmüştür. Hedeflenen web tabanlı, süreç bazlı otomasyon sistemi, elektronik yönetim esaslı olacağından tüm verileri tek bir ilişkisel veri tabanında yönetmek ve kurumsal bir veri tabanı platformu oluşturmak durumundadır.

Sistemde felaket kurtarma senaryosu olması gerekliliğinden dolayı, aktif-aktif (canlı) veri tabanından felaket kurtarma (Disaster) veri tabanına sürekli eşitleme yapılacaktır. Aktif - aktif (canlı veritabanı) kurgusunda, bu sunucular üzerinde kurulacak olan veri tabanının sistem gereksinimleri canlı ortamdaki 2 CPU lisanslı veri tabanı ile aynı olacağından en az 2 CPU lisanslı veritabanı da aktif veritabanı için düşünülüp toplamda en az 4 CPU lisanslı Oracle Enterprise Edition talep edilmiştir.

Zorunluluk nedeni, aynı anda 2 veya daha fazla ayrıık sunucuda tek veritabanı olarak çalıştırmak istediğimiz kurgu için Oracle Enterprise Edition dışında başka bir veritabanında bu alternatif bulunmamasıdır.

Ek Teknik Açıklamalar:

İdarenin mevcut yapıda kullandığı tüm sistemlerin verileri Oracle veritabanında tutulmaktadır. İdaremiz tarafından bütünleşik sisteme veri aktarımının aynı altyapıya sahip kurumsal bir veritabanı

yönetim sistemiyle yapılması, performans, hız ve güvenlik açısından ihale konusu iş için çok önemli bir gerekliliktir.

İdaremiz belediye binası ve dış birimler olmak üzere yüzlerce çalışanın kullanımına açılmış, tam bütünleşik olmayan sistemlerle ve yazılım parçalarıyla vatandaşımıza hizmet vermektedir. Bu bağlamda vatandaşlarımızın verilerinin güvenliğini, sürdürülebilirliğini, işlerliğini ve korunmasını sağlamak bir kamu kurumu olarak öncelikli önem alanımıza girmektedir.

İş bu ki, 4 Ocak 2017 tarihinde Elektronik Belge Yönetim Sistemimizin veritabanında yanlış yapılan bir çalışma sonucunda idaremiz evrak/veri kaybına uğramıştır. Yaşanan bu kötü tecrübenin ardından insan faktörü hatasını minimize eden hatta sıfıra indirgeyen bir veritabanı çözümüne ihtiyacımızın olduğu sonucuna varılmıştır. Mevcut sistemimizde kullandığımız veritabanı olan Oracle Standart Edition yerine, Oracle Enterprise Edition versiyonuna sahip olunması durumunda, teknik olarak, yaşanmış olan bu veri kaybının önüne geçilebilmesinin mümkün olduğu tespit edilmiş ve sözkonusu ihale için Oracle Enterprise Edition versiyonunun talep edilmesi tercih edilmiştir.

Bunun yanında veri kaybı risk faktörünü azaltmak için, güçlü bir yedekleme ve felaket kurtarma senaryomuz olması gerekmektedir. Şöyle ki, felaket kurtarma senaryosunun kurgulanması için İdaremiz iki ayrı veritabanı temin etmelidir. Bu veritabanları İdarenin isteğine göre paralel ve eşzamanlı aktif kalabilmeli veya biri aktif (canlı) diğeri pasif (disaster) kurgulanabilmelidir.

Pasif kalacak veritabanı canlı ortamdaki veri tabanının anlık olarak eşitleme yapacağı veri tabanıdır. Bu veri tabanı pasif olarak duracaktır ve herhangi bir felaket durumunda (yangın, deprem, sel felaketi, vb.) canlı ortamdaki veri tabanının bozulması sonucunda ya da iş göremez duruma gelmesi halinde, hemen aksiyon alınıp pasif durumda olan disaster veritabanı aktif hale getirilebilecektir. Bu durumda veri kaybını önlemekle beraber, veritabanı kaynaklı olabilecek sistemin canlı çalışmasındaki kesintiler de minimum seviyeye indirilecek ya da ortadan kaldırılacaktır.

Oracle Enterprise Edition dışındaki veri tabanı versiyonlarında, felaket senaryosu gerçekleştiğinde, örneğin bir tabloda sorun çıktığında - kayıtların yanlışlıkla silinmesi, tablonun yanlışlıkla drop edilmesi vb. gibi - eğer hala vakit varsa, UNDO'dan FLASHBACK ile dönmeye çalışılırken, bunun olmadığı durumlarda da full veritabanı restore'undan sonra tablo export-import etmek dışında pek fazla bir seçenek bulunmamaktadır. Bu da kesintiye ve ciddi bir zaman kaybına sebep olabilmektedir.

Oracle Enterprise Edition ile birlikte full veri tabanı restore'u yapmadan tabloları restore etmek mümkün olmaktadır. Full veritabanı restore'u için geçen zaman, destek hizmeti ve kaynak ihtiyacı düşünüldüğünde tercihimiz önemli bir gereklilik olarak karşımıza çıkmaktadır.

Bu ve benzer felaket durumlarına karşı her veri tabanı yönetim sistemi (Oracle, SQL Server, MySQL, vb.) bir felaket kurtarma çözümü ortaya koymaktadır. Ancak, iki ayrı veritabanının da (ana ve yedek) aktif aktif çalışmasını sağlayacak kullanım özelliği sadece Oracle Enterprise Edition sürümünde mevcuttur.

Böylece ana veritabanında herhangi bir sıkıntı yaşandığı anda hızlıca yedek veri tabanından devam edilebilmektedir. Bunu Oracle Enterprise Edition'ın Active Dataguard özelliği sağlamaktadır. Burada Dataguard'ın en önemli rollerinden birisi ana veritabanının sadece bir yedek veritabanını oluşturması değil, aynı zamanda canlı verilerle yedeği beslediği için oluşturulan konfigürasyona göre anlık yedeğini oluşturmasıdır.

Oracle Enterprise Edition versiyonunun geliştirilmiş güvenlik opsiyonlarının yanı sıra, aynı anda iki ayrı sunucudan erişilen tek veritabanı olarak çalıştırabilmek isteyeceğimiz senaryo için, Oracle Enterprise Edition dışında başka hiçbir veritabanında alternatif bulunmamaktadır.

Günlük iş/veri yoğunluğunu yük dağılımı (load balancing) ile sistemdeki diğer sunuculara (standby nodes) paylaştırarak veri tabanı ve uygulamanın iş katmanlarının performansı en üst seviyede tutulacaktır. Böylece hem online veri yedekliliği, hem de sistemdeki sunucuların tekil arızalanması durumunda standby sunucuların devreye girmesi sağlanmış olacak, vatandaşlarımıza kesintisiz hizmet vermemiz mümkün olacaktır. Bu yapıyı sağlamak için, idaremizdeki mevcut sunucu altyapısının dataya erişen, eş zamanlı çalışan node'unda ve veri güvenliği ile yedekleme yönetimi için diğer node'unda veri tabanı yönetim sistemi yazılımlarının kurulu olması gerekmektedir.

Oracle veri tabanlarının yukarıda belirtilen konfigürasyona uygun kurulumu ve devamında verimli çalışabilmesi için, Oracle kendi yayınladığı dokümanlarda (whitepaper) ihtiyaç duyulan minimum CPU değerini 2 olarak belirtmektedir. Bunun istenmesindeki en büyük neden olarak da multiprocess çalışma ve bu proses'lerin eş zamanlı çalışması için olanak sağlanması olduğu belirtilmektedir. Ana sunucunun bir yedeği olarak kurgulanacak Standby sunucu, ana sunucunun devre dışı kalması durumunda anlık çalışmaya başlayacaktır. Bunun için her iki sunucu (node) arasında aktif-aktif kurgusu yapılması gerekecektir. Canlı sistemin aktif-aktif özelliğiyle çalışabilmesi için veri tabanı lisansının minimum 2 CPU olması bir zorunluluktur ve ayrıca performans için de çok önemli bir gerekliliktir.

Sistemde ana ve standby sunucuların fiziksel konumu dışında bir felaket kurtarma altyapısı (Disaster) ve senaryosu olması gerekliliğinden dolayı, aktif-aktif (canlı) veri tabanından pasif (Disaster) veri tabanına sürekli eşitleme yapılacaktır.

Aktif (Canlı)/Pasif (Disaster) kurgusunda, pasif taraftaki sunucuların üzerinde kurulacak olan veri tabanının sistem gereksinimlerinin canlı ortamdaki 2 CPU lisanslı veri tabanı ile aynı olması gerektiğinden, en az 2 CPU lisanslı veritabanı da pasif veritabanı için düşünölmelidir. Böylece toplamda en az 4 CPU lisanslı Oracle Enterprise Edition talep edilmiştir.

Enterprise Edition sürümünün talep edilmesinin bir diğör nedeni, veri tabanının kayıtlı olduđu disk alanlarının (storage) sağlıklı ve güvenli yönetimidir. Kayıt, yedekleme ve sürekli büyüme disk alanlarının etkin yönetimini gerektirmektedir (partitioning). Veri tabanına bağılı disk alanı yönetimi (partitioning) özellikleri kurumsal sürüm olan Enterprise Edition'da bulunmaktadır.

2) Teknik Şartname gereğince talep edilen Oracle Enterprise Edition'ın alternatif marka ve modellerinin bulunup bulunmadığı, alternatifleri bulunuyor ise isimleri ve idarenizce ihale konusu iş kapsamında tercih edilmeme gerekçeleri, bu çerçevede ihale konusu hizmet ile alınacak veri tabanı yönetim sisteminin idarenizin mevcut sistemi ile entegrasyonunun alternatif marka ve modellerle mümkün olup olmadığı konusunda teknik açıklama.

24.04.2018 Tarihli Açıklama:

Oracle Enterprise Edition'a alternatif marka model olarak, PostgreSQL, EnterpriseDB ve MS SQL Server ihtiyacı karşılayabilecek nitelikleri taşıyabilmektedir. Oracle Linux Server işletim sistemi sürümünün üretildiğı Redhat EnterpriseDB de sorunsuz çalışabilmektedir. Ancak, yaygınlığı ve desteğı açısından idare olarak Oracle veri tabanı yönetim sistemini talep etmekteyiz. Bilindiğı üzere e-devlet uygulamasında ve Bakanlıklarda Oracle Enterprise Edition tercih edilmektedir. PostgreSQL EnterpriseDB'nin yaygın desteğı ve modifikasyon garantisi bulunmamaktadır.

Bu projede fazladan maliyet ortaya çıkarmamak ve mevcut kaynakları etkin kullanmak için donanım altyapısı alımı düşünölmemiştir. İdaremizin mevcut sisteminde halihazırda Oracle veri tabanı kullanılmakta olup, sunucu altyapımız da dikkate alındığında, bu alternatif marka ve modellerle entegrasyon ek donanım, işletim sistemi, uzman personel ve eğitim maliyeti doğuracağından, entegrasyonun mümkünlüğü oldukça maliyetli olmaktadır.

Ek Teknik Açıklamalar:

Yaygın olarak kullanılan veri tabanı yönetim sistemlerinden MS Access, MySQL, Postgre SQL, Oracle Standart Edition ve Oracle Standart Edition One küçük ölçekli uygulamalardaki gereksinimleri

karşılatabilecek niteliktedir. Tek bir veri tabanı tablosunda depolanabilen veri boyutları ihtiyacımızı karşılamamaktadır. Ayrıca kurumsal sürümleri olmadığından, idaremiz tarafından talep edilen Oracle Enterprise Edition'a alternatif değillerdir.

Oracle Enterprise Edition'a alternatif olabilecek marka ve modeller olarak PostareSQL Enterprise DB, MS SQL Server, Oracle Linux Server işletim sistemi sürümünün üretildiği Redhat Enterprise DB ihtiyacı karşılayabilecek nitelikleri taşıyabilmektedir.

Postgre SQL ve Redhat Enterprise DB açık kaynak kodlu veri tabanı yönetim sistemleri olup, Türkiye'de yerleşik, yaygın satış ve destek ağı bulunmamaktadır. Çözüm geliştirme, modifikasyonlar ve olası teknik problemlerde ihtiyaç duyulabilecek destek hizmetleri maliyetlerinin öngörülemez olması idaremizce risk faktörü olarak değerlendirilmiştir.

MS SQL Server, orta ve büyük ölçekli bir veri tabanı yönetim sistemidir ancak sadece MS Windows işletim sistemleri üzerinde çalışmaktadır. Mevcut sunucu altyapımız Unix/Linux işletim sistemi tabanlı IBM AIX POWER 7.0'dır. Bu projede fazladan maliyet ortaya çıkarmamak ve mevcut kaynakları etkin kullanmak için donanım altyapısı alımı düşünülmemiştir.

İdaremizin halihazırda, mevcut altyapıda kullandığı tüm sistemlerin verileri Oracle veritabanında tutulmaktadır,

Talep edilen, ihale konusu yazılım sisteminin arayüzleri, analiz ve raporlamaları, web ortamından bilgi/hizmet sunma işlemleri, iş zekası uygulamaları, sahadan online veri alma/işleme prosesleri, e-devlet uygulamaları, entegrasyonlar, mobil uygulamalar ve diğer bileşenler dikkate alındığında, böyle bir sistemin altyapısında, kamuda yaygın kullanılan, performansı ve yeteneği tescil edilmiş, kurumsal ve çok güçlü bir ilişkisel veri tabanı yönetim sistemi olması gerekmektedir.

İdaremiz bilgi İşlem biriminde, mevcut sistemimizde kullanılan Oracle veri tabanı konusunda deneyimli çalışanlar bulunmaktadır. Veri tabanı yönetiminin sağlıklı bir şekilde sürdürülebilmesi, yeni uygulamaların devreye alınması, güncellemeler, çıkan sorunlara anında müdahale edilmesi, kayıpsız ve hızlı çözüm üretilmesi açısından bu çalışanlar kilit konumdadır. Ayrıca ihale konusu iş kapsamında geliştirilecek yeni otomasyon sistemiyle birlikte idaremizde mevcut veri tabanı sisteminin kurumsal sürümüne geçilmesi hedeflenmektedir. Böylece söz konusu deneyimli çalışanlar, veri aktarımı, kontroller, denetim ve geliştirmeler, modüllerin veri altyapısı, veri tabanı tablo ve alanları konusundaki bilgi ve deneyimlerini kullanacaktır.

Başka bir veri tabanı yönetim sisteminin mevcut sisteme ve/veya ihale konusu iş kapsamında talep edilen yeni otomasyon sistemine entegrasyonu, ek lisans, ilave personel ve/veya eğitim maliyeti doğurmasının yanı sıra, proje ve deneyim için uzun süreler gerektirecektir.

Bu durumda, kamuda yaygın kullanılan Oracle veri tabanı ürünlerinin versiyonlarını karşılaştırdığımızda, mevcut yapımızdaki Oracle Standart Edition'ın hedeflediğimiz büyük çaplı proje için yetersiz kaldığı değerlendirilmektedir.

Oracle Enterprise Edition versiyonunun dışında yer alan yukarıda bahsi geçen hiçbir veri tabanında aynı anda 2 ayrı sunucuda tek veri tabanı olarak çalıştırabilme kabiliyeti de yoktur.

Oracle Versiyonlarının Teknik Karşılaştırması

Kişisel Verilerin Korunması İçin Data Masking Çözüm

6698 Sayılı Kişisel Verilerin Korunması Kanunu'na göre, gerçek kişilere ait veriler kanun kapsamına alınmıştır ve bu kişilerle ilişkilendirilecek her türlü bilgi bu kanun kapsamında korunmaktadır. Bu durum, "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi" yönetmeliğinde açık şekilde belirtilmiştir.

Veri tabanlarında tutulan hassas verilerin bu kapsamda korunabilmesi için kullanılan yöntemlerin en yaygın olanı veri maskeleyedir. Veri maskeleye, tablolarda tutulan verilerin çeşitli yöntemler ile değiştirilerek orijinalinden tanınmaz hale getirilmesi işlemidir.

Oracle veri tabanları için veri maskeleye işlemini Oracle Enterprise Manager 12c Cloud Control üzerinde sunulan Data Masking eklentisi kullanılarak yapılmaktadır. Yukarıda bahsi geçen diğer veri tabanı yönetim sistemlerinde güvenliği ve gizliliği tesis eden bu özellik bulunmamaktadır. Binlerce vatandaşa kamu hizmeti veren kurumumuzda vatandaşlara ait bilgileri kişisel verilerin gizliliği kapsamında saklamak istediğimizden bu durum önem arz etmektedir.

...

Veritabanı Yetkilendirme ve Bilgi Güvenliği Özelliği

Bir veri tabanı yaratıldıktan sonra, veri tabanı yöneticisi diğer kullanıcılara erişim hakkı sağlamak için, veri tabanına erişim ve üzerinde bazı uygulamaları gerçekleştirme hakkı vermek durumundadır. Güvenliği sağlamak için, yönetici kimlerin veri tabanına bağlanacağını ve hangi uygulamaları gerçekleştireceğini belirlemelidir. Kullanıcı isimleri ve şifreler oluşturulduktan sonra, kullanıcılara veri tabanı üzerinde yapabilecekleri işlemler atanır. ISO 27001 Bilgi Güvenliği Yönetim Standardı bu

proje kapsamında ulaşmayı hedeflediğimiz güvenlik standardı olmakla beraber, aynı standardın “Görevler Ayrılığı” ilkesine göre, verilerimizi yönetmeyi istemekteyiz.

Kuruluşun varlıklarının yetkisiz veya farkında olmadan değiştirilme ya da kötüye kullanılma fırsatlarını azaltmak için, görevler ve sorumluluk alanlarını kişisel bazda ayırmayı hedeflemekteyiz.

Oracle Database üzerinde bir opsiyon olarak gelen ‘Database Vault’ seçeneği, veri tabanını daha güvenli hale getirmek için yapılacak konfigürasyondur. Sistem performansına çok düşük bir etkiyle aktifleştirilip, yüksek yetkili kullanıcıların veri tabanı üzerinde hassas veriye ulaşması engellenebilir. Database Vault Oracle Enterprise edition sürümü ile birlikte gelir.

...

Aktif Data Guard Özelliği

‘Data Guard’ temel anlamda bir veri tabanının başka bir yere anlık kopyalanması ve her hangi bir anda kopya veri tabanının açılarak production olarak hizmet sunabilmesidir. Bu felaket durumlarına karşı her veri tabanı yönetim sistemi (Oracle, MS SQL Server, MySQL) bir felaket kurtarma çözümü ortaya koymaktadır. Ancak iki ayrı veri tabanının da (ana ve yedek) aktif aktif çalışmasını sağlayacak özellik Oracle Enterprise Edition sürümünde "Active Data Guard" özelliği ile birlikte gelmektedir.

Böylece ana veri tabanında herhangi bir sıkıntı yaşandığı anda hızlıca yedek veri tabanından devam edilebilmektedir. Burada Dataguard’ın en önemli rollerinden birisi ana veri tabanının sadece bir yedek veri tabanını oluşturması değil, aynı zamanda eşzamanlı olarak canlı verilerle yedeği beslediği için oluşturulan konfigürasyona göre anlık yedeğini oluşturmasıdır. ...” ifadelerine yer verilmiştir.

Şikâyet dilekçesinde yer alan söz konusu iddialarla ilgili olarak akademik bir kuruluştan 08.05.2018 tarihli yazımız ile teknik görüş talep edilmiş olup, akademik kuruluşun 22.05.2018 tarihli yazısı ile gönderilen teknik görüş yazısında “Teknik olarak, ihalesi yapılacak olan "Süreç Bazlı Web Tabanlı Yönetim Bilgi Sistemi Yazılım Modülleri ve Elektronik Belge Yönetim Sistemi" nihayetinde bir yazılım sistemidir. Bir yazılım sistemi, doğal olarak ve genellikle bir veritabanı sistemi ile birlikte çalışacaktır. Herhangi bir yazılım sistemi, kullanıcılarının gereksinimlerini karşılaması gereken özellikleri barındırmalıdır. Bu gereksinimler genellikle işlevsel ve işlevsel olmayan gereksinimler olarak ifade edilmektedir. İşlevsel gereksinimlerin karşılanması noktasında veritabanı yönetim sistemine herhangi bir bağımlılık bulunmamaktadır. Ancak, işlevsel olmayan gereksinimlerin karşılanması noktasında, yazılım sistemi ile birlikte kullanılacak olan veritabanı yönetim sisteminin sahip olduğu özellikler nedeniyle bazı bağımlılıklar olabilir. Ancak, bu durum bir zorunluluk değildir. Kaldı ki, yazılım sisteminin karşılaması gereken işlevsel olmayan gereksinimler bir veya

daha fazla sayıda alternative veritabanı yönetim sistemi tarafından karşılanabilir. Hatta bu işlevsel gereksinimlerin karşılanması için, ilgili veritabanı yönetim sisteminin ihtiyaç duyacağı donanım sistemini de tarifleyebilir.

Şikayet konusunda belirtilen her bir şikayet gerekçesi için ilgili şikayet gerekçesi ve bu gerekçenin teknik açıdan değerlendirmesi şu şekildedir:

Şikayet gerekçesi-1: "Teknik Şartname'nin 18.1. maddesi kapsamında talep edilen Oracle Enterprise Edition 4 CPU lisansının ihale konusu işe ilişkin modüllerin çalışması için zorunluluk arz etmediği"

Şikayet gerekçesi-1 için teknik değerlendirme: "Süreç Bazlı Web Tabanlı Yönetim Bilgi Sistemi Yazılım Modülleri ve Elektronik Belge Yönetim Sistemi" bir yazılım sistemi olduğundan, Teknik Şartname'de bu yazılım sisteminin ihtiyaç duyacağı işlevsel olmayan gereksinimlerin tarif edilmesi gerekirdi. Bu açıdan değerlendirildiğinde, Teknik Şartname'de belirtilen Oracle Enterprise Edition 4 CPU lisansının ihale konusu işe ilişkin modüllerin çalışması için zorunluluk arz etmediği düşünülmektedir. Farklı bir bakış açısıyla, Kadıköy Belediyesinde halen çalışmakta olan yazılım sistemlerinde kullanılan veritabanı yönetim sisteminin Oracle olması söz konusu ise, Kadıköy Belediyesinde Oracle veritabanı yönetim sistemi yöneticisi veya uzmanı halen istihdam edilmekteyse, diğer yazılım sistemlerinde alternatif veritabanı yönetim sistemleri kullanılmıyorsa, diğer alternatif veritabanı yönetim sistemleri için herhangi bir yönetici veya uzman mevcut değilse Teknik Şartname'de bu durum yazılım sisteminin bir zorunluluğu olarak değil, mevcut altyapı ve çalışan profiline bir kısıtı olarak belirtilmesi gerekirdi. Kaldı ki, günümüz teknolojisinde farklı veritabanı yönetim sistemlerinin birlikte çalışabilirliği de söz konusu olduğundan bu yönde bir zorunluluğun "Süreç Bazlı Web Tabanlı Yönetim Bilgi Sistemi Yazılım Modülleri ve Elektronik Belge Yönetim Sistemi" isimli yazılım sistemi için belirtilmesi bu açıdan da uygun değildir.

Kadıköy Belediyesi idaresince gönderilen cevabi açıklama yazısında belirtilen "Oracle Enterprise Edition dışında başka bir veritabanında bu alternatif bulunmamasıdır" ifadesi doğru değildir. Bu ifadenin doğruluğu yukarıda belirtilen gerekçe nedeniyle geçerli olabilir. Kadıköy Belediyesi'nde ilgili yazılım sisteminin işletilmesi ve sürdürülebilirliğinin sağlanması için gerekli istihdamın olmaması, mevcut veritabanı yönetim sistemi ve ilgili donanım altyapısının Oracle Enterprise Edition ile uyumlu olması gibi gerekçeler ile bu ifade doğru olarak kabul edilebilir. Ancak, idarenin belirttiği gerekçe doğru bir gerekçe değildir.

Şikayet gerekçesi-2: "Teknik Şartname'nin 18.2. maddesinde Oracle Türkiye temsilciliğinden idare adına alınması istenilen lisans ve özet yetki belgesi talep edildiği"

Şikayet gerekçesi-2 için teknik değerlendirme: 1 numaralı şikayet gerekçesine neden olan Oracle Enterprise Edition kısıtı nedeniyle bu gerekçe olağandır. İlgili yazılım sisteminin Oracle Enterprise Edition ile çalıştırılması talebi noktasında, bu talebi karşılayabilecek firma için şikayet gerekçesinde belirtilen "Oracle Türkiye temsilciliğinden idare adına lisans alınması ve özet yetki belgesi talep edilmesi" olağandır. Dolayısıyla 1 numaralı şikayet gerekçesi doğal olarak 2 numaralı şikayet gerekçesini de doğurmaktadır. Bu açıdan değerlendirildiğinde, 2 numaralı şikayet gerekçesi 1 numaralı şikayet gerekçesinin doğal bir sonucu durumundadır. Bu durumun şikayete söz konusu olması gereksiz ve anlamsızdır. Çünkü, 1 numaralı şikayet gerekçesinde belirtilen "Oracle Enterprise Edition" kısıtının sağlıklı bir şekilde gerçekleştirilebilmesi için 2 numaralı şikayet gerekçesi doğal bir zorunluluktur.

Şikayet gerekçesi-3: "söz konusu düzenleme ile rekabet ortamının ortadan kaldırıldığı, ihaleye katılmak isteyenlerin katılımını engellediği"

Şikayet gerekçesi-3 için teknik değerlendirme: 1 numaralı şikayet gerekçesine konu olan kısıt altında dahi, 3 numaralı şikayet gerekçesinde belirtilen "rekabet ortamının ortadan kalkması" gibi bir durum söz konusu olamaz. Türkiye'de Oracle Enterprise Edition veritabanı yönetim sistemini kullanarak ilgili yazılım sistemini sunabilecek onlarca firma bulunmaktadır. Bu firmalar da halihazırda Oracle Türkiye temsilciliğinden idare adına lisans alabilir ve özel yetki belgesi talep edebilir. Şikayette bulunulmasının tek gerekçesi farklı bir veritabanı yönetim sisteminin alternatif olarak değerlendirilemeyecek olmasından kaynaklandığı düşünülmektedir. Bu açıdan değerlendirildiğinde kısmi olarak rekabet ortamının kısıtlandığı kabul edilebilir ancak bu durum rekabet ortamının ortadan kaldırıldığı anlamına gelmez.

Sonuç olarak, Teknik Şartname'de özellikle "Oracle Enterprise Edition" kısıtının belirtilmesi kanımca, 4734 sayılı kanunun 5. ve 12. maddelerinde belirtilen hususlar gereğince, uygun değildir. Şikayet gerekçesi-1 ile ilgili teknik değerlendirmede de belirttiğim üzere, "Süreç Bazlı Web Tabanlı Yönetim Bilgi Sistemi Yazılım Modülleri ve Elektronik Belge Yönetim Sistemi" isimli yazılım sistemi için işlevsel olmayan gereksinimler tariflenerek Teknik Şartname'nin yazılması daha uygun olurdu. Ancak, 4734 sayılı kanunun 12. maddesinde belirtilen "...Ancak, mal veya hizmet atımları ile yapım işlerinin özelliği nedeniyle idarelerce hazırlanmasının mümkün olmadığının ihale yetkilisi tarafından onaylanması kaydıyla, teknik şartnameler bu Kanun hükümlerine göre hazırlanabilir." ifadesine dayanarak, Kadıköy Belediyesi'nin mevcut donanım altyapısı, mevcut veritabanı yönetim sistemleri ve mevcut bilişim personeli istihdamına uygun olarak ilgili Teknik Şartname'nin "Oracle Enterprise Edition" kısıtıyla yazılması daha uygun olurdu." ifadelerine yer verilmiştir.

Yukarıda aktarılan teknik görüş, ihale dokümanında yer alan düzenlemeler ve iddia konusu husus birlikte değerlendirildiğinde;

a, b- İdarece veri tabanı yönetim sistemi(VTYS) olarak Oracle Enterprise Edition talep edildiği, Teknik Şartname’de yer verilen ihtiyaçlar doğrultusunda veri tabanı yönetim sistemi olarak Oracle Enterprise Edition’ın zorunluluk olmadığı, Teknik Şartname’de belirtilen işe ilişkin ihtiyacın karşılanmasında alternatif marka ve modellerin bulunduğu,

İdarenin ihtiyaçları doğrultusunda işin teknik tüm gerekliliklerine Teknik Şartname’de yer vermesi gerektiği, bu çerçevede İdarece Kurum’a gönderilen açıklama yazılarında yer verilen gerekçelere Teknik Şartname’de açıkça yer verilmediği (idarede mevcut donanım yapısının kullanılması, mevcut VTYS ile entegrasyonun sağlıklı şekilde yapılması ve entegrasyonda veri kaybının yaşanmaması, mevcut personelin eğitimi, felaket kurtarmaya ilişkin özel şartlar vb.), idarenin ihale konusu iş için gerekli gördüğü şartları Teknik Şartname’de yer vermesi ve tek bir marka ve model belirtmeden ihtiyaçlarını karşılamaya çalışmasının kamu ihale mevzuatına daha uygun olacağı,

Akademik kuruluştan alınan teknik görüş doğrultusunda söz konusu Teknik Şartname düzenlemelerinin Kamu İhale Kanunu’nun “Temel İlkeler” başlıklı 5’inci maddesine ve “Şartnameler” başlıklı 12’nci maddesine aykırılık teşkil ettiği anlaşıldığından başvuru sahibinin iddiasının yerinde olduğu sonucuna varılmıştır.

c- Teknik Şartname’nin 18.2’nci maddesinde Oracle Türkiye temsilciliğinden idare adına alınması istenilen lisans zorunluluğu ve özel yetki belgesi talep edildiği, söz konusu düzenlemenin VTYS olarak Oracle Enterprise Edition istenilmesinin doğal bir sonucu olmakla birlikte katılımın Oracle Enterprise Edition kullanılarak yazılım geliştiren istekliler ile kısıtlandığı, bu çerçevede idarenin anılan belgelerin belirli bir marka için talep edilmesinin rekabeti kısıtlayıcı olduğu sonucuna varılmıştır.

Yukarıda yer verilen değerlendirmeler çerçevesinde, başvuruya konu ihalenin iptal edilmesi gerektiği sonucuna varılmıştır.

4) Başvuru sahibinin 4’üncü iddiasına ilişkin olarak:

Teknik Şartname’nin “İhtiyaç Duyulan Sistem, Yazılım ve Hizmet Bileşenleri” başlıklı 10’uncu maddesinde “10.5. İdare’de kurulacak yeni, Web Tabanlı ve Süreç Bazlı Yönetim Bilgi Sistemi için ihtiyaç duyulan sistem ve hizmet bileşenleri; yazılım altyapısı, yazılım, modül, uygulama, entegrasyon, analiz ve modelleme hizmetleri, ana başlıklar halinde aşağıdaki tabloda belirtilmiştir.

Aşağıdaki bileşenler, Yüklenici tarafından tek ve tam bütünlük bir yapıyı oluşturacak şekilde kurulmalı, ilişkisel olarak tanımlanmalı ve kullanıma sunulmalıdır.

...

Yönetim Bilgi Sistemi İş Süreçleri Analizi (İdare'nin yaklaşık 500 adet sürecinin tanımlanması)...” düzenlemesi,

Aynı Şartname'nin “İşin Süresi ve Projenin Fazları” başlıklı 11'inci maddesinde “Yüklenici, Sistem'i Şartname'nin bu bölümünde tanımlanan, işin süresi ile ilgili madde ve alt maddelerde belirtilen zamanda tamamlamakla yükümlüdür. İdare'nin ihtiyaçları ve talepleri doğrultusunda proje süresi fazlara ayrılmıştır ve her fazda gerçekleştirilecek olan bileşenler belirtilmiştir.

Proje, İdare'nin ihtiyaçları ve talepleri doğrultusunda 3 (üç) faza bölünmüştür.

...

11.2. Birinci Faz: Sözleşmenin imzalanmasından 90 gün sonra tamamlanmalıdır.

Ekli listede belirtilen yaklaşık 500 adet iş sürecinin (ana ve alt süreçler dahil olmak üzere) analizinin yapılması, İdarece ihtiyaç duyulduğu takdirde bu faz kapsamında kurum içerisinde tespit edilen mevzuata uygun yeni süreçlerinde eklenebilmesi gerekmektedir. Süreçler istenildiği takdirde cd ortamında Gizlilik sözleşmesi ile istekliye verilecektir.

EBYS ve YBS süreç altyapısına uygun şekilde Müdürlüklerle yapılan görüşmeler sonucunda iş akışlarının çıkarılması. (İdare'de mevcut önceki iş süreçleri, PDF formatında, Bilgi İşlem Müdürlüğü tarafından dijital ortamda Yüklenici'ye teslim edilecektir.)

Çıkarılan iş akışları dinamik olmalıdır. Aynı zamanda belirtilen tarihe kadar süreçlerin işlediğine dair test ortamında gerçekleştirilmesinden sonra kabul edilecektir.

Çağrı Merkezi ve EBYS Entegrasyonunun sağlanması.

Süreç Tabanlı Elektronik Belge Yönetim Sisteminin devreye alınması.” düzenlemesi yer almaktadır.

Teknik Şartname'nin sonunda yer alan ve ihale konusu işin süreçlerini belirten tablo aşağıda yer almaktadır.

ANA SÜREÇ

1. KENTSEL GELİŞİM VE YÖNETİM ANA SÜRECİ

SÜREÇLER

1.1. İmar Planı İşlemleri Süreci

- 1.2. İmar Durumu İşlemleri Süreci
- 1.3. Harita ve Numarataj İşlemleri Süreci
- 1.4. Yapı Ruhsatı İşlemleri
- 1.5. Kat irtifakı Kurulması Süreci
- 1.6. Tesisat-Isı Yalıtım ve Asansör Kontrol Süreci
- 1.7. Düşük Beton Sınıfı Sonucu Revize Edilmiş Statik Hesap Kontrol Süreci
- 1.8. Taşıyıcı Sistemle İlgili Şikayet Süreci
- 1.9. Bağımsız Bölüm Numarası Düzeltilmesi Süreci
- 1.10. Proje Sureti ve İmar Dosyası Sureti Düzenlenmesi Süreci
- 1.11. Tescilli Eski Eser Binalar İle İlgili İşlemler Süreci
- 1.12. Restorasyon Denetim İşlemi
- 1.13. Eski Eserlerle İlgili Şikayetlerin Yönetilmesi Süre
- 1.14. Kurum/ Vatandaş Verilen İzin ve Belgeler Süreci
- 1.15. Mevcut ve Yeni Binaların Ruhsat ve Tasdikli Projelerine Uygunluğunun Tespit ve Kontrolü Süreci
- 1.16. Yapı Tatil Tutanağının Düzenlenmesi Süreci
- 1.17. Yapı Denetim Otomasyon Sistemine Bilgi Girişi Süreci
- 1.18. Jeolojik ve Jeofizik Çalışmaların Yapılması Süreci
- 1.19. Test Kontrolü İşlemlerin Yapılması Süreci
- 1.20. Kentsel Yenileme Rapor Kontrolü Ve Kentsel Yenileme Raporu Hazırlanması
- 1.21. İmar İşlem Dosyalarının ve Evrakların Taranması - Arşivlenmesi Ve Ekspertiz Süreci
- 1.22. Şikayetlerin Değerlendirilmesi Süreci
- 1.23. 6306 Sayılı Yasa Kapsamında Riskli Binaların Tebligatları Süreci
- 1.24. 6306 Sayılı Yasa Kapsamında Kira Yardımının Yapılması Süreci
- 1.25. Alt Yapı ve Üst Yapı Hizmetlerinin Yürütülmesi Süreci
- 1.26. Kentsel Tasarım Çalışmalarının Yürütülmesi Süreci

1.27. Kadıköy'ün Araştırmacı, Katılımcı ve Tasarımcı Yönünün Güçlendirilmesi Süreci

1.28. Araştırma ve Geliştirme Süreci

1.29. Yapı ve Açık Alan Projelerinin Çizilmesi Süreci

İhale konusu işin idarenin ihtiyacı olan Yönetim Bilgi Sistemi Yazılım Modülleri ve Elektronik Belge Yönetim Sistemi Hizmeti olduğu, idarece söz konusu iş kapsamında yer alan işlerin ana süreçlerinin ve alt süreçlerinin başlıklar halinde Teknik Şartname'de belirtildiği, ayrıca süreçlerin ayrıntılı gösterildiği tabloların istenildiği takdirde CD ortamında gizlilik sözleşmesi ile istekliye verileceğinin Teknik Şartname'de belirtildiği, süreç kavramından idarenin yönetsel işlerinin bilgisayar ortamında gerçekleştirilmesinin kastedildiği, bu kapsamda idarece yaklaşık 500 iş sürecinin belirtildiği, değişen ve gelişen iş ortamında iş süreçlerinin net bir sayı olarak belirlenmesinin beklenemeyeceği, idarenin ihtiyaçları doğrultusunda artıp azalmasının mümkün olduğu göz önüne alındığında başvuru sahibinin bahse konu iddiasının yerinde olmadığı sonucuna varılmıştır.

5) Başvuru sahibinin 5'inci iddiasına ilişkin olarak:

Sözleşme Tasarısı'nın "Sözleşmenin ekleri" başlıklı 8'inci maddesinde "8.1. İhale dokümanı, bu sözleşmenin eki ve ayrılmaz parçası olup, İdareyi ve Yükleniciyi bağlar. Ancak, sözleşme hükümleri ile ihale dokümanını oluşturan belgelerdeki hükümler arasında çelişki veya farklılık olması halinde, ihale dokümanında yer alan hükümler esas alınır.

8.2. İhale dokümanını oluşturan belgeler arasındaki öncelik sıralaması aşağıdaki gibidir:

- 1) Hizmet İşleri Genel Şartnamesi,
- 2) İdari Şartname,
- 3) Sözleşme Tasarısı,
- 4) Birim fiyat tarifleri (varsa),
- 5) Özel Teknik Şartname (varsa),
- 6) Teknik Şartname,
- 7) Açıklamalar (varsa),

İdari şartnamedeki 5.1.e maddesindeki belgeler" düzenlemesi,

Aynı Tasarı'nın "Alt yüklenicilere ilişkin bilgiler ve sorumluluklar" başlıklı 15'inci maddesinde "15.1. Bu işte alt yüklenici çalıştırılmayacak ve işlerin tamamı yüklenicinin kendisi tarafından yapılacaktır." düzenlemesi,

Teknik Şartname'nin "Genel Şartlar" başlıklı 3'üncü maddesinde "3.9. Yüklenici, Şartname'ye konu sistemin ve sistem ile ilişkili sair hizmetleri sunarken, idarenin önceden yazılı iznini almaksızın üçüncü tarafların hizmetlerinden yararlanamaz, alt yüklenici kullanamaz." düzenlemesi yer almaktadır.

Yukarıda yer verilen ihale dokümanı düzenlemeleri incelendiğinde, Sözleşme Tasarısı'nın 15'inci maddesinde açıkça ihale konusu işte alt yüklenici çalıştırmayacağını belirtildiği, Teknik Şartname'nin 3.9'uncu maddesinde de "idarenin önceden yazılı iznini almaksızın üçüncü tarafların hizmetlerinden yararlanamaz, alt yüklenici kullanamaz" ifadelerine yer verildiği, söz konusu ifadenin alt yüklenici çalıştırılabilir anlamı taşımadığı, dolayısıyla anılan düzenlemelerin birbirine aykırılık teşkil etmediği, kaldı ki Sözleşme Tasarısı'nın 8'inci maddesinde ihale dokümanını oluşturan belgeler arasındaki öncelik sıralamasının belirtildiği, bu sıralamaya göre Sözleşme Tasarısı'nın Teknik Şartname'den önce geldiğinin anlaşıldığı, dolayısıyla ihale konusu işte alt yüklenici çalıştırmayacağı anlaşıldığından başvuru sahibinin bahse konu iddiasının yerinde olmadığı değerlendirilmiştir.

6) Başvuru sahibinin 7'nci iddiasına ilişkin olarak:

Hizmet İşleri Genel Şartnamesi'nin "İşlerin bakımı" başlıklı 21'inci maddesinde "Yüklenici, işe başlama tarihinden işlerin tümü için kabul belgesinin tanzim edildiği tarihe kadar işlere, malzemelere ve tesise gereken özen ve bakımı gösterme sorumluluğu altında olacaktır.

Yüklenici, garanti süresi içinde taahhüt ettiği bütün işlerin ve malzemelerin ve ilgili tesislerin bakım ve özeninden bu sürenin sonuna kadar sorumlu olacaktır." hükmü,

Aynı Şartname'nin "Yüklenicinin bakım ve düzeltme sorumlulukları" başlıklı 33'üncü maddesinde "Yapılan işlerin her türlü sorumluluğu, kabul işlemlerinin idarece onaylanması tarihine kadar, tümüyle yükleniciye aittir. Bu nedenle yüklenici, gerek malzemenin kötülüğünden ve gerekse işlerin kusur ve eksikliklerinden dolayı, idarece gerekli görülecek bütün onarım ve düzeltmeler ile sürekli bakım işlerini kendi hesabına derhal yapmak zorundadır." hükmü,

Anılan Şartname'nin "Kabul sürecindeki bakım ve giderler" başlıklı 48'inci maddesinde "Yüklenici, kabul sürecinin başlangıcından sonuna kadar geçen süre içinde işlerin bakımını yapmak, tümünü iyi bir şekilde korumak ve çıkabilecek kusur ve aksaklıkları gidermek zorundadır.

Yüklenicinin kusurları dışındaki nedenlerin gerektirdiği onarımlar bakım yükümlülüğünün dışındadır.

Kullanma ve işletme sonucu olmaksızın ortaya çıkan kusur ve aksaklıkların giderilmesi ile iş bitim tarihinden kabul tarihine kadar geçen sürede işlerin bakım giderleri yükleniciye aittir.” hükmü,

Anılan Şartname'nin “Garanti dönemi olan işlerde kabul işlemi” başlıklı 49'uncu maddesinde “Sözleşmesinde işe ilişkin bir garanti dönemi belirtilmiş olması durumunda, yüklenicinin başvurusu üzerine idarece verilecek talimat üzerine kontrol teşkilatınca işlerin garanti şartlarını karşılayıp karşılamadığı ve varsa bu dönemde yüklenicinin temerrüdünden dolayı idarece yapılmak zorunda kalan masraflar tespit edilir. Kurulan kabul komisyonu, kontrol teşkilatının verilerine ve kendi gözlemlerine dayanarak işin kabulünü yapar veya yüklenicinin hakedişinden veya teminatından düşülecek bedeli belirleyerek kabul işlemini tamamlar. Bu gibi kusur ve eksikliklerin niteliğinin ve kesilecek bedelin kabul tutanağında gösterilmesi gereklidir.

Bu kabul işlemlerinde varsa sözleşmesindeki hükümler uygulanır.” hükmü,

Teknik Şartname'nin “Genel Şartlar” başlıklı 3'üncü maddesinde “3.5. Yüklenici, Sözleşme imza tarihinden itibaren, bu Şartname'de öngörülen Proje Süresi boyunca ve Proje Süresi sonunda, işin tamamlanmasını takip eden 1 (bir) yıllık Garanti Süresi boyunca, Sistem'in ve Sistem için kuracağı bütün modüllerin sürüm koruma ve teknik desteğini sağlayacaktır. Yüklenici, hiçbir suretle söz konusu Sistem için, Proje Süresi boyunca lisans/bakım/destek ücreti adı altında ek ücret talep edemez. Proje Süresi ve Garanti Süresi boyunca, Sistem ve Sistem dahilindeki modüllerin tüm güncellemeleri (yeni çıkan sürümleri), Yüklenici tarafından ücretsiz olarak İdare'ye verilecektir.

3.6. Proje Süresi'nin dolmasını takip eden dönemde, lisans güncelleme, sürüm koruma, bakım ve yazılım teknik destek hizmetinin devamlılığı için, İdare kendi takdirine bağlı olarak, Yüklenici ile yıllık ya da süresi 1 (bir) yıldan fazla olan, belirli süreli lisans güncelleme ve destek sözleşmeleri yapabilir. Proje Süresi'nin dolmasından sonraki ilk yıl için, Yüklenici tarafından verilecek olan yıllık lisans güncelleme, sürüm koruma, bakım ve destek hizmetinin bedeli, personel hariç, Yüklenici'nin ihalede teklif ettiği bedelin %18'ini aşmayacaktır. Sonraki yıllarda teklif edilecek bakım bedeli, önceki yılın bakım bedelinin %10 fazlasından yüksek olamaz.” düzenlemesi yer almaktadır.

Başvuru sahibinin iddiasının b kısmına yönelik olarak idarece “... Bakım sözleşmesi yapıldığında garanti süresi dolmuş olacağından personel desteğine de ihtiyaç kalmayacaktır. Teknik şartnamenin 3.6 maddesinde belirtilen sözleşme bedelinin %18'in aşmayacak şekilde yapılacak ilk bakım sözleşmesi personel giderleri hariç tutulmuştur. ...” denilerek cevap verilmiştir.

a- Yukarıda yer verilen Teknik Şartname düzenlemeleri incelendiğinde, Teknik Şartname'nin 3.5'inci maddesinde proje süresinin sonundan itibaren 1 yıllık garanti süresinin öngörüldüğü, bu garantinin

kapsamının kurulacak sistemin sağlıklı çalışmasını teminat altına almak olduğu, Teknik Şartname'nin 3.6'ncı maddesinde proje süresinin dolmasını takip eden dönem için yeni bir sözleşme imzalanmasından bahsedildiği, idarenin cevabından da anlaşılacağı üzere süresi 1 yıldan fazla olan bu sözleşmenin proje tesliminden sonra karşılaşılabilecek sürüm güncelleme, hizmet gereği ihtiyaç duyulan modül ekleme gibi işlemlerini kapsadığı, dolayısıyla garanti kapsamında olan işlerden bahsedilmediği anlaşıldığından başvuru sahibinin bahse konu iddiasının yerinde olmadığı sonucuna varılmıştır.

b- İdarece söz konusu iddianın b kısmına ilişkin verilen cevaptan anlaşıldığı üzere Teknik Şartname'nin 3.6'ncı maddesinde belirtilen sözleşme kapsamında yaptırılacak işler için personel gideri öngörülmediği ve yönde düzenleme yapıldığı anlaşıldığından başvuru sahibinin bahse konu iddiasının yerinde olmadığı sonucuna varılmıştır.

c- Kamu İhale Sözleşmeleri Kanunu'nun "Sözleşme kapsamında yaptırılacak ilave işler, iş eksilişi ve işin tasfiyesi" başlıklı 24'üncü maddesinde "Mal ve hizmet alımlarıyla yapım sözleşmelerinde, öngörülemeyen durumlar nedeniyle bir iş artışının zorunlu olması halinde, artışa konu olan iş;

a) Sözleşmeye esas proje içinde kalması,

b) İdareyi külfete sokmaksızın asıl işten ayrılmasının teknik veya ekonomik olarak mümkün olmaması,

Şartlarıyla, anahtar teslimi götürü bedel ihale edilen yapım işlerinde sözleşme bedelinin % 10'una, birim fiyat teklif almak suretiyle ihale edilen mal ve hizmet alımlarıyla yapım işleri sözleşmelerinde ise % 20 'sine kadar oran dahilinde, süre hariç sözleşme ve ihale dokümanındaki hükümler çerçevesinde aynı yükleniciye yaptırılabilir." hükmü bulunmaktadır.

Teknik Şartname'nin 3.6'ncı maddesinde belirtilen sözleşmenin Kamu İhale Sözleşmeleri Kanunu'nun "Sözleşme kapsamında yaptırılacak ilave işler, iş eksilişi ve işin tasfiyesi" başlıklı 24'üncü maddesi kapsamındaki iş artışını kapsamadığı, idarenin takdiri ile şikayete konu işin devamı niteliğinde sayılabilecek yeni bir işin sözleşmesinden bahsedildiği, dolayısıyla idarece o işe ilişkin işlemlerin ayrıca yürütüleceği anlaşıldığından başvuru sahibinin bahse konu iddiasının yerinde olmadığı sonucuna varılmıştır.

7) Başvuru sahibinin 8'inci iddiasına ilişkin olarak:

4735 sayılı Kamu İhale Sözleşmeleri Kanunu'nun "Sözleşmede yer alması zorunlu hususlar" başlıklı 7'nci maddesinde "Bu Kanuna göre düzenlenecek sözleşmelerde aşağıdaki hususların belirtilmesi zorunludur:

...

l) Garanti istenilen hallerde süresi ve garantiye ilişkin şartlar." hükmü,

Sözleşme Tasarısı'nın "Garanti ile ilgili şartlar" başlıklı 34'üncü maddesinde "34.1. Bu madde boş bırakılmıştır." düzenlemesi,

Teknik Şartname'nin "Genel Şartlar" başlıklı 3'üncü maddesinde "3.5. Yüklenici, Sözleşme imza tarihinden itibaren, bu Şartname'de öngörülen Proje Süresi boyunca ve Proje Süresi sonunda, işin tamamlanmasını takip eden 1 (bir) yıllık Garanti Süresi boyunca, Sistem'in ve Sistem için kuracağı bütün modüllerin sürüm koruma ve teknik desteğini sağlayacaktır. Yüklenici, hiçbir suretle söz konusu Sistem için, Proje Süresi boyunca lisans/bakım/destek ücreti adı altında ek ücret talep edemez. Proje Süresi ve Garanti Süresi boyunca, Sistem ve Sistem dâhilindeki modüllerin tüm güncellemeleri (yeni çıkan sürümleri), Yüklenici tarafından ücretsiz olarak İdare'ye verilecektir." düzenlemesi bulunmaktadır.

Yukarıda yer verilen mevzuat hükümleri ve ihale dokümanı düzenlemeleri incelendiğinde, anılan Kanun'da yer alan garanti şartlarına İdari Şartname'de yer almasına ilişkin hüküm ile istekli olabileceklerin garanti konusunda bilgilendirilmesinin amaçlandığı, başvuruya konu ihaleye ait Sözleşme Tasarısı'nın "Garanti ile ilgili şartlar" başlıklı 34'üncü maddesinde herhangi bir düzenlemeye yer verilmediği, ancak Teknik Şartname'de garantiye ilişkin düzenlemelere yer verildiği, istekli olabileceklerin garantiye ilişkin tereddüt duydukları hususlarda idareden açıklama talep edebilmelerinin mümkün olduğu hususları bir arada değerlendirildiğinde söz konusu durumun ihalenin iptaline gerekçe oluşturacak nitelikte olmadığı anlaşıldığından başvuru sahibinin iddiasının yerinde olmadığı sonucuna varılmıştır.

8) Başvuru sahibinin 9'uncu iddiasına ilişkin olarak:

İdari Şartname'nin "İhaleye katılabilmek için gereken belgeler ve yeterlik kriterleri" başlıklı 7'nci maddesinde "7.5. Mesleki ve teknik yeterliğe ilişkin belgeler ve bu belgelerin taşınması gereken kriterler:

7.1. İsteklilerin ihaleye katılabilmeleri için aşağıda sayılan belgeleri teklifleri kapsamında sunmaları gerekir:

...

h) ...

3- TUBİTAK Kamu Sertifikasyon Merkezi tarafından verilen E-İmza uyum değerlendirme raporu

...

7.5.4. İsteklinin teklifi kapsamında sunması gerektiği teknik şartnamede belirtilen belgeler.” düzenlemesi,

Teknik Şartname'nin “Elektronik Bilgi Belge ve Arşiv Yönetim Sistemi Genel Özellikleri” başlıklı 14.2'nci maddesinde “14.2.5. İstekliler, Kamu Sertifikasyon Merkezinin verdiği, ürünün ulusal ve uluslararası elektronik imza standartlarına uygunluğunu belgeleyen kapsamlı test ve E-İmza Uygunluk Raporunu teklifiyle birlikte sunmalıdır.” düzenlemesi yer almaktadır.

Başvuru sahibinin iddiasında yer verilen 9.19'uncu maddesi şikayete konu ihaleye ait Teknik Şartname'de yer almamaktadır. Teknik Şartname'nin 14.2.5'inci maddesinde yer verilen “E-İmza Uygunluk Raporu”na İdari Şartname'nin 7'nci maddesinde “Kamu Sertifikasyon Merkezi tarafından verilen E-İmza uyum değerlendirme raporu” olarak yer verilmiştir. Ayrıca İdari Şartname'de “7.5.4. İsteklinin teklifi kapsamında sunması gerektiği teknik şartnamede belirtilen belgeler” düzenlemesine yer verilerek Teknik Şartname'de teklif kapsamında sunulması gereken belgelere yer verilebileceği anlaşıldığından başvuru sahibinin iddiasının yerinde olmadığı sonucuna varılmıştır..

9) Başvuru sahibinin 10'uncu ve 13'üncü iddialarına ilişkin olarak:

4734 sayılı Kamu İhale Kanunu'nun “İhalelere yönelik başvurular” başlıklı 54'üncü maddesinin birinci fıkrasında, ihale sürecindeki hukuka aykırı işlem veya eylemler nedeniyle bir hak kaybına veya zarara uğradığını veya zarara uğramasının muhtemel olduğunu iddia eden adayların, isteklilerin ve istekli olabileceklerin, bu Kanun'da belirtilen şekil ve usul kurallarına uygun olmak şartıyla şikâyet ve itirazın şikâyet başvurusunda bulunabileceği hükmüne yer verilmiş, ilgili maddenin dilekçelerde yer alacak hususları sayan dördüncü fıkrasının (d) bendinde, başvurunun konusu, sebepleri ve dayandığı deliller belirtilmiş ve anılan maddenin onbirinci fıkrasının (c) bendinde süre, usul ve şekil kurallarına uygun olmayan başvuruların reddedileceği hükme bağlanmıştır.

İhalelere Yönelik Başvurular Hakkında Yönetmelik'in “Başvuruların şekil unsurları” başlıklı 8'inci maddesinin ikinci fıkrasının (ç) bendinde, “başvurunun konusu, sebepleri ve dayandığı deliller”in itirazın şikâyet başvuru dilekçesinde bulunması gerektiği belirtilmiş, 15'inci maddesinde, Kuruma yapılan başvuruların, öncelikle 16'ncı madde çerçevesinde inceleneceği, 16'ncı maddenin birinci fıkrasının (ı) bendinde, başvurunun konusu, sebepleri ve dayandığı delillerin belirtilip belirtilmediğinin inceleneceği, 17'nci maddenin birinci fıkrasında ise, 16'ncı maddenin birinci fıkrası

bakımından bir aykırılığın tespiti üzerine Kurul tarafından başvurunun reddine karar verileceği düzenlemelerine yer verilmiştir.

Diğer taraftan İhalelere Yönelik Başvurular Hakkında Tebliğ'in "İtirazen şikâyet başvurularında aranılacak şekil unsurları" başlıklı 11'inci maddesinin sekizinci fıkrasında "Yönetmeliğin 8 inci maddesinin ikinci fıkrasının (ç) bendinde başvurunun konusu, sebepleri ve dayandığı delillerin başvuru dilekçelerinde belirtilmesi gerektiği düzenlendiğinden, başvuruda bulunulan hususların dilekçelerde somut bir biçimde, mevzuata aykırı bulunma sebepleri ile birlikte gösterilmesi gerekmektedir. İşlemin hangi unsurlarının hangi gerekçelerle hukuka aykırı olduğu belirtilmeksizin sadece mevzuata aykırı olduğu gibi soyut ve mesnetsiz iddialara yer verilmesi halinde, Yönetmeliğin 8 inci maddesine aykırı olduğu gerekçesiyle başvurunun reddine ilişkin sorumluluk başvurana ait olacağından bu hususa dikkat edilmesi gerekmektedir" açıklaması yer almaktadır.

Yukarıda aktarılan mevzuat hükümlerinden aday veya istekli ile istekli olabilecekler tarafından yapılan başvuruların esas yönünden incelenebilmesi için; idarenin hukuka aykırı bir işlem veya eylemi nedeniyle hak kaybına veya zarara uğradığı veya zarara uğramasının muhtemel olduğu iddiasına yer verilmesi ve başvuruya ilişkin Kanun'da öngörülen diğer şartların yanı sıra, konu ve sebep unsurları ile iddianın dayanağını oluşturan delillerin gösterilmesi gerektiği anlaşılmaktadır.

Bu çerçevede başvuru sahibinin şikâyet ve itirazen şikâyet başvuru dilekçelerinde Teknik Şartname ile İdari Şartname arasında tezatlıklar bulunduğu iddia olunmaktaysa da, söz konusu iddia kapsamında Teknik Şartname ile İdari Şartname'nin hangi maddelerinin tezatlıklar barındırdığının belirtmediği,

Söz konusu ihale kapsamında alımı düşünülen otomasyon sisteminin 6698 sayılı Kişisel Verilerin Korunması Kanunu'na uygun olarak çalışması gerektiği iddialarına yer verilmekteyse de, söz konusu iddia kapsamında anılan Kanun'a aykırılığa ilişkin bir delil sunulmadığı, aykırılığın somut bir şekilde ifade edilmediği dikkate alındığında somut delillere dayandırılmayan iddiaların uygun bulunmadığı, bu bakımdan söz konusu iddiaların 4734 sayılı Kanun'un 54'üncü maddesinin onbirinci fıkrasının (c) bendi gereğince reddi gerektiği sonucuna varılmıştır.

10) Başvuru sahibinin 11'inci iddiasına ilişkin olarak:

4735 sayılı Kamu İhale Sözleşmeleri Kanunu'nun "Sözleşmede yer alması zorunlu hususlar" başlıklı 7'nci maddesinde "Bu Kanuna göre düzenlenecek sözleşmelerde aşağıdaki hususların belirtilmesi zorunludur:

...

n) Gecikme halinde alınacak cezalar." hükmü,

Sözleşme Tasarısı'nın "Cezalar ve sözleşmenin feshi" başlıklı 16'ncı maddesinde "16.1. İdare tarafından uygulanacak cezalar aşağıda belirtilmiştir:

16.1.1. 1- Sözleşme hükümlerinin tamamını yerine getirmediği takdirde %0,05 (onbindebeş) oranında gecikme cezası uygulanır ve bu gecikme ihtarına rağmen aynı durumun devam etmesi halinde ayrıca protesto çekmeye gerek kalmaksızın kesin teminat gelir kaydedilir ve sözleşme fesh edilerek hesabı genel hükümlere göre tasfiye edilir.

2- Sistem vasıtasıyla internet üzerinden yapılan ödemelerle ilişkili olarak ortaya çıkan Sistem hatalarından kaynaklanan, vatandaşın uğradığı zararlar dahil olmak üzere sistemden kaynaklanan nedenlerle üçüncü kişilerin ve İdare'nin uğradığı zararların tazmin edilmesinden Yüklenici sorumlu olacaktır.

3- Herhangi bir süreçte veri aktarımının Yüklenici tarafından kaynaklanan bir sebepten dolayı tam ya da gereği gibi gerçekleşmemesi halinde İdare Yükleniciden Sözleşme bedelinin %3'ü oranında cezai şart talep etme hakkına sahiptir.

4- Yüklenici İdare'nin onayı olmadan iş için görevlendirdiği herhangi bir personeli geri çekemez veya başka bir projede görevlendiremez. Böyle bir durumda, bu durumun yaşandığı tarihten itibaren sözleşme bedelinin % 1'i (yüzde bir) oranında günlük para cezası kesilecektir.

5-Yüklenici zamanında tamamlanmayan çalışmalar olması durumunda, gecikilen her gün için sözleşme bedelinin % 1'i (yüzde bir) oranında ceza ödemekle yükümlü olacak ve bu ceza tutarları İdare tarafından Yüklenici'ye ödenecek bedelden mahsup edilecektir.

6-Fazların zamanında tamamlanmaması halinde İdare'nin Sözleşmeyi tek taraflı ve tazminatsız olarak fesih hakkı saklıdır.

7-Herhangi bir süreçte veri aktarımının Yüklenici tarafından kaynaklanan bir sebepten dolayı tam ya da gereği gibi gerçekleşmemesi halinde İdare Yükleniciden Sözleşme bedelinin %3'ü oranında cezai şart talep etme hakkına sahiptir.

İdare tarafından kesilecek cezanın toplam tutarı, hiçbir durumda, sözleşme bedelinin % 30'unu geçmeyecektir.

16.2. Yukarıda belirtilen cezalar ayrıca protesto çekmeye gerek kalmaksızın yükleniciye yapılacak ödemelerden kesilir. Cezanın ödemelerden karşılanamaması halinde ceza tutarı yükleniciden ayrıca tahsil edilir.

16.3. İhtarda belirtilen sürenin bitmesine rağmen aynı durumun devam etmesi halinde, ayrıca protesto çekmeye gerek kalmaksızın kesin teminat ve varsa ek kesin teminat gelir kaydedilir ve sözleşme feshedilerek hesabı genel hükümlere göre tasfiye edilir.” düzenlemesi,

Teknik Şartname'nin “Genel Şartlar” başlıklı 3'üncü maddesinde “Ybs Yazılım Altyapısı Servis Süresi Planlaması

Tablodaki unsurlar örnek kabilinden sayılmış olup olayın kritiklik derecesinin ne olduğu İdare tarafından belirlenecektir.

Yüklenici'nin minör olaylar için yukarıda belirtilen süreler içinde sorunu çözüme ulaştıramadığı durumlarda İdare, gecikilen her bir gün için Sözleşme bedelinin %1'i (yüzde biri) oranında cezai şart uygulayacaktır. Majör olaylar içinse yukarıda belirtilen süreler içinde sorunun çözülemediği durumlarda gecikilen her bir gün için Sözleşme bedelinin %3'ü (yüzde üçü) oranında cezai şart uygulayacaktır.” düzenlemesi,

Aynı Şartname'nin “Yüklenicinin Yükümlülükleri” başlıklı 9'uncu maddesinde “9.24 Yüklenici, işin öngörülen sürede yapılması için gerekli olan iş gücü ve insan kaynakları planlamasını yapacak ve İdare'ye bir proje yöneticisi atayacaktır. Yüklenici, söz konusu uzman proje yöneticisi dahil olmak üzere, en az 5 (beş) kişiden oluşan bir proje analiz ve destek ekibi teşkil edecek ve bu ekibi Proje Süresi boyunca İdare'de görevlendirecektir. Yüklenici, bu ekibin sağlayacağı hizmetler de dahil olmak üzere, diğer hizmetlerinde, geliştirme, kurulum, güncelleme, uyarılma ve uygulama faaliyetlerinde kendi iş gücü ve insan kaynaklarını kullanacaktır. İdare Yüklenici'nin bu Şartname'ye konu iş için görevlendirdiği personeli herhangi bir gerekçe belirtmeden değiştirme talebinde bulunduğu; Yüklenici bu değişiklik talebini en geç 3 (üç) iş günü içerisinde yerine getirecektir. Yüklenici İdare'nin onayı olmadan iş için görevlendirdiği herhangi bir personeli geri çekemez veya başka bir projede görevlendiremez. Böyle bir durumda, bu durumun yaşandığı tarihten itibaren ihalede teklif edilen bedelin % 1'i (yüzde bir) oranında günlük para cezası kesilecektir. Yüklenici ayrıca İdare tarafından teşkil edilecek ilave bir analiz ve destek ekibinin yönetimini ve eğitimini de üstlenecektir.” düzenlemesi,

Anılan Şartname'nin “İşin Süresi ve Projenin Fazları” başlıklı 11'inci maddesinde “11.8. Yüklenici zamanında tamamlanmayan çalışmalar olması durumunda, gecikilen her gün için sözleşme bedelinin % 1'i (yüzde bir) oranında ceza ödemekle yükümlü olacak ve bu ceza tutarları idare tarafından Yüklenici'ye ödenecek bedelden mahsup edilecektir.” düzenlemesi yer almaktadır.

Sözleşme Tasarısı'nın "Sözleşmenin ekleri" başlıklı 8'inci maddesinde "8.1. İhale dokümanı, bu sözleşmenin eki ve ayrılmaz parçası olup, İdareyi ve Yükleniciyi bağlar. Ancak, sözleşme hükümleri ile ihale dokümanını oluşturan belgelerdeki hükümler arasında çelişki veya farklılık olması halinde, ihale dokümanında yer alan hükümler esas alınır.

8.2. İhale dokümanını oluşturan belgeler arasındaki öncelik sıralaması aşağıdaki gibidir:

- 1) Hizmet İşleri Genel Şartnamesi,
- 2) İdari Şartname,
- 3) Sözleşme Tasarısı,
- 4) Birim fiyat tarifleri (varsa),
- 5) Özel Teknik Şartname (varsa),
- 6) Teknik Şartname,
- 7) Açıklamalar (varsa),

İdari Şartnamedeki 5.1.e maddesindeki belgeler" düzenlemesi bulunmaktadır.

Yukarıda yer verilen mevzuat hükümleri ve ihale dokümanı düzenlemeleri incelendiğinde, işin gereği gibi yapılmaması veya eksik yapılması durumunda yüklenici tarafından ödenecek cezaların oranlarına Sözleşme Tasarısı'nda ve Teknik Şartname'de yer verildiği, ihale dokümanını oluşturan belgeler arasındaki öncelik sıralamasına bakıldığında Sözleşme Tasarısı'nın önce geldiği, dolayısıyla Sözleşme Tasarısı ile Teknik Şartname arasındaki uyumsuzluk bulunması durumunda Sözleşme Tasarısı'ndaki düzenlemenin uygulanacağı, bu açıdan başvuru sahibinin iddiasının yerinde olmadığı, Sözleşme Tasarısı'nda yer verilen "Sözleşme hükümlerinin tamamını yerine getirmediği takdirde %0,05 (onbindebeş) oranında gecikme cezası uygulanır." düzenlemesinden işin bütünüdür zamanında bitirilememesi durumunda uygulanacak "gecikme cezası"ndan bahsedildiği, dolayısıyla "tamamı" ifadesi yerine "her biri" ifadesi gelmesi gerektiği yönündeki iddianın yerinde olmadığı sonucuna varılmıştır..

11) Başvuru sahibinin 12'inci iddiasına ilişkin olarak:

4734 sayılı Kamu İhale Kanunu'nun "Şartnameler" başlıklı 12'nci maddesinde "İhale konusu mal veya hizmet alımları ile yapım işlerinin her türlü özelliğini belirten idari ve teknik şartnamelerin idarelerce hazırlanması esastır. Ancak, mal veya hizmet alımları ile yapım işlerinin özelliği nedeniyle idarelerce hazırlanmasının mümkün olmadığı ihale yetkilisi tarafından onaylanması kaydıyla, teknik şartnameler bu Kanun hükümlerine göre hazırlattırılabilir.

İhale konusu mal veya hizmet alımları ile yapım işlerinin teknik kriterlerine ihale dokümanının bir parçası olan teknik şartnamelerde yer verilir. Belirlenecek teknik kriterler, verimliliği ve fonksiyonelliği sağlamaya yönelik olacak, rekabeti engelleyici hususlar içermeyecek ve bütün istekliler için fırsat eşitliği sağlayacaktır.” hükmü,

Hizmet Alımı İhaleleri Uygulama Yönetmeliği'nin “Teknik şartname” başlıklı 16'ncı maddesinde “(1) İşin teknik ayrıntılarını ve şartlarını gösteren bir teknik şartname hazırlanarak ihale dokümanına dahil edilir. Teknik şartnamelerde belirlenecek teknik kriterlerin, verimliliği ve fonksiyonelliği sağlamaya yönelik olması, rekabeti engelleyici hususlar içermemesi ve bütün istekliler için fırsat eşitliği sağlaması zorunludur.

(2) Teknik şartnamede, varsa ulusal ve/veya uluslararası teknik standartlara uygunluğu sağlamaya yönelik düzenlemeler de yapılır. Bu şartnamede teknik özelliklere ve tanımlamalara yer verilir. ...

(3) Teknik şartnamenin idare tarafından hazırlanması esastır. Ancak, işin özelliğinin gerektirdiği hallerde ihale yetkilisi tarafından onaylanması kaydıyla teknik şartname, Kanun hükümlerine uygun olarak danışmanlık hizmet sunucularına hazırlattırılabilir. yer almaktadır.” hükmü yer almaktadır.

Anılan Kanun ve Yönetmelik hükümlerinden anlaşılacağı üzere, ihalelere ait şartnamelerin ihtiyaçlar doğrultusunda idarelerce hazırlanması esastır. Şikâyete konu ihaleyi yapan idarenin belediye başkanlığı olduğu, söz konusu iddiada yer verilen diğer idarelerin de belediye başkanlıkları olduğu, farklı belediye başkanlıklarının görev ve yetkileri kapsamındaki işlerin aynı veya benzer olabileceği, bu açıdan bakıldığında belediyelerin yazılım ihtiyaçlarının da birbirileri ile aynı veya benzer olmasının olağan olduğu, benzer ihalelerin şartnamelerinde aynı veya benzer hükümlerin bulunmasının, idarelerin şartnameleri kendilerinin hazırlamadığı anlamına gelmeyeceği, şartnamelerin birbirine benzer olmasının tek başına rekabeti engelleyici unsur olarak kabul edilemeyeceği, anılan Kanun'un temel ilkelerini ihlal ettiği iddia edilen düzenlemelerin ayrı ayrı ele alınarak değerlendirilebileceği anlaşıldığından, başvuru sahibinin şikayete konu ihaleye ait Teknik Şartname'nin, Darıca Belediye Başkanlığı ve Beykoz Belediye Başkanlığı tarafından gerçekleştirilen benzer işe ait ihalelerin teknik şartnameleri ile benzerlik taşımasının temel ilkelere aykırı olduğu yönündeki iddiasının yerinde olmadığı sonucuna varılmıştır.

Sonuç olarak, yukarıda mevzuata aykırılıkları belirtilen işlemlerin düzeltici işlemle giderilemeyecek nitelikte işlemler olduğu tespit edildiğinden, ihalenin iptali gerekmektedir.

Açıklanan nedenlerle, 4734 sayılı Kanun'un 65'inci maddesi uyarınca bu kararın tebliğ edildiği veya tebliğ edilmiş sayıldığı tarihi izleyen 30 gün içerisinde Ankara İdare Mahkemelerinde dava yolu açık olmak üzere,

Anılan Kanun'un 54'üncü maddesinin onbirinci fıkrasının (a) bendi gereğince ihalenin iptaline, Oybirliği ile karar verildi.

Kamu İhale Kurulu Kararı - KİK (K. 2016/UH.II-1732)

Kamu İhale Kurulu Kararı - KİK, K. 2016/UH.II-1732 T. 29.06.2016

2016/108298 İhale Kayıt Numaralı "Çalışma Ve Sosyal Güvenlik Ortak İletişim "Alo 170" Çağrı Merkezi" İhalesi

TOPLANTIYA KATILAN ÜYELER:

Başkan: Hamdi GÜLEÇ

Üyeler: II. Başkan Şinasi CANDAN, Osman DURU, Köksal SARINCA, Dr. Ahmet İhsan ŞATIR, Oğuzhan YILDIZ

BAŞVURU SAHİBİ: Pusula Call Center İletişim A.Ş. - Callus Bilgi ve İletişim Hizmetleri A.Ş.,
Meşrutiyet Mahallesi Atatürk Bulvarı Gama İş Merkezi No: 97/26 Kızılay/ Çankaya/ANKARA

İHALEYİ YAPAN İDARE: Sosyal Güvenlik Kurumu Başkanlığı Destek Hizmetleri Daire Başkanlığı,
Ziyabey Caddesi No:6 06520 Çankaya/ANKARA

BAŞVURUYA KONU İHALE: 2016/108298 İhale Kayıt Numaralı "Çalışma ve Sosyal Güvenlik Ortak İletişim "Alo 170" Çağrı Merkezi" İhalesi

KURUMCA YAPILAN İNCELEME:

Sosyal Güvenlik Kurumu Başkanlığı Destek Hizmetleri Daire Başkanlığı tarafından 13.05.2016 tarihinde açık ihale usulü ile gerçekleştirilen "Çalışma ve Sosyal Güvenlik Ortak İletişim "Alo 170" Çağrı Merkezi" ihalesine ilişkin olarak Pusula Call Center İletişim A.Ş. - Callus Bilgi ve İletişim Hizmetleri A.Ş. tarafından 13.06.2016 tarih ve 35416 sayı ile Kurum kayıtlarına alınan 13.06.2016 tarihli dilekçe ile itirazın şikâyet başvurusunda bulunulmuştur.

Başvuruya ilişkin olarak 2016/1408 sayılı şikâyet dosyası kapsamında yapılan inceleme neticesinde esas inceleme raporu tanzim edilmiştir.

KARAR: Esas inceleme raporu ve ekleri incelendi.

İtirazın şikâyet dilekçesinde özetle; 2016/108298 İhale Kayıt Numaralı Çalışma ve Sosyal Güvenlik Ortak İletişim "Alo 170" Çağrı Merkezi İhalesi'ne teklif verdikleri, tekliflerinin idare tarafından aşırı düşük teklif olarak tespit edildiği, kendilerinden aşırı düşük tekliflerine ilişkin açıklama istenildiği, yapmış oldukları açıklamanın idare tarafından uygun bulunduğu ve tekliflerinin ekonomik açıdan

en avantajlı teklif olarak belirlendiği, 07.06.2016 tarihinde EKAP üzerinden kendilerine gönderilen yazıda “Çalışma ve Sosyal Güvenlik Ortak İletişim “Alo 170” Çağrı Merkezi ihalesi, ihale yetkilisi tarafından ihale dokümanlarının ve projeye ilgili diğer tüm süreçlerin, ihale onay tarihinden sonra yayımlanan Kişisel Verilerin Korunması Kanunu’na uygunluk sağlanması bakımından yeniden değerlendirilmesi ve bu konuda Kurumumuzca gerekli önlemlerin alınması zarurieti ortaya çıkması nedeniyle iptal edilmiştir.” ifadelerinin yer aldığı, idarenin iptal gerekçesinin hiçbir yasal dayanağının olmadığı ve söz konusu iptal gerekçesinin mevzuata uygun olmadığı, şöyle ki idarece iptal gerekçesi olarak öne sürülen Kişisel Verilerin Korunması Kanunu’nun 07.04.2016 tarih ve 29677 sayılı Resmi Gazete’de yayımlandığı, söz konusu ihale ilanının 11.04.2016, ihale tarihinin ise 13.05.2016 olduğu, ihalenin bu süreçte iptal edilmediği, anılan Kanun’un ihale yapıldıktan veya sözleşme imzalandıktan sonra yürürlüğe girmiş olmasının bu Kanun’un uygulanmayacağı sonucunu doğurmayacağı, idare ile henüz sözleşme imzalanmadığı için ilgili hususların sözleşmeye dercedilebileceği ihale yetkilisi ve ihale sürecinde görev alan kişilerin bu durumu göz önünde bulundurmadan görevlerini kanuni gereklere uygun ve tarafsızlıkla yapmadıkları, bu nedenle haklarında 4734 sayılı Kamu İhale Kanunu’nun 60’ıncı maddesi uyarınca işlem tesis edilmesi gerektiği iddialarına yer verilmiştir.

İptal gerekçeleri ile sınırlı olarak yapılan inceleme sonucunda aşağıdaki hususlar tespit edilmiştir.

İhaleye ilişkin İdari Şartname’ nin “İhale konusu işe ilişkin bilgiler” başlıklı 2’nci maddesinde “2.1. İhale konusu hizmetin;

- a) Adı: Çalışma ve Sosyal Güvenlik Ortak İletişim "Alo 170" Çağrı Merkezi
- b) Miktarı ve türü: Çalışma ve Sosyal Güvenlik Ortak İletişim "Alo 170" çağrı merkezi hizmeti alınması işi.
- c) Yapılacağı yer: Çalışma ve Sosyal Güvenlik Ortak İletişim "Alo 170" Çağrı Merkezi hizmet alımı Karaman, Şanlıurfa, Sivas, Kütahya, Ankara ve Trabzon İllerinde hizmet verecektir.
- ç) Bu bent boş bırakılmıştır.” düzenlemesi,

4734 sayılı Kanun’un “Temel ilkeler” başlıklı 5’inci maddesinde “İdareler, bu Kanuna göre yapılacak ihalelerde; saydamlığı, rekabeti, eşit muameleyi, güvenilirliği, gizliliği, kamuoyu denetimini, ihtiyaçların uygun şartlarla ve zamanında karşılanmasını ve kaynakların verimli kullanılmasını sağlamakla sorumludur.

...” hükmü,

Anılan Kanun'un "İhalenin karara bağlanması ve onaylanması" başlıklı 40'ncı maddesinde "... İhale komisyonu gerekçeli kararını belirleyerek, ihale yetkilisinin onayına sunar. Kararlarda isteklilerin adları veya ticaret unvanları, teklif edilen bedeller, ihalenin tarihi ve hangi istekli üzerine hangi gerekçelerle yapıldığı, ihale yapılmamış ise nedenleri belirtilir.

İhale yetkilisi, karar tarihini izleyen en geç beş iş günü içinde ihale kararını onaylar veya gerekçesini açıkça belirtmek suretiyle iptal eder.

İhale; kararın onaylanması halinde geçerli, iptal edilmesi halinde ise hükümsüz sayılır.

..." hükmü,

Anılan Kanun'un 54'üncü maddesinin onuncu fıkrasının (c) bendinde "Başvurunun süre, usul ve şekil kurallarına uygun olmaması, usulüne uygun olarak sözleşme imzalanmış olması veya şikâyete konu işlemlerde hukuka aykırılığın tespit edilememesi veya itirazın şikâyet başvurusuna konu hususun Kurumun görev alanında bulunmaması hallerinde başvurunun reddine karar verilir." hükmü,

Aynı Kanun'un "Kuruma itirazın şikâyet başvurusu" başlıklı 56'ncı maddesinde "... İhalenin iptaline ilişkin işlem ve kararlardan, sadece şikâyet ve itirazın şikâyet üzerine alınanlar itirazın şikâyete konu edilebilir ve bu kararlara karşı beş gün içinde doğrudan Kuruma başvuruda bulunulabilir.

...

İdare tarafından şikâyet veya itirazın şikâyet üzerine alınan ihalenin iptal edilmesi işlemine karşı yapılacak itirazın şikâyet başvuruları ise idarenin iptal gerekçeleriyle sınırlı incelenir." hükmü,

İhalelere Yönelik Başvurular Hakkında Tebliğ'in "İdareye şikâyet başvurusu" başlıklı 2'nci maddesinde "... (2) Ancak, idare tarafından şikâyet veya itirazın şikâyet üzerine alınan ihalenin iptal edilmesi işlemine karşı idareye şikâyet başvurusunda bulunulmadan, doğrudan Kuruma itirazın şikâyet başvurusunda bulunulması gerekmektedir.

..." açıklaması,

Aynı Tebliğ'in "İtirazın şikâyet başvurusu" başlıklı 8'inci maddesinde ise "(1) İdareye yapılan şikâyet başvurusu üzerine idare tarafından alınan kararın uygun bulunmaması veya on günlük süre içinde idare tarafından bir karar alınmaması hallerinde veya şikâyet ya da itirazın şikâyet üzerine idare tarafından alınan ihalenin iptali kararlarına karşı doğrudan Kuruma itirazın şikâyet başvurusunda bulunulabilir.

(2) İhalenin iptali kararlarından sadece aşağıda belirtilenler itirazın şikâyete konu edilebilir:

a) Şikâyet başvurusu üzerine idare tarafından şikâyet dilekçesinin kayıtlara alındığı tarih veya sonrasında herhangi bir nedenle idare tarafından alınan iptal kararları.

b) İtirazen şikâyet üzerine Kurul tarafından başvurunun reddine veya düzeltici işlem belirlenmesine karar verildikten sonra idare tarafından alınan iptal kararları.

(3) Herhangi bir şikâyet veya itirazen şikâyet başvurusu olmaksızın idare tarafından alınan ihalenin iptali kararlarına karşı Kuruma itirazen şikâyet başvurusunda bulunulamayacağından, bu kararlar ancak idari yargı mercilerinde dava konusu edilebilir." açıklamaları yer almaktadır.

Yukarıda aktarılan mevzuat hüküm ve açıklamaları gereği yapılan incelemede, ihale sürecinde idareye yapılan bir şikâyet başvurusunun olduğu ve başvuru sahibi isteklinin teklifinin geçerli olduğu, başvuru sahibinin iptale ilişkin işlemi 07.06.2016 tarihinde öğrendiği, bu tarihten itibaren beş gün içinde doğrudan Kuruma başvurduğu, dolayısıyla 13.06.2016 tarihli şikâyet başvurusunun ihalenin iptali işlemine karşı süresi içerisinde yapılan bir başvuru olarak değerlendirilmesi gerektiği anlaşılmıştır.

13.05.2016 tarihinde yapılan ihalede 10 doküman satın alındığı, ihaleye 4 isteklinin katıldığı 31.05.2016 tarihli ihale komisyonu kararı ile başvuru sahibi Pusula Call Center İletişim A.Ş., Callus Bilgi ve İletişim Hizmetleri A.Ş. İş Ortaklığının ekonomik açıdan en avantajlı teklif sahibi ve Lapis Eğitim Organizasyon ve Sosyal Hizmetler Limited Şirketi -Prizma Personel Destek Hizmetleri Limited Şirketi İş Ortaklığının da ekonomik açıdan en avantajlı ikinci teklif sahibi olarak belirlendiği, Başvuru sahibi isteklinin teklifinin idarece hesaplanan sınır değerinin altında olduğu ve kendisine 20.05.2016 tarihinde EKAP üzerinden aşırı düşük teklif sorgulaması yapıldığı, yapılan aşırı düşük teklif açıklamasının 31.05.2016 tarihli ihale komisyonu kararı ile uygun bulunduğu anlaşılmıştır.

02.02.2016 tarih ve 2016/200 sayılı Sosyal Güvenlik Kurumu Yönetim Kurulu'nun (ihale yetkilisinin) aşağıda yer alan gerekçelerle 31.05.2016 tarihli ihale komisyonu kararını iptal ettiği görülmüştür.

Söz konusu gerekçeler "...Kişisel verilerin tutulması ve işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak, kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul esasları düzenlemek maksadıyla Kişisel Verilerin Korunması Kanunu'nun 07.04.2016 tarihinde Resmi Gazetede yayımlandığı,

Bu kanun ile kişisel verileri işleyen gerçek ve tüzel kişilere, kişisel verilerin işlenmesi, silinmesi, yok edilmesi, anonim hale getirilmesi, yurt içinde ve yurt dışına aktarılması, veri sahiplerinin aydınlatılması ve veri güvenliği konularında bir takım önemli yükümlülükler getirildiği,

Bu kapsamda gerçek ve tüzel kişilerin, veri sorumlusunu belirlemek, kişisel verilerin hukuka aykırı olarak işlenmesini ve hukuka aykırı olarak erişilmesi önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda oldukları,

Ayrıca veri sorumlusunun, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi halinde, yukarıda belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumlu olduğu gibi, kendi kurum ve kuruluşlarında, Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorunluluğunun bulunduğu,

Kanunda belirtilen yükümlülükleri yerine getirmeyen veri sorumluları hakkında 1 yıla 6 yıl 9 ay arasında hapis cezalarının ve 5.000 TL'den başlayıp 1.000.000 TL'ye varan para cezalarının düzenlenmiş olduğu,

Alo 170 İletişim Merkezi Projesi kapsamında sunulan hizmetlerde vatandaşlara ilişkin önemli kişisel verilerin tutulduğu, toplandığı, işlenmekte olduğu, yedeklendiği dikkate alındığında ilgili Kanun'da belirtilen yükümlülüklerle uyum sağlanması zarureti ve hizmet sunan yüklenici üzerinde bu anlamda gerekli denetimlerin yapılmasının da büyük önem arz etmekte olduğu,

İhale konusu işin İdari ve Teknik Şartnamelerinin 2016 yılı başında oluşturulduğu ve 6698 sayılı Kanun'un yayımlanmasından önce 31.03.2016 tarihli ve 2016/136 sayılı Kurulumuz kararı ile ihale kararının alınmış olduğu,

Tüm bu süreçler tamamlandıktan ve ihaleye çıktıktan sonra 07.04.2016 tarihinde Kişisel Verilerin Korunması Kanun'u yayımlanarak, yürürlüğe girmiş olduğu ve bu nedenle de ihale konusu işte bahse konu Kanunda belirtilen hizmetin sunumunda yasal olarak yapılması zorunlu olan sorumluluk tanımlanması, işin tanımı, usulü ve yaptırımları içinde bunlara yer verilmesinin gerçekleştirilememiş olduğu,

Bunun yanı sıra yüklenicinin yerine getirmesi gereken yükümlülükler ve sorumluluklara da İdari ve Teknik Şartnamelerde yer verilemediği,

İhale dokümanlarında bu hususlara yer verilmemiş olması sözleşmenin uygulanması aşamasında kanundan kaynaklanan yükümlülükleri kimin yerine getireceği, bunun maliyetlerinin teklif edilen toplam bedele dahil olup olmayacağı, yerine getirilmemesi halinde kesilecek cezalardan, Kurumumuz mu yüklenici mi yükümlü olacağı, bu hususların uygulanacak usuller konusunda belirsizliklere ve hukuki ihtilaflara neden olacağı,

Aynı zamanda Kanun'da belirtilen yükümlülükler ve idari para cezalarının oluşturacağı muhtemel maliyetlerin proje giderlerinde artışlara neden olmasına rağmen, ihale dokümanlarında bu hususlara yer verilmemiş olması nedeniyle, ihale neticesinde oluşan fiyatın uygulanabilir olmayacağı ve bu durumun harcama bütçesi ve gerçekleştirmelerde uyumsuzluklar oluşturacağı,

Bu nedenle Alo 170 İletişim Merkezi Projesi ve hizmetleri kapsamında hazırlanan ihale dokümanlarının ve projeye ilgili diğer tüm süreçlerin, Kanunu'na uygunluk sağlanması bakımından yeniden değerlendirilmesi ve bu konuda Kurumumuzca gerekli önlemlerin alınması zarurieti ortaya çıktığından, İhale Komisyonunca düzenlenen 31.05.2016 tarihli ve 16 sayılı kararın iptal edilmesine ..." şeklinde ifade edilmiştir.

Yapılan inceleme neticesinde, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 07.04.2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlandığı, söz konusu ihale ilanının 11.04.2016, ihale tarihinin ise 13.05.2016 olduğu tespit edilmiştir. 6698 sayılı Kanun'un "Yürürlük" başlıklı 32'nci maddesinde bazı hükümlerin yayımı tarihinden altı ay sonra, diğer maddelerin ise yayımı tarihinde yürürlüğe gireceği hüküm altına alınmıştır. Dolayısıyla kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenleyen bu hükümlerin birçoğunun 07.04.2016 tarihinden itibaren etkili olacağı açıktır. İhale işlemlerinin belli bir süreci kapsamaması nedeniyle, ihale süreci içerisinde yürürlüğe giren anılan Kanun hükümlerinin yürürlük tarihinden itibaren ihale işlemlerinde ve ihale sonucunda etkili olacağı kuşku bulunmamaktadır.

Kanun, herkes için bağlayıcı olan hukuk kurallarını içine alır ve bunu uygulamakla vazifeli organları ve herkesi bağlar. İdari merciler de bu organlardan biri olup, kanun hükümlerinin gereğini yerine getirmek zorundadırlar. Bu nedenle, söz konusu Kanun ile getirilen yeni düzenlemelerin devam eden ihale sürecine uygulanması gerekmektedir. Eğer söz konusu gerekliliğin yerine getirilmemesi ihale sürecinin devam etmesine engel oluşturuyor ve anılan Kanun ve ihale dokümanı arasındaki uyumun sağlanması düzeltici işlemle giderilemiyorsa, ihalenin iptal edilmesi gerekmektedir.

Kaldı ki 4734 sayılı Kanun'un 40'nci maddesinden ihale yetkilisinin ihale komisyon kararını onaylamak veya gerekçesini açıkça belirtmek suretiyle iptal etme yetkisinin bulunduğu anlaşılmaktadır. Söz konusu yetkinin dayanağı kamu yararı ve hizmet gerekleridir. Dolayısıyla ihale yetkilisinin kamu yararı ve hizmet gerekleri nedeniyle, ihale dokümanının Kişisel Verilerin Korunması Kanunu'nun getirdiği düzenlemeler doğrultusunda yeniden değerlendirilmesi ve bu konuda gerekli önlemlerin alınması nedeniyle ihaleyi iptal etmesinde mevzuata aykırılık bulunmadığı sonucuna varılmıştır.

Açıklanan nedenlerle, 4734 sayılı Kanun'un 65'inci maddesi uyarınca bu kararın tebliğ edildiği veya tebliğ edilmiş sayıldığı tarihi izleyen 30 gün içerisinde Ankara İdare Mahkemelerinde dava yolu açık olmak üzere,

Anılan Kanun'un 54'üncü maddesinin onbirinci fıkrasının (c) bendi gereğince itirazen şikâyet başvurusunun reddine,

Oybirliği ile karar verildi.

Hamdi GÜLEÇ

Başkan

Şinasi CANDAN

II. Başkan

Osman DURU

Kurul Üyesi

Köksal SARINCA

Kurul Üyesi

Dr. Ahmet İhsan ŞATIR

Kurul Üyesi

Oğuzhan YILDIZ

Kurul Üyesi

ULUSLARARASI DÜZENLEMELER

Bölüm İçeriği

- Avrupa Konseyi
- Avrupa Birliđi
- Uluslararası Diđer Düzenlemeler

AVRUPA KONSEYİ

Bölüm İçeriği

- İnsan Hakları Avrupa Sözleşmesi
- Avrupa Konseyi - 108 nolu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi
- Avrupa Konseyi - 108 nolu Sözleşme (İngilizce)
- Avrupa Konseyi - 108 nolu Sözleşmeye Ek Protokol
- Avrupa Konseyi - 108 nolu Sözleşmeye Ek Protokol (İngilizce)
- Avrupa Konseyi - 108+ Sözleşmesi (108 Plus)

İnsan Hakları Avrupa Sözleşmesi

European Convention on Human Rights

Rome, 4.XI.1950

Article 8 - Right to respect for private and family life

1. Everyone has the right to respect for his private and family, life, his home and his correspondence.
2. There shall be no interference by a public authority with the, exercise of this right except such as is in accordance with the, law and is necessary in a democratic society in the interests of, national security, public safety or the economic well-being of the, country, for the prevention of disorder or crime, for the protection, of health or morals, or for the protection of the rights and freedoms, of others.

İnsan Hakları Avrupa Sözleşmesi

Türkiye, Sözleşmeyi 4.11.1950 tarihinde imzalamış ve 10.03.1954 tarih ve 6366 sayılı Kanun ile onaylamıştır.

Madde 8 - Özel hayata ve aile hayatına saygı hakkı

1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.
2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.

Avrupa Konseyi - 108 nolu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

108 nolu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data

28.01.1981”

Türkiye, bu sözleşmeyi imzalayan ilk Avrupa Konseyi üyesi ülkelerden birisi olmuş; ancak sözleşmenin kanunla uygun bulunması ve onaylanması yaklaşık 35 yıl sürmüştür. Sözleşme, 17 Mart 2016 tarihli ve 29656 sayılı Resmi Gazete’de yayımlanarak iç hukuka dâhil edilmiştir.

Gerekçesi: Günümüzde insan haklarının korunması bilincinin gelişmesiyle eş zamanlı olarak, kişisel verilerin korunmasının önemi de her geçen gün artmaktadır. Bu çerçevede gelişmiş ülkelerde kişisel verilerin korunması alanında detaylı yasal düzenlemelerin uygulanmakta olduğu dikkat çekmektedir. Öte yandan, 20 inci yüzyılda bilgi ve iletişim teknolojilerinde yaşanan hızlı gelişmeler nedeniyle kişisel verilerin kayıt altına alınmasında ciddi bir artış yaşanmış, internetin yaygınlaşması ise konuyu daha hassas bir boyuta taşımıştır.

Türkiye, kişisel verilerin korunmasıyla ilgili uluslararası düzenlemeleri takip ederek, ulusal düzenlemelerine bu çerçevede yön vermektedir. 2010 yılında Anayasada yapılan değişikliklerle kişisel verilerin korunması anayasal bir hak haline getirilmiştir.

Avrupa Konseyi (AK) bünyesinde hazırlanarak 28 Ocak 1981 tarihinde Strazburg'da imzaya açılan ve 1 Ekim 1985 tarihinde yürürlüğe giren 'Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi' ülkemiz tarafından 28 Ocak 1981 tarihinde imzalanmıştır. Anılan Sözleşmeye AK dışındaki ülkelerin de taraf olma imkanı bulunmaktadır.

108 sayılı Sözleşme olarak da bilinen ve 27 maddeden oluşan Sözleşmenin temel amacı; her üye ülkede, uyruğu veya ikametgahı ne olursa olsun gerçek kişilerin, temel hak ve özgürlüklerini ve özellikle kendilerini ilgilendiren kişisel nitelikteki verilerin otomatik bilgi işleme tabi tutulması

karşısında özel yaşam haklarını güvence altına almaktır. Bu itibarla Sözleşme, hükümetlerin vatandaşlarını korumasına yönelik önemli bir araç niteliğindedir.

Bugüne kadar AK üyesi bütün ülkeler ve AK dışından Uruguay olmak üzere toplam 47 ülke Sözleşmeye taraf olmuş, 46 ülke ise Sözleşmeyi onaylamıştır. Türkiye Sözleşmeyi imzalamış olmasına rağmen, onay işlemlerini henüz tamamlamayıp yürürlüğe koymayan tek ülke konumundadır.

108 sayılı Sözleşmenin ülkemizce onaylanarak yürürlüğe konması konusunda zamanında yapılan değerlendirmede, Sözleşmenin iç hukuk düzenlemelerinin tamamlanmasının ardından onaylanması ve yürürlüğe konulmasının uygun olacağı sonucuna varılmıştır. Konunun önemi çerçevesinde, Sözleşme ile ilgili iç hukuk gereklerinin Sözleşmenin onay süreciyle birlikte eş zamanlı yürütülmesi keyfiyeti gündeme gelmiştir.

Ülkemizde kişisel verilerin korunması bağlamında sürdürülmekte olan ulusal mevzuat çalışmalarına da paralel olarak, sözkonusu Sözleşmenin onaylanması, ülkemizin Avrupa Konseyi çerçevesinde oluşturulan ortak hukuk sistemine kişisel verilerin korunması alanında da dâhil olmasını sağlayarak, vatandaşlarımızın insan haklarının ihlal edilmesinin önüne geçilmesine ve ülkemizin uluslararası saygınlığına katkıda bulunacaktır.

Giriş

İşbu Sözleşmeyi imzalayan Avrupa Konseyi Üyesi Devletler,

Avrupa Konseyinin amacının özellikle hukukun üstünlüğüne ve insan hakları ile temel özgürlüklere saygılı olarak, üyeleri arasında daha yakın bir birliğin gerçekleştirilmesi olduğuna inanarak;

Otomatik işleme tabi olan kişisel verilerin sınırlar ötesi akışının yoğunluk kazanması karşısında, temel hak ve özgürlüklere ilişkin güvencelerin, özellikle de özel yaşama saygı hakkının genişletilmesinin arzu edilebilir olduğunu değerlendirerek;

Aynı zamanda sınırları dikkate almaksızın haber alma özgürlüğüne ilişkin yükümlülüklerini de teyit ederek;

Temel değerler olan özel yaşama saygı ile halklar arasında serbest bilgi akışını birbiriyle uzlaştırma gerekliliğini kabul ederek;

Aşağıdaki hususlarda anlaşmışlardır:

Bölüm I

Genel hükümler

Madde 1

Konu ve amaç

İşbu Sözleşmenin amacı, her bir Tarafın ülkesinde, uyruğu veya ikamet yeri ne olursa olsun her gerçek kişinin temel hak ve özgürlüklerini ve özellikle kendisiyle ilgili kişisel verilerin otomatik işleme tabi tutulması karşısında özel hayata saygı hakkını güvence altına almaktır. ("verilerin korunması").

Madde 2

Tanımlar

Bu Sözleşmenin amaçları bakımından:

- a) "Kişisel veriler": Kimliği belirli veya belirlenebilir bir gerçek kişi ("ilgili kişi") hakkındaki tüm bilgileri ifade eder;
- b) "Otomatik veri dosyası" otomatik işleme konu olan bilgilerin tümünü ifade eder;
- c) "Otomatik işlem"den, tamamen veya kısmen otomatik yöntemlerle gerçekleştirilen; verilerin kaydı, bu verilere mantıksal ve/veya aritmetik işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya dağıtılması anlaşılır.
- d) "Dosya yöneticisi", otomatik veri dosyasının amacının ne olacağı, hangi kişisel veri kategorilerinin kaydedilmesi gerektiği ve bunlara hangi işlemlerin uygulanacağı hakkında karar verebilecek olan gerçek veya tüzel kişileri, kamu kurumunu, birimi veya ulusal kanunlara göre yetkili olan diğer kuruluşları ifade eder.

Madde 3

Kapsam

1. Taraflar, işbu Sözleşmeyi kamu sektöründe ve özel sektörde, otomatik kişisel veri dosyalarına ve kişisel verilerin otomatik işleme tabi tutulması konusunda uygulamayı taahhüt ederler.
2. Her devlet, imza sırasında veya onay, kabul, uygun bulma veya taraf olma belgelerinin tevdi edilmesi sırasında veya daha sonra herhangi bir zamanda Avrupa Konseyi Genel Sekreterine muhatap bir beyanla:
 - a) İşbu Sözleşmeyi, listesi tevdi edilecek olan belli otomatik kişisel veri dosyası kategorilerine uygulamayacağını bildirebilir. Ancak, devlet bu listeye, kendi iç hukukunun otomatik verilerin korunmasına ilişkin hükümlerine tabi olan otomatik dosya kategorilerini dahil edemez. Bu nedenle,

ilave otomatik kişisel veri dosyası kategorilerinin kendi iç hukukunun verilerin korunmasına ilişkin hükümlerine tabi kılınması halinde, yapacağı yeni bir beyanla sözkonusu listeyi tadil eder;

b) İşbu Sözleşmeyi, topluluklar, dernekler, vakıflar, şirketler, kurumlar ve tüzel kişiliğe sahip olsun veya olmasın, doğrudan veya dolaylı olarak gerçek kişilerin bir araya gelmesiyle oluşmuş her çeşit diğer kuruluş hakkında da uygulayacağını bildirebilir;

c) İşbu Sözleşmeyi, otomatik bilgi işleme konu olmayan kişisel veri dosyaları hakkında da uygulayacağını bildirebilir.

3. Yukarıdaki 2. fıkranın b veya c bendinde tanımlanan beyanlardan biriyle işbu Sözleşmen.in uygulama alanını genişleten her devlet, sözkonusu beyanda, genişletmen.in ancak tevdi edeceği bir listede gösterilen bazı kişisel dosya kategorilerine uygulanacağını belirtebilir.

4. Yukarıdaki 2. fıkranın a bendinde öngörülen beyanla belli otomatik kişisel veri dosyası kategorilerini Sözleşmen.in uygulama alanı dışında tutan Taraf, bunları uygulama alanı dışında tutmayan bir Taraftan işbu Sözleşmenin sözkonusu kategoriler hakkında uygulanmasını isteyemez.

5. Keza, işbu maddenin 2. b ve 2. c bentlerinde öngörülen kapsam genişletmelerinden herhangi birini yapmayan Taraf, bu genişletmeleri yapan herhangi bir Tarafın bu hususlarda Sözleşmeyi uygulaması gerektiğini öne süremez.

6. İşbu maddenin yukarıdaki 2. fıkrasında öngörülen beyanlar, bunları yapmış olan Devlet bakımından, bu beyanların imza sırasında veya onay, kabul, uygun bulma veya taraf olma belgelerinin tevdi edilmesi sırasında yapılması halinde, sözleşmen.in yürürlüğe girdiği tarihte; eğer beyanlar daha sonra yapılmışsa bunların Avrupa Konseyi Genel Sekreteri tarafından alınmasından üç ay sonra hüküm ifade eder. Bu beyanlar Avrupa Konseyi Genel Sekreterine muhatap bir bildirim ile kısmen veya tamamen geri alınabilir. Beyanların geri alınması, bildirim alındığı tarihten üç ay sonra hüküm ifade eder.

Bölüm II

Verilerin korunmasına ilişkin temel ilkeler

Madde 4

Tarafların Görevleri

1. Her Taraf, kendi iç hukukunda, işbu bölümde yer alan verilerin korunmasına ilişkin temel ilkelere işlerlik kazandırmak amacıyla gerekli önlemleri alır.

2. Bu önlemlerin Tarafça, en geç, Sözleşmenin kendisi bakımından yürürlüğe girdiği tarihte alınması zorunludur.

Madde 5

Verilerin niteliği

Otomatik işleme konu olan kişisel veriler:

- a) Adil biçimde ve yasal yoldan elde edilir ve işlenir;
- b) Belli ve meşru amaçlar için kaydedilir ve bu amaçlara aykırı şekilde kullanılmaz;
- c) Kaydedilme amaçlarına göre uygun ve yerinde olur ve aşırı olmaz;
- d) Doğru bilgileri yansıtır ve gerektiğinde güncellenir;
- e) Kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkan veren bir biçimde saklanır.

Madde 6

Özel veri kategorileri

İç hukukta uygun güvenceler sağlanmadıkça, ırksal kökeni, siyasi düşünceleri, dini veya diğer inançları ortaya koyan kişisel veriler ile sağlık veya cinsel hayatla ilgili kişisel veriler, otomatik işleme tabi tutulmaz. Aynı şey ceza mahkumiyetiyle ilgili kişisel veriler için de geçerlidir.

Madde 7

Verilerin güvenliği

Otomatik dosyalara kaydedilen kişisel verileri korumak için, bunların kaza sonucu veya izinsiz olarak imhasına veya kaza sonucu kaybolmasına veya bunların izinsiz olarak elde edilmesine, değiştirilmesine veya dağıtılmasına karşı uygun güvenlik önlemleri alınır,

Madde 8

İlgili kişi hakkındaki ek güvenceler

Herkes:

- a) Otomatik kişisel veri dosyasının mevcudiyetini, temel amaçlarını, dosya yöneticisinin kimliğini ve mutad ikamet yerini veya başlıca işyerini öğrenmek;

b) Makul aralıklarla ve aşırı gecikmeye veya masrafa maruz kalmadan kendisi ile ilgili kişisel verilerin otomatik dosyada bulunup bulunmadığının teyidini almak ve bu bilgilerin kendisine anlaşılır bir biçim altında iletilmesini sağlamak;

c) Gerekli olan durumlarda, bu verileri düzelttirmek veya bunların, işbu Sözleşmenin 5. ve 6. maddelerinde belirtilen temel ilkelere işlerlik sağlayan iç hukuk hükümlerinin ihlali suretiyle işlenmiş olması halinde, sözkonusu verileri sildirmek;

d) İşbu maddenin b ve c fıkralarında öngörülen teyit talebinin veya duruma göre bildirim, düzeltme veya silme talebinin yerine getirilmemesi halinde bir başvuru yolundan yararlanmak hakkına sahiptir.

Madde 9

İstisnalar ve kısıtlamalar

1. İşbu maddede belirtilen sınırlar dışında, Sözleşmenin 5, 6 ve 8. maddeleri hükümlerine hiçbir istisna getirilemez.

2. Taraf devletin kanunlarında öngörülmüş olması ve demokratik bir toplumda aşağıdaki hususların sağlanması için gerekli bir önlem oluşturması halinde işbu Sözleşmenin 5, 6 ve 8. maddelerine istisna getirilebilir:

a) Devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi;

b) İlgili kişinin veya başkasının hak ve özgürlüklerinin korunması.

3. İlgili kişilerin özel yaşamlarına tecavüz tehlikesi bulunmadığının açık olduğu durumlarda, 8. maddenin b, c ve d fıkralarında düzenlenen haklar istatistiki veya bilimsel amaçlar için kullanılan kişisel veri dosyaları bakımından kanunla kısıtlanabilir.

Madde 10

Yaptırımlar ve başvuru yolları

Her bir Taraf, işbu bölümde düzenlenen verilerin korunması hakkındaki temel ilkelere işlerlik sağlayan iç hukuk kurallarının ihlaliyle ilgili uygun yaptırımlar ve başvuru yolları getirmekle yükümlüdür.

Madde 11

Genişletilmiş koruma

İşbu bölümde yer alan hükümlerden hiçbiri, her devletin, ilgili kişilere işbu Sözleşmede öngörülenden daha fazla koruyucu önlem sağlaması imkanını sınırlayacak veya buna hanel getirecek şekilde yorumlanamaz.

Bölüm III

Sınır ötesi veri akışları

Madde 12

Kişisel verilerin sınır ötesi akışı ve iç hukuk

1. Otomatik işleme konu olan veya otomatik işleme konu olmak üzere toplanmış olan kişisel verilerin her türlü yoldan ulusal sınırların ötesine transferinde aşağıdaki hükümler uygulanır.

2. Bir Taraf, münhasıran özel yaşamın korunması amacıyla kişisel verilerin diğer bir Tarafa sınır ötesi akışını yasaklayamaz veya özel müsaadeye tabi tutamaz.

3. Bununla birlikte her bir Taraf, 2. fıkradaki hükümlere aşağıdaki durumlarda istisnalar getirebilir:

a) Kendi mevzuatının, belli kişisel veri veya otomatik kişisel veri dosyası kategorileri için, bu verilerin veya dosyaların doğasından kaynaklanan özel düzenlemeler içermesi, diğer Tarafın düzenlemelerinin ise eşdeğer bir koruma içermemesi durumunda;

b) Bu transferin bir Tarafın ülkesinden, bir diğer Taraf üzerinden Taraf olmayan bir devletin ülkesine yapılması durumunda, bu bendin başında atıfta bulunulan Tarafın mevzuatının boşluklarından yararlanmak üzere yapılacak bu tür transferleri engellemek amacıyla.

Bölüm IV

Karşılıklı yardımlaşma

Madde 13

Taraflar arasında işbirliği

1. Taraflar, işbu Sözleşmeyi uygulamak üzere birbirlerine karşılıklı yardımda bulunmayı taahhüt ederler.

2. Bu amaçla:

a) Taraflardan her biri bir veya birden fazla makam tayin ederek, bunların isim ve adreslerini Avrupa Konseyi Genel Sekreterine bildirir;

b) Birden fazla makam tayin eden her bir Taraf, yukarıdaki bentte atıfta bulunulan bildirimde, bu mercilerden her birinin yetkisini belirtir.

3. Taraflardan birinin tayin ettiği bir makam, diğer Tarafın tayin ettiği bir makamın talebi üzerine:

a) Verilerin korunması hakkındaki hukukuna ve idari uygulamalara ilişkin bilgileri verir.

b) İç hukukuna ve münhasıran özel yaşamın korunması amacına uygun olarak, otomatik işleme konu olan kişisel verilerin kendileri istisna olmak üzere, ülkesinde gerçekleştirilen otomatik işlemlerle ilgili somut bilgilerin sağlanması için gerekli tüm önlemleri alır.

Madde 14

Yabancı ülkelerde ikamet eden ilgili kişilere yardım

1. Taraflardan her biri, kendi iç hukukunda öngörülen, işbu Sözleşmenin 8. maddesinde belirtilen ilkelere işlerlik kazandıran hakların kullanılması için, yabancı ülkede ikamet eden tüm kişilere yardımda bulunur.

2. Eğer böyle bir kişi diğer bir Tarafın ülkesinde ikamet ediyorsa, talebini bu Tarafın tayin ettiği makama yapma imkanına da sahip olmalıdır.

3. Yardım talebi, gerekli tüm bilgileri, diğerleri yanında özellikle aşağıdakilerle ilgili bilgileri içerir:

a) Talepte bulunanın isim ve adresi ile bu kişiyi belirlemeye yarayan tüm hususlar,

b) Talebin konusu kişisel verilerin yer aldığı otomatik dosya veya yöneticisi,

c) Talebin amacı.

Madde 15

Tayin edilen makamlarca sağlanan yardıma ilişkin güvenceler

1. Bir Tarafın tayin ettiği makam, ne kendisine muhatap bir yardım talebini desteklemek amacıyla talebe eklenen bilgiyi, ne de kendi talep ettiği yardım üzerine diğer bir Tarafın tayin ettiği makamdan sağladığı bilgiyi, yardım talebinde belirtilen amaçlar dışında kullanabilir.

2. Taraflardan her biri, tayin edilen makamın personelinin veya bu makam adına hareket eden kişilerin, bu bilgilerin gizli tutulması veya paylaşılmaması hususunda yükümlülüklerine tabi olmasını sağlayacaktır.

3. Tayin edilen makam hiçbir durumda, 14. maddenin 2. fıkrasına göre yabancı ülkede ika eden ilgili kişinin muvafakatini almadan, kendi inisiyatifıyla bu kişi adına yardım talebinde bulunmaya yetkili kılınmayacaktır.

Madde-16

Yardım taleplerinin reddi

İşbu Sözleşmenin 13 ve 14. maddeleri uyarınca kendisine yardım talebi intikal eden tayin edilmiş makam, aşağıdaki durumlar dışında yardım talebini reddedemez:

- a) Yapılan talep, yanıt vermekle sorumlu makamın verilerin korunması konusundaki yetkisi dışında kalıyorsa;
- b) Talep, işbu Sözleşme hükümlerine uygun değilse;
- c) Talebin yerine getirilmesi, bunu yerine getirecek makamın bağlı olduğu devletin egemenliğine, güvenliğine veya kamu düzenine veya bu devletin yetkisi altındaki kişilerin haklarına ve temel özgürlüklerine aykırı ise.

Madde 17

Yardım giderleri ve yöntemleri

1. Tarafların 13. madde uyarınca birbirlerine yaptıkları karşılıklı yardım ile 14. madde uyarınca yabancı ülkede ikamet eden ilgili kişilere yaptıkları yardım, uzman ve tercüman ücretleri dışında, hiçbir masraf veya harcı gerektirmeyecektir. Bu masraf ve harçlar, yardım talebinde bulunan makamı tayin eden Tarafça karşılanacaktır.
2. İlgili kişi, bir başka Tarafın ülkesinde kendi hesabına yapılan işlemlerle ilgili olarak, bu Tarafın ülkesinde ikamet eden kişilerce yasal olarak ödenmesi gereken harç ve masraf dışında, hiçbir harç ve masraf ödemek zorunda olmayacaktır.
3. Yardımla ilgili diğer hususlar ve özellikle yardımın şekli ve usulü ile kullanılacak dile ilişkin konular, ilgili Taraflar arasında doğrudan kararlaştırılacaktır.

Bölüm V

Danışma Komitesi

Madde 18

Komitenin oluşumu

1. İşbu Sözleşmenin yürürlüğe girmesinden sonra bir Danışma Komitesi kurulur.
2. Taraflardan her biri, bu komiteye bir asıl temsilci, bir de temsilci vekili tayin eder. Sözleşmeye taraf olmayan Avrupa Konseyi üyesi her devlet Danışma Komitesinde bir gözlemci tarafından temsil edilme hakkına sahiptir.

3. Danışma Komitesi, oybirliği ile alacağı bir kararla, Avrupa Konseyi üyesi olmayan ve Sözleşmeye taraf olmayan herhangi bir devleti, belli bir oturumunda bir gözlemci tarafından temsil edilmeye davet edebilir.

Madde 19

Komitenin işlevleri

Danışma Komitesi:

- a. Sözleşmenin uygulanmasını kolaylaştırmak veya iyileştirmek amacıyla önerilerde bulunabilir;
- b. Aşağıdaki 21. Maddeye uygun olarak Sözleşmede değişiklik yapılmasını önerebilir;
- c. Sözleşmede değişiklik yapılmasına ilişkin olarak 21. maddenin 3. fıkrası uyarınca kendisine sunulan tüm öneriler hakkında görüş bildirir;
- d. Taraflardan birinin talebi üzerine, işbu Sözleşmenin uygulanması ile ilgili tüm sorular hakkında görüş bildirebilir.

Madde 20

Usul

1. Danışma Komitesi, Avrupa Konseyi Genel Sekreteri tarafından toplantıya çağırılır. Komite ilk toplantısını, işbu Sözleşmenin yürürlüğe girmesini izleyen on iki ay içerisinde yapar. Komite, müteakip toplantılarını en az iki yılda bir yapar; ayrıca Tarafların temsilcilerinin üçte birinin talebi üzerine herhangi bir zamanda toplanır.
2. Danışma Komitesi toplantısı yeter sayısı, Taraf temsilcilerinin salt çoğunluğudur.
3. Danışma Komitesi, her toplantı sonunda, yaptığı çalışmalar ve Sözleşmenin işleyişi hakkında Avrupa Konseyi Bakanlar Komitesine bir rapor sunar.
4. İşbu Sözleşme hükümlerine tabi olmak üzere Danışma Komitesi iç tüzüğünü kendisi düzenler.

Bölüm VI

Değişiklikler

Madde 21

Değişiklikler

1. Taraflardan biri, Avrupa Konseyi Bakanlar Komitesi veya Danışma Komitesi işbu Sözleşmede değişiklik yapılmasını önerebilir.

2. Her deęişiklik önerisi, Avrupa Konseyi Genel Sekreteri tarafından, Avrupa Konseyi üyesi Devletlere ve 23. madde hükümleri uyarınca Sözleşmeye katılan veya katılmaya çağrılan üye olmayan her devlete bildirilir.

3. Taraflardan biri veya Bakanlar Komitesi tarafından yapılan her deęişiklik önerisi, Bakanlar Komitesine deęişiklik hakkında görüş sunacak olan Danışma Komitesine bildirilir.

4. Bakanlar Komitesi, teklif edilen deęişikliği ve Danışma Komitesi tarafından sunulabilecek her türlü görüşü dikkate alarak söz konusu deęişikliği kabul edebilir.

5. Bakanlar Komitesi tarafından bu maddenin 4. fıkrasına göre kabul edilen her türlü deęişiklik metni, kabul için Taraflara iletilir.

6 İşbu Maddenin 4. fıkrası uyarınca kabul edilen herhangi bir deęişiklik, tüm Tarafların bununu kabul ettiklerini Genel Sekretere bildirmelerini izleyen otuzuncu günde yürürlüğe girer.

Bölüm XI,

Son hükümler

Madde 22

Yürürlüğe girme

1 İşbu Sözleşme Avrupa Konseyi üyesi devletlerin imzasına açıktır. Onay, kabul ya da uygun bulmaya tabidir. Onay, kabul ya da uygun bulma belgeleri, Avrupa Konseyi Genel Sekreterine teslim edilir.

2 Bu Sözleşme, en az beş Avrupa Konseyi üye devletinin önceki fıkranın hükümlerine göre Sözleşmeyle bağlı olma yönündeki muvafakatlerini ifade ettikleri tarihten itibaren üç aylık sürenin sona ermesini takip eden ayın ilk günü yürürlüğe girer.

3. Daha sonra Sözleşme ile bağlı olmak istediğini beyan eden herhangi bir üye devlet bakımından Sözleşme; onay, kabul ya da uygun bulma belgesini teslim etme tarihinden itibaren üç aylık sürenin sona ermesini takip eden ayın ilk günü yürürlüğe girer.

Madde 23

Üye olmayan devletlerin katılımı

1. İşbu Sözleşmenin yürürlüğe girmesinden sonra, Avrupa Konseyi Bakanlar Komitesi, Avrupa Konseyi Statüsünün 20. maddesinin d. fıkrasında öngörülen çoğunlukla ve komiteye katılma hakkına

sahip Taraf Devlet temsilcilerinin oybirliđiyle Avrupa Konseyine üye olmayan herhangi bir Devleti işbu Sözleşmeye katılmaya davet edebilir.

2. Katılan her Devlet için Sözleşme, katılma belgesinin Avrupa Konseyi Genel Sekreterine tevdi edildiđi tarihten sonraki üç aylık dönemin bitimini izleyen ayın ilk günü yürürlüđe girer.

Madde 24

Ülkesel hükümler

1. Herhangi bir Devlet, imza sırasında veya onay, kabul, uygun bulma veya taraf olma belgelerini tevdi ederken, Sözleşmenin uygulanacağı ülkeyi veya ülkeleri belirtebilir.

2. Herhangi bir Devlet, daha sonraki bir tarihte Avrupa Konseyi Genel Sekreterine muhatap bir bildirimle, işbu Sözleşmenin uygulama alanını, bildirimde belirtilen başka herhangi bir ülkeye teşmil edebilir. Sözleşme, sözkonusu ülke bakımından, söz konusu beyanın Genel Sekreter tarafından alınma tarihinden itibaren üç aylık sürenin sona ermesini takip eden ayın ilk günü yürürlüđe girer.

3. Önceki iki fıkra uyarınca yapılan herhangi bildirim, sözkonusu bildirimde belirtilen herhangi bir ülke bakımından Avrupa Konseyi Genel Sekreterine muhatap bir bildirim ile geri çekilebilir. Sözkonusu geri çekme, sözkonusu bildirim Genel Sekreter tarafından alınma tarihinden itibaren altı aylık sürenin sona ermesini takip eden ayın ilk günü geçerlilik kazanır.

Madde 25

Çekinceler

İşbu Sözleşme hükümlerine hiçbir çekince konulamaz.

Madde 26

Fesih

1. Taraflardan herhangi biri, herhangi bir zamanda Avrupa Konseyi Genel Sekreterine muhatap bir bildirim yoluyla bu Sözleşmeyi feshedebilir.

2. Söz konusu fesih, söz konusu bildirim Genel Sekreter tarafından alınma tarihinden itibaren altı aylık sürenin sona ermesini takip eden ayın ilk günü geçerlilik kazanır.

Madde 27

Bildirimler

Avrupa Konseyi Genel Sekreteri Konsey üyesi Devletlere ve bu Sözleşmeye katılan her Devlete aşağıdakileri bildirecektir:

- a. her imzayı;
- b. tevdi edilen her onay, kabul, uygun bulma veya taraf olma belgesini;
- c. MADDE 22, 23 ve 24 uyarınca her yürürlüğe giriş tarihini;
- d. bu Sözleşme ile ilgili diğer her tür belge, bildirim ya da muhaberatı.

Keyfiyeti tevsiken, usulüne uygun olarak yetkilendirilmiş Sözleşmeyi imzalamışlardır.

Strazburg'da 28 Ocak 1981 tarihinde İngilizce ve Fransızca dillerinde ve her iki metin eşit derecede geçerli olacak şekilde, Avrupa Konseyi arşivlerinde saklanmak üzere tek nüsha olarak imzalanmıştır. Avrupa Konseyi Genel Sekreteri, her bir Avrupa Konseyi üye Devletine ve Sözleşmeye taraf olmaya davet edilen her Devlete onaylı nüshalarını gönderecektir.

Avrupa Konseyi - 108 nolu Sözleşme (İngilizce)

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data European Treaty Series - No. 108

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
Strasbourg, 28.I.1981

Preamble

The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:

Chapter I - General provisions

Article 1 - Object and purpose

The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

Article 2 - Definitions

For the purposes of this Convention:

a- "personal data" means any information relating to an identified or identifiable individual ("data subject");

b- "automated data file" means any set of data undergoing automatic processing;

c- "automatic processing" includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination;

d- "controller of the file" means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.

Article 3 - Scope

1- The Parties undertake to apply this Convention to automated personal data files and automatic processing of personal data in the public and private sectors.

2- Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:

a- that it will not apply this Convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law;

b- that it will also apply this Convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality;

c- that it will also apply this Convention to personal data files which are not processed automatically.

3- Any State which has extended the scope of this Convention by any of the declarations provided for in sub-paragraph 2.b or c above may give notice in the said declaration that such extensions shall apply only to certain categories of personal data files, a list of which will be deposited.

4- Any Party which has excluded certain categories of automated personal data files by a declaration provided for in sub-paragraph 2.a above may not claim the application of this Convention to such categories by a Party which has not excluded them.

5- Likewise, a Party which has not made one or other of the extensions provided for in subparagraphs 2.b and c above may not claim the application of this Convention on these points with respect to a Party which has made such extensions.

6- The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the Convention with regard to the State which has made them if they have been made at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been made at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.

Chapter II - Basic principles for data protection

Article 4 - Duties of the Parties

1- Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.

2- These measures shall be taken at the latest at the time of entry into force of this Convention in respect of that Party.

Article 5 - Quality of data

Personal data undergoing automatic processing shall be:

a- obtained and processed fairly and lawfully;

b- stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c- adequate, relevant and not excessive in relation to the purposes for which they are stored;

d- accurate and, where necessary, kept up to date;

e- preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6 - Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law

provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Article 7 - Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

Article 8 - Additional safeguards for the data subject

Any person shall be enabled:

a- to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b- to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c- to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention;

d- to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

Article 9 - Exceptions and restrictions

1- No exception to the provisions of Articles 5, 6 and 8 of this Convention shall be allowed except within the limits defined in this article.

2- Derogation from the provisions of Articles 5, 6 and 8 of this Convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a- protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b- protecting the data subject or the rights and freedoms of others.

3- Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific

research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

Article 10 - Sanctions and remedies

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

Article 11 - Extended protection

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this Convention.

Chapter III - Transborder data flows

Article 12 - Transborder flows of personal data and domestic law

1- The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.

2- A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.

3- Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:

a- insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;

b- when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

Chapter IV - Mutual assistance

Article 13 - Co-operation between Parties

1- The Parties agree to render each other mutual assistance in order to implement this Convention.

2- For that purpose:

a- each Party shall designate one or more authorities, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe;

b- each Party which has designated more than one authority shall specify in its communication referred to in the previous sub-paragraph the competence of each authority.

3- An authority designated by a Party shall at the request of an authority designated by another Party:

a- furnish information on its law and administrative practice in the field of data protection;

b- take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed.

Article 14 - Assistance to data subjects resident abroad

1- Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this Convention.

2- When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the authority designated by that Party.

3- The request for assistance shall contain all the necessary particulars, relating inter alia to:

a- the name, address and any other relevant particulars identifying the person making the request;

b- the automated personal data file to which the request pertains, or its controller;

c- the purpose of the request.

Article 15 - Safeguards concerning assistance rendered by designated authorities

1- An authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information for purposes other than those specified in the request for assistance.

2- Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information.

3- In no case may a designated authority be allowed to make under Article 14, paragraph 2, a request for assistance on behalf of a data subject resident abroad, of its own accord and without the express consent of the person concerned.

Article 16 - Refusal of requests for assistance

A designated authority to which a request for assistance is addressed under Articles 13 or 14 of this Convention may not refuse to comply with it unless:

- a- the request is not compatible with the powers in the field of data protection of the authorities responsible for replying;
- b- the request does not comply with the provisions of this Convention;
- c- compliance with the request would be incompatible with the sovereignty, security or public policy (ordre public) of the Party by which it was designated, or with the rights and fundamental freedoms of persons under the jurisdiction of that Party.

Article 17 - Costs and procedures of assistance

1- Mutual assistance which the Parties render each other under Article 13 and assistance they render to data subjects abroad under Article 14 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party which has designated the authority making the request for assistance.

2- The data subject may not be charged costs or fees in connection with the steps taken on his behalf in the territory of another Party other than those lawfully payable by residents of that Party.

3- Other details concerning the assistance relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.

Chapter V - Consultative Committee

Article 18 - Composition of the committee

1- A Consultative Committee shall be set up after the entry into force of this Convention.

2- Each Party shall appoint a representative to the committee and a deputy representative. Any member State of the Council of Europe which is not a Party to the Convention shall have the right to be represented on the committee by an observer.

3- The Consultative Committee may, by unanimous decision, invite any non-member State of the Council of Europe which is not a Party to the Convention to be represented by an observer at a given meeting.

Article 19 - Functions of the committee

The Consultative Committee:

- a- may make proposals with a view to facilitating or improving the application of the Convention;

- b-** may make proposals for amendment of this Convention in accordance with Article 21;
- c-** shall formulate its opinion on any proposal for amendment of this Convention which is referred to it in accordance with Article 21, paragraph 3;
- d-** may, at the request of a Party, express an opinion on any question concerning the application of this Convention.

Article 20 - Procedure

- 1-** The Consultative Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this Convention. It shall subsequently meet at least once every two years and in any case when one-third of the representatives of the Parties request its convocation.
- 2-** A majority of representatives of the Parties shall constitute a quorum for a meeting of the Consultative Committee.
- 3-** After each of its meetings, the Consultative Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the Convention.
- 4-** Subject to the provisions of this convention, the Consultative Committee shall draw up its own Rules of Procedure.

Chapter VI - Amendments

Article 21 - Amendments

- 1-** Amendments to this Convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Consultative Committee.
- 2-** Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe and to every non-member State which has acceded to or has been invited to accede to this Convention in accordance with the provisions of Article 23.
- 3-** Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Consultative Committee, which shall submit to the Committee of Ministers its opinion on that proposed amendment.
- 4-** The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Consultative Committee and may approve the amendment.

5- The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance.

6- Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Chapter VII - Final clauses

Article 22 - Entry into force

1- This Convention shall be open for signature by the member States of the Council of Europe. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

2- This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five member States of the Council of Europe have expressed their consent to be bound by the Convention in accordance with the provisions of the preceding paragraph.

3- In respect of any member State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of ratification, acceptance or approval.

Article 23 - Accession by non-member States

1- After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this Convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee.

2- In respect of any acceding State, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 24 - Territorial clause

1- Any State may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2- Any State may at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following

the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.

3- Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.

Article 25 - Reservations

No reservation may be made in respect of the provisions of this Convention.

Article 26 - Denunciation

1- Any Party may at any time denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2- Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.

Article 27 - Notifications

The Secretary General of the Council of Europe shall notify the member States of the Council and any State which has acceded to this Convention of:

- a- any signature;
- b- the deposit of any instrument of ratification, acceptance, approval or accession;
- c- any date of entry into force of this Convention in accordance with Articles 22, 23 and 24;
- d- any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Strasbourg, the 28th day of January 1981, in English and in French, both texts being equally authoritative, in a single copy which shall remain deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe and to any State invited to accede to this Convention.

Avrupa Konseyi - 108 nolu Sözleşmeye Ek Protokol

108 nolu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol (181 nolu Sözleşme)

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows / 08.11.2011

Türkiye, sözleşmeyi 08.11.2001 tarihinde imzalamış ve 05.05.2016 tarihli 29703 sayılı Resmi Gazete'de yayımlanarak iç hukuka dâhil edilmiştir.

Giriş

Strazburg'da 28 Ocak 1981 tarihinde imzaya açılan Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin (bundan böyle "Sözleşme" olarak anılacaktır) tarafları;

Görevlerini tam bağımsızlıkla yerine getiren denetleyici makamların, kişisel verilerin işlenmesi karşısında bireylerin etkili şekilde korunmasının bir unsurunu teşkil ettiklerine kani olarak;

Toplumlar arasındaki bilgi akışının önemini göz önüne alarak;

Ulusal sınırlar arasında kişisel veri alışverişinin artmasıyla, insan haklarının ve temel özgürlüklerin ve özellikle de kişisel veri alışverişi karşısında özel hayatın gizliliği hakkının etkili şekilde korunmasını sağlamanın gerekliliğini göz önüne alarak;

Aşağıdaki hususlarda anlaşmaya varmışlardır:

Madde 1 - Denetleyici Makamlar

1. Taraf devletler, Sözleşme'nin II. ve III. bölümlerinde ve bu Protokol'de belirtilen ilkeleri uygulamaya koyan iç hukukundaki önlemlere uyulmasını sağlamakla yükümlü bir ya da daha fazla yetkili makam belirler.

2. a) Bu amaçla, söz konusu makamlar soruşturma ve müdahale yetkilerinin yanı sıra, kanuni takibata dâhil olma ya da bu Protokol'ün 1. Maddesinin I. fıkrasında 'belirtilen ilkeleri uygulamaya koyan iç hukuk hükümlerinin ihlallerini yetkili adli makamların dikkatine getirme yetkisine sahiptir.

b) Her denetleyici makam, yetkileri dahilinde, kişisel verilerin işlenmesi karşısında her kişinin haklarının ve temel özgürlüklerinin korunmasına dair taleplerini dinler.

3. Denetleyici makamlar görevlerini tam bağımsızlıkla yerine getirir.

4. Denetleyici makamların şikayetlere yol açan kararlarına mahkemeler yoluyla itiraz edilebilir.

5. IV. Bölüm hükümlerine uygun olarak ve Sözleşme'nin 13. Maddesinin hükümlerine hâlel getirmeksizin, denetleyici makamlar görevlerinin yerine getirilmesinin gerektirdiği ölçüde, özellikle tüm faydalı bilgileri teati ederek birbirleriyle işbirliği yaparlar.

Madde 2 - Sözleşme Taraflarından Birinin Yetki Alanına Tabi Olmayan Bir Alıcıya Sınıraşan Kişisel Veri Akışı

1. Taraf devletler, Sözleşme'ye taraf olmayan bir devletin ya da kuruluşun yetki alanına tabi bir alıcıya, yalnızca bu devletin ya da kuruluşun hedeflenen veri transferinin yeterli seviyede korunmasını garanti etmesi durumunda, kişisel veri transferi yapılmasını sağlar.

2. Bu Protokol'ün 2. Maddesinin 1. Fıkrasından derogasyon yoluyla taraflardan her biri:

a) iç hukukun:

- veri sahibinin belirli menfaatleri veya

- özellikle önemli kamu menfaatleri olmak üzere meşru üstün menfaatler nedeniyle öngörmesi veya

b) bilhassa akdi hükümlerden kaynaklanabilecek güvencelerin transferden sorumlu kontrolör tarafından sağlanması ve iç hukuka uygun olarak bunların yetkili makamlarca yeterli bulunması durumunda kişisel veri akışına müsaade edebilir.

Madde 3 - Nihai Hükümler

1. Bu Protokol'ün 1. Ve 2. Maddelerinin hükümleri, taraflarca Sözleşme'ye ek maddeler olarak kabul edilir ve Sözleşme'nin tüm hükümleri buna göre uygulanır.

2. Bu Protokol, Sözleşme'nin İmzacı Devletlerinin imzasına açıktır. Koşulları uyarınca Sözleşme'ye katılmalarının ardından Avrupa Toplulukları bu Protokol'ü imzalayabilir. Bu Protokol, onaya, kabule veya uygun bulmaya tabidir. Bu Protokol'e İmzacı Taraf daha önce ya da eş zamanlı olarak Sözleşme'yi onaylamamış, kabul etmemiş ya da uygun bulmamış ya da Sözleşme'ye katılmamış ise bu Protokol'ü onaylayamaz, kabul edemez ya da uygun bulamaz. Bu Protokol'e ilişkin onay, kabul veya uygun bulma belgeleri, Avrupa Konseyi Genel Sekreterine tevdi edilir.

3. a) Bu Protokol, beş İmzacı Tarafın 3. Maddenin 2. fıkrası hükümleri uyarınca Protokol'e tabi olmak için rızalarını ifade ettikleri tarihi takip eden üç aylık sürenin dolmasını takip eden ayın ilk günü yürürlüğe girer.

b) Daha sonradan Protokol'e bağlı olmak için rızasını ifade eden bir İmzacı Taraf bakımından Protokol; onay, kabul ya da uygun bulma belgesini tevdi etme tarihinden itibaren üç aylık sürenin sona ermesini takip eden ayın ilk günü yürürlüğe girer.

4. a) Bu Protokol'ün yürürlüğe girmesinden sonra, Sözleşme'ye katılan herhangi bir Devlet Protokol'e de katılabilir.

b) Katılma, katılım belgesinin Avrupa Konseyi Genel Sekreterine tevdi edildiği tarihten sonraki üç aylık dönemin bitimini izleyen ayın ilk günü yürürlüğe girer.

5. a) Taraflardan herhangi biri bu Protokol'ü Avrupa Konseyi Genel Sekreterine muhatap bir bildirim yoluyla herhangi bir tarihte feshedebilir.

b) Söz konusu fesih Avrupa Konseyi Genel Sekreterine atfedilen bildirim kabul edilme tarihinden sonraki üç aylık sürenin dolmasını takip eden ayın ilk günü yürürlüğe girer.

6. Avrupa Konseyi Genel Sekreteri Konsey üyesi Devletlere, Avrupa Topluluklarına ve bu Protokol'e katılan her Devlete aşağıdakileri bildiri:

a) Her imzayı

b) Tevdi edilen her onay, kabul ve uygun bulma belgesini;

c) Bu Protokol'ün 3. Maddeye göre yürürlüğe girdiği her tarihi;

d) Bu Protokol ile ilgili diğer her türlü belge, bildirim ya da muhaberatı.

Yukarıdaki hususları tasdiklen, usulüne uygun olarak yetkilendirilmiş aşağıda imzaları bulunanlar, bu Protokol'ü imzalamışlardır.

Avrupa Konseyi arşivinde saklanmak ve her iki metin de aynı derecede geçerli olmak üzere İngilizce ve Fransızca tek nüsha halinde 8 Kasım 2001 tarihinde Strazburg'da düzenlenmiştir. Avrupa Konseyi Genel Sekreteri, her bir Avrupa Konseyi üye Devletine, Avrupa Topluluklarına ve Protokol'e katılmaya davet edilen her devlete onaylı nüshalarını gönderir.

Avrupa Konseyi - 108 nolu Sözleşmeye Ek Protokol (İngilizce)

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (European Treaty Series - No. 181)

Preamble

The Parties to this additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature in Strasbourg on 28 January 1981 (hereafter referred to as "the Convention");

Convinced that supervisory authorities, exercising their functions in complete independence, are an element of the effective protection of individuals with regard to the processing of personal data;

Considering the importance of the flow of information between peoples;

Considering that, with the increase in exchanges of personal data across national borders, it is necessary to ensure the effective protection of human rights and fundamental freedoms, and in particular the right to privacy, in relation to such exchanges of personal data,

Have agreed as follows:

Article 1 - Supervisory authorities

1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.

2. a. To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.

b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.

3. The supervisory authorities shall exercise their functions in complete independence.

4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.

5. In accordance with the provisions of Chapter IV, and without prejudice to the provisions of Article 13 of the Convention, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

Article 2 - Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention

1. Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer.

2. By way of derogation from paragraph 1 of Article 2 of this Protocol, each Party may allow for the transfer of personal data:

a. if domestic law provides for it because of :

- specific interests of the data subject, or

- legitimate prevailing interests, especially important public interests, or

b. if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.

Article 3 - Final provisions

1. The provisions of Articles 1 and 2 of this Protocol shall be regarded by the Parties as additional articles to the Convention and all the provisions of the Convention shall apply accordingly.

2. This Protocol shall be open for signature by States Signatories to the Convention. After acceding to the Convention under the conditions provided by it, the European Communities may sign this Protocol. This Protocol is subject to ratification, acceptance or approval. A Signatory to this Protocol may not ratify, accept or approve it unless it has previously or simultaneously ratified, accepted or approved the Convention or has acceded to it. Instruments of ratification, acceptance or approval of this Protocol shall be deposited with the Secretary General of the Council of Europe.

3. a. This Protocol shall enter into force on the first day of the month following the expiry of a period of three months after the date on which five of its Signatories have expressed their consent to be bound by the Protocol in accordance with the provisions of paragraph 2 of Article 3.

b. In respect of any Signatory to this Protocol which subsequently expresses its consent to be bound by it, the Protocol shall enter into force on the first day of the month following the expiry of a period of three months after the date of deposit of the instrument of ratification, acceptance or approval.

4. a. After the entry into force of this Protocol, any State which has acceded to the Convention may also accede to the Protocol.

b. Accession shall be effected by the deposit with the Secretary General of the Council of Europe of an instrument of accession, which shall take effect on the first day of the month following the expiry of a period of three months after the date of its deposit.

5. a. Any Party may at any time denounce this Protocol by means of a notification addressed to the Secretary General of the Council of Europe.

b. Such denunciation shall become effective on the first day of the month following the expiry of a period of three months after the date of receipt of such notification by the Secretary General.

6. The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the European Communities and any other State which has acceded to this Protocol of:

a. any signature;

b. the deposit of any instrument of ratification, acceptance or approval;

c. any date of entry into force of this Protocol in accordance with Article 3;

d. any other act, notification or communication relating to this Protocol.

In witness whereof the undersigned, being duly authorised thereto, have signed this Protocol.

Done at Strasbourg, this 8th day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, the European Communities and any State invited to accede to the Convention.

Avrupa Konseyi - 108+ Sözleşmesi (108 Plus)

Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data

128th Session of the Committee of Ministers (Elsinore, Denmark, 17-18 May 2018)

Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data - Consolidated text

Preamble

The member States of the Council of Europe, and the other signatories hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is necessary to secure the human dignity and protection of the human rights and fundamental freedoms of every individual and, given the diversification, intensification and globalisation of data processing and personal data flows, personal autonomy based on a person's right to control of his or her personal data and the processing of such data;

Recalling that the right to protection of personal data is to be considered in respect of its role in society and that it has to be reconciled with other human rights and fundamental freedoms, including freedom of expression;

Considering that this Convention permits account to be taken, in the implementation of the rules laid down therein, of the principle of the right of access to official documents;

Recognising that it is necessary to promote at the global level the fundamental values of respect for privacy and protection of personal data, thereby contributing to the free flow of information between people;

Recognising the interest of a reinforcement of international co-operation between the Parties to the Convention,

Have agreed as follows:

Chapter I - General provisions

Article 1 - Object and purpose

The purpose of this Convention is to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy.

Article 2 - Definitions

For the purposes of this Convention:

- a. "personal data" means any information relating to an identified or identifiable individual ("data subject");
- b. "data processing" means any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data;
- c. Where automated processing is not used, "data processing" means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria;
- d. "controller" means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has decision-making power with respect to data processing;
- e. "recipient" means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;
- f. "processor" means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.

Article 3 - Scope

1. Each Party undertakes to apply this Convention to data processing subject to its jurisdiction in the public and private sectors, thereby securing every individual's right to protection of his or her personal data.
2. This Convention shall not apply to data processing carried out by an individual in the course of purely personal or household activities.

Chapter II - Basic principles for the protection of personal data

Article 4 - Duties of the Parties

1. Each Party shall take the necessary measures in its law to give effect to the provisions of this Convention and secure their effective application.

2. These measures shall be taken by each Party and shall have come into force by the time of ratification or of accession to this Convention.

3. Each Party undertakes:

a. to allow the Convention Committee provided for in Chapter VI to evaluate the effectiveness of the measures it has taken in its law to give effect to the provisions of this Convention; and

b. to contribute actively to this evaluation process.

Article 5 - Legitimacy of data processing and quality of data

1. Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake.

2. Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law.

3. Personal data undergoing processing shall be processed lawfully.

4. Personal data undergoing processing shall be:

a. processed fairly and in a transparent manner;

b. collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes;

c. adequate, relevant and not excessive in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date;

e. preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.

Article 6 - Special categories of data

1. The processing of:

- genetic data;

- personal data relating to offences, criminal proceedings and convictions, and related security measures;
- biometric data uniquely identifying a person;
- personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life,

shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention.

2. Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.

Article 7 - Data security

1. Each Party shall provide that the controller, and, where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data.

2. Each Party shall provide that the controller notifies, without delay, at least the competent supervisory authority within the meaning of Article 15 of this Convention, of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.

Article 8 - Transparency of processing

1. Each Party shall provide that the controller informs the data subjects of:

- a. his or her identity and habitual residence or establishment;
- b. the legal basis and the purposes of the intended processing;
- c. the categories of personal data processed;
- d. the recipients or categories of recipients of the personal data, if any; and
- e. the means of exercising the rights set out in Article 9,

as well as any necessary additional information in order to ensure fair and transparent processing of the personal data.

2. Paragraph 1 shall not apply where the data subject already has the relevant information.

3. Where the personal data are not collected from the data subjects, the controller shall not be required to provide such information where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts.

Article 9 - Rights of the data subject

1. Every individual shall have a right:

a. not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration;

b. to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with Article 8, paragraph 1;

c. to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her;

d. to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms;

e. to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this Convention;

f. to have a remedy under Article 12 where his or her rights under this Convention have been violated;

g. to benefit, whatever his or her nationality or residence, from the assistance of a supervisory authority within the meaning of Article 15, in exercising his or her rights under this Convention.

2. Paragraph 1.a shall not apply if the decision is authorised by a law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

Article 10 - Additional obligations

1. Each Party shall provide that controllers and, where applicable, processors, take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate, subject to the domestic legislation adopted in accordance with Article 11, paragraph 3, in particular to the

competent supervisory authority provided for in Article 15, that the data processing under their control is in compliance with the provisions of this Convention.

2. Each Party shall provide that controllers and, where applicable, processors, examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.

3. Each Party shall provide that controllers, and, where applicable, processors, implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.

4. Each Party may, having regard to the risks arising for the interests, rights and fundamental freedoms of the data subjects, adapt the application of the provisions of paragraphs 1, 2 and 3 in the law giving effect to the provisions of this Convention, according to the nature and volume of the data, the nature, scope and purpose of the processing and, where appropriate, the size of the controller or processor.

Article 11 - Exceptions and restrictions

1. No exception to the provisions set out in this Chapter shall be allowed except to the provisions of Article 5 paragraph 4, Article 7 paragraph 2, Article 8 paragraph 1 and Article 9, when such an exception is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for:

a. the protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest;

b. the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.

2. Restrictions on the exercise of the provisions specified in Articles 8 and 9 may be provided for by law with respect to data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes when there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects.

3. In addition to the exceptions allowed for in paragraph 1 of this article, with reference to processing activities for national security and defense purposes, each Party may provide, by law and only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfill such aim, exceptions to Article 4 paragraph 3, Article 14 paragraphs 5 and 6 and Article 15, paragraph 2, litterae a, b, c and d.

This is without prejudice to the requirement that processing activities for national security and defense purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party.

Article 12 - Sanctions and remedies

Each Party undertakes to establish appropriate judicial and non-judicial sanctions and remedies for violations of the provisions of this Convention.

Article 13 - Extended protection

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this Convention.

Chapter III - Transborder flows of personal data

Article 14 - Transborder flows of personal data

1. A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may, however, do so if there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention. A Party may also do so, if bound by harmonised rules of protection shared by States belonging to a regional international organisation.

2. When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to this Convention, the transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Convention is secured.

3. An appropriate level of protection can be secured by:

a. the law of that State or international organisation, including the applicable international treaties or agreements; or

b. ad hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing.

4. Notwithstanding the provisions of the previous paragraphs, each Party may provide that the transfer of personal data may take place if:

a. the data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards; or

b. the specific interests of the data subject require it in the particular case; or

c. prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society; or

d. it constitutes a necessary and proportionate measure in a democratic society for freedom of expression.

5. Each Party shall provide that the competent supervisory authority within the meaning of Article 15 of this Convention is provided with all relevant information concerning the transfers of data referred to in paragraph 3.b and, upon request, paragraphs 4.b and 4.c.

6. Each Party shall also provide that the supervisory authority is entitled to request that the person who transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests and that the supervisory authority may, in order to protect the rights and fundamental freedoms of data subjects, prohibit such transfers, suspend them or subject them to condition.

Chapter IV - Supervisory authorities

Article 15 - Supervisory authorities

1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the provisions of this Convention.

2. To this end, such authorities:

a. shall have powers of investigation and intervention;

b. shall perform the functions relating to transfers of data provided for under Article 14, notably the approval of standardised safeguards;

c. shall have powers to issue decisions with respect to violations of the provisions of this Convention and may, in particular, impose administrative sanctions;

d. shall have the power to engage in legal proceedings or to bring to the attention of the competent judicial authorities violations of the provisions of this Convention;

e. shall promote:

i. public awareness of their functions and powers as well as their activities;

ii. public awareness of the rights of data subjects and the exercise of such rights;

iii. awareness of controllers and processors of their responsibilities under this Convention;

specific attention shall be given to the data protection rights of children and other vulnerable individuals.

3. The competent supervisory authorities shall be consulted on proposals for any legislative or administrative measures which provide for the processing of personal data.

4. Each competent supervisory authority shall deal with requests and complaints lodged by data subjects concerning their data protection rights and shall keep data subjects informed of progress.

5. The supervisory authorities shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions.

6. Each Party shall ensure that the supervisory authorities are provided with the resources necessary for the effective performance of their functions and exercise of their powers.

7. Each supervisory authority shall prepare and publish a periodical report outlining its activities.

8. Members and staff of the supervisory authorities shall be bound by obligations of confidentiality with regard to confidential information to which they have access, or have had access to, in the performance of their duties and exercise of their powers.

9. Decisions of the supervisory authorities may be subject to appeal through the courts.

10. The supervisory authorities shall not be competent with respect to processing carried out by bodies when acting in their judicial capacity.

Chapter V - Co-operation and mutual assistance

Article 16 - Designation of supervisory authorities

1. The Parties agree to co-operate and render each other mutual assistance in order to implement this Convention.

2. For that purpose:

- a. each Party shall designate one or more supervisory authorities within the meaning of Article 15 of this Convention, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe;
- b. each Party which has designated more than one supervisory authority shall specify the competence of each authority in its communication referred to in the previous littera.

Article 17 - Forms of co-operation

1. The supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties and exercise of their powers, in particular by:
 - a. providing mutual assistance by exchanging relevant and useful information and co-operating with each other under the condition that, as regards the protection of personal data, all the rules and safeguards of this Convention are complied with;
 - b. co-ordinating their investigations or interventions, or conducting joint actions;
 - c. providing information and documentation on their law and administrative practice relating to data protection.
2. The information referred to in paragraph 1 shall not include personal data undergoing processing unless such data are essential for co-operation, or where the data subject concerned has given explicit, specific, free and informed consent to its provision.
3. In order to organise their co-operation and to perform the duties set out in the preceding paragraphs, the supervisory authorities of the Parties shall form a network.

Article 18 - Assistance to data subjects

1. Each Party shall assist any data subject, whatever his or her nationality or residence, to exercise his or her rights under Article 9 of this Convention.
2. Where a data subject resides on the territory of another Party, he or she shall be given the option of submitting the request through the intermediary of the supervisory authority designated by that Party.
3. The request for assistance shall contain all the necessary particulars, relating inter alia to:
 - a. the name, address and any other relevant particulars identifying the data subject making the request;
 - b. the processing to which the request pertains, or its controller;

c. the purpose of the request.

Article 19 - Safeguards

1. A supervisory authority which has received information from another supervisory authority, either accompanying a request or in reply to its own request, shall not use that information for purposes other than those specified in the request.

2. In no case may a supervisory authority be allowed to make a request on behalf of a data subject of its own accord and without the express approval of the data subject concerned.

Article 20 - Refusal of requests

A supervisory authority to which a request is addressed under Article 17 of this Convention may not refuse to comply with it unless:

a. the request is not compatible with its powers;

b. the request does not comply with the provisions of this Convention;

c. compliance with the request would be incompatible with the sovereignty, national security or public order of the Party by which it was designated, or with the rights and fundamental freedoms of individuals under the jurisdiction of that Party.

Article 21 - Costs and procedures

1. Co-operation and mutual assistance which the Parties render each other under Article 17 and assistance they render to data subjects under Articles 9 and 18 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party making the request.

2. The data subject may not be charged costs or fees in connection with the steps taken on his or her behalf in the territory of another Party other than those lawfully payable by residents of that Party.

3. Other details concerning the co-operation and assistance, relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.

Chapter VI - Convention Committee

Article 22 - Composition of the committee

1. A Convention Committee shall be set up after the entry into force of this Convention.

2. Each Party shall appoint a representative to the committee and a deputy representative. Any member State of the Council of Europe which is not a Party to the Convention shall have the right to be represented on the committee by an observer.

3. The Convention Committee may, by a decision taken by a majority of two-thirds of the representatives of the Parties, invite an observer to be represented at its meetings.

4. Any Party which is not a member of the Council of Europe shall contribute to the funding of the activities of the Convention Committee according to the modalities established by the Committee of Ministers in agreement with that Party.

Article 23 - Functions of the committee

The Convention Committee:

a. may make recommendations with a view to facilitating or improving the application of the Convention;

b. may make proposals for amendment of this Convention in accordance with Article 25;

c. shall formulate its opinion on any proposal for amendment of this Convention which is referred to it in accordance with Article 25, paragraph 3;

d. may express an opinion on any question concerning the interpretation or application of this Convention;

e. shall prepare, before any new accession to the Convention, an opinion for the Committee of Ministers relating to the level of personal data protection of the candidate for accession and, where necessary, recommend measures to take to reach compliance with the provisions of this Convention;

f. may, at the request of a State or an international organisation, evaluate whether the level of personal data protection the former provides is in compliance with the provisions of this Convention and, where necessary, recommend measures to be taken to reach such compliance;

g. may develop or approve models of standardised safeguards referred to in Article 14;

h. shall review the implementation of this Convention by the Parties and recommend measures to be taken in the case where a Party is not in compliance with this Convention;

i. shall facilitate, where necessary, the friendly settlement of all difficulties related to the application of this Convention.

Article 24 - Procedure

1. The Convention Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this Convention. It shall subsequently meet at least once a year, and in any case when one-third of the representatives of the Parties request its convocation.
2. After each of its meetings, the Convention Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of this Convention.
3. The voting arrangements in the Convention Committee are laid down in the elements for the Rules of Procedure appended to Protocol CETS No. [223].
4. The Convention Committee shall draw up the other elements of its Rules of Procedure and establish, in particular, the procedures for evaluation and review referred to in Article 4, paragraph 3, and Article 23, litterae e, f and h on the basis of objective criteria.

Chapter VII - Amendments

Article 25 - Amendments

1. Amendments to this Convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Convention Committee.
2. Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the Parties to this Convention, to the other member States of the Council of Europe, to the European Union and to every non-member State or international organisation which has been invited to accede to this Convention in accordance with the provisions of Article 27.
3. Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Convention Committee, which shall submit to the Committee of Ministers its opinion on that proposed amendment.
4. The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Convention Committee and may approve the amendment.
5. The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance.
6. Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.
7. Moreover, the Committee of Ministers may, after consulting the Convention Committee, decide unanimously that a particular amendment shall enter into force at the expiration of a period of three

years from the date on which it has been opened to acceptance, unless a Party notifies the Secretary General of the Council of Europe of an objection to its entry into force. If such an objection is notified, the amendment shall enter into force on the first day of the month following the date on which the Party to this Convention which has notified the objection has deposited its instrument of acceptance with the Secretary General of the Council of Europe.

Chapter VIII - Final clauses

Article 26 - Entry into force

1. This Convention shall be open for signature by the member States of the Council of Europe and by the European Union. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

2. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five member States of the Council of Europe have expressed their consent to be bound by the Convention in accordance with the provisions of the preceding paragraph.

3. In respect of any Party which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of ratification, acceptance or approval.

Article 27 - Accession by non-member States or international organisations

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may, after consulting the Parties to this Convention and obtaining their unanimous agreement, and in light of the opinion prepared by the Convention Committee in accordance with Article 23.e, invite any State not a member of the Council of Europe or an international organisation to accede to this Convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2. In respect of any State or international organisation acceding to this Convention according to paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 28 - Territorial clause

1. Any State, the European Union or other international organisation may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2. Any State, the European Union or other international organisation may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.

Article 29 - Reservations

No reservation may be made in respect of the provisions of this Convention.

Article 30 - Denunciation

1. Any Party may at any time denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2. Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.

Article 31 - Notifications

The Secretary General of the Council of Europe shall notify the member States of the Council and any Party to this Convention of:

- a. any signature;
- b. the deposit of any instrument of ratification, acceptance, approval or accession;
- c. any date of entry into force of this Convention in accordance with Articles 26, 27 and 28;
- d. any other act, notification or communication relating to this Convention.

Appendix to the Protocol: Elements for the Rules of Procedure of the Convention Committee

1. Each Party has a right to vote and shall have one vote.

2. A two-thirds majority of representatives of the Parties shall constitute a quorum for the meetings of the Convention Committee. In case the amending Protocol to the Convention enters into force in accordance with its Article 37 (2) before its entry into force in respect of all Contracting States to the Convention, the quorum for the meetings of the Convention Committee shall be no less than 34 Parties to the Protocol.
3. The decisions under Article 23 shall be taken by a four-fifths majority. The decisions pursuant to Article 23 littera h shall be taken by a four-fifths majority, including a majority of the votes of States Parties not members of a regional integration organisation that is a Party to the Convention.
4. Where the Convention Committee takes decisions pursuant to Article 23 littera h, the Party concerned by the review shall not vote. Whenever such a decision concerns a matter falling within the competence of a regional integration organisation, neither the organisation nor its member States shall vote.
5. Decisions concerning procedural issues shall be taken by a simple majority.
6. Regional integration organisations, in matters within their competence, may exercise their right to vote in the Convention Committee, with a number of votes equal to the number of their member States that are Parties to the Convention. Such an organisation shall not exercise its right to vote if any of its member States exercises its right.
7. In case of vote, all Parties must be informed of the subject and time for the vote, as well as whether the vote will be exercised by the Parties individually or by a regional integration organisation on behalf of its member States.
8. The Convention Committee may further amend its rules of procedure by a two-thirds majority, except for the voting arrangements which may only be amended by unanimous vote of the Parties and to which Article 25 of the Convention applies.

AVRUPA BİRLİĐİ

Bölüm İÇeriĐi

- Avrupa BirliĐi'nin İřleyiři Hakkında Anlařma
- Avrupa BirliĐi Temel Haklar řartı
- Avrupa BirliĐi Genel Veri Koruma TüzüĐü (GDPR)
- GDPR Recitals
- 95/46 sayılı Direktif (Türkçe)
- 95/46 sayılı Direktif (İngilizce)
- E-Mahremiyet Direktifi (E-Privacy Directive)
- Polis ve Yargı Kiřisel Veriler Direktifi (LED Directive)
- Açık Veri Direktifi (Open Data Directive)
- European Declaration on Digital Rights and Principles for the Digital Decade

Avrupa Birliđi'nin İřleyiři Hakkında Anlařma

The Treaty on the Functioning of the European Union

Article 16

(ex Article 286 TEC)

1. Everyone has the right to the protection of personal data concerning them.
2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

Avrupa Birliđi'nin İřleyiři Hakkında Anlařma

Madde 16

1. Herkes, kendisine iliřkin kiřisel verilerinin korunması hakkına sahiptir.
2. Avrupa Parlamentosu ve Konsey, Birlik hukuku kapsamına giren faaliyetlerin yurütulmesinde, Birlik kurum, organ, ofis veya ajansları ile üye devletler tarafından kiřisel verilerin iřlenmesi sırasında bireylerin korunmasına ve bu bilgilerin serbest dolařımına iliřkin kuralları olađan yasama usulü uyarınca belirler. Bu kurallara uyulması, bađımsız otoritelerin denetimine tabidir.

Bu maddeye dayanarak kabul edilen kurallar, Avrupa Birliđi Antlařması'nın 39. Maddesinde yer alan spesifik kurallara halel getirmez.

Avrupa Birliđi Temel Haklar Őartı

Charter of Fundamental Rights of the European Union

Official Journal, C 326/391, 26.10.2012

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Avrupa Birliđi Temel Haklar Őartı

Madde 8

KiŐisel verilerin korunması

1. Herkes, kendisiyle ilgili kiŐisel verilerinin korunması hakkına sahiptir.
2. Bu veriler belirli amaçlar için adil biçimde, ilgili kiŐinin rızasına ya da yasalarca belirlenmiŐ diđer meŐru temellere dayanarak iŐlenir. Herkes, kendisiyle ilgili toplanan verilere eriŐme ve bunları dŐzeltirme hakkına sahiptir.
3. Bu kurallara riayet etme, bađımsız bir otoritenin kontrolŐne tâbidir.

Avrupa Birliđi Genel Veri Koruma Tüzüđü (GDPR)

2016/679 sayılı Avrupa Birliđi Genel Veri Koruma Tüzüđü

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

4.5.2016 Official Journal of the European Union L 119/1

Chapter 1: General provisions

Article 1 - Subject-matter and objectives

Article 2 - Material scope

Article 3 - Territorial scope

Article 4 - Definitions

Chapter 2: Principles

Article 5 - Principles relating to processing of personal data

Article 6 - Lawfulness of processing

Article 7 - Conditions for consent

Article 8 - Conditions applicable to child's consent in relation to information society services

Article 9 - Processing of special categories of personal data

Article 10 - Processing of personal data relating to criminal convictions and offences

Article 11 - Processing which does not require identification

Chapter 3: Rights of the data subject

Section 1: Transparency and modalities

Article 12 - Transparent information, communication and modalities for the exercise of the rights of the data subject

Section 2: Information and access to personal data

Article 13 - Information to be provided where personal data are collected from the data subject

Article 14 - Information to be provided where personal data have not been obtained from the data subject

Article 15 - Right of access by the data subject

Section 3: Rectification and erasure

Article 16 - Right to rectification

Article 17 - Right to erasure ('right to be forgotten')

Article 18 - Right to restriction of processing

Article 19 - Notification obligation regarding rectification or erasure of personal data or restriction of processing

Article 20 - Right to data portability

Section 4: Right to object and automated individual decision-making

Article 21 - Right to object

Article 22 - Automated individual decision-making, including profiling

Section 5: Restrictions

Article 23 - Restrictions

Chapter 4: Controller and processor

Section 1: General obligations

Article 24 - Responsibility of the controller

Article 25 - Data protection by design and by default

Article 26 - Joint controllers

Article 27 - Representatives of controllers or processors not established in the Union

Article 28 - Processor

Article 29 - Processing under the authority of the controller or processor

Article 30 - Records of processing activities

Article 31 - Cooperation with the supervisory authority

Section 2: Security of personal data

Article 32 - Security of processing

Article 33 - Notification of a personal data breach to the supervisory authority

Article 34 - Communication of a personal data breach to the data subject

Section 3: Data protection impact assessment and prior consultation

Article 35 - Data protection impact assessment

Article 36 - Prior consultation

Section 4: Data protection officer

Article 37 - Designation of the data protection officer

Article 38 - Position of the data protection officer

Article 39 - Tasks of the data protection officer

Section 5: Codes of conduct and certification

Article 40 - Codes of conduct

Article 41 - Monitoring of approved codes of conduct

Article 42 - Certification

Article 43 - Certification bodies

Chapter 5: Transfers of personal data to third countries or international organisations

Article 44 - General principle for transfers

Article 45 - Transfers on the basis of an adequacy decision

Article 46 - Transfers subject to appropriate safeguards

Article 47 - Binding corporate rules

Article 48 - Transfers or disclosures not authorised by Union law

Article 49 - Derogations for specific situations

Article 50 - International cooperation for the protection of personal data

Chapter 6: Independent supervisory authorities

Section 1: Independent status

Article 51 - Supervisory authority

Article 52 - Independence

Article 53 - General conditions for the members of the supervisory authority

Article 54 - Rules on the establishment of the supervisory authority

Section 2: Competence, tasks and powers

Article 55 - Competence

Article 56 - Competence of the lead supervisory authority

Article 57 - Tasks

Article 58 - Powers

Article 59 - Activity reports

Chapter 7: Cooperation and consistency

Section 1: Cooperation

Article 60 - Cooperation between the lead supervisory authority and the other supervisory authorities concerned

Article 61 - Mutual assistance

Article 62 - Joint operations of supervisory authorities

Section 2: Consistency

Article 63 - Consistency mechanism

Article 64 - Opinion of the Board

Article 65 - Dispute resolution by the Board

Article 66 - Urgency procedure

Article 67 - Exchange of information

Section 3: European data protection board

Article 68 - European Data Protection Board

Article 69 - Independence

Article 70 - Tasks of the Board

Article 71 - Reports

Article 72 - Procedure

Article 73 - Chair

Article 74 - Tasks of the Chair

Article 75 - Secretariat

Article 76 - Confidentiality

Chapter 8: Remedies, liability and penalties

Article 77 - Right to lodge a complaint with a supervisory authority

Article 78 - Right to an effective judicial remedy against a supervisory authority

Article 79 - Right to an effective judicial remedy against a controller or processor

Article 80 - Representation of data subjects

Article 81 - Suspension of proceedings

Article 82 - Right to compensation and liability

Article 83 - General conditions for imposing administrative fines

Article 84 - Penalties

Chapter 9: Provisions relating to specific processing situations

Article 85 - Processing and freedom of expression and information

Article 86 - Processing and public access to official documents

Article 87 - Processing of the national identification number

Article 88 - Processing in the context of employment

Article 89 - Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Article 90 - Obligations of secrecy

Article 91 - Existing data protection rules of churches and religious associations

Chapter 10: Delegated acts and implementing acts

Article 92 - Exercise of the delegation

Article 93 - Committee procedure

Chapter 11: Final provisions

Article 94 - Repeal of Directive 95/46/EC

Article 95 - Relationship with Directive 2002/58/EC

Article 96 - Relationship with previously concluded Agreements

Article 97 - Commission reports

Article 98 - Review of other Union legal acts on data protection

Article 99 - Entry into force and application

CHAPTER I

General provisions

Article 1

Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Article 2

Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
2. This Regulation does not apply to the processing of personal data:

- (a) in the course of an activity which falls outside the scope of Union law;
 - (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
 - (c) by a natural person in the course of a purely personal or household activity;
 - (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.
3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.
4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
 - (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
 - (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Article 4

Definitions

For the purposes of this Regulation:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(6) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(10) 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(12) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(13) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(15) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(16) 'main establishment' means:

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

(17) 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

(18) 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

(19) 'group of undertakings' means a controlling undertaking and its controlled undertakings;

(20) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

(21) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51;

(22) 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority;

(23) 'cross-border processing' means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

(24) 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

(25) 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (19);

(26) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

CHAPTER II

Principles

Article 5

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, *inter alia*: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, *inter alia*:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7

Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8

Conditions applicable to child's consent in relation to information society services

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 9

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data

protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 10

Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Article 11

Processing which does not require identification

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.
2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

CHAPTER III

Rights of the data subject

Section 1

Transparency and modalities

Article 12

Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.
2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Section 2

Information and access to personal data

Article 13

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

- (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
- (b) the contact details of the data protection officer, where applicable;
- (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- (e) the recipients or categories of recipients of the personal data, if any;
- (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

- (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 14

Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the

Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

- (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- (b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- (c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
- (d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- (e) the right to lodge a complaint with a supervisory authority;
- (f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
- (g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

- (a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
- (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
- (c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Article 15

Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Section 3

Rectification and erasure

Article 16

Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 17

Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Article 18

Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 19

Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 20

Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Section 4

Right to object and automated individual decision-making

Article 21

Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 22

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Section 5

Restrictions

Article 23

Restrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- (a) national security;
- (b) defence;
- (c) public security;
- (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;
- (f) the protection of judicial independence and judicial proceedings;
- (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
- (i) the protection of the data subject or the rights and freedoms of others;
- (j) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

- (a) the purposes of the processing or categories of processing;
- (b) the categories of personal data;
- (c) the scope of the restrictions introduced;

- (d) the safeguards to prevent abuse or unlawful access or transfer;
- (e) the specification of the controller or categories of controllers;
- (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
- (g) the risks to the rights and freedoms of data subjects; and
- (h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

CHAPTER IV

Controller and processor

Section 1

General obligations

Article 24

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement

appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 26

Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Article 27

Representatives of controllers or processors not established in the Union

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

2. The obligation laid down in paragraph 1 of this Article shall not apply to:

(a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

(b) a public authority or body.

3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Article 28

Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

- (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
- (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- (c) takes all measures required pursuant to Article 32;
- (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
- (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
- (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
- (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
- (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other

processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 29

Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Article 30

Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

- (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- (b) the purposes of the processing;
- (c) a description of the categories of data subjects and of the categories of personal data;
- (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- (f) where possible, the envisaged time limits for erasure of the different categories of data;
- (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

- (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
- (b) the categories of processing carried out on behalf of each controller;
- (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Article 31

Cooperation with the supervisory authority

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

Section 2

Security of personal data

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- (a) the pseudonymisation and encryption of personal data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).
3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
 - (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
 - (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
 - (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Section 3

Data protection impact assessment and prior consultation

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and

freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.

1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Article 36

Prior consultation

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of

receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(b) the purposes and means of the intended processing;

(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

(d) where applicable, the contact details of the data protection officer;

(e) the data protection impact assessment provided for in Article 35; and

(f) any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

Section 4

Data protection officer

Article 37

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 38

Position of the data protection officer

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 39

Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Section 5

Codes of conduct and certification

Article 40

Codes of conduct

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

- (a) fair and transparent processing;
- (b) the legitimate interests pursued by controllers in specific contexts;
- (c) the collection of personal data;
- (d) the pseudonymisation of personal data;
- (e) the information provided to the public and to data subjects;
- (f) the exercise of the rights of data subjects;
- (g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;
- (h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;
- (i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;
- (j) the transfer of personal data to third countries or international organisations; or

(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.

11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

Article 41

Monitoring of approved codes of conduct

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6. This Article shall not apply to processing carried out by public authorities and bodies.

Article 42

Certification

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Article 43

Certification bodies

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

(a) the supervisory authority which is competent pursuant to Article 55 or 56;

(b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council (20) in accordance with EN-ISO/IEC 17065/2012 and with the

additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:

(a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

(b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;

(c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

(d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means.

7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

CHAPTER V

Transfers of personal data to third countries or international organisations

Article 44

General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Article 45

Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

Article 46

Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

- (a) a legally binding and enforceable instrument between public authorities or bodies;
- (b) binding corporate rules in accordance with Article 47;
- (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
- (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
- (e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- (f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

- (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
- (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Article 47

Binding corporate rules

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

(h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(i) the complaint procedures;

(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

Article 48

Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 49

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

- (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- (d) the transfer is necessary for important reasons of public interest;
- (e) the transfer is necessary for the establishment, exercise or defence of legal claims;
- (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

Article 50

International cooperation for the protection of personal data

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

- (a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;
- (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
- (c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;
- (d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

CHAPTER VI

Independent supervisory authorities

Section 1

Independent status

Article 51

Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').
2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.
3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 52

Independence

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

Article 53

General conditions for the members of the supervisory authority

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

-

their parliament;

-
their government;

-
their head of State; or

-
an independent body entrusted with the appointment under Member State law.

2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

Article 54

Rules on the establishment of the supervisory authority

1. Each Member State shall provide by law for all of the following:

(a) the establishment of each supervisory authority;

(b) the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;

(c) the rules and procedures for the appointment of the member or members of each supervisory authority;

(d) the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;

(f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.

Section 2

Competence, tasks and powers

Article 55

Competence

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Article 56

Competence of the lead supervisory authority

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates

only to an establishment in its Member State or substantially affects data subjects only in its Member State.

3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.

6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

Article 57

Tasks

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

- (f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;
- (g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;
- (h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;
- (i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;
- (j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);
- (k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);
- (l) give advice on the processing operations referred to in Article 36(2);
- (m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);
- (n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);
- (o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);
- (p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
- (q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
- (r) authorise contractual clauses and provisions referred to in Article 46(3);

- (s) approve binding corporate rules pursuant to Article 47;
- (t) contribute to the activities of the Board;
- (u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and
- (v) fulfil any other tasks related to the protection of personal data.

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 58

Powers

1. Each supervisory authority shall have all of the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(b) to carry out investigations in the form of data protection audits;

(c) to carry out a review on certifications issued pursuant to Article 42(7);

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

- (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
- (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
- (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
- (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
- (e) to order the controller to communicate a personal data breach to the data subject;
- (f) to impose a temporary or definitive limitation including a ban on processing;
- (g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
- (h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
- (i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;
- (j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

3. Each supervisory authority shall have all of the following authorisation and advisory powers:

- (a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;
- (b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;
- (c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;
- (d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

- (e) to accredit certification bodies pursuant to Article 43;
- (f) to issue certifications and approve criteria of certification in accordance with Article 42(5);
- (g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);
- (h) to authorise contractual clauses referred to in point (a) of Article 46(3);
- (i) to authorise administrative arrangements referred to in point (b) of Article 46(3);
- (j) to approve binding corporate rules pursuant to Article 47.

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.

Article 59

Activity reports

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

CHAPTER VII

Cooperation and consistency

Section 1

Cooperation

Article 60

Cooperation between the lead supervisory authority and the other supervisory authorities concerned

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.
2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.
3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.
4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.
5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.
6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.
7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.

8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.

10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.

11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.

12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.

Article 61

Mutual assistance

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the

request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. The requested supervisory authority shall not refuse to comply with the request unless:

(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or

(b) compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.

6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Article 62

Joint operations of supervisory authorities

1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.
2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56(1) or (4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.
3. A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.
4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.
5. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.

6. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.

7. Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).

Section 2

Consistency

Article 63

Consistency mechanism

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

Article 64

Opinion of the Board

1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:

(a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);

(b) concerns a matter pursuant to Article 40(7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;

(c) aims to approve the criteria for accreditation of a body pursuant to Article 41(3) or a certification body pursuant to Article 43(3);

(d) aims to determine standard data protection clauses referred to in point (d) of Article 46(2) and in Article 28(8);

(e) aims to authorise contractual clauses referred to in point (a) of Article 46(3); or

(f) aims to approve binding corporate rules within the meaning of Article 47.

2. Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.

3. In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.

4. Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.

5. The Chair of the Board shall, without undue, delay inform by electronic means:

(a) the members of the Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and

(b) the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.

6. The competent supervisory authority shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.

7. The supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardised format.

8. Where the supervisory authority concerned informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply.

Article 65

Dispute resolution by the Board

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

(a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

(b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

(c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.

3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall be adopted by the vote of its Chair.

4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.

6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

Article 66

Urgency procedure

1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms

of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.

4. By derogation from Article 64(3) and Article 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.

Article 67

Exchange of information

The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Section 3

European data protection board

Article 68

European Data Protection Board

1. The European Data Protection Board (the 'Board') is hereby established as a body of the Union and shall have legal personality.
2. The Board shall be represented by its Chair.
3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.
4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.
5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.

6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

Article 69

Independence

1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.

2. Without prejudice to requests by the Commission referred to in point (b) of Article 70(1) and in Article 70(2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

Article 70

Tasks of the Board

1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:

(a) monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;

(b) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

(c) advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;

(d) issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17(2);

(e) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;

(f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);

(g) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

(h) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1).

(i) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;

(j) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);

(k) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the setting of administrative fines pursuant to Article 83;

(l) review the practical application of the guidelines, recommendations and best practices referred to in points (e) and (f);

(m) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);

(n) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;

(o) carry out the accreditation of certification bodies and its periodic review pursuant to Article 43 and maintain a public register of accredited bodies pursuant to Article 43(6) and of the accredited controllers or processors established in third countries pursuant to Article 42(7);

(p) specify the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies under Article 42;

(q) provide the Commission with an opinion on the certification requirements referred to in Article 43(8);

(r) provide the Commission with an opinion on the icons referred to in Article 12(7);

(s) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.

(t) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;

(u) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;

(v) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;

(w) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.

(x) issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and

(y) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.

2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.

4. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.

Article 71

Reports

1. The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.
2. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.

Article 72

Procedure

1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.
2. The Board shall adopt its own rules of procedure by a two-thirds majority of its members and organise its own operational arrangements.

Article 73

Chair

1. The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.
2. The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.

Article 74

Tasks of the Chair

1. The Chair shall have the following tasks:
 - (a) to convene the meetings of the Board and prepare its agenda;
 - (b) to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned;
 - (c) to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.

2. The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.

Article 75

Secretariat

1. The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.

2. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.

3. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.

4. Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.

5. The secretariat shall provide analytical, administrative and logistical support to the Board.

6. The secretariat shall be responsible in particular for:

(a) the day-to-day business of the Board;

(b) communication between the members of the Board, its Chair and the Commission;

(c) communication with other institutions and the public;

(d) the use of electronic means for the internal and external communication;

(e) the translation of relevant information;

(f) the preparation and follow-up of the meetings of the Board;

(g) the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.

Article 76

Confidentiality

1. The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.

2. Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council (21).

CHAPTER VIII

Remedies, liability and penalties

Article 77

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.
2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

Article 78

Right to an effective judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.
2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.
3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.
4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

Article 79

Right to an effective judicial remedy against a controller or processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Article 80

Representation of data subjects

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

Article 81

Suspension of proceedings

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court

in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

Article 82

Right to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

Article 83

General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

- (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
- (b) the intentional or negligent character of the infringement;
- (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
- (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
- (e) any relevant previous infringements by the controller or processor;
- (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
- (g) the categories of personal data affected by the infringement;
- (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
- (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
- (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
- (k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

Article 84

Penalties

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

CHAPTER IX

Provisions relating to specific processing situations

Article 85

Processing and freedom of expression and information

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory

authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

Article 86

Processing and public access to official documents

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

Article 87

Processing of the national identification number

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

Article 88

Processing in the context of employment

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 89

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Article 90

Obligations of secrecy

1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.
2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 91

Existing data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.
2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

CHAPTER X

Delegated acts and implementing acts

Article 92

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from 24 May 2016.

3. The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 93

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER XI

Final provisions

Article 94

Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed with effect from 25 May 2018.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Article 95

Relationship with Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

Article 96

Relationship with previously concluded Agreements

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

Article 97

Commission reports

1. By 25 May 2020 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.
2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of:
 - (a) Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;
 - (b) Chapter VII on cooperation and consistency.
3. For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.
4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.

5. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.

Article 98

Review of other Union legal acts on data protection

The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.

Article 99

Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

2. It shall apply from 25 May 2018.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 27 April 2016.

For the European Parliament

The President

M. SCHULZ

For the Council

The President

J.A. HENNIS-PLASSCHAERT

[1] OJ C 229, 31.7.2012, p. 90.

[2] OJ C 391, 18.12.2012, p. 127.

[3] Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

[5] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422) (OJ L 124, 20.5.2003, p. 36).

[6] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

[7] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA (see page 89 of this Official Journal).

[8] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

[9] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

[10] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).

[11] Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).

[12] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

[13] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

[14] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ L 345, 31.12.2003, p. 90).

[15] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158, 27.5.2014, p. 1).

[16] Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164).

[17] OJ C 192, 30.6.2012, p. 7.

[18] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

[19] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

[20] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

[21] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

GDPR Recitals

UNOFFICIAL RECITAL INDEX

- (1)** Data Protection as a Fundamental Right
- (2)** Respect of the Fundamental Rights and Freedoms
- (3)** Directive 95/46/EC Harmonisation
- (4)** Data Protection in Balance with Other Fundamental Rights
- (5)** Cooperation Between Member States to Exchange Personal Data
- (6)** Ensuring a High Level of Data Protection Despite the Increased Exchange of Data
- (7)** The Framework is Based on Control and Certainty
- (8)** Adoption into National Law
- (9)** Different Standards of Protection by the Directive 95/46/EC
- (10)** Harmonised Level of Data Protection Despite National Scope
- (11)** Harmonisation of the Powers and Sanctions
- (12)** Authorization of the European Parliament and the Council
- (13)** Taking Account of Micro, Small and Medium-Sized Enterprises
- (14)** Not Applicable to Legal Persons
- (15)** Technology Neutrality
- (16)** Not Applicable to Activities Regarding National and Common Security
- (17)** Adaptation of Regulation (EC) No 45/2001
- (18)** Not Applicable to Personal or Household Activities
- (19)** Not Applicable to Criminal Prosecution
- (20)** Respecting the Independence of the Judiciary
- (21)** Liability Rules of Intermediary Service Providers Shall Remain Unaffected
- (22)** Processing by an Establishment

- (23) Applicable to Controllers/Processors Not Established in the Union if Data Subjects Within the Union are Targeted
- (24) Applicable to Controllers/Processors Not Established in the Union if Data Subjects Within the Union are Profiled
- (25) Applicable to Controllers Due to International Law
- (26) Not Applicable to Anonymous Data
- (27) Not Applicable to Data of Deceased Persons
- (28) Introduction of Pseudonymisation
- (29) Pseudonymisation at the Same Controller
- (30) Online Identifiers for Profiling and Identification
- (31) Not Applicable to Public Authorities in Connection with Their Official Tasks
- (32) Conditions for Consent
- (33) Consent to Certain Areas of Scientific Research
- (34) Genetic Data
- (35) Health Data
- (36) Determination of the Main Establishment
- (37) Group of undertakings
- (38) Special Protection of Children's Personal Data
- (39) Principles of Data Processing
- (40) Lawfulness of Data Processing
- (41) Legal Basis or Legislative Measures
- (42) Burden of Proof and Requirements for Consent
- (43) Freely Given Consent
- (44) Performance of a Contract
- (45) Fulfillment of Legal Obligations
- (46) Vital Interests of the Data Subject

- (47) Overriding Legitimate Interest
- (48) Overriding Legitimate Interest Within Group of Undertakings
- (49) Network and Information Security as Overriding Legitimate Interest
- (50) Further Processing of Personal Data
- (51) Protecting Sensitive Personal Data
- (52) Exceptions to the Prohibition on Processing Special Categories of Personal Data
- (53) Processing of Sensitive Data in Health and Social Sector
- (54) Processing of Sensitive Data in Public Health Sector
- (55) Public Interest in Processing by Official Authorities for Objectives of Recognized Religious Communities
- (56) Processing Personal Data on People's Political Opinions by Parties
- (57) Additional Data for Identification Purposes
- (58) The Principle of Transparency
- (59) Procedures for the Exercise of the Rights of the Data Subjects
- (60) Information Obligation
- (61) Time of Information
- (62) Exceptions to the Obligation to Provide Information
- (63) Right of Access
- (64) Identity Verification
- (65) Right of Rectification and Erasure
- (66) Right to be Forgotten
- (67) Restriction of Processing
- (68) Right of Data Portability
- (69) Right to Object
- (70) Right to Object to Direct Marketing
- (71) Profiling

- (72) Guidance of the European Data Protection Board Regarding Profiling
- (73) Restrictions of Rights and Principles
- (74) Responsibility and Liability of the Controller
- (75) Risks to the Rights and Freedoms of Natural Persons
- (76) Risk Assessment
- (77) Risk Assessment Guidelines
- (78) Appropriate Technical and Organisational Measures
- (79) Allocation of the Responsibilities
- (80) Designation of a Representative
- (81) The Use of Processors
- (82) Record of Processing Activities
- (83) Security of Processing
- (84) Risk Evaluation and Impact Assessment
- (85) Notification Obligation of Breaches to the Supervisory Authority
- (86) Notification of Data Subjects in Case of Data Breaches
- (87) Promptness of Reporting / Notification
- (88) Format and Procedures of the Notification
- (89) Elimination of the General Reporting Requirement
- (90) Data Protection Impact Assessment
- (91) Necessity of a Data Protection Impact Assessment
- (92) Broader Data Protection Impact Assessment
- (93) Data Protection Impact Assessment at Authorities
- (94) Consultation of the Supervisory Authority
- (95) Support by the Processor
- (96) Consultation of the Supervisory Authority in the Course of a Legislative Process
- (97) Data Protection Officer

- (98) Preparation of Codes of Conduct by Organisations and Associations
- (99) Consultation of Stakeholders and Data Subjects in the Development of Codes of Conduct
- (100) Certification
- (101) General Principles for International Data Transfers
- (102) International Agreements for an Appropriate Level of Data Protection
- (103) Appropriate Level of Data Protection Based on an Adequacy Decision
- (104) Criteria for an Adequacy Decision
- (105) Consideration of International Agreements for an Adequacy Decision
- (106) Monitoring and Periodic Review of the Level of Data Protection
- (107) Amendment, Revocation and Suspension of Adequacy Decisions
- (108) Appropriate Safeguards
- (109) Standard Data Protection Clauses
- (110) Binding Corporate Rules
- (111) Exceptions for Certain Cases of International Transfers
- (112) Data Transfers due to Important Reasons of Public Interest
- (113) Transfers Qualified as Not Repetitive and that Only Concern a Limited Number of Data Subjects
- (114) Safeguarding of Enforceability of Rights and Obligations in the Absence of an Adequacy Decision
- (115) Rules in Third Countries Contrary to the Regulation
- (116) Cooperation Among Supervisory Authorities
- (117) Establishment of Supervisory Authorities
- (118) Monitoring of the Supervisory Authorities
- (119) Organisation of Several Supervisory Authorities of a Member State
- (120) Features of Supervisory Authorities
- (121) Independence of the Supervisory Authorities
- (122) Responsibility of the Supervisory Authorities

- (123) Cooperation of the Supervisory Authorities with Each Other and with the Commission
- (124) Lead Authority Regarding Processing in Several Member States
- (125) Competences of the Lead Authority
- (126) Joint Decisions
- (127) Information of the Supervisory Authority Regarding Local Processing
- (128) Responsibility Regarding Processing in the Public Interest
- (129) Tasks and Powers of the Supervisory Authorities
- (130) Consideration of the Authority with which the Complaint has been Lodged
- (131) Attempt of an Amicable Settlement
- (132) Awareness-Raising Activities and Specific Measures
- (133) Mutual Assistance and Provisional Measures
- (134) Participation in Joint Operations
- (135) Consistency Mechanism
- (136) Binding Decisions and Opinions of the Board
- (137) Provisional Measures
- (138) Urgency Procedure
- (139) European Data Protection Board
- (140) Secretariat and Staff of the Board
- (141) Right to Lodge a Complaint
- (142) The Right of Data Subjects to Mandate a Not-For-Profit Body, Organisation or Association
- (143) Judicial Remedies
- (144) Related Proceedings
- (145) Choice of Venue
- (146) Indemnity
- (147) Jurisdiction
- (148) Penalties

- (149) Penalties for Infringements of National Rules
- (150) Administrative Fines
- (151) Administrative Fines in Denmark and Estonia
- (152) Power of Sanction of the Member States
- (153) Processing of Personal Data Solely for Journalistic Purposes or for the Purposes of Academic, Artistic or Literary Expression
- (154) Principle of Public Access to Official Documents
- (155) Processing in the Employment Context
- (156) Processing for Archiving, Scientific or Historical Research or Statistical Purposes
- (157) Information from Registries and Scientific Research
- (158) Processing for Archiving Purposes
- (159) Processing for Scientific Research Purposes
- (160) Processing for Historical Research Purposes
- (161) Consenting to the Participation in Clinical Trials
- (162) Processing for Statistical Purposes
- (163) Production of European and National Statistics
- (164) Professional or Other Equivalent Secrecy Obligations
- (165) No Prejudice of the Status of Churches and Religious Associations
- (166) Delegated Acts of the Commission
- (167) Implementing Powers of the Commission
- (168) Implementing Acts on Standard Contractual Clauses
- (169) Immediately Applicable Implementing Acts
- (170) Principle of Subsidiarity and Principle of Proportionality
- (171) Repeal of Directive 95/46/EC and Transitional Provisions
- (172) Consultation of the European Data Protection Supervisor
- (173) Relationship to Directive 2002/58/EC

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(3) Directive 95/46/EC of the European Parliament and of the Council (4) seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

(4) The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion,

freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

(5) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

(6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

(7) Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

(8) Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law.

(9) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of

economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

(11) Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.

(12) Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data.

(13) In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent

sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC (5).

(14) The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

(15) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

(16) This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

(17) Regulation (EC) No 45/2001 of the European Parliament and of the Council (6) applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in this Regulation and applied in the light of this Regulation. In order to provide a strong and coherent data protection framework in the Union, the

necessary adaptations of Regulation (EC) No 45/2001 should follow after the adoption of this Regulation, in order to allow application at the same time as this Regulation.

(18) This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

(19) The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council (7). Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation.

With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the

safeguarding against and the prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

(20) While this Regulation applies, *inter alia*, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.

(21) This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council (8), in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.

(22) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

(23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to

ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

(24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

(25) Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

(27) This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.

(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

(29) In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.

(30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

(31) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.

(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has

multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

(34) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

(35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council (9) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

(36) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means

and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

(37) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.

(38) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

(39) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns,

in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

(40) In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

(41) Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights.

(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive

93/13/EEC (10) a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

(44) Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.

(45) Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health

purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.

(46) The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

(48) Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

(50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, *inter alia*: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in

particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

(51) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

(52) Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in

particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

(53) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

(54) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, ‘public health’ should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council [11], namely all elements related to health, namely health

status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

(55) Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations, is carried out on grounds of public interest.

(56) Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

(57) If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.

(58) The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

(59) Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal

data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

(60) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.

(61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

(62) However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

(63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be

aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

(65) A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of

public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

(66) To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.

(67) Methods by which to restrict the processing of personal data could include, *inter alia*, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

(68) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with

this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

(69) Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

(70) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

(71) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or

performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

(72) Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles. The European Data Protection Board established by this Regulation (the 'Board') should be able to issue guidance in that context.

(73) Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others,

including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

(77) Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of

approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

(79) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(80) Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes

of the processing or if the controller is a public authority or body. The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

(81) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.

(82) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

(83) In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

(84) In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(86) The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of

the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

(87) It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

(88) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.

(89) Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

(90) In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

(91) This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.

(92) There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

(93) In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or

set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.

(94) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

(95) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

(96) A consultation of the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.

(97) Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary

level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

(98) Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.

(99) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.

(100) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

(101) Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

(102) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of

personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.

(103) The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.

(104) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

(105) Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol

should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations.

(106) The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or specified sector within a third country, or an international organisation, and monitor the functioning of decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any relevant findings to the Committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council (12) as established under this Regulation, to the European Parliament and to the Council.

(107) The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(108) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or

judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.

(109) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.

(110) A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

(111) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons

or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.

(112) Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Member States should notify such provisions to the Commission. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.

(113) Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable. For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer.

(114) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide

data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.

(115) Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, *inter alia*, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.

(116) When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international cooperation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with this Regulation.

(117) The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.

(118) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subject to control or monitoring mechanisms regarding their financial expenditure or to judicial review.

(119) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth cooperation with other supervisory authorities, the Board and the Commission.

(120) Each supervisory authority should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks, including those related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.

(121) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members are to be appointed, by means of a transparent procedure, either by the parliament, government or the head of State of the Member State on the basis of a proposal from the government, a member of the government, the parliament or a chamber of the parliament, or by an independent body entrusted under Member State law. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, refrain from any action that is incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. The supervisory authority should have its own staff, chosen by the supervisory authority or an independent body established by Member State law, which should be subject to the exclusive direction of the member or members of the supervisory authority.

(122) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data carried out by public authorities or private bodies acting in the public interest, processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory. This should include handling

complaints lodged by a data subject, conducting investigations on the application of this Regulation and promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.

(123) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.

(124) Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned. Within its tasks to issue guidelines on any question covering the application of this Regulation, the Board should be able to issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection.

(125) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.

(126) The decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.

(127) Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide, whether it will handle the case pursuant to the provision on cooperation between the lead supervisory authority and other supervisory authorities concerned ('one-stop-shop mechanism'), or whether the supervisory authority which informed it should handle the case at local level. When deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision vis-à-vis the controller or processor. Where the lead supervisory authority decides to handle the case, the supervisory authority which informed it should have the possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in that one-stop-shop mechanism.

(128) The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or private body is established.

(129) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to

the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.

(130) Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.

(131) Where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the Member State where the complaint has been lodged or the possible infringement detected and the

matter does not substantially affect or is not likely to substantially affect data subjects in other Member States, the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers. This should include: specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or processing that has to be assessed taking into account relevant legal obligations under Member State law.

(132) Awareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons in particular in the educational context.

(133) The supervisory authorities should assist each other in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. A supervisory authority requesting mutual assistance may adopt a provisional measure if it receives no response to a request for mutual assistance within one month of the receipt of that request by the other supervisory authority.

(134) Each supervisory authority should, where appropriate, participate in joint operations with other supervisory authorities. The requested supervisory authority should be obliged to respond to the request within a specified time period.

(135) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for cooperation between the supervisory authorities should be established. That mechanism should in particular apply where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States. It should also apply where any supervisory authority concerned or the Commission requests that such matter should be handled in the consistency mechanism. That mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

(136) In applying the consistency mechanism, the Board should, within a determined period of time, issue an opinion, if a majority of its members so decides or if so requested by any supervisory authority concerned or the Commission. The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it

should issue, in principle by a two-thirds majority of its members, legally binding decisions in clearly specified cases where there are conflicting views among supervisory authorities, in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, in particular whether there is an infringement of this Regulation.

(137) There may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. A supervisory authority should therefore be able to adopt duly justified provisional measures on its territory with a specified period of validity which should not exceed three months.

(138) The application of such mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and mutual assistance and joint operations might be carried out between the supervisory authorities concerned on a bilateral or multilateral basis without triggering the consistency mechanism.

(139) In order to promote the consistent application of this Regulation, the Board should be set up as an independent body of the Union. To fulfil its objectives, the Board should have legal personality. The Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Commission should participate in the Board's activities without voting rights and the European Data Protection Supervisor should have specific voting rights. The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union. The Board should act independently when performing its tasks.

(140) The Board should be assisted by a secretariat provided by the European Data Protection Supervisor. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation should perform its tasks exclusively under the instructions of, and report to, the Chair of the Board.

(141) Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an

effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(142) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. A Member State may provide for such a body, organisation or association to have the right to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes this Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate.

(143) Any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court of Justice under the conditions provided for in Article 263 TFEU. As addressees of such decisions, the supervisory authorities concerned which wish to challenge them have to bring action within two months of being notified of them, in accordance with Article 263 TFEU. Where decisions of the Board are of direct and individual concern to a controller, processor or complainant, the latter may bring an action for annulment against those decisions within two months of their publication on the website of the Board, in accordance with Article 263 TFEU. Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority

which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with that Member State's procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them.

Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation. Furthermore, where a decision of a supervisory authority implementing a decision of the Board is challenged before a national court and the validity of the decision of the Board is at issue, that national court does not have the power to declare the Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice, where it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down in Article 263 TFEU.

(144) Where a court seized of proceedings against a decision by a supervisory authority has reason to believe that proceedings concerning the same processing, such as the same subject matter as regards processing by the same controller or processor, or the same cause of action, are brought before a competent court in another Member State, it should contact that court in order to confirm the existence of such related proceedings. If related proceedings are pending before a court in another Member State, any court other than the court first seized may stay its proceedings or may, on request of one of the parties, decline jurisdiction in favour of the court first seized if that court has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear

and determine them together in order to avoid the risk of irreconcilable judgments resulting from separate proceedings.

(145) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.

(146) The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.

(147) Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council (13) should not prejudice the application of such specific rules.

(148) In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional

character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.

(149) Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice.

(150) In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.

(151) The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark the

fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanour procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.

(152) Where this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of this Regulation, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.

(153) Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the Charter. This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights. Member States should adopt such exemptions and derogations on general principles, the rights of the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations. Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

(154) This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should

reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council [14] leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.

(155) Member State law or collective agreements, including ‘works agreements’, may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

(156) The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public

interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

(157) By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.

(158) Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes.

(159) Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.

(160) Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

(161) For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council (15) should apply.

(162) Where personal data are processed for statistical purposes, this Regulation should apply to that processing. Union or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality. Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose. The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.

(163) The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU, while national statistics should also comply with Member State law.

Regulation (EC) No 223/2009 of the European Parliament and of the Council (16) provides further specifications on statistical confidentiality for European statistics.

(164) As regards the powers of the supervisory authorities to obtain from the controller or processor access to personal data and access to their premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. This is without prejudice to existing Member State obligations to adopt rules on professional secrecy where required by Union law.

(165) This Regulation respects and does not prejudice the status under existing constitutional law of churches and religious associations or communities in the Member States, as recognised in Article 17 TFEU.

(166) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

(167) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

(168) The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country, a territory or a specified sector within that third country, or an international organisation; standard protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate

rules; mutual assistance; and arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board.

(169) The Commission should adopt immediately applicable implementing acts where available evidence reveals that a third country, a territory or a specified sector within that third country, or an international organisation does not ensure an adequate level of protection, and imperative grounds of urgency so require.

(170) Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(171) Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.

(172) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012 [17].

(173) This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council (18), including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation,

HAVE ADOPTED THIS REGULATION:

Avrupa Birliđi - 95/46 sayılı Direktif (Türkçe)

95/46 sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data/ 27.10.1995

Resmi Gazete, L 281 , 23/11/1995 P. 0031 - 0050

Başlangıç

AVRUPA PARLAMENTOSU VE AVRUPA BİRLİĐİ KONSEYİ,

Avrupa Topluluđunu Kuran Anlaşmayı ve özellikle ilgili 100a maddesini göz önünde bulundurarak,

Komisyonun teklifini göz önünde bulundurarak,

Ekonomik ve Sosyal Komite'nin görüşünü göz önünde bulundurarak,

Anlaşmanın 189b maddesinde ortaya koyulan prosedür uyarınca hareket ederek aşağıda sıralanan nedenlerden dolayı:

(1) Topluluk'un amaçları, Avrupa Birliđi Anlaşması tarafından tadil edildiđi, Anlaşmada öngörüldüğü şekilde; İnsan Hakları ve Temel Özgürlüklerin Korunması Hakkındaki Avrupa Sözleşmesi'nde ve Üye Devletler'in anayasaları ve yasalarında tanınan temel haklar üzerinden demokrasiyi geliştirerek ve barış ve özgürlüğü koruyup güçlendirerek halklarının yaşama koşullarının sürekli iyileştirilmesini teşvik ederek, Avrupa'yı bölen engelleri gidermek için ortak eylemle ekonomik ve sosyal ilerlemeyi sağlayarak, Topluluk'a mensup Devletlerarasında daha yakın ilişkileri teşvik etmeyi içerir;

(2) Veri işleme sistemleri insana hizmet etmek üzere tasarlanır ve böyle olmalıdır; gerçek kişilerin milliyetine veya ikametgahlarına bakmaksızın, başta kişisel mahremiyet olmak üzere, temel haklarını ve özgürlüklerini korumalıdır ve bireylerin ekonomik ve sosyal ilerlemesine, refahına ve ticari genişlemeye katkıda bulunmalıdır;

- (3) Malların, kişilerin, servislerin ve sermayenin serbest dolaşımının sağlanması hakkındaki Anlaşmanın 7a maddesi uyarınca bir iç pazarın kurulması ve işletilmesi; yalnızca kişisel verilerin bir Üye Devlettten diğerine serbestçe akabilmesini değil, aynı zamanda bireylerin temel haklarının güvenceye alınmasını gerektirir;
- (4) Topluluk'a, ekonomik ve sosyal faaliyetin çeşitli alanlarında kişisel verilerin işlenmesine dönük olarak artan sıklıkta başvuru yapılmaktadır; bilgi teknolojisinde sağlanan ilerlemeler, bu tür verilerin işlenmesini ve değişimini önemli ölçüde kolaylaştırmaktadır;
- (5) Anlaşmanın 7a maddesinin anlamı kapsamında iç pazarın kurulması ve işlemeden kaynaklanan ekonomik ve sosyal entegrasyon; Üye Devletlerde ekonomik ve sosyal faaliyete özel veya kamu sıfatıyla katılan herkes arasında kişisel verilerin sınır ötesi akışında zorunlu olarak önemli bir artışa yol açacaktır. Farklı Üye Devletlerdeki teşebbüsler arasında kişisel verilerin alışverişi artmaya başlamıştır; çeşitli Üye Devletlerdeki ulusal makamlardan, iç pazarın sınırları dikkate almaksızın diğer bir Üye Devletteki bir makam adına görevlerini yerine getirebilmek veya görevlerini yapabilmek hususunda topluluk hukukuna binaen, kişisel verileri takas etmesi ve iş birliği yapması istenmektedir;
- (6) Üstelik Toplulukta yeni haberleşme ağlarının eşgüdümlü uygulanması ve bilimsel ve teknik işbirliğindeki artış, kişisel verilerin sınır ötesi akışını gerektirmekte ve kolaylaştırmaktadır;
- (7) Üye Devletlerde uygulanan kişisel verilerin işlenmesine dair başta kişisel mahremiyet hakkı olmak üzere bireylerin hakları ve özgürlüklerinin korunma seviyesindeki farklılıklar, bir Üye Devlet toprağından diğer Üye Devlete bu tür verilerin iletilmesini engelleyebilir; bu nedenle bu fark, Topluluk seviyesindeki birtakım ekonomik faaliyetlerin takibi için bir engel oluşturabilir, rekabeti bozabilir ve Topluluk hukuku kapsamında makamların sorumluluklarını yerini getirmesini engelleyebilir; koruma seviyesindeki bu fark, çok çeşitli ulusal kanunlar, yönetmelikler ve idari hükümlerin varlığından dolayıdır;
- (8) Kişisel verilerin akışındaki engelleri kaldırmak için, bireylerin hak ve özgürlüklerinin korunma seviyesi bu tür verilerin işlenmesine ilişkin olarak tüm Üye Devletlerde eşit olmalıdır; bu amaç iç pazar için hayattır ancak özellikle Anlaşmanın 7a maddesinde belirtilen iç pazar amacına uyan tutarlı bir şekilde kişisel verilerin sınır ötesi akışının düzenlenmesini temin etmek hususunda Üye Devletlerdeki ilgili kanunlar arasında mevcut uyumsuzlukların ölçeği göz önüne alındığında bu, Üye Devletler tarafından tek başına başarılamaz; bu yüzden bu kanunları yaklaştırmak için Topluluk eylemine gerek duyulmaktadır;

(9) Ulusal kanunların yakınlaştırılmasından kaynaklanan eşdeğer koruma dikkate alındığında, Üye Devletler, özellikle kişisel gizlilik hakkı başta olmak üzere, bireylerin özgürlükleri ve haklarının korunması gerekçesiyle, kişisel verilerin aralarında serbest dolaşımını artık engelleyemeyeceklerdir; Üye Devletlere, Direktifin uygulanması bağlamında, iş ve sosyal ortaklar tarafından da yerine getirilebilecek bir manevra alanı bırakılacaktır; bu nedenle Üye Devletler veri işlemenin yasallığını yöneten genel koşulları, kendi ulusal yasalarına koyabileceklerdir. Üye Devletler bu şekilde kendi mevzuatlarıyla güncel olarak sağlanan korumayı geliştirmeye çalışacaklardır; bu manevra alanının limitleri dâhilinde ve Topluluk kanuna uygun olarak, Direktifin uygulanmasında eşitsizlikler ortaya çıkabilir ve bu, Topluluğun yanı sıra bir Üye Devlet bünyesinde verilerin dolaşımı etkileyebilir;

(10) Kişisel verilerin işlenmesi hakkındaki ulusal kanunların amacı, başta kişisel mahremiyet hakkı olmak üzere, hem Topluluk kanununun genel esaslarında, hem de İnsan Hakları ve Temel Özgürlüklerini Koruma hakkındaki Avrupa Sözleşmesinin 8. maddesinde tanınan temel hakları ve özgürlükleri korumaktır; bu nedenle, bu kanunların yakınlaştırılması, sağladıkları korumanın azalmasına yol açmamalı aksine, Topluluk içinde yüksek seviyeli bir korumanın sağlanması için çabalamalıdır;

(11) Kişisel mahremiyet başta olmak üzere bireylerin haklarının ve özgürlüklerinin korunması hakkında bu Direktifte belirtilen esaslar, Kişisel Verilerin Otomatik İşlenmesine İlişkin Bireylerin Korunması Hakkındaki 28 Ocak 1981 tarihli Avrupa Konseyi Sözleşmesinde belirtilenleri güçlendirir ve genişletir;

(12) Koruma esasları, faaliyetleri Topluluk hukukunca yönetilen herhangi bir kişinin kişisel verilerinin tüm işlenmesine uygulanmalıdır; adres kayıtlarını tutma ve yazışma gibi özellikle şahsi veya ailevi olan aktiviteler esnasında, bir gerçek kişinin gerçekleştirdiği veri işleme, hariç tutulmalıdır;

(13) Avrupa Topluluğunu Kuran Anlaşmanın 100a maddesi veya madde 56 (2), madde 57 kapsamında Üye Devletler üzerine düşen yükümlülükler saklı kalmak üzere; kamu güvenliği, savunma, devlet güvenliğine dair Avrupa Birliği Anlaşmasının V ve VI. Başlığında atıfta bulunulan faaliyetler ile ceza kanunları alanındaki Devlet faaliyetleri; Topluluk hukuku kapsamında değildir; Devletin güvenlik konularıyla ilişkili olduğunda, devletin ekonomik refahını güvenceye almak için gerekli olan kişisel verilerin işlenmesi, bu Direktifin kapsamında değildir;

(14) Gerçek kişilere ilişkin ses ve görüntü verilerini yakalamak, iletmek, değiştirmek, kaydetmek, saklamak veya nakletmek için kullanılan teknolojilerin, bilgi toplumu çerçevesinde devam eden

gelişmelerinin önemi dikkate alındığında, bu Direktif bu tür verileri gerektiren işlemeye uygulanmalıdır;

(15) Bu tür verilerin işlenmesi; söz konusu kişisel verilere kolay erişime izin vermek için, yalnızca otomatik olursa veya işlenen veriler, bireylere ilişkin özel kriterlere göre yapılandırılan bir dosyalama sistemi içine alınır veya alınması planlanırsa, bu Direktif kapsamındadır;

(16) Video gözetim durumlarındaki gibi, ses ve görüntü verilerinin işlenmesi; ceza hukuku alanına ilişkin Devlet faaliyetleri esnasında veya ulusal güvenlik, savunma kamu güvenliği amacıyla veya Topluluk hukuku kapsamına girmeyen diğer faaliyetler için yürütülürse bu Direktif kapsamına girmez;

(17) Başta görsel işitsel alan olmak üzere, ilgili edebi ve sanatsal ifade amaçlarının yanı sıra gazetecilik amaçları için ses ve görüntü verilerinin işlenmesinde; Direktifin esasları, madde 9'da öngörülen hükümlere göre, sınırlı bir şekilde uygulanacaktır;

(18) Bireylerin, bu Direktif kapsamında sağlanan korumadan yoksun kalmamalarını sağlamak için, Topluluktaki herhangi bir kişisel veri işlenmesi, Üye Devletler'den birinin kanununa uygun olarak yerine getirilmelidir; bu bağlamda, bir Üye Devlette yerleşik bir denetleyicinin sorumluluğu altında yapılan işlem, o Devletin kanununca yönetilmelidir;

(19) Bir Üye Devletin sınırları içindeki kuruluş, istikrarlı düzenlemeler aracılığıyla faaliyetin etkin ve reel olarak gerçekleştirilmesini sağlar. İster bir tüzel kişiliğin şubesi veya bağlı kuruluşu olsun bu tür kuruluşun yasal biçimi; bu bakımdan belirleyici bir faktör değildir; özellikle bağlı kuruluşlar aracılığıyla çeşitli Üye Devletlerin topraklarında tek bir denetleyici kuruluş kurulursa, ulusal kuralların boşluklarından yararlanmayı önlemek için, denetleyici kuruluşların her birinin, faaliyetlerine uygulanan ulusal kanunun emrettiği yükümlülükleri yerine getirmesi sağlanmalıdır;

(20) Verilerin işlenmesinin üçüncü bir ülkede kurulan bir tüzel kişilik tarafından yapılması, bu Direktifte sağlanan bireylerin korunma biçimine engel olmamalıdır; bu durumlarda, işleme, kullanılan yöntemlerin bulunduğu Üye Devlet kanununca yönetilmelidir ve bu Direktifte sağlanan hakların, uygulamada gözetilmesini sağlayacak garantiler olmalıdır;

(21) Bu Direktif, ülkesellik ilkeleri saklı kalmak üzere ceza konularına uygulanır;

(22) Üye Devletler, işleminin yasallığına dair genel koşulları, çıkardıkları yasalarda veya bu Direktif kapsamındaki tedbirleri yürürlüğe koyduklarında, daha hassas olarak tanımlayacaklardır; madde 7 ve 8 ile bağlantılı olarak özellikle madde 5, genel kurallardan bağımsız olarak Üye Devletlere, madde

8'in kapsadığı çeşitli veri kategorileri için ve belirli sektörler için, özel işleme koşulları koymaya izin verir.

(23) Üye Devletler, hem kişisel verilerin işlenmesi hususunda bireylerin korunması hakkındaki genel kanunlar, hem de örneğin istatistik enstitülerine ilişkin olanlar gibi sektörel kanunlar yoluyla bireylerin korunmasını uygulamayı temin etmek üzere yetkilendirilmişlerdir;

(24) Kendilerini ilgilendiren verileri işlemeye dair tüzel kişilerin korunmasına ilişkin mevzuat, bu Direktiften etkilenmez;

(25) Korumanın esasları; bir taraftan, başta işlemenin yürütülebileceği koşullar ve denetleme makamına bildirim, teknik güvenlik ve veri kalitesi olmak üzere işlemeden sorumlu diğer kuruluşlar veya kişiler, kamu makamları, işletmeler, temsilciler üzerine yüklenen yükümlülüklerle ve diğer taraftan, bireylere verilen haklara, işlemenin konusu olan verilere, işlemenin yapıldığını bildirim, verileri danışmaya, düzeltme talep etmeye ve hatta bazı koşullarda işlemeye itiraza yansıtılmalıdır;

(26) Koruma esasları, tespit edilmiş veya tespit edilebilir bir kişiye ilişkin herhangi bir bilgiye uygulanmalıdır; bir kişinin tespit edilebilir olup olmadığını belirlemek için, adı geçen şahsı tespit etmek için herhangi bir diğer kişi tarafından veya denetleyici tarafından kullanılacak makul tüm araçlar dikkate alınmalıdır; koruma esasları, veri öznesinin artık tespit edilebilir olmadığı bir biçimde anonimleşmiş verilere uygulanmayacaktır; madde 27'nin anlamı dahilindeki davranış kuralları, verilerin anonimleşebilmesine ve veri öznesinin tespitinin artık mümkün olmadığı bir biçimde alıkonma biçimlerine dair rehberlik sağlamak için yararlı bir araç olabilir;

(27) Bireylerin korunması, manuel işlemenin yanı sıra verilerin otomatik işlenmesinde de uygulanmalıdır; bu korumanın kapsamı kullanılan tekniklere bağlı olarak geçerli olmamalıdır, aksi takdirde, bu ciddi bir kanun boşluklarından yararlanma riski yaratacaktır; yine de manuel işlemeye dair bu Direktif yapılandırılmamış dosyaları değil yalnızca dosyalama sistemlerini kapsar, özellikle bir dosyalama sisteminin içeriği, kişisel verilere kolay erişime olanak veren bireylere ilişkin özel kriterlere göre yapılandırılmalıdır; madde 2 (c)deki tanım doğrultusunda, kişisel verilerin yapılandırılmış bir dizisinin bileşenlerini belirlemek için farklı kriterler ve bu tür bir veri dizisine erişimi yöneten farklı kriterler, her bir Üye Devlet tarafından belirlenebilir; özel kriterlere göre yapılandırılmamış kapak sayfalarının yanı sıra dosyalar veya dosya dizileri, hiçbir koşul altında bu Direktifin kapsamına girmeyecektir;

(28) Kişisel verilerin işlenmesi, ilgili bireyler için yasal ve adil olmalıdır; özellikle veriler uygun, ilgili olmalıdır ve işlendikleri amacı aşmamalıdır; bu tür amaçlar açık ve meşru olmalı ve verilerin

toplanma zamanında belirlenmelidir; toplama sonrasındaki işleme amaçları, başlangıçta belirtilen amaçlarla uyumsuz olmamalıdır;

(29) Tarihsel, istatistiksel veya bilimsel amaçlarla kişisel verilerin ayrıca işlenmesi, Üye Devletlerin uygun korunma önlemleri sağlaması koşuluyla önceden toplanmış verilerin amaçlarıyla uyumsuz olarak kabul edilmez, bu korunma önlemleri özellikle, herhangi bir özel bireye dair tedbirlerin veya kararların desteklenmesinde verilerin kullanımına imkan vermemelidir;

(30) Kişisel verilerin işlenmesi, ayrıca veri öznesinin haklarının ve özgürlüklerinin çiğnenmemesi koşuluyla, yasal olması amacıyla, veri öznesinin rızasıyla yürütülmelidir veya veri öznesi hakkında bağlayıcı bir sözleşmenin yerine getirilmesi veya sonuçlandırılması için veya gerçek veya tüzel bir kişinin meşru menfaati için veya resmi otoritenin uygulanması için veya kamu menfaatine yürütülen bir görevin yerine getirilmesi için gerekli olmalıdır; özellikle etkin rekabeti garanti ederken, ilgili menfaatler arasında bir denge sağlamak için, Üye Devletler, şirketlerin veya diğer kuruluşların olağan meşru iş faaliyetleri bağlamında kişisel verilerin kullanılabilme veya üçüncü bir şahsa açıklanma koşullarını belirleyebilirler; benzer şekilde Üye Devletler, örneğin nedenlerini belirtmeksizin ve bedelsiz olarak, hakkındaki verilerin işlenmesine itiraz etmek için bir veri öznesine izin veren hükümlere tabi olan ister siyasi yapıdaki herhangi diğer bir dernek veya vakıf veya yardım kuruluşu tarafından isterse ticari olarak yürütülen pazarlama amaçları için, kişisel verilerin üçüncü bir şahsa açıklanabilme koşullarını belirtebilirler;

(31) Veri öznesinin yaşamı için asıl olan bir menfaati korumak için yapıldığında kişisel verilerin işlenmesi, aynı derecede yasal kabul edilmelidir;

(32) Kamu menfaatinde veya resmi otoritenin uygulamasında yürütülen bir görevi yerine getiren denetleyicinin, bir kamu idaresi veya kamu hukuku veya bir meslek örgütü gibi özel bir kanun tarafından yönetilen başka bir tüzel veya gerçek kişi mi olacağını belirlemek ulusal mevzuata kalmaktadır;

(33) Veri öznesi açık şekilde rıza göstermezse, temel özgürlükleri veya kişisel mahremiyeti ihlal eden yapıdaki veriler işlenmemelidir; ancak, temel özgürlüklerin yerine getirilmesine izin verecek amaçlar için, bazı derneklerin veya vakıfların meşru faaliyetleri esnasında veya mesleki gizlilik hakkındaki yasal bir yükümlülüğe tabi kişiler tarafından bu verilerin sağlık amaçları için kullanılması durumunda; bu yasaklamaya uymama durumu açıkça belirtilmelidir;

(34) Sağlık sigortası sistemindeki hizmetler ve yardımlar için talepleri belirtmede kullanılan prosedürlerin kalitesini ve maliyet etkinliğini temin etmek başta olmak üzere - kamu menfaati için

önemli nedenlerle gerekçelendirildiğinde, önemli kamu menfaati gerekçesine dayanması durumunda; bilimsel araştırma ve hükümet istatistikleri halk sağlığı ve sosyal koruma gibi alanlarda, Üye Devletlerin verilerin hassas kategorilerini işleme yasağına uymamasına da izin verilmelidir; ancak bireylerin kişisel gizlilik ve temel haklarını korumak hususunda özel ve uygun korunma önlemlerini sağlamak, Üye Devletlerin ödevidir;

(35) Ayrıca, resmi olarak tanınan dini derneklerle ilgili veya uluslararası kamu hukuku veya anayasa hukukunda öngörülen amaçları başarmak için resmi makamlar tarafından kişisel verilerin işlenmesi, kamu menfaatinin önemli gerekçeleri üzerine yürütülür;

(36) Belirli Üye Devletlerde, seçim faaliyetleri esnasında demokratik sistemin işlemesi, siyasi partilerin halkın siyasi görüşü hakkındaki verileri derlemesini gerektirir, uygun korunma önlemlerinin sağlanması koşuluyla bu tür verilerin işlenmesine önemli kamu menfaati nedeniyle izin verilebilir;

(37) Başta görsel işitsel alan olmak üzere, sanatsal ifade, edebi amaçları için veya gazetecilik amaçları için kişisel verilerin işlenmesi; özellikle, İnsan Hakları ve Temel Özgürlüklerinin Korunması hakkındaki Avrupa Sözleşmesinin 10. maddesinde garanti edildiği gibi, özellikle bilgi alma ve verme hakkı ve bilgilendirme hakkıyla bireylerin temel haklarını uzlaştırmanın gerekli olması durumunda, bu Direktifin bazı hükümlerinin koşullarından muaf tutulmaya yetki vermelidir. Bu yüzden üye Devletler, denetleme makamının yetkisi ve üçüncü ülkelere verilerin aktarılması hakkındaki tedbirlere, veri işlemenin yasallığı hakkındaki genel tedbirlere dair temel haklar arasında denge sağlama amacı için gerekli muafiyetleri ve derogasyonları belirtmelidir;

(38) Verilerin işlenmesinin adil olması için, veri öznesi, işleme faaliyetinin varlığını öğrenecek konumda olmalıdır ve veriler ondan toplandığında, toplama koşullarını dikkate alan doğru ve tam bilgi verilmelidir;

(39) Bazı verilerin işlenmesi, denetleyicinin veri öznesinden doğrudan toplamadığı verileri gerektirir, ayrıca, veri öznesinden veriler toplandığı esnada, ifşa beklenmese bile, veriler üçüncü bir şahsa yasal olarak ifşa edilebilir; tüm bu durumlarda, veri öznesi, veriler kaydedildiğinde veya en geç veriler ilk kez bir üçüncü şahsa ifşa edildiğinde, bilgilendirilmelidir;

(40) Ancak, veri öznesinin önceden bilgili olması durumunda, bu yükümlülüğü uygulamak gereksizdir; ayrıca, açıklama veya kaydetme açık şekilde yasayla sağlanırsa veya veri öznesine bilgi sağlamanın imkansızlığı kanıtlanırsa veya işlemenin tarihsel, istatistiki veya bilimsel amaçlar için olması halinde gerekebilecek aşırı çabayı gerektirmesi halinde bu tür bir yükümlülük olmayacaktır;

bu bakımdan, veri öznelerinin sayısı, verilerin yaşı ve kabul edilen herhangi dengeleyici tedbirler dikkate alınmalıdır;

(41) Her kişi, özellikle işlemenin yasallığını ve verilerin doğruluğunu onaylamak için işlenmekte olan ona ait verilere erişim hakkını kullanabilmelidir; aynı nedenlerle, her veri öznesi en azından madde 15(1)de atıfta bulunulan otomatik kararlar durumunda, ona ilişkin verilerin otomatik işlenmesiyle ilgili mantığı bilme hakkına sahip olmalıdır; bu hak, başta yazılımı koruyan telif hakkını ve ticari sırları veya fikri mülkiyeti ters şekilde etkilememelidir; ancak bu düşünceler, veri öznesinin bilgilendirilmemesine yol açmamalıdır;

(42) Üye Devletler, veri öznesinin menfaati için veya diğerlerinin hak ve özgürlüklerini korumak için bilgiye erişim hakkını sınırlandırabilirler; örneğin, tıbbi verilere erişimin yalnızca bir sağlık uzmanı tarafından elde edilebileceğini belirtebilirler;

(43) Benzer şekilde denetleyicinin bazı yükümlülükleri ve bilgilendirme ve erişim hakları üzerindeki sınırlandırmalar; örneğin, düzenlenen mesleklerdeki etik ihlallerine dair kriminal soruşturmalar, takibatlar ve davaların yanı sıra bir Üye Devlet veya Birliğin ulusal güvenlik, savunma, kamu güvenliği veya önemli ekonomik veya mali menfaatlerini güvence altına almanın gerektirdiği ölçüde Üye Devletler tarafından uygulanabilir; istisnalar ve sınırlamaların listesi, kamu güvenliği, ekonomik veya mali menfaatler ve suç önlemeye ilişkin en son söz edilen üç alanda gerekli yönetmelik veya izleme, denetim görevlerini içermelidir; bu üç alandaki görevlerin listelenmesi, Devlet güvenlik veya savunma nedenleri için sınırlamaları veya istisnaların meşruiyetini etkilemez;

(44) Üye Devletler, Topluluk hukuku gerekçesiyle, yukarıda atıfta bulunulan amaçların bazısını güvenceye almak için, verilerin kalitesi ve bireyleri bilgilendirme yükümlülüğü, erişim hakkına ilişkin bu Direktifin hükümlerine uymayabilir;

(45) Verilerin, gerçek veya tüzel bir kişinin meşru menfaatleri veya resmi otorite, kamu menfaati gerekçesiyle yasal olarak işlenebileceği durumlarda, herhangi bir veri öznesine, yine de kendisine ait herhangi bir verinin işlenmesine itiraz etmek için özel durumuna ilişkin meşru ve mecburi gerekçelerle izin verilmelidir; bununla birlikte Üye Devletler bunun aksine ulusal hüküm koyabilirler;

(46) Kişisel verilerin işlenmesine dair veri öznelerinin haklarının ve özgürlüklerinin korunması, hem, güvenliği sağlamak ve bu suretle herhangi bir yetkisiz işlemeyi önlemek için işlemenin kendi zamanında hem de işleme sisteminin tasarımı zamanında uygun teknik ve kurumsal tedbirlerin alınmasını gerektirir; bu tedbirlere denetleyicilerin uymasını sağlamak Üye Devletlerin ödevidir, bu

tedbirler, korunacak verilerin yapısı ve işlemenin yapısındaki risklere ilişkin uygulamanın maliyetlerini ve durumunu dikkate alarak uygun güvenlik seviyesini sağlamalıdır;

(47) Tek amacı verilerin iletilmesi olan, kişisel verileri içeren bir mesajın bir iletişim aracıyla veya elektronik posta servisiyle iletilmesi durumunda, mesajda belirtilen kişisel verilere dair denetleyici; iletim servislerini sunan kişi yerine, mesajın çıktığı kişi olarak kabul edilecektir; bununla birlikte bu tür servisleri sunanlar, normal olarak, servisin çalışması için gerekli ek kişisel verilerin işlenmesi bakımından denetleyici olarak kabul edilecektir;

(48) Denetleme makamını bilgilendirmeye dönük prosedürler, faaliyetin, bu Direktif kapsamında alınan ulusal tedbirlere uygun olduğunu doğrulama amacı için, herhangi bir işleme faaliyetinin amaçlarının ve ana özelliklerinin açıklanmasını sağlamak üzere tasarlanmıştır;

(49) Uygun olmayan idari formalitelerden kaçınmak için, gerekli bildirim yükümlülüğünden muafiyetler; sınırlarını belirten bir Üye Devlet tarafından alınan bir tedbire uyumlu olması koşuluyla, işlemenin, veri öznelerinin haklarını ve özgürlüklerini olumsuz şekilde etkilemesinin mümkün olmadığı durumlarda, Üye Devlet tarafından koyulabilir; benzer şekilde muafiyet veya basitleştirme, denetleyici tarafından atanan bir kişinin yürütülen işlemenin veri öznelerinin haklarını ve özgürlüklerini olumsuz şekilde etkilemesinin olanaksız olmasını sağladığında, Üye Devletler tarafından koyulabilir; ister denetleyicinin bir çalışanı olsun veya olmasın bu tür bir veri koruma görevlisi tam bağımsızlık içinde işlevlerini yerine getirecek bir konumda olmalıdır;

(50) Muafiyet veya basitleştirme, meşru bir menfaati kanıtlayan bir kişi veya kamu tarafından danışmaya açma ve kamuya bilgi sağlamak için ulusal yasaya göre tek amacı kayıt tutma olan işleme faaliyetleri için öngörülebilir;

(51) Yine de bildirim yükümlülüğünden muafiyet veya basitleştirme denetleyiciyi bu Direktiften kaynaklanan diğer yükümlülüklerinin herhangi birisinden kurtarmayacaktır;

(52) Bu bağlamda, genel olarak yetkili makamlar tarafından olaydan sonra doğrulama yeterli bir tedbir olarak kabul edilmelidir;

(53) Ancak bazı işleme faaliyetlerinin, yeni teknolojilerin özel kullanımından dolayı veya bir sözleşme, hak, faydadan bireyleri kapsam dışı tutanlar gibi kendi amaçlarının kapsamı nedeniyle veri öznelerinin hak ve özgürlüklerine özel riskler yaratması olasıdır; Üye Devletler isterlerse mevzuatlarında bu tür riskleri belirtebilirler;

(54) Toplulukta yapılan tüm işlemeye ilişkin olarak; özel riskleri ortaya çıkaran miktar çok sınırlı olmalıdır; Üye Devletler denetleme makamı veya makamla işbirliği içindeki veri koruma görevlisinin,

işlenmesinden önce kontrolün yapılmasını sağlamalıdır; bu ön kontrolün ardından, ulusal yasasına göre denetleme makamı, işlemeye dair bir görüş veya bir izin verebilir; bu tür kontrol; ya ulusal parlamentonun bir tedbirin ya da işlemenin yapısını tanımlayan ve uygun korunma önlemlerini belirten bir yasal tedbirin hazırlanmasıyla eş zamanlı olabilir;

(55) Denetleyici veri öznelerinin haklarını gözetmezse, ulusal mevzuat bir yargı yolu sağlamalıdır; yasadışı işlemenin bir sonucu olarak bir kişinin maruz kalabileceği herhangi bir zarar; mücbir sebepler durumunda ya da hatanın veri öznesinin tarafında olduğunu saptadığı durumlarda; zarardan sorumlu olmadığını kanıtlarsa yükümlülükten muaf tutulacak olan denetleyici tarafından tazmin edilmelidir; yaptırımlar, bu Direktif kapsamında alınan ulusal tedbirlere uymayanın kamu veya özel hukuk tarafından yönetilen herhangi bir kişi olduğuna bakılmaksızın uygulanmalıdır;

(56) Kişisel verilerin sınır ötesi dolaşımı, uluslararası ticaretin genişletilmesi için gereklidir, Bu Direktifle Topluluk bünyesinde garanti edilen bireylerin korunması; yeterli koruma seviyesini sağlayan üçüncü ülkelere kişisel verilerin aktarılmasını önlememelidir; üçüncü bir ülke tarafından sağlanan koruma seviyesinin yeterliliği, transfer işlemleri veya transfer işlemi çevreleyen tüm koşulların ışığında değerlendirilmelidir;

(57) Diğer taraftan yeterli ve elverişli koruma seviyesini sağlamayan üçüncü bir ülkeye, kişisel verilerin transferi yasaklanmalıdır;

(58) Transferin, yasayla belirlenen bir kayıttan ve meşru menfaate sahip kamu veya kişiler tarafından danışma için yapıldığı veya örneğin, sosyal güvenlik konularında yetkili servisler arasında veya gümrük veya vergi idareleri arasında verilerin uluslararası transferi durumunda, önemli kamu menfaati korumasının bunu gerektirdiği bir sözleşme veya yasal hak talebine ilişkin transferin gerektiği, veri öznesinin rızasını verdiği bazı durumlarda bu yasaktan muafiyet için önlemler alınmalıdır; bu tür bir transferin kayıttaki mevcut tüm veri kategorilerini veya verilerin tümünü gerektirmediği durumlarda ve kayıt, meşru bir menfaate sahip kişiler tarafından danışılma içinse, transfer yalnızca bu kişilerin talebi üzerine veya bunlar alıcı olacaklarsa yapılmalıdır;

(59) Denetleyicinin, uygun korunma önlemleri sunduğu durumlarda, üçüncü bir ülkede koruma olmayışını tazmin etmek için özel önlemler alınmalıdır; ayrıca Topluluk ve bu tür üçüncü ülkeler arasındaki müzakere prosedürleri için önlem alınmalıdır;

(60) Herhangi bir durumda, üçüncü ülkelere transferler, bu Direktif ve özellikle ilgili 8. maddesi uyarınca, yalnızca Üye Devletler tarafından kabul edilen hükümlere tam uygun şekilde gerçekleştirilebilir;

(61) Üye Devletler ve Komisyon, kendi ilgili yetki alanları içinde, uygulanması için benimsenen ulusal hükümleri gözetererek ve bazı sektörlerde yerine getirilen işlemin özel karakteristiklerini göz önüne alarak, bu Direktifin uygulanmasını kolaylaştırmak hususunda, davranış kurallarını düzenlemeleri için ticari birlikleri ve ilgili diğer temsilci kuruluşları teşvik etmelidir;

(62) Denetim makamına ilişkin Üye Devletlerdeki tam bağımsız olarak işlevlerini yerine getiren kuruluşlar; kişisel verilerin işlenmesine dair bireylerin korunmasında, zorunlu bir bileşendir;

(63) Bu tür makamlar, özellikle yasal takibata kalkışma yetkisi ve bireylerden şikayet durumlarında inceleme ve müdahale yetkileri dahil olmak üzere kendi görevlerini yerine getirmek için gerekli araçlara sahip olmalıdır; bu tür makamlar, kendi yetki alanlarındaki Üye Devletlerde; işlemin şeffaflığını sağlamak için yardımcı olmalıdırlar;

(64) Farklı Üye Devletlerdeki makamlar, Avrupa Birliği çapında, koruma kurallarının uygun şekilde gözetilmesini sağlamak için kendi görevlerini yerine getirmede birbirlerini desteklemeye ihtiyaç duyacaklardır;

(65) Topluluk düzeyinde, kişisel verilerin işlenmesine dair Bireylerin Korunması hakkında bir Çalışma Grubu kurulmalıdır ve işlevlerini yerine getirmede tamamen bağımsız olmalıdır; özel yapılarını dikkate alarak, Komisyona tavsiyelerde bulunmalıdır ve özellikle bu Direktif uyarınca kabul edilen ulusal kuralların homojen uygulanmasına katkı sağlamalıdır;

(66) Bu direktif, üçüncü ülkelere verilerin transferine ilişkin olarak, 87/373/EEC4 sayılı Konsey kararında belirtilen şekilde bir prosedürün tesisini ve Komisyon üzerindeki uygulama yetkilerinin verilmesini gerektirir5;

(67) AT Anlaşmasının madde 189 b'sinde öngörülen prosedüre uygun olarak kabul edilen eylemler için tedbirleri uygulamaya dair, Avrupa Parlamentosu, Konsey ve Komisyon arasında GEÇİCİ bir anlaşma üzerine mutabakata 20 Aralık 1994 tarihinde erişilmiştir;

(68) Bu Direktifte düzenlenen kişisel verilerin işlenmesine dair, kişisel mahremiyet hakkı başta olmak üzere; bireylerin hak ve özgürlüklerinin korunmasına dair prensiplere; özellikle, bu prensiplere dayalı özel kurullarla ilgili belirli sektörlerle göre, ilave yapılabilir veya daha açık şekilde anlatılabilir;

(69) Üye Devletlere, önceden devam eden tüm işleme faaliyetlerine, yeni ulusal kuralları kademeli şekilde uygulamak için, bu Direktifin yerini alan ulusal tedbirlerin uygulamaya girdiği yıldan itibaren üç yılı geçemeyen bir süre verilmelidir; maliyet etkin uygulanmasını kolaylaştırmak için, Direktif hükümlerinin bazısıyla mevcut manuel dosyalama sistemlerinin uyumunu sağlamak üzere, bu Direktifin kabul edilme tarihinden 12 yıl sonra biten başka bir süre Üye Devletlere verilecektir; bu tür

dosyalama sistemlerinde bulunan veriler bu genişletilmiş geçiş dönemi esnasında manuel olarak işlenir. Bu sistemler, bu işleme sırasındaki hükümlerle uyumlu hale getirilmelidir;

(70) Bu hükümlerin yürürlüğe girmesinden önce bildirilen rıza ve ücrete dayalı sonuçlandırılan bir sözleşmenin yerine getirilmesinde gerekli herhangi bir hassas veri için, bu Direktif uyarınca alınan ulusal hükümler yürürlüğe girdikten sonra, veri öznesinin sürece devam etmesi için denetleyiciye yine izin vermesine gerek yoktur;

(71) Bu tür düzenleme, kişisel verilerin işlenmesine dair bireylerin korunmasını ilgilendirmediğinde, Bu Direktif, ülkede oturan tüketicilere yönelik pazarlama faaliyetlerini düzenleyen bir üye Devlet yönteminin yerini almaz;

(72) Bu Direktif, bu Direktifte düzenlenen prensipler uygulandığında, dikkate alınması gereken resmi belgelere kamu erişim esaslarına olanak sağlar;

BU DİREKTİFİ KABUL ETMİŞTİR:

Bölüm I

Genel Hükümler

Madde 1

Direktifin Amacı

(1) Bu Direktife uygun olarak, Üye Devletler, kişisel verilerin işlenmesine dair başta kişisel mahremiyet hakkı olmak üzere gerçek kişilerin temel haklarını ve özgürlüklerini koruyacaktır;

(2) Üye Devletler 1. paragraf kapsamında sağlanan korumayla bağlantılı nedenler için Üye Devletler arasında kişisel verilerin akışını yasaklamayacak ya da engellemeyeceklerdir;

Madde 2

Tanımlar

Bu Direktifin amacı için:

a. "kişisel veri" fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen bir tespit edilebilir kişi; tespit edilmiş veya tespit edilebilir gerçek kişiye ("veri öznesi) ilişkin herhangi bir bilgiyi kastedecektir;

- b. "kişisel verilerin işlenmesi (işleme)", silme veya tahrip etme, engelleme, birleştirme veya sıralama, sağlama ya da dağıtma, iletlemeyle açıklama, toplama, kaydetme, organizasyon, depolama, adaptasyon veya değiştirme, kurtarma, danışma gibi otomatik ya da otomatik olmayan araçlarla kişisel veriler üzerinde yapılan herhangi bir faaliyet veya faaliyet dizisini kastedecektir;
- c. "kişisel veri dosyalama sistemi (dosyalama sistemi)" ister merkezi ister merkezi olmayan ya da bir işlevsel veya coğrafi tabana dağıtılmış özel kriterlere göre erişilebilir olan herhangi bir yapılandırılmış kişisel veri dizisini kastedecektir;
- d. "denetleyici", kişisel verilerin işleme araçlarını ve amaçlarını tek başına ya da diğerleriyle ortaklaşa belirleyen gerçek veya tüzel kişiyi, kamu makamını, devlet dairesini veya başka bir kuruluşu kastedecektir; işleme amaçları ve araçları ulusal veya Topluluk hukuku veya yönetmelikleriyle belirlendiğinde, denetleyici veya atanması için özel kriterler, ulusal veya topluluk hukukuyla belirlenebilir;
- e. "işleyici", denetleyici adına kişisel verileri işleyen bir gerçek veya tüzel kişiyi, kamu makamını, devlet dairesini veya diğer bir kuruluşu kastedecektir;
- f. "üçüncü şahıs", veri işlemek için yetkilendirilen işleyici veya denetleyicinin doğrudan yetkisi altındaki kişiler ve işleyici, denetleyici, veri öznesi dışındaki herhangi bir gerçek veya tüzel kişi, kamu makamını, devlet dairesini veya başka bir kuruluşu kastedecektir;
- g. "alıcı", ister bir üçüncü şahıs olsun ya da olmasın, verilerin açıklandığı bir gerçek veya tüzel kişiyi, kamu makamını, devlet dairesini veya başka bir kuruluşu kastedecektir; ancak, özel bir soruşturma çerçevesinde verileri alan makamlar alıcı olarak kabul edilmeyecektir;
- h. "veri öznesinin rızası", kendisine dair kişisel verilerin işlenmesi için veri öznesinin kabulüne işaret eden, özgürce ve bilgilendirilme yapıldıktan sonra alınan rızayı kastedecektir.

Madde 3

Kapsam

(1) Bu Direktif, bir dosyalama sisteminin parçasını oluşturması istenen veya bir dosyalama sisteminin parçasını oluşturan kişisel verilerin otomatik araçlar dışında işlenmesine ve kısmen veya tamamen otomatik araçlarla kişisel verilerin işlenmesine uygulanacaktır.

(2) Bu Direktif, kişisel verilerin işlenmesine uygulanmayacaktır:

- ceza hukuku alanındaki Devlet faaliyetleri ve (işleme faaliyeti Devlet güvenlik konularını ilgilendirdiğinde, Devletin ekonomik refahı dahil olmak üzere) Devlet güvenliği, savunma, kamu

güvenliğine ilişkin verilerin işlenmesi için herhangi bir durumda ve Avrupa Birliği Anlaşmasının V ve VI. başlıklarıyla belirtilenler gibi Topluluk hukuku kapsamının dışına düşen bir faaliyet esnasında, - bir gerçek kişi tarafından, tamamen kişisel veya ev içi faaliyeti esnasında.

Madde 4

Uygulanacak ulusal kanun

(1) Her bir Üye Devlet, aşağıdaki durumlarda, kişisel verilerin işlenmesi için bu Direktif uyarınca kabul ettikleri ulusal hükümleri uygulayacaklardır:

a. İşleme, Üye Devletin topraklarındaki denetleyici kuruluşunun faaliyetleri bağlamında yapıldığında; aynı denetleyici, çeşitli Üye Devletlerin toprağında yerleşikse, bu kuruluşların her birinin, uygulanan ulusal mevzuatlarda öngörülen yükümlülüklere uymasını temin edecek gerekli tedbirleri almalıdır;

b. denetleyici Üye Devletin topraklarında yerleşik olmayıp, uluslararası kamu hukukuna göre ulusal hukukun uygulandığı bir yerde bulunuyorsa;

c. denetleyici Topluluk topraklarında yerleşik değilse ve işleme amaçları için, kişisel veriler, bahse konu Üye devlet topraklarında konumlanan otomatik cihazları kullanırsa, bu tür cihazlar yalnızca Topluluk toprağı boyunca iletme amacı için kullanılmadıkça;

(2) 1 (c) paragrafında atıfta bulunulan koşullarda, denetleyici, denetleyicinin kendisine karşı başlatılabilecek davalara zarar vermeksizin o Üye Devlet toprağında yerleşik bir temsilci atmalıdır.

Bölüm II

Kişisel Verilerin İşlenmesinin Yasallığı Hakkındaki Genel Kurallar

Madde 5

Üye Devletler, bu bölüm hükümlerinin sınırları kapsamında, kişisel verileri işlemenin yasal olduğu koşulları daha hassas şekilde belirleyeceklerdir.

I. Kısım

Veri Kalitesine İlişkin Prensipler

Madde 6

(1) Üye Devletler, kişisel verilerin aşağıdaki şekilde olmasını sağlayacaklardır:

a. adil ve yasal olarak işlenmiş;

- b. belirli, açık ve meşru amaçlar için toplanmış ve bu amaçlarla uyumsuz biçimde başkaca işlenmemiş. Üye Devletlerin uygun korunma önlemleri sağlaması koşuluyla; tarihsel, istatistiksel veya bilimsel amaçlar için verilerin detaylı işlenmesi; uyumsuz olarak kabul edilmeyecektir;
- c. toplandığı ve/veya ayrıca işlendiği amaçlara ilişkin olarak yeterlidir, ilgilidir ve bu amacı aşmaz;
- d. doğrudur ve gerektiği yerde güncel tutulur. Toplanma ve sonrasındaki işleme, silinme veya düzeltilme amaçlarını göz önünde tutarak verilerin yanlış veya eksik olmamasını sağlayacak tüm makul önlemler alınmalıdır;
- e. verilerin toplandığı esnada veya sonrasında işlendiği amaçlar için gerekenden daha uzun olmayan süre boyunca, veri öznelerinin tespitine izin veren biçimde tutulur. Üye Devletler, tarihsel, istatistiksel veya bilimsel kullanım amacıyla daha uzun süreli depolanan kişisel veriler için uygun koruma önlemleri alacaktır.

(2) 1. paragrafta uyulmasını sağlamak, denetleyicinin sorumluluğunda olacaktır.

II. Kısım

Veri İşlemeyi Yasallaştırma Kriterleri

Madde 7

Üye Devletler, kişisel verilerin işlenebilmesini yalnızca aşağıdaki koşullar sağlanırsa sağlayacaklardır:

- a. Veri öznesi açık, kesin ve net bir biçimde rızasını vermişse veya
- b. İşleme, bir sözleşme yapmadan önce veri öznesinin talebi üzerine önlem almak için ya da veri öznesinin taraf olduğu bir sözleşmenin yerine getirilmesi için gerekliyse veya
- c. İşleme denetleyicinin konusu olan bir yasal yükümlülüğe uyum için gerekirse, veya
- d. (d) İşleme, veri öznesinin hayati menfaatlerini korumak için gerekliyse; veya
- e. İşleme, verilerin açıklandığı üçüncü bir şahıs veya denetleyiciye yetki veren kamu makamının uygulamasında veya kamu menfaatine yapılan bir görevin yerine getirilmesi için gerekliyse; veya
- f. İşleme, bu tür menfaatlerin, madde 1(1) kapsamında koruma gerektiren veri öznesinin temel hak ve özgürlükleriyle ilgili menfaatleri çığnemesi haricinde, verilerin açıklandığı üçüncü şahıs veya şahıslar tarafından ya da denetleyici tarafından takip edilen meşru menfaatlerin amaçları için gerekliyse;

III. Kısım

Özel İşleme Kategorileri

Madde 8

Verilerin özel işleme kategorileri

(1) Üye Devletler, sağlık durumuna veya cinsel yaşama ilişkin verilerin işlenmesini ve sendika üyeliğini, dini veya felsefi inançları, siyasi görüşleri, ırk veya etnik kökeni açıklayan kişisel verilerin işlenmesini yasaklayacaktır.

(2) 1. paragraf aşağıdaki durumlarda uygulanmayacaktır:

a. veri öznesinin rızasını vermesiyle 1. paragrafta atıfta bulunulan yasağın kaldırılamayacağını Üye Devlet kanunlarının belirtmesi haricinde, bu verilerin işlenmesinde veri öznesi açık rızasını vermişse; veya

b. işlemenin, yeterli korunma önlemleri için sağlanan ulusal kanunla yetkilendirildiği kadarıyla, istihdam kanunu alanında, denetleyicinin yükümlülüklerini ve özel haklarını yerine getirme amacı için gerekli olduğunda; veya

c. işleme, veri öznesinin rızasını vermesinin fiziksel veya yasal olarak elverişsiz olduğu durumda, diğer bir kişinin veya veri öznesinin hayati menfaatlerini korumak için gerekliyse; veya

d. işleme; veri öznelerinin rızası olmaksızın verilerin üçüncü şahıslara açıklanmadığı ve işlemenin yalnızca amaçlarıyla bağlantılı olarak düzenli iletişimde oldukları kişileri veya kuruluş mensuplarını ilgilendirmesi koşuluyla bir vakıf, dernek veya siyasi, felsefi, dini veya ticaret birliği amaçlı başka bir kar amacı gütmeyen kuruluş tarafından uygun teminatlı meşru faaliyetler esnasında yapılırsa, veya

e. işleme, veri öznesi tarafından açıkça halka duyurulan verilere ilişkinse ya da kanuni hakların tesisi, yerine getirilmesi veya savunulması için gerekliyse.

(3) Paragraf 1, sağlık hizmetlerinin yönetimi veya bakım veya tedavinin sağlanması, tıbbi teşhis, önleyici tıp amaçları için veri işlemenin gerektiği yerde ve mesleki gizlilik yükümlülüğü için ulusal yetkili kuruluşlar tarafından veya eşdeğer gizlilik yükümlülüğüne tabi diğer bir kişi tarafından saptanan ulusal kanun kapsamında bir sağlık uzman öznesi tarafından bu verilerin işlendiği yerde uygulanmayacaktır.

(4) Uygun korunma önlemlerinin sağlanmasına tabi olarak, Üye Devletler, önemli kamu menfaati nedenleri için, ya ulusal yasa ya da denetleme makamının kararıyla paragraf 2'de belirtilenlere ek olarak muafiyetler koyabilir.

(5) Suçlar, adli hükümler veya güvenlik tedbirlerine ilişkin verilerin işlenmesi, yalnızca resmi makamın kontrolü altında yapılabilir veya ulusal yasa kapsamında uygun özel korunma önlemleri sağlanırsa, uygun özel korunma önlemleri sağlayan ulusal hükümler kapsamında Üye Devlet tarafından verilebilecek tadillere tabi olabilir. Ancak, adli hükümlerin tam bir kaydı yalnızca resmi makamın kontrolü altında tutulabilir.

Üye Devletler, hukuk davalarındaki kararlar veya idari müeyyidelere ilişkin verilerin de resmi makamın kontrolü altında işlenmesini sağlayabilirler.

(6) 4 ve 5. paragraflar için 1. paragraftan tadiller komisyona haber verilecektir.

(7) Üye Devletler, ulusal bir tespit numarası veya genel başvurunun diğer belirtecinin işlenebileceği koşulları belirleyecektir.

Madde 9

İfade özgürlüğü ve kişisel verilerin işlenmesi

Üye Devletler, kişisel verilerin ifade özgürlüğünü yöneten kurallarla kişisel gizlilik hakkını uzlaştırmak için gerekirse, yalnızca, edebi veya sanatsal açıklama amacı veya gazetecilik amaçları için kişisel verilerin işlenmesinde Kısım IV ve Kısım VI, bu Bölümün hükümlerinden muafiyetler veya derogasyonlar sağlayacaktır.

IV. Kısım

Veri Öznesine Verilecek Bilgiler

Madde 10

Veri öznesinden verilerin toplanma durumlarında bilgilendirme

Üye Devletler, önceden mevcut olması haricinde, kendine dair bilgilerin toplandığı bir veri öznesine, denetleyici veya temsilcisinin en azından aşağıdaki bilgileri vermesini sağlamalıdır:

- a. Denetleyici ve varsa temsilcisinin kimliği;
- b. Kastedilen veri işleme amaçları;
- c. Aşağıdakiler gibi herhangi bir başka bilgi;

- verilerin alıcıları veya alıcı kategorileri,

- yanıt vermemenin olası sonuçlarının yanı sıra soruların yanıtlarının zorunlu veya gönüllü olup olmadığı,

- (özneyle) ilgili verileri düzeltme hakkının ve verilere erişim hakkının olması, (denetleyici veya temsilcisi) bu tür başka bilgilendirmenin gerekli olmasına göre, verilerin toplanmasındaki özel koşulları göz önünde bulundurarak veri öznesine ilişkin adil işlemeyi garanti etmelidirler.

Madde 11

Verilerin veri öznesinden elde edilmediğinde bilgilendirme

Veriler veri öznesinden elde edilmediğinde, Üye Devletler, (veri öznesinin bu bilgilere) önceden sahip olması hariç, kişisel verilerin kaydının yapılması esnasında ya da üçüncü bir şahsa ifşa öngörüldüğünde, verilerin ilk ifşa zamanından önce, denetleyici veya temsilcisinin en azından aşağıdaki bilgileri veri öznesine vermesini sağlayacaktır:

a. Denetleyicinin ve varsa temsilcisinin kimliği;

b. İşlemenin amaçları;

c. Aşağıdakiler gibi herhangi bir başka bilgi;

- verilerin alıcıları veya alıcı kategorileri,

- yanıt vermemenin olası sonuçlarının yanı sıra soruların yanıtlarının zorunlu veya gönüllü olup olmadığı,

- (özneyle) ilgili verileri düzeltme hakkı ve verilere (kendisinin) erişim hakkının olması,

(denetleyici veya temsilcisi) bu tür başka bilgilendirmenin gerekli olmasına göre, verilerin toplanmasındaki özel koşulları göz önünde bulundurarak veri öznesine ilişkin adil işlemeyi garanti etmelidirler.

Kayıt veya ifşa açıkça yasayla belirtilirse ya da aşırı bir çaba gerektirecek ya da imkansızlığı kanıtlanan verilerin sağlanması için, tarihsel veya bilimsel araştırma amaçları için veya istatistiksel amaçlar için işleme durumunda; Paragraf 1 uygulanmayacaktır. Bu durumlarda, Üye Devletler uygun korunma önlemleri sağlayacaktır.

V. Kısım

Veri Öznelerinin Verilere Erişme Hakkı

Madde 12

Erişim hakkı

Üye Devletler, her veri öznesinin denetleyiciden (aşağıdakileri) temin etme hakkını garanti edecektir:

a. aşırı gecikme veya masraf olmaksızın ve makul aralıklarla, sınırlama olmaksızın:

-kendisine dair verilerin işlenip işlenmeyeceği hususunda onay ve en azından, verilerin açıklandığı alıcı kategorileri veya alıcıları ve ilgili verilerin kategorileri, işleme amaçları hususunda bilgi,

-kaynakları hususunda herhangi bir mevcut bilginin ve işleme tabi tutulan verilerin anlaşılır biçimde ona iletilmesi,

-en azından madde 15(1)'de atıfta bulunulan otomatik kararlar durumunda, kendisine ilişkin verilerin otomatik işlenmesiyle ilgili mantık bilgisi;

b. Özellikle verinin eksik veya yanlış yapısı yüzünden, bu Direktifin hükümlerine uymayan işlemede, verilerin engellenmesi veya silinmesi, uygun olarak düzeltilmesi;

c. Bunun imkansız olduğu gösterilmezse veya orantısız çabayı gerektirmezse, (b) bendine uygun olarak yapılan herhangi bir düzeltme, silme veya engelleme hakkında, verilerin açıklandığı üçüncü şahıslara bildirim.

VI. Kısım

Muafiyetler ve Sınırlamalar

Madde 13

Muafiyetler ve sınırlamalar

(1) Bu tür bir sınırlama, aşağıdakileri sağlamak için gerekli tedbirleri oluşturduğunda, Üye Devletler, 6(1), 10, 11(1), 12 ve 21 maddelerinde belirtilen hak ve yükümlülüklerin kapsamını sınırlandıracak yasal tedbirleri kabul edebilirler:

a. ulusal güvenlik;

b. savunma;

c. kamu güvenliği;

d. düzenlenmiş meslekler için etik ihlallerinin veya ceza gerektiren suçların önlenmesi, incelenmesi, tespiti ve kovuşturulması;

e. parasal, bütçe ve vergilendirme konuları dahil olmak üzere, Avrupa Birliği'nin veya bir Üye Devletin önemli bir ekonomik veya mali menfaati;

f. c), (d) ve (e)'de atıfta bulunulan durumlarda, resmi makamın yürütmesiyle ara sıra da olsa bağlantılı düzenleyici fonksiyon veya izleme, denetim;

g. diğerlerinin hak ve özgürlüklerinin veya veri öznesinin korunması.

(2) Üye Devletler, yeterli yasal korunma önlemlerine tabi olarak özellikle veriler herhangi özel bir bireye dair kararlar veya tedbirler almak için kullanılmadığında, veri öznesinin gizlilik hakkını ihlal riski açıkça yoksa, veriler yalnızca bilimsel araştırma amacı için işlendiğinde veya yalnızca istatistik yaratma amacı için gerekli dönemi aşmayan bir süre için kişisel formda tutulduğunda, madde 12'de belirtilen hakları bir yasama tedbirleriyle sınırlandırabilir.

VII. Kısım

Veri Öznesinin İtiraz Hakkı

Madde 14

Veri öznesinin itiraz hakkı

Üye Devletler aşağıdaki hakları veri öznesine vereceklerdir:

a. En azından madde 7 (e) ve (f)'de atıfta bulunulan durumlarda, ulusal mevzuat tarafından aksinin belirtilmesi haricinde, kendisine dair verilerin işlenmesinde, özel durumuna ilişkin zorlayıcı kanuni gerekçelere her zaman itiraz etmek. Gerekçeli bir itiraz olduğunda, denetleyici tarafından başlatılan işleme, artık bu verileri kapsamayabilir;

b. Denetleyicinin doğrudan pazarlama amaçları için işlenmesini öngördüğü, kendine ait kişisel verilerin işlenmesine ücretsiz ve istek üzerine itiraz etme (hakkı) veya kişisel veriler üçüncü şahıslara ilk kez ifşa edilmeden veya doğrudan pazarlama amaçları için üçüncü şahıslar adına kullanılmadan önce bilgilendirilme (hakkı) ve bu tür ifşalara veya kullanımlara ücretsiz itiraz hakkının açık şekilde sunulması;

Üye Devletler, (b)'nin ilk alt paragrafında atıfta bulunulan hakkın varlığından veri öznelerinin haberdar olmasını temin etmek için gerekli tedbirleri alacaklardır.

Madde 15

Otomatik bireysel kararlar

(1) Üye Devletler, her kişiye, işte performans, kredibilite, güvenilirlik, tutum v.b gibi kendisine ilişkin bazı kişisel yönleri değerlendirmek için yalnızca verilerin otomatik işlenmesine dayalı ve onu önemli derecede etkileyen veya ona ilişkin yasal etkiler üreten bir karara tabi kalmama hakkı verecektir.

(2) Bu Direktifin diğer maddelerine tabi olarak Üye Devletler şayet karar aşağıdaki şekilde alındı veya yetki veriyorsa, 1. paragrafta atıfta bulunulan türde bir karara bir kişinin tabi olabildiğini sağlayacaklardır:

a. kendi görüşünü belirtmesine izin veren düzenlemeler gibi meşru menfaatlerini güvenceye alacak uygun tedbirler olduğunda ya da veri öznesi tarafından sunulan sözleşmenin yapılması veya yerine getirilme talebinin karşılanması koşuluyla bir sözleşmenin yapılması veya yerine getirilmesi esnasında alınrsa veya;

b. öznenin meşru menfaatlerini güvenceye alacak tedbirleri de belirten bir yasa tarafından yetkilendirilirse.

VIII. Kısım

İşlemenin Gizliliği Ve Güvenliği

Madde 16

İşlemenin güvenliği

Kişisel verilere erişme hakkı olan işleyicinin kendisi dahil olmak üzere, işleyicinin veya denetleyicinin yetkisi altındaki herhangi bir kişi, bunu yapması kanun tarafından istenmezse, denetleyicinin talimatı haricinde verileri işlememelidir.

Madde 17 İşlemenin güvenliği

(1) Üye Devletler, özellikle işlemenin bir ağ üzerinde verilerin iletilmesini gerektirdiğinde ve işlemenin tüm diğer yasa dışı biçimlerine karşı, yetkisiz açıklama veya erişim, değiştirme, kazara kayıp veya kazara veya yasa dışı tahribe karşı kişisel verileri korumak için gereken uygun teknik ve kurumsal tedbirleri, denetleyicinin uygulamasını sağlayacaklardır.

Bu tür tedbirler, uygulamalarının durum ve maliyetini dikkate alarak, korunacak verinin yapısına ve işleme tarafından sunulan risklere uygun seviyede güvenlik sağlayacaktır.

(2) Üye Devletler, işleme kendi adına yürütüldüğünde, denetleyicinin yürütülecek işlemeyi yöneten teknik güvenlik tedbirlerine ve kurumsal tedbirlere dair yeterli garantiler sağlayan bir işleyiciyi seçmesini ve bu tedbirlerle uyum sağlamasını temin edecektir.

(3) İşleyici vasıtasıyla işlemenin yapılması özellikle aşağıdakileri şart koşan ve işleyiciyi denetleyiciye bağlayan yasal belge veya bir sözleşme ile yönetilmelidir:

- işleyici yalnızca denetleyiciden gelen talimatlara göre hareket edecektir.

- işleyicinin yerleşik olduğu Üye Devlet kanunuyla tanımlandığı şekilde, 1. paragrafta düzenlenen yükümlülükler işleyicinin de ödevi olacaktır.

(4) Paragraf 1'de atıfta bulunulan tedbirlere dair koşullara ve veri korunmasına ilişkin yasal belge veya sözleşmenin parçaları, kanıtı tutma amaçları için yazılı veya eşdeğer diğer bir biçimde olacaktır.

IX. Kısım

Bildirim

Madde 18

Denetleme makamına bildirimde bulunma yükümlülüğü

(1) Üye Devletler, kısmen veya tamamen otomatik işleme faaliyeti veya tek amaç veya ilgili çeşitli amaçlara hizmet etmesi istenen bu tür bir dizi faaliyeti yürütmeden önce denetleyici ve varsa temsilcisinin, madde 28'de atıfta bulunulan denetleme makamına bildirimde bulunmasını sağlayacaklardır.

(2) Üye Devletler, yalnızca aşağıdaki durumlarda ve aşağıdaki koşullarda bildirimden muafiyeti veya bildirim basitleştirilmesini sağlayabilirler:

- veri öznelerinin haklarını ve özgürlüklerini olumsuz şekilde etkileyecek, işlenecek verileri muhtemelen dikkate almayan işleme faaliyeti kategorileri için, depolanacak veriler süre uzunluğu ve verilerin ifşa edileceği alıcılar veya alıcı kategorileri, veri öznesi kategorisi veya kategorileri, işlemeye tabi veri kategorileri veya veriler, işleme amaçlarını belirtirler, ve/veya;

- denetleyici, kendisini yöneten ulusal kanunla uyumlu olarak özellikle aşağıdakilerden sorumlu bir kişisel veri koruma görevlisi atar;

- bu Direktif uyarınca, alınan ulusal hükümlerin bağımsız şekilde dahili uygulamasını sağlama;

- madde 21(2)'de atıfta bulunulan bilgilendirme maddelerini içeren şekilde, denetleyici tarafından yürütülen işleme faaliyetlerinin kaydını tutma;

- böylece, veri öznelerinin hak ve özgürlüklerinin, işleme faaliyetleri tarafından olumsuz şekilde etkilenmesinin olanaksız olmasını sağlama.

(3) Üye Devletler, bir meşru menfaat gösteren herhangi bir kişi tarafından veya genel olarak kamu tarafından danışmaya açık olan ve kamuya bilgi sağlamak amaçlı kanunlara veya yönetmeliklere göre tek amacı bir kayıt tutma olan işlemeye 1. paragrafın uygulanmamasını sağlayabilir.

(4) Üye Devletler, madde 8(2)(d)'de atıfta bulunulan işleme faaliyetleri durumunda, bildirim basitleştirilmesini veya bildirimde bulunma yükümlülüğünden muafiyeti sağlayabilirler.

(5) Üye Devletler, kişisel verileri kapsayan belirli veya tüm otomatik olmayan işleme faaliyetlerinin bildirilmesini şart koşabilirler ya da bu işleme faaliyetlerinin basitleştirilmiş bildirim tabi olmasını belirtebilirler.

Madde 19

Bildirim içeriği

(1) Üye Devletler, bildirimde verilecek bilgileri belirteceklerdir. Bunlar en azından aşağıdakileri içerecektir:

- a. Denetleyici ve varsa temsilcisinin adı ve adresi;
- b. İşlemenin amacı veya amaçları;
- c. Bunlara ilişkin veri kategorileri veya verinin ve özne verisinin kategorileri veya kategorisinin tanımı;
- d. Verilerin açıklanabileceği alıcılar veya alıcı kategorileri;
- e. Üçüncü ülkelere önerilen veri transferleri;
- f. Veri güvenliğini sağlamak üzere madde 17 uyarınca alınan tedbirlerin uygunluğunun sağlanması için bir ön değerlendirmeye olanak sağlayan genel bir tanım;

(2) Üye Devletler paragraf 1'de atıf yapılan bilgileri etkileyen herhangi bir değişikliğin denetleme makamına bildirilmesine dönük prosedürleri belirletecektir.

Madde 20

Ön kontrol

(1) Üye Devletler, veri öznelerinin haklarına ve özgürlüklerine özel riskler sunması, olası işleme faaliyetlerini belirleyecektir ve bu işleme faaliyetlerinin başlatılmasından önce incelenmesini kontrol edecektir.

(2) Bu tür ön kontroller, şüphe durumunda denetim makamına danışması gereken bir veri koruma görevlisi tarafından veya denetleyiciden bir bildirim alınmasını takiben denetleme makamı tarafından yerine getirilecektir.

(3) Üye Devletler ya ulusal parlamentonun bir tedbiri ya da işlemenin yapısını tanımlayan ve uygun korunma önlemlerini belirten bu tür bir yasama tedbirine dayalı bir tedbirin hazırlanması bağlamında, bu tür kontrolleri de yapabilir.

Madde 21

İşleme faaliyetlerinin duyurulması

(1) Üye Devletler, işleme faaliyetlerinin duyurulmasını temin etmek için tedbirler alacaktır.

(2) Üye Devletler, madde 18'e uygun olarak, bildirilen işleme faaliyetlerinin bir kaydının denetleme makamı tarafından tutulmasını sağlayacaktır.

Kayıt, en azından madde 19(1) (a) (e) de listelenen bilgileri içerecektir.

Kayıt herhangi bir kişi tarafından denetlenebilir.

(3) Üye Devletler, bildirim tabi olmayan işleme faaliyetlerine ilişkin olarak, Üye Devletler tarafından atanan denetleyicilerin veya diğer bir kuruluşun, talep üzerine herhangi bir kişiye uygun biçimde en azından madde 19(1) (a) (e)de atıfta bulunulan bilgileri sağlamasını temin edecektir.

Üye Devletler ya meşru menfaat kanıtını temin edebilen herhangi bir kişi tarafından ya da genel olarak kamu tarafından danışmaya açık olan ve kamuya bilgi sağlaması kastedilen yönetmeliklere veya yasalara göre; tek amacı bir kayıt tutulması olan işlemeye bu hükmün uygulanmamasını sağlayabilir.

Bölüm III

Yargı Yolları, Sorumluluk Ve Müeyyideler

Madde 22

Yargı yolları

Yargı makamına başvurudan önce, madde 28'de atıfta bulunulan denetleme makamı öncesinde, diğerlerine ilaveten koyulabilecek hüküm için herhangi bir idari çözüme zarar vermeksizin, Üye Devletler, söz konusu işlemeye uygulanan ulusal kanun tarafından garanti edilen hakların herhangi bir ihlali için bir yargı yolunu, her kişinin hakkı olarak sağlayacaktır.

Madde 23

Sorumluluk

(1) Üye Devletler, bu Direktif uyarınca kabul edilen ulusal hükümlerle uyumsuz herhangi bir işlemenin veya yasadışı bir işleme faaliyetinin sonucu olarak zarara uğrayan herhangi bir kişinin, uğradığı zarar için denetleyiciden tazminat almaya hak kazanmasını sağlayacaktır.

(2) Denetleyici, zarara yol açan olayda sorumlu olmadığını kanıtlarsa, kısmen ya da tamamen bu yükümlülükten muaf tutulabilir.

Madde 24

Müeyyideler

Üye Devletler, bu Direktifin hükümlerinin tam uygulanmasını sağlayacak uygun tedbirleri kabul edecektir ve özellikle, bu direktif uyarınca kabul edilen hükümlerin ihlali durumunda uygulanacak müeyyideleri koyacaktır.

Bölüm IV

Kişisel Verilerin Üçüncü Ülkelere Transferi

Madde 25

Prensipeler

(1) Üye Devletler, bu Direktifin diğer hükümleri uyarınca benimsenen ulusal hükümlere uyuma zarar vermeksizin, yalnızca söz konusu üçüncü ülke yeterli koruma seviyesi sağlarsa, transfer sonrası işleme için istenen veya işlemeye tabi olan kişisel verilerin bir üçüncü ülkeye transferinin gerçekleşebilmesini sağlayacaktır.

(2) Bir üçüncü ülke tarafından sağlanan koruma seviyesinin yeterliliği, veri transfer faaliyetlerinin dizisinin veya bir veri transfer faaliyetini çevreleyen tüm koşulların ışığında değerlendirilecektir. O ülkeyle uyumlu meslek kuralları ve güvenlik tedbirleri ve söz konusu üçüncü ülkedeki yürürlükte olan hem genel hem sektörel yasa hükümleri, son varış ülkesi ve menşe ülke, önerilen faaliyet veya faaliyetlerin süresi ve amacı, verilerin yapısına özel önem verilecektir.

(3) Üye Devletler ve Komisyon, 2. paragrafın anlamı dahilinde yeterli koruma seviyesini bir üçüncü ülkenin sağlamadığını düşündükleri durumlarda birbirlerini bilgilendireceklerdir.

(4) Komisyon, bu maddenin 2. paragrafının anlamında, bir üçüncü ülkenin yeterli koruma seviyesini sağlamadığını madde 31 (2) kapsamında sağlanan prosedüre göre tespit ederse, Üye Devletler, söz konusu üçüncü ülkeye aynı tipte verilerin herhangi bir transferini önlemek için gerekli önlemleri alacaklardır.

(5) Komisyon, uygun bir zamanda, paragraf 4 uyarınca sağlanan bulgudan kaynaklanan durumu çözmek amacıyla müzakerelere başlayacaktır.

(6) Komisyon, madde 31 (2)'de atıfta bulunulan prosedüre uygun olarak; bireylerin temel haklarının ve özel yaşamlarının korunması için, özellikle paragraf 5'te atıfta bulunulan müzakerelerin sonuçlanması üzerine, giriştiği uluslararası taahhütler veya kendi yerel yasası nedeniyle, bu maddenin 2. paragrafı anlamı dahilinde üçüncü bir ülkenin yeterli bir koruma seviyesini temin etmesini isteyebilir.

Üye Devletler, Komisyonun kararıyla uyum sağlamak için gerekli tedbirleri alacaktır.

Madde 26,

İstisnalar

(1) Madde 25'den derogasyon (uygulama dışı tutma) yoluyla ve özel durumları yöneten iç hukukun aksini belirtmesi haricinde, Üye Devletler, aşağıdaki koşullarda madde 25 (2)'nin anlamı dahilinde yeterli koruma seviyesini sağlamayan üçüncü bir ülkeye kişisel verilerin transfer dizisini veya transferinin yapılabilmesini sağlayacaktır:

- a. Veri öznesi önerilen transfer için açık şekilde rızasını vermişse veya
- b. Veri öznesinin talebine yanıt olarak alınan ön sözleşme tedbirlerinin uygulanması veya denetleyici ve veri öznesi arasındaki bir sözleşmenin yerine getirilmesi için transfer gerekliyse; veya
- c. Üçüncü bir şahıs ve denetleyici arasında veri öznesinin menfaatine sonuçlanan bir sözleşmenin yerine getirilmesi veya sonuçlandırılması için transfer gerekliyse, veya
- d. Transfer; kanuni hakların tesisi, işletilmesi veya savunulması için veya önemli kamu menfaati zemininde yasal olarak gerekliyse veya zorunluysa, veya
- e. Veri öznesinin hayati menfaatlerinin korunması için transfer gerekirse, veya
- f. Özel durumda yapılan konsültasyon için kanunda öngörülen koşullar ölçüsünde, bir meşru menfaat gösteren herhangi bir kişi tarafından veya genel olarak kamu tarafından danışmaya açık olan ve kamuya bilgi sağlamak amaçlı kanunlar veya yönetmeliklere göre transfer bir kayıttan sağlanırsa.

(2) Paragraf 1'e zarar vermeksizin, bir Üye Devlet, ilgili hakların işletilmesine dair ve bireylerin temel hak ve özgürlükleri ve kişisel mahremiyet hakkının korunmasına ilişkin anlam dahilinde, yeterli koruma seviyesini sağlamayan üçüncü bir ülkeye kişisel veri transferler dizisine veya bir transferine izin verebilir, bu tür korunma önlemleri özellikle uygun sözleşme maddelerinden kaynaklanabilir.

(3) Üye Devlet, paragraf 2 uyarınca verdiği izinlerden Üye Devletleri ve Komisyonu haberdar edecektir.

Bir Üye Devlet veya Komisyon, bireylerin temel hakları ve özgürlükleri ve mahremiyetinin korunmasını gerektiren gerekçeli dayanaklara itiraz ederse, Komisyon, madde 31 (2)'de belirtilen prosedüre göre uygun tedbirleri alacaktır.

Üye Devletler Komisyonun kararına uymak için gerekli tedbirleri alacaklardır.

(4) Madde 31 (2)'de atıfta bulunulan prosedüre uygun olarak, Komisyon, bazı standart sözleşme maddelerinin paragraf 2'nin gerektirdiği şekilde yeterli teminat sunmasına karar verirse, Üye Devletler, Komisyon kararına uymak için gerekli tedbirleri alacaklardır.

Bölüm V

Davranış Kuralları

Madde 27

(1) Üye Devletler ve Komisyon, çeşitli sektörlerin özel niteliklerini dikkate alarak, bu Direktif uyarınca Üye Devletler tarafından benimsenen ulusal hükümlerin doğru uygulanmasına katkı sağlamak için planlanan davranış kurallarını düzenlemeye teşvik edecektir.

(2) Üye Devletler, mevcut ulusal kodları tadil etme veya genişletme niyetine sahip veya taslak ulusal kodları hazırlamış denetleyicilerin diğer kategorilerini temsil eden diğer kuruluşlar ve ticari kurumların, davranış kurallarını ulusal makamın görüşüne sunabilmesi için önlem alacaktır.

Üye Devletler, sunulan taslakların, bu Direktif uyarınca kabul edilen ulusal hükümlerle uyumlu olup olmadığını ulusal makamın belirlemesi için önlem alacaktır. Komisyon, taslağı uygun görürse, ulusal makam, kendi temsilcilerinin veya veri öznelerinin görüşlerini isteyecektir.

(3) Taslak Topluluk kodları ve mevcut Topluluk kodlarının uzantıları veya düzeltmeleri, madde 29'da atıfta bulunulan çalışma grubuna sunulabilir. Bu çalışma grubu diğer şeyler arasında, sunulan taslağın, bu Direktif uyarınca kabul edilen ulusal hükümlere uygun olup olmadığını belirleyecektir. Uygun bulursa, (ulusal) makam, veri öznelerinin ve kendi temsilcilerinin görüşlerini isteyecektir. Komisyon, Çalışma Grubu tarafından onaylanmış kuralların uygun şekilde tanıtımını sağlayabilir.

Bölüm VI

Kişisel Verilerin İşlenmesine Dair Bireylerin Korunması Hakkındaki Çalışma Grubu ve Denetleme Makamı

Madde 28

Denetleme makamı

(1) Her bir Üye Devlet, , bu Direktif uyarınca Üye Devletler tarafından kabul edilen hükümlerin kendi ülkesindeki uygulamasını izlemekten, bir veya daha fazla kamu makamının sorumlu olmasını sağlayacaktır.

Bu makamlar, onlara tevdi edilen işlevleri yerine getirmede tam bağımsız olarak hareket edeceklerdir.

(2) Her bir Üye Devlet, kişisel verilerin işlenmesine dair bireylerin hak ve özgürlüklerinin korunmasına ilişkin idari tedbirleri veya yönetmelikleri hazırlarken, denetim makamına danışılmasını sağlayacaktır.

(3) Her bir makama özellikle sağlanacaktır:

- denetim görevlerinin yerine getirilmesi için gerekli tüm bilgileri toplama yetkileri ve işleme faaliyetlerinin konusunu oluşturan verilere erişim yetkileri gibi araştırma yetkileri;
- örneğin ulusal parlamentolar veya diğer siyasi kuruluşlara konuyu havale etme veya denetleyiciye ihtar verme veya uyarma, işleme üzerinde GEÇİCİ veya kesin yasaklama koyma, verilerin yok edilmesini veya silinmesini, engellenmesini emretme, bu tür görüşlerin uygun şekilde yayınlanmasını sağlama ve madde 20'e uygun olarak işleme faaliyetlerinin yerine getirilmesinden önce görüş bildirme gibi etkin müdahale yetkileri;
- Bu Direktif uyarınca kabul edilen ulusal hükümler ihlal edildiğinde veya bu ihlalleri yargı makamlarının dikkatine sunma için kanuni kovuşturmaya girişme yetkisi.

Denetleme makamının şikayetlere yol açan kararları; mahkemelerde temyiz edilebilir.

(4) Her bir denetim makamı, kişisel verilerin işlenmesine dair hak ve özgürlüklerin korunmasına ilişkin o kişiyi temsil eden bir dernek veya herhangi bir kişi tarafından arzedilen iddiaları dinleyecektir.

Her bir denetim makamı, özellikle, bu Direktifin 13. maddesi uyarınca kabul edilen ulusal hükümler uygulandığında, herhangi bir kişi tarafından arz edilen veri işlemenin yasallığı hakkındaki kontroller için iddiaları dinleyecektir. Kişi, bir kontrolün yapıldığından her halükarda bilgilendirilecektir.

(5) Her denetleme makamı, faaliyetleri hakkında düzenli aralıklarla bir rapor hazırlayacaktır. Rapor, kamuya açıklanacaktır.

(6) Her denetleme makamı, sözkonusu işlemeye uygulanan ulusal kanun her ne olursa olsun, paragraf 3'e uygun olarak verilen yetkileri kendi Üye Devletinin toprağında uygulamaya yetkilidir. Her bir makamdan, diğer bir Üye Devletin makamı ile yetkilerini uygulaması istenebilir.

Denetleme makamları, özellikle tüm yararlı bilgileri takas ederek, kendi görevlerini yerine getirmek için gerekli ölçüde birbirleriyle iş birliği yapacaklardır.

(7) Üye Devletler, görevlerinin bitiminden sonra bile, denetleme makamının personellerinin ve mensuplarının, eriştikleri gizli bilgilere dair mesleki gizlilik görevine tabi olmalarını sağlayacaktır.

Madde 29

Kişisel Verilerin İşlenmesine dair Bireylerin Korunması Hakkındaki Çalışma Grubu

(1) Bundan böyle "Çalışma Grubu" denilecek olan, Kişisel Verilerin İşlenmesine dair Bireylerin Korunması hakkında bir çalışma grubu, bu belgeyle kurulmaktadır.

Danışma statüsüne sahip olacak ve bağımsız olarak hareket edecektir.

(2) Çalışma Grubu, Komisyon'un bir temsilcisi ve Topluluk kurumları ve kuruluşları için kurulan makamların veya makamın birer temsilcisi ve her bir Üye Devlet tarafından atanan denetleme makamı veya makamlarının birer temsilcisinden oluşacaktır.

Çalışma Grubunun her bir üyesi, temsil ettikleri makam veya makamlar, kurumlar tarafından atanacaklardır. Bir Üye Devlet birden fazla denetleme makamı atamışsa, bunlar ortak bir temsilci atayacaklardır. Aynısı, Topluluk kurum ve kuruluşları için saptanan makamlara uygulanacaktır.

(3) Çalışma Grubu, denetleme makamları temsilcilerinin salt (kendi) çoğunluğuyla kararlar alacaktır.

(4) Çalışma Grubu, başkanını seçer. Başkanın görev süresi iki yıl olacaktır. Başkan yeniden seçilebilecektir.

(5) Çalışma Grubunun sekreteryası Komisyon tarafından sağlanacaktır.

(6) Çalışma Grubu, kendi prosedür kurallarını kabul edecektir.

(7) Çalışma Grubu, ya Komisyon'un talebi veya denetleme makamının bir temsilcisinin talebi üzerine veya kendi inisiyatifıyla, başkanı tarafından gündemine getirilen maddeleri ele alacaktır.

Madde 30

(1) Çalışma Grubu:

a. Bu tür tedbirlerin düzenli uygulanmasına katkı sağlamak için bu Direktif kapsamında benimsenen ulusal tedbirlerin uygulanmasını kapsayan herhangi bir sorunu inceleyecektir;

- b. Topluluktaki ve üçüncü ülkelerdeki koruma seviyesi hakkında Komisyon'a görüş verecektir;
- c. Kişisel verilerin işlenmesine dair gerçek kişilerin hak ve özgürlüklerini güvenceye alacak ek veya özel tedbirler hakkında ve bu tür hak ve özgürlükleri etkileyen diğer önerilmiş Topluluk tedbirleri hakkında, bu Direktifin herhangi bir önerilen tadili üzerinde Komisyona tavsiyede bulunacaktır;
- d. Topluluk seviyesinde hazırlanan davranış kuralları hakkında görüş verecektir.

(2) Çalışma Grubu, Topluluktaki kişisel verilerin işlenmesine dair kişilerin korunmasında eşdeğerliği muhtemelen etkileyecek uyumsuzlukların Üye Devletlerin uygulamalarından ya da kanunlarından kaynaklandığını saptarsa, bu doğrultuda Komisyon'u bilgilendirecektir.

(3) Çalışma Grubu kendi inisiyatifiyle, Toplulukta kişisel verilerin işlenmesine dair kişilerin korunmasına ilişkin tüm konularda tavsiyelerde bulunabilir.

(4) Çalışma Grubunun fikirleri ve tavsiyeleri, madde 31'de atıfta bulunulan komiteye ve Komisyon'a iletilecektir.

(5) Komisyon, görüş ve tavsiyelerine yanıt olarak aldığı önlemleri Çalışma Grubu'na bildirecektir. Bunu Avrupa Parlamentosu ve Konseyi'ne de iletilecek bir raporla yapacaktır. Rapor kamuya açık olacaktır.

(6) Çalışma Grubu, Komisyon, Avrupa Parlamentosu ve Konseyi'ne iletilecek olan üçüncü ülkelerde ve topluluktaki kişisel verilerin işlenmesine dair gerçek kişilerin korunmasına dair durum hakkında bir yıllık rapor hazırlayacaktır. Rapor halka duyurulacaktır.

Bölüm VII

Tedbirleri Uygulayan Topluluk

Madde 31

Komite

(1) Komisyon'a, Üye Devletlerin temsilcilerinden oluşan ve başkanlığını Komisyon temsilcisinin yaptığı bir Komite yardımcı olacaktır.

(2) Komisyon temsilcisi, komiteye, alınacak önlemlerin bir taslağını sunacaktır. Komite, taslak hakkındaki görüşlerini başkan tarafından konunun aciliyetine bağlı olarak saptanacak olan bir süre içinde bildirecektir.

Görüş, Antlaşmanın madde 148 (2) saptanmış olan çoğunluk ile bildirilecektir. Komitede Üye Devletlerin temsilcilerinin oyları, aynı Madde'de belirtildiği şekilde ağırlık taşıyacaktır. Başkan, oy kullanmayacaktır.

Komisyon, derhal uygulanacak olan önlemleri benimseyecektir. Ancak, eğer bu önlemler komitenin görüşüne uygun değilse, Komisyon tarafından Konsey'e derhal iletilecektir. Böyle bir durumda:

- Komisyon, üzerinde karar varmış olduğu önlemlerin uygulanmasını, söz konusu iletiyi aldığı tarihten itibaren üç aylık bir süre için erteleyecektir,

- Konsey, birinci paragrafta belirtilmiş olan süre zarfında nitelikli çoğunlukla hareket ederek farklı bir karar alabilir.

Nihai Hükümler

Madde 32

(1) Üye Devletler, bu Direktifle uyum sağlamak için gerekli idari hükümleri, yasaları ve yönetmelikleri kabul edilme tarihinden itibaren en geç üç yıllık dönemin bitimine kadar yürürlüğe koyacaklardır.

Üye Devletler bu kararları kabul ettiğinde, bunlar, bu Direktife bir atfı içerecektir veya kendi resmi yayımları dolayısıyla bu tür bir atf eşlik edecektir. Bu tür referans yapma yöntemleri, Üye Devletler tarafından öngörülecektir.

(2) Üye Devletler, bu Direktif uyarınca kabul edilen ulusal hükümlerin yürürlüğe girdiği tarihte devam eden işlemenin; bu yürürlük tarihinden itibaren üç yıl içinde, bu hükümlerle uygun hale getirilmesini temin edeceklerdir.

Önceki alt paragraftan derogasyon yoluyla, Üye Devletler, bu Direktifin uygulanmasına ilişkin benimsenen ulusal hükümlerin yürürlüğe koyulduğu tarihte manuel dosyalama sisteminde tutulan verilerin işlenmesinin kabul tarihinden itibaren 12 yıl içinde, bu Direktifin 6, 7 ve 8. maddelerine uyumlu hale getirilmesini sağlayabilirler. Ancak, Üye Devletler, denetleyici tarafından izlenen meşru amaçlarla uyumsuz bir biçimde depolanan veya eksik, yanlış olan verilerin engellenmesi veya silinmesi, düzeltilmesi ve elde etme hakkını, özellikle erişim hakkını yerine getirme zamanında ve talebi üzerine veri öznesine vereceklerdir.

(3) Paragraf 2'den derogasyon yoluyla, Üye Devletler, uygun korunma önlemlerine tabii olarak, yalnızca, tarihsel araştırma amacıyla tutulan verilerin bu Direktifin 6, 7 ve 8. Maddesine uyumlu hale getirilmesine gerek olmadığını belirtebilirler.

(4) Üye Devletler, bu Direktifle kapsanan alanda kabul ettikleri iç hukuk hükümlerinin metnini Komisyona iletacaktır.

Madde 33

Komisyon, gerekirse, tadiller için uygun önerileri raporuna ekleyerek, bu Direktifin uygulanması hakkında madde 326 de atıfta bulunulan tarihin 3 yıl öncesinden başlayarak düzenli aralıklarla Avrupa Parlamentosu ve Konseye rapor sunacaktır. Rapor halka duyurulacaktır.

Komisyon, özellikle, gerçek kişilere ilişkin ses ve görüntü verilerinin işlenmesinde bu Direktifin uygulanmasını inceleyecektir ve bilgi toplumundaki ilerleme durumunun ışığında ve bilgi teknolojisindeki gelişmeleri dikkate alarak gerekeceği kanıtlanan herhangi uygun önerileri sunacaktır.

Madde 34

Bu Direktif Üye Devletlere hitap etmektedir.

Avrupa Birliđi - 95/46 sayılı Direktif (İngilizce)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Official Journal L 281 , 23/11/1995 P. 0031 - 0050

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(6) Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

(9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

(12) Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

(13) Whereas the activities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the activities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56 (2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

(14) Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;

(15) Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;

(16) Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;

(17) Whereas, as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9;

(18) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which

the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

(21) Whereas this Directive is without prejudice to the rules of territoriality applicable in criminal matters;

(22) Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

(23) Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws such as those relating, for example, to statistical institutes;

(24) Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive;

(25) Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

(26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

(27) Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques

used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2 (c), the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set, may be laid down by each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive;

(28) Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;

(29) Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;

(30) Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

(31) Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;

(32) Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association;

(33) Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;

(34) Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection - especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;

(35) Whereas, moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations is carried out on important grounds of public interest;

(36) Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established;

(37) Whereas the processing of personal data for purposes of journalism or for purposes of literary or artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and

impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities;

(38) Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection;

(39) Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;

(40) Whereas, however, it is not necessary to impose this obligation if the data subject already has the information; whereas, moreover, there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;

(41) Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

(42) Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;

(43) Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

(44) Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above;

(45) Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

(46) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

(47) Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

(48) Whereas the procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive;

(49) Whereas, in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided for by Member States in cases where processing is unlikely adversely to affect the rights and freedoms of data subjects, provided that it is in accordance with a measure taken by a Member State specifying its limits; whereas exemption or simplification may similarly be provided for by Member States where a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects; whereas such a data protection official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence;

(50) Whereas exemption or simplification could be provided for in cases of processing operations whose sole purpose is the keeping of a register intended, according to national law, to provide information to the public and open to consultation by the public or by any person demonstrating a legitimate interest;

(51) Whereas, nevertheless, simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive;

(52) Whereas, in this context, ex post facto verification by the competent authorities must in general be considered a sufficient measure;

(53) Whereas, however, certain processing operation are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their legislation;

(54) Whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out; whereas following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing; whereas such checking may equally take place in the course of the preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing and lays down appropriate safeguards;

(55) Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeure; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive;

(56) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

(58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

(59) Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

(60) Whereas, in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

(61) Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation;

(62) Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) Whereas such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; whereas such authorities must help to ensure transparency of processing in the Member States within whose jurisdiction they fall;

(64) Whereas the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union;

(65) Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of its functions; whereas, having regard to its specific nature, it must advise the Commission and, in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive;

(66) Whereas, with regard to the transfer of data to third countries, the application of this Directive calls for the conferment of powers of implementation on the Commission and the establishment of a procedure as laid down in Council Decision 87/373/EEC (1);

(67) Whereas an agreement on a modus vivendi between the European Parliament, the Council and the Commission concerning the implementing measures for acts adopted in accordance with the procedure laid down in Article 189b of the EC Treaty was reached on 20 December 1994;

(68) Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

(69) Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules progressively to all processing operations already under way; whereas, in order to facilitate their cost-effective implementation, a further period expiring 12 years after the date on which this Directive is adopted will be allowed to Member States to ensure the conformity of existing manual filing systems with certain of the Directive's provisions; whereas, where data contained in such filing systems are manually processed during this extended transition period, those systems must be brought into conformity with these provisions at the time of such processing;

(70) Whereas it is not necessary for the data subject to give his consent again so as to allow the controller to continue to process, after the national provisions taken pursuant to this Directive enter into force, any sensitive data necessary for the performance of a contract concluded on the basis of free and informed consent before the entry into force of these provisions;

(71) Whereas this Directive does not stand in the way of a Member State's regulating marketing activities aimed at consumers residing in territory in so far as such regulation does not concern the protection of individuals with regard to the processing of personal data;

(72) Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2

Definitions

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

- by a natural person in the course of a purely personal or household activity.

Article 4

National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

CHAPTER II

GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

SECTION I

PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:

- (a) processed fairly and lawfully;
- (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
- (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II

CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7

Member States shall provide that personal data may be processed only if:

- (a) the data subject has unambiguously given his consent; or
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
- (d) processing is necessary in order to protect the vital interests of the data subject; or
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

SECTION III

SPECIAL CATEGORIES OF PROCESSING

Article 8

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.
2. Paragraph 1 shall not apply where:
 - (a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or
 - (b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
 - (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9

Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic

purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

SECTION IV

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10

Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

- (a) the identity of the controller and of his representative, if any;
 - (b) the purposes of the processing for which the data are intended;
 - (c) any further information such as
 - the recipients or categories of recipients of the data,
 - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
 - the existence of the right of access to and the right to rectify the data concerning him
- in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11

Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

- (a) the identity of the controller and of his representative, if any;
- (b) the purposes of the processing;
- (c) any further information such as
 - the categories of data concerned,

- the recipients or categories of recipients,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

SECTION V

THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12

Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

SECTION VI

EXEMPTIONS AND RESTRICTIONS

Article 13

Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

SECTION VII

THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14

The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Article 15

Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

SECTION VIII

CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 16

Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

SECTION IX

NOTIFICATION

Article 18

Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or

- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive

- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Article 19

Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:

(a) the name and address of the controller and of his representative, if any;

(b) the purpose or purposes of the processing;

- (c) a description of the category or categories of data subject and of the data or categories of data relating to them;
- (d) the recipients or categories of recipient to whom the data might be disclosed;
- (e) proposed transfers of data to third countries;
- (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

Article 20

Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.
2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.
3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

Article 21

Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.
2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.

The register shall contain at least the information listed in Article 19 (1) (a) to (e).

The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request.

Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest.

CHAPTER III

JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 22

Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23

Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24

Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

CHAPTER IV

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

- (a) the data subject has given his consent unambiguously to the proposed transfer; or
- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
- (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
- (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
- (e) the transfer is necessary in order to protect the vital interests of the data subject; or
- (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER V

CODES OF CONDUCT

Article 27

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

CHAPTER VI

SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 28

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 29

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up.

It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies.

3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

4. The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.

5. The Working Party's secretariat shall be provided by the Commission.

6. The Working Party shall adopt its own rules of procedure.

7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.

Article 30

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

CHAPTER VII

COMMUNITY IMPLEMENTING MEASURES

Article 31

The Committee

1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.

2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter.

The opinion shall be delivered by the majority laid down in Article 148 (2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairman shall not vote.

The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. In that event:

- the Commission shall defer application of the measures which it has decided for a period of three months from the date of communication,
- the Council, acting by a qualified majority, may take a different decision within the time limit referred to in the first indent.

FINAL PROVISIONS

Article 32

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption.

When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall ensure that processing already under way on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within three years of this date.

By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 of this Directive within 12 years of the date on which it is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.

3. By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research need not be brought into conformity with Articles 6, 7 and 8 of this Directive.

4. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field covered by this Directive.

Article 33

The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32 (1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public.

The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.

Article 34

This Directive is addressed to the Member States.

Done at Luxembourg, 24 October 1995.

For the European Parliament

The President

K. HAENSCH

For the Council

The President

L. ATIENZA SERNA

(1) OJ No C 277, 5. 11. 1990, p. 3 and OJ No C 311, 27. 11. 1992, p. 30.

(2) OJ No C 159, 17. 6. 1991, p 38.

(3) Opinion of the European Parliament of 11 March 1992 (OJ No C 94, 13. 4. 1992, p. 198), confirmed on 2 December 1993 (OJ No C 342, 20. 12. 1993, p. 30); Council common position of 20 February 1995 (OJ No C 93, 13. 4. 1995, p. 1) and Decision of the European Parliament of 15 June 1995 (OJ No C 166, 3. 7. 1995).

(1) OJ No L 197, 18. 7. 1987, p. 33.

Avrupa Birliđi - E-Mahremiyet Direktifi (E-Privacy Directive)

2002/58 sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin Korunmasına İlişkin Direktif

Consolidated text: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Article 1 - Scope and aim

Article 2 - Definitions

Article 3 - Services concerned

Article 4 - Security of processing

Article 5 - Confidentiality of the communications

Article 6 - Traffic data

Article 7 - Itemised billing

Article 8 - Presentation and restriction of calling and connected line identification

Article 9 - Location data other than traffic data

Article 10 - Exceptions

Article 11 - Automatic call forwarding

Article 12 - Directories of subscribers

Article 13 - Unsolicited communications

Article 14 - Technical features and standardisation

Article 14a - Committee procedure

Article 15 - Application of certain provisions of Directive 95/46/EC

Article 15a - Implementation and enforcement

Article 16 - Transitional arrangements

Article 17 - Transposition

Article 18 - Review

Article 19 - Repeal

Article 20 - Entry into force

Article 21 - Addressees

DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Having consulted the Committee of the Regions,

Acting in accordance with the procedure laid down in Article 251 of the Treaty (3),

Whereas:

(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (4) requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.

(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

(3) Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of the Member States.

(4) Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (5)

translated the principles set out in Directive 95/46/EC into specific rules for the telecommunications sector. Directive 97/66/EC has to be adapted to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used. That Directive should therefore be repealed and replaced by this Directive.

(5) New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. The development of the information society is characterised by the introduction of new electronic communications services. Access to digital mobile networks has become available and affordable for a large public. These digital networks have large capacities and possibilities for processing personal data. The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk.

(6) The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.

(7) In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.

(8) Legal, regulatory and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interest of legal persons, in the electronic communication sector, should be harmonised in order to avoid obstacles to the internal market for electronic communication in accordance with Article 14 of the Treaty. Harmonisation should be limited to requirements necessary to guarantee that the promotion and development of new electronic communications services and networks between Member States are not hindered.

(9) The Member States, providers and users concerned, together with the competent Community bodies, should cooperate in introducing and developing the relevant technologies where this is necessary to apply the guarantees provided for by this Directive and taking particular account of the objectives of minimising the processing of personal data and of using anonymous or pseudonymous data where possible.

(10) In the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. Directive 95/46/EC applies to non-public communications services.

(11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(12) Subscribers to a publicly available electronic communications service may be natural or legal persons. By supplementing Directive 95/46/EC, this Directive is aimed at protecting the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons. This Directive does not entail an obligation for Member States to extend the application of Directive 95/46/EC to the protection of the legitimate interests of legal persons, which is ensured within the framework of the applicable Community and national legislation.

(13) The contractual relation between a subscriber and a service provider may entail a periodic or a one-off payment for the service provided or to be provided. Prepaid cards are also considered as a contract.

(14) Location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.

(15) A communication may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication. Traffic

data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission. Traffic data may, *inter alia*, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network.

(16) Information that is part of a broadcasting service provided over a public communications network is intended for a potentially unlimited audience and does not constitute a communication in the sense of this Directive. However, in cases where the individual subscriber or user receiving such information can be identified, for example with video-on-demand services, the information conveyed is covered within the meaning of a communication for the purposes of this Directive.

(17) For the purposes of this Directive, consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC. Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website.

(18) Value added services may, for example, consist of advice on least expensive tariff packages, route guidance, traffic information, weather forecasts and tourist information.

(19) The application of certain requirements relating to presentation and restriction of calling and connected line identification and to automatic call forwarding to subscriber lines connected to analogue exchanges should not be made mandatory in specific cases where such application would prove to be technically impossible or would require a disproportionate economic effort. It is important for interested parties to be informed of such cases and the Member States should therefore notify them to the Commission.

(20) Service providers should take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network. Such risks may especially occur for electronic communications services over an open network such as the Internet or analogue mobile telephony. It is particularly important for subscribers and users of such services to be fully informed by their service provider of the existing security risks which lie outside the scope of possible remedies by the service provider. Service providers who offer publicly available electronic communications services over the Internet should inform users and subscribers of measures they can take to protect the security of their

communications for instance by using specific types of software or encryption technologies. The requirement to inform subscribers of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge except for any nominal costs which the subscriber may incur while receiving or collecting the information, for instance by downloading an electronic mail message. Security is appraised in the light of Article 17 of Directive 95/46/EC.

(21) Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. National legislation in some Member States only prohibits intentional unauthorised access to communications.

(22) The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed. Where this is necessary for making more efficient the onward transmission of any publicly accessible information to other recipients of the service upon their request, this Directive should not prevent such information from being further stored, provided that this information would in any case be accessible to the public without restriction and that any data referring to the individual subscribers or users requesting such information are erased.

(23) Confidentiality of communications should also be ensured in the course of lawful business practice. Where necessary and legally authorised, communications can be recorded for the purpose of providing evidence of a commercial transaction. Directive 95/46/EC applies to such processing. Parties to the communications should be informed prior to the recording about the recording, its purpose and the duration of its storage. The recorded communication should be erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged.

(24) Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.

(25) However, such devices, for instance so-called 'cookies', can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.

(26) The data relating to subscribers processed within electronic communications networks to establish connections and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time. Any further processing of such data which the provider of the publicly available electronic communications services may want to perform, for the marketing of electronic communications services or for the provision of value added services, may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available

electronic communications services about the types of further processing it intends to perform and about the subscriber's right not to give or to withdraw his/her consent to such processing. Traffic data used for marketing communications services or for the provision of value added services should also be erased or made anonymous after the provision of the service. Service providers should always keep subscribers informed of the types of data they are processing and the purposes and duration for which this is done.

(27) The exact moment of the completion of the transmission of a communication, after which traffic data should be erased except for billing purposes, may depend on the type of electronic communications service that is provided. For instance for a voice telephony call the transmission will be completed as soon as either of the users terminates the connection. For electronic mail the transmission is completed as soon as the addressee collects the message, typically from the server of his service provider.

(28) The obligation to erase traffic data or to make such data anonymous when it is no longer needed for the purpose of the transmission of a communication does not conflict with such procedures on the Internet as the caching in the domain name system of IP addresses or the caching of IP addresses to physical address bindings or the use of log-in information to control the right of access to networks or services.

(29) The service provider may process traffic data relating to subscribers and users where necessary in individual cases in order to detect technical failure or errors in the transmission of communications. Traffic data necessary for billing purposes may also be processed by the provider in order to detect and stop fraud consisting of unpaid use of the electronic communications service.

(30) Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. Any activities related to the provision of the electronic communications service that go beyond the transmission of a communication and the billing thereof should be based on aggregated, traffic data that cannot be related to subscribers or users. Where such activities cannot be based on aggregated data, they should be considered as value added services for which the consent of the subscriber is required.

(31) Whether the consent to be obtained for the processing of personal data with a view to providing a particular value added service should be that of the user or of the subscriber, will depend on the data to be processed and on the type of service to be provided and on whether it is technically, procedurally and contractually possible to distinguish the individual using an electronic communications service from the legal or natural person having subscribed to it.

(32) Where the provider of an electronic communications service or of a value added service subcontracts the processing of personal data necessary for the provision of these services to another entity, such subcontracting and subsequent data processing should be in full compliance with the requirements regarding controllers and processors of personal data as set out in Directive 95/46/EC. Where the provision of a value added service requires that traffic or location data are forwarded from an electronic communications service provider to a provider of value added services, the subscribers or users to whom the data are related should also be fully informed of this forwarding before giving their consent for the processing of the data.

(33) The introduction of itemised bills has improved the possibilities for the subscriber to check the accuracy of the fees charged by the service provider but, at the same time, it may jeopardise the privacy of the users of publicly available electronic communications services. Therefore, in order to preserve the privacy of the user, Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services, for example calling cards and facilities for payment by credit card. To the same end, Member States may ask the operators to offer their subscribers a different type of detailed bill in which a certain number of digits of the called number have been deleted.

(34) It is necessary, as regards calling line identification, to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made and the right of the called party to reject calls from unidentified lines. There is justification for overriding the elimination of calling line identification presentation in specific cases. Certain subscribers, in particular help lines and similar organisations, have an interest in guaranteeing the anonymity of their callers. It is necessary, as regards connected line identification, to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected, in particular in the case of forwarded calls. The providers of publicly available electronic communications services should inform their subscribers of the existence of calling and connected line identification in the network and of all services which are offered on the basis of calling and connected line identification as well as the privacy options which are available. This will allow the subscribers to make an informed choice about the privacy facilities they may want to use. The privacy options which are offered on a per-line basis do not necessarily have to be available as an automatic network service but may be obtainable through a simple request to the provider of the publicly available electronic communications service.

(35) In digital mobile networks, location data giving the geographic position of the terminal equipment of the mobile user are processed to enable the transmission of communications. Such data are traffic data covered by Article 6 of this Directive. However, in addition, digital mobile networks may have the capacity to process location data which are more precise than is necessary for the transmission of communications and which are used for the provision of value added services such as services providing individualised traffic information and guidance to drivers. The processing of such data for value added services should only be allowed where subscribers have given their consent. Even in cases where subscribers have given their consent, they should have a simple means to temporarily deny the processing of location data, free of charge.

(36) Member States may restrict the users' and subscribers' rights to privacy with regard to calling line identification where this is necessary to trace nuisance calls and with regard to calling line identification and location data where this is necessary to allow emergency services to carry out their tasks as effectively as possible. For these purposes, Member States may adopt specific provisions to entitle providers of electronic communications services to provide access to calling line identification and location data without the prior consent of the users or subscribers concerned.

(37) Safeguards should be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others. Moreover, in such cases, it must be possible for subscribers to stop the forwarded calls being passed on to their terminals by simple request to the provider of the publicly available electronic communications service.

(38) Directories of subscribers to electronic communications services are widely distributed and public. The right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine whether their personal data are published in a directory and if so, which. Providers of public directories should inform the subscribers to be included in such directories of the purposes of the directory and of any particular usage which may be made of electronic versions of public directories especially through search functions embedded in the software, such as reverse search functions enabling users of the directory to discover the name and address of the subscriber on the basis of a telephone number only.

(39) The obligation to inform subscribers of the purpose(s) of public directories in which their personal data are to be included should be imposed on the party collecting the data for such inclusion. Where the data may be transmitted to one or more third parties, the subscriber should be informed of this possibility and of the recipient or the categories of possible recipients. Any transmission should be subject to the condition that the data may not be used for other purposes than those for which they

were collected. If the party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose, the renewed consent of the subscriber is to be obtained either by the initial party collecting the data or by the third party to whom the data have been transmitted.

(40) Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them. The single market requires a harmonised approach to ensure simple, Community-wide rules for businesses and users.

(41) Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details in accordance with Directive 95/46/EC. When electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage. This opportunity should continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal.

(42) Other forms of direct marketing that are more costly for the sender and impose no financial costs on subscribers and users, such as person-to-person voice telephony calls, may justify the maintenance of a system giving subscribers or users the possibility to indicate that they do not want to receive such calls. Nevertheless, in order not to decrease existing levels of privacy protection, Member States should be entitled to uphold national systems, only allowing such calls to subscribers and users who have given their prior consent.

(43) To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes.

(44) Certain electronic mail systems allow subscribers to view the sender and subject line of an electronic mail, and also to delete the message, without having to download the rest of the electronic mail's content or any attachments, thereby reducing costs which could arise from downloading

unsolicited electronic mails or attachments. These arrangements may continue to be useful in certain cases as an additional tool to the general obligations established in this Directive.

(45) This Directive is without prejudice to the arrangements which Member States make to protect the legitimate interests of legal persons with regard to unsolicited communications for direct marketing purposes. Where Member States establish an opt-out register for such communications to legal persons, mostly business users, the provisions of Article 7 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce) (6) are fully applicable.

(46) The functionalities for the provision of electronic communications services may be integrated in the network or in any part of the terminal equipment of the user, including the software. The protection of the personal data and the privacy of the user of publicly available electronic communications services should be independent of the configuration of the various components necessary to provide the service and of the distribution of the necessary functionalities between these components. Directive 95/46/EC covers any form of processing of personal data regardless of the technology used. The existence of specific rules for electronic communications services alongside general rules for other components necessary for the provision of such services may not facilitate the protection of personal data and privacy in a technologically neutral way. It may therefore be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected. The adoption of such measures in accordance with Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity (7) will ensure that the introduction of technical features of electronic communication equipment including software for data protection purposes is harmonised in order to be compatible with the implementation of the internal market.

(47) Where the rights of the users and subscribers are not respected, national legislation should provide for judicial remedies. Penalties should be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive.

(48) It is useful, in the field of application of this Directive, to draw on the experience of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data composed of

representatives of the supervisory authorities of the Member States, set up by Article 29 of Directive 95/46/EC.

(49) To facilitate compliance with the provisions of this Directive, certain specific arrangements are needed for processing of data already under way on the date that national implementing legislation pursuant to this Directive enters into force,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Scope and aim

1. This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community. 2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons. 3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

Article 2

Definitions

Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (8) shall apply.

The following definitions shall also apply:

- (a) 'user' means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;
- (b) 'traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

(c) 'location data' means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

(d) 'communication' means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

(f) 'consent' by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC;

(g) 'value added service' means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof;

(h) 'electronic mail' means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient;

(i) 'personal data breach' means ◀ a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.

Article 3

Services concerned

This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.

Article 4

Security of processing

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having

regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

1a. Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least:

- ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,
- protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and,
- ensure the implementation of a security policy with respect to the processing of personal data,

Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

3. In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority.

When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.

Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so.

The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.

4. Subject to any technical implementing measures adopted under paragraph 5, the competent national authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification is to be made. They shall also be able to audit whether providers have complied with their notification obligations under this paragraph, and shall impose appropriate sanctions in the event of a failure to do so.

Providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the competent national authorities to verify compliance with the provisions of paragraph 3. The inventory shall only include the information necessary for this purpose.

5. In order to ensure consistency in implementation of the measures referred to in paragraphs 2, 3 and 4, the Commission may, following consultation with the European Network and Information Security Agency (ENISA), the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC and the European Data Protection Supervisor, adopt technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements referred to in this Article. When adopting such measures, the Commission shall involve all relevant stakeholders particularly in order to be informed of the best available technical and economic means of implementation of this Article.

Those measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 14a(2).

Article 5

Confidentiality of the communications

1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications

services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, *inter alia*, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

Article 6

Traffic data

1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

Article 7

Itemised billing

1. Subscribers shall have the right to receive non-itemised bills.

2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative privacy enhancing methods of communications or payments are available to such users and subscribers.

Article 8

Presentation and restriction of calling and connected line identification

1. Where presentation of calling line identification is offered, the service provider must offer the calling user the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.

2. Where presentation of calling line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge for reasonable use of this function, of preventing the presentation of the calling line identification of incoming calls.

3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber

the possibility, using a simple means, of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber.

4. Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling user.

5. Paragraph 1 shall also apply with regard to calls to third countries originating in the Community. Paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries.

6. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available electronic communications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.

Article 9

Location data other than traffic data

1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

Article 10

Exceptions

Member States shall ensure that there are transparent procedures governing the way in which a provider of a public communications network and/or a publicly available electronic communications service may override:

(a) the elimination of the presentation of calling line identification, on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls. In this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public communications network and/or publicly available electronic communications service;

(b) the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organisations dealing with emergency calls and recognised as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls.

Article 11

Automatic call forwarding

Member States shall ensure that any subscriber has the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the subscriber's terminal.

Article 12

Directories of subscribers

1. Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory.

2. Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge.

3. Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers.

4. Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected.

Article 13

Unsolicited communications

1. The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent.

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the time of their collection and on the occasion of each message in case the customer has not initially refused such use.

3. Member States shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers or users concerned or in respect of subscribers or users who do not wish to receive these communications, the choice between these options to be determined by national legislation, taking into account that both options must be free of charge for the subscriber or user.

4. In any event, the practice of sending electronic mail for the purposes of direct marketing which disguise or conceal the identity of the sender on whose behalf the communication is made, which contravene Article 6 of Directive 2000/31/EC, which do not have a valid address to which the recipient may send a request that such communications cease or which encourage recipients to visit websites that contravene that Article shall be prohibited.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

6. Without prejudice to any administrative remedy for which provision may be made, *inter alia*, under Article 15a(2), Member States shall ensure that any natural or legal person adversely affected by infringements of national provisions adopted pursuant to this Article and therefore having a legitimate interest in the cessation or prohibition of such infringements, including an electronic communications service provider protecting its legitimate business interests, may bring legal proceedings in respect of such infringements. Member States may also lay down specific rules on penalties applicable to providers of electronic communications services which by their negligence contribute to infringements of national provisions adopted pursuant to this Article.

Article 14

Technical features and standardisation

1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs 2 and 3, that no mandatory requirements for specific technical features are imposed on terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.

2. Where provisions of this Directive can be implemented only by requiring specific technical features in electronic communications networks, Member States shall inform the Commission in accordance with the procedure provided for by Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services (9).

3. Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications (10).

Article 14a

Committee procedure

1. The Commission shall be assisted by the Communications Committee established by Article 22 of Directive 2002/21/EC (Framework Directive).

2. Where reference is made to this paragraph, Article 5a(1) to (4) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

3. Where reference is made to this paragraph, Article 5a(1), (2), (4) and (6) and Article 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

Article 15

Application of certain provisions of Directive 95/46/EC

1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

1a. Paragraph 1 shall not apply to data specifically required by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (11) to be retained for the purposes referred to in Article 1(1) of that Directive.

1b. Providers shall establish internal procedures for responding to requests for access to users' personal data based on national provisions adopted pursuant to paragraph 1. They shall provide the competent national authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.

2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.

3. The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.

Article 15a

Implementation and enforcement

1. Member States shall lay down the rules on penalties, including criminal sanctions where appropriate, applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive and may be applied to cover the period of any breach, even where the breach has subsequently been rectified. The Member States shall notify those provisions to the Commission by 25 May 2011, and shall notify it without delay of any subsequent amendment affecting them.

2. Without prejudice to any judicial remedy which might be available, Member States shall ensure that the competent national authority and, where relevant, other national bodies have the power to order the cessation of the infringements referred to in paragraph 1.

3. Member States shall ensure that the competent national authority and, where relevant, other national bodies have the necessary investigative powers and resources, including the power to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant to this Directive.

4. The relevant national regulatory authorities may adopt measures to ensure effective cross-border cooperation in the enforcement of the national laws adopted pursuant to this Directive and to create harmonised conditions for the provision of services involving cross-border data flows.

The national regulatory authorities shall provide the Commission, in good time before adopting any such measures, with a summary of the grounds for action, the envisaged measures and the proposed course of action. The Commission may, having examined such information and consulted ENISA and the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC, make comments or recommendations thereupon, in particular to ensure that the envisaged measures do not adversely affect the functioning of the internal market. National regulatory authorities shall take the utmost account of the Commission's comments or recommendations when deciding on the measures.

Article 16

Transitional arrangements

1. Article 12 shall not apply to editions of directories already produced or placed on the market in printed or off-line electronic form before the national provisions adopted pursuant to this Directive enter into force.
2. Where the personal data of subscribers to fixed or mobile public voice telephony services have been included in a public subscriber directory in conformity with the provisions of Directive 95/46/EC and of Article 11 of Directive 97/66/EC before the national provisions adopted in pursuance of this Directive enter into force, the personal data of such subscribers may remain included in this public directory in its printed or electronic versions, including versions with reverse search functions, unless subscribers indicate otherwise, after having received complete information about purposes and options in accordance with Article 12 of this Directive.

Article 17

Transposition

1. Before 31 October 2003 Member States shall bring into force the provisions necessary to comply with this Directive. They shall forthwith inform the Commission thereof.

When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field governed by this Directive and of any subsequent amendments to those provisions.

Article 18

Review

The Commission shall submit to the European Parliament and the Council, not later than three years after the date referred to in Article 17(1), a report on the application of this Directive and its impact on economic operators and consumers, in particular as regards the provisions on unsolicited communications, taking into account the international environment. For this purpose, the Commission may request information from the Member States, which shall be supplied without undue delay. Where appropriate, the Commission shall submit proposals to amend this Directive,

taking account of the results of that report, any changes in the sector and any other proposal it may deem necessary in order to improve the effectiveness of this Directive.

Article 19

Repeal

Directive 97/66/EC is hereby repealed with effect from the date referred to in Article 17(1).

References made to the repealed Directive shall be construed as being made to this Directive.

Article 20

Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

Article 21

Addressees

This Directive is addressed to the Member States.

(1) OJ C 365 E, 19.12.2000, p. 223.

(2) OJ C 123, 25.4.2001, p. 53.

(3) Opinion of the European Parliament of 13 November 2001 (not yet published in the Official Journal), Council Common Position of 28 January 2002 (OJ C 113 E, 14.5.2002, p. 39) and Decision of the European Parliament of 30 May 2002 (not yet published in the Official Journal). Council Decision of 25 June 2002.

(4) OJ L 281, 23.11.1995, p. 31.

(5) OJ L 24, 30.1.1998, p. 1.

(6) OJ L 178, 17.7.2000, p. 1.

(7) OJ L 91, 7.4.1999, p. 10.

(8) OJ L 108, 24.4.2002, p. 33.

(9) OJ L 204, 21.7.1998, p. 37. Directive as amended by Directive 98/48/EC (OJ L 217, 5.8.1998, p. 18).

(10) OJ L 36, 7.2.1987, p. 31. Decision as last amended by the 1994 Act of Accession.

(11) OJ L 105, 13.4.2006, p. 54.

Avrupa Birliđi - Polis ve Yargı Kişisel Veriler Direktifi (LED Directive)

2016/680 sayılı Kişisel Verilerin Ceza Adaleti ve Polis İşbirliđi Alanında Kullanılmasına Yönelik Gerçek Kişilere Ait Kişisel Verilerin Yetkili Otoriteler Tarafından Suçların Önlenmesi, Soruşturulması ve Tespit Edilmesi veya Cezaların İnfazı Amacıyla İşlenmesi ve Bu Nevi Kişisel Verilerin Serbest Dolaşımı Hakkında Direktif

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Official Journal of the European Union L 119/89, 4.5.2016

LED DIRECTIVE

CHAPTER I - General provisions

Article 1 - Subject-matter and objectives

Article 2 - Scope

Article 3 - Definitions

CHAPTER II - Principles

Article 4 - Principles relating to processing of personal data

Article 5 - Time-limits for storage and review

Article 6 - Distinction between different categories of data subject

Article 7 - Distinction between personal data and verification of quality of personal data

Article 8 - Lawfulness of processing

Article 9 - Specific processing conditions

Article 10 - Processing of special categories of personal data

Article 11 - Automated individual decision-making

CHAPTER III - Rights of the data subject

Article 12 - Communication and modalities for exercising the rights of the data subject

Article 13 - Information to be made available or given to the data subject

Article 14 - Right of access by the data subject

Article 15 - Limitations to the right of access

Article 16 - Right to rectification or erasure of personal data and restriction of processing

Article 17 - Exercise of rights by the data subject and verification by the supervisory authority

Article 18 - Rights of the data subject in criminal investigations and proceedings

CHAPTER IV - Controller and processor

Section 1 - General obligations

Article 19 - Obligations of the controller

Article 20 - Data protection by design and by default

Article 21 - Joint controllers

Article 22 - Processor

Article 23 - Processing under the authority of the controller or processor

Article 24 - Records of processing activities

Article 25 - Logging

Article 26 - Cooperation with the supervisory authority

Article 27 - Data protection impact assessment

Article 28 - Prior consultation of the supervisory authority

Section 2 - Security of personal data

Article 29 - Security of processing

Article 30 - Notification of a personal data breach to the supervisory authority

Article 31 - Communication of a personal data breach to the data subject

Section 3 - Data protection officer

Article 32 - Designation of the data protection officer

Article 33 - Position of the data protection officer

Article 34 - Tasks of the data protection officer

CHAPTER V - Transfers of personal data to third countries or international organisations

Article 35 - General principles for transfers of personal data

Article 36 - Transfers on the basis of an adequacy decision

Article 37 - Transfers subject to appropriate safeguards

Article 38 - Derogations for specific situations

Article 39 - Transfers of personal data to recipients established in third countries

Article 40 - International cooperation for the protection of personal data

CHAPTER VI - Independent supervisory authorities

Section 1 - Independent status

Article 41 - Supervisory authority

Article 42 - Independence

Article 43 - General conditions for the members of the supervisory authority

Article 44 - Rules on the establishment of the supervisory authority

Section 2 - Competence, tasks and powers

Article 45 - Competence

Article 46 - Tasks

Article 47 - Powers

Article 48 - Reporting of infringements

Article 49 - Activity reports

CHAPTER VII - Cooperation

Article 50 - Mutual assistance

Article 51 - Tasks of the Board

CHAPTER VIII - Remedies, liability and penalties

Article 52 - Right to lodge a complaint with a supervisory authority

Article 53 - Right to an effective judicial remedy against a supervisory authority

Article 54 - Right to an effective judicial remedy against a controller or processor

Article 55 - Representation of data subjects

Article 56 - Right to compensation

Article 57 - Penalties

CHAPTER IX - Implementing acts

Article 58 - Committee procedure

CHAPTER X - Final provisions

Article 59 - Repeal of Framework Decision 2008/977/JHA

Article 60 - Union legal acts already in force

Article 61 - Relationship with previously concluded international agreements in the field of judicial cooperation in criminal matters and police cooperation

Article 62 - Commission reports

Article 63 - Transposition

Article 64 - Entry into force

Article 65 - Addressees

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the Committee of the Regions (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union ('the Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Directive is intended to contribute to the accomplishment of an area of freedom, security and justice.

(3) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows personal data to be processed on an unprecedented scale in order to pursue activities such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

(4) The free flow of personal data between competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security within the Union and the transfer of such personal data to third countries and international organisations, should be facilitated while ensuring a high level of protection of personal data. Those developments require the building of a strong and more coherent framework for the protection of personal data in the Union, backed by strong enforcement.

(5) Directive 95/46/EC of the European Parliament and of the Council (3) applies to all processing of personal data in Member States in both the public and the private sectors. However, it does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as activities in the areas of judicial cooperation in criminal matters and police cooperation.

(6) Council Framework Decision 2008/977/JHA (4) applies in the areas of judicial cooperation in criminal matters and police cooperation. The scope of application of that Framework Decision is limited to the processing of personal data transmitted or made available between Member States.

(7) Ensuring a consistent and high level of protection of the personal data of natural persons and facilitating the exchange of personal data between competent authorities of Member States is crucial in order to ensure effective judicial cooperation in criminal matters and police cooperation. To that

end, the level of protection of the rights and freedoms of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, should be equivalent in all Member States. Effective protection of personal data throughout the Union requires the strengthening of the rights of data subjects and of the obligations of those who process personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States.

(8) Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data.

(9) On that basis, Regulation (EU) 2016/679 of the European Parliament and of the Council (5) lays down general rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the Union.

(10) In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU may prove necessary because of the specific nature of those fields.

(11) It is therefore appropriate for those fields to be addressed by a directive that lays down the specific rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, respecting the specific nature of those activities. Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive. Where such a body or entity processes personal data for purposes other than for the purposes of this Directive, Regulation (EU) 2016/679 applies. Regulation (EU) 2016/679 therefore applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject. For example, for the purposes of

investigation detection or prosecution of criminal offences financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law. A body or entity which processes personal data on behalf of such authorities within the scope of this Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to this Directive, while the application of Regulation (EU) 2016/679 remains unaffected for the processing of personal data by the processor outside the scope of this Directive.

(12) The activities carried out by the police or other law-enforcement authorities are focused mainly on the prevention, investigation, detection or prosecution of criminal offences, including police activities without prior knowledge if an incident is a criminal offence or not. Such activities can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. They also include maintaining law and order as a task conferred on the police or other law-enforcement authorities where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence. Member States may entrust competent authorities with other tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of Regulation (EU) 2016/679.

(13) A criminal offence within the meaning of this Directive should be an autonomous concept of Union law as interpreted by the Court of Justice of the European Union (the 'Court of Justice').

(14) Since this Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU) should not be considered to be activities falling within the scope of this Directive.

(15) In order to ensure the same level of protection for natural persons through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between competent authorities, this Directive should provide for harmonised rules for the protection and the free movement of personal data processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the

safeguarding against and the prevention of threats to public security. The approximation of Member States' laws should not result in any lessening of the personal data protection they afford but should, on the contrary, seek to ensure a high level of protection within the Union. Member States should not be precluded from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities.

(16) This Directive is without prejudice to the principle of public access to official documents. Under Regulation (EU) 2016/679 personal data in official documents held by a public authority or a public or private body for the performance of a task carried out in the public interest may be disclosed by that authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data.

(17) The protection afforded by this Directive should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.

(18) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Directive.

(19) Regulation (EC) No 45/2001 of the European Parliament and of the Council (6) applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in Regulation (EU) 2016/679.

(20) This Directive does not preclude Member States from specifying processing operations and processing procedures in national rules on criminal procedures in relation to the processing of personal data by courts and other judicial authorities, in particular as regards personal data contained in a judicial decision or in records in relation to criminal proceedings.

(21) The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by

another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is no longer identifiable.

(22) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data protection rules according to the purposes of the processing.

(23) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or health of that natural person and which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained. Considering the complexity and sensitivity of genetic information, there is a great risk of misuse and re-use for various purposes by the controller. Any discrimination based on genetic features should in principle be prohibited.

(24) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council (7) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk,

medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

(25) All Member States are affiliated to the International Criminal Police Organisation (Interpol). To fulfil its mission, Interpol receives, stores and circulates personal data to assist competent authorities in preventing and combating international crime. It is therefore appropriate to strengthen cooperation between the Union and Interpol by promoting an efficient exchange of personal data whilst ensuring respect for fundamental rights and freedoms regarding the automatic processing of personal data. Where personal data are transferred from the Union to Interpol, and to countries which have delegated members to Interpol, this Directive, in particular the provisions on international transfers, should apply. This Directive should be without prejudice to the specific rules laid down in Council Common Position 2005/69/JHA (8) and Council Decision 2007/533/JHA (9).

(26) Any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law. This does not in itself prevent the law-enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned. The data protection principle of fair processing is a distinct notion from the right to a fair trial as defined in Article 47 of the Charter and in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing. In particular, the specific purposes for which the personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate and relevant for the purposes for which they are processed. It should, in particular, be ensured that the personal data collected are not excessive and not kept longer than is necessary for the purpose for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for

erasure or for a periodic review. Member States should lay down appropriate safeguards for personal data stored for longer periods for archiving in the public interest, scientific, statistical or historical use.

(27) For the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected.

(28) In order to maintain security in relation to processing and to prevent processing in infringement of this Directive, personal data should be processed in a manner that ensures an appropriate level of security and confidentiality, including by preventing unauthorised access to or use of personal data and the equipment used for the processing, and that takes into account available state of the art and technology, the costs of implementation in relation to the risks and the nature of the personal data to be protected.

(29) Personal data should be collected for specified, explicit and legitimate purposes within the scope of this Directive and should not be processed for purposes incompatible with the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. If personal data are processed by the same or another controller for a purpose within the scope of this Directive other than that for which it has been collected, such processing should be permitted under the condition that such processing is authorised in accordance with applicable legal provisions and is necessary for and proportionate to that other purpose.

(30) The principle of accuracy of data should be applied while taking account of the nature and purpose of the processing concerned. In particular in judicial proceedings, statements containing personal data are based on the subjective perception of natural persons and are not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.

(31) It is inherent to the processing of personal data in the areas of judicial cooperation in criminal matters and police cooperation that personal data relating to different categories of data subjects are processed. Therefore, a clear distinction should, where applicable and as far as possible, be made between personal data of different categories of data subjects such as: suspects; persons convicted of a criminal offence; victims and other parties, such as witnesses; persons possessing relevant information or contacts; and associates of suspects and convicted criminals. This should not prevent

the application of the right of presumption of innocence as guaranteed by the Charter and by the ECHR, as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively.

(32) The competent authorities should ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. In order to ensure the protection of natural persons, the accuracy, completeness or the extent to which the personal data are up to date and the reliability of the personal data transmitted or made available, the competent authorities should, as far as possible, add necessary information in all transmissions of personal data.

(33) Where this Directive refers to Member State law, a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a Member State law, legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it, as required by the case-law of the Court of Justice and the European Court of Human Rights. Member State law regulating the processing of personal data within the scope of this Directive should specify at least the objectives, the personal data to be processed, the purposes of the processing and procedures for preserving the integrity and confidentiality of personal data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.

(34) The processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, should cover any operation or set of operations which are performed upon personal data or sets of personal data for those purposes, whether by automated means or otherwise, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, restriction of processing, erasure or destruction. In particular, the rules of this Directive should apply to the transmission of personal data for the purposes of this Directive to a recipient not subject to this Directive. Such a recipient should encompass a natural or legal person, public authority, agency or any other body to which personal data are lawfully disclosed by the competent authority. Where personal data were initially collected by a competent authority for one of the purposes of this Directive, Regulation (EU) 2016/679 should apply to the processing of those data for purposes other than the purposes of this Directive where such processing is authorised by Union or Member State law. In particular, the rules of Regulation (EU) 2016/679 should apply to the transmission of personal

data for purposes outside the scope of this Directive. For the processing of personal data by a recipient that is not a competent authority or that is not acting as such within the meaning of this Directive and to which personal data are lawfully disclosed by a competent authority, Regulation (EU) 2016/679 should apply. While implementing this Directive, Member States should also be able to further specify the application of the rules of Regulation (EU) 2016/679, subject to the conditions set out therein.

(35) In order to be lawful, the processing of personal data under this Directive should be necessary for the performance of a task carried out in the public interest by a competent authority based on Union or Member State law for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Those activities should cover the protection of vital interests of the data subject. The performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require or order natural persons to comply with requests made. In such a case, the consent of the data subject, as defined in Regulation (EU) 2016/679, should not provide a legal ground for processing personal data by competent authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes. This should not preclude Member States from providing, by law, that the data subject may agree to the processing of his or her personal data for the purposes of this Directive, such as DNA tests in criminal investigations or the monitoring of his or her location with electronic tags for the execution of criminal penalties.

(36) Member States should provide that where Union or Member State law applicable to the transmitting competent authority provides for specific conditions applicable in specific circumstances to the processing of personal data, such as the use of handling codes, the transmitting competent authority should inform the recipient of such personal data of those conditions and the requirement to respect them. Such conditions could, for example, include a prohibition against transmitting the personal data further to others, or using them for purposes other than those for which they were transmitted to the recipient, or informing the data subject in the case of a limitation of the right of information without the prior approval of the transmitting competent authority. Those obligations should also apply to transfers by the transmitting competent authority to recipients in third countries or international organisations. Member States should ensure that the transmitting competent authority does not apply such conditions to recipients in other Member States or to agencies, offices

and bodies established pursuant to Chapters 4 and 5 of Title V of the TFEU other than those applicable to similar data transmissions within the Member State of that competent authority.

(37) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Directive does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. Such personal data should not be processed, unless processing is subject to appropriate safeguards for the rights and freedoms of the data subject laid down by law and is allowed in cases authorised by law; where not already authorised by such a law, the processing is necessary to protect the vital interests of the data subject or of another person; or the processing relates to data which are manifestly made public by the data subject. Appropriate safeguards for the rights and freedoms of the data subject could include the possibility to collect those data only in connection with other data on the natural person concerned, the possibility to secure the data collected adequately, stricter rules on the access of staff of the competent authority to the data and the prohibition of transmission of those data. The processing of such data should also be allowed by law where the data subject has explicitly agreed to the processing that is particularly intrusive to him or her. However, the consent of the data subject should not provide in itself a legal ground for processing such sensitive personal data by competent authorities.

(38) The data subject should have the right not to be subject to a decision evaluating personal aspects relating to him or her which is based solely on automated processing and which produces adverse legal effects concerning, or significantly affects, him or her. In any case, such processing should be subject to suitable safeguards, including the provision of specific information to the data subject and the right to obtain human intervention, in particular to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision. Profiling that results in discrimination against natural persons on the basis of personal data which are by their nature particularly sensitive in relation to fundamental rights and freedoms should be prohibited under the conditions laid down in Articles 21 and 52 of the Charter.

(39) In order to enable him or her to exercise his or her rights, any information to the data subject should be easily accessible, including on the website of the controller, and easy to understand, using clear and plain language. Such information should be adapted to the needs of vulnerable persons such as children.

(40) Modalities should be provided for facilitating the exercise of the data subject's rights under the provisions adopted pursuant to this Directive, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and restriction of processing. The controller should be obliged to respond to requests of the data subject without undue delay, unless the controller applies limitations to data subject rights in accordance with this Directive. Moreover, if requests are manifestly unfounded or excessive, such as where the data subject unreasonably and repetitiously requests information or where the data subject abuses his or her right to receive information, for example, by providing false or misleading information when making the request, the controller should be able to charge a reasonable fee or refuse to act on the request.

(41) Where the controller requests the provision of additional information necessary to confirm the identity of the data subject, that information should be processed only for that specific purpose and should not be stored for longer than needed for that purpose.

(42) At least the following information should be made available to the data subject: the identity of the controller, the existence of the processing operation, the purposes of the processing, the right to lodge a complaint and the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing. This could take place on the website of the competent authority. In addition, in specific cases and in order to enable the exercise of his or her rights, the data subject should be informed of the legal basis for the processing and of how long the data will be stored, in so far as such further information is necessary, taking into account the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

(43) A natural person should have the right of access to data which has been collected concerning him or her, and to exercise this right easily and at reasonable intervals, in order to be aware of and verify the lawfulness of the processing. Every data subject should therefore have the right to know, and obtain communications about, the purposes for which the data are processed, the period during which the data are processed and the recipients of the data, including those in third countries. Where such communications include information as to the origin of the personal data, the information should not reveal the identity of natural persons, in particular confidential sources. For that right to be complied with, it is sufficient that the data subject be in possession of a full summary of those data in an intelligible form, that is to say a form which allows that data subject to become aware of those data and to verify that they are accurate and processed in accordance with this Directive, so that it is

possible for him or her to exercise the rights conferred on him or her by this Directive. Such a summary could be provided in the form of a copy of the personal data undergoing processing.

(44) Member States should be able to adopt legislative measures delaying, restricting or omitting the information to data subjects or restricting, wholly or partly, the access to their personal data to the extent that and as long as such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, to protect public security or national security, or to protect the rights and freedoms of others. The controller should assess, by way of a concrete and individual examination of each case, whether the right of access should be partially or completely restricted.

(45) Any refusal or restriction of access should in principle be set out in writing to the data subject and include the factual or legal reasons on which the decision is based.

(46) Any restriction of the rights of the data subject must comply with the Charter and with the ECHR, as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively, and in particular respect the essence of those rights and freedoms.

(47) A natural person should have the right to have inaccurate personal data concerning him or her rectified, in particular where it relates to facts, and the right to erasure where the processing of such data infringes this Directive. However, the right to rectification should not affect, for example, the content of a witness testimony. A natural person should also have the right to restriction of processing where he or she contests the accuracy of personal data and its accuracy or inaccuracy cannot be ascertained or where the personal data have to be maintained for purpose of evidence. In particular, instead of erasing personal data, processing should be restricted if in a specific case there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. In such a case, restricted data should be processed only for the purpose which prevented their erasure. Methods to restrict the processing of personal data could include, inter alia, moving the selected data to another processing system, for example for archiving purposes, or making the selected data unavailable. In automated filing systems the restriction of processing should in principle be ensured by technical means. The fact that the processing of personal data is restricted should be indicated in the system in such a manner that it is clear that the processing of the personal data is restricted. Such rectification or erasure of personal data or restriction of processing should be communicated to recipients to whom the data have been disclosed and to the competent authorities from which the

inaccurate data originated. The controllers should also abstain from further dissemination of such data.

(48) Where the controller denies a data subject his or her right to information, access to or rectification or erasure of personal data or restriction of processing, the data subject should have the right to request that the national supervisory authority verify the lawfulness of the processing. The data subject should be informed of that right. Where the supervisory authority acts on behalf of the data subject, the data subject should be informed by the supervisory authority at least that all necessary verifications or reviews by the supervisory authority have taken place. The supervisory authority should also inform the data subject of the right to seek a judicial remedy.

(49) Where the personal data are processed in the course of a criminal investigation and court proceedings in criminal matters, Member States should be able to provide that the exercise the right to information, access to and rectification or erasure of personal data and restriction of processing is carried out in accordance with national rules on judicial proceedings.

(50) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and should be able to demonstrate that processing activities are in compliance with this Directive. Such measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons. The measures taken by the controller should include drawing up and implementing specific safeguards in respect of the treatment of personal data of vulnerable natural persons, such as children.

(51) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy, unauthorised reversal of pseudonymisation or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs or trade union membership; where genetic data or biometric data are processed in order to uniquely identify a person or where data concerning health or data concerning sex life and sexual orientation or criminal convictions and offences or related security measures are processed; where personal aspects are evaluated, in particular analysing and

predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(52) The likelihood and severity of the risk should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, through which it is established whether data-processing operations involve a high risk. A high risk is a particular risk of prejudice to the rights and freedoms of data subjects.

(53) The protection of the rights and freedoms of natural persons with regard to the processing of personal data requires that appropriate technical and organisational measures are taken, to ensure that the requirements of this Directive are met. The implementation of such measures should not depend solely on economic considerations. In order to be able to demonstrate compliance with this Directive, the controller should adopt internal policies and implement measures which adhere in particular to the principles of data protection by design and data protection by default. Where the controller has carried out a data protection impact assessment pursuant to this Directive, the results should be taken into account when developing those measures and procedures. The measures could consist, inter alia, of the use of pseudonymisation, as early as possible. The use of pseudonymisation for the purposes of this Directive can serve as a tool that could facilitate, in particular, the free flow of personal data within the area of freedom, security and justice.

(54) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities set out in this Directive, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(55) The carrying-out of processing by a processor should be governed by a legal act including a contract binding the processor to the controller and stipulating, in particular, that the processor should act only on instructions from the controller. The processor should take into account the principle of data protection by design and by default.

(56) In order to demonstrate compliance with this Directive, the controller or processor should maintain records regarding all categories of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records available to it on request, so that they might serve for monitoring those processing

operations. The controller or the processor processing personal data in non-automated processing systems should have in place effective methods of demonstrating the lawfulness of the processing, of enabling self-monitoring and of ensuring data integrity and data security, such as logs or other forms of records.

(57) Logs should be kept at least for operations in automated processing systems such as collection, alteration, consultation, disclosure including transfers, combination or erasure. The identification of the person who consulted or disclosed personal data should be logged and from that identification it should be possible to establish the justification for the processing operations. The logs should solely be used for the verification of the lawfulness of the processing, self-monitoring, for ensuring data integrity and data security and criminal proceedings. Self-monitoring also includes internal disciplinary proceedings of competent authorities.

(58) A data protection impact assessment should be carried out by the controller where the processing operations are likely to result in a high risk to the rights and freedoms of data subjects by virtue of their nature, scope or purposes, which should include, in particular, the measures, safeguards and mechanisms envisaged to ensure the protection of personal data and to demonstrate compliance with this Directive. Impact assessments should cover relevant systems and processes of processing operations, but not individual cases.

(59) In order to ensure effective protection of the rights and freedoms of data subjects, the controller or processor should consult the supervisory authority, in certain cases, prior to the processing.

(60) In order to maintain security and to prevent processing that infringes this Directive, the controller or processor should evaluate the risks inherent in the processing and should implement measures to mitigate those risks, such as encryption. Such measures should ensure an appropriate level of security, including confidentiality and take into account the state of the art, the costs of implementation in relation to the risk and the nature of the personal data to be protected. In assessing data security risks, consideration should be given to the risks that are presented by data processing, such as the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed, which may, in particular, lead to physical, material or non-material damage. The controller and processor should ensure that the processing of personal data is not carried out by unauthorised persons.

(61) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss,

unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(62) Natural persons should be informed without undue delay where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, in order to allow them to take the necessary precautions. The communication should describe the nature of the personal data breach and include recommendations for the natural person concerned to mitigate potential adverse effects. Communication to data subjects should be made as soon as reasonably feasible, in close cooperation with the supervisory authority, and respecting guidance provided by it or other relevant authorities. For example, the need to mitigate an immediate risk of damage would call for a prompt communication to data subjects, whereas the need to implement appropriate measures against continuing or similar data breaches may justify more time for the communication. Where avoiding obstruction of official or legal inquiries, investigations or procedures, avoiding prejudice to the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, protecting public security, protecting national security or protecting the rights and freedoms of others cannot be achieved by delaying or restricting the communication of a personal data breach to the natural person concerned, such communication could, in exceptional circumstances, be omitted.

(63) The controller should designate a person who would assist it in monitoring internal compliance with the provisions adopted pursuant to this Directive, except where a Member State decides to exempt courts and other independent judicial authorities when acting in their judicial capacity. That person could be a member of the existing staff of the controller who received special training in data protection law and practice in order to acquire expert knowledge in that field. The necessary level of expert knowledge should be determined, in particular, according to the data processing carried out and the protection required for the personal data processed by the controller. His or her task could be carried out on a part-time or full-time basis. A data protection officer may be appointed jointly by

several controllers, taking into account their organisational structure and size, for example in the case of shared resources in central units. That person can also be appointed to different positions within the structure of the relevant controllers. That person should help the controller and the employees processing personal data by informing and advising them on compliance with their relevant data protection obligations. Such data protection officers should be in a position to perform their duties and tasks in an independent manner in accordance with Member State law.

(64) Member States should ensure that a transfer to a third country or to an international organisation takes place only if necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, and that the controller in the third country or international organisation is an authority competent within the meaning of this Directive. A transfer should be carried out only by competent authorities acting as controllers, except where processors are explicitly instructed to transfer on behalf of controllers. Such a transfer may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level of protection, where appropriate safeguards have been provided, or where derogations for specific situations apply. Where personal data are transferred from the Union to controllers, to processors or to other recipients in third countries or international organisations, the level of protection of natural persons provided for in the Union by this Directive should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers or processors in the same or in another third country or international organisation.

(65) Where personal data are transferred from a Member State to third countries or international organisations, such a transfer should, in principle, take place only after the Member State from which the data were obtained has given its authorisation to the transfer. The interests of efficient law-enforcement cooperation require that where the nature of a threat to the public security of a Member State or a third country or to the essential interests of a Member State is so immediate as to render it impossible to obtain prior authorisation in good time, the competent authority should be able to transfer the relevant personal data to the third country or international organisation concerned without such a prior authorisation. Member States should provide that any specific conditions concerning the transfer should be communicated to third countries or international organisations. Onward transfers of personal data should be subject to prior authorisation by the competent authority that carried out the original transfer. When deciding on a request for the authorisation of an onward transfer, the competent authority that carried out the original transfer should take due account of all

relevant factors, including the seriousness of the criminal offence, the specific conditions subject to which, and the purpose for which, the data was originally transferred, the nature and conditions of the execution of the criminal penalty, and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred. The competent authority that carried out the original transfer should also be able to subject the onward transfer to specific conditions. Such specific conditions can be described, for example, in handling codes.

(66) The Commission should be able to decide with effect for the entire Union that certain third countries, a territory or one or more specified sectors within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such a level of protection. In such cases, transfers of personal data to those countries should be able to take place without the need to obtain any specific authorisation, except where another Member State from which the data were obtained has to give its authorisation to the transfer.

(67) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security, as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

(68) Apart from the international commitments the third country or international organisation has entered into, the Commission should also take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems, in particular in relation to the protection of personal data, as well as the implementation of such obligations. In

particular the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult with the European Data Protection Board established by Regulation (EU) 2016/679 (the 'Board') when assessing the level of protection in third countries or international organisations. The Commission should also take into account any relevant Commission adequacy decision adopted in accordance with Article 45 of Regulation (EU) 2016/679.

(69) The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or a specified sector within a third country, or an international organisation. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be undertaken in consultation with the third country or international organisation in question and should take into account all relevant developments in the third country or international organisation.

(70) The Commission should also be able to recognise that a third country, a territory or a specified sector within a third country, or an international organisation, no longer ensures an adequate level of data protection. Consequently, the transfer of personal data to that third country or international organisation should be prohibited unless the requirements in this Directive relating to transfers subject to appropriate safeguards and derogations for specific situations are fulfilled. Provision should be made for procedures for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(71) Transfers not based on such an adequacy decision should be allowed only where appropriate safeguards have been provided in a legally binding instrument which ensures the protection of personal data or where the controller has assessed all the circumstances surrounding the data transfer and, on the basis of that assessment, considers that appropriate safeguards with regard to the protection of personal data exist. Such legally binding instruments could, for example, be legally binding bilateral agreements which have been concluded by the Member States and implemented in their legal order and which could be enforced by their data subjects, ensuring compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. The controller should be able to take into account cooperation agreements concluded between Europol or Eurojust and third countries which allow for the exchange

of personal data when carrying out the assessment of all the circumstances surrounding the data transfer. The controller should be able to also take into account the fact that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition, the controller should take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment. While those conditions could be considered to be appropriate safeguards allowing the transfer of data, the controller should be able to require additional safeguards.

(72) Where no adequacy decision or appropriate safeguards exist, a transfer or a category of transfers could take place only in specific situations, if necessary to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; for the prevention of an immediate and serious threat to the public security of a Member State or a third country; in an individual case for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or in an individual case for the establishment, exercise or defence of legal claims. Those derogations should be interpreted restrictively and should not allow frequent, massive and structural transfers of personal data, or large-scale transfers of data, but should be limited to data strictly necessary. Such transfers should be documented and should be made available to the supervisory authority on request in order to monitor the lawfulness of the transfer.

(73) Competent authorities of Member States apply bilateral or multilateral international agreements in force, concluded with third countries in the field of judicial cooperation in criminal matters and police cooperation, for the exchange of relevant information to allow them to perform their legally assigned tasks. In principle, this takes place through, or at least with, the cooperation of the authorities competent in the third countries concerned for the purposes of this Directive, sometimes even in the absence of a bilateral or multilateral international agreement. However, in specific individual cases, the regular procedures requiring contacting such an authority in the third country may be ineffective or inappropriate, in particular because the transfer could not be carried out in a timely manner, or because that authority in the third country does not respect the rule of law or international human rights norms and standards, so that competent authorities of Member States could decide to transfer personal data directly to recipients established in those third countries. This may be the case where there is an urgent need to transfer personal data to save the life of a person who is in danger of

becoming a victim of a criminal offence or in the interest of preventing an imminent perpetration of a crime, including terrorism. Even if such a transfer between competent authorities and recipients established in third countries should take place only in specific individual cases, this Directive should provide for conditions to regulate such cases. Those provisions should not be considered to be derogations from any existing bilateral or multilateral international agreements in the field of judicial cooperation in criminal matters and police cooperation. Those rules should apply in addition to the other rules of this Directive, in particular those on the lawfulness of processing and Chapter V.

(74) Where personal data move across borders it may put at increased risk the ability of natural persons to exercise data protection rights to protect themselves from the unlawful use or disclosure of those data. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers and inconsistent legal regimes. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information with their foreign counterparts.

(75) The establishment in Member States of supervisory authorities that are able to exercise their functions with complete independence is an essential component of the protection of natural persons with regard to the processing of their personal data. The supervisory authorities should monitor the application of the provisions adopted pursuant to this Directive and should contribute to their consistent application throughout the Union in order to protect natural persons with regard to the processing of their personal data. To that end, the supervisory authorities should cooperate with each other and with the Commission.

(76) Member States may entrust a supervisory authority already established under Regulation (EU) 2016/679 with the responsibility for the tasks to be performed by the national supervisory authorities to be established under this Directive.

(77) Member States should be allowed to establish more than one supervisory authority to reflect their constitutional, organisational and administrative structure. Each supervisory authority should be provided with the financial and human resources, premises and infrastructure, which are necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.

(78) Supervisory authorities should be subject to independent control or monitoring mechanisms regarding their financial expenditure, provided that such financial control does not affect their independence.

(79) The general conditions for the member or members of the supervisory authority should be laid down by Member State law and should in particular provide that those members should be either appointed by the parliament or the government or the head of State of the Member State based on a proposal from the government or a member of the government, or the parliament or its chamber, or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, should refrain from any action incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. In order to ensure the independence of the supervisory authority, the staff should be chosen by the supervisory authority which may include an intervention by an independent body entrusted by Member State law.

(80) While this Directive applies also to the activities of national courts and other judicial authorities, the competence of the supervisory authorities should not cover the processing of personal data where courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. That exemption should be limited to judicial activities in court cases and not apply to other activities where judges might be involved in accordance with Member State law. Member States should also be able to provide that the competence of the supervisory authority does not cover the processing of personal data of other independent judicial authorities when acting in their judicial capacity, for example public prosecutor's office. In any event, the compliance with the rules of this Directive by the courts and other independent judicial authorities is always subject to independent supervision in accordance with Article 8(3) of the Charter.

(81) Each supervisory authority should handle complaints lodged by any data subject and should investigate the matter or transmit it to the competent supervisory authority. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be provided to the data subject.

(82) In order to ensure effective, reliable and consistent monitoring of compliance with and enforcement of this Directive throughout the Union pursuant to the TFEU as interpreted by the Court of Justice, the supervisory authorities should have in each Member State the same tasks and effective powers, including investigative, corrective, and advisory powers which constitute necessary means to perform their tasks. However, their powers should not interfere with specific rules for criminal proceedings, including investigation and prosecution of criminal offences, or the independence of the judiciary. Without prejudice to the powers of prosecutorial authorities under Member State law, supervisory authorities should also have the power to bring infringements of this Directive to the attention of the judicial authorities or to engage in legal proceedings. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards laid down by Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Directive, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure that would adversely affect the person concerned is taken, and avoiding superfluous costs and excessive inconvenience to the person concerned. Investigative powers as regards access to premises should be exercised in accordance with specific requirements in Member State law, such as the requirement to obtain a prior judicial authorisation. The adoption of a legally binding decision should be subject to judicial review in the Member State of the supervisory authority that adopted the decision.

(83) The supervisory authorities should assist one another in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of the provisions adopted pursuant to this Directive.

(84) The Board should contribute to the consistent application of this Directive throughout the Union, including advising the Commission and promoting the cooperation of the supervisory authorities throughout the Union.

(85) Every data subject should have the right to lodge a complaint with a single supervisory authority and to an effective judicial remedy in accordance with Article 47 of the Charter where the data subject considers that his or her rights under provisions adopted pursuant to this Directive are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The competent supervisory authority should inform the data

subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be provided to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(86) Each natural or legal person should have the right to an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, that right does not encompass other measures of supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with Member State law. Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it.

(87) Where a data subject considers that his or her rights under this Directive are infringed, he or she should have the right to mandate a body which aims to protect the rights and interests of data subjects in relation to the protection of their personal data and is constituted according to Member State law to lodge a complaint on his or her behalf with a supervisory authority and to exercise the right to a judicial remedy. The right of representation of data subjects should be without prejudice to Member State procedural law which may require mandatory representation of data subjects by a lawyer, as defined in Council Directive 77/249/EEC (10), before national courts.

(88) Any damage which a person may suffer as a result of processing that infringes the provisions adopted pursuant to this Directive should be compensated by the controller or any other authority competent under Member State law. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Directive. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. When reference is made to processing that is unlawful or that infringes the provisions adopted pursuant to this Directive it also covers processing that infringes implementing acts adopted pursuant to this Directive. Data subjects should receive full and effective compensation for the damage that they have suffered.

(89) Penalties should be imposed on any natural or legal person, whether governed by private or public law, who infringes this Directive. Member States should ensure that the penalties are effective, proportionate and dissuasive and should take all measures to implement the penalties.

(90) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission with regard to the adequate level of protection afforded by a third country, a territory or a specified sector within a third country, or an international organisation and the format and procedures for mutual assistance and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council (11).

(91) The examination procedure should be used for the adoption of implementing acts on the adequate level of protection afforded by a third country, a territory or a specified sector within a third country, or an international organisation and on the format and procedures for mutual assistance and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, given that those acts are of a general scope.

(92) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country, a territory or a specified sector within a third country, or an international organisation which no longer ensure an adequate level of protection, imperative grounds of urgency so require.

(93) Since the objectives of this Directive, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free exchange of personal data by competent authorities within the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the TEU. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives

(94) Specific provisions of acts of the Union adopted in the field of judicial cooperation in criminal matters and police cooperation which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, should remain unaffected, such as, for example, the specific provisions concerning the protection of personal

data applied pursuant to Council Decision 2008/615/JHA (12), or Article 23 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (13). Since Article 8 of the Charter and Article 16 TFEU require that the fundamental right to the protection of personal data be ensured in a consistent manner throughout the Union, the Commission should evaluate the situation with regard to the relationship between this Directive and the acts adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, in order to assess the need for alignment of those specific provisions with this Directive. Where appropriate, the Commission should make proposals with a view to ensuring consistent legal rules relating to the processing of personal data.

(95) In order to ensure a comprehensive and consistent protection of personal data in the Union, international agreements which were concluded by Member States prior to the date of entry into force of this Directive and which comply with the relevant Union law applicable prior to that date should remain in force until amended, replaced or revoked.

(96) Member States should be allowed a period of not more than two years from the date of entry into force of this Directive to transpose it. Processing already under way on that date should be brought into conformity with this Directive within the period of two years after which this Directive enters into force. However, where such processing complies with the Union law applicable prior to the date of entry into force of this Directive, the requirements of this Directive concerning the prior consultation of the supervisory authority should not apply to the processing operations already under way on that date given that those requirements, by their very nature, are to be met prior to the processing. Where Member States use the longer implementation period expiring seven years after the date of entry into force of this Directive for meeting the logging obligations for automated processing systems set up prior to that date, the controller or the processor should have in place effective methods for demonstrating the lawfulness of the data processing, for enabling self-monitoring and for ensuring data integrity and data security, such as logs or other forms of records.

(97) This Directive is without prejudice to the rules on combating the sexual abuse and sexual exploitation of children and child pornography as laid down in Directive 2011/93/EU of the European Parliament and of the Council (14).

(98) Framework Decision 2008/977/JHA should therefore be repealed.

(99) In accordance with Article 6a of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the TEU and to the TFEU,

the United Kingdom and Ireland are not bound by the rules laid down in this Directive which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 TFEU.

(100) In accordance with Articles 2 and 2a of Protocol No 22 on the position of Denmark, as annexed to the TEU and to the TFEU, Denmark is not bound by the rules laid down in this Directive or subject to their application which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU. Given that this Directive builds upon the Schengen acquis, under Title V of Part Three of the TFEU, Denmark, in accordance with Article 4 of that Protocol, is to decide within six months after adoption of this Directive whether it will implement it in its national law.

(101) As regards Iceland and Norway, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis (15).

(102) As regards Switzerland, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis (16).

(103) As regards Liechtenstein, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis (17).

(104) This Directive respects the fundamental rights and observes the principles recognised in the Charter as enshrined in the TFEU, in particular the right to respect for private and family life, the right to the protection of personal data, the right to an effective remedy and to a fair trial. Limitations placed on those rights are in accordance with Article 52(1) of the Charter as they are necessary to meet

objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

(105) In accordance with the Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents, Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition measures. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

(106) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012 (18).

(107) This Directive should not preclude Member States from implementing the exercise of the rights of data subjects on information, access to and rectification or erasure of personal data and restriction of processing in the course of criminal proceedings, and their possible restrictions thereto, in national rules on criminal procedure,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

General provisions

Article 1

Subject-matter and objectives

1. This Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

2. In accordance with this Directive, Member States shall:

(a) protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data; and

(b) ensure that the exchange of personal data by competent authorities within the Union, where such exchange is required by Union or Member State law, is neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

3. This Directive shall not preclude Member States from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities.

Article 2

Scope

1. This Directive applies to the processing of personal data by competent authorities for the purposes set out in Article 1(1).

2. This Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

3. This Directive does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Union institutions, bodies, offices and agencies.

Article 3

Definitions

For the purposes of this Directive:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(6) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(7) 'competent authority' means:

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(8) 'controller' means the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(9) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(10) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(11) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(12) 'genetic data' means personal data, relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(13) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(14) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(15) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 41;

(16) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

CHAPTER II

Principles

Article 4

Principles relating to processing of personal data

1. Member States shall provide for personal data to be:

(a) processed lawfully and fairly;

(b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2. Processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted in so far as:

(a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and

(b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.

3. Processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use, for the purposes set out in Article 1(1), subject to appropriate safeguards for the rights and freedoms of data subjects.

4. The controller shall be responsible for, and be able to demonstrate compliance with, paragraphs 1, 2 and 3.

Article 5

Time-limits for storage and review

Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed.

Article 6

Distinction between different categories of data subject

Member States shall provide for the controller, where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects, such as:

- (a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;
- (b) persons convicted of a criminal offence;
- (c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and
- (d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b).

Article 7

Distinction between personal data and verification of quality of personal data

1. Member States shall provide for personal data based on facts to be distinguished, as far as possible, from personal data based on personal assessments.
2. Member States shall provide for the competent authorities to take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, each competent authority shall, as far as practicable, verify the quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of personal data, necessary information enabling the receiving competent authority to assess the degree of accuracy, completeness and reliability of personal data, and the extent to which they are up to date shall be added.
3. If it emerges that incorrect personal data have been transmitted or personal data have been unlawfully transmitted, the recipient shall be notified without delay. In such a case, the personal data shall be rectified or erased or processing shall be restricted in accordance with Article 16.

Article 8

Lawfulness of processing

1. Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law.
2. Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing.

Article 9

Specific processing conditions

1. Personal data collected by competent authorities for the purposes set out in Article 1(1) shall not be processed for purposes other than those set out in Article 1(1) unless such processing is authorised by Union or Member State law. Where personal data are processed for such other purposes, Regulation (EU) 2016/679 shall apply unless the processing is carried out in an activity which falls outside the scope of Union law.

2. Where competent authorities are entrusted by Member State law with the performance of tasks other than those performed for the purposes set out in Article 1(1), Regulation (EU) 2016/679 shall apply to processing for such purposes, including for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, unless the processing is carried out in an activity which falls outside the scope of Union law.

3. Member States shall, where Union or Member State law applicable to the transmitting competent authority provides specific conditions for processing, provide for the transmitting competent authority to inform the recipient of such personal data of those conditions and the requirement to comply with them.

4. Member States shall provide for the transmitting competent authority not to apply conditions pursuant to paragraph 3 to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the TFEU other than those applicable to similar transmissions of data within the Member State of the transmitting competent authority.

Article 10

Processing of special categories of personal data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:

- (a) where authorised by Union or Member State law;
- (b) to protect the vital interests of the data subject or of another natural person; or
- (c) where such processing relates to data which are manifestly made public by the data subject.

Article 11

Automated individual decision-making

1. Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.
2. Decisions referred to in paragraph 1 of this Article shall not be based on special categories of personal data referred to in Article 10, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.
3. Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law.

CHAPTER III

Rights of the data subject

Article 12

Communication and modalities for exercising the rights of the data subject

1. Member States shall provide for the controller to take reasonable steps to provide any information referred to in Article 13 and make any communication with regard to Articles 11, 14 to 18 and 31 relating to processing to the data subject in a concise, intelligible and easily accessible form, using clear and plain language. The information shall be provided by any appropriate means, including by electronic means. As a general rule, the controller shall provide the information in the same form as the request.
2. Member States shall provide for the controller to facilitate the exercise of the rights of the data subject under Articles 11 and 14 to 18.
3. Member States shall provide for the controller to inform the data subject in writing about the follow up to his or her request without undue delay.
4. Member States shall provide for the information provided under Article 13 and any communication made or action taken pursuant to Articles 11, 14 to 18 and 31 to be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

5. Where the controller has reasonable doubts concerning the identity of the natural person making a request referred to in Article 14 or 16, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

Article 13

Information to be made available or given to the data subject

1. Member States shall provide for the controller to make available to the data subject at least the following information:

(a) the identity and the contact details of the controller;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended;

(d) the right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority;

(e) the existence of the right to request from the controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject.

2. In addition to the information referred to in paragraph 1, Member States shall provide by law for the controller to give to the data subject, in specific cases, the following further information to enable the exercise of his or her rights:

(a) the legal basis for the processing;

(b) the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period;

(c) where applicable, the categories of recipients of the personal data, including in third countries or international organisations;

(d) where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.

3. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:

- (a) avoid obstructing official or legal inquiries, investigations or procedures;
- (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- (c) protect public security;
- (d) protect national security;
- (e) protect the rights and freedoms of others.

4. Member States may adopt legislative measures in order to determine categories of processing which may wholly or partly fall under any of the points listed in paragraph 3.

Article 14

Right of access by the data subject

Subject to Article 15, Member States shall provide for the right of the data subject to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- (a) the purposes of and legal basis for the processing;
- (b) the categories of personal data concerned;
- (c) the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations;
- (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject;
- (f) the right to lodge a complaint with the supervisory authority and the contact details of the supervisory authority;
- (g) communication of the personal data undergoing processing and of any available information as to their origin.

Article 15

Limitations to the right of access

1. Member States may adopt legislative measures restricting, wholly or partly, the data subject's right of access to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:

- (a) avoid obstructing official or legal inquiries, investigations or procedures;
- (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- (c) protect public security;
- (d) protect national security;
- (e) protect the rights and freedoms of others.

2. Member States may adopt legislative measures in order to determine categories of processing which may wholly or partly fall under points (a) to (e) of paragraph 1.

3. In the cases referred to in paragraphs 1 and 2, Member States shall provide for the controller to inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may be omitted where the provision thereof would undermine a purpose under paragraph 1. Member States shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

4. Member States shall provide for the controller to document the factual or legal reasons on which the decision is based. That information shall be made available to the supervisory authorities.

Article 16

Right to rectification or erasure of personal data and restriction of processing

1. Member States shall provide for the right of the data subject to obtain from the controller without undue delay the rectification of inaccurate personal data relating to him or her. Taking into account the purposes of the processing, Member States shall provide for the data subject to have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

2. Member States shall require the controller to erase personal data without undue delay and provide for the right of the data subject to obtain from the controller the erasure of personal data concerning him or her without undue delay where processing infringes the provisions adopted pursuant to Article 4, 8 or 10, or where personal data must be erased in order to comply with a legal obligation to which the controller is subject.

3. Instead of erasure, the controller shall restrict processing where:

(a) the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or

(b) the personal data must be maintained for the purposes of evidence.

Where processing is restricted pursuant to point (a) of the first subparagraph, the controller shall inform the data subject before lifting the restriction of processing.

4. Member States shall provide for the controller to inform the data subject in writing of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal. Member States may adopt legislative measures restricting, wholly or partly, the obligation to provide such information to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned in order to:

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

Member States shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

5. Member States shall provide for the controller to communicate the rectification of inaccurate personal data to the competent authority from which the inaccurate personal data originate.

6. Member States shall, where personal data has been rectified or erased or processing has been restricted pursuant to paragraphs 1, 2 and 3, provide for the controller to notify the recipients and

that the recipients shall rectify or erase the personal data or restrict processing of the personal data under their responsibility.

Article 17

Exercise of rights by the data subject and verification by the supervisory authority

1. In the cases referred to in Article 13(3), Article 15(3) and Article 16(4) Member States shall adopt measures providing that the rights of the data subject may also be exercised through the competent supervisory authority.
2. Member States shall provide for the controller to inform the data subject of the possibility of exercising his or her rights through the supervisory authority pursuant to paragraph 1.
3. Where the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications or a review by the supervisory authority have taken place. The supervisory authority shall also inform the data subject of his or her right to seek a judicial remedy.

Article 18

Rights of the data subject in criminal investigations and proceedings

Member States may provide for the exercise of the rights referred to in Articles 13, 14 and 16 to be carried out in accordance with Member State law where the personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings.

CHAPTER IV

Controller and processor

Section 1

General obligations

Article 19

Obligations of the controller

1. Member States shall provide for the controller, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Directive. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

Article 20

Data protection by design and by default

1. Member States shall provide for the controller, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, both at the time of the determination of the means for processing and at the time of the processing itself, to implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing, in order to meet the requirements of this Directive and protect the rights of data subjects.

2. Member States shall provide for the controller to implement appropriate technical and organisational measures ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Article 21

Joint controllers

1. Member States shall, where two or more controllers jointly determine the purposes and means of processing, provide for them to be joint controllers. They shall, in a transparent manner, determine their respective responsibilities for compliance with this Directive, in particular as regards the exercise of the rights of the data subject and their respective duties to provide the information referred to in Article 13, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement shall designate the contact point for data subjects. Member States may designate which of the joint controllers can act as a single contact point for data subjects to exercise their rights.

2. Irrespective of the terms of the arrangement referred to in paragraph 1, Member States may provide for the data subject to exercise his or her rights under the provisions adopted pursuant to this Directive in respect of and against each of the controllers.

Article 22

Processor

1. Member States shall, where processing is to be carried out on behalf of a controller, provide for the controller to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Directive and ensure the protection of the rights of the data subject.

2. Member States shall provide for the processor not to engage another processor without prior specific or general written authorisation by the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Member States shall provide for the processing by a processor to be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) acts only on instructions from the controller;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) assists the controller by any appropriate means to ensure compliance with the provisions on the data subject's rights;

(d) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of data processing services, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(e) makes available to the controller all information necessary to demonstrate compliance with this Article;

(f) complies with the conditions referred to in paragraphs 2 and 3 for engaging another processor.

4. The contract or the other legal act referred to in paragraph 3 shall be in writing, including in an electronic form.

5. If a processor determines, in infringement of this Directive, the purposes and means of processing, that processor shall be considered to be a controller in respect of that processing.

Article 23

Processing under the authority of the controller or processor

Member States shall provide for the processor and any person acting under the authority of the controller or of the processor, who has access to personal data, not to process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Article 24

Records of processing activities

1. Member States shall provide for controllers to maintain a record of all categories of processing activities under their responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller and the data protection officer;

(b) the purposes of the processing;

(c) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(d) a description of the categories of data subject and of the categories of personal data;

(e) where applicable, the use of profiling;

(f) where applicable, the categories of transfers of personal data to a third country or an international organisation;

(g) an indication of the legal basis for the processing operation, including transfers, for which the personal data are intended;

(h) where possible, the envisaged time limits for erasure of the different categories of personal data;

(i) where possible, a general description of the technical and organisational security measures referred to in Article 29(1).

2. Member States shall provide for each processor to maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors, of each controller on behalf of which the processor is acting and, where applicable, the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation where explicitly instructed to do so by the controller, including the identification of that third country or international organisation;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 29(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

The controller and the processor shall make those records available to the supervisory authority on request.

Article 25

Logging

1. Member States shall provide for logs to be kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure. The logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.

2. The logs shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.

3. The controller and the processor shall make the logs available to the supervisory authority on request.

Article 26

Cooperation with the supervisory authority

Member States shall provide for the controller and the processor to cooperate, on request, with the supervisory authority in the performance of its tasks on request.

Article 27

Data protection impact assessment

1. Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Member States shall provide for the controller to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.
2. The assessment referred to in paragraph 1 shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

Article 28

Prior consultation of the supervisory authority

1. Member States shall provide for the controller or processor to consult the supervisory authority prior to processing which will form part of a new filing system to be created, where:
 - (a) a data protection impact assessment as provided for in Article 27 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or
 - (b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.
2. Member States shall provide for the supervisory authority to be consulted during the preparation of a proposal for a legislative measure to be adopted by a national parliament or of a regulatory measure based on such a legislative measure, which relates to processing.
3. Member States shall provide that the supervisory authority may establish a list of the processing operations which are subject to prior consultation pursuant to paragraph 1.
4. Member States shall provide for the controller to provide the supervisory authority with the data protection impact assessment pursuant to Article 27 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in

particular of the risks for the protection of personal data of the data subject and of the related safeguards.

5. Member States shall, where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 of this Article would infringe the provisions adopted pursuant to this Directive, in particular where the controller has insufficiently identified or mitigated the risk, provide for the supervisory authority to provide, within a period of up to six weeks of receipt of the request for consultation, written advice to the controller and, where applicable, to the processor, and may use any of its powers referred to in Article 47. That period may be extended by a month, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor of any such extension within one month of receipt of the request for consultation, together with the reasons for the delay.

Section 2

Security of personal data

Article 29

Security of processing

1. Member States shall provide for the controller and the processor, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data referred to in Article 10.

2. In respect of automated processing, each Member State shall provide for the controller or processor, following an evaluation of the risks, to implement measures designed to:

(a) deny unauthorised persons access to processing equipment used for processing ('equipment access control');

(b) prevent the unauthorised reading, copying, modification or removal of data media ('data media control');

(c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data ('storage control');

- (d) prevent the use of automated processing systems by unauthorised persons using data communication equipment ('user control');
- (e) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation ('data access control');
- (f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control');
- (g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('input control');
- (h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control');
- (i) ensure that installed systems may, in the case of interruption, be restored ('recovery');
- (j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity').

Article 30

Notification of a personal data breach to the supervisory authority

1. Member States shall, in the case of a personal data breach, provide for the controller to notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
 - (a) describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. Member States shall provide for the controller to document any personal data breaches referred to in paragraph 1, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

6. Member States shall, where the personal data breach involves personal data that have been transmitted by or to the controller of another Member State, provide for the information referred to in paragraph 3 to be communicated to the controller of that Member State without undue delay.

Article 31

Communication of a personal data breach to the data subject

1. Member States shall, where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, provide for the controller to communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and shall contain at least the information and measures referred to in points (b), (c) and (d) of Article 30(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technological and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve a disproportionate effort. In such a case, there shall instead be a public communication or a similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so, or may decide that any of the conditions referred to in paragraph 3 are met.

5. The communication to the data subject referred to in paragraph 1 of this Article may be delayed, restricted or omitted subject to the conditions and on the grounds referred to in Article 13(3).

Section 3

Data protection officer

Article 32

Designation of the data protection officer

1. Member States shall provide for the controller to designate a data protection officer. Member States may exempt courts and other independent judicial authorities when acting in their judicial capacity from that obligation.

2. The data protection officer shall be designated on the basis of his or her professional qualities and, in particular, his or her expert knowledge of data protection law and practice and ability to fulfil the tasks referred to in Article 34.

3. A single data protection officer may be designated for several competent authorities, taking account of their organisational structure and size.

4. Member States shall provide for the controller to publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 33

Position of the data protection officer

1. Member States shall provide for the controller to ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller shall support the data protection officer in performing the tasks referred to in Article 34 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

Article 34

Tasks of the data protection officer

Member States shall provide for the controller to entrust the data protection officer at least with the following tasks:

- (a) to inform and advise the controller and the employees who carry out processing of their obligations pursuant to this Directive and to other Union or Member State data protection provisions;
- (b) to monitor compliance with this Directive, with other Union or Member State data protection provisions and with the policies of the controller in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 27;
- (d) to cooperate with the supervisory authority;
- (e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 28, and to consult, where appropriate, with regard to any other matter.

CHAPTER V

Transfers of personal data to third countries or international organisations

Article 35

General principles for transfers of personal data

1. Member States shall provide for any transfer by competent authorities of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation including for onward transfers to another third country or international organisation to take place, subject to compliance with the national provisions adopted pursuant to other provisions of this Directive, only where the conditions laid down in this Chapter are met, namely:

- (a) the transfer is necessary for the purposes set out in Article 1(1);
- (b) the personal data are transferred to a controller in a third country or international organisation that is an authority competent for the purposes referred to in Article 1(1);
- (c) where personal data are transmitted or made available from another Member State, that Member State has given its prior authorisation to the transfer in accordance with its national law;
- (d) the Commission has adopted an adequacy decision pursuant to Article 36, or, in the absence of such a decision, appropriate safeguards have been provided or exist pursuant to Article 37, or, in the absence of an adequacy decision pursuant to Article 36 and of appropriate safeguards in accordance with Article 37, derogations for specific situations apply pursuant to Article 38; and
- (e) in the case of an onward transfer to another third country or international organisation, the competent authority that carried out the original transfer or another competent authority of the same Member State authorises the onward transfer, after taking into due account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data was originally transferred and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred.

2. Member States shall provide for transfers without the prior authorisation by another Member State in accordance with point (c) of paragraph 1 to be permitted only if the transfer of the personal data is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed without delay.

3. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons ensured by this Directive is not undermined.

Article 36

Transfers on the basis of an adequacy decision

1. Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation, which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with data protection rules, including adequate enforcement powers, for assisting and advising data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide a mechanism for periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 58(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 58(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 58(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. Member States shall provide for a decision pursuant to paragraph 5 to be without prejudice to transfers of personal data to the third country, the territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 37 and 38.

8. The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

Article 37

Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 36(3), Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where:

(a) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or

(b) the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with regard to the protection of personal data.

2. The controller shall inform the supervisory authority about categories of transfers under point (b) of paragraph 1.

3. When a transfer is based on point (b) of paragraph 1, such a transfer shall be documented and the documentation shall be made available to the supervisory authority on request, including the date

and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

Article 38

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 36, or of appropriate safeguards pursuant to Article 37, Member States shall provide that a transfer or a category of transfers of personal data to a third country or an international organisation may take place only on the condition that the transfer is necessary:

(a) in order to protect the vital interests of the data subject or another person;

(b) to safeguard legitimate interests of the data subject, where the law of the Member State transferring the personal data so provides;

(c) for the prevention of an immediate and serious threat to public security of a Member State or a third country;

(d) in individual cases for the purposes set out in Article 1(1); or

(e) in an individual case for the establishment, exercise or defence of legal claims relating to the purposes set out in Article 1(1).

2. Personal data shall not be transferred if the transferring competent authority determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer set out in points (d) and (e) of paragraph 1.

3. Where a transfer is based on paragraph 1, such a transfer shall be documented and the documentation shall be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

Article 39

Transfers of personal data to recipients established in third countries

1. By way of derogation from point (b) of Article 35(1) and without prejudice to any international agreement referred to in paragraph 2 of this Article, Union or Member State law may provide for the competent authorities referred to in point (7)(a) of Article 3, in individual and specific cases, to transfer

personal data directly to recipients established in third countries only if the other provisions of this Directive are complied with and all of the following conditions are fulfilled:

- (a) the transfer is strictly necessary for the performance of a task of the transferring competent authority as provided for by Union or Member State law for the purposes set out in Article 1(1);
- (b) the transferring competent authority determines that no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand;
- (c) the transferring competent authority considers that the transfer to an authority that is competent for the purposes referred to in Article 1(1) in the third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time;
- (d) the authority that is competent for the purposes referred to in Article 1(1) in the third country is informed without undue delay, unless this is ineffective or inappropriate;
- (e) the transferring competent authority informs the recipient of the specified purpose or purposes for which the personal data are only to be processed by the latter provided that such processing is necessary.

2. An international agreement referred to in paragraph 1 shall be any bilateral or multilateral international agreement in force between Member States and third countries in the field of judicial cooperation in criminal matters and police cooperation.

3. The transferring competent authority shall inform the supervisory authority about transfers under this Article.

4. Where a transfer is based on paragraph 1, such a transfer shall be documented.

Article 40

International cooperation for the protection of personal data

In relation to third countries and international organisations, the Commission and Member States shall take appropriate steps to:

- (a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;
- (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and

information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

CHAPTER VI

Independent supervisory authorities

Section 1

Independent status

Article 41

Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Directive, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

2. Each supervisory authority shall contribute to the consistent application of this Directive throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and with the Commission in accordance with Chapter VII.

3. Member States may provide for a supervisory authority established under Regulation (EU) 2016/679 to be the supervisory authority referred to in this Directive and to assume responsibility for the tasks of the supervisory authority to be established under paragraph 1 of this Article.

4. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which are to represent those authorities in the Board referred to in Article 51.

Article 42

Independence

1. Each Member State shall provide for each supervisory authority to act with complete independence in performing its tasks and exercising its powers in accordance with this Directive.

2. Member States shall provide for the member or members of their supervisory authorities in the performance of their tasks and exercise of their powers in accordance with this Directive, to remain free from external influence, whether direct or indirect, and that they shall neither seek nor take instructions from anybody.

3. Members of Member States' supervisory authorities shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

Article 43

General conditions for the members of the supervisory authority

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

- their parliament;

- their government;

- their head of State; or

- an independent body entrusted with the appointment under Member State law.

2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform their duties and exercise their powers.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

Article 44

Rules on the establishment of the supervisory authority

1. Each Member State shall provide by law for all of the following:

- (a) the establishment of each supervisory authority;
- (b) the qualifications and eligibility conditions required to be appointed as a member of each supervisory authority;
- (c) the rules and procedures for the appointment of the member or members of each supervisory authority;
- (d) the duration of the term of the member or members of each supervisory authority of not less than four years, except for the first appointment after 6 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;
- (e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;
- (f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or the exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Directive.

Section 2

Competence, tasks and powers

Article 45

Competence

1. Each Member State shall provide for each supervisory authority to be competent for the performance of the tasks assigned to, and for the exercise of the powers conferred on, it in accordance with this Directive on the territory of its own Member State.

2. Each Member State shall provide for each supervisory authority not to be competent for the supervision of processing operations of courts when acting in their judicial capacity. Member States may provide for their supervisory authority not to be competent to supervise processing operations of other independent judicial authorities when acting in their judicial capacity.

Article 46

Tasks

1. Each Member State shall provide, on its territory, for each supervisory authority to:

(a) monitor and enforce the application of the provisions adopted pursuant to this Directive and its implementing measures;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing;

(c) advise, in accordance with Member State law, the national parliament, the government and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Directive;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Directive and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) deal with complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 55, and investigate, to the extent appropriate, the subject-matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g) check the lawfulness of processing pursuant to Article 17, and inform the data subject within a reasonable period of the outcome of the check pursuant to paragraph 3 of that Article or of the reasons why the check has not been carried out;

(h) cooperate with, including by sharing information, and provide mutual assistance to other supervisory authorities, with a view to ensuring the consistency of application and enforcement of this Directive;

(i) conduct investigations on the application of this Directive, including on the basis of information received from another supervisory authority or other public authority;

(j) monitor relevant developments insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;

(k) provide advice on the processing operations referred to in Article 28; and

(l) contribute to the activities of the Board.

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and for the data protection officer.

4. Where a request is manifestly unfounded or excessive, in particular because it is repetitive, the supervisory authority may charge a reasonable fee based on its administrative costs, or may refuse to act on the request. The supervisory authority shall bear the burden of demonstrating that the request is manifestly unfounded or excessive.

Article 47

Powers

1. Each Member State shall provide by law for each supervisory authority to have effective investigative powers. Those powers shall include at least the power to obtain from the controller and the processor access to all personal data that are being processed and to all information necessary for the performance of its tasks.

2. Each Member State shall provide by law for each supervisory authority to have effective corrective powers such as, for example:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe the provisions adopted pursuant to this Directive;

(b) to order the controller or processor to bring processing operations into compliance with the provisions adopted pursuant to this Directive, where appropriate, in a specified manner and within a specified period, in particular by ordering the rectification or erasure of personal data or restriction of processing pursuant to Article 16;

(c) to impose a temporary or definitive limitation, including a ban, on processing.

3. Each Member State shall provide by law for each supervisory authority to have effective advisory powers to advise the controller in accordance with the prior consultation procedure referred to in Article 28 and to issue, on its own initiative or on request, opinions to its national parliament and its government or, in accordance with its national law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data.

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, as set out in Union and Member State law in accordance with the Charter.

5. Each Member State shall provide by law for each supervisory authority to have the power to bring infringements of provisions adopted pursuant to this Directive to the attention of judicial authorities and, where appropriate, to commence or otherwise engage in legal proceedings, in order to enforce the provisions adopted pursuant to this Directive.

Article 48

Reporting of infringements

Member States shall provide for competent authorities to put in place effective mechanisms to encourage confidential reporting of infringements of this Directive.

Article 49

Activity reports

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of penalties imposed. Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, the Commission and the Board.

CHAPTER VII

Cooperation

Article 50

Mutual assistance

1. Each Member State shall provide for their supervisory authorities to provide each other with relevant information and mutual assistance in order to implement and apply this Directive in a consistent manner, and to put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out consultations, inspections and investigations.
2. Each Member States shall provide for each supervisory authority to take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.
3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.
4. The requested supervisory authority shall not refuse to comply with the request unless:
 - (a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or
 - (b) compliance with the request would infringe this Directive or Union or Member State law to which the supervisory authority receiving the request is subject.
5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.
6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.
7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.
8. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by

electronic means between supervisory authorities, and between supervisory authorities and the Board. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 58(2).

Article 51

Tasks of the Board

1. The Board established by Regulation (EU) 2016/679 shall perform all of the following tasks in relation to processing within the scope of this Directive:

(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Directive;

(b) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Directive and issue guidelines, recommendations and best practices in order to encourage consistent application of this Directive;

(c) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 47(1) and (3);

(d) issue guidelines, recommendations and best practices in accordance with point (b) of this subparagraph for establishing personal data breaches and determining the undue delay referred to in Article 30(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

(e) issue guidelines, recommendations and best practices in accordance with point (b) of this subparagraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons as referred to in Article 31(1);

(f) review the practical application of the guidelines, recommendations and best practices referred to in points (b) and (c);

(g) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country, a territory or one or more specified sectors within a third country, or an international organisation, including for the assessment whether such a third country, territory, specified sector, or international organisation no longer ensures an adequate level of protection;

(h) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;

(i) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;

(j) promote the exchange of knowledge and documentation on data protection law and practice with data protection supervisory authorities worldwide.

With regard to point (g) of the first subparagraph, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with the territory or specified sector within that third country, or with the international organisation.

2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The Board shall forward its opinions, guidelines, recommendations and best practices to the Commission and to the committee referred to in Article 58(1) and make them public.

4. The Commission shall inform the Board of the action it has taken following opinions, guidelines, recommendations and best practices issued by the Board.

CHAPTER VIII

Remedies, liability and penalties

Article 52

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, Member States shall provide for every data subject to have the right to lodge a complaint with a single supervisory authority, if the data subject considers that the processing of personal data relating to him or her infringes provisions adopted pursuant to this Directive.

2. Member States shall provide for the supervisory authority with which the complaint has been lodged to transmit it to the competent supervisory authority, without undue delay if the complaint is not lodged with the supervisory authority that is competent pursuant to Article 45(1). The data subject shall be informed about the transmission.

3. Member States shall provide for the supervisory authority with which the complaint has been lodged to provide further assistance on request of the data subject.

4. The data subject shall be informed by the competent supervisory authority of the progress and the outcome of the complaint, including of the possibility of a judicial remedy pursuant to Article 53.

Article 53

Right to an effective judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, Member States shall provide for the right of a natural or legal person to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Article 45(1) does not handle a complaint or does not inform the data subject within three months of the progress or outcome of the complaint lodged pursuant to Article 52.

3. Member States shall provide for proceedings against a supervisory authority to be brought before the courts of the Member State where the supervisory authority is established.

Article 54

Right to an effective judicial remedy against a controller or processor

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 52, Member States shall provide for the right of a data subject to an effective judicial remedy where he or she considers that his or her rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of his or her personal data in non-compliance with those provisions.

Article 55

Representation of data subjects

Member States shall, in accordance with Member State procedural law, provide for the data subject to have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with Member State law, has statutory objectives which are in the public interest and is active in the field of protection of data subject's rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf and to exercise the rights referred to in Articles 52, 53 and 54 on his or her behalf.

Article 56

Right to compensation

Member States shall provide for any person who has suffered material or non-material damage as a result of an unlawful processing operation or of any act infringing national provisions adopted pursuant to this Directive to have the right to receive compensation for the damage suffered from the controller or any other authority competent under Member State law.

Article 57

Penalties

Member States shall lay down the rules on penalties applicable to infringements of the provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.

CHAPTER IX

Implementing acts

Article 58

Committee procedure

1. The Commission shall be assisted by the committee established by Article 93 of Regulation (EU) 2016/679. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.
3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER X

Final provisions

Article 59

Repeal of Framework Decision 2008/977/JHA

1. Framework Decision 2008/977/JHA is repealed with effect from 6 May 2018.
2. References to the repealed Decision referred to in paragraph 1 shall be construed as references to this Directive.

Article 60

Union legal acts already in force

The specific provisions for the protection of personal data in Union legal acts that entered into force on or before 6 May 2016 in the field of judicial cooperation in criminal matters and police cooperation, which regulate processing between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive, shall remain unaffected.

Article 61

Relationship with previously concluded international agreements in the field of judicial cooperation in criminal matters and police cooperation

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 6 May 2016 and which comply with Union law as applicable prior to that date shall remain in force until amended, replaced or revoked.

Article 62

Commission reports

1. By 6 May 2022, and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Directive to the European Parliament and to the Council. The reports shall be made public.
2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 36(3) and Article 39.
3. For the purposes of paragraphs 1 and 2, the Commission may request information from Member States and supervisory authorities.
4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council and of other relevant bodies or sources.
5. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Directive, in particular taking account of developments in information technology and in the light of the state of progress in the information society.
6. By 6 May 2019, the Commission shall review other legal acts adopted by the Union which regulate processing by the competent authorities for the purposes set out in Article 1(1) including those

referred to in Article 60, in order to assess the need to align them with this Directive and to make, where appropriate, the necessary proposals to amend those acts to ensure a consistent approach to the protection of personal data within the scope of this Directive.

Article 63

Transposition

1. Member States shall adopt and publish, by 6 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions. They shall apply those provisions from 6 May 2018.

When Member States adopt those provisions, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. By way of derogation from paragraph 1, a Member State may provide, exceptionally, where it involves disproportionate effort, for automated processing systems set up before 6 May 2016 to be brought into conformity with Article 25(1) by 6 May 2023.

3. By way of derogation from paragraphs 1 and 2 of this Article, a Member State may, in exceptional circumstances, bring an automated processing system as referred to in paragraph 2 of this Article into conformity with Article 25(1) within a specified period after the period referred to in paragraph 2 of this Article, if it would otherwise cause serious difficulties for the operation of that particular automated processing system. The Member State concerned shall notify the Commission of the grounds for those serious difficulties and the grounds for the specified period within which it shall bring that particular automated processing system into conformity with Article 25(1). The specified period shall in any event not be later than 6 May 2026.

4. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 64

Entry into force

This Directive shall enter into force on the day following that of its publication in the Official Journal of the European Union.

Article 65

Addressees

This Directive is addressed to the Member States.

Done at Brussels, 27 April 2016.

For the European Parliament

The President

M. SCHULZ

For the Council

The President

J.A. HENNIS-PLASSCHAERT

(1) OJ C 391, 18.12.2012, p. 127.

(2) Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal).
Position of the European Parliament of 14 April 2016.

(3) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

(4) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60).

(5) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (see page 1 of this Official Journal).

(6) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

(7) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

(8) Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol (OJ L 27, 29.1.2005, p. 61).

- (9) Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).
- (10) Council Directive 77/249/EEC of 22 March 1977 to facilitate the effective exercise by lawyers of freedom to provide services (OJ L 78, 26.3.1977, p. 17).
- (11) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).
- (12) Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 1).
- (13) Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (OJ C 197, 12.7.2000, p. 1).
- (14) Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).
- (15) OJ L 176, 10.7.1999, p. 36.
- (16) OJ L 53, 27.2.2008, p. 52.
- (17) OJ L 160, 18.6.2011, p. 21.
- (18) OJ C 192, 30.6.2012, p. 7.

Avrupa Birliđi - Açık Veri Direktifi (Open Data Directive)

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information

Official Journal of the European Union, L 172/56, 26.6.2019

DIRECTIVE (EU) 2019/1024 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 June 2019 on open data and the re-use of public sector information (recast)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) Directive 2003/98/EC of the European Parliament and of the Council (3) has been substantially amended. Since further amendments are to be made, that Directive should be recast in the interests of clarity.

(2) Pursuant to Article 13 of Directive 2003/98/EC and five years after the adoption of Directive 2013/37/EU of the European Parliament and of the Council (4), which amended Directive 2003/98/EC, the Commission, after consulting the relevant stakeholders, evaluated and reviewed the functioning of Directive 2003/98/EC in the framework of a regulatory fitness and performance programme.

(3) Following the stakeholder consultation and in the light of the result of the impact assessment, the Commission considered that action at Union level was necessary in order to address the remaining and emerging barriers to a wide re-use of public sector and publicly funded information across the Union, in order to bring the legislative framework up to date with the advances in digital technologies and to further stimulate digital innovation, especially with regard to artificial intelligence.

(4) The substantive changes introduced to the legal text so as to fully exploit the potential of public sector information for the European economy and society should focus on the following areas: the provision of real-time access to dynamic data via adequate technical means, the increase of the supply of valuable public data for re-use, including from public undertakings, research performing organisations and research funding organisations, the tackling of the emergence of new forms of exclusive arrangements, the use of exceptions to the principle of charging the marginal cost and the relationship between this Directive and certain related legal instruments, including Regulation (EU) 2016/679 of the European Parliament and of the Council (5) and Directives 96/9/EC (6), 2003/4/EC (7) and 2007/2/EC (8) of the European Parliament and of the Council.

(5) Access to information is a fundamental right. The Charter of Fundamental Rights of the European Union (Charter) provides that everyone has the right to freedom of expression, including the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

(6) Article 8 of the Charter guarantees the right to the protection of personal data and provides that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law, and subject to control by an independent authority.

(7) The Treaty on the Functioning of the European Union (TFEU) provides for the establishment of an internal market and of a system ensuring that competition in the internal market is not distorted. Harmonisation of the rules and practices in the Member States relating to the exploitation of public sector information contributes to the achievement of those objectives.

(8) The public sector in Member States collects, produces, reproduces and disseminates a wide range of information in many areas of activity, such as social, political, economic, legal, geographical, environmental, meteorological, seismic, touristic, business, patent-related and educational areas. Documents produced by public sector bodies of the executive, legislature or judiciary constitute a vast, diverse and valuable pool of resources that can benefit society. Providing that information, which includes dynamic data, in a commonly used electronic format allows citizens and legal entities to find new ways to use them and create new, innovative products and services. Member States and public sector bodies may be able to benefit from and receive adequate financial support from relevant Union funds and programmes, ensuring a wide use of digital technologies or the digital transformation of public administrations and public services, in their efforts to make data easily available for re-use.

(9) Public sector information represents an extraordinary source of data that can contribute to improving the internal market and to the development of new applications for consumers and legal entities. Intelligent data usage, including their processing through artificial intelligence applications, can have a transformative effect on all sectors of the economy.

(10) Directive 2003/98/EC established a set of minimum rules governing the re-use and the practical arrangements for facilitating re-use of existing documents held by public sector bodies of the Member States, including executive, legislative and judicial bodies. Since the adoption of the first set of rules on re-use of public sector information, the amount of data in the world, including public data, has increased exponentially and new types of data are being generated and collected. In parallel, there is a continuous evolution in technologies for analysis, exploitation and processing of data, such as machine learning, artificial intelligence and the internet of things. That rapid technological evolution makes it possible to create new services and new applications, which are built upon the use, aggregation or combination of data. The rules originally adopted in 2003, and amended in 2013, no longer keep pace with those rapid changes, and as a result, the economic and social opportunities offered by the re-use of public data risk being missed.

(11) The evolution towards a data-based society, where data from different domains and activities are used, influences the life of every citizen in the Union, inter alia, by enabling them to gain new ways of accessing and acquiring knowledge.

(12) Digital content plays an important role in that evolution. Content production has given rise to rapid job creation in recent years and continues to do so. Most of those jobs are created by innovative start-ups and small and medium-sized enterprises (SMEs).

(13) One of the principal aims of the establishment of an internal market is the creation of conditions conducive to the development of services and products Union-wide and within Member States. Public sector information or information collected, produced, reproduced, and disseminated within the exercise of a public task or a service of general interest, is an important primary material for digital content products and services and will become an even more important content resource with the development of advanced digital technologies, such as artificial intelligence, distributed ledger technologies and the internet of things. Broad, cross-border geographical coverage will also be essential in that context. Increased possibilities of re-using such information is expected, inter alia, to allow all Union businesses, including microenterprises and SMEs, as well as civil society, to exploit its potential and contribute to economic development and high-quality job creation and protection,

especially for the benefit of local communities, and to important societal goals such as accountability and transparency.

(14) Allowing the re-use of documents held by a public sector body adds value for the benefit of re-users, end users and society in general and in many cases for the benefit of the public sector body itself, by promoting transparency and accountability and by providing feedback from re-users and end users, which allows the public sector body concerned to improve the quality of the information collected and the performance of its tasks.

(15) There are considerable differences in the rules and practices in the Member States relating to the exploitation of public sector information resources, which constitute barriers to bringing out the full economic potential of that key document resource. The fact that practice in public sector bodies in exploiting public sector information continues to vary among Member States should be taken into account. Minimum harmonisation of national rules and practices on the re-use of public sector documents should therefore be pursued where the differences in national regulations and practices or the absence of clarity hinder the smooth functioning of the internal market and the proper development of the information society in the Union.

(16) Open data as a concept is generally understood to denote data in an open format that can be freely used, re-used and shared by anyone for any purpose. Open data policies which encourage the wide availability and re-use of public sector information for private or commercial purposes, with minimal or no legal, technical or financial constraints, and which promote the circulation of information not only for economic operators but primarily for the public, can play an important role in promoting social engagement, and kick-start and promote the development of new services based on novel ways to combine and make use of such information. Member States are therefore encouraged to promote the creation of data based on the principle of 'open by design and by default', with regard to all documents falling within the scope of this Directive. In doing so they should ensure a consistent level of protection of public interest objectives, such as public security, including where sensitive critical infrastructure protection related information are concerned. They should also ensure the protection of personal data, including where information in an individual data set does not present a risk of identifying or singling out a natural person, but when that information is combined with other available information, it could entail such a risk.

(17) Moreover, without minimum harmonisation at Union level, legislative activity at national level, which has already been initiated in a number of Member States in order to respond to the technological challenges, might result in even more significant divergence. The impact of such

legislative divergence and uncertainties will become more significant with the further development of the information society, which has already greatly increased cross-border exploitation of information.

(18) Member States have established re-use policies under Directive 2003/98/EC and some of them have been adopting ambitious open data approaches to make the re-use of accessible public data easier for citizens and legal entities beyond the minimum level set by that Directive. There is a risk that diverging rules across Member States act as a barrier to the cross-border offer of products and services and prevent comparable public data sets from being re-usable for pan-Union applications based on them. Therefore, minimum harmonisation is required to determine what public data are available for re-use in the internal information market, consistent with and not affecting the relevant access regimes, both general and sectoral, such as that defined in Directive 2003/4/EC. The provisions of Union and national law that go beyond those minimum requirements, in particular in cases of sectoral law, should continue to apply. Examples of provisions that exceed the minimum harmonisation level of this Directive include lower thresholds for permissible charges for re-use than the thresholds provided for in this Directive or less restrictive licensing terms than those referred to in this Directive. In particular, this Directive is without prejudice to provisions that exceed the minimum harmonisation level of this Directive as laid down in Commission delegated regulations adopted under Directive 2010/40/EU of the European Parliament and of the Council (9).

(19) Moreover, Member States are encouraged to go beyond the minimum requirements set out in this Directive by applying its requirements to documents held by public undertakings, which are related to activities that have been found, pursuant to Article 34 of Directive 2014/25/EU of the European Parliament and of the Council (10), to be directly exposed to competition. Member States may also decide to apply the requirements of this Directive to private undertakings, in particular those that provide services of general interest.

(20) A general framework for the conditions governing re-use of public sector documents is needed in order to ensure fair, proportionate and non-discriminatory conditions for the re-use of such information. Public sector bodies collect, produce, reproduce and disseminate documents to fulfil their public tasks. Public undertakings collect, produce, reproduce and disseminate documents to provide services in the general interest. Use of such documents for other reasons constitutes re-use. Member States' policies can go beyond the minimum standards established in this Directive, thus allowing for more extensive re-use. When transposing this Directive, Member States can use terms

other than 'document', provided that they retain the full scope of the definition of 'document' set out in this Directive.

(21) This Directive should apply to documents the supply of which forms part of the public tasks of the public sector bodies concerned, as defined by law or by other binding rules in the Member States. In the absence of such rules the public tasks should be defined in accordance with common administrative practice in the Member States, provided that the scope of the public tasks is transparent and subject to review. The public tasks could be defined generally or on a case-by-case basis for individual public sector bodies.

(22) This Directive should apply to documents that are made accessible for re-use when public sector bodies license, sell, disseminate, exchange or provide information. To avoid cross-subsidies, re-use should include further use of documents within the organisation itself for activities falling outside the scope of its public tasks. Activities falling outside the public task typically include supply of documents that are produced and charged for exclusively on a commercial basis and in competition with others in the market.

(23) This Directive does not restrict or impair the performance of the statutory tasks of public authorities and other public sector bodies. This Directive lays down an obligation for Member States to make all existing documents re-usable unless access is restricted or excluded under national rules on access to documents or subject to the other exceptions laid down in this Directive. This Directive builds on the existing access regimes in the Member States and does not change the national rules for access to documents. It does not apply to cases in which citizens or legal entities can, under the relevant access regime, obtain a document only if they can prove a particular interest. At Union level, Article 41 on the right to good administration and Article 42 on the right of access to documents in the Charter recognise the right of any citizen of the Union and any natural or legal person residing or having its registered office in a Member State to have access to documents held by the European Parliament, the Council and the Commission. Public sector bodies should be encouraged to make available for re-use any documents held by them. Public sector bodies should promote and encourage re-use of documents, including official texts of a legislative and administrative nature in those cases where the public sector body has the right to authorise their re-use.

(24) Member States often entrust the provision of services in the general interest with entities outside of the public sector while maintaining a high degree of control over such entities. At the same time, Directive 2003/98/EC applies only to documents held by public sector bodies, while excluding public undertakings from its scope. This leads to poor availability for re-use of documents produced in the

performance of services in the general interest in a number of areas, in particular in the utility sectors. It also greatly reduces the potential for the creation of cross-border services based on documents held by public undertakings that provide services in the general interest.

(25) Directive 2003/98/EC should therefore be amended in order to ensure that it can be applied to the re-use of existing documents produced in the performance of services in the general interest by public undertakings pursuing one of the activities referred to in Articles 8 to 14 of Directive 2014/25/EU, as well as by public undertakings acting as public service operators pursuant to Article 2 of Regulation (EC) No 1370/2007 of the European Parliament and of the Council (11), public undertakings acting as air carriers fulfilling public service obligations pursuant to Article 16 of Regulation (EC) No 1008/2008 of the European Parliament and of the Council (12), and public undertakings acting as Community shipowners fulfilling public service obligations pursuant to Article 4 of Council Regulation (EEC) No 3577/92 (13).

(26) This Directive does not contain a general obligation to allow the re-use of documents produced by public undertakings. The decision whether or not to authorise re-use should remain with the public undertaking concerned, except where otherwise required by this Directive or by Union or national law. Only after the public undertaking has made a document available for re-use, should it observe the relevant obligations laid down in Chapters III and IV of this Directive, in particular as regards format, charging, transparency, licences, non-discrimination and prohibition of exclusive arrangements. On the other hand, public undertakings should not be required to comply with the requirements laid down in Chapter II, such as the rules applicable to processing of requests. When allowing the re-use of documents, particular attention should be given to sensitive critical infrastructure protection related information as defined in Council Directive 2008/114/EC (14) and of essential services within the meaning of Directive (EU) 2016/1148 of the European Parliament and of the Council (15).

(27) The volume of research data generated is growing exponentially and has potential for re-use beyond the scientific community. In order to be able to address mounting societal challenges efficiently and in a holistic manner, it has become crucial and urgent to be able to access, blend and re-use data from different sources, as well as across sectors and disciplines. Research data includes statistics, results of experiments, measurements, observations resulting from fieldwork, survey results, interview recordings and images. It also includes meta-data, specifications and other digital objects. Research data is different from scientific articles reporting and commenting on findings resulting from their scientific research. For many years, the open availability and re-usability of

scientific research data stemming from public funding has been subject to specific policy initiatives. Open access is understood as the practice of providing online access to research outputs free of charge for the end user and without restrictions on use and re-use beyond the possibility to require acknowledgement of authorship. Open access policies aim in particular to provide researchers and the public at large with access to research data as early as possible in the dissemination process and to facilitate its use and re-use. Open access helps enhance quality, reduce the need for unnecessary duplication of research, speed up scientific progress, combat scientific fraud, and it can overall favour economic growth and innovation. Beside open access, commendable efforts are being made to ensure that data management planning becomes a standard scientific practice and to support the dissemination of research data that are findable, accessible, interoperable and re-usable (the FAIR principle).

(28) For the reasons explained above, it is appropriate to set an obligation on Member States to adopt open access policies with respect to publicly funded research data and ensure that such policies are implemented by all research performing organisations and research funding organisations. Research performing organisations and research funding organisations could also be organised as public sector bodies or public undertakings. This Directive applies to such hybrid organisations only in their capacity as research performing organisations and to their research data. Open access policies typically allow for a range of exceptions from making scientific research results openly available. The Commission Recommendation of 25 April 2018 on access to and preservation of scientific information describes, among other things, relevant elements of open access policies. Additionally, the conditions, under which certain research data can be re-used, should be improved. For that reason, certain obligations stemming from this Directive should be extended to research data resulting from scientific research activities subsidised by public funding or co-funded by public and private-sector entities. Under the national open access policies, publicly funded research data should be made open as the default option. However, in this context, concerns in relation to privacy, protection of personal data, confidentiality, national security, legitimate commercial interests, such as trade secrets, and to intellectual property rights of third parties should be duly taken into account, according to the principle ‘as open as possible, as closed as necessary’. Moreover, research data which are excluded from access on grounds of national security, defence or public security should not be covered by this Directive. In order to avoid any administrative burden, obligations stemming from this Directive should apply only to such research data that have already been made publicly available by researchers, research performing organisations or research funding organisations through an institutional or subject-based repository and should not impose extra costs for the retrieval of the

datasets or require additional curation of data. Member States may extend the application of this Directive to research data made publicly available through other data infrastructures than repositories, through open access publications, as an attached file to an article, a data paper or a paper in a data journal. Documents other than research data should continue to be exempt from the scope of this Directive.

(29) The definition of ‘public sector body’ is based on the definition in point (1) of Article 2(1) of Directive 2014/24/EU of the European Parliament and of the Council (16). The definition of ‘body governed by public law’ set out in that Directive and the definition of ‘public undertaking’ set out in Directive 2014/25/EU should apply to this Directive.

(30) This Directive lays down the definition of the term ‘document’ and that definition should include any part of a document. The term ‘document’ should cover any representation of acts, facts or information - and any compilation of such acts, facts or information - whatever its medium (paper, or electronic form or as a sound, visual or audiovisual recording). The definition of ‘document’ is not intended to cover computer programmes. Member States may extend the application of this Directive to computer programmes.

(31) Public sector bodies are increasingly making their documents available for re-use in a proactive manner, by ensuring online discoverability and actual availability of documents and associated metadata in an open format that can be machine-readable and that ensure interoperability, re-use and accessibility. Documents should also be made available for re-use following a request lodged by a re-user. In those cases, the time limit for replying to requests for re-use should be reasonable and in accordance with the equivalent time for requests to access the document under the relevant access regimes. Public undertakings, educational establishments, research performing organisations and research funding organisations should however be exempt from that requirement. Reasonable time limits throughout the Union will stimulate the creation of new aggregated information products and services at pan-Union level. This is particularly important for dynamic data (including environmental, traffic, satellite, meteorological and sensor generated data), the economic value of which depends on the immediate availability of the information and of regular updates. Dynamic data should therefore be made available immediately after collection, or in the case of a manual update immediately after the modification of the dataset, via an application programming interface (API) so as to facilitate the development of internet, mobile and cloud applications based on such data. Where this is not possible due to technical or financial constraints, public sector bodies should make the documents available in a timeframe that allows their full economic potential to be exploited. Specific measures should be

taken in order to lift relevant technical and financial constraints. Should a licence be used, the timely availability of documents may be a part of the terms of the licence. Where data verification is essential in the light of justified public interest reasons, in particular for public health and safety, dynamic data should be made available immediately after verification. Such essential verification should not affect the frequency of the updates.

(32) In order to get access to the data opened for re-use by this Directive, it would be useful to ensure access to dynamic data through well-designed APIs. An API is a set of functions, procedures, definitions and protocols for machine-to-machine communication and the seamless exchange of data. APIs should be supported by clear technical documentation that is complete and available online. Where possible, open APIs should be used. Union or internationally recognised standard protocols should be applied and international standards for datasets should be used where applicable. APIs can have different levels of complexity and can mean a simple link to a database to retrieve specific datasets, a web interface, or more complex set-ups. There is general value in re-using and sharing data via a suitable use of APIs as this will help developers and start-ups to create new services and products. It is also a crucial ingredient of creating valuable ecosystems around data assets that are often unused. The set-up and use of API needs to be based on several principles: availability, stability, maintenance over lifecycle, uniformity of use and standards, user-friendliness as well as security. For dynamic data, meaning frequently updated data, often in real time, public sector bodies and public undertakings should make this available for re-use immediately after collection by ways of suitable APIs and, where relevant, as a bulk download, save for cases where this would impose a disproportionate effort. Assessment of the proportionality of the effort should take into account the size and operating budget of the public sector body or the public undertaking in question.

(33) The possibilities for re-use can be improved by limiting the need to digitise paper-based documents or to process digital files to make them mutually compatible. Therefore, public sector bodies should make documents available in any pre-existing format or language, through electronic means where possible and appropriate. Public sector bodies should view requests for extracts from existing documents favourably when to grant such a request would involve only a simple operation. Public sector bodies should not, however, be obliged to provide an extract from a document or to modify the format of the requested information where this involves a disproportionate effort. To facilitate re-use, public sector bodies should make their own documents available in a format which, as far as possible and appropriate, is not dependent on the use of specific software. Where possible and appropriate, public sector bodies should take into account the possibilities for the re-use of

documents by and for persons with disabilities by providing the information in an accessible format in accordance with the requirements of Directive (EU) 2016/2102 of the European Parliament and of the Council (17).

(34) To facilitate re-use, public sector bodies should, where possible and appropriate, make documents, including those published on websites, available through an open and machine-readable format and together with their metadata, at the best level of precision and granularity, in a format that ensures interoperability, for example by processing them in a way consistent with the principles governing the compatibility and usability requirements for spatial information under Directive 2007/2/EC.

(35) A document should be considered to be in a machine-readable format if it is in a file format that is structured in such a way that software applications can easily identify, recognise and extract specific data from it. Data encoded in files that are structured in a machine-readable format should be considered to be machine-readable data. A machine-readable format can be open or proprietary. They can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format. Member States should, where possible and appropriate, encourage the use of a Union or internationally recognised open, machine-readable format. The European interoperability framework should be taken into account, where applicable, when designing technical solutions for the re-use of documents.

(36) Charges for the re-use of documents constitute an important market entry barrier for start-ups and SMEs. Documents should therefore be made available for re-use free of charge and, where charges are necessary, they should in principle be limited to the marginal costs. Where public sector bodies carry out a particularly extensive search for requested information or extremely costly modifications of the format of requested information, either voluntarily or as required under national law, marginal costs may cover the costs associated with such activities. In exceptional cases, the necessity of not hindering the normal running of public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks should be taken into consideration. This also applies where a public sector body has made data available as open data but is obliged to generate revenue to cover a substantial part of their costs relating to the performance of other public tasks. The role of public undertakings in a competitive economic environment should also be acknowledged. In such cases, public sector bodies and public undertakings should therefore be able to charge above marginal costs. Those charges should be set

according to objective, transparent and verifiable criteria and the total income from supplying and allowing re-use of documents should not exceed the cost of collection and production, including purchasing from third parties, reproduction, maintenance, storage and dissemination, together with a reasonable return on investment. Where applicable, it should also be possible to include in the eligible cost the costs of anonymisation of personal data and costs of measures taken to protect the confidentiality of data. Member States may require public sector bodies and public undertakings to disclose those costs. The requirement to generate revenue to cover a substantial part of the public sector bodies' costs relating to the performance of their public tasks or the scope of the services of general interest entrusted with public undertakings does not have to be a legal requirement and may stem, for example, from administrative practices in Member States. Such a requirement should be regularly reviewed by the Member States.

(37) The return on investment can be understood as a percentage, in addition to marginal costs, allowing for the recovery of the cost of capital and the inclusion of a real rate of return. As the cost of capital is closely linked to credit institutions' interest rates, which are themselves based on the fixed rate of the European Central Bank (ECB) on main refinancing operations, the reasonable return on investment should not be more than 5 % above the ECB's fixed interest rate.

(38) Libraries, including university libraries, museums and archives should be able to charge above marginal costs in order not to hinder their normal running. In the case of such public sector bodies, the total income from supplying and allowing re-use of documents over the appropriate accounting period should not exceed the cost of collection, production, reproduction, dissemination, preservation and rights clearance, together with a reasonable return on investment. Where applicable, the costs of anonymisation of personal data or of commercially sensitive information should also be included in the eligible cost. For the purpose of libraries, including university libraries, museums and archives, and bearing in mind their particularities, the prices charged by the private sector for the re-use of identical or similar documents could be considered when calculating a reasonable return on investment.

(39) The upper limits for charges set in this Directive are without prejudice to the right of Member States to apply lower charges or no charges at all.

(40) Member States should lay down the criteria for charging above marginal costs. For example, they should be able to lay down such criteria in national rules or to designate an appropriate body or appropriate bodies, other than the public sector body itself, competent to lay down such criteria. That body should be organised in accordance with the constitutional and legal systems of the Member

States. It could be an existing body with budgetary executive powers and under political responsibility.

(41) Ensuring that the conditions for re-use of public sector documents are clear and publicly available is a pre-condition for the development of a Union-wide information market. Therefore, all applicable conditions for the re-use of documents should be made clear to the potential re-users. Member States should encourage the creation of indices accessible on line, where appropriate, of available documents so as to promote and facilitate requests for re-use. Applicants for re-use of documents held by entities other than public undertakings, educational establishments, research performing organisations and research funding organisations should be informed of available means of redress relating to decisions or practices affecting them. This will be particularly important for start-ups and SMEs, which may not be familiar with interactions with public sector bodies from other Member States and corresponding means of redress.

(42) The means of redress should include the possibility of review by an impartial review body. That body could be an already existing national authority, such as the national competition authority, the supervisory authority established in accordance with Regulation (EU) 2016/679, the national access to documents authority or a national judicial authority. That body should be organised in accordance with the constitutional and legal systems of Member States. Recourse to that body should not preempt any means of redress otherwise available to applicants for re-use. It should however be distinct from the Member State mechanism laying down the criteria for charging above marginal costs. The means of redress should include the possibility of review of negative decisions but also of decisions which, although permitting re-use, could still affect applicants on other grounds, in particular by the charging rules applied. The review process should be swift, in accordance with the needs of a rapidly changing market.

(43) Making public all generally available documents held by the public sector - concerning not only the political process but also the legal and administrative process - is a fundamental instrument for extending the right to knowledge, which is a basic principle of democracy. That objective is applicable to institutions at every level, be it local, national or international.

(44) The re-use of documents should not be subject to conditions. However, in some cases justified by a public interest objective, a licence may be issued imposing conditions on the re-use by the licensee dealing with issues such as liability, the protection of personal data, the proper use of documents, guaranteeing non-alteration and the acknowledgement of source. If public sector bodies license documents for re-use, the licence conditions should be objective, proportionate and non-

discriminatory. Standard licences that are available online may also play an important role in this respect. Therefore Member States should provide for the availability of standard licences. Any licences for the re-use of public sector information should, in any event, place as few restrictions on re-use as possible, for example limiting restrictions to an indication of source. Open licences in the form of standardised public licences available online which allow data and content to be freely accessed, used, modified and shared by anyone for any purpose, and which rely on open data formats, should play an important role in this respect. Therefore, Member States should encourage the use of open licences that should eventually become common practice across the Union. Without prejudice to liability requirements laid down in Union or national law where a public sector body or a public undertaking makes documents available for re-use without any other conditions or restrictions, that public sector body or public undertaking may be allowed to waive all liability with regards to the documents made available for re-use.

(45) If the competent authority decides no longer to make available certain documents for re-use, or to cease updating those documents, it should make those decisions publicly known, at the earliest opportunity, by electronic means where possible.

(46) Conditions for re-use should be non-discriminatory for comparable categories of re-use. In that regard, the prohibition of discrimination should not, for example, prevent the exchange of information between public sector bodies free of charge for the exercise of public tasks, whilst other parties are charged for re-use of the same documents. Neither should it prevent the adoption of a differentiated charging policy for commercial and non-commercial re-use.

(47) Member States should in particular ensure that re-use of documents of public undertakings does not lead to market distortion and that fair competition is not undermined.

(48) Public sector bodies should comply with Union and national competition rules when establishing the principles for re-use of documents avoiding as far as possible exclusive agreements between themselves and private partners. However, in order to provide a service of general economic interest, an exclusive right to re-use specific public sector documents may sometimes be necessary. This may be the case if no commercial publisher would publish the information without such an exclusive right. In this regard, it is appropriate to take into account public service contracts that are excluded from the scope of Directive 2014/24/EU pursuant to Article 11 of that Directive and innovation partnerships as referred to in Article 31 of Directive 2014/24/EU.

(49) There are numerous cooperation arrangements between libraries, including university libraries, museums, archives and private partners, which involve digitisation of cultural resources granting

exclusive rights to private partners. Practice has shown that such public-private partnerships can facilitate worthwhile use of cultural collections and at the same time accelerate access to the cultural heritage for members of the public. It is therefore appropriate to take into account current divergences between Member States with regard to digitisation of cultural resources, by a specific set of rules pertaining to agreements on digitisation of such resources. Where an exclusive right relates to digitisation of cultural resources, a certain period of exclusivity might be necessary in order to give the private partner the possibility to recoup its investment. That period should, however, be limited to as short a time as possible in order to comply with the principle that public domain material should stay in the public domain once it is digitised. The period of an exclusive right to digitise cultural resources should in general not exceed 10 years. Any period of exclusivity longer than 10 years should be subject to review, taking into account technological, financial and administrative changes in the environment since the arrangement was entered into. In addition, any public private partnership for the digitisation of cultural resources should grant the partner cultural institution full rights with respect to the post-termination use of digitised cultural resources.

(50) Arrangements between data holders and data re-users which do not expressly grant exclusive rights but which can reasonably be expected to restrict the availability of documents for re-use should be subject to additional public scrutiny. The essential aspects of such arrangements should therefore be published online at least two months before coming into effect, namely two months before the agreed date on which the performance of the obligations of the parties is set to begin. The publication should give interested parties an opportunity to request the re-use of the documents covered by those arrangements and prevent the risk of restricting the range of potential re-users. In any event, the essential aspects of such arrangements in their final form agreed by the parties should also be made public online without undue delay following their conclusion.

(51) This Directive aims to minimise the risk of excessive first-mover advantage that could limit the number of potential re-users of the data. Where contractual arrangements are likely, in addition to a Member State's obligations under this Directive to grant documents, to entail a transfer of that Member State's resources within the meaning of Article 107(1) TFEU, this Directive should be without prejudice to the application of the competition and State aid rules laid down in Articles 101 to 109 TFEU. It follows from the State aid rules laid down in Articles 107, 108 and 109 TFEU that a Member State must check *ex ante* whether State aid may be involved in the relevant contractual arrangement and ensure that it complies with the State aid rules.

(52) This Directive does not affect the protection of individuals with regard to the processing of personal data under Union and national law, particularly Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council (18) and including any supplementing provisions of national law. This means, *inter alia*, that the re-use of personal data is permissible only if the principle of purpose limitation as set out in point (b) of Article 5(1) and Article 6 of Regulation (EU) 2016/679 is met. Anonymous information is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or is no longer identifiable. Rendering information anonymous is a means of reconciling the interests in making public sector information as re-usable as possible with the obligations under data protection law, but it comes at a cost. It is appropriate to consider that cost to be one of the cost items to be considered to be part of the marginal cost of dissemination as referred to in this Directive.

(53) When taking decisions on the scope and conditions for the re-use of public sector documents containing personal data, for example in the health sector, data protection impact assessments may have to be performed in accordance with Article 35 of Regulation (EU) 2016/679.

(54) The intellectual property rights of third parties are not affected by this Directive. For the avoidance of doubt, the term 'intellectual property rights' refers to copyright and related rights only, including *sui generis* forms of protection. This Directive does not apply to documents covered by industrial property rights, such as patents and registered designs and trade marks. The Directive neither affects the existence or ownership of intellectual property rights of public sector bodies, nor does it limit the exercise of these rights in any way beyond the boundaries set by this Directive. The obligations imposed in accordance with this Directive should apply only insofar as they are compatible with international agreements on the protection of intellectual property rights, in particular the Berne Convention for the Protection of Literary and Artistic Works (Berne Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) and the WIPO Copyright Treaty (WCT). Public sector bodies should, however, exercise their copyright in a way that facilitates re-use.

(55) Taking into account Union law and the international obligations of Member States and of the Union, particularly under the Berne Convention and the TRIPS Agreement, documents for which third parties hold intellectual property rights should be excluded from the scope of this Directive. If a third party was the initial owner of the intellectual property rights for a document held by libraries, including university libraries, museums and archives and the term of protection of those rights has

not expired, that document should, for the purpose of this Directive, be considered to be a document for which third parties hold intellectual property rights.

(56) This Directive should be without prejudice to the rights, including economic and moral rights, that employees of public sector bodies may enjoy under national law.

(57) Moreover, where any document is made available for re-use, the public sector body concerned should retain the right to exploit that document.

(58) This Directive is without prejudice to Directive 2014/24/EU.

(59) Tools that help potential re-users to find documents available for re-use and the conditions for re-use can facilitate considerably the cross-border use of public sector documents. Member States should therefore ensure that practical arrangements are in place that help re-users in their search for documents available for re-use. Examples of such practical arrangements are assets lists, which should preferably be accessible online, of main documents (documents that are extensively re-used or that have the potential to be extensively re-used), and portal sites that are linked to decentralised assets lists. Member States should also facilitate the long-term availability for re-use of public sector information, in accordance with the applicable preservation policies.

(60) The Commission should facilitate the cooperation among Member States and support the design, testing, implementation and deployment of interoperable electronic interfaces that enable more efficient and secure public services.

(61) This Directive is without prejudice to Directive 2001/29/EC of the European Parliament and of the Council (19). It provides for conditions within which public sector bodies can exercise their intellectual property rights in the internal information market when allowing re-use of documents. Where public sector bodies are holders of the right provided for in Article 7(1) of Directive 96/9/EC, they should not exercise that right in order to prevent re-use or to restrict the re-use of existing documents beyond the limits provided for in this Directive.

(62) The Commission has supported the development of an online open data maturity report with relevant performance indicators for the re-use of public sector information in all the Member States. A regular update of that report will contribute to the exchange of information between the Member States and the availability of information on policies and practices across the Union.

(63) It is necessary to ensure that the Member States monitor the extent of the re-use of public sector information, the conditions under which it is made available, and the redress practices.

(64) The Commission may assist the Member States in implementing this Directive in a consistent way by issuing and updating existing guidelines, particularly on recommended standard licences, datasets and charging for the re-use of documents, after consulting interested parties.

(65) One of the principal aims of the establishment of the internal market is the creation of conditions conducive to the development of Union-wide services. Libraries, including university libraries, museums and archives hold a significant amount of valuable public sector information resources, in particular since digitisation projects have multiplied the amount of digital public domain material. Those cultural heritage collections and related metadata are a potential base for digital content products and services and have a huge potential for innovative re-use in sectors such as learning and tourism. Other types of cultural establishment, such as orchestras, operas, ballets and theatres, including the archives that are part of those establishments, should remain outside the scope of this Directive because of their specificity as performing arts and the fact that almost all of their material is subject to third-party intellectual property rights.

(66) In order to provide for conditions supporting the re-use of documents which is associated with important socioeconomic benefits having a particular high value for the economy and society, a list of thematic categories of high-value datasets should be set out in an Annex. By way of illustration, and without prejudice to the implementing acts identifying the high-value datasets to which the specific requirements set out in this Directive should apply, taking into account the Commission guidelines on recommended standard licences, datasets and charging for the reuse of documents, the thematic categories could, *inter alia*, cover postcodes, national and local maps (geospatial), energy consumption and satellite images (earth observation and environment), in situ data from instruments and weather forecasts (meteorological), demographic and economic indicators (statistics), business registers and registration identifiers (companies and company ownership), road signs and inland waterways (mobility).

(67) In order to amend the list of thematic categories of high-value datasets by adding further thematic categories, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making (20). In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member

States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(68) An Union-wide list of datasets with a particular potential to generate socioeconomic benefits together with harmonised re-use conditions constitutes an important enabler of cross-border data applications and services. In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission to support the re-use of documents associated with important socioeconomic benefits by adopting a list of specific high-value datasets to which specific requirements of this Directive apply, along with the arrangements for their publication and re-use. Consequently, those specific requirements will not apply prior to the adoption by the Commission of implementing acts. The list should take into account sectoral Union legal acts that regulate the publication of datasets, such as Directives 2007/2/EC and 2010/40/EU, to ensure that datasets are made available under corresponding standards and sets of metadata. The list should be based on the thematic categories set out in this Directive. In preparing the list, the Commission should carry out appropriate consultations, including at expert level. Moreover, when deciding on the inclusion in the list of data held by public undertakings or on their free availability, the effects on competition in the relevant markets should be taken into account. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council (21).

(69) For the purpose of ensuring their maximum impact and to facilitate re-use, the high-value datasets should be made available for re-use with minimal legal restrictions and free of charge. They should also be published via APIs. However, this does not preclude public sector bodies from charging for services that they provide in relation to the high-value datasets in their exercise of public authority, in particular certifying the authenticity or veracity of documents.

(70) Since the objectives of this Directive, namely to facilitate the creation of Union-wide information products and services based on public sector documents, to ensure the effective cross-border use of public sector documents on the one hand by private businesses, particularly by SMEs, for added-value information products and services, and on the other hand by citizens to facilitate the free circulation of information and communication, cannot be sufficiently achieved by the Member States but can rather, by reason of the pan-Union scope of the proposed action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(71) This Directive respects the fundamental rights and observes the principles recognised in particular by the Charter, including the right to privacy, the protection of personal data, the right to property and the integration of persons with disabilities. Nothing in this Directive should be interpreted or implemented in a manner that is inconsistent with the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms.

(72) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council (22) and delivered an opinion on 10 July 2018 (23).

(73) The Commission should carry out an evaluation of this Directive. Pursuant to the Interinstitutional Agreement of 13 April 2016 on Better Law-Making, that evaluation should be based on the five criteria of efficiency, effectiveness, relevance, coherence and value added and should provide the basis for impact assessments of options for further action.

(74) This Directive should be without prejudice to the obligations of the Member States relating to the time-limit for the transposition into national law of the Directives set out in Annex II, Part B,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. In order to promote the use of open data and stimulate innovation in products and services, this Directive establishes a set of minimum rules governing the re-use and the practical arrangements for facilitating the re-use of:

- (a) existing documents held by public sector bodies of the Member States;
- (b) existing documents held by public undertakings that are:
 - (i) active in the areas defined in Directive 2014/25/EU;
 - (ii) acting as public service operators pursuant to Article 2 of Regulation (EC) No 1370/2007;
 - (iii) acting as air carriers fulfilling public service obligations pursuant to Article 16 of Regulation (EC) No 1008/2008; or

(iv) acting as Community shipowners fulfilling public service obligations pursuant to Article 4 of Regulation (EEC) No 3577/92;

(c) research data pursuant to the conditions set out in Article 10.

2. This Directive does not apply to:

(a) documents the supply of which is an activity falling outside the scope of the public task of the public sector bodies concerned as defined by law or by other binding rules in the Member State, or, in the absence of such rules, as defined in accordance with common administrative practice in the Member State in question, provided that the scope of the public tasks is transparent and subject to review;

(b) documents held by public undertakings:

(i) produced outside the scope of the provision of services in the general interest as defined by law or other binding rules in the Member State;

(ii) related to activities directly exposed to competition and therefore, pursuant to Article 34 of Directive 2014/25/EU, not subject to procurement rules;

(c) documents for which third parties hold intellectual property rights;

(d) documents, such as sensitive data, which are excluded from access by virtue of the access regimes in the Member State, including on grounds of:

(i) the protection of national security (namely, State security), defence, or public security;

(ii) statistical confidentiality;

(iii) commercial confidentiality (including business, professional or company secrets);

(e) documents access to which is excluded or restricted on grounds of sensitive critical infrastructure protection related information as defined in point (d) of Article 2 of Directive 2008/114/EC;

(f) documents access to which is restricted by virtue of the access regimes in the Member States, including cases whereby citizens or legal entities have to prove a particular interest to obtain access to documents;

(g) logos, crests and insignia;

(h) documents, access to which is excluded or restricted by virtue of the access regimes on grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law

concerning the protection of individuals with regard to the processing of personal data or as undermining the protection of privacy and the integrity of the individual, in particular in accordance with Union or national law regarding the protection of personal data;

(i) documents held by public service broadcasters and their subsidiaries, and by other bodies or their subsidiaries for the fulfilment of a public service broadcasting remit;

(j) documents held by cultural establishments other than libraries, including university libraries, museums and archives;

(k) documents held by educational establishments of secondary level and below, and, in the case of all other educational establishments, documents other than those referred to in point (c) of paragraph 1;

(l) documents other than those referred to in point (c) of paragraph 1 held by research performing organisations and research funding organisations, including organisations established for the transfer of research results.

3. This Directive builds on, and is without prejudice to, Union and national access regimes.

4. This Directive is without prejudice to Union and national law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC and the corresponding provisions of national law.

5. The obligations imposed in accordance with this Directive shall apply only insofar as they are compatible with the provisions of international agreements on the protection of intellectual property rights, in particular the Berne Convention, the TRIPS Agreement and the WCT.

6. The right for the maker of a database provided for in Article 7(1) of Directive 96/9/EC shall not be exercised by public sector bodies in order to prevent the re-use of documents or to restrict re-use beyond the limits set by this Directive.

7. This Directive governs the re-use of existing documents held by public sector bodies and public undertakings of the Member States, including documents to which Directive 2007/2/EC applies.

Article 2

Definitions

For the purpose of this Directive, the following definitions apply:

(1) 'public sector body' means the State, regional or local authorities, bodies governed by public law or associations formed by one or more such authorities or one or more such bodies governed by public law;

(2) 'bodies governed by public law' means bodies that have all of the following characteristics:

(a) they are established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character;

(b) they have legal personality; and

(c) they are financed, for the most part by the State, regional or local authorities, or by other bodies governed by public law; or are subject to management supervision by those authorities or bodies; or have an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities, or by other bodies governed by public law;

(3) 'public undertaking' means any undertaking active in the areas set out in point (b) of Article 1(1) over which the public sector bodies may exercise directly or indirectly a dominant influence by virtue of their ownership of it, their financial participation therein, or the rules which govern it. A dominant influence on the part of the public sector bodies shall be presumed in any of the following cases in which those bodies, directly or indirectly:

(a) hold the majority of the undertaking's subscribed capital;

(b) control the majority of the votes attaching to shares issued by the undertaking;

(c) can appoint more than half of the undertaking's administrative, management or supervisory body;

(4) 'university' means any public sector body that provides post-secondary-school higher education leading to academic degrees;

(5) 'standard licence' means a set of predefined re-use conditions in a digital format, preferably compatible with standardised public licences available online;

(6) 'document' means:

(a) any content whatever its medium (paper or electronic form or as a sound, visual or audiovisual recording); or

(b) any part of such content;

(7) 'anonymisation' means the process of changing documents into anonymous documents which do not relate to an identified or identifiable natural person, or the process of rendering personal data anonymous in such a manner that the data subject is not or no longer identifiable;

(8) 'dynamic data' means documents in a digital form, subject to frequent or real-time updates, in particular because of their volatility or rapid obsolescence; data generated by sensors are typically considered to be dynamic data;

(9) 'research data' means documents in a digital form, other than scientific publications, which are collected or produced in the course of scientific research activities and are used as evidence in the research process, or are commonly accepted in the research community as necessary to validate research findings and results;

(10) 'high-value datasets' means documents the re-use of which is associated with important benefits for society, the environment and the economy, in particular because of their suitability for the creation of value-added services, applications and new, high-quality and decent jobs, and of the number of potential beneficiaries of the value-added services and applications based on those datasets;

(11) 're-use' means the use by persons or legal entities of documents held by:

(a) public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced, except for the exchange of documents between public sector bodies purely in pursuit of their public tasks; or

(b) public undertakings, for commercial or non-commercial purposes other than for the initial purpose of providing services in the general interest for which the documents were produced, except for the exchange of documents between public undertakings and public sector bodies purely in pursuit of the public tasks of public sector bodies;

(12) 'personal data' means personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679;

(13) 'machine-readable format' means a file format structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure;

(14) 'open format' means a file format that is platform-independent and made available to the public without any restriction that impedes the re-use of documents;

(15) 'formal open standard' means a standard which has been laid down in written form, detailing specifications for the requirements on how to ensure software interoperability;

(16) 'reasonable return on investment' means a percentage of the overall charge, in addition to that needed to recover the eligible costs, not exceeding 5 percentage points above the fixed interest rate of the ECB;

(17) 'third party' means any natural or legal person other than a public sector body or a public undertaking that holds the data.

Article 3

General principle

1. Subject to paragraph 2 of this Article, Member States shall ensure that documents to which this Directive applies in accordance with Article 1 shall be re-usable for commercial or non-commercial purposes in accordance with Chapters III and IV.

2. For documents in which libraries, including university libraries, museums and archives hold intellectual property rights and for documents held by public undertakings, Member States shall ensure that, where the re-use of such documents is allowed, those documents shall be re-usable for commercial or non-commercial purposes in accordance with Chapters III and IV.

CHAPTER II

REQUESTS FOR RE-USE

Article 4

Processing of requests for re-use

1. Public sector bodies shall, through electronic means where possible and appropriate, process requests for re-use and shall make the document available for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant within a reasonable time that is consistent with the time frames laid down for the processing of requests for access to documents.

2. Where no time limits or other rules regulating the timely provision of documents have been established, public sector bodies shall process the request and shall deliver the documents for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant as soon as possible, and in any event within 20 working days of receipt. That time frame may be extended by a further 20 working days in the case of extensive or complex requests. In such cases, the applicant shall be notified

as soon as possible, and in any event within three weeks of the initial request, that more time is needed to process the request and the reasons why.

3. In the event of a negative decision, the public sector bodies shall communicate the grounds for refusal to the applicant on the basis of the relevant provisions of the access regime in that Member State or of the provisions transposing this Directive, in particular points (a) to (h) of Article 1(2) or Article 3. Where a negative decision is based on point (c) of Article 1(2), the public sector body shall include a reference to the natural or legal person who is the rightsholder, where known, or alternatively to the licensor from which the public sector body has obtained the relevant material. Libraries, including university libraries, museums and archives, shall not be required to include such a reference.

4. Any decision on re-use shall contain a reference to the means of redress where the applicant wishes to challenge the decision. The means of redress shall include the possibility of review by an impartial review body with the appropriate expertise, such as the national competition authority, the relevant access to documents authority, the supervisory authority established in accordance with Regulation (EU) 2016/679 or a national judicial authority, whose decisions are binding upon the public sector body concerned.

5. For the purposes of this Article, Member States shall establish practical arrangements to facilitate effective re-use of documents. Those arrangements may in particular include the means to supply adequate information on the rights provided for in this Directive and to offer relevant assistance and guidance.

6. The following entities shall not be required to comply with this Article:

(a) public undertakings;

(b) educational establishments, research performing organisations and research funding organisations.

CHAPTER III

CONDITIONS FOR RE-USE

Article 5

Available formats

1. Without prejudice to Chapter V, public sector bodies and public undertakings shall make their documents available in any pre-existing format or language and, where possible and appropriate, by

electronic means, in formats that are open, machine-readable, accessible, findable and re-usable, together with their metadata. Both the format and the metadata shall, where possible, comply with formal open standards.

2. Member States shall encourage public sector bodies and public undertakings to produce and make available documents falling within the scope of this Directive in accordance with the principle of 'open by design and by default'.

3. Paragraph 1 shall not imply an obligation for public sector bodies to create or adapt documents or provide extracts in order to comply with that paragraph where this would involve disproportionate effort, going beyond a simple operation.

4. Public sector bodies shall not be required to continue the production and storage of a certain type of document with a view to the re-use of such documents by a private or public sector organisation.

5. Public sector bodies shall make dynamic data available for re-use immediately after collection, via suitable APIs and, where relevant, as a bulk download.

6. Where making dynamic data available for re-use immediately after collection, as referred to in paragraph 5, would exceed the financial and technical capacities of the public sector body, thereby imposing a disproportionate effort, those dynamic data shall be made available for re-use within a time frame or with temporary technical restrictions that do not unduly impair the exploitation of their economic and social potential.

7. Paragraphs 1 to 6 shall apply to existing documents held by public undertakings which are available for re-use.

8. The high-value datasets, as listed in accordance with Article 14(1) shall be made available for re-use in machine-readable format, via suitable APIs and, where relevant, as a bulk download.

Article 6

Principles governing charging

1. The re-use of documents shall be free of charge.

However, the recovery of the marginal costs incurred for the reproduction, provision and dissemination of documents as well as for anonymisation of personal data and measures taken to protect commercially confidential information may be allowed.

2. By way of exception, paragraph 1 shall not apply to the following:

(a) public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks;

(b) libraries, including university libraries, museums and archives;

(c) public undertakings.

3. Member States shall publish online a list of the public sector bodies referred to in point (a) of paragraph 2.

4. In the cases referred to in points (a) and (c) of paragraph 2, the total charges shall be calculated in accordance with objective, transparent and verifiable criteria. Such criteria shall be laid down by Member States.

The total income from supplying and allowing the re-use of documents over the appropriate accounting period shall not exceed the cost of their collection, production, reproduction, dissemination and data storage, together with a reasonable return on investment, and - where applicable - the anonymisation of personal data and measures taken to protect commercially confidential information.

Charges shall be calculated in accordance with the applicable accounting principles.

5. Where charges are made by the public sector bodies referred to in point (b) of paragraph 2, the total income from supplying and allowing the re-use of documents over the appropriate accounting period shall not exceed the cost of collection, production, reproduction, dissemination, data storage, preservation and rights clearance and, where applicable, the anonymisation of personal data and measures taken to protect commercially confidential information, together with a reasonable return on investment.

Charges shall be calculated in accordance with the accounting principles applicable to the public sector bodies involved.

6. The re-use of the following shall be free of charge for the user:

(a) subject to Article 14(3), (4) and (5), the high-value datasets, as listed in accordance with paragraph 1 of that Article;

(b) research data referred to in point (c) of Article 1(1).

Article 7

Transparency

1. In the case of standard charges for the re-use of documents, any applicable conditions and the actual amount of those charges, including the calculation basis for such charges, shall be pre-established and published, through electronic means where possible and appropriate.

2. In the case of charges for the re-use other than those referred to in paragraph 1, the factors that are taken into account in the calculation of those charges shall be indicated at the outset. Upon request, the holder of the documents in question shall also indicate the way in which such charges have been calculated in relation to a specific re-use request.

3. Public sector bodies shall ensure that applicants for re-use of documents are informed of available means of redress relating to decisions or practices affecting them.

Article 8

Standard licences

1. The re-use of documents shall not be subject to conditions, unless such conditions are objective, proportionate, non-discriminatory and justified on grounds of a public interest objective.

When re-use is subject to conditions, those conditions shall not unnecessarily restrict possibilities for re-use and shall not be used to restrict competition.

2. In Member States where licences are used, Member States shall ensure that standard licences for the re-use of public sector documents, which can be adapted to meet particular licence applications, are available in digital format and can be processed electronically. Member States shall encourage the use of such standard licences.

Article 9

Practical arrangements

1. Member States shall make practical arrangements facilitating the search for documents available for re-use, such as asset lists of main documents with relevant metadata, accessible where possible and appropriate online and in machine-readable format, and portal sites that are linked to the asset lists. Where possible, Member States shall facilitate the cross-linguistic search for documents, in particular by enabling metadata aggregation at Union level.

Member States shall also encourage public sector bodies to make practical arrangements facilitating the preservation of documents available for re-use.

2. Member States shall, in cooperation with the Commission, continue efforts to simplify access to datasets, in particular by providing a single point of access and by progressively making available

suitable datasets held by public sector bodies with regard to the documents to which this Directive applies, as well as to data held by Union institutions, in formats that are accessible, readily findable and re-usable by electronic means.

Article 10

Research data

1. Member States shall support the availability of research data by adopting national policies and relevant actions aiming at making publicly funded research data openly available ('open access policies'), following the principle of 'open by default' and compatible with the FAIR principles. In that context, concerns relating to intellectual property rights, personal data protection and confidentiality, security and legitimate commercial interests, shall be taken into account in accordance with the principle of 'as open as possible, as closed as necessary'. Those open access policies shall be addressed to research performing organisations and research funding organisations.

2. Without prejudice to point (c) of Article 1(2), research data shall be re-usable for commercial or non-commercial purposes in accordance with Chapters III and IV, insofar as they are publicly funded and researchers, research performing organisations or research funding organisations have already made them publicly available through an institutional or subject-based repository. In that context, legitimate commercial interests, knowledge transfer activities and pre-existing intellectual property rights shall be taken into account.

CHAPTER IV

NON-DISCRIMINATION AND FAIR TRADING

Article 11

Non-discrimination

1. Any applicable conditions for the re-use of documents shall be non-discriminatory for comparable categories of re-use, including for cross-border re-use.

2. If documents are re-used by a public sector body as input for its commercial activities which fall outside the scope of its public tasks, the same charges and other conditions shall apply to the supply of the documents for those activities as apply to other users.

Article 12

Exclusive arrangements

1. The re-use of documents shall be open to all potential actors in the market, even if one or more market actors already exploit added-value products based on those documents. Contracts or other arrangements between the public sector bodies or public undertakings holding the documents and third parties shall not grant exclusive rights.

2. However, where an exclusive right is necessary for the provision of a service in the public interest, the validity of the reason for granting such an exclusive right shall be subject to regular review, and shall, in any event, be reviewed every three years. The exclusive arrangements established on or after 16 July 2019 shall be made publicly available online at least two months before they come into effect. The final terms of such arrangements shall be transparent and shall be made publicly available online.

This paragraph shall not apply to digitisation of cultural resources.

3. Notwithstanding paragraph 1, where an exclusive right relates to the digitisation of cultural resources, the period of exclusivity shall in general not exceed 10 years. Where that period exceeds 10 years, its duration shall be subject to review during the 11th year and, if applicable, every seven years thereafter.

The arrangements granting exclusive rights referred to in the first subparagraph shall be transparent and made public.

In the case of an exclusive right referred to in the first subparagraph, the public sector body concerned shall be provided free of charge with a copy of the digitised cultural resources as part of those arrangements. That copy shall be available for re-use at the end of the period of exclusivity.

4. Legal or practical arrangements that, without expressly granting an exclusive right, aim at, or could reasonably be expected to lead to, a restricted availability for the re-use of documents by entities other than the third party participating in the arrangement, shall be made publicly available online at least two months before their coming into effect. The effect of such legal or practical arrangements on the availability of data for re-use shall be subject to regular reviews and shall, in any event, be reviewed every three years. The final terms of such arrangements shall be transparent and made publicly available online.

5. Exclusive arrangements existing on 17 July 2013 that do not qualify for the exceptions set out in paragraphs 2 and 3 and that were entered into by public sector bodies shall be terminated at the end of the contract and in any event not later than on 18 July 2043.

Exclusive arrangements existing on 16 July 2019 that do not qualify for the exceptions set out in paragraphs 2 and 3, and that were entered into by public undertakings, shall be terminated at the end of the contract and in any event not later than on 17 July 2049.

CHAPTER V

HIGH-VALUE DATASETS

Article 13

Thematic categories of high-value datasets

1. In order to provide for conditions to support the re-use of high-value datasets, a list of thematic categories of such datasets is set out in Annex I.
2. The Commission is empowered to adopt delegated acts in accordance with Article 15 in order to amend Annex I by adding new thematic categories of high-value datasets in order to reflect technological and market developments.

Article 14

Specific high-value datasets and arrangements for publication and re-use

1. The Commission shall adopt implementing acts laying down a list of specific high-value datasets belonging to the categories set out in Annex I and held by public sector bodies and public undertakings among the documents to which this Directive applies.

Such specific high-value datasets shall be:

- (a) available free of charge, subject to paragraphs 3, 4 and 5;
- (b) machine readable;
- (c) provided via APIs; and
- (d) provided as a bulk download, where relevant.

Those implementing acts may specify the arrangements for the publication and re-use of high-value datasets. Such arrangements shall be compatible with open standard licences.

The arrangements may include terms applicable to re-use, formats of data and metadata and technical arrangements for dissemination. Investments made by the Member States in open data approaches, such as investments into the development and roll-out of certain standards, shall be taken into account and balanced against the potential benefits from inclusion in the list.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 16(2).

2. The identification of specific high-value datasets pursuant to paragraph 1 shall be based on the assessment of their potential to:

- (a) generate significant socioeconomic or environmental benefits and innovative services;
- (b) benefit a high number of users, in particular SMEs;
- (c) assist in generating revenues; and
- (d) be combined with other datasets.

For the purpose of identifying such specific high-value datasets, the Commission shall carry out appropriate consultations, including at expert level, conduct an impact assessment and ensure complementarity with existing legal acts, such as Directive 2010/40/EU, with respect to the re-use of documents. That impact assessment shall include a cost-benefit analysis and an analysis of whether providing high-value datasets free of charge by public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks would lead to a substantial impact on the budget of such bodies. With regard to high-value datasets held by public undertakings, the impact assessment shall give special consideration to the role of public undertakings in a competitive economic environment.

3. By way of derogation from point (a) of the second subparagraph of paragraph 1, the implementing acts referred to in paragraph 1 shall provide that the availability of high-value datasets free of charge is not to apply to specific high-value datasets held by public undertakings where that would lead to a distortion of competition in the relevant markets.

4. The requirement to make high-value datasets available free of charge pursuant to point (a) of the second subparagraph of paragraph 1 shall not apply to libraries, including university libraries, museums and archives.

5. Where making high-value datasets available free of charge by public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks would lead to a substantial impact on the budget of the bodies involved, Member States may exempt those bodies from the requirement to make those high-value datasets available free of charge for a period of no more than two years following the entry into force of the relevant implementing act adopted in accordance with paragraph 1.

CHAPTER VI

FINAL PROVISIONS

Article 15

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The power to adopt delegated acts referred to in Article 13(2) shall be conferred on the Commission for a period of five years from 16 July 2019. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.
3. The delegation of power referred to in Article 13(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.
5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
6. A delegated act adopted pursuant to Article 13(2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of three months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 16

Committee procedure

1. The Commission shall be assisted by a Committee on open data and the re-use of public sector information. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 17

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 17 July 2021. They shall immediately communicate the text of those measures to the Commission.

When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. They shall also include a statement that references in existing laws, regulations and administrative provisions to the Directive repealed by this Directive shall be construed as references to this Directive. Member States shall determine how such reference is to be made and how that statement is to be formulated.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 18

Commission evaluation

1. No sooner than 17 July 2025, the Commission shall carry out an evaluation of this Directive, and submit a report on the main findings of that evaluation to the European Parliament and to the Council as well as to the European Economic and Social Committee.

Member States shall provide the Commission with the information necessary for the preparation of that report.

2. The evaluation shall, in particular, address the scope and social and economic impact of this Directive, including:

(a) the extent of the increase in re-use of public sector documents to which this Directive applies, especially by SMEs;

(b) the impact of the high-value datasets;

- (c) the effects of the principles applied to charging and the re-use of official texts of a legislative and administrative nature;
- (d) the re-use of documents held by other entities than public sector bodies,
- (e) the availability and the use of APIs;
- (f) the interaction between data protection rules and re-use possibilities;
- (g) further possibilities of improving the proper functioning of the internal market and supporting economic and labour market development.

Article 19

Repeal

Directive 2003/98/EC, as amended by the Directive listed in Annex II, Part A, is repealed with effect from 17 July 2021, without prejudice to the obligations of the Member States relating to the time-limits for the transposition into national law and the dates of application of the Directives set out in Annex II, Part B.

References to the repealed Directive shall be construed as references to this Directive and shall be read in accordance with the correlation table in Annex III.

Article 20

Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

Article 21

Addressees

This Directive is addressed to the Member States.

Done at Brussels, 20 June 2019.

For the European Parliament

The President

A. TAJANI

For the Council

The President

G. CIAMBA

(1) OJ C 62, 15.2.2019, p. 238.

(2) Position of the European Parliament of 4 April 2019 (not yet published in the Official Journal) and Decision of the Council of 6 June 2019.

(3) Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ L 345, 31.12.2003, p. 90).

(4) Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information (OJ L 175, 27.6.2013, p. 1).

(5) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

(6) Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (OJ L 77, 27.3.1996, p. 20).

(7) Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC (OJ L 41, 14.2.2003, p. 26).

(8) Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE) (OJ L 108, 25.4.2007, p. 1).

(9) Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).

(10) Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC (OJ L 94, 28.3.2014, p. 243).

- (11) Regulation (EC) No 1370/2007 of the European Parliament and of the Council of 23 October 2007 on public passenger transport services by rail and by road and repealing Council Regulations (EEC) Nos 1191/69 and 1107/70 (OJ L 315, 3.12.2007, p. 1).
- (12) Regulation (EC) No 1008/2008 of the European Parliament and of the Council of 24 September 2008 on common rules for the operation of air services in the Community (OJ L 293, 31.10.2008, p. 3).
- (13) Council Regulation (EEC) No 3577/92 of 7 December 1992 applying the principle of freedom to provide services to maritime transport within Member States (maritime cabotage) (OJ L 364, 12.12.1992, p. 7).
- (14) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).
- (15) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).
- (16) Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).
- (17) Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies (OJ L 327, 2.12.2016, p. 1).
- (18) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).
- (19) Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ L 167, 22.6.2001, p. 10).
- (20) OJ L 123, 12.5.2016, p. 1.
- (21) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(22) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

(23) OJ C 305, 30.8.2018, p. 7.

ANNEX I

List of thematic categories of high-value datasets, as referred to in Article 13(1)

1. Geospatial
2. Earth observation and environment
3. Meteorological
4. Statistics
5. Companies and company ownership
6. Mobility

Avrupa Birliği - European Declaration on Digital Rights and Principles for the Digital Decade

European Declaration on Digital Rights and Principles for the Digital Decade

The European Parliament, the Council and the Commission solemnly proclaim the following joint Declaration on Digital Rights and Principles for the Digital Decade

Preamble

Whereas:

(1) The European Union (EU) is a 'union of values', as enshrined in Article 2 of the Treaty on European Union, founded on respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. Moreover according to the Charter of fundamental rights of the European Union, the EU is founded on the indivisible, universal values of human dignity, freedom, equality and solidarity. The Charter also reaffirms the rights as they result, in particular, from international obligations common to the Member States.

(2) The digital transformation affects every aspect of people's lives. It offers significant opportunities for a better quality of life, economic growth and sustainability.

(3) The digital transformation also presents challenges for our democratic societies, our economies and for individuals. With the acceleration of the digital transformation, the time has come for the EU to spell out how its values and fundamental rights applicable offline should be applied in the digital environment. The digital transformation should not entail the regression of rights. What is illegal offline, is illegal online. This Declaration is without prejudice to 'offline policies', such as having access to key public services offline.

(4) The Parliament has made several calls for the establishment of ethical principles guiding the EU's approach to the digital transformation, as well as ensuring the full compliance with fundamental rights such as data protection, the right to privacy, non-discrimination and gender equality, and with principles such as consumer protection, technological and net neutrality, trustworthiness and inclusiveness. It has also called for a strengthened protection of users' rights in the digital environment, as well as workers' rights and the right to disconnect (1).

(5) Building on previous initiatives such as the 'Tallinn Declaration on eGovernment' and the 'Berlin Declaration on Digital Society and Value-based Digital Government', the Member States have called, through the 'Lisbon Declaration – Digital Democracy with a Purpose', for a model of digital

transformation that strengthens the human dimension of the digital ecosystem with the Digital Single Market at its core. Member States have called for a model of digital transformation that ensures that technology assists in addressing the need to take climate action and protect the environment.

(6) The EU vision for digital transformation puts people at the centre, empowers individuals and fosters innovative businesses. The Decision on the 'Digital Decade Policy Programme 2030' sets out the concrete digital targets based on four cardinal points (digital skills, digital infrastructures, digitalisation of businesses and of public services). The EU way for the digital transformation of our societies and economy encompasses in particular digital sovereignty in an open manner, respect for fundamental rights, rule of law and democracy, inclusion, accessibility, equality, sustainability, resilience, security, improving quality of life, the availability of services and respect of everyone's rights and aspirations. It should contribute to a dynamic, resource efficient, and fair economy and society in the EU.

(7) This Declaration spells out shared political intentions and commitments, and recalls the most relevant rights in the context of the digital transformation. The Declaration should also guide policy makers when reflecting on their vision of the digital transformation: putting people at the centre of the digital transformation; supporting solidarity and inclusion, through connectivity, digital education, training and skills, fair and just working conditions as well as access to digital public services online; restating the importance of freedom of choice in interactions with algorithms and artificial intelligence systems and in a fair digital environment; fostering participation in the digital public space; increasing safety, security and empowerment in the digital environment, in particular for children and young people, while ensuring privacy and individual control over data; promoting sustainability. The various chapters of this Declaration should form a holistic reference framework and should not be read in isolation.

(8) This Declaration should also serve as a reference point for businesses and other relevant actors when developing and deploying new technologies. Promoting research and innovation is important in this respect. Special attention should also be given to SMEs and start-ups.

(9) The democratic functioning of the digital society and economy should be further strengthened, in full respect of the rule of law, effective remedies and law enforcement. This Declaration does not affect lawful limits on the exercise of rights, in order to reconcile them with the exercise of other rights, or necessary and proportionate restrictions in the public interest.

(10) This Declaration notably builds on primary EU law, in particular the Treaty on European Union, the Treaty on the Functioning of the European Union, the Charter of Fundamental Rights of the

European Union, as well as on secondary law and the case-law of the Court of Justice of the European Union. It also builds on and complements the European Pillar of Social Rights. It has a declaratory nature and, as such, does not affect the content of legal rules or their application.

(11) The EU should promote the Declaration in its relations with other international organisations and third countries, including by reflecting these rights and principles in its trade relations, with the ambition that the principles guide international partners towards a digital transformation that puts people and their universal human rights at the centre throughout the world. The Declaration should notably serve as a reference for activities in the context of international organisations, such as the realisation of the Agenda 2030 for Sustainable Development, as well as the multistakeholder approach to Internet governance.

(12) The promotion and implementation of the Declaration is a shared political commitment and responsibility of the EU and its Member States within their respective competences and in full compliance with EU law. The Commission will regularly report to the Parliament and the Council on the progress made. The Member States and Commission should take into account the digital principles and rights as laid down in this Declaration when cooperating in view of achieving the general objectives as set out in the Decision on the 'Digital Decade Policy Programme 2030'.

Declaration on Digital Rights and Principles for the Digital Decade

We aim to promote a European way for the digital transformation, putting people at the centre, built on European values and EU fundamental rights, reaffirming universal human rights, and benefiting all individuals, businesses, and society as a whole.

We therefore declare:

CHAPTER I

Putting people at the centre of the digital transformation

1. People are at the centre of the digital transformation in the European Union. Technology should serve and benefit all people living in the EU and empower them to pursue their aspirations, in full security and respect for their fundamental rights.

We commit to:

a) strengthening the democratic framework for a digital transformation that benefits everyone and improves the lives of all people living in the EU;

- b) taking necessary measures to ensure that the values of the EU and the rights of individuals as recognised by EU law are respected online as well as offline;
- c) fostering and ensuring responsible and diligent action by all actors, public and private, in the digital environment;
- d) actively promoting this vision of the digital transformation, also in our international relations.

CHAPTER II

Solidarity and inclusion

2. Technology should be used to unite, and not divide, people. The digital transformation should contribute to a fair and inclusive society and economy in the EU.

We commit to:

- a) making sure that the design, development, deployment and use of technological solutions respect fundamental rights, enable their exercise and promote solidarity and inclusion;
- b) a digital transformation that leaves nobody behind. It should benefit everyone, achieve gender balance, and include notably elderly people, people living in rural areas, persons with disabilities, or marginalised, vulnerable or disenfranchised people and those who act on their behalf. It should also promote cultural and linguistic diversity;
- c) developing adequate frameworks so that all market actors benefiting from the digital transformation assume their social responsibilities and make a fair and proportionate contribution to the costs of public goods, services and infrastructures, for the benefit of all people living in the EU.

Connectivity

3. Everyone, everywhere in the EU, should have access to affordable and high-speed digital connectivity.

We commit to:

- a) ensuring access to high-quality connectivity, with available Internet access, for everyone wherever in the EU, including for those with low income;
- b) protecting and promoting a neutral and open Internet where content, services, and applications are not unjustifiably blocked or degraded.

Digital education, training and skills

4. Everyone has the right to education, training and lifelong learning and should be able to acquire all basic and advanced digital skills.

We commit to:

- a) promoting high-quality digital education and training, including with a view to bridging the digital gender divide;
- b) supporting efforts that allow all learners and teachers to acquire and share the necessary digital skills and competences, including media literacy, and critical thinking, to take an active part in the economy, society, and in democratic processes;
- c) promoting and supporting efforts to equip all education and training institutions with digital connectivity, infrastructure and tools;
- d) giving everyone the possibility to adjust to changes brought by the digitalisation of work through up-skilling and re-skilling.

Fair and just working conditions

5. Everyone has the right to fair, just, healthy and safe working conditions and appropriate protection in the digital environment as in the physical work place, regardless of their employment status, modality or duration.

6. Trade unions and employers' organisations play an important role in the digital transformation, particularly in relation to the definition of fair and just working conditions, including with regard to the use of digital tools at work.

We commit to:

- a) ensuring that everyone is able to disconnect and benefit from safeguards for work-life balance in a digital environment;
- b) ensuring that, in the working environment, digital tools do not put workers' physical and mental health at risk in any way;
- c) ensuring respect for workers' fundamental rights in the digital environment, including their right to privacy and the right to associate, right of collective bargaining and action, as well as protection against unlawful and unjustified surveillance;

- d) ensuring that the use of artificial intelligence in the workplace is transparent and follows a risk-based approach and that corresponding prevention measures are taken to maintain a safe and healthy working environment;
- e) ensuring in particular that human oversight is guaranteed in important decisions affecting workers, and that workers are generally informed that they are interacting with artificial intelligence systems.

Digital public services online

7. Everyone should have online access to key public services in the EU. Nobody is to be asked to provide data more often than necessary when accessing and using digital public services.

We commit to:

- a) ensuring that people living in the EU are offered the possibility to use an accessible, voluntary, secure and trusted digital identity that gives access to a broad range of online services;
- b) ensuring wide accessibility and re-use of public sector information;
- c) facilitating and supporting seamless, secure and interoperable access across the EU to digital public services designed to meet people's needs in an effective manner, including and in particular digital health and care services, notably access to electronic health records.

CHAPTER III

Freedom of choice

Interactions with algorithms and artificial intelligence systems

- 8. Artificial intelligence should serve as a tool for people, with the ultimate aim of increasing human well-being.
- 9. Everyone should be empowered to benefit from the advantages of algorithmic and artificial intelligence systems including by making their own, informed choices in the digital environment, while being protected against risks and harm to one's health, safety and fundamental rights.

We commit to:

- a) promoting human-centric, trustworthy and ethical artificial intelligence systems throughout their development, deployment and use, in line with EU values;
- b) ensuring an adequate level of transparency about the use of algorithms and artificial intelligence, and that people are empowered to use them and are informed when interacting with them;

- c) ensuring that algorithmic systems are based on adequate datasets to avoid discrimination and enable human supervision of all outcomes affecting people's safety and fundamental rights;
- d) ensuring that technologies such as artificial intelligence are not used to pre-empt people's choices, for example regarding health, education, employment, and their private life;
- e) providing for safeguards and taking appropriate action, including by promoting trustworthy standards, to ensure that artificial intelligence and digital systems are, at all times, safe and used in full respect for fundamental rights;
- f) taking measures to ensure that research in artificial intelligence respects the highest ethical standards and relevant EU law.

A fair digital environment

10. Everyone should be able to effectively and freely choose which online services to use, based on objective, transparent, easily accessible and reliable information.

11. Everyone should have the possibility to compete fairly and innovate in the digital environment. This should also benefit businesses, including SMEs.

We commit to:

a) ensuring a safe and secure digital environment based on fair competition, where fundamental rights are protected, users rights and consumer protection in the Digital Single Market are ensured, and responsibilities of platforms, especially large players and gatekeepers, are well defined;

b) promoting interoperability, transparency, open technologies and standards as a way to further strengthen trust in technology as well as consumers' ability to make autonomous and informed choices.

CHAPTER IV

Participation in the digital public space

12. Everyone should have access to a trustworthy, diverse and multilingual digital environment. Access to diverse content contributes to a pluralistic public debate and effective participation in democracy in a non-discriminatory manner.

13. Everyone has the right to freedom of expression and information, as well as freedom of assembly and of association in the digital environment.

14. Everyone should be able to access information on who owns or controls the media services they are using.

15. Online platforms, particularly very large online platforms, should support free democratic debate online. Given the role of their services in shaping public opinion and discourse, very large online platforms should mitigate the risks stemming from the functioning and use of their services, including in relation to misinformation and disinformation campaigns, and protect freedom of expression.

We commit to:

a) continuing safeguarding all fundamental rights online, notably the freedom of expression and information, including media freedom and pluralism;

b) supporting the development and best use of digital technologies to stimulate people's engagement and democratic participation;

c) taking proportionate measures to tackle all forms of illegal content, in full respect for fundamental rights, including the right to freedom of expression and information, and without establishing any general monitoring obligations or censorship;

d) creating a digital environment where people are protected against disinformation and information manipulation and other forms of harmful content, including harassment and gender-based violence;

e) supporting effective access to digital content reflecting the cultural and linguistic diversity in the EU;

f) empowering individuals to make freely given, specific choices and limiting the exploitation of vulnerabilities and biases, namely through targeted advertising.

CHAPTER V

Safety, security and empowerment

A protected, safe and secure digital environment

16. Everyone should have access to digital technologies, products and services that are by design safe, secure, and privacy-protective, resulting in a high level of confidentiality, integrity, availability and authenticity of the information processed.

We commit to:

a) taking further measures to promote the traceability of products and make sure only products which are safe and compliant with EU legislation are offered on the Digital Single Market;

b) protecting the interests of people, businesses and public institutions against cybersecurity risks and cybercrime including data breaches and identity theft or manipulation. This includes cybersecurity requirements for connected products placed on the single market;

c) countering and holding accountable those that seek to undermine, within the EU, security online and the integrity of the digital environment or that promote violence and hatred through digital means.

Privacy and individual control over data

17. Everyone has the right to privacy and to the protection of their personal data. The latter right includes the control by individuals on how their personal data are used and with whom they are shared.

18. Everyone has the right to the confidentiality of their communications and the information on their electronic devices, and not to be subjected to unlawful online surveillance, unlawful pervasive tracking or interception measures.

19. Everyone should be able to determine their digital legacy, and decide what happens with their personal accounts and information that concerns them after their death.

We commit to:

a) ensuring that everyone has effective control of their personal and non-personal data in line with EU data protection rules and relevant EU law;

b) ensuring effectively the possibility for individuals to easily move their personal and non-personal data between different digital services in line with portability rights;

c) effectively protecting communications from unauthorised third party access;

d) prohibiting unlawful identification as well as unlawful retention of activity records.

Protection and empowerment of children and young people in the digital environment

20. Children and young people should be empowered to make safe and informed choices and express their creativity in the digital environment.

21. Age-appropriate materials and services should improve experiences, well-being and participation of children and young people in the digital environment.

22. Specific attention should be paid to the right of children and young people to be protected from all crimes, committed via or facilitated through digital technologies.

We commit to:

- a) providing opportunities to all children and young people to acquire the necessary skills and competences, including media literacy and critical thinking, in order to navigate and engage in the digital environment actively, safely and to make informed choices;
- b) promoting positive experiences for children and young people in an age-appropriate and safe digital environment;
- c) protecting all children and young people against harmful and illegal content, exploitation, manipulation and abuse online, and preventing the digital space from being used to commit or facilitate crimes;
- d) protecting all children and young people against illegal tracking, profiling and targeting, in particular for commercial purposes;
- e) involving children and young people in the development of digital policies that concern them.

CHAPTER VI

Sustainability

23. To avoid significant harm to the environment, and to promote a circular economy, digital products and services should be designed, produced, used, repaired, recycled and disposed of in a way that mitigates their negative impact on the environment and on society and avoids premature obsolescence.

24. Everyone should have access to accurate, easy-to-understand information on the environmental impact and energy consumption of digital products and services, their reparability and lifetime, allowing them to make responsible choices.

We commit to:

- a) supporting the development and use of sustainable digital technologies that have minimal negative environmental and social impact;
- b) incentivising sustainable consumer choices and business models, and fostering sustainable and responsible corporate behaviour throughout global value chains of digital products and services, including with a view to combating forced labour;
- c) promoting the development, deployment and active use of innovative digital technologies with a positive impact on the environment and climate, in order to accelerate the green transition;

d) promoting sustainability standards and labels for digital products and services.

(1) 2020/2216(INI); 2020/2018(INL); 2020/2019(INL); 2020/2022(INI); 2020/2012(INL); 2020/2014(INL);
2020/2015 (INI); 2020/2017 (INI); 2019/2186(INI); 2019/2181(INL); 2022/2266 (INI)

ULUSLARARASI DİĞER DÜZENLEMELER

Bölüm İçeriği

- İnsan Hakları Evrensel Beyannamesi
- Medeni ve Siyasal Haklar Sözleşmesi
- OECD - Özel Yaşamın Korunması ve Kişisel Verilerin Sınırlanması Akışına İlişkin Rehber İlkeler
- Birleşmiş Milletler - Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler

İnsan Hakları Evrensel Beyannamesi

Universal Declaration of Human Rights (10.12.1948)

Article 12

No one shall be subjected to arbitrary, interference with his privacy, family,, home or correspondence, nor to attacks, upon his honour and reputation. Everyone has the right to the protection of the, law against such interference or attacks.

İnsan Hakları Evrensel Beyannamesi

6 Nisan 1949 tarih ve 9119 Sayılı Bakanlar Kurulu ile "İnsan Hakları Evrensel Beyannamesi'nin Resmi Gazete ile yayımlanması kararlaştırılmıştır. Anılan Bakanlar Kurulu Kararı 27.05.1949 tarihli 7217 sayılı Resmi Gazete'de yayımlanmıştır.

Birleşmiş Milletler Genel Kurulu;

İnsanlık topluluğunun bütün bireyleriyle kuruluşlarının bu Bildirgeyi her zaman göz önünde tutarak eğitim ve öğretim yoluyla bu hak ve özgürlüklere saygıyı geliştirmeye, giderek artan ulusal ve uluslararası önlemlerle gerek üye devletlerin halkları ve gerekse bu devletlerin yönetimi altındaki ülkeler halkları arasında bu hakların dünyaca etkin olarak tanınmasını ve uygulanmasını sağlamaya çaba göstermeleri amacıyla tüm halklar ve uluslar için ortak ideal ölçüleri belirleyen bu İnsan Hakları Evrensel Bildirgesini ilan eder.

Madde 12

Kimsenin özel yaşamına, ailesine konutuna ya da haberleşmesine keyfi olarak karışılmaz, şeref ve adına saldırılamaz. Herkesin bu gibi karışma ve saldırılara karşı yasa tarafından korunmaya hakkı vardır.

Medeni ve Siyasal Haklar Sözleşmesi

International Covenant on Civil and Political Rights (19.12.1966)

Article 17

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

Medeni ve Siyasal Haklar Sözleşmesi

Türkiye Sözleşme'yi 15 Ağustos 2000 tarihinde imzalamış ve 18.06.2003 tarihli Resmî Gazete'de yayımlanan 4868 sayılı Kanun'la onaylanmıştır.

Madde 17- Mahremiyet Hakkı

- (1) Hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez; onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz.
- (2) Herkes bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahiptir.

**OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data /
Recommendation Of The Council Concerning Guidelines Governing The Protection of Privacy
And Transborder Flows Of Personal Data**

OECD/LEGAL/0188 - Adopted on: 23/09/1980, Amended on: 11/07/2013

**Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and
Transborder Flows of Personal Data**

THE COUNCIL,

HAVING REGARD to Article 5 b) of the Convention on the Organisation for Economic Co operation and Development of 14 December 1960;

HAVING REGARD to the Ministerial Declaration on the Protection of Privacy on Global Networks [Annex 1 to C(98)177]; the Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks [C(2002)131/FINAL], the Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy [C(2007)67], the Declaration for the Future of the Internet Economy (The Seoul Declaration) [C(2008)99], the Recommendation of the Council on Principles for Internet Policy Making [C(2011)154], the Recommendation of the Council on the Protection of Children Online [C(2011)155] and the Recommendation of the Council on Regulatory Policy and Governance [C(2012)37];

RECOGNISING that Member countries have a common interest in promoting and protecting the fundamental values of privacy, individual liberties and the global free flow of information;

RECOGNISING that more extensive and innovative uses of personal data bring greater economic and social benefits, but also increase privacy risks;

RECOGNISING that the continuous flows of personal data across global networks amplify the need for improved interoperability among privacy frameworks as well as strengthened cross-border co-operation among privacy enforcement authorities;

RECOGNISING the importance of risk assessment in the development of policies and safeguards to protect privacy;

RECOGNISING the challenges to the security of personal data in an open, interconnected environment in which personal data is increasingly a valuable asset;

DETERMINED to further advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among them;

On the proposal of the Committee for Information, Computer and Communications Policy:

I. RECOMMENDS that Member countries:

- Demonstrate leadership and commitment to the protection of privacy and free flow of information at the highest levels of government;
- Implement the Guidelines contained in the Annex to this Recommendation, and of which they form an integral part, through processes that include all relevant stakeholders;
- Disseminate this Recommendation throughout the public and private sectors;

II. INVITES non-Members to adhere to this Recommendation and to collaborate with Member countries in its implementation across borders.

III. INSTRUCTS the Committee for Information, Computer and Communication Policy to monitor the implementation of this Recommendation, review that information, and report to the Council within five years of its adoption and thereafter as appropriate.

This Recommendation revises the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58/FINAL].

ANNEX

GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

PART ONE. GENERAL

Definitions

1. For the purposes of these Guidelines:

a) "data controller" means a party who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;

- b)** “personal data” means any information relating to an identified or identifiable individual (data subject);
- c)** “laws protecting privacy” means national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with these Guidelines;
- d)** “privacy enforcement authority” means any public body, as determined by each Member country, that is responsible for enforcing laws protecting privacy, and that has powers to conduct investigations or pursue enforcement proceedings;
- e)** “transborder flows of personal data” means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties.

3. The principles in these Guidelines are complementary and should be read as a whole. They should not be interpreted:

- a)** as preventing the application of different protective measures to different categories of personal data, depending upon their nature and the context in which they are collected, stored, processed or disseminated; or
- b)** in a manner which unduly limits the freedom of expression.

4. Exceptions to these Guidelines, including those relating to national sovereignty, national security and public policy (“ordre public”), should be:

- a)** as few as possible, and
- b)** made known to the public.

5. In the particular case of federal countries the observance of these Guidelines may be affected by the division of powers in the federation.

6. These Guidelines should be regarded as minimum standards which can be supplemented by additional measures for the protection of privacy and individual liberties, which may impact transborder flows of personal data.

PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up to date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) with the consent of the data subject; or
- b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. Individuals should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;
- b) to have communicated to them, data relating to them
 - i. within a reasonable time;

- ii. at a charge, if any, that is not excessive;
 - iii. in a reasonable manner; and
 - iv. in a form that is readily intelligible to them;
- c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

PART THREE. IMPLEMENTING ACCOUNTABILITY

15. A data controller should:

- a) Have in place a privacy management programme that:
- i. gives effect to these Guidelines for all personal data under its control;
 - ii. is tailored to the structure, scale, volume and sensitivity of its operations;
 - iii. provides for appropriate safeguards based on privacy risk assessment;
 - iv. is integrated into its governance structure and establishes internal oversight mechanisms;
 - v. includes plans for responding to inquiries and incidents;
 - vi. is updated in light of ongoing monitoring and periodic assessment;
- b) Be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines; and
- c) Provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects.

PART FOUR. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

16. A data controller remains accountable for personal data under its control without regard to the location of the data.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.

18. Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.

PART FIVE. NATIONAL IMPLEMENTATION

19. In implementing these Guidelines, Member countries should:

a) develop national privacy strategies that reflect a co-ordinated approach across governmental bodies;

b) adopt laws protecting privacy;

c) establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis;

d) encourage and support self regulation, whether in the form of codes of conduct or otherwise;

e) provide for reasonable means for individuals to exercise their rights;

f) provide for adequate sanctions and remedies in case of failures to comply with laws protecting privacy;

g) consider the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures which help to protect privacy;

h) consider the role of actors other than data controllers, in a manner appropriate to their individual role; and

i) ensure that there is no unfair discrimination against data subjects.

PART SIX. INTERNATIONAL CO OPERATION AND INTEROPERABILITY

20. Member countries should take appropriate measures to facilitate cross-border privacy law enforcement co-operation, in particular by enhancing information sharing among privacy enforcement authorities.

21. Member countries should encourage and support the development of international arrangements that promote interoperability among privacy frameworks that give practical effect to these Guidelines.

22. Member countries should encourage the development of internationally comparable metrics to inform the policy making process related to privacy and transborder flows of personal data.

23. Member countries should make public the details of their observance of these Guidelines.

Guidelines for the Regulation of Computerized Personal Data Files

Adopted by General Assembly resolution 45/95 of 14 December 1990

The procedures for implementing regulations concerning computerized personal data files are left to the initiative of each State subject to the following orientations:

A. PRINCIPLES CONCERNING THE MINIMUM GUARANTEES THAT SHOULD BE PROVIDED IN NATIONAL LEGISLATIONS

1. Principle of lawfulness and fairness

Information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the United Nations.

2. Principle of accuracy

Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission and that they are kept up to date regularly or when the information contained in a file is used, as long as they are being processed.

3. Principle of the purpose-specification

The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that:

- (a) All the personal data collected and recorded remain relevant and adequate to the purposes so specified;
- (b) None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified;
- (c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purposes so specified.

4. Principle of interested-person access

Everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, to be informed of the addressees. Provision should be made for a remedy, if need be with the supervisory authority specified in principle 8 below. The cost of any rectification shall be borne by the person responsible for the file. It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence.

5. Principle of non-discrimination

Subject to cases of exceptions restrictively envisaged under principle 6, data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled.

6. Power to make exceptions

Departures from principles 1 to 4 may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, inter alia, the rights and freedoms of others, especially persons being persecuted (humanitarian clause) provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards.

Exceptions to principle 5 relating to the prohibition of discrimination, in addition to being subject to the same safeguards as those prescribed for exceptions to principles I and 4, may be authorized only within the limits prescribed by the International Bill of Human Rights and the other relevant instruments in the field of protection of human rights and the prevention of discrimination.

7. Principle of security

Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses.

8. Supervision and sanctions

The law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This authority shall offer guarantees of impartiality, independence vis-a- vis persons or agencies responsible for

processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies.

9. Transborder data flows

When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands.

10. Field of application

The present principles should be made applicable, in the first instance, to all public and private computerized files as well as, by means of optional extension and subject to appropriate adjustments, to manual files. Special provision, also optional, might be made to extend all or part of the principles to files on legal persons particularly when they contain some information on individuals.

B. APPLICATION OF THE GUIDELINES TO PERSONAL DATA FILES KEPT BY GOVERNMENTAL INTERNATIONAL ORGANIZATIONS

The present guidelines should apply to personal data files kept by governmental international organizations, subject to any adjustments required to take account of any differences that might exist between files for internal purposes such as those that concern personnel management and files for external purposes concerning third parties having relations with the organization.

Each organization should designate the authority statutorily competent to supervise the observance of these guidelines.

Humanitarian clause: a derogation from these principles may be specifically provided for when the purpose of the file is the protection of human rights and fundamental freedoms of the individual concerned or humanitarian assistance.

A similar derogation should be provided in national legislation for governmental international organizations whose headquarters agreement does not preclude the implementation of the said national legislation as well as for non-governmental international organizations to which this law is applicable.

AVRUPA BİRLİĞİ ADALET DİVANİ KARARLARI (GENEL ÇERÇEVE)

Avrupa Birliği Adalet Divanının kişisel verileri ilgilendiren muhtelif içtihadı vardır. Bu bölümde Mahkemenin bu konuda yaptığı derleme kararlar yer almaktadır.³⁶

Protection of personal data

The right to the protection of personal data is a fundamental right compliance with which is an important objective for the European Union.

It is enshrined in the Charter of Fundamental Rights of the European Union ('the Charter') which provides, in Article 8, that:

- '1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.'

That fundamental right is, moreover, closely connected with the right to respect for private and family life enshrined in Article 7 of the Charter.

The right to the protection of personal data is also laid down in Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), which succeeded Article 286 EC in that respect.

As regards secondary legislation, the European Community has, since the mid-1990s, developed a range of instruments to ensure the protection of personal data. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, adopted on the basis of Article 100a EC, is the Union's principal legal instrument in this area. It lays down the general rules on the lawfulness of the processing of such data and the rights of data subjects and provides in particular for the establishment of independent supervisory authorities in Member States.

³⁶ İçeriğin orjinal hali https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf adresinden erişilebilir.

Directive 2002/58/EC subsequently supplemented Directive 95/46/EC by harmonising the provisions of Member States' legislation on the protection of the right to privacy, notably with respect to the processing of personal data in the electronic communications sector. It should be noted that the Union legislature is considering a review of that directive. In that regard, on 10 January 2017, the Commission put forward a proposition to replace that directive by a regulation relating to privacy and electronic communications.

In addition, in the area of freedom, security and justice (ex Articles 30 and 31 TEU), Framework Decision 2008/977/JHA regulates (until May 2018) the protection of personal data in the areas of judicial cooperation in criminal matters and police cooperation.

In 2016, the European Union reformed the overall legal framework in this area. To that end, it adopted Regulation (EU) 2016/679 on data protection, which repeals Directive 95/46/EC and has been applicable from 25 May 2018, and Directive (EU) 2016/680 on the protection of such data in criminal matters, which repeals Framework Decision 2008/977/JHA and was required to be transposed by Member States by 6 May 2018.

Last, in the context of the processing of personal data by the EU institutions and bodies, Regulation (EC) No 45/2001 ensured, first of all, the protection of such data. In particular, the regulation enabled the European Data Protection Supervisor to be established in 2004. In 2018, the European Union adopted a new legal framework in this area, in particular through the adoption of Regulation (EU) 2018/1725, which repeals Regulation (EC) No 45/2001 and Decision No 1247/2002/EC 10 and is applicable from 11 December 2018. In the interest of a coherent approach to personal data protection throughout the Union, that new regulation aims to align as far as possible the rules in this area with the regime established by Regulation (EU) 2016/679.

The right to the protection of personal data recognised by the Charter of Fundamental Rights of the European Union

Compatibility of secondary EU law with the right to the protection of personal data

Volker und Markus Schecke and Eifert (C-92/09 and C-93/09, EU:C:2010:662) - Judgment of 9 November 2010 (Grand Chamber)

In this case, the main proceedings were brought by agricultural operators against the Land of Hesse, and concerned the publication on the website of the Bundesanstalt für Landwirtschaft und Ernährung (German Federal Office for Agriculture and Food) of personal data relating to them as beneficiaries

of funds from the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD). The agricultural operators objected to such publication, claiming, in particular, that it was not justified by an overriding public interest. The Land of Hesse contended that the publication of the data arose from Regulations (EC) No 1290/2005 and No 259/2008, which governed the financing of the common agricultural policy and required the publication of information on natural persons in receipt of aid from the EAGF and EAFRD.

In that context, the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany) referred a number of questions to the Court concerning the validity of certain provisions of Regulation (EC) No 1290/2005 and that of Regulation (EC) No 259/2008, which required such information to be made available to the public, in particular through websites operated by the national offices.

The Court stated, with regard to the relationship between the right to the protection of personal data recognised by the Charter and the obligation of transparency in relation to European funds, that publication on a website of data naming the beneficiaries of the funds and indicating the amounts received by them constitutes, because the site is freely accessible to third parties, an interference with the right of the beneficiaries concerned to respect for their private life in general and to the protection of their personal data in particular (paragraphs 56-64).

In order to be justified, such interference must be provided for by law, respect the essence of those rights and, pursuant to the principle of proportionality, be necessary and genuinely meet objectives of general interest recognised by the European Union, whilst derogations from and limitations on those rights must apply only in so far as is strictly necessary (paragraph 65). In this context, the Court held that, whilst in a democratic society taxpayers have a right to be kept informed of the use of public funds, the Council and the Commission were nevertheless required to strike a proper balance between the various interests involved, and it was therefore necessary, before adopting the contested provisions, to ascertain whether publication of the data via a single website in a Member State went beyond what was necessary for achieving the legitimate aims pursued (paragraphs 77, 79, 85, 86).

Thus, the Court declared certain provisions of Regulation (EC) No 1290/2005, and Regulation (EC) No 259/2008 in its entirety, to be invalid to the extent to which, with regard to natural persons who are beneficiaries of EAGF and EAFRD aid, those provisions impose an obligation to publish personal data relating to each beneficiary without drawing a distinction based on relevant criteria such as the periods during which those persons received such aid, the frequency of such aid or the nature and amount thereof (paragraph 92, operative part 1). However, the Court did not call in question the

effects of the publication of the lists of beneficiaries of such aid by the national authorities during the period prior to the date on which judgment was delivered (paragraph 94, operative part 2).

Schwarz (C-291/12, EU:C:2013:670) - Judgment of 17 October 2013

Mr Schwarz had applied to the City of Bochum (Germany) for a passport, but had refused at that time to have his fingerprints taken. After Bochum had rejected his application, Mr Schwarz brought an action before the Verwaltungsgericht Gelsenkirchen (Administrative Court, Gelsenkirchen, Germany) in which he requested that the municipality be ordered to issue him with a passport without taking his fingerprints. In the proceedings before that court, Mr Schwarz disputed the validity of Regulation (EC) No 2252/2004 which created the obligation to take the fingerprints of persons applying for passports, claiming, *inter alia*, that the regulation infringed the right to the protection of personal data and the right to respect for private life.

In that context, the Verwaltungsgericht Gelsenkirchen made a reference to the Court for a preliminary ruling in order to establish whether that regulation is valid, particularly in the light of the Charter, in so far as it obliges any person applying for a passport to provide fingerprints and provides for those fingerprints to be stored in that passport.

The Court replied in the affirmative, ruling that, although the taking and storing of fingerprints by the national authorities which is governed by Article 1(2) of Regulation (EC) No 2252/2004 constitutes an infringement of the rights to respect for private life and the protection of personal data, that infringement is justified by the aim of protecting against any fraudulent use of passports.

First of all, such a limitation, provided for by law, pursues an objective of general interest recognised by the Union, in so far as it is designed to prevent, *inter alia*, illegal entry into the European Union (paragraphs 35 to 38). Next, the taking and storing of fingerprints is appropriate for attaining that objective. Although the use of fingerprints as a means of ascertaining identity is not wholly reliable, it significantly reduces the likelihood of unauthorised persons being accepted. Moreover, a mismatch between the fingerprints of the holder of a passport and the data in that document does not mean that the person concerned will automatically be refused entry to the European Union but will simply result in a more detailed check in order definitively to establish that person's identity (paragraphs 42-45).

Last, as regards whether such processing is necessary, the Court was not made aware of any measures that are sufficiently effective but less of a threat to the rights recognised by Articles 7 and 8 of the Charter than the measures deriving from the method based on the use of fingerprints (paragraph 53). Article 1(2) of Regulation (EC) No 2252/2004 does not require the processing of any fingerprints taken

to go beyond what is necessary to achieve the aim pursued. The regulation explicitly states that fingerprints may be used only for verifying the authenticity of a passport and the identity of its holder. Furthermore, Article 1(2) of the regulation ensures protection against the risk of data including fingerprints being read by unauthorised persons and does not provide for the storage of fingerprints except within the passport itself, which belongs to the holder alone (paragraphs 54-57, 60, 63).

Digital Rights Ireland and Seitlinger and Others (Joined Cases C-293/12 and C-594/12, EU:C:2014:238) - Judgment of 8 April 2014 (Grand Chamber)

This judgment has its origin in requests, made in national proceedings before the courts of Ireland and Austria, for a determination of the validity of Directive 2006/24/EC on the retention of data by reference to the fundamental rights to respect for private life and the protection of personal data. In Case C-293/12, proceedings were brought before the High Court (Ireland) by Digital Rights, a company, against the Irish authorities regarding the legality of national measures concerning the retention of data relating to electronic communications. In Case C-594/12, a number of constitutional cases came before the Verfassungsgerichtshof (Constitutional Court, Austria), in which annulment was sought of national legislation transposing Directive 2006/24/EC into Austrian law.

By their requests for a preliminary ruling, the Irish and Austrian courts referred questions to the Court concerning the validity of Directive 2006/24/EC in the light of Articles 7, 8 and 11 of the Charter. More specifically, the referring courts asked the Court whether the obligation which that directive places on providers of publicly available electronic communications or public communications networks to retain, for a certain period, data relating to a person's private life and to his communications and to allow the competent national authorities to access those data entailed an unjustified interference with those fundamental rights. The types of data concerned include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.

The Court, first of all, held that, by imposing such obligations on those providers, Directive 2006/24/EC constituted a particularly serious interference with the fundamental rights to respect for private life and the protection of personal data, guaranteed by Articles 7 and 8 of the Charter. In that context, the Court found that that interference may be justified where it pursues an objective of general interest, such as the fight against organised crime. The Court stated in that regard, in the first place, that the retention of data required by the directive was not such as to adversely affect the essence of the fundamental rights to respect for privacy and the protection of personal data, in so far as it did not permit the acquisition of knowledge of the content of the electronic communications as such and provided that providers of services or of networks must respect certain principles of data protection and data security. In the second place, the Court observed that the retention of data for possible transmission to the competent national authorities genuinely satisfied an objective of general interest, namely the fight against serious crime and, ultimately, public security (paragraphs 38-44).

However, the Court found that, by adopting the directive on data retention, the EU legislature had exceeded the limits imposed by compliance with the principle of proportionality. Accordingly, it declared the directive invalid, on the ground that the wide-ranging and particularly serious interference with fundamental rights that it entailed was not sufficiently circumscribed to ensure that that interference was limited to what was strictly necessary (paragraph 65). Directive 2006/24/EC covered, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting serious crime (paragraphs 57-59). The directive also failed to lay down any objective criterion by which to ensure that the competent national authorities would have access to the data and be able to use them for the sole purpose of preventing, investigating and prosecuting offences capable of being considered to be sufficiently serious to justify such an interference, or the substantive and procedural conditions relating to such access or such use (paragraphs 60-62). Finally, so far as the data retention period was concerned, the directive required that data be retained for a period of at least six months, without any distinction being made between the categories of data according to the persons concerned or on the basis of the possible usefulness of the data for the purposes of the objective pursued (paragraphs 63, 64).

Furthermore, as regards the requirements arising under Article 8(3) of the Charter, the Court held that Directive 2006/24/EC did not provide for sufficient safeguards to ensure effective protection of the data against the risk of abuse and against any unlawful access to and use of the data, nor did it require that the data be retained within the European Union.

Consequently, the directive did not fully ensure control by an independent authority of compliance with the requirements of protection and security, as explicitly required by the Charter (paragraphs 66-68).

Respect for the right to the protection of personal data in the implementation of EU law

Tele2 Sverige (Joined Cases C-203/15 and C-698/15, EU:C:2016:970) - Judgment of 21 December 2016 (Grand Chamber)

Following the judgment in *Digital Rights Ireland and Seitlinger and Others* in which Directive 2006/24/EC was declared invalid (see above), two cases were brought before the Court concerning the general obligation imposed, in Sweden and in the United Kingdom, on providers of electronic communications services to retain the data relating to such communications, retention of which was required by the invalid directive.

On the day following delivery of the judgment in *Digital Rights Ireland and Seitlinger and Others*, the telecommunications company Tele2 Sverige informed the Swedish Post and Telecom Authority that it had decided that it would no longer retain data and that it intended to erase data previously recorded (Case C-203/15). Swedish law required the providers of electronic communications services to retain, systematically and continuously, and with no exceptions, all the traffic and location data of all their subscribers and registered users, with respect to all means of electronic communication. In Case C-698/15, three individuals brought actions challenging the United Kingdom rules on the retention of data which enabled the Secretary of State for the Home Department to require public telecommunications operators to retain all the data relating to communications for a maximum period of 12 months, although retention of the content of those communications was excluded.

In requests for a preliminary ruling from the *Kammarrätten i Stockholm* (Administrative Court of Appeal, Stockholm, Sweden) and the Court of Appeal (England and Wales) (Civil Division) (United Kingdom), the Court was asked to rule on the interpretation of Article 15(1) of Directive 2002/58/EC (the 'Privacy and Electronic Communications' directive), which enables the Member States to introduce certain exceptions to the obligation laid down in that directive to ensure the confidentiality of electronic communications and related traffic data.

In its judgment, the Court first of all held that Article 15(1) of Directive 2002/58/EC, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, precludes national legislation such as the Swedish legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating

to all means of electronic communication. According to the Court, such legislation exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1), read in the light of the aforementioned provisions of the Charter (paragraphs 99-105, 107, 112, operative part 1).

The same article, read in the light of the same provisions of the Charter, also precludes national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union (paragraphs 118-122, 125, operative part 2).

The Court, however, considered that Article 15(1) of Directive 2002/58/EC does not preclude legislation which permits the targeted retention of such data, as a preventive measure, for the purpose of fighting serious crime, provided that that retention is limited to what is strictly necessary with respect to the categories of data affected, the means of communication affected, the persons concerned and the retention period adopted. In order to satisfy those requirements, that national legislation must, first, lay down clear and precise rules ensuring the effective protection of data against the risk of misuse. It must, in particular, indicate the circumstances and conditions under which a data retention measure may be adopted as a preventive measure, thereby ensuring that such a measure is limited to what is strictly necessary. Second, as regards the substantive conditions which must be satisfied by national legislation, if it is to be ensured that data retention is limited to what is strictly necessary, the retention of data must continue to meet objective criteria that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and thus the public affected. As regards the setting of limits on such a measure, the national legislation must be based on objective evidence which makes it possible to identify a public whose data are likely to reveal a link, at least an indirect one, with serious criminal offences, to contribute in one way or another to fighting serious crime or to prevent a serious risk to public security (paragraphs 108-111).

The processing of personal data within the meaning of Directive 95/46/EC

Personal data-processing operations excluded from the scope of Directive 95/46/EC

Parliament v Council (C-317/04 and C-318/04, EU:C:2006:346) - Judgment of 30 May 2006 (Grand Chamber)

Following the terrorist attacks of 11 September 2001, the United States had passed legislation providing that air carriers operating flights to or from the United States or across United States territory had to provide the United States authorities with electronic access to the data contained in their reservation and departure control systems, known as Passenger Name Records (PNR).

The Commission considered that those provisions could come into conflict with European legislation and with that of the Member States on data protection and entered into negotiations with the United States authorities. Following those negotiations the Commission adopted, on 14 May 2004, Decision 2004/535/EC finding that the United States Bureau of Customs and Border Protection (CBP) ensured an adequate level of protection for PNR data transferred from the Community ('the decision on adequacy'). Next, on 17 May 2004, the Council adopted Decision 2004/496/EC approving the conclusion of an agreement between the European Community and the United States on the processing and transfer of PNR data to the CBP by air carriers located within the territory of the Member States of the European Community.

The European Parliament applied to the Court for annulment of those two decisions, contending, in particular, that adoption of the decision on adequacy had been *ultra vires*, that Article 95 EC (now Article 114 TFEU) did not constitute an appropriate legal basis for the decision approving the conclusion of the agreement and, in both cases, that fundamental rights had been infringed.

As regards the decision on adequacy, the Court examined, first of all, whether the Commission could validly adopt its decision on the basis of Directive 95/46/EC. In that context, it noted that it was apparent from the decision on adequacy that the transfer of PNR data to the CBP constituted processing operations concerning public security and the activities of the State in areas of criminal law. According to the Court, although PNR data were initially collected by airlines in the course of an activity which came within the scope of EU law, namely sale of an aeroplane ticket which provided entitlement to a supply of services, the data processing which was taken into account in the decision on adequacy was quite different in nature. That decision concerned not data processing necessary for a supply of services, but data processing regarded as necessary for safeguarding public security and for law-enforcement purposes (paragraphs 56, 57).

In that respect, the Court noted that the fact that the PNR data had been collected by private operators for commercial purposes, and that it was they who arranged for transfer of the data to a third country, did not prevent that transfer from being regarded as data processing that was excluded from the scope of the directive. The transfer fell within a framework established by the public authorities that related to public security. Consequently, the Court concluded that the decision on adequacy did not fall

within the scope of the directive because it concerned processing of personal data that was excluded from it. The Court therefore annulled the decision on adequacy (paragraphs 58, 59).

As regards the Council decision, the Court found that Article 95 EC, read in conjunction with Article 25 of Directive 95/46/EC, could not justify Community competence to conclude the agreement with the United States that was at issue. That agreement related to the same transfer of data as the decision on adequacy and therefore to data-processing operations which were excluded from the scope of the directive. Consequently, the Court annulled the Council decision approving the conclusion of the agreement (paragraphs 67-69).

Rynes (C-212/13, EU:C:2014:2428) - Judgment of 11 December 2014

In response to repeated attacks, Mr Rynes had installed a surveillance camera on his house. Following a further attack on his house, the recordings made by that camera had made it possible to identify two suspects, who had subsequently been prosecuted before the criminal courts. One of the suspects disputed, before the Czech Office for Personal Data Protection, the legality of the processing of the data recorded by the surveillance camera. The Office found that Mr Rynes had infringed the personal data-protection rules and fined him.

The Nejvyšší správní soud (Supreme Administrative Court, Czech Republic), hearing an appeal by Mr Rynes against a decision of the Městský soud v Praze (Prague City Court) which had confirmed the decision of the Office, asked the Court whether the recording made by Mr Rynes for the purposes of protecting his life, health and property constituted a category of data processing that was not covered by Directive 95/46/EC, on the ground that that recording had been made by a natural person in the course of a purely personal or household activity within the meaning of the second indent of Article 3(2) of that directive.

The Court ruled that the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space, does not amount to the processing of data in the course of a purely personal or household activity (paragraph 35 and operative part).

It noted in that regard that the protection of the fundamental right to private life guaranteed under Article 7 of the Charter requires that derogations and limitations in relation to the protection of personal data apply only in so far as is strictly necessary. Since the provisions of Directive 95/46/EC, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in

particular the right to privacy, must necessarily be interpreted in the light of the fundamental rights set out in the Charter, the exception provided for in the second indent of Article 3(2) of that directive must be narrowly construed (paragraphs 27-29). Furthermore, the actual wording of that provision is such that Directive 95/46/EC does not cover the processing of data where the activity in the course of which that processing is carried out is a 'purely' personal or household activity. To the extent that video surveillance covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely 'personal or household' activity for the purposes of that provision (paragraphs 30, 31, 33).

Concept of 'personal data'

Breyer (C-582/14, EU:C:2016:779) - Judgment of 19 October 201

Mr Breyer had brought an action before the German civil courts for an order prohibiting the Federal Republic of Germany from storing, or arranging for third parties to store, computerised data transmitted at the end of each consultation of websites of the German federal institutions. With a view to preventing attacks and making it possible to prosecute 'pirates', the provider of online media services of the German federal institutions was registering data consisting in a 'dynamic' IP address - an IP address which changes each time there is a new connection to the internet - and the date and time when the website was accessed. Unlike static IP addresses, dynamic IP addresses do not immediately enable a link to be established, through files accessible to the public, between a given computer and the physical connection to the network used by the internet service provider. The registered data would not, in themselves, enable the online media services provider to identify the user. However, the internet service provider did have additional information which, if combined with the IP address, would make it possible for the user to be identified.

In that context, the Bundesgerichtshof (Federal Court of Justice, Germany), before which an appeal on a point of law had been brought, asked the Court whether an IP address which is stored by an online media service provider when his website is accessed constitutes personal data for that service provider.

The Court noted, first of all, that, for information to be treated as 'personal data' within the meaning of Article 2(a) of Directive 95/46/EC, there is no requirement that all the information enabling the identification of the data subject must be in the hands of one person. The fact that the additional information necessary to identify the user of a website is held not by the online media services provider but by that user's internet service provider does not, therefore, appear to preclude dynamic

IP addresses registered by the online media services provider from constituting personal data within the meaning of Article 2(a) of Directive 95/46/EC (paragraphs 43, 44).

Consequently, the Court found that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of Article 2(a) of Directive 95/46/EC, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person (paragraph 49, operative part 1).

Nowak (C-434/16, EU:C:2017:994) - Judgment of 20 December 2017

Mr Nowak, a trainee accountant, had failed the examination set by the Institute of Chartered Accountants of Ireland. He submitted a data access request, under section 4 of Ireland's Data Protection Act, seeking all the personal data relating to him held by the Institute of Chartered Accountants. That institute sent certain documents to Mr Nowak, but refused to send to him his examination script, on the ground that it did not contain personal data relating to him, within the meaning of the data protection legislation.

Since the Data Protection Commissioner had also declined to grant his access request on the same grounds, Mr Nowak turned to the national courts. The Supreme Court (Ireland), hearing the appeal brought by Mr Nowak, asked the Court whether Article 2(a) of Directive 95/46/EC must be interpreted as meaning that, in circumstances such as those at issue in the main proceedings, the written answers submitted by a candidate at a professional examination and any examiner's comments with respect to those answers constitute personal data relating to that candidate, within the meaning of that provision.

In the first place, the Court noted that, for information to be treated as 'personal data' within the meaning of Article 2(a) of Directive 95/46/EC, there is no requirement that all the information enabling the identification of the data subject must be in the hands of one person. Furthermore, in the event that the examiner does not know the identity of the candidate when marking the answers submitted by that candidate in an examination, the body that set the examination, in this case the Institute of Chartered Accountants, does, nevertheless, have available to it the information needed to enable it easily and infallibly to identify that candidate through his identification number, placed on the examination script or its cover sheet, and thereby to ascribe the answers to that candidate.

In the second place, the Court found that the written answers submitted by a candidate at a professional examination constitute information that is linked to him as a person. The content of those

answers reflects the extent of the candidate's knowledge and competence in a given field and, in some cases, his intellect, thought processes, and judgment. In addition, the purpose of collecting those answers is to evaluate the candidate's professional abilities and his suitability to practise the profession concerned. Moreover, the use of that information - one consequence of that use being the candidate's success or failure at the examination concerned - is liable to have an effect on his rights and interests, in that it may determine or influence, for example, the chance of entering the profession aspired to or of obtaining the post sought. It is equally true that the written answers submitted by a candidate at a professional examination constitute information that relates to that candidate by reason of its content, purpose or effect, where the examination is an open-book examination.

In the third place, as regards the comments of an examiner with respect to the candidate's answers, the Court considered that they, no less than the answers submitted by the candidate at the examination, constitute information relating to that candidate, since they reflect the opinion or the assessment of the examiner of the individual performance of the candidate in the examination, particularly of his knowledge and competences in the field concerned. The purpose of those comments is, moreover, precisely to record the examiner's evaluation of the candidate's performance, and those comments are liable to have effects for the candidate.

In the fourth place, the Court ruled that the written answers submitted by a candidate at a professional examination and any comments made by an examiner with respect to those answers are liable to be checked for, in particular, their accuracy and the need for their retention, within the meaning of Article 6(1)(d) and (e) of Directive 95/46/EC, and may be subject to rectification or erasure, under Article 12(b) of the directive. To give a candidate a right of access to those answers and to those comments, under Article 12(a) of that directive, serves the purpose of that directive of guaranteeing the protection of that candidate's right to privacy with regard to the processing of data relating to him, irrespective of whether that candidate does or does not also have such a right of access under the national legislation applicable to the examination procedure. However, the Court pointed out that the rights of access and rectification, under Article 12(a) and (b) of Directive 95/46/EC, do not extend to the examination questions, which do not as such constitute the candidate's personal data.

In the light of these points, the Court concluded that, in circumstances such as those at issue in the main proceedings, the written answers submitted by a candidate at a professional examination and any examiner's comments with respect to those answers constitute personal data, within the meaning of Article 2(a) of Directive 95/46/EC.

Concept of 'processing of personal data'

Lindqvist (C-101/01, EU:C:2003:596) - Judgment of 6 November 2003 (Grand Chamber)

Mrs Lindqvist, a voluntary worker in a parish of the Protestant Church in Sweden, had set up, on her personal computer, internet pages on which she published personal data relating to a number of people working with her on a voluntary basis in the parish. Mrs Lindqvist was fined, on the ground that she had used the personal data by automatic means without giving prior written notice to the Swedish Datainspektion (supervisory authority for the protection of electronically transmitted data), that she had transferred the data to a third country without authorisation and that she had processed sensitive personal data.

In the appeal brought before the Göta hovrätt (Court of Appeal, Sweden) by Mrs Lindqvist against that decision, the national court referred questions to the Court for a preliminary ruling in order, in particular, to ascertain whether Mrs Lindqvist had carried out 'the processing of personal data wholly or partly by automatic means' within the meaning of Directive 95/46/EC.

The Court held that the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by stating their telephone number or information regarding their working conditions and hobbies, constitutes 'the processing of personal data wholly or partly by automatic means' within the meaning of that directive (paragraph 27, operative part 1). Such processing of personal data in the course of charitable or religious activities is not covered by any of the exceptions to the scope of the directive, in so far as it does not fall within the category of activities concerning public security, or the category of a purely personal or household activity, which are outside the scope of the directive (paragraphs 38, 43-48, operative part 2).

Google Spain and Google (C-131/12, EU:C:2014:317) - Judgment of 13 May 2014 (Grand Chamber)

In 2010, a Spanish national had lodged with the Agencia Espanola de Proteccion de Datos (Spanish Data Protection Agency, 'the AEPD') a complaint against La Vanguardia Ediciones SL, the publisher of a daily newspaper with a large circulation in Spain, and against Google Spain and Google. The complainant contended that, when an internet user entered his name in the search engine of the Google group, the list of results would display links to two pages of La Vanguardia's newspaper, from 1998, which contained an announcement of an auction organised following attachment proceedings for the recovery of his debts. By his complaint, the complainant requested, first, that La Vanguardia be required either to remove or alter the pages in question, or to use certain tools made available by search engines in order to protect the data. Second, he requested that Google Spain or

Google be required to remove or conceal the personal data relating to him so that they would disappear from the search results and links to La Vanguardia.

The AEPD had rejected the complaint against La Vanguardia, taking the view that the information in question had been lawfully published by it. However, it had upheld the complaint as regards Google Spain and Google and requested those two companies to take the necessary measures to withdraw the data from their index and to render access to the data impossible in the future. The companies brought two actions before the Audiencia Nacional (National High Court, Spain) for annulment of the AEPD's decision, and the Spanish court referred a series of questions to the Court.

Thus, the Court had occasion to clarify the concept of 'processing of personal data' on the internet in the light of Directive 95/46/EC.

The Court held that the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as processing of personal data when that information contains personal data (operative part 1 of the judgment). The Court also noted that the operations referred to by the directive must be classified as processing where they exclusively concern material that has already been published in that form in the media. A general derogation from the application of the directive in such a case would largely deprive the directive of its effect (paragraphs 29 and 30).

Jehovan todistajat (C-25/17, EU:C:2018:551) - Judgment of 10 July 2018 (Grand Chamber)

The Finnish Data Protection Board adopted a decision prohibiting the Jehovah's Witnesses Community from collecting or processing personal data in the course of door-to-door preaching by its members unless the requirements of Finnish legislation relating to the processing of personal data were observed. The members of the Jehovah's Witnesses Community take notes in the course of their door-to-door preaching concerning visits to persons who are unknown to themselves or to that community. Those data are collected as a memory aid and in order to be retrieved for any subsequent visit without the knowledge or consent of the persons concerned. In that respect, the Jehovah's Witnesses Community has given its members guidelines on the taking of such notes which appear in at least one of its magazines which is dedicated to the activity of preaching.

The Court held that the collection of personal data by members of a religious community in the course of door-to-door preaching and the subsequent processing of those data does not come within the exceptions to the scope of Directive 95/46/EC since it does not constitute either the processing of

personal data for the purpose of activities referred to in Article 3(2), first indent, of that directive or the processing of personal data carried out by a natural person in the course of a purely personal or household activity, within the meaning of Article 3(2), second indent, thereof (paragraph 51, operative part 1).

Buivids (C-345, EU:C:2019:122) - Judgment of 14 February 2019

In this case, the Court examined the interpretation of, first, the scope of Directive 95/46/EC and, second, the concept of ‘processing of personal data solely for journalistic purposes’ in Article 9 of that directive.

This judgment was delivered in the context of a request for a preliminary ruling made by the Supreme Court of Latvia, adopted in proceedings between Mr Buivids (‘the applicant’) and the National Data Protection Agency concerning an action seeking a declaration as to the illegality of a decision of that authority, according to which the applicant infringed national law as regards protection of personal data by publishing a video, filmed by him, on an internet site of the statement which he made in the context of administrative proceedings involving the imposition of a penalty in a station of the Latvian national police. Following the dismissal of his action by two lower courts, the applicant brought an appeal in cassation before the Supreme Court. He invoked, before that court, his right to freedom of expression, claiming that the video in question shows public officials of the Latvian national police - namely public persons in a place accessible to the public - who, on that ground, fall outside the scope of the Personal Data Protection Law.

First of all, as regards the scope of Directive 95/46/EC, the Court stated, first, that the recorded images of the police officers constitute personal data and second, that the video recording which was stored in the memory of the camera used by the applicant constitutes a processing of personal data. The Court thus added that the act of publishing a video recording, which contains personal data, on a video website on which users can watch and share videos, constitutes processing of those data wholly or partly by automatic means. Furthermore, the Court notes that that recording and publication of the video in question do not come within the scope of the exceptions to the scope of Directive 95/46/EC, which concern, in particular, the processing of data for the exercise of an activity which falls outside the scope of that directive and processing in the course of a purely personal or household activity. Therefore, the Court concluded that the recording of a video of police officers in a police station, while a statement is being made, and the publication of that video on a website, on which users can send, watch and share videos, are matters which come within the scope of Directive 95/46/EC (paragraphs 31, 32, 35, 39, 42, 43 and operative part 1).

Second, as regards the concept of ‘processing personal data solely for journalistic purposes’, the Court noted, first, that, by interpreting the notion of ‘journalism’ broadly, the exemptions in Article 9 of Directive 95/46/EC apply to every person engaged in journalism. Thus, the Court held that the fact that the applicant is not a professional journalist does not appear to be capable of excluding the possibility that the recording of the video in question and its transmission may constitute ‘processing of personal data solely for journalistic purposes’. Moreover, the Court stated that the exemptions and derogations in Article 9 of Directive 95/46/EC must be applied only where they are necessary in order to reconcile two fundamental rights, namely the right to privacy and the right to freedom of expression. In that respect, the Court noted that it cannot be ruled out that the recording and publication of the video in question, which took place without the police officers in that video being informed of the recording and its purposes, constitutes an interference with the fundamental right to privacy of those persons. Therefore, the Court held that the recording and publication of the video in question on a video website may constitute a processing of personal data solely for journalistic purposes in so far as it is apparent from that video that the sole object of that recording and publication thereof is the disclosure of information, opinions or ideas to the public, this being a matter which it is for the referring court to determine (paragraphs 51, 52, 55, 63, 67 and operative part 2).

Concept of a 'personal data filing system'

Jehovan todistajat (C-25/17, EU:C:2018:551) - Judgment of 10 July 2018 (Grand Chamber)

In this judgment (see also Section II.3. ‘Concept of “processing of personal data”’), the Court clarified the concept of a ‘filing system’ in Article 2(c) of Directive 95/46/EC.

Thus, after pointing out that that directive applies to the manual processing of personal data only where the data processed form part of a filing system or are intended to form part of a filing system, the Court held that that concept covers a set of personal data collected in the course of door-to-door preaching, consisting of the names and addresses and other information concerning the persons contacted, if those data are structured according to specific criteria which, in practice, enable them to be easily retrieved for subsequent use. In order for such a set of data to come within that concept, it is not necessary that they include data sheets, specific lists or other search methods (paragraph 62, operative part 2).

Concept of a 'controller of the processing of personal data'

Jehovan todistajat (C-25/17, EU:C:2018:551) - Judgment of 10 July 2018 (Grand Chamber)

In this judgment (see also Sections II.3. and II.4. 'Concept of "processing of personal data"' and 'Concept of a "personal data filing system"'), the Court adjudicated on the responsibility of a religious community with regard to the processing of personal data carried out in the context of door-to-door preaching organised, coordinated and encouraged by that community.

Thus, the Court found that the obligation for every person to comply with the rules of EU law on the protection of personal data cannot be regarded as amounting to an interference in the organisational autonomy of religious communities. In that regard, the Court held that Article 2(d) of Directive 95/46/EC, read in the light of Article 10(1) of the Charter, must be interpreted as supporting the finding that a religious community is a controller, jointly with its members who engage in preaching, of the processing of personal data carried out by the latter in the context of door-to-door preaching organised, coordinated and encouraged by that community, without it being necessary that the community has access to those data and without it being necessary to establish that that community has given its members written guidelines or instructions concerning that data processing (paragraphs 74, 75, operative part 3).

Wirtschaftsakademie Schleswig Holstein (C-210/16, EU:C:2018:388) - Judgment of 5 June 2018 (Grand Chamber)

The German data protection authority, in its capacity as supervisory authority within the meaning of Article 28 of Directive 95/46/EC, had ordered a German company, operating in the field of education and offering educational services by means of a fan page hosted on the social networking site Facebook, to deactivate its page. According to that authority, neither the company nor Facebook informed visitors to the fan page that Facebook, by means of cookies, collected personal data concerning them and that the company and Facebook then processed those data.

In that context, the Court clarified the concept of a 'controller of the processing' of personal data. In that respect, it took the view that the administrator of a fan page hosted on Facebook, such as the company at issue in the main proceedings, takes part, by its definition of parameters (depending in particular on its target audience and the objectives of managing and promoting its activities), in the determination of the purposes and means of processing the personal data of the visitors to that fan page. According to the Court, that administrator must therefore be categorised as a controller responsible for such processing within the European Union, jointly with Facebook Ireland (the subsidiary in the European Union of the US company Facebook), within the meaning of Article 2(d) of Directive 95/46/EC (paragraph 39).

Fashion ID (C-40/17, EU:C:2019:629) - Judgment of 29 July 2019

In this judgment, the Court had occasion to clarify the concept of a 'controller of the processing of personal data' as regards the embedding of a social plugin on a website.

In this case, Fashion ID, a German online clothing retailer, had embedded on its website the 'Like' social plugin from the social network Facebook. The act of embedding that plugin appears to have made it possible for Facebook Ireland to obtain the personal data of visitors to the Fashion ID website. That transmission of data appears to occur regardless of whether or not the visitor is aware of such an operation, is a member of the social network Facebook or has clicked on the Facebook 'Like' button.

The Verbraucherzentrale NRW, a German public-service association tasked with safeguarding the interests of consumers, criticises Fashion ID for transmitting to Facebook Ireland personal data belonging to visitors to its website, first, without their consent and, second, in breach of the duties to inform set out in the provisions relating to the protection of personal data. In the context of that dispute, the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany) requested the Court to provide an interpretation of a number of provisions of Directive 95/46/EC.

The Court held, first, that the operator of a website, such as Fashion ID, can be considered to be a controller within the meaning of Article 2(d) of Directive 95/46/EC. That status is, however, limited to the operation or set of operations involving the processing of personal data in respect of which it actually determines the purposes and means, that is to say, the collection and disclosure by transmission of the data at issue. By contrast, the Court states that it seems, at the outset, impossible that Fashion ID determines the purposes and means of subsequent operations involving the processing of personal data carried out by Facebook Ireland following their transmission to the latter, with the result that Fashion ID cannot be considered to be a controller in respect of those operations within the meaning of Article 2(d) (paragraphs 76, 85, operative part 2).

Furthermore, the Court noted that it is necessary that that operator and that provider each pursue a legitimate interest, within the meaning of Article 7(f) of Directive 95/46/EC, through those processing operations in order for those operations to be justified in respect of each of them (paragraph 97, operative part 3).

Lastly, the Court stated that the consent of the data subject, referred to in Article 2(h) and Article 7(a) of Directive 95/46/EC, must be obtained by the operator of a website only with regard to the operations involving the processing of personal data in respect of which that operator determines the purposes and means. In such a situation, the duty to inform laid down in Article 10 of that directive is incumbent also on that operator, but the information that the latter must provide to the data subject need relate only to the operation or set of operations involving the processing of personal data in

respect of which that operator actually determines the purposes and means (paragraph 106, operative part 4).

Conditions for lawful processing of personal data in the light of Article 7 of Directive 95/46/EC

Huber (C-524/06, EU:C:2008:724) - Judgment of 16 December 2008 (Grand Chamber)

The Federal Office for Migration and Refugees (Bundesamt für Migration und Flüchtlinge, Germany) was responsible for maintaining a central register of foreign nationals which contained certain personal data relating to foreign nationals who were resident in Germany for a period of more than three months. The register was used for statistical purposes and in the exercise by the security and police services and by the judicial authorities of their powers in relation to the prosecution and investigation of activities which were criminal or which threatened public security.

Mr Huber, an Austrian national, moved to Germany in 1996 in order to carry on business there as a self-employed insurance agent. He took the view that he had been discriminated against by reason of the processing of the data concerning him contained in the register in question, there being no such database in respect of German nationals, and requested that the data be deleted.

In that context, the Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Higher Administrative Court for the Land North Rhine-Westphalia, Germany), before which proceedings were brought, asked the Court whether the processing of personal data of the kind undertaken in the register in question was compatible with EU law.

The Court noted, first of all, that the right of residence of an EU citizen in a Member State of which he is not a national is not unconditional but may be subject to limitations. Thus, the use of such a register for the purpose of providing support to the authorities responsible for the application of the legislation relating to the right of residence is, in principle, legitimate and, having regard to its nature, compatible with the prohibition of discrimination on grounds of nationality laid down by Article 12(1) EC (now first paragraph of Article 18 TFEU). However, such a register must not contain any information other than what is necessary for that purpose, as provided for by the directive on the protection of personal data (paragraphs 54, 58, 59).

As regards the concept of the necessity of the processing under Article 7(e) of Directive 95/46/EC, the Court noted first of all that what was at issue was a concept which had its own independent meaning in EU law and which had to be interpreted in a manner that fully reflected the objective of Directive 95/46/EC as defined in Article 1(1) thereof. The Court went on to find that a system for processing personal data complies with EU law if it contains only the data which are necessary for the application

by those authorities of that legislation and if its centralised nature enables that legislation to be more effectively applied as regards the right of residence of Union citizens who are not nationals of that Member State.

The storage and processing of personal data containing individualised personal information in such a register for statistical purposes cannot, on any basis, be considered to be necessary within the meaning of Article 7(e) of Directive 95/46/EC (paragraphs 52, 66, 68).

Furthermore, with regard to the question of the use of the data contained in the register for the purposes of the fight against crime, the Court stated, in particular, that that objective involves the prosecution of crimes and offences committed, irrespective of the nationality of their perpetrators. It follows that, as regards a Member State, the situation of its nationals cannot, as regards the objective of fighting crime, be different from that of Union citizens who are not nationals of that Member State and who are resident in its territory. Consequently, a difference in treatment between those nationals and those Union citizens which arises by virtue of the systematic processing of personal data relating only to Union citizens who are not nationals of the Member State concerned for the purposes of fighting crime constitutes discrimination which is prohibited by Article 12(1) EC (paragraphs 78-80).

ASNEF and FECEMD (C-468/10 and C-469/10, EU:C:2011:777) - Judgment of 24 November 2011

The Asociación Nacional de Establecimientos Financieros de Crédito (National Association of Credit Institutions) (ASNEF) and the Federación de Comercio Electrónico y Marketing Directo (Federation of Electronic Commerce and Direct Marketing) (FECEMD) brought administrative proceedings before the Tribunal Supremo (Supreme Court, Spain) challenging several articles of Royal Decree 1720/2007 which had implemented Organic Law 15/1999 transposing Directive 95/46/EC.

In particular, ASNEF and FECEMD submitted that, in order to enable personal data to be processed in the absence of the data subject's consent, Spanish law had added a condition not contained in Directive 95/46/EC, requiring that the data appear in 'public sources', as set out in Article 3(j) of Organic Law 15/1999. They contended that that law and Royal Decree 1720/2007 restricted the scope of Article 7(f) of Directive 95/46/EC, which makes the processing of personal data without the data subject's consent conditional only upon the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed.

In that regard, the Court noted, first of all, that Article 7 of Directive 95/46/EC sets out an exhaustive, restrictive list of cases in which the processing of personal data may be regarded as being lawful in the absence of the data subject's consent. Under Article 5 of the directive, Member States may not,

therefore, introduce principles relating to the lawfulness of the processing of personal data other than those listed in Article 7, or alter, by additional requirements, the scope of the principles provided for in Article 7. Article 5 merely authorises

Member States to specify, within the limits of Chapter II of that directive and, accordingly, Article 7 thereof, the conditions under which the processing of personal data is lawful (paragraphs 30, 32, 33).

In particular, in order to carry out the necessary balancing of the opposing rights and interests, provided for in Article 7(f) of the directive, Member States may establish guidelines. They may take into consideration, too, the fact that the seriousness of the infringement of the data subject's fundamental rights resulting from that processing can vary depending on whether or not the data in question already appear in public sources (paragraphs 44 and 46).

However, the Court considered that, if national rules exclude the possibility of processing certain categories of personal data by definitively prescribing, for those categories, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of an individual's particular circumstances, that is no longer a case of precision within the meaning of Article 5 of Directive 95/46/EC. In consequence, the Court concluded that Article 7(f) of Directive 95/46/EC precludes Member States from excluding, categorically and in general, the possibility of processing certain categories of personal data without allowing the opposing rights and interests at issue to be balanced against each other in a particular case (paragraphs 47, 48).

Breyer (C-582/14, EU:C:2016:779) - Judgment of 19 October 2016

In this judgment (see also Section II.2. 'Concept of "personal data"'), the Court also ruled on the question whether Article 7(f) of Directive 95/46/EC precludes a provision in national law under which an online media services provider may collect and use a user's personal data without his consent only to the extent necessary in order to facilitate, and charge for, the specific use of the telemedium by the user concerned, and under which the purpose of ensuring the general operability of the telemedium cannot justify use of the data beyond the end of the particular use of the telemedium.

The Court held that Article 7(f) of Directive 95/46/EC precluded the legislation in question. Under that provision, personal data may be processed as provided for by that provision if processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. In that instance, the German legislation had excluded, categorically and in general, the possibility of processing certain categories of personal data,

without allowing the opposing rights and interests at issue to be balanced against each other in a particular case. In so doing, it had unlawfully reduced the scope of the principle laid down in Article 7(f) of Directive 95/46/EC by excluding the possibility of balancing the objective of ensuring the general operability of the online media against the interests or fundamental rights and freedoms of those users (paragraphs 62-64, operative part 2).

RTgas satiksme (C-13/16, EU:C:2017:336) - Judgment of 4 May 2017

This case arose in proceedings between the Latvian national police and Rigas satiksme, a trolleybus company in the city of Riga, concerning a request for disclosure of data identifying the perpetrator of an accident. In this case, in a traffic accident, a taxi driver had stopped his vehicle at the side of the road. While a trolleybus of Rigas satiksme was passing alongside the taxi, a passenger sitting in the back seat of the taxi had opened the door, which had scraped against and damaged the trolleybus. In order to issue civil proceedings, Rigas satiksme had, inter alia, asked the national police to disclose data identifying the perpetrator of the accident. The police had refused to disclose the passenger's identity document number and address and the documents relating to the explanations given by those involved in the accident on the ground that documents relating to administrative proceedings leading to penalties could be disclosed only to the parties to that case, and, as regards the identity document number and address, that the law on the protection of personal data prohibited the disclosure of such information concerning private individuals.

In those circumstances, the Augstākās tiesas Administratīvo lietu departaments (Supreme Court, Administrative Division, Latvia) decided to ask the Court whether Article 7(f) of Directive 95/46/EC imposes an obligation to disclose personal data to a third party in order to enable him to bring an action for damages before a civil court for harm caused by the person concerned by the protection of those data, and whether the fact that that person is a minor has a bearing on the interpretation of that provision.

The Court held that Article 7(f) of Directive 95/46/EC must be interpreted as not imposing an obligation to disclose personal data to a third party in order to enable him to bring an action for damages before a civil court for harm caused by the person concerned by the protection of those data. However, that provision would not preclude such disclosure if it were made on the basis of national law, in accordance with the conditions laid down in that provision (paragraphs 27, 34 and operative part).

In that context, the Court noted that, subject to the determination to be carried out in that respect by the national court, it did not appear to be justified, in circumstances such as those at issue in the main

proceedings, to refuse to disclose to an injured party the personal data necessary for bringing an action for damages against the person who caused the harm, or, where appropriate, the persons exercising parental authority, on the ground that the person who caused the damage was a minor (paragraph 33).

Puskar (C-73/16, EU:C:2017:725) - Judgment of 27 September 2017

In the dispute in the main proceedings, Mr Puskar had brought an action before the Najvyšší súd Slovenskej republiky (Supreme Court of the Slovak Republic) for an order requiring the Finančné riaditeľstvo (Finance Directorate), all tax offices under its control and the Kriminálny úrad finančnej spravy (Financial Administration Criminal Office) not to include his name on the list of persons considered by the Finance Directorate to be 'front men', drawn up by the latter in the context of tax collection and the updating of which was carried out by the Finance Directorate and the Financial Administration Criminal Office ('the list at issue'). He also sought to have any reference to him removed from those lists and from the finance authority's IT system.

In those circumstances, the Najvyšší súd referred, inter alia, a question to the Court as to whether the right to respect for private and family life, home and communications, in Article 7, and the right to the protection of personal data, in Article 8 of the Charter, could be interpreted in such a way as not to allow a Member State to create, without the consent of the person concerned, a list of personal data for the purposes of tax administration, so that the fact that personal data were made available to a public authority for the purpose of combating tax fraud in itself constituted a risk.

The Court concluded that Article 7(e) of Directive 95/46/EC does not preclude the processing of personal data by the authorities of a Member State for the purpose of collecting tax and combating tax fraud such as that effected by the drawing-up of a list of persons such as that at issue in the main proceedings, without the consent of the data subjects, provided that, first, those authorities were invested by the national legislation with tasks carried out in the public interest within the meaning of that article, that the drawing-up of that list and the inclusion on it of the names of the data subjects is in fact adequate and necessary for the attainment of the objectives pursued and that there are sufficient indications to assume that the data subjects are rightly included in that list, and, second, that all of the conditions for the lawfulness of that processing of personal data imposed by Directive 95/46/EC are satisfied (paragraph 117, operative part 3).

In that regard, the Court noted that it is for the national court to determine whether the establishment of the list at issue is necessary for the performance of the tasks carried out in the public interest at issue in the main proceedings, taking account, in particular, of the precise purpose of the

establishment of the list at issue, the legal effects to which the persons appearing on it are subject and whether or not that list is of a public nature. In the light of the principle of proportionality, it is, moreover, for the national court to ascertain whether the establishment of the list at issue and the inclusion of the names of the data subjects on it are suitable for achieving the objectives pursued by them and whether there is no other less restrictive means of achieving those objectives (paragraphs 111, 112, 113).

The Court further held that the fact that a person is placed on the list at issue is likely to infringe some of his rights. Indeed, inclusion in that list could harm his reputation and affect his relations with the tax authorities. Likewise, such inclusion could affect the presumption of that person's innocence, set out in Article 48(1) of the Charter, as well as the freedom of legal persons associated with the natural persons included in the list at issue to conduct a business, enshrined in Article 16 of the Charter. Consequently, an infringement of this kind can be proportionate only if there are sufficient grounds to suspect the person concerned of purportedly acting as a company director of the legal persons associated with him and of thus undermining the collection of taxes and the combating of tax fraud (paragraph 114).

Furthermore, the Court found that if there were grounds for limiting, under Article 13 of Directive 95/46/EC, certain of the rights provided for in Articles 6 and 10 to 12 thereof, such as the data subject's right to information, such a limitation should be necessary for the protection of an interest referred to in Article 13(1), such as, inter alia, an important economic and financial interest in the field of taxation, and be based on legislative measures (paragraph 116).

The processing of personal data within the meaning of Directive 2002/58/EC

Ministerio Fiscal (C-207/16, EU:C:2018:788) - Judgment of 2 October 2018 (Grand Chamber)

At issue in the main proceedings was the refusal by a Spanish investigating magistrate to grant a request made in the context of an investigation into the robbery of a wallet and mobile telephone. In particular, the police had asked the investigating magistrate to grant access, over a period of 12 days from the date of the robbery, to data identifying the users of telephone numbers activated with the stolen telephone. The refusal had been based on the reasoning that that the acts giving rise to the criminal investigation did not constitute a 'serious' offence - that is to say, an offence punishable under Spanish law by a term of imprisonment of more than five years - access to identification data being possible only in respect of that category of offences.

After pointing out that the access of public authorities to personal data retained by providers of electronic communications services in connection with a criminal investigation comes within the scope of Directive 2002/58, the Court held that the access of public authorities to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as the surnames, forenames and, if need be, addresses of the owners of the SIM cards, constitutes an interference with the fundamental right to respect for private life and the fundamental right to the protection of personal data enshrined in the Charter, even in the absence of circumstances which would allow that interference to be defined as 'serious', without it being relevant that the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way as a result of that interference. However, the Court made clear that such interference is not sufficiently serious to require that access to be limited, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime. Although Directive 2002/58 contains an exhaustive list of the objectives capable of justifying national legislation governing the access of public authorities to the data concerned and thereby derogating from the principle of confidentiality of electronic communications, it being necessary for such access to correspond, genuinely and strictly, to one of those objectives, the Court observed that as regards the objective of preventing, investigating, detecting and prosecuting criminal offences, the wording of Directive 2002/58 does not limit that objective to the fight against serious crime alone, but refers to 'criminal offences' generally (paragraphs 38, 42, 59 to 63, and operative part).

Against that background, the Court stated that although, in its judgment in *Tele2 Sverige and Watson and Others*, it had held that only the objective of fighting serious crime is capable of justifying the access of public authorities to personal data retained by providers of communications services which, taken as a whole, allow precise conclusions to be drawn concerning the private lives of the persons whose data are concerned, that interpretation was based on the fact that the objective pursued by legislation governing that access must be proportionate to the seriousness of the interference with the fundamental rights in question which that access entails. Thus, having regard to the principle of proportionality, a serious interference can be justified, in this field, only by the objective of fighting crime which must also be defined as 'serious'. By contrast, when the interference is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally (paragraphs 54 to 57).

As regards the case in hand, the Court took the view that access to only the data referred to in the request at issue could not be defined as a 'serious' interference with the fundamental rights of the

persons whose data are concerned, as those data do not allow precise conclusions to be drawn in respect of their private lives. The Court concluded that the interference that access to such data entails is therefore capable of being justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally, without it being necessary that those offences be defined as 'serious' (paragraphs 61, 62).

Transfer of personal data to third countries

Lindqvist (C-101/01, EU:C:2003:596) - Judgment of 6 November 2003 (Grand Chamber)

In this case (see also Section II.3. 'Concept of "processing of personal data"'), the referring court sought, in particular, to establish whether Mrs Lindqvist had carried out a transfer of data to a third country within the meaning of that directive.

The Court held that there is no 'transfer [of data] to a third country' within the meaning of Article 25 of Directive 95/46/EC where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country (paragraph 71, operative part 4).

Given, first, the state of development of the internet at the time when Directive 95/46/EC was drawn up and, second, the absence of criteria applicable to use of the internet in Chapter IV in which Article 25 appears and which is intended to allow the Member States to monitor transfers of personal data to third countries and to prohibit such transfers where those countries do not offer an adequate level of protection, it cannot be presumed that the Community legislature intended the expression 'transfer [of data] to a third country' to cover such loading of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them (paragraphs 63, 64, 68).

Schrems (C-362/14, EU:C:2015:650) - Judgment of 6 October 2015 (Grand Chamber)

Mr Schrems, an Austrian citizen and user of the Facebook social network, had made a complaint to Ireland's Data Protection Commissioner on the ground that Facebook Ireland was transferring the personal data of its users to the United States and retaining those data on servers in the United States, where the data were processed. According to Mr Schrems, United States law and practice did not provide adequate protection against surveillance by the public authorities of data transferred to that country. The Data Protection Commissioner had refused to investigate the complaint on the ground,

in particular, that the Commission had, in Decision 2000/520/EC, found that, in the context of the 'safe harbour' regime, the United States ensured an adequate level of protection for the personal data transferred.

It is against that background that a request was made to the Court by the High Court (Ireland) for interpretation of Article 25(6) of Directive 95/46/EC, under which the Commission may find that a third country ensures a level of protection that is adequate for the data transferred, together with, in essence, a request for determination of the validity of Decision 2000/520/EC, which was adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC.

The Court declared the Commission's decision invalid in its entirety, stating, first of all, that its adoption required a duly reasoned finding by the Commission that the third country concerned does in fact ensure a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order. Since the Commission did not so find in Decision 2000/520/EC, Article 1 of that decision fails to comply with the requirements laid down in Article 25(6) of Directive 95/46/EC, read in the light of the Charter, and is accordingly invalid. Indeed, the 'safe harbour' principles are applicable solely to self-certified United States organisations receiving personal data from the European Union, and United States public authorities are not required to comply with them. Moreover, Decision 2000/520/EC enables interference with the fundamental rights of the persons whose personal data are or could be transferred from the European Union to the United States, without containing any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with those rights and without referring to the existence of effective legal protection against interference of that kind (paragraphs 82, 87-89, 96-98, operative part 2).

In addition, the Court declared Article 3 of Decision 2000/520/EC to be invalid in so far as it denied the national supervisory authorities the powers which they derive from Article 28 of Directive 95/46/EC, where a person puts forward matters that may call into question whether a Commission decision that has found that a third country ensures an adequate level of protection is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals (paragraphs 102-104). The Court concluded that the invalidity of Articles 1 and 3 of Decision 2000/520/EC affected the validity of that decision in its entirety (paragraphs 105, 106).

As regards the impossibility of justifying such interference, the Court, first of all, observed that EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must lay down clear and precise rules governing the scope and application of a measure and

imposing minimum safeguards, so that the persons whose personal data are concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access to and use of those data. The need for such safeguards is all the greater where personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data (paragraph 91).

Furthermore and above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary (paragraph 92). Thus, legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data have been transferred from the European Union without any differentiation, limitation or exception being made in the light of the objective pursued, and without any objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of the subsequent use of those data, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to those data and their use entail (paragraph 93). In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications compromises the essence of the fundamental right to respect for private life. Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter (paragraphs 94, 95).

Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017 (Grand Chamber) (EU:C:2017:592)

On 26 July 2017, the Court delivered its first ruling on the compatibility of a draft international agreement with the Charter of Fundamental Rights of the European Union, and, in particular, with provisions relating to respect for private life and the protection of personal data.

The European Union and Canada negotiated an agreement on the transfer and processing of Passenger Name Record data (PNR Agreement) which was signed in 2014. The Council of the European Union having requested the European Parliament's approval of the agreement, the European Parliament decided to refer the matter to the Court in order to ascertain whether the envisaged agreement was compatible with EU law.

The envisaged agreement permits the systematic and continuous transfer of PNR data of all air passengers to a Canadian authority with a view to those data being used and retained, and possibly transferred subsequently to other authorities and to other third countries, for the purpose of

combating terrorism and serious transnational crime. To that end, the envisaged agreement, amongst other things, provides for a data storage period of five years and lays down particular requirements in relation to PNR data security and integrity, such as immediate masking of sensitive data, whilst also providing for rights of access to and correction and erasure of data, and for the possibility of administrative and judicial redress.

The PNR data covered by the envisaged agreement include, *inter alia*, besides the name(s) of the air passenger(s) and contact information: information necessary to the reservation, such as the dates of intended travel and the travel itinerary, information relating to tickets, groups of persons checked-in under the same reservation numbers, information relating to the means of payment or billing, information concerning baggage and general remarks regarding the passengers.

The ruling given by the Court in the Opinion was that the PNR Agreement could not be concluded in its current form because several of its provisions were incompatible with the fundamental rights recognised by the European Union.

The Court found, in the first place, that both the transfer of PNR data from the European Union to the Canadian competent authority and the framework negotiated by the European Union with Canada of the conditions concerning the retention of those data, their use and their subsequent transfer to other Canadian authorities, Europol, Eurojust, judicial or police authorities of the Member States or indeed to authorities of other third countries constitute interferences with the right guaranteed in Article 7 of the Charter. Those operations also constitute an interference with the fundamental right to the protection of personal data guaranteed in Article 8 of the Charter since they constitute the processing of personal data (paragraphs 125, 126).

Furthermore, the Court emphasised that even if some of the PNR data, taken in isolation, do not appear to be liable to reveal important information about the private life of the persons concerned, the fact remains that, taken as a whole, the data may, *inter alia*, reveal a complete travel itinerary, travel habits, relationships existing between air passengers and the financial situation of air passengers, their dietary habits or state of health, and may even provide sensitive information about those passengers, as defined in Article 2(e) of the envisaged agreement (information that reveals racial or ethnic origin, political opinions, religious beliefs, etc.) (paragraph 128).

In this connection, the Court considered that, although the interferences in question could be justified by the pursuit of an objective of general interest (to ensure public security in the context of the fight against terrorist offences and serious transnational crime), several provisions of the agreement were not limited to what is strictly necessary and did not lay down clear and precise rules.

In particular, the Court pointed out that, having regard to the risk of processing contrary to the principle of non-discrimination, a transfer of sensitive data to Canada requires a precise and particularly solid justification, based on grounds other than the protection of public security against terrorism and serious transnational crime. In this instance, however, there was no such justification. The Court concluded from this that the provisions of the agreement on the transfer of sensitive data to Canada and on the processing and retention of those data were incompatible with fundamental rights (paragraphs 165, 232).

In the second place, the Court found that the continued storage of the PNR data of all air passengers after their departure from Canada, which the envisaged agreement permits, was not limited to what is strictly necessary. As regards air passengers in respect of whom no risk has been identified as regards terrorism or serious transnational crime on their arrival in Canada and up to their departure from that country, there would not appear to be, once they have left, any connection - even a merely indirect connection - between their PNR data and the objective pursued by the envisaged agreement which would justify those data being retained. By contrast, in the case of air passengers in respect of whom there is objective evidence from which it may be inferred that they may present a risk in terms of the fight against terrorism and serious transnational crime even after their departure from Canada, the storage of their PNR data is permissible beyond their stay in Canada, even for a period of five years (paragraphs 205, 207, 209).

In the third place, the Court held that the fundamental right to respect for private life, enshrined in Article 7 of the Charter, means that the person concerned may be certain that his personal data are processed in a correct and lawful manner. In order to carry out the necessary checks, that person must have a right of access to the data relating to him which are being processed.

The Court pointed out in that regard that, in the envisaged agreement, air passengers must be notified of the transfer of their PNR data to the third country concerned and of the use of those data as soon as that information is no longer liable to jeopardise the investigations being carried out by the government authorities referred to in the envisaged agreement. That information is, in fact, necessary to enable the air passengers to exercise their rights to request access to data concerning them and, if appropriate, rectification of those data, and, in accordance with the first paragraph of Article 47 of the Charter, to an effective remedy before a tribunal.

Consequently, in the situations in which there is objective evidence justifying the use of the PNR data in order to combat terrorism and serious transnational crime and necessitating the prior authorisation of a judicial authority or an independent administrative body, it is necessary to notify air passengers

individually. The same is true in the cases in which air passengers' PNR data are disclosed to other government authorities or to individuals. However, that information must be provided only once it is no longer liable to jeopardise the investigations being carried out by the government authorities referred to in the envisaged agreement (paragraphs 219, 220, 223, 224).

Facebook Ireland and Schrems (C-311/18, ECLI:EU:C:2020:559) - Judgment of 16 July 2020 (Grand Chamber)

The General Data Protection Regulation ('the GDPR') provides that the transfer of such data to a third country may, in principle, take place only if the third country in question ensures an adequate level of data protection. According to the GDPR, the Commission may find that a third country ensures, by reason of its domestic law or its international commitments, an adequate level of protection. In the absence of an adequacy decision, such a transfer may take place only if the personal data exporter established in the European Union has provided appropriate safeguards, which may arise, in particular, from standard data protection clauses adopted by the Commission, and if data subjects have enforceable rights and effective legal remedies.

Furthermore, the GDPR details the conditions under which such a transfer may take place in the absence of an adequacy decision or appropriate safeguards.

Maximillian Schrems, an Austrian national residing in Austria, has been a Facebook user since 2008. As in the case of other users residing in the European Union, some or all of Mr Schrems's personal data are transferred by Facebook Ireland to servers belonging to Facebook Inc. that are located in the United States, where they undergo processing. Mr Schrems lodged a complaint with the Irish supervisory authority seeking, in essence, to prohibit those transfers. He claimed that the law and practices in the United States do not offer sufficient protection against access by the public authorities to the data transferred to that country. That complaint was rejected on the ground, *inter alia*, that, in Decision 2000/520, the Commission had found that the United States ensured an adequate level of protection. In a judgment delivered on 6 October 2015, the Court, before which the High Court (Ireland) had referred questions for a preliminary ruling, declared that decision invalid ('the Schrems I judgment') (paragraphs 52, 53).

Following the Schrems I judgment and the subsequent annulment by the referring court of the decision rejecting Mr Schrems's complaint, the Irish supervisory authority asked Mr Schrems to reformulate his complaint in the light of the declaration by the Court that Decision 2000/520 was invalid. In his reformulated complaint, Mr Schrems claims that the United States does not offer sufficient protection of data transferred to that country. He seeks the suspension or prohibition of

future transfers of his personal data from the European Union to the United States, which Facebook Ireland now carries out pursuant to the standard data protection clauses set out in the Annex to Decision 2010/87. Taking the view that the outcome of Mr Schrems's complaint depends, in particular, on the validity of Decision 2010/87, the Irish supervisory authority brought proceedings before the High Court in order for it to refer questions to the Court for a preliminary ruling. After the initiation of those proceedings, the Commission adopted Decision 2016/1250 on the adequacy of the protection provided by the EU-US Privacy Shield (paragraphs 54, 55, 57).

By its request for a preliminary ruling, the referring court asked the Court whether the GDPR applies to transfers of personal data pursuant to the standard data protection clauses in Decision 2010/87, what level of protection is required by the GDPR in connection with such a transfer and what obligations are incumbent on supervisory authorities in those circumstances. The High Court also raised the question of the validity both of Decision 2010/87 and of Decision 2016/1250.

The Court found that examination of Decision 2010/87 in the light of the Charter of Fundamental Rights of the European Union ('the Charter') disclosed nothing to affect the validity of that decision. However, the Court declared Decision 2016/1250 invalid (operative part 4 and 5).

The Court considered, first of all, that EU law, and in particular the GDPR, applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, even if, at the time of that transfer or thereafter, that data may be processed by the authorities of the third country in question for the purposes of public security, defence and State security. The Court added that this type of data processing by the authorities of a third country cannot preclude such a transfer from the scope of the GDPR (paragraphs 86, 88, 89 and operative part 1).

Regarding the level of protection required in respect of such a transfer, the Court held that the requirements laid down for such purposes by the GDPR concerning appropriate safeguards, enforceable rights and effective legal remedies must be interpreted as meaning that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses must be afforded a level of protection essentially equivalent to that guaranteed within the European Union by the GDPR, read in the light of the Charter. In those circumstances, the Court specified that the assessment of that level of protection must take into consideration both the contractual clauses agreed between the data exporter established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that

third country to the data transferred, the relevant aspects of the legal system of that third country (paragraph 105 and operative part 2).

Regarding the supervisory authorities' obligations in connection with such a transfer, the Court held that, unless there is a valid Commission adequacy decision, those competent supervisory authorities are required to suspend or prohibit a transfer of personal data to a third country where they take the view, in the light of all the circumstances of that transfer, that the standard data protection clauses are not or cannot be complied with in that country and that the protection of the data transferred that is required by EU law cannot be ensured by other means, where the data exporter established in the European Union has not itself suspended or put an end to such a transfer (paragraph 121 and operative part 3).

Next, the Court examined the validity of Decision 2010/87. The Court considered that the validity of that decision was not called into question by the mere fact that the standard data protection clauses in that decision do not, given that they are contractual in nature, bind the authorities of the third country to which data may be transferred. However, that validity, the Court added, depends on whether the decision includes effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law and that transfers of personal data pursuant to such clauses are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them. The Court found that Decision 2010/87 establishes such mechanisms. In that regard, the Court pointed out, in particular, that that decision imposes an obligation on a data exporter and the recipient of the data to verify, prior to any transfer, whether that level of protection is respected in the third country concerned and that the decision requires the recipient to inform the data exporter of any inability to comply with the standard data protection clauses, the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract with the former (paragraphs 132, 136, 137, 142, 148 and operative part 4).

Lastly, the Court examined the validity of Decision 2016/1250 in the light of the requirements arising from the GDPR, read in the light of the provisions of the Charter guaranteeing respect for private and family life, personal data protection and the right to effective judicial protection. In that regard, the Court noted that that decision enshrines the position, as did Decision 2000/520, that the requirements of US national security, public interest and law enforcement have primacy, thus condoning interference with the fundamental rights of persons whose data are transferred to that third country. In the view of the Court, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from

the European Union to that third country, which the Commission assessed in Decision 2016/1250, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary. On the basis of the findings made in that decision, the Court pointed out that, in respect of certain surveillance programmes, those provisions do not indicate any limitations on the power they confer to implement those programmes, or the existence of guarantees for potentially targeted non-US persons. The Court added that, although those provisions lay down requirements with which the US authorities must comply when implementing the surveillance programmes in question, the provisions do not grant data subjects actionable rights before the courts against the US authorities (paragraphs 164, 165, 180-182, 184, 185).

As regards the requirement of judicial protection, the Court held that, contrary to the view taken by the Commission in Decision 2016/1250, the Ombudsperson mechanism referred to in that decision does not provide data subjects with any cause of action before a body which offers guarantees substantially equivalent to those required by EU law, such as to ensure both the independence of the Ombudsperson provided for by that mechanism and the existence of rules empowering the Ombudsperson to adopt decisions that are binding on the US intelligence services. On all those grounds, the Court declared Decision 2016/1250 invalid (paragraphs 195-197, 201 and operative part 5).

Protection of personal data on the internet

Right to object to the processing of personal data ('right to be forgotten')

Google Spain and Google (C-131/12, EU:C:2014:317) - Judgment of 13 May 2014 (Grand Chamber)

In this judgment (see also Section II.3. 'Concept of "processing of personal data"'), the Court clarified the scope of the right of access and the right to object to the processing of personal data on the internet, provided for by Directive 95/46/EC.

Thus, when ruling on the question of the extent of the responsibility of the operator of a search engine on the internet, the Court held, in essence, that, in order to comply with the right of access and the right to object guaranteed by Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46/EC, and in so far as the conditions laid down by those provisions are satisfied, that operator is, in certain circumstances, obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages published by third parties and containing information relating to that person. The Court stated that such an obligation may also exist

where that name or the information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful (paragraph 88, operative part 3).

Furthermore, questioned as to whether the directive enables the data subject to ask for links to web pages to be removed from such a list of results because he wishes the information displayed there and relating to him personally to be 'forgotten' after a certain time, the Court noted, first of all, that even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed, in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes or in the light of the time that has elapsed (paragraph 93). Therefore, if it is found, following a request by the data subject, that the inclusion of those links in the list is, at this point in time, incompatible with the directive, the information and links in that list must be erased (paragraph 94). In this context, it is not necessary, in order to find a right of the data subject that the information relating to him personally should no longer be linked to his name by a list of results, that the inclusion of the information in question in the list of results causes prejudice to him (paragraph 96, operative part 4).

Last, the Court made clear that, as the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public by its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question (paragraph 97, operative part 4).

Processing of personal data and intellectual property rights

Promusicae (C-275/06, EU:C:2008:54) - Judgment of 29 January 2008 (Grand Chamber)

Promusicae, a Spanish non-profit-making organisation of producers and publishers of musical and audiovisual recordings, had brought proceedings before the Spanish courts for an order that Telefonica de Espana SAU (a commercial company whose activities include the provision of internet access services) be required to disclose the identities and physical addresses of certain

persons to whom that company provided internet access services and whose IP addresses and the date and time of connection were known. According to Promusicae, those persons were using the peer-to-peer or P2P program (a transparent method of file sharing which is independent, decentralised, and features advanced search and download functions) and providing access in shared files of personal computers to phonograms in which the members of Promusicae held the exploitation rights. It had therefore sought disclosure of that information in order to be able to bring civil proceedings against the persons concerned.

In those circumstances, the Juzgado de lo Mercantil no 5 de Madrid (Commercial Court No 5, Madrid, Spain) referred a question to the Court as to whether EU legislation requires Member States to lay down, in order to ensure effective protection of copyright, an obligation to communicate personal data in the context of civil proceedings.

According to the Court, that request for a preliminary ruling raised the question of the need to reconcile the requirements of the protection of different fundamental rights, namely the right to respect for private life, on the one hand, and the rights to protection of property and to an effective remedy, on the other.

In that respect, the Court concluded that Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, Directive 2004/48/EC on the enforcement of intellectual property rights, and Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) do not require the Member States to lay down, in a situation such as that in the main proceedings, an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings. However, EU law requires that, when transposing those directives, the Member States take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality (paragraph 70 and operative part).

Scarlet Extended (C-70/10, EU:C:2011:771) - Judgment of 24 November 2011

The Societe belge des auteurs, compositeurs et editeurs SCRL (SABAM) had established that internet users using the services of Scarlet Extended SA, an internet service provider ('Scarlet'), were downloading works in SABAM's catalogue from the internet, without authorisation and without paying royalties, by means of peer-to-peer networks. SABAM brought proceedings before the national court and obtained, at first instance, an order requiring Scarlet to bring those copyright infringements to an end by making it impossible for its customers to send or receive in any way electronic files containing a musical work in the SABAM catalogue using peer-to-peer software.

Following an appeal by Scarlet, the cour d'appel de Bruxelles (Court of Appeal, Brussels, Belgium) stayed proceedings in order to ask the Court for a preliminary ruling on whether such an injunction was compatible with EU law.

The Court held that Directives 95/46/EC, 2000/31/EC, 2001/29/EC, 2002/58/EC and 2004/48/EC, read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction made against Scarlet which requires it to install a system for filtering all electronic communications passing via its services, in particular those involving peer-to-peer software, which applies indiscriminately to all its customers, as a preventive measure, exclusively at its own expense, and for an unlimited period, and which is capable of identifying on that provider's network the movement of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold intellectual property rights, with a view to blocking the transfer of files the sharing of which infringes copyright (paragraph 54 and operative part).

According to the Court, such an injunction both infringes the prohibition on imposing a general monitoring obligation on such a provider laid down by Article 15(1) of Directive 2000/31/EC, and fails to comply with the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other (paragraphs 40, 49).

In that context, the Court noted that, first, the injunction requiring installation of the contested filtering system would involve a systematic analysis of all content and the collection and identification of users' IP addresses from which unlawful content on the network is sent. Those addresses are protected personal data because they allow those users to be precisely identified (paragraph 51). Second, that injunction could potentially undermine freedom of information since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications. Indeed, it is not contested that the

reply to the question whether a transmission is lawful also depends on the application of statutory exceptions to copyright which vary from one Member State to another. Moreover, in some Member States certain works fall within the public domain or can be posted online free of charge by the authors concerned (paragraph 52).

Consequently, the Court held that, in granting the injunction requiring Scarlet to install the contested filtering system, the national court concerned would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other (paragraph 53).

Bonnier Audio and Others (C-461/10, EU:C:2012:219) - Judgment of 19 April 2012

The Högsta domstolen (Supreme Court, Sweden) made a reference to the Court of Justice for a preliminary ruling on the interpretation of Directives 2002/58/EC and 2004/48/EC in proceedings between Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB and Storyside AB ('the applicants in the main proceedings') and Perfect Communication Sweden AB ('ePhone') concerning the latter's opposition to an injunction obtained by the applicants in the main proceedings ordering the disclosure of data.

In this case, the applicants in the main proceedings were publishing companies holding, inter alia, exclusive rights to the reproduction, publishing and distribution to the public of 27 works in the form of audio books. They claimed that their exclusive rights had been infringed by the public distribution of these 27 works, without their consent, by means of an FTP ('file transfer protocol') server which allowed file sharing and data transfer between computers connected to the internet. They therefore applied to the Swedish courts for an order for disclosure of data for the purpose of communicating the name and address of the person using the IP address from which it was assumed that the files in question had been sent.

In that context, the Högsta domstolen, hearing an appeal in cassation, asked the Court whether EU law precludes the application of a national provision which is based on Article 8 of Directive 2004/48/EC and which permits an internet service provider in civil proceedings, in order to identify a particular subscriber, to be ordered to give a copyright holder or its representative information on the subscriber to whom the internet service provider provided a specific IP address, which address, it was claimed, had been used in the infringement. The question was based on the assumption that the applicant had adduced clear evidence of the infringement of a particular copyright and that the measure was proportionate.

The Court noted first of all that Article 8(3) of Directive 2004/48/EC, read in conjunction with Article 15(1) of Directive 2002/58/EC, does not preclude Member States from imposing an obligation to disclose to private persons personal data in order to enable them to bring civil proceedings for copyright infringements, but nor does it require those Member States to lay down such an obligation. However, the authorities and courts of Member States must not only interpret their national law in a manner consistent with those directives, but must also make sure that they do not rely on an interpretation of them which would conflict with those fundamental rights or with the other general principles of EU law, such as the principle of proportionality (paragraphs 55, 56).

The Court found, in that regard, that the national legislation in question required, *inter alia*, that, for an order for disclosure of the data in question to be made, there be clear evidence of an infringement of an intellectual property right, that the information can be regarded as facilitating the investigation into an infringement of copyright or impairment of such a right and that the reasons for the measure outweigh the nuisance or other harm which the measure could entail for the person affected by it or for some other conflicting interest (paragraph 58).

Consequently, the Court concluded that Directives 2002/58/EC and 2004/48/EC do not preclude national legislation such as that at issue in the main proceedings in so far as that legislation enables the national court seised of an application for an order for disclosure of personal data, made by a person who is entitled to act, to weigh the conflicting interests involved, on the basis of the facts of each case and taking due account of the requirements of the principle of proportionality (paragraph 61 and operative part).

De-referencing of personal data

GC and Others (De-referencing of sensitive data) (C-136/17, EU:C:2019:773) - Judgment of 24 September 2019 (Grand Chamber)

In this judgment, the Court, sitting as the Grand Chamber, clarified the obligations of operators of a search engine in the context of a request for de-referencing relating to sensitive data.

Google had refused to accede to the requests of four individuals for the de-referencing, in the list of results displayed by the search engine in response to searches against their names, of various links leading to web pages published by third parties, including press articles. Following complaints by those four individuals, the Commission nationale de l'informatique et des libertes (CNIL) (French Data Protection Authority, France) refused to serve formal notice on Google to carry out the de-referencing requested. The Conseil d'Etat (Council of State, France), before which the case was

brought, asked the Court to clarify the obligations of an operator of a search engine when handling a request for de-referencing under Directive 95/46/EC.

First, the Court recalled that the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life is prohibited, subject to certain exceptions and derogations. As regards the processing of data relating to offences, criminal convictions or security measures, this may in principle be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law (paragraphs 39 and 40).

The Court ruled that the prohibition and restrictions relating to the processing of those special categories of data apply to the operator of a search engine, in the same way as any other controller of personal data. The purpose of those prohibitions and restrictions is to ensure enhanced protection as regards such processing, which, because of the particular sensitivity of the data, is liable to constitute a particularly serious interference with the fundamental rights to privacy and the protection of personal data (paragraphs 42 to 44).

However, the operator of a search engine is responsible not because personal data appear on a web page published by a third party but because of the referencing of that page. In those circumstances, the prohibition and restrictions relating to the processing of sensitive data apply to that operator only by reason of that referencing and thus via a verification, under the supervision of the competent national authorities, on the basis of a request by the data subject (paragraphs 46 and 47).

Second, the Court held that when the operator receives a request for de-referencing relating to sensitive data, he is in principle required, subject to certain exceptions, to accede to that request. As regards those exceptions, the operator may, *inter alia*, refuse to accede to such a request if he establishes that the links lead to data which are manifestly made public by the data subject, provided that the referencing of those links satisfies the other conditions of lawfulness of the processing of personal data and unless the data subject has the right to object to that referencing on grounds relating to the data subject's particular situation (paragraphs 65 and 69).

In any event, when the operator of a search engine receives a request for de-referencing, he must ascertain whether the inclusion in the list of results, displayed following a search on the basis of the data subject's name of the link to a web page on which sensitive data are published, is strictly necessary for protecting the freedom of information of internet users potentially interested in accessing that web page by means of such a search. In that regard, the Court pointed out that, while the rights to privacy and the protection of personal data override, as a general rule, the freedom of

information of internet users, that balance may, however, depend, in specific cases, on the nature of the information in question and on its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, depending on the role played by the data subject in public life (paragraphs 66 and 68).

Third, the Court ruled that, in the context of a request for de-referencing in respect of data relating to criminal proceedings brought against the data subject, concerning an earlier stage of the proceedings and no longer corresponding to the current situation, it is for the operator of a search engine to assess whether, in the light of all the circumstances of the case, the data subject has a right to have the information in question no longer, in the present state of things, linked with the data subject's name by a list of results displayed following a search carried out on the basis of that name. However, even if it is not the case because the inclusion of the link in question is strictly necessary for reconciling the data subject's rights to privacy and the protection of personal data with the freedom of information of potentially interested internet users, the operator is required, at the latest on the occasion of the request for de-referencing, to adjust the list of results in such a way that the overall picture it gives the internet user reflects the current legal position, which means in particular that links to web pages containing information on that point must appear in the first place on the list (paragraphs 77 and 78).

Google (Territorial scope of dereferencing) (C-507/17, EU:C:2019:772) - Judgment of 24 September 2019 (Grand Chamber)

The Commission nationale de l'informatique et des libertes (French Data Protection Authority, France) ('the CNIL') served formal notice on Google that, in the case where that company accedes to a request for de-referencing, it must remove, from the list of results displayed on all its search engine's domain name extensions following a search conducted on the basis of the name of the data subject, links to web pages containing personal data concerning that data subject. Following Google's refusal to comply with that formal notice, the CNIL imposed a penalty of EUR 100 000 on that company. The Conseil d'Etat (Council of State, France), in the proceedings brought before it by Google, asked the Court to specify the territorial scope of the obligation for a search engine operator to give effect to the right to de-referencing under Directive 95/46/EC.

First of all, the Court recalled the possibility, under EU law, for natural persons to assert their right to de-referencing against a search engine operator who has one or more establishments in the territory of the European Union, regardless of whether or not the processing of personal data (in the present case, the referencing of links to web pages containing personal data concerning the person availing himself of that right) takes place in the European Union.

With regard to the scope of the right to de-referencing, the Court took the view that the operator of a search engine is required to carry out the de-referencing not on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States. It noted in this regard that, while a universal de-referencing would, in view of the characteristics of the internet and search engines, meet the EU legislature's objective of guaranteeing a high level of protection of personal data throughout the European Union in full, it is in no way apparent from EU law that, for the purposes of achieving such an objective, the legislature would have chosen to confer a scope on the right to de-referencing which would go beyond the territory of the Member States. In particular, while EU law establishes cooperation mechanisms between the supervisory authorities of the Member States in order that they may come to a joint decision based on a weighing of the right to privacy and of the protection of personal data, on the one hand, against the interest of the public in various Member States in having access to information, on the other, no provision is currently made for such mechanisms as regards the scope of a de-referencing outside the European Union (paragraphs 62 and 73).

As EU law currently stands, it is for the operator of a search engine to carry out the requested de-referencing not only on the version of the search engine corresponding to the Member State of residence of the person benefiting from that de-referencing but on the versions of the search engine corresponding to the Member States, in order, in particular, to ensure a consistent and high level of protection throughout the European Union. Moreover, it is for such an operator to take, if necessary, sufficiently effective measures to prevent or, at the very least, seriously discourage EU internet users from gaining access, as the case may be from a version of the search engine corresponding to a third country, to the links concerned by the de-referencing, and it is for the national court to ascertain whether the measures adopted by the operator meet that requirement (paragraph 70).

Lastly, the Court emphasised that, although EU law does not require the operator of a search engine to carry out a de-referencing on all the versions of its search engine, it also does not prohibit such a practice. Accordingly, a supervisory or judicial authority of a Member State remains competent to weigh up, in the light of national standards of protection of fundamental rights, a data subject's right to privacy and the protection of personal data concerning him or her, on the one hand, and the right to freedom of information, on the other, and, after weighing those rights against each other, to order, where appropriate, the operator of that search engine to carry out a de-referencing concerning all versions of that search engine (paragraphs 65 and 72).

Consent by a website user to the storage of or access to information in the form of cookies

Planet49 (C-673/17, EU:C:2019:801) - Judgment of 1 October 2019 (Grand Chamber)

By this judgment, the Court ruled that consent to the storage of, or access to, information in the form of cookies installed on a website user's terminal equipment is not validly constituted if given by way of a pre-checked checkbox, irrespective of whether or not the information in question constitutes personal data. Furthermore, the Court made clear that the information that the service provider must give to an internet user includes the duration of the operation of cookies and whether or not third parties may have access to those cookies.

The case in the main proceedings concerned a promotional lottery organised by Planet49 on the website www.dein-macbook.de. Internet users wishing to take part in that lottery were required to enter their names and addresses on a web page with checkboxes. The checkbox authorising the installation of cookies contained a preselected tick. In an appeal brought by the German Federation of Consumer Organisations, the Bundesgerichtshof (Federal Court of Justice, Germany) harboured doubts as to the validity of the consent obtained from internet users by means of the preselected checkbox and as to the extent of the information obligation owed by the service provider.

The request for a preliminary ruling concerned, in substance, the concept of consent referred to in the Directive on privacy and electronic communications, read in conjunction with Directive 95/46/EC, and the General Data Protection Regulation.

First, the Court observed that Article 2(h) of Directive 95/46/EC, to which Article 2(f) of the Directive on privacy and electronic communications refers, defines 'consent' as being 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'. It noted that the requirement of an 'indication' of the data subject's wishes points clearly to active, rather than passive, behaviour. However, consent given in the form of a preselected tick in a checkbox does not imply active behaviour on the part of a website user. Furthermore, the legislative origins of Article 5(3) of the Directive on privacy and electronic communications, which, as amended by Directive 2009/136/EC, provides that the user must have 'given his or her consent' to the storage of cookies, appears to indicate that user consent may no longer be presumed but must be the result of active behaviour on the part of the user. Finally, active consent is now provided for by the General Data Protection Regulation, Article 4(11) of which requires an indication of the data subject's wishes in the form of 'clear affirmative action' and recital 32 of which expressly precludes 'silence, pre-ticked boxes or inactivity' from constituting consent (paragraphs 49, 52, 56 and 62).

The Court therefore held that consent is not validly given if the storage of information, or access to information already stored in the website user's terminal equipment, is permitted by way of a pre-ticked checkbox which the user must deselect in order to refuse his consent. It added that the fact that a user selects the button to participate in the lottery in question cannot therefore suffice for the conclusion that the user has validly given his or her consent to the storage of cookies (paragraph 63).

Second, the Court stated that Article 5(3) of the Directive on privacy and electronic communications seeks to protect the user from interference with his or her private sphere, regardless of whether or not that interference involves personal data. It follows that the concept of consent must not be interpreted differently according to whether or not the information stored or accessed on a website user's terminal equipment constitutes personal data

(paragraphs 69 and 71).

Third, the Court noted that Article 5(3) of the Directive on privacy and electronic communications requires that the user concerned must have given his or her consent, having been provided with clear and comprehensive information, inter alia, about the purposes of the processing. Clear and comprehensive information implies that a user is in a position to be able to determine easily the consequences of any consent he or she might give and to ensure that the consent given is well informed. In that regard, the Court held that the duration of the operation of the cookies and whether or not third parties may have access to those cookies form part of the clear and comprehensive information that must be provided to a website user by the service provider (paragraphs 73 to 75 and 81).

National supervisory authorities

Scope of the requirement of independence

Commission v Germany (C-518/07, EU:C:2010:125)

By its application, the European Commission had requested the Court to declare that, by making the authorities responsible for monitoring the processing of personal data outside the public sector in the different German Lander subject to State oversight, and by thus incorrectly transposing the requirement of 'complete independence' of the supervisory authorities responsible for ensuring the protection of those data, the Federal Republic of Germany had failed to fulfil its obligations under the second subparagraph of Article 28(1) of Directive 95/46/EC.

The Federal Republic of Germany contended that the second subparagraph of Article 28(1) of Directive 95/46/EC requires the supervisory authorities to have functional independence in the sense that those authorities must be independent of the non-public sector under their supervision and that they must not be exposed to external influences. In the view of the Federal Republic of Germany, the State scrutiny exercised in the Lander did not constitute such an external influence, but rather the administration's internal monitoring mechanism, implemented by the authorities attached to the same administrative machinery as the supervisory authorities and required, like the latter, to fulfil the aims of Directive 95/46/EC.

The Court held that the guarantee of the independence of national supervisory authorities provided for by Directive 95/46/EC is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was not established in order to grant a special status to those authorities themselves as well as their agents, but in order to strengthen the protection of individuals and bodies affected by their decisions, the supervisory authorities being consequently required to act objectively and impartially when carrying out their duties (paragraph 25).

The Court found that these supervisory authorities responsible for supervising the processing of personal data outside the public sector must enjoy an independence allowing them to perform their duties free from external influence. That independence precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task of establishing a fair balance between the protection of the right to private life and the free movement of personal data. The mere risk that the scrutinising authorities could exercise a political influence over the decisions of the competent supervisory authorities is enough to hinder the latter authorities' independent performance of their tasks. First, there could be 'prior compliance' on the part of those authorities in the light of the scrutinising authority's decision-making practice. Second, for the purposes of the role adopted by those supervisory authorities as guardians of the right to private life, it is necessary that their decisions, and therefore the authorities themselves, remain above any suspicion of partiality. According to the Court, State scrutiny of national supervisory authorities is not, therefore, compatible with the requirement of independence (paragraphs 30, 36, 37 and operative part).

Commission v Austria (C-614/10, EU:C:2012:631) - Judgment of 16 October 2012 (Grand Chamber)

By its application, the European Commission had asked the Court to declare that, by failing to take all of the measures necessary to ensure that the legislation in force in Austria met the requirement of independence with regard to the Datenschutzkommission (Data Protection Commission), which was established as a supervisory authority for the protection of personal data, Austria had failed to fulfil its obligations under the second subparagraph of Article 28(1) of Directive 95/46/EC.

The Court declared that Austria had failed to fulfil its obligations, finding, in essence, that a Member State which lays down a regulatory framework under which that authority's managing member is a federal official subject to supervision, whose office is integrated with national government departments, and in respect of which the head of the national government has an unconditional right to information covering all aspects of that authority's work does not meet the requirement of independence of a supervisory authority, laid down by Directive 95/46/EC (paragraph 66 and operative part).

The Court, first of all, recalled that the words 'with complete independence' in the second subparagraph of Article 28(1) of Directive 95/46/EC mean that the supervisory authorities must enjoy an independence which allows them to perform their duties free from external influence. The fact that such an authority has functional independence in so far as its members are independent and are not bound by instructions of any kind in the performance of their duties is not by itself sufficient to protect that supervisory authority from all external influence. The independence required in that connection is intended to preclude not only direct influence, in the form of instructions, but also any indirect influence which is liable to have an effect on the supervisory authority's decisions. Moreover, in the light of the role adopted by the supervisory authorities as guardians of the right to private life, their decisions, and therefore the authorities themselves, must remain above any suspicion of partiality (paragraphs 41-43, 52).

The Court stated that, in order to be able to satisfy the criterion of independence set out in the aforementioned provision of Directive 95/46/EC, a national supervisory authority need not be given a separate budget, such as that provided for in Article 43(3) in Regulation (EC) No 45/2001. Member States are not obliged to reproduce in their national legislation provisions similar to those of Chapter V of Regulation (EC) No 45/2001 in order to ensure the total independence of their respective supervisory authorities, and they can therefore provide that, from the point of view of budgetary law, the supervisory authorities are to come under a specified ministerial department. However, the attribution of the necessary equipment and staff to such authorities must not prevent them from

acting 'with complete independence' in exercising the functions entrusted to them within the meaning of the second subparagraph of Article 28(1) of Directive 95/46/EC (paragraph 58).

Commission v Hungary (C-288/12, EU:C:2014:237) - Judgment of 8 April 2014 (Grand Chamber)

In this case, the Commission had asked the Court to declare that, by prematurely bringing to an end the term served by the supervisory authority for the protection of personal data, Hungary had failed to fulfil its obligations under Directive 95/46/EC.

The Court held that a Member State fails to fulfil its obligations under Directive 95/46/EC if it prematurely brings to an end the term served by the supervisory authority for the protection of personal data (paragraph 62, operative part 1).

According to the Court, the supervisory authorities responsible for supervising the processing of those data must enjoy an independence allowing them to perform their duties free from external influence in whatever form, whether direct or indirect, which may have an effect on their decisions and which could call into question the performance by those authorities of their task of striking a fair balance between the protection of the right to private life and the free movement of personal data (paragraph 51).

The Court also pointed out that, since operational independence is not sufficient in itself to protect supervisory authorities from all external influence, the mere risk that State scrutinising authorities could exercise political influence over the decisions of the supervisory authorities is enough to hinder the latter in the independent performance of their tasks. If it were permissible for every Member State to compel a supervisory authority to vacate office before serving its full term, in contravention of the rules and safeguards established in that regard by the legislation applicable, the threat of such premature termination to which that authority would be exposed throughout its term of office could lead it to enter into a form of prior compliance with the political authority, which is incompatible with the requirement of independence. Moreover, in such a situation, the supervisory authority cannot be regarded as being able, in all circumstances, to operate above all suspicion of partiality (paragraphs 52-55).

Determination of the applicable law and of the competent supervisory authority

Weltimmo (C-230/14, EU:C:2015:639) - Judgment of 1 October 2015

The Nemzeti Adatvédelmi és Információs Zsábadóság (National Authority for Data Protection and Freedom of Information, Hungary) imposed a fine on Weltimmo, a company registered in Slovakia running property-dealing websites concerning Hungarian properties, on the ground that it

had not deleted the personal data of advertisers on those sites, despite their requests to that effect, and had forwarded those data to debt-collection agencies for the purpose of obtaining settlement of unpaid bills. According to the Hungarian supervisory authority, Weltimmo had, in so doing, infringed the Hungarian law transposing Directive 95/46/EC.

On hearing an appeal in cassation, the Kuria (Supreme Court, Hungary) expressed doubts concerning the determination of the applicable law and the powers of the Hungarian data protection authority under Articles 4(1) and 28 of Directive 95/46/EC. It therefore referred a number of questions to the Court for a preliminary ruling.

As regards the national law applicable, the Court ruled that Article 4(1)(a) of Directive 95/46/EC permits the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing of those data is registered, in so far as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity - even a minimal one - in the context of which that processing is carried out. In order to ascertain whether that is the case, the referring court may, in particular, take account of the fact that the activity of the controller in respect of that processing, in the context of which that processing takes place, consists of the running of property-dealing websites concerning properties situated in the territory of that Member State and written in that Member State's language and that it is, as a consequence, mainly or entirely directed at that Member State. The referring court may, moreover, also take account of the fact that that controller has a representative in that Member State, who is responsible for recovering the debts resulting from that activity and for representing the controller in the administrative and judicial proceedings relating to the processing of the data concerned. By contrast, the Court made clear that the issue of the nationality of the persons concerned by such data processing is irrelevant (paragraph 41, operative part 1).

As regards the competence and powers of the supervisory authority to which complaints have been submitted in accordance with Article 28(4) of Directive 95/46/EC, the Court held that that authority may examine those complaints irrespective of the applicable law and before even knowing which national law is applicable to the processing in question (paragraph 54). However, if it reaches the conclusion that the law of another Member State is applicable, it cannot impose penalties outside the territory of its own Member State. In such a situation, it must, in fulfilment of the duty of cooperation laid down in Article 28(6) of that directive, request the supervisory authority of that other Member State to establish whether there has been an infringement of that law and to impose penalties if that

law permits, based, where necessary, on the information which the authority of the first Member State has transmitted to the authority of that other Member State (paragraphs 57, 60, operative part 2).

Powers of the national supervisory authorities

Schrems (C-362/14, EU:C:2015:650) - Judgment of 6 October 2015 (Grand Chamber)

In this case (see also Section IV ‘Transfer of personal data to third countries’), the Court ruled, *inter alia*, that national supervisory authorities have the power to control transfers of personal data to third countries.

In that regard, the Court found, first of all, that national supervisory authorities have a wide range of powers and that those powers, listed on a non-exhaustive basis in Article 28(3) of Directive 95/46/EC, constitute necessary means by which to perform their duties. Thus, those authorities possess, in particular, investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings (paragraph 43).

As regards the power to control transfers of personal data to third countries, the Court ruled that it is, admittedly, apparent from Article 28(1) and (6) of Directive 95/46/EC that the powers of the national supervisory authorities concern processing of personal data carried out on the territory of their own Member State, with the result that they do not have powers on the basis of Article 28 in respect of the processing of such data in a third country (paragraph 44).

However, the operation consisting in having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data carried out in a Member State. Consequently, as, in accordance with Article 8(3) of the Charter and Article 28 of Directive 95/46/EC, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of individuals with regard to the processing of personal data, each of them is vested with the power to check whether a transfer of those data from its own Member State to a third country complies with the requirements laid down by that directive (paragraphs 45, 47).

Wirtschaftsakademie Schleswig - Holstein (C-210/16, EU:C:2018:388) - Judgment of 5 June 2018 (Grand Chamber)

In this judgment (see also Section II.5. ‘Concept of a “controller of the processing of personal data”’) relating to, *inter alia*, the interpretation of Articles 4 and 28 of Directive 95/46/EC, the Court ruled on

the extent of the powers of intervention of supervisory authorities with regard to the processing of personal data which involves the participation of several parties.

Thus, the Court held that where an undertaking established outside the European Union (such as the US company Facebook) has several establishments in different Member States, the supervisory authority of a Member State is entitled to exercise the powers conferred on it by Article 28(3) of that directive with respect to an establishment of that undertaking situated in the territory of that Member State (in this case, Facebook Germany) even if, as a result of the division of tasks within the group, first, that establishment is responsible solely for the sale of advertising space and other marketing activities in the territory of that Member State and, secondly, exclusive responsibility for collecting and processing personal data belongs, for the entire territory of the European Union, to an establishment situated in another Member State (in this case, Facebook Ireland) (paragraph 64, operative part 2).

Furthermore, the Court stated that where the supervisory authority of a Member State intends to exercise, with respect to an entity established in the territory of that Member State, the powers of intervention referred to in Article 28(3) of Directive 95/46/EC, on the ground of infringements of the rules on the protection of personal data committed by a third party responsible for the processing of that data whose seat is in another Member State (in this case, Facebook Ireland), that supervisory authority is competent to assess, independently of the supervisory authority of the other Member State (Ireland), the lawfulness of such data processing and may exercise its powers of intervention with respect to the entity established in its territory without first calling on the supervisory authority of the other Member State to intervene (paragraph 74, operative part 3).

Territorial application of EU legislation

Google Spain and Google (C-131/12, EU:C:2014:317) - Judgment of 13 May 2014 (Grand Chamber)

In this judgment (see also Sections II.3. 'Concept of "processing of personal data"' and V.1. 'Right to object to the processing of personal data ("right to be forgotten")'), the Court also ruled on the territorial scope of Directive 95/46/EC.

Thus, the Court held that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of Directive 95/46/EC, when the operator of a search engine, despite having its seat in a third State, sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered

by that engine and which orientates its activity towards the inhabitants of that Member State (paragraphs 55, 60, operative part 2).

In such circumstances, the activities of the operator of the search engine and those of its establishment situated in a Member State, although separate, are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed (paragraph 56).

Right of public access to documents of the institutions of the European Union and protection of personal data

Commission v Bavarian Lager (C-28/08 P, EU:C:2010:378) - Judgment of 29 June 2010 (Grand Chamber)

Bavarian Lager, a company established for the importation of German beer for public houses and bars in the United Kingdom, had been unable to sell its product, since a large number of publicans in the United Kingdom were tied by exclusive purchasing contracts obliging them to obtain their supplies of beer from certain breweries.

Under United Kingdom legislation on the supply of beer, known as the Guest Beer Provision ('the GBP'), British breweries were required to allow pub managers the possibility of buying a beer from another brewery, on condition that it had been conditioned in a cask. However, most beers produced outside the United Kingdom could not be regarded as 'cask-conditioned beers' within the meaning of the GBP, and thus did not fall within its scope. Bavarian Lager took the view that that legislation constituted a measure having equivalent effect to a quantitative restriction on imports and lodged a complaint with the Commission.

During the infringement proceedings initiated by the Commission against the United Kingdom, representatives of the Community and United Kingdom administrative authorities and of the Confederation des Brasseurs du Marche Commun (CBMC) had attended a meeting held on 11 October 1996. The United Kingdom authorities informed the Commission that the legislation in question was to be amended, so as to allow bottle-conditioned beer to be sold as a guest beer as well as cask-conditioned beer. Thereupon, the Commission had told Bavarian Lager that the infringement proceedings were to be suspended.

Bavarian Lager had lodged an application requesting the full minutes of the October 1996 meeting, including the names of all the participants, which the Commission had subsequently refused by

decision of 18 March 2004, invoking in particular the privacy of those individuals, as guaranteed by the legislation on the protection of personal data.

Bavarian Lager then brought an action before the General Court seeking annulment of that Commission decision. By judgment of 8 November 2007, the General Court annulled the Commission's decision, finding in particular that the mere inclusion of the names of persons on the list of participants at a meeting, acting on behalf of the bodies they represented, did not adversely affect or jeopardise their privacy. The Commission, supported by the United Kingdom and the Council, then lodged an appeal with the Court against that judgment of the General Court.

The Court noted, first of all, that where a request based on Regulation (EC) No 1049/2001, regarding access to documents, seeks to obtain access to documents including personal data, the provisions of Regulation (EC) No 45/2001 become applicable in their entirety, including the provision requiring the recipient of personal data to establish the need for their disclosure and the provision which confers on the data subject the right to object at any time, on compelling legitimate grounds relating to his or her particular situation, to the processing of data relating to him or her (paragraph 63).

The Court then went on to find that the list of participants at a meeting held in the context of infringement proceedings which appeared in the minutes of that meeting contained personal data for the purposes of Article 2(a) of Regulation (EC) No 45/2001, since the persons who participated in that meeting could be identified (paragraph 70).

Last, it concluded that, in requiring, in respect of those persons who had not given their express consent to the disclosure of personal data concerning them contained in those minutes, that the necessity of having the personal data transferred be established, the Commission had complied with the provisions of Article 8(b) of that regulation (paragraph 77).

Where, in the context of a request for access to those minutes under Regulation (EC) No 1049/2001, no express or legitimate justification or any convincing argument is provided in order to demonstrate the necessity for those personal data to be transferred, the Commission is unable to weigh up the various interests of the parties concerned. Nor can it verify whether there is any reason to assume that the data subjects' legitimate interests might be prejudiced by that transfer, as required by Article 8(b) of Regulation (EC) No 45/2001 (paragraph 78).

ClientEarth and PAN Europe v EFSA (C-615/13 P, EU:C:2015:489) - Judgment of 16 July 2015

The European Food Safety Authority (EFSA) had established a working group to develop guidance as to how to implement Article 8(5) of Regulation (EC) No 1107/2009 60, according to which an

applicant for authorisation to place a plant protection product on the market is to add to the dossier scientific peer-reviewed open literature, as determined by EFSA, on the active substance and its relevant metabolites dealing with side-effects on health, the environment and non-target species.

The draft guidance was submitted for public consultation, and ClientEarth and Pesticide Action Network Europe (PAN Europe) submitted comments on it. In that context, they had jointly submitted to EFSA an application requesting access to a number of documents related to the preparation of the draft guidance, including the comments of the external experts.

EFSA granted ClientEarth and PAN Europe access to, inter alia, the individual comments of the external experts on the draft guidance document. It stated, however, that it had redacted the names of those experts, in accordance with Article 4(1)(b) of Regulation (EC) No 1049/2001 and the EU legislation on the protection of personal data, in particular Regulation (EC) No 45/2001. It stated in that regard that the disclosure of the names of those experts was a transfer of personal data, within the meaning of Article 8 of Regulation (EC) No 45/2001, and that the conditions for such a transfer laid down in that article were not fulfilled in this case.

Consequently, ClientEarth and PAN Europe brought an action for annulment of that EFSA decision before the General Court. Following the General Court's dismissal of that action, ClientEarth and PAN Europe brought an appeal against the General Court's judgment before the Court of Justice.

In the first place, the Court noted that, because the information sought would make it possible to connect to one particular expert or another a particular comment, it concerned identified natural persons and accordingly constituted a set of personal data, within the meaning of Article 2(a) of Regulation (EC) No 45/2001. Since the concepts of 'personal data' within the meaning of Article 2(a) of Regulation (EC) No 45/2001 and of 'data relating to private life' are not to be confused, the Court further considered the claim made by ClientEarth and PAN Europe that the information at issue did not fall within the scope of the private life of the experts concerned to be ineffective (paragraphs 29, 32).

The Court examined, in the second place, the argument of ClientEarth and PAN Europe based on the existence of a climate of suspicion in regard to EFSA, often accused of partiality because of its use of experts with vested interests due to their links with industrial lobbies, and on the necessity of ensuring the transparency of EFSA's decision-making process. That argument was supported by a study which identified links between a majority of the expert members of an EFSA working group and industrial lobbies. The Court held that obtaining the information at issue was necessary so that the impartiality of each of those experts in carrying out their tasks as scientists in the service of EFSA could be

specifically ascertained. The Court therefore set aside the judgment of the General Court, ruling that the General Court was wrong to hold that the aforementioned argument of ClientEarth and PAN Europe was not sufficient to establish that the transfer of the information at issue was necessary (paragraphs 57-59).

In the third place, in order to assess the legality of the EFSA decision at issue, the Court examined whether or not there was any reason to assume that that transfer might have prejudiced the legitimate interests of the data subjects. It found, in that regard, that the allegation by EFSA that the disclosure of the information at issue would have been likely to undermine the privacy and integrity of the experts was a consideration of a general nature which was not otherwise supported by any factor specific to the case. The Court considered, on the contrary, that such disclosure would, by itself, have made it possible for the suspicions of partiality in question to be dispelled or would have afforded experts who might be concerned the opportunity to dispute, if necessary by available legal remedies, the merits of those allegations of partiality. In the light of those points, the Court also annulled EFSA's decision (paragraphs 69, 73).

AVRUPA BİRLİĞİ ADALET DİVANI KARARLARI (TAM METİN)

Bölüm İçeriği

- Österreichische Post (C-154/21)
- Autoriteit Persoonsgegevens (C-245/20)
- Meta Platforms Ireland (Case C-319/20)
- PNR Directive (C-817/19)
- Schrems II - Data Protection Commissioner v. Facebook Ireland Ltd. (C-311/18)
- Prokuratuur Case (C-746/18)
- G.D. v The Commissioner of the Garda Síochána Case (C-140/20)

Judgment of the Court in Case C-154/21 | Österreichische Post (Information regarding the recipients of personal data)

Every person has the right to know to whom his or her personal data have been disclosed

Nevertheless, the controller may indicate only the categories of recipient if it is impossible to identify the recipients or the request is manifestly unfounded or excessive

A citizen requested Österreichische Post, the principal operator of postal and logistical services in Austria, to disclose to him the identity of the recipients to whom it had disclosed his personal data.

He relied on the EU General Data Protection Regulation (GDPR). That regulation provides that the data subject has the right to obtain from the controller information about the recipients or categories of recipient to whom his or her personal data have been or will be disclosed.

In response to the citizen's request, Österreichische Post merely stated that it uses personal data, to the extent permissible by law, in the course of its activities as a publisher of telephone directories and that it offers those personal data to trading partners for marketing purposes. The citizen therefore brought proceedings against Österreichische Post before the Austrian courts.

During the judicial proceedings, Österreichische Post further informed the citizen that his data had been forwarded to customers, including advertisers trading via mail order and stationary outlets, IT companies, mailing list providers and associations such as charitable organisations, non-governmental organisations (NGOs) or political parties.

The Oberster Gerichtshof (Supreme Court, Austria), hearing the dispute at last instance, wishes to know whether the GDPR leaves the data controller the choice to disclose either the specific identity of the recipients or only the categories of recipient, or whether it gives the data subject the right to know their specific identity.

In today's judgment, the Court replies that where personal data have been or will be disclosed to recipients, there is an obligation on the part of the controller to provide the data subject, on request, with the actual identity of those recipients. It is only where it is not (yet) possible to identify those recipients that the controller may indicate only the categories of recipient in question. That is also the case where the controller demonstrates that the request is manifestly unfounded or excessive.

The Court points out that the data subject's right of access is necessary to enable the data subject to exercise other rights conferred by the GDPR, namely his or her right to rectification, right to erasure ('right to be forgotten'), right to restriction of processing, right to object to processing or right of action where he or she suffers damage.

JUDGMENT OF THE COURT (First Chamber)

12 January 2023 (*)

(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 15(1)(c) – Data subject’s right of access to his or her data – Information about the recipients or categories of recipient to whom the personal data have been or will be disclosed – Restrictions)

In Case C-154/21,

REQUEST for a preliminary ruling under Article 267 TFEU from the Oberster Gerichtshof (Supreme Court, Austria), made by decision of 18 February 2021, received at the Court on 9 March 2021, in the proceedings

RW

v

Österreichische Post AG,

THE COURT (First Chamber),

composed of A. Arabadjiev, President of the Chamber, L. Bay Larsen, Vice-President of the Court, acting as Judge of the First Chamber, P.G. Xuereb, A. Kumin and I. Ziemele (Rapporteur), Judges,

Advocate General: G. Pitruzzella,

Registrar: A. Calot Escobar,

having regard to the written procedure,

after considering the observations submitted on behalf of:

- RW, by R. Haupt, Rechtsanwalt,
- Österreichische Post AG, by R. Marko, Rechtsanwalt,
- the Austrian Government, by G. Kunnert, A. Posch and J. Schmoll, acting as Agents,
- the Czech Government, by M. Smolek and J. Vláčil, acting as Agents,
- the Italian Government, by G. Palmieri, acting as Agent, and by M. Russo, avvocato dello Stato,
- the Latvian Government, by J. Davidoviča, I. Hūna and K. Pommere, acting as Agents,
- the Romanian Government, by L.-E. Baţagoi, E. Gane and A. Wellman, acting as Agents,

– the Swedish Government, by H. Eklinder, J. Lundberg, C. Meyer-Seitz, A.M. Runeskjöld, M. Salborn Hodgson, R. Shahsavan Eriksson, H. Shev and O. Simonsson, acting as Agents,

– the European Commission, by F. Erlbacher and H. Kranenborg, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 9 June 2022,

gives the following

Judgment

1. This request for a preliminary ruling concerns the interpretation of Article 15(1)(c) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1) ('the GDPR').

2. The request has been made in proceedings between RW and Österreichische Post AG ('Österreichische Post') concerning a request for access to personal data pursuant to Article 15(1)(c) of the GDPR.

Legal context

3. Recitals 4, 9, 10, 39, 63 and 74 of the GDPR are worded as follows:

'(4) ... The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. ...

...

(9) The objectives and principles of Directive 95/46/EC [of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)] remain sound, but it has not prevented fragmentation in the implementation of data protection across the [European] Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in

the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. ...

...

(39) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. ...

...

(63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. ... Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. ... That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. ...

...

(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.'

4. Article 1 of the GDPR, headed 'Subject matter and objectives', provides in paragraph 2:

'This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.'

5. Article 5 of the GDPR, headed 'Principles relating to processing of personal data', provides:

'1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");

...

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability").'

6. Article 12 of the GDPR, headed 'Transparent information, communication and modalities for the exercise of the rights of the data subject', states:

'1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

...

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

...'

7. Article 13 of the GDPR, headed 'Information to be provided where personal data are collected from the data subject', provides in paragraph 1:

'Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

...

(e) the recipients or categories of recipients of the personal data, if any;

...'

8. Article 14 of the GDPR, headed 'Information to be provided where personal data have not been obtained from the data subject', provides in paragraph 1:

'Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

...

(e) the recipients or categories of recipients of the personal data, if any;

...'

9. As set out in Article 15 of the GDPR, headed 'Right of access by the data subject':

'1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.'

10. Article 16 of the GDPR, headed 'Right to rectification', provides:

'The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.'

11. As set out in Article 17 of the GDPR, headed 'Right to erasure ("right to be forgotten")':

'1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

...'

12. Article 18 of the GDPR, headed 'Right to restriction of processing', provides in paragraph 1:

'The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

...'

13. Article 19 of the GDPR is worded as follows:

'The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.'

14. Under Article 21 of the GDPR, headed 'Right to object':

'1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC [of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37)], the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.'

15. Article 79 of the GDPR, headed 'Right to an effective judicial remedy against a controller or processor', states in paragraph 1:

‘Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.’

16. Article 82 of the GDPR, headed ‘Right to compensation and liability’, provides in paragraph 1:

‘Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.’

The dispute in the main proceedings and the question referred for a preliminary ruling

17. On 15 January 2019, RW asked Österreichische Post for access under Article 15 of the GDPR to the personal data concerning him which were being stored or had previously been stored by Österreichische Post and, if the data had been disclosed to third parties, for information as to the identity of the recipients.

18. In response to that request, Österreichische Post merely stated that it uses data, to the extent permissible by law, in the course of its activities as a publisher of telephone directories and that it offers those personal data to trading partners for marketing purposes. It also referred to a website that set out more information and further data processing purposes. It did not disclose to RW the identity of the specific recipients of the data.

19. RW brought proceedings against Österreichische Post before the Austrian courts, seeking an order that Österreichische Post provide him with, inter alia, the identity of the recipient(s) of the personal data disclosed.

20. During the judicial proceedings thus initiated, Österreichische Post informed RW that his personal data had been processed for marketing purposes and forwarded to customers, including advertisers trading via mail order and stationary outlets, IT companies, mailing list providers and associations such as charitable organisations, non-governmental organisations (NGOs) or political parties.

21. The courts at first instance and on appeal dismissed RW’s action on the ground that Article 15(1)(c) of the GDPR, by referring to ‘recipients or categories of recipient’, gives the controller the option of informing the data subject only of the categories of recipient, without having to identify by name the specific recipients to whom personal data are transferred.

22. RW brought an appeal on a point of law (Revision) before the Oberster Gerichtshof (Supreme Court, Austria), the referring court.

23. That court is uncertain as to the interpretation of Article 15(1)(c) of the GDPR, in so far as it is not clear from the wording of that provision whether it grants the data subject the right of access to information relating to the specific recipients of the disclosed data, or whether the controller has discretion as to how it proposes to respond to a request for access to information about the recipients.

24. The referring court nevertheless observes that the underlying objective of that provision supports the interpretation that it is the data subject who has the option of requesting information about the categories of recipient or requesting information about the specific recipients of his or her personal data. In the referring court's view, any contrary interpretation would seriously undermine the effectiveness of the legal remedies available to the data subject for the protection of his or her data. If controllers had the option of informing data subjects of the specific recipients or only of the categories of recipient, the fear would be that, in practice, almost no controller would provide information about specific recipients.

25. In addition, unlike Article 13(1)(e) and Article 14(1)(e) of the GDPR, which lay down an obligation on the part of the controller to provide the information set out in those articles, Article 15(1) of that regulation focuses on the scope of the data subject's right of access, a fact which, according to the referring court, also tends to indicate that the data subject has the right to choose between requesting information about the specific recipients or about categories of recipient.

26. Lastly, the referring court adds that the right of access provided for in Article 15(1) of the GDPR covers not only personal data currently being processed but also all data processed previously. In that regard, it states that the considerations set out in the judgment of 7 May 2009, *Rijkeboer* (C-553/07, EU:C:2009:293), based on the purpose of the right of access provided for by Directive 95/46, may be transferred to the right of access under Article 15 of the GDPR, especially since it can be deduced from recitals 9 and 10 of the GDPR that the EU legislature did not intend to reduce the level of protection as compared to that directive.

27. In those circumstances, the Oberster Gerichtshof (Supreme Court) decided to stay the proceedings and to refer the following question to the Court of Justice for a preliminary ruling:

'Is Article 15(1)(c) of [the GDPR] to be interpreted as meaning that the right of access is limited to information concerning categories of recipient where specific recipients have not yet been determined

in the case of planned disclosures, but that right must necessarily also cover recipients of those disclosures in cases where data [have] already been disclosed?’

Consideration of the question referred

28. By its question, the referring court asks, in essence, whether Article 15(1)(c) of the GDPR must be interpreted as meaning that the data subject’s right of access to personal data concerning him or her, provided for by that provision, entails, where those data have been or will be disclosed to recipients, an obligation on the part of the controller to provide the data subject with the specific identity of those recipients.

29. As a preliminary point, it should be borne in mind that, in accordance with settled case-law, the interpretation of a provision of EU law requires that account be taken not only of its wording, but also of its context and the objectives and purpose pursued by the act of which it forms part (judgment of 15 March 2022, *Autorité des marchés financiers*, C-302/20, EU:C:2022:190, paragraph 63). Furthermore, where a provision of EU law is open to several interpretations, preference must be given to that interpretation which ensures that the provision retains its effectiveness (judgment of 7 March 2018, *Cristal Union*, C-31/17, EU:C:2018:168, paragraph 41 and the case-law cited).

30. As regards, first of all, the wording of Article 15(1)(c) of the GDPR, that provision states that the data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and information about the recipients or categories of recipient to whom the personal data have been or will be disclosed.

31. It should be noted that the terms ‘recipients’ and ‘categories of recipient’ in that provision are used in succession, without it being possible to infer an order of priority between them.

32. It is thus clear that the wording of Article 15(1)(c) of the GDPR does not make it possible to determine unequivocally whether the data subject would have the right to be informed, when personal data concerning him or her have been or will be disclosed, of the specific identity of the recipients of the data.

33. Next, as regards the context of Article 15(1)(c) of the GDPR, it should be pointed out, in the first place, that recital 63 of that regulation states that the data subject is to have the right to know and obtain communication in particular with regard to the recipients of the personal data and does not state that that right may be restricted solely to categories of recipient, as the Advocate General observed in point 23 of his Opinion.

34. In the second place, it should also be borne in mind that, in order to respect the right of access, all processing of personal data of natural persons must comply with the principles set out in Article 5 of the GDPR (see, to that effect, judgment of 16 January 2019, *Deutsche Post*, C-496/17, EU:C:2019:26, paragraph 57).

35. Those principles include the principle of transparency set out in Article 5(1)(a) of the GDPR, which, as is clear from recital 39 of that regulation, requires that the data subject have information about how his or her personal data are processed and that that information be easily accessible and easy to understand.

36. In the third place, it should be noted, as the Advocate General stated in point 21 of his Opinion, that, unlike Articles 13 and 14 of the GDPR, which lay down an obligation on the part of the controller to provide the data subject with information relating to the categories of recipient or the specific recipients of the personal data concerning him or her where personal data are collected from the data subject and where personal data have not been obtained from the data subject, Article 15 of the GDPR lays down a genuine right of access for the data subject, with the result that the data subject must have the option of obtaining either information about the specific recipients to whom the data have been or will be disclosed, where possible, or information about the categories of recipient.

37. In the fourth place, the Court has previously held that the exercise of that right of access must enable the data subject to verify not only that the data concerning him or her are correct, but also that they are processed in a lawful manner (see, by analogy, judgments of 17 July 2014, *YS and Others*, C-141/12 and C-372/12, EU:C:2014:2081, paragraph 44, and of 20 December 2017, *Nowak*, C-434/16, EU:C:2017:994, paragraph 57), and in particular that they have been disclosed to authorised recipients (see, by analogy, judgment of 7 May 2009, *Rijkeboer*, C-553/07, EU:C:2009:293, paragraph 49).

38. In particular, that right of access is necessary to enable the data subject to exercise, depending on the circumstances, his or her right to rectification, right to erasure ('right to be forgotten') or right to restriction of processing, conferred, respectively, by Articles 16, 17 and 18 of the GDPR (see, by analogy, judgments of 17 July 2014, *YS and Others*, C-141/12 and C-372/12, EU:C:2014:2081, paragraph 44, and of 20 December 2017, *Nowak*, C-434/16, EU:C:2017:994, paragraph 57), and the data subject's right to object to his or her personal data being processed, laid down in Article 21 of the GDPR, and right of action where he or she suffers damage, laid down in Articles 79 and 82 of the GDPR (see, by analogy, judgment of 7 May 2009, *Rijkeboer*, C-553/07, EU:C:2009:293, paragraph 52).

39. Thus, in order to ensure the effectiveness of all of the rights referred to in the preceding paragraph of the present judgment, the data subject must have, in particular, the right to be informed of the identity of the specific recipients where his or her personal data have already been disclosed.

40. Such an interpretation is confirmed, in the fifth and last place, by a reading of Article 19 of the GDPR, which provides, in its first sentence, that the controller is, in principle, to communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed and, in its second sentence, that the controller is to inform the data subject about those recipients if the data subject requests it.

41. Thus, the second sentence of Article 19 of the GDPR expressly confers on the data subject the right to be informed of the specific recipients of the data concerning him or her by the controller, in the context of the controller's obligation to inform all the recipients of the exercise of the data subject's rights under Article 16, Article 17(1) and Article 18 of the GDPR.

42. It follows from the above contextual analysis that Article 15(1)(c) of the GDPR is one of the provisions intended to ensure transparency vis-à-vis the data subject of the manner in which personal data are processed and enables that person, as the Advocate General observed in point 33 of his Opinion, to exercise the rights laid down, inter alia, in Articles 16 to 19, 21, 79 and 82 of the GDPR.

43. Accordingly, the information provided to the data subject pursuant to the right of access provided for in Article 15(1)(c) of the GDPR must be as precise as possible. In particular, that right of access entails the ability of the data subject to obtain from the controller information about the specific recipients to whom the data have been or will be disclosed or, alternatively, to elect merely to request information concerning the categories of recipient.

44. Lastly, as regards the purpose of the GDPR, it should be pointed out that its purpose is, inter alia, as is apparent from recital 10 of that regulation, to ensure a high level of protection of natural persons within the European Union (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 207). In that regard, as the Advocate General observed, in essence, in point 14 of his Opinion, the general legal framework created by the GDPR implements the requirements arising from the fundamental right, protected by Article 8 of the Charter of Fundamental Rights of the European Union, to the protection of personal data, in particular the requirements expressly laid down in Article 8(2) thereof (see, to that effect, judgment of 9 March 2017, *Manni*, C-398/15, EU:C:2017:197, paragraph 40).

45. That objective supports the interpretation of Article 15(1) of the GDPR set out in paragraph 43 above.

46. Therefore, it also follows from the objective pursued by the GDPR that the data subject has the right to obtain from the controller information about the specific recipients to whom the personal data concerning him or her have been or will be disclosed.

47. That said, it must, lastly, be emphasised that, as is apparent from recital 4 of the GDPR, the right to the protection of personal data is not an absolute right. That right must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality, as the Court reaffirmed, in essence, in paragraph 172 of the judgment of 16 July 2020, Facebook Ireland and Schrems (C-311/18, EU:C:2020:559).

48. Accordingly, it may be accepted that, in specific circumstances, it is not possible to provide information about specific recipients. Therefore, the right of access may be restricted to information about categories of recipient if it is impossible to disclose the identity of specific recipients, in particular where they are not yet known.

49. In addition, it should be borne in mind that, under Article 12(5)(b) of the GDPR, the controller may, pursuant to the principle of responsibility referred to in Article 5(2) and recital 74 of that regulation, refuse to act on requests from a data subject where those requests are manifestly unfounded or excessive, it being specified that it is for the controller to demonstrate that those requests are unfounded or excessive.

50. In the present case, it is apparent from the request for a preliminary ruling that Österreichische Post refused the request made by RW under Article 15(1) of the GDPR to be informed of the identity of the recipients to whom Österreichische Post had disclosed the personal data concerning him. It will be for the referring court to determine whether, in the light of the circumstances of the main proceedings, Österreichische Post has demonstrated that that request is manifestly unfounded or excessive.

51. In the light of all the foregoing considerations, the answer to the question referred for a preliminary ruling is that Article 15(1)(c) of the GDPR must be interpreted as meaning that the data subject's right of access to personal data concerning him or her, provided for by that provision, entails, where those data have been or will be disclosed to recipients, an obligation on the part of the controller to provide the data subject with the actual identity of those recipients, unless it is impossible to identify those recipients or the controller demonstrates that the data subject's requests for access are manifestly

unfounded or excessive within the meaning of Article 12(5) of the GDPR, in which cases the controller may indicate to the data subject only the categories of recipient in question.

Costs

52. Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (First Chamber) hereby rules:

Article 15(1)(c) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), must be interpreted as meaning that the data subject's right of access to the personal data concerning him or her, provided for by that provision, entails, where those data have been or will be disclosed to recipients, an obligation on the part of the controller to provide the data subject with the actual identity of those recipients, unless it is impossible to identify those recipients or the controller demonstrates that the data subject's requests for access are manifestly unfounded or excessive within the meaning of Article 12(5) of Regulation 2016/679, in which cases the controller may indicate to the data subject only the categories of recipient in question.

[Signatures]

* Language of the case: German.

JUDGMENT OF THE COURT (First Chamber)

24 March 2022 (*)

(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Competence of the supervisory authority – Article 55(3) – Processing operations of courts acting in their judicial capacity – Concept – Making available to a journalist of documents arising from court proceedings containing personal data)

In Case C-245/20,

REQUEST for a preliminary ruling under Article 267 TFEU from the Rechtbank Midden-Nederland (District Court, Central Netherlands), made by decision of 29 May 2020, received at the Court on the same day, in the proceedings

X,

Z

v

Autoriteit Persoonsgegevens

THE COURT (First Chamber),

composed of K. Lenaerts, President of the Court, acting as President of the First Chamber, L. Bay Larsen, Vice-President of the Court, N. Jääskinen, J.-C. Bonichot (Rapporteur) and M. Safjan, Judges,

Advocate General: M. Bobek,

Registrar: L. Carrasco Marco, Administrator,

having regard to the written procedure and further to the hearing on 14 July 2021,

after considering the observations submitted on behalf of:

- X and Z, by S.A.J.T. Hoogendoorn, advocaat,
- the Autoriteit Persoonsgegevens, by G. Dictus and N.N. Bontje, advocaten,
- the Netherlands Government, by K. Bulterman and C.S. Schillemans, acting as Agents,
- the Spanish Government, by L. Aguilera Ruiz, acting as Agent,

– the Polish Government, by B. Majczyna, acting as Agent,
– the Portuguese Government, by L. Inez Fernandes and by P. Barros da Costa, L. Medeiros and I. Oliveira, acting as Agents,
– the Finnish Government, by H. Leppo, acting as Agent,
– the European Commission, by F. Erlbacher, H. Kranenborg and D. Nardi, acting as Agents,
after hearing the Opinion of the Advocate General at the sitting on 6 October 2021,
gives the following

Judgment

1. This request for a preliminary ruling concerns the interpretation of Article 55(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1).

2. The request has been made in proceedings between X and Z and the Autoriteit Persoonsgegevens (Data Protection Authority, Netherlands; ‘the AP’) concerning the access of journalists to personal data concerning them, included in a court file, at the hearing held before the Administrative Jurisdiction Division of the Raad van State (Council of State, Netherlands), in proceedings in which Z was a party and represented by X.

Legal context

European Union law

3. Recital 20 of Regulation 2016/679 states:

‘While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.’

4. Under Article 2 of that regulation:

'1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 [of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8, p. 1)] applies. Regulation [No 45/2001] and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.

...'

5. Article 4(2) of the said regulation defines the concept of 'processing' as:

'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.

6. Pursuant to Article 51(1) of the same regulation:

'Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ("supervisory authority").'

7. Last, Article 55 of Regulation 2016/679 provides as follows:

'1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.'

Netherlands law

8. For the purposes of implementing Regulation 2016/679, the Kingdom of the Netherlands adopted the wet houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming) (Law laying down the rules for the implementation of Regulation 2016/679 (Law implementing the General Data Protection Regulation)) of 16 May 2018 (Stb. 2018, No 144). Article 6 of that law entrusts the AP with the task of supervising compliance with Regulation 2016/679 in the Netherlands. None of the provisions of that law reproduces the exception provided for in Article 55(3) of Regulation 2016/679.

9. On 31 May 2018, the president of the Administrative Jurisdiction Division of the Raad van State (Council of State), the judicial administrations of the Centrale Raad van Beroep (Netherlands) and the College van Beroep voor het bedrijfsleven (Administrative Court of Appeal for Trade and Industry, Netherlands) adopted the regeling verwerking Persoonsgegevens bestuursrechtelijke colleges (Regulation on the processing of personal data in administrative courts). The latter act created the AVG-commissie bestuursrechtelijke colleges (Data Protection Commission for Administrative Law Tribunals, Netherlands; 'the GDPR Commission'). The latter is responsible for advising the president of the Administrative Jurisdiction Division of the Raad van State (Council of State), the judicial authorities of the Centrale Raad van Beroep (Higher Social Security and Civil Service Court) and the College van Beroep voor het bedrijfsleven (Administrative Court of Appeal for Trade and Industry) on the handling of complaints relating to respect of the rights guaranteed by Regulation 2016/679.

The dispute in the main proceedings and the question referred for a preliminary ruling

10. At the hearing held on 30 October 2018 before the Administrative Jurisdiction Division of the Raad van State (Council of State) in court proceedings in which Z was a party, represented by X, those two persons were approached by a journalist. During their conversation, X noted that that journalist had at his disposal documents from the case file concerned – including documents that he himself had drafted – showing his name and address in particular as well as Z's national identification number. That journalist told him that those documents had been made available to him under the right of access to the case file which the Administrative Jurisdiction Division of the Raad van State (Council of State) grants to journalists.

11. By letter of 21 November 2018, the president of the Administrative Jurisdiction Division of the Raad van State (Council of State) confirmed to X that that division was providing the media with a certain number of documents on pending cases. He informed him that, on the day of the hearing, the communication department of the Raad van State (Council of State) made available to the journalists present documents intended to enable them to follow hearings, namely a copy of the notice of appeal, a copy of the response and, where appropriate, a copy of the contested judicial decision, those documents being destroyed at the end of the day.

12. X and Z then requested the AP to adopt with regard to the Raad van State (Council of State) 'enforcement measures' in respect of the rules on the protection of personal data. By their requests – which were akin to complaints – they claimed that, by allowing journalists to have access to personal data concerning them, originating from the documents in a court file, the Raad van State (Council of State) had infringed Regulation 2016/679.

13. In response to those requests, the AP stated that, pursuant to Article 55(3) of Regulation 2016/679, it was not competent to supervise processing operations of the personal data concerned, carried out by the Raad van State (Council of State). It subsequently forwarded the requests of X and Z to the GDPR Commission, which in turn forwarded them to the president of the Administrative Jurisdiction Division of the Raad van State (Council of State).

14. The president of the Administrative Jurisdiction Division of the Raad van State (Council of State) assessed the requests of X and Z as complaints relating to his letter of 21 November 2018 and, after having consulted the GDPR Commission, formulated a new policy on access to documents from court files, which was published on the website of the Raad van State (Council of State).

15. X and Z challenged, before the referring court, the Rechtbank Midden-Nederland (District Court, Central Netherlands), the decision by which the AP had found itself not competent to hear their requests.

16. According to that court, giving a journalist access to the documents in a court file containing personal data and making them temporarily available to him or her constitutes 'processing' of personal data within the meaning of Article 4(2) of Regulation 2016/679, to which, in this case, X and Z had not consented. With a view to determining whether the AP was indeed not competent to rule on the requests of X and Z, the referring court questions, however, the interpretation that should be given to Article 55(3) of that regulation, which provides that the supervisory authority is not competent to supervise processing operations of courts 'acting in their judicial capacity'.

17. It is against this background that the Rechtbank Midden-Nederland (District Court, Central Netherlands) decided to stay the proceedings and to refer the following question to the Court of Justice for a preliminary ruling:

'Is Article 55(3) of [Regulation 2016/679] to be interpreted as meaning that "processing operations of courts acting in their judicial capacity" can be understood to mean the provision by a judicial authority of access to procedural documents containing personal data, where such access is granted by making copies of those procedural documents available to a journalist, as described in the order for reference?

– In answering that question, is it relevant whether the national supervisory authority's supervision of that form of data processing affects independent judicial decisions in specific cases?

– In answering that question, is it relevant that, according to the judicial authority, the nature and purpose of the data processing is to inform a journalist in order to enable the journalist to better report on a public hearing in court proceedings, thereby serving the interests of openness and transparency in the administration of justice?

– In answering that question, is it relevant whether there is any express legal basis for such data processing under national law?'

Consideration of the question referred

18. By its question, the referring court asks, in essence, whether Article 55(3) of Regulation 2016/679 must be interpreted as meaning that the fact that a court makes temporarily available to journalists documents from court proceedings containing personal data falls within the exercise, by that court, of its 'judicial capacity', within the meaning of that provision. In that context, it asks whether, in order

to answer that question, it is necessary to take into account the interference which the supervisory authority's exercise of its powers might have with the independence of the judges in the judgment of specific cases. It also asks whether it is necessary to take into consideration the nature and purpose of that making available of procedural documents – to enable journalists better to report on the course of court proceedings – or indeed whether that making available has an explicit legal basis in domestic law.

19. As a preliminary point, Z submits, first, that the question referred is hypothetical and that it is, as such, inadmissible. In his view, contrary to what the request for a preliminary ruling indicates, the processing of the data concerned is a matter not for the Administrative Jurisdiction Division of the Raad van State (Council of State), but for the latter's communication department, which is not a court or tribunal. The request is also vitiated by several other errors or inaccuracies, in particular as regards the status of the person who approached X and Z at the end of the hearing and the exact content of the requests forwarded by the AP to the president of the Administrative Jurisdiction Division of the Raad van State (Council of State).

20. In that regard, it should be recalled that, according to settled case-law, questions relating to EU law enjoy a presumption of relevance. The Court may refuse to rule on a question referred by a national court for a preliminary ruling only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose, where the Court does not have before it the legal or factual material necessary to give a useful answer to the questions submitted to it or where the problem is hypothetical (see judgment of 24 November 2020, *Openbaar Ministerie (Forgery of documents)*, C-510/19, EU:C:2020:953, paragraph 26 and the case-law cited).

21. What is more, in proceedings under Article 267 TFEU, which are based on a clear separation of functions between the national courts and the Court, the national court alone has jurisdiction to find and assess the facts in the case before it (see judgment of 26 April 2017, *Farkas*, C-564/15, EU:C:2017:302, paragraph 37 and the case-law cited).

22. It is apparent from the request for a preliminary ruling that the referring court is bound to take a position on the application of Article 55(3) of Regulation 2016/679 to the making available of procedural documents containing personal data at issue in the dispute in the main proceedings to determine whether or not the review of the lawfulness of the latter fell within the AP's competence. It follows moreover from the case-law cited in the preceding paragraph of the present judgment that Z cannot rebut the presumption enjoyed by the question asked by the referring court merely by

disputing the facts it mentions in its request, on which it is not for the Court to take a position. It follows that the plea of inadmissibility raised by Z must be rejected.

23. Second, Z submits that Article 55(3) of Regulation 2016/679 should be declared invalid by the Court on the ground that the lack of competence of the supervisory authority concerned as regards processing operations carried out by courts ‘acting in their judicial capacity’, provided for by that provision, is not coupled with the obligation for the Member States to lay down specific supervisory arrangements in respect of those processing operations, which he argues is contrary to the requirements arising from the right to an effective remedy.

24. However, such a line of argument cannot succeed since, as is apparent from recital 20 of Regulation 2016/679, the EU legislature, in enacting Article 55(3) of that regulation, did not intend to shield from all supervision processing operations carried out by courts ‘acting in their judicial capacity’, but merely ruled out the entrusting of the supervision of those operations to an external authority.

25. In order to answer the question asked by the national court, summarised in paragraph 18 above, it must first of all be noted that Article 2(1) of Regulation 2016/679 provides that that regulation applies to any ‘processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system’, without any distinction being made according to the identity of the person who carried out the processing concerned. It follows that, subject to the cases mentioned in Article 2(2) and (3) thereof, Regulation 2016/679 applies to processing operations carried out both by private persons and by public authorities, including, as recital 20 thereof indicates, judicial authorities, such as courts.

26. That reading is supported by the fact that several of the provisions of Regulation 2016/679 are subject to adjustments to take account of the specificities of the processing operations carried out by courts. That is particularly the case with Article 55(3) of that regulation, which excludes any competence of the supervisory authority in respect of processing operations carried out by courts ‘acting in their judicial capacity’.

27. Regulation 2016/679 can be distinguished in that regard from Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC (OJ 2003 L 41, p. 26), which does not apply to courts and tribunals (judgment of 15 April 2021, *Friends of the Irish Environment*, C-470/19, EU:C:2021:271, paragraphs 34 to 40).

28. In order to determine the scope of the concept of processing operations carried out by courts acting in their judicial capacity, within the meaning of Article 55(3) of Regulation 2016/679, it must be recalled that the interpretation of a provision of EU law must consider not only its wording, but also the context in which it occurs and the objectives pursued by the legislation of which it is part (see, to that effect, *inter alia*, judgment of 6 October 2020, *Jobcenter Krefeld*, C-181/19, EU:C:2020:794, paragraph 61 and the case-law cited).

29. In that regard, it is apparent from Article 55 of Regulation 2016/679 that the purpose of that article is to define competence in matters of supervision of the processing of personal data and, in particular, to delimit the competence vested in the national supervisory authority.

30. Article 55(3) of Regulation 2016/679 thus provides that processing operations carried out by courts 'acting in their judicial capacity' fall outside the competence of that supervisory authority.

31. Recital 20 of Regulation 2016/679, in the light of which that Article 55(3) must be read, states that it should be possible to entrust supervision of processing operations carried out by the courts 'acting in their judicial capacity' to specific bodies within the judicial system of the Member State concerned rather than to the supervisory authority under the authority of that Member State, in order to 'safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making'.

32. As the Advocate General observed in points 80 and 81 of his Opinion, it is apparent from the very wording of recital 20 of Regulation 2016/679, and in particular from the use of the expression 'including', that the scope of the objective pursued by Article 55(3) of that regulation, consisting in safeguarding the independence of the judiciary in the performance of its judicial tasks, cannot be confined solely to guaranteeing the independence of the judges in the adoption of a given judicial decision.

33. After all, safeguarding the independence of the judiciary presupposes, in general, that judicial functions are exercised wholly autonomously, without the courts being subject to any hierarchical constraint or subordinate relationship and without taking orders or instructions from any source whatsoever, thus being protected from any external intervention or pressure liable to jeopardise the independent judgment of their members and to influence their decisions. Observance of the guarantees of independence and impartiality necessary under EU law requires rules in order to dispel any reasonable doubt in the minds of individuals as to the imperviousness of the body in question to external factors and its neutrality with respect to the interests concerned (see, to that effect, *inter alia*, judgments of 27 February 2018, *Associação Sindical dos Juízes Portugueses*, C-64/16, EU:C:2018:117,

paragraph 44; of 25 July 2018, Minister for Justice and Equality (Deficiencies in the system of justice), C-216/18 PPU, EU:C:2018:586, paragraph 63; of 24 June 2019, Commission v Poland (Independence of the Supreme Court), C-619/18, EU:C:2019:531, paragraph 72; and of 21 December 2021, Euro Box Promotion and Others, C-357/19, C-379/19, C-547/19, C-811/19, C-840/19, EU:C:2021:1034, paragraph 225).

34. Accordingly, the reference in Article 55(3) of Regulation 2016/679 to processing operations carried out by courts 'acting in their judicial capacity' must be understood, in the context of that regulation, as not being limited to the processing of personal data carried out by courts in specific cases, but as referring, more broadly, to all processing operations carried out by courts in the course of their judicial activity, such that those processing operations whose supervision by the supervisory authority would be likely, whether directly or indirectly, to have an influence on the independence of their members or to weigh on their decisions are excluded from that authority's competence.

35. In that regard, while the nature and purpose of the processing carried out by a court relate principally to the examination of the lawfulness of that processing, they may constitute indicia that that processing falls within the exercise, by that court, of its 'judicial capacity'.

36. On the other hand, the question whether the processing has an explicit legal basis in domestic law or whether the personal data contained therein may lawfully be disclosed to third parties relates exclusively to the examination of the lawfulness of the processing, those elements being irrelevant to determining whether the supervisory authority is competent to ensure the supervision of that processing operation on the basis of Article 55 of Regulation 2016/679.

37. As regards processing such as that at issue in the main proceedings, it must be held that, without prejudice to compliance with the substantive obligations laid down by Regulation 2016/679, the processing of personal data carried out by courts in the context of their communication policy on cases before them, such as those consisting in the temporary making available to journalists of documents from a court case file in order to enable them to cover it in the media, *inter alia*, falls outside the competence of the supervisory authority, pursuant to Article 55(3) of that regulation.

38. The determination, having regard to the subject matter and context of a given case, of the information from a court case file that may be provided to journalists in order to enable them to report on the course of court proceedings or to shed light on one or other aspect of a decision delivered is clearly linked to the exercise, by such courts, of their 'judicial capacity', the supervision of which by an external authority would be liable to undermine, in general, the independence of the judiciary.

39. In the light of all the foregoing considerations, the answer to the question referred is that Article 55(3) of Regulation 2016/679 must be interpreted as meaning that the fact that a court makes temporarily available to journalists documents from court proceedings containing personal data in order to enable them better to report on the course of those proceedings falls within the exercise, by that court, of its 'judicial capacity', within the meaning of that provision.

Costs

40. Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (First Chamber) hereby rules:

Article 55(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) must be interpreted as meaning that the fact that a court makes temporarily available to journalists documents from court proceedings containing personal data in order to enable them better to report on the course of those proceedings falls within the exercise, by that court, of its 'judicial capacity', within the meaning of that provision.

[Signatures]

* Language of the case: Dutch.

ABAD - Meta Platforms Ireland (Case C-319/20)

Judgment in Case C-319/20

Meta Platforms Ireland

Consumer protection associations may bring representative actions against infringements of personal data protection

Such an action may be brought independently of the specific infringement of a data subject's right to the protection of his or her personal data and in the absence of a mandate to that effect

Meta Platforms Ireland, formerly Facebook Ireland Limited, is the controller of the personal data of users of the online social network Facebook in the European Union.

The Federal Union of Consumer Organisations and Associations (Germany) brought an action for an injunction against Meta Platforms Ireland, alleging that it had infringed, in the context of making available to users free games provided by third parties, 1 rules on the protection of personal data, the combat of unfair commercial practices and consumer protection.

The Federal Court of Justice (Germany) observes that the Federal Union's action is well founded, but it has doubts as to its admissibility.

That court asks whether, following the entry into force of the General Data Protection Regulation (GDPR), 2 a consumer protection association, such as the Federal Union, still has standing to bring proceedings in the civil courts against infringements of that regulation, independently of the specific infringement of rights of individual data subjects and without being mandated to do so by those data subjects. Moreover, it observes that it can be inferred from the GDPR that it is principally for the supervisory authorities to verify the application of the provisions of that regulation.

By today's judgment, the Court finds that the GDPR does not preclude national legislation which allows a consumer protection association to bring legal proceedings, in the absence of a mandate conferred on it for that purpose and independently of the infringement of specific rights of the data subjects, against the person allegedly responsible for an infringement of the laws protecting personal data, on the basis of the infringement of the prohibition of unfair commercial practices, a breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions, where the data processing concerned is liable to affect the rights that identified or identifiable natural persons derive from that regulation.

As a preliminary point, the Court notes that the GDPR brings about harmonisation of national legislation on the protection of personal data which is, in principle, full. However, certain provisions of the GDPR make it possible for Member States to lay down additional rules which leave them a margin of discretion as to the manner in which those provisions may be implemented, provided that the national rules adopted do not undermine the content and objectives of that regulation. In that regard, the Member States also have the option to provide for a representative action mechanism against the person allegedly responsible for an infringement of the laws protecting personal data, while setting out a number of requirements which must be complied with.

The Court notes first that a consumer protection association, such as the Federal Union, falls within the scope of the concept of a “body that has standing to bring proceedings” for the purposes of the GDPR in that it pursues a public interest objective consisting in safeguarding the rights of consumers. The infringement of the rules on consumer protection and unfair commercial practices may be related to the infringement of a rule on the protection of personal data.

Next, the Court states that the bringing of a representative action presupposes that such an association, independently of any mandate conferred on it, ‘considers’ that the rights of a data subject laid down in the GDPR have been infringed as a result of the processing of his or her personal data, without it being necessary to identify, individually and beforehand, the person specifically concerned by that processing and to allege the existence of a specific infringement of the rights deriving from the data protection rules.

Such an interpretation is consistent with the objective pursued by the GDPR consisting in, in particular, ensuring a high level of protection of personal data.

Finally, according to the Court, the GDPR does not preclude national provisions which provide for the bringing of representative actions against infringements of the rights conferred by that regulation through, as the case may be, rules intended to protect consumers or combat unfair commercial practices.

[1] When consulting the App Center of some of those games, an indication appears informing the user that the use of the application concerned enables the gaming company to obtain a certain amount of personal data and, by that use, permission is given for it to publish data on behalf of that user. That use implies that the user accepts the general terms and conditions of the application and its data protection policy.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

JUDGMENT OF THE COURT (Third Chamber)

28 April 2022 (*)

(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 80 – Representation of the data subjects by a not-for-profit association – Representative action brought by a consumer protection association in the absence of a mandate and independently of the infringement of specific rights of a data subject – Action based on the prohibition of unfair commercial practices, the infringement of a consumer protection law or the prohibition of the use of invalid general terms and conditions)

In Case C-319/20,

REQUEST for a preliminary ruling under Article 267 TFEU from the Bundesgerichtshof (Federal Court of Justice, Germany), made by decision of 28 May 2020, received at the Court on 15 July 2020, in the proceedings

Meta Platforms Ireland Limited, formerly Facebook Ireland Limited,

v

Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.,

THE COURT (Third Chamber),

composed of A. Prechal, President of the Second Chamber, acting as President of the Third Chamber, J. Passer, F. Biltgen, L.S. Rossi (Rapporteur) and N. Wahl, Judges,

Advocate General: J. Richard de la Tour,

Registrar: M. Krausenböck, Administrator,

having regard to the written procedure and further to the hearing on 23 September 2021,

after considering the observations submitted on behalf of:

– Meta Platforms Ireland Limited, by H.-G. Kamann, M. Braun and H. Frey, Rechtsanwälte, and by V. Wettner, Rechtsanwältin,

– Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V., by P. Wassermann, Rechtsanwalt,

– for the German government, by D. Klebs and J. Möller, acting as Agents,

– the Austrian Government, by A. Posch and Dr G. Kunnert and J. Schmoll, acting as Agents,
– the Portuguese Government, by L. Inez Fernandes and C. Vieira Guerra, P. Barros da Costa and L. Medeiros, acting as Agents,
– the European Commission, initially by F. Erlbacher, H. Kranenborg and D. Nardi, and subsequently by F. Erlbacher and H. Kranenborg, acting as Agents,
after hearing the Opinion of the Advocate General at the sitting on 2 December 2021,

gives the following

Judgment

1. This request for a preliminary ruling concerns the interpretation of Article 80(1) and (2) and Article 84(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1) ('the GDPR').

2. The request has been made in proceedings between Meta Platforms Ireland Limited, formerly Facebook Ireland Limited, whose registered office is in Ireland, and Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. (Federal Union of Consumer Organisations and Associations, Germany) ('the Federal Union') concerning the infringement by Meta Platforms Ireland of the German legislation on the protection of personal data constituting, at the same time, an unfair commercial practice, an infringement of a law relating to consumer protection and a breach of the prohibition of the use of invalid general terms and conditions.

Legal context

European Union law

The GDPR

3. Recitals 9, 10, 13 and 142 of the GDPR state:

'(9) The objectives and principles of Directive [95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)] remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons,

in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive [95/46].

(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. ...

...

(13) In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. ...

...

(142) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. A Member State may provide for such a body, organisation or association to have the right to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject

have been infringed as a result of the processing of personal data which infringes this Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate.'

4. Article 1 of that regulation, entitled 'Subject matter and objectives', provides, in paragraph 1 thereof:

'This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.'

5. Article 4(1) of the GDPR provides:

'For the purposes of this Regulation:

(1) "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'

6. Chapter III of the GDPR, which includes Articles 12 to 23, is entitled 'Rights of the data subject'.

7. Article 12 of that regulation, headed 'Transparent information, communication and modalities for the exercise of the rights of the data subject', lay down, in paragraph 1 thereof:

'The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.'

8. Article 13 of the GDPR, entitled 'Information to be provided where personal data are collected from the data subject', provides, in paragraph 1(c) and (e) thereof:

'Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

...

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

...

(e) the recipients or categories of recipients of the personal data, if any ...'

9. Chapter VIII of that regulation, which comprises Articles 77 to 84, is entitled 'Remedies, liability and penalties'.

10. Article 77 of the GDPR, headed 'Right to lodge a complaint with a supervisory authority', provides, in paragraph 1 thereof:

'Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.'

11. Article 78 of the GDPR, headed 'Right to an effective judicial remedy against a supervisory authority', lays down, in paragraph 1 thereof:

'Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.'

12. Article 79 of the GDPR, headed 'Right to an effective judicial remedy against a controller or processor', provides, in paragraph 1 thereof:

'Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.'

13. Article 80 of the GDPR, entitled 'Representation of data subjects', is worded as follows:

'1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to

exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.'

14. Article 82 of that regulation, headed 'Right to compensation and liability', provides, in paragraph 1 thereof:

'Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.'

15. Article 84 of the GDPR, entitled 'Penalties', lays down, in paragraph 1 thereof:

'Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.'

Directive 2005/29/EC

16. The objective of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (OJ 2005 L 149, p. 22) is, according to Article 1 thereof, to contribute to the proper functioning of the internal market and achieve a high level of consumer protection by approximating the laws, regulations and administrative provisions of the Member States on unfair commercial practices harming consumers' economic interests.

17. Under Article 5 of Directive 2005/29, entitled 'Prohibition of unfair commercial practices':

'1. Unfair commercial practices shall be prohibited.

2. A commercial practice shall be unfair if:

(a) it is contrary to the requirements of professional diligence,

and

(b) it materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers.

...

5. Annex I contains the list of those commercial practices which shall in all circumstances be regarded as unfair. ...'

18. Article 11(1) of that directive, entitled 'Enforcement', provides:

'Member States shall ensure that adequate and effective means exist to combat unfair commercial practices in order to enforce compliance with the provisions of this Directive in the interest of consumers.

Such means shall include legal provisions under which persons or organisations regarded under national law as having a legitimate interest in combating unfair commercial practices, including competitors, may:

(a) take legal action against such unfair commercial practices;

and/or

(b) bring such unfair commercial practices before an administrative authority competent either to decide on complaints or to initiate appropriate legal proceedings.

It shall be for each Member State to decide which of these facilities shall be available and whether to enable the courts or administrative authorities to require prior recourse to other established means of dealing with complaints, including those referred to in Article 10. These facilities shall be available regardless of whether the consumers affected are in the territory of the Member State where the trader is located or in another Member State.

...'

19. Annex I to Directive 2005/29, which contains the list of unfair commercial practices in all circumstances, provides, in point 26 thereof:

'Making persistent and unwanted solicitations by telephone, fax, e-mail or other remote media except in circumstances and to the extent justified under national law to enforce a contractual obligation. This is without prejudice to ... [Directive 95/46] ...'

Directive 2009/22/EC

20. Under Article 1 of Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests (OJ 2009 L 110, p. 30), entitled 'Scope':

'1. The purpose of this Directive is to approximate the laws, regulations and administrative provisions of the Member States relating to actions for an injunction referred to in Article 2 aimed at the protection of the collective interests of consumers included in the Directives listed in Annex I, with a view to ensuring the smooth functioning of the internal market.

2. For the purposes of this Directive, an infringement means any act contrary to the Directives listed in Annex I as transposed into the internal legal order of the Member States which harms the collective interests referred to in paragraph 1.'

21. Article 7 of Directive 2009/22, entitled 'Provisions for wider action', is worded as follows:

'This Directive shall not prevent Member States from adopting or maintaining in force provisions designed to grant qualified entities and any other person concerned more extensive rights to bring action at national level.'

22. Annex I to Directive 2009/22 contains the list of EU directives referred to in Article 1 thereof. Point 11 of that annex refers to Directive 2005/29.

Directive (EU) 2020/1828

23. Recitals 11, 13 and 15 of Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ 2020 L 409, p. 1) state:

'(11) This Directive should not replace existing national procedural mechanisms for the protection of collective or individual consumer interests. Taking into account their legal traditions, it should leave it to the discretion of the Member States whether to design the procedural mechanism for representative actions required by this Directive as part of an existing or as part of a new procedural mechanism for collective injunctive measures or redress measures, or as a distinct procedural mechanism, provided that at least one national procedural mechanism for representative actions complies with this Directive. ... If there were procedural mechanisms in place at national level in

addition to the procedural mechanism required by this Directive, the qualified entity should be able to choose which procedural mechanism to use.

...

(13) The scope of this Directive should reflect recent developments in the field of consumer protection. Since consumers now operate in a wider and increasingly digitalised marketplace, achieving a high level of consumer protection requires that areas such as data protection, financial services, travel and tourism, energy, and telecommunications be covered by the Directive, in addition to general consumer law. ...

...

(15) This Directive should be without prejudice to the legal acts listed in Annex I and therefore it should not change or extend the definitions laid down in those legal acts or replace any enforcement mechanism that those legal acts might contain. For example, the enforcement mechanisms provided for in or based on [the GDPR] could, where applicable, still be used for the protection of the collective interests of consumers.'

24. Article 2 of that directive, headed 'Scope', provides, in paragraph 1 thereof:

'This Directive applies to representative actions brought against infringements by traders of the provisions of Union law referred to in Annex I, including such provisions as transposed into national law, that harm or may harm the collective interests of consumers. This Directive is without prejudice to the provisions of Union law referred to in Annex I. ...'

25. Article 24(1) of that directive, entitled 'Transposition', provides:

Member States shall adopt and publish, by 25 December 2022, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof.

They shall apply those measures from 25 June 2023.

...'

26. Annex I to Directive 2020/1828, which contains the list of provisions of EU law referred to in Article 2(1) thereof, refers to the GDPR in point 56 thereof.

German law

Law on injunctions

27. Under Paragraph 2 of the Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen (Unterlassungsklagengesetz – UKlaG) (Law on injunctions against infringements of consumer law and other infringements) of 26 November 2001 (BGBl. 2001 I, p. 3138), in the version applicable to the dispute in the main proceedings (‘the Law on Injunctions’):

‘(1) Any person who infringes rules in place to protect consumers (consumer protection laws), other than in the application or recommendation of general terms and conditions, may be subject to an order to cease and desist or a prohibition order in the interest of consumer protection. ...

(2) For the purposes of this provision, “consumer protection laws” means, in particular:

...

11. the rules defining lawfulness

(a) of the collection of personal data of a consumer by an undertaking or

(b) the processing or use of personal data which have been collected by a business in relation to a consumer,

where the data are collected, processed or used for the purposes of publicity, market and opinion research, use by an information agency, a personality and usage profile establishment, of any other data business or for similar commercial purposes.’

28. The Bundesgerichtshof (Federal Court of Justice, Germany) states that, under point 1 of the first sentence of Paragraph 3(1) of the Law on Injunctions, bodies with standing to bring proceedings, within the meaning of Paragraph 4 of that law, may, first, in accordance with Paragraph 1 of that law, seek an injunction against the use of invalid general terms and conditions under Paragraph 307 of the Bürgerliches Gesetzbuch (Civil Code) and, second, seek an injunction against infringements of consumer protection law, within the meaning of Paragraph 2(2) of that law.

Law against unfair competition

29. Paragraph 3(1) of the Gesetz gegen den unlauteren Wettbewerb (Law against unfair competition) of 3 July 2004 (BGBl. 2004 I, p. 1414), in the version applicable to the main proceedings (‘the Law against unfair competition’), provides:

‘Unfair commercial practices shall be prohibited.’

30. Paragraph 3a of the Law against unfair competition is worded as follows:

‘A person shall be considered to be acting unfairly where he or she infringes a statutory provision that is also intended to regulate market behaviour in the interests of market participants and the infringement is liable to have a significantly adverse effect on the interests of consumers, other market participants or competitors.’

31. Paragraph 8 of the Law against unfair competition lays down:

‘(1) Any commercial practice which is unlawful under Paragraph 3 or Paragraph 7 may give rise to an order to cease and desist and, in the event of recurrence, an order to refrain or a prohibition order.

...

...

(3) Applications for the injunctions referred to in subparagraph (1) may be made:

...

3. by qualified entities which provide evidence that they are included in the list of qualified entities, in accordance with Paragraph 4 of the [Law on injunctions] ...’

The Law on Electronic Media

32. The Bundesgerichtshof (Federal Court of Justice) states that Paragraph 13(1) of the Telemediengesetz (‘the Law on Electronic Media’) of 26 February 2007 (BGB1. 2007 I, p. 179) was applicable until the GDPR came into force. As from that date, that provision has been replaced by Articles 12 to 14 of the GDPR.

33. Under the first sentence of Paragraph 13(1) of the Law on Electronic Media:

‘From the outset of the use, the service provider shall inform the user in a universally comprehensible form of the mode, the extent and the purpose of the collection and use of personal data and of the processing of his or her data in States which do not come within the scope of [Directive 95/46] in so far as he or she has not already been so informed.’

The dispute in the main proceedings and the question referred for a preliminary ruling

34. Meta Platforms Ireland, which manages the provision of services of the online social network Facebook in the European Union, is the controller of the personal data of users of that social network in the European Union. Facebook Germany GmbH, which has its registered office in Germany, promotes the sale of advertising space at the internet address www.facebook.de. The Facebook internet platform contains, inter alia, at the internet address www.facebook.de, an area called ‘App-Zentrum’ (‘App Center’) on which Meta Platforms Ireland makes available to users free games

provided by third parties. When consulting the App Center of some of those games, an indication appears informing the user that the use of the application concerned enables the gaming company to obtain a certain amount of personal data and, by that use, permission is given for it to publish data on behalf of that user, such as his or her score and other information. The consequence of that use is that the user accepts the general terms and conditions of the application and its data protection policy. In addition, in the case of a specific game, it is stated that the application has permission to post the status, photos and other information on behalf of that user.

35. The Federal Union, a body which has standing under Paragraph 4 of the Law on Injunctions, considers that the information provided by the games concerned in the App Center is unfair, in particular in terms of the failure to comply with the legal requirements which apply to the obtention of valid consent from the user under the provisions governing data protection. Moreover, it considers that the statement that the application has permission to publish certain personal information of the user on his or her behalf constitutes a general condition which unduly disadvantages the user.

36. In that context, the Federal Union brought an action for an injunction before the Landgericht Berlin (Regional Court, Berlin, Germany) against Meta Platforms Ireland based on Paragraph 3a of the Law against unfair competition, the first sentence of point 11 of Paragraph 2(2) of the Law on Injunctions and the Civil Code. It brought that action independently of a specific infringement of a data subject's right to protection of his or her data and without being mandated to do so by such a person.

37. The Landgericht Berlin (Regional Court, Berlin) ruled against Meta Platforms Ireland, in accordance with the form of order sought by the Federal Union. The appeal brought by Meta Platforms Ireland before the Kammergericht Berlin (Higher Regional Court, Berlin, Germany) was dismissed. Meta Platforms Ireland then brought an appeal on a point of law (Revision) before the referring court against the dismissal decision adopted by the Kammergericht Berlin (Higher Regional Court, Berlin).

38. The referring court considers that the action brought by the Federal Union is well founded, in so far as Meta Platforms Ireland infringed Paragraph 3a of the Law against unfair competition and the first sentence of point 11 of Paragraph 2(2) of the Law on Injunctions, and used an invalid general condition, within the meaning of Paragraph 1 of the Law on Injunctions.

39. However, that court has doubts as to the admissibility of the action brought by the Federal Union. It takes the view that it cannot be ruled out that the Federal Union, which did indeed have standing to bring proceedings on the date on which it brought the action – on the basis of Paragraph 8(3) of the Law against unfair competition and point 1 of the first sentence of Paragraph 3(1) of the Law on

Injunctions – lost that status during the proceedings, following the entry into force of the GDPR and, in particular, Article 80(1) and (2) and Article 84(1) thereof. If that were the case, the referring court would have to uphold the appeal on a point of law brought by Meta Platforms Ireland and dismiss the action of the Federal Union, since, under German procedural law, standing to bring proceedings must endure until the end of the proceedings at last instance.

40. According to the referring court, the answer in that regard is not clear from the assessment of the wording, scheme and objectives of the provisions of the GDPR.

41. As regards the wording of the provisions of the GDPR, the referring court notes that the existence of standing to bring proceedings of not-for-profit bodies, organisations or associations which have been properly constituted in accordance with the law of a Member State, pursuant to Article 80(1) of the GDPR, presupposes that the data subject has mandated a body, organisation or association for it to exercise on his or her behalf the rights referred to in Articles 77 to 79 of the GDPR and the right to compensation referred to in Article 82 of the GDPR where the law of a Member State so provides.

42. The referring court states that standing to bring proceedings under Paragraph 8(3)(3) of the Law against unfair competition does not cover such an action brought on the basis of a mandate and on behalf of a data subject in order to assert his or her personal rights. On the contrary, it confers on an association, by virtue of a right peculiar to it and stemming from Paragraph 3(1) and Paragraph 3a of the Law against unfair competition, standing to bring proceedings on an objective basis against infringements of the provisions of the GDPR, independently of the infringement of specific rights of data subjects and of a mandate conferred by them.

43. In addition, the referring court observes that Article 80(2) of the GDPR does not provide for an association's standing to bring proceedings in order to secure the application, objectively, of the law on the protection of personal data since that provision presupposes that the rights of a data subject laid down in the GDPR have actually been infringed as a result of the processing of specific data.

44. Furthermore, an association's standing to bring proceedings, such as that provided for in Paragraph 8(3) of the Law against unfair competition, cannot result from Article 84(1) of the GDPR, under which the Member States are to lay down the rules on other penalties applicable to infringements of that regulation and are to take all measures necessary to ensure that they are implemented. The standing of an association, such as that referred to in Paragraph 8(3) of the Law against unfair competition, cannot be regarded as constituting a 'penalty' within the meaning of that provision of the GDPR.

45. As regards the scheme of the provisions of the GDPR, the referring court considers that it may be inferred from the fact that it harmonised, *inter alia*, the powers of the supervisory authorities that it is principally for those authorities to verify the application of the provisions of that regulation. However, the expression ‘without prejudice to any other ... remedy’, which appears in Article 77(1), Article 78(1) and (2) and Article 79(1) of the GDPR, may undermine the argument that oversight of the application of the law is exhaustively governed by that regulation.

46. As regards the objective of the provisions of the GDPR, the referring court notes that the effectiveness of that regulation may support an argument in favour of associations having standing to bring proceedings on the basis of competition law, in accordance with Paragraph 8(3)(3) of the Law against unfair competition, independently of the infringement of specific rights of data subjects, since that would allow an additional opportunity to supervise the application of the law to remain, in order to ensure as high a level as possible of protection of personal data, in accordance with recital 10 of the GDPR. Nonetheless, accepting that associations have standing to bring proceedings under competition law may be considered to run counter to the objective of harmonisation pursued by the GDPR.

47. In the light of those considerations, the Bundesgerichtshof (Federal Court of Justice) decided to stay the proceedings and to refer the following question to the Court of Justice for a preliminary ruling:

‘Do the rules in Chapter VIII, in particular in Article 80(1) and (2) and Article 84(1), of [the GDPR] preclude national rules which – alongside the powers of intervention of the supervisory authorities responsible for monitoring and enforcing the Regulation and the options for legal redress for data subjects – empower, on the one hand, competitors and, on the other, associations, entities and chambers entitled under national law, to bring proceedings for breaches of [the GDPR], independently of the infringement of specific rights of individual data subjects and without being mandated to do so by a data subject, against [the person responsible for that infringement] before the civil courts on the basis of the prohibition of unfair commercial practices or breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions?’

Consideration of the question referred

48. As a preliminary point, it should be noted that, as is apparent, in particular, from paragraph 36 and from paragraphs 41 to 44 above, the dispute in the main proceedings is between a consumer protection association, such as the Federal Union, and Meta Platforms Ireland and concerns the question whether such an association may bring proceedings against that company in the absence of

a mandate granted to it for that purpose and independently of the infringement of specific rights of the data subjects.

49. In those circumstances, as the Commission correctly observed in its written observations, the answer to the question referred for a preliminary ruling depends solely on the interpretation of Article 80(2) of the GDPR, since the provisions of Article 80(1) of the GDPR and of Article 84 of the GDPR are not relevant in the present case. First, the application of Article 80(1) of the GDPR presupposes that the data subject has mandated the not-for-profit body, organisation or association referred to in that provision to take on his or her behalf the legal measures provided for in Articles 77 to 79 of the GDPR. It is common ground that that is not the case in the main proceedings, since the Federal Union acts independently of any mandate from a data subject. Second, it is common ground that Article 84 of the GDPR concerns the administrative and criminal penalties applicable to infringements of that regulation, which is also not at issue in the main proceedings.

50. Furthermore, it should be noted that the case in the main proceedings does not raise the question of a competitor's standing to bring proceedings. Consequently, it is only necessary to answer the part of the question which relates to the standing to bring proceedings of associations, bodies and chambers authorised under national law, referred to in Article 80(2) of the GDPR.

51. It follows that the question referred by the referring court must be understood as seeking to ascertain, in essence, whether Article 80(2) of the GDPR must be interpreted as precluding national legislation which allows a consumer protection association to bring legal proceedings, in the absence of a mandate conferred on it for that purpose and independently of the infringement of specific rights of a data subject, against the person allegedly responsible for an infringement of the laws protecting personal data, by alleging infringement of the prohibition of unfair commercial practices, consumer protection legislation or the prohibition of the use of invalid general terms and conditions.

52. In order to answer that question, it must be borne in mind that, as is apparent from recital 10 of the GDPR, that regulation seeks, *inter alia*, to ensure consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data throughout the European Union and to remove obstacles to flows of personal data within the European Union.

53. In that context, Chapter VIII of that regulation governs, *inter alia*, the legal remedies enabling the protection of the data subject's rights where his or her personal data have been the subject of processing that is allegedly contrary to the provisions of that regulation. The protection of those rights

may thus be sought either directly by the data subject or by an authorised entity, whether there is a mandate to that end or not, pursuant to Article 80 of the GDPR.

54. Thus, first of all, the data subject has the right to lodge a complaint himself or herself with a supervisory authority of a Member State or to bring an action before the national civil courts. More specifically, that data subject has the right to lodge a complaint with a supervisory authority, in accordance with Article 77 of the GDPR, the right to an effective judicial remedy against a supervisory authority, pursuant to Article 78 of the GDPR, the right to an effective judicial remedy against a controller or processor, provided for in Article 79 of the GDPR, and the right to obtain from the controller or processor compensation for the harm suffered, under Article 82 of the GDPR.

55. Next, in accordance with Article 80(1) of the GDPR, the data subject has the right to mandate a not-for-profit body, organisation or association, subject to certain conditions, to lodge a complaint on his or her behalf or to exercise the rights referred to in the articles referred to above on his or her behalf.

56. In accordance with Article 80(2) of the GDPR, Member States may provide that any body, organisation or association, independently of a data subject's mandate granted by a data subject, has the right to lodge, in the Member State in question, a complaint with the supervisory authority, pursuant to Article 77 of that regulation, and to exercise the rights referred to in Articles 78 and 79 thereof, if it considers that the rights of a data subject under that regulation have been infringed as a result of the processing of personal data concerning him or her.

57. In that regard, it should be noted that, as is apparent from Article 1(1) of the GDPR, read in the light, *inter alia*, of recitals 9, 10 and 13 thereof, that regulation seeks to ensure the harmonisation of national legislation on the protection of personal data which is, in principle, full. However, the provisions of that regulation make it possible for Member States to lay down additional, stricter or derogating national rules, which leave them a margin of discretion as to the manner in which those provisions may be implemented ('opening clauses').

58. In that regard, it must be recalled that, according to the Court's settled case-law, pursuant to Article 288 TFEU and by virtue of the very nature of regulations and of their function in the system of sources of EU law, the provisions of those regulations generally have immediate effect in the national legal systems without it being necessary for the national authorities to adopt measures of application. Nonetheless, some of those provisions may necessitate, for their implementation, the adoption of measures of application by the Member States (judgment of 15 June 2021, *Facebook Ireland and Others*, C-645/19, EU:C:2021:483, paragraph 110 and the case-law cited).

59. That is the case, *inter alia*, of Article 80(2) of the GDPR, which leaves the Member States a discretion with regard to its implementation. Thus, in order for it to be possible to proceed with the representative action without a mandate provided for in that provision, Member States must make use of the option made available to them by that provision to provide in their national law for that mode of representation of data subjects.

60. However, as the Advocate General observed, in points 51 and 52 of his Opinion, when the Member States exercise the option granted to them by such an opening clause, they must use their discretion under the conditions and within the limits laid down by the provisions of the GDPR and must therefore legislate in such a way as not to undermine the content and objectives of that regulation.

61. In this instance, as was confirmed by the German Government at the hearing in the present case, the German legislature did not adopt, following the entry into force of the GDPR, particular provisions specifically designed to implement Article 80(2) of that regulation in its national law. The national legislation at issue in the main proceedings, adopted in order to transpose Directive 2009/22, already allows consumer protection associations to bring legal proceedings against the person allegedly responsible for an infringement of the laws protecting personal data. That government observes, moreover, that, in its judgment of 29 July 2019, *Fashion ID* (C-40/17, EU:C:2019:629), concerning the interpretation of the provisions of Directive 95/46, the Court held that those provisions do not preclude that national legislation.

62. In those circumstances, as the Advocate General observed in point 60 of his Opinion, it is necessary, in essence, to ascertain whether the national rules at issue in the main proceedings fall within the scope of the discretion conferred on each Member State by Article 80(2) of the GDPR and thus to interpret that provision taking into account its wording and the scheme and objectives of that regulation.

63. In that regard, it should be noted that Article 80(2) of the GDPR allows Member States to provide for a representative action mechanism against the person allegedly responsible for an infringement of the laws protecting personal data, while setting out a number of requirements at the level of the personal and material scope which must be complied with for that purpose.

64. As regards, in the first place, the personal scope of such a mechanism, standing to bring proceedings is conferred on a body, organisation or association which meets the criteria set out in Article 80(1) of the GDPR. In particular, that provision refers to 'not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has

statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data'.

65. It must be held that a consumer protection association, such as the Federal Union, may fall within the scope of that concept in that it pursues a public interest objective consisting in safeguarding the rights and freedoms of data subjects in their capacity as consumers, since the attainment of such an objective is likely to be related to the protection of the personal data of those persons.

66. The infringement of the rules intended to protect consumers or to combat unfair commercial practices – infringement which a consumer protection association, such as the Federal Union, aims to prevent and penalise, inter alia by recourse to actions for an injunction provided for in the applicable national legislation – may be related, as in the present case, to the infringement of the rules on the protection of personal data of those consumers.

67. As regards, in the second place, the material scope of that mechanism, the exercise of the representative action provided for in Article 80(2) of the GDPR by an entity meeting the conditions referred to in paragraph 1 of that article presupposes that that entity, independently of any mandate conferred on it, 'considers that the rights of a data subject under [that r]egulation have been infringed as a result of the processing' of his or her personal data.

68. In that regard, it must be stated, first, that for the purposes of bringing a representative action, within the meaning of Article 80(2) of the GDPR, such an entity cannot be required to carry out a prior individual identification of the person specifically concerned by data processing that is allegedly contrary to the provisions of the GDPR.

69. It is sufficient to note that the concept of 'data subject', within the meaning of Article 4(1) of that regulation, covers not only an 'identified natural person', but also an 'identifiable natural person', namely a natural person 'who can be identified', directly or indirectly, by reference to an identifier such as, inter alia, a name, an identification number, location data or an online identifier. In those circumstances, the designation of a category or group of persons affected by such treatment may also be sufficient for the purpose of bringing such representative action.

70. Secondly, under Article 80(2) of the GDPR, the bringing of a representative action is also not subject to the existence of a specific infringement of the rights which a person derives from the data protection rules.

71. As is apparent from the very wording of that provision, recalled in paragraph 67 of the present judgment, the lodging of a representative action presupposes only that the entity concerned

'considers' that the rights of a data subject laid down in that regulation have been infringed as a result of the processing of his or her personal data and therefore alleges the existence of data processing that is contrary to the provisions of that regulation.

72. It follows that, in order to recognise that such an entity has standing to bring proceedings under that provision, it is sufficient to claim that the data processing concerned is liable to affect the rights which identified or identifiable natural persons derive from that regulation, without it being necessary to prove actual harm suffered by the data subject, in a given situation, by the infringement of his or her rights.

73. Such an interpretation is consistent with the requirements stemming from Article 16 TFEU and Article 8 of the Charter of Fundamental Rights of the European Union and, thus, with the objective pursued by the GDPR consisting in ensuring effective protection of the fundamental rights and freedoms of natural persons and, in particular, of ensuring a high level of protection of the right of every person to the protection of personal data concerning him or her (see, to that effect, judgment of 15 June 2021, *Facebook Ireland and Others*, C-645/19, EU:C:2021:483, paragraphs 44, 45 and 91).

74. Authorising consumer protection associations, such as the Federal Union, to bring, by means of a representative action mechanism, actions seeking to have processing contrary to the provisions of that regulation brought to an end, independently of the infringement of the rights of a person individually and specifically affected by that infringement, undoubtedly contributes to strengthening the rights of data subjects and ensuring that they enjoy a high level of protection.

75. Furthermore, it should be noted that the bringing of such a representative action, in so far as it makes it possible to prevent a large number of infringements of the rights of data subjects by the processing of their personal data, could prove more effective than the action that a single person individually and specifically affected by an infringement of his or her right to the protection of his or her personal data may bring against the person responsible for that infringement.

76. As the Advocate General observed in point 76 of his Opinion, the preventive function of actions brought by consumer protection associations, such as the Federal Union, could not be guaranteed if the representative action provided for in Article 80(2) of the GDPR allowed only the infringement of the rights of a person individually and specifically affected by that infringement to be invoked.

77. In the third place, it is still necessary to ascertain, as requested by the referring court, whether Article 80(2) of the GDPR precludes the bringing of a representative action independently of a specific infringement of a right of a data subject and of a mandate conferred by that data subject, where

infringement of data protection rules has been alleged in the context of an action seeking to review the application of other legal rules intended to ensure consumer protection.

78. In that regard, it should be noted at the outset that, as has been observed, in essence, in paragraph 66 of the present judgment, the infringement of a rule relating to the protection of personal data may at the same time give rise to an infringement of rules on consumer protection or unfair commercial practices.

79. Therefore, as the Advocate General observed in point 72 of his Opinion, that provision does not preclude the Member States from exercising the option it offers them in that consumer protection associations are entitled to take action against infringements of the rights provided for by the GDPR through, as the case may be, rules intended to protect consumers or combat unfair commercial practices, such as those provided for by Directive 2005/29 and Directive 2009/22.

80. That interpretation of Article 80(2) of the GDPR is moreover supported by Directive 2020/1828 which repeals and replaces, as from 25 June 2023, Directive 2009/22. In that context, it must be observed that, in accordance with Article 2(1) thereof, Directive 2020/1828 applies to representative actions brought in relation to traders' infringements of the provisions of EU law referred to in Annex I of that directive, which mentions the GDPR in point 56.

81. It is true that Directive 2020/1828 is not applicable in the context of the dispute in the main proceedings and its transposition deadline has not yet expired. However, it contains several elements which confirm that Article 80 of the GDPR does not preclude the bringing of additional representative actions in the field of consumer protection.

82. Although, as is apparent from recital 11 of that directive, it remains possible to provide a procedural mechanism for additional representative actions in the field of consumer protection, the application mechanisms provided for in the GDPR or based on that regulation, such as that provided for in Article 80 of that regulation, cannot be replaced or amended, as stated in recital 15 of that directive, and they may thus be used to protect the collective interests of consumers.

83. In the light of all the foregoing considerations, the answer to the question referred is that Article 80(2) of the GDPR must be interpreted as not precluding national legislation which allows a consumer protection association to bring legal proceedings, in the absence of a mandate conferred on it for that purpose and independently of the infringement of specific rights of the data subjects, against the person allegedly responsible for an infringement of the laws protecting personal data, on the basis of the infringement of the prohibition of unfair commercial practices, a breach of a consumer protection

law or the prohibition of the use of invalid general terms and conditions, where the data processing concerned is liable to affect the rights that identified or identifiable natural persons derive from that regulation.

Costs

84. Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Third Chamber) hereby rules:

Article 80(2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) must be interpreted as not precluding national legislation which allows a consumer protection association to bring legal proceedings, in the absence of a mandate conferred on it for that purpose and independently of the infringement of specific rights of the data subjects, against the person allegedly responsible for an infringement of the laws protecting personal data, on the basis of the infringement of the prohibition of unfair commercial practices, a breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions, where the data processing concerned is liable to affect the rights that identified or identifiable natural persons derive from that regulation.

[Signatures]

* Language of the case: German.

ABAD - PNR Directive (C-817/19)

Judgment of the Court in Case C-817/19

The Court considers that respect for fundamental rights requires that the powers provided for by the PNR Directive be limited to what is strictly necessary

In the absence of a genuine and present or foreseeable terrorist threat to a Member State, EU law precludes national legislation providing for the transfer and processing of the PNR data of intra-EU flights and transport operations carried out by other means within the European Union

The PNR Directive 1 requires the systematic processing of a significant amount of PNR (Passenger Name Record) data relating to air passengers on extra-EU flights entering and leaving the European Union, for the purposes of combating terrorist offences and serious crime. In addition, Article 2 of that directive provides Member States with the possibility to apply the directive to intra-EU flights also.

The Ligue des droits humains (LDH) is a not-for-profit association which filed an action for annulment with the Cour constitutionnelle (Constitutional Court, Belgium) in July 2017 against the Law of 25 December 2016 which transposed into domestic law the PNR Directive, the API Directive 2 and also Directive 2010/65. 3 According to LDH, that law infringes the right to respect for private life and the right to the protection of personal data guaranteed under Belgian and EU law. It criticises, first, the very broad nature of the PNR data and, secondly, the general nature of the collection, transfer and processing of those data. In its view, the law also infringes the free movement of persons in that it indirectly re-establishes border controls by extending the PNR system to intra-EU flights, as well as to transport by other means within the European Union.

In October 2019, the Belgian Constitutional Court referred ten questions to the Court of Justice for a preliminary ruling on, among other things, the validity of the PNR Directive and the compatibility of the Law of 25 December 2016 with EU law.

In its judgment delivered today, the Court held, first, that since the interpretation given by the Court to the provisions of the PNR Directive in the light of the fundamental rights guaranteed by Articles 7, 8 and 21 and Article 52(1) of the Charter of Fundamental Rights of the European Union ('the Charter') ensures that that directive is consistent with those articles, the examination of the questions referred has revealed nothing capable of affecting the validity of the said directive.

It should be noted as a preliminary point that an EU act must be interpreted, as far as possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter. Member States must therefore ensure that they do not rely on an interpretation of that act that would be in conflict with the fundamental rights protected by the EU legal order or with the other general principles recognised by EU law. The Court states that many of the recitals and provisions of the PNR Directive require such an interpretation, stressing the importance that the EU legislature, by referring to the high level of data protection, gives to the full respect for fundamental rights enshrined in the Charter.

The Court states that the PNR Directive entails undeniably serious interferences with the rights guaranteed in Articles 7 and 8 of the Charter, in so far, *inter alia*, as it seeks to introduce a surveillance regime that is continuous, untargeted and systematic, including the automated assessment of the personal data of everyone using air transport services. It notes that the question whether the Member States may justify that interference must be

assessed by measuring its seriousness and by verifying that the importance of the objective of general interest

pursued is proportionate to that seriousness.

The Court concludes that the transfer, processing and retention of PNR data provided for by that directive may be regarded as being limited to what is strictly necessary for the purposes of combating terrorist offences and serious crime, provided that the powers provided for by that directive are interpreted restrictively. In that regard, today's judgment states, *inter alia*, that:

- The system established by the PNR Directive must cover only clearly identifiable and circumscribed information contained in the headings of Annex I thereto, relating to the flight operated and to the passenger concerned, which implies that, for certain headings of that annex, only the information specifically referred to is covered.

- The application of the system established by the PNR Directive must be limited to terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air. As regards those crimes, the application of that system cannot be extended to offences which, although meeting the criterion laid down in that directive relating to the threshold of severity and being referred to in

Annex II thereto, amount to ordinary crime in view of the particular features of the domestic criminal justice system.

- The possible extension of the application of the PNR Directive to selected or all intra-EU flights, which a Member State may decide by exercising the power provided for in that directive, should be limited to what is strictly necessary. To that end, it must be open to effective review, either by a court or by an independent administrative body whose decision is binding. In that regard, the Court states that:

- in the sole situation where the Member State establishes that there are sufficiently solid grounds for considering that it is confronted with a terrorist threat which is shown to be genuine and present or foreseeable, the application of that directive to all intra-EU flights from or to the said Member State, for a period which is limited to what is strictly necessary but may be extended, does not go beyond what is strictly necessary;

- in the absence of such a terrorist threat, the application of the directive cannot be extended to all intra- EU flights, but must be limited to intra-EU flights relating, inter alia, to certain routes or travel patterns or to certain airports for which there are, at the discretion of the Member State concerned, indications that would justify that application. The strictly necessary nature of that application to the selected intra-EU flights must be regularly reviewed in accordance with changes in the circumstances that justified their selection.

- For the purposes of the advance assessment of PNR data, the objective of which is to identify persons who require further examination before their arrival or departure and which is initially carried out by means of automated processing, the passenger information unit (PIU) may compare those data only against the databases on persons or objects sought or under alert. Those databases must be non-discriminatory and must be used by the competent authorities in the context of their mission to combat terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air. As regards, moreover, the advance assessment in the light of the pre-determined criteria, the PIU may not use

artificial intelligence technology in self-learning systems ('machine learning'), capable of modifying without human intervention or review the assessment process and, in particular, the assessment criteria on which the result of the application of that process is based as well as the weighting of those criteria. Those criteria must be defined in such a way that their application targets, specifically, individuals who might be reasonably suspected of involvement in terrorist offences or serious crime and to take into consideration both 'incriminating' as well as 'exonerating' evidence, and, in so doing, must not give rise to direct or indirect discrimination.

- Given the margin of error inherent in such automated processing of PNR data and the fairly substantial number of 'false positives' obtained as a result of their application in 2018 and 2019, the appropriateness of the system established by the PNR Directive to achieve the objectives pursued depends essentially on the proper functioning of the verification of the positive results obtained under those processing operations

carried out by the PIU, as a second step, by non-automated means. In that regard, Member States must lay

down clear and precise rules capable of providing guidance and support for the analysis carried out by the PIU agents in charge of that individual review for the purposes of ensuring full respect for the fundamental

rights enshrined in Articles 7, 8 and 21 of the Charter and, in particular, guarantee a uniform administrative practice within the PIU that observes the principle of non-discrimination. In particular, they must ensure that the PIU establishes objective review criteria enabling its agents to verify, on the one hand, whether and to what extent a positive match ('hit') concerns effectively an individual who may be involved in the terrorist offences or serious crime, as well as, on the other hand, the non-discriminatory nature of the automated processing operations. In that context, the Court also stresses that the competent authorities must ensure that the person concerned can understand the operation of the pre-determined assessment criteria and programs applying those criteria, so that it is possible for that person to decide with full knowledge of the relevant facts whether or not to exercise his or her right to judicial redress. Similarly, in the context of such an action, the

court responsible for reviewing the legality of the decision adopted by the competent authorities as well as, except in the case of threats to State security, the persons concerned themselves must have had an opportunity to examine both all the grounds and the evidence on the basis of which the decision was taken, including the pre-determined assessment criteria and the operation of the programs applying those criteria.

- The subsequent disclosure and assessment of PNR data after the arrival or departure of the person concerned may be carried out only on the basis of new circumstances and objective evidence capable of

giving rise to a reasonable suspicion of that person's involvement in serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air, or from which it can be inferred that those data could, in a given case, contribute effectively to combating terrorist offences

with such a link. Disclosure of PNR data for the purposes of such subsequent assessment must, as a general rule, except in the event of duly justified urgency, be subject to a prior review carried out either by a court or by an independent administrative authority, upon a reasoned request from the competent authorities, regardless of whether that request was introduced before or after the expiry of a period of six months following the transfer of those data to the PIU.

Secondly, the Court considers that the PNR Directive, read in the light of the Charter, precludes national legislation which authorises the processing of PNR data collected in accordance with that directive to be processed for purposes other than those expressly referred to in Article 1(2) of the said directive.

Thirdly, as regards the retention period for PNR data, the Court held that Article 12 of the PNR Directive, read in the light of Articles 7 and 8 as well as Article 52(1) of the Charter, precludes national legislation which provides for a general retention period of five years for such data, applicable indiscriminately to all air passengers.

According to the Court, after expiry of the initial retention period of six months, the retention of PNR data does not appear to be limited to what is strictly necessary in respect of those air passengers for whom neither the advance assessment nor any verification carried out during the initial six-month retention period nor any other circumstance have revealed the existence of objective evidence – such as the fact that the PNR data of the passengers concerned gave rise to a verified positive match during the advance assessment – that would be capable of establishing a risk that relates to terrorist offences or serious crime having an objective link, even if only an indirect one, with those passengers' air travel. On the other hand, it considers that, during the initial six-month period, the retention of the PNR data of all air passengers subject to the system established by that directive does not appear, as a matter of principle, to go beyond what is strictly necessary.

Fourthly, the Court holds that EU law precludes national legislation which, in the absence of a genuine and present or foreseeable terrorist threat to which the Member State concerned is confronted, provides for a system for the transfer, by air carriers and tour operators, as well as for the processing, by the competent authorities, of the PNR data of all intra-EU flights and transport operations carried out by other means within the European Union and departing from, going to or transiting through that Member State, for the purposes of

combating terrorist offences and serious crime. In such a situation, the application of the system established by the PNR Directive must be limited to the transfer and processing of the PNR data of flights and/or transport operations relating, inter alia, to certain routes or travel patterns or to certain

airports, stations or seaports for which there are indications that would justify that application. Furthermore, the Court states that EU law precludes national legislation providing for such a system for the transfer and processing of those data for the purposes of improving border controls and combating illegal immigration.

[1] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ 2016 L 119, p. 132).

[2] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (OJ 2004 L 261, p. 24).

[3] Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC (OJ 2010 L 283, p. 1).

JUDGMENT OF THE COURT (Grand Chamber)

21 June 2022 (*)

Table of contents

(Reference for a preliminary ruling – Processing of personal data – Passenger Name Records (PNR) – Regulation (EU) 2016/679 – Article 2(2)(d) – Scope – Directive (EU) 2016/681 – Use of PNR data of air passengers of flights operated between the European Union and third countries – Power to include data of air passengers of flights operated within the European Union – Automated processing of that data – Retention period – Fight against terrorist offences and serious crime – Validity – Charter of Fundamental Rights of the European Union – Articles 7, 8 and 21 as well as Article 52(1) – National legislation extending the application of the PNR system to other transport operations within the European Union – Freedom of movement within the European Union – Charter of Fundamental Rights – Article 45)

In Case C-817/19,

REQUEST for a preliminary ruling under Article 267 TFEU from the Cour constitutionnelle (Constitutional Court, Belgium), made by decision of 17 October 2019, received at the Court on 31 October 2019, in the proceedings

Ligue des droits humains

v

Conseil des ministres,

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, A. Arabadjiev, S. Rodin, I. Jarukaitis and N. Jääskinen, Presidents of Chambers, T. von Danwitz (Rapporteur), M. Safjan, F. Biltgen, P.G. Xuereb, N. Piçarra, L.S. Rossi, A. Kumin and N. Wahl, Judges,

Advocate General: G. Pitruzzella,

Registrar: M. Krausenböck, Administrator,

having regard to the written procedure and further to the hearing on 13 July 2021,

after considering the observations submitted on behalf of:

– the Ligue des droits humains, by C. Forget, avocate,

– the Belgian Government, by P. Cottin, J.-C. Halleux, C. Pochet, M. Van Regemorter, acting as Agents, and by C. Caillet, advocaat, E. Jacobowitz, avocat, G. Ceuppens, V. Dethy and D. Vertongen,

- the Czech Government, by T. Machovičová, O. Serdula, M. Smolek and J. Vlášil, acting as Agents,
- the Danish Government, by M. Jespersen, J. Nymann-Lindgren, V. Pasternak Jørgensen and M. Søndahl Wolff, acting as Agents,
- the German Government, by D. Klebs and J. Möller, acting as Agents,
- the Estonian Government, by N. Grünberg, acting as Agent,
- Ireland, by M. Browne, A. Joyce, J. Quaney, acting as Agents, and D. Fennelly, Barrister-at-Law,
- the Spanish Government, by L. Aguilera Ruiz, acting as Agent,
- the French Government, by D. Dubois, E. de Moustier and T. Stéhelin, acting as Agents,
- the Cypriot Government, by I. Neofytou, acting as Agent,
- the Latvian Government, by E. Bārdiņš, K. Pommere and V. Soņeca, acting as Agents,
- the Netherlands Government, by M.K. Bulterman, A. Hanje, J. Langer and C.S. Schillemans, acting as Agents,
- the Austrian Government, by G. Kunnert, A. Posch and J. Schmoll, acting as Agents,
- the Polish Government, by B. Majczyna, acting as Agent,
- the Slovak Government, by B. Ricziová, acting as Agent,
- the Finnish Government, by A. Laine and H. Leppo, acting as Agent,
- the European Parliament, by O. Hrstková Šolcová and P. López-Carceller, acting as Agents,
- the Council of the European Union, by J. Lotarski, N. Rouam, E. Sitbon and C. Zadra, acting as Agents,
- the European Commission, by D. Nardi and M. Wasmeier, acting as Agents,
- the European Data Protection Supervisor, by P. Angelov, A. Buchta, F. Coudert and C.-A. Marnier, acting as Agents,
- the European Union Agency for Fundamental Rights, by L. López, T. Molnar, M. Nespór and M. O’Flaherty, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 27 January 2022,

gives the following

Judgment

1. This reference for a preliminary ruling, in essence, concerns:

- the interpretation of Article 2(2)(d) and Article 23 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; ‘the GDPR’), of Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (OJ 2004 L 261, p. 24; ‘the API Directive’) and of Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC (OJ 2010 L 283, p. 1);
- the interpretation and validity, in the light of Articles 7 and 8 as well as Article 52(1) of the Charter of Fundamental Rights of the European Union (‘the Charter’), of Article 3(4) and Articles 6 and 12 of, as well as Annex I to, Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ 2016 L 119, p. 132; ‘the PNR Directive’), and
- the interpretation and validity, in the light of Article 3(2) TEU and Article 45 of the Charter, of the API Directive.

2. The request has been made in proceedings between the Ligue des droits humains and the Conseil des ministres (Council of Ministers, Belgium) concerning the legality of the loi du 25 décembre 2016, relative au traitement des données des passagers (Law of 25 December 2016 on the processing of passenger data).

I. Legal context

A. European Union law

1. Directive 95/46/EC

3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) was repealed by the GDPR, with effect from 25 May 2018. Article 3(2) of that directive provided:

‘This Directive shall not apply to the processing of personal data:

– in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

– by a natural person in the course of a purely personal or household activity.’

2. The API Directive

4. Recitals 1, 7, 9 and 12 of the API Directive state:

‘(1) In order to combat illegal immigration effectively and to improve border control, it is essential that all Member States introduce provisions laying down obligations on air carriers transporting passengers into the territory of the Member States. In addition, in order to ensure the greater effectiveness of this objective, the financial penalties currently provided for by the Member States for cases where carriers fail to meet their obligations should be harmonised to the extent possible, taking into account the differences in legal systems and practices between the Member States.

...

(7) The obligations to be imposed on carriers by virtue of this Directive are complementary to those established pursuant to the provisions of Article 26 of the 1990 Schengen Convention implementing the Schengen Agreement of 14 June 1985, as supplemented by Council Directive 2001/51/EC [of 28 June 2001 supplementing the provisions of Article 26 of the Convention implementing the Schengen Agreement of 14 June 1985 (OJ 2001 L 187, p. 45)], the two types of obligation serving the same objective of curbing migratory flows and combating illegal immigration.

...

(9) In order to combat illegal immigration more effectively and in order to ensure the greater effectiveness of this objective, it is essential that, without prejudice to the provisions of Directive [95/46], account be taken at the earliest opportunity of any technological innovation, especially with reference to the integration and use of biometric features in the information to be provided by the carriers.

...

(12) Directive [95/46] applies with regard to the processing of personal data by the authorities of the Member States. This means, that whereas it would be legitimate to process the passenger data

transmitted for the performance of border checks also for the purposes of allowing their use as evidence in proceedings aiming at the enforcement of the laws and regulations on entry and immigration, including their provisions on the protection of public policy (*ordre public*) and national security, any further processing in a way incompatible with those purposes would run counter to the principle set out in Article 6(1)(b) of Directive [95/46]. Member States should provide for a system of sanctions to be applied in the event of use contrary to the purpose of the present Directive.'

5. Article 1 of the API Directive, entitled 'Objective', provides:

'This Directive aims at improving border controls and combating illegal immigration by the transmission of advance passenger data by carriers to the competent national authorities.'

6. Article 2 of that directive, entitled 'Definitions', states:

'For the purpose of this Directive:

(a) "carrier" means any natural or legal person whose occupation it is to provide passenger transport by air;

(b) "external borders" means the external borders of the Member States with third countries;

(c) "border control" means a check carried out at a border in response exclusively to an intention to cross that border, regardless of any other consideration;

(d) "border crossing point" means any crossing point authorised by the competent authorities for crossing external borders;

(e) "personal data", "processing of personal data" and "personal data filing system" have the meaning as stipulated under Article 2 of Directive [95/46].'

7. Article 3 of that directive, entitled 'Data transmission', provides, in its paragraphs 1 and 2:

'1. Member States shall take the necessary steps to establish an obligation for carriers to transmit at the request of the authorities responsible for carrying out checks on persons at external borders, by the end of check-in, information concerning the passengers they will carry to an authorised border crossing point through which these persons will enter the territory of a Member State.

2. The information referred to above shall comprise:

- the number and type of travel document used,
- nationality,
- full names,

- the date of birth,
- the border crossing point of entry into the territory of the Member States,
- code of transport,
- departure and arrival time of the transportation,
- total number of passengers carried on that transport,
- the initial point of embarkation.’

8. Article 6 of the API Directive, entitled ‘Data processing’, provides:

‘1. The personal data referred to in Article 3(1) shall be communicated to the authorities responsible for carrying out checks on persons at external borders through which the passenger will enter the territory of a Member State, for the purpose of facilitating the performance of such checks with the objective of combating illegal immigration more effectively.

Member States shall ensure that these data are collected by the carriers and transmitted electronically or, in case of failure, by any other appropriate means to the authorities responsible for carrying out border checks at the authorised border crossing point through which the passenger will enter the territory of a Member State. The authorities responsible for carrying out checks on persons at external borders shall save the data in a temporary file.

After passengers have entered, these authorities shall delete the data, within 24 hours after transmission, unless the data are needed later for the purposes of exercising the statutory functions of the authorities responsible for carrying out checks on persons at external borders in accordance with national law and subject to data protection provisions under Directive [95/46].

Member States shall take the necessary measures to oblige carriers to delete, within 24 hours of the arrival of the means of transportation pursuant to Article 3(1), the personal data they have collected and transmitted to the border authorities for the purposes of this Directive.

In accordance with their national law and subject to data protection provisions under Directive [95/46], Member States may also use the personal data referred to in Article 3(1) for law enforcement purposes.

2. Member States shall take the necessary measures to oblige the carriers to inform the passengers in accordance with the provisions laid down in Directive [95/46]. This shall also comprise the information referred to in Article 10(c) and Article 11(1)(c) of Directive [95/46].’

3. Directive 2010/65

9. Directive 2010/65 is to be repealed, pursuant to Article 25 of Regulation (EU) 2019/1239 of the European Parliament and of the Council of 20 June 2019 establishing a European Maritime Single Window environment and repealing Directive 2010/65 (OJ 2019 L 198, p. 64), from 15 August 2025.

10. Recital 2 of that directive states:

‘For the facilitation of maritime transport and in order to reduce the administrative burdens for shipping companies, the reporting formalities required by legal acts of the [European] Union and by Member States need to be simplified and harmonised to the greatest extent possible. ...’

11. Article 1 of that directive, entitled ‘Subject matter and scope’, provides, in its paragraphs 1 and 2:

‘1. The purpose of this Directive is to simplify and harmonise the administrative procedures applied to maritime transport by making the electronic transmission of information standard and by rationalising reporting formalities.

2. This Directive shall apply to the reporting formalities applicable to maritime transport for ships arriving in and ships departing from ports situated in Member States.’

12. Under Article 8 of that directive, entitled ‘Confidentiality’:

‘1. Member States shall, in accordance with the applicable legal acts of the [European] Union or national legislation, take the necessary measures to ensure the confidentiality of commercial and other confidential information exchanged in accordance with this Directive.

2. Member States shall take particular care to protect commercial data collected under this Directive. In respect of personal data, Member States shall ensure that they comply with Directive [95/46]. The [EU] institutions and bodies shall ensure that they comply with Regulation (EC) No 45/2001 [of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8, p. 1)].’

4. The GDPR

13. Recital 19 of the GDPR states:

‘The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific [EU] legal

act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific [EU] legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council [of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89)]. Member States may entrust competent authorities within the meaning of [Directive 2016/680] with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of [EU] law, falls within the scope of this Regulation.

...'

14. Article 2 of that regulation, entitled 'Material scope', provides in its paragraphs 1 and 2:

'1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of [EU] law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V [TEU];

...

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'

15. Article 4 of that regulation, entitled 'Definitions', provides:

'For the purposes of this Regulation:

(1) "personal data" means any information relating to an identified or identifiable natural person ...;

(2) “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

...'

16. Article 23 of the GDPR, entitled 'Restrictions', provides:

'1. [EU] or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as in Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

...

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

...

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.'

17. Article 94 of that regulation, entitled 'Repeal of Directive [95/46]' provides:

'1. Directive [95/46] is repealed with effect from 25 May 2018.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive [95/46] shall be construed as references to the European Data Protection Board established by this Regulation.'

5. Directive 2016/680

18. Directive 2016/680, in accordance with Article 59 thereof, repealed and replaced Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ 2008 L 350, p. 60), from 6 May 2018.

19. Recitals 9 to 11 of Directive 2016/680 state:

'(9) On that basis, [the GDPR] lays down general rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the [European] Union.

(10) In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and on the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU could prove necessary because of the specific nature of those fields.

(11) It is therefore appropriate for those fields to be addressed by a directive that lays down the specific rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding

against and the prevention of threats to public security, respecting the specific nature of those activities. Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive. Where such a body or entity processes personal data for purposes other than for the purposes of this Directive, [the GDPR] applies. [The GDPR] therefore applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject. For example, for the purposes of investigation detection or prosecution of criminal offences financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law. A body or entity which processes personal data on behalf of such authorities within the scope of this Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to this Directive, while the application of [the GDPR] remains unaffected for the processing of personal data by the processor outside the scope of this Directive.'

20. Article 1 of that directive, entitled 'Subject matter and objectives', which corresponds, in essence, to Article 1 of Framework Decision 2008/977, provides, in its paragraph 1:

'This Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'

21. Under Article 3 of that directive, entitled 'Definitions':

'For the purposes of this Directive:

...

7. "competent authority" means:

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences

or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

...'

6. The PNR Directive

22. Recitals 4 to 12, 15, 19, 20, 22, 25, 27, 28, 33, 36 and 37 of the PNR Directive state:

'(4) [The API Directive] regulates the transfer of advance passenger information (API) data by air carriers to the competent national authorities for the purpose of improving border controls and combating illegal immigration.

(5) The objectives of this Directive are, *inter alia*, to ensure security, to protect the life and safety of persons, and to create a legal framework for the protection of PNR data with regard to their processing by competent authorities.

(6) Effective use of PNR data, for example by comparing PNR data against various databases on persons and objects sought, is necessary to prevent, detect, investigate and prosecute terrorist offences and serious crime and thus enhance internal security, to gather evidence and, where relevant, to find associates of criminals and unravel criminal networks.

(7) Assessment of PNR data allows identification of persons who were unsuspected of involvement in terrorist offences or serious crime prior to such an assessment and who should be subject to further examination by the competent authorities. By using PNR data it is possible to address the threat of terrorist offences and serious crime from a different perspective than through the processing of other categories of personal data. However, to ensure that the processing of PNR data remains limited to what is necessary, the creation and application of assessment criteria should be limited to terrorist offences and serious crime for which the use of such criteria is relevant. Furthermore, the assessment criteria should be defined in a manner which keeps to a minimum the number of innocent people wrongly identified by the system.

(8) Air carriers already collect and process their passengers' PNR data for their own commercial purposes. This Directive should not impose any obligation on air carriers to collect or retain any additional data from passengers or any obligation on passengers to provide any data in addition to that already being provided to air carriers.

(9) Some air carriers retain as part of the PNR data the API data they collect, while others do not. The use of PNR data together with API data has added value in assisting Member States in verifying the

identity of an individual, thus reinforcing the law enforcement value of that result and minimising the risk of carrying out checks and investigations on innocent people. It is therefore important to ensure that where air carriers collect API data, they transfer it irrespective of whether they retain API data by different technical means as for other PNR data.

(10) To prevent, detect, investigate and prosecute terrorist offences and serious crime, it is essential that all Member States introduce provisions laying down obligations on air carriers operating extra-EU flights to transfer PNR data they collect, including API data. Member States should also have the possibility to extend this obligation to air carriers operating intra-EU flights. Those provisions should be without prejudice to [the API Directive].

(11) The processing of personal data should be proportionate to the specific security goals pursued by this Directive.

(12) The definition of terrorist offences applied in this Directive should be the same as in Council Framework Decision 2002/475/JHA [of 13 June 2002 on combating terrorism (OJ 2002 L 164, p. 3)]. The definition of serious crime should encompass the categories of offence listed in Annex II to this Directive.

...

(15) A list of the PNR data to be obtained by a [passenger information unit (PIU)] should be drawn up with the objective of reflecting the legitimate requirements of public authorities to prevent, detect, investigate and prosecute terrorist offences or serious crime, thereby improving internal security within the Union as well as protecting the fundamental rights, in particular privacy and the protection of personal data. To that end, high standards should be applied in accordance with [the Charter], the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention No 108"), and the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed at Rome on 4 November 1950] (the "ECHR"). Such a list should not be based on a person's race or ethnic origin, religion or belief, political or any other opinion, trade union membership, health, sexual life or sexual orientation. The PNR data should only contain details of passengers' reservations and travel itineraries that enable competent authorities to identify air passengers representing a threat to internal security.

...

(19) Each Member State should be responsible for assessing the potential threats related to terrorist offences and serious crime.

(20) Taking fully into consideration the right to the protection of personal data and the right to non-discrimination, no decision that produces an adverse legal effect on a person or significantly affects that person should be taken only by reason of the automated processing of PNR data. Moreover, in respect of Articles 8 and 21 of the Charter, no such decision should discriminate on any grounds such as a person's sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation. The [European] Commission should also take those principles into account when reviewing the application of this Directive.

...

(22) Taking fully into consideration the principles outlined in recent relevant case-law of the Court of Justice of the European Union, the application of this Directive should ensure full respect for fundamental rights, for the right to privacy and for the principle of proportionality. It should also genuinely meet the objectives of necessity and proportionality in order to achieve the general interests recognised by the [European] Union and the need to protect the rights and freedoms of others in the fight against terrorist offences and serious crime. The application of this Directive should be duly justified and the necessary safeguards put in place to ensure the lawfulness of any storage, analysis, transfer or use of PNR data.

...

(25) The period during which PNR data are to be retained should be as long as is necessary for and proportionate to the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. Because of the nature of the data and their uses, it is necessary that the PNR data be retained for a sufficiently long period to carry out analysis and for use in investigations. To avoid disproportionate use, after the initial retention period the PNR data should be depersonalised through masking out of data elements. To ensure the highest level of data protection, access to the full PNR data, which enable direct identification of the data subject, should be granted only under very strict and limited conditions after that initial period.

...

(27) The processing of PNR data in each Member State by the PIU and by competent authorities should be subject to a standard of protection of personal data under national law in line with Framework Decision [2008/977] and the specific data protection requirements laid down in this

Directive. References to Framework Decision [2008/977] should be understood as references to legislation currently in force as well as to legislation that will replace it.

(28) Taking into consideration the right to the protection of personal data, the rights of data subjects concerning the processing of their PNR data, such as the rights of access, rectification, erasure and restriction and the rights to compensation and judicial redress, should be in line both with Framework Decision [2008/977] and with the high level of protection provided by the Charter and the ECHR.

...

(33) This Directive does not affect the possibility for Member States to provide, under their national law, for a system of collecting and processing PNR data from non-carrier economic operators, such as travel agencies and tour operators which provide travel-related services – including the booking of flights – for which they collect and process PNR data, or from transportation providers other than those specified in this Directive, provided that such national law complies with [EU] law.

...

(36) This Directive respects the fundamental rights and the principles of the Charter, in particular the right to the protection of personal data, the right to privacy and the right to non-discrimination as protected by Articles 8, 7 and 21 thereof; it should therefore be implemented accordingly. This Directive is compatible with data protection principles and its provisions are in line with Framework Decision [2008/977]. Furthermore, to comply with the proportionality principle, on specific issues this Directive provides for stricter rules on data protection than Framework Decision [2008/977].

(37) The scope of this Directive is as limited as possible since: it provides for the retention of PNR data in the PIUs for a period of time not exceeding five years, after which the data should be deleted; it provides for the data to be depersonalised through masking out of data elements after an initial period of six months; and it prohibits the collection and use of sensitive data. To ensure efficiency and a high level of data protection, Member States are required to ensure that an independent national supervisory authority and, in particular, a data protection officer are responsible for advising and monitoring the way PNR data are processed. All processing of PNR data should be logged or documented for the purposes of verifying its legality, self-monitoring and ensuring proper data integrity and secure processing. Member States should also ensure that passengers are clearly and precisely informed about the collection of PNR data and their rights.'

23. Article 1 of the PNR Directive, entitled 'Subject matter and scope', is worded as follows:

'1. This Directive provides for:

(a) the transfer by air carriers of passenger name record (PNR) data of passengers of extra-EU flights, (b) the processing of the data referred to in point (a), including its collection, use and retention by Member States and its exchange between Member States.

2. PNR data collected in accordance with this Directive may be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, as provided for in points (a), (b) and (c) of Article 6(2).'

24. In accordance with Article 2 of that directive, entitled 'Application of this Directive to intra-EU flights':

'1. If a Member State decides to apply this Directive to intra-EU flights, it shall notify the Commission in writing. A Member State may give or revoke such a notification at any time. The Commission shall publish that notification and any revocation of it in the Official Journal of the European Union.

2. Where a notification referred to in paragraph 1 is given, all the provisions of this Directive shall apply to intra-EU flights as if they were extra-EU flights and to PNR data from intra-EU flights as if they were PNR data from extra-EU flights.

3. A Member State may decide to apply this Directive only to selected intra-EU flights. In making such a decision, the Member State shall select the flights it considers necessary in order to pursue the objectives of this Directive. The Member State may decide to change the selection of intra-EU flights at any time.'

25. Under Article 3 of that directive, entitled 'Definitions':

'For the purposes of this Directive the following definitions apply:

(1) "air carrier" means an air transport undertaking with a valid operating licence or equivalent permitting it to carry out carriage of passengers by air;

(2) "extra-EU flight" means any scheduled or non-scheduled flight by an air carrier flying from a third country and planned to land on the territory of a Member State or flying from the territory of a Member State and planned to land in a third country, including in both cases flights with any stop-overs in the territory of Member States or third countries;

(3) "intra-EU flight" means any scheduled or non-scheduled flight by an air carrier flying from the territory of a Member State and planned to land on the territory of one or more of the other Member States, without any stop-overs in the territory of a third country;

(4) “passenger” means any person, including persons in transfer or transit and excluding members of the crew, carried or to be carried in an aircraft with the consent of the air carrier, such consent being manifested by that person’s registration in the passengers list;

(5) “passenger name record” or “PNR” means a record of each passenger’s travel requirements which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person, whether it is contained in reservation systems, departure control systems used to check passengers onto flights, or equivalent systems providing the same functionalities;

(6) “reservation system” means the air carrier’s internal system, in which PNR data are collected for the handling of reservations;

(7) “push method” means the method whereby air carriers transfer PNR data listed in Annex I into the database of the authority requesting them;

(8) “terrorist offences” means the offences under national law referred to in Articles 1 to 4 of Framework Decision [2002/475];

(9) “serious crime” means the offences listed in Annex II that are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State;

(10) “to depersonalise through masking out of data elements” means to render those data elements which could serve to identify directly the data subject invisible to a user.’

26. Article 4 of the PNR Directive, entitled ‘Passenger information unit’, provides in paragraphs 1 to 3:

‘1. Each Member State shall establish or designate an authority competent for the prevention, detection, investigation or prosecution of terrorist offences and of serious crime or a branch of such an authority, to act as its passenger information unit (“PIU”).

2. The PIU shall be responsible for:

(a) collecting PNR data from air carriers, storing and processing those data and transferring those data or the result of processing them to the competent authorities referred to in Article 7;

(b) exchanging both PNR data and the result of processing those data with the PIUs of other Member States and with Europol in accordance with Articles 9 and 10.

3. Staff members of a PIU may be seconded from competent authorities. Member States shall provide the PIUs with adequate resources for them to fulfil their tasks.'

27. Article 5 of that directive, entitled 'Data protection officer in the PIU' is worded as follows:

'1. The PIU shall appoint a data protection officer responsible for monitoring the processing of PNR data and implementing relevant safeguards.

2. Member States shall provide data protection officers with the means to perform their duties and tasks in accordance with this Article effectively and independently.

3. Member States shall ensure that a data subject has the right to contact the data protection officer, as a single point of contact, on all issues relating to the processing of that data subject's PNR data.'

28. Article 6 of that directive, entitled 'Processing of PNR data', provides that:

'1. The PNR data transferred by the air carriers shall be collected by the PIU of the relevant Member State as provided for in Article 8. Where the PNR data transferred by air carriers include data other than those listed in Annex I, the PIU shall delete such data immediately and permanently upon receipt.

2. The PIU shall process PNR data only for the following purposes:

(a) carrying out an assessment of passengers prior to their scheduled arrival in or departure from the Member State to identify persons who require further examination by the competent authorities referred to in Article 7, and, where relevant, by Europol in accordance with Article 10, in view of the fact that such persons may be involved in a terrorist offence or serious crime;

(b) responding, on a case-by-case basis, to a duly reasoned request based on sufficient grounds from the competent authorities to provide and process PNR data in specific cases for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime, and to provide the competent authorities or, where appropriate, Europol with the results of such processing; and

(c) analysing PNR data for the purpose of updating or creating new criteria to be used in the assessments carried out under point (b) of paragraph 3 in order to identify any persons who may be involved in a terrorist offence or serious crime.

3. When carrying out the assessment referred to in point (a) of paragraph 2, the PIU may:

(a) compare PNR data against databases relevant for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, including databases on persons or

objects sought or under alert, in accordance with [EU], international and national rules applicable to such databases; or

(b) process PNR data against pre-determined criteria.

4. Any assessment of passengers prior to their scheduled arrival in or departure from the Member State carried out under point (b) of paragraph 3 against pre-determined criteria shall be carried out in a non-discriminatory manner. Those pre-determined criteria must be targeted, proportionate and specific. Member States shall ensure that those criteria are set and regularly reviewed by the PIU in cooperation with the competent authorities referred to in Article 7. The criteria shall in no circumstances be based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.

5. Member States shall ensure that any positive match resulting from the automated processing of PNR data conducted under point (a) of paragraph 2 is individually reviewed by non-automated means to verify whether the competent authority referred to in Article 7 needs to take action under national law.

6. The PIU of a Member State shall transmit the PNR data of persons identified in accordance with point (a) of paragraph 2 or the result of processing those data for further examination to the competent authorities referred to in Article 7 of the same Member State. Such transfers shall only be made on a case-by-case basis and, in the event of automated processing of PNR data, after individual review by non-automated means.

7. Member States shall ensure that the data protection officer has access to all data processed by the PIU. If the data protection officer considers that processing of any data has not been lawful, the data protection officer may refer the matter to the national supervisory authority.

...

9. The consequences of the assessments of passengers referred to in point (a) of paragraph 2 of this Article shall not jeopardise the right of entry of persons enjoying the [EU] right of free movement into the territory of the Member State concerned as laid down in Directive 2004/38/EC of the European Parliament and of the Council [of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ 2004 L 158, p. 77)]. In addition, where assessments are carried out in relation to intra-EU flights between Member States to which

Regulation (EC) No 562/2006 of the European Parliament and of the Council [of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ 2006 L 105, p. 1)] applies, the consequences of such assessments shall comply with that Regulation.'

29. Under Article 7 of the PNR Directive, entitled 'Competent authorities':

'1. Each Member State shall adopt a list of the competent authorities entitled to request or receive PNR data or the result of processing those data from the PIU in order to examine that information further or to take appropriate action for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.

2. The authorities referred to in paragraph 1 shall be authorities competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime.

...

4. The PNR data and the result of processing those data received by the PIU may be further processed by the competent authorities of the Member States only for the specific purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime.

5. Paragraph 4 shall be without prejudice to national law enforcement or judicial powers where other offences, or indications thereof, are detected in the course of enforcement action further to such processing.

6. The competent authorities shall not take any decision that produces an adverse legal effect on a person or significantly affects a person only by reason of the automated processing of PNR data. Such decisions shall not be taken on the basis of a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.'

30. Article 8 of that directive, entitled 'Obligations on air carriers regarding transfers of data', provides in its paragraphs 1 to 3:

'1. Member States shall adopt the necessary measures to ensure that air carriers transfer, by the "push method", the PNR data listed in Annex I, to the extent that they have already collected such data in the normal course of their business, to the database of the PIU of the Member State on the territory of which the flight will land or from the territory of which the flight will depart. Where the flight is code-shared between one or more air carriers, the obligation to transfer the PNR data of all passengers on the flight shall be on the air carrier that operates the flight. Where an extra-EU flight has one or more

stop-overs at airports of the Member States, air carriers shall transfer the PNR data of all passengers to the PIUs of all the Member States concerned. This also applies where an intra-EU flight has one or more stop-overs at the airports of different Member States, but only in relation to Member States which are collecting PNR data from intra-EU flights.

2. In the event that the air carriers have collected any [API] data listed under item 18 of Annex I but do not retain those data by the same technical means as for other PNR data, Member States shall adopt the necessary measures to ensure that air carriers also transfer, by the “push method”, those data to the PIU of the Member States referred to in paragraph 1. In the event of such a transfer, all the provisions of this Directive shall apply in relation to those API data.

3. Air carriers shall transfer PNR data by electronic means using the common protocols and supported data formats to be adopted in accordance with the examination procedure referred to in Article 17(2) or, in the event of technical failure, by any other appropriate means ensuring an appropriate level of data security:

(a) 24 to 48 hours before the scheduled flight departure time; and

(b) immediately after flight closure, that is once the passengers have boarded the aircraft in preparation for departure and it is no longer possible for passengers to board or leave.’

31. Article 12 of that directive, entitled ‘Period of data retention and depersonalisation’, provides:

‘1. Member States shall ensure that the PNR data provided by the air carriers to the PIU are retained in a database at the PIU for a period of five years after their transfer to the PIU of the Member State on whose territory the flight is landing or departing.

2. Upon expiry of a period of six months after the transfer of the PNR data referred to in paragraph 1, all PNR data shall be depersonalised through masking out of the following data elements which could serve to identify directly the passenger to whom the PNR data relate:

(a) name(s), including the names of other passengers on the PNR and number of travellers on the PNR travelling together;

(b) address and contact information;

(c) all forms of payment information, including billing address, to the extent that it contains any information which could serve to identify directly the passenger to whom the PNR relate or any other persons;

(d) frequent flyer information;

(e) general remarks to the extent that they contain any information which could serve to identify directly the passenger to whom the PNR relate; and

(f) any API data that have been collected.

3. Upon expiry of the period of six months referred to in paragraph 2, disclosure of the full PNR data shall be permitted only where it is:

(a) reasonably believed that it is necessary for the purposes referred to in point (b) of Article 6(2) and

(b) approved by:

(i) a judicial authority; or

(ii) another national authority competent under national law to verify whether the conditions for disclosure are met, subject to informing the data protection officer of the PIU and to an ex post review by that data protection officer.

4. Member States shall ensure that the PNR data are deleted permanently upon expiry of the period referred to in paragraph 1. This obligation shall be without prejudice to cases where specific PNR data have been transferred to a competent authority and are used in the context of specific cases for the purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime, in which case the retention of such data by the competent authority shall be regulated by national law.

5. The result of the processing referred to in point (a) of Article 6(2) shall be kept by the PIU only as long as necessary to inform the competent authorities and, in accordance with Article 9(1), to inform the PIUs of other Member States of a positive match. Where the result of automated processing has, further to individual review by non-automated means as referred to in Article 6(5), proven to be negative, it may, however, be stored so as to avoid future “false” positive matches for as long as the underlying data are not deleted under paragraph 4 of this Article.’

32. Article 13 of the PNR Directive, entitled ‘Protection of personal data’, provides in paragraphs 1 to 5:

‘1. Each Member State shall provide that, in respect of all processing of personal data pursuant to this Directive, every passenger shall have the same right to protection of their personal data, rights of access, rectification, erasure and restriction and rights to compensation and judicial redress as laid down in [EU] and national law and in implementation of Articles 17, 18, 19 and 20 of Framework Decision [2008/977]. Those Articles shall therefore apply.

2. Each Member State shall provide that the provisions adopted under national law in implementation of Articles 21 and 22 of Framework Decision [2008/977] regarding confidentiality of processing and data security shall also apply to all processing of personal data pursuant to this Directive.

3. This Directive is without prejudice to the applicability of Directive [95/46] to the processing of personal data by air carriers, in particular their obligations to take appropriate technical and organisational measures to protect the security and confidentiality of personal data.

4. Member States shall prohibit the processing of PNR data revealing a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. In the event that PNR data revealing such information are received by the PIU, they shall be deleted immediately.

5. Member States shall ensure that the PIUs maintain documentation relating to all processing systems and procedures under their responsibility. That documentation shall contain at least:

(a) the name and contact details of the organisation and personnel in the PIU entrusted with the processing of the PNR data and the different levels of access authorisation;

(b) the requests made by competent authorities and PIUs of other Member States;

(c) all requests for and transfers of PNR data to a third country.

The PIU shall make all documentation available, upon request, to the national supervisory authority.'

33. According to Article 15 of that directive, entitled 'National supervisory authority':

'1. Each Member State shall provide that the national supervisory authority referred to in Article 25 of Framework Decision [2008/977] is responsible for advising on and monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. Article 25 of Framework Decision [2008/977] shall apply.

2. Those national supervisory authorities shall conduct activities under paragraph 1 with a view to protecting fundamental rights in relation to the processing of personal data.

3. Each national supervisory authority shall:

(a) deal with complaints lodged by any data subject, investigate the matter and inform the data subjects of the progress and the outcome of their complaints within a reasonable time period;

(b) verify the lawfulness of the data processing, conduct investigations, inspection and audits in accordance with national law, either on its own initiative or on the basis of a complaint referred to in point (a).

4. Each national supervisory authority shall, upon request, advise any data subject on the exercise of the rights laid down in provisions adopted pursuant to this Directive.'

34. Article 19 of the directive, entitled 'Review', provides:

'1. On the basis of information provided by the Member States, including the statistical information referred to in Article 20(2), the Commission shall by 25 May 2020 conduct a review of all the elements of this Directive and submit and present a report to the European Parliament and to the Council [of the European Union].

2. In conducting its review, the Commission shall pay special attention to:

(a) compliance with the applicable standards of protection of personal data,

(b) the necessity and proportionality of collecting and processing PNR data for each of the purposes set out in this Directive,

(c) the length of the data retention period,

(d) the effectiveness of exchange of information between the Member States, and

(e) the quality of the assessments including with regard to the statistical information gathered pursuant to Article 20.

3. The report referred to in paragraph 1 shall also include a review of the necessity, proportionality, and effectiveness of including within the scope of this Directive the mandatory collection and transfer of PNR data relating to all or selected intra-EU flights. The Commission shall take into account the experience gained by Member States, especially those Member States that apply this Directive to intra-EU flights in accordance with Article 2. The report shall also consider the necessity of including non-carrier economic operators, such as travel agencies and tour operators which provide travel-related services, including the booking of flights, within the scope of this Directive.

4. If appropriate, in light of the review conducted pursuant to this Article, the Commission shall make a legislative proposal to the European Parliament and to the Council with a view to amending this Directive.'

35. Article 21 of that directive, entitled 'Relationship to other instruments', provides, in paragraph 2:

'This Directive is without prejudice to the applicability of Directive [95/46] to the processing of personal data by air carriers.'

36. Annex I to the PNR Directive, entitled 'Passenger name record data as far as collected by air carriers', provides:

1. PNR record locator

2. Date of reservation/issue of ticket

3. Date(s) of intended travel

4. Name(s)

5. Address and contact information (telephone number, email address)

6. All forms of payment information, including billing address

7. Complete travel itinerary for specific PNR

8. Frequent flyer information

9. Travel agency/travel agent

10. Travel status of passenger, including confirmations, check-in status, no-show or go-show information

11. Split/divided PNR information

12. General remarks (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent)

13. Ticketing field information, including ticket number, date of ticket issuance and one-way tickets, automated ticket fare quote fields

14. Seat number and other seat information

15. Code share information

16. All baggage information

17. Number and other names of travellers on the PNR

18. Any advance passenger information (API) data collected (including the type, number, country of issuance and expiry date of any identity document, nationality, family name, given name, gender,

date of birth, airline, flight number, departure date, arrival date, departure port, arrival port, departure time and arrival time)

19. All historical changes to the PNR listed in numbers 1 to 18.'

37. Annex II to that directive, entitled 'List of offences referred to in point (9) of Article 3', is worded as follows:

- '1. participation in a criminal organisation,
2. trafficking in human beings,
3. sexual exploitation of children and child pornography,
4. illicit trafficking in narcotic drugs and psychotropic substances,
5. illicit trafficking in weapons, munitions and explosives,
6. corruption,
7. fraud, including that against the financial interests of the Union,
8. laundering of the proceeds of crime and counterfeiting of currency, including the euro,
9. computer-related crime/cybercrime,
10. environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
11. facilitation of unauthorised entry and residence,
12. murder, grievous bodily injury,
13. illicit trade in human organs and tissue,
14. kidnapping, illegal restraint and hostage-taking,
15. organised and armed robbery,
16. illicit trafficking in cultural goods, including antiques and works of art,
17. counterfeiting and piracy of products,
18. forgery of administrative documents and trafficking therein,
19. illicit trafficking in hormonal substances and other growth promoters,
20. illicit trafficking in nuclear or radioactive materials,
21. rape,

22. crimes within the jurisdiction of the International Criminal Court,
23. unlawful seizure of aircraft/ships,
24. sabotage,
25. trafficking in stolen vehicles,
26. industrial espionage.'

7. Framework Decision 2002/475

38. Article 1 of Framework Decision 2002/475 defined the concept of 'terrorist offence' by listing intentional acts referred to in points (a) to (i) of that article, committed with the aim of 'seriously intimidating a population', 'unduly compelling a Government or international organisation to perform or abstain from performing any act', or 'seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation'. Articles 2 and 3 of that framework decision defined the concepts of 'offences relating to a terrorist group' and of 'offences linked to terrorist activities', respectively. Article 4 of the said framework decision governed the charges of inciting and aiding or abetting those offences as well as that of attempting to commit them.

39. Framework Decision 2002/475 was repealed by Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Framework Decision 2002/475 and amending Council Decision 2005/671/JHA (OJ 2017 L 88, p. 6), Articles 3 to 14 of which include similar definitions.

B. Belgian law

1. The Constitution

40. Article 22 of the Constitution provides as follows:

'Everyone is entitled to respect for private and family life except in the cases and under the circumstances laid down by law.

The laws, decrees and rules referred to in Article 134 guarantee the protection of this right.'

2. The Law of 25 December 2016

41. Article 2 of the loi du 25 décembre 2016, relative au traitement des données des passagers (Law of 25 December 2016 on the processing of passenger data, Moniteur belge of 25 January 2017, p. 12905; 'the Law of 25 December 2016') is worded as follows:

'The present law and the royal decrees which shall be adopted in implementation of the present law transpose [the API Directive] and [the PNR Directive]. The present law and the royal decree concerning the maritime sector partially transpose Directive [2010/65].'

42. Article 3 of that law provides:

'1. This law lays down the obligations of carriers and tour operators regarding the transfer of data relating to passengers travelling to or from or transiting through Belgian territory.

2. The King shall prescribe, by decree deliberated in the Council of Ministers, in respect of each sector of the transport industry and in respect of tour operators, the passenger data to be transferred and how they are to be transferred, after an opinion has been given by the Commission de la protection de la vie privée [(Commission for the protection of privacy)].'

43. Under Article 4 of that law:

'For the purposes of this law and its implementing decrees, the following definitions shall apply:

...

(8) "the competent services": the services under Article 14(1)(2);

(9) "PNR": a record of each passenger's travel requirements which contains the information referred to in Article 9, which is necessary to enable reservations to be processed and controlled by the booking and participating carriers and tour operators for each journey booked by or on behalf of any person, whether it is contained in reservation systems, departure control systems used to check passengers onto flights, or equivalent systems providing the same functionalities;

(10) "passenger": any person, including persons in transfer or transit and excluding members of the crew, carried or to be carried by the carrier with its consent, such consent being manifested by that person's registration in the passengers list;

...'

44. Article 8 of the Law of 25 December 2016 states:

'1. Passenger data shall be processed for the purposes of:

(1) detection and prosecution (including the execution of penalties or measures depriving the person concerned of his or her liberty) of the offences referred to Article 90ter(2), ...(7), ...(8), ...(11), ...(14), ...(17), (18), (19) and Article 90ter(3) of the Code d'instruction criminelle [(Criminal Procedure Code)];

(2) detection and prosecution (including the execution of penalties or measures depriving the person of his or her liberty) of the offences referred to in Article 196, in so far as concerns the offences of forgery of authentic and public documents, Article 198, 199, 199bis, 207, 213, 375 and 505 of the Code pénal [(Criminal Code)];

...

(4) monitoring the activities referred to in Article 7(1) and (3/1) and Article 11(1)(1) to (3) and (5) of the loi du 30 novembre 1998 organique des services de renseignement et de sécurité [(Organic law of 30 November 1998 on the intelligence and security services)];

(5) detection and prosecution of the offences referred to in Article 220(2) of the loi générale sur les douanes et accises du 18 juillet 1977 [(General customs and excise law of 18 July 1977)] and the third paragraph of Article 45 of the loi du 22 décembre 2009 relative au régime général d'accise [(Law of 22 December 2009 on the general excise regime)] ...

2. Subject to the conditions in Chapter 11, passenger data shall also be processed with a view to improving external border controls on individuals, and with a view to combating illegal immigration.'

45. Article 14(1) of that law states:

'The PIU shall be made up of:

...

(2) members seconded from the following competent services:

(a) the police services covered by the loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux [(Law of 7 December 1998 organising an integrated police service, with a two-tier structure)];

(b) the Sûreté de l'État [(State security services)] covered by the [Organic law of 30 November 1998 on the intelligence and security services];

(c) the Service général de Renseignement et de Sécurité [(General intelligence and security services)] covered by the [Organic law of 30 November 1998 on the intelligence and security services];

...'

46. Article 24 of the said law, in Section 1 thereof, entitled 'Processing of passenger data in connection with the advance assessment of passengers', of Chapter 10 of that law, on data processing, is worded as follows:

'1. Passenger data shall be processed with a view to carrying out an assessment of passengers prior to their scheduled arrival in, departure from, or transit through Belgian territory, in order to identify persons who require further examination.

2. For the purposes referred to in Article 8(1)(1), (4) and (5), or relating to the threats referred to in Article 8(1)(a), (b), (c), (d), (f) and (g) and Article 11(2) of the [Organic law of 30 November 1998 on the intelligence and security services], the advance assessment of passengers shall be based on a positive match resulting from comparing passenger data against:

(1) the databases managed by the competent services or which are directly available or accessible to those services in the course of their functions or against the lists of individuals drawn up by the competent services in the course of their functions.

(2) the assessment criteria pre-determined by the PIU, as referred to in Article 25.

3. For the purposes referred to in Article 8(1)(3), the advance assessment of passengers shall be based on a positive match resulting from comparing passenger data against the databases referred to in Article 8(2)(1).

4. Positive matches shall be validated by the PIU within 24 hours of receipt of the automated notification of the positive match.

5. From the moment of that validation, the competent service which originally identified the positive match shall take further action without delay.'

47. Chapter 11 of the Law of 25 December 2016, entitled 'Processing of passenger data with a view to improving border controls and combating illegal immigration', comprises Articles 28 to 31 thereof.

48. Article 28 of that law provides:

'1. This Chapter applies to the processing of passenger data by the police services responsible for carrying out border checks and by the Office des étrangers [(Immigration Office)], carried out with a view to improving the checks on persons at external borders and with a view to combating illegal immigration.

2. It applies without prejudice to the obligations incumbent on the police services responsible for carrying out border checks and on the [Immigration Office] to transfer personal data or information in accordance with legal or statutory provisions.'

49. Under Article 29 of that law:

1. For the purposes of Article 28(1) passenger data are transferred to the police services responsible for carrying out border checks and to the [Immigration Office] to enable them to perform their statutory duties, within the limits provided for in this article.

2. Only the passenger data referred to in Article 9(1)(18) concerning the following passenger categories shall be transferred:

(1) passengers who intend to enter or have entered Belgian territory at an external border;

(2) passengers who intend to leave or have left Belgian territory at an external border;

(3) passengers who intend to pass through, are located in, or have passed through an international transit area situated on Belgian territory.

3. The passenger data referred to in paragraph (2) shall be transferred to the police services responsible for carrying out checks at Belgium's external border immediately after they have been entered in the passenger database. The said services shall save those data in a temporary file and delete them within 24 hours of the transfer.

4. When it needs them to perform its statutory duties, the passenger data referred to in paragraph (2) shall be transferred to the [Immigration Office] immediately after they have been entered in the passenger database. The Office shall save those data in a temporary file and delete them within 24 hours of the transfer.

After that period has passed, if the [Immigration Office] requires access to the passenger data referred to in paragraph (2) for the purposes of performing its statutory duties, it shall send a duly reasoned request to the PIU.

...'

50. The Law of 25 December 2016 became applicable to airlines, carriers operating international passenger service (HST carriers) and travel intermediaries in a contract with those carriers (HST ticket distributors), and bus carriers, respectively, by the arrêté royal du 1 juillet 2017 relatif à l'exécution de la loi du 25 décembre 2016, reprenant les obligations pour les compagnies aériennes (Royal Decree of 18 July 2017 implementing the Law of 25 December 2016 on the obligations incumbent on airlines, Moniteur belge of 28 July 2017, p. 75934), by the arrêté royal du 3 février 2019 relatif à l'exécution de la loi du 25 décembre 2016, reprenant les obligations pour les transporteurs HST et distributeurs de tickets HST (Royal Decree of 3 February 2019 implementing the Law of 25 December 2016 on the obligations incumbent on HST carriers and HST ticket distributors, Moniteur belge of 12 February

2019, p. 13018) and by the arrêté royal du 3 février 2019 relatif à l'exécution de la loi du 25 décembre 2016, reprenant les obligations pour les transporteurs par bus (Royal Decree of 3 February 2019 implementing the Law of 25 December 2016 on the obligations incumbent on bus carriers, Moniteur belge of 12 February 2019, p. 13023).

II. The dispute in the main proceedings and the questions referred for a preliminary ruling

51. By application of 24 July 2017, the Ligue des droits humains brought an action before the Cour constitutionnelle (Constitutional Court, Belgium) seeking annulment in full or in part of the Law of 25 December 2016.

52. The referring court states that that law transposes, into domestic law, the PNR Directive and the API Directive as well as, in part, Directive 2010/65. According to the referring court, it follows from the travaux préparatoires that that law seeks to 'create a legal framework requiring international passenger transport carriers in various sectors (air, rail, international road and sea), as well as tour operators, to transfer data on their passengers to a database managed by the [Service public fédéral intérieur (Home Affairs Federal Public Service, Belgium)]'. The national legislature also stated that the intended purposes of the Law of 25 December 2016 fall into three categories, namely (i) the prevention, detection, investigation and prosecution of criminal offences or the enforcement of criminal penalties; (ii) the tasks of the intelligence and security services; and (iii) improving external border controls and combating illegal immigration.

53. In support of its action, the Ligue des droits humains raises two pleas, the first, alleging breach of Article 22 of the Constitution, read in conjunction with Article 23 of the GDPR, Articles 7, 8 as well as Article 52(1) of the Charter as well as Article 8 ECHR, and the second, alleging, in the alternative, breach of Article 22 of the Charter, read in conjunction with Article 3(2) TEU and Article 45 of the Charter.

54. By its first plea, the Ligue des droits humains submits, in essence, that that law entails an interference with the rights to respect for private life and the protection of personal data, which does not comply with Article 52(1) of the Charter and, inter alia, the principle of proportionality. The scope of that law and the definition of the data collected, which may reveal sensitive information, are too broad. Similarly, the concept of 'passenger', within the meaning of that same law, leads to systematic, non-targeted automated processing of the data of all passengers. Moreover, the nature and detailed rules of the 'pre-screening' method and the databases against which those data are compared, once transmitted, are not defined in a sufficiently clear manner. Furthermore, the Law of 25 December 2016

pursues objectives other than those of the PNR Directive. Finally, the five-year period laid down by that law for the retention of those data is disproportionate.

55. By its second plea, concerning Article 3(1), Article 8(2) and Articles 28 to 31 of the Law of 25 December 2016, the Ligue des droits humains submits that, by extending the system provided for by the PNR Directive to intra-EU transport operations, those provisions have the effect of indirectly restoring internal border control, in breach of the free movement of persons. Once a person is on Belgian territory, whether on arrival, departure or during a stop-over, their data are automatically collected.

56. The Council of Ministers disputes those arguments. It considers, in particular, that the first plea is inadmissible in so far as it concerns the GDPR, which is not applicable to the Law of 25 December 2016. Furthermore, the processing of data provided for by that law, in accordance with the PNR Directive, is an essential tool for, *inter alia*, the fight against terrorism and serious crime, and the measures stemming from that law are necessary to achieve the aims pursued and are proportionate.

57. As regards the first plea, the referring court asks, first of all, whether the protection provided for by the GDPR applies to the processing of data established by the Law of 25 December 2016, which is intended to implement, primarily, the PNR Directive. Next, that court notes, with reference to the case-law stemming from Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017 (EU:C:2017:592), that the definition of PNR data in Article 3(5) of and Annex I to that directive may, first, not be sufficiently clear and precise, on account of the non-exhaustive nature of the description of some of those data contained in those provisions and, secondly, lead indirectly to the disclosure of sensitive data. Furthermore, the definition of the concept of ‘passenger’ in Article 3(4) of that directive may result in the collection, transfer, processing and retention of PNR data constituting generalised and indiscriminate obligations, applying to every person carried or to be carried who appears on the passengers list, regardless of whether there are serious grounds for believing that that person has committed or is about to commit an offence or has been found guilty of an offence.

58. The referring court also observes that PNR data, in accordance with the provisions of the PNR Directive, are systematically subject to advance assessment involving cross-checks with databases or pre-determined criteria with a view to finding matches. The Consultative Committee of Convention No 108 of the Council of Europe indicated in its Opinion of 19 August 2016 on the Data protection implications of the processing of Passenger Name Records (T-PD(2016)18rev) that the processing of personal data concerns all passengers and not only the targeted individuals suspected of involvement in a criminal offence or posing an immediate threat to national security or public order, and that PNR

data may not only be compared ('data matching') to databases but also be processed by 'data mining' according to selectors or predictive algorithms, with the aim of identifying anyone who may be involved or might engage in criminal activities, as this assessment of passengers by data mining may raise the question of predictability, in particular when operated on the basis of predictive algorithms using dynamic criteria that may constantly evolve in light of self-learning capacities. In that context, the referring court considers that, although the pre-determined criteria for identifying high-risk profiles must be specific, reliable and non-discriminatory, in accordance with Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017 (EU:C:2017:592), it seems to be impossible technically to define those criteria further.

59. As regards the five-year retention period and access to the data provided for in Article 12 of the PNR Directive, the referring court notes that the Commission for the protection of privacy (Belgium), in its avis d'initiative no 01/2010 du 13 janvier 2010 relatif au projet de loi portant assentiment à l'accord PNR UE-États-Unis d'Amérique (own-initiative Opinion No 01/2010 of 13 January 2010 on the Draft law ratifying the PNR Agreement between the European Union and the United States of America), considered that when data is retained for a long period and is stored en masse, the risk of the data subjects being profiled rises, as does the potential for improper use of the data for purposes other than those originally intended. It is also apparent from the Opinion of 19 August 2016 of the Consultative Committee of Convention No 108 of the Council of Europe that masked out data still enables individuals to be identified and continue as such to constitute personal data, and that their retention should be limited in time in order to avoid permanent and general surveillance.

60. In those circumstances, having regard to the case-law resulting in particular from Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017 (EU:C:2017:592), the referring court asks whether the system for the collection, transfer, processing and retention of PNR data established by the PNR Directive may be regarded as coming within the limits of what is strictly necessary. That court considers that it is also appropriate to ascertain whether that directive precludes national legislation authorising the processing of PNR data for a purpose other than that provided for by that directive and whether disclosure of the full data after they have been depersonalised, pursuant to Article 12 of that directive, may be approved by a national authority such as the PIU created by the Law of 25 December 2016.

61. As regards the second plea, the referring court states that Article 3(1) of that law lays down the obligations of carriers and tour operators regarding the transfer of data relating to passengers 'travelling to or from or transiting through Belgian territory'. That court adds, with regard to the scope

of that law, that the national legislature decided to ‘inclu[de] intra-EU travel in the data collection’ in order to obtain ‘a fuller picture of passenger movements representing a potential threat to intra-Community and national security’, as envisaged by Article 2 of the PNR Directive, read in conjunction with recital 10 thereof, for flights within the European Union. The referring court also states that the Commission for the protection of privacy, in its Opinion No 55/2015 of 16 December 2015 on the draft bill which became the Law of 25 December 2016, had raised the issue of whether the Belgian PNR system might conflict with the principle of the free movement of persons, in so far as that system includes transport operations carried out within the European Union.

62. It is in those circumstances that the Cour constitutionnelle (Constitutional Court) decided to stay proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

‘(1) Is Article 23 of [the GDPR], read in conjunction with Article 2(2)(d) of that regulation, to be interpreted as applying to national legislation such as the [Law of 25 December 2016], which transposes [the PNR Directive] as well as [the API Directive] and Directive [2010/65]?’

(2) Is Annex I to [the PNR Directive] compatible with Articles 7, 8 and 52(1) of [the Charter], given that the data it refers to are very wide in scope – particularly the data referred to in paragraph 18 of Annex I to [that directive], which go beyond the data referred to in Article 3(2) of [the API Directive] – and also given that, taken together, they may reveal sensitive information, and thus go beyond what is “strictly necessary”?

(3) Are paragraphs 12 and 18 of Annex I to [the PNR Directive] compatible with Articles 7, 8 and 52(1) of [the Charter], given that, having regard to the word “including”, the data referred to in those paragraphs is given by way of example and not exhaustively, such that the requirement for precision and clarity in rules which interfere with the right to respect for private life and the right to protection of personal data is not satisfied?

(4) Are Article 3(4) of [the PNR Directive] and Annex I to that directive compatible with Articles 7, 8 and 52(1) of [the Charter], given that the system of generalised collection, transfer and processing of passenger data established by those provisions relates to any person using the mode of transport concerned, regardless of whether there is any objective ground for considering that that person may present a risk to public security?

(5) Is Article 6 of [the PNR Directive], read in conjunction with Articles 7, 8 and 52(1) of [the Charter], to be interpreted as precluding national legislation such as the contested law, which includes, among the purposes for which PNR data is processed, [monitoring] activities within the remit of the

intelligence and security services, thus treating that purpose as an integral part of the prevention, detection, investigation and prosecution of terrorist offences and serious crime?

(6) Is Article 6 of [the PNR Directive] compatible with Articles 7, 8 and 52(1) of [the Charter], given that the advance assessment for which it provides, which is made by comparing passenger data against databases and pre-determined criteria, applies to such data in a systematic and generalised manner, regardless of whether there is any objective ground for considering that the passengers concerned may present a risk to public security?

(7) Can the expression “another national authority competent under national law” in Article 12(3) of [the PNR Directive] be interpreted as including the PIU created by the Law of 25 December 2016, which would then have power to authorise access to PNR data after six months had passed, for the purposes of ad hoc searches?

(8) Is Article 12 of [the PNR Directive], read in conjunction with Articles 7, 8 and 52(1) of [the Charter], to be interpreted as precluding national legislation such as the contested law which provides for a general data retention period of five years, without making any distinction in terms of whether the advance assessment indicated that the passengers might present a risk to public security?

(9) (a) Is [the API Directive] compatible with Article 3(2) [TEU] and Article 45 of [the Charter], given that the obligations for which it provides apply to flights within the European Union?

(b) Is [the API Directive], read in conjunction with Article 3(2) [TEU] and Article 45 of [the Charter], to be interpreted as precluding national legislation such as the contested law which, for the purposes of combating illegal immigration and improving border controls, authorises a system of collection and processing of data relating to passengers “travelling to, from or transiting through Belgian territory”, which may indirectly involve a re-establishment of internal border controls?

(10) If, on the basis of the answers to the preceding questions, the Cour constitutionnelle (Constitutional Court) concludes that the contested law, which transposes, inter alia, [the PNR Directive], fails to fulfil one or more of the obligations arising under the provisions referred to in those questions, would it be open to it to maintain the effects of the [Law of 25 December 2016], on a temporary basis, in order to avoid legal uncertainty and enable the data hitherto collected and retained to continue to be used for the purposes envisaged by the law?

III. Consideration of the questions referred

A. Question 1

63. By its Question 1, the referring court asks, in essence, whether Article 2(2)(d) and Article 23 of the GDPR must be interpreted as meaning that that regulation applies to the processing of personal data envisaged by national legislation intended to transpose, into domestic law, the provisions of the PNR Directive, those of the API Directive and also those of Directive 2010/65, in particular, the transfer, the retention and the processing of PNR data.

64. As is apparent from Article 2(1) of the GDPR, that regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of such data which form part of a filing system or are intended to form part of a filing system. The concept of 'processing' is defined in broad terms in Article 4(2) of that regulation as including, *inter alia*, collection, recording, storage, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or erasure of such data or sets of data.

65. The Belgian Government submits however that the transfer of PNR data by economic operators to the PIU, for the purposes of the prevention and detection of criminal offences, as provided for in Article 1(1)(a) and (2) and Article 8 of the PNR Directive, which constitutes 'processing' of personal data within the meaning of Article 4(2) of the GDPR, as well as the advance collection thereof, fall outside the scope of Article 2(2)(d) of the said regulation, on the ground that the case-law stemming from the judgment of 30 May 2006, *Parliament v Council and Commission*, C-317/04 and C-318/04, EU:C:2006:346 (paragraphs 57 to 59), relating to the first indent of Article 3(2) of Directive 95/46, is applicable to that provision of the regulation.

66. In that regard, it is true that, as previously held by the Court, the first indent of Article 3(2) of Directive 95/46, which was repealed and replaced by the GDPR with effect from 25 May 2018, generally excluded from its scope 'processing operations concerning public security, defence [and] State security', without drawing any distinction according to the person carrying out the data processing operation concerned. Thus, processing operations carried out by private operators resulting from obligations imposed by the public authorities could, where appropriate, fall within the scope of the exception laid down in that provision, given that the wording of that provision covered all processing operations concerning public security, defence or State security, regardless of the person carrying out those operations (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 101).

67. However, Article 2(2)(d) of the GDPR draws such a distinction, since, as noted by the Advocate General in points 41 and 46 of his Opinion, it is clearly apparent from the wording of that provision that two conditions need to be met for data processing to fall within the scope of the exception it lays

down. While the first one of those conditions related to the purposes of the processing operation, namely, the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, the second condition relates to the person carrying out that operation, namely a 'competent authority' within the meaning of that provision.

68. As the Court has also held, it is apparent from Article 23(1)(d) and (h) of the GDPR that the processing of personal data carried out by individuals for the purposes set out in Article 2(2)(d) of that regulation falls within the scope of thereof (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 102).

69. It follows that the case-law stemming from the judgment of 30 May 2006, *Parliament v Council and Commission* (C-317/04 and C-318/04, EU:C:2006:346), relied on by the Belgian Government, is not applicable to the exception to the scope of the GDPR set out in Article 2(2)(d) thereof.

70. In addition, that exception, like the other exceptions to the scope of the GDPR laid down in Article 2(2) of that regulation, must be interpreted strictly.

71. As is apparent from recital 19 of the GDPR, the reason for that exception is that the processing of personal data by authorities competent for the purposes, *inter alia*, of the prevention and detection of criminal offences, including the safeguarding against and the prevention of threats to public security is governed by a more specific EU legal act, namely Directive 2016/680, which was adopted on the same day as the GDPR (judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 69).

72. As is stated, moreover, in recitals 9 to 11 of Directive 2016/680, the latter lays down the specific rules relating to the protection of natural persons with regard to such processing operations, respecting the specific nature of those activities in the fields of judicial cooperation in criminal matters and police cooperation, while the GDPR defines general rules concerning the protection of those persons which are intended to apply to those processing operations when Directive 2016/680, as a more specific legal act, does not apply. In particular, according to recital 11 of that directive, the GDPR applies to processing of personal data that is carried out by a 'competent authority' within the meaning of Article 3(7) of the said directive, but for purposes other than those of that directive (see, to that effect, judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 70).

73. As regards the first condition set out in paragraph 67 above, and, specifically, the purposes for which the personal data are to be processed under the PNR Directive, it is appropriate to recall that, in accordance with Article 1(2) of that directive, PNR data may be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. Those purposes are covered by those set out in Article 2(2)(d) of the GDPR and Article 1(1) of Directive 2016/680, with the result that such processing operations may be caught by the exception laid down in Article 2(2)(d) of that regulation and, consequently, be within the scope of that directive.

74. By contrast, that is not the case with regard to the processing operations covered by the API Directive and Directive 2010/65, the purposes of which are other than those in Article 2(2)(d) of the GDPR and Article 1(1) of Directive 2016/680.

75. Indeed, the API Directive aims at improving border controls and combating illegal immigration, as is apparent from recitals 1, 7 and 9 as well as Article 1 thereof, by the transmission of advance passenger data by carriers to the competent national authorities. Moreover, several recitals and provisions of that directive make clear that the data processing operations envisaged for its implementation are within the scope of the GDPR. Recital 12 of that directive states that ‘Directive [95/46] applies with regard to the processing of personal data by the authorities of the Member States’. In addition, the fifth subparagraph of Article 6(1) of the API Directive specifies that Member States may also use API data for law enforcement purposes, ‘subject to data protection provisions under Directive [95/46]’, that phrase being used also in the third subparagraph of that provision. Similarly, the phrase ‘without prejudice to the provisions of Directive [95/46]’ is used, *inter alia*, in recital 9 of the API Directive. Article 6(2) of the API Directive provides, lastly, that passengers must be informed by carriers ‘in accordance with the provisions laid down in Directive [95/46]’.

76. As to Directive 2010/65, it follows from recital 2 and Article 1(1) thereof that the purpose of that directive is to simplify and harmonise the administrative procedures applied to maritime transport by making the electronic transmission of information standard and by rationalising reporting formalities, for the facilitation of maritime transport, and in order to reduce the administrative burden for shipping companies. Article 8(2) of the said directive confirms that the data processing operations envisaged for its implementation fall within the scope of the GDPR, since that provision requires Member States, concerning personal data, to ensure compliance with Directive 95/46.

77. It follows that the data processing operations envisaged by national legislation transposing, into domestic law, the provisions of the API Directive and of Directive 2010/65 are within the scope of the GDPR. By contrast, data processing operations envisaged by national legislation that transpose, into

domestic law, the PNR Directive may, pursuant to the exception in Article 2(2)(d) of that regulation, fall outside the scope of the regulation, subject to compliance with the second condition recalled in paragraph 67 above, namely that the person carrying out the processing operations is a competent authority within the meaning of the latter provision.

78. As regards that second condition, the Court has held that, in so far as Directive 2016/680 defines, in Article 3(7) thereof, the concept of ‘competent authority’, such a definition must be applied, by analogy, to Article 2(2)(d) of the GDPR (see, to that effect, judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 69).

79. Pursuant to Articles 4 and 7 of the PNR Directive, each Member State must, respectively, designate, as its PIU, an authority competent for the prevention, detection, investigation or prosecution of terrorist offences and of serious crime and adopt a list of the competent authorities entitled to request or receive PNR data or the result of processing those data from the PIU, the latter authorities being also competent for those purposes, as specified in Article 7(2) of that directive.

80. It follows therefrom that the processing of PNR data by the PIU and the said competent authorities for such purposes satisfy both conditions referred to in paragraph 67 above, with the result that those operations are covered by the provisions of the PNR Directive itself as well as those of Directive 2016/680 and not those of the GDPR, as confirmed, moreover, by recital 27 of the PNR Directive.

81. By contrast, since economic operators such as air carriers, although they have a legal obligation to transfer PNR data, are neither in charge of exercising public authority nor entrusted with public powers by that directive, they cannot be regarded as being competent authorities within the meaning of Article 3(7) of Directive 2016/680 and Article 2(2)(d) of the GDPR, with the result that the collection of those data and transfer to the PIU, by air carriers, are covered by that regulation. The same applies in a situation, such as that provided for by the Law of 25 December 2016, where the collection and transfer of the said data are operated by other carriers or by tour operators.

82. The referring, lastly, raises the question of the impact, if any, of the adoption of national legislation intended to transpose the provisions of the PNR Directive, those of the API Directive and also those of Directive 2010/65, such as the Law of 25 December 2016. In that regard, it should be borne in mind that, as is apparent from paragraphs 72 and 75 to 77 above, the data processing operations provided for under those last two directives fall within the scope of the GDPR, which entails general rules on the protection of natural persons with regard to the processing of personal data.

83. Thus, when a data processing operation carried out on the basis of that legislation is covered by the API Directive and/or Directive 2010/65, the GDPR applies to that operation. The same is true of a data processing operation carried out on that same basis and, in terms of its purpose and in addition to the PNR Directive, falls within the API Directive and/or Directive 2010/65. Lastly, when a data processing operation carried out on the basis of that same legislation, in terms of its purpose, falls outside the PNR Directive, the GDPR applies if the operation relates to the collection of PNR data and transfer to the PIU, by air carriers. By contrast, where such a processing operation is carried out by the PIU or the authorities competent for the purposes referred to in Article 1(2) of the PNR Directive, that operation is covered by Directive 2016/680, in addition to national law.

84. In the light of the foregoing, the answer to Question 1 is that Article 2(2)(d) and Article 23 of the GDPR must be interpreted as meaning that that regulation applies to the processing of personal data envisaged by national legislation intended to transpose, into domestic law, the provisions of the API Directive, those of Directive 2010/65 and also those of the PNR Directive in respect of, on the one hand, data processing operations carried out by private operators and, on the other hand, data processing operations carried out by public authorities covered, solely or in addition, by the API Directive or Directive 2010/65. By contrast, the said regulation does not apply to the data processing operations envisaged by such legislation which are covered only by the PNR Directive and are carried out by the PIU or by the authorities competent for the purposes referred to in Article 1(2) of that directive.

B. Questions 2 to 4 and Question 6

85. By its Questions 2 to 4 and Question 6, which it is appropriate to consider together, the referring court asks the Court, in essence, whether the PNR Directive is valid in the light of Articles 7 and 8 as well as Article 52(1) of the Charter. Those questions concern, *inter alia*:

- Annex I to that directive and the data listed in that annex, in particular those referred to in paragraphs 12 and 18 thereof, concerning the requirements for clarity and precision (Questions 2 and 3);
- Article 3(4) of the said directive and Annex I thereto, in that the system of generalised collection, transfer and processing of PNR data established by those provisions may apply to any person on a flight covered by the provisions of that directive (Question 4), and
- Article 6 of the PNR Directive in that it provides for advance assessment, by comparing PNR data against databases and/or processing them against pre-determined criteria, which applies to such data

in a systematic and generalised manner, regardless of whether there is any objective ground for considering that the passengers concerned may present a risk to public security (Question 6).

86. It should be noted as a preliminary point that, in accordance with a general principle of interpretation, an EU act must be interpreted, as far as possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter. Thus, if the wording of secondary EU legislation is open to more than one interpretation, preference should be given to the interpretation which renders the provision consistent with primary law rather than to the interpretation which leads to its being incompatible with primary law (judgment of 2 February 2021, *Consob*, C-481/19, EU:C:2021:84, paragraph 50 and the case-law cited).

87. In addition, it is settled case-law that, when a directive allows the Member States discretion to define transposition measures adapted to the various situations possible, they must, when implementing those measures, not only interpret their national law in a manner consistent with the directive in question but also ensure that they do not rely on an interpretation of the directive that would be in conflict with the fundamental rights protected by the EU legal order or with the other general principles recognised by EU law (see, to that effect, judgments of 15 February 2016, *N.*, C-601/15 PPU, EU:C:2016:84, paragraph 60 and the case-law cited, and of 16 July 2020, *État belge (Family reunification – Minor child)*, C-133/19, C-136/19 and C-137/19, EU:C:2020:577, paragraph 33 and the case-law cited).

88. As regards the PNR Directive, it should be noted that recitals 15, 20, 22, 25, 36 and 37 thereof stress the importance that the EU legislature, by referring to the high level of data protection, gives to the full respect for fundamental rights enshrined in Articles 7, 8 and 21 of the Charter as well as the principle of proportionality, with the result that, as stated in recital 36, that directive ‘should ... be implemented accordingly’.

89. In particular, recital 22 of the PNR Directive points out that, ‘[by] taking fully into consideration the principles outlined in recent relevant case-law of the [Court], the application of th[at] Directive should ensure full respect for fundamental rights, for the right to privacy and for the principle of proportionality’ and ‘genuinely meet the objectives of necessity and proportionality in order to achieve the general interests recognised by the [European] Union and the need to protect the rights and freedoms of others in the fight against terrorist offences and serious crime’. That recital adds that that application ‘should be duly justified and the necessary safeguards put in place to ensure the lawfulness of any storage, analysis, transfer or use of PNR data’.

90. Moreover, under Article 19(2) of the PNR Directive, the Commission, when reviewing the directive, must pay special attention to ‘compliance with the applicable standards of protection of personal data’, ‘the necessity and proportionality of collecting and processing PNR data for each of the purposes set out in this Directive’ and ‘the length of the data retention period’.

91. It is therefore appropriate to determine whether the PNR Directive, in accordance with, in particular, the requirements set out in its recitals and its provisions referred to in paragraphs 88 to 90 above, may be interpreted in a way that ensures full respect for the fundamental rights guaranteed in Articles 7 and 8 of the Charter as well as the principle of proportionality enshrined in Article 52(1) thereof.

1. Interferences with the fundamental rights guaranteed in Articles 7 and 8 of the Charter resulting from the PNR Directive

92. Article 7 of the Charter guarantees everyone the right to respect for his or her private and family life, home and communications, while Article 8(1) of the Charter expressly confers on everyone the right to the protection of personal data concerning him or her.

93. As is apparent from Article 3(5) of the PNR Directive and the list in Annex I thereto, the PNR data covered by that directive include, inter alia, besides the name(s) of the air passenger(s), information necessary to the reservation, such as the dates of intended travel and the travel itinerary, information relating to tickets, groups of persons checked-in under the same reservation number, passenger contact information, information relating to the means of payment or billing, information concerning baggage and general remarks regarding the passengers.

94. Since the PNR data therefore include information on identified individuals, namely the air passengers concerned, the various forms of processing to which those data may be subject affect the fundamental right to respect for private life, guaranteed in Article 7 of the Charter (see, to that effect, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 121 and 122 and the case-law cited).

95. Furthermore, the processing of PNR data such as that covered by the PNR Directive also falls within the scope of Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, accordingly, must necessarily satisfy the data protection requirements laid down in that article (see, to that effect, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 123 and the case-law cited).

96. It is settled case-law that the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined Articles 7 and 8 of the Charter, whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to those data with a view to their use by public authorities. In this connection, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference (Opinion 1/15, (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 124 and 126 and the case-law cited).

97. Thus, both the transfer of PNR data by air carriers to the PIU of the Member State concerned, provided for in Article 1(1)(a) of the PNR Directive, read in conjunction with Article 8 thereof, and the framework of conditions governing the retention of those data, their use and any further transfer to the competent authorities of that Member State, to the PIUs and the competent authorities of the other Member States, to Europol or to the authorities of third countries, which are permitted, *inter alia*, by Articles 6, 7, 9 and 10 to 12 of that directive, constitute interferences with the rights guaranteed in Articles 7 and 8 of the Charter.

98. As regards the seriousness of those interferences, it should be noted, first, that according to Article 1(1)(a), read in conjunction with Article 8 thereof, the PNR Directive provides for the systematic and continuous transfer to the PIUs of PNR data relating to any air passenger on an extra-EU flight within the meaning of Article 3(2) of that directive, operated between third countries and the European Union. As noted by the Advocate General in point 73 of his Opinion, such a transfer involves general and full access, by the PIUs, to the PNR data disclosed, concerning all the persons using air transport services, irrespective of subsequent use of those data.

99. Secondly, Article 2 of the PNR Directive provides, in paragraph 1 thereof, that Member States may decide to apply the directive to intra-EU flights within the meaning of Article 3(3) thereof, and specifies, in paragraph 2 thereof, that in that case all the provisions of the said directive 'shall apply to intra-EU flights as if they were extra-EU flights and to PNR data from intra-EU flights as if they were PNR data from extra-EU flights'.

100. Thirdly, even if some of the PNR data listed on Annex I to the PNR Directive, as summarised in paragraph 93 above, taken in isolation, do not appear to be liable to reveal precise information about the private life of the persons concerned, the fact remains that, taken as a whole, the data may, *inter alia*, reveal a complete travel itinerary, travel habits, relationships existing between one or more persons and the financial situation of air passengers, their dietary habits or state of health, and may

even reveal sensitive information about those passengers (see, to that effect, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 128).

101. Fourthly, under Article 6(2)(a) and (b) of the PNR Directive, the data transferred by air carriers are intended for advance assessment, prior to the passengers' scheduled arrival or departure, as well as subsequent assessment.

102. As regards advance assessment, it is apparent from Article 6(2)(a) and (3) of the PNR Directive that that assessment is carried out by the PIUs of the Member States, systematically and by automated means, that is to say continuously and regardless of whether there is any indication that there is a risk that the person concerned is involved in terrorist offences or serious crime. To that end, those provisions provide that PNR data may be compared against 'relevant databases' and be processed against 'pre-determined' criteria.

103. Against this background, it should be borne in mind that the Court has already held that the extent of the interference which automated analyses of PNR data entail in respect of the rights enshrined in Articles 7 and 8 of the Charter essentially depends on the pre-determined models and criteria and on the databases on which that type of data processing is based (Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 172).

104. As noted by the Advocate General in point 78 of his Opinion, the processing operation provided for in Article 6(3)(a) of the PNR Directive, namely the comparison of PNR data against 'relevant databases', may provide additional information on the private lives of air passengers and may allow very precise conclusions to be drawn in that regard.

105. As to the processing of PNR data against 'pre-determined criteria' provided for in Article 6(3)(b) of the PNR Directive, it is true that Article 6(4) of that directive requires that any assessment of passengers by those means must be carried out in a non-discriminatory manner and, in particular, should not be based on a series of characteristics referred to in the last sentence of that paragraph 4. In addition, the criteria used must be targeted, proportionate and specific.

106. That being said, the Court has already held that, since automated analyses of PNR data are carried out on the basis of unverified personal data and are based on pre-determined models and criteria, they necessarily present some margin of error (see, by analogy, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 169). In particular, as noted, in essence, by the Advocate General in point 78 of his Opinion, it is apparent from Commission Working Document (SWD(2020) 128 final) annexed to its report of 24 July 2020 on the review of the PNR Directive that

the number of positive matches from automated processing under Article 6(3)(a) and (b) of that directive which prove to be incorrect following individual review by non-automated means is fairly substantial, amounting in 2018 and 2019 to at least five out of six individuals identified. Those processing operations thus lead to a careful analysis of the PNR data relating to the said persons.

107. As regards the subsequent assessment of PNR data provided for in Article 6(2)(b) of the PNR Directive, it is apparent from that provision that, during the period of six months after the transfer of the PNR data, referred to in Article 12(2) of that directive, the PIU is required, upon request from the competent authorities, to provide them with the PNR data and process those data in specific cases, for the purposes of combating terrorist offences and serious crime.

108. In addition, even if, upon expiry of that period of six months, PNR data are depersonalised through masking out of certain data elements, the PIU may be required, pursuant to Article 12(3) of the PNR Directive, to disclose, following such a request, full PNR data in a form which permits the identification of the data subject by the competent authorities where it is reasonably believed that it is necessary for the purposes referred to Article 6(2)(b) of that directive, such disclosure being however subject to approval granted by a judicial authority or ‘another [competent] national authority’.

109. Fifthly, by providing, in Article 12(1) thereof, without providing further details in that regard, that PNR data are to be retained in a database for a period of five years following their transfer to the PIU of the Member State on the territory of which the flight is landing or departing, the PNR Directive, given the fact that, despite being depersonalised upon expiry of the initial period of six months through masking out of certain data elements, full PNR data may still be disclosed in the scenario referred to in the preceding paragraph, makes it possible for information on the private life of air passengers to be available for a period of time which the Court, in its Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017 (EU:C:2017:592, paragraph 132), has already described as being particularly long.

110. Given how common use of air transport services is, the effect of a retention period that long is that a very large part of the population of the European Union is liable to have its PNR data retained, repeatedly, under the system established by the PNR Directive and, accordingly, be accessible for analyses carried out in the context of advance and subsequent assessments by the PIU and competent authorities over a considerable – even indefinite – period of time, in the case of persons who travel by air more than once every five years.

111. In the light of all of the foregoing, it is appropriate to find that the PNR Directive entails undeniably serious interferences with the rights guaranteed in Articles 7 and 8 of the Charter, in so

far, *inter alia*, as it seeks to introduce a surveillance regime that is continuous, untargeted and systematic, including the automated assessment of the personal data of everyone using air transport services.

2. Justification for the interferences resulting from the PNR Directive

112. It must be borne in mind that the fundamental rights enshrined in Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society (Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 136 and the case-law cited, and judgment of 6 October 2020, *Privacy International*, C-623/17, EU:C:2020:790, paragraph 63 and the case-law cited).

113. Under the first sentence of Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Under the second sentence of Article 52(1) of the Charter, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. In this connection, Article 8(2) of the Charter states that personal data must, *inter alia*, be processed 'for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.

114. It should be added that the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the act which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned, bearing in mind, on the one hand, that that requirement does not preclude the limitation in question from being formulated in terms which are sufficiently open to be able to adapt to different scenarios and keep pace with changing circumstances (see, to that effect, judgment of 26 April 2022, *Poland v Parliament and Council*, C-401/19, EU:C:2022:297, paragraphs 64 and 74 and the case-law cited) and, on the other hand, that the Court may, where appropriate, specify, by means of interpretation, the actual scope of the limitation in the light of the very wording of the EU legislation in question as well as its general scheme and the objectives it pursues, as interpreted in view of the fundamental rights guaranteed by the Charter.

115. As regards observance of the principle of proportionality, the protection of the fundamental right to respect for private life at EU level requires, in accordance with settled case-law of the Court, that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary. In addition, an objective of general interest may not be pursued without having

regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue (Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 140, and judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 52 and the case-law cited).

116. More specifically, the question whether the Member States may justify a limitation on the rights guaranteed in Articles 7 and 8 of the Charter must be assessed by measuring the seriousness of the interference which such a limitation entails and by verifying that the importance of the objective of general interest pursued by that limitation is proportionate to that seriousness (see, to that effect, judgments of 2 October 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, paragraph 55 and the case-law cited, and of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 53 and the case-law cited).

117. In order to satisfy the proportionality requirement, the legislation in question entailing the interference must lay down clear and precise rules governing the scope and application of the measures provided for and imposing minimum safeguards, so that the persons whose data have been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data are subject to automated processing. Those considerations apply especially where the PNR data are liable to reveal sensitive passenger data (Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 141, and judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 132 and the case-law cited).

118. Thus, legislation that provides for the retention of personal data must continue to satisfy objective criteria that establish a connection between the data to be retained and the objective pursued (see, to that effect, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 191 and the case-law cited, and judgments of 3 October 2019, A and Others, C-70/18, EU:C:2019:823, paragraph 63, and of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 133).

(a) Observance of the principle of legality and respect for the essence of the fundamental rights in question

119. Provision is made in an EU legislative act for the limitation of the exercise of the fundamental rights guaranteed in Articles 7 and 8 of the Charter stemming from the system established by the PNR Directive. As to the question whether, in accordance with the case-law referred to in paragraph 114 above, that directive, as an act of EU law which permits interference with those rights, itself defines the scope of the limitation on the exercise of the rights concerned, it must be noted that the provisions of the said directive as well as Annexes I and II thereto, first, list PNR data and, secondly, provide a framework for processing those data, inter alia, by laying down the purposes and detailed rules governing those processing operations. Moreover that question is largely the same as that of compliance with the proportionality requirement referred to in paragraph 117 above (see, to that effect, judgment of 16 July 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559, paragraph 180), and will be examined in paragraph 125 et seq. below.

120. As regards respect for the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter, it is true that PNR data may, in some circumstances, reveal very specific information on the private life of a person. However, in so far as, on the one hand, the nature of that information is limited to certain aspects of a person's private life, concerning that person's air travel in particular, and, on the other hand, the PNR Directive expressly prohibits in Article 13(4) thereof the processing of sensitive data within the meaning of Article 9(1) of the GDPR, the data covered by that directive do not by themselves allow for a full overview of the private life of a person. In addition, that directive, in Article 1(2) thereof read in conjunction with Article 3(8) and (9) thereof as well as Annex II thereto, circumscribes the purposes for which those data are to be processed. Lastly, that same directive, in Articles 4 to 15 thereof, lays down the rules governing the transfer, processing and retention of those data as well as the rules intended to ensure, inter alia, the security, confidentiality and integrity of those data, and to protect them against unlawful access and processing. In those circumstances, the interferences which the PNR Directive entails do not adversely affect the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter.

(b) Objective of general interest and appropriateness of the processing of PNR data having regard to that objective

121. As to the question whether the system established by the PNR Directive pursues an objective of general interest, it is apparent from recitals 5, 6 and 15 of that directive that the objectives thereof are to ensure the internal security of the European Union and thus protect the life and safety of persons, while creating a legal framework that guarantees a high level of protection of passengers'

fundamental rights, in particular the right to the respect for private life and that of the protection of personal data, where PNR data are processed by the competent authorities.

122. To that end, Article 1(2) of the PNR Directive provides that PNR data collected in accordance with that directive may be subject to the processing operations referred to in Article 6(2)(a) to (c) thereof only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. Those purposes undoubtedly constitute objectives of general interest of the European Union that are capable of justifying even serious interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter (see, to that effect, judgment of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 42, and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 148 and 149).

123. As to the whether the system established by the PNR Directive is appropriate for the purpose of attaining the objectives pursued, it should be noted that while the possibility of ‘false negatives’ and the fairly substantial number of ‘false positives’ resulting, as noted in paragraph 106 above, from automated processing under that directive in 2018 and 2019, are liable to limit the appropriateness of that system, they are not capable, however, of rendering the said system inappropriate for the purpose of contributing to the attainment of the objective of combating terrorist offences and serious crime. As is apparent from the Commission working document referred to in paragraph 106 above, automated processing carried out under the said directive have indeed already made it possible to identify air passengers presenting a risk in the context of the fight against terrorist offences and serious crime.

124. In addition, having regard to the margin of error inherent in the automated processing of PNR data and, in particular, the fairly substantial number of ‘false positives’, the appropriateness of the system established by the PNR Directive essentially depends on the proper functioning of the subsequent verification of the results obtained under those processing operations, by non-automated means, which, pursuant to that directive, is task for the PIU. The provisions laid down to that effect by the said directive thus contribute to the attainment of those objectives.

(c) Whether the interferences from the PNR Directive are necessary

125. According to the case-law recalled in paragraphs 115 to 118 above, it must be determined whether the interferences resulting from the PNR Directive are limited to what is strictly necessary and, *inter alia*, whether that directive lays down clear and precise rules governing the scope and application of the measures provided for and whether the system it establishes continues to meet objective criteria that establish a connection between PNR data, closely linked to booking for and engaging in air travel,

and the objectives pursued by that directive, namely the fight against terrorist offences and serious crime.

(1) Air passenger data covered by the PNR Directive

126. It is necessary to assess whether the data headings in Annex I to the PNR Directive define in a clear and precise manner the PNR data which air carriers are required to provide to the PIU.

127. As a preliminary point, it must be recalled that, as is apparent from recital 15 of the PNR Directive, the EU legislature intended for the list of the PNR data to be obtained by a PIU to be drawn up ‘with the objective of reflecting the legitimate requirements of public authorities to prevent, detect, investigate and prosecute terrorist offences or serious crime, thereby improving internal security within the [European] Union as well as protecting the fundamental rights, in particular privacy and the protection of personal data’. In particular, under that same recital, those data ‘should only contain details of passengers’ reservations and travel itineraries that enable competent authorities to identify air passengers representing a threat to internal security’. In addition, the PNR Directive prohibits, in the first sentence of Article 13(4) thereof, ‘the processing of PNR data revealing a person’s race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation’.

128. Consequently, PNR data collected and provided in accordance with Annex I to the PNR Directive must relate directly to the flight operated and the passenger concerned and must be limited in such a way as to, on the one hand, meet solely the legitimate requirements of public authorities to prevent, detect, investigate and prosecute terrorist offences or serious crime and, on the other, exclude sensitive data.

129. Headings 1 to 4, 7, 9, 11, 15, 17 and 19 of Annex I to the PNR Directive meet those requirements as well as those of clarity and precision, in that they concern clearly identifiable and circumscribed information directly related to the flight operated and the passenger concerned. As noted by the Advocate General in point 165 of his Opinion, the same is true of headings 10, 13, 14 and 16, despite their ‘open-ended’ wording.

130. However, clarifications are needed for the purposes of interpreting headings 5, 6, 8, 12 and 18.

131. Heading 5, entitled ‘address and contact information (telephone number, email address)’, does not expressly specify whether the said address and contact information refer to the air passenger alone or also cover third parties who made the flight reservation for the air passenger, third parties through whom an air passenger may be contacted, or indeed third parties who are to be informed in the event

of an emergency. However, as noted by the Advocate General, in essence, in point 162 of his Opinion, given the requirements of clarity and precision, that heading cannot be interpreted as allowing, implicitly, also the collection and transfer of personal data of such third parties. Consequently, that heading should be interpreted as referring only to the postal address and contact information, namely the telephone number and email address, of the air passenger on behalf of whom the reservation is made.

132. As to heading 6, which relates to ‘all forms of payment information, including billing address’, that heading, in order to meet the requirements of clarity and precision, must be interpreted as covering solely information relating to the payment methods for, and billing of, the air ticket, to the exclusion of any other information not directly relating to the flight (see, by analogy, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 159).

133. Heading 8, which relates to ‘frequent flyer information’, must be interpreted, as noted by the Advocate General in point 164 of his Opinion, as referring exclusively to data relating to the status of the passenger concerned in the context of a customer loyalty programme of a given airline or a given group of airlines as well as the number identifying that passenger as a ‘frequent flyer’. Heading 8 thus does not permit the collection of information relating to transactions through which that status was acquired.

134. Heading 12 concerns ‘general remarks (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent)’.

135. In that regard, it must be noted from the outset that whereas the phrase ‘general remarks’ does not meet the requirements of clarity and precision in that it does not set, as such, any limitation on the nature and scope of the information that may be collected and provided to a PIU under heading 12 (see, to that effect, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 160), the list in brackets does.

136. Consequently, in order to interpret heading 12, in accordance with the case-law recalled in paragraph 86 above, in a manner that complies with the requirements of clarity and precision and, more generally, with Articles 7 and 8 as well as Article 52(1) of the Charter, it is appropriate to consider that only the collection and provision of information expressly listed under that heading are allowed, namely the name and gender of minor air passengers, their age, language(s) spoken, the name and

contact details of the guardian on departure and relationship to the minor, the name and contact details of the guardian on arrival and relationship to the minor, departure and arrival agent.

137. Lastly, heading 18 refers to ‘any advance passenger information (API) data collected (including the type, number, country of issuance and expiry date of any identity document, nationality, family name, given name, gender, date of birth, airline, flight number, departure date, arrival date, departure port, arrival port, departure time and arrival time)’.

138. As noted, in essence, by the Advocate General, in points 156 to 160 of his Opinion, it is apparent from that heading 18, read in the light of recitals 4 and 9 of the PNR Directive, that the information to which it refers is exhaustively the API data listed in the said heading as well as in Article 3(2) of the API Directive.

139. Thus heading 18, in so far as it is construed as covering only the information expressly referred to in that heading and in Article 3(2) of the API Directive, may be regarded as meeting the requirements of clarity and precision (see, by analogy, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 161).

140. Accordingly, it must be held that, interpreted in accordance with the considerations set out *inter alia* in paragraphs 130 to 139 above, Annex I to the PNR Directive is of a sufficiently clear and precise nature overall, thus defining the scope of the interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter.

(2) The purposes for which PNR data may be processed

141. As is apparent from Article 1(2) of the PNR Directive, the PNR data collected in accordance with that directive are to be processed for the purposes of combating ‘terrorist offences’ and ‘serious crime’.

142. As to whether the PNR Directive provides, in that context, for clear and precise rules that limit the application of the system established by that directive to what is strictly necessary for those purposes, it should be borne in mind, first, that the phrase ‘terrorist offences’ is defined in Article 3(8) of the said directive by reference to the ‘offences under national law referred to in Articles 1 to 4 of Framework Decision [2002/475]’.

143. In addition to the fact that that framework decision, in Articles 1 to 3 thereof, defined in a clear and precise manner ‘terrorist offences’, ‘offences related to a terrorist group’ and ‘offences related to terrorist activities’, which Member States had to ensure were made punishable as criminal offences under that framework decision, Directive 2017/541, in Articles 3 to 14 thereof, also defines those same offences in a clear and precise manner.

144. Secondly, Article 3(9) of the PNR Directive defines ‘serious crime’ by reference to the ‘offences listed in Annex II [to that directive] that are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State’.

145. However, first of all, that annex lists exhaustively the different categories of offences that might be covered by the notion of ‘serious crime’ referred to in Article 3(9) of the PNR Directive.

146. Next, having regard to the particular features, at the time that directive was adopted, of the criminal justice systems of the Member States in the absence of harmonisation of the offences thus referred to, it was possible for the EU legislature merely to refer to categories of offences without defining the constitutive elements thereof, especially since those elements are necessarily defined under the national law to which Article 3(9) of the PNR Directive refers, in that Member States are bound by the respect for the principle of legality of criminal offences and penalties as a component of the common value, shared with the European Union, of the rule of law under Article 2 TEU (see, by analogy, judgment of 16 February 2022, *Hungary v Parliament and Council*, C-156/21, EU:C:2022:97, paragraphs 136, 160 and 234), which principle is, moreover, is enshrined in Article 49(1) of the Charter, which Member States are required to observe when they implement an EU measure such as the PNR Directive (see, to that effect, judgment of 10 November 2011, *QB*, C-405/10, EU:C:2011:722, paragraph 48 and the case-law cited). Thus, in the light of the usual meaning of the terms used in that annex, it must be found that the said annex determines, in a sufficiently clear and precise manner, the offences that may constitute serious crime.

147. It is true that paragraphs 7, 8, 10 and 16 of Annex II relate to categories of offences that are very general (fraud, laundering of the proceeds of crime and counterfeiting of currency, environmental crime, illicit trafficking in cultural goods) while nonetheless referring to specific offences falling within those general categories. In order to ensure the requisite level of precision under Article 49 of the Charter also, those paragraphs must be interpreted as referring to the said offences, as defined in the relevant area of national and/or EU law. When interpreted that way those paragraphs can be regarded as meeting the requirements of clarity and precision.

148. Lastly, it is important also to bear in mind that, although, in accordance with the principle of proportionality, the objective of combating serious crime is capable of justifying the serious interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter which the PNR Directive entails, the same is not true of the objective of combating criminality in general, since the latter objective may justify solely non-serious interferences (see, by analogy, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 59 and the case-

law cited). Thus, that directive must ensure, by means of clear and precise rules, that the application of the system established by the said directive is limited to offences amounting to serious crime and thereby excludes those amounting to ordinary crime.

149. In that regard, as noted by the Advocate General in point 121 of his Opinion, many of the offences listed in Annex II to the PNR Directive – such as human trafficking, the sexual exploitation of children and child pornography, illicit trafficking in weapons munitions and explosives, money laundering, cybercrime, illicit trade in human organs and tissue, illicit trafficking in narcotic drugs and psychotropic substances, illicit trafficking in nuclear or radioactive materials, unlawful seizure of aircraft/ships, serious crimes within the jurisdiction of the International Criminal Court, murder, rape, kidnapping, illegal restraint and hostage-taking – are inherently and indisputably extremely serious.

150. In addition, although other offences, also referred to in that Annex II, are less likely, a priori, to be associated with serious crime, it is nevertheless apparent from Article 3(9) of the PNR Directive that those offences may be considered to amount to serious crime only if they are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of the Member State concerned. The requirements flowing from that provision, which relate to the nature and severity of the penalty applicable, are, in principle, such as to limit the application of the system established by that directive to offences that have the requisite level of seriousness to justify the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter stemming from the system established by the said directive.

151. Nonetheless, since Article 3(9) of the PNR Directive refers to the maximum rather than the minimum penalty applicable, it cannot be ruled out that PNR data may be processed for the purposes of combating offences which, although meeting the criterion laid down by that provision relating to the threshold of severity, amount to ordinary crime rather than serious crime, having regard to the particular features of the domestic criminal justice system.

152. It is thus for the Member States to ensure that the application of the system established by the PNR Directive is effectively limited to combating serious crime and that that system does not extend to offences that amount to ordinary crime.

(3) The link between PNR data and the purposes for which those data are processed

153. It is true that, as noted, in essence, by the Advocate General in point 119 of his Opinion, the wording of Article 3(8) and Article 3(9) of the PNR Directive, read in conjunction with Annex II thereto, does not expressly refer to a criterion that is capable of confining the scope of that directive

solely to offences that may, by their nature, have an objective link, even if only indirect one, with air travel and, therefore, with the categories of data transferred, processed and retained pursuant to that directive.

154. Nevertheless, as pointed out by the Advocate General in point 121 of his Opinion, certain offences listed in Annex II to the PNR Directive, such as human trafficking, illicit trafficking in narcotic drugs or weapons, facilitation of unauthorised entry and residence and the unlawful seizure of aircraft, are, by their very nature, likely to have a direct link with the carriage of passengers by air. The same is true of certain terrorist offences, such as causing extensive destruction to a transport system or an infrastructure facility or seizure of aircraft, offences under Article 1(1)(d) and (e) of Framework Decision 2002/475, to which Article 3(8) of the PNR Directive refers, or travelling for the purpose of terrorism and organising or otherwise facilitating such travelling, offences under Articles 9 and 10 of Directive 2017/541.

155. Against that background, it must also be borne in mind that the Commission provided reasons for its Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime of 2 February 2011 (COM(2011) 32 final), which became the PNR Directive, emphasising the fact that ‘the terrorist attacks in the United States in 2001, the aborted terrorist attack in August 2006 aimed at blowing up a number of aircraft on their way from the United Kingdom to the United States, and the attempted terrorist attack on board a flight from Amsterdam to Detroit in December 2009 showed the ability of terrorists to mount attacks, targeting international flights, in any country’ and that ‘most terrorist activities are transnational in character and involve international travel, inter alia to training camps outside the [European Union]’. In addition, in order to justify the need for analysis of PNR data for the purposes of combating serious crime, the Commission referred, by way of example, to the case of a group of human traffickers who had used fake documents to check in for a flight as well as that of a human and drug trafficking network which, for the purposes of importing drugs to several destinations in Europe, had used persons who were themselves trafficked persons and had bought their air tickets with stolen credit cards. All of those cases concerned offences having a direct link with the carriage of passengers by air in that they were offences targeting the carriage of passengers by air as well as offences committed during or through travel by air.

156. In addition, it is important to note that even offences that have no such direct link with the carriage of passengers by air may, depending on the circumstances of the case, have an indirect link with the carriage of passengers by air. Such is the case, in particular, when air transport is used as a

means of preparing such offences or evading criminal prosecution after committing such offences. By contrast, offences having no objective link, not even an indirect one, with the carriage of passengers by air cannot justify the application of the system established by the PNR Directive.

157. In those circumstances, Article 3(8) and (9) of that directive, read in conjunction with Annex II thereto and in the light of the requirements stemming from Articles 7 and 8 as well as Article 52(1) of the Charter, requires Member States, in particular upon individual review by non-automated means as referred to in Article 6(5) of that directive, to ensure that the application of the system established by it be limited to terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air.

(4) The air passengers and flights concerned

158. The system established by the PNR Directive covers the PNR data of anyone who meets the definition of 'passenger' within the meaning of Article 3(4) of that directive on a flight falling within the scope thereof.

159. According to Article 8(1) of the said directive, those data are transferred to the PIU of the Member State on the territory of which the flight will land or from the territory of which the flight will depart, regardless of whether there is any objective evidence from which it may be inferred that the passengers concerned may present a risk of being involved in a terrorist offence or serious crime. The data thus transferred are, inter alia, processed by automated means in connection with the advance assessment under Article 6(2)(a) and (3) of the PNR Directive, the objective of that assessment, as is apparent from recital 7 of that directive, being the identification of persons who were not suspected of involvement in terrorist offences or serious crime prior to that assessment and who should be subject to further examination by the competent authorities.

160. Specifically, it is apparent from Article 1(1)(a) and Article 2 of the PNR Directive that the latter distinguishes between passengers of extra-EU flights, operated between the European Union and third countries, and those of intra-EU flights, operated between different Member States.

161. As regards passengers of extra-EU flights, it must be recalled that, in respect of passengers flying between the European Union and Canada, the Court has already held that the automated processing of their PNR data, before their arrival in Canada, facilitates and expedites security checks, in particular at borders. Furthermore, the exclusion of certain categories of persons, or of certain areas of origin, would be liable to prevent the achievement of the objective of automated processing of PNR data, namely identifying, through verification of that data, persons liable to present a risk to public security

from amongst all air passengers, and make it possible for that verification to be circumvented (see, to that effect, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 187).

162. Those considerations can be applied *mutatis mutandis* to the situation of passengers flying between the European Union and all third countries, whom Member States are required to subject to the system established by the PNR Directive pursuant to Article 1(1)(a) of that directive, read in conjunction with Article 3(2) and (4) of the said directive. The transfer and advance assessment of the PNR data of air passengers entering or leaving the European Union cannot be restricted to a particular group of air passengers, given the very nature of the threats to public security that may stem from terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air between the European Union and third countries. Thus, it must be found that the necessary connection between those data and the objective of combating such offences exists, with the result that the PNR Directive does not go beyond what is strictly necessary merely because it imposes on Member States the systematic transfer and advance assessment of the PNR data of all those passengers.

163. As regards passengers flying between different Member States of the European Union, Article 2(1) of the PNR Directive, read in conjunction with recital 10 thereof, provides only that Member States may extend the application of the system established by that directive to intra-EU flights.

164. Thus, the EU legislature did not intend to oblige Member States to extend the application of the system established by the PNR Directive to intra-EU flights but, as is apparent from Article 19(3) of that directive, reserved its decision concerning such an extension, while taking the view that it should be preceded by a detailed assessment of the legal implications thereof, in particular for the fundamental rights of the data subjects.

165. In that regard, it should be noted that, by stating that the Commission's review report referred to in Article 19(1) of the PNR Directive must 'also include a review of the necessity, proportionality, and effectiveness of including within the scope of th[at] Directive the mandatory collection and transfer of PNR data relating to all or selected intra-EU flights' and that it must, in that regard, take into account 'the experience gained by Member States, especially those Member States that apply th[at] Directive to intra-EU flights in accordance with Article 2', Article 19(3) of that directive makes apparent that, for the EU legislature, the system established by the said directive must not necessarily extend to all intra-EU flights.

166. In a similar vein, Article 2(3) of the PNR Directive provides that Member States may decide to apply that directive only to selected intra-EU flights when they consider it necessary in order to pursue the objectives of the said directive, while being able to change the selected flights at any time.

167. In any event, the Member States' power to extend the application of the system established by the PNR Directive to intra-EU flights is to be exercised, as is apparent from recital 22 thereof, in full respect for the fundamental rights guaranteed in Articles 7 and 8 of the Charter. In that regard, while, according to recital 19 of the directive, it is for the Member States to assess the threats linked to terrorist offences and serious crime, the fact remains that the exercise of that power presupposes that, upon that assessment, Member States find that there is a threat related to those offences which is capable of justifying the application of the said directive to intra-EU flights also.

168. In those circumstances, a Member State, when it wishes to exercise the power provided for in Article 2 of the PNR Directive, either for all intra-EU flights under paragraph 2 of that article or only for such selected flights under paragraph 3 of the said article, is not exempt from the requirement to verify that the extension of the application of that directive to selected or all intra-EU flights is effectively necessary and proportionate for the purposes of attaining the objective set out in Article 1(2) of the said directive.

169. Thus, given recitals 5 to 7, 10 and 22 of the PNR Directive, the Member State must verify that the processing, under that directive, of the PNR data of passengers of intra-EU flights or selected such flights is strictly necessary, having regard to the seriousness of the interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter, in order to ensure the internal security of the European Union or, at least, that of that Member State and, thus, protect the life and safety of persons.

170. As regards, in particular, the threats related to terrorist offences, it is apparent from the Court's case-law that terrorist activities are amongst those capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, particularly, of directly threatening society, the population or the State itself, and that it is of paramount interest for each Member State to prevent and punish those activities to protect the essential functions of the State and the fundamental interests of society in order to safeguard national security. Such threats are distinguishable, by their nature, their particular seriousness and the specific nature of the circumstances of which they are constituted, from the general and permanent risk of serious criminal offences being committed (see, to that effect, judgments of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 135 and 136, and of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraphs 61 and 62).

171. Thus, in a situation where it is established, on the basis of the assessment carried out by a Member State, that there are sufficiently solid grounds for considering that the latter is confronted with a terrorist threat which is shown to be genuine and present or foreseeable, the fact that that Member State makes provision for the application of the PNR Directive, pursuant to Article 2(1) of that directive, to all intra-EU flights from or to the said Member State, for a limited period of time, does not appear to go beyond what is strictly necessary. The existence of that threat is, in itself, capable of establishing a connection between, on the one hand, the transfer and processing of the data concerned and, on the other, the fight against terrorism (see, by analogy, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 137).

172. The decision providing for that application must be open to effective review, either by a court or by an independent administrative body whose decision is binding, in order to verify that that situation exists and that the conditions and safeguards which must be laid down are observed. The period of application must also be limited in time to what is strictly necessary but may be extended if that threat persists (see, by analogy, judgments of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 168, and of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 58).

173. By contrast, in the absence of a genuine and present or foreseeable terrorist threat with which the Member State concerned is confronted, the indiscriminate application by that Member State of the system established by the PNR Directive not only to extra-EU flights but also to all intra-EU flights would not be considered to be limited to what is strictly necessary.

174. In such a situation, the application of the system established by the PNR Directive to selected intra-EU flights must be limited to the transfer and processing of the PNR data of flights relating, *inter alia*, to certain routes or travel patterns or to certain airports in respect of which there are indications that are such as to justify that application. It is for the Member State concerned, in that situation, to select the intra-EU flights, according to the outcome of the assessment which it must carry out on the basis of the requirements set out in paragraphs 163 to 169 above, and to review that assessment regularly in accordance with changes in the circumstances that justified their selection, for the purposes of ensuring that the application of the system established by that directive to intra-EU flights continues to be limited to what is strictly necessary.

175. It follows from the foregoing that the interpretation, thus followed, of Article 2 and Article 3(4) of the PNR Directive, in the light of Articles 7 and 8 as well as Article 52(1) of the Charter, is capable of ensuring that those provisions are within the limits of what is strictly necessary.

(5) Advance assessment of PNR data by automated processing

176. Under Article 6(2)(a) of the PNR Directive, the objective of the advance assessment provided for therein is to identify persons who require further examination, inter alia by the competent authorities referred to in Article 7 of that directive, in view of the fact that such persons may be involved in a terrorist offence or serious crime.

177. That advance assessment is carried out in two stages. As a first step, the PIU of the Member State concerned, pursuant to Article 6(3) of the PNR Directive, processes PNR data by automated means by comparing them against databases or pre-determined criteria. As a second step, should that processing by automated means lead to a positive match ('hit'), that unit, pursuant to Article 6(5) of the said directive, is to carry out an individual review by non-automated means to verify whether the competent authorities referred to in Article 7 of the said directive need to take action under national law ('match').

178. As recalled in paragraph 106 above, automated processing necessarily presents a fairly substantial margin of error, since it is carried out on the basis of unverified personal data and is based on pre-determined criteria.

179. In those circumstances, and given the need, highlighted in the fourth recital of the preamble to the Charter, to strengthen the protection of fundamental rights in the light, inter alia, of scientific and technological developments, it must be ensured, as stated in recital 20 and Article 7(6) of the PNR Directive, that no decision that produces an adverse legal effect on a person or significantly affects a person may be taken by the competent authorities only by reason of the automated processing of PNR data. Moreover, in accordance with Article 6(6) of that directive, the PIU itself may transfer PNR data to those authorities only after individual review by non-automated means. Lastly, in addition to those verifications which the PIU and the competent authorities are to carry out themselves, the lawfulness of all automated processing must be open to review by the data protection officer and the national supervisory authority, in accordance with Article 6(7) and Article 15(3)(b), respectively, of that directive as well as by the national courts in the context of the judicial redress referred to in Article 13(1) of that same directive.

180. As noted, in essence, by the Advocate General in point 207 of his Opinion, the national supervisory authority, the data protection officer and the PIU must be provided with the material and human resources necessary to carry out their review under the PNR Directive. Furthermore, it is important that the national legislation transposing that directive into domestic law and authorising the automated processing provided for by the directive lays down clear and precise rules for the

determination of the databases and criteria for analysis used, without relying, for the purposes of advance assessment, on other methods not referred to expressly in Article 6(2) of that directive.

181. Moreover, it follows from Article 6(9) of the PNR Directive that the consequences of advance assessment under Article 6(2)(a) thereof do not jeopardise the right of entry of persons enjoying the right of free movement within the territory of the Member State concerned as laid down in Directive 2004/38 and must, also, comply with Regulation No 562/2006. Thus, the system established by the PNR Directive does not allow the competent authorities to limit that right beyond what is prescribed by Directive 2004/38 and Regulation No 562/2006.

(i) Comparing PNR data against databases

182. Under Article 6(3)(a) of the PNR Directive, the PIU 'may', when carrying out the assessment referred to in Article 6(2)(a) of that directive, compare PNR data against '[relevant] databases' for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, 'including databases on persons or objects sought or under alert, in accordance with [EU], international and national rules applicable to such databases'.

183. Although it follows from the very wording of that Article 6(3)(a) of the PNR Directive, in particular from the word 'including', that the databases on persons or objects sought or under alert are among the 'relevant databases' referred to in that provision, that provision does not specify which other databases could also be considered to be 'relevant' in the light of the objectives pursued by that directive. As noted by the Advocate General in point 217 of his Opinion, that provision does not expressly indicate the nature of the data that those databases may contain or their relationship to those objectives nor does it mention whether PNR data must be compared exclusively against databases managed by public authorities or whether they may also be compared against databases managed by private individuals.

184. In those circumstances, Article 6(3)(a) of the PNR Directive could, *prima facie*, lend itself to an interpretation according to which PNR data may be used as mere search criteria for the purposes of conducting analyses using various databases, including databases managed and exploited by the security and intelligence agencies of Member States in order to pursue objectives other than those referred to in that directive, and that those analyses may take the form of 'data mining'. The fact that such analyses can be conducted and PNR data compared to such databases may give rise in the minds of passengers of carriage by air to the feeling that their private life is under a form of surveillance. Thus, while the advance assessment provided for in that provision relies on a relatively limited set of PNR data, such an interpretation of that Article 6(3)(a) cannot be adopted, since it would lead to a

disproportionate use of those data providing the means of establishing a detailed profile of the individuals concerned solely because they intend to travel by air.

185. Therefore, according to the case-law recalled in paragraphs 86 and 87 above, Article 6(3)(a) of the PNR Directive must be interpreted in such a way as to ensure full respect for the fundamental rights enshrined in Articles 7 and 8 of the Charter.

186. In that regard, it is apparent from recitals 7 and 15 of the PNR Directive that the automated processing provided for in Article 6(3)(a) of that directive must be limited to what is strictly necessary for the purposes of combating terrorist offences and serious crime, while ensuring a high level of protection of those fundamental rights.

187. In addition, as observed, in essence, by the Commission in response to a question put by the Court, the wording of that provision, that the PIU 'may' compare PNR data against the databases referred to therein, allows the PIU to choose a processing method that is limited to what is strictly necessary, depending on the particular situation. In the light of the obligation to comply with the requirements of clarity and precision necessary to ensure the protection of the fundamental rights enshrined in Articles 7 and 8 of the Charter, the PIU must limit the automated processing provided for in Article 6(3)(a) of the PNR Directive to the databases identifiable under that provision. In that regard, whereas the reference, in the latter provision, to 'relevant databases' does not lend itself to an interpretation defining in a sufficiently clear and precise manner the databases thus referred to, the same is not true of the reference to 'databases on persons or objects sought or under alert, in accordance with [EU], international and national rules applicable to such databases'.

188. Accordingly, as noted, in essence, by the Advocate General in point 219 of his Opinion, Article 6(3)(a) of the PNR Directive must, in the light of those fundamental rights, be interpreted as meaning that the latter databases are the only databases against which the PIU may compare PNR data.

189. As regards the requirements which those databases must satisfy, it is appropriate to note that, under Article 6(4) of the PNR Directive, advance assessment against pre-determined criteria must, pursuant to Article 6(3)(b) of that directive, be carried out in a non-discriminatory manner, those criteria must be targeted, proportionate and specific, and must be set and regularly reviewed by the PIUs in cooperation with the competent authorities referred to in Article 7 of the directive. If, by referring to Article 6(3)(b) of that directive, the wording of Article 6(4) thereof covers only the processing of PNR data against pre-determined criteria, the latter provision must be interpreted, in the light of Articles 7, 8 and 21 of the Charter, as meaning that the requirements it lays down apply *mutatis mutandis* to the comparison of those data against the databases referred in the preceding

paragraph, especially since those requirements correspond, in essence, to those adopted by the case-law arising from Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017 (EU:C:2017:592, paragraph 172), for the purposes of cross-checking PNR data against databases.

190. In that regard, it should be stated that the requirement as to the non-discriminatory nature of those databases implies, *inter alia*, that entry into the databases on persons sought or under alert is based on objective and non-discriminatory factors, defined in EU, international and national rules applicable to such databases (see, by analogy, judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 78).

191. In addition, in order to satisfy the requirement as to the targeted, proportionate and specific nature of the pre-determined criteria, the databases referred to in paragraph 188 above must be used in relation to the fight against terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air.

192. Moreover, the databases used pursuant to Article 6(3)(a) of the PNR Directive must, in view of the considerations set out in paragraphs 183 and 184 above, be managed by the competent authorities referred to in Article 7 of that directive or, with regard to EU databases as well as international databases, be exploited by those authorities in the context of their mission to combat terrorist offences and serious crime. That is the case of the databases on persons or objects sought or under alert, in accordance with the EU, international and national rules applicable to such databases.

(ii) Processing PNR data against pre-determined criteria

193. Article 6(3)(b) of the PNR Directive provides that the PIU may also process PNR data against pre-determined criteria. As is apparent from Article 6(2)(a) of that directive, the advance assessment and, accordingly, the processing of PNR data against pre-determined criteria is intended, in essence, to identify persons who may be involved in a terrorist offence or serious crime.

194. As regards the criteria that the PIU may use to that end, it should be noted, first, that according to the very wording of Article 6(3)(b) of the PNR Directive those must be ‘pre-determined’ criteria. As noted by the Advocate General in point 228 of his Opinion, that requirement precludes the use of artificial intelligence technology in self-learning systems (‘machine learning’), capable of modifying without human intervention or review the assessment process and, in particular, the assessment criteria on which the result of the application of that process is based as well as the weighting of those criteria.

195. It is important to add that use of such technology would be liable to render redundant the individual review of positive matches and monitoring of lawfulness required by the provisions of the PNR Directive. As observed, in essence, by the Advocate General in point 228 of his Opinion, given the opacity which characterises the way in which artificial intelligence technology works, it might be impossible to understand the reason why a given program arrived at a positive match. In those circumstances, use of such technology may deprive the data subjects also of their right to an effective judicial remedy enshrined in Article 47 of the Charter, for which the PNR Directive, according to recital 28 thereof, seeks to ensure a high level of protection, in particular in order to challenge the non-discriminatory nature of the results obtained.

196. Concerning, next, the requirements flowing from Article 6(4) of the PNR Directive, that provision states, in its first sentence, that any advance assessment against pre-determined criteria is to be carried out in a non-discriminatory manner and indicates, in its fourth sentence, that those criteria are in no circumstances to be based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.

197. Thus Member States cannot use, as pre-determined criteria, criteria that are based on the characteristics referred to in the preceding paragraph and use of which may result in discrimination. In that regard, it follows from the wording of the fourth sentence of Article 6(4) of the PNR Directive, according to which pre-determined criteria are 'in no circumstances' to be based on those characteristics, that that provision covers both direct and indirect discrimination. That interpretation is, moreover, confirmed by Article 21(1) of the Charter, in the light of which the said provision must be read, which prohibits 'any' discrimination based on the said characteristics. In those circumstances, pre-determined criteria must be defined in such a way that, while worded in a neutral fashion, their application does not place persons having the protected characteristics at a particular disadvantage.

198. As to the requirements relating to the targeted, proportionate and specific nature of pre-determined criteria, referred to in the second sentence of Article 6(4) of the PNR Directive, it follows from those requirements that the criteria used for the purposes of advance assessment must be determined in such a way as to target, specifically, individuals who might be reasonably suspected of involvement in terrorist offences or serious crime covered by that directive. That reading is supported by the very wording of Article 6(2)(a) thereof, which emphasises the 'fact' that the persons concerned 'may' be involved in 'a' terrorist offence or serious crime. In the same vein, recital 7 of the said directive states that the creation and application of assessment criteria should be limited to terrorist offences and serious crime 'for which the use of such criteria is relevant'.

199. In order to target in that way the persons thus referred to and given the risk of discrimination that criteria based on the characteristics set out in the fourth sentence of Article 6(4) of the PNR Directive entail, the PIU and the competent authorities cannot, generally, rely on those characteristics. By contrast, as pointed out by the German Government at the hearing, they can *inter alia* take into consideration specific features in the factual conduct of persons when preparing and engaging in air travel which, following the findings of and experience acquired by the competent authorities, might suggest that the persons acting in that way may be involved in terrorist offences or serious crime.

200. In that context, as noted by the Commission in response to a question put by the Court, pre-determined criteria must be defined in such a way as to take into consideration both ‘incriminating’ as well as ‘exonerating’ circumstances, since that requirement may contribute to the reliability of those criteria and, in particular, ensure that they are proportionate, as required by the second sentence Article 6(4) of the PNR Directive.

201. Lastly, the third sentence of Article 6(4) of that directive provides that pre-determined criteria must be reviewed regularly. In the context of that review, those criteria must be updated in accordance with changes in the circumstances that justified their being taken into consideration for the purposes of advance assessment, thus making it possible, *inter alia*, to react to developments in the fight against terrorist offences and serious crime referred to in paragraph 157 above (see, by analogy, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 82). In particular, that review must take into account the experience acquired in the context of the application of pre-determined criteria, in order to reduce, as much as possible, the number of ‘false positives’ and, thereby, contribute to the strictly necessary nature of the application of those criteria.

(iii) Safeguards surrounding the automated processing of PNR data

202. Compliance with the requirements to which the automated processing of PNR data is subject under Article 6(4) of the PNR Directive is required not only when determining and reviewing the databases as well as the pre-determined criteria provided for in that provision, but also, as noted by the Advocate General in point 230 of his Opinion, throughout the process of processing those data.

203. As regards pre-determined criteria specifically, it is appropriate, first of all, to specify that, although the PIU, as stated in recital 7 of the PNR Directive, must define the assessment criteria in a manner which keeps to a minimum the number of innocent people wrongly identified by the system established by that directive, that unit must still, in accordance with Article 6(5) and (6) of the said directive, individually review any positive match by non-automated means in order to identify, as

much as possible, any 'false positives'. In addition, notwithstanding the fact that they must set the assessment criteria in a non-discriminatory manner, the PIU is required to carry out such a review for the purposes of excluding any discriminatory results. The PIU must comply with that same review obligation when comparing PNR data against databases.

204. Thus, the PIU must refrain from transferring the results of those automated processing operations to the competent authorities referred to Article 7 of the PNR Directive when, having regard to the considerations set out in paragraph 198 above, they do not, following that review, have anything capable of giving rise, to the requisite legal standard, to a reasonable suspicion of involvement in terrorist offences or serious crime in respect of the persons identified by means of those automated processing operations or when they have reason to believe that those processing operations lead to discriminatory results.

205. As regards the verifications which the PIU must carry out to that end, it follows from Article 6(5) and (6) of the PNR Directive, read in conjunction with recitals 20 and 22 thereof, that Member States must lay down clear and precise rules capable of providing guidance and support for the analysis carried out by the agents in charge of the individual review, for the purposes of ensuring full respect for the fundamental rights enshrined in Articles 7, 8 and 21 of the Charter and, in particular, guarantee a uniform administrative practice within the PIU that observes the principle of non-discrimination.

206. In particular, given the fairly substantial number of 'false positives', mentioned in paragraph 106 above, Member States must ensure that the PIU establishes, in a clear and precise manner, objective review criteria enabling its agents to verify, on the one hand, whether and to what extent a positive match ('hit') concerns effectively an individual who may be involved in the terrorist offences or serious crime referred to in paragraph 157 above and must, therefore, be subject to further examination by the competent authorities referred to Article 7 of that directive, as well as, on the other hand, the non-discriminatory nature of automated processing operations under that directive and, in particular, the pre-determined criteria and databases used.

207. In that context, Member States are required to ensure that, in accordance with Article 13(5) of the PNR Directive, read in conjunction with recital 37 thereof, the PIUs maintain documentation relating to all processing of PNR data carried out in connection with the advance assessment, including in the context of the individual review by non-automated means, for the purpose of verifying its lawfulness and for the purpose of self-monitoring.

208. Next, the competent authorities, pursuant to the first sentence of Article 7(6) of the PNR Directive, cannot take any decision that produces an adverse legal effect on a person or significantly affects a

person only by reason of the automated processing of PNR data, which means, in connection with the advance assessment, that they must take into consideration and, where applicable, give preference to the result of the individual review conducted by non-automated means by the PIU over that obtained by automated processing. The second sentence of that Article 7(6) specifies that those decisions must not be discriminatory.

209. In that context, the competent authorities must ensure the lawfulness of the automated processing, in particular its non-discriminatory nature, as well as that of the individual review.

210. In particular, the competent authorities must ensure that the person concerned – without necessarily allowing that person, during the administrative procedure, to become aware of the pre-determined assessment criteria and programs applying those criteria – is able to understand how those criteria and those programs work, so that it is possible for that person to decide with full knowledge of the relevant facts whether or not to exercise his or her right to the judicial redress guaranteed in Article 13(1) of the PNR Directive, in order to call in question, as the case may be, the unlawful and, *inter alia*, discriminatory nature of the said criteria (see, by analogy, judgment of 24 November 2020, *Minister van Buitenlandse Zaken*, C-225/19 and C-226/19, EU:C:2020:951, paragraph 43 and the case-law cited). The same must apply to the review criteria mentioned in paragraph 206 above.

211. Lastly, in the context of redress introduced pursuant to Article 13(1) of the PNR Directive, the court responsible for reviewing the legality of the decision adopted by the competent authorities as well as, except in the case of threats to State security, the persons concerned themselves must have had an opportunity to examine both all the grounds and the evidence on the basis of which the decision was taken (see, by analogy, judgment of 4 June 2013, *ZZ*, C-300/11, EU:C:2013:363, paragraphs 54 to 59), including the pre-determined assessment criteria and the operation of the programs applying those criteria.

212. Moreover, according to Article 6(7) and Article 15(3)(b), respectively, of the PNR Directive, it is for the data protection officer and the national supervisory authority to ensure the monitoring of the lawfulness of the automated processing carried out by the PIU in connection with the advance assessment, monitoring which covers, *inter alia*, whether those operations are not discriminatory. While the first of those provisions states, to that end, that the data protection officer has access to all data processed by the PIU, that access must necessarily cover the pre-determined criteria and databases used by that unit in order to guarantee effectiveness and a high level of data protection that that officer must ensure in accordance with recital 37 of that directive. Similarly, the investigations,

inspections and audits that the national supervisory authority conducts pursuant to the second of those provisions may also concern those pre-determined criteria and those databases.

213. It follows from all of the foregoing that the provisions of the PNR Directive governing the advance assessment of PNR data under Article 6(2)(a) of that directive lend themselves to an interpretation that is consistent with Articles 7, 8 and 21 of the Charter and comes within the limits of what is strictly necessary.

(6) The disclosure and subsequent assessment of PNR data

214. According to Article 6(2)(b) of the PNR Directive, PNR data may also, on request of the competent authorities, be provided to the latter and assessed subsequently to the scheduled arrival in or departure from the Member State.

215. As regards the circumstances in which that disclosure and assessment may occur, it is apparent from the wording of that provision that the PIU may process PNR data in order to respond 'on a case-by-case basis' to 'a duly reasoned request based on sufficient grounds' from the competent authorities to have those data disclosed to them and processed 'in specific cases for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime'. In addition, where a request is introduced more than six months after the transfer of the PNR data to the PIU, a period upon the expiry of which the PNR data are depersonalised through masking out of certain elements, pursuant to Article 12(2) of that directive, Article 12(3) of the said directive provides that disclosure of the full PNR data and, therefore, a non-depersonalised version thereof, is permitted only under the dual condition that, first, it is reasonably believed that it is necessary for the purposes referred to in Article 6(2)(b) of the said directive and, secondly, it is approved by a judicial authority or another national authority competent under national law.

216. In that regard, it is apparent, first of all, from the very wording of Article 6(2)(b) of the PNR Directive that the PIU cannot systematically proceed to the subsequent disclosure and assessment of the PNR data of all air passengers and that it can only respond 'on a case-by-case basis' to requests relating to such processing operations 'in specific cases'. Having said that, in so far as that provision referred to 'specific cases', those processing operations must not necessarily be limited to the PNR data of a single air passenger but may, as noted by the Commission in response to a question put by the Court, also concern groups of persons provided that the persons concerned share a certain number of characteristics allowing them to be considered to constitute together a 'specific case' for the purposes of the intended data disclosure and assessment.

217. Concerning, next, the substantive conditions required for the PNR data of air passengers to be disclosed and assessed subsequently, although Article 6(2)(b) and Article 12(3)(a) of the PNR Directive use 'sufficient grounds' and 'reasonably', respectively, without expressly specifying the nature of such grounds, it nonetheless follows from the very wording of the first of those provisions, which refers to the purposes mentioned in Article 1(2) of the said directive, that PNR data can be disclosed and assessed subsequently only in order to verify whether there are indications that the data subject may be involved in terrorist offences or serious crime having, as follows from paragraph 157 above, an objective link, even if only an indirect one, with the carriage of passengers by air.

218. In the context of the system established by the PNR Directive, the disclosure and processing of PNR data under Article 6(2)(b) of that directive concern the data of persons who have already been subject to advance assessment prior to their scheduled arrival in or departure from the Member State concerned. In addition, a request for subsequent assessment may relate, *inter alia*, to persons whose PNR data have not been transferred to the competent authorities following an advance assessment, in so far as the latter has revealed nothing to suggest that those persons may be involved in terrorist offences or serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air. In those circumstances, the disclosure and processing of those data for the purposes of their subsequent assessment must be based on new circumstances justifying that use (see, to that effect, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 200 and the case-law cited).

219. As to the nature of the circumstances capable of justifying the disclosure and processing of PNR data for the purposes of their subsequent assessment, it is settled case-law that, since general access to all retained data, regardless of whether there is any, at least indirect, link with the intended purpose, cannot be regarded as being limited to what is strictly necessary, the legislation concerned, be it EU legislation or a national rule intended to transpose the latter, must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data in question. In that regard, such access can, as a general rule, be granted, in relation to the objective of combating crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be inferred that that data might, in a specific case, make an effective contribution to combating such activities

(judgments of 2 March 2021, Prokuratuur (Conditions of access to data relating to electronic communications), C-746/18, EU:C:2021:152, paragraph 50 and the case-law cited, and of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 105).

220. Thus, the terms ‘sufficient grounds’ and ‘reasonably’ in Article 6(2)(b) and Article 12(3)(a), respectively, of the PNR Directive must be interpreted, in the light of Articles 7 and 8 of the Charter, as referring to objective evidence capable of giving rise to a reasonable suspicion that the person concerned is involved in one way or another in serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air, whereas, as regards terrorist offences having such a link, that requirement is satisfied when there is objective evidence from which it can be inferred that the PNR data could, in a given case, contribute effectively to combating such offences.

221. Lastly, as regards the procedural conditions governing the disclosure and processing of PNR data for the purposes of their subsequent assessment, Article 12(3)(b) of the PNR Directive requires, where the request is introduced more than six months after their transfer to the PIU, that is to say when, pursuant to paragraph 2 of that article, those data have been depersonalised through masking out of the elements referred to in that paragraph 2, that the disclosure of the full PNR data and, therefore, of a non-depersonalised version thereof, must be approved by a judicial authority or by another national authority competent under national law. In that context, it is for those authorities to examine in full the merits of the request and, in particular, to ascertain whether the evidence in support of that request is likely to substantiate the substantive condition for the existence of ‘reasonabl[e]’ grounds referred to in the preceding paragraph.

222. It is true that, where a request for the subsequent disclosure and assessment of PNR data is introduced before the expiry of the period of six months after the transfer of those data, Article 6(2)(b) of the PNR Directive does not expressly provide for such a procedural requirement. Nonetheless, the interpretation of the latter provision must take into consideration recital 25 of that directive, from which it is apparent that, by laying down the said procedural requirement, the EU legislature intended ‘to ensure the highest level of data protection’ concerning access to PNR data in a form which permits direct identification of the data subject. Any request for subsequent disclosure and assessment implies such access to those data, irrespective of whether that request is introduced before the expiry of the period of six months after the transfer of the PNR data to the PIU or whether it is introduced after the expiry of that period.

223. In particular, in order to ensure, in practice, that fundamental rights are fully observed in the system put in place by the PNR Directive and, in particular, the conditions set out in paragraphs 218

and 219 above, it is essential that disclosure of PNR data for the purposes of subsequent assessment be, as a general rule, except in the event of duly justified urgency, subject to a prior review carried out either by a court or by an independent administrative authority, and that the decision of that court or body be made following a reasoned request by the competent authorities submitted, *inter alia*, within the framework of procedures for the prevention, detection or prosecution of crime. In the event of duly justified urgency, the review must take place within a short time (see, by analogy, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 202 and the case-law cited, and judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 110).

224. In those circumstances, the requirement for prior review under Article 12(3)(b) of the PNR Directive, for requests for the disclosure of PNR data introduced after the expiry of a period of six months following the transfer of those data to the PIU must also apply, *mutatis mutandis*, where the request for disclosure is introduced before the expiry of that period.

225. Moreover, if Article 12(3)(b) of the PNR Directive does not expressly specify the requirements which the authority responsible for carrying out the prior review must satisfy, it is settled case-law that, in order to ensure that the interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter which results from access to personal data is limited to what is strictly necessary, that authority must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue. As regards a criminal investigation in particular, it is a requirement of such a review that that authority must be able to strike a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access (judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 107 and the case-law cited).

226. For that purpose, such an authority must have a status that enables it to act objectively and impartially when carrying out its duties and must, therefore, be free from any external influence. That requirement of independence means that that authority must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review, free from any external influence. In particular, in the criminal field, the requirement of independence entails that the said authority, first, should not be involved in the conduct of the criminal investigation in question and, secondly, must have a neutral stance *vis-a-vis* the parties to the criminal proceedings

(see, to that effect, judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 108 and the case-law cited).

227. Accordingly, the provisions of the PNR Directive governing the subsequent disclosure and assessment of PNR data pursuant to Article 6(2)(b) of that directive lend themselves to an interpretation that is consistent with Articles 7 and 8 as well as Article 52(1) of the Charter and comes within the limits of what is strictly necessary.

228. In the light of all the foregoing, given that an interpretation of the PNR Directive in the light of Articles 7, 8 and 21 as well as Article 52(1) of the Charter ensures that that directive is consistent with those articles of the Charter, the examination of Questions 2 to 4 and Question 6 has revealed nothing capable of affecting the validity of the said directive.

C. Question 5

229. By its Question 5, the referring court seeks to ascertain whether Article 6 of the PNR Directive, read in the light of Articles 7 and 8 as well as Article 52(1) of the Charter, must be interpreted as precluding national legislation which authorises PNR data collected in accordance with that directive to be processed for the purposes of monitoring activities by the intelligence and security services.

230. It follows from the request for a preliminary ruling that, by that question, the referring court refers specifically to the activities covered by the *Sûreté de l'État* (State Security Services, Belgium) and the *Service général du renseignement et de la sécurité* (General intelligence and security services, Belgium), in the context of their respective duties relating to the protection of national security.

231. In that regard, in order to comply with the principles of legality and proportionality referred to in Article 52(1) of the Charter, the EU legislature provided clear and precise rules governing the purposes of the measures provided for by the PNR Directive which interfere with the fundamental rights guaranteed in Articles 7 and 8 of the Charter.

232. Article 1(2) of the PNR Directive states expressly that the PNR data collected in accordance with that directive may be processed 'only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, as provided for in points (a), (b) and (c) of Article 6(2) [of the said directive]'. The latter provision confirms the principle set out in that Article 1(2), by referring systematically to the concepts of 'terrorist offence' and 'serious crime'.

233. It is thus clear from the wording of those provisions that the list included therein of the objectives pursued by the processing of PNR data under the PNR Directive is exhaustive.

234. That interpretation is supported, *inter alia*, by recital 11 of the PNR Directive, according to which the processing of PNR data should be proportionate to ‘the specific security goals’ pursued by that directive, and by Article 7(4) thereof, according to which the PNR data and the result of processing those data received by the PIU may be further processed ‘only for the specific purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime’.

235. Moreover, the exhaustive nature of the purposes set out in Article 1(2) of the PNR Directive means also that PNR data may not be retained in a single database that may be consulted both for those as well as other purposes. Retention of those data in such a database would entail the risk that those data be used for purposes other than those referred to in that Article 1(2).

236. In the present case, in so far as, according to the referring court, the national legislation at issue in the main proceedings includes, among the purposes for which PNR data is to be processed, monitoring activities within the remit of the intelligence and security services, thus treating that purpose as an integral part of the prevention, detection, investigation and prosecution of terrorist offences and serious crime, that legislation is liable to disregard the exhaustive nature of the list of the objectives pursued by the processing of PNR data under the PNR Directive, which is a matter for the referring court to verify.

237. Accordingly, the answer to Question 5 is that Article 6 of the PNR Directive, read in the light of Articles 7 and 8 as well as Article 52(1) of the Charter, must be interpreted as precluding national legislation which authorises PNR data collected in accordance with that directive to be processed for purposes other than those expressly referred to in Article 1(2) of the said directive.

D. Question 7

238. By its Question 7, the referring court asks, in essence, whether Article 12(3)(b) of the PNR Directive must be interpreted as precluding national legislation pursuant to which the authority put in place as the PIU is also designated as a competent national authority with power to approve the disclosure of PNR data upon expiry of the period of six months after the transfer of those data to the PIU.

239. As a preliminary point, it must be noted that the Belgian Government harbours doubts as to whether the Court has jurisdiction to answer that question, as formulated by the referring court, given that the latter court is the only one with jurisdiction to interpret provisions of national law and, in particular, assess the requirements stemming from the Law of 25 December 2016 in the light of Article 12(3)(b) of the PNR Directive.

240. In that regard, suffice it to note that, by that question, the referring court is seeking the interpretation of a provision of EU law. In addition, if, in proceedings brought on the basis of Article 267 TFEU, the interpretation of provisions of national law is a matter for the courts of the Member States, not for the Court of Justice, and the Court has no jurisdiction to rule on the compatibility of rules of national law with EU law, the Court does have jurisdiction to provide the national court with all the guidance as to the interpretation of EU law necessary to enable that court to determine whether those national rules are compatible with EU law (judgment of 30 April 2020, CTT – Correios de Portugal, C-661/18, EU:C:2020:335, paragraph 28 and the case-law cited). It follows that the Court has jurisdiction to answer Question 7.

241. As to the substance, it should be noted that the wording of Article 12(3)(b) of the PNR Directive, which in its points (i) and (ii) refers to ‘a judicial authority’ and ‘another national authority competent under national law to verify whether the conditions for disclosure are met’, respectively, places both authorities on the same footing as is apparent from the use of the conjunction ‘or’ between those points (i) and (ii). It thus follows from that wording that the ‘other’ competent national authority thus referred to is an alternative to the judicial authority and, accordingly, must have a level of independence and impartiality similar to the latter.

242. That analysis is supported by the objective of the PNR Directive, mentioned in recital 25 thereof, to ensure the highest level of data protection concerning access to the full PNR data, which enable direct identification of the data subject. That same recital specifies, moreover, that that access should be granted only under very strict conditions after the period of six months following the transfer of PNR data to the PIU.

243. That analysis is also corroborated by the history of the PNR Directive. Whereas the proposal for a directive mentioned in paragraph 155 above, which became the PNR Directive, simply provided that ‘access to the full PNR data shall be permitted only by the Head of the Passenger Information Unit’, the version of Article 12(3)(b) of that directive finally adopted by the EU legislature designates, placing them on the same footing, the judicial authority and ‘another national authority’ competent to verify whether the conditions for disclosure of the full PNR data are met and approve such disclosure.

244. In addition and, most importantly, according to the settled case-law recalled in paragraphs 223, 225 and 226 above, it is essential that access to retained data by the competent authorities be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body be made following a reasoned request by those authorities submitted,

inter alia, within the framework of procedures for the prevention, detection or prosecution of crime. The requirement of independence that the body responsible for carrying out the prior review must satisfy also means that that body must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review objectively and impartially, and free from any external influence. In particular, in the criminal field the requirement of independence entails that the authority responsible for that prior review, first, should not be involved in the conduct of the criminal investigation in question and, secondly, must have a neutral stance vis-a-vis the parties to the criminal proceedings.

245. As noted by the Advocate General in point 271 of his Opinion, Article 4 of the PNR Directive, in paragraphs 1 and 3 thereof, provides that the PIU established or designated in each Member State is an authority competent for the prevention, detection, investigation and prosecution of terrorist offences and of serious crime, and that its staff members may be agents seconded from the competent authorities referred to in Article 7 of that directive, so that the PIU appears necessarily linked to those authorities. The PIU may also, pursuant to Article 6(2)(b) of the said directive, process PNR data and disclose the results to the said authorities. In the light of the foregoing, the PIU cannot be considered to be a third party in relation to those authorities and, accordingly, to have all the qualities of independence and impartiality required to carry out the prior review mentioned in the preceding paragraph and verify whether the conditions for disclosure of the full PNR data are met, as provided for in Article 12(3)(b) of that directive.

246. Furthermore, the fact that the latter provision requires, in its point (ii), where disclosure of the full PNR data has been approved by ‘another [competent] national authority’, that the data protection officer of the PIU ‘[is] inform[ed] and [carries out] an ex post review’, whereas this is not the case for approval by the judicial authority, is not such as to call that assessment into question. In accordance with well-established case-law, a subsequent review, such as that carried out by the data protection officer, does not enable the objective of a prior review, consisting in preventing the authorisation of access to the data in question that exceeds what is strictly necessary, to be met (see, to that effect, judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 110 and the case-law cited).

247. In the light of all of those considerations, the answer to Question 7 is that Article 12(3)(b) of the PNR Directive must be interpreted as precluding national legislation pursuant to which the authority put in place as the PIU is also designated as a competent national authority with power to approve

the disclosure of PNR data upon expiry of the period of six months after the transfer of those data to the PIU.

E. Question 8

248. By its Question 8, the referring court asks, in essence, whether Article 12 of the PNR Directive, read in conjunction with Articles 7 and 8 as well as Article 52(1) of the Charter, must be interpreted as precluding national legislation which provides for a general retention period of five years for PNR data, without drawing any distinction based on whether or not the passengers concerned present a risk that relates to terrorist offences or serious crime.

249. It must be recalled that, under Article 12(1) and (4) of that directive, the PIU of the Member State on the territory of which the flight concerned is landing or departing retains the PNR data provided by the air carriers in a database for a period of five years after their transfer to that unit and deletes such data permanently upon expiry of that period of five years.

250. As recalled in recital 25 of the PNR Directive, ‘the period during which PNR data are to be retained should be as long as is necessary for and proportionate to the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime’.

251. Consequently, the retention of PNR data pursuant to Article 12(1) of the PNR Directive cannot be justified in the absence of an objective connection between that retention and the objectives pursued by that directive, namely the fight against terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air.

252. In that regard, as is apparent from recital 25 of the PNR Directive, a distinction must be drawn between, on the one hand, the initial retention period of six months, referred to in Article 12(2) of that directive, and, on the other hand, the later period referred to in Article 12(3) of the said directive.

253. The interpretation of Article 12(1) of the PNR Directive must take into account the provisions in paragraphs 2 and 3 of that article, which lay down a set of rules for the retention of and access to PNR data retained after expiry of the initial retention period of six months. As is apparent from recital 25 of that directive, those provisions reflect, on the one hand, the objective of ensuring ‘that the PNR data be retained for a sufficiently long period to carry out analysis and for use in investigations’, which may be carried out already during the initial retention period of six months. On the other hand, according to that recital 25, they seek to ‘avoid disproportionate use’ through masking out of those data and to ‘ensure the highest level of data protection’ by granting access to those data in a form which permits direct identification of the data subject ‘only under very strict and limited conditions

after that initial period', thus having regard to the fact that the longer the period for the retention of PNR data, the more serious the resulting interference.

254. The distinction between the initial retention period of six months referred to in Article 12(2) of the PNR Directive and the later period referred to in Article 12(3) of that directive applies also to the obligation to comply with the requirement referred to in paragraph 251 above.

255. Thus, in view of the aims pursued by the PNR Directive and of the needs of the investigation and prosecution of terrorist offences and serious crime, the Court finds that the retention, during the initial period of six months, of the PNR data of all air passengers subject to the system established by that directive, without any indication as to their involvement in terrorist offences or serious crime does not appear, as a matter of principle, to go beyond what is strictly necessary, in so far as it allows the necessary searches to be carried out for the purposes of identifying the persons who were not suspected of involvement in terrorist offences or serious crime.

256. By contrast, as to the later period, set out in Article 12(3) of the PNR Directive, the retention of the PNR data of all air passengers subject to the system established by that directive, in addition to the fact that, by reason of the significant quantity of data that may be retained continuously, it entails an inherent risk of disproportionate use and abuse (see, by analogy, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 119), runs counter to the requirement in recital 25 of the said directive that the period during which those data are to be retained should be as long as is necessary for and proportionate to the objectives pursued, since the EU legislature intended to establish the highest level of protection of PNR data allowing direct identification of the data subjects.

257. As regards air passengers for whom neither the advance assessment under Article 6(2)(a) of the PNR Directive nor any verification carried out during the period of six months referred to in Article 12(2) of that directive nor any other circumstance have revealed the existence of objective evidence capable of establishing a risk that relates to terrorist offences or serious crime having an objective link, even if only an indirect one, with those passengers' air travel, there would not appear to be, in such circumstances, any connection – even a merely indirect one – between the PNR data of those passengers and the objective pursued by the said directive which would justify the retention of those data (see, by analogy, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 204 and 205).

258. The continued storage of the PNR data of all air passengers after the initial period of six months is not therefore limited to what is strictly necessary (see, by analogy Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 206).

259. However, in so far as, in specific cases, objective evidence, such as the PNR data of passengers which gave rise to a verified positive match, is identified from which it may be inferred that certain passengers may present a risk that relates to terrorist offences or serious crime, it seems permissible to store their PNR data beyond that initial period (see, by analogy, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 207 and the case-law cited).

260. Identification of that objective evidence is capable of establishing a connection with the objectives pursued by processing under the PNR Directive, with the result that the retention of the PNR data of those passengers is justified during the maximum period permitted by the said directive, namely during five years.

261. In the present case, in so far as the legislation at issue in the main proceedings appears to prescribe a general retention period of five years for PNR data, applicable indiscriminately to all passengers, including those for whom neither the advance assessment under Article 6(2)(a) of the PNR Directive nor any verification carried out in the initial period of six months nor any other circumstance have revealed the existence of objective evidence capable of establishing a risk that relates to terrorist offences or serious crime, that legislation is liable to infringe Article 12(1) of that directive, read in the light of Articles 7 and 8 as well as Article 52(1) of the Charter, unless it may be interpreted in a manner that is consistent with those provisions, which is a matter for the referring court to ascertain.

262. In the light of the foregoing, the answer to the Question 8 is that Article 12(1) of the PNR Directive, read in conjunction with Articles 7 and 8 as well as Article 52(1) of the Charter, must be interpreted as precluding national legislation which provides for a general retention period of five years for PNR data, applicable indiscriminately to all air passengers, including those for whom neither the advance assessment under Article 6(2)(a) of that directive nor any verification carried out during the period of six months referred to in Article 12(2) of the said directive nor any other circumstance have revealed the existence of objective evidence capable of establishing a risk that relates to terrorist offences or serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air.

F. Question 9(a)

263. By its Question 9(a), the referring court raises the question, in essence, of the validity of the API Directive in the light of Article 3(2) TEU and Article 45 of the Charter, based on the premiss that the obligations introduced by that directive apply to intra-EU flights.

264. As noted by the Advocate General in point 277 of his Opinion and as observed by the Council, the Commission and several governments, that premiss is incorrect.

265. Article 3(1) of the API Directive provides that Member States are to take the necessary steps to establish an obligation for carriers to transmit at the request of the authorities responsible for carrying out checks on persons at external borders, by the end of check-in, information concerning the passengers they will carry to an authorised border crossing point through which these persons will enter the territory of a Member State. Those data are to be communicated, pursuant to Article 6(1) of the said directive, to the authorities responsible for carrying out checks at external borders through which the passenger will enter that territory and are to be processed in accordance with the latter provision.

266. It is clear from those provisions, read in the light of Article 2(a), (b) and (d) of the API Directive, where the concepts of ‘carrier’, ‘external borders’ and ‘border crossing point’, are defined, respectively, that that directive imposes the obligation, for air carriers, to transmit the data referred to in Article 3(2) thereof, to the authorities responsible for carrying out external border checks only in the case of flights transporting passengers to an authorised crossing point for crossing the Member States’ external borders with third countries and provides that only the data relating to those flights are to be processed.

267. By contrast, the said directive does not impose any obligation concerning the data of passengers travelling on flights that cross only internal borders between Member States.

268. It should be added that the PNR Directive, by including among PNR data, as is apparent from recital 9 and Article 8(2) thereof, the data referred to in Article 3(2) of the API Directive collected in accordance with that directive and retained by certain air carriers, and by granting Member States the power to apply the PNR Directive, pursuant to Article 2 thereof, to the intra-EU flights selected by them, altered neither the scope of the provisions of the API Directive nor the limitations stemming from that directive.

269. In the light of the foregoing, the answer to Question 9(a) is that the API Directive must be interpreted as not applying to intra-EU flights.

G. Question 9(b)

270. While, by its Question 9(b), the referring court refers to the API Directive, read in conjunction with Article 3(2) TEU and Article 45 of the Charter, it is apparent from the request for a preliminary ruling that that court has doubts as to whether the system for the transfer and processing of passenger data established by the Law of 25 December 2016 is compatible with the free movement of persons and the abolition of internal border control provided for by EU law, in that that system applies not only to transport by air, but also transport by rail, by road or even by sea, departing from or going to Belgium and carried out within the European Union, without crossing external borders with third countries.

271. As is apparent from paragraphs 265 to 269 above, the API Directive, which does not apply to intra-EU flights and does not impose any obligation to transfer and process the data of passengers travelling by air or by another mode of transport within the European Union, without crossing external borders with third countries, is irrelevant for the purposes of answering that question.

272. However, and whereas, according to Article 67(2) TFEU, the European Union is to ensure the absence of internal border controls for persons, Article 2 of the PNR Directive, on which the Belgian legislature relied to adopt the Law of 25 December 2016 at issue in the main proceedings, as is apparent from the request for a preliminary ruling, authorises Member States to apply that directive to intra-EU flights.

273. In those circumstances, in order to provide a useful answer to the referring court, it is appropriate to reformulate Question 9(b) as seeking to clarify, in essence, whether EU law, in particular Article 2 of the PNR Directive, read in the light of Article 3(2) TEU, Article 67(2) TFEU and Article 45 of the Charter, must be interpreted as precluding national legislation which provides for a system for the transfer, by carriers and tour operators, as well as for the processing, by the competent authorities, of the PNR data of flights and transport operations carried out by other means within the European Union and departing from, going to or transiting through the Member State which adopted the said legislation.

274. First of all, Article 45 of the Charter enshrines the free movement of persons, which is, moreover, one of the fundamental freedoms of the internal market (see, to that effect, judgment of 22 June 2021, *Ordre des barreaux francophones et germanophone and Others (Preventive measures for removal)*, C-718/19, EU:C:2021:505, paragraph 54).

275. That article guarantees, in paragraph 1 thereof, the right of every citizen of the European Union to move and reside freely within the territory of the Member States, a right which, according to the Explanations relating to the Charter of Fundamental Rights (OJ 2007 C 303, p. 17), corresponds to that

guaranteed in the first subparagraph of Article 20(2) TFEU, under (a), and is to be exercised, under the second subparagraph of Article 20(2) TFEU and Article 52(2) of the Charter, in accordance with the conditions and the limits defined by the Treaties and by the measures adopted thereunder.

276. Next, Article 3(2) TEU provides that the European Union is to offer its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect, *inter alia*, to external border controls and the prevention and combating of crime. Similarly, according to Article 67(2) TFEU, the European Union is to ensure the absence of internal border controls for persons and to frame a common policy on, *inter alia*, external border control.

277. In accordance with the Court's established case-law, national legislation which places certain nationals at a disadvantage simply because they have exercised their freedom to move and to reside in another Member State is a restriction of the freedoms conferred by Article 45(1) of the Charter to every Union citizen (see, to that effect, concerning Article 21(1) TFEU, judgments of 8 June 2017, Freitag, C-541/15, EU:C:2017:432, paragraph 35 and the case-law cited, and of 19 November 2020, ZW, C-454/19, EU:C:2020:947, paragraph 30).

278. National legislation such as that at issue in the main proceedings, which applies the system provided for by the PNR Directive not only to extra-EU flights but also, pursuant to Article 2(1) of that directive, to intra-EU flights as well as, beyond what is envisaged under that provision, to transport by other means within the European Union, results in the systematic and continuous transfer and processing of the PNR data of any passenger travelling by those means within the European Union while exercising his or her freedom of movement.

279. As noted in paragraphs 98 to 111 above, the transfer and processing of data of passengers of extra-EU and intra-EU flights stemming from the system established by the PNR Directive entail undeniably serious interferences with the fundamental rights of the data subjects enshrined in Articles 7 and 8 of the Charter. The seriousness of those interferences is even greater where the application of that system covers other means of transport within the European Union. Such interferences are, for the same reasons as those set out in those paragraphs, also such as to place at a disadvantage and, therefore, deter from exercising their freedom of movement, within the meaning of Article 45 of the Charter, the nationals of the Member States which adopted such a legislation as well as, generally, Union citizens travelling by those means of transport within the European Union from or to those Member States, with the result that that legislation entails a restriction of that fundamental freedom.

280. In accordance with settled case-law, an obstacle to the freedom of movement of persons can be justified only where it is based on objective considerations and is proportionate to the legitimate objective of the national provisions. A measure is proportionate if, while appropriate for securing the attainment of the objective pursued, it does not go beyond what is necessary in order to attain that objective (see, to that effect, judgment of 5 June 2018, *Coman and Others*, C-673/16, EU:C:2018:385, paragraph 41 and the case-law cited).

281. It should be added that a national measure that is liable to obstruct the exercise of freedom of movement for persons may be justified only where such a measure is consistent with the fundamental rights guaranteed by the Charter, it being the task of the Court to ensure that those rights are respected (judgment of 14 December 2021, *Stolichna obshtina, rayon 'Pancharevo'*, C-490/20, EU:C:2021:1008, paragraph 58 and the case-law cited).

282. In particular, in accordance with the case-law recalled in paragraphs 115 and 116 above, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue. In that regard, the possibility of Member States justifying a limitation of the right guaranteed in Article 45(1) of the Charter must be assessed by measuring the seriousness of the interference which such a limitation entails and by verifying that the importance of the objective of general interest pursued by that limitation is proportionate to that seriousness.

283. As recalled in paragraph 122 above, the objective of combating terrorist offences and serious crime that the PNR Directive pursues is undoubtedly an objective of general interest of the European Union.

284. As to the question whether national legislation adopted for the purposes of transposing the PNR Directive that extends the system provided for by that directive to intra-EU flights and other modes of transport within the European Union is appropriate for securing the attainment of the objective pursued, it is apparent from the information in the file before the Court that use of PNR data allows identification of persons who were unsuspected of involvement in terrorist offences or serious crime and who should be subject to further examination, so that such legislation appears to be appropriate for the purpose of attaining the intended objective of combating terrorist offences and serious crime.

285. As to whether such legislation is necessary, the exercise by the Member States of the power provided for in Article 2(1) of the PNR Directive, read in the light of Articles 7 and 8 of the Charter, must be limited to what is strictly necessary for securing the attainment of that objective in the light of the requirements mentioned in paragraphs 163 to 174 above.

286. Those requirements apply, a fortiori, where the system provided for by the PNR Directive is applied to other means of transport within the European Union.

287. Moreover, as follows from the information in the request for a preliminary ruling, the national legislation at issue in the main proceedings transposes, in a single act, the PNR Directive, the API Directive and, in part, Directive 2010/65. To that end, it provides for the application of the system laid down in the PNR Directive to all intra-EU flights and transport by train, by road or even by sea carried out within the European Union departing from, going to or transiting through Belgium, and applies also to tour operators, while also pursuing objectives other than the fight against terrorist offences and serious crime. Following the said information, it appears that all the data collected in the context of the system established by that national legislation are retained by the PIU in a single database encompassing the PNR data, including the data covered by Article 3(2) of the API Directive, for all the passengers of the transport operations covered by that legislation.

288. In that regard, in so far as the referring court referred to the objective of improving border controls and combating illegal immigration in its Question 9(b), which is the objective of the API Directive, it should be borne in mind that, as follows from paragraphs 233, 234 and 237 above, the list of objectives pursued by the processing of PNR data under the PNR Directive is an exhaustive list with the result that national legislation authorising the processing of PNR data collected in accordance with that directive, for purposes other than those provided for therein, namely for the purposes of improving border controls and combating illegal immigration, is contrary to Article 6 of the said directive, read in the light of the Charter.

289. In addition, as is apparent from paragraph 235 above, Member States cannot create a single database containing both the PNR data collected under the PNR Directive and relating to extra-EU and intra-EU flights and the data of passengers of other means of transport as well as the data covered by Article 3(2) of the API Directive, in particular where that database can be consulted not only for the purposes referred to in Article 1(2) of the PNR Directive but for other purposes also.

290. Lastly and in any event, as noted by the Advocate General in point 281 of his Opinion, Articles 28 to 31 of the Law of 25 December 2016 can only be compatible with EU law, and with Article 67(2) TFEU in particular, if they are interpreted and applied as relating only to the transfer and processing of the API data of passengers crossing Belgium's external borders with third countries. A measure whereby a Member State would extend the provisions of the API Directive, for the purposes of improving border controls and combating illegal immigration, to intra-EU and, a fortiori, other modes of transport carrying passengers within the European Union departing from, going to or transiting

through that Member State, in particular the obligation to provide the data covered by Article 3(1) of that directive, would amount to allowing the competent authorities, when internal borders of the said Member State are crossed, to ensure systematically that those passengers can be authorised to enter its territory or to leave it and would thus have an effect equivalent to the checks carried out at external borders with third countries.

291. In view of all of those considerations, the answer to Question 9(b) is that EU law, in particular Article 2 of the PNR Directive, read in the light of Article 3(2) TEU, Article 67(2) TFEU and Article 45 of the Charter, must be interpreted as precluding:

– national legislation which, in the absence of a genuine and present or foreseeable terrorist threat with which the Member State concerned is confronted, establishes a system for the transfer, by air carriers and tour operators, as well as for the processing, by the competent authorities, of the PNR data of all intra-EU flights and transport operations carried out by other means within the European Union and departing from, going to or transiting through that Member State, for the purposes of combating terrorist offences and serious crime. In such a situation, the application of the system established by the PNR Directive must be limited to the transfer and processing of the PNR data of flights and/or transport operations relating, *inter alia*, to certain routes or travel patterns or to certain airports, stations or seaports for which there are indications that are such as to justify that application. It is for the Member State concerned to select the intra-EU flights and/or the transport operations carried out by other means within the European Union for which there are such indications and to review regularly that application in accordance with changes in the circumstances that justified their selection, for the purposes of ensuring that the application of that system to those flights and/or those transport operations continues to be limited to what is strictly necessary, and

– national legislation providing for such a system for the transfer and processing of those data for the purposes of improving external border controls and combating illegal immigration.

H. Question 10

292. By its Question 10, the referring court asks, in essence, whether EU law must be interpreted as meaning that a national court may limit the temporal effects of a declaration of illegality which it is bound to make under national law in respect of national legislation requiring carriers by air, by rail and by land as well as tour operators to transfer PNR data, and providing for the processing and retention of those data, in breach of the provisions of the PNR Directive, read in the light of Article 3(2) TEU, Article 67(2) TFEU and Articles 7, 8 and 45 as well as Article 52(1) of the Charter.

293. The principle of the primacy of EU law establishes the pre-eminence of EU law over the law of the Member States. That principle therefore requires all Member State bodies to give full effect to the various provisions of EU law, and the law of the Member States may not undermine the effect accorded to those various provisions in the territory of those States. In the light of that principle, where it is unable to interpret national legislation in compliance with the requirements of EU law, the national court which is called upon within the exercise of its jurisdiction to apply provisions of EU law is under a duty to give full effect to those provisions, if necessary refusing of its own motion to apply any conflicting provision of national legislation, even if adopted subsequently, and it is not necessary for that court to request or await the prior setting aside of such provision by legislative or other constitutional means (judgments of 15 July 1964, *Costa*, 6/64, EU:C:1964:66, pp. 593 and 594; of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 214 and 215; and of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 118).

294. Only the Court may, in exceptional cases, on the basis of overriding considerations of legal certainty, allow the temporary suspension of the ousting effect of a rule of EU law with respect to national law that is contrary thereto. Such a restriction on the temporal effects of the interpretation of that law, made by the Court, may be granted only in the actual judgment ruling upon the interpretation requested. The primacy and uniform application of EU law would be undermined if national courts had the power to give provisions of national law primacy in relation to EU law contravened by those provisions, even temporarily (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 119 and the case-law cited).

295. Unlike a breach of a procedural obligation such as the prior assessment of the impact of a project on the environment, at issue in the case that gave rise to the judgment of 29 July 2019, *Inter-Environnement Wallonie and Bond Beter Leefmilieu Vlaanderen* (C-411/17, EU:C:2019:622, paragraphs 175, 176, 179 and 181), in which the Court accepted the temporary suspension of that ousting effect, a failure to comply with the provisions of the PNR Directive, read in the light of Articles 7, 8 and 45 as well as Article 52(1) of the Charter, cannot be remedied by a procedure comparable to the procedure allowed in that case. Maintaining the effects of national legislation such as the Law of 25 December 2016 would mean that that legislation would continue to impose on air carriers and other carriers as well as tour operators obligations which are contrary to EU law and which seriously interfere with the fundamental rights of the persons whose data have been transferred, retained and processed as well as restrictions on the freedom movement of those persons going beyond what is

necessary (see, by analogy, judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 122 and the case-law cited).

296. Therefore, the referring court cannot limit the temporal effects of a declaration of illegality which it is bound to make under national law in respect of the national legislation at issue in the main proceedings (see, by analogy, judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 123 and the case-law cited).

297. Lastly, in so far as the referring court raises the question of the impact of a finding of incompatibility, if any, of the Law of 25 December 2016 with the provisions of the PNR Directive, read in the light of the Charter, on the admissibility and use of the evidence and information secured from the data transferred by the carriers and tour operators concerned in the context of criminal proceedings, it suffices to refer to the Court's case-law on that subject, in particular to the principles recalled in paragraphs 41 to 44 of the judgment of 2 March 2021, Prokuratuur (Conditions of access to data relating to electronic communications) (C-746/18, EU:C:2021:152), from which it follows that that admissibility is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, *inter alia*, with the principles of equivalence and effectiveness (see, by analogy, judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 127).

298. In the light of the foregoing, the answer to the Question 10 is that EU law must be interpreted as precluding a national court from limiting the temporal effects of a declaration of illegality which it is bound to make under national law in respect of national legislation requiring carriers by air, by rail and by road as well as tour operators to transfer PNR data, and providing for the processing and retention of those data, in breach of the provisions of the PNR Directive, read in the light of Article 3(2) TEU, Article 67(2) TFEU and Articles 7, 8 and 45 as well as Article 52(1) of the Charter. The admissibility of the evidence thus obtained is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, *inter alia*, with the principles of equivalence and effectiveness.

IV. Costs

299. Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Grand Chamber) hereby rules:

1. Article 2(2)(d) and Article 23 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), must be interpreted as meaning that that regulation applies to the processing of personal data envisaged by national legislation intended to transpose, into domestic law, the provisions of Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, those of Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC and also those of Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, in respect of, on the one hand, data processing operations carried out by private operators and, on the other hand, data processing operations carried out by public authorities covered, solely or in addition, by Directive 2004/82 or Directive 2010/65. By contrast, the said regulation does not apply to the data processing operations envisaged by such legislation which are covered only by Directive 2016/681 and are carried out by the passenger information unit (PIU) or by the authorities competent for the purposes referred to in Article 1(2) of that directive.

2. Given that an interpretation of Directive 2016/681 in the light of Articles 7, 8 and 21 as well as Article 52(1) of the Charter of Fundamental Rights of the European Union ensures that that directive is consistent with those articles of the Charter of Fundamental Rights, the examination of Questions 2 to 4 and Question 6 referred for a preliminary ruling has revealed nothing capable of affecting the validity of the said directive.

3. Article 6 of Directive 2016/681, read in the light of Articles 7 and 8 as well as Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation which authorises passenger name records (PNR data) collected in accordance with that directive to be processed for purposes other than those expressly referred to in Article 1(2) of the said directive.

4. Article 12(3)(b) of Directive 2016/681 must be interpreted as precluding national legislation pursuant to which the authority put in place as the passenger information unit (PIU) is also designated as a competent national authority with power to approve the disclosure of PNR data upon expiry of the period of six months after the transfer of those data to the PIU.

5. Article 12(1) of Directive 2016/681, read in conjunction with Articles 7 and 8 as well as Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation which

provides for a general retention period of five years for PNR data, applicable indiscriminately to all air passengers, including those for whom neither the advance assessment under Article 6(2)(a) of that directive nor any verification carried out during the period of six months referred to in Article 12(2) of the said directive nor any other circumstance have revealed the existence of objective evidence capable of establishing a risk that relates to terrorist offences or serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air.

6. Directive 2004/82 must be interpreted as not applying to flights, whether scheduled or non-scheduled, carried out by an air carrier flying from the territory of a Member State and that are planned to land on the territory of one or more of the other Member States, without any stop-overs in the territory of a third country (intra-EU flights).

7. EU law, in particular Article 2 of Directive 2016/681, read in the light of Article 3(2) TEU, Article 67(2) TFEU and Article 45 of the Charter of Fundamental Rights, must be interpreted as precluding:

– national legislation which, in the absence of a genuine and present or foreseeable terrorist threat with which the Member State concerned is confronted, establishes a system for the transfer, by air carriers and tour operators, as well as for the processing, by the competent authorities, of the PNR data of all intra-EU flights and transport operations carried out by other means within the European Union, departing from, going to or transiting through that Member State, for the purposes of combating terrorist offences and serious crime. In such a situation, the application of the system established by Directive 2016/681 must be limited to the transfer and processing of the PNR data of flights and/or transport operations relating, inter alia, to certain routes or travel patterns or to certain airports, stations or seaports for which there are indications that are such as to justify that application. It is for the Member State concerned to select the intra-EU flights and/or the transport operations carried out by other means within the European Union for which there are such indications and to review regularly that application in accordance with changes in the circumstances that justified their selection, for the purposes of ensuring that the application of that system to those flights and/or those transport operations continues to be limited to what is strictly necessary, and

– national legislation providing for such a system for the transfer and processing of those data for the purposes of improving external border controls and combating illegal immigration.

8. EU law must be interpreted as precluding a national court from limiting the temporal effects of a declaration of illegality which it is bound to make under national law in respect of national legislation requiring carriers by air, by rail and by road as well as tour operators to transfer PNR data, and providing for the processing and retention of those data, in breach of the provisions of Directive

2016/681, read in the light of Article 3(2) TEU, Article 67(2) TFEU, Articles 7, 8 and 45 as well as Article 52(1) of the Charter of Fundamental Rights. The admissibility of the evidence thus obtained is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, *inter alia*, with the principles of equivalence and effectiveness.

[Signatures]

* Language of the case: French.

Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems

The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield

However, it considers that Commission Decision 2010/87 on standard contractual clauses for the transfer of personal data to processors established in third countries is valid.

The General Data Protection Regulation¹ ('the GDPR') provides that the transfer of such data to a third country may, in principle, take place only if the third country in question ensures an adequate level of data protection. According to the GDPR, the Commission may find that a third country ensures, by reason of its domestic law or its international commitments, an adequate level of protection.² In the absence of an adequacy decision, such transfer may take place only if the personal data exporter established in the EU has provided appropriate safeguards, which may arise, in particular, from standard data protection clauses adopted by the Commission, and if data subjects have enforceable rights and effective legal remedies.³ Furthermore, the GDPR details the conditions under which such a transfer may take place in the absence of an adequacy decision or appropriate safeguards.⁴

Maximillian Schrems, an Austrian national residing in Austria, has been a Facebook user since 2008. As in the case of other users residing in the European Union, some or all of Mr Schrems's personal data is transferred by Facebook Ireland to servers belonging to Facebook Inc. that are located in the United States, where it undergoes processing. Mr Schrems lodged a complaint with the Irish supervisory authority seeking, in essence, to prohibit those transfers. He claimed that the law and practices in the United States do not offer sufficient protection against access by the public authorities to the data transferred to that country. That complaint was rejected on the ground, inter alia, that, in Decision 2000/5205 ('the Safe Harbour Decision'), the Commission had found that the United States ensured an adequate level of protection. In a judgment delivered on 6 October 2015, the Court of Justice, before which the High Court (Ireland) had referred questions for a preliminary ruling, declared that decision invalid ('the Schrems I judgment').⁶

Following the Schrems I judgment and the subsequent annulment by the referring court of the decision rejecting Mr Schrems's complaint, the Irish supervisory authority asked Mr Schrems to

reformulate his complaint in the light of the declaration by the Court that Decision 2000/520 was invalid. In his reformulated complaint, Mr Schrems claims that the United States does not offer sufficient protection of data transferred to that country. He seeks the suspension or prohibition of future transfers of his personal data from the EU to the United States, which Facebook Ireland now carries out pursuant to the standard data protection clauses set out in the Annex to Decision 2010/87.⁷ Taking the view that the outcome of Mr Schrems's complaint depends, in particular, on the validity of Decision 2010/87, the Irish supervisory authority brought proceedings before the High Court in order for it to refer questions to the Court of Justice for a preliminary ruling. After the initiation of those proceedings, the Commission adopted Decision 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield⁸ ('the Privacy Shield Decision').

By its request for a preliminary ruling, the referring court asks the Court of Justice whether the GDPR applies to transfers of personal data pursuant to the standard data protection clauses in Decision 2010/87, what level of protection is required by the GDPR in connection with such a transfer, and what obligations are incumbent on supervisory authorities in those circumstances. The High Court also raises the question of the validity both of Decision 2010/87 and of Decision 2016/1250.

In today's judgment, the Court of Justice finds that examination of Decision 2010/87 in the light of the Charter of Fundamental Rights has disclosed nothing to affect the validity of that decision. However, the Court declares Decision 2016/1250 invalid.

The Court considers, first of all, that EU law, and in particular the GDPR, applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, even if, at the time of that transfer or thereafter, that data may be processed by the authorities of the third country in question for the purposes of public security, defence and State security. The Court adds that this type of data processing by the authorities of a third country cannot preclude such a transfer from the scope of the GDPR.

Regarding the level of protection required in respect of such a transfer, the Court holds that the requirements laid down for such purposes by the GDPR concerning appropriate safeguards, enforceable rights and effective legal remedies must be interpreted as meaning that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses must be afforded a level of protection essentially equivalent to that guaranteed within the EU by the GDPR, read in the light of the Charter. In those circumstances, the Court specifies that the assessment of that level of protection must take into consideration both the contractual clauses agreed between

the data exporter established in the EU and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the data transferred, the relevant aspects of the legal system of that third country.

Regarding the supervisory authorities' obligations in connection with such a transfer, the Court holds that, unless there is a valid Commission adequacy decision, those competent supervisory authorities are required to suspend or prohibit a transfer of personal data to a third country where they take the view, in the light of all the circumstances of that transfer, that the standard data protection clauses are not or cannot be complied with in that country and that the protection of the data transferred that is required by EU law cannot be ensured by other means, where the data exporter established in the EU has not itself suspended or put an end to such a transfer.

Next, the Court examines the validity of Decision 2010/87. The Court considers that the validity of that decision is not called into question by the mere fact that the standard data protection clauses in that decision do not, given that they are contractual in nature, bind the authorities of the third country to which data may be transferred. However, that validity, the Court adds, depends on whether the decision includes effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law and that transfers of personal data pursuant to such clauses are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them. The Court finds that Decision 2010/87 establishes such mechanisms. In that regard, the Court points out, in particular, that that decision imposes an obligation on a data exporter and the recipient of the data to verify, prior to any transfer, whether that level of protection is respected in the third country concerned and that the decision requires the recipient to inform the data exporter of any inability to comply with the standard data protection clauses, the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract with the former.

Lastly, the Court examines the validity of Decision 2016/1250 in the light of the requirements arising from the GDPR, read in the light of the provisions of the Charter guaranteeing respect for private and family life, personal data protection and the right to effective judicial protection. In that regard, the Court notes that that decision enshrines the position, as did Decision 2000/520, that the requirements of US national security, public interest and law enforcement have primacy, thus condoning interference with the fundamental rights of persons whose data are transferred to that third country. In the view of the Court, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to that third country, which the Commission assessed in Decision 2016/1250, are

not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary. On the basis of the findings made in that decision, the Court pointed out that, in respect of certain surveillance programmes, those provisions do not indicate any limitations on the power they confer to implement those programmes, or the existence of guarantees for potentially targeted non-US persons. The Court adds that, although those provisions lay down requirements with which the US authorities must comply when implementing the surveillance programmes in question, the provisions do not grant data subjects actionable rights before the courts against the US authorities.

As regards the requirement of judicial protection, the Court holds that, contrary to the view taken by the Commission in Decision 2016/1250, the Ombudsperson mechanism referred to in that decision does not provide data subjects with any cause of action before a body which offers guarantees substantially equivalent to those required by EU law, such as to ensure both the independence of the Ombudsperson provided for by that mechanism and the existence of rules empowering the Ombudsperson to adopt decisions that are binding on the US intelligence services. On all those grounds, the Court declares Decision 2016/1250 invalid.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ 2016 L 119, p. 1).

[2] Article 45 of the GDPR.

[3] Article 46(1) and (2)(c) of the GDPR.

[4] Article 49 of the GDPR.

[5] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 p.7).

[6] Case:C-362/14 Schrems see also Press Release No. 117/15.

[7] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344, p. 100).

[8] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (OJ 2016 L 207, p. 1).

JUDGMENT OF THE COURT (Grand Chamber)

16 July 2020 (*)

(Reference for a preliminary ruling — Protection of individuals with regard to the processing of personal data — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Regulation (EU) 2016/679 — Article 2(2) — Scope — Transfers of personal data to third countries for commercial purposes — Article 45 — Commission adequacy decision — Article 46 — Transfers subject to appropriate safeguards — Article 58 — Powers of the supervisory authorities — Processing of the data transferred by the public authorities of a third country for national security purposes — Assessment of the adequacy of the level of protection in the third country — Decision 2010/87/EU — Protective standard clauses on the transfer of personal data to third countries — Suitable safeguards provided by the data controller — Validity — Implementing Decision (EU) 2016/1250 — Adequacy of the protection provided by the EU-US Privacy Shield — Validity — Complaint by a natural person whose data was transferred from the European Union to the United States)

In Case C-311/18,

REQUEST for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 4 May 2018, received at the Court on 9 May 2018, in the proceedings

Data Protection Commissioner

v

Facebook Ireland Ltd,

Maximillian Schrems,

intervening parties:

The United States of America,

Electronic Privacy Information Centre,

BSA Business Software Alliance Inc.,

Digitaleurope,

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, R. Silva de Lapuerta, Vice-President, A. Arabadjiev, A. Prechal, M. Vilaras, M. Safjan, S. Rodin, P.G. Xuereb, L.S. Rossi and I. Jarukaitis, Presidents of Chambers, M. Ilešič, T. von Danwitz (Rapporteur), and D. Šváby, Judges,

Advocate General: H. Saugmandsgaard Øe,

Registrar: C. Strömholm, Administrator,

having regard to the written procedure and further to the hearing on 9 July 2019,

after considering the observations submitted on behalf of:

- the Data Protection Commissioner, by D. Young, Solicitor, B. Murray and M. Collins, Senior Counsel, and C. Donnelly, Barrister-at-Law,
- Facebook Ireland Ltd, by P. Gallagher and N. Hyland, Senior Counsel, A. Mulligan and F. Kieran, Barristers-at-Law, and P. Nolan, C. Monaghan, C. O'Neill and R. Woulfe, Solicitors,
- Mr Schrems, by H. Hofmann, Rechtsanwalt, E. McCullough, J. Doherty and S. O'Sullivan, Senior Counsel, and G. Rudden, Solicitor,
- the United States of America, by E. Barrington, Senior Counsel, S. Kingston, Barrister-at-Law, S. Barton and B. Walsh, Solicitors,
- the Electronic Privacy Information Centre, by S. Lucey, Solicitor, G. Gilmore and A. Butler, Barristers-at-Law, and C. O'Dwyer, Senior Counsel,
- BSA Business Software Alliance Inc., by B. Van Vooren and K. Van Quathem, advocaten,
- Digitaleurope, by N. Cahill, Barrister, J. Cahir, Solicitor, and M. Cush, Senior Counsel,
- Ireland, by A. Joyce and M. Browne, acting as Agents, and D. Fennelly, Barrister-at-Law,
- the Belgian Government, by J.-C. Halleux and P. Cottin, acting as Agents,
- the Czech Government, by M. Smolek, J. Vláčil, O. Serdula and A. Kasalická, acting as Agents,
- the German Government, by J. Möller, D. Klebs and T. Henze, acting as Agents,
- the French Government, by A.-L. Desjonquères, acting as Agent,
- the Netherlands Government, by C.S. Schillemans, M.K. Bulterman and M. Noort, acting as Agents,
- the Austrian Government, by J. Schmoll and G. Kunnert, acting as Agents,
- the Polish Government, by B. Majczyna, acting as Agent,

- the Portuguese Government, by L. Inez Fernandes, A. Pimenta and C. Vieira Guerra, acting as Agents,

- the United Kingdom Government, by S. Brandon, acting as Agent, and J. Holmes QC, and C. Knight, Barrister,

- the European Parliament, by M.J. Martínez Iglesias and A. Caiola, acting as Agents,

- the European Commission, by D. Nardi, H. Krämer and H. Kranenborg, acting as Agents,

- the European Data Protection Board (EDPB), by A. Jelinek and K. Behn, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 19 December 2019,

gives the following

Judgment

1. This reference for a preliminary ruling, in essence, concerns:

- the interpretation of the first indent of Article 3(2), Articles 25 and 26 and Article 28(3) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), read in the light of Article 4(2) TEU and of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union ('the Charter');
- the interpretation and validity of Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46 (OJ 2010 L 39, p. 5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344, p. 100) ('the SCC Decision'); and
- the interpretation and validity of Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46 on the adequacy of the protection provided by the EU-US Privacy Shield (OJ 2016 L 207, p. 1; 'the Privacy Shield Decision').

2. The request has been made in proceedings between the Data Protection Commissioner (Ireland) ('the Commissioner'), on the one hand, and Facebook Ireland Ltd and Maximillian Schrems, on the other, concerning a complaint brought by Mr Schrems concerning the transfer of his personal data by Facebook Ireland to Facebook Inc. in the United States.

Legal context

Directive 95/46

3. Article 3 of Directive 95/46, under the heading 'Scope', stated, in paragraph 2:

'This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

- ...'

4. Article 25 of that directive provided:

'1. The Member States shall provide that the transfer to a third country of personal data ... may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; ...

...

6. The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's Decision.'

5. Article 26(2) and (4) of the directive provided:

'2. Without prejudice to paragraph 1, a Member State may authorise a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

...

4. Where the Commission decides, in accordance with the procedure referred to in Article 31(2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.'

6. Pursuant to Article 28(3) of that directive:

'Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been infringed or to bring those infringements to the attention of the judicial authorities.

...'

The GDPR

7. Directive 95/46 was repealed and replaced by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation) (OJ 2016 L 119, p. 1; 'the GDPR').

8. Recitals 6, 10, 101, 103, 104, 107 to 109, 114, 116 and 141 of the GDPR state:

'(6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within

the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

...

(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ("sensitive data"). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

...

(101) Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in these flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

...

(103) The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.

(104) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

...

(107) The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(108) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. ...

(109) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.

...

(114) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.

...

(116) When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by

insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. ...

...

(141) Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. ...'

9. Article 2(1) and (2) of the GDPR provides:

'1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'

10. Article 4 of the GDPR provides:

'For the purposes of this Regulation:

...

(2) "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

...

(7) “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) “processor”, means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) “recipient” means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

...'

11. Article 23 of the GDPR states:

'1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

...

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

- (a) the purposes of the processing or categories of processing;
- (b) the categories of personal data;
- (c) the scope of the restrictions introduced;
- (d) the safeguards to prevent abuse or unlawful access or transfer;
- (e) the specification of the controller or categories of controllers;
- (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
- (g) the risks to the rights and freedoms of data subjects; and
- (h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.'

12. Chapter V of the GDPR, under the heading 'Transfers of personal data to third countries or international organisations', contains Articles 44 to 50 of that regulation. According to Article 44 thereof, under the heading 'General principle for transfers':

'Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.'

13. Article 45 of the GDPR, under the heading 'Transfers on the basis of an adequacy decision', provides, in paragraphs 1 to 3:

'1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).'

14. Article 46 of the GDPR, under the heading 'Transfers subject to appropriate safeguards', provides, in paragraphs 1 to 3:

'1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

- (a) a legally binding and enforceable instrument between public authorities or bodies;
- (b) binding corporate rules in accordance with Article 47;
- (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
- (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
- (e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- (f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

- (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
- (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.'

15. Article 49 of the GDPR, under the heading 'Derogations for specific situations', states:

'1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

- (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- (d) the transfer is necessary for important reasons of public interest;
- (e) the transfer is necessary for the establishment, exercise or defence of legal claims;
- (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.'

16. Under Article 51(1) of the GDPR:

'Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ("supervisory authority").'

17. In accordance with Article 55(1) of the GDPR, 'each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State'.

18. Article 57(1) of that regulation states as follows:

'Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

...

(f) handle complaints lodged by a data subject ... and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

...'

19. According to Article 58(2) and (4) of the GDPR:

'2. Each supervisory authority shall have all of the following corrective powers:

...

(f) to impose a temporary or definitive limitation including a ban on processing;

...

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

...

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.'

20. Article 64(2) of the GDPR states:

'Any supervisory authority, the Chair of the [European Data Protection Board (EDPB)] or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.'

21. Under Article 65(1) of the GDPR:

'In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

...

(c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.'

22. Article 77 of the GDPR, under the heading 'Right to lodge a complaint with a supervisory authority', states:

'1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.'

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.'

23. Article 78 of the GDPR, under the heading 'Right to an effective judicial remedy against a supervisory authority', provides, in paragraphs 1 and 2:

'1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to [an] effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.'

24. Article 94 of the GDPR provides:

'1. Directive [95/46] is repealed with effect from 25 May 2018.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive [95/46] shall be construed as references to the European Data Protection Board established by this Regulation.'

25. Pursuant to Article 99 of the GDPR:

'1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

2. It shall apply from 25 May 2018.'

The SCC Decision

26. Recital 11 of the SCC Decision reads as follows:

'Supervisory authorities of the Member States play a key role in this contractual mechanism in ensuring that personal data are adequately protected after the transfer. In exceptional cases where data exporters refuse or are unable to instruct the data importer properly, with an imminent risk of grave harm to the data subjects, the standard contractual clauses should allow the supervisory authorities to audit data importers and sub-processors and, where appropriate, take decisions which are binding on data importers and sub-processors. The supervisory authorities should have the power

to prohibit or suspend a data transfer or a set of transfers based on the standard contractual clauses in those exceptional cases where it is established that a transfer on contractual basis is likely to have a substantial adverse effect on the warranties and obligations providing adequate protection for the data subject.'

27. Article 1 of the SCC Decision states:

'The standard contractual clauses set out in the Annex are considered as offering adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights as required by Article 26(2) of Directive [95/46].'

28. In accordance with the second paragraph of Article 2 of the SCC Decision, that decision 'shall apply to the transfer of personal data by controllers established in the European Union to recipients established outside the territory of the European Union who act only as data processors'.

29. Article 3 of the SCC Decision provides:

'For the purposes of this Decision, the following definitions shall apply:

...

(c) "data exporter" means the controller who transfers the personal data;

(d) "data importer" means the processor established in a third country who agrees to receive from the data exporter personal data intended for processing on the data exporter's behalf after the transfer in accordance with his instructions and the terms of this Decision and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive [95/46];

...

(f) "applicable data protection law" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

...'

30. According to its original wording, prior to the entry into force of Implementing Decision 2016/2297, Article 4 of Decision 2010/87 provided:

‘1. ‘Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to Chapters II, III, V and VI of Directive [95/46], the competent authorities in the Member States may exercise their existing powers to prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing of their personal data in cases where:

(a) it is established that the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive [95/46] where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses;

(b) a competent authority has established that the data importer or a sub-processor has not respected the standard contractual clauses in the Annex; or

(c) there is a substantial likelihood that the standard contractual clauses in the Annex are not being or will not be complied with and the continuing transfer would create an imminent risk of grave harm to the data subjects.

2. The prohibition or suspension pursuant to paragraph 1 shall be lifted as soon as the reasons for the suspension or prohibition no longer exist.

3. When Member States adopt measures pursuant to paragraphs 1 and 2, they shall, without delay, inform the Commission which will forward the information to the other Member States.’

31. Recital 5 of Implementing Decision 2016/2297, adopted after the judgment of 6 October 2015, Schrems (C-362/14, EU:C:2015:650) was handed down, reads as follows:

‘Mutatis mutandis, a Commission decision adopted pursuant to Article 26(4) of Directive [95/46] is binding on all organs of the Member States to which it is addressed, including their independent supervisory authorities, in so far as it has the effect of recognising that transfers taking place on the basis of standard contractual clauses set out therein offer sufficient safeguards as required by Article 26(2) of that Directive. This does not prevent a national supervisory authority from exercising its powers to oversee data flows, including the power to suspend or ban a transfer of personal data when it determines that the transfer is carried out in violation of EU or national data protection law, such as, for instance, when the data importer does not respect the standard contractual clauses.’

32. According to its current wording, resulting from Implementing Decision 2016/2297, Article 4 of the SCC Decision states:

‘Whenever the competent authorities in Member States exercise their powers pursuant to Article 28(3) of Directive [95/46] leading to the suspension or definitive ban of data flows to third countries in order to protect individuals with regard to the processing of their personal data, the Member State concerned shall, without delay, inform the Commission which will forward the information to the other Member States.’

33. The annex to the SCC Decision, under the heading ‘Standard Contractual Clauses (Processors)’, is comprised of 12 standard clauses. Clause 3 thereof, itself under the heading ‘Third-party beneficiary clause’, provides:

‘1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

...’

34. According to Clause 4 in that annex, under the heading ‘Obligations of the data exporter’:

‘The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter’s behalf and in accordance with the applicable data protection law and the Clauses;

...

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive [95/46];

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

...'

35. Clause 5 in that annex, under the heading 'Obligations of the data importer ...', provides:

'The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

...

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

...'

36. The footnote to the heading of Clause 5 states:

'Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive [95/46], that is, if they constitute a necessary measure to safeguard national security,

defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. ...'

37. Clause 6 in the annex to the SCC Decision, under the heading 'Liability', provides:

'1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter ...

...'

38. Clause 8 in that annex, under the heading 'Cooperation with supervisory authorities', stipulates, in paragraph 2 thereof:

'The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.'

39. Clause 9 in that annex, under the heading 'Governing law', specifies that the clauses are to be governed by the law of the Member State in which the data exporter is established.

40. According to Clause 11 in that annex, under the heading 'Sub-processing':

'1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses ...

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter

or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

...'

41. Clause 12 in the annex to the SCC Decision, under the heading 'Obligation after the termination of personal data-processing services', states, in paragraph 1 thereof:

'The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. ...'

The Privacy Shield Decision

42. In the judgment of 6 October 2015, Schrems (C-362/14, EU:C:2015:650), the Court declared Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7), in which the Commission had found that that third country ensured an adequate level of protection, invalid.

43. Following the delivery of that judgment, the Commission adopted the Privacy Shield Decision, after having, for the purposes of adopting that decision, assessed the US legislation, as stated in recital 65 of the decision:

'The Commission has assessed the limitations and safeguards available in U.S. law as regards access and use of personal data transferred under the EU-U.S. Privacy Shield by U.S. public authorities for national security, law enforcement and other public interest purposes. In addition, the U.S. government, through its Office of the Director of National Intelligence (ODNI) ..., has provided the Commission with detailed representations and commitments that are contained in Annex VI to this decision. By letter signed by the Secretary of State and attached as Annex III to this decision the U.S. government has also committed to create a new oversight mechanism for national security interference, the Privacy Shield Ombudsperson, who is independent from the Intelligence Community. Finally, a representation from the U.S. Department of Justice, contained in Annex VII to

this decision, describes the limitations and safeguards applicable to access and use of data by public authorities for law enforcement and other public interest purposes. In order to enhance transparency and to reflect the legal nature of these commitments, each of the documents listed and annexed to this decision will be published in the U.S. Federal Register.'

44. The Commission's assessment of those limitations and guarantees is summarised in recitals 67 to 135 of the Privacy Shield Decision, while the Commission's conclusions on the adequate level of protection in the context of the EU-US Privacy Shield are set out in recitals 136 to 141 thereof.

45. In particular, Recitals 68, 69, 76, 77, 109, 112 to 116, 120, 136 and 140 of the Privacy Shield Decision state:

'(68) Under the U.S. Constitution, ensuring national security falls within the President's authority as Commander in Chief, as Chief Executive and, as regards foreign intelligence, to conduct U.S. foreign affairs ... While Congress has the power to impose limitations, and has done so in various respects, within these boundaries the President may direct the activities of the U.S. Intelligence Community, in particular through Executive Orders or Presidential Directives. ... At present, the two central legal instruments in this regard are Executive Order 12333 ("E.O. 12333") ... and Presidential Policy Directive 28.

(69) Presidential Policy Directive 28 ("PPD-28"), issued on 17 January 2014, imposes a number of limitations for "signals intelligence" operations ... This presidential directive has binding force for U.S. intelligence authorities ... and remains effective upon change in the U.S. Administration ... PPD-28 is of particular importance for non-US persons, including EU data subjects. ...

...

(76) Although not phrased in ... legal terms, [the] principles [of PPD-28] capture the essence of the principles of necessity and proportionality. ...

(77) As a directive issued by the President as the Chief Executive, these requirements bind the entire Intelligence Community and have been further implemented through agency rules and procedures that transpose the general principles into specific directions for day-to-day operations. ...

...

(109) Conversely, under Section 702 [of the Foreign Intelligence Surveillance Act (FISA)], the [United States Foreign Intelligence Surveillance Court (FISC)] does not authorise individual surveillance measures; rather, it authorises surveillance programs (like PRISM, UPSTREAM) on the basis of annual

certifications prepared by the [US] Attorney General and the Director of National Intelligence [(DNI)]. ... As indicated, the certifications to be approved by the FISC contain no information about the individual persons to be targeted but rather identify categories of foreign intelligence information ... While the FISC does not assess — under a probable cause or any other standard — that individuals are properly targeted to acquire foreign intelligence information ..., its control extends to the condition that “a significant purpose of the acquisition is to obtain foreign intelligence information” ...

(112) First, the [FISA] provides a number of remedies, available also to non-U.S. persons, to challenge unlawful electronic surveillance ... This includes the possibility for individuals to bring a civil cause of action for money damages against the United States when information about them has been unlawfully and wilfully used or disclosed ...; to sue U.S. government officials in their personal capacity (“under colour of law”) for money damages ...; and to challenge the legality of surveillance (and seek to suppress the information) in the event the U.S. government intends to use or disclose any information obtained or derived from electronic surveillance against the individual in judicial or administrative proceedings in the United States ...

(113) Second, the U.S. government referred the Commission to a number of additional avenues that EU data subjects could use to seek legal recourse against government officials for unlawful government access to, or use of, personal data, including for purported national security purposes ...

(114) Finally, the U.S. government has pointed to the [Freedom of Information Act (FOIA)] as a means for non-U.S. persons to seek access to existing federal agency records, including where these contain the individual’s personal data ... Given its focus, the FOIA does not provide an avenue for individual recourse against interference with personal data as such, even though it could in principle enable individuals to get access to relevant information held by national intelligence agencies. ...

(115) While individuals, including EU data subjects, therefore have a number of avenues of redress when they have been the subject of unlawful (electronic) surveillance for national security purposes, it is equally clear that at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered. Moreover, even where judicial redress possibilities in principle do exist for non-U.S. persons, such as for surveillance under FISA, the available causes of action are limited ... and claims brought by individuals (including U.S. persons) will be declared inadmissible where they cannot show “standing” ..., which restricts access to ordinary courts ...

(116) In order to provide for an additional redress avenue accessible for all EU data subjects, the U.S. government has decided to create a new Ombudsperson Mechanism as set out in the letter from the U.S. Secretary of State to the Commission which is contained in Annex III to this decision. This mechanism builds on the designation, under PPD-28, of a Senior Coordinator (at the level of Under-Secretary) in the State Department as a contact point for foreign governments to raise concerns regarding U.S. signals intelligence activities, but goes significantly beyond this original concept.

...

(120) ... the U.S. government commits to ensure that, in carrying out its functions, the Privacy Shield Ombudsperson will be able to rely on the cooperation from other oversight and compliance review mechanisms existing in U.S. law. ... Where any non-compliance has been found by one of these oversight bodies, the Intelligence Community element (e.g. an intelligence agency) concerned will have to remedy the non-compliance as only this will allow the Ombudsperson to provide a “positive” response to the individual (i.e. that any non-compliance has been remedied) to which the U.S. government has committed. ...

...

(136) In the light of [those] findings, the Commission considers that the United States ensures an adequate level of protection for personal data transferred from the Union to self-certified organisations in the United States under the EU-U.S. Privacy Shield.

...

(140) Finally, on the basis of the available information about the U.S. legal order, including the representations and commitments from the U.S. government, the Commission considers that any interference by U.S. public authorities with the fundamental rights of the persons whose data are transferred from the Union to the United States under the Privacy Shield for national security, law enforcement or other public interest purposes, and the ensuing restrictions imposed on self-certified organisations with respect to their adherence to the Principles, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that there exists effective legal protection against such interference.’

46. Under Article 1 of the Privacy Shield Decision:

‘1. For the purposes of Article 25(2) of [Directive 95/46], the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the EU-U.S. Privacy Shield.

2. The EU-U.S. Privacy Shield is constituted by the Principles issued by the U.S. Department of Commerce on 7 July 2016 as set out in Annex II and the official representations and commitments contained in the documents listed in Annexes I [and] III to VII.

3. For the purpose of paragraph 1, personal data are transferred under the EU-U.S. Privacy Shield where they are transferred from the Union to organisations in the United States that are included in the “Privacy Shield List”, maintained and made publicly available by the U.S. Department of Commerce, in accordance with Sections I and III of the Principles set out in Annex II.’

47. Under the heading ‘EU-U.S. Privacy Shield Framework Principles issued by the U.S. Department of Commerce’, Annex II to the Privacy Shield Decision, provides, in paragraph I.5 thereof, that adherence to those principles may be limited, inter alia, ‘to the extent necessary to meet national security, public interest, or law enforcement requirements’.

48. Annex III to that decision contains a letter from Mr John Kerry, then Secretary of State (United States), to the Commissioner for Justice, Consumers and Gender Equality from 7 July 2016, to which a memorandum, Annex A, was attached, entitled ‘EU-U.S. Privacy Shield Ombudsperson mechanism regarding signals intelligence’, the latter of which contains the following passage:

‘In recognition of the importance of the EU-U.S. Privacy Shield Framework, this Memorandum sets forth the process for implementing a new mechanism, consistent with [PPD-28], regarding signals intelligence ...

... President Obama announced the issuance of a new presidential directive — PPD-28 — to “clearly prescribe what we do, and do not do, when it comes to our overseas surveillance.”

Section 4(d) of PPD-28 directs the Secretary of State to designate a “Senior Coordinator for International Information Technology Diplomacy” (Senior Coordinator) “to [...] serve as a point of contact for foreign governments who wish to raise concerns regarding signals intelligence activities conducted by the United States.” ...

...

1. ... The Senior Coordinator will serve as the Privacy Shield Ombudsperson and ... will work closely with appropriate officials from other departments and agencies who are responsible for processing requests in accordance with applicable United States law and policy. The Ombudsperson is independent from the Intelligence Community. The Ombudsperson reports directly to the Secretary of State who will ensure that the Ombudsperson carries out its function objectively and free from improper influence that is liable to have an effect on the response to be provided.

...'

49. Annex VI to the Privacy Shield Decision contains a letter from the Office of the Director of National Intelligence to the United States Department of Commerce and to the International Trade Administration from 21 June 2016, in which it is stated that PPD-28 allows for “bulk” collection ... of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target ... to focus the collection’.

The dispute in the main proceedings and the questions referred for a preliminary ruling

50. Mr Schrems, an Austrian national residing in Austria, has been a user of the Facebook social network (‘Facebook’) since 2008.

51. Any person residing in the European Union who wishes to use Facebook is required to conclude, at the time of his or her registration, a contract with Facebook Ireland, a subsidiary of Facebook Inc. which is itself established in the United States. Some or all of the personal data of Facebook Ireland’s users who reside in the European Union is transferred to servers belonging to Facebook Inc. that are located in the United States, where it undergoes processing.

52. On 25 June 2013, Mr Schrems filed a complaint with the Commissioner whereby he requested, in essence, that Facebook Ireland be prohibited from transferring his personal data to the United States, on the ground that the law and practice in force in that country did not ensure adequate protection of the personal data held in its territory against the surveillance activities in which the public authorities were engaged. That complaint was rejected on the ground, inter alia, that, in Decision 2000/520, the Commission had found that the United States ensured an adequate level of protection.

53. The High Court (Ireland), before which Mr Schrems had brought judicial review proceedings against the rejection of his complaint, made a request to the Court for a preliminary ruling on the interpretation and validity of Decision 2000/520. In a judgment of 6 October 2015, Schrems (C-362/14, EU:C:2015:650), the Court declared that decision invalid.

54. Following that judgment, the referring court annulled the rejection of Mr Schrems’s complaint and referred that decision back to the Commissioner. In the course of the Commissioner’s investigation, Facebook Ireland explained that a large part of personal data was transferred to Facebook Inc. pursuant to the standard data protection clauses set out in the annex to the SCC Decision. On that basis, the Commissioner asked Mr Schrems to reformulate his complaint.

55. In his reformulated complaint lodged on 1 December 2015, Mr Schrems claimed, *inter alia*, that United States law requires Facebook Inc. to make the personal data transferred to it available to certain United States authorities, such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI). He submitted that, since that data was used in the context of various monitoring programmes in a manner incompatible with Articles 7, 8 and 47 of the Charter, the SCC Decision cannot justify the transfer of that data to the United States. In those circumstances, Mr Schrems asked the Commissioner to prohibit or suspend the transfer of his personal data to Facebook Inc.

56. On 24 May 2016, the Commissioner published a 'draft decision' summarising the provisional findings of her investigation. In that draft decision, she took the provisional view that the personal data of EU citizens transferred to the United States were likely to be consulted and processed by the US authorities in a manner incompatible with Articles 7 and 8 of the Charter and that US law did not provide those citizens with legal remedies compatible with Article 47 of the Charter. The Commissioner found that the standard data protection clauses in the annex to the SCC Decision are not capable of remedying that defect, since they confer only contractual rights on data subjects against the data exporter and importer, without, however, binding the United States authorities.

57. Taking the view that, in those circumstances, Mr Schrems's reformulated complaint raised the issue of the validity of the SCC Decision, on 31 May 2016, the Commissioner brought an action before the High Court, relying on the case-law arising from the judgment of 6 October 2015, *Schrems* (C-362/14, EU:C:2015:650, paragraph 65), in order for the High Court to refer a question on that issue to the Court. By order of 4 May 2018, the High Court made the present reference for a preliminary ruling to the Court.

58. In an annex to the order for reference, the High Court provided a copy of a judgment handed down on 3 October 2017, in which it had set out the results of an examination of the evidence produced before it in the national proceedings, in which the US Government had participated.

59. In that judgment, to which the request for a preliminary ruling refers on several occasions, the referring court stated that, as a matter of principle, it is not only entitled, but is obliged, to consider all of the facts and arguments presented to it and to decide on the basis of those facts and arguments whether or not a reference is required. The High Court considers that, in any event, it is required to take into account any amendments that may have occurred in the interval between the institution of the proceedings and the hearing which it held. That court stated that, in the main proceedings, its own assessment is not confined to the grounds of invalidity put forward by the Commissioner, as a

result of which it may of its own motion decide that there are other well-founded grounds of invalidity and, on those grounds, refer questions for a preliminary ruling.

60. According to the findings in that judgment, the US authorities' intelligence activities concerning the personal data transferred to the United States are based, inter alia, on Section 702 of the FISA and on E.O. 12333.

61. In its judgment, the referring court specifies that Section 702 of the FISA permits the Attorney General and the Director of National Intelligence to authorise jointly, following FISC approval, the surveillance of individuals who are not United States citizens located outside the United States in order to obtain 'foreign intelligence information', and provides, inter alia, the basis for the PRISM and UPSTREAM surveillance programmes. In the context of the PRISM programme, Internet service providers are required, according to the findings of that court, to supply the NSA with all communications to and from a 'selector', some of which are also transmitted to the FBI and the Central Intelligence Agency (CIA).

62. As regards the UPSTREAM programme, that court found that, in the context of that programme, telecommunications undertakings operating the 'backbone' of the Internet — that is to say, the network of cables, switches and routers — are required to allow the NSA to copy and filter Internet traffic flows in order to acquire communications from, to or about a non-US national associated with a 'selector'. Under that programme, the NSA has, according to the findings of that court, access both to the metadata and to the content of the communications concerned.

63. The referring court found that E.O. 12333 allows the NSA to access data 'in transit' to the United States, by accessing underwater cables on the floor of the Atlantic, and to collect and retain such data before arriving in the United States and being subject there to the FISA. It adds that activities conducted pursuant to E.O. 12333 are not governed by statute.

64. As regards the limits on intelligence activities, the referring court emphasises the fact that non-US persons are covered only by PPD-28, which merely states that intelligence activities should be 'as tailored as feasible'. On the basis of those findings, the referring court considers that the United States carries out mass processing of personal data without ensuring a level of protection essentially equivalent to that guaranteed by Articles 7 and 8 of the Charter.

65. As regards judicial protection, the referring court states that EU citizens do not have the same remedies as US citizens in respect of the processing of personal data by the US authorities, since the Fourth Amendment to the Constitution of the United States, which constitutes, in United States law,

the most important cause of action available to challenge unlawful surveillance, does not apply to EU citizens. In that regard, the referring court states that there are substantial obstacles in respect of the causes of action open to EU citizens, in particular that of locus standi, which it considers to be excessively difficult to satisfy. Furthermore, according to the findings of the referring court, the NSA's activities based on E.O. 12333 are not subject to judicial oversight and are not justiciable. Lastly, the referring court considers that, in so far as, in its view, the Privacy Shield Ombudsperson is not a tribunal within the meaning of Article 47 of the Charter, US law does not afford EU citizens a level of protection essentially equivalent to that guaranteed by the fundamental right enshrined in that article.

66. In its request for reference preliminary ruling, the referring court also states that the parties to the main proceedings disagree, *inter alia*, on the applicability of EU law to transfers to a third country of personal data which are likely to be processed by the authorities of that country, *inter alia*, for purposes of national security and on the factors to be taken into consideration for the purposes of assessing whether that country ensures an adequate level of protection. In particular, that court notes that, according to Facebook Ireland, the Commission's findings on the adequacy of the level of protection ensured by a third country, such as those set out in the Privacy Shield Decision, are also binding on the supervisory authorities in the context of a transfer of personal data pursuant to the standard data protection clauses in the annex to the SCC Decision.

67. As regards those standard data protection clauses, that court asks whether the SCC Decision may be considered to be valid, despite the fact that, according to that court, those clauses are not binding on the State authorities of the third country concerned and, therefore, are not capable of remedying a possible lack of an adequate level of protection in that country. In that regard, it considers that the possibility, afforded to the competent authorities in the Member States by Article 4(1)(a) of Decision 2010/87, in its version prior to the entry into force of Implementing Decision 2016/2297, of prohibiting transfers of personal data to a third country that imposes requirements on the importer that are incompatible with the guarantees contained in those clauses, demonstrates that the state of the law in the third country can justify prohibiting the transfer of data, even when carried out pursuant to the standard data protection clauses in the annex to the SCC Decision, and therefore makes clear that those requirements may be insufficient in ensuring an adequate level of protection. Nonetheless, the referring court harbours doubts as to the extent of the Commissioner's power to prohibit a transfer of data based on those clauses, despite taking the view that discretion cannot be sufficient to ensure adequate protection.

68. In those circumstances, the High Court decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

(1) In circumstances in which personal data is transferred by a private company from a European Union (EU) Member State to a private company in a third country for a commercial purpose pursuant to [the SCC Decision] and may be further processed in the third country by its authorities for purposes of national security but also for purposes of law enforcement and the conduct of the foreign affairs of the third country, does EU law (including the Charter) apply to the transfer of the data notwithstanding the provisions of Article 4(2) TEU in relation to national security and the provisions of the first indent of Article 3(2) of Directive [95/46] in relation to public security, defence and State security?

(2) (a) In determining whether there is a violation of the rights of an individual through the transfer of data from the [European Union] to a third country under the [SCC Decision] where it may be further processed for national security purposes, is the relevant comparator for the purposes of [Directive 95/46]:

(i) the Charter, the EU Treaty, the FEU Treaty, [Directive 95/46], the [European Convention for the Protection of Human Rights and Fundamental Freedoms, signed at Rome on 4 November 1950] (or any other provision of EU law); or

(ii) the national laws of one or more Member States?

(b) If the relevant comparator is (ii), are the practices in the context of national security in one or more Member States also to be included in the comparator?

(3) When assessing whether a third country ensures the level of protection required by EU law to personal data transferred to that country for the purposes of Article 26 of [Directive 95/46], ought the level of protection in the third country be assessed by reference to:

(a) the applicable rules in the third country resulting from its domestic law or international commitments, and the practice designed to ensure compliance with those rules, to include the professional rules and security measures which are complied with in the third country;

or

(b) the rules referred to in (a) together with such administrative, regulatory and compliance practices and policy safeguards, procedures, protocols, oversight mechanisms and non-judicial remedies as are in place in the third country?

(4) Given the facts found by the High Court in relation to US law, if personal data is transferred from the European Union to the United States under [the SCC Decision] does this violate the rights of individuals under Articles 7 and/or 8 of the Charter?

(5) Given the facts found by the High Court in relation to US law, if personal data is transferred from the European Union to the United States under [the SCC Decision]:

(a) does the level of protection afforded by the United States respect the essence of an individual's right to a judicial remedy for breach of his or her data privacy rights guaranteed by Article 47 of the Charter?

If the answer to Question 5(a) is in the affirmative:

(b) are the limitations imposed by US law on an individual's right to a judicial remedy in the context of US national security proportionate within the meaning of Article 52 of the Charter and do not exceed what is necessary in a democratic society for national security purposes?

(6) (a) What is the level of protection required to be afforded to personal data transferred to a third country pursuant to standard contractual clauses adopted in accordance with a decision of the Commission under Article 26(4) [of Directive 95/46] in light of the provisions of [Directive 95/46] and in particular Articles 25 and 26 read in the light of the Charter?

(b) What are the matters to be taken into account in assessing whether the level of protection afforded to data transferred to a third country under [the SCC Decision] satisfies the requirements of [Directive 95/46] and the Charter?

(7) Does the fact that the standard contractual clauses apply as between the data exporter and the data importer and do not bind the national authorities of a third country who may require the data importer to make available to its security services for further processing the personal data transferred pursuant to the clauses provided for in [the SCC Decision] preclude the clauses from adducing adequate safeguards as envisaged by Article 26(2) of [Directive 95/46]?

(8) If a third country data importer is subject to surveillance laws that in the view of a data protection authority conflict with the [standard contractual clauses] or Article 25 and 26 of [Directive 95/46] and/or the Charter, is a data protection authority required to use its enforcement powers under Article 28(3) of [Directive 95/46] to suspend data flows or is the exercise of those powers limited to exceptional cases only, in light of recital 11 of [the SCC Decision], or can a data protection authority use its discretion not to suspend data flows?

(9) (a) For the purposes of Article 25(6) of [Directive 95/46], does [the Privacy Shield Decision] constitute a finding of general application binding on data protection authorities and the courts of the Member States to the effect that the United States ensures an adequate level of protection within the meaning of Article 25(2) of [Directive 95/46] by reason of its domestic law or of the international commitments it has entered into?

(b) If it does not, what relevance, if any, does the Privacy Shield Decision have in the assessment conducted into the adequacy of the safeguards provided to data transferred to the United States which is transferred pursuant to the [SCC Decision]?

(10) Given the findings of the High Court in relation to US law, does the provision of the Privacy Shield ombudsperson under Annex A to Annex III to the Privacy Shield Decision when taken in conjunction with the existing regime in the United States ensure that the US provides a remedy to data subjects whose personal data is transferred to the United States under the [SCC Decision] that is compatible with Article 47 of the Charter?

(11) Does the [SCC Decision] violate Articles 7, 8 and/or 47 of the Charter?’

Admissibility of the request for a preliminary ruling

69. Facebook Ireland and the German and United Kingdom Governments claim that the request for a preliminary ruling is inadmissible.

70. With regard to the objection raised by Facebook Ireland, that company observes that the provisions of Directive 95/46, on which the questions referred for a preliminary ruling are based, were repealed by the GDPR.

71. In that regard, although Directive 95/46 was, under Article 94(1) of the GDPR, repealed with effect from 25 May 2018, that directive was still in force when, on 4 May 2018, the present request for a preliminary ruling, received at the Court on 9 May 2018, was made. In addition, the first indent of Article 3(2) and Articles 25, 26 and 28(3) of Directive 95/46 cited in the questions referred, were, in essence, reproduced in Article 2(2) and Articles 45, 46 and 58 of the GDPR, respectively. Furthermore, it must be borne in mind that the Court has a duty to interpret all provisions of EU law which national courts require in order to decide the actions pending before them, even if those provisions are not expressly indicated in the questions referred to the Court of Justice by those courts (judgment of 2 April 2020, *Ruska Federacija*, C-897/19 PPU, EU:C:2020:262, paragraph 43 and the case-law cited). On those grounds, the fact that the referring court referred its questions by reference solely to the provisions of Directive 95/46 cannot render the present request for a preliminary ruling inadmissible.

72. For its part, the German Government bases its objection of inadmissibility on the fact, first, that the Commissioner merely expressed doubts, and not a definitive opinion, as to the validity of the SCC Decision and, second, that the referring court failed to ascertain whether Mr Schrems had unambiguously given his consent to the transfers of data at issue in the main proceedings, which, if that had been the case, would have the effect of rendering an answer to that question redundant. Lastly, the United Kingdom Government maintains that the questions referred for a preliminary ruling are hypothetical since that court did not find that that data had actually been transferred on the basis of that decision.

73. It follows from settled case-law of the Court that it is solely for the national court before which the dispute has been brought, and which must assume responsibility for the subsequent judicial decision, to determine, in the light of the particular circumstances of the case, both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it submits to the Court. Consequently, where the questions referred concern the interpretation or the validity of a rule of EU law, the Court is in principle bound to give a ruling. It follows that questions referred by national courts enjoy a presumption of relevance. The Court may refuse to rule on a question referred by a national court only where it appears that the interpretation sought bears no relation to the actual facts of the main action or its object, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (judgments of 16 June 2015, *Gauweiler and Others*, C-62/14, EU:C:2015:400, paragraphs 24 and 25; of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, paragraph 45; and of 19 December 2019, *Dobersberger*, C-16/18, EU:C:2019:1110, paragraphs 18 and 19).

74. In the present case, the request for a preliminary ruling contains sufficient factual and legal material to understand the significance of the questions referred. Furthermore, and most importantly, nothing in the file before the Court leads to the conclusion that the interpretation of EU law that is requested is unrelated to the actual facts of the main action or its object, or that the problem is hypothetical, *inter alia*, on the basis that the transfer of the personal data at issue in the main proceedings may have been based on the express consent of the data subject of that transfer rather than based on the SCC Decision. As indicated in the request for a preliminary ruling, Facebook Ireland has acknowledged that it transfers the personal data of its subscribers residing in the European Union to Facebook Inc. and that those transfers, the lawfulness of which Mr Schrems disputes, were in large part carried out pursuant to the standard data protection clauses in the annex to the SCC Decision.

75. Moreover, it is irrelevant to the admissibility of the present request for a preliminary ruling that the Commissioner did not express a definitive opinion on the validity of that decision in so far as the referring court considers that an answer to the questions referred for a preliminary ruling concerning the interpretation and validity of rules of EU law is necessary in order to dispose of the case in the main proceedings.

76. It follows that the request for a preliminary ruling is admissible.

Consideration of the questions referred

77. As a preliminary matter, it must be borne in mind that the present request for a preliminary ruling has arisen following a complaint made by Mr Schrems requesting that the Commissioner order the suspension or prohibition, in the future, of the transfer by Facebook Ireland of his personal data to Facebook Inc. Although the questions referred for a preliminary ruling refer to the provisions of Directive 95/46, it is common ground that the Commissioner had not yet adopted a final decision on that complaint when that directive was repealed and replaced by the GDPR with effect from 25 May 2018.

78. That absence of a national decision distinguishes the situation at issue in the main proceedings from those which gave rise to the judgments of 24 September 2019, *Google* (Territorial scope of de-referencing) (C-507/17, EU:C:2019:772), and of 1 October 2019, *Planet49* (C-673/17, EU:C:2019:801), in which decisions adopted prior to the repeal of that directive were at issue.

79. The questions referred for a preliminary ruling must therefore be answered in the light of the provisions of the GDPR rather than those of Directive 95/46.

The first question

80. By its first question, the referring court wishes to know, in essence, whether Article 2(1) and Article 2(2)(a), (b) and (d) of the GDPR, read in conjunction with Article 4(2) TEU, must be interpreted as meaning that that regulation applies to the transfer of personal data by an economic operator established in a Member State to another economic operator established in a third country, in circumstances where, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of that third country for the purposes of public security, defence and State security.

81. In that regard, it should be made clear at the outset that the rule in Article 4(2) TEU, according to which, within the European Union, national security remains the sole responsibility of each Member State, concerns Member States of the European Union only. That rule is therefore irrelevant, in the present case, for the purposes of interpreting Article 2(1) and Article 2(2)(a), (b) and (d) of the GDPR.

82. Under Article 2(1) of the GDPR, that regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. Article 4(2) of that regulation defines ‘processing’ as ‘any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means’ and mentions, by way of example, ‘disclosure by transmission, dissemination or otherwise making available’, but does not distinguish between operations which take place within the European Union and those which are connected with a third country. Furthermore, the GDPR subjects transfers of personal data to third countries to specific rules in Chapter V thereof, entitled ‘Transfers of personal data to third countries or international organisations’, and also confers specific powers on the supervisory authorities for that purpose, which are set out in Article 58(2)(j) of that regulation.

83. It follows that the operation of having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 4(2) of the GDPR, carried out in a Member State, and falls within the scope of that regulation under Article 2(1) thereof (see, by analogy, as regards Article 2(b) and Article 3(1) of Directive 95/46, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 45 and the case-law cited).

84. As to whether such an operation may be regarded as being excluded from the scope of the GDPR under Article 2(2) thereof, it should be noted that that provision lays down exceptions to the scope of that regulation, as defined in Article 2(1) thereof, which must be interpreted strictly (see, by analogy, as regards Article 3(2) of Directive 95/46, judgment of 10 July 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, paragraph 37 and the case-law cited).

85. In the present case, since the transfer of personal data at issue in the main proceedings is from Facebook Ireland to Facebook Inc., namely between two legal persons, that transfer does not fall within Article 2(2)(c) of the GDPR, which refers to the processing of data by a natural person in the course of a purely personal or household activity. Such a transfer also does not fall within the exceptions laid down in Article 2(2)(a), (b) and (d) of that regulation, since the activities mentioned therein by way of example are, in any event, activities of the State or of State authorities and are unrelated to fields in which individuals are active (see, by analogy, as regards Article 3(2) of Directive 95/46, judgment of 10 July 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, paragraph 38 and the case-law cited).

86. The possibility that the personal data transferred between two economic operators for commercial purposes might undergo, at the time of the transfer or thereafter, processing for the purposes of public

security, defence and State security by the authorities of that third country cannot remove that transfer from the scope of the GDPR.

87. Indeed, by expressly requiring the Commission, when assessing the adequacy of the level of protection afforded by a third country, to take account, *inter alia*, of ‘relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation’, it is patent from the very wording of Article 45(2)(a) of that regulation that no processing by a third country of personal data for the purposes of public security, defence and State security excludes the transfer at issue from the application of the regulation.

88. It follows that such a transfer cannot fall outside the scope of the GDPR on the ground that the data at issue is liable to be processed, at the time of that transfer or thereafter, by the authorities of the third country concerned, for the purposes of public security, defence and State security.

89. Therefore, the answer to the first question is that Article 2(1) and (2) of the GDPR must be interpreted as meaning that that regulation applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security.

The second, third and sixth questions

90. By its second, third and sixth questions, the referring court seeks clarification from the Court, in essence, on the level of protection required by Article 46(1) and Article 46(2)(c) of the GDPR in respect of a transfer of personal data to a third country based on standard data protection clauses. In particular, the referring court asks the Court to specify which factors need to be taken into consideration for the purpose of determining whether that level of protection is ensured in the context of such a transfer.

91. As regards the level of protection required, it follows from a combined reading of those provisions that, in the absence of an adequacy decision under Article 45(3) of that regulation, a controller or processor may transfer personal data to a third country only if the controller or processor has provided ‘appropriate safeguards’, and on condition that ‘enforceable data subject rights and effective legal remedies for data subjects’ are available, such safeguards being able to be provided, *inter alia*, by the standard data protection clauses adopted by the Commission.

92. Although Article 46 of the GDPR does not specify the nature of the requirements which flow from that reference to ‘appropriate safeguards’, ‘enforceable rights’ and ‘effective legal remedies’, it should be noted that that article appears in Chapter V of that regulation and, accordingly, must be read in the light of Article 44 of that regulation, entitled ‘General principle for transfers’, which lays down that ‘all provisions [in that chapter] shall be applied in order to ensure that the level of protection of natural persons guaranteed by [that regulation] is not undermined’. That level of protection must therefore be guaranteed irrespective of the provision of that chapter on the basis of which a transfer of personal data to a third country is carried out.

93. As the Advocate General stated in point 117 of his Opinion, the provisions of Chapter V of the GDPR are intended to ensure the continuity of that high level of protection where personal data is transferred to a third country, in accordance with the objective set out in recital 6 thereof.

94. The first sentence of Article 45(1) of the GDPR provides that a transfer of personal data to a third country may be authorised by a Commission decision to the effect that that third country, a territory or one or more specified sectors within that third country, ensures an adequate level of protection. In that regard, although not requiring a third country to ensure a level of protection identical to that guaranteed in the EU legal order, the term ‘adequate level of protection’ must, as confirmed by recital 104 of that regulation, be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the regulation, read in the light of the Charter. If there were no such requirement, the objective referred to in the previous paragraph would be undermined (see, by analogy, as regards Article 25(6) of Directive 95/46, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 73).

95. In that context, recital 107 of the GDPR states that, where ‘a third country, a territory or a specified sector within a third country ... no longer ensures an adequate level of data protection. ... the transfer of personal data to that third country ... should be prohibited, unless the requirements [of that regulation] relating to transfers subject to appropriate safeguards ... are fulfilled’. To that effect, recital 108 of the regulation states that, in the absence of an adequacy decision, the appropriate safeguards to be taken by the controller or processor in accordance with Article 46(1) of the regulation must ‘compensate for the lack of data protection in a third country’ in order to ‘ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union’.

96. It follows, as the Advocate General stated in point 115 of his Opinion, that such appropriate guarantees must be capable of ensuring that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded, as in the context of a transfer based on an adequacy decision, a level of protection essentially equivalent to that which is guaranteed within the European Union.

97. The referring court also asks whether the level of protection essentially equivalent to that guaranteed within the European Union must be determined in the light of EU law, in particular the rights guaranteed by the Charter and/or the fundamental rights enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms ('the ECHR'), or in the light of the national law of the Member States.

98. In that regard, it should be noted that, although, as Article 6(3) TEU confirms, the fundamental rights enshrined in the ECHR constitute general principles of EU law and although Article 52(3) of the Charter provides that the rights contained in the Charter which correspond to rights guaranteed by the ECHR are to have the same meaning and scope as those laid down by that convention, the latter does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into EU law (judgments of 26 February 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, paragraph 44 and the case-law cited, and of 20 March 2018, Menci, C-524/15, EU:C:2018:197, paragraph 22).

99. In those circumstances, the Court has held that the interpretation of EU law and examination of the legality of EU legislation must be undertaken in the light of the fundamental rights guaranteed by the Charter (see, by analogy, judgment of 20 March 2018, Menci, C-524/15, EU:C:2018:197, paragraph 24).

100. Furthermore, the Court has consistently held that the validity of provisions of EU law and, in the absence of an express reference to the national law of the Member States, their interpretation, cannot be construed in the light of national law, even national law of constitutional status, in particular fundamental rights as formulated in the national constitutions (see, to that effect, judgments of 17 December 1970, *Internationale Handelsgesellschaft*, 11/70, EU:C:1970:114, paragraph 3; of 13 December 1979, *Hauer*, 44/79, EU:C:1979:290, paragraph 14; and of 18 October 2016, *Nikiforidis*, C-135/15, EU:C:2016:774, paragraph 28 and the case-law cited).

101. It follows that, since, first, a transfer of personal data, such as that at issue in the main proceedings, for commercial purposes by an economic operator established in one Member State to another economic operator established in a third country, falls, as is apparent from the answer to the

first question, within the scope of the GDPR and, second, the purpose of that regulation is, *inter alia*, as is apparent from recital 10 thereof, to ensure a consistent and high level of protection of natural persons within the European Union and, to that end, to ensure a consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of such natural persons with regard to the processing of personal data throughout the European Union, the level of protection of fundamental rights required by Article 46(1) of that regulation must be determined on the basis of the provisions of that regulation, read in the light of the fundamental rights enshrined in the Charter.

102. The referring court also seeks to ascertain what factors should be taken into consideration for the purposes of determining the adequacy of the level of protection where personal data is transferred to a third country pursuant to standard data protection clauses adopted under Article 46(2)(c) of the GDPR.

103. In that regard, although that provision does not list the various factors which must be taken into consideration for the purposes of assessing the adequacy of the level of protection to be observed in such a transfer, Article 46(1) of that regulation states that data subjects must be afforded appropriate safeguards, enforceable rights and effective legal remedies.

104. The assessment required for that purpose in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country. As regards the latter, the factors to be taken into consideration in the context of Article 46 of that regulation correspond to those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.

105. Therefore, the answer to the second, third and sixth questions is that Article 46(1) and Article 46(2)(c) of the GDPR must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter. To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by

the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.

The eighth question

106. By its eighth question, the referring court wishes to know, in essence, whether Article 58(2)(f) and (j) of the GDPR must be interpreted as meaning that the competent supervisory authority is required to suspend or prohibit a transfer of personal data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of the GDPR and by the Charter, cannot be ensured, or as meaning that the exercise of those powers is limited to exceptional cases.

107. In accordance with Article 8(3) of the Charter and Article 51(1) and Article 57(1)(a) of the GDPR, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of natural persons with regard to the processing of personal data. Each of those authorities is therefore vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down in that regulation (see, by analogy, as regards Article 28 of Directive 95/46, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 47).

108. It follows from those provisions that the supervisory authorities' primary responsibility is to monitor the application of the GDPR and to ensure its enforcement. The exercise of that responsibility is of particular importance where personal data is transferred to a third country since, as is clear from recital 116 of that regulation, 'when personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information'. In such cases, as is stated in that recital, 'supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders'.

109. In addition, under Article 57(1)(f) of the GDPR, each supervisory authority is required on its territory to handle complaints which, in accordance with Article 77(1) of that regulation, any data subject is entitled to lodge where that data subject considers that the processing of his or her personal data infringes the regulation, and is required to examine the nature of that complaint as necessary. The supervisory authority must handle such a complaint with all due diligence (see, by analogy, as

regards Article 25(6) of Directive 95/46, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 63).

110. Article 78(1) and (2) of the GDPR recognises the right of each person to an effective judicial remedy, in particular, where the supervisory authority fails to deal with his or her complaint. Recital 141 of that regulation also refers to that ‘right to an effective judicial remedy in accordance with Article 47 of the Charter’ in circumstances where that supervisory authority ‘does not act where such action is necessary to protect the rights of the data subject’.

111. In order to handle complaints lodged, Article 58(1) of the GDPR confers extensive investigative powers on each supervisory authority. If a supervisory authority takes the view, following an investigation, that a data subject whose personal data have been transferred to a third country is not afforded an adequate level of protection in that country, it is required, under EU law, to take appropriate action in order to remedy any findings of inadequacy, irrespective of the reason for, or nature of, that inadequacy. To that effect, Article 58(2) of that regulation lists the various corrective powers which the supervisory authority may adopt.

112. Although the supervisory authority must determine which action is appropriate and necessary and take into consideration all the circumstances of the transfer of personal data in question in that determination, the supervisory authority is nevertheless required to execute its responsibility for ensuring that the GDPR is fully enforced with all due diligence.

113. In that regard, as the Advocate General also stated in point 148 of his Opinion, the supervisory authority is required, under Article 58(2)(f) and (j) of that regulation, to suspend or prohibit a transfer of personal data to a third country if, in its view, in the light of all the circumstances of that transfer, the standard data protection clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.

114. The interpretation in the previous paragraph is not undermined by the Commissioner’s reasoning that Article 4 of Decision 2010/87, in its version prior to the entry into force of Implementing Decision 2016/2297, read in the light of recital 11 of that decision, confined the power of supervisory authorities to suspend or prohibit a transfer of personal data to a third country to certain exceptional circumstances. As amended by Implementing Decision 2016/2297, Article 4 of the SCC Decision refers to the power of the supervisory authorities, now under Article 58(2)(f) and (j) of the GDPR, to suspend or ban such a transfer, without confining the exercise of that power to exceptional circumstances.

115. In any event, the implementing power which Article 46(2)(c) of the GDPR grants to the Commission for the purposes of adopting standard data protection clauses does not confer upon it competence to restrict the national supervisory authorities' powers on the basis of Article 58(2) of that regulation (see, by analogy, as regards Article 25(6) and Article 28 of Directive 95/46, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraphs 102 and 103). Moreover, as stated in recital 5 of Implementing Decision 2016/2297, the SCC Decision 'does not prevent a [supervisory authority] from exercising its powers to oversee data flows, including the power to suspend or ban a transfer of personal data when it determines that the transfer is carried out in violation of EU or national data protection law'.

116. It should, however, be pointed out that the powers of the competent supervisory authority are subject to full compliance with the decision in which the Commission finds, where relevant, under the first sentence of Article 45(1) of the GDPR, that a particular third country ensures an adequate level of protection. In such a case, it is clear from the second sentence of Article 45(1) of that regulation, read in conjunction with recital 103 thereof, that transfers of personal data to the third country in question may take place without requiring any specific authorisation.

117. Under the fourth paragraph of Article 288 TFEU, a Commission adequacy decision is, in its entirety, binding on all the Member States to which it is addressed and is therefore binding on all their organs in so far as it finds that the third country in question ensures an adequate level of protection and has the effect of authorising such transfers of personal data (see, by analogy, as regards Article 25(6) of Directive 95/46, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 51 and the case-law cited).

118. Thus, until such time as a Commission adequacy decision is declared invalid by the Court, the Member States and their organs, which include their independent supervisory authorities, cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection (judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 52 and the case-law cited) and, as a result, to suspend or prohibit transfers of personal data to that third country.

119. However, a Commission adequacy decision adopted pursuant to Article 45(3) of the GDPR cannot prevent persons whose personal data has been or could be transferred to a third country from lodging a complaint, within the meaning of Article 77(1) of the GDPR, with the competent national supervisory authority concerning the protection of their rights and freedoms in regard to the processing of that data. Similarly, a decision of that nature cannot eliminate or reduce the powers

expressly accorded to the national supervisory authorities by Article 8(3) of the Charter and Article 51(1) and Article 57(1)(a) of the GDPR (see, by analogy, as regards Article 25(6) and Article 28 of Directive 95/46, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 53).

120. Thus, even if the Commission has adopted a Commission adequacy decision, the competent national supervisory authority, when a complaint is lodged by a person concerning the protection of his or her rights and freedoms in regard to the processing of personal data relating to him or her, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the GDPR and, where relevant, to bring an action before the national courts in order for them, if they share the doubts of that supervisory authority as to the validity of the Commission adequacy decision, to make a reference for a preliminary ruling for the purpose of examining its validity (see, by analogy, as regards Article 25(6) and Article 28 of Directive 95/46, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraphs 57 and 65).

121. In the light of the foregoing considerations, the answer to the eighth question is that Article 58(2)(f) and (j) of the GDPR must be interpreted as meaning that, unless there is a valid Commission adequacy decision, the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of the GDPR and by the Charter, cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.

The 7th and 11th questions

122. By its 7th and 11th questions, which it is appropriate to consider together, the referring court seeks clarification from the Court, in essence, on the validity of the SCC Decision in the light of Articles 7, 8 and 47 of the Charter.

123. In particular, as is clear from the wording of the seventh question and the corresponding explanations in the request for a preliminary ruling, the referring court asks whether the SCC Decision is capable of ensuring an adequate level of protection of the personal data transferred to third countries given that the standard data protection clauses provided for in that decision do not bind the supervisory authorities of those third countries.

124. Article 1 of the SCC Decision provides that the standard data protection clauses set out in its annex are considered to offer adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals in accordance with the requirements of Article 26(2) of Directive 95/46. The latter provision was, in essence, reproduced in Article 46(1) and Article 46(2)(c) of the GDPR.

125. However, although those clauses are binding on a controller established in the European Union and the recipient of the transfer of personal data established in a third country where they have concluded a contract incorporating those clauses, it is common ground that those clauses are not capable of binding the authorities of that third country, since they are not party to the contract.

126. Therefore, although there are situations in which, depending on the law and practices in force in the third country concerned, the recipient of such a transfer is in a position to guarantee the necessary protection of the data solely on the basis of standard data protection clauses, there are others in which the content of those standard clauses might not constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country concerned. That is the case, in particular, where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates.

127. Thus, the question arises whether a Commission decision concerning standard data protection clauses, adopted pursuant to Article 46(2)(c) of the GDPR, is invalid in the absence, in that decision, of guarantees which can be enforced against the public authorities of the third countries to which personal data is or could be transferred pursuant to those clauses.

128. Article 46(1) of the GDPR provides that, in the absence of an adequacy decision, a controller or processor may transfer personal data to a third country only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. According to Article 46(2)(c) of the GDPR, those safeguards may be provided by standard data protection clauses drawn up by the Commission. However, those provisions do not state that all safeguards must necessarily be provided for in a Commission decision such as the SCC Decision.

129. It should be noted in that regard that such a standard clauses decision differs from an adequacy decision adopted pursuant to Article 45(3) of the GDPR, which seeks, following an examination of the legislation of the third country concerned taking into account, *inter alia*, the relevant legislation on national security and public authorities' access to personal data, to find with binding effect that a third country, a territory or one or more specified sectors within that third country ensures an adequate

level of protection and that the access of that third country's public authorities to such data does not therefore impede transfers of such personal data to the third country. Such an adequacy decision can therefore be adopted by the Commission only if it has found that the third country's relevant legislation in that field does in fact provide all the necessary guarantees from which it can be concluded that that legislation ensures an adequate level of protection.

130. By contrast, in the case of a Commission decision adopting standard data protection clauses, such as the SCC Decision, in so far as such a decision does not refer to a third country, a territory or one or more specific sectors in a third country, it cannot be inferred from Article 46(1) and Article 46(2)(c) of the GDPR that the Commission is required, before adopting such a decision, to assess the adequacy of the level of protection ensured by the third countries to which personal data could be transferred pursuant to such clauses.

131. In that regard, it must be borne in mind that, according to Article 46(1) of the GDPR, in the absence of a Commission adequacy decision, it is for the controller or processor established in the European Union to provide, *inter alia*, appropriate safeguards. Recitals 108 and 114 of the GDPR confirm that, where the Commission has not adopted a decision on the adequacy of the level of data protection in a third country, the controller or, where relevant, the processor 'should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject' and that 'those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies ... in the Union or in a third country'.

132. Since by their inherently contractual nature standard data protection clauses cannot bind the public authorities of third countries, as is clear from paragraph 125 above, but that Article 44, Article 46(1) and Article 46(2)(c) of the GDPR, interpreted in the light of Articles 7, 8 and 47 of the Charter, require that the level of protection of natural persons guaranteed by that regulation is not undermined, it may prove necessary to supplement the guarantees contained in those standard data protection clauses. In that regard, recital 109 of the regulation states that 'the possibility for the controller ... to use standard data-protection clauses adopted by the Commission ... should [not] prevent [it] ... from adding other clauses or additional safeguards' and states, in particular, that the controller 'should be encouraged to provide additional safeguards ... that supplement standard [data] protection clauses'.

133. It follows that the standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country. In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection.

134. In that regard, as the Advocate General stated in point 126 of his Opinion, the contractual mechanism provided for in Article 46(2)(c) of the GDPR is based on the responsibility of the controller or his or her subcontractor established in the European Union and, in the alternative, of the competent supervisory authority. It is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses.

135. Where the controller or a processor established in the European Union is not able to take adequate additional measures to guarantee such protection, the controller or processor or, failing that, the competent supervisory authority, are required to suspend or end the transfer of personal data to the third country concerned. That is the case, in particular, where the law of that third country imposes on the recipient of personal data from the European Union obligations which are contrary to those clauses and are, therefore, capable of impinging on the contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data.

136. Therefore, the mere fact that standard data protection clauses in a Commission decision adopted pursuant to Article 46(2)(c) of the GDPR, such as those in the annex to the SCC Decision, do not bind the authorities of third countries to which personal data may be transferred cannot affect the validity of that decision.

137. That validity depends, however, on whether, in accordance with the requirement of Article 46(1) and Article 46(2)(c) of the GDPR, interpreted in the light of Articles 7, 8 and 47 of the Charter, such a standard clauses decision incorporates effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law and that transfers of personal data

pursuant to the clauses of such a decision are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them.

138. As regards the guarantees contained in the standard data protection clauses in the annex to the SCC Decision, it is clear from Clause 4(a) and (b), Clause 5(a), Clause 9 and Clause 11(1) thereof that a data controller established in the European Union, the recipient of the personal data and any processor thereof mutually undertake to ensure that the processing of that data, including the transfer thereof, has been and will continue to be carried out in accordance with ‘the applicable data protection law’, namely, according to the definition set out in Article 3(f) of that decision, ‘the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established’. The provisions of the GDPR, read in the light of the Charter, form part of that legislation.

139. In addition, a recipient of personal data established in a third country undertakes, pursuant to Clause 5(a), to inform the controller established in the European Union promptly of any inability to comply with its obligations under the contract concluded. In particular, according to Clause 5(b), the recipient certifies that it has no reason to believe that the legislation applicable to it prevents it from fulfilling its obligations under the contract entered into and undertakes to notify the data controller about any change in the national legislation applicable to it which is likely to have a substantial adverse effect on the warranties and obligations provided by the standard data protection clauses in the annex to the SCC Decision, promptly upon notice thereof. Furthermore, although Clause 5(d)(i) allows a recipient of personal data not to notify a controller established in the European Union of a legally binding request for disclosure of the personal data by a law enforcement authority, in the event of legislation prohibiting that recipient from doing so, such as a prohibition under criminal law the aim of which is to preserve the confidentiality of a law enforcement investigation, the recipient is nevertheless required, pursuant to Clause 5(a) in the annex to the SCC Decision, to inform the controller of his or her inability to comply with the standard data protection clauses.

140. Clause 5(a) and (b), in both cases to which it refers, confers on the controller established in the European Union the right to suspend the transfer of data and/or to terminate the contract. In the light of the requirements of Article 46(1) and (2)(c) of the GDPR, read in the light of Articles 7 and 8 of the Charter, the controller is bound to suspend the transfer of data and/or to terminate the contract where the recipient is not, or is no longer, able to comply with the standard data protection clauses. Unless

the controller does so, it will be in breach of its obligations under Clause 4(a) in the annex to the SCC Decision as interpreted in the light of the GDPR and of the Charter.

141. It follows that Clause 4(a) and Clause 5(a) and (b) in that annex oblige the controller established in the European Union and the recipient of personal data to satisfy themselves that the legislation of the third country of destination enables the recipient to comply with the standard data protection clauses in the annex to the SCC Decision, before transferring personal data to that third country. As regards that verification, the footnote to Clause 5 states that mandatory requirements of that legislation which do not go beyond what is necessary in a democratic society to safeguard, inter alia, national security, defence and public security are not in contradiction with those standard data protection clauses. Conversely, as stated by the Advocate General in point 131 of his Opinion, compliance with an obligation prescribed by the law of the third country of destination which goes beyond what is necessary for those purposes must be treated as a breach of those clauses. Operators' assessments of the necessity of such an obligation must, where relevant, take into account a finding that the level of protection ensured by the third country in a Commission adequacy decision, adopted under Article 45(3) of the GDPR, is appropriate.

142. It follows that a controller established in the European Union and the recipient of personal data are required to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned. The recipient is, where appropriate, under an obligation, under Clause 5(b), to inform the controller of any inability to comply with those clauses, the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract.

143. If the recipient of personal data to a third country has notified the controller, pursuant to Clause 5(b) in the annex to the SCC Decision, that the legislation of the third country concerned does not allow him or her to comply with the standard data protection clauses in that annex, it follows from Clause 12 in that annex that data that has already been transferred to that third country and the copies thereof must be returned or destroyed in their entirety. In any event, under Clause 6 in that annex, breach of those standard clauses will result in a right for the person concerned to receive compensation for the damage suffered.

144. It should be added that, under Clause 4(f) in the annex to the SCC Decision, a controller established in the European Union undertakes, where special categories of data could be transferred to a third country not providing adequate protection, to inform the data subject before, or as soon as possible after, the transfer. That notice enables the data subject to be in a position to bring legal action against the controller pursuant to Clause 3(1) in that annex so that the controller suspends the

proposed transfer, terminates the contract concluded with the recipient of the personal data or, where appropriate, requires the recipient to return or destroy the data transferred.

145. Lastly, under Clause 4(g) in that annex, the controller established in the European Union is required, when the recipient of personal data notifies him or her, pursuant to Clause 5(b), in the event of a change in the relevant legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the standard data protection clauses, to forward any notification to the competent supervisory authority if the controller established in the European Union decides, notwithstanding that notification, to continue the transfer or to lift the suspension. The forwarding of such a notification to that supervisory authority and its right to conduct an audit of the recipient of personal data pursuant to Clause 8(2) in that annex enable that supervisory authority to ascertain whether the proposed transfer should be suspended or prohibited in order to ensure an adequate level of protection.

146. In that context, Article 4 of the SCC Decision, read in the light of recital 5 of Implementing Decision 2016/2297, supports the view that the SCC Decision does not prevent the competent supervisory authority from suspending or prohibiting, as appropriate, a transfer of personal data to a third country pursuant to the standard data protection clauses in the annex to that decision. In that regard, as is apparent from the answer to the eighth question, unless there is a valid Commission adequacy decision, the competent supervisory authority is required, under Article 58(2)(f) and (j) of the GDPR, to suspend or prohibit such a transfer, if, in its view and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.

147. As regards the fact, underlined by the Commissioner, that transfers of personal data to such a third country may result in the supervisory authorities in the various Member States adopting divergent decisions, it should be added that, as is clear from Article 55(1) and Article 57(1)(a) of the GDPR, the task of enforcing that regulation is conferred, in principle, on each supervisory authority on the territory of its own Member State. Furthermore, in order to avoid divergent decisions, Article 64(2) of the GDPR provides for the possibility for a supervisory authority which considers that transfers of data to a third country must, in general, be prohibited, to refer the matter to the European Data Protection Board (EDPB) for an opinion, which may, under Article 65(1)(c) of the GDPR, adopt a binding decision, in particular where a supervisory authority does not follow the opinion issued.

148. It follows that the SCC Decision provides for effective mechanisms which, in practice, ensure that the transfer to a third country of personal data pursuant to the standard data protection clauses in the annex to that decision is suspended or prohibited where the recipient of the transfer does not comply with those clauses or is unable to comply with them.

149. In the light of all of the foregoing considerations, the answer to the 7th and 11th questions is that examination of the SCC Decision in the light of Articles 7, 8 and 47 of the Charter has disclosed nothing to affect the validity of that decision.

The 4th, 5th, 9th and 10th questions

150. By its ninth question, the referring court wishes to know, in essence, whether and to what extent findings in the Privacy Shield Decision to the effect that the United States ensures an adequate level of protection are binding on the supervisory authority of a Member State. By its 4th, 5th and 10th questions, that court asks, in essence, whether, in view of its own findings on US law, the transfer to that third country of personal data pursuant to the standard data protection clauses in the annex to the SCC Decision breaches the rights enshrined in Articles 7, 8 and 47 of the Charter and asks the Court, in particular, whether the introduction of the ombudsperson referred to in Annex III to the Privacy Shield Decision is compatible with Article 47 of the Charter.

151. As a preliminary matter, it should be noted that, although the Commissioner's action in the main proceedings only calls into question the SCC Decision, that action was brought before the referring court prior to the adoption of the Privacy Shield Decision. In so far as, by its fourth and fifth questions, that court asks the Court, at a general level, what protection must be ensured, under Articles 7, 8 and 47 of the Charter, in the context of such a transfer, the Court's analysis must take into consideration the consequences arising from the subsequent adoption of the Privacy Shield Decision. A fortiori that is the case in so far as the referring court asks expressly, by its 10th question, whether the protection required by Article 47 of the Charter is ensured by the offices of the ombudsperson to which the Privacy Shield Decision refers.

152. In addition, it is clear from the information provided in the order for reference that, in the main proceedings, Facebook Ireland claims that the Privacy Shield Decision is binding on the Commissioner in respect of the finding on the adequacy of the level of protection ensured by the United States and therefore in respect of the lawfulness of a transfer to that third country of personal data pursuant to the standard data protection clauses in the annex to the SCC Decision.

153. As appears from paragraph 59 above, in its judgment of 3 October 2017, provided in an annex to the order for reference, the referring court stated that it was obliged to take account of amendments to the law that may have occurred in the interval between the institution of the proceedings and the hearing of the action before it. Thus, that court would appear to be obliged to take into account, in order to dispose of the case in the main proceedings, the change in circumstances brought about by the adoption of the Privacy Shield Decision and any binding force it may have.

154. In particular, the question whether the finding in the Privacy Shield Decision that the United States ensures an adequate level of protection is binding is relevant for the purposes of assessing both the obligations, set out in paragraphs 141 and 142 above, of the controller and recipient of personal data transferred to a third country pursuant to the standard data protection clauses in the annex to the SCC Decision and also any obligations to which the supervisory authority may be subject to suspend or prohibit such a transfer.

155. As to whether the Privacy Shield Decision has binding effects, Article 1(1) of that decision provides that, for the purposes of Article 45(1) of the GDPR, ‘the United States ensures an adequate level of protection for personal data transferred from the [European] Union to organisations in the United States under the EU-U.S. Privacy Shield’. In accordance with Article 1(3) of the decision, personal data are regarded as transferred under the EU-US Privacy Shield where they are transferred from the Union to organisations in the United States that are included in the ‘Privacy Shield List’, maintained and made publicly available by the US Department of Commerce, in accordance with Sections I and III of the Principles set out in Annex II to that decision.

156. As follows from the case-law set out in paragraphs 117 and 118 above, the Privacy Shield Decision is binding on the supervisory authorities in so far as it finds that the United States ensures an adequate level of protection and, therefore, has the effect of authorising personal data transferred under the EU-US Privacy Shield. Therefore, until the Court should declare that decision invalid, the competent supervisory authority cannot suspend or prohibit a transfer of personal data to an organisation that abides by that privacy shield on the ground that it considers, contrary to the finding made by the Commission in that decision, that the US legislation governing the access to personal data transferred under that privacy shield and the use of that data by the public authorities of that third country for national security, law enforcement and other public interest purposes does not ensure an adequate level of protection.

157. The fact remains that, in accordance with the case-law set out in paragraphs 119 and 120 above, when a person lodges a complaint with the competent supervisory authority, that authority must

examine, with complete independence, whether the transfer of personal data at issue complies with the requirements laid down by the GDPR and, if, in its view, the arguments put forward by that person with a view to challenging the validity of an adequacy decision are well founded, bring an action before the national courts in order for them to make a reference to the Court for a preliminary ruling for the purpose of examining the validity of that decision.

158. A complaint lodged under Article 77(1) of the GDPR, by which a person whose personal data has been or could be transferred to a third country contends that, notwithstanding what the Commission has found in a decision adopted pursuant to Article 45(3) of the GDPR, the law and practices of that country do not ensure an adequate level of protection must be understood as concerning, in essence, the issue of whether that decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals (see, by analogy, as regards Article 25(6) and Article 28(4) of Directive 95/46, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 59).

159. In the present case, in essence, Mr Schrems requested the Commissioner to prohibit or suspend the transfer by Facebook Ireland of his personal data to Facebook Inc., established in the United States, on the ground that that third country did not ensure an adequate level of protection. Following an investigation into Mr Schrems's claims, the Commissioner brought the matter before the referring court and that court appears, in the light of the evidence adduced and of the competing arguments put by the parties before it, to be unsure whether Mr Schrems's doubts as to the adequacy of the level of protection ensured in that third country are well founded, despite the subsequent findings of the Commission in the Privacy Shield Decision, and that has led that court to refer the 4th, 5th and 10th questions to the Court for a preliminary ruling.

160. As the Advocate General observed in point 175 of his Opinion, those questions must therefore be regarded, in essence, as calling into question the Commission's finding, in the Privacy Shield Decision, that the United States ensures an adequate level of protection of personal data transferred from the European Union to that third country, and, therefore, as calling into question the validity of that decision.

161. In the light of the considerations set out in paragraphs 121 and 157 to 160 above and in order to give the referring court a full answer, it should therefore be examined whether the Privacy Shield Decision complies with the requirements stemming from the GDPR read in the light of the Charter (see, by analogy, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 67).

162. In order for the Commission to adopt an adequacy decision pursuant to Article 45(3) of the GDPR, it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order (see, by analogy, as regards Article 25(6) of Directive 95/46, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 96).

The Privacy Shield Decision

163. The Commission found, in Article 1(1) of the Privacy Shield Decision, that the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the EU-US Privacy Shield, the latter being comprised, inter alia, under Article 1(2) of that decision, of the Principles issued by the US Department of Commerce on 7 July 2016 as set out in Annex II to the decision and the official representations and commitments contained in the documents listed in Annexes I and III to VII to that decision.

164. However, the Privacy Shield Decision also states, in paragraph I.5. of Annex II, under the heading 'EU-U.S. Privacy Shield Framework Principles', that adherence to those principles may be limited, inter alia, 'to the extent necessary to meet national security, public interest, or law enforcement requirements'. Thus, that decision lays down, as did Decision 2000/520, that those requirements have primacy over those principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard the principles without limitation where they conflict with the requirements and therefore prove incompatible with them (see, by analogy, as regards Decision 2000/520, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 86).

165. In the light of its general nature, the derogation set out in paragraph I.5 of Annex II to the Privacy Shield Decision thus enables interference, based on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States (see, by analogy, as regards Decision 2000/520, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 87). More particularly, as noted in the Privacy Shield Decision, such interference can arise from access to, and use of, personal data transferred from the European Union to the United States by US public authorities through the PRISM and UPSTREAM surveillance programmes under Section 702 of the FISA and E.O. 12333.

166. In that context, in recitals 67 to 135 of the Privacy Shield Decision, the Commission assessed the limitations and safeguards available in US law, inter alia under Section 702 of the FISA, E.O. 12333

and PPD-28, as regards access to, and use of, personal data transferred under the EU-US Privacy Shield by US public authorities for national security, law enforcement and other public interest purposes.

167. Following that assessment, the Commission found, in recital 136 of that decision, that ‘the United States ensures an adequate level of protection for personal data transferred from the [European] Union to self-certified organisations in the United States’, and, in recital 140 of the decision, it considered that, ‘on the basis of the available information about the U.S. legal order, ... any interference by U.S. public authorities with the fundamental rights of the persons whose data are transferred from the [European] Union to the United States under the Privacy Shield for national security, law enforcement or other public interest purposes, and the ensuing restrictions imposed on self-certified organisations with respect to their adherence to the Principles, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that there exists effective legal protection against such interference’.

The finding of an adequate level of protection

168. In the light of the factors mentioned by the Commission in the Privacy Shield Decision and the referring court’s findings in the main proceedings, the referring court harbours doubts as to whether US law in fact ensures the adequate level of protection required under Article 45 of the GDPR, read in the light of the fundamental rights guaranteed in Articles 7, 8 and 47 of the Charter. In particular, that court considers that the law of that third country does not provide for the necessary limitations and safeguards with regard to the interferences authorised by its national legislation and does not ensure effective judicial protection against such interferences. As far as concerns effective judicial protection, it adds that the introduction of a Privacy Shield Ombudsperson cannot, in its view, remedy those deficiencies since an ombudsperson cannot be regarded as a tribunal within the meaning of Article 47 of the Charter.

169. As regards, in the first place, Articles 7 and 8 of the Charter, which contribute to the level of protection required within the European Union, compliance with which must be established by the Commission before it adopts an adequacy decision under Article 45(1) of the GDPR, it must be borne in mind that Article 7 of the Charter states that everyone has the right to respect for his or her private and family life, home and communications. Article 8(1) of the Charter expressly confers on everyone the right to the protection of personal data concerning him or her.

170. Thus, access to a natural person’s personal data with a view to its retention or use affects the fundamental right to respect for private life guaranteed in Article 7 of the Charter, which concerns

any information relating to an identified or identifiable individual. Such processing of data also falls within the scope of Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, accordingly, must necessarily satisfy the data protection requirements laid down in that article (see, to that effect, judgments of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, EU:C:2010:662, paragraphs 49 and 52, and of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 29; and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 122 and 123).

171. The Court has held that the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to that data with a view to its use by public authorities, irrespective of whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference (see, to that effect, judgments of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraphs 74 and 75, and of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 33 to 36; and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 124 and 126).

172. However, the rights enshrined in Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society (see, to that effect, judgments of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, EU:C:2010:662, paragraph 48 and the case-law cited, and of 17 October 2013, *Schwarz*, C-291/12, EU:C:2013:670, paragraph 33 and the case-law cited; and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 136).

173. In this connection, it should also be observed that, under Article 8(2) of the Charter, personal data must, *inter alia*, be processed 'for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.

174. Furthermore, in accordance with the first sentence of Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Under the second sentence of Article 52(1) of the Charter, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

175. Following from the previous point, it should be added that the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned (Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 139 and the case-law cited).

176. Lastly, in order to satisfy the requirement of proportionality according to which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary, the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing (see, to that effect, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 140 and 141 and the case-law cited).

177. To that effect, Article 45(2)(a) of the GDPR states that, in its assessment of the adequacy of the level of protection in a third country, the Commission is, in particular, to take account of 'effective and enforceable data subject rights' for data subjects whose personal data are transferred.

178. In the present case, the Commission's finding in the Privacy Shield Decision that the United States ensures an adequate level of protection for personal data essentially equivalent to that guaranteed in the European Union by the GDPR, read in the light of Articles 7 and 8 of the Charter, has been called into question, *inter alia*, on the ground that the interference arising from the surveillance programmes based on Section 702 of the FISA and on E.O. 12333 are not covered by requirements ensuring, subject to the principle of proportionality, a level of protection essentially equivalent to that guaranteed by the second sentence of Article 52(1) of the Charter. It is therefore necessary to examine whether the implementation of those surveillance programmes is subject to such requirements, and it is not necessary to ascertain beforehand whether that third country has complied with conditions essentially equivalent to those laid down in the first sentence of Article 52(1) of the Charter.

179. In that regard, as regards the surveillance programmes based on Section 702 of the FISA, the Commission found, in recital 109 of the Privacy Shield Decision, that, according to that article, 'the FISC does not authorise individual surveillance measures; rather, it authorises surveillance programs

(like PRISM, UPSTREAM) on the basis of annual certifications prepared by the Attorney General and the Director of National Intelligence (DNI)'. As is clear from that recital, the supervisory role of the FISC is thus designed to verify whether those surveillance programmes relate to the objective of acquiring foreign intelligence information, but it does not cover the issue of whether 'individuals are properly targeted to acquire foreign intelligence information'.

180. It is thus apparent that Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes. In those circumstances and as the Advocate General stated, in essence, in points 291, 292 and 297 of his Opinion, that article cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter, as interpreted by the case-law set out in paragraphs 175 and 176 above, according to which a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards.

181. According to the findings in the Privacy Shield Decision, the implementation of the surveillance programmes based on Section 702 of the FISA is, indeed, subject to the requirements of PPD-28. However, although the Commission stated, in recitals 69 and 77 of the Privacy Shield Decision, that such requirements are binding on the US intelligence authorities, the US Government has accepted, in reply to a question put by the Court, that PPD-28 does not grant data subjects actionable rights before the courts against the US authorities. Therefore, the Privacy Shield Decision cannot ensure a level of protection essentially equivalent to that arising from the Charter, contrary to the requirement in Article 45(2)(a) of the GDPR that a finding of equivalence depends, inter alia, on whether data subjects whose personal data are being transferred to the third country in question have effective and enforceable rights.

182. As regards the monitoring programmes based on E.O. 12333, it is clear from the file before the Court that that order does not confer rights which are enforceable against the US authorities in the courts either.

183. It should be added that PPD-28, with which the application of the programmes referred to in the previous two paragraphs must comply, allows for "'bulk" collection ... of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target ... to focus the collection', as stated in a letter

from the Office of the Director of National Intelligence to the United States Department of Commerce and to the International Trade Administration from 21 June 2016, set out in Annex VI to the Privacy Shield Decision. That possibility, which allows, in the context of the surveillance programmes based on E.O. 12333, access to data in transit to the United States without that access being subject to any judicial review, does not, in any event, delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data.

184. It follows therefore that neither Section 702 of the FISA, nor E.O. 12333, read in conjunction with PPD-28, correlates to the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary.

185. In those circumstances, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter.

186. In the second place, as regards Article 47 of the Charter, which also contributes to the required level of protection in the European Union, compliance with which must be determined by the Commission before it adopts an adequacy decision pursuant to Article 45(1) of the GDPR, it should be noted that the first paragraph of Article 47 requires everyone whose rights and freedoms guaranteed by the law of the Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. According to the second paragraph of that article, everyone is entitled to a hearing by an independent and impartial tribunal.

187. According to settled case-law, the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter (judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 95 and the case-law cited).

188. To that effect, Article 45(2)(a) of the GDPR requires the Commission, in its assessment of the adequacy of the level of protection in a third country, to take account, in particular, of 'effective administrative and judicial redress for the data subjects whose personal data are being transferred'.

Recital 104 of the GDPR states, in that regard, that the third country 'should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities', and adds that 'the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress'.

189. The existence of such effective redress in the third country concerned is of particular importance in the context of the transfer of personal data to that third country, since, as is apparent from recital 116 of the GDPR, data subjects may find that the administrative and judicial authorities of the Member States have insufficient powers and means to take effective action in relation to data subjects' complaints based on allegedly unlawful processing, in that third country, of their data thus transferred, which is capable of compelling them to resort to the national authorities and courts of that third country.

190. In the present case, the Commission's finding in the Privacy Shield Decision that the United States ensures a level of protection essentially equivalent to that guaranteed in Article 47 of the Charter has been called into question on the ground, *inter alia*, that the introduction of a Privacy Shield Ombudsperson cannot remedy the deficiencies which the Commission itself found in connection with the judicial protection of persons whose personal data is transferred to that third country.

191. In that regard, the Commission found, in recital 115 of the Privacy Shield Decision, that 'while individuals, including EU data subjects, ... have a number of avenues of redress when they have been the subject of unlawful (electronic) surveillance for national security purposes, it is equally clear that at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered'. Thus, as regards E.O. 12333, the Commission emphasised, in recital 115, the lack of any redress mechanism. In accordance with the case-law set out in paragraph 187 above, the existence of such a lacuna in judicial protection in respect of interferences with intelligence programmes based on that presidential decree makes it impossible to conclude, as the Commission did in the Privacy Shield Decision, that United States law ensures a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter.

192. Furthermore, as regards both the surveillance programmes based on Section 702 of the FISA and those based on E.O. 12333, it has been noted in paragraphs 181 and 182 above that neither PPD-28 nor E.O. 12333 grants data subjects rights actionable in the courts against the US authorities, from which it follows that data subjects have no right to an effective remedy.

193. The Commission found, however, in recitals 115 and 116 of the Privacy Shield Decision, that, as a result of the Ombudsperson Mechanism introduced by the US authorities, as described in a letter

from the US Secretary of State to the European Commissioner for Justice, Consumers and Gender Equality from 7 July 2016, set out in Annex III to that decision, and of the nature of that Ombudsperson's role, in the present instance, a 'Senior Coordinator for International Information Technology Diplomacy', the United States can be deemed to ensure a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter.

194. An examination of whether the ombudsperson mechanism which is the subject of the Privacy Shield Decision is in fact capable of addressing the Commission's finding of limitations on the right to judicial protection must, in accordance with the requirements arising from Article 47 of the Charter and the case-law recalled in paragraph 187 above, start from the premiss that data subjects must have the possibility of bringing legal action before an independent and impartial court in order to have access to their personal data, or to obtain the rectification or erasure of such data.

195. In the letter referred to in paragraph 193 above, the Privacy Shield Ombudsperson, although described as 'independent from the Intelligence Community', was presented as '[reporting] directly to the Secretary of State who will ensure that the Ombudsperson carries out its function objectively and free from improper influence that is liable to have an effect on the response to be provided'. Furthermore, in addition to the fact that, as found by the Commission in recital 116 of that decision, the Ombudsperson is appointed by the Secretary of State and is an integral part of the US State Department, there is, as the Advocate General stated in point 337 of his Opinion, nothing in that decision to indicate that the dismissal or revocation of the appointment of the Ombudsperson is accompanied by any particular guarantees, which is such as to undermine the Ombudsman's independence from the executive (see, to that effect, judgment of 21 January 2020, *Banco de Santander*, C-274/14, EU:C:2020:17, paragraphs 60 and 63 and the case-law cited).

196. Similarly, as the Advocate General stated, in point 338 of his Opinion, although recital 120 of the Privacy Shield Decision refers to a commitment from the US Government that the relevant component of the intelligence services is required to correct any violation of the applicable rules detected by the Privacy Shield Ombudsperson, there is nothing in that decision to indicate that that ombudsperson has the power to adopt decisions that are binding on those intelligence services and does not mention any legal safeguards that would accompany that political commitment on which data subjects could rely.

197. Therefore, the ombudsperson mechanism to which the Privacy Shield Decision refers does not provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter.

198. Therefore, in finding, in Article 1(1) of the Privacy Shield Decision, that the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in that third country under the EU-US Privacy Shield, the Commission disregarded the requirements of Article 45(1) of the GDPR, read in the light of Articles 7, 8 and 47 of the Charter.

199. It follows that Article 1 of the Privacy Shield Decision is incompatible with Article 45(1) of the GDPR, read in the light of Articles 7, 8 and 47 of the Charter, and is therefore invalid.

200. Since Article 1 of the Privacy Shield Decision is inseparable from Articles 2 and 6 of, and the annexes to, that decision, its invalidity affects the validity of the decision in its entirety.

201. In the light of all of the foregoing considerations, it is to be concluded that the Privacy Shield Decision is invalid.

202. As to whether it is appropriate to maintain the effects of that decision for the purposes of avoiding the creation of a legal vacuum (see, to that effect, judgment of 28 April 2016, *Borealis Polyolefine and Others*, C-191/14, C-192/14, C-295/14, C-389/14 and C-391/14 to C-393/14, EU:C:2016:311, paragraph 106), the Court notes that, in any event, in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum. That article details the conditions under which transfers of personal data to third countries may take place in the absence of an adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR.

Costs

203. Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Grand Chamber) hereby rules:

1. Article 2(1) and (2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), must be interpreted as meaning that that regulation applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security.

2. Article 46(1) and Article 46(2)(c) of Regulation 2016/679 must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter of Fundamental Rights of the European Union. To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.

3. Article 58(2)(f) and (j) of Regulation 2016/679 must be interpreted as meaning that, unless there is a valid European Commission adequacy decision, the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of that regulation and by the Charter of Fundamental Rights, cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.

4. Examination of Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EU of the European Parliament and of the Council, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights has disclosed nothing to affect the validity of that decision.

5. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield is invalid.

Lenaerts

Silva de Lapuerta

Arabadjiev

Prechal

Vilaras

Safjan

Rodin

Xuereb

Rossi

Jarukaitis

Ilešič

von Danwitz

Šváby

Delivered in open court in Luxembourg on 16 July 2020.

A. Calot Escobar

K. Lenaerts

Registrar

President

* Language of the case: English.

ABAD - Prokuratuur Case (C-746/18)

Judgment in Case C-746/18

H. K. v Prokuratuur

Access, for purposes in the criminal field, to a set of traffic or location data in respect of electronic communications, allowing precise conclusions to be drawn concerning a person's private life, is permitted only in order to combat serious crime or prevent serious threats to public security

In addition, EU law precludes national legislation that confers upon the public prosecutor's office the power to authorise access of a public authority to such data for the purpose of conducting a criminal investigation

Criminal proceedings were brought in Estonia against H. K. on counts of theft, use of another person's bank card and violence against persons party to court proceedings. A court of first instance convicted H. K. of those offences and imposed a custodial sentence of two years. That judgment was then upheld on appeal.

The reports relied upon in order to find H. K. guilty of those offences were drawn up, inter alia, on the basis of personal data generated in the context of the provision of electronic communications services. The Riigikohus (Supreme Court, Estonia), before which H. K. lodged an appeal on a point of law, expressed doubts as to whether the conditions under which the investigating authority had access to those data were compatible with EU law. ¹

Those doubts concerned, first, whether the length of the period in respect of which the investigating authority has had access to the data is a criterion for assessing the seriousness of the interference, constituted by that access, with the fundamental rights of the persons concerned. Thus, the referring court raised the question whether, where that period is very short or the quantity of data gathered is very limited, the objective of combating crime in general, and not only combating serious crime, is capable of justifying such an interference. Second, the referring court had doubts as to whether it is possible to regard the Estonian public prosecutor's office, in the light of the various duties which are assigned to it by national legislation, as an 'independent' administrative authority, within the meaning of the judgment in *Tele2 Sverige and Watson and Others*, ² that is capable of authorising access of the investigating authority to the data concerned.

By its judgment, delivered by the Grand Chamber, the Court holds that the directive on privacy and electronic communications, read in the light of the Charter, precludes national legislation that permits

public authorities to have access to traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and to allow precise conclusions to be drawn concerning his or her private life, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without such access being confined to procedures and proceedings to combat serious crime or prevent serious threats to public security. According to the Court, the length of the period in respect of which access to those data is sought and the quantity or nature of the data available in respect of such a period are irrelevant in that regard. The Court further holds that that directive, read in the light of the Charter, precludes national legislation that confers upon the public prosecutor's office the power to authorise access of a public authority to traffic and location data for the purpose of conducting a criminal investigation.

Findings of the Court

As regards the circumstances in which access to traffic and location data retained by providers of electronic communications services may, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, be granted to public authorities, pursuant to a measure adopted under the directive on privacy and electronic communications, ³ the Court recalls the content of its ruling in *La Quadrature du Net and Others*. ⁴ Thus, that directive authorises the Member States to adopt, for those purposes amongst others, legislative measures to restrict the scope of the rights and obligations provided for by the directive, inter alia the obligation to ensure the confidentiality of communications and traffic data, ⁵ only if the general principles of EU law – which include the principle of proportionality – and the fundamental rights guaranteed by the Charter ⁶ are observed. Within that framework, the directive precludes legislative measures which impose on providers of electronic communications services, as a preventive measure, an obligation requiring the general and indiscriminate retention of traffic and location data.

So far as concerns the objective of preventing, investigating, detecting and prosecuting criminal offences, which is pursued by the legislation at issue, in accordance with the principle of proportionality the Court holds that only the objectives of combating serious crime or preventing serious threats to public security are capable of justifying public authorities having access to a set of traffic or location data, that are liable to allow precise conclusions to be drawn concerning the private lives of the persons concerned, and other factors relating to the proportionality of a request for access, such as the length of the period in respect of which access to such data is sought, cannot have the

effect that the objective of preventing, investigating, detecting and prosecuting criminal offences in general is capable of justifying such access.

As regards the power conferred upon the public prosecutor's office to authorise access of a public authority to traffic and location data for the purpose of conducting a criminal investigation, the Court points out that it is for national law to determine the conditions under which providers of electronic communications services must grant the competent national authorities access to the data in their possession. However, in order to satisfy the requirement of proportionality, such legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and must indicate in what circumstances and under which substantive and procedural conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary.

According to the Court, in order to ensure, in practice, that those conditions are fully observed, it is essential that access of the competent national authorities to retained data be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body be made following a reasoned request by those authorities submitted, *inter alia*, within the framework of procedures for the prevention, detection or prosecution of crime. In cases of duly justified urgency, the review must take place within a short time.

In that regard, the Court states that one of the requirements for the prior review is that the court or body entrusted with carrying it out must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue. As regards a criminal investigation in particular, it is a requirement of such a review that that court or body must be able to strike a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access. Where that review is carried out not by a court but by an independent administrative body, that body must have a status enabling it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence.

According to the Court, it follows that the requirement of independence that has to be satisfied by the authority entrusted with carrying out the prior review means that that authority must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry

out the review objectively and impartially and free from any external influence. In particular, in the criminal field the requirement of independence entails that the authority entrusted with the prior review, first, must not be involved in the conduct of the criminal investigation in question and, second, has a neutral stance vis-à-vis the parties to the criminal proceedings. That is not so in the case of a public prosecutor's office which, like the Estonian public prosecutor's office, directs the investigation procedure and, where appropriate, brings the public prosecution. It follows that the public prosecutor's office is not in a position to carry out the prior review.

[1] To be more precise, with Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) ('the directive on privacy and electronic communications'), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union ('the Charter').

[2] Judgment of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15 paragraph 120; see also Press Release No 145/16.

[3] Article 15(1) of the directive on privacy and electronic communications.

[4] Judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, paragraphs 166 to 169; see also Press Release No 123/20.

[5] Article 5(1) of the directive on privacy and electronic communications.

[6] In particular, Articles 7, 8 and 11 and Article 52(1) of the Charter.

JUDGMENT OF THE COURT (Grand Chamber)

2 March 2021 (*)

(Reference for a preliminary ruling - Processing of personal data in the electronic communications sector - Directive 2002/58/EC - Providers of electronic communications services - Confidentiality of the communications - Limitations - Article 15(1) - Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union - Legislation providing for the general and indiscriminate retention of traffic and location data by providers of electronic communications services - Access of national authorities to retained data for the purpose of investigations - Combating of crime in general - Authorisation given by the public prosecutor's office - Use of data in criminal proceedings as evidence - Admissibility)

In Case C-746/18,

REQUEST for a preliminary ruling under Article 267 TFEU from the Riigikohus (Supreme Court, Estonia), made by decision of 12 November 2018, received at the Court on 29 November 2018, in criminal proceedings against

H. K.,

other party:

Prokuratuur,

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, R. Silva de Lapuerta, Vice-President, J.-C. Bonichot, A. Arabadjiev, A. Prechal and L. Bay Larsen, Presidents of Chambers, T. von Danwitz (Rapporteur), M. Safjan, K. Jürimäe, C. Lycourgos and P.G. Xuereb, Judges,

Advocate General: G. Pitruzzella,

Registrar: C. Strömholm, Administrator,

having regard to the written procedure and further to the hearing on 15 October 2019,

after considering the observations submitted on behalf of:

- H. K., by S. Reinsaar, vandeadvokaat,

- the Prokuratuur, by T. Pern and M. Voogma, acting as Agents,

- the Estonian Government, by N. Grünberg, acting as Agent,
 - the Danish Government, by J. Nymann-Lindgren and M.S. Wolff, acting as Agents,
 - Ireland, by M. Brown, G. Hodge, J. Quaney and A. Joyce, acting as Agents, and D. Fennelly, Barrister-at-Law,
 - the French Government, initially by D. Dubois, D. Colas, E. de Moustier and A.-L. Desjonquères, and subsequently by D. Dubois, E. de Moustier and A.-L. Desjonquères, acting as Agents,
 - the Latvian Government, initially by V. Kalniņa and I. Kucina, and subsequently by V. Soņeca and V. Kalniņa, acting as Agents,
 - the Hungarian Government, by M.Z. Fehér and A. Pokoraczki, acting as Agents,
 - the Polish Government, by B. Majczyna, acting as Agent,
 - the Portuguese Government, by L. Inez Fernandes, P. Barros da Costa, L. Medeiros and I. Oliveira, acting as Agents,
 - the Finnish Government, by J. Heliskoski, acting as Agent,
 - the United Kingdom Government, by S. Brandon and Z. Lavery, acting as Agents, G. Facenna QC and C. Knight, Barrister,
 - the European Commission, initially by H. Kranenborg, M. Wasmeier, P. Costa de Oliveira and K. Toomus, and subsequently by H. Kranenborg, M. Wasmeier and E. Randvere, acting as Agents,
- after hearing the Opinion of the Advocate General at the sitting on 21 January 2020,
- gives the following

Judgment

1. This request for a preliminary ruling concerns the interpretation of Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) ('Directive 2002/58'), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union ('the Charter').

2. The request has been made in the context of criminal proceedings brought against H. K. on counts of theft, use of another person's bank card and violence against persons party to court proceedings.

Legal context

EU law

3. Recitals 2 and 11 of Directive 2002/58 state:

'(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the [Charter]. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of [the] Charter.

...

(11) Like Directive 95/46/EC [of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by [EU] law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, [signed in Rome on 4 November 1950,] as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.'

4. Article 2 of Directive 2002/58, headed 'Definitions', provides:

'Save as otherwise provided, the definitions in Directive [95/46] and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [(OJ 2002 L 108, p. 33)] shall apply.

The following definitions shall also apply:

(a) “user” means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;

(b) “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

(c) “location data” means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

(d) “communication” means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

...'

5. As set out in Article 5 of Directive 2002/58, headed ‘Confidentiality of the communications’:

‘1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

...

3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive [95/46], inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.’

6. Article 6 of Directive 2002/58, headed 'Traffic data', provides:

'1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

...

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

...'

7. Article 9 of Directive 2002/58, headed 'Location data other than traffic data', provides in paragraph 1:

'Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. ...'

8. Article 15 of Directive 2002/58, headed 'Application of certain provisions of Directive [95/46]', states in paragraph 1:

'Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive [95/46]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of [EU] law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.'

Estonian law

The Law on electronic communications

9. Paragraph 1111 of the elektroonilise side seadus (Law on electronic communications, RT I 2004, 87, 593; RT I, 22.05.2018, 3), in the version applicable at the material time ('the Law on electronic communications'), a provision which is headed 'Obligation to retain data', states:

'...

(2) Providers of telephone and mobile telephone services and of telephone network and mobile telephone network services are obliged to retain the following data:

- 1) the number of the calling party and the name and address of the subscriber;
- 2) the number of the called party and the name and address of the subscriber;
- 3) when use is made of an additional service, including call forwarding or call transfer, the number dialled and the name and address of the subscriber;
- 4) the date and time of the start and end of the call;
- 5) the telephone or mobile telephone service used;
- 6) the International Mobile Subscriber Identity (IMSI) of the calling and called party;
- 7) the International Mobile Equipment Identity (IMEI) of the calling and called party;
- 8) the cell ID at the start of the call;

9) data on the geographical location of the base station by reference to its cell ID during the period for which data are retained;

10) in the case of pre-paid anonymous mobile telephone services, the date and time of the initial activation of the service and the cell ID from which the service was activated.

...

(4) The data referred to in subparagraphs 2 and 3 of this paragraph shall be retained for one year from the time of the communication if those data were generated or processed in the course of providing a communications service. ...

...

(11) The data referred to in subparagraphs 2 and 3 of this paragraph shall be forwarded:

1) in accordance with the kriminaalmenetluse seadustik (Code of Criminal Procedure), to an investigating authority, a surveillance authority, the public prosecutor's office and the court;

...'

The Code of Criminal Procedure

10. Paragraph 17 of the Code of Criminal Procedure (kriminaalmenetluse seadustik, RT I 2003, 27, 166; RT I, 31.05.2018, 22) provides:

(1) The parties to court proceedings are the public prosecutor's office ...

...'

11. Paragraph 30 of that code is worded as follows:

'(1) The public prosecutor's office shall direct the pre-trial procedure, guaranteeing its lawfulness and effectiveness, and represent the public prosecution before the court.

(2) The powers of the public prosecutor's office in criminal proceedings shall be exercised in the name of the public prosecutor's office by a public prosecutor who acts independently and is only bound by the law.'

12. Paragraph 901 of the code provides:

'...

(2) The investigating authority may, in the pre-trial procedure with the authorisation of the public prosecutor's office or in judicial proceedings with the authorisation of the court, ask an electronic

communications undertaking for the data listed in Paragraph 1111(2) and (3) of the Law on electronic communications which is not specified in subparagraph 1 of the present paragraph. The authorisation of the request shall note the period for which the data request is allowed with precise date indications.

(3) A request may be made pursuant to this paragraph only where this is essential for achieving the objective of the criminal proceedings.'

13. Paragraph 211 of the code states:

'(1) The objective of the pre-trial procedure is to gather evidence and create the other conditions for judicial proceedings.

(2) In the pre-trial procedure, the investigating authority and the public prosecutor's office shall ascertain the circumstances exonerating and incriminating the suspect or accused.'

The Law on the public prosecutor's office

14. Paragraph 1 of the prokuratuuriseadus (Law on the public prosecutor's office, RT I 1998, 41, 625; RT I, 06.07.2018, 20), in the version applicable at the material time, provides:

'(1) The public prosecutor's office is a government authority falling under the jurisdiction of the Ministry of Justice which participates in planning the monitoring activities necessary for fighting and investigating criminal offences, directs the pre-trial procedure, guaranteeing its lawfulness and effectiveness, represents the public prosecution before the court, and performs other duties assigned to the prosecutor's office by law.

(11) The public prosecutor's office shall perform its statutory duties independently and act in accordance with the present law, other laws and legislation adopted on the basis of those laws.

...'

15. Paragraph 2(2) of that law states:

'The public prosecutor shall perform his or her duties independently and act exclusively according to the law and his or her convictions.'

The dispute in the main proceedings and the questions referred for a preliminary ruling

16. By judgment of 6 April 2017, the Viru Maakohus (Court of First Instance, Viru, Estonia) imposed on H. K. a custodial sentence of two years for having committed, between 17 January 2015 and 1 February 2016, a number of thefts of goods (of a value ranging from EUR 3 to EUR 40) and cash (in amounts between EUR 5.20 and EUR 2 100), used another person's bank card, causing that person a

loss of EUR 3 941.82, and performed acts of violence against persons party to court proceedings concerning her.

17. In order to find H. K. guilty of those acts, the Viru Maakohus (Court of First Instance, Viru) relied, *inter alia*, on several reports which were drawn up on the basis of data relating to electronic communications, as referred to in Paragraph 1111(2) of the Law on electronic communications, that the investigating authority had obtained in the pre-trial procedure from a provider of electronic telecommunications services, after having been granted several authorisations for that purpose by the Viru Ringkonnaprokuratuur (Viru District Public Prosecutor's Office, Estonia) in accordance with Paragraph 901 of the Code of Criminal Procedure. Those authorisations, granted on 28 January and 2 February 2015, 2 November 2015 and 25 February 2016, related to data concerning several telephone numbers of H. K. and various IMEI codes of hers, in respect of the period from 1 January to 2 February 2015, of 21 September 2015, and of the period from 1 March 2015 to 19 February 2016.

18. H. K. brought an appeal against the judgment of the Viru Maakohus (Court of First Instance, Viru) before the Tartu Ringkonnakohus (Court of Appeal, Tartu, Estonia), which dismissed the appeal by judgment of 17 November 2017.

19. H. K. lodged an appeal on a point of law against the latter judgment before the Riigikohus (Supreme Court, Estonia), contesting, *inter alia*, the admissibility of the reports drawn up on the basis of the data obtained from the provider of electronic communications services. In her submission, it follows from the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, 'Tele2', EU:C:2016:970), that the provisions of Paragraph 1111 of the Law on electronic communications which lay down the obligation on service providers to retain communications data, as well as the use of such data for the purpose of her conviction, are contrary to Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.

20. According to the referring court, the question arises whether the reports drawn up on the basis of data referred to in Paragraph 1111(2) of the Law on electronic communications may be regarded as constituting admissible evidence. That court observes that the admissibility of the reports at issue in the main proceedings as evidence depends on the question of the extent to which the gathering of the data on the basis of which those reports were drawn up was in conformity with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.

21. The referring court considers that, in order to answer that question, it needs to be determined whether Article 15(1) of Directive 2002/58, read in the light of the Charter, must be interpreted as meaning that the access of State authorities to data making it possible to identify the source and

destination of a telephone communication from a suspect's landline or mobile telephone, to determine the date, time, duration and type of that communication, to identify the communications equipment used and to establish the location of the mobile communication equipment used amounts to interference with the fundamental rights at issue which is so serious that such access should be restricted to combating serious crime, regardless of the period in respect of which the State authorities have sought access to the retained data.

22. The referring court takes the view, however, that the length of that period is an essential factor for assessing the seriousness of the interference represented by access to traffic and location data. Thus, where that period is very short or the quantity of data gathered is very limited, the question should be raised whether the objective of combating crime in general, and not only combating serious crime, is capable of justifying such an interference.

23. Finally, the referring court has doubts as to whether it is possible to regard the Estonian public prosecutor's office as an independent administrative authority, for the purposes of paragraph 120 of the judgment of 21 December 2016, *Tele2* (C-203/15 and C-698/15, EU:C:2016:970), which is capable of authorising access of the investigating authority to data relating to electronic communications such as the data referred to in Paragraph 1111(2) of the Law on electronic communications.

24. The referring court states that the public prosecutor's office directs the pre-trial procedure, while guaranteeing its lawfulness and effectiveness. Since the objective of that procedure is, *inter alia*, to gather evidence, the investigating authority and the public prosecutor's office verify the circumstances incriminating and exonerating any suspect or person accused. If the public prosecutor's office is satisfied that all the necessary evidence has been gathered, it brings the public prosecution against the accused. The powers of the public prosecutor's office are exercised in its name by a public prosecutor who carries out his or her duties independently, as follows from Paragraph 30(1) and (2) of the Code of Criminal Procedure and Paragraphs 1 and 2 of the Law on the public prosecutor's office.

25. In that context, the referring court observes that its doubts as to the independence required by EU law are principally attributable to the fact that the public prosecutor's office not only directs the pre-trial procedure, but also represents the public prosecution at the trial, that authority being, pursuant to national law, party to the criminal proceedings.

26. It was in those circumstances that the *Riigikohus* (Supreme Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'(1) Is Article 15(1) of Directive [2002/58], in conjunction with Articles 7, 8, 11 and 52(1) of the [Charter], to be interpreted as meaning that in criminal proceedings the access of State authorities to data making it possible to establish the source and destination, the date, the time, the duration and the type of the communication, the terminal used and the location of the mobile terminal used, in relation to a telephone or mobile telephone communication of a suspect, constitutes so serious an interference with the fundamental rights enshrined in those articles of the Charter that that access in the area of prevention, investigation, detection and prosecution of criminal offences must be restricted to the fighting of serious crime, regardless of the period to which the retained data to which the State authorities have access relate?

(2) Is Article 15(1) of Directive [2002/58], on the basis of the principle of proportionality expressed in the judgment of [2 October 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788)], paragraphs 55 to 57, to be interpreted as meaning that, if the amount of data mentioned in the first question, to which the State authorities have access, is not large (both in terms of the type of data and in terms of its temporal extent), the associated interference with fundamental rights is justified by the objective of prevention, investigation, detection and prosecution of criminal offences generally, and that the greater the amount of data to which the State authorities have access, the more serious the criminal offences which are intended to be fought by the interference must be?

(3) Does the requirement mentioned in the judgment of [21 December 2016, Tele2 (C-203/15 and C-698/15, EU:C:2016:970)], second point of the operative part, that the data access of the competent State authorities must be subject to prior review by a court or an independent administrative authority mean that Article 15(1) of Directive [2002/58] must be interpreted as meaning that the public prosecutor's office which directs the pre-trial procedure, with it being obliged by law to act independently and only being bound by the law, and ascertains the circumstances both incriminating and exonerating the accused in the pre-trial procedure, but later represents the public prosecution in the judicial proceedings, may be regarded as an independent administrative authority?'

Consideration of the questions referred

The first and second questions

27. By its first and second questions, which it is appropriate to examine together, the referring court asks, in essence, whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that permits public authorities to have access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding

the location of the terminal equipment which he or she uses and to allow precise conclusions to be drawn concerning his or her private life, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without such access being confined to procedures and proceedings to combat serious crime, regardless of the length of the period in respect of which access to those data is sought and the quantity and the nature of the data available in respect of such a period.

28. It is apparent from the request for a preliminary ruling that, as the Estonian Government confirmed at the hearing, the data to which the national investigating authority had access in the main proceedings is the data kept under Paragraph 1111(2) and (4) of the Law on electronic communications, which obliges providers of electronic communications services to retain, generally and indiscriminately, for one year traffic and location data so far as concerns fixed and mobile telephony. Those data make it possible, in particular, to trace and identify the source and destination of a communication from a person's landline or mobile telephone, to determine the date, time, duration and type of that communication, to identify the communications equipment used, and to establish the location of the mobile telephone without a communication necessarily being conveyed. In addition, they enable the frequency of a user's communications with certain persons over a given period of time to be established. Furthermore, as the Estonian Government confirmed at the hearing, access to those data may, in relation to combating crime, be sought in respect of any type of criminal offence.

29. As regards the circumstances in which access to traffic and location data retained by providers of electronic communications services may, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, be granted to public authorities, pursuant to a measure adopted under Article 15(1) of Directive 2002/58, the Court has held that such access may be granted only in so far as those data have been retained by a provider in a manner that is consistent with Article 15(1) (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 167).

30. In this connection, the Court has also held that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, precludes legislative measures which, for such purposes, provide, as a preventive measure, for the general and indiscriminate retention of traffic and location data (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 168).

31. As to the objectives capable of justifying public authorities having access to data retained by providers of electronic communications services pursuant to a measure consistent with those

provisions, it is apparent, first, from the Court's case-law that such access may be justified only by the public interest objective for which those service providers were ordered to retain the data (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 166).

32. Second, the Court has held that the question whether the Member States may justify a limitation on the rights and obligations laid down, *inter alia*, in Articles 5, 6 and 9 of Directive 2002/58 must be assessed by measuring the seriousness of the interference entailed by such a limitation and by verifying that the importance of the public interest objective pursued by that limitation is proportionate to the seriousness of the interference (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 131 and the case-law cited).

33. So far as concerns the objective of preventing, investigating, detecting and prosecuting criminal offences, which is pursued by the legislation at issue in the main proceedings, in accordance with the principle of proportionality only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, such as the interference entailed by the retention of traffic and location data, whether the retention be general and indiscriminate or targeted. Accordingly, only non-serious interference with those fundamental rights may be justified by the objective, pursued by the legislation at issue in the main proceedings, of preventing, investigating, detecting and prosecuting criminal offences in general (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 140 and 146).

34. In that regard, it has *inter alia* been held that legislative measures concerning the processing of data in themselves relating to the civil identity of users of electronic communications systems, including the retention of and access to those data, solely for the purpose of identifying the user concerned, and without it being possible for those data to be associated with information on the communications made, are capable of being justified by the objective of preventing, investigating, detecting and prosecuting criminal offences in general, to which the first sentence of Article 15(1) of Directive 2002/58 refers. Those data do not, in themselves, make it possible to ascertain the date, time, duration and recipients of the communications made, or the locations where those communications took place or their frequency with specific people during a given period, with the result that they do not provide, apart from the contact details of users of means of electronic communication, such as

their addresses, any information on the communications sent and, consequently, on the users' private lives. Thus, the interference entailed by a measure relating to those data cannot, in principle, be classified as serious (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 157 and 158 and the case-law cited).

35. Accordingly, only the objectives of combating serious crime or preventing serious threats to public security are capable of justifying public authorities having access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and that allow precise conclusions to be drawn concerning the private lives of the persons concerned (see, to that effect, judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, paragraph 54), and other factors relating to the proportionality of a request for access, such as the length of the period in respect of which access to such data is sought, cannot have the effect that the objective of preventing, investigating, detecting and prosecuting criminal offences in general is capable of justifying such access.

36. Access to a set of traffic or location data, such as the data retained pursuant to Paragraph 1111 of the Law on electronic communications, is indeed liable to allow precise, or even very precise, conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 117).

37. It is true that, as the referring court suggests, the longer that the period is in respect of which access is sought, the greater, in principle, is the quantity of data liable to be retained by providers of electronic communications services, regarding the electronic communications sent, the places of residence stayed in and the movements made by the user of a means of electronic communication, thus allowing a greater number of conclusions concerning that user's private life to be drawn from the data consulted. A similar finding may be made so far as concerns the categories of data sought.

38. It is, therefore, for the purpose of satisfying the requirement of proportionality, under which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 130 and the case-law cited), that it is for the competent national authorities to ensure, in each individual case, that both the category or categories of data

covered and the period in respect of which access to those data is sought are, on the basis of the circumstances of the case, limited to what is strictly necessary for the purposes of the investigation in question.

39. However, the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter that is entailed by a public authority's access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses, is in any event serious regardless of the length of the period in respect of which access to those data is sought and the quantity or nature of the data available in respect of such a period, when, as in the main proceedings, that set of data is liable to allow precise conclusions to be drawn concerning the private life of the person or persons concerned.

40. Even access to a limited quantity of traffic or location data or access to data in respect of a short period may be liable to provide precise information on the private life of a user of a means of electronic communication. Furthermore, the quantity of the data available and the specific information on the private life of the person concerned that results from the data are matters that can be assessed only after the data have been consulted. However, authorisation of access, granted by the court having jurisdiction or the competent independent authority, necessarily occurs before the data and the information resulting therefrom can be consulted. Thus, the assessment of the seriousness of the interference that the access constitutes is necessarily carried out on the basis of the risk generally pertaining to the category of data sought for the private lives of the persons concerned, without it indeed mattering whether or not the resulting information relating to the person's private life is in actual fact sensitive.

41. Finally, given the fact that the referring court has before it a claim that the reports drawn up on the basis of the traffic and location data are inadmissible, on the ground that Paragraph 1111 of the Law on electronic communications is contrary to Article 15(1) of Directive 2002/58 as regards both retention of and access to data, it should be noted that, as EU law currently stands, it is, in principle, for national law alone to determine the rules relating to the admissibility and assessment, in criminal proceedings against persons suspected of having committed criminal offences, of information and evidence obtained by general and indiscriminate retention of such data contrary to EU law (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 222) or by access of the national authorities thereto contrary to EU law.

42. The Court has consistently held that, in the absence of EU rules on the matter, it is for the national legal order of each Member State, in accordance with the principle of procedural autonomy, to establish procedural rules for actions intended to safeguard the rights that individuals derive from EU law, provided, however, that those rules are no less favourable than the rules governing similar situations subject to domestic law (the principle of equivalence) and do not render impossible in practice or excessively difficult the exercise of rights conferred by EU law (the principle of effectiveness) (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 223 and the case-law cited).

43. As regards the principle of effectiveness in particular, it should be noted that the objective of national rules on the admissibility and use of information and evidence is, in accordance with the choices made by national law, to prevent information and evidence obtained unlawfully from unduly prejudicing a person who is suspected of having committed criminal offences. That objective may be achieved under national law not only by prohibiting the use of such information and evidence, but also by means of national rules and practices governing the assessment and weighting of such material, or by factoring in whether that material is unlawful when determining the sentence (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 225).

44. In deciding whether to exclude information and evidence obtained in contravention of the requirements of EU law, regard must be had, in particular, to the risk of breach of the adversarial principle and, therefore, of the right to a fair trial entailed by the admissibility of such information and evidence. If a court takes the view that a party is not in a position to comment effectively on evidence pertaining to a field of which the judges have no knowledge and that is likely to have a preponderant influence on the findings of fact, it must find an infringement of the right to a fair trial and exclude that evidence in order to avoid such an infringement. Therefore, the principle of effectiveness requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law or by means of access of the competent authority thereto in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 226 and 227).

45. In the light of the foregoing considerations, the answer to the first and second questions is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that permits public authorities to have access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and to allow precise conclusions to be drawn concerning his or her private life, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without such access being confined to procedures and proceedings to combat serious crime or prevent serious threats to public security, and that is so regardless of the length of the period in respect of which access to those data is sought and the quantity or nature of the data available in respect of such a period.

The third question

46. By its third question, the referring court asks, in essence, whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that confers upon the public prosecutor's office, whose task is to direct the criminal pre-trial procedure and to bring, where appropriate, the public prosecution in subsequent proceedings, the power to authorise access of a public authority to traffic and location data for the purposes of a criminal investigation.

47. The referring court explains in this connection that, whilst the Estonian public prosecutor's office is, under national law, obliged to act independently, is subject only to the law and must examine the incriminating and exculpatory evidence in the pre-trial procedure, the objective of that procedure nevertheless remains the gathering of evidence and fulfilment of the other conditions necessary for judicial proceedings. It states that it is that authority which represents the public prosecution at the trial and it is therefore also party to the proceedings. Furthermore, it is apparent from the documents before the Court that, as the Estonian Government and the Prokuratuur also confirmed at the hearing, the Estonian public prosecutor's office is organised hierarchically and that requests for access to traffic and location data are not subject to particular formal requirements and may be made by the public prosecutor him or herself. Finally, the persons to whose data access may be granted are not only those suspected of involvement in a criminal offence.

48. It is true that, as the Court has already held, it is for national law to determine the conditions under which providers of electronic communications services must grant the competent national authorities access to the data in their possession. However, in order to satisfy the requirement of proportionality,

such legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary (see, to that effect, judgments of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 117 and 118; of 6 October 2020, *Privacy International*, C-623/17, EU:C:2020:790, paragraph 68; and of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 132 and the case-law cited).

49. In particular, national legislation governing the access of the competent authorities to retained traffic and location data, adopted pursuant to Article 15(1) of Directive 2002/58, cannot be limited to requiring that the authorities' access to the data be consistent with the objective pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use (judgments of 6 October 2020, *Privacy International*, C-623/17, EU:C:2020:790, paragraph 77, and of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 176 and the case-law cited).

50. Accordingly, and since general access to all retained data, regardless of whether there is any, at least indirect, link with the intended purpose, cannot be regarded as being limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data in question. In that regard, such access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities (see, to that effect, judgments of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 119, and of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 188).

51. In order to ensure, in practice, that those conditions are fully observed, it is essential that access of the competent national authorities to retained data be subject to a prior review carried out either by a

court or by an independent administrative body, and that the decision of that court or body be made following a reasoned request by those authorities submitted, *inter alia*, within the framework of procedures for the prevention, detection or prosecution of crime. In cases of duly justified urgency, the review must take place within a short time (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 189 and the case-law cited).

52. As the Advocate General has observed, in essence, in point 105 of his Opinion, one of the requirements for that prior review is that the court or body entrusted with carrying it out must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue. As regards a criminal investigation in particular, it is a requirement of such a review that that court or body must be able to strike a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access.

53. Where that review is carried out not by a court but by an independent administrative body, that body must have a status enabling it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence (see, to that effect, judgment of 9 March 2010, *Commission v Germany*, C-518/07, EU:C:2010:125, paragraph 25, and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 229 and 230).

54. It follows from the foregoing considerations that the requirement of independence that has to be satisfied by the authority entrusted with carrying out the prior review referred to in paragraph 51 of the present judgment means that that authority must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review objectively and impartially and free from any external influence. In particular, in the criminal field, as the Advocate General has observed, in essence, in point 126 of his Opinion, the requirement of independence entails that the authority entrusted with the prior review, first, must not be involved in the conduct of the criminal investigation in question and, second, has a neutral stance *vis-à-vis* the parties to the criminal proceedings.

55. That is not so in the case of a public prosecutor's office which directs the investigation procedure and, where appropriate, brings the public prosecution. The public prosecutor's office has the task not of ruling on a case in complete independence but, acting as prosecutor in the proceedings, of putting it, where appropriate, before the court that has jurisdiction.

56. The fact that the public prosecutor's office may, in accordance with the rules governing its powers and status, be required to verify the incriminating and exculpatory evidence, to guarantee the lawfulness of the pre-trial procedure and to act exclusively according to the law and the prosecutor's convictions cannot be sufficient to confer upon it the status of a third party in relation to the interests at issue as referred to in paragraph 52 of the present judgment.

57. It follows that the public prosecutor's office is not in a position to carry out the prior review referred to in paragraph 51 of the present judgment.

58. Since the referring court has raised, furthermore, the issue whether the lack of a review by an independent authority may be made up for by a subsequent review carried out by a court as to whether a national authority's access to traffic and location data was lawful, it must be pointed out that, as required by the case-law recalled in paragraph 51 of the present judgment, the independent review must take place before any access, except in the event of duly justified urgency, in which case the review must take place within a short time. As the Advocate General has stated in point 128 of his Opinion, such subsequent review would not enable the objective of a prior review, consisting in preventing the authorisation of access to the data in question that exceeds what is strictly necessary, to be met.

59. Accordingly, the answer to the third question referred for a preliminary ruling is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that confers upon the public prosecutor's office, whose task is to direct the criminal pre-trial procedure and to bring, where appropriate, the public prosecution in subsequent proceedings, the power to authorise access of a public authority to traffic and location data for the purposes of a criminal investigation.

Costs

60. Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Grand Chamber) hereby rules:

1. Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in

the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation that permits public authorities to have access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and to allow precise conclusions to be drawn concerning his or her private life, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without such access being confined to procedures and proceedings to combat serious crime or prevent serious threats to public security, and that is so regardless of the length of the period in respect of which access to those data is sought and the quantity or nature of the data available in respect of such a period.

2. Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation that confers upon the public prosecutor's office, whose task is to direct the criminal pre-trial procedure and to bring, where appropriate, the public prosecution in subsequent proceedings, the power to authorise access of a public authority to traffic and location data for the purposes of a criminal investigation.

[Signatures]

ABAD - G.D. v The Commissioner of the Garda Síochána Case (C-140/20)

JUDGMENT OF THE COURT (Grand Chamber)

5 April 2022 (*)

(Reference for a preliminary ruling - Processing of personal data in the electronic communications sector - Confidentiality of the communications - Providers of electronic communications services - General and indiscriminate retention of traffic and location data - Access to retained data - Subsequent court supervision - Directive 2002/58/EC - Article 15(1) - Charter of Fundamental Rights of the European Union - Articles 7, 8 and 11 and Article 52(1) - Possibility for a national court to restrict the temporal effect of a declaration of the invalidity of national legislation that is incompatible with EU law - Excluded)

In Case C-140/20,

REQUEST for a preliminary ruling under Article 267 TFEU from the Supreme Court (Ireland), made by decision of 25 March 2020, received at the Court on 4 August 2016, in the proceedings

G.D.

v

Commissioner of An Garda Síochána,

Minister for Communications, Energy and Natural Resources,

Attorney General,

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, A. Arabadjiev, A. Prechal, S. Rodin, I. Jarukaitis and N. Jääskinen, Presidents of Chambers, T. von Danwitz (Rapporteur), M. Safjan, F. Biltgen, P.G. Xuereb, N. Piçarra, L.S. Rossi and A. Kumin, Judges,

Advocate General: M. Campos Sánchez-Bordona,

Registrar: D. Dittert, Head of Unit,

having regard to the written procedure and further to the hearing on 13 September 2021,

after considering the observations submitted on behalf of:

- G.D., by J. Dunphy, Solicitor, R. Kennedy, Senior Counsel, and R. Farrell, Senior Counsel, and K. McCormack, Barrister-at-Law,
- the Commissioner of An Garda Síochána, the Minister for Communications, Energy and Natural Resources and the Attorney General, by M. Browne, S. Purcell, C. Stone and J. Quaney and by A. Joyce, acting as Agents, and by S. Guerin, Senior Counsel, and P. Gallagher, Senior Counsel, D. Fennelly and L. Dwyer, Barristers-at-Law,
- the Belgian Government, by P. Cottin and J.-C. Halleux, acting as Agents, and by J. Vanpraet, advocaat,
- the Czech Government, by M. Smolek, O. Serdula and J. Vláčil, acting as Agents,
- the Danish Government, initially by J. Nymann-Lindegren, M. Jespersen and M. Wolff, and subsequently by M. Wolff and V. Jørgensen, acting as Agents,
- the Estonian Government, by A. Kalbus and M. Kriisa, acting as Agents,
- the Spanish Government, by L. Aguilera Ruiz, acting as Agent,
- the French Government, by E. de Moustier and A. Daniel and by D. Dubois, T. Stéhelin and J. Illouz, acting as Agents,
- the Cypriot Government, by I. Neophytou, acting as Agent,
- the Netherlands Government, by C.S. Schillemans, M.K. Bulterman and A. Hanje, acting as Agents,
- the Polish Government, by B. Majczyna and J. Sawicka, acting as Agents,
- the Portuguese Government, by L. Inez Fernandes and by P. Barros da Costa and I. Oliveira, acting as Agents,
- the Finnish Government, by M. Pere and A. Laine, acting as Agents,
- the Swedish Government, by O. Simonsson and J. Lundberg and by H. Shev, C. Meyer-Seitz, A. Runeskjöld, M. Salborn Hodgson, R. Shahsavan Eriksson and H. Eklinder, acting as Agents,
- the European Commission, by S.L. Kalèda, H. Kranenborg, M. Wasmeier and F. Wilman, acting as Agents,
- the European Data Protection Supervisor, by D. Nardi, N. Stolič and K. Ujazdowski and by A. Buchta, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 18 November 2021,

gives the following

Judgment

1. This request for a preliminary ruling concerns the interpretation of Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) ('Directive 2002/58'), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union ('the Charter').

2. The request has been made in proceedings between G.D. and the Commissioner of An Garda Síochána (Commissioner of the national police force, Ireland), the Minister for Communications, Energy and Natural Resources (Ireland) and the Attorney General, concerning the validity of the Communications (Retention of Data) Act 2011 ('the 2011 Act').

Legal context

European Union law

3. Recitals 2, 6, 7 and 11 of Directive 2002/58 state:

'(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by [the Charter]. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of [the Charter].

...

(6) The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.

(7) In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.

...

(11) Like Directive 95/46/EC [of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)], this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by [EU] law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms[, signed in Rome on 4 November 1950], as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.'

4. Article 1 of Directive 2002/58, headed 'Scope and aim', provides:

'1. This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the [European Union].

2. The provisions of this Directive particularise and complement Directive [95/46] for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of [the TFEU], such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.'

5. Article 2 of Directive 2002/58, headed 'Definitions', provides:

'Save as otherwise provided, the definitions in Directive [95/46] and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for

electronic communications networks and services (Framework Directive) [(OJ 2002 L 108, p. 33)] shall apply.

The following definitions shall also apply:

(a) “user” means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;

(b) “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

(c) “location data” means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

(d) “communication” means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

...'

6. Article 3 of Directive 2002/58, headed ‘Services concerned’, provides:

‘This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the [European Union], including public communications networks supporting data collection and identification devices.’

7. Article 5 of the directive, headed ‘Confidentiality of the communications’, provides:

‘1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.’

...

3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive [95/46], inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.'

8. Article 6 of Directive 2002/58, entitled 'Traffic data', provides:

'1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

...

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

...'

9. Article 9 of that directive, entitled 'Location data other than traffic data', provides, in paragraph 1 thereof:

'Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. ...'

10. Article 15 of Directive 2002/58, entitled 'Application of certain provisions of Directive [95/46]', provides, in paragraph 1 thereof:

'Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive [95/46]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of [EU] law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.'

Irish law

11. As stated in the order for reference, the 2011 Act was adopted in order to transpose into the Irish legal order Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

12. Section 1 of the 2011 Act defines 'data' as 'traffic data or location data and the related data necessary to identify the subscriber or user' and a 'serious offence' as one which is punishable by imprisonment for a term of five years or more and also those other offences listed in Schedule 1 to that act.

13. Section 3(1) of the 2011 Act requires all providers of electronic communications services to retain the data referred to in Schedule 2, Part 1, for a period of two years and the data referred to in Schedule 2, Part 2, for a period of one year.

14. Schedule 2, Part 1, to the 2011 Act applies, inter alia, to fixed network telephony data and mobile telephony data that permit the identification of the source, the destination, and the date and time of the start and end of a communication, the type of communication involved, the type of location and the geographic location of the communications equipment used. In particular, point 6 of Part 1 of Schedule 2 provides for the retention of data necessary to identify the location of mobile communication equipment, those data being, first, the identity of the cell ('cell ID') and, second, data identifying the geographical location of cells by reference to their cell ID during the period for which communication data are retained.

15. Schedule 2, Part 2, to the 2011 Act covers data relating to internet access, internet email and internet telephony and includes, inter alia, the user identification number ('user ID') and telephone number, the Internet Protocol (IP) address and the date, time and duration of a communication. The content of communications does not fall within this type of data.

16. Under sections 4 and 5 of the 2011 Act, service providers must take specified measures to ensure that data are protected against unauthorised access.

17. Section 6 of the 2011 Act, which lays down the conditions under which a disclosure request may be made, provides in paragraph 1:

'A member of the Garda Síochána not below the rank of chief superintendent may request a service provider to disclose to that member data retained by the service provider in accordance with section 3 where that member is satisfied that the data are required for—

(a) the prevention, detection, investigation or prosecution of a serious offence,

(b) the safeguarding of the security of the State,

(c) the saving of human life.'

18. Section 7 of the 2011 Act requires service providers to comply with disclosure requests referred to in section 6 thereof.

19. For the purpose of reviewing the decision of the member of the Garda Síochána referred to in section 6 of the 2011 Act, a complaint procedure is provided for in section 10 thereof and a procedure

before the designated judge, within the meaning of section 12 thereof, who is responsible for examining the application of the provisions of that act.

The dispute in the main proceedings and the questions referred for a preliminary ruling

20. In March 2015, G.D. was sentenced to life imprisonment for the murder of a person who disappeared in August 2012 and whose remains were not discovered until September 2013. In the appeal against his conviction, G.D. criticised the first-instance court in particular for having incorrectly admitted as evidence traffic and location data relating to telephone calls, on the ground that the 2011 Act, which governed the retention of that data and on the basis of which the police carrying out the investigation had obtained access to those data, infringed rights conferred on him by EU law. That appeal is currently pending.

21. In order to be able to contest, as part of the criminal proceedings, the admissibility of that evidence, G.D. brought civil proceedings before the High Court (Ireland) seeking a declaration that some of the provisions of the 2011 Act are invalid. By decision of 6 December 2018, that court upheld G.D.'s submission and held that section 6(1)(a) of that act was incompatible with Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 and Article 52(1) of the Charter. Ireland appealed against that decision to the Supreme Court (Ireland), which is the referring court.

22. The criminal proceedings pending before the Court of Appeal (Ireland) were stayed until the delivery of the referring court's decision in the main civil proceedings.

23. Before the referring court, Ireland submitted that, in order to determine whether interference with the right to private life enshrined in Article 7 of the Charter as a result of the retention of traffic and location data under the 2011 Act is proportionate, it is necessary to examine the objectives of the regime established by that law as a whole. In addition, according to that Member State, that act established a detailed framework governing access to retained data by virtue of which the section responsible, within the national police force, for the prior examination of requests for access was functionally independent from the national police in the conduct of its duties and, therefore, satisfied the requirement for a prior review to be carried out by an independent administrative entity. That system of review is complemented by a complaints procedure and by judicial review. Finally, that Member State submits that, if the 2011 Act is ultimately held to be inconsistent with EU law, the temporal effect of any declaration which the referring court makes as a result should be prospective only.

24. For his part, G.D. submits that the system of general and indiscriminate retention of data established by the 2011 Act and the regime for access to those data provided for by that law are incompatible with EU law as interpreted, in particular, by the Court in paragraph 120 of the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970).

25. The referring court states, as a preliminary matter, that it is for it to determine only whether the High Court was correct in law to hold that section 6(1)(a) of the 2011 Act was incompatible with EU law and that, by contrast, the question of the admissibility of the evidence submitted in the context of the criminal proceedings falls within jurisdiction of the Court of Appeal which is seised of the appeal brought against the conviction.

26. In that context, the referring court has doubts, first of all, as to the requirements of EU law as regards the retention of data for the purposes of combating serious crime. In that regard, it considers, in essence, that only the general and indiscriminate retention of traffic and location data allows serious crime to be combated effectively, which the targeted and expedited retention (quick freeze) of data does not make possible. As regards targeted retention, the referring court wonders whether it is possible to target specific groups or geographic areas for the purposes of combating serious crimes, since some serious crimes rarely involve circumstances known to the competent national authorities enabling them to suspect the commission of an offence in advance. In addition, targeted retention could give rise to discrimination. As for expedited retention, the referring court considers that that is only useful in situations where it is possible to identify a suspect in the very early stages of an investigation.

27. As regards, next, access to data retained by providers of electronic communications services, the referring court explains that the national police force established, within its organisation, a system of self-certification of requests addressed to those service providers. Thus, it is clear from the evidence produced before the High Court that the Commissioner of the national police force decided, by an internal measure, that the requests for access made pursuant to the 2011 Act must be dealt with in a centralised manner, by a single national police officer of the rank of Chief Superintendent, namely the head of the security and intelligence section. If that official considers that the data concerned are necessary for the purposes, *inter alia*, of the prevention, detection, investigation or prosecution of a serious offence, he or she may address a request for access to the providers of electronic communications services. In addition, the Commissioner of the national police force established, within the police force, an independent unit entitled the Telecommunications Liaison Unit ('the TLU')

in order to provide support to the head of the security and intelligence section in the exercise of his or her duties and to serve as a single point of contact with those service providers.

28. The referring court adds that, during the period concerned by the criminal investigation brought against G.D., all the requests for access were required to be approved in the first place by a superintendent or inspector acting in that capacity, before they were sent to the TLU to be processed, and that the investigators were directed to include sufficient detail in their requests for access so that an informed decision could be taken. In addition, the TLU and the head of the security and intelligence section were required to examine the legality, necessity and proportionality of requests for access, taking into account the fact that that head could be called upon to answer for his or her decision before the judge designated by the High Court. Furthermore, the TLU is also subject to audit by the Data Protection Commissioner (Ireland).

29. Finally, the referring court is uncertain as to the scope and temporal effects of a possible declaration of incompatibility of the 2011 Act with EU law. In that regard, it states that such a declaration could only be applied prospectively on the ground the data used as evidence in the criminal proceedings against G.D. were the subject of retention and access at the end of 2013, namely in a period during which Ireland was required to apply the provisions of the 2011 Act transposing Directive 2006/24. According to Ireland, that solution would also be appropriate since, otherwise, the investigation and prosecution of serious offences in Ireland, and the situation of persons already tried and convicted could be seriously impacted.

30. It was in those circumstances that the Supreme Court decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

‘(1) Is a general/universal data retention regime - even subject to stringent restrictions on retention and access - per se contrary to the provisions of Article 15 of Directive [2002/58], interpreted in the light of the Charter?

(2) In considering whether to grant a declaration of inconsistency of a national measure implemented pursuant to Directive [2006/24], and making provision for a general data retention regime (subject to the necessary stringent controls on retention and/or in relation to access), and in particular in assessing the proportionality of any such regime, is a national court entitled to have regard to the fact that data may be retained lawfully by service providers for their own commercial purposes, and may be required to be retained for reasons of national security excluded from the provisions of Directive [2002/58]?

(3) In assessing, in the context of determining the compatibility with [EU] law and in particular with Charter Rights of a national measure for access to retained data, what criteria should a national court apply in considering whether any such access regime provides the required independent prior scrutiny as determined by the Court of Justice in its case-law? In that context, can a national court, in making such an assessment, have any regard to the existence of ex post judicial or independent scrutiny?

(4) In any event, is a national court obliged to declare the inconsistency of a national measure with the provisions of Article 15 of [Directive 2002/58], if the national measure makes provision for a general data retention regime for the purpose of combating serious crime, and where the national court has concluded, on all the evidence available, that such retention is both essential and strictly necessary to the achievement of the objective of combating serious crime?

(5) If a national court is obliged to conclude that a national measure is inconsistent with the provisions of Article 15 of Directive [2002/58], as interpreted in the light of the Charter, is it entitled to limit the temporal effect of any such declaration, if satisfied that a failure to do so would lead to “resultant chaos and damage to the public interest” (in line with the approach taken, for example, in *R (National Council for Civil Liberties) v Secretary of State for Home Department and Secretary of State for Foreign Affairs* [2018] EWHC 975, at paragraph 46)?

(6) May a national court invited to declare the inconsistency of national legislation with Article 15 of [Directive 2002/58], and/or to disapply this legislation, and/or to declare that the application of such legislation had breached the rights of an individual, either in the context of proceedings commenced in order to facilitate an argument in respect of the admissibility of evidence in criminal proceedings or otherwise, be permitted to refuse such relief in respect of data retained pursuant to the national provision enacted pursuant to the obligation under Article 288 TFEU to faithfully introduce into national law the provisions of a directive, or to limit any such declaration to the period after the declaration of invalidity of [Directive 2006/24] issued by the [judgment of 8 April 2014, *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238)]?’

Consideration of the questions referred

The first, second and fourth questions

31. By its first, second and fourth question, which it is appropriate to examine together, the referring court asks, in essence, whether Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that provides

for the general and indiscriminate retention of traffic and location data for the purposes of combating serious crime.

32. It should be noted, as a preliminary point, that it is settled case-law that, in interpreting a provision of EU law, it is necessary not only to refer to its wording but also to consider its context and the objectives of the legislation of which it forms part, and in particular the origin of that legislation (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 105 and the case-law cited).

33. It is clear from the wording itself of Article 15(1) of Directive 2002/58 that the legislative measures that it authorises Member States to take, under the conditions that it lays down, may seek only 'to restrict the scope' of the rights and obligations laid down inter alia in Articles 5, 6 and 9 of Directive 2002/58.

34. As regards the system established by that directive of which Article 15(1) forms part, it must be recalled that, pursuant to the first and second sentences of Article 5(1) of that directive, Member States are required to ensure, through their national legislation, the confidentiality of communications by means of a public communications network and publicly available electronic communications services, as well as of the related traffic data. In particular, they are required to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1) of the same directive.

35. In that regard, the Court has already held that Article 5(1) of Directive 2002/58 enshrines the principle of confidentiality of both electronic communications and the related traffic data and requires inter alia that, in principle, persons other than users be prohibited from storing, without those users' consent, those communications and data (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 107).

36. That provision reflects the objective pursued by the EU legislature when adopting Directive 2002/58. It is apparent from the Explanatory Memorandum of the Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM(2000) 385 final), which gave rise to Directive 2002/58, that the EU legislature sought to 'ensure that a high level of protection of personal data and privacy will continue to be guaranteed for all electronic communications services regardless of the technology used'. As is apparent from, inter alia, recitals 6 and 7 thereof, the purpose of that directive is to protect users of electronic communications services from risks for their personal

data and privacy resulting from new technologies and, in particular, from the increasing capacity for automated storage and processing of data. In particular, as stated in recital 2 of the directive, the EU legislature's intent is to ensure full respect for the rights set out in Articles 7 and 8 of the Charter (see, to that effect, judgments of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 83, and of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 106).

37. In adopting Directive 2002/58, the EU legislature gave concrete expression to those rights, so that the users of electronic communications services are entitled to expect, in principle, that their communications and data relating thereto will remain anonymous and may not be recorded, unless they have agreed otherwise (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 109).

38. As regards the processing and storage by electronic communications service providers of subscribers' and users' traffic data, Article 6 of Directive 2002/58 provides, in paragraph 1, that those data must be erased or made anonymous when they are no longer needed for the purpose of the transmission of a communication, and states, in paragraph 2, that the traffic data necessary for the purposes of subscriber billing and interconnection fees may only be processed up to the end of the period during which the bill may lawfully be challenged or payments pursued in order to obtain payment. As regards location data other than traffic data, Article 9(1) of that directive provides that those data may be processed only subject to certain conditions and after they have been made anonymous or the consent of the users or subscribers obtained.

39. Therefore, Directive 2002/58 does not merely create a framework for access to such data through safeguards to prevent abuse, but also enshrines, in particular, the principle of the prohibition of their storage by third parties.

40. In so far as Article 15(1) of Directive 2002/58 permits Member States to adopt legislative measures that 'restrict the scope' of the rights and obligations laid down inter alia in Articles 5, 6 and 9 of that directive, such as those arising from the principles of confidentiality of communications and the prohibition on storing related data recalled in paragraph 35 of this judgment, that provision provides for an exception to the general rule provided for inter alia in Articles 5, 6 and 9 and must thus, in accordance with settled case-law, be the subject of a strict interpretation. That provision, therefore, cannot permit the exception to the obligation of principle to ensure the confidentiality of electronic communications and data relating thereto and, in particular, to the prohibition on storage of that data, laid down in Article 5 of that directive, to become the rule, if the latter provision is not to be rendered

largely meaningless (see, to that effect, judgments of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 89, and of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 111).

41. As regards the objectives that are capable of justifying a limitation of the rights and obligations laid down, in particular, in Articles 5, 6 and 9 of Directive 2002/58, the Court has previously held that the list of objectives set out in the first sentence of Article 15(1) of that directive is exhaustive, as a result of which a legislative measure adopted under that provision must correspond, genuinely and strictly, to one of those objectives (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 112 and the case-law cited).

42. Furthermore, it is clear from the third sentence in Article 15(1) of Directive 2002/58 that measures taken by the Member States must comply with the general principles of EU law, which include the principle of proportionality, and ensure respect for the fundamental rights guaranteed by the Charter. In that regard, the Court has previously held that the obligation imposed on providers of electronic communications services by a Member State by way of national legislation to retain traffic data for the purpose of making them available, if necessary, to the competent national authorities raises issues relating to compatibility not only with Articles 7 and 8 of the Charter, relating to the protection of privacy and to the protection of personal data, respectively, but also with Article 11 of the Charter, relating to the freedom of expression (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 113 and the case-law cited).

43. Thus, the interpretation of Article 15(1) of Directive 2002/58 must take account of the importance both of the right to privacy, guaranteed in Article 7 of the Charter, and of the right to protection of personal data, guaranteed in Article 8 thereof, as derived from the case-law of the Court, as well as the importance of the right to freedom of expression, given that that fundamental right, guaranteed in Article 11 of the Charter, constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 114 and the case-law cited).

44. It should be made clear, in that regard, that the retention of traffic and location data constitutes, in itself, first, a derogation from the prohibition laid down in Article 5(1) of Directive 2002/58 barring any person other than the users from storing those data, and, second, an interference with the fundamental rights to the respect for private life and the protection of personal data, enshrined in Articles 7 and 8 of the Charter, irrespective of whether the information in question relating to private

life is sensitive, whether the persons concerned have been inconvenienced in any way on account of that interference, or, furthermore, whether the data retained will or will not be used subsequently (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 115 and 116 and the case-law cited).

45. That conclusion is all the more justified since traffic and location data may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health, given that such data moreover enjoy special protection under EU law. Taken as a whole, those data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data have been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, those data provide the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 117 and the case-law cited).

46. Therefore, first, the retention of traffic and location data for policing purposes is liable, in itself, to infringe the right to respect for communications, enshrined in Article 7 of the Charter, and to deter users of electronic communications systems from exercising their freedom of expression, guaranteed in Article 11 of the Charter, effects that are all the more serious given the quantity and breadth of data retained. Second, in view of the significant quantity of traffic and location data that may be continuously retained under a general and indiscriminate retention measure, as well as the sensitive nature of the information that may be gleaned from those data, the mere retention of such data by providers of electronic communications services entails a risk of abuse and unlawful access (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 118 and 119 and the case-law cited).

47. In that regard, it must be emphasised that the retention of and access to those data each constitute, as is clear from the case-law recalled in paragraph 44 of this judgment, separate interferences with the fundamental rights guaranteed by Articles 7 and 11 of the Charter, requiring a separate justification pursuant to Article 52(1) of the Charter. It follows that national legislation ensuring full respect for the conditions established by the case-law interpreting Directive 2002/58 as regards access to retained data cannot, by its very nature, be capable of either limiting or even remedying the serious

interference, which results from the general retention of those data provided for under that national legislation, with the rights guaranteed by Articles 5 and 6 of that directive and by the fundamental rights to which those articles give specific effect.

48. That being said, in so far as Article 15(1) of Directive 2002/58 allows Member States to introduce the derogations referred to in paragraph 34 to 37 of this judgment, that provision reflects the fact that the rights enshrined in Articles 7, 8 and 11 of the Charter are not absolute rights, but must be considered in relation to their function in society. Indeed, as can be seen from Article 52(1) of the Charter, that provision allows limitations to be placed on the exercise of those rights, provided that those limitations are provided for by law, that they respect the essence of those rights and that, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. Thus, in order to interpret Article 15(1) of Directive 2002/58 in the light of the Charter, account must also be taken of the importance of the rights enshrined in Articles 3, 4, 6 and 7 of the Charter and of the importance of the objectives of protecting national security and combating serious crime in contributing to the protection of the rights and freedoms of others (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 120 to 122 and the case-law cited).

49. Thus as regards, in particular, effective action to combat criminal offences committed against, *inter alia*, minors and other vulnerable persons, it should be borne in mind that positive obligations of the public authorities may result from Article 7 of the Charter, requiring them to adopt legal measures to protect private and family life. Such obligations may also arise from Article 7, concerning the protection of an individual's home and communications, and Articles 3 and 4, as regards the protection of an individual's physical and mental integrity and the prohibition of torture and inhuman and degrading treatment (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 126 and the case-law cited).

50. It is against the backdrop of those different positive obligations that the Court must strike a balance between the various interests and rights at issue. The European Court of Human Rights has held that the positive obligations flowing from Articles 3 and 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, whose corresponding safeguards are set out in Articles 4 and 7 of the Charter, require, in particular, the adoption of substantive and procedural provisions as well as practical measures enabling effective action to combat crimes against the person through effective investigation and prosecution, that obligation being all the more important when a child's

physical and moral well-being is at risk. However, the measures to be taken by the competent authorities must fully respect due process and the other safeguards limiting the scope of criminal investigation powers, as well as other freedoms and rights. In particular, according to that court, a legal framework should be established enabling a balance to be struck between the various interests and rights to be protected (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 127 and 128 and the case-law cited).

51. In that context, it is clear from the wording itself of the first sentence of Article 15(1) of Directive 2002/58 that the Member States may adopt a measure derogating from the principle of confidentiality referred to in paragraph 35 of this judgment where such a measure is ‘necessary, appropriate and proportionate ... within a democratic society’, and recital 11 of the directive specifies, in that respect, that a measure of that nature must be ‘strictly’ proportionate to the intended purpose (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 129).

52. In that regard, it should be borne in mind that the protection of the fundamental right to privacy requires, according to the settled case-law of the Court, that derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 130 and the case-law cited).

53. More specifically, it follows from the Court’s case-law that the question whether the Member States may justify a limitation on the rights and obligations laid down, *inter alia*, in Articles 5, 6 and 9 of Directive 2002/58 must be assessed by measuring the seriousness of the interference entailed by such a limitation and by verifying that the importance of the public interest objective pursued by that limitation is proportionate to that seriousness (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 131 and the case-law cited).

54. In order to satisfy the requirement of proportionality, the national legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that those data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring

that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data are subjected to automated processing, in particular where there is a significant risk of unlawful access to those data. Those considerations apply especially where the protection of the particular category of personal data that are sensitive data is at stake (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 132 and the case-law cited).

55. Thus, national legislation requiring the retention of personal data must always meet objective criteria that establish a connection between the data to be retained and the objective pursued. In particular, as regards combating serious crime, the data whose retention is provided for must be capable of contributing to the prevention, detection or prosecution of serious offences (see, to that effect, judgments of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 59, and of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 133).

56. As regards the public interest objectives that may justify a measure taken pursuant to Article 15(1) of Directive 2002/58, it is clear from the Court's case-law, in particular the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), that, in accordance with the principle of proportionality, there is a hierarchy amongst those objectives according to their respective importance and that the importance of the objective pursued by such a measure must be proportionate to the seriousness of the interference that it entails.

57. In that regard, the Court held that the importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU according to which national security remains the sole responsibility of each Member State, exceeds that of the other objectives referred to in Article 15(1) of Directive 2002/58, *inter alia* the objectives of combating crime in general, even serious crime, and of safeguarding public security. Subject to meeting the other requirements laid down in Article 52(1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 135 and 136).

58. It is for that reason that the Court held that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, does not preclude legislative measures that allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data

in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable, where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 168).

59. As regards the objective of preventing, investigating, detecting and prosecuting criminal offences, the Court held that, in accordance with the principle of proportionality, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, such as the interference entailed by the retention of traffic and location data. Accordingly, only non-serious interference with those fundamental rights may be justified by the objective of preventing, detecting and prosecuting criminal offences in general (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 140 and the case-law cited).

60. At the hearing, the European Commission submitted that particularly serious crime could be treated in the same way as a threat to national security.

61. However, the Court has already held that the objective of protecting national security corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society through the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 135).

62. It should also be observed that, unlike crime, even particularly serious crime, a threat to national security must be genuine and present, or, at the very least, foreseeable, which presupposes that sufficiently concrete circumstances have arisen to be able to justify a generalised and indiscriminate measure of retention of traffic and location data for a limited period of time. Such a threat is therefore distinguishable, by its nature, its seriousness, and the specific nature of the circumstances of which it is constituted, from the general and permanent risk of the occurrence of tensions or disturbances, even of a serious nature, that affect public security, or from that of serious criminal offences being

committed (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 136 and 137).

63. Thus, criminal behaviour, even of a particularly serious nature, cannot be treated in the same way as a threat to national security. As the Advocate General observed in points 49 to 50 of his Opinion, to treat those situations in the same way would be likely to create an intermediate category between national security and public security for the purpose of applying to the latter the requirements inherent in the former.

64. It also follows that the fact, recalled in the second question referred for a preliminary ruling, that traffic and location data were legally the object of retention for the purpose of safeguarding national security does not have any bearing on the legality of their retention for the purpose of combating serious crime.

65. As regards the objective of combating serious crime, the Court held that national legislation providing, for that purpose, for the general and indiscriminate retention of traffic and location data exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society. In view of the sensitive nature of the information that traffic and location data may provide, the confidentiality of those data is essential for the right to respect for private life. Thus, and also taking into account, first, the dissuasive effect on the exercise of the fundamental rights enshrined in Articles 7 and 11 of the Charter, referred to in paragraph 46 of this judgment, which is liable to result from the retention of those data, and, second, the seriousness of the interference entailed by such retention, it is necessary, within a democratic society, that retention be the exception and not the rule, as provided for in the system established by Directive 2002/58, and that those data should not be retained systematically and continuously. That conclusion applies even having regard to the objectives of combating serious crime and preventing serious threats to public security and to the importance that must be attached to them (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 141 and 142 and the case-law cited).

66. In addition, the Court has emphasised that national legislation providing for the general and indiscriminate retention of traffic and location data covers the electronic communications of practically the entire population without any differentiation, limitation or exception being made in the light of the objective pursued. Such legislation is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons with respect to

whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with that objective of combating serious crime and, in particular, without there being any relationship between the data whose retention is provided for and a threat to public security. In particular, as the Court has already held, such legislation is not restricted to retention in relation to (i) data pertaining to a time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to combating serious crime (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 143 and 144 and the case-law cited).

67. However, in paragraph 168 of the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), the Court stated that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8, 11 and Article 52(1) of the Charter, does not preclude legislative measures that provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for

- the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;
- the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;
- the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and
- recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention (quick freeze) of traffic and location data in the possession of those service providers,

provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.

68. In the present order for reference, which was lodged with the Court before the judgments of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), and of 2 March 2021, *Prokuratuur* (Conditions of access to data relating to electronic communications)

(C-746/18, EU:C:2021:152), were delivered, the referring court considered however that only the general and indiscriminate retention of traffic and location data allows serious crime to be combated effectively. At the hearing on 13 September 2021, it was submitted, inter alia by Ireland and the French Government, that that conclusion was not invalidated by the fact that it was possible for the Member States to have recourse to the measures referred to in the preceding paragraph.

69. In that regard, it must be observed, in the first place, that the effectiveness of criminal proceedings generally depends not on a single means of investigation but on all the means of investigation available to the competent national authorities for those purposes.

70. In the second place, it must be noted that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, as interpreted by the case-law recalled in paragraph 67 of this judgment, allows Member States to adopt, for the purposes of combating serious crime and preventing serious threats to public security, not only measures for targeted retention and expedited retention, but also measures providing for the general and indiscriminate retention, first, of data relating to the civil identity of users of electronic communications systems and, second, of IP addresses assigned to the source of a connection.

71. In that respect, it is common ground that retention of data relating to the civil identity of users of electronic communications systems may contribute to the fight against serious crime to the extent that those data make it possible to identify persons who have used those means in the context of planning or committing an act constituting serious crime.

72. As is clear from the case-law summarised in paragraph 67 of this judgment, Directive 2002/58 does not preclude, for the purposes of combating crime in general, the general retention of data relating to civil identity. In those circumstances, it must be stated that neither the directive nor any other EU law act precludes national legislation, which has the purpose of combating serious crime, pursuant to which the purchase of a means of electronic communication, such as a pre-paid SIM card, is subject to a check of official documents establishing the purchaser's identity and the registration, by the seller, of that information, with the seller being required, should the case arise, to give access to that information to the competent national authorities.

73. In addition, it should be recalled that the generalised retention of IP addresses of the source of connection constitutes a serious interference in the fundamental rights enshrined in Articles 7 and 8 of the Charter as those IP addresses may allow precise conclusions to be drawn concerning the private life of the user of the means of electronic communication concerned and may be a deterrent to the exercise of freedom of expression guaranteed in Article 11 of the Charter. However, as regards such

retention, the Court has held that in order to strike the necessary balance between the rights and interests at issue as required by the case-law referred to in paragraphs 50 to 53 of this judgment, it is necessary to take into account, in a case of an offence committed online and, in particular, in cases of the acquisition, dissemination, transmission or making available online of child pornography, within the meaning of Article 2(c) of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ 2011 L 335, p. 1), the fact that the IP address might be the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the offence to be identified (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 153 and 154).

74. Hence, the Court held that such general and indiscriminate retention solely of IP addresses assigned to the source of a connection does not, in principle, appear to be contrary to Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 of the Charter, provided that that possibility is subject to strict compliance with the substantive and procedural conditions which should regulate the use of those data, as referred to in paragraphs 155 and 156 of the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791).

75. In the third place, as regards legislative measures providing for a targeted retention and an expedited retention of traffic and location data, the indications provided in the order for reference show a narrower understanding of the scope of those measures than that upheld in the case-law recalled in paragraph 67 of this judgment. While, as is recalled in paragraph 40 of this judgment, those retention measures are a derogation within the system established by Directive 2002/58, that directive, read in the light of the fundamental rights enshrined in Articles 7, 8 and 11 and Article 52(1) of the Charter, does not make the possibility of issuing an order requiring a targeted retention subject to the condition either that the places likely to be the location of a serious crime or the persons suspected of being involved in such an act must be known in advance. Likewise, that directive does not require that the order requiring an expedited retention be limited to suspects identified in advance of that order.

76. As regards, first, targeted retention, the Court held that Article 15(1) of Directive 2002/58 does not preclude national legislation based on objective evidence which makes it possible to target persons whose traffic and location data are likely to reveal a link, at least an indirect one, with serious criminal offences, to contribute in one way or another to combating serious crime or to preventing a serious

risk to public security or a risk to national security (judgments of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 111, and of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 148).

77. The Court stated, in that regard, that, while the objective evidence may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the persons thus targeted may, in particular, be persons who have been identified beforehand, in the course of the applicable national procedures and on the basis of objective and non-discriminatory factors, as posing a threat to public or national security in the Member State concerned (see, to that effect, judgments of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 110, and of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 149).

78. Member States thus have, *inter alia*, the option of imposing retention measures targeting persons who, on the basis of an identification, are the subject of an investigation or other measures of current surveillance or of a reference in the national criminal record relating to an earlier conviction for serious crimes with a high risk of reoffending. Where that identification is based on objective and non-discriminatory factors, defined in national law, targeted retention in respect of persons thus identified is justified.

79. Second, a targeted measure for the retention of traffic and location data may, at the choice of the national legislature and in strict compliance with the principle of proportionality, also be set using a geographical criterion where the competent national authorities consider, on the basis of objective and non-discriminatory factors, that there exists, in one or more geographical areas, a situation characterised by a high risk of preparation for or commission of serious criminal offences. Those areas may include places with a high incidence of serious crime, places that are particularly vulnerable to serious crime, such as places or infrastructure which regularly receive a very high volume of visitors, or strategic locations, such as airports, stations, maritime ports or tollbooth areas (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 150 and the case-law cited).

80. It should be borne in mind that, according to that case-law, the competent national authorities may adopt, for areas referred to in the preceding paragraph, a targeted measure of retention using a geographic criterion, such as, *inter alia*, the average crime rate in a geographical area, without that authority necessarily having specific indications as to the preparation or commission, in the areas concerned, of acts of serious crime. Since a targeted retention using that criterion is likely to concern,

depending on the serious criminal offences in question and the situation specific to the respective Member States, both the areas marked by a high incidence of serious crime and areas particularly vulnerable to the commission of those acts, it is, in principle, not likely moreover to give rise to discrimination, as the criterion drawn from the average rate of serious crime is entirely unconnected with any potentially discriminatory factors.

81. In addition and above all, a targeted measure of retention covering places or infrastructures which regularly receive a very high volume of visitors, or strategic places, such as airports, stations, maritime ports or tollbooth areas, allows the competent authorities to collect traffic data and, in particular, location data of all persons using, at a specific time, a means of electronic communication in one of those places. Thus, such a targeted retention measure may allow those authorities to obtain, through access to the retained data, information as to the presence of those persons in the places or geographical areas covered by that measure as well as their movements between or within those areas and to draw, for the purposes of combating serious crime, conclusions as to their presence and activity in those places or geographical areas at a specific time during the period of retention.

82. It should also be noted that the geographic areas covered by such a targeted retention measure may and, where appropriate, must be amended in accordance with changes in the circumstances that justified their selection, thus making it possible to react to developments in the fight against serious crime. The Court has held that the duration of those targeted retention measures described in paragraphs 76 to 81 of this judgment must not exceed what is strictly necessary in the light of the objective pursued and the circumstances justifying them, without prejudice to the possibility of extending those measures should such retention continue to be necessary (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 151).

83. As regards the possibility of providing distinctive criteria other than a personal or geographic criterion for the targeted retention of traffic and location data, it is possible that other objective and non-discriminatory criteria may be considered in order to ensure that the scope of a targeted retention measure is as limited as is strictly necessary and to establish a connection, at least indirectly, between serious criminal acts and the persons whose data are retained. However, since Article 15(1) of Directive 2002/58 refers to legislative measures of the Member States, it is for the latter and not for the Court to identify those criteria, it being understood that there can be no question of reinstating, by that means, the general and indiscriminate retention of traffic and location data.

84. In any event, as Advocate General Campos Sánchez-Bordona observed in point 50 of his Opinion in Joined Cases SpaceNet and Telekom Deutschland (C-793/19 and C-794/19, EU:C:2021:939), the fact that it may be difficult to provide a detailed definition of the circumstances and conditions under which targeted retention may be carried out is no reason for the Member States, by turning the exception into a rule, to provide for the general retention of traffic and location data.

85. As regards, second, the expedited retention of traffic and location data processed and stored by providers of electronic communications services on the basis of Articles 5, 6 and 9 of Directive 2002/58 or on the basis of legislative measures taken under Article 15(1) of that directive, it should be noted that those data must, in principle, be erased or made anonymous, depending on the circumstances, at the end of the statutory periods within which those data must be processed and stored in accordance with the national provisions transposing that directive. Nevertheless, the Court has held that during that processing and storage, situations may arise in which it becomes necessary to retain those data after those time periods have ended in order to shed light on serious criminal offences or acts adversely affecting national security; this is the case both in situations where those offences or acts having adverse effects have already been established and where, after an objective examination of all of the relevant circumstances, such offences or acts having adverse effects may reasonably be suspected (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 160 and 161).

86. In such a situation, in the light of the balance that must be struck between the rights and interests at issue referred to in paragraphs 50 to 53 of this judgment, it is permissible for Member States to provide, in legislation adopted pursuant to Article 15(1) of Directive 2002/58, for the possibility of instructing, by means of a decision of the competent authority subject to effective judicial review, providers of electronic communications services to undertake the expedited retention of traffic and location data at their disposal for a specified period of time (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 163).

87. To the extent that the purpose of that expedited retention no longer corresponds to the purpose for which those data were initially collected and retained and since any processing of data must, under Article 8(2) of the Charter, be consistent with specified purposes, Member States must make clear, in their legislation, for what purpose the expedited retention of data may occur. In the light of the serious nature of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter which such retention may entail, only actions to combat serious crime and, a fortiori, to safeguard national security are such as to justify such interference, on the condition that the measure

and access to the retained data comply with the limits of what is strictly necessary, as set out in paragraphs 164 to 167 of the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791).

88. The Court has stated that a measure of retention of that nature need not be limited to the data of persons who have been identified previously as being a threat to public security or national security of the Member State concerned or of persons specifically suspected of having committed a serious criminal offence or acts adversely affecting national security. According to the Court, while it must comply with the framework established by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, and taking into account the findings in paragraph 55 of this judgment, such a measure may, at the choice of the national legislature and subject to the limits of what is strictly necessary, be extended to traffic and location data relating to persons other than those who are suspected of having planned or committed a serious criminal offence or acts adversely affecting national security, provided that those data can, on the basis of objective and non-discriminatory factors, shed light on such an offence or acts adversely affecting national security, such as data concerning the victim thereof, and his or her social or professional circle (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 165).

89. Thus, a legislative measure may authorise the issuing of an instruction to providers of electronic communications services to carry out the expedited retention of traffic and location data, *inter alia*, of persons with whom, prior to the serious threat to public security arising or a serious crime being committed, a victim was in contact via those electronic means of communications.

90. Such expedited retention may, according to the Court's case-law recalled in paragraph 88 of this judgment and under the same conditions as those referred to in that paragraph, also be extended to specific geographic areas, such as the places of the commission of or preparation for the offence or attack on national security in question. It should be stated that the subject matter of such a measure may also be the traffic and location data relating to a place or a person, possibly the victim of a serious crime, who has disappeared, on condition that that measure and access to the data so retained comply with the limits of what is strictly necessary, as set out in paragraphs 164 to 167 of the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791).

91. Furthermore, it must be stated that Article 15(1) of Directive 2002/58 does not preclude the competent national authorities from ordering a measure of expedited retention at the first stage of an investigation into a serious threat for public security or a possible serious crime, namely from the time

when the authorities may, in accordance with the provisions of national law, commence such an investigation.

92. As regards the variety of measures for the retention of traffic and location data referred to in paragraph 67 of this judgment, it must be stated that those various measures may, at the choice of the national legislature and subject to the limits of what is strictly necessary, be applied concurrently. Accordingly, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, as interpreted by case-law resulting from the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), does not preclude a combination of those measures.

93. In the fourth and final place, it must be emphasised that the proportionality of the measures adopted pursuant to Article 15(1) of Directive 2002/58 requires, according to the Court's settled case-law, as recalled in the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), compliance not only with the requirements of aptitude and of necessity but also with that of the proportionate nature of those measures in relation to the objective pursued.

94. In that context, it should be recalled that, in paragraph 51 of its judgment of 8 April 2014, *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238), the Court held that while the fight against serious crime is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques, that objective of general interest, however fundamental it may be, does not, in itself, justify that a measure providing for the general and indiscriminate retention of all traffic and location data, such as that established by Directive 2006/24, should be considered to be necessary.

95. In the same vein, the Court stated, in paragraph 145 of the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), that even the positive obligations of the Member States which may arise, depending on the circumstances, from Articles 3, 4 and 7 of the Charter and which relate, as pointed out in paragraph 49 of this judgment, to the establishment of rules to facilitate effective action to combat criminal offences, cannot have the effect of justifying interference that is as serious as that entailed by legislation providing for the retention of traffic and location data with the fundamental rights, enshrined in Articles 7 and 8 of the Charter, of practically the entire population, in circumstances where the data of the persons concerned are not liable to disclose a link, at least an indirect one, between those data and the objective pursued.

96. At the hearing, the Danish Government submitted that the competent national authorities should be able to access, for the purpose of fighting serious crime, traffic and location data which have been retained in a general and indiscriminate way, in accordance with the line of case-law resulting from the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 135 to 139), in order to address a serious threat to national security that is genuine and present, or foreseeable.

97. It should be observed, first of all, that the fact of authorising access for the purpose of combating serious crime to traffic and location data which have been retained in a general and indiscriminate way would make that access depend upon facts that fall outside that objective, according to whether or not, in the Member State concerned there was a serious threat to national security as referred to in the preceding paragraph, whereas, in view of the sole objective of the fight against serious crime which must justify the retention of those data and access thereto, there is nothing to justify a difference in treatment, in particular, as between the Member States.

98. As the Court has already held, access to traffic and location data retained by providers in accordance with a measure taken under Article 15(1) of Directive 2002/58, which must be given effect in full compliance with the conditions resulting from the case-law interpreting Directive 2002/58, may, in principle, be justified only by the public interest objective for which those providers were ordered to retain those data. It is otherwise only if the importance of the objective pursued by access is greater than that of the objective which justified retention (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 165 and 166).

99. The Danish Government's submission refers to a situation in which the objective pursued by the access request proposed, namely the fight against serious crime, is of lesser importance in the hierarchy of objectives of public interest than that which justified the retention, namely the safeguarding of national security. To authorise, in that situation, access to retained data would be contrary to that hierarchy of public interest objectives recalled in the preceding paragraph, and also to paragraphs 53, 56, 57 and 59 of this judgment.

100. In addition and moreover, in accordance with the case-law recalled in paragraph 65 of this judgment, traffic and location data cannot be the object of general and indiscriminate retention for the purpose of combating serious crime and, therefore, access to those data cannot be justified for that same purpose. Where those data have exceptionally been retained in a general and indiscriminate way for the purpose of the safeguarding of national security against a genuine and present or

foreseeable threat, in the circumstances referred to in paragraph 58 of this judgment, the national authorities competent to undertake criminal investigations cannot access those data in the context of criminal proceedings, without depriving of any effectiveness the prohibition on such retention for the purpose of combating serious crime, recalled in paragraph 65.

101. In the light of all of the foregoing considerations, the answer to the first, second and fourth questions is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding legislative measures which provide, as a preventive measure, for the purposes of combating serious crime and for the prevention of serious threats to public security, for the general and indiscriminate retention of traffic and location data. However, Article 15(1), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not preclude legislative measures that, for the purposes of combating serious crime and preventing serious threats to public security, provide for:

- the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;
- the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;
- the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and
- recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers,

provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.

The third question

102. By its third question, the referring court asks, in essence, whether, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation pursuant to which the centralised processing of requests for access to retained data, issued by the police in the context of the investigation or prosecution of serious

criminal offences, is the responsibility of a police officer, assisted by a unit established within the police service which enjoys a degree of autonomy in the exercise of its duties and whose decisions may subsequently be subject to judicial review.

103. As a preliminary matter, it should be borne in mind that, while it is for national law to determine the conditions under which providers of electronic communications services must grant the competent national authorities access to data in their possession, the national legislation must, in order to satisfy the requirement of proportionality, as recalled in paragraph 54 of this judgment, lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that those data will be effectively protected against the risk of abuse (see, to that effect, judgment of 2 March 2021, *Prokuratuur* (Conditions of access to data relating to electronic communications), C-746/18, EU:C:2021:152, paragraph 48 and the case-law cited).

104. In particular, national legislation governing the access by the competent authorities to retained traffic and location data, adopted pursuant to Article 15(1) of Directive 2002/58, cannot be limited to requiring that the authorities' access to the data be consistent with the objective pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use (judgment of 2 March 2021, *Prokuratuur* (Conditions of access to data relating to electronic communications), C-746/18, EU:C:2021:152, paragraph 49 and the case-law cited).

105. Accordingly, since general access to all retained data, regardless of whether there is any, at least indirect, link with the intended purpose, cannot be regarded as being limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data in question. In that regard, such access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that those data might, in a specific case, make an effective contribution to combating such activities (judgment of 2 March 2021, *Prokuratuur* (Conditions of access to data relating to electronic communications), C-746/18, EU:C:2021:152, paragraph 50 and the case-law cited).

106. In order to ensure, in practice, that those conditions are fully observed, it is essential that access by the competent national authorities to retained data be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body be made following a reasoned request by those authorities submitted, *inter alia*, within the framework of procedures for the prevention, detection or prosecution of crime (judgment of 2 March 2021, Prokuratuur (Conditions of access to data relating to electronic communications), C-746/18, EU:C:2021:152, paragraph 51 and the case-law cited).

107. One of the requirements for the prior review is that the court or independent administrative body entrusted with carrying it out must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue. As regards a criminal investigation in particular, it is a requirement of such a review that that court or body must be able to strike a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access (judgment of 2 March 2021, Prokuratuur (Conditions of access to data relating to electronic communications), C-746/18, EU:C:2021:152, paragraph 52).

108. Where that review is carried out not by a court but by an independent administrative body, that body must have a status that enables it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence. Accordingly, it follows that the requirement of independence that has to be satisfied by the body entrusted with carrying out the prior review means that that body must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review objectively and impartially and free from any external influence. In particular, in the criminal field the requirement of independence entails that the body entrusted with the prior review, first, should not be involved in the conduct of the criminal investigation in question and, second, must have a neutral stance *vis-à-vis* the parties to the criminal proceedings (see, to that effect, judgment of 2 March 2021, Prokuratuur (Conditions of access to data relating to electronic communications), C-746/18, EU:C:2021:152, paragraphs 53 and 54).

109. Thus, the Court has, *inter alia*, found that a public prosecutor's office, which directs the investigation procedure and, where appropriate, brings the public prosecution cannot be considered to have third party status in relation to the interests at issue, since it has the task not of ruling on a case in complete independence but, acting as prosecutor in the proceedings, of bringing it, where appropriate, before the court that has jurisdiction. Consequently, a public prosecutor's office is not in

a position to carry out the prior review of requests for access to retained data (see, to that effect, judgment of 2 March 2021, *Prokuratuur* (Conditions of access to data relating to electronic communications), C-746/18, EU:C:2021:152, paragraphs 55 and 57).

110. Finally, the independent review required in accordance with Article 15(1) of Directive 2002/58 must take place before any access to the data concerned, except in the event of duly justified urgency, in which case the review must take place within a short time. A subsequent review would not enable the objective of a prior review, consisting in preventing the authorisation of access to the data in question that exceeds what is strictly necessary, to be met (see, to that effect, judgments of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 189, and of 2 March 2021, *Prokuratuur* (Conditions of access to data relating to electronic communications), C-746/18, EU:C:2021:152, paragraph 58).

111. In the present case, it is apparent from the order for reference that the 2011 Act assigns to a police officer, whose rank is not below that of chief superintendent, the power to carry out the prior review of requests for access to data issued by the police investigation services and to request the providers of electronic communications services to transmit the data that they retain to those services. To the extent that that officer does not have the status of a third party in relation to those services, he or she does not fulfil the requirements for independence and impartiality recalled in paragraph 108 of this judgment, notwithstanding the fact that he or she is assisted in that duty by a police unit, in this case the TLU, which benefits from a certain degree of autonomy in the exercise of its duties.

112. Next, while it is true that the 2011 Act provides for mechanisms of review subsequent to the decision of the competent police officer in the form of a complaint procedure and a procedure before a judge responsible for examining the application of the provisions of that act, it is clear from the case-law recalled in paragraph 110 of this judgment that a review carried out subsequently cannot be substituted for the requirement, recalled in paragraph 106 of this judgment, for a review that is independent and, except in duly justified urgent cases, undertaken beforehand.

113. Finally, the 2011 Act does not lay down any objective criteria which define precisely the conditions and circumstances in which national authorities must be granted access to data and the police officer responsible for processing the requests for access to retained data is solely competent, as Ireland confirmed at the hearing, to assess the suspicions that exist with respect to the persons concerned and the need for access to data that relate to them.

114. Consequently, the answer to the third question is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding

national legislation pursuant to which the centralised processing of requests for access to data retained by providers of electronic communications services, issued by the police in the context of the investigation or prosecution of serious criminal offences, is the responsibility of a police officer, who is assisted by a unit established within the police service which has a degree of autonomy in the exercise of its duties, and whose decisions may subsequently be subject to judicial review.

The fifth and sixth questions

115. By its fifth and sixth questions, which it is appropriate to examine together, the referring courts asks, in essence, whether EU law must be interpreted as meaning that a national court may limit the temporal effects of a declaration of invalidity which it is required to make, under national law, with respect to national legislation imposing on providers of electronic communications services the general and indiscriminate retention of traffic and location data owing to the incompatibility of that legislation with Article 15(1) of Directive 2002/58 read in the light of the Charter.

116. It is apparent from the information provided by the referring court that the national legislation at issue in the main proceedings, namely the 2011 Act, was adopted in order to transpose into national law Directive 2006/24, which was later declared invalid by the Court in its judgment of 8 April 2014, *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238).

117. In addition, the referring court states that, while the assessment of the admissibility of the evidence based on data retained pursuant to the 2011 Act and relied on as regards G.D. in the context of the criminal proceedings is a matter for the criminal court, it is nevertheless, in the context of the civil proceedings, its responsibility to rule on the validity of the provisions at issue of that act and on the temporal effects of a declaration of invalidity of those provisions. Thus, while the sole issue raised before the referring court is that of the validity of the provisions of the 2011 Act, that court considers however that it is necessary to inquire of the Court as to the effect of a possible finding of invalidity on the admissibility of the evidence obtained by means of the general and indiscriminate retention of data that that act permitted.

118. In the first place, it should be recalled that the principle of the primacy of EU law establishes the pre-eminence of EU law over the law of the Member States. That principle therefore requires all Member State bodies to give full effect to the various provisions of EU law, and the law of the Member States may not undermine the effect accorded to those various provisions in the territory of those States. In the light of that principle, where it is unable to interpret national legislation in compliance with the requirements of EU law, the national court which is called upon within the exercise of its jurisdiction to apply provisions of EU law is under a duty to give full effect to those provisions, if

necessary refusing of its own motion to apply any conflicting provision of national legislation, even if adopted subsequently, and it is not necessary for that court to request or await the prior setting aside of such provision by legislative or other constitutional means (see, to that effect, judgments of 15 July 1964, *Costa*, 6/64, EU:C:1964:66, p. 594; of 19 November 2019, *A. K. and Others (Independence of the Disciplinary Chamber of the Supreme Court)*, C-585/18, C-624/18 and C-625/18, EU:C:2019:982, paragraphs 157, 158 and 160; and of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 214 and 215).

119. Only the Court may, in exceptional cases, on the basis of overriding considerations of legal certainty, allow the temporary suspension of the ousting effect of a rule of EU law with respect to national law that is contrary thereto. Such a restriction on the temporal effects of the interpretation of that law, made by the Court, may be granted only in the actual judgment ruling upon the interpretation requested. The primacy and uniform application of EU law would be undermined if national courts had the power to give provisions of national law primacy in relation to EU law contravened by those provisions, even temporarily (judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 216 and 217 and the case-law cited).

120. It is true that the Court has held, in a case concerning the lawfulness of measures adopted in breach of the obligation under EU law to conduct a prior assessment of the impact of a project on the environment and on a protected site, that if domestic law allows it, a national court may, by way of exception, maintain the effects of such measures where such maintenance is justified by overriding considerations relating to the need to nullify a genuine and serious threat of interruption in the electricity supply in the Member State concerned, which cannot be remedied by any other means or alternatives, particularly in the context of the internal market, and continues only for as long as is strictly necessary to remedy the breach (see, to that effect, judgment of 29 July 2019, *Inter-Environnement Wallonie and Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU:C:2019:622, paragraphs 175, 176, 179 and 181).

121. However, unlike a breach of a procedural obligation such as the prior assessment of the impact of a project in the specific field of environmental protection, a failure to comply with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, cannot be remedied by a procedure comparable to the procedure referred to in the preceding paragraph (see, to that effect, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 219).

122. Maintaining the effects of national legislation such as the 2011 Act would mean that the legislation would continue to impose on providers of electronic communications services obligations which are contrary to EU law and which seriously interfere with the fundamental rights of the persons whose data have been retained (see, by analogy, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 219).

123. Therefore, the referring court cannot limit the temporal effects of a declaration of invalidity which it is bound to make under national law in respect of the national legislation at issue in the main proceedings (see, by analogy, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 220).

124. In that regard, as the Advocate General observed in essence in point 75 of his Opinion, the fact that that legislation was adopted in order to transpose Directive 2006/24 into national law is irrelevant since, due to the Court's decision that that directive was invalid, the invalidity has effect as from the date of its entry into force (see, to that effect, judgment of 8 February 1996, *FMC and Others*, C-212/94, EU:C:1996:40, paragraph 55), the validity of that national legislation must be assessed by the referring court in the light of Directive 2002/58 and the Charter, as interpreted by the Court.

125. As regards, more specifically, the interpretation of Directive 2002/58 and the Charter upheld by the Court in its judgments of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970), and of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), it should be recalled that, according to settled case-law, the interpretation that the Court gives to a rule of EU law, in the exercise of the jurisdiction conferred upon it by Article 267 TFEU, clarifies and defines the meaning and scope of that rule as it must be, or ought to have been, understood and applied from the time of its coming into force. It follows that the rule as thus interpreted may and must be applied by the courts to legal relationships arising and established before the judgment ruling on the request for interpretation, provided that in other respects the conditions for bringing an action relating to the application of that rule before the courts having jurisdiction are satisfied (judgment of 16 September 2020, *Romenergo and Aris Capital*, C-339/19, EU:C:2020:709, paragraph 47 and the case-law cited).

126. In that regard, it should also be stated that a temporal limitation of the effects of the interpretation given was not imposed in the judgments of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970), and of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), with the result that, in accordance with the case-

law recalled in paragraph 119 of this judgment, it should not be imposed in a judgment of the Court subsequent to those judgments.

127. Finally, as regards the effect of a declaration of the potential incompatibility of the 2011 Act with Directive 2002/58, read in the light of the Charter, on the admissibility of evidence relied on against G.D. in the context of the criminal proceedings, it suffices to refer to the Court's case-law on that subject, in particular the principles recalled in paragraphs 41 to 44 of the judgment of 2 March 2021, *Prokuratuur* (Conditions of access to data relating to electronic communications) (C-746/18, EU:C:2021:152), from which it follows that that admissibility is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, *inter alia*, with the principles of equivalence and effectiveness.

128. Having regard to the foregoing considerations, the answer to the fifth and sixth questions is that EU law must be interpreted as precluding a national court from limiting the temporal effects of a declaration of invalidity which it is bound to make, under national law, with respect to national legislation imposing on providers of electronic communications services the general and indiscriminate retention of traffic and location data, owing to the incompatibility of that legislation with Article 15(1) of Directive 2002/58 read in the light of the Charter. The admissibility of evidence obtained by means of such retention is, in accordance with the principle of procedural autonomy of the Member State, a matter for national law, subject to compliance, *inter alia*, with the principles of equivalence and effectiveness.

Costs

129. Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Grand Chamber) hereby rules:

1. Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding legislative measures which, as a preventive measure for the purposes of combating serious crime and preventing serious threats to public security, provide for

the general and indiscriminate retention of traffic and location data. However, that Article 15(1), read in the light of Articles 7, 8, 11 and 52(1) of the Charter of Fundamental Rights, does not preclude legislative measures that provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for

- the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;

- the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;

- the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and

- recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers,

provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.

2. Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation pursuant to which the centralised processing of requests for access to data, which have been retained by providers of electronic communications services, issued by the police in the context of the investigation or prosecution of serious criminal offences, is the responsibility of a police officer, who is assisted by a unit established within the police service which has a degree of autonomy in the exercise of its duties, and whose decisions may subsequently be subject to judicial review.

3. EU law must be interpreted as precluding a national court from limiting the temporal effects of a declaration of invalidity which it is bound to make, under national law, with respect to national legislation imposing on providers of electronic communications services the general and indiscriminate retention of traffic and location data, owing to the incompatibility of that legislation with Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of the Charter of Fundamental Rights. The admissibility of evidence obtained by means of such retention is,

in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, *inter alia*, with the principles of equivalence and effectiveness.

Delivered in open court in Luxembourg on 5 April 2022.

AVRUPA İNSAN HAKLARI MAHKEMESİ (AİHM) KARARLARI

Avrupa İnsan Hakları Mahkemesinin yeni teknolojileri doğrudan veya dolaylı ilgilendiren muhtelif içtihadı vardır. Bu bölümde Mahkemenin bu konuda yaptığı derleme kararlar yer almaktadır.³⁷

Factsheet - Personal data protection

January 2023

This factsheet does not bind the Court and is not exhaustive

New technologies

Electronic data

S. and Marper v. the United Kingdom

4 December 2008 (Grand Chamber)

This case concerned the indefinite retention in a database of the applicants' fingerprints, cell samples and DNA profiles³⁸ after criminal proceedings against them had been terminated by an acquittal in one case and discontinued in the other case.

The European Court of Human Right held that there had been a violation of Article 8 (right to respect for private life) of the European Convention on Human Rights. It considered in particular that the use of modern scientific techniques in the criminal- justice system could not be allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private- life interests. Any State claiming a pioneer role in the development of new technologies bore special responsibility for "striking the right balance". The Court concluded that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in this particular case, failed to strike a fair balance between the competing public and private interests.

B.B. v. France (application no. 5335/06), Gardel v. France and M.B. v. France (no.22115/06)

17 December 2009

³⁷ İçeriğin orjinal hali https://www.echr.coe.int/Documents/FS_Data_ENG.pdf adresinden erişilebilir.

³⁸ DNA profiles are digitised information which is stored electronically on the National DNA Database together with details of the person to whom it relates.

The three applicants - convicted of rape of 15 year-old minors by a person in a position of authority - complained, in particular, about their inclusion in the national Sex Offender Database.

The Court held that there had been no violation of Article 8 (right to respect for private life) of the Convention. It took the view that the length of the data conservation - 30 years maximum - was not disproportionate in relation to the aim pursued - prevention of crime - by the retention of the information. Moreover, the consultation of such data by the court, police and administrative authorities, was subject to a duty of confidentiality and was restricted to precisely determined circumstances.

Shimovolos v. Russia³⁹

21 June 2011

This case concerned the registration of a human rights activist in the so-called “surveillance database”, which collected information about his movements, by train or air, within Russia, and his arrest.

The Court held that there had been a violation of Article 8 (right to respect for private life) of the Convention. It observed that the creation and maintenance of the database and the procedure for its operation were governed by a ministerial order which had never been published or otherwise made accessible to the public. Consequently, the Court found that the domestic law did not indicate with sufficient clarity the scope and manner of exercise of the discretion conferred on the domestic authorities to collect and store information on individuals’ private lives in the database. In particular, it did not set out in a form accessible to the public any indication of the minimum safeguards against abuse. The Court also held that there had been a violation of Article 5 (right to liberty and security) of the Convention.

Mandil v. France, Barreau and Others v. France and Deceuninck v. France

13 November 2011 (decisions on the admissibility)

The applicants were “Faucheurs volontaires” (Volunteer Reapers) who had participated in digging up experimental crops of transgenic beetroot. The applicant in the first case complained about his conviction for refusing to provide a biological sample to be stored on the national computerised DNA database; the applicants in the second case argued that the storage of their DNA on the national computerised database and the conviction of a number of them for refusing to provide a biological

³⁹ On 16 September 2022 the Russian Federation ceased to be a Party to the European Convention on Human Rights (“the Convention”).

sample amounted to a violation of their right to respect for private life; the applicant in the third case submitted in particular that the order to take cell samples containing his genetic information constituted a disproportionate interference with his integrity and his private life.

The Court declared the applications inadmissible for failure to respect duty of confidentiality in friendly settlement negotiations. It considered that the applicants had violated the principle of confidentiality enshrined in Article 39 § 2 of the Convention and Rule 62 of the Rules of Court and that their conduct had constituted a violation of the right of individual petition for the purposes of Article 35 § 3 (a) of the Convention.

Robathin v. Austria

3 July 2012

A practising lawyer, the applicant complained about a search carried out in his office in 2006 and seizure of documents as well as all his electronic data following criminal proceedings brought against him on suspicion of theft, embezzlement and fraud of his clients. He was ultimately acquitted of all charges against him in 2011.

The Court held that there had been a violation of Article 8 (right to respect for correspondence) of the Convention. It observed in particular that, although the applicant had benefited from a number of procedural safeguards, the review chamber to which he had referred the case had given only brief and rather general reasons when authorising the search of all the electronic data from the applicant's law office, rather than data relating solely to the relationship between the applicant and the victims of his alleged offences. In view of the specific circumstances prevailing in a law office, particular reasons should have been given to allow such an all-encompassing search. In the absence of such reasons, the Court found that the seizure and examination of all the data had gone beyond what was necessary to achieve the legitimate aim.

Bernh Larsen Holding As and Others v. Norway

14 March 2013

This case concerned the complaint by three Norwegian companies about a decision of the tax authorities ordering tax auditors to be provided with a copy of all data on a computer server used jointly by the three companies. The applicant companies alleged in particular that the measure in question had been taken in an arbitrary manner.

The Court held that there had been no violation of Article 8 (right to respect for home and correspondence) of the Convention. It agreed with the Norwegian courts' argument that, for efficiency reasons, tax authorities' possibilities to act should not be limited by the fact that a tax payer was using a "mixed archive", even if that archive contained data belonging to other tax payers. Moreover, there were adequate safeguards against abuse.

M.K. v. France (no. 19522/09)

18 April 2013

The applicant, who had been the subject of two investigations concerning book theft, which ended in one case with his acquittal and in the other with a decision not to prosecute, complained of the fact that his fingerprints had been retained on a database by the French authorities.

The Court held that there had been a violation of Article 8 (right to respect for private life) of the Convention. It considered, in view of the circumstances of the case, that the retention of the data in question had amounted to disproportionate interference with the applicant's right to respect for his private life.

Youth Initiative For Human Rights v. Serbia 25 June 2013

This case concerned access to information obtained via electronic surveillance by the Serbian Intelligence Agency. The applicant NGO complained that the intelligence agency's refusal to provide it with the information it had requested - it had requested to be provided with information on how many people the agency had subjected to electronic surveillance in 2005 - prevented it from exercising its role as "public watchdog".

The Court held that there had been a violation of Article 10 (freedom of expression) of the Convention. It found that the agency's obstinate reluctance to comply with a final and binding order to provide information it had obtained was in defiance of domestic law and was tantamount to being arbitrary. Under Article 46 (binding force and implementation) of the Convention, the Court further held that the most natural way to implement its judgment in this case would be to ensure that the agency provided the applicant NGO with the information it had requested on how many people had been subjected to electronic surveillance in 2005.

Nagla v. Latvia

16 July 2013

This case concerned the search by the police of a well-known broadcast journalist's home, and their seizure of data storage devices. The applicant's home was searched following a broadcast she had aired in February 2010 informing the public of an information leak from the State Revenue Service database. The applicant complained that the search of her home meant that she had been compelled to disclose information that had enabled a journalistic source to be identified, violating her right to receive and impart information.

The Court held that there had been a violation of Article 10 (freedom of expression) of the Convention. It emphasised that the right of journalist's not to disclose their sources could not be considered a privilege, dependent on the lawfulness or unlawfulness of their sources, but rather as an intrinsic part of the right to information that should be treated with the utmost caution. In this case the investigating authorities had failed to properly balance the interest of the investigation in securing evidence against the public interest in protecting the journalist's freedom of expression.

Peruzzo and Martens v. Germany

4 June 2013 (decision on the admissibility)

The applicants, who had been convicted of serious criminal offences, complained about the domestic courts' orders to collect cellular material from them and to store it in a database in the form of DNA profiles for the purpose of facilitating the investigation of possible future crimes.

The Court declared the application inadmissible as being manifestly ill-founded. The measures complained of were found to constitute a proportionate interference with the applicants' right to respect for their private life and were necessary in a democratic society.

Brunet v. France

18 September 2014

The applicant complained in particular of an interference with his private life as a result of being added to the police database STIC (system for processing recorded offences) - containing information from investigation reports, listing the individuals implicated and the victims - after the discontinuance of criminal proceedings against him.

The Court held that there had been a violation of Article 8 (right to respect for private life) of the Convention, finding that the French State had overstepped its discretion ("margin of appreciation") to decide on such matters: the retention could be regarded as a disproportionate breach of the applicant's right to respect for his private life and was not necessary in a democratic society. The

Court considered in particular that the applicant had not had a real possibility of seeking the deletion from the database of the information concerning him and that the length of retention of that data, 20 years, could be assimilated, if not to indefinite retention, at least to a norm rather than to a maximum limit.

Servulo & Associados - Sociedade de Advogados, RL v. Portugal

3 September 2015

This case concerned the search of a law firm's offices and the seizure of computer files and email messages, during an investigation into suspected corruption, acquisition of prohibited interests and money laundering in connection with the purchase by the Portuguese Government of two submarines from a German consortium.

The Court held that there had been no violation of Article 8 (right to respect for private life and correspondence) of the Convention. It found that, notwithstanding the scope of the search and seizure warrants, the safeguards afforded to the applicants against abuse, arbitrariness and breaches of legal professional secrecy had been adequate and sufficient. Hence, the search and seizure operations had not amounted to disproportionate interference with the legitimate aim pursued. The Court observed in particular that, after viewing the computer files and emails that had been seized, the investigating judge from the Central Criminal Investigation Court had ordered the deletion of 850 records which he considered to be private, to be covered by professional secrecy or to have no direct bearing on the case. The Court saw no reason to call into question the assessment made by the judge, who had intervened to review the lawfulness of the search and seizure operations and especially to protect legal professional secrecy. Moreover, in response to the applicants' objection that the computer records seized had not been returned to them, the Court noted that the originals had been given back and that there was no obligation to return the copies, which could be retained throughout the limitation period for the crimes in question.

Szabo and Vissy v. Hungary

12 January 2016

This case concerned Hungarian legislation on secret anti-terrorist surveillance introduced in 2011. The applicants complained in particular that they could potentially be subjected to unjustified and disproportionately intrusive measures within the Hungarian legal framework on secret surveillance for national security purposes (namely, "section 7/E (3) surveillance"). They notably alleged that this legal framework was prone to abuse, notably for want of judicial control.

In this case the Court held that there had been a violation of Article 8 of the Convention. It accepted that it was a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies, including massive monitoring of communications, in pre-empting impending incidents. However, the Court was not convinced that the legislation in question provided sufficient safeguards to avoid abuse. Notably, the scope of the measures could include virtually anyone in Hungary, with new technologies enabling the Government to intercept masses of data easily concerning even persons outside the original range of operation. Furthermore, the ordering of such measures was taking place entirely within the realm of the executive and without an assessment of whether interception of communications was strictly necessary and without any effective remedial measures, let alone judicial ones, being in place. The Court further held that there had been no violation of Article 13 (right to an effective remedy) of the Convention taken together with Article 8, reiterating that Article 13 could not be interpreted as requiring a remedy against the state of domestic law.

Trabajo Rueda v. Spain

30 May 2017

This case concerned the seizure of the applicant's computer on the grounds that it contained child pornography material. The applicant complained that the police seizure and inspection of his computer had amounted to an interference with his right to respect for his private life and correspondence.

The Court held that there had been a violation of Article 8 (right to respect for private life) of the Convention. It first noted that the police access to files in the applicant's personal computer and his conviction had amounted to an interference with his right to respect for his private life. That interference was prescribed by domestic law. It also pursued the legitimate aim of "prevention of crime" and "protection of the rights of others". In this respect, the Court emphasised in particular that "sexual abuse is unquestionably an abhorrent type of wrongdoing, with debilitating effects on its victims" and that "children and other vulnerable individuals are entitled to State protection, in the form of effective deterrence, from such grave types of interference with essential aspects of their private lives". However, the Court deemed that the police seizure of the computer and inspection of the files which it contained, without prior judicial authorisation, had not been proportionate to the legitimate aims pursued and had not been "necessary in a democratic society". It found that it was difficult to assess the urgency of the situation requiring the police to seize the files from the applicant's personal computer and to access their content, bypassing the normal requirement of prior judicial

authorisation, when in fact the computer in question was already in the hands of the police and prior authorisation could have been obtained fairly quickly without impeding the police inquiries.

Dagregorio and Mosconi v. France

30 May 2017 (decision on the admissibility)

The applicants are two trade unionists who took part in the occupation and immobilisation of the Societe nationale Corse Mediterranee (SNCM) ferry "Pascal Paoli" during the company takeover by a financial operator. The case concerned their refusal to undergo biological testing, the results of which were to be included in the national computerised DNA database (FNAEG). The applicants, having been convicted at first instance and on appeal, did not lodge an appeal on points of law.

The Court declared the application inadmissible for non-exhaustion of domestic remedies. It emphasised in particular that in the absence of any judicial precedent applicable to the applicants' situation, there was doubt as to the effectiveness of an appeal on points of law owing to a decision given by the Constitutional Council. The Court considered that it was therefore a point which should have been submitted to the Court of Cassation. The mere fact of harbouring doubts as to the prospects of a given appeal succeeding was not sufficient reason for omitting to use the remedy in question.

Aycaguer v. France

22 June 2017

The applicant alleged that there had been a breach of his right to respect for his private life on account of the order to provide a biological sample for inclusion in the national computerised DNA database (FNAEG) and the fact that his refusal to comply with that order had resulted in a criminal conviction.

The Court held that there had been a violation of Article 8 (right to respect for private life) of the Convention. It observed in particular that on 16 September 2010 the Constitutional Council had given a decision to the effect that the provisions on the FNAEG were in conformity with the Constitution, subject inter alia to "determining the duration of storage of such personal data depending on the purpose of the file stored and the nature and/or seriousness of the offences in question". The Court noted that, to date, no appropriate action had been taken on that reservation and that there was currently no provision for differentiating the period of storage depending on the nature and gravity of the offences committed. The Court also ruled that the regulations on the storage of DNA profiles in the FNAEG did not provide the data subjects with sufficient protection, owing to its duration and the fact that the data could not be deleted. The regulations therefore failed to strike a fair balance between the competing public and private interests.

Ivashchenko v. Russia⁴⁰

13 February 2018

This case concerned the copying of the data from a photojournalist's laptop by Russian customs officials.

The Court held that there had been a violation of Article 8 (right to respect for private life) of the Convention, finding that, overall, the Russian Government had not shown that the legislation and practice applied in the case had provided the necessary safeguards against abuse when it came to applying the customs sampling procedure for electronic data contained in an electronic device.

Libert v. France

22 February 2018

This case concerned the dismissal of an SNCF (French national railway company) employee after the seizure of his work computer had revealed the storage of pornographic files and forged certificates drawn up for third persons. The applicant complained in particular that his employer had opened, in his absence, personal files stored on the hard drive of his work computer.

The Court held that there had been no violation of Article 8 (right to respect for private life) of the Convention, finding that in the present case the French authorities had not overstepped the margin of appreciation available to them. The Court noted in particular that the consultation of the files by the applicant's employer had pursued a legitimate aim of protecting the rights of employers, who might legitimately wish to ensure that their employees were using the computer facilities which they had placed at their disposal in line with their contractual obligations and the applicable regulations. The Court also observed that French law comprised a privacy protection mechanism allowing employers to open professional files, although they could not surreptitiously open files identified as being personal. They could only open the latter type of files in the employee's presence. The domestic courts had ruled that the said mechanism would not have prevented the employer from opening the files at issue since they had not been duly identified as being private. Lastly, the Court considered that the domestic courts had properly assessed the applicant's allegation of a violation of his right to respect for his private life, and that those courts' decisions had been based on relevant and sufficient grounds.

Catt v. the United Kingdom

⁴⁰ On 16 September 2022 the Russian Federation ceased to be a Party to the Convention.

24 January 2019

This case concerned the complaint of the applicant, a lifelong activist, about the collection and retention of his personal data in a police database for “domestic extremists”.

The Court held that there had been a violation of Article 8 (right to respect for private life) of the Convention. It found in particular that the data held on the applicant concerned his political views and that such information required particular protection. The Court also had regard to the applicant’s age (94), and the fact he had no history or prospect of committing acts of violence. The Court further noted that, while collecting the information on him had been justified, retaining it had not, particularly owing to a lack of safeguards, such as time-limits.

Buturuga v. Romania

11 February 2020

This case concerned allegations of domestic violence and of violation of the confidentiality of electronic correspondence by the former husband of the applicant, who complained of shortcomings in the system for protecting victims of this type of violence. The applicant complained in particular of the ineffectiveness of the criminal investigation into the domestic violence which she claimed to have suffered. She also complained that her personal safety had not been adequately secured, and criticised the authorities’ refusal to consider her complaint concerning her former husband’s breach of the confidentiality of her correspondence.

The Court held that there had been a violation of Article 3 (prohibition of inhuman or degrading treatment) and Article 8 (right to respect for private life and correspondence) of the Convention on account of the State’s failure to fulfil its positive obligations under those provisions. It found in particular that the national authorities had not addressed the criminal investigation as raising the specific issue of domestic violence, and that they had thereby failed to provide an appropriate response to the seriousness of the facts complained of by the applicant. The investigation into the acts of violence had been defective, and no consideration had been given to the merits of the complaint regarding violation of the confidentiality of correspondence, which was closely linked to the complaint of violence. On that occasion the Court lastly pointed out that cyberbullying was currently recognised as an aspect of violence against women and girls, and that it could take on a variety of forms, including cyber breaches of privacy, intrusion into the victim’s computer and the capture, sharing and manipulation of data and images, including private data.

Gaughran v. the United Kingdom

13 February 2020

This case concerned a complaint about the indefinite retention of personal data (DNA profile, fingerprints and photograph) of a man who had a spent conviction for driving with excess alcohol in Northern Ireland.

The Court held that there had been a violation of Article 8 (right to respect for private life) of the Convention, finding that the United Kingdom had overstepped the acceptable margin of appreciation and the retention at issue constituted a disproportionate interference with the applicant's right to respect for private life, which could not be regarded as necessary in a democratic society. The Court underlined in particular that it was not the duration of the retention of data that had been decisive, but the absence of certain safeguards. In the applicant's case his personal data had been retained indefinitely without consideration of the seriousness of his offence, the need for indefinite retention and without any real possibility of review. Noting also that the technology being used had been shown to be more sophisticated than that considered by the domestic courts in this case, particularly regarding storage and analysis of photographs, the Court considered that the retention of the applicant's data had failed to strike a fair balance between the competing public and private interests.

Privacy International and Others v. the United Kingdom

7 July 2020 (*decision on the admissibility*)

The applicants - an NGO registered in London, an Internet service provider registered in London, an association of "hacktivists" registered in Germany, two companies registered in the United States providing Internet services and communications services respectively, and an Internet service provider registered in South Korea - believed that their equipment had been subject to interference, colloquially known as "hacking", over an undefined period by the United Kingdom Government Communications Headquarters and/or the Secret Intelligence Service. They complained in particular that the power under Section 7 of the Intelligence Services Act⁴¹ was not in accordance with the law, that it contained no requirement for judicial authorisation, that there was no information in the public domain about how it might be used to authorise Equipment Interference, and that there was no requirement for filtering to exclude irrelevant material. They added that the Investigatory Powers

⁴¹ Section 7 of the Intelligence Services Act 1994 ("the ISA") allows the Secretary of State to authorise a person to undertake (and to exempt them from liability for) an act outside the British Islands in relation to which they would be liable if it were done in the United Kingdom.

Tribunal did not provide an effective remedy as it did not rule on the Section 7 regime in the domestic litigation.

The Court declared the applicants' complaints under Article 8 (right to respect for private life and correspondence), Article 10 (freedom of expression) and Article 13 (right to an effective remedy) of the Convention inadmissible, finding that, in the circumstances of the case, the applicants had not provided the domestic courts, notably the Investigatory Powers Tribunal, with the opportunity which is in principle intended by Article 35 (admissibility criteria) of the Convention to be afforded to a Contracting State, namely the opportunity of addressing, and thereby preventing or putting right, the particular Convention violation alleged against it. The Court noted in particular the general arguments advanced by the applicants and also underlined in the interventions of the third parties that the surveillance complained of was particularly intrusive and that there was a need for safeguards in this domain. In that respect, it recalled the importance of examining compliance with the principles of Article 8 of the Convention where the powers vested in the State are obscure, creating a risk of arbitrariness especially where the technology available is continually becoming more sophisticated. However, that importance reinforced in the context of exhaustion of domestic remedies the need to provide the domestic courts with the possibility to rule on such matters where they have the potential to do so.

Big Brother Watch and Others v. the United Kingdom

25 May 2021 (Grand Chamber)

These applications were lodged after revelations by Edward Snowden (former contractor with the US National Security Agency) about programmes of surveillance and intelligence sharing between the USA and the United Kingdom. The case concerned complaints by journalists and human-rights organisations in regard to three different surveillance regimes: (1) the bulk interception of communications; (2) the receipt of intercept material from foreign governments and intelligence agencies; (3) the obtaining of communications data from communication service providers⁴².

The Grand Chamber held: unanimously, that there had been a violation of Article 8 (right to respect for private and family life/communications) of the Convention in respect of the bulk intercept regime;

⁴² At the relevant time, the regime for bulk interception and obtaining communications data from communication service providers had a statutory basis in the Regulation of Investigatory Powers Act 2000. This had since been replaced by the Investigatory Powers Act 2016. The findings of the Grand Chamber relate solely to the provisions of the 2000 Act, which had been the legal framework in force at the time the events complained of had taken place.

unanimously, that there had been a violation of Article 8 in respect of the regime for obtaining communications data from communication service providers; by twelve votes to five, that there had been no violation of Article 8 in respect of the United Kingdom's regime for requesting intercepted material from foreign Governments and intelligence agencies; unanimously, that there had been a violation of Article 10 (freedom of expression) of the Convention, concerning both the bulk interception regime and the regime for obtaining communications data from communication service providers; and, by twelve votes to fives, that there had been no violation of Article 10 in respect of the regime for requesting intercepted material from foreign Governments and intelligence agencies. The Court considered in particular that, owing to the multitude of threats States face in modern society, operating a bulk interception regime did not in and of itself violate the Convention. However, such a regime had to be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation were being defined; and that the operation should be subject to supervision and independent ex post facto review. Having regard to the bulk interception regime operated in the UK, the Court identified the following deficiencies: bulk interception had been authorised by the Secretary of State, and not by a body independent of the executive; categories of search terms defining the kinds of communications that would become liable for examination had not been included in the application for a warrant; and search terms linked to an individual (that is to say specific identifiers such as an email address) had not been subject to prior internal authorisation. The Court also found that the bulk interception regime had not contained sufficient protections for confidential journalistic material. The regime for obtaining communications data from communication service providers was also found to have not been in accordance with the law. However, the Court held that the regime by which the UK could request intelligence from foreign governments and/or intelligence agencies had had sufficient safeguards in place to protect against abuse and to ensure that UK authorities had not used such requests as a means of circumventing their duties under domestic law and the Convention.

Centrum För Rättvisa v. Sweden

25 May 2021 (Grand Chamber)

This case concerned the alleged risk that the applicant foundation's communications had been or would be intercepted and examined by way of signals intelligence, as it communicated on a daily

basis with individuals, organisations and companies in Sweden and abroad by email, telephone and fax, often on sensitive matters.

The Grand Chamber held, by fifteen votes to two, that there had been a violation of Article 8 (right to respect for private and family life, the home and correspondence) of the Convention. It found, in particular, that although the main features of the Swedish bulk interception regime met the Convention requirements on quality of the law, the regime nevertheless suffered from three defects: the absence of a clear rule on destroying intercepted material which did not contain personal data; the absence of a requirement in the Signals Intelligence Act or other relevant legislation that, when making a decision to transmit intelligence material to foreign partners, consideration was given to the privacy interests of individuals; and the absence of an effective ex post facto review. As a result of these deficiencies, the system did not meet the requirement of “end-to-end” safeguards, it overstepped the margin of appreciation left to the respondent State in that regard, and overall did not guard against the risk of arbitrariness and abuse.

Nuh Uzun and Others v. Turkey

29 March 2022

At the time of the events the fourteen applicants were detained in various prisons in Turkey in connection with alleged membership of a terrorist organisation, following the attempted military coup of 15 July 2016. The case mainly concerned the uploading of their correspondence, while they were in detention, onto the National Judicial Network Server (“UYAP”).

The Court held that there had been a violation of Article 8 (right to respect for private life/right to respect for correspondence) of the Convention, finding that the interference with the applicants’ right to respect for their private life and correspondence could not be said to have been “in accordance with the law”. It noted, in particular, that the uploading of the correspondence of remand and convicted prisoners onto the UYAP server stemmed directly and specifically from an instruction issued by the Ministry of Justice in October 2016 and reissued in March 2017. That instruction had been addressed to the public prosecutors and prison authorities. The documents in question were therefore unpublished internal documents which as a matter of principle did not have binding force. In the Court’s view, texts of this kind, which were not issued under any rule-making powers, could not be regarded as “law” of sufficient “quality” for the purposes of the Court’s case-law.

See also, recently:

Ringler v. Austria

12 May 2020 (*Committee - decision on the admissibility*)

Tretter and Others v. Austria

29 September 2020 (*Committee - decision on the admissibility*)

Pending applications

Association confraternelle de la presse judiciaire v. France and 11 other applications (nos. 49526/15, 49615/15, 49616/15, 49617/15, 49618/15, 49619/15, 49620/15, 49621/15, 55058/15, 55061/15, 59602/15 and 59621/15)

Applications communicated to the French Government on 26 April 2017

These applications, which were lodged by lawyers and journalists, as well as legal persons connected with these professions, concern the French Intelligence Act of 24 July 2015.

The Court gave notice of the applications to the French Government and put questions to the parties under Articles 8 (right to respect for private life and correspondence), 10 (freedom of expression) and 13 (right to an effective remedy) of the Convention.

Similar applications pending: Follorou v. France (no. 30635/17) and Johannes v. France (no. 30636/17), communicated to the French Government on 4 July 2017.

E-mail

Copland v. the United Kingdom

3 April 2007

The applicant was employed by a college of further education, a statutory body administered by the State, as a personal assistant to the principal. From the end of 1995 she was required to work closely with the deputy principal. Her telephone, e-mail and internet usage were subjected to monitoring at the deputy principal's instigation. According to the UK Government, this was in order to ascertain whether the applicant was making excessive use of college facilities for personal purposes.

The Court held that there had been a violation of Article 8 (right to respect for private life and correspondence) of the Convention. It first observed that telephone calls from business premises were *prima facie* covered by the notions of "private life" and "correspondence". It followed logically that e-mails sent from work should be similarly protected, as should information derived from the monitoring of personal internet usage. In the instant case, the Court considered that the collection and storage of personal information relating to the applicant's use of the telephone, e-mail and internet,

without her knowledge, had amounted to an interference with her right to respect for her private life and correspondence. While leaving open the question whether the monitoring of an employee's use of a telephone, e-mail or internet at the place of work might be considered "necessary in a democratic society" in certain situations in pursuit of a legitimate aim, the Court concluded that, in the absence of any domestic law regulating monitoring at the material time, the interference was not "in accordance with the law".

Muscio v. Italy

13 November 2007 (decision on the admissibility)

This case concerned the president of a Catholic parents' association who had received unsolicited e-mails (spam) of an obscene nature. Having instituted proceedings against a person or persons unknown, he contested the decision to take no further action on his complaint.

The Court declared inadmissible, as being manifestly ill-founded, the applicant's complaint under Article 8 (right to respect for private and family life) of the Convention. It considered that receiving undesirable messages amounted to interference with the right to respect for private life. However, once connected to the Internet, e-mail users no longer enjoyed effective protection of their privacy and exposed themselves to the risk of receiving undesirable messages. In that context, the legal action brought by the applicant had had no chance of succeeding, since the national authorities and Internet service providers encountered objective difficulties in combating spam. The Court could not therefore require the State to make additional efforts to discharge its positive obligations under Article 8 of the Convention.

Benediktsdottir v. Iceland

16 June 2009 (decision on the admissibility)

The applicant complained that, by affording her insufficient protection against unlawful publication of her private e-mails in the media, Iceland had failed to secure her right to respect for private life and correspondence. She submitted that an unknown third party had obtained the e-mails in question, without her knowledge and consent from a server formerly owned and operated by her former employer who had gone bankrupt. The communications consisted in particular of direct quotations or paraphrasing of e-mail exchanges between the applicant and the former colleague of a multinational company's Chief Executive Officer and his wishes to find a suitable lawyer to assist him in handing over to the police allegedly incriminating material he had in his possession and to represent him in a future court case against the leaders of the multinational company in question. At

the time there was an ongoing public debate in Iceland relating to allegations that undue influence had been exerted by prominent figures on the most extensive criminal investigations ever carried out in the country.

The Court declared the application inadmissible as being manifestly ill-founded. It found that there was nothing to indicate that the Icelandic authorities had transgressed their margin of appreciation and had failed to strike a fair balance between the newspaper's freedom of expression and the applicant's right to respect for her private life and correspondence under Article 8 of the Convention.

Helander v. Finland

10 September 2013 (decision on the admissibility)

This case concerned a complaint brought by a prisoner that the prison authority had refused to forward legal correspondence to him, which had been sent to the prison's official e-mail address by his lawyer.

The Court declared the case inadmissible, as being manifestly ill-founded, as the applicant's lawyer had immediately been informed that his e-mail would not be conveyed to his client and that lawyer and client remained able at all times to communicate quickly by telephone, letter or personal visit. The Court also recognised that, under Finland's current legislation, lawyer-client confidentiality could not be guaranteed in e-mail correspondence, and that the prison authority therefore had a genuine reason for not forwarding the message on.

Servulo & Associados - Sociedade de Advogados, RL v. Portugal

3 September 2015

See above, under "Electronic data".

M.P. v. Portugal (no. 27516/14)

7 September 2021

The applicant's former husband accessed emails that she had exchanged on a dating site and produced them, without her consent, in the context, firstly, of proceedings that he had brought for shared parental responsibility and, secondly, divorce proceedings. The Family Affairs Court did not ultimately take these emails into consideration. The applicant complained about the fact that the courts had not punished her husband for disclosing them.

The Court held that there had been no violation of Article 8 (right to respect for private life and correspondence) of the Convention, finding that the Portuguese State had discharged its positive

obligation to protect the applicant's rights to respect for her private life and the confidentiality of her correspondence. It noted, in particular, that the effects of the disclosure of the emails in question on the applicant's private life had been limited, as they had been disclosed only in the civil proceedings, and public access to files in this type of proceedings was limited. The Court also noted that these emails had not ultimately been examined, since the Family Affairs Court had not actually ruled on the merits of the husband's requests. In the Court's view, the Portuguese authorities had balanced the competing interests, in compliance with the criteria laid down in its case-law. In addition, given that the applicant had waived the right to any civil claims in the context of the criminal proceedings, the only question which remained to be decided was that of the husband's criminal liability, a matter on which the Court could not rule.

GPS (Global Positioning System)

Uzun v. Germany

2 September 2010

The applicant, suspected of involvement in bomb attacks by a left-wing extremist movement, complained in particular that his surveillance via GPS and the use of the data obtained thereby in the criminal proceedings against him had violated his right to respect for private life.

The Court held that there had been no violation of Article 8 (right to respect for private life) of the Convention. Given that the criminal investigation had concerned very serious crimes, it found that the GPS surveillance of the applicant had been proportionate.

Ben Faiza v. France

8 February 2018

This case concerned surveillance measures taken against the applicant in a criminal investigation into his involvement in drug-trafficking offences. The applicant alleged that these measures (both the installation of a geolocation device on his vehicle and the court order issued to a mobile telephone operator to obtain records of his incoming and outgoing calls, together with the cell tower pings from his telephones, thus enabling the subsequent tracking of his movements) had constituted an interference with his right to respect for his private life.

The Court held that there had been a violation of Article 8 (right to respect for private life) of the Convention as regards the real-time geolocation of the applicant's vehicle by means of a GPS device on 3 June 2010, finding that, in the sphere of real-time geolocation measures, French law (neither

statute law nor case-law) did not at the relevant time indicate with sufficient clarity to what extent and how the authorities were entitled to use their discretionary power. The applicant had therefore not enjoyed the minimum protection afforded by the rule of law in a democratic society. The Court noted, however, that subsequently France had adopted a legislative mechanism governing the use of geolocation and strengthening the right to respect for privacy (Law of 28 March 2014). The Court further held that there had been no violation of Article 8 concerning the court order issued to a mobile telephone operator on 24 July 2009 to obtain the list of cell towers pinged by the applicant's phone for subsequent tracking of his movements. It noted in particular that the court order had constituted an interference with the applicant's private life but was in accordance with the law. Further, the order had been aimed at establishing the truth in the context of criminal proceedings for the importing of drugs in an organised gang, criminal conspiracy and money laundering, and had thus pursued the legitimate aims of preventing disorder or crime or protecting public health. The Court also considered that the measure had been necessary in a democratic society because it was aimed at breaking up a major drug-trafficking operation. Lastly, the information obtained had been used in an investigation and a criminal trial during which the applicant had been guaranteed an effective review consistent with the rule of law.

Internet⁴³

Perrin v. the United Kingdom

18 October 2005 (decision on the admissibility)

The case concerned the conviction and sentencing to 30 months' imprisonment of a French national based in the United Kingdom - and operating a United States-based Internet company with sexually explicit content - for publishing obscene articles on Internet.

The Court rejected the applicant's complaint under Article 10 (freedom of expression) of the Convention as inadmissible (manifestly ill-founded). It was satisfied that the criminal conviction was necessary in a democratic society in the interests of the protection of morals and/or the rights of others and that the sentence was not disproportionate.

Paeffgen GmbH v. Germany

18 September 2007 (decision on the admissibility)

⁴³ See also the factsheet on "Access to Internet and freedom to impart information".

The case concerned proceedings brought against the applicant company, engaged in e-commerce, by other companies and private individuals claiming that its registration and use of certain Internet domains breached their trademark rights and / or their rights to a (business) name.

The Court declared inadmissible, as being manifestly ill-founded, the applicant company's complaint under Article 1 (protection of property) of Protocol No. 1 to the Convention. It found that the court orders requiring the applicant company to cancel the domains had struck a fair balance between the protection of its possessions and the requirements of the general interest (i.e. to prevent the company from continuing to violate third parties' trademark rights).

K.U. v. Finland (application no. 2872/02)

2 December 2008

This case concerned an advertisement of a sexual nature posted about a 12-year old boy on an Internet dating site. Under Finnish legislation in place at the time⁴⁴, the police and the courts could not require the Internet provider to identify the person who had posted the ad. In particular, the service provider refused to identify the person responsible, claiming it would constitute a breach of confidentiality.

The Court held that there had been a violation of Article 8 (right to respect for private and family life) of the Convention. It considered that posting the ad was a criminal act which made a minor a target for paedophiles. The legislature should have provided a framework for reconciling the confidentiality of Internet services with the prevention of disorder or crime and the protection of the rights and freedoms of others, and in particular children and other vulnerable individuals.

Times Newspapers Ltd v. the United Kingdom (nos. 1 & 2)

10 March 2009

The applicant company, owner and publisher of The Times newspaper, alleged that the rule under United Kingdom law, whereby a new cause of action in libel proceedings accrues each time defamatory material on the Internet is accessed ("the Internet publication rule"), constituted an unjustifiable and disproportionate restriction on its right to freedom of expression. In December 1999 the applicant newspaper published two articles that were allegedly defamatory of a private individual. Both articles were uploaded onto The Times' website on the same day as they were published in the paper version of the newspaper. During the subsequent libel proceedings against the

⁴⁴ A legal framework had been introduced by the time of the European Court of Human Rights' judgment under the Exercise of Freedom of Expression in Mass Media Act.

applicant newspaper, it was required to add a notice to both articles in the Internet archive announcing that they were subject to libel litigation and were not to be reproduced or relied on without reference to the applicant company's legal department.

In this judgment the Court underlined that, in the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general. In the present case, it found that there had been no violation of Article 10 (freedom of expression) of the Convention: since the archives were managed by the newspaper itself and the domestic courts had not suggested that the articles be removed altogether, the requirement to add an appropriate qualification to the Internet version had not been disproportionate.

Willem v. France

16 July 2009

This case concerned the call for a boycott of Israeli products by a mayor, notably via the municipality's internet site. The mayor was subsequently convicted of provoking discrimination.

The Court found that there had been no violation of Article 10 (freedom of expression) of the Convention. The reasons given by the French courts to justify the interference with the applicant's freedom of expression had been "relevant and sufficient" for the purposes of Article 10. In addition, the fine imposed had been relatively moderate and proportionate to the aim pursued.

Renaud v. France

25 February 2010

The applicant complained of his conviction for defaming and publicly insulting a mayor on the Internet site of the association of which he was president and webmaster.

The Court held that there had been a violation of Article 10 (freedom of expression) of the Convention. It considered that the applicant's conviction had been disproportionate to the legitimate aim of protecting the reputation and rights of others.

Editorial Board of Pravoye Delo and Shtekel v. Ukraine

5 May 2011

This case mainly concerned the lack of adequate safeguards in Ukrainian law for journalists' use of information obtained from the Internet. In particular, defamation proceedings had been brought against a local newspaper and its editor-in-chief following their publication of a letter downloaded

from the Internet alleging that senior local officials were corrupt and involved with the leaders of an organised criminal gang. The domestic courts ruled against the applicants and ordered them to publish an apology and pay 15,000 Ukrainian hryvnias (approximately EUR 2,394), eventually waived via a friendly settlement.

The Court held that the order to the editor-in-chief to apologise had not been done in accordance with the law, and had, therefore, been in violation of Article 10 (freedom of expression) of the Convention. It further held that there had been a violation of Article 10 because of the lack of adequate safeguards for journalists using information obtained from the Internet. Notably, “having regard to the role the Internet plays in the context of professional media activities ... and its importance for the exercise of the right to freedom of expression generally ..., the Court consider[ed] that the absence of a sufficient legal framework at the domestic level allowing journalists to use information obtained from the Internet without fear of incurring sanctions seriously hinders the exercise of the vital function of the press as a ‘public watchdog’ ...” (§ 64 of the judgment).

Mosley v. the United Kingdom

10 May 2011

This case concerned the publication of articles, images and video footage in the News of the World newspaper and on its website which disclosed details of Max Mosley’s sexual activities. The applicant complained about the authorities’ failure to impose a legal duty on the newspaper to notify him in advance of further publication of the material so that he could seek an interim injunction.

The Court found that there had been no violation of Article 8 (right to respect for private life) of the Convention. It held in particular that the European Convention on Human Rights did not require media to give prior notice of intended publications to those who feature in them.

Ahmet Yıldırım v. Turkey

18 December 2012

This case concerned a court decision to block access to Google Sites, which hosted an Internet site whose owner was facing criminal proceedings for insulting the memory of Atatürk. As a result of the decision, access to all other sites hosted by the service was blocked. The applicant complained that he was unable to access his own Internet site because of this measure ordered in the context of criminal proceedings without any connection to him or his site. He submitted that the measure infringed his right to freedom to receive and impart information and ideas.

The Court held that there had been a violation of Article 10 (freedom of expression) of the Convention. It found that the effects of the measure in question had been arbitrary and the judicial review of the blocking of access had been insufficient to prevent abuses.

Ashby Donald and Others v. France

10 January 2013

This case concerned the conviction of fashion photographers for copyright infringement following the publication on the Internet site of a fashion company run by two of the applicants, without the authorisation of the fashion houses concerned, of photos taken by the other applicant at fashion shows in 2003.

The Court held that there had been no violation of Article 10 (freedom of expression) of the Convention. In the circumstances of the case and regard being had to the particularly wide margin of appreciation open to the domestic authorities, the nature and gravity of the penalties imposed on the applicants were not such that the Court could find that the interference in issue was disproportionate to the aim pursued.

Neij and Sunde Kolmisoppi v. Sweden

19 February 2013 (decision on the admissibility)

This case concerned the complaint by two of the co-founders of "The Pirate Bay", one of the world's largest websites for sharing torrent files, that their conviction for complicity to commit crimes in violation of the Copyright Act had breached their freedom of expression.

The Court declared the application inadmissible as being manifestly ill-founded. It held that sharing, or allowing others to share, files of this kind on the Internet, even copyright-protected material and for profit-making purposes, was covered by the right to "receive and impart information" under Article 10 (freedom of expression) of the Convention. However, it considered that the domestic courts had rightly balanced the competing interests at stake - i.e. the right of the applicants to receive and impart information and the necessity to protect Copyright - when convicting the applicants.

Akdeniz v. Turkey

11 March 2014 (decision on the admissibility)

This case concerned the blocking of access to two websites on the grounds that they streamed music without respecting copyright legislation. The applicant, who had applied to the European Court of

Human Rights as a user of the websites in question, complained in particular of a violation of his freedom of expression.

The Court declared the application inadmissible (incompatible *ratione personae*), finding that the applicant could not claim to be a “victim” in the sense of Article 34 (right of individual application) of the Convention. While stressing that the rights of internet users are of paramount importance, the Court nevertheless noted that the two music streaming websites had been blocked because they operated in breach of copyright law. As a user of these websites, the applicant had benefited from their services, and he had only been deprived of one way among others of listening to music. The Court further observed that the applicant had at his disposal many means to access to a range of musical works, without thereby contravening the rules governing copyright.

Delfi AS v. Estonia

16 June 2015 (Grand Chamber)

This was the first case in which the Court had been called upon to examine a complaint about liability for user-generated comments on an Internet news portal. The applicant company, which runs a news portal run on a commercial basis, complained that it had been held liable by the national courts for the offensive comments posted by its readers below one of its online news articles about a ferry company. At the request of the lawyers of the owner of the ferry company, the applicant company removed the offensive comments about six weeks after their publication.

The Court held that there had been no violation of Article 10 (freedom of expression) of the Convention, finding that the Estonian courts’ finding of liability against the applicant company had been a justified and proportionate restriction on the portal’s freedom of expression, in particular, because: the comments in question had been extreme and had been posted in reaction to an article published by the applicant on its professionally managed news portal run on a commercial basis; the steps taken by the applicant to remove the offensive comments without delay after their publication had been insufficient; and the 320 euro fine had by no means been excessive for the applicant, one of the largest Internet portals in Estonia.

Cengiz and Others v. Turkey

1 December 2015

This case concerned the blocking of access to YouTube, a website enabling users to send, view and share videos. The applicants complained in particular of an infringement of their right to freedom to receive and impart information and ideas.

The Court held that there had been a violation of Article 10 (freedom of expression) of the Convention, finding in particular that the applicants, all academics in different universities, had been prevented from accessing YouTube for a lengthy period of time and that, as active users, and having regard to the circumstances of the case, they could legitimately claim that the blocking order in question had affected their right to receive and impart information and ideas. The Court also observed that YouTube was a single platform which enabled information of specific interest, particularly on political and social matters, to be broadcast and citizen journalism to emerge. The Court further found that there was no provision in the law allowing the domestic courts to impose a blanket blocking order on access to the Internet, and in the present case to YouTube, on account of one of its contents.

Kalda v. Estonia

19 January 2016

This case concerned a prisoner's complaint about the authorities' refusal to grant him access to three Internet websites, containing legal information, run by the State and by the Council of Europe. The applicant complained in particular that the ban under Estonian law on his accessing these specific websites had breached his right to receive information via the Internet and prevented him from carrying out legal research for court proceedings in which he was engaged.

The Court held that there had been a violation of Article 10 (freedom of expression) of the Convention. It found in particular that Contracting States are not obliged to grant prisoners access to Internet. However, if a State is willing to allow prisoners access, as is the case in Estonia, it has to give reasons for refusing access to specific sites. In the specific circumstances of the applicant's case, the reasons, namely the security and costs implications, for not allowing him access to the Internet sites in question had not been sufficient to justify the interference with his right to receive information. Notably, the authorities had already made security arrangements for prisoners' use of Internet via computers specially adapted for that purpose and under the supervision of the prison authorities and had borne the related costs. Indeed, the domestic courts had undertaken no detailed analysis as to the possible security risks of access to the three additional websites in question, bearing in mind that they were run by an international organisation and by the State itself.

See also: *Jankovskis v. Lithuania*, judgment of 17 January 2017.

Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary

2 February 2016

This case concerned the liability of a self-regulatory body of Internet content providers and an Internet news portal for vulgar and offensive online comments posted on their websites following the publication of an opinion criticising the misleading business practices of two real estate websites. The applicants complained about the Hungarian courts' rulings against them, which had effectively obliged them to moderate the contents of comments made by readers on their websites, arguing that that had gone against the essence of free expression on the Internet.

The Court held that there had been a violation of Article 10 (freedom of expression) of the Convention. It reiterated in particular that, although not publishers of comments in the traditional sense, Internet news portals had to, in principle, assume duties and responsibilities. However, the Court considered that the Hungarian courts, when deciding on the notion of liability in the applicants' case, had not carried out a proper balancing exercise between the competing rights involved, namely between the applicants' right to freedom of expression and the real estate websites' right to respect for its commercial reputation. Notably, the Hungarian authorities accepted at face value that the comments had been unlawful as being injurious to the reputation of the real estate websites.

Dallas v. the United Kingdom

11 February 2016

This case concerned the applicant's conviction for contempt of court as a result of her conducting Internet research in relation to the criminal case she was trying as a juror. The applicant complained that the common law offence of contempt of court had not been sufficiently clear.

The Court held that there had been no violation of Article 7 (no punishment without law) of the Convention. It found in particular that the test for contempt of court applied in her case had been both accessible and foreseeable. The law-making function of the courts had remained within reasonable limits and the judgment in her case could be considered, at most, a step in the gradual clarification of the rules of criminal liability for contempt of court through judicial interpretation. Any development of the law had been consistent with the essence of the offence and could be reasonably foreseen.

Pihl v. Sweden

7 February 2017 (decision on the admissibility)

The applicant had been the subject of a defamatory online comment, which had been published anonymously on a blog. He made a civil claim against the small non-profit association which ran the blog, claiming that it should be held liable for the third-party comment. The claim was rejected by the Swedish courts and the Chancellor of Justice. The applicant complained to the Court that by failing

to hold the association liable, the authorities had failed to protect his reputation and had violated his right to respect for his private life.

The Court declared the application inadmissible as being manifestly ill-founded. It noted in particular that, in cases such as this, a balance must be struck between an individual's right to respect for his private life, and the right to freedom of expression enjoyed by an individual or group running an internet portal. In light of the circumstances of this case, the Court found that national authorities had struck a fair balance when refusing to hold the association liable for the anonymous comment. In particular, this was because: although the comment had been offensive, it had not amounted to hate speech or an incitement to violence; it had been posted on a small blog run by a non-profit association; it had been taken down the day after the applicant had made a complaint; and it had only been on the blog for around nine days.

Barbulescu v. Romania

5 September 2017 (Grand Chamber)

This case concerned the decision of a private company to dismiss an employee - the applicant - after monitoring his electronic Communications and accessing their contents. The applicant complained that his employer's decision was based on a breach of his privacy and that the domestic courts had failed to protect his right to respect for his private life and correspondence.

The Grand Chamber held, by eleven votes to six, that there had been a violation of Article 8 (right to respect for private life and correspondence) of the Convention, finding that the Romanian authorities had not adequately protected the applicant's right to respect for his private life and correspondence. They had consequently failed to strike a fair balance between the interests at stake. In particular, the national courts had failed to determine whether the applicant had received prior notice from his employer of the possibility that his communications might be monitored; nor had they had regard either to the fact that he had not been informed of the nature or the extent of the monitoring, or the degree of intrusion into his private life and correspondence. In addition, the national courts had failed to determine, firstly, the specific reasons justifying the introduction of the monitoring measures; secondly, whether the employer could have used measures entailing less intrusion into the applicant's private life and correspondence; and thirdly, whether the communications might have been accessed without his knowledge.

M.L. and W.W. v. Germany (nos. 60798/10 and 65599/10)

28 June 2018

This case concerned the refusal by the Federal Court of Justice to issue an injunction prohibiting three different media from continuing to allow Internet users access to documentation concerning the applicants' conviction for the murder of a famous actor and mentioning their names in full. The applicants complained of an infringement of their right to respect for their private life

The Court held that there had been no violation of Article 8 (right to respect for private life) of the Convention. It shared in particular the findings of the German Federal Court, which had reiterated that the media had the task of participating in the creation of democratic opinion, by making available to the public old news items that had been preserved in their archives. The Court also reiterated that the approach to covering a given subject was a matter of journalistic freedom and that Article 10 (freedom of expression) of the Convention left it to journalists to decide what details ought to be published, provided that these decisions corresponded to the profession's ethical norms. The inclusion in a report of individualised information, such as the full name of the person in question, was an important aspect of the press's work, especially when reporting on criminal proceedings which had attracted considerable attention that remained undiminished with the passage of time. Lastly, the Court noted that during their most recent request to reopen proceedings in 2004, the applicants had themselves contacted the press, transmitting a number of documents while inviting journalists to keep the public informed. This attitude put a different perspective on their hope of obtaining anonymity in the reports, or on the right to be forgotten online. In conclusion, having regard to the margin of appreciation left to the national authorities when weighing up divergent interests, the importance of maintaining the accessibility of press reports which had been recognised as lawful, and the applicants' conduct vis-a-vis the press, the Court considered that there were no substantial grounds for it to substitute its view for that of the Federal Court of Justice.

Savva Terentyev v. Russia⁴⁵

28 August 2018

This case concerned the applicant's conviction for inciting hatred after making insulting remarks about police officers in a comment under a blog post.

The Court held that there had been a violation of Article 10 (freedom of expression) of the Convention. It found in particular that while the applicant's language had been offensive and shocking that alone was not enough to justify interfering with his right to freedom of expression. The domestic courts should have looked at the overall context of his comments, which had been a provocative attempt to

⁴⁵ On 16 September 2022 the Russian Federation ceased to be a Party to the Convention.

express his anger at what he perceived to be police interference, rather than an actual call to physical violence against the police.

Magyar Jeti Zrt v. Hungary

4 December 2018

This case concerned the applicant company being found liable for posting a hyperlink to an interview on YouTube which was later found to contain defamatory content. The applicant company complained that by finding it liable for posting the hyperlink on its website the domestic courts had unduly restricted its rights.

The Court held that there had been a violation of Article 10 (freedom of expression) of the Convention. It underscored in particular the importance of hyperlinking for the smooth operation of the Internet and distinguished the use of hyperlinks from traditional publishing - hyperlinks directed people to available material rather than provided content. Updating its case-law on these issues, the Court set down elements which need to be considered under Article 10 when looking at whether posting a hyperlink could lead to liability and said that an individual assessment was necessary in each case. In the present case, the Court found that the Hungarian domestic law on objective (strict) liability for disseminating defamatory material had excluded the possibility of any meaningful assessment of the applicant company's right to freedom of expression in a situation where the courts should have scrutinised the issue carefully. Such objective liability for using a hyperlink could undermine the flow of information on the Internet, dissuading article authors and publishers from using such links if they could not control the information they led to. That could have a chilling effect on freedom of expression on the Internet. The Court therefore found that, overall, the applicant company had suffered an undue restriction of its rights.

Høiness v. Norway

19 March 2019

This case concerned the Norwegian courts' refusal to impose civil liability on an Internet forum host after vulgar comments about the applicant had been posted on the forum. The applicant complained that the authorities had violated her rights by not sufficiently protecting her right to protection of her reputation and by requiring her to pay litigation costs to the extent seen in her case.

The Court held that there had been no violation of Article 8 (right to respect for private life) of the Convention, finding that the Norwegian courts had sufficiently safeguarded the applicant's rights under that provision. It considered in particular that the national courts had acted within their

discretion (“margin of appreciation”) when seeking to establish a balance between the applicant’s rights under Article 8 and the opposing right to freedom of expression under Article 10 of the Convention of the news portal and host of the debate forums. Moreover, the domestic courts’ rulings on litigation costs being awarded to the defendants had not as such violated Article 8 of the Convention.

Beizaras and Levickas v. Lithuania

14 January 2020

The applicants, two young men who were in a relationship, alleged that they had been discriminated against on the grounds of sexual orientation because of the authorities’ refusal to launch a pre-trial investigation into the hate comments on the Facebook page of one of them. The latter had posted a photograph of them kissing on his Facebook page, which led to hundreds of online hate comments. Some were about LGBT people in general, while others personally threatened the applicants. The applicants submitted that they had been discriminated against on the grounds of sexual orientation. They also argued that the refusal had left them with no possibility of legal redress.

The Court held that there had been a violation of Article 14 (prohibition of discrimination) taken in conjunction with Article 8 (right to respect for private life) of the Convention, finding that the applicants had suffered discrimination on the grounds of their sexual orientation and that the Lithuanian Government had not provided any justification showing that the difference in treatment had been compatible with the standards of the Convention. It noted in particular that the applicants’ sexual orientation had played a role in the way they had been treated by the authorities, which had quite clearly expressed disapproval of them so publicly demonstrating their homosexuality when refusing to launch a pre-trial investigation. Such a discriminatory attitude had meant that the applicants had not been protected, as was their right under the criminal law, from undisguised calls for an attack on their physical and mental integrity. The Court also held that there had been a violation of Article 13 (right to an effective remedy) of the Convention because the applicants had been denied an effective domestic remedy for their complaints.

Vladimir Kharitonov v. Russia, OOO Flavus and Others v. Russia, Bulgakov v. Russia and Engels v. Russia⁴⁶

23 June 2020

⁴⁶ On 16 September 2022 the Russian Federation ceased to be a Party to the Convention.

These cases concerned the blocking of websites in Russia and, in particular, different types of blocking measures, including “collateral” blocking (where the IP address that was blocked was shared by several sites including the targeted one); “excessive” blocking (where the whole website was blocked because of a single page or file), and “wholesale” blocking (three online media were blocked by the Prosecutor General for their coverage of certain news). The applicants complained that the blocking of access to their websites had been unlawful and disproportionate, and that the Russian courts had failed to consider the substance of their complaints.

The Court held that there had been a violation of Article 10 (right to freedom of expression) of the Convention and a violation of Article 13 (right to an effective remedy) in conjunction with Article 10. It highlighted in particular the importance of the Internet as a vital tool in exercising the right to freedom of expression. Among other things, the Court found that the provisions of Russia’s Information Act used to block the websites had produced excessive and arbitrary effects and had not provided proper safeguards against abuse.

Societe Editrice de Mediapart and Others v. France

14 January 2021

This case concerned an order issued against Mediapart, a news website, its publishing editor and a journalist to remove from the news company’s website audio extracts and transcripts of illegal recordings made at the home of Ms Bettencourt, principal shareholder of the L’Oreal group. The applicants alleged that the court order in question had breached their right to freedom of expression.

The Court held that there had been no violation of Article 10 (freedom of expression) of the Convention, finding that the reasons relied upon by the domestic courts had been both relevant and sufficient to show that the interference complained of was “necessary in a democratic society” and that the order in question had not gone beyond what was necessary to protect Ms Bettencourt from the interference with her right to respect for private life. It noted, in particular, that notwithstanding the vital role played by the press in a democratic society, journalists could not, in principle, be released from their duty to obey the ordinary criminal law on the basis that Article 10 of the Convention afforded them a cast-iron defence. Further, breaches of privacy resulting from intrusion in the intimate life of individuals through the use of technical devices for illegal tapping, video- recording or photography had to be subject to particularly attentive protection. The Court also observed that internet sites were an information and communication tool particularly distinct from the printed media, especially with regard to their capacity to store and transmit information, and the risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights

and freedoms, particularly the right to respect for private life, was certainly higher than that posed by the press.

Biancardi v. Italy

25 November 2021

This case concerned the “right to be forgotten”. The applicant, a former editor-in-chief of an online newspaper, was found liable in civil proceedings for having kept on his newspaper’s website an article reporting on a fight in a restaurant, giving details on the related criminal proceedings. The courts noted in particular that the applicant had failed to de-index the tags to the article, meaning that anyone could type into a search engine the name of the restaurant or its owner and have access to sensitive information on the criminal proceedings, despite the owner’s request to have the article removed.

This was the first case in which the Court had examined whether a journalist’s civil liability for not de-indexing information published on the Internet had been compatible with Article 10 (freedom of expression) of the Convention. The Court held that there had been no violation of Article 10 of the Convention in the present case, finding that the domestic jurisdictions findings had constituted a justifiable restriction on the applicant’s freedom of expression - all the more so given the fact that he had not been obliged to permanently remove the article from the Internet. In particular, the Court noted that not only Internet search engine providers could be obliged to de-index material but also administrators of newspaper or journalistic archives accessible through the Internet, such as the applicant. It also agreed with the domestic courts’ rulings that the prolonged and easy access to information on the criminal proceedings concerning the restaurant owner had breached his right to reputation.

Wikimedia Foundation, Inc. v. Turkey

1 March 2022 (decision on the admissibility)

This case concerned a request by the Telecommunications and Information Technology Directorate for the removal of pages from the applicant foundation’s website and the subsequent order blocking access to the entire website as it was not technically feasible to block only certain pages. The applicant alleged that the blocking of access to the entire Wikipedia website amounted to unjustified interference with its right to freedom of expression, and that the procedure for judicial review of blocking orders against websites was inadequate to prevent abuse. It further alleged that no effective remedy was available under Turkish law and that its individual application to the Turkish

Constitutional Court had been rendered ineffective since its activity consisted in publishing the content of its webpages in a timely manner.

The Court declared the application inadmissible, finding that the applicant could no longer claim victim status. It observed, in particular, that it had found, in numerous cases concerning freedom of expression, that an application to the Constitutional Court was to be regarded as a remedy to be exhausted for the purposes of Article 35 § 1 (admissibility criteria) of the Convention in respect of such complaints. The Court took note of the systemic nature of the problem raised in the present case. Nevertheless, it did not have sufficiently relevant information to suggest that the Turkish Constitutional Court was not capable of remedying the problem. That court had delivered several judgments concerning the blocking of websites, establishing numerous criteria to be followed by the national authorities and the courts called upon to examine blocking orders. In the present case, the Court found that in ruling on the individual application before it the Constitutional Court had acknowledged in substance the violation of Article 10 (freedom of expression) of the Convention and had afforded appropriate and sufficient redress for the damage sustained by the applicant foundation.

Xavier Lucas v. France

9 June 2022

This case concerned a requirement to issue proceedings in the Court of Appeal electronically using the e-barreau platform. The Court of Appeal had held that the applicant's paper application to set aside an arbitral award could be entertained on the ground that the online form did not allow users to enter that type of application or the capacity in which the parties were named. However, the Court of Cassation took the opposite view, holding that the application should have been filed electronically. The applicant complained that the dismissal of his set-aside application without consideration on the merits for failure to file it electronically had violated his right of access to a court.

The Court held that there had been a violation of Article 6 § 1 (right to a fair trial) of the Convention, finding that a disproportionate burden had been placed on the applicant, upsetting the proper balance between, on the one hand, the legitimate concern of ensuring adherence to the formalities for the issuance of court proceedings and, on the other, the right of access to a court. Consistent with the applicant's submission that it had been impossible in fact to file the application on the e-barreau platform, the Court noted, in particular, that in order to file it electronically on e-barreau the applicant's lawyer would have had to fill out the form using inaccurate legal terms. It further observed that the French Government had not shown that specific information about how to lodge such an application had been made available to users. The Court concluded that by giving precedence to the

rule that proceedings in the Court of Appeal were to be issued electronically, while disregarding the practical hurdles faced by the applicant in doing so, the Court of Cassation had taken a formalistic approach that was not needed to ensure legal certainty or the proper administration of justice and which therefore had to be regarded as excessive.

Pending applications

Hurbain v. Belgium (no. 57292/16)

22 June 2021 (Chamber judgment) - case referred to the Grand Chamber in October 2021

This case concerns a civil judgment against the applicant, in his capacity as publisher of the daily newspaper *Le Soir*, ordering him to anonymise an article in its electronic archive which mentioned the full name of a driver who had been responsible for a deadly road accident in 1994. The order was based on the individual's right to be forgotten.

In its Chamber judgment of 22 June 2021, the Court, by six votes to one, held that there had been no violation of Article 10 (freedom of expression) of the Convention, finding that the reasons given by the domestic courts had been relevant and sufficient, and that the measure imposed on the applicant could be regarded as proportionate to the legitimate aim pursued and as striking a fair balance between the competing rights at stake.

On 11 October 2021 the Grand Chamber Panel accepted the applicant's request that the case be referred to the Grand Chamber.

On 9 March 2022 the Grand Chamber held a hearing in the case.

Akdeniz and Altiparmak v. Turkey (no. 5568/20)

Application communicated to the Turkish Government on 26 August 2020

This application concerns the restriction of access to more than 600 Internet contents (news sites and social network accounts) by decisions adopted in 2015 and 2016 by the telecommunications administrative entity.

The Court gave notice of the application to the Turkish Government and put questions to the parties under Article 10 (freedom of expression) and Article 18 (limitation on use of restrictions on rights) of the Convention.

Akdeniz and Altiparmak v. Turkey (no. 35278/20)

Application communicated to the Turkish Government on 9 February 2021

This application concerns the restriction of access to 111 contents on the Internet (news sites, video sites and social network accounts) by a decision adopted in October 2015 by the telecommunications administrative entity.

The Court gave notice of the application to the Turkish Government and put questions to the parties under Article 10 (freedom of expression) and Article 18 (limitation on use of restrictions on rights) of the Convention.

Mobile telephone

Magyar Kétfarkú Kutya Part v. Hungary

20 January 2020

This case concerned a political party's mobile application which allowed voters to photograph, anonymously upload and comment on invalid votes cast during a referendum on immigration in 2016. The applicant party complained about a violation of its rights under Article 10 (right to freedom of expression) of the Convention.

The Grand Chamber found in particular that the provision of domestic election law relied on by the authorities (a breach of the principle of the exercise of rights in accordance with their purpose) had not allowed the applicant party to foresee that it could be penalised for providing such an app, which had been an exercise of its freedom of expression. It concluded that the considerable uncertainty about the potential effects of the provision had exceeded what was acceptable under the Convention and that the lack of sufficient precision in the law to rule out arbitrariness and allow the applicant party to regulate its conduct had led to a violation of Article 10 (freedom of expression) of the Convention.

Pending application

Minteh v. France (no. 23624/20)

Application communicated to the French Government on 31 May 2021

This case concerns the criminal conviction of the applicant for refusing to disclose to the police the security code to unlock his mobile phone while he was in police custody.

The Court gave notice of the application to the French Government and put questions to the parties under Articles 6 § 1 (right to a fair trial) and 8 (right to respect for private life and correspondence) of the Convention.

Copyright of books and musical work

SIA AKKA/LAA v. Latvia

12 July 2016

This case concerned a complaint about the restriction on the copyright of authors' musical work. The applicant, an organisation responsible for managing the copyright of the musical works of a large number of Latvian and international authors, complained about decisions by the national courts ordering the applicant organisation and two radio companies to enter into a licence agreement and to set an equitable royalty rate. The applicant organisation notably alleged that those decisions had restricted the exclusive rights of the authors they represented to freely conclude licence agreements for the use of their musical works.

The Court held that there had been no violation of Article 1 (protection of property) of Protocol No. 1 to the Convention and no violation of Article 6 § 1 (right to fair trial) of the Convention. It found in particular that the Latvian authorities had struck a fair balance between the demands of the public interest (namely, the radio companies' interest in obtaining a licence allowing them to legally broadcast work as well as the general public's interest in having access to musical works), on the one hand, and the rights of the applicant organisation to obtain equitable remuneration from the use of musical work, on the other. Indeed, the effort to maintain a balance between the competing interests could be seen in their decisions, which had observed that protected works were being broadcast without a valid licence over an extended period of time and that that situation had to a certain extent been due to the applicant organisation's limited efficiency in carrying out negotiations with the radio companies.

Safarov v. Azerbaijan

1 September 2022

The applicant, who was the author of a book on the history of Azerbaijan, alleged an infringement of his copyright on account of the unauthorised reproduction of his book and its online publication by a private party without his authorisation or paying him any royalties. His subsequent civil claim was dismissed, as was ultimately his cassation appeal. The applicant complains of the State's failure to protect his intellectual property interests and that the domestic courts' judgments in his case had not been reasoned.

The Court held that there had been a violation of Article 1 (protection of property) of Protocol No. 1 to the Convention in the present case, finding that the respondent State had failed to discharge its

positive obligation under Article 1 of Protocol No. 1 to protect intellectual property notably through effective remedial measures.

Korotyuk v. Ukraine

*19 January 2023*⁴⁷

This case concerned a book written by the applicant - Scientific and Practical Commentary to the Law of Ukraine on Notaries - being made available for paid download on a textbook website without her consent. She complained to the police in 2013 and the investigation was apparently still ongoing. Before the Court, the applicant complained of a lack of an effective investigation into the illegal downloading of her book and of the State's failure to protect her intellectual property.

The Court held that there had been a violation of Article 1 (protection of property) of Protocol No. 1 to the Convention in the applicant's case. It noted in particular that although copyright disputes were in general of civil law nature, in the specific circumstances of the present case, which concerned an alleged criminal offence, the respondent State had been under a positive duty under Article 1 of Protocol No. 1 to conduct an effective criminal investigation. In this regard, the Court observed that the criminal investigation had been characterised by a number of flaws. It found that the cumulative result of the flagrant and serious deficiencies that had characterised the criminal investigation was that the State had failed to fulfil its positive obligations in respect of the applicant's property.

Online harassment

Volodina v. Russia (no. 2)⁴⁸

14 September 2021

This case concerned the applicant's allegation that the Russian authorities had failed to protect her against repeated acts of cyberharassment. She submitted, in particular, that her former partner had used her name, personal details and intimate photographs to create fake social media profiles, that he had planted a GPS tracker in her handbag, that he had sent her death threats via social media; and that the authorities had failed to effectively investigate these allegations.

The Court held that there had been a violation of Article 8 (right to respect for private life) of the Convention, finding that the Russian authorities had failed to comply with their obligations under that provision to protect the applicant from severe abuse. It noted, in particular, that, despite having

⁴⁷ This judgment will become final in the circumstances set out in Article 44 § 2 (final judgments) of the European Convention on Human Rights.

⁴⁸

the legal tools available to prosecute the applicant's partner, the authorities had not carried out an effective investigation and had not considered at any point in time what could and should have been done to protect the applicant from recurrent online harassment.

Radio communications

Brambilla and Others v. Italy

23 June 2016

This case concerned the conviction of three journalists who intercepted radio communications between carabinieri in order to arrive quickly at crime scenes and report on them for their local newspaper.

The Court held that there had been no violation of Article 10 (freedom of expression) of the Convention. Stressing the notion of responsible journalism and noting that the decisions of the domestic courts had been duly reasoned and had focused primarily on the need to protect national security and prevent crime and disorder, the Court found in particular that the Italian courts had made an appropriate distinction between on the one hand the duty of the three journalists to comply with domestic law, which prohibited in general terms the interception by any persons of communications not addressed to them, including those of the law-enforcement agencies, and on the other hand the pursuit of their journalistic activities, which had not been restricted per se. The Court also noted that the penalties ordered by the domestic courts, consisting in the seizure of the radio equipment and the imposition of custodial sentences, had not been disproportionate, as the sentences of the three journalists had been suspended and the authorities had not prohibited them from bringing news items to the public's attention.

Satellite dish

Khurshid Mustafa and Tarzibachi v. Sweden

16 December 2008

This case concerned a court decision not to prolong a private tenancy agreement owing to the refusal by the tenants, a married couple of Iraqi origin with three minor children, to remove a satellite dish used to receive television programmes from their country of origin. The landlord offered to allow the applicants to stay if they agreed to remove the satellite dish, but they refused and had to move out. The applicants complained of a violation of their freedom to receive information.

The Court held that there had been a violation of Article 10 (freedom of expression - freedom to receive information) of the Convention. It observed in particular that the satellite dish had enabled the applicants and their children to receive television programmes in Arabic and Farsi from their native country and region. That information - which included political and social news and, almost equally importantly, cultural expression and entertainment - was of particular interest to them as an immigrant family who wished to maintain contact with the culture and language of their country of origin. It had not been claimed that the applicants had any other means of receiving such programmes at the time or that they could have placed the satellite dish elsewhere. Nor could news obtained from foreign newspapers and radio programmes in any way be equated with information available via television broadcasts. The landlord's concerns about safety had been examined by the domestic courts, who had found that the installation did not pose any real safety threat. Moreover, the fact that the applicants had effectively been evicted from their home with their three children had been disproportionate to the aim pursued.

Telecommunications

Roman Zakharov v. Russia⁴⁹

4 December 2015

This case concerned the system of secret interception of mobile telephone communications in Russia. The applicant, an editor-in-chief of a publishing company, complained in particular that mobile network operators in Russia were required by law to install equipment enabling law-enforcement agencies to carry out operational-search activities and that, without sufficient safeguards under Russian law, this permitted blanket interception of communications.

The Court held that there had been a violation of Article 8 (right to respect for private life and correspondence) of the Convention, finding that the Russian legal provisions governing interception of communications did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which was inherent in any system of secret surveillance, and which was particularly high in a system such as in Russia where the secret services and the police had direct access, by technical means, to all mobile telephone communications. In particular, the Court found shortcomings in the legal framework in the following areas: the circumstances in which public authorities in Russia are empowered to resort to secret surveillance measures; the duration of such measures, notably the circumstances in which they should be discontinued; the procedures for authorising interception as

⁴⁹ On 16 September 2022 the Russian Federation ceased to be a Party to the Convention.

well as for storing and destroying the intercepted data; the supervision of the interception. Moreover, the effectiveness of the remedies available to challenge interception of communications was undermined by the fact that they were available only to persons who were able to submit proof of interception and that obtaining such proof was impossible in the absence of any notification system or possibility of access to information about interception.

Breyer v. Germany

30 January 2020

In accordance with 2004 amendments to the German Telecommunications Act companies had to collect and store the personal details of all their customers, including users of pre-paid SIM cards, which had not previously been required. The applicants, civil liberties activists and critics of State surveillance, were users of such cards and therefore had to register their personal details, such as their telephone numbers, date of birth, and their name and address, with their service providers. They complained about the storage of their personal data as users of pre-paid SIM cards.

The Court held that there had been no violation of Article 8 (right to respect for private life) of the Convention, finding that, overall, Germany had not overstepped the limits of its discretion (“margin of appreciation”) it had in applying the law concerned, when choosing the means to achieve the legitimate aims of protecting national security and fighting crime, and that the storage of the applicants’ personal data had been proportionate and “necessary in a democratic society”. There had thus been no violation of the Convention. The Court considered in particular that collecting the applicants’ names and addresses as users of pre-paid SIM cards had amounted to a limited interference with their rights. It noted, however, that the law in question had additional safeguards while people could also turn to independent data supervision bodies to review authorities’ data requests and seek legal redress if necessary.

Pending applications

A.L. v. France (no. 44715/20) and E.J. v. France (no. 47930/21)

Applications communicated to the French Government on 8 December 2021

These applications concern in particular the infiltration by the French authorities of the encrypted communication network “EncroChat” and the capture, copying and analysis of data stored and exchanged with the devices connected to this network.

The Court gave notice of the applications to the French Government and put questions to the parties under Articles 6 § 1 (right to a fair trial), 8 (right to respect for private life and correspondence), 13 (right to an effective remedy), 34 (right of individual application) and 35 (admissibility criteria) of the Convention.

Use of hidden cameras

Haldimann and Others v. Switzerland

24 February 2015

This case concerned the conviction of four journalists for having recorded and broadcast an interview of a private insurance broker using a hidden camera, as part of a television documentary intended to denounce the misleading advice provided by insurance brokers. The applicants complained that their sentence to payment of fines had amounted to a disproportionate interference in their right to freedom of expression.

In this case, the Court was for the first time called on to examine an application concerning the use of hidden cameras by journalists to provide public information on a subject of general interest, whereby the person filmed was targeted not in any personal capacity but as a representative of a particular professional category. The Court held that, in the applicants' case, there had been a violation of Article 10 (freedom of expression) of the Convention, considering in particular that the interference in the private life of the broker, who had turned down an opportunity to express his views on the interview in question, had not been serious enough to override the public interest in information on malpractice in the field of insurance brokerage. The Court further also asserted that the applicants deserved the benefit of the doubt in relation to their desire to observe the ethics of journalism as defined by Swiss law, citing the example of their limited use of the hidden camera.

Bremner v. Turkey

13 October 2015

This case concerned the broadcasting of a television documentary in which the applicant, who was shown promoting his evangelical Christian beliefs, was described as a "foreign pedlar of religion" engaged in covert activities in Turkey. The applicant alleged that the broadcasting of the documentary and the refusal of the judicial authorities to grant his request for compensation had breached his right to respect for his private life.

The Court held that there had been a violation of Article 8 (right to respect for private life) of the Convention, finding in particular that the broadcasting of the applicant's image without blurring it could not be regarded as a contribution to any debate of general interest for society, regardless of the degree of public interest in the question of religious proselytising. As regards the method used, the Court was of the view that a technique as intrusive and as damaging to private life must in principle be used restrictively. The Court was not unaware that, in certain cases, the use of hidden cameras might prove necessary for journalists when information was difficult to obtain by any other means. However, that tool had to be used in compliance with ethical principles and with restraint.

See also:

Erdtmann v. Germany

5 January 2016 (decision on the admissibility)

Video surveillance

Peck v. the United Kingdom

28 January 2003

In this case the applicant, who was suffering from depression, complained about the disclosure in the media of footage from a closed-circuit television (CCTV) camera mounted in the street showing him walking alone with a kitchen knife in his hand (he had subsequently attempted suicide by cutting his wrists, but the CCTV footage did not show this), which had resulted in images of himself being published and broadcast widely. He further complained of the lack of an effective domestic remedy in that regard. The Court found that the disclosure of the footage by the municipal council had not been accompanied by sufficient safeguards and constituted disproportionate and unjustified interference with the applicant's private life, in breach of Article 8 (right to respect for private life) of the Convention. Furthermore, at the relevant time, the applicant had not had an effective remedy for breach of confidence, in violation of Article 13 (right to an effective remedy) read in conjunction with Article 8 of the Convention.

Perry v. the United Kingdom

17 July 2003

The applicant was arrested in connection with a series of armed robberies of mini-cab drivers and released pending an identification parade. When he failed to attend that and several further identification parades, the police requested permission to video him covertly. The applicant

complained that the police had covertly videotaped him for identification purposes and used the videotape in the prosecution against him.

The Court held that there had been a violation of Article 8 (right to respect for private life) of the Convention. It noted that there had been no indication that the applicant had had any expectation that footage would be taken of him in the police station for use in a video identification procedure and, potentially, as evidence prejudicial to his defence at trial. That ploy adopted by the police had gone beyond the normal use of this type of camera and amounted to an interference with the applicant's right to respect for his private life. The interference in question had further not been in accordance with the law because the police had failed to comply with the procedures set out in the applicable code: they had not obtained the applicant's consent or informed him that the tape was being made; neither had they informed him of his rights in that respect.

Köpke v. Germany

5 October 2010 (decision on the admissibility)

The applicant, a supermarket cashier, was dismissed without notice for theft, following a covert video surveillance operation carried out by her employer with the help of a private detective agency. She unsuccessfully challenged her dismissal before the labour courts. Her constitutional complaint was likewise dismissed.

The Court rejected the applicant's complaint under Article 8 (right to respect for private life) of the Convention as inadmissible (manifestly ill-founded). It concluded that the domestic authorities had struck a fair balance between the employee's right to respect for her private life and her employer's interest in the protection of its property rights and the public interest in the proper administration of justice. It observed, however, that the competing interests concerned might well be given a different weight in the future, having regard to the extent to which intrusions into private life were made possible by new, more and more sophisticated technologies.

Riina v. Italy

11 March 2014 (decision on the admissibility)

The applicant, who was sentenced to life imprisonment for having committed very serious crimes, including mafia-type conspiracy and multiple assassinations, complained of the fact that he was under constant video surveillance in his cell, including in the toilets. He contended that the domestic remedies available in respect of these measures were ineffective.

The Court declared the application inadmissible under Articles 3 (prohibition of inhuman or degrading treatment) and 8 (right to respect for private and family life) of the Convention, finding that the applicant had not exhausted the domestic remedies available to him to appeal against the application of the video surveillance measure.

Vasilica Mocanu v. Romania

6 December 2016

This case concerned the conditions in which the applicant was held on police premises. The applicant also alleged that his cell had been fitted with a system of permanent CCTV monitoring by which he was filmed.

The Court held that there had been a violation of Article 8 (right to respect of private life) of the Convention, finding that the surveillance of the applicant by a video camera which was present in the cell where he had been placed on the premises of the County police had not been in accordance with the domestic law.

Antovic and Mirkovic v. Montenegro

28 November 2017

This case concerned an invasion of privacy complaint by two professors at the University of Montenegro's School of Mathematics after video surveillance had been installed in areas where they taught. They stated that they had had no effective control over the information collected and that the surveillance had been unlawful. The domestic courts rejected a compensation claim however, finding that the question of private life had not been at issue as the auditoriums where the applicants taught were public areas.

The Court held that there had been a violation of Article 8 (right to respect for private life) of the Convention, finding that the camera surveillance had not been in accordance with the law. It first rejected the Government's argument that the case was inadmissible because no privacy issue had been at stake as the area under surveillance had been a public, working area. In this regard the Court noted in particular that it had previously found that private life might include professional activities and considered that was also the case with the applicants. Article 8 was therefore applicable. On the merits of the case, the Court then found that the camera surveillance had amounted to an interference with the applicants' right to privacy and that the evidence showed that that surveillance had violated the provisions of domestic law. Indeed, the domestic courts had never even considered any legal

justification for the surveillance because they had decided from the outset that there had been no invasion of privacy.

Gorlov and Others v. Russia⁵⁰

2 July 2019

This case concerned the permanent video surveillance of detainees in their cells by closed-circuit television cameras. The applicants complained, in particular, that constant surveillance of their cells, at times by female guards, had violated their right to respect for their private life.

The Court held that there had been a violation of Article 8 (right to respect for private life) of the Convention, finding that the measure in question had not been in accordance with the law. Although the Court could accept that it might be necessary to monitor certain areas of penal institutions, or certain detainees on a permanent basis, it found in particular that the existing legal framework in Russia could not be regarded as being sufficiently clear, precise and detailed to afford appropriate protection against arbitrary interference by the public authorities with the right to respect for private life. The Court also held that there had been a violation of Article 13 (right to an effective remedy) of the Convention in conjunction with Article 8 in respect of two of the applicants, finding that they had not had at their disposal an effective domestic remedy for their complaint of a violation of the right to respect for their private life.

See also: *Izmestyev v. Russia*, judgment of 27 August 2019.

Lopez Ribalda and Others v. Spain

17 October 2019 (Grand Chamber)

This case concerned the covert video-surveillance of employees which led to their dismissal. The applicants complained about the covert video-surveillance and the Spanish courts' use of the data obtained to find that their dismissals had been fair.

The applicants who signed settlement agreements also complained that the agreements had been made under duress owing to the video material and should not have been accepted as evidence that their dismissals had been fair.

The Grand Chamber held that there had been no violation of Article 8 (right to respect for private life) of the Convention in respect of the five applicants. It found in particular that the Spanish courts had carefully balanced the rights of the applicants - supermarket employees suspected of theft - and those

⁵⁰ On 16 September 2022 the Russian Federation ceased to be a Party to the Convention.

of the employer, and had carried out a thorough examination of the justification for the video-surveillance. A key argument made by the applicants was that they had not been given prior notification of the surveillance, despite such a legal requirement, but the Court found that there had been a clear justification for such a measure owing to a reasonable suspicion of serious misconduct and to the losses involved, taking account of the extent and the consequences of the measure. In the present case the domestic courts had thus not exceeded their power of discretion (“margin of appreciation”) in finding the monitoring proportionate and legitimate. The Court also held that there had been no violation of Article 6 § 1 (right to a fair trial) of the Convention, finding in particular that the use of the video material as evidence had not undermined the fairness of the trial.

MUHTELİF ÜLKE DÜZENLEMELERİ

Bölüm İçeriği

- ABD Federe Devlet Anayasalarında Özel Hayat ve Mahremiyet
- ABD - California Consumer Privacy Act of 2018 (CCPA)
- ABD - Virginia Consumer Data Protection Act (CDPA)
- ABD - Colorado Privacy Act (CPA)
- Almanya - Federal Data Protection Act (BDSG)
- İrlanda - Data Protection Act 2018
- Estonya - Personal Data Protection Act
- Çin - Personal Information Protection Law of the People's Republic of China
- Çin - Data Security Law of the People's Republic of China
- Güney Kore - Personal Information Protection Act
- Güney Kore - Personal Information Safeguard and Security Standard
- Japonya - Act on the Protection of Personal Information
- Katar - Personal Data Privacy Protection
- Kuzey Kıbrıs Türk Cumhuriyeti - 89/2007 Kişisel Verilerin Korunması Yasası
- Asya-Pasifik Ekonomik İş Birliği Forumu (APEC) - APEC Privacy Framework
- OECD Declaration on Government Access to Personal Data Held by Private Sector Entities

ABD Federe Devlet Anayasalarında Özel Hayat ve Mahremiyet

Alaska

Art. I § 22. Right of Privacy

The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section.

Arizona

Art. II § 8. Right to privacy

No person shall be disturbed in his private affairs, or his home invaded, without authority of law.

California

Art. I § 1

All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.

Florida

Art. I § 23. Right of privacy

Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law.

Art. I § 12. Searches and seizures

The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, and against the unreasonable interception of private communications by any means, shall not be violated. (No warrant shall be issued except upon probable cause, supported by affidavit, particularly describing the place or places to be searched, the person or persons, thing or things to be seized, the communication to be intercepted, and the nature of evidence to be obtained.

This right shall be construed in conformity with the 4th Amendment to the United States Constitution, as interpreted by the United States Supreme Court. Articles or information obtained in violation of this right shall not be admissible in evidence if such articles or information would be inadmissible under decisions of the United States Supreme Court construing the 4th Amendment to the United States Constitution.)

Hawaii

Art. I § 6. Right to Privacy

The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right.

Art. I § 7. Searches, Seizures and Invasion of Privacy

The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches, seizures and invasions of privacy shall not be violated; and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized or the communications sought to be intercepted.

Illinois

Art. I § 6. Searches, Seizures, Privacy and Interceptions

The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means. No warrant shall issue without probable cause, supported by affidavit particularly describing the place to be searched and the persons or things to be seized.

Louisiana

Art. I § 5. Right to Privacy

Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy. No warrant shall issue without probable cause supported by oath or affirmation, and particularly describing the place to be searched, the persons or things to be seized, and the lawful purpose or reason for the search. Any person

adversely affected by a search or seizure conducted in violation of this Section shall have standing to raise its illegality in the appropriate court.

Montana

Art. II § 10. Right of privacy

The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.

New Hampshire

Art. 2-b Right of Privacy

An individual's right to live free from governmental intrusion in private or personal information is natural, essential, and inherent.

South Carolina

Art. I § 10. Searches and seizures; invasions of privacy

The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated, and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, the person or thing to be seized, and the information to be obtained.

Washington

Art. I § 7. Invasion of Private Affairs or Home Prohibited

No person shall be disturbed in his private affairs, or his home invaded, without authority of law.

ABD - California Consumer Privacy Act of 2018 (CCPA)

CCPA - California Consumer Privacy Act of 2018

CIVIL CODE - CIV

DIVISION 3. OBLIGATIONS [1427 - 3273.16] (Heading of Division 3 amended by Stats. 1988, Ch. 160, Sec. 14.)

PART 4. OBLIGATIONS ARISING FROM PARTICULAR TRANSACTIONS [1738 - 3273.16] (Part 4 enacted 1872.)

TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100] (Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3.)

1798.100. (a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

(b) A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

(c) A business shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.

(d) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

(e) This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or

otherwise link information that is not maintained in a manner that would be considered personal information.

(Amended by Stats. 2019, Ch. 757, Sec. 1. (AB 1355) Effective January 1, 2020. Superseded on January 1, 2023; see amendment by Proposition 24.)

1798.100. General Duties of Businesses that Collect Personal Information

(a) A business that controls the collection of a consumer's personal information shall, at or before the point of collection, inform consumers of the following:

(1) The categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected without providing the consumer with notice consistent with this section.

(2) If the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected without providing the consumer with notice consistent with this section.

(3) The length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose.

(b) A business that, acting as a third party, controls the collection of personal information about a consumer may satisfy its obligation under subdivision (a) by providing the required information prominently and conspicuously on the homepage of its internet website. In addition, if a business acting as a third party controls the collection of personal information about a consumer on its premises, including in a vehicle, then the business shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the

categories of personal information are used, and whether that personal information is sold, in a clear and conspicuous manner at the location.

(c) A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.

(d) A business that collects a consumer's personal information and that sells that personal information to, or shares it with, a third party or that discloses it to a service provider or contractor for a business purpose shall enter into an agreement with the third party, service provider, or contractor, that:

(1) Specifies that the personal information is sold or disclosed by the business only for limited and specified purposes.

(2) Obligates the third party, service provider, or contractor to comply with applicable obligations under this title and obligate those persons to provide the same level of privacy protection as is required by this title.

(3) Grants the business rights to take reasonable and appropriate steps to help ensure that the third party, service provider, or contractor uses the personal information transferred in a manner consistent with the business' obligations under this title.

(4) Requires the third party, service provider, or contractor to notify the business if it makes a determination that it can no longer meet its obligations under this title.

(5) Grants the business the right, upon notice, including under paragraph (4), to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

(e) A business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Section 1798.81.5.

(f) Nothing in this section shall require a business to disclose trade secrets, as specified in regulations adopted pursuant to paragraph (3) of subdivision (a) of Section 1798.185.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 4. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.105. (a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.

(c) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

(d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law.

(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

(6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(8) Comply with a legal obligation.

(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

(Amended by Stats. 2019, Ch. 751, Sec. 1. (AB 1146) Effective January 1, 2020. Superseded on January 1, 2023; see amendment by Proposition 24.)

1798.105. Consumers' Right to Delete Personal Information

(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.

(c) (1) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records, notify any service providers or contractors to delete the consumer's personal information from their records, and notify all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information unless this proves impossible or involves disproportionate effort.

(2) The business may maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of a consumer who has submitted a deletion request from being sold, for compliance with laws or for other purposes, solely to the extent permissible under this title.

(3) A service provider or contractor shall cooperate with the business in responding to a verifiable consumer request, and at the direction of the business, shall delete, or enable the business to delete and shall notify any of its own service providers or contractors to delete personal information about the consumer collected, used, processed, or retained by the service provider or the contractor. The service provider or contractor shall notify any service providers, contractors, or third parties who may have accessed personal information from or through the service provider or contractor, unless the information was accessed at the direction of the business, to delete the consumer's personal information unless this proves impossible or involves disproportionate effort. A service provider or contractor shall not be required to comply with a deletion request submitted by the consumer directly to the service provider or contractor to the extent that the service provider or contractor has collected, used, processed, or retained the consumer's personal information in its role as a service provider or contractor to the business.

(d) A business, or a service provider or contractor acting pursuant to its contract with the business, another service provider, or another contractor, shall not be required to comply with a consumer's request to delete the consumer's personal information if it is reasonably necessary for the business, service provider, or contractor to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated by the consumer within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) Help to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for those purposes.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law.

(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

(6) Engage in public or peer-reviewed scientific, historical, or statistical research that conforms or adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the ability to complete such research, if the consumer has provided informed consent.

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business and compatible with the context in which the consumer provided the information.

(8) Comply with a legal obligation.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 5. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.106. Consumers' Right to Correct Inaccurate Personal Information

(a) A consumer shall have the right to request a business that maintains inaccurate personal information about the consumer to correct that inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's right to request correction of inaccurate personal information.

(c) A business that receives a verifiable consumer request to correct inaccurate personal information shall use commercially reasonable efforts to correct the inaccurate personal information as directed by the consumer, pursuant to Section 1798.130 and regulations adopted pursuant to paragraph (8) of subdivision (a) of Section 1798.185.

(Added November 3, 2020, by initiative Proposition 24, Sec. 6. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.110. (a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

- (1) The categories of personal information it has collected about that consumer.
- (2) The categories of sources from which the personal information is collected.
- (3) The business or commercial purpose for collecting or selling personal information.
- (4) The categories of third parties with whom the business shares personal information.
- (5) The specific pieces of personal information it has collected about that consumer.

(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer.

(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130:

- (1) The categories of personal information it has collected about consumers.
- (2) The categories of sources from which the personal information is collected.
- (3) The business or commercial purpose for collecting or selling personal information.
- (4) The categories of third parties with whom the business shares personal information.
- (5) That a consumer has the right to request the specific pieces of personal information the business has collected about that consumer.

(d) This section does not require a business to do the following:

(1) Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.

(2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

(Amended by Stats. 2019, Ch. 757, Sec. 2. (AB 1355) Effective January 1, 2020. Superseded on January 1, 2023; see amendment by Proposition 24.)

1798.110. Consumers' Right to Know What Personal Information is Being Collected. Right to Access Personal Information

(a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

- (1) The categories of personal information it has collected about that consumer.
- (2) The categories of sources from which the personal information is collected.
- (3) The business or commercial purpose for collecting, selling, or sharing personal information.
- (4) The categories of third parties to whom the business discloses personal information.
- (5) The specific pieces of personal information it has collected about that consumer.

(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to subparagraph (B) of paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer, provided that a business shall be deemed to be in compliance with paragraphs (1) to (4), inclusive, of subdivision (a) to the extent that the categories of information and the business or commercial purpose for collecting, selling, or sharing personal information it would be required to disclose to the consumer pursuant to paragraphs (1) to (4), inclusive, of subdivision (a) is the same as the information it has disclosed pursuant to paragraphs (1) to (4), inclusive, of subdivision (c).

(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130:

- (1) The categories of personal information it has collected about consumers.
- (2) The categories of sources from which the personal information is collected.
- (3) The business or commercial purpose for collecting, selling, or sharing personal information.
- (4) The categories of third parties to whom the business discloses personal information.

(5) That a consumer has the right to request the specific pieces of personal information the business has collected about that consumer.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 7. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.115. (a) A consumer shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

- (1) The categories of personal information that the business collected about the consumer.
- (2) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each category of third parties to whom the personal information was sold.
- (3) The categories of personal information that the business disclosed about the consumer for a business purpose.

(b) A business that sells personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose, pursuant to paragraph (4) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) to the consumer upon receipt of a verifiable consumer request from the consumer.

(c) A business that sells consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose, pursuant to subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130:

- (1) The category or categories of consumers' personal information it has sold, or if the business has not sold consumers' personal information, it shall disclose that fact.
- (2) The category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed the consumers' personal information for a business purpose, it shall disclose that fact.

(d) A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120.

(Amended by Stats. 2019, Ch. 757, Sec. 3. (AB 1355) Effective January 1, 2020. Superseded on January 1, 2023; see amendment by Proposition 24.)

1798.115. Consumers' Right to Know What Personal Information is Sold or Shared and to Whom

(a) A consumer shall have the right to request that a business that sells or shares the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

(1) The categories of personal information that the business collected about the consumer.

(2) The categories of personal information that the business sold or shared about the consumer and the categories of third parties to whom the personal information was sold or shared, by category or categories of personal information for each category of third parties to whom the personal information was sold or shared.

(3) The categories of personal information that the business disclosed about the consumer for a business purpose and the categories of persons to whom it was disclosed for a business purpose.

(b) A business that sells or shares personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose, pursuant to paragraph (4) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) to the consumer upon receipt of a verifiable consumer request from the consumer.

(c) A business that sells or shares consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose, pursuant to subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The category or categories of consumers' personal information it has sold or shared, or if the business has not sold or shared consumers' personal information, it shall disclose that fact.

(2) The category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed consumers' personal information for a business purpose, it shall disclose that fact.

(d) A third party shall not sell or share personal information about a consumer that has been sold to, or shared with, the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 8. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.120. (a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out.

(b) A business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the "right to opt-out" of the sale of their personal information.

(c) Notwithstanding subdivision (a), a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. This right may be referred to as the "right to opt-in."

(d) A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell the minor consumer's personal information shall be prohibited, pursuant to paragraph (4) of subdivision (a) of Section 1798.135, from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.

(Amended by Stats. 2019, Ch. 757, Sec. 4. (AB 1355) Effective January 1, 2020. Superseded on January 1, 2023; see amendment by Proposition 24.)

1798.120. Consumers' Right to Opt Out of Sale or Sharing of Personal Information

(a) A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. This right may be referred to as the right to opt-out of sale or sharing.

(b) A business that sells consumers' personal information to, or shares it with, third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold or shared and that consumers have the "right to opt-out" of the sale or sharing of their personal information.

(c) Notwithstanding subdivision (a), a business shall not sell or share the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale or sharing of the consumer's personal information. A business that

willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age.

(d) A business that has received direction from a consumer not to sell or share the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell or share the minor consumer's personal information, shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from selling or sharing the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides consent, for the sale or sharing of the consumer's personal information.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 9. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.121. Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information

(a) A consumer shall have the right, at any time, to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, to perform the services set forth in paragraphs (2), (4), (5), and (8) of subdivision (e) of Section 1798.140, and as authorized by regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185. A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in this subdivision shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be used, or disclosed to a service provider or contractor, for additional, specified purposes and that consumers have the right to limit the use or disclosure of their sensitive personal information.

(b) A business that has received direction from a consumer not to use or disclose the consumer's sensitive personal information, except as authorized by subdivision (a), shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from using or disclosing the consumer's sensitive personal information for any other purpose after its receipt of the consumer's direction unless the consumer subsequently provides consent for the use or disclosure of the consumer's sensitive personal information for additional purposes.

(c) A service provider or contractor that assists a business in performing the purposes authorized by subdivision (a) may not use the sensitive personal information after it has received instructions from the business and to the extent it has actual knowledge that the personal information is sensitive

personal information for any other purpose. A service provider or contractor is only required to limit its use of sensitive personal information received pursuant to a written contract with the business in response to instructions from the business and only with respect to its relationship with that business.

(d) Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to this section, as further defined in regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185, and shall be treated as personal information for purposes of all other sections of this act, including Section 1798.100.

(Added November 3, 2020, by initiative Proposition 24, Sec. 10. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.125. (a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(2) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.

(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the business by the consumer's data.

(2) A business that offers any financial incentives pursuant to this subdivision shall notify consumers of the financial incentives pursuant to Section 1798.130.

(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.130 that clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.

(4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

(Amended by Stats. 2019, Ch. 757, Sec. 5. (AB 1355) Effective January 1, 2020. Superseded on January 1, 2023; see amendment by Proposition 24.)

1798.125. Consumers' Right of No Retaliation Following Opt Out or Exercise of Other Rights

(a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(E) Retaliating against an employee, applicant for employment, or independent contractor, as defined in subparagraph (A) of paragraph (2) of subdivision (m) of Section 1798.145, for exercising their rights under this title.

(2) Nothing in this subdivision prohibits a business, pursuant to subdivision (b), from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.

(3) This subdivision does not prohibit a business from offering loyalty, rewards, premium features, discounts, or club card programs consistent with this title.

(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale or sharing of personal information, or the retention of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is reasonably related to the value provided to the business by the consumer's data.

(2) A business that offers any financial incentives pursuant to this subdivision, shall notify consumers of the financial incentives pursuant to Section 1798.130.

(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.130 that clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time. If a consumer refuses to provide opt-in consent, then the business shall wait for at least 12 months before next requesting that the consumer provide opt-in consent, or as prescribed by regulations adopted pursuant to Section 1798.185.

(4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 11. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.130. (a) In order to comply with Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

(1) (A) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

(B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

(2) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business' duty to disclose and deliver the information within 45 days of receipt of the consumer's request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business' receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or

electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request. If the consumer maintains an account with the business, the business may require the consumer to submit the request through that account.

(3) For purposes of subdivision (b) of Section 1798.110:

(A) To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected.

(4) For purposes of subdivision (b) of Section 1798.115:

(A) Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information of the consumer that the business sold in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).

(C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall

disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its internet website and update that information at least once every 12 months:

(A) A description of a consumer's rights pursuant to Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125 and one or more designated methods for submitting requests.

(B) For purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.

(C) For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:

(i) A list of the categories of personal information it has sold about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold, or if the business has not sold consumers' personal information in the preceding 12 months, the business shall disclose that fact.

(ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describe the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(D) In the case of a business that sells or discloses deidentified patient information not subject to this title pursuant to clause (i) of subparagraph (A) of paragraph (4) of subdivision (a) of Section 1798.146, whether the business sells or discloses deidentified patient information derived from patient information and if so, whether that patient information was deidentified pursuant to one or more of the following:

(i) The deidentification methodology described in Section 164.514(b)(1) of Title 45 of the Code of Federal Regulations, commonly known as the HIPAA expert determination method.

(ii) The deidentification methodology described in Section 164.514(b)(2) of Title 45 of the Code of Federal Regulations, commonly known as the HIPAA safe harbor method.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business' privacy practices or the business' compliance with this title are informed of all requirements in Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

(7) Use any personal information collected from the consumer in connection with the business' verification of the consumer's request solely for the purposes of verification.

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections 1798.110 and 1798.115 shall follow the definition of personal information in Section 1798.140.

(Amended by Stats. 2020, Ch. 172, Sec. 1. (AB 713) Effective September 25, 2020. Superseded on January 1, 2023; see amendment by Proposition 24.)

1798.130. Notice, Disclosure, Correction, and Deletion Requirements

(a) In order to comply with Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

(1) (A) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively, including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or for requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively.

(B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively.

(2) (A) Disclose and deliver the required information to a consumer free of charge, correct inaccurate personal information, or delete a consumer's personal information, based on the consumer's request, within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall

not extend the business's duty to disclose and deliver the information, to correct inaccurate personal information, or to delete personal information within 45 days of receipt of the consumer's request. The time period to provide the required information, to correct inaccurate personal information, or to delete personal information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure of the required information shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request provided that if the consumer, has an account with the business, the business may require the consumer to use that account to submit a verifiable consumer request.

(B) The disclosure of the required information shall cover the 12-month period preceding the business' receipt of the verifiable consumer request provided that, upon the adoption of a regulation pursuant to paragraph (9) of subdivision (a) of Section 1798.185, a consumer may request that the business disclose the required information beyond the 12-month period, and the business shall be required to provide that information unless doing so proves impossible or would involve a disproportionate effort. A consumer's right to request required information beyond the 12-month period, and a business's obligation to provide that information, shall only apply to personal information collected on or after January 1, 2022. Nothing in this subparagraph shall require a business to keep personal information for any length of time.

(3) (A) A business that receives a verifiable consumer request pursuant to Section 1798.110 or 1798.115 shall disclose any personal information it has collected about a consumer, directly or indirectly, including through or by a service provider or contractor, to the consumer. A service provider or contractor shall not be required to comply with a verifiable consumer request received directly from a consumer or a consumer's authorized agent, pursuant to Section 1798.110 or 1798.115, to the extent that the service provider or contractor has collected personal information about the consumer in its role as a service provider or contractor. A service provider or contractor shall provide assistance to a business with which it has a contractual relationship with respect to the business' response to a verifiable consumer request, including, but not limited to, by providing to the business the

consumer's personal information in the service provider or contractor's possession, which the service provider or contractor obtained as a result of providing services to the business, and by correcting inaccurate information or by enabling the business to do the same. A service provider or contractor that collects personal information pursuant to a written contract with a business shall be required to assist the business through appropriate technical and organizational measures in complying with the requirements of subdivisions (d) to (f), inclusive, of Section 1798.100, taking into account the nature of the processing.

(B) For purposes of subdivision (b) of Section 1798.110:

(i) To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(ii) Identify by category or categories the personal information collected about the consumer for the applicable period of time by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected; the categories of sources from which the consumer's personal information was collected; the business or commercial purpose for collecting, selling, or sharing the consumer's personal information; and the categories of third parties to whom the business discloses the consumer's personal information.

(iii) Provide the specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance. "Specific pieces of information" do not include data generated to help ensure security and integrity or as prescribed by regulation. Personal information is not considered to have been disclosed by a business when a consumer instructs a business to transfer the consumer's personal information from one business to another in the context of switching services.

(4) For purposes of subdivision (b) of Section 1798.115:

(A) Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information of the consumer that the business sold or shared during the applicable period of time by reference to the enumerated category in subdivision

(c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold or shared during the applicable period of time by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold or shared. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).

(C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose during the applicable period of time by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of persons to whom the consumer's personal information was disclosed for a business purpose during the applicable period of time by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its internet website, and update that information at least once every 12 months:

(A) A description of a consumer's rights pursuant to Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, and 1798.125 and two or more designated methods for submitting requests, except as provided in subparagraph (A) of paragraph (1) of subdivision (a).

(B) For purposes of subdivision (c) of Section 1798.110:

(i) A list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.

(ii) The categories of sources from which consumers' personal information is collected.

(iii) The business or commercial purpose for collecting, selling, or sharing consumers' personal information.

(iv) The categories of third parties to whom the business discloses consumers' personal information.

(C) For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:

(i) A list of the categories of personal information it has sold or shared about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold or shared, or if the business has not sold or shared consumers' personal information in the preceding 12 months, the business shall prominently disclose that fact in its privacy policy.

(ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business' privacy practices or the business' compliance with this title are informed of all requirements in Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

(7) Use any personal information collected from the consumer in connection with the business' verification of the consumer's request solely for the purposes of verification and shall not further disclose the personal information, retain it longer than necessary for purposes of verification, or use it for unrelated purposes.

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections 1798.100, 1798.110, and 1798.115 shall follow the definitions of personal information and sensitive personal information in Section 1798.140 by describing the categories of personal information using the specific terms set forth in subparagraphs (A) to (K), inclusive, of paragraph (1) of subdivision (v) of Section 1798.140 and by describing the categories of sensitive personal information using the specific terms set forth in paragraphs (1) to (9), inclusive, of subdivision (ae) of Section 1798.140.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 12. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.135. (a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.

(2) Include a description of a consumer's rights pursuant to Section 1798.120, along with a separate link to the "Do Not Sell My Personal Information" Internet Web page in:

(A) Its online privacy policy or policies if the business has an online privacy policy or policies.

(B) Any California-specific description of consumers' privacy rights.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Section 1798.120 and this section and how to direct consumers to exercise their rights under those sections.

(4) For consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer.

(5) For a consumer who has opted-out of the sale of the consumer's personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information.

(6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

(b) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

(c) A consumer may authorize another person solely to opt-out of the sale of the consumer's personal information on the consumer's behalf, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 8. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198. Superseded on January 1, 2023; see amendment by Proposition 24.)

1798.135. Methods of Limiting Sale, Sharing, and Use of Personal Information and Use of Sensitive Personal Information

(a) A business that sells or shares consumers' personal information or uses or discloses consumers' sensitive personal information for purposes other than those authorized by subdivision (a) of Section 1798.121 shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business's internet homepages, titled "Do Not Sell or Share My Personal Information," to an internet web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale or sharing of the consumer's personal information.

(2) Provide a clear and conspicuous link on the business' internet homepages, titled "Limit the Use of My Sensitive Personal Information," that enables a consumer, or a person authorized by the consumer, to limit the use or disclosure of the consumer's sensitive personal information to those uses authorized by subdivision (a) of Section 1798.121.

(3) At the business' discretion, utilize a single, clearly labeled link on the business' internet homepages, in lieu of complying with paragraphs (1) and (2), if that link easily allows a consumer to opt out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information.

(4) In the event that a business responds to opt-out requests received pursuant to paragraph (1), (2), or (3) by informing the consumer of a charge for the use of any product or service, present the terms of any financial incentive offered pursuant to subdivision (b) of Section 1798.125 for the retention, use, sale, or sharing of the consumer's personal information.

(b) (1) A business shall not be required to comply with subdivision (a) if the business allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications set forth in regulations adopted pursuant to paragraph (20) of subdivision (a) of Section 1798.185, to the business indicating the consumer's intent to opt out of the business' sale or sharing of the consumer's personal information or to limit the use or disclosure of the consumer's sensitive personal information, or both.

(2) A business that allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information pursuant to paragraph (1) may provide a link to a web page that enables the consumer to consent to the business ignoring the opt-out preference signal with respect to that business' sale or sharing of the consumer's personal information or the use of the consumer's sensitive personal information for additional purposes provided that:

(A) The consent web page also allows the consumer or a person authorized by the consumer to revoke the consent as easily as it is affirmatively provided.

(B) The link to the web page does not degrade the consumer's experience on the web page the consumer intends to visit and has a similar look, feel, and size relative to other links on the same web page.

(C) The consent web page complies with technical specifications set forth in regulations adopted pursuant to paragraph (20) of subdivision (a) of Section 1798.185.

(3) A business that complies with subdivision (a) is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b).

(c) A business that is subject to this section shall:

(1) Not require a consumer to create an account or provide additional information beyond what is necessary in order to direct the business not to sell or share the consumer's personal information or to limit use or disclosure of the consumer's sensitive personal information.

(2) Include a description of a consumer's rights pursuant to Sections 1798.120 and 1798.121, along with a separate link to the "Do Not Sell or Share My Personal Information" internet web page and a separate link to the "Limit the Use of My Sensitive Personal Information" internet web page, if applicable, or a single link to both choices, or a statement that the business responds to and abides by opt-out preference signals sent by a platform, technology, or mechanism in accordance with subdivision (b), in:

(A) Its online privacy policy or policies if the business has an online privacy policy or policies.

(B) Any California-specific description of consumers' privacy rights.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in

Sections 1798.120, 1798.121, and this section and how to direct consumers to exercise their rights under those sections.

(4) For consumers who exercise their right to opt-out of the sale or sharing of their personal information or limit the use or disclosure of their sensitive personal information, refrain from selling or sharing the consumer's personal information or using or disclosing the consumer's sensitive personal information and wait for at least 12 months before requesting that the consumer authorize the sale or sharing of the consumer's personal information or the use and disclosure of the consumer's sensitive personal information for additional purposes, or as authorized by regulations.

(5) For consumers under 16 years of age who do not consent to the sale or sharing of their personal information, refrain from selling or sharing the personal information of the consumer under 16 years of age and wait for at least 12 months before requesting the consumer's consent again, or as authorized by regulations or until the consumer attains 16 years of age.

(6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

(d) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

(e) A consumer may authorize another person to opt-out of the sale or sharing of the consumer's personal information and to limit the use of the consumer's sensitive personal information on the consumer's behalf, including through an opt-out preference signal, as defined in paragraph (1) of subdivision (b), indicating the consumer's intent to opt out, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General regardless of whether the business has elected to comply with subdivision (a) or (b). For purposes of clarity, a business that elects to comply with subdivision (a) may respond to the consumer's opt-out consistent with Section 1798.125.

(f) If a business communicates a consumer's opt-out request to any person authorized by the business to collect personal information, the person shall thereafter only use that consumer's personal

information for a business purpose specified by the business, or as otherwise permitted by this title, and shall be prohibited from:

(1) Selling or sharing the personal information.

(2) Retaining, using, or disclosing that consumer's personal information.

(A) For any purpose other than for the specific purpose of performing the services offered to the business.

(B) Outside of the direct business relationship between the person and the business.

(C) For a commercial purpose other than providing the services to the business.

(g) A business that communicates a consumer's opt-out request to a person pursuant to subdivision (f) shall not be liable under this title if the person receiving the opt-out request violates the restrictions set forth in the title provided that, at the time of communicating the opt-out request, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation. Any provision of a contract or agreement of any kind that purports to waive or limit in any way this subdivision shall be void and unenforceable.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 13. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.140. For purposes of this title:

(a) "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been de-identified.

(b) "Biometric information" means an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(c) "Business" means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) Has annual gross revenues in excess of twenty-five million dollars (\$25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

(2) Any entity that controls or is controlled by a business as defined in paragraph (1) and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark.

(d) "Business purpose" means the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are:

(1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, provided that the personal information is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.

(5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.

(6) Undertaking internal research for technological development and demonstration.

(7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

(e) "Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.

(f) "Commercial purposes" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. "Commercial purposes" do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

(g) "Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

(h) "Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

- (2) Has implemented business processes that specifically prohibit reidentification of the information.
- (3) Has implemented business processes to prevent inadvertent release of deidentified information.
- (4) Makes no attempt to reidentify the information.
- (i) "Designated methods for submitting requests" means a mailing address, email address, internet web page, internet web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.
- (j) "Device" means any physical object that is capable of connecting to the internet, directly or indirectly, or to another device.
- (k) "Health insurance information" means a consumer's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer's application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.
- (l) "Homepage" means the introductory page of an internet website and any internet web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information," or settings page, and any other location that allows consumers to review the notice required by subdivision (a) of Section 1798.135, including, but not limited to, before downloading the application.
- (m) "Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.
- (n) "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.
- (o) (1) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following

if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

(B) Any categories of personal information described in subdivision (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(2) "Personal information" does not include publicly available information. For purposes of this paragraph, "publicly available" means information that is lawfully made available from federal, state, or local government records. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

(3) "Personal information" does not include consumer information that is deidentified or aggregate consumer information.

(p) “Probabilistic identifier” means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

(q) “Processing” means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.

(r) “Pseudonymize” or “Pseudonymization” means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

(s) “Research” means scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer’s interactions with a business’s service or device for other purposes shall be:

(1) Compatible with the business purpose for which the personal information was collected.

(2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.

(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(4) Subject to business processes that specifically prohibit reidentification of the information.

(5) Made subject to business processes to prevent inadvertent release of deidentified information.

(6) Protected from any reidentification attempts.

(7) Used solely for research purposes that are compatible with the context in which the personal information was collected.

(8) Not be used for any commercial purpose.

(9) Subjected by the business conducting the research to additional security controls that limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.

(t) (1) “Sell,” “selling,” “sale,” or “sold,” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.

(2) For purposes of this title, a business does not sell personal information when:

(A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer’s intent to interact with a third party.

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer’s personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer’s personal information.

(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:

(i) The business has provided notice of that information being used or shared in its terms and conditions consistent with Section 1798.135.

(ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

(D) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with Sections 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with Section 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(u) "Service" or "services" means work, labor, and services, including services furnished in connection with the sale or repair of goods.

(v) "Service provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

(w) "Third party" means a person who is not any of the following:

(1) The business that collects personal information from consumers under this title.

(2) (A) A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:

(i) Prohibits the person receiving the personal information from:

(I) Selling the personal information.

(II) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.

(III) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.

(ii) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

(B) A person covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at

the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation.

(x) "Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

(y) "Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.100, 1798.105, 1798.110, and 1798.115 if the business cannot verify, pursuant to this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

(Amended by Stats. 2019, Ch. 757, Sec. 7.5. (AB 1355) Effective January 1, 2020. Superseded on January 1, 2023; see amendment by Proposition 24.)

1798.140. Definitions

For purposes of this title:

(a) "Advertising and marketing" means a communication by a business or a person acting on the business' behalf in any medium intended to induce a consumer to obtain goods, services, or employment.

(b) "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or

reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.

(c) "Biometric information" means an individual's physiological, biological, or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(d) "Business" means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars (\$25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or households.

(C) Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business and with whom the business shares consumers' personal information. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding"

means a shared name, servicemark, or trademark that the average consumer would understand that two or more entities are commonly owned.

(3) A joint venture or partnership composed of businesses in which each business has at least a 40 percent interest. For purposes of this title, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.

(4) A person that does business in California, that is not covered by paragraph (1), (2), or (3), and that voluntarily certifies to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by, this title.

(e) "Business purpose" means the use of personal information for the business' operational purposes, or other notified purposes, or for the service provider or contractor's operational purposes, as defined by regulations adopted pursuant to paragraph (11) of subdivision (a) of Section 1798.185, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed or for another purpose that is compatible with the context in which the personal information was collected. Business purposes are:

(1) Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.

(5) Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.

(6) Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers.

(7) Undertaking internal research for technological development and demonstration.

(8) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

(f) “Collects,” “collected,” or “collection” means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer’s behavior.

(g) “Commercial purposes” means to advance a person’s commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.

(h) “Consent” means any freely given, specific, informed, and unambiguous indication of the consumer’s wishes by which the consumer, or the consumer’s legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.

(i) “Consumer” means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

(j) (1) “Contractor” means a person to whom the business makes available a consumer’s personal information for a business purpose, pursuant to a written contract with the business, provided that the contract:

(A) Prohibits the contractor from:

(i) Selling or sharing the personal information.

(ii) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract, or as otherwise permitted by this title.

(iii) Retaining, using, or disclosing the information outside of the direct business relationship between the contractor and the business.

(iv) Combining the personal information that the contractor receives pursuant to a written contract with the business with personal information that it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, provided that the contractor may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) and in regulations adopted by the California Privacy Protection Agency.

(B) Includes a certification made by the contractor that the contractor understands the restrictions in subparagraph (A) and will comply with them.

(C) Permits, subject to agreement with the contractor, the business to monitor the contractor’s compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.

(2) If a contractor engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the contractor engages another person to assist in processing personal information for that business purpose, it shall notify the business of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).

(k) “Cross-context behavioral advertising” means the targeting of advertising to a consumer based on the consumer’s personal information obtained from the consumer’s activity across businesses,

distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

(l) “Dark pattern” means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation.

(m) “Deidentified” means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possesses the information:

(1) Takes reasonable measures to ensure that the information cannot be associated with a consumer or household.

(2) Publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision.

(3) Contractually obligates any recipients of the information to comply with all provisions of this subdivision.

(n) “Designated methods for submitting requests” means a mailing address, email address, internet web page, internet web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

(o) “Device” means any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device.

(p) “Homepage” means the introductory page of an internet website and any internet web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application’s platform page or download page, a link within the application, such as from the application configuration, “About,” “Information,” or settings page, and any other location that allows consumers to review the notices required by this title, including, but not limited to, before downloading the application.

(q) “Household” means a group, however identified, of consumers who cohabitate with one another at the same residential address and share use of common devices or services.

(r) “Infer” or “inference” means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(s) “Intentionally interacts” means when the consumer intends to interact with a person, or disclose personal information to a person, via one or more deliberate interactions, including visiting the person’s website or purchasing a good or service from the person. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer’s intent to interact with a person.

(t) “Nonpersonalized advertising” means advertising and marketing that is based solely on a consumer’s personal information derived from the consumer’s current interaction with the business with the exception of the consumer’s precise geolocation.

(u) “Person” means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(v) (1) “Personal information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.

(B) Any personal information described in subdivision (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an internet website application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(L) Sensitive personal information.

(2) "Personal information" does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. For purposes of this paragraph, "publicly available" means: information that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

(3) "Personal information" does not include consumer information that is deidentified or aggregate consumer information.

(w) "Precise geolocation" means any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as prescribed by regulations.

(x) "Probabilistic identifier" means the identification of a consumer or a consumer's device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

(y) "Processing" means any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means.

(z) "Profiling" means any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185, to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning

that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(aa) "Pseudonymize" or "Pseudonymization" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

(ab) "Research" means scientific analysis, systematic study, and observation, including basic research or applied research that is designed to develop or contribute to public or scientific knowledge and that adheres or otherwise conforms to all other applicable ethics and privacy laws, including, but not limited to, studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business' service or device for other purposes shall be:

- (1) Compatible with the business purpose for which the personal information was collected.
- (2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, by a business.
- (3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain, other than as needed to support the research.
- (4) Subject to business processes that specifically prohibit reidentification of the information, other than as needed to support the research.
- (5) Made subject to business processes to prevent inadvertent release of deidentified information.
- (6) Protected from any reidentification attempts.
- (7) Used solely for research purposes that are compatible with the context in which the personal information was collected.
- (8) Subjected by the business conducting the research to additional security controls that limit access to the research data to only those individuals as are necessary to carry out the research purpose.

(ac) "Security and integrity" means the ability of:

- (1) Networks or information systems to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.

(2) Businesses to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions and to help prosecute those responsible for those actions.

(3) Businesses to ensure the physical safety of natural persons.

(ad) (1) “Sell,” “selling,” “sale,” or “sold,” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to a third party for monetary or other valuable consideration.

(2) For purposes of this title, a business does not sell personal information when:

(A) A consumer uses or directs the business to intentionally:

(i) Disclose personal information.

(ii) Interact with one or more third parties.

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer’s personal information or limited the use of the consumer’s sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sale of the consumer’s personal information or limited the use of the consumer’s sensitive personal information.

(C) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with this title. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with this title. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(ae) “Sensitive personal information” means:

(1) Personal information that reveals:

(A) A consumer’s social security, driver’s license, state identification card, or passport number.

(B) A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

(C) A consumer's precise geolocation.

(D) A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership.

(E) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.

(F) A consumer's genetic data.

(2) (A) The processing of biometric information for the purpose of uniquely identifying a consumer.

(B) Personal information collected and analyzed concerning a consumer's health.

(C) Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

(3) Sensitive personal information that is "publicly available" pursuant to paragraph (2) of subdivision (v) shall not be considered sensitive personal information or personal information.

(af) "Service" or "services" means work, labor, and services, including services furnished in connection with the sale or repair of goods.

(ag) (1) "Service provider" means a person that processes personal information on behalf of a business and that receives from or on behalf of the business consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the person from:

(A) Selling or sharing the personal information.

(B) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract for the business, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract with the business, or as otherwise permitted by this title.

(C) Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business.

(D) Combining the personal information that the service provider receives from, or on behalf of, the business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that the service provider may combine personal information to perform any business purpose as defined in regulations adopted

pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of this section and in regulations adopted by the California Privacy Protection Agency. The contract may, subject to agreement with the service provider, permit the business to monitor the service provider's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.

(2) If a service provider engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the service provider engages another person to assist in processing personal information for that business purpose, it shall notify the business of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).

(ah) (1) "Share," "shared," or "sharing" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

(2) For purposes of this title, a business does not share personal information when:

(A) A consumer uses or directs the business to intentionally disclose personal information or intentionally interact with one or more third parties.

(B) The business uses or shares an identifier for a consumer who has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information.

(C) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with this title. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently

with this title. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(ai) “Third party” means a person who is not any of the following:

(1) The business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer’s current interaction with the business under this title.

(2) A service provider to the business.

(3) A contractor.

(aj) “Unique identifier” or “unique personal identifier” means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device that is linked to a consumer or family. For purposes of this subdivision, “family” means a custodial parent or guardian and any children under 18 years of age over which the parent or guardian has custody.

(ak) “Verifiable consumer request” means a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, or by a person who has power of attorney or is acting as a conservator for the consumer, and that the business can verify, using commercially reasonable methods, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115, to delete personal information pursuant to Section 1798.105, or to correct inaccurate personal information pursuant to Section 1798.106, if the business cannot verify, pursuant to this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer’s behalf.

(Amended (as amended November 3, 2020, by Prop. 24, Sec. 14) by Stats. 2021, Ch. 525, Sec. 3. (AB 694) Effective January 1, 2022.)

1798.145. (a) The obligations imposed on businesses by this title shall not restrict a business' ability to:

(1) Comply with federal, state, or local laws.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(4) Exercise or defend legal claims.

(5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.

(6) Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

(b) The obligations imposed on businesses by Sections 1798.110 to 1798.135, inclusive, shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

(c) (1) This title shall not apply to any of the following:

(A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45

of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.

(2) For purposes of this subdivision, the definitions of “medical information” and “provider of health care” in Section 56.05 shall apply and the definitions of “business associate,” “covered entity,” and “protected health information” in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

(d) (1) This title shall not apply to an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in subdivision (f) of Section 1681a of Title 15 of the United States Code, by a furnisher of information, as set forth in Section 1681s-2 of Title 15 of the United States Code, who provides information for use in a consumer report, as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code, and by a user of a consumer report as set forth in Section 1681b of Title 15 of the United States Code.

(2) Paragraph (1) shall apply only to the extent that such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act, Section 1681 et seq., Title 15 of the United States Code and the information is not used, communicated, disclosed, or sold except as authorized by the Fair Credit Reporting Act.

(3) This subdivision shall not apply to Section 1798.150.

(e) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code). This subdivision shall not apply to Section 1798.150.

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.). This subdivision shall not apply to Section 1798.150.

(g) (1) Section 1798.120 shall not apply to vehicle information or ownership information retained or shared between a new motor vehicle dealer, as defined in Section 426 of the Vehicle Code, and the vehicle's manufacturer, as defined in Section 672 of the Vehicle Code, if the vehicle information or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall conducted pursuant to Sections 30118 to 30120, inclusive, of Title 49 of the United States Code, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose.

(2) Section 1798.120 shall not apply to vessel information or ownership information retained or shared between a vessel dealer and the vessel's manufacturer, as defined in Section 651 of the Harbors and Navigation Code, if the vessel information or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vessel repair covered by a vessel warranty or a recall conducted pursuant to Section 4310 of Title 46 of the United States Code, provided that the vessel dealer or vessel manufacturer with which that vessel information or ownership information is shared does not sell, share, or use that information for any other purpose.

(3) For purposes of this subdivision:

(A) "Ownership information" means the name or names of the registered owner or owners and the contact information for the owner or owners.

(B) "Vehicle information" means the vehicle information number, make, model, year, and odometer reading.

(C) "Vessel dealer" means a person who is engaged, wholly or in part, in the business of selling or offering for sale, buying or taking in trade for the purpose of resale, or exchanging, any vessel or

vessels, as defined in Section 651 of the Harbors and Navigation Code, and receives or expects to receive money, profit, or any other thing of value.

(D) "Vessel information" means the hull identification number, model, year, month and year of production, and information describing any of the following equipment as shipped, transferred, or sold from the place of manufacture, including all attached parts and accessories:

(i) An inboard engine.

(ii) An outboard engine.

(iii) A stern drive unit.

(iv) An inflatable personal flotation device approved under Section 160.076 of Title 46 of the Code of Federal Regulations.

(h) (1) This title shall not apply to any of the following:

(A) Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business.

(B) Personal information that is collected by a business that is emergency contact information of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the personal information is collected and used solely within the context of having an emergency contact on file.

(C) Personal information that is necessary for the business to retain to administer benefits for another natural person relating to the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the personal information is collected and used solely within the context of administering those benefits.

(2) For purposes of this subdivision:

(A) "Contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Medical staff member" means a licensed physician and surgeon, dentist, or podiatrist, licensed pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code and a clinical psychologist as defined in Section 1316.5 of the Health and Safety Code.

(D) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(E) "Owner" means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall not apply to subdivision (b) of Section 1798.100 or Section 1798.150.

(4) This subdivision shall become inoperative on January 1, 2021.

(i) Notwithstanding a business' obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to any verified consumer request may be extended by up to 90 additional days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The

business shall bear the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.

(j) A business that discloses personal information to a service provider shall not be liable under this title if the service provider receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title.

(k) This title shall not be construed to require a business to collect personal information that it would not otherwise collect in the ordinary course of its business, retain personal information for longer than it would otherwise retain such information in the ordinary course of its business, or reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

(l) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers.

(m) The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution.

(n) (1) The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit, or government agency.

(2) For purposes of this subdivision:

(A) "Contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) “Director” means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) “Officer” means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(D) “Owner” means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall become inoperative on January 1, 2021.

(Amended (as amended by Stats. 2019, Ch. 763, Sec. 2.3) by Stats. 2021, Ch. 700, Sec. 1. (AB 335) Effective January 1, 2022. Superseded on January 1, 2023; see amendment by Proposition 24. But see now the immediately operative subdivisions (m) and (n) in Prop. 24’s amendment. Note: In Prop. 24’s amendment, on December 16, 2020, its new subd. (m) becomes operative, and its subd. (n) supersedes the subd. (n) in this version.)

1798.145. Exemptions

(a) The obligations imposed on businesses by this title shall not restrict a business’ ability to:

(1) Comply with federal, state, or local laws or comply with a court order or subpoena to provide information.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities. Law enforcement agencies, including police and sheriff’s departments, may direct a business pursuant to a law enforcement agency-approved investigation with an active case number not to delete a consumer’s personal information, and, upon receipt of that direction, a business shall not delete the personal information for 90 days in order to allow the law enforcement agency to obtain a court-issued subpoena, order, or warrant to obtain a consumer’s personal information. For good cause and only to the extent necessary for investigatory purposes, a law enforcement agency may direct a business not to delete the consumer’s personal information for additional 90-day periods. A business that has received direction from a law enforcement agency not

to delete the personal information of a consumer who has requested deletion of the consumer's personal information shall not use the consumer's personal information for any purpose other than retaining it to produce to law enforcement in response to a court-issued subpoena, order, or warrant unless the consumer's deletion request is subject to an exemption from deletion under this title.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(4) Cooperate with a government agency request for emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury provided that:

(A) The request is approved by a high-ranking agency officer for emergency access to a consumer's personal information.

(B) The request is based on the agency's good faith determination that it has a lawful basis to access the information on a nonemergency basis.

(C) The agency agrees to petition a court for an appropriate order within three days and to destroy the information if that order is not granted.

(5) Exercise or defend legal claims.

(6) Collect, use, retain, sell, share, or disclose consumers' personal information that is deidentified or aggregate consumer information.

(7) Collect, sell, or share a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not prohibit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

(b) The obligations imposed on businesses by Sections 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, and 1798.135 shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

(c) (1) This title shall not apply to any of the following:

(A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) Personal information collected as part of a clinical trial or other biomedical research study subject to, or conducted in accordance with, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration, provided that the information is not sold or shared in a manner not permitted by this subparagraph, and, if it is inconsistent, that participants be informed of that use and provide consent.

(2) For purposes of this subdivision, the definitions of “medical information” and “provider of health care” in Section 56.05 shall apply and the definitions of “business associate,” “covered entity,” and “protected health information” in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

(d) (1) This title shall not apply to an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer’s creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in subdivision (f) of Section 1681a of Title 15 of the United States Code, by a furnisher of information, as set forth in Section 1681s-2 of Title 15 of the United States Code, who provides information for use in a consumer report, as defined in subdivision (d) of

Section 1681a of Title 15 of the United States Code, and by a user of a consumer report as set forth in Section 1681b of Title 15 of the United States Code.

(2) Paragraph (1) shall apply only to the extent that such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act, Section 1681 et seq., Title 15 of the United States Code and the information is not collected, maintained, used, communicated, disclosed, or sold except as authorized by the Fair Credit Reporting Act.

(3) This subdivision shall not apply to Section 1798.150.

(e) This title shall not apply to personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code), or the federal Farm Credit Act of 1971 (as amended in 12 U.S.C. 2001-2279cc and implementing regulations, 12 C.F.R. 600, et seq.). This subdivision shall not apply to Section 1798.150.

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.). This subdivision shall not apply to Section 1798.150.

(g) (1) Section 1798.120 shall not apply to vehicle information or ownership information retained or shared between a new motor vehicle dealer, as defined in Section 426 of the Vehicle Code, and the vehicle's manufacturer, as defined in Section 672 of the Vehicle Code, if the vehicle information or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall conducted pursuant to Sections 30118 to 30120, inclusive, of Title 49 of the United States Code, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose.

(2) Section 1798.120 shall not apply to vessel information or ownership information retained or shared between a vessel dealer and the vessel's manufacturer, as defined in Section 651 of the Harbors and Navigation Code, if the vessel information or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vessel repair covered by a vessel warranty or a recall conducted pursuant to Section 4310 of Title 46 of the United States Code, provided that the vessel dealer or vessel manufacturer with which that vessel information or ownership information is shared does not sell, share, or use that information for any other purpose.

(3) For purposes of this subdivision:

(A) "Ownership information" means the name or names of the registered owner or owners and the contact information for the owner or owners.

(B) "Vehicle information" means the vehicle information number, make, model, year, and odometer reading.

(C) "Vessel dealer" means a person who is engaged, wholly or in part, in the business of selling or offering for sale, buying or taking in trade for the purpose of resale, or exchanging, any vessel or vessels, as defined in Section 651 of the Harbors and Navigation Code, and receives or expects to receive money, profit, or any other thing of value.

(D) "Vessel information" means the hull identification number, model, year, month and year of production, and information describing any of the following equipment as shipped, transferred, or sold from the place of manufacture, including all attached parts and accessories:

(i) An inboard engine.

(ii) An outboard engine.

(iii) A stern drive unit.

(iv) An inflatable personal floatation device approved under Section 160.076 of Title 46 of the Code of Federal Regulations.

(h) Notwithstanding a business' obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to a consumer for any verifiable consumer request may be extended by up to a total of 90 days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested,

or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verifiable consumer request is manifestly unfounded or excessive.

(i) (1) A business that discloses personal information to a service provider or contractor in compliance with this title shall not be liable under this title if the service provider or contractor receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider or contractor intends to commit such a violation. A service provider or contractor shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title provided that the service provider or contractor shall be liable for its own violations of this title.

(2) A business that discloses personal information of a consumer, with the exception of consumers who have exercised their right to opt out of the sale or sharing of their personal information, consumers who have limited the use or disclosure of their sensitive personal information, and minor consumers who have not opted in to the collection or sale of their personal information, to a third party pursuant to a written contract that requires the third party to provide the same level of protection of the consumer's rights under this title as provided by the business shall not be liable under this title if the third party receiving the personal information uses it in violation of the restrictions set forth in this title provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the third party intends to commit such a violation.

(j) This title shall not be construed to require a business, service provider, or contractor to:

(1) Reidentify or otherwise link information that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

(2) Retain any personal information about a consumer if, in the ordinary course of business, that information about the consumer would not be retained.

(3) Maintain information in identifiable, linkable, or associable form, or collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating a verifiable consumer request with personal information.

(k) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other natural persons. A verifiable consumer request

for specific pieces of personal information pursuant to Section 1798.110, to delete a consumer's personal information pursuant to Section 1798.105, or to correct inaccurate personal information pursuant to Section 1798.106, shall not extend to personal information about the consumer that belongs to, or the business maintains on behalf of, another natural person. A business may rely on representations made in a verifiable consumer request as to rights with respect to personal information and is under no legal requirement to seek out other persons that may have or claim to have rights to personal information, and a business is under no legal obligation under this title or any other provision of law to take any action under this title in the event of a dispute between or among persons claiming rights to personal information in the business' possession.

(l) The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution.

(m) (1) This title shall not apply to any of the following:

(A) Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or an independent contractor of, that business.

(B) Personal information that is collected by a business that is emergency contact information of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that business to the extent that the personal information is collected and used solely within the context of having an emergency contact on file.

(C) Personal information that is necessary for the business to retain to administer benefits for another natural person relating to the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that business to the extent that the personal information is collected and used solely within the context of administering those benefits.

(2) For purposes of this subdivision:

(A) "Independent contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) “Director” means a natural person designated in the articles of incorporation as director, or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) “Medical staff member” means a licensed physician and surgeon, dentist, or podiatrist, licensed pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code and a clinical psychologist as defined in Section 1316.5 of the Health and Safety Code.

(D) “Officer” means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, including a chief executive officer, president, secretary, or treasurer.

(E) “Owner” means a natural person who meets one of the following criteria:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall not apply to subdivision (a) of Section 1798.100 or Section 1798.150.

(4) This subdivision shall become inoperative on January 1, 2023.

(n) (1) The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.121, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who acted or is acting as an employee, owner, director, officer, or independent contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit, or government agency.

(2) For purposes of this subdivision:

(A) “Independent contractor” means a natural person who provides any service to a business pursuant to a written contract.

(B) “Director” means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(D) "Owner" means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall become inoperative on January 1, 2023.

(o) (1) Sections 1798.105 and 1798.120 shall not apply to a commercial credit reporting agency's collection, processing, sale, or disclosure of business controller information to the extent the commercial credit reporting agency uses the business controller information solely to identify the relationship of a consumer to a business that the consumer owns or contact the consumer only in the consumer's role as the owner, director, officer, or management employee of the business.

(2) For the purposes of this subdivision:

(A) "Business controller information" means the name or names of the owner or owners, director, officer, or management employee of a business and the contact information, including a business title, for the owner or owners, director, officer, or management employee.

(B) "Commercial credit reporting agency" has the meaning set forth in subdivision (b) of Section 1785.42.

(C) "Owner" means a natural person that meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(D) "Director" means a natural person designated in the articles of incorporation of a business as director, or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(E) “Officer” means a natural person elected or appointed by the board of directors of a business to manage the daily operations of a corporation, including a chief executive officer, president, secretary, or treasurer.

(F) “Management employee” means a natural person whose name and contact information is reported to or collected by a commercial credit reporting agency as the primary manager of a business and used solely within the context of the natural person’s role as the primary manager of the business.

(p) The obligations imposed on businesses in Sections 1798.105, 1798.106, 1798.110, and 1798.115 shall not apply to household data.

(q) (1) This title does not require a business to comply with a verifiable consumer request to delete a consumer’s personal information under Section 1798.105 to the extent the verifiable consumer request applies to a student’s grades, educational scores, or educational test results that the business holds on behalf of a local educational agency, as defined in subdivision (d) of Section 49073.1 of the Education Code, at which the student is currently enrolled. If a business does not comply with a request pursuant to this section, it shall notify the consumer that it is acting pursuant to this exception.

(2) This title does not require, in response to a request pursuant to Section 1798.110, that a business disclose on educational standardized assessment or educational assessment or a consumer’s specific responses to the educational standardized assessment or educational assessment if consumer access, possession, or control would jeopardize the validity and reliability of that educational standardized assessment or educational assessment. If a business does not comply with a request pursuant to this section, it shall notify the consumer that it is acting pursuant to this exception.

(3) For purposes of this subdivision:

(A) “Educational standardized assessment or educational assessment” means a standardized or nonstandardized quiz, test, or other assessment used to evaluate students in or for entry to kindergarten and grades 1 to 12, inclusive, schools, postsecondary institutions, vocational programs, and postgraduate programs that are accredited by an accrediting agency or organization recognized by the State of California or the United States Department of Education, as well as certification and licensure examinations used to determine competency and eligibility to receive certification or licensure from a government agency or government certification body.

(B) “Jeopardize the validity and reliability of that educational standardized assessment or educational assessment” means releasing information that would provide an advantage to the consumer who has submitted a verifiable consumer request or to another natural person.

(r) Sections 1798.105 and 1798.120 shall not apply to a business' use, disclosure, or sale of particular pieces of a consumer's personal information if the consumer has consented to the business' use, disclosure, or sale of that information to produce a physical item, including a school yearbook containing the consumer's photograph if:

- (1) The business has incurred significant expense in reliance on the consumer's consent.
- (2) Compliance with the consumer's request to opt out of the sale of the consumer's personal information or to delete the consumer's personal information would not be commercially reasonable.
- (3) The business complies with the consumer's request as soon as it is commercially reasonable to do so.

(Amended (as amended November 3, 2020, by initiative Proposition 24, Section 15) by Stats. 2021, Ch. 700, Sec. 2.5. (AB 335) Effective January 1, 2022. Subdivisions (m) and (n) inoperative January 1, 2023, by their own provisions.)

1798.146. (a) This title shall not apply to any of the following:

- (1) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the federal Health Information Technology for Economic and Clinical Health Act, Title XIII of the federal American Recovery and Reinvestment Act of 2009 (Public Law 111-5).
- (2) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains, uses, and discloses patient information in the same manner as medical information or protected health information as described in paragraph (1).
- (3) A business associate of a covered entity governed by the privacy, security, and data breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the federal Health

Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the federal Health Information Technology for Economic and Clinical Health Act, Title XIII of the federal American Recovery and Reinvestment Act of 2009 (Public Law 111-5), to the extent that the business associate maintains, uses, and discloses patient information in the same manner as medical information or protected health information as described in paragraph (1).

(4) (A) Information that meets both of the following conditions:

(i) It is deidentified in accordance with the requirements for deidentification set forth in Section 164.514 of Part 164 of Title 45 of the Code of Federal Regulations.

(ii) It is derived from patient information that was originally collected, created, transmitted, or maintained by an entity regulated by the Health Insurance Portability and Accountability Act, the Confidentiality Of Medical Information Act, or the Federal Policy for the Protection of Human Subjects, also known as the Common Rule.

(B) Information that met the requirements of subparagraph (A) but is subsequently reidentified shall no longer be eligible for the exemption in this paragraph, and shall be subject to applicable federal and state data privacy and security laws, including, but not limited to, the Health Insurance Portability and Accountability Act, the Confidentiality Of Medical Information Act, and this title.

(5) Information that is collected, used, or disclosed in research, as defined in Section 164.501 of Title 45 of the Code of Federal Regulations, including, but not limited to, a clinical trial, and that is conducted in accordance with applicable ethics, confidentiality, privacy, and security rules of Part 164 of Title 45 of the Code of Federal Regulations, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, good clinical practice guidelines issued by the International Council for Harmonisation, or human subject protection requirements of the United States Food and Drug Administration.

(b) For purposes of this section, all of the following shall apply:

(1) "Business associate" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(2) "Covered entity" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(3) "Identifiable private information" has the same meaning as defined in Section 46.102 of Title 45 of the Code of Federal Regulations.

(4) "Individually identifiable health information" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(5) "Medical information" has the same meaning as defined in Section 56.05.

(6) "Patient information" shall mean identifiable private information, protected health information, individually identifiable health information, or medical information.

(7) "Protected health information" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(8) "Provider of health care" has the same meaning as defined in Section 56.05.

(Added by Stats. 2020, Ch. 172, Sec. 2. (AB 713) Effective September 25, 2020.)

1798.148. (a) A business or other person shall not reidentify, or attempt to reidentify, information that has met the requirements of paragraph (4) of subdivision (a) of Section 1798.146, except for one or more of the following purposes:

(1) Treatment, payment, or health care operations conducted by a covered entity or business associate acting on behalf of, and at the written direction of, the covered entity. For purposes of this paragraph, "treatment," "payment," "health care operations," "covered entity," and "business associate" have the same meaning as defined in Section 164.501 of Title 45 of the Code of Federal Regulations.

(2) Public health activities or purposes as described in Section 164.512 of Title 45 of the Code of Federal Regulations.

(3) Research, as defined in Section 164.501 of Title 45 of the Code of Federal Regulations, that is conducted in accordance with Part 46 of Title 45 of the Code of Federal Regulations, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule.

(4) Pursuant to a contract where the lawful holder of the deidentified information that met the requirements of paragraph (4) of subdivision (a) of Section 1798.146 expressly engages a person or entity to attempt to reidentify the deidentified information in order to conduct testing, analysis, or validation of deidentification, or related statistical techniques, if the contract bans any other use or disclosure of the reidentified information and requires the return or destruction of the information that was reidentified upon completion of the contract.

(5) If otherwise required by law.

(b) In accordance with paragraph (4) of subdivision (a) of Section 1798.146, information reidentified pursuant this section shall be subject to applicable federal and state data privacy and security laws

including, but not limited to, the Health Insurance Portability and Accountability Act, the Confidentiality of Medical Information Act, and this title.

(c) Beginning January 1, 2021, any contract for the sale or license of deidentified information that has met the requirements of paragraph (4) of subdivision (a) of Section 1798.146, where one of the parties is a person residing or doing business in the state, shall include the following, or substantially similar, provisions:

(1) A statement that the deidentified information being sold or licensed includes deidentified patient information.

(2) A statement that reidentification, and attempted reidentification, of the deidentified information by the purchaser or licensee of the information is prohibited pursuant to this section.

(3) A requirement that, unless otherwise required by law, the purchaser or licensee of the deidentified information may not further disclose the deidentified information to any third party unless the third party is contractually bound by the same or stricter restrictions and conditions.

(d) For purposes of this section, “reidentify” means the process of reversal of deidentification techniques, including, but not limited to, the addition of specific pieces of information or data elements that can, individually or in combination, be used to uniquely identify an individual or usage of any statistical method, contrivance, computer software, or other means that have the effect of associating deidentified information with a specific identifiable individual.

(Added by Stats. 2020, Ch. 172, Sec. 3. (AB 713) Effective September 25, 2020.)

1798.150. (a) (1) Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

(b) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.

(c) The cause of action established by this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.

(Amended by Stats. 2019, Ch. 757, Sec. 9. (AB 1355) Effective January 1, 2020. Superseded on January 1, 2023; see amendment by Proposition 24.)

1798.150. Personal Information Security Breaches

(a) (1) Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, or whose email address in combination with a password or security question and answer that would permit access to the account is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices

appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

(b) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. The implementation and maintenance of reasonable security procedures and practices pursuant to Section 1798.81.5 following a breach does not constitute a cure with respect to that breach. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.

(c) The cause of action established by this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 16. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.155. (a) Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title.

(b) A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars (\$2,500) for each violation or seven thousand five hundred dollars (\$7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.

(c) Any civil penalty assessed for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision (b), shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160 with the intent to fully offset any costs incurred by the state courts and the Attorney General in connection with this title.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 12. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198. Superseded on January 1, 2023; see amendment by Proposition 24.)

1798.155. Administrative Enforcement

(a) Any business, service provider, contractor, or other person that violates this title shall be liable for an administrative fine of not more than two thousand five hundred dollars (\$2,500) for each violation or seven thousand five hundred dollars (\$7,500) for each intentional violation or violations involving the personal information of consumers whom the business, service provider, contractor, or other person has actual knowledge are under 16 years of age, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185, in an administrative enforcement action brought by the California Privacy Protection Agency.

(b) Any administrative fine assessed for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision (a), shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160 with the intent to

fully offset any costs incurred by the state courts, the Attorney General, and the California Privacy Protection Agency in connection with this title.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 17. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.160. Consumer Privacy Fund

(a) A special fund to be known as the “Consumer Privacy Fund” is hereby created within the General Fund in the State Treasury, and is available upon appropriation by the Legislature first to offset any costs incurred by the state courts in connection with actions brought to enforce this title, the costs incurred by the Attorney General in carrying out the Attorney General’s duties under this title, and then for the purposes of establishing an investment fund in the State Treasury, with any earnings or interest from the fund to be deposited in the General Fund, and making grants to promote and protect consumer privacy, educate children in the area of online privacy, and fund cooperative programs with international law enforcement organizations to combat fraudulent activities with respect to consumer data breaches.

(b) Funds transferred to the Consumer Privacy Fund shall be used exclusively as follows:

(1) To offset any costs incurred by the state courts and the Attorney General in connection with this title.

(2) After satisfying the obligations under paragraph (1), the remaining funds shall be allocated each fiscal year as follows:

(A) Ninety-one percent shall be invested by the Treasurer in financial assets with the goal of maximizing long term yields consistent with a prudent level of risk. The principal shall not be subject to transfer or appropriation, provided that any interest and earnings shall be transferred on an annual basis to the General Fund for appropriation by the Legislature for General Fund purposes.

(B) Nine percent shall be made available to the California Privacy Protection Agency for the purposes of making grants in California, with 3 percent allocated to each of the following grant recipients:

(i) Nonprofit organizations to promote and protect consumer privacy.

(ii) Nonprofit organizations and public agencies, including school districts, to educate children in the area of online privacy.

(iii) State and local law enforcement agencies to fund cooperative programs with international law enforcement organizations to combat fraudulent activities with respect to consumer data breaches.

(c) Funds in the Consumer Privacy Fund shall not be subject to appropriation or transfer by the Legislature for any other purpose.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 18. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.175. This title is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information, including, but not limited to, Chapter 22 (commencing with Section 22575) of Division 8 of the Business and Professions Code and Title 1.81 (commencing with Section 1798.80). The provisions of this title are not limited to information collected electronically or over the Internet, but apply to the collection and sale of all personal information collected by a business from consumers. Wherever possible, law relating to consumers' personal information should be construed to harmonize with the provisions of this title, but in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198. Superseded on January 1, 2023; see amendment by Proposition 24.)

1798.175. Conflicting Provisions

This title is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information, including, but not limited to, Chapter 22 (commencing with Section 22575) of Division 8 of the Business and Professions Code and Title 1.81 (commencing with Section 1798.80). The provisions of this title are not limited to information collected electronically or over the Internet, but apply to the collection and sale of all personal information collected by a business from consumers. Wherever possible, law relating to consumers' personal information should be construed to harmonize with the provisions of this title, but in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 19. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.180. This title is a matter of statewide concern and supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county,

municipality, or local agency regarding the collection and sale of consumers' personal information by a business.

(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative September 23, 2018, pursuant to Section 1798.199. Superseded on January 1, 2023; see amendment by Proposition 24.)

1798.180. Preemption

This title is a matter of statewide concern and supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection and sale of consumers' personal information by a business.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 20. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.185. Regulations

(a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

(1) Updating or adding categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision (v) of Section 1798.140, and updating or adding categories of sensitive personal information to those enumerated in subdivision (ae) of Section 1798.140 in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(2) Updating as needed the definitions of "deidentified" and "unique identifier" to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and adding, modifying, or deleting categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business pursuant to Section 1798.130. The authority to update the definition of "deidentified" shall not apply to deidentification standards set forth in Section 164.514 of Title 45 of the Code of Federal Regulations, where such information previously was "protected health information" as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage

of this title and as needed thereafter, with the intention that trade secrets should not be disclosed in response to a verifiable consumer request.

(4) Establishing rules and procedures for the following:

(A) To facilitate and govern the submission of a request by a consumer to opt-out of the sale or sharing of personal information pursuant to Section 1798.120 and to limit the use of a consumer's sensitive personal information pursuant to Section 1798.121 to ensure that consumers have the ability to exercise their choices without undue burden and to prevent business from engaging in deceptive or harassing conduct, including in retaliation against consumers for exercising their rights, while allowing businesses to inform consumers of the consequences of their decision to opt out of the sale or sharing of their personal information or to limit the use of their sensitive personal information.

(B) To govern business compliance with a consumer's opt-out request.

(C) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

(5) Adjusting the monetary thresholds, in January of every odd-numbered year to reflect any increase in the Consumer Price Index, in: subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.140; subparagraph (A) of paragraph (1) of subdivision (a) of Section 1798.150; subdivision (a) of Section 1798.155; Section 1798.199.25; and subdivision (a) of Section 1798.199.90.

(6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentives within one year of passage of this title and as needed thereafter.

(7) Establishing rules and procedures to further the purposes of Sections 1798.105, 1798.106, 1798.110, and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to delete personal information, correct inaccurate personal information pursuant to Section 1798.106, or obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business's determination that a request for information received from a consumer is a verifiable consumer request, including treating a request submitted through a

password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

(8) Establishing how often, and under what circumstances, a consumer may request a correction pursuant to Section 1798.106, including standards governing the following:

(A) How a business responds to a request for correction, including exceptions for requests to which a response is impossible or would involve disproportionate effort, and requests for correction of accurate information.

(B) How concerns regarding the accuracy of the information may be resolved.

(C) The steps a business may take to prevent fraud.

(D) If a business rejects a request to correct personal information collected and analyzed concerning a consumer's health, the right of a consumer to provide a written addendum to the business with respect to any item or statement regarding any such personal information that the consumer believes to be incomplete or incorrect. The addendum shall be limited to 250 words per alleged incomplete or incorrect item and shall clearly indicate in writing that the consumer requests the addendum to be made a part of the consumer's record.

(9) Establishing the standard to govern a business' determination, pursuant to subparagraph (B) of paragraph (2) of subdivision (a) of Section 1798.130, that providing information beyond the 12-month period in a response to a verifiable consumer request is impossible or would involve a disproportionate effort.

(10) Issuing regulations further defining and adding to the business purposes, including other notified purposes, for which businesses, service providers, and contractors may use consumers' personal information consistent with consumers' expectations, and further defining the business purposes for which service providers and contractors may combine consumers' personal information obtained from different sources, except as provided for in paragraph (6) of subdivision (e) of Section 1798.140.

(11) Issuing regulations identifying those business purposes, including other notified purposes, for which service providers and contractors may use consumers' personal information received pursuant to a written contract with a business, for the service provider or contractor's own business purposes, with the goal of maximizing consumer privacy.

(12) Issuing regulations to further define “intentionally interacts,” with the goal of maximizing consumer privacy.

(13) Issuing regulations to further define “precise geolocation,” including if the size defined is not sufficient to protect consumer privacy in sparsely populated areas or when the personal information is used for normal operational purposes, including billing.

(14) Issuing regulations to define the term “specific pieces of information obtained from the consumer” with the goal of maximizing a consumer’s right to access relevant personal information while minimizing the delivery of information to a consumer that would not be useful to the consumer, including system log information and other technical data. For delivery of the most sensitive personal information, the regulations may require a higher standard of authentication provided that the agency shall monitor the impact of the higher standard on the right of consumers to obtain their personal information to ensure that the requirements of verification do not result in the unreasonable denial of verifiable consumer requests.

(15) Issuing regulations requiring businesses whose processing of consumers’ personal information presents significant risk to consumers’ privacy or security, to:

(A) Perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent. The factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities.

(B) Submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public. Nothing in this section shall require a business to divulge trade secrets.

(16) Issuing regulations governing access and opt-out rights with respect to businesses’ use of automated decisionmaking technology, including profiling and requiring businesses’ response to

access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer.

(17) Issuing regulations to further define a “law enforcement agency-approved investigation” for purposes of the exception in paragraph (2) of subdivision (a) of Section 1798.145.

(18) Issuing regulations to define the scope and process for the exercise of the agency’s audit authority, to establish criteria for selection of persons to audit, and to protect consumers’ personal information from disclosure to an auditor in the absence of a court order, warrant, or subpoena.

(19) (A) Issuing regulations to define the requirements and technical specifications for an opt-out preference signal sent by a platform, technology, or mechanism, to indicate a consumer’s intent to opt out of the sale or sharing of the consumer’s personal information and to limit the use or disclosure of the consumer’s sensitive personal information. The requirements and specifications for the opt-out preference signal should be updated from time to time to reflect the means by which consumers interact with businesses, and should:

(i) Ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business.

(ii) Ensure that the opt-out preference signal is consumer-friendly, clearly described, and easy to use by an average consumer and does not require that the consumer provide additional information beyond what is necessary.

(iii) Clearly represent a consumer’s intent and be free of defaults constraining or presupposing that intent.

(iv) Ensure that the opt-out preference signal does not conflict with other commonly used privacy settings or tools that consumers may employ.

(v) Provide a mechanism for the consumer to selectively consent to a business’ sale of the consumer’s personal information, or the use or disclosure of the consumer’s sensitive personal information, without affecting the consumer’s preferences with respect to other businesses or disabling the opt-out preference signal globally.

(vi) State that in the case of a page or setting view that the consumer accesses to set the opt-out preference signal, the consumer should see up to three choices, including:

(I) Global opt out from sale and sharing of personal information, including a direction to limit the use of sensitive personal information.

(II) Choice to “Limit the Use of My Sensitive Personal Information.”

(III) Choice titled “Do Not Sell/Do Not Share My Personal Information for Cross-Context Behavioral Advertising.”

(B) Issuing regulations to establish technical specifications for an opt-out preference signal that allows the consumer, or the consumer’s parent or guardian, to specify that the consumer is less than 13 years of age or at least 13 years of age and less than 16 years of age.

(C) Issuing regulations, with the goal of strengthening consumer privacy while considering the legitimate operational interests of businesses, to govern the use or disclosure of a consumer’s sensitive personal information, notwithstanding the consumer’s direction to limit the use or disclosure of the consumer’s sensitive personal information, including:

(i) Determining any additional purposes for which a business may use or disclose a consumer’s sensitive personal information.

(ii) Determining the scope of activities permitted under paragraph (8) of subdivision (e) of Section 1798.140, as authorized by subdivision (a) of Section 1798.121, to ensure that the activities do not involve health-related research.

(iii) Ensuring the functionality of the business’ operations.

(iv) Ensuring that the exemption in subdivision (d) of Section 1798.121 for sensitive personal information applies to information that is collected or processed incidentally, or without the purpose of inferring characteristics about a consumer, while ensuring that businesses do not use the exemption for the purpose of evading consumers’ rights to limit the use and disclosure of their sensitive personal information under Section 1798.121.

(20) Issuing regulations to govern how a business that has elected to comply with subdivision (b) of Section 1798.135 responds to the opt-out preference signal and provides consumers with the opportunity subsequently to consent to the sale or sharing of their personal information or the use and disclosure of their sensitive personal information for purposes in addition to those authorized by subdivision (a) of Section 1798.121. The regulations should:

(A) Strive to promote competition and consumer choice and be technology neutral.

(B) Ensure that the business does not respond to an opt-out preference signal by:

(i) Intentionally degrading the functionality of the consumer experience.

(ii) Charging the consumer a fee in response to the consumer’s opt-out preferences.

(iii) Making any products or services not function properly or fully for the consumer, as compared to consumers who do not use the opt-out preference signal.

(iv) Attempting to coerce the consumer to opt in to the sale or sharing of the consumer's personal information, or the use or disclosure of the consumer's sensitive personal information, by stating or implying that the use of the opt-out preference signal will adversely affect the consumer as compared to consumers who do not use the opt-out preference signal, including stating or implying that the consumer will not be able to use the business' products or services or that those products or services may not function properly or fully.

(v) Displaying any notification or pop-up in response to the consumer's opt-out preference signal.

(C) Ensure that any link to a web page or its supporting content that allows the consumer to consent to opt in:

(i) Is not part of a popup, notice, banner, or other intrusive design that obscures any part of the web page the consumer intended to visit from full view or that interferes with or impedes in any way the consumer's experience visiting or browsing the web page or website the consumer intended to visit.

(ii) Does not require or imply that the consumer must click the link to receive full functionality of any products or services, including the website.

(iii) Does not make use of any dark patterns.

(iv) Applies only to the business with which the consumer intends to interact.

(D) Strive to curb coercive or deceptive practices in response to an opt-out preference signal but should not unduly restrict businesses that are trying in good faith to comply with Section 1798.135.

(21) Review existing Insurance Code provisions and regulations relating to consumer privacy, except those relating to insurance rates or pricing, to determine whether any provisions of the Insurance Code provide greater protection to consumers than the provisions of this title. Upon completing its review, the agency shall adopt a regulation that applies only the more protective provisions of this title to insurance companies. For the purpose of clarity, the Insurance Commissioner shall have jurisdiction over insurance rates and pricing.

(22) Harmonizing the regulations governing opt-out mechanisms, notices to consumers, and other operational mechanisms in this title to promote clarity and the functionality of this title for consumers.

(b) The Attorney General may adopt additional regulations as necessary to further the purposes of this title.

(c) The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.

(d) Notwithstanding subdivision (a), the timeline for adopting final regulations required by the act adding this subdivision shall be July 1, 2022. Beginning the later of July 1, 2021, or six months after the agency provides notice to the Attorney General that it is prepared to begin rulemaking under this title, the authority assigned to the Attorney General to adopt regulations under this section shall be exercised by the California Privacy Protection Agency. Notwithstanding any other law, civil and administrative enforcement of the provisions of law added or amended by this act shall not commence until July 1, 2023, and shall only apply to violations occurring on or after that date. Enforcement of provisions of law contained in the California Consumer Privacy Act of 2018 amended by this act shall remain in effect and shall be enforceable until the same provisions of this act become enforceable.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 21. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.190. If a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title.

(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198. Superseded on January 1, 2023; see amendment by Proposition 24.)

1798.190. Anti-Avoidance

A court or the agency shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title:

(a) If a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell or share.

(b) If steps or transactions were taken to purposely avoid the definition of sell or share by eliminating any monetary or other valuable consideration, including by entering into contracts that do not include

an exchange for monetary or other valuable consideration, but where a party is obtaining something of value or use.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 22. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.192. Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt-out of a business's sale of the consumer's personal information, or authorizing a business to sell the consumer's personal information after previously opting out.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 14. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198. Superseded on January 1, 2023; see amendment by Proposition 24.)

1798.192. Waiver

Any provision of a contract or agreement of any kind, including a representative action waiver, that purports to waive or limit in any way rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt out of a business's sale of the consumer's personal information, or authorizing a business to sell or share the consumer's personal information after previously opting out.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 23. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.194. This title shall be liberally construed to effectuate its purposes.

(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.196. This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 15. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.198. (a) Subject to limitation provided in subdivision (b), and in Section 1798.199, this title shall be operative January 1, 2020.

(b) This title shall become operative only if initiative measure No. 17-0039, The Consumer Right to Privacy Act of 2018, is withdrawn from the ballot pursuant to Section 9604 of the Elections Code.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 16. (SB 1121) Effective September 23, 2018.)

1798.199. Notwithstanding Section 1798.198, Section 1798.180 shall be operative on the effective date of the act adding this section.

(Added by Stats. 2018, Ch. 735, Sec. 17. (SB 1121) Effective September 23, 2018. Operative September 23, 2018.)

1798.199.10. (a) There is hereby established in state government the California Privacy Protection Agency, which is vested with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018. The agency shall be governed by a five-member board, including the chairperson. The chairperson and one member of the board shall be appointed by the Governor. The Attorney General, Senate Rules Committee, and Speaker of the Assembly shall each appoint one member. These appointments should be made from among Californians with expertise in the areas of privacy, technology, and consumer rights.

(b) The initial appointments to the agency shall be made within 90 days of the effective date of the act adding this section.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.1. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.15. Members of the agency board shall:

(a) Have qualifications, experience, and skills, in particular in the areas of privacy and technology, required to perform the duties of the agency and exercise its powers.

(b) Maintain the confidentiality of information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers, except to the extent that disclosure is required by the Public Records Act.

(c) Remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from another.

(d) Refrain from any action incompatible with their duties and engaging in any incompatible occupation, whether gainful or not, during their term.

(e) Have the right of access to all information made available by the agency to the chairperson.

(f) Be precluded, for a period of one year after leaving office, from accepting employment with a business that was subject to an enforcement action or civil action under this title during the member's tenure or during the five-year period preceding the member's appointment.

(g) Be precluded for a period of two years after leaving office from acting, for compensation, as an agent or attorney for, or otherwise representing, any other person in a matter pending before the agency if the purpose is to influence an action of the agency.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.2. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.20. Members of the agency board, including the chairperson, shall serve at the pleasure of their appointing authority but shall serve for no longer than eight consecutive years.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.3. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.25. For each day on which they engage in official duties, members of the agency board shall be compensated at the rate of one hundred dollars (\$100), adjusted biennially to reflect changes in the cost of living, and shall be reimbursed for expenses incurred in performance of their official duties.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.4. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.30. The agency board shall appoint an executive director who shall act in accordance with agency policies and regulations and with applicable law. The agency shall appoint and discharge officers, counsel, and employees, consistent with applicable civil service laws, and shall fix the compensation of employees and prescribe their duties. The agency may contract for services that cannot be provided by its employees.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.5. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.35. The agency board may delegate authority to the chairperson or the executive director to act in the name of the agency between meetings of the agency, except with respect to resolution of enforcement actions and rulemaking authority.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.6. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.40. The agency shall perform the following functions:

(a) Administer, implement, and enforce through administrative actions this title.

(b) On and after the later of July 1, 2021, or within six months of the agency providing the Attorney General with notice that it is prepared to assume rulemaking responsibilities under this title, adopt, amend, and rescind regulations pursuant to Section 1798.185 to carry out the purposes and provisions of the California Consumer Privacy Act of 2018, including regulations specifying recordkeeping requirements for businesses to ensure compliance with this title.

(c) Through the implementation of this title, protect the fundamental privacy rights of natural persons with respect to the use of their personal information.

(d) Promote public awareness and understanding of the risks, rules, responsibilities, safeguards, and rights in relation to the collection, use, sale, and disclosure of personal information, including the rights of minors with respect to their own information, and provide a public report summarizing the risk assessments filed with the agency pursuant to paragraph (15) of subdivision (a) of Section 1798.185 while ensuring that data security is not compromised.

(e) Provide guidance to consumers regarding their rights under this title.

(f) Provide guidance to businesses regarding their duties and responsibilities under this title and appoint a Chief Privacy Auditor to conduct audits of businesses to ensure compliance with this title pursuant to regulations adopted pursuant to paragraph (18) of subdivision (a) of Section 1798.185.

(g) Provide technical assistance and advice to the Legislature, upon request, with respect to privacy-related legislation.

(h) Monitor relevant developments relating to the protection of personal information and, in particular, the development of information and communication technologies and commercial practices.

(i) Cooperate with other agencies with jurisdiction over privacy laws and with data processing authorities in California, other states, territories, and countries to ensure consistent application of privacy protections.

(j) Establish a mechanism pursuant to which persons doing business in California that do not meet the definition of business set forth in paragraph (1), (2), or (3) of subdivision (d) of Section 1798.140 may voluntarily certify that they are in compliance with this title, as set forth in paragraph (4) of subdivision (d) of Section 1798.140, and make a list of those entities available to the public.

(k) Solicit, review, and approve applications for grants to the extent funds are available pursuant to paragraph (2) of subdivision (b) of Section 1798.160.

(l) Perform all other acts necessary or appropriate in the exercise of its power, authority, and jurisdiction and seek to balance the goals of strengthening consumer privacy while giving attention to the impact on businesses.

(Amended by Stats. 2021, Ch. 525, Sec. 5. (AB 694) Effective January 1, 2022.)

1798.199.45. (a) Upon the sworn complaint of any person or on its own initiative, the agency may investigate possible violations of this title relating to any business, service provider, contractor, or person. The agency may decide not to investigate a complaint or decide to provide a business with a time period to cure the alleged violation. In making a decision not to investigate or provide more time to cure, the agency may consider the following:

(1) Lack of intent to violate this title.

(2) Voluntary efforts undertaken by the business, service provider, contractor, or person to cure the alleged violation prior to being notified by the agency of the complaint.

(b) The agency shall notify in writing the person who made the complaint of the action, if any, the agency has taken or plans to take on the complaint, together with the reasons for that action or nonaction.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.8. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.50. No finding of probable cause to believe this title has been violated shall be made by the agency unless, at least 30 days prior to the agency's consideration of the alleged violation, the business, service provider, contractor, or person alleged to have violated this title is notified of the violation by service of process or registered mail with return receipt requested, provided with a

summary of the evidence, and informed of their right to be present in person and represented by counsel at any proceeding of the agency held for the purpose of considering whether probable cause exists for believing the person violated this title. Notice to the alleged violator shall be deemed made on the date of service, the date the registered mail receipt is signed, or if the registered mail receipt is not signed, the date returned by the post office. A proceeding held for the purpose of considering probable cause shall be private unless the alleged violator files with the agency a written request that the proceeding be public.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.9. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.55. (a) When the agency determines there is probable cause for believing this title has been violated, it shall hold a hearing to determine if a violation has or violations have occurred. Notice shall be given and the hearing conducted in accordance with the Administrative Procedure Act (Chapter 5 (commencing with Section 11500), Part 1, Division 3, Title 2, Government Code). The agency shall have all the powers granted by that chapter. If the agency determines on the basis of the hearing conducted pursuant to this subdivision that a violation or violations have occurred, it shall issue an order that may require the violator to do all or any of the following:

(1) Cease and desist violation of this title.

(2) Subject to Section 1798.155, pay an administrative fine of up to two thousand five hundred dollars (\$2,500) for each violation, or up to seven thousand five hundred dollars (\$7,500) for each intentional violation and each violation involving the personal information of minor consumers to the Consumer Privacy Fund within the General Fund of the state. When the agency determines that no violation has occurred, it shall publish a declaration so stating.

(b) If two or more persons are responsible for any violation or violations, they shall be jointly and severally liable.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.10. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.60. Whenever the agency rejects the decision of an administrative law judge made pursuant to Section 11517 of the Government Code, the agency shall state the reasons in writing for rejecting the decision.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.11. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.65. The agency may subpoena witnesses, compel their attendance and testimony, administer oaths and affirmations, take evidence and require by subpoena the production of any books, papers, records, or other items material to the performance of the agency's duties or exercise of its powers, including, but not limited to, its power to audit a business' compliance with this title.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.12. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.70. No administrative action brought pursuant to this title alleging a violation of any of the provisions of this title shall be commenced more than five years after the date on which the violation occurred.

(a) The service of the probable cause hearing notice, as required by Section 1798.199.50, upon the person alleged to have violated this title shall constitute the commencement of the administrative action.

(b) If the person alleged to have violated this title engages in the fraudulent concealment of the person's acts or identity, the five-year period shall be tolled for the period of the concealment. For purposes of this subdivision, "fraudulent concealment" means the person knows of material facts related to the person's duties under this title and knowingly conceals them in performing or omitting to perform those duties for the purpose of defrauding the public of information to which it is entitled under this title.

(c) If, upon being ordered by a superior court to produce any documents sought by a subpoena in any administrative proceeding under this title, the person alleged to have violated this title fails to produce documents in response to the order by the date ordered to comply therewith, the five-year period shall be tolled for the period of the delay from the date of filing of the motion to compel until the date the documents are produced.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.13. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.75. (a) In addition to any other available remedies, the agency may bring a civil action and obtain a judgment in superior court for the purpose of collecting any unpaid administrative fines imposed pursuant to this title after exhaustion of judicial review of the agency's action. The action may be filed as a small claims, limited civil, or unlimited civil case depending on the jurisdictional amount. The venue for this action shall be in the county where the administrative fines were imposed by the agency. In order to obtain a judgment in a proceeding under this section, the agency shall show,

following the procedures and rules of evidence as applied in ordinary civil actions, all of the following:

(1) That the administrative fines were imposed following the procedures set forth in this title and implementing regulations.

(2) That the defendant or defendants in the action were notified, by actual or constructive notice, of the imposition of the administrative fines.

(3) That a demand for payment has been made by the agency and full payment has not been received.

(b) A civil action brought pursuant to subdivision (a) shall be commenced within four years after the date on which the administrative fines were imposed.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.14. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.80. (a) If the time for judicial review of a final agency order or decision has lapsed, or if all means of judicial review of the order or decision have been exhausted, the agency may apply to the clerk of the court for a judgment to collect the administrative fines imposed by the order or decision, or the order as modified in accordance with a decision on judicial review.

(b) The application, which shall include a certified copy of the order or decision, or the order as modified in accordance with a decision on judicial review, and proof of service of the order or decision, constitutes a sufficient showing to warrant issuance of the judgment to collect the administrative fines. The clerk of the court shall enter the judgment immediately in conformity with the application.

(c) An application made pursuant to this section shall be made to the clerk of the superior court in the county where the administrative fines were imposed by the agency.

(d) A judgment entered in accordance with this section has the same force and effect as, and is subject to all the provisions of law relating to, a judgment in a civil action and may be enforced in the same manner as any other judgment of the court in which it is entered.

(e) The agency may bring an application pursuant to this section only within four years after the date on which all means of judicial review of the order or decision have been exhausted.

(f) The remedy available under this section is in addition to those available under any other law.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.15. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.85. Any decision of the agency with respect to a complaint or administrative fine shall be subject to judicial review in an action brought by an interested party to the complaint or administrative fine and shall be subject to an abuse of discretion standard.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.16. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.90. (a) Any business, service provider, contractor, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars (\$2,500) for each violation or seven thousand five hundred dollars (\$7,500) for each intentional violation and each violation involving the personal information of minor consumers, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The court may consider the good faith cooperation of the business, service provider, contractor, or other person in determining the amount of the civil penalty.

(b) Any civil penalty recovered by an action brought by the Attorney General for a violation of this title, and the proceeds of any settlement of any said action, shall be deposited in the Consumer Privacy Fund.

(c) The agency shall, upon request by the Attorney General, stay an administrative action or investigation under this title to permit the Attorney General to proceed with an investigation or civil action and shall not pursue an administrative action or investigation, unless the Attorney General subsequently determines not to pursue an investigation or civil action. The agency may not limit the authority of the Attorney General to enforce this title.

(d) No civil action may be filed by the Attorney General under this section for any violation of this title after the agency has issued a decision pursuant to Section 1798.199.85 or an order pursuant to Section 1798.199.55 against that person for the same violation.

(e) This section shall not affect the private right of action provided for in Section 1798.150.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.17. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.95. (a) There is hereby appropriated from the General Fund of the state to the agency the sum of five million dollars (\$5,000,000) during the fiscal year 2020-2021, and the sum of ten million dollars (\$10,000,000) adjusted for cost-of-living changes, during each fiscal year thereafter, for expenditure to support the operations of the agency pursuant to this title. The expenditure of funds

under this appropriation shall be subject to the normal administrative review given to other state appropriations. The Legislature shall appropriate those additional amounts to the commission and other agencies as may be necessary to carry out the provisions of this title.

(b) The Department of Finance, in preparing the state budget and the Budget Act bill submitted to the Legislature, shall include an item for the support of this title that shall indicate all of the following:

(1) The amounts to be appropriated to other agencies to carry out their duties under this title, which amounts shall be in augmentation of the support items of those agencies.

(2) The additional amounts required to be appropriated by the Legislature to the agency to carry out the purposes of this title, as provided for in this section.

(3) In parentheses, for informational purposes, the continuing appropriation during each fiscal year of ten million dollars (\$10,000,000), adjusted for cost-of-living changes made pursuant to this section.

(c) The Attorney General shall provide staff support to the agency until the agency has hired its own staff. The Attorney General shall be reimbursed by the agency for these services.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.18. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.199.100. The agency and any court, as applicable, shall consider the good faith cooperation of the business, service provider, contractor, or other person in determining the amount of any administrative fine or civil penalty for a violation of this title. A business shall not be required by the agency, a court, or otherwise to pay both an administrative fine and a civil penalty for the same violation.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.19. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

ABD - Virginia Consumer Data Protection Act (CDPA)

Virginia Consumer Data Protection Act (CDPA)

VIRGINIA ACTS OF ASSEMBLY - CHAPTER

An Act to amend the Code of Virginia by adding in Title 59.1 a chapter numbered 52, consisting of sections numbered 59.1-571 through 59.1-581, relating to Consumer Data Protection Act,

Approved

Be it enacted by the General Assembly of Virginia:

1. That the Code of Virginia is amended by adding in Title 59.1 a chapter numbered 52, consisting of sections numbered 59.1-571 through 59.1-581, as follows:

CHAPTER 52.

CONSUMER DATA PROTECTION ACT.

59.1-571. Definitions.

As used in this chapter, unless the context requires a different meaning:

“Affiliate” means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity. For the purposes of this definition, “control” or “controlled” means (i) ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company; (ii) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or (iii) the power to exercise controlling influence over the management of a company.

“Authenticate” means verifying through reasonable means that the consumer, entitled to exercise his consumer rights in § 59.1-573, is the same consumer exercising such consumer rights with respect to the personal data at issue.

“Biometric data” means data generated by automatic measurements of an individual’s biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. “Biometric data” does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.

“Business associate” means the same meaning as the term established by HIPAA.

“Child” means any natural person younger than 13 years of age.

“Consent” means a clear affirmative act signifying a consumer’s freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.

“Consumer” means a natural person who is a resident of the Commonwealth acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context.

“Controller” means the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data.

“Covered entity” means the same as the term is established by HIPAA.

“Decisions that produce legal or similarly significant effects concerning a consumer” means a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.

“De-identified data” means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person. A controller that possesses “de-identified data” shall comply with the requirements of subsection A of § 59.1-577.

“Fund” means the Consumer Privacy Fund established pursuant to § 59.1-581.

“Health record” means the same as that term is defined in § 32.1-127.1:03.

“Health care provider” means the same as that term is defined in § 32.1-276.3.

“HIPAA” means the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d et seq.).

“Identified or identifiable natural person” means a person who can be readily identified, directly or indirectly.

“Institution of higher education” means a public institution and private institution of higher education, as those terms are defined in § 23.1-100.

“Nonprofit organization” means any corporation organized under the Virginia Nonstock Corporation Act (§ 13.1-801 et seq.) or any organization exempt from taxation under § 501(c)(3),

501(c)(6), or 501 (c)(12) of the Internal Revenue Code, and any subsidiaries and affiliates of entities organized pursuant to Chapter 9.1 (§ 56-231.15 et seq.) of Title 56.

“Personal data” means any information that is linked or reasonably linkable to an identified or identifiable natural person. “Personal data” does not include de-identified data or publicly available information.

“Precise geolocation data” means information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of a natural person with precision and accuracy within a radius of 1,750 feet. “Precise geolocation data” does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

“Process” or “processing” means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

“Processor” means a natural or legal entity that processes personal data on behalf of a controller.

“Profiling” means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person’s economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

“Protected health information” means the same as the term is established by HIPAA.

“Pseudonymous data” means personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

“Publicly available information” means information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.

“Sale of personal data” means the exchange of personal data for monetary consideration by the controller to a third party. “Sale of personal data” does not include:

1. The disclosure of personal data to a processor that processes the personal data on behalf of the controller;
2. The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;
3. The disclosure or transfer of personal data to an affiliate of the controller;
4. The disclosure of information that the consumer (i) intentionally made available to the general public via a channel of mass media and (ii) did not restrict to a specific audience; or
5. The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

"Sensitive data" means a category of personal data that includes:

1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;
2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;
3. The personal data collected from a known child; or
4. Precise geolocation data.

"State agency" means the same as that term is defined in § 2.2-307.

"Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests.

"Targeted advertising" does not include:

1. Advertisements based on activities within a controller's own websites or online applications;
2. Advertisements based on the context of a consumer's current search query, visit to a website, or online application;
3. Advertisements directed to a consumer in response to the consumer's request for information or feedback; or
4. Processing personal data processed solely for measuring or reporting advertising performance, reach, or frequency.

“Third party” means a natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller.

59.1-572. Scope; exemptions.

A. This chapter applies to persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that (i) during a calendar year, control or process personal data of at least 100,000 consumers or (ii) control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data.

B. This chapter shall not apply to any (i) body, authority, board, bureau, commission, district, or agency of the Commonwealth or of any political subdivision of the Commonwealth; (ii) financial institution or data subject to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.); (iii) covered entity or business associate governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164 established pursuant to HIPAA, and the Health Information Technology for Economic and Clinical Health Act (P.L. 111-5); (iv) nonprofit organization; or (v) institution of higher education.

C. The following information and data is exempt from this chapter:

1. Protected health information under HIPAA;
2. Health records for purposes of Title 32.1;
3. Patient identifying information for purposes of 42 U.S.C. § 290dd-2;
4. Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. Part 46; identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by The International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use; the protection of human subjects under 21 C.F.R. Parts 6, 50, and 56, or personal data used or shared in research conducted in accordance with the requirements set forth in this chapter, or other research conducted in accordance with applicable law;
5. Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986 (42 U.S.C. § 11101 et seq.);
6. Patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act (42 U.S.C. § 299b-21 et seq.);

7. Information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA;

8. Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as information exempt under this subsection that is maintained by a covered entity or business associate as defined by HIPAA or a program or a qualified service organization as defined by 42 U.S.C. § 290dd-2;

9. Information used only for public health activities and purposes as authorized by HIPAA;

10. The collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);

11. Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721 et seq.);

12. Personal data regulated by the federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g et seq.);

13. Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (12 U.S.C. § 2001 et seq.); and

14. Data processed or maintained (i) in the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role; (ii) as the emergency contact information of an individual under this chapter used for emergency contact purposes; or (iii) that is necessary to retain to administer benefits for another individual relating to the individual under clause (i) and used for the purposes of administering those benefits.

D. Controllers and processors that comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) shall be deemed compliant with any obligation to obtain parental consent under this chapter.

59.1-573. Personal data rights; consumers.

A. consumer may invoke the consumer rights authorized pursuant to this subsection at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to invoke. A known child's parent or legal guardian may invoke such consumer rights on behalf of the child regarding processing personal data belonging to the known child. A controller shall comply with an authenticated consumer request to exercise the right:

1. To confirm whether or not a controller is processing the consumer's personal data and to access such personal data;
2. To correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;
3. To delete personal data provided by or obtained about the consumer;
4. To obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means; and
5. To opt out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

B. Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to subsection A as follows:

1. A controller shall respond to the consumer without undue delay, but in all cases within 45 days of receipt of the request submitted pursuant to the methods described in § 59.1-573 A. The response period may be extended once by 45 additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of any such extension within the initial 45-day response period, together with the reason for the extension.
2. If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but in all cases and at the latest within 45 days of receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision pursuant to subsection C.

3. Information provided in response to a consumer request shall be provided by a controller free of charge, up to twice annually per consumer. If requests from a consumer are manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request.

4. If a controller is unable to authenticate the request using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action under subsection A and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

C. A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision pursuant to subdivision B 2. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to subsection A. Within 60 days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

59.1-574. Data controller responsibilities; transparency.

A. A controller shall:

1. Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer;
2. Except as otherwise provided in this chapter, not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;
3. Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue;
4. Not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services,

charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, nothing in this subdivision shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised his right to opt out pursuant to § 59.1-573 or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program; and

5. Not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.).

B. Any provision of a contract or agreement of any kind that purports to waive or limit in any way consumer rights pursuant to § 59.1-573 shall be deemed contrary to public policy and shall be void and unenforceable.

C. Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

1. The categories of personal data processed by the controller;
2. The purpose for processing personal data;
3. How consumers may exercise their consumer rights pursuant § 59.1-573, including how a consumer may appeal a controller's decision with regard to the consumer's request;
4. The categories of personal data that the controller shares with third parties, if any; and
5. The categories of third parties, if any, with whom the controller shares personal data.

D. If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing.

E. A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights under this chapter. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to authenticate the identity of the consumer making the request. Controllers shall not require a consumer

to create a new account in order to exercise consumer rights pursuant to § 59.1-573 but may require a consumer to use an existing account.

59.1-575. Responsibility according to role; controller and processor.

A. A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this chapter. Such assistance shall include:

1. Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests pursuant to § 59.1-573.
2. Taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security of the system of the processor pursuant to § 18.2-186.6 in order to meet the controller's obligations.
3. Providing necessary information to enable the controller to conduct and document data protection assessments pursuant to § 59.1-576.

B. A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract shall also include requirements that the processor shall:

1. Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;
2. At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;
3. Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter;
4. Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and

assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request; and

5. Engage any subcontractor pursuant to a written contract in accordance with subsection C that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

C. Nothing in this section shall be construed to relieve a controller or a processor from the liabilities imposed on it by virtue of its role in the processing relationship as defined by this chapter.

D. Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is

to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

59.1-576. Data protection assessments.

A. A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

1. The processing of personal data for purposes of targeted advertising;
2. The sale of personal data;
3. The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers;
4. The processing of sensitive data; and
5. Any processing activities involving personal data that present a heightened risk of harm to consumers.

B. Data protection assessments conducted pursuant to subsection A shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of de-identified data and the reasonable expectations of consumers, as well as the

context of the processing and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into this assessment by the controller.

C. The Attorney General may request, pursuant to a civil investigative demand, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in § 59.1-574. Data protection assessments shall be confidential and exempt from public inspection and copying under the Virginia Freedom of Information Act (§ 2.2-3700 et seq.). The disclosure of a data protection assessment pursuant to a request from the Attorney General shall not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

D. A single data protection assessment may address a comparable set of processing operations that include similar activities.

E. Data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may comply under this section if the assessments have a reasonably comparable scope and effect.

F. Data protection assessment requirements shall apply to processing activities created or generated after January 1, 2023, and are not retroactive.

59.1-577. Processing de-identified data; exemptions.

A. The controller in possession of de-identified data shall:

1. Take reasonable measures to ensure that the data cannot be associated with a natural person;
2. Publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and
3. Contractually obligate any recipients of the de-identified data to comply with all provisions of this chapter.

B. Nothing in this chapter shall be construed to (i) require a controller or processor to re-identify de-identified data or pseudonymous data or (ii) maintain data in identifiable form, or collect, obtain, retain, or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

C. Nothing in this chapter shall be construed to require a controller or processor to comply with an authenticated consumer rights request, pursuant to § 59.1-573, if all of the following are true:

1. The controller is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;
2. The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer; and
3. The controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

D. The consumer rights contained in subdivisions A 1 through 4 of § 59.1-573 and § 59.1-574 shall not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

E. A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

59.1-578. Limitations.

A. Nothing in this chapter shall be construed to restrict a controller's or processor's ability to:

1. Comply with federal, state, or local laws, rules, or regulations;
2. Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;
3. Cooperate with law-enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;
4. Investigate, establish, exercise, prepare for, or defend legal claims;
5. Provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer prior to entering into a contract;

6. Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;

7. Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action;

8. Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or similar independent oversight entities that determine: (i) if the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller; (ii) the expected benefits of the research outweigh the privacy risks; and (iii) if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; or

9. Assist another controller, processor, or third party with any of the obligations under this subsection.

B. The obligations imposed on controllers or processors under this chapter shall not restrict a controller's or processor's ability to collect, use, or retain data to:

1. Conduct internal research to develop, improve, or repair products, services, or technology;

2. Effectuate a product recall;

3. Identify and repair technical errors that impair existing or intended functionality; or

4. Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

C. The obligations imposed on controllers or processors under this chapter shall not apply where compliance by the controller or processor with this chapter would violate an evidentiary privilege under the laws of the Commonwealth. Nothing in this chapter shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of the Commonwealth as part of a privileged communication.

D. A controller or processor that discloses personal data to a third-party controller or processor, in compliance with the requirements of this chapter, is not in violation of this chapter if the third-party controller or processor that receives and processes such personal data is in violation of this chapter, provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation. A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this chapter is likewise not in violation of this chapter for the transgressions of the controller or processor from which it receives such personal data.

E. Nothing in this chapter shall be construed as an obligation imposed on controllers and processors that adversely affects the rights or freedoms of any persons, such as exercising the right of free speech pursuant to the First Amendment to the United States Constitution, or applies to the processing of personal data by a person in the course of a purely personal or household activity.

F. Personal data processed by a controller pursuant to this section shall not be processed for any purpose other than those expressly listed in this section unless otherwise allowed by this chapter. Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is:

1. Reasonably necessary and proportionate to the purposes listed in this section; and
2. Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used, or retained pursuant to subsection B shall, where applicable, take into account the nature and purpose or purposes of such collection, use, or retention. Such data shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use, or retention of personal data.

G. If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in subsection F.

H. Processing personal data for the purposes expressly identified in subdivisions A 1 through 9 shall not solely make an entity a controller with respect to such processing.

59.1-579. Investigative authority.

Whenever the Attorney General has reasonable cause to believe that any person has engaged in, is engaging in, or is about to engage in any violation of this chapter, the Attorney General is empowered

to issue a civil investigative demand. The provisions of § 59.1-9.10 shall apply mutatis mutandis to civil investigative demands issued under this section.

59.1-580. Enforcement; civil penalty; expenses.

A. The Attorney General shall have exclusive authority to enforce the provisions of this chapter.

B. Prior to initiating any action under this chapter, the Attorney General shall provide a controller or processor 30 days' written notice identifying the specific provisions of this chapter the Attorney General alleges have been or are being violated. If within the 30-day period, the controller or processor cures the noticed violation and provides the Attorney General an express written statement that the alleged violations have been cured and that no further violations shall occur, no action shall be initiated against the controller or processor.

C. If a controller or processor continues to violate this chapter following the cure period in subsection B or breaches an express written statement provided to the Attorney General under that subsection, the Attorney General may initiate an action in the name of the Commonwealth and may seek an injunction to restrain any violations of this chapter and civil penalties of up to \$7,500 for each violation under this chapter.

D. The Attorney General may recover reasonable expenses incurred in investigating and preparing the case, including attorney fees, in any action initiated under this chapter.

E. Nothing in this chapter shall be construed as providing the basis for, or be subject to, a private right of action for violations of this chapter or under any other law.

59.1-581. Consumer Privacy Fund.

There is hereby created in the state treasury a special nonreverting fund to be known as the Consumer Privacy Fund. The Fund shall be established on the books of the Comptroller. All civil penalties, expenses, and attorney fees collected pursuant to this chapter shall be paid into the state treasury and credited to the Fund. Interest earned on moneys in the Fund shall remain in the Fund and be credited to it. Any moneys remaining in the Fund, including interest thereon, at the end of each fiscal year shall not revert to the general fund but shall remain in the Fund. Moneys in the Fund shall be used to support the work of the Office of the Attorney General to enforce the provisions of this chapter, subject to appropriation.

2. The Chairman of the Joint Commission on Technology and Science shall create a work group composed of the Secretary of Commerce and Trade, the Secretary of Administration, the Attorney

General, the Chairman of the Senate Committee on Transportation, representatives of businesses who control or process personal data of at least 100,000 persons, and consumer rights advocates. The work group shall review the provisions of this act and issues related to its implementation. The Chairman of the Joint Commission on Technology and Science shall submit the work group's findings, best practices, and recommendations regarding the implementation of this act to the Chairmen of the Senate Committee on General Laws and Technology and the House Committee on Communications, Technology and Innovation no later than November 1, 2021.

3. That any reference to federal law or statute in this act shall be deemed to include any accompanying rules or regulations or exemptions thereto. Further, this enactment is declaratory of existing law.

4. That the provisions of the first and third enactments of this act shall become effective on January 1, 2023.

ABD - Colorado Privacy Act (CPA)

Colorado Privacy Act (CPA)

SENATE BILL 21-190

BY Senator(s) Rodriguez and Lundeen, Bridges, Buckner, Coleman, Cooke, Danielson, Donovan, Fenberg, Gardner, Ginal, Gonzales, Hansen, Hisey, Holbert, Jaquez Lewis, Kirkmeyer, Kolker, Lee, Liston, Moreno, Pettersen, Priola, Rankin, Scott, Simpson, Sonnenberg, Story, Winter, Woodward, Garcia; also Representative(s) Duran and Carver, Bennett, Bird, Cutter, Exum, Gonzales-Gutierrez, Gray, Herod, Jodeh, Lynch, McCluskie, McCormick, Mullica, Ricks, Snyder, Titone, Valdez A., Woodrow.

CONCERNING ADDITIONAL PROTECTION OF DATA RELATING TO PERSONAL PRIVACY.

Be it enacted by the General Assembly of the State of Colorado:

SECTION 1.

In Colorado Revised Statutes, add part 13 to article 1 of title 6 as follows:

PART 13 - COLORADO PRIVACY ACT

6-1-1301. Short title.

THE SHORT TITLE OF THIS PART 13 IS THE "COLORADO PRIVACY ACT".

6-1-1302. Legislative declaration.

(1) The general assembly hereby:

(a) finds that:

(I) the people of colorado regard their privacy as a fundamental right and an essential element of their individual freedom;

(II) colorado's constitution explicitly provides the right to privacy under Section 7 of article ii, and fundamental privacy rights have long been, and continue to be, integral to protecting coloradans and to safeguarding our temocratic republic;

(III) ongoing advances in technology have produced exponential growth in the volume and variety of personal data being generated, collected, stored, and analyzed and these advances present both promise and potential peril;

(IV) the ability to harness and use data in positive ways is driving innovation and brings beneficial technologies to society, but it has also created risks to privacy and freedom; and

(V) the unauthorized disclosure of personal information and loss of privacy can have devastating impacts ranging from financial fraud, identity theft, and unnecessary costs in personal time and finances to destruction of property, harassment, reputational damage, emotional distress, and physical harm;

(b) determines that:

(I) technological innovation and new uses of data can help solve societal problems and improve lives, and it is possible to build a world where technological innovation and privacy can coexist; and

(II) states across the United States are looking to this Part 13 and similar models to enact state-based data privacy requirements and to exercise the leadership that is lacking at the national level; and

(c) declares that:

(I) by enacting this part 13, Colorado will be among the states that empower consumers to protect their privacy and require companies to be responsible custodians of data as they continue to innovate;

(II) this part 13 addresses issues of statewide concern and:

(A) provides consumers the right to access, correct, and delete personal data and the right to opt out not only of the sale of personal data but also of the collection and use of personal data;

(B) imposes an affirmative obligation upon companies to safeguard personal data; to provide clear, understandable, and transparent information to consumers about how their personal data are used; and to strengthen compliance and accountability by requiring data protection assessments in the collection and use of personal data; and

(C) empowers the attorney general and district attorneys to access and evaluate a company's data protection assessments, to impose penalties where violations occur, and to prevent future violations.

6-1-1303. Definitions. as used in this part 13, unless the context otherwise requires:

(1) "affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity. as used in this Subsection (1), "control" means:

(a) ownership of, control of, or power to vote twenty-five percent or more of the outstanding shares of any class of voting security of the entity, directly or indirectly, or acting through one or more other persons;

(b) control in any manner over the election of a majority of the directors, trustees, or general partners of the entity or of individuals exercising similar functions; or

(c) the power to exercise, directly or indirectly, a controlling influence over the management or policies of the entity as determined by the applicable prudential regulator, as that term is defined in 12 U.S.C. Sec. 5481 (24), if any.

(2) "authenticate" means to use reasonable means to determine that a request to exercise any of the rights in Section 6-1-1306 (1) is being made by or on behalf of the consumer who is entitled to exercise the rights.

(3) "business associate" has the meaning established in 45 CFR 160.103.

(4) "child" means an individual under thirteen years of age.

(5) "consent" means a clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement, such as by a written statement, including by electronic means, or other clear, affirmative action by which the consumer signifies agreement to the processing of personal data. The following does not constitute consent:

(a) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information;

(b) hovering over, muting, pausing, or closing a given piece of content; and

(c) agreement obtained through dark patterns.

(6) "consumer":

(a) means an individual who is a colorado resident acting only in an individual or household context; and

(b) does not include an individual acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context.

(7) "controller" means a person that, alone or jointly with others, determines the purposes for and means of processing personal data.

(8) "covered entity" has the meaning established in 45 CFR 160.103.

(9) “dark pattern” means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.

(10) “decisions that produce legal or similarly significant effects concerning a consumer” means a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services.

(11) “de-identified data” means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such an individual, if the controller that possesses the data:

(a) takes reasonable measures to ensure that the data cannot be associated with an individual;

(b) publicly commits to maintain and use the data only in a de-identified fashion and not attempt to re-identify the data; and

(c) contractually obligates any recipients of the information to comply with the requirements of this Subsection (11).

(12) “health-care facility” means any entity that is licensed, certified, or otherwise authorized or permitted by law to administer medical treatment in this state.

(13) “health-care information” means individually identifiable information relating to the past, present, or future health status of an individual.

(14) “health-care provider” means a person licensed, certified, or registered in this state to practice medicine, pharmacy, chiropractic, nursing, physical therapy, podiatry, dentistry, optometry, occupational therapy, or other healing arts under title 12.

(15) “HIPAA” means the federal “health insurance portability and accountability act of 1996”, as amended, 42 U.S.C. secs. 1320d to 1320d-9.

(16) “identified or identifiable individual” means an individual who can be readily identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, specific geolocation data, or an online identifier.

(17) “personal data”:

(a) means information that is linked or reasonably linkable to an identified or identifiable individual; and

(b) does not include de-identified data or publicly available information. as used in this Subsection (17)(b), “publicly available information” means information that is lawfully made available from federal, state, or local government records and information that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public.

(18) “process” or “processing” means the collection, use, sale, storage, disclosure, analysis, deletion, or modification of personal data and includes the actions of a controller directing a processor to process personal data.

(19) “processor” means a person that processes personal data on behalf of a controller.

(20) “profiling” means any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual’s economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(21) “protected health information” has the meaning established in 45 CFR 160.103.

(22) “pseudonymous data” means personal data that can no longer be attributed to a specific individual without the use of additional information if the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to a specific individual.

(23) (a) “sale”, “sell”, or “sold” means the exchange of personal data for monetary or other valuable consideration by a controller to a third party.

(b) “sale”, “sell”, or “sold” does not include the following:

(I) the disclosure of personal data to a processor that processes the personal data on behalf of a controller;

(II) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;

(III) the disclosure or transfer of personal data to an affiliate of the controller;

(IV) the disclosure or transfer to a third party of personal data as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller’s assets; or

(V) the disclosure of personal data:

(A) that a consumer directs the controller to disclose or intentionally discloses by using the controller to interact with a third party; or

(B) intentionally made available by a consumer to the general public via a channel of mass media.

(24) "sensitive data" means:

(a) personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status;

(b) genetic or biometric data that may be processed for the purpose of uniquely identifying an individual; or

(c) personal data from a known child.

(25) "targeted advertising":

(a) means displaying to a consumer an advertisement that is selected based on personal data obtained or inferred over time from the consumer's activities across nonaffiliated websites, applications, or online services to predict consumer preferences or interests; and

(b) does not include:

(I) advertising to a consumer in response to the consumer's request for information or feedback;

(II) advertisements based on activities within a controller's own websites or online applications;

(III) advertisements based on the context of a consumer's current search query, visit to a website, or online application; or

(IV) processing personal data solely for measuring or reporting advertising performance, reach, or frequency.

(26) "third party" means a person, public authority, agency, or body other than a consumer, controller, processor, or affiliate of the processor or the controller.

6-1-1304. Applicability of part.

(1) Except as specified in Subsection (2) of this Section, this Part 13 applies to a controller that:

(a) conducts business in colorado or produces or delivers commercial products or services that are intentionally targeted to residents of colorado; and

(b) satisfies one or both of the following thresholds:

(I) controls or processes the personal data of one hundred thousand consumers or more during a calendar year; or

(II) derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of twenty-five thousand consumers or more.

(2) this Part 13 does not apply to:

(a) protected health information that is collected, stored, and processed by a covered entity or its business associates;

(b) health-care information that is governed by Part 8 of article 1 of title 25 solely for the purpose of access to medical records;

(c) patient identifying information, as defined in 42 CFR 2.11, that are governed by and collected and processed pursuant to 42 CFR 2, established pursuant to 42 U.S.C. sec. 290dd-2;

(d) identifiable private information, as defined in 45 CFR 46.102, for purposes of the federal policy for the protection of human subjects pursuant to 45 CFR 46; identifiable private information that is collected as part of human subjects research pursuant to the ich e6 good clinical practice guideline issued by the international council for harmonisation of technical requirements for pharmaceuticals for human use or the protection of human subjects under 21 CFR 50 and 56; or personal data used or shared in research conducted in accordance with one or more of the categories set forth in this Subsection (2)(d);

(e) information and documents created by a covered entity for purposes of complying with HIPAA and its implementing regulations;

(f) patient safety work product, as defined in 42 CFR 3.20, that is created for purposes of patient safety improvement pursuant to 42 CFR 3, established pursuant to 42 U.S.C. secs.

299b-21 to 299b-26;

(g) information that is:

(I) de-identified in accordance with the requirements for de-identification set forth in 45 CFR 164; and

(II) derived from any of the health-care-related information described in this Section.

(h) information maintained in the same manner as information under Subsections (2)(a) to (2)(g) of this Section by:

(I) a covered entity or business associate;

(II) a health-care facility or health-care provider; or

(III) a program of a qualified service organization as defined in 42 CFR 2.11;

(i)(i) except as provided in Subsection (2)(i)(ii) of this Section, an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal data bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by:

(A) a consumer reporting agency as defined in 15 U.S.C. sec. 1681a (f);

(B) a furnisher of information as set forth in 15 U.S.C. sec. 1681s-2 that provides information for use in a consumer report, as defined in 15 U.S.C. sec. 1681a (d); or

(C) a user of a consumer report as set forth in 15 U.S.C. sec. 1681b.

(ii) this Subsection (2)(i) applies only to the extent that the activity is regulated by the federal "fair credit reporting act", 15 U.S.C. sec. 1681 et seq., as amended, and the personal data are not collected, maintained, disclosed, sold, communicated, or used except as authorized by the federal "fair credit reporting act", as amended.

(j) personal data:

(I) collected and maintained for purposes of article 22 of title 10;

(II) collected, processed, sold, or disclosed pursuant to the federal "gramm-leach-bliley act", 15 U.S.C. sec. 6801 et seq., as amended, and implementing regulations, if the collection, processing, sale, or disclosure is in compliance with that law;

(III) collected, processed, sold, or disclosed pursuant to the federal "driver's privacy protection act of 1994", 18 U.S.C. sec. 2721 et seq., as amended, if the collection, processing, sale, or disclosure is regulated by that law, including implementing rules, regulations, or exemptions;

(IV) regulated by the federal "children's online privacy protection act of 1998", 15 U.S.C. secs. 6501 to 6506, as amended, if collected, processed, and maintained in compliance with that law; or

(V) regulated by the federal "family educational rights

and privacy act of 1974", 20 U.S.C. sec. 1232g et seq., as amended, and its implementing regulations;

(k) data maintained for employment records purposes;

(l) an air carrier as defined in and regulated under 49 U.S.C.

sec. 40101 et seq., as amended, and 49 U.S.C. sec. 41713, as amended;

(m) a national securities association registered pursuant to the federal “securities exchange act of 1934”, 15 U.S.C. sec. 78o-3, as amended, or implementing regulations;

(n) customer data maintained by a public utility as defined in Section 40-1-103 (1)(a)(i) or an authority as defined in Section 43-4-503 (1), if the data are not collected, maintained, disclosed, sold, communicated, or used except as authorized by state and federal law;

(o) data maintained by a state institution of higher education, as defined in Section 23-18-102 (10), the state, the judicial department of the state, or a county, city and county, or municipality if the data is collected, maintained, disclosed, communicated, and used as authorized by state and federal law for noncommercial purposes. this Subsection (2)(o) does not effect any other exemption available under this Part 13.

(p) information used and disclosed in compliance with 45 CFR 164.512; or

(q) a financial institution or an affiliate of a financial institution as defined by and that is subject to the federal “gramm-leach-bliley act”, 15 u.s.c. sec. 6801 et seq., as amended, and implementing regulations, including regulation p, 12 CFR 1016.

(3) the obligations imposed on controllers or processors under this Part 13 do not:

(a) restrict a controller’s or processor’s ability to:

(I) comply with federal, state, or local laws, rules, or regulations;

(II) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

(III) cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local law;

(IV) investigate, exercise, prepare for, or defend actual or anticipated legal claims;

(V) conduct internal research to improve, repair, or develop products, services, or technology;

(VI) identify and repair technical errors that impair existing or intended functionality;

(VII) perform internal operations that are reasonably aligned with the expectations of the consumer based on the consumer’s existing relationship with the controller;

(VIII) provide a product or service specifically requested by a consumer or the parent or guardian of a child, perform a contract to which the consumer is a party, or take steps at the request of the consumer prior to entering into a contract;

(IX) protect the vital interests of the consumer or of another individual;

(X) prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, or malicious, deceptive, or illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action;

(XI) process personal data for reasons of public interest in the area of public health, but solely to the extent that the processing:

(A) is subject to suitable and specific measures to safeguard the rights of the consumer whose personal data are processed; and

(B) is under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law; or

(XII) assist another person with any of the activities set forth in this Subsection (3);

(b) apply where compliance by the controller or processor with this pPartart 13 would violate an evidentiary privilege under colorado law;

(c) prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under colorado law as part of a privileged communication;

(d) apply to information made available by a third party that the controller has a reasonable basis to believe is protected speech pursuant to applicable law; and

(e) apply to the processing of personal data by an individual in the course of a purely personal or household activity.

(4) personal data that are processed by a controller pursuant to an exception provided by this Section:

(a) shall not be processed for any purpose other than a purpose expressly listed in this Section or as otherwise authorized by this Part 13; and

(b) shall be processed solely to the extent that the processing is necessary, reasonable, and proportionate to the specific purpose or purposes listed in this Section or as otherwise authorized by this Part 13.

(5) if a controller processes personal data pursuant to an exemption in this Section, the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with the requirements in Subsection (4) of this Section.

6-1-1305. Responsibility according to role.

- (1) Controllers and processors shall meet their respective obligations established under this Part 13.
- (2) processors shall adhere to the instructions of the controller and assist the controller to meet its obligations under this Part 13. taking into account the nature of processing and the information available to the processor, the processor shall assist the controller by:
 - (a) taking appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to consumer requests to exercise their rights pursuant to Section 6-1-1306;
 - (b) helping to meet the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of the security of the system pursuant to Section 6-1-716; and
 - (c) providing information to the controller necessary to enable the controller to conduct and document any data protection assessments required by Section 6-1-1309. the controller and processor are each responsible for only the measures allocated to them.
- (3) notwithstanding the instructions of the controller, a processor shall:
 - (a) ensure that each person processing the personal data is subject to a duty of confidentiality with respect to the data; and
 - (b) engage a subcontractor only after providing the controller with an opportunity to object and pursuant to a written contract in accordance with Subsection (5) of this Section that requires the subcontractor to meet the obligations of the processor with respect to the personal data.
- (4) taking into account the context of processing, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between them to implement the measures.
- (5) processing by a processor must be governed by a contract between the controller and the processor that is binding on both parties and that sets out:
 - (a) the processing instructions to which the processor is bound, including the nature and purpose of the processing;
 - (b) the type of personal data subject to the processing, and the duration of the processing;
 - (c) the requirements imposed by this Subsection (5) and Subsections (3) and (4) of this Section; and
 - (d) the following requirements:

(I) at the choice of the controller, the processor shall delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

(II) (a) the processor shall make available to the controller all information necessary to demonstrate compliance with the obligations in this Part 13; and

(b) the processor shall allow for, and contribute to, reasonable audits and inspections by the controller or the controller's designated auditor. alternatively, the processor may, with the controller's consent, arrange for a qualified and independent auditor to conduct, at least annually and at the processor's expense, an audit of the processor's policies and technical and organizational measures in support of the obligations under this Part 13 using an appropriate and accepted control standard or framework and audit procedure for the audits as applicable. the processor shall provide a report of the audit to the controller upon request.

(6) in no event may a contract relieve a controller or a processor from the liabilities imposed on them by virtue of its role in the processing relationship as defined by this Part 13.

(7) determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data are to be processed. a person that is not limited in its processing of personal data pursuant to a controller's instructions, or that fails to adhere to the instructions, is a controller and not a processor with respect to a specific processing of data. a processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. if a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, it is a controller with respect to the processing.

(8) (a) a controller or processor that discloses personal data to another controller or processor in compliance with this Part 13 does not violate this Part 13 if the recipient processes the personal data in violation of this Part 13, and, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation.

(b) a controller or processor receiving personal data from a controller or processor in compliance with this Part 13 as specified in Subsection (8)(a) of this Section does not violate this Part 13 if the controller or processor from which it receives the personal data fails to comply with applicable obligations under this Part 13.

6-1-1306. Consumer personal data rights - repeal.

(1) Consumers may exercise the following rights by submitting a request using the methods specified by the controller in the privacy notice required under Section 6-1-1308 (1)(a). The method must take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication relating to the request, and the ability of the controller to authenticate the identity of the consumer making the request. controllers shall not require a consumer to create a new account in order to exercise consumer rights pursuant to this Section but may require a consumer to use an existing account. a consumer may submit a request at any time to a controller specifying which of the following rights the consumer wishes to exercise:

(a) Right to opt out. (i) a consumer has the right to opt out of the processing of personal data concerning the consumer for purposes of:

(A) targeted advertising;

(B) the sale of personal data; or

(C) profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.

(II) a consumer may authorize another person, acting on the consumer's behalf, to opt out of the processing of the consumer's personal data for one or more of the purposes specified in Subsection (1)(a)(i) of this Section, including through a technology indicating the consumer's intent to opt out such as a web link indicating a preference or browser setting, browser extension, or global device setting. a controller shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf if the controller is able to authenticate, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

(III) a controller that processes personal data for purposes of targeted advertising or the sale of personal data shall provide a clear and conspicuous method to exercise the right to opt out of the processing of personal data concerning the consumer pursuant to Subsection (1)(a)(i) of this Section. the controller shall provide the opt-out method clearly and conspicuously in any privacy notice required to be provided to consumers under this Part 13, and in a clear, conspicuous, and readily accessible location outside the privacy notice.

(IV) (a) a controller that processes personal data for purposes of targeted advertising or the sale of personal data may allow consumers to exercise the right to opt out of the processing of personal data concerning the consumer for purposes of targeted advertising or the sale of personal data pursuant

to Subsections (1)(a)(i)(a) and (1)(a)(i)(b) of this Section by controllers through a user-selected universal opt-out mechanism that meets the technical specifications established by the attorney general pursuant to Section 6-1-1313. this Subsection (1)(a)(iv)(a) is repealed, effective July 1, 2024.

(B) effective July 1, 2024, a controller that processes personal data for purposes of targeted advertising or the sale of personal data shall allow consumers to exercise the right to opt out of the processing of personal data concerning the consumer for purposes of targeted advertising or the sale of personal data pursuant to Subsections (1)(a)(i)(a) and (1)(a)(i)(b) of this Section by controllers through a user-selected universal opt-out mechanism that meets the technical specifications established by the attorney general pursuant to Section 6-1-1313.

(C) notwithstanding a consumer's decision to exercise the right to opt out of the processing of personal data through a universal opt-out mechanism pursuant to Subsection (1)(a)(iv)(b) of this Section, a controller may enable the consumer to consent, through a web page, application, or a similar method, to the processing of the consumer's personal data for purposes of targeted advertising or the sale of personal data, and the consent takes precedence over any choice reflected through the universal opt-out mechanism. before obtaining a consumer's consent to process personal data for purposes of targeted advertising or the sale of personal data pursuant to this Subsection (1)(a)(iv)(c), a controller shall provide the consumer with a clear and conspicuous notice informing the consumer about the choices available under this Section, describing the categories of personal data to be processed and the purposes for which they will be processed, and explaining how and where the consumer may withdraw consent. the web page, application, or other means by which a controller obtains a consumer's consent to process personal data for purposes of targeted advertising or the sale of personal data must also allow the consumer to revoke the consent as easily as it is affirmatively provided.

(b) Right of access. a consumer has the right to confirm whether a controller is processing personal data concerning the consumer and to access the consumer's personal data.

(c) Right to correction. a consumer has the right to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.

(d) Right to deletion. a consumer has the right to delete personal data concerning the consumer.

(e) Right to data portability. when exercising the right to access personal data pursuant to Subsection (1)(b) of this Section, a consumer has the right to obtain the personal data in a portable and, to the

extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity without hindrance. a consumer may exercise this right no more than two times per calendar year. nothing in this Subsection (1)(e) requires a controller to provide the data to the consumer in a manner that would disclose the controller's trade secrets.

(2) Responding to consumer requests. (a) a controller shall inform a consumer of any action taken on a request under Subsection (1) of this Section without undue delay and, in any event, within forty-five days after receipt of the request. the controller may extend the forty-five-day period by forty-five additional days where reasonably necessary, taking into account the complexity and number of the requests. the controller shall inform the consumer of an extension within forty-five days after receipt of the request, together with the reasons for the delay.

(b) if a controller does not take action on the request of a consumer, the controller shall inform the consumer, without undue delay and, at the latest, within forty-five days after receipt of the request, of the reasons for not taking action and instructions for how to appeal the decision with the controller as described in Subsection (3) of this Section.

(c) upon request, a controller shall provide to the consumer the information specified in this Section free of charge; except that, for a second or subsequent request within a twelve-month period, the controller may charge an amount calculated in the manner specified in Section 24-72-205 (5)(a).

(d) a controller is not required to comply with a request to exercise any of the rights under Subsection (1) of this Section if the controller is unable to authenticate the request using commercially reasonable efforts, in which case the controller may request the provision of additional information reasonably necessary to authenticate the request.

(3) (a) a controller shall establish an internal process whereby consumers may appeal a refusal to take action on a request to exercise any of the rights under Subsection (1) of this Section within a reasonable period after the consumer's receipt of the notice sent by the controller under Subsection (2)(b) of this Section. the appeal process must be conspicuously available and as easy to use as the process for submitting a request under this Section.

(b) within forty-five days after receipt of an appeal, a controller shall inform the consumer of any action taken or not taken in response to the appeal, along with a written explanation of the reasons in support of the response. the controller may extend the forty-five-day period by sixty additional days where reasonably necessary, taking into account the complexity and number of requests serving as

the basis for the appeal. the controller shall inform the consumer of an extension within forty-five days after receipt of the appeal, together with the reasons for the delay.

(c) the controller shall inform the consumer of the consumer's ability to contact the attorney general if the consumer has concerns about the result of the appeal.

6-1-1307. Processing de-identified data.

(1) This Part 13 does not require a controller or processor to do any of the following solely for purposes of complying with this Part 13:

(a) reidentify de-identified data;

(b) comply with an authenticated consumer request to access, correct, delete, or provide personal data in a portable format pursuant to section 6-1-1306 (1), if all of the following are true:

(I) (a) the controller is not reasonably capable of associating the request with the personal data; or

(b) it would be unreasonably burdensome for the controller to associate the request with the personal data;

(II) the controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with other personal data about the same specific consumer; and

(III) the controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party, except as otherwise authorized by the consumer; or

(c) maintain data in identifiable form or collect, obtain, retain, or access any data or technology in order to enable the controller to associate an authenticated consumer request with personal data.

(2) a controller that uses de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the de-identified data are subject and shall take appropriate steps to address any breaches of contractual commitments.

(3) the rights contained in Section 6-1-1306 (1)(b) to (1)(e) do not apply to pseudonymous data if the controller can demonstrate that the information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

6-1-1308. Duties of controllers.

(1) Duty of transparency. (a) a controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

(I) the categories of personal data collected or processed by the controller or a processor;

(II) the purposes for which the categories of personal data are processed;

(III) how and where consumers may exercise the rights pursuant to Section 6-1-1306, including the controller's contact information and how a consumer may appeal a controller's action with regard to the consumer's request;

(IV) the categories of personal data that the controller shares with third parties, if any; and

(V) the categories of third parties, if any, with whom the controller shares personal data.

(b) if a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the sale or processing, as well as the manner in which a consumer may exercise the right to opt out of the sale or processing.

(c) a controller shall not:

(I) require a consumer to create a new account in order to exercise a right; or

(II) based solely on the exercise of a right and unrelated to feasibility or the value of a service, increase the cost of, or decrease the availability of, the product or service.

(d) nothing in this Part 13 shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discount, or club card program.

(2) Duty of purpose specification. a controller shall specify the express purposes for which personal data are collected and processed.

(3) Duty of data minimization. a controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed.

(4) Duty to avoid secondary use. a controller shall not process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes for which the personal data are processed, unless the controller first obtains the consumer's consent.

(5) Duty of care. a controller shall take reasonable measures to secure personal data during both storage and use from unauthorized acquisition. the data security practices must be appropriate to the volume, scope, and nature of the personal data processed and the nature of the business.

(6) Duty to avoid unlawful discrimination. a controller shall not process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers.

(7) Duty regarding sensitive data. a controller shall not process a consumer's sensitive data without first obtaining the consumer's consent or, in the case of the processing of personal data concerning a known child, without first obtaining consent from the child's parent or lawful guardian.

6-1-1309. Data protection assessments - attorney general access and evaluation - definition.

(1) A controller shall not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment of each of its processing activities that involve personal data acquired on or after the effective date of this Section that present a heightened risk of harm to a consumer.

(2) for purposes of this Section, "processing that presents a heightened risk of harm to a consumer" includes the following:

(a) processing personal data for purposes of targeted advertising or for profiling if the profiling presents a reasonably foreseeable risk of:

(I) unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

(II) financial or physical injury to consumers;

(III) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or

(IV) other substantial injury to consumers;

(b) selling personal data; and

(c) processing sensitive data.

(3) data protection assessments must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public

against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that the controller can employ to reduce the risks. the controller shall factor into this assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(4) a controller shall make the data protection assessment available to the attorney general upon request. the attorney general may evaluate the data protection assessment for compliance with the duties contained in Section 6-1-1308 and with other laws, including this article 1. data protection assessments are confidential and exempt from public inspection and copying under the “colorado open records act”, Part 2 of article 72 of title 24. the disclosure of a data protection assessment pursuant to a request from the attorney general under this Subsection (4) does not constitute a waiver of any attorney-client privilege or work-product protection that might otherwise exist with respect to the assessment and any information contained in the assessment.

(5) a single data protection assessment may address a comparable set of processing operations that include similar activities.

(6) data protection assessment requirements apply to processing activities created or generated after july 1, 2023, and are not retroactive.

6-1-1310. Liability.

(1) Notwithstanding any provision in Part 1 of this article 1, this Part 13 does not authorize a private right of action for a violation of this Part 13 or any other provision of law. this Subsection (1) neither relieves any party from any duties or obligations imposed, nor alters any independent rights that consumers have, under other laws, including this article 1, the state constitution, or the united states constitution.

(2) Where more than one controller or processor, or both a controller and a processor, involved in the same processing violates this Part 13, the liability shall be allocated among the parties according to principles of comparative fault.

6-1-1311. Enforcement - penalties - repeal.

(1) (a) Notwithstanding any other provision of this article 1, the attorney general and district attorneys have exclusive authority to enforce this Part 13 by bringing an action in the name of the state or as parens patriae on behalf of persons residing in the state to enforce this Part 13 as provided in this article 1, including seeking an injunction to enjoin a violation of this part 13.

(b) notwithstanding any other provision of this article 1, nothing in this Part 13 shall be construed as providing the basis for, or being subject to, a private right of action for violations of this Part 13 or any other law.

(c) for purposes only of enforcement of this Part 13 by the attorney general or a district attorney, a violation of this Part 13 is a deceptive trade practice.

(d) prior to any enforcement action pursuant to Subsection (1)(a) of this Section, the attorney general or district attorney must issue a notice of violation to the controller if a cure is deemed possible. if the controller fails to cure the violation within sixty days after receipt of the notice of violation, an action may be brought pursuant to this Section. this Subsection (1)(d) is repealed, effective january 1, 2025.

(2) the state treasurer shall credit all receipts from the imposition of civil penalties under this Part 13 pursuant to Section 24-31-108.

6-1-1312. Preemption - local governments.

This Part 13 supersedes and preempts laws, ordinances, resolutions, regulations, or the equivalent adopted by any statutory or home rule municipality, county, or city and county regarding the processing of personal data by controllers or processors.

6-1-1313. Rules - opt-out mechanism.

(1) The attorney general may promulgate rules for the purpose of carrying out this Part 13.

(2) by july 1, 2023, the attorney general shall adopt rules that detail the technical specifications for one or more universal opt-out mechanisms that clearly communicate a consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data pursuant to Section 6-1-1306 (1)(a)(i)(a) or (1)(a)(i)(b). the attorney general may update the rules that detail the technical specifications for the mechanisms from time to time to reflect the means by which consumers interact with controllers. the rules must:

(a) not permit the manufacturer of a platform, browser, device, or any other product offering a universal opt-out mechanism to unfairly disadvantage another controller;

(b) require controllers to inform consumers about the opt-out choices available under Section 6-1-1306 (1)(a)(i);

(c) not adopt a mechanism that is a default setting, but rather clearly represents the consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data pursuant to Section 6-1-1306 (1)(a)(i)(a) or (1)(a)(i)(b);

(d) adopt a mechanism that is consumer-friendly, clearly described, and easy to use by the average consumer;

(e) adopt a mechanism that is as consistent as possible with any other similar mechanism required by law or regulation in the united states; and

(f) permit the controller to accurately authenticate the consumer as a resident of this state and determine that the mechanism represents a legitimate request to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data pursuant to Section 6-1-1306 (1)(a)(i)(a) or (1)(a)(i)(b).

(3) by January 1, 2025, the attorney general may adopt rules that govern the process of issuing opinion letters and interpretive guidance to develop an operational framework for business that includes a good faith reliance defense of an action that may otherwise constitute a violation of this Part 13. the rules must become effective by July 1, 2025.

SECTION 2.

In Colorado Revised Statutes, amend 6-1-104 as follows:

6-1-104. Cooperative reporting.

The district attorneys may cooperate in a statewide reporting system by receiving, on forms provided by the attorney general, complaints from persons concerning deceptive trade practices listed in Section 6-1-105 or Part 7 OR 13 of this Article 1 and transmitting the complaints to the attorney general.

SECTION 3.

In Colorado Revised Statutes, 6-1-105, add (1)(nnn) as follows:

6-1-105. Unfair or deceptive trade practices.

(1) A person engages in a deceptive trade practice when, in the course of the person's business, vocation, or occupation, the person:

(nnn) violates any provision of Part 13 of this article 1 as specified in Section 6-1-1311 (1)(c).

SECTION 4.

In Colorado Revised Statutes, 6-1-107, amend (1) introductory portion as follows:

6-1-107. Powers of attorney general and district attorneys.

(1) When the Attorney General or a District Attorney has reasonable cause to believe that any person, whether in this state or elsewhere, has engaged in or is engaging in any deceptive trade practice listed in Section 6-1-105 or Part 7 OR 13 of this Article 1, the Attorney General or District Attorney may:

SECTION 5.

In Colorado Revised Statutes, 6-1-108, amend (1) as follows:

6-1-108. Subpoenas - hearings - rules.

(1) When the attorney general or a district attorney has reasonable cause to believe that a person, whether in this state or elsewhere, has engaged in or is engaging in a deceptive trade practice listed in Section 6-1-105 or Part 7 or 13 of this article 1, the attorney general or a district attorney, in addition to other powers conferred upon the Attorney General or a District Attorney by this Article 1, may issue subpoenas to require the attendance of witnesses or the production of documents, administer oaths, conduct hearings in aid of any investigation or inquiry, and prescribe such forms and promulgate such rules as may be necessary to administer the provisions of this Article 1.

SECTION 6.

In Colorado Revised Statutes, 6-1-110, amend (1) and (2) as follows:

6-1-110. Restraining orders - injunctions - assurances of discontinuance.

(1) Whenever the attorney general or a district attorney has cause to believe that a person has engaged in or is engaging in any deceptive trade practice listed in Section 6-1-105 or Part 7 or 13 of this Article 1, the attorney general or district attorney may apply for and obtain, in an action in the appropriate district court of this state, a temporary restraining order or injunction, or both, pursuant to the Colorado rules of civil procedure, prohibiting the person from continuing The practices, or engaging therein, or doing any act in furtherance thereof. The court may make such orders or judgments as may be necessary to prevent the use or employment by the person of any such deceptive trade practice or that may be necessary to completely compensate or restore to the original position of any person injured by means of any such practice or to prevent any unjust enrichment by any person through the use or employment of any deceptive trade practice.

(2) Where the attorney general or a district attorney has authority to institute a civil action or other proceeding pursuant to the provisions of this Article 1, the attorney general or district attorney may accept, in lieu thereof or as a Part thereof, an assurance of discontinuance of any deceptive trade practice listed in Section 6-1-105 or Part 7 OR 13 of this Article 1. The assurance may include a

stipulation for the voluntary payment by the alleged violator of the costs of investigation and any action or proceeding by the attorney general or a district attorney and any amount necessary to restore to any person any money or property that may have been acquired by the alleged violator by means of any such deceptive trade practice. Any such assurance of discontinuance accepted by the attorney general or a district attorney and any such stipulation filed with the court as a part of any such action or proceeding is a matter of public record unless the attorney general or the district attorney determines, at the discretion the attorney general or district attorney, that it will be confidential to the parties to the action or proceeding and to the court and its employees. Upon the filing of a civil action by the attorney general or a district attorney alleging that a confidential assurance of discontinuance or stipulation accepted pursuant to this Subsection (2) has been violated, the assurance of discontinuance or stipulation becomes a public record and open to inspection by any person. Proof by a preponderance of the evidence of a violation of any such assurance or stipulation constitutes prima facie evidence of a deceptive trade practice for the purposes of any civil action or proceeding brought thereafter by the attorney general or a district attorney, whether a new action or a subsequent motion or petition in any pending action or proceeding.

SECTION 7. Act subject to petition - effective date - applicability

(1) This act takes effect July 1, 2023; except that, if a referendum petition is filed pursuant to Section 1(3) of article V of the state constitution against this act or an item, Section, or Part of this act within the ninety-day period after final adjournment of the general assembly, then the act, item, Section, or Part will not take effect unless approved by the people at the general election to be held in November 2022 and, in such case, will take effect July 1, 2023, or on the date of the official declaration of the vote thereon by the governor, whichever is later.

(2) This act applies to conduct occurring on or after the applicable effective date of this act.

Almanya - Federal Data Protection Act (BDSG)

Federal Data Protection Act (BDSG)

Full citation: Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626).

Part I

Common provisions

Chapter 1

Scope and definitions

Section 1

Scope of the Act

(1) This Act shall apply to the processing of personal data by

1. public bodies of the Federation,
2. public bodies of the Länder, where data protection is not governed by Land law and where they
 - a) carry out federal law or
 - b) act in the capacity of judicial bodies in matters other than administrative matters.

For private bodies, this Act shall apply to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system unless such processing is conducted by natural persons in the course of a purely personal or domestic activity.

(2) Other federal data protection legislation shall take precedence over the provisions of this Act. If such legislation does not govern a matter conclusively or at all which is covered by this Act, then this Act shall apply. The duty to observe the legal obligation of maintaining secrecy or professional or special official confidentiality not based on legal provisions shall remain unaffected.

(3) The provisions of this Act shall take precedence over those of the Administrative Procedure Act where personal data are processed to establish the facts.

(4) This Act shall apply to public bodies. It shall apply to private bodies if

1. the controller or processor processes personal data in Germany,
2. personal data are processed in the context of the activities of an establishment of the controller or processor in Germany, or if,
3. although the controller or processor has no establishment in a Member State of the European Union or another contracting state of the European Economic Area, it does fall within the scope of Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119 of 4 May 2016, p. 1; L 314 of 22 November 2016, p. 72; L 127 of 23 May 2018, p. 2) in the applicable version.

If this Act does not apply in accordance with the second sentence, only Sections 8 to 21 and 39 to 44 shall apply to the controller or processor.

(5) The provisions of this Act shall not apply where the law of the European Union, in particular Regulation (EU) 2016/679 in the applicable version, directly applies.

(6) The contracting states of the European Economic Area shall have equal status with the Member States of the European Union with regard to processing for purposes in accordance with Article 2 of Regulation (EU) 2016/679. Other states shall be regarded as third countries.

(7) With regard to processing for purposes in accordance with Article 1 (1) of Directive (EU) 2016/680 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119 of 4 May 2016, p. 89), the states associated with the implementation, application and development of the Schengen Acquis shall have equal status with the Member States of the European Union. Other states shall be regarded as third countries.

(8) Regulation (EU) 2016/679 and Parts 1 and 2 of this Act shall apply accordingly to processing of personal data by public bodies in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680 unless otherwise provided for in this or another Act.

Section 2

Definitions

(1) Public bodies of the Federation are the authorities, judicial bodies and other public law institutions of the Federation, of direct federal corporations, statutory bodies and foundations established under public law and of their associations irrespective of their legal form.

(2) Public bodies of the Länder are the authorities, judicial bodies and other public law institutions of a Land, a municipality, an association of municipalities or of other legal persons under public law subject to Land supervision and of their associations irrespective of their legal form.

(3) Associations of public bodies of the Federation and the Länder which are established under private law and perform tasks of public administration shall be regarded as public bodies of the Federation irrespective of the participation of private bodies if

1. they operate beyond the borders of a Land, or
2. the Federation holds the absolute majority of shares or controls the absolute majority of votes.

Otherwise they shall be regarded as public bodies of the Länder.

(4) Private bodies are natural and legal persons, societies and other associations established under private law unless they are covered by subsections 1 to 3. If a private body performs sovereign tasks of the public administration, it shall be a public body as defined in this Act.

(5) Public bodies of the Federation shall be regarded as private bodies as defined in this Act if they take part in competition as enterprises governed by public law. Public bodies of the Länder shall also be regarded as private bodies as defined in this Act if they take part in competition as enterprises governed by public law and carry out federal law, and if data protection is not governed by Land law.

Chapter 2

Legal basis for processing personal data

Section 3

Processing of personal data by public bodies

Public bodies shall be permitted to process personal data if such processing is necessary to perform the task for which the controller is responsible or to exercise official authority which has been vested in the controller.

Section 4

Video surveillance of publicly accessible spaces

(1) Monitoring publicly accessible areas with optical-electronic devices (video surveillance) shall be permitted only as far as it is necessary

1. for public bodies to perform their tasks,
2. to exercise the right to determine who shall be allowed or denied access or
3. to safeguard legitimate interests for specifically defined purposes

and if there is nothing to indicate legitimate overriding interests of the data subjects. For video surveillance of

1. large publicly accessible facilities, such as sport facilities, places of gathering and entertainment, shopping centres and car parks, or
2. vehicles and large publicly accessible facilities of public rail, ship or bus transport,

protecting the lives, health and freedom of persons present shall be regarded as a very important interest.

(2) Appropriate measures shall be taken to make the surveillance and the controller's name and contact details identifiable as early as possible.

(3) Storing or using data collected pursuant to subsection 1 shall be permitted if necessary to achieve the intended purpose and if there is nothing to indicate legitimate overriding interests of the data subjects. Subsection 1, second sentence, shall apply accordingly. The data may be further processed for another purpose only if necessary to prevent threats to state and public security and to prosecute crimes.

(4) If data collected from video surveillance are attributed to a particular person, that person shall be informed of the processing in accordance with Articles 13 and 14 of Regulation (EU) 2016/679. Section 32 shall apply accordingly.

(5) The data shall be deleted without delay, if they are no longer needed for the intended purpose or if the data subject's legitimate interests stand in the way of any further storage.

Chapter 3

Data protection officers of public bodies

Section 5

Designation

(1) Public bodies shall designate a data protection officer. This shall also apply to public bodies as defined in Section 2 (5) which take part in competition.

(2) A single data protection officer may be designated for several public bodies, taking account of their organizational structure and size.

(3) The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Section 7.

(4) The data protection officer may be a staff member of the public body, or fulfil the tasks on the basis of a service contract.

(5) The public body shall publish the contact details of the data protection officer and communicate them to the Federal Commissioner for Data Protection and Freedom of Information.

Section 6

Position

(1) The public body shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

(2) The public body shall support the data protection officer in performing the tasks referred to in Section 7 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

(3) The public body shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. The data protection officer shall directly report to the highest management level of the public body. The data protection officer shall not be dismissed or penalized by the public body for performing his or her tasks.

(4) The dismissal of the data protection officer shall be permitted only by applying Section 626 of the Civil Code accordingly. The data protection officer's employment shall not be terminated unless there are facts which give the public body just cause to terminate without notice. After the activity as data protection officer has ended, the data protection officer may not be terminated for a year following the end of appointment, unless the public body has just cause to terminate without notice.

(5) Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under Regulation (EU) 2016/679, this Act and other data protection legislation. The data protection officer shall be bound by secrecy concerning the

identity of data subjects and concerning circumstances enabling data subjects to be identified, unless they are released from this obligation by the data subject.

(6) Where in the course of their activities data protection officers become aware of data for which the head of a public body or a person employed by such a body has the right to refuse to give evidence for employment-related reasons, this right shall also apply to the data protection officer and his or her assistants. The person to whom the right to refuse to give evidence applies for employment-related reasons shall decide whether to exercise this right unless it is impossible to effect such a decision in the foreseeable future. Where the right of the data protection officer to refuse to give evidence applies, his or her files and other documents shall not be subject to seizure.

Section 7

Tasks

(1) In addition to the tasks listed in Regulation (EU) 2016/679, the data protection officer shall have at least the following tasks:

1. to inform and advise the public body and the employees who carry out processing of their obligations pursuant to this Act and other data protection legislation, including legislation enacted to implement Directive (EU) 2016/680;
2. to monitor compliance with this Act and other data protection legislation, including legislation enacted to implement Directive (EU) 2016/680, and with the policies of the public body in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
3. to provide advice as regards the data protection impact assessment and monitor its implementation pursuant to Section 67 of this Act;
4. to cooperate with the supervisory authority;
5. to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Section 69 of this Act, and to consult, where appropriate, with regard to any other matter.

In the case of a data protection officer ordered by a court, these tasks shall not refer to the action of the court acting in its judicial capacity.

(2) The data protection officer may perform other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

(3) The data protection officer shall in the performance of his or her tasks give due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Chapter 4

Federal Commissioner for Data Protection and Freedom of Information

Section 8

Establishment

(1) The Federal Commissioner for Data Protection and Freedom of Information (Federal Commissioner) shall be a supreme federal authority. It is located in Bonn.

(2) Civil servants of the Federal Commissioner shall be federal civil servants.

(3) The Federal Commissioner may delegate human resources administration and management tasks to other federal bodies as long as doing so does not affect the Federal Commissioner's independence. Personal data of staff members may be transmitted to these bodies as needed for them to perform their delegated tasks.

Section 9

Competence

(1) The Federal Commissioner shall be competent to supervise the public bodies of the Federation, also if they take part in competition as enterprises governed by public law, as well as businesses which process data of natural or legal persons for the commercial provision of telecommunications services, unless the responsibility for supervision is already indicated in Section 115 (4) of the Telecommunications Act. The provisions of this chapter shall also apply to processors if they are private bodies in which the Federation holds the absolute majority of shares or controls the absolute majority of votes and they process data on behalf of a public body of the Federation.

(2) The Federal Commissioner shall not be competent to supervise processing operations of federal courts acting in their judicial capacity.

Section 10

Independence

(1) The Federal Commissioner shall act with complete independence in performing his or her tasks and exercising his or her powers. The Federal Commissioner shall remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

(2) The Federal Commissioner shall be subject to audit by the Bundesrechnungshof as long as this does not affect his or her independence.

Section 11

Appointment and term of office

(1) At the proposal of the Federal Government, the German Bundestag shall elect without debate the Federal Commissioner with more than half of the statutory number of its members. The person elected shall be appointed by the Federal President. The Federal Commissioner must be at least 35 years old at the time of election. He or she shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform his or her duties and exercise his or her powers. In particular, the Federal Commissioner must have knowledge of data protection law acquired from the relevant professional experience and be qualified for judicial office or higher administrative service.

(2) The Federal Commissioner shall swear the following oath before the Federal President: "I swear to do everything in my power to further the good and the benefit of the German people, to protect them from harm and to defend the Basic Law and the laws of the Federation, to perform my duties conscientiously and to exercise justice in all my dealings, so help me God." The reference to God may be omitted from the oath.

(3) The Federal Commissioner's term of office shall be five years. It may be renewed once.

Section 12

Official relationship

(1) The Federal Commissioner shall, in accordance with this Act, have official federal status under public law.

(2) The official relationship shall begin upon delivery of the certificate of appointment. It shall end upon expiry of the term of office or upon resignation. The Federal President shall remove the Federal Commissioner from office at the request of the President of the Bundestag if the Federal Commissioner has committed serious misconduct or no longer meets the requirements for performing his or her tasks. If the official relationship is ended or the Federal Commissioner is

removed from office, the Federal Commissioner shall be given a document signed by the Federal President. Removal from office shall be effective upon delivery of this document. If the official relationship ends upon expiry of the term of office, at the request of the President of the Bundestag the Federal Commissioner shall be obligated to continue his or her work for no more than six months until a successor has been appointed.

(3) The senior civil servant shall exercise the rights of the Federal Commissioner if the latter is unable to perform his or her duties or if his or her term of office has expired and he or she is no longer obligated to continue his or her work. Section 10 (1) shall apply accordingly.

(4) From the start of the calendar month in which the official relationship commences until the end of the calendar month in which it ends, or, in the case of subsection 2, sixth sentence, until the end of the month in which he or she ceases his or her work, the Federal Commissioner shall be paid at the level of a federal civil servant in pay grade B 11 plus the family allowance according to Annex V of the Federal Civil Servants' Remuneration Act. The Federal Travel Expenses Act and the Federal Relocation Expenses Act shall apply accordingly. In all other respects, Section 12 (6), Sections 13 through 20 and 21a (5) of the Act on Federal Ministers shall apply, except that the four-year term of office stipulated in Section 15 (1) of the Act on Federal Ministers shall be replaced by a five-year term. By way of derogation from the third sentence in conjunction with Sections 15 through 17 and 21a (5) of the Act on Federal Ministers, the Federal Commissioner's pension shall be calculated, counting his or her term as Federal Commissioner as a pensionable period of service, on the basis of the Federal Act Governing Civil Servants' Pensions and Allowances, if this is more favourable and if, before his or election as Federal Commissioner, he or she was a civil servant or judge in at least the last position to be held before reaching pay grade B 11.

Section 13

Rights and obligations

(1) The Federal Commissioner shall refrain from any action incompatible with his or her duties and shall not, during his or her term of office, engage in any incompatible occupation, whether gainful or not. In particular, the Federal Commissioner shall not hold any other paid office or pursue any commercial activity or occupation in addition to his or her official duties and shall not belong to the management or supervisory board of a profit-oriented enterprise, nor to a government or legislative body of the Federation or a Land. The Federal Commissioner shall not deliver extra-judicial opinions in exchange for payment.

(2) The Federal Commissioner shall inform the President of the Bundestag of any gifts received in connection with his or her office. The President of the Bundestag shall decide how such gifts shall be used. He or she may issue procedural rules and regulations.

(3) The Federal Commissioner shall have the right to refuse to give testimony concerning persons who have confided in him or her in his or her capacity as Federal Commissioner and concerning the information confided. This shall also apply to the staff of the Federal Commissioner, on the condition that the Federal Commissioner decides on the exercise of this right. Within the scope of the Federal Commissioner's right of refusal to give testimony, he or she shall not be required to submit or surrender files or other documents.

(4) Even after his or her official relationship has ended, the Federal Commissioner shall be obligated to secrecy concerning matters of which he or she is aware by reason of his or her official duties. This obligation shall not apply to official communications or to matters which are common knowledge or which by their nature do not require confidentiality. The Federal Commissioner shall decide at his or her due discretion whether and to what extent he or she will testify in or outside court or make statements concerning such matters; if he or she is no longer in office, the permission of the Federal Commissioner in office shall be required. This shall not affect the legal obligation to report crimes and to uphold the free and democratic order wherever it is threatened. Sections 93, 97, 105 (1), Section 111 (5) in conjunction with Section 105 (1) and Section 116 (1) of the German Fiscal Code shall not apply to the Federal Commissioner or his or her staff. The fifth sentence shall not apply where the financial authorities require such knowledge in order to conduct legal proceedings due to a tax offence and related tax proceedings, in the prosecution of which there is compelling public interest, or where the person required to provide information or persons acting on his or her behalf have intentionally provided false information. If the Federal Commissioner determines that data protection provisions have been violated, he or she shall be authorized to report the violation and inform the data subject accordingly.

(5) The Federal Commissioner may testify as a witness unless such testimony would

1. be detrimental to the welfare of the Federation or a Land, in particular to the security of the Federal Republic of Germany or its relations with other countries, or
2. would violate fundamental rights.

If the testimony concerns ongoing or completed processes which are or could be considered core aspects of executive responsibility, the Federal Commissioner may testify only with the approval of the Federal Government. Section 28 of the Federal Constitutional Court Act shall remain unaffected.

(6) Subsections 3 and 4, fifth to seventh sentences, shall apply accordingly to the public bodies responsible for monitoring compliance with the data protection provisions in the Länder.

Section 14

Tasks

(1) In addition to the tasks listed in Regulation (EU) 2016/679, the Federal Commissioner shall have the following tasks:

1. to monitor and enforce the application of this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680;
2. to promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data, paying special attention to measures specifically for children;
3. to advise the German Bundestag, the Bundesrat, the Federal Government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data;
4. to promote the awareness of controllers and processors of their obligations under this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680;
5. upon request, to provide information to any data subject concerning the exercise of their rights under this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680, and if appropriate, to cooperate with the supervisory authorities in other Member States to that end;
6. to handle complaints lodged by a data subject, or by a body, organization or association in accordance with Article 55 of Directive (EU) 2016/680, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;
7. to cooperate with, including by sharing information, and provide mutual assistance to other supervisory authorities, to ensure the consistency of application and enforcement of this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680;

8. to conduct investigations on the application of this Act and other data protection legislation, including legislation adopted to implement Directive (EU) 2016/680, also on the basis of information received from another supervisory authority or other public authority;
9. to monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;
10. to provide advice on the processing operations referred to in Section 69; and
11. to contribute to the activities of the European Data Protection Board.

Within the scope of Directive (EU) 2016/680, the Federal Commissioner shall also perform the task pursuant to Section 60.

(2) To carry out the task listed in subsection 1, first sentence, no. 3, the Federal Commissioner may, on request or at its own initiative, make recommendations to the German Bundestag or one of its committees, the Bundesrat, the Federal Government, other institutions and bodies and the public concerning all matters related to the protection of personal data. At the request of the German Bundestag, one of its committees or of the Federal Government, the Federal Commissioner shall also investigate data protection matters and incidents at public bodies of the Federation.

(3) The Federal Commissioner shall facilitate the submission of complaints referred to in subsection 1, first sentence, no. 6 by measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(4) The performance of the duties of the Federal Commissioner shall be free of charge for the data subject. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the Federal Commissioner may charge a reasonable fee based on administrative costs, or refuse to act on the request. The Federal Commissioner shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Section 15

Activity reports

The Federal Commissioner shall produce an annual activity report which may contain a list of the types of violations reported and the types of measures taken, including penalties and measures taken in accordance with Article 58 (2) of Regulation (EU) 2016/679. The Federal Commissioner shall submit

this report to the German Bundestag, the Bundesrat and the Federal Government and shall make it available to the public, the European Commission and the European Data Protection Board.

Section 16

Powers

(1) The Federal Commissioner shall have, within the scope of Regulation (EU) 2016/679, the powers referred to in Article 58 of Regulation (EU) 2016/679. If the Federal Commissioner concludes that data protection legislation has been violated or that there are other problems with the processing of personal data, he or she shall inform the competent authority for legal or technical matters and, before exercising the powers referred to in Article 58 (2) (b) to (g), (i) and (j) of Regulation (EU) 2016/679, shall give this authority the opportunity to provide its opinion to the controller within a reasonable period. The opportunity to provide an opinion may be dispensed with if an immediate decision seems necessary due to imminent danger or in the public interest, or if it would conflict with compelling public interests. The opinion should also include a description of the measures taken on the basis of the information from the Federal Commissioner.

(2) If the Federal Commissioner finds that, in data processing for purposes beyond the scope of Regulation (EU) 2016/679, public bodies of the Federation have violated this Act or other data protection legislation or there are other insufficiencies with their processing or use of personal data, the Federal Commissioner shall lodge a complaint with the competent supreme federal authority and shall require this authority to respond within a period to be determined by the Federal Commissioner. The Federal Commissioner may dispense with a complaint or a response, especially if the problems involved are insignificant or have been remedied in the meantime. The response should also describe the measures taken as a result of the Federal Commissioner's complaint. The Federal Commissioner may also warn a controller that intended processing operations are likely to violate provisions of this Act and other data protection provisions which apply to the data processing in question.

(3) The powers of the Federal Commissioner shall also extend to

1. personal data obtained by bodies of the Federation subject to the Federal Commissioner's supervision concerning the contents of and specific circumstances relating to postal communications and telecommunications, and
2. personal data subject to professional or special official secrecy, especially tax secrecy under Section 30 of the German Fiscal Code.

The fundamental right to privacy of correspondence, posts and telecommunications in Article 10 of the Basic Law shall be limited accordingly.

(4) The public bodies of the Federation shall be obligated to provide the Federal Commissioner and his or her assistants with the following:

1. access to all official premises at all times, including to any data processing equipment and means, and to all personal data and all information necessary to perform their tasks; and
2. all information necessary to perform their tasks.

The obligation of the first sentence, no. 1 shall apply to private bodies only during their usual hours of operation and business.

(5) The Federal Commissioner shall work to cooperate with the public bodies responsible for monitoring compliance with data protection provisions in the Länder and with the supervisory authorities under Section 40. Section 40 (3), first sentence, second half-sentence, shall apply accordingly.

Chapter 5

Representation on the European Data Protection Board, single contact point, cooperation among the federal supervisory authorities and those of the Länder concerning European Union matters

Section 17

Representation on the European Data Protection Board, single contact point

(1) The Federal Commissioner shall serve as the joint representative on the European Data Protection Board and single contact point (joint representative). The Bundesrat shall elect the head of the supervisory authority of a Land to serve as the joint representative's deputy (deputy). The term shall be five years. When the head of the supervisory authority of a Land leaves office, his or her function as deputy shall end at the same time. The deputy may be re-elected.

(2) At the deputy's request, the joint representative shall delegate to him or her the leadership of negotiations and the voting right in the European Data Protection Board in matters dealing with the performance of a task for which the Länder alone have the right to legislate, or which affect the establishment or procedures of Land authorities.

Section 18

Procedures for cooperation among the federal and Länder supervisory authorities

(1) The Federal Commissioner and the supervisory authorities of the Länder (supervisory authorities of the Federation and the Länder) shall work together in European Union matters with the aim of consistently applying Regulation (EU) 2016/679 and Directive (EU) 2016/680. Before submitting a common position to the supervisory authorities of the other Member States, the European Commission or the European Data Protection Board, the supervisory authorities of the Federation and the Länder shall give each other the opportunity to comment at an early stage. For this purpose, they shall share all relevant information. The supervisory authorities of the Federation and the Länder shall consult the specific supervisory authorities established under Articles 85 and 91 of Regulation (EU) 2016/679 if these authorities are affected by the matter.

(2) If the supervisory authorities of the Federation and the Länder fail to achieve agreement on a common position, the lead supervisory authority, or, in the absence of a lead authority, the joint representative and his or her deputy, shall present a recommendation for a common position. If the joint representative and his or her deputy fail to agree on a recommendation for a common position, the deputy shall determine the recommendation for a common position in matters dealing with the performance of a task for which the Länder alone have the right to legislate, or which affect the establishment or procedures of Land authorities. For matters other than those referred to in the second sentence in which the joint representative and deputy fail to agree, the joint representative shall determine the common position. The negotiations shall be based on the position recommended pursuant to the first to third sentences unless the supervisory authorities of the Federation and the Länder adopt a different position with a simple majority. The Federation and each Land each have one vote. Abstentions shall not be counted.

(3) The joint representative and his or her deputy shall be bound by the common position pursuant to subsections 1 and 2 and shall determine by mutual agreement the conduct of negotiations according to this common position. Should they fail to reach agreement, the deputy shall decide the further conduct of negotiations for the matters referred to in Section 18 (2), second sentence. For other matters, the joint representative shall have the deciding vote.

Section 19

Responsibilities

(1) The lead supervisory authority of a Land in the one-stop-shop mechanism pursuant to Chapter VII of Regulation (EU) 2016/679 shall be the supervisory authority of the Land in which the controller or processor has its main establishment, as referred to in Article 4 no. 16 of Regulation (EU) 2016/679 or its single establishment in the European Union, as referred to in Article 56 (1) of Regulation (EU)

2016/679. Article 56 (1) in conjunction with Article 4 no. 16 of Regulation (EU) 2016/679 shall apply accordingly within the Federal Commissioner's area of responsibility. If there is no agreement on determining the lead supervisory authority, the procedure described in Section 18 (2) shall be applied accordingly.

(2) The supervisory authority with which a data subject has lodged a complaint shall forward the complaint to the lead supervisory authority referred to in subsection 1; in the absence of such a lead supervisory authority, the complaint shall be forwarded to the supervisory authority of a Land in which the controller or processor has an establishment. If a complaint is lodged with a supervisory authority which is not responsible for the matter, this authority shall forward the complaint to the supervisory authority where the applicant resides, if it is not possible to forward the complaint as referred to in the first sentence. The receiving supervisory authority shall be regarded as the supervisory authority according to Chapter VII of Regulation (EU) 2016/679 with whom the complaint was lodged, and shall fulfil the obligations referred to in Article 60 (7) to (9) and Article 65 (6) of Regulation (EU) 2016/679. Within the Federal Commissioner's area of responsibility, the supervisory authority which received a complaint shall forward it to the Federal Commissioner, if it is not possible to forward the complaint as referred to in subsection 1.

Chapter 6

Legal remedies

Section 20

Judicial remedy

(1) Recourse to the administrative courts shall be provided for disputes between natural or legal persons and a supervisory authority of the Federation or a Land concerning rights according to Article 78 (1) and (2) of Regulation (EU) 2016/679 and Section 61. The first sentence shall not apply to administrative fine proceedings.

(2) The Code of Administrative Court Procedure shall be applied in compliance with subsections 3 to 7.

(3) For proceedings pursuant to subsection 1, first sentence, the administrative court in whose district the supervisory authority is located shall be locally competent.

(4) In proceedings pursuant to subsection 1, first sentence, the supervisory authority shall be competent to take part.

(5) Parties to proceedings pursuant to subsection 1, first sentence, shall be

1. the natural or legal person as plaintiff or applicant, and
2. the supervisory authority as defendant or respondent.

Section 63 nos. 3 and 4 of the Code of Administrative Court Procedure shall remain unaffected.

(6) No preliminary proceedings shall take place.

(7) With respect to an authority or its legal entity, the supervisory authority shall not order immediate execution in accordance with Section 80 (2), first sentence, no. 4 of the Code of **Administrative Court Procedure**.

Section 21

Application of the supervisory authority for a court decision if it believes that an adequacy decision by the European Commission violates the law

(1) If a supervisory authority believes that an adequacy decision of the European Commission or a decision on the recognition of standard protection clauses or on the general validity of approved codes of conduct, on the validity of which a decision of the supervisory authority depends, violates the law, the supervisory authority shall suspend its procedure and lodge an application for a court decision.

(2) Recourse to the administrative courts shall be provided for proceedings pursuant to subsection 1. The Code of Administrative Court Procedure shall be applied in compliance with subsections 3 to 6.

(3) The Federal Administrative Court shall decide in the first and last instance on an application by the supervisory authority pursuant to subsection 1.

(4) In proceedings pursuant to subsection 1, the supervisory authority shall be competent to take part. The supervisory authority shall be a party to proceedings pursuant to subsection 1 as applicant; Section 63 nos. 3 and 4 of the Code of Administrative Court Procedure shall remain unaffected. The Federal Administrative Court may give the European Commission the opportunity to comment within a period of time to be determined.

(5) If a proceeding to review the validity of a European Commission decision pursuant to subsection 1 is pending at the European Court of Justice, the Federal Administrative Court may order its proceeding to be suspended until the proceeding at the European Court of Justice has been concluded.

(6) In proceedings pursuant to subsection 1, Section 47 (5), first sentence and (6) of the Code of Administrative Court Procedure shall apply accordingly. If the Federal Administrative Court finds

that the European Commission's decision pursuant to subsection 1 is valid, it shall state this in its decision. Otherwise it shall refer the question as to the validity of the decision in accordance with Article 267 of the Treaty on the Functioning of the European Union to the European Court of Justice.

Part 2

Implementing provisions for processing for purposes in accordance with Article 2 of Regulation (EU) 2016/679

Chapter 1

Legal basis for processing personal data

Sub-chapter 1

Processing of special categories of personal data and processing for other purposes

Section 22

Processing of special categories of personal data

(1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted

1. by public and private bodies if

a) processing is necessary to exercise the rights derived from the right of social security and social protection and to meet the related obligations;

b) processing is necessary for the purposes of preventive medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to the data subject's contract with a health professional and if these data are processed by health professionals or other persons subject to the obligation of professional secrecy or under their supervision;

c) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices; in addition to the measures referred to in subsection 2, in particular occupational and criminal law provisions to ensure professional secrecy shall be complied with; or

d) processing is urgently necessary for reasons of substantial public interest;

2. by public bodies if

- a) processing is necessary to prevent a substantial threat to public security;
- b) processing is urgently necessary to prevent substantial harm to the common good or to safeguard substantial concerns of the common good; or
- c) processing is necessary for urgent reasons of defence or to fulfil supra- or intergovernmental obligations of a public body of the Federation in the field of crisis management or conflict prevention or for humanitarian measures;

and as far as the interests of the controller in data processing in the cases of no. 1 (d) and no. 2 outweigh the interests of the data subject.

(2) In the cases of subsection 1, appropriate and specific measures shall be taken to safeguard the interests of the data subject. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, these measures may include in particular the following:

1. technical organizational measures to ensure that processing complies with Regulation (EU) 2016/679;
2. measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed;
3. measures to increase awareness of staff involved in processing operations;
4. designation of a data protection officer;
5. restrictions on access to personal data within the controller and by processors;
6. the pseudonymization of personal data;
7. the encryption of personal data;
8. measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident;
9. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;
10. specific rules of procedure to ensure compliance with this Act and with Regulation (EU) 2016/679 in the event of transfer or processing for other purposes.

Section 23

Processing for other purposes by public bodies

(1) Public bodies shall be permitted to process personal data for a purpose other than the one for which the data were collected where such processing is necessary for them to perform their duties and if

1. it is obviously in the interest of the data subject and there is no reason to assume that the data subject would refuse consent if he or she were aware of the other purpose;
2. it is necessary to check information provided by the data subject because there is reason to believe that this information is incorrect;
3. processing is necessary to prevent substantial harm to the common good or a threat to public security, defence or national security; to safeguard substantial concerns of the common good; or to ensure tax and customs revenues;
4. processing is necessary to prosecute criminal or administrative offences, to carry out or enforce punishment or measures as referred to in Section 11 (1) no. 8 of the Criminal Code or educational or disciplinary measures as referred to in the Juvenile Court Act or to enforce fines;
5. processing is necessary to prevent serious harm to the rights of another person; or
6. processing is necessary to exercise powers of supervision and monitoring, to conduct audits or organizational analyses of the controller; this shall also apply to processing for training and examination purposes by the controller, as long as it does not conflict with the legitimate interests of the data subject.

(2) The processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 for a purpose other than the one for which the data were collected shall be permitted if the conditions of subsection 1 are met and an exception pursuant to Article 9 (2) of Regulation (EU) 2016/679 or pursuant to Section 22 applies.

Section 24

Processing for other purposes by private bodies

(1) Private bodies shall be permitted to process personal data for a purpose other than the one for which the data were collected if

1. processing is necessary to prevent threats to state or public security or to prosecute criminal offences; or

2. processing is necessary for the establishment, exercise or defence of legal claims, unless the data subject has an overriding interest in not having the data processed.

(2) The processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 for a purpose other than the one for which the data were collected shall be permitted if the conditions of subsection 1 are met and an exception pursuant to Article 9 (2) of Regulation (EU) 2016/679 or pursuant to Section 22 applies.

Section 25

Transfer of data by public bodies

(1) The transfer of personal data by public bodies to public bodies shall be permitted if it is necessary for the transferring body or the third party to whom the data are transferred to perform their duties and the conditions are met which would permit processing pursuant to Section 23. The third party to whom the data are transferred shall process the transferred data only for the purpose for which they were transferred. Processing for other purposes shall be permitted only if the conditions of Section 23 are met.

(2) Public bodies shall be permitted to transfer personal data to private bodies if

1. transfer is necessary for the transferring body to perform its duties and the conditions are met which would permit processing pursuant to Section 23;

2. the third party to whom the data are transferred credibly presents a legitimate interest in knowledge of the data to be transferred and the data subject does not have a legitimate interest in not having the data transferred; or

3. processing is necessary for the establishment, exercise or defence of legal claims;

and the third party has promised the public body transferring the data that it will process them only for the purpose for which they were transferred. Processing for other purposes shall be permitted if transfer pursuant to the first sentence would be permitted and the transferring body has consented to the transfer.

(3) The transfer of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted if the conditions of subsection 1 or 2 are met and an exception pursuant to Article 9 (2) of Regulation (EU) 2016/679 or pursuant to Section 22 applies.

Sub-chapter 2

Special processing situations

Section 26

Data processing for employment-related purposes

(1) Personal data of employees may be processed for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract or to exercise or satisfy rights and obligations of employees' representation laid down by law or by collective agreements or other agreements between the employer and staff council. Employees' personal data may be processed to detect crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the processing of such data is necessary to investigate the crime and is not outweighed by the data subject's legitimate interest in not processing the data, and in particular the type and extent are not disproportionate to the reason.

(2) If personal data of employees are processed on the basis of consent, then the employee's level of dependence in the employment relationship and the circumstances under which consent was given shall be taken into account in assessing whether such consent was freely given. Consent may be freely given in particular if it is associated with a legal or economic advantage for the employee, or if the employer and employee are pursuing the same interests. Consent shall be given in written or electronic form, unless a different form is appropriate because of special circumstances. The employer shall inform the employee in text form of the purpose of data processing and of the employee's right to withdraw consent pursuant to Article 7 (3) of Regulation (EU) 2016/679.

(3) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 for employment-related purposes shall be permitted if it is necessary to exercise rights or comply with legal obligations derived from labour law, social security and social protection law, and there is no reason to believe that the data subject has an overriding legitimate interest in not processing the data. Subsection 2 shall also apply to consent to the processing of special categories of personal data; consent must explicitly refer to these data. Section 22 (2) shall apply accordingly.

(4) The processing of personal data, including special categories of personal data of employees for employment-related purposes, shall be permitted on the basis of collective agreements. The negotiating partners shall comply with Article 88 (2) of Regulation (EU) 2016/679.

(5) The controller must take appropriate measures to ensure compliance in particular with the principles for processing personal data described in Article 5 of Regulation (EU) 2016/679.

(6) The rights of participation of staff councils shall remain unaffected.

(7) Subsections 1 to 6 shall also apply when personal data, including special categories of personal data, of employees are processed without forming or being intended to form part of a filing system.

(8) For the purposes of this Act, employees are

1. dependently employed workers, including temporary workers contracted to the borrowing employer;

2. persons employed for occupational training purposes;

3. participants in benefits to take part in working life, in assessments of occupational aptitude or work trials (persons undergoing rehabilitation);

4. persons employed in accredited workshops for persons with disabilities;

5. volunteers working pursuant to the Youth Volunteer Service Act or the Federal Volunteer Service Act;

6. persons who should be regarded as equivalent to dependently employed workers because of their economic dependence; these include persons working at home and their equivalents;

7. federal civil servants, federal judges, military personnel and persons in the alternative civilian service.

Applicants for employment and persons whose employment has been terminated shall be regarded as employees.

Section 27

Data processing for purposes of scientific or historical research and for statistical purposes

(1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted also without consent for scientific or historical research purposes or statistical purposes, if such processing is necessary for these purposes and the interests of the controller in processing substantially outweigh those of the data subject in not processing the data. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2), second sentence.

(2) The rights of data subjects provided in Articles 15, 16, 18 and 21 of Regulation (EU) 2016/679 shall be limited to the extent that these rights are likely to render impossible or seriously impair the achievement of the research or statistical purposes, and such limits are necessary for the fulfilment of the research or statistical purposes. Further, the right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply if the data are necessary for purposes of scientific research and the provision of information would involve disproportionate effort.

(3) In addition to the measures listed in Section 22 (2), special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 processed for scientific or historical research purposes or statistical purposes shall be rendered anonymous as soon as the research or statistical purpose allows, unless this conflicts with legitimate interests of the data subject. Until such time, the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be stored separately. They may be combined with the information only to the extent required by the research or statistical purpose.

(4) The controller may publish personal data only if the data subject has provided consent or if doing so is indispensable for the presentation of research findings on contemporary events.

Section 28

Data processing for archiving purposes in the public interest

(1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted if necessary for archiving purposes in the public interest. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2), second sentence.

(2) The right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply if the archival material is not identified with the person's name or no information is given which would enable the archival material to be found with reasonable administrative effort.

(3) The right of the data subject to rectification according to Article 16 of Regulation (EU) 2016/679 shall not apply if the personal data are processed for archiving purposes in the public interest. If the data subject disputes the accuracy of the personal data, he or she shall have the opportunity to present his or her version. The responsible archive shall be obligated to add this version to the files.

(4) The rights provided in Article 18 (1) (a), (b) and (d) and in Articles 20 and 21 of Regulation (EU) 2016/679 shall not apply as far as these rights are likely to render impossible or seriously impair the

achievement of the archiving purposes in the public interest, and the exceptions are necessary to fulfil those purposes.

Section 29

Rights of the data subject and powers of the supervisory authorities in the case of secrecy obligations

(1) In addition to the exceptions in Article 14 (5) of Regulation (EU) 2016/679, the obligation to provide information to the data subject according to Article 14 (1) to (4) of Regulation (EU) 2016/679 shall not apply as far as meeting this obligation would disclose information which by its nature must be kept secret, in particular because of overriding legitimate interests of a third party. The right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply as far as access would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party. In addition to the exception in Article 34 (3) of Regulation (EU) 2016/679, the obligation to inform the data subject of a personal data breach according to Article 34 of Regulation (EU) 2016/679 shall not apply as far as meeting this obligation would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party. By derogation from the exception pursuant to the third sentence, the data subject pursuant to Article 34 of Regulation (EU) 2016/679 shall be informed if the interests of the data subject outweigh the interest in secrecy, in particular taking into account the threat of damage.

(2) If in the context of a client-lawyer relationship the data of third persons are transferred to persons subject to a legal obligation of professional secrecy, the transferring body shall not be obligated to inform the data subject according to Article 13 (3) of Regulation (EU) 2016/679 unless the data subject has an overriding interest in being informed.

(3) The supervisory authorities shall not have the investigative powers according to Article 58 (1) (e) and (f) of Regulation (EU) 2016/679 with regard to the persons listed in Section 203 (1), (2a) and (3) of the Criminal Code or their processors as far as exercising these powers would violate these persons' obligations to secrecy. If in the context of an investigation a supervisory authority becomes aware of data subject to an obligation of secrecy as referred to in the first sentence, the obligation of secrecy shall also apply to the supervisory authority.

Section 30

Consumer loans

(1) Any body which for the purpose of transfer commercially collects, stores or modifies personal data which may be used to evaluate the creditworthiness of consumers shall treat requests for information from lenders in other European Union Member States the same way it treats information requests from domestic lenders.

(2) Anyone who refuses to conclude a consumer loan contract or a contract concerning financial assistance for payment with a consumer as the result of information provided by a body as referred to in subsection 1 shall immediately notify the consumer of this refusal and the information received. Such notification shall not be made if doing so would endanger public security or order. Section 37 shall remain unaffected.

Section 31

Protection of commercial transactions in the case of scoring and credit reports

(1) For the purpose of deciding on the creation, execution or termination of a contractual relationship with a natural person, the use of a probability value for certain future action by this person (scoring) shall be permitted only if

1. the provisions of data protection law have been followed;
2. the data used to calculate the probability value are demonstrably essential for calculating the probability of the action on the basis of a scientifically recognized mathematic-statistical procedure;
3. other data in addition to address data are used to calculate the probability value; and
4. if address data are used, the data subject was notified ahead of time of the planned use of these data; this notification shall be documented.

(2) The use of a probability value calculated by credit reporting agencies to determine a natural person's ability and willingness to pay shall be permitted in the case of including information on claims only as far as the conditions of subsection 1 are met and only claims concerning a performance owed which has not been rendered on time are considered

1. which have been established by a final decision or a decision declared enforceable for the time being, or if an executory title has been issued under Section 794 of the Code of Civil Procedures,
2. which have been established under Section 178 of the Insolvency Act and have not been disputed by the debtor at the verification meeting,
3. which the debtor has explicitly acknowledged,

4. for which

- a) the debtor has received at least two written reminders after the due date of the claim,
- b) at least four weeks have elapsed since the first reminder,
- c) the debtor was previously informed, at least in the first reminder, of possible consideration by a credit reporting agency and
- d) the debtor has not disputed the claim, or

5. the contractual relationship on which the claim is based can be terminated without prior notice for payment in arrears and the debtor has been informed of possible consideration by a credit reporting agency.

The lawfulness of processing, including the calculation of probability values, other data relevant for credit reports pursuant to general data protection law shall remain unaffected.

Chapter 2

Rights of the data subject

Section 32

Information to be provided where personal data are collected from the data subject

(1) In addition to the exception in Article 13 (4) of Regulation (EU) 2016/679, the obligation to provide information to the data subject according to Article 13 (3) of Regulation (EU) 2016/679 shall not apply if providing information about the planned further use

1. concerns the further processing of data stored in analogue form, for which the controller directly contacts the data subject through the further processing; the purpose is compatible with the original purpose for which the data were collected in accordance with Regulation (EU) 2016/679; the communication with the data subject does not take place in digital form; and the interest of the data subject in receiving the information can be regarded as minimal, given the circumstances of the individual case, in particular with regard to the context in which the data were collected;

2. would, in the case of a public body, endanger the proper performance of tasks as referred to in Article 23 (1) (a) to (e) of Regulation (EU) 2016/679 for which the controller is responsible, and the controller's interests in not providing the information outweigh the interests of the data subject;

3. would endanger public security or order or would otherwise be detrimental to the welfare of the Federation or a Land, and the controller's interests in not providing the information outweigh the interests of the data subject;

4. would interfere with the establishment, exercise or defence of legal claims, and the controller's interests in not providing the information outweigh the interests of the data subject; or

5. would endanger a confidential transfer of data to public bodies.

(2) If information is not provided to the data subject pursuant to subsection 1, the controller shall take appropriate measures to protect the legitimate interests of the data subject, including providing the information referred to in Article 13 (1) and (2) of Regulation (EU) 2016/679 for the public in precise, transparent, understandable and easily accessible form in clear and simple language. The controller shall set down in writing the reasons for not providing information. The first and second sentences shall not apply in the cases of subsection 1 nos. 4 and 5.

(3) If notification is not provided in the cases of subsection 1 because of a temporary obstacle, the controller shall meet the obligation to provide information, while taking into account the specific circumstances of processing, within an appropriate period after the obstacle has ceased to exist, but no later than two weeks.

Section 33

Information to be provided where personal data have not been obtained from the data subject

(1) In addition to the exception in Article 14 (5) of Regulation (EU) 2016/679 and in Section 29 (1), first sentence, the obligation to provide information to the data subject according to Article 14 (1), (2) and (4) of Regulation (EU) 2016/679 shall not apply if providing information

1. in the case of a public body

a) would endanger the proper performance of tasks as referred to in Article 23 (1) (a) to (e) of Regulation (EU) 2016/679 for which the controller is responsible, or

b) would threaten the public security or order or otherwise be detrimental to the Federation or a Land, and therefore the data subject's interest in receiving the information must not take precedence;

2. in the case of a private body

a) would interfere with the establishment, exercise or defence of legal claims, or processing includes data from contracts under private law and is intended to prevent harm from criminal offences, unless the data subject has an overriding legitimate interest in receiving the information; or

b) the responsible public body has determined with respect to the controller that disclosing the data would endanger public security or order or would otherwise be detrimental to the welfare of the Federation or a Land; in the case of data processing for purposes of law enforcement, no determination pursuant to the first half-sentence shall be required.

(2) If information is not provided to the data subject pursuant to subsection 1, the controller shall take appropriate measures to protect the legitimate interests of the data subject, including providing the information referred to in Article 14 (1) and (2) of Regulation (EU) 2016/679 for the public in precise, transparent, understandable and easily accessible form in clear and simple language. The controller shall set down in writing the reasons for not providing information.

(3) If the provision of information relates to the transfer by public bodies of personal data to the authorities for the protection of the Constitution, the Federal Intelligence Service, the Military Counterintelligence Service and, as far as the security of the Federation is affected, other authorities of the Federal Ministry of Defence, such provision shall be permitted only with the approval of these bodies.

Section 34

Right of access by the data subject

(1) In addition to the exceptions in Section 27 (2), 28 (2) and 29 (1), second sentence, the data subject's right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply if

1. the data subject shall not be informed pursuant to Section 33 (1) no. 1, no. 2 (b) or (3), or

2. the data

a) were recorded only because they may not be erased due to legal or statutory provisions on retention, or

b) only serve purposes of monitoring data protection or safeguarding data,

and providing information would require a disproportionate effort, and appropriate technical and organizational measures make processing for other purposes impossible.

(2) The reasons for the refusal to provide information shall be documented. The data subject shall be informed of the reasons for refusing to provide information, unless providing the reasons in law and

in fact on which the decision is based would undermine the intended purpose of refusing to provide the information. Data stored for the purpose of providing information to the data subject and preparing such provision may be processed only for this purpose and for purposes of data protection monitoring; processing for other purposes shall be restricted according to Article 18 of Regulation (EU) 2016/679.

(3) If a public body of the Federation does not provide information to a data subject, such information shall be provided to the Federal Commissioner at the request of the data subject, unless the responsible supreme federal authority determines in the individual case that doing so would endanger the security of the Federation or a Land. The notification from the Federal Commissioner to the data subject with the results of the data protection assessment shall not permit any conclusions to be drawn concerning the information held by the controller unless the latter agrees to the provision of more extensive information.

(4) The data subject shall have the right to information about personal data processed by a public body neither in automated nor in non-automated form and stored in a filing system only if the data subject provides information enabling the data to be located and if the effort required is not disproportionate to the data subject's interest in the information.

Section 35

Right to erasure

(1) If in the case of non-automated data processing erasure would be impossible or would involve a disproportionate effort due to the specific mode of storage and if the data subject's interest in erasure can be regarded as minimal, the data subject shall not have the right to erasure and the controller shall not be obligated to erase personal data in accordance with Article 17 (1) of Regulation (EU) 2016/679 in addition to the exceptions given in Article 17 (3) of Regulation (EU) 2016/679. In this case, restriction of processing in accordance with Article 18 of Regulation (EU) 2016/679 shall apply in place of erasure. The first and second sentences shall not apply if the personal data were processed unlawfully.

(2) In addition to Article 18 (1) (b) and (c) of Regulation (EU) 2016/679, subsection 1, first and second sentences shall apply accordingly in the case of Article 17 (1) (a) and (d) of Regulation (EU) 2016/679 as long and as far as the controller has reason to believe that erasure would adversely affect legitimate interests of the data subject. The controller shall inform the data subject of the restriction of processing if doing so is not impossible or would not involve a disproportionate effort.

(3) In addition to Article 17 (3) (b) of Regulation (EU) 2016/679, subsection 1 shall apply accordingly in the case of Article 17 (1) (a) of Regulation (EU) 2016/679 if erasure would conflict with retention periods set by statute or contract.

Section 36

Right to object

The right to object according to Article 21 (1) of Regulation (EU) 2016/679 with regard to a public body shall not apply if there is an urgent public interest in the processing which outweighs the interests of the data subject or if processing is required by law.

Section 37

Automated individual decision-making, including profiling

(1) In addition to the exceptions given in Article 22 (2) (a) and (c) of Regulation (EU) 2016/679, the right according to Article 22 (1) of Regulation (EU) 2016/679 not to be subject to a decision based solely on automated processing shall not apply if the decision is made in the context of providing services pursuant to an insurance contract and

1. the request of the data subject was fulfilled, or
2. the decision is based on the application of binding rules of remuneration for therapeutic treatment and the controller takes suitable measures, in the event that the request is not granted in full, to safeguard the data subject's legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision; the controller shall inform the data subject of these rights no later than the notification indicating that the data subject's request will not be granted in full.

(2) Decisions pursuant to subsection 1 may be based on the processing of health data as referred to in Article 4 no. 15 of Regulation (EU) 2016/679. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2), second sentence.

Chapter 3

Obligations of controllers and processors

Section 38

Data protection officers of private bodies

(1) In addition to Article 37 (1) (b) and (c) of Regulation (EU) 2016/679, the controller and processor shall designate a data protection officer if they constantly employ as a rule at least 20 persons dealing with the automated processing of personal data. If the controller or processor undertake processing subject to a data protection impact assessment pursuant to Article 35 of Regulation (EU) 2016/679, or if they commercially process personal data for the purpose of transfer, of anonymized transfer or for purposes of market or opinion research, they shall designate a data protection officer regardless of the number of persons employed in processing.

(2) Section 6 (4), (5), second sentence, and (6) shall apply, Section 6 (4) however shall apply only if designating a data protection officer is mandatory.

Section 39

Accreditation

The power to act as a certification body in accordance with Article 43 (1), first sentence of Regulation (EU) 2016/679 shall be granted by the supervisory authority of the Federation or the Länder responsible for data protection supervision of the certification body on the basis of accreditation by the German accreditation body. Section 2 (3), second sentence, Section 4 (3) and Section 10 (1), first sentence, no. 3 of the Accreditation Body Act shall apply on the condition that data protection falls within the scope of Section 1 (2), second sentence.

Chapter 4

Supervisory authorities for data processing by private bodies

Section 40

Supervisory authorities of the Länder

(1) The authorities pursuant to Land law shall monitor the application by private bodies of data protection legislation within the scope of Regulation (EU) 2016/679.

(2) If the controller or processor has more than one establishment in Germany, Article 4 no. 16 of Regulation (EU) 2016/679 shall apply accordingly in determining which supervisory authority is competent. If more than one authority considers itself competent or not competent, or when the competence is unclear for other reasons, the supervisory authorities shall make a joint decision in accordance with Section 18 (2). Section 3 (3) and (4) of the Administrative Procedure Act shall apply accordingly.

(3) The supervisory authority may process the data it has stored only for purposes of supervision; to this end, it may transfer data to other supervisory authorities. Processing for another purpose shall be permitted in addition to Article 6 (4) of Regulation (EU) 2016/679 if

1. it is obviously in the interest of the data subject and there is no reason to assume that the data subject would refuse consent if he or she were aware of the other purpose;

2. processing is necessary to prevent substantial harm to the common good or a threat to public security or to safeguard substantial concerns of the common good; or

3. processing is necessary to prosecute crimes or administrative offences, to carry out or enforce punishment or measures as referred to in Section 11 (1) no. 8 of the Criminal Code or educational or disciplinary measures as referred to in the Juvenile Court Act or to enforce fines.

If the supervisory authority determines that data protection legislation has been violated, it shall have the power to inform the data subjects concerned, to report the violation to other bodies responsible for prosecution or punishment and, in the case of serious violations, to notify the trade supervisory authority to take measures under trade and industry law. Section 13 (4), fourth to seventh sentences shall apply accordingly.

(4) The bodies subject to monitoring and the persons responsible for their management shall provide a supervisory authority on request with the information necessary to perform their tasks. The person required to provide information may refuse to answer those questions which would expose him- or herself or a relative as referred to in Section 383 (1) nos. 1 to 3 of the Code of Civil Procedure to the risk of criminal prosecution or proceedings under the Administrative Offences Act. The person required to provide information shall be informed accordingly.

(5) Persons assigned by the supervisory authority to monitor compliance with data protection legislation shall be authorized, as needed to perform their tasks, to enter the property and premises of the body and to have access to all data processing equipment and means. The body shall be obligated to tolerate such access. Section 16 (4) shall apply accordingly.

(6) The supervisory authorities shall advise and support the data protection officers to meet their typical needs. They may demand the dismissal of a data protection officer if he or she does not have the expert knowledge needed to perform his or her tasks or if there is a serious conflict of interests as referred to in Article 38 (6) of Regulation (EU) 2016/679.

(7) The application of the Trade Regulation Code shall remain unaffected.

Chapter 5

Penalties

Section 41

Application of provisions concerning criminal proceedings and proceedings to impose administrative fines

(1) Unless this Act provides otherwise, the provisions of the Administrative Offences Act shall apply accordingly to violations pursuant to Article 83 (4) to (6) of Regulation (EU) 2016/679. Sections 17, 35 and 36 of the Administrative Offences Act shall not apply. Section 68 of the Administrative Offences Act shall apply on the condition that the regional court shall decide if the administrative fine exceeds the amount of one hundred thousand euros.

(2) Unless this Act provides otherwise, the provisions of the Administrative Offences Act and the general laws on criminal procedures, namely the Code of Criminal Procedure and the Judicature Act, shall apply accordingly in proceedings for violations pursuant to Article 83 (4) to (6) of Regulation (EU) 2016/679. Sections 56 to 58, 87, 88, 99 and 100 of the Administrative Offences Act shall not apply. Section 69 (4), second sentence of the Administrative Offences Act shall apply on the condition that the public prosecutor's office may stop the proceedings only with the approval of the supervisory authority which issued the administrative decision imposing a fine.

Section 42

Penal provisions

(1) The following actions done deliberately and without authorization with regard to the personal data of a large number of people which are not publicly accessible shall be punishable with imprisonment of up to three years or a fine:

1. transferring the data to a third party or
2. otherwise making them accessible

for commercial purposes.

(2) The following actions done with regard to personal data which are not publicly accessible shall be punishable with imprisonment of up to two years or a fine:

1. processing without authorization, or
2. fraudulently acquiring

and doing so in return for payment or with the intention of enriching oneself or someone else or harming someone.

(3) Such offences shall be prosecuted only if a complaint is filed. The data subject, the controller, the Federal Commissioner and the supervisory authority shall be entitled to file complaints.

(4) A notification pursuant to Article 33 of Regulation (EU) 2016/679 or a communication pursuant to Article 34 (1) of Regulation (EU) 2016/679 may be used in criminal proceedings against the person required to provide a notification or a communication or relatives as referred to in Section 52 (1) of the Code of Criminal Procedure only with the consent of the person required to provide a notification or a communication.

Section 43

Provisions on administrative fines

(1) Intentionally or negligently engaging in the following shall be deemed an administrative offence:

1. in violation of Section 30 (1) failing to treat a request for information properly, or
2. in violation of Section 30 (2), first sentence, failing to inform a consumer or doing so incorrectly, incompletely or too late.

(2) An administrative offence may be punished by a fine of up to fifty thousand euros.

(3) Authorities and other public bodies as referred to in Section 2 (1) shall not be subject to any administrative fines.

(4) A notification pursuant to Article 33 of Regulation (EU) 2016/679 or a communication pursuant to Article 34 (1) of Regulation (EU) 2016/679 may be used in proceedings pursuant to the Administrative Offences Act against the person required to provide a notification or a communication or relatives as referred to in Section 52 (1) of the Code of Criminal Procedure only with the consent of the person required to provide a notification or a communication.

Chapter 6

Legal remedies

Section 44

Proceedings against a controller or processor

(1) Proceedings against a controller or a processor for a violation of data protection law within the scope of Regulation (EU) 2016/679 or the rights of the data subject contained therein may be brought

by a data subject before the court in the place where the controller or processor has an establishment. Proceedings pursuant to the first sentence may also be brought before the court in the place where the data subject has his or her habitual residence.

(2) Subsection 1 shall not apply to proceedings against public authorities acting in the exercise of their sovereign powers.

(3) If the controller or processor has designated a representative pursuant to Article 27 (1) of Regulation (EU) 2016/679, this representative shall also be an authorized recipient in civil law proceedings pursuant to subsection 1. Section 184 of the Code of Civil Procedure shall remain unaffected.

Part 3

Implementing provisions for processing for purposes in accordance with Article 1 (1) of Directive (EU) 2016/680

Chapter 1

Scope, definitions and general principles for processing personal data

Section 45

Scope

The provisions of this Part shall apply to the processing of personal data by public bodies competent for the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal or administrative penalties, as far as they process data for the purpose of carrying out these tasks. The public bodies shall be regarded in that case as controllers. The prevention of criminal offences as referred to in the first sentence shall include protection against and prevention of threats to public security. The first and second sentences shall also apply to those public bodies responsible for executing penalties, measures as referred to in Section 11 (1) no. 8 of the Criminal Code, educational or disciplinary measures as referred to in the Juvenile Court Act or fines. As far as this Part contains provisions for processors, it shall also apply to them.

Section 46

Definitions

For the purposes of this Act

1. 'personal data' means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;
2. 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure or destruction;
3. 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;
4. 'profiling' means any form of automated processing of personal data involving the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
5. 'pseudonymization' means the processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data cannot be attributed to an identified or identifiable natural person;
6. 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
7. 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data;
8. 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
9. 'recipient' means a natural or legal person, public authority, agency or other body to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or other law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

10. 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data processed;
11. 'genetic data' means personal data, relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
12. 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person, in particular facial images or dactyloscopic data;
13. 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
14. 'special categories of personal data'
- a) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
 - b) genetic data;
 - c) biometric data for the purpose of uniquely identifying a natural person;
 - d) data concerning health; and
 - e) data concerning a natural person's sex life or sexual orientation;
15. 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 41 of Directive (EU) 2016/680;
16. 'international organization' means an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;
17. 'consent' means any freely given, specific, informed and unambiguous indication of the data subject's wishes in a particular case by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Section 47

General principles for processing personal data

Personal data shall be

1. processed lawfully and fairly;
2. collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
3. adequate, relevant and not excessive in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Chapter 2

Legal basis for processing personal data

Section 48

Processing of special categories of personal data

(1) The processing of special categories of personal data shall be allowed only where strictly necessary for the performance of the controller's tasks.

(2) If special categories of personal data are processed, appropriate safeguards for the legally protected interests of the data subject shall be implemented. Appropriate safeguards may be in particular

1. specific requirements for data security or data protection monitoring;
2. special time limits within which data must be reviewed for relevance and erasure;
3. measures to increase awareness of staff involved in processing operations;
4. restrictions on access to personal data within the controller;
5. separate processing of such data;
6. the pseudonymization of personal data;

7. the encryption of personal data; or
8. specific codes of conduct to ensure lawful processing in case of transfer or processing for other purposes.

Section 49

Processing for other purposes

Processing personal data for a purpose other than the one for which they were collected shall be permitted if the other purpose is one of the purposes listed in Section 45, the controller is authorized to process data for this purpose, and processing is necessary and proportionate to this purpose. Processing personal data for another purpose not listed in Section 45 shall be permitted if it is allowed by law.

Section 50

Processing for archiving, scientific and statistical purposes

Personal data may be processed in the context of purposes listed in Section 45 in archival, scientific or statistical form if doing so is in the public interest and appropriate safeguards for the legally protected interests of data subjects are implemented. Such safeguards may consist of rendering the personal data anonymous as quickly as possible, taking measures to prevent unauthorized disclosure to third parties, or in processing them organizationally and spatially separate from other tasks.

Section 51

Consent

- (1) If personal data may be processed by law on the basis of consent, the controller must be able to present evidence of the data subject's consent.
- (2) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.
- (3) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. The data subject shall be informed of this before giving consent.
- (4) Consent shall be effective only when based on the data subject's free decision. When assessing whether consent was freely given, the circumstances in which it was given must be taken into account.

The data subject shall be informed of the intended purpose of the processing. If necessary in the individual case or on request, the data subject shall also be informed of the consequences of withholding consent.

(5) If special categories of personal data are to be processed, the consent must explicitly refer to these data.

Section 52

Processing on instructions from the controller

Any person acting under the authority of the controller or of the processor who has access to personal data shall not process those data except on instructions from the controller, unless required to do so by law.

Section 53

Confidentiality

Persons employed in data processing shall not process personal data without authorization (confidentiality). They shall be obligated when taking up their duties to maintain confidentiality. The obligation of confidentiality shall continue after their employment ends.

Section 54

Automated individual decision

(1) A decision based solely on automated processing which produces an adverse legal effect concerning the data subject or significantly affects him or her shall be permitted only when authorized by law.

(2) Decisions referred to in subsection 1 shall not be based on special categories of personal data unless suitable measures to safeguard the data subject's legally protected and legitimate interests are in place.

(3) Profiling that results in discrimination against natural persons on the basis of special categories of personal data shall be prohibited.

Chapter 3

Rights of the data subject

Section 55

General information on data processing

The controller shall provide general and publicly accessible information on

1. the purposes of the processing,
2. the rights of data subjects with regard to the processing of their personal data to access, rectification, erasure and restriction of processing,
3. the names and contact details of the controller and the data protection officer,
4. the right to lodge a complaint with the Federal Commissioner, and
5. the contact details of the Federal Commissioner.

Section 56

Notification of data subjects

(1) If special legislation provides for or requires notifying data subjects of the processing of their personal data, especially in the case of undercover operations, such notification shall include at least the following information:

1. the information listed in Section 55;
2. the legal basis for the processing;
3. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
4. the categories of recipients of the personal data, if any;
5. where necessary, further information, in particular where the personal data were collected without the knowledge of the data subject.

(2) In the cases of subsection 1, the controller may postpone, limit or refrain from notification if and so long as

1. the performance of the tasks listed in Section 45,
2. public security, or
3. the legally protected interests of third parties

would otherwise be threatened, if the interest in avoiding these threats overrides the interest of the data subject in the information.

(3) If the notification relates to the transfer of personal data to the authorities for the protection of the Constitution, the Federal Intelligence Service, the Military Counterintelligence Service and, as far as

the security of the Federation is affected, other authorities of the Federal Ministry of Defence, such notification shall be permitted only with the approval of these bodies.

(4) Section 57 (7) shall apply accordingly in case of restriction pursuant to subsection 2.

Section 57

Right of access

(1) The controller shall inform data subjects on request whether data concerning them are being processed. Data subjects shall also have the right to information about

1. the personal data being processed and the categories to which they belong;
2. the available information on the origin of the data;
3. the purposes of and legal basis for the processing;
4. the recipients or categories of recipients to whom the data have been disclosed, in particular recipients in third countries or international organizations;
5. the period for which the data will be stored, or if that is not possible, the criteria used to determine that period;
6. the existence of the right to rectification or erasure of data or restriction of processing of data by the controller;
7. the right pursuant to Section 60 to lodge a complaint with the Federal Commissioner, and
8. the contact details of the Federal Commissioner.

(2) Subsection 1 shall not apply to personal data recorded only because they may not be erased due to legal or statutory provisions on retention, or only for purposes of monitoring data protection or safeguarding data, if providing information would require a disproportionate effort, and appropriate technical and organizational measures make processing for other purposes impossible.

(3) No information shall be provided if the data subject does not provide information enabling the data to be located and if the effort required is therefore disproportionate to the data subject's interest in the information.

(4) Subject to the conditions of Section 56 (2), the controller may dispense with the provision of information pursuant to subsection 1, first sentence, or restrict, wholly or partly, the provision of information pursuant to subsection 1, second sentence.

(5) If the information to be provided relates to the transfer of personal data to the authorities for the protection of the Constitution, the Federal Intelligence Service, the Military Counterintelligence Service and, as far as the security of the Federation is affected, other authorities of the Federal Ministry of Defence, such provision shall be permitted only with the approval of these bodies.

(6) The controller shall notify the data subject, without delay, in writing of any refusal or restriction of access. This shall not apply if providing this information would entail a threat as referred to in Section 56 (2). The notification pursuant to the first sentence shall include the reasons for the refusal or the restriction unless providing the reasons would undermine the intended purpose of the refusal or restriction of access.

(7) If the data subject is notified pursuant to subsection 6 of the refusal or restriction of access, he or she may exercise his or her right of access also via the Federal Commissioner. The controller shall inform the data subject of this possibility and that, in accordance with Section 60, the data subject may lodge a complaint with the Federal Commissioner or seek a judicial remedy. If the data subject exercises his or her right pursuant to the first sentence, the information shall be provided to the Federal Commissioner at the request of the data subject, unless the responsible supreme federal authority determines in the individual case that doing so would threaten the security of the Federation or a Land. The Federal Commissioner shall at least inform the data subject that all necessary checks have been conducted or that the Federal Commissioner has conducted a review. This notification may include information as to whether violations of data protection law were found. The notification from the Federal Commissioner to the data subject shall not permit any conclusions to be drawn concerning the information held by the controller unless the latter agrees to the provision of more extensive information. The controller may refuse to such provision only as far as and for as long as he or she could dispense with or restrict information pursuant to subsection 4. The Federal Commissioner shall also inform the data subject of his or her right to seek a judicial remedy.

(8) The controller shall document the factual or legal reasons on which the decision is based.

Section 58

Right to rectification and erasure and to restriction of processing

(1) The data subject shall have the right to obtain from the controller without delay the rectification of inaccurate data concerning him or her. In particular in the case of statements or assessments, the question of accuracy is not relevant for the content of the statement or assessment. If the accuracy or inaccuracy of the data cannot be ascertained, the controller shall restrict processing instead of erasing

the data. In this case, the controller shall inform the data subject before lifting the restriction of processing. The data subject may also ask to have incomplete personal data completed, if doing so is appropriate when taking into account the purposes of processing.

(2) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without delay where processing such data is unlawful, knowledge of the data is no longer necessary for the performance of tasks, or the data must be erased to comply with a legal obligation.

(3) Instead of erasure, the controller may restrict processing where

1. there is reason to assume that erasure would adversely affect legitimate interests of the data subject,
2. the data must be retained for the purposes of evidence in proceedings serving the purposes of Section 45, or
3. erasure would be impossible or would involve a disproportionate effort due to the specific mode of storage.

Data subject to restricted processing pursuant to the first sentence may be processed only for the purpose which prevented their erasure.

(4) In automated filing systems, technical measures shall ensure that the restriction of processing is clearly recognizable and processing for other purposes is not possible without further examination.

(5) If the controller has rectified inaccurate data, he or she shall communicate the rectification to the body from which he or she received the personal data. In cases of rectification, erasure or restriction of processing pursuant to subsections 1 to 3, the controller shall inform recipients to whom the data were transferred about these measures. The recipient shall rectify or erase the data or restrict their processing.

(6) The controller shall inform the data subject in writing of any refusal to rectify or erase personal data or restrict its processing. This shall not apply if providing this information would entail a threat as referred to in Section 56 (2). The information pursuant to the first sentence shall include the reasons for the refusal unless providing the reasons would undermine the intended purpose of the refusal.

(7) Section 57 (7) and (8) shall apply accordingly.

Section 59

Modalities for exercising the rights of the data subject

(1) The controller shall communicate with data subjects in a concise, intelligible and easily accessible form, using clear and plain language. Regardless of special formal requirements, when responding to requests, the controller shall provide the information in the same form as the request.

(2) When responding to requests, without prejudice to Section 57 (6) and Section 58 (6) the controller shall inform the data subject in writing about the follow-up to his or her request without delay.

(3) Information provided pursuant to Section 55, any communication made pursuant to Sections 56 and 66, and requests processed pursuant to Sections 57 and 58 shall be free of charge. Where a request pursuant to Sections 57 and 58 is manifestly unfounded or excessive, the controller may charge a reasonable fee based on its administrative costs, or may refuse to act on the request. In this case, the controller must be able to demonstrate the manifestly unfounded or excessive character of the request.

(4) Where the controller has reasonable doubts concerning the identity of a data subject making the request pursuant to Sections 57 or 58, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

Section 60

Right to lodge a complaint with the Federal Commissioner

(1) Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with the Federal Commissioner, if the data subject believes that the processing by public bodies of personal data relating to him or her for the purposes listed in Section 45 infringes his or her rights. This shall not apply to the processing of personal data by courts, if they have processed these data in the context of their judicial activities. The Federal Commissioner shall inform the data subject of the progress and the outcome of the complaint and of the possibility of a judicial remedy pursuant to Section 61.

(2) If a complaint about processing is lodged with the Federal Commissioner instead of the competent supervisory authority in another Member State of the European Union, the Federal Commissioner shall transmit the complaint to the competent supervisory authority without delay. In this case, the Federal Commissioner shall inform the data subject about the transmission of his or her complaint and shall provide further support at the data subject's request.

Section 61

Legal remedies against decisions of the Federal Commissioner or if he or she fails to take action

(1) Without prejudice to any other legal remedy, every natural or legal person shall have the right to take legal action against a legally binding decision of the Federal Commissioner.

(2) Subsection 1 shall apply accordingly to data subjects if the Federal Commissioner does not handle a complaint pursuant to Section 60 or does not inform the data subject within three months of the progress or outcome of the complaint.

Chapter 4

Obligations of controllers and processors

Section 62

Processing carried out on behalf of a controller

(1) Where personal data are processed by other persons or bodies on behalf of a controller, the controller shall ensure compliance with the provisions of this Act and other data protection provisions. The data subject shall assert his or her rights to access, rectification, erasure, restriction of processing and the right to receive compensation against the controller.

(2) A controller may use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the law and ensure the protection of the rights of the data subjects.

(3) Processors shall not engage other processors without prior written authorization by the controller. If the controller has given the processor general authorization to engage other processors, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors. In this case, the controller may object to such changes.

(4) Where a processor engages another processor, the former shall impose on the latter the same data protection obligations as set out in the contract between the controller and the processor as referred to in subsection 5 if these obligations are not already binding for the latter processor because of other legislation. Where that other processor fails to fulfil these obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

(5) Processing by a processor shall be governed by a contract or other legal instrument that is binding on the processor with regard to the controller and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal instrument shall stipulate, in particular, that the processor

1. acts only on instructions from the controller; if the processor believes that an instruction is unlawful, the processor shall inform the controller without delay;
2. ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
3. assists the controller by any appropriate means to ensure compliance with the provisions on the data subject's rights;
4. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of data processing services, and deletes existing copies unless law requires storage of the personal data;
5. makes available to the controller all information necessary, in particular the logs kept in accordance with Section 76, to demonstrate compliance with these obligations;
6. allows for and contributes to audits conducted by the controller or another auditor mandated by the controller;
7. complies with the conditions referred to in subsections 3 and 4 for engaging another processor;
8. takes all measures required pursuant to Section 64; and
9. assists the controller in ensuring compliance with the obligations pursuant to Sections 64 to 67 and 69 taking into account the nature of processing and the information available to the processor.

(6) The contract referred to in subsection 5 shall be in writing or in an electronic form.

(7) A processor that determines, in violation of this provision, the purposes and means of processing, shall be considered a controller in respect of that processing.

Section 63

Joint controllers

Where two or more controllers jointly determine the purposes and means of processing, they shall be considered joint controllers. Joint controllers shall determine their respective tasks and responsibilities under data protection law in a transparent manner in an agreement, unless these tasks and responsibilities are already determined by law. In particular, this agreement must indicate which of them must meet which information obligations, and how and with respect to whom data subjects may exercise their rights. Such an agreement shall not prevent data subjects from asserting their rights against each of the joint controllers.

Section 64

Requirements for the security of data processing

(1) The controller and the processor, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the legally protected interests of natural persons, shall implement the necessary technical and organizational measures to ensure a level of security appropriate to the risk when processing personal data, in particular as regards the processing of special categories of personal data. In doing so, the controller shall take into account the relevant Technical Guidelines and recommendations from the Federal Office for Information Security.

(2) The measures referred to in subsection 1 may include pseudonymization and encryption of personal data, if such means are possible in view of the purposes of processing. The measures pursuant to subsection 1 should ensure

1. the ongoing confidentiality, integrity, availability and resilience of processing systems and services in connection with processing; and
2. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

(3) In respect of automated processing, the controller and processor, following an evaluation of the risks, shall implement measures designed to

1. deny unauthorized persons access to processing equipment used for processing ('equipment access control');
2. prevent the unauthorized reading, copying, modification or erasure of data media ('data media control');
3. prevent the unauthorized input of personal data and the unauthorized inspection, modification or deletion of stored personal data ('storage control');
4. prevent the use of automated processing systems by unauthorized persons using data communication equipment ('user control');
5. ensure that persons authorized to use an automated processing system have access only to the personal data covered by their access authorization ('data access control');
6. ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control');

7. ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('input control');
8. ensure that the confidentiality and integrity of personal data are protected during transfers of personal data or during transport of data media ('transport control');
9. ensure that installed systems may, in the case of interruption, be restored ('recovery');
10. ensure that all system functions perform and that the appearance of faults in the functions is reported ('reliability');
11. ensure that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity');
12. ensure that personal data processed on behalf of the controller can only be processed in compliance with the controller's instructions ('processing control');
13. ensure that personal data are protected against loss and destruction ('availability control');
14. ensure that personal data collected for different purposes can be processed separately ('separability').

A purpose pursuant to the first sentence, nos. 2 to 5 may be achieved in particular by using state-of-the-art encryption.

Section 65

Notifying the Federal Commissioner of a personal data breach

(1) In the case of a personal data breach, the controller shall notify the Federal Commissioner without delay and, if possible, not later than 72 hours after having become aware of it, of the personal data breach, unless the personal data breach is unlikely to result in a risk to the legally protected interests of natural persons. If the Federal Commissioner is not notified within 72 hours, the notification shall be accompanied by reasons for the delay.

(2) A processor shall notify the controller of a personal data breach without delay.

(3) The notification referred to in subsection 1 shall include at least the following information:

1. a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

2. the name and contact details of the data protection officer or other contact point where more information can be obtained;

3. a description of the likely consequences of the personal data breach; and

4. a description of the measures taken or proposed by the controller to address the personal data breach, including measures to mitigate its possible adverse effects.

(4) If it is not possible to provide the information pursuant to subsection 3 with the notification, the controller shall provide this information as soon as it is available.

(5) The controller shall document any personal data breaches. This documentation shall include all the facts relating to the personal data breach, its effects and the remedial action taken.

(6) If the personal data breach involves personal data that have been transmitted by or to a controller in another Member State of the European Union, the information referred to in subsection 3 shall be communicated to the controller in that Member State without delay.

(7) Section 42 (4) shall apply accordingly.

(8) Additional obligations of the controller regarding notifications of personal data breaches shall remain unaffected.

Section 66

Notifying data subjects affected by a personal data breach

(1) If a personal data breach is likely to result in a substantial risk to the legally protected interests of natural persons, the controller shall notify the data subject of the personal data breach without delay.

(2) The notification of the data subject pursuant to subsection 1 shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in Section 65 (3) nos. 2 to 4.

(3) Notification shall not be required if any of the following conditions are met:

1. the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access them, such as encryption;

2. the controller has taken subsequent measures which ensure that the substantial risk referred to in subsection 1 is no longer likely to exist;

3. it would involve a disproportionate effort; in this case, a public communication shall be made or a similar measure taken to inform the data subjects in an equally effective manner.

(4) If the controller has not informed the data subjects of a personal data breach, the Federal Commissioner may formally determine that, in his or her opinion, the conditions referred to in subsection 3 have not been met. In doing so, the Federal Commissioner shall consider the likelihood of the personal data breach resulting in a high risk as referred to in subsection 1.

(5) The notification of data subjects pursuant to subsection 1 may be delayed, restricted or omitted under the conditions referred to in Section 56 (2) unless the interests of the data subjects outweigh those of the controller owing to the high risk resulting from the personal data breach as referred to in subsection 1.

(6) Section 42 (4) shall apply accordingly.

Section 67

Conducting a data protection impact assessment

(1) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a substantial risk to the legally protected interests of data subjects, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the data subjects.

(2) A joint assessment may address a set of similar processing operations that present similar substantial risks.

(3) The controller shall involve the Federal Commissioner in carrying out the impact assessment.

(4) The impact assessment shall take the rights of the data subjects affected by the processing into account and shall contain at least the following:

1. a systematic description of the envisaged processing operations and the purposes of the processing;
2. an assessment of the necessity and proportionality of the processing operations in relation to their purposes;
3. an assessment of the risks to the legally protected interests of the data subjects; and
4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the law.

(5) Where necessary, the controller shall carry out a review to assess whether processing is performed in accordance with the data protection impact assessment.

Section 68

Cooperation with the Federal Commissioner

The controller shall cooperate with the Federal Commissioner in carrying out the latter's tasks.

Section 69

Prior consultation of the Federal Commissioner

(1) The controller shall consult the supervisory authority prior to processing which will form part of a new filing system if

1. a data protection impact assessment pursuant to Section 67 indicates that the processing would result in a substantial risk to the legally protected interests of data subjects in the absence of measures taken by the controller to mitigate the risk; or
2. the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a substantial risk to the legally protected interests of data subjects.

The Federal Commissioner may draw up a list of the processing operations which are subject to prior consultation pursuant to the first sentence.

(2) In the case of subsection 1, the Federal Commissioner shall be presented with

1. the data protection impact assessment carried out pursuant to Section 67;
2. where applicable, information on the respective responsibilities of the controller, joint controllers and processors involved in the processing;
3. information on the purposes and means of the envisaged processing;
4. information on the measures and safeguards intended to protect the legally protected interests of the data subjects; and
5. the name and contact details of the data protection officer.

On request, the Federal Commissioner shall be given any other information he or she requires to assess the lawfulness of the processing and, in particular, the existing risks to the protection of the data subjects' personal data and the related safeguards.

(3) If the Federal Commissioner believes that the planned processing would violate the law, in particular because the controller has not sufficiently identified the risk or has not taken sufficient measures to mitigate the risk, he or she may provide, within a period of up to six weeks of receipt of the request for consultation, written advice to the controller and, where applicable, to the processor, as to which additional measures should be taken. The Federal Commissioner may extend this period by a month, if the planned processing is especially complex. In this case, the Federal Commissioner shall inform the controller and, where applicable, the processor of the extension within one month of receipt of the request for consultation.

(4) If the envisaged processing has substantial significance for the controller's performance of tasks and is therefore especially urgent, the controller may initiate processing after the consultation has started but before the period referred to in subsection 3, first sentence, has expired. In this case, the recommendations of the Federal Commissioner shall be taken into account after the fact, and the way the processing is carried out shall be adjusted where applicable.

Section 70

Records of processing activities

(1) The controller shall keep a record of all categories of processing activities under its responsibility. This record shall contain all of the following information:

1. the name and contact details of the controller and, where applicable, of the joint controller; and the name and contact details of the data protection officer;
2. the purposes of the processing;
3. the categories of recipients to whom the personal data have been or are to be disclosed;
4. a description of the categories of data subjects and of the categories of personal data;
5. where applicable, the use of profiling;
6. where applicable, the categories of transfers of personal data to bodies in a third country or to an international organization;
7. information about the legal basis for the processing;
8. the envisaged time limits for the erasure or for a review of the need to store the various categories of personal data; and

9. a general description of the technical and organizational security measures referred to in Section 64.

(2) The processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing

1. the name and contact details of the processor, of each controller on behalf of which the processor is acting and, where applicable, the data protection officer;

2. where applicable, transfers of personal data to bodies in a third country or to an international organization, including the identification of that third country or international organization; and

3. a general description of the technical and organizational security measures according to Section 64.

(3) The records referred to in subsections 1 and 2 shall be in writing or in electronic form.

(4) Controllers and processors shall make these records available to the Federal Commissioner on request.

Section 71

Data protection by design and by default

(1) The controller, both at the time the means of processing are determined and at the time of the processing itself, shall take appropriate measures to implement data protection principles, such as data minimization, in an effective manner, to ensure compliance with legal requirements and to protect the rights of data subjects. In doing so, the controller shall take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the legally protected interests of the data subject posed by the processing. In particular, personal data shall be processed, and processing systems shall be selected and designed in accordance with the aim of processing as few personal data as possible. Personal data shall be rendered anonymous or pseudonymized as early as possible, as far as possible in accordance with the purpose of processing.

(2) The controller shall implement appropriate technical and organizational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That applies to the amount of data collected, the extent of their processing, the period of their storage and their accessibility. In particular, the measures must ensure that by default the data are not made accessible by automated means to an indefinite number of persons.

Section 72

Distinction between different categories of data subjects

When processing personal data, the controller shall, as far as possible, make a clear distinction between different categories of data subjects. This applies in particular to the following categories:

1. persons with regard to whom there are serious grounds for believing that they have committed a criminal offence;
2. persons with regard to whom there are serious grounds for believing that they are about to commit a criminal offence;
3. persons convicted of a criminal offence;
4. victims of a criminal offence or persons with regard to whom certain facts indicate that they could be the victim of a criminal offence; and
5. other persons, such as witnesses, persons who can provide information, or contacts or associates of the persons referred to in nos. 1 to 4.

Section 73

Distinction between facts and personal assessments

In processing, the controller shall distinguish, as far as possible, personal data based on facts from personal data based on personal assessments. To this end, the controller shall identify evaluations based on personal assessments as such, as far as possible and reasonable in the context of the processing in question. It must also be possible to determine which body keeps the records on which an evaluation based on a personal assessment is based.

Section 74

Procedures for data transfers

(1) The controller shall take appropriate measures to ensure that personal data which are inaccurate or no longer up to date are not transmitted or otherwise made available. To that end, the controller shall, as far as possible with reasonable effort, verify the quality of the data before they are transmitted or made available. The controller shall also, as far as possible and reasonable, in all transmissions of personal data include the necessary information to enable the recipient to assess the degree of accuracy, completeness and reliability of the data, and the extent to which they are up to date.

(2) If the processing of personal data is subject to special conditions, in transmissions of data the transmitting body shall inform the recipient of these conditions and the requirement to respect them. The obligation of providing information may be met by marking the data accordingly.

(3) The transmitting body shall not apply conditions to recipients in other Member States of the European Union or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the Third Part of the Treaty on the Functioning of the European Union other than those applicable to similar domestic transmissions.

Section 75

Rectification and erasure of personal data and restriction of processing

(1) The controller shall rectify inaccurate personal data.

(2) The controller shall erase personal data without delay if their processing is unlawful, they must be erased to comply with a legal obligation, or knowledge of the data is no longer necessary for the controller to perform its tasks.

(3) Section 58 (3) to (5) shall apply accordingly. The recipient shall also be informed if inaccurate personal data have been transmitted, or if personal data have been transmitted unlawfully.

(4) Without prejudice to any time limits for storing or erasing data defined in law, the controller shall provide for appropriate time limits for the erasure of personal data or for a periodic review of the need for the storage of personal data and shall take procedural measures to ensure that these time limits are observed.

Section 76

Logging

(1) Controllers and processors shall provide for logs to be kept for at least the following processing operations in automated processing systems:

1. collection,
2. alteration,
3. consultation,
4. disclosure including transfers,
5. combination, and
6. erasure.

(2) The logs of consultation and disclosure must make it possible to ascertain the justification, date and time of such operations and, as far as possible, the identity of the person who consulted or disclosed personal data, and the identity of the recipients of the data.

(3) The logs may be used only by the data protection officer, the Federal Commissioner or the data subject to verify the lawfulness of the processing; and for self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.

(4) The log data shall be erased at the end of the year following the year in which they were generated.

(5) The controller and the processor shall make the logs available to the Federal Commissioner on request.

Section 77

Confidential reporting of violations

The controller shall ensure that it is able to receive confidential reports of violations of data protection law which have occurred in its area of responsibility.

Chapter 5

Transfers of data to third countries and to international organizations

Section 78

General requirements

(1) If all other conditions applicable to data transfers are met, the transfer of personal data to bodies in third countries or to international organizations shall be permitted if

1. the body or international organization is responsible for the purposes referred to in Section 45, and
2. the European Commission has adopted an adequacy decision pursuant to Article 36 (3) of Directive (EU) 2016/680.

(2) No transfer of personal data shall be permitted, despite an adequacy decision as referred to in subsection 1 no. 2 and the public interest in the data transfer to be taken into account, if in the individual case it cannot be ensured that the data will be handled appropriately in terms of data protection law and in accordance with fundamental human rights in the area of responsibility of the recipient, or if a transfer would conflict with other overriding legitimate interests of a data subject. The controller shall base its assessment on whether the recipient in the individual case guarantees appropriate protection of the transferred data.

(3) If personal data which have been transmitted or made available from another European Union Member State are to be transferred pursuant to subsection 1, the competent body of the other Member State must provide prior authorization of the transfer. Transfers without the prior authorization shall be permitted only if the transfer is necessary to prevent an immediate and serious threat to the public security of a country or to essential interests of a Member State and the prior authorization cannot be obtained in time. In the case of the second sentence, the other Member State's body responsible for giving prior authorization shall be informed of the transfer without delay.

(4) The controller transferring data pursuant to subsection 1 shall take appropriate measures to ensure that the recipient will transfer the data onward to other third countries or other international organizations only with the prior authorization of the controller. When deciding whether to authorize the transfer, the controller shall take into account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data were originally transferred and the level of personal data protection in the third country or international organization to which the data are to be transferred onward. The transfer shall be authorized only if a direct transfer to the other third country or international organization would be lawful. The responsibility for issuing authorization may also be otherwise provided for.

Section 79

Data transfers with appropriate safeguards

(1) In the absence of a decision pursuant to Article 36 (3) of Directive (EU) 2016/680, transfers which meet the remaining requirements of Section 78 shall be permitted also if

1. appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or
2. the controller has assessed all the circumstances surrounding the transfer and concludes that appropriate safeguards exist for the protection of personal data.

(2) The controller shall document transfers pursuant to subsection 1 no. 2. The documentation shall include the date and time of the transfer, the identity of the recipient, the reason for the transfer and the personal data transferred. It shall be provided to the Federal Commissioner on request.

(3) The controller shall file a report to the Federal Commissioner at least once a year covering transfers conducted on the basis of an assessment pursuant to subsection 1 no. 2. In this report, the controller may categorize the recipients and the purpose of the transfers appropriately.

Section 80

Data transfers without appropriate safeguards

(1) If in derogation from Section 78 (1) no. 2, no decision pursuant to Article 36 (3) of Directive (EU) 2016/680 or appropriate safeguards as referred to in Section 79 (1) exist, transfers which meet the remaining requirements of Section 78 shall be permitted also if they are necessary

1. to protect the vital interests of a natural person;
2. to safeguard legitimate interests of the data subject;
3. to prevent an immediate and serious threat to the public security of a country;
4. in individual cases for the purposes referred to in Section 45; or
5. in an individual case for the establishment, exercise or defence of legal claims relating to the purposes referred to in Section 45.

(2) The controller shall not transfer data pursuant to subsection 1 if the fundamental rights of the data subject override the public interest in the transfer.

(3) Section 79 (2) shall apply accordingly to transfers pursuant to subsection 1.

Section 81

Other data transfers to recipients in third countries

(1) In special individual cases and if all other requirements for data transfers to third countries are met, controllers may transfer personal data directly to recipients in third countries not referred to in Section 78 (1) no. 1 if the transfer is strictly necessary for the performance of their tasks and

1. in the specific case no fundamental rights of the data subject override the public interest in the transfer;
2. transfer to the bodies referred to in Section 78 (1) no. 1 would be ineffective or inappropriate, in particular because the transfer cannot be carried out in time; and
3. the controller informs the recipient of the purposes of processing and instructs the recipient that the transferred data may be processed only to the extent necessary for these purposes.

(2) In the case of subsection 1, the controller shall inform the bodies referred to in Section 78 (1) no. 1 of the transfer without delay, unless this is ineffective or inappropriate.

(3) Section 79 (2) and (3) shall apply accordingly to transfers pursuant to subsection 1.

(4) In the case of transfers pursuant to subsection 1, the transmitting controller shall obligate the recipient to process the transferred personal data without the controller's consent only for the purpose for which they were transferred.

(5) Agreements in the field of judicial cooperation in criminal matters and police cooperation shall remain unaffected.

Chapter 6

Cooperation among supervisory authorities

Section 82

Mutual assistance

(1) The Federal Commissioner shall provide the supervisory authorities in other European Union Member States with information and mutual assistance as far as necessary to implement and apply Directive (EU) 2016/680 in a consistent manner. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out consultations, inspections and investigations.

(2) The Federal Commissioner shall take all appropriate measures required to reply to a request for mutual assistance without delay and no later than one month after receiving the request.

(3) The Federal Commissioner may refuse to comply with the request only if

1. he or she is not competent for the subject matter of the request or for the measures he or she is asked to execute; or

2. compliance with the request would violate the law.

(4) The Federal Commissioner shall inform the other state's requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in response to the request. In the case of subsection 3, he or she shall provide reasons for refusing to comply with the request.

(5) The Federal Commissioner shall, as a rule, supply the information requested by the other state's supervisory authority by electronic means and using a standardized format.

(6) The Federal Commissioner shall not charge a fee for action taken pursuant to a request for mutual assistance unless he or she has agreed with the other state's supervisory authority in the individual case on the reimbursement of expenses incurred.

(7) The Federal Commissioner's requests for assistance shall contain all the necessary information, including in particular the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

Chapter 7

Liability and penalties

Section 83

Compensation

(1) If a controller has caused a data subject to suffer damage by processing personal data in violation of this Act or other law applicable to this processing, the controller or its legal entity shall be obligated to provide compensation to the data subject. This obligation to provide compensation shall not apply if, in the case of non-automated processing, the damage was not the result of fault by the controller.

(2) The data subject may request appropriate financial compensation for non-material damage.

(3) If, in the case of automated processing of personal data, it is not possible to determine which of several controllers caused the damage, each controller or its legal entity shall be liable.

(4) Section 254 of the Civil Code shall apply to contributory negligence on the part of the data subject.

(5) The limitation provisions stipulated for tortious acts in the Civil Code shall apply accordingly with regard to statutory limitation.

Section 84

Penal provisions

Section 42 shall apply accordingly to the processing of personal data by public bodies in the context of activities pursuant to Section 45, first, third or fourth sentences.

Part 4

Special provisions for processing in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680

Section 85

Processing of personal data in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680

(1) The transfer of personal data to a third country, to supranational or intergovernmental bodies or to international organizations in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680 shall be permitted in addition to the cases permitted under Regulation (EU) 2016/679 also if the processing is necessary to perform tasks for urgent reasons of defence or to fulfil supra- or intergovernmental obligations of a public body of the Federation in the field of crisis management or conflict pre-vention or for humanitarian measures. The recipient shall be instructed that the transferred data may be used only for the purpose for which they were transferred.

(2) Section 16 (4) shall not apply to processing in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680 by workplaces within the remit of the Federal Ministry of Defence if the Federal Ministry of Defence determines in the individual case that meeting the obligations referred to in that provision would endanger the security of the Federation.

(3) Processing by public bodies of the Federation in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU) 2016/680 shall not be subject to the obligation to provide information in accordance with Article 13 (1) and (2) of Regulation (EU) 2016/679

1. in the cases referred to in Section 32 (1) nos. 1 to 3, or

2. if meeting this obligation would disclose information which by law or by its nature must be kept secret, in particular because of legitimate interests of a third party which outweigh the interests of the data subject in obtaining the information.

If the data subject is not to be informed in the cases of the first sentence, no right of access shall apply. Sections 32 (2) and 33 (2) shall not apply.

Section 86

Processing of personal data for purposes of government awards and honours

(1) To prepare and conduct government procedures for awards and honours, both the responsible bodies and other public and private bodies may process the necessary personal data, including special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679, also without the knowledge of the data subject. Section 1 (8) shall apply to private bodies accordingly. Processing of personal data pursuant to the first sentence for other purposes shall be permitted only with the consent of the data subject.

(2) If processing is conducted solely for the purposes listed in subsection 1, first sentence, Articles 13 to 16, 19 and 21 of Regulation (EU) 2016/679 shall not apply.

(3) When processing special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679, the controller shall take appropriate and specific measures to safeguard the rights of the data subject in accordance with Section 22 (2).

Írlanda - Data Protection Act 2018

Number 7 of 2018

DATA PROTECTION ACT 2018

CONTENTS

PART 1

Preliminary and General

1. Short title, citation and commencement
2. Interpretation
3. Designation by appropriate authority
4. Obligation not to require data subject to exercise right of access under Data Protection Regulation and Directive in certain circumstances
5. Expenses
6. Regulations
7. Repeals and revocations
8. Application of Data Protection Act 1988

PART 2

Data Protection Commission

9. Establishment day
10. Establishment of Data Protection Commission
11. Supervisory authority for Data Protection Regulation and Directive
12. Functions of Commission
13. Performance of functions of Commission by Commissioner or member of staff
14. Transfer of functions of Data Protection Commissioner to Commission
15. Membership of Commission
16. Appointment of chairperson of Commission

17. Resignation, removal, disqualification of Commissioner, ineligibility to become Commissioner
18. Acting Commissioner
19. Accountability of Commissioner to Oireachtas Committees
20. Assignment and transfer of staff to Commission
21. Staff of Commission
22. Superannuation of Commissioners
23. Accounts of Commission
24. Annual report
25. Accountability for accounts of Commission
26. Prohibition on disclosure of confidential information
27. Civil proceedings for contravention of section 26

PART 3

Data Protection Regulation

Chapter 1

General

28. Fees
29. Child for purposes of application of Data Protection Regulation
30. Micro-targeting and profiling of children
31. Consent of child in relation to information society services
32. Codes of conduct: children
33. Right to be forgotten: children
34. Designation of data protection officer
35. Accreditation of certification bodies by Irish National Accreditation Board
36. Suitable and specific measures for processing
37. Limitation on transfers of personal data outside the European Union
38. Processing for a task carried out in the public interest or in the exercise of official authority

39. Communication with data subjects by political parties, candidates for and holders of certain elective political offices
40. Processing of personal data and special categories of personal data by elected representatives
41. Processing for purpose other than purpose for which data collected
42. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
43. Data processing and freedom of expression and information
44. Data processing and public access to official documents

Chapter 2

Processing of special categories of personal data and processing of personal data relating to criminal convictions and offences

45. Processing of special categories of personal data
46. Processing of special categories of personal data for purposes of employment and social welfare law
47. Processing of special categories of personal data for purpose of legal advice and legal proceedings
48. Processing of personal data revealing political opinions for electoral activities and functions of Referendum Commission
49. Processing of special categories of personal data for purposes of administration of justice and performance of functions
50. Processing of special categories of personal data for insurance and pension purposes
51. Processing of special categories of personal data and Article 10 data for reasons of substantial public interest
52. Processing of special categories of personal data for purposes of Article 9(2)(h)
53. Processing of special categories of personal data for purposes of public interest in the area of public health
54. Processing of special categories of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
55. Processing of personal data relating to criminal convictions and offences

Chapter 3

Rights, and restrictions of rights, of data subject and restrictions on obligations of controllers

- 56. Right of access to results and scripts of examination and results of appeal
- 57. Rights in relation to automated decision making
- 58. Direct marketing for purposes of Article 21
- 59. Restriction on right of data subject to object to processing for election purposes and processing by Referendum Commission
- 60. Restrictions on obligations of controllers and rights of data subjects for important objectives of general public interest
- 61. Restriction on exercise of data subjects' rights: archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

PART 4

Provisions Consequent on Repeal of Certain Provisions of Data Protection Act 1988

- 62. Transfer of property of Data Protection Commissioner to Commission
- 63. Transfer of rights and liabilities of Data Protection Commissioner to Commission
- 64. Liability for loss occurring before establishment day
- 65. Provisions consequent upon transfer of functions, assets, rights and liabilities to Commission
- 66. Final accounts and final annual report of Data Protection Commissioner
- 67. Saver for scheme relating to superannuation
- 68. Saver for regulations under Act of 1988

PART 5

Processing of Personal Data for Law Enforcement Purposes

Chapter 1

Preliminary and general (Part 5)

- 69. Interpretation (Part 5)
- 70. Application of Part 5

Chapter 2

General principles of data protection

71. Processing of personal data

72. Security measures for personal data

73. Processing of special categories of personal data (Part 5)

74. Data quality

Chapter 3

Obligations of controllers and processors

75. General obligations of controller with regard to technical and organisational measures

76. Data protection by design and by default

77. Security of automated processing

78. Technical and organisational measures

79. Joint controllers

80. Processors

81. Record of data processing activities

82. Data logging for automated processing system

83. Cooperation with Commission

84. Data protection impact assessment and prior consultation with Commission

85. Notification of personal data breach by processor

86. Notification of personal data breach to Commission, etc.

87. Communication of personal data breach to data subject

88. Data protection officer

Chapter 4

Rights, and restriction of rights, of data subject (Part 5)

89. Rights in relation to automated decision making (Part 5)

90. Right to information

91. Right of access

92. Right to rectification or erasure and restriction of processing

93. Communication with data subject

94. Restrictions on exercise of data subject rights (Part 5)

95. Indirect exercise of rights and verification by Commission

Chapter 5

Transfers of personal data to third countries or international organisations

96. Transfer to third country or international organisation

97. Adequacy decision

98. Transfer subject to appropriate safeguards

99. Derogations for specific situations

100. Transfer to recipient in third country

Chapter 6

Independent supervisory authority

101. Functions of Commission under Part 5

102. Power of the Commission to advise and issue opinions

103. Mutual assistance

104. Requests by Commission for mutual assistance

PART 6

Enforcement of Data Protection Regulation and Directive

Chapter 1

Preliminary

105. Interpretation (Part 6)

106. Service of documents (Part 6)

Chapter 2

Enforcement of Data Protection Regulation

107. Interpretation (Chapter 2)

108. Complaints under Chapter 2: General

109. Commission to handle complaint under Chapter 2

110. Commission may conduct inquiry into suspected infringement of relevant enactment

111. Decision of Commission where inquiry under Chapter 2 conducted of own volition

112. Decision of Commission where inquiry conducted in respect of complaint to which Article 55 or 56(5) applies

113. Complaint to which Article 60 applies

114. Commission to adopt decision in certain circumstances

115. Exercise by Commission of corrective power

116. Notification of decision of Commission under Chapter 2

117. Judicial remedy for infringement of relevant enactment

Chapter 3

Enforcement of Directive

118. Interpretation (Chapter 3)

119. Data subject may lodge complaint with Commission

120. Representation of data subjects

121. Complaints under Chapter 3: General

122. Commission to handle complaint under Chapter 3

123. Commission may conduct inquiry into suspected infringements of relevant provision

124. Decision of Commission in respect of inquiry under Chapter 3 conducted of own volition

125. Decision of Commission where inquiry conducted in respect of complaint under Chapter 3

126. Notification of decision of Commission under Chapter 3

127. Corrective powers of Commission (Chapter 3)

128. Judicial remedy for infringement of relevant provision

Chapter 4

Inspection, Audit and Enforcement

129. Authorised officers

130. Powers of authorised officers

131. Search warrants

132. Information notice

133. Enforcement notice

134. Circumstances in which application may be made to the High Court for suspension or restriction of processing of data

135. Power to require report

136. Data Protection Audit

Chapter 5

Investigations

137. Investigations

138. Conduct of investigation under section 137

139. Investigation report

140. Commission to consider investigation report

Chapter 6

Administrative Fines

141. Power of Commission to decide to impose administrative fine: General

142. Appeal against administrative fine

143. Circuit Court to confirm decision to impose administrative fine

Chapter 7

Offences

144. Unauthorised disclosure by processor

145. Disclosure of personal data obtained without authority

146. Offences by directors, etc., of bodies corporate

147. Prosecution of summary offences by Commission

Chapter 8

Miscellaneous

148. General provisions relating to complaints

149. Publication of convictions, sanctions, etc.

150. Right to effective judicial remedy (Part 6)

151. Privileged legal material

152. Presumptions

153. Expert evidence

154. Immunity from suit

155. Jurisdiction of Circuit Court

156. Hearing of proceedings

PART 7

Miscellaneous Provisions

157. Supervisory authority for courts acting in judicial capacity

158. Restrictions on obligations of controllers and rights of data subjects for objective of safeguarding judicial independence and court proceedings

159. Processing of personal data where court is controller

160. Publication of judgment or decision of court or court list

161. Rules of court for data protection actions

162. Legal privilege

163. Application to High Court concerning adequate level of protection or appropriate safeguards

164. Court may order destruction, erasure of data

PART 8

Amendments of other Acts of Oireachtas

165. Reference to personal data in enactment

166. Reference to processing in enactment

167. Amendment of Firearms Act 1925
168. Amendment of section 33AK of Central Bank Act 1942
169. Amendment of section 2 of Civil Service Regulation Act 1956
170. Amendment of section 24 of Misuse of Drugs Act 1977
171. Amendment of section 15A of Control of Clinical Trials Act 1987
172. Amendment of Data Protection Act 1988
173. Amendment of Bankruptcy Act 1988
174. Amendment of Firearms and Offensive Weapons Act 1990
175. Amendment of section 13A of Electoral Act 1992
176. Amendment of Comptroller and Auditor General (Amendment) Act 1993
177. Amendment of section 8 of Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993
178. Amendment of section 24 of Statistics Act 1993
179. Amendment of section 57B of Irish Aviation Authority Act 1993
180. Amendment of section 18F of Health Insurance Act 1994
181. Amendment of section 142 of Consumer Credit Act 1995
182. Amendment of section 32B of Irish Medicines Board Act 1995
183. Amendment of section 77 of Central Bank Act 1997
184. Amendment of section 1 of Health (Provision of Information) Act 1997
185. Amendment of section 9M of Electricity Regulation Act 1999
186. Amendment of British-Irish Agreement Act 1999
187. Amendment of section 7D of Comhairle Act 2000
188. Amendment of section 33 of Commission To Inquire Into Child Abuse Act 2000
189. Amendment of section 2 of Merchant Shipping (Investigation of Marine Casualties) Act 2000
190. Amendment of section 28 of Education (Welfare) Act 2000
191. Amendment of section 38 of Planning and Development Act 2000

192. Amendment of section 14 of Dormant Accounts Act 2001
193. Amendment of section 30 of Residential Institutions Redress Act 2002
194. Amendment of section 2 of Official Languages Act 2003
195. Amendment of section 86 of Personal Injuries Assessment Board Act 2003
196. Amendment of section 12 of Unclaimed Life Assurance Policies Act 2003
197. Amendment of section 66 of Civil Registration Act 2004
198. Amendment of section 39 of Commissions of Investigation Act 2004
199. Amendment of section 55H of Health Act 2004
200. Amendment of section 2 of Safety, Health and Welfare at Work Act 2005
201. Amendment of section 265 of Social Welfare Consolidation Act 2005
202. Amendment of Disability Act 2005
203. Amendment of section 2 of Railway Safety Act 2005
204. Amendment of section 12 of Health (Repayment Scheme) Act 2006
205. Amendment of section 19 of Electoral (Amendment) Act 2006
206. Amendment of section 67 of Pharmacy Act 2007
207. Amendment of Passports Act 2008
208. Amendment of Criminal Justice (Mutual Assistance) Act 2008
209. Amendment of section 2 of Chemicals Act 2008
210. Amendment of Nursing Homes Support Scheme Act 2009
211. Amendment of section 23 of Criminal Justice (Miscellaneous Provisions) Act 2009
212. Amendment of section 201 of National Asset Management Agency Act 2009
213. Amendment of Criminal Justice (Money Laundering and Terrorist Financing) Act 2010
214. Amendment of section 12 of Communications (Retention of Data) Act 2011
215. Amendment of section 17A of Ministers and Secretaries (Amendment) Act 2011
216. Amendment of section 28 of Student Support Act 2011
217. Amendment of Communications Regulation (Postal Services) Act 2011

218. Amendment of Property Services (Regulation) Act 2011
219. Amendment of section 56 of Credit Union and Co-operation with Overseas Regulators Act 2012
220. Amendment of Europol Act 2012
221. Amendment of Personal Insolvency Act 2012
222. Amendment of section 2 of Animal Health and Welfare Act 2013
223. Amendment of section 8 of Health (Alteration of Criteria for Eligibility) Act 2013
224. Insertion of section 957A to Companies Act 2014
225. Amendment of Health Identifiers Act 2014
226. Amendment of section 15 of Freedom of Information Act 2014
227. Amendment of section 41 of Customs Act 2015
228. Amendment of section 7 of Regulation of Lobbying Act 2015
229. Amendment of Sport Ireland Act 2015
230. Amendment of section 12 of Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016
231. Amendment of section 62 of Financial Services and Pensions Ombudsman Act 2017
232. Amendment of National Shared Services Office Act 2017

SCHEDULE 1

Statutory Instruments Revoked

SCHEDULE 2

Data Protection Commission

SCHEDULE 3

Provisions Applicable to Oral Hearing Conducted by an Authorised Officer Under Section 138

Acts Referred to

Animal Health and Welfare Act 2013 (No. 15)

Bankruptcy Act 1988 (No. 27)

British-Irish Agreement Act 1999 (No. 1)

Central Bank Act 1942 (No. 22)

Central Bank Act 1997 (No. 8)

Chemicals Act 2008 (No. 13)

Children Act 2001 (No. 24)

Civil Registration Act 2004 (No. 3)

Civil Service Regulation Act 1956 (No. 46)

Comhairle Act 2000 (No. 1)

Commission To Inquire Into Child Abuse Act 2000 (No. 7)

Commissions of Investigation Act 2004 (No. 23)

Communications (Retention of Data) Act 2011 (No. 3)

Communications Regulation (Postal Services) Act 2011 (No. 21)

Companies Act 2014 (No. 38)

Competition Act 2002 (No. 14)

Comptroller and Auditor General (Amendment) Act 1993 (No. 8)

Consumer Credit Act 1995 (No. 24)

Control of Clinical Trials Act 1987 (No. 28)

Credit Union and Co-operation with Overseas Regulators Act 2012 (No. 40)

Criminal Justice (Forensic Evidence and DNA Database System) Act 2014 (No. 11)

Criminal Justice (Miscellaneous Provisions) Act 2009 (No. 28)

Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (No. 6)

Criminal Justice (Mutual Assistance) Act 2008 (No. 7)

Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016 (No. 4)

Customs Act 2015 (No. 18)

Data Protection (Amendment) Act 2003 (No. 6)

Data Protection Act 1988 (No. 25)

Data Protection Acts 1988 and 2003

Data Protection Acts 1988 to 2003

Defence Act 1954 (No. 18)

Dentists Act 1985 (No. 9)

Disability Act 2005 (No. 14)

Dormant Accounts Act 2001 (No. 32)

Education (Welfare) Act 2000 (No. 22)

Education Act 1998 (No. 51)

Electoral (Amendment) Act 2006 (No. 33)

Electoral Act 1992 (No. 23)

Electricity Regulation Act 1999 (No. 23)

European Parliament Elections Act 1997 (No. 2)

Europol Act 2012 (No. 53)

Financial Services and Pensions Ombudsman Act 2017 (No. 22)

Firearms (Firearm Certificates For Non-Residents) Act 2000 (No. 20)

Firearms Act 1925 (No. 17)

Firearms and Offensive Weapons Act 1990 (No. 12)

Freedom of Information Act 2014 (No. 30)

Health (Alteration of Criteria for Eligibility) Act 2013 (No. 10)

Health (Corporate Bodies) Act 1961 (No. 27)

Health (Provision of Information) Act 1997 (No. 9)

Health (Repayment Scheme) Act 2006 (No. 17)

Health Act 2004 (No. 42)

Health Identifiers Act 2014 (No. 15)

Health Insurance Act 1994 (No. 16)

Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 (No. 10)

Interpretation Act 2005 (No. 23)

Irish Aviation Authority Act 1993 (No. 29)

Irish Medicines Board Act 1995 (No. 29)

Local Government Act 2001 (No. 37)

Medical Practitioners Act 1978 (No. 4)

Medical Practitioners Act 2007 (No. 25)

Merchant Shipping (Investigation of Marine Casualties) Act 2000 (No. 14)

Ministers and Secretaries (Amendment) Act 2011 (No. 10)

Misuse of Drugs Act 1977 (No. 12)

National Asset Management Agency Act 2009 (No. 34)

National Shared Services Office Act 2017 (No. 26)

Nursing Homes Support Scheme Act 2009 (No. 15)

Official Languages Act 2003 (No. 32)

Passports Act 2008 (No. 4)

Personal Injuries Assessment Board Act 2003 (No. 46)

Personal Insolvency Act 2012 (No. 44)

Petty Sessions (Ireland) Act 1851 (14 & 15 Vict., c.93)

Pharmacy Act 2007 (No. 20)

Planning and Development Act 2000 (No. 30)

Prisons Acts 1826 to 2015

Property Services (Regulation) Act 2011 (No. 40)

Public Service Superannuation (Miscellaneous Provisions) Act 2004 (No. 7)

Railway Safety Act 2005 (No. 31)

Regulation of Lobbying Act 2015 (No. 5)

Residential Institutions Redress Act 2002 (No. 13)

Safety, Health and Welfare at Work Act 2005 (No. 10)

Social Welfare Consolidation Act 2005 (No. 26)

Sport Ireland Act 2015 (No. 15)

Statistics Act 1993 (No. 21)

Student Support Act 2011 (No. 4)

Unclaimed Life Assurance Policies Act 2003 (No. 2)

Vehicle Registration Data (Automated Searching and Exchange) Act 2018 (No. 5)

Number 7 of 2018

DATA PROTECTION ACT 2018

An Act to establish a body to be known as An Coimisiún um Chosaint Sonraí or, in the English language, the Data Protection Commission; to give further effect to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016¹ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); to give effect to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016² on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA; to give further effect to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data done at Strasbourg on the 28th day of January 1981 and for those and other purposes to amend the Data Protection Act 1988 ; to provide for the consequential amendment of certain other enactments; and to provide for related matters.

[24th May, 2018]

Be it enacted by the Oireachtas as follows:

PART 1

Preliminary and General

Short title, citation and commencement

1. (1) This Act may be cited as the Data Protection Act 2018.
- (2) This Act and the Data Protection Acts 1988 and 2003 may be cited together as the Data Protection Acts 1988 to 2018.
- (3) This Act shall come into operation on such day or days as the Minister may by order or orders appoint either generally or with reference to any particular purpose or provision and different days may be so appointed for different purposes or different provisions, and for the repeal of different enactments or provisions of enactments effected by section 7 .

Interpretation

2. (1) In this Act-

“Act of 1988” means the Data Protection Act 1988 ;

“Act of 2014” means the Companies Act 2014 ;

“authorised officer” means a person appointed, or deemed to be appointed, to be an authorised officer under section 129 ;

“chairperson” means the chairperson of the Commission;

“civil servant” has the meaning assigned to it by the Civil Service Regulation Act 1956 ;

“Commission” has the meaning assigned to it by section 10 ;

“Commissioner” has the meaning assigned to it by section 15 and includes a member of staff authorised to act in place of a Commissioner under section 18 ;

“Data Protection Regulation” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

“Directive” means Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA;

“enactment” has the same meaning as it has in the Interpretation Act 2005 ;

“local authority” means a local authority within the meaning of section 2 of the Local Government Act 2001 ;

“Minister” means the Minister for Justice and Equality;

“political party” means a political party registered in the Register of Political Parties in accordance with section 25 of the Electoral Act 1992 ;

“prescribe” means prescribe by regulations;

“public authority” means-

(a) a Department of State,

- (b) a regional assembly,
- (c) a local authority,
- (d) the office of the Director of Corporate Enforcement,
- (e) the Irish Auditing and Accounting Supervisory Authority,
- (f) any other person established by or under an enactment (other than the Act of 2014 or a former enactment relating to companies within the meaning of section 5 of that Act) other than-
 - (i) a recognised school or board within the meaning of section 2 of the Education Act 1998 but including a recognised school established and maintained by an education and training board and a board of a school so established and maintained, and
 - (ii) a management committee established under section 37 (3) of the Education Act 1998 ,
- (g) a person with whom the Health Service Executive has, under section 38 (1) of the Health Act 2004 , entered into an arrangement for the provision of a health or personal social service by that person on behalf of the Executive,

(h) the Garda Síochána;

“public body” means-

- (a) a company (within the meaning of the Act of 2014 or a former enactment relating to companies within the meaning of section 5 of that Act) a majority of the shares in which are held by or on behalf of a Minister of the Government,
- (b) a subsidiary (within the meaning of section 7 of the Act of 2014) of a company referred to in paragraph (a);

“special categories of personal data”, other than in Part 5 , means-

- (a) personal data revealing-
 - (i) the racial or ethnic origin of the data subject,
 - (ii) the political opinions or the religious or philosophical beliefs of the data subject, or
 - (iii) whether the data subject is a member of a trade union,
- (b) genetic data,
- (c) biometric data for the purposes of uniquely identifying an individual,
- (d) data concerning health, or

(e) personal data concerning an individual's sex life or sexual orientation.

(2) Subject to subsection (1), a word or expression used in this Act, other than in Part 5 , that is also used in the Data Protection Regulation has, unless the context otherwise requires, the same meaning in this Act as it has in that Regulation.

(3) Unless the context otherwise requires, a reference in this Act (other than in Part 5) to a numbered Article is a reference to the Article so numbered of the Data Protection Regulation.

Designation by appropriate authority

3. (1) An appropriate authority (within the meaning of the Civil Service Regulation Act 1956) may, as respects all or part of the personal data kept by the authority, designate a civil servant in relation to whom it is the appropriate authority to be a controller and while the designation is in force the civil servant so designated shall, other than for the purposes of sections 105 (3) and 141 (2) and (3), be deemed, for the purposes of this Act and the Data Protection Regulation, to be the controller in respect of the data concerned.

(2) Without prejudice to subsection (1), the Minister for Defence may, as respects all or part of the personal data kept by him in relation to the Defence Forces, designate an officer of the Permanent Defence Force who holds a commissioned rank therein to be a controller and while the designation is in force the officer so designated shall, other than for the purposes of sections 105 (3) and 141 (2) and (3), be deemed, for the purposes of this Act and the Data Protection Regulation, to be the controller in respect of the data concerned.

(3) For the purposes of this Act and the Data Protection Regulation-

(a) where a designation by the relevant appropriate authority under subsection (1) is not in force, a civil servant in relation to whom that authority is the appropriate authority shall be deemed to be its employee and, where such a designation is in force, such a civil servant (other than the civil servant the subject of the designation) shall be deemed to be an employee of the last mentioned civil servant,

(b) where a designation under subsection (2) is not in force, a member of the Defence Forces shall be deemed to be an employee of the Minister for Defence and, where such a designation is in force, such a member (other than the officer the subject of the designation) shall be deemed to be an employee of that officer, and

(c) a member of the Garda Síochána (other than the Commissioner of the Garda Síochána) shall be deemed to be an employee of the Commissioner of the Garda Síochána.

Obligation not to require data subject to exercise right of access under Data Protection Regulation and Directive in certain circumstances

4. (1) A person shall not, in connection with-

- (a) the recruitment of an individual as an employee,
- (b) the continued employment of the individual, or
- (c) a contract for the provision of services to the person by an individual,

require that individual to-

- (i) make a request under Article 15 or under section 91 , or
- (ii) supply the person with data relating to that individual obtained as a result of such a request.

(2) A person who contravenes subsection (1) shall be guilty of an offence and shall be liable-

- (a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or
- (b) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both.

Expenses

5. The expenses incurred by the Commission and any Minister of the Government in the administration of this Act shall, to such an extent as may be sanctioned by the Minister for Public Expenditure and Reform, be paid out of moneys provided by the Oireachtas.

Regulations

6. (1) Regulations made under this Act may contain such incidental, supplementary and consequential provisions as appear to the person making the regulations to be necessary or expedient for the purposes of the regulations.

(2) Every regulation made under this Act, other than under section 51 , 60 or 73 , shall be laid before each House of the Oireachtas as soon as may be after it is made.

(3) Either House of the Oireachtas may, by a resolution passed within 21 sitting days after the day on which a regulation is laid before it under subsection (2), annul the regulation.

(4) The annulment of a regulation under subsection (3) takes effect immediately on the passing of the resolution concerned but does not affect the validity of anything done under the regulation before the passing of the resolution.

(5) Regulations may be made under section 51 , 60 or 73 only if-

(a) a draft of the proposed regulations has been laid before each House of the Oireachtas, and

(b) a resolution approving the draft has been passed by each House.

Repeals and revocations

7. (1) Subject to subsection (4), the following provisions of the Act of 1988 are repealed:

(a) in section 1-

(i) subsection (1), the definition of “direct marketing”, “financial institution” and “the register”, and

(ii) subsection (5);

(b) section 2(7) and (8);

(c) section 4(2), (6), (8) and (13);

(d) section 5(1)(d);

(e) section 9 and the Second Schedule;

(f) section 11(3) and (4)(b);

(g) sections 13, 14, 16, 17, 18, 19, 20, 22A and 33.

(2) Subject to subsection (4), section 14 (2) of the Data Protection (Amendment) Act 2003 is repealed.

(3) Subject to subsection (4), the enactments specified in column (3) of Schedule 1 are revoked to the extent specified in column (4) of that Schedule.

(4) The repeals and revocations effected by this section shall not apply for the purposes of subsections (1)(b), (2) and (3) of section 8 .

Application of Data Protection Act 1988

8. (1) Subject to this section, the Act of 1988 shall, on and from the date on which this section comes into operation, cease to apply to the processing of personal data (within the meaning of that Act) other than-

(a) the processing of such data for the purposes of safeguarding the security of the State, the defence of the State or the international relations of the State, or

(b) the processing of such data under the Criminal Justice (Forensic Evidence and DNA Database System) Act 2014 or the Vehicle Registration Data (Automated Searching and Exchange) Act 2018 to the extent that the Act of 1988 is applied in those Acts.

(2) The Act of 1988 shall apply to-

(a) a complaint by an individual under section 10 of that Act made before the commencement of this section, and

(b) a contravention of that Act that occurred before such commencement.

(3) An investigation under section 10 of the Act of 1988 that was begun but not completed before the commencement of this section shall be completed in accordance with that Act and that Act shall apply to such an investigation.

PART 2

Data Protection Commission

Establishment day

9. The Minister shall, by order, appoint a day to be the establishment day for the purposes of this Act.

Establishment of Data Protection Commission

10. (1) On the establishment day there shall stand established a body to be known as An Coimisiún um Chosaint Sonraí or, in the English language, the Data Protection Commission (in this Act referred to as the “Commission”).

(2) Schedule 2 shall have effect in relation to the Commission.

Supervisory authority for Data Protection Regulation and Directive

11. The Commission shall be the supervisory authority within the meaning of, and for the purposes specified in-

(a) the Data Protection Regulation, and

(b) the Directive.

Functions of Commission

12. (1) In addition to the functions assigned to the Commission by virtue of its being the supervisory authority for the purposes of the Data Protection Regulation and the Directive, the general functions of the Commission shall include-

(a) any functions assigned to it by or under this Act,

(b) functions transferred to the Commission under section 14 , and

(c) such other functions as may be assigned to it from time to time by or under any other enactment.

(2) The Commission shall monitor the lawfulness of processing of personal data in accordance with-

(a) Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013⁵ on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), and

(b) Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013⁶ establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast).

(3) The Commission is designated for the purposes of Chapter IV (Mutual assistance) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data done at Strasbourg on the 28th day of January 1981.

(4) The Minister may, following consultation with the Commission, make any regulations that he or she considers necessary or expedient for the purpose of enabling Chapter IV (as referred to in subsection (3)) to have full effect.

(5) The Commission shall have all such powers as are necessary or expedient for the performance of its functions.

(6) The Commission shall disseminate, to such extent and in such manner as it considers appropriate, information in relation to the functions performed by it.

(7) The Commission shall be independent in the performance of its functions.

(8) Subject to this Act, the Commission shall regulate its own procedures.

Performance of functions of Commission by Commissioner or member of staff

13. (1) Where more than one Commissioner stands appointed under section 15, the functions of the Commission, other than the functions specified in subsection (3), may be performed through or by a Commissioner where he or she is authorised in that behalf by the Commission.

(2) The functions of the Commission, other than the functions specified in subsection (3), may be performed through or by any member of staff of the Commission where he or she is authorised in that behalf by the Commission.

(3) The functions referred to in subsections (1) and (2) are the functions of the Commission under sections 12 (8), 21, 28, 43, 84 (9) and (10), 129, 134 (1) and (4), 135 (1), 149 (other than subsection (1)), paragraph 1 of Schedule 2 and its function, as supervisory authority, under Article 35(4) and (5) of the Data Protection Regulation.

(4) A Commissioner or member of staff of the Commission who performs any of the functions of the Commission is presumed in any proceedings to have been authorised to do so on its behalf unless the contrary is shown.

Transfer of functions of Data Protection Commissioner to Commission

14. (1) All functions that, immediately before the establishment day, were vested in the Data Protection Commissioner are transferred to the Commission.

(2) A reference in any enactment or instrument under an enactment to the Data Protection Commissioner or to the Office of the Data Protection Commissioner shall be construed as a reference to the Commission.

(3) A reference in the Act of 1988 (other than in section 1(3)(c)(iii) in so far as it refers to the Commissioner of the Garda Síochána) to the Commissioner shall be construed as a reference to the Commission.

(4) This section shall come into operation on the establishment day.

Membership of Commission

15. (1) The Commission shall consist of such and so many members (not being more than 3) as the Government determines.

(2) Each member of the Commission shall be known as a Commissioner for Data Protection (in this Act referred to as a “Commissioner”).

(3) Subject to subsections (4), (8) and (9) and section 18 , a Commissioner shall be appointed by the Government on the recommendation of the Public Appointments Service and the appointment shall be for a period of not less than 4 and not more than 5 years from the date of his or her appointment.

(4) If, immediately before the establishment day, there is a person holding office as the Data Protection Commissioner, he or she shall, on the establishment day, be a Commissioner for the remainder of the term of office, and upon the same terms and conditions, for which he or she was appointed as the Data Protection Commissioner.

(5) Subject to subsection (7), the Public Appointments Service shall recommend a person for appointment as Commissioner following an open selection competition held by the Service for that purpose.

(6) The Public Appointments Service shall appoint a selection panel to assist it in holding an open selection competition.

(7) The Public Appointments Service shall ensure that a person is recommended under subsection (5) for appointment only if it is satisfied that the person has the qualifications, experience and skills necessary to enable the Commission to effectively perform its functions.

(8) A Commissioner to whom subsection (3) applies and whose term of office expires by the efflux of time may be reappointed to the Commission by the Government for one further period of not less than 4 and not more than 5 years without the need for a further recommendation by the Public Appointments Service.

(9) A Commissioner to whom subsection (4) applies and whose term of office expires by the efflux of time may be reappointed to the Commission by the Government for one further period of not less than 4 and not more than 5 years.

(10) A Commissioner shall-

(a) act on a full-time basis subject to such terms and conditions (other than the payment of remuneration and allowances for expenses) as the Government may determine,

(b) be paid by the Commission such remuneration and allowances for expenses (if any) as the Minister may, with the consent of the Minister for Public Expenditure and Reform, from time to time determine,

(c) not hold any other office or occupy any other position in respect of which emoluments are payable or carry on any business, and

(d) cease to be a Commissioner on reaching the age of 70 years, but where the person is a new entrant (within the meaning of section 2 of the Public Service Superannuation (Miscellaneous Provisions) Act 2004) the requirement to cease to be a Commissioner on grounds of age shall not apply.

Appointment of chairperson of Commission

16. (1) The Minister shall, where the Commission consists of more than one Commissioner, appoint one of the Commissioners to be chairperson and such allowance (if any) may be paid by the Commission to the chairperson as the Minister may, with the consent of the Minister for Public Expenditure and Reform, from time to time determine.

(2) The chairperson shall have a casting vote in the case of decisions to be taken by the Commission in the event of a tied vote.

(3) Where a chairperson stands appointed under subsection (1), and is unavailable to perform his or her duties due to absence or incapacity, the Minister shall appoint another existing Commissioner to act as chairperson for the duration of the period of absence or incapacity.

Resignation, removal, disqualification of Commissioner, ineligibility to become Commissioner

17. (1) A Commissioner may resign from office by giving notice in writing to the Government of his or her resignation and the resignation shall take effect from such date as is specified in the notice which date shall be at least 90 days after the giving of the notice to the Government.

(2) The Government may remove a Commissioner from office if they are satisfied that one or more of the grounds referred to in subsection (3) apply to the Commissioner.

(3) The grounds referred to in subsection (2) are that a Commissioner-

(a) has become incapable through ill health or otherwise of effectively performing the functions of the office, or

(b) has engaged in serious misconduct.

(4) Where the Government propose to remove a Commissioner under subsection (2), they shall notify the Commissioner concerned in writing of their proposal.

(5) A notification under subsection (4) shall include a statement-

(a) of the reasons for the proposed removal,

(b) that the Commissioner may, within a period of 30 working days from the sending of the notification or such other period as the Government may, having regard to the requirements of natural justice, specify in the notice, make representations to the Government in such form and manner as may be specified by the Government, as to why the Commissioner should not be removed from office, and

(c) that where no representations are received within the period referred to in paragraph (b) the Government will, without further notice to the Commissioner, proceed with the removal of the Commissioner from office in accordance with this section.

(6) In considering whether to remove a Commissioner from office under subsection (2), the Government shall take into account-

(a) any representations made by the Commissioner under subsection (5)(b) within the period referred to in that subsection, and

(b) any other matter the Government consider relevant for the purpose of their decision.

(7) Where, having taken into account the matters referred to in subsection (6), the Government decide the Commissioner should be removed from office in accordance with this section, they shall notify the Commissioner in writing of their decision and the reasons for their decision.

(8) Where the Government decide to remove a Commissioner from office in accordance with this section, they shall prepare a statement of the reason or reasons for such removal and cause that statement to be laid before each House of the Oireachtas as soon as practicable after the decision is made.

(9) A Commissioner shall cease to hold office if he or she-

(a) is convicted on indictment of an offence,

(b) is convicted of an offence involving fraud or dishonesty,

(c) has a declaration made against him or her under section 819 of the Act of 2014 or is deemed to be subject to such a declaration by virtue of Chapter 5 of Part 14 of that Act, or

(d) is subject to, or is deemed to be subject to, a disqualification order within the meaning of Chapter 4 of Part 14 of the Act of 2014 whether by virtue of that Chapter or of any other provision of that Act.

(10) A person shall not be eligible for appointment as a Commissioner if any of paragraphs (a) to (d) of subsection (9) are applicable in respect of the person.

Acting Commissioner

18. (1) Where one Commissioner only stands appointed for the time being under section 15 , the Minister may authorise a member of staff of the Commission to perform the functions of a Commissioner during any period when that Commissioner is absent from duty or absent from the State or is, for any other reason, unable to perform the functions of a Commissioner.

(2) Where a vacancy occurs in the office of Commissioner and no Commissioner stands appointed for the time being under section 15 , the Minister may authorise a member of staff of the Commission to perform the functions of a Commissioner during the period of that vacancy, but an authorisation under this subsection shall cease upon the appointment of a Commissioner under section 15 whether or not such appointment was made for the purpose of filling that vacancy.

(3) An authorisation under subsection (2) shall not remain in force for a period of more than 6 months unless the Minister is satisfied that it is not reasonably practicable for an appointment under section 15 to be made within that period, in which case he or she may extend that period by such further period as he or she is satisfied is a period within which it is reasonably practicable for an appointment to be made under that section.

(4) The Minister may at any time terminate an authorisation under this section.

(5) A member of staff of the Commission in respect of whom an authorisation under this section is in force may perform the functions of a Commissioner under this Act, and, for that purpose, references to a Commissioner in this Act (other than in sections 15 (3), 17 (2) to (8) and 22) shall be construed as including references to such member of staff.

Accountability of Commissioner to Oireachtas Committees

19. (1) In this section, "Committee" means a Committee appointed by either House of the Oireachtas or jointly by both Houses of the Oireachtas (other than a committee referred to in section 19 (1) of the Comptroller and Auditor General (Amendment) Act 1993 or the Committee on Members' Interests of Dáil Éireann or the Committee on Members' Interests of Seanad Éireann) or a sub-committee of such a Committee.

(2) Subject to subsection (3), a Commissioner shall, at the request in writing of a Committee, attend before it to give account for the general administration of the Commission.

(3) The Commissioner shall not be required to give account before a Committee for any matter which is or has been or may at a future time be the subject of proceedings before a court or tribunal.

(4) Where the Commissioner is of the opinion that a matter in respect of which he or she is requested to give an account before a Committee is a matter to which subsection (3) applies, he or she shall inform the Committee of that opinion and the reasons for the opinion and, unless the information is conveyed to the Committee at a time when the Commissioner is before it, the information shall be so conveyed in writing.

(5) Where the Commissioner has informed a Committee of his or her opinion in accordance with subsection (4) and the Committee does not withdraw the request referred to in subsection (2) in so far as it relates to a matter the subject of that opinion-

(a) the Commissioner may, not later than 21 days after being informed by the Committee of its decision not to do so, apply to the High Court in a summary manner for determination of the question whether the matter is one to which subsection (3) applies, or

(b) the Chairperson of the Committee may, on behalf of the Committee, make such an application, and the High Court shall determine the matter.

(6) Pending the determination of an application under subsection (5), the Commissioner shall not attend before the Committee to give account for the matter the subject of the application.

(7) If the High Court determines that the matter concerned is one to which subsection (3) applies, the Committee shall withdraw the request referred to in subsection (2), but if the High Court determines that subsection (3) does not apply, the Commissioner shall attend before the Committee and give account for the matter.

(8) In this section, a reference to "Commissioner" shall, where more than one Commissioner has been appointed under section 15, be taken to be a reference to the chairperson.

Assignment and transfer of staff to Commission

20. (1) Every civil servant who, immediately before the establishment day, stands assigned to act as a member of staff of the Data Protection Commissioner shall, on the establishment day, stand assigned to act as a member of staff of the Commission.

(2) The Minister may, as he or she considers appropriate, designate in writing such and so many persons who stand assigned under subsection (1) to act as members of staff of the Commission to become and be members of staff of the Commission on and from such date as the Minister may specify in the designation (in this section referred to as the "effective date").

(3) A member of staff designated in accordance with subsection (2) shall become and be a member of staff of the Commission on and from the effective date.

Staff of Commission

21. (1) The Commission may, subject to the approval of the Minister given with the consent of the Minister for Public Expenditure and Reform, appoint such number of persons to be members of its staff as it may determine.

(2) The Commission shall, subject to the approval of the Minister given with the consent of the Minister for Public Expenditure and Reform, determine the grades of members of its staff and the numbers in each grade.

(3) Members of staff of the Commission shall be civil servants.

Superannuation of Commissioners

22. (1) The Minister may, with the consent of the Minister for Public Expenditure and Reform, make a scheme or schemes for-

(a) the granting of superannuation benefits to or in respect of a Commissioner ceasing to hold office, or

(b) the making of contributions to a pension scheme approved of by the Minister with the consent of the Minister for Public Expenditure and Reform which has been entered into by the Commissioner.

(2) The Minister may, with the consent of the Minister for Public Expenditure and Reform, make a scheme amending or revoking a scheme made under subsection (1), including a scheme amended under this subsection.

(3) If any dispute arises as to the claim of a Commissioner to, or the amount of, any superannuation benefit payable in pursuance of a scheme made under subsection (1), such dispute shall be submitted to the Minister who shall refer it to the Minister for Public Expenditure and Reform for determination by him or her.

(4) A scheme made under subsection (1) shall be carried out by the Minister in accordance with its terms.

(5) No superannuation benefit shall be granted by the Minister to or in respect of any Commissioner ceasing to hold office otherwise than-

(a) in accordance with a scheme under subsection (1), or

(b) with the consent of the Minister for Public Expenditure and Reform.

(6) A scheme made under subsection (1) shall be laid before each House of the Oireachtas as soon as may be after it is made and, if a resolution annulling the scheme is passed by either such House within the next 21 days on which that House has sat after the scheme is laid before it, the scheme shall be annulled accordingly but without prejudice to the validity of anything previously done under that scheme prior to the resolution.

(7) In this section, “superannuation benefits” means pensions, gratuities and other allowances payable on resignation, retirement or death.

Accounts of Commission

23. (1) The Commission shall keep, in such form as may be approved by the Minister with the consent of the Minister for Public Expenditure and Reform, all proper and usual accounts of all money received or expended by it and, in particular, shall keep in such form as aforesaid all such special accounts as the Minister may, with the consent of the Minister for Public Expenditure and Reform, from time to time direct.

(2) Accounts kept in accordance with this section shall be submitted, not later than 1 April in the year immediately following the financial year to which they relate or on such earlier date as the Minister may from time to time specify, by the Commission to the Comptroller and Auditor General for audit and, immediately after the audit, a copy of the accounts, and of such other special accounts (if any) kept in accordance with this section as the Minister, after consultation with the Minister for Public Expenditure and Reform, may direct and a copy of the Comptroller and Auditor General’s report on the accounts shall be presented to the Minister and the Commission shall, as soon as may be thereafter, cause copies thereof to be laid before each House of the Oireachtas.

(3) Subject to subsections (4) and (5), subsections (1) and (2) shall cease to have effect on the date of the coming into operation of section 176 (b).

(4) Accounts kept in accordance with this section that relate to the period specified under subsection (5) shall be submitted by the Commission to the Comptroller and Auditor General for audit not later than 3 months after the date of the coming into operation of section 176 (b).

(5) The Minister may, for the purposes of subsection (4), specify a period which-

(a) shall end on the date immediately preceding the date of the coming into operation of section 176

(b), and

(b) may be longer or shorter than a financial year of the Commission.

Annual report

24. (1) The Commission shall, not later than 30 June in each year-

(a) prepare a report on its activities in the immediately preceding year, and

(b) cause copies of the report to be laid before each House of the Oireachtas.

(2) Notwithstanding subsection (1), if but for this subsection, the first report under this section would relate to a period of less than 6 months, the report shall relate to that period and to the year immediately following that period and shall be made as soon as may be, but not later than 6 months after the end of that year.

(3) The Commission may, at any time after subsection (1)(b) has been complied with, publish its annual report in such form and manner as it considers appropriate.

(4) For the purposes of the law of defamation, a report under subsection (1) shall be absolutely privileged.

Accountability for accounts of Commission

25. (1) The Commissioner, or where more than one Commissioner has been appointed under section 15, the chairperson, is the accounting officer in relation to the appropriation accounts of the Commission for the purpose of the Comptroller and Auditor General Acts 1866 to 1998.

(2) Section 19 (2) of the Comptroller and Auditor General (Amendment) Act 1993 shall, in so far as it relates to data protection matters, not apply to the Commissioner or chairperson who is the accounting officer pursuant to subsection (1).

Prohibition on disclosure of confidential information

26. (1) A relevant person shall not disclose confidential information obtained by him or her while performing functions under this Act or the Data Protection Regulation unless he or she is required or permitted by law, or duly authorised by the Commission, to do so.

(2) Subsection (1) shall not operate to prevent the disclosure by a relevant person of information-

(a) in a report to the Commission or a Commissioner,

(b) to a Minister of the Government, and

(c) to a public authority, whether in the State or otherwise, for the purposes of facilitating cooperation between the Commission and such authority in the performance of their respective functions.

(3) Subject to section 154 , a person who contravenes subsection (1) commits an offence and is liable on summary conviction to a class A fine.

(4) In this section-

“confidential information” includes information that is expressed by the Commission to be confidential either as regards particular information or as regards information of a particular class or description;

“relevant person” means-

(a) a Commissioner,

(b) a member of staff of the Commission,

(c) an authorised officer,

(d) any other person engaged under a contract for services by the Commission or a member of the staff of such a person, or

(e) a person who has acted in a capacity referred to in any of paragraphs (a) to (d).

Civil proceedings for contravention of section 26

27. (1) A person who suffers loss or harm as a result of a contravention of section 26 (1) may, subject to section 154 , bring proceedings against the person specified in subsection (2) seeking relief by way of-

(a) an injunction or declaration, or

(b) damages,

or both.

(2) The person specified for the purposes of subsection (1) is-

(a) where it is alleged that the contravention was committed by a Commissioner, member of staff of the Commission or an authorised officer and the applicant under that subsection is seeking an injunction or declaration, the Commissioner, member of staff or authorised officer concerned,

(b) where it is alleged that the contravention was committed by a Commissioner, member of staff of the Commission or an authorised officer and the applicant under that subsection is seeking damages, the Commission, and

(c) where it is alleged that the contravention was committed by a person other than a Commissioner, member of staff of the Commission or an authorised officer, that person.

(3) Proceedings under subsection (1), in so far as they seek the relief referred to in paragraph (b) of that subsection, shall be founded on tort.

PART 3

Data Protection Regulation

Chapter 1

General

Fees

28. The Commission may, with the consent of the Minister, prescribe the fees to be paid to it-

(a) for the performance of its functions under Article 57(1)(r) and (s), and

(b) in relation to requests that are manifestly unfounded or excessive in accordance with Article 57(4).

Child for purposes of application of Data Protection Regulation

29. For the purposes of the application of the Data Protection Regulation in the State, a reference to “child” in the Regulation shall be taken to be a reference to a person under the age of 18 years.

Micro-targeting and profiling of children

30. It shall be an offence under this Act for any company or corporate body to process the personal data of a child as defined by section 29 for the purposes of direct marketing, profiling or micro-targeting. Such an offence shall be punishable by an administrative fine under section 141.

Consent of child in relation to information society services

31. (1) The age of a child specified for the purposes of Article 8 is 16 years of age.

(2) For the purposes of the application of Article 8 in the State, the reference in that Article to “information society services” does not include a reference to preventative or counselling services.

(3) The Minister shall-

(a) not later than 3 years after the coming into operation of this section, commence a review of the operation of subsection (1), and

(b) complete that review not later than one year after its commencement.

Codes of conduct: children

32. (1) Without prejudice to the generality of Article 40, the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of the Data Protection Regulation with regard to-

- (a) the protection of children,
- (b) the information to be provided by a controller to children,
- (c) the manner in which the consent of the holders of parental responsibility over a child is to be obtained for the purposes of Article 8,
- (d) integrating the necessary safeguards into processing in order to protect the rights of children in an age-appropriate manner for the purpose of Article 25, and
- (e) the processing of the personal data of children for the purposes of direct marketing and creating personality and user profiles.

(2) For the purpose of considering whether a draft code of conduct or an extension or amendment to an existing code of conduct referred to in Article 40 provides sufficient appropriate safeguards referred to in that Article, the Commission may, where the draft, extension or amendment, as the case may be, concerns the application of the Data Protection Regulation to children, consult with such persons as it considers appropriate including-

- (a) children and bodies who appear to the Commission to represent the interests of children,
- (b) the holders of parental responsibility over children, and
- (c) the Ombudsman for Children.

Right to be forgotten: children

33. (1) Subject to subsection (3), in accordance with Article 17, a controller shall, at the request of a data subject, without undue delay erase personal data of the data subject where the data have been collected in relation to the offer to that data subject of information society services referred to in Article 8(1).

(2) Subject to subsection (3), where a controller has disclosed the personal data which are the subject of a request under subsection (1) to another controller or controllers, the first-mentioned controller shall, taking account of available technology and the cost of implementation, take all reasonable steps, including technical measures, to inform the other controller or controllers which are processing that

personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, that personal data.

(3) Subsections (1) and (2) shall not apply to the extent that the processing of the personal data concerned is necessary for the purposes set out in Article 17(3).

Designation of data protection officer

34. (1) The Minister may, following consultation with such other Minister of the Government as he or she considers appropriate and the Commission, make regulations requiring controllers, processors, associations or other bodies representing categories of controllers or processors to designate a data protection officer in accordance with Article 37(4).

(2) Regulations under subsection (1) may apply to-

(a) one or more than one class of controller,

(b) one or more than one class of processor, or

(c) one or more than one class of association or other body representing categories of controllers or processors.

(3) In making regulations under subsection (1) the Minister shall have regard to the need for the protection of individuals with regard to the processing of their personal data and, without prejudice to the generality of the foregoing, shall have regard in particular to-

(a) the nature, scope, context and purposes of the processing,

(b) risks arising for the rights and freedoms of individuals,

(c) the likelihood and the severity of such risk for the individuals concerned, and

(d) the costs of implementation of any requirement if it were imposed under that subsection.

Accreditation of certification bodies by Irish National Accreditation Board

35. The Irish National Accreditation Board is the accreditation body for the purposes of Article 43(1).

Suitable and specific measures for processing

36. (1) Where a requirement that suitable and specific measures be taken to safeguard the fundamental rights and freedoms of data subjects in processing personal data of those subjects is imposed by this Act or regulations made under this Act, those measures may include in particular the following-

- (a) explicit consent of the data subject for the processing of his or her personal data for one or more specified purposes,
- (b) limitations on access to the personal data undergoing processing within a workplace in order to prevent unauthorised consultation, alteration, disclosure or erasure of personal data,
- (c) strict time limits for the erasure of personal data and mechanisms to ensure that such limits are observed,
- (d) specific targeted training for those involved in processing operations, and
- (e) having regard to the state of the art, the context, nature, scope and purposes of data processing and the likelihood of risk to, and the severity of any risk to, the rights and freedoms of data subjects-
- (i) logging mechanisms to permit verification of whether and by whom the personal data have been consulted, altered, disclosed or erased,
- (ii) in cases in which it is not mandatory under the Data Protection Regulation, designation of a data protection officer,
- (iii) where the processing involves data relating to the health of a data subject, a requirement that the processing is undertaken by a person referred to in section 52 (2),
- (iv) pseudonymisation of the personal data, and
- (v) encryption of the personal data.

(2) Regulations may be made for either or both of the following purposes-

- (a) to identify additional suitable and specific measures (to those referred to in paragraphs (a) to (e) of subsection (1)) that may be taken to safeguard the fundamental rights and freedoms of data subjects in the processing of personal data of those subjects for the purposes of the requirement referred to in subsection (1),
- (b) to specify that a measure or measures referred to in paragraphs (a) to (e) of subsection (1) or an additional measure or measures identified under paragraph (a), or both, is or are mandatory in respect of the processing to which they are stated to apply.

(3) Without prejudice to the generality of subsection (2)(a), additional suitable and specific measures identified in regulations made under that subsection may relate to-

- (a) governance structures,
- (b) processes or procedures for risk assessment purposes,

(c) processes or procedures for the management and conduct of research projects, and

(d) other technical and organisational measures designed to ensure that the processing is carried out in accordance with the Data Protection Regulation and processes for testing and evaluating the effectiveness of such measures.

(4) Regulations under subsection (2) may-

(a) identify different measures for different categories of personal data, different categories of controllers, different types of processing or categories of processing, and

(b) specify that a measure or measures referred to in subsection (2)(b) is or are mandatory in respect of the processing of different categories of personal data, processing by different categories of controllers and in respect of different types of processing or categories of processing.

(5) Subject to subsection (6), regulations may be made under subsection (2)-

(a) by the Minister following consultation with such other Minister of the Government as he or she considers appropriate, or

(b) by any other Minister of the Government following consultation with the Minister and such other Minister of the Government as he or she considers appropriate.

(6) The Minister or any other Minister of the Government shall consult with the Commission before making regulations under subsection (2).

(7) The Commission may, on being consulted under subsection (6), make observations in writing on any matter which is of significant concern to it in relation to the proposed regulations and, if the Minister or any other Minister of the Government proposes to proceed to make the regulations notwithstanding that concern, that Minister shall, before making the regulations, give a written explanation as to why he or she is so proceeding to-

(a) the Committee established jointly by Dáil Éireann and Seanad Éireann known as the Committee on Justice and Equality or any Committee established to replace that Committee, and

(b) any other Committee (within the meaning of section 19 (1)) which that Minister considers appropriate having regard to the subject matter of the regulations.

(8) In making regulations under subsection (2), the Minister or any other Minister of the Government, as the case may be, shall have regard to the public interest and the need for protection of individuals with regard to the processing of their personal data and, without prejudice to the generality of the foregoing shall have regard to-

- (a) the nature, scope, context and purposes of the processing,
- (b) risks arising for the rights and freedoms of individuals, and
- (c) the likelihood and the severity of the risks for the individuals concerned.

Limitation on transfers of personal data outside the European Union

37. (1) The Minister may, in the absence of an adequacy decision under Article 45, following consultation with such other Minister of the Government as he or she considers appropriate and the Commission, make regulations restricting the transfer of categories of personal data to a third country or an international organisation for important reasons of public policy.

(2) Regulations under subsection (1) shall specify the important reasons of public policy for restricting the transfer concerned and may be expressed to apply by reference to one or more of the following-

- (a) a category or categories of personal data,
- (b) a third country or classes of third country, or
- (c) an international organisation.

(3) In making regulations under subsection (1), the Minister shall have regard to the public interest and the need for protection of individuals with regard to the processing of their personal data and, without prejudice to the generality of the foregoing, shall in particular have regard to-

- (a) the nature, scope, context and purposes of the processing,
- (b) the desirability of facilitating international transfers of data,
- (c) risks arising for the rights and freedoms of individuals, and
- (d) the likelihood and the severity of such risks for individuals concerned.

Processing for a task carried out in the public interest or in the exercise of official authority

38. (1) The processing of personal data shall be lawful to the extent that such processing is necessary and proportionate for-

- (a) the performance of a function of a controller conferred by or under an enactment or by the Constitution, or
- (b) the administration by or on behalf of a controller of any non-statutory scheme, programme or funds where the legal basis for such administration is a function of a controller conferred by or under an enactment or by the Constitution.

(2) Subject to subsection (3), the processing of personal data and disclosure of that data to a person for the purposes of preserving the Common Travel Area, or any part of that Area, shall be lawful where the controller is an Irish air carrier, an air carrier or a sea carrier.

(3) The Minister shall, following consultation with such other Minister of the Government as he or she considers appropriate and the Commission, make regulations for the purposes of subsection (2) specifying-

(a) the part of the Common Travel Area to which the regulations apply,

(b) the personal data that may be processed,

(c) the circumstances in which the personal data may be disclosed, including specifying the person to whom the data may be disclosed, and

(d) such other conditions (if any) as the Minister considers appropriate to impose on such processing.

(4) Subject to subsection (5), the processing of personal data which is necessary for the performance of a task carried out in the public interest by a controller or which is necessary in the exercise of official authority vested in a controller may be specified in regulations made-

(a) by the Minister following consultation with such other Minister of the Government as he or she considers appropriate, or

(b) by any other Minister of the Government following consultation with the Minister and such other Minister of the Government as he or she considers appropriate.

(5) The Minister or any other Minister of the Government shall consult with the Commission before making regulations under subsection (4).

(6) The Commission may, on being consulted under subsection (5), make observations in writing on any matter which is of significant concern to it in relation to the proposed regulations and, if the Minister or any other Minister of the Government proposes to proceed to make the regulations notwithstanding that concern, that Minister shall, before making the regulations, give a written explanation as to why he or she is so proceeding to-

(a) the Committee established jointly by Dáil Éireann and Seanad Éireann known as the Committee on Justice and Equality or any Committee established to replace that Committee, and

(b) any other Committee (within the meaning of section 19 (1)) which that Minister considers appropriate having regard to the subject matter of the regulations.

(7) Regulations made under subsection (4) shall specify-

(a) the personal data that may be processed,

(b) the circumstances in which the personal data may be processed, including specifying the persons to whom the data may be disclosed, and

(c) such other conditions (if any) as the Minister or any other Minister of the Government, as the case may be, considers appropriate to impose on such processing.

(8) In this section-

“air carrier” means an undertaking established in the State that provides air services;

“air service” has the meaning it has in Regulation (EC) No. 1008/2008 of the European Parliament and of the Council of 24 September 2008 on common rules for the operation of air services in the Community (Recast);

“Common Travel Area” means the State, the United Kingdom of Great Britain and Northern Ireland, the Channel Islands and the Isle of Man;

“Irish air carrier” means an undertaking with a valid operating licence, within the meaning of Regulation (EC) No. 1008/2008 of the European Parliament and of the Council of 24 September 2008, granted by the Commission for Aviation Regulation;

“passenger” means a person carried by an air carrier on an aircraft, or as the case may be, a sea carrier in a passenger ship, other than a member of the crew of the aircraft or passenger ship concerned;

“passenger ship” means a sea-going ship that carries more than 12 passengers;

“sea carrier” means an undertaking established in the State that, for remuneration, carries passengers by sea in a passenger ship.

Communication with data subjects by political parties, candidates for and holders of certain elective political offices

39. (1) A specified person may, in the course of that person’s electoral activities in the State, use the personal data of a data subject for the purpose of communicating in writing (including by way of newsletter or circular) with the data subject.

(2) Communicating in accordance with subsection (1) shall, for the purposes of Article 6(1)(e), be considered to be the performance of a task carried out in the public interest.

(3) In this section, “specified person” means-

(a) a political party,

(b) a member of either House of the Oireachtas, the European Parliament or a local authority, or

(c) a candidate for election to the office of President of Ireland or for membership of either House of the Oireachtas, the European Parliament or a local authority.

(4) In this section and in sections 48 , 58 and 59 , “electoral activities” includes the dissemination of information, including information as to a person’s activities and policies, that might reasonably be of interest to electors.

Processing of personal data and special categories of personal data by elected representatives

40. (1) For the purpose of enabling an elected representative to perform his or her functions as such a representative, the processing of personal data and special categories of personal data of a data subject by or on behalf of that representative shall be lawful where he or she receives a request or representation from the data subject or where, in accordance with subsection (2), he or she receives a request or representation from another person on behalf of the data subject.

(2) A person may make a request or representation on behalf of a data subject where the data subject-

(a) has given his or her consent to the making of the request or representation, as the case may be, or

(b) is, by reason of his or her physical or mental incapacity or age, unable to make a request or representation on his or her own behalf.

(3) In processing special categories of personal data under subsection (1), an elected representative shall impose limitations on access to that data to prevent unauthorised consultation, alteration, disclosure or erasure of that data.

(4) For the purpose referred to in subsection (1) and to the extent that disclosure is necessary and proportionate to enable an elected representative to deal with a request or representation referred to in that subsection, subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of the data subject, it shall be lawful for a person to disclose to the representative or a person acting on his or her behalf personal data and special categories of personal data of a data subject who makes the request or representation, or on whose behalf the request or representation is made, as the case may be, to enable that representative respond to that request or representation.

(5) In this section, “elected representative” means-

(a) a member of either House of the Oireachtas,

(b) a member of the European Parliament,

(c) a member of a local authority.

Processing for purpose other than purpose for which data collected

41. Without prejudice to the processing of personal data for a purpose other than the purpose for which the data has been collected which is lawful under the Data Protection Regulation, the processing of personal data and special categories of personal data for a purpose other than the purpose for which the data has been collected shall be lawful to the extent that such processing is necessary and proportionate for the purposes-

(a) of preventing a threat to national security, defence or public security,

(b) of preventing, detecting, investigating or prosecuting criminal offences, or

(c) set out in paragraph (a) or (b) of section 47 .

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

42. (1) Subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, personal data may be processed, in accordance with Article 89, for-

(a) archiving purposes in the public interest,

(b) scientific or historical research purposes, or

(c) statistical purposes.

(2) Processing of personal data for the purposes referred to in subsection (1) shall respect the principle of data minimisation.

(3) Where the purposes referred to in paragraph (a), (b) or (c) of subsection (1) can be fulfilled by processing which does not permit, or no longer permits, identification of data subjects, the processing of information for such purposes shall be fulfilled in that manner.

Data processing and freedom of expression and information

43. (1) The processing of personal data for the purpose of exercising the right to freedom of expression and information, including processing for journalistic purposes or for the purposes of academic, artistic or literary expression, shall be exempt from compliance with a provision of the Data Protection Regulation specified in subsection (2) where, having regard to the importance of the right of freedom

of expression and information in a democratic society, compliance with the provision would be incompatible with such purposes.

(2) The provisions of the Data Protection Regulation specified for the purposes of subsection (1) are Chapter II (principles), other than Article 5(1)(f), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries and international organisations), Chapter VI (independent supervisory authorities) and Chapter VII (cooperation and consistency).

(3) The Commission may, on its own initiative, refer any question of law which involves consideration of whether processing of personal data is exempt in accordance with subsection (1) to the High Court for its determination.

(4) An appeal shall, by leave of the High Court, lie from a determination of that Court on a question of law under subsection (3) to the Court of Appeal.

(5) In order to take account of the importance of the right to freedom of expression and information in a democratic society that right shall be interpreted in a broad manner.

Data processing and public access to official documents

44. (1) For the purposes of Article 86, personal data contained in a record may be disclosed where a request for access to the record is granted under and in accordance with the Act of 2014 pursuant to an FOI request.

(2) For the purposes of Article 86, personal data contained in environmental information may be disclosed where the information is made available under and in accordance with the Access to Information on the Environment Regulations pursuant to a request within the meaning of those Regulations.

(3) In this section-

“Access to Information on the Environment Regulations” means the European Communities (Access to Information on the Environment) Regulations 2007 (S.I. No. 133 of 2007);

“Act of 2014” means the Freedom of Information Act 2014 ;

“environmental information” has the same meaning as it has in the Access to Information on the Environment Regulations;

“FOI request” has the same meaning as it has in the Act of 2014;

“record” has the same meaning as it has in the Act of 2014.

Chapter 2

Processing of special categories of personal data and processing of personal data relating to criminal convictions and offences

Processing of special categories of personal data

45. Subject to compliance with the Data Protection Regulation and any other relevant enactment or rule of law, the processing of special categories of personal data shall be lawful to the extent the processing is-

- (a) authorised by section 41 and sections 46 to 54 , or
- (b) otherwise authorised by Article 9.

Processing of special categories of personal data for purposes of employment and social welfare law

46. Subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, the processing of special categories of personal data shall be lawful where the processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the controller or the data subject in connection with employment or social welfare law.

Processing of special categories of personal data for purpose of legal advice and legal proceedings

47. The processing of special categories of personal data shall be lawful where the processing-

- (a) is necessary for the purposes of providing or obtaining legal advice or for the purposes of, or in connection with, legal claims, prospective legal claims, legal proceedings or prospective legal proceedings, or
- (b) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Processing of personal data revealing political opinions for electoral activities and functions of Referendum Commission

48. Subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, the processing of personal data revealing political opinions shall be lawful where the processing is carried out-

(a) in the course of electoral activities in the State for the purpose of compiling data on peoples' political opinions by-

(i) a political party, or

(ii) a candidate for election to, or a holder of, elective political office in the State,

and

(b) by the Referendum Commission in the performance of its functions.

Processing of special categories of personal data for purposes of administration of justice and performance of functions

49. Subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, the processing of special categories of personal data shall be lawful where the processing respects the essence of the right to data protection and is necessary and proportionate for-

(a) the administration of justice, or

(b) the performance of a function conferred on a person by or under an enactment or by the Constitution.

Processing of special categories of personal data for insurance and pension purposes

50. Subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, the processing of data concerning health shall be lawful where the processing is necessary and proportionate for the purposes of the following:

(a) a policy of insurance or life assurance,

(b) a policy of health insurance or health-related insurance,

(c) an occupational pension, a retirement annuity contract or any other pension arrangement, or

(d) the mortgaging of property.

Processing of special categories of personal data and Article 10 data for reasons of substantial public interest

51. (1) Processing of special categories of personal data shall be lawful where the processing is carried out in accordance with regulations made under subsection (3).

(2) Article 10 data may be processed where the processing is carried out in accordance with regulations made under subsection (3).

(3) Regulations may be made authorising the processing, where necessary for reasons of substantial public interest, of either or both of the following-

(a) special categories of personal data, and

(b) without prejudice to the Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016 , Article 10 data.

(4) Without prejudice to the generality of subsection (3), regulations made under that subsection shall identify-

(a) the substantial public interest concerned, and

(b) the suitable and specific measures to be taken to safeguard the fundamental rights and freedoms of data subjects in processing the personal data which is authorised by the regulations.

(5) For the purposes of subsection (4)(b), subsections (2) to (8) of section 36 shall apply in like manner to regulations made under subsection (3) as they apply to regulations made under section 36 .

(6) Regulations may be made under subsection (3) by-

(a) the Minister, following consultation with such other Minister of the Government as he or she considers appropriate and the Commission, or

(b) any other Minister of the Government following consultation with the Minister, such other Minister of the Government as he or she considers appropriate and the Commission.

(7) The Minister or any other Minister of the Government, as the case may be, making regulations under subsection (3) shall have regard to the need for the protection of individuals with regard to the processing of their personal data, and without prejudice to the generality of that need, have regard to-

(a) the nature, scope and purposes of the processing,

(b) the nature of the substantial public interest concerned,

(c) any benefits likely to arise for the data subjects concerned,

(d) any risks arising for the rights and freedoms of such subjects, and

(e) the likelihood of any such risks arising and the severity of such risks.

(8) Regulations made under subsection (3) shall-

(a) respect the essence of the right to data protection, and

(b) enable processing of such data only in so far as is necessary and proportionate to the aim sought to be achieved.

(9) In this section, "Article 10 data" has the meaning assigned to it by section 55 .

Processing of special categories of personal data for purposes of Article 9(2)(h)

52. (1) Subject to subsection (2) and to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, the processing of special categories of personal data shall be lawful where it is necessary-

(a) for the purposes of preventative or occupational medicine,

(b) for the assessment of the working capacity of an employee,

(c) for medical diagnosis,

(d) for the provision of medical care, treatment or social care,

(e) for the management of health or social care systems and services, or

(f) pursuant to a contract with a health practitioner.

(2) Processing shall be lawful in accordance with subsection (1) where it is undertaken by or under the responsibility of-

(a) a health practitioner, or

(b) a person who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that which would exist if that person were a health practitioner.

(3) In this section, "health practitioner" has the same meaning as it has in the Health Identifiers Act 2014 .

Processing of special categories of personal data for purposes of public interest in the area of public health

53. Subject to suitable and specific measures to safeguard the fundamental rights and freedoms of data subjects, the processing of special categories of personal data shall be lawful where it is necessary for public interest reasons in the area of public health including-

(a) protecting against serious cross-border threats to health, and

(b) ensuring high standards of quality and safety of health care and of medicinal products and medical devices.

Processing of special categories of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

54. Subject to compliance with section 42 , the processing of special categories of personal data is lawful where such processing is necessary and proportionate for-

- (a) archiving purposes in the public interest,
- (b) scientific or historical research purposes, or
- (c) statistical purposes.

Processing of personal data relating to criminal convictions and offences

55. (1) Without prejudice to the Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016 and subject to compliance with Article 6(1) and to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of the data subject, personal data referred to in Article 10 (in this section referred to as “Article 10 data”) may be processed-

- (a) under the control of official authority, or
- (b) where-
 - (i) the data subject has given explicit consent to the processing for one or more specified purposes except where the law of the European Union or the law of the State prohibits such processing,
 - (ii) processing is necessary and proportionate for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract,
 - (iii) processing is-
 - (I) necessary for the purpose of providing or obtaining legal advice or for the purposes of, or in connection with, legal claims, prospective legal claims, legal proceedings or prospective legal proceedings, or
 - (II) otherwise necessary for the purposes of establishing, exercising or defending legal rights,
 - (iv) processing is necessary to prevent injury or other damage to the data subject or another person or loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or another person, or

(v) processing is permitted in regulations made under subsection (3) or is otherwise authorised by the law of the State.

(2) Processing under the control of official authority referred to in subsection (1)(a) includes processing required for the following purposes:

(a) the administration of justice;

(b) the exercise of a regulatory, authorising or licensing function or determination of eligibility for benefits or services;

(c) protection of the public against harm arising from dishonesty, malpractice, breaches of ethics or other improper conduct by, or the unfitness or incompetence of, persons who are or were authorised to carry on a profession or other activity;

(d) enforcement actions aimed at preventing, detecting or investigating breaches of the law of the European Union or the law of the State that are subject to civil or administrative sanctions;

(e) archiving in the public interest, scientific or historical research purposes or statistical purposes where the processing is carried out in accordance with section 42 for those purposes by or on behalf of a public authority or public body.

(3) Without prejudice to the Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016 and subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of the data subject and subject to subsection (7), regulations may be made permitting the processing of Article 10 data where the processing is necessary and proportionate to-

(a) assess the risk of fraud or prevent fraud,

(b) assess the risk of bribery or corruption, or both, or to prevent bribery or corruption, or both, or

(c) ensure network and information systems security, and prevent attacks on and damage to computer and electronic communications systems.

(4) Subject to subsection (5), regulations may be made under subsection (3)-

(a) by the Minister following consultation with such other Minister of the Government as he or she considers appropriate, or

(b) by any other Minister of the Government following consultation with the Minister and such other Minister of the Government as he or she considers appropriate.

(5) The Minister or any other Minister of the Government shall consult with the Commission before making regulations under subsection (3).

(6) The Commission may, on being consulted under subsection (5), make observations in writing on any matter which is of significant concern to it in relation to the proposed regulations and, if the Minister or any other Minister of the Government proposes to proceed to make the regulations notwithstanding that concern, that Minister shall, before making the regulations, give a written explanation as to why he or she is so proceeding to-

(a) the Committee established jointly by Dáil Éireann and Seanad Éireann known as the Committee on Justice and Equality or any Committee established to replace that Committee, and

(b) any other Committee (within the meaning of section 19 (1)) which that Minister considers appropriate having regard to the subject matter of the regulations.

(7) The Minister or any other Minister of the Government, as the case may be, making regulations under subsection (3) shall have regard to the need for the protection of individuals with regard to the processing of their personal data and without prejudice to the generality of that need, have regard to-

(a) the nature, scope and purposes of the processing,

(b) any risks arising for the rights and freedoms of individuals, and

(c) the likelihood of any such risks arising and the severity of such risks.

(8) A person who knowingly or recklessly contravenes this section or any regulations made under subsection (3) shall be guilty of an offence and shall be liable-

(a) on summary conviction to a class A fine or imprisonment for a term not exceeding 12 months or both, or

(b) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both.

(9) In this section, "Article 10 data" shall include personal data relating to the alleged commission of an offence and any proceedings in relation to such an offence.

Chapter 3

Rights, and restrictions of rights, of data subject and restrictions on obligations of controllers

Right of access to results and scripts of examination and results of appeal

56. (1) Subject to subsection (3), a request by a data subject under Article 15 in relation to the result of an examination at which he or she was a candidate, or in relation to a script completed by him or her in the course of such an examination shall, for the purposes of that Article, be taken to have been made on the later of-

(a) the date of the first publication of the results of the examination, or

(b) the date of the request.

(2) A request by a data subject under Article 15 in relation to the result of an appeal by the data subject against the result of an examination at which he or she was a candidate shall, for the purposes of that Article, be taken to have been made on the later of-

(a) the date of the first publication of the results of the appeal, or

(b) the date of the request.

(3) Where-

(a) a request by a data subject referred to in subsection (1) relates to a script completed by him or her in the course of an examination in the Leaving Certificate Examinations conducted by the State Examinations Commission, and

(b) the data subject, whether before or after the making of that request, appeals the result of the examination referred to in paragraph (a),

that request shall be taken to have been made on the date of the first publication of the results of the appeal referred to in paragraph (b).

(4) In this section-

“appeal” means any formal process to enable a candidate to request a recheck of an examination result which is specified by a person who operates the examination;

“examination” means any process for determining the knowledge, intelligence, skill or ability of a person by reference to his or her performance in any test, work or other activity;

“script” means any work produced by a candidate as part of an examination including any examination answer-book (whether in written or digital form), journal, portfolio, audio and visual recording, practical piece or artefact and, for the purposes of this definition, shall be deemed to include-

(a) an audio or visual recording, produced in the course of an examination, of the performance of the candidate in the examination, and

(b) any marks or comments added to the script, or made in relation to the script, by an examiner in the course of his or her marking of the script.

Rights in relation to automated decision making

57. (1) Subject to Article 22(4) and to suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject, for the purposes of Article 22(2)(b), the right of a data subject not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her shall, in addition to the grounds identified in Article 22(2)(a) and (c), not apply where-

(a) the decision is authorised or required by or under an enactment, and

(b) either-

(i) the effect of that decision is to grant a request of the data subject, or

(ii) in all other cases (where subparagraph (i) is not applicable), adequate steps have been taken by the controller to safeguard the legitimate interests of the data subject which steps shall include the making of arrangements to enable him or her to-

(I) make representations to the controller in relation to the decision,

(II) request human intervention in the decision-making process,

(III) request to appeal the decision.

(2) In the case of requests made under subsection (1)(b)(ii)(II) or (III) the controller shall-

(a) comply with the request, and

(b) notify the data subject in writing of-

(i) the steps taken to comply with the request, and

(ii) in the case of an appeal under subsection (1)(b)(ii)(III), the outcome of the appeal.

Direct marketing for purposes of Article 21

58. For the purposes of the application of Article 21 in the State, the reference to “direct marketing” includes a reference to direct mailing other than direct mailing carried out-

(a) in the course of electoral activities in the State by-

- (i) a political party or its members, or
 - (ii) a candidate for election to, or a holder of, elective political office in the State,
- and
- (b) by the Referendum Commission in the performance of its functions.

Restriction on right of data subject to object to processing for election purposes and processing by Referendum Commission

59. The right of a data subject to object at any time to the processing of personal data concerning him or her under Article 21 shall not apply to processing carried out-

- (a) in the course of electoral activities in the State by-
 - (i) a political party, or
 - (ii) a candidate for election to, or a holder of, elective political office in the State,
- and
- (b) by the Referendum Commission in the performance of its functions.

Restrictions on obligations of controllers and rights of data subjects for important objectives of general public interest

60. (1) The rights and obligations provided for in Articles 12 to 22 and Article 34, and Article 5 in so far as any of its provisions correspond to the rights and obligations in Articles 12 to 22-

- (a) are restricted to the extent specified in subsection (3), and
 - (b) may be restricted in regulations made under subsections (5) or (6).
- (2) Subsection (1) is without prejudice to any other enactment or rule of law which restricts the rights and obligations referred to in that subsection.
- (3) Subject to subsection (4), the rights and obligations referred to in subsection (1) are restricted to the extent that-
- (a) the restrictions are necessary and proportionate-
 - (i) to safeguard cabinet confidentiality, parliamentary privilege, national security, defence and the international relations of the State,
 - (ii) for the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties,

(iii) for the administration of any tax, duty or other money due or owing to the State or a local authority in any case in which the non-application of the restrictions concerned would be likely to prejudice the aforementioned administration,

(iv) in contemplation of or for the establishment, exercise or defence of, a legal claim, prospective legal claim, legal proceedings or prospective legal proceedings whether before a court, statutory tribunal, statutory body or an administrative or out-of-court procedure,

(v) for the enforcement of civil law claims, including matters relating to any liability of a controller or processor in respect of damages, compensation or other liabilities or debts related to the claim, or

(vi) for the purposes of estimating the amount of the liability of a controller on foot of a claim for the payment of a sum of money, whether in respect of damages or compensation, in any case in which the application of those rights or obligations would be likely to prejudice the commercial interests of the controller in relation to the claim,

(b) the personal data relating to the data subject consist of an expression of opinion about the data subject by another person given in confidence or on the understanding that it would be treated as confidential to a person who has a legitimate interest in receiving the information, or

(c) the personal data concerned are kept-

(i) by the Commission for the performance of its functions,

(ii) by the Information Commissioner for the performance of his or her functions, or

(iii) by the Comptroller and Auditor General for the performance of his or her functions.

(4) The Minister may prescribe requirements to be complied with when the rights and obligations referred to in subsection (1) are restricted in accordance with subsection (3).

(5) Subject to subsection (9), regulations may be made by a Minister of the Government where he or she considers it necessary for the protection of a data subject or the rights and freedoms of others restricting the rights and obligations referred to in subsection (1)-

(a) (i) if the application of those rights and obligations would be likely to cause serious harm to the physical or mental health of the data subject, and

(ii) to the extent to which, and for as long as, such application would be likely to cause such serious harm,

and

(b) in relation to personal data kept for, or obtained in the course of, the carrying out of social work by a public authority, public body, a voluntary organisation or other body.

(6) Subject to subsection (9), regulations may be made restricting the rights and obligations referred to in subsection (1) where such restrictions are necessary for the purposes of safeguarding important objectives of general public interest and such regulations shall include, where appropriate, specific provisions required by Article 23(2).

(7) Important objectives of general public interest referred to in subsection (6) include:

(a) preventing threats to public security and public safety;

(b) avoiding obstructions to any official or legal inquiry, investigation or process, including any out-of-court redress procedure, proceedings pending or due before a court, tribunal of inquiry or commission of investigation;

(c) preventing, detecting, investigating and prosecuting breaches of discipline by, or the unfitness or incompetence of, persons who are or were authorised by law to carry on a profession or any other regulated activity and the imposition of sanctions for same;

(d) preventing, detecting, investigating or prosecuting breaches of ethics for regulated professions;

(e) taking any action for the purposes of considering and investigating a complaint made to a regulatory body in respect of a person carrying out a profession or other regulated activity where the profession or activity is regulated by that body and the imposition of sanctions on foot of such a complaint;

(f) preventing, detecting, investigating or prosecuting, whether in the State or elsewhere, breaches of the law which are subject to civil or administrative sanctions and enforcing such sanctions;

(g) the identification of assets which are derived from, or are suspected to derive from, criminal conduct and the taking of appropriate action to deprive or deny persons of those assets or the benefits of those assets and any investigation or preparatory work in relation to any related proceedings;

(h) ensuring the effective operation of the immigration system, the system for granting persons international protection in the State and the system for the acquisition by persons of Irish citizenship, including by preventing, detecting and investigating abuses of those systems or breaches of the law relating to those systems;

(i) safeguarding the economic or financial interests of the European Union or the State, including on monetary, budgetary and taxation matters;

(j) safeguarding monetary policy, the smooth operation of payment systems, the resolution of regulated financial service providers (within the meaning of the Central Bank Act 1942), the operation of deposit-guarantee schemes, the protection of consumers and the effective regulation of financial service providers (within the meaning of the Central Bank Act 1942);

(k) protecting members of the public against-

(i) financial loss or detriment due to the dishonesty, malpractice or other improper conduct of, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate or other entities,

(ii) financial loss or detriment due to the conduct of individuals who have been adjudicated bankrupt, or

(iii) financial loss or detriment due to the conduct of individuals who have been involved in the management of a body corporate which has been the subject of a receivership, examinership or liquidation under the Act of 2014;

(l) protecting-

(i) the health, safety, dignity, well-being of individuals at work against risks arising out of or in connection with their employment, and

(ii) members of the public against discrimination or unfair treatment in the provision of goods or services to them;

(m) the keeping of public registers for reasons of general public interest, whether the registers are accessible to the public on a general or restricted basis;

(n) safeguarding the integrity and security of examinations systems;

(o) safeguarding public health, social security, social protection and humanitarian activities.

(8) Where the rights and obligations referred to in subsection (1) are restricted in regulations made under subsection (6) on the basis of important objectives of general public interest of the State, other than the objectives referred to in subsection (7), the important objective or objectives of general public interest shall be identified in those regulations.

(9) Subject to subsection (10), regulations may be made under subsection (5) or (6)-

(a) by the Minister following consultation with such other Minister of the Government as he or she considers appropriate, or

(b) by any other Minister of the Government following consultation with the Minister and such other Minister of the Government as he or she considers appropriate.

(10) The Minister or any other Minister of the Government shall consult with the Commission before making regulations under subsection (5) or (6).

(11) The Commission may, on being consulted under subsection (10), make observations in writing on any matter which is of significant concern to it in relation to the proposed regulations and, if the Minister or any other Minister of the Government proposes to proceed to make the regulations notwithstanding that concern, that Minister shall, before making the regulations, give a written explanation as to why he or she is so proceeding to-

(a) the Committee established jointly by Dáil Éireann and Seanad Éireann known as the Committee on Justice and Equality or any Committee established to replace that Committee, and

(b) any other Committee (within the meaning of section 19 (1)) which that Minister considers appropriate having regard to the subject matter of the regulations.

(12) Regulations made under this section shall-

(a) respect the essence of the right to data protection and protect the interests of the data subject, and

(b) restrict the exercise of data subjects' rights only in so far as is necessary and proportionate to the aim sought to be achieved.

Restriction on exercise of data subjects' rights: archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

61. (1) Subject to subsection (3), where processing of data is for archiving purposes in the public interest, the rights of a data subject set out in Articles 15, 16, 18, 19, 20 and 21 are restricted to the extent that-

(a) the exercise of any of those rights would be likely to render impossible, or seriously impair, the achievement of those purposes, and

(b) such restriction is necessary for the fulfilment of those purposes.

(2) Subject to subsection (4), where processing of data is for scientific or historical research purposes or statistical purposes, the rights of a data subject set out in Articles 15, 16, 18 and 21 are restricted to the extent that-

(a) the exercise of any of those rights would be likely to render impossible, or seriously impair, the achievement of those purposes, and

(b) such restriction is necessary for the fulfilment of those purposes.

(3) Where data is being processed for purposes referred to in subsection (1) and the processing serves another purpose at the same time, that subsection applies only to the extent that the processing relates to the purposes referred to in that subsection.

(4) Where data is being processed for purposes referred to in subsection (2) and the processing serves another purpose at the same time, that subsection applies only to the extent that the processing relates to the purposes referred to in that subsection.

PART 4

Provisions Consequent on Repeal of Certain Provisions of Data Protection Act 1988

Transfer of property of Data Protection Commissioner to Commission

62. (1) On the establishment day, all property (other than land), including choses-in-action, that immediately before that day was vested in the Data Protection Commissioner shall stand vested in the Commission.

(2) Every chose-in-action vested in the Commission by virtue of subsection (1) may, on and from the establishment day, be sued on, recovered or enforced by the Commission in its own name, and it shall not be necessary for the Commission to give notice to any person bound by the chose-in-action of the vesting effected by that subsection.

(3) On the establishment day all records that, immediately before that day, were records of the Data Protection Commissioner shall be records of the Commission and shall, accordingly, be transferred to the Commission.

Transfer of rights and liabilities of Data Protection Commissioner to Commission

63. (1) All rights and liabilities of the Data Protection Commissioner subsisting immediately before the establishment day and arising by virtue of any contract or commitment (express or implied) shall on that day stand transferred to the Commission.

(2) Every right and liability transferred by subsection (1) to the Commission may, on and after the establishment day, be sued on, recovered or enforced by or against the Commission in its own name, and it shall not be necessary for the Commission to give notice to the person whose right or liability is transferred by that subsection of such transfer.

Liability for loss occurring before establishment day

64. (1) A claim in respect of any loss or injury alleged to have been suffered by any person arising out of the performance before the establishment day of any of the functions of the Data Protection Commissioner shall after that day, lie against the Commission and not against the Data Protection Commissioner.

(2) Any legal proceedings pending immediately before the establishment day to which the Data Protection Commissioner is a party, shall be continued, with the substitution in the proceedings of the Commission for the Data Protection Commissioner.

(3) Where, before the establishment day, agreement has been reached between the parties concerned in settlement of a claim to which subsection (1) relates, the terms of which have not been implemented, or judgment in such a claim has been given in favour of a person but has not been enforced, the terms of the agreement or judgment, as the case may be, shall, in so far as they are enforceable against the Data Protection Commissioner, be enforceable against the Commission and not the Data Protection Commissioner.

(4) Any claim made or proper to be made by the Data Protection Commissioner in respect of any loss or injury arising from the act or default of any person before the establishment day shall be regarded as having been made by or proper to be made by the Commission and may be pursued and sued for by the Commission as if the loss or injury had been suffered by the Commission.

Provisions consequent upon transfer of functions, assets, rights and liabilities to Commission

65. (1) Anything commenced and not completed before the establishment day by or under the authority of the Data Protection Commissioner may, in so far as it relates to a function transferred to the Commission under section 14 , be carried on or completed on or after the establishment day by the Commission.

(2) Every instrument made under an enactment and every document (including any certificate or notice) granted, made or issued, in the performance of a function transferred by section 14 , shall, if and in so far as it was operative immediately before the establishment day, have effect on and after that day as if it had been granted, made or issued by the Commission.

(3) References to the Data Protection Commissioner in the memorandum or articles of association of any company shall, on and after the establishment day, be construed as references to the Commission.

(4) A certificate signed by the Minister that any property, right or liability has or, as the case may be, has not vested in the Commission under section 62 or 63 shall be sufficient evidence, unless the contrary is shown, of the fact so certified for all purposes.

Final accounts and final annual report of Data Protection Commissioner

66. (1) The Commission shall, in respect of the period specified under subsection (3), prepare final accounts of the Data Protection Commissioner.

(2) The Commission shall submit the final accounts to the Comptroller and Auditor General for audit not later than 3 months after the establishment day.

(3) For the purposes of subsection (1), the Minister may specify a period that is longer or shorter than a financial year of the Data Protection Commissioner.

(4) The Commission shall prepare the final annual report for the Data Protection Commissioner and cause a copy of the report to be laid before each House of the Oireachtas not later than 6 months after the establishment day.

Saver for scheme relating to superannuation

67. A scheme made under section 9 and paragraph 7(a) of the Second Schedule to the Act of 1988 that was in force immediately prior to coming into operation of section 7 in so far as it relates to the repeal of section 9 and paragraph 7(a) of the Second Schedule to the Act of 1988 shall continue in force on and after that coming into operation as if the scheme had been made under section 22 and-

(a) a person who was a member of the scheme on that coming into operation shall continue to be a member, and

(b) the provisions of that section shall apply accordingly.

Saver for regulations under Act of 1988

68. (1) Notwithstanding subsection (1) of section 8 , the Data Protection Act 1988 (Section 2A) Regulations 2013 (S.I. No. 313 of 2013) and the Data Protection Act 1988 (Section 2A) Regulations 2016 (S.I. No. 220 of 2016) shall, in addition to applying for the purposes referred to in that subsection, apply for all other purposes for which they applied immediately before the commencement of that subsection and, in so far only as they apply for the second-mentioned purposes, they shall be deemed to have been made under section 38 and may be amended or revoked accordingly.

(2) (a) The Data Protection Health Regulations shall continue in force upon and after the commencement of section 7 (in so far as it relates to the repeal of section 4(8) of the Act of 1988) until the first set of regulations are made under section 60 (5)(a).

(b) The Data Protection Health Regulations are amended-

(i) in Regulation 3, by-

(I) the deletion of the definition of “the Act”,

(II) the deletion of the definition of “health professional”, and

(III) the insertion of the following definitions:

“ ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

‘health practitioner’ has the same meaning as it has in the Health Identifiers Act 2014 .”,

(ii) in Regulation 4(1), by-

(I) the substitution of “a request under Article 15 of the Data Protection Regulation” for “a request under section 4(1)(a) of the Act”, and

(II) the substitution of “the physical or mental health of the data subject, but this restriction on providing information applies only to the extent to which, and for so long as, that likelihood pertains.” for “the physical or mental health of the data subject.”,

(iii) in Regulation 5, by-

(I) the substitution of “health practitioner” for “health professional” in each place it occurs,

(II) the substitution, in paragraph (1)(a), of “a request under the said Article 15 of the Data Protection Regulation” for “a request under the said section 4(1)(a)”, and

(III) the substitution, in paragraph (2)(a), of “within the meaning of section 2 of the Medical Practitioners Act 2007 or a medical practitioner practising medicine pursuant to section 50 of that Act” for “within the meaning of the Medical Practitioners Act 1978 (No. 4 of 1978), or registered dentist, within the meaning of the Dentists Act 1985 (No. 9 of 1985)”,

and

(iv) by the deletion of Regulation 6.

(c) A request referred to in Regulation 4(1) of the Data Protection Health Regulations which includes a request for health data (within the meaning of those Regulations) that was received but not responded to before the commencement of section 7 (in so far as it relates to the repeal of section 4(8) of the Act of 1988) shall be treated as if it were a request under Article 15 of the Data Protection Regulation.

(3) (a) The Data Protection Social Work Regulations shall continue in force upon and after the commencement of section 7 (in so far as it relates to the repeal of section 4(8) of the Act of 1988) until the first set of regulations are made under section 60 (5)(b).

(b) The Data Protection Social Work Regulations are amended-

(i) in Regulation 3, by-

(I) the deletion of the definition of "the Act",

(II) the insertion of the following definition:

" 'Data Protection Regulation' means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);",

and

(III) the substitution of the following definition for the definition of "social work data":

" 'social work data' means personal data kept for, or obtained in the course of, carrying out social work by a public authority, public body, voluntary organisation or other body but excludes any health data within the meaning of the Data Protection (Access Modification) (Health) (Regulations) 1989 (S.I. No. 82 of 1989) and 'social work' shall be construed accordingly.",

(ii) in Regulation 4-

(I) in paragraph (1), by-

(A) the substitution of "a request under Article 15 of the Data Protection Regulation" for "a request under section 4(1)(a) of the Act", and

(B) the substitution of "the physical or mental health or emotional condition of the data subject, but this restriction on providing information applies only to the extent to which, and for as long as, that likelihood pertains." for "the physical or mental health or emotional condition of the data subject.",

and

(II) in paragraph (3), by the substitution of “under Article 15 of the Data Protection Regulation” for “under section 4(1)(a) of the Act”,

and

(iii) the deletion of Regulation 5.

(c) A request referred to in Regulation 4(1) of the Data Protection Social Work Regulations which includes a request for social work data (within the meaning of those Regulations) that was received but not responded to before the commencement of section 7 (in so far as it relates to the repeal of section 4(8) of the Act of 1988) shall be treated as if it were a request under Article 15 of the Data Protection Regulation.

(4) The Regulations of 2011 shall apply to-

(a) each special category of personal data that, immediately before the coming into operation of this section-

(i) constituted sensitive personal data to which those Regulations applied, or

(ii) would have constituted sensitive personal data to which those Regulations applied had the data existed immediately before such commencement,

and

(b) Article 10 data that, immediately before such coming into operation-

(i) constituted sensitive personal data to which those Regulations applied, or

(ii) would have constituted sensitive personal data to which those Regulations applied had the data existed immediately before such coming into operation.

(5) The Regulations of 2011 are amended-

(a) in Regulation 3, by the substitution of “Subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, processing” for “Processing”,

(b) in Regulation 4, by the substitution of “Subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, processing” for “Processing”, and

(c) by the insertion of the following Regulation after Regulation 6:

“7. In these Regulations, “suitable and specific measures to safeguard the fundamental rights and freedoms of data subjects” shall be construed in accordance with section 36 of the Data Protection Act 2018.”.

(6) The Regulations of 2015 shall, in addition to applying to sensitive personal data to which the Act of 1988 applies, apply to-

(a) each special category of personal data that, immediately before the coming into operation of this section-

(i) constituted sensitive personal data to which those Regulations applied, or

(ii) would have constituted sensitive personal data to which those Regulations applied had the data existed immediately before such commencement,

and

(b) Article 10 data that, immediately before such coming into operation-

(i) constituted sensitive personal data to which those Regulations applied, or

(ii) would have constituted sensitive personal data to which those Regulations applied had the data existed immediately before such coming into operation.

(7) The Regulations of 2015 are amended-

(a) in Regulation 2, by the substitution of “Subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, the processing” for “The processing”, and

(b) by the insertion of the following Regulation after Regulation 2:

“3. In these Regulations, “suitable and specific measures to safeguard the fundamental rights and freedoms of data subjects” shall be construed in accordance with section 36 of the Data Protection Act 2018.”.

(8) The Regulations of 2016 shall, in addition to applying to sensitive personal data to which the Act of 1988 applies, apply to-

(a) each special category of personal data that, immediately before the coming into operation of this section-

(i) constituted sensitive personal data to which those Regulations applied, or

(ii) would have constituted sensitive personal data to which those Regulations applied had the data existed immediately before such commencement,

and

(b) Article 10 data that, immediately before such coming into operation-

(i) constituted sensitive personal data to which those Regulations applied, or

(ii) would have constituted sensitive personal data to which those Regulations applied had the data existed immediately before such coming into operation.

(9) The Regulations of 2016 are amended-

(a) in Regulation 2, by the substitution of “Subject to suitable and specific measures to safeguard the fundamental rights and freedoms of data subjects, the processing” for “The processing”, and

(b) by the insertion of the following Regulation after Regulation 2:

“3. In these Regulations, “suitable and specific measures to safeguard the fundamental rights and freedoms of data subjects” shall be construed in accordance with section 36 of the Data Protection Act 2018.”.

(10) In this section-

“Article 10 data” has the meaning assigned to it in section 55 ;

“Data Protection Health Regulations” means the Data Protection (Access Modification) (Health) Regulations 1989 (S.I. No. 82 of 1989);

“Data Protection Social Work Regulations” means the Data Protection (Access Modification) (Social Work) Regulations 1989 (S.I. No. 83 of 1989);

“Regulations of 2011” means the Data Protection Act 1988 (Section 2B) Regulations 2011 (S.I. No. 486 of 2011);

“Regulations of 2015” means the Data Protection Act 1988 (Section 2B) Regulations 2015 (S.I. No. 240 of 2015);

“Regulations of 2016” means the Data Protection Act 1988 (Section 2B) (No. 2) Regulations 2016 (S.I. No. 427 of 2016);

“sensitive personal data” has the meaning assigned to it by the Act of 1988.

PART 5

Processing of Personal Data for Law Enforcement Purposes

Chapter 1

Preliminary and general (Part 5)

Interpretation (Part 5)

69. (1) In this Part-

“biometric data” means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual that allow or confirm the unique identification of the individual, including facial images or dactyloscopic data;

“competent authority”, subject to subsection (2), means-

(a) a public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in the State, including the safeguarding against, and the prevention of, threats to public security, or

(b) any other body or entity authorised by law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in the State, including the safeguarding against, and the prevention of, threats to public security;

“controller”, subject to subsection (2), means-

(a) a competent authority that, whether alone or jointly with others, determines the purposes and means of the processing of personal data, or

(b) where the purposes and means of the processing of personal data are determined by the law of the European Union or otherwise by the law of the State, a controller nominated-

(i) by that law, or

(ii) in accordance with criteria specified in that law;

“data concerning health” means personal data relating to the physical or mental health of an individual, including the provision of health care services to the individual, that reveal information about the status of his or her health;

“data protection impact assessment” has the meaning assigned to it by section 84 (1);

“data protection officer” has the meaning assigned to it by section 88 (1);

“data subject” means an individual to whom personal data relate;

“genetic data” means personal data relating to the inherited or acquired genetic characteristics of an individual that give unique information about the physiology or the health of the individual and that result, in particular, from an analysis of a biological sample from the individual in question;

“international organisation” means-

(a) an organisation, and subordinate bodies of an organisation, governed by public international law,
or

(b) any other body that is established by, or on the basis of, an agreement between two or more states;

“joint controller” has the meaning assigned to it by section 79 (1);

“online identifier” includes an internet protocol address, a cookie identifier or other identifier such as a radio frequency identification tag;

“personal data” means information relating to-

(a) an identified living individual, or

(b) a living individual who can be identified from the data, directly or indirectly, in particular by reference to-

(i) an identifier such as a name, an identification number, location data or an online identifier, or

(ii) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual;

“personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

“processing”, of or in relation to personal data, means an operation or a set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, including-

(a) the collection, recording, organisation, structuring or storing of the data,

(b) the adaptation or alteration of the data,

(c) the retrieval, consultation or use of the data,

(d) the disclosure of the data by their transmission, dissemination or otherwise making the data available,

(e) the alignment or combination of the data, or

(f) the restriction, erasure or destruction of the data;

“processor” means an individual who, or a legal person, public authority, agency or other body that, processes personal data on behalf of a controller, but does not include an employee of a controller who processes such data in the course of his or her employment;

“profiling” means any form of automated processing of personal data consisting of the use of the data to evaluate certain personal aspects relating to an individual, including to analyse or predict aspects concerning the individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

“pseudonymisation” means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that-

(a) such additional information is kept separately from the data, and

(b) is subject to technical and organisational measures to ensure that the data are not attributed to an identified or identifiable individual;

“rectification”, of or in relation to personal data, includes, where the data concerned are incomplete, the completion of the data, whether by means of a supplementary statement or otherwise;

“recipient”, of or in relation to personal data, means an individual to whom, or a legal person, public authority, agency or other body to which, the data are disclosed, and includes a third party;

“relevant filing system” means a set of personal data, whether centralised, decentralised or dispersed on a functional or geographical basis, where the set is structured according to specific criteria in such a way that the data are readily accessible according to those criteria;

“restrict”-

(a) in relation to the exercise of the right of a data subject-

(i) under section 87 (1) to be notified of a personal data breach,

(ii) under section 92 (10) to be notified of the restriction of the processing of personal data under subsection (9) of that section, or

(iii) under section 92 (11) to be notified of a decision not to rectify or erase data pursuant to a request under subsection (1) or (3) of that section, as the case may be,

means-

(I) to delay the notification concerned,

(II) to limit the information contained in the notification concerned, or

(III) not to make the notification concerned,

and

(b) in relation to the exercise of the right of a data subject-

(i) under section 90 (1) in so far as relates to the provision to the data subject of information specified in subsection (2)(f) of that section, or

(ii) under section 91 (1)(a) or (b),

means-

(I) to delay the provision of the information concerned,

(II) to limit the information concerned provided to the data subject, or

(III) not to provide the information concerned;

“restriction of processing” means the marking, by or on behalf of a controller, of personal data for which the controller is responsible for the purpose of limiting their processing in the future;

“special categories of personal data” means-

(a) personal data revealing-

(i) the racial or ethnic origin of the data subject,

(ii) the political opinions or the religious or philosophical beliefs of the data subject, or

(iii) whether the data subject is a member of a trade union,

(b) genetic data,

(c) biometric data for the purposes of uniquely identifying an individual,

(d) data concerning health, or

(e) personal data concerning an individual’s sex life or sexual orientation.

(2) Where a reference is made in this Part-

- (a) to a controller in a Member State other than the State, for the purposes of that reference-
 - (i) in the definition of “competent authority” in subsection (1), the references to “in the State” shall be construed as meaning “in the Member State concerned”, and
 - (ii) in the definition of “controller” in subsection (1), the reference to “the law of the State” shall be construed as meaning “the law of the Member State concerned”,

or

- (b) to a controller in a third country, for the purposes of that reference-
 - (i) in the definition of “competent authority” in subsection (1), the references to “in the State” shall be construed as meaning “in the state concerned”, and
 - (ii) in the definition of “controller” in subsection (1), the reference to “the law of the European Union or the law of the State” shall be construed as meaning “the law of the state concerned”.

(3) A word or expression that is used in this Part and is also used in the Directive has, unless the context otherwise requires, the same meaning in this Part as it has in the Directive.

Application of Part 5

70. (1) This Part applies, subject to subsection (2), to the processing of personal data by or on behalf of a controller where the processing is carried out-

- (a) for the purposes of-
 - (i) the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against, and the prevention of, threats to public security, or
 - (ii) the execution of criminal penalties,

and

- (b) by means that-
 - (i) are wholly or partly automated, or
 - (ii) where the personal data form part of, or are intended to form part of, a relevant filing system, are not automated.

(2) This Part shall not apply to the processing of personal data-

- (a) that occurs in the course of an activity falling outside the scope of the law of the European Union,
- (b) by an institution, body, office or agency of the European Union, or

(c) to which section 8 (1)(b) applies.

Chapter 2

General principles of data protection

Processing of personal data

71. (1) A controller shall, as respects personal data for which it is responsible, comply with the following provisions:

- (a) the data shall be processed lawfully and fairly;
- (b) the data shall be collected for one or more specified, explicit and legitimate purposes and shall not be processed in a manner that is incompatible with such purposes;
- (c) the data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed;
- (d) the data shall be accurate, and, where necessary, kept up to date, and every reasonable step shall be taken to ensure that data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- (e) the data shall be kept in a form that permits the identification of a data subject for no longer than is necessary for the purposes for which the data are processed;
- (f) the data shall be processed in a manner that ensures appropriate security of the data, including, by the implementation of appropriate technical or organisational measures, protection against-
 - (i) unauthorised or unlawful processing, and
 - (ii) accidental loss, destruction or damage.

(2) The processing of personal data shall be lawful where, and to the extent that-

- (a) the processing is necessary for the performance of a function of a controller for a purpose specified in section 70 (1)(a) and the function has a legal basis in the law of the European Union or the law of the State, or
- (b) the data subject has, subject to subsection (3), given his or her consent to the processing.

(3) Where the processing of personal data is to be carried out on the basis of the consent of the data subject referred to in subsection (2)(b), the processing shall be lawful only where, and to the extent that-

(a) having been informed of the intended purpose of the processing and the identity of the controller, the data subject gives his or her consent freely and explicitly,

(b) the request for consent is expressed in clear and plain language, and where such consent is given in the context of a written statement that also concerns other matters, the request for consent is presented to the data subject in a manner that is clearly distinguishable from those other matters, and

(c) the data subject may withdraw his or her consent at any time, and he or she shall be informed of this possibility prior to giving consent.

(4) Where a data subject withdraws his or her consent to the processing of personal data pursuant to subsection (3)(c), the withdrawal of consent shall not affect the lawfulness of processing based on that consent prior to the consent being withdrawn.

(5) Where a controller collects personal data for a purpose specified in section 70 (1)(a), the controller or another controller may process the data for a purpose so specified other than the purpose for which the data were collected, in so far as-

(a) the controller is authorised to process such personal data for such a purpose in accordance with the law of the European Union or the law of the State, and

(b) the processing is necessary and proportionate to the purpose for which the data are being processed.

(6) A controller may process personal data, whether the data were collected by the controller or another controller, for-

(a) archiving purposes in the public interest,

(b) scientific or historical research purposes, or

(c) statistical purposes,

provided that the said processing-

(i) is for a purpose specified in section 70 (1)(a), and

(ii) is subject to appropriate safeguards for the rights and freedoms of data subjects.

(7) A controller shall ensure, in relation to personal data for which it is responsible, that an appropriate time limit is established for-

(a) the erasure of the data, or

(b) the carrying out of periodic reviews of the need for the retention of the data.

(8) Where a time limit is established in accordance with subsection (7), the controller shall ensure, by means of procedural measures, that the time limit is observed.

(9) A processor, or any person acting under the authority of the controller or of the processor who has access to personal data, shall not process the data unless the processor or person is-

(a) authorised to do so by the controller, or

(b) required to do so by the law of the European Union or the law of the State,

and then only to the extent so authorised or required, as the case may be.

(10) A controller shall ensure that it is in a position to demonstrate that the processing of personal data for which it is responsible is in compliance with subsections (1) to (8) of this section.

Security measures for personal data

72. (1) In determining appropriate technical or organisational measures for the purposes of section 71 (1)(f), a controller shall ensure that the measures provide a level of security appropriate to the harm that might result from accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, the data concerned.

(2) A controller or processor shall take all reasonable steps to ensure that-

(a) persons employed by the controller or the processor, as the case may be, and

(b) other persons at the place of work concerned,

are aware of and comply with the relevant technical or organisational measures referred to in subsection (1).

Processing of special categories of personal data (Part 5)

73. (1) The processing of a special category of personal data shall be lawful only where-

(a) section 71 is complied with, and

(b) at least one of the following conditions is met:

(i) where the processing is to be carried out on the basis of the consent of the data subject pursuant to section 71 (2)(b), the consent referred to in that paragraph explicitly refers to the special category of personal data concerned;

(ii) the processing is necessary-

(I) to prevent injury or other damage to the data subject or another individual,

(II) to prevent loss in respect of, or damage to, property, or

(III) otherwise to protect the vital interests of the data subject or another individual;

(iii) the personal data to which the processing relates have been made public as a result of steps deliberately taken by the data subject;

(iv) the processing is necessary for-

(I) the administration of justice,

(II) the performance of a function conferred on a person by or under an enactment, or

(III) the performance of a function of the Government or a Minister of the Government;

(v) the processing-

(I) is required for the purposes of providing or obtaining legal advice or for the purposes of, or in connection with, legal claims, prospective legal claims, legal proceedings or prospective legal proceedings, or

(II) is otherwise required for the purposes of establishing, exercising or defending legal rights;

(vi) the processing is necessary for medical purposes and is carried out by, or under the responsibility of-

(I) a health practitioner, or

(II) a person who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that which would exist if that person were a health practitioner;

(vii) the processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the controller or the data subject in connection with employment or social welfare law;

(viii) the processing is carried out pursuant to section 71 (6);

(ix) the processing is authorised by regulations made under subsection (2).

(2) Regulations may be made permitting the processing of special categories of personal data for the purposes of subsection (1)(b)(ix) where the processing is necessary for reasons of substantial public interest, and without prejudice to the generality of the foregoing, such regulations shall identify the public interest concerned.

(3) Subject to subsection (4), regulations may be made under subsection (2)-

(a) by the Minister following consultation with such other Minister of the Government as he or she considers appropriate, or

(b) by any other Minister of the Government following consultation with the Minister and such other Minister of the Government as he or she considers appropriate.

(4) The Minister or any other Minister of the Government shall consult with the Commission before making regulations under subsection (2).

(5) The Commission may, on being consulted under subsection (4), make observations in writing on any matter which is of significant concern to it in relation to the proposed regulations and if the Minister or any other Minister of the Government proposes to proceed to make the regulations notwithstanding that concern, that Minister shall, before making the regulations, give a written explanation as to why he or she is so proceeding to-

(a) the Committee established jointly by Dáil Éireann and Seanad Éireann known as the Committee on Justice and Equality or any Committee established to replace that Committee, and

(b) any other Committee (within the meaning of section 19 (1)) which that Minister considers appropriate having regard to the subject matter of the regulations.

(6) The Minister or any other Minister of the Government, as the case may be, making regulations under subsection (2) shall have regard to the need for the protection of individuals with regard to the processing of their personal data and without prejudice to the generality of that need, have regard to-

(a) the nature, scope and purposes of the processing,

(b) the nature of the substantial public interest concerned,

(c) any benefits likely to arise for the data subjects concerned,

(d) any risks arising for the rights and freedoms of such subjects, and

(e) the likelihood of any such risks arising and the severity of such risks.

(7) Where a special category of personal data is processed in accordance with this section, the controller shall ensure that the processing is carried out with appropriate safeguards for the rights and freedoms of the data subject.

(8) In this section-

“health practitioner” has the same meaning as it has in the Health Identifiers Act 2014 ;

“medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of medical care and treatment and the management of healthcare services.

Data quality

74. (1) A controller shall, where relevant and in so far as is possible, make a distinction between the personal data of different categories of data subject.

(2) A controller shall, in so far as is possible, ensure that personal data based on facts are distinguished from personal data based on personal assessments.

(3) A controller shall-

(a) take all reasonable steps to ensure that personal data that are inaccurate, incomplete or no longer up to date are not transmitted or otherwise made available,

(b) verify, in so far as is possible, the quality of personal data before they are transmitted or otherwise made available, and

(c) provide, in so far as is possible, in a transmission of personal data, the information necessary for the recipient to assess the accuracy, completeness and reliability of the data and the extent to which the data are up to date.

(4) Other than where section 92 applies, where a controller becomes aware that incorrect personal data have been transmitted or personal data have been unlawfully transmitted-

(a) the controller shall ensure that the recipient of the personal data is notified without delay of that fact, and

(b) the recipient shall ensure that the personal data are rectified or erased or the processing of the data is restricted, as may be appropriate.

Chapter 3

Obligations of controllers and processors

General obligations of controller with regard to technical and organisational measures

75. (1) A controller shall implement appropriate technical and organisational measures for the purposes of-

(a) ensuring that the processing of personal data for which it is responsible is performed in compliance with this Part, and

(b) demonstrating such compliance.

(2) A controller shall ensure that measures implemented in accordance with subsection (1) are reviewed at regular intervals and, where required, updated.

(3) The measures referred to in subsection (1) shall include the implementation of an appropriate data protection policy by the controller, where such implementation is proportionate in relation to the processing activities carried out by the controller.

Data protection by design and by default

76. (1) A controller shall, without prejudice to the generality of section 75 (1), for the purposes of meeting the requirements of this Part and protecting the rights of data subjects-

(a) when determining the means of processing personal data, and

(b) when carrying out the said processing,

implement appropriate technical and organisational measures that are designed-

(i) to implement the principles of the protection of personal data contained in this Part in an effective manner, and

(ii) to integrate the necessary safeguards into the said processing.

(2) Without prejudice to the generality of section 75 (1) and subsection (1), a controller shall, subject to subsection (3), when processing personal data implement appropriate technical and organisational measures to ensure that only personal data that are necessary for each specific purpose of the processing are processed.

(3) The requirement in subsection (2) applies in relation to-

(a) the amount of personal data collected for the processing concerned,

(b) the extent of the processing of the personal data concerned,

(c) the period for which the personal data concerned are stored, and

(d) the accessibility of the personal data concerned.

(4) Technical and organisational measures implemented in accordance with subsection (2) shall ensure that personal data are not made generally available unless, and only to the extent, authorised by the controller.

Security of automated processing

77. A controller or processor, prior to carrying out automated processing, shall-

(a) evaluate the risks to the rights and freedoms of individuals arising from the processing concerned, and

(b) implement measures designed to-

(i) deny access to the processing equipment used for the processing to any person other than the persons authorised in that regard by the controller or processor, as the case may be,

(ii) prevent the reading, copying, modification or removal of the data media concerned, other than in so far as is authorised by the controller or processor, as the case may be,

(iii) prevent the input of personal data other than in so far as is authorised by the controller or processor, as the case may be,

(iv) prevent the inspection, modification or deletion of the data other than in so far as is authorised by the controller or processor, as the case may be,

(v) prevent the use of the automated processing system by persons using data communication equipment who are not authorised to do so by the controller or processor, as the case may be,

(vi) ensure that where a person is authorised to use the automated processing system concerned, he or she has access to personal data on the system only in so far as he or she is so authorised by the controller or processor, as the case may be,

(vii) ensure that it is possible to verify or establish the persons to whom personal data have been or may be transmitted or made available using data communication equipment,

(viii) ensure that it is possible to verify or establish which personal data have been input into an automated processing system, and in relation to such data, to verify and establish the person who input the data and when the data were input,

(ix) prevent the reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media, other than in so far as is authorised by the controller or processor, as the case may be,

(x) ensure that an installed automated system may be restored in the event of an interruption in the service of the system,

(xi) ensure that the automated processing system properly performs its function and the appearance of a fault in the automated processing system is reported to the controller or processor, as the case may be, and

(xii) ensure that personal data that are stored on the automated processing system cannot be corrupted by means of a malfunctioning of the system.

Technical and organisational measures

78. For the purposes of determining the appropriate technical and organisational measures in relation to personal data that are required to be taken by a controller or processor in order to ensure compliance with this Part, and in particular sections 71 (1)(f), 75 (1), 76 and 80 , the controller or processor, as the case may be, shall, where relevant, have regard to the following matters:

- (a) the nature of the personal data concerned;
- (b) the accessibility of the data;
- (c) the nature, scope, context and purpose of the processing concerned;
- (d) any risks to the rights and freedoms of individuals arising from the processing concerned;
- (e) the likelihood of any such risks arising and the severity of such risks;
- (f) the state of the art and the cost of implementation;
- (g) guidelines, recommendations and descriptions of best practice issued by the Commission or the European Data Protection Board.

Joint controllers

79. (1) Where 2 or more controllers jointly determine the purposes and means of the processing of personal data (in this Part referred to as “joint controllers”), they shall determine their respective responsibilities for compliance with this Part in a transparent manner by means of an agreement in writing between them, save in so far as the said responsibilities are determined by the law of the European Union or the law of the State.

(2) An agreement in writing referred to in subsection (1)-

(a) shall include a determination of-

(i) the respective responsibilities of the joint controllers concerned as regards the exercise by data subjects of their rights under this Part, and

(ii) the respective duties of the joint controllers concerned as regards the provision to a data subject of the information specified in section 90 (2),

and

(b) may designate a single point of contact in respect of the processing concerned for the data subject to whom it relates, where such designation is not otherwise determined by the law of the State.

Processors

80. (1) A controller shall engage a processor to carry out processing on its behalf only where-

(a) the processing is carried out, subject to subsection (3), in pursuance of a contract in writing between the controller and the processor that provides for the matters specified in subsection (2), and

(b) the processor provides sufficient guarantees to implement appropriate technical and organisational measures to ensure that-

(i) the processing shall comply with the provisions of this Part, and

(ii) the rights and freedoms of the data subjects are protected.

(2) A contract entered into between a controller and a processor in accordance with subsection (1)(a) shall-

(a) specify the subject matter, duration, nature and purpose of the processing to be carried out thereunder,

(b) specify the type of personal data to be processed thereunder and the categories of data subjects to whom the personal data relate,

(c) specify the obligations and rights of the controller in relation to the processing, and

(d) provide that the processor shall-

(i) act only on instructions from the controller in relation to the processing, except in so far as the law of the European Union or the law of the State requires the processor to act otherwise,

(ii) procure the services of another processor (in this section referred to as a “secondary processor”) in relation to the processing only where authorised to do so in advance and in writing by the controller, which authorisation may be specific or general in nature,

(iii) ensure that any person authorised to process the personal data has undertaken to maintain the confidentiality of the personal data or is under an appropriate statutory obligation to do so,

(iv) assist the controller in ensuring compliance with this Part in so far as it relates to the exercise by a data subject of his or her rights,

(v) erase or return to the controller, at the election of the controller, all personal data upon completion of the processing services carried out by the processor on behalf of the controller and erase any copy

of the data, unless the processor is required by the law of the European Union or the law of the State to retain the data, and

(vi) make available to the controller all information necessary to demonstrate compliance by the processor with this section.

(3) Subsection (1)(a) shall not apply in relation to processing where the form of the processing and the role of the controller and the processor concerned are otherwise specified in the law of the European Union or the law of the State.

(4) Where a controller gives an authorisation, whether specific or general in nature, to a processor, including a secondary processor (in this section referred to as “the procuring processor”) to procure the services of a secondary processor, the procuring processor shall inform-

(a) the controller, and

(b) where relevant, any processor who procured the services of the procuring processor in relation to the processing concerned,

in advance of any such procurement or of a change in the terms of such procurement.

(5) Where a procuring processor procures the services of a secondary processor to carry out processing on behalf of a controller, subsections (1) and (2) shall apply to the procuring processor and the secondary processor, subject to the following modifications and any other necessary modifications:

(a) a reference to a “controller”, other than in subparagraphs (ii), (iv), (v) and (vi) of subsection (2)(d), shall be construed as a reference to the procuring processor;

(b) a reference to a “controller” in subsection (2)(d)(iv) shall be construed as a reference to the controller and the procuring processor;

(c) a reference to a “controller” in subsection (2)(d)(v) shall be construed as a reference to the controller or the procuring processor, as appropriate; and

(d) a reference to a “processor” shall be construed as a reference to a secondary processor.

(6) Where a person, who by virtue of the operation of this Part is a processor of personal data, when purporting to act as such a processor, determines the purpose and means of the processing of the data, the obligations that are placed on a controller under this Part shall apply thereafter to the person as though the person were a controller of the data.

Record of data processing activities

81. (1) A controller shall create and maintain a record in writing containing the following information in relation to each category of processing activity for which it is responsible:

(a) the identity and contact details of the controller and, where applicable, the controller's data protection officer or any joint controller;

(b) a description of-

(i) the purpose of the processing,

(ii) the categories of personal data concerned,

(iii) the categories of data subjects to which the personal data relate,

(iv) the categories of recipients to which the personal data have been or will be disclosed, including recipients in a third country or an international organisation, if any,

(v) the categories of transfer of personal data to a third country or an international organisation, if any,

(vi) the legal basis for the processing operation for which the personal data are intended, including the transfer of the data, where applicable, and

(vii) where possible, the proposed time limit within which each category of personal data shall be erased;

(c) whether the processing involves the use of profiling;

(d) where possible, a general description of the technical and organisational security measures implemented in respect of the processing activity in accordance with section 72 (1).

(2) A processor shall create and maintain a record in writing of each category of processing activity carried out by the processor on behalf of a controller containing the following information:

(a) the identity and contact details of-

(i) the processor,

(ii) each controller on behalf of which the processor is carrying out the processing, and

(iii) the processor's data protection officer, where applicable;

(b) a description of each category of processing carried out on behalf of each controller;

(c) details of any transfer of personal data to a third country or an international organisation, if applicable, including the identification of the third country or international organisation to which the data are transferred;

(d) where possible, a general description of the technical and organisational security measures implemented in respect of the processing activity in accordance with section 72 (1).

(3) A controller or processor shall, where requested to do so, make a record created and maintained pursuant to subsection (1) or (2), as the case may be, available to the Commission for inspection and examination.

Data logging for automated processing system

82. (1) Subject to subsection (5), where a controller or processor carries out processing of personal data by automated means, the controller or processor, as the case may be, shall create and maintain a log (in this section referred to as a “data log”) of the following processing operations carried out in automated processing systems in respect of that processing:

(a) the collection of personal data for the purposes of such processing and the alteration of any such data;

(b) the consultation of the personal data by any person;

(c) the disclosure of the personal data, including the transfer of the data, to any other person;

(d) the combination of the personal data with other data;

(e) the erasure of the personal data, or some of the data.

(2) Where a data log contains information specified in paragraph (b) or (c) of subsection (1), the controller or processor, as the case may be, shall ensure that the data log contains sufficient information to establish the following:

(a) the date and time of the consultation or disclosure, as the case may be;

(b) the reason for the consultation or disclosure, as the case may be;

(c) in so far as is possible, the identification of the person who consulted or disclosed, as the case may be, the personal data;

(d) the identity of any recipient to whom the personal data were disclosed.

(3) A data log shall not be used by any person for any purpose other than-

(a) verifying the lawfulness of the processing,

- (b) the monitoring by the controller of processing carried out by the controller,
- (c) the monitoring by the processor of processing carried out by the processor,
- (d) ensuring the integrity and security of the personal data concerned, or
- (e) for the purposes of criminal proceedings.

(4) A controller or processor shall, where requested to do so, make a data log created and maintained by the controller or processor, as the case may be, available to the Commission for inspection and examination.

(5) This section shall not apply, in respect of an automated processing system established on or before 6 May 2016-

(a) prior to 6 May 2023, where compliance by a controller or processor, as the case may be, with this section prior to that date would involve disproportionate effort, or

(b) prior to 6 May 2026, where compliance by a controller or a processor, as the case may be, with this section prior to that date would cause serious difficulties for the operation of the automated processing system to which the data log relates.

(6) A controller or processor who intends to rely upon subsection (5)(b) in respect of an automated processing system operated by the controller or processor, as the case may be, shall notify the Minister in writing of the said intention on or before 31 December 2022.

(7) A notification referred to in subsection (6) shall include a description of the serious difficulties referred to in subsection (5)(b) in respect of the automated processing system concerned.

Cooperation with Commission

83. A controller or a processor shall, on request by the Commission, cooperate with and assist the Commission in the performance of its functions under this Part.

Data protection impact assessment and prior consultation with Commission

84. (1) Where having regard to its nature, scope, context and purposes, a type of processing, and in particular a type of processing using new technology, is likely to result in a high risk to the rights and freedoms of individuals, the controller that is proposing to carry out the processing shall conduct an assessment of the likely impact of the proposed processing operations on the protection of personal data (in this Part referred to as a “data protection impact assessment”) prior to carrying out the processing.

(2) A data protection impact assessment carried out in accordance with subsection (1) shall include:

(a) a general description of the proposed processing operations to which it relates;

(b) an assessment of the potential risks to the rights and freedoms of data subjects as a result of the proposed processing; and

(c) a description of any safeguards, security measures or mechanisms proposed to be implemented by the controller to mitigate any risk referred to in paragraph (b) and to ensure the protection of the personal data in compliance with this Part.

(3) Where-

(a) it appears to a controller, having conducted a data protection impact assessment, that the processing concerned would, despite the implementation of safeguards, security measures or mechanisms referred to in subsection (2)(c), result in a high risk to the rights and freedoms of individuals, or

(b) the controller proposes to carry out processing of a type prescribed by the Commission under subsection (9),

the controller shall, prior to commencing the processing, consult the Commission by request in that regard in writing.

(4) A controller shall, when making a request under subsection (3), provide the Commission with-

(a) the data protection impact assessment conducted in relation to the processing concerned, and

(b) any other information required by the Commission to enable it to assess-

(i) the potential risks to the rights and freedoms of individuals arising from the proposed processing, and

(ii) the compliance of the proposed processing with this Part.

(5) The Commission shall, where it is of the view that the proposed processing would not comply with this Part, in particular where it is of the view that the controller has insufficiently identified or mitigated the potential risks to the rights and freedoms of individuals arising from the proposed processing, issue written advice in relation to the processing to the controller and, where applicable, any proposed processor.

(6) Subject to subsection (8), where the Commission issues written advice pursuant to subsection (5), it shall do so within a period of 6 weeks from the date on which it receives the request under subsection (3).

(7) For the purposes of responding to a request under subsection (3), the Commission may use any of its powers referred to in Chapter 4 of Part 6.

(8) Where, taking into account the complexity of the proposed processing, the Commission is of the opinion that it requires additional time to consider a request made under subsection (3), it may, once only and within one month from the date of the receipt of the request, extend the time period referred to in subsection (6) by such further period not exceeding one month as it may specify by notice in writing to the controller concerned.

(9) The Commission may, following consultation with the Minister, make regulations prescribing a type of processing for the purposes of subsection (3)(b) as a type of processing in relation to which a controller shall consult the Commission prior to commencing the processing.

(10) The Commission shall, when prescribing a type of processing under subsection (9), have regard to-

(a) the nature, scope and purposes of the type of processing,

(b) the type of processing involved, in particular where the use of new technology is likely to result in a high risk to the rights and freedoms of individuals,

(c) the likelihood of any such risks arising and the severity of such risks, and

(d) any submissions received pursuant to subsection (11)(c) in relation to the proposed regulations.

(11) The Commission shall, prior to making regulations under subsection (9), publish a notice on the website of the Commission and in at least one daily newspaper circulating generally in the State-

(a) indicating that it proposes to make regulations under this section,

(b) indicating that a draft of the regulations is available for inspection on that website for a period specified in the notice, being not less than 28 days from the date of the publication of the notice in the newspaper, and

(c) stating that submissions in relation to the draft regulations may be made in writing to the Commission before a date specified in the notice, which shall be not less than 28 days after the end of the period referred to in paragraph (b).

(12) Where there is a proposal for a legislative measure for which a Minister of the Government is responsible that relates to the processing of personal data, the relevant Minister shall consult with the Commission during the process of the preparation of the legislative measure.

Notification of personal data breach by processor

85. Where a processor becomes aware of a personal data breach, the processor shall notify the controller on whose behalf the data are being processed of the breach-

(a) in writing, and

(b) without undue delay.

Notification of personal data breach to Commission, etc.

86. (1) Subject to subsection (3), where a personal data breach occurs, the controller shall, without undue delay and where feasible within 72 hours of becoming aware of the breach, notify the Commission of the breach.

(2) Where a controller does not notify the Commission under subsection (1) of a personal data breach within 72 hours of becoming aware of the breach, the controller shall include in the notification the reason for not so notifying.

(3) Subsection (1) shall not apply where, taking into account the nature of the personal data and the scope, context and purposes of the processing, the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

(4) A notification under subsection (1) shall include-

(a) a description of the personal data breach, including, where possible the categories and number, or approximate number, of-

(i) data subjects concerned, and

(ii) personal data records concerned,

(b) a description of the likely consequences of the personal data breach,

(c) a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including any measures taken or proposed to be taken to mitigate its possible adverse effects, and

(d) the name and contact details of the controller's data protection officer (if any) or other point of contact.

(5) Where, at the time of the making of a notification under subsection (1), it is not possible for a controller to include in the notification all the information specified in subsection (4) in relation to the personal data breach concerned, the controller shall-

(a) nevertheless make the notification including such information as is possible to include at that time, and

(b) supply the Commission with such information specified in subsection (4) as is outstanding without undue delay.

(6) A controller shall create and maintain a detailed record in writing of a personal data breach, including a description of-

(a) the breach,

(b) the effects of the breach, and

(c) the measures taken to address the breach, including any measures taken to mitigate its possible adverse effects.

(7) A controller shall, where so requested by the Commission, provide a copy of a record created and maintained under subsection (6) to the Commission.

(8) Where a personal data breach involves personal data that have been transmitted-

(a) by a controller in the State to a controller in another Member State, or

(b) by a controller in another Member State to a controller in the State,

the controller in the State shall provide the controller in the other Member State with the information specified in subsection (4) without undue delay.

Communication of personal data breach to data subject

87. (1) Subject to subsections (2), (4) and (7), where a personal data breach occurs that is likely to result in a high risk to the rights and freedoms of a data subject, the controller shall, without undue delay, notify the data subject to whom the breach relates.

(2) Subsection (1) shall not apply where-

(a) the controller has implemented appropriate technological and organisational protection measures that were applied to the personal data affected by the personal data breach, in particular where the said measures, including encryption, render the personal data unintelligible to any person who is not authorised to access it, or

(b) the controller has taken measures in response to the personal data breach that ensure that the high risk to the rights and freedoms of a data subject from the breach is no longer likely to materialise.

(3) A notification under subsection (1) shall-

(a) describe, in clear and plain language, the nature of the personal data breach concerned, and

(b) contain at least the information specified in paragraphs (b) to (d) of section 86 (4).

(4) Where a notification under subsection (1) would involve a disproportionate effort, the controller shall notify the data subjects concerned of the personal data breach by way of public communication or other similar measure that ensures the data subjects are informed of the personal data breach in an equally effective manner.

(5) A notification under subsection (4) shall-

(a) describe, in clear and plain language, the nature of the personal data breach concerned, and

(b) contain such other information as is appropriate in all the circumstances.

(6) Where-

(a) a controller notifies the Commission under section 86 of a personal data breach, and

(b) the controller has not notified the data subject to whom the personal data relate under subsection (1) or (4), as the case may be, of the personal data breach,

the Commission may, having considered the likelihood of the data breach resulting in a high risk to the rights and freedoms of a data subject-

(i) require the controller to notify the data subject under subsection (1) or (4), as the case may be, or

(ii) determine that subsection (2) applies in relation to the personal data breach.

(7) A controller may, in relation to the exercise of the right of a data subject to be notified under subsection (1) of a personal data breach, restrict the exercise of the said right where to do so constitutes a necessary and proportionate measure in a democratic society, with due regard for the fundamental rights and legitimate interests of the data subject, for a purpose specified in section 94 (2).

(8) Where a controller restricts the exercise of the right of a data subject under subsection (7), subsections (5), (6) and (7) of section 94 shall apply in respect of the said restriction, with all necessary modifications.

Data protection officer

88. (1) A controller, other than-

(a) a court, or

(b) another independent judicial authority,

acting in its judicial capacity, shall, subject to subsections (2) and (3), appoint a person to carry out the functions specified in subsection (5) in respect of the controller (in this Part referred to as a “data protection officer”).

(2) Two or more controllers may, subject to subsection (3), having regard to their organisational structure and size, appoint a single data protection officer to carry out the functions specified in subsection (5) in respect of each of the controllers.

(3) A controller, when appointing a data protection officer, shall do so on the basis of-

(a) the person’s expert knowledge of the law and the practice relating to the protection of personal data, and

(b) his or her ability to carry out the functions specified in subsection (5).

(4) Where a controller appoints a data protection officer, the controller shall-

(a) publish or cause to be published the contact details of the data protection officer,

(b) inform the Commission of the appointment of the data protection officer and provide the Commission with his or her contact details,

(c) ensure that the data protection officer-

(i) reports directly, in relation to his or her functions under subsection (5), to the highest level of management of the controller,

(ii) does not receive any instructions regarding the exercise of such functions, and

(iii) is involved in an appropriate and timely manner in all matters relating to the protection of personal data, and

(d) support the data protection officer in performing his or her functions under subsection (5), including by-

(i) providing him or her with the resources that he or she requires to perform those functions,

(ii) ensuring that he or she has access to processing operations carried out by the controller, and

(iii) assisting him or her to maintain his or her expert knowledge in the law and practice relating to the protection of personal data.

(5) The functions of a data protection officer shall include the following:

(a) informing and advising the controller, and the employees of the controller who carry out processing, of their obligations under this Part and under any other law of the European Union or law of the State that relates to the protection of personal data;

(b) monitoring the compliance of the controller with-

(i) this Part,

(ii) any other law of the European Union or law of the State that relates to the protection of personal data, and

(iii) the policies of the controller in relation to the protection of personal data, including the assignment of responsibilities in the controller in relation to the protection of personal data, the raising of awareness and the training of staff involved in processing operations in that regard, and any audit activity related to the protection of personal data;

(c) providing advice, where requested to do so, in relation to the carrying out of a data protection impact assessment in accordance with section 84 and monitoring any steps taken on foot of that assessment;

(d) acting as the contact point for data subjects with regard to all issues related to the processing of their personal data and to the exercise of their rights under this Part;

(e) cooperating with the Commission and acting as a contact point for the Commission for issues related to processing carried out by the controller, including consultation by the controller with the Commission under section 84 .

Chapter 4

Rights, and restriction of rights, of data subject (Part 5)

Rights in relation to automated decision making (Part 5)

89. (1) Subject to subsection (2), a decision that produces an adverse legal effect for a data subject or significantly affects a data subject shall not be based solely on automated processing, including profiling, of personal data that relate to him or her.

(2) Subsection (1) shall not apply where-

(a) the taking of a decision based solely on automated processing is authorised by the law of the European Union or the law of the State and the law so authorising contains appropriate safeguards for the rights and freedoms of the data subject, including the right of the data subject to make representations to the controller in relation to the decision, and

(b) the controller has taken adequate steps to safeguard the legitimate interests of the data subject.

(3) Profiling that results in discrimination against an individual on the basis of a special category of personal data shall be prohibited.

Right to information

90. (1) Subject to subsection (4) and section 94 , a controller shall ensure that the data subject is provided with, or, as appropriate, has made available to him or her, the information specified in subsection (2) in relation to personal data relating to him or her within a reasonable period after the date on which the controller obtains the personal data concerned, having regard to the circumstances in which the data are or are to be processed.

(2) The information to which subsection (1) applies is:

(a) the identity and the contact details of the controller;

(b) the contact details of the data protection officer of the controller, where applicable;

(c) the purpose for which the personal data are intended to be processed or are being processed;

(d) information detailing the right of the data subject to request from the controller access to, and the rectification or erasure of, the personal data;

(e) information detailing the right of the data subject to lodge a complaint with the Commission and the contact details of the Commission;

(f) in individual cases where further information is necessary to enable the data subject to exercise his or her rights under this Part, having regard to the circumstances in which the personal data are or are to be processed, including the manner in which the data are or have been collected, any such information including:

(i) the legal basis for the processing of the data concerned, including the legal basis for any transfers of data;

(ii) the period for which the data concerned will be retained, or where it is not possible to determine the said period at the time of the giving of the information, the criteria used to determine the said period;

(iii) where applicable, each category of recipients of the data.

(3) The information referred to in paragraphs (a) to (e) of subsection (2) may be made available to the data subject by means of publication on the website of the controller.

(4) Without prejudice to section 94 , subsection (1) shall not apply to information specified in subsection (2)-

(a) where the information is already in the possession of the data subject, or

(b) where, in particular in the case of processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, the provision of the information proves impossible or would involve a disproportionate effort.

Right of access

91. (1) Subject to subsections (7), (9) and (12) and sections 93 (4)(ii) and 94 , an individual who believes that personal data relating to him or her have been or are being processed by or on behalf of a controller, if he or she so requests the controller by notice in writing shall-

(a) be informed by the controller whether personal data relating to him or her have been or are being processed by or on behalf of the controller, and

(b) where such data have been or are being so processed, be provided by the controller with the following information:

(i) a description of-

(I) the purpose of, and the legal basis for, the processing,

(II) the categories of personal data concerned,

(III) the recipients or categories of recipients to whom the personal data concerned have been disclosed, and

(IV) the period for which the personal data concerned will be retained, or where it is not possible to determine the said period at the time of the giving of the information, the criteria used to determine the said period;

(ii) information detailing the right of the data subject to request from the controller the rectification or erasure of the personal data concerned;

(iii) information detailing the right of the data subject to lodge a complaint with the Commission and the contact details of the Commission;

(iv) a communication of the personal data concerned;

(v) any available information as to the origin of the personal data concerned, unless the communication of that information is contrary to the public interest.

(2) A controller shall respond to a request made under subsection (1) and provide the information specified in paragraph (b) thereof to the data subject as soon as may be and, subject to subsections (4) and (5), in any event not later than one month after the date on which the request is made.

(3) When making a request under subsection (1), the individual making the request shall provide the controller with such information as the controller may reasonably require to satisfy itself of the identity of the individual and to locate any relevant personal data or information.

(4) Where a controller has reasonable doubts as to the identity of an individual making a request under subsection (1) or reasonably requires additional information to locate any relevant personal data, it may request such additional information from the data subject as may be necessary to confirm his or her identity or to enable it to locate such personal data or information, as the case may be, and the period of time from the making of such a request for additional information until the request is complied with shall not be reckonable for the purposes of subsection (2).

(5) Where, taking into account the complexity of a request made under subsection (1) and the number of such requests received by the controller, the controller is of the opinion that it requires additional time to consider the request, it may, once only and within one month from the date of the receipt of the request, extend the time period referred to in subsection (2) by such further period not exceeding 2 months as it may specify by notice in writing to the individual making the request.

(6) A notice in writing referred to in subsection (5) shall include the reason for which the controller is of the opinion that it requires additional time to consider the request made under subsection (1).

(7) Where information that a controller would otherwise be required to provide to a data subject pursuant to subsection (1) includes personal data relating to another individual that would reveal, or would be capable of revealing, the identity of the individual, the controller-

(a) shall not, subject to subsection (8), provide the data subject with the information that constitutes such personal data relating to the other individual, and

(b) shall provide the data subject with a summary of the personal data concerned that-

(i) in so far as is possible, permits the data subject to exercise his or her rights under this Part, and

(ii) does not reveal, or is not capable of revealing, the identity of the other individual.

(8) Subsection (7) shall not apply where the individual to whom the personal data that would reveal, or would be capable of revealing, his or her identity, relate consents to the provision of the information concerned to the data subject making a request pursuant to subsection (1).

(9) Subsection (1) shall not apply-

(a) in respect of personal data relating to the data subject that consists of an expression of opinion about the data subject by another person given in confidence or on the understanding that it would be treated as confidential, or

(b) to information specified in paragraph (b)(i)(III) of that subsection in so far as a recipient referred to therein is a public authority which may receive data in the context of a particular inquiry in accordance with the law of the State.

(10) Information provided pursuant to a request under subsection (1) may take account of any amendment of the personal data concerned made since the receipt of the request by the controller (being an amendment that would have been made irrespective of the receipt of the request) but not of any other amendment.

(11) The obligations imposed by subparagraphs (iv) and (v) of subsection (1)(b) shall be complied with by supplying the data subject with a copy of the information concerned in permanent form unless-

(a) the supply of such a copy is not possible or would involve disproportionate effort, or

(b) the data subject agrees otherwise.

(12) Where a controller has previously complied with a request under subsection (1), the controller is not obliged to comply with a subsequent identical or similar request under that subsection by the same individual unless, in the opinion of the controller, a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

(13) In determining for the purposes of subsection (12) whether the reasonable interval specified in that subsection has elapsed, regard shall be had to the nature of the personal data, the purpose for which the personal data are processed and the frequency with which the personal data are altered.

(14) Where a controller, pursuant to subsection (12) refuses to act upon a request under subsection (1), it shall, as soon as practicable, so notify the data subject in writing.

Right to rectification or erasure and restriction of processing

92. (1) Where a data subject is of the opinion that a controller is processing personal data relating to him or her that are inaccurate, the data subject may make a request in writing to the controller for the controller to rectify the data concerned.

(2) A controller that receives a request under subsection (1) shall, subject to subsections (6), (7) and (9) and section 93 (4)(ii), where it is satisfied that the personal data to which the request relates are inaccurate, rectify the data as soon as may be and in any event no later than one month after the date on which the request is made.

(3) Where a data subject is of the opinion that a controller is processing personal data relating to him or her-

(a) in a manner that contravenes subsections (1) to (6) of section 71 or section 73 (1), or

(b) that are required to be erased by the controller in accordance with a legal obligation to which the controller is subject,

the data subject may make a request in writing to the controller to erase the data concerned.

(4) A controller that receives a request under subsection (3) shall, subject to subsections (6), (7) and (9) and section 93 (4)(ii), where it is satisfied that paragraph (a) or (b) of subsection (3) applies to the personal data to which the request relates, erase the data as soon as may be and in any event no later than one month after the date on which the request is made.

(5) When making a request under subsection (1) or (3), the data subject shall provide such information as the controller may reasonably require to-

(a) satisfy itself as to the identity of the data subject,

(b) locate any relevant personal data, and

(c) satisfy itself as to whether the personal data concerned are inaccurate or as to the basis on which the data should be erased, as the case may be.

(6) Where a controller-

(a) has reasonable doubts as to the identity of an individual making a request under subsection (1) or (3), or

(b) reasonably requires additional information-

(i) to locate any relevant personal data, or

(ii) to satisfy itself as to whether the personal data concerned are inaccurate or as to the basis on which the data should be erased, as the case may be,

it may request such additional information from the data subject as may be necessary to confirm his or her identity or to so locate or satisfy itself, as the case may be, and the period of time from the making of such a request for additional information until the request is complied with shall not be reckonable for the purposes of subsection (2) or (4), as the case may be.

(7) Where, taking into account the complexity of a request made under subsection (1) or (3) and the number of such requests received by the controller, the controller is of the opinion that it requires additional time to consider the request, it may, once only and within one month from the date of the receipt of the request, extend the time period referred to in subsection (2) or (4), as the case may be, by such further period not exceeding 2 months as it may specify by notice in writing to the data subject making the request.

(8) A notice in writing referred to in subsection (7) shall include the reason for which the controller is of the opinion that it requires additional time to consider the request made under subsection (1) or (3), as the case may be.

(9) Where a data subject makes a request under subsection (1) or (3), and-

(a) the accuracy of the data is contested by the data subject and it is not possible to ascertain whether the data are so inaccurate, or

(b) the personal data are required for the purposes of evidence in proceedings before a court or tribunal or in another form of official inquiry,

the controller shall restrict the processing of the data and shall not rectify or erase the data, as the case may be.

(10) Where a controller-

(a) complies with a request under subsection (1) or (3), or

(b) restricts the processing of personal data under subsection (9),

the controller shall, as soon as practicable, notify in writing-

(i) subject to section 94 , the data subject concerned,

(ii) each controller from which the personal data concerned were received, and

(iii) each person to whom the personal data concerned were disclosed,

of the rectification, erasure or restriction concerned, as the case may be.

(11) Where a controller receives a request under subsection (1) or (3), and-

(a) the controller is not satisfied that, as the case may be,-

(i) in relation to a request under subsection (1), the personal data to which the request relates should be rectified pursuant to subsection (2), or

(ii) in relation to a request under subsection (3), the personal data to which the request relates should be erased pursuant to subsection (4),

and

(b) subsection (9) does not apply to the data,

the controller shall, subject to section 94 , as soon as practicable, so notify the data subject in writing.

(12) A notification under subsection (11) shall include-

(a) the reasons for the controller's decision under that subsection, and

(b) information relating to the data subject's right under section 95 to request the Commission to verify the lawfulness of the processing concerned.

(13) Where a person to whom personal data were disclosed is notified under subsection (10) of-

(a) the rectification or erasure of the data pursuant to a request under subsection (1) or (3), as the case may be, or

(b) the restriction of the processing of the data under subsection (9),

the person shall rectify or erase, or restrict the processing of, as the case may be, any of the data concerned that the person has under his or her control in the same manner, and to the same extent, as the controller making the notification has rectified or erased, or restricted the processing of, as the case may be, the data concerned.

(14) Where a controller has restricted the processing of personal data pursuant to subsection (9) and proposes to lift the said restriction, the controller shall inform the data subject prior to the lifting of the restriction.

(15) Where a controller that restricted the processing of personal data pursuant to subsection (9) lifts the said restriction-

(a) the controller shall notify any person who was notified under subsection (10) of the said restriction of the lifting of the restriction as soon as practicable, and

(b) the person so notified shall lift any restriction of the processing of the data concerned implemented under subsection (13) in the same manner, and to the same extent, as the controller making the notification has lifted the restriction on the processing of the data concerned.

(16) This section shall not apply to personal data that are contained in witness statements.

(17) For the purposes of this section, personal data are inaccurate if-

(a) they are incorrect or misleading as to any matter of fact, or

(b) they are incomplete in a material manner.

Communication with data subject

93. (1) Where a controller-

(a) provides or makes available information to a data subject under section 90 ,

(b) provides or makes available information to, or communicates with, a data subject pursuant to a request under section 91 or 92,

the controller shall take all reasonable steps to ensure the information is provided or made available, or the communication is made, as the case may be, in a concise, intelligible and easily accessible form using clear and plain language.

(2) The information or communication, as the case may be, referred to in subsection (1), shall-

(a) be provided to the data subject by appropriate means, including by electronic means, and

(b) in the case of a communication with a data subject pursuant to a request under section 91 or 92 , in so far as is possible, be provided in the same form as that in which the request is made.

(3) A controller shall not impose a charge on a data subject for information provided to him or her under section 90 or, subject to subsection (4)(i), pursuant to a request under section 91 or 92.

- (4) Where a data subject makes a request to a controller under section 91 or 92 that is-
- (a) manifestly unfounded, or
 - (b) excessive in nature, having regard to the number of requests made by the data subject to the controller under those sections,
- the controller may-
- (i) charge a reasonable fee to the data subject in respect of the request, having regard to the administrative cost to the controller of complying with the request, or
 - (ii) refuse to act upon the request.
- (5) Where a controller, pursuant to subsection (4)(ii), refuses to act upon a request under section 91 or 92 it shall, as soon as practicable, so notify the data subject in writing.
- (6) A notification under subsection (5) shall include-
- (a) the reasons for which the controller is refusing to act upon the request under section 91 or 92, as the case may be, pursuant to subsection (4)(ii), and
 - (b) information relating to the right of the data subject under Chapter 3 of Part 6 to lodge a complaint with the Commission and the contact details of the Commission.
- (7) Where, pursuant to subsection (4)(ii), a controller refuses to act upon a request made to the controller by a data subject under section 91 or 92, it shall be for the controller to demonstrate that the request was manifestly unfounded or excessive in nature.
- (8) In this section, a reference to a "data subject" shall be construed as including an individual who makes a request under section 91 (1), irrespective of whether the controller is processing personal data relating to the individual.

Restrictions on exercise of data subject rights (Part 5)

94. (1) Subject to subsection (2), a controller, with respect to personal data for which it is responsible, may restrict, wholly or partly, the exercise of a right of a data subject specified in subsection (4).

(2) Subsection (1) shall apply where the controller is satisfied that restricting the exercise of a right under that subsection constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the data subject for the purposes of-

- (a) avoiding obstructing official or legal inquiries, investigations or procedures,

(b) avoiding prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties,

(c) protecting public security,

(d) protecting national security, or

(e) protecting the rights and freedoms of other persons.

(3) Without prejudice to the generality of subsection (2), the purposes specified in paragraphs (a) to (e) of subsection (2) include the following:

(a) the prevention, detection or investigation of offences, the apprehension or prosecution of offenders or the effectiveness of lawful methods, systems, plans or procedures employed for the purposes of the matters aforesaid;

(b) the enforcement of, compliance with or administration of any enactment related to a purpose specified in section 70 (1)(a);

(c) ensuring the safety of the public and the safety or security of individuals and property;

(d) ensuring the fairness of criminal proceedings in a court or other tribunal;

(e) ensuring the security of-

(i) a penal institution,

(ii) a children detention school within the meaning of section 3 of the Children Act 2001 ,

(iii) a remand centre designated under section 88 of the Children Act 2001 ,

(iv) the Central Mental Hospital, or

(v) any system of communications, whether internal or external, of the Garda Síochána, the Defence Forces, the Revenue Commissioners or a penal institution;

(f) protecting the life, safety or well-being of any person;

(g) preventing the facilitation of the commission of an offence;

(h) avoiding the prejudice or impairment of national security, defence or the international relations of the State;

(i) avoiding the obstruction or impairment of official or legal inquiries, investigations or procedures or the operation of legal privilege;

(j) the performance by the Commission of its functions.

(4) The rights of a data subject to which subsection (1) applies are:

(a) the right of the data subject under section 90 (1) in so far as relates to information specified in subsection (2)(f) of that section;

(b) the rights of the data subject under paragraphs (a) and (b) of section 91 (1);

(c) the right of the data subject to be notified-

(i) under section 92 (10) of the restriction of the processing of personal data under subsection (9) of that section, or

(ii) under section 92 (11) of a decision not to rectify or erase data pursuant to a request under subsection (1) or (3) of that section, as the case may be.

(5) Subject to subsection (6), where a controller restricts, pursuant to subsection (1), the exercise of the right of a data subject specified in paragraph (b) or (c) of subsection (4), the controller shall notify the data subject in writing of-

(a) the restriction of the exercise of the said right and the reasons for such restriction, and

(b) the right of the data subject-

(i) under section 95 to request the Commission to verify the lawfulness of the processing concerned, or

(ii) under section 128 to seek a judicial remedy in relation to the said restriction.

(6) Subsection (5) shall not apply where to notify the data subject in accordance with that subsection of the matters specified therein would be contrary to a purpose specified in subsection (2).

(7) Where a controller restricts, pursuant to subsection (1), the exercise of the right of a data subject specified in paragraph (b) or (c) of subsection (4), the controller shall-

(a) create and maintain a record in writing of the factual or legal basis for the decision to so restrict the right concerned, and

(b) make such a record available to the Commission, if so requested by the Commission.

(8) Regulations may be made specifying a category of processing to be a category of processing in respect of which the exercise of the rights specified in subsection (4) may, in accordance with subsection (2), be restricted under subsection (1).

(9) Regulations under subsection (8) may be made by-

(a) the Minister, following consultation with such other Minister of the Government as he or she considers appropriate and the Commission, or

(b) any other Minister of the Government, following consultation with the Minister, such other Minister of the Government as he or she considers appropriate and the Commission.

(10) The Minister of the Government making regulations under subsection (8) shall have regard to-

(a) the nature, scope and purposes of the category of processing concerned,

(b) whether, having regard to the matters referred to in paragraph (a), the restriction concerned is one to which subsection (2) would apply, and

(c) any risks arising for the rights and freedoms of data subjects.

(11) Regulations made under this section shall-

(a) respect the essence of the right to data protection and protect the interests of the data subject, and

(b) restrict the exercise of data subject rights only in so far as is necessary and proportionate to the aim sought to be achieved.

(12) For the purposes of this section, "penal institution" means-

(a) a place to which the Prisons Acts 1826 to 2015 apply, or

(b) a military prison or detention barrack within the meaning, in each case, of the Defence Act 1954 .

Indirect exercise of rights and verification by Commission

95. (1) Where an individual-

(a) is aware, having been notified under section 94 (5), that the exercise of his or her rights have been restricted by a controller pursuant to section 94 , or

(b) believes that the exercise of his or her rights have been so restricted and that he or she has not been notified of the said restriction by virtue of the operation of subsection (6) of that section,

the individual may make a request in writing to the Commission to verify whether the controller is processing personal data relating to him or her and if so, whether the processing is in compliance with this Part.

(2) Where the Commission receives a request under subsection (1), it may take such steps as appear to it to be appropriate, including the exercise of its powers under section 132 .

(3) The Commission, having taken the steps referred to in subsection (2), shall inform the individual making the request under subsection (1)-

(a) that all necessary verifications or reviews have been carried out by the Commission, and

(b) of his or her right to seek a judicial remedy under section 128 .

(4) Nothing in this section shall require the Commission to disclose to a data subject whether or not a controller has processed, or is processing, personal data relating to him or her.

Chapter 5

Transfers of personal data to third countries or international organisations

Transfer to third country or international organisation

96. (1) The transfer of personal data to a third country or an international organisation shall not take place, subject to section 100 , unless-

(a) the transfer is necessary for a purpose specified in section 70 (1)(a),

(b) the personal data are to be transferred to a controller in a third country or an international organisation that is an authority competent for the purposes specified in section 70 (1)(a),

(c) where the personal data were transmitted or made available to the controller making the transfer from a controller in another Member State, subject to subsection (2), the controller in the other Member State or another relevant controller in that state has given its prior authorisation to the transfer,

(d) section 97 , 98 or 99 applies, and

(e) the transfer is subject to a condition that a subsequent transfer to another third country or international organisation from the third country or international organisation to which the data are being transferred by the controller shall only occur where the controller authorises the subsequent transfer, having taken into due account all relevant factors, including-

(i) the seriousness of any criminal offence to which the data relate,

(ii) the purpose for which the data were originally transferred, and

(iii) the level of protection for personal data in the third country or the international organisation to which the data are to be transferred onwards.

(2) Subsection (1)(c) shall not apply where-

(a) the transfer of the personal data concerned is necessary for the prevention of an immediate and serious threat to-

(i) public security in a Member State or a third country, or

(ii) the essential interests of a Member State,

and

(b) an authorisation under the said subsection (1)(c) cannot be obtained in good time.

(3) Where subsection (2) applies and personal data are transferred to a third country or an international organisation without an authorisation from the controller in the other Member State that transmitted or made available the personal data, the controller making the transfer, or on whose behalf the transfer is being made, shall inform the controller in the other Member State of the transfer without delay.

(4) Without prejudice to the generality of section 71, a processor shall not transfer personal data to a third country or an international organisation, or to a recipient in a third country, under this Chapter unless explicitly instructed in writing to do so by the controller.

Adequacy decision

97. (1) Personal data may be transferred in accordance with section 96 (1), subject to subsection (2), to a third country or an international organisation where a decision has been taken by the European Commission under Article 36 of the Directive that the third country or the international organisation, as the case may be, ensures an adequate level of protection of personal data.

(2) Where the European Commission has taken a decision under Article 36 of the Directive that applies to a specified territory within a third country or a specified sector in a third country, personal data may be transferred under subsection (1) to a controller in the specified territory or sector only, as the case may be.

Transfer subject to appropriate safeguards

98. (1) Personal data may be transferred in accordance with section 96 (1) to a third country, a territory or sector thereof, or an international organisation, in respect of which a decision has not been taken by the European Commission under Article 36 of the Directive that the third country, territory or sector thereof, or the international organisation, as the case may be, ensures an adequate level of protection of personal data, where-

(a) there is a legally binding instrument that applies to the transfer and that ensures appropriate safeguards with regard to the processing of personal data, or

(b) the controller transferring the personal data, or on whose behalf the personal data are being transferred, has-

(i) assessed all the circumstances relating to the transfer, and

(ii) is satisfied that appropriate safeguards exist with regard to the protection of the personal data.

(2) Where personal data are transferred to a third country, a territory or sector thereof, or an international organisation pursuant to subsection (1)(b), the controller transferring the personal data, or on whose behalf the personal data are being transferred, shall-

(a) inform the Commission about each category of such transfers, and

(b) create and maintain a record in writing of each such transfer containing at least the following:

(i) details of the personal data transferred;

(ii) the date and time of the transfer;

(iii) information about the controller in the third country or the international organisation to which the data were transferred;

(iv) the reasons for the transfer.

(3) A controller shall make available a record created and maintained pursuant to subsection (2)(b) to the Commission for inspection upon a request in that regard by the Commission.

Derogations for specific situations

99. (1) Where section 97 or 98 does not apply in relation to a transfer of personal data to a third country or an international organisation, personal data may be transferred in accordance with section 96 (1) to the third country or the international organisation, where the transfer is necessary-

(a) to protect the vital interests of the data subject or another individual,

(b) to safeguard the legitimate interests of a data subject,

(c) for the prevention of an immediate and serious threat to public security in a Member State or a third country,

(d) subject to subsection (2), in an individual case, for a purpose specified in section 70 (1)(a), or

(e) subject to subsection (2), in an individual case, for the establishment, exercise or defence of legal claims relating to a purpose specified in section 70 (1)(a).

(2) Paragraphs (d) and (e) of subsection (1) shall not apply where the controller transferring the personal data, or on whose behalf the personal data are being transferred, is of the opinion that the rights and freedoms of the data subject override the public interest in the transfer concerned.

(3) Where personal data are transferred to a third country or an international organisation pursuant to subsection (1), the controller transferring the personal data, or on whose behalf the personal data are being transferred, shall create and maintain a record in writing of each such transfer containing at least the following:

(a) details of the personal data transferred;

(b) the date and the time of the transfer;

(c) information about the controller in the third country or the international organisation to which the data were transferred;

(d) the reasons for the transfer.

(4) A controller shall make available a record created and maintained pursuant to subsection (3) to the Commission for inspection upon a request in that regard by the Commission.

Transfer to recipient in third country

100. (1) Notwithstanding section 96 (1)(b) and the provisions of any relevant international agreement, a controller may, in an individual case, transfer personal data directly to a recipient located in a third country who is not a controller or organisation referred to in section 96 (1)(b) where the relevant provisions of this Part are complied with and each of the following conditions are fulfilled-

(a) the transfer is necessary for the performance of a function of the controller making the transfer under the law of the European Union or the law of the State for a purpose specified in section 70 (1)(a);

(b) the transfer is in the public interest;

(c) the controller is satisfied that the fundamental rights and freedoms of the data subject do not override the public interest necessitating the transfer in the particular instance;

(d) the controller is satisfied that the transfer of the data to an authority in the third country that is competent for the purposes specified in section 70 (1)(a) would be ineffective or inappropriate, having

regard to the purpose for which the data are being transferred, in particular where the transfer could not be made to such an authority in time to achieve the purpose of the transfer.

(2) A controller, when transferring personal data to a recipient pursuant to subsection (1) shall-

(a) specify to the recipient the purpose for which the recipient may process the data, and

(b) inform the recipient that the data are to be processed by the recipient for the specified purpose only and then only to the extent that such processing is necessary for that purpose.

(3) Where a controller transfers personal data to a recipient pursuant to subsection (1), the controller shall-

(a) notify the relevant authority in the third country that is competent for the purpose for which the data are transferred of the transfer without undue delay, unless to do so would be ineffective or inappropriate, having regard to the purpose for which the data are being transferred,

(b) notify the Commission of the transfer, and

(c) create and maintain a record in writing of the transfer containing at least the following information:

(i) details of the personal data transferred;

(ii) the date and the time of the transfer;

(iii) the identity of the recipient;

(iv) the reason for which the data were transferred.

(4) A controller shall make available a record created and maintained pursuant to subsection (3)(c) to the Commission for inspection upon a request in that regard by the Commission.

(5) In this section-

“controller” means a controller that is a competent authority specified in paragraph (a) of the definition of “competent authority” in section 69 ;

“relevant international agreement” means an international agreement-

(a) to which the State and the third country in which the recipient is located are parties, and

(b) that relates to judicial cooperation in criminal matters or to police cooperation.

Chapter 6

Independent supervisory authority

Functions of Commission under Part 5

101. (1) Subject to subsection (2), the functions of the Commission under this Part shall be to-

- (a) monitor and enforce application of this Part and regulations made under it,
- (b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing,
- (c) advise, on request by the body concerned, the Houses of the Oireachtas, Government and public authorities on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to processing,
- (d) promote the awareness of controllers and processors of their obligations under this Part and the Directive,
- (e) provide, on request by them, information to data subjects on the exercise of their rights under this Part and the Directive and, where appropriate, cooperate with the supervisory authorities of other Member States for that purpose,
- (f) handle, in accordance with Part 6, complaints lodged by or on behalf of a data subject under Chapter 3 of that Part,
- (g) examine the lawfulness of processing pursuant to section 95 and inform the data subject within a reasonable period of the outcome of the examination or of the reasons why the examination has not been carried out,
- (h) cooperate with, and provide mutual assistance to, other supervisory authorities in accordance with section 103 and Chapter VII of the Directive with a view to ensuring consistent application and enforcement of the Directive,
- (i) conduct, of its own volition or on the basis of information received from another supervisory authority or other public authority, investigations, in accordance with Part 6, on the application of this Part,
- (j) monitor relevant developments insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies,
- (k) provide advice to a controller or processor, as the case may be, pursuant to section 84 , and
- (l) contribute to the activities of the European Data Protection Board.

(2) The Commission shall not be competent for the supervision of data processing operations of the courts when acting in their judicial capacity.

(3) Subject to subsections (4) and (5), the Commission shall not charge a data subject or data protection officer a fee in respect of the performance by it of its functions under this section.

(4) Where a request referred to in Article 46(4) of the Directive is manifestly unfounded or excessive, the Commission may-

(a) charge the person who made the request a reasonable fee, based on its administrative costs, or

(b) refuse to act on the request.

(5) It shall be for the Commission to demonstrate that a request referred to in subsection (4) is manifestly unfounded or excessive.

(6) In this section, “excessive” includes, in particular, repetitive.

(7) For the purposes of this section, a request is repetitive where it is substantially the same as a request previously made by or on behalf of the same person and dealt with under this Part.

Power of the Commission to advise and issue opinions

102. The Commission shall have the power to issue opinions on matters related to the protection of personal data to-

(a) on its own initiative or on request by the body concerned, the Houses of the Oireachtas, Government, public authorities and bodies, and

(b) on its own initiative, the public.

Mutual assistance

103. (1) The Commission shall, for the purposes referred to in section 101 (1)(h)-

(a) in accordance with this Chapter, provide other supervisory authorities with mutual assistance, and

(b) put in place measures for effective cooperation with those authorities.

(2) The Commission, on receipt by it of a request of another supervisory authority (“requesting supervisory authority”) shall-

(a) without undue delay and no later than one month after receiving the request, take all appropriate measures required to reply to the request, and

(b) inform the requesting supervisory authority of the results of, or progress made in response to, the request.

(3) The measures referred to in subsection (2)(a) include the exercise by the Commission of its powers under Chapters 3, 4 and 5 of Part 6.

(4) (a) The Commission shall not refuse to comply with a request unless-

(i) it is not responsible under the Directive for the subject matter of the request or for the measures it is requested to carry out, or

(ii) compliance with the request would infringe the law of the State or European Union.

(b) The Commission shall provide the requesting supervisory authority concerned with the reasons for its refusal under paragraph (a) to comply with a request.

(5) The Commission, where providing information to a requesting supervisory authority in response to a request, shall, insofar as practicable, and in accordance with any implementing acts to which Article 50(8) of the Directive apply, do so-

(a) by electronic means, and

(b) using a standardised format, if any.

(6) Without prejudice to subsection (7), the Commission shall not charge a fee for any action taken in response to a request for mutual assistance.

(7) The Commission may enter into an agreement with other supervisory authorities on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

(8) In this section and section 104 -

“mutual assistance” includes-

(a) responding to requests for information, and

(b) undertaking supervisory measures, such as the carrying out of inspections or investigations under Part 6 or consultations;

“request” means a request for mutual assistance referred to in Article 50 of the Directive.

Requests by Commission for mutual assistance

104. (1) A request by the Commission to another supervisory authority shall contain all the information necessary for the purpose of the request, which shall include the purpose of and reasons for the request.

(2) The Commission shall use information received by it from another supervisory authority in response to a request only for the purpose for which it was requested.

PART 6

Enforcement of Data Protection Regulation and Directive

Chapter 1

Preliminary

Interpretation (Part 6)

105. (1) In this Part-

“complaint” means a complaint within the meaning of Chapter 2 or 3;

“investigation” means an investigation under Chapter 5;

“investigation report” has the meaning assigned to it by section 139 ;

“relevant enactment” means-

(a) the Data Protection Regulation, or

(b) a provision of this Act, or a regulation under this Act, that gives further effect to the Data Protection Regulation;

“relevant provision” means a provision of this Act, or a regulation under this Act, that gives effect to the Directive.

(2) A reference in this Part (other than in Chapter 2) to a controller or a processor includes a reference to a controller or a processor, as the case may be, within the meaning of Part 5.

(3) Where a person is a controller by virtue of his or her being the subject of a designation under subsection (1) or (2) of section 3 -

(a) a reference in sections 117 , 128 and 135 (10) to a controller shall be deemed to be a reference to the appropriate authority that, or the Minister who, made the designation, and not to the person, and

(b) a reference in sections 132 (6) and 133 (10) to a controller shall be deemed not to include a reference to the person.

(4) A reference in this Part to information obtained in an inquiry (within the meaning of section 110 or 123) shall be construed as including, where applicable-

(a) an investigation report prepared in the course of the inquiry, and any submissions annexed to the report, and

(b) any additional information obtained, in the course of the inquiry, by the Commission under section 140 (2).

Service of documents (Part 6)

106. (1) Subject to section 116 (4)(a), a notice or other document that is required to be served on or given to a person under this Part shall be addressed to the person concerned by name and shall be so served on or given to the person in one of the following ways:

(a) by delivering it to the person;

(b) by leaving it at the address at which the person ordinarily resides or carries on business or, in a case in which an address for service has been furnished, at that address;

(c) by sending it by post in a prepaid registered letter or by any other form of recorded delivery service to the address referred to in paragraph (b); or

(d) by electronic means, in a case in which the person has given notice in writing to the person serving or giving the notice or document concerned of his or her consent to the notice or document (or notices or documents of a class to which the notice or document belongs) being served on, or given to, him or her in that manner.

(2) For the purposes of this section, a company within the meaning of the Act of 2014 is deemed to be ordinarily resident at its registered office, and every other body corporate and every unincorporated body of persons shall be deemed to be ordinarily resident at its principal office or place of business.

Chapter 2

Enforcement of Data Protection Regulation

Interpretation (Chapter 2)

107. In this Chapter-

“complainant” means a data subject who lodges a complaint or, as the case may be, a not-for-profit body, organisation or association that, in accordance with Article 80(1), lodges a complaint on behalf of a data subject;

“complaint” means a complaint lodged pursuant to Article 77(1) or in accordance with Article 80(1), and shall be deemed to include a complaint so lodged by or on behalf of a data subject where-

(a) the data subject considers that the processing of personal data relating to him or her infringes a relevant enactment, and

(b) the Commission is the competent supervisory authority in respect of the complaint;

“corrective power” means a power conferred by Article 58(2) of the Data Protection Regulation;

“infringement” means an infringement of a relevant enactment;

“inquiry” means an inquiry referred to in section 110 (1).

Complaints under Chapter 2: General

108. (1) Where a complaint is lodged with the Commission, the Commission shall, as soon as practicable, give the complainant concerned a notice in writing acknowledging the lodging of the complaint, and informing the complainant of-

(a) where the Commission is the competent supervisory authority in respect of the complaint, the complainant’s right under section 150 (5) and (7), and

(b) where a supervisory authority other than the Commission is the competent supervisory authority in respect of the complaint, the complainant’s right to a judicial remedy against that competent supervisory authority where it does not-

(i) handle the complaint, or

(ii) inform the complainant within 3 months from the date on which the complaint is received by that authority on the progress or outcome of the complaint.

(2) Where the Commission is the competent supervisory authority in respect of a complaint, it shall-

(a) handle the complaint in accordance with this Part, and

(b) inform the complainant, within 3 months from the date on which the complaint is received by the Commission, on the progress or outcome of the complaint.

(3) For the purposes of subsection (2)(b), the Commission shall be taken to have informed a complainant of the outcome of the complaint concerned where it gives the complainant a notice under section 109 (6) or, as the case may be, section 116 .

Commission to handle complaint under Chapter 2

109. (1) For the purposes of section 108 (2)(a), the Commission shall examine the complaint and shall, in accordance with this section, take such action in respect of it as the Commission, having regard to the nature and circumstances of the complaint, considers appropriate.

(2) The Commission, where it considers that there is a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint, may take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.

(3) Where the parties concerned reach an amicable resolution of the subject matter of the complaint, the complaint shall, from the date on which the amicable resolution is reached, be deemed to have been withdrawn by the complainant concerned.

(4) Where the Commission considers that an amicable resolution cannot be reached by the parties within a reasonable time, it shall proceed-

(a) in the case of a complaint to which section 113 applies, to comply with section 113 (2), or

(b) in the case of any other complaint, to take an action specified in subsection (5).

(5) The actions referred to in subsection (4)(b) include one or more than one of the following:

(a) rejection of the complaint;

(b) dismissal of the complaint;

(c) provision to the complainant of advice in relation to the subject matter of the complaint;

(d) serving on the controller or processor concerned of an enforcement notice, requiring it to do one or more than one of the following:

(i) comply with the data subject's request to exercise his or her rights pursuant to a relevant enactment;

(ii) where the enforcement notice is given to the controller, communicate a personal data breach to the data subject;

(iii) rectify or erase personal data or restrict processing pursuant to Article 16, 17 or 18, and, in respect of that action, to comply with Article 19 and, where applicable, Article 17(2);

(e) causing of such inquiry as the Commission thinks fit to be conducted in respect of the complaint;

(f) taking of such other action in respect of the complaint as the Commission considers appropriate.

(6) The Commission shall, as soon as practicable after taking an action referred to in subsection (5) (other than paragraph (e) of that subsection), give the complainant a notice in writing informing the complainant of the action taken.

Commission may conduct inquiry into suspected infringement of relevant enactment

110. (1) The Commission, whether for the purpose of section 109 (5)(e), section 113 (2), or of its own volition, may, in order to ascertain whether an infringement has occurred or is occurring, cause such inquiry as it thinks fit to be conducted for that purpose.

(2) The Commission may, for the purposes of subsection (1), where it considers it appropriate to do so, in particular do either or both of the following:

(a) cause any of its powers under Chapter 4 (other than section 135) to be exercised;

(b) cause an investigation under Chapter 5 to be carried out.

Decision of Commission where inquiry under Chapter 2 conducted of own volition

111. (1) Where an inquiry has been conducted of the Commission's own volition, the Commission, having considered the information obtained in the inquiry, shall-

(a) if satisfied that an infringement by the controller or processor to which the inquiry relates has occurred or is occurring, make a decision to that effect, and

(b) if not so satisfied, make a decision to that effect.

(2) Where the Commission makes a decision under subsection (1)(a), it shall, in addition, make a decision-

(a) as to whether a corrective power should be exercised in respect of the controller or processor concerned, and

(b) where it decides to so exercise a corrective power, the corrective power that is to be exercised.

(3) The Commission, where it makes a decision referred to in subsection (2)(b), shall exercise the corrective power concerned.

Decision of Commission where inquiry conducted in respect of complaint to which Article 55 or 56(5) applies

112. (1) Where an inquiry has been conducted in respect of a complaint in respect of which the Commission is the competent supervisory authority under Article 55 or 56(5), the Commission, having considered the information obtained in the examination, may-

(a) if satisfied that an infringement by the controller or processor to which the complaint relates has occurred or is occurring, make a decision to that effect, or

(b) if not so satisfied, make a decision to dismiss the complaint.

(2) Where the Commission makes a decision under subsection (1)(a), it shall, in addition, make a decision-

(a) as to whether a corrective power should be exercised in respect of the controller or processor concerned, and

(b) where it decides to so exercise a corrective power, the corrective power that is to be exercised.

(3) The Commission, where it makes a decision referred to in subsection (2)(b), shall exercise the corrective power concerned.

Complaint to which Article 60 applies

113. (1) This section applies to a complaint in respect of which the Commission is the lead supervisory authority.

(2) Where section 109 (4)(a) applies, the Commission shall-

(a) in accordance with subsection (3), make a draft decision in respect of the complaint (or, as the case may be, part of the complaint) and, where applicable, as to the envisaged action to be taken in relation to the controller or processor concerned, and

(b) in accordance with Article 60 and, where appropriate, Article 65, adopt its decision in respect of the complaint or, as the case may be, part of the complaint.

(3) In making a draft decision under subsection (2)(a), the Commission shall, where applicable, have regard to-

(a) the information obtained by the Commission in its examination of the complaint, including, where an inquiry has been conducted in respect of the complaint, the information obtained in the inquiry, and

(b) any draft for a decision that is submitted to the Commission by a supervisory authority in accordance with Article 56(4).

(4) Where the Commission adopts a decision under subsection (2)(b) to the effect that an infringement by the controller or processor concerned has occurred or is occurring, it shall, in addition, make a decision-

(a) where an inquiry has been conducted in respect of the complaint-

(i) as to whether a corrective power should be exercised in respect of the controller or processor concerned, and

(ii) where it decides to so exercise a corrective power, the corrective power that is to be exercised,
or

(b) where an inquiry has not been conducted in respect of the complaint-

(i) as to whether an action specified in subsection (6) should be taken in respect of the controller or processor concerned, and

(ii) where it decides to take such an action, the action that is to be taken.

(5) The Commission, in making its decision under subsection (4), shall have due regard to the decision as to the envisaged action to be taken in relation to the controller or processor included in the Commission's draft decision under subsection (2)(a) or, as the case may be, its revised draft decision under Article 60.

(6) The actions referred to in subsection (4)(b) include either or both of the following:

(a) the serving on the controller or processor concerned of an enforcement notice, requiring it to do one or more than one of the following:

(i) comply with the data subject's request to exercise his or her rights pursuant to a relevant enactment;

(ii) where the enforcement notice is given to the controller, communicate a personal data breach to the data subject;

(iii) rectify or erase personal data or restrict processing pursuant to Article 16, 17 or 18, and, in respect of that action, to comply with Article 19 and, where applicable, Article 17(2);

(b) the taking of such other action in respect of the complaint as the Commission considers appropriate.

(7) The Commission-

(a) where it makes a decision referred to in subsection (4)(a)(ii), shall exercise the corrective power concerned, and

(b) where it makes a decision referred to in subsection (4)(b)(ii), shall take the action concerned.

Commission to adopt decision in certain circumstances

114. Where-

(a) a complaint is lodged with the Commission, or a complaint is lodged with another supervisory authority and the Commission is the supervisory authority in respect of the complainant concerned,

(b) another supervisory authority is the lead supervisory authority in respect of the complaint, and
(c) a decision is made, in accordance with Article 60, to dismiss or reject the complaint or, where Article 60(9) applies, part of the complaint,
the Commission shall adopt the decision referred to in paragraph (c) in respect of the complaint or, as the case may be, part of the complaint.

Exercise by Commission of corrective power

115. (1) For the purposes of exercising a corrective power under section 111 , 112 or 113, the Commission may do either or both of the following:

(a) subject to Chapter 6, decide to impose an administrative fine on the controller or processor concerned;

(b) exercise any other corrective power specified in Article 58(2).

(2) Without prejudice to the generality of subsection (1)(b), the Commission may, for the purposes of exercising a power referred to in that provision, serve on the controller or processor concerned an enforcement notice requiring it to take such steps as the Commission considers necessary for those purposes.

Notification of decision of Commission under Chapter 2

116. (1) The Commission shall-

(a) as soon as practicable after it makes a decision under section 111 or 112, give the controller or processor concerned a notice in writing setting out-

(i) the decision and the reasons for it, and

(ii) where applicable, the corrective power that the Commission has decided to exercise in respect of the controller or processor,

and

(b) in the case of a decision under section 112 , and as soon as practicable after the giving of the notice under paragraph (a), give the complainant concerned a notice in writing setting out-

(i) the decision and the reasons for it, and

(ii) where applicable, the corrective power that the Commission has decided to exercise in respect of the controller or processor.

(2) Subject to subsection (4), the Commission shall-

(a) as soon as practicable after it adopts a decision under section 113 (2)(b), give the controller or processor concerned a notice in writing setting out-

(i) the decision and the reasons for it, and

(ii) where applicable, the corrective power that the Commission has decided to exercise or, as the case may be, the action that it has decided to take, in respect of the controller or processor,

and

(b) in the case of a complaint lodged with the Commission, and as soon as practicable after the giving of the notice under paragraph (a), give the complainant concerned a notice in writing setting out-

(i) the decision and the reasons for it, and

(ii) where applicable, the corrective power that the Commission has decided to exercise or, as the case may be, the action that it has decided to take, in respect of the controller or processor.

(3) The Commission shall, as soon as practicable after it adopts a decision under section 114 , give-

(a) the complainant concerned, and

(b) the controller or processor concerned,

a notice in writing informing them of the rejection or dismissal of the complaint or, as the case may be, the part of the complaint.

(4) Where the Commission is the lead supervisory authority in relation to a complaint to which Article 60(9) applies, the Commission shall, as soon as practicable after it adopts its decision under Article 60(9)-

(a) give the controller or processor concerned, at its main establishment or single establishment, a notice in writing setting out-

(i) the decision and the reasons for it, and

(ii) where applicable, the corrective power that the Commission has decided to exercise or, as the case may be, the action that it has decided to take in respect of the controller or processor,

and

(b) give the complainant concerned a notice in writing setting out-

(i) the decision and the reasons for it, and

(ii) where applicable, the corrective power that the Commission has decided to exercise or, as the case may be, the action that it has decided to take in respect of the controller or processor.

Judicial remedy for infringement of relevant enactment

117. (1) Subject to subsection (9), and without prejudice to any other remedy available to him or her, including his or her right to lodge a complaint, a data subject may, where he or she considers that his or her rights under a relevant enactment have been infringed as a result of the processing of his or her personal data in a manner that fails to comply with a relevant enactment, bring an action (in this section referred to as a “data protection action”) against the controller or processor concerned.

(2) A data protection action shall be deemed, for the purposes of every enactment and rule of law, to be an action founded on tort.

(3) The Circuit Court shall, subject to subsections (5) and (6), concurrently with the High Court, have jurisdiction to hear and determine data protection actions.

(4) The court hearing a data protection action shall have the power to grant to the plaintiff one or more than one of the following reliefs:

(a) relief by way of injunction or declaration; or

(b) compensation for damage suffered by the plaintiff as a result of the infringement of a relevant enactment.

(5) The compensation recoverable in a data protection action in the Circuit Court shall not exceed the amount standing prescribed, for the time being by law, as the limit of that court’s jurisdiction in tort.

(6) The jurisdiction conferred on the Circuit Court by this section may be exercised by the judge of any circuit in which-

(a) the controller or processor against whom the data protection action is taken has an establishment, or

(b) the data subject has his or her habitual residence.

(7) A data protection action may be brought on behalf of a data subject by a not-for-profit body, organisation or association to which Article 80(1) applies that has been mandated by the data subject to do so.

(8) The court hearing a data protection action brought by a not-for-profit body, organisation or association under subsection (7) shall have the power to grant to the data subject on whose behalf the action is being brought one or more of the following reliefs:

(a) relief by way of injunction or declaration; or

(b) compensation for damage suffered by the plaintiff as a result of the infringement of the relevant enactment.

(9) A data subject may not bring a data protection action against a controller or processor that is a public authority of another Member State acting in the exercise of its public powers.

(10) In this section-

“damage” includes material and non-material damage;

“injunction” means-

(a) an interim injunction,

(b) an interlocutory injunction, or

(c) an injunction of indefinite duration.

Chapter 3

Enforcement of Directive

Interpretation (Chapter 3)

118. In this Chapter-

“competent supervisory authority” shall be construed in accordance with the Directive;

“complainant” means a data subject who or, as the case may be, a body mandated in accordance with section 120 that, lodges a complaint;

“complaint” means a complaint lodged in accordance with section 119 ;

“controller” and “processor” have the meanings they have in Part 5;

“corrective power” means a power conferred on the Commission by section 127 ;

“inquiry” means an inquiry referred to in section 123 ;

“infringement” means an infringement of a relevant provision.

Data subject may lodge complaint with Commission

119. (1) Without prejudice to any other remedy available to him or her, and subject to section 120 , a data subject who considers that processing of his or her personal data infringes a relevant provision, or provisions adopted by another Member State giving effect to a right to the data subject under the Directive, may lodge a complaint with the Commission.

(2) (a) Without prejudice to the right of a data subject under subsection (1), the Commission may specify the form of a complaint lodged under that subsection.

(b) When specifying a form under paragraph (a), the Commission shall, without excluding other means of communication, ensure that the form is capable of being completed electronically.

(3) The Commission, where it is not the competent supervisory authority in respect of a complaint lodged with it under subsection (1), shall-

(a) without undue delay, transmit the complaint to the competent supervisory authority, and

(b) inform the data subject of the transmission of the complaint.

(4) Where a complaint is transmitted to the Commission in accordance with the law of a Member State giving effect to Article 52(2) of the Directive, the complaint shall, for the purposes of this Part, be deemed to be a complaint lodged, on the date on which the complaint is received by the Commission, with the Commission in accordance with subsection (1).

Representation of data subjects

120. (1) A data subject may mandate a body, organisation or association to which subsection (2) applies to do either or both of the following on his or her behalf:

(a) lodge a complaint under section 119 ;

(b) exercise the rights referred to in section 128 and section 150 .

(2) This subsection applies to a body, organisation or association-

(a) that provides its services on a not-for-profit basis,

(b) that has been properly constituted in accordance with the law of the State or another Member State,

(c) whose objectives, as specified in the documents establishing the body, organisation or association concerned, are in the public interest, and

(d) that is active with regard to the protection of data subject rights and freedoms, including protection of their personal data.

(3) Where the Commission or a court, in performing its functions under this Act, has reasonable doubts as to whether a particular body, organisation or association is one to which subsection (2) applies, it may request the provision by the body, organisation or association concerned of such additional information as is necessary in order to confirm that it is such a body, organisation or association.

Complaints under Chapter 3: General

121. (1) Where a complaint is lodged, or deemed to be lodged, with the Commission under section 119 (1), and section 119 (3) does not apply to the complaint, the Commission shall as soon as practicable give the complainant concerned a notice-

(a) acknowledging the lodging of the complaint or, as the case may be, its receipt by the Commission referred to in section 119 (4), and

(b) informing the complainant of the complainant's rights under section 128 .

(2) Where subsection (1) applies, the Commission shall-

(a) handle the complaint in accordance with this Part, and

(b) inform the complainant within 3 months from the date on which the complaint is lodged, of the progress or outcome of the complaint.

(3) For the purposes of subsection (2)(b), the Commission shall be taken to have informed a complainant of the outcome of the complaint concerned where it gives the complainant a notice under section 122 (5) or, as the case may be, section 126 .

Commission to handle complaint under Chapter 3

122. (1) For the purposes of section 121 (2)(a), the Commission shall examine the complaint and shall, in accordance with this section, take such action in respect of it as the Commission, having regard to the nature and circumstances of the complaint, considers appropriate.

(2) The Commission, where it considers that there is a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint, may take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.

(3) Where the parties concerned reach an amicable resolution of the subject matter of the complaint, the complaint shall, from the date on which the amicable resolution is reached, be deemed to have been withdrawn by the complainant concerned.

(4) Where the Commission considers that an amicable resolution cannot be reached by the parties within a reasonable time, it shall proceed to take one or more than one of the following actions:

(a) rejection of the complaint;

(b) dismissal of the complaint;

(c) provision to the complainant of advice in relation to the subject matter of the complaint;

(d) serving on the controller or processor concerned of an enforcement notice, requiring it to do one or more than one of the following:

(i) comply with the data subject's request to exercise his or her rights under a relevant provision;

(ii) bring processing into compliance with a relevant provision, in a specified manner and within a specified period;

(iii) where the enforcement notice is given to the controller, communicate a personal data breach to data subjects;

(e) causing of such inquiry as the Commission thinks fit to be conducted in respect of the complaint;

(f) taking of such other action in respect of the complaint as the Commission considers appropriate.

(5) The Commission shall, as soon as practicable after taking an action referred to in subsection (4) (other than paragraph (e) of that subsection), give the complainant a notice in writing informing the complainant of the action taken.

Commission may conduct inquiry into suspected infringements of relevant provision

123. (1) The Commission, whether for the purpose of section 122 (4)(e) or of its own volition, may, in order to ascertain whether an infringement has occurred or is occurring, cause such inquiry as it thinks fit to be conducted for that purpose.

(2) The Commission may, for the purposes of subsection (1), where it considers it appropriate to do so, in particular do either or both of the following:

(a) cause any of its powers under Chapter 4 (other than sections 134 and 135) to be exercised;

(b) cause an investigation under Chapter 5 to be carried out.

Decision of Commission in respect of inquiry under Chapter 3 conducted of own volition

124. (1) Where an inquiry has been conducted of the Commission's own volition, the Commission, having considered the information obtained in the inquiry, shall-

(a) if satisfied that an infringement by the controller or processor to which the inquiry relates has occurred or is occurring, make a decision to that effect, or

(b) if not so satisfied, make a decision to that effect.

(2) Where the Commission makes a decision under subsection (1)(a), it shall, in addition, make a decision-

(a) as to whether a corrective power should be exercised in respect of the controller or processor concerned, and

(b) where it decides to so exercise a corrective power, the corrective power that is to be exercised.

(3) The Commission, where it makes a decision referred to in subsection (2)(b), shall exercise the corrective power concerned.

Decision of Commission where inquiry conducted in respect of complaint under Chapter 3

125. (1) Where an inquiry has been conducted in respect of a complaint, the Commission, having considered the information obtained in the inquiry, may-

(a) if satisfied that an infringement by the controller or processor to which the complaint relates has occurred or is occurring, make a decision to that effect, or

(b) if not so satisfied, make a decision to dismiss the complaint.

(2) Where the Commission makes a decision under subsection (1)(a), it shall, in addition, make a decision-

(a) as to whether a corrective power should be exercised in respect of the controller or processor concerned, and

(b) where it decides to so exercise a corrective power, the corrective power that is to be exercised.

(3) The Commission, where it makes a decision referred to in subsection (2)(b), shall exercise the corrective power concerned.

Notification of decision of Commission under Chapter 3

126. The Commission shall-

(a) as soon as practicable after the decision under section 124 or 125 is made by it, give the controller or processor concerned a notice in writing setting out-

(i) the decision and the reasons for it, and

(ii) where applicable, the corrective power that the Commission has exercised in respect of the controller or processor,

and

(b) in the case of a decision under section 125 , give, as soon as practicable after the notice under paragraph (a) is given, the complainant a notice in writing setting out-

(i) the decision and the reasons for it, and

(ii) where applicable, the corrective power that the Commission has exercised in respect of the controller or processor.

Corrective powers of Commission (Chapter 3)

127. (1) The Commission may, for the purposes of sections 124 (3) and 125 (3), do one or more than one of the following:

(a) issue a warning to the controller or processor that intended data processing is likely to infringe a relevant provision;

(b) issue a reprimand to the controller or processor where data processing by the controller or processor has infringed a relevant provision;

(c) order the controller or processor to comply with a data subject's request to exercise his or her rights under a relevant provision;

(d) order the controller or processor to bring processing into compliance with a relevant provision, in a specified manner and within a specified period;

(e) order the controller to communicate a personal data breach to data subjects;

(f) impose a temporary or definitive limitation, including a ban on processing;

(g) impose a restriction on processing by the controller or processor;

(h) order the suspension of data transfers to a recipient in a third country or to an international organisation.

(2) Without prejudice to the generality of sections 124 (2)(b) and 125 (2)(b), the Commission may, for the purposes of exercising a power specified in subsection (1), serve on the controller or processor concerned an enforcement notice requiring it to take such steps as the Commission considers necessary for those purposes.

Judicial remedy for infringement of relevant provision

128. (1) Subject to subsection (8), and without prejudice to any other remedy available to him or her, including his or her right under section 119 to lodge a complaint, a data subject may, where he or she considers that his or her rights under a relevant provision have been infringed as a result of the processing of his or her personal data in a manner that fails to comply with a relevant provision, bring an action (in this section referred to as a “data protection action”) against the controller or processor concerned.

(2) A data protection action shall be deemed, for the purposes of every enactment and rule of law, to be an action founded on tort.

(3) The Circuit Court shall, subject to subsections (5) and (6), concurrently with the High Court, have jurisdiction to hear and determine data protection actions.

(4) The court hearing a data protection action shall have the power to grant to the plaintiff one or more than one of the following reliefs:

(a) relief by way of injunction or declaration; or

(b) compensation for damage suffered by the plaintiff as a result of the infringement of a relevant provision.

(5) The compensation recoverable in a data protection action in the Circuit Court shall not exceed the amount standing prescribed, for the time being by law, as the limit of that court’s jurisdiction in tort.

(6) The jurisdiction conferred on the Circuit Court by this section may be exercised by the judge of any circuit in which-

(a) the controller or processor against whom the data protection action is taken has an establishment, or

(b) the data subject has his or her habitual residence.

(7) The court hearing a data protection action that has been brought, in accordance with section 120 (1)(b), on behalf of a data subject by a body, organisation or association to which subsection (2) of that section applies shall have the power to grant to the data subject on whose behalf the action is being brought one or more of the following reliefs:

(a) relief by way of injunction or declaration; or

(b) compensation for damage suffered by the plaintiff as a result of the infringement of the relevant enactment.

(8) A data subject may not bring a data protection action against a controller or processor that is a public authority of another Member State acting in the exercise of its public powers.

(9) In this section-

“damage” includes material and non-material damage;

“injunction” means-

(a) an interim injunction,

(b) an interlocutory injunction, or

(c) an injunction of indefinite duration.

Chapter 4

Inspection, Audit and Enforcement

Authorised officers

129. (1) The Commission may appoint such and so many members of its staff, and such and so many other suitably qualified persons, as it considers appropriate to be authorised officers for the purposes of this Act.

(2) A person appointed under subsection (1) shall, on his or her appointment, be furnished by the Commission with a certificate of his or her appointment and, when exercising a power conferred by this Act shall, on request by any person thereby affected, produce such certificate together with a form of personal identification to that person for inspection.

(3) A person who, immediately before the commencement of this section, was an authorised officer under section 24 of the Act of 1988 shall-

(a) for the unexpired period of his or her term of appointment under that section, and

(b) subject to the same terms and conditions as applied to that appointment,

be deemed to be an authorised officer appointed under subsection (1), and accordingly paragraph (a) of subsection (4) shall apply in respect of that authorised officer.

(4) An appointment shall cease-

(a) if the Commission revokes, in writing, the appointment,

(b) in the case of a person who at the time of his or her appointment was a member of staff of the Commission, upon the person ceasing to be such a member of staff, or

(c) in the case of an appointment for a fixed period, upon the expiry of that period.

(5) In this section, “suitably qualified person” means a person other than a member of staff of the Commission who, in the opinion of the Commission, has the expertise and experience necessary to perform the functions conferred on an authorised officer by this Act.

Powers of authorised officers

130. (1) For the purposes of this Act, a relevant enactment or a relevant provision, an authorised officer may-

(a) subject to subsection (6), enter, at any reasonable time, any place-

(i) where any activity connected with the processing of personal data takes place,

(ii) where the authorised officer has reasonable grounds for believing any activity connected with the processing of personal data takes place, or

(iii) at which the authorised officer has reasonable grounds for believing documents, records, statements or other information relating to the processing of personal data is being kept,

(b) search and inspect the place and any documents, records, statements or other information found there,

(c) require any person at the place, being a controller or processor, or an employee or agent of either of them, to produce to him or her any documents or records relating to the processing of personal data which are in that person’s power or control and, in the case of information in a non-legible form, to reproduce it in a legible form, and to give to the authorised officer such information as he or she may reasonably require in relation to any entries in such documents or records,

(d) secure for later inspection-

(i) any documents or records so provided or found and any data equipment, including any computer, in which those records may be held, or

(ii) any such place, or part thereof, in which-

(I) documents, records, statements or data equipment are kept, or

(II) there are reasonable grounds for believing that such documents, records, statements or data equipment are kept,

for such period as the authorised officer may reasonably consider necessary for the purposes of the performance of his or her functions or the functions of the Commission under this Act, a relevant enactment or a relevant provision,

(e) inspect and take extracts from or make copies of any such documents or records (including, in the case of information in a non-legible form, a copy of or extract from such information in a permanent legible form),

(f) remove and retain such documents or records for such period as the authorised officer reasonably considers necessary for the purposes of the performance of his or her functions or the functions of the Commission under this Act, a relevant enactment or a relevant provision, or require any person referred to in paragraph (c) to retain and maintain such documents or records for such period of time, as the authorised officer reasonably considers necessary for those purposes,

(g) if a person who is required under paragraph (c) to provide a particular record is unable to provide it, require the person to state, to the best of that person's knowledge and belief, where the record is located or from whom it may be obtained, and

(h) require any person referred to in paragraph (c) to give to the authorised officer any information relating to the processing of personal data that the officer may reasonably require for the purposes of the performance of his or her functions or the functions of the Commission under this Act, a relevant enactment or a relevant provision and to afford the officer all reasonable assistance in relation thereto.

(2) An authorised officer may, in the performance of his or her functions under this Act, a relevant enactment or a relevant provision-

(a) operate any data equipment, including any computer, or cause any such data equipment or computer to be operated by a person accompanying the authorised officer, and

(b) require any person who appears to the authorised officer to be in a position to facilitate access to the documents or records stored in any data equipment or computer or which can be accessed by the use of that data equipment or computer to give the authorised officer all reasonable assistance in relation to the operation of the data equipment or computer or access to the records stored in it, including by-

(i) providing the documents or records to the authorised officer in a form in which they can be taken and in which they are, or can be made, legible and comprehensible,

(ii) giving to the authorised officer any password necessary to make the documents or records concerned legible and comprehensible, or

(iii) otherwise enabling the authorised officer to examine the documents or records in a form in which they are legible and comprehensible.

(3) When performing a function under this Act, a relevant enactment or a relevant provision, an authorised officer may, subject to any warrant under section 131, be accompanied by such and so many other authorised officers or members of the Garda Síochána as he or she considers appropriate.

(4) An authorised officer may require a person to provide him or her with his or her name and address where the authorised officer has reasonable grounds for requiring such information for the purpose of applying for a warrant under section 131.

(5) Where an authorised officer in the performance of his or her functions or the functions of the Commission under this Act, a relevant enactment or a relevant provision is prevented from entering any place, he or she may make an application under section 131 for a warrant to authorise such entry.

(6) An authorised officer shall not enter a dwelling, other than-

(a) with the consent of the occupier, or

(b) in accordance with a warrant under section 131.

(7) A person shall be guilty of an offence if he or she-

(a) obstructs, impedes or assaults an authorised officer in the performance of his or her functions under this Act, a relevant enactment or a relevant provision,

(b) fails or refuses to comply with a requirement of an authorised officer under this section,

(c) alters, suppresses or destroys any documents, records, statements or other information which the person concerned has been required by an authorised officer to produce, or may reasonably expect to be so required to produce,

(d) in purported compliance with a requirement under this section, gives to an authorised officer information, documents or records which the person knows to be false or misleading in a material respect,

(e) falsely represents himself or herself to be an authorised officer, or

(f) procures or attempts to procure any action referred to in paragraphs (a) to (e).

(8) A person guilty of an offence under subsection (7) shall be liable-

(a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or

(b) on conviction on indictment, to a fine not exceeding €250,000 or imprisonment for a term not exceeding 5 years or both.

(9) A statement or admission made by a person pursuant to a requirement under subsection (1) or (2) shall not be admissible in evidence in proceedings for an offence (other than an offence under paragraph (b) of subsection (7)) brought against the person.

(10) In this section and section 131, “place” includes-

(a) a dwelling or a part thereof,

(b) a building or a part thereof,

(c) any other premises or part thereof, and

(d) a vehicle, vessel, aircraft or any other means of transport.

Search warrants

131. (1) If a judge of the District Court is satisfied on the sworn information of an authorised officer that there are reasonable grounds for suspecting that information required by an authorised officer for the purpose of performing his or her functions under this Part is held at any place, the judge may issue a warrant authorising him or her, accompanied if the officer considers it necessary by such other person or a member of the Garda Síochána, at any time or times from the date of issue of the warrant, on production, if so required, of the warrant, to enter, if need be by reasonable force, the place and exercise all or any of the powers conferred on an authorised officer under section 130 .

(2) The period of validity of a warrant shall be 28 days from its date of issue, but that period of validity may be extended in accordance with subsections (3) and (4).

(3) The authorised officer may, during the period of validity of a warrant (including such period as previously extended under subsection (4)), apply to a judge of the District Court for an order extending the period of validity of the warrant and such an application shall be grounded upon information on oath laid by the authorised officer stating, by reference to the purpose or purposes for which the warrant was issued, the reasons why the authorised officer considers the extension to be necessary.

(4) If, on the making of an application under subsection (3), the judge of the District Court is satisfied that there are reasonable grounds for believing, having regard to that information so laid, that further

time is needed so that the purpose or purposes for which the warrant was issued can be fulfilled, the judge may make an order extending the period of validity of the warrant by such period as, in the opinion of the judge, is appropriate and just; and where such an order is made, the judge shall cause the warrant to be suitably endorsed to indicate its extended period of validity.

(5) Nothing in subsections (1) to (4) prevents a judge of the District Court from issuing, on the making of a new application under subsection (1), a further search warrant under this section in relation to the same place.

Information notice

132. (1) The Commission or an authorised officer may, by notice in writing (referred to in this Act as an “information notice”) served on a controller or processor, require the controller or processor to furnish, in writing, within such period as may be specified in the notice and, if applicable, in the format or manner specified in the notice, such information in relation to matters specified in the notice as is necessary or expedient for the performance by the Commission of its, or by the authorised officer of his or her, functions under this Part.

(2) Subject to subsection (3)-

(a) an information notice shall include a statement informing the controller or processor concerned of his entitlement under section 150 (1) to appeal against the requirement specified in the notice,

(b) the period, referred to in subsection (1), specified in an information notice shall not be less than 28 days from the date on which the notice is served, and

(c) if an appeal is brought under section 150 (1) against a requirement specified in an information notice, the requirement need not be complied with and subsection (6) shall not apply in relation to the requirement, pending the determination or withdrawal of the appeal.

(3) Where the Commission or authorised officer-

(a) by reason of special circumstances, is of the opinion that a requirement specified in an information notice should be complied with urgently, and

(b) includes a statement to that effect in the information notice,

subsection (2) shall not apply in relation to the notice, but the notice-

(i) shall include a statement of the effect of subsections (3) and (4) of section 150 , and

(ii) shall not require compliance with the requirement before the end of the period of 7 days beginning on the date on which the notice is served.

(4) (a) Nothing in this section shall be taken to compel a controller or processor, in complying with an information notice, to furnish information that would be exempt from production in proceedings in a court on the ground of legal professional privilege.

(b) A document furnished in compliance with an information notice shall not be admissible in evidence in proceedings for an offence (other than an offence under this section) brought against any person who furnishes or concurs in the furnishing of the document.

(5) The controller or processor concerned shall inform the Commission of any documents, records, statements or other information withheld by it under subsection (4)(a).

(6) A controller or processor that without reasonable excuse fails to comply with a requirement specified in an information notice or that, in purported compliance with such a requirement, gives to the Commission or an authorised officer information which the controller or processor knows to be false or misleading in a material respect, shall be guilty of an offence and shall be liable-

(a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or

(b) on conviction on indictment, to a fine not exceeding €250,000 or imprisonment for a term not exceeding 5 years or both.

(7) (a) An information notice may be cancelled-

(i) where it has been issued by the Commission, by the Commission, and

(ii) where it has been issued by an authorised officer, by the Commission or that authorised officer.

(b) A person who cancels an information notice under paragraph (a) shall notify in writing the controller or processor on which the notice was served.

Enforcement notice

133. (1) In this Part, “enforcement notice” means a notice in writing served in accordance with subsection (2), subsection (3) or section 109 (5)(d), 115 (2), 122 (4)(d) or 127 (2), on a controller or processor, requiring the controller or processor to take such steps as are specified in the notice, within such time as may be so specified.

(2) Notwithstanding anything contained in Chapter 2, the Commission or an authorised officer, where of the opinion that a controller or processor has contravened or is contravening a relevant enactment, may serve on the controller or processor an enforcement notice requiring the controller or processor to take one or more than one of the steps specified in section 109 (5)(d).

(3) Notwithstanding anything contained in Chapter 3, the Commission or an authorised officer, where of the opinion that a controller or processor has contravened or is contravening a relevant provision, may serve on the controller or processor an enforcement notice requiring the controller or processor to take one or more than one of the steps specified in section 122 (4)(d).

(4) An enforcement notice shall include a statement informing the controller or processor concerned of its entitlement under section 150 (1) to appeal against a requirement specified in the notice.

(5) Where an enforcement notice is served under section 109 (5)(d), 122 (4)(d), subsection (2) or subsection (3)-

(a) the notice shall specify the relevant enactment or relevant provision, as applicable, that in the opinion of the Commission or, where applicable, authorised officer, has been or is being contravened and the reasons for having formed that opinion, and

(b) subject to subsection (6)-

(i) the period, referred to in subsection (1), specified in an enforcement notice shall be not less than 28 days from the date on which the notice is served, and

(ii) if an appeal is brought under section 150 (1) against a requirement specified in the notice, the requirement need not be complied with and, pending the determination or withdrawal of the appeal, subsections (9) and (10) shall not apply in relation to the requirement.

(6) Where the Commission or authorised officer-

(a) by reason of special circumstances, is of the opinion that a requirement specified in an enforcement notice referred to in subsection (5) should be complied with urgently, and

(b) includes a statement to that effect in the enforcement notice,

subsection (5)(b) shall not apply in relation to the notice, but the notice-

(i) shall include a statement of the effect of subsections (3) and (4) of section 150 , and

(ii) shall not require compliance with the requirement before the end of the period of 7 days beginning on the date on which the notice is served.

(7) (a) Subject to paragraph (b), a controller or processor, having complied with an enforcement notice, shall, as soon as may be and in any event not more than 28 days after such compliance, notify the following of the steps taken to comply with the enforcement notice:

(i) the Commission or the authorised officer concerned;

(ii) any data subject concerned.

(b) Where the compliance with an enforcement notice has involved the rectification or erasure of personal data or the restriction of processing, the controller and processor shall, in complying with paragraph (a), in addition-

(i) notify any recipient to whom the data have been disclosed, or

(ii) where compliance with subparagraph (i) proves impossible or involves a disproportionate effort, and where the data subject so requests, notify the data subject of the recipients or the categories of recipients.

(8) (a) An enforcement notice may be cancelled-

(i) where it has been issued by the Commission, by the Commission, and

(ii) where it has been issued by an authorised officer, by the Commission or that authorised officer.

(b) A person who cancels an enforcement notice under paragraph (a) shall notify in writing the controller or processor on which the notice was served.

(9) (a) The Commission may, subject to Chapter 6, decide to impose an administrative fine on a controller or processor that, without reasonable excuse, fails to comply with a requirement specified in an enforcement notice served on the controller or processor under section 109 (5)(d), 115 (2) or subsection (2).

(b) The Commission, as soon as practicable after making its decision under paragraph (a), shall give the controller or processor concerned a notice in writing informing it of the decision.

(10) A controller or processor that, without reasonable excuse, fails to comply with-

(a) a requirement specified in an enforcement notice, or

(b) subsection (7),

shall be guilty of an offence and shall be liable-

(i) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or

(ii) on conviction on indictment, to a fine not exceeding €250,000 or imprisonment for a term not exceeding 5 years or both.

Circumstances in which application may be made to the High Court for suspension or restriction of processing of data

134. (1) Without prejudice to Articles 58(2) and 66 of the Data Protection Regulation and subsection (4), the Commission, where it considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects under a relevant enactment, until steps or further steps are taken under the relevant enactment, may, on notice to the controller or processor concerned, make an application in a summary manner to the High Court for an order under subsection (2).

(2) The High Court may determine an application under subsection (1) by-

(a) making any order that it considers appropriate, including an order suspending, restricting or prohibiting-

(i) the processing by the controller or processor of the personal data concerned, or

(ii) the transfer by the controller or processor of such data to a recipient in a third country or to an international organisation,

for such period, or until the occurrence of such event, as is specified in the order, and

(b) giving to the Commission any other direction that the High Court considers appropriate.

(3) The Commission shall, on complying with a direction of the High Court under subsection (2)(b), give notice in writing to the controller or processor concerned of the Commission's compliance with the direction.

(4) Where the Commission considers that the immediate suspension, restriction or prohibition of the processing of personal data or the transfer of such data to a recipient in a third country or to an international organisation is necessary in order to protect the rights and freedoms of data subjects under a relevant enactment, it may apply in a summary manner *ex parte* to the High Court for an interim order under subsection (6).

(5) An application under subsection (4) shall be grounded on an affidavit sworn by or on behalf of the Commission.

(6) (a) The High Court may, on an application under subsection (4), where, having regard to the circumstances of the case, the Court considers it necessary to do so for the protection of the rights and freedoms of data subjects, make an interim order suspending, restricting or prohibiting-

- (i) the processing by the controller or processor of the personal data concerned, or
- (ii) the transfer by the controller or processor of such data to a recipient in a third country or to an international organisation.

(b) Without prejudice to subsection (7), where an interim order is made under this subsection, the Commission shall, as soon as is practicable, serve a copy of the order and of the affidavit referred to in subsection (5) on the controller or processor concerned.

(c) An interim order under this subsection shall have effect for such period, not exceeding 7 working days, as is specified in the order, and shall cease to have effect on the determination by the High Court of an application under subsection (1).

(7) (a) An interim order under subsection (6) shall take effect on notification of its making being given to the controller or processor.

(b) Oral communication to the controller or processor by or on behalf of the Commission of the fact that an interim order has been made, together with production of a copy of such order, shall, without prejudice to any other form of notification, be taken to be sufficient notification to the controller or processor concerned of the making of the order.

(8) The Commission shall communicate the details of an order made by the High Court under this section to the-

- (a) European Commission,
- (b) European Data Protection Board, and
- (c) other supervisory authorities concerned.

Power to require report

135. (1) The Commission may, for the purposes of proper and effective monitoring of the application of a relevant enactment, and having regard to the matters set out in subsection (3), by notice in writing given to a controller or processor, require the controller or processor to provide to the Commission, in accordance with such notice, a report on any matter specified in the notice about which the Commission has required or could require the provision of information, or the production of any statement, record or document under any provision of a relevant enactment.

(2) A notice under subsection (1) shall be in writing and shall state-

- (a) the date on which the notice is given,

(b) the period within which the controller or processor shall nominate a person to the Commission for approval under subsection (4),

(c) the purpose, scope and form of the report,

(d) the matters required to be reported on,

(e) the timetable for completion of the report,

(f) whether the report is to include recommendations in relation to the improved compliance by the controller or processor with a relevant enactment,

(g) where appropriate, the methodology to be used in preparation of the report, and

(h) such other matters relating to the report as the Commission considers appropriate.

(3) Before giving a notice under this section, the Commission, taking account of the purpose for which the report is required, shall have regard to at least the following matters-

(a) whether any other powers that may be exercised by the Commission may be more appropriate in the circumstances concerned,

(b) the relevant knowledge and expertise available to the controller or processor, and

(c) the level of resources available to the controller or processor and the likely benefit to the controller or processor of providing the report.

(4) A report required to be provided to the Commission under this section shall be prepared by a person (referred to as the "reviewer")-

(a) nominated by the controller or processor, within such period as is specified in the notice given under subsection (1), and approved by the Commission, or

(b) nominated by the Commission, where-

(i) no person is nominated by the controller or processor within the period specified in the notice under subsection (1), or

(ii) the Commission is not satisfied with the person so nominated.

(5) When considering whether to approve a nomination under subsection (4)(a) or make a nomination under subsection (4)(b), the Commission shall have regard to the circumstances giving rise to the requirement for a report and whether the person it proposes to so approve or nominate as reviewer appears to have-

- (a) the competence and expertise necessary to prepare the report,
 - (b) the ability to complete the report within the period specified by the Commission in the notice given under subsection (1),
 - (c) any relevant specialised knowledge, including specialised knowledge of the data processing activities carried on by the controller or processor and the matters to be reported on,
 - (d) any potential conflict of interest in reviewing the matters to be reported on,
 - (e) sufficient detachment, having regard to any existing professional or commercial relationship, to give an objective opinion, and
 - (f) any previous experience in preparing reports under this section or reports of a similar nature.
- (6) Where the Commission approves a nomination under subsection (4)(a) or makes a nomination under subsection (4)(b), it shall notify the controller or processor, in writing, accordingly.
- (7) Where the nomination of a reviewer is approved or made by the Commission under subsection (4), the controller or processor shall enter into a contract with the reviewer.
- (8) It shall be a term of the contract referred to in subsection (7)-
- (a) that the reviewer is required to prepare for the controller or processor a report in accordance with the notice given under subsection (1),
 - (b) that the reviewer is required and permitted to provide to the Commission the following where the Commission so requests:
 - (i) periodic updates on progress and issues arising;
 - (ii) interim reports; and
 - (iii) copies of any draft reports given to the controller or processor,
- and
- (c) that the contract is governed by the law of the State.
- (9) If the Commission considers it appropriate, it may request the controller or processor to provide the Commission with a copy of the draft contract before it is made and the Commission may require such modifications to the draft contract as it considers appropriate.
- (10) The costs of and incidental to the preparation of a report under this section shall be borne by the controller or processor.

(11) A controller or processor shall give all such assistance to a reviewer as he or she may reasonably require for the purposes of the preparation of a report under this section.

(12) A reviewer shall, where requested by the Commission, in such form and within such period as the Commission may specify, provide an explanation of all or any part of a report under this section or the recommendations, if any, made in the report, or of such other matters relating to the report as the Commission considers appropriate.

(13) The Commission shall not be bound by the content of a report under this section and such a report shall not be taken to be a decision or opinion of the Commission for any purpose.

(14) The Commission shall not be liable for any acts or omissions of a reviewer or controller or processor relating to a report under this section.

(15) A person who-

(a) obstructs or impedes a reviewer in the preparation of a report under this section,

(b) in relation to the preparation of a report under this section, gives information to a reviewer that the person knows to be false or misleading in a material respect, or

(c) is a reviewer and in relation to the preparation of a report under this section gives information to the Commission which the reviewer knows to be false or misleading in a material respect,

shall be guilty of an offence and shall be liable-

(i) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or

(ii) on conviction on indictment, to a fine not exceeding €250,000 or imprisonment for a term not exceeding 5 years or both.

Data Protection Audit

136. (1) Where Part 5 applies to a controller or processor, the Commission may carry out or cause to be carried out such examination in the form of an audit as it considers appropriate in order to determine whether the practices and procedures of the controller or processor are in compliance with that Part and regulations made under it.

(2) The Commission may, for the purposes of an audit under subsection (1) or a data protection audit, require the controller or processor concerned to produce any documents, records, statements or other

information within that person's possession or control, or within that person's procurement, that are relevant to or required for the conduct of the audit.

(3) Before commencing an audit under subsection (1), or a data protection audit, the Commission shall give the controller or processor concerned notice of its proposal to conduct such an audit, which notice shall-

(a) specify the matters to which the proposed audit will relate, and

(b) specify the date, which shall be not earlier than 7 days from the date on which the notice is given on which the audit will be commenced.

(4) In this section, "data protection audit" means a data protection audit conducted for the purpose of Article 58(1)(b) of the Data Protection Regulation.

Chapter 5

Investigations

Investigations

Investigations

137. (1) The Commission may, for the purposes of an inquiry referred to in section 110 (1) or 123 (1), cause such investigation as it thinks fit to be carried out.

(2) The Commission may, for the purposes of subsection (1), direct one or more authorised officers-

(a) to carry out the investigation, and

(b) to submit to the Commission an investigation report following the completion of the investigation.

(3) The Commission may define the scope and terms of the investigation to be carried out, whether as respects the matters or the period to which it is to extend or otherwise, and may, in particular, limit the investigation to matters connected with particular circumstances.

(4) Where more than one authorised officer has been directed to carry out an investigation, the investigation report shall be prepared jointly by the authorised officers so directed and this section and sections 138 to 140 shall, with all necessary modifications, be construed accordingly.

(5) As soon as is practicable after being appointed to carry out an investigation, the authorised officer shall-

(a) give the controller or processor concerned notice in writing-

(i) where the examination concerned is being carried out in respect of a complaint within the meaning of Chapter 2 or 3, setting out the particulars of the complaint concerned, or

(ii) where the examination is being carried out of the Commission's own volition, setting out the matters to which the investigation relates,

and

(b) afford to the controller or processor an opportunity to respond to the notice under paragraph (a) within 7 days from the date on which the notice was given (or such further period not exceeding 28 days as the authorised officer allows).

Conduct of investigation under section 137

138. (1) An authorised officer who has been directed under section 137 (2) to carry out an investigation may, for the purposes of the investigation-

(a) require a person, being a controller or processor, or an employee or agent of such controller or processor, who, in the authorised officer's opinion-

(i) possesses information that is relevant to the investigation, or

(ii) has any record or document within the person's possession or control or within the person's procurement that are relevant to the investigation,

to provide that record or document, as the case may be, to the authorised officer, and

(b) where the authorised officer thinks fit, require that person to attend before him or her for the purpose of so providing that information, record or document, as the case may be,

and the person shall comply with the requirement.

(2) A requirement under subsection (1) shall specify-

(a) a period within which, or a date and time on which, the person the subject of the requirement is to comply with the requirement, and

(b) as the authorised officer concerned thinks fit-

(i) the place at which the person shall attend to give the information concerned or to which the person shall deliver the record or document concerned, or

(ii) the place to which the person shall send the information, record or document concerned.

(3) A person required to attend before an authorised officer under subsection (2)-

(a) is also required to answer fully and truthfully any question put by the authorised officer, and

(b) if so required by the authorised officer, shall answer any such question under oath.

(4) Where it appears to an authorised officer that a person has failed or is failing to comply or fully comply with a requirement under subsection (2) or (3), the authorised officer may, on notice to the person and with the consent of the Commission, apply in a summary manner to the Circuit Court for an order under subsection (5).

(5) The Circuit Court, on hearing an application under subsection (4), where satisfied that the person concerned has failed or is failing to comply or fully comply with the requirement concerned, may-

(a) make an order requiring the person, within such period as the Court may specify, to comply or fully comply, as the case may be, with the requirement, or

(b) substitute a different requirement for the requirement concerned.

(6) The administration of an oath referred to in subsection (3)(b) by an authorised officer is hereby authorised.

(7) A person the subject of a requirement under subsection (1) or (3) shall be entitled to the same immunities and privileges in respect of compliance with such requirement as if the person were a witness before the High Court.

(8) Any statement or admission made by a person pursuant to a requirement under subsection (1) or (3) shall not be admissible in evidence in proceedings for an offence (other than an offence under subsection (12)) brought against the person, and this shall be explained to the person in ordinary language by the authorised officer concerned.

(9) Nothing in this section shall be taken to compel the production by any person of statements, records or other documents or other information which would be exempt from production in proceedings in a court on the ground of legal professional privilege.

(10) For the purposes of an investigation, an authorised officer may, if he or she thinks it proper to do so, of his or her own volition conduct an oral hearing.

(11) Schedule 3 shall have effect for the purposes of an oral hearing referred to in subsection (10).

(12) Subject to subsection (9), a person who-

(a) withholds, destroys, conceals or refuses to provide any information or statements, records or other documents required for the purposes of an investigation,

(b) fails or refuses to comply with any requirement of an authorised officer under this section,

(c) in purported compliance with a requirement under this section, gives to an authorised officer information, documents or records which the person knows to be false or misleading in a material respect, or

(d) otherwise obstructs or hinders an authorised officer in the performance of functions under this Act,

shall be guilty of an offence and shall be liable-

(i) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or

(ii) on conviction on indictment, to a fine not exceeding €250,000 or imprisonment for a term not exceeding 5 years or both.

(13) In this section, a reference to a document or record includes a reference to copies of such document or record.

(14) The powers conferred under this section on an authorised officer to whom subsection (1) applies are in addition to the powers conferred on such an authorised officer under Chapter 4.

Investigation report

139. (1) Where an authorised officer has completed an investigation, he or she shall, as soon as is practicable after having considered, in so far as they are relevant to the investigation-

(a) any information, records or other documents provided to him or her,

(b) any statement or admission made by any person,

(c) any submissions made, and

(d) any evidence presented (whether at an oral hearing or otherwise),

prepare a draft, in writing, of the investigation report (“draft investigation report”) and give, or cause to be given, to the controller or processor to which the investigation relates-

(i) a copy of the draft investigation report, and

(ii) a notice in writing stating that the controller or processor concerned may, not later than 28 days from the date on which the notice was served on it (or such further period not exceeding 28 days as the authorised officer allows), make submissions in writing to the authorised officer on the content of the draft investigation report.

(2) An authorised officer shall-

(a) as soon as is practicable after the expiration of the period referred to in subsection (1)(ii), and

(b) having-

(i) considered the submissions (if any) made in accordance with subsection (1)(ii), and

(ii) made any revisions to the draft investigation report which, in the opinion of the authorised officer, are warranted following such consideration,

prepare the investigation report and submit it to the Commission with any such submissions annexed to it.

(3) An investigation report and a draft investigation report under this section shall be in writing and shall state-

(a) whether the authorised officer-

(i) is satisfied that an infringement of a relevant provision or, as the case may be, a relevant enactment by the controller or processor to which the investigation relates has occurred or is occurring, or

(ii) is not so satisfied,

(b) where paragraph (a)(i) applies, the grounds on which the authorised officer is so satisfied, and

(c) where paragraph (a)(ii) applies-

(i) the basis on which the authorised officer is not so satisfied, and

(ii) the authorised officer's opinion, in view of such basis, on whether or not a further investigation of the controller or processor is warranted and, if warranted, the authorised officer's opinion on the principal matters to which the further investigation should relate.

(4) Where an investigation report or a draft investigation report contains a statement referred to in subsection (3)(a)(i), the authorised officer shall not make any recommendation, or express any opinion, in such report as to the corrective power under Chapter 2 or 3, as applicable, that he or she considers ought to be exercised in respect of the controller or processor in respect of such infringement in the event that the Commission is also satisfied that an infringement has occurred or is occurring.

Commission to consider investigation report

140. (1) The Commission, on receipt under section 139 (2) of an investigation report, shall, for the purposes of the inquiry concerned, consider the report and any submissions annexed to it.

(2) Where the Commission, in considering the documents referred to in subsection (1), forms the view that further information is required for the purpose of enabling it to make a decision under section 111 , 112 , 124 or 125 , or a draft decision under section 113 , as the case may be, it may, as it considers appropriate, do one or more than one of the following:

(a) conduct an oral hearing;

(b) give the controller or processor to which the investigation concerned relates-

(i) a copy of the investigation report, and

(ii) a notice in writing stating that the controller or processor concerned may, within 21 days from the date on which the notice was served on it (or such further period not exceeding 21 days as the Commission allows), make submissions in writing to the Commission in relation to such matters as the Commission may specify in the notice;

or

(c) direct an authorised officer to conduct such further investigation into such matters as the Commission considers necessary having regard to the investigation report and submissions (if any) annexed to it.

(3) Schedule 3 shall, with any necessary modification, have effect for the purposes of an oral hearing referred to in subsection (2)(a).

(4) Sections 138 and 139 and this section shall apply to a further investigation conducted in compliance with a direction under subsection (2)(c), as if the reference to an authorised officer in those sections was a reference to an authorised officer directed under subsection (2)(c) to conduct the further investigation.

Chapter 6

Administrative Fines

Power of Commission to decide to impose administrative fine: General

141. (1) The Commission, in considering-

(a) whether to make a decision to impose an administrative fine, and

(b) where applicable, the amount of such a fine,

shall act in accordance with this section and Article 83.

(2) Where a controller to whom section 111 (2)(b), 112 (2)(b) or 133 (9) applies is a controller by virtue of his or her being the subject of a designation under subsection (1) or (2) of section 3 , a decision by the Commission to impose an administrative fine in respect of the infringement or failure concerned shall be a decision to impose an administrative fine on the appropriate authority that, or, as the case may be, the Minister who, made the designation, and not on the controller.

(3) Where subsection (2) applies, a reference in sections 115 (1)(a), 133 (9)(b) and this Chapter to a controller shall be construed as a reference to the appropriate authority or Minister concerned.

(4) Where the Commission decides to impose an administrative fine on a controller or processor that-

(a) is a public authority or a public body, but

(b) is not a public authority or a public body that acts as an undertaking within the meaning of the Competition Act 2002 ,

the amount of the administrative fine concerned shall not exceed €1,000,000.

(5) The Commission, as soon as practicable after-

(a) a decision to impose an administrative fine is confirmed under section 142 (3)(a) or 143 (2), or

(b) the court decides, under section 142 (3)(b), to impose a different fine,

shall give the controller or processor concerned a notice in writing, requiring the controller or processor to pay the amount of the fine concerned to the Commission within the period of 28 days commencing on the date of the notice.

(6) A controller or processor shall comply with a requirement referred to in subsection (5).

(7) All payments received by the Commission under this section shall be paid into or disposed of for the benefit of the Exchequer in such manner as the Minister for Finance may direct.

(8) In this section and section 142 , a reference to a decision to impose an administrative fine shall be construed as a reference to a decision by the Commission, under section 111 , 112, 113 or 133 (9), to impose such a fine.

Appeal against administrative fine

142. (1) Without prejudice to section 150 , a controller or processor that is the subject of a decision under section 111 , 112 , 113 or 133 (9) to impose an administrative fine may, within 28 days from the date on which notice of the decision concerned was given to it under section 116 or, as the case may be, section 133 (9)(b) appeal to the court against the decision.

(2) The court, on hearing an appeal under subsection (1), may consider any evidence adduced or argument made by the controller or processor concerned, whether or not already adduced or made to an authorised officer or the Commission.

(3) Subject to subsections (4) and (5), the court may, on the hearing of an appeal under subsection (1)-

(a) confirm the decision the subject of the appeal,

(b) replace the decision with such other decision as the court considers just and appropriate, including a decision to impose a different fine or no fine, or

(c) annul the decision.

(4) The court shall, for the purposes of subsection (3), act in accordance with Article 83.

(5) Where the decision the subject of the appeal is one to which section 141 (4) applies, and the court decides under subsection (3)(b) to impose a different fine, the amount of the fine imposed by the court shall not exceed €1,000,000.

(6) In this section, “court” means-

(a) the Circuit Court, where the amount of the administrative fine the subject of the appeal does not exceed €75,000, or

(b) in any other case, the High Court.

Circuit Court to confirm decision to impose administrative fine

143. (1) Where a controller or processor does not appeal in accordance with section 142 (1) against a decision by the Commission to impose an administrative fine on the controller or processor, the Commission shall, as soon as is practicable after the expiration of the period referred to in that subsection, and on notice to the controller or processor concerned, make an application in a summary manner to the Circuit Court for confirmation of the decision.

(2) The Circuit Court shall, on the hearing of an application under subsection (1), confirm the decision the subject of the application unless the Court sees good reason not to do so.

Chapter 7

Offences

Unauthorised disclosure by processor

144. (1) Personal data processed by a processor shall not be disclosed by the processor or by an employee or agent of the processor, without the prior authority of the controller on behalf of whom the data are processed.

(2) A person who knowingly or recklessly contravenes subsection (1) shall be guilty of an offence and shall be liable-

(a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or

(b) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both.

(3) Subsection (1) does not apply to a person who shows that the disclosing concerned was required or authorised by or under any enactment, rule of law or order of a court.

Disclosure of personal data obtained without authority

145. (1) A person who, without the prior authority of the controller or processor-

(a) obtains personal data, and

(b) discloses the data or information to another person,

shall be guilty of an offence and shall be liable-

(i) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or

(ii) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both.

(2) Subsection (1) does not apply to a person who shows that the disclosing was required or authorised by or under any enactment, rule of law or order of a court.

(3) A person who sells personal data that were disclosed to the person in contravention of subsection (1) shall be guilty of an offence and shall be liable-

(a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or

(b) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both.

(4) A person who offers to sell personal data obtained without the prior authority of the controller or processor shall be guilty of an offence and shall be liable-

(a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or

(b) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both.

Offences by directors, etc., of bodies corporate

146. Where an offence under this Act is committed by a body corporate and is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, a person being a director, manager, secretary or other officer of the body corporate or a person who was purporting to act in any such capacity, that person, as well as the body corporate, shall be guilty of that offence and shall be liable to be proceeded against and punished as if he or she were guilty of the first-mentioned offence.

Prosecution of summary offences by Commission

147. (1) Summary proceedings for an offence under this Act may be brought and prosecuted by the Commission.

(2) Notwithstanding section 10 (4) of the Petty Sessions (Ireland) Act 1851, summary proceedings for an offence under this Act may be brought-

(a) at any time within 3 years from the date on which the offence was alleged to have been committed, or

(b) if, at the expiry of that period, the person against whom the proceedings are to be brought is outside the State, within 6 months of the date on which he or she next enters the State,

whichever is the later, provided that no such proceedings shall be commenced later than 5 years from the date on which the offence concerned was alleged to have been committed.

(3) Where a person is convicted of an offence under this Act, the court may, where it is satisfied that there are good reasons for so doing, order the person to pay the costs and expenses, measured by the court, incurred by the Commission in relation to the investigation, detection and prosecution of the offence, including the expenses of and incidental to an examination of any information provided to the Commission or an authorised officer.

(4) An order for costs and expenses under subsection (3) is in addition to and not instead of any fine or other penalty the court may impose.

Chapter 8

Miscellaneous

General provisions relating to complaints

148. (1) Subject to subsection (2), sections 108 and 121 shall cease to apply where the complaint concerned is withdrawn, or deemed to have been withdrawn, by the data subject concerned, or on behalf of the data subject by a body mandated by the data subject in accordance with Article 80(1) of the Data Protection Regulation or section 120, as the case may be.

(2) Where subsection (1) applies, nothing in that subsection shall be construed as preventing the Commission, where it is satisfied that there is good and sufficient reason for so doing, from proceeding or, as the case may be, continuing to examine, in accordance with Chapter 2 or 3, as applicable, the subject matter of the complaint.

(3) Where it has reasonable doubts concerning the identity of a complainant, the Commission may request from the complainant or, where applicable, the supervisory authority with which the complaint was lodged, such additional information as is necessary to confirm such identity.

Publication of convictions, sanctions, etc.

149. (1) The Commission shall publish particulars of any-

(a) conviction of a person for a contravention of this Act,

(b) exercise by it of its power-

(i) to impose an administrative fine, or

(ii) to order the suspension of data transfers to a recipient in a third country or to an international organisation, under Article 58(2)(j),

or

(c) order of the Court under section 134 .

(2) The publication under subsection (1) of the particulars referred to in that subsection shall be in such form and manner and in respect of such period as the Commission thinks fit.

(3) The Commission may publish particulars, in such form and manner and in respect of such period as it thinks fit, of the exercise by it of its corrective powers under Article 58(2) (other than those referred to in subsection (1)) or section 127 .

(4) Subject to subsection (5), the Commission may, if it considers it in the public interest to do so, publish particulars of any report under section 135 , report by the Commission of any investigation or audit carried out, or other function performed, by it under the Data Protection Regulation or this Act, or any matter relating to or arising in the course of such an investigation, audit or performance.

(5) The Commission shall ensure that the publication under subsection (4) of information referred to in that subsection is done in such a manner that commercially sensitive information relating to a person is not disclosed.

(6) The publication by the Commission of particulars of any report or matters referred to in subsection (3) or (4) and any other report of the Commission shall, for the purposes of the law of defamation, be absolutely privileged.

(7) In this section, “commercially sensitive information” means-

(a) financial, commercial, scientific, technical or other information the disclosure of which could reasonably be expected to result in a material financial loss or gain to the person to whom it relates, or could prejudice the competitive position of that person in the conduct of his or her business or otherwise in his or her occupation, or

(b) information the disclosure of which could prejudice the conduct or outcome of contractual or other negotiations of the person to whom it relates.

Right to effective judicial remedy (Part 6)

150. (1) A controller or processor on which an information notice or enforcement notice or a notice under section 135 (1) is served may, within 28 days from the date on which the notice is served, appeal against a requirement specified in the notice.

(2) The court, on hearing an appeal under subsection (1), shall-

(a) annul the requirement concerned,

(b) substitute a different requirement for the requirement concerned, or

(c) dismiss the appeal.

(3) This subsection applies to an appeal brought under subsection (1)-

(a) against a requirement specified in an information notice to which section 132 (3) applies, or an enforcement notice to which section 133 (6) applies, and

(b) that is brought within the period specified in the notice concerned.

(4) Notwithstanding any provision of this Act, the court, on hearing an appeal to which subsection (3) applies, may on application to it in that behalf, determine that non-compliance by the controller or processor concerned with a requirement specified in the notice, during the period ending with the determination or withdrawal of the appeal or during such other period as the court may determine, shall not constitute an offence.

(5) A data subject or other person affected by a legally binding decision of the Commission under Chapter 2 or 3 may, within 28 days from the date on which notice of the decision is received by him or her, appeal against the decision.

(6) The court, on hearing an appeal under subsection (5), shall-

(a) annul the decision concerned,

(b) substitute its own determination for the decision, or

(c) dismiss the appeal.

(7) Where the Commission, being the competent supervisory authority in respect of a complaint within the meaning of Chapter 2 or 3, does not comply with section 108 (2) or, as the case may be, section 121 (2), the complainant concerned may apply to the court for an order under subsection (8)(a).

(8) The court, on hearing an application under subsection (7), shall-

(a) order the Commission to comply with the provision concerned, or

(b) dismiss the application.

(9) The Circuit Court shall, concurrently with the High Court, have jurisdiction to hear and determine proceedings under this section.

(10) The jurisdiction conferred on the Circuit Court by this section shall be exercised by the judge for the time being assigned to the circuit where-

(a) in the case of an appeal under subsection (1), the controller or processor is established,

(b) in the case of an appeal under subsection (5), the data subject or other person resides or is established, or

(c) in the case of an application under subsection (7), the data subject resides,

or, at the option of the controller, processor, data subject or person concerned, by a judge of the Circuit Court for the time being assigned to the Dublin circuit.

(11) A decision of the Circuit Court or High Court, as the case may be, under this section shall be final save that an appeal shall lie to the High Court or Court of Appeal, as the case may be, on a point of law.

(12) For the purposes of this section, a “legally binding decision” means a decision-

(a) under paragraph (a) or (b) of section 109 (5) or paragraph (a) or (b) of section 122 (4),

(b) under section 111 (1)(a), 112 (1), 113 (2)(b), 114 , 124 (1)(a) or 125 (1), or

(c) to exercise a corrective power under Chapter 2 or 3.

Privileged legal material

151. (1) Where a controller or processor, when requested under this Part to produce information, or provide access to it, refuses to do so on the grounds that the information contains privileged legal material, the Commission or an authorised officer may, at any time within 28 days or such longer period as the High Court may allow of the date of such refusal, apply to the High Court for a determination as to whether the information, or any part of the information, is privileged legal material where-

(a) in relation to the information concerned-

(i) the Commission or authorised officer has reasonable grounds for believing that it is not privileged legal material, or

(ii) due to the manner or extent to which such information is presented together with any other information, it is impossible or impractical to extract only such information,

and

(b) the Commission or authorised officer has reasonable grounds to suspect that the information contains evidence relating to an infringement of a relevant enactment or a relevant provision.

(2) A controller or processor referred to in subsection (1) who refuses to produce information or provide access to it on the grounds that the information contains privileged legal material shall preserve the information and keep it in a safe and secure place and manner pending the determination of an application under subsection (1) and shall, if the information is so determined not to be

privileged legal material, produce it in accordance with such order as the High Court considers appropriate.

(3) A person shall be considered to have complied with the requirement under subsection (2) to preserve information where the person has complied with such requirements as may be imposed by an authorised officer under paragraph (d) of section 130 (1).

(4) Where an application is made by the Commission or an authorised officer under subsection (1), the High Court may give such interim or interlocutory directions as it considers appropriate including, without prejudice to the generality of the foregoing, directions as to the appointment of a person with suitable legal qualifications possessing the level of experience and independence from any interest falling to be determined between the parties concerned, that the Court considers to be appropriate for the purpose of-

(a) examining the information, and

(b) preparing a report for the Court with a view to assisting or facilitating the Court in the making of its determination as to whether the information is privileged legal material.

(5) An application under subsection (1) shall be by motion and may, if so directed, be heard otherwise than in public.

Presumptions

152. (1) The presumptions specified in this section shall apply in any proceedings under the Data Protection Regulation or this Act.

(2) Where a document purports to have been created by a person it shall be presumed, unless the contrary is shown, that the document was created by that person and that any statement or record contained in it, unless the document expressly attributes its making to some other person, was made by that person.

(3) Where a document purports to have been created by a person and addressed and sent to a second person, it shall be presumed, unless the contrary is shown, that the document or record was created and sent by the first person and received by the second person, and that any statement or record contained in it-

(a) unless the document or record expressly attributes its making to some other person, was made by the first person, and

(b) came to the notice of the second person.

(4) Where a document or record is retrieved from an electronic storage and retrieval system, it shall be presumed, unless the contrary is shown, that the author of the document is the person who ordinarily uses that electronic storage and retrieval system in the course of his or her business.

(5) Where an authorised officer who, in the exercise of his or her powers, has removed one or more documents or records from any premises or place, gives evidence in any proceedings that, to the best of his or her knowledge and belief, the material is the property of any person, then the material shall be presumed, unless the contrary is shown, to be the property of that person.

(6) Where, in accordance with subsection (5), material is presumed in proceedings to be the property of a person and the authorised officer concerned gives evidence that, to the best of his or her knowledge and belief, the material is material which relates to any trade, profession, or, as the case may be, other activity, carried on by that person, the material shall be presumed, unless the contrary is proved, to be material which relates to that trade, profession, or, as the case may be, other activity, carried on by that person.

(7) References in this section to a document or record are references to a document or record in written or electronic form and, for this purpose “written” includes any form of notation or code whether by hand or otherwise and regardless of the method by which, or medium in or on which, the document or record concerned is recorded.

Expert evidence

153. (1) In any proceedings under the Data Protection Regulation or this Act, the opinion of any witness who appears to possess the appropriate qualifications or experience as respects the matter to which his or her evidence relates shall, subject to subsection (2), be admissible in evidence as regards any matter calling for expertise or special knowledge that is relevant to the proceedings and, in particular and without prejudice to the generality of the foregoing, the following matters, namely-

(a) the effects that types of data processing such as profiling may have, or have had, on the protection of personal data, and

(b) an explanation of any relevant practices or the application of such practice, where such an explanation would assist the proceedings.

(2) Notwithstanding subsection (1), a court may, where in its opinion the interests of justice require it to so direct in the proceedings concerned, direct that evidence of a general or specific kind referred to in that subsection shall not be admissible in proceedings or shall be admissible in such proceedings for specified purposes only.

Immunity from suit

154. Civil or criminal proceedings shall not lie in any court against the Commission, a Commissioner, an authorised officer or a member of the staff of the Commission in respect of anything said or done in good faith by the Commission, Commissioner, authorised officer or member of staff in the course of the performance or purported performance of a function of the Commission, Commissioner, authorised officer or member of staff.

Jurisdiction of Circuit Court

155. An application under section 138 (4), 142 (1), 143 (1) or paragraph 5 of Schedule 3 shall be made to a judge of that Court for the circuit in which the person to whom the application relates ordinarily resides or, if a controller or processor, has an establishment or, at the option of the person, by a judge of the Circuit Court for the time being assigned to the Dublin circuit.

Hearing of proceedings

156. The whole or any part of any proceedings under this Part may, at the discretion of the court, be heard otherwise than in public.

PART 7

Miscellaneous Provisions

Supervisory authority for courts acting in judicial capacity

157. (1) The judge (“assigned judge”) for the time being assigned for that purpose by the Chief Justice shall be competent for supervision of data processing operations of the courts when acting in their judicial capacity.

(2) The assigned judge shall, in particular-

(a) promote awareness among judges of the provisions of the Data Protection Regulation, the Directive and any enactment, rule made under section 158 (3) or other rule of law that gives further effect to the Data Protection Regulation or effect to the Directive, and ensure compliance with those provisions, and

(b) handle, and investigate to the extent appropriate, complaints in relation to data processing operations of the courts when acting in their judicial capacity.

Restrictions on obligations of controllers and rights of data subjects for objective of safeguarding judicial independence and court proceedings

158. (1) The rights and obligations provided for in-

(a) Articles 12 to 22 and Article 34, and Article 5 in so far as any of its provisions correspond to the rights and obligations in Articles 12 to 22, and

(b) sections 87 , 90 , 91 , 92 and 93 , and section 71 in so far as it relates to those sections,

are restricted to the extent that the restrictions are necessary and proportionate to safeguard judicial independence and court proceedings.

(2) Subsection (1) is without prejudice to any other enactment or rule of law which restricts the rights and obligations referred to in that subsection.

(3) Without prejudice to the generality of subsection (1), a panel may make such rules as it considers necessary for the purpose of ensuring the effective application of a restriction under that subsection.

(4) Rules made under subsection (3) may relate to such matters as the panel considers appropriate for the purpose referred to in that subsection and, without prejudice to the generality of that subsection, may-

(a) relate to one or more than one of the following:

(i) a class or classes of data subject;

(ii) a category or categories of personal data;

(iii) civil or criminal proceedings, or both;

(iv) a class or classes of civil or criminal proceedings, or both;

(v) the circumstances in which, or the conditions under which, a restriction under subsection (1) shall apply,

(b) include, where relevant, specific provisions as to the matters referred to in Article 23(2), and

(c) make provision for such incidental, supplementary and consequential matters as appear to the panel to be necessary or expedient for the purposes of the rule.

(5) Rules under subsection (3) shall be published in such manner (which may include publication on the website of the Courts Service) as the panel considers appropriate.

(6) In this section, “panel” means a panel of three judges nominated by the Chief Justice for the purposes of this section.

Processing of personal data where court is controller

159. (1) The Superior Courts Rules Committee may make processing rules in respect of personal data that are contained in a record of a superior court of record.

(2) The Circuit Court Rules Committee may make processing rules in respect of personal data that are contained in a record of the Circuit Court.

(3) The District Court Rules Committee may make processing rules in respect of personal data that are contained in a record of the District Court.

(4) The panel referred to in section 158 (6) may make processing rules in respect of personal data-

(a) that are not personal data to which subsection (1), (2) or (3) applies, and

(b) in respect of which a court, when acting in its judicial capacity, is a controller.

(5) Processing rules made under this section shall be binding on a processor of personal data in respect of which the rules are made.

(6) Processing rules made under subsection (4) shall be published in such manner (which may include publication on the website of the Courts Service) as the panel referred to in that subsection considers appropriate.

(7) Subject to subsection (8), a Committee referred to in subsection (1), (2) or (3) may make rules-

(a) authorising the disclosure, for the purpose of facilitating the fair and accurate reporting of the proceedings, to a bona fide member of the Press or broadcast media and at the member's request, of information contained in a record of proceedings before a court for which the Committee is the rule-making authority, and

(b) prescribing any conditions subject to which such disclosure is to be made.

(8) Rules made under subsection (7)-

(a) shall not apply to proceedings required by law to be held otherwise than in public, and

(b) shall apply subject to any order made or direction given by a court in the proceedings concerned.

(9) In this section, "processing rules", in relation to personal data, means rules made for the purposes of Article 28(3) of the Data Protection Regulation and Article 22(3) of the Directive, governing the processing by a processor of the personal data.

Publication of judgment or decision of court or court list

160. The processing of personal data shall be lawful where that processing-

(a) consists of the publication of-

(i) a judgment or decision of a court, or

(ii) a list or schedule of court proceedings or hearings in court proceedings,

or

(b) is necessary for the purposes of such publication.

Rules of court for data protection actions

161. (1) It shall be the function of the courts in data protection actions to ensure that parties to such actions comply with such rules of court as apply in relation to such actions so that the trial of data protection actions within a reasonable period of their having been commenced is secured.

(2) Where rules of court prescribe a period of time for the service of a document, or the doing of any other thing, in relation to a data protection action, the period within which that document may be served or thing may be done, shall not be extended beyond the period so prescribed unless-

(a) the parties to the action agree to the period being extended, or

(b) the court considers that-

(i) in all the circumstances the extension of the period by such further period as it may direct is necessary or expedient to enable the action to be properly prosecuted or defended, and

(ii) the interests of justice require the extension of the period by that further period.

(3) For the purposes of ensuring compliance by a party to a data protection action with rules of court, a court may make such orders as to the payment of costs as it considers appropriate.

(4) Nothing in this section shall be construed as limiting or reducing the power of an authority, having (for the time being) power to make rules regulating the practice and procedure of a court, to-

(a) make such rules in relation to data protection actions provided such rules do not derogate from, and are not inconsistent with, any provision of the Data Protection Regulation or this Act, or

(b) make such rules in relation to proceedings or actions other than data protection actions.

(5) In this section, "data protection action" means a data protection action under section 117 or section 128 .

(6) In subsections (1) and (2), a reference to the courts or the court includes a reference to the Master of the High Court and a county registrar.

Legal privilege

162. The rights and obligations provided for in-

(a) Articles 12 to 22 and 34 of the Data Protection Regulation (as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22), and

(b) sections 87 , 90 , 91 , 92 and 93 and section 71 , insofar as it relates to those sections,

do not apply-

(i) to personal data processed for the purpose of seeking, receiving or giving legal advice,

(ii) to personal data in respect of which a claim of privilege could be made for the purpose of or in the course of legal proceedings, including personal data consisting of communications between a client and his or her legal advisers or between those advisers, or

(iii) where the exercise of such rights or performance of such obligations would constitute a contempt of court.

Application to High Court concerning adequate level of protection or appropriate safeguards

163. (1) The Commission, where it considers that a place to which personal data are to be transferred does not ensure an adequate level of protection, may apply to the High Court for a determination as to whether the level of protection ensured by the place is adequate.

(2) An application under subsection (1) may be made notwithstanding that the place concerned is the subject of an implementing act pursuant to Article 45(3) of the Data Protection Regulation or, as the case may be, Article 36(3) of the Directive.

(3) The Commission, where it considers that a standard data protection clause does not provide for appropriate safeguards, may apply to the High Court for a determination as to whether the standard data protection clause provides for appropriate safeguards.

(4) For the purposes of this section, the adequacy of the level of protection referred to in subsection (1) shall be assessed in accordance with, as the case may be, Article 45(2) of the Regulation or Article 36(2) of the Directive.

(5) In this section-

“place” means a third country, a territory or one or more specified sectors within a third country, or an international organisation;

“standard data protection clause” means a standard data protection clause to which point (c) or (d) of Article 46(2) of the Data Protection Regulation applies.

Court may order destruction, erasure of data

164. (1) Where a person is convicted of an offence under this Act, the court may order any personal data that appears to the court to be connected with the commission of the offence to be destroyed or erased.

(2) The court shall not make an order under subsection (1) where it considers that a person other than the person convicted of the offence concerned may be the owner of, or otherwise interested in, the data concerned, unless such steps as are reasonably practicable have been taken for notifying that person and giving him or her an opportunity to show cause why the order should not be made.

PART 8

Amendments of other Acts of Oireachtas

Reference to personal data in enactment

165. Subject to this Act, a reference in any enactment to personal data within the meaning of the Act of 1988 shall be construed as including a reference to personal data within the meaning of-

- (a) the Data Protection Regulation, and
- (b) Part 5.

Reference to processing in enactment

166. Subject to this Act, a reference in any enactment to processing within the meaning of the Act of 1988 shall be construed as including a reference to processing within the meaning of-

- (a) the Data Protection Regulation, and
- (b) Part 5.

Amendment of Firearms Act 1925

167. The Firearms Act 1925 is amended by the insertion of the following section after section 27A:

“Provision of information by Commissioner to Minister for purposes of Act and Firearms (Firearm Certificates For Non-Residents) Act 2000

27B. (1) The Minister may request the Commissioner to provide any information necessary for the performance of the Minister’s functions under sections 9, 10, 11 and 17 and under section 2 of the

Firearms (Firearm Certificates For Non-Residents) Act 2000 , and the Commissioner shall, notwithstanding anything contained in any other enactment or rule of law, but subject to the Data Protection Regulation and the Data Protection Act 2018, comply with that request.

(2) In this section, 'Data Protection Regulation' means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016¹¹ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).".

Amendment of section 33AK of Central Bank Act 1942

168. Section 33AK(5) of the Central Bank Act 1942 is amended-

(a) in paragraph (az), by the substitution of "(S.I. No. 349 of 2016), or" for "(S.I. No. 349 of 2016).",

(b) by the insertion of the following paragraph:

"(ba) to the Data Protection Commission that is required for the performance of that Commission's functions under the Data Protection Regulation or the Data Protection Acts 1988 to 2018.",

and

(c) by the insertion in subsection (10) of the following definition:

" 'Data Protection Regulation' means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016¹² on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);".

Amendment of section 2 of Civil Service Regulation Act 1956

169. Section 2 (2) of the Civil Service Regulation Act 1956 is amended-

(a) in paragraph (h), by the deletion of "and",

(b) in paragraph (i), by the substitution of "Síochána, and" for "Síochána.", and

(c) by the insertion of the following paragraph after paragraph (i):

"(j) in relation to a member of staff of the Data Protection Commission, the Commissioner for Data Protection or, where more than one Commissioner for Data Protection stands appointed, the chairperson (within the meaning of the Data Protection Act 2018).".

Amendment of section 24 of Misuse of Drugs Act 1977

170. Section 24 of the Misuse of Drugs Act 1977 is amended-

(a) in subsection (1)(c), by the substitution of “(including those containing any data that constitutes personal data)” for “(including any data within the meaning of the Data Protection Acts 1988 and 2003)”,

(b) in subsection (2)(c), by the substitution of “(including those containing any data that constitutes personal data)” for “(including any data within the meaning of the Data Protection Acts 1988 and 2003)”, and

(c) by the insertion of the following subsection after subsection (7):

“(8) In this section-

‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016¹³ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

‘personal data’ means personal data within the meaning of-

(a) the Data Protection Regulation, or

(b) Part 5 of the Data Protection Act 2018.”.

Amendment of section 15A of Control of Clinical Trials Act 1987

171. Section 15A of the Control of Clinical Trials Act 1987 is amended-

(a) by the substitution of the following paragraph for paragraph (d):

“(d) inspect and copy or extract information from any data including data that constitutes personal data within the meaning of-

(i) the Data Protection Regulation, or

(ii) Part 5 of the Data Protection Act 2018.”,

and

(b) the insertion of the following subsection after subsection (10):

“(11) In this section, ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016¹⁴ on the protection of natural persons with regard to

the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of Data Protection Act 1988

172. (1) The Act of 1988 is amended-

(a) in section 24, by the substitution of the following subsection for subsection (1):

“(1) In this section ‘authorised officer’ has the same meaning that it has in section 2 (1) of the Data Protection Act 2018.”,

and

(b) in section 26-

(i) in subsection (1)-

(I) in paragraph (b), by the substitution of “notice, and” for “notice”, and

(II) by the deletion of paragraph (c),

and

(ii) in subsection (4)-

(I) in paragraph (a), by the substitution of “paragraph (a) or (b) of subsection (1) of this section” for “paragraph (a), (b) or (c) of subsection (1) of this section”, and

(II) by the substitution of “with a requirement or prohibition specified in the notice” for “with a requirement or prohibition specified in the notice, or, as the case may be, a contravention by him of section 19 of this Act,”.

(2) The amendments effected by subsection (1) shall not apply for the purposes of subsections (1)(b), (2) and (3) of section 8 .

Amendment of Bankruptcy Act 1988

173. The Bankruptcy Act 1988 is amended by the insertion of the following section:

“Restriction of right of access to personal data in certain circumstances

140D. (1) Article 15 (Right of access) of the Data Protection Regulation is restricted to the extent necessary and proportionate to safeguard the effective performance by the Official Assignee of his or her functions under section 61, where the performance of those functions gives rise to the processing of personal data to which the Data Protection Regulation applies.

(2) In this section, ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016¹⁵ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of Firearms and Offensive Weapons Act 1990

174. The Firearms and Offensive Weapons Act 1990 is amended by the insertion of the following section after section 16:

“Provision of information by Commissioner to Minister

16A. (1) The Minister may request the Commissioner of the Garda Síochána to provide any information necessary for the performance of the Minister’s functions under sections 9C and 9E and the Commissioner shall, notwithstanding anything contained in any other enactment or rule of law, but subject to the Data Protection Regulation and the Data Protection Act 2018, comply with that request.

(2) In this section ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016¹⁶ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of section 13A of Electoral Act 1992

175. Section 13A of the Electoral Act 1992 is amended by the insertion of the following subsection after subsection (3B):

“(3C) In addition to any other electoral purpose for which the information contained in the register prepared under section 13, including a draft register or the supplement to the register prepared under section 15 or an electors list published under section 16, being information which is excluded from the edited register, may be used, that information may be used-

(a) by a specified person (within the meaning of section 39 of the Data Protection Act 2018), for the purpose of communicating with a data subject in accordance with section 39 of that Act, or

(b) by an elected representative (within the meaning of section 40 of the Data Protection Act 2018) for the purposes of section 40 of that Act.”.

Amendment of Comptroller and Auditor General (Amendment) Act 1993

176. The Comptroller and Auditor General (Amendment) Act 1993 is amended-

(a) in section 10, by the substitution of the following subsection for subsection (3):

“(3) In this section-

‘automated data’ means information that-

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, or

(b) is recorded with the intention that it should be processed by means of such equipment;

‘data’ means automated data and manual data;

‘data equipment’ means equipment for processing data;

‘data material’ means any document or other material used in connection with, or produced by, data equipment;

‘manual data’ means information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;

‘relevant filing system’ means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible;”,

and

(b) by the insertion of the following section after section 18B:

“Application of this Act to the Data Protection Commission

18C. This Act applies to the Data Protection Commission as if it were a Department.”.

Amendment of section 8 of Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993

177. Section 8 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 is amended in subsection (1A) by the substitution of “the functions of the Data Protection Commission under section 10 of the Data Protection Act 1988 and Part 6 of the Data Protection Act 2018” for “the functions of the Data Protection Commissioner under section 10 of the Data Protection Act 1988 ”.

Amendment of section 24 of Statistics Act 1993

178. Section 24 of the Statistics Act 1993 is amended-

(a) by the substitution of the following subsection for subsection (2):

“(2) Without prejudice to the Data Protection Regulation and the Data Protection Act 2018, persons and undertakings may provide information and records, or copies thereof, which they may possess to the Director General or officers of statistics on invitation under the provisions of this Act.”,

and

(b) by the insertion of the following subsection:

“(3) In this section, ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016¹⁷ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of section 57B of Irish Aviation Authority Act 1993

179. Section 57B(1) of the Irish Aviation Authority Act 1993 is amended by the substitution of the following paragraph for paragraph (d):

“(d) inspect, copy or extract information from any material (including information in any form) or thing found or produced to the authorised person.”.

Amendment of section 18F of Health Insurance Act 1994

180. Section 18F of the Health Insurance Act 1994 is amended-

(a) in subsection (2)(d), by the substitution of “data (including data that constitutes personal data)” for “data (within the meaning of the Data Protection Acts 1988 and 2003)”, and

(b) in subsection (12), by the insertion of the following definitions:

“ ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016¹⁸ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

‘personal data’ means personal data within the meaning of-

(a) the Data Protection Regulation, or

(b) Part 5 of the Data Protection Act 2018.”.

Amendment of section 142 of Consumer Credit Act 1995

181. Section 142 of the Consumer Credit Act 1995 is amended-

(a) in subsection (2), by the substitution of the following paragraph for paragraph (b):

“(b) which relates to information that constitutes personal data to which the Data Protection Regulation applies.”,

(b) in subsection (4), by the substitution of the following paragraph for paragraph (b):

“(b) which relates to information that constitutes personal data to which the Data Protection Regulation applies.”,

and

(c) by the insertion of the following subsection after subsection (4):

“(5) In this section, ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of section 32B of Irish Medicines Board Act 1995

182. Section 32B of the Irish Medicines Board Act 1995 is amended-

(a) in subsection (3), by the substitution of the following paragraph for paragraph (l):

“(l) inspect and copy or extract information from any data, including data that constitutes personal data within the meaning of-

(i) the Data Protection Regulation, or

(ii) Part 5 of the Data Protection Act 2018.”,

and

(b) by the insertion of the following subsection after subsection (11):

“(12) In this section, ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of section 77 of Central Bank Act 1997

183. Section 77 of the Central Bank Act 1997 is amended by the substitution of the following subsection for subsection (12):

“(12) In this section-

‘automated data’ means information that-

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, or

(b) is recorded with the intention that it should be processed by means of such equipment;

‘data’ means automated data and manual data;

‘data equipment’ means equipment for processing data;

‘data material’ means any document or other material used in connection with, or produced by data equipment;

‘manual data’ means information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;

‘relevant filing system’ means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.”.

Amendment of section 1 of Health (Provision of Information) Act 1997

184. The Health (Provision of Information) Act 1997 is amended by the substitution of the following section for section 1:

“Requests for and provision of information

1. (1) The National Cancer Registry Board (established under the Health (Corporate Bodies) Act 1961) may request from any person personal data (including data concerning health and genetic data within the meaning of the Data Protection Regulation) held by, or in the possession of, that person for the purposes of the performance of that Board of its functions.

(2) Without prejudice to his or her obligations under the Data Protection Regulation and the Act of 2018, the person to whom a request is made under subsection (1) shall provide the personal data requested to the extent it is held by, or in the possession of, that person.

(3) The Health Service Executive may, for the purposes of compiling and maintaining a record of the names, addresses, telephone numbers, e-mail addresses and dates of birth of persons who, for public health reasons, may be invited to participate in any cancer screening (including any breast, cervical or bowel cancer screening) programme operated by the Executive, request from any person the names, addresses, telephone numbers, e-mail addresses and dates of birth of persons held by, or in the possession of, that person.

(4) Without prejudice to his or her obligations under the Data Protection Regulation and the Act of 2018, the person to whom a request is made under subsection (3) may provide that information to the extent it is held by, or in the possession of, that person.

(5) In this section-

‘Act of 2018’ means the Data Protection Act 2018;

‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016²¹ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

‘personal data’ means personal data within the meaning of the Data Protection Regulation.”.

Amendment of section 9M of Electricity Regulation Act 1999

185. Section 9M of the Electricity Regulation Act 1999 is amended-

(a) in subsection (4), by the substitution of “the Data Protection Regulation or the Data Protection Act 2018” for “the Data Protection Acts 1988 and 2003”, and

(b) by the insertion of the following subsection after subsection (10):

“(11) In this section, ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016²² on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of British-Irish Agreement Act 1999

186. Section 51 of the British-Irish Agreement Act 1999 is amended-

(a) in subsection (1) by-

(i) the substitution of the following definition for the definition of “Act of 1988”:

“ ‘Act of 1988’ means the Data Protection Act 1988 , as amended by the Data Protection Act 2018;”,
and

(ii) the substitution of the following definition for the definition of “established”:

“ ‘established’, in relation to a data controller or a data processor, shall be construed in accordance with section 1(3B)(b) of the Act of 1988;”,

and

(b) by the deletion of subsection (6).

Amendment of section 7D of Comhairle Act 2000

187. Section 7D of the Comhairle Act 2000 is amended-

(a) in subsection (3), by the substitution of “Subject to the Data Protection Regulation and the Data Protection Act 2018” for “Subject to the Data Protection Acts 1988 and 2003”, and

(b) by the substitution of the following subsection for subsection (8):

“(8) In this section-

‘application’, ‘assessment’ and ‘service statement’ have the meanings assigned to them respectively by Part 2 of the Disability Act 2005 ;

‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016²³ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of section 33 of Commission To Inquire Into Child Abuse Act 2000

188. The Commission To Inquire Into Child Abuse Act 2000 is amended by the substitution of the following section for section 33:

“33. (1) Article 15 (Right of access) of the Data Protection Regulation is restricted, to the extent necessary and proportionate to safeguard the effective performance by the Commission of its functions or a Committee of its functions, in so far as it relates to personal data (within the meaning of that Regulation) provided to the Commission or a Committee while the data is in the custody of the Commission or a Committee, or in the case of such data provided to the Confidential Committee, of a body to which it is transferred by the Commission upon the dissolution of the Commission.

(2) In this section, ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016²⁴ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of section 2 of Merchant Shipping (Investigation of Marine Casualties) Act 2000

189. Section 2 (1) of the Merchant Shipping (Investigation of Marine Casualties) Act 2000 is amended in the definition of “record” by the deletion of the words “any form in which data (within the meaning of the Data Protection Act 1988) are held,”.

Amendment of section 28 of Education (Welfare) Act 2000

190. Section 28 of the Education (Welfare) Act 2000 is amended-

(a) by the substitution of “controller” for “data controller” in each place it occurs, and

(b) in subsection (3), by the deletion of “ ‘data controller’ and ‘personal data’ have the meanings assigned to them by the Data Protection Act 1988 ” and the insertion of the following:

“ ‘controller’ means a controller within the meaning of the Data Protection Regulation;

‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016²⁵ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

‘personal data’ means personal data within the meaning of the Data Protection Regulation;”.

Amendment of section 38 of Planning and Development Act 2000

191. Section 38 of the Planning and Development Act 2000 is amended in subsection (2) by the deletion of “and the Data Protection Acts 1988 and 2003”.

Amendment of section 14 of Dormant Accounts Act 2001

192. Section 14 (5) of the Dormant Accounts Act 2001 is amended by the substitution of the following paragraph for paragraph (b):

“(b) Nothing in paragraph (a) shall be construed as restricting the right of a person to inspect the register, in relation to an account, where the person-

(i) proves to the satisfaction of an institution that he or she is, or may be, the account holder,

(ii) proves to the satisfaction of an institution that he or she is authorised by the account holder to so inspect, or

(iii) may act on behalf of the account holder in relation to that account pursuant to regulations made under section 9.”.

Amendment of section 30 of Residential Institutions Redress Act 2002

193. The Residential Institutions Redress Act 2002 is amended by the substitution of the following section for section 30:

“30. (1) Article 15 (Right of access) of the Data Protection Regulation is restricted, to the extent necessary and proportionate to safeguard the effective performance by the Board of its functions and the Review Committee of its functions, in so far as it relates to personal data (within the meaning of that Regulation) provided to the Board while the data is in the custody of the Board or the Review Committee.

(2) In this section, ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of section 2 of Official Languages Act 2003

194. Section 2 (1) of the Official Languages Act 2003 is amended-

(a) in the Irish text, in the definition of “taifead”, by the substitution of “aon fhoirm ina gcoimeádtar sonraí (lena n-áirítear foirm mheaisín-inléite) nó rud” for “aon fhoirm ina gcoimeádtar sonraí (de réir bhrí an Achta um Chosaint Sonraí 1988), aon fhoirm eile (lena n-áirítear foirm mheaisín-inléite) nó rud eile” and

(b) in the English text, in the definition of “record”, by the substitution of “any form in which data are held (including machine-readable form)” for “any form in which data (within the meaning of the Data Protection Act 1988) are held, any other form (including machine-readable form)”.

Amendment of section 86 of Personal Injuries Assessment Board Act 2003

195. Section 86 of the Personal Injuries Assessment Board Act 2003 is amended-

(a) in subsection (1), by the substitution of “but only if the processing (within the meaning of the Data Protection Regulation) of any particulars constituting personal data (within the meaning of that Regulation) in the database is in accordance with the Data Protection Regulation and the Data

Protection Act 2018.” for “but only if the database is, for the time being, maintained in accordance with the Data Protection Act 1988 ”, and

(b) by the insertion of the following subsection after subsection (4):

“(5) In this section, ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016²⁷ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of section 12 of Unclaimed Life Assurance Policies Act 2003

196. Section 12 (5) of the Unclaimed Life Assurance Policies Act 2003 is amended by the substitution of the following paragraph for paragraph (b):

“(b) Nothing in paragraph (a) shall be construed as restricting the right of a person to inspect the register in relation to a policy where the person-

(i) proves to the satisfaction of an insurance undertaking that he or she is, or may be, the policy holder,

(ii) proves to the satisfaction of an insurance undertaking that he or she is authorised by the policy holder to so inspect, or

(iii) may act on behalf of the policy holder in relation to that policy pursuant to regulations made under section 7.”.

Amendment of section 66 of Civil Registration Act 2004

197. Section 66 of the Civil Registration Act 2004 is amended-

(a) in subsection (1), by the substitution of “Notwithstanding anything contained in any other enactment, but subject to the Data Protection Regulation and the Data Protection Act 2018, an tArd-Chlárathóir may” for “Notwithstanding anything contained in the Data Protection Acts 1988 to 2003 or any other enactment, an tArd-Chlárathóir may”, and

(b) by the substitution of the following subsection for subsection (2):

“(2) In this section-

‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016²⁸ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

‘information’ includes personal data;

‘personal data’ means personal data within the meaning of-

- (a) the Data Protection Act 1988 ,
- (b) the Data Protection Regulation, or
- (c) Part 5 of the Data Protection Act 2018.”.

Amendment of section 39 of Commissions of Investigation Act 2004

198. Section 39 of the Commissions of Investigation Act 2004 is amended-

- (a) by designating the section as subsection (1),
- (b) in that designated subsection (1), by the substitution of “Article 15 (Right of access) of the Data Protection Regulation is restricted, to the extent necessary and proportionate to safeguard the effective operation of commissions and the future cooperation of witnesses, in so far as it relates to personal data (within the meaning of that Regulation) provided to a commission” for “ Section 4 of the Data Protection Act 1988 does not apply to personal data provided to a commission”, and

(c) by the insertion of the following subsection after subsection (1):

“(2) In this section, ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016²⁹ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of section 55H of Health Act 2004

199. Section 55H of the Health Act 2004 is amended-

(a) in subsection (8), by the substitution of the following paragraph for paragraph (a):

“(a) submit a draft of the proposed procedures to the Data Protection Commission for its opinion as to whether any provision of the procedures would, if given effect, be likely to result in a contravention of the Data Protection Regulation or the Data Protection Act 2018, and”,

(b) in subsection (9), by the substitution of “the Data Protection Commission” for “the Data Protection Commissioner”, and

(c) by the insertion of the following subsection after subsection (9):

“(10) In this section, ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016³⁰ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of section 2 of Safety, Health and Welfare at Work Act 2005

200. Section 2 (1) of the Safety, Health and Welfare at Work Act 2005 is amended-

(a) by the substitution of the following definition for the definition of “record”:

“ ‘record’ includes any memorandum, book, report, statement, register, plan, chart, map, drawing, specification, diagram, pictorial or graphic work or other document, any photograph, film or recording (whether of sound or images or both), any form in which data (including data that constitute personal data within the meaning of the Data Protection Regulation or Part 5 of the Data Protection Act 2018) are held, any form (including machine-readable form) or thing in which information is held or stored manually, mechanically or electronically, and anything that is a part or copy, in any form, of any of, or any combination of, the foregoing;” ,

and

(b) by the insertion of the following definition:

“ ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016³¹ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);” .

Amendment of section 265 of Social Welfare Consolidation Act 2005

201. Section 265 of the Social Welfare Consolidation Act 2005 is amended-

(a) in subsection (1)-

(i) by the substitution of the following definitions for the definitions of “data controller” and “personal data”:

“ ‘controller’ means a controller within the meaning of-

(a) the Data Protection Regulation, or

(b) Part 5 of the Act of 2018;

‘personal data’ means personal data within the meaning of-

(a) the Data Protection Regulation, or

(b) Part 5 of the Act of 2018;”,

and

(ii) by the insertion of the following definitions:

“ ‘Act of 2018’ means the Data Protection Act 2018;

‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016³² on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);”,

and

(b) in subsection (2), by the substitution of “controller” for “data controller”.

Amendment of Disability Act 2005

202. The Disability Act 2005 is amended-

(a) in section 12, by the deletion of subsection (3),

(b) in section 13, by the deletion of subsection (4),

(c) in section 41-

(i) by the deletion of the definition of “the Acts”,

(ii) by the substitution of the following definition for the definition of “processing”:

“ ‘processing’ means processing within the meaning of the Data Protection Regulation;”,

and

(iii) by the insertion of the following definition:

“ ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016³³ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);”,

(d) in section 42-

(i) by the substitution, in subsection (1)(b), of “the Data Protection Regulation”, for “the Acts”,

(ii) by the deletion, in subsection (2)(a), of “save in accordance with the provisions of section 12A of the Data Protection Act 1988 (as inserted by the Data Protection (Amendment) Act 2003 ”,

(iii) by the substitution of the following subsection for subsection (4):

“(4) A person who contravenes subsection (2) or (3) shall be guilty of an offence and shall be liable-

(a) on summary conviction, to a class A fine, or

(b) on conviction on indictment, to a fine not exceeding €100,000.”,

and

(iv) by the insertion of the following subsections:

“(5) Where a person is convicted of an offence under subsection (4), the court may order any personal data that appears to the court to be connected with the commission of the offence to be destroyed or erased.

(6) The court shall not make an order under subsection (5) where it considers that a person other than the person convicted of the offence concerned may be the owner of, or otherwise interested in, the data concerned, unless such steps as are reasonably practicable have been taken for notifying that person and giving him or her an opportunity to show cause why the order should not be made.”,

(e) by the deletion of section 43, and

(f) in section 45, by the deletion of subsection (1).

Amendment of section 2 of Railway Safety Act 2005

203. Section 2 (1) of the Railway Safety Act 2005 is amended in the definition of “record” by the deletion of the words “in which data (within the meaning of the Data Protection Act 1988) are held, any other form”.

Amendment of section 12 of Health (Repayment Scheme) Act 2006

204. Section 12 (3) of the Health (Repayment Scheme) Act 2006 is amended by the substitution of “except after consultation with the Data Protection Commission” for “except after consultation with the Data Protection Commissioner within the meaning of the Data Protection Acts 1988 and 2003”.

Amendment of section 19 of Electoral (Amendment) Act 2006

205. Section 19 of the Electoral (Amendment) Act 2006 is amended by the substitution of “A registration authority may,” for “Notwithstanding anything in the Data Protection Acts 1988 and 2003, a registration authority may,”.

Amendment of section 67 of Pharmacy Act 2007

206. Section 67 of the Pharmacy Act 2007 is amended-

(a) in subsection (3), by the substitution of the following paragraph for paragraph (l):

“(l) inspect and copy or extract information from any data, including data that constitutes personal data within the meaning of-

(i) the Data Protection Regulation, or

(ii) Part 5 of the Data Protection Act 2018.”,

and

(b) by the insertion of the following subsection after subsection (12):

“(13) In this section, ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 201634 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of Passports Act 2008

207. The Passports Act 2008 is amended-

(a) in section 2, by-

(i) the deletion of the definitions of “Act of 1988”, “automated data” and “data”,

(ii) the insertion of the following definition:

“ ‘Act of 2018’ means the Data Protection Act 2018;”,

(iii) the substitution of the following definition for the definition of “biometric data”:

“ ‘biometric data’ means biometric data within the meaning of-

(a) the Data Protection Regulation, or

(b) Part 5 of the Act of 2018;”,

(iv) the insertion of the following definition:

“ ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 201635 on the protection of natural persons with regard to the processing of

personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);”,

(v) the substitution of the following definition for the definition of “personal data”:

“ ‘personal data’ means personal data within the meaning of-

(a) the Data Protection Regulation, or

(b) Part 5 of the Act of 2018;”,

and

(vi) the substitution of the following definition for the definition of “processing”:

“ ‘processing’ means processing within the meaning of-

(a) the Data Protection Regulation, or

(b) Part 5 of the Act of 2018.”,

(b) in section 8, by the substitution in subsection (1) of “Subject to the Data Protection Regulation and the Act of 2018” for “Subject to the Data Protection Acts 1988 and 2003”, and

(c) in section 21(1)(b), by the substitution of “personal data” for “data” in each place it occurs.

Amendment of Criminal Justice (Mutual Assistance) Act 2008

208. The Criminal Justice (Mutual Assistance) Act 2008 is amended-

(a) in section 76(1), by the insertion of the following definition:

“ ‘controller’ means a controller within the meaning of Part 5 of the Data Protection Act 2018;”,

(b) in section 79C(7), by the insertion of “or, as the case may be, controller” after “data controller” in each place it occurs,

(c) in section 94, by-

(i) the substitution of the following subsections for subsections (5) and (6):

“(5) Article 7, in its application in relation to the use of personal data contained in evidence or information obtained under the Treaty by a person in the State, is without prejudice to the application of-

(a) subject to section 8 of the Act of 2018, section 7 (duty of care owed by data controllers and data processors) of the Act of 1988 in respect of the use of such data (within the meaning of the Act of 1988), and

(b) Part 5 of the Act of 2018, in respect of the use of such data (within the meaning of that Part).

(6) (a) Subject to section 8 of the Act of 2018, the Data Protection Acts 1988 and 2003 apply in relation to personal data referred to in subsection (5)(a), in respects other than those related to their use.

(b) Part 5 of the Act of 2018 applies in relation to personal data referred to in subsection (5)(b), in respects other than those related to their use.”,

and

(ii) the insertion of the following subsection:

“(8) In this section-

‘Act of 1988’ means the Data Protection Act 1988 ;

‘Act of 2018’ means the Data Protection Act 2018.”,

and

(d) in section 107, by-

(i) the substitution of the following subsections for subsections (2) and (3):

“(2) Subsection (1) is without prejudice to the application of-

(a) subject to section 8 of the Act of 2018, section 7 (duty of care owed by data controllers and data processors) of the Act of 1988 in respect of the use of such data (within the meaning of the Act of 1988), and

(b) Part 5 of the Act of 2018, in respect of the use of such data (within the meaning of that Part).

(3) (a) Subject to section 8 of the Act of 2018, the Data Protection Acts 1988 and 2003 apply in relation to personal data referred to in subsection (2)(a), in respects other than those related to their use.

(b) Part 5 of the Act of 2018 applies in relation to personal data referred to in subsection (5)(b), in respects other than those related to their use.”,

and

(ii) by the insertion of the following subsection after subsection (4):

“(5) In this section-

‘Act of 1988’ means the Data Protection Act 1988 ;

‘Act of 2018’ means the Data Protection Act 2018.”.

Amendment of section 2 of Chemicals Act 2008

209. Section 2 (1) of the Chemicals Act 2008 is amended by-

(a) the substitution of the following definition for the definition of “record”-

“ ‘record’ includes any memorandum, book, report, statement, register, plan, chart, map, drawing, specification, diagram, pictorial or graphic work or other document, any photograph, film or recording (whether of sound or images or both), any form in which data (including data that constitute personal data within the meaning of the Data Protection Regulation or Part 5 of the Data Protection Act 2018) are held, any form (including machine-readable form) or thing in which information is held or stored manually, mechanically or electronically, and anything that is a part or copy, in any form, of any of, or any combination of, the foregoing;” ,

and

(b) the insertion of the following definition:

“ ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 201636 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);” .

Amendment of Nursing Homes Support Scheme Act 2009

210. The Nursing Homes Support Scheme Act 2009 is amended-

(a) in section 26, by the deletion of subsection (12), and

(b) in section 45(1), by the substitution of “Subject to the Data Protection Regulation and the Data Protection Act 2018” for “Notwithstanding any provision of the Data Protection Acts 1988 to 2003” .

Amendment of section 23 of Criminal Justice (Miscellaneous Provisions) Act 2009

211. Section 23 of the Criminal Justice (Miscellaneous Provisions) Act 2009 is amended by the substitution of the following subsections for subsection (2):

“(2) The Data Protection Act 1988 shall, subject to any necessary modifications, apply and have effect in relation to the processing (within the meaning of that Act) of personal data (within the meaning of that Act) for the purposes of the operation of the Council Decision and the Schengen Convention.

(3) The Data Protection Act 2018 shall, subject to any necessary modifications, apply and have effect to the processing (within the meaning of Part 5 of that Act) of personal data (within the meaning of that Part) for the purposes of the operation of the Council Decision and the Schengen Convention.”.

Amendment of section 201 of National Asset Management Agency Act 2009

212. The National Asset Management Agency Act 2009 is amended by the substitution of the following section for section 201:

“201. (1) For the avoidance of doubt, an obligation on a credit institution or any other person under this Act to disclose information to NAMA, a NAMA group entity or the NTMA extends to personal data within the meaning of the Data Protection Regulation.

(2) In this section, ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 201637 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of Criminal Justice (Money Laundering and Terrorist Financing) Act 2010

213. The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 is amended-

(a) in section 2(1), by the insertion of the following definitions:

“ ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 201638 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

‘personal data’ means personal data within the meaning of-

(i) the Data Protection Act 1988 ,

(ii) the Data Protection Regulation, or

(iii) Part 5 of the Data Protection Act 2018;”,

(b) in section 52(2), by the deletion of “(within the meaning of the Data Protection Acts 1988 and 2003)”, and

(c) in section 88(2), by the deletion of “(within the meaning of the Data Protection Acts 1988 and 2003)”.

Amendment of section 12 of Communications (Retention of Data) Act 2011

214. Section 12 of the Communications (Retention of Data) Act 2011 is amended by the substitution of the following subsections for subsection (4):

“(4) The designated judge may, if he or she considers it desirable to do so, communicate with the Taoiseach or the Minister concerning disclosure requests and with the Data Protection Commission in connection with its functions under the Data Protection Regulation and the Data Protection Acts 1988 to 2018.

(5) In this section, ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 201639 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of section 17A of Ministers and Secretaries (Amendment) Act 2011

215. Section 17A of the Ministers and Secretaries (Amendment) Act 2011 is amended-

(a) in subsection (2), by the substitution of “Data Protection Regulation” for “Data Protection Acts 1988 and 2003”, and

(b) by the insertion of the following subsection after subsection (3):

“(4) In this section, ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 201640 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of section 28 of Student Support Act 2011

216. Section 28 of the Student Support Act 2011 is amended-

(a) by the substitution of “controller” for “data controller” in each place it occurs,

(b) in subsection (1), by the substitution of “Notwithstanding anything contained in any enactment (other than the Act of 2018)” for “Notwithstanding anything contained in the Data Protection Acts 1988 and 2003 or any other enactment”, and

(c) in subsection (5), by-

(i) the substitution of the following definitions for the definition of “data controller”:

“ ‘Act of 2018’ means the Data Protection Act 2018;

‘controller’ means a controller within the meaning of-

(a) the Data Protection Regulation, or

(b) Part 5 of the Act of 2018;

‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016⁴¹ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);”,

(ii) the substitution of the following definition for the definition of “personal data”:

“ ‘personal data’ means personal data within the meaning of-

(a) the Data Protection Regulation, or

(b) Part 5 of the Act of 2018;”,

and

(iii) the substitution of the following definition for the definition of “processing”:

“ ‘processing’ means processing with the meaning of-

(a) the Data Protection Regulation, or

(b) Part 5 of the Act of 2018;”.

Amendment of Communications Regulation (Postal Services) Act 2011

217. The Communications Regulation (Postal Services) Act 2011 is amended-

(a) in section 65A(1), by-

(i) the deletion of the definition of “Act of 1988”,

(ii) the insertion of the following definition:

“ ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016⁴² on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);”,

(iii) the substitution of the following definition for the definition of “personal data”:

“ ‘personal data’ means personal data within the meaning of the Data Protection Regulation;”,

and

(iv) the substitution of the following definition for the definition of “processing”:

“ ‘processing’ means processing within the meaning of the Data Protection Regulation;”,

(b) in section 66A(2), by the deletion of paragraph (a), and

(c) in section 66C-

(i) in subsection (1), by the substitution of “the Data Protection Regulation and the Data Protection Act 2018” for “the Data Protection Acts 1988 to 2003”, and

(ii) by the substitution of the following subsection for subsection (2):

“(2) Article 21 (Right to object) of the Data Protection Regulation shall not apply to processing of personal data that is required for the purposes of carrying out legitimate postcode activity.”.

Amendment of Property Services (Regulation) Act 2011

218. The Property Services (Regulation) Act 2011 is amended-

(a) in section 2(1), by the insertion of the following definition after the definition of “connected relative”:

“ ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016⁴³ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);”,

(b) in section 42, by the substitution of the following subsection for subsection (2):

“(2) The Commissioner of the Garda Síochána shall, notwithstanding anything contained in any other enactment or rule of law, but subject to the Data Protection Regulation and the Data Protection Act 2018, comply with a request under subsection (1).”,

and

(c) by the substitution of the following section for section 93:

“Restriction of right of access to personal data in certain circumstances

93. Article 15 (Right of access) of the Data Protection Regulation is restricted, to the extent necessary and proportionate to enable the Authority to effectively perform its functions under this Act in so far as the functions relate to carrying out an investigation, in so far as it relates to personal data (within the meaning of that Regulation) processed by the Authority.”.

Amendment of section 56 of Credit Union and Co-operation with Overseas Regulators Act 2012

219. Section 56 of the Credit Union and Co-operation with Overseas Regulators Act 2012 is amended-

(a) by the substitution of the following subsection for subsection (2):

“(2) A credit union may disclose to ReBo personal data within the meaning of the Data Protection Regulation.”,

and

(b) by the insertion of the following subsection after subsection (3):

“(4) In this section, ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016⁴⁴ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of Europol Act 2012

220. Section 1 of the Europol Act 2012 is amended by-

(a) the substitution of the following definition for the definition of “data”:

“ ‘data’ means automated data and manual data;”,

(b) the substitution of the following definition for the definition of “personal data”:

“ ‘personal data’ has the meaning it has in Part 5 of the Data Protection Act 2018;”,

(c) by the substitution of the following definition for the definition of “processing”:

“ ‘processing’, in relation to personal data, has the meaning it has in Part 5 of the Data Protection Act 2018;”,

and

(d) the insertion of the following definitions:

“ ‘automated data’ means information that-

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, or

(b) is recorded with the intention that it should be processed by means of such equipment;

'manual data' means information that is recorded as part of a relevant filing system, or with the intention that it should form part of a relevant filing system;

'relevant filing system' means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible;".

Amendment of Personal Insolvency Act 2012

221. The Personal Insolvency Act 2012 is amended-

(a) in section 2(1), by-

(i) the insertion of the following definition:

“ 'Data Protection Regulation' means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016⁴⁵ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);”,

and

(ii) the substitution of the following definition for the definition of “personal data”:

“ 'personal data' means personal data within the meaning of-

(a) the Data Protection Regulation, or

(b) Part 5 of the Data Protection Act 2018;”,

(b) by the deletion of section 21A, and

(c) by the substitution of the following section for section 186:

“Restriction of right of access to personal data in certain circumstances

186. Article 15 (Right of access) of the Data Protection Regulation, in so far as it relates to personal data (within the meaning of that Regulation) processed by the following persons or bodies, is restricted to the extent necessary and proportionate to enable the person or body to effectively perform his, her or its functions under this Act, in so far as those functions relate to the supervision of personal insolvency practitioners in accordance with section 176A or to carrying out an investigation under this Part:

- (a) the Insolvency Service;
- (b) an inspector appointed under section 176;
- (c) an authorised officer appointed under section 176B;
- (d) the Complaints Committee.”.

Amendment of section 2 of Animal Health and Welfare Act 2013

222. Section 2 (1) of the Animal Health and Welfare Act 2013 is amended, in the definition of “record”, by the deletion of “(within the meaning of the Data Protection Acts 1988 and 2003)”.

Amendment of section 8 of Health (Alteration of Criteria for Eligibility) Act 2013

223. Section 8 of the Health (Alteration of Criteria for Eligibility) Act 2013 is amended-

- (a) in subsection (4), by the substitution of “Subject to compliance with the Data Protection Regulation and the Act of 2018 and subject to this section” for “Notwithstanding anything contained in the Data Protection Acts 1988 and 2003, but subject to this section”,
- (b) in subsection (7), by the substitution of “the Data Protection Commission” for “the Data Protection Commissioner”,
- (c) by the deletion of subsection (8),
- (d) in subsection (9), by the substitution of “references in this section to personal data shall include references to special categories of personal data (within the meaning of section 2 of the Act of 2018)” for “references in this section to personal data shall include references to sensitive personal data”, and
- (e) by the substitution of the following subsection for subsection (10):

“(10) In this section-

‘Act of 2018’ means the Data Protection Act 2018;

‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016⁴⁶ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

‘personal data’ means personal data within the meaning of the Data Protection Regulation.”.

Insertion of section 957A to Companies Act 2014

224. The Companies Act 2014 is amended by the insertion of the following section after section 957:

“Restriction of application of certain articles of Data Protection Regulation

957A. (1) Articles 14 (Information to be provided where personal data have not been obtained from the data subject) and 15 (Right of access by the data subject) of the Data Protection Regulation are restricted, to the extent necessary and proportionate to safeguard the effective performance by the Director of his or her functions referred to in paragraph (b) and (e) of section 949(1), where the performance of those functions give rise to the processing of personal data to which the Data Protection Regulation applies.

(2) In this section, ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016⁴⁷ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of Health Identifiers Act 2014

225. The Health Identifiers Act 2014 is amended-

(a) in section 2(1)-

(i) by the insertion of the following definition after the definition of “Act of 2013”:

“ ‘Act of 2018’ means the Data Protection Act 2018;”,

(ii) by the insertion of the following definition after the definition of “conditions”:

“ ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016⁴⁸ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);”,

(iii) by the substitution of the following definition for the definition of “personal data”:

“ ‘personal data’ means personal data within the meaning of-

(a) the Data Protection Regulation, or

(b) Part 5 of the Act of 2018;”,

(iv) by the substitution of the following definition for the definition of “processing”:

“ ‘processing’ means processing within the meaning of-

(a) the Data Protection Regulation, or

(b) Part 5 of the Act of 2018;”,

(v) in paragraph (g)(iii) of the definition of “secondary purpose”, by the substitution of “in accordance with the Data Protection Regulation and the Act of 2018” for “in accordance with the Data Protection Acts 1988 and 2003”,

and

(b) by the substitution of the following Part for Part 6:

“PART 6

Application of Data Protection Regulation

Application of Data Protection Regulation

27. Article 32 of the Data Protection Regulation shall apply to a deceased individual’s relevant information (individual) as it applies to a living individual’s relevant information (individual).”.

Amendment of section 15 of Freedom of Information Act 2014

226. Section 15 of the Freedom of Information Act 2014 is amended-

(a) by the substitution of the following subsection for subsection (3):

“(3) A record shall not be within subsection (2) by reason only of the fact that it contains information constituting-

(a) personal data within the meaning of the Data Protection Act 1988 to which that Act applies,

(b) personal data within the meaning of the Data Protection Regulation to which that Regulation and the Act of 2018 apply, or

(c) personal data within the meaning of Part 5 of the Act of 2018 to which that Act applies.”,

and

(b) by the insertion of the following subsection after subsection (4):

“(5) In this section-

‘Act of 2018’ means the Data Protection Act 2018;

‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016⁴⁹ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of section 41 of Customs Act 2015

227. Section 41 of the Customs Act 2015 is amended by the deletion of subsections (4), (5) and (10).

Amendment of section 7 of Regulation of Lobbying Act 2015

228. Section 7 of the Regulation of Lobbying Act 2015 is amended-

(a) by the insertion of the following definition after the definition of "Commission":

" 'Data Protection Regulation' means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016⁵⁰ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);",

and

(b) by the substitution of the following definition for the definition of "personal data":

" 'personal data' means personal data within the meaning of-

(a) the Data Protection Regulation, or

(b) Part 5 of the Data Protection Act 2018."

Amendment of Sport Ireland Act 2015

229. The Sport Ireland Act 2015 is amended-

(a) in section 40, by-

(i) the insertion of the following definition before the definition of "anti-doping organisation":

" 'Act of 2018' means the Data Protection Act 2018;",

(ii) the insertion of the following definition after the definition of "anti-doping rule violation":

" 'Data Protection Regulation' means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016⁵¹ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);",

(iii) the substitution of the following definition for the definition of "personal data":

" 'personal data' means personal data within the meaning of the Data Protection Regulation;",

and

(iv) the substitution of the following definition for the definition of “processing”:

“ ‘processing’ means processing within the meaning of the Data Protection Regulation;”,

(b) in section 42(4), by the substitution of “Subject to compliance with the Data Protection Regulation and the Act of 2018, Sport Ireland shall” for “Sport Ireland shall”, and

(c) in section 43-

(i) in subsection (1), by the substitution of “Data Protection Regulation and the Act of 2018” for “Data Protection Acts 1988 and 2003”, and

(ii) by the deletion of subsection (3).

Amendment of section 12 of Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016

230. Section 12 of the Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016 is amended-

(a) by designating the section as subsection (1),

(b) in that designated subsection (1), by the deletion of “(within the meaning of the Data Protection Act 1988)”, and

(c) by the insertion of the following subsection after subsection (1):

“(2) In this section-

‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016⁵² on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

‘personal data’ means personal data within the meaning of-

(a) the Data Protection Act 1988 ,

(b) the Data Protection Regulation, or

(c) Part 5 of the Data Protection Act 2018.”.

Amendment of section 62 of Financial Services and Pensions Ombudsman Act 2017

231. Section 62 of the Financial Services and Pensions Ombudsman Act 2017 is amended-

(a) in subsection (2), by the substitution of the following paragraph for paragraph (b):

“(b) ensures compliance with the Data Protection Regulation and the Data Protection Act 2018.”,

and

(b) by the insertion of the following subsection after subsection (4):

“(5) In this section, ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016⁵³ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”.

Amendment of National Shared Services Office Act 2017

232. The National Shared Services Office Act 2017 is amended-

(a) in section 2, by the insertion of the following definition:

“ ‘Data Protection Regulation’ means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016⁵⁴ on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).”,

(b) in section 9(2)(a)(iv), by the substitution of “processing (within the meaning of the Data Protection Regulation) personal data (also within the meaning of that Regulation)” for “processing (within the meaning of the Data Protection Act 1988) personal data (also within the meaning of that Act)”, and

(c) in section 35-

(i) in subsection (1)-

(I) by the substitution of “Notwithstanding anything contained in any enactment, but subject to the Data Protection Regulation and the Data Protection Act 2018” for “Notwithstanding anything contained in the Data Protection Acts 1988 and 2003”, and

(II) by the substitution of “controller” for “data controller” in each place it occurs,

(ii) in subsection (3), by the substitution of “controller” for “data controller”, and

(iii) in subsection (4)-

(I) by the substitution of the following definition for the definition of “data controller”:

“ ‘controller’ has the same meaning as it has in the Data Protection Regulation;”,

and

(II) by the deletion of the definition of “data subject”.

SCHEDULE 1

Statutory Instruments Revoked

Section 7(3)

Item

(1)

S.I. No. and Year

(2)

Short Title

(3)

Extent of Revocation

(4)

1.

S.I. No. 347 of 1988

Data Protection (Fees) Regulations 1988

The whole Regulations

2.

S.I. No. 350 of 1988

Data Protection (Registration Period) Regulations 1988

The whole Regulations

3.

S.I. No. 351 of 1988

Data Protection (Registration) Regulations 1988

The whole Regulations

4.

S.I. No. 81 of 1989

Data Protection (Restriction of section 4) Regulations 1989

The whole Regulations

5.

S.I. No. 95 of 1993

Data Protection Act 1988 (Section 5(1)(d)) (Specifications) Regulations 1993

The whole Regulations

6.

S.I. No. 657 of 2007

Data Protection Act 1988 (Section 16(1)) Regulations 2007

The whole Regulations

7.

S.I. No. 658 of 2007

Data Protection (Fees) Regulations 2007

The whole Regulations

8.

S.I. No. 687 of 2007

Data Protection (Processing of Genetic Data) Regulations 2007

The whole Regulations

9.

S.I. No. 421 of 2009

Data Protection Act 1988 (Section 5(1)(d)) (Specification) Regulations 2009

The whole Regulations

10.

S.I. No. 426 of 2016

Data Protection (Section 2B) Regulations 2016

The whole Regulations

SCHEDULE 2

Data Protection Commission

Section 10

1. The Commission shall be a body corporate with perpetual succession and an official seal and shall have power to sue, and may be sued, in its corporate name and shall, with the consent of the Minister and the Minister for Public Expenditure and Reform have the power to acquire, hold and dispose of land or an interest in land, and shall have the power to acquire, hold and dispose of any other property.

2. The seal of the Commission shall be authenticated by the signatures of-

(a) a Commissioner, and

(b) a member of staff of the Commission authorised by the Commission for that purpose.

3. Judicial notice shall be taken of the seal of the Commission and any document purporting to be an instrument made by, and to be sealed with the seal of, the Commission shall, unless the contrary is proved, be received in evidence and be deemed to be such instrument without further proof.

4. Any contract or instrument which, if entered into or executed by an individual, would not require to be under seal may be entered into or executed on behalf of the Commission by any person generally or specially authorised by the Commission in that behalf.

5. (1) Where a Commissioner is-

(a) nominated as a member of Seanad Éireann,

(b) elected as a member of either House of the Oireachtas or to be a member of the European Parliament,

(c) regarded pursuant to Part XIII of the Second Schedule to the European Parliament Elections Act 1997 as having been elected to that Parliament, or

(d) is elected or co-opted as a member of a local authority,

he or she shall thereupon cease to be a Commissioner.

(2) A person who is for the time being-

(a) entitled under the Standing Orders of either House of the Oireachtas to sit therein,

(b) a member of the European Parliament, or

(c) entitled under the standing orders of a local authority to sit as a member thereof, shall, while he or she is so entitled as mentioned in clause (a) or (c) or is such a member as mentioned in clause (b), be disqualified for membership of the Commission or for employment in any capacity by the Commission.

SCHEDULE 3

Provisions Applicable to Oral Hearing Conducted by an Authorised Officer Under Section 138

Section 138 (11)

Provisions Applicable to Oral Hearing Conducted by an Authorised Officer Under Section 138

1. The authorised officer conducting an oral hearing under section 138 (11) for the purposes of an investigation may take evidence on oath, and the administration of such an oath by the authorised officer is hereby authorised.
2. The authorised officer may by notice in writing require a person to attend the oral hearing at such time and place as is specified in the notice to give evidence in respect of any matter in issue in the investigation or to produce any documents, records, statements or other information within his or her possession or control or within his or her procurement.
3. Subject to paragraph 4, a person referred to in paragraph 2 may be examined and cross-examined at the oral hearing.
4. A person referred to in paragraph 2 shall be entitled to the same immunities and privileges in respect of compliance with any requirement referred to in that paragraph as if the person were a witness before the High Court.
5. Where a person referred to in paragraph 2 does not comply or fully comply with a requirement referred to in that paragraph, the authorised officer may apply in a summary manner to the Circuit Court, on notice to that person, for an order requiring the person to comply or fully comply, as the case may be, with the requirement within a period to be specified by the Court, and the Court may make the order sought or such other order as it thinks fit or refuse to make any order.
6. The oral hearing shall be held otherwise than in public.

1. OJ No. L 119, 4.5.2016, p.1

2. OJ No. L 119, 4.5.2016, p.89

3. OJ No. L 119, 4.5.2016, p.1

4. OJ No. L 119, 4.5.2016, p.89
5. OJ No. L 180, 29.06.2013, p.1
6. OJ No. L 180, 29.06.2013, p.31
7. OJ No. L 293, 31. 10. 2008, p.3
8. OJ No. L 293, 31.10.2008, p.3
9. OJ No. L 119, 4.5.2016, p.1
10. OJ No. L 119, 4.5.2016, p.1
11. OJ No. L 119, 4.5.2016, p.1
12. OJ No. L 119, 4.5.2016, p.1
13. OJ No. L 119, 4.5.2016, p.1
14. OJ No. L 119, 4.5.2016, p.1
15. OJ No. L 119, 4.5.2016, p.1
16. OJ No. L 119, 4.5.2016, p.1
17. OJ No. L 119, 4.5.2016, p.1
18. OJ No. L 119, 4.5.2016, p.1
19. OJ No. L 119, 4.5.2016, p.1
20. OJ No. L 119, 4.5.2016, p.1
21. OJ No. L 119, 4.5.2016, p.1
22. OJ No. L 119, 4.5.2016, p.1
23. OJ No. L 119, 4.5.2016, p.1
24. OJ No. L 119, 4.5.2016, p.1
25. OJ No. L 119, 4.5.2016, p.1
26. OJ No. L 119, 4.5.2016, p.1
27. OJ No. L 119, 4.5.2016, p.1
28. OJ No. L 119, 4.5.2016, p.1
29. OJ No. L 119, 4.5.2016, p.1

30. OJ No. L 119, 4.5.2016, p.1
31. OJ No. L 119, 4.5.2016, p.1
32. OJ No. L 119, 4.5.2016, p.1
33. OJ No. L 119, 4.5.2016, p.1
34. OJ No. L 119, 4.5.2016, p.1
35. OJ No. L 119, 4.5.2016, p.1
36. OJ No. L 119, 4.5.2016, p.1
37. OJ No. L 119, 4.5.2016, p.1
38. OJ No. L 119, 4.5.2016, p.1
39. OJ No. L 119, 4.5.2016, p.1
40. OJ No. L 119, 4.5.2016, p.1
41. OJ No. L 119, 4.5.2016, p.1
42. OJ No. L 119, 4.5.2016, p.1
43. OJ No. L 119, 4.5.2016, p.1
44. OJ No. L 119, 4.5.2016, p.1
45. OJ No. L 119, 4.5.2016, p.1
46. OJ No. L 119, 4.5.2016, p.1
47. OJ No. L 119, 4.5.2016, p.1
48. OJ No. L 119, 4.5.2016, p.1
49. OJ No. L 119, 4.5.2016, p.1
50. OJ No. L 119, 4.5.2016, p.1
51. OJ No. L 119, 4.5.2016, p.1
52. OJ No. L 119, 4.5.2016, p.1
53. OJ No. L 119, 4.5.2016, p.1
54. OJ No. L 119, 4.5.2016, p.1

Estonya - Personal Data Protection Act

Personal Data Protection Act

Issuer: Riigikogu

Type: act

In force from: 15.01.2019

In force until: In force

Translation published: 23.01.2019

Personal Data Protection Act

Passed 12.12.2018

Chapter 1 GENERAL PROVISIONS

§1. Scope of regulation of Act

(1) This Act regulates:

1) protection of natural persons upon processing of personal data to the extent in which it elaborates and supplements the provisions contained in Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 04.05.2016, pp. 1-88);

2) protection of natural persons upon processing of personal data by law enforcement authorities in the prevention, detection and proceedings of offences and execution of punishments.

(2) This Act provides for:

1) standards for implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council;

2) standards for transposition of Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of

criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 04.05.2016, pp. 89-131);

3) procedure for exercise of state supervision over compliance with the requirements for the processing of personal data;

4) liability for the violation of the requirements for processing of personal data.

§2. Specifications for application of Act and Regulation (EU) 2016/679 of the European Parliament and of the Council

This Act and Regulation (EU) 2016/679 of the European Parliament and of the Council shall apply to:

1) offence proceedings and judicial proceedings with the specifications provided by procedural law;

2) constitutional institutions insofar as this does not concern the performance of their constitutional duties and is not regulated in the specific Acts that concern them.

§3. Application of Administrative Procedure Act

The provisions of the Administrative Procedure Act apply to the administrative proceedings prescribed in this Act, taking account of the specifications provided for in this Act.

Chapter 2

SPECIFIC GROUNDS FOR PROCESSING OF PERSONAL DATA

§4. Processing of personal data for journalistic purposes

Personal data may be processed and disclosed in the media for journalistic purposes without the consent of the data subject, in particular disclosed in the media, if there is public interest therefor and this is in accordance with the principles of journalism ethics. Disclosure of personal data must not cause excessive damage to the rights of any data subjects.

§5. Processing of personal data for academic, artistic and literary expression

Personal data may be processed without the consent of the data subject for the purpose of academic, artistic and literary expression, in particular disclosed if this does not cause excessive damage to the rights of the data subject.

§6. Processing of personal data for needs of scientific and historical research and official statistics

(1) Personal data may be processed without the consent of the data subject for the needs of scientific and historical research and official statistic, in particular in a pseudonymised format or a format which provides equivalent level of protection. Prior to transmission of personal data for processing

for the needs of scientific and historical research or official statistics, personal data shall be replaced by pseudonymised data or data in a format which provides equivalent level of data protection.

(2) Depseudonymisation or any other method by which the data not enabling identification of persons are changed again into the data which enable identification of persons are only permitted for the needs of additional scientific and historical research or official statistics. Processors of personal data shall designate a person identified by name who has access to the information allowing pseudonymisation.

(3) Processing of data concerning any data subjects for the needs of scientific and historical research or official statistics without the consent of the data subject in a format which enables identification of the data subject is permitted only in the case the following conditions are met:

1) the purposes of data processing can no longer be achieved after removal of the data enabling identification or it would be unreasonably difficult to achieve these purposes;

2) there is overriding public interest for it in the estimation of the persons conducting scientific and historical research or compiling official statistics;

3) the scope of obligations of the data subject is not changed based on the processed personal data or the rights of the data subject are not excessively damaged in any other manner.

(4) If scientific and historical research is based on special categories of personal data, the ethics committee of the area concerned shall first verify compliance with the terms and conditions provided for in this section. If there is no ethics committee in the scientific area, the compliance with the requirements shall be verified by the Estonian Data Protection Inspectorate. With regard to any personal data retained at the National Archives, the National Archives shall have the rights of the ethics committee.

(5) For the purposes of this Act, scientific research is deemed to also include any analyses and studies by executive power which are carried out for the purposes of policy development. In order to prepare these, the executive power has the rights to make queries to databases of another controller or processor and process the personal data received. The Estonian Data Protection Inspectorate shall verify, prior to the beginning of the specified processing of personal data, compliance with the terms and conditions provided for in this section, except in the case the objectives of the studies conducted for policy development and the scope of processing of personal data derive from legislation.

(6) Where personal data are processed for the purpose of scientific and historical research or official statistics, the controller or processor may restrict the rights of data subjects provided for in Articles

15, 16, 18 and 21 of Regulation (EU) 2016/679 of the European Parliament and of the Council insofar as the exercise of these rights is likely to make the achievement of the objectives of the scientific and historical research or official statistics impossible or impedes it to a significant extent.

§7. Processing of personal data for archiving in public interest

(1) If personal data are processed for the purpose of archiving in the public interest, the controller or processor may restrict the rights of the data subject provided for in Articles 15, 16 and 18-21 of Regulation (EU) 2016/679 of the European Parliament and of the Council insofar as the exercise of these rights is likely to make the achievement of the purpose of archiving in the public interest impossible or impedes it to a significant extent.

(2) The rights of data subjects specified in subsection (1) of this section may be restricted in order not to endanger the condition, authenticity, reliability, integrity and usability of the records.

Chapter 3 OTHER CASES OF PROCESSING PERSONAL DATA

§8. Processing of children's personal data for provision of information society services

(1) If Article 6(1)(a) of Regulation (EU) 2016/679 of the European Parliament and of the Council applies in connection with provision of information society services directly to a child, processing of the child's personal data is permitted only in the case the child is at least 13 years old.

(2) If the child is below the age of 13 years, processing of personal data is permitted only in the case and to the extent for which consent has been given by the legal representative of the child.

§9. Processing of personal data after death of data subject

(1) The consent of a data subject shall remain valid during the lifetime of the data subject and for 10 years after the death of the data subject, unless the data subject decided otherwise. If the data subject died as a minor, his or her consent shall be valid for the term of 20 years after the death of the data subject.

(2) After the death of the data subject, processing of his or her personal data is permitted only with the consent of the successors of the data subject, except in the case:

- 1) 10 years have passed since the death of the data subject;
- 2) 20 years have passed since the death of a data subject who was a minor;
- 3) personal data are processed under any other legal bases.

(3) In the case of several successors, processing of the personal data of the data subject is permitted with the consent of any of them.

(4) The consent specified in subsection (1) of this section is not required if the processed personal data only contain the data subject's name, sex, date of birth and death, the fact of death, and the time and place of burial.

§10. Processing of personal data in connection with violation of obligation

(1) Transmission of personal data related to violation of any obligation to third parties and processing of the transmitted data by any third party is permitted for the purpose of assessment of the creditworthiness of the data subject or for any other similar purposes and only in the case the controller or processor has verified the accuracy of the data transmitted and the legal basis for transmission of personal data and registered the data transmission.

(2) Collection and transmission of data to third parties for the purposes specified in subsection (1) of this section is not permitted if:

1) special categories of personal data are processed for the purposes of Article 9(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council;

2) these are data concerning commission of an offence or falling victim to an offence before a public court hearing, or making of a decision in the matter of the offence or termination of the court proceeding in the matter; 3) it would excessively damage the rights or freedoms of the data subject;

4) less than 30 days have passed from the violation of a contract;

5) more than five years have passed from the end of the violation of an obligation.

§11. Processing of personal data in public places

Unless otherwise provided by law, upon making in public places of audio or visual recordings intended for future disclosure, the consent of data subjects shall be substituted by an obligation to notify the data subjects thereof in a manner which allows the persons to understand the fact of the recording of the audio or visual images and to give the persons an opportunity to prevent the recording of their person if they so wish. The notification obligation does not apply in the case of public events, recording of which for the purposes of disclosure may be reasonably presumed.

Chapter 4

PROCESSING OF PERSONAL DATA BY LAW ENFORCEMENT AUTHORITIES IN PREVENTION, DETECTION AND PROCEEDINGS OF OFFENCES

AND EXECUTION OF PUNISHMENTS

Subchapter 1 General Provisions

§12. Application of this Chapter

(1) This Chapter shall apply to processing of personal data by law enforcement authorities in the prevention, detection and proceedings of offences and execution of punishments.

(2) This Chapter shall not apply to processing of personal data upon exercise of state supervision and administrative supervision.

(3) This Chapter prescribes the specifications applicable to law enforcement authorities. Regulation (EU) 2016/679 of the European Parliament and of the Council shall not apply to law enforcement authorities, unless otherwise provided for in this Act.

§13. Terms

(1) Terms in this Chapter shall have the meaning specified in Article 4 and Article 9(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council.

(2) For the purposes of this Chapter, law enforcement authorities are deemed to include any agencies or structural entities of agencies which are competent pursuant to law to prevent, detect and proceed offences and execute punishments.

Subchapter 2 Principles

§14. Principles of processing personal data

The following principles have to be complied with upon processing of personal data:

- 1) legality and fairness - personal data are processed legally and fairly;
- 2) purposefulness - personal data are collected for specified, explicit and legitimate purposes and they shall not be processed in any manner which is incompatible with these purposes;
- 3) quality - personal data must be adequate and appropriate and must not be excessive given the purposes of the data processing;
- 4) accuracy - personal data must be accurate and, if necessary, kept up to date; reasonable measures are taken to ensure that any personal data which are inaccurate with respect to the purpose of data processing shall be erased or rectified without delay;
- 5) retention - personal data are retained in the format which enables to identify the data subject only until this is necessary for achievement of the purpose for which the personal data is processed;

6) security - personal data are processed in a manner that ensures appropriate security thereof, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by means of implementing appropriate technical or organisational measures.

§15. Lawfulness of processing of personal data

Law enforcement authorities may process personal data pursuant to law if the processing thereof is required for performance of the functions arising from the purpose of prevention, detection and proceedings of offences and execution of punishments.

§16. Processing of personal data for purposes different from initial ones

(1) Processing of personal data by the same or another controller for other purposes provided for in subsection 12 (1) of this Act, which are not the initial purposes for which the personal data was collected, is permitted insofar as:

- 1) the controller has the grounds pursuant to law or the legislation of the European Union for processing of personal data for such purposes; and
- 2) such processing of personal data is required according to law or the legislation of the European Union and it is proportional with the purpose pursued.

(2) Personal data collected or to be collected by law enforcement authorities for the purposes provided for in subsection 12 (1) of this Act may not be processed for any other purposes, except in the cases provided for in subsection (1) of this section or if such processing is permitted by law or the legislation of the European Union. If personal data are processed for such other purposes, Regulation (EU) 2016/679 of the European Parliament and of the Council shall apply, except in the case personal data are processed in the course of such activities which are not in the scope of regulation of the specified regulation. In any situation where the purposes of processing are not in the scope of application of the specified regulation, the Estonian law shall apply.

(3) If law enforcement authorities also perform, in accordance with law, other functions besides those which are performed for the purposes provided for in subsection 12 (1) of this Act, Regulation (EU) 2016/679 of the European Parliament and of the Council shall apply to processing of personal data for such purposes. In any situation where the purposes of processing are not in the scope of application of the specified regulation, the Estonian law shall apply.

§17. Retention of personal data

(1) A retention period shall be established for processed personal data by law or regulation. In exceptional cases where no retention period has been established by law or regulation for personal data, the controller must establish this term.

(2) The retention period established pursuant to subsection (1) of this section may be extended only in justified cases, except when the retention period is provided for in a legislative act.

(3) If no specific retention period can be established, the controller must implement legal and technological measures which enable to continuously assess the need for continued processing of the data.

(4) If the term for retention of personal data expires, the controller and processor are required to permanently erase the personal data. For this purpose, the controller must implement appropriate legal and technological measures.

§18. Differentiation between different categories of data subjects

If possible and appropriate, the controller shall distinguish, upon processing of personal data, between persons subject to proceedings, suspects, accused, injured parties, witnesses, imprisoned persons, detained persons, probationers and other persons as different categories of data subjects.

§19. Distinguishing of personal data based on assessments

The controller shall distinguish, as far as possible, personal data based on facts from personal data based on personal assessments.

§20. Specifications for processing of personal data of special categories

(1) Processing of personal data of special categories is permitted only if this is strictly necessary and only in the following cases:

- 1) admissibility of processing is provided for in the legislation;
- 2) processing is necessary in order to protect the vital interests of the data subject or of any other natural person; or
- 3) processing relates to personal data which are manifestly made public by the data subject.

(2) Appropriate safeguards for protection of the rights and freedoms of data subjects apply to processing of personal data of special categories specified in subsection (1) of this section.

§21. Automatic processing

(1) It is prohibited to make a decision based on only automatic processing, including profiling, if it brings adverse legal consequences for the data subject pertaining to the data subject or has any other significant effect on the data subject. Such decision may be made if making of the decision is permitted by law which provides for appropriate measures to protect the rights and freedoms and legitimate interests of the data subjects.

(2) The data subject has the right to raise objections to the decision specified in subsection (1) of this section to the controller for the protection of the data subject's legitimate interests.

(3) The decision specified in subsection (1) of this section must not be based on personal data of special categories, except in the case appropriate measures are applied for the protection of the rights, freedoms and legitimate interests of the data subjects.

(4) It is prohibited to make decisions based on profiling as a result of which natural persons are discriminated on the basis of special categories of personal data.

Subchapter 3 Rights of Data Subjects

§22. Information to be made available to data subjects

(1) The controller is required to disclose the following information:

- 1) the intended purpose of processing of personal data;
- 2) the right of the person to access his or her data and to rectify, erase or restrict thereof and the procedure for the exercise of these rights;
- 3) the name and contact details of the controller and data protection specialist;
- 4) the contact details of the Estonian Data Protection Inspectorate;
- 5) the right to file a complaint to the Estonian Data Protection Inspectorate, if the rights of data subjects have been violated upon processing of personal data.

(2) Disclosure of information on the website of the controller or in any other places which are easily accessible by data subjects is considered to be the disclosure specified in subsection (1) of this section.

§23. Information provided upon notification of data subjects

(1) If an obligation to notify data subjects of processing of their personal data is provided by law, the controller shall provide the following additional information to the data subject:

- 1) the information specified in subsection 22 (1) of this Act;
- 2) the legal basis for processing of personal data;

- 3) the retention period of personal data or the bases for determining the retention period;
- 4) the categories of the recipients to whom transmission of the personal data is permitted;
- 5) if necessary, any other additional information.

(2) In the cases provided by law, the controller may also transmit the information provided for in subsection (1) of this section to data subjects later, restrict the transmission thereof or not transmit it, if this may:

- 1) prevent or impair prevention, detection or proceedings of offences or execution of punishments;
- 2) damage the rights and freedoms of other persons;
- 3) endanger the national security;
- 4) endanger protection of public order;
- 5) hinder formal investigation or proceedings.

§24. Right of data subjects to obtain information and personal data concerning them

(1) Data subjects have the right to obtain a confirmation from the processor of processing of their personal data. At the request of the data subject, the processor of personal data shall communicate the following to the data subject:

- 1) the personal data concerning the data subject and the categories of the personal data concerned;
- 2) the information available about the origin of the personal data;
- 3) the purposes of and legal basis for processing of personal data;
- 4) the recipients or the categories thereof to whom personal data of the data subject have been disclosed;
- 5) the intended retention period of the personal data or the bases for determining the retention period;
- 6) the right to apply to the controller for rectification of the personal data of the data subject, erasure or restriction of processing thereof;
- 7) the right to file a complaint with the Estonian Data Protection Inspectorate and the contact details of the Estonian Data Protection Inspectorate.

(2) In the cases provided by law, the controller may also transmit the information provided for in subsection (1) of this section to data subjects later, restrict the transmission thereof or refuse to issue it if this may:

- 1) prevent or impair prevention, detection or proceedings of offences or execution of punishments;
- 2) damage the rights and freedoms of other persons;
- 3) endanger the national security;
- 4) endanger protection of public order;
- 5) hinder formal investigation or proceedings.

(3) The controller shall notify data subjects immediately in writing of restricting access to the information specified in subsection (1) of this section or refusal to access such information and the reasons for it. The controller need not state the reasons if provision of such information would bring about any of the circumstances specified in subsection (2) of this section.

(4) Upon notification of data subjects in accordance with subsection (3) of this section, the controller shall notify the data subjects of their right to address the Estonian Data Protection Inspectorate or a court in order to appeal the decision.

(5) The controller shall document any factual and legal bases of the decision made pursuant to subsection (2) of this section and, if necessary, make this information available to the Estonian Data Protection Inspectorate.

§25. Right of data subjects to request rectification and erasure of personal data

(1) Data subjects have the right to demand from the processor rectification of any inaccurate personal data based on facts concerning the data subject.

(2) Data subjects have the right to request from the controller erasure of any incomplete personal data concerning the data subject if this is appropriate in light of the purpose of processing of personal data.

(3) Data subjects have the right to demand from the controller erasure of the personal data collected if:

- 1) the processing of personal data is not permitted pursuant to law;
- 2) the principles of processing of personal data were not taken into account upon processing of the personal data; or
- 3) the controller is obliged to erase the data in order to comply with any obligations under the law, judgment, international agreement or other binding agreements.

(4) The controller shall restrict processing of personal data instead of erasing thereof if:

1) the data subject contests the accuracy of the personal data and the accuracy or inaccuracy thereof cannot be ascertained; or

2) the personal data must be retained for verification purposes.

(5) If the controller has implemented, instead of erasure of personal data, restriction of processing of personal data provided for in clause (4) 1) of this section, the controller must notify the data subject of removal of such restriction.

(6) The controller is required to immediately notify the data subject in writing, if the controller refuses to rectify or erase the personal data or restrict the processing thereof, and state the reasons for the refusal. The controller need not state the reasons if provision of such information would bring about any of the circumstances specified in subsection 24 (2) of this Act.

(7) Upon notification of data subjects in accordance with subsection (6) of this section, the controller shall notify the data subjects of their right to address the Estonian Data Protection Inspectorate or a court in order to appeal the decision.

§26. Controller's obligation to notify of rectification, erasure of personal data and restriction of processing thereof

(1) In the case of rectification of personal data, the controller is required to immediately notify a competent authority, from which the incorrect personal data were received, of the rectification and the subject matter of the rectification.

(2) If any personal data have been rectified or erased pursuant to §25 of this Act or the processing thereof has been restricted, the controller is required to notify the recipients to whom the data had been earlier transmitted.

(3) The recipients specified in subsection (2) of this section are required to rectify or erase the personal data under their responsibility or restrict the processing thereof.

§27. Procedure for exercise of rights of data subjects

(1) The controller is required to respond to any applications of data subjects in a concise, intelligible and easily accessible form, using clear and plain wording. If possible, the data subject's request will be answered in the manner requested by the data subject.

(2) The controller shall notify the data subject without any undue delay within one month after the receipt of the application of the activities carried out based on the request of the data subject.

(3) The controller may request the data subject to compensate for any reasonable costs associated with dealing with the request and provided by law or legislation issued pursuant to law or refuse to take the measures requested, if the request of the data subject is unreasonable or excessive.

(4) The controller shall identify the data subject and the right of the data subject to receive information and personal data concerning the data subject or the right to request rectification and erasure of the personal data.

§28. Data subject's right to address Estonian Data Protection Inspectorate

(1) If any data subject finds that the rights of the data subject are violated upon processing of personal data, the data subject has the right to address the Estonian Data Protection Inspectorate with a complaint.

(2) The Estonian Data Protection Inspectorate shall notify the data subject of the decision made based on the data subject's complaint and the right to have recourse to courts in order to contest the decision of the Estonian Data Protection Inspectorate.

(3) If a competent supervisory authority of another Member State of the European Union has jurisdiction in solving the complaint of the data subject, the Estonian Data Protection Inspectorate shall refer the data subject to the competent supervisory authority of the other Member State of the European Union for filing the complaint.

Subchapter 4 Obligations of Controllers and Processors

§29. Controller and processor of database

(1) The controller shall implement appropriate technical and organisational measures to ensure compliance with the requirements of this Act upon processing of personal data. If necessary, the controller is required to demonstrate compliance with the requirements provided for in this Act.

(2) The controller shall provide the processor with mandatory instructions for processing of personal data and shall be responsible for the processor's compliance with the personal data processing requirements.

(3) The controller may use only such processors which provide sufficient guarantees that they implement appropriate technical and organisational measures in such a manner that processing of personal data will meet the requirements of this Act and ensure the protection of the rights of the data subject.

(4) The processor may involve other processors in processing of personal data only pursuant to law or legislation issued pursuant to law or with a written authorisation of the controller and provided that the powers granted to the processor are not exceeded. In the case of powers granted by a written authorisation, the processor must always notify the controller of adding or replacing of other processors. In this case the controller may state objections to the changes.

(5) If the processor determines the purposes and means for processing of personal data in violation of this Act, the processor in questions shall be the controller with regard to such processing.

§30. Designation and obligations of processor

(1) The controller may designate a processor to process personal data pursuant to law, legislation issued pursuant to law or under a written contract which provides for the subject matter and duration of processing of personal data, the nature and purposes thereof, categories of personal data processed and categories of data subjects and the obligations and rights of the controller.

(2) The Act specified in subsection (1) of this section, legislation issued on the basis of the Act or contract shall provide, in particular, that the processor is required to:

- 1) act only in accordance with the instructions of the controller;
- 2) ensure that the persons authorised to process personal data would keep the confidentiality of personal data which become known upon performance of their duties;
- 3) ensure protection of the rights of the data subject;
- 4) after the end of the provision of data processing services, erase or return to the controller at the choice thereof all the personal data and erase any existing copies thereof, unless otherwise provided by law;
- 5) make available to the controller any information relating to processing of personal data which is required for demonstrating compliance with the requirements provided for in this section;
- 6) comply with the terms and conditions provided for in subsection 29 (4) of this Act and this section for involvement of another processors.

§31. Joint controllers

(1) Where two or more controllers jointly determine the purposes and means of processing of personal data, they shall be joint controllers.

(2) The responsibility of joint controllers and the scope of the obligations thereof shall be determined in law, legislation issued pursuant to law or a contract entered into between joint controllers.

(3) A contact point through which data subjects are able to exercise their rights shall be determined in the contract specified in subsection (2) of this section for the data subjects.

(4) The data subject may exercise the rights under this Act with respect to each controller.

§32. Processing of personal data in name of controller and processor

(1) Any person who processes personal data in the name of a controller or processor is required to process these data only in accordance with the instructions given by the controller, unless otherwise provided by law.

(2) The right of the person to process personal data in the name of the controller or processor must be based on law, legislation issued pursuant to law, contract entered into between the controller or processor and the person or the legal instrument governing the service relationship.

§33. Data protection by design and by default

(1) The controller and processor shall take technical and organizational measures upon determining the means of processing and for processing of personal data and implement them consistently.

(2) The controller and processor shall implement appropriate technical and organizational measures which ensure that by default only the personal data are processed which are required for achievement of each specific purpose of processing.

§34. Personal data processing requirements

In the processing of personal data, the controllers and processors are required to:

- 1) rectify inaccurate personal data;
- 2) erase personal data, if processing of the personal data is not permitted pursuant to law or this does not conform to the principles of processing of personal data;
- 3) notify the recipient if the personal data have been transmitted illegally or if inaccurate personal data have been transmitted;
- 4) co-operate with the Estonian Data Protection Inspectorate.

§35. Personal data transmission requirements

(1) The controller is required to take and implement appropriate measures in order to avoid transmission or making available of incomplete, inaccurate or outdated personal data.

(2) If possible, the controller shall add, upon transmission of personal data, the required information which allows the competent authority which receives the data to assess the accuracy, integrity, reliability and relevance of the personal data.

(3) If special terms and conditions apply to processing of personal data, the controller shall notify the receiver upon transmission of such personal data of the terms and conditions in questions and the requirement to comply with them.

(4) Upon transmission of personal data to other receivers in the European Union and agencies established in accordance with Chapters 4 and 5 of Section V of the Treaty on the Functioning of the European Union, no special terms and conditions for processing of personal data shall apply compared to those which are applied to transmission of personal data within the country.

§36. Logging

(1) The controller and processor must keep logs at least of the following personal data processing activities carried out in automated systems:

- 1) collection;
- 2) amendment;
- 3) reading;
- 4) disclosure;
- 5) transmission;
- 6) combination;
- 7) erasure.

(2) Logs recording reading, disclosure and transmission must enable to ascertain the reasoning for conduct of the specified activities, the date and time thereof and the information about the person who read, disclosed or transmitted the personal data, and the names of the recipients of such personal data.

(3) It is allowed to use the logs for verification of legality of personal data processing activities, internal monitoring, ensuring integrity and security of personal data and for offence proceedings.

(4) At the request of the Estonian Data Protection Inspectorate, the controller and processor shall make the information specified in subsection (1) of this section available to the Estonian Data Protection Inspectorate.

(5) The controller shall establish the retention periods of logs.

§37. Records of personal data processing activities

(1) The controller shall maintain a record of all the types of personal data processing activities under its responsibility. The following information must be recorded:

- 1) the name and contact details of the controller and, where appropriate, joint controller;
- 2) the name and contact details of the data protection specialist;
- 3) the purposes of processing of personal data;
- 4) the recipients and the categories thereof to whom the personal data have been or will be disclosed;
- 5) the description of the categories of data subjects and of the categories of personal data;
- 6) where appropriate, the use of profiling;
- 7) where appropriate, types of transmission of personal data to third countries or international organizations;
- 8) information on the legal basis of processing of personal data;
- 9) if possible, time limits prescribed for erasure of special categories of personal data;
- 10) if possible, a description of the organizational and technical security measures taken to process personal data pursuant to §43 of this Act.

(2) The processor shall record all the types of operations related to processing of personal data made in the name of the controller. The following information must be recorded:

- 1) the name and contact details of the processor, and the name and contact details of the controller in the name of whom the processor operates;
- 2) where appropriate, the name and contact details of the data protection officer;
- 3) the types of personal data processing carried out in the name of the controller;
- 4) where appropriate, transmission of personal data to third countries or international organizations, including data for identification of the third country or international organization in question;
- 5) if possible, a description of the organizational and technical security measures taken to process personal data pursuant to §43 of this Act.

(3) The information specified in subsections (1) and (2) of this section shall be recorded in a format which can be reproduced in writing.

(4) At the request of the Estonian Data Protection Inspectorate, the controller or the processor shall make the information specified in subsections (1) and (2) of this section available to the Estonian Data Protection Inspectorate.

§38. Data protection impact assessment

(1) The controller shall assess, prior to processing of personal data, the impact of intended personal data processing operations to the protection of personal data, if the processing of personal data may involve a great risk for the personal rights and freedoms of natural persons taking into account the nature, extent, context and purposes of processing.

(2) The impact assessment must include at least the following:

- 1) a systematic description of the intended personal data processing operations and processing purposes;
- 2) an assessment of the need and proportionality of personal data processing operations taking into account the purposes of processing of personal data;
- 3) an assessment of the risks to the rights and freedoms of data subjects;
- 4) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act, taking into account the rights and legitimate interests of data subjects and other persons concerned.

§39. Consultation with Estonian Data Protection Inspectorate

(1) If the controller or processor intends to process personal data which are entered into a new filing system to be created, the controller or processor must first consult the Estonian Data Protection Inspectorate in the following cases:

- 1) the data protection impact assessment issued pursuant to §38 of this Act indicates that the processing of personal data would result in a high risk in the absence of measures taken by the controller;
- 2) the nature of processing of personal data involves a high risk to the rights and freedoms of data subjects.

(2) For assessment of conformity with personal data processing requirements, the controller shall submit the following information to the Estonian Data Protection Inspectorate:

- 1) the data protection impact assessment provided for in §38 of this Act;

- 2) the purposes and manner of intended personal data processing;
- 3) the measures and guarantees prescribed for the protection of the rights and freedoms of data subjects;
- 4) the contact details of the data protection officer, where applicable;
- 5) where appropriate, responsibilities of controllers, joint controllers and processors upon processing of personal data;
- 6) other information requested by the Estonian Data Protection Inspectorate.

(3) If, in the opinion of the Estonian Data Protection Inspectorate, the intended processing of personal data specified in subsection (1) of this section would violate the requirements of this Act, the Estonian Data Protection Inspectorate shall give written advice to the controller and, where appropriate, the processor on how to bring the data processing into compliance with the requirements of this Act.

(4) The Estonian Data Protection Inspectorate shall give advice to the controller or processor within six weeks as of the receipt of the information specified in subsection (2) of this section.

(5) The term specified in subsection (4) of this section may be extended by one month, taking into account the complexity of the intended processing of personal data. The Estonian Data Protection Inspectorate shall notify the controller or processor of extension of the term within one month after receipt of the consultation request. The reasons for extending the term have to be indicated.

(6) The Estonian Data Protection Inspectorate may prepare a list of the personal data processing operations in the case of which the earlier consultations specified in subsection (1) of this section are required.

Subchapter 5 Data Protection Specialist

§40. Designation of data protection specialist

(1) Law enforcement authorities designate data protection specialists. Courts are released from this obligation upon performance of the function of administration of justice.

(2) Law enforcement authorities may designate one data protection specialist for several agencies or bodies depending on the structure and size of these organizations.

(3) Designation of a data protection specialist shall be based on his or her professional skills and expert knowledge of data protection legislation and practice and his or her ability to perform the functions provided for in §41 of this Act.

(4) A data protection specialist may be an official or employee in the service of a law enforcement authority or fulfil the tasks on the basis of a service contract.

§41. Tasks of data protection specialist

(1) A data protection specialist shall perform at least the following tasks:

1) inform and advise the law enforcement authority and the officials and employees who process personal data on behalf of the latter in connection with their obligations under this Act and other data protection standards of the European Union or its Member States;;

2) ensure consistency with this Act, if necessary, with data protection standards of the European Union or its Member States and the internal policies of the controller which concern the principles of personal data protection and awareness-raising and training of officials and employees involved in processing of personal data;

3) provide advise as regards the data protection impact assessment and monitor its performance pursuant to §38 of this Act;

4) co-operate with the Estonian Data Protection Inspectorate;

5) act as the contact person in the issues of personal data processing for the Estonian Data Protection Inspectorate, including in the course of the earlier consultation provided for in §39 of this Act, and also consult in other issues, if necessary.

(2) The data protection specialist of a court shall not perform the tasks specified in subsection (1) of this section with regard to any activities of the court related to administration of justice.

(3) A data protection specialist may perform other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests for the data protection specialist.

§42. Position of data protection specialist

(1) The controller shall ensure that the data protection specialist is involved, properly and in a timely manner, in all the issues which relate to the protection of personal data.

(2) The controller shall support the data protection specialist in performing the tasks referred to in §41 of this Act by providing the resources necessary to carry out the tasks in question and access to personal data and processing operations thereof, and to maintain his or her expert knowledge.

(3) The provisions of Article 38(3)-(6) of Regulation (EU) No 2016/679 of the European Parliament and of the Council apply to the position of a data protection specialist.

Subchapter 6

Security measures of processing personal data and notification of violations related to personal data

§43. Security measures of processing personal data

The controller and the processor are required to take and implement organizational and technical security measures to the protect personal data in order to:

- 1) prohibit access of unauthorised persons to data processing equipment used for processing of personal data;
- 2) prevent unauthorized reading, copying, modification and removal of storage media;
- 3) prevent unauthorised input of personal data and unauthorised inspection, modification or deletion of retained personal data;
- 4) prevent deletion of data processing systems by unauthorised persons by means of data communication equipment;
- 5) ensure access by users who hold an authorisation for the use of automated data processing systems only to such personal data which are covered by the access authorisation of the users;
- 6) ensure an opportunity to verify and establish to which agencies personal data have been or may be transmitted or made available using data communication equipment;
- 7) ensure an opportunity to verify and establish what personal data have been input into automated data processing systems and when and by whom the data were input;
- 8) prevent unauthorised reading, copying, modification or deletion of personal data during transmissions of personal data or during transportation of storage media;
- 9) ensure an opportunity to restore installed data processing systems in the case of interruptions;
- 10) ensure functioning of data processing systems and notification of any faults in the functions thereof;
- 11) prevent misrepresentation of personal data as a result of system malfunctions.

§44. Notification of Estonian Data Protection Inspectorate of personal data breach

(1) If a personal data breach is likely to entail a high risk to the rights and freedoms of natural persons, the controller shall immediately notify the Estonian Data Protection Inspectorate of the breach, if possible within 72 hours after becoming aware thereof.

(2) The processor shall immediately notify the controller after becoming aware of a personal data breach.

(3) The following information shall be submitted in the notice specified in subsection (1) of this section:

1) the subject matter of the breach, including the nature of the personal data breach, if possible, categories of relevant data subjects and their approximate number, and relevant categories of personal data and their approximate number;

2) the name and contact details of the data protection officer;

3) the description of possible consequences of the personal data breach;

4) measures taken or intended by the controller to resolve personal data breaches, including measures to mitigate any adverse impact of possible consequences of breaches.

(4) If the Estonian Data Protection Inspectorate is notified of a personal data breach after the expiry of 72 hours from becoming aware of it, the reasons thereof shall be stated.

(5) If a personal data breach concerns personal data which have been transmitted by a controller of another Member State of the European Union or to a controller of another Member State of the European Union, the information referred to in subsection (3) of this section shall be transmitted without undue delay to the controller of the Member State in question.

(6) The controller shall document all the personal data breaches specified in subsection (1) of this section, including the circumstances of the breaches, the impact thereof and remedial measures taken.

§45. Notification of data subject of personal data breach

(1) When a breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall immediately notify the data subject of the personal data breach.

(2) The notification specified in subsection (1) of this section shall describe, in clear and simple language, the nature of the personal data breach and state at least the information specified in clauses 44 (3) 2)-4) of this Act.

(3) The notification specified in subsection (1) of this section shall not be required if at least one of the following conditions is met:

1) the controller has implemented appropriate technological and organizational safeguards and these safeguards have been applied to the personal data affected by the breach;

2) the controller has taken subsequent measures which exclude realisation of the high risk specified in subsection (1) of this section to the rights and freedoms of the data subject;

3) individual notification of the data subject would lead to disproportionate costs and the public has been notified of the breach.

(4) If the controller has not yet notified the data subject of the personal data breach, the Estonian Data Protection Inspectorate may decide, after assessment of the gravity of the breach, whether the notification of the data subject of the personal data breach is required or any of the cases specified in subsection (3) of this section occurs.

(5) The data subject may be notified of the breach specified in subsection (1) of this section later, to a limited extent, or the notification of the data subject may be withheld, if this may:

1) prevent or impair prevention, detection or proceedings of offences or execution of punishments;

2) damage the rights and freedoms of other persons;

3) endanger the national security;

4) endanger protection of public order;

5) hinder formal investigation or proceedings.

Subchapter 7

Transmission of Personal Data to Third Countries and International Organisations

§46. General terms and conditions of transmission of personal data to third countries and international organisations

(1) It is permitted to transmit personal data to third countries or international organisations only in the case all the following terms and conditions are met:

1) transmission is necessary for prevention, detection or processing of offences or execution of punishments;

2) personal data are transmitted to the controller in any third country or international organisation that is competent to prevent, detect and proceed offences or execute punishments;

3) consent of another Member State of the European Union for further use of the data, if the data transmitted have been received from this Member State;

4) the European Commission has adopted a decision pursuant to Article 36 of Directive (EU) 2016/680 of the European Parliament and Council on adequacy of the protection or, in the absence of such decision, the safeguards specified in §47 of this Act or in the absence thereof the exception specified in §48 of this Act is applied;

5) it is ensured upon transmission of personal data that the controller that transmits data has given an earlier consent for further transmission of personal data to another third country or international organization.

(2) If the authorisation specified in clause (3) 1) of this section for transmission of personal data cannot be obtained in due time and transmission of personal data is necessary to prevent any immediate and serious threats to the public order of the state or any third country or to protect essential interest of the state, the personal data may be transmitted without the authorisation specified in clause (3) 1) of this section. The competent authority of the Member State of the European Union which transmitted personal data shall be immediately notified of the data exchange provided for in this subsection.

(3) When giving the consent specified subsection clause (1) 5) of this section, the controller or processor shall inter alia take into consideration the gravity of the offence, the purpose of initial transmission of personal data and the protection level of personal data in this third country or international organization where the personal data are sent.

(4) If the European Commission has adopted the decision specified in Article 36(5) of Directive (EU) 2016/680 of the European Parliament and of the Council, personal data may be transmitted to third countries or international organizations pursuant to §§47 and 48 of this Act.

§47. Transmission of personal data subject to application of appropriate safeguards

In the absence of the decision of the European Commission specified in clause 46 (1) 4) of this Act on the adequacy of the protection, personal data may be transmitted to third countries or international organizations in the following cases:

1) the appropriate safeguards taken for the protection of personal data are provided for in a legally binding legal instrument;

2) the controller has assessed all the circumstances relating to transmission of personal data and found that all the safeguards appropriate from the point of view of protection of personal data have been taken.

§48. Transmission of personal data in exceptional cases

(1) If the absence of the decision of the European Commission specified in clause 46 (1) 4) of this Act or in the absence of appropriate safeguards specified in §47 of this Act, transmission of personal data to third countries or international organizations is permitted if this is required in order to:

- 1) protect the rights and freedoms of data subjects or any other persons;
- 2) protect the legitimate interests of data subjects;
- 3) prevent immediate and serious threat to public order;
- 4) prevent, detect or process offences or execute punishments; or
- 5) compile, submit or defend a particular legal claim related to the aim of prevention, detection or processing of a particular offence or enforcement of punishment.

(2) If the rights of the data subject outweigh the interest provided for in clauses (1) 4) and 5) of this section, transmission of personal data shall not be permitted.

§49. Transmission of personal data to recipients in third countries

Personal data may be transmitted directly to a recipient in any third country if all the following conditions are met:

- 1) the transmission is strictly necessary for performance of the tasks of the law enforcement authority, which transmits the personal data, for the purpose of prevention, detection and proceeding of offences or execution of punishments;
- 2) the public interest outweighs the rights and freedoms of the data subject;
- 3) the transmission of personal data to an agency of any third country, which is competent to prevent, detect and process the offence or execute the punishment, is not effective or appropriate;
- 4) the agencies of third countries which are competent to prevent, detect and proceed offences or execute punishments shall be notified immediately, except in the case this is not effective or appropriate;
- 5) the recipient shall be notified of the specific purpose of processing of personal data and is directed to process personal data only for the specified purpose.

§50. Notification of Estonian Data Protection Inspectorate and documentation of transmission of personal data

(1) The controller or processor shall provide an overview to the Estonian Data Protection Inspectorate of transmission of personal data pursuant to clause 47 2) and §49 of this Act at least once a year.

(2) If personal data is transmitted pursuant to clause 47 2), subsection 48 (1) or §49 of this Act, the controller or processor shall document such transmission, including the date and time of transmission, the details of the receiving competent authority, the explanation of transmission and the personal data transmitted.

(3) At the request of the Estonian Data Protection Inspectorate, the controller or processor shall make the information specified in subsection (2) of this section available to it.

Chapter 5

STATE AND ADMINISTRATIVE SUPERVISION

Subchapter 1 Supervisory Authority

§51. Formation of independent supervisory authority

(1) An independent supervisory authority for the purposes of Article 51(1) of Regulation (EU) 2016/679 of the European Parliament and the Council and Article 41 of Directive (EU) 2016/680 of the European Parliament and the Council is the Estonian Data Protection Inspectorate.

(2) In the performance of its functions, the Estonian Data Protection Inspectorate is independent and acts pursuant to this Act, Regulation (EU) 2016/679 of the European Parliament and the Council, other Acts and legislation established on the basis thereof.

§52. Qualifications required to be appointed as head of Estonian Data Protection Inspectorate

(1) Any person with management skills and higher education who has expertise in the legal regulation of personal data protection and in information systems and information and communications technology may be employed as the head of the Estonian Data Protection Inspectorate.

(2) The head of the Estonian Data Protection Inspectorate may not participate in the activities of political parties or hold any other remunerative position or office during his or her term of office, except in the field of pedagogical work or research.

§53. Security check of candidate for head of Estonian Data Protection Inspectorate

(1) The candidate for head of Estonian Data Protection Inspectorate must pass a security check before being appointed the head of Estonian Data Protection Inspectorate, except if he or she has a valid access authorisation to access state secrets classified as top secret or, if at the time of becoming a candidate, he or she holds a position which grants the right by virtue of office to access all classifications of state secrets.

(2) The security check of the candidate for the head of Estonian Data Protection Inspectorate shall be carried out by the Security Police Board pursuant to the procedure provided for in the Security Authorities Act.

(3) In order to pass the security check, the candidate for the head of Estonian Data Protection Inspectorate shall submit a completed form for an applicant for an authorisation to access state secrets classified as top secret to the Security Police Board through the Ministry of Justice, and sign a consent which permits the agency which performs security checks to obtain information concerning the person from natural and legal persons and state and local government agencies and bodies during the performance of the security check.

(4) The Security Police Board shall, within three months as of receipt of the documents specified in subsection (3) of this section, communicate the information gathered as a result of the security check to the minister responsible for the area and provide an opinion concerning the compliance of the candidate for the head of Estonian Data Protection Inspectorate with the conditions for the issue of an authorisation for access to state secrets.

(5) In the cases where the authority of the head of Estonian Data Protection Inspectorate has terminated prematurely, the security check of the candidate for the head of Estonian Data Protection Inspectorate shall be carried out within one month as of the receipt of the documents specified in subsection (3) of this section. With the permission of the Committee for the Protection of State Secrets, the term for carrying out the security check may be extended by one month if circumstances specified in clause 33 (4) 1) or 2) of the State Secrets and Classified Information of Foreign States Act become evident or circumstances specified in clause 3) or 4) may become evident within one month.

(6) Based on the information gathered in the course of the security checks carried out, a candidate for the position of the head of the Estonian Data Protection Inspectorate may be appointed to office within nine months as of the forwarding of the information gathered throughout the security checks to the minister responsible for the area by the Estonian Internal Security Service. A candidate for the position of the head of the Estonian Data Protection Inspectorate may be appointed to office later than the above term after passing a new security check.

§54. Appointment to and dismissal from office of head of Estonian Data Protection Inspectorate

(1) The Government of the Republic shall appoint the head of Estonian Data Protection Inspectorate to office for a term of five years at the proposal of the minister responsible for the area after having heard the opinion of the Constitutional Committee of the Riigikogu.

(2) Before premature dismissal from office of the head of the Estonian Data Protection Inspectorate, the opinion of the Constitutional Committee of the Riigikogushall be heard.

§55. Competence of Estonian Data Protection Inspectorate upon accreditation of certification authority

The competent authority for the purposes of Article 43(1) of Regulation (EU) 2016/679 of the European Parliament and the Council, which is competent to accredit certification authorities that have an appropriate level of expertise in relation to data protection is the Estonian Data Protection Inspectorate.

Subchapter 2 Exercise of State and Administrative Supervision

§56. Competence of Estonian Data Protection Inspectorate upon exercise of state and administrative supervision

(1) State and the administrative supervision over compliance with the requirements provided for in this Act, legislation established on the basis thereof and Regulation (EU) 2016/679 of the European Parliament and of the Council and the requirements established in other Acts for processing of personal data shall be exercised by the Estonian Data Protection Inspectorate.

(2) In addition to the provision of Article 57 of Regulation (EU) No. 2016/679 of the European Parliament and of the Council, the Estonian Data Protection Inspectorate is competent to:

1) improve the awareness and understanding of the public, controllers and processors of the risks in the processing of personal data, the standards and safeguards in force for processing and the rights related to processing of personal data; the Estonian Data Protection Inspectorate may give recommended instructions for the performance of this function;

2) provide information to data subjects upon request about the exercise of the rights arising from this Act and, where appropriate, co-operate for this purpose with the supervisory authorities of other Member States of the European Union;

- 3) if necessary, initiate misdemeanour proceedings and impose a punishment, in the case no other administrative measures allow to achieve compliance with the requirements provided by law or Regulation (EU) 2016/679 of the European Parliament and the Council;
- 4) co-operate with international data protection supervision organisations and other data protection supervision authorities and other competent foreign authorities and persons;
- 5) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communications technologies;
- 6) give advice on the personal data processing operations referred to in §39 of this Act;
- 7) participate in the European Data Protection Board;
- 8) apply administrative coercion on the bases, to the extent and pursuant to the procedure prescribed by Acts;
- 9) present opinions on own initiative or upon request in the issues related to protection of personal data to the Riigikogu, the Government of the Republic, the Chancellor of Justice and other agencies and the public;
- 10) perform other duties arising from Acts.

(3) In addition to the provisions of Article 57 of Regulation (EU) No. 2016/679 of the European Parliament and of the Council, the Estonian Data Protection Inspectorate has the right to:

- 1) warn controllers and processors that intended processing operations are likely to infringe this Act;
- 2) demand rectification of personal data;
- 3) demand erasure of personal data;
- 4) demand restrictions on processing of personal data;
- 5) demand termination of processing of personal data, including destruction or forwarding to an archive;
- 6) where necessary, immediately apply, in order to prevent damage to the rights and freedoms of persons, organisational, physical or information technology security measures to protect personal data pursuant to the procedure provided for in the Substitutional Performance and Non-Compliance Levies Act, unless the personal data are processed by a state agency;
- 7) implement temporary or permanent restrictions on processing of personal data, including prohibition on processing of personal data;

8) initiate supervision proceedings on the basis of a complaint or on its own initiative.

§57. Special state supervision measures

In order to exercise state supervision provided for in this Act, the Estonian Data Protection Inspectorate may apply the specific state supervision measures provided for in §§30-32, 44, 49-53 of the Law Enforcement Act on the basis of and pursuant to the procedure provided for in the Law Enforcement Act.

§58. Specifications for state supervision

(1) The Estonian Data Protection Inspectorate may implement upon exercise of state supervision the measures provided for in Article 58 of Regulation (EU) No 2016/679 of the European Parliament and of the Council.

(2) The Estonian Data Protection Inspectorate may make enquiries to electronic communications undertakings about the data required for the identification of an end-user related to the identification tokens used in public electronic communications networks, except for the data relating to the fact of transmission of messages if identification of an end-user related to the identification tokens is impossible in any other manner.

§59. Specifications for administrative supervision

(1) When exercising administrative supervision, the Estonian Data Protection Inspectorate may, upon failure to comply with a precept issued subject to Article 83 (7) of Regulation (EU) 2016/679 of the European Parliament and Council and provisions of §§751 and 752 of the Government of the Republic Act, address a superior agency, person or body of the recipient of the precept for supervisory control to be organised or for commencement of disciplinary proceedings against an official.

(2) A person exercising supervisory control or a person with the right to commence disciplinary proceedings is required to review an application within one month as of receipt thereof and submit a reasoned opinion to the Estonian Data Protection Inspectorate. Upon supervisory control or commencement of disciplinary proceedings, the person exercising supervisory control or the person with the right to commence disciplinary proceedings is required to immediately notify the Estonian Data Protection Inspectorate of the results of relevant proceedings.

(3) If a state agency who is the processor of personal data fails to comply with the precept of the Estonian Data Protection Inspectorate within the term specified therein, the Estonian Data Protection

Inspectorate shall file a protest with an administrative court pursuant to procedure provided for in the Code of Administrative Court Procedure.

§60. Non-compliance levy rate

Upon failure to comply with a precept of the Estonian Data Protection Inspectorate, the actual upper limit of the non-compliance levy applicable pursuant to the procedure provided for in the Substitutional Performance and Non-Compliance Levies Act is up to 20,000,000 euros, or in the case of undertakings up to 4 per cent of the total global annual turnover of the undertaking for the previous financial year, whichever amount is the higher.

§61. Term for review of complaints

(1) The Estonian Data Protection Inspectorate shall settle a complaint within 30 days after the date of filing the complaint with the Estonian Data Protection Inspectorate.

(2) The Estonian Data Protection Inspectorate may extend the term for review of a complaint by up to 60 days in order to additionally clarify circumstances relevant to the settling of the complaint. A person filing the complaint shall be notified of extension of the term in writing.

(3) If co-operation with other relevant supervisory authorities is necessary for settlement of the complaint, review of the complaint shall be extended by a reasonable time period which is necessary to hear the cooperating other supervisory authorities or to state its opinion.

Chapter 6

LIABILITY

§62. Violation of obligations of controller and processor

(1) Violation of the obligations of controllers and processors provided for in Articles 8, 11, 25-39, 42 and 43 of Regulation (EU) No 2016/679 of the European Parliament and of the Council

is punishable by a fine of up to 10,000,000 euros.

(2) The same act, if committed by a legal entity,

is punishable by a fine of up to 10,000,000 euros or up to 2 per cent of its total global annual turnover for the previous financial year, whichever amount is the higher.

§63. Violation of certification procedure

(1) Violation of the certification procedure provided for in Articles 42 and 43 of Regulation (EU) No 2016/679 of the European Parliament and of the Council

is punishable by a fine of up to 10,000,000 euros.

(2) The same act, if committed by a legal entity,

is punishable by a fine of up to 10,000,000 euros or up to 2 per cent of its total global annual turnover for the previous financial year, whichever amount is the higher.

§64. Violation of procedure for supervision over compliance with code of conduct

(1) Violation of the procedure for supervision over compliance with the code of conduct provided for in Article 41(4) of Regulation (EU) No 2016/679 of the European Parliament and of the Council

is punishable by a fine of up to 10,000,000 euros.

(2) The same act, if committed by a legal entity,

is punishable by a fine of up to 10,000,000 euros or up to 2 per cent of its total global annual turnover for the previous financial year, whichever amount is the higher.

§65. Violation of personal data processing principles

(1) Violation of the principles of processing personal data provided for in Article 5 of Regulation (EU) 2016/679 of the European Parliament and Council, and violation of the procedure for giving the data subject's consent provided for in Articles 5-7 and 9 of the same Regulation

is punishable by a fine of up to 20,000,000 euros.

(2) The same act, if committed by a legal entity,

is punishable by a fine of up to 20,000,000 euros or up to 4 per cent of its total global annual turnover for the previous financial year, whichever amount is the higher.

§66. Violation of data subject's rights

(1) Violation of the rights of a data subject provided for in Articles 12-22 of Regulation (EU) No. 2016/679 of the European Parliament and of the Council

is punishable by a fine of up to 20,000,000 euros.

(2) The same act, if committed by a legal entity,

is punishable by a fine of up to 20,000,000 euros or up to 4 per cent of its total global annual turnover for the previous financial year, whichever amount is the higher.

§67. Violation of procedure for transmission of personal data

(1) Violation of the procedure for transmission of personal data provided for in Articles 44-49 of Regulation (EU) No. 2016/679 of the European Parliament and of the Council

is punishable by a fine of up to 20,000,000 euros.

(2) The same act, if committed by a legal entity,

is punishable by a fine of up to 20,000,000 euros or up to 4 per cent of its total global annual turnover for the previous financial year, whichever amount is the higher.

§68. Violation of procedure established for specific principles of personal data processing

(1) Violation of the procedure established for specific principles of personal data processing provided for in Chapter 2 of this Act is punishable by a fine of up to 20,000,000 euros.

(2) The same act, if committed by a legal entity, is punishable by a fine of up to 20,000,000 euros or up to 4 per cent of its total global annual turnover for the previous financial year, whichever amount is the higher.

§69. Failure to comply with orders of Estonian Data Protection Inspectorate

(1) Failure to comply with the order provided for in Article 58(2) of Regulation (EU) No 2016/679 of the European Parliament and of the Council

is punishable by a fine of up to 20,000,000 euros.

(2) The same act, if committed by a legal entity,

is punishable by a fine of up to 20,000,000 euros or up to 4 per cent of its total global annual turnover for the previous financial year, whichever amount is the higher.

§70. Violation of granting access to Estonian Data Protection Inspectorate

(1) Failure to comply with the order issued based on the investigative powers provided for in Article 58(1) of Regulation (EU) 2016/679 of the European Parliament and Council, if the Estonian Data Protection Inspectorate is thereby refused access to personal data, other information or premises, is punishable by a fine of up to 20,000,000 euros.

(2) The same act, if committed by a legal entity,

is punishable by a fine of up to 20,000,000 euros or up to 4 per cent of its total global annual turnover for the previous financial year, whichever amount is the higher.

§71. Illegal processing of personal data outside performance of employment or service duties

Illegal collection, viewing, reading, use of personal data, enabling access thereto or making inquiries or extracts thereof by any person who has access to personal data based on his or her employment or service duties, if this does not involve the necessary elements of an offence provided for in §§157 and 1571 of the Penal Code, is punishable by a fine of up to 200 fine units.

§72. Violation of other personal data processing requirements

Violation of personal data protection requirements, if this does not involve the necessary elements of an offence provided for in §§62-71 of this Act and §§157 and 1571 of the Penal Code, is punishable by a fine of up to 200 fine units.

§73. Proceedings

The Estonian Data Protection Inspectorate is the extra-judicial body which conducts proceedings in misdemeanour proceedings provided for in this section.

Chapter 7 IMPLEMENTING PROVISIONS

§74. Register of processors of personal data and persons responsible for protection of personal data

(1) The data of the register of processors of personal data and persons responsible for protection of personal data shall be retained in archived form for the term of up to five years after entry into force of this Act. Upon expiry of the term, the registry data shall be erased.

(2) In order to access the registry data, an application shall be filed with the Estonian Data Protection Inspectorate.

(3) A register entry concerning processing of sensitive personal data is informative until the initial expiry date specified for it.

§75. Repeal of Personal Data Protection Act

The Personal Data Protection Act (RT I 2007, 24, 127) is repealed.

§76. Entry into force of Act

This Act enters into force on 15 January 2019.

* Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of

criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 04.05.2016, pp. 89-131).

Eiki Nestor

President of the Riigikogu

Çin - Personal Information Protection Law of the People's Republic of China

Personal Information Protection Law of the People's Republic of China

(Adopted at the 30th Meeting of the Standing Committee of the Thirteenth National People's Congress on August 20, 2021)

Contents

Chapter I - General Provisions

Chapter II - Personal Information Processing Rules

Section 1 - General Rules

Section 2 - Rules on Processing Sensitive Personal Information

Section 3 - Special Provisions on the Processing of Personal Information by State Organs

Chapter III - Rules on Provision of Personal Information Across Border

Chapter IV - Individuals' Rights in Personal Information Processing Activities

Chapter V - Obligations of Personal Information Processors

Chapter VI - Departments with Personal Information Protection Duties

Chapter VII - Legal Liability

Chapter VIII - Supplementary Provisions

Chapter I

General Provisions

Article 1

This Law is enacted in accordance with the Constitution for the purposes of protecting the rights and interests on personal information, regulating personal information processing activities, and promoting reasonable use of personal information.

Article 2

The personal information of natural persons shall be protected by law. No organization or individual may infringe upon natural persons' rights and interests on their personal information.

Article 3

This Law shall apply to the processing of personal information of natural persons within the territory of the People's Republic of China.

This Law shall also apply to the processing outside the territory of the People's Republic of China of the personal information of natural persons within the territory of the People's Republic of China, under any of the following circumstances:

- (1) for the purpose of providing products or services for natural persons inside the People's Republic of China;
- (2) analyzing or evaluating the behaviors of natural persons within the territory of the People's Republic of China; and
- (3) any other circumstance as provided by any law or administrative regulation.

Article 4

"Personal information" refers to various information related to an identified or identifiable natural person recorded electronically or by other means, but does not include anonymized information.

Personal information processing includes personal information collection, storage, use, processing, transmission, provision, disclosure and deletion, among others.

Article 5

Personal information shall be processed according to law when it is necessary, with justified reason, and in good faith, and the processing may not involve misguidance, fraud, coercion, and the like.

Article 6

Personal information processing shall be based on explicit and reasonable purposes and directly related to those purposes, and shall exert the minimum impacts on the rights and interests of individuals.

The collection of personal information shall be limited to the minimum scope required by the purpose of processing, and personal information may not be collected excessively.

Article 7

The principles of openness and transparency shall be observed in the processing of personal information, the rules for processing personal information shall be disclosed, and the purposes, means, and scope of processing shall be explicitly indicated.

Article 8

The quality of personal information shall be guaranteed in personal information processing, to avoid adverse impacts on the rights and interests of individuals caused by inaccurate and incomplete personal information.

Article 9

Personal information processors shall be responsible for their personal information processing activities and take necessary measures to ensure the security of the personal information they process.

Article 10

No organization or individual shall illegally collect, use, process, or transmit the personal information of other persons, or illegally trade, provide or disclose the personal information of other persons, or engage in personal information processing activities that endanger national security or harm public interests.

Article 11

The state shall establish and improve the personal information protection system to prevent and punish infringements upon the rights and interests on personal information, strengthen publicity and education on personal information protection, and promote a favorable environment for the government, enterprises, relevant industry organizations, and the public to jointly participate in personal information protection.

Article 12

The state will actively engage in the development of international rules on personal information protection, promote the international exchanges and cooperation in personal information protection, and encourage the mutual recognition of personal information protection rules and standards, among others, with other countries, regions, and international organizations.

Chapter II

Personal Information Processing Rules

Section 1

General Rules

Article 13

A personal information processor can process personal information of an individual only if one of the following circumstances exists:

- (1) the individual's consent has been obtained;
- (2) the processing is necessary for the conclusion or performance of a contract in which the individual is a party, or necessary for human resources management in accordance with the labor rules and regulations established in accordance with the law and the collective contracts signed in accordance with the law;
- (3) the processing is necessary for the performance of statutory duties or obligations;
- (4) the processing is necessary for the response to public health emergencies, or for the protection of life, health, and property safety of natural persons in emergencies;
- (5) the personal information is reasonably processed for news reporting, media supervision, and other activities conducted in the public interest;
- (6) the personal information disclosed by the individual himself or other legally disclosed personal information of the individual is reasonably processed in accordance with this Law; and
- (7) other circumstances as provided by laws or administrative regulations.

Individual consent shall be obtained for processing personal information if any other relevant provisions of this Law so provide, except under the circumstances specified in Subparagraphs (2) to (7) of the preceding paragraph.

Article 14

Where personal information processing is based on individual consent, the individual consent shall be voluntary, explicit, and fully informed. Where any other law or administrative regulation provides that an individual's separate consent or written consent must be obtained for processing personal information, such provisions shall apply.

In the case of any change of the purposes or means of personal information processing, or the category of processed personal information, a new consent shall be obtained from the individual.

Article 15

Where personal information processing is based on individual consent, an individual shall have the right to withdraw his consent. Personal information processors shall provide convenient ways for individuals to withdraw their consents.

The withdrawal of consent shall not affect the validity of the processing activities conducted based on consent before it is withdrawn.

Article 16

A personal information processor shall not refuse to provide products or services for an individual on the grounds that the individual withholds his consent for the processing of his personal information or has withdrawn his consent for the processing of personal information, except where the processing of personal information is necessary for the provision of products or services.

Article 17

A personal information processor shall, before processing personal information, truthfully, accurately and fully inform an individual of the following matters in a easy-to-notice manner and in clear and easy-to-understand language:

- (1) the name and contact information of the personal information processor;
- (2) the purposes and means of personal information processing, and the categories and storage periods of the personal information to be processed;
- (3) the methods and procedures for the individual to exercise his rights as provided in this Law; and
- (4) other matters that the individual should be notified of as provided by laws and administrative regulations.

Where any matter as set forth in the preceding paragraph changes, the individual shall be informed of the change.

Where the personal information processor informs an individual of the matters specified in the first paragraph by formulating personal information processing rules, the processing rules shall be made public and be easy to consult and save.

Article 18

When processing personal information, personal information processors are permitted not to inform individuals of the matters specified in the first paragraph of the preceding article where laws or administrative regulations require confidentiality or provide no requirement for such notification.

Where it is impossible to notify individuals in a timely manner in a bid to protect natural persons' life, health and property safety in case of emergency, the personal information processors shall notify them without delay after the emergency is removed.

Article 19

Except as otherwise provided by laws and administrative regulations, the storage period of personal information shall be the minimum time necessary to achieve the purpose of processing.

Article 20

Where two or more personal information processors jointly determine the purposes and means of processing certain personal information, they shall reach an agreement on their respective rights and obligations in processing the personal information. However, this agreement shall not affect an individual's request to any one of them to exercise his rights as provided in this Law.

Where, in jointly processing certain personal information, a processor infringes the rights and interests on personal information and causes damages, other personal information processors shall bear joint and several liability in accordance with law.

Article 21

A personal information processor entrusting the processing of certain personal information to a party shall reach an agreement with the entrusted party on the purposes, period and means of processing, the categories of personal information to be processed and the protection measures, as well as the rights and obligations of both parties, among others, and shall supervise the personal information processing activities of the entrusted party.

The entrusted party shall process personal information in accordance with the agreement and may not process personal information beyond the purposes, means and other conditions as agreed upon. Where the entrustment contract has not taken effect, or is invalid, or is revoked or terminated, the entrusted party shall return the personal information in question to the personal information processor or delete it and shall not retain the personal information.

Without the consent of the personal information processor, the entrusted party may not sub-contract the processing of personal information to any other party.

Article 22

Where a personal information processor needs to transfer personal information due to a merger, division, dissolution, or bankruptcy or for other reasons, the processor shall inform the individuals of

the name and contact information of the recipient of the transferred personal information. The recipient shall continue to perform the obligations of the said personal information processor. Any change of the original purposes or means of processing by the recipient shall be subject to individual consent in accordance with this Law.

Article 23

To provide personal information for any other processor, a personal information processor shall inform the individuals of the recipient's name and contact information, the purposes and means of processing and the categories of personal information to be processed, and shall obtain the individuals' separate consent. The recipient shall process personal information within the scope of the purposes, means, and categories of personal information mentioned above. Any change of the purposes or means of processing by the recipient shall be subject to individual consent in accordance with this Law.

Article 24

Personal information processors using personal information for automated decision making shall ensure the transparency of the decision making and the fairness and impartiality of the results, and may not apply unreasonable differential treatment to individuals in terms of transaction prices and other transaction conditions.

Information push and commercial marketing to individuals based on automated decision making shall be simultaneously accompanied by options not specific to their personal characteristics or with convenient means for individuals to refuse.

Where a decision that may have a significant impact on an individual's rights and interests is made through automated decision making, the individual shall have the right to request clarification from the personal information processor and the right to refuse the processor for making the decision only through automated decision making.

Article 25

Personal information processors shall not disclose the personal information they process, except where separate consents has been obtained from the individuals.

Article 26

Image collection and personal identification equipment in public places shall be installed only when it is necessary for the purpose of maintaining public security, and shall be installed in compliance

with the relevant provisions of the state and with prominent reminders. The personal images and identification information collected can only be used for the purpose of maintaining public security and, unless the individuals' separate consents are obtained, shall not be used for any other purpose.

Article 27

A personal information processor may reasonably process the personal information disclosed by an individual himself or other legally disclosed personal information, except where the individual expressly refuses. Where the processing of disclosed personal information may have a significant impact on an individual's rights and interests, the personal information processors shall first obtain the individual's consent in accordance with the provisions of this Law.

Section 2

Rules on Processing Sensitive Personal Information

Article 28

"Sensitive personal information" is personal information that once leaked or illegally used, may easily lead to the infringement of the personal dignity of a natural person or may endanger his personal safety or property, including information such as biometrics, religious belief, specific identity, medical health status, financial accounts, and the person's whereabouts, as well as the personal information of a minor under the age of 14 years.

Personal information processors can process sensitive personal information only when there is a specific purpose and when it is of necessity, under the circumstance where strict protective measures are taken.

Article 29

For the processing of sensitive personal information, individual's separate consent shall be obtained. Where other laws or administrative regulations provide that written consent shall be obtained for the processing of sensitive personal information, such provisions shall prevail.

Article 30

In addition to the matters specified in the first paragraph of Article 17 of this Law, a processor processing sensitive personal information shall notify an individual of the necessity of processing his sensitive personal information and the impact it has on his rights and interests, except where such notification is not required in accordance with the provisions of this Law.

Article 31

To process the personal information of minors under the age of 14, personal information processors shall obtain the consent of the parents or other guardians of the minors.

Personal information processors processing the personal information of minors under the age of 14 shall develop special rules for processing such personal information.

Article 32

Where other laws or administrative regulations provide that relevant administrative permit shall be obtained for the processing of sensitive personal information or impose other restrictions, such provisions shall prevail.

Section 3

Special Provisions on the Processing of Personal Information by State Organs

Article 33

This Law shall apply to the processing of personal information by state organs; where there are special provisions in this Section, the provisions of this Section shall prevail.

Article 34

When state organs process personal information in order to perform their statutory duties, they shall act in accordance with the authority and procedures prescribed by laws and administrative regulations, and shall not exceed the scope and limits necessary to perform their statutory duties.

Article 35

When state organs process personal information in order to perform their statutory duties, they shall fulfill the obligation of notification in accordance with the provisions of this Law, except under the circumstances specified in the first paragraph of Article 18 of this Law or where notification will hinder the state organs from performing their statutory duties.

Article 36

Personal information processed by state organs shall be stored within the territory of the People's Republic of China. A security assessment shall be conducted where it is truly necessary to provide such information for any party outside of the territory of the People's Republic of China. In the security assessment the relevant departments shall provide support and assistance if so requested.

Article 37

Where organizations authorized by laws or regulations with the function of administering public affairs process personal information in order to fulfill their statutory duties, the provisions herein on the processing of personal information by state organs shall apply.

Chapter III

Rules on Provision of Personal Information Across Border

Article 38

A personal information processor that truly needs to provide personal information for a party outside the territory of the People's Republic of China for business sake or other reasons, shall meet one of the following requirements:

- (1) passing the security assessment organized by the national cyberspace department in accordance with Article 40 of this Law;
- (2) obtaining personal information protection certification from the relevant specialized institution according to the provisions issued by the national cyberspace department;
- (3) concluding a contract stipulating both parties' rights and obligations with the overseas recipient in accordance with the standard contract formulated by the national cyberspace department; and
- (4) meeting other conditions set forth by laws and administrative regulations and by the national cyberspace department.

Where an international treaty or agreement that the People's Republic of China has concluded or acceded to stipulates conditions for providing personal information for a party outside the territory of the People's Republic of China, such stipulations may be followed.

The personal information processor shall take necessary measures to ensure that the personal information processing activities of the overseas recipient meet the personal information protection standards set forth in this Law.

Article 39

Where a personal information processor provides personal information for any party outside the territory of the People's Republic of China, the processor shall inform the individuals of the overseas recipient's name and contact information, the purposes and means of processing, the categories of personal information to be processed, as well as the methods and procedures for the individuals to exercise their rights as provided in this Law over the overseas recipient, etc., and shall obtain individual's separate consent.

Article 40

Critical information infrastructure operators and the personal information processors that process personal information up to the amount prescribed by the national cyberspace department shall store domestically the personal information collected and generated within the territory of the People's Republic of China. Where it is truly necessary to provide the information for a party outside the territory of the People's Republic of China, the matter shall be subjected to security assessment organized by the national cyberspace department. Where laws, administrative regulations, or the provisions issued by the national cyberspace department provide that security assessment is not necessary, such provisions shall prevail.

Article 41

The competent authorities of the People's Republic of China shall handle foreign judicial or law enforcement authorities' requests for personal information stored within China in accordance with relevant laws and the international treaties and agreements concluded or acceded to by the People's Republic of China, or under the principle of equality and reciprocity. Without the approval of the competent authorities of the People's Republic of China, no organization or individual shall provide data stored in the territory of the People's Republic of China for any foreign judicial or law enforcement authority.

Article 42

Where overseas organizations or individuals engage in personal information processing activities, which infringe upon the rights and interests of citizens of the People's Republic of China on personal information or endanger the national security or public interests of the People's Republic of China, the national cyberspace department may include them in a list of restricted or prohibited recipients of personal information, publicize the list, and take measures such as restricting or prohibiting the provision of personal information for such organizations and individuals.

Article 43

Where any country or region adopts any prohibitive, restrictive or other similar discriminatory measures against the People's Republic of China in terms of personal information protection, the People's Republic of China may take countermeasures against the aforesaid country or region based on actual situations.

Chapter IV

Individuals' Rights in Personal Information Processing Activities

Article 44

Individuals shall have the right to be informed, the right to make decisions on the processing of their personal information, and the right to restrict or refuse the processing of their personal information by others, except as otherwise provided by laws or administrative regulations.

Article 45

Individuals shall have the right to consult and duplicate their personal information from personal information processors, except under circumstances as set out in the first paragraph of Article 18 and Article 35 of this Law.

Where an individual requests the consultation or duplication of his personal information, the requested personal information processor shall provide such information in a timely manner.

Where an individual requests the transfer of his personal information to a designated personal information processor, which meets the requirements of national cyberspace department for transferring personal information, the requested personal information processor shall provide means for the transfer.

Article 46

Where an individual discovers that his personal information is incorrect or incomplete, he shall have the right to request the personal information processors to rectify or supplement relevant information.

Where an individual requests the rectification or supplementation of his personal information, the personal information processors shall verify the information in question, and make rectification or supplementation in a timely manner.

Article 47

In any of the following circumstances, a personal information processor shall take the initiative to erase personal information, and an individual has the right to request the deletion of his personal information if the personal information processor fails to erase the information:

- (1) the purposes of processing have been achieved or cannot be achieved, or such information is no longer necessary for achieving the purposes of processing;
- (2) the personal information processor ceases to provide products or services, or the storage period has expired;

- (3) the individual withdraws his consent;
- (4) the personal information processor processes personal information in violation of laws, administrative regulations, or agreements; or
- (5) other circumstances as provided by laws and administrative regulations.

Where the storage period provided by any law or administrative regulation has not expired, or it is difficult to erase personal information technically, the personal information processor shall cease the processing of personal information other than storing and taking necessary security protection measures for such information.

Article 48

An individual has the right to request a personal information processor to interpret the personal information processing rules developed by the latter.

Article 49

The close relatives of a deceased natural person may, for their own legal and legitimate interests, exercise the rights to handle the personal information of the deceased, such as consultation, duplication, rectification, and deletion, as provided in this Chapter, except as otherwise arranged by the deceased before death.

Article 50

A personal information processor shall establish the mechanism for receiving and handling individuals' requests for exercising their rights. Where an individual's request is rejected, the reasons therefor shall be given.

Where an individual's request to exercise his rights is rejected by a personal information processor, the individual may file a lawsuit with the people's court in accordance with the law.

Chapter V

Obligations of Personal Information Processors

Article 51

Personal information processors shall take the following measures to ensure that their personal information processing activities are in compliance with laws and administrative regulations based on the purpose and means of processing, the categories of personal information to be processed, the

impact on personal rights and interests, and the potential security risks, among others, and shall prevent unauthorized access to, as well as breach, tampering or loss of any personal information:

- (1) formulating internal management system and operational procedures;
- (2) implementing classified management of personal information;
- (3) adopting corresponding security technical measures such as encryption and de-identification;
- (4) reasonably determining the operational authority of personal information processing, and regularly conducting safety education and training for practitioners;
- (5) formulating contingent plans for personal information security emergencies and organizing the implementation of such plans; and
- (6) other measures as provided by laws and administrative regulations.

Article 52

A personal information processor that processes personal information up to the amount prescribed by the national cyberspace department shall designate a person in charge of personal information protection, who shall supervise the personal information processing activities of the processor as well as the protective measures taken thereby, among others.

The personal information processor shall disclose the contact information of the person in charge of personal information protection, and submit the said person's name, contact information, and other information to the departments with personal information protection duties.

Article 53

Personal information processors outside the territory of the People's Republic of China as specified in the second paragraph of Article 3 of this Law shall set up specialized agencies or designate representatives within the territory of the People's Republic of China to be responsible for handling personal information protection related matters, and shall submit the names, contact information, and other information of the agencies and representatives to the departments with personal information protection duties.

Article 54

Personal information processors shall regularly conduct compliance audits of their personal information processing activities with laws and administrative regulations.

Article 55

In any of the following circumstances, a personal information processor shall assess in advance the impact on personal information protection and keep a record of the course of the processing:

- (1) processing sensitive personal information;
- (2) using personal information to conduct automated decision making;
- (3) entrusting personal information processing to another party, providing personal information for another party, or publicizing personal information;
- (4) providing personal information for any party outside the territory of the People's Republic of China; or
- (5) conducting other personal information processing activities which may have significant impacts on individuals.

Article 56

The assessment of impact on personal information protection shall include the following contents:

- (1) whether the purposes and means of personal information processing, are legitimate, justified and necessary;
- (2) the impact on individuals' rights and interests, and security risks; and
- (3) whether the protection measures taken are legitimate, effective, and compatible with the degree of risks.

The report of the impact assessment on personal information protection and the processing record shall be retained for at least three years.

Article 57

Where the breach, tampering, or loss of personal information occurs or may occur, a personal information processor shall immediately take remedial measures and notify the departments with personal information protection duties and the relevant individuals. The notice shall include the following items:

- (1) the categories of personal information that has been or may be breached, tampered with or lost, and the reasons and possible harm of the breach, tampering and loss;
- (2) the remedial measures adopted by the personal information processor and the measures the individuals may take to mitigate the harm; and
- (3) the contact information of the personal information processor.

Where the measures taken by the personal information processor can effectively avoid the harm caused by breach, tampering, or loss of personal information, the personal information processor is not required to notify individuals; where the departments with personal information protection duties consider that harm may be caused, they have the authority to request the personal information processor to notify individuals.

Article 58

A personal information processor that provides important internet platform services involving a huge number of users and complicated business types shall perform the following obligations:

- (1) establishing and improving the personal information protection compliance system in accordance with the provisions of the state and establishing an independent organization mainly composed of external members to supervise the protection of personal information;
- (2) following the principles of openness, fairness, and justice, formulating platform rules, and clarifying the norms and obligations that product or service providers within the platform should meet when processing personal information;
- (3) stopping providing services for product or service providers within the platforms that process personal information in serious violation of laws and administrative regulations; and
- (4) regularly publishing social responsibility reports on personal information protection for public supervision.

Article 59

The party entrusted with the processing of personal information shall, in accordance with this Law and relevant laws and administrative regulations, take the necessary measures to ensure the security of the personal information entrusted for processing, and assist the entrusting personal information processor in fulfilling the obligations provided by this Law.

Chapter VI

Departments with Personal Information Protection Duties

Article 60

The national cyberspace department shall be responsible for the overall planning and coordination of personal information protection and related supervision and administration. The relevant departments of the State Council shall, in accordance with this Law and other relevant laws and

administrative regulations, be responsible for personal information protection and related supervision and administration within the scope of their respective duties.

The duties of personal information protection and related supervision and administration of the relevant departments of the local people's governments at or above the county level shall be determined in accordance with the relevant provisions of the state.

The departments provided in the preceding two paragraphs are collectively referred to as the departments with personal information protection duties.

Article 61

Departments with personal information protection duties shall perform the following personal information protection duties:

- (1) conducting publicity and education on personal information protection, and guiding and supervising personal information processors in their protection of personal information;
- (2) receiving and handling complaints and reports related to personal information protection;
- (3) organizing evaluations on applications, etc. in terms of personal information protection and publish the results of such evaluations;
- (4) investigating and handling illegal personal information processing activities; and
- (5) other duties as provided by laws and administrative regulations.

Article 62

The national cyberspace department shall coordinate relevant departments to promote personal information protection through the following efforts in accordance with this Law:

- (1) formulating specific rules and standards for personal information protection;
- (2) developing special personal information protection rules and standards for small personal information processors, the processing of sensitive personal information, and new technologies and applications such as face recognition and artificial intelligence;
- (3) supporting the research and development, and promoting the application of secure and convenient electronic identity authentication technology, and advancing the public services for network identity authentication;

(4) promoting the development of a personal information protection service system with the participation of various social sectors, and supporting relevant institutions in providing personal information protection assessment and certification services; and

(5) improving the complaint and reporting mechanism related to personal information protection.

Article 63

A department with personal information protection duties when fulfilling related duties may take the following measures:

(1) questioning relevant parties, and investigating circumstances related to personal information processing activities;

(2) consulting and duplicating the parties' contracts, records, account books and other relevant materials related to personal information processing activities;

(3) conducting on-site inspections, and investigating suspected illegal personal information processing activities; and

(4) inspecting equipment and articles related to personal information processing activities; and sealing up or seizing equipment and articles related to illegal personal information processing activities as proved by evidence after submitting written reports to and obtaining approval from the principal person in charge of the departments with personal information protection duties.

When departments with personal information protection duties carry out their duties in accordance with the law, the parties concerned shall cooperate and provide assistance, and shall not reject or obstruct them.

Article 64

Where a department with personal information protection duties finds, when performing its duties, relatively high risks in personal information processing activities or the occurrence of personal information security incidents, the department may hold an interview with the legal representative or the principal person in charge of the personal information processor according to the provided authority and procedures, or request the processor to entrust a professional institution to conduct compliance audits of the personal information processing activities. The personal information processor shall adopt measures to make rectification and eliminate potential risks as required.

Where a department with personal information protection duties, in performing its duties, finds an illegal personal information processing activity that may involve a crime, the department shall transfer the case to the public security organ in a timely manner in accordance with the law.

Article 65

Any organization or individual has the right to complain and report to a department with personal information protection duties about illegal personal information processing. The department that receives such a complaint or report shall handle it in a timely manner in accordance with the law, and notify the complainant or informant of the results.

Departments with personal information protection duties shall publish their contact information for receiving complaints and reports.

Chapter VII

Legal Liability

Article 66

Where personal information is processed in violation of the provisions of this Law or without fulfilling the personal information protection obligations provided in this Law, the departments with personal information protection duties shall order the violator to make corrections, give a warning, confiscate the illegal gains, and order the suspension or termination of provision of services by the applications that illegally process personal information; where the violator refuses to make corrections, a fine of not more than RMB one million yuan shall be imposed thereupon; and the directly liable persons in charge and other directly liable persons shall each be fined not less than RMB 10,000 yuan nor more than RMB 100,000 yuan.

In case of an illegal act as prescribed in the preceding paragraph and the circumstances are serious, the departments with personal information protection duties at or above the provincial level shall order the violator to make corrections, confiscate the illegal gains, impose a fine of not more than RMB 50 million yuan or not more than five percent of the previous year's turnover; may also order the suspension of relevant businesses, or order the suspension of all the business operations for an overhaul, and notify the competent authorities to revoke relevant business permits or license; shall impose a fine of not less than RMB 100,000 yuan but not more than RMB 1 million yuan upon each of the directly liable persons in charge and other directly liable persons, and may decide to prohibit the abovementioned persons from serving as directors, supervisors, senior managers, or the persons in charge of relevant companies within a specific period of time.

Article 67

Any violation of the provisions of this Law shall be entered in the relevant credit record and be published in accordance with the provisions of the relevant laws and administrative regulations.

Article 68

Where any state organ fails to fulfill the personal information protection obligations as provided in this Law, the organ at the higher level or the departments with personal information protection duties shall order it to make corrections, and discipline the directly liable person in charge and other directly liable persons in accordance with the law.

Where a staff member of a department with personal information protection duties neglects duties, abuses power, or practices favoritism, which does not constitute a crime, the staff member shall be subject to sanction in accordance with the law.

Article 69

Where a personal information processor infringes the rights or interests on personal information due to any personal information processing activity and cannot prove that the processor is not at fault, the processor shall assume the liability for damages and other tort liability.

The liability for damages prescribed in the preceding paragraph shall be determined based on the losses of individuals incurred thereby and the benefits acquired by the infringing personal information processor; and where it is difficult to determine the aforementioned losses or the benefits, the amount of damages shall be determined based on the actual circumstances.

Article 70

Where a personal information processor processes personal information in violation of the provisions of this Law and infringes the rights and interests of many individuals, the people's procuratorate, the consumer organizations specified by law, and the organization designated by the national cyberspace department may file a lawsuit with the people's court in accordance with the law.

Article 71

Any violation of this Law which constitutes a violation of public security administration shall be subject to public security administration penalty in accordance with the law. If the violation constitutes a crime, the violator shall be held criminally liable in accordance with the law.

Chapter VIII

Supplementary Provisions

Article 72

This Law is not applicable where a natural person processes personal information for personal or household affairs.

Where other laws provide personal information processing in statistical or archives management activities organized and conducted by the people's governments at all levels and their relevant departments, the provisions of such laws shall prevail.

Article 73

For purposes of this Law, the following terms shall have the following meanings:

- (1) "A personal information processor" refers to an organization or individual that autonomously determines the purposes and means of personal information processing.
- (2) "automated decision making" refers to the activities of automatically analyzing and evaluating personal behaviors, hobbies, or economic, health, and credit status, among others, through computer programs, and making decisions.
- (3) "de-identification" refers to processing personal information to make it impossible to identify specific natural persons in the absence of the support of additional information.
- (4) "anonymization" refers to the process of processing personal information to make it impossible to identify specific natural persons and impossible to restore.

Article 74

This Law shall come into force as of November 1st , 2021.

Çin - Data Security Law of the People's Republic of China

Data Security Law of the People's Republic of China

No. 84

The Data Security Law of the People's Republic of China, adopted at the 29th Meeting of the Standing Committee of the Thirteenth National People's Congress of the People's Republic of China on June 10, 2021, is hereby promulgated, and shall go into effect on September 1, 2021.

Xi Jinping

President of the People's Republic of China

June 10, 2021

Data Security Law of the People's Republic of China

(Adopted at the 29th Meeting of the Standing Committee of the Thirteenth National People's Congress on June 10, 2021)

Contents

Chapter I - General Provisions

Chapter II - Data Security and Development

Chapter III - Data Security Systems

Chapter IV - Data Security Protection Obligations

Chapter V - Security and Openness of Government Data

Chapter VI - Legal Liability

Chapter VII - Supplementary Provisions

Chapter I

General Provisions

Article 1

This Law is enacted for the purpose of regulating data processing, ensuring data security, promoting development and utilization of data, protecting the lawful rights and interests of individuals and organizations, and safeguarding the sovereignty, security, and development interests of the state.

Article 2

This Law shall apply to data processing activities and security supervision and regulation of such activities within the territory of the People's Republic of China.

Where data processing outside the territory of People's Republic of China harms the national security, public interests, or the lawful rights and interests of individuals or organizations of the People's Republic of China, legal liability shall be investigated in accordance with the law.

Article 3

For the purpose of this Law, the term "data" refers to any record of information in electronic or any other form.

"Data processing" includes the collection, storage, use, processing, transmission, provision, and disclosure of data, among others.

"Data security" refers to ensuring that data is effectively protected and lawfully used through adopting necessary measures, and to possessing the capacity to guarantee the continuous security of data.

Article 4

In preserving data security, the holistic approach to national security shall be adopted, sound data security governance systems shall be established, and data security and protection capabilities shall be improved.

Article 5

The central leading authority for national security shall be responsible for the decision-making, deliberation and coordination of the national data security work; researching, formulating, and guiding the implementation of the national data security strategy and related major guidelines and policies; coordinating major matters and important work in respect of national data security; and establishing a coordination mechanism for national data security.

Article 6

All localities and departments shall bear responsibility for the management of the data collected or generated in their work as well as for the data security thereof.

The competent departments of industry, telecommunications, transport, finance, natural resources, health, education, technology and other relevant competent departments shall assume the responsibilities of supervising and regulating data security in their respective trades and sectors.

Public security organs and national security organs, etc. shall assume the responsibilities of supervising and regulating data security within the scopes of their respective duties in accordance with the provisions of this Law and other relevant laws and administrative regulations.

The national cyberspace affairs department shall be in charge of the overall planning and coordination of network data security and the related supervision and regulation in accordance with the provisions of this Law and other relevant laws and administrative regulations.

Article 7

The state shall protect the data-related rights and interests of individuals and organizations, encourage the lawful, reasonable, and effective use of data, ensure free flow of data in an orderly manner and in accordance with the law, and promote the development of a digital economy with data as the key factor.

Article 8

Whoever processes data shall observe laws and regulations, respect social morality and ethics, observe business and professional ethics, uphold honesty and trustworthiness, fulfill data security protection obligations, and undertake social responsibilities; and shall not endanger national security and public interests, nor harm the lawful rights and interests of individuals and organizations.

Article 9

The state supports the dissemination and popularization of knowledge of data security to raise public awareness in this regard and ability to protect data security, and promotes the joint participation by relevant departments, industry organizations, research institutions, enterprises, and individuals in data security protection, so as to create a good environment for members of the whole society to jointly protect data, ensure data security and promote development of relevant industries.

Article 10

Relevant industry associations shall, in accordance with their articles of association, formulate the code of conduct and standards to ensure data security according to the law, strengthen self-regulation

in their respective industries, guide members to strengthen data security protection, improve their protection level and promote the healthy development of the industries.

Article 11

The state shall actively carry out international exchanges and cooperation in fields such as data security governance and data development and utilization, participate in the formulation of relevant international rules and standards for data security, and promote the safe and free flow of data across borders.

Article 12

Any individual or organization shall have the right to file complaints about or report violations of this Law to the competent departments. The departments receiving such complaints or reports shall deal with them in a timely manner in accordance with the law.

The competent departments shall keep confidential the relevant information of those making such complaints or reports, and protect their lawful rights and interests.

Chapter II

Data Security and Development

Article 13

The state shall make an overall plan to coordinate development and security, to promote data security through data development and utilization and through industrial development on one hand, and on the other hand, to ensure that data security facilitates data development and utilization as well as industrial development.

Article 14

The state shall implement the big data strategy, advance the construction of data infrastructure, and encourage and support the innovative application of data in all industries and fields.

People's governments at or above the provincial level shall incorporate the development of digital economy into their national economic and social development plans, and formulate development plans for the digital economy as needed.

Article 15

The state supports development and utilization of data to render public services smarter. In providing smarter public services, the needs of the elderly and the disabled shall be taken into full account to avoid posing obstacles to their daily lives.

Article 16

The state supports research on development and utilization of data and on data security related technologies, encourages popularization and commercial innovation of technologies in the foregoing fields, and fosters and develops products and industrial systems for development and utilization of data and for data security.

Article 17

The state shall advance the forming of the standards for data development and the standards for data utilization technologies and data security. The department in charge of standardization under the State Council and other relevant departments under the State Council shall, within the scopes of their respective duties and functions, organize the establishment of, and make revisions in due time to the standards for technologies and products for data development and data utilization and the standards for data security. The state shall support enterprises, social groups, and education or research institutions, etc. in their participation in the establishment of such standards.

Article 18

The state encourages the development of services such as data security testing, evaluation, and accreditation, and supports agencies specialized in data security testing, evaluation, accreditation, etc. to provide services according to the law.

The state supports collaboration among relevant departments, industry associations, enterprises, education and research institutions, relevant specialized agencies, etc. in the fields such as data security related risk assessment, prevention, and disposal .

Article 19

The state shall establish sound systems for data trading management, standardize data trading activities, and foster a data trading market.

Article 20

The state supports education and research institutions, enterprises, and other entities in carrying out education and training on technologies for data development and utilization and on data security,

cultivates professionals in data development and utilization technologies and in data security by a variety of means, and promotes talent exchanges.

Chapter III

Data Security Systems

Article 21

The state shall establish a categorized and classified system and carry out data protection based on the importance of the data in economic and social development, as well as the extent of harm to national security, public interests, or the lawful rights and interests of individuals or organizations that will be caused once the data are altered, destroyed, leaked, or illegally obtained or used. The coordination mechanism for national data security shall coordinate the relevant departments to formulate a catalog of important data and strengthen protection of important data.

Data concerning national security, lifelines of the national economy, important aspects of people's lives, major public interests, ect., are core data of the state, for which a stricter management system shall be implemented.

All localities and departments shall, in accordance with the categorized and classified data protection system, prepare specific catalogs of important data for their respective regions, departments, and relevant industries and sectors, and give priority to the data listed in the catalogs in terms of data protection.

Article 22

The state shall establish a centralized, unified, highly effective, and authoritative mechanism for assessing, reporting, information sharing, monitoring, and early alert of data security risks. The coordinating mechanism for national data security shall make an overall plan on and coordinate relevant departments in strengthening the work about acquiring, analyzing, researching and evaluating information of data security risks and the work about early alert of such risks.

Article 23

The state shall establish a data security emergency response mechanism. Where a data security incident occurs, the relevant competent departments shall initiate emergency response in accordance with the plan and the law, take corresponding measures to prevent further harm and eliminate security hazards, and send out warnings to the public by publishing information relevant thereto in a timely manner.

Article 24

The state shall establish a review system for data security, conducting national security reviews of data processing that affects or may affect national security.

Security review decisions made in accordance with the law are final decisions.

Article 25

The state shall apply export control in accordance with the law on data that are controlled items and concern national security and interests and the performance of international obligations.

Article 26

Where any country or region adopts discriminatory prohibitions, restrictions, or other similar measures against the People's Republic of China in respect of investment, trade or any other field related to data and data development and utilization technologies, the People's Republic of China may take countermeasures against that country or region in light of the actual circumstances.

Chapter IV

Data Security Protection Obligations

Article 27

In data processing, the laws and regulations shall be complied with, a sound data security management system throughout the whole process shall be established, data security education and training shall be organized and conducted, and corresponding technical measures and other necessary measures shall be adopted to ensure data security. In data processing by making use of the internet or any other information networks, the abovementioned data security obligations shall be fulfilled on the basis of the classified protection system for cyber security.

Processors of important data shall be clear about their persons responsible for data security and the data security management bodies, and fulfill the responsibilities for data security.

Article 28

Data processing as well as research and development of new data technologies shall be conducive to furthering economic and social development, and improving the well-being of people, and shall conform to social morals and ethics.

Article 29

Closer risk monitoring shall be applied in data processing. Where data security defects, bugs, or other risks are discovered, remedial measures shall be taken immediately. Where a data security incident occurs, measures shall be taken immediately to address it, and users shall be notified and reports made to relevant competent departments in a timely manner in accordance with relevant provisions.

Article 30

Processors of important data shall, in accordance with the relevant provisions, conduct risk assessments of their data processing on a regular basis and submit risk assessment reports to relevant competent departments.

Risk assessment reports shall include the types and amounts of important data processed, information on data processing, data security risks and the response measures for them.

Article 31

The provisions of the Cyber Security Law of the People's Republic of China shall apply to the outbound security management of the important data collected or produced by critical information infrastructure operators during their operation within the territory of the People's Republic of China, and the measures for the outbound security management of the important data collected or produced by others data processors during their operation within the territory of the People's Republic of China shall be formulated by the national cyberspace authority in conjunction with the relevant departments under the State Council.

Article 32

An organization or individual shall collect data by lawful and proper means, and shall not acquire data by theft or in other illegal manners.

Where laws or administrative regulations have provisions on the purposes or scopes of data collection and use, data shall be collected and used for the purposes and within the scopes provided for by those laws and administrative regulations.

Article 33

When providing services, data transaction intermediaries shall require data providers to specify the sources of the data, verify the identities of both parties to the transactions, and retain the verification and transaction records.

Article 34

Where laws or administrative regulations require that administrative permissions be acquired for providing services related to data processing, service providers shall obtain such administrative permissions in accordance with these provisions.

Article 35

Where a public security organ or national security organ needs to obtain data for the sake of national security or for investigating crimes in accordance with the law, strict approval formalities shall be completed in accordance with the relevant provisions of the state and data be obtained in accordance with the law, and the relevant organizations and individuals shall cooperate.

Article 36

The competent authorities of the People's Republic of China shall handle requests for data made by foreign judicial or law enforcement authorities, in accordance with the relevant laws and international treaties or agreements concluded or acceded to by the People's Republic of China, or in accordance with the principles of equality and reciprocity. Without the approval of the competent authorities of the People's Republic of China, organizations or individuals in the People's Republic of China shall not provide data stored within the territory of the People's Republic of China to any overseas judicial or law enforcement body.

Chapter V

Security and Openness of Government Data

Article 37

The state shall make great efforts to promote the development of e-government, make government database more scientific, accurate, and time-efficient, and improve the ability of using data to serve economic and social development.

Article 38

Where state organs need to collect or use data to perform their statutory duties, they shall collect or use data within the scope as needed for performance of their statutory duties and under the conditions and procedures provided by laws and administrative regulations. They shall, in accordance with the law, preserve the confidentiality of the data accessed in the course of performing their duties, such as personal privacy, personal information, trade secrets, and confidential business information, and shall not divulge such data or illegally provide them to others.

Article 39

State organs shall, in accordance with the provisions of laws and administrative regulations, establish sound data security management systems, fulfill data security protection responsibilities, and ensure the security of government data.

Article 40

Where a state organ entrusts others to construct or maintain e-government systems, or to store or process government data, the state organ shall go through strict approval procedures, and shall supervise the entrusted party in the performance of data security protection obligations. The entrusted party shall perform its data security protection obligations in accordance with the provisions of laws, regulations, and contracts signed, and shall not retain, use, divulge, or provide others with government data without authorization.

Article 41

State organs shall, under the principles of fairness, equality and convenience for the people, disclose government data in a timely and accurate manner in accordance with the provisions, except those which shall not be disclosed in accordance with the law.

Article 42

The state shall formulate the catalog of open government data, build an open, uniform, standardized, interconnected, safe and controllable government data platform, and promote the release and utilization of government data.

Article 43

The provisions of this Chapter shall apply to the data processing carried out by the organizations with the functions of administering public affairs as authorized by laws and regulations for the purpose of performing their statutory duties.

Chapter VI

Legal Liability

Article 44

Where competent departments discover the existence of major security risks in data processing when they perform their regulatory duties as regards data security, they may, in accordance with the prescribed limits of authority and procedures, conduct regulatory talks with the relevant organizations and/or individuals, and require the relevant organizations and/or individuals to adopt measures to make rectifications and eliminate potential hazards.

Article 45

Where an organization or individual that processes data fails to perform the data security protection obligations provided in Articles 27, 29 and 30 of this Law, the organization or individual shall be ordered to make rectifications and be given a warning, and may be concurrently fined not less than RMB 50,000 yuan but not more than RMB 500,000 yuan by the competent department, and the directly liable persons in charge and other directly liable persons may be fined not less than RMB 10,000 yuan but not more than RMB 100,000 yuan. Where the organization or individual refuses to make rectifications or has caused serious consequences such as a massive data breach, the organization or individual shall be fined not less than RMB 500,000 yuan but not more than RMB 2 million yuan, and may be ordered to suspend the relevant business or suspend operations for rectification, or have relevant business permits or the business license revoked, and the directly liable persons in charge and other directly liable persons shall be fined not less than RMB 50,000 yuan but not more than RMB 200,000 yuan.

Where the organization or individual violates the national core data management rules and endangers national sovereignty, security, or development interests of the state, the competent department shall impose upon the organization or individual a fine of not less than RMB 2 million yuan but not more than RMB 10 million yuan, and may, based on the circumstances, order a suspension of relevant business or a suspension of operations for rectification, or revoke relevant business permits or the business license. Where a crime is constituted, criminal responsibilities shall be investigated in accordance with the law.

Article 46

Whoever, in violation of the provisions of Article 31 of this Law, provides important data abroad, shall be ordered to make rectifications and be given a warning by the competent department, and may be concurrently fined not less than RMB 100,000 yuan but not more than RMB 1 million yuan, and the directly liable persons in charge and other directly liable persons may be fined not less than RMB 10,000 yuan but not more than RMB 100,000 yuan. Where the circumstances are serious, the violator shall be fined not less than RMB 1 million but not more than RMB 10 million yuan, and may also be ordered to suspend the relevant business or suspend operations for rectification, or have relevant business permits or the business license revoked, and the directly liable persons in charge and other directly liable persons shall be fined not less than RMB 100,000 yuan but not more than RMB 1 million yuan.

Article 47

Where a data transaction intermediary fails to perform the obligations prescribed in Article 33 of this Law, it shall be ordered by the competent department to make rectifications, its illegal gains, if any, shall be confiscated, and it shall also be fined not less than the amount of but not more than ten times the amount of the illegal gains; if there are no illegal gains or the illegal gains are less than RMB 100,000 yuan, it shall be fined not less than RMB 100,000 yuan but not more than RMB 1 million yuan. It may be concurrently ordered to suspend the relevant business or suspend operations for rectification, or have relevant business permits or the business license revoked. The directly liable persons in charge and other directly liable persons shall be fined not less than RMB 10,000 yuan but not more than RMB 100,000 yuan.

Article 48

Whoever in violation of Article 35 of this Law, refuses to cooperate when a public organ or national security organ needs to access the data, shall be ordered by the competent department to make rectifications and be given a warning, and shall be concurrently fined not less than RMB 50,000 yuan but nor more than RMB 500,000 yuan, and the directly liable persons in charge and other directly liable persons may be fined not less than RMB 10,000 yuan but not more than RMB 100,000 yuan.

Whoever, in violation of Article 36 of this Law, provides data to an overseas judicial or law enforcement body without the approval of the competent authorities, shall be given a warning by the competent department, and may be concurrently fined not less than RMB 100,000 yuan but not more than RMB 1 million yuan, and the directly liable persons in charge and other directly liable persons may be fined not less than RMB 10,000 yuan but not more than RMB 100,000 yuan. If serious consequences are caused, the violator shall be fined not less than RMB 1 million yuan but not more than RMB 5 million yuan, and may be ordered to suspend the relevant business or suspend operations for rectification, or have relevant business permits or the business license revoked. The directly liable persons in charge and other directly liable persons shall be fined not less than RMB 50,000 yuan but not more than RMB 500,000 yuan.

Article 49

Where a state organ fails to perform data security obligations as provided for in this Law, the directly liable persons in charge and other directly liable persons shall be given a sanction in accordance with the law.

Article 50

Any state functionary performing data security related regulation neglects his duty, abuses power, or engages in malpractice for personal gain, shall be given a sanction in accordance with the law.

Article 51

Whoever obtains data through theft or by any other illegal means, or eliminates or restricts competition in data processing, or harms the lawful rights and interests of individuals or organizations, shall be punished in accordance with the provisions of relevant laws and administrative regulations.

Article 52

Whoever, in violation of this Law, causes damages to others shall bear civil liability in accordance with the law.

Where a violation of the provisions of this Law constitutes a violation of public security administration, a public security administrative penalty shall be given in accordance with the law.

Where a crime is constituted, criminal responsibility shall be investigated in accordance with the law.

Chapter VII

Supplementary Provisions

Article 53

The provisions of the Law of the People's Republic of China on Guarding State Secrets and other relevant laws and administrative regulations shall apply to data processing that involves state secrets.

The provisions of relevant laws and administrative regulations shall also be observed when data are processed in statistical or archival work and in data processing involving personal information.

Article 54

Measures for the military data security and protection shall be separately formulated by the Central Military Commission in accordance with this Law.

Article 55

This Law shall come into force as of September 1, 2021.

Güney Kore - Personal Information Protection Act

PERSONAL INFORMATION PROTECTION ACT

[Enforcement Date 05. Aug, 2020.] [Act No.16930, 04. Feb, 2020., Partial Amendment]

2020.09.14

CHAPTER I GENERAL PROVISIONS

Article 1 (Purpose) The purpose of this Act is to protect the freedom and rights of individuals, and further, to realize the dignity and value of the individuals, by prescribing the processing and protection of personal information. <Amended by Act No. 12504, Mar. 24, 2014>

Article 2 (Definitions) The terms used in this Act shall be defined as follows: <Amended by Act No. 12504, Mar. 24, 2014; Act No. 16930, Feb. 4, 2020>

1. The term "personal information" means any of the following information relating to a living individual:

(a) Information that identifies a particular individual by his or her full name, resident registration number, image, etc.;

(b) Information which, even if it by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual. In such cases, whether or not there is ease of combination shall be determined by reasonably considering the time, cost, technology, etc. used to identify the individual such as likelihood that the other information can be procured;

(c) Information under items (a) or (b) above that is pseudonymized in accordance with subparagraph 1-2 below and thereby becomes incapable of identifying a particular individual without the use or combination of information for restoration to the original state (hereinafter referred to as "pseudonymized information");

1-2. The term "pseudonymization" means a procedure to process personal information so that the information cannot identify a particular individual without additional information, by deleting in part, or replacing in whole or in part, such information;

2. The term “processing” means the collection, generation, connecting, interlocking, recording, storage, retention, value-added processing, editing, searching, output, correction, recovery, use, provision, disclosure, and destruction of personal information and other similar activities;

3. The term “data subject” means an individual who is identifiable through the information processed and is the subject of that information;

4. The term “personal information file” means a set or sets of personal information arranged or organized in a systematic manner based on a certain rule for easy search of the personal information;

5. The term “personal information controller” means a public institution, legal person, organization, individual, etc. that processes personal information directly or indirectly to operate the personal information files as part of its activities;

6. The term "public institution" means any of the following institutions:

(a) The administrative bodies of the National Assembly, the Courts, the Constitutional Court, and the National Election Commission; the central administrative agencies (including agencies under the Presidential Office and the Prime Minister’s Office) and their affiliated entities; and local governments;

(b) Other national agencies and public entities prescribed by Presidential Decree;

7. The term "visual data processing devices" means the devices prescribed by Presidential Decree, which are continuously installed at a certain place to take pictures of persons or images of things, or transmit such pictures or images via wired or wireless networks.

8. The term “scientific research” means research that applies scientific methods, such as technological development and demonstration, fundamental research, applied research and privately funded research.

Article 3 (Principles for Protecting Personal Information) (1) The personal information controller shall specify explicitly the purposes for which personal information is processed; and shall collect personal information lawfully and fairly to the minimum extent necessary for such purposes.

(2) The personal information controller shall process personal information in an appropriate manner necessary for the purposes for which the personal information is processed, and shall not use it beyond such purposes.

(3) The personal information controller shall ensure personal information is accurate, complete, and up to date to the extent necessary in relation to the purposes

for which the personal information is processed.

(4) The personal information controller shall manage personal information safely according to the processing methods, types, etc. of personal information, taking into account the possibility of infringement on the data subject's rights and the severity of the relevant risks.

(5) The personal information controller shall make public its privacy policy and other matters related to personal information processing; and shall guarantee the data subject's rights, such as the right to access their personal information.

(6) The personal information controller shall process personal information in a manner to minimize the possibility of infringing the privacy of a data subject.

(7) If it is still possible to fulfil the purposes of collecting personal information by processing anonymized or pseudonymised personal information, the personal information controller shall endeavor to process personal information through anonymization, where anonymization is possible, or through pseudonymisation, if it is impossible to fulfil the purposes of collecting personal information through anonymization.<Amended by Act No. 16930, 4. February, 2020 >

(8) The personal information controller shall endeavor to obtain trust of data subjects by observing and performing such duties and responsibilities as provided for in this Act and other related statutes.

Article 4 (Rights of Data Subjects) A data subject has the following rights in relation to the processing of his or her own personal information:

1. The right to be informed of the processing of such personal information;
2. The right to determine whether or not to consent and the scope of consent regarding the processing of such personal information;
3. The right to confirm whether or not personal information is being processed and to request access (including the provision of copies; hereinafter the same applies) to such personal information;
4. The right to suspend the processing of, and to request correction, deletion, and destruction of such personal information;
5. The right to appropriate redress for any damage arising out of the processing of such personal information through a prompt and fair procedure.

Article 5 (Obligations of State, etc.) (1) The State and a local government shall formulate policies to prevent harmful consequences of beyond-purpose collection, abuse and misuse of personal

information, indiscrete surveillance and tracking, etc. and to enhance the dignity of human beings and individual privacy.

(2) The State and a local government shall establish policy measures, such as improving statutes, necessary to protect the data subject's rights as provided for in Article 4.

(3) The State and local government shall respect, promote, and support selfregulating data protection activities of personal information controllers to improve unreasonable social practices relating to the processing of personal information.

(4) The State and a local government shall enact or amend any statutes or municipal ordinances in conformity with the purpose of this Act.

Article 6 (Relationship to other Acts) The protection of personal information shall be governed by this Act, except as otherwise specifically provided for in other Acts. <Amended by Act No. 12504, Mar. 24, 2014>

CHAPTER II ESTABLISHMENT OF PERSONAL INFORMATION PROTECTION POLICIES, ETC.

Article 7 (Personal Information Protection Commission) (1) The Personal Information Protection Commission (hereinafter referred to as the "Protection Commission") shall be established under the Prime Minister to independently conduct work relating to the protection of personal information. <Amended by Act No. 16930, 4. February, 2020 > (2) The Protection Commission shall be deemed a central administrative agency under Article 2 of the Government Organization Act: Provided, That Article 18 of the Government Organization Act shall not apply to any of the following matters: <Amended by Act No. 16930, 4. February, 2020 >

1. Affairs specified in subparagraphs 3 and 4 of Article 7-8 (1);
2. Matters falling under subparagraph 1 among those to be deliberated and resolved on under Article 7-9 (1).

(2) through (9) Deleted.<by Act No. 16930, Feb. 4, 2020>

Article 7-2 (Composition of the Protection Commission) (1) The Protection Commission shall be comprised of nine Commissioners including two Standing Commissioners (one Chairperson and one Vice Chairperson).

(2) Commissioners of the Protection Commission shall be selected from among any of the following persons with sufficient experience and expertise in the protection of personal information, with the

Chairperson and Vice Chairperson being proposed by the Prime Minister, two other Commissioners being proposed by Chairperson, two other Commissioners being recommended by the negotiation body of the political party to which the President belongs or belonged, and three other persons being recommended by another negotiation body and named or appointed by the President:

1. A person who serves, or served, as a public official of Grade III or higher (including public officials belonging to the Senior Executive Service) who is responsible for personal information protection;
2. A person who has been serving, or served, as a judge, prosecutor or lawyer for ten years or longer;
3. A person who served as an officer at a public institution or group (including groups comprised of personal information controllers) for three years or longer or a person recommended by the above public institution or group who was in charge of personal information protection for three years or longer;
4. A person who has expertise in a field relating to personal information and has been serving, or served, as an associate professor or higher at a school set forth in subparagraph 1 of Article 2 of the Higher Education Act for five years or longer.

(3) The Chairperson and the Vice Chairperson shall be appointed from among public officials in political service.

(4) The Chairperson, Vice Chairperson and the head of the secretariat under Article 7-13 shall become cabinet member, notwithstanding Article 10 of the Government Organization Act.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 7-3 (Chairperson) (1) The Chairperson shall represent the Protection Commission, preside over meetings of the Protection Commission, and oversee the related work.

(2) If the Chairperson cannot perform his/her duties for inevitable reasons, the Vice Chairperson shall act on his or her behalf, and if both the Chairperson and Vice Chairperson cannot perform his/her duties for inevitable reasons, another Commissioner, determined by the Protection Commission in advance, shall act on behalf of Chairperson.

(3) The Chairperson may attend the National Assembly and make statements in relation to the work of the Protection Commission, and if required by the National Assembly, he or she shall attend the National Assembly to make a report or respond to questions.

(4) The Chairperson may attend a meeting of the State Council and recommend the Prime Minister to submit a bill concerning the affairs under his/her jurisdiction.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 7-4 (Term of Office of Commissioners) (1) A Commissioner shall serve for a term of three years but may be consecutively appointed one time.

(2) When the post of a Commissioner becomes vacant, a new Commissioner shall be named or appointed without delay. In such cases, the term of the named or appointed succeeding Commissioner shall be newly commenced.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 7-5 (Status Guarantee for Commissioners) (1) No Commissioner shall be dismissed or de-commissioned against his or her will except in the following cases:

1. Where he or she is unable to perform his/her duties for a long period due to mental or physical disorder;
2. Where he or she falls under any ground for disqualification provided for in Article 7-7;
3. Where he or she violates his/her official duties under this Act or any other Act.

(2) Each Commissioner shall independently perform his or her duties in compliance with the law and his/her conscience.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 7-6 (Prohibition on Dual Office Holding) (1) Each Commissioner shall neither concurrently engage in any of the following posts, nor engage in any affairs for profits related to his or her duties:

1. Member of the National Assembly or Local Council;
2. State or local public official;
3. Other positions prescribed by Presidential Decree.

(2) Matters relating to for-profit businesses set forth in paragraph (1) shall be prescribed by Presidential Decree.

(3) A Commissioner shall not engage in political activities.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 7-7 (Grounds for Disqualification) (1) Persons falling under any of the following cannot be a Commissioner:

1. Non-Korean national;
2. A person falling under any of the subparagraphs under Article 33 of the State Public Officials Act;
3. A Member of political party set forth in Article 22 of the Political Parties Act.

(2) A Commissioner falling under any of the above subparagraphs 1 through 3 shall be automatically discharged from his or her position: Provided, That, in the case of subparagraph 2 of Article 33 of the State Public Officials Act, this only applies to a person who was declared bankrupt and did not apply for immunity within the application deadline, or received a confirmed decision of immunity disapproval or cancellation, according to the Debtor Rehabilitation and Bankruptcy Act; in the case of subparagraph 5 of Article 33 of the Same Act, this only applies to Articles 129 through 132 of the Criminal Act, Article 2 of the Act on Special Cases Concerning the Punishment, Etc. of Sexual Crimes, subparagraph 2 of Article 2 of the Act on the Protection of Children and Youth against Sex Offenses and a person who committed a crime prescribed in Articles 355 or 356 of the Criminal Act with regard to his or her duties and received a suspended sentence of imprisonment without labor or a heavier punishment.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 7-8 (Affairs under Jurisdiction of the Protection Commission) (1) The Protection Commission shall perform the following affairs:

1. Matters concerning the improvement of law relating to personal information protection;
2. Matters concerning the establishment or execution of policies, systems or plans relating to personal information protection;
3. Matters concerning investigation into infringement upon the right of data subjects and the ensuing dispositions;
4. Handling of complaints or remedial procedures relating to personal information processing and mediation of disputes over personal information;
5. Exchange and cooperation with international organizations and foreign personal information protection agencies to protect personal information;
6. Matters concerning the investigation and study, education and promotion of law, policies, systems and status relating to personal information protection;

7. Matters concerning the support of technological development and dissemination relating to personal information protection and nurturing of experts;

8. Matters provided for in this Act and other statutes as affairs under the jurisdiction of the Protection Commission.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 7-9 (Matters to be Deliberated and Resolved on by the Protection Commission) (1) The Protection Commission shall deliberate and resolve on the following matters:

1. Matters concerning the assessment of data breach incident factors under Article 8-2;
2. Establishment of the Master Plan referred to in Article 9 and the Implementation Plan referred to in Article 10;
3. Matters concerning the improvement of policies, systems, and law relating to personal information protection;
4. Matters concerning the coordination of positions taken by public institutions with respect to the processing of personal information;
5. Matters concerning the interpretation and operation of law related to the protection of personal information;
6. Matters concerning the use and provision of personal information under Article 18 (2) 5;
7. Matters concerning the results of the privacy impact assessment under Article 33 (3);
8. Matters concerning the imposition of penalty surcharges under Articles 28-6, 34-2 and 39-15;
9. Matters concerning the presentation of opinions and recommendation for improvement under Article 61;
10. Matters concerning corrective measures under Article 64;
11. Matters concerning indictment and recommendation for disciplinary actions under Article 65;
12. Matters concerning the publication of processing results under Article 66;
13. Matters concerning the imposition of administrative fines under Article 75;
14. Matters concerning the enactment, amendment and abolition of law under its jurisdiction and rules of the Protection Commission;

15. Matters referred to a meeting by Chairperson or at least two Commissioners of the Protection Commission with respect to the protection of personal information;

16. Other matters which the Protection Commission deliberates or resolves pursuant to this Act or other statutes.

(2) The Protection Commission may take the following measures if necessary to deliberate and resolve matters provided for in paragraph (1):

1. Listening to the opinions of relevant public officials, experts in personal information protection, civic organizations and relevant business operators;

2. Requesting submission of relevant materials or facts with respect to relevant agencies.

(3) Relevant agencies in receipt of a request made under paragraph (2) shall comply with the request unless there are extraordinary circumstances.

(4) Upon deliberating and resolving on matters provided for in paragraph (1) 3, the Protection Commission may advise on the improvement of such matters to the relevant agency.

(5) The Protection Commission may inspect whether the details of its advice given under paragraph (4) has been implemented or not.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 7-10 (Meetings) (1) Meetings of the Protection Commission shall be convened by the Chairperson when he or she deems it necessary or at the request of not less than 1/4 of all incumbent Commissioners.

(2) The Chairperson or at least two Commissioners of the Protection Commission may propose a bill to the Protection Commission.

(3) The quorum for holding meetings of the Protection Commission shall be the presence of a majority of its members enrolled, and any resolution shall require the affirmative votes of a majority of the members present.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 7-11 (Disqualification of, Challenge to, and Refrainment by, Commissioners) (1) A Commissioner of the Protection Commission shall be excluded from participating in deliberation and resolution for a case if:

1. The Commissioner or his or her current or former spouse is a party to the relevant case or is a joint right holder or a joint obligator with respect to the case;
2. The Commissioner is or was a relative of a party to the case;
3. The Commissioner has given any testimony, expert opinion, or legal advice with respect to the case;
4. The Commissioner is or was involved in the case as an agent or representative of a party to the case;
5. The Commissioner or a public institution, corporation or group where he or she belongs shares interests with a person who provides advice or other support for the case.

(2) When any party finds it impracticable to expect fair deliberation and resolution from a Commissioner, he or she may file an application for recusal, and the Protection Commission shall make a decision by resolution.

(3) A Commissioner may refrain from the case on the grounds provided for in paragraphs (1) or (3).

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 7-12 (Subcommission) (1) The Protection Commission may have subcommissions which will deliberate and resolve minor personal information infringement cases or similar or repetitive matters to ensure more efficient work procedures.

(2) Each sub-commission shall be comprised of three members.

(3) Matters deliberated and resolved by the sub-commission pursuant to paragraph (1) shall be deemed deliberated and resolved by the Protection Commission.

(4) Resolution for a meeting of the sub-commission shall be made by the presence of all the members enrolled and affirmative votes of all members present.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 7-13 (Secretariat) The Protection Commission shall have a secretariat to handle its work, and matters that are not specified in this Act in relation to the organization of the Protection Commission shall be prescribed by Presidential Decree.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 7-14 (Operation) Matters that are not specified in this Act and other statutes in relation to the operation of the Protection Commission shall be prescribed by the rules of the Protection Commission.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 8 Deleted. <by Act No. 16930, Feb. 4, 2020>

Article 8-2 (Assessment of Data Breach Incident Factors) (1) The head of a central administrative agency shall request the Protection Commission to assess the factors of data breach incident where a policy or system that entails personal information processing is adopted or changed by the enactment or amendment of any statute under his or her jurisdiction.

(2) Upon receipt of a request made pursuant to paragraph (1), the Protection Commission may advise the head of the relevant agency of the matters necessary to improve the relevant statute by analyzing and reviewing the data breach incident factors of such statute.

(3) Necessary matters concerning the procedure and method to assess the data breach incident factors under paragraph (1) shall be prescribed by Presidential Decree.

[This Article Newly Inserted by Act No. 13423, Jul. 24, 2015]

Article 9 (Master Plan) (1) The Protection Commission shall establish a Master Plan to protect personal information (hereinafter referred to as a “Master Plan”) every three years in consultation with the heads of related central administrative agencies to ensure the protection of personal information and the rights and interests of data subjects. <Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No.

13423, Jul. 24, 2015>

(2) The Master Plan shall include the following:

1. Basic goals and intended directions of the protection of personal information;
2. Improvement of systems and statutes related to the protection of personal information;
3. Measure to prevent personal information breaches;
4. Vitalization of self-regulation to protect personal information;
5. Promoting education and public relations to protect personal information;
6. Training of specialists in the protection of personal information;
7. Other matters necessary to protect personal information.

(3) The National Assembly, the Court, the Constitutional Court, and the National Election Commission may establish and implement its own Master Plan to protect personal information of relevant institutions, (including affiliated entities).

Article 10 (Implementation Plan) (1) The head of a central administrative agency shall establish an implementation plan to protect personal information each year in accordance with the Master Plan and submit it to the Protection Commission, and shall execute the implementation plan subject to the deliberation and resolution of the Protection Commission.

(2) Matters necessary for the establishment and execution of the implementation plan shall be prescribed by Presidential Decree.

Article 11 (Request for Materials, etc.) (1) To efficiently establish the Master Plan, the Protection Commission may request materials or opinions regarding the status of regulatory compliance, personal information management, etc. by personal information controllers from personal information controllers, the heads of relevant central administrative agencies, the heads of local governments and related organizations or associations, etc. <Amended by Act No. 11690, Mar. 23, 2013; Act No.

12844, Nov. 19, 2014; Act No. 13423, Jul. 24, 2015>

(2) The Protection Commission may conduct an investigation with respect to data controllers, the competent head of the central administrative departments or agencies and local governments, and the competent agencies and organizations about the level and actual status of how personal data is managed where necessary to implement policies for personal data protection and to evaluate performance, etc.

<Newly Inserted by Act No. 13423, Jul. 24, 2015; Act No. 14839, Jul. 26, 2017; Act No. 16930, 4. February, 2020 >

(3) The head of a central administrative agency may request the materials referred to in paragraph (1) from personal information controllers in the fields under his or her jurisdiction to efficiently establish and promote Implementation Plans.<Amended by Act No. 13423, Jul. 24, 2015>

(4) Any person in receipt of a request to furnish the materials under paragraphs (1) through (3) shall comply with the request unless there are extraordinary circumstances.<Amended by Act No. 13423, Jul. 24, 2015>

(5) The scope and method to furnish the materials under paragraphs (1) through (3) and other necessary matters shall be prescribed by Presidential Decree.<Amended by Act No. 13423, Jul. 24, 2015>

Article 12 (Personal Information Protection Guidelines) (1) The Protection Commission may establish the Standard Personal Information Protection Guidelines (hereinafter referred to as the “Standard Guidelines”) regarding the personal information processing standard, types of personal information breaches, preventive measures, etc., and recommend that personal information controllers comply with such Guidelines. <Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>

(2) The head of a central administrative agency may establish the personal information protection guidelines regarding the personal information processing in the fields under his or her jurisdiction in accordance with the Standard Guidelines; and may recommend that personal information controllers comply with such guidelines.

(3) The National Assembly, the Court, the Constitutional Court, and the National Election Commission may establish and implement its own personal information protection guidelines for each relevant institution (including affiliated entities).

Article 13 (Promotion and Support of Self-Regulation) The Protection Commission shall establish policies necessary for the following matters to promote and support self-regulating activities of personal information controllers to protect personal information:<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>

1. Education and public relations concerning the protection of personal information;
2. Promotion and support of agencies and organizations related to the protection of personal information;
3. Introduction and facilitation of privacy mark;
4. Support for personal information controllers in the establishment and implementation of self-regulatory rules;
5. Other matters necessary to support the self-regulating data protection activities of personal information controllers.

Article 14 (International Cooperation) (1) The Government shall establish policy measures necessary to enhance the personal information protection standard in the international environment.

(2) The Government shall establish relevant policy measures so that the rights of data subjects may not be infringed on owing to the cross-border transfer of personal information.

CHAPTER III PROCESSING OF PERSONAL INFORMATION

SECTION 1 Collection, Use, Provision, etc. of Personal Information

Article 15 (Collection and Use of Personal Information) (1) A personal information controller may collect personal information in any of the following circumstances, and use it with the scope of the purpose of collection:

1. Where consent is obtained from a data subject;
2. Where special provisions exist in laws or it is inevitable to observe legal obligations;
3. Where it is inevitable for a public institution's performance of its duties under its jurisdiction as prescribed by statutes, etc.;
4. Where it is inevitably necessary to execute and perform a contract with a data subject;
5. Where it is deemed manifestly necessary for the protection of life, bodily or property interests of the data subject or third party from imminent danger where the data subject or his or her legal representative is not in a position to express intention, or prior consent cannot be obtained owing to unknown addresses, etc.;
6. Where it is necessary to attain the justifiable interest of a personal information controller, which such interest is manifestly superior to the rights of the data subject. In such cases, processing shall be allowed only to the extent the processing is substantially related to the justifiable interest of the personal information controller and does not go beyond a reasonable scope.

(2) A personal information controller shall inform a data subject of the following matters when it obtains consent under paragraph (1) 1. The same shall apply when any of the following is modified.

1. The purpose of the collection and use of personal information;
2. Particulars of personal information to be collected;
3. The period for retaining and using personal information;
4. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent.

(3) A personal information controller may use personal information without the consent of a data subject within the scope reasonably related to the initial purpose of the collection as prescribed by Presidential Decree, in consideration whether disadvantages have been caused to the data subject and whether necessary measures have been taken to secure such as encryption, etc. < This Article Newly Inserted by Act No. 16930, 4. February, 2020 >

Article 16 (Limitation to Collection of Personal Information) (1) A personal information controller shall collect the minimum personal information necessary to attain the purpose when collecting personal information pursuant to Article 15 (1). In such cases, the burden of proof that the minimum personal information is collected shall be borne by the personal information controller.

(2) A personal information controller shall collect personal information by specifically informing a data subject of the fact that he or she may deny the consent to the collection of other personal information than the minimum information necessary in case of collecting the personal information through the consent of the data subject.<Newly Inserted by Act No. 11990, Aug. 6, 2013>

(3) A personal information controller shall not deny the provision of goods or services to a data subject on ground that the data subject does not consent to the collection of personal information exceeding minimum requirement.<Amended by Act

No. 11990, Aug. 6, 2013

Article 17 (Provision of Personal Information) (1) A personal information controller may provide (or share; hereinafter the same shall apply) the personal information of a data subject to a third party in any of the following circumstances: <Amended by Act No 16930, February. 4, 2020>

1. Where the consent is obtained from the data subject;
2. Where the personal information is provided within the scope of purposes for which it is collected pursuant to Articles 15 (1) 2, 3 and 5 and 39-3 (2) 2 and 3.

(2) A personal information controller shall inform a data subject of the following matters when it obtains the consent under paragraph (1) 1. The same shall apply when any of the following is modified:

1. The recipient of personal information;
2. The purpose for which the recipient of personal information uses such information;
3. Particulars of personal information to be provided;
4. The period during which the recipient retains and uses personal information;
5. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent.

(3) A personal information controller shall inform a data subject of the matters provided for in paragraph (2), and obtain the consent from the data subject in order to provide personal information

to a third party overseas; and shall not enter into a contract for the cross-border transfer of personal information in violation of this Act.

(4) A personal information controller may provide personal information without the consent of a data subject within the scope reasonably related to the purposes for which the personal information was initially collected, in accordance with the matters prescribed by Presidential Decree taking into consideration whether disadvantages are caused to the data subject, whether necessary measures to secure safety, such as encryption, have been taken, etc. <Newly Inserted by Act No. 16930, 4. February, 2020 >

Article 18 (Limitation to Out-of-Purpose Use and Provision of Personal Information)

(1) A personal information controller shall not use personal information beyond the scope provided for in Articles 15 (1) and 39-3 (1) and (2), or provide it to any third party beyond the scope provided for in Article 17 (1) and (3). <Amended by Act No.

16930, Feb. 4, 2020>

(2) Notwithstanding paragraph (1), where any of the following subparagraphs applies, a personal information controller may use personal information or provide it to a third party for other purposes, unless doing so is likely to unfairly infringe on the interest of a data subject or third party: Provided, That information and communications service providers (as set forth in Article 2 (1) 3 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.; hereinafter the same shall apply) processing the personal information of users (as set forth in Article 2 (1) 4 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.; hereinafter the same shall apply) are only subject to subparagraphs 1 and 2, and subparagraphs 5 through 9 are applicable only to public institutions:<Amended by Act No. 16930, Feb. 4, 2020>

1. Where additional consent is obtained from the data subject;
2. Where special provisions in other laws so require;
3. Where it is deemed manifestly necessary for the protection of life, bodily or property interests of the data subject or third party from imminent danger where the data subject or his or her legal representative is not in a position to express intention, or prior consent cannot be obtained owing to unknown addresses;
4. Deleted;<by Act No. 16930, Feb. 4, 2020>

5. Where it is impossible to perform the duties under its jurisdiction as provided for in any Act, unless the personal information controller uses personal information for other purpose than the intended one, or provides it to a third party, and it is subject to the deliberation and resolution by the Commission;

6. Where it is necessary to provide personal information to a foreign government or international organization to perform a treaty or other international convention;

7. Where it is necessary for the investigation of a crime, indictment and prosecution;

8. Where it is necessary for a court to proceed with trial-related duties;

9. Where it is necessary for the enforcement of punishment, probation and custody.

(3) A personal information controller shall inform the data subject of the following matters when it obtains the consent under paragraph (2) 1. The same shall apply when any of the following is modified.

1. The recipient of personal information;

2. The purpose of use of personal information (in the case of provision of personal information, it means the purpose of use by the recipient);

3. Particulars of personal information to be used or provided;

4. The period for retaining and using personal information (where personal information is provided, it means the period for retention and use by the recipient);

5. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent.

(4) Where a public institution uses personal information, or provides it to a third party for other purpose than the intended one collected under paragraph (2) 2 through 6, 8, and 9, the public institution shall post the legal grounds for such use or provision, purpose and scope, and other necessary matters on the Official Gazette or its website requirements for such use or provision including the legal basis, purpose, scope, etc. as prescribed by Notification of the Protection Commission.<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>

(5) Where a personal information controller provides personal information to a third party for other purpose than the intended one in any case provided for in paragraph (2), the personal information controller shall request the recipient of the personal information to limit the purpose and method of

use and other necessary matters, or to prepare necessary safeguards to ensure the safety of the personal information. In such cases, the person in receipt of such request shall take necessary measures to ensure the safety of the personal information.

Article 19 (Limitation to Use and Provision of Personal Information on Part of Its Recipients) A person who receives personal information from a personal information controller shall not use the personal information, or provide it to a third party, for any purpose other than the intended one, except in the following circumstances:

1. Where additional consent is obtained from the data subject;
2. Where special provisions in other laws so require.

Article 20 (Notification on Sources, etc. of Personal Information Collected from Third Parties) (1)

When a personal information controller processes personal information collected from third parties, the personal information controller shall immediately

notify the data subject of the following matters at the request of such data subject:

1. The source of collected personal information;
2. The purpose of processing personal information;
3. The fact that the data subject is entitled to demand suspension of processing of personal information, as prescribed in Article 37.

(2) Notwithstanding paragraph (1), when a personal information controller satisfying the criteria prescribed by Presidential Decree taking into account the types and amount of processed personal information, number of employees, amount of sales, etc., collects personal information from third parties and processes the same pursuant to Article 17 (1) 1, the personal information controller shall notify the data subject of the matters referred to in paragraph (1): Provided, That this shall not apply where the information collected by the personal information controller does not contain any personal information, such as contact information, through which notification can be given to the data subject.<Newly Inserted by Act No. 14107, Mar. 29, 2016; Act No 16930, February. 4, 2020>

(3) Necessary matters in relation to the time, method, and procedure of giving notification to the data subject pursuant to the main sentence of paragraph (2), shall be prescribed by Presidential Decree.<Newly Inserted by Act No. 14107, Mar. 29, 2016> (4) Paragraph (1) and the main clause of paragraph (2) shall not apply to any of the following circumstances: Provided, That this shall be the

case only where it is manifestly superior to the rights of data subjects under this Act:<Amended by Act No. 14107, Mar. 29, 2016>

1. Where personal information, which is subject to a notification request, is included in the personal information files referred to in any of the subparagraphs of Article 32 (2);
2. Where such notification is likely to cause harm to the life or body of any other person, or unfairly damages the property and other interests of any other person.

Article 21 (Destruction of Personal Information) (1) A personal information controller shall destroy personal information without delay when the personal information becomes unnecessary owing to the expiry of the retention period, attainment of the purpose of processing the personal information, etc.: Provided, That this shall not apply where the retention of such personal information is mandatory by other

statutes.

(2) When a personal information controller destroys personal information pursuant to paragraph (1), necessary measures to prevent recovery and revival shall be taken.

(3) Where a personal information controller is obliged to retain, rather than destroy, personal information pursuant to the proviso to paragraph (1), the relevant personal information or personal information files shall be stored and managed separately from other personal information.

(4) Other necessary matters, such as the methods to destroy personal information and its destruction process, shall be prescribed by Presidential Decree.

Article 22 (Methods of Obtaining Consent) (1) Where a personal information controller intends to obtain the consent of the data subject (including his or her legal representative as stated in paragraph (6): hereafter in this Article the same applies) to the processing of his or her personal information, the personal information controller shall present the request for consent to the data subject in a clearly recognizable manner where each matter requiring consent is distinctly presented, and obtain his or her consent thereto, respectively. <Amended by Act No. 14765, Apr. 18, 2017>

(2) Where a personal information controller obtains the consent under paragraph (1) in writing (including electronic documents under Article 2, subparagraph 1 of the Framework Act on Electronic Documents and Transactions), the personal information controller shall clearly specify important matters prescribed by Presidential Decree such as the purpose of collection and use of personal information and the items of personal information to be collected and used, in the manner prescribed

by Notification of the Protection Commission, so as to make such matters easy to be understood.<Newly Inserted by Act No. 14765, Apr. 18, 2017; Act No. 14839, Jul. 26, 2017; Act No. 16930, 4. February, 2020 >

(3) Where a personal information controller obtains the consent of a data subject to the processing of his or her personal information pursuant to Articles 15 (1) 1, 17 (1) 1, 23 (1) 1, and 24 (1) 1, the personal information controller shall distinguish personal information that may be processed without the data subject's consent for the purpose of executing a contract with the data subject, etc., from personal information that may be processed only with the data subject's consent. In such cases, the burden of proof that no consent is required in processing the personal information shall be borne by the personal information controller.<Amended by Act No. 14107, Mar. 29, 2016; Act No. 14765, Apr. 18, 2017>

(4) Where a personal information controller intends to obtain the consent of the data subject to the processing of his or her personal information in order to promote goods or services or solicit purchase thereof, the personal information controller shall notify the data subject of the fact in a clearly recognizable manner, and obtain his/her consent thereto.<Amended by Act No. 14765, Apr. 18, 2017>

(5) A personal information controller shall not deny the provision of goods or services to a data subject on ground that the data subject would not consent to the matter eligible for selective consent pursuant to paragraph (3), or would not consent pursuant to paragraph (4) and Article 18 (2) 1.<Amended by Act No. 14765, Apr. 18, 2017>

(6) When it is required to obtain consent pursuant to this Act to process personal information of a child under 14 years of age, a personal information controller shall obtain the consent of his/her legal representative. In such cases, minimum personal information necessary to obtain the consent of the legal representative may be collected directly from such child without the consent of his/her legal representative. <Amended by Act No. 14765, Apr. 18, 2017>

(7) Except as otherwise expressly provided for in paragraphs (1) through (6), other matters necessary in relation to detailed methods to obtain the consent of data subjects and the minimum information referred to in paragraph (6) shall be prescribed by Presidential Decree, in consideration of the collection media of personal information.<Amended by Act No. 14765, Apr. 18, 2017>

SECTION 2 Limitation to Processing of Personal Information

Article 23 (Limitation to Processing of Sensitive Information) (1) A personal information controller shall not process any information prescribed by Presidential Decree (hereinafter referred to as "sensitive information"), including ideology, belief, admission to or withdrawal from a trade union

or political party, political opinions, health, sex life, and other personal information that is likely to markedly threaten the privacy of any data subject: Provided, That this shall not apply in any of the following circumstances: <Amended by Act No. 14107, Mar. 29, 2016>

1. Where the personal information controller informs the data subject of the matters provided for in Article 15 (2) or 17 (2), and obtains the consent of the data subject apart from the consent to the processing of other personal information;

2. Where other statutes require or permit the processing of sensitive information.

(2) Where a personal information controller processes sensitive information pursuant to paragraph (1), the personal information controller shall take measures necessary to ensure safety pursuant to Article 29 so that the sensitive information may not be lost, stolen, divulged, forged, altered, or damaged. <Newly Inserted by Act No. 14107, Mar. 29, 2016>

Article 24 (Limitation to Processing of Personally Identifiable Information) (1) A personal information controller shall not process any information prescribed by Presidential Decree that can be used to identify an individual in accordance with statutes (hereinafter referred to as "personally identifiable information"), except in any of the following cases:

1. Where the personal information controller informs a data subject of the matters provided for in Article 15 (2) or 17 (2), and obtains the consent of the data subject apart from the consent to the processing of other personal information;

2. Where other statutes specifically require or permit the processing of unique identification information.

(2) Deleted.<Act No. 11990, Aug. 6, 2013>

(3) Where a personal information controller processes personally identifiable information pursuant to paragraph (1), the personal information controller shall take measures necessary to ensure safety, including encryption, as prescribed by Presidential Decree, so that the personally identifiable information may not be lost, stolen, divulged, forged, altered, or damaged.<Amended by Act No. 13423, Jul. 24, 2015>

(4) The Protection Commission shall regularly inspect whether a personal information controller meeting the criteria prescribed by Presidential Decree taking into account the types and amount of processed personal information, number of employees, amount of sales, etc., has taken the measures

necessary to ensure safety pursuant to paragraph (3), as prescribed by Presidential Decree.<Newly Inserted by Act No. 14107, Mar. 29, 2016; Act No. 14839, Jul. 26, 2017 ; Act No 16930, February. 4, 2020>

(5) The Protection Commission may authorize specialized institutions prescribed by Presidential Decree to conduct the inspection referred to in paragraph (4).<Newly Inserted by Act No. 14107, Mar. 29, 2016; Act No. 14839, Jul. 26, 2017 ; Act No 16930, February. 4, 2020>

Article 24-2 (Limitation to Processing of Resident Registration Numbers) (1) Notwithstanding Article 24 (1), a personal information controller shall not process any resident registration number, except in any of the following cases: <Amended by Act No. 14107, Mar. 29, 2016; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

1. Where any Act, Presidential Decree, National Assembly Regulations, Supreme Court Regulations, Constitutional Court Regulations, National Election Commission Regulations or Board of Audit and Inspection Regulations specifically requires or permits the processing of resident registration numbers;

2. Where it is deemed manifestly necessary for the protection, from imminent danger, of life, bodily and property interests of a data subject or a third party;

3. Where it is inevitable to process resident registration numbers in line with subparagraphs 1 and 2 in circumstances publicly notified by the Protection Commission.

(2) Notwithstanding Article 24 (3), a personal information controller shall retain resident registration numbers in a safe manner by means of encryption so that the resident registration numbers may not be lost, stolen, divulged, forged, altered, or damaged. In such cases, any necessary matters in relation to the scope of encryption objects and encryption timing by object, etc. shall be prescribed by Presidential Decree, taking into account the amount of personal information processed, data breach impact, etc.<Newly Inserted by Act No. 12504, Mar. 24, 2014; Act No. 13423, Jul. 24, 2015>

(3) A personal information controller shall provide data subjects with an alternative sign-up tool without using their resident registration numbers in the stage of being admitted to membership via the website while processing the resident registration numbers pursuant to paragraph (1).

(4) The Protection Commission may prepare and support such measures as legislative arrangements, policy-making, necessary facilities, and systems build-up in order to support the provision of the measures provided for in paragraph (3).

<Amended by Act No. 12504, Mar. 24, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>

[This Article Newly Inserted by Act No. 11990, Aug. 6, 2013]

Article 25 (Limitation to Installation and Operation of Visual Data Processing Devices)

(1) No one shall install and operate any visual data processing device at open places, except in any of the following circumstances:

1. Where specifically allowed by statutes;
2. Where it is necessary for the prevention and investigation of crimes;
3. Where it is necessary for the safety of facilities and prevention of fire;
4. Where it is necessary for regulatory control of traffic;
5. Where it is necessary for the collection, analysis, and provision of traffic information.

(2) No one shall install and operate any visual data processing device so as to look into the places which is likely to noticeably threaten individual privacy, such as a bathroom, restroom, sauna, and dressing room used by multiple unspecified persons: Provided, That the same shall not apply to the facilities prescribed by Presidential Decree, which detain or protect persons in accordance with statutes, such as correctional facilities and mental health care centers.

(3) The head of a public institution who intends to install and operate visual data processing devices pursuant to paragraph (1) and a person who intends to install and operate visual data processing devices pursuant to the proviso to paragraph (2) shall gather opinions of relevant specialist and interested persons through the formalities prescribed by Presidential Decree such as public hearings and information sessions. (4) A person who installs and operates visual data processing devices pursuant to paragraph (1) (hereinafter referred to as "VDPD operator") shall take necessary measures including posting on a signboard the following matters, so that data subjects may easily recognize such devices: Provided, That this shall not apply to military installations defined in subparagraph 2 of Article 2 of the Protection of Military Bases and Installations Act, important national facilities defined in subparagraph 13 of Article 2 of the United Defense Act, and other facilities prescribed by Presidential Decree:<Amended by Act No. 14107, Mar. 29, 2016>

1. The purpose and place of installation;
2. The scope and hours of photographing;

3. The name and contact information of the person in charge of its management;

4. Other matters prescribed by Presidential Decree.

(5) A VDPD operator shall not handle arbitrarily the visual data processing devices for other purposes than the initial one; direct the said devices toward different spots; nor use sound recording functions.

(6) Every VDPD operator shall take measures necessary to ensure safety pursuant to Article 29 so that the personal information may not be lost, stolen, divulged, forged, altered, or damaged.<Amended by Act No. 13423, Jul. 24, 2015>

(7) Every VDPD operator shall establish an appropriate policy to operate and manage the visual data processing devices, as prescribed by Presidential Decree. In such cases, the VDPD operator may be exempted from adopting a Privacy Policy pursuant to Article 30.

(8) A VDPD operator may outsource the installation and operation of visual data processing devices to a third party: Provided, That the public institutions shall comply with the procedures and requirements prescribed by Presidential Decree when outsourcing the installation and operation of visual data processing devices to a third party.

Article 26 (Limitation to Personal Information Processing Subsequent to Outsourcing of Work) (1)

A personal information controller shall, when outsourcing personal information processing to a third party, effect such outsourcing through a document that states the following:

1. Prevention of personal information processing for other purposes than the outsourced purpose;
2. Technical and managerial safeguards of personal information;
3. Other matters prescribed by Presidential Decree to ensure safe management of personal information.

(2) A personal information controller that outsources personal information processing pursuant to paragraph (1) (hereinafter referred to as "outsourcer") shall disclose the details of the outsourced work and the entity that processes personal information (hereinafter referred to as "outsourcee") under an outsourcing contract in the manner prescribed by Presidential Decree so that data subjects may recognize it with ease at any time.

(3) The outsourcer shall, in case of outsourcing the promotion of goods or services, or soliciting of sales thereof, notify data subjects of the outsourced work and the outsourcee in the manners prescribed by Presidential Decree. The same shall apply where the outsourced work or the outsourcee has been changed.

(4) The outsourcer shall educate the outsourcee so that personal information of data subjects may not be lost, stolen, leaked, forged, altered, or damaged owing to the outsourcing of work, and supervise how the outsourcee processes such personal information safely by inspecting the status of processing, etc., as prescribed by Presidential Decree.<Amended by Act No. 13423, Jul. 24, 2015>

(5) An outsourcee shall not use any personal information beyond the scope of the work outsourced by the personal information controller, nor provide personal information to a third party.

(6) With respect to the compensation of damage arising out of the processing of personal information outsourced to an outsourcee in violation of this Act, the outsourcee shall be deemed an employee of the personal information controller. (7) Articles 15 through 25, 27 through 31, 33 through 38, and 59 shall apply mutatis mutandis to outsourcees.

Article 27 (Limitation to Transfer of Personal Information following Business Transfer, etc.) (1) A personal information controller shall notify in advance the data subjects of the following matters in the manner prescribed by Presidential Decree in the case of transfer of personal information to a third party owing to the transfer of some or all of his or her business, a merger, etc.:

1. The fact that the personal information will be transferred;
2. The name (referring to the company name in case of a legal person), address, telephone number and other contact information of the recipient of the personal information (hereinafter referred to as "business transferee, etc.");
3. The method and procedure for withdrawing consent if the data subject does not wish his or her personal information to be transferred.

(2) Upon receiving personal information, the business transferee, etc. shall, without delay, notify data subjects of the fact in the manner prescribed by Presidential

Decree: Provided, That this shall not apply where the personal information controller has already notified the data subjects of the fact of such transfer pursuant to paragraph (1).

(3) Upon receiving personal information owing to business transferee, etc., a merger, etc., the business transferee may use, or provide a third party with, the personal information only for the initial purposes dating to the time of the transfer. In such cases, the business transferee shall be deemed the personal information controller.

Article 28 (Supervision of Personal Information Handlers) (1) While processing personal information, a personal information controller shall conduct appropriate control and supervision

against the persons who process the personal information under his or her command and supervision, such as an officer or employee, temporary agency worker and part-time worker (hereinafter referred to as “personal information handler”) to ensure the safe management of the personal information.

(2) A personal information controller shall provide personal information handlers with necessary educational programs on a regular basis in order to ensure the appropriate handling of personal information.

SECTION 3 Special Cases concerning Pseudonymous Data

Article 28-2 (Processing of Pseudonymous Data) (1) A personal information controller may process pseudonymized information without the consent of data subjects for statistical purposes, scientific research purposes, and archiving purposes in the public interest, etc.

(2) A personal information controller shall not include information that may be used to identify a certain individual when providing pseudonymized information to a third party according to paragraph (1).

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 28-3 (Restriction on Combination of Pseudonymous Data) (1) Notwithstanding Article 28-2, the combination of pseudonymized information processed by different personal information controllers for statistical purposes, scientific research and preservation of records for public interest, etc. shall be conducted by a specialized institution designated by the Protection Commission or the head of the related central administrative agency.

(2) A personal information controller who intends to release the combined information outside the organization that combined the information shall obtain approval from the head of the specialized institution after processing the information into pseudonymized information or the form referred to in Article 58-2.

(3) Necessary matters including the procedures and methods of combination pursuant to paragraph (1), standards and procedures to designate, or cancel the designation of, a specialized institution management and supervision, and standards and procedures of exporting and approval pursuant to paragraph (2) shall be prescribed by Presidential Decree.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 28-4 (Obligation to Take Safety Measures for Pseudonymous Data) (1) When processing the pseudonymized information, a personal information controller shall take such technical,

organizational and physical measures as separately storing and managing additional information needed for restoration to the original state, as may be necessary to ensure safety as prescribed by Presidential Decree so that the personal information may not be lost, stolen, divulged, forged, altered, or damaged.

(2) A personal information controller who intends to process the pseudonymized information shall prepare and keep records relating to matters prescribed by the Presidential Decree including the purpose of processing the pseudonymized information, and a third party recipient when pseudonymized information is provided, to manage the processing of pseudonymized information.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 28-5 (Prohibited Acts for the Processing of the Pseudonymized Information) (1) No one shall process the pseudonymized information for the purpose of identifying a certain individual.

(2) When information identifying a certain individual is generated while the pseudonymized information is processed, the personal information controller shall cease the processing of the information, and retrieve and destroy the information immediately.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 28-6 (Imposition of Administrative Surcharges for the Processing of the Pseudonymized Information) (1) The Commission may impose a fine equivalent to less than three-hundredths of total sales on data controller who has processed data for the purpose of identifying a specific individual in violation of Article 28-5 (1): Provided, That in case where there is no sales or difficulty in calculating the sales revenues, the data controller may be subject to a fine of not more than 400 million won or three-hundredths of the capital amount, whichever is greater.

(2) Article 34-2 (3) through (5) shall apply mutatis mutandis to matters necessary to impose and collect administrative surcharges.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 28-7 (Scope of Application) @Articles 20, 21, 27, 34 (1), 35 through 37, 39-3, 39-4, 39-6 through 39-8 shall not apply to the pseudonymized information.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

CHAPTER IV SAFEGUARD OF PERSONAL INFORMATION

Article 29 (Duty of Safeguards) Every personal information controller shall take such technical, managerial, and physical measures as establishing an internal management plan and preserving

access records, etc. that are necessary to ensure safety as prescribed by Presidential Decree so that the personal information may not be lost, stolen, divulged, forged, altered, or damaged.<Amended by Act No. 13423, Jul. 24, 2015>

Article 30 (Establishment and Disclosure of Privacy Policy) (1) Every personal information controller shall establish a personal information processing policy including the following matters (hereinafter referred to as "Privacy Policy"). In such cases, public institutions shall establish the Privacy Policy for the personal information files to be registered pursuant to Article 32: <Amended by Act No. 14107, Mar. 29, 2016>

1. The purposes for which personal information is processed;
 2. The period for processing and retaining personal information;
 3. Provision of personal information to a third party (if applicable);
 - 3-2. Procedures and methods for destroying personal information (if personal information shall be preserved according to the proviso of Article 21 (1), this shall include the basis of preservation and particulars of personal information to be preserved);
 4. Outsourcing personal information processing (if applicable);
 5. The rights and obligations of data subjects and legal representatives, and how to exercise such rights;
 6. Contact information, such as the name of a privacy officer designated under Article 31 or the name, telephone number, etc. of the department which performs the duties related to personal information protection and handles related grievances;
 7. Installation and operation of an automatic collection tool for personal information, including internet access data files, and the denial thereof (if applicable);
 8. Other matters prescribed by Presidential Decree regarding the processing of personal information.
- (2) Upon establishing or modifying the Privacy Policy, a personal information controller shall disclose the content so that data subjects may easily recognize it in such a way as prescribed by Presidential Decree.
- (3) Where there exist discrepancies between the Privacy Policy and the agreement executed by and between the personal information controller and data subjects, the terms that are beneficial to the data subjects shall prevail.

(4) The Protection Commission may prepare the Privacy Policy Guidelines and encourage the personal information controllers to comply with such Guidelines. <Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>

Article 31 (Designation of Privacy Officers) (1) A personal information controller shall designate a privacy officer who comprehensively takes charge of personal information processing.

(2) Every privacy officer shall perform the following functions:

1. To establish and implement a personal information protection plan;
2. To conduct a regular survey of the status and practices of personal information processing, and to improve shortcomings;
3. To handle grievances and remedial compensation in relation to personal information processing;
4. To build the internal control system to prevent the divulgence, abuse, and misuse of personal information;
5. To prepare and implement an education program about personal information protection;
6. To protect, control, and manage the personal information files;
7. Other functions prescribed by Presidential Decree for the appropriate processing of personal information.

(3) In performing the functions provided for in paragraph (2), a privacy officer may inspect the status of personal information processing and systems frequently, if necessary, and may request a report thereon from the relevant parties.

(4) Where a privacy officer becomes aware of any violation of this Act or other relevant statutes in relation to the protection of personal information, the privacy officer shall take corrective measures immediately, and shall report such corrective measures to the head of the institution or organization to which he or she belongs, if necessary.

(5) A personal information controller shall not have the chief privacy officer impose or be subject to disadvantages without any justifiable ground while performing the functions provided for in paragraph (2).

(6) The requirements for designation as privacy officers, functions, qualifications, and other necessary matters, shall be prescribed by Presidential Decree.

Article 32 (Registration and Disclosure of Personal Information Files) (1) Upon operating personal information files, the head of a public institution shall register the following matters with the Protection Commission. The same shall also apply where the registered matters are modified.
<Amended by Act No. 11690, Mar. 23, 2013; Act No.

12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>

1. The titles of the personal information files;
2. The grounds and purposes for the operation of the personal information files;
3. Particulars of personal information that are recorded in the personal information files;
4. The method of processing personal information;
5. The period for retaining personal information;
6. The recipient of personal information, if it is provided routinely or repetitively;
7. Other matters prescribed by Presidential Decree.

(2) Paragraph (1) shall not apply to any of the following personal information files:

1. Personal information files that record national security, diplomatic secrets, and other matters relating to grave national interests;
2. Personal information files that record the investigation of crimes, indictment and prosecution, punishment, and probation and custody, corrective orders, protective orders, security observation orders, and immigration;
3. Personal information files that record the investigations of violations of the Punishment of Tax Offenses Act and the Customs Act;
4. Personal information files exclusively used for internal job performance of public institutions;
5. Classified personal information files pursuant to other statutes.

(3) The Protection Commission may, if necessary, review the registration and content of the personal information files referred to in paragraph (1), and advise the head of the relevant public institution to make improvements. <Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>

(4) The Protection Commission shall make public the status of registered personal information files under paragraph (1) so that anyone may access them with ease. <Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>

(5) Necessary matters regarding the registration referred to in paragraph (1), the method, scope, and procedure of public disclosure referred to in paragraph (4), shall be prescribed by Presidential Decree.

(6) The registration and public disclosure of the personal information files retained by the National Assembly, the Court, the Constitutional Court and the National Election Commission (including their affiliated entities) shall be prescribed by the National Assembly Regulations, the Supreme Court Regulations, the Constitutional

Court Regulations, and the National Election Commission Regulations.

Article 32-2 (Certification of Personal Information Protection) (1) The Protection Commission may certify whether the data processing and other data protection-related action of a personal information controller abide by this Act, etc. <Amended by Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>

(2) The certification provided for in paragraph (1) shall be effective for three years.

(3) In any of the following cases, the Protection Commission may revoke the certification granted under paragraph (1), as prescribed by Presidential Decree: Provided, That it shall be revoked in cases falling under subparagraph 1:<Amended by Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

1. Where personal information protection has been certified by fraud or other unjust means;
2. Where follow-up management provided for in paragraph (4) has been denied or obstructed;
3. Where the certification criteria provided for in paragraph (8) have not been satisfied;
4. Where personal information protection-related statutes are breached seriously.

(4) The Protection Commission shall conduct follow-up management at least once annually to maintain the effectiveness of the certification of personal information protection.<Amended by Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

(5) The Protection Commission may authorize the specialized institutions prescribed by Presidential Decree to perform the duties related to certification under paragraph (1), revocation of certification under paragraph (3), follow-up management under paragraph (4), management of certification examiners under paragraph (7).<Amended by Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

(6) Any person who has obtained certification subject to paragraph (1) may indicate or promote the certification, as prescribed by Presidential Decree.

(7) Qualifications of certification examiners who conduct the certification examination subject to paragraph (1), criteria for disqualification, and other related matters shall be prescribed by Presidential Decree, taking into account specialty, career, and other necessary matters.

(8) Other necessary matters for the certification criteria, method, procedure, etc. subject to paragraph (1), including whether the personal information management system, guarantee of data subjects' rights, and measures to ensure safety are based on this Act, shall be prescribed by Presidential Decree.

[This Article Newly Inserted by Act No. 13423, Jul. 24, 2015]

Article 33 (Privacy Impact Assessment) (1) In the case there is a risk of an infringement with respect to personal information of data subjects due to the operation of personal information files meeting the criteria prescribed by Presidential Decree, the head of a public institution shall conduct an assessment to analyze risk factors and improve them (hereinafter referred to as "privacy impact assessment"), and submit the results thereof to the Protection Commission. In such cases, the head of the public institution shall request the privacy impact assessment from any of the institutions designated by the Protection Commission (hereinafter referred to as "PIA institution"). <Amended by Act No. 11690, Mar. 23, 2013; Act No.

12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>

(2) The privacy impact assessment shall cover the following matters:

1. The number of personal information being processed;
2. Whether the personal information is provided to a third party;
3. The probability to violate the rights of the data subjects and the degree of risks;
4. Other matters prescribed by Presidential Decree.

(3) The Protection Commission may provide its opinion on the results of the privacy impact assessment submitted under paragraph (1).<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>

(4) The head of a public institution shall register the personal information files in accordance with Article 32 (1), for which the privacy impact assessment has been conducted pursuant to paragraph (1), with the results of the privacy impact assessment attached thereto.

(5) The Protection Commission shall take necessary measures, such as fostering relevant specialists, and developing and disseminating criteria for the privacy impact assessment, to promote the privacy

impact assessment.<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

(6) Necessary matters in relation to the privacy impact assessment, such as the criteria for designation as PIA institutions, revocation of designation, assessment criteria, method and procedure, etc. pursuant to paragraph (1), shall be prescribed by Presidential Decree.

(7) Matters regarding the privacy impact assessment conducted by the National Assembly, the Court, the Constitutional Court and the National Election Commission (including their affiliated entities) shall be prescribed by the National Assembly Regulations, the Supreme Court Regulations, the Constitutional Court Regulations, and the National Election Commission Regulations.

(8) A personal information controller other than public institutions shall proactively endeavor to conduct a privacy impact assessment, if there is a risk of an infringement with respect to personal information of data subjects in operating the personal information files.

Article 34 (Data Breach Notification) (1) A personal information controller shall notify data subjects of the following matters without delay when the personal information controller becomes aware their personal information has been divulged:

1. Particulars of the personal information divulged;
2. When and how personal information has been divulged;
3. Any information about how the data subjects can minimize the risk of damage from divulgence, etc.;
4. Countermeasures taken by the personal information controller and remedial procedure;
5. Help desk and contact points for the data subjects to report damage.

(2) A personal information controller shall prepare countermeasures to minimize the risk of damage in the case of divulgence of personal information and take necessary measures.

(3) Where a breach of personal information above the scale prescribed by Presidential Decree takes place, the personal information controller shall, without delay, report the results of notification given under paragraph (1) and the results of measures taken under paragraph (2) to the Protection Commission or a specialized institution designated by Presidential Decree. In such cases, the Protection Commission and the specialized institution designated by Presidential Decree may provide technical assistance for the prevention and recovery of further damage, etc. <Amended by

Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>

(4) Necessary matters in relation to the time, method, and procedure of data breach notification pursuant to paragraph (1), shall be prescribed by Presidential Decree.

Article 34-2 (Imposition, etc. of Penalty Surcharges) (1) The Protection Commission may impose and collect a penalty surcharge not exceeding 500 million won where a personal information controller has failed to prevent any loss, theft, divulgence, forgery, alteration, or damage of resident registration numbers: Provided, That this shall not apply where the personal information controller has fully taken measures necessary to ensure safety under Article 24 (3) to prevent any loss, theft, divulgence, forgery, alteration, or damage of resident registration numbers.

<Amended by Act No. 12844, Nov. 19, 2014; Act No. 13423, Jul. 24, 2015; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

(2) The Protection Commission shall take into account the following when imposing the administrative surcharge pursuant to paragraph (1):<Amended by Act No. 12844, Nov. 19, 2014; Act No. 13423, Jul. 24, 2015; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>

1. Scale of efforts taken to perform the measures necessary to ensure safety under Article 24 (3);
2. Status of the resident registration numbers which have been lost, stolen, divulged, forged, altered or damaged;
3. Fulfillment of subsequent measures to prevent further damage.

(3) The Protection Commission shall collect a late-payment penalty prescribed by Presidential Decree in an amount not exceeding 6/100 per annum of the unpaid administrative surcharge for the period beginning on the following day of the expiration of the payment deadline and ending on the day immediately preceding the day of payment of the administrative surcharge where a person liable to pay the administrative surcharge under paragraph (1) fails to pay the same by the payment deadline. In such cases, the late-payment penalty shall be collected for a maximum period of 60 months.<Amended by Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>

(4) Where a person liable to pay the administrative surcharge under paragraph (1) fails to pay the same by the payment deadline, the Protection Commission shall give notice with the period of payment specified therein; and where the administrative surcharge and late-payment penalty are not

paid within the specified period, the Protection Commission shall collect such administrative surcharge and late-payment penalty in the same manner as delinquent national taxes are collected.<Amended by Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>

(5) Other matters necessary for imposing and collecting penalty surcharges shall be prescribed by Presidential Decree.

[This Article Newly Inserted by Act No. 11990, Aug. 6, 2013]

CHAPTER V GUARANTEE OF RIGHTS OF DATA SUBJECTS

Article 35 (Access to Personal Information) (1) A data subject may request access to his or her own personal information, which is processed by a personal information controller, from the personal information controller.

(2) Notwithstanding paragraph (1), where a data subject intends to request access to his or her own personal information from a public institution, the data subject may request such access directly from the said public institution, or indirectly via the Protection Commission, as prescribed by Presidential Decree.<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No 16930, February. 4, 2020>

(3) Upon receipt of a request for access filed under paragraphs (1) and (2), a personal information controller shall grant the data subject access to his or her own personal information within the period prescribed by Presidential Decree. In such cases, if there is any justifiable ground not to permit access during such period, the personal information controller may postpone access after notifying the relevant data subject of the said ground. If the said ground ceases to exist, the data subject shall be permitted to access the personal information without delay.

(4) In any of the following cases, a personal information controller may limit or deny access after it notifies a data subject of the cause:

1. Where access is prohibited or limited by Acts;
2. Where access may cause damage to the life or body of a third party, or unjustified infringement of property and other interests of any other person;
3. Where a public institution has grave difficulties in performing any of the following duties:
 - (a) Imposition, collection or refund of taxes;

(b) Evaluation of academic achievements or admission affairs at the schools of each level established under the Elementary and Secondary Education Act and the Higher Education Act, lifelong educational facilities established under the Lifelong Education Act, and other higher educational institutions established under other Acts;

(c) Testing and qualification examination regarding academic competence, technical capability and employment;

(d) Ongoing evaluation or decision-making in relation to compensation or grant assessment;

(e) Ongoing audit and examination under other Acts.

(5) Necessary matters in relation to the methods and procedures to file access requests, to limit access, to give notification, etc. pursuant to paragraphs (1) through (4) shall be prescribed by Presidential Decree.

Article 36 (Rectification or Erasure of Personal Information) (1) A data subject who has accessed his or her personal information pursuant to Article 35 may request a correction or erasure of such personal information from the relevant personal information controller: Provided, That the erasure is not permitted where the said personal information shall be collected by other statutes.

(2) Upon receipt of a request by a data subject pursuant to paragraph (1), the personal information controller shall investigate the personal information in question without delay; shall take necessary measures to correct or erase as requested by the data subject unless otherwise specifically provided by other statutes in relation to correction or erasure; and shall notify such data subject of the result.

(3) The personal information controller shall take measures not to recover or revive the personal information in case of erasure pursuant to paragraph (2).

(4) Where the request of a data subject falls under the proviso to paragraph (1), a personal information controller shall notify the data subject of the details thereof without delay.

(5) While investigating the personal information in question pursuant to paragraph (2), the personal information controller may, if necessary, request from the relevant data subject the evidence necessary to confirm a correction or erasure of the personal information.

(6) Necessary matters in relation to the request of correction and erasure, notification method and procedure, etc. pursuant to paragraphs (1), (2) and (4) shall be prescribed by Presidential Decree.

Article 37 (Suspension of Processing of Personal Information) (1) A data subject may request the relevant personal information controller to suspend the processing of his or her personal information. In such cases, if the personal information controller is a public institution, the data subject may request the suspension of processing of only the personal information contained in the personal information files to be registered pursuant to Article 32.

(2) Upon receipt of the request under paragraph (1), the personal information controller shall, without delay, suspend processing of some or all of the personal information as requested by the data subject: Provided, That, where any of the following is applicable, the personal information controller may deny the request of such data subject:

1. Where special provisions in other laws so require or it is inevitable to observe legal obligations;
2. Where access may cause damage to the life or body of a third party, or unjustified infringement of property and other interests of any other person;
3. Where the public institution cannot perform its work as prescribed by any Act without processing the personal information in question;
4. Where it is impracticable to perform a contract such as the provision of services as agreed upon with the said data subject without processing the personal information in question, and the data subject has not clearly expressed the desire to terminate the agreement.

(3) When denying the request pursuant to the proviso to paragraph (2), the personal information controller shall notify the data subject of the reason without delay.

(4) The personal information controller shall, without delay, take necessary measures including destruction of the relevant personal information when suspending the processing of personal information as requested by data subjects.

(5) Necessary matters in relation to the methods and procedures to request the suspension of processing, to deny such request, and to give notification, etc. pursuant to paragraphs (1) through (3) shall be prescribed by Presidential Decree.

Article 38 (Methods and Procedures for Exercise of Rights) (1) A data subject may authorize his or her representative to file requests for access pursuant to Article 35, correction or erasure pursuant to Article 36, suspension of processing pursuant to Article 37, and withdrawal of consent pursuant to Article 39-7 (hereinafter referred to as “request for access, etc.”) by the methods and procedure

prescribed by Presidential Decree, such as written documents. <Amended by Act No 16930, February. 4, 2020>

(2) The legal representative of a child under 14 years of age may file a request for access, etc. to the personal information of the child with a personal information controller.

(3) A personal information controller may demand a fee and postage (only in case of a request to mail the copies), as prescribed by Presidential Decree, from a person who files a request for access, etc.

(4) A personal information controller shall prepare the detailed method and procedure to enable data subjects to file requests for access, etc., and publicly announce such method and procedure so that the data subjects may become aware of them.

(5) A personal information controller shall prepare and provide necessary procedures for data subjects to raise objections regarding the denial of a request for access, etc. from such data subjects.

Article 39 (Responsibility for Compensation) (1) A data subject who suffers damage by reason of a violation of this Act by a personal information controller is entitled to claim compensation from the personal information controller for such damage. In such cases, the said personal information controller may not be released from responsibility for compensation if it fails to prove the non-existence of wrongful intent or negligence.

(2) Deleted.<by Act No. 13423, Jul. 24, 2015>

(3) Where a data subject suffers damage out of loss, theft, divulgence, forgery, alteration, or damage of his or her own personal information, caused by wrongful intent or negligence of a personal information controller, the Court may determine the amount of compensation for damage not exceeding three times such damage: Provided, That the same shall not apply to the personal information controller who has proved non-existence of his or her wrongful intent or negligence.<Newly Inserted by Act No. 13423, Jul. 24, 2015>

(4) The Court shall take into account the following when determining the amount of compensation for damage pursuant to paragraph (3):<Newly Inserted by Act No. 13423, Jul. 24, 2015>

1. The degree of wrongful intent or expectation of damage;
2. The amount of loss caused by the violation;
3. Economic benefits the personal information controller gained in relation to the violation;
4. A fine and a penalty surcharge to be levied subject to the violation;

5. The duration, frequency, etc. of violations;
6. The property of the personal information controller;
7. The personal information controller's efforts to retrieve the affected personal information after the loss, theft, or divulgence of personal information;
8. The personal information controller's efforts to remedy damage suffered by the data subject.

Article 39-2 (Claims for Statutory Compensation) (1) Notwithstanding Article 39 (1), a data subject, who suffers damage out of loss, theft, divulgence, forgery, alteration, or damage of his or her own personal information, caused by wrongful intent or negligence of a personal information controller, may claim a reasonable amount of damages not exceeding three million won. In such cases, the said personal information controller may not be released from the responsibility for compensation if it fails to prove non-existence of his or her wrongful intent or negligence.

(2) In the case of a claim made under paragraph (1), the Court may determine a reasonable amount of damages not exceeding the amount provided for in paragraph (1) taking into account all arguments in the proceedings and the results of examining evidence.

(3) A data subject who has claimed compensation pursuant to Article 39 may change such claim to the claim provided for in paragraph (1) until the closure of fact-finding proceedings.

[This Article Newly Inserted by Act No. 13423, Jul. 24, 2015]

CHAPTER VI SPECIAL CASES CONCERNING PROCESSING OF PERSONAL INFORMATION BY PROVIDERS OF INFORMATION AND COMMUNICATIONS SERVICES OR SIMILAR

Article 39-3 (Special Provisions on Consent to the Collection and Use of Personal Information) (1) Notwithstanding Article 15 (1), an information and communications service provider who intends to collect and use personal information of users shall notify users of the following matters and obtain consent therefor. The same shall apply when changes are made for the following matters:

1. The purpose of the collection and use of personal information;
2. Particulars of personal information to be collected;
3. The period for retaining and using personal information.

(2) An information and communications service provider may collect and use personal information of users without their consent under paragraph (1) in any of the following cases:

1. Where the information is necessary in implementing a contract for provision of information and communications services (referring to the information and communications services defined in Article 2 (1) 2 of the Act on Promotion of Information and Communications Network Utilization and Information Protection; hereinafter the same shall apply), but it is clearly difficult to obtain ordinary consent for economic and technical reasons;

2. Where the information is necessary to calculate fees for the provision of information and communications services;

3. Where special provisions in other laws so require.

(3) No information and communications service provider shall reject the provision of services for the reason that a user does not provide his/her personal information beyond the minimum personal information required. The minimum personal information refers to information that is necessary for the performance of the fundamental functions of the services.

(4) An information and communications provider who intends to obtain consent from children aged under 14 for the collection, use and provision of personal information shall obtain such consent from his/her legal representative and confirm whether the legal representative has granted consent as prescribed by the Presidential Decree. (5) An information and communications provider shall, when notifying children aged under 14 of matters relating to the processing of personal information, use understandable forms and plain and readily comprehensible language.

(6) The Protection Commission shall take measures to protect the personal information of children aged under 14 who may not clearly understand matters such as the risks and results of personal information processing and users' rights.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 39-4 (Special Cases on the Notification and Reporting on the Divulgence of Personal Information) (1) Notwithstanding Article 34 (1) and (3), information and communications service provider and a person who receives personal information of users therefrom pursuant to Article 17 (1) (hereinafter referred to as "information and communications service provider, etc.") shall notify the relevant users of the following matters without delay upon becoming aware that their personal information has been lost, stolen or divulged (hereinafter referred to as "divulgence, etc."), report such case to a specialized institution prescribed by the Protection Commission or Presidential Decree, and shall notify the users or report that matter not later than 24 hours since he or she became aware of such fact, without a justifiable reason: Provided, That if there is a justifiable reason such as users'

contact number being unknown, other measures may be taken in lieu of notification as prescribed by Presidential Decree:

1. Particulars of the personal information divulged, etc.;
2. The time when the personal information has been divulged, etc.;
3. Any measure that users can take;
4. Countermeasures to be taken by of the information and communications service provider, etc.;
5. Department and contact points to which the user can apply for consultation.

(2) A specialized institution prescribed by Presidential Decree which receives a report pursuant to paragraph (1) shall notify the Protection Commission of the case without delay.

(3) An information and communications service provider, etc. shall explain any justifiable reason pursuant to paragraph (1) to the Protection Commission.

(4) Necessary matters in relation to the methods and procedures of notification and reporting under paragraph (1) shall be prescribed by the Presidential Decree.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 39-5 (Special Cases on Safeguards for Personal Information) Information and communications service provider, etc. shall limit the number of persons who process users' personal information to the minimum extent.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 39-6 (Special Cases on the Destruction of Personal Information) (1) Information and communications service provider, etc. shall take necessary measures as prescribed by Presidential Decree such as destruction to protect the personal information of users who have not used information and communications services for one year: Provided, That, if the period is designated otherwise by other statutes or at the request of the user, the designated period shall apply.

(2) Information and communications service provider, etc. shall notify users of matters prescribed by Presidential Decree such as the fact that their personal information will be destroyed, the expiration date, and the particulars of personal information to be destroyed by a method prescribed by Presidential Decree such as e-mail, at least 30 days prior to the expiration of the above designated period.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 39-7 (Special Cases on Users' Rights) (1) Users may withdraw consent to the collection, use and provision of personal information at any time from information and communications service provider, etc.

(2) Information and communications service providers, etc. must make it easier for users to request to withdraw their consent under paragraph (1), to access their information under Article 35, and to rectify under Article 36 than to give consent to the collection of their personal information.

(3) Once a user withdraws his or her consent pursuant to paragraph (1), the information and communications service provider, etc. shall take necessary measures without delay such as destroying the information to such an extent that it is not recoverable or revivable.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 39-8 (Notification of the Use History of Personal Information) (1) Information and communications service provider, etc. meeting standards prescribed by President Decree shall notify users of the use history of their personal information collected pursuant to Articles 23 and 39-3 (including provision pursuant to Article 17) on a regular basis: Provided, That this shall not apply where the collected information does not include a contact number, etc. that enables notification to users, (2) The type of information to be notified to users under paragraph (1), the types of information to be notified, the frequency and method of notification, and other matters necessary for the notification of the details shall be determined by Presidential Decree.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 39-9 (Indemnity for Losses) (1) Information and communications service providers, etc. shall take necessary measures such as purchasing insurance or deduction plans or accumulating reserves to fulfil its liabilities for compensation pursuant to Articles 39 and 39-2.

(2) Necessary matters including the scope of personal information controllers subject to the obligation pursuant to paragraph (1) and relevant standards shall be prescribed by Presidential Decree.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 39-10 (Deletion and Blocking of Exposed Personal Information) (1) Information and communications service provider, etc. shall ensure that users' personal information including resident registration number, bank account information and credit card information is not exposed to the public through information and communications networks.

(2) Notwithstanding paragraph (1), at the request of the Protection Commission or specialized institutions designated by Presidential Decree in relation to personal information exposed to the public, information and communications service provider, etc. shall take necessary measures such as deleting and blocking.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 39-11 (Designation of Domestic Agents) (1) Information and communications service provider, etc. with no address or business office in Korea meeting the criteria prescribed by Presidential Decree in consideration of the number of users and revenues shall designate an agent to act on his or her behalf with respect to the following (hereinafter referred to as "domestic agent") in writing:

1. Duties of a privacy officer under Article 31;
2. Notification and reporting under Article 39-4;
3. Submission of related articles, documents, etc. under Article 63 (1).

(2) A domestic agent shall have an address or business office in Korea.

(3) When a domestic agent is designated pursuant to paragraph (1), the following matters shall all be included in the Privacy Policy pursuant to Article 30:

1. Name of the domestic agent (for a corporation, the title and name of the representative);
2. Address of the domestic agent (for a corporation, location of a business office), telephone number, e-mail address.

(4) If the domestic agent violates this Act in relation to each item of paragraph (1), the information and communications service provider, etc. shall be deemed to have committed such a violation.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 39-12 (Protection of Information Transferred Overseas) (1) The information and communications service provider, etc. shall not execute an international contract in violation of this Act in relation to users' personal information.

(2) Notwithstanding Article 17 (3), information and communications service provider, etc. shall obtain users' consent if intending to provide (including accessing), outsource the processing of, or store (hereinafter referred to as "transfer" in this Article) users' personal information overseas: Provided, That if all items of paragraph (3) below are made public pursuant to Article 30 (2) or notified to users

by a method prescribed by the Presidential Decree such as e-mail, the information and communications service provider, etc. may opt not to obtain users' consent to outsourcing the processing of, or storing, personal information. (3) The information and communications service provider, etc. shall notify users of the following matters in advance if intending to obtain consent under paragraph (2): 1. Particulars of the personal information to be transferred;

2. The country to which the personal information is transferred, transfer date and method;

3. Name of the entity to which the personal information is transferred (referring to the name of a corporation and the contact information of the person responsible for the management of information, if the person is a corporation);

4. The purpose of using personal information by the entity to which the information is transferred and the period of retaining and using personal information.

(4) The information and communications service provider, etc. shall implement safeguards as prescribed by Presidential Decree if intending to transfer personal information overseas with consent obtained pursuant to paragraph (2).

(5) where a person who receives personal information of the users transfers it to a third country, he or she shall comply with paragraphs (1) through (4). In such cases, "information and communications service providers, etc." shall be regarded as "personal information recipient," and "personal information recipient" shall be regarded as "a person who receives personal information from a third country. [This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 39-13 (Reciprocity) Notwithstanding Article 39-12, information and communications service providers, etc. in a country that restricts cross-border transfer may face an equivalent level of restrictions in another country: Provided, That this shall not apply where cross-border transfer is necessary to implement a pact or other international arrangements.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 39-14 (Special Cases for Broadcasting Service Providers) If entities falling under subparagraphs 3 (a) through (e), 6, 9, 12 and 14 of Article 2 of the Broadcasting Act (hereinafter referred to as "broadcasting service provider, etc.") process the personal information of viewers, the broadcasting service provider, etc.

shall observe regulations applicable to an information and communications service provider, etc. In such cases, “broadcasting service provider, etc.” shall be deemed to be “information and communications service provider, etc.” and “viewers” to be “users.”

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 39-15 (Special Cases for the Imposition of Administrative Surcharges) (1) Upon information and communications service provider, etc. conducting any of the following acts, the Protection Commission may impose administrative surcharges not exceeding 3/100 of the total revenues relating to the concerned violation:

1. Using or providing personal information in violation of Articles 17 (1), 17 (2), 18 (1), 18 (2), and 19 (including applicable cases pursuant to Article 39-14);
2. Collecting personal information of a child aged under 14 without his/her legal representative’s consent in violation of Article 22 (6) (including applicable cases pursuant to Article 39-14);
3. Collecting sensitive information without the user’s consent in violation of Article 23 (1) 1 (including applicable cases pursuant to Article 39-14);
4. Where it neglects its control, supervision, or education under Article 26 (4) (including where the aforesaid provisions apply mutatis mutandis pursuant to Article 39-14), thereby causing an outsourcee subject to special cases to violate this Act;
5. Losing, stealing, divulging, forging, altering, or damaging users’ personal information and failing to take measures (excluding matters on the establishment of internal management plan) set forth in Article 29 (including applicable cases pursuant to Article 39-14);
6. Collecting users’ personal information without their consent in violation of Article 39-3 (1) (including applicable cases pursuant to Article 39-14);
7. Providing users’ personal information overseas without their consent in violation of the main clause of Article 39-12 (2) (including applicable cases pursuant to paragraph (5) of the same Article).

(2) When administrative surcharges are imposed in accordance to paragraph (1), but the information and communications service provider, etc. either refuses to submit basic materials for revenue calculation or submits false documents, their revenues may be estimated based on the accounting documents, such as financial statements, and operational status, such as the number of subscribers and usage fees, of similarsized information and communications service providers, etc.: Provided, That up to 400 won million may be imposed as administrative surcharges on an information and

communications service provider, etc. having no revenues or revenues difficult to calculate as prescribed by Presidential Decree.

(3) The Protection Commission shall consider the following matters to impose administrative surcharges under paragraph (1):

1. Details and degree of the violation;
2. Period and number of the violation;
3. Size of profits gained from the violation.

(4) Administrative surcharges under paragraph (1) shall be calculated in consideration of paragraph (3), but the detailed calculation standards and procedures shall be prescribed by Presidential Decree.

(5) The Protection Commission shall collect a late-payment penalty in the amount not exceeding 6/100 per annum of the unpaid administrative surcharges for the period beginning on the following day of the expiration of the payment deadline.

(6) Where a person liable to pay the administrative surcharges under paragraph (1) fails to pay it by the payment deadline, the Protection Commission shall give notice with the period of payment specified in it; and where the administrative surcharges and late-payment penalty under paragraph (5) are not paid within the specified period, the Protection Commission shall collect such administrative surcharges and late-payment penalty in the same manner as delinquent national taxes are collected.

(7) When the administrative surcharges imposed according to paragraph (1) are refunded for such reasons as a court's decision, the Protection Commission shall make additional payments in the amount calculated based on the interest rate prescribed by Presidential Decree considering the deposit interest rates of financial companies, etc., for the period beginning on the following day of the payment of administrative surcharges and ending on the day of the refund.

(8) Notwithstanding paragraph (7), when a disposition of imposing administrative surcharges is revoked due to a court's decision and new administrative surcharges are imposed based on the reasoning of the decision, additional payments shall be calculated and paid with respect to the amount that remains after the newly imposed administrative surcharges are deducted from the already paid administrative surcharges.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

CHAPTER VII PERSONAL INFORMATION DISPUTE MEDIATION COMMITTEE

Article 40 (Establishment and Composition) (1) There shall be established a Personal Information Dispute Mediation Committee (hereinafter referred to as the “Dispute Mediation Committee”) to mediate disputes over personal information.

(2) The Dispute Mediation Committee shall be comprised of not more than 20 members, including one chairperson, and the members shall be ex officio members and commissioned members. <Amended by Act No. 13423, Jul. 24, 2015>

(3) The commissioned members shall be commissioned by the Chairperson of the Protection Commission from among the following persons, and public officials of the national agencies prescribed by Presidential Decree shall be ex officio members: <Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 13423, Jul. 24, 2015>

1. Persons who previously served as members of the Senior Executive Service of the central administrative agencies in charge of personal information protection, or persons who presently work or have worked at equivalent positions in the public sector and related organizations, and have job experience in personal information protection;

2. Persons who presently serve or have served as associate professors or higher positions in universities or in publicly recognized research institutes;

3. Persons who presently serve or have served as judges, public prosecutors, or attorneys-at-law;

4. Persons recommended by data protection-related civic organizations or consumer groups;

5. Persons who presently work or have worked as senior officers for the trade associations comprised of personal information controllers.

(4) The chairperson shall be commissioned by the Chairperson of the Protection Commission from among Committee members who are not public officials. <Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 13423, Jul. 24, 2015>

(5) The term of office for the chairperson and commissioned members shall be two years, and their term may be renewable for one further term.<Amended by Act No. 13423, Jul. 24, 2015>

(6) In order to conduct dispute settlement efficiently, the Dispute Mediation Committee may, if necessary, establish a mediation panel that is comprised of not more than five Committee members in each sector of mediation cases, as prescribed by Presidential Decree. In this case, the resolution of the mediation panel delegated by the Dispute Mediation Committee shall be construed as that of the Dispute Mediation Committee.

(7) The quorum for holding a Dispute Mediation Committee or a mediation panel shall be the presence of a majority of its members, and any resolution shall require the affirmative votes of a majority of the members present.

(8) The Protection Commission may deal with the administrative affairs necessary for dispute mediation, such as receiving dispute mediation cases and fact-finding. <Amended by Act No. 13423, Jul. 24, 2015>

(9) Except as otherwise expressly provided for in this Act, matters necessary to operate the Dispute Mediation Committee shall be prescribed by Presidential Decree.

Article 41 (Guarantee of Members' Status) None of the Committee members shall be dismissed or de-commissioned against his or her will except when he or she is sentenced to the suspension of qualification or a heavier punishment, or unable to perform his or her duties due to mental or physical incompetence.

Article 42 (Exclusion, Recusal, and Refrainment of Members) (1) A member of the Dispute Mediation Committee shall be excluded from participating in the deliberation and resolution of a case requested for dispute mediation pursuant to Article 43 (1) (hereafter in this Article referred to as "case") if:

1. The member or his/her current or former spouse is a party to the case or is a joint right holder or a joint obligator with respect to the case;
2. The member is or was a relative of a party to the case;
3. The member has given any testimony, expert opinion, or legal advice with respect to the case;
4. The member is or was involved in the case as an agent or representative of a party to the case.

(2) Where any party finds it impracticable to expect a fair deliberation and resolution from a Committee member, such party may file an application for recusal with the chairperson. In such cases, the chairperson shall determine with respect to such application for recusal without any resolution of the Dispute Mediation Committee. (3) Where any committee member falls under the case of paragraph (1) or (2), he/she may refrain from the deliberation and resolution of the case.

Article 43 (Application for Mediation) (1) Any person who wishes a dispute over personal information mediated may apply for mediation of the dispute to the Dispute Mediation Committee.

(2) Upon receipt of an application for dispute mediation from a party to the case, the Dispute Mediation Committee shall notify the counterparty of the application for mediation.

(3) Where a public institution is notified of dispute mediation under paragraph (2), the public institution shall respond to it unless there are extraordinary circumstances.

Article 44 (Time Limitation of Mediation Proceedings) (1) The Dispute Mediation Committee shall examine the case and prepare a draft mediation decision within 60 days from the date of receiving an application pursuant to Article 43 (1); Provided, That the Dispute Mediation Committee may pass a resolution to extend such period by reason of inevitable circumstances.

(2) Where the period is extended pursuant to the proviso to paragraph (1), the Dispute Mediation Committee shall inform the applicant of the reasons for extending the period and other matters concerning the extension of such period.

Article 45 (Request for Materials) (1) Upon receipt of an application for dispute mediation pursuant to Article 43 (1), the Dispute Mediation Committee may request disputing parties to provide materials necessary to mediate the dispute. In such cases, such parties shall comply with the request unless any justifiable ground exists.

(2) The Dispute Mediation Committee may require disputing parties or relevant witnesses to appear before the Committee to hear their opinions, if deemed necessary.

Article 46 (Settlement Advice before Mediation) Upon receipt of an application for dispute mediation pursuant to Article 43 (1), the Dispute Mediation Committee may present a draft settlement to the disputing parties and recommend a settlement before mediation.

Article 47 (Dispute Mediation) (1) The Dispute Mediation Committee may prepare a draft mediation decision including the following matters:

1. Suspension of the violation to be investigated;
2. Restitution, compensation and other necessary remedies;
3. Any measure necessary to prevent recurrence of the identical or similar violations.

(2) Upon preparing a draft mediation pursuant to paragraph (1), the Dispute Mediation Committee shall present the draft mediation to each party without delay.

(3) Each party presented with the draft mediation decision prepared under paragraph (1) shall notify the Dispute Mediation Committee of his/her acceptance or denial of the draft mediation decision within 15 days from the date of receipt of such draft mediation decision, without which such mediation shall be deemed rejected.

(4) If the parties accept the draft mediation decision, the Dispute Mediation Committee shall prepare a written mediation decision, and the chairperson of the Dispute Mediation Committee and the parties shall have their names and seals affixed thereon.

(5) The mediation agreed upon pursuant to paragraph (4) shall have the same effect as a settlement before the court.

Article 48 (Rejection and Suspension of Mediation) (1) Where the Dispute Mediation Committee deems that it is inappropriate to mediate any dispute in view of its nature, or that an application for mediation of any dispute is filed for an unfair purpose, it may reject the mediation. In this case, the reasons for rejecting the mediation shall be notified to the applicant.

(2) If one of the parties files a lawsuit while mediation proceedings are pending, the Dispute Mediation Committee shall suspend the dispute mediation and notify the parties thereof.

Article 49 (Collective Dispute Mediation) (1) The State, a local government, a data protection organization or institution, a data subject, and a personal information controller may request or apply for a collective dispute mediation (hereinafter referred to as “collective dispute mediation”) to the Dispute Mediation Committee where damages or infringement on rights occur to multiple data subjects in an identical or similar manner, and such incident is such as prescribed by Presidential Decree.

(2) Upon receipt of a request or an application for collective dispute mediation under paragraph (1), the Dispute Mediation Committee may commence, by its resolution, collective dispute mediation proceedings pursuant to paragraphs (3) through (7). In such cases, the Dispute Mediation Committee shall publicly announce the commencement of such proceedings for a period prescribed by Presidential Decree.

(3) The Dispute Mediation Committee may accept an application from any data subject or personal information controller other than the parties to the collective dispute mediation to participate in the collective dispute mediation additionally as a party.

(4) The Dispute Mediation Committee may, by its resolution, select one or a few persons as a representative party, who most appropriately represents the common interest among the parties to the collective dispute mediation pursuant to paragraphs (1) and (3).

(5) When the personal information controller accepts a collective dispute mediation award presented by the Dispute Mediation Committee, the Dispute Mediation Committee may advise the personal

information controller to prepare and submit a compensation plan for the benefit of the non-party data subjects suffered from the same incident.

(6) Notwithstanding Article 48 (2), if a group of data subjects among a multitude of data subject parties to the collective dispute mediation files a lawsuit before the court, the Dispute Mediation Committee shall not suspend the proceedings but exclude the relevant data subjects, who have filed the lawsuit, from the proceedings. (7) The period for collective dispute mediation shall not exceed 60 days from the following day when public announcement referred to in paragraph (2) ends: Provided, That the period can be extended by the resolution of the Dispute Mediation Committee in extenuating circumstances.

(8) Other necessary matters, such as the procedures for collective dispute mediation, shall be prescribed by Presidential Decree.

Article 50 (Mediation Procedures) (1) Except as otherwise expressly provided for in Articles 43 through 49, the method and procedures to mediate disputes and matters necessary to deal with such dispute mediation shall be prescribed by Presidential Decree.

(2) Except as otherwise expressly provided for in this Act, the Judicial Conciliation of Civil Disputes Act shall apply mutatis mutandis to the operation of the Dispute Mediation Committee and dispute mediation proceedings.

CHAPTER VIII CLASS-ACTION LAWSUIT OVER DATA INFRINGEMENT

Article 51 (Parties to Class Action Lawsuit) Any of the following organizations may file a lawsuit (hereinafter referred to as “class action lawsuit”) with the court to prevent or suspend an infringement with respect to personal information if a personal information controller rejects or would not accept the collective dispute mediation under Article 49:

1. A consumer group registered with the Fair Trade Commission pursuant to Article 29 of the Framework Act on Consumers that meets all of the following criteria:

(a) Its by-laws shall constantly state the purpose to augment the rights and interests of data subjects;

(b) The number of full members shall exceed 1000;

(c) Three years shall have passed since the registration under Article 29 of the Framework Act on Consumers;

2. A non-profit, non-governmental organization referred to in Article 2 of the Assistance for Non-Profit, Non-Governmental Organizations Act that meets all of the following criteria:

- (a) At least 100 data subjects, who experienced the same infringement as a matter of law or fact, shall submit a request to file a class action lawsuit;
- (b) Its by-laws shall state the purpose of data protection and it has conducted such activities for the most recent 3 years;
- (c) The number of regular members shall be at least 5000;
- (d) It shall be registered with any central administrative agency.

Article 52 (Exclusive Jurisdictions) (1) A class action lawsuit shall be subject to the exclusive jurisdiction of the competent district court (panel of judges) at the place of business or main office, or at the address of the business manager in the case of no business establishment, of the defendant.

(2) Where paragraph (1) applies to a foreign business entity, the same shall be determined by the place of business or main office, or the address of the business manager located in the Republic of Korea.

Article 53 (Retention of Litigation Attorney) The plaintiff of a class-action lawsuit shall retain an attorney-at-law as a litigation attorney.

Article 54 (Application for Permission of Lawsuit) (1) An organization that intends to file a class action shall submit to the court an application for permission of lawsuit describing the following in addition to the complaint:

1. Plaintiff and his or her litigation attorney;
2. Defendant;
3. Detailed violation of the rights of data subjects.

(2) An application for certification of lawsuit filed under paragraph (1) shall be accompanied by the following materials:

1. Materials that prove that the organization which has filed a lawsuit meets all criteria provided for in Article 51;
2. Documentary evidence that proves that the personal information controller has rejected the dispute mediation or would not accept the mediation award.

Article 55 (Requirements for Permission of Lawsuit) (1) The court shall permit a class action only when all of the following requirements are satisfied:

1. That the personal information controller has rejected the dispute mediation or would not accept the mediation award;

2. That none of the descriptions in the application for permission of lawsuit filed under Article 54 is defective.

(2) The court decision that permits, or refuses to permit, a class action may be challenged through immediate appeal.

Article 56 (Effect of Conclusive Judgment) When a judgment dismissing a plaintiff's complaint becomes conclusive, any other organizations provided for in Article 51 cannot file a class-action lawsuit regarding the identical case: Provided, That this shall not apply in any of the following circumstances:

1. Where, after the judgment became conclusive, new evidence has been found by the State, a local government, or a State or local government-invested institution regarding the said case;

2. Where the judgment dismissing the lawsuit proves to have been caused intentionally by the plaintiff.

Article 57 (Application of Civil Procedure Act) (1) Except as otherwise expressly provided for in this Act, the Civil Procedure Act shall apply to a class action.

(2) When a decision to permit a class action lawsuit is made under Article 55, a preservation order provided for in PART IV of the Civil Execution Act may be issued.

(3) Matters necessary for class action lawsuit proceedings shall be provided by the Supreme Court Regulations.

CHAPTER IX SUPPLEMENTARY PROVISIONS

Article 58 (Partial Exclusion of Application) (1) Chapter III through VII shall not apply to any of the following personal information:

1. Personal information collected pursuant to the Statistics Act for processing by public institutions;

2. Personal information collected or requested to be provided for the analysis of information related to national security;

3. Personal information processed temporarily where it is urgently necessary for the public safety and security, public health, etc.;

4. Personal information collected or used for its own purposes of reporting by the press, missionary activities by religious organizations, and nomination of candidates by political parties, respectively.

(2) Articles 15, 22, 27 (1) and (2), 34, and 37 shall not apply to any personal information that is processed by means of the visual data processing devices

installed and operated at open places pursuant to Article 25 (1).

(3) Articles 15, 30 and 31 shall not apply to any personal information that is processed by a personal information controller to operate a group or association for friendship, such as an alumni association and a hobby club.

(4) In the case of processing personal information pursuant to paragraph (1), a personal information controller shall process the personal information to the minimum extent necessary to attain the intended purpose for the minimum period; and shall also make necessary arrangements, such as technical, managerial and physical safeguards, individual grievance handling and other necessary measures for the safe management and appropriate processing of such personal information.

Article 58-2 (Exemption from Application) This Act shall not apply to information that no longer identifies a certain individual when combined with other information, reasonably considering time, cost, technology, etc.

[This Article Newly Inserted by Act No. 16930, Feb. 4, 2020]

Article 59 (Prohibited Activities) Anyone who processes or has processed personal information shall be prohibited from undertaking any of the following activities:

1. To acquire personal information or to obtain consent to personal information processing by fraud, improper or unjust means;
2. To divulge personal information acquired in the course of business, or to provide it for any third party's use without authority;
3. To damage, destroy, alter, forge, or divulge other's personal information without legal authority or beyond proper authority.

Article 60 (Confidentiality) Any person who performs or has performed the following affairs shall not divulge any confidential information acquired in the course of performing his or her duties to any other person, nor use such information for any purpose other than for his or her duties: Provided, That, the same shall not apply where specific provisions exist in other Acts: <Amended by Act No. 16930, Feb. 4, 2020> 1. Affairs of the Protection Commission provided for in Article 8;

1-2. Certification of personal information protection provided for in Article 32-2;

2. Impact assessments provided for in Article 33;

3. Dispute mediation of the Dispute Mediation Committee established under Article 40.

Article 61 (Suggestions and Recommendations for Improvements) (1) The Protection Commission may provide its opinion to any relevant agency through deliberation and resolution where it is deemed necessary with respect to the statutes or municipal ordinances containing provisions that are likely to affect the protection of personal information. <Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, February. 4, 2020>

(2) The Protection Commission may advise a personal information controller to improve the status of personal information processing where doing so is deemed necessary to protect personal information. In such cases, upon receiving the advice, the personal information controller shall make sincere efforts to comply with the advice, and shall inform the Protection Commission of the results. <Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

(3) The head of a related central administrative agency may recommend that a personal information controller improve the status of personal information processing pursuant to the statutes under the related central administrative agency's jurisdiction where doing so is deemed necessary to protect personal information. In such cases, upon receiving the recommendation, the personal information controller shall make sincere efforts to comply with the recommendation, and shall inform the head of the related central administrative agency of the results.

(4) Central administrative agencies, local governments, the National Assembly, the Court, the Constitutional Court, and the National Election Commission may provide their opinions, or provide guidance or inspection with respect to the protection of personal information to their affiliated entities and the public institutions under their jurisdiction.

Article 62 (Reporting on Infringements) (1) Anyone who suffers infringement of rights or interests relating to his or her personal information in the course of personal information processing by a personal information controller may report such infringement to the Protection Commission. <Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

(2) The Protection Commission may designate a specialized institution in order to efficiently receive and handle the claim reports pursuant to paragraph (1), as prescribed by Presidential Decree. In such cases, such specialized institution shall establish and operate a personal information infringement call

centre (hereinafter referred to as the “Privacy Call Center”). <Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

(3) The Privacy Call Center shall perform the following duties:

1. To receive claim reports and provide consultation in relation to personal information processing;
2. To investigate and confirm incidents and hear opinions of related parties;
3. Duties incidental to subparagraphs 1 and 2.

(4) The Protection Commission may, if necessary, dispatch its public official to the specialized institution designated under paragraph (2) pursuant to Article 32-4 of the State Public Officials Act in order to efficiently investigate and confirm the incidents pursuant to paragraph (3) 2. <Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

Article 63 (Requests for Materials and Inspections) (1) The Protection Commission may request relevant materials, such as articles and documents, from a personal information controller in any of the following cases: <Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020> 1. Where any violation of this Act is found or suspected;

2. Where any violation of this Act is reported or a civil complaint thereon is received;
3. In cases prescribed by Presidential Decree where it is necessary to protect the personal information of data subjects.

(2) Where a personal information controller fails to furnish materials pursuant to paragraph (1) or is regarded as having violated this Act, the Protection Commission may require its public official to enter the offices or places of business of the personal information controller and other persons related to such violation to inspect the status of business operations, ledgers, documents, etc. In such cases, the public official who conducts the inspection shall carry a certificate indicating his/her authority and show it to the related persons. <Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 13423, Jul. 24, 2015; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

(3) The head of a related central administrative agency may, in accordance with statutes under the related central administrative agency’s jurisdiction, request materials from a personal information controller pursuant to paragraph (1), or may inspect the personal information controller and other

persons related to the relevant violation of such statutes pursuant to paragraph (2). <Amended by Act No. 13423, Jul. 24, 2015>

(4) Upon discovering any violation of this Act or becoming aware of any suspected violation of this Act, the Protection Commission may demand that the head of the related central administrative agency (if there is a corporation authorized to conduct inspection in accordance with the direction and supervision of the head of the related central administrative agency, this refers to the corporation) investigate the personal information controller after setting a specific scope, and if necessary, request a public official under the Protection Commission to jointly engage in the investigation. In such cases, upon receiving such demand, the head of the related central administrative agency shall comply therewith unless there are extraordinary circumstances. <Amended by Act No. 16930, Feb. 4, 2020>

(5) The Protection Commission may request the head of the related central administrative agency (if there is a corporation authorized to conduct inspection in accordance with the direction and supervision of the head of the related central administrative agency, this refers to the corporation) to take corrective measures on the relevant personal information processor with regard to the result of the inspection conducted pursuant to paragraph (4) or provide opinions on dispositions, etc. <Amended by Act No. 16930, Feb. 4, 2020>

(6) Matters concerning the methods, procedures, etc. for paragraphs (4) and (5) shall be prescribed by Presidential Decree. <Amended by Act No. 16930, Feb. 4, 2020>

(7) The Protection Commission may inspect the status of personal information protection jointly with the head of a related central administrative agency for the prevention of personal information breach incidents and efficient response. <Newly Inserted by Act No. 13423, Jul. 24, 2015; Amended by Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

(8) The Protection Commission and the head of the related central administrative agency shall not provide any third party with the documents, materials, etc. furnished or collected pursuant to paragraphs (1) and (2), nor disclose them to the general public, except as otherwise required by this Act. <Newly Inserted by Act No. 16930, Feb. 4, 2020>

(9) Where receiving materials via information and communications networks, or digitalizing the collected materials, etc., the Protection Commission and the head of the related central administrative agency shall take systematic and technical security measures to prevent the breach of personal information, trade secrets, etc. <Newly Inserted by Act No. 16930, Feb. 4, 2020>

Article 64 (Corrective Measures) (1) Where the Protection Commission deems that there is substantial ground to deem that there has been infringement with respect to personal information, and failure to take action is likely to cause damage that is difficult to remedy, it may order the violator of this Act (excluding central administrative agencies, local governments, the National Assembly, the Court, the Constitutional Court, and the National Election Commission) to take any of the following measures:
<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

1. To suspend infringement with respect to personal information;
2. To temporarily suspend personal information processing;
3. Other measures necessary to protect personal information and to prevent personal information infringement.

(2) Where the head of a related central administrative agency deems that there is substantial ground to deem that there has been an infringement of personal information, and failure to take action is likely to cause damage that is difficult to remedy, he or she may order a personal information controller to take any of the measures provided for in paragraph (1) pursuant to the statutes under such related central administrative agency's jurisdiction.

(3) A local government, the National Assembly, the Court, the Constitutional Court, or the National Election Commission may order their affiliated entities and public institutions, which are found to have violated this Act, to take any of the measures provided for in paragraph (1).

(4) When a central administrative agency, a local government, the National Assembly, the Court, the Constitutional Court, or the National Election Commission violates this Act, the Protection Commission may recommend the head of the relevant agency to take any of the measures provided for in paragraph (1). In such cases, upon receiving the recommendation, the agency shall comply therewith unless there are extraordinary circumstances.

Article 65 (Accusation and Recommendation for Disciplinary Action) (1) When there is deemed substantial ground for suspecting a criminal violation of this Act or other data protection-related statutes, the Protection Commission may make an accusation to the competent investigative agency.
<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

(2) When there is deemed substantial ground for deeming that there has been a violation of this Act or other data protection-related statutes, the Protection Commission may recommend the relevant

personal information controller to take disciplinary action against the person responsible for such violation (including the representative and the executive officer in charge). In such cases, upon receiving the recommendation, the relevant personal information controller shall comply therewith, and notify the Protection Commission of the results.<Amended by Act No. 11690, Mar. 23, 2013; Act No. 11990, Aug. 6, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

(3) The head of a related central administrative agency may file a criminal complaint against a personal information controller pursuant to paragraph (1), or recommend that the head of an affiliated agency, organization, etc. take disciplinary action pursuant to paragraph (2), in accordance with the statutes under the central administrative agency' s jurisdiction. In such cases, upon receiving the recommendation under paragraph (2), the head of an affiliated agency, organization, etc. shall comply therewith, and notify the head of the related central administrative agency of the results.

Article 66 (Disclosure of Results) (1) The Protection Commission may disclose the recommendation for improvement pursuant to Article 61; the order to take corrective measures pursuant to Article 64; the accusation or recommendation to take disciplinary action pursuant to Article 65; and the imposition of administrative fines pursuant to Article 75 and the results thereof. <Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

(2) The head of a related central administrative agency may disclose the matters provided for in paragraph (1) in accordance with the statutes under the central administrative agency' s jurisdiction.

(3) The method, criteria, procedure, etc. for disclosure pursuant to paragraphs (1) and (2) shall be prescribed by Presidential Decree.

Article 67 (Annual Reports) (1) The Protection Commission shall prepare a report each year, based on necessary materials furnished by related agencies, etc., in relation to the establishment and implementation of personal information protection policy measures, and submit (including transmission via an information and communications networks) it to the National Assembly before the opening of the regular session.

(2) The annual report referred to in paragraph (1) shall contain the following matters:<Amended by Act No. 14107, Mar. 29, 2016>

1. Infringement on the rights of data subjects and the status of remedies thereof;
2. Results of the survey in relation to the status of personal information processing;

3. Status of implementation of the personal information protection policy measures and achievements;
4. Global legislative and policy trends regarding personal information;
5. Status of the enactment and amendment of Acts, Presidential Decrees, the National Assembly Regulations, the Supreme Court Regulations, the Constitutional Court Regulations, the National Election Commission Regulations, and the Board of Audit and Inspection Regulations, in relation to processing of resident registration numbers;
6. Other matters to be disclosed or reported in relation to the personal information protection policy.

Article 68 (Delegation and Entrustment of Authority) (1) The authority of the Protection Commission or the head of a related central administrative agency under this Act may in part be delegated or entrusted, as prescribed by Presidential Decree, to the Special Metropolitan City Mayor, Metropolitan City Mayors, Do Governors, Special Self-Governing Province Governors, or the specialized institutions prescribed by Presidential Decree. <Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, February. 4, 2020>

(2) The agencies to which the authority of the Protection Commission or the head of a related central administrative agency has been partially delegated or entrusted pursuant to paragraph (1) shall notify the Protection Commission or the head of the related central administrative agency of the results of performing the affairs delegated or entrusted.<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

(3) Where delegating or entrusting a part of the authority to a specialized institution pursuant to paragraph (1), the Protection Commission may provide a contribution to the special institution to cover expenses incurred in performing the affairs.<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

Article 69 (Persons Deemed to be Public Officials for Purposes of Penalty Provisions) (1) Among the Commissioners of the Protection Commission, Commissioners other than public officials and employees other than public officials shall be deemed a public official for the purposes of applying penalty under the Criminal Act or other statutes. <Newly Inserted by Act No. 16930, Feb. 4, 2020>

(2) Any executive or employee of a relevant agency that performs the affairs entrusted by the Protection Commission or the head of a related central administrative agency shall be deemed a public official for the purposes of Articles 129 through 132 of the Criminal Act.<Newly Inserted by Act No. 16930, Feb. 4, 2020>

CHAPTER X PENALTY PROVISIONS

Article 70 (Penalty Provisions) Any of the following persons shall be punished by imprisonment with labor for not more than 10 years, or by a fine not exceeding 100 million won: <Amended by Act No. 13423, Jul. 24, 2015>

1. A person who causes the suspension, paralysis or other severe hardship of work of a public institution by altering or erasing the personal information processed by the public institution for the purpose of disturbing the personal information processing of such public institution;
2. A person who obtains any personal information processed by third parties by fraud or other unjust means or methods and provides it to a third party for a profit-making or unjust purpose, and a person who abets or arranges such conduct.

Article 71 (Penalty Provisions) Any of the following persons shall be punished by imprisonment with labour for not more than 5 years, or by a fine not exceeding 50 million won: <Amended by Act No. 14107, Mar. 29, 2016; Act No. 16930, Feb. 4, 2020>

1. A person who provides personal information to a third party without the consent of a data subject in violation of Article 17 (1) 1 even though Article 17 (1) 2 is not applicable, and a person who knowingly receives such personal information;
2. A person who uses personal information or provides personal information to a third party in violation of Articles 18 (1) and (2) (including where the aforesaid provisions apply mutatis mutandis pursuant to Article 39-14), 19, 26 (5), 27 (3), or 28-2 and a person who knowingly receives such personal information for a profit-making or unfair purpose;
3. A person who processes sensitive information in violation of Article 23 (1);
4. A person who processes personally identifiable information in violation of Article 24 (1);
- ~~4- 2.~~ A person who processes or provides a third party with pseudonymised information in violation of Article 28-3, and a person who knowingly receives such pseudonymised information for profit-making or unfair purposes;
- ~~4- 3.~~ A person who processes pseudonymised information for the purpose of identifying a certain individual in violation of Article 28-5 (1);
- ~~4- 4.~~ An information and communications service provider who uses or provides a third party with personal information without taking necessary measures for correction or deletion requests (including necessary measures to be taken in accordance with a request for access, etc. provided for

in Article 38 (2)) pursuant to Article 36 (2) (including a person to whom personal information has been transferred from information and communications service provider, etc. pursuant to Article 27 and applicable cases pursuant to Article 39-14);

~~4- 5.~~ A person who collects personal information without users' consent in violation of Article 39-3 (1) (including where the aforesaid provisions apply mutatis mutandis pursuant to Article 39-14);

~~4- 6.~~ A person who collects the personal information of children aged under 14 without his or her legal representative's consent or without confirming whether the legal representative has given consent or not in violation of Article 39-3 (4) (including applicable cases pursuant to Article 39-14);

5. A person who divulges personal information acquired in the course of business or provides it for any other person's use without authority in violation of subparagraph 2 of Article 59, and a person who knowingly receives such personal information for a profit-making or unfair purposes;

6. A person who damages, destroys, alters, forges, or divulges any third party's personal information in violation of subparagraph 3 of Article 59.

Article 72 (Penalty Provisions) Any of the following persons shall be punished by imprisonment with labor for not more than 3 years, or by a fine not exceeding 30 million won:

1. A person who arbitrarily handles visual data processing devices for any purpose other than the purpose for which the device was installed, directs such devices toward different spots, or uses a sound recording function in violation of Article 25 (5);

2. A person who acquires personal information or obtains consent to personal information processing by fraud or other unjust means in violation of subparagraph 1 of Article 59, and a person who knowingly receives such personal information for a profit-making or unfair purpose;

3. A person who divulges confidential information acquired while performing his or her duties, or uses such information for purposes other than for the purpose of discharging his/her duties in violation of Article 60.

Article 73 (Penalty Provisions) Any of the following persons shall be punished by imprisonment with labor for not more than 2 years, or by a fine not exceeding 20 million won:<Amended by Act No. 13423, Jul. 24, 2015; Act No. 14107, Mar. 29, 2016; Act No. 16930, Feb. 4, 2020>

1. A person who fails to take necessary measures to ensure safety in violation of Article 23 (2), 24 (3), 25 (6), 28-4 (1), or 29 and causes personal information to be lost, stolen, divulged, forged, altered, or damaged;

- 1-2. Information and communications service provider, etc. who fails to destroy personal information in violation of Article 21 (1) (including applicable cases pursuant to Article 39-14);
2. A person who fails to take necessary measures to rectify or erase personal information in violation of Article 36 (2), and continuously uses, or provides a third party with, the personal information;
3. A person who fails to suspend processing of personal information in violation of Article 37 (2), and continuously uses, or provides a third party with, the personal information.

Article 74 (Joint Penalty Provisions) (1) If the representative of a corporation, or an agent or employee of, or any other person employed by, a corporation or an individual commits any of the offenses provided for in Article 70 in connection with the business affairs of the corporation or individual, not only shall such offender be punished, but also the corporation or individual shall be punished by a fine not exceeding 70 million won: Provided, That the same shall not apply where such corporation or individual has not been negligent in taking due care and supervisory activities concerning the relevant business affairs to prevent such offense.

(2) If the representative of a corporation, or an agent or employee of, or any other person employed by, a corporation or an individual commits any of the offenses provided for in Articles 71 through 73 in connection with the business affairs of the corporation or individual, not only shall such offender be punished, but also the corporation or individual shall be punished by a fine prescribed in the relevant Article: Provided, That the same shall not apply where such corporation or individual has not been negligent in taking due care and supervisory activities concerning the relevant business affairs to prevent such offense.

Article 74-2 (Confiscation and Collection) Any money or goods or other profits acquired by a person who has violated Articles 70 through 73 in relation to such violation may be confiscated, or, if confiscation is impossible, the value thereof may be collected. In such cases, such confiscation or collection may be levied in addition to other penalty provisions.

[This Article Newly Inserted by Act No. 13423, Jul. 24, 2015]

Article 75 (Administrative Fines) (1) Any of the following persons shall be subject to an administrative fine not exceeding 50 million won: <Amended by Act No. 14765, Apr. 18, 2017

1. A person who collects personal information in violation of Article 15 (1);
2. A person who fails to obtain the consent of a legal representative in violation of Article 22 (6);
3. A person who installs and operates visual data processing devices in violation of Article 25 (2).

(2) Any of the following persons shall be subject to an administrative fine not exceeding 30 million won:<Amended by Act No. 11990, Aug. 6, 2013; Act No. 12504, Mar. 24, 2014; Act No. 13423, Jul. 24, 2015; Act No. 14107, Mar. 29, 2016; Act No. 14765, Apr. 18, 2017; Act No. 16930, Feb. 4, 2020>

1. A person who fails to notify a data subject of necessary information in violation of Article 15 (2), 17 (2), 18 (3), or 26 (3);
2. A person who denies the provision of goods or services to a data subject in violation of Article 16 (3) or 22 (5);
3. A person who fails to notify a data subject of the matters provided for in Article 20 (1) or (2) in violation of Article 20 (1) or (2);
4. A person who fails to take necessary measures, such as destroying personal information, in violation of Article 21 (1) or Article 39-6 (including applicable cases pursuant to Article 39-14);
- 4-2. A person who processes resident registration numbers in violation of Article 24-2 (1);
- 4-3. A person who fails to adopt encryption measures in violation of Article 24-2 (2);
5. A person who fails to provide a data subject with an alternative method without using his or her resident registration number in violation of Article 24-2 (3);
6. A person who fails to take measures necessary to ensure safety in violation of Article 23 (2), 24 (3), 25 (6), 28-4 (1), or 29;
7. A person who installs and operates visual data processing devices in violation of Article 25 (1);
- 7-2. A person who fails to cease the use of, collect or destroy, information which has been generated to identify a certain individual, in violation of Article 28-5 (2);
- 7-3. A person who indicates and promotes the certification by fraud despite a failure to obtain such certification, in violation of Article 32-2 (6);
8. A person who fails to notify a data subject of the facts provided for in Article 34 (1) in violation of same paragraph;
9. A person who fails to report the results of measures taken, in violation of Article 34 (3);
10. A person who limits or denies access to personal information in violation of Article 35 (3);
11. A person who fails to take necessary measures to correct or erase personal information, in violation of Article 36 (2);

12. A person who fails to take necessary measures, such as destruction of the personal information whose processing has been suspended, in violation of Article 37 (4);

12-2. A person who refuses to provide services in violation of Article 39-3 (3) (including applicable cases pursuant to Article 39-14);

12-3. A person who fails to notify or report the relevant users, the Protection Commission or a specialized institution or notifies or reports after the lapse of 24 hours without any just cause, in violation of Article 39-4 (1) (including applicable cases pursuant to Article 39-14);

12-4. A person who fails to explain or falsely explains just cause, in violation of Article 39-4 (3);

12-5. A person who fails to provide methods of withdrawing consent, and accessing to, or correcting, personal information, in violation of Article 39-7 (2) (including applicable cases pursuant to Article 39-14);

12-6. Information and communications service provider, etc. who fails to take necessary measures in violation of Article 39-7 (3) (including applicable cases pursuant to Article 39-14 and any person to whom personal information has been transferred from information and communications service provider, etc. pursuant to Article 27);

12-7. A person who fails to notify users of the use history of their personal information in violation of the main clause of Article 39-8 (1) (including applicable cases pursuant to Article 39-14);

12-8. A person who fails to take protective measures, in violation of Article 39-12 (4) (including applicable cases pursuant to paragraph (5) of the same Article);

13. A person who fails to comply with corrective orders taken under Article 64 (1).

(3) Any of the following persons shall be subject to an administrative fine not exceeding 20 million won:<Newly Inserted by Act No. 16930, Feb. 4, 2020>

1. A person who fails to take necessary measures such as purchasing an insurance, joining a mutual aid organization, or accumulating reserves, in violation of Article 39-9 (1);

2. A person who fails to designate a domestic agent, in violation of Article 39-11 (1);

3. A person who outsources the processing of, or stores, users' personal information overseas without disclosing or informing all matters provided for in Article 39-12 (3) or notifying users in violation of the proviso of Article 39-12 (2).

(4) Any of the following persons shall be subject to an administrative fine not exceeding 10 million won:<Amended by Act No. 14765, Apr. 18, 2017; Act No. 16930, Feb. 4, 2020>

1. A person who fails to store and manage personal information separately in violation of Article 21 (3);
2. A person who obtains consent in violation of Article 22 (1) through (4);
3. A person who fails to take necessary measures including posting a signboard in violation of Article 25 (4);
4. A person who fails to execute a document stating the matters provided for in Article 26 (1) when outsourcing the work in violation of the same paragraph;
5. A person who fails to disclose the outsourced work and the outsourcee in violation of Article 26 (2);
6. A person who fails to notify a data subject of the transfer of his or her personal information in violation of Article 27 (1) or (2);
- 6-2. A person who fails to prepare and keep a record of relevant matters in violation of Article 28-4 (2);
7. A person who fails to establish, or disclose, the Privacy Policy in violation of Article 30 (1) or (2);
8. A person who fails to designate a privacy officer in violation of Article 31 (1);
9. A person who fails to notify a data subject of necessary information in violation of Article 35 (3) and (4), 36 (2) and (4), or 37 (3);
10. A person who fails to furnish materials, such as articles and documents pursuant to Article 63 (1), or who submits false materials;
11. A person who refuses, interferes with, or evades access or an inspection pursuant to Article 63 (2).

(5) Administrative fines provided for in paragraphs (1) through (4) shall be imposed and collected by the Protection Commission and the head of a related central administrative agency, as prescribed by Presidential Decree. In such cases, the head of a related central administrative agency shall impose and collect administrative fines from the personal information controllers in the field under his or her jurisdiction.<Amended by Act No. 11690, Mar. 23, 2013; Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 16930, Feb. 4, 2020>

Article 76 (Special Exemption to Application of Provisions on Administrative Fines) For the purposes of the provisions on administrative fines provided for in Article 75, no additional

administrative fine shall be imposed on any act subject to penalty surcharges pursuant to Article 34-2.

[This Article Newly Inserted by Act No. 11990, Aug. 6, 2013]

ADDENDA <No. 11690, 23. Mar, 2013>

Article 1 (Enforcement Date)

(1) This Act shall enter into force on the date of its promulgation.

(2) Omitted.

Articles 2 through 7 Omitted.

ADDENDA <No. 11990, 06. Aug, 2013>

Article 1 (Enforcement Date)

This Act shall enter into force one year after the date of its promulgation.

Article 2 (Transitional Measures concerning Limitation to Processing of Resident Registration Numbers)

(1) A person who processes resident registration numbers as at the time this Act enters into force shall destroy the resident registration numbers possessed, within two years after this Act enters into force: Provided, That any of the cases falling under the amended subparagraphs of Article 24-2 (1) shall be excluded from the destruction.

(2) Where resident registration numbers are not destroyed within the period referred to in paragraph (1), the amended provisions of Article 24-2 (1) shall be deemed to have been violated.

ADDENDA <No. 12504, 24. Mar, 2014>

This Act shall enter into force on the date of its promulgation: Provided, That the amended provisions of Articles 24-2 and 75 (2) 5 of the Personal Information Protection Act (Act No. 11990) shall enter into force on January 1, 2016.

ADDENDA <No. 12844, 19. Nov, 2014>

Article 1 (Enforcement Date)

This Act shall enter into force on the date of its promulgation. (Proviso Omitted.) Articles 2 through 7 Omitted.

ADDENDA <No. 13423, 24. Jul, 2015>

Article 1 (Enforcement Date)

This Act shall enter into force on the date of its promulgation: Provided, That the amended provisions of Articles 8 (1), 8-2, 9, 11 (1), 32-2, 39 (3) and (4), 39-2, 40, and 75 (2) 7-2 shall enter into force one year after the date of its promulgation, and the amended provisions of the former part of Article 24-2 (2) and Article 75 (2) 4-3 of the Personal Information Protection Act (Act No. 12504) shall enter into force on January 1, 2016, respectively.

Article 2 (Applicability to Compensation)

The amended provisions of Articles 39 (3) and (4) and 39-2 shall apply, beginning with the first claim for compensation for personal information suffering loss, theft, divulgence, forgery, alteration, or damage after this Act enters into force.

Article 3 (Transitional Measures concerning Personal Information Protection Certification)

Any person who has obtained the personal information protection certification from the Minister of the Interior before this Act enters into force shall be deemed obtained the personal information protection certification under the amended provisions of Article 32-2.

Article 4 (Transitional Measures concerning Qualifications for Certification Examiners of Personal Information Protection)

Any person qualified as a certification examiner of personal information protection before this Act enters into force shall be deemed qualified under this Act.

Article 5 (Transitional Measures concerning Terms of Office of Members of Personal Information Dispute Mediation Committee)

Members of the Dispute Mediation Committee appointed or commissioned by the Minister of the Interior before this Act enters into force shall be deemed members of the Dispute Mediation Committee commissioned by the Protection Commission under the amended provisions of Article 40.

Article 6 (Transitional Measures concerning Penalty Provisions, etc.)

The former provisions shall apply to the application of penalty provisions or imposition of administrative fines for offenses committed before this Act enters into force.

ADDENDA <No. 14107, 29. Mar, 2016>

Article 1 (Enforcement Date)

This Act shall enter into force six months after the date of its promulgation: Provided, That the amended provisions of Articles 24-2 (1) 1 and 67 (2) 5 shall enter into force one year after the date of its promulgation.

Article 2 (Applicability to Notification of Other Sources, etc. of Personal Information than Data Subjects)

The amended provisions of Article 20 (2) and (3) shall apply, beginning with the first case where any personal information is collected from a person other than the data subjects after this Act enters into force.

Article 3 (Transitional Measures concerning Privacy Policy)

(1) The Privacy Policy established under the former provisions as at the time this Act enters into force shall be deemed the Privacy Policy established under the amended provisions of Article 30 (1).

(2) Each personal information controller shall amend the Privacy Policy referred to in paragraph (1) to meet the purport of amending Article 30 (1) within six months after this Act enters into force.

ADDENDA <No. 14765, 18. Apr, 2017>

This Act shall enter into force six months after the date of its promulgation.

ADDENDA <No. 14839, 26. Jul, 2017>

Article 1 (Enforcement Date)

This Act shall enter into force on the date of its promulgation: Provided, That any amendment to the Acts made pursuant to Article 5 of this Addenda, promulgated before this Act enters into force, which have not yet entered into force, shall enter into force on the date the corresponding Act takes effect.

Articles 2 through 6 Omitted.

ADDENDA <No. 16930, 04. Feb, 2020>

Article 1 (Enforcement Date)

This Act shall enter into force six months after the date of its promulgation.

Article 2 (Transitional Measures concerning Terms of Office of Commissioners)

The term of office of the Commissioners of the Protection Commission appointed under the previous provisions as at the time this Act enters into force, shall be deemed expired on the date preceding the enforcement date of this Act.

Article 3 (Transitional Measures concerning Duties Following Adjustment of Functions) (1)

Among the duties of the Korea Communications Commission under Article 11 (1) of the Act on the Establishment and Operation of Korea Communications Commission as at the time this Act enters into force, those relating to personal information protection shall be transferred to the Protection Commission.

(2) Among the duties of the Minister of the Interior and Safety as at the time this Act enters into force, those pursuant to the amended provisions in Article 7-8 shall be assumed by the Protection Commission.

(3) Among the notifications, administrative dispositions and other acts of the Minister of the Interior and Safety, and acts conducted with respect to the Minister of the Interior and Safety such as filing of an application or report before this Act enters into force, those relating to matters for which competent authority is transferred from the Minister of the Interior and Safety to the Protection Commission shall be deemed to be the acts of, or acts conducted with respect to, the Protection Commission.

(4) Among the notifications, administrative dispositions and other acts of the Korea Communications Commission, and acts conducted with respect to the Korea Communications Commission such as filing of a report before this Act enters into force, those relating to matters for which competent authority is transferred from the Korea Communications Commission to the Protection Commission shall be deemed to be the acts of, or acts conducted with respect to, the Protection Commission pursuant to this Act.

(5) Among the public officials of the Ministry of the Interior and Safety or the Korea Communications Commission as at the time this Act enters into force, those prescribed by Presidential Decree shall be deemed to be the public officials of the Protection Commission pursuant to this Act.

Article 4 (Transitional Measures concerning the Protection Commission)

(1) The acts of, or acts conducted with respect to, the Protection Commission pursuant to the previous provisions as at the time this Act enters into force shall be deemed to be the acts of, or acts conducted with respect to, the Protection Commission pursuant to this Act.

Article 5 (Transitional Measures concerning Certifying Organizations for Personal Information Protection Management System)

(1) Entities designated as a certifying or examining organization pursuant to Article 47-3 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc. (hereinafter referred to as the “Network Act”) as at the time this Act enters into force, shall be deemed to have been designated as a specialized organization in accordance with Article 32-2 of this Act. (2) Entities certified for personal information protection management system or qualified as a certification examiner pursuant to Article 47-3 of the Network Act as of the effective date of this Act shall be deemed to have been certified for personal information protection management system or qualified as a certification examiner pursuant to Article 32-2 of this Act.

Article 6 (Transitional Measures concerning Delegation or Entrustment of Authority) The Special Metropolitan City Mayor, a Metropolitan City Mayor, a Do Governor, the Special Self-Governing Province Governor, the Special Self-Governing City Mayor or specialized institutions who have been delegated or entrusted with part of the authority of the Minister of the Interior and Safety pursuant to the previous provisions as of the effective date of this Act shall be deemed to have been delegated or entrusted with part of the authority of the Protection Commission pursuant to this Act.

Article 7 (Transitional Measures concerning Penalty Provisions and Administrative Fines) Application of penalty and administrative fines on acts that were committed before this Act enters into force shall be governed by the previous provisions.

Article 8 (Transitional Measures concerning Imposition of Administrative Surcharges) Imposition of administrative surcharges on acts that were committed before this Act enters into force shall be governed by the previous provisions.

Article 9 Omitted.

Article 10 (Relationship to Other Statutes)

(1) When other statutes (including statutes that were promulgated before this Act enters into force but the enforcement date of which has not arrived yet) state the “ Korea Communications Commission” or “ Chairperson of the Korea Communications Commission” in relation to the work of the Korea Communications Commission and the Ministry of the Interior and Safety that is transferred to the Protection Commission according to this Act as at the time this Act enters into force, such terms are regarded as the “Protection Commission” or “Chairperson of the Protection Commission” as applicable; “ public officials of the Korea Communications Commission” as “public officials of the Protection Commission;” “Ministry of the Interior and Safety” or “Minister of the Interior and Safety” as “Protection Commission” or “Chairperson of the Protection Commission” as

applicable; and “public officials of the Ministry of the Interior and Safety” as “public officials of the Protection Commission”.

(2) If other statutes quote the previous Network Act or provisions therein as at the time this Act enters into force, and if there is any corresponding provision in this Act, such statutes or the provisions therein are regarded as this Act or provisions of this Act.

Güney Kore - Personal Information Safeguard and Security Standard

PERSONAL INFORMATION SAFEGUARD AND SECURITY STANDARD

Established by MOPAS Notification No. 2011-43, Sep. 30, 2011

Amended by MOI Notification No. 2014-7, Dec. 30, 2014

Article 1 (Purpose)

The purpose of this Standard is to provide for detailed standards to secure safety so that personal information may not be lost, stolen, leaked, forged, altered or damaged when the personal information controller processes personal information pursuant to Articles 24(3) and 29 of the Personal Information Protection Act (hereinafter referred to as the "Act") and Articles 21 and 30 of the Enforcement Decree of the same Act (hereinafter referred to as the "Decree").

Article 2 (Definitions)

The terms used in this Standard shall be defined as follows:

1. "Data subject" means the natural person who is identifiable by the information processed hereby to become the subject of such information;
2. "Personal information file" means a set or sets of personal information arranged or organized in a systematic manner based on a certain rule for easy access to the personal information;
3. "Personal information controller" means a public institution, legal person, organization, individual, etc. that processes directly or indirectly personal information to operate personal information files for official or business purposes;
4. "Micro enterprise" means a business entity as defined in Article 2 of the Enforcement Decree of the Act on the Protection and Support of Micro Enterprises, b
5. "Small and medium enterprise" means a personal information controller whose full-time employees are numbered more than five (5) and less than 50; provided, however, that, in case of mining, manufacturing, construction and transportation industries pursuant to Article 2(1) i of the Enforcement Decree of the Act on the Protection and Support of Micro Enterprises, means a personal information controller whose full-time employees are numbered more than ten (10) and less than 50.
6. "Chief privacy officer" means the person, as set forth in Article 32(2) i and ii of the Decree, who is comprehensively responsible for and in charge of processing of personal information;

7. "Personal information handler" means the officer or employee, dispatched worker, part-time worker, etc. who is processing personal information under the direction and supervision of the personal information controller;
8. "Information and communications network" means the information and communications system which utilizes the electric communication facilities subject to Article 2 ii of the Framework Act on Communications; or collects, processes, stores, retrieves, transmits or receives information taking advantage of the electric communication facilities, computers and computer-using technologies;
9. "Personal information processing system" means a database system organized systemically to process personal information; provided, however, that it shall exclude the system of a micro enterprise or small and medium enterprise which contains only personal information of its own employees;
10. "Internal network" means the section of the Internet section with access controlled or blocked by means of the physical separation of network, access control system, etc.;
11. "Internal management plan" means the internal standards established and implemented by the personal information controller through the internal decision-making process to process personal information safely;
12. "Password" means the inherent string of letters and numbers kept secret to be transmitted to the system with ID so that a data subject or personal information handler, etc. may prove his/her authentic authority to access when he/she intends to be connected to the personal information processing system, computer for business operation or information and communications network;
13. "Log-on record" means the electronic record of the facts of access including ID, date and time of access, information to identify the person of access, tasks carried out which the personal information handler, etc. has performed while being connected to the personal information processing system;
14. "Biometric information" means the information on bodily or behavioral characteristic including fingerprint, face, iris, vein, voice, handwriting, etc. which may identify an individual, or other information processed or generated from the original information;
15. "Auxiliary storage media" means the storage media including portable hard disk, USB memory, compact disk (CD), digital versatile disk (DVD), floppy diskette, etc., which may be easily connected or disconnected with the personal information processing system or personal computer, etc.

16. "Risk analysis" means the action to analyze the personal information protection means applicable to the personal information processing system, the probability to violate the right of data subjects and the degree of inherent risk in case of data breach;

17. "Mobile devices" mean the portable devices used in processing personal information including PDA, smartphone, tablet PC, etc. using wireless networks; and

18. "Open wireless network" means the network that many and unspecified persons may use the Internet via a wireless access point (AP).

Article 3 (Establishment and Implementation of Internal Management Plan)

(1) The personal information controller shall establish and implement the internal management plan including the following subparagraphs in order to process personal information safely:

1. Matters on designate a chief privacy officer;
2. Matters on the role and responsibility of a chief privacy officer and personal information handler;
3. Matters on the measures necessary for the security of personal information;
4. Matters on the education of personal information controllers;
5. Matters on the management and supervision of the trustee in case of entrusting personal information processing; and
6. Other matters necessary for the personal information protection.

(2) Micro enterprises may not establish the internal management plan subject to paragraph (1).

(3) The personal information controller shall modify and implement the internal management plan reflecting immediately material changes in each subparagraphs stated in paragraph (1), if any, and preserve such modification history.

Article 4 (Control of Access Authority)

(1) The personal information controller shall grant the authority to access the personal information processing system to a person within a minimum scope in a discriminating manner necessary to conduct business

(2) The personal information controller shall alter or delete the authority to access the personal information processing system without delay when the personal information handler is changed owing to transfer, quit or change of personnel.

(3) The personal information controller shall record the grant, alteration and deletion of authority to access pursuant to paragraphs (1) and (2), and maintain the records for at least three years.

(4) When the personal information controller issues a user account so as to access the personal information processing system, the user account shall be issued to each personal information handler and shall not be shared with other personal information handler.

(5) The personal information controller shall establish and implement the rule to make a password so that personal information handlers or data subjects may form and use a safe password.

Article 5 (Access Control)

(1) The personal information controller shall take measures including the following subparagraphs in order to prevent unauthorized access to, and incidents of, the personal information processing system via the information and communications network:

1. To control the unauthorized access by limiting the authority to access to the Internet Protocol (IP) address, etc.; and

2. To analyze the IP address being connected to the personal information processing system, and detect any attempt to make illegal personal information leak.

(2) The personal information controller shall apply safe connecting means including virtual private networks (VPN) or exclusive communication lines when personal information handlers intend to access to the personal information processing system from outside via the information and communications network.

(3) The personal information controller shall check the additional information of a data subject at the Internet homepage in case where the name and resident registration number are used for the authentication of the data subject pursuant to the other laws and regulations.

(4) The personal information controller shall take necessary measures to the personal information processing system, computers for business operation, mobile devices, etc. lest personal information being processed should be known or leaked to an unauthorized person by means of the Internet homepage, P2P, sharing of data, open wireless network, etc.

(5) The personal information controller dealing with unique identifiers shall inspect the weak points more than once a year lest such unique identifiers should be leaked, altered or damaged at the Internet homepage.

(6) When the personal information controller processes personal information using computers for business operation or mobile devices other than the personal information processing system, paragraph (1) may not apply. In this case, the access control provided by the operating systems (OS) of such computers for business operation or mobile devices, security programs, etc. may be utilized.

(7) The personal information controller shall take protective measures of mobile devices for business operation including password, etc. lest personal information should be leaked owing to loss, theft, etc. of such mobile devices.

Article 6 (Encryption of Personal Information)

(1) The personal information to be encrypted pursuant to Articles 21 and 30(1) iii of the Decree shall be unique identifiers, password and biometric information.

(2) The personal information controller shall encrypt the personal information subject to paragraph (1) when such information is transmitted via the information and communications network or delivered by means of auxiliary storage media.

(3) The personal information controller shall encrypt and store the password and biometric information; provided, however, that the password shall be encrypted and stored by only one way lest it should be decoded.

(4) The personal information controller shall encrypt unique identifiers when they are stored in the Internet section and in the demilitarized zone (DMZ) between the Internet section and the internal network.

(5) When the personal information controller stores unique identifiers in the internal network, the following subparagraphs may apply to whether and how much in scope the encryption will be performed:

1. The result of the privacy impact assessment (PIA) in case of the public institution which is subject to such PIA pursuant to Article 33 of the Act; or

2. The result of the risk analysis.

(6) When the personal information controller encrypts the personal information subject to paragraph (1), such personal information shall be encrypted by safe encryption algorithm in order to be stored.

(7) When the personal information controller stores and manages unique identifiers in the computers for business operation or mobile devices, such unique identifiers shall be encrypted by using commercial encryption softwares or safe encryption algorithm in order to be stored.

Article 7 (Maintenance and Inspection of Log-on Records)

(1) The personal information controller shall maintain and manage log-on records which the personal information handler has accessed the personal information processing system for more than six months.

(2) The personal information controller shall inspect the log-on records of the personal information processing system for more than once semi-annually for the prompt response to the leak, alteration, damage, etc. of personal information.

(3) The personal information controller shall maintain the log-on records of the personal information handler in a safe manner lest such log-on records should be forged, altered, stolen or lost.

Article 8 (Prevention of Malicious Program, etc.)

(1) The personal information controller shall install and run the security programs including vaccine softwares which prevent and cure malicious programs, and observe the following subparagraphs:

1. To activate the automatic update function of the security programs, or maintain the latest condition by regularly updating such programs for more than once a day;
2. To update immediately the security programs in case where the malicious program alert is issued or the security update notification is provided by the software house of application programs in use or operating softwares

Article 9 (Prevention of Physical Access)

(1) When the personal information controller has a physical storage place separately like a computer room, storage room, etc., the access control procedure thereto shall be established and operated.

(2) The personal information controller shall keep documents, auxiliary storage media, etc. containing personal information locked in a secure area.

(3) The personal information controller shall put security measures in motion to control the bringing-in and out of auxiliary storage media containing personal information; provided, however, that it may not apply when the personal information is processed by the computers for business operation or mobile devices rather than the separate personal information processing system

Article 10 (Maintenance and Inspection of Log-on Records)

(1) The personal information controller shall take any of the following measures when the personal information is destroyed:

1. Complete destruction including incineration or crushing;
2. Deletion using the exclusive deleting facilities; or
3. Initialization or overwriting lest the data should be restored.

(2) When the personal information controller destroy a part of personal information, the following subparagraphs shall be observed if it is difficult to destroy by the method as stated in paragraph (1):

1. In case of electronic files: deleting personal information and then controlling lest it should be restored; or
2. In case of records, prints-out, documents other recording media than subparagraph 1: masking, punching and deleting the relevant part.

ADDENDA

<MOPAS Notification No. 2011-43, Sep. 30, 2011>

Article 1 (Enforcement Date)

This Standard shall enter into force on the day of notification.

Article 2 (Exclusion of Application of the Safety and Security Measures to Visual Data Processing Devices)

In relation to the safety and security measures for visual data processing devices, the standard for installation and operation of visual data processing devices as included in the Standard Personal Information Protection Guideline shall apply.

Article 3 (Safeguards in the Operational Environment like Internet Data Center, Cloud Computing Center, etc.)

When the personal information controller processes personal information by leasing hardwares, softwares, etc. on a contract basis with the Internet Data Center (IDC) or Cloud Computing Center, the safeguards in such contract or Service Level Agreement (SLA) being existent and equivalent to this Standard shall be deemed to be performed just like this Standard.

ADDENDUM

<MOI Notification No. 2014-7, Dec. 30, 2014>

This Standard shall enter into force on the day of notification.

Japonya - Act on the Protection of Personal Information

Amended Act on the Protection of Personal Information (Tentative Translation)

This is an English translation of the amended Act on the Protection of Personal Information.

The Amendment Bill of the Act on the Protection of Personal Information, etc., submitted to the ordinary session (201st Session) of the Diet on 10th March 2020, was approved by the Diet on 5th June 2020 and promulgated on 12th June 2020.

The Amendment Act, except for some parts, will come into force within a period not exceeding two years from the date of the promulgation.

NOTICE

This translation has neither had its texts checked by a native English speaker nor a legal language editor, and thus may be subject to change.

Only the original Japanese text of the law has legal effect, and the translation is to be used solely as reference material to aid in the understanding of the law.

Table of Contents

Chapter I General Provisions (Articles 1 to 3)

Chapter II Responsibilities etc. of the Central and Local Governments (Articles 4 to 6)

Chapter III Measures etc. relating to the Protection of Personal Information
Section 1 Basic Policy on the Protection of Personal Information (Article 7)
Section 2 Measures by the Central Government (Articles 8 to 10)

Section 3 Measures by the Local Governments (Articles 11 to 13)

Section 4 Cooperation between the Central and Local Governments (Article 14)

Chapter IV Obligations etc. of a Personal Information Handling Business Operator

Section 1 Obligations of a Personal Information Handling Business Operator etc. (Articles 15 to 35)

Section 2 Obligations of a Pseudonymously Processed Information Handling Business Operator etc.
(Article 35-2 and Article 35-3)

Section 3 Obligations of an Anonymously Processed Information Handling Business Operator etc.
(Articles 36 to 39)

Section 4 Supervision (Articles 40 to 46)

Section 5 Private Sector Body's Promotion for the Protection of Personal Information (Articles 47 to 58)

Section 6 Service (Articles 58-2 to 58-5)

Chapter V The Personal Information Protection Commission (Articles 59 to 74)

Chapter VI Miscellaneous Provisions (Articles 75 to 81) Chapter VII Penal Provisions (Articles 82 to 88)

Chapter I General Provisions

(Purpose)

Article 1

This Act aims to protect an individual's rights and interests while considering the utility of personal information including that the proper and effective application of personal information contributes to the creation of new industries and the realization of a vibrant economic society and an enriched quality of life for the people of Japan; by setting forth the overall vision for the proper handling of personal information, creating a governmental basic policy with regard to this, and establishing other matters to serve as a basis for measures to protect personal information, as well as by clarifying the responsibilities etc. of the central and local governments and establishing obligations etc. that a personal information handling business operator shall fulfill, in light of the significantly expanded utilization of personal information as our advanced information- and communication-based society evolves.

(Definition)

Article 2

(1) "Personal information" in this Act means that information relating to a living individual which falls under any of each following item:

(i) those containing a name, date of birth, or other descriptions etc. (meaning any and all matters (excluding an individual identification code) stated, recorded or otherwise expressed using voice, movement or other methods in a document, drawing or electromagnetic record (meaning a record kept in an electromagnetic form (meaning an electronic, magnetic or other forms that cannot be recognized through the human senses; the same shall apply in the succeeding paragraph, item (ii)); the same shall apply in Article 18, paragraph

(2) and Article 28, paragraph (1)); hereinafter the same) whereby a specific individual can be identified (including those which can be readily collated with other information and thereby identify a specific individual)

(ii) those containing an individual identification code

(2) An "individual identification code" in this Act means those prescribed by cabinet order which are any character, letter, number, symbol or other codes falling under any of each following item.

(i) those able to identify a specific individual that are a character, letter, number, symbol or other codes into which a bodily partial feature of the specific individual has been converted in order to be provided for use by computers

(ii) those character, letter, number, symbol or other codes which are assigned in regard to the use of services provided to an individual or to the purchase of goods sold to an individual, or which are stated or electromagnetically recorded in a card or other document issued to an individual so as to be able to identify a specific user or purchaser, or recipient of issuance by having made the said codes differently assigned or, stated or recoded for the said user or purchaser, or recipient of issuance

(3) "Special care-required personal information" in this Act means personal information comprising a principal's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions etc. prescribed by cabinet order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal.

(4) A "personal information database etc." in this Act means those set forth in the following which are a collective body of information comprising personal information (excluding those prescribed by cabinet order as having little possibility of harming an individual's rights and interests considering their utilization method).

(i) those systematically organized so as to be able to search for particular personal information using a computer;

(ii) besides those set forth in the preceding item, those prescribed by cabinet order as having been systematically organized so as to be able to easily search for particular personal information.

(5) A "personal information handling business operator" in this Act means a person providing a personal information database etc. for use in business; however, excluding a person set forth in the following;

(i) a central government organization;

(ii) a local government;

(iii) an incorporated administrative agency etc. (meaning an independent administrative agency etc. prescribed in Article 2, paragraph (1) of the Act

on the Protection of Personal Information Held by Incorporated Administrative Agencies (Act No. 59 of 2003); hereinafter the same);

(iv) a local incorporated administrative agency (meaning a local incorporated administrative agency prescribed in Article 2, paragraph (1) of the Local Incorporated Administrative Agencies Act (Act No. 118 of 2003); hereinafter the same);

(6) "Personal data" in this Act means personal information constituting a personal information database etc.

(7) "Retained personal data" in this Act means personal data which a personal information handling business operator has the authority to disclose, correct, add or delete the contents of, cease the utilization of, erase, and cease the third-party provision of, and which shall not be those prescribed by cabinet order as likely to harm the public or other interests if their presence or absence is made known.

(8) A "principal" in relation to personal information in this Act means a specific individual identifiable by personal information.

(9) "Pseudonymously processed information" in this Act means information relating to an individual that can be produced from processing personal information so as not to be able to identify a specific individual unless collated with other information by taking action prescribed in each following item in accordance with the divisions of personal information set forth in each said item.

(i) personal information falling under paragraph (1), item (i); Deleting a part of descriptions etc. contained in the said personal information (including replacing the said part of descriptions etc. with

other descriptions etc. using a method with no regularity that can restore the said part of descriptions etc.)

(ii) personal information falling under paragraph (1), item (ii); Deleting all individual identification codes contained in the said personal information (including replacing the said individual identification codes with other descriptions etc. using a method with no regularity that can restore the said personal identification codes)

(10) A “pseudonymously processed information handling business operator” in this Act means a person who provides for use in business a collective body of information comprising pseudonymously processed information which has been systematically organized so as to be able to search using a computer for specific pseudonymously processed information or similar others prescribed by cabinet order as systematically organized so as to be able to search easily for specific pseudonymously processed information (referred to as an “pseudonymously processed information database etc.” in Article 35-2, paragraph (1)). However, a person set forth in each item of paragraph (5) is

excluded.

(11) “Anonymously processed information” in this Act means information relating to an individual that can be produced from processing personal information so as neither to be able to identify a specific individual by taking action prescribed in each following item in accordance with the divisions of personal information set forth in each said item nor to be able to restore the personal information.

(i) personal information falling under paragraph (1), item (i); Deleting a part of descriptions etc. contained in the said personal information (including replacing the said part of descriptions etc. with other descriptions etc. using a method with no regularity that can restore the said part of descriptions etc.)

(ii) personal information falling under paragraph (1), item (ii); Deleting all individual identification codes contained in the said personal information (including replacing the said individual identification codes with other descriptions etc. using a method with no regularity that can restore the said personal identification codes)

(12) An “anonymously processed information handling business operator” in this Act means a person who provides for use in business a collective body of information comprising anonymously processed information which has been systematically organized so as to be able to search using a computer for specific anonymously processed information or similar others prescribed by cabinet order as

systematically organized so as to be able to search easily for specific anonymously processed information (referred to as an “anonymously processed information database etc.” in Article 36, paragraph (1)). However, a person set forth in each item of paragraph (5) is excluded.

(Overall Vision)

Article 3

Personal information, considering it should be carefully handled under the vision of respecting the personality of an individual, shall be made subject to proper handling.

Chapter II Responsibilities etc. of the Central and Local Governments

(Responsibilities of the Central Government)

Article 4

The central government shall have the responsibilities for comprehensively developing and implementing necessary measures to ensure the proper handling of personal information in conformity with the purport of this Act.

(Responsibilities of the Local Governments)

Article 5

The local governments shall have the responsibilities for developing and implementing necessary measures to ensure the proper handling of personal information based on the characteristics of their local area in conformity with the purport of this Act.

(Legislative Action etc.)

Article 6

The government shall, considering the nature and utilization method of personal information, take necessary legislative and other action so as to be able to take discreet action for protecting personal information that especially requires ensuring the strict implementation of its proper handling in order to seek enhanced protection of an individual’s rights and interests, and shall take necessary action in collaboration with the governments in other countries to construct an internationally conformable system concerning personal information through fostering cooperation with an international organization and other international framework.

Chapter III Measures etc. for the Protection of Personal Information

Section 1 Basic Policy on the Protection of Personal Information

Article 7

(1) The government shall establish a basic policy on the protection of personal information (hereinafter referred to as a “basic policy”) in order to seek to comprehensively and integrally promote measures concerning the protection of personal information.

(2) A basic policy shall prescribe those matters set forth in the following.

(i) a basic direction for promoting measures concerning the protection of personal information

(ii) a matter concerning action to be taken by the central government for the protection of personal information

(iii) a basic matter concerning action to be taken by a local government for the protection of personal information

(iv) a basic matter concerning action to be taken by an incorporated administrative agency etc. for the protection of personal information

(v) a basic matter concerning action to be taken by a local incorporated administrative agency for the protection of personal information

(vi) a basic matter concerning action to be taken by a personal information handling business operator, a pseudonymously processed information

handling business operator, and an anonymously processed information handling business operator, and, an accredited personal information protection organization prescribed in Article 50, paragraph (1) for the protection of personal information

(vii) a matter concerning dealing smoothly with a complaint about the handling of personal information

(viii) other important matters concerning promoting measures for the protection of personal information

(3) The Prime Minister shall call for a cabinet decision on a basic policy developed by the Personal Information Protection Commission.

(4) The Prime Minister shall, when a cabinet decision was made pursuant to the provisions of the preceding paragraph, disclose a basic policy to the public without delay.

(5) The provisions under the preceding two paragraphs shall apply mutatis mutandis when altering a basic policy.

Section 2 Measures by the Central Government

(Support to a Local Government etc.)

Article 8

The central government shall provide information, develop guidelines to ensure the proper and effective implementation of action to be taken by a business operator etc., and take other necessary action in order to support measures for the protection of personal information developed or implemented by a local government and activities undertaken by a Japanese citizen, or a business operator etc. in relation to seeking the proper handling of personal information.

(Action for Dealing with a Complaint)

Article 9

The central government shall take necessary action to seek the proper and prompt dealing of a complaint caused between a business operator and a principal about the handling of personal information.

(Action for Ensuring the Proper Handling of Personal Information)

Article 10

The central government shall, through the appropriate division of roles between a local government and itself, take necessary action prescribed in the succeeding Chapter in order to ensure the proper handling of personal information by a personal information handling business operator.

Section 3 Measures by the Local Governments

(Protection of Personal Information Retained by a Local Government etc.)

Article 11

(1) A local government shall, considering the nature of personal information it retains, the purpose of retaining the personal information, and so on, strive to take necessary action so as to ensure the proper handling of the retained personal information.

(2) A local government shall, in response to the characteristics and business contents of a local incorporated administrative agency that it has established, strive to take necessary action so as to ensure the proper handling of personal information that the agency retains.

(Support to a Business Operator etc. in a Local Area)

Article 12

A local government shall, in order to ensure the proper handling of personal information, strive to take necessary action to support a business operator and a resident in a local area.

(Mediation etc. for Dealing with a Complaint)

Article 13

A local government shall, in order for a complaint caused between a business operator and a principal about the handling of personal information to be dealt with appropriately and promptly, strive to mediate dealing with the complaint and take other necessary action.

Section 4 Cooperation between the Central and Local Governments

Article 14

The central and local governments shall cooperate with one another in implementing measures relating to the protection of personal information.

Chapter IV Obligations etc. of a Personal Information Handling Business Operator

Section 1 Obligations of a Personal Information Handling Business Operator etc.

(Specifying a Utilization Purpose)

Article 15

(1) A personal information handling business operator shall, in handling personal information, specify the purpose of utilizing the personal information (hereinafter referred to as a “utilization purpose”) as explicitly as possible.

(2) A personal information handling business operator shall, in case of altering a utilization purpose, not do so beyond the scope recognized reasonably relevant to the pre-altered utilization purpose.

(Restriction due to a Utilization Purpose)

Article 16

(1) A personal information handling business operator shall not handle personal information without obtaining in advance a principal’s consent beyond the necessary scope to achieve a utilization purpose specified pursuant to the provisions under the preceding Article.

(2) A personal information handling business operator shall, in case of having acquired personal information accompanied with succeeding a business from another personal information handling business operator because of a merger or other reason, not handle the personal information without

obtaining in advance a principal's consent beyond the necessary scope to achieve the pre- succession utilization purpose of the said personal information.

(3) The provisions under the preceding two paragraphs shall not apply to those cases set forth in the following.

(i) cases based on laws and regulations

(ii) cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent

(iii) cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent

(iv) cases in which there is a need to cooperate in regard to a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs

(Prohibition of Inappropriate Utilization)

Article 16-2

A Personal Information Handling Business Operator shall not utilize personal information using a method that has the possibility of fomenting or prompting unlawful or unfair act.

(Proper Acquisition)

Article 17

(1) A personal information handling business operator shall not acquire personal information by deceit or other improper means.

(2) A personal information handling business operator shall, except in those cases set forth in the following, not acquire special care-required personal information without obtaining in advance a principal's consent.

(i) cases based on laws and regulations

(ii) cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent

(iii) cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent

(iv) cases in which there is a need to cooperate in regard to a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs

(v) cases in which the said special care-required personal information is being open to the public by a principal, a government organization, a local government, a person set forth in each item of Article 76, paragraph (1) or other persons prescribed by rules of the Personal Information Protection Commission

(vi) other cases prescribed by cabinet order as equivalent to those cases set forth in each preceding item

(Notification etc. of a Utilization Purpose when Acquiring)

Article 18

(1) A personal information handling business operator shall, in case of having acquired personal information except in cases where a utilization purpose has been disclosed in advance to the public, promptly inform a principal of, or disclose to the public, the utilization purpose.

(2) A personal information handling business operator shall, notwithstanding the provisions under the preceding paragraph, in cases where it acquires, accompanied by concluding a contract with a principal, the principal's personal

information stated in a written contract or other document (including an electromagnetic record; hereinafter the same in this paragraph) or other similar cases where it acquires directly from a principal his or her personal information stated in a written document, state a utilization purpose explicitly to the said principal. This, however, shall not apply in cases where there is an urgent need to protect a human life, body or fortune.

(3) A personal information handling business operator shall, in case of altering a utilization purpose, inform a principal of, or disclose to the public, a post- altered utilization purpose.

(4) The provisions of the preceding three paragraphs shall not apply in those cases set forth in the following.

(i) cases in which there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would harm a principal or third party's life, body, fortune or other rights and interests

(ii) cases in which there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would harm the rights or legitimate interests of the said personal information handling business operator

(iii) cases in which there is a need to cooperate in regard to a central government organization or a local government performing affairs prescribed by laws and regulations, and when there is a possibility that informing a principal of, or disclosing to the public, a utilization purpose would interfere with the performance of the said affairs

(iv) cases in which it can be recognized, judging from the acquisitional circumstances, that a utilization purpose is clear

(Assurance etc. about the Accuracy of Data Contents)

Article 19

A personal information handling business operator shall strive to keep personal data accurate and up to date within the scope necessary to achieve a utilization purpose, and to delete the personal data without delay when such utilization has become unnecessary.

(Security Control Action)

Article 20

A personal information handling business operator shall take necessary and appropriate action for the security control of personal data including preventing the leakage, loss or damage of its handled personal data.

(Supervision over Employees)

Article 21

A personal information handling business operator shall, in having its employees handle personal data, exercise necessary and appropriate supervision over the employees so as to seek the security control of the personal data.

(Supervision over a Trustee)

Article 22

A personal information handling business operator shall, in case of entrusting a whole or part of the handling of personal data, exercise necessary and appropriate supervision over an entrusted person so as to seek the security control of the personal data of which the handling has been entrusted.

(Report etc. of Leakage etc.)

Article 22-2

(1) A personal information handling business operator shall, pursuant to rules of the Personal Information Protection Commission, report to the Personal Information Protection Commission when there is a leakage, loss or damage and other situation concerning the insurance of security of its handled personal data and it is prescribed by the rule of Personal Information Protection Commission as those of which there is a large possibility of harming an individual's rights and interests. This, however, shall not apply in cases where the said personal information handling business operator entrusted by other personal information handling business operator a whole or part of the said handling of personal data informed the occurrence of said situation to the said other personal information handling business operator as prescribed by rules of the Personal Information Protection Commission.

(2) In those cases prescribed by the preceding paragraph, a personal information handling business operator (excluding those who informed pursuant to the provisions of the proviso of the preceding paragraph) shall, pursuant to rules of the Personal Information Protection Commission, notify a principal of the occurrence of the said situation. This, however, shall not apply when it is difficult to inform a principal and when necessary alternative action is taken to protect a principal's rights and interests.

(Restriction on Third Party Provision)

Article 23

(1) A personal information handling business operator shall, except in those cases set forth in the following, not provide personal data to a third party without obtaining in advance a principal's consent.

(i) cases based on laws and regulations

(ii) cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent

(iii) cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent

(iv) cases in which there is a need to cooperate in regard to a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and

regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs

(2) A personal information handling business operator, in regard to personal data provided to a third party, may, in cases where it is set to cease in response to a principal's request a third-party provision of personal data that can identify the principal and when pursuant to rules of the Personal Information Protection Commission it has in advance informed a principal of those matters set forth in the following or put them into a state where a principal can easily know, and notified them to the Personal Information Protection Commission, provide the said personal data to a third party notwithstanding the provisions of the preceding paragraph. This, however, shall not apply in cases where personal data provided to a third party is a special care-required personal information, or, has been acquired in violation of the provisions of Article 17 or has been provided by another personal information handling business operator pursuant to the provisions in the main clause of this paragraph (including their wholly or partially duplicated or processed ones).

(i) The name or appellation and address and, for a corporate body, the name of its representative (for a non-corporate body having appointed a representative or administrator, the said representative or administrator; hereinafter the same in this Article, Article 26, paragraph (1), item (i), and Article 27, paragraph (1), item (i)) of a personal information handling business operator that provides to a third party.

(ii) to set a third-party provision as a utilization purpose

(iii) the categories of personal data provided to a third party

(iv) a method of acquiring personal data provided to a third party (v) a method of a third-party provision

(vi) to cease, in response to a principal's request, a third-party provision of personal data that can identify the principal

(vii) a method of receiving a principal's request

(viii) other matters prescribed by rules of the Personal Information Protection Commission as those necessary to protect an individual's rights and interests

(3) A personal information handling business operator shall, in case of those matters set forth in item (i) of the preceding paragraph are altered or when the personal data provision is stopped pursuant to the provisions of the preceding paragraph, without delay, and when intending to alter those matters

set forth in item (iii) to item (v), item (vii) or item (viii) of the preceding paragraph, in advance inform a principal to that effect or put them into a state where a principal can easily know and notify them to the Personal Information Protection Commission pursuant to rules of the Personal Information Protection Commission.

(4) The Personal Information Protection Commission shall, when notified pursuant to paragraph (2), disclose to the public a matter relating to the notification pursuant to rules of the Personal Information Protection Commission. The same shall apply when notified pursuant to the preceding paragraph.

(5) In those cases set forth in the following, a person receiving the provision of the said personal data shall not fall under a third party in regard to applying the provisions of each preceding paragraph.

(i) cases in which personal data is provided accompanied by a personal information handling business operator entrusting a whole or part of the handling of the personal data within the necessary scope to achieve a utilization purpose

(ii) cases in which personal data is provided accompanied with business succession caused by a merger or other reason

(iii) cases in which personal data to be jointly utilized by a specified person is provided to the specified person, and when a principal has in advance been informed or a state has been in place where a principal can easily know to that effect as well as of the categories of the jointly utilized personal data, the scope of a jointly utilizing person, the utilization purpose for the utilizing person and the name or appellation and address, and, for a corporate body, the name of its representative of a person responsible for controlling the said personal data

(6) A personal information handling business operator shall, in case of altering the name, appellation or address, or, for a corporate body, the name of its representative of a person responsible for controlling personal data prescribed in item (iii) of the preceding paragraph, without delay, and in case of altering a utilization purpose for a utilizing person or the person responsible prescribed in item (iii) of the preceding paragraph, in advance inform a principal of the contents to be altered or put them into a state where a principal can easily know.

(Restriction on Provision to a Third Party in a Foreign Country)

Article 24

(1) A personal information handling business operator, except in those cases set forth in each item of the preceding Article, paragraph (1), shall, in case of providing personal data to a third party

(excluding a person establishing a system conforming to standards prescribed by rules of the Personal Information Protection Commission as necessary for continuously taking action equivalent to the one that a personal information handling business operator shall take concerning the handling of personal data pursuant to the provisions of this Section (referred to as “equivalent action” in paragraph (3)); hereinafter the same in this paragraph, the succeeding paragraph and Article 26-2, paragraph (1), item(ii)) in a foreign country (meaning a country or region located outside the territory of Japan; hereinafter the same) (excluding those prescribed by rules of the Personal Information Protection Commission as a foreign country establishing a personal information protection system recognized to have equivalent standards to that in Japan in regard to the protection of an individual’s rights and interests; hereinafter the same in this Article and the succeeding paragraph, and, Article 26-2, paragraph (1), item (ii)), in advance obtain a principal’s consent to the effect that he or she approves the provision to a third party in a foreign country. In this case, the provisions of the preceding Article shall not apply.

(2) A personal information handling business operator shall, in case of intending to obtain a principal’s consent pursuant to the provisions of the preceding paragraph, in advance provide the principal with information on the personal information protection system of the foreign country, on the action the third party takes for the protection of personal information, and other information that is to serve as a reference to the principal, pursuant to rules of the Personal Information Protection Commission.

(3) A personal information handling business operator shall, when having provided personal data to a third party (limited to person establishing a system prescribed in paragraph (1)) in a foreign country, pursuant to rules of the Personal Information Protection Commission, take necessary action to ensure continuous implementation of the equivalent action by the third party, and, in response to a principal's request, provide information on the necessary action, to the principal.

(Keeping etc. of a Record on a Third-Party Provision)

Article 25

(1) A personal information handling business operator shall, when having provided personal data to a third party (excluding a person set forth in each item of Article 2, paragraph (5); hereinafter the same in this Article and the succeeding Article (including cases where it is applied mutatis mutandis pursuant to Article 26-2, paragraph (3) following the deemed replacement of terms)), keep a record pursuant to rules of the Personal Information Protection Commission on the date of the personal data

provision, the name or appellation of the third party, and other matters prescribed by rules of the Personal Information Protection Commission. This, however, shall not apply in cases where the personal data provision falls under any of each item of Article 23, paragraph (1) or paragraph (5) (this means, in case of a personal data provision pursuant to the provisions of the preceding Article, paragraph (1), any of each item of Article 23, paragraph (1)).

(2) A personal information handling business operator shall maintain a record under the preceding paragraph for a period of time prescribed by rules of the Personal Information Protection Commission from the date when it kept the record.

(Confirmation etc. when Receiving a Third Party Provision)

Article 26

(1) A personal information handling business operator shall, when receiving the provision of personal data from a third party, confirm those matters set forth in the following pursuant to rules of the Personal Information Protection Commission. This, however, shall not apply in cases where the said personal data provision falls under any of each item of Article 23, paragraph

(1) or paragraph (5).

(i) the name or appellation and address and, for a corporate body, the name of its representative of the third party

(ii) circumstances under which the said personal data was acquired by the said third party

(2) A third party under the preceding paragraph shall, in cases where a personal information handling business operator confirms pursuant to the provisions of the preceding paragraph, not deceive the personal information handling business operator on a matter relating to the confirmation.

(3) A personal information handling business operator shall, when having confirmed pursuant to the provisions of paragraph (1), keep a record pursuant to rules of the Personal Information Protection Commission on the date when it received the provision of personal data, a matter concerning the said confirmation, and other matters prescribed by rules of the Personal Information Protection Commission.

(4) A personal information handling business operator shall maintain a record under the preceding paragraph for a period of time prescribed by rules of the Personal Information Protection Commission from the date when it kept the record.

(Restriction on Third Party Provision of Personally Referable Information)

Article 26-2

(1) A personally referable information handling business operator (meaning a person providing a personally referable information database etc. (Meaning a collective body of information comprising personally referable information (Meaning information relating to a living individual which does not fall under personal information, pseudonymously processed information or anonymously processed information; the same applies hereinafter) which has been systematically organized so as to be able to search using a computer for specific personally referable information or similar others prescribed by cabinet order as systematically organized so as to be able to search easily for specific personally referable information; the same applies hereinafter) for use in business, however, excluding a person set forth in each item of Article 2, paragraph (5); the same applies hereinafter) shall, if it is assumed that a third party will acquire personally referable information (limited to those constituting personally referable information database etc.; the same applies hereinafter) as personal data, except in those cases set forth in each item of Article 23, paragraph (1), not provide the personally referable information to a third party without confirming those matters set forth in the following pursuant to rules of the Personal Information Protection Commission.

(i) The principal's consent to the effect that he or she approves that the third party acquires personally referable information as personal data that can identify the principal receives the provision of personally referable information from handling business operator, has been obtained.

(ii) For a provision to a third party in a foreign country, in case of intending to obtain the principal's consent referred to in the preceding item, pursuant to rules of the Personal Information Protection Commission, information on the personal information protection system of the foreign country, on the action the third party takes for the protection of personal information, and other information that is to serve as a reference to the principal, have been provided in advance to the principal.

(2) The provisions of Article 24, paragraph (3) shall apply mutatis mutandis to the case that a personally referable information handling business operator provides personally referable information pursuant to the provisions of the preceding paragraph. In this case, the term "take necessary action to ensure continuous implementation of the equivalent action by the third party, and, in response to a principal's request, provide information on the necessary action, to the principal." in Article 24, paragraph (3) is deemed to be replaced with "take necessary action to ensure continuous implementation of the equivalent action by the third party."

(3) The provisions of preceding Article, paragraph (2) through paragraph (4) shall

apply mutatis mutandis to the case that a personally referable information handling business operator confirms pursuant to the provisions of paragraph (1). In this case, the term “received the provision of” in the preceding Article, paragraph (3) is deemed to be replaced with “provided.”

(Public Disclosure etc. on Matters relating to Retained Personal Data)

Article 27

(1) A personal information handling business operator shall, concerning its retained personal information, put those matters set forth in the following into a state where a principal can know (including those cases in which it, at the request of a principal, responds without delay).

(i) the name or appellation and address and, for a corporate body, the name of its representative of the said personal information handling business operator

(ii) the utilization purpose of all retained personal data (excluding those cases falling under item (i) through item (iii) of Article 18, paragraph (4))

(iii) the procedures for responding to a request pursuant to the provisions of the succeeding paragraph, or, a demand pursuant to the provisions of the succeeding Article, paragraph (1) (including as applied mutatis mutandis pursuant to the succeeding Article, paragraph (5)); Article 29, paragraph (1); or Article 30, paragraph (1), paragraph (3) or paragraph (5) (including, when the amount of a fee has been decided pursuant to the provisions of Article 33, paragraph (2), the amount of the fee)

(iv) besides those set forth under the preceding three items, those prescribed by cabinet order as a necessary matter to ensure the proper handling of retained personal data

(2) A personal information handling business operator shall, when requested by a principal to get informed of a utilization purpose of retained personal data that can identify the principal, inform the said principal thereof without delay. This, however, shall not apply in those cases falling under any of each following item.

(i) cases in which the utilization purpose of retained personal data that can identify the said principal is clear pursuant to the provisions of the preceding paragraph

(ii) cases falling under item (i) through item (iii) of Article 18, paragraph (4)

(3) A personal information handling business operator shall, when having been requested based on the provisions of the preceding paragraph but decided not to inform a principal of the utilization purpose of retained personal data, inform the principal to that effect without delay.

(Disclosure)

Article 28

(1) A principal may demand of a personal information handling business operator disclosure of retained personal data that can identify him or herself by a method of providing electromagnetic record or other methods prescribed by rules of the Personal Information Protection Commission.

(2) A personal information handling business operator shall, when having received a demand pursuant to the provisions of the preceding paragraph, disclose retained personal data to a principal without delay pursuant to a method the principal demands pursuant to the provisions of the preceding paragraph (in cases where disclosure by the method requires a large amount of expenses or when disclosure by other said method is difficult, by a method of delivering a written document). However, in cases where disclosing such data falls under any of each following item, a whole or part thereof may not be disclosed.

(i) cases in which there is a possibility of harming a principal or third party's life, body, fortune or other rights and interests

(ii) cases in which there is a possibility of interfering seriously with the said personal information handling business operator implementing its business properly

(iii) cases of violating other laws or regulations

(3) A personal information handling business operator shall, when having decided not to disclose a whole or part of retained personal data in connection with a demand pursuant to the provisions of paragraph (1), when the retained personal data does not exist, or, when disclosure by a method a principal demanded pursuant to the provisions of the said paragraph is difficult, inform a principal thereof without delay.

(4) In cases where a whole or part of retained personal data that can identify a principal is to be disclosed to the principal pursuant to the provisions of other laws or regulations using a method equivalent to that prescribed in the main clause of paragraph (2), the provisions of paragraph (1) and paragraph (2) shall not apply in regard to the said whole or part of retained personal data.

(5) The provisions of paragraph (1) through paragraph (3) shall apply mutatis mutandis to records (excluding those prescribed by cabinet order as likely to harm the public or other interests if their presence or absence is made known; referred to as a "Third party provision record" in Article 32,

paragraph (2)) in Article 25, paragraph (1) and Article 26, paragraph (3) related to personal data that can identify the principal.

(Correction etc.)

Article 29

(1) A principal may, when the contents of retained personal data that can identify the principal are not factual, demand of a personal information handling business operator making a correction, addition or deletion (hereinafter referred to as a “correction etc.” in this Article) in regard to the contents of the retained personal data.

(2) A personal information handling business operator shall, in case of having received a demand pursuant to the provisions of the preceding paragraph except in cases where special procedure concerning a correction etc. of the contents is prescribed by the provisions of other laws or regulations, conduct a necessary investigation without delay to the extent necessary to achieve a utilization purpose and, based on the result thereof, make a correction etc. of the contents of the retained personal data.

(3) A personal information handling business operator shall, when having made a correction etc. on a whole or part of the contents of the retained personal data in connection with a demand pursuant to the provisions under paragraph (1) or when having made a decision not to make a correction etc., inform a principal without delay to that effect (including, when having made a correction etc., the contents thereof).

(Utilization Cease etc.)

Article 30

(1) A principal may, when retained personal data that can identify the principal is being handled in violation of the provisions of Article 16 or Article 16-2, or, has been acquired in violation of the provisions of Article 17, demand of a personal information handling business operator a utilization cease or deletion (hereinafter referred to as a “utilization cease etc.” in this Article) of the retained personal data.

(2) A personal information handling business operator shall, in case of having received a demand pursuant to the provisions of the preceding paragraph and when it has become clear that there is a reason in the demand, fulfill a utilization cease etc. of the said retained personal data to the extent necessary to redress a violation without delay. This, however, shall not apply in cases where a

utilization cease etc. of the said retained personal data requires a large amount of expenses or other cases where it is difficult to fulfil a utilization cease etc. and when necessary alternative action is taken to protect a principal's rights and interests.

(3) A principal may, when retained personal data that can identify the principal is being provided to a third party in violation of the provisions of Article 23, paragraph (1) or Article 24, demand of a personal information handling business operator ceasing a third-party provision of the retained personal data.

(4) A personal information handling business operator shall, in case of having received a demand pursuant to the provisions of the preceding paragraph and when it has become clear that there is a reason in the demand, cease a third- party provision of the retained personal data without delay. This, however, shall not apply in cases where ceasing a third-party provision of the said retained personal data requires a large amount of expenses or other cases where it is difficult to cease a third-party provision and when necessary alternative action is taken to protect a principal's rights and interests.

(5) A principal may demand that the personal information handling business operator fulfill a utilization cease etc. of the retained personal data, or cease a third-party provision, if it has become unnecessary for a personal information handling business operator to utilize retained personal data that can identify the principal, if a situation prescribed in the main clause of Article 22-2, paragraph

(1) has occurred in connection with the retained personal data that can identify the principal, or there is a possibility that handling of the retained personal data that can identify the principal would harm the rights or legitimate interests of the principal.

(6) A personal information handling business operator shall, in case of having received a demand pursuant to the provisions of the preceding paragraph and when it has become clear that there is a reason in the demand, fulfill a utilization cease etc. or cease a third-party provision of the said retained personal data to the extent necessary to prevent an infringement of a principal's rights and interests without delay. This, however, shall not apply in cases where a utilization cease etc. or ceasing a third-party provision of the said retained personal data requires a large amount of expenses or other cases where it is difficult to fulfil a utilization cease etc. or to cease a third-party provision and when necessary alternative action is taken to protect a principal's rights and interests.

(7) A personal information handling business operator shall, when having fulfilled a utilization cease etc. or decided not to fulfill a utilization cease etc. of a whole or part of retained personal data in connection with a demand pursuant to the provisions of paragraph (1) or paragraph (5), or, when

having ceased a third- party provision or decided not to cease a third-party provision of a whole or part of retained personal data in connection with a demand pursuant to the provisions of paragraph (3) or paragraph (5), inform a principal to that effect without delay.

(Explanation of Reason)

Article 31

A personal information handling business operator shall, in case of informing a principal to the effect that, as regards a whole or part of action

requested or demanded by the principal pursuant to the provisions of Article 27, paragraph (3); Article 28, paragraph (3) (including as applied mutatis mutandis pursuant to the succeeding Article 28, paragraph (5)); Article 29, paragraph (3); or the preceding Article, paragraph (7), the action will not be taken, or to the effect that different action from the said action will be taken, strive to explain a reason therefor to the said principal.

(Procedure for Responding to a Demand etc. for Disclosure etc.)

Article 32

(1) A personal information handling business operator may, as regards a request pursuant to the provisions of Article 27, paragraph (2), or, a demand pursuant to the provisions of Article 28, paragraph (1) (including as applied mutatis mutandis pursuant to the succeeding Article 28, paragraph (5); the same apply in the following Article, paragraph (1) and Article 34); Article 29, paragraph (1); Article 30, paragraph (1), paragraph (3) or paragraph (5) (hereinafter referred to as a "demand etc. for disclosure etc." in this Article and Article 53, paragraph (1)), decide on a method of receiving a request or demand pursuant to those prescribed by cabinet order. In this case, a principal shall make a demand etc. for disclosure etc. in accordance with the method.

(2) A personal information handling business operator may, as regards a demand etc. for disclosure etc., request a principal to present a matter sufficient to specify retained personal data or a third party provision record subject to the demand etc. In this case, a personal information handling business operator shall take appropriate action in consideration of a principal's convenience such as providing information conducive to specify the retained personal data or the third party provision record so that the principal would be able to easily and precisely make a demand etc. for disclosure etc.

(3) A demand etc. for disclosure etc. may be made through an agent pursuant to those prescribed by cabinet order.

(4) A personal information handling business operator shall, in establishing a procedure for responding to a demand etc. for disclosure etc. based on the provisions of the preceding three paragraphs, give consideration so as not to impose excessive burden on a principal.

(Fee)

Article 33

(1) A personal information handling business operator may, when having been requested to inform of a utilization purpose pursuant to the provisions of Article 27, paragraph (2) or when having received a demand for disclosure pursuant to the provisions of Article 28, paragraph (1), collect a fee in relation to taking

such action.

(2) A personal information handling business operator shall, in case of collecting a fee pursuant to the provisions of the preceding paragraph, decide on the amount of the fee within a range recognized as reasonable considering actual expenses.

(Advance Demand)

Article 34

(1) A principal may, when intending to file a lawsuit in connection with a demand pursuant to the provisions of Article 28, paragraph (1); Article 29, paragraph (1); or Article 30, paragraph (1), paragraph (3) or paragraph (5), not file the lawsuit unless the principal had previously issued the demand against a person who should become a defendant in the lawsuit and two weeks have passed from the delivery day of the issued demand. This, however, shall not apply when the person who should become a defendant in the lawsuit has rejected the demand.

(2) A demand under the preceding paragraph is deemed as having been delivered at the time when such a demand should have normally been delivered.

(3) The provisions of the preceding two paragraphs shall apply mutatis mutandis to a petition for a provisional disposition order in connection with a demand pursuant to the provisions of Article 28, paragraph (1); Article 29, paragraph (1); or Article 30, paragraph (1), paragraph (3) or paragraph (5).

(Personal Information Handling Business Operator's Dealing with a Complaint)

Article 35

(1) A personal information handling business operator shall strive to deal appropriately and promptly with a complaint about the handling of personal information.

(2) A personal information handling business operator shall strive to establish a system necessary to achieve a purpose under the preceding paragraph.

Section 2 Obligations of a Pseudonymously Processed Information Handling Business Operator etc.

(Production etc. of Pseudonymously Processed Information)

Article 35-2

(1) A personal information handling business operator shall, when producing pseudonymously processed information (limited to those constituting pseudonymously processed information database etc.; hereinafter the same), process personal information in accordance with standards prescribed by rules of the Personal Information Protection Commission as those necessary to make it impossible to identify a specific individual unless collated with other information.

(2) A personal information handling business operator, when having produced pseudonymously processed information or having acquired pseudonymously processed information and deleted information etc. (meaning information related to descriptions etc. and individual identification codes that were deleted from personal information that was used to produce the pseudonymously processed information, and, a method of processing carried out pursuant to the provisions of the preceding paragraph; hereinafter the same applies in this Article, and in Article 35-2, paragraph (7), as applied mutatis mutandis pursuant to Article 35-3, paragraph (3) following the deemed replacement of terms) related to the pseudonymously processed information shall, in accordance with standards prescribed by rules of the Personal Information Protection Commission as those necessary to prevent the leakage of deleted information etc., take action for the security control of deleted information etc.

(3) A pseudonymously processed information handling business operator (limited to those that are personal information handling business operators; hereinafter the same applies in this Article) shall, notwithstanding the provision of Article 16, except in cases based on laws and regulations, not handle a pseudonymously processed information (limited to those that are personal information;

hereinafter the same applies in this Article) beyond the necessary scope to achieve the utilization purpose specified pursuant to the provisions of Article 15, paragraph (1).

(4) With regard to applying the provisions of Article 18 related to pseudonymously processed information, the phrase “inform a principal of, or disclose to the public” in Article 18, paragraph (1) and paragraph (3) is deemed to be replaced with “disclose to the public”; the phrase “informing a principal of, or disclosing to the public,” in the provisions of Article 18, paragraph (4), item (i) through (iii), is deemed to be replaced with “disclosing to the public”.

(5) A pseudonymously processed information handling business operator shall strive to delete personal data that are pseudonymously processed information and deleted information etc. without delay when utilization of the personal data and the deleted information etc. has become unnecessary. In this case, the provisions of Article 19 shall not apply.

(6) A pseudonymously processed information handling business operator shall, notwithstanding the provisions of Article 23, paragraph (1) and paragraph (2), and, Article 24, paragraph (1), except in cases based on laws and regulations, not provide personal data that is pseudonymously processed information to a third party. In this case, the phrase “each preceding paragraph” in Article 23, paragraph (5) is deemed to be replaced with “Article 35-2, paragraph (6)”; the phrase “a principal has in advance been informed or a state has been in place

where a principal can easily know” in item (iii) of the said paragraph, is deemed to be replaced with “it is disclosed to the public in advance”; the phrase “inform a principal of the contents to be altered or put them into a state where a principal can easily know” in Article 23, paragraph (6), is deemed to be replaced with “disclose to the public, the contents to be altered”; the phrase “any of each item of Article 23, paragraph (1) or paragraph (5) (this means, in case of a personal data provision pursuant to the provisions of the preceding Article, any of each item of Article 23, paragraph (1))” in the proviso of Article 25, paragraph (1), and, the phrase “any of each item of Article 23, paragraph (1) or paragraph (5)” in the proviso of Article 26, paragraph (1), is deemed to be replaced with “cases based on laws and regulations or any of each item of Article 23, paragraph (5)”.

(7) A pseudonymously processed information handling business operator, shall, in handling pseudonymously processed information, not collate the said pseudonymously processed information with other information in order to identify a principal concerned with personal information used to produce the pseudonymously processed information.

(8) A pseudonymously processed information handling business operator, shall, in handling pseudonymously processed information, not utilize a contact address and other information contained in the pseudonymously processed information for telephoning, sending by post or by a correspondence delivery prescribed in Article 2, paragraph (2) of the Act on Correspondence Delivery by Private Business Operators (Act No. 99 of 2002) conducted by a general correspondence delivery operator prescribed in Article 2, paragraph (6) or a specified letter delivery operator prescribed in Article 2, paragraph (9), delivering a telegram, transmitting by using a facsimile machine or electronic or magnetic means (meaning means that use electronic data processing system or means that utilize other information communication technology as prescribed by rules of the Personal Information Protection Commission), or, visiting a residence.

(9) The provisions of Article 15, paragraph (2), Article 22-2 and Article 27 through Article 34 shall not apply in regard to pseudonymously processed information, personal data that is pseudonymously processed information and retained personal data that is pseudonymously processed information.

(Restriction etc. on Third Party Provision of Pseudonymously Processed Information)

Article 35-3

(1) A pseudonymously processed information handling business operator shall, except in cases based on laws and regulations, not provide pseudonymously processed information (excluding those that are personal information; the same shall apply in the succeeding paragraph and paragraph (3)) to a third party.

(2) The provisions of Article 23, paragraph (5) and paragraph (6) shall apply mutatis mutandis to a person receiving the provision of pseudonymously

processed information. In this case, the phrase “each preceding paragraph” in Article 23, paragraph (5) is deemed to be replaced with “Article 35-3, paragraph (1)”; the term “personal information handling business operator” in item (i) of the said paragraph, is deemed to be replaced with “pseudonymously processed information handling business operator”; the phrase “a principal has in advance been informed or a state has been in place where a principal can easily know” in item (iii) of the said paragraph, is deemed to be replaced with “it is disclosed to the public”; the term “personal information handling business operator” in Article 23, paragraph (6), is deemed to be replaced with “pseudonymously processed information handling business operator” and the phrase “inform a principal of the contents to be altered or put them into a state where a principal can easily know” is

deemed to be replaced with “disclose to the public, the contents to be altered” in Article 23, paragraph (6).

(3) The provisions of Article 20 through Article 22, Article 35, and, paragraph (7) and paragraph (8) of the preceding Article shall apply mutatis mutandis to the handling of pseudonymously processed information by a pseudonymously processed information handling business operator. In this case, the phrase “leakage, loss or damage” in Article 20 is deemed to be replaced with “leakage” and the phrase “not” in Article 35-2, paragraph (7) is deemed to be replaced with “neither acquire deleted information etc., nor”.

Section 3 Obligations of an Anonymously Processed Information Handling Business Operator etc.

(Production etc. of Anonymously Processed Information)

Article 36

(1) A personal information handling business operator shall, when producing anonymously processed information (limited to those constituting anonymously processed information database etc.; hereinafter the same), process personal information in accordance with standards prescribed by rules of the Personal Information Protection Commission as those necessary to make it impossible to identify a specific individual and restore the personal information used for the production.

(2) A personal information handling business operator, when having produced anonymously processed information, shall, in accordance with standards prescribed by rules of the Personal Information Protection Commission as those necessary to prevent the leakage of information relating to those descriptions etc. and individual identification codes deleted from personal information used to produce the anonymously processed information, and information relating to a processing method carried out pursuant to the provisions of the preceding paragraph, take action for the security control of such information.

(3) A personal information handling business operator, when having produced anonymously processed information, shall, pursuant to rules of the Personal Information Protection Commission, disclose to the public the categories of information relating to an individual contained in the anonymously processed information.

(4) A personal information handling business operator, when having produced anonymously processed information and providing the anonymously processed information to a third party, shall, pursuant to rules of the Personal Information Protection Commission, in advance disclose to the

public the categories of information concerning an individual contained in anonymously processed information to be provided to a third party and its providing method, and state to the third party explicitly to the effect that the information being provided is anonymously processed information.

(5) A personal information handling business operator shall, when having produced anonymously processed information and making itself handle the anonymously processed information, not collate the said anonymously processed information with other information in order to identify a principal concerned with personal information used to produce the said anonymously processed information.

(6) A personal information handling business operator shall, when having produced anonymously processed information, strive to take itself necessary and appropriate action for the security control of the anonymously processed information and necessary action for ensuring the proper handling of the anonymously processed information such as dealing with a complaint about the handling, including producing, of the said anonymously processed information, and strive to disclose to the public the contents of such action taken.

(Provision of Anonymously Processed Information)

Article 37

An anonymously processed information handling business operator, when providing anonymously processed information (excluding those which it produced itself by processing personal information; hereinafter the same in this Section) to a third party, shall, pursuant to rules of the Personal Information Protection Commission, in advance disclose to the public the categories of personal information contained in anonymously processed information to be provided to a third party and state to the third party explicitly to the effect that the provided information is anonymously processed information.

(Prohibition against the Act of Identifying)

Article 38

An anonymously processed information handling business operator, shall, in handling anonymously processed information, neither acquire information relating to those descriptions etc. or individual identification codes deleted from the personal information and information relating to a processing method carried out pursuant to the provisions of Article 36, paragraph (1), nor collate the said anonymously processed information with other information in order to identify a principal concerned with personal information used to produce the anonymously processed information.

(Security Control Action etc.)

Article 39

An anonymously processed information handling business operator shall strive to take itself necessary and appropriate action for the security control of anonymously processed information and necessary action to ensure the proper handling of anonymously processed information such as dealing with a complaint about the handling of anonymously processed information, and shall strive to disclose to the public the contents of such action taken.

Section 4 Supervision

(Report and Onsite Inspection)

Article 40

(1) The Personal Information Protection Commission may, to the extent necessary to implement the provisions under the preceding three Sections and this Section, require a personal information handling business operator, a personally referable information handling business operator, pseudonymously processed information business operator or anonymously processed information handling business operator (hereinafter referred to collectively as a “personal information handling business operator etc.”) and other concerned person to submit necessary information or material relating to the handling of personal information, personally referable information, pseudonymously processed information or anonymously processed information (hereinafter referred to collectively as “personal information etc.”), or have its officials enter a business office or other necessary place of a personal information handling business operator etc. or other concerned person, inquire about the handling of personal information etc., or inspect a book, document and other property.

(2) An official who conducts an onsite inspection pursuant to the provisions of the preceding paragraph shall carry a certificate for identification, and present it when requested by a person concerned.

(3) An onsite inspection authority pursuant to the provisions of paragraph (1) shall not be construed as granted for a criminal investigation.

(Guidance and Advice)

Article 41

The Personal Information Protection Commission may, to the extent necessary to implement the provisions under the preceding three Sections, provide a personal information handling business operator etc. with necessary guidance or advice on the handling of personal information etc.

(Recommendation and Order)

Article 42

(1) The Personal Information Protection Commission may, when recognizing there is a need for protecting an individual's rights and interests in cases where a personal information handling business operator has violated the provisions under Article 16 through Article 17, Article 18 (including the cases where the provisions under paragraph (1), (3) and (4) are applied with replacement of terms pursuant to the Article 35-2, paragraph (4)), Article 20 through Article 22- 2, Article 23 (excluding paragraph (4); including the cases where the provisions under paragraph (5) and (6) are applied with replacement of terms pursuant to Article 35-2, paragraph (6)), Article 24, Article 25 (including the cases where the provisions of proviso of paragraph (1) is applied with replacement of terms pursuant to Article 35-2, paragraph (6)), Article 26 (excluding paragraph (2); including the cases where the provisions of proviso of paragraph (1) is applied with replacement of terms pursuant to Article 35-2, paragraph (6)), Article 27, Article 28 (excluding paragraph (1) (including as applied mutatis mutandis pursuant to paragraph (5)), Article 29, paragraph (2) or (3), Article 30 (excluding paragraph (1), (3) and (5)), Article 33, paragraph (2), Article 35-2 (excluding paragraph (4) and (5)) or Article 36 (excluding paragraph (6)), in cases where a personally referable information handling business operator has violated the provisions under Article 26-2, paragraph (1), or, the provisions of Article 24, paragraph (3), as applied mutatis mutandis pursuant to Article 26-2, paragraph

(2) following the deemed replacement of terms, or, the provisions of Article 26, paragraph (3) or (4), as applied mutatis mutandis pursuant to Article 26-2, paragraph (3) following the deemed replacement of terms, in cases where a pseudonymously processed information handling business operator has violated the provisions under Article 35-3, paragraph (1), or, Article 23, paragraph (5) or (6), as applied mutatis mutandis pursuant to Article 35-3, paragraph (2) following the deemed replacement of terms, or, the provisions under Article 20 through Article 22 or Article 35-2, paragraph (7) or (8) as applied mutatis mutandis pursuant to Article 35-3, paragraph (3) following the deemed replacement of terms, or, in cases where an anonymously processed information handling business operator has violated the provisions under Articles 37 or 38, recommend the personal information

handling business operator etc. to suspend the act of violating or take other necessary action to rectify the violation.

(2) The Personal Information Protection Commission may, when recognizing that a serious infringement of an individual's rights and interests is imminent in cases where a personal information handling business operator etc. having received a recommendation pursuant to the provisions under the preceding paragraph did not take action in line with the recommendation without legitimate ground, order the personal information handling business operator etc. to take action in line with the said recommendation.

(3) The Personal Information Protection Commission may, notwithstanding the provisions under the preceding two paragraphs when recognizing there is a

need to take urgent action because there is a fact that seriously harms an individual's rights and interests in cases where a personal information handling business operator has violated the provisions under Article 16 through Article 17, Article 20 through Article 22-2, Article 23, paragraph (1), Article 24,

paragraph (1) or (3), Article 35-2, paragraph (1) through (3), or paragraph (6)

through (8), or Article 36, paragraph (1), paragraph (2) or paragraph (5), in cases where a personally referable information handling business operator has violated the provisions under Article 26-2, paragraph (1), or, Article 24, paragraph (3), as applied mutatis mutandis pursuant to Article 26-2, paragraph

(2) following the deemed replacement of terms, in cases where a pseudonymously processed information handling business operator has violated the provisions under Article 35-3, paragraph (1), or, Article 20 through Article 22 or Article 35-2, paragraph (7) or (8), as applied mutatis mutandis pursuant to Article 35-3, paragraph (3) following the deemed replacement of terms, or, in cases where an anonymously processed information handling business operator has violated the provisions under Article 38, order the personal information handling business operator etc. to take necessary action to rectify the violation such as suspending the act of violation.

(4) The Personal Information Protection Commission may, in case of issuing an order pursuant to the provisions under the preceding two paragraphs, when the personal information handling business operator etc. that has received the order has violated the order, make public announcement to that effect.

(Restriction on the Personal Information Protection Commission's Exercising the Authority)

Article 43

(1) The Personal Information Protection Commission shall, in the course of requiring the submission of a report or material from, conducting an onsite inspection of, or giving a guidance, advice, recommendation or order to, a personal information handling business operator etc., not hinder the freedom of expression, freedom of academia, freedom of religion, and freedom of political activity.

(2) In light of the purport of the provisions of the preceding paragraph, the Personal Information Protection Commission shall not exercise the authorities in regard to a personal information handling business operator's act of providing personal information etc. to a person set forth in each item of Article 76, paragraph (1) (limited to those cases where each person handles personal information etc. for a purpose stipulated in each said item respectively).

(Delegation of Authority)

Article 44

(1) The Personal Information Protection Commission may, when recognizing that there is a need for effectively giving a personal information handling business operator a recommendation pursuant to the provisions of Article 42, paragraph

(1) or order pursuant to the provisions of Article 42, paragraph (2) or (3) because there is a need to urgently and intensively seek ensuring the proper handling of personal information etc. or similar other circumstances prescribed by cabinet order, delegate an authority under the provisions of Article 22-2, paragraph (1), Article 40, paragraph (1), the Code of Civil Procedure (Act No. 109 of 1996) Article 99, Article 101, Article 103, Article 105, Article 106, Article 108 and Article 109, as applied mutatis mutandis pursuant to Article 58-3 following the deemed replacement of terms, Article 58-4 and Article 58-5 to a business jurisdictional minister as prescribed by cabinet order.

(2) A business jurisdictional minister shall, when having exercised an authority delegated pursuant to the provisions of the preceding paragraph, report the results thereof to the Personal Information Protection Commission as prescribed by cabinet order.

(3) A business jurisdictional minister may, as prescribed by cabinet order, delegate a whole or part of an authority delegated pursuant to the provisions of paragraph (1) or a whole or part of an authority pursuant to the provisions of the preceding paragraph to a head of a local branch bureau under Article 43 of the Act for Establishment of the Cabinet Office (Act No.89 of 1999) or other bureau or organ prescribed by cabinet order.

(4) The Prime Minister delegates an authority delegated pursuant to the provisions of paragraph (1) and an authority under the provisions of paragraph (2) (limited to those relating to the Financial Services Agency's jurisdiction and excluding those prescribed by cabinet order) to a Commissioner of the Financial Services Agency.

(5) A Commissioner of the Financial Services Agency may, as prescribed by cabinet order, delegate part of an authority delegated pursuant to the provisions of the preceding paragraph to the Securities and Exchange Surveillance Commission.

(6) A Commissioner of the Financial Services Agency may, as prescribed by cabinet order, delegate part of an authority delegated pursuant to the provisions of paragraph (4) (excluding those delegated to the Securities and Exchange Surveillance Commission pursuant to the provisions of the preceding paragraph) to a Director-General of a local finance bureau or local finance branch bureau.

(7) The Securities and Exchange Surveillance Commission may, as prescribed by cabinet order, delegate part of an authority delegated pursuant to the provisions of paragraph (5) to a Director-General of a local finance bureau or local finance branch bureau.

(8) As for administrative affairs relating to an authority delegated to a Director-General of a local finance bureau or local finance branch bureau pursuant to the provisions of the preceding paragraph, the Securities and Exchange Surveillance Commission directs and supervises a Director-General of a local finance bureau or local finance branch bureau.

(9) In case of paragraph (5), a request for administrative review concerning the Securities and Exchange Surveillance Commission's requiring the submission of a report or material (including those cases in which a Director-General of a local finance bureau or local finance branch bureau do so pursuant to the provisions of paragraph (7)) may only be filed against the Securities and Exchange Surveillance Commission.

(Request by Business Jurisdictional Minister)

Article 45

A business jurisdictional minister may, when recognizing that there is a need for ensuring the proper handling of personal information etc. by a personal information handling business operator etc. including that there is an act of a personal information handling business operator etc. violating the provisions under the preceding three Sections, request the Personal Information Protection Commission to take appropriate action in accordance with the provisions of this Act.

(Business Jurisdictional Minister)

Article 46

A business jurisdictional minister in the provisions of this Section shall be as follows.

(i) as for those relating to employment management involved in the handling of personal information etc. by a personal information handling business operator etc.; a Minister of Health, Labor and Welfare (as for those relating to a mariner's employment management; a Minister of Land, Infrastructure, Transport and Tourism), and a minister having jurisdiction over a business conducted by a said personal information handling business operator or the National Public Safety Commission (referred to collectively as a "Minister etc." in the succeeding item)

(ii) as for those other than the ones set forth in the preceding item involved in the handling of personal information etc. by a personal information handling business operator etc.; a Minister etc. having jurisdiction over a business conducted by a said personal information handling business operator

Section 5 Private-Sector Body's Promotion for the Protection of Personal Information

(Accreditation)

Article 47

(1) A corporation (including a non-corporate body which has appointed a representative or administrator; the same shall apply in the succeeding Article, item (iii), (b)) which intends to render the following services in order to ensure the proper handling of personal information etc. (excluding personally referable information; hereinafter the same applies in this Section) by a personal information handling business operator etc. (excluding personally referable information handling business operator; hereinafter the same applies in this Section) may receive an accreditation from the Personal Information Protection Commission.

(i) dealing with a complaint under the provisions of Article 52 about the handling of personal information etc. by a personal information handling business operator covered by the services (hereinafter referred to as a "covered business operator")

(ii) providing a covered business operator with information concerning a matter contributory to ensuring the proper handling of personal information etc.

(iii) besides those set forth in the preceding two items, rendering necessary services related to ensuring the proper handling of personal information etc. by a covered business operator

(2) The accreditation set forth in the preceding paragraph may be limited in respect of the type or scope of services of personal information handling business operator etc.

(3) A person who intends to receive an accreditation under paragraph (1) shall, as prescribed by cabinet order, apply to the Personal Information Protection Commission.

(4) The Personal Information Protection Commission shall, when having granted an accreditation under the paragraph (1), announce to the public to that effect (including the scope of services concerning the accreditation, in cases of the accreditation limiting the scope of services pursuant to the provisions of paragraph (2)).

(Disqualification)

Article 48

A person falling under any of each following item shall not receive an accreditation under the paragraph (1) of the preceding Article.

(i) a person who has been sentenced to imprisonment pursuant to the provisions of this Act and for whom two years have not elapsed since the date of either the completion of, or the conclusion of being subject to, the execution of the sentence

(ii) a person whose accreditation was rescinded pursuant to the provisions of Article 58, paragraph (1) and for whom two years have not elapsed since the date of the rescission

(iii) those of which the directors rendering the said services (including a representative or administrator of a non-corporate body which has appointed a representative or administrator; hereinafter the same in this Article) encompass a person who falls under any of the following

(a) a person who has been sentenced to imprisonment or a severer punishment or who has been sentenced pursuant to the provisions of this Act and for whom two years have not elapsed since the date of either the completion of, or the conclusion of being subject to, the execution of the sentence

(b) a person who was a director of a corporation whose accreditation was rescinded pursuant to the provisions of Article 58, paragraph (1) within thirty days prior to the date of the rescission and for whom two years have not elapsed since the date of the rescission

(Accreditation Standards)

Article 49

The Personal Information Protection Commission shall not grant an accreditation unless it recognizes that an accreditation application under Article 47, paragraph (1) conforms to all of each following item.

(i) a service-rendering method has been devised necessary to perform properly and assuredly those services set forth in each item of Article 47, paragraph (1)

(ii) knowledge, capability and financial base have been demonstrated as sufficient to perform properly and assuredly those services set forth in each item of Article 47, paragraph (1)

(iii) in cases where services other than those services set forth in each item of Article 47, paragraph (1) are being rendered, there is no possibility that rendering such other services disturb the fairness of those services set forth in each item of the said paragraph

(Accreditation of alteration etc.)

Article 49-2

(1) A person who has received an accreditation under Article 47, paragraph (1) (including the accreditation limiting the scope of services pursuant to the provisions of Article 47, paragraph (2); the same applies to Article 48, paragraph (1) and Article 58, paragraph (1), item (v)) must, when intending to

alter the scope of services concerning the accreditation, receive an accreditation from the Personal Information Protection Commission. This, however, shall not apply to a minor alteration as specified by the rules of the Personal Information Protection Commission.

(2) The provisions of Article 47, paragraph (3), (4) and the preceding Article shall apply mutatis mutandis to the accreditation of alteration in the preceding paragraph.

(Notification of Termination)

Article 50

(1) A person who has received an accreditation (including the accreditation of alteration in the preceding Article, paragraph (1)) under Article 47, paragraph

(1) (hereinafter referred to as an “accredited personal information protection organization”) shall, when intending to terminate services concerning the accreditation (hereinafter referred to as “accredited services”), in advance notify the Personal Information Protection Commission to that effect as prescribed by cabinet order.

(2) The Personal Information Protection Commission shall, when notified pursuant to the provisions of the preceding paragraph, announce to the public to that effect.

(Covered Business Operator)

Article 51

(1) An accredited personal information protection organization shall make its covered business operators composed of a personal information handling business operator etc. who has consented to becoming covered by the accredited services. In this case, if a covered business operator does not fulfill the personal information protection guideline prescribed by Article 53, paragraph (1) even though actions pursuant to Article 53, paragraph (4) was taken, the covered business operator may be excluded from being covered by the accredited services.

(2) An accredited personal information protection organization shall announce to the public the name or appellation of its covered business operators.

(Dealing with a Complaint)

Article 52

(1) An accredited personal information protection organization shall, when petitioned by a principal or other concerned person to resolve a complaint about its covered business operator's handling of personal information etc., hold consultation, give necessary advice to the petitioner and investigate circumstances surrounding the complaint, as well as inform the covered business operator of the complaint contents and request its expeditious resolution.

(2) An accredited personal information protection organization may, when recognizing that there is a need in regard to the resolution of a complaint in connection with a petition under the preceding paragraph, request the covered business operator to provide a written or oral explanation or submit a referential material.

(3) A covered business operator shall, when requested by an accredited personal information protection organization pursuant to the provisions of the preceding paragraph, not refuse the request without a justifiable reason.

(Personal Information Protection Guideline)

Article 53

(1) An accredited personal information protection organization shall, for the purpose of ensuring a covered business operator's proper handling of personal information etc., strive to develop a guideline conformable to the purport of the provisions of this Act (hereinafter referred to as a "personal information protection guideline") by asking a person representing consumers or other concerned person for their opinion in regard to a matter related to personal information including utilization purpose specification, security control action and procedures for responding to a demand etc. for disclosure etc. as well as a matter related to pseudonymously processed information or anonymously processed information including its production method and security control action for such information.

(2) An accredited personal information protection organization shall, when having developed a personal information protection guideline pursuant to the provisions of the preceding paragraph, notify without delay the Personal information Protection Commission of the personal information protection guideline pursuant to rules of the Personal Information Protection Commission. When this has been modified, the same shall apply.

(3) The Personal Information Protection Commission shall, when having been notified of a personal information protection guideline under the provisions of the preceding paragraph, announce to the public the personal information protection guideline pursuant to rules of the Personal Information Protection Commission.

(4) An accredited personal information protection organization shall, when a personal information protection guideline has been announced to the public

pursuant to the provisions of the preceding paragraph, take action against a covered business operator such as providing guidance or recommendation necessary to make the covered business operator follow the said personal information protection guideline.

(Prohibition of Utilization for Unintended Purpose)

Article 54

An accredited personal information protection organization shall not utilize information obtained in the course of rendering accredited services for the other purposes than for use in such accredited services.

(Restriction on Use of Appellation)

Article 55

A person who is not an accredited personal information protection organization shall not use the appellation of the accredited personal information protection organization or any other confusing appellation therewith.

(Calling for a Report)

Article 56

The Personal Information Protection Commission may, to the extent necessary to implement the provisions under this section, call for an accredited personal information protection organization to report on its accredited services.

(Order)

Article 57

The Personal Information Protection Commission may, to the extent necessary to implement the provisions of this section, order an accredited personal information protection organization to improve a method of rendering accredited services, amend a personal information protection guideline, or take any other necessary action.

(Rescinding the Accreditation)

Article 58

(1) The Personal Information Protection Commission may, when an accredited personal information protection organization falls under any of each following item, rescind the accreditation.

(i) when having led to falling under Article 48, item (i) or item (iii)

(ii) when having become unconformable to any of each item of Article 49

(iii) when having violated the provisions of Article 54

(iv) when disobeying an order under the preceding Article

(v) when having received an accreditation under Article 47, paragraph (1), or an accreditation of alteration under Article 49-2, paragraph (1) by improper means

(2) The Personal Information Protection Commission shall, when having rescinded an accreditation pursuant to the provisions of the preceding paragraph, announce to the public to that effect.

Section 6 Service

(Document to be served)

Article 58-2

(1) A requirement to submit a report or material pursuant to the provisions of Article 40, paragraph (1), a recommendation pursuant to the provisions of Article 42, paragraph (1) or an order pursuant to Article 42, paragraph (2) or (3), a call for a report pursuant the provisions of to Article 56, an order pursuant to the provisions of Article 57, or a rescission pursuant to the provisions of the preceding Article, paragraph (1), is given by serving a document specified by rules of the Personal Information Protection Commission.

(2) A notice under Article 15, paragraph (1) or Article 30 of the Administrative Procedure Act (Act No. 88 of 1993) relating to the order pursuant to the provisions of Article 42, paragraph (2) or (3) or Article 57, or, rescission pursuant to the preceding Article, paragraph (1), is given by serving a document of the Article 15, paragraph (1) and (2) or Article 30 of the Act. In this case, the provisions of Article 15, paragraph (3) of the Act (including cases where it is applied mutatis mutandis pursuant to Article 31 of the Act following the deemed replacement of terms) shall not apply.

(Application Mutatis Mutandis of the Code of Civil Procedure Concerning Service)

Article 58-3

The provisions of Articles 99, 101, 103, 105, 106, 108, and 109 of the Code of Civil Procedure apply mutatis mutandis to the service pursuant to the provisions of the preceding Article. In this case, the term “court execution officer” in Article 99, paragraph (1) of the Act is deemed to be replaced by “official of the Personal Information Protection Commission”, and the terms “presiding judge” in Article 108 of the Act and “court” in Article 109 of the Act are deemed to be replaced by “Personal Information Protection Commission”.

(Service by Publication)

Article 58-4

(1) The Personal Information Protection Commission may effect service by publication in the following cases:

- (i) if the domicile or residence of the person to be served or the place where service is to be effected is unknown;
- (ii) if, with regard to service that would be effected in a foreign country, it is impossible to effect service by the means prescribed in Article 108 of the Code of Civil Procedure as applied mutatis

mutandis pursuant to the preceding Article following the deemed replacement of terms, or it is found to be impossible to effect service by those means; or

(iii) if, even after six months have passed since a commission was issued to the competent government agency of a foreign country pursuant to the provisions of Article 108 of the Code of Civil Procedure as applied mutatis mutandis pursuant to the preceding Article following the deemed replacement of terms, no document that certifies that the agency has effected service has been sent.

(2) Service by publication is effected by posting on the notice board of the Personal Information Protection Commission to the effect that the documents to be served will be delivered at any time to the person to be served.

(3) Service by publication becomes effective once two weeks have passed from the date on which the posting under the provisions of the preceding paragraph was commenced.

(4) The period set forth in the preceding paragraph is six weeks for service by publication that is done for service that would be effected in a foreign country.

(Use of Electronic Data Processing Systems)

Article 58-5

When an official of the Personal Information Protection Commission administers affairs related to those that are to be given by serving a document pursuant to the provisions of Article 58-2, and a disposition notice, etc. prescribed in Article 3, item (ix) of the Act on Use of Information and Communications Technology in Administrative Procedure (Act No. 151 of 2002) using an electronic data processing system prescribed in Article 6, paragraph (1) of the Act pursuant to Article 7, paragraph (1) of the Act, the official must use that electronic data processing system, to record the particulars of the service under the provisions of Article 109 of the Code of Civil Procedure as applied mutatis mutandis pursuant to Article 58-3, in a file that is stored on a computer (including input or output device) used by the Personal Information Protection Commission instead of preparing and submitting a document that states those particulars.

Chapter V The Personal Information Protection Commission

(Establishment)

Article 59

(1) The Personal Information Protection Commission (hereinafter referred to as the “Commission”) is to be established based on the provisions of Article 49, paragraph (3) of the Act for Establishment of the Cabinet Office.

(2) The Commission belongs to the jurisdiction of the Prime Minister.

(Duties)

Article 60

The Commission is to assume the duties of pursuing ensuring the proper handling of personal information (including taking action such as giving guidance and advice to an individual number utilizing business etc. related implementer (meaning an individual number utilizing business etc. related implementer prescribed in Article 12 of the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedures (Act No.27 of 2013; hereinafter referred to as the “Numbers Use Act”))) in order to protect an individual’s rights and interests while considering the utility of personal information including that the proper and effective application of personal information contributes to the creation of new industries and the realization of a vibrant economic society and an enriched quality of life for the people of Japan.

(Jurisdictional Affairs)

Article 61

The Commission is to administer the following affairs in order to fulfil the duties under the preceding Article.

(i) affairs related to the formulation and promotion of a basic policy

(ii) affairs (excluding those set forth in item (iv)) related to supervision related to the handling of personal information by a personal information handling business operator, the handling of personally referable information by a personally referable information handling business operator, the handling of pseudonymously processed information by a personal information handling business operator and a pseudonymously processed information handling business operator, and, the handling of anonymously processed information by a personal information handling business operator and anonymously processed information handling business operator, supervision related to the handling, by an Administrative Organ prescribed in Article 2, paragraph (1) of the Act on the Protection of Personal Information Held by Administrative Organs, of an Anonymized Personal Information Held by Administrative Organ (limited to those constituting an Anonymized Personal

Information File Held by Administrative Organs as prescribed in paragraph (10) of the same Article) prescribed in paragraph (9) of the same Article, supervision related to the handling, by an incorporated administrative agency, etc., of an anonymized personal information held by an incorporated administrative agency, etc. prescribed in Article 2, paragraph (9) of the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. (limited to those constituting an anonymized personal Information file of an incorporated administrative agency, etc. as prescribed in paragraph (10) of the same Article), and, affairs related to necessary mediation on a lodged complaint related to the handling of personal information, pseudonymously processed information and anonymously processed information, and to cooperation offered to a business operator who deals with that complaint.

(iii) affairs related to an accredited personal information protection organization

(iv) affairs related to monitoring and supervision over the handling of specific personal information (meaning specific personal information prescribed in Article 2, paragraph (8) of the Numbers Use Act; the same shall apply in Article 63, paragraph (4)) and those related to necessary mediation on a lodged complaint and cooperation offered to a business operation who deals with the complaint

(v) affairs related to specific personal information protection assessment (meaning specific personal information protection assessment prescribed in Article 27, paragraph (1) of the Numbers Use Act)

(vi) affairs related to public relations and an enlightenment campaign on the protection of, and the proper and effective application of, personal information

(vii) affairs related to an investigation or research necessary to administer those affairs set forth in each preceding item

(viii) affairs related to international cooperation on the jurisdictional affairs

(ix) besides those set forth in each preceding item, those affairs which have been made by law (including an order based thereon) to belong to the Commission

(Independence on Exercising the Authority)

Article 62

A chairperson and commissioners of the Commission are to exercise their official authority independently.

(Organization etc.)

Article 63

(1) The Commission is to be composed of a chairperson and eight commissioners.

(2) Four of the commissioners are to serve on a part-time basis.

(3) A chairperson and a commissioner are to be appointed by the Prime Minister with consent of both Houses of the Diet from among those with high character and deep insight.

(4) A chairperson and commissioners are to encompass a person who has academic experience concerning the protection of, and the proper and effective application of, personal information, a person who has sufficient knowledge and experience concerning the protection of consumers, a person who has academic experience concerning information processing technologies, a person who has academic experience concerning public administrative fields utilizing specific personal information, a person who has sufficient knowledge and experience concerning private-sector business practices, and a person recommended by a federate organization (meaning a federate organization under Article 263-3, paragraph (1) of the Local Autonomy Act (Act No.67 of 1947) that has given a notification pursuant to the provisions of the said paragraph).

(Term of Office etc.)

Article 64

(1) The term of office for a chairperson and a commissioner is to be five years; however, the term of office of a chairperson or a commissioner appointed to fill a vacancy shall be the remaining term of office of his or her predecessor.

(2) A chairperson and a commissioner may be reappointed.

(3) When the term of office for a chairperson or a commissioner has expired, the chairperson or commissioner are to continue to fulfil their duties until their successor is appointed.

(4) In cases where the term of office of a chairperson or a commissioner has expired or where a vacancy has occurred, when consent by both Houses of the Diet cannot be obtained due to the closing of the Diet or the dissolution of the House of Representatives, the Prime Minister may, notwithstanding the provisions of the preceding Article, paragraph (3), appoint a chairperson or a commissioner from among those persons who have those qualifications prescribed in the said paragraph.

(5) In those cases under the preceding paragraph, an ex post facto approval by both Houses of the Diet shall be obtained in the first Diet session after the appointment. In this case, when the ex post

facto approval cannot be obtained by both Houses of the Diet, the Prime Minister shall immediately dismiss the chairperson or the commissioner.

(Guarantee of Status)

Article 65

A chairperson and a commissioner shall not be dismissed against their will while in office except in those cases falling under any of each following item.

- (i) when having received a decision on the commencement of bankruptcy proceedings
- (ii) when having been punished in violation of this Act or the Numbers Use Act
- (iii) when having been punished by imprisonment without work or severer sentence
- (iv) when, by the Commission, having been recognized to be incapable of fulfilling his or her duties because of a mental or physical disorder, or having been recognized to be committing a violation of obligation in the course of duties or other misconduct unbecoming to a chairperson or a commissioner

(Dismissal)

Article 66

The Prime Minister shall, when a chairperson or a commissioner falls under any of each item of the preceding Article, dismiss the chairperson or the commissioner.

(Chairperson)

Article 67

- (1) A chairperson is to preside over the rules and proceedings of the Commission and represent the Commission.
- (2) The Commission shall designate in advance from among full-time commissioners a person to be an acting chairperson in cases where the chairperson is in an accident.

(Meeting)

Article 68

- (1) A meeting of the Commission is to be called by a chairperson.
- (2) The Commission may, unless a chairperson and four or more commissioners are present, neither hold a meeting nor make a decision.

(3) A decision of the Commission is to be adopted by a majority of attendees, and when in a tie, a chairperson is to make a decision.

(4) A recognition pursuant to the provisions of Article 65, item (iv), notwithstanding the provisions of the preceding paragraph, shall be allowed with the unanimous concurrence of all commissioners except for the commissioner concerned.

(5) With regard to applying the provisions of this Article, paragraph (2) in cases where a chairperson is in an accident, a person to be an acting chairperson prescribed in the preceding Article, paragraph (2) shall be deemed as a chairperson.

(Specialist Commissioner)

Article 69

(1) In the Commission may a specialist commissioner be posited to have a specialized matter investigated.

(2) A specialist commissioner is to be appointed by the Prime Minister based on a proposal made by the Commission.

(3) A specialist commissioner shall be relieved of his or her post when an investigation into the specialized matter has been finished.

(4) A specialist commissioner is to serve on a part-time basis.

(Secretariat)

Article 70

(1) For the purpose of having commissary affairs administered, a secretariat is to be posited.

(2) In a secretariat are a secretary general and other staff to be posited.

(3) A secretary general is to administer secretarial affairs under the order of a chairperson.

(Prohibition of a Political Campaign etc.)

Article 71

(1) A chairperson and commissioners shall, while in office, neither become a director of a political party or other political organization nor actively conduct a political campaign.

(2) A chairperson and a full-time commissioner shall, while in office except in those cases where there has been permission from the Prime Minister, not engage in

any other duties paying remuneration, operate a profit-making business, or perform other services for the purpose of gaining monetary profit.

(Confidentiality Obligation)

Article 72

A chairperson, commissioner, specialist commissioner and secretarial staff shall not divulge or use by stealth any secret that may have come to their knowledge in the course of duties. The same shall also apply after they have left their position.

(Remuneration)

Article 73

The remuneration of a chairperson and a commissioner shall be prescribed separately by law.

(Establishment of Rules)

Article 74

The Commission may establish rules of the Personal Information Protection Commission regarding its jurisdictional affairs in order to enforce a law or cabinet order, or on the basis of a special delegation under a law or cabinet order.

Chapter VI Miscellaneous Provisions

(Scope of Application)

Article 75

This Act shall also apply in those cases where a personal information handling business operator etc., in relation to supplying a good or service to a person in Japan, handles the personal information that has a person in Japan as the principal, personally referable information that is to be acquired as the said personal information, pseudonymously processed information or anonymously processed information produced by using the said personal information, in a foreign country.

(Exclusion from Application)

Article 76

(1) To a person set forth in each following item who is a personal information handling business operator shall the provisions of Chapter IV not apply when a whole or part of the purpose of handling personal information etc. is a purpose prescribed in each said item respectively.

(i) a broadcasting institution, newspaper publisher, communication agency and other press organization (including an individual engaged in the press as his or her business): a purpose of being provided for use in the press

(ii) a person who practices writing as a profession: a purpose of being provided for use in writing

(iii) a university and other organization or group aimed at academic studies, or a person belonging thereto: a purpose of being provided for use in academic studies

(iv) a religious body: a purpose of being provided for use in a religious activity (including those activities accessory thereto)

(v) a political body: a purpose of being provided for use in a political activity (including those activities accessory thereto)

(2) The “press” prescribed in item (1) of the preceding paragraph means informing a large number of unspecified people of an objective fact as such (including stating an opinion or view based thereon).

(3) A personal information handling business operator etc. set forth in each item of paragraph (1) shall strive to take itself necessary and appropriate action for the security control of personal data, pseudonymously processed information or anonymously processed information and necessary action to ensure the proper handling of personal information etc. (excluding personally referable information; hereinafter the same applies in this paragraph) such as dealing with a complaint about the handling of personal information etc., as well as announce to the public the contents of such action taken.

(Affairs Administered by a Local Government)

Article 77

Administrative affairs belonging to the Commission’s authority prescribed in this Act and an authority delegated to a business jurisdictional minister or a Commissioner of the Financial Services Agency pursuant to the provisions of Article 44, paragraph (1) or paragraph (4) may be managed by a head of a local government or other executive agency as prescribed by cabinet order.

(Information Provision to the Foreign Enforcement Authorities)

Article 78

(1) The Commission may provide the foreign authorities enforcing those foreign laws and regulations equivalent to this Act (hereinafter referred to as the “foreign enforcement authorities” in this Article)

with information recognized as contributory to fulfilling their duties (limited to those equivalent to the Commission's duties prescribed in this Act; the same shall apply in the succeeding paragraph).

(2) Concerning the provision of information pursuant to the preceding paragraph, appropriate action shall be taken so that the information is neither used for purposes other than for the foreign enforcement authorities fulfilling their duties nor used for a foreign criminal case investigation (limited to the one conducted after the criminal facts subject to the investigation have been specified) or adjudication (hereinafter collectively referred to as an "investigation etc.") without consent pursuant to the succeeding paragraph.

(3) The Commission may, when having received a request from the foreign enforcement authorities, consent that the information it provided pursuant to paragraph (1) be used for a foreign criminal case investigation etc. in connection with the request except for those cases falling under any of each following item.

(i) when a crime subject to the criminal case investigation etc. in connection with the said request is a political crime, or when the said request is recognized to have been made for the purpose of conducting the investigation etc. into a political crime

(ii) when an act relating to the crime subject to a criminal case investigation etc. in connection with the said request, if it were committed in Japan, shall not constitute a criminal offense according to the laws and regulations in Japan

(iii) when there is no assurance that the requesting country will accept the same kind of request from Japan

(4) The Commission shall, in case of consenting under the preceding paragraph, obtain a Minister of Justice's confirmation of the case not falling under item (i) and item (ii) of the preceding paragraph, and a Minister of Foreign Affairs' confirmation of the case not falling under item (iii) of the preceding paragraph respectively.

(Sincere Implementation of International Agreements etc.)

Article 78-2

In the enforcement of this Act, care must be taken not to prevent the sincere implementation of treaties and other international agreements which Japan has concluded, and established international law must be complied with.

(Report to the Diet)

Article 79

The Commission shall annually report to the Diet through the Prime Minister the current status of administering its jurisdictional affairs, and announce to the public a summary thereof.

(Communication and Cooperation)

Article 80

The Prime Minister and a head of an administrative organization related to the implementation of this Act (meaning an organization established in the Cabinet based on the provisions of laws (excluding the Cabinet Office), an organization under the jurisdiction of the Cabinet, the Cabinet Office, the Imperial Household Agency, an organization prescribed in Article 49, paragraph (1) and paragraph (2) of the Act for Establishment of the Cabinet Office, and an organization prescribed in Article 3, paragraph (2) of the National Government Organization Act (Act No.120 of 1948)) shall closely communicate and cooperate with one another.

(Delegation to Cabinet Order)

Article 81

A matter necessary to implement this Act other than those prescribed in this Act is to be prescribed by cabinet order.

Chapter VII Penal Provisions

Article 82

A person who has divulged or used by stealth a secret in violation of the provisions of Article 72 shall be punished by imprisonment with work for not more than two years or a fine of not more than 1,000,000 yen.

Article 83

In cases where an order pursuant to the provisions of Article 42, paragraph (2) or paragraph (3) is violated, the person who has done the act of violating shall be punished by imprisonment with labor for not more than one year or a fine of not more than 1,000,000 yen.

Article 84

A personal information handling business operator (or its director, representative or administrator if it is a corporate body (including a non- corporate body having appointed a representative or administrator; the same shall apply in Article 87, paragraph (1)), its employee, or a person who used

to be such a business operator or employee shall, when having provided or used by stealth personal information database etc. (including their wholly or partially duplicated or processed ones) that they handled in relation to their business for the purpose of seeking their own or a third party's illegal profits, be punished by imprisonment with work for not more than one year or a fine of not more than 500,000 yen.

Article 85

In cases that fall under any of each following item, the person who has done the act of violation shall be punished by a fine of not more than 500,000 yen.

(i) If a person failed to submit a report or material under the provisions of Article 40, paragraph (1) or did falsely submit a report or material, or who failed to answer a question posed by the staff concerned or did falsely answer a question, or refused, obstructed or evaded an inspection

(ii) If a person failed to submit a report under the provisions of Article 56, or did falsely submit a report

Article 86

The provisions of Article 82 and Article 84 shall apply to a person who has committed an offense under these Articles outside of Japan.

Article 87

(1) When a representative of a corporate body, or an agent, employee or other worker of a corporate body or natural person has committed a violating act set forth in each following item in relation to the corporate body or natural person's business, the actor shall be punished, and a fine set forth in each following item shall be imposed on the corporate body, and a fine set forth in the respective Articles shall be imposed on the said natural person.

(i) Article 83 and Article 84 a fine of not more than 100 million yen

(ii) Article 85 a fine set forth in the same Article

(2) In cases where the provisions of the preceding paragraph apply to a non- corporate body, its representative or administrator shall represent the non- corporate body in regard to an act of litigation, and the provisions of a law on a criminal suit in the cases where a corporate body is a defendant or suspect shall apply *mutatis mutandis*.

Article 88

A person falling under any of each following item shall be punished by a non-criminal fine of not more than 100,000 yen.

(i) a person who has violated the provisions of Article 26, paragraph (2) (including as applied *mutatis mutandis* pursuant to Article 26-2, paragraph (3)), or Article 55

(ii) a person who failed to submit a notification or did falsely submit a notification under the provisions of Article 50, paragraph (1)

Katar - Personal Data Privacy Protection

Personal Data Privacy Protection

Law No.13 of 2016

Law No. (13) of 2016 on Protecting Personal Data Privacy

We, Tamim Bin Hamad Al-Thani, Emir of the State of Qatar

After having perused the Constitution, Telecommunications law promulgated by Decree-Law No. (34) of 2006, Electronic Transactions and Commerce law promulgated by Decree-Law No. (16) of 2010, Law No. (2) of 2011 on Official Statistics, as amended by law No. (4) of 2015, Cybercrimes Combatting law promulgated by Law No. (14) of 2014, Emiri Resolution No. (42) of 2014 on the Establishment of the Communications Regulatory Authority, Emiri resolution No. (8) of 2016 on the Organizational Structure of the Ministry of Transport and Communications, The proposal of the minister of transport and communications, and The draft law submitted by the Council of Ministers, and After consulting the Shura Council,

Have decided the following Law,

Chapter One

Definitions and General Provisions

Article (1)

For the implementation of the provisions hereof, the following terms and words shall have such meanings assigned to the same, unless otherwise required by context:

Ministry: Ministry of Transport and Communications.

Minister: Minister of Transport and Communication.

Competent Department: the competent administrative unit at the Ministry.

Competent Authority: any government entity competent, as per law, to regulate acts or procedures pertinent to Personal Data Processing and supervision of the same.

Individual: a natural person whose Personal Data are processed.

Controller: a natural or legal person who, whether acting individually or jointly with others, determines how Personal Data may be processed and determines the purpose(s) of any such processing Personal Data Processing.

Processor: a natural or legal person who processes Personal Data for the Controller.

Personal Data: data of an individual whose identity is defined or can be reasonably defined whether through such Personal Data or through the combination of such data with any other data.

Personal Data Processing: Personal Data Processing through one operation or more such as gathering, receipt, registration, organization, storage, preparation, modification, retrieval, usage, disclosure, publication, transfer, withholding, destruction, erasure and cancellation.

Cross-Border Data Flows: access, watch, retrieve, use or store Personal Data without restrictions of the State's borders.

Lawful Purpose: The purpose for which Personal Data of an Individual is processed, in accordance with the law.

Acceptable Practices: processing activities determined or approved by the Competent Department with regard to various types of Lawful Purposes.

Direct Marketing: sending any advertising or marketing material, in whatsoever means, to certain individuals.

Wire and Wireless Communications: sending, broadcasting or receiving signals, images, shapes, sound, data, texts or information, of whatsoever kind or nature, via wire, wireless, radio, visual means, other electromagnetic communication means or any other similar communication means.

Electronic Communication: a communication by means of any of Wire and Wireless Communications.

Electronic Communication Establishment: establish, send or transfer an Electronic Communication or help therewith, or give directions to the Processor to do that.

Website Operator: an individual who operates a web site, or offers products or services therethrough and gathers or processes Personal Data of users or visitors of such website.

Article (2)

Provisions hereof shall apply to Personal Data when it is electronically processed, or obtained, gathered or extracted in preparation in any other way for electronic processing, or when processed via a combination of electronic and traditional processing.

Provisions hereof shall not apply to Personal Data processed by individuals within a private or a family scope, or to any Personal Data processed for the purpose of obtaining official statistical data as per provisions of the referred to law No (2) of 2011.

Chapter Two

Rights of Individuals

Article (3)

Each Individual has the right to the protection of the Personal Data thereof that shall be processed only within the framework of transparency, honesty, and respect of human dignity, and acceptable practices according to provisions hereof.

Article (4)

The Controller shall process Personal Data only after obtaining the consent of the Individual, unless data processing is necessary to achieve a Lawful Purpose for the Controller or the other recipient of such data.

Article (5)

An Individual may, at any time:

1. Withdraw the prior consent thereof for Personal Data Processing.
2. Object to processing the Personal Data thereof if such processing is not necessary to achieve the purposes for which such Personal Data have been collected or where such collected Personal Data are beyond the extent required, discriminatory, unfair or illegal.
3. Request omission or erasure of the Personal Data thereof in any of the cases referred to in the preceding two items, upon cessation of the purpose for which the processing has been conducted, or where all justifications for maintaining such Personal Data by the Controller cease to exist.
4. Request corrections to the Personal Data thereof. A request so made shall be accompanied with proof of the accuracy of such request.

Article (6)

An Individual may, at any time, access the Personal Data thereof and apply to review the same, in facing any Controller, and an Individual has, in particular, the right to:

1. Be notified of processing the Personal Data thereof and the purposes for which such processing is conducted.

2. Be notified of any disclosure of inaccurate Personal Data.
3. Obtain a copy of the Personal Data thereof after paying an amount that shall not exceed the service charge.

Article (7)

The controls and procedures, related to individuals' exercise of rights provided for in the two preceding Articles, shall be specified by a decision of the Minister.

Chapter Three

Liabilities of Controller and Processor

Article (8)

The Controller shall abide by the following:

1. Processing Personal Data honestly and legitimately.
2. Consider the controls related to designing, changing or developing products, systems and services pertinent to Personal Data Processing.
3. Taking appropriate administrative, technical and financial precautions to protect Personal Data, in accordance with what is determined by the Competent Department.
4. The privacy protecting policies developed by the Competent Department, and a decision thereon shall be issued by the Minister.

Article (9)

The Controller shall, prior to starting processing any Personal Data, inform the Individual with the following:

1. The Controller's details or any other party conducting the processing for the Controller or to be used thereby.
2. The Lawful Purposes that the Controller or any other party wants to process the Personal Data therefor.
3. Comprehensive and accurate description of the processing activities and the levels of disclosure of such Personal Data for the Lawful Purposes, and if the Controller fails to do so, the Controller shall provide the Individual with a general description thereof.

4. Any other information that is necessary and required for fulfilling conditions of Personal Data Processing.

Article (10)

The Controller shall verify that Personal Data that he collects, or being collected for the benefit thereof, is relevant to Lawful Purposes and adequate for achieving the same. The Controller shall, also, ensure such data is accurate, complete and up to date to meet such Lawful Purposes. In addition, the Controller shall not keep any Personal Data for a period of time that exceeds the necessary period for achieving such purposes.

Article (11)

The Controller shall take the following procedures:

1. Reviewing privacy protection measures before proceeding with new processing operations.
2. Identifying Processors responsible for Personal Data protection.
3. Training and raising awareness of Processors on protecting personal data.
4. Developing internal systems to receive and investigate complaints, and data access and omission or correction requests; and they shall be made available to individuals.
5. Developing internal systems for the effective management of Personal Data, and reporting any breach of measures aiming at the protection thereof.
6. Using appropriate technologies to enable individuals to exercise their rights to directly access, review and correct their respective Personal Data.
7. Conducting comprehensive audits and reviews on the compliance extent with Personal Data protection requirements.
8. Verifying Processor's compliance with the instructions directed thereto, taking the appropriate precautions to protect Personal Data, and monitoring and following-up the same constantly.

Article (12)

The Controller shall, at the time of disclosing Personal Data or transferring it to the Processor, take into consideration that it is in line with Lawful Purposes and is processed according to provisions hereof.

Article (13)

Each of the Controller and the Processor shall take the precautions necessary to protect Personal Data against loss, damage, change, disclosure, access thereto, or the inadvertent or illegal use thereof.

Such precautions shall be commensurate with the nature and the importance of the Personal Data intended to be protected.

The Processor shall forthwith notify the Controller of the existence of any breach of the precautions referred to, or where any risk arises threatening Personal Data in any way.

Article (14)

The Controller shall inform the Individual and Competent Department of the occurrence of any breach of the precautions provided for in the preceding Article, and if such breach may cause serious damage to Personal Data or individual privacy.

Article (15)

Taking into account the liabilities provided for hereto, the Controller shall be forbidden from taking any decision or measure that may limit the CrossBorder Data Flow, unless the processing of such data is in breach of this Law, or where such processing may cause serious damage to the Personal Data or to the Individual's privacy.

Chapter Four

Personal Data with Special Nature

Article (16)

The Personal data, related to ethnic origin, children, health, physical or psychological condition, religious creeds, marital relations, and criminal offenses, shall be regarded as Personal data with special nature.

The Minister may add other types of Personal Data of a special nature, where the misuse or disclosure of the same may cause serious damage to Individual.

Personal Data of a special nature may only be processed after obtaining the permission from the Competent Department, as per the measures and controls determined by a decision issued by the Minister.

The Minister may, upon a decision therefrom, imposing additional precautions with the intent of protecting Personal Data of a special nature.

Article (17)

Taking into consideration the liabilities provided for hereto, an owner or operator of any website addressing children shall take into account the following:

1. Posting a notification on the website as to what child data is, the way of its use, and the policies followed in the disclosure thereof.
2. Obtaining, either electronically or through any other appropriate means, an explicit consent from the guardian of the child whose Personal Data is processed.
3. Providing a child's guardian, upon the request thereof, and after verifying the identity thereof, with a description of the type of the Personal Data processed, along with stating the purpose of the process together with a copy of the data processed or gathered about the child.
4. Deleting, removing or suspending processing any Personal Data that has been gathered from or about a child, if such is requested by child's guardian.
5. A child's participation in a game, promotional award or any other activity shall not be conditional on the child's provision of Personal Data in excess of the necessary for the participation in such activity.

Chapter Five

Exemptions

Article (18)

The Competent Authority may decide to process some Personal Data, without abiding by the provisions of Articles (4), (9), (15) and (17) hereof, for achieving any of the following purposes:

1. Protecting National and public security.
2. Protecting international relations of the State.
3. Protecting the economic or financial interests of the State.
4. Preventing any criminal offense, or gathering information thereon or investigating therein.

The Competent Authority shall keep a special record where the data achieving the aforementioned purposes shall be entered. Conditions, controls and statuses of entry on such record shall be specified by virtue of a decision issued by the Minister.

Article (19)

The Controller shall be exempted from the provisions of Articles (4), (5\ Items 1, 2, and 3) and (6) hereof, in any of the following cases:

1. Executing a task related to the public interest as per the law.
2. Implementing a legal obligation or an order rendered by a competent court.
3. Protecting vital interests of Individual.
4. Achieving purposes of scientific research which is underway for public interest.
5. Gathering necessary information for investigation into a criminal offense, upon an official request of investigative bodies.

Article (20)

The Controller shall be exempted from disclosing the reasons for the refusal thereof of abiding by the rights of the Individual, as provided for in Article (6) hereof, if such disclosure would prevent achieving the purposes stipulated in Article (18) hereof.

Article (21)

Taking into consideration the provisions of the preceding two Article, the Controller shall be exempted from abiding by provisions of Article (6) hereof, in either of the following two cases:

1. When disclosure would cause harm to commercial interests of another individual.
2. When implementation of such liability would cause disclosing Personal Data related to another Individual who does not consent thereto, and disclosure may lead to physical or moral damage either to this Individual or to any other Individual.

Chapter Six

Electronic Communication for the Purpose of Direct Marketing

Article (22)

The transmission of any Electronic Communication to an Individual, for the purpose of Direct Marketing, shall be forbidden, except after obtaining the prior consent thereof.

The Electronic Communication shall include the identity of the originator thereof, and highlight that it is sent for the purpose of Direct Marketing. In addition, it shall include a valid address for easy access thereto and through which an Individual can send a request to the originator to stop such communications or revoke the consent on the sending thereof.

Chapter Seven

Penalties

Article (23)

Without prejudice to any more severe penalty stipulated in any other law, a penalty that shall not exceed (1, 000,000) one million QR shall be applicable to anyone violating any of the provisions of the Articles (4, 8, 9, 10, 11, 12, 14, 15, and 22) hereof.

Article (24)

Without prejudice to any more severe penalty stipulated in any other law, a penalty that shall not exceed (5, 000, 000) five million QR shall be applicable to anyone violating any of the provisions of the Articles (13), (16\ paragraph 3), and (17) hereof.

Article (25)

A penalty that shall not exceed (1,000,000) One million QR shall be applicable to violating legal person, in the event of committing any of those crimes stipulated herein on the name or for the interest thereof, without prejudice to criminal liability taken by affiliated natural person.

Chapter Eight**Final Provisions****Article (26)**

An Individual may file a complaint to the Competent Department in case of violating provisions hereof and the issued decisions in the implementation thereof.

The Competent Department may, after investigating received complaints and proving the seriousness thereof, issue a reasoned decision binding the Controller or Processor, as the case may be, to rectify such breach within a period it specifies.

The Controller or Processor may raise a grievance against such decision to the Minister, within sixty days from the notification date thereof.

The Minister shall decide on the grievance within sixty days from the date of the submission thereof, and the lapse of such period without a response shall be considered as an implicit rejection of the grievance, and the decision of the Minister thereon shall be final.

Article (27)

The Competent Department may, for the purpose of applying and implementing provisions hereof, take all necessary measures thereto, and in particular the following:

1. Coordinating with any professional group or association, and any other association representing Controllers or Website Operators for the purpose of self-organization encouragement and development, and raising awareness of this Law and developing training and learning programs.
2. Working with organizations and societies interested in family affairs to enhance the safety of children on the internet.
3. Conducting researches and monitor developments in technology's fields related to issues covered by this Law, and preparing reports or recommendations on the same.

Article (28)

Any contract or agreement made in violation of the provisions hereof shall be regarded as null and void.

Article (29)

The Ministry employees, authorized as law enforcement officers as per a decision by the Public Prosecutor, in agreement with the Minister, may detect and prove crimes committed in violation of provisions hereof.

Article (30)

Parties falling under provisions hereof shall, within six months from the date of the effectiveness thereof, adjust their conditions in line with provisions hereof.

Such period may be extended for other similar period or periods by virtue of a decision of the Council of Ministers, upon the proposal of the Minister.

Article (31)

The Minister shall issue the necessary decisions for the implementation of the provisions hereof.

Article 32

All the competent authorities, each within the competences thereof, shall implement this Law, and it shall be published in the official gazette.

Tamim Bin Hamad Al Thani

Emir of the State of Qatar

Issued at the Emiri Diwan on: 03/02/1438 (AH)

Corresponding to: 03/11/2016 (AD)

KİŞİSEL VERİLERİN KORUNMASI YASASI

İÇDÜZENİ

Madde 1. Kısa İsim

BİRİNCİ KISIM

Genel Kurallar

Madde 2. Tefsir

Madde 3. Amaç

Madde 4. Kapsam

İKİNCİ KISIM

Kişisel Verinin İşlenmesi

Madde 5. Kişisel Veriler İşlenirken Uygulanacak İlkeler

Madde 6. Yasal İşleme

Madde 7. Hassas Verinin İşlenmesi

Madde 8. Başkana Bildirim

Madde 9. Kişisel Veri Dosya Sistemlerinin Birleştirilmesi

Madde 10. Veri Koruma Görevlisi

ÜÇÜNCÜ KISIM

Veri Transferi ve Gizlilik

Madde 11. Diğer Ükelere Veri Transferi

Madde 12. İşlemenin Gizliliği ve Güvenliği

DÖRDÜNCÜ KISIM

Bilgiye Konu Kişinin Hakları

Madde 13. Bilgilendirme Yükümlülüğü

Madde 14. Erişim Hakkı

Madde 15. İtiraz Hakkı

Madde 16. Erişim ve İtiraz Haklarının Kullanılması

Madde 17. Doğrudan veya Dolaylı Pazarlama İçin İşleme

Madde 18. Tazmin Hakkı

Madde 19. Kontrolör ve İşlemcinin Gizlilik Yükümlülüğü

BEŞİNCİ KISIM

Kişisel Verileri Koruma Kurulunun Oluşumu, Yetki ve Görevleri

Madde 20. Kişisel Verileri Koruma Kurulu

Madde 21. Kurulun Oluşumu

Madde 22. Kurul Başkan ve Üyelerinin Nitelikleri

Madde 23. Kurul Başkanının Görev ve Yetkileri

Madde 24. Kurul Başkan ve Üyelerinin Görev Süresi ve Yeniden Atanabilmesi

Madde 25. Kurul Başkan ve Üyelerinin Siyasal Parti Organlarında Görev Alamayacakları

Madde 26. Kurul Başkanlığı veya Üyeliğinin Boşalması

Madde 27. Kurulun Toplantıları

Madde 28. Kurulun Görevleri

Madde 29. Kurulun Gelirleri, Bütçesi, Kesin Hesapları ve Denetim

Madde 30. Kurul Başkanının Tam Zamanlı Çalışması ve Kurul Başkan ve Üyelerinin Ödenekleri

Madde 31. Kurul Hizmetlerinin Yürütülmesi ve Kurul Personelinin Statüsü

Madde 32. Personele İlişkin Kurallar

Madde 33. Kurul Başkanının, Üyelerinin ve Personelinin Sır Saklama Yükümlülüğü

Madde 34. Şikayet Başvurusu

ALTINCI KISIM

Suç ve Cezalar

Madde 35. İdari Para Cezaları

Madde 36. Suç ve Cezalar

YEDİNCİ KISIM

Geçici ve Son Kurallar

Madde 37. Ruhsat ve Ücretlerle İlgili Tüzük Yapma Yetkisi

Geçici Madde 1. Mevcut Durumun Yasaya Uydurulması

Madde 38. Yürütme Yetkisi

Madde 39. Yürürlüğe Giriş

89/2007

KİŞİSEL VERİLERİN KORUNMASI YASASI

Kuzey Kıbrıs Türk Cumhuriyeti Cumhuriyet Meclisi aşağıdaki Yasayı yapar:

Kısa İsim

1. Bu Yasa, Kişisel Verilerin Korunması Yasası olarak isimlendirilir.

BİRİNCİ KISIM

Genel Kurallar

Tefsir

2. Bu Yasada metin başka türlü gerektirmedikçe:

“Başbakan”, Kuzey Kıbrıs Türk Cumhuriyeti Başbakanını anlatır.

“Başkan”, Bu Yasanın 20’nci maddesi ile kurulan Kişisel Verileri Koruma Kurulunun Başkanını anlatır.

“Bilgiye konu kişi”, bilgilerin ait olduğu ve kimliği bilinen veya dolaylı veya dolaysız olarak, özellikle kimlik numarası veya fiziksel, fizyolojik, zihinsel, ekonomik, kültürel, siyasal veya sosyal kimliğine dair bir veya birden fazla faktör esas alınarak tesbit edilebilen gerçek kişiyi anlatır.

“Birleştirme”, bir dosyalama sistemindeki verilerin diğer bir kontrolör veya kontrolörler tarafından tutulan veya aynı kontrolör tarafından başka bir amaçla tutulan verilerle bir araya getirilmesine imkan verecek şekilde işleme bağlı tutulmasını anlatır.

“Devlet”, Kuzey Kıbrıs Türk Cumhuriyeti Devletini anlatır.

“Hassas veri”, ırksal veya etnik kökeni, siyasi görüşleri, dinsel veya diğer inançları ortaya koyan veya cinsel yönelim, sağlık veya cinsel hayatla veya cezai soruşturmayla ilgili konuları açığa çıkaran kişisel verileri anlatır.

“İşlemci”, şahsi veriyi kontrolör adına işleyen kişiyi anlatır.

“İşleme” veya “Kişisel verilerin işlenmesi”, Kişiyeye ilişkin tüm verilerin, toplanması, kaydedilmesi, işlenmesi, saklanması, silinmesi, değerlendirilmesi, kullanılması, uyarlanması veya değiştirilmesi, durdurulması, yokedilmesi gibi işlevlerden herhangi birisinin, birkaçının veya hepsinin, herhangi bir yöntem ve araç kullanılarak uygulanmasını anlatır.

“Kişisel veri”, kimliği belirli veya kimliği belirlenebilir bir kişiye ilişkin tüm bilgileri anlatır.

“Kişisel veri dosya sistemi”, işlevsel veya coğrafi esaslara göre merkezi veya dağıtık olarak bir sistemde muhafaza edilen ve belirli yöntemlerle ulaşılabilen kişisel veri topluluğunu anlatır.

“Kontrolör”, kendi başına veya başkalarıyla birlikte, kişisel verilerin işleme tabi tutulmasının amaç ve yöntemlerini belirleyen, kişisel veri dosya sistemini oluşturma, işletme, denetim hak ve yetkisine sahip olan Kamu Kurum ve Kuruluşları ile gerçek ve tüzel kişileri anlatır.

“Kurul”, bu Yasanın 20’nci maddesi ile kurulan Kişisel Verileri Koruma Kurulunu anlatır.

“Kurum ve Kuruluş”, genel ve katma bütçeli daireler ile Bakanlıkları, yerel yönetimleri, üniversiteleri ve bunlara bağlı sabit ve döner sermayeli kuruluşları, kamu iktisadi teşebbüslerini, kamu ve özel bankaları, yüksek kurulları, özerk, tarafsız kurum ve kuruluşları, bağımsız düzenleyici kurum ve kurulları, kamu kurumu niteliğindeki meslek kuruluşlarını, birlikleri, dernekleri ve vakıfları anlatır.

“Üçüncü taraf”, bilgiye konu kişi, kontrolör ve işlemci haricindeki her türlü kişiyi anlatır.

Amaç

3. Bu Yasanın amacı, kişisel verilerin işleme bağlı tutulmasında kişiliğin, temel hak ve özgürlüklerin korunması ve bir dosyalama sisteminin bir bölümünü oluşturan veya oluşturması planlanan kişisel verilerin otomatik veya otomatik olmayan yöntem ve araçlarla, tamamen veya kısmen işlenmesine ve transferine ilişkin esas ve usulleri düzenlemektir.

Kapsam

4. Bu Yasa kuralları, kişisel verileri işleme tâbi tutulan kişiler ile bu verileri işleme tâbi tutan kurum veya kuruluşlar ile gerçek ve tüzel kişilere uygulanır.

Ancak gerçek kişilerce ticari, mesleki kazanç amacı olmaksızın başkalarına aktarmamak kaydıyla ve sadece kendileri tarafından kullanılmak üzere işlenen kişisel veriler bu Yasa kapsamı dışındadır.

İKİNCİ KISIM

Kişisel Verinin İşlenmesi

Kişisel Veriler İşlenirken Uygulanacak İlkeler

5. (1) Kişisel veriler işlenirken kontrolörün aşağıdaki ilkelere uyması zorunludur:

(A) Kişisel verilerin yasal ve adil yoldan elde edilmesi ve işlenmesi,

(B) Kişisel verilerin belirli, açık ve meşru amaçlarla derlenmesi ve bu amaçlara uygun olarak işlenmesi ve bu amaçlarla uyumlu olmayan şekillerde işlem görmemesi,

(C) Kişisel verilerin doğru ve gerektiği takdirde güncel olması,

(Ç) Kişisel verilerin derlenme ve işleme amaçlarının yerine getirilmesi sağlanırken, Başkanın takdiriyle, verinin, sahibinin kimliğinin belirlenmesine izin verecek bir formda gereğinden uzun bir süre tutulmaması.

Ancak bu sürenin bitiminde, Başkan, bilgiye konu kişinin veya üçüncü tarafların haklarının etkilenmediğine kanaat getirmesi halinde, gerekçeli bir kararla kişisel verinin tarihsel, bilimsel veya istatistiki amaçlarla muhafazasına izin verebilir.

(2) Kontrolör, yukarıdaki (1)'inci fıkra kurallarına aykırı şekilde derlenmiş veya işlenmeye devam edilmiş kişisel verileri imha etmekle mükelleftir. Başkan, resen veya bir şikayet üzerine, (1)'inci fıkra kurallarına aykırı hareket edildiğini belirlemesi halinde, derleme veya işlemenin durdurulması ve derlenmiş veya işlenmiş bulunan kişisel verilerin imha edilmesi talimatını verir.

Ancak bu tür verilerin tarihsel veya bilimsel amaçlı muhafazasının Milli Arşiv ve Araştırma Dairesi (Kuruluş, Görev ve Çalışma Esasları) Yasası ile oluşturulan Milli Arşiv Kurulu Başkanı tarafından gerekli görülmesi halinde Başkan, bunların Milli Arşivde muhafazasına izin verebilir.

Yasal İşleme

6. Kişisel veriler, bilgiye konu kişinin şüpheye sebebiyet vermeyecek şekilde onay vermesi halinde işlenebilir.

Ancak, kişisel veriler, aşağıdaki durumlarda bilgiye konu kişinin onayı olmadan da işlenebilir:

(1) İşlemenin, kontrolörün tabi olduğu yasal yükümlülüğü yerine getirmek için gerekli olması,

- (2) İşlemenin, bilgiye konu kişinin taraf olduğu bir sözleşmenin yerine getirilmesi için gerekli olması veya bilgiye konu kişinin talebi üzerine, sözleşmeye taraf olmadan önce önlem alınması amacıyla yapılması,
- (3) İşlemenin, bilgiye konu kişinin hayati çıkarlarının korunması için gerekli olması,
- (4) İşlemenin, kamu çıkarı adına bir görevin yerine getirilmesi veya kontrolöre veya verinin iletildiği üçüncü bir tarafa verilmiş olan kamu yetkisinin ifası için gerekli olması,
- (5) İşlemenin, bilgiye konu kişinin hakları, çıkarları ve temel özgürlüklerinin üstün geldiği durumlar hariç, kontrolör veya verinin iletildiği üçüncü tarafça izlenen yasal çıkarlar amacıyla gerekli olması.

Hassas Verinin İşlenmesi

7. (1) Hassas verinin derlenmesi ve işlenmesi yasaktır.

Ancak bilgiye konu kişinin açık onayının olması veya bilgiye konu kişinin fiziksel veya yasal olarak onay vermediği durumlarda, kendisinin veya bir başka kişinin hayati çıkarlarının korunması için gerekli olması veya yasal bir yükümlülüğünden kaynaklanması halinde hassas veriler derlenebilir ve işlenebilir.

(2) Sağlık ile ilgili hassas veriler yukarıdaki (1)'inci fıkradaki yasak kapsamı dışındadır. Bu tür veriler, meslek olarak sağlık hizmeti veren ve gizlilik yükümlülüğü bulunan veya ilgili davranış ilkelerine tabi olan kişi veya kurumlarca derlenebilir veya işlenebilir.

(3) Yukarıdaki (1)'inci ve (2)'nci fıkra kuralları uyarınca derlenip işlenen hassas veriler, yalnızca bilgiye konu kişinin onayı ile üçüncü taraflara iletebilir.

(4) Bakanlar Kurulu, Kurulun oybirliği ile alacağı bir karar doğrultusunda yapacağı tavsiye üzerine, kamu çıkarını ilgilendiren konularda hassas verilerin işlenmesine dair düzenlemeler içeren kararlar alabilir.

Başkana Bildirim

8. (1) Kontrolör, bir kişisel veri dosyalama sisteminin kurulması ve işletilmesi veya işlemenin başlatılması konusunda Başkana yazılı olarak bildirimde bulunmak zorundadır.

(2) Kontrolör, yukarıdaki (1)'inci fıkrada bahse konu bildirimde aşağıdaki hususları belirtmek zorundadır:

(A) Açık adını, mesleki adını veya unvanını ve adresini.

Kontrolör Kuzey Kıbrıs Türk Cumhuriyetinde yerleşik değilse, bunlara ilave olarak, Kuzey Kıbrıs Türk Cumhuriyetindeki temsilcisinin açık adını, mesleki adını veya unvanı ile adresini belirtmek zorundadır.

(B) Kişisel veri dosyalama sisteminin bulunduğu veya işleme için gerekli temel teçhizatın yerleştirildiği adres,

(C) İşlenen veya işlenmesi planlanan veya kişisel veri dosyalama sistemine dahil edilen veya dahil edilmesi planlanan verilerin işleme amacının izahı,

(Ç) Bilgiye konu kişilerin kategori veya kategorilerinin izahı,

(D) İşlenen veya işlenmesi planlanan veya kişisel veri dosyalama sistemine dahil edilen veya dahil edilmesi planlanan veri kategorileri,

(E) Kontrolörün işlemeyi yürüteceği veya dosyalama sistemini muhafaza edeceği süre,

(F) Kontrolörün veriyi ilettiği veya iletebileceği alıcılar veya alıcı kategorileri,

(G) Üçüncü ülkeler için önerilen veri transmisyonu ve bunun amacı,

(Ğ) Sistemin temel özellikleri ve dosyalama sisteminin veya işlemenin güvenliğine yönelik önlemler.

(3) İşleme veya dosyalama sisteminin, Başkan tarafından işleme konusunda belirlenen özel kuralların bulunduğu kategorilerden birinde yer alması halinde, kontrolör Başkana, işlemenin sözkonusu özel kurallara göre yürütüleceğini veya dosyalama sisteminin bu kurallara göre tutulacağını teyid eden bir bildirimde bulunur. Bu özel kurallar, aynı zamanda bildirimde özellikle şeklini ve içeriğini de belirler.

(4) Yukarıdaki (2)'nci fıkrada bahse konu bilgi, Başkan tarafından tutulan "Dosyalama Sistemleri ve İşlemleri Sicili"nde kaydedilir.

(5) Yukarıdaki (2)'nci fıkrada atıfta bulunulan bilgide olabilecek her türlü değişiklik, kontrolör tarafından yazılı olarak ve gecikmeksizin Başkana bildirilir

(6) Kontrolör, yukarıdaki (1)'inci fıkrada öngörülen bildirim yükümlülüğünden aşağıdaki durumlarda muaf sayılır:

(A) İşlemenin sadece yapılacak çalışmayla ilgili amaçlar için yapılması ve veri konusunun önceden bildirilmesi kaydıyla, yasal bir yükümlülüğün yerine getirilmesi veya bir sözleşmenin ifası için gerekli olması,

(B) İşlemenin, verilerin üçüncü taraflara transfer edilmemesi veya iletilmemesi kaydıyla, kontrolörün müşterilerini veya tedarikçilerini ilgilendirmesi durumunda,

(a) Bu bendin uygulanmasında, transmasyon veya haberleşmenin herhangi bir yasa veya mahkeme kararıyla yapılmış olması kaydıyla, mahkemeler ve kamu makamları üçüncü taraf olarak görülmezler.

(b) Sigorta şirketleri tüm sigorta çeşitleri için, eczacılık şirketleri, veri tedarik şirketleri ve bankalar ve kredi kartı veren şirketler gibi mali kurumlar bildirim yükümlülüğünden muaf değillerdir.

(C) İşlemenin bir topluluk, dernek, şirket veya siyasi parti tarafından yapılması ve üyelerin onay vermiş olmaları ve verilerin üçüncü taraflara transfer edilmemesi veya iletilmemesi kaydıyla, bunların üyelerine dair veriler içermesi durumunda yukarıda bahse konu topluluk, dernek, şirket veya siyasi partilerin amaçları doğrultusunda üyelerine bildirimde bulunulduğu takdirde üyeler; bildirimde ilgili mevzuat veya mahkeme kararıyla yapılması halinde mahkemeler ve kamu makamları, üçüncü taraf olarak addedilmezler.

(Ç) İşlemenin, kontrolörün tıbbi gizliliğe veya ilgili mevzuatın veya davranış kurallarının gerektirdiği diğer gizliliğe bağlı olması ve verilerin üçüncü taraflara transfer edilmemesi veya iletilmemesi kaydıyla, doktorlar veya sağlık hizmeti veren diğer kişiler tarafından yapılması ve tıbbi bilgiler içermesi durumunda; işleme, tele-tıp operasyonlarıyla ilgili programlar veya tıbbi hizmetlerin bir şebeke aracılığıyla sağlanması çerçevesinde gerçekleştiriliyor ise, klinikler, hastaneler, sağlık merkezleri, nekahat ve zehirli maddelerden arınma merkezleri, sigorta fonları ve sigorta şirketleri ile kişisel verilerin kontrolörleri bildirim yükümlülüğünden muaf değillerdir.

(D) Kontrolörün ilgili yasanın gerektirdiği gizliliğe bağlı kalması ve verilerin, gerekli ve müvekkillerinin talepleriyle doğrudan bağlantılı olması halinde, üçüncü taraflara gönderilmemesi veya iletilmemesi kaydıyla, işlemenin avukatlar tarafından yapılması ve müvekkillerine yasal hizmetlerin sağlanmasını ilgilendirmesi durumunda.

Kişisel Veri Dosya Sistemlerinin Birleştirilmesi

9. (1) Kişisel veri dosya sistemlerinin birleştirilmesine yalnızca, bu birleştirme önemli bir kamu çıkarı için olduğu takdirde, bu Yasanın 6'ncı maddesinde belirtilen koşullar altında izin verilir.

(2) Her birleştirme, iki veya daha fazla kişisel veri dosya sistemini birleştirecek kontrolör veya kontrolörler tarafından ortaklaşa yapılacak bir başvuru ile Başkana bildirilir.

(3) (A) Birleřtirilecek dosya sistemlerinden birisinin dahi hassas veri iermesi, veya birleřtirme sonucu hassas verinin aıa ıkması veya yapılacak birleřtirme iin tek bir kod numarası kullanılması halinde ise birleřtirme sadece Kurulun cret karřılıėında vereceėi “Birleřtirme Ruhsatı” ile mmkndr.

(B) Birleřtirme ruhsatı, kontrolrlerin dosyalama sistemleri hakkındaki grřleri alındıktan sonra verilir ve ařaėıdaki hususları ierir:

(a) Birleřtirmenin neden gerekli olduėu,

(b) Birleřtirmenin ilgili olduėu kiřisel verinin kategorisi,

(c) Birleřtirmeye izin verilen zaman dilimi ve

() Bilgiye konu kiřinin ve nc tarafların bařta mahremiyet hakları olmak zere, hak ve zgrlklerini korumak amacıyla ileri srlen her trl řart ve kořul.

(C) Birleřtirme ruhsatı, kontrolrlerin bařvurusunu mteakip yenilenebilir.

(4) Yukarıdaki (2)'nci fıkrada sz edilen bařvurular ile “Birleřtirme Ruhsatı” suretleri, Bařkan tarafından tutulan Birleřtirme Sicilinde yer alır.

Veri Koruma Grevlisi

10. (1) Kiřisel veri iřleyen her kurum ve kuruluř, iřlediėi veriyi koruyacak en az bir personel grevlendirmekle ykmldr.

(2) Veri Koruma Grevlisi, bu Yasa erevesinde, kontrolrn isteyebileceėi bilgiler doėrultusunda, kurumdaki kiřisel verilerin iřlenmesini ve korunmasını izler ve gzetir.

NC KISIM

Veri Transferi ve Gizlilik

Diėer lkelere Veri Transferi

11. (1) Bu Yasa kurallarına baėlı olarak iřlenmiř veya iřlenmeye niyet edilmiř verinin diėer lkelere transferi, Kurulun cret karřılıėında vereceėi “Transfer Ruhsatı” ile mmkndr. Kurul, ancak ilgili lkenin yeterli seviyede koruma saėlaması halinde szkonusu ruhsatı verir. “Transfer Ruhsatı” verilirken, verinin niteliėi, iřleme ama ve sresi, hukukun genel ve zel ilkeleri, davranıř ilkeleri ve verinin korunması iin gvenlik nlemleri ile menře lkesindeki koruma seviyesi, verinin iletilme řekli ve nihai hedefi gznnde bulundurulur.

(2) Kiřisel verinin yeterli dzeyde koruma saėlamayan bir lkeye transferine, ařaėıdaki kořullardan bir veya daha fazlasının yerine getirilmesi halinde izin verilir:

(A) Bilgiye konu kişinin, herhangi bir kuşkuya yer bırakmayacak şekilde ve hukuka veya kabul edilmiş ahlak değerlerine aykırı olmayacak şekilde alınmış olmak kaydıyla transfere onay vermesi.

(B) Aşağıdaki koşullar altında transfer gereklidir:

(a) Bilgiye konu kişinin hayati çıkarlarının korunması veya

(b) Bilgiye konu kişi ile kontrolör veya kontrolörle üçüncü taraf arasında, bilgiye konu kişinin çıkarı için yapılmış olan bir sözleşmenin tamamlanması veya kurallarının yerine getirilmesi için veya

(c) Bilgiye konu kişinin talebi üzerine alınan, bilgiye konu kişi ile kontrolör arasında yapılacak sözleşme öncesi önlemlerin uygulanması için.

(C) Transferin önemli kamu çıkarı, özellikle diğer ülkenin kamu makamlarıyla işbirliğine ilişkin sözleşmenin kurallarının yerine getirilmesi nedeniyle gerekli olması veya bu nedenlerle transfere hukuken ihtiyaç duyulması.

(Ç) Transferin bir mahkemeye yöneltilecek hukuki iddiaların oluşturulması, öne sürülmesi ve savunulması için gerekli olması.

(D) Transferin, ilgili yasa uyarınca kamuya bilgi veren ve kamuya veya meşru çıkarı olan herkese açık olan bir kamu kayıt merkezinden, kayıt merkezine erişimin yasal olarak mümkün olması halinde, yapılması.

(3) Kurul, yeterli düzeyde koruma sağlamayan bir ülkeye, kontrolörün özel ve temel hakların korunmasına ilişkin yeterli teminat vermesi ve bu hakların ve teminatın uygun sözleşme kurallarından kaynaklanması halinde, veri transferine izin verebilir.

İşlemenin Gizliliği ve Güvenliği

12. (1) Verinin işlenmesi gizlidir. Bu işlem yalnızca kontrolör, işlemci veya işlemcinin yetkisi altında görev yapan kişilerce ve yalnızca kontrolörden alınan talimat uyarınca yapılır.

(2) İşlemenin yapılması için, kontrolörün uygun nitelikleri haiz, teknik bilgi açısından yeterli teminatı sağlayan ve gizliliğe riayet açısından şahsi güvenilirliği olan kişileri seçmesi gerekir.

(3) Kontrolör, verinin istem dışı veya yasadışı zarara uğraması, istem dışı kaybı, değiştirilmesi, yetkisiz kişilere iletilmesi veya erişim imkanı sağlanması ve her türlü diğer yasadışı işleme tabi tutulmasına karşı gizliliğinin ve korunmasının sağlanması için uygun kurumsal ve teknik önlemleri almalıdır. Bu önlemler, işleme sürecindeki ve veri işlemenin doğasına uygun düşecek riskleri karşılamada güvenliği temin etmelidir.

(4) Başkan, teknolojik gelişmeleri de gözönünde bulundurarak, verinin güvenliğine ve her kategoride veri için gerekli koruma önlemlerine ilişkin olarak zaman zaman talimat verebilir.

(5) İşleme, kontrolör adına kendi denetimi altında olmayan bir işlemci tarafından icra edilmekteyse, işleme görevinin verilmesinin yazılı olarak yapılması gerekir. Görevlendirme, işlemcinin işlemeyi yalnızca kontrolörden aldığı talimat üzerine yapmasını ve bu kısımda yeralan diğer yükümlülükleri de üstlenmesini sağlamalıdır.

DÖRDÜNCÜ KISIM

Bilgiye Konu Kişinin Hakları

Bilgilendirme Yükümlülüğü

13. (1) Kontrolör, bilgiye konu kişiden kişisel verilerin toplanması aşamasında, bilgiye konu kişi eğer halihazırda sahip değilse, kendisine uygun ve açık bir şekilde, en azından aşağıdaki bilgileri vermekle yükümlüdür:

(A) Kendisinin ve varsa temsilcisinin kimliği,

(B) İşlemenin amacı.

(2) Kontrolör, bilgiye konu kişiyi aşağıdaki konularda da ayrıca bilgilendirmekle yükümlüdür:

(A) Verinin alıcıları veya alıcı kategorileri,

(B) Veriye erişim ve verinin düzeltilmesi hakkının varlığı, ve

(C) Bu verinin gerekli olması halinde, verinin güvenlik içerisinde işlenmesinin sağlanması koşuluyla, bilgiye konu kişinin yasal olarak yardım etmek mecburiyetinde olup olmadığı, mecbursa bunu reddetmesinin sonuçları.

(3) (A) Bilginin üçüncü taraflardan alınması halinde, bilgiye konu kişi, yukarıdaki (1)'inci fıkra uyarınca, bilginin kaydı sırasında veya bilginin üçüncü taraflara iletilmesinin beklendiği aşamada, henüz bilgilendirilmemişse, bilgilendirilecektir.

(B) İşlemenin özellikle istatistiki ve tarihi amaçlarla, veya bilimsel araştırma amacıyla yapılması halinde, bilgiye konu kişiyi haberdar etmek imkansız ise veya onu haberdar etmek için orantısız bir çaba gerekliyse veya bilginin iletilmesi başka bir yasayla mümkünse, her koşulda Başkanın izni alınmak kaydıyla, yukarıdaki (A) bendi kuralları uygulanmaz.

(4) Kontrolörün başvurusu ve Başkanın kararı üzerine, kişisel verinin toplanması konusunda yukarıdaki (1)'inci, (2)'nci ve (3)'üncü fıkralar uyarınca haberdar etme yükümlülüğü, Devletin

savunması, ulusal ihtiyaçları veya ulusal güvenliği veya cezai suçların önlenmesi, tespiti, soruşturulması ve kovuşturulması amacıyla, kısmen veya tamamen gözardı edilebilir.

(5) Bilgiye konu kişinin bu Yasanın 14'üncü ve 15'inci maddelerinde de atıfta bulunulan haklarına hanel gelmeksizin ve mahremiyet hakkı ve aile yaşamının ihlal edilmemesi koşuluyla, derlemenin yalnızca gazetecilik amacıyla yapılması halinde, haberdar etme yükümlülüğü bulunmamaktadır.

Erişim Hakkı

14. (1) Herkesin kendisine ait kişisel verinin işlenip işlenmediğini bilmeye hakkı vardır. Bu nedenle, kontrolör kendisine yazılı olarak yanıt vermelidir.

(2) Bilgiye konu kişi, aşağıdaki hususlarda, kontrolöre, soru sorma ve yanıt alma hakkına sahiptir:

(A) (a) İşlemeye tabi tutulmuş, kendisine ait tüm kişisel veri ve aynı zamanda bunların kaynağı,

(b) İşlemenin amacı, bu bilgiyi alanlar veya alan kategoriler ile işlenmiş veya işlemeye tabi tutulmakta olan verinin kategorileri,

(c) Bir önceki bilgilendirmeden beri işlemede kaydedilen ilerleme.

(B) Verinin düzeltilmesi, silinmesi veya bloke edilmesi, özellikle yanlışlıklar ve eksiklikler nedeniyle bu Yasanın kuralları uyarınca icra edilmemiş olan işleme.

(C) İmkansız olmadığı ve orantısız çaba gerektirmediği sürece, verinin iletildiği üçüncü taraflara (B) bendi uyarınca yapılmış olan her türlü düzeltme, silme ve bloke etme hakkında bildirim yapılması.

(3) Kontrolör, başvurunun sunulmasından itibaren otuz gün içinde yanıt vermediği veya yanıtı tatmin edici olmadığı takdirde, bilgiye konu kişi Kurula başvuru hakkına sahiptir. Kurul bu konudaki kararı verir.

(4) Bilgiye konu kişi, erişim hakkını bir uzmanın yardımıyla kullanabilir.

(5) Sağlığa ilişkin veri, bilgiye konu kişiye doktor aracılığıyla bildirilir.

(6) Kontrolör, Kurulun kararı ile bilgiye konu kişiye, bilgi verilmesini;

(A) Özel yasada açıkça öngörülmüş olması,

(B) Üstün nitelikte bir kamu yararı, özellikle Devletin iç ve dış güvenliğinin korunması açısından gerekli olması,

(C) Bilgi verilmesinin idari veya cezai bir soruşturmanın amacının gerçekleşmesini güçleştirmesi durumlarında sınırlayabilir, erteleyebilir veya reddedebilir, ayrıca bunların sebebini ilgili kişiye yazılı olarak bildirir.

İtiraz Hakkı

15. (1) Bilgiye konu kişinin, herhangi bir zamanda, içinde bulunduğu özel duruma ilişkin meşru nedenlerle, kendisine ait işlenmiş, işlenmekte olan veya işlenmesi planlanan verinin işlenmesine itiraz hakkı bulunmaktadır. İtiraz yazılı olarak, kontrolöre yapılır ve düzeltme, kullanımdan geçici olarak imtina, bloke etme, iletilmesinden veya silinmeden imtina, işlenmeme ve silinme gibi belirli bir işlemin yapılması veya yapılmaması talebini içermelidir. Kontrolör, bu itirazlara, talebin iletilmesini takiben onbeş iş günü içinde yazılı olarak yanıt vermelidir. Yanıtında, yaptığı işlem veya gerekli hallerde talebin yerine getirilmemesine ilişkin nedenlere yer vermelidir. İtirazların reddedilmesi halinde, yanıtın Kurula iletilmesi gerekmektedir.

(2) Kontrolör, kendisine tanınan zaman dilimi içinde yanıt vermezse, veya yanıtı tatmin edici bulunmazsa, bilgiye konu kişi Kurula başvurma ve itirazının incelenmesini talep etme hakkına sahiptir. Kurul bu konudaki kararı verir. Başkan, bilgiye konu kişinin mağduriyet riskinin yüksek olması ve itirazları mantıklı bulması ve işlemin devam etmesi halinde, itirazlar hakkında nihai karar verilene kadar işlemeyi derhal askıya alma talimatı verebilir.

Erişim ve İtiraz Haklarının Kullanılması

16. Erişim ve itiraz hakları, kontrolöre başvurunun sunulması suretiyle kullanılır. Kişinin erişim hakkını kullanarak veriye ulaşması, bu Yasanın 37'nci maddesinin (2)'nci fıkrasında belirtilen ücret karşılığında olur. Kontrolör veya Kurulun, verinin düzeltilmesi veya silinmesi talebini yerinde bulması halinde, kontrolör başvuru sahibine, gecikmeksizin ve hiçbir ücret almaksızın, anlaşılabilir bir dille kendisini ilgilendiren işlemin düzeltilmiş halini vermekle yükümlüdür.

Doğrudan veya Dolaylı Pazarlama İçin İşleme

17. (1) Bilgiye konu kişi kontrolöre yazılı onay vermeden, kişisel veri, doğrudan veya dolaylı olarak mal veya hizmetin pazarlanması amacıyla kimse tarafından kullanılamaz.

(2) Kontrolörün, yukarıdaki (1)'inci fıkrada belirtilen amaçlar nedeniyle kişisel veriyi kullanma isteği devam ediyorsa konu kişinin onayını almak için, bilginin kamuya açık kaynaklardan temin edilmesi kaydıyla, bilgiye konu kişinin adını ve adresini kullanabilir.

Tazmin Hakkı

18. Kontrolör, zararı doğuran olaydan dolayı sorumlu olmadığını kanıtlamadıkça, bu Yasanın herhangi bir kuralının ihlalden ötürü zarar gören bilgiye konu kişinin zararını tazmin eder.

Kontrolör ve İşlemcinin Gizlilik Yükümlülüğü

19. Kontrolör ve işlemciler, bu Yasa kuralları çerçevesinde öğrendikleri kişilere ait verileri, yasal olarak iletebilecekleri kişi veya mercilerden başkasına iletmezler veya açıklamazlar. Sözkonusu kişilerin bu yükümlülükleri görevlerinden ayrıldıktan sonra da devam eder.

BEŞİNCİ KISIM

Kişisel Verileri Koruma Kurulunun

Oluşumu, Yetki ve Görevleri

Kişisel Verileri Koruma Kurulu

20. Kişisel verinin korunması ve kişisel verinin işlenmesi çerçevesinde bireylerin korunmasına ilişkin kuralların uygulanmasını denetlemek ve izlemekten sorumlu, tüzel kişiliğe sahip, idari ve mali özerkliğe sahip bir Kişisel Verileri Koruma Kurulu oluşturulur.

Kurulun Oluşumu

21. (1) Kurul, bir başkan ve on üye olmak üzere onbir kişiden oluşur;

(2) (A) Kurul Başkanı Cumhurbaşkanı tarafından atanır ve atama işlemi Cumhuriyet Meclisince onaylanır.

(B) Cumhurbaşkanınca, bir kişi Kurul Başkanı olarak atandıktan sonra, konu Cumhuriyet Meclisinin onayını almak üzere Cumhuriyet Meclisi Başkanlığına sunulur.

(C) Cumhuriyet Meclisi Başkanlığı, atama işlemi değerlendirme üzere konuyu, Hukuk ve Siyasi İşler Komitesine iletir. Hukuk ve Siyasi İşler Komitesi, Kurul Başkanı olarak atanan kişinin, bu Yasanın 22'nci maddesinde öngörülen nitelikleri taşıyıp taşımadığını inceler ve değerlendirme sonuçlarını içeren bir Rapor hazırlayarak Genel Kurula sunar.

(Ç) Raporun Genel Kurulda kabul edilmesi halinde oylamaya geçilir. Oylama Cumhuriyet Meclisi İçtüzüğü'nün 163'üncü maddesi kuralları çerçevesinde yapılır.

(D) Onay için üye tam sayısının salt çoğunluğu aranır. Gerekli çoğunluğun sağlanamaması durumunda ikinci tur bir oylama yapılır ve bu turda onay için, toplantıya katılan üyelerin salt çoğunluğu yeterli olur.

(3) (A) Kurulun diğer üyeleri aşağıda belirtilen kişilerden oluşur:

(a) Cumhuriyet Meclisince atanacak iki üye,

(b) Biri, Bakanlar Kurulu Kararı ile oluşturulan Kamu Net Üst Kurulunda görev yapan üyeler arasından olmak üzere Başbakanın önerisi ile Bakanlar Kurulunca atanacak iki üye,

(c) Barolar Birliđi, Kıbrıs Türk Ticaret Odası, Kıbrıs Türk Sanayi Odası, Kıbrıs Türk Mühendis ve Mimar Odaları Birliđi ve Kıbrıs Türk Tabipler Birliđinin kendi üyeleri arasından atayacakları birer üye ve

(ç) Yükseköğretim Planlama, Denetleme ve Akreditasyon ve Koordinasyon Kurulunun akademisyenler arasından atayacağı bir üye.

(B) (a) Cumhuriyet Meclisi tarafından Kurula yapılacak atama için, Cumhuriyet Meclisinde grubu bulunan her siyasi parti ve milletvekilleri aday gösterebilir. Ayrıca, doğrudan doğruya aday olmak isteyenler de adaylık başvurusunda bulunabilirler.

(b) Kurula, Cumhuriyet Meclisince atanacak üyeleri belirlemekle ilgili kurallar Cumhuriyet Meclisi İctüzüğü çerçevesinde yapılır.

(c) Cumhuriyet Meclisi Başkanlığı, siyasi parti gruplarınca veya milletvekillerince aday gösterilen veya doğrudan doğruya aday olmak isteyenlere ilişkin dosyaları, adayların aşğıdaki 22'nci maddede öngörülen nitelikleri taşıyıp taşımadıklarına ilişkin değerlendirmeyi yapmak üzere Hukuk ve Siyasi İşler Komitesine iletir. Komite, değerlendirme sonuçlarını içeren bir Rapor hazırlayarak Genel Kurula sunar.

(ç) Seçim, birleşik oy pusulası üzerinde ve Cumhuriyet Meclisi İctüzüğünün 163'üncü maddesi kuralları çerçevesinde yapılır ve seçim sonucu atama işlemleri gerçekleşir.

Kurul Başkan ve Üyelerinin Nitelikleri

22. (1) Kurul Başkan ve üyesi olarak atanacak kişilerde aşğıdaki nitelikler aranır:

(A) Kuzey Kıbrıs Türk Cumhuriyeti Yurttası olmak,

(B) Üniversite veya dengi bir yüksekokuldan mezun olmak,

(C) Kamu haklarından yasaklı bulunmamak,

(Ç) Bir yıldan fazla hapis cezasına çarptırılmamış olmak veya affa uğramış olsalar dahi, rüşvet, hırsızlık, dolandırıcılık, sahtekarlık, irtikap, ırza geçme, hileli iflas ve benzeri yüz kızartıcı suçlardan dolayı mahkum olmamış olmak,

(D) Disiplin suçundan ötürü Kamu hizmetinden azledilmemiş olmak.

(2) Kurul Başkanı olarak atanacak kişide yukarıdaki (1)'inci fıkrada öngörülen nitelikler yanında aşğıdaki nitelikler aranır:

(A) Kamu görevinde veya kamu görevi dışında sorumluluk taşıyan bir görevde en az on yıl çalışmış olmak veya

(B) Doktora seviyesinde lisans üstü eğitim yapmış ve kamu görevinde veya kamu görevi dışında sorumluluk taşıyan bir görevde en az beş yıl çalışmış olmak.

Kurul Başkanının Görev ve Yetkileri

23. Kurul Başkanının görev ve yetkileri şunlardır:

- (1) Kurulu, yurt içinde ve yurt dışında temsil etmek ve Kurul toplantılarını yönetmek,
- (2) Kurula bu Yasa ile verilen yetkilerin kullanılmasını ve görevlerin gerektirdiği hizmetlerin yürütülmesini sağlamak,
- (3) Kurul personelinin çalışmalarını gözetmek, denetlemek ve onların verimliliklerini artırma yönünde gerekli önlemleri almak,
- (4) Kurul bütçesinin ve kesin hesaplarının hazırlanmasını ve uygulanmasını sağlamak ve Kurul bütçesinin ita amirliğini yapmak,
- (5) Hizmet için gerekli araç, gereç ve aygıtların Kurul kararlarına uygun olarak satın alınmasını sağlamak,
- (6) Bu Yasa ile kendisine verilen diğer görevleri yerine getirmek ve yetkileri kullanmak.

Kurul Başkan ve Üyelerinin Görev Süresi ve Yeniden Atanabilmesi

24. (1) Kurul Başkan ve üyelerinin görev süresi dört yıldır.

(2) Kurul Başkan veya üyeliğinde bu Yasanın 26'ncı maddesi uyarınca boşalma olması halinde, boşalan Başkanlık veya üyelik boşalma tarihinden başlayarak bir ay içinde bu Yasanın 21'inci maddesi kuralları çerçevesinde doldurulur. Boşalan üyelik hangi kontenjandan olmuşsa yeni üyenin atanması da o kontenjandan olur. Kurul Başkanlığında veya Cumhuriyet Meclisince atanan üyeliklerde, Cumhuriyet Meclisinin tatilde olduğu bir tarihte boşalma olması halinde, tatilin bitiminden itibaren bir ay içinde onaylama veya atama işlemi gerçekleştirilir.

(3) Boşalan Kurul Başkanlığına veya üyeliğine seçilen kimse, yerine seçildiği Kurul Başkanı veya üyenin süresini tamamlar.

(4) Yeni Kurul Başkanı ve üyeleri atanuncaya kadar eski Kurul Başkanı ve üyelerinin görevi devam eder. Ancak bu Yasanın 26'ncı maddesinin (1)'inci fıkrasının (Ç) bendi uyarınca görevden alınan Başkan ve üyelerin görevleri devam etmez.

(5) Görev süresi dolan Kurul Başkanı veya üyesi yeniden atanabilir.

Kurul Başkan ve Üyelerinin Siyasal Parti Organlarında Görev Alamayacakları

25. Kurul Başkanı veya üyesi olarak atananlar, atandıkları tarihten başlayarak siyasal partilerin organlarında görev alamazlar.

Kurul Başkanlığı veya Üyeliğinin Boşalması

26. (1) Aşağıdaki hallerde Kurul Başkanlığı veya üyeliği boşalır:

(A) Kurul Başkanı veya üyesinin ölümü veya istifa etmesi halinde,

(B) Bu Yasanın 22'nci maddesinde öngörülen niteliklerden bir veya daha fazlasının yitirmesi halinde,

(C) Özürsüz olarak üst üste üç toplantıya katılmaması halinde,

(Ç) Atayan makam veya kurumca görevden alınması halinde; Kurul Başkanının Cumhurbaşkanınca görevden alınması halinde bu işlemi Meclis Genel Kurulunun onaylaması gerekir. Bu durumda işlemin onayı için toplantıya katılan üyelerin salt çoğunluğu aranır.

(2) Kurul Başkanı, bu madde uyarınca boşalan üyeliği yazılı olarak Cumhurbaşkanına, Cumhuriyet Meclisi Başkanlığına, Bakanlar Kuruluna, Barolar Birliğine, Kıbrıs Türk Ticaret Odasına, Kıbrıs Türk Sanayi Odasına, Kıbrıs Türk Mühendis ve Mimar Odaları Birliğine, Kıbrıs Türk Tabipler Birliğine ve Yükseköğretim Planlama, Denetleme, Akreditasyon ve Koordinasyon Kuruluna bildirir. Cumhuriyet Meclisi Başkanlığı konuyu Genel Kurulun bilgisine sunar. Yukarıda belirtilen bildirim, Kurul Başkanlığının boşalması halinde, Kurulun en yaşlı üyesi tarafından yapılır.

Kurulun Toplantıları

27. (1) Kurul toplantılarına Başkan, yokluğunda ise en yaşlı üye başkanlık eder.

(2) Kurul toplantılarında toplantı yeter sayısı üye tam sayısının salt çoğunluğu, karar yeter sayısı ise toplantıya katılanların salt çoğunluğudur. Kabul ve ret oylarının eşit olması halinde oya konan husus reddedilmiş olur. Çekimser oylar toplantı yeter sayısına dahil olup, karar yetersayısı açısından dikkate alınmaz.

(3) Kurul kararları açık oyla alınır.

(4) Sürekli çalışan Kurul, ayda en az bir kez toplanır. Gerektiği takdirde Başkanın veya en az dört üyenin istemi ile Kurul olağanüstü toplanabilir. Olağan ve olağanüstü toplantıların günü, saati ve gündemi Başkan tarafından saptanır ve üyelere yazılı olarak duyurulur.

(5) Kurul üyeleri, kendileri veya temsil ettikleri kurumların taraf olduđu Őikayet konularına iliŐkin kararlara katılamazlar.

Kurulun Grevleri

28. Kurulun grevleri Őunlardır:

(1) KiŐisel verilerin iŐleme tabi tutulmasına iliŐkin konularda tavsiye ve nerilerde bulunmak ve bunları kendi takdirine bađlı olarak kamuoyunun dikkatine getirmek, gerekmesi halinde bu konularda tzk taslakları hazırlayıp Bakanlar Kurulunun onayına sunmak; standartları belirlemek ve bunlara iliŐkin bildirim yayımlamak.

(2) KiŐisel veri iŐlenmesiyle bađlantılı olarak kiŐileri koruyucu kuralların uygulanmasına ynelik talimatlar vermek.

(3) Bu Yasada ngrlen ruhsatları vermek.

(4) KiŐisel verilerin kontrolrler tarafından iŐlenmesi dolayısıyla kiŐilik haklarının ihlal edildiđini iddia edenlerin Őikayetleri hakkında karar vermek, bunu yaparken de bu tr veri iŐlenmesinin yasallıđını soruŐturmak, denetlemek, tm bunlarla ilgili iŐlemlerden baŐvuru sahiplerini haberdar etmek.

(5) Diđer lkelere veri aktarımı konusunda diđer lkede yasal bakımdan eŐdeđer korunmanın bulunduđu hususunda onay vermek.

(6) Kendi yetkisine veya bir Őikayete dayanarak herhangi bir dosyayı denetlemek. Bu bađlamda avukat ile mvekkili arasındaki mahremiyete tabi verinin dıŐındaki her trl mahrem de dahil olmak zere, kiŐisel verilere ulaŐma ve her trl veriyi toplama hakkında sahiptir. İstisnai olarak, ulusal gvenlik veya zellikli ciddi suların ortaya ıkarılması gerekesiyle tutulan dosyalarda isimleri kayıtlı olanlara iliŐkin ayrıntılara eriŐemez. Denetleme, Kurul tarafından bu amala grevlendirilmiŐ alıŐan tarafından yrtlr. Kurul BaŐkanı, ulusal gvenlik nedeniyle tutulmuŐ bir dosyaya bađlı bir denetlemede Őahsen hazır bulunur. Denetlemeye iliŐkin usul, Kurul tarafından hazırlanıp, BaŐbakanlıka nerilecek ve Bakanlar Kurulunca onaylanacak bir tzkle belirlenir.

(7) Bir nceki takvim yılına ait yıllık grev raporunu hazırlamak. Sz konusu rapor, gerekli olması halinde ilgili mevzuatta yapılması gerekli deđiŐiklik nerilerini de kapsar.

(8) Bu Yasa kurallarına aykırılık taŐıyan herhangi bir hususu yetkili makamların dikkatine getirmek.

(9) Bu Yasa uyarınca verilen yetki ve grevlerin gerektirdiđi hizmetlerin yrtlebilmesi iin gerekli personeli bu Yasa kuralları erevesinde istihdam etmek.

(10) Görevlerini yerine getirmesi bağlamında diğer ülkelerde kurulmuş olan muadil kurul veya kurumlarla işbirliği içinde olmak.

Kurulun Gelirleri, Bütçesi, Kesin Hesapları ve Denetim

29. (1) Kurulun gelirleri şunlardır:

(A) Kurul tarafından verilecek "Birleştirme Ruhsatı" ve "Transfer Ruhsatı" karşılığında alınacak, bu Yasanın 37'nci maddesi uyarınca yapılacak tüzükte öngörülen ücret,

(B) Genel Bütçeye konulacak ödenek,

(C) Kurula yapılacak her türlü yardım ve bağışlar,

(Ç) Diğer gelirler.

(2) Cumhuriyet Meclisince onaylanıp yürürlüğe girmedikçe Kurul bütçesinden harcama yapılamaz.

Ancak, herhangi bir nedenle yeni mali yıl bütçe yasasının yürürlüğe girmemesi halinde, yeni mali yıl bütçe yasasının yürürlüğe gireceği tarihe kadar geçmiş yıl bütçe yasasına bağlı gider cetvellerinde öngörülen ödeneklerin 1/12'sinin aylık olarak uygulanmasına ve gelirlerin tahsiline devam edilebilir.

(3) Kurulun mali yılı 1 Ocakta başlayıp 31 Aralıkta sona eren takvim yılıdır.

(4) (A) Kurulun gelir ve giderleri, Kurul bütçesinde gösterilir.

(B) Kurulun bütçesi, her mali yılın başlangıcından en az üç ay önce Kurul tarafından hazırlanarak Başbakanlıkça Bakanlar Kuruluna gönderilir ve Bakanlar Kurulunca Cumhuriyet Meclisine sunulur.

(5) (A) Kurul bütçesi, Sayıştayın denetimine bağlıdır.

(B) Bütçe kesin hesapları, Sayıştayın uygunluk bildirimini ile birlikte, her mali yılın sona ermesinden başlayarak en geç altı ay içinde Cumhuriyet Meclisinin onayına sunulur.

Kurul Başkanının Tam Zamanlı Çalışması ve Kurul Başkan ve Üyelerinin Ödenekleri

30. (1) (A) Kurul Başkanı, tam zamanlı olarak görev yapar ve Başkanlığı süresince başka herhangi bir işle iştigal edemez.

(B) Kurul Başkanına, Bakanlar Kurulunca 18A bareminin en üst basamağından az olmamak kaydıyla saptanan aylık ödenek ödenir.

(C) Kurul Başkanı kamu görevlileri arasından atanmışsa, kamu görevlisinin asli kadrosunda çekmekte olduğu maaşı, Bakanlar Kurulunun bu fıkranın (B) bendi uyarınca saptayacağı miktara tamamlanır. Ancak bu ödenek emeklilik amaçları bakımından dikkate alınmaz. Görev süresinin

dolması veya görevden alınması halinde Başkan, eski baremi ile birlikte eski görevine iade edilir. Bu gibi hallerde Başkan olarak geçirdiği süre, barem içi artışında ve emeklilik amaçları açısından fiili hizmet süresi olarak dikkate alınır. Kamu görevi dışından atanan Kurul Başkanının görev süresinin sona ermesi veya görev süresi içinde görevine son verilmesi halinde bu kişinin Kurul ile ilişkisi kesilir.

(2) Kurul üyelerine, görev yaptıkları her toplantı günü için Bakanlar Kurulunca saptanacak miktarda huzur hakkı ödenir.

Kurul Hizmetlerinin Yürütülmesi ve Kurul Personelinin Statüsü

31. (1) Başkan ve Kurula, bu Yasa ile verilen yetki ve görevlerin gerektirdiği hizmetleri yürütmek üzere bir büro kurulur.

(2) Büroda istihdam edilecek personelin İş Yasası kuralları çerçevesinde istihdam edilmesi ve sözleşmeli olması esastır. Personel sayısı, 1 Koordinatör, 1 Hukukçu, 3 Bilgi/ Belge Yöneticisi, 2 Denetleme Memuru, 1 Mali İşler Memuru, 1 Sekreter, 1 Odacı/şöför olmak üzere 10 kişiyi geçemez.

Personele İlişkin Kurallar

32. (1) Personel, Kurul tarafından istihdam edilir ve hizmet koşulları sözleşmelerinde belirtilir.

(2) Personele verilecek ücretler, Bakanlar Kurulunca saptanmış olan kademe ve derecelere göre verilir ve her yıl Kurul Bütçesinde gösterilir.

Kurul Başkanının, Üyelerinin ve Personelinin Sır Saklama Yükümlülüğü

33. Kurul Başkanı, üyeleri ve kurulda çalışan her türlü personel, çalışmalarını ve denetlemelerini sırasında ilgililere ve üçüncü kişilere ait öğrendikleri sırları, bu konuda yasal olarak yetkili kılınan mercilerden başkasına açıklayamazlar ve kendi yararlarına kullanamazlar.

Bu yükümlülük, görevlerinden ayrılmalarından sonra da devam eder.

Şikayet Başvurusu

34. Bu Yasa kurallarının uygulanmasından kaynaklanan şikayetler bir başvuru ile Kurula yapılır. Kurul, şikayetleri inceleyip 30 gün içerisinde ilgiliye yazılı cevap vermekle yükümlüdür.

ALTINCI KISIM

Suç ve Cezalar

İdari Para Cezaları

35. (1) Bu Yasanın:

(A) 5'inci, 6'ncı ve 8'inci, 13'üncü, 14'üncü ve 15'inci maddelerdeki yükümlülükleri yerine getirmeyenlere 1,000 YTL (Bin Yeni Türk Lirası);

(B) 9'uncu, 11'inci ve 17'nci maddelerdeki yükümlülükleri yerine getirmeyenlere 2,000 YTL (İki Bin Yeni Türk Lirası);

(C) 7'nci ve 12'nci maddelerdeki yükümlülükleri yerine getirmeyenlere 3,000 YTL (Üç Bin Yeni Türk Lirası);

idari para cezası verilir.

(2) Yukarıdaki (1)'inci fıkrada öngörülen idari para cezaları Kurul tarafından verilir ve tebliğ edilir. Kurulun bu kararlarına karşı Yüksek İdare Mahkemesine başvurulabilir. İdari para cezaları, Yüksek İdare Mahkemesine başvurulmadığı takdirde başvurma süresinin son bulunduğu tarihten itibaren bir ay içinde; Yüksek İdare Mahkemesine başvurulduğu takdirde ise karar kişi aleyhine ise kesin kararın ilgiliye tebliğ edildiği tarihten itibaren bir ay içinde ödenir.

(3) Kurul tarafından bu madde uyarınca verilen para cezaları Kamu Alacaklarının Tahsil Usulü Yasasına göre tahsil edilir.

Suç ve Cezalar

36. (1) Yetkili olmadığı halde, kişisel veri içeren bir dosyaya müdahale eden veya buradaki veriye sahip olan veya veriyi silen, değiştiren, bozan, tahrip eden, işleyen, ileten ve nakleden veya verinin yetkisiz ellere geçmesine sebep olan veya bu tür kimselerin veriye sahip olmalarına izin veren veya bu veriyi bir şekilde kullanan bir kişi suç işlemiş olur ve mahkumiyeti halinde 15,000 YTL (On Beş Bin Yeni Türk Lirası)'na kadar para cezasına veya beş yıla kadar hapis cezasına veya her iki cezaya birden çarptırılabilir.

(2) Bu Yasanın 19'uncu ve 33'üncü maddeleri kurallarına aykırı hareket edenler bir suç işlemiş olurlar ve mahkumiyetleri halinde 10,000 YTL (Yirmi Bin Yeni Türk Lirası)'na kadar para cezasına çarptırılabilirler.

(3) Bu Yasanın 28'inci maddesinin (6)'ncı fıkrası uyarınca Kurul veya görevlendireceği personel tarafından yapılacak denetlemeye yasal gerekçesi olmadan engel olan veya izin vermeyenler bir suç işlemiş olurlar ve mahkumiyetleri halinde 10,000 YTL (On Bin Yeni Türk Lirası)'na kadar para cezasına çarptırılabilirler.

YEDİNCİ KISIM

Geçici ve Son Kurallar

Ruhsat ve Ücretlerle İlgili Tüzük Yapma Yetkisi

37. (1) “Birleştirme Ruhsatı” ve “Transfer Ruhsatı” için ödenecek ücret ve ruhsat verilirken uygulanacak şekil ve usule ilişkin kurallar

ve

(2) Bu Yasanın 16’ncı maddesinde öngörülen bilgiye erişim için ödenecek ücret,

Kurul tarafından hazırlanıp, Başbakanlıkça önerilecek ve Bakanlar Kurulunca onaylanacak bir tüzükte düzenlenir. Belirlenecek ücret, aylık asgari ücretin binde beşinden az ve aylık asgari ücret miktarından fazla olamaz.

Geçici Madde Mevcut Durumun Yasaya Uydurulması

1. Kişisel verileri işleme tabi tutan kamu kurum veya kuruluşları ile gerçek ve tüzel kişiler, Kurulun ilan edeceği tarihten itibaren altı ay içinde, durumlarını bu Yasa kurallarına uygun hale getirmek zorundadırlar.

Yürütme Yetkisi

38. Bu Yasayı, Bakanlar Kurulu adına Başbakan yürütür.

Yürürlüğe Giriş

39. Bu Yasa, Resmi Gazete’de yayımlandığı tarihten başlayarak yürürlüğe girer.

APEC PRIVACY FRAMEWORK (2015)

CONTENTS

Part I. Preamble

Part II. Scope

Part III. APEC Information Privacy Principles

Part IV. Implementation

Part A. Domestic Implementation

Part B. International Implementation

APEC PRIVACY FRAMEWORK (2015)

Foreword

APEC member economies realize the enormous potential of the digital economy to continue to expand business opportunities, reduce costs, increase efficiency, improve the quality of life, and facilitate the greater participation of small business in global commerce. A framework to protect privacy within and beyond economies and to enable regional transfers of personal information benefits consumers, businesses, and governments. Ministers have endorsed the APEC Privacy Framework, recognizing the importance of the development of effective privacy protections that avoid barriers to information flows and ensure continued trade and economic growth in the APEC region.

Part I. Preamble

1. APEC economies recognize the importance of protecting information privacy while maintaining information flows among economies in the Asia Pacific region and among their trading partners. As APEC Ministers acknowledged in endorsing the 1998 Blueprint for Action on Electronic Commerce, the potential of electronic commerce cannot be realized without government and business cooperation “to develop and implement technologies and policies, which build trust and confidence in safe, secure and reliable communication, information and delivery systems, and which address

issues including privacy...". Consumer trust and confidence in the privacy and security of online transactions, information networks and management of personal information is critical in enabling member economies to reap the benefits of electronic commerce and participate in today's information-driven economy. APEC economies realize that a key part of efforts to improve consumer confidence and ensure the growth of electronic commerce and innovation must be cooperation to promote both effective information privacy protection and the free flow of information in the Asia Pacific region, while respecting domestic laws and regulations, applicable international frameworks for information privacy protection, and strengthening information security in the Asia Pacific region.

2. Information and communications technologies, including mobile technologies, that link to the Internet and other information networks have made it possible to collect, store and access information from anywhere in the world. These technologies deliver social and economic benefits for individuals, governments, businesses and society at large, including increased consumer choice, market expansion, productivity, education, communication and product innovation. However, while these technologies make it easier and cheaper to collect, analyze and use large quantities of information, the way they are designed and used often make these activities undetectable to individuals. It can be more difficult for individuals to retain a measure of control over their personal information. As a result, individuals have become concerned about the harmful consequences that may arise from the use and misuse of their information. Therefore, there is a need to promote and enforce ethical and trustworthy information practices in on- and off-line contexts to bolster the confidence of individuals and businesses.

3. Business operations and consumer expectations have undergone a major shift due to, changes in technology and the nature of information flows: businesses and other, organizations now require simultaneous input and access to data 24-hours a day in, order to meet business, customer and societal needs, and to provide efficient and, cost-effective services. Regulatory systems that unnecessarily restrict this flow or, place burdens on it have adverse implications for global business, economies and, individuals. Therefore, in promoting and enforcing ethical information practices, there is also a need to develop systems for protecting privacy that account for these, realities in the global environment.,

4. APEC economies endorse the principles-based APEC Privacy Framework as an important tool in encouraging the development of appropriate privacy protections and ensuring the free flow of information in the Asia Pacific region.

5. The Framework, which aims at promoting electronic commerce throughout the Asia Pacific region, is consistent with the core values of the OECD's Guidelines on the Protection of Privacy and Trans-

Border Flows of Personal Data (OECD Guidelines), and reaffirms the value of privacy to individuals and to the information society. The previous version of the Framework (2005) was modelled upon the OECD Guidelines (1980) which at that time represented the international consensus on what constitutes fair and trustworthy treatment of personal information. The updated Framework (2015) draws upon concepts introduced into the OECD Guidelines (2013)⁵¹ with due consideration for the different legal features and context of the APEC region

6. The Framework specifically addresses the importance of protecting privacy while maintaining information flows, as well as issues of particular relevance to APEC member economies. Its practical and distinctive approach is to focus attention on consistent rather than identical privacy protection. In so doing, it seeks to reconcile privacy with business and societal needs and commercial interests, and at the same time, accords due recognition to cultural and other diversities that exist within member economies.

7. The Framework is intended to provide clear guidance and direction to businesses and government entities in APEC economies on common privacy issues and the impact of privacy issues upon the way legitimate business practice and government functions are to be conducted. It does so by highlighting the reasonable privacy expectations of the modern consumer. Businesses and member economies should respect individuals' privacy interests in a way that is consistent with the Principles outlined in the Framework.

8. The Framework was developed and updated in recognition of the importance of:

- Implementing appropriate privacy protections for personal information, particularly from the harmful consequences of intrusions and the misuse of personal information;
- The free flow of information to trade, and to economic and social growth in both developed and developing market economies;
- Enabling global companies that collect, access, use or process data in APEC member economies to develop and implement uniform approaches within their organizations for global access to and use of personal information;
- Empowering Privacy Enforcement Authorities to fulfill their mandate to protect individual privacy;

⁵¹ www.oecd.org/internet/ieconomy/privacy-guidelines.htm

- Advancing international and regional mechanisms, including the APEC Cross Border Privacy Rules (CBPR) system, to promote and enforce privacy and to maintain the continuity of information flows among APEC economies and with their trading partners;
- Encouraging organizations to be accountable for all personal information under their control; and
- Promoting interoperability between the Framework, and its implementing measures such as the CPEA and CBPR system, and privacy arrangements in other regions.

Part II. Scope

The purpose of Part II of the APEC Privacy Framework is to make clear the extent of coverage of the Principles.

Core definitions

9. Personal information means any, information about an identified or, identifiable individual.

COMMENTARY: 9. The Framework is intended to apply to, information about natural living, persons, not legal persons. The, Framework applies to personal, information, which is information that, can be used to identify an individual. It, also includes information that would not, meet this criteria alone, but when put, together with other information would, identify an individual. For example,, certain types of metadata, when, aggregated, can reveal personal, information and can give an insight into, an individual's behavior, social, relationships, private preferences and, identity

10. Personal information controller, means a person or organization who, controls the collection, holding,, processing, use, disclosure or, transfer of personal information. It, includes a person or organization, who instructs another person or, organization to collect, hold,, process, use, transfer or disclose, personal information on his or her, behalf, but excludes a person or, organization who performs such, functions as instructed by another, person or organization. It also excludes an individual who collects,, holds, processes or uses personal, information in connection with the, individual's personal, family or, household affairs.

COMMENTARY: 10. The Framework applies to persons or, organizations in the public and private, sectors who control the collection,, holding, processing, use, transfer or, disclosure of personal information. For, the purposes of the Framework, where a, person or organization instructs another, person or organization to collect, hold,, use, process, transfer or disclose, personal information on its

behalf, the, instructing person or organization is the, personal information controller and is, responsible for ensuring compliance, with the Principles.,

Individuals will often collect, hold and use personal information for personal, family or household purposes. For example, they often keep address books and phone lists or prepare family newsletters. The Framework is not intended to apply to such personal, family or household activities.

11. Publicly available information, means personal information about, an individual that the individual, knowingly makes or permits to be, made available to the public, or that, is legally obtained and accessed, from;

a) government records that are, available to the public;

b) journalistic reports; or,

c) information required by law to be, made available to the public.

COMMENTARY: 11. The Framework has limited application, to publicly available information. Notice, and choice requirements, in particular,, often are superfluous where the, information is already publicly available,, and the personal information controller, does not collect the information directly, from the individual concerned. Publicly, available information may be contained, in government records that are available, to the public, such as registers of people, who are entitled to vote, or in news, items broadcast or published by the, news media.

Additional definitions

12. CBPR system is the abbreviation of the APEC Cross Border Privacy Rules system.⁵²

COMMENTARY: 12. The APEC Cross Border Privacy Rules system, endorsed by APEC Leaders in 2011, is a voluntary accountabilitybased scheme to facilitate privacyrespecting personal information flows among APEC economies. It has four main components:

- set criteria for bodies to become recognised as CBPR system Accountability Agents;

⁵² For more information see: www.cbprs.org

- a process for information controllers to be certified as APEC CBPR system compliant by a recognised Accountability Agent;
- assessment criteria for use by recognised Accountability Agents when reviewing whether an information controller meets CBPR system requirements; and
- arrangements for enforcing CBPR system requirements through complaints processes provided by recognised Accountability Agents backed up by a Privacy Enforcement Authority (PEA) that is a participant in the CPEA.

13. CPEA is the abbreviation of the APEC, Cross-border Privacy Enforcement, Arrangement which is a practical, multilateral mechanism which, enables Privacy Enforcement, Authorities to cooperate in crossborder, privacy enforcement by, creating a framework under which, authorities may, on a voluntary, basis, share information and request, and render assistance in certain, ways.⁵³

COMMENTARY: 13. The CPEA is a multilateral mechanism, which enables Privacy Enforcement, Authorities in the APEC region to, cooperate in cross-border privacy, enforcement of Privacy Laws. Any, Privacy Enforcement Authority in an, APEC member economy may, participate. The CPEA aims to:

- facilitate information sharing among, Privacy Enforcement Authorities in, APEC member economies,;
- provide mechanisms to promote, effective cross-border cooperation, between Privacy Enforcement, Authorities in the enforcement of, Privacy Law; and,
- encourage information sharing and, cooperation on privacy investigation, and enforcement with privacy, enforcement authorities outside the, APEC region.

14. Privacy Enforcement Authority, means any public body that is, responsible for enforcing Privacy, Law, and that has powers to conduct, investigations and/or pursue, enforcement proceedings.

⁵³ The CPEA's formal title is "APEC Cooperation Arrangement for Cross-border Privacy Enforcement"., For more information see: www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-, Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx

COMMENTARY: 14. A Privacy Enforcement Authority is a public body that is responsible for enforcing an APEC economy's Privacy, Law. It will have powers to conduct, investigations and/or pursue, enforcement proceedings. An economy, may have more than one Privacy, Enforcement Authority.

15. Privacy Law means laws and, regulations of an APEC member, economy, the enforcement of which, have the effect of protecting, personal information consistent with, the APEC Privacy Framework.

COMMENTARY: 15. Privacy Laws in APEC member, economies come in a variety of forms., Some are general privacy or data, protection statutes while others take a, sectoral approach covering particular, areas such as credit reporting or health, information. In some cases the relevant, legal provisions are contained within, broader laws dealing with such issues as, telecommunications or consumer, protection. It is not important for the, purposes of the definition what the laws, are called: it is the effect of the laws that, matters.

16. PRP system is the abbreviation of, the APEC Privacy Recognition for, Processors system.

COMMENTARY: 16. The PRP system represents the baseline, requirements a processor must meet in, order to be recognized by an APEC recognized, Accountability Agent and, provide assurances with respect to the, processor's privacy policies and, practices. The PRP system helps, personal information processors to, demonstrate their ability to provide, effective implementation of a personal, information controller's privacy, obligations related to the processing of, personal information.

Application

17. In view of the differences in social,, cultural, economic and legal, backgrounds of each member, economy, there should be flexibility, in implementing these Principles.

COMMENTARY: 17. Although it is not essential for, electronic commerce that all laws and, practices within APEC be identical,, compatible approaches to privacy, protection among APEC economies will, greatly facilitate international, commerce and privacy enforcement, cooperation. Nonetheless,

the, Framework recognizes the need also to, take into account social, cultural and, other differences among economies.

18. Exceptions to these Principles contained in Part III of this Framework, including those relating to national sovereignty, national security, public safety and public policy should be:

a) limited and proportional to meeting the objectives to which the exceptions relate; and,

b) (i) made known to the public; or, (ii) in accordance with law.

COMMENTARY: 18. Economies implementing the, Framework at a domestic level may, adopt suitable exceptions that suit, their particular domestic, circumstances.

While recognizing the importance of, governmental respect for privacy, the, Framework is not intended to impede, governmental actions authorized by law, when taken to protect national security, public safety, national sovereignty or, achieve other important public policy, objectives. Nonetheless, member, economies should endeavor to ensure, that the impact of these activities upon, the rights, responsibilities and, legitimate interests of individuals and, organizations is as limited as possible.

Part III. APEC Information Privacy Principles

19. The Information Privacy Principles should be viewed and interpreted as a whole rather than looking at particular principles in isolation as there is a close interrelationship.⁵⁴

PRINCIPLES

I. Preventing Harm

20. Recognizing the interests of the, individual to legitimate, expectations of privacy, personal, information protection should be, designed to prevent the misuse of, such information. Further, acknowledging the risk that harm, may result from such misuse of, personal information, specific, obligations should take account of, such risk, and remedial measures, should be proportionate to

⁵⁴ There may be some minor inconsistency in language usage between principles (e.g. in relation to, how the principles describe the use of personal information). A future revision project that includes the, wording of the principles within its scope might usefully align the language. In the meantime, unless the, context suggests otherwise, 'use' of personal information should be considered to include collection,, holding, processing, use, disclosure or transfer of personal information.

the, likelihood and severity of the harm, threatened by the collection, use, and transfer of personal, information.

COMMENTARY: 20. This Principle recognizes that one of the, primary objectives of the Framework is, to prevent misuse of personal, information and consequent harm to, individuals. Therefore, privacy, protections, including self-regulatory, efforts, education and awareness, campaigns, laws, regulations, and, enforcement mechanisms, should be, designed to prevent harm to individuals, from the wrongful collection and misuse, of their personal information.

Hence, organizational controls should, be designed to prevent harms resulting, from the wrongful collection or misuse, of personal information, and should be, proportionate to the likelihood and, severity of any harm threatened by the, collection, use or transfer of personal, information.

Where there has been a significant, security breach affecting personal, information, it may help to reduce the risk of harmful consequences to the, individuals concerned to give notice to, Privacy Enforcement Authorities and/or, the individuals concerned.⁵⁵

II. Notice

21. Personal information controllers, should provide clear and easily, accessible statements about their, practices and policies with respect to, personal information that should, include; a) the fact that personal, information is being collected;

b) the purposes for which personal, information is collected;

c) the types of persons or, organizations to whom personal, information might be disclosed;

d) the identity and location of the, personal information controller,, including information on how to, contact them about their, practices and handling of, personal information;

e) the choices and means the, personal information controller, offers individuals for limiting the, use and disclosure of, and for, accessing and correcting, their, personal information.

22. All reasonably practicable steps shall, be taken to ensure that such notice is, provided either before or at the time, of collection of personal information., Otherwise, such notice should be, provided as soon after as is, practicable.

⁵⁵ See clause 54 below.

23. It may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information.

COMMENTARY: 21-23. This Principle is directed towards, ensuring that individuals are able to, know what information is collected, about them and for what purpose it is to, be used. By providing notice, personal, information controllers may enable an, individual to make a more informed, decision about interacting with the, organization.

Depending on the context in which the, personal information is collected, notice, may be provided using various methods., For example, one common method of, compliance with this Principle is for, personal information controllers to post, notices on their websites. Where, organizations engage individuals in, offline settings, such as in person or via, the telephone, posted or written notices, or telephone scripts may be used. In, other situations, placement of notices, on intranet sites or in employee, handbooks, for example, may be, appropriate. There are practical, challenges to giving notice in the mobile, context. To provide notice on small, screens, personal information, controllers may want to consider the, value of standard notices, icons, or other, measures.

Organizations should inform relevant, individuals at the time of, or before,, information is collected about them. At, the same time, the Principle also, recognizes that there are circumstances, in which it would not be practicable to, give notice at or before the time of, collection, such as in some cases where, digital technology automatically collects, information when a prospective, customer initiates contact, as is often, the case with the use of cookies.

Moreover, where personal information, is not obtained directly from the, individual, but from a third party, it may, not be practicable to give notice at or, before the time of collection of the, information. For example, when an, insurance company collects employees', information from an employer in order, to provide medical insurance services, it, may not be practicable for the insurance, company to give notice at or before the, time of collection of the employees', personal information.

Additionally, there are situations in, which it would not be necessary to, provide notice, such as in the collection, and use of publicly available, information, or of business contact, information and other professional, information that identifies an individual, in his or her professional capacity in a, business context. For example, if an, individual gives his or her business card, to another individual in the context of a, business relationship, the individual, would not expect to be given notice, regarding the collection and normal use, of that information for expected, business purposes.

Further, if colleagues who work for the, same company as an individual were to, provide the individual's business contact, information to potential customers of, that company, the individual would not, have an expectation that notice would, be provided regarding the transfer or, the expected use of that information.

III. Collection Limitation

24. The collection of personal, information should be limited to, information that is relevant to the, purposes of collection and any such, information should be obtained by, lawful and fair means, and where, appropriate, with notice to, or, consent of, the individual concerned.

COMMENTARY: 24. This Principle limits collection of, personal information by reference to, the purposes for which it is collected., The collection of the personal, information should be relevant to such, purposes, and necessity and, proportionality to the fulfillment of, such purposes may be factors in, determining what is relevant.

This Principle also provides that, collection methods must be lawful and, fair. So, for example, obtaining, personal information under false, pretenses (e.g., where an organization, uses phishing, telemarketing calls, or, pretexting emails to fraudulently, misrepresent itself as another, company in order to deceive, consumers and induce them to disclose, their credit card numbers, bank, account information or other sensitive, personal information) may in many, economies be considered unlawful., Therefore, even in those economies, where there is no explicit law against, these specific methods of collection,, they may be considered to be unfair, means of collection.

The Principle also recognizes that there, are circumstances where providing, notice to, or obtaining consent of,, individuals would be inappropriate., For example, in a situation where there, is an outbreak of food poisoning, it, would be appropriate for the relevant, health authorities to collect the, personal information of patrons from, restaurants without providing notice to, or obtaining the consent of individuals, in order to inform them of the, potential health risk.

IV. Uses of Personal Information

25. Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except:

a) with the consent of the individual whose personal information is collected;

b) when necessary to provide a service or product requested by the individual; or,

c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.

COMMENTARY: 25. This Principle limits the use of personal, information to fulfilling the purposes of, collection and other compatible or, related purposes. For the purposes of, this Principle, “uses of personal, information” includes the transfer or, disclosure of personal information.

Application of this Principle requires, consideration of the nature of the, personal information, the context of, collection, the individual’s expectations, and the intended use of the, information. The fundamental criterion, in determining whether a purpose is, compatible with or related to the stated, purposes is whether the extended usage, stems from or is in furtherance of such, purposes. The use of personal, information for “compatible or related, purposes” would extend, for example,, to matters such as the creation and use, of a centralized database to manage, personnel in an effective and efficient, manner; the processing of employee, payrolls by a third party; or, the use of information collected by an, organization for the purpose of granting, credit for the subsequent purpose of, collecting debt owed to that, organization.

V. Choice

26. Where appropriate, individuals, should be provided with clear,, prominent, easily understandable,, accessible and affordable, mechanisms to exercise choice in, relation to the collection, use and, disclosure of their personal, information. It may not be, appropriate for personal information, controllers to provide these, mechanisms when collecting publicly, available information.

COMMENTARY: 26. The general purpose of the Choice, Principle is to ensure that individuals are, provided with choice in relation to, collection, use transfer and disclosure of, their personal information. Whether, the choice is conveyed electronically, in, writing or by other means, notice of, such choice should be clearly worded, and displayed clearly and conspicuously., The mechanisms for exercising choice, should be accessible and affordable to, individuals. Ease of access and, convenience are factors that should be, taken into account.

Where an organization provides, information on available mechanisms, for exercising choice, consideration, should be given to tailoring the, information and the way it is conveyed, to make it

more “easily understandable”, to particular groups of individuals (e.g., by providing explanations in relevant, languages, if the information is aimed at, children, in ways that are ageappropriate).

This Principle also recognizes, through, the introductory words “where, appropriate”, that there are certain, situations where it would not be, necessary to provide a mechanism to, exercise choice.

In many situations it would not be, necessary or practicable to provide a, mechanism to exercise choice when, collecting publicly available, information. For example, it would not, be necessary to provide a mechanism to, exercise choice to individuals when, collecting their name and address from, a public record or a newspaper.

In specific and limited circumstances it, would not be necessary or practicable to, provide a mechanism to exercise choice, when collecting, using, transferring or, disclosing other types of information., For example, when business contact, information or other professional, information that identifies an individual, in his or her professional capacity is, being exchanged in a business context it, is generally impractical or unnecessary, to provide a mechanism to exercise, choice, as in these circumstances, individuals would expect that their, information be used in this way.

Further, in certain situations, it would, not be practicable for employers to, provide a mechanism to exercise choice, related to the use of the personal, information of their employees when, using such information for employment, purposes. For example, if an, organization has decided to centralize, human resources information, that, organization should not be required to, provide a mechanism to exercise choice, to its employees before engaging in, such an activity.

VI. Integrity of Personal Information

27. Personal information should be, accurate, complete and kept up-to-date, to the extent necessary for the, purposes of use.

COMMENTARY: 27. This Principle recognizes that a personal, information controller is obliged to, maintain the accuracy and, completeness of records and keep them, up to date as necessary to fulfill the, purposes of use. Making decisions, about individuals based on inaccurate,, incomplete or out of date information, may not be in the interests of individuals, or organizations.

VII. Security Safeguards

28. Personal information controllers, should protect personal information, that they hold with appropriate, safeguards against risks, such as loss, or unauthorized access to personal, information, or unauthorized, destruction, use, modification or, disclosure of information or other, misuses. Such safeguards should be, proportional to the likelihood and, severity of the harm threatened, the, sensitivity of the information and the, context in which it is held, and should, be subject to periodic review and, reassessment.

COMMENTARY: 28. This Principle recognizes that individuals, whose personal information is, entrusted to others are entitled to, expect that their information be, protected with reasonable security, safeguards.

VIII. Access and Correction

29. Individuals should be able to:

- a) obtain from the personal, information controller, confirmation of whether or not, the personal information controller holds personal, information about them;
- b) have communicated to them,, after having provided sufficient, proof of their identity, personal, information about them;; i. within a reasonable time;; ii. at a charge, if any, that is not, excessive;; iii. in a reasonable manner;; iv. in a form that is generally, understandable; and,
- c) challenge the accuracy of, personal information relating to, them and, if possible and as, appropriate, have the, information rectified, completed,, amended or deleted.

30. Such access and opportunity for correction should be provided except where:

- (i) the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question;
- (ii) the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or
- (iii) the information privacy of persons other than the individual would be violated.

31. If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial.

COMMENTARY: 29-31. The ability to access and correct, personal information, while generally, regarded as a central aspect of privacy, protection, is not an absolute right., This Principle includes

specific, conditions for what would be considered reasonable in the provision, of access, including conditions related, to timing, fees, and the manner and, form in which access would be, provided. What is to be considered, reasonable in each of these areas will, vary from one situation to another, depending on circumstances, such as, the nature of the information, processing activity. Access will also be, conditioned by security requirements, that preclude the provision of direct, access to information and will require, sufficient proof of identity prior to, provision of access.

Access must be provided in a, reasonable manner and form. A, reasonable manner should include the, normal methods of interaction, between organizations and individuals., For example, if a computer was, involved in the transaction or request,, and the individual's email address is, available, email would be considered "a, reasonable manner" to provide, information. Organizations that have, transacted with an individual may, reasonably be expected to answer, requests in a form that is similar to, what has been used in prior exchanges, with said individual or in the form that, is used and available within the, organization, but should not be, understood to require separate, language translation or conversion of, code into text.

Both the copy of personal information, supplied by an organization in response, to an access request and any, explanation of codes used by the, organization should be readily, comprehensible. This obligation does not extend to the conversion of, computer language (e.g. machinereadable, instructions, source codes or, object codes) into text. However,, where a code represents a particular, meaning, the personal information, controller must explain the meaning of, that code to the individual. For, example, if the personal information, held by the organization includes the, age range of the individual, and that is, represented by a particular code (e.g.,, "1" means 18-25 years old, "2" means, "26-35 years old, etc.), then when, providing the individual with such a, code, the organization shall explain to, the individual what age range that code, represents.

Where individual requests access to his, or her information, that information, should be provided in the language in, which it is currently held. Where, information is held in a language, different to the language of original, collection, and if the individual, requests the information be provided, in that original language, an, organization should supply the, information in the original language if, the individual pays the cost of, translation.

The details of the procedures by which, the ability to access and correct, information is provided may differ, depending on the nature of the, information and other interests. For, this reason, in certain circumstances, it, may be impossible, impracticable or, unnecessary to change, suppress or, delete records.

Consistent with the fundamental, nature of access, organizations should, always make good faith efforts to, provide access. For example, where, certain information needs to be, protected and can be readily separated, from other information subject to an, access request, the organization should, redact the protected information and, make available the other information., However, in some situations, it may be, necessary for organizations to deny, claims for access and correction, and, this Principle sets out the conditions, that must be met in order for such, denials to be considered acceptable,, which include: situations where claims, would constitute an unreasonable, expense or burden on the personal, information controller, such as when, claims for access are repetitious or, vexatious by nature; cases where, providing the information would, constitute a violation of laws or would, compromise security; or, incidences, where it would be necessary in order to, protect commercial confidential, information that an organization has, taken steps to protect from disclosure,, where disclosure would benefit a, competitor in the marketplace, such as, a particular computer or modeling, program.

“Confidential commercial information”, is information that an organization has, taken steps to protect from disclosure,, where such disclosure would facilitate, a competitor in the market to use or, exploit the information against the, business interest of the organization, causing significant financial loss. The, particular computer program or, business process an organization uses, such as a modeling program, or the, details of that program or business, process may be confidential, commercial information. Where, confidential commercial information, can be readily separated from other, information subject to an access, request, the organization should redact, the confidential commercial, information and make available the, non-confidential information, to the, extent that such information, constitutes personal information of the, individual concerned. Organizations, may deny or limit access to the extent, that it is not practicable to separate the, personal information from the, confidential commercial information, and where granting access would, reveal the organization’s own, confidential commercial information as, defined above, or where it would reveal, the confidential commercial, information of another organization, that is subject to an obligation of, confidentiality.

When an organization denies a request, for access, for the reasons specified, above, such an organization should, provide the individual with an, explanation as to why it has made that, determination and information on how, to challenge that denial. An, organization would not be expected to, provide an explanation in cases where, such explanation would violate a law or, judicial order.

IX. Accountability

32. A personal information controller, should be accountable for complying, with measures that give effect to the, Principles stated above. When, personal information is to be, transferred to another person or, organization, whether domestically, or internationally, the personal, information controller should obtain, the consent of the individual or, exercise due diligence and take, reasonable steps to ensure that the, recipient person or organization will, protect the information consistently, with these Principles.

COMMENTARY: 32. Efficient and cost effective business, models often require information, transfers between different types of, organizations in different locations with, varying relationships. When, transferring information, personal, information controllers should be, accountable for ensuring that the, recipient will protect the information, consistently with these Principles when, not obtaining consent. Thus,, information controllers should take, reasonable steps to ensure the, information is protected, in accordance, with these Principles, after it is, transferred.

There are certain situations where such, due diligence may be impractical or, impossible, for example, when there is, no on-going relationship between the, personal information controller and the, third party to whom the information is, disclosed. In these types of, circumstances, personal information, controllers may choose to use other, means, such as obtaining consent, to, assure that the information is being, protected consistently with these, Principles. However, in cases where, disclosures are required by domestic, law, the personal information controller, would be relieved of any due diligence, or consent obligations.

A useful means for a personal, information controller to help ensure, accountability for the personal information it holds is to have in place a, privacy management programme.⁵⁶

Part. IV. Implementation

33. Part IV provides guidance to member economies on implementing the APEC Privacy, Framework. Section A. focuses on those measures member economies should, consider in implementing the Framework domestically, while Section B sets out, APEC-wide arrangements for the implementation of the Framework's cross-border, elements.

⁵⁶ See clauses 43-45 below.

A. GUIDANCE FOR DOMESTIC IMPLEMENTATION

34. Member economies should have regard to the following basic concept in considering, the adoption of measures designed for domestic implementation of the APEC Privacy, Framework:

I. Maximizing Benefits of Privacy Protections and Information Flows

35. Personal information should be collected, held, processed, used, transferred, and, disclosed in a manner that protects individuals' privacy and allows individuals and, economies to maximize the benefits of information flows within and across borders.

36. Consequently, as part of establishing or reviewing their privacy protections to give, effect to the APEC Privacy Framework, member economies should take all reasonable, and appropriate steps to identify and remove unnecessary barriers to information, flows and avoid the creation of any such barriers.

II. Giving Effect to the APEC Privacy Framework

37. There are several options for giving effect to the Framework and securing privacy protections for individuals including legislative, administrative, industry selfregulatory or a combination of these policy instruments. In practice, the Framework is meant to be implemented in a flexible manner that can accommodate various models of enforcement, including through Privacy Enforcement Authorities, multiagency enforcement bodies, a network of designated industry bodies, courts and tribunals, or a combination of the above, as member economies deem appropriate.

38. The means of giving effect to the Framework will often differ between member economies. An individual member economy may determine that different Information Privacy Principles call for different means of domestic implementation. Whatever approach is adopted in a particular circumstance, the overall goal should be to develop compatible privacy protection approaches in the APEC region that are respectful of individual economies' requirements.

39. APEC economies should adopt non-discriminatory practices in giving effect to the Framework's principles and in protecting individuals from privacy protection violations occurring in that member economy's jurisdiction. [For example, member economies should ensure that laws or other approaches that give effect to the protections in the Framework do not impede individuals living in other economies from benefitting from those protections.

40. Coordination across government agencies and other stakeholders is important to identify ways to strengthen privacy without creating obstacles to national security, public safety, and other public policy objectives.

41. Member economies should consider establishing and maintaining Privacy Enforcement Authorities. Privacy Enforcement Authorities that are established should be provided with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis.

42. Privacy Enforcement Authorities may find it useful to apply a risk-based approach to selected oversight efforts and, where permitted, to prioritize their enforcement efforts according to the likelihood and severity of harm that might result from privacy violations or from an action taken or proposed.⁵⁷

III. Privacy Management Programmes

43. An operative privacy management programme will provide a sound basis for a personal information controller to demonstrate that it is complying with measures that give effect to the privacy protections in the Framework.

44. Accordingly, member economies should consider encouraging personal information controllers to develop and implement privacy management programmes for all personal information under their control. Privacy management programmes should:

- a) be tailored to the structure and scale of the operations of the personal information controller, as well as the volume and sensitivity of the personal information under its control;
- b) provide appropriate safeguards based upon risk assessment that takes into account the potential harm to individuals;
- c) establish mechanisms for internal oversight and response to inquiries and incidents;
- d) be overseen by designated accountable and appropriately trained personnel; and
- e) be monitored and be regularly updated.

45. Personal information controllers should be prepared to demonstrate their privacy management programmes at the request of a competent Privacy Enforcement Authority of that economy or in

⁵⁷ See the Preventing Harm Principle.

response to a valid request by another appropriate entity, such as an accountability agent designated under the CBPR system or under an industry code of conduct giving effect to the Framework.

IV. Promotion of technical measures to protect privacy

46. Technical measures can make a significant contribution to the overall effectiveness and impact of domestic privacy regimes, by supplementing and complementing legal protections of privacy. Therefore, when considering approaches to give effect to the Framework, member economies should promote technical measures which help to protect privacy.

47. Member economies may, for example, encourage personal information controllers to make full use of readily available technical safeguards and measures. In addition, they may promote research and development, encourage further privacy innovation and support the development of technical standards that embed best privacy practice into systems engineering.

V. Public education and communication

48. For the Framework to be of practical effect, it must be known and accessible. Accordingly, member economies should:

a) publicize how their Privacy Laws and other domestic arrangements provide privacy protections to individuals;

b) engage in activities that raise awareness amongst:

i. personal information controllers about the economy's privacy protections and the controllers' responsibilities;

ii. Personal information processors about practices that help provide effective implementation of a personal information controller's privacy obligations related to the processing of personal information; and, iii. individuals about how they can report violations and how remedies can be pursued; and

c) Encourage or require Privacy Enforcement Authorities and other bodies having responsibilities to administer privacy protections established at domestic level (for example, CBPR system accountability agents or bodies established to give effect to self-regulatory schemes) to report publicly on their activities where appropriate.

VI. Cooperation within and between the Public and Private Sectors

49. Active participation of non-governmental entities will help ensure that the full benefits of the Framework can be realized. Accordingly, member economies should engage in a dialogue with

relevant non-government stakeholders, including those representing citizens, consumers and industry and technical and academic communities, to obtain input on privacy protection and information flow issues and to seek cooperation in furthering the Framework's objectives. Furthermore, member economies that have not yet established domestic privacy protection regimes should pay ample attention to the interests and needs of non-government stakeholders when developing privacy protections.

50. Member economies should seek the cooperation of non-governmental entities such as those representing citizens and consumers in raising public awareness about privacy protection issues. As well, member economies should encourage these entities to actively engage in promoting and supporting the privacy interests of individuals, for example by referring complaints to Privacy Enforcement Authorities and publicizing the outcomes of those complaints.

51. Member economies should consider developing strategies that reflect a coordinated approach to implementing privacy protections across governmental bodies.

52. Member economies should also consider undertaking consultation and capacity building efforts across the public and private sectors, and with non-government stakeholders, including, for example, by:

- a) developing or supporting networks of individuals responsible for privacy compliance within organizations; and
- b) producing informational materials and arranging experience sharing events.

VII. Providing for appropriate remedies in situations where privacy protections are violated

53. A member economy's system of privacy protections should include appropriate remedies for privacy violations, which could include redress, the ability to stop a violation from continuing, and other remedies. In determining the range of remedies for privacy violations, member economies should take a number of factors into account including:

- a) the particular system in that member economy for providing privacy protections (e.g., legislative enforcement powers, which may include rights of individuals to pursue legal action, industry self-regulation, or a combination of systems); and
- b) the importance of having a range of remedies commensurate with the extent of the actual or potential harm to individuals resulting from such violations.

54. A member economy should consider encouraging or requiring personal information controllers to provide notice, as appropriate, to Privacy Enforcement Authorities and/or other relevant authorities in the event of a significant security breach affecting personal information under its control. Where it is reasonable to believe that the breach is likely to affect individuals, timely notification directly to affected individuals should be encouraged or required, where feasible and reasonable.

VIII. Mechanism for Reporting Domestic Implementation of the APEC Privacy Framework

55. Member economies should make known to APEC, domestic implementation of the Framework through the completion of and periodic updates to the Individual Action Plan (IAP) on Information Privacy.

B. GUIDANCE FOR INTERNATIONAL IMPLEMENTATION

56. In addressing the international implementation of the APEC Privacy Framework, and consistent with the provisions of Part A, member economies should consider the following points relating to the protection of the privacy of personal information:

I. Information sharing among member economies

57. Member economies are encouraged to share and exchange information, surveys and research in respect of matters that have a significant impact on privacy protection.

58. Member economies are encouraged to educate one another in issues related to privacy protection and to share and exchange information on promotional, educational and training programs for the purpose of raising public awareness and enhancing understanding of the importance of privacy protection and compliance with relevant laws and regulations.

59. Member economies are encouraged to share experiences on various techniques in investigating violations of privacy protections and regulatory strategies in resolving disputes involving such violations including, for instance, complaints handling and alternative dispute resolution mechanisms.

60. Member economies should designate and make known to the other member economies the public authorities within their own jurisdictions that will be responsible for facilitating cross-border cooperation and information sharing between economies in connection with privacy protection.

61. Member economies should encourage the development of internationally comparable metrics to inform the policy making process relating to privacy and personal information flows.

II. Cross-border cooperation in investigation and enforcement

62. Taking into consideration existing international arrangements (including the CPEA) and existing or developing self-regulatory or co-regulatory approaches, and to the extent permitted by domestic law and policy, member economies should expand their use of existing cooperative arrangements and consider developing additional cooperative arrangements or procedures, as necessary, to facilitate cross-border cooperation in the enforcement of privacy laws. Such cooperative arrangements may take the form of bilateral or multilateral arrangements.

63. The preceding paragraph is to be construed with regard to the right of member economies to decline or limit cooperation on particular investigations or matters on the ground that compliance with a request for cooperation would be inconsistent with domestic laws, policies or priorities, or on the ground of resource constraints, or based on the absence of a mutual interest in the investigations in question.

64. In civil enforcement of privacy laws, cooperative cross-border arrangements may include the following aspects:

a) mechanisms for promptly, systematically and efficiently notifying designated public authorities in other member economies of investigations or privacy enforcement initiatives that target conduct that is inconsistent with the protections set forth in the Framework and that may affect individuals or personal information controllers in those other economies;

b) mechanisms for effectively sharing information necessary for successful cooperation in cross-border privacy investigation and enforcement cases;

c) mechanisms for investigative assistance in privacy enforcement cases;

d) mechanisms to prioritize cases for cooperation with public authorities in other economies based on the severity of the unlawful infringements of privacy, the actual or potential harm involved, as well as other relevant considerations;

e) steps to maintain the appropriate level of confidentiality in respect of information exchanged under the cooperative arrangements.

III. Cross-border privacy mechanisms

65. APEC recognized the importance of protecting privacy while maintaining the free flow of personal information across borders and has encouraged member economies to implement the Framework to

provide conditions in which information can flow safely and accountably, for instance through the use of the CBPR system.

66. Member economies will endeavor to support the development and recognition or acceptance of cross-border privacy mechanisms for use by organizations to transfer personal information across the APEC region, recognizing that organizations would still be responsible for complying with the local privacy requirements, as well as with all applicable laws. Such mechanisms should apply the APEC Information Privacy Principles.

67. To give effect to paragraph 65, member economies have developed the CBPR system⁵⁸, which provides a practical mechanism for participating economies to implement the APEC Privacy Framework in an international, cross-border context, and to provide a means for organizations to transfer personal information across borders in a manner in which individuals may trust that the privacy of their personal information is protected.

68. Member economies worked with appropriate stakeholders to develop the PRP system to complement the CBPR system to help personal information processors demonstrate their ability to provide effective implementation of a personal information controller's obligations related to the processing of personal information.

IV. Cross-border transfers

69. A member economy should refrain⁵⁹ from restricting cross border flows of personal information between itself and another member economy where (a) the other economy has in place legislative or regulatory instruments that give effect to the Framework or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures (such as the CBPR) put in place by the personal information controller to ensure a continuing level of protection consistent with the Framework and the laws or policies that implement it.

70. Any restrictions to cross border flows of personal information should be proportionate to the risks presented by the transfer, taking into account the sensitivity of the information, and the purpose and context of the cross border transfer.

⁵⁸ The 2011 Leaders Declaration states "We will take the following steps to further open markets and, facilitate regional trade: [...] implement the APEC CBPR to reduce barriers to information flows, enhance, consumer privacy, and promote interoperability across regional data privacy regimes.", (http://www.apec.org/Meeting-Papers/Leaders-Declarations/2011/2011_aelm.aspx)

⁵⁹ Cross border data flows remain subject to member economies applicable domestic laws, regulations, and, international agreements and commitments.

V. Interoperability between privacy frameworks

71. Recognizing that personal information flows do not stop at regional boundaries, member economies should encourage and support the development of international arrangements that promote interoperability amongst privacy instruments that give practical effect to this Framework.

72. Improving the global interoperability of privacy frameworks can bring benefits in improved personal information flows, help ensure that privacy requirements are maintained when personal information flows beyond member economies and can simplify compliance for personal information controllers and processors. Global interoperability can also assist individuals to assert their privacy rights in a global environment and help authorities to improve cross-border privacy enforcement.

OECD Declaration on Government Access to Personal Data Held by Private Sector Entities

Declaration on Government Access to Personal Data held by Private Sector Entities

WE THE MINISTERS AND REPRESENTATIVES OF Australia, Austria, Belgium, Canada, Chile, Colombia, Costa Rica, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Türkiye, the United Kingdom, the United States, and the European Union, met in the Island of Gran Canaria in Spain, on 14-15 December 2022, under the leadership of Spain as Ministerial Chair and with Denmark, Japan, Türkiye, the United Kingdom and the United States as Vice-Chairs, for the meeting of the Committee on Digital Economy Policy (CDEP) at Ministerial level under the theme “driving long-term recovery and economic growth by building a trusted, sustainable, and inclusive digital future”.

Legitimate government access on the basis of common values

WE RECALL our shared commitment to upholding democracy and the rule of law, protecting privacy and other human rights and freedoms, promoting data free flow with trust in the digital economy, and maintaining a global, open, accessible, interconnected, interoperable, reliable and secure Internet.

WE RECOGNISE that ongoing digital transformation is creating more data, including personal data, as digital technologies are used across all sectors of the global economy.

WE FURTHER RECOGNISE the central role of data in the functioning of our societies and economies, and that cross-border data flows underpin international trade and global commerce and economic co-operation and development; greatly contribute to innovation and research and development across sectors; and are necessary to conduct business and to advance economic and societal goals.

WE RECALL the 1980 Recommendation concerning OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, last revised in 2013 [OECD/LEGAL/0188] (hereafter, “OECD Privacy Guidelines”), which provides a basic common reference point for the protection of personal data, whether in the public or private sector, and promotes and facilitates the transborder flows of personal data while upholding democratic values, the rule of law and the protection of privacy and other human rights and freedoms.

WE RECOGNISE the sovereign duty and responsibility of every country to protect the safety of its population by preventing, detecting and confronting criminal activity and threats to public order and national security, in adherence to democratic values, the rule of law, and the protection of privacy and other human rights and freedoms.

WE ACKNOWLEDGE that government access to personal data held by private sector entities is recognised in our national legal frameworks as essential to meeting these sovereign duties and responsibilities, and that law enforcement and national security authorities are therefore vested with powers to lawfully access such data.

WE REJECT any approach to government access to personal data held by private sector entities that, regardless of the context, is inconsistent with democratic values and the rule of law, and is unconstrained, unreasonable, arbitrary or disproportionate. Such approaches violate privacy and other human rights and freedoms, breach international obligations, undermine trust and create a serious impediment to data flows to the detriment of the global economy. By contrast, our countries' approach to government access is in accordance with democratic values; safeguards for privacy and other human rights and freedoms; and the rule of law including an independent judiciary. These protections also contribute to promoting trust by private sector entities in meeting their responsibilities in this context.

WE EMPHASISE, taking into account the justified exceptions to the OECD Privacy Guidelines on grounds of law enforcement and national security, the importance of enhancing trust based on a common understanding of the protections that our countries apply when accessing personal data held by private sector entities in these circumstances.

WE RECOGNISE that our existing practices and safeguards, in this regard, while not identical to one another, are founded upon similar principles that reflect a shared commitment to protecting privacy and other human rights and freedoms.

WE NOTE stakeholders' calls for additional work and engagement to identify existing common safeguards in OECD Member countries to protect privacy and freedom of expression, and therefore promote trust, in the context of purchasing commercially available personal data, accessing publicly available personal data, and receiving voluntary disclosures of personal data by law enforcement and national security authorities.

WE REITERATE our ambition to build a shared understanding among like-minded democracies of protections for privacy and other human rights and freedoms in place for law enforcement and

national security access to personal data held by private sector entities in order to better inform efforts to promote data free flow with trust.

Promoting trust in cross-border data flows

WE REAFFIRM our commitment to data free flow with trust as a means of providing confidence to individuals and businesses when transferring personal data internationally.

WE REGARD the below principles as an important expression of our shared democratic values and commitment to the rule of law, which distinguishes our countries from other countries whose law enforcement or national security access to personal data are inconsistent with democratic values and the rule of law, are unconstrained, unreasonable, arbitrary or disproportionate, or amount to violations of human rights.

WE RECOGNISE that where our legal frameworks require that transborder data flows are subject to safeguards, our countries take into account a destination country's effective implementation of the principles as a positive contribution towards facilitating transborder data flows in the application of those rules.

Principles for government access to personal data held by private sector entities

WE DECLARE the following shared principles as reflecting commonalities drawn from OECD Members' existing laws and practices. These principles:

- complement each other in protecting privacy and other human rights and freedoms;
- apply to government access to and processing of personal data in the possession or control of private sector entities when governments are pursuing law enforcement and national security purposes within their respective territories in accordance with their national legal framework, including situations where countries have the authority under their national legal framework to mandate that private sector entities provide data to the government when the private sector entity or data are not located within their territory (hereafter referred to as "government access");
- are interpreted subject to national legal frameworks and may be applied by countries in different manners, depending on the specific context and circumstances, such as the type of access sought;
- should be read in light of the following definitions:

a) "Personal data" refers to any information relating to an identified or identifiable individual.

b) "Legal framework" for government access to personal data refers to national laws, executive or judicial orders, administrative regulations, case law, and other legally binding instruments or

requirements, including legal obligations arising from international and supranational law as applicable in the country.

c)“Private sector entities” refers to individuals and any non-governmental for-profit and not-for-profit organisations.

These principles are:

I. Legal basis

Government access to personal data held by private sector entities is provided for and regulated by the country’s legal framework, which is binding on government authorities and is adopted and implemented by democratically established institutions operating under the rule of law. The legal framework sets out purposes, conditions, limitations and safeguards concerning government access, so that individuals have sufficient guarantees against the risk of misuse and abuse.

II. Legitimate aims

Government access supports the pursuit of specified and legitimate aims. Governments seek access only for such aims, in conformity with the rule of law. Government access is carried out in a manner that is not excessive in relation to the legitimate aims and in accordance with legal standards of necessity, proportionality, reasonableness and other standards that protect against the risk of misuse and abuse, as set out in and interpreted within the country’s legal framework.

Governments do not seek access to personal data for the purpose of suppressing or burdening criticism or dissent; or disadvantaging persons or groups solely on the basis of characteristics including, but not limited to: age, mental or physical disability, ethnicity, indigenous status, gender identity or expression, sexual orientation, or political or religious affiliation.

III. Approvals

Prior approval (“approval”) requirements for government access are established in the legal framework to ensure that access is conducted in accordance with applicable standards, rules and processes. They are commensurate with the degree of interference with privacy and other human rights and freedoms that will occur as a result of government access. Such requirements specify the criteria for seeking and granting approval, the procedure to be followed, and the entity providing the approval.

Stricter approval requirements are in place for cases of more serious interference, and may include seeking approval from judicial or impartial non-judicial authorities. Emergency exceptions to

approval requirements are provided for in the legal framework, and are clearly defined, including justifications, conditions, and duration.

Decisions on approvals are appropriately documented. They are made objectively, on a factual basis in pursuit of a specified and legitimate aim and upon satisfaction that the approval requirements are met.

In situations where approval is not required, other safeguards established in the legal framework apply to protect against misuse and abuse, including clear rules that impose conditions or limitations on the access, as well as effective oversight.

IV. Data handling

Personal data acquired through government access can be processed and handled only by authorised personnel. Such processing and handling is subject to requirements provided for in the legal framework that include putting in place physical, technical and administrative measures to maintain privacy, security, confidentiality, and integrity. They also include mechanisms to ensure that personal data are processed lawfully, are retained only for as long as authorised in the legal framework in view of the purpose and taking into account the sensitivity of the data, and are kept accurate and up to date to the extent appropriate having regard to the context.

Internal controls are put in place to detect, prevent and remedy data loss or unauthorised or accidental data access, destruction, use, modification, or disclosure, and to report such instances to oversight bodies.

V. Transparency

The general legal framework for government access is clear and easily accessible to the public so that individuals are able to consider the potential impact of government access on their privacy and other human rights and freedoms.

Mechanisms exist for providing transparency about government access to personal data that balance the interest of individuals and the public to be informed with the need to prevent the disclosure of information that would harm national security or law enforcement activities.

These mechanisms include public reporting by oversight bodies on government compliance with legal requirements as well as procedures for requesting access to government records. Other measures include, for instance, regular reporting by governments and, where applicable, individual notification.

Private sector entities are allowed to issue aggregate statistical reports regarding government access requests in conformity with the legal framework.

VI. Oversight

Mechanisms exist for effective and impartial oversight to ensure that government access complies with the legal framework.

Oversight is provided through bodies including internal compliance offices, courts, parliamentary or legislative committees and independent administrative authorities.

Countries' oversight systems are comprised of such bodies acting according to their individual mandates and that have powers that include the ability to obtain and review relevant information, conduct investigations or inquiries, execute audits, engage with government entities on compliance and mitigation, and address non-compliance. In addition, such bodies receive and respond to reports of non-compliance to ensure that government entities are accountable, and may also exercise redress functions in response to individuals' complaints.

In the exercise of their functions, oversight bodies are protected from interference and have the financial, human and technical resources to effectively carry out their mandate. They document their findings, produce reports, and make recommendations, which are made publicly available to the greatest extent possible.

VII. Redress

The legal framework provides individuals with effective judicial and non-judicial redress to identify and remedy violations of the national legal framework.

Such redress mechanisms take into account the need to preserve confidentiality of national security and law enforcement activities. This may include limitations on the ability to inform individuals whether their data were accessed or whether a violation occurred.

Available remedies include, subject to applicable conditions, terminating access, deleting improperly accessed or retained data, restoring the integrity of data and the cessation of unlawful processing. They may also include, depending on the circumstances, compensation for damages suffered by an individual.

WE WELCOME the work of the OECD on data free flow with trust and WE CALL on the Organisation to support countries in their promotion of this Declaration.

Background information

The Declaration on Government Access to Personal Data Held by Private Sector Entities was adopted by Ministers and high-level representatives of OECD Members and the European Union on 14 December 2022, on the occasion of the Ministerial meeting of the Committee on Digital Economy Policy (CDEP) held in the island of Gran Canaria, Spain.

As the first intergovernmental agreement on common approaches to safeguard privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes, it seeks to promote trust in cross-border data flows, a critical enabler of the global economy.

OECD work on cross-border data flows

The review of the implementation of the 1980 Recommendation concerning OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [OECD/LEGAL/0188], completed in 2021, identified policy gaps affecting the cross-border flow of personal data, which are essential for business transactions and operations as well as for social interactions online. A critical gap identified was the lack of a common articulation at the international level of the safeguards that countries put in place to protect privacy and other human rights and freedoms when they access personal data held by private entities in the course of fulfilling their sovereign responsibilities related to national security and law enforcement.

The importance of such an articulation is two-fold: i) increase trust among rule-of-law democratic systems that, while not identical, share significant commonalities in order to support cross-border flows of personal data between them; ii) and provide a standard for how democratic, rule-of-law based systems limit and constrain government power in contrast with approaches that are unconstrained, unreasonable, arbitrary or disproportionate, in violation of human rights and in breach of international obligations.

Process for developing the Declaration

The CDEP began work on this topic in February 2021 following discussions at its November 2020 meeting and building on prior work and discussions of the Working Party on Data Governance and Privacy (WPDGP) in the context of the Report on implementation, dissemination and continued relevance of the Privacy Guidelines [C(2021)42].

To this end, an informal drafting group of experts, ultimately consisting of experts from 33 OECD Members and the European Union, was convened. The drafting group met 18 times in 2021-2022. Drawing on these sessions, expert and stakeholder input and two fact-finding surveys, the OECD

identified seven common principles that reflect OECD Members' existing laws and practices, and are at the heart of this Declaration.

Scope of the Declaration

The Declaration consists of three main sections:

1. "Legitimate government access on the basis of common values," recognising the important role data transfers play in the global economy and recalling the rationale for government access to personal data, the importance of safeguards to protect privacy and other human rights and freedoms, and the existence of commonalities between OECD Members in this regard;
2. "Promoting trust in cross-border data flows," reaffirming countries' commitment to data free flow with trust, considering the principles in section three of the Declaration as an expression of their democratic values, and recognising their effective implementation by a destination country as a positive contribution towards facilitating cross-border data flows;
3. "Principles for government access to personal data held by private sector entities," listing seven principles which reflect commonalities across OECD Members based on their existing laws and practices, and complement each other in protecting privacy and other human rights and freedoms: legal basis; legitimate aims; approvals; data handling; transparency; oversight; redress. This section further includes definition and scope for the application of these principles.

BİBLİYOGRAFYA

Çalışmalar yayım yılı içerisinde alfabetik olarak sıralanmıştır. Bu alanı güncel tutmak için önerilerinizi bekleriz.

Kitap

2004

- Nilgün Başalp (2004) *Kişisel Verilerin Korunması ve Saklanması*, Yetkin.

2006

- Leyla Keser Berber, Murat Lostar (2006) *Bilişimde Biyometrik Yöntemler*, Yetkin.

2008

- Oğuz Şimşek (2008) *Anayasa Hukukunda Kişisel Verilerin Korunması*, Beta.

2009

- Hayrunnisa Özdemir (2009) *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*, Seçkin.
- Leyla Keser Berber, Mahir Ülgü, Cüneyd Er (2009) *Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği*, Karakter Color.

2010

- Hüseyin Can Aksoy (2010) *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, Çakmak.
- İkbâl Gür (2010) *Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları*, Turhan.

2013

- Hale Akdağ (2013) *Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, Adalet.
- Zeki Okur (2013) *İş Hukukunda Elektronik Gözetleme*, Legal.

2014

- İbrahim Gül, İsmail Alagöz (2014) *Kişisel Verilerin Korunmasına Yönelik İhlalleri ve Uluslararası Düzenlemeler*, Seçkin.

- Leyla Keser (2014) *Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması*, On İki Levha.

2015

- Sedat Erdem Aydın (2015) *AİHM İctihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu*, On İki Levha.
- Türkay Henkoğlu (2015) *Bilgi Güvenliği ve Kişisel Verilerin Korunması*, Yetkin.
- Mine Kaya (2015) *Elektronik Ortamda Kişilik Hakkının Korunması*, Seçkin.

2016

- Armağan Ebru Bozkurt Yüksel (2016) *Bulut Bilişimde Kişisel Verilerin Korunması*, Yetkin.
- Aydın Akgül (2016) *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, Beta.
- İlke Gürsel (2016) *İşçinin Kişisel Verilerinin Korunması Hakkı*, Adalet.

2017

- Canan Erdoğan (2017) *Kişilik Hakkı Kapsamında İşçilerin İzlenmesi ve Gözetlenmesi*, Yetkin Yayınları.
- Eren Sözüer (2017) *Unutulma Hakkı-İnsan Hakları Hukuku Perspektifinden Bir İnceleme*, On İki Levha.
- Furkan Güven Taştan (2017) *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, 2. Baskı, On İki Levha.
- Hüseyin Murat Develioğlu (2017) *6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku*, On İki Levha Yayıncılık.

2018

- Erbil Beytar (2018) *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, On İki Levha.
- Selen Uncular (2018) *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, 2. Baskı, Seçkin.
- Şehriban İpek Aşıkoğlu (2018) *Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri*, On İki Levha.
- Zafer Babür (2018) *Donanım, Yazılım, Lisans, Hizmet BT Sözleşmeleri Bulut – Kişisel Verilerin Korunması – GDPR – Siber Sigorta Ekleri*, Seçkin.

2019

- Ceren Yakışır (2019) *Türk Ceza Kanunu'nda Kişisel Verilerin Basın Yayın Yoluyla Açıklanması Suçu*, On İki Levha.

- Çiğdem Ayözger (2019) *Kişisel Verilerin Korunması: Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil*, 2. Baskı, Beta.
- İbrahim Korkmaz (2019) *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, 2. Baskı, Seçkin.
- Kerem Aydın, H. Gökçe Üstündağ (2019) *Kişisel Verilerin Korunması Kanunu ve İşletmeler*, Karahan Kitapevi.
- Remzi Demir (2019) *Hukuksal Yönleriyle İnsan Geni Üzerindeki İncelemeler*, Seçkin.
- S. Hilal Üçüncü (2019) *Medeni Yargılama Hukukunda Kişisel Verilerin ve Sırların Korunması*, On İki Levha.
- Şeyma Sert (2019) *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, Seçkin.
- Zeynel T. Kangal (2019) *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, On İki Levha.

2020

- Abdülhamid Zor (2020) *Veri Sorumlusunun Yükümlülükleri ve Bu Yükümlülükleri İhlalinden Doğan Özel Hukuk Sorumluluğu*, On İki Levha.
- Armağan Ebru Bozkurt Yüksel (2020) *Sokak Fotoğrafçılığı ve Kişisel Verilerin Korunması*, Aristo.
- Begüm Gürel, Berfin Helin Bulgurcu (2020) *Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı*, Platon Hukuk.
- Beşir Orak (2020) *Kişisel Sağlık Verilerinin Korunması*, Yetkin.
- Can Yavuz (2020) *İnternetteki Arama Sonuçlarından Kişisel Verilerin Kaldırılması: Unutulma Hakkı*, 3. Baskı, Seçkin.
- Canan İmançlı (2020) *Kişisel Sağlık Verilerinin Korun(a)mamasından Doğan Özel Hukuk Sorumluluğu*, On İki Levha.
- Cemal Başar (2020) *Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması*, On İki Levha.
- Cengiz Apaydın (2020) *Cevap ve Düzeltme Hakkı-İnternette Erişimin Engellenmesi-Unutulma Hakkı*, Seçkin.
- Elif Küzeci (2020) *Kişisel Verilerin Korunması*, 4. Baskı, On İki Levha.
- Emine Hizarci (2020) *6698 Sayılı Kişisel Verilerin Korunması Kanununun AB Veri Koruma Hukuku Işığında Değerlendirilmesi*, Yetkin.
- Esra Demir (2020) *Ceza Muhakemesi Hukukunda Moleküler Genetik İncelemeler*, Seçkin.
- Eşref Barış Börekçi (2020) *Kişisel Verileri Verme, Yayma veya Ele Geçirme Suçu (TCK m. 136)*, On İki Levha.
- Göknül Özcan (2020) *Bankacılık İş ve İşlemlerinde Kişisel Verilerin Korunması*, On İki Levha.

- Hamza Bayındır (2020) *Özel Sağlık Kurumları Kapsamında Kişisel Sağlık Verilerinin İşlenmesi ve Korunması*, On İki Levha.
- İbrahim Gül, İsmail Alagöz (2020) *Kişisel Verilerin Korunmasına Yönelik İhlalleri ve Uluslararası Düzenlemeler*, Yargı.
- İsmail Şahin (2020) *Kişisel Verilerin Korunması Kanunu*, Yetkin.
- Mehmet Bedii Kaya (2020) *Elektronik Ticaret Hukuku: Ticari Elektronik İletiler*, 2. Baskı, On İki Levha.
- Mesut Serdar Çekin (2020) *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu*, 3. Baskı, On İki Levha.
- Mine Demirezen (2020) *Kişisel Verilerin Korunması Hukuku ve Uyum Projelerinin Yürütülmesi*, Platon Hukuk.
- Muhammet Sefa Mutlu (2020) *Kişisel Verilerin Soruşturma Evresinde İşlenmesi ve İnsan Hakları Kapsamında Korunması*, Adalet.
- Murat Altındere (2020) *Kişisel Verilerin Korunması Hukuku ve Uygulaması*, Adalet.
- Murat Volkan Dülger (2020) *Kişisel Verilerin Korunması Hukuku*, 3. Baskı, Hukuk Akademisi.
- Mustafa Alkan, Turhan Menteş, Mehmet Ali İnceefe (2020) *Kişisel Verileri Koruma El Kitabı*, Nobel Akademik Yayıncılık.
- Nazlı Elbir (2020) *Kişiliğin Korunması Bağlamında İşçiye Ait Kişisel Verilerin Korunması*, Yetkin.
- Oğulcan Özkan (2020) *Kişisel Verilerin Korunması*, Yetkin.
- Ramazan Özkepir, Salih Zeki Kocaman, Erkal Hilmi Kart (2020) *Sosyal Medya ve Basın Hukuku*, Seçkin.
- Sevgi Eraslan (2020) *Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller*, 2. Baskı, On İki Levha.
- Sezen Kama Işık (2020) *Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış*, On İki Levha.
- Sinan Sami Akkurt (2020) *Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması*, 2. Baskı, Seçkin.
- Sinem Göçmen Uyarer (2020) *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, 2. Baskı, Seçkin.
- Sinem Göçmen Uyarer (2020) *Kişisel Verilerin Korunması*, 2. Baskı, Seçkin.
- Soner Hamza Çetin (2020) *Türk Ceza Hukuku'nda Elektronik İzleme*, Adalet.
- Süleyman Yılmaz- Gökçe Filiz Çavuşoğlu (2020) *Kişisel Verileri Koruma Hukuku*, Yetkin.
- Yusuf Mansur Özer (2020) *Kişisel Verilerin Korunmasında Blok Zinciri Modeli: Vaatler ve Hukuki Engeller*, On İki Levha.

2021

- Alaattin Bük (2021) *Bilişim Alanında Kişisel Verilerin Korunması*, Yetkin.
- Arzu Kalyon (2021) *Türk Vergi Hukukunda Kişisel Verilerin Korunması*, Seçkin.
- Bahri Öztürk, Elif Altınok Çalışkan, Serkan Seyhan (2021) *Kişisel Verilerin Korunması Hukuku*, Seçkin.
- Başak Ozan Özparlak (2021) *Büyük Veri Çağında Yapay Zekâ Sistemlerinin Çalışma İlişkilerinde Kullanımı: Hukuki Bir Değerlendirme*, On İki Levha.
- Beste Ekin (2021) *Kişisel Verilerin Korunması ve Rekabet Hukuku Boyutuyla Büyük Veri*, On İki Levha.
- Bilal Toprak (2021) *KVKK ve GVKT Açısından İşçinin Kişisel Verilerinin Korunması*, Yetkin.
- Bülent Öz (2021) *KVKK Kişisel Verileri Koruma Kanunu Mevzuatı ve Örnek Uygulamaları*, 2. Baskı, Ekin Kitabevi Yayınları.
- Cihan Avcı Braun (2021) *Kişisel Verilerin Korunmasında Hukuki Sorunlar*, Legal.
- Demet Çelik Ulusoy (2021) *Kuzey Kıbrıs Türk Cumhuriyeti'nde Kişisel Verilerin Korunması Hukuku*, Yetkin.
- Dilara Tekinoğlu (2021) *Kişisel Verilerin Korunması Hukuku Açısından Mobil Uygulamalarda Konum Gizliliği*, On İki Levha.
- Elif Sinem Kabadayı (2021) *Unutulma Hakkı*, Yetkin.
- Elif Yıldız (2021) *Kişisel Verilerin Korunması Hukuku*, Bilge Yayınevi.
- Enes Şahin, Özge Demirdelen, Şevval Ceyhan (2021) *KVKK Alanında Uygulamalar*, Bilge.
- Esra Tepe (2021) *Kişisel Verilerin Korunması*, Adalet.
- Ezgi Hakalmaz (2021) *Hekimlik Sözleşmesi Bağlamında Kişisel Sağlık Verilerinin İşlenmesi ve Korunması*, On İki Levha.
- Gökçe Filiz Çavuşoğlu (2021) *Kişisel Verilerin Yapay Zekâyla İşlenmesinden Doğan Özel Hukuk Sorunları*, Yetkin.
- Habip Bozkurt (2021) *Kişisel Verilerin İşlenmesinin Hukuki Boyutu*, Yetkin.
- Halil Altındağ (2021) *Kişisel Verileri Koruma Kurulu Tarafından Verilen İdari Para Cezaları*, Adalet.
- Hande Seven (2021) *Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu (TCK M.136)*, Yetkin.
- İlknur Deniz (2021) *Çocuklara Ait Kişisel Verilerin Türk Medeni Kanunu ve Kişisel Verilerin Korunması Kanunu Kapsamında Korunması*, Seçkin.
- İslam Safa Kaya, Yüksel Tolun (2021) *Türkiye'de, Avrupa'da ve California'da Kişisel Verilerin İşlenmesi*, Adalet.

- Lothar Determann (2021) *Kişisel Verilerin Korunması Uygulama Kılavuzu*, (Hilal Temel, Çev.) 2. Baskı, On İki Levha.
- Mahmut Koca, Ramazan Çağlayan, Rıza Saka (2021) *Kişisel Verilerin İmhası*, Seçkin.
- Mehmet Maden (2021) *Ceza Hukukunda Kişisel Verilerin Korunması*, Adalet.
- Melike Köse Aysun (2021) *Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)*, Seçkin.
- Merve Ezgi Hisli (2021) *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, Platon Hukuk.
- Metin Turan (2021) *Karşılaştırmalı Hukukta Kişisel Verilerin Korunması*, 4. Baskı, Seçkin.
- Muhammed Alparslan Budak, Seda Malkoç (2021) *Kişisel Verilerin Korunması Kanunu'na Aykırı Davranılmasında Hukuki Sorumluluk*, Adalet.
- Muhammet Özekes (Ed.), *Covid-19 Salgınının Hukuki Boyutu*, 2. Baskı, On İki Levha.
- Nazlı Töre (2021) *Milletlerarası Hukukta Mülteci Verilerinin Korunması*, Turhan.
- Neslihan Can (2021) *Kolluk ve Adli Makamlar Tarafından İşlenen Kişisel Verilerin Korunması*, On İki Levha.
- Nur Buğçe Bakirel (2021) *Veri Sorumlusu ve Veri İşleyen Arasındaki Sorumluluk Paylaşımı*, Seçkin.
- Onur Baskın (2021) *Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması*, Seçkin.
- Onur Korucu (2021) *Veri Güvenliğinin İyileştirilmesi Sürecinde Küresel Standart, Çerçeve ve En İyi Uygulamaların Hukuki Uyuma Desteği*, Adalet.
- Ozan Selek (2021) *Kişisel Verilerin Korunması ve Verileri Yok Etmeme Suçu (TCK m.138)*, On İki Levha.
- Pınar Bacaksız (2021) *Kişisel Sağlık Verilerinin Korunması ve Covid-19 Süreci*
- Rüya Tuna Toparlık (2021) *Veri Korunması Hukukunda Bağlayıcı Şirket Kuralları: 2016/679 Sayılı Genel Veri Koruma Tüzüğü ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu Karşılaştırması*, On İki Levha.
- Sabire Senem Yılmaz (2021) *Tıp Alanında Kişisel Verilerin Açıklanması Suçu*, 5. Baskı, Seçkin.
- Şermin Birtane, Fatih Alkan, Ali Kozan, Ferhat Yıldız, Hilal Yazıcı, Çağlar Öncel, Taylan Barın (2021) *Özel Hayata ve Aile Hayatına Saygı Hakkı Karar Özetleri*, Anayasa Mahkemesi.
- Yonca Dursun (2021) *6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Korunması*, Seçkin.

2022

- Ayşe Elif Kaya (2022) *Rethinking the Right of Withdrawal Under the GDPR in the Context of Biobank Research*, On İki Levha.
- Ayşe Yasemin Aydoğmuş Gisoldi (2022) *Milletlerarası Özel Hukukta Kişisel Verilerin Korunması*, On İki Levha.

- Bahri Öztürk, Elif Altınok Çalışkan, Serkan Seyhan (2022) *Kişisel Verilerin Korunması Hukuku*, 2. Baskı, Seçkin.
- Bayram Doğan (2022) *Kişisel Verilerin Korunması Hakkı*, Adalet.
- Bekir Gürses (2022) *AB ve Türk Hukukunda Kişisel Verilerin Korunması Mevzuat Uyumuna Yönelik Bir Değerlendirme*, Platon Hukuk.
- Berrak Yılmaz (2022) *Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, Yetkin.
- Ece Taşçı Aydemir (2022) *Kişisel Verilerin Kaydedilmesi Suçu*, Seçkin.
- Elif Beyza Akkanat Öztürk (2022) *Karşı Edim Olarak Kişisel Veriler*, On İki Levha.
- Emin Hamdi Uysal, Bilal Karagöz (2022) *Tüm Dokümanlarla KVKK Uyum Süreci*, 2. Baskı, Seçkin.
- Esra Yiğit (2022) *İş İlişkisinde Kişisel Verilerin Korunması*, On İki Levha.
- Fatma Koç (2022) *İş İlişkisinde Kişisel Sağlık Verilerinin İşlenmesi*, On İki Levha.
- Irmak Erdoğan (2022) *Yapay Zeka ve Profilleme Teknolojilerinin Ceza Muhakemesinde Kişisel Veri İşlenmesine Etkileri*, Seçkin.
- Işıl Çelik (2022) *6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Kişisel Verilerin Yurt Dışına Aktarılması*, On İki Levha.
- İslam Safa Kaya (2022) *Türkiye’de, Avrupa’da ve California’da Kişisel Verilerin İşlenmesi*, 2. Baskı, Adalet.
- Mehmet Akçakoca (2022) *Tıp Ceza Hukukunda Kişisel Verilerin Korunması*, Adalet.
- Mehmet Şükrü Gündüz (2022) *Uluslararası İnsan Hakları Açısından Kişisel Veri Güvenliği*, Adalet.
- Mustafa Baysal (2022) *KVKK Kişisel Verilerin Korunması Kanunu El Kitabı*, On İki Levha.
- Osman Gazi Güçlütürk (2022) *Yapay Zeka ve Verinin Kullanımı*, On İki Levha.
- Pınar Nur (2022) *Vergi Hukuku Açısından Kişisel Verilerin Korunması*, On İki Levha.
- Senem Ovalıoğlu Seyis (2022) *Avrupa Birliği Hukukunda Kişisel Verilerin Korunması*, On İki Levha.
- Serdar Çelikel (2022) *Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri*, Seçkin.
- Türkan Pelin Uzun (2022) *Sağlık Hizmetlerinde Kişisel Verilerin Korunması*, Turhan.
- Umut Emre Yağlıdere (2022) *KVKK Kapsamında Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme*, Platon Hukuk.

2023

- Beste Yılmaz (2023) *Kişisel Verilerin Korunması ve Rekabet Hukuku Bağlamında Veri Taşınabilirliği Hakkı*, On İki Levha.

- Çağla Tansuğ (2023) *İdari Faaliyetlerde İşlenen Kişisel Verilerin İdare Tarafından Korunması*, On İki Levha.
- Ezgi Sivrikaya (2023) *Gözetim Toplumu Çağında Çocukların Kişisel Verilerine Mahremiyet Hakkı Kapsamında Karşılaştırmalı Bir Bakış*, Yetkin.
- Mustafa Serdar Çekin, Ahmet Esad Berktaş, Muhammed Furkan Akıncı (2023) *Veri Hukuku*, On İki Levha.
- Özge Nefise Kaya (2023) *Kişisel Verilerin Korunması Kapsamında Hasta ve Hasta Yakınlarına Gerçeğin Söylenmesi*, Seçkin.
- Ramazan Furkan Kaya (2023) *Kişisel Verilerin Korunması Hukukunda Ticari Elektronik İletiler*, Adalet.
- Yonca Dursun (2023) *Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Korunması*, Seçkin.

Kitap Bölümleri

2009

- Hüseyin Can Aksoy (2009) *Kişisel Verilerin İşlenmesi Kapsamında Rıza Unsuru ve Sınırlı Ehliyetsizlerin Durumu*, Halûk Konuralp Anısına Armağan, Cilt 3, s. 47-67.

2011

- Zeki Okur (2011) *Türk İş Hukukunda İşçinin Kişisel Verilerinin Korunması Hakkı*, İş Dünyası ve Hukuk-Prof. Dr. Tankut Centel'e Armağan, s. 368-408, İstanbul Üniversitesi Hukuk Fakültesi Yayınları.

2016

- Tuğba Cengiz (2016) *Uluslararası Düzenlemelerde ve Türkiye'de Kişisel Verilerin Korunması*, Peschke/Lutz, Peschke/Seldağ Güneş (Editör) *New Media and Law: A Comparative Study* Yeni Medya ve Hukuk: Karşılaştırmalı Bir Çalışma, Yetkin.

2017

- Mehmet Bedii Kaya (2017) *Büyük Verinin Hukuki Boyutları*, Şeref Sağıroğlu, Orhan Koç (Editör) *Büyük Veri ve Açık Veri Analitiği: Yöntemler ve Uygulamalar*, s. 142-152, Grafiker.
- Alper Oturaklı (2017) *Kişisel Verilerin Korunması Mevzuatı ve Sigorta Sektörü Uygulamaları*, Sigorta Hukukunun Bazı Güncel Sorunları, s. 11-28, On İki Levha.

2020

- Cüneyt Pekmez (2020) *Alman Karayolları Trafik Kanunu'nda 20. 06. 2017'de Yapılan Değişiklikler Çerçevesinde Otonomlaştırılmış Araçlardan Elde Edilen Kişisel Verilerin Korunması*, Sanem Aksoy Dursun, Arzu Genç Arıdemir (Editör) *Kişilik Haklarına İlişkin Güncel Sorunlar*, On İki Levha.
- Emine Hizarcı (2020) *6698 Sayılı Kişisel Verilerin Korunması Kanununun AB Veri Koruma Hukuku Işığında Değerlendirilmesi*, Yetkin.

2021

- E. Eylem Aksoy Retornaz, Osman Gazi Güçlütürk (2021) *Yapay Zekanın Kişisel Veri Kavramı ve Kişisel Verilerin İşlenmesinde Temel İlkelerle İlişkisi*, E. Eylem Aksoy Retornaz, Osman Gazi Güçlütürk (Editör) *Gelişen Teknolojiler ve Hukuk II-Yapay Zeka*, On İki Levha.
- Elif Küzeci (2021) *Blokszinciri, Hukuk ve Kişisel Verilerin Korunması: Yeni Bir Güven Mekanizması Kurmak Olanaklı Mı?*, E. Eylem Aksoy Retornaz, Osman Gazi Güçlütürk (Editör), *Gelişen Teknolojiler ve Hukuk I-Blokszincir*, On İki Levha.
- Mesut Serdar Çekin (2021) *Covid-19 Pandemisi Karşısında Kişisel Sağlık Verilerinin İşlenmesine Dair KVKK Hükümlerinin İş İlişkileri Kapsamında Değerlendirilmesi*, Muhammet Özekes (Editör), *Covid-19 Salgınının Hukuki Boyutu*, 2. Baskı, On İki Levha.

Editörlü Kitaplar

2016

- Hasan Oğan (Editör) (2016) *Kişisel Sağlık Verileri Ulusal Kongresi*, Türk Tabipler Birliği.

2017

- Hasan Oğan (Editör) (2017) *Kişisel Sağlık Verileri II. Ulusal Kongresi*, Türk Tabipler Birliği.
- Samim Ünan (2017) *Sigorta Hukukunun Bazı Güncel Sorunları Kişisel Veriler-Kredi Bağlantılı Sigortalar-Zorunlu Trafik Sigortası*, On İki Levha.

2018

- Hasan Oğan (Editör) (2018) *Kişisel Sağlık Verileri "Genetik"*, Türk Tabipler Birliği.

2020

- Leyla Keser Berber, Ali Cem Bilgili (Editörler) (2020) *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku*, On İki Levha.

2021

- Hüseyin Özcan, Mehmet Başar, Ferhat Kayış, H. Derya Ormanoğlu (Editörler) (2021) *Kişisel Verilerin Korunması Alanında Yeni Gelişmeler Sempozyumu*, Adalet.
- Süleyman Yılmaz (Editör) (2021) *Bilişim Hukuku Güncel Sorunlar II*, Yetkin.

Makaleler

1991

- Durmuş Tezcan (1991) *Bilgisayar Karşısında Özel Hayatın Korunması*, Anayasa Yargısı Dergisi, Cilt 8, s. 385-392.

2000

- Faruk Petriçli (2000) *Gelişen Teknoloji Çalışma İlişkilerini Zorluyor: Çalışanların Telefon Görüşmelerinin İşverenler Tarafından Kayda Alınması*, Türkiye Barolar Birliği Dergisi, Sayı 3, s. 802-814.

2005

- Olgun Değirmenci (2005) *2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi*, Türkiye Barolar Birliği Dergisi, Sayı 58, s. 195-208.

2006

- Ayhan Döner (2006) *Kişisel Verilerin Korunması Hakkında Federal Kanun*, Erzincan Üniversitesi Hukuk Fakültesi Dergisi, Cilt 10, Sayı 1-2, s. 461-476.
- Katoğlu Tuğrul (2006) *Türk Hukukunun Bir Parçası Olarak Avrupa Konseyi İnsan Hakları ve Biyotıp Sözleşmesi*, Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt 55, Sayı 1, s. 157-193.

2007

- Muammer Ketizmen, Çağlar Ülküderner (2007) *E-Devlet Uygulamalarında Kişisel Verilerin Korun(ma)ması*, XII. "Türkiye'de İnternet" Konferansı.
- Mustafa Fadıl Yıldırım (2007) *Gen Analizleri ve Kişilik Haklarının Korunması*, Erzincan Üniversitesi Hukuk Fakültesi Dergisi, Cilt 11, Sayı 3-4, s. 20.
- Tamer Soysal (2007) *Elektronik Posta Yoluyla Kişilik Haklarına Müdahaleden Doğan Hukuki Sorumluluk*, Ankara Barosu Dergisi, Cilt 65, Sayı 1, s. 144-167.

2008

- Hüseyin Can Aksoy (2008) *The Right to Personality and Its Different Manifestations as the Core of Personal Data*, Ankara Law Review, Cilt 5, Sayı 2, s. 235-249.

- Metin Uğur Aytekin (2008) *Kişisel Verilerin Korunması, Strasbourg Sözleşmesi, Avrupa Birliği ve Türkiye*, Legal Hukuk Dergisi, Sayı 53.
- Tekin Akıllıoğlu (2008) *İdari Usul ve Kişisel Verilerin Korunması*, Maltepe Üniversitesi Hukuk Fakültesi Dergisi, Sayı 72, s. 13-27.
- Yener Ünver (2008) *Kişisel Verilerin Korunması*, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Sayı 71, s. 163-196.

2009

- Ersan Şen (2009) *Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi*, İstanbul Barosu Dergisi, Sayı: 833, s. 1197-1214.
- Hayrunnisa Özdemir (2009) *Haberleşmenin Gizliliği ve Kişisel Veriler*, Erzincan Üniversitesi Hukuk Fakültesi Dergisi, Cilt XIII, Sayı 1-2, s. 285-303.
- Zeki Hafizoğulları, Muharrem Özen (2009) *Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*, Ankara Barosu Dergisi, Sayı 4, s. 9-22.

2010

- Çetin Arslan (2010) *Avrupa Birliği Hukukunda Kişisel Verilerin Üçüncü Ülkelere Aktarılması*, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Köksal Bayraktar'a Armağan, Cilt 1, Sayı 2010/1, s. 447-487.
- Hayrunnisa Özdemir (2010) *İşyerinde İşçilerin İzlenmesi ve İşçinin Kişilik Haklarının Korunması*, Erzincan Üniversitesi Hukuk Fakültesi Dergisi, Cilt 9, Sayı 1-2, s. 231-270.
- Mine Kaya (2010) *Telekomünikasyon Alanında Kişilik Haklarının Korunması*, Ankara Barosu Dergisi, Sayı 4, s. 279-334.
- R. Barış Erman (2010) *Adli Yargı Sisteminde DNA Örnekleri ve Profilleri – S. Ve Marper – Birleşik Krallık Davası*, Fasikül Hukuk Dergisi, Sayı: 211, s. 20-23.
- Songül Atak (2010) *Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler*, Türkiye Barolar Birliği Dergisi, Sayı 87, s. 90-120.
- Sultan Tahmazoğlu Üzeltürk (2010) *Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği*, Legal Hukuk Dergisi, Sayı 93, s. 3151-3156.

2011

- Cemil Kaya (2011) *Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt LXIX, Sayı 1-2, s. 317-334.

- İsmail Köküarı (2011) *Hak Arama Özgürlüğü ve 2010 Anayasa Değişiklikleri*, Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt 15, Sayı 1, s. 163-208.

2012

- Dinç Şanver (2012) *Türkiye ve Dünyada Yaşanan Gelişmeler Işığında İnternet Ortamında Kişisel Bilgilerin Depolanması ve Kullanılması*, Legal Hukuk Dergisi, Sayı 111.
- Doğan Kılınç (2012) *Anayasal Bir Hak Olarak Kişisel Verilerin Korunması*, Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt 61, Sayı 3, s. 1089-1169.
- Emel Badur (2012) *Hastanın Özel Yaşamına Saygı Gösterilmesini Talep Hakkı*, Ankara Barosu Dergisi, Sayı 2, s. 101-121.
- İbrahim Çiçek (2013) *GBT (Genel Bilgi Toplama) Kayıtlarının Silinmesi*, Terazi Hukuk Dergisi, Sayı 888, s. 44-48.
- Serdar Gülenler (2012) *Dijital Hafızadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak "Unutulma Hakkı"*, Türkiye Barolar Birliği Dergisi, Sayı 102, s. 219-240.

2013

- Cansu Çakan (2013) *Kişilik Hakkı Kapsamında Korunan Bir Değer Olarak Kişisel Veriler*, Maltepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt 12, Sayı 2, s. 187-222.
- Çağrı Zeybek Ünsal (2013) *Google'ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri İle Uyumluluğu Ve Avrupa Birliği'nin 95/46/EC Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi*, Hacettepe Hukuk Fakültesi Dergisi, Cilt 3, Sayı 1, s. 99-124.
- Durmuş Tezcan (2013) *Özel Hayatın Gizliliğini İhlal ve Kişisel Verilerin Kaydedilmesi Suçu ile İlgili Bazı Gözlemler*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 71, Sayı 1, s. 1159-1164-1164.
- Gunnar Duttge (2013) *Genetik Verilerin Korunması İhtiyacı-Genetik İstisnacılık*, Legal Tıp Hukuku Dergisi, Sayı 4.
- Habip Oğuz (2013) *Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum*, Uyuşmazlık Mahkemesi Dergisi, Sayı 3, s. 1-38.
- Murat Balcı (2013) *Kimlik Bildirme Kanunu Kapsamında Toplanan Kişisel Verilerin Ceza Muhakemesinde ve Disiplin Soruşturmasında Delil Olarak Kullanılması*, Hukuk ve Adalet Eleştirel Hukuk Dergisi, Cilt 5, Sayı 13.
- Seldağ Güneş Peschke, Lutz Peschke (2013) *Protection Of The Mediatized Privacy In The Social Media: Aspects Of The Legal Situation In Turkey And Germany*, Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt XVII, Sayı 1-2, s. 853-883.

- Yavuz Erdoğan (2013) *Kişisel Verilerin Korunması Bakımından Türk Ceza Kanunu Hükümlerinin Değerlendirilmesi (Madde 135, 136, 137, 138)*, Erciyes Üniversitesi Hukuk Fakültesi Dergisi, Cilt 8, Sayı 2.
- Yusuf Başlar (2013) *Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri*, Uyuşmazlık Mahkemesi Dergisi, Sayı 3, s. 82-105.

2014

- Allı Yeşilyurt (2014) *Hastanın Kişisel Verilerinin Korunması ve İdarenin Yükümlülükleri*, Erciyes Üniversitesi Hukuk Fakültesi Dergisi, Cilt 9, Sayı 2, s. 215-277.
- İrem Laçın (2014) *Unutulma Hakkı*, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi: Doç. Dr. Melike Batur Yamaner'in Anısına Armağan, Cilt 13, Sayı 1, s. 391-418.
- İsmail Dursun (2014) *Türk Ceza Kanununda Verileri Yok Etmeme Suçu*, Kocaeli Üniversitesi Hukuk Fakültesi Dergisi, Cilt 5 Sayı 10, s. 9-37.
- Leyla Keser Berber (2014) *ISO/IEC 29100 Standardı ile ICT Sistemlerine Getirilen Mahremiyet Çerçevesi*, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt 11, Sayı 1, 73-105.
- M. Cumhur İzgi (2014) *Mahremiyet Kavramı Bağlamında Kişisel Sağlık Verileri*, Türkiye Biyoetik Dergisi, Cilt 1, Sayı 1, s. 25-37.
- Mahmut Erdemli, Tolga Onur (2014) *Türkiyede Özel Hayat ve Bilgi Edinme Hakkı İlişkisi: Bilgi Edinme Kurulundan İki Adım İleri Bir Adım Geri*, Ankara Barosu Dergisi, Sayı 3, s. 285-311.
- Monika Kuschewsky (2014) *AB Veri Korumasına Yönelik Köklü Reform (Çeviren: Nurullah Tekin)*, Küresel Bakış Çeviri Hukuk Dergisi, Sayı:12, s. 5.
- Nurullah Tekin (2014) *Kişisel Verilerin Korunması ile İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi*, Uyuşmazlık Mahkemesi Dergisi, Sayı 4, s. 222-262.
- Servet Yetim (2014) *Yargı Kararlarına Erişim Hakkı*, Uyuşmazlık Mahkemesi Dergisi, Sayı 4, s. 47-92.
- Yasemin Durak (2014) *İnternet Yoluyla Kişilik Haklarına Saldırı ve Hukuki Korunma*, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Cilt 22, Sayı 1, s. 101-125.

2015

- Ali Haydar Doğu (2015) *5237 Sayılı Kanun Yönünden İnternet Ortamında Kişisel Veriler ve Korunması*, İstanbul Barosu Dergisi, Cilt 89, Sayı 3, s. 146-154.
- Aydın Akgül (2015) *Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı*, Türkiye Barolar Birliği Dergisi, Sayı 118, s. 199-222.

- Aydın Akgül (2015) *Kişisel Verilerin Korunmasında Yeni Bir Hak: “Unutulma Hakkı” ve AB Adalet Divanı’nın “Google Kararı”*, Türkiye Barolar Birliği Dergisi, Sayı 116, s. 11-38.
- Eda Manav (2015) *İş İlişkisinde İşçinin Kişisel Verisinin Korunması*, Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt 19, Sayı 2.
- Lutz Peschke (2015) *“The Web Never Forgets!”: Aspects of the Right to be Forgotten*, Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt 19, Sayı 1, s. 151-160.
- Mehmet Bedii Kaya (2015) *Avrupa Birliği Adalet Divanı’nın 13 Mayıs 2014 Tarihli Google Unutulma Hakkı Kararı (Karar Çevirisi)*, Küresel Bakış, Sayı 17, s. 23-57.
- Meral Gürbüz (2015) *Özel Hayatın Gizliliği Bağlamında Kişisel Sağlık Verilerinin Korunması*, Legal Hukuk Dergisi, Cilt 13, Sayı 49.
- Mine Kaya (2015) *Sosyal Medya ve Sosyal Medyada Üçüncü Kişilerin Kişilik Haklarının İhlâli*, Türkiye Barolar Birliği Dergisi, Cilt 28, Sayı 119, s. 277-306.
- Muharrem Özen- Gürkan Özçak (2015) *Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK m. 134)*, Ankara Barosu Dergisi, s. 41-77.
- Murat Volkan Dülger (2015) *Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti*, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, Cilt 1, Sayı 2, s. 43-80.
- Nilgün Başalp (2015) *Avrupa Birliği Veri Koruması Genel Regülasyonu’nun Temel Yenilikleri*, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt 21, Sayı 1, s. 77-105.
- Salih Benli (2015) *Yolcu İsim Kayıtları*, Terazi Hukuk Dergisi, 41-48.

2016

- Abdullah Ömercioğlu (2016) *Vergi Denetim Müesseseleri Açısından Hayatın Gizli Alanına Karşı Suçlar*, Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt 65, Sayı 4, s. 2277-2304.
- Ceren Küpeli (2016) *Şiddet Mağduru Kadınların Unutulma Hakkı*, MÜHF-HAD, Cilt 22, Sayı 1, s. 229-238.
- Derya Altınok Villemin (2016) *İşçinin E-maillerinin Kontrol Edilmesi ve Özel Hayatın Gizliliği ve Korunması Hakkı*, İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi, Cilt 15, Sayı 1-2, s. 73-95.
- Gülsüm Korkmazer (2016) *Unutulma Hakkına Dair Avrupa Birliği Adalet Divanı Google Kararının Değerlendirilmesi*, Türk Hukuk Araştırmaları Dergisi, s. 125-129.
- Hasan Elmalıca (2016) *Bilişim Çağının Ortaya Çıkardığı Temel Bir İnsan Hakkı Olarak Unutulma Hakkı*, Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt 65, Sayı 4, s. 1603-1636.
- İbrahim Korkmaz (2016) *Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme*, Türkiye Barolar Birliği Dergisi, Sayı 124, s. 81-152.

- İlke Gürsel (2016) *Kişisel Verilerin Korunması Hakkının İşçi ve İşveren İlişkisine Etkileri*, İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, Cilt 13, Sayı 50.
- Kemal Atasoy (2016) *Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası*, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt 22, Sayı 3, s. 269-301.
- Mehmet Alkan (2016) *Avrupa Konseyi Bakanlar Komitesinin İnsan Hakları ve Terörle Mücadele Hakkındaki İlkeleri ve Türkiye'nin Terörle Mücadele Mevzuatı*, Türkiye Barolar Birliği Dergisi, Sayı 125, s. 9-38.
- Mesut Serdar Çekin (2016) *6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 74, Sayı 2, s. 629-644.
- Murat Volkan Dülger (2016) *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması*, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, Cilt 3, Sayı 2, s. 101-167.
- Mutlu Kağıtçıoğlu (2016) *Kişisel Verileri Koruma Kurumuna İdare Hukuku Çerçevesinden Bir Bakış*, İstanbul Kemerburgaz Üniversitesi Sosyal Bilimler Dergisi, Cilt 1, Sayı 2, s. 77-99.
- Necat Batur (2016) *Ceza Yargılamasında Moleküler Genetik İnceleme*, Türkiye Barolar Birliği Dergisi, Sayı 126, s. 26.
- Osman Açıkgöz (2016) *Kişisel Verilerin Hukuka Aykırı Şekilde Elde Edilmesi ve İnternet Bankacılığında Kullanılması Sonucu Malvarlığı Zarara Uğratılan Bankaya Karşı Mevduat Sahibinin Hukuki Sorumluluğu*, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt 22, Sayı 1, s. 390-431.
- R. Cengiz Derdiman, Nihal Tataroğlu (2016) *Devlet Gözetimi ile İnsan Haklarının Uyumlaştırılması Sorunu ve Çözüm Önerileri*, İnönü Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 7, Sayı: 1, s. 247-294.
- Selin Sert (2016) *İnternet Yoluyla Elde Edilen Kişisel Verilerin Genel Boşanma Sebepleri Arasında Değerlendirilmesi Meselesi*, Türkiye Barolar Birliği Dergisi, Sayı 116, s. 275-292.
- Servet Yetim (2016) *Sürücüsüz Araçlar ve Getirdiği / Getireceği Hukuki Sorunlar*, Ankara Barosu Dergisi, Sayı 1, s. 127-184.
- Sinan Sami Akkurt (2016) *17.06.2015 Tarih, E. 2014/4-56, K. 2015/1679 Sayılı Yargıtay Hukuk Genel Kurulu Kararı ve Mukayeseli Hukuk Çerçevesinde Unutulma Hakkı*, Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 65, Sayı: 4, 2605-2635.
- Tuğçe Karaçoban Güneş (2016) *Vergi Ödevlilerinin Kişisel Verilerinin Korunması ve Kişisel Verilerin Korunması Kanunu Tasarısı*, İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi, Cilt 15, Sayı 1.

2017

- Alptekin Burak Boydak (2017) *İşyerlerinde Uygulanan Parmak İzli Giriş Kontrol Sistemine Hukuki Bakış*, Türkiye Adalet Akademisi Dergisi, Sayı 30, s. 321-336.
- Ayşe Merve Belge (2017) *Özellikle Kişisel Verilerin Korunması Kanunu Çerçevesinde İşçilerin Kişisel Verilerinin İhlâli ve Korunması Yolları*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt 19, Özel Sayı-2017, s. 1025-1051.
- C. Gökhan Erbaş (2017) *6698 sayılı Kişisel Verilerin Korunması Kanunu Kapsamında İşçinin Elektronik Ortamda Gözetlenmesi*, Hacettepe Hukuk Fakültesi Dergisi, Cilt 7, Sayı 1, s. 97-108.
- Canan Erdoğan (2017) *İşçilerin E-Posta Hesaplarının İşveren Tarafından İncelenmesi Hakkındaki 24.03.2016 Tarihli ve 2013/4825 Başvuru Numaralı Anayasa Mahkemesi Kararı Üzerine*, İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, Cilt 14, Sayı 55, s. 1351-1386.
- Damla Gürpınar (2017) *Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt 19, Sayı Özel Sayı, s. 679-694.
- Dursun Ali Demirboğa (2017) *Avrupa Veri Koruma Tüzüğü'nün (GDPR) Sınırışan Sorumluluk Hükümlerinin Türk Hukuku Kapsamında Değerlendirilmesi*, Çukurova Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 4 Sayı: 7, s. 29-52.
- Feyzan Özbay (2017) *Terörle Mücadelede Devletin Gözetlemesi Karşısında Bireyin Özel Hayatının Gizliliğinin Korunması Hakkının Karşılaştırmalı Bir Değerlendirmesi Birleşik Krallık ve Türkiye*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: 75, Sayı: 1, s. 115-158.
- Gizem Gültekin Várkonyi (2017) *Yolcu İsim Kayıtlarının Terörle Mücadele Kapsamında Yurt Dışına Yasal Aktarımı: Avrupa Birliği Uygulamaları ve Türkiye*, Türkiye Barolar Birliği Dergisi, Cilt 30, Sayı 132, s. 44.
- Murat Önok (2017) *Kişisel Verilerin Korunması Bağlamında "Unutulma Hakkı" Ve Türkiye Açısından Değerlendirmeler*, İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi, Cilt 16, Sayı 1.
- Nafiye Yücedağ (2017) *Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt LXXV, Sayı 2, s. 765-790.
- Neslihan Karataş Durmuş (2017) *Ticari Sırların ve Kişisel Verilerin Korunması Kapsamında Vergi Mahremiyeti*, Türkiye Adalet Akademisi Dergisi, Sayı 31, s. 371-409.

- Nüket Örnek Büken, Çağrı Zeybek Ünsal (2017) *Kişisel Verilerin Korunması Kanunununun Biyomedikal Alana Yansımaları Açısından Değerlendirilmesi*, Hacettepe Hukuk Fakültesi Dergisi, Cilt: 7, Sayı: 2, s. 33-54.
- Tekin Memiş (2017) *Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni*, Beykent Üniversitesi Hukuk Fakültesi Dergisi, Cilt 3, Sayı 6, s. 9-23.
- Yeşim Çelik (2017) *Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı*, Türkiye Adalet Akademisi Dergisi, Sayı 32, s. 391-410.

2018

- Ayşenur Ocak (2018) *Hakları Dengelemek: Unutulma Hakkı İfade Özgürlüğüne Karşı*, Türkiye Adalet Akademisi Dergisi, Sayı 33, s. 507-536.
- Cihan Avcı Braun (2018) *Kişisel Verilerin İşlenmesinde Rıza*, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt 15, Sayı 1, s. 13-33.
- Çağla Tansuğ (2018) *2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Karşısında Kişisel Verileri Koruma Kurumunun Bağımsızlığı*, Legal Hukuk Dergisi, Cilt 16, Sayı 183.
- Esin Gürsel-Fatih Düğmeci (2018) *Yapısal Anlamda Türkiye Kişisel Verileri Koruma Kurumu'na İlişkin Bir Değerlendirme*, Research Studies Anatolia Journal, Cilt 1, Sayı 2, s. 318-329.
- Ezgi Çırak (2018) *Dijital Çağda Sonsuza Kadar Hatırlamaya Karşı: Unutulma Hakkı*, Ceza Hukuku Dergisi, Cilt: 13, Sayı: 36, s. 161-189.
- Gönenç Gürkaynak, Simge Alatan, Elifcan Ayşe Çepoğlu (2018) *An Evaluation of Tracking Location Data from a Data Protection Law Perspective*, Legal Hukuk Dergisi, Sayı 186.
- Gülşah Bostancı Bozbayındır (2018) *Avrupa Birliği Ceza Hukuku'nda Polis ve Ceza Adaleti Otoritelerine Yönelik 2018/680 Sayılı Direktif: Kişisel Verilerin Ceza Adalet Mekanizmalarında Korunmasına Getirilen Standartlar ve Direktife Yönelik Eleştiriler*, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Cilt 2, Sayı 2, s. 51-103.
- Mehmet Oğuz Vuraloğlu (2018) *Kişisel Verilerin İşlenmesi Suretiyle Kişilik Hakkı İhlâlinde Kazancın Devri Talebi*, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt 15, Sayı 1, s. 181-203.
- Muhammet Sefa Mutlu (2018) *Hekimin Cezai Sorumluluğu Açısından Kişisel Verilerin Kaydedilmesi Suçunun (TCK m. 135) Değerlendirilmesi*, Kadir Has Üniversitesi Hukuk Fakültesi Dergisi, Cilt 6, Sayı 1, s. 29-58.
- Mustafa Tefvik Kartal (2018) *Kişisel Verilerin Korunması: Türk Bankacılık Sektörü Üzerine Kavramsal Bir Değerlendirme*, Uluslararası Ekonomi ve Yenilik Dergisi, Cilt 4, Sayı 1, s. 1-18.

- Nafiye Yücedağ (2018) *İsviçre, Avrupa Birliği ve Türk Hukuklarına Göre İlgili Kişi Tarafından Kamuya Sunulmuş Verinin İşlenmesi*, Annales de la Faculté de Droit d'Istanbul, Sayı 67, s. 125-140.
- Nurten İnce Akman (2018) *Mirasbırakanın Dijital Bilgilerinin Mirasçılara Geçişini Dijital Tereke*, İnönü Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 9, Sayı: 2, s. 527-560.
- Özgür Oğuz (2018) *Kişisel Verilerin Korunması Kanunu'nun Çalışma Hayatına Yansımaları*, İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, Cilt 15, Sayı 60.
- Sefer Oğuz (2018) *Kişisel Verilerin Korunması Hukukunun Genel İlkeleri*, Bilgi Ekonomisi ve Yönetimi Dergisi, Cilt 13, Sayı 2, s. 121-138.
- Seray Nalbantoğlu (2018) *Bir Temel Hak Olarak Unutulma Hakkı*, Türkiye Adalet Akademisi Dergisi, Sayı 35, s. 583-605.
- Simay Sevinçer (2018) *Biyometrik Yöntemlerle Elde Edilen Kişisel Verilerin Site Konutların Güvenlik Sistemlerinde Kullanımı*, İstanbul Barosu Dergisi, Cilt: 92, Sayı: 2, s. 233-244.
- Tefvik Sönmez Küçük (2018) *Kişisel Verilerin Korunması Hakkı Çerçevesinde Kamuya Açık Alanların Kamu Tüzel Kişileri Tarafından Video Kamera Aracılığı ile Önleyici Amaçla İzlenmesi*, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 25, Sayı: 1, s. 49-87.

2019

- Aslıhan Kart, Muammer Ketizmen (2019) *Kabahatler Kanunu'nun İctima Hükümleri Açısından Kişisel Verilerin Korunmasına İlişkin Suç ve Kabahatler ile Kurul'un İdari Ceza Kararlarına İlişkin Bir Değerlendirme*, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 2, s. 17-29.
- Aylin Erdoğan (2019) *Bankacılık Sektöründe Kişisel Verilerin Korunması ve Müşteri İlişkileri Yönetimi*, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 2, s. 87-94.
- Ayşe Özge Atalay (2019) *Ceza Muhakemesi Hukukunda Moleküler Genetik İncelemelerin Özel Nitelikli Kişisel Verilerin Korunması Açısından Değerlendirilmesi*, Journal of Penal Law and Criminology, Cilt 7, Sayı 2, s. 127-184.
- Baran Kızılırmak (2019) *Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla Öngörülen İstisnaların Ulusal ve Uluslararası Hukuka Göre Değerlendirilmesi*, Kadir Has Üniversitesi Hukuk Fakültesi Dergisi, Cilt 7, Sayı 2, s. 225-261.
- Berna Akçalı Gür (2019) *Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması*, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt 25, Sayı 2, s. 850-872.
- Bilgin Metin, Sema Erkan, İdil Atasu, Enes Yılmaz (2019) *Privacy Impact Assessment as a Tool for GDPR Compliance Preparation*, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 2.

- Canan Erdoğan (2019) *Çocukların Kişisel Verilerinin Korunması (Sosyal Medya Örneği Kapsamında)*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt 21, Sayı Özel Sayı: Prof. Dr. Durmuş Tezcan'a Armağan, s. 2445-2467.
- Cansu Akgün Tekgül (2019) *Brüksel 1Bis Tüzüğü İle Avrupa Birliği Genel Veri Koruma Tüzüğü Çerçevesinde Kişisel Verilerin İhlaline İlişkin Özel Hukuk Uyuşmazlıklarında Milletlerarası Yetki Kuralları*, Hacettepe Hukuk Fakültesi Dergisi, Cilt 9, Sayı 1, s. 232-275.
- Cuneyt Pekmez (2019) *Kişisel Verilerin Korunması Kanunu Kapsamında Veri İşleyen ve Veri Sorumlusu Kavramı Üzerine Değerlendirme*, Annales de la Faculté de Droit d'Istanbul, Sayı 67, s. 59-71.
- Elif Küzeci, Şebnem Kılıç (2019) *6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun İş Sözleşmesi Çerçevesinde Değerlendirilmesi: Veri Sorumlusu, Veri İşleyen ve Diğer Aktörler*, İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, Cilt 16, Sayı 63.
- Eren Solmaz (2019) *Avrupa İnsan Hakları Mahkemesi Kararları'nın "Kişisel Verilerin Korunması"na Katkısı*, İdare Hukuku ve İlimleri Dergisi, Cilt 18, Sayı 1, s. 61-78.
- Gürbüz Yüksel (2019) *Kişisel Sağlık Verilerinin Hukuki Korunması*, Sağlık Akademisyenleri Dergisi, Cilt 6, Sayı 1, s. 1-10.
- Halil Altındağ (2019) *Kişisel Verilerin Korunması Bağlamında İdarenin Sorumluluğu*, İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 18, Sayı: 2, s. 387-401.
- Hilal Tuğba Öksüzöğlü (2019) *6698 sayılı Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği Hukukunda Kişisel Verilerin Silinmesi ve Düzeltilmesi*, Bilişim Hukuku Dergisi, Cilt 1, Sayı 2, s. 185-242.
- Işık Aslı Han (2019) *Kişisel Verilerin İşlenmesi Bağlamında Hukuka Uygunluk Sebebi Olarak Veri Sahibinin Rızası*, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Köksal Bayraktar'a Armağan, Cilt 1, Sayı 2019/1, s. 417-458.
- Leyla Keser Berber (2019) *E-Gizlilik Tüzük Taslağının Son Versiyonu Üzerine Düşünceler*, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 2, s. 9.
- Leyla Keser Berber, Ayça Atabey, Melis Mert (2019) *E-Gizlilik Tüzük Taslağının Son Versiyonu Üzerine Düşünceler*, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 2, s. 66-74.
- Mesut Serdar Çekin (2019) *Borçlar Hukuku ile Veri Koruma Hukuku Açısından Blockchain Teknolojisi ve Akıllı Sözleşmeler: Hukuk Düzenimizde Bir Paradigma Değişimine Gerek Var mı?*, İstanbul Hukuk Mecmuası, Cilt 77, Sayı 1, s. 315-341.
- Muammer Ketizmen, Aslıhan Kart (2019) *Kişisel Veri ve Rekabet Hukuku Kapsamında "Big Data"*, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 1, s. 64-76.

- Murat Volkan Dülger (2019) *Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması*, Yaşar Hukuk Dergisi, Cilt 1, Sayı 2, s. 71-174.
- Naciye Betül Haliloğlu (2019) *Yargılamaya ve Mahkûmiyete İlişkin Verilerin Genel Bilgi Toplama GBT Sisteminde Tutulması: Anayasa Mahkemesinin Bülent Kaya ve E.Ç.A. Kararlarının Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Değerlendirilmesi*, Anayasa Yargısı, Cilt: 36, Sayı: 2, s. 349-400.
- Nafiye Yücedağ (2019) *Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler*, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 1, s. 47-63.
- Nilüfer Boran Güneysu, Burak Memiş (2019) *Kişisel Verilerin Korunması Kanunu Kapsamında Avukatın Yükümlülük ve Sorumlulukları*, Anadolu Üniversitesi Hukuk Fakültesi Dergisi, Cilt 5, Sayı 2, s. 313-337.
- Osman Gazi Güçlütürk (2019) *Blokszincir Üzerinde Depolanan Verilerin Kişisel Veri Niteliği ve Silinemezlik, Yok Edilemezlik Sorunu*, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 2, s. 30-40.
- Oya Boyar, Sezen Kama Işık (2019) *Dördüncü Kuşak Haklar ve Bilişim Teknolojilerinin Doğuşunda Mahremiyet Kavramına Karşılaştırmalı Bir Bakış*, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt 25, Sayı 2, s. 602-623.
- Ozan Selek (2019) *Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt 21, Sayı 2, s. 911-951.
- Özge Apiş, Zahit Yılmaz (2019) *Çocuğun Özel Hayatının Gizliliği Hakkı Kapsamında Velayet Hakkının Ceza Hukuku Bakımından Sınırı*, Legal Hukuk Dergisi, Cilt 17, Sayı 194.
- Salih Polater (2019) *Kişisel Verilerin Reklam Amaçlı İşlenmesinde Hukuka Uygunluk Sebepleri*, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 1, s. 1-20.
- Şehriban İpek Aşıkoğlu (2019) *Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-*, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 2, s. 41-65.
- Tamer Soysal (2019) *Unutulma Hakkının Avrupa Birliği'nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi*, Uyuşmazlık Mahkemesi Dergisi, Sayı 13.
- Turan Atlı (2019) *Kişisel Verilerin Önleyici, Koruyucu ve İstihbari Faaliyetler Amacıyla İşlenmesi*, Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi, Cilt 2, Sayı 1, s. 4-22.
- Ufuk Dal (2019) *Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Ülke Dışı Uygulama Yetkisi ve Bu Yetkinin Uluslararası Hukukta Meşruiyeti*, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 1, s. 21-33.
- Yasemin Maraşlı Dinç (2019) *Ölümden Sonra Sosyal Medya Hesaplarının Hukuki Akıbeti: Dijital Miras*, TBB Dergisi, Sayı: 142, s. 273-287.
- Yiğit Yıldız (2019) *Kişisel Verilerin Korunmasının Vergi Mahremiyeti ile Etkileşimi*, Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 2, s. 1-16.

- Yiğit Yıldız (2019) *Kişisel Verilerin Korunmasının Vergi Mahremiyeti ile Etkileşimi*, *Kişisel Verileri Koruma Dergisi*, Cilt 1, Sayı 2, s. 1-16.
- Zeki Emre Kurt (2019) *Cambridge Analytica Skandalı Kişisel Verilerin Etkili Bir Şekilde Korunması Hususunda Alınacak Tedbirlere Vesile Oldu Mu? Hiç Sanmıyoruz!*, *Fikri ve Sınai Haklar Dergisi*, Sayı 57.

2020

- Abdullah Ömeroğlu (2020) *Kişilik Haklarının Alkaya-Türkiye Davası Bağlamında Kişisel Verilerin Korunması Hukukuna Göre İncelenmesi*, *Uyuşmazlık Mahkemesi Dergisi*, Sayı 15, s. 309-342.
- Adem Yelmen (2020) *Bilgisayar Programlarına İlişkin Lisans Sözleşmelerindeki Gizlilik Hükümleri Hakkında Değerlendirmeler*, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, Cilt: 22, Sayı: 2, s. 991-1019.
- Asuman Çapar (2020) *Kamu Personelinin Atanmasında Güvenlik Soruşturması Uygulaması*, *Erciyes Üniversitesi Hukuk Fakültesi Dergisi*, Cilt 15, Sayı 2, s. 569-612.
- Ata Umur Kalender (2020) *Parçalı Bulutlar: Cloud Act ve Etkileri*, *Kişisel Verileri Koruma Dergisi*, Cilt 2, Sayı 2, s. 74-107.
- Atilla Erkal (2020) *Avrupa Genel Veri Koruma Düzenlemesi Bağlamında Memurların Kişisel Verilerinin Korunması Hakkı*, *Anayasa Yargısı*, Cilt 37, Sayı 2, s. 205-253.
- Ayla Çalışkan (2020) *Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, *Çankaya Üniversitesi Hukuk Fakültesi Dergisi*, Cilt 5, Sayı 1.
- Ayşenur Ocak (2020) *İnsan Hakları Açısından Devlet Tarafından İşlenen Kişisel Verilerin Açıklanması*, *Ankara Barosu Dergisi*, Cilt 78, Sayı 2020/4, s. 37-74.
- Berke Ada (2020) *İş İlişkisinde İşçinin Kişisel Bilgilerinin Hukuka Aykırı Olarak Kullanılması ve Hukuki Sonuçları*, *Antalya Bilim Üniversitesi Hukuk Fakültesi Dergisi*, Cilt 816, s. 967-1011.
- Bilal Osmanoğlu (2020) *Genel Bilgi Toplama (GBT) Sisteminde Kişilere İlişkin Tutulan Kayıtlar Üzerine Bir İnceleme*, *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, Cilt 26, Sayı 2, s. 946-979.
- Burcu Görkemli (2020) *Türk Ceza Hukukunda Kişisel Verilerin Kaydedilmesi Suçu*, *Ceza Hukuku Dergisi*, Cilt 15, Sayı 44.
- Cemal Başar (2020) *Kişisel Verilerin Korunması Bakımından Kişisel Verileri Koruma Kurulu'na Yapılan Şikâyet Başvurusu*, *Fasikül Hukuk Dergisi*, Cilt 12, Sayı 125.
- Derya Tekin (2020) *Kişinin Tarafı Olduğu Haberleşmenin Gizliliğini İhlal Suçuna (TCK m.132/3) İlişkin Güncel Sorunlar*, *Ceza Hukuku Dergisi*, Cilt 15, Sayı 43.

- Dilek Dulay Yangın (2020) *Avrupa İnsan Hakları Mahkemesi Büyük Daire'nin İşçilerin Gizli Kamera ile İzlenmesine İlişkin 17 Ekim 2019 Tarihli Lopez Ribalda ve Diğerleri Kararı'nın Değerlendirilmesi*, Çalışma ve Toplum, 3, s. 1703-1728.
- Dilek Gökçe Başdağ (2020) *4857 Sayılı İş Kanunu Bağlamında Çalışan Sağlık Verilerinin İşleme Koşulları*, Çankaya Üniversitesi Hukuk Fakültesi Dergisi, Cilt 1, Sayı 1.
- Dilşat Yılmaz (2020) *Yeni Bir İdari Faaliyet Alanı: "VERBİS" (Veri Sorumluları Sicil Bilgi Sistemi)*, Yıldırım Beyazıt Hukuk Dergisi, Sayı 2, s. 83-118.
- Furkan Güven Taştan, Utku Saruhan (2020) *Açık Bankacılık: Kişisel Verilerin Korunmasına Bir Tehdit Mi?*, Çevrimiçi Yayın, Researchgate.net, s. 1-44.
- Furkan Övündür (2020) *Dijital Tek Pazar Stratejisinin Hukuki Bağlamında Kişisel Veri Güvenliğinin Sağlanması*, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Cilt 19, Sayı 38, s. 118-131.
- Gamze Aşçıoğlu (2020) *Corona (Covid 19) Gölgesinde Geleceğin Hukuku ve Dijital Ekonomi Çağında Rekabet Hukuku*, Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt 69, Sayı 1, 2020, s. 33-56.
- Gamze Turan Başara (2020) *Kişisel Veri İşleme Sözleşmesi*, Uyuşmazlık Mahkemesi Dergisi, Sayı: 16, s. 57-90.
- Gizem Gültekin Várkonyi (2020) *Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Gerçek Kişilerin Kişisel Sosyal Robot Kullanımından Doğabilecek Sorumlulukları*, Kişisel Verileri Koruma Dergisi, Cilt 2, Sayı 2, s. 19-29.
- Göksu Hazar Erdiñç (2020) *Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi*, Kişisel Verileri Koruma Dergisi, Cilt 2, Sayı 1, s. 1-19.
- Hasan Sınar (2020) *Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma Veya Ele Geçirme Suçu (TCK md. 136)*, Kişisel Verileri Koruma Dergisi, Cilt 2, Sayı 1, s. 33-62.
- Hüseyin Aksoy, Mesut Halıoğlu (2020) *E-Gizlilik Tüzüğü Çalışmaları Işığında Türk Hukukunda Elektronik Haberleşmenin Gizliliğinin Korunması*, Kişisel Verileri Koruma Dergisi, Cilt 2, Sayı 2, s. 1-18.
- İhsan Hüseyin (2020) *İngiliz Hukukuna Göre Mahremiyet Hakkının İhlalleri*, Hasan Kalyoncu Üniversitesi Hukuk Fakültesi Dergisi, 1020), s. 241-277.
- İrem Betül Pektaş (2020) *Karekodlu Çeklerde İşlenen Kişisel Verilerin Hukuka Uygunluğu*, Banka ve Finans Hukuku Dergisi, Cilt 9, Sayı 35.
- Kadri İnce (2020) *Önleme ve İstihbari Amaçlı İletişimin Denetlenmesinin Özel Hayatın Gizliliği ve Haberleşme Özgürlüğü Çerçevesinde Değerlendirilmesi*, Çankaya Üniversitesi Hukuk Fakültesi Dergisi, Cilt 1, Sayı 2.

- Kayıhan İçel (2020) *Ceza Hukuku Açısından Kişisel Verilerin Korunmasında Kişisel Veri ve Hukuka Aykırılık Kavramları*, İstanbul Barosu Dergisi, Cilt: 94, Sayı: 2, s. 15-23.
- Kerim Çakır (2020) *Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)*, Antalya Bilim Üniversitesi Hukuk Fakültesi Dergisi, Cilt 8, Sayı 16.
- Leyla Keser Berber- Ayça Atabey (2020) *Çevrim İçi Oyun Platformlarının Gizlilik Taraması: "Gamecell" Analizi*, Annales de la Faculté de Droit d'Istanbul, Sayı 69, s. 181-225.
- Mehmet Kahraman, Muhammed Şahin (2020) *Anayasa Mahkemesi Kararlarına Göre Güvenlik Soruşturması ve Özel Hayata Saygı Hakkı*, Erciyes Üniversitesi Hukuk Fakültesi Dergisi, Cilt 15, Sayı 2, s. 415-449.
- Metin Bulut (2020) *Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler*, Ankara Barosu Dergisi, Cilt 78, Sayı 3, s. 99-150.
- Miray Özer Deniz (2020) *Kişisel Verilerin Korunması Kanunu İle Arabuluculuğa Hâkim Gizlilik İlkesinin Birlikte Değerlendirilmesi*, Kişisel Verileri Koruma Dergisi, Cilt 2, Sayı 1, s. 63-71.
- Muhammed Emin Karakaş (2020) *Dijital Geçmişin İnternet Erişiminden Kaldırılması "Unutulma Hakkı" ve Türk Hukukunda Görünümü*, Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi, Cilt 3, Sayı 2, s. 262-289.
- Murat Volkan Dülger, Onur Özkan (2020) *Kolluk Teşkilatında ve Ceza Yargılamalarında Kişisel Verilerin Korunması: "Unutulan" Direktifin Kapsamlı*, Ceza Hukuku Dergisi, Cilt 15, Sayı 42.
- Neslihan Can (2020) *Hasta Mahremiyeti Hakkı*, TBB Dergisi, Sayı 147, s. 183-219.
- Nuray Ekşi (2020) *Türk Vatandaşlarının Biyometrik Verilerinin İşlenmesinin Türkiye-AB Ortaklık Konseyi Kararlarına Aykırı Olmadığına İlişkin 3.11.2019 Tarihli ABAD Kararının Tercümesi*, Kişisel Verileri Koruma Dergisi, Cilt 2, Sayı 1, s. 72-88.
- Onur Kaplan (2020) *Karar İncelemesi: "COVID-19 Salgını Karşısında İdari Faaliyetlerde Drone Kullanımı ve Kişisel Verilerin Üzerine"*, Terazi Hukuk Dergisi, Cilt 15, Sayı 166, s. 1262-1266.
- Ozan Can, İlgün Mağden Çamlı (2020) *Türk Hukukuna Göre Anonim Şirketlerde Pay Sahiplerinin Kişisel Verilerinin İşlenmesi ve Korunması*, BATİDER, Cilt 36, Sayı 3, s. 129-161.
- Ömer Ali Girgin, Seray Gönal (2020) *Çocuğun Kişisel Verilerinin Sosyal Medyada Ebeveyn Tarafından Paylaşılmasının Hukuki Sonuçları*, Türkiye Adalet Akademisi Dergisi, Sayı 44, s. 99-128.
- Özge Apiş (2020) *Hükümlünün Unutulma Hakkı ve Resosyalizasyonu*, Ceza Hukuku Dergisi, Cilt 15, Sayı 44, s. 831-864.
- Remzi Demir (2020) *Unutulma Hakkının Türk Medeni Kanunu ve Türk Borçlar Kanunu Açısından Değerlendirilmesi*, Antalya Bilim Üniversitesi Hukuk Fakültesi Dergisi, Cilt 8, Sayı 16, s. 1013-1032.

- Sabire Sanem Yılmaz (2020) *Anayasa Mahkemesi Kararları Işığında Kişisel Sağlık Verilerine Bakış*, Terazi Hukuk Dergisi, Cilt 15, Sayı 161, s. 101-110.
- Samet Saygı (2020) *6698 Sayılı Kanun'un Sistematiğinde Yargısal Başvuru Yolları*, Kişisel Verileri Koruma Dergisi, Cilt 2, Sayı 2, s. 30-61.
- Selen Uncular (2020) *Kişisel Verilerin Korunması Kanunu'nda Yer Alan Hakların ve Yükümlülüklerin İş İlişkisindeki Yansımaları*, Çankaya Üniversitesi Hukuk Fakültesi Dergisi, Cilt 1, Sayı 3, s. 3405-3427.
- Sinan Sami Akkurt (2020) *Kişisel Sağlık Verilerinin İşlenmesine ve Covid-19 Pandemisi Sürecinde Mobil Uygulamalarla Paylaşılmasına Hukukî Bir Bakış*, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Cilt 19, Sayı 38, s. 142-160.
- Sinan Sami Akkurt (2020) *Kişisel Veri Kavramının Hukukî Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış*, Kişisel Verileri Koruma Dergisi, Cilt 2, Sayı 1, s. 20-32.
- Süleyman Yılmaz, Vehbi Umut Erkan (2020) *Sosyal Medya Hesaplarının Miras Yoluyla İntikal Edip Edemeyeceği Sorusunun Kişisel Verileri Koruma Hukuku Kapsamında İncelenmesi*, İnönü Üniversitesi Hukuk Fakültesi Dergisi, Cilt 11, Sayı 2, s. 567-586.
- Tekin Memiş, Cemile Turgut (2020) *Dijital Miras Konusunda Gözden Kaçanlar*, Beykent Üniversitesi Hukuk Fakültesi Dergisi, Cilt 6, Sayı 12, s. 201-215.
- Ufuk Tekin (2020) *"Kişisel Veri" Kavramının Ticaret Şirketleri Bakımından Düşündürdükleri*, Çankaya Üniversitesi Hukuk Fakültesi Dergisi, Cilt 5, Sayı 1-3, s. 3127-3140.
- Yakup Korkmaz (2020) *Hasta Hakkı Olarak Özel Hayatın Korunması Bağlamında Beden Mahremiyeti*, Uyuşmazlık Mahkemesi Dergisi, 15, s. 573-598.
- Yasin Üstün, Ayşe Günel (2020) *İş İlişkilerinde Bazı Yaygın Uygulamaların Kişisel Verilerin Korunması Kanunu Kapsamında Değerlendirilmesi*, Kişisel Verileri Koruma Dergisi, Cilt 2, Sayı 2, s. 62-73.
- Yaşar Salihpaşaoğlu, Burcu Değirmencioğlu (2020) *Unutulma Hakkının Bir "İnsan Hakkı"na Dönüşme Yolculuğu*, Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, Cilt 24, Sayı 2, s. 361-388.
- Yıldırım Keser (2020) *Tüketicinin Kişisel Verisinin İşlenmesinde Açık Rıza*, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Cilt 28, Sayı 3, s. 1181-1215.

2021

- Ayça Atabey-Leyla Berber (2021) *Yapay Zeka Sistemlerinin Çocuk Haklarına Etkilerinin Değerlendirilme Yöntemi: Çocuk Hakları Etki Analizi*, Adalet Dergisi, Sayı 66, s. 55-85.

- Berat Duman (2021) *Whatsapp Veri Paylaşım Politikasının Kişisel Verilerin Korunması Hukuku Kapsamında Değerlendirilmesi (AB Hukuku ile Mukayeseli)*, Adalet Dergisi, Sayı 66, s. 543-567.
- Buket Günay (2021) *Kişilik Hakkı Perspektifinden Kadın Cinayetlerinde Hükümlünün Unutulma Hakkı*, Yaşar Hukuk Dergisi, Cilt 3, Sayı 2, s. 129-160.
- Cenk Konukpay, Uğur Tabak (2021) *Kişisel Verilerin İşleme Amacının Sonradan Değişmesi: Uyumluluk Kriterlerinin Uygulanması Sorunu*, Kişisel Verileri Koruma Dergisi, Cilt 3, Sayı 2, s. 15-33.
- Ece Karaduman (2021) *Yükseköğretim Kurumları Tarafından Kullanılan Uzaktan Öğretim Teknolojileri Çerçevesinde Öğrencilerin Kişisel Verilerinin ve Kişilik Haklarının Korunması*, Başkent Üniversitesi Hukuk Fakültesi Dergisi, Cilt 7, Sayı 1, s. 91-136.
- Erdem Büyüksağış (2021) *Yapay Zeka Karşısında Kişisel Verilerin Korunması ve Revizyon İhtiyacı*, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt 18, Sayı 2, s. 529-541.
- Fatma Esenyel Hanaz (2021) *Çevrimiçi Eğitimde Üniversite Öğrencilerinin Kişisel Verilerinin İşlenmesinin Hukuki Sebepleri*, TBB Dergisi, Sayı 155, s. 409-460.
- Fatmagül Kale Özçelik (2021) *COVID-19 Salgını Sürecinde Üniversite Eğitiminde Kullanılan Uzaktan Eğitim Platformlarının 6698 Sayılı Kişisel Verilerin Korunması Kanunu Çerçevesinde Değerlendirilmesi*, Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi, Cilt 11, Sayı 1, s. 135-170.
- Gülşah Bostancı Bozbayındır (2021) *Avrupa Genel Veri Koruma Tüzüğü Çerçevesinde Çocukların Kişisel Verilerinin Korunması ve 'Sharenting'*, Terazi Hukuk Dergisi, Cilt 16, Sayı 180, s. 1498-1516.
- Hatice Hocaoğlu, Fatma Sümeyra Doğan, Zeynep Sena Saltık (2021) *Bulut Yasası ve Schrems II Kararı Işığında Türkiye'de Müşteri Hizmeti Uygulamaları Hakkında Uygulamacı Perspektifinden Değerlendirmeler*, Terazi Hukuk Dergisi, Cilt 16, Sayı 174, s. 364-368.
- Hüseyin Can Aksoy-Mesut Halıoğlu (2021) *AB ve Türk Hukuklarında Çerezler: Kişisel Verilerin Korunması Açısından Karşılaştırmalı Bir Değerlendirme*, Kişisel Verileri Koruma Dergisi, Cilt 3, Sayı 1, s. 61-88.
- İbrahim Barış Sayar (2021) *Genel Veri Koruma Tüzüğü İdari Para Cezaları Rejimi ve Etkiliği*, Kişisel Verileri Koruma Dergisi, Cilt 3, Sayı 1, s. 1-16.
- İlyas Arslan (2021) *Kişisel Verilerin Yabancı Unsurlu Sözleşmelere Aykırı Olarak İşlenmesinden veya Korunmamasından Kaynaklanan Uyuşmazlıklara Uygulanacak Hukukun Tespiti*, İstanbul Hukuk Mecmuası, Cilt 79, Sayı 1, s. 135-191.
- İntizar Sultanlı (2021) *Anayasal Bir Hak Olan Kişisel Verilerin Korunması Hakkı Ve Mahremiyet İle İlişkisi*, Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi, Cilt 4, Sayı 1, s. 23-34.

- İsmail Yazıcıoğlu, Fatma Ebru Gündüz (2021) *Bilgi Edinme Hakkı Çerçevesinde Kişisel Verilerin Korunması*, Anayasa Yargısı, Cilt 38, Sayı 1, s. 171-204.
- Kamile Türkoğlu Üstün (2021) *Güvenlik Soruşturmalarında Kişisel Verilerin Korunması*, Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, Cilt 25, Sayı 2, s. 787-837.
- Kerim Kılıç (2021) *Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)*, Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi, Cilt 25, Sayı 1, s. 1-45.
- Mehmet Bedii Kaya (2021) *Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi*, İstanbul Hukuk Mecmuası, Cilt 78, Sayı 4, s. 1859-1897.
- Mehmet Bedii Kaya (2021) *Self-Disclosure or Burying the Evidence Dilemma: A Legal Review of the Data Breach Rules under the Turkish Personal Data Protection Law*, Annales de la Faculté de Droit d'Istanbul, Sayı 70, s. 195-241.
- Mehmet Semih Öztekin (2021) *Brezilya Veri Koruma Yasasının 6698 Sayılı Kişisel Verilerin Korunması Kanunu İle Mukayeseli Olarak İncelenmesi*, Kişisel Verileri Koruma Dergisi, Cilt 3, Sayı 2, s. 50-65.
- Meltem Ertuğrul (2021) *Çocuğun Kişisel Verilerinin Velisi Tarafından Sosyal Medyada Kullanılmasının Kişilik Hakkı Bakımından Değerlendirilmesi*, Yıldırım Beyazıt Hukuk Dergisi, Sayı 2, s. 513-564.
- Mert Karamustafaoğlu, Sevgi Ünsal Özden, İdil Uz (2021) *Kişisel Veri Aktarımı ve Bankacılık Kanunu Madde 73 Değişikliği*, Kişisel Verileri Koruma Dergisi, Cilt 3, Sayı 1, s. 17-40.
- Miray Özer Deniz (2021) *İşçilerin Özel Nitelikli Kişisel Verilerinin Korunması ve Bundan Doğan Sorumluluk*, Türkiye Adalet Akademisi Dergisi, Sayı 45, s. 355-378.
- Muammer Ketizmen, Aslıhan Kart (2021) *Kişisel Verilerin Korunması Kanununun 17. Maddesi ve Yargıtay Kararları Doğrultusunda, Kişisel Verilerin Korunmasına İlişkin Suç Teşkil Eden Fiiller Açısından Uygulanacak Norm Hakkında Değerlendirme*, Kırıkkale Hukuk Mecmuası, Cilt 1, Sayı 2, s. 256-268.
- Murat Uçak (2021) *Kişisel Verilerin Hukuka Uygun İşlenmesinde Çocuğun Rızası*, Kişisel Verileri Koruma Dergisi, Cilt 3, Sayı 1, s. 41-60.
- Murat Uçak (2021) *Kişisel Verilerin Ölümden Sonra Korunması*, İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Dergisi, Cilt 6, Sayı 10, s. 97-123.
- Noor Talaat Azzat Sahar (2021) *6698 Sayılı Kişisel Verilerin Korunması Kanununda Yer Alan Temel Kavramlar ile Terminoloji*, Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi, Cilt 4, Sayı 1, s. 35-52.
- Ömer Faruk Kuntoğlu (2021) *Elektronik Ticarete Kişisel Verilerin Korunması*, Bilişim Hukuku Dergisi, Cilt 3, Sayı 1, s. 176-229.
- Özge Yenice Ceylan (2021) *Unutulma Hakkının Basın Özgürlüğü Karşısındaki Konumu*, Kişisel Verileri Koruma Dergisi, Cilt 3, Sayı 2, s. 1-14.

- Rabia Özkan (2021) *Kişisel Veri Koruma Hukukunun Kişilik Hakkının Korunması Çerçevesinde Değerlendirilmesi*, Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Dergisi, Cilt 3, Sayı 2, s. 675-733.
- Salih İnan (2021) *Kişisel Verilerin Korunması Kapsamında İhdas Edilen Yaptırım Kararlarına Karşı Yargısal Başvuru Yolları: Karşılaştırmalı Bir İnceleme*, Kişisel Verileri Koruma Dergisi, Cilt 3, Sayı 2, s. 34-49.
- Selin Sert Sütçü (2021) *Covid-19'un Kişisel Sağlık Verilerinin Korunması Üzerindeki Etkilerinin İncelenmesi*, Terazi Hukuk Dergisi, Cilt 16, Sayı 177, s. 931-938.
- Serdar Çelikel (2021) *Kişisel Verilerin İşlenmesinde, Açık Rıza Hukuka Uygunluk Nedeninin, 95/46 Sayılı Direktif Ve GDPR'la Karşılaştırmalı Olarak İncelenmesi*, Uyuşmazlık Mahkemesi Dergisi, Sayı 17, s. 161-190.
- Sevgi Erarslan (2021) *Türk Hukukunda Kişisel Verilerin Yurt Dışına Aktarılması Sorunu: Açık Rıza Kapsamında Bir Değerlendirme*, Kırıkkale Hukuk Mecmuası, Cilt 1, Sayı 1, s. 82-115.
- Sümeyye Şimşek (2021) *Yenilenen WhatsApp Gizlilik Politikası ve Kişisel Verileri Koruma Kurumu İncelemesi*, Bilişim Hukuku Dergisi, Cilt 3, Sayı s. 494-548.
- Uğur Aşkın (2021) *Hekimin Sır Saklama Yükümlülüğü ile Suçu Bildirmeme Suçu Arasındaki İlişki*, Hacettepe Hukuk Fakültesi Dergisi, Cilt 11, Sayı 2, s. 1368-1394.
- Umniyahashghar Yosif (2021) *Kişisel Verilerin İşlenmesi Şartları ve 6698 Sayılı Kişisel Verilerin Korunması Kanununun Ruhu Olarak Genel İlkeler*, Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi, Cilt 4, Sayı 1, s.1-22.
- Veli Durmuş (2021) *Kişisel Sağlık Verilerinin Korunmasında İdarenin Hukuki Sorumluluğu*, Dokuz Eylül Üniversitesi Hemşirelik Fakültesi Elektronik Dergisi, Cilt 14, Sayı 1, s. 67-76.
- Yahya Usman (2021) *Kişisel Verileri Koruma Kurumunca Uygulanan Yaptırımların Yargısal Denetiminde Görevli Mahkeme*, Terazi Hukuk Dergisi, Cilt 16, Sayı 180, s. 1517-1531.
- Yasin Aydoğdu (2021) *Kamu İdaresinde Kişisel Verilerin Korunması*, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Cilt 29, Sayı 1, s. 263-293.
- Yiliyaer Abudureyimu, Yücel Oğurlu (2021) *Yapay Zekâ Uygulamalarının Kişisel Verilerin Korumasına Dair Doğurabileceği Sorunlar ve Çözüm Önerileri*, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Cilt 20, Sayı 41, s. 765-782.

2022

- Abdurrahim Çınar (2022) *Unutulma Hakkının Ortaya Çıkış Serüveni ve Kapsamının Değerlendirilmesi*, Türkiye Adalet Akademisi Dergisi, Sayı 49, s. 551-584.

- Alpkaan Ertan (2022) *Nesnelerin İnternetinin Kişisel Verilerin Korunması Kapsamında İncelenmesi*, Kişisel Verileri Koruma Dergisi, Cilt 4, Sayı 2, s. 48-68.
- Ayşe Aslı Alçın (2022) *Türk Hukukunda Kişisel Sağlık Verileri ve İdarenin Kişisel Sağlık Verilerini Koruma Yükümlülüğü*, Türkiye Adalet Akademisi Dergisi, Sayı 51, s. 365-410.
- Ayşe Nida Günal, Yasin Üstün (2022) *İş İlişkilerinde Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebebi Olarak "Meşru Menfaat"*, Kişisel Verileri Koruma Dergisi, Cilt 4, Sayı 2, 1-18.
- Derya Yurteri Çetin, 6698 Sayılı Kişisel Verileri Koruma Kanunu Kapsamında Çalışanlara ve Çalışan Adaylarına Yapılabilecek Testler, Kişisel Verileri Koruma Dergisi, Cilt: 4, Sayı: 1, s. 14-24.
- Elif Yılmaz Furtuna, Sibel Bilgin (2022) *Kişisel Verilerin Korunması ve Lekelenmeme Hakkı Açısından Vergi Mahremiyeti*, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Cilt 30, Sayı 2, s. 727-753.
- Ezgi Alımcı (2022) *Kişisel Verilerin Korunması Hukuku ve Bankaların Güven Kuruluşu Olarak Kabul Edilmesi Kapsamında Banka Bünyesinde Gerçekleşen Veri İhlalinin Değerlendirilmesi*, Ankara Barosu Dergisi, Cilt 80, Sayı 1, s. 47-76.
- Gaye Tuğ Levent (2022) *Sosyal Medyada Çocuğun Kişilik Hakkı İhlaline Karşı Çocuğun Unutulma Hakkı*, Van Yüzüncü Yıl Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 40. Yıl Özel Sayısı, s. 56-77.
- Hüseyin Can Aksoy (2022) *Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme*, Kişisel Verileri Koruma Dergisi, Cilt 4, Sayı 2, s. 69-87.
- İrfan Ertekin (2022) *Kamu Yönetimi ve Halkla İlişkiler Yönüyle Kişisel Verilerin Korunması Kanunu (KVKK)*, Ombudsman Akademik, Cilt 8, Sayı 16, s. 39-67.
- Kübra Kaya (2022) *Özel Hayatın Gizliliği Hakkı ile Kişisel Verilerin Korunması Hakkı Bağlamında Ortaya Çıkan Bir Hak Olarak Unutulma Hakkının Değerlendirilmesi*, Türkiye İnsan Hakları ve Eşitlik Kurumu Akademik Dergisi, Cilt 5, Sayı 8, s. 177-196.
- Mehmet Ali İnceefe, Abdulkerim Oğuzhan Alkan, Alper Tanrısever (2022) *Doğmamış Bebeklerin ve Ölmüş Kişilerin Kişisel Verilerinin Korunmasında Düzenleyici Yaklaşımlar*, Bilişim Teknolojileri Dergisi, Cilt 15, Sayı 3, s. 331-338.
- Miray Özer Deniz, Memet Turan Özer (2022) *Biyometrik Verilerin İşlenmesinin Yargı Kararları Işığında Değerlendirilmesi*, Çukurova Üniversitesi Hukuk Araştırmaları Dergisi, Sayı 1, s. 92-110.
- Nurcan Diri, Bahattin Yalçınkaya (2022) *Blokzincir Uygulamalarında Kişisel Veri Problemi: Depolama Riskleri ve Öneriler*, Bilgi Yönetimi, Cilt 5, Sayı 1, s. 47-67.
- Oğuzhan Yeşiltuna, *Türkçe Hukuk Yazınında Kişisel Verilerin Korunması Üzerine Bir Araştırma (2000-2020)*, Kişisel Verileri Koruma Dergisi, Cilt: 4, Sayı: 1, s. 25-37.

- Ozan Akman, Naz Calay (2022) *Birleşme Devralma Süreçlerinde Due Diligence Aşamasının Kişisel Verilerin Korunması Hukuku Paralelinde Değerlendirilmesi*, *Kişisel Verileri Koruma Dergisi*, Cilt 4, Sayı 2, s. 19-33.
- Ömer Özkaya, İbrahim Toprak (2022), *Anayasa Mahkemesi Kararları Işığında Bir İnsan Hakkı Olarak Kişisel Verilerin Korunması*, *Sayıştay Dergisi*, Cilt 33, Sayı 124, s. 71-99.
- Öykü Beste Bayram, *Bir Uyum Aracı Olarak Veri Koruma Etki Analizinin Türk Hukuku Bakımından Değerlendirilmesi*, *Kişisel Verileri Koruma Dergisi*, Cilt: 4, Sayı: 1, s. 38-53.
- Salih Tayfun İnce (2022) *European Union Law and Mitigation of Artificial Intelligence-Related Discrimination Risks in the Private Sector: With Special Focus on the Proposed Artificial Intelligence Act*, *Annales de la Faculté de Droit d'Istanbul*, Sayı 71.
- Sevgi Erarslan (2022) *Bilgi Edinme Hakkı ve Kişisel Verilerin Korunması Hakkı: Çatışma mı Yoksa Sıkı Bir İşbirliği Mi?*, *BUHFD*, Cilt 12, Sayı 206, s. 287-318.
- Tuğçe Kaya (2022) *İş Görüşmeleri Sürecinde Aday İşçinin Kişisel Verilerinin Korunması*, *Kişisel Verileri Koruma Dergisi*, Cilt 4, Sayı 2, s. 34-47.
- Uğur Orhan (2022) *Kişisel Verilerin Korunmasına İlişkin Türk Ceza Hukuku Düzenlemeleri Üzerine Değerlendirmeler*, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, Cilt 70, Sayı 4, s. 1359-1384.
- Ünal Yıldız, *Habeas Data Kavramı ve Arjantin Örneği*, *Kişisel Verileri Koruma Dergisi*, Cilt: 4, Sayı: 1, s. 1-13.
- Yasin Aydoğdu (2022) *Mobil Uygulamalarda Kişisel Verilerin İşlenmesi ve Yasal Olarak Dikkat Edilmesi Gereken Hususlar*, *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, Cilt 26, Sayı 1, s. 399-425.

Raporlar

2014

- Ahmet Ceran (2014) *Kişisel Verilerin Korunması: Avrupa ve Türkiye*, Cilt s. 8, İKV.
- Leyla Keser, Mehmet Bedii Kaya, Batu Kınıkoğlu, Ussal Şahbaz, İdil Bilgiç Alpaslan, Ali Sökmen (2014) *Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi*, İstanbul Bilgi Üniversitesi, TEPAV.

2017

- Ayşe Nur Akıncı (2017) *Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi*, Cilt s. 37, Kalkınma Bakanlığı.

2019

- TBV (2019) *Kişisel Verilerin Korunması Hukuku ve Blokzinciri Teknolojisi Raporu*.

2020

- Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü (2020), *Kişisel Verilerin Korunmasına İlişkin Düzenlemeler Çerçevesinde Uluslararası Veri Aktarımı Yeni Gelişmeler ve Uygulamaya İlişkin Hukuki Değerlendirmeler, Veri Aktarımı Raporu*.

Mevzuat Derlemeleri

2018

- Hakan Tokbaş (2018) *Kişisel Verilerin Korunması Kanunu ve İlgili Mevzuat*, Aristo.
- Mustafa Afyonluoğlu (2018) *Kişisel Veriler Mevzuatı*, afyonluoglu.org.

2019

- Mehmet Bedii Kaya, Furkan Güven Taştan (2019) *Kişisel Veri Koruma Hukuku: Mevzuat-İçtihat-Bibliyografya*, On İki Levha.

2020

- Bora Gemicioğlu, Zeynephan Gemicioğlu (2020) *Kişisel Verilerin Korunması Mevzuatı Uluslararası Düzenlemeler ve İçtihatlar*, 2. Baskı, On İki Levha.

2021

- Murat Volkan Dülger (2021) *Bilişim, Kişisel Verilerin Korunması ve İnternet İletişimi Mevzuatı*, 7. Baskı, Seçkin.
- Hürriyet Sümer, Ülkemdeniz Kala (2021) *Kişisel Verilerin Korunması Mevzuatı*, Platon Hukuk.

2022

- Mehmet Bedii Kaya, Furkan Güven Taştan (2022) *Kişisel Veri Koruma Hukuku: Mevzuat-İçtihat-Bibliyografya*, çevrimiçi yayın.
- Ömrüncegül İçöz Koyuncuoğlu, Melis Ulusel, Tuğçe Bozkurt (2022) *Kişisel Verileri Koruma Kurulu Kararları-31 Aralık 2021 Tarihi İtibariyle Yayınlanmış Karar Özetleri ve Anahtar Kelimeler*, 2. Baskı, On İki Levha.

